SMG-1016M, SMG-2016

Operation manual, firmware version 3.10.1

Digital gateway

SMG-1016M Firmware Version: V. 3.10.1.2530
SMG-2016 Firmware Version: V. 3.10.1.2530

SIP adapter version: 3.10.1.18

Document version	Firmware version	Issue date	Revisions
Version 3.5	V.3.10.1	23.07.2018	Added: — edit identifier of the link for V5.2; — own subscribers via PRI; — RADIUS servers aggregation into groups for different servers usage in RADIUS profiles; — an opportunity to send non-modified CgPN or CdPN in User-Name to RADIUS independent from assigned CgPN and CdPN modifiers; — an option to ignore HOLD indication in SS7 linkset settings; — "Blacklist" VAS (for SMG-2016); — "Do not disturb" VAS (for SMG-2016); — NTP server; — NTP servers advertisemnt through DHCP.
Version 3.4	V. 3.10.0	06.12.2017	Changed: — the section "fail2ban" has been renamed to "dynamic firewall"; — the section " firewall profiles" has been renamed to "static firewall"; — rules of blocking in dynamic firewall has been separated for different services. Added: — numbers modification while dial plan changing ; — delayed applying of configuration changes in dial plans; — the mask "exception" when a number is selected; — an opportunity to set the description of a trunk group; — automatic uploading of configuration via FTP and TFTP protocols; — transmission of requests to RADIUS according to selection by modifiers tables; — transmission of subscriber IP address to RADIUS in Framed-IP-Address attribute; — settings of SNMP notifications on RADIUS requests; — BLF and intercom configuring while subscriber configuration via SNMP; — access to call records according to call records category; — automatic uploading of call records to FTP; — call recording to USB storage; — a name of recorded call contains a dial plan; — hop counter settings in SS7 linksets; — Location Number modification; — SIP headers transit; — optional display-name filling when a call without display-name is received; — automatic gain management; — notification of subscribers by recorded message; — SIP subscribers authorization only via IP address; — settings of subscriber displayed name and priority of using configured name; — traceroute functions.
Version 3.3	V. 3.9.0	31.07.2017	Added — new V5.2 LE protocol; — new VAS types: access to intercity calls via password, password activation, outgoing calls restriction (Appendix I. Working with VAS services); — copying of prefixes among dial plans (3.1.6 Dial plans); — selection of egress RADIUS profile in SIP interface settings (section 3.1.7.3.1.1 SIP interface settings tab); — opportunity to change order of SIP interfaces in the list; — selection of dial plan in Dial block of IVR scenario; — opportunity to download MIB files from the device;

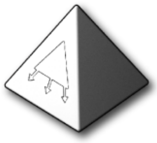
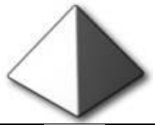
			– local GateKeeper operation description.
Version 3.2	V. 3.8.0	09.01.2017	Added – Time rounding selection for RADIUS parameters; – Conversation record file name transmission in RADIUS parameters; – 'Clear All' service management through RADIUS for dynamic subscribers; – # and * usage in IVR select blocks; – The quantity of numbering plans has been extended to 255 on SMG-2016[1]; – Common prefix creation for all pickup groups; – Number modifiers testing; – Selective E1 stream assignment from SS7 linksets to different trunk groups; – SS7 channel continuity testing through the WEB interface; – If SIP RURI and To fields has a distinction, Redirecting and Original Called numbers issuing will be disabled; – Diversion field can be issued in SIP URI format; – + symbol transmission can be disabled for international numbers; – subnet address assignment for incoming calls is available in SIP interface configuration; – DTMF transmission by SIP NOTIFY (Cisco DTMF); – Incoming and outgoing calls restrictions can be configured separately for SIP subscribers; – Language selection and saving based on browser configurations and user selection; – Call hold in incoming trunk with automatic connection via alternative route, in case of connection loss; – INVITE duplication to SMS receiver server; – SMS receiving via SMPP, then transmission via SIP to SMS server. Changed – All IVR settings were moved to IVR configuration tab – 'IVR Caller Info' block keeps initial subscriber's name , if it is out of the number mask (initial name was deleted in previous firmware versions)
Version 3.1	V.3.7.0	26.08.2016	Added: – Setting of SM-VP submodule usage – Customizable set of CDR fields – List of CDR fields is extended – Restriction of call duration on prefix – Optional outgiving a MOH in settings of trunk group – Setting a BLF monitoring group – New options of SIP headers for general loudspeaker system (intercom)
Version 3.0	V.3.6.0	14.06.2016	Added: – Intercom and paging calls – Restriction for quantity of calls (CPS) at trunks – Fault indication for CPS limit exceeded at trunks – SS7 signal link management via web configurator – SS7 (CIC) channel management via web configurator – RADIUS profile selection for outgoing communications in trunk group settings – 'Local ringback for early-media' option QSIG tunneling protocol in SIP (SIP-Q)
Version 2.9	V.3.5.1	04.04.2016	Added: – P-Early-Media support (RFC5009).
Version 2.8	V.3.5.0	21/03/2016	Added: – Voice notification on conversation recording start – WEB, TELNET, SSH intrusion protection in Fail2ban – Configurable Q.850 release causes list for redundant trunk group transition – Detection of * and # digits as a flash; – Conference assembly with the consequent assembly with re-INVITE with sendonly flag – RADIUS-acct optional sending to both connection branches – Dial plan name is displayed in settings tree – Text description for each modification rule – Changed mask order in prefix and modifier table – Caller ID request in trunk group for incoming communication – Call duration optional rounding up or down in CDR – Configuration file upload in format cfg_${dev-name}_YYYYMMDD.yaml – RFC6432 'Carrying Q.850 Codes in Reason Header Fields in SIP (Session Initiation Protocol) Responses' support – VLAN configuration on switch for SMG-2016
Version 2.7	V.3.4.2	06.11.2015	Added: – Call hold/release by pressing *, # – Optional AV-Pair Class usage for SS7 subscriber category transmission – Extended T303 timer for Q.931 protocol to 40sec – Reduced T301 lower timer limit for Q.931 protocol to 30sec
Version 2.6	V.3.4.0	03.09.2015	Added: – Configuration of CDR file creation mode

[1] Available only under VAS license

			– Configuration of CDR data storage directories – Ability to add disconnection initiator tag to CDR – IVR scenario prefix type – Pickup group prefix type – Clear Channel configuration – Clear Channel override configuration – Clear Channel-transit configuration – local direction configuration for trunk – Caller dial plan and mask configuration for call group
Version 2.5	V.3.3.0	21.05.2015	Added: – Per-core CPU monitoring – SIP response list for redundant trunk group transition – 'Redirecting number' usage in call forwarding – New call group operation modes – REC and Caller Info blocks in IVR scenarios – Blocking by fail2ban addresses list – Original or processed numbers transmission in RADIUS messages – RADIUS- Authorization transmission during local redirection – Time transmission in UTC format in RADIUS-Accounting messages – Playing of standard voice message phrases upon receiving denial message from RADIUS server with a reason for denial
Version 2.4	V.3.2.1	30.03.2015	Added: – IVR scenario configuration – Storage path for IVR scenarios and audio – Storage media information – Conference with consequent assembly and assembly by the list – Conference prefix type – IVR scenario prefix type
Version 2.3	V.3.2.0	28.10.2014	Added: – Call Group and Pickup Group prefix type – 'Send up to 15 digits to IAM' and 'Check presence of Redirecting/Original Called in incoming redirection' options in SS7 link set settings – 'Transitional registration' option in SIP interface – Configuration of call groups – Configuration of pickup groups – Ability to define gateway for network interfaces – Dynamic subscriber group configuration
Version 2.2	V.3.0.0	02.09.2014	Added: – Global Dual Homing port redundancy – Ability to select Ethernet port operation mode – Device firmware update via FTP – 'NAT keep-alive' option in SIP profile – https connection option
Version 2.1	V.2.15.02	02.05.2014	Added: – Emergency phasing in case of a single signal link in linkset – Fault indication when opposite device is not available via SIP – Caller category transmission via SIP in cpc and cpc-rus fields – Restriction for optional field transmission in SIP messages – VAS timeouts – SS7 timers – Conversation recording feature
Version 2.0	V.2.15.01	07.02.2014	Added: – VAS configuration – VAS operation application – Radius call management configuration
Version 1.12	V.2.14.02	12.12.2013	Added: – LACP settings – Configuration for dialing digits transmission to IAM during overlap – Configuration for minimum subscriber registration interval – DTMF RFC2833 PT transmission
Version 1.11	V.2.14.01	10.10.2013	Added: – H.323 protocol operation support – Q.850-causes and SIP-replies match table configuration – Scheduled routing configuration – RTP port range configuration – FTP server configuration – Firewall profile configuration – Voice message usage configuration – Device selection for fault logging – View submodule link connection information – SMG connection method example for operation in SS7 quasi-associated mode via PBX with STP features.

			– SMG connection method example for operation in combined mode – Appendix. Voice messages and music on hold (MOH).
Version 1.10	V.2.12.01	20.05.2013	Added: – Appendix 'Guidelines for SMG operation in public network'
Version 1.9	V.2.12.01	1.04.2013	Added: – Network services section — Configuration of NTP, DHCP, SNMP parameters and allowed address list in separate section – Assigning system parameters – E1 channel monitoring – VoIP submodule monitoring – Trunk direction configuration – Original CdPN and RedirPN modifiers – Q.931 timer configuration – Device access restriction settings – Incoming or outgoing communication restriction for subscriber – Configuration of network interface for signal SIP messages and voice traffic reception and transmission
Version 1.8	V.2.11.02	09.01.2013	Added: – Expanded list of E1 stream monitoring parameters – SFP module monitoring – Fault state monitoring – Alarm events list – MTP3 (DPC-MTP3) destination point code function support – ISUP (DPC- ISUP) destination point code function support – Dial plan wildcard search – NAT (comedia mode) for SIP operation via NAT – VPN/PPTP interface configuration – Creation of list of allowed addresses used for device connection – Trace filters: – restriction on number of simultaneous calls for subscriber
Version 1.7	V.2.10.04	20.09.2012	Added: – Modifier table configuration in separate menu – Modifier selection from table during cdr configuration – Modifier selection from table during pbx record configuration – Modifier selection from table during RADIUS record configuration – Modifier selection from table during trunk group configuration
Version 1.6	V.2.10.02	20.08.2012	Added: – Fail2ban settings – CPU utilization monitoring – Modifier operation examples – Configuration of SIP interface registration parameters – View list of addresses issued via DHCP – STUN server settings – Digest authorization settings – SIP subscribers group editing
Version 1.5	V.2.9.05	20.03.2012	Added: – PBX profiles for SIP subscribers – Additional settings for CDRs (redirection tags, redirecting number) – Separate interface for RADIUS message exchange
Version 1.4	V.2.9.03	28.12.2011	Added: – Maximum number of trunk groups and SIP interfaces increased up to 64 – SNMP trap configuration – DHCP server management – IP-MAC address binding – Apply/confirm switch settings w/o gateway reboot – Apply/confirm VLAN settings w/o gateway reboot – Subscriber number availability check against configured SIP subscriber database – Availability check for routing by number – Ability to read CDR from local drives – Reception monitoring for media traffic coming from the specific IP
Version 1.3	V.2.1.01	3.11.2011	Added: – CDR configuration
Version 1.2	V.2.1.01	21.10.2011	Bugfixes
Version 1.1	V.2.0.10	10.10.2011	Added: — DHCP server settings – Received/transferred signal volume settings
Version 1.0	V.2.0.10	12.09.2011	First edition

CONVENTIONAL SYMBOLS

Symbol	Description
Calibri	Notes, warnings, chapter headings, titles, table titles are written in bold.
Calibri	Important information is written in italic.
`Courier New`	Command entry examples, command execution results and program output data are written in Courier New semibold.
<KEY>	Keyboard keys are written in upper-case and enclosed in angle brackets.
	Analogue phone unit icon
	SMG digital gateway icon
	Softswitch ECSS-10 software switch icon
	Digital subscriber PBX icon
	Network Connection icon
	Optical transmission medium

Notes and warnings

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

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

TARGET AUDIENCE

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

TABLE OF CONTENTS

INTRODUCTION

Today, means of communication utilizing state-of-the-art hardware and software solutions evolve rapidly. At that, the following problem arises: how to implement new communication devices that utilize alternative data transmission principles into existing communication networks. The solution is to use special equipment that interconnects the diverse network segments. Currently, such equipment is represented by digital gateways. They allow for gradual transition from existing communication networks to more efficient ones that utilize alternative operation principles.

At present, IP networks are considered to be the most efficient as they are weakly related to the data transfer environment or data type and also flexible and manageable. Designed and manufactured by Eltex, SMG digital gateway allows for the interfacing of traditional communication networks based on the circuit-switching principle with communication networks used packet-switching data transmission.

This operation manual details main features of SMG-1016M and SMG-2016 digital gateways. In this document you will find technical specifications of the gateway and its components. Also, it contains an overview of the operation procedure and software-based maintenance.

1 DEVICE DESCRIPTION

1.1 Application

Digital gateways SMG-1016M and SMG-2016 allow for the interfacing of PSTN (E1) signalling and media streams and VoIP networks, and also perform media gateway functions (codec conversion, conference call establishing, tone signal/DTMF reception and generation, voice message output).

SMG supports up to 16 E1 paths, up to 495 E1-side and 768 VoIP-side voice (media) links (when G.711 codec is used with packetization time 20ms or greater).

Submodule gateway design allows for flexible capacity alteration, and the minimum module type quantity makes it easier to expand and upgrade the system.

SMG is an optimal and robust solution for telecommunication infrastructure upgrade, development and migration from PSTN to NGN.

SMG main specifications:

- Number of E1 interfaces: 4 to 16, in increments of 4
- Up to 768 VoIP channels (128 channels in TDM for connecting to a single submodule)
- Number of Ethernet ports for SMG-1016M:
  - 3 x 10/100/1000BASE-T ports
  - 2 x 1000-Base-X (SFP) ports
- Number of Ethernet ports for SMG-2016:
  - 4 x 10/100/1000BASE-T ports
  - 2 x 1000-Base-X (SFP) combo-ports
- Static address and DHCP support
- DNS server
- VoIP protocols: SIP, SIP-T, SIP-I, H.323, MGCP[1], MEGACO[1], SIGTRAN[1]
- TDM protocols: ISDN PRI(Q.931), QSIG and CORNET for subscriber name transmission, SS7 (associated and quasi-associated modes operation), V5.2;
- SIP subscriber registration support:
  - Up to 2000 for SMG-1016M
  - Up to 3000 for 2016
- DTMF transmission (SIP INFO, RFC2833, in-band, SIP NOTIFY)
- Echo cancellation (G.168 recommendation)
- Voice activity detector (VAD)

[1] Not supported in the current firmware version

- Comfortable noise generator (CNG)
- Adaptive or fixed jitter buffer
- V.152 data transmission
- fax transmission:
  - G.711 pass through
  - T.38 UDP Real-Time Fax
- NTP support
- DNS support
- SNMP support
- Bandwidth and QoS restriction for SMG-1016M
- ToS and CoS for RTP and signalling
- VLAN for RTP, signalling and management
- Firmware update: via 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 3398 ISUP/SIP Mapping;
- 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 3666 SIP to PSTN Call Flows;
- 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;
- SIP/SIP-T/SIP-I interaction;
- SIP Enable/Disable 302 Responses;
- Delay offer;
- SIP OPTIONS Keep-Alive (SIP Busy Out);
- NAT support (comedia mode);
- SIP registrar (optional).

1.2 Typical Application Diagrams

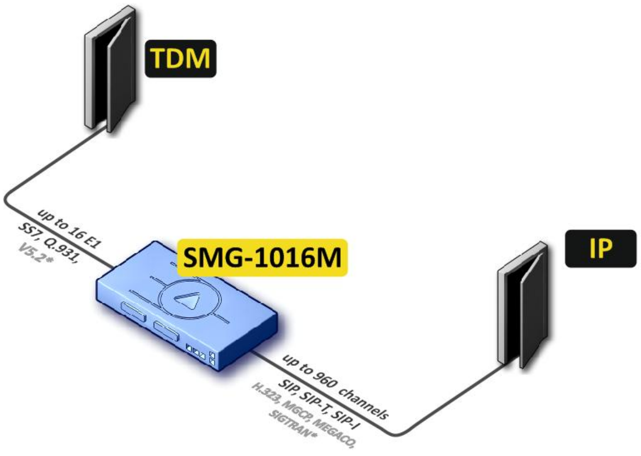
This manual covers several SMG device connection methods:

Interfacing of TDM and VoIP network signalling and media streams

In this configuration, device enables connection for up to 16 E1 streams with various signalling protocols (SS7, ISDN PRI/QSIG/CORNET, V5.2[1]) and maintenance for up to 768 channels uncompressed (G.711 codec), up to 432 channels compressed (G.729 A / 20-80), or 324 T.38 fax channels.

Device connects to the IP network via 10/100/1000 BASE-T network interface using H.323/SIP/SIP-T/ SIP-I protocols.

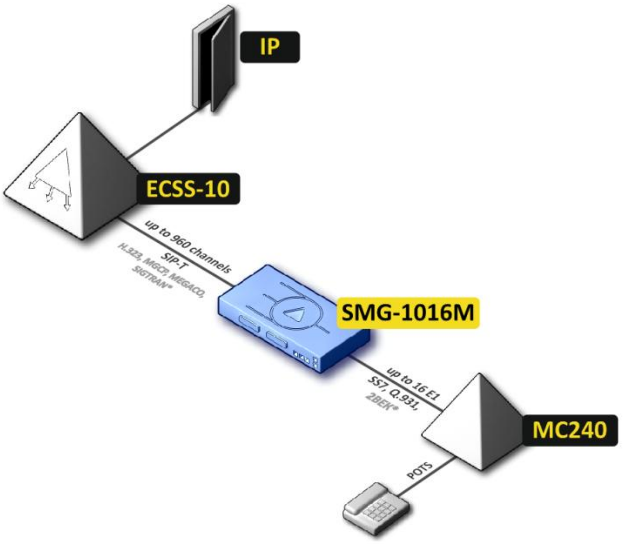
[1] Not supported in the current firmware version.



* — Not supported in the current version

Fig. 1 — Interfacing of TDM and VoIP network signalling and media streams

Fig. 2 shows TDM and VoIP network interfacing example on interaction between MC240 digital PBX and ECSS-10 software switch.



* — Not supported in the current version

Fig. 2 — Interfacing of TDM and VoIP network signalling and media streams

1.2.1 *Mini IP-PBX*

In this configuration, device allows for registration of up to 2000 subscribers for SMG-1016M and up to 3000 for SMG-2016 as well as the interaction with PSTN network via 16 E1 streams with various signalling protocols (SS7, ISDN PRI/QSIG/CORNET, V5.2).

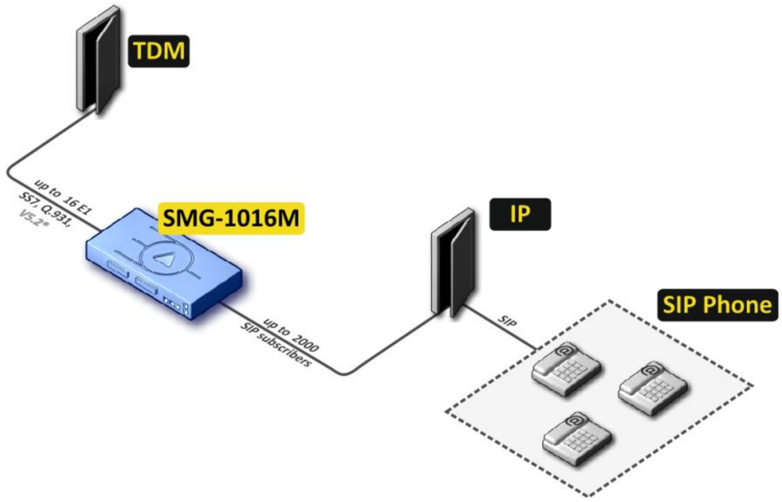


Fig. 3 — Mini IP-PBX based on SMG-1016M

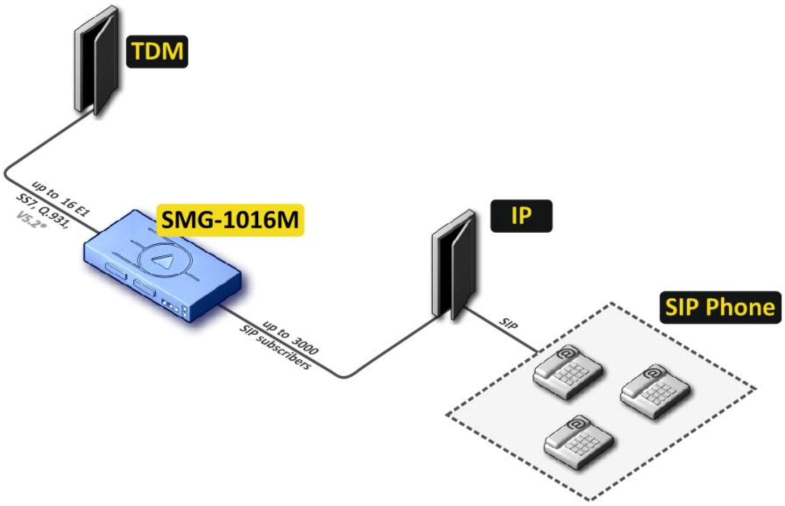


Fig. 4 — Mini IP-PBX based on SMG-2016

1.2.1 *Outstation via V5.2*

The activation of additional features of IP PBX ECSS-10 software module allows to arrange digital loop carrier via V5.2 and to service up to 2000 subscribers through SMG-1016M and up to 3000 subscribers through SMG-2000 with support for wide VAS set. You may use equipment supporting V5.2 of any manufacturer as an outstation.

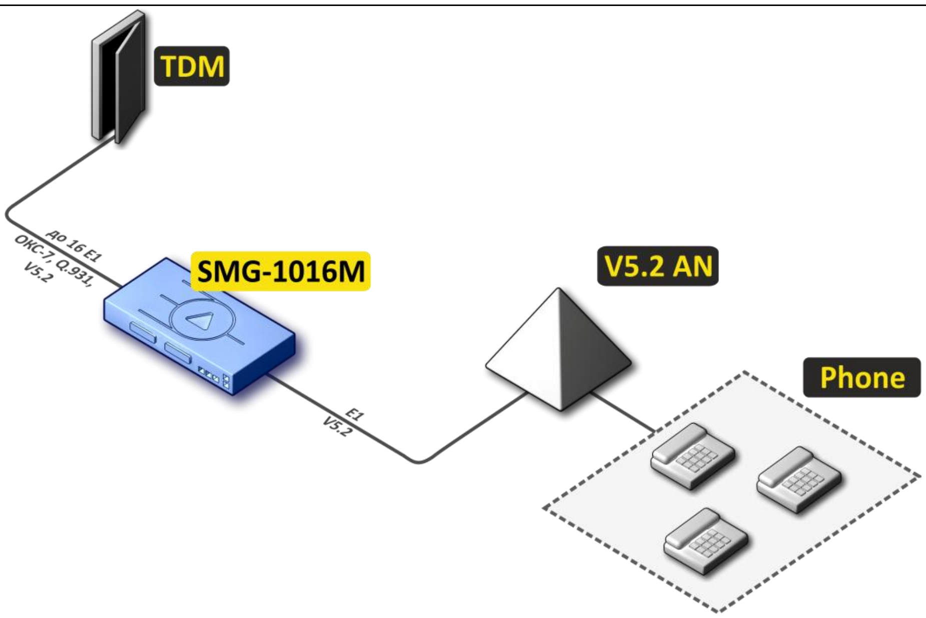


Fig. 5 – V5.2 AN outstation based on SMG-1016M

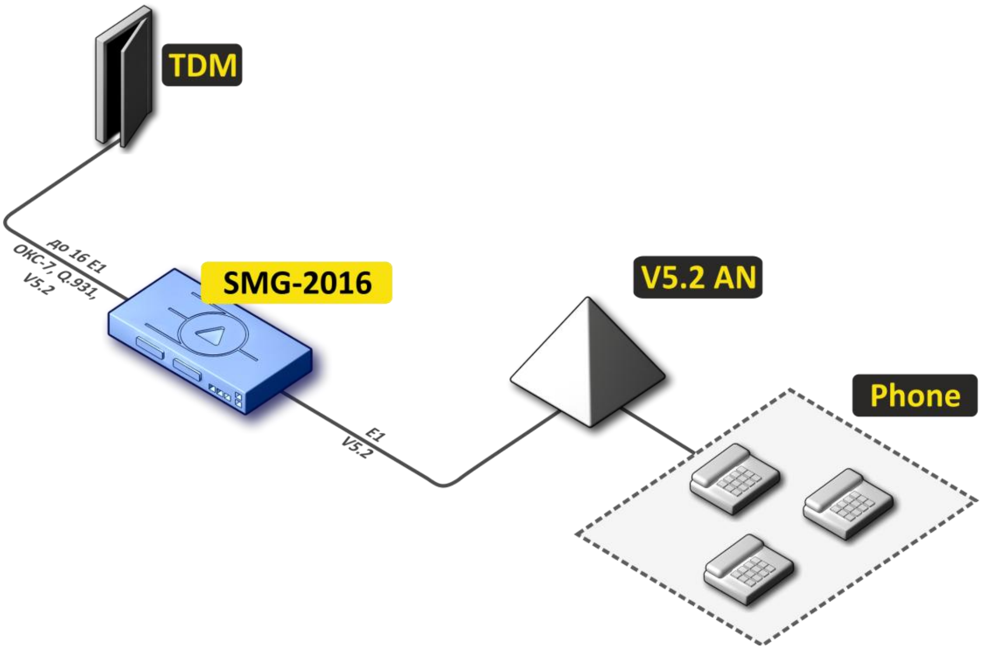


Fig. 6 – V5.2 AN outstation based on SMG-2016

1.3 Device Design and Operating Principle

1.3.1 SMG-1016M Design

SMG-1016M features submodule architecture and contains the following elements:

- Controller featuring:
  - Controlling CPU
  - Flash memory: 64Mb
  - RAM: 512Mb
- Up to 4 E1 stream submodules C4E1
- Up to 6 IP submodules SM-VP-M300
- Ethernet switch (L2), 3 x 10/100/1000BASE-T ports, 2 x MiniGBIC (SFP) ports
- Switch fabric
- Phase-lock-loop (PLL) frequency control system

The figure below shows SMG-1016M functional chart.

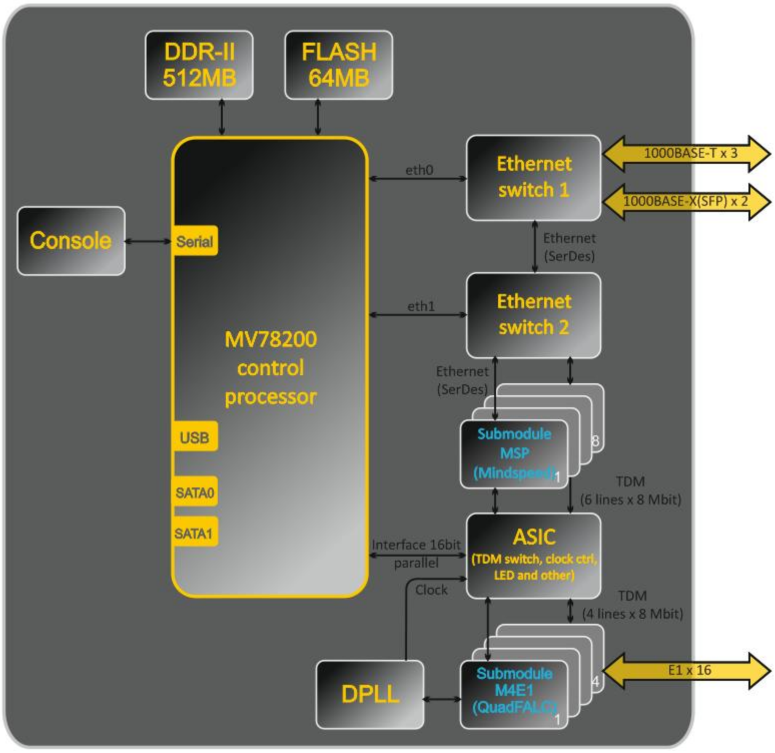


Fig. 7 — SMG-1016M functional chart

1.3.2 SMG-2016 Design

SMG-2016 features submodule architecture and contains the following elements:

- Controller featuring:
  - Controlling CPU
  - Flash memory: 1024 MB
  - RAM: 4096 MB
- Up to 4 E1 stream submodules C4E1
- Up to 6 IP submodules SM-VP-M300
- Ethernet switch (L2), 4 x 10/100/1000BASE-T ports, 2 x MiniGBIC (SFP) combo ports
- Switch fabric
- Phase-lock-loop (PLL) frequency control system

The figure below shows SMG-2016 functional chart.

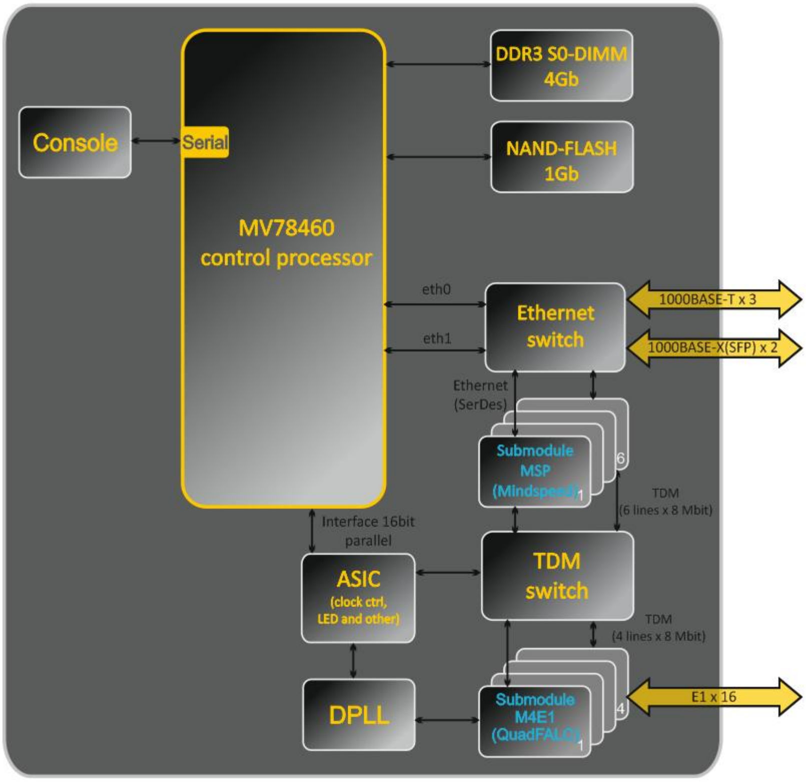


Fig. 8 — SMG-2016 functional chart

1.3.3 SMG Operating Principle

In TDM-IP direction, signal coming to E1 streams is transferred to VoIP submodule audio codecs (6 lines x 128 TDM channels) via the intrasystem backbone to be encoded using one of the selected standards and transferred further in the form of digital packets to the Ethernet switch. In IP-TDM direction, digital packets coming from Ethernet switch are transferred to VoIP submodules to be decoded and transferred further to E1 streams via the intrasystem backbone.

External 2 Mbps E1 streams are transmitted to framers through matching transformers. At that, synchronization signal is extracted from the stream and fed to the common synchronization line of the device. Synchronization line priority management is performed at the software level according to the defined algorithm.

Switch fabric is integrated into the intrasystem backbone and enables communication between the E1 (C4E1) and VoIP (SM-VP-M300) submodules.

For device firmware architecture, see the figure below.

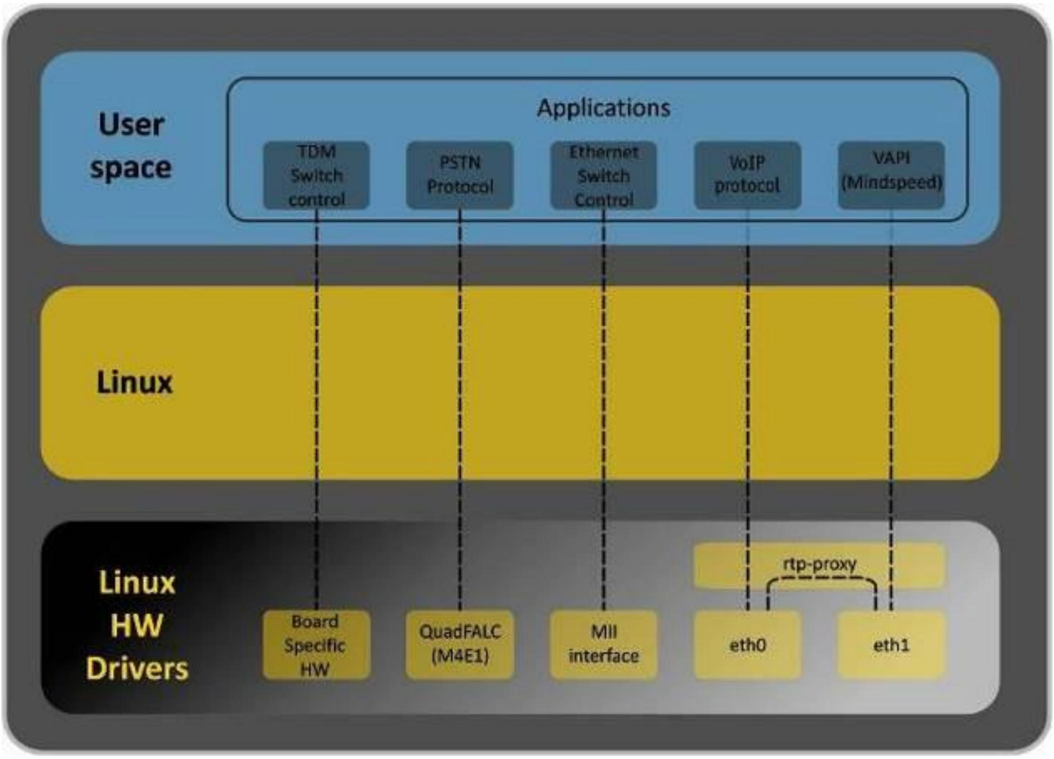


Fig. 9 — SMG firmware architecture

1.4 Main Specifications

Table below lists main specifications of the terminal.

Table 1 — Main specifications

VoIP Protocols

Supported protocols	SIP-T/SIP-I SIP SIP-Q H.323v2/v3/v4 MGCP[1] MEGACO SIGTRAN (M2UA, IUA) SIGTRAN (M3UA)[1] T.38

Audio Codecs

Codecs	G.711 (A/U) G.729 AB G.723.1 (6.3 Kbps, 5.3 Kbps) G.726 (32 Kbps)

Quantity of VoIP channels supported by a submodule depending on the codec type

Codec/packetization time, ms	Channel quantity
G.711 (A/U) / 20-60	128
G.711 (A/U) / 10	112
G.729 A / 20-80	72
G.729 A / 10	62
G.723.1 (6.3 Kbps, 5.3 Kbps)	58
G.726 / 20	98
G.726 / 10	88
T.38	54
TDM channels per 1 submodule	128
Three-way conferences per 1 submodule	27

Electrical Ethernet interface specifications

No. of interfaces	SMG-1016M	SMG-2016
	3	4
Electric port	RJ-45	
Data rate, Mbps	Autodetection, 10/100/1000Mbps duplex	
Supported standards	10/100/1000BaseT	

Optical Ethernet interface specifications

No. of interfaces	SMG-1016M	SMG-2016
	2	2 combo ports
Optical port	Mini-Gbic (SFP): 1) duplex, double fiber, wave length 1310nm (Single-Mode), 1000BASE-LX (LC connector), distance — up to 10km, supply voltage — 3.3V 2) duplex, single fiber, reception/transmission wave lengths 1310/1550nm, 1000BASE-LX (SC connector), distance — up to 10km, supply voltage — 3.3V	
Data rate, Mbps	1000Mbps, duplex	
Supported standards	1000BaseX	

[1] Not supported in the current firmware version.

Console Parameters

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

E1 Interface Parameters:

No. of channels	According to ITU-T G.703,G.704 guidelines
Line data transfer rate	2048Mbps
Line code	HDB3, AMI
Line output signal	3.0V peak for 120Ω load 2.37V peak for 75Ω load (acc. to CCITT G.703 guidelines)
Entry signal from the line	From 0 to -6dB in relation to the standard output impulse
Elastic buffer	2 frame capacity
Signalling protocols	ISDN PRI (Q.931), QSIG and CORNET for subscriber name transmission, SS7, V5.2

External synchronization signal parameters

Number of synchronisation inputs	2
Cable type	Symmetric 2-wire line (twisted pair)
Input impedance of synchronization receivers	120 Ohm
Incoming signal parameters	According to ITU-T G.703 recommendations, section 15: 2048kHz synchronization interface (T12)
Shape and frequency of incoming signal	squarewave signal 2048 kHz

General parameters

Operating temperature range		From 0 to +40°C	
Relative humidity		Up to 80%	
Power voltage		AC: 220V+-20%, 50Hz DC: -48V+30%-20% Power options: - Single AC or DC power supply - Two AC or DC power supplies with hot swapping	
Power supply		AC:	DC:
	PM designation	PM160-220/12	PM100-48/12
	PM rated power	160W	100W
Power consumption		50W max.	
Dimensions (W x H x D)		SMG-1016M	SMG-2016
		430x45x260mm	430x45x340mm
Form-factor		19" form-factor, 1U size	
Net weight	Complete device package	SMG-1016M	SMG-2016
		3.2kg	5.3kg
	Power supply	0.5kg	
	Vent panel	0.1kg	
	SATA storage device[1]	0.1kg	

[1] For SMG-2016 only

1.5 Design

1.5.1 SMG-1016M

SMG-1016M digital gateway has a metal case available for 19” form-factor rack-mount 1U shelf installation.

The front panel of the device is shown in the figure below.

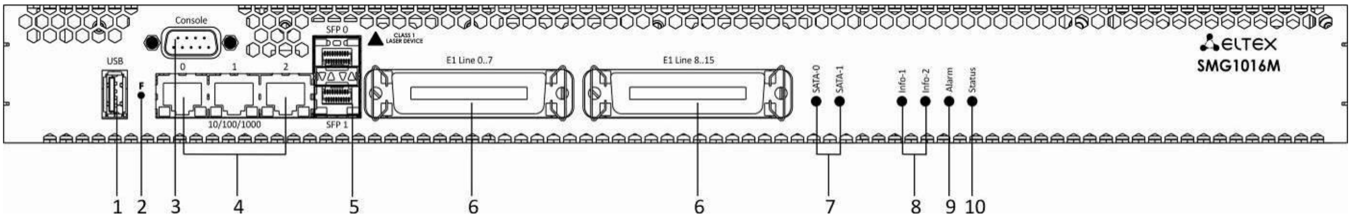


Fig. 10 — SMG-1016M front panel layout

Connectors, LEDs and controls located on the front panel of the device are listed in Table 2.

Table 2 — Description of connectors, LEDs, and controls located on the front panel

№	***Front panel elements***	***Description***
1	***USB***	USB port for external storage device connection
2	***F***	Function button
3	***Console***	RS-232 console port for local device management (for connector wiring, see Appendix A)
4	***10/100/1000 0..2***	3 x RJ-45 ports of Ethernet 10/100/1000 Base-T interfaces
5	***SFP 0, SFP 1***	2 chassis for 1000Base-X Gigabit uplink interface optical SFP modules used for IP network connection
6	***E1 Line 0..7,E1 Line 8..15***	2 x CENC-36M connectors for E1 streams connection (for connector wiring, see Appendix A)
7	***SATA-0, SATA-1***	SATA interface activity indicator
8	***Info1, Info2***	SFP optical interface activity indicator
9	***Alarm***	Device alarm indicator
10	***Status***	Device operation indicator

The rear panel of the device is shown in the figure below.

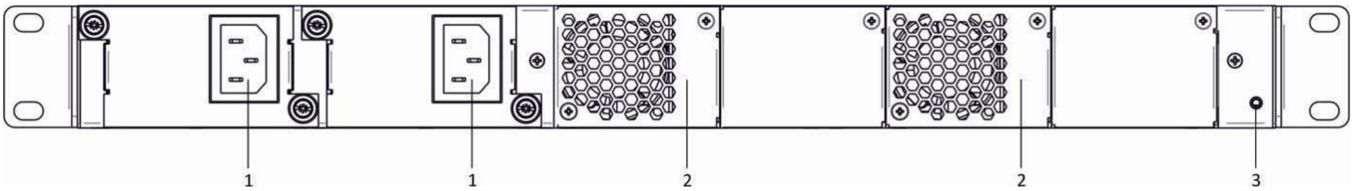


Fig. 11 — SMG-1016M rear panel layout

The following table lists rear panel connectors of the switch.

Table 3 — Description of rear panel connectors of the switch

Item	Rear Panel Element	Description
1	Power supply connector	Connector for power supply
2	Removable fans	Removable ventilation modules with hot-swapping
3	Earth bonding point ⏚	Earth bonding point of the device

1.5.2 *SMG-2016*

SMG-2016 digital gateway has a metal case available for 19” form-factor rack-mount 1U shelf installation.

The front panel of the device is shown in the figure below.

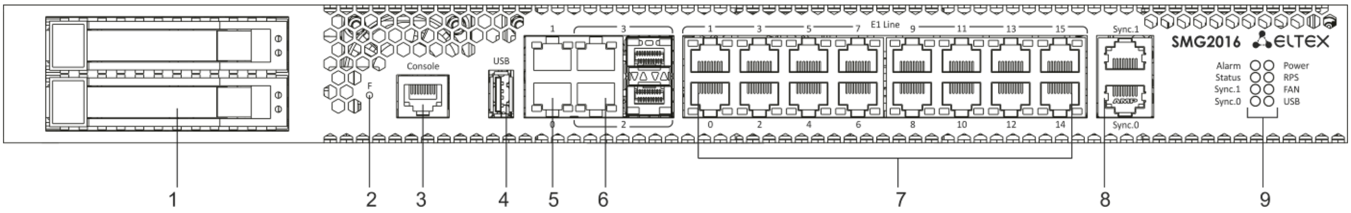


Fig. 12 — SMG-2016 front panel layout

Connectors, LEDs and controls located on the front panel of the device are listed in Table 4.

Table 4 — Description of connectors, LEDs, and controls located on the front panel

№	*Front panel elements*	*Description*
1	*SATA disk ports*	Cradle connectors for SATA drive installation
2	*F*	Function button
3	*Console*	Console port for local device management (for connector wiring, see Appendix A)
4	*USB*	USB port for external storage device connection
5	*0, 1*	2 x 10/100/1000 Base-T Gigabit uplink interface RJ-45 Ethernet connectors used for IP network connection
6	*2,3*	2 chassis for 1000 Base-X uplink interface SFP modules used for IP network connection
		2 x 10/100/1000 Base-T Gigabit uplink interface RJ-45 connectors used for IP network connection
7	*E1 Line 0..15*	16 x RJ-48 connectors for E1 streams connection (for connector wiring, see Appendix A)
8	*Sync.0, Sync.1*	2 x RJ-45 ports for connection of external synchronization sources
Indicators		
9	*Alarm*	Device alarm indicator
	Status	Device operation indicator
	Sync.1	*Sync.2* external synchronization interface operation indicator

	Sync.0	***Sync.1*** external synchronization interface operation indicator
	Power	Device power indicator
	RPS	Device aux power indicator
	FAN	Fan operation indicator
	USB	USB operation indicator

The rear panel of the device is shown in the figure below.

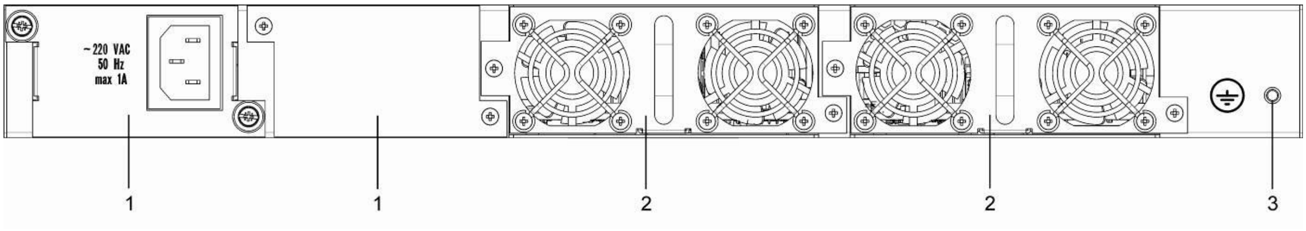


Fig. 13 — SMG-2016 rear panel layout

Table below lists rear panel connectors of the switch.

Table 5 — Description of rear panel connectors of the switch

Item	***Rear Panel Element***	***Description***
1	Power modules	Modules with connector for power supply
2	Fan panels	Removable ventilation modules with hot-swapping
3	Earth bonding point ⏚	Earth bonding point of the device

1.6 LED Indication

LED indicators located on the front panel represent the current state of the device.

1.6.1 Device light indication in operation

1.6.1.1 SMG-1016M

For device light indication in operation, see Table 6.

Table 6 — Light indication of the device status in operation

Indicator	***Indicator State***	***Device State***
Info1	Off	SFP0 link lost
	Lights green	SFP0 link in operation
Info2	Off	SFP1 link lost
	Lights green	SFP1 link in operation
	Lights red	Device starts up
Alarm	Flashes red	Critical device failure
	Lights red	Non-critical device failure

	Lights yellow	No failures, non-critical warnings
	Lights green	Normal operation
Status	Lights green	Normal operation
	Off	Device power lost

1.6.1.2 SMG-2016

For device light indication in operation, see Table 7.

Table 7 — Light indication of the device in operation

Indicator	***Indicator State***	***Device State***
Alarm	Flashes red	Critical device failure:
	Lights red	Non-critical device failure
	Lights yellow	No failures, non-critical warnings
	Lights green	Normal operation
Status	Lights green	Normal operation
	Off	Device power lost
Sync.0, Sync.1	Lights green	Synchronization with an external source
	Off	External synchronization source disconnected
Power	Lights green	Powered by Power supply no.1
	Lights orange	Power supply no.1 is installed, but not energized
RPS	Lights green	Power supply no.2 is installed and energized
	Lights red	Power supply no.2 is installed, but not energized
	Off	Power supply no.2 is not installed
FAN	Lights green	All removable fan modules are installed, all fans are operational
	Lights orange	All removable fan modules are installed, some fans are down
	Lights red	Single or both removable fan modules are not installed
USB	Lights green	USB flash is installed
	Off	USB flash is not installed

1.6.2 LED indication of E1 stream status

For LED indication of E1[1] stream status, see Table 8.

Table 8 — Indication of E1 stream status

0-15 x RJ-48 ports	**Indication (flashing period)**		
Status	**Red**	**Yellow**	**Green**
E1 is disabled in the gateway configuration	Off	Off	Off
E1 stream failure state	Flashes (200ms)	Off	Off
Loss of signal (LoS)	On		
AIS failure	On	Flashes (200ms)	Off
LOF failure	On	On	Off
LOMF failure	On	On	Off
E1 stream normal operation	Off	Off	On
Failure on the remote host (RAI)	Off	Flashes (200ms)	Flashes (200ms)
E1 stream is in operation, there are SLIPs in the stream.	Off	Flashes (300ms)	Flashes (1500ms)
E1 stream test is being performed	Flashes (200ms)	Flashes (200ms)	Flashes (200ms)

[1] For SMG-2016 only

1.6.3 Light indication of Ethernet 1000/100 interfaces

Ethernet interface state is shown by 1000/100 socket built-in LED indicators and listed in the Table below.

Table 9 — Light indication of Ethernet 1000/100 interfaces

Device Status	*LED/Status*	
	Yellow LED 1000/100	*Green LED 1000/100*
Port operates in 1000Base-T, data transfer is inactive	Lights on	Lights on
Port is in 1000Base-T mode, data transfer	Lights on	Flashes
Port is in 10/100Base-TX mode, no data transfer	Off	Lights on
Port is in 10/100Base-TX mode, data transfer	Off	Flashes

1.6.4 Light indication during startup and reset to factory defaults

1.6.4.1 SMG-1016M

For light indication during startup and reset to factory defaults, see Table below.

Table 10 — Light indication during startup and reset to factory defaults

Item	*Indication*				*Reset to factory defaults procedure (device is on)*
	Info1	*Info1*	*Alarm*	*Status*	
1	Yellow	Yellow	Yellow	Yellow	Press and hold F button for 1 second until the following pattern appears, then release the button. The device will be rebooted in 3 seconds.
2	Green	Red	Yellow	Red	Reset to factory defaults has been initiated. This LED pattern will appear only when the device startup begins.
3	Yellow	Yellow	Yellow	Yellow	At this step, LED functionality check will be performed — all LEDs will turn on yellow including SATA-0 and SATA-1.
4	Off	Off	Green	Green	At this step, the gateway operating system will be loaded. To change network parameters and restore the device configuration to factory defaults, when the pattern appears press and hold F button for 40-45 seconds. (When you press and hold the button, pattern 2 may appear shortly; ignore it and continue holding the button until the pattern 4 appears.)
5	Yellow	Yellow	Yellow	Yellow	When the pattern appears, release F button. After a while, the following message will be displayed in the console. <<<BOOTING IN SAFE-MODE.RESTORING DEFAULT PARAMETERS>>> Reset to factory settings is complete.

Do not hold F button pressed during the device reset procedure — device operation will be halted. To resume the operation, you will have to power-on reset the device.

Also, you may perform reset to factory settings during the device startup.
In this case, skip the 1st step.

1.6.4.2 SMG-2016

For light indication during startup and reset to factory defaults, see Table below.

Table 11 — Light indication during startup and reset to factory defaults

Item	***Indication***				***Reset to factory defaults procedure*** ***(device in operation)***
	Alarm	***Status***	***Sync.1***	***Sync.2***	
1	Yellow	Yellow	Yellow	Yellow	Press and hold F button for 1 second until the following pattern appears. The device will be rebooted in 3 seconds.
2	Yellow	Red	Yellow	Yellow	Reset to factory defaults has been initiated. This LED pattern will appear only when the device startup begins.
4	-	-	-	-	At this step, the gateway operating system will be loaded. To change network parameters and restore the device configuration to factory defaults, when the pattern appears press and hold F button for 40-45 seconds.
5	Yellow	Yellow	-	-	When the pattern appears, release F button. After a while, the following message will be displayed in the console. `<<<BOOTING IN SAFE-MODE.RESTORING DEFAULT PARAMETERS>>>` Reset to factory settings is complete.

State of POWER, RPS, FAN, and USB LEDs during reset procedure can be ignored.

Also, you may perform reset to factory settings during the device startup.
In this case, skip the 1st step.

1.6.5 Fault LED Indication

The table below lists detailed description of faults represented by the status of Alarm LED.

CDR file saving indication

When FTP server is not available, CDRs will be saved to the device RAM. Storage space for CDR files amounts to 30Mb. When the memory is filled within the specific limits, the fault will be indicated.

Table 12 — Fault LED Indication

Alarm LED State	***Fault level***	***Fault description***
Flashes red	Critical	Configuration error
		SIP module loss
		SS7 link set fault (when *'Fault indication'* checkbox is selected in *'Routing/SS7 linksets'* menu)
		Stream fault (when *'Alarm indication'* checkbox is selected in *'E1 streams/Physical parameters'* menu)
		FTP server is unavailable, utilization of RAM for CDR file storage exceeds 50%
Lights red	Non-critical (errors)	SS7 link fault (when *'Fault indication'* checkbox is selected in *'Routing/SS7 linksets'* menu)
		VoIP submodule (MSP) loss
		Synchronization fault (free-run mode operation)

		FTP server is unavailable, utilization of RAM for CDR file storage is more than 15%
Solid yellow	Warnings (warning)	Remote stream fault
		Synchronization from the lower priority source (the one with the higher priority is not available)
		FTP server is unavailable, utilization of RAM for CDR file storage is more than 5%
		CPS fault threshold is exceeded for one of the trunk groups
		INVITE duplication failure received from emergency call service node

1.7 'F' button operation

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

To perform reset to factory defaults on operating device, see Section 1.6.4:Table 10, Table 11.

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

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

Next, you may save the factory configuration, restore password or reboot the device.

1.8 Saving factory configuration

To save the factory configuration:

- Reset the device to factory defaults (Section 1.6.4)
- Connect via telnet or console with login **admin**, password **rootpasswd**
- Enter ***sh*** command (device will exit the CLI mode and enter the SHELL mode)
- Enter ***save*** command
- Reboot the device using the ***reboot*** command

The gateway will be restarted with the factory configuration.

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

smg login: admin
Password: rootpasswd

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

Welcome! It is Wed Mar 11 08:45:20 NOVT 2015
SMG> sh
/home/admin # save
tar: removing leading '/' from member names
*********
*********
***Saved successful
```

```
New image 1
Restored successful
/home/admin #
# reboot
```

1.9 Password recovery

To recover the password:

- Reset the device to factory defaults (Section 1.6.4)
- Connect via Telnet, SSH, or Console
- Enter ***sh*** command (device will exit the cli mode and enter the shell mode)
- Enter ***restore*** command (current configuration will be restored)
- Enter ***passwd*** command (device will ask for a new password and its confirmation)
- Enter ***save*** command
- Reboot the device using the ***reboot*** command

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

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

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

smg login: admin
Password: rootpasswd

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

Welcome! It is Fri Jul  2 12:57:56 UTC 2010
SMG>sh
/home/admin # restore
New image 1
Restored successful
/home/admin # passwd admin
Changing password for admin
New password: 1q2w3e4r5t6y
Retype password: 1q2w3e4r5t6y
Password for admin changed by root
/home/admin # save
tar: removing leading '/' from member names
**********
**********
***Saved successful
New image 0
Restored successful
# reboot
```

1.10 Delivery Package

1.10.1 SMG-1016M

SMG-1016M standard delivery package includes:

- SMG-1016M digital gateway
- 2 x CENC-36M connectors — (if UTP CAT5E 18 pairs cable were not included in order)
- RS-232 DB9(F)–DB9(F) connection cable
- A mounting set for 19'' rack
- Operation manual (on a CD disk)
- Technical passport

If ordered, delivery package may also include:

- 2 x Mini-Gbic (SFP)
- UTP CAT5E — 18 pairs cable

1.10.2 SMG-2016

SMG-2016 standard delivery package includes:

- SMG-2016 digital gateway
- A mounting set for 19'' rack
- Operation manual (on a CD disk)
- Technical passport

If ordered, delivery package may also include:

- Mini-Gbic (SFP).

1.11 Safety instructions

1.11.1 General Guidelines

Any operations with the equipment should comply to 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 engineers should undergo special training.

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

The digital gateway can be permanently used provided the following requirements are met:

- Ambient temperature from 0 to +40°C
- Relative humidity up to 80% at +25°C
- Atmosphere pressure from 6,0x10*4 to 10,7x10*4 Pa (from 450 to 800 mm Hg)

The device should be 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.

1.11.2 Electrical Safety Requirements

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

PC and measurement instruments should be grounded prior to connection to the device. The potential difference between the equipment case and the cases of the instruments should be less than 1 V.

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

Make sure the device power sources is off, when installing or removing the case.

Power supply modules installation and removal should be conducted only when the device is powered off according to the procedure described in Section 1.12.4.

1.11.3 Electrostatic Discharge Safety Measures

In order to avoid failures caused by electrostatic discharge, we strongly recommend to wear ESD belt, shoes and wrist strap which prevent electrostatic charge accumulation (for wrist strap, make sure that it has a secure fit against the skin) and connect the cable to grounding prior to operation.

1.11.4 Power Supply Requirements

1.11.4.1 Power supply type requirements

The device should be powered by 48VDC power supply with grounded positive potential or by the remote 220VAC power supply.

1.11.4.2 Permissible voltage variation requirements for DC power supply

Permissible variations of 48VDC power supply voltage are from 40.5V to 57V.

When the power supply voltage is restored after being below the permissible threshold, the device specifications will be restored automatically.

1.11.4.3 Permissible interference requirements for DC power supply

The equipment should operate normally, when the power supply interference is below the values listed in the table below.

Table 13 — Permissible interference requirements for DC power supply

Interference type	*Value*
Permissible voltage deviation from rated value, % Duration 50ms Duration 5ms	 –20 40
Harmonical component voltage ripple, mV eff. up to 300Hz 300Hz to 150kHz	 50 7

1.11.4.4 Requirements to interference produced by equipment in power supply circuit

Voltage values of interference produced by the equipment in the power supply circuit should not exceed values listed in Table below.

Table 14 — Requirements to interference produced by equipment in power supply circuit

Interference type	*Value*
Total interference in the range of 25Hz to 150Hz, mV eff.	50
Selective interference in the range of 300Hz to 150kHz, mV eff.	7
Weighted (psophometric) interference, mV psoph.	2

1.11.4.5 AC power supply requirements

AC power supply parameters should be as follows:

- Maximum allowed voltage — 220V max.
- Power supply should feature residual current device (RCD).
- Insulation strength of AC power supply circuits against the housing should withstand at least 1000V peak (in normal conditions).

1.12 SMG Installation

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

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

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

Mount the device. The device is intended to be installed into 19" rack using the mounting set or mounted on the horizontally oriented perforated shelf.

Ground the case of the device after installation. This should be done prior to connecting the device to the power supply. An insulated multiconductor wire should be used for grounding. The device grounding and the grounding wire section should comply with Electric Installation Code. The earth bonding point is located at the right bottom corner of the side panel, Fig. 11, Fig. 13.

1.12.1 Startup sequence

1. Connect digital streams, optical and electrical Ethernet cables to corresponding gateway connectors.

   For digital stream overvoltage protection, the linear side of the distribution cross should be equipped with complex protection devices. We recommend to use KRONE complex protection plugs 'Com Protect 2/1 CP HGB 180 A1'.

2. Connect the power supply cable to the device. To connect the device to DC power supply, use the cable with cross-section not less than 1mm^2.
3. If a PC is supposed to be connected to SMG console port, connect SMG console port to PC COM port. PC should be powered off and grounded at the same point with the digital gateway.
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.

1.12.2 Support brackets mounting

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

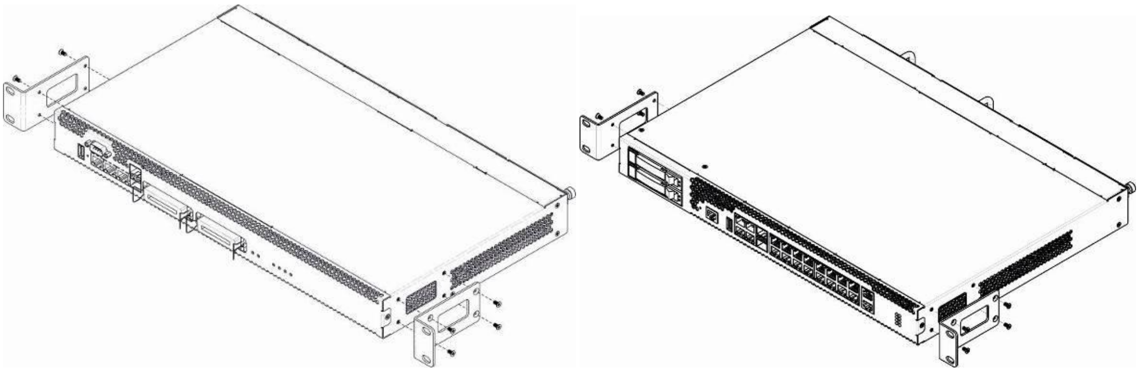


Fig. 14 — Support brackets mounting for SMG-1016M (left) and SMG-2016 (right)

To install the support brackets:

1. Align four mounting holes in the support bracket with the corresponding holes in the side panel of the device, Fig. 14.
2. Use a screwdriver to screw the support bracket to the case.

Repeat steps 1 and 2 for the second support bracket.

1.12.3 Device rack installation

To install the device to the rack:

1. Attach the device to the vertical guides of the rack.
2. Align mounting holes in the support bracket with the corresponding holes in the rack guides. Use the holes of the same level on both sides of the guides to ensure the device horizontal installation.
3. Use a screwdriver to screw the device to the rack.
4. To dismount a device, disconnect cables and remove support bracket screws from the rack. Remove the device from the rack.

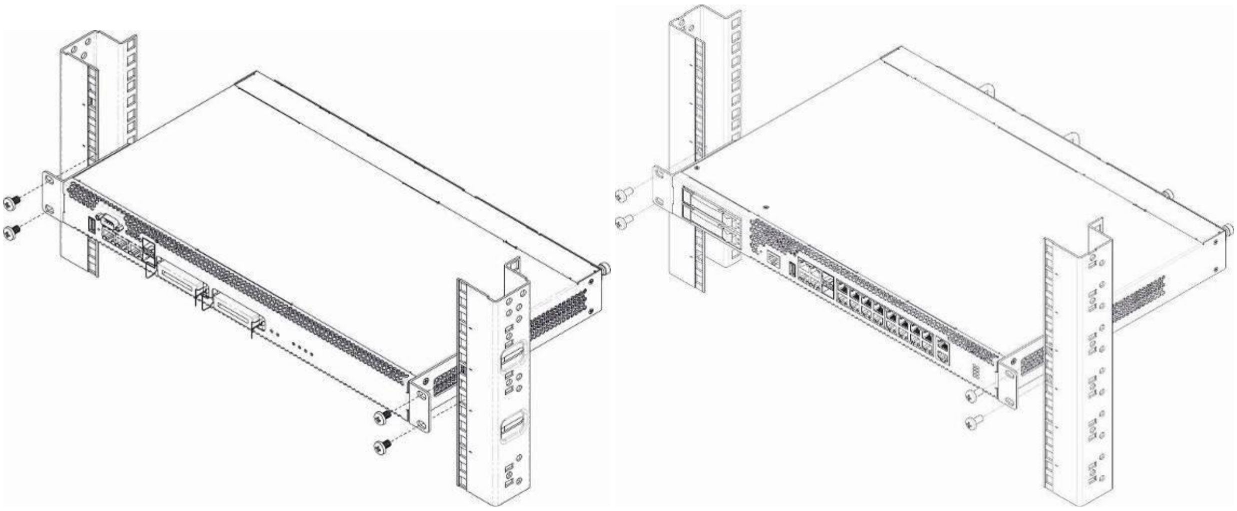


Fig. 15 — Device rack installation for SMG-1016M (left) and SMG-2016 (right)

1.12.4 Power module installation

Device can operate with one or two power modules. The second power module installation is necessary when the device operates under strict reliability requirements.

From the electric point of view, both places for power module installation are identical. In the context of device operation, the power module located closer to the edge is considered as the main module, and the one closer to the center_—_as the backup module. Power modules can be inserted and removed without powering the device off. When additional power module is inserted or removed, the device continues operation without reboot.

The device has two fuses with nominal current 3.15A. The fuses are not user-serviceable. They should be replaced by the qualified service specialists in the manufacturer's service center.

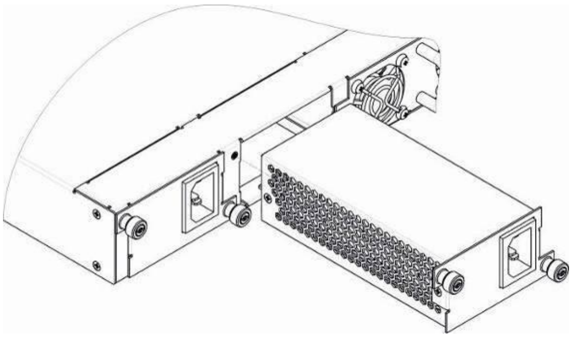


Fig. 16 — Power module installation

1.12.5 Removing the housing

First, disconnect SMG from the power supply, disconnect all the cables and remove the device from rack if necessary (see Paragraph 1.12.3).

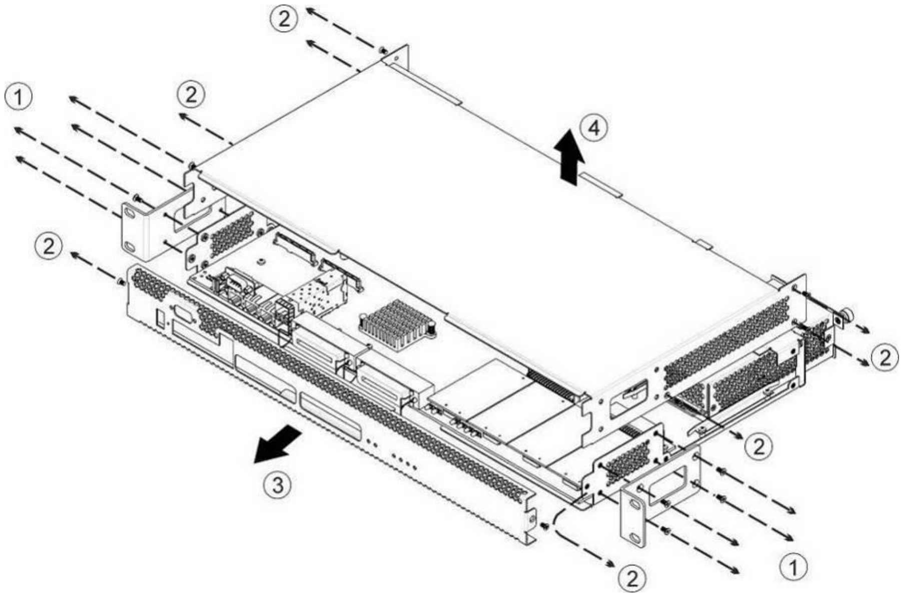


Fig. 17 — SMG-1016M housing removal procedure

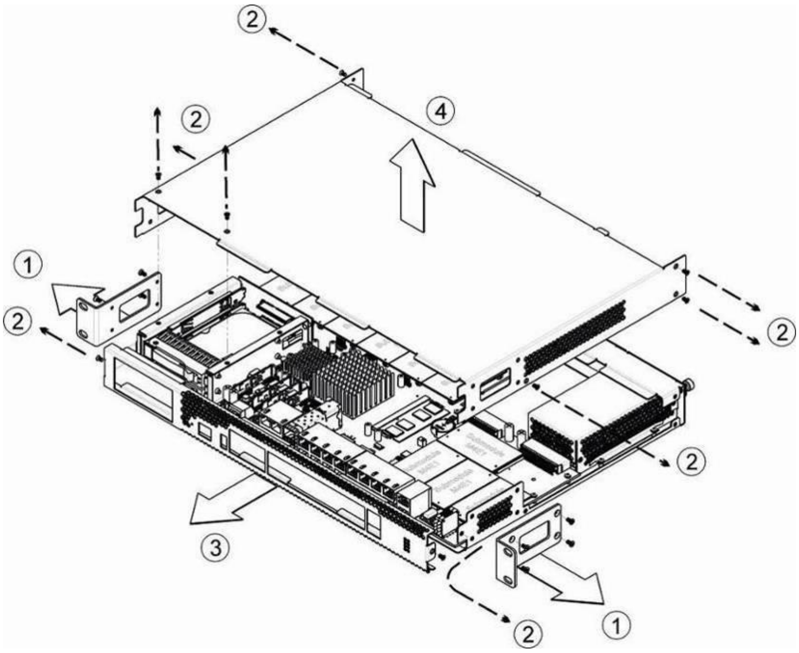


Fig. 18 — SMG-2016 housing removal procedure

1. Use a screwdriver to remove support brackets from the device housing.

2. **Only for SMG-1016M:** untwist the fixation srews on the front panel, pull the front panel to separate it from the top and side panels (*Fig. 17*).
3. Untwist the screws on the top panel
4. Pull the top panel of the device to remove it.

For the device assembly, repeat all mentioned steps in the reverse order.

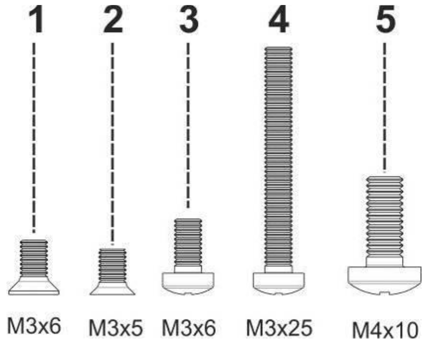


Fig. 19 — Types of screws used for SMG assembly

The figure above shows types of screws used for device assembly into the housing:

1. Support brackets mounting for rack installation
2. Housing parts mounting
3. Board, ventilation unit, covers, guides mounting
4. Fan mounting screw
5. Grounding screw

During the device assembly, avoid using inappropriate screw type for the operations specified. Changing screw type may cause the device failure.

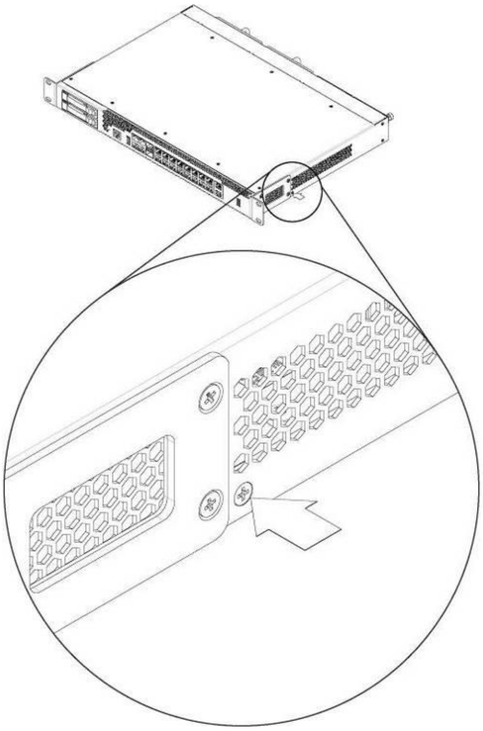


Fig. 20 — SMG assembly into housing

During SMG assembly, install the manufacturer-provided screw into place as shown in the figure above. Changing screw type may cause the device failure.

1.12.6 Submodule Installation

Device features modular design and may accommodate up to 6 x IP submodules IP SM-VP-M300 *(Submodule MSP)* and up to 4 x E1 stream submodules *(Submodule C4E1)* in slots shown in the figures below.

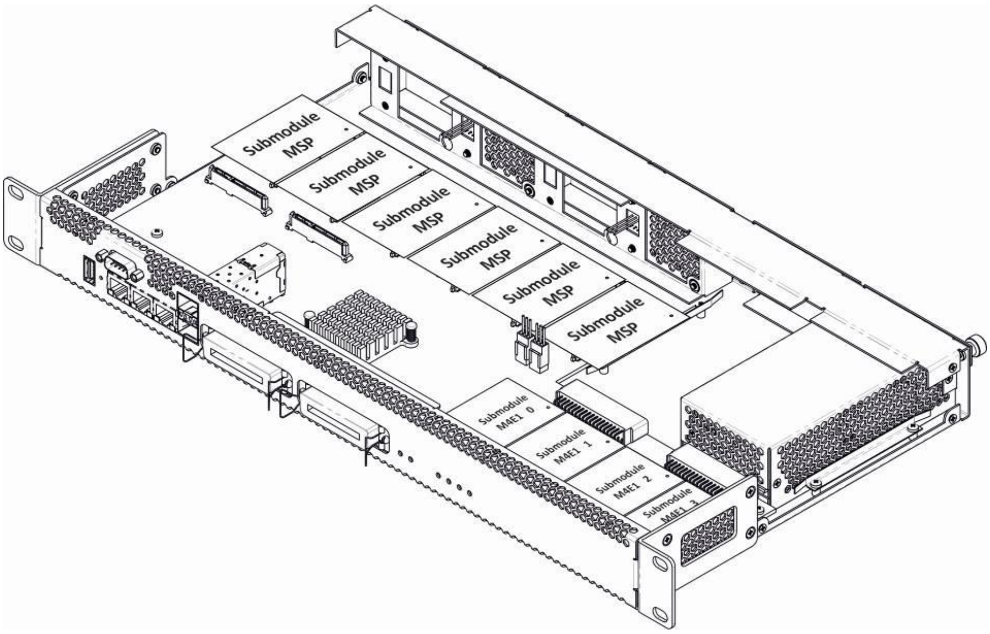


Fig. 21 — SMG-1016M submodule location

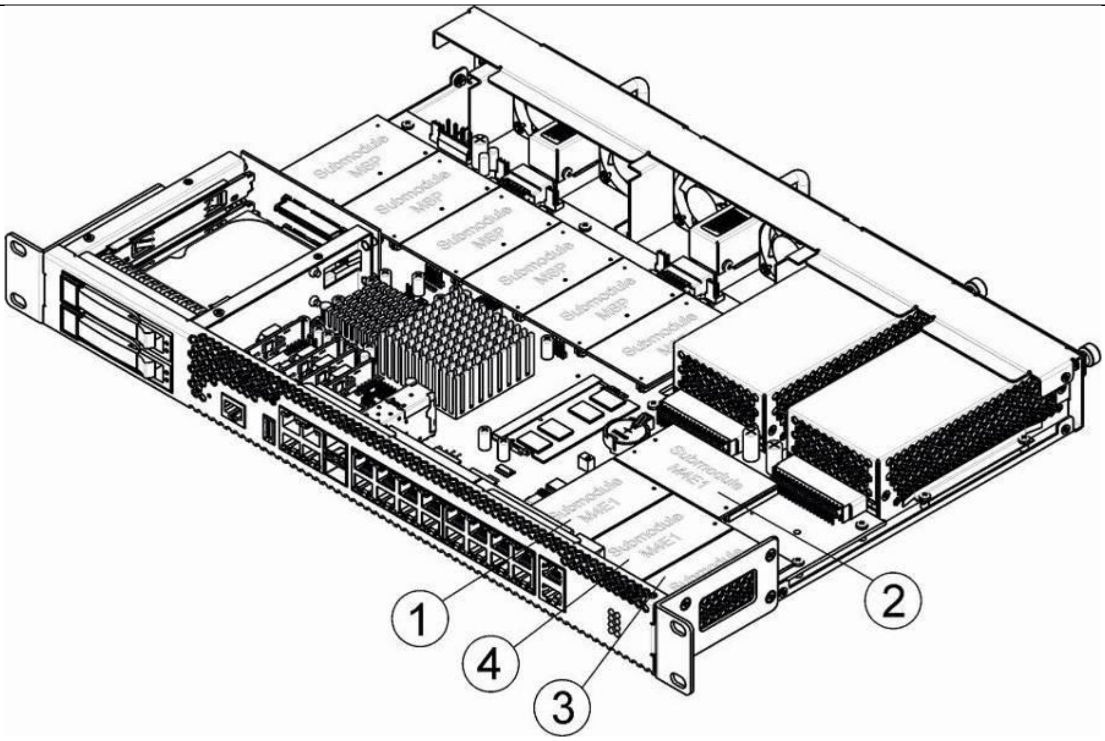


Fig. 22 — SMG-2016 submodule location

SMG submodule installation order:

1. Check if the device is energized.
2. If the voltage is present, disconnect the power supply.
3. Remove the device from rack if necessary (see Section 1.12.3).
4. Remove the device housing (see Section 1.12.5).
5. Install the module into the empty slot (see *Fig. 21*, *Fig. 22*).
6. C4E1 submodule slots are mapped to E1 stream numbers as follows:

For SMG-1016M

- Submodule C4E1 0 — E1 Stream 0-3
- Submodule C4E1 1 — E1 Stream 4-7
- Submodule C4E1 2 — E1 Stream 8-11
- Submodule C4E1 3 — E1 Stream 12-15

For SMG-2016

- Submodule C4E1 *1* — E1 Stream *0-3*
- Submodule C4E1 *2* — E1 Stream *4-7*
- Submodule C4E1 *3* — E1 Stream *8-11*
- Submodule C4E1 *4* — E1 Stream *12-15*

1.12.7 Installation of ventilation units

The device design allows ventilation units replacement even when the power is on.

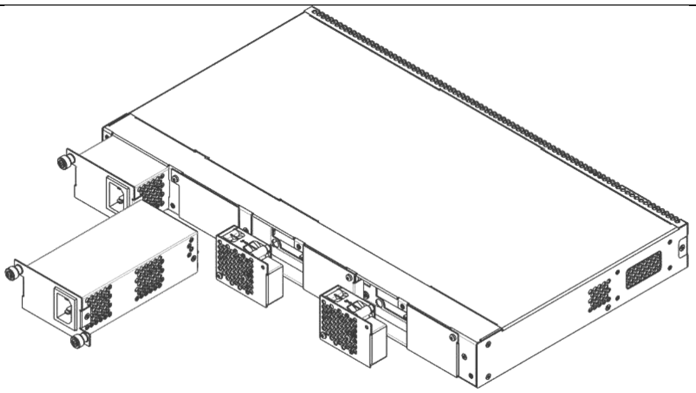


Fig. 23 — SMG-1016M ventilation unit Installation into case

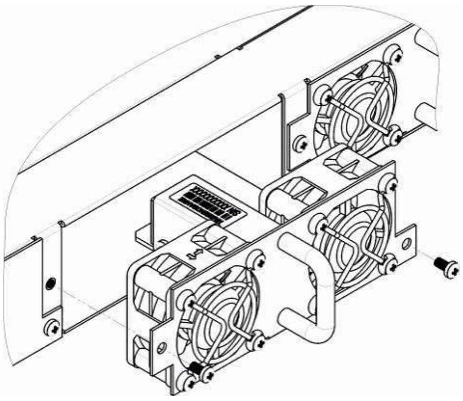


Fig. 24 — SMG-2016 ventilation unit Installation into case

To remove a ventilation unit, perform the following actions:

1. Use a screwdriver to remove the right screw connecting the ventilation unit with the rear panel.
2. Carefully pull the unit until it is removed from the case.
3. Disconnect the unit from the terminal socket, Fig. 25.

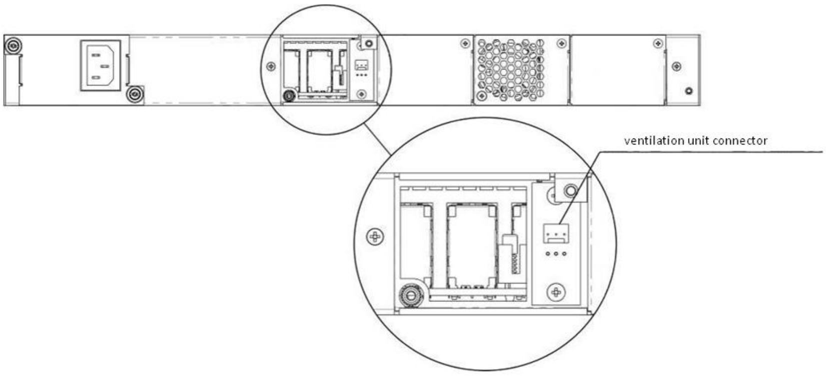


Fig. 25 — SMG-1016M ventilation unit connector

To install a ventilation unit, perform the following actions:

1. Connect the unit to the terminal socket.
2. Insert the unit into the terminal case.
3. Screw the ventilation unit to the rear panel.

1.12.8 SSD installation for SMG-1016M

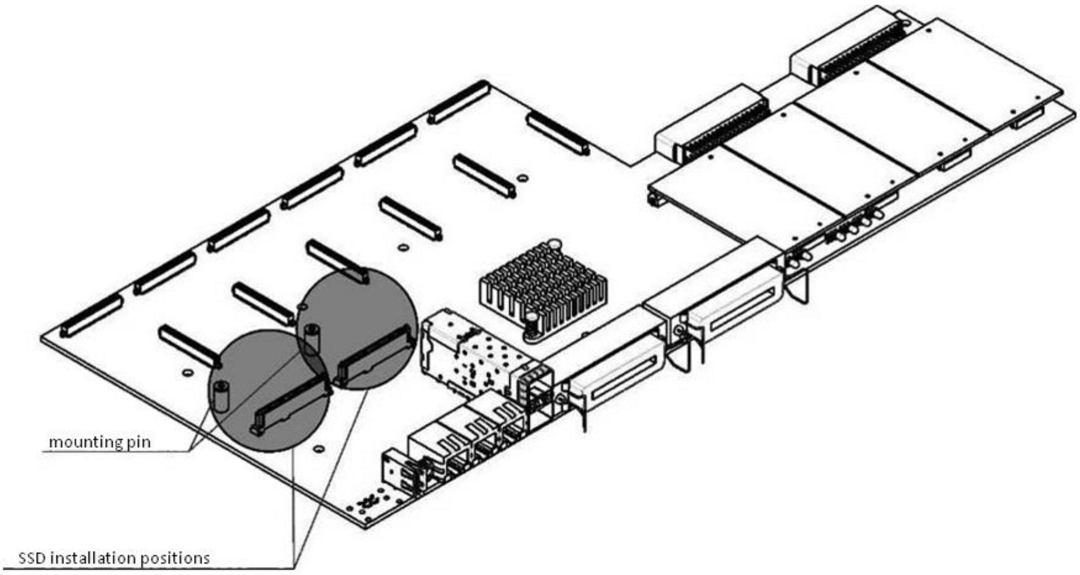


Fig 26 — SSD installation procedure

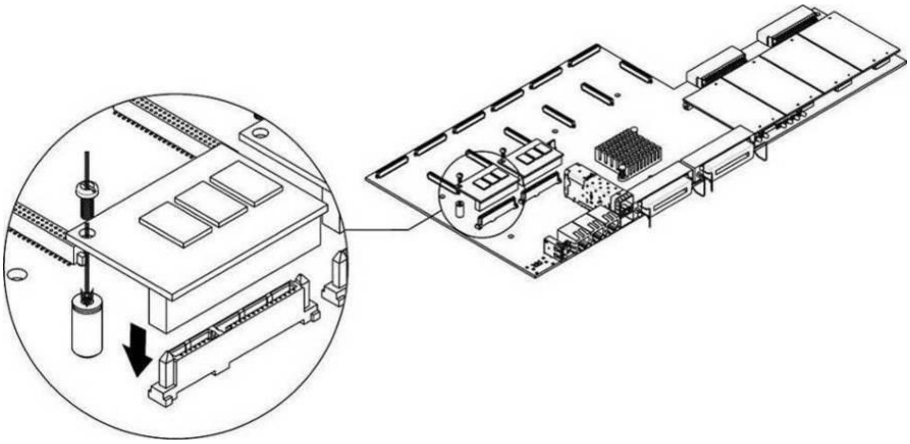


Fig 27 — SSD mounting procedure

1. Check if the device is energized.
2. If the voltage is present, disconnect the power supply.
3. Remove the device from rack if necessary (see Paragraph 1.12.3).
4. Remove the device housing (see Paragraph 1.12.5).
5. If the mounting sleeve (see Fig 26) is missing from the device board, use the removable stand:
   a. Mount the SSD onto the fixing stand
   b. Remove the liner from the adhesive layer of the fixing stand
6. Install the drive into a vacant slot (2 slots are available in total — see Fig 26), and if the mounting sleeve is present on the board, fasten the drive with a screw, Fig 27.

   For the SSD removal, repeat all mentioned steps in the reverse order.

1.12.9 SATA drive installation for SMG-2016

SATA drives may be additionally included in the device delivery package.

Installation of SATA drives:

1. Remove the cradle from the device housing (Fig. 12, Element 1). To do this, press the button on the right until the ejector knob is released, pull the knob to remove the cradle from the housing.
2. Remove the mounting kit located under the ejector knob, Fig. 28.
3. Fix the drive in the cradle tray, Fig. 29.
4. Insert the cradle with the SATA drive installed back into slot and push the ejector knob until it fits with a click.

For the SATA drive removal, repeat all mentioned steps in the reverse order.

You may also install and/or remove SATA drives when the device in energized.

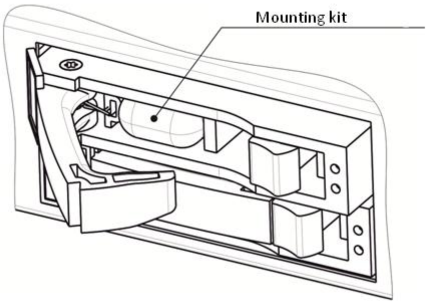


Fig. 28 — Mounting kit location in shipping

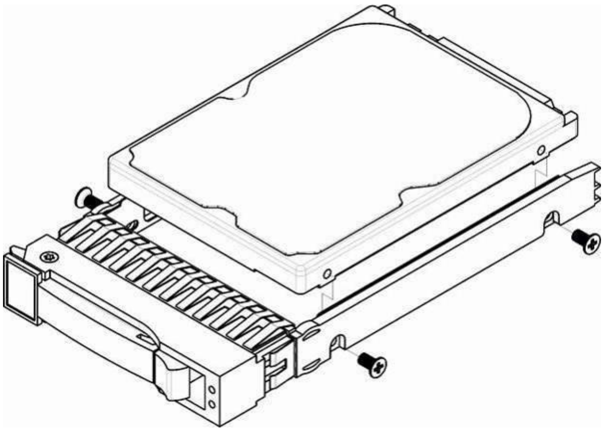


Fig. 29 — Mounting SATA drive into cradle tray

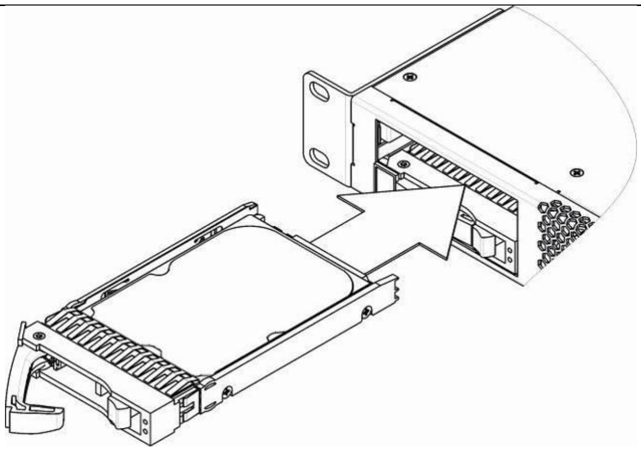


Fig. 30 — Installation of SATA drive into device housing

1.12.10 RTC battery replacement

RTC (electric circuit designed for automatic chronometric data metering — current time, date, day of the week, etc.) located on the device board features a battery which specifications are listed in Table below.

Table 15 — RTC battery specifications

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

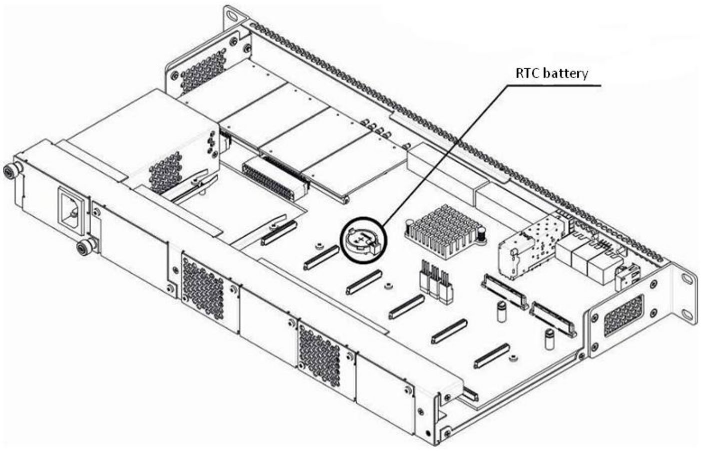


Fig. 31 — RTC battery location for SMG-1016M

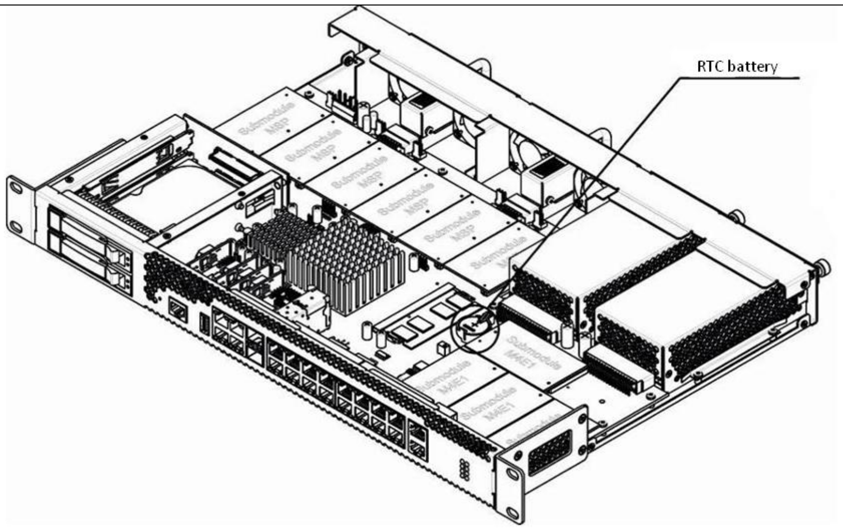


Fig. 32 — RTC battery location for SMG-2016

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

1. Check if the device is energized.
2. If the voltage is present, disconnect the power supply.
3. Remove the device from rack if necessary (see Paragraph 1.12.3).
4. Remove the device housing (see Paragraph 1.12.5).
5. Remove used battery (Fig. 31, Fig. 32) and install a new one into the same position.

For the device assembly, repeat all mentioned steps in the reverse order.

If NTP synchronization is disabled, you should set the system date and time after RTC battery replacement.

Used batteries should be recycled accordingly.

2 GENERAL SWITCH OPERATION GUIDELINES

The easiest way to configure and monitor the device is to use the web configurator, so we recommend you to use it for these purposes.

In order to prevent an unauthorized access to the device, we recommend changing the password for telnet and console access (default username: admin, password: rootpasswd) and administrator password for web configurator access. For setting password for telnet and console access, see Section 3.3.2 Changing password for CLI access to device**.** For setting password for web configurator access, see Section 3.1.25 Setting password for web configurator access. We recommend to write down and store defined passwords in a safe place, inaccessible by intruders.

In order to prevent device configuration data loss, e.g. after reset to factory settings, we recommend making configuration backup copies and storing them on a PC each time significant changes are made.

3 DEVICE CONFIGURATION

You can connect to the device using the following methods: via web configurator, via Telnet/SSH protocols, or using RS-232 cable. (CLI is utilized for RS-232, SSH or Telnet access.)

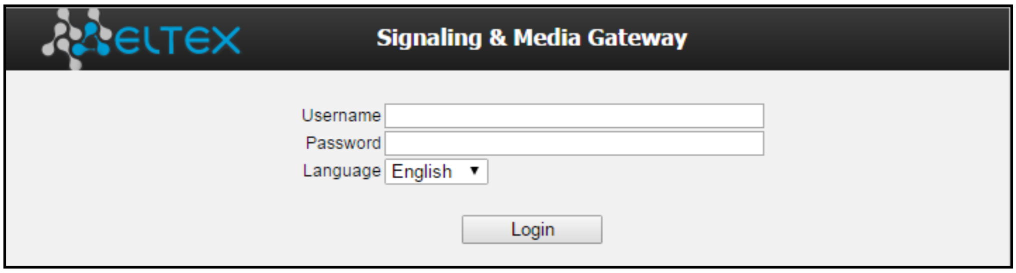
✓ **All settings will take effect without gateway restart. To save changes made to configuration into the non-volatile memory, use 'Service/Save configuration into Flash' menu in the web configurator or 'copy running_to_startup' command in CLI.**

3.1 SMG configuration via web configurator

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

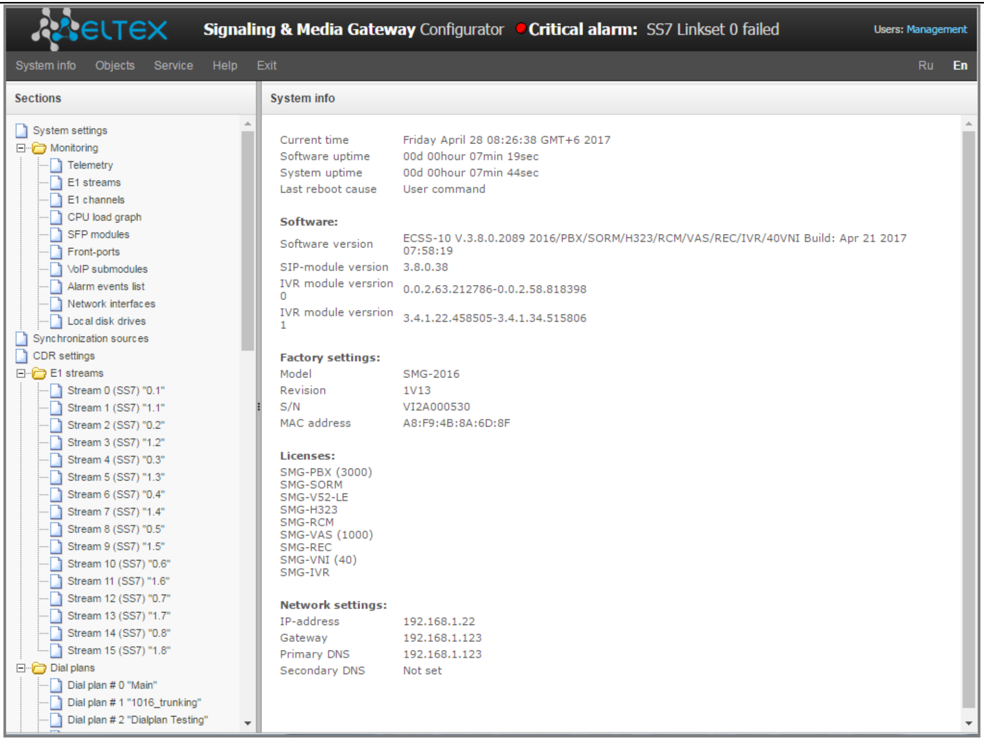
✓ **SMG factory default IP address — 192.168.1.2, network mask — 255.255.255.0**

After entering IP address the device will request username and password.



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

When web configurator access is established, you will see the *'System information'* page.



System info

Current time	Friday April 28 08:26:38 GMT+6 2017
Software uptime	00d 00hour 07min 19sec
System uptime	00d 00hour 07min 44sec
Last reboot cause	User command

Software:

Software version	ECSS-10 V.3.8.0.2089 2016/PBX/SORM/H323/RCM/VAS/REC/IVR/40VNI Build: Apr 21 2017 07:58:19
SIP-module version	3.8.0.38
IVR module versrion 0	0.0.2.63.212786-0.0.2.58.818398
IVR module versrion 1	3.4.1.22.458505-3.4.1.34.515806

Factory settings:

Model	SMG-2016
Revision	1V13
S/N	VI2A000530
MAC address	A8:F9:4B:8A:6D:8F

Licenses:

SMG-PBX (3000)
SMG-SORM
SMG-V52-LE
SMG-H323
SMG-RCM
SMG-VAS (1000)
SMG-REC
SMG-VNI (40)
SMG-IVR

Network settings:

IP-address	192.168.1.22
Gateway	192.168.1.123
Primary DNS	192.168.1.123
Secondary DNS	Not set

The figure below shows web configurator navigation elements.

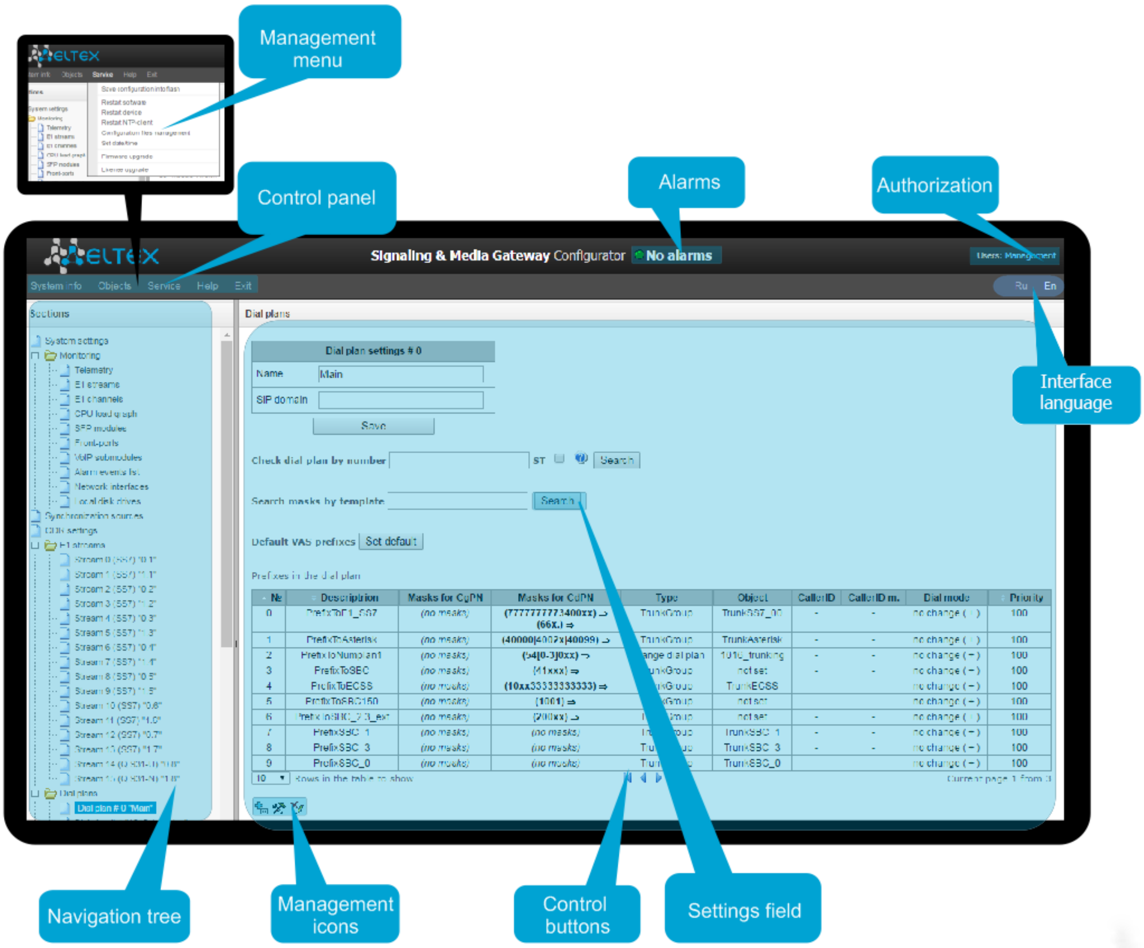


Fig. 33 — Web configurator navigation elements

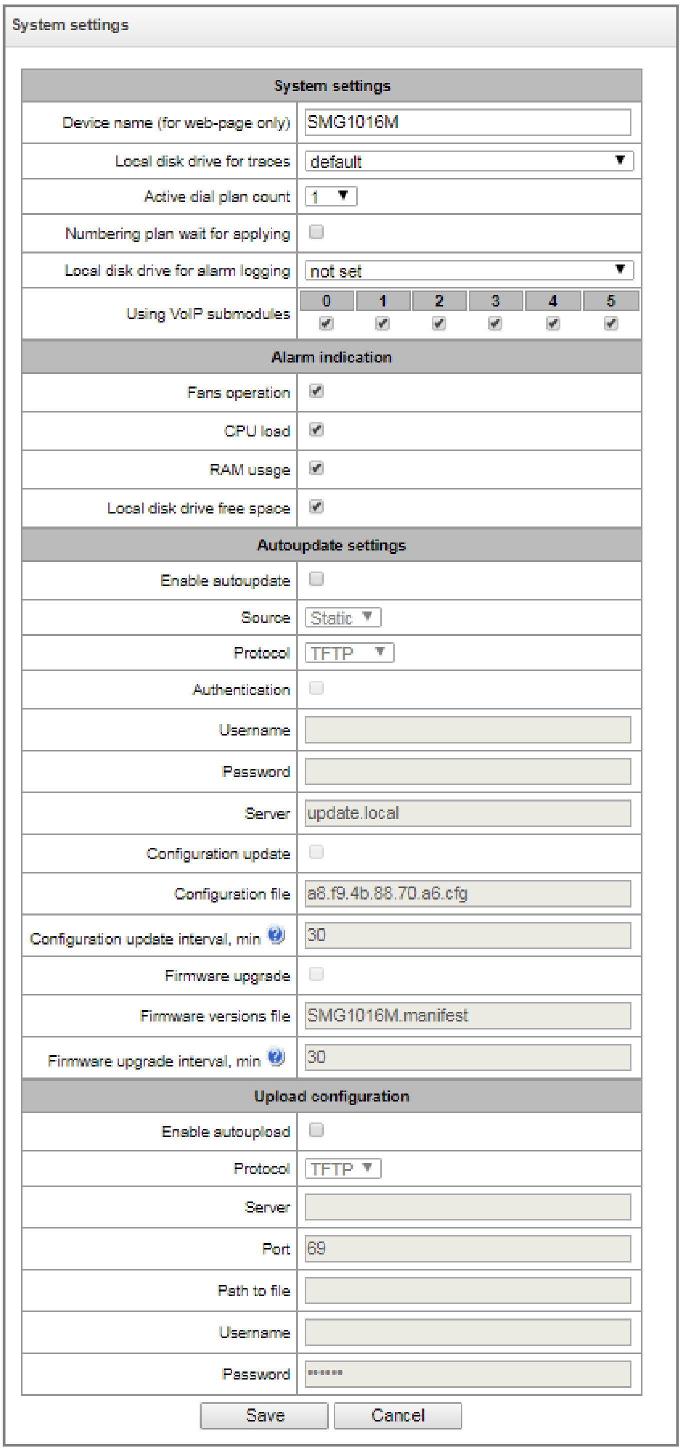
The user interface is divided into several areas.

Navigation tree	is used for access to management sections. Navigation tree contains the hierarchy of management sections and nested menus.
Settings field	is based on the user selection in navigation tree. Allows to view device settings and enter configuration data.
Control panel	panel for setting field objects and device firmware status management.
Management menu	drop-down menus of the panel for settings field objects and device firmware status management.
Alarms	displays the current highest-priority fault and serves as a link for the fault events log operations.
Authorization	link for management of passwords used to access the web configurator.
Interface language	buttons to switching interface language
Management icons	controls that allow for the settings field objects management; duplicate 'Objects' menu of the control panel: *— Add object* *— Edit object* *— Delete object* *— View object*
Management buttons	controls that allow for settings field operation.

To prevent unauthorized access to device in the future, it's recommended to change password (see Section 3.1.25 **Setting password for web configurator access**).

The 'Tip' button located next to the editing element provides explanation for the particular parameter.

3.1.1 System settings



System settings

System settings	
Device name (for web-page only)	SMG1016M
Local disk drive for traces	default
Active dial plan count	1
Numbering plan wait for applying	□
Local disk drive for alarm logging	not set
Using VoIP submodules	0 ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑
Alarm indication	
Fans operation	☑
CPU load	☑
RAM usage	☑
Local disk drive free space	☑
Autoupdate settings	
Enable autoupdate	□
Source	Static
Protocol	TFTP
Authentication	□
Username	
Password	
Server	update.local
Configuration update	□
Configuration file	a8.f9.4b.88.70.a6.cfg
Configuration update interval, min	30
Firmware upgrade	□
Firmware versions file	SMG1016M.manifest
Firmware upgrade interval, min	30
Upload configuration	
Enable autoupload	□
Protocol	TFTP
Server	
Port	69
Path to file	
Username	
Password	••••••

- *Device name (for web-page only)* — name of the device. This name is used in the device web configurator header.
- *Local disk drive for traces* — device allows for the debug information (tracing) storage in RAM or on the installed storage device:
  - default — debug information is stored in RAM
  - /mnt/sda 1 — path to local storage device; setting is displayed when the storage device is installed. If the storage device is selected, the system will create 'logs' directory for tracing files.

- *Active dial plan count* — quantity of simultaneously active dial plans; you may configure up to 16 (up to 255 on SMG-2016 if there is a VAS license) independent dial plans with an ability to add subscribers and create custom call routing table.

- *Numbering plan wait for applying* – if checked, SMG will not apply setting without confirming. The specifying of the feature helps to operate with long dial plans. It allows you to avoid long processing of dial plans after each change in settings.

- *Local disk drive for alarm logging* — select the device used for critical alarm message storage into non-volatile memory. This option may be required for troubleshooting device restart or failure issues.

  – */mnt/sda 1* — select path to a local storage device. When this option is enabled, the file 'alarm.txt' containing alarm data will be created on the storage device.

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 — event current state (OК — alarm is resolved, ALARM — alarm is active)

Table 16 — Alarm message examples

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

- *Using VoIP submodules* — select SM-VP submodules, which will be in operation.

Alarm Indication

- *Fans operation* — when checked, fault indication will appear in case of cooling fan failure (ALARM LED will light up, alarm will be added to alarm log).
- *CPU load* — when checked, fault indication will appear in case of high CPU utilization (ALARM LED will light up, alarm will be added to alarm log).
- *RAM usage* — when checked, fault indication will appear in case of high RAM utilization (more than 75% of the total RAM amount) (ALARM LED will light up, alarm will be added to alarm log).
- *Local disk drive free space* — when checked, fault indication will appear, if the utilization of a single external storage device with capacity less than 5Gb exceeds 80% (or there is less than 1024MB of free space on an external storage device with capacity exceeding 5Gb) (ALARM LED will light up, alarm will be added to alarm log).

Autoupdate settings

SMG can automatically obtain configuration and firmware files from server with specified frequency. SMG will apply new configuration after completing of all active calls or before a reboot.

Firmware version description file contains information about firmware versions on the server: numbers of versions and file names. In this file you can define time to update. Format of the file must be as followings:

<Number of firmware version>;<Firmware file name>;<permitted update time, hour>

- *Number of firmware version* - defines completely, including assembling version;
- *Firmware file name* must have .bin extension;
- It is not necessary to assign *permitted update time*. SMG will be updated as soon as active calls are finished. If you specify the time, SMG will be updated only within this time range.

Example of firmware description file:
3.7.0.1944;smg1016m_firmware_3.7.0.1944.bin
3.8.0.2050;smg1016m_firmware_3.8.0.2050.bin;9-13

- Enable autoupdate — enable automatic firmware update;
- Source — server information source select;
  - Static — information about server is written and saved on SMG
  - DHCP (interface name) — information on a server is obtained on specified interface via DHCP option 66, information on a version and configuration file names is obtained via option 67;
- Protocol — protocol selection for server connection;
- Authentication — use authentication to get access to the server (for FTP, HTTP, HTTPS);
  - Username — name (login) for access to the server;
  - Password — password for access to the server;
- Server — IP address or domain name of server. Available if you select Static Source;
- Configuration update — allows configuration update from server;

- Configuration file — configuration file name. The name must have .cfg extension and contains up to 64 symbols;
- Configuration update interval, min — frequency of server validation for configuration update;

- Firmware upgrade — enable firmware upgrade from server;

  - Firmware versions file name — file name with firmware versions. The name must have .manifest extension and contains up to 64 symbols.
  - Firmware upgrade interval, min — frequency of server validation for firmware upgrade.

Upload configuration

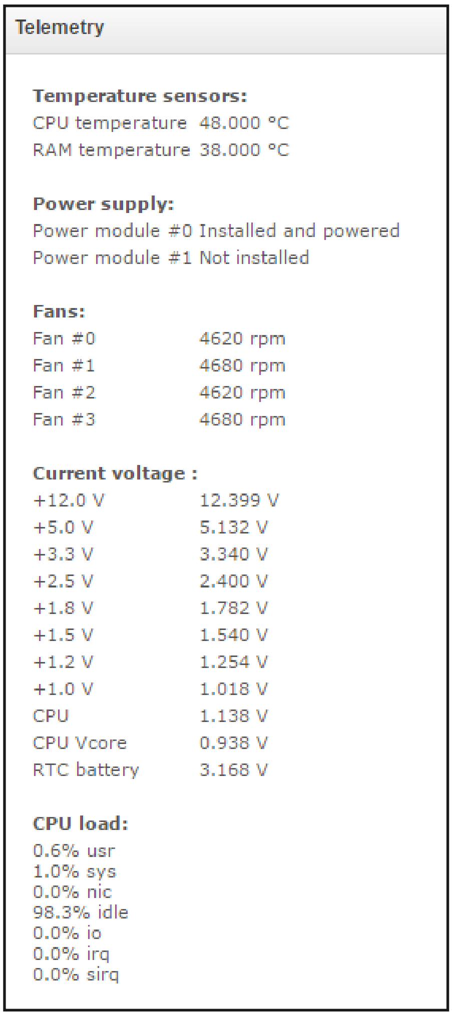
SMG can upload a configuration to FTP/TFTP server automatically each time it is saved to non-volatile memory.

- *Enable autoupload* – enable the function of automatic configuration upload;
- *Protocol* – select a protocol for uploading. FTP and TFTP are supported.
- *Server* – IP addres of the server for uploading the configuration;
- *Port* – port of the server through which the uploading will be implemented.
- *Path to file* – directory located on the server where the configuration will be stored.
- *Username* – a name for authentication in case of FTP using;
- *Password* – a password for authentication in case of FTP using.

3.1.2 Monitoring

3.1.2.1 Telemetry

This section contains information on the device telemetric sensor readings as well as the information on power supplies and fans installed.



```
Telemetry

Temperature sensors:
CPU temperature  48.000 °C
RAM temperature  38.000 °C

Power supply:
Power module #0 Installed and powered
Power module #1 Not installed

Fans:
Fan #0          4620 rpm
Fan #1          4680 rpm
Fan #2          4620 rpm
Fan #3          4680 rpm

Current voltage :
+12.0 V         12.399 V
+5.0 V          5.132 V
+3.3 V          3.340 V
+2.5 V          2.400 V
+1.8 V          1.782 V
+1.5 V          1.540 V
+1.2 V          1.254 V
+1.0 V          1.018 V
CPU             1.138 V
CPU Vcore       0.938 V
RTC battery     3.168 V

CPU load:
0.6% usr
1.0% sys
0.0% nic
98.3% idle
0.0% io
0.0% irq
0.0% sirq
```

Temperature sensors

For SMG-1016M:

- Sensor #0 – CPU temperature
- Sensor #1 – RAM module temperature

For SMG-2016:

- Sensor #0 – CPU temperature

Power supply

- *Power module #0* — status of power supply installed in slot 0
- *Power module #1* — status of power supply installed in slot 1

Possible power supply states:

- *Installed* — power supply is installed

- *Not installed* — power supply is not installed
- *In operation* — power supply is energized with feed voltage
- *Not in operation* — power supply is de-energized

Fans

- Fan #N — information on fan N and its rotation speed (e.g. 9600 rpm)

There are two fans installed in SMG-1016M and four fans in SMG-2016.

Current voltage[1]

- *Internal voltage (+12V)* — 12V voltage sensor status details.

Current voltage[2]

- *+12.0V* — 12V voltage sensor status details
- *+5.0V* — 5V voltage sensor status details
- *+3.3V* — 3.3V voltage sensor status details
- *+2.5V* — 2.5V voltage sensor status details
- *+1.8V* — 1.8V voltage sensor status details
- *+1.5V* — 1.5V voltage sensor status details
- *+1.2V* — 1.2V voltage sensor status details
- *+1.0V* — 1V voltage sensor status details
- *CPU* — CPU voltage status details
- *CPU Vcore* — CPU core voltage status details
- *RTC battery* — real-time clock battery voltage status details

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 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 hardware interruptions' processing

[1] For SMG-1016M only

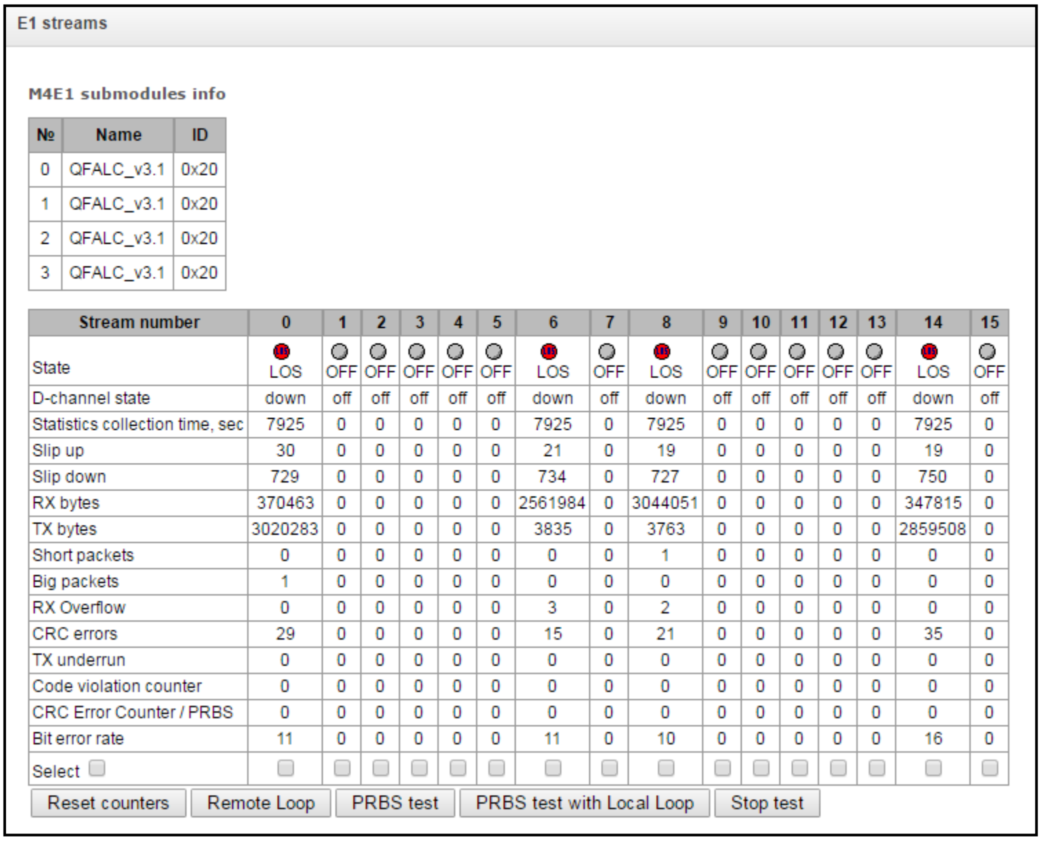
[2] For SMG-2016 only

- *SIRQ* — percentage of CPU time spent on software interruptions' processing

3.1.2.2 E1 stream monitoring

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

For E1 chips, the table lists installation position number (see Section 1.12.6 Submodule Installation), chip name and identifier.



E1 streams

M4E1 submodules info

№	Name	ID
0	QFALC_v3.1	0x20
1	QFALC_v3.1	0x20
2	QFALC_v3.1	0x20
3	QFALC_v3.1	0x20

Stream number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
State	● LOS	○ OFF	○ OFF	○ OFF	○ OFF	○ OFF	● LOS	○ OFF	● LOS	○ OFF	○ OFF	○ OFF	○ OFF	○ OFF	● LOS	○ OFF
D-channel state	down	off	off	off	off	off	down	off	down	off	off	off	off	off	down	off
Statistics collection time, sec	7925	0	0	0	0	0	7925	0	7925	0	0	0	0	0	7925	0
Slip up	30	0	0	0	0	0	21	0	19	0	0	0	0	0	19	0
Slip down	729	0	0	0	0	0	734	0	727	0	0	0	0	0	750	0
RX bytes	370463	0	0	0	0	0	2561984	0	3044051	0	0	0	0	0	347815	0
TX bytes	3020283	0	0	0	0	0	3835	0	3763	0	0	0	0	0	2859508	0
Short packets	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
Big packets	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RX Overflow	0	0	0	0	0	0	3	0	2	0	0	0	0	0	0	0
CRC errors	29	0	0	0	0	0	15	0	21	0	0	0	0	0	35	0
TX underrun	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Code violation counter	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CRC Error Counter / PRBS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bit error rate	11	0	0	0	0	0	11	0	10	0	0	0	0	0	16	0
Select □	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Stream parameters:

- State — stream status:

  – *WORK* — stream is in operation
  – *LOS* — signal is lost
  – *OFF* — stream is disabled in configuration
  – *NONE* — submodule is not installed
  – *AIS* — alarm state indication signal (signal that contains all ONEs)
  – *LOMF* — multi-frame alarm state indication signal
  – *RAI* — remote alarm indication
  – *TEST* — stream test indication (PRBS test, local or remote loop)

- D-channel state — state of D channel, service management channel

  – *up* — *D*-channel is in operation
  – *down* — *D*-channel is not in operation
  – *no* — there is no management channel for the stream
  – *off* — signalling is disabled for the stream

- Statistics collection time, sec — statistics collection period in seconds
- Slip up — number of positive bit slips for the stream
- Slip down — number of negative bit slips for the stream
- Rx bytes — number of bytes received from the stream
- Tx bytes — number of bytes sent to the stream
- Short packets — number of packets received which size is less than standard
- Big packets — number of packets received which size is bigger than standard
- Rx Overflow — buffer overrun error counter
- CRC errors — CRC error counter
- Tx underrun — 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 buttons below the table:

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

3.1.2.3 E1 channel monitoring

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
Connection information for stream # and channel #:

- *Port/channel* — this section is divided into two parts:
  - Signalling protocol (PRI/SS7)

- Port location Stream #:Channel #

- *Connected port/channel* — this section is divided into two parts:
  - Linked port signalling protocol (PRI/SS7/VoIP)
  - Linked port location Stream #:Channel # for PRI/SS7 or VoIP submodule #: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 — incoming/outgoing call dialing
  - In-Call/ Out-Call — incoming or outgoing occupation
  - In-Busy/ Out-Busy — sending 'busy' tone
  - Talk — channel is in call state
  - Release — channel release
  - Wait-Ack — waiting for acknowledgement
  - Wait-CID — waiting for CgPN (Caller ID)
  - Wait-Num — waiting for call dialing
  - Hold — subscriber is on hold

- *State timer* — channel last known state duration

- *Incoming SS7 category* — SS7 category of an incoming call before modification

- *Incoming CdPN* — callee number before modification

- *Incoming CgPN* — caller number before modification

- *Outgoing SS7 category* — SS7 category of an incoming call after modification

- *Outgoing CdPN* — callee number after modification

- *Outgoing CgPN* — caller number after modification

Stream state — information table with matrix symbol interpretations

- *State* — stream status:
  - NONE — missing C4E1 submodule
  - OFF — stream is disabled in configuration
  - ALARM — C4E1 submodule initialization error
  - LOS — signal is lost
  - AIS — alarm state indication signal (signal that contains all ONEs)
  - LOF — loss of frame
  - LOMF — multi-frame alarm state indication signal
  - WORK/RAI — remote alarm indication
  - WORK/SLIP — SLIP indication for the stream
  - WORK — stream is in operation
  - TEST — stream test indication (PRBS test, local or remote loop)

Channel state — information table with matrix symbol interpretations

- *State* — channel status:
  - OFF — channel is disabled in configuration
  - Idle — channel is in initial state
  - Block — channel is blocked
  - Incoming dialing — incoming call dialing
  - Outgoing dialing — outgoing call dialing
  - Incoming alerting — incoming occupation, callee is disengaged
  - Outgoing alerting — outgoing occupation, callee is disengaged
  - Busy, Release — channel release, sending 'busy' tone
  - Talk, Hold — channel is in call state, on hold
  - Waiting — waiting for response from the opposite party (waiting for occupation acknowledgement, waiting for Caller ID, waiting for call dialing)
  - *3way, Conference* – conference mode (3-WAY conference or conference Add-on).

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

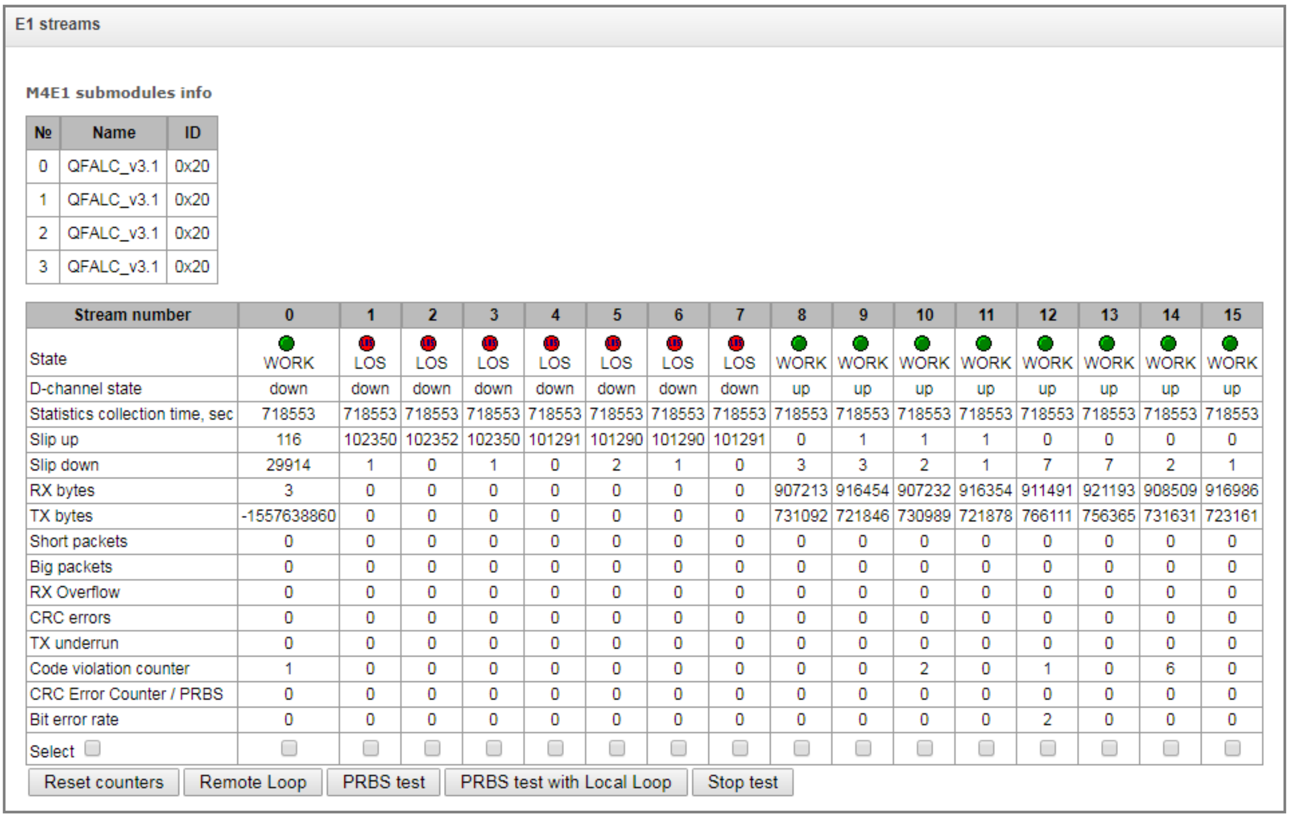
Channel state updates in 5 seconds interval.

Link management

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

SS7 link management — SS7 signal link management table

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



E1 streams

M4E1 submodules info

№	Name	ID
0	QFALC_v3.1	0x20
1	QFALC_v3.1	0x20
2	QFALC_v3.1	0x20
3	QFALC_v3.1	0x20

Stream number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
State	● WORK	● LOS	● LOS	● LOS	● LOS	● LOS	● LOS	● LOS	● WORK	● WORK	● WORK	● WORK	● WORK	● WORK	● WORK	● WORK
D-channel state	down	down	down	down	down	down	down	down	up	up	up	up	up	up	up	up
Statistics collection time, sec	718553	718553	718553	718553	718553	718553	718553	718553	718553	718553	718553	718553	718553	718553	718553	718553
Slip up	116	102350	102352	102350	101291	101290	101290	101291	0	1	1	1	0	0	0	0
Slip down	29914	1	0	1	0	2	1	0	3	3	2	1	7	7	2	1
RX bytes	3	0	0	0	0	0	0	0	907213	916454	907232	916354	911491	921193	908509	916986
TX bytes	-1557638860	0	0	0	0	0	0	0	731092	721846	730989	721878	766111	756365	731631	723161
Short packets	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Big packets	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RX Overflow	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CRC errors	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TX underrun	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Code violation counter	1	0	0	0	0	0	0	0	0	0	2	0	1	0	6	0
CRC Error Counter / PRBS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bit error rate	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0
Select □	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

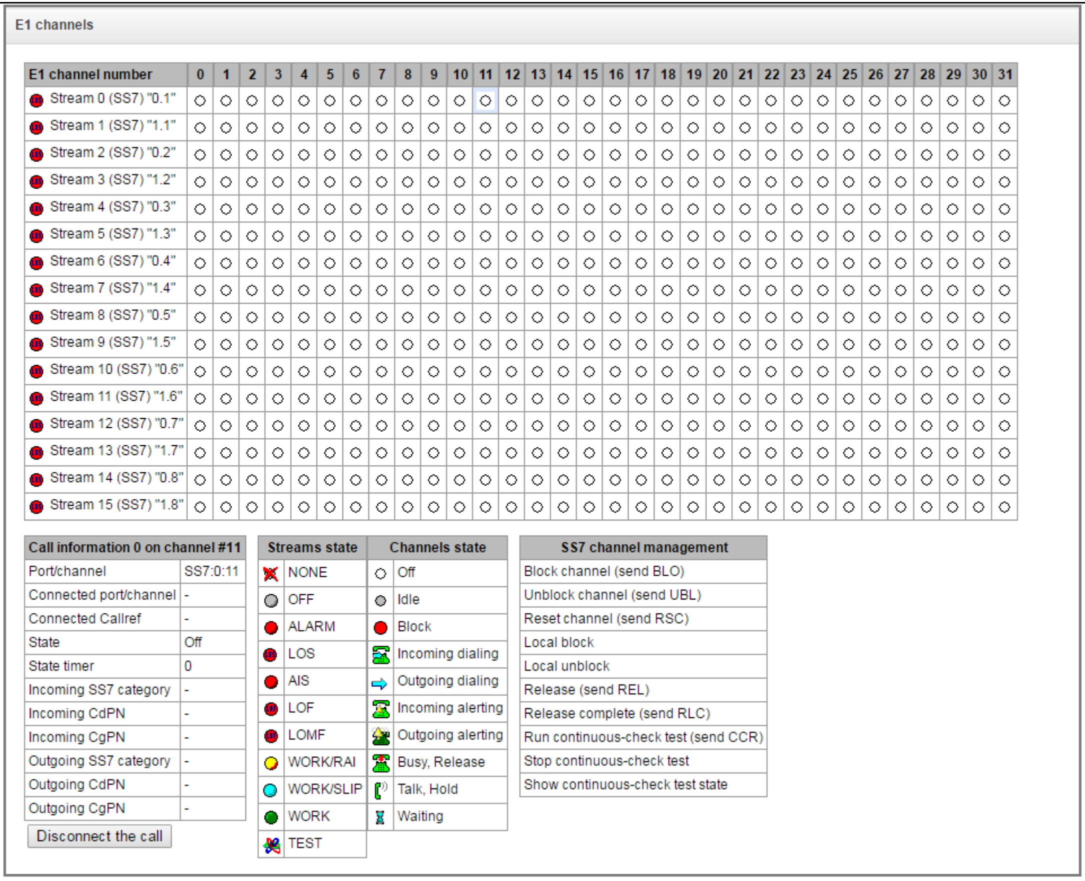
Channel management

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 2 in Stream 1 (SS7). Next, in 'SS7 channel management' table, select the field with the required action and left-click it. Pop-up informational message about the command execution will be shown on screen.

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

SS7 channel management — SS7 (CIC) channel management table:

- *Block channel (send BLO)* — send BLO message to block channel
- *Unblock channel (send UBL)* — send UBL message to unblock channel
- Reset channel (send RSC) — send RSC message
- *Local block* — block channel locally without BLO message transmission
- *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* - stop channel continuity test;
- *Show continuous-check test state* - show current continuous-check test state.



E1 channels

E1 channel number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
🔴 Stream 0 (SS7) "0.1"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 1 (SS7) "1.1"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 2 (SS7) "0.2"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 3 (SS7) "1.2"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 4 (SS7) "0.3"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 5 (SS7) "1.3"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 6 (SS7) "0.4"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 7 (SS7) "1.4"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 8 (SS7) "0.5"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 9 (SS7) "1.5"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 10 (SS7) "0.6"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 11 (SS7) "1.6"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 12 (SS7) "0.7"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 13 (SS7) "1.7"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 14 (SS7) "0.8"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
🔴 Stream 15 (SS7) "1.8"	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Call information 0 on channel #11	
Port/channel	SS7:0:11
Connected port/channel	-
Connected Callref	-
State	Off
State timer	0
Incoming SS7 category	-
Incoming CdPN	-
Incoming CgPN	-
Outgoing SS7 category	-
Outgoing CdPN	-
Outgoing CgPN	-

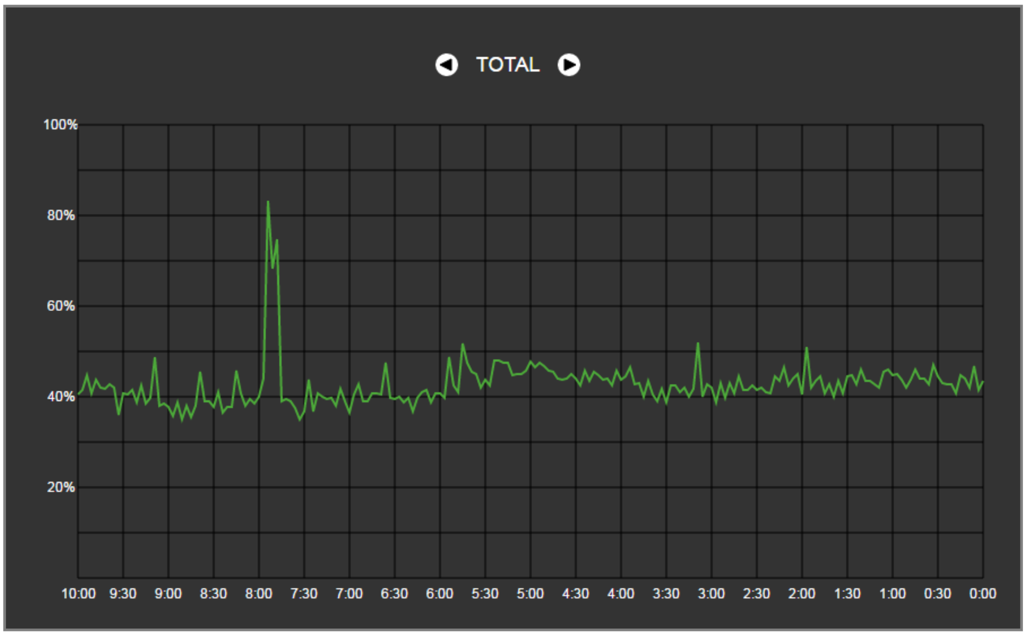
Disconnect the call

Streams state		Channels state	
✗	NONE	○	Off
⚪	OFF	⊙	Idle
🔴	ALARM	🔴	Block
🔴	LOS	☎	Incoming dialing
🔴	AIS	⇨	Outgoing dialing
🔴	LOF	☎	Incoming alerting
🔴	LOMF	☎	Outgoing alerting
🟡	WORK/RAI	☎	Busy, Release
🔵	WORK/SLIP	☎	Talk, Hold
🟢	WORK	⧗	Waiting
✗	TEST		

SS7 channel management
Block channel (send BLO)
Unblock channel (send UBL)
Reset channel (send RSC)
Local block
Local unblock
Release (send REL)
Release complete (send RLC)
Run continuous-check test (send CCR)
Stop continuous-check test
Show continuous-check test state

3.1.2.4 CPU utilization chart

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

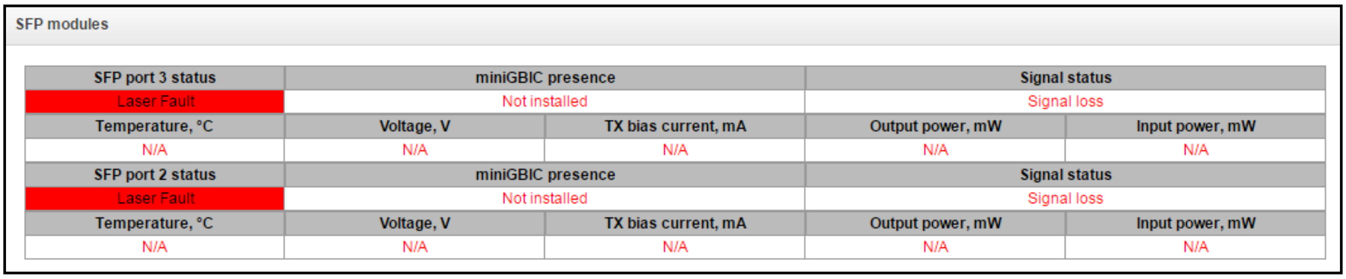


To navigate between specific parameters in monitoring charts, use buttons ◀ and ▶. To facilitate visual identification, all charts have different colors.

- *TOTAL* — total CPU utilization percentage
- *IO* — percentage of CPU time spent on I/O operations
- *IRQ* — percentage of CPU time spent on hardware interruptions' processing
- *SIRQ* — percentage of CPU time spent on software interruptions' processing
- *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 modified priority

3.1.2.5 SFP module monitoring

This section contains status indication and optical line parameters.



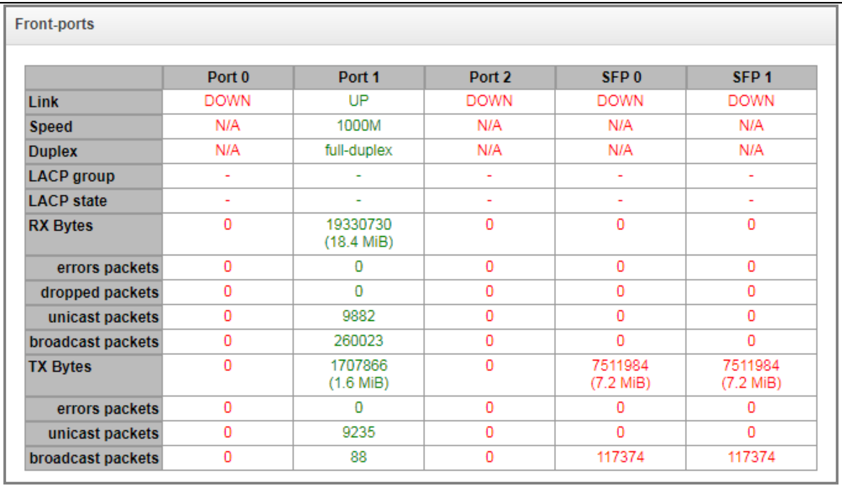
SFP modules

SFP port 3 status	miniGBIC presence		Signal status	
Laser Fault	Not installed		Signal loss	
Temperature, °C	Voltage, V	TX bias current, mA	Output power, mW	Input power, mW
N/A	N/A	N/A	N/A	N/A
SFP port 2 status	miniGBIC presence		Signal status	
Laser Fault	Not installed		Signal loss	
Temperature, °C	Voltage, V	TX bias current, mA	Output power, mW	Input power, mW
N/A	N/A	N/A	N/A	N/A

- *SFP port X status* — optical module status:
  - miniGBIC presence — indication of module installation (module is installed, module is not installed)
  - Signal status — signal loss indication (signal is lost, in operation)
  - Temperature, °C — optical module temperature
  - Voltage, V — optical module power supply voltage, V
  - Tx bias current, mA — transmission bias current, mA
  - Input power, mW — receiving signal power, mW
  - Output power, mW — transmitting signal power, mW

3.1.2.6 Front ports monitoring

This section contains information about physical switch port state - link state, committed data rate and mode of transmission. Dual port (copper and optical connectors) is marked with «SFP» label near its number. There is no label, if dual port is active and connected with copper cable.



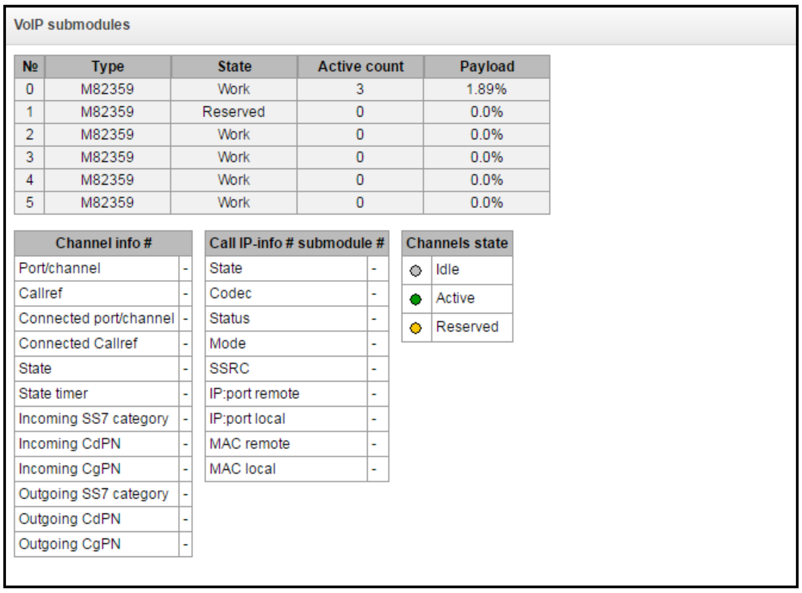
Front-ports

	Port 0	Port 1	Port 2	SFP 0	SFP 1
Link	DOWN	UP	DOWN	DOWN	DOWN
Speed	N/A	1000M	N/A	N/A	N/A
Duplex	N/A	full-duplex	N/A	N/A	N/A
LACP group	-	-	-	-	-
LACP state	-	-	-	-	-
RX Bytes	0	19330730 (18.4 MiB)	0	0	0
errors packets	0	0	0	0	0
dropped packets	0	0	0	0	0
unicast packets	0	9882	0	0	0
broadcast packets	0	260023	0	0	0
TX Bytes	0	1707866 (1.6 MiB)	0	7511984 (7.2 MiB)	7511984 (7.2 MiB)
errors packets	0	0	0	0	0
unicast packets	0	9235	0	0	0
broadcast packets	0	88	0	117374	117374

- *Link* - cable connection state on port (UP/DOWN);
- *Speed* - committed data rate on port;
- *Duplex* - data transmission mode (half-/full-duplex).
- *LACP group* – LACP channel including the port and its state (UP/DOWN);
- *LACP state* –port mode (active/backup);
- *Rx bytes* – storage counter of received packets, including different types of received packets;
- *Tx bytes* – storage counter of transmitted packets, including different types of transmitted packets.

3.1.2.7 VoIP submodule monitoring

This section contains information on SM-VP submodules installed and their channel state.



VoIP submodules

№	Type	State	Active count	Payload
0	M82359	Work	3	1.89%
1	M82359	Reserved	0	0.0%
2	M82359	Work	0	0.0%
3	M82359	Work	0	0.0%
4	M82359	Work	0	0.0%
5	M82359	Work	0	0.0%

Channel info #	
Port/channel	-
Callref	-
Connected port/channel	-
Connected Callref	-
State	-
State timer	-
Incoming SS7 category	-
Incoming CdPN	-
Incoming CgPN	-
Outgoing SS7 category	-
Outgoing CdPN	-
Outgoing CgPN	-

Call IP-info # submodule #	
State	-
Codec	-
Status	-
Mode	-
SSRC	-
IP:port remote	-
IP:port local	-
MAC remote	-
MAC local	-

Channels state	
○	Idle
🟢	Active
🟡	Reserved

- *№* –SM-VP submodule sequential number
- *Type* — installed submodule type

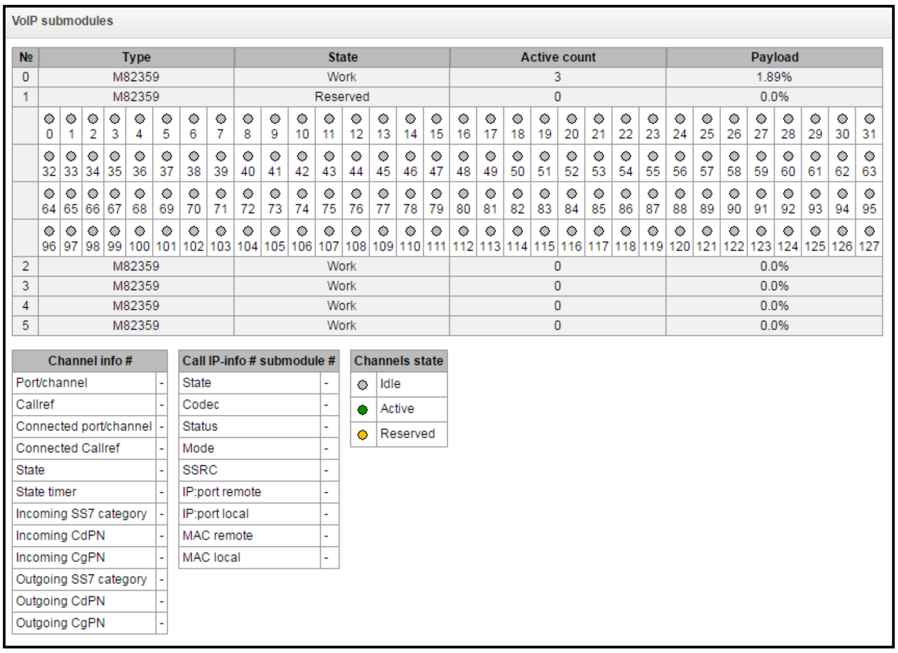
- State:

  - Not Present — not installed
  - No init — not initialized, no initialization attempts
  - Off — disabled, no submodule load attempts
  - Wait Ack — waiting for acknowledgement from CPU after submodule load
  - Failed — no response from submodule
  - Work — submodule normal operation
  - Recovery — no control packets coming from submodule

- *Active count* — number of active connections on the submodule at the given moment

- *Payload* — submodule resource utilization percentage at the given moment

For channel state monitoring, left-click the row containing the required submodule number. To hide the information, left-click the row again.



VoIP submodules

№	Type	State	Active count	Payload
0	M82359	Work	3	1.89%
1	M82359	Reserved	0	0.0%

○ 0	○ 1	○ 2	○ 3	○ 4	○ 5	○ 6	○ 7	○ 8	○ 9	○ 10	○ 11	○ 12	○ 13	○ 14	○ 15	○ 16	○ 17	○ 18	○ 19	○ 20	○ 21	○ 22	○ 23	○ 24	○ 25	○ 26	○ 27	○ 28	○ 29	○ 30	○ 31
○ 32	○ 33	○ 34	○ 35	○ 36	○ 37	○ 38	○ 39	○ 40	○ 41	○ 42	○ 43	○ 44	○ 45	○ 46	○ 47	○ 48	○ 49	○ 50	○ 51	○ 52	○ 53	○ 54	○ 55	○ 56	○ 57	○ 58	○ 59	○ 60	○ 61	○ 62	○ 63
○ 64	○ 65	○ 66	○ 67	○ 68	○ 69	○ 70	○ 71	○ 72	○ 73	○ 74	○ 75	○ 76	○ 77	○ 78	○ 79	○ 80	○ 81	○ 82	○ 83	○ 84	○ 85	○ 86	○ 87	○ 88	○ 89	○ 90	○ 91	○ 92	○ 93	○ 94	○ 95
○ 96	○ 97	○ 98	○ 99	○ 100	○ 101	○ 102	○ 103	○ 104	○ 105	○ 106	○ 107	○ 108	○ 109	○ 110	○ 111	○ 112	○ 113	○ 114	○ 115	○ 116	○ 117	○ 118	○ 119	○ 120	○ 121	○ 122	○ 123	○ 124	○ 125	○ 126	○ 127

№	Type	State	Active count	Payload
2	M82359	Work	0	0.0%
3	M82359	Work	0	0.0%
4	M82359	Work	0	0.0%
5	M82359	Work	0	0.0%

Channel info #	
Port/channel	-
Callref	-
Connected port/channel	-
Connected Callref	-
State	-
State timer	-
Incoming SS7 category	-
Incoming CdPN	-
Incoming CgPN	-
Outgoing SS7 category	-
Outgoing CdPN	-
Outgoing CgPN	-

Call IP-info # submodule #	
State	-
Codec	-
Status	-
Mode	-
SSRC	-
IP:port remote	-
IP:port local	-
MAC remote	-
MAC local	-

Channels state	
○	Idle
🟢	Active
🟡	Reserved

Channel connection information:

- *Port/channel* — port/channel data:

  - Signaling protocol (VoIP)
  - Port location VoIP submodule #/Channel #

- *Callref* — internal call identifier

- *Connected port/channel* — linked port/channel data:

  - Linked port signaling protocol (PRI/SS7/VoIP)
  - Linked port location Stream #:Channel # for PRI/SS7 or VoIP submodule #: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* — incoming/outgoing call dialing
  - *In-Call/ Out-Call* — incoming or outgoing occupation
  - *In-Busy/ Out-Busy* — sending 'busy' tone
  - *Talk* — channel is in call state
  - *Release* — channel release
  - *Wait-Ack* — waiting for acknowledgement
  - *Wait-CID* — waiting for CgPN (Caller ID)
  - *Wait-Num* — waiting for call dialing
  - *Hold* — subscriber is on hold

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

Channel states:

- *Idle (grey)* — initial state, channel is ready to serve the call
- *Active (green)* — active state, channel is engaged with active call
- *Reserved (yellow)* — channel is reserved for service needs (sending 'busy', 'ringback', 'PBX response' tone) or for a new call.

To view detailed channel information, left-click to select it from the table.

Channel connection information:

- *State* — channel state (see description above)
- *Codec* — utilized codecs (Payload Type is defined in square brackets)
- *Status* — media information transfer status, options:
  - *Good* — channel is in operation
  - *Loss of RTP* — loss of the opposite RTP stream (when 'RTP packet timeout' expires)
  - *VBD* — communication in data transfer mode has been established through the channel
  - *T38* — fax connection utilizing T.38 protocol has been established through the channel
- *Mode* — media channel operating mode:
  - *sendrecv* — channel operates in duplex mode (reception and transmission)
  - *sendonly* — channel operates in simplex mode, transmission only
  - *recvonly* — channel operates in simplex mode, reception only
  - *inactive* — channel is not active, reception and transmission are inactive
- *SSRC* — SSRC (Synchronization Source) field value for outgoing device RTP stream

- *IP:port remote* — remote IP address and port of RTP stream source
- *IP:port local* — local IP address and port of RTP stream source
- *MAC remote* — remote MAC address of RTP stream source
- *MAC local* — local MAC address of RTP stream source

There is a button 'Disconnect the call' below the tables, which allows disconnection

3.1.2.8 Fault alarms. Alarm events list.

When a failure occurs, related information containing the fault stream number, SS7 link set, signal link or faulty module will be output to the web configurator header. If there are multiple active alarms, the most critical alarm at the given moment will be shown in the web configurator header.

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

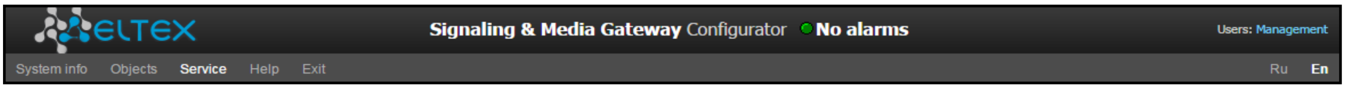


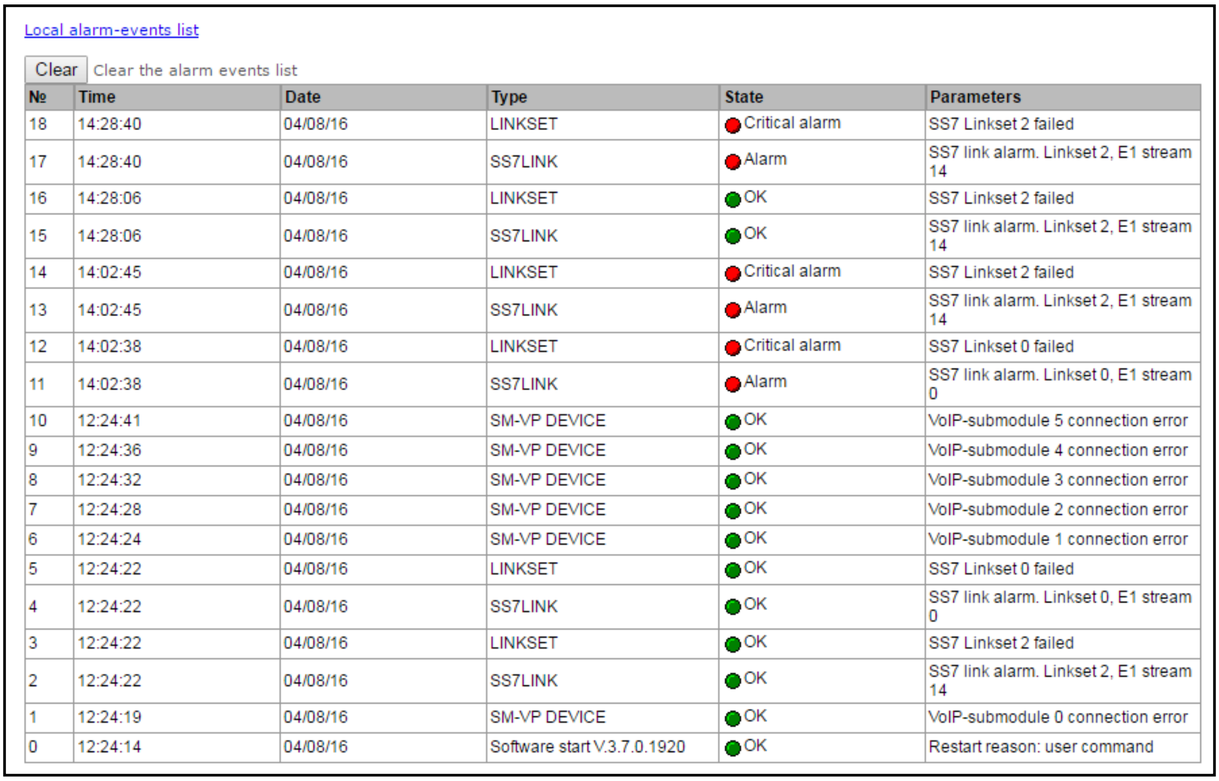
Table 17 — Alarm message examples

Alarm message	***Meaning***
Configuration is not read	Configuration file error
SIP-module connection error	Failure of a software module responsible for SIP operation
SS7 Linkset failed	SS7 link set failure
E1 stream alarm	E1 stream failure
SS7 link alarm	SS7 signal channel failure
Synchronization from local source. All configured sources are failed	Synchronization with a local source All defined sources are inoperable
E1 stream remote alarm	E1 stream remote fault
Synchronization from low-priority source	Primary synchronization source is lost, priority of the current source is lower
Failed to send CDR-files to FTP-server	Failed to send CDR file to FTP server
VoIP-submodule connection error	No communication with SM-VP submodule
RAM is almost exhausted	High RAM utilization alarm
No power on PSU	Primary power main is missing on one of the power supply units
H323-module connection error	Failure of a software module responsible for H.323 operation

High CPU temperature	Temperature 70°C - warning;
	85°C - alarm;
	100°C - critical alarm

SIP-interface is not responding on OPTIONS-requests	One of the SIP interfaces is not available
High CPU load	more than 90% - warning; more than 95% - alarm
Fans malfunction	One or multiple fans are inoperable
Low free space on a USB/HDD drive	Low free space on one of the external storage devices
CPS threshold is exceeded for TrunkGroup	Number of calls coming to one of the trunk groups per second exceeds the value defined by 'Alarm CPS value' option
SIP-interface INVITE duplication error	Duplication failures of INVITE received from emergency call service node. Failure might occur if duplication server is not available.

In 'Alarm events list' menu, you may find the list of alarm events arranged by time or date. The 'Clear' button deletes all the data in the current log.



№	Time	Date	Type	State	Parameters
18	14:28:40	04/08/16	LINKSET	🔴 Critical alarm	SS7 Linkset 2 failed
17	14:28:40	04/08/16	SS7LINK	🔴 Alarm	SS7 link alarm. Linkset 2, E1 stream 14
16	14:28:06	04/08/16	LINKSET	🟢 OK	SS7 Linkset 2 failed
15	14:28:06	04/08/16	SS7LINK	🟢 OK	SS7 link alarm. Linkset 2, E1 stream 14
14	14:02:45	04/08/16	LINKSET	🔴 Critical alarm	SS7 Linkset 2 failed
13	14:02:45	04/08/16	SS7LINK	🔴 Alarm	SS7 link alarm. Linkset 2, E1 stream 14
12	14:02:38	04/08/16	LINKSET	🔴 Critical alarm	SS7 Linkset 0 failed
11	14:02:38	04/08/16	SS7LINK	🔴 Alarm	SS7 link alarm. Linkset 0, E1 stream 0
10	12:24:41	04/08/16	SM-VP DEVICE	🟢 OK	VoIP-submodule 5 connection error
9	12:24:36	04/08/16	SM-VP DEVICE	🟢 OK	VoIP-submodule 4 connection error
8	12:24:32	04/08/16	SM-VP DEVICE	🟢 OK	VoIP-submodule 3 connection error
7	12:24:28	04/08/16	SM-VP DEVICE	🟢 OK	VoIP-submodule 2 connection error
6	12:24:24	04/08/16	SM-VP DEVICE	🟢 OK	VoIP-submodule 1 connection error
5	12:24:22	04/08/16	LINKSET	🟢 OK	SS7 Linkset 0 failed
4	12:24:22	04/08/16	SS7LINK	🟢 OK	SS7 link alarm. Linkset 0, E1 stream 0
3	12:24:22	04/08/16	LINKSET	🟢 OK	SS7 Linkset 2 failed
2	12:24:22	04/08/16	SS7LINK	🟢 OK	SS7 link alarm. Linkset 2, E1 stream 14
1	12:24:19	04/08/16	SM-VP DEVICE	🟢 OK	VoIP-submodule 0 connection error
0	12:24:14	04/08/16	Software start V.3.7.0.1920	🟢 OK	Restart reason: user command

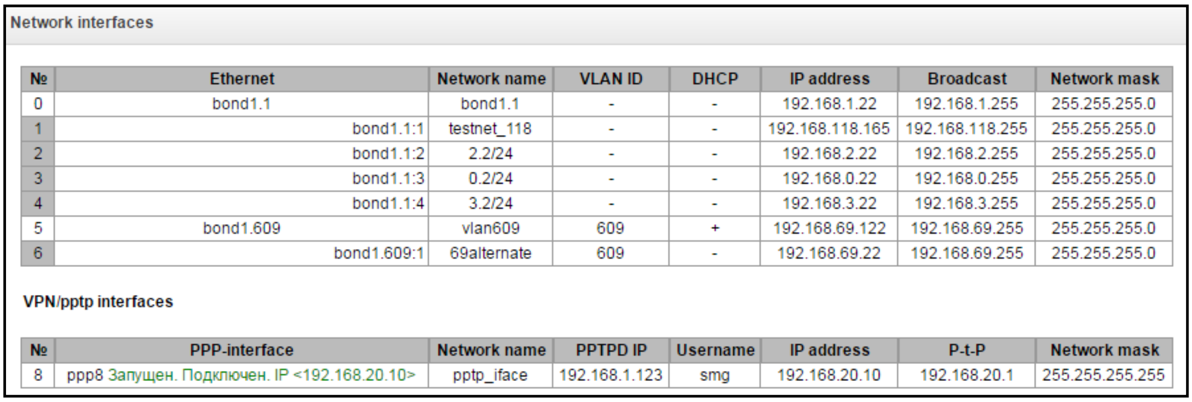
Alarm table:

- *Clear* — delete the current fault events table
- № — fault sequential number
- *Time* — fault occurrence time in HH:MM:SS format
- *Date* — fault occurrence date in DD/MM/YY format
- *Type* — fault type:
  - *CONFIG* — critical fault, configuration file fault
  - *SIPT-MODULE* — critical fault, failure of a software module responsible for VoIP operation
  - *LINKSET* — critical fault, SS7 link set is not in operation
  - *STREAM* — critical fault, E1 stream is in operation
  - *SM-VP DEVICE* — fault, SM-VP module failure
  - *SS7LINK* — SS7 signal channel failure
  - *SYNC* — synchronization fault, synchronization source is missing
  - *STREAM-REMOTE* — warning, E1 stream remote fault
  - *CDR-FTP* — fault or warning, failed to send CDR file to FTP server
  - *TRUNK-CPS* — permitted number of calls per second is exceeded for a trunk group
  - *SIP-DUPLICATE* - duplication failures of INVITE received from emergency call service node;
- *State* — fault state status:
  - *critical fault, flashing red icon* — fault requires immediate intervention of the service personnel, affects device operation and provisioning of communication services
  - *fault, red icon* — non-critical fault, also requires intervention of the service personnel
  - *warning, yellow icon* — fault does not affect provisioning of communication services
  - *OK, green icon* — fault is resolved
- *Parameters* — text description of fault details Depending on the fault type, may appear as follows:

- CONFIG
- SIPT-MODULE — no communication with SIP module
- LINKSET — SS7 link set XX is not in operation, where XX is SS7 link set number
- STREAM — E1 XX stream failure, where XX is stream number
- *SM-VP DEVICE* — no communication with VoIP submodule XX, where XX is SM-VP submodule number
- *SS7LINK* — SS7 link failure Linkset XX, E1 stream YY, where XX is SS7 link set number, YY is a signal channel number in SS7 group
- *TRUNK-CPS* — 'XX' trunk group exceeds CPS threshold, where XX is a trunk group name
- *SIP-DUPLICATE* - SIP interface 'XX'. INVITE duplication to the '<YY>' server failure, where XX - SIP interface name, on which failure was occurred; YY - duplication server address, on which failure was occurred.

3.1.2.9 Network interface monitoring

This section allows for monitoring of network interfaces (tagged/untagged/VPN) and viewing users connected to VPN device.



Network interfaces

№	Ethernet	Network name	VLAN ID	DHCP	IP address	Broadcast	Network mask
0	bond1.1	bond1.1	-	-	192.168.1.22	192.168.1.255	255.255.255.0
1	bond1.1:1	testnet_118	-	-	192.168.118.165	192.168.118.255	255.255.255.0
2	bond1.1:2	2.2/24	-	-	192.168.2.22	192.168.2.255	255.255.255.0
3	bond1.1:3	0.2/24	-	-	192.168.0.22	192.168.0.255	255.255.255.0
4	bond1.1:4	3.2/24	-	-	192.168.3.22	192.168.3.255	255.255.255.0
5	bond1.609	vlan609	609	+	192.168.69.122	192.168.69.255	255.255.255.0
6	bond1.609:1	69alternate	609	-	192.168.69.22	192.168.69.255	255.255.255.0

VPN/pptp interfaces

№	PPP-interface	Network name	PPTPD IP	Username	IP address	P-t-P	Network mask
8	ppp8 Запущен. Подключен. IP <192.168.20.10>	pptp_iface	192.168.1.123	smg	192.168.20.10	192.168.20.1	255.255.255.255

- *Ethernet* — Ethernet interface name
- *Network name* — name that the current network settings are associated with
- *VLAN ID* — virtual network identifier (for tagged interface)
- *DHCP* — DHCP usage status, allows to obtain network settings automatically (DHCP server is required in the operator network)
- *IP address*, *network mask*, *broadcast* — interface network settings (if DHCP is not used)

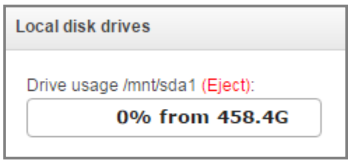
VPN/pptp interfaces

- *PPP interface* — name of the interface
- *Network name* — name that the current network settings are associated with
- *PPTPD IP* — PPTP server IP address used for connection
- *Username* — username identifier
- *IP address*, *P-t-P, network mask* — interface network settings

3.1.2.10 Local disk drives

This section contains information on the connected storage media.

- *Remove* — click this link to safely remove the storage device.



Local disk drives

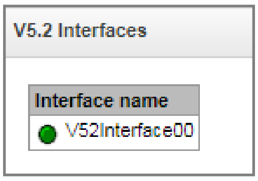
Drive usage /mnt/sda1 (Eject):

0% from 458.4G

3.1.2.11 V5.2 interfaces

The state of V5.2 interfaces is displayed in this section[1].

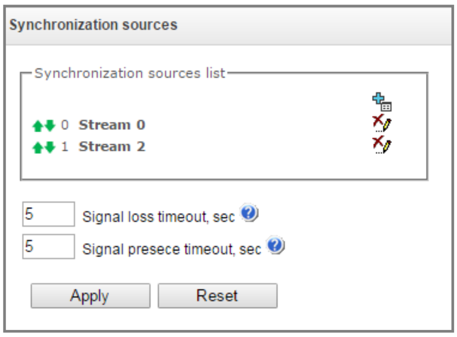
– *Red*— the interface is out of the operation;
– *Green* — the interface is on operation.



V5.2 Interfaces

Interface name
● V52Interface00

3.1.3 Synchronization sources



Synchronization sources

Synchronization sources list

0 Stream 0

1 Stream 2

5 Signal loss timeout, sec

5 Signal presece timeout, sec

Apply Reset

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

You may specify up to 18 synchronization sources (each of 16 E1 streams and 2 external sources).

The ports receiving external signals have the impedance of 120 Ohm. According to ITU-T G.703 recommendation, section 15, the incoming signal should have the parameters as presented on the figure on the right.

To generate the list, use the following buttons:

➕ — *'Add source'*;

✗ — *'Remove'*.

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

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

- *Return timeout* — time interval of the restored higher priority synchronization signal activity that should pass before the system switches to that signal.

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

3.1.4 CDR settings

In this section, you may configure parameters for storing detailed call records.

[1] Available for the devices with V5.2 license. Read more detailed information on licenses in the section 3.1.23 Licenses.

CDR is a detailed call record that enables saving history of calls performed through SMG.

CDR settings

- *Enable CDR* — when checked, the gateway will generate CDRs

CDR files settings

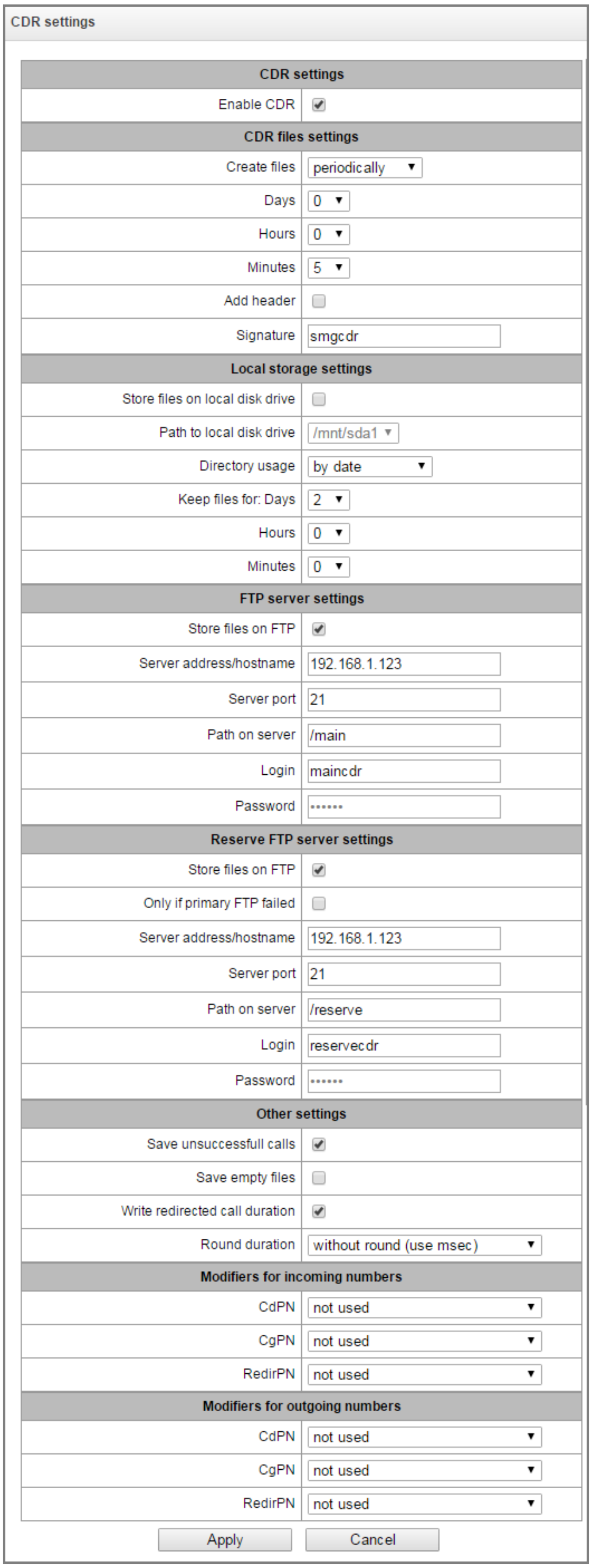
- *Create files* — CDR file creation mode:
  - *periodically* — CDR file will be created upon the expiry of the specific period from the device startup
  - *once per day* — CDR file will be created once a day at the defined time
  - *once per hour* — CDR file will be created once an hour at the defined minute

- *Saving period Days, Hours, Minutes* — time period for CDR generation and saving in the device RAM

- *Add header* — when checked, the following header will be written at the beginning of CDR file: SMG1016. CDR. File started at 'YYYYMMDDhhmmss', where 'YYYYMMDDhhmmss' is the record saving start time.

- *Signature* — specify distinctive feature that will facilitate identification of the device that created the record.

- *Filename format* – change CDR file format. The option is available only when 'once per day' is selected. The following values are available:
  - *Date and time* – change the CDR fie format according to the following template "YYYYMMDDhhmmss.cdr";
  - *Date only* – change the CDR fie format according to the following template "YYYYMMDD.cdr".



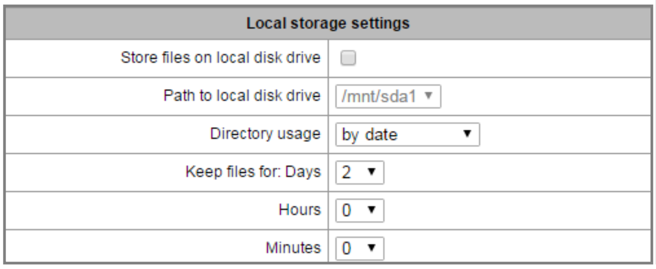
CDR settings

CDR settings	
Enable CDR	☑
CDR files settings	
Create files	periodically ▼
Days	0 ▼
Hours	0 ▼
Minutes	5 ▼
Add header	☐
Signature	smgcdr
Local storage settings	
Store files on local disk drive	☐
Path to local disk drive	/mnt/sda1 ▼
Directory usage	by date ▼
Keep files for: Days	2 ▼
Hours	0 ▼
Minutes	0 ▼
FTP server settings	
Store files on FTP	☑
Server address/hostname	192.168.1.123
Server port	21
Path on server	/main
Login	maincdr
Password	••••••
Reserve FTP server settings	
Store files on FTP	☑
Only if primary FTP failed	☐
Server address/hostname	192.168.1.123
Server port	21
Path on server	/reserve
Login	reservecdr
Password	••••••
Other settings	
Save unsuccessfull calls	☑
Save empty files	☐
Write redirected call duration	☑
Round duration	without round (use msec) ▼
Modifiers for incoming numbers	
CdPN	not used ▼
CgPN	not used ▼
RedirPN	not used ▼
Modifiers for outgoing numbers	
CdPN	not used ▼
CgPN	not used ▼
RedirPN	not used ▼

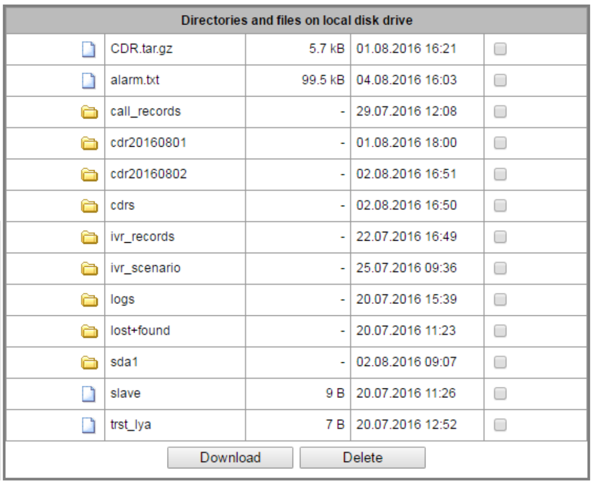
Local storage settings

- *Store files on local disk drive* — when checked, save CDRs on local storage media.
- *Path to local disk drive* — path to local storage media. When the path to disk is specified, list of folders and files located on that disk will be shown in the menu. To download data to the PC,

select checkboxes located next to the required records and click *'Download'*. At that, record folder will be moved to the archive, which should be deleted in order to avoid disk overfill. To delete obsolete data, select checkboxes located next to the required records and click *'Delete'*.



Local storage settings	
Store files on local disk drive	□
Path to local disk drive	/mnt/sda1 ▼
Directory usage	by date ▼
Keep files for: Days	2 ▼
Hours	0 ▼
Minutes	0 ▼



Directories and files on local disk drive				
🗋	CDR.tar.gz	5.7 kB	01.08.2016 16:21	□
🗋	alarm.txt	99.5 kB	04.08.2016 16:03	□
🗀	call_records	-	29.07.2016 12:08	□
🗀	cdr20160801	-	01.08.2016 18:00	□
🗀	cdr20160802	-	02.08.2016 16:51	□
🗀	cdrs	-	02.08.2016 16:50	□
🗀	ivr_records	-	22.07.2016 16:49	□
🗀	ivr_scenario	-	25.07.2016 09:36	□
🗀	logs	-	20.07.2016 15:39	□
🗀	lost+found	-	20.07.2016 11:23	□
🗀	sda1	-	02.08.2016 09:07	□
🗋	slave	9 B	20.07.2016 11:26	□
🗋	trst_lya	7 B	20.07.2016 12:52	□

- *Directory usage* — select directories for CDR data storage
  - *by date* — CDRs will be saved in separate directories, directory names correspond to the CDR file creation date, name format is 'cdrYYYYMMDD', for example: cdr20150818
  - *single directory* — all CDRs will be saved into a single folder 'cdr_all' located on the specified storage device.
- *Keep files for*: *Days, Hours, Minutes* — period of CDR storage on the local device.

✓ **When FTP server is not available, CDRs will be saved to the device RAM. When the memory is filled, the warning will be indicated first, then alarm. For CDR file saving indication, see Section 1.6.5.**

✓ **When the specific alarm level is achieved, the system sends corresponding SNMP trap.**

CDR storage memory limits table.

If FTP server is not available for data storage, certain memory volume is allocated on the device for temporary CDR storage. Warnings and alarms are indicated in case of memory overloading.

	SMG-1016M	SMG-2016
Allocated memory:	30 MB	512 MB
Critical values:		
- warning	512 KB	20 MB
- alarm	5 MB	85 MB
- critical alarm	15 MB	255 MB

One CDR entry takes from 200 to 400 bytes. Thus, 1 MB keeps from 2600 to 5200 entries.

FTP server settings

- *Store files on FTP* — when checked, CDRs will be transferred to FTP server
- Server address/hostname — FTP server IP address
- *Server port* — FTP server TCP port
- *Path on server* — defines path to FTP server folder for CDR storage
- *Login* — username for FTP server access
- *Password* — user password for FTP server access

Reserve FTP server settings

When the main FTP server is unavailable, CDRs will be sent to a redundant server (when the redundant FTP server is configured respectively) until the connection with the main FTP server is restored.

- *Store files on FTP* — when checked, CDRs will be transferred to a redundant FTP server
- *Only if primary FTP failed* – if the option is set, the saving of CDR files on a redundant FTP 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 main and redundant FTP servers simultaneously.
- *Server address/hostname* — redundant FTP server IP address
- *Server port* — redundant FTP server TCP port
- *Path on server* — defines path to a redundant FTP server folder for CDR storage
- *Login* — username for redundant FTP server access
- *Password* — user password for redundant FTP server access

Other settings

- *Save unsuccessful calls* — when checked, store unsuccessful calls (not resulted in conversation) into CDR files.
- *Save empty files* — when checked, save CDR files without records.
- *Write redirected call duration* — when checked, CDR for a call redirected from 'discinfo: redirected call;' will contain an actual call duration; when unchecked, duration will be set to zero.
- *Swap redirecting number and CgPN* – the option might be used for redirected calls in case of simultaneous use of CgPN and Redirecting number fields in CDR entries. In case of absence of Redirecting number field in an CDR entry, CgPN is replaced by Redirecting number for redirected calls.
- *Round duration* — this option specifies duration rounding mode in CDRs:
  - *Upwards* — call duration rounding mode; call duration value will be rounded up when it exceeds 330ms;
  - *Downwards* — call duration rounding mode; call duration value will be rounded down when it exceed 850ms.
  - *Without round (use msec)* — in the mode, call duration will be not rounded and it will be recorded within the accuracy of milliseconds.

Modifiers for incoming numbers

Incoming number modifiers — modifiers that modify CDR fields containing subscriber numbers and apply to these fields before a call proceeds through the dial plan.

- *CdPN* — designed for modifications based on the analysis of the callee number received from the incoming channel.
- *CgPN* — designed for modifications based on the analysis of the caller number received from the incoming channel.
- *RedirPN* — designed for modifications based on the analysis of the number of the subscriber that performed call redirection received from the incoming channel.

Modifiers for outgoing numbers

Outgoing number modifiers — modifiers that modify CDR fields containing subscriber numbers and apply to these fields after a call proceeds through the dial plan.

- *CdPN* — designed for modifications based on the analysis of the callee number sent to the outgoing channel.
- *CgPN* — designed for modifications based on the analysis of the caller number sent to the outgoing channel.
- *RedirPN* — designed for modifications based on the analysis of the number of the subscriber that performed call redirection sent to the outgoing channel.

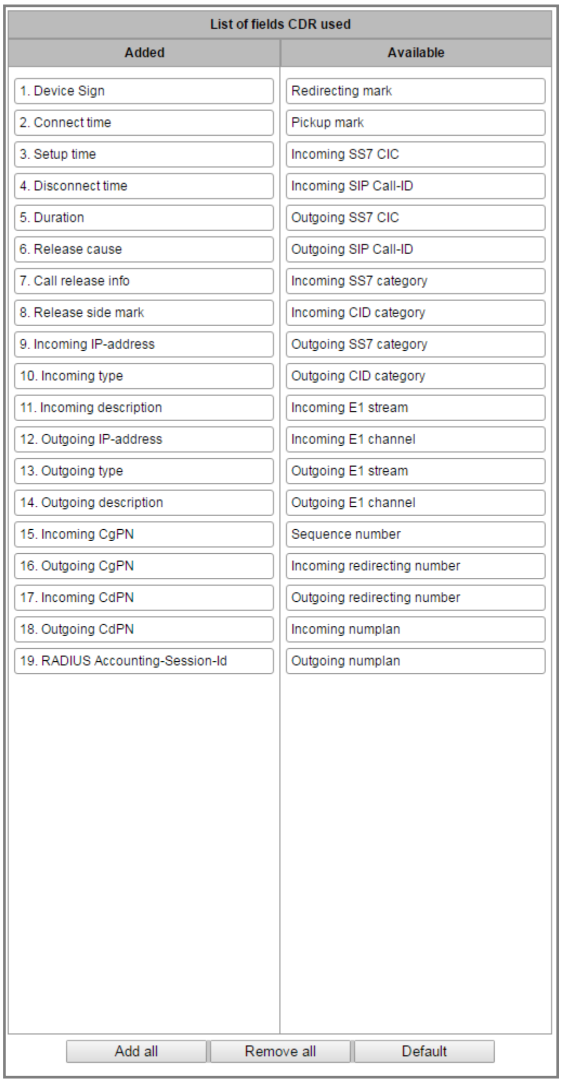
3.1.4.1 List of fields CDR used

You may select fields that will be written in CDR files and you may configure their order. All the fields which are available for adding are displayed in 'Available' column. Added fields are displayed in 'Added' column in order of recording to CDR files.

The following buttons are located under the list:

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

Drag-and-drop the necessary fields to corresponding column by left mouse button to add or delete fields. 'Added' column has numeration which displays sequential field number in CDR.



List of fields CDR used

Added	Available
1. Device Sign	Redirecting mark
2. Connect time	Pickup mark
3. Setup time	Incoming SS7 CIC
4. Disconnect time	Incoming SIP Call-ID
5. Duration	Outgoing SS7 CIC
6. Release cause	Outgoing SIP Call-ID
7. Call release info	Incoming SS7 category
8. Release side mark	Incoming CID category
9. Incoming IP-address	Outgoing SS7 category
10. Incoming type	Outgoing CID category
11. Incoming description	Incoming E1 stream
12. Outgoing IP-address	Incoming E1 channel
13. Outgoing type	Outgoing E1 stream
14. Outgoing description	Outgoing E1 channel
15. Incoming CgPN	Sequence number
16. Outgoing CgPN	Incoming redirecting number
17. Incoming CdPN	Outgoing redirecting number
18. Outgoing CdPN	Incoming numplan
19. RADIUS Accounting-Session-Id	Outgoing numplan

3.1.4.2 Default CDR format

- First line - header, general for a whole CDR file (parameter is present, if the corresponding setting is selected).
- Next line - CDR records in the form of fields separated by ‘;’. Basic set of fields is following:

  - 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

- Caller information:

  - Incoming IP address
  - Incoming type
  - Incoming description - subscriber/trunk name (TG)
  - Incoming CgPN - caller number on input
  - Outgoing CgPN - caller number on output

- Callee information:

  - Outgoing IP address
  - Outgoing type
  - Outgoing description - subscriber/trunk name (TG)
  - Incoming CdPN
  - Outgoing CdPN
  - Connect time in format: YYYY-MM-DD hh:mm:ss;
  - Disconnect time in format: YYYY-MM-DD hh:mm:ss.

3.1.4.3 CDR entries description

Device sign — a line configured by user that identifies a device;

Connect time, setup time, disconnect time — time in «YYYY-MM-DD HH:MM:SS.msec» format;

Duration is displayed in seconds. If you choose 'without rounding' seconds are displayed with milliseconds as 'SS.msec'

Release cause — code of disconnection, according to ITU-T Q.850 recommendations;

Call release info — call status in case of disconnection

- *user answer* — successful call
- *user called, but unanswer* — unsuccessful call, no reply from subscriber
- *unassigned number* — unsuccessful call, number is not assigned
- *user busy* — unsuccessful, user is busy
- *uncomplete number* — unsuccessful call, number is not complete

- *out of order* — unsuccessful call, terminal equipment is not available
- *unavailable trunk line* — unsuccessful call, 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 RADIUS server
- *unspecified* — unsuccessful call, other reason.

Incoming/outgoing IP address - IP address, if a call is implemented via SIP/H.323. '0.0.0.0' value will be displayed in case call is transmitted not via an IP network.

Incoming/outgoing types

- *SIP-user* — SIP subscriber
- *v52-user – V*5.2 subscriber;
- *user-service* – VAS call, only for source type;
- *trunk-SIP* — SIP trunk
- *trunk-SS7* — SS7 trunk
- *trunk-Q931* — ISDN PRI trunk
- *trunk-H.323 — H.323 trunk*

Incoming description - contains name of the trunk through which a call or subscriber title has been transmitted. If the call is initiated by value added service, the description may have the following values:

- *Redirection*;
- *CallTransfer*;
- *CallPickup*;
- *ServiceManagement* – value added services management;
- *Conference* – conference add-on;
- *IVR* – ringing from IVR;
- *3way* – 3-Way conference.

Incoming/outgoing CgPN - number of a caller on input (before modifications in incoming trunk group) or number of a caller on output (after modifications in incoming and outgoing trunk group)

Incoming/outgoing CdPN - number of a callee on input (before modifications in incoming trunk group) or number of a callee on output (after modifications in incoming and outgoing trunk group)

Redirecting mark

- *normal* — call w/o redirection

- *redirecting* — the caller has redirected a call to the callee;
- *redirected* — caller was forwarded to another subscriber.

Pickup mark:

- *normal* - a call was not picked up;
- *pickup* - a call was picked up.

Release side mark – side where signal of connectivity break came from. This signal takes the next values:

1) originate –caller ends the call;
2) answer –callee ends the call.

Incoming/outgoing SS7 CIC - number CIC for incoming/outgoing call. If a call wasn't performed via SS7 interface field will be empty;

Incoming/outgoing SIP Call-ID - Call-ID of incoming/outgoing call. If a call wasn't performed via SIP field will be empty;

Incoming/outgoing SS7 category - category of SS7 caller on input (before modification on incoming TG) or on output (after modifications of incoming and outgoing TG);

Incoming/outgoing CID category – CID category on input (before modification on incoming TG) or on output (after all modifications of incoming and outgoing TG);

Incoming/outgoing E1 stream– number of incoming/outgoing E1 flow. If call wasn't performed by E1 flow the field will be empty;

Incoming/outgoing E1 channel– number of incoming/outgoing E1 channel. If a call wasn't performed via E1 field will be empty;

Sequence number – two numbers separated by hyphen. First is a time tag generated during the device start, the second – sequence number of the CDR record.

Incoming/outgoing redirecting number – for warder number on input (before modification in incoming TG) or on output (after all modifications in incoming and outgoing TG);

RADIUS Accounting-Session-Id - 'Acct-Session-Id' attribute value transmitted to RADIUS.

Global Callref – Global Call Reference field which is formed by the following rule: "|XX.XX.XX|YY.YY.YY.YY.YY", where:

XX.XX.XX - originating point code in the form of little-endian HEX;
YY.YY.YY.YY.YY - sequence number of a call in the form of little-endian HEX;

Incoming/outgoing numplan– dial plan number through which call was transmitted and received.

3.1.4.4 Example of CDR file

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

1. Sequence number;

2. Device sign;
3. Connect time;
4. Setup time;
5. Disconnect time;
6. Duration;
7. Release cause;
8. Call release info;
9. Release side mark;
10. Redirecting mark;
11. Pickup mark;
12. Incoming type;
13. Incoming description;
14. Incoming E1 stream;
15. Incoming IP address;
16. Incoming CgPN;
17. Outgoing CgPN;
18. Outgoing type;
19. Outgoing description;
20. Outgoing E1 stream;
21. Outgoing IP address;
22. Incoming CdPN;
23. Outgoing CdPN;

RADIUS Accounting-Session-Id
SMG2016. CDR. File started at '20161213115258'

20161210124301-00000;SMG 2016 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 2016 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 2016 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.

3.1.4.5 The maximum size of CDR fields

Parameter	The maximum size of the field
Device Sign	63
Setup time	63

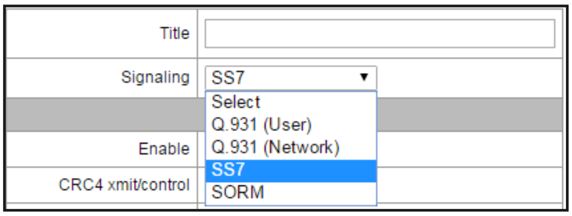
Connect time	63
Disconnect time	63
Duration	15
Release cause	4
Call release info	63
Incoming IP-address	31
Incoming type	63
Incoming description	63
Outgoing IP-address	31
Outgoing type	63
Outgoing description	63
Incoming CgPN	41
Outgoing CgPN	41
Incoming CdPN	41
Outgoing CdPN	41
Incoming redirecting number	41
Outgoing redirecting number	41
Redirecting mark	31
Pickup mark	31
Release side mark	31
Incoming SS7 CIC	15
Incoming SIP Call-ID	255
Outgoing SS7 CIC	15
Outgoing SIP Call-ID	255
Incoming SS7 category	3
Incoming Calling party category (RUS)	3
Outgoing SS7 category	3
Outgoing Calling party category (RUS)	3
Incoming E1 stream	3
Incoming E1 channel	3
Outgoing E1 stream	3
Outgoing E1 channel	3
Sequence number	15
RADIUS Accounting-Session-Id	63
Global Callref	63
Incoming numplan	3
Outgoing numplan	3

3.1.5 E1 streams

In this section, you may configure signaling and parameters for each E1 stream.

3.1.5.1 Signaling protocol selection

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



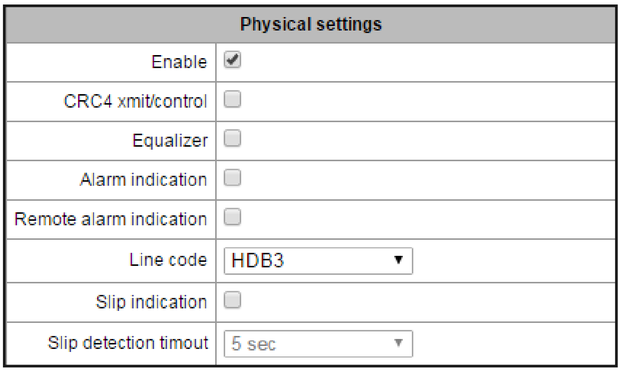
Title

Signaling: SS7

Device supports the following signaling protocols:

- Q.931 (User);
- Q.931 (Network);
- SS7;
- V5.2 (LE);
- M2UA[1];
- IUA (User)[1];
- IUA (Network)[1];
- Media Gateway[1].

3.1.5.2 Configuration of physical parameters



Physical settings	
Enable	☑
CRC4 xmit/control	□
Equalizer	□
Alarm indication	□
Remote alarm indication	□
Line code	HDB3 ▼
Slip indication	□
Slip detection timout	5 sec ▼

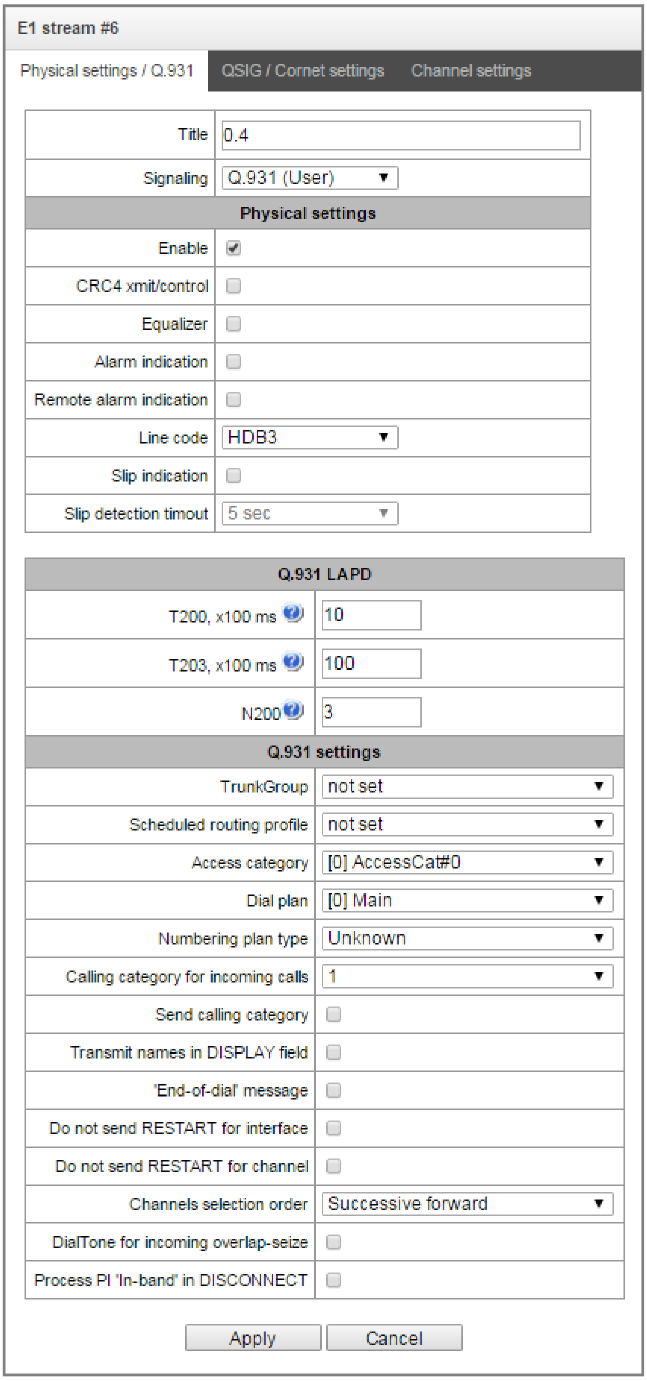
Physical settings:

- *Title* — E1 stream name.
- *Enable* — physically enable stream.
- *CRC4 xmit/control* — CRC4 check sum generation during transmission and control during 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 added 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 added 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.

[1] Not supported in the current firmware version

3.1.5.3 Q.931 signaling protocol configuration

3.1.5.3.1 'Physical parameters/Q.931' tab



E1 stream #6

Physical settings / Q.931 | QSIG / Cornet settings | Channel settings

Title	0.4
Signaling	Q.931 (User) ▼
Physical settings	
Enable	☑
CRC4 xmit/control	□
Equalizer	□
Alarm indication	□
Remote alarm indication	□
Line code	HDB3 ▼
Slip indication	□
Slip detection timout	5 sec ▼

Q.931 LAPD	
T200, x100 ms	10
T203, x100 ms	100
N200	3
Q.931 settings	
TrunkGroup	not set ▼
Scheduled routing profile	not set ▼
Access category	[0] AccessCat#0 ▼
Dial plan	[0] Main ▼
Numbering plan type	Unknown ▼
Calling category for incoming calls	1 ▼
Send calling category	□
Transmit names in DISPLAY field	□
'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	□

Q.931 LAPD – LAPD channel-level parameters of Q.931 protocol

- *T200* — transmission timer. This timer defines time period for frame response reception that will enable the following frames' transmission. This time period should be greater than the time required for frame transmission and its acknowledgement reception.
- *T203* — maximum time during which the device may not exchange frames with the opposite device.
- *N200* — quantity of frame retransmission attempts.

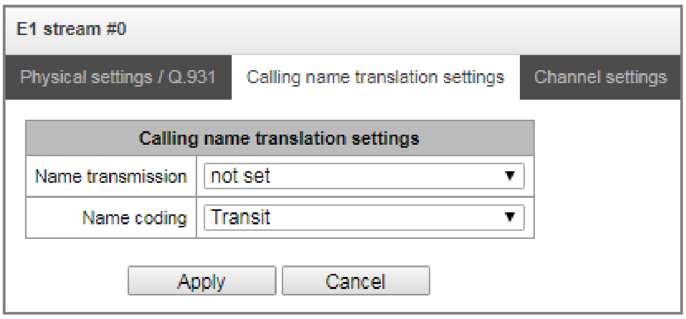
_Q._931 parameters

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

Proper operation requires that this mode is supported by the opposite party.

- *'End of dial' message* — produce 'Sending Complete' informational element upon 'End of dial' event (such event arrives from the linked channel side, achieved maximum quantity of digits according to prefix, dialing timeout for the next digit).
- *Do not send RESTART for interface* — when checked, gateway will not send RESTART message into the line when the stream is restored (channel level LAPD is established).
- *Do not send RESTART for channel* — when checked, gateway will not send RESTART message upon the expiration of T308 timer. This timer activates when RELEASE message is sent into the channel and resets when it receives RELEASE COMPLETE message as a response. If RELEASE COMPLETE message is not received during T308 timer active state, RESTART message is transmitted in order to release the channel.
- *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 engagement('PBX response' ready signal). In this case, overlap engagement is a reception of SETUP message without 'sending complete' indication.
- *Process PI 'In-Band' in DISCONNECT* — when checked, field *PI In-Band* contained in DISCONNECT message will be processed for call release voice message transmission, otherwise this field is ignored.

3.1.5.3.2 «Calling name translation settings» tab


E1 stream #0

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

Calling name translation settings

Name transmission	not set
Name coding	Transit

On this tab, you may configure the method of subscriber names receiving/transmitting and the coding of receiving/transmitting names.

– *Name transmission:*

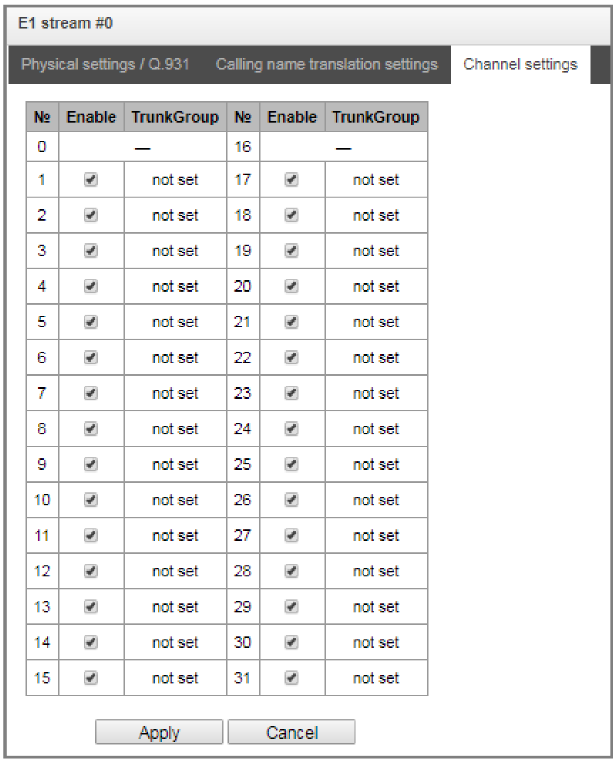
- *Not set* – transmission of names is disabled;
- *Q.931 DISPLAY* – transmission in Q.931 Display element with Codeset 5;
- *QSIG-NA* – transmission via QSIG-NA (ECMA-164);
- *CORNET* – transmission via Siemens CorNet;
- *CORNET HICOM-350* – transmission via Siemens CorNet with additional information for Hicom PBX;
- *AVAYA DISPLAY* – transmission in Q.931 Display element with Codeset 6.

– *Name coding:*

- *Transit* – re-coding is disabled (a name is supposed to be received in UTF-8, by default);
- *CP 1251* – Windows-1251 coding;
- *Siemens adaptation* – Siemens PBX coding;
- *AVAYA adaptation* – AVAYA PBX coding;
- Latin transliteration – Russian names will be transliterated with Latin letters.

3.1.5.3.3 «Channel settings» tab

You may enable or disable an E1 channel in this menu. For this, you need to check (or uncheck) the box next to the necessary channel. The numbers of the group, in which the channels are configured (it is used when a trunk group is set not for the whole stream but for stream's channels), are displayed in the «Trunk group» column.

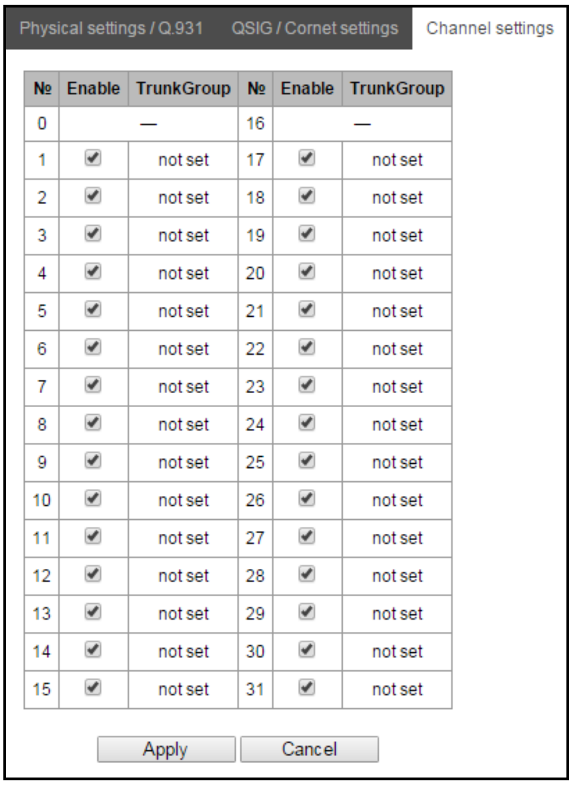


E1 stream #0

№	Enable	TrunkGroup	№	Enable	TrunkGroup
0		—	16		—
1	☑	not set	17	☑	not set
2	☑	not set	18	☑	not set
3	☑	not set	19	☑	not set
4	☑	not set	20	☑	not set
5	☑	not set	21	☑	not set
6	☑	not set	22	☑	not set
7	☑	not set	23	☑	not set
8	☑	not set	24	☑	not set
9	☑	not set	25	☑	not set
10	☑	not set	26	☑	not set
11	☑	not set	27	☑	not set
12	☑	not set	28	☑	not set
13	☑	not set	29	☑	not set
14	☑	not set	30	☑	not set
15	☑	not set	31	☑	not set

3.1.5.3.4 Channel settings tab

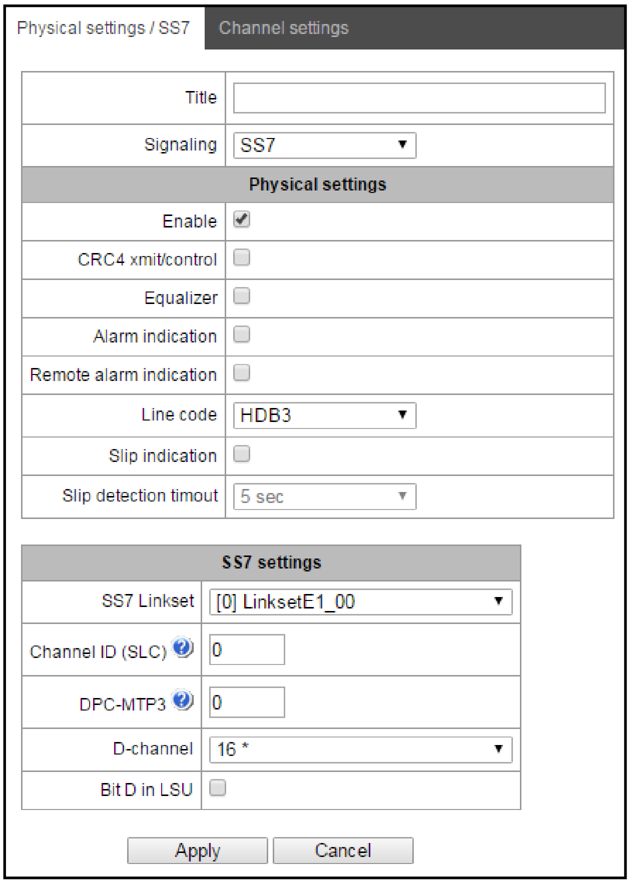
Use this tab to configure channel usage — select the checkbox next to the used channel number.



№	Enable	TrunkGroup	№	Enable	TrunkGroup
0		—	16		—
1	☑	not set	17	☑	not set
2	☑	not set	18	☑	not set
3	☑	not set	19	☑	not set
4	☑	not set	20	☑	not set
5	☑	not set	21	☑	not set
6	☑	not set	22	☑	not set
7	☑	not set	23	☑	not set
8	☑	not set	24	☑	not set
9	☑	not set	25	☑	not set
10	☑	not set	26	☑	not set
11	☑	not set	27	☑	not set
12	☑	not set	28	☑	not set
13	☑	not set	29	☑	not set
14	☑	not set	30	☑	not set
15	☑	not set	31	☑	not set

3.1.5.4 SS7 signaling protocol configuration

3.1.5.4.1 Physical parameters/SS7 tab



Title	
Signaling	SS7
Physical settings	
Enable	☑
CRC4 xmit/control	□
Equalizer	□
Alarm indication	□
Remote alarm indication	□
Line code	HDB3
Slip indication	□
Slip detection timout	5 sec

SS7 settings	
SS7 Linkset	[0] LinksetE1_00
Channel ID (SLC)	0
DPC-MTP3	0
D-channel	16 *
Bit D in LSU	□

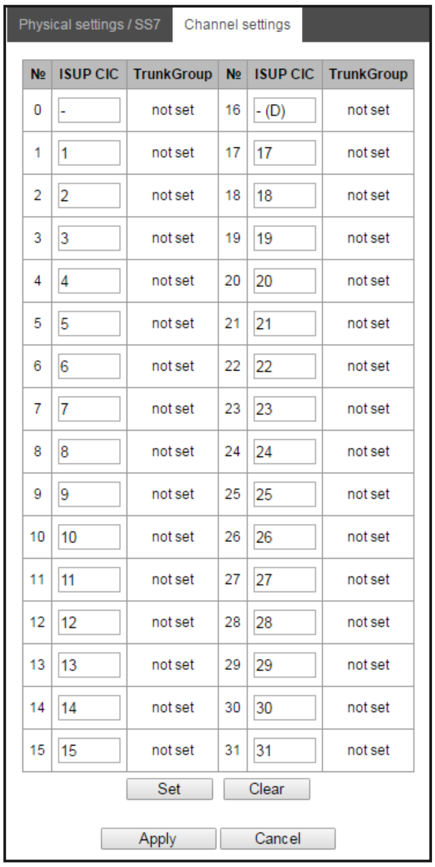
SS7 settings

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

3.1.5.4.2 Channel settings tab



Physical settings / SS7 | Channel settings

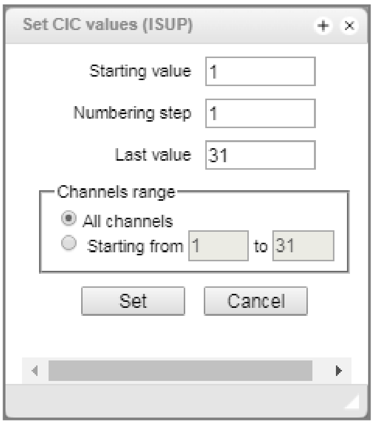
№	ISUP CIC	TrunkGroup	№	ISUP CIC	TrunkGroup
0	-	not set	16	- (D)	not set
1	1	not set	17	17	not set
2	2	not set	18	18	not set
3	3	not set	19	19	not set
4	4	not set	20	20	not set
5	5	not set	21	21	not set
6	6	not set	22	22	not set
7	7	not set	23	23	not set
8	8	not set	24	24	not set
9	9	not set	25	25	not set
10	10	not set	26	26	not set
11	11	not set	27	27	not set
12	12	not set	28	28	not set
13	13	not set	29	29	not set
14	14	not set	30	30	not set
15	15	not set	31	31	not set

- *ISUP CIC — channel identifier code* — setting voice link numbers(CIC).

For voice link automatic numbering, click *'Set'* button.

At that, the following menu will open:

- *Starting value* — number of the first voice link.
- *Numbering step* — channel numbering step. A number will be assigned to each of the subsequent channels that is greater by the numbering step than of the previous channel.
- *Last value* – a number which will be assigned to the last CIC channel in the range;
- *Channels range* — select values in this block to assign numbering for all stream channels or for specific channel range.



Set CIC values (ISUP)

Starting value: 1

Numbering step: 1

Last value: 31

Channels range

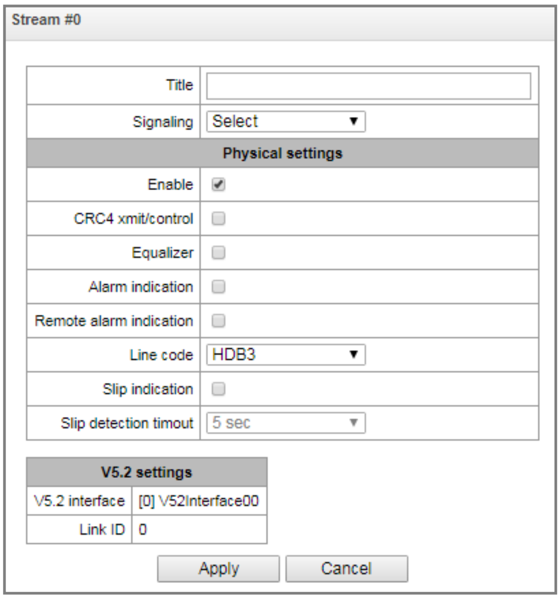
● All channels

○ Starting from 1 to 31

3.1.5.5 V5.2 settings

The assignment of the V5.2 interface might be implemented in the V5.2 interface settings tab.

The section includes parameters of the current V5.2 interface to which the stream is assigned and the identifier of the stream of V5.2 interface.



Stream #0

Title	
Signaling	Select ▼
Physical settings	
Enable	☑
CRC4 xmit/control	□
Equalizer	□
Alarm indication	□
Remote alarm indication	□
Line code	HDB3 ▼
Slip indication	□
Slip detection timout	5 sec ▼

V5.2 settings	
V5.2 interface	[0] V52Interface00
Link ID	0

3.1.6 Dial plans

In this section, you may configure the device dial plan.

The device features up to 16 independent dial plan (up to 255 for SMG-2016 with VAS license). Each dial plan may have its own subscribers and prefixes. To set the quantity of active plans, see Section 3.1.1.

Call routing on the device is performed using 3 criteria:

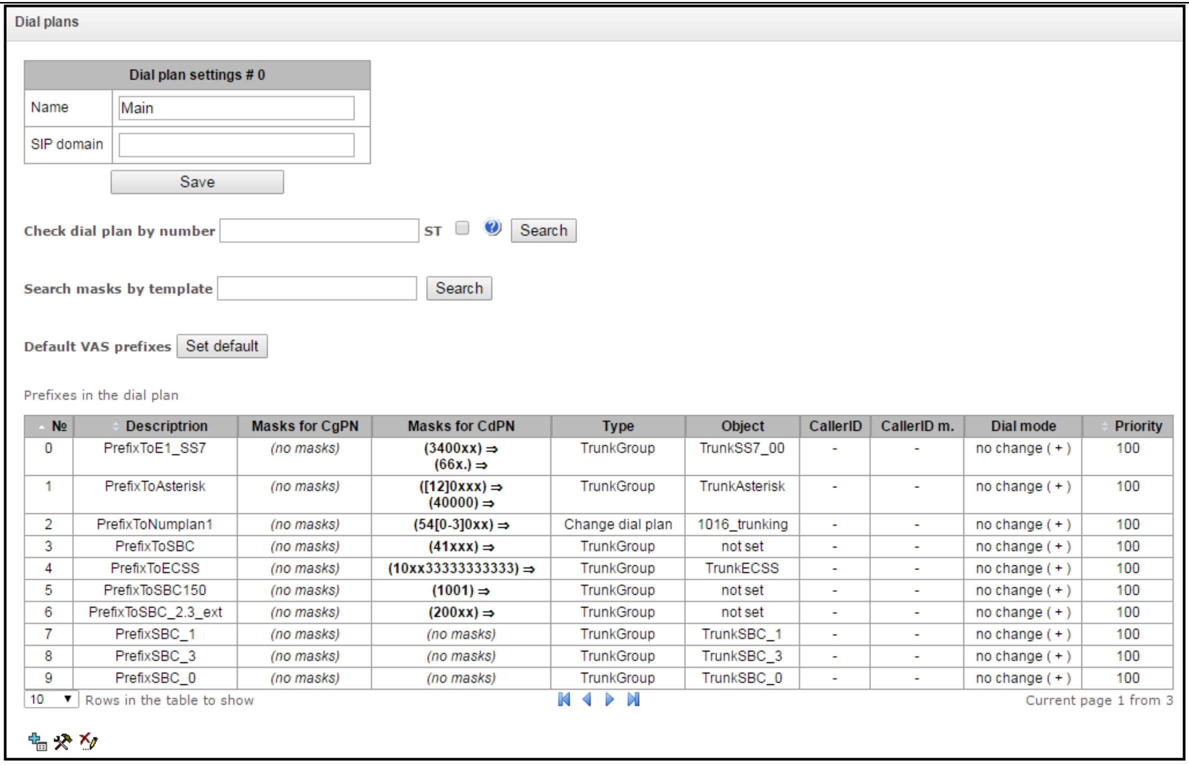
- Search by caller number — CgPN (Calling Party Number).
- Search by callee number — CdPN (Called Party Number).
- Search in a database containing subscribers configured on the device.

When the call arrives to the dial plan, its routing begins; originally, a search for CgPN number mask matches is performed followed by search in a database containing subscribers configured on the device. If match is found by one of the parameters, the routing will be performed and further search will stop.

Search and call routing using a database containing subscribers configured on the device will be 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 will be performed.

If CgPN and CdPN number masks are configured simultaneously in the prefix parameters, this rule uses OR logic, i.e. CgPN and CdPN number will not be analyzed simultaneously.



Dial plans

Dial plan settings # 0	
Name	Main
SIP domain	

Check dial plan by number ST □

Search masks by template

Default VAS prefixes

Prefixes in the dial plan

№	Descriptrion	Masks for CgPN	Masks for CdPN	Type	Object	CallerID	CallerID m.	Dial mode	Priority
0	PrefixToE1_SS7	*(no masks)*	**(3400xx) ⇒** **(66x.) ⇒**	TrunkGroup	TrunkSS7_00	-	-	no change (+)	100
1	PrefixToAsterisk	*(no masks)*	**([12]0xxx) ⇒** **(40000) ⇒**	TrunkGroup	TrunkAsterisk	-	-	no change (+)	100
2	PrefixToNumplan1	*(no masks)*	**(54[0-3]0xx) ⇒**	Change dial plan	1016_trunking	-	-	no change (+)	100
3	PrefixToSBC	*(no masks)*	**(41xxx) ⇒**	TrunkGroup	not set	-	-	no change (+)	100
4	PrefixToECSS	*(no masks)*	**(10xx33333333333) ⇒**	TrunkGroup	TrunkECSS	-	-	no change (+)	100
5	PrefixToSBC150	*(no masks)*	**(1001) ⇒**	TrunkGroup	not set	-	-	no change (+)	100
6	PrefixToSBC_2.3_ext	*(no masks)*	**(200xx) ⇒**	TrunkGroup	not set	-	-	no change (+)	100
7	PrefixSBC_1	*(no masks)*	*(no masks)*	TrunkGroup	TrunkSBC_1	-	-	no change (+)	100
8	PrefixSBC_3	*(no masks)*	*(no masks)*	TrunkGroup	TrunkSBC_3	-	-	no change (+)	100
9	PrefixSBC_0	*(no masks)*	*(no masks)*	TrunkGroup	TrunkSBC_0	-	-	no change (+)	100

10 Rows in the table to show

Current page 1 from 3

Dial plan settings:

- *Name* — dial plan name.

Check dial plan by number — availability check for routing by number entered into this field.

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

- *ST* — when checked, end dial marker will be used in search.

Search masks by template — search prefix by the number template.
The check provides the routing possibility data for this number:

- *calling-table* — routing by the caller table.
- *called-table* — routing by the callee table.
- *NOT found in* — routing by this table is not possible.
- *found in* — routing by this table is possible.
- *Abonent 'SIP' idx[4]* — SIP subscriber [database record number for this subscriber].
- *Prefix [6]* — routing by prefix [prefix number in the list].

Copy prefixes to anothe dial plans

- *Copy all prefixes to the dial plan* – the option allows you to copy all the prefixes of the current dial plan to another dial plan. It is the same as "Copy selected prefixes to the dial plan" but you do not need to select prefixes.
- *Copy selected prefixes to the dial plan* – the option allows you to copy selected prefixes to another dial plan. Select necessary prefixes and the target dial plan and click the "Copy" button.

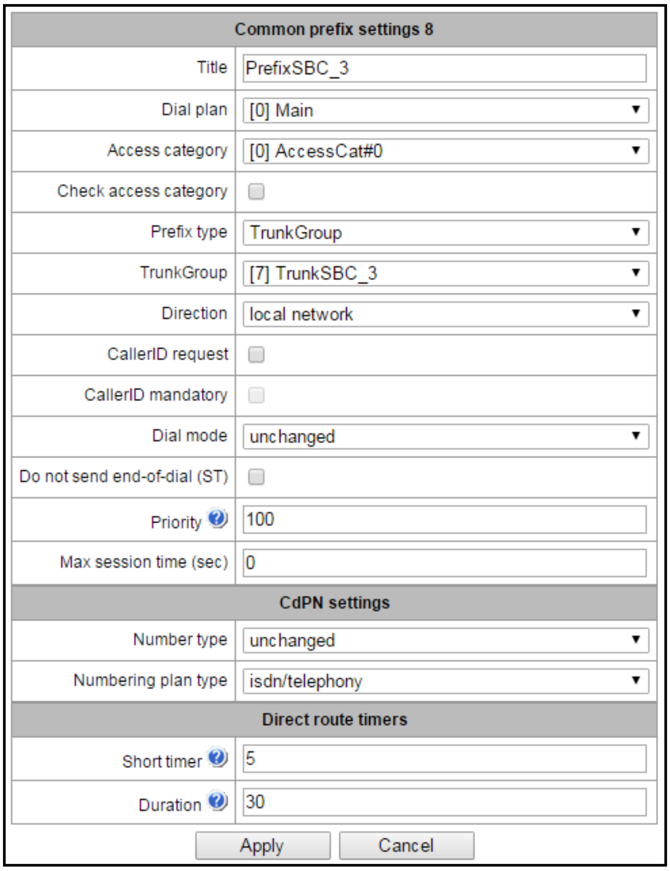
3.1.6.1 Creating a prefix in dial plan

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

Common prefix settings:

- *Title* — prefix name.
- *Dial plan* — select dial plan.
- *Access category* — set access category.
- *Check access category* — when checked, possibility check is performed for routing by this prefix based on rules determined by access categories.
- *Prefix type* — set prefix type:
  - *Trunk Group* — transition to trunk group.
  - *Trunk Direction* — transition to trunk direction.
  - *Change dial plan* — allows to enter another dial plan when this prefix is dialed. When this prefix type is selected, 'new dial plan' option will become available where you should specify the dial plan for transition.

  - *Modifier* — enables definition of the device numbering capacity. If the number is present in the numbering capacity but it is not assigned to a subscriber, call to such a number will result in release message with the cause code: 1 — Unallocated (unassigned) number.
  - *VAS prefix* — enables VAS management from the phone unit.
  - *Pickup group* — enables configuration of the pickup group transition prefix.
  - *IVR scenario* — enables configuration of the IVR scenario transition prefix.



Common prefix settings 8	
Title	PrefixSBC_3
Dial plan	[0] Main
Access category	[0] AccessCat#0
Check access category	□
Prefix type	TrunkGroup
TrunkGroup	[7] TrunkSBC_3
Direction	local network
CallerID request	□
CallerID mandatory	□
Dial mode	unchanged
Do not send end-of-dial (ST)	□
Priority	100
Max session time (sec)	0
CdPN settings	
Number type	unchanged
Numbering plan type	isdn/telephony
Direct route timers	
Short timer	5
Duration	30

'Trunk group and trunk direction' prefix parameters

General prefix parameters:

- *Trunk group* — trunk group that the call will be routed to by this prefix.
- *Direction* — trunk group access type: local, emergency, zone, private, long-distance, international. Enables communication restriction during RADIUS server data exchange failure (see Section 3.1.15 RADIUS configuration).
- *CallerID request* — defines Caller ID information necessity (caller number and category) for transition to the trunk group specified in *'Trunk group'* field*.* When the 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 signalling).
- *CallerID mandatory* — indicates that Caller ID information is *mandatory* during the direction transition. If Caller ID information cannot be received from the calling party, connection establishment process will be interrupted.
- *Dial mode* — number transmission method:
  - *enblock* — after the address information accumulation.
  - *overlap* — w/o the wait for the address information accumulation.
- *Do not send end-of-dial (ST)* — when checked, do not send end dial marker (ST in SS7 or 'sending complete' in PRI).
- *Priority* – in case of presence of overlapping masks in a dial plan, calls will be implemented according to the prefix with the highest priority. Value 0 – the highest priority, 100 – the lowest.
- *Max session time (sec)* – the duration limiting for calls implemented through the prefix.

CdPN settings:

- *Number type* — callee number type: unknown, subscriber number, national number, international number, network specific, no change. Selected number type will be sent in SS7, ISDN PRI, SIP-I/T signalling messages during outgoing call by a prefix (*'no change'* — do not modify number type, i.e. send it as it was received from the incoming channel).
- *Numbering plan type* — callee dial plan type, may take the following values: unknown, isdn/telephony, national, private, no change. Selected dial plan type will be sent in SS7, ISDN PRI, SIP-I/T signalling messages during outgoing call by a prefix (*'no change'* — do not modify number type, i.e. send it as it was received from the incoming channel).

Direct route timers (used in direct trunk group forwarding without prefix mask analysis — *'Direct prefix'* function in trunk group settings).

These timers work only when dial is performed in overlap mode:

- *Short timer* — time in seconds during which the digital gateway will wait for further dialing if the part of an address information has already been received. Default value — 5 sec.
- *Duration* — number dial duration timer. Default value — 30 sec.

'Change dial plan' prefix parameters

- *New dial plan* — dial plan that the call will be transferred to.
- *New access category* — category assigned to the caller after transfer to another dial plan.

Calls modifiers in "change dial plan":

- *CdPN modifiers* – dedicated to modification based on the calling party number analysis;
- *CgPN modifiers* – dedicated to modification based on the called party number analysis.

'VAS prefix' parameters

- *VAS type* — Select VAS service type for management from the subscriber's phone unit:
  - *CFU* — call forward unconditional
  - *CFB* — call forward on busy
  - *CFNR* — call forward on no reply
  - *CFOS* — call forward on out of service
  - *Call pickup* — call pickup
  - *Conference* — conference call
  - *Clear all* — cancel all services
  - *Intercom* — intercom call (with automatic reply from the party B)
  - *Paging* — similar to Intercom but with a call to conference numbers
  - *Password* – set the password;
  - *Password once* – access via password;
  - *Password access* – password activation;
  - *Restrict out* – egress communication restriction;
  - *DND* – do not disturb;
  - *Blacklist* – black list.
- *Action* — select action for the service:
  - *Configure* — set VAS service.
  - *Cancel* — cancel VAS service
  - *Control* — VAS service activity control
  - *numberAdd* – add a number;
  - *numberDel* – remove a number.

'Pickup group' prefix parameters

- Pickup group — pickup group that will be used for call pickup when this prefix is dialed. If you choose 'Any', pickup will be enabled for all groups.
- *Caller ID request* — defines Caller ID information necessity (caller number and category) for transition to the trunk group specified in *'Trunk group'* field. When the 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 signalling).
- *Caller ID mandatory* — indicates that Caller ID information is *mandatory* during the direction transition. If Caller ID information cannot be received from the calling party, connection establishment process will be interrupted.
- *Priority* — configure prefix priority in the range from 0 to 100. Prefix which parameter value is lower will have a greater priority (0 — the highest priority, 100 — the lowest priority).

- *Call duration limiting (sec)* – duration limiting of the calls implemented through the prefix.

Direct route timers

- *Short timer* — time in seconds during which the digital gateway will wait for further dialing if the dialed number matches some sample in the dial plan, but the dialing of additional digits is possible at the same time that will cause a match with another sample. Default value — 5 sec.
- *Duration* — number dial duration timer. Default value — 30 sec.

IVR scenario prefix parameters

- *IVR scenario* — IVR scenario that the call will be routed to by this prefix.

- *Caller ID request* — defines Caller ID information necessity (caller number and category).When the 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 signalling).

- *Caller ID mandatory* — indicates that Caller ID information is *mandatory* during the direction transition. If Caller ID information cannot be received from the calling party, connection establishment process will be interrupted.

- *Priority* — configure prefix priority in the range from 0 to 100. Prefix which parameter value is lower will have a greater priority (0 — the highest priority, 100 — the lowest priority).

- *Call duration limiting (sec)* – duration limiting of the calls implemented through the prefix.

Direct route timers

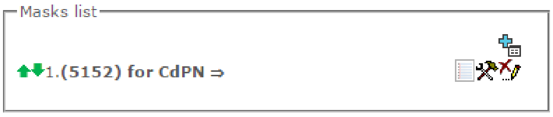
- *Short timer* — time in seconds during which the digital gateway will wait for further dialing if the dialed number matches some sample in the dial plan, but the dialing of additional digits is possible at the same time that will cause a match with another sample. Default value — 5 sec.
- *Duration* — number dial duration timer. Default value — 30 sec.

Mask list

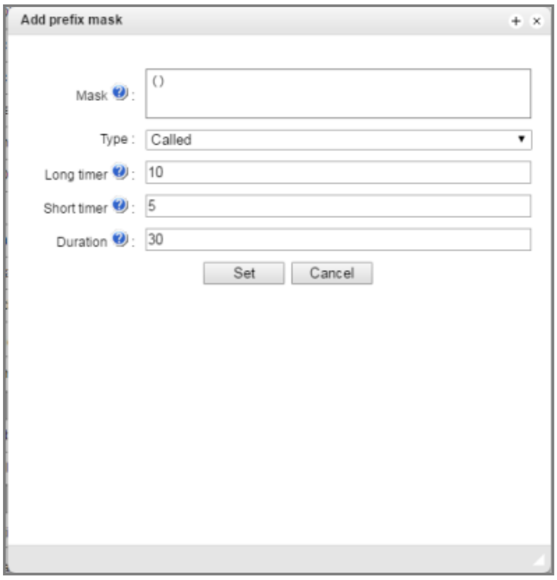
For dial plan created in *'Mask list'* section, number masks are configured for routing by this prefix.

To generate the list, use the following buttons:

— *'Add mask'*
— *'Edit mask'*
— *'Delete mask'*
— *'View mask'*



Green arrows on the left from the created mask allow you to move records in the table to order (prioritize) them.



Add prefix mask

Mask: ()

Type: Called

Long timer: 10

Short timer: 5

Duration: 30

- *Mask* — a template or set of templates, that the caller or callee number received from the incoming channel will be compared to, and designed for the further call routing (for mask syntax, see Section 3.1.3.1).
- *Type* — mask type. Defines the number for the forwarding — caller number (calling) or callee number (called).
- *Long timer* — time in seconds during which the digital gateway will wait for the next digit dialing until a match to some sample from the dial plan is established. Default value — 10 sec.
- *Short timer* — time in seconds during which the digital gateway will wait for further dialing if the dialed number matches some sample in the dial plan, but the dialing of additional digits is possible at the same time that will cause a match with another sample. Default value — 5 sec.
- *Duration* — number dial duration timer. Default value — 30 sec.

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

To *delete the prefix,* select the prefix and click ☒ button located below the list or select *'Objects'* — *'Remove object'* menu.

3.1.6.2 Number mask description and its syntax

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

Syntax:

- **X** or **x** — any digit
- ***** — * character
- **#** — # character
- **0-9** — digits from 0 to 9

- **D** — D digit.
- **.** — 'dot' special symbol means that preceding character may be repeated unlimited times (30 characters max. for a number), e.g.:

  (34x.) — all possible number combinations that begin with '34'.
- **[ ] —** define prefix ranges (with a hyphen) or enumeration (w/o spaces, commas, and other characters between the digits), e.g.:

  range **([1-5]XXX)** — all 4-digit numbers that begin with 1, 2, 3, 4, or 5.

  enumeration **([138]xx)** — all 3-digit numbers that begin with 1, 3, or 8.
- **{min, max}** — define the repetition count for a character located outside the parentheses, e.g.:

  (1x{3,5}) — means that there may be from 3 to 5 arbitrary digits (**x**) equal to mask **(1xxx|1xxxx|1xxxxx)**.
- **| —** vertical line **—** logical **OR**. Enables separation of templates in a mask.
- **!** - exclamation sign. The use of it before a template sets negative value (sets mismatching of number and the template);
- **(-)** — mask used only in CgPN number modifier tables for calls without caller number. Allows to add the caller number if it was missing and to set indicators for that number.

If there are overlapping prefixes present in the dial plan, during number processing in the dial plan, the highest priority will be that of the prefix with the most accurate mask for the specific number, e.g.:
Prefix 1: (2xxxx)
Prefix 2: (23xxx)
When number 23456 arrives to the dial plan, it will be processed with the prefix 2.

Also, masks that contain arbitrary repetition number (x.) or range {min, max} will have a lower priority than masks with the accurate character count, e.g.:
Prefix 1: (2x{4,7})
Prefix 2: (23xxx)
When number 23456 arrives to the dial plan, it will be processed with the prefix 2.

Masks with the specified repetition range {min, max} will have a higher priority than masks with arbitrary repetition number (x.), e.g.:
Prefix 1: (2x.)
Prefix 2: (2x{4,7})
When number 23456 arrives to the dial plan, it will be processed with the prefix 2.

3.1.6.3 Mask operation examples

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

Mask contains 9 templates:

1. **#XX#** — any 4-digit number will be dialed that begins and ends with #, 2nd and 3rd number digits may take any values from 0 to 9, as well as * or #.

In general, such template disables VAS utilization from the phone unit.

2. ***#XX#** — any 5-digit number will be dialed that begins with ***#** and ends with **#**, 3rd and 4th number digits may take any values from 0 to 9, as well as * or #.
   In general, such template allows for control of VAS utilization from the phone unit.
3. ***XX*X.#** — N-digit number is dialed that begins with *, then two arbitrary number digits (from 0 to 9, as well as * and #), then *, then any number of any digits (from 0 to 9, *) until there is **#** in the dial.
   In general, such template allows to order VAS utilization from the phone unit.
4. 112 — dial specific 3-digit number 112.
5. 011 — dial specific 3-digit number 011.
6. 0[1-4] — 2-digit number dialing that begins with 0 and ends with 1, 2, 3, or 4, i.e. 01, 02, 03, and 04.
7. 6[2-9]XXX — 5-digit number is dialed that begins with 6, second digit of the number — any digit in the range from 2 to 9, three last digits — any digit in the range from 0 to 9, as well as * and #.
8. 5[224]XXXXX — 7-digit number is dialed that begins with 5, second digit of the number — 2 or 4, five last digits — any digit in the range from 0 to 9, as well as * and #.
9. 810X{11, 15} — number is dialed that begins with 810, followed by 11 to 15 arbitrary digits in the range from 0 to 9, as well as * and #. Considering the first three digits, number length according to this rule is from 14 to 18 digits.

***Example 2*.**

You should configure dial plan in a way, that all numbers that begin with 1 and have length of 3 would have been routed to Trunk0, and number 117 separately to Trunk1.

To solve this task, configure prefixes as follows:

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

Templates in the second prefix overlap all '1xx' numbers except for 117.

Example 3.

You should configure a dial plan excluding several numbers from the group.

The group of numbers –2340000-2349999, exclude the following numbers: 2341111, 2341112, 2341113, 2341114, 2341115, 2341234.

Set the mask as follows: **(234xxxx|!234111[1-5]|!2341234)**

3.1.6.4 Timer operation examples

Consider example of timer operation for the dialing with 011 number overlap (example 1 from the previous section). Let us assume that timer values are as follows:

L = 10 sec.
S = 5 sec.

First digit reception — 0. There are 2 rules in a mask for such a dialing: 011 and 0[1-4]. There is no full match with any of the rules after the reception of the first digit, and L-timer is activated (10 seconds) for next digit reception. (If the next digit is not received in 10 seconds interval, timeout will be triggered, and given that there is no match with any on the rules, the dial error will occur.)

Second digit reception — 1. Match with the 6th rule 0[1-4] (prefix 01); given that there is a match with a rule but there is a possibility of a match with the 5th rule 011, S-timer is activated (5 seconds) for next digit reception. (If the next digit is not received in 5 seconds interval, timeout will be triggered, and given that there is a match, the call will be forwarded directed using this mask.)

Third digit reception — 1, match with 6th rule is lost and match with 5th rule appears. This match final, given that there are no rules in the mask for the further dialing to match with. The call will be immediately routed using 5th rule.

3.1.6.5 Configuration example for prefix with modifier type

Objective

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

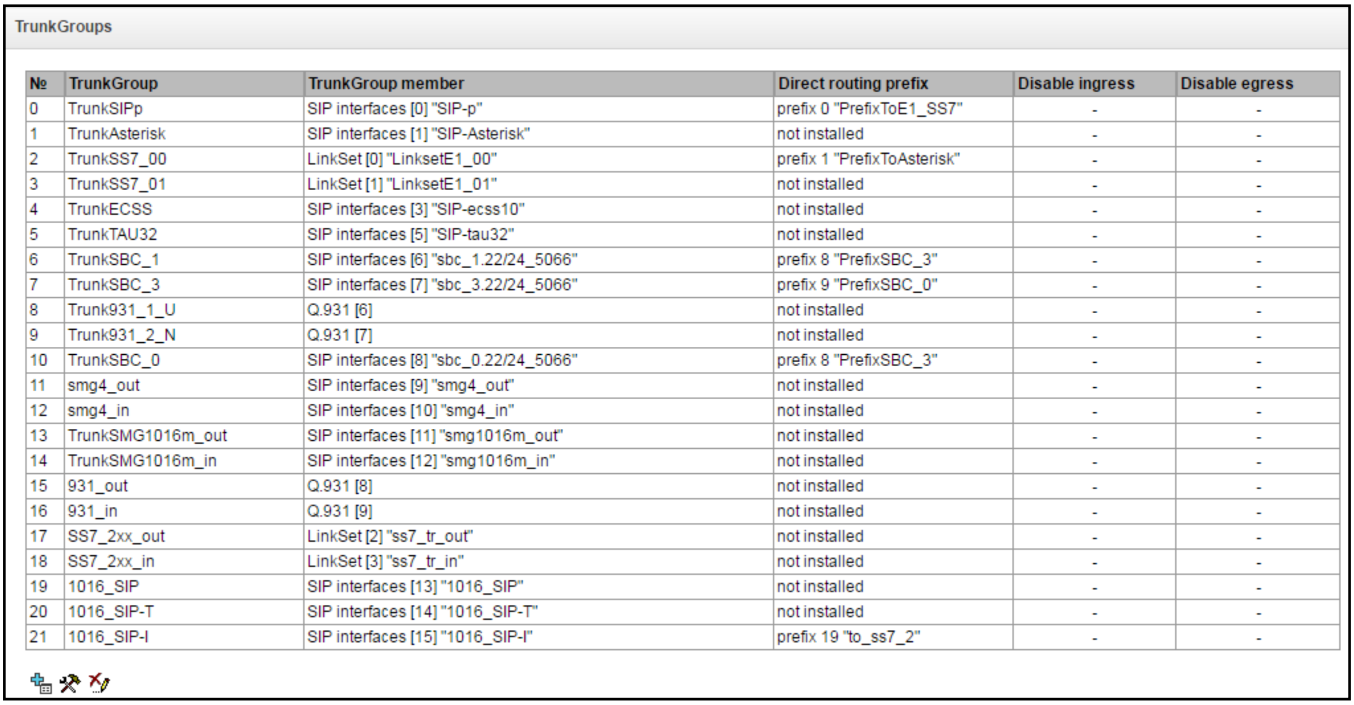
Solution

For correct hanging up reason transmission, you should create a local numbering — configure a 'Modifier' type prefix.

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

3.1.7 Call routing

3.1.7.1 Trunk groups



TrunkGroups

№	TrunkGroup	TrunkGroup member	Direct routing prefix	Disable ingress	Disable egress
0	TrunkSIPp	SIP interfaces [0] "SIP-p"	prefix 0 "PrefixToE1_SS7"	-	-
1	TrunkAsterisk	SIP interfaces [1] "SIP-Asterisk"	not installed	-	-
2	TrunkSS7_00	LinkSet [0] "LinksetE1_00"	prefix 1 "PrefixToAsterisk"	-	-
3	TrunkSS7_01	LinkSet [1] "LinksetE1_01"	not installed	-	-
4	TrunkECSS	SIP interfaces [3] "SIP-ecss10"	not installed	-	-
5	TrunkTAU32	SIP interfaces [5] "SIP-tau32"	not installed	-	-
6	TrunkSBC_1	SIP interfaces [6] "sbc_1.22/24_5066"	prefix 8 "PrefixSBC_3"	-	-
7	TrunkSBC_3	SIP interfaces [7] "sbc_3.22/24_5066"	prefix 9 "PrefixSBC_0"	-	-
8	Trunk931_1_U	Q.931 [6]	not installed	-	-
9	Trunk931_2_N	Q.931 [7]	not installed	-	-
10	TrunkSBC_0	SIP interfaces [8] "sbc_0.22/24_5066"	prefix 8 "PrefixSBC_3"	-	-
11	smg4_out	SIP interfaces [9] "smg4_out"	not installed	-	-
12	smg4_in	SIP interfaces [10] "smg4_in"	not installed	-	-
13	TrunkSMG1016m_out	SIP interfaces [11] "smg1016m_out"	not installed	-	-
14	TrunkSMG1016m_in	SIP interfaces [12] "smg1016m_in"	not installed	-	-
15	931_out	Q.931 [8]	not installed	-	-
16	931_in	Q.931 [9]	not installed	-	-
17	SS7_2xx_out	LinkSet [2] "ss7_tr_out"	not installed	-	-
18	SS7_2xx_in	LinkSet [3] "ss7_tr_in"	not installed	-	-
19	1016_SIP	SIP interfaces [13] "1016_SIP"	not installed	-	-
20	1016_SIP-T	SIP interfaces [14] "1016_SIP-T"	not installed	-	-
21	1016_SIP-I	SIP interfaces [15] "1016_SIP-I"	prefix 19 "to_ss7_2"	-	-

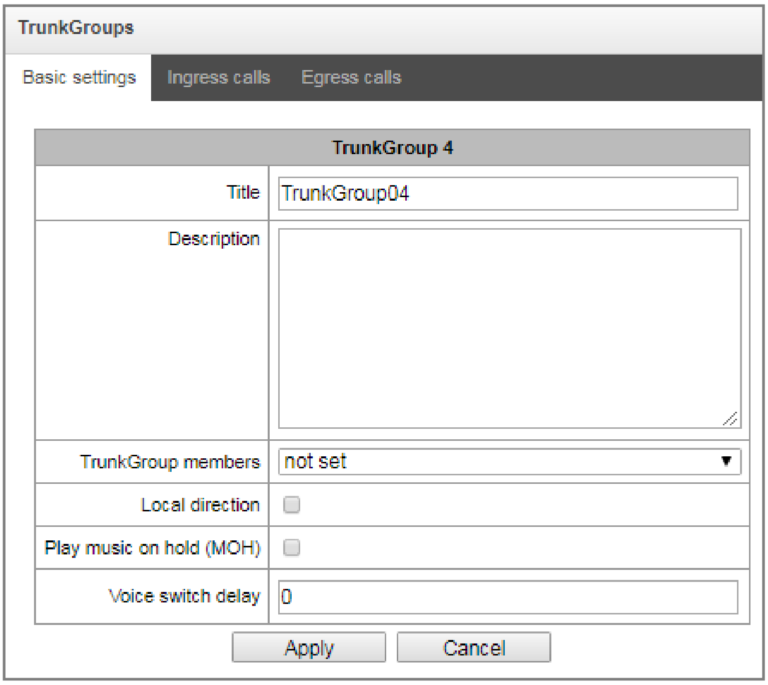
Trunk group is a set of connectivity lines (trunks) that may be represented by E1 stream channels, data transfer environment bandwidth (IP channels). Q.931, SS7 signalling works via E1 stream channels, SIP/SIP-T/SIP-I/H.323 interface — via IP channels. To *edit the trunk group,* double-click the corresponding row in the group table with the left mouse button or select the group and click the ⚒ button below the list.

To *delete the trunk group,* select the group and click button located below the list or select *'Objects'* — *'Remove object'* menu.

You may create up to 255 trunk groups.

3.1.7.1.1 «Basic settings» tab

Click , to add a trunk group, then fill the following fields:



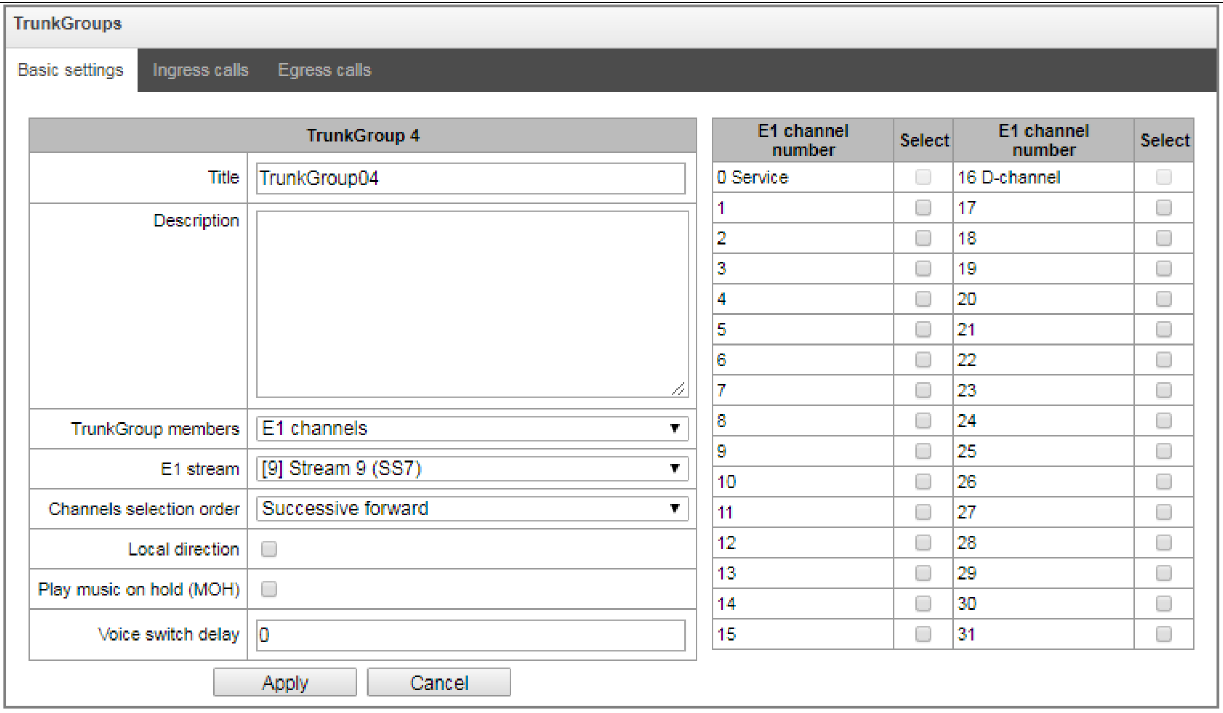
TrunkGroups

TrunkGroup 4

Title	TrunkGroup04
Description	
TrunkGroup members	not set ▼
Local direction	□
Play music on hold (MOH)	□
Voice switch delay	0

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

- *Title* — trunk group name.
- *Description* – the description which will be added to the trunk group;
- *TrunkGroup members* — trunk group contents:
  - Stream with Q.931 signalling, SS link set, SIP or H323 interfaces;
  - E1 channels — E1 stream channels with Q.931, SS7 signalling protocols
  - SS7 Linkset Lines;
- *E1 stream* — select E1 stream for trunk group assignment to E1 stream channels this menu is active only when 'E1 stream channels' value is selected for *'Group contents'.*



TrunkGroup 4	
Title	TrunkGroup04
Description	
TrunkGroup members	E1 channels ▼
E1 stream	[9] Stream 9 (SS7) ▼
Channels selection order	Successive forward ▼
Local direction	☐
Play music on hold (MOH)	☐
Voice switch delay	0

Apply | Cancel

E1 channel number	Select	E1 channel number	Select
0 Service	☐	16 D-channel	☐
1	☐	17	☐
2	☐	18	☐
3	☐	19	☐
4	☐	20	☐
5	☐	21	☐
6	☐	22	☐
7	☐	23	☐
8	☐	24	☐
9	☐	25	☐
10	☐	26	☐
11	☐	27	☐
12	☐	28	☐
13	☐	29	☐
14	☐	30	☐
15	☐	31	☐

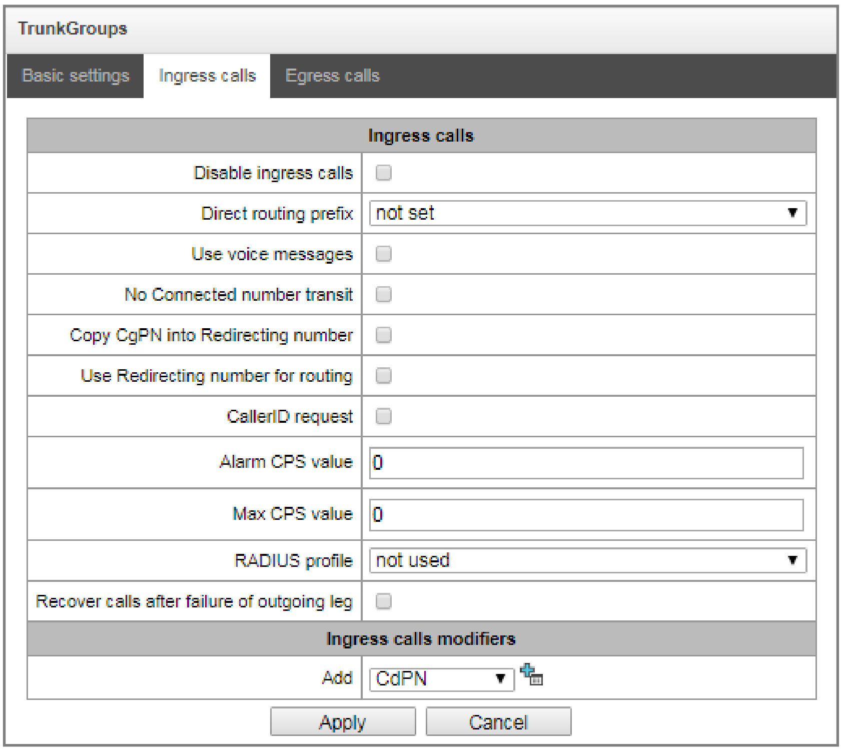
A single trunk group may be assigned to channels only within a single E1 stream.

- *SS7 Linkset Lines* – SS7 Linkset Lines for E1 streams selection. The menu is available when you choose 'SS7 Linkset Lines' in 'Trunk Group members' menu.
- *Channels selection order* – channel selection order in E1 streams. This menu is available when you chose E1 streams from SS7 Linkset;

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

- *Local direction* — when checked, subscribers of this direction are considered as local.
- *Play music on hold (MOH)* – option 'Music On Hold' is enabled, when you get hold party attribute.
- *Voice switch delay* — forced voice frequency path delay after the subscriber's answer.

3.1.7.1.2 «Ingress calls» tab



TrunkGroups

Ingress calls	
Disable ingress calls	□
Direct routing prefix	not set ▼
Use voice messages	□
No Connected number transit	□
Copy CgPN into Redirecting number	□
Use Redirecting number for routing	□
CallerID request	□
Alarm CPS value	0
Max CPS value	0
RADIUS profile	not used ▼
Recover calls after failure of outgoing leg	□
Ingress calls modifiers	
Add	CdPN ▼

- *Disable ingress calls* — when checked, the incoming call reception will be barred. Setting call barring will not disrupt any of the established connections.

- *Direct routing prefix* — transition to the prefix 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 the dialing is performed in the overlap mode, direct dialing timers are used, configured in the direct prefix.

- *Use voice messages* — when checked, pre-recorded voice messages stored in the device memory will be played upon the occurrence of specific events; for detailed description, see Appendix I. Voice messages and music on hold (MOH).

- *No Connected number transmit* — disable transmission of the Connected number field.

- *Copy CgPN into Redirecting number* – when checked, the *Redirecting number* will be formed from CgPN if there is no *Redirecting number* in the incoming call.

- *Use Redirecting number for routing* — when checked, the *'Redirecting number'* field will be used for SS7 or Q.931 signalling protocols, or SIP protocol *'diversion'* field for incoming call routing in the dial plan using CgPN number masks.

- *CallerID request* — defines Caller ID information necessity (caller number and category) for transition to the trunk group specified in *'Trunk group'* field. When the 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 signalling).

- *Alarm CPS value* — number of calls per second that will lead to alarm record in the log. 0 value — disable alarm indication. Alarm indication time — 5 minutes after the define CPS threshold has been exceeded.

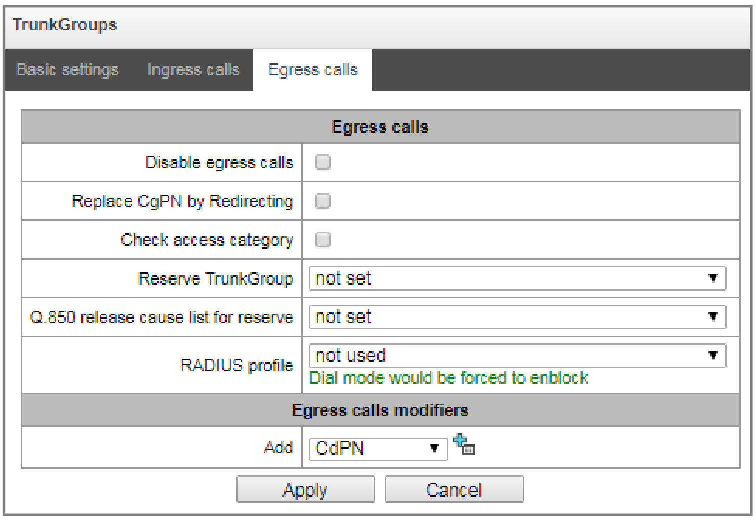
- *Max CPS value* — maximum number of calls per second that may be received by the trunk group. 0 value — disable call restrictions. CPS is calculated as a moving average value for the last 3 seconds. For example, if 3xCPS calls arrive during the first second, they will be accepted, but calls that will arrive in the next two seconds will be rejected.

- *RADIUS profile* — select RADIUS profile to use (to configure profiles, use *«RADIUS configuration/Profile list»,* Section 3.1.15.2).
- *Recover calls after failure of outgoing leg* - if a call which was received via trunk group with activated setting was released not from incoming side, the SMG will recover connection on the A leg recalling or using alternative routes (if main route is not available) without call interruption.

Ingress calls modifiers

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

3.1.7.1.3 «Egress calls» tab



TrunkGroups

Egress calls	
Disable egress calls	□
Replace CgPN by Redirecting	□
Check access category	□
Reserve TrunkGroup	not set
Q.850 release cause list for reserve	not set
RADIUS profile	not used Dial mode would be forced to enblock
Egress calls modifiers	
Add	CdPN

- *Disable egress calls* — when checked, the outgoing call transmission will be barred. Setting call barring will not disrupt any of the established connections.
- *Replace CgPN with Redirecting* — when checked, CgPN number will be substituted with Redirecting number.
- *Check access category* — when checked, possibility check is performed for routing based on rules determined by access categories.
- *Reserve trunk group* — specify a trunk group that the call routing will be transferred to, when the forwarding to the current trunk group is not possible (all channel are engaged or inoperable).
- *Q.850 release cause list for resreve* — select *'Q.850 release cause list'* table to configure Q.850 release causes used for transition to redundant trunk group.
- *RADIUS profile* — select RADIUS profile to use (to configure profiles, use *«RADIUS configuration/Profile list»,* Section 3.1.15.2).

Egress calls modifiers

- *CdPN modifiers* — designed for modifications based on the analysis of the callee number sent to the outgoing channel.

- *CgPN modifiers* — designed for modifications based on the analysis of the caller number sent to the outgoing channel.
- *Original CdPN modifiers* — designed for modifications based on the analysis of the initial callee number (original Called party number) sent to the outgoing channel.
- *RedirPN modifiers* — designed for modifications based on the analysis of the redirecting number sent to the outgoing channel.
- *GenericPN modifiers* — designed for modifications based on the analysis of the special number (generic number) sent to the outgoing channel.
- *LocationNumber modifiers* – designed for modifications based on analysis of location number that is transmitted to an egress channel.

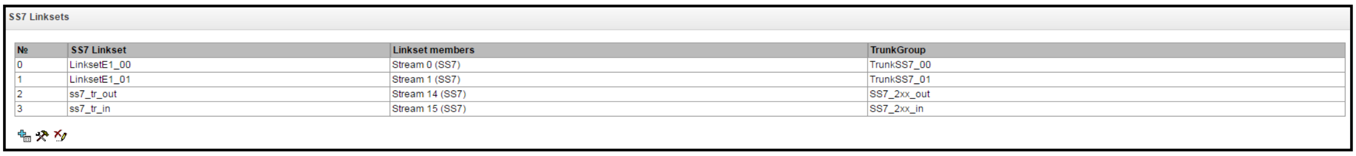
To create, edit or remove groups (as well as other objects), use *'Objects'* — *'Add object', 'Objects'* — *'Edit object'* and *'Objects'* — *'Remove object'* menus and the following buttons:

➕ — *'Add trunk group'*

⚒ — *'Edit trunk group parameters'*

✗ — *'Delete trunk group'*

3.1.7.2 SS7 Linksets



SS7 Linksets

№	SS7 Linkset	Linkset members	TrunkGroup
0	LinksetE1_00	Stream 0 (SS7)	TrunkSS7_00
1	LinksetE1_01	Stream 1 (SS7)	TrunkSS7_01
2	ss7_tr_out	Stream 14 (SS7)	SS7_2xx_out
3	ss7_tr_in	Stream 15 (SS7)	SS7_2xx_in

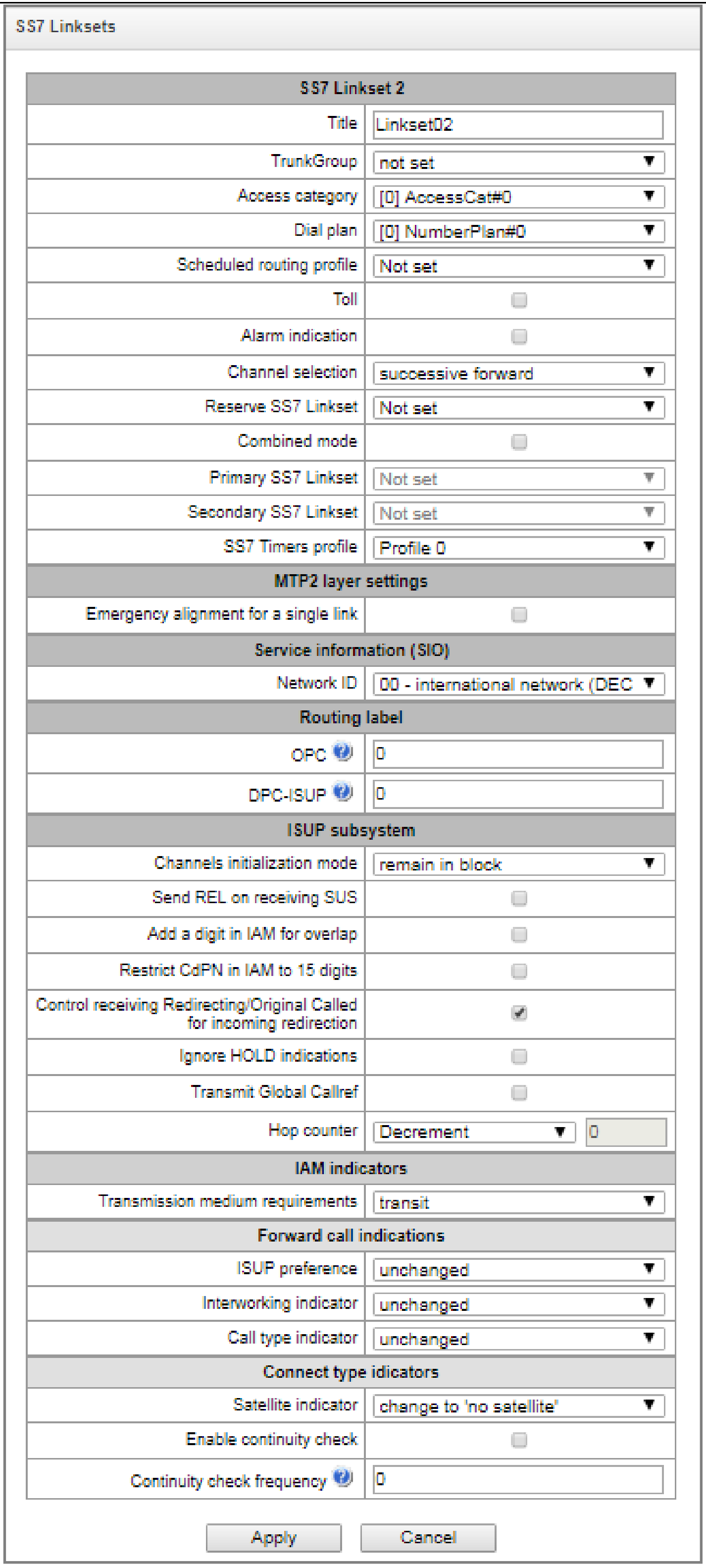
✓ **For SS7 signalling protocol configuration, see 'E1 streams' (Section 3.1.5.4).**

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

➕ – *'Add' - add SS7 link set*

⚒ – *'Edit' - edit SS7 link set*

✗ – *'Delete' - delete SS7 link set*



SS7 Linksets

SS7 Linkset 2		
Title	Linkset02	
TrunkGroup	not set	
Access category	[0] AccessCat#0	
Dial plan	[0] NumberPlan#0	
Scheduled routing profile	Not set	
Toll	□	
Alarm indication	□	
Channel selection	successive forward	
Reserve SS7 Linkset	Not set	
Combined mode	□	
Primary SS7 Linkset	Not set	
Secondary SS7 Linkset	Not set	
SS7 Timers profile	Profile 0	
MTP2 layer settings		
Emergency alignment for a single link	□	
Service information (SIO)		
Network ID	00 - international network (DEC	
Routing label		
OPC	0	
DPC-ISUP	0	
ISUP subsystem		
Channels initialization mode	remain in block	
Send REL on receiving SUS	□	
Add a digit in IAM for overlap	□	
Restrict CdPN in IAM to 15 digits	□	
Control receiving Redirecting/Original Called for incoming redirection	☑	
Ignore HOLD indications	□	
Transmit Global Callref	□	
Hop counter	Decrement	0
IAM indicators		
Transmission medium requirements	transit	
Forward call indications		
ISUP preference	unchanged	
Interworking indicator	unchanged	
Call type indicator	unchanged	
Connect type idicators		
Satellite indicator	change to 'no satellite'	
Enable continuity check	□	
Continuity check frequency	0	

SS7 link set parameters

- *Title* — SS7 link set name.
- *TrunkGroup* — name of a trunk group that SS7 link set operates with.
- *Access category* — select access category.
- *Dial plan* — define dial plan that will be used for routing in this group (necessary for dial plan negotiation).

- *Scheduled routing profile* — select 'scheduled routing' service profile, configured in the 'Internal resources' section.
- *Toll* — means that the signal link is connected to ALDE. This parameter allows for the correct operation with the long-distance type calls (used in transits in CAS signalling).
- *Alarm indication* — when checked, fault indication will appear in case of SS7 signal link fault (ALARM LED will light up, alarm will be added to alarm log).
- *Channel selection* — channel engagement order for the outgoing calls. Available options:
  - Successive forward
  - Successive backward
  - From first forward
  - From last backward
  - Successive forward (even)
  - Successive back (even)
  - Successive forward (odd)
  - Successive back (odd)

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

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

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

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

MTP2 level

- *Emergency alignment for a single link* — enable 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* — originating point code.
- *DPC-ISUP* — destination point code of the ISUP subsystem.

ISUP subsystem

- *Channel initialization mode* — device operations during stream recovery:
  - *Remain in block* — channels will remain blocked (BLO).
  - *Individual unblock* — unblock command (UBL) is sent for each channel.
  - *Group unblock* — channel group unblock command (CGU) is sent.
  - *Group reset* — group reset command (GRS) is sent.

- *Send REL on receiving SUS* — release message is sent in response to Suspend message.

- *Add a digit in IAM for overlap* — send a single digit to *Called Party number* field of IAM message during overlap dialing method.

- *Restrict CdPN in IAM to 15 digits* — when checked, up to 15 digits of CdPN number will be sent in IAM message, other digits will be sent in SAM message.

- *Control receiving Redirecting/Original Called for incoming redirection* — checkbox that enables presence check for *Redirecting/Original Called* fields containing redirection information in incoming IAM message; when checked, the call will be rejected if these fields are missing.

- *Ignore HOLD indications* – when checked, SMG will ignore CPG messages with *remote hold* or *remote retrieval* features;

- *Transmit Global Callref* – when there is no Global Call Reference (GCR) field in an incoming leg, SMG will form it automatically;

- *Hop counter* – set rules for operation with hop counter:
  - *Decrement* – transmission with decreasing of the value;
  - *No change* – transmission without any changes;
  - *Preset* – always transmit with pre-assigned value;
  - *Don't send* – disable hop counter issue.

IAM message indicators

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

Forward call indicators

- *ISUP preference* — rule that governs 'ISUP preference indicator' modification. In a standard situation, these bits should not be changed.

- *Interworking indicator* — defines whether the interaction indicator should be modified (defines whether the interaction with non-ISDN network has occurred).

- Call type indicator — 'National/international call indicator' parameter modifications inFCI.

Connect type indicators

- *Satellite indicator* — identifies the presence of the satellite channel.

- *Change to "no satellite"* — change identifier value to *'no satellite'* regardless of the value received from the incoming channel.
- *Unchanged* — keep the indicator value unchanged.
- *Add one satellite* — this setting is used, if the signal link operates via satellite channel. In this case, satellite channel parameter transmitted in the 'nature of connection' indicators will be increased by 1.

- *Enable continuity check* — enables integrity check support in the SS7 link set. During the outgoing call, the called party establishes a remote loop in the stream, SMG sends the frequency to the channel that will be detected on reception after transmission through the channel. If the frequency is detected, the call will be served through this channel; if it is not detected, the similar attempt will be performed at the next channel. After 3 unsuccessful attempts (for three different channels), call serving will stop.

- *Continuity check frequency* — define the frequency of channel integrity checks during outgoing calls performed through the SS7 link set. For example, value 3 means that each third outgoing call will be performed with the channel integrity check.

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

Examples

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

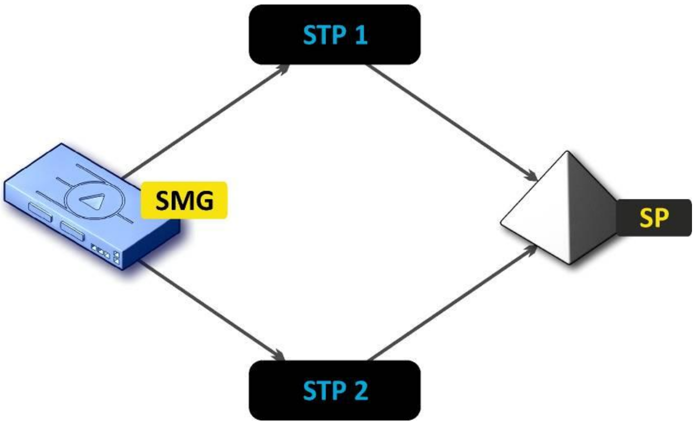


Fig. 34 — SMG connection method for operation in SS7 quasi-associated mode via STP

Objective

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

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

Solution

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

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

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

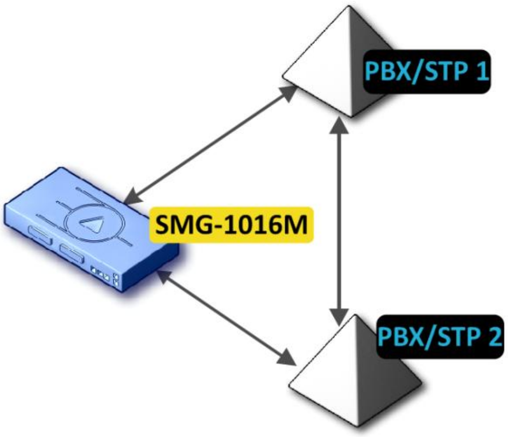


Fig. 35 — SMG connection method for operation in SS7 quasi-associated mode via PBX with STP

LS — SS7 link set

Objective

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

Solution

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

3. SMG connection method example for operation in combined mode

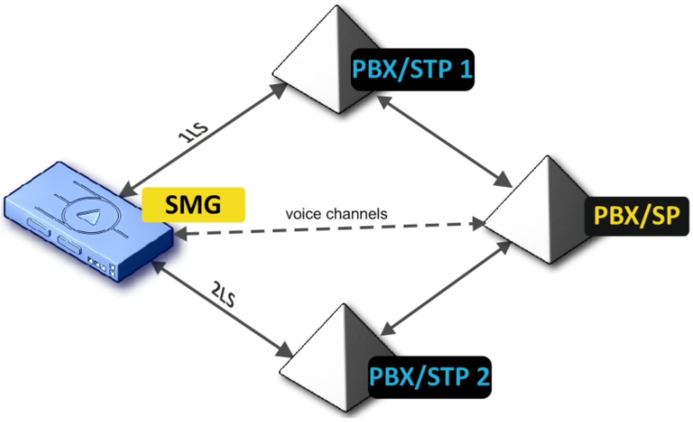


Fig. 36 — SMG connection method for operation in combined mode

Objective

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

Solution

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

3.1.7.3 SIP/SIP-T/SIP-I interfaces, SIP profiles

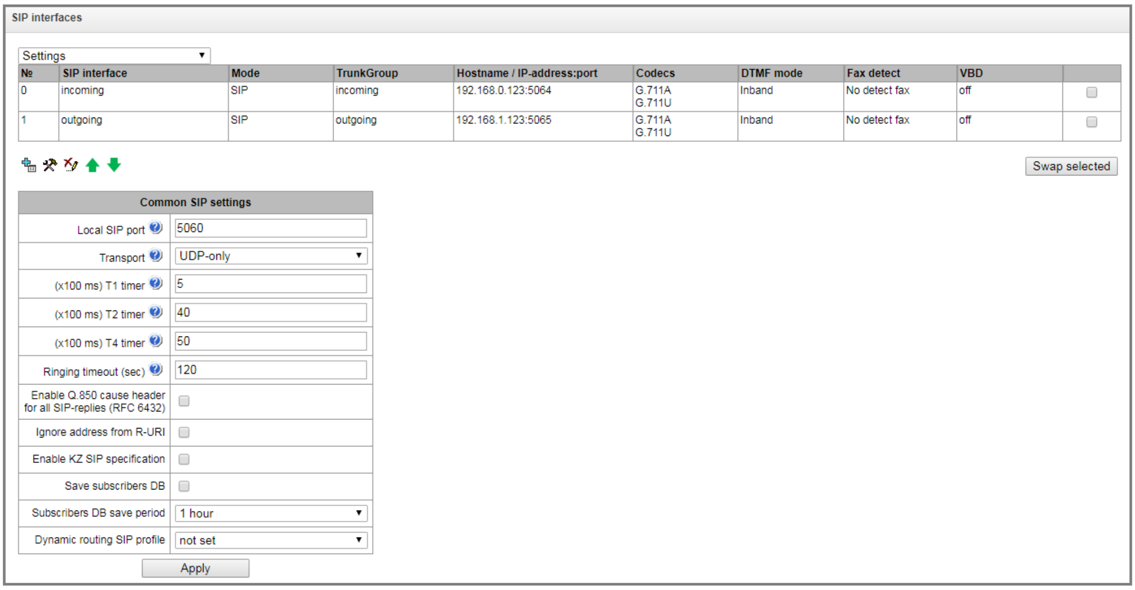
3.1.7.3.1 Configuration

In this section, you may configure SIP stack general configuration parameters, custom settings for each direction operating via SIP/SIP-T/SIP-I protocol and SIP subscriber profiles.

SIP (Session Initiation Protocol) is a signalling protocol, used in IP telephony. It performs basic call management tasks such as starting and finishing session.

Addressing in SIP network based on SIP URI scheme:
sip:user@host:port;uri-parameters
user — number of a SIP subscriber.
@ — separator between the number and domain of a SIP subscriber.
host — domain or IP address of a SIP subscriber.
port — UDP port used for subscriber's SIP service operation.
uri-parameters — additional parameters.

One of the additional SIP URI parameters: user=phone. When this parameter is used, SIP subscriber number syntax should match TEL URI syntax described in RFC 3966. In this case, requests with SIP subscriber numbers containing '+', ';', '=', '?' characters will be processed; also when SIP-T protocol is used and the call is performed to the international number, SMG will automatically add '+' character before the number of the callee.



№	SIP interface	Mode	TrunkGroup	Hostname / IP-address:port	Codecs	DTMF mode	Fax detect	VBD	
0	incoming	SIP	incoming	192.168.0.123:5064	G.711A G.711U	Inband	No detect fax	off	□
1	outgoing	SIP	outgoing	192.168.1.123:5065	G.711A G.711U	Inband	No detect fax	off	□

Common SIP settings	
Local SIP port	5060
Transport	UDP-only
(x100 ms) T1 timer	5
(x100 ms) T2 timer	40
(x100 ms) T4 timer	50
Ringing timeout (sec)	120
Enable Q.850 cause header for all SIP-replies (RFC 6432)	□
Ignore address from R-URI	□
Enable KZ SIP specification	□
Save subscribers DB	□
Subscribers DB save period	1 hour
Dynamic routing SIP profile	not set

Common SIP settings:

- *Local SIP port* — UDP port that will be used for SIP message transmission and reception.
- *Transport* — select transport layer protocol, used for SIP message transmission and reception:
  - *TCP-prefer* — reception via UDP and TCP. Transmission via TCP. If TCP connection was not established, transmission will be performed via UDP.
  - *UDP-prefer* — reception via UDP and TCP. Packets exceeding 1300 bytes will be sent via TCP, under 1300 bytes — via UDP.
  - *UDP-only* — use UDP protocol only.
  - *TCP-only* — use TCP protocol only.
- *T1 timer* — timeout of the request; upon expiration, request will be re-sent. Maximum retranslation interval for INVITE requests is equal to 64*T1.
- *T2 timer* — maximum retranslation interval for INVITE request responses and all requests except for the INVITE.
- *T4 timer* — maximum time allotted for all retranslations of the final response.
- *Ringing timeout (seconds)* — pre-answer 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 replies (RFC 6432*) — when checked, the device analyzes Q.850 cause field in all final SIP messages. When unchecked, Q.850 cause will be analyzed in BYE and CANCEL messages only.
- *Ignore address from R-URI* — when checked, address information after '@' separator in Request-URI will be ignored; otherwise, the gateway will check if the address information matches to the device IP address and host name, and if there is no match, the call will be rejected.
- *Save subscribers DB* — when checked, save information on registered subscribers into the gateway non-volatile memory. It allows you to keep the registered subscribers' database in case of device reboot due to power loss or failure. In case of reboot from the WEB or CLI, the gateway will store the current database into the non-volatile memory regardless of this setting.
- *Subscribers DB save period* — setting that governs archive database update period (from 1 to 16 hours),

SIP protocol defines two types of responses for connection initiating request (INVITE) — provisional and final. 2xx, 3xx, 4xx, 5xx and 6xx-class responses are final and their transfer is reliable, with ACK message confirmation. 1xx-class responses, except for '100 Trying' response, are provisional, without confirmation (RFC3261). These responses contain information on the current INVITE request processing step; in SIP-T/SIP-I protocols, SS7 messages are encapsulated into 1xx class responses, therefore the loss of these responses is unacceptable. Utilization of reliable provisional responses is also stated in SIP (RFC3262) protocol and defined by '100rel' tag presence in the initiating request. In this case, provisional responses are confirmed with PRACK message.

You may create up to 255 interfaces. To create, edit or remove SIP/SIP-T interfaces, use *'Objects' — 'Add object', 'Objects' — 'Edit object'* and *'Objects' — 'Remove object'* menus and the following buttons:

⊞ — *'Add interface'*
⚒ — *'Edit interface parameters'*
✗ — *'Remove* interface*'*

⬆⬇ – *'Move interfaces up and down'*

The signal processor of the gateway encodes analogue voice traffic and fax/modem data into digital signal and performs its reverse decoding. Gateway supports the following codecs: G.711A, G.711U, G.729, T.38 protocol and CLEARMODE.

G.711 is a PCM codec that does not employ a compression of voice data. This codec must be supported by all VoIP equipment manufacturers. G.711A and G.711U codecs differ from each other in encoding law (A-law is a linear encoding and U-law is non-linear). The U-law encoding is used in North America, and the A-law encoding — in Europe.

G.726 is an ADPCM ITU-T standard that describes voice data transmission using 16, 24, 32, and 40kbps bands. **G.726-32** substitutes G.721 that describes ADPCM voice data transmission using 32kbps band.

G.723.1 is a voice data compression codec, allows for two operation modes: 6.3kbps and 5.3kbps. G.723.1 codec has a voice activity detector and performs comfort noise generation at the remote end during period of silence (Annex A).

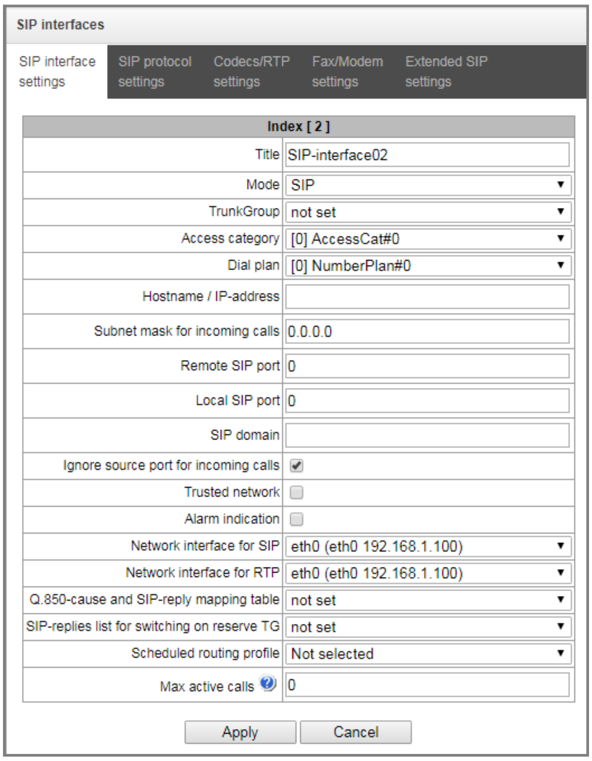
G.729 is also a voice data compression codec with the rate of 8kbps. As with G.723.1, G.729 codec supports voice activity detector and performs comfort noise generation (Annex B).

T.38 is a standard for sending facsimile messages in real time over IP networks. Signals and data sent by the fax unit are copied to T.38 protocol packets. Generated packets may feature redundancy data from previous packets that allows to perform reliable fax transmissions through unstable channels.

CLEARMODE – mode without coding/decoding of signals. The mode provides transparent digital data transmission with the rate of 64 kbps (RFC4040).

3.1.7.3.1.1 SIP interface settings tab

You may use the menu «Objects» – «Add and object» or the button ⊞ to create SIP/SIP-T interfaces:

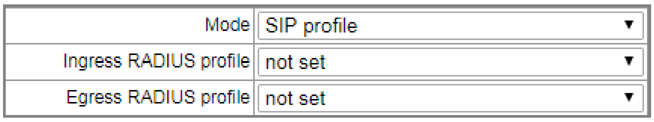


Index [2]	
Title	SIP-interface02
Mode	SIP
TrunkGroup	not set
Access category	[0] AccessCat#0
Dial plan	[0] NumberPlan#0
Hostname / IP-address	
Subnet mask for incoming calls	0.0.0.0
Remote SIP port	0
Local SIP port	0
SIP domain	
Ignore source port for incoming calls	☑
Trusted network	□
Alarm indication	□
Network interface for SIP	eth0 (eth0 192.168.1.100)
Network interface for RTP	eth0 (eth0 192.168.1.100)
Q.850-cause and SIP-reply mapping table	not set
SIP-replies list for switching on reserve TG	not set
Scheduled routing profile	Not selected
Max active calls	0

- *Title* — interface name.

- *Mode* — select protocol for the interface (*SIP/SIP-T/SIP-I/SIP profile*).

- *Ingress RADIUS profile* — select RADIUS profile for the *SIP profile* interface for incoming connection (for the rest of interfaces, RADIUS profile is assigned in the trunk group).



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

- *Egress RADIUS profile* — select RADIUS profile for the *SIP profile* interface for outgoing connection (for the rest of interfaces, RADIUS profile is assigned in the trunk group).

- *Trunk group*[1] — name of a trunk group, that the interface belongs to.

- *Access category* — select access category.

- *Dial plan* — define dial plan that will be used for dialing from this port (necessary for dial plan negotiation).

- *Host name/IP address* — IP address or name of the host communicating via gateway SIP/SIP-T protocol.

- *Subnet mask for incoming calls* – define subnet mask in order to receive calls from the subnet, which is owned to interacting host specified in 'Host name/IP address'. In case of defining mask as 0.0.0.0 (/0), 255.255.255.255 (/32) or 255.255.255.254 (/31), SMG will receive calls only from the address specified in 'Host name/IP address' not a subnet mask;

- *Remote SIP port*[1] — UDP/TCP port of the communicating gateway used for SIP/SIP-T signalling reception.

- *Local SIP port*[1] — local UDP/TCP port of the device used for SIP/SIP-T signalling reception from the device that communicates via this interface.

- *SIP domain* — domain that is inserted into *from* field during the outgoing call via the interface and used in the SIP interface registration.

- *Ignore source port for incoming calls* — when checked, signalling transmission UDP port of the communicating gateway specified in the 'Port for SIP signalling reception' setting will not be checked out; otherwise, it will be checked out and if the INVITE request is received from the other port, the call will be cleared back. If the INVITE request is received via TCP, the port will not be checked out regardless of the setting value.

- *Trusted network* — means that the interface is connected to the trusted network. This option governs INVITE request field generation for hidden caller number calls (presentation restricted). When checked, the caller number information will be transmitted in *from* and *P-Asserted-identity* fields together with the information on its hidden state in *Privacy: id* field; otherwise, caller number information will not be sent.

- *Alarm indication* — when checked, SMG will indicate the fault when connection to the opposite device is lost. For correct operation of this option, select the 'Opposite party availability control using OPTIONS messages' checkbox in SIP settings.

- *Network interface for SIP* — select network interface for signalling SIP message transmission and reception.

[1] The field is not active in SIP profile mode.

- *Network interface for RTP* — select network interface for voice traffic transmission and reception.

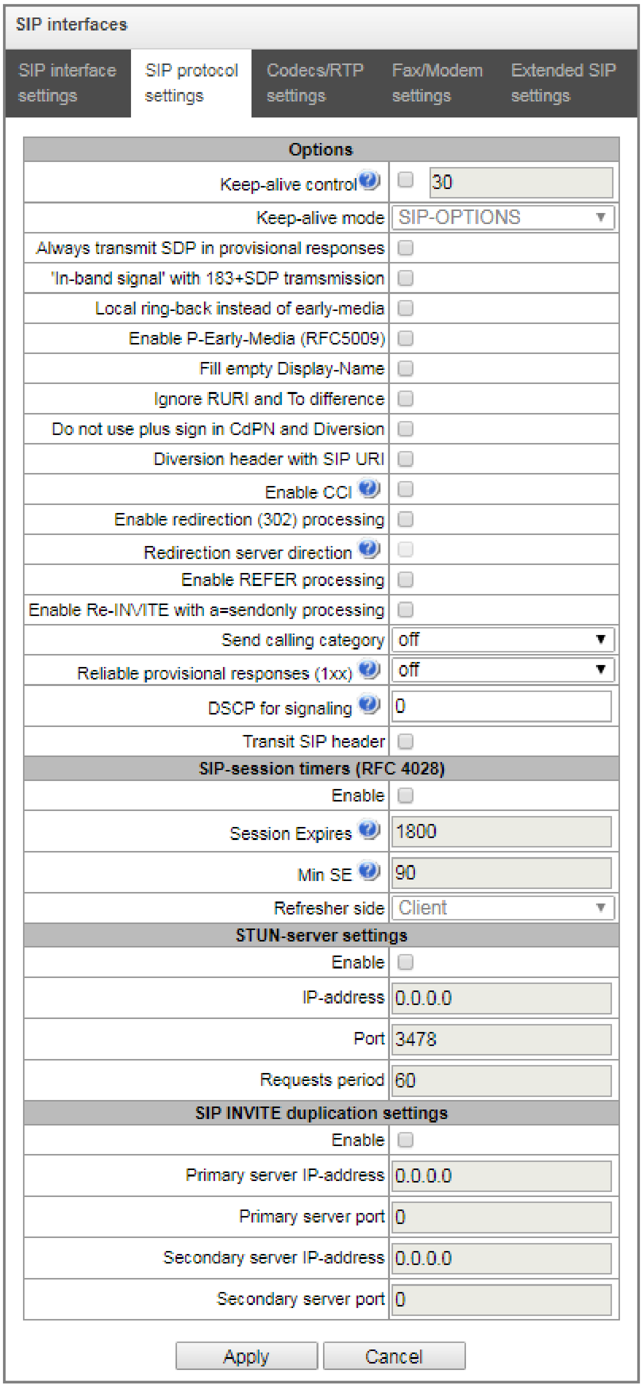
- *Q.850-cause and SIP-reply mapping table* — select correspondence table for Q.850-cause and SIP-reply codes. To configure correspondence tables, use 'Internal resources' menu.

- *SIP replies list for switching on reserve TG* — select the table of 4XX – 6XX class SIP replies used for the redundant trunk group transition. To configure reply lists, use Section 3.1.8 Internal resources.

- *Scheduled routing profile* — select 'scheduled routing' service profile, the configuration is described in 3.1.8 Internal resources.

- *Max active calls* — maximum number of simultaneous (incoming and outgoing) connection through the interface specified.

3.1.7.3.1.2 SIP protocol settings tab



Options	
Keep-alive control	□ 30
Keep-alive mode	SIP-OPTIONS
Always transmit SDP in provisional responses	□
'In-band signal' with 183+SDP tramsmission	□
Local ring-back instead of early-media	□
Enable P-Early-Media (RFC5009)	□
Fill empty Display-Name	□
Ignore RURI and To difference	□
Do not use plus sign in CdPN and Diversion	□
Diversion header with SIP URI	□
Enable CCI	□
Enable redirection (302) processing	□
Redirection server direction	□
Enable REFER processing	□
Enable Re-INVITE with a=sendonly processing	□
Send calling category	off
Reliable provisional responses (1xx)	off
DSCP for signaling	0
Transit SIP header	□
SIP-session timers (RFC 4028)	
Enable	□
Session Expires	1800
Min SE	90
Refresher side	Client
STUN-server settings	
Enable	□
IP-address	0.0.0.0
Port	3478
Requests period	60
SIP INVITE duplication settings	
Enable	□
Primary server IP-address	0.0.0.0
Primary server port	0
Secondary server IP-address	0.0.0.0
Secondary server port	0

SIP/SIP-T/SIP-I options configuration:

- *Keep-alive control* — direction availability control function that utilizes OPTIONS requests; when the direction is not available, the call will be performed through the redundant trunk group. Also, this function analyzes received OPTIONS request responses, that allows to avoid usage of *100rel*, *replaces* and *timer* features configured in this direction if the opposite party supports them. Parameter defines the request transmission period and may take up values in the range 30–3600 seconds.

- Keep-alive mode:

  - *SIP-OPTIONS* — device will send OPTIONS control message with the defined opposite party control interval. A response should be provided to that message; if there is no response, the direction will be considered as unavailable and the alarm state will be initiated on the device.
  - *SIP-NOTIFY* — device will send NOTIFY control message with the defined opposite party control interval. A response should be provided to that message; if there is no response, the direction will be considered as unavailable and the alarm state will be initiated on the device.
  - *UDP-CRLF* — device will send an empty UDP packet with the defined opposite party control interval; the opposite party response to an empty UDP packet is not applicable; consequently, fault state will not be initiated on the device.

☑ **These methods also perform connection keep-alive function on NAT.**

- *Always transmit SDP in provisional responses* — allows to perform an early forwarding of voice frequency path. For example, when unchecked, SMG will send reply 180 without SDP session description and with this reply the outgoing party will play the ringback tone; when checked, SMG will send reply 180 together with SDP session description and the ringback tone will be played by the incoming party.

- *'In-band signal' with 183+SDP transmission* — issue SIP reply 183 with SDP session description for voice frequency path forwarding after reception of CALL PROCEEDING or PROGRESS messages from ISDN PRI containing progress indicator=8 (In-band signal).

- *Local ring-back instead of early-media* — when 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 P-Early-Media header, described in RFC 5009. During the outgoing call, the device will transmit P-Early-Media: supported header in the INVITE message. When INVITE is received with P-Early-Media: supported marker, P-Early-Media: sendrecv header will be transmitted in the 18X reply messages.

- *Fill empty Display-Name* – if checked, when there is no display-name in a receiving call, SMG fill it with a user name (or number) which has been taken from URI;

- *Ignore RURI and To difference* – disable Redirecting and Original Called number issuing in case of calls from SS7;

- *Do not use plus sign in CdPN and Diversion* – disable '+' adding to a number, if the number is international;

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

- *Enable CCI* — enable sending SIP-I/T IAM with 'Continuity check indication' value equal to 2. **The option is available for SIP-T and SIP-I protocols.**
- *Enable redirection (302) processing* — when checked, the gateway is allowed to perform redirection after reception of the reply 302 from this interface. When unchecked and reply 302 is received, the gateway will reject the call and not perform the redirection.
- *Redirection server direction* — option is available when reply 302 processing is enabled (parameter *'Enable redirection (302)'*). Allows to redirect the call sent using the public address to the subscriber's private address received in the reply 302 without the dial plan routing. The routing will be performed directly to the address contained in the reply 302 'contact' header received from the redirection server.
- *Enable REFER processing* — REFER request is transferred by the communicating gateway in order to enable the 'Call transfer' service. When checked, the gateway is allowed to process REFER requests received from this interface. When unchecked, after REFER request reception the gateway will reject the call and will not perform 'Call transfer' service.
- *Enable Re-INVITE with a=sendonly processing* — checkbox that allows to put the call on hold when Re-INVITE message is received with a=sendonly marker in SDP.
- *Send calling category* — select method of the caller category transmission through SIP. Implemented methods are as follows:
  - *off* — Caller ID category transmission and reception is disabled.
  - *category* — caller category transmission and reception in the separate *category* field of the INVITE message; in this case, SS7 category is transmitted with values 0–255.
  - *cpc* — caller category transmission and reception using 'cpc=' tag sent in the *from* field; in this case, Caller ID category is transmitted with values 1–10.
  - *cpc-rus* — caller category transmission and reception using 'cpc-rus=' tag sent in the *from* field; in this case, Caller ID category is transmitted with values 1–10.
- *Reliable provisional responses (1xx)* — when checked, INVITE request and 1xx class provisional responses will contain the option require: 100rel that requires assured confirmation of provisional responses.
  - *off* — reliable delivery of provisional responses is disabled.
  - *support* — INVITE request and 1xx class provisional responses will contain the option support: 100rel.
  - *support+* — duplicate SDP in 200 OK message with support: 100rel.
  - *require* — INVITE request and 1xx class provisional responses will contain the option require: 100rel that requires assured confirmation of provisional responses.
  - *require+* — duplicate SDP in 200 OK message with require: 100rel.
- *DSCP for Signalling* — service (DSCP) type for SIP signalling traffic.

✓ **The DSCP setting for RTP and DSCP setting for SIP will be ignored while using VLAN for RTP transmission and signalling. *Class of Service* VLAN is used for prioritization in this case.**

- *Transit SIP header* – the option allows to implement transit of received SIP headers to an incoming leg.

SIP session timers (RFC 4028)

- *Enable* — when checked, enables support of SIP session timers (RFC 4028). Session is renewed via re-INVITE request transmission during the session.

- *Session Expires* — period of time in seconds that should pass before the forced session termination if the session is not renewed in time (90 to 64800sec, recommended value is 1800sec).

- *Minimum session keep alive period (Min SE)* — minimal time interval for connection health checks (90 to 32000 seconds). This value should not exceed session forced termination timeout '*Sessions expires*'.

- *Refresher side* — defines the party that will perform session renewal (client (uac) — client (caller) party, server (uas) — server (callee) party).

Registration settings*[1]*:

- *Upper registration* — select type of registration on the upstream server:
  - *No registration* — do not register 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 its 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* — name used for authentication.

- *Password* — password used for authentication.

- *Username/Number* — user number utilized as a caller number for outgoing trunk calls.

- *Default CdPN* — CdPN number that will be used for substitution in all calls performed via this SIP interface.

- *Replace CgPN on egress call* — when checked, caller number (CgPN) will be taken from the *'Username/Number'* parameter; otherwise, CgPN number received in the incoming call will be used.

- *Registration period (sec)* — registration renewal time period.

- *Registration requests interval (ms)* — minimum 'Register' message transmission interval designed for protection from high traffic caused by simultaneous registration of large number of subscribers.

STUN server settings:

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

- *Enable* — when checked, enable STUN.

- *IP address* — STUN server IP address

[1] Parameter block is available for SIP mode only.

- *Port* — server port for request transmission (default value is 3478).
- *Requests period* — time interval between requests (10–1800 seconds).

Before signalling message transmission, the request (Binding Request) is 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 are generated before each SIP signalling message transmission, but not more often than the configured request period time.

***DSCP settings for RTP* and *DSCP for SIP* will be ignored when VLAN is used for RTP and signalling transmission. In this case, '*Class of Service VLAN*' will be used for traffic prioritization.**

SIP INVITE duplication settings

In this section you can configure reception of INVITE request with SMS text from emergency call service node and duplication of the requests to SMS servers. Also you can configure SMPP server's parameters for messages receiving via SMPP and redirecting to SMS servers via SIP.

Redundancy implementation:

After activation of the option, INVITE requests with SMS text (which defines by precense of Content-Type: text/plain header or Content-Type: multipart/mixed with text/plain in the Content) received on SIP interface are redirected by SMG via TCP to duplication server. The server must reply '403 Forbidden' to confirm the delivery. Another replies will be considered as duplication failure, with corresponding alarm notification. The call is completed with '403 Forbidden' message.

If INVITE request comes without an SMS text, the request will be duplicated and call will be processed as usual.

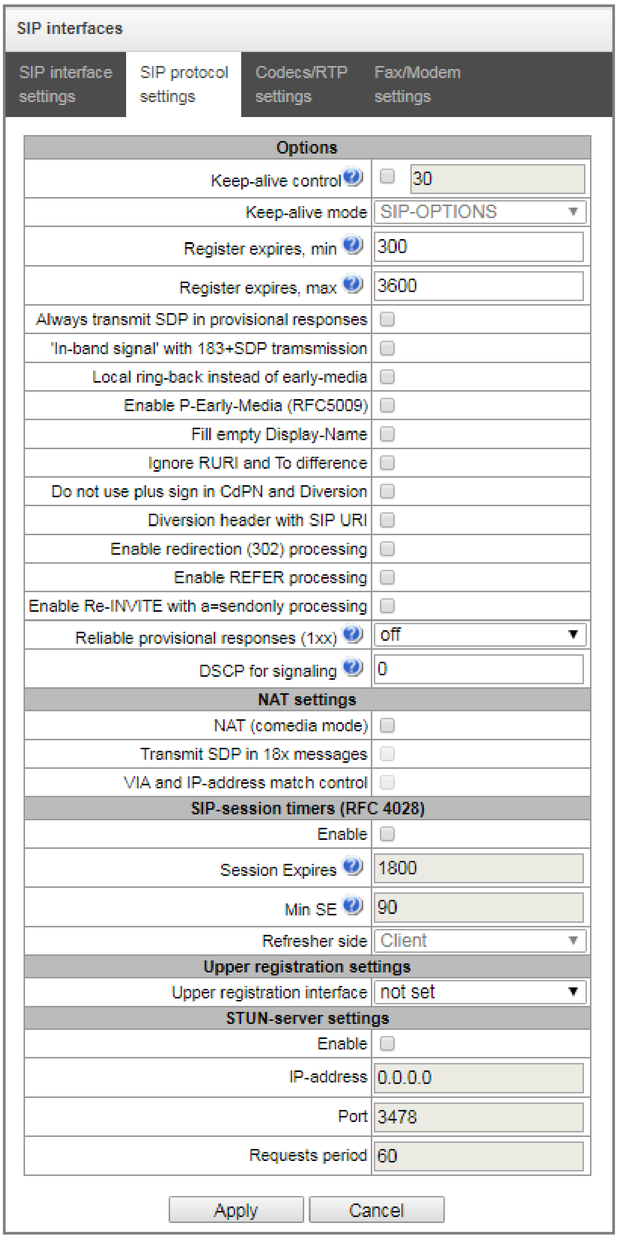
- *Enable* - activate duplication of INVITE requests;

Duplication is implemented via TCP. Thus, you need to configure 'Transport' in 'Common SIP settings' to enable work via TCP (UDP-prefer, TCP-prefer or TCP-only).

- *Primary server IP address; primary server port* — address of the main (primary) server;
- *Secondary server IP address; secondary server port* —address of the secondary server;
- *Port for SMS reception*[1] — port for SMS reception via SMPP. If you enable this option, SMG will receive connections on specified port via SMPP and transmit received SMS to backup (duplication) servers via SIP. Encryption of transmitted messages in text/plain will comply to encryption of incoming messages and have Content-Type (with charset parameter) and Content-Transfer-Encoding headers in INVITE message.

[1] Available for the devices with SMG-SMS license. Read more detailed information on licenses in the section 3.1.23 Licenses.

Configuration of options for SIP profile mode:



SIP interfaces

Options	
Keep-alive control	□ 30
Keep-alive mode	SIP-OPTIONS
Register expires, min	300
Register expires, max	3600
Always transmit SDP in provisional responses	□
'In-band signal' with 183+SDP tramsmission	□
Local ring-back instead of early-media	□
Enable P-Early-Media (RFC5009)	□
Fill empty Display-Name	□
Ignore RURI and To difference	□
Do not use plus sign in CdPN and Diversion	□
Diversion header with SIP URI	□
Enable redirection (302) processing	□
Enable REFER processing	□
Enable Re-INVITE with a=sendonly processing	□
Reliable provisional responses (1xx)	off
DSCP for signaling	0
NAT settings	
NAT (comedia mode)	□
Transmit SDP in 18x messages	□
VIA and IP-address match control	□
SIP-session timers (RFC 4028)	
Enable	□
Session Expires	1800
Min SE	90
Refresher side	Client
Upper registration settings	
Upper registration interface	not set
STUN-server settings	
Enable	□
IP-address	0.0.0.0
Port	3478
Requests period	60

- *Keep-alive control* — direction availability control function (NAT keep-alive) that utilizes SIP-OPTIONS, SIP-NOTIFY, or an empty UDP methods. Parameter defines the request transmission period and may take up values in the range 30–3600 seconds.

- Keep-alive mode:

  – *SIP-OPTIONS* — device will send OPTIONS control message with the defined opposite party control interval. A response should be provided to that message; if there is no response, the direction will be considered as unavailable and the alarm state will be initiated on the device.

  – *SIP-NOTIFY* — device will send NOTIFY control message with the defined opposite party control interval. A response should be provided to that message; if there is no response, the direction will be considered as unavailable and the alarm state will be initiated on the device.

  - *UDP-CRLF* — device will send an empty UDP packet with the defined opposite party control interval; the opposite party response to an empty UDP packet is not applicable; consequently, fault state will not be initiated on the device.

✓ **These methods also perform connection keep-alive function on NAT.**

- *Register expires, min* — minimum value of 'expires' registration time.

- *Register expires, max* — maximum value of 'expires' registration time.

- *Always transmit SDP in provisional responses* — allows to perform an early forwarding of voice frequency path. For example, when unchecked, SMG will send reply 180 without SDP session description and with this reply the outgoing party will play the ringback tone; when checked, SMG will send reply 180 together with SDP session description and the ringback tone will be played by the incoming party.

- *'In-band signal' with 183+SDP transmission* — issue SIP reply 183 with SDP session description for voice frequency path forwarding after reception of CALL PROCEEDING or PROGRESS messages from ISDN PRI containing progress indicator=8 (In-band signal).

- *Local ring-back instead of early-media* — when early media marker is received via outgoing connection leg, ringback tone will be played to the caller instead of an inband voice message.

- *Enable P-Early-Media (RFC5009)* — use P-Early-Media header described in RFC 5009. During the outgoing call, the device will transmit P-Early-Media: supported header in the INVITE message. When INVITE is received with P-Early-Media: supported marker, P-Early-Media: sendrecv header will be transmitted in the 18X reply messages.

- *Fill empty Display-Name* – if checked, when there is no display-name in a receiving call, SMG fill it with a user name (or number) which has been taken from URI;

- *Ignore RURI and To difference* – disable *Redirecting* and *Original Called* numbers issuing while ringing via SS7 if SIP RURI and To fields are different;

- *Do not use plus sign in CdPN and Diversion* – disable '+' adding to a number, if the number is international;

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

- *Enable redirection (302) processing* — when checked, the gateway is allowed to perform redirection after reception of the reply 302 from this interface. When unchecked and reply 302 is received, the gateway will reject the call and will not perform the redirection.

- *Enable REFER processing* — REFER request is transferred by the communicating gateway in order to enable the 'Call transfer' service. When checked, the gateway is allowed to process REFER requests received from this interface. When unchecked, after REFER request reception the gateway will reject the call and will not perform 'Call transfer' service.

- Enable re-INVITE with a=sendonly processing — checkbox that allows to put the call on hold when Re-INVITE message is received with a=sendonly marker in SDP.

- *Reliable provisional responses (1xx)* — when checked, INVITE request and 1xx class provisional responses will contain the option require: 100rel that requires assured confirmation of provisional responses.

  - *off* — reliable delivery of provisional responses is disabled.

  - *support* — INVITE request and 1xx class provisional responses will contain the option support: 100rel;
  - *require* — INVITE request and 1xx class provisional responses will contain the option require: 100rel that requires assured confirmation of provisional responses.

- *DSCP for signalling* – service type (DSCP) for SIP signalling traffic.

✓ **The DSCP setting for RTP and DSCP setting for SIP will be ignored while using VLAN for RTP transmission and signalling. Class of Service VLAN is used for prioritization in this case.**

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.

- *Transmit SDP in 18x messages* — translate SDP attachment in 18x provisional replies when NAT option is enabled (comedia mode). Allows to perform 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* - option of bypassing NAT. If you enable the option, address in VIA header and IP-address of transmitting device (which request was transmitted from) will be analyzed. If the addresses are the same, the device is not located behind NAT.

SIP session timers (RFC 4028)

- *Enable* — when checked, enables support of SIP session timers (RFC 4028). Session is renewed via re-INVITE request transmission during the session.

- *Session Expires* — period of time in seconds that should pass before the forced session termination if the session is not renewed in time (90 to 64800sec, recommended value is 1800sec).

- *Minimum session keep-alive period (Min SE)* — minimal time interval for connection health checks (90 to 32000 seconds). This value should not exceed session forced termination timeout '*Sessions expires*'.

- *Refresher side* — defines the party that will perform session renewal (client (uac) — client (caller) party, server (uas) — server (callee) party).

Upper registration settings[1]

- Upper registration interface – select SIP interface for transit registration

STUN server settings:

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

- *Enable* — when checked, enable STUN.

- *IP address* — STUN server IP address

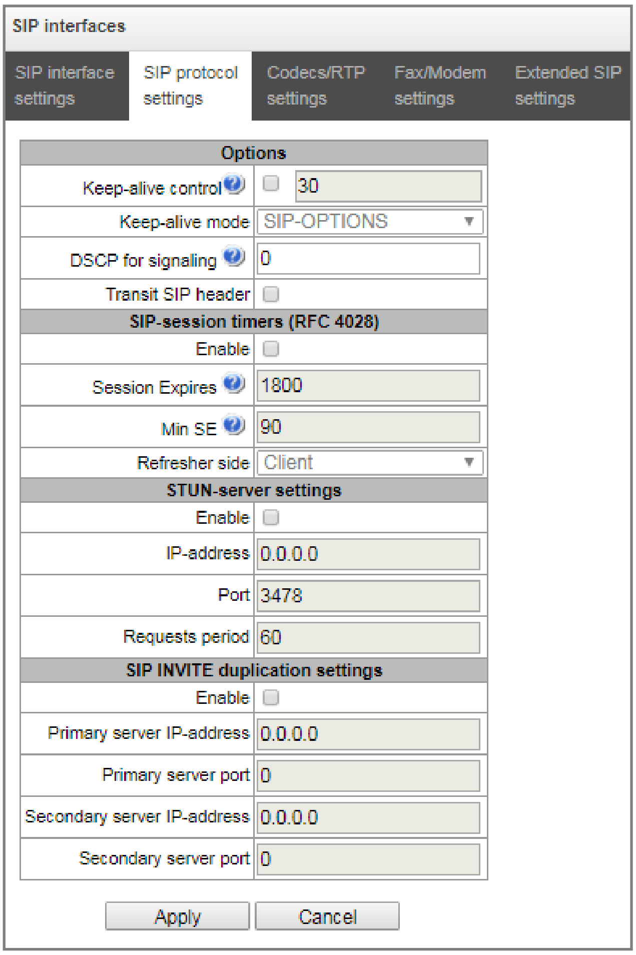
[1] Parameter block is available for SIP profile mode only

- *Port* — server port for request transmission (default value is 3478).
- *Requests period* — time interval between requests (10–1800 seconds).

Before signalling message transmission, the request (Binding Request) is 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 are generated before each SIP signalling message transmission, but not more often than the configured request period time.

Configuration of options for SIP-Q profile mode:



SIP interfaces

Options	
Keep-alive control	□ 30
Keep-alive mode	SIP-OPTIONS ▾
DSCP for signaling	0
Transit SIP header	□
SIP-session timers (RFC 4028)	
Enable	□
Session Expires	1800
Min SE	90
Refresher side	Client ▾
STUN-server settings	
Enable	□
IP-address	0.0.0.0
Port	3478
Requests period	60
SIP INVITE duplication settings	
Enable	□
Primary server IP-address	0.0.0.0
Primary server port	0
Secondary server IP-address	0.0.0.0
Secondary server port	0

- *Keep-alive control* — direction availability control function (NAT keep-alive) that utilizes SIP-OPTIONS, SIP-NOTIFY, or an empty UDP methods. Parameter defines the request transmission period and may take up values in the range 30–3600 seconds.
- Keep-alive mode:
  - *SIP-OPTIONS* — device will send OPTIONS control message with the defined opposite party control interval. A response should be provided to that message; if there is no response, the direction will be considered as unavailable and the alarm state will be initiated on the device.
  - *SIP-NOTIFY* — device will send NOTIFY control message with the defined opposite party control interval. A response should be provided to that message; if there is no response, the direction will be considered as unavailable and the alarm state will be initiated on the device.

- *UDP-CRLF* — device will send an empty UDP packet with the defined opposite party control interval; the opposite party response to an empty UDP packet is not applicable; consequently, fault state will not be initiated on the device.

These methods also perform connection keep-alive function on NAT.

- *DSCP for signalling* — service (DSCP) type for SIP signalling traffic.

The DSCP setting for RTP and DSCP setting for SIP will be ignored while using VLAN for RTP transmission and signalling. *Class of Service* VLAN is used for prioritization in this case.

- *Transit SIP header* – the option allows to implement transit of received SIP headers to an incoming leg.

SIP session timers (RFC 4028)

- *Enable* — when checked, enables support of SIP session timers (RFC 4028). Session is renewed via re-INVITE request transmission during the session.
- *Session Expires* — period of time in seconds that should pass before the forced session termination if the session is not renewed in time (90 to 64800sec, recommended value is 1800sec).
- *Minimum session keep alive period (Min SE)* — minimal time interval for connection health checks (90 to 32000 seconds). This value should not exceed session forced termination timeout '*Sessions expires*'.
- *Refresher side* — defines the party that will perform session renewal (client (uac) — client (caller) party, server (uas) — server (callee) party).

STUN server settings:

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

- *Enable* — when checked, enable STUN.
- *IP address* — STUN server IP address
- *Port* — server port for request transmission (default value is 3478).
- *Requests period* — time interval between requests (10–1800 seconds).

Before signalling message transmission, the request (Binding Request) is 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 are generated before each SIP signalling message transmission, but not more often than the configured request period time.

SIP INVITE duplication settings

In this section, you may configure reception of ingress INVITE requests with SMS text from emergency services equipment. Also, you may configure SMPP server parameters for receiving messages via SMPP and retransmitting them to SMS servers via SIP.

The duplication is implemented as follows: after the activation of the option on a SIP interface, when an INVITE request with SMS text is received (it is defined when the message contains body with Content-Type: text/plain or Content-Type: multipart/mixed, where there is text/plain among the context), SMG will redirect the request to a duplication server via TCP. The server transmits the message 403 Forbidden to confirm the delivery. Another release from the server will be taken as duplication failure with the corresponding alarm. The call will be released with the 403 Forbidden message.

If INVITE request is received without SMS text when the option is enabled, the INVITE request will be duplicated and the call will be processed as usual.

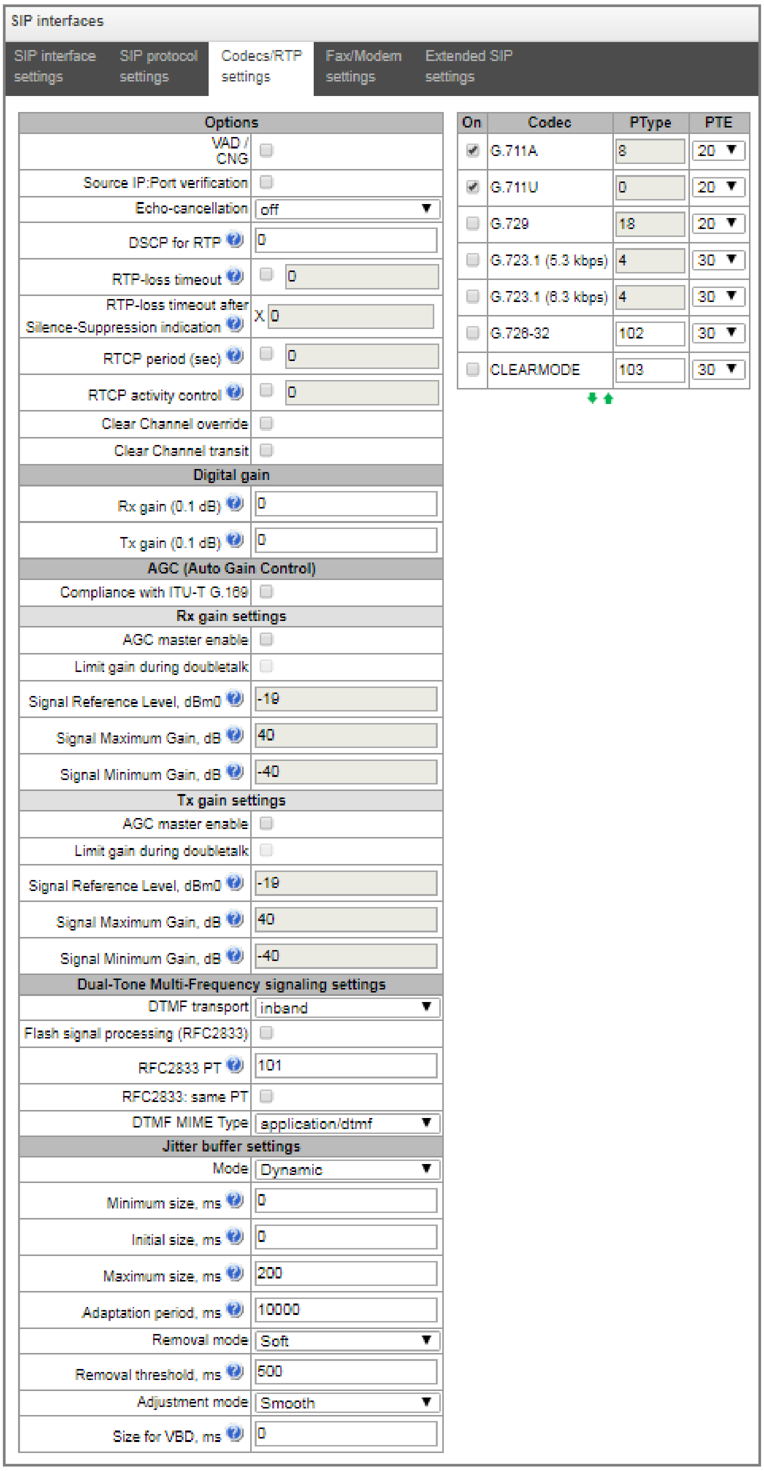
1) *Enable* – activate INVITE requests duplication;

✓ **Duplication operates via TCP, so you should configure Transport setting to make operation via TCP available (select UDP-prefer, TCP-prefer or TCP-only in Common SIP settings, see 3.1.7.3.1.3)**

2) *Primary server IP-address; Primary server port* – an IP address and a port of a main server;
3) *Secondary server IP-address; Secondary server port* – an IP address and a port of a main server;
4) *SMS*[1] – a port for SMS receiving via SMPP. When the option is enabled, SMG will receive connections on the interface via SMPP and retransmit SMS messages to duplication server via SIP. The coding of the transmitting messages in text/plain will correspond the coding of the incoming messages and will be clarified by the Content-Type (charset parameter) and Content-Transfer-Encoding headers in INVITE message.

[1] Available for the devices with SMG-SMS license. Read more detailed information on licenses in the section 3.1.23 Licenses.

3.1.7.3.1.3 Codecs/RTP settings tab



SIP interfaces

SIP interface settings | SIP protocol settings | Codecs/RTP settings | Fax/Modem settings | Extended SIP settings

Options	
VAD / CNG	□
Source IP:Port verification	□
Echo-cancellation	off ▼
DSCP for RTP	0
RTP-loss timeout	□ 0
RTP-loss timeout after Silence-Suppression indication	x 0
RTCP period (sec)	□ 0
RTCP activity control	□ 0
Clear Channel override	□
Clear Channel transit	□
Digital gain	
Rx gain (0.1 dB)	0
Tx gain (0.1 dB)	0
AGC (Auto Gain Control)	
Compliance with ITU-T G.169	□
Rx gain settings	
AGC master enable	□
Limit gain during doubletalk	□
Signal Reference Level, dBm0	-19
Signal Maximum Gain, dB	40
Signal Minimum Gain, dB	-40
Tx gain settings	
AGC master enable	□
Limit gain during doubletalk	□
Signal Reference Level, dBm0	-19
Signal Maximum Gain, dB	40
Signal Minimum Gain, dB	-40
Dual-Tone Multi-Frequency signaling settings	
DTMF transport	inband ▼
Flash signal processing (RFC2833)	□
RFC2833 PT	101
RFC2833: same PT	□
DTMF MIME Type	application/dtmf ▼
Jitter buffer settings	
Mode	Dynamic ▼
Minimum size, ms	0
Initial size, ms	0
Maximum size, ms	200
Adaptation period, ms	10000
Removal mode	Soft ▼
Removal threshold, ms	500
Adjustment mode	Smooth ▼
Size for VBD, ms	0

On	Codec	PType	PTE
☑	G.711A	8	20 ▼
☑	G.711U	0	20 ▼
□	G.729	18	20 ▼
□	G.723.1 (5.3 kbps)	4	30 ▼
□	G.723.1 (6.3 kbps)	4	30 ▼
□	G.726-32	102	30 ▼
□	CLEARMODE	103	30 ▼

Options:

- *Voice activity detector / Comfort noise generator (VAD/CNG)* — when checked, silence detector and comfort noise generator are enabled. Voice activity detector disables transmission of RTP packets during periods of silence, reducing loads in data networks.

- *Source IP: Port verification* — when this setting is checked, control of media traffic received from IP address and UDP port specified in SDP communication session description will be enabled; otherwise the traffic from any IP address and UDP port will be accepted.

- *Echo cancellation* — echo cancellation mode:
  - *voice(default)* — echo cancellers are enabled in the voice data transmission mode.
  - *voice nlp-off* — echo cancellers are enabled in voice mode, non-linear processor (NLP) is disabled. When signal levels on transmission and reception significantly differ, weak signal may become suppressed by the NLP. Use this echo canceller operation mode to prevent the signal suppression.
  - *modem* — echo cancellers are enabled in the modem operation mode (direct component filtering is disabled, NLP control is disabled, CNG is disabled).
  - *voice nlp-option 1* – echo cancellers are enabled in the voice mode, non linear processor NLP is enabled in the mode of less intensive effect on a signal than by default;
  - *voice nlp-option 2* – echo cancellers are enabled in the voice mode, non linear processor NLP is enabled in the mode of more intensive effect on a signal than by default;
  - *off* — do not use echo cancellation (this mode is set by default).

- *DSCP for RTP* — service type (DSCP) for RTP and UDPTL (T.38) packets.

The DSCP setting for RTP and DSCP setting for SIP will be ignored while using VLAN for RTP transmission and signalling. *Class of Service* VLAN is used for prioritization in this case.

- *RTP loss timeout* — voice frequency path status control function that monitors the presence of RTP traffic from the communicating device. Permitted value range is from 10 to 300sec. When unchecked, RTP control is disabled; when checked, it is enabled. Control is performed as follows: if there are no RTP packets coming from the opposite device for the duration of the timeout and the last packet was not a silence suppression packet, the call will be rejected.

- *RTP loss timeout after Silence-Suppression indication* — RTP packet timeout for the silence suppression option utilization. Permitted value range is from 1 to 30. Coefficient is a multiplier that applies to the *'RTP packet timeout'* value. Control is performed as follows: if there are no RTP packets coming from the opposite device for the duration of the timeout and the last packet was a silence suppression packet, the call will be rejected.

- *RTCP period (sec.)* — time period in seconds (5-65535), after which the device send control packets via RTCP protocol. When unchecked, RTCP will not be used.

- *RTCP activity control* — voice frequency path status control function, may take up values in the range 2–255. Quantity of time periods (RTCP timer) during which the opposite party will wait for RTCP protocol packets. When there is no packets in the specified period of time, established connection will be terminated. At that, cause of disconnection '*cause 3 no route to destination*' is assigned to the TDM and IP protocols. Control period value is calculated using the following equation: ***RTCP timer* RTCP control period*** sec. When unchecked, feature will be disabled.

- *Clear Channel* — channel established for the transparent digital data transfer; when this channel is established, the device will not attempt to recode it and will transfer it transparently. To establish such a connection, reception of '*Transmission Medium Requirement*' field is required with the following values:
  - restricted digital info (Q.931 protocol)
  - unrestricted dig.info (Q.931 protocol)
  - video (Q.931 protocol)
  - 64 kbit/s unrestricted (SS7 protocol)

- *Clear Channel override* — when checked, during 'clear channel' organization, a single codec CLEARMODE will be specified in SDP (if operation via Clear Channel was requested on the first call leg). When unchecked, the complete list of selected codecs will be always transferred to SDP in priority order.

- *ClearChannel-transit* is a mode that allows to transfer RTP directly from the incoming connection branch to the outgoing connection branch in SIP – SIP connection skipping internal switch buses of the device and preserving RTP traffic including packetization time.

Digital gain

- *Rx gain (0.1 dB)* – volume of a receiving signal, amplification/attenuation of the level of signal received from an interacting gateway;
- *Tx gain (0.1 dB)* – volume of a transmitting signal, amplification/attenuation of the level of signal transmitted to an interacting gateway.

AGC (Auto Gain Control)

- *Compliance with ITU-T G.169* – when the option is enabled, the automatic amplification operates in compliance with ITU-T G.169. The operation mode uses some algorithms different from the recommendations, which provide better background noise suppresion in the absence of speech.

Rx gain settings

- *AGC master enable* – enable automatic amplification of receiving signals;
- *Limit gain during double talk* – limit a signal level if subscribers are talking simultaneously;
- *Signal reference gain, dBm0* – the level of the signal to which amplification will tend;
- *Signal maximum gain, dB* – the maximum permissible value of the amplification of an original signal ;
- *Signal minimum gain, dB* – the minimum permissible value of the amplification of an original signal;

Tx gain settings

- *AGC master enable* – enable automatic amplification of transmitting signals;
- *Limit gain during double talk* – limit a signal level if subscribers are talking simultaneously;
- *Signal reference gain, dBm0* – the level of the signal to which amplification will tend;
- *Signal maximum gain, dB* – the maximum permissible value of the amplification of an original signal;
- *Signal minimum gain*, dB – the minimum permissible value of the amplification of an original signal.

Dual-Tone Multi-Frequency signalling settings:

- *DTMF transport* — method of DTMF transmission via IP network.
  - *inband* — in RTP packets, inband.
  - *RFC2833* — in RTP packets according to RFC2833 recommendation.
  - *SIP-INFO* — outband, via SIP, INFO messages are used; at that, DTMF signal appearance will depend on the MIME extension type.

- *SIP-NOTIFY* - NOTIFY messages are used via SIP protocol and out-of-band. This DTMF transmission is an implementation of the method that is used on Cisco equipment.

In order to be able to use extension dialing during the call, make sure that the similar DTMF tone transmission method is configured on the opposite gateway.

- *Flash signal processing (RFC2833)* — checkbox that governs activation of FLASH signal processing using INFO, RFC2833, and re-invite methods for *'Call transfer'* VAS operation.

- *RFC2833 PT* — type of payload used to transfer DTMF packets via RFC2833. Permitted values: 96 to 127. RFC2833 recommendation describes the transmission of DTMF via RTP protocol. This parameter should conform to the similar parameter of a communicating gateway (the most frequently used values: 96, 101).

- *RFC2833: same PT* — when checked, if SMG is the party that sends 'offer SDP', RFC2833 packets are expected for reception with PT value sent in 'answer SDP'; otherwise, RFC2833 packets are expected for reception with the same PT value that SMG has sent in 'offer SDP'.

- *DTMF MIME Type* — specify payload 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).

Jitter buffer parameters:

- *Mode* — jitter buffer operation mode: static or dynamic.

- *Minimum size, ms* — size of fixed jitter buffer or lower limit (minimum size) of adaptive jitter buffer. Permitted value range is from 0 to 200ms.

- *Initial size, ms* — initial value of adaptive jitter buffer. Permitted value range is from 0 to 200ms.

- *Maximum size, ms* — upper limit (maximum size) of adaptive jitter buffer, in milliseconds. Permitted value range is from 'Min size' to 200ms.

- *Adaptation period, ms* — time of buffer adaptation to the lower limit without faults in packet sequence order.

- *Removal mode* — buffer adjustment mode. Defines the method of packet deletion during buffer adjustment to lower limit.

  - *Soft* — device uses intelligent selection pattern for deletion of packets that exceed the threshold.
  - *Hard* — packets which delay exceeds the threshold will be deleted immediately.

- *Removal threshold, ms* — threshold for immediate deletion of a packet, in milliseconds. When buffer size grows and packet delay exceeds this threshold, packets will be deleted immediately. Permitted value range is from max size to 500ms.

- *Adjustment mode* — select the adaptive jitter buffer adjustment mode for its increase (gradual/instant).

- *Size for VBD, ms* — size of a fixed jitter buffer used for data transmission in VBD mode (modem communication). Permitted value range is from 0 to 200ms.

Codecs:

In this section, you may select codecs for an interface and an order of their usage on connection establishment. Codec with the highest priority should be placed in top position.

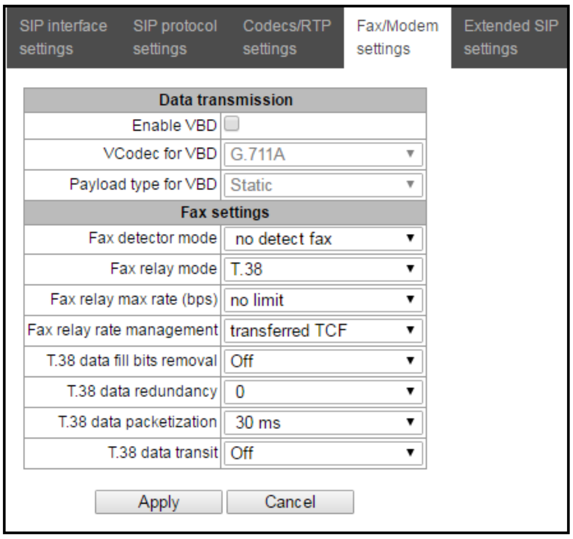
Click the left mouse button to highlight the row with the selected codec. Use arrow buttons ⬇⬆ (up, down) to change the codec priority.

- *On* — when checked, use a codec specified in the adjacent field.
- *Codec* — codec, used for voice data transmission. Supported codecs: G.711A, G.711U, G.729A, G.729B, G.723.1, G.726-32.

When VAD/CNG are enabled, G.729 codec operates as G.729B, otherwise as G729A, and G.723.1 codec operates with annex A support, otherwise without annex A support.

- *PType* — payload type for a codec. Field is available for editing only when G.726 codec is selected (permitted values: from 96 to 127, or 2 for negotiation with devices that does not support dynamic payload type for this codec). For other codecs, it is assigned automatically.
- *PTE* — packetization time — amount of voice data in milliseconds (ms), transmitted in a single packet.

3.1.7.3.1.4 Fax/Modem settings tab



Data transmission	
Enable VBD	□
VCodec for VBD	G.711A
Payload type for VBD	Static
Fax settings	
Fax detector mode	no detect fax
Fax relay mode	T.38
Fax relay max rate (bps)	no limit
Fax relay rate management	transferred TCF
T.38 data fill bits removal	Off
T.38 data redundancy	0
T.38 data packetization	30 ms
T.38 data transit	Off

Data transmission:

- *Enable VBD* — when checked, create VBD channel according to V.152 recommendation for modem transmission. When CED signal is detected, the device enters *Voice band data* mode. Deselect the checkbox to disable modem tone detection; at that, modem communication will not be affected (switching to modem codec will not be initiated, but such operation still may be performed by the opposite gateway).
- *VCodec for VBD* — codec, used for data transmission in VBD mode
- *Payload type for VBD* — payload type, used for data transmission in VBD mode
  - Static — use payload type standard values for a codec (for G.711A codec payload type is 8, for G.711U payload type is 0).
  - 96-127 — payload types from the dynamic range.

Fax settings:

- *Fax detector mode* — detects transmission direction for fax tone detection and subsequent switching to fax codec:
  - no detect fax — disables fax tone detection, but will not affect fax transmission (switching to fax codec will not be initiated, but such operation still may be performed by the opposite gateway).
  - Caller and Callee — tones are detected during both fax transmission and receiving. During fax transmission, CNG FAX signal is detected from the subscriber's line. During fax receiving, V.21 signal is detected from the subscriber's line.
  - Caller — tones are detected only during fax transmission. During fax transmission, CNG FAX signal is detected from the subscriber's line.
  - Callee — tones are detected only during fax reception. During fax receiving, V.21 signal is detected from the subscriber's line.

✓ **V.21 signal may also be detected from fax performing transmission.**

- *Fax relay mode* — select protocol for fax transmission.

- *Fax relay max rate (bps)* — maximum transfer rate of fax transmitted via T.38 protocol. This setting affects the ability of a gateway to work with high-speed fax units. If fax units support data transfer at 14400 baud, and the gateway is configured to 9600 baud, the maximum rate of connection between fax units and the gateway will be limited at 9600 baud. And vice versa, if fax units support data transfer at 9600 baud, and the gateway is configured to 14400 baud, this setting will not affect the interaction, maximum rate will be defined by the performance of fax units.

- *Fax relay rate management* — set the data transfer rate management method:
  - *local TCF* — method requires that the TCF tuning signal was generated locally by the recipient gateway. In general, used in T.38 transmission via TCP.
  - *transferred TCF* — method requires that the TCF tuning signal was sent from the sender device to the recipient device. In general, used in T.38 transmission via UDP.

- *T.38 data fill bits removal* — padding bit removals and inserts for data that does not relate to ECM (error correction mode).

- *T.38 data redundancy* — redundancy amount in T.38 data packets (amount of previous packets in the following T.38 packet). Introduction of redundancy allows to restore the transmitted data sequence on reception when packets were lost during transmission.

- *T.38 data packetization* — define T.38 packet generation frequency in milliseconds (ms). This option allows to adjust the size of a transmitted packet. If the communicating gateway is able to receive datagrams with max. size of 72 bytes (maxdatagrammSize: 72), packetization time should be set to a minimum on SMG.

- *T.38 data transit* — when the call is performed using two SIP interfaces and T.38 fax transfer protocol is used by both interfaces, this setting allows to transit T.38 packets between interfaces with a minimum delay.

<u>'Service type' (IP DSCP) field value for RTP, T.38 and SIP/SIP-T/SIP-I:</u>

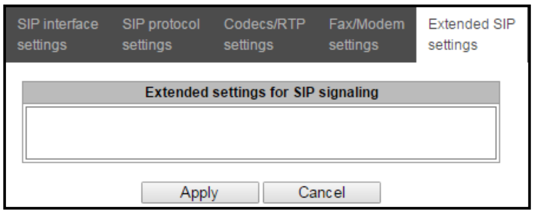
0 (DSCP 0x00, Diffserv 0x00) – Best effort – default value
8 (DSCP 0x08, Diffserv 0x20) – Class 1
10 (DSCP 0x0A, Diffserv 0x28) – assured forwarding, low drop precedence (Class1, AF11)

12 (DSCP 0x0A, Diffserv 0x28) – assured forwarding, medium drop precedence (Class1, AF12)
14 (DSCP 0x0E, Diffserv 0x38) – assured forwarding, high drop precedence (Class1, AF13)
16 (DSCP 0x10, Diffserv 0x40) – Class 2
18 (DSCP 0x12, Diffserv 0x48) – assured forwarding, low drop precedence (Class2, AF21)
20 (DSCP 0x14, Diffserv 0x50) – assured forwarding, medium drop precedence (Class2, AF22)
22 (DSCP 0x16, Diffserv 0x58) – assured forwarding, high drop precedence (Class2, AF23)
24 (DSCP 0x18, Diffserv 0x60) – Class 3
26 (DSCP 0x1A, Diffserv 0x68) – assured forwarding, low drop precedence (Class3, AF31)
28 (DSCP 0x1C, Diffserv 0x70) – assured forwarding, medium drop precedence (Class3, AF32)
30 (DSCP 0x1E, Diffserv 0x78) – assured forwarding, high drop precedence (Class3, AF33)
32 (DSCP 0x20, Diffserv 0x80) – Class 4
34 (DSCP 0x22, Diffserv 0x88) – assured forwarding, low drop precedence (Class4, AF41)
36 (DSCP 0x24, Diffserv 0x90) – assured forwarding, medium drop precedence (Class4, AF42)
38 (DSCP 0x26, Diffserv 0x98) – assured forwarding, high drop precedence (Class4, AF43)
40 (DSCP 0x28, Diffserv 0xA0) – Class 5
46 (DSCP 0x2E, Diffserv 0xB8) – expedited forwarding (Class5, Expedited Forwarding).

IP Precedence:
0 – IPP0 (Routine);
8 – IPP1 (Priority);
16 – IPP2 (Immediate);
24 – IPP3 (Flash);
32 – IPP4 (Flash Override);
40 – IPP5 (Critical);
48 – IPP6 (Internetwork Control);
56 – IPP7 (Network Control).

3.1.7.3.1.5 Advanced settings tab

In this section, you will find SIP advanced settings. These settings allow you to modify SIP message fields using defined rules.



Field entry format

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

where:

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

Modification rules

Modification rules are described by the following characters:

- $ — keep the text that follows

- ! — delete the remaining text
- +(ABC) — add the text specified
- -(ABC) — delete the text specified

For implementation examples of operation rules, see the Table below.

To implement SIP headers transmission, you need to set "SIP header transit" option on the SIP interface from which the headers will be selected.

Table 18 — Implementation examples of operation rules

Operation	***Initial header***	***Rule***	***Result***
Do not send the header	Accept: application/SDP	[sipheader:accept=disable]	
Transmit the header from the first leg without change.	Additional headers on the first leg: P-Asserted-Identity: username@domain Subject: Test call	[sipheader:[LIST_OF_MESSAGES]:[HEADER_MASK]=transit] [sipheader:[HEADER_MASK]=transit] In INVITE and 200 messages: [sipheader:INVITE,200:Subject=transit] In any messages: [sipheader:Subject=transit]	The defined header appears on the second leg: Subject: Test call
Transmit the group of headers from the first leg without changes.	Additional headers on the first 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 following rule: [sipheader:*=transit] will not be operate, as the * character can replace only a part of a name.	The defined headers appear on the second leg: P-Asserted-Identity: sip:username@domain P-Called-Party-ID: sip:username@domain
Insert a header		[sipheader:insert[LIST_OF_HEADERS]:RemoteIp=+(TEXT)] In all requests: [sipheader:insert:RemoteIp=+(example.SMG)] In INVITE request: [sipheader:insert,INVITE:RemoteIp=+(example.SMG)] Only in specified requests (e.g. INVITE and ACK): [sipheader:insert,INVITE,ACK:RemoteIp =+(example.SMG)]	RemoteIp:example.SMG
Add text at the beginning	Accept: application/SDP	[sipheader:accept=+(application/ISUP,)$]	Accept: application/ISUP,application/SDP
Add text at the end	Accept: application/SDP	[sipheader:accept=$+(,application/ISUP)]	Accept: application/SDP,application/ISUP

Delete text	Accept: application/SDP,application/ISUP	[sipheader:accept=-(application/SDP,)$]	Accept: application/ISUP
Delete beginning from the specific place	Accept: application/SDP,text/plain	[sipheader:accept=-(text)!]	Accept: application/SDP
Replace text completely	Accept: application/SDP	[sipheader:accept=+(application/ISUP)!]	Accept: application/ISUP
Replace text	Accept: application/SDP,text/plain	[sipheader:accept=-(SDP)+(ISUP)$]	Accept: application/ISUP,text/plain
Replace text, discarding data at the end	Accept: application/SDP,text/plain	[sipheader:accept=-(SDP)+(ISUP)!]	Accept: application/ISUP,text/plain
Complete the text	To: "Ivanov A.A." <sip:123@eltex>	[sipheader:to=-(eltex)+(eltexdomain.loc)$]	To: "Ivanov A.A." <sip:123@eltexdomain.loc>
Example of a complex modification	From: <sip:who@host>;tag=aBc	[sipheader:from=+(DISPLAY)-(who)+(12345)-(>)+(;user=phone>)$+(;line=abc)]	From: DISPLAY <sip:12345@host;user=phone>;tag=aBc;line=abc

Example

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

In this example, all SIP messages sent by the device via the current SIP interface will follow without *Accept* and *user-agent* fields*.*

The list of compulsory headers of SIP messages which are prohibited to ignore and transit: *via, from , to, call-id, cseq, contact, content-type, content-length.*

3.1.7.4 H323 interfaces

In this section, you may configure H.323[1] stack general configuration parameters, custom settings for each direction operating via H.323 protocol.

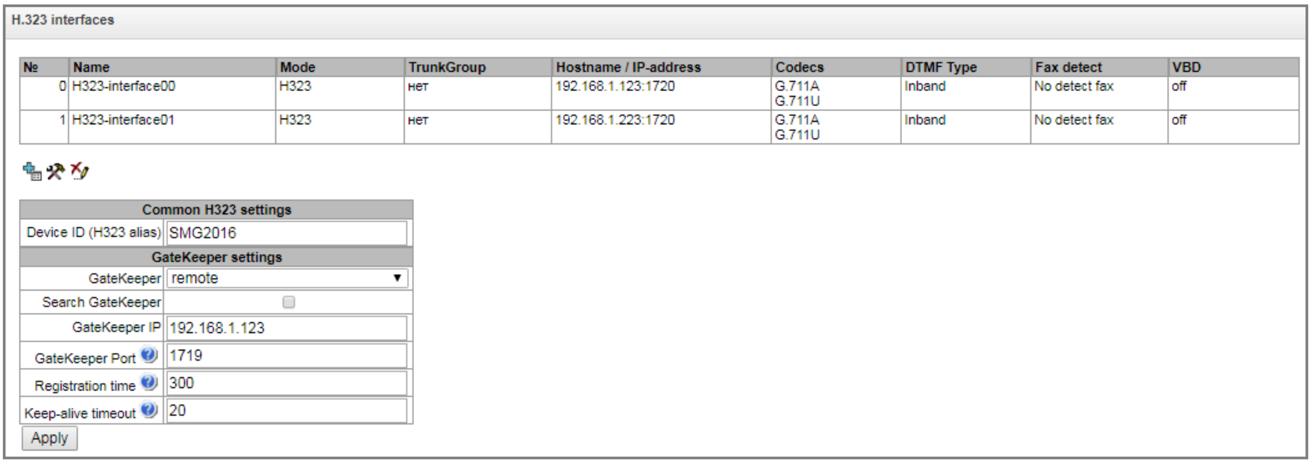
H.323 protocol is a signaling protocol utilized in VoIP applications for multimedia data transmission via **packed-based data networks**. It performs basic call management tasks such as starting and finishing session.

H.323 signaling is a stack of protocols based on the **Q.931** recommendation implemented in ISDN. Recommendations utilized by the gateway: **H.225.0** and **H.245.**

SMG may operate within a method that may or may not feature the **Gatekeeper**. The separate license allows to use SMG gateway as a gatekeeper and to interact with Directory gatekeeper for defining subscriber location.

[1] The menu is available for the devices with H.323 license. Read more detailed information on licenses in the section 3.1.23 Licenses.

Common H.323 settings



H.323 interfaces

№	Name	Mode	TrunkGroup	Hostname / IP-address	Codecs	DTMF Type	Fax detect	VBD
0	H323-interface00	H323	нет	192.168.1.123:1720	G.711A G.711U	Inband	No detect fax	off
1	H323-interface01	H323	нет	192.168.1.223:1720	G.711A G.711U	Inband	No detect fax	off

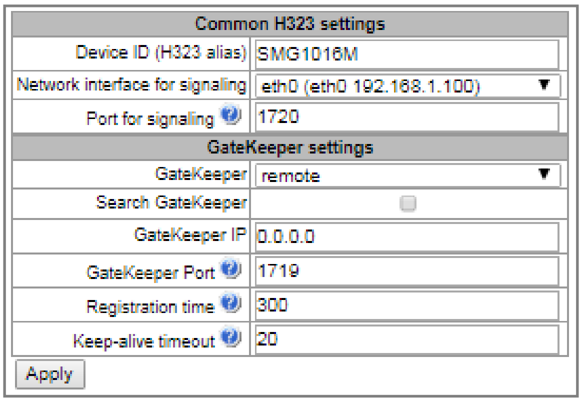
Common H323 settings	
Device ID (H323 alias)	SMG2016
GateKeeper settings	
GateKeeper	remote ▼
Search GateKeeper	□
GateKeeper IP	192.168.1.123
GateKeeper Port	1719
Registration time	300
Keep-alive timeout	20

- *Device ID (H323 alias)* — gateway name during registration at the Gatekeeper.
- *Network interface for signalling* — select the network interface for H.323 signaling.
- *Port for signaling* — local TCP port for H.323 signaling message reception.

GateKeeper settings

- GateKeeper – define the mode of gatekeeper operation. In the "remote" mode, SMG interacts with external gatekeeper. In the "local" mode, SMG operates as a gatekeeper.

Settings for «remote» mode:



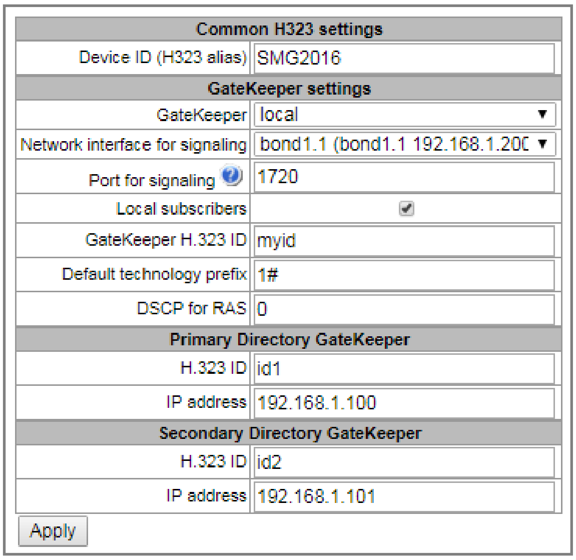
Common H323 settings	
Device ID (H323 alias)	SMG1016M
Network interface for signaling	eth0 (eth0 192.168.1.100) ▼
Port for signaling	1720
GateKeeper settings	
GateKeeper	remote ▼
Search GateKeeper	□
GateKeeper IP	0.0.0.0
GateKeeper Port	1719
Registration time	300
Keep-alive timeout	20

- *Search GateKeeper* — when checked, automatic Gatekeeper discovery method will be used in multicast mode using IP address 224.0.1.41 and UDP port 1718, otherwise this method will not be used and the Gatekeeper will have a specific IP address.
- *GateKeeper IP* — identification of the gatekeeper at the specific IP.
- *GateKeeper Port* — gatekeeper UDP port (port 1719 is used by the majority of gatekeepers by default).
- *Registration time* — time period in seconds, for which the device will keep its registration on a gatekeeper.
- *Keep-alive timeout* — time period in seconds, after which the device will renew its registration on a gatekeeper.

To ensure the successful renewal of device registration on gatekeeper, specify *Keep Alive Time* renewal period equal to 2/3 of *'Registration time'* registration period. At that, for *'Registration time'* parameter, we recommend specifying the same value as for the gatekeeper, so the registration renewal period *'Keep Alive Time'* of the gateway was less or equal to *'Registration time'* value transferred in responses. Otherwise, invalid configuration may lead to situations, where gatekeeper will void the gateway registration before the renewal, which in turn may lead to termination of all active connections, established through the gatekeeper.

When settings are applied in this section, H.323 will be restarted and all established H.323 voice connections will be forcedly terminated, also H323-MODULE LOST fault may appear shortly.

Settings for «local» mode[1]:



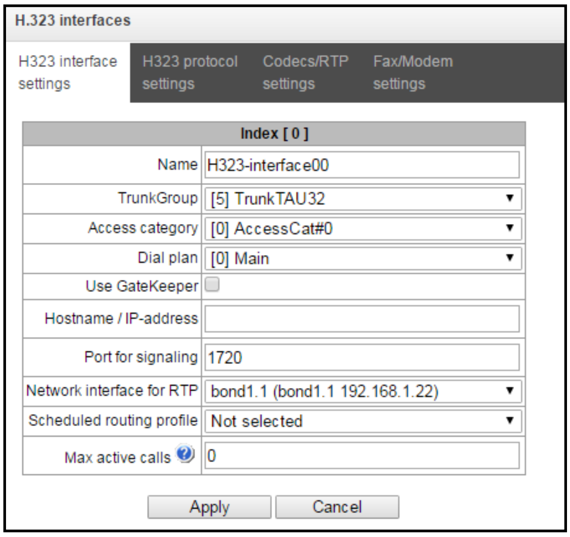
Common H323 settings	
Device ID (H323 alias)	SMG2016
GateKeeper settings	
GateKeeper	local ▾
Network interface for signaling	bond1.1 (bond1.1 192.168.1.20(▾
Port for signaling	1720
Local subscribers	☑
GateKeeper H.323 ID	myid
Default technology prefix	1#
DSCP for RAS	0
Primary Directory GateKeeper	
H.323 ID	id1
IP address	192.168.1.100
Secondary Directory GateKeeper	
H.323 ID	id2
IP address	192.168.1.101

- GateKeeper H.323 ID – an identifier of local Gatekeeper operating on SMG;
- *Defualt technology prefix* – defines the default directions to which the GateKeeper will transmit calls returned from Directory GateKeeper and not intended for SMG SIP subscribers. The direction must be registered on a local GateKepper of SMG;
- *DSCP for RAS* – type of service (DSCP) for signaling traffic (H.323 RAS);
- *Primary Directory Gatekeeper* and *Secondary Directory Gatekeeper* – settings for interaction with a main and redundant Directory GateKeepers;
- *H.323 ID* – an identifier of Directory Gatekeeper;
- *IP address* – an IP address of Directory Gatekeeper.

The interaction of local GateKeeper and Directory GateKeeper is performed as follows: While egress call: SMG transmits location request (RAS LRQ) to Directory GateKeeper. Directory GateKeeper defines the subscriber location and transmits its signal address in location confirm message (RAS LCF). If the Directory GateKeeper cannot define the location, the call will be released with the location reject message (RAS LRJ). While ingress call: Directory GateKeeper transmits location request (RAS LRQ) to SMG. If the callee is a subscriber of SMG, SMG transmits its signal address in location confirm message (RAS LCF). If the callee is not a subscriber of SMG, but has a registered technology prefix, SMG transmits a signal address of a device which registered this prefix in location confirm (RAS LCF). If there is no registered prefix, SMG releases the call with location reject message (RAS LRJ).

[1] The menu is available for the devices with H.323-GK license. Read more detailed information on licenses in the section 3.1.23 Licenses.

3.1.7.4.1 H.323 interface settings tab

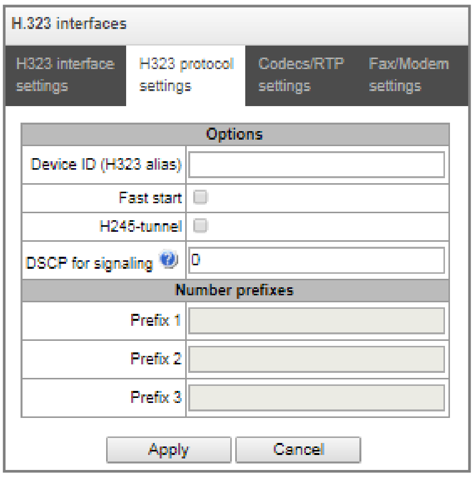

H.323 interfaces

Index [0]

Name	H323-interface00
TrunkGroup	[5] TrunkTAU32
Access category	[0] AccessCat#0
Dial plan	[0] Main
Use GateKeeper	□
Hostname / IP-address	
Port for signaling	1720
Network interface for RTP	bond1.1 (bond1.1 192.168.1.22)
Scheduled routing profile	Not selected
Max active calls	0

- *Name* — interface name.
- *TrunkGroup* — select a trunk group, that the interface belongs to.
- *Access category* — select access category.
- *Dial plan* — define dial plan that will be used for dialing from this interface (necessary for dial plan negotiation).
- *Use GateKeeper* — when checked, the current interface will interact with the GateKeeper which settings are specified in 'H.323 general configuration' section.
- *Host name/IP address* — IP address or name of the host communicating via gateway H.323 protocol.
- *Port for signaling* — signaling TCP port of the communicating gateway used for H323 signaling reception.
- *Network interface for RTP* — select network interface for voice traffic transmission and reception.
- *Scheduled routing profile* — select 'Scheduled routing' service profile, configured in the 'Internal resources' section.
- *Max active calls* — maximum number of simultaneous (incoming and outgoing) connection through the interface specified.

3.1.7.4.2 H.323 protocol settings tab



H.323 interfaces

H323 interface settings | H323 protocol settings | Codecs/RTP settings | Fax/Modem settings

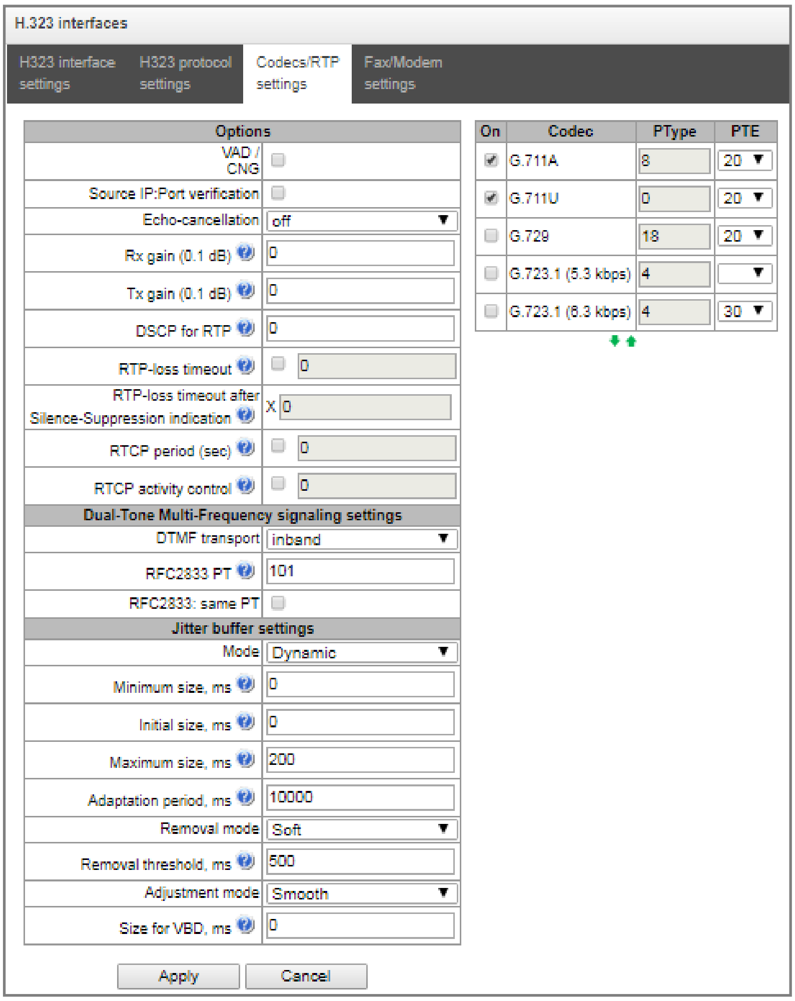
Options	
Device ID (H323 alias)	
Fast start	□
H245-tunnel	□
DSCP for signaling	0
Number prefixes	
Prefix 1	
Prefix 2	
Prefix 3	

- *Device ID (H323 alias)* — gateway name during registration at the Gatekeeper.
- *Fast start* — when checked, fast start function is enabled, otherwise it is disabled. When option is used, session description for media channel establishing is performed via H.225 protocol, otherwise via H.245 protocol.
- *H245-tunnel* — when checked, H.245 signaling tunneling is enabled through the Q.931 signal channel, otherwise it is disabled.
- *DSCP for signaling* — service (DSCP) type for SIP signaling traffic (H.323).

The DSCP setting for RTP and DSCP setting for SIP will be ignored while using VLAN for RTP transmission and signalling. Class of Service VLAN is used for prioritization in this case.

- *Number prefixes (Prefix 1, Prefix 2, Prefix 3)* – numbers, which SMG register on a Gatekeeper according to settings – local or remote. The table is filled with the numbers or initial digits of numbers of SIP subscribers registered on SMG in order to gatekeeper could forward calls to SMG (for example, it is sufficient to write prefix 10010 for subscribers with numbers 100101 and 100102).

3.1.7.4.3 RTP/ codec configuration tab



H.323 interfaces

Options	
VAD / CNG	□
Source IP:Port verification	□
Echo-cancellation	off ▼
Rx gain (0.1 dB)	0
Tx gain (0.1 dB)	0
DSCP for RTP	0
RTP-loss timeout	□ 0
RTP-loss timeout after Silence-Suppression indication	X 0
RTCP period (sec)	□ 0
RTCP activity control	□ 0
Dual-Tone Multi-Frequency signaling settings	
DTMF transport	inband ▼
RFC2833 PT	101
RFC2833: same PT	□
Jitter buffer settings	
Mode	Dynamic ▼
Minimum size, ms	0
Initial size, ms	0
Maximum size, ms	200
Adaptation period, ms	10000
Removal mode	Soft ▼
Removal threshold, ms	500
Adjustment mode	Smooth ▼
Size for VBD, ms	0

On	Codec	PType	PTE
☑	G.711A	8	20 ▼
☑	G.711U	0	20 ▼
□	G.729	18	20 ▼
□	G.723.1 (5.3 kbps)	4	▼
□	G.723.1 (6.3 kbps)	4	30 ▼

Options:

- *Voice activity detector / Comfort noise generator (VAD/CNG)* — when checked, silence detector and comfort noise generator are enabled. Voice activity detector disables transmission of RTP packets during periods of silence, reducing loads in data networks.

- *RTP source IP: Port verification* — when this setting is checked, control of media traffic received from IP address and UDP port specified in SDP communication session description will be enabled; otherwise the traffic from any IP address and UDP port will be accepted.

- *Echo cancellation* — echo cancellation mode:

  – *voice(default)* — echo cancellers are enabled in the voice data transmission mode.
  – *voice nlp-off* — echo cancellers are enabled in voice mode, non-linear processor (NLP) is disabled. When signal levels on transmission and reception significantly differ, weak signal may become suppressed by the NLP. Use this echo canceller operation mode to prevent the signal suppression.
  – *modem* — echo cancellers are enabled in the modem operation mode (direct component filtering is disabled, NLP control is disabled, CNG is disabled).
  – *voice nlp-option 1* – echo cancellers are enabled in the voice mode, non linear processor NLP is enabled in the mode of less intensive effect on a signal than by default;
  – *voice nlp-option 2* – echo cancellers are enabled in the voice mode, non linear processor NLP is enabled in the mode of more intensive effect on a signal than by default;
  – *off* — do not use echo cancellation (this mode is set by default).

- *Rx gain (0.1 dB)* — volume of signal received, gain of the signal received from the communicating gateway.

- *Tx gain (0.1 dB)* — volume of signal transmitted, gain of the signal transmitted to the communicating gateway direction.

- *DSCP for RTP* — service type (DSCP) for RTP and UDPTL (T.38) packets.

The DSCP setting for RTP and DSCP setting for SIP will be ignored while using VLAN for RTP transmission and signalling. Class of Service VLAN is used for prioritization in this case.

- *RTP loss timeout* – the function that controls the presence of RTP traffic from interacting device on a voice-frequency path. The permissible values are from 10 to 300 seconds. When unchecked, RTP control is disabled, when checked – enabled. The control is implemented as follows: if during the set timeout there is no RTP packets received and the last packet was not the packet of pause suppression, the call will be released.

- *RTP loss timeout after Silence-Suppression indication (coefficient)* – timeout for RTP packets when using the option of pause suppression. The permissible values are from 1 to 30. The coefficient defines how many times this value greater than RTP-loss timeout. The control is implemented as follows: if there is no RTP packets received and the last packet was the packet of pause suppression, the call will be released.

- *RTCP period (sec.)* — time period in seconds (5-65535), after which the device send control packets via RTCP protocol. When unchecked, RTCP will not be used.

- *RTCP activity control* — voice frequency path status control function, may take up values in the range 2–255 seconds. Quantity of time periods (RTCP timer) during which the opposite party will wait for RTCP protocol packets. When there is no packets in the specified period of time, established connection will be terminated. At that, cause of disconnection '*cause 3 no route to destination*' is assigned to the TDM and IP protocols. Control period value is calculated using the following equation: ***RTCP timer* RTCP control period*** sec. When unchecked, feature will be disabled.

DTMF transmission:

- *DTMF transport* — a method of DTMF transmission via IP network.
  - inband — inband, in RTP voice packets.
  - RFC2833 — according to RFC2833 recommendation, as a dedicated payload in RTP voice packets.
  - H.245-ALPHANUM — outband; in H.245 userInput messages, basicstring compatibility is used for DTMF transmission.
  - H.245-SIGNAL — outband; in H.245 userInput messages, dtmf compatibility is used for DTMF transmission.
  - Q931 Keypad — outband; Keypad information element is used for DTMF transmission in Q.931 INFORMATION message.

In order to be able to use extension dialing during the call, make sure that the similar DTMF tone transmission method is configured on the opposite gateway.

- *RFC2833 PT* — type of payload used to transfer DTMF packets via RFC2833. Permitted values: 96 to 127. RFC2833 recommendation describes the transmission of DTMF via RTP protocol. This parameter should conform to the similar parameter of a communicating gateway (the most frequently used values: 96, 101).

- *RFC2833: same PT* – when checked, if SMG is an initiating side of connection, RFC2833 packets with PT value which **has been transmitted by OpenLogicalChannelAck**, are expected to be received. Otherwise, the RFC2833 with the PT value, which **has been transmitted in OpenLogicalChannelAck request by SMG**, are expected to be received.

Jitter buffer parameters:

- *Mode* — jitter buffer operation mode: fixed or adaptive.
- *Min size, ms* — size of fixed jitter buffer or lower limit (minimum size) of adaptive jitter buffer. Permitted value range is from 0 to 200ms.
- *Initial size, ms* — initial value of adaptive jitter buffer. Permitted value range is from 0 to 200ms.
- *Max size, ms* — upper limit (maximum size) of adaptive jitter buffer, in milliseconds. Permitted value range is from 'Min size' to 200ms.
- *Adaptation period, ms* — time of buffer adaptation to the lower limit without faults in packet sequence order.
- *Deletion mode* — buffer adjustment mode. Defines the method of packet deletion during buffer adjustment to lower limit.
  - *Soft* — device uses intelligent selection pattern for deletion of packets that exceed the threshold.
  - *Hard* — packets which delay exceeds the threshold will be deleted immediately.
- *Deletion threshold, ms* — threshold for immediate deletion of a packet, in milliseconds. When buffer size grows and packet delay exceeds this threshold, packets will be deleted immediately. Permitted value range is from 'Max size' to 500ms.
- *Adjustment mode* — select the adaptive jitter buffer adjustment mode for its increase (gradual/instant).
- *Size for VBD, ms* — size of a fixed jitter buffer used for data transmission in VBD mode (modem communication). Permitted value range is from 0 to 200ms.

Codecs:

In this section, you may select codecs for an interface and an order of their usage on connection establishment. Codec with the highest priority should be placed in top position.

Click the left mouse button to highlight the row with the selected codec. Use arrow buttons ⬇⬆ (up, down) to change the codec priority.

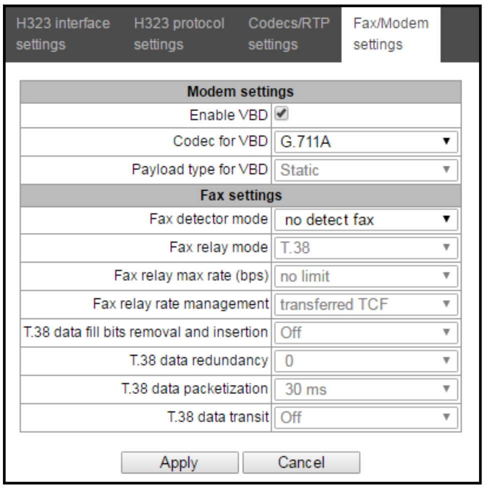
- *Enable* — when checked, use a codec specified in the adjacent field.
- *Codec* — codec, used for voice data transmission. Supported codecs: G.711A, G.711U, G.729A, G.729B, G.723.1.

When VAD/CNG are enabled, G.729 codec operates as G.729B, otherwise as G729A, and G.723.1 codec operates with annex A support, otherwise without annex A support.

- *PType* — payload type for a codec. Field is available for editing only when G.726 codec is selected (permitted values: from 96 to 127, or 2 for negotiation with devices that does not support dynamic payload type for this codec). For other codecs, it is assigned automatically.

- *PTE* — packetization time — amount of voice data in milliseconds (ms), transmitted in a single packet.

3.1.7.4.4 Fax and data transfer configuration tab



Modem settings	
Enable VBD	☑
Codec for VBD	G.711A
Payload type for VBD	Static
Fax settings	
Fax detector mode	no detect fax
Fax relay mode	T.38
Fax relay max rate (bps)	no limit
Fax relay rate management	transferred TCF
T.38 data fill bits removal and insertion	Off
T.38 data redundancy	0
T.38 data packetization	30 ms
T.38 data transit	Off

Moden settings:

- *Enable VBD* — when checked, create VBD channel according to V.152 recommendation for modem transmission. When CED signal is detected, the device enters *Voice band data* mode. Deselect the checkbox to disable modem tone detection; at that, modem communication will not be affected (switching to modem codec will not be initiated, but such operation still may be performed by the opposite gateway).

- *Codec for VBD* — codec, used for data transmission in VBD mode

- *Payload type for VBD* — payload type, used for data transmission in VBD mode

  - *Static* — use payload type standard values for a codec (for G.711A codec payload type is 8, for G.711U payload type is 0).
  - *96-127* — payload types from the dynamic range.

Fax settings:

- *Fax detector mode* — detects transmission direction for fax tone detection and subsequent switching to fax codec:

  - no detect fax — disables fax tone detection, but will not affect fax transmission (switching to fax codec will not be initiated, but such operation still may be performed by the opposite gateway).
  - Caller and Callee — tones are detected during both fax transmission and receiving. During fax transmission, CNG FAX signal is detected from the subscriber's line. During fax receiving, V.21 signal is detected from the subscriber's line.
  - Caller — tones are detected only during fax transmission. During fax transmission, CNG FAX signal is detected from the subscriber's line.
  - Callee — tones are detected only during fax reception. During fax receiving, V.21 signal is detected from the subscriber's line.

V.21 signal may also be detected from fax performing transmission.

- *Fax relay mode* — select protocol for fax transmission.

- *Fax relay max rate (bps)* — maximum transfer rate of fax transmitted via T.38 protocol. This setting affects the ability of a gateway to work with high-speed fax units. If fax units support data transfer at 14400 baud, and the gateway is configured to 9600 baud, the maximum speed of connection between fax units and the gateway will be limited at 9600 baud. And vice versa, if fax units support data transfer at 9600 baud, and the gateway is configured to 14400 baud, this setting will not affect the interaction, maximum speed will be defined by the performance of fax units.

- *Fax relay rate management* — set the data transfer speed management method:
  - *local TCF* — method requires that the TCF tuning signal was generated locally by the recipient gateway. In general, used in T.38 transmission via TCP.
  - *transferred TCF* — method requires that the TCF tuning signal was sent from the sender device to the recipient device. In general, used in T.38 transmission via UDP.

- *T.38 data fill bits removal and insertion* — padding bit removals and inserts for data that does not relate to ECM (error correction mode).

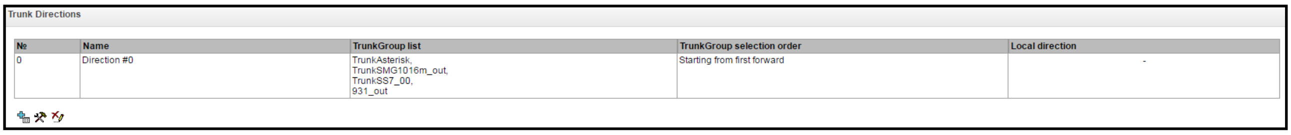
- *T.38 data redundancy* — redundancy amount in T.38 data packets (amount of previous packets in the following T.38 packet). Introduction of redundancy allows to restore the transmitted data sequence on reception when packets were lost during transmission.

- *T.38 data packetization* — define T.38 packet generation frequency in milliseconds (ms). This option allows to adjust the size of a transmitted packet. If the communicating gateway is able to receive datagrams with max. size of 72 bytes (maxdatagrammSize: 72), packetization time should be set to a minimum on SMG.

- *T.38 data transit* — when the call is performed using two VoIP interfaces and T.38 fax transfer protocol is used by both interfaces, this setting allows to transit T.38 packets between interfaces with a minimum delay.

3.1.7.5 Trunk directions

Trunk direction is a set of trunk groups. For a call to a trunk direction, you may specify the selection order for trunk groups comprising this direction.



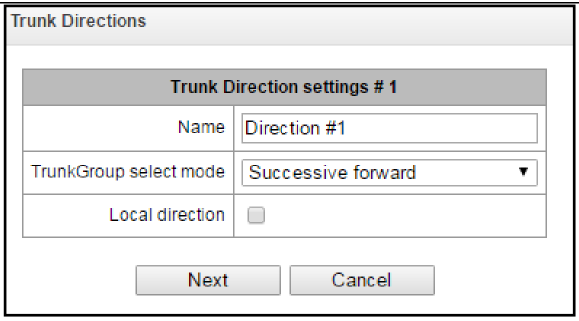
Trunk Directions

№	Name	TrunkGroup list	TrunkGroup selection order	Local direction
0	Direction #0	TrunkAsterisk, TrunkSMG1016m_out, TrunkSS7_00, 931_out	Starting from first forward	-

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

- — *'Add direction'*
- — *'Edit direction parameters'*
- — *'Remove direction'*

✓ **To access the trunk direction, the device configuration should include prefixes that perform transition to this direction.**

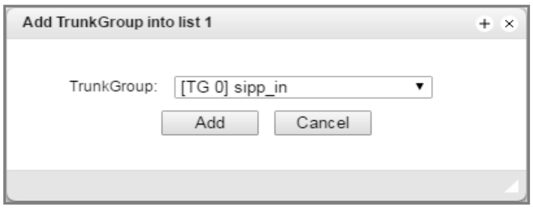


Trunk Directions

Trunk Direction settings # 1	
Name	Direction #1
TrunkGroup select mode	Successive forward
Local direction	□

- *Name* — trunk direction name.
- *TrunkGroup select mode* — trunk group selection order in the direction:
  - *Sequential forward* — all trunk groups comprising the direction are selected in turns beginning from the first in the list.
  - *Sequential back* — all trunk groups comprising the direction are selected in turns beginning from the last in the list.
  - *From the first and forward* — the first free trunk group comprising the direction is selected beginning from the first in the list.
  - *From the last and back* — the first free trunk group comprising the direction is selected beginning from the last in the list.
- *Local direction* — when checked, subscribers of this direction are considered as local.

List of trunk groups in direction



Add TrunkGroup into list 1

TrunkGroup: [TG 0] sipp_in

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

— *'Add'*

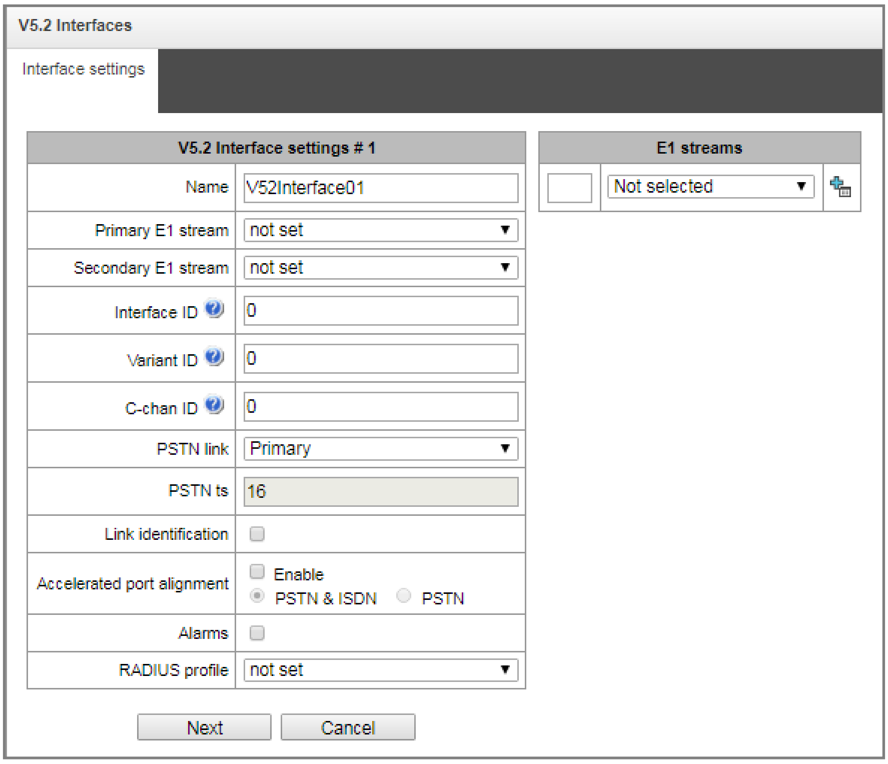
— '*Remove*'

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

3.1.7.6 V5.2 interfaces

The menu is dedicated to V5.2 interface parameters configuration. Click on the "V5.2 Interfaces" sumbenu page ("Call routing" menu) to add a new V5.2 interface. The quantity of created interfaces must be equal to the quantity of outstations.

3.1.7.6.1 «Interface settings» tab



V5.2 Interfaces

Interface settings

V5.2 Interface settings # 1	
Name	V52Interface01
Primary E1 stream	not set ▾
Secondary E1 stream	not set ▾
Interface ID	0
Variant ID	0
C-chan ID	0
PSTN link	Primary ▾
PSTN ts	16
Link identification	□
Accelerated port alignment	□ Enable ● PSTN & ISDN ○ PSTN
Alarms	□
RADIUS profile	not set ▾

E1 streams		
	Not selected ▾	

Next Cancel

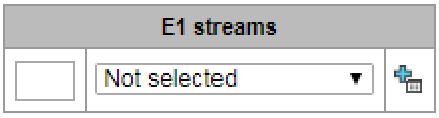
– *Name* – a displayed interface name;
– *Primary E1 stream* – a primary stream for the V5.2 interface;
– *Secondary E1* – a secondary stream for the V5.2 interface;
– *Interface ID* – interface identifier;
– *Variant ID* – a variant of supplying in iitial configuration;
– *C-chan ID* – logic C-channel identifier;
– *PSTN link* – a number of a stream to which a PSTN protocol will be assigned;
– *PSTN ts* – a number of a channel time slot to which a PTSN protocol will be assigned;
– *Link identification* – check the compliance of E1 links ID on LE and AN sides when the interface is launched;
– *Accelerated port alignment* – use accelerated port alignment mechanism when the interface is launched. The following parameters are available:

- PSTN&ISTN – unlock PSTN and ISDN ports;
- PSTN – unlock only PSTN ports.

– Alarms – when checked, the alarm messages are displayed;
– RADIUS profile – select RADIUS profile for the interface.

– *«Add a E1 stream»;*

To add a new E1 stream, you should define its link ID in the field in the left column.

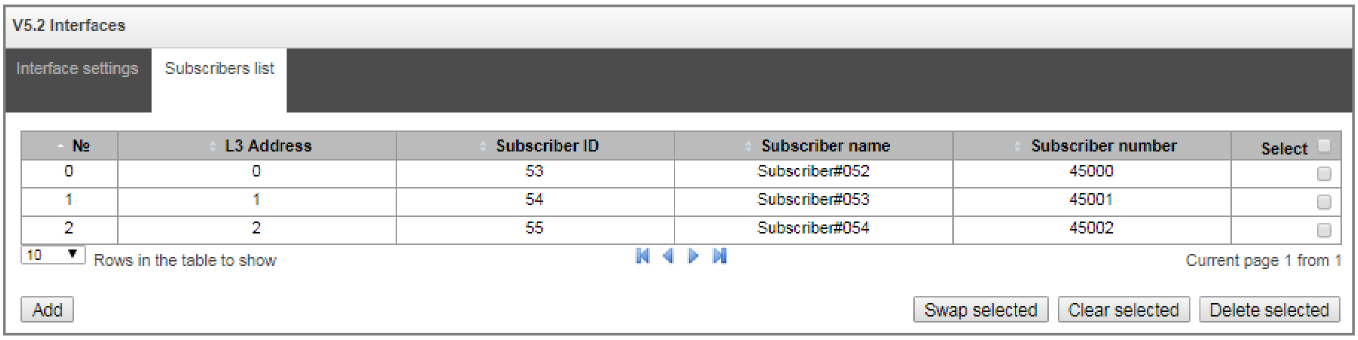


E1 streams		
	Not selected ▾	

To change the order of E1 streams in the list, use ⬇⬆ arrows.

3.1.7.7 «Subscribers list»

The section is dedicated to attach created V5.2 subscribers to the specified V5.2 interface. Each subscriber cell contains the "L3 Address" which is unique within a single interface.



№	L3 Address	Subscriber ID	Subscriber name	Subscriber number	Select □
0	0	53	Subscriber#052	45000	□
1	1	54	Subscriber#053	45001	□
2	2	55	Subscriber#054	45002	□

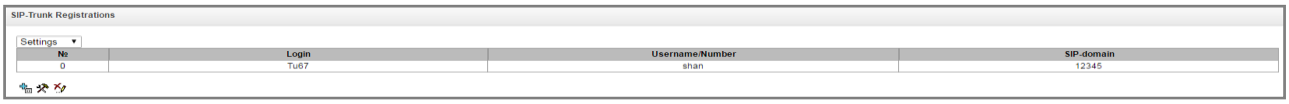
- *№* –serial number of a subscriber;
- *L3 address* – subscriber Layer 3 address, it is used to identify a subscriber within V5.2 interface;
- *Subscriber ID* – a unique subscriber identifier;
- *Subscriber name*;
- *Subscriber number* – subscriber phone number.

To edit the list use the following buttons:

- *Add* – add V5.2 subscriber;
- *Swap selected* – exchange the positions of two selected subscribers;
- *Clear selected* – clear the subscriber cell, but do not remove L3 address from the list. It is used to remove subscribers located in the middle of the list.
- *Delete selected* – delete the subscriber cell and remove L3 address. It is used to remove subscribers located at the end of the list.

3.1.7.8 Registration

3.1.7.8.1 Configuration



№	Login	Username/Number	SIP-domain
0	Tu67	shan	12345

Subscriber registration and authentication parameters for interfaces with the subscriber registration type.

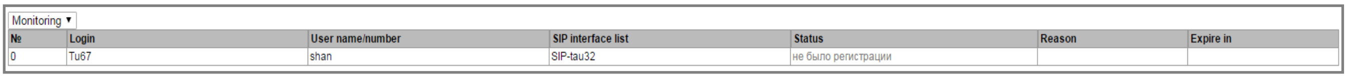
Registration parameters:

- *Login* — name used for authentication.
- *Password* — password used for authentication.
- *Username/Number* — number of the user registered at SIP domain.
- *SIP domain* — domain that is used for subscriber registration on the upstream server.

In the list of SIP interfaces, you may assign/remove registration binding to a specific SIP interface. This allows to define a list of subscribers that are allowed to perform calls via this interface.

3.1.7.8.2 Monitoring

When you choose 'Monitoring' item from the drop down list, a table will be shown that enables monitoring of the subscriber registration on the upstream server.



Monitoring ▾

№	Login	User name/number	SIP interface list	Status	Reason	Expire in
0	Tu67	shan	SIP-tau32	не было регистрации		

- *Login* — name used for authentication.
- *Username/Number* — number of the user registered on the upstream server.
- *SIP interface list* — list of interfaces with enabled access for the current subscriber.
- *Status* — subscriber registration status (registered, not registered, registration expired).
- *Reason* — possible reason for missing registration.
- *Registration expires* — remaining time until the registration expiration.

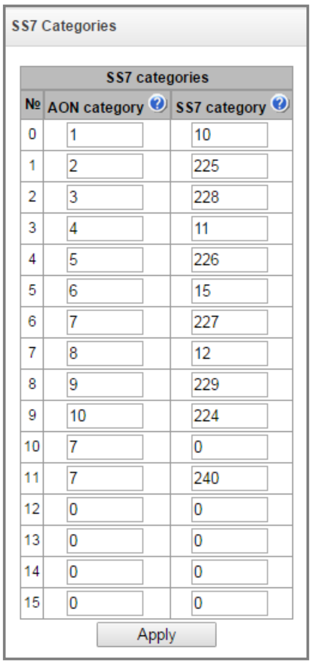
3.1.8 Internal resources

3.1.8.1 SS category

In this section, you may specify correspondence between Caller ID categories and SS7 protocol categories.

Generally accepted correspondence between SS7 categories and Caller ID categories is provided below.

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



SS7 Categories

SS7 categories		
№	AON category	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	0	0
13	0	0
14	0	0
15	0	0

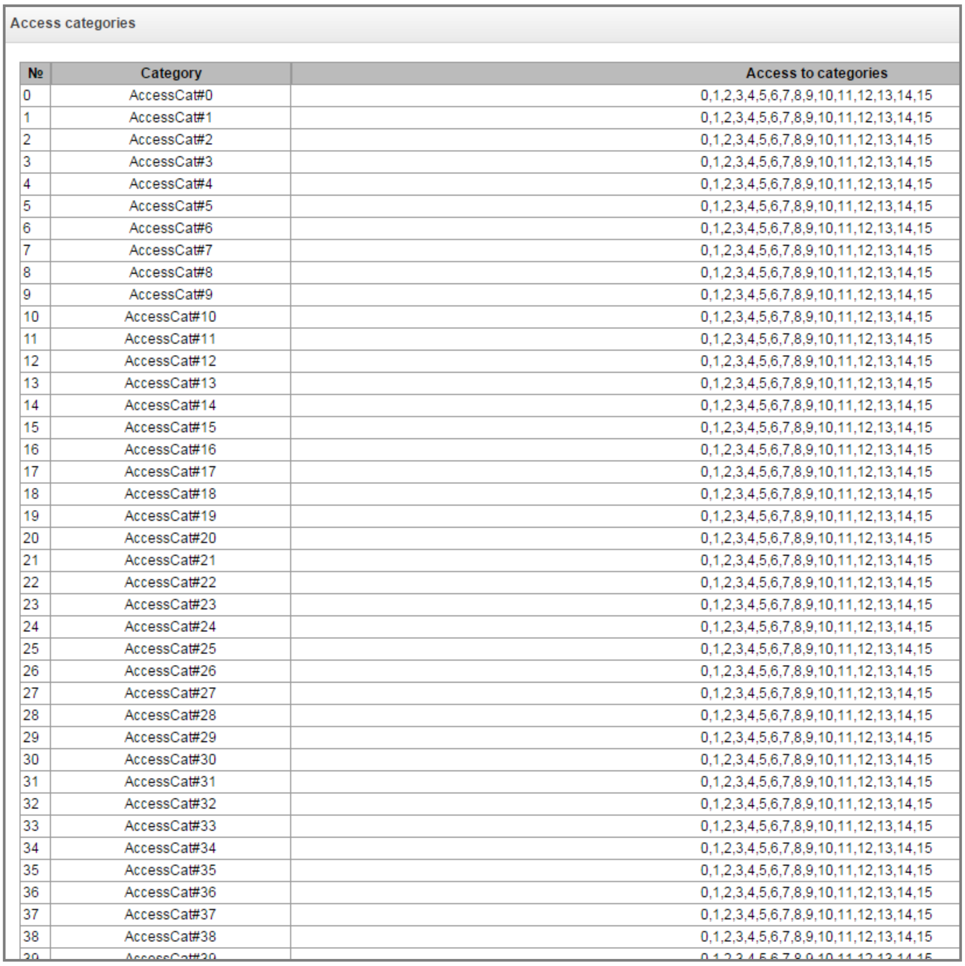
3.1.8.2 Access categories

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

To restrict an access to an object, you should assign the corresponding category; for other categories, specify accessibility to a category assigned to an object in this menu (deny access — deselect the checkbox next to the corresponding category, allow access — select the checkbox next to the corresponding category).

128 access categories are available for configuration in total. By default, access on each of them is defined for the first 16 categories.

To proceed to category configuration and editing, click ⚒ button.



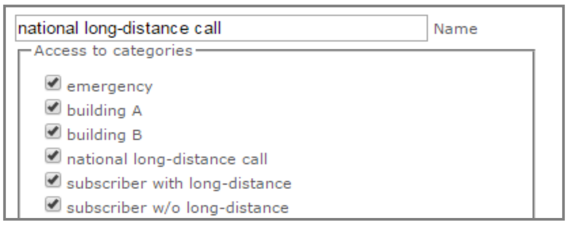
Access categories

№	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

Access restriction configuration example

To restrict the long-distance communication, you should:

1. Select an access category for the long-distance communication. Specify name 'National long-distance call' for convenience.

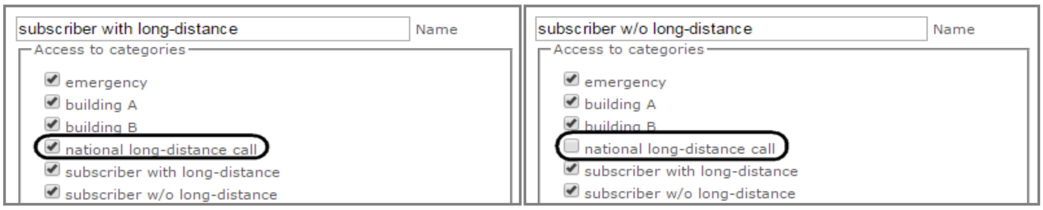


Name: national long-distance call

Access to categories

☑ emergency
☑ building A
☑ building B
☑ national long-distance call
☑ subscriber with long-distance
☑ subscriber w/o long-distance

2. Select 2 categories for subscribers: *«Subscriber with long-distance»* and *«Subscriber w/o long-distance»* and allow/deny an access to *'National long-distance call'* category respectively (select/deselect the checkbox next to *'National long-distance call'* category).



Name: subscriber with long-distance

Access to categories

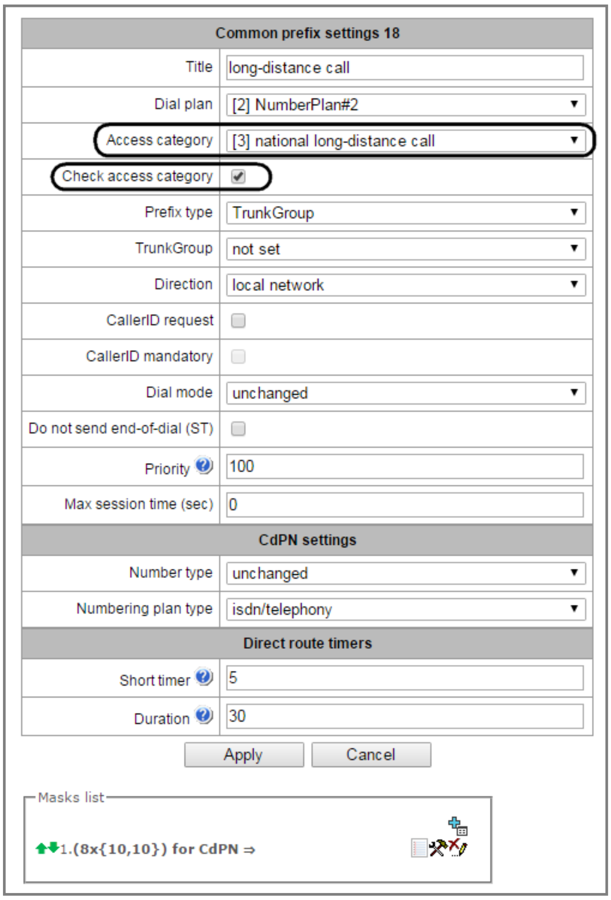
☑ emergency
☑ building A
☑ building B
☑ national long-distance call
☑ subscriber with long-distance
☑ subscriber w/o long-distance

Name: subscriber w/o long-distance

Access to categories

☑ emergency
☑ building A
☑ building B
☐ national long-distance call
☑ subscriber with long-distance
☑ subscriber w/o long-distance

3. For transition to 8 prefix, select *'National long-distance call'* category and *'Check access category'* checkbox.



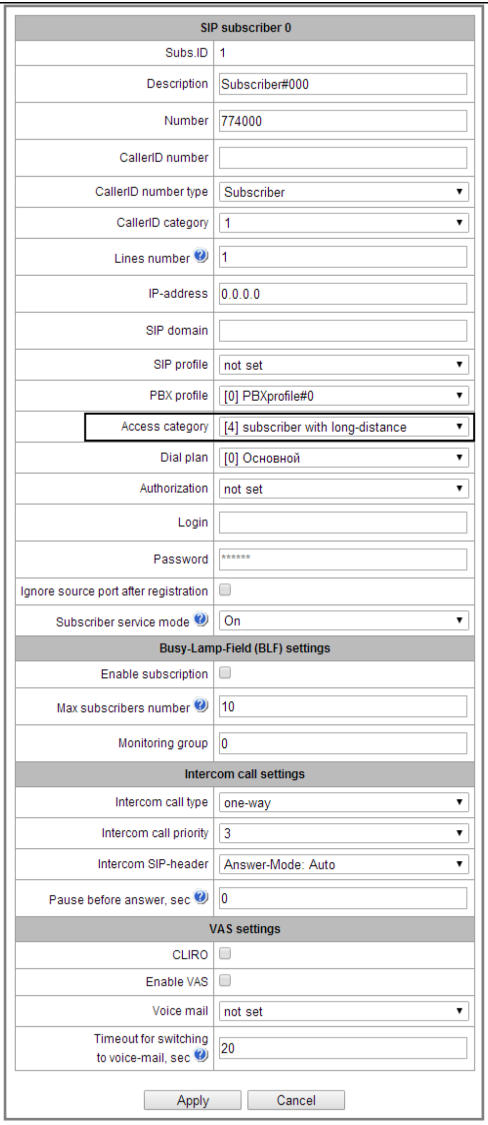
Common prefix settings 18	
Title	long-distance call
Dial plan	[2] NumberPlan#2
Access category	[3] national long-distance call
Check access category	☑
Prefix type	TrunkGroup
TrunkGroup	not set
Direction	local network
CallerID request	□
CallerID mandatory	□
Dial mode	unchanged
Do not send end-of-dial (ST)	□
Priority	100
Max session time (sec)	0
CdPN settings	
Number type	unchanged
Numbering plan type	isdn/telephony
Direct route timers	
Short timer	5
Duration	30

Masks list

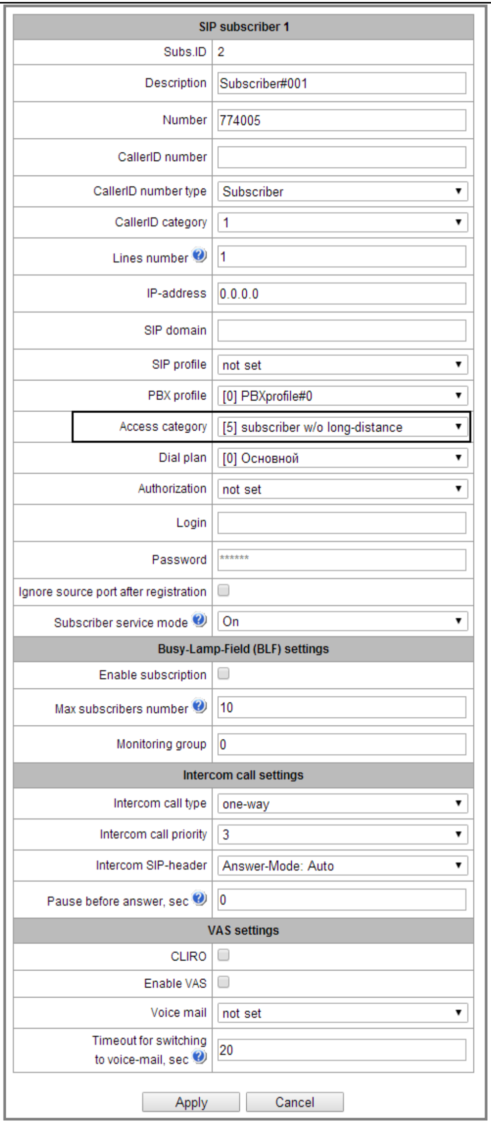
1.(8x{10,10}) for CdPN ⇒

4. Assign *«Subscriber with long-distance»* category to subscribers with enabled access to long-distance communication.

5. Assign *«Subscriber w/o long-distance»* category to subscribers with disabled access to long-distance communication.



SIP subscriber 0	
Subs.ID	1
Description	Subscriber#000
Number	774000
CallerID number	
CallerID number type	Subscriber
CallerID category	1
Lines number	1
IP-address	0.0.0.0
SIP domain	
SIP profile	not set
PBX profile	[0] PBXprofile#0
Access category	[4] subscriber with long-distance
Dial plan	[0] Основной
Authorization	not set
Login	
Password	******
Ignore source port after registration	☐
Subscriber service mode	On
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	☐
Voice mail	not set
Timeout for switching to voice-mail, sec	20



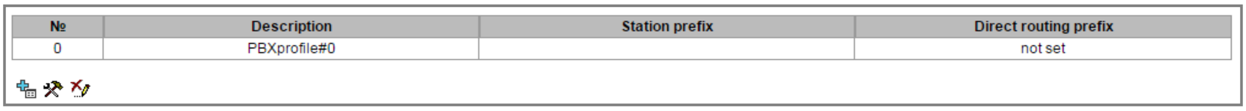
SIP subscriber 1	
Subs.ID	2
Description	Subscriber#001
Number	774005
CallerID number	
CallerID number type	Subscriber
CallerID category	1
Lines number	1
IP-address	0.0.0.0
SIP domain	
SIP profile	not set
PBX profile	[0] PBXprofile#0
Access category	[5] subscriber w/o long-distance
Dial plan	[0] Основной
Authorization	not set
Login	
Password	******
Ignore source port after registration	☐
Subscriber service mode	On
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	☐
Voice mail	not set
Timeout for switching to voice-mail, sec	20

Items 4 and 5 may be performed via subscriber group editing:

- **Select 'Selection' checkboxes next to the required subscribers.**
- **Click 'Edit selected' button.**
- **Select the required parameter for editing by selecting a checkbox next to it.**

3.1.8.3 PBX profiles

PBX profles allow for assignment of additional parameters to SIP subscribers.



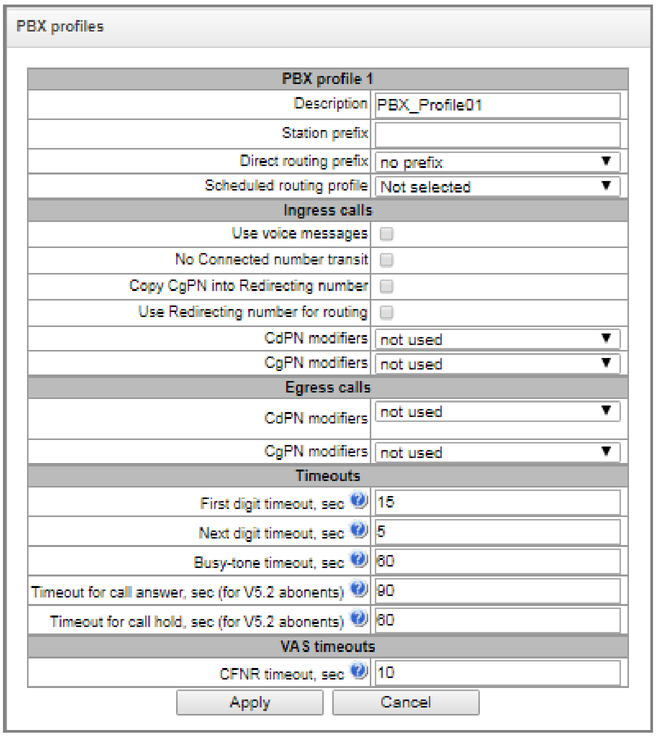
№	Description	Station prefix	Direct routing prefix
0	PBXprofile#0		not set

To create, edit or remove PBX profile, use 'Objects' — 'Add object', 'Objects' — 'Edit object' and 'Objects' — 'Remove object' menus and the following buttons:

— *'Add profile'*

— *'Edit profile parameters'*

— *'Remove profile'*



PBX profiles

PBX profile 1	
Description	PBX_Profile01
Station prefix	
Direct routing prefix	no prefix ▼
Scheduled routing profile	Not selected ▼
Ingress calls	
Use voice messages	☐
No Connected number transit	☐
Copy CgPN into Redirecting number	☐
Use Redirecting number for routing	☐
CdPN modifiers	not used ▼
CgPN modifiers	not used ▼
Egress calls	
CdPN modifiers	not used ▼
CgPN modifiers	not used ▼
Timeouts	
First digit timeout, sec	15
Next digit timeout, sec	5
Busy-tone timeout, sec	60
Timeout for call answer, sec (for V5.2 abonents)	90
Timeout for call hold, sec (for V5.2 abonents)	60
VAS timeouts	
CFNR timeout, sec	10

PBX profile:

- *Description* — name of the profile.
- *Station prefix* — prefix added into the beginning of the SIP subscriber number (CgPN).
- *Direct routing prefix* — transition to the prefix without caller or callee number analysis. It enables switching of all calls coming from SIP subscriber to a trunk group configured on the direct prefix regardless of the dialed number (without mask creation in prefixes).
- *Scheduled routing profile* — select 'scheduled routing' service profile, configured in the 'Internal resources' section.

Ingress calls:

- *Use voice messages* — when checked, pre-recorded voice messages stored in the device memory will be played upon the occurrence of specific events; for details, see Appendix I. Voice messages and music on hold (MOH).
- No Connected number transit — disable transmission of the Connected number field.
- *Copy CgPN в Redlirecting* – when checked, if there is no Redirecting number in an incoming call, it will be formed from CgPN number;
- *Use Redirection for routing* — when checked, the *'Redirecting number'* field will be used for SS7 or Q.931 signaling protocols, or SIP protocol *'diversion'* field for incoming call routing in the dial plan using CgPN number masks.
- *CdPN modifiers* — designed for modifications based on the analysis of the callee number received from the incoming channel.
- *CgPN modifiers* — designed for modifications based on the analysis of the caller number received from the incoming channel.

Egress calls:

- *CdPN modifiers* are dedicated for modifications based on callee number analysis before sending to an egress channel
- *CgPN modifiers* are dedicated for modifications based on caller number analysis before sending to an egress channel.

TImeouts:

- *First digit timeout, sec* — dialing timeout for the first digit of a number after the subscriber presses FLASH button during 'call transfer' service. When this timeout expires, busy tone will be played to a subscriber, range is from 5 to 20 seconds.
- *Next digit timeout, sec* — dialing timeout for the digit that follows the first digit of a number during 'call transfer' service. When this timeout expires, end of dial will be detected and the call will be routed, range is from 5 to 20 seconds.
- *Busy tone timeout, sec* — busy tone timeout for the unsuccessful dialing during 'call transfer' service. When this timeout expires, call will be switched to the subscriber being on hold.
- *Timeout for call answer, sec (for V5.2 abonents)* – timeout for answering a call, when it expires, the call will be released.
- *Timeout for call hold, sec (for V5.2 abonents)* – timeout for subscribers being on hold.

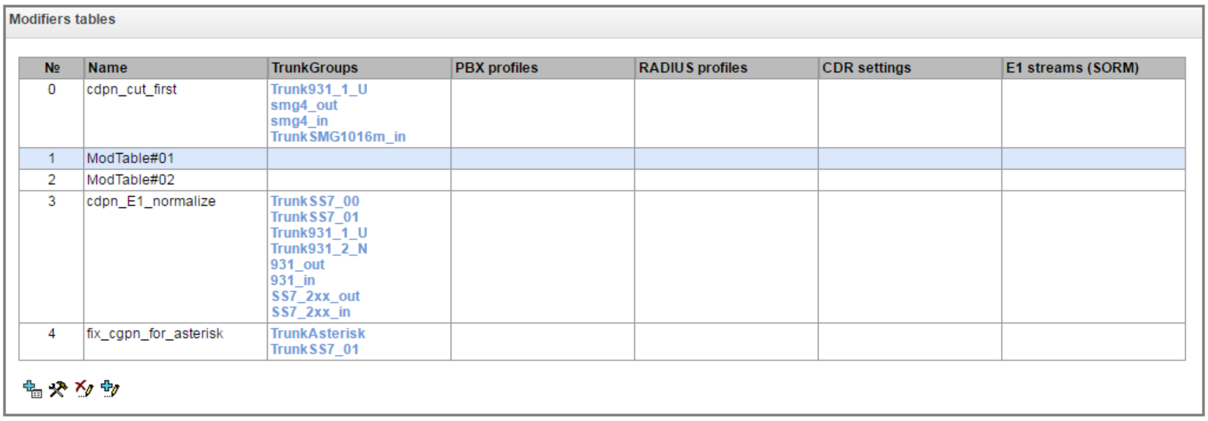
VAS timeouts:

- *CFNR timeout, sec* – when this timeout expires, the VAS "Call forward on no response" will be activated. The range is 5 – 60 seconds.

Flash mode (for V5.2 abonents):

- *Treats as on-hook* – the flash signal is taken as short hangup;
- *Flash1,2,3* – select flash signals parameters block. The block of paramneters is configured on AN.

3.1.8.4 Modifier tables

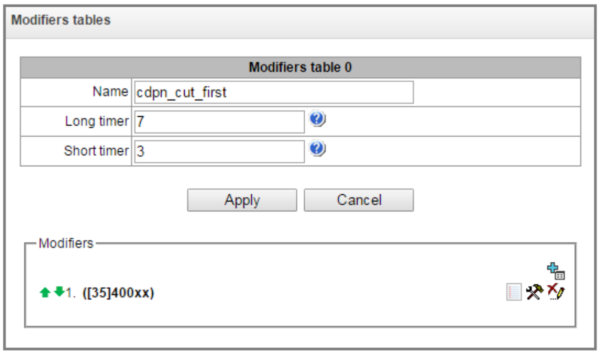


Modifiers tables

№	Name	TrunkGroups	PBX profiles	RADIUS profiles	CDR settings	E1 streams (SORM)
0	cdpn_cut_first	Trunk931_1_U smg4_out smg4_in TrunkSMG1016m_in				
1	ModTable#01					
2	ModTable#02					
3	cdpn_E1_normalize	TrunkSS7_00 TrunkSS7_01 Trunk931_1_U Trunk931_2_N 931_out 931_in SS7_2xx_out SS7_2xx_in				
4	fix_cgpn_for_asterisk	TrunkAsterisk TrunkSS7_01				

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

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



Modifiers tables

Modifiers table 0

Name	cdpn_cut_first
Long timer	7
Short timer	3

1. ([35]400xx)

— *'Add modifier'*

— *'Edit modifier parameters'*

— *'Remove modifier'*

— *'Add modifier by copying'*

Common settings of modifiers table:

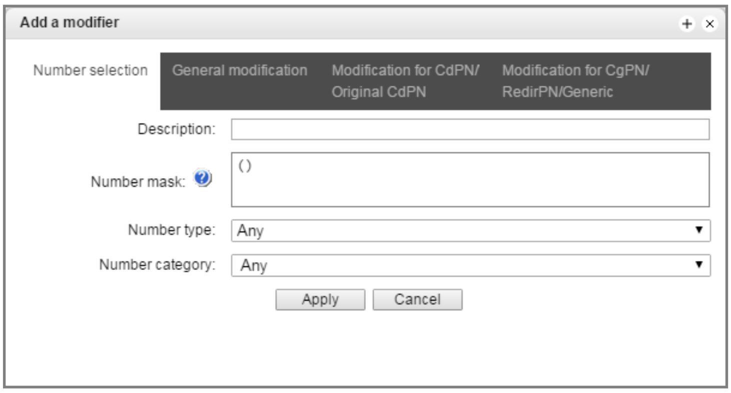
- *Name* – the displayed name of the table;
- *Long timer* – timeout for number dialing in overlap mode;
- *Short timer* – timeout for digit dialing in overlap mode;
- *Modifiers* – the list of modifiers used in the table.

To assign/edit parameters of created modifier, select the respective row and click ⚒.

To confirm changes of the modifier parameters, click *'Apply'* button; or click *'Cancel'* to exit without saving changes.

Click the link "Check number" below the modifiers table to check modifiers operation. The description of check procedure is presented in the section 3.1.8.4.4.2 Modifiers check.

3.1.8.4.1 Number selection tab



Add a modifier

Number selection
General modification
Modification for CdPN/ Original CdPN
Modification for CgPN/ RedirPN/Generic

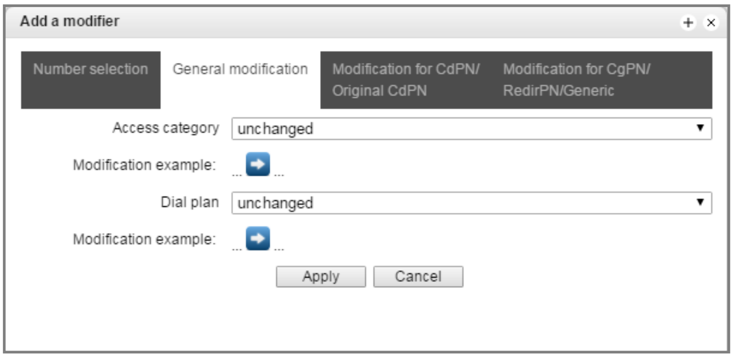
Description:	
Number mask:	()
Number type:	Any
Number category:	Any

- *Description* — modifier description.
- *Number mask* — template or set of templates that the subscriber number will be compared with (for mask syntax, see Section 3.1.6.21).
- *Number type* — subscriber number type:
  - *Subscriber* — subscriber number (SN) in E.164 format.
  - *National* — national number. Number format: NDC + SN, where NDC — national destination code.
  - *International* — international number. Number format: CC + NDC + SN, where CC — country code for geographic area.
  - *Network specific* — specific network number.
  - *Unknown* — unknown number type.

- *Any* — modification will be performed for any number type.
- *Unsupported* – a number type which is not supported on SMG .

- *Number category* — subscriber's Caller ID category.

3.1.8.4.2 General modification tab


Add a modifier
+ ×
Number selection
General modification
Modification for CdPN/ Original CdPN
Modification for CgPN/ RedirPN/Generic
Apply
Cancel

Access category: unchanged

Modification example: ... ...

Dial plan: unchanged

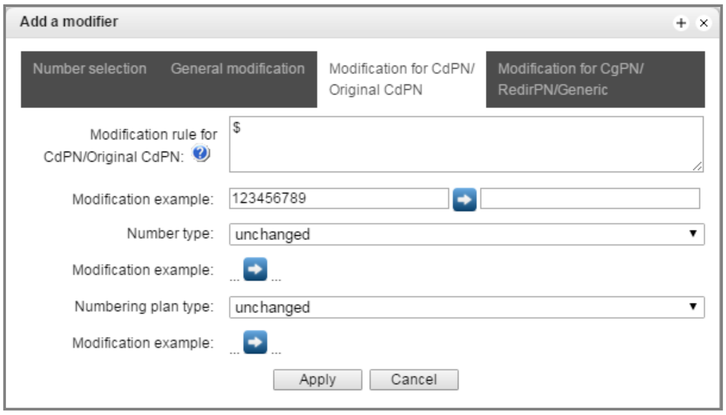
Modification example: ... ...

- *Modification example* — click ➡ button to view the modification summary after application of the modification rules specified.

- *Access category* — allows to modify the access category.

- *Dial plan* — allows to modify dial plan that will be used for further routing (necessary for dial plan negotiation).

3.1.8.4.3 CdPN/Original CdPN modification tab


Add a modifier
+ ×
Number selection
General modification
Modification for CdPN/ Original CdPN
Modification for CgPN/ RedirPN/Generic
Apply
Cancel

Modification rule for CdPN/Original CdPN: $

Modification example: 123456789

Number type: unchanged

Modification example: ... ...

Numbering plan type: unchanged

Modification example: ... ...

- *Modification rule for CdPN/Original CdPN* — callee number modification rule. For syntax being used, see Section 3.1.8.4.4.1; for example use, see Appendix C. This rule also applies to modification of the callee initial number (original Called party number) when this modifier table is selected in the 'trunk group' session for Original CdPN modification.

- *Modification example* — click ➡ button to view the modification summary after application of the specified modification rules. We recommend defining a number that will be subject to modification instead of number 123456789 entered in the rule check example.

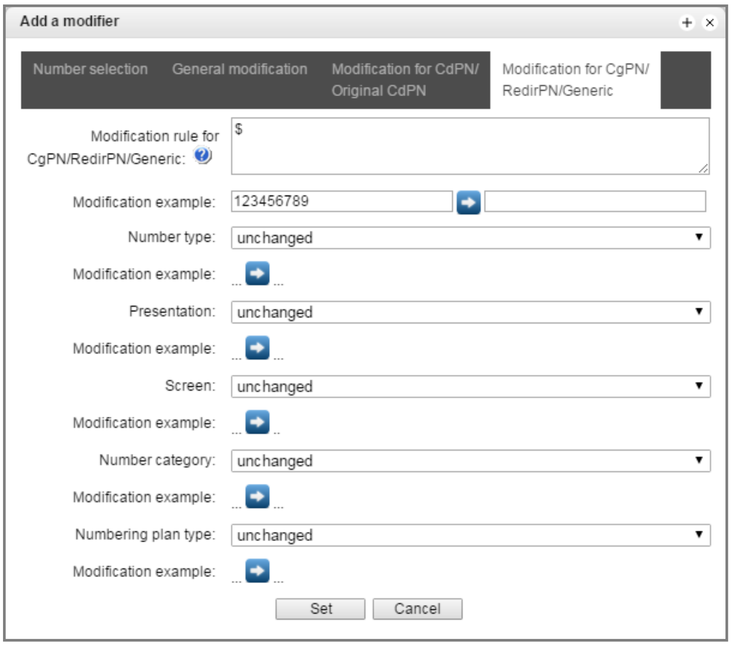
- *Number type* — callee number type modification rule.

  - *Unknown* – undefined number;
  - *Subscriber* – subscriber number (SN) in E.164 format;

- *National* – national number. The number has the following format: NDC + SN, where NDC – a geographic zone code;
- *International* – international number. The number has the following format: CC + NDC + SN, where CC is a country code;
- *Network specific* – specific network number;
- *Unchanged* – leave the type of a number unchanged.

- *Numbering plan type* — dial plan type modification rule.
  - Unchanged;
  - *Unknown* – unknown type of dial plan;
  - *Isdn/telephony* – a dial plan according to ITU-T E.164 recommendations;
  - *National* – national number. The number has the following format: NDC + SN, where NDC – a geographic zone code;
  - *Private* – a private dial plan.

3.1.8.4.4 CgPN/RedirPN/Generic/Location modification tab



Add a modifier

Number selection
General modification
Modification for CdPN/ Original CdPN
Modification for CgPN/ RedirPN/Generic
Set
Cancel

Modification rule for CgPN/RedirPN/Generic: $

Modification example: 123456789 ➡

Number type: unchanged

Modification example: ... ➡ ...

Presentation: unchanged

Modification example: ... ➡ ...

Screen: unchanged

Modification example: ... ➡ ...

Number category: unchanged

Modification example: ... ➡ ...

Numbering plan type: unchanged

Modification example: ... ➡ ...

- *Modification rule for CgPN/RedirPN/Generic* — callee number modification rule. For syntax being used, see Section 3.1.8.4.4.1; for example use, see Appendix C. This rule also applies to modification of the callee redirecting number when this modifier table is selected in the 'trunk group' session for Redir PN modification; for Generic Number modification, if the table is selected in GenericPN modification section; for Location Number modification, if the table is selected in LocationNumber modification section.

- *Modification example* — click ➡ button to view the modification summary after application of the modification rules specified. We recommend defining a number that will be subject to modification instead of number 123456789 entered in the rule check example.

- *Number type* — caller number type modification rule.

- *Presentation* — caller presentation modification rule.

- *Screen* — caller screen indicator modification rule.

- *Number category* — caller category modification rule.
- *Numbering plan type* — dial plan type modification rule:
  - unchanged;
  - *Unknown* – unknown type of dial plan;
  - *Isdn/telephony* – a dial plan according to ITU-T E.164 recommendations;
  - *National* – national number. The number has the following format: NDC + SN, where NDC – a geographic zone code;
  - *Private* – a private dial plan.

3.1.8.4.4.1 Modification rule syntax

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

- **'.'** and **'-'**: special characters indicating the removal of digits at the current position and the transposition of digits that follow to a location of that digit.
- **'X'**, **'x'**: special characters indicating that the digit remains unchanged at the current position (the digit is mandatory at the current position).
- **'?'**: special character indicating that the digit remains unchanged at the current position (the digit is arbitrary at the current position).
- **'+'**: special character indicating that all characters located between the current position and the next special character (or end of sequence) are inserted at the specified location of the number.
- **'!'**: special character indicating the breakdown finish, all other digits of a number are truncated.
- **'$'**: special character indicating the breakdown finish, all other digits of a number remain unchanged.
- **0-9, D, # and *** (**without preceding special character '+'**): informational characters that substitute the digit at the specified location of the number.

Modification example:

Add the city code 383 to the number 2220123
Modifier: **+383**
Result: **38322201234**

Replace country code with 7 in the number 83832220123
Modifier: **7**
Result: **738322201234**

Replace the third digit in the number 2220123 with 6
Modifier: **xx6$ or XX6$**
Result: **22601234**

Remove the prefix 99# in the number 99#2220123
Modifier: **---$**
Result: **2220123**

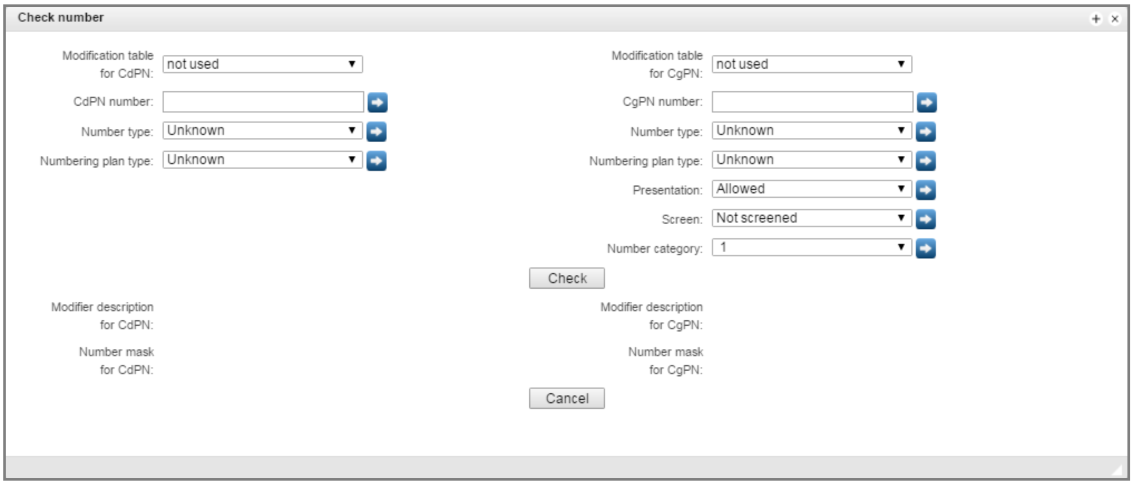
Remove the last 4 digits in the number 22201239876
Modifier: **$----**
Result: **2220123**

Select the first seven digits of the number 222012349876
Modifier: **xxxxxxx!**
Result: **2220123**

Remove the last two digits, replace the third digit with 6 and add the city code 383 to the number 222012398
Modifier: **+383xx6$--**
Result: **3832260123**

3.1.8.4.4.2 Modifiers check

You can check modifiers on a number with parameters specifying, using a «Check number» button below the table.



Check number

Modification table for CdPN:	not used	Modification table for CgPN:	not used
CdPN number:		CgPN number:	
Number type:	Unknown	Number type:	Unknown
Numbering plan type:	Unknown	Numbering plan type:	Unknown
		Presentation:	Allowed
		Screen:	Not screened
		Number category:	1
Modifier description for CdPN:		Modifier description for CgPN:	
Number mask for CdPN:		Number mask for CgPN:	

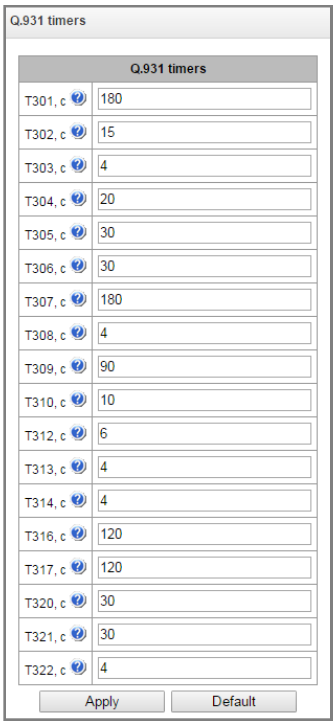
Set CdPN and CgPN numbers, fill «Number type», «Numbering plan type», «Presentation», «Screen», «Number category» fields, then choose needed modification table for CgPN and CdPN and click the «Check» button. The values which will be assigned to the number will be displayed next to the blue arrows. The numbers masks which were investigated and descriptions of modifiers which were included to the modifiers table will be displayed below.

3.1.8.5 Q.931 timers

In this section, you may configure third level timers required for Q.931 signaling protocol operation.

Timer names and default values are described in Q.931 ITU-T recommendation, Paragraph no. 9, List of system parameters.

Name	Default value, seconds	Range, seconds
T301	180	30 – 360
T302	15	10 – 25
T303	4	4 – 10
T304	20	20 -30
T305	30	30 – 40
T306	30	30 -40
T307	180	180 – 240
T308	4	4 – 10



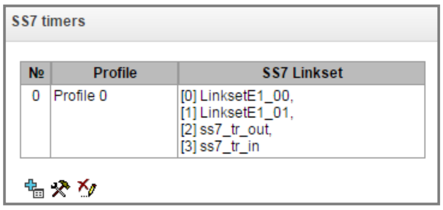
Q.931 timers

Q.931 timers	
T301, c	180
T302, c	15
T303, c	4
T304, c	20
T305, c	30
T306, c	30
T307, c	180
T308, c	4
T309, c	90
T310, c	10
T312, c	6
T313, c	4
T314, c	4
T316, c	120
T317, c	120
T320, c	30
T321, c	30
T322, c	4

T309	90	6 -90
T310	10	10 – 20
T312	6	6 -12
T313	4	4 – 10
T314	4	4 – 10
T316	120	120 – 240
T317	120	120 – 240 T316 or greater
T320	30	30 – 60
T321	30	30 – 60
T322	4	4 – 10

The timer values might be reset to values recommended in ITU-T Q.703, Q.704 and Q.764 by using the button "by default".

3.1.8.6 SS7 timers



SS7 timers

№	Profile	SS7 Linkset
0	Profile 0	[0] LinksetE1_00, [1] LinksetE1_01, [2] ss7_tr_out, [3] ss7_tr_in

In this section, you may configure MTP2, MTP3 and ISUP level timers of SS7 protocol.

To create, edit or remove a profile, use the following buttons:

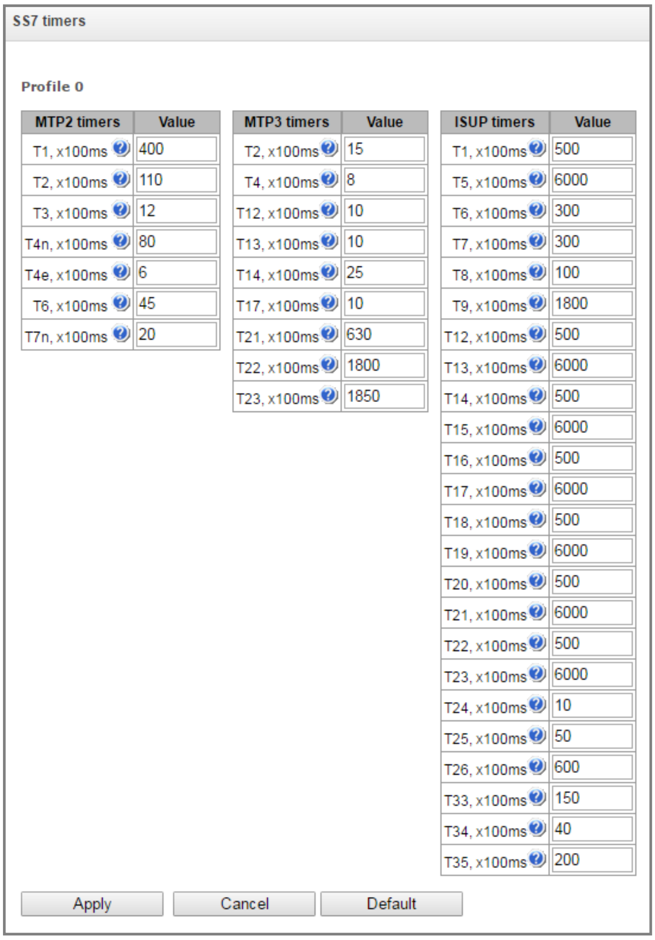
— '*Add profile*'

— '*Edit profile parameters*'

— '*Removeprofile*'

- *No.* — SS7 timer profile sequence number.
- *Profile* — profile name.
- *SS7 Linkset* — list of SS7 link sets that have this profile selected.

Profile settings:



SS7 timers

Profile 0

MTP2 timers	Value
T1, x100ms	400
T2, x100ms	110
T3, x100ms	12
T4n, x100ms	80
T4e, x100ms	6
T6, x100ms	45
T7n, x100ms	20

MTP3 timers	Value
T2, x100ms	15
T4, x100ms	8
T12, x100ms	10
T13, x100ms	10
T14, x100ms	25
T17, x100ms	10
T21, x100ms	630
T22, x100ms	1800
T23, x100ms	1850

ISUP timers	Value
T1, x100ms	500
T5, x100ms	6000
T6, x100ms	300
T7, x100ms	300
T8, x100ms	100
T9, x100ms	1800
T12, x100ms	500
T13, x100ms	6000
T14, x100ms	500
T15, x100ms	6000
T16, x100ms	500
T17, x100ms	6000
T18, x100ms	500
T19, x100ms	6000
T20, x100ms	500
T21, x100ms	6000
T22, x100ms	500
T23, x100ms	6000
T24, x100ms	10
T25, x100ms	50
T26, x100ms	600
T33, x100ms	150
T34, x100ms	40
T35, x100ms	200

Table 19 —MTP2 level timers names and default settings are described in Q.703 ITU-T recommendation, Paragraph 12.3, Timers.

Name	Default value, seconds	Range, seconds
T1	50	40 – 50
T2	50	5 – 150
T3	2	1 – 2
T4n	8.2	7.5 – 9.5
T4e	0.5	0.4 – 0.6
T6	6	3 – 6
T7n	2	0.5 – 2

Table 20 —MTP3 level timers names and default settings are described in Q.704 ITU-T recommendation, Paragraph 16.8, Timers and timer values.

Name	Default value, seconds	Range, seconds
T2	2	0.7 – 2
T4	1.2	0.5 – 1.2
T12	1.5	0.8 – 1.5
T13	1.5	0.8 – 1.5
T14	3	2 – 3
T17	1.5	0.8 – 1.5
T22	180	180 – 360
T23	180	180 – 360

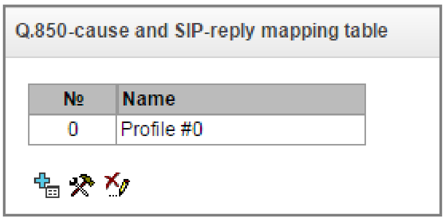
Table 21 —ISUP level timer name and default values are described in Q.764 ITU-T recommendation, Appendix A, Table A.1/Q.764 – Timers in the ISDN user part

Name	Default value, seconds	Range, seconds
T1	60	15 – 60
T5	900	150 – 900
T6	30	10 – 60
T7	30	20 – 30
T8	15	10 – 15
T9	180	30 – 240
T12	60	15 – 60
T13	900	150 – 900
T14	60	15 – 60
T15	900	150 – 900
T16	60	15 – 60
T17	900	150 – 900
T18	60	15 – 60
T19	900	150 – 900
T20	60	15 – 60
T21	900	150 – 900
T22	60	15 – 60
T23	900	150 – 900
T24	2	0 – 2
T25	10	1 – 10
T26	180	60 – 180
T33	15	12 – 15
T34	4	2 – 4
T35	20	15 – 20

3.1.8.7 Q.850-cause and SIP-reply code correspondence table

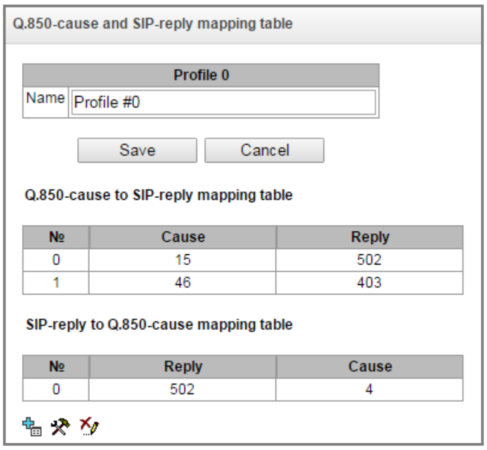
In this section, you may establish a correspondence between release causes described in Q.850 recommendations for SS7, PRI protocols and 4xx, 5xx, 6xx class SIP replies.

By default, the correspondence is used described in the Order no.10 dated 27.01.2009 issued by Ministry of Communications and Mass Media (MinComSvyaz) of the Russian Federation; for reasons not described in this Order, correspondence described in Q.1912.5 recommendation for SIP-I and RFC3398 for SIP/SIP-T is used.



Q.850-cause and SIP-reply mapping table

№	Name
0	Profile #0



Q.850-cause and SIP-reply mapping table

Profile 0	
Name	Profile #0

Q.850-cause to SIP-reply mapping table

№	Cause	Reply
0	15	502
1	46	403

SIP-reply to Q.850-cause mapping table

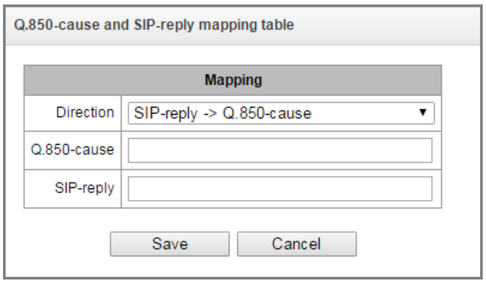
№	Reply	Cause
0	502	4

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

— *'Add rule'*
— *'Edit rule parameters'*
— *'Removerule'*

- Name — Q.850-cause and SIP-reply correspondence table name.

Profile settings:



Q.850-cause and SIP-reply mapping table

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

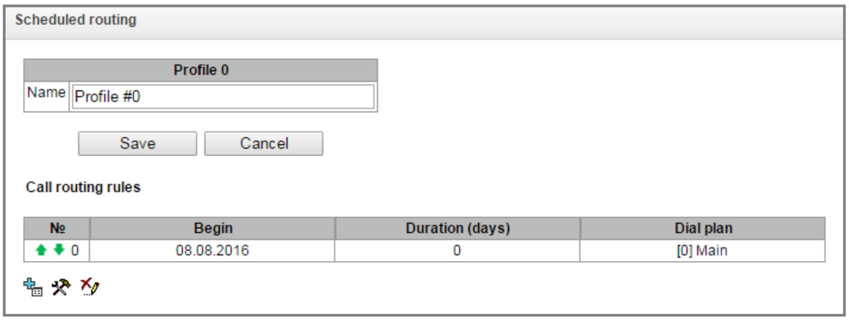
- Direction:
  - *SIP-reply -> Q.850-cause* — direction from SIP side to Q.850 side.
  - *Q.850-cause -> SIP-reply* — direction from Q.850 side to SIP side.

- *Q.850-cause* — Q.850 cause value.

- *SIP-reply* — 4xx, 5xx, 6xx class SIP reply value.

3.1.8.8 Scheduled routing

In this section, you may configure scheduled routing function that allows to use different dial plans depending on the time and day of the week.

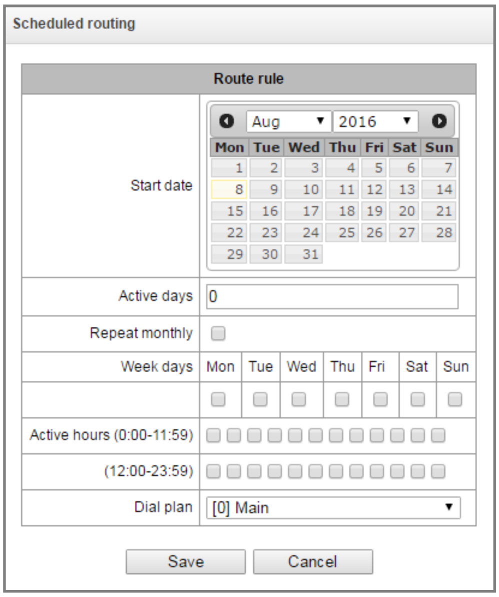


Scheduled routing

Profile 0	
Name	Profile #0

Call routing rules

№	Begin	Duration (days)	Dial plan
0	08.08.2016	0	[0] Main



Scheduled routing

Route rule

Start date: Aug ▼ 2016 ▼

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

Active days: 0

Repeat monthly: □

Week days	Mon	Tue	Wed	Thu	Fri	Sat	Sun
	□	□	□	□	□	□	□

Active hours (0:00-11:59) □ □ □ □ □ □ □ □ □ □ □ □

(12:00-23:59) □ □ □ □ □ □ □ □ □ □ □ □

Dial plan: [0] Main ▼

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

— *'Add rule'*
— *'Edit rule parameters'*
— *'Removerule'*

Routing rule:

- *Start date* — select start date for scheduled routing rule operation.

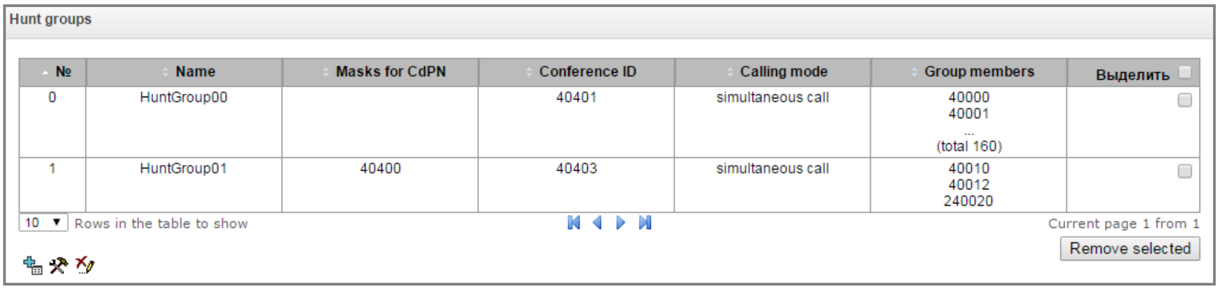
- *Active days* — scheduled routing rule operation duration.
- *Repeat monthly* — option that allows you to set the repetition of routing rule operation for each month.
- *Week days* — select days of the week for scheduled routing rule operation.
- *Active hours* — select hours for scheduled routing rule operation
- *Dial plan* — select dial plan that will be used during scheduled routing rule operation.

3.1.8.9 Hunt groups

Hunt group[1] — group of numbers used for call initialization by the device with different types of rings for these numbers when the call arrives to the call group prefix.

Call group allows you to establish a call center or office connection with simultaneous or successive ringing for employees from the same call group.

You can create up to 1,000 call groups in total.



Hunt groups

№	Name	Masks for CdPN	Conference ID	Calling mode	Group members	Выделить ☐
0	HuntGroup00		40401	simultaneous call	40000 40001 ... (total 160)	☐
1	HuntGroup01	40400	40403	simultaneous call	40010 40012 240020	☐

10 ▼ Rows in the table to show

Current page 1 from 1

Remove selected

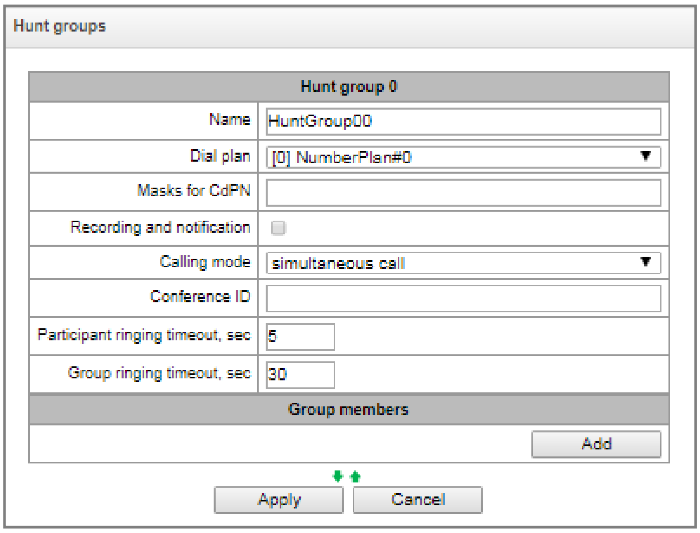
To create, edit or remove table records, use the following buttons:

— *'Add record'*

— *'Edit record parameters'*

— *'Remove record'*

The call group may contain numbers of device subscribers as well as the external numbers.



Hunt groups

Hunt group 0	
Name	HuntGroup00
Dial plan	[0] NumberPlan#0 ▼
Masks for CdPN	
Recording and notification	☐
Calling mode	simultaneous call ▼
Conference ID	
Participant ringing timeout, sec	5
Group ringing timeout, sec	30

Group members

- *Name* — call group name.
- *Dial plan* — select dial plan that the call group will belong to.
- *Masks for CdPN* — mask of the caller number that is used for the callee number comparison arrived to the dial plan designed for further call routing (for mask syntax, see Section 3.1.6.2).
- *Recording and notification* – a notification which were recorded by the iniator of the call will be played.

[1] The option is available for the devices with SMG-VAS license. Read more detailed information on licenses in the section 3.1.23 Licenses.

Operation algorithm:

- The initiator of notification makes a call to a group number;
- SMG answers to a call in 10 seconds and issues a tone signal 1400 Hz for a second, the recording is started;
- Initiator records the message and hangs up;
- In 3 seconds, SMG starts ringing members of the group. When they answer, the SMG plays the recorded notification.
- If a member of the group listened less than 1/3 of the message, the notification is considered to be unsuccessful and there will be one more attempt of notifying in 5 seconds.
- When there is a sequential notification, the next notification attempt will be performed in 3 seconds.
- If the member of the group does not answer before timeout expires, the next attempt will be performed after 60 seconds pause. There will be 5 attempts of notification.
- When there is a sequential notification, the members of the group who was not notified are put at the end of the call queue, and the SMG will ringing the next subscriber in a queue.

- *Calling mode* — call group member ringing method:

  - *simultaneous call* — simultaneous call for all call group members.
  - *sequential from first* — method that always dials the first number in the call group number list when a new call comes to this group; when S-timer expires, call addressed to the current group member will be cancelled and the call will be addressed to the next group member.
  - *sequential from next* — method that will enable ringing inside the group, beginning with the number that has ended the previous call to that call group. This method is necessary for load balancing between the group members; when S-timer expires, call addressed to the current group member will be cancelled and the call will be addressed to the next group member.
  - *sequential all from first* — method that always dials the first number in the call group number list when a new call comes to this group; when S-timer expires, call addressed to the current group member will not be cancelled and the call will be addressed to the next group member.
  - *sequential all from next* — method that will enable ringing inside the group, beginning with the number that has ended the previous call to that call group; this method is necessary for load balancing between the group members; when S-timer expires, call addressed to the current group member will not be cancelled and the call will be addressed to the next group member.
  - *serial search from first* — method that will discover the first available subscriber from the beginning of the list; only subscribers of this gateway can be members of this group.
  - *serial search from last* — method that will discover the first available subscriber from the end of the list; only subscribers of this gateway can be members of this group.

- *Conference ID* — number that when dialed after the service prefix VAS Conference all members of this group will be added to a conference call.

Choosing the option *«Recording and notification*»

- *Calling mode can have the following states:*

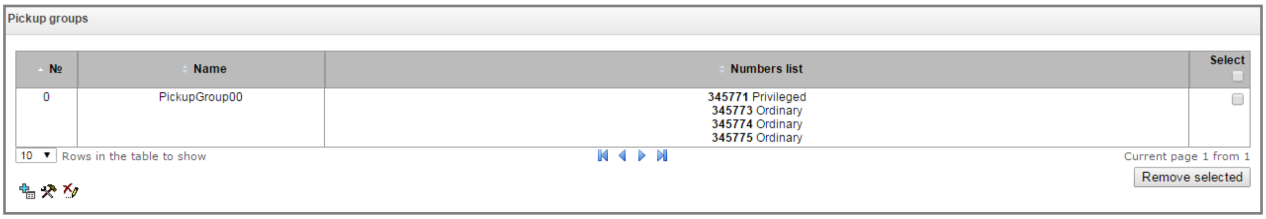
  - *recording and simultaneous notification* – after recording a notification, group members will be notified simultaneously;

– *recording and sequential notification* – after recording a notification, group members will be notified sequentially starting from the first in the group;

- *Participant ringing timeout, sec* — call timeout for a group member.
- *Maximum recording time, sec* – the setting is available when "Recording and notification" is activated. It sets the maximum duration of the message which can be recorded for the group.
- Group ringing timeout, sec - general call timeout for the whole call group.
- *Group members* — call group contents, up to 40 members on SMG-1016M and up to 160 members on SMG-2016. If the group is used for conference organization, the maximum group size reduces to 30 participant on SMG-1016M and 120 participants on SMG-2016.

3.1.8.10 Pickup groups

Pickup group[1] is a group of device subscribers. When a call comes to one of the pickup group subscribers, another group member can pick up this call by dialing an exit prefix for this call group.



Pickup groups

№	Name	Numbers list	Select ☐
0	PickupGroup00	345771 Privileged 345773 Ordinary 345774 Ordinary 345775 Ordinary	☐

10 ▾ Rows in the table to show

Current page 1 from 1

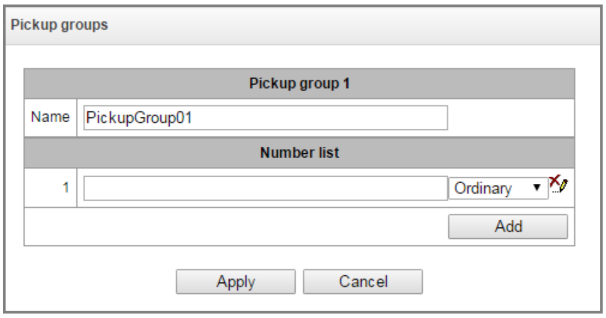
Remove selected

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

— *'Add record'*

— *'Edit record parameters'*

— *'Remove record'*



Pickup groups

Pickup group 1

Name: PickupGroup01

Number list

1 | | Ordinary ▾

Add

Apply | Cancel

Group can contain device subscribers only.

- *Name* — pickup group name.
- *Number list* — pickup group contents.

[1] The option is available for the devices with SMG-VAS license. Read more detailed information on licenses in the section 3.1.23 Licenses.

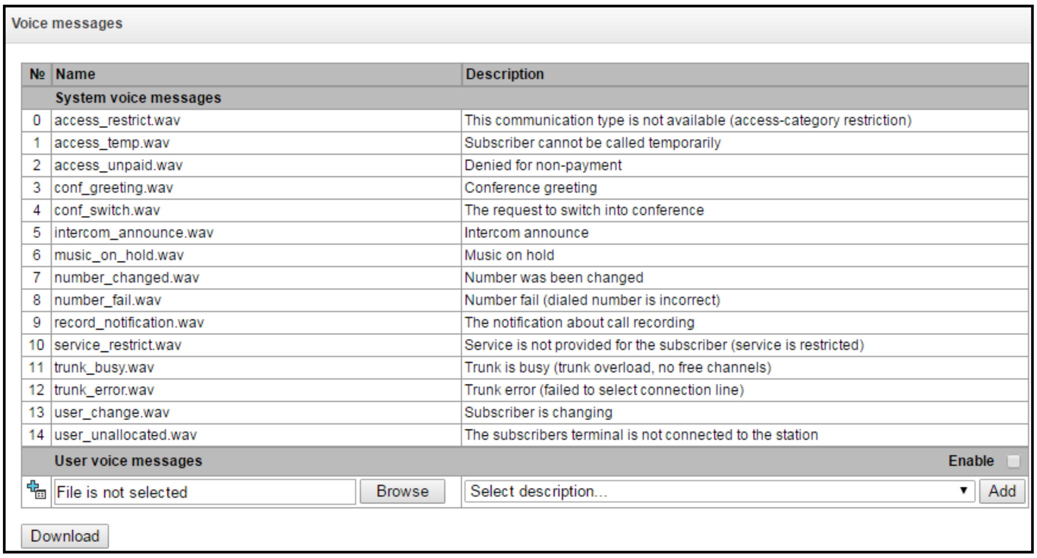
Pickup group member type

- *limited* — cannot perform the pickup, but the call directed to this member can be picked up by another group member.
- *common* — may pickup calls directed to common and limited members, but cannot pickup calls directed to privileged group member.
- *privileged* — may pickup calls directed at any pickup group member.

3.1.8.11 Voice messages

The device features 15 standard voice message phrases that are used for provisioning information to subscribers. In this section, you may upload custom voice message files.

File should be in WAV format compressed using codec G.711a, 8bit, 8KHz, mono. File size should not exceed 2Mb.



Voice messages

№	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 was been changed
8	number_fail.wav	Number fail (dialed number is incorrect)
9	record_notification.wav	The notification about call recording
10	service_restrict.wav	Service is not provided for the subscriber (service is restricted)
11	trunk_busy.wav	Trunk is busy (trunk overload, no free channels)
12	trunk_error.wav	Trunk error (failed to select connection line)
13	user_change.wav	Subscriber is changing
14	user_unallocated.wav	The subscribers terminal is not connected to the station
	User voice messages	Enable □
	File is not selected [Browse]	Select description... ▾ [Add]

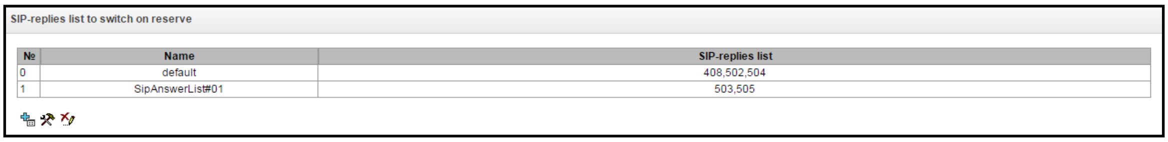
- *No.* — voice message file sequential number.
- *Name* — voice message file name.
- *Description* — voice message file description.

You may add your files to the voice messages list (by the "Add" button) and choose a description of an event (by the "Add" button). When the event is occured your file will be played.

- *Enable* — enable voice message file playback.

3.1.8.12 SIP replies list to switch on reserve

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

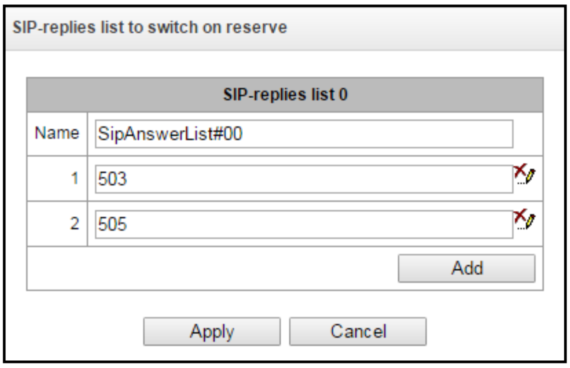


SIP-replies list to switch on reserve

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

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

- ➕ – *'Add reply list'*
- 🛠 – *'Edit reply list'*
- ❌ – *'Remove reply list'*



SIP-replies list to switch on reserve

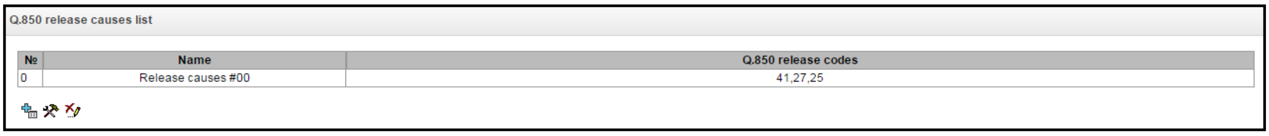
SIP-replies list 0	
Name	SipAnswerList#00
1	503 ❌
2	505 ❌
	Add

Apply Cancel

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

3.1.8.13 Q.850 release causes list

In this section, you may 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 the next trunk of the trunk direction.



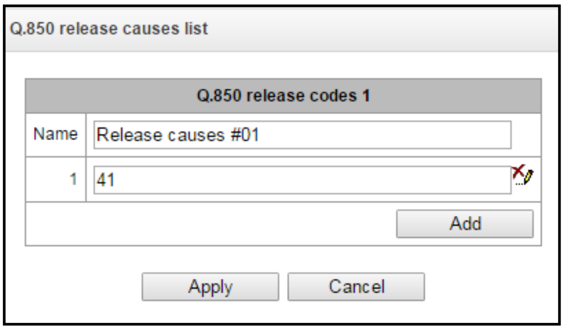
Q.850 release causes list

№	Name	Q.850 release codes
0	Release causes #00	41,27,25

➕ 🛠 ❌

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

- ➕ – *'Add reply list'*
- 🛠 – *'Edit reply list'*
- ❌ – *'Remove reply list'*



Q.850 release causes list

Q.850 release codes 1	
Name	Release causes #01
1	41 ❌
	Add

Apply Cancel

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

3.1.9 IVR

IVR *(Interactive Voice Response)* is a system of smart call routing based on the information entered by the client from the phone keypad using DTMF, current time and day of the week, caller and callee number, that enables voice notification of subscribers using voice files uploaded to the device. This function is necessary for call centers, taxi services, technical support, etc.

In this section, you may configure scenario and IVR audio lists and manage recorded conversation files.

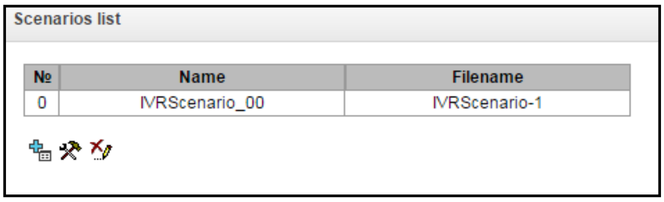
3.1.9.1 Scenarios list

In this section, you may create IVR[1] service operation scenarios.

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

— *'Add record'*
— *'Edit record parameters'*
— *'Remove record'*
– *«Download a scenario»* – download selected scenarios from the scenarios list to a user PC.

The table **'Scenarios list' —** this table contains all created IVR scenarios.



Scenarios list

№	Name	Filename
0	IVRScenario_00	IVRScenario-1

- *Name* — IVR scenario name.
- *File name* — select IVR scenario file from the list of files created on the device.

The table **'System settings'** contains 'Path to local disk drive for IVR scenarios storage' setting which defines storage for scenarios

The table **'File list'** — this table contains created IVR scenario files.

Click "Browse" in a dialog window to select a file and click "Upload" to add pre-saved IVR file.

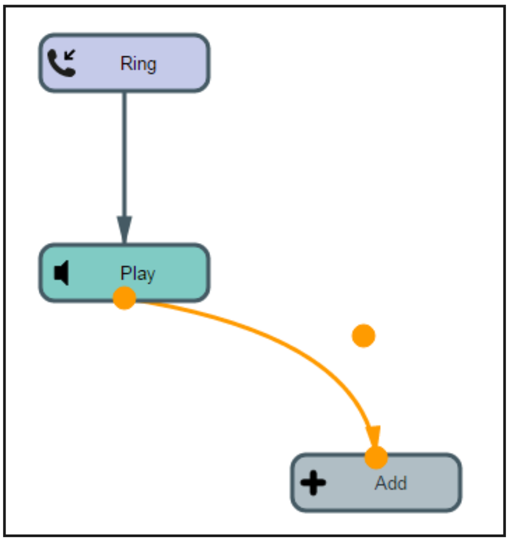
The table **'Typical scenarios list'** — this table contains all IVR common scenario files available for editing.

Scenario creation and editing menu provides a design view: in the central field, IVR scenario flowgraph is generated, 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 the block in the flowgraph, left-click it. Borders of the selected block will turn orange.

[1] The option is available for the devices with SMG-IVR license. Read more detailed information on licenses in the section 3.1.23 Licenses.

To add a block, select an empty block *'Add'* and select the required action from the collection of common blocks by left-clicking it. In the field on the right, configure parameters for created block. Logical connections for a newly created element will be added automatically. Logical connection for *'Goto'* block should be assigned manually; to do this, click *'Select block on the flowgraph'* button in the block parameters and select the required block. Logical connection *'Goto'* is represented by the dotted line.



When the selected block has been configured, click *'Save'* button to save changes in this unit or click *'Discard'* to discard them.

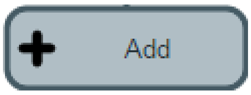
To remove the selected block from the flowgraph, click *'Remove block'* button.If this block has any lower-level logical connections, the whole branch of its child objects will be removed.

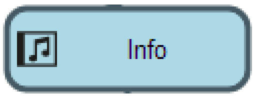
You may move blocks on the field; to do this, select the required block and move it to the desired place while holding left mouse button. At that, all logical connections will remain intact.

Also, you may left-click the logical connection between blocks, to change its type. Selected line will turn orange and three edit points will appear: for configuration of block exit location, block entry location and line curvature.

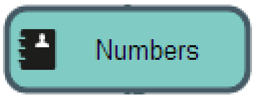
For IVR block description, see the table below.

Table 22 — IVR block description

Designation	***Name***	***Description***
	**Add**	Empty unit designed for block addition.
	Ring	Block that enables ringback tone playback for the subscriber; this block is always in the first position in the scenario list. When call arrives to RING block, call state remains unaffected. **Parameters** *Ringback playback duration, seconds* — select duration of the ringback tone playback or disable it. **Connections** *Entry* — beginning of the call to IVR. *Exit* — a single exit, incoming call parameter information is available on the block exit (number A, number B). **Features** Block does not affect the call state.

	**Info**	Block is required for playback of a single or multiple voice messages to the caller in the pre-answer state (w/o Subscriber B lifting the headset). I.e. connection fee is not incurred for this block playback. In scenario, this block may be placed after blocks that do not affect the call state and when there was no transition to an answer state. This block may be used for provisioning service information to the callee, until the resource that is able to process the call is freed. **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 3.1.8.11 Voice messages. To specify the drive for file storage, see Section 3.1.1 System **.** *Looped playback* — select the quantity of message playback loops; messages are played in order beginning from the first one. **Connections** *Entry* — incoming call in the pre-answer state. *Exit* — finish the playback of selected files. **Features** Info block may be preceded only by blocks that do not affect the call state (Ring, Info, Digitmap, Time, Goto).
	Play	Block is required for playback of a single or multiple voice messages to the caller in the conversation state (after the Subscriber B answers). Block is used for provisioning information to the 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 3.1.8.11Voice messages. To specify the drive for file storage, see Section 3.1.1System **.** *Looped playback* — select the quantity of message playback loops. Messages are played in order beginning from the first one. **Connections** *Entry* — incoming call in the pre-answer or conversation state. *Exit* — finish the playback of selected files.
	IVR	A block that is required for implementation of the interactive voice response function. This block features logical selection of the call path by pressing specific digit combinations, subscriber number extension dialing using internal

		dial plan and playback of audio files, system sounds (ringback tone, ringing tone, busy tone) and DTMF digits for subscriber notification. **Parameters** *Type* — type of audio file for playback. *File* — audio file uploaded to the device. For IVR audio list configuration, see Section 3.1.9.2 Tones list. *Tone* — select system sound for playback (DTMF digit, dialtone, busy, ringback). *Select subscriber* — configure logic for further call path. By pressing the configured combination of digits, the device identifies the IVR block outbound branch. If the subscriber does not press anything, 'No Match' branch will be selected. *Subscriber selection timeout, seconds* — additional number dialing timer; when this timer expires, IVR outbound branch will be selected. *Enable extension dialing* — when checked, extension dialing will be enabled followed by the device dial plan routing, e.g. internal subscriber number can be dialed. *Access category* — select access category. Access category allows you to define call barring for the number dialed by the subscriber in IVR block. *Quantity of digits for extension dialing* — maximum quantity of digits that can be dialed in the extension dialing. *Interdigit delay, seconds* — extension number interdigit delay value. **Connections** *Entry* – incoming call in the pre-answer state or active call phase. *Exit* — quantity of exits is configurable; extension dialing of a subscriber number may also be an exit. **Features** If the call is in the pre-answer state at the block entry, the block will automatically convert it into an active state (send an answer to the caller), and the further block logics will be executed.
	Dial	Block required for the specified number dialing, the number routing will be performed according to the device dial plan. **Parameters** *Number* — specified number. Dial plan: *Transit* – does not change a dial plan.

		Connections *Entry* — incoming call in the pre-answer state or active call phase. *Exit* — exit is not available, this is the end block of the scenario. **Features** Finishes scenario branch.
	Time	Block required for the selection of call path logic according to the current time and day of the week. **Parameters** *Time* — select time and day of the week template. Time is defined in 24h format. **Connections** *Entry* — incoming call in the pre-answer state or active call phase. *Exit* — block has 2 exits, the first one when time matches the defined template ('yes' exit), the second one when the match is not achieved ('no' exit). **Features** Block does not affect the call state.
	**Numbers**	Block required for the selection of call path logic according to the caller number. **Parameters** *Number* — caller number template. **Connections** *Entry* — incoming call in the pre-answer state or active call phase. *Exit* — block has 2 exits, the first one when caller number matches the defined template ('yes' exit), the second one when the match is not achieved ('no' exit). **Features** Block does not affect the call state.
	Digitmap	Block required for the selection of call path logic according to the callee number. Callee number is verified at the digitmap block entry phase. **Parameters** *Mask* — callee number mask.

		Connections *Entry* — incoming call in the pre-answer state or active call phase. *Exit* — block has 2 exits, the first one when callee number matches the defined template ('yes' exit), the second one when the match is not achieved ('no' exit). **Features** Block does not affect the call state.
	Goto	Block required for call transfer to another arbitrary scenario block. **Parameters** *Select block on the flowgraph* — click this button to select the block on the flowgraph to perform the transfer. *Maximum quantity of actuations* — select the quantity of passes for a call through this block to ensure the call looping protection. **Connections** *Entry* — incoming call in the pre-answer state or active call phase. *Exit* — a single exit to the block that the call is being transferred to. **Features** Block does not affect the call state.
	REC	Block required to begin the conversation recording; when the call logic passes through the block, subscriber conversation will be recorded into the file. **Connections** *Entry* — incoming call in the active call phase. *Exit* — block has a single exit. **Features** Block does not affect the call state. Conversation recording end only after the disconnection. To configure directory for IVR conversation recording file storage, go to Section 3.1.17.1 Call recording , 'IVR conversation recording folder name' parameter. For recording management, see Section **3.1.9.3 Call records**.

	Caller Info	Block allows to change the caller name that will be shown on the callee phone screen. Block allows to display caller name, organization and other data on the callee phone screen. **Parameters:** *Number mask* — caller number template. *Subscriber name* — new subscriber name. **Connections** *Entry* — incoming call in the pre-answer state or active call phase. *Exit* — block has a single exit. **Features** Block does not affect the call state.

When the scenario flowgraph has been created, specify its name and save by clicking *'Save scenario'* button. Click *'Back to list'* button to exit the design view without saving any changes.

3.1.9.2 Tones list

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

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

The table **'System settings'** contains 'Path to local disk drive for IVR sounds storage' which defines storage for conversation records from IVR.

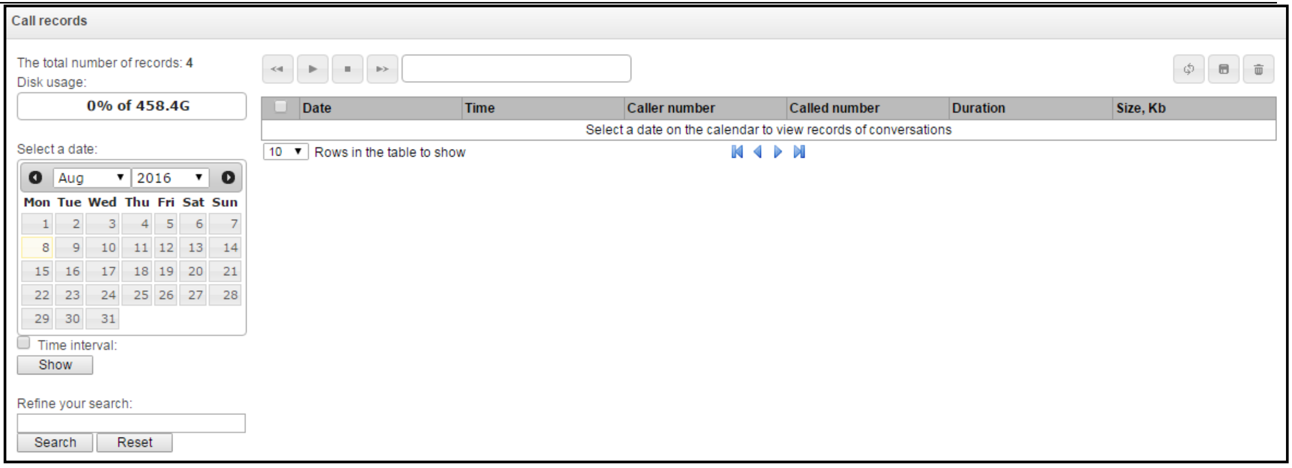
- *IVR sounds* — list of uploaded files.
- *Duration* — uploaded file length.
- *Browse* — select the audio file to be uploaded to the device.
- Upload — command to upload the selected file.

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

- *Play* — listen to the selected file.
- *Stop* — stop the file playback.
- *Delete* — delete the selected file.
- *Download* — download the selected file from the device.

3.1.9.3 Call records (IVR)

This section enables management of IVR conversation recording files. If there is **REC** block present in IVR scenario, all recorded conversations will be represented in a table.



Call records

The total number of records: 4

Disk usage:

0% of 458.4G

Select a date:

Aug 2016

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

□ Time interval:

Show

Refine your search:

Search Reset

□	Date	Time	Caller number	Called number	Duration	Size, Kb
Select a date on the calendar to view records of conversations						

10 Rows in the table to show

- *The total number of records* — total quantity of conversation recording files in the selected directory for conversation recordings.
- *Disk usage* — display used space on disk selected for conversation recording.
- *Select a date* — select a date to display the conversation recording files.
- *Time interval* — select time interval to display the conversation recording files.
- *Refine your search* — search for conversation recording files; search function uses any matches of the entered value to conversation recording file name.

For record control buttons description, see Table below.

Table 23 — Record control buttons

Button	Function
◂◂	previous record
▶	begin playback
■	stop playback
▸▸	next record
↻	repeat record playback
💾	save record
🗑	delete record

Call records table decsription:

- *Date/time* – date and time of the recording start;
- *Caller number/called number* – the number of the subscribers participating in the conversation;
- *DIal plan* – a dial plan in which the record is implemented;
- *Category* – conversation record category;
- *FTP* – shows whether the record was uploaded to FTP;
- *Duration* – conversation duration;
- *Size, KB* – the size of the record in kilobytes.

Conversation recording file format

1. A common call without call redirection 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 name, if it is missing, value 'none' will be used.
CdPN — callee number.

Example:
Subscriber 7111 calls Subscriber 7222, file name should be as follows:
2014-05-20_12-05-35_7111_7222.wav

2. A call that uses call redirection service:

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 name, if it is missing, value 'none' will be used.
RdNum — redirecting number — number with configured call redirection service.
cf — marker indicating that call forwarding has taken place.
CdPN — callee number — a number that the call is actually comes to.

Example:
Subscriber 7111 calls Subscriber 7222 that has configured a call redirection to 7333.

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

3. A call that uses call transfer service:

Call transfer service engages 3 subscribers — call initiating subscriber (Subscriber A), call transferring subscriber (Subscriber B) and transferred call recipient subscriber (Subscriber C).
For call transfer, 3 conversation recording files will be created.

- *Subscriber A* — Subscriber B conversation
- *Subscriber B* — Subscriber C conversation
- *Subscriber A* — Subscriber C conversation after the call transfer

Example:
Subscriber 7111 calls Subscriber 7222 that transfers the call to Subscriber 7333.

The following files will be created:

2014-05-20_12-05-35_7111_7222.wav — Subscriber A — Subscriber B conversation.

2014-05-20_12-06-36_7222_7333.wav — Subscriber B — Subscriber C conversation after the Subscriber B has put the Subscriber A on hold.

2014-05-20_12-05-35_7111_7222ct7333.wav — Subscriber A — Subscriber C conversation after the call transfer by Subscriber B; ct in the file name is a call transfer marker.

3.1.10 TCP/IP settings

In this section, you may configure the device network settings, IP packet routing rules.

- **DHCP** is a protocol that allows to automatically obtain IP address and other settings required for operation in TCP/IP network. Allows the gateway to obtain all necessary network settings from DHCP server.

- **SNMP** is a simple network management protocol. Allows the gateway to send real-time messages on occurred failures to controlling SNMP manager. Also, gateway SNMP agent supports monitoring of gateway sensors' status on request from SNMP manager.

- **DNS** is a protocol that allows to obtain domain information. Allows the gateway to obtain IP address of the communicating device by its network name (hostname). It may be necessary, e.g. when specifying hosts in the routing plan or using network name of the SIP server as its address.

- **TELNET** is a protocol that allows to establish mechanisms of control over the network. Allows you to remotely connect to the gateway from a computer for configuration and management purposes. For TELNET protocol operation, the data transfer process is not encrypted.

- **SSH** is a protocol that allows to establish mechanisms of control over the network. Unlike the TELNET, this protocol implies encryption of all data transferred through the network, including passwords.

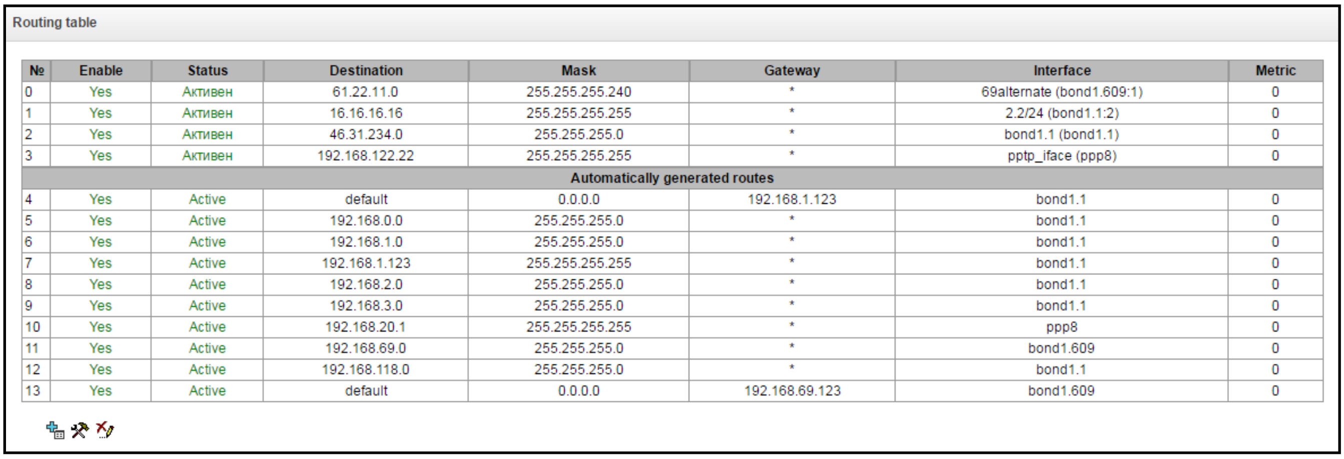
3.1.10.1 Routing table

In this submenu, you may configure static routes.

Static routing allows you to route packets to defined IP networks or IP addresses through the specified gateways. Packets sent to IP addresses not belonging to the gateway IP network and falling outside the scope of static routing rules will be sent to the default gateway.

Routing table is separated into 2 parts — manually configured routes that are displayed in the top part of the table and automatically created routes.

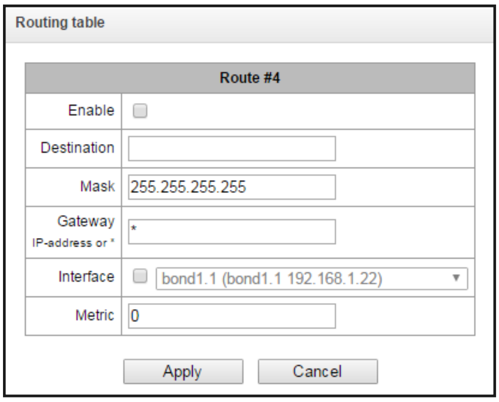
Automatically created routes cannot be changed as they are created automatically when the network and VPN/PPTP interfaces are established and required for their normal operation.



Routing table

№	Enable	Status	Destination	Mask	Gateway	Interface	Metric
0	Yes	Активен	61.22.11.0	255.255.255.240	*	69alternate (bond1.609:1)	0
1	Yes	Активен	16.16.16.16	255.255.255.255	*	2.2/24 (bond1.1:2)	0
2	Yes	Активен	46.31.234.0	255.255.255.0	*	bond1.1 (bond1.1)	0
3	Yes	Активен	192.168.122.22	255.255.255.255	*	pptp_iface (ppp8)	0
Automatically generated routes							
4	Yes	Active	default	0.0.0.0	192.168.1.123	bond1.1	0
5	Yes	Active	192.168.0.0	255.255.255.0	*	bond1.1	0
6	Yes	Active	192.168.1.0	255.255.255.0	*	bond1.1	0
7	Yes	Active	192.168.1.123	255.255.255.255	*	bond1.1	0
8	Yes	Active	192.168.2.0	255.255.255.0	*	bond1.1	0
9	Yes	Active	192.168.3.0	255.255.255.0	*	bond1.1	0
10	Yes	Active	192.168.20.1	255.255.255.255	*	ppp8	0
11	Yes	Active	192.168.69.0	255.255.255.0	*	bond1.609	0
12	Yes	Active	192.168.118.0	255.255.255.0	*	bond1.1	0
13	Yes	Active	default	0.0.0.0	192.168.69.123	bond1.609	0

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



Routing table

Route #4	
Enable	□
Destination	
Mask	255.255.255.255
Gateway IP-address or *	*
Interface	□ bond1.1 (bond1.1 192.168.1.22) ▼
Metric	0

— *'Add route'*

— *'Edit route parameters'*

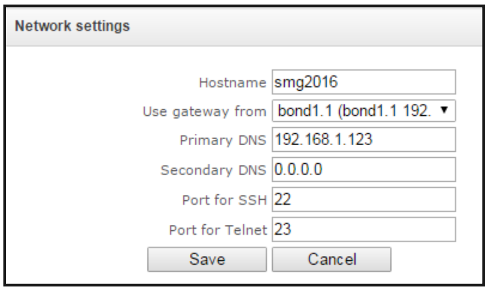
— *'Remove route'*

Route parameters:

- *Enable* — when checked, the route is enabled.
- *Destination* — IP network.
- *Mask* — specify a network mask for the defined IP network (use mask 255.255.255.255 for IP address).
- *Gateway* — define IP address of route gateway.
- *Interface* — select outbound network interface.
- *Metric* — route metrics.

3.1.10.2 Network Settings

In this submenu, you may specify the device name, change the network gateway address, DNS server address and SSH/Telnet access ports.

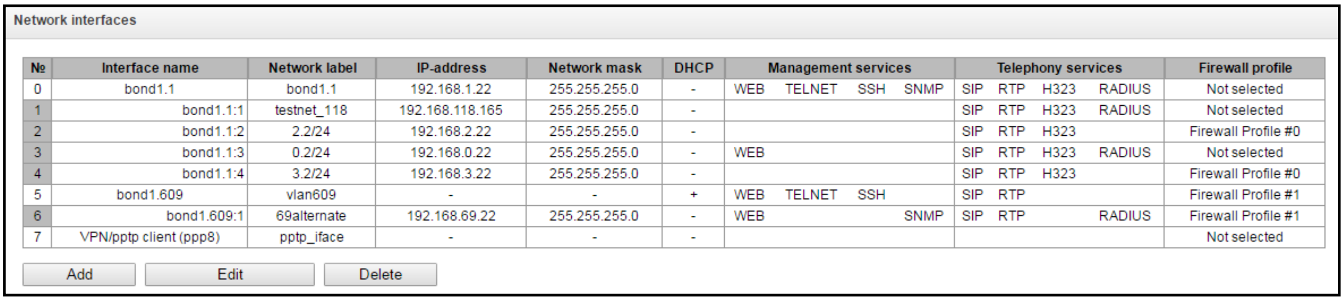


Network settings

Hostname	smg2016
Use gateway from	bond1.1 (bond1.1 192. ▼
Primary DNS	192.168.1.123
Secondary DNS	0.0.0.0
Port for SSH	22
Port for Telnet	23

- *Hostname* — device network name.
- *Use gateway from* — select network interface that the gateway will consider as a primary for the device.
- *Primary DNS* — primary DNS server.
- *Secondary DNS* — secondary DNS server.
- *Port for SSH* — TCP port for the device access via SSH protocol, default value is 22.
- *Port for Telnet* — TCP port for the device access via Telnet protocol, default value is 23.

3.1.10.3 Network interfaces



Network interfaces

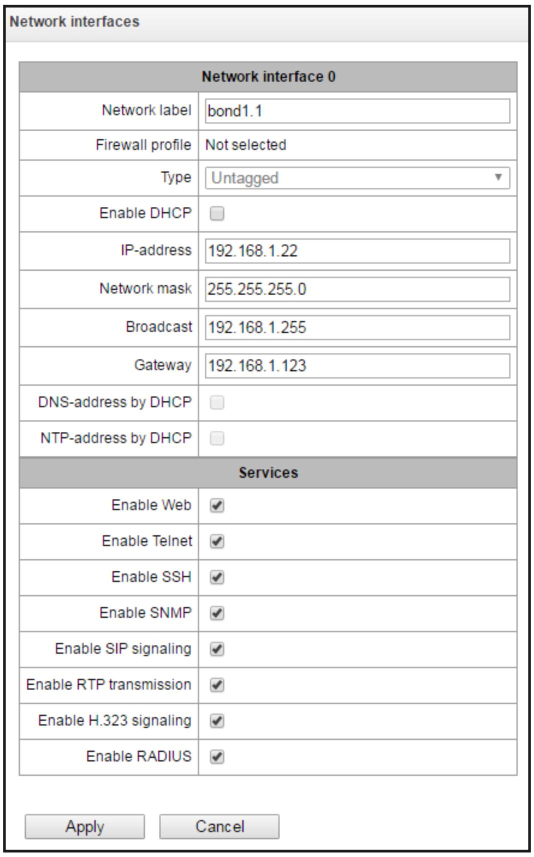
№	Interface name	Network label	IP-address	Network mask	DHCP	Management services	Telephony services	Firewall profile
0	bond1.1	bond1.1	192.168.1.22	255.255.255.0	-	WEB TELNET SSH SNMP	SIP RTP H323 RADIUS	Not selected
1	bond1.1:1	testnet_118	192.168.118.165	255.255.255.0	-		SIP RTP H323 RADIUS	Not selected
2	bond1.1:2	2.2/24	192.168.2.22	255.255.255.0	-		SIP RTP H323	Firewall Profile #0
3	bond1.1:3	0.2/24	192.168.0.22	255.255.255.0	-	WEB	SIP RTP H323 RADIUS	Not selected
4	bond1.1:4	3.2/24	192.168.3.22	255.255.255.0	-		SIP RTP H323	Firewall Profile #0
5	bond1.609	vlan609	-	-	+	WEB TELNET SSH	SIP RTP	Firewall Profile #1
6	bond1.609:1	69alternate	192.168.69.22	255.255.255.0	-	WEB SNMP	SIP RTP RADIUS	Firewall Profile #1
7	VPN/pptp client (ppp8)	pptp_iface	-	-	-			Not selected

The device allows you to configure 1 primary network interface eth0 and up to 9 additional interfaces; these interfaces may include VLAN interfaces as well as Aliases for primary interface eth0 or Aliases for VLAN interface.

Alias is an additional network interface based on the existing primary network interface eth0 or VLAN interface.

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

Add
Edit
Remove



Network interfaces

Network interface 0	
Network label	bond1.1
Firewall profile	Not selected
Type	Untagged ▾
Enable DHCP	□
IP-address	192.168.1.22
Network mask	255.255.255.0
Broadcast	192.168.1.255
Gateway	192.168.1.123
DNS-address by DHCP	□
NTP-address by DHCP	□
Services	
Enable Web	☑
Enable Telnet	☑
Enable SSH	☑
Enable SNMP	☑
Enable SIP signaling	☑
Enable RTP transmission	☑
Enable H.323 signaling	☑
Enable RADIUS	☑

Network interface settings:

Basic settings:

- *Network label* — network name.
- *Firewall profile* — show the selected firewall profile for the current interface.
- *Type* — interface type (always untagged for eth0 interface).
  - untagged – untagged interface (without VLAN);
  - tagged – tagged interface (with VLAN);
  - VPN/pptp client – client interface for VPN connection to a remote server via PPTP;
- *VLAN ID* — VLAN identifier (1–4095) (only for tagged type interfaces).
- *Enable DHCP* — obtain IP address dynamically from DHCP server (not supported for aliases).
- *IP address* — device network address.
- *Network mask* — device network address.
- *Broadcast* — address for broadcasting packets.
- *Gateway* — network gateway for the current interface (not supported for aliases).
- *DNS address by DHCP* — obtain DNS server IP address dynamically from DHCP server (not supported for aliases).
- *NTP address by DHCP* — obtain NTP server IP address dynamically from DHCP server (not supported for aliases).

Services — configuration menu for services that are enabled the current interface:

- *Enable Web* — enables access to configurator through the interface
- *Enable Telnet* — enables access via telnet protocol through the interface.
- *Enable SSH* — enables access via ssh protocol through the interface.
- *Enable SNMP* — enables SNMP utilization through the interface.
- *Enable SIP signaling* — enables SIP signaling information reception and transmission through the interface.

- *Enable RTP transmission* — enables RTP voice traffic reception and transmission through the interface.

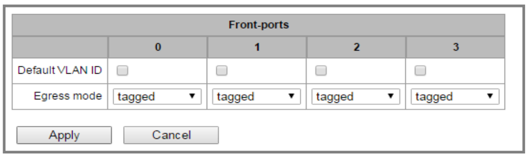
- *Enable H.323 signaling* — enables H.323 signaling information reception and transmission through the interface.

- *Enable RADIUS* — enables RADIUS protocol utilization through the interface.

If IP address or network mask has been changed or 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 when two minute timeout expires.

Front-ports[1] — external front port configuration

This setting is available for tagged VLAN interfaces only (*'Tagged'* value is defined in *'Type'* parameter).

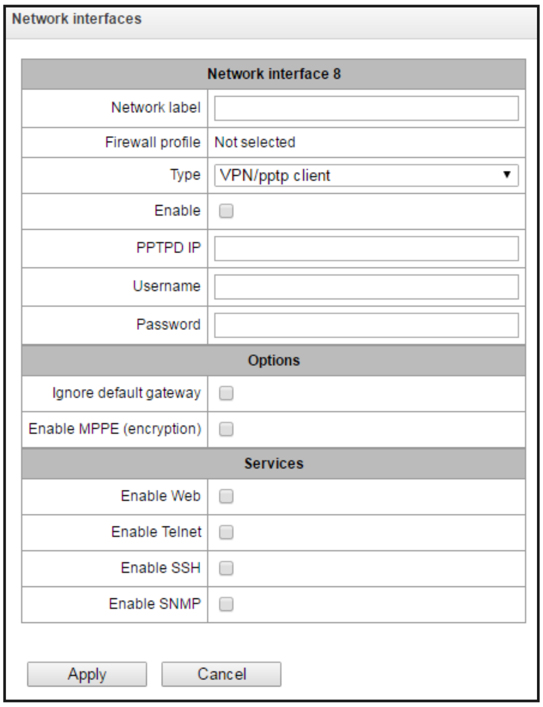


Front-ports				
	0	1	2	3
Default VLAN ID	☐	☐	☐	☐
Egress mode	tagged ▾	tagged ▾	tagged ▾	tagged ▾

- *Default VLAN ID* — when a packet without VLAN ID tag comes to the port, this packet will be tagged with VLAN ID tag of the selected network interface, if the packet is received with VLAN ID tag, this tag remains unchanged.

- *Egress mode* — VLAN tag operation rules during packet transfer from the port:
  - *tagged* — send packet with the selected interface VLAN ID.
  - *untagged* — send packet without VLAN ID.

VPN/PPP interface settings:



Network interfaces

Network interface 8	
Network label	
Firewall profile	Not selected
Type	VPN/pptp client ▾
Enable	☐
PPTPD IP	
Username	
Password	
Options	
Ignore default gateway	☐
Enable MPPE (encryption)	☐
Services	
Enable Web	☐
Enable Telnet	☐
Enable SSH	☐
Enable SNMP	☐

Basic settings:

- *Network label* — network name.

- *Firewall profile* — show the selected firewall profile for the current interface.

- *Type* — VPN/pptp client.

- *Enable* — enable VPN/PPP interface.

- *PPTPD IP* — PPTP server IP address.

- *Username* — username (login) used by the device for the network connection.

- *Password* — VPN connection password.

Options:

- *Ignore default gateway* — ignore the gateway setting in the *'Network parameters'* section.

[1] For SMG-2016 only

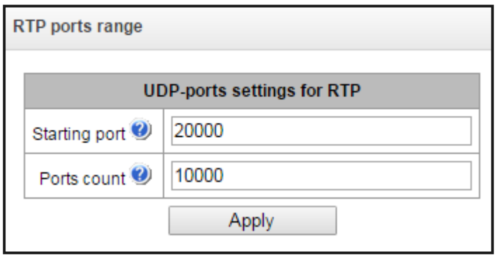
- Enable MPPE (encryption) — enable encryption.

Services — configuration menu for services enabled the current interface:

- *Enable Web* — enables access to configurator through the interface
- *Enable Telnet* — enables access via telnet protocol through the interface.
- *Enable SSH* — enables access via ssh protocol through the interface.
- *Enable SNMP* — enables SNMP utilization through the interface.

3.1.10.4 RTP ports range

In this section, you may configure UDP port range for voice RTP packets transmission.



RTP ports range

UDP-ports settings for RTP	
Starting port	20000
Ports count	10000

UDP port parameters:

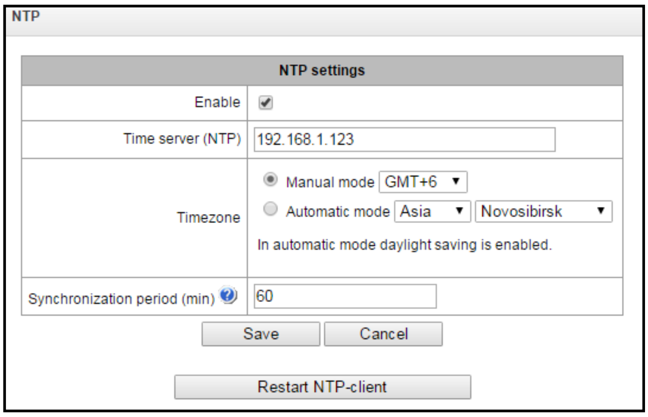
- *Starting port* — starting UPD port number used for voice traffic (RTP) and data transmission via T.38 protocol.
- *Ports count* — range (quantity) of UPD ports used for voice traffic (RTP) and data transmission via T.38 protocol.

To avoid conflicts, ports used for RTP and T.38 transmission should not overlap the ports used for SIP signaling (default port 5060).

3.1.11 Network services

3.1.11.1 NTP

NTP is a protocol designed for synchronization of real-time clock of the device. Allows to synchronize date and time used by the gateway against their reference values.



NTP

NTP settings	
Enable	☑
Time server (NTP)	192.168.1.123
Timezone	● Manual mode GMT+6 ○ Automatic mode Asia Novosibirsk In automatic mode daylight saving is enabled.
Synchronization period (min)	60

- *Enable* — enable time synchronization via NTP.
- *Time server (NTP)* — NTP server IP address or host name.

- *Timezone* — timezone and GMT (Greenwich Mean Time) offset configuration:

  – *Manual mode* — define GMT offset.
  – *Automatic mode* — in this mode, you may select the device location, GMT offset will be defined automatically, also this mode enables automatic daylight saving change.

- *Synchronization period, minutes* — time synchronization request transmission period.

- *Enable local NTP server* – activate a local NTP server for time synchronization with external devices. The option is available when "Enable" box is checked.

- *Network interface* – select a network interface through which the local NTP-server will answer on requests.

Use "Save" button to save the setting and "Cancel" to clear the settings. To perform forced time synchronization with the server, click *'Restart NTP client'* button (NTP client will be restarted).

3.1.11.2 SNMP settings

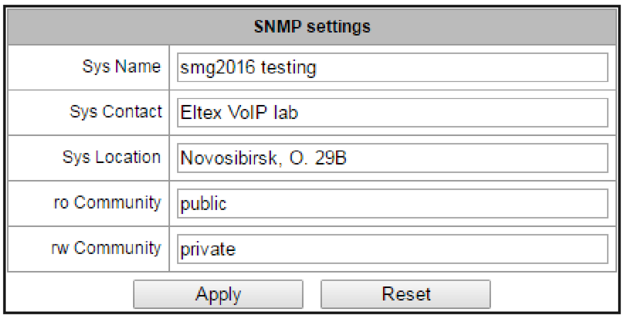
SMG software allows to monitor status of the device via SNMP. In SNMP submenu, you can configure settings of SNMP agent.

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

- Gateway name
- Device type
- Firmware version
- IP address
- E1 stream statistics
- IP submodule statistics
- Linkset state
- E1 stream channel state
- IP channel state (statistics for the current calls via IP)

Statistics for the current calls performed via IP channels contains the following data:

- Channel number
- Channel state
- Call identifier
- Caller MAC address
- Caller IP address
- Caller number
- Callee MAC address



SNMP settings

Sys Name	smg2016 testing
Sys Contact	Eltex VoIP lab
Sys Location	Novosibirsk, O. 29B
ro Community	public
rw Community	private

- Callee IP address
- Callee number
- Channel engagement duration

SNMP settings

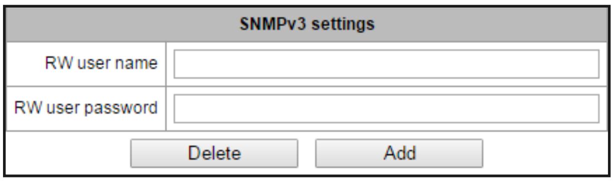
- *Sys Name* — device name.
- *Sys Contact* — contact information.
- *Sys Location* — device location.
- *ro Community* — parameter read password/community.
- *rw Community* — parameter write password/community.

Use "Apply" button to apply settings and "Reset" to cancel the settings.

3.1.11.3 SNMPv3

SNMPv3 configuration:
The system uses a single SNMPv3 user.

- RW User name — username.
- 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.

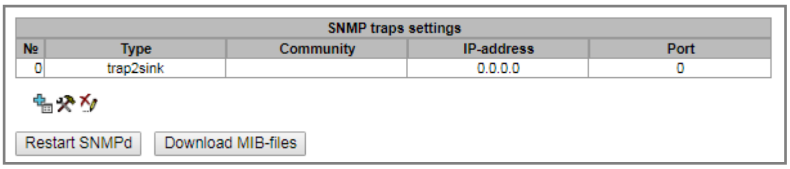
3.1.11.4 SNMP trap settings

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

SNMP agent sends SNMPv2-trap message, 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 stream fault
- Configuration error corrected

- SIP-T module normal operation restored after failure
- IP submodule normal operation restored after failure
- Linkset normal operation restored after failure
- SS7 signal channel normal operation restored after failure
- Synchronization from the higher priority source is restored
- No stream fault (after the failure or remote failure)
- FTP server is unavailable, utilization of RAM for CDR file storage exceeds 50% (15–30Mb)
- FTP server is unavailable, utilization of RAM for CDR file storage is below 50% (5–15Mb)
- FTP server is unavailable, utilization of RAM for CDR file storage is below 5Mb
- Software update or configuration file upload/download status



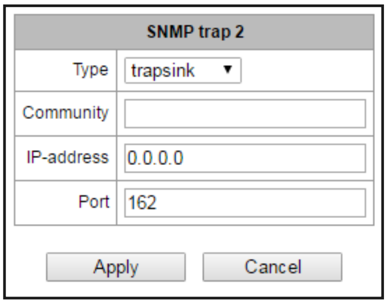
SNMP traps settings

№	Type	Community	IP-address	Port
0	trap2sink		0.0.0.0	0

- *Restart SNMPd* — click the 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'*



SNMP trap 2

Type	trapsink
Community	
IP-address	0.0.0.0
Port	162

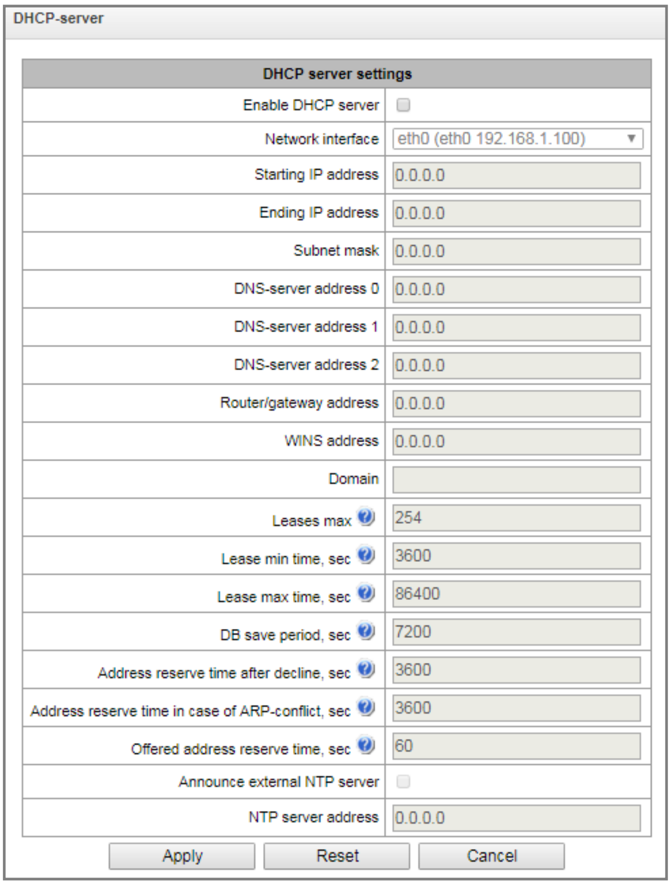
- *Type* — SNMP message type (TRAPv1, TRAPv2, INFORM).
- *Community* — password contained in traps.
- *IP address* — trap recipient IP address.
- *Port* — trap recipient UDP port (default port: 162).

3.1.11.5 DHCP server settings

Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to network devices automatically.

When the request is received, DHCP server selects the IP address from the address pool in its database and offers it to DHCP client. If the latter accepts the offer, network settings, i.e. IP address, mask and other parameters will be leased to the client for the limited term.

DHCP server parameters:



DHCP-server

DHCP server settings	
Enable DHCP server	☐
Network interface	eth0 (eth0 192.168.1.100)
Starting IP address	0.0.0.0
Ending IP address	0.0.0.0
Subnet mask	0.0.0.0
DNS-server address 0	0.0.0.0
DNS-server address 1	0.0.0.0
DNS-server address 2	0.0.0.0
Router/gateway address	0.0.0.0
WINS address	0.0.0.0
Domain	
Leases max	254
Lease min time, sec	3600
Lease max time, sec	86400
DB save period, sec	7200
Address reserve time after decline, sec	3600
Address reserve time in case of ARP-conflict, sec	3600
Offered address reserve time, sec	60
Announce external NTP server	☐
NTP server address	0.0.0.0

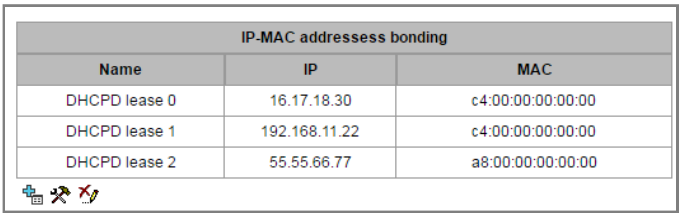
- Enable DHCP server — when checked, DHCP server will be started upon the gateway startup.
- Network interface — select DHCP server network interface.
- Starting IP address — starting address in the range of assigned IP addresses.
- Ending IP address — ending address in the range of assigned IP addresses.
- Subnet mask — network mask.
- DNS server 0/1/2 address — DNS server addresses from the operator's networks.
- Router/gateway address — default router or gateway address assigned by DHCP server to clients.
- WINS address — WINS server IP address in the operator's network.
- Domain — network domain name.
- Leases max, seconds — restrict the number of simultaneously leased addresses.
- Lease min time, seconds — set the minimum lease time for IP address assigned by DHCP server to the client, 10 seconds or more.
- Lease max time, seconds — set the maximum lease time for IP address assigned by DHCP server to the client, from 10 to 10,000,000 seconds.
- DB save period, seconds — time interval for saving information on leased addresses to dhcpd.leases file. Select 'off' to disable saving of the information on the leased addresses.

- Address reserve time after decline — time period that the IP address will remain reserved for the client upon the DHCP decline reception, 10 seconds or more.
- Address reserve time in case of ARP conflict, seconds — time period that the IP address will remain reserved for the client upon MAC address conflict identification, 10 seconds or more.
- Offered address reserve time, seconds — time period that the IP address requested by client will remain reserved, 10 seconds or more.
- Announce local NTP server – the option is available only if local NTP server is activated in "NTP" section and an interface is defined for the server. When DHCP option is activated, the server will announce the address of the set local NTP server via DHCP option 42.
- Announce external NTP server – when DHCP option is activated, the server will announce the address of the NTP servers defined in "NTP server address" via DHCP option 42;
- NTP server address – NTP server address, which SMG will announce via option 42 if "Announce external NTP server" is enabled.

DHCP server DB settings

- Start server — launch DHCP server.
- Stop server — stop DHCP server operation.
- Clear records — remove established IP-MAC associations from the DHCP server memory.

IP-MAC addresses bonding — assign static associations between IP addresses and MAC addresses.



IP-MAC addressess bonding

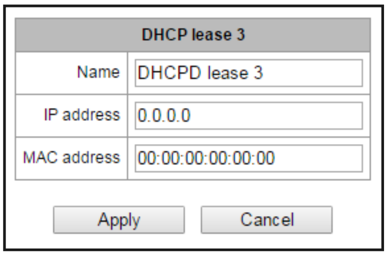
Name	IP	MAC
DHCPD lease 0	16.17.18.30	c4:00:00:00:00:00
DHCPD lease 1	192.168.11.22	c4:00:00:00:00:00
DHCPD lease 2	55.55.66.77	a8:00:00:00:00:00

To assign a new association, edit or remove parameters, use the following buttons:

— *'Add'*

— *'Edit'*

— *'Remove'*

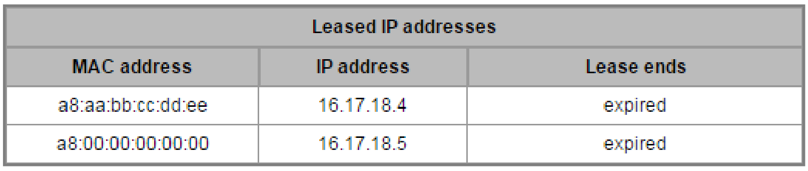


DHCP lease 3

Name	DHCPD lease 3
IP address	0.0.0.0
MAC address	00:00:00:00:00:00

- Name — name of the mapping
- IP address — client IP address
- MAC address — client MAC address

Leased IP addresses:



Leased IP addresses

MAC address	IP address	Lease ends
a8:aa:bb:cc:dd:ee	16.17.18.4	expired
a8:00:00:00:00:00	16.17.18.5	expired

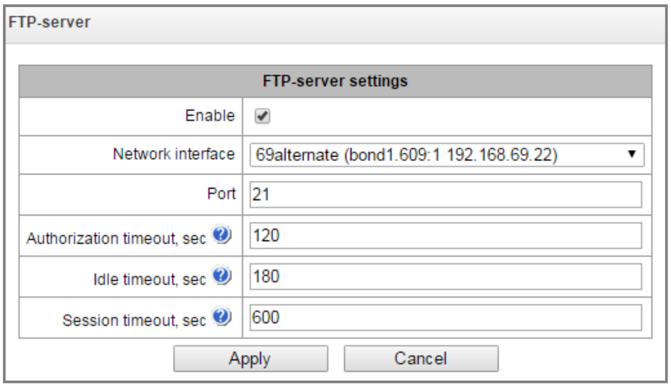
- MAC address — client MAC address
- IP address — address issued from the pool of IP addresses
- Expires In — remaining time of the address lease:
- Expired — address lease has expired

3.1.11.6 FTP server

In this section, you may configure an integrated FTP server used for provisioning FTP access to the following directories:

- cdr — directory containing CDR files.
- log — directory containing tracing files and other debug data.
- mnt — directory containing files located on external storage devices (SSD drives, SATA drives, USB flash drives).

FTP server settings



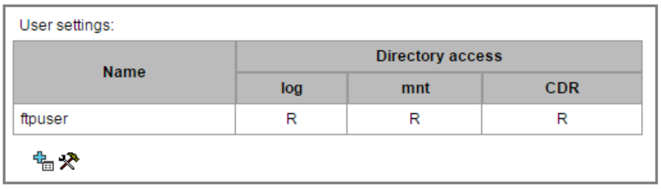
FTP-server

FTP-server settings	
Enable	☑
Network interface	69alternate (bond1.609:1 192.168.69.22) ▾
Port	21
Authorization timeout, sec	120
Idle timeout, sec	180
Session timeout, sec	600

- *Enable* — enable/disable integrated FTP server.
- *Network interface* — select network interface for the FTP server to run on.
- *Port* — select TCP port for the FTP server to run on.
- *Authorization timeout, seconds* — data entry timeout for subscriber authorization at FTP server; when this timeout expires, the server will forcedly terminate the connection.
- *Idle timeout, seconds* — timeout for the user to be idle at FTP server; when this timeout expires, the server will forcedly terminate the connection.
- Session timeout, seconds — session duration.

User settings:

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



User settings:

Name	Directory access		
	log	mnt	CDR
ftpuser	R	R	R

- *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* – access settings for /etc/config catalogue, read/record.

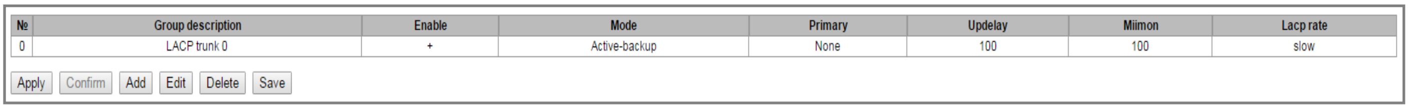
3.1.12 Switch[1]

In *'Switch'* menu, you may configure switch ports.

3.1.12.1 LACP settings

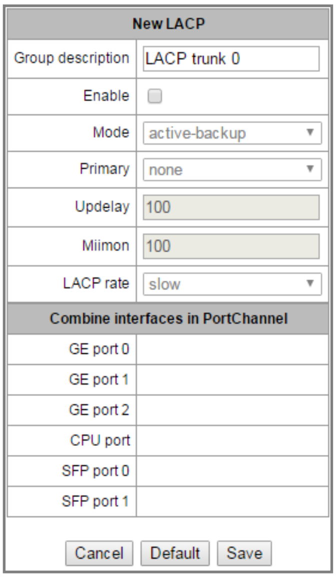
In this section, you may configure LACP groups.

Link Aggregation Control Protocol (LACP) is a protocol, designed for combining multiple physical channels into one logical channel.



№	Group description	Enable	Mode	Primary	Updelay	Miimon	Lacp rate
0	LACP trunk 0	+	Active-backup	None	100	100	slow

To create, edit or remove LACP groups, use the following buttons: *Add, Edit, Remove, Apply.*



New LACP	
Group description	LACP trunk 0
Enable	□
Mode	active-backup
Primary	none
Updelay	100
Miimon	100
LACP rate	slow
Combine interfaces in PortChannel	
GE port 0	
GE port 1	
GE port 2	
CPU port	
SFP port 0	
SFP port 1	

- Group description — LACP group name
- *Enable* — when checked, LACP will be enabled
- Mode — LACP operation mode:
  - *active-backup* — one interface operates in active mode, while others in standby mode. If an active interface goes out of service, the control will be transferred to one of the standby interfaces. This function doesn't have to be supported by the switch.
  - *balance-xor* — packet transfer is distributed between the aggregated interfaces by the following equation: ((source MAC address) XOR (recipient MAC addresses)) % number of interfaces. A certain interface operates with a specific recipient. This mode allows to balance the load and increase the robustness.

[1] For SMG-1016M only

  - *802.3ad* — dynamic port aggregation. This mode enables significant boost of the incoming and outgoing traffic bandwidth through utilization of every single aggregated interface. This function must be supported by the switch, and in some cases it requires an additional switch setting.

- *Primary* — primary interface configuration.
- *Updelay* — interface change time when the primary interface becomes unavailable.
- *Miimon* — MII monitoring time, frequency in milliseconds.
- *LACP rate* — time interval for transmission of LACPDU packets.
  - *fast* – 1 second transmission interval;
  - *slow* – 30 seconds transmission interval.
- Combine interfaces in PortChannel — list of ports added to LACP group.

3.1.12.2 Configuration of switch ports

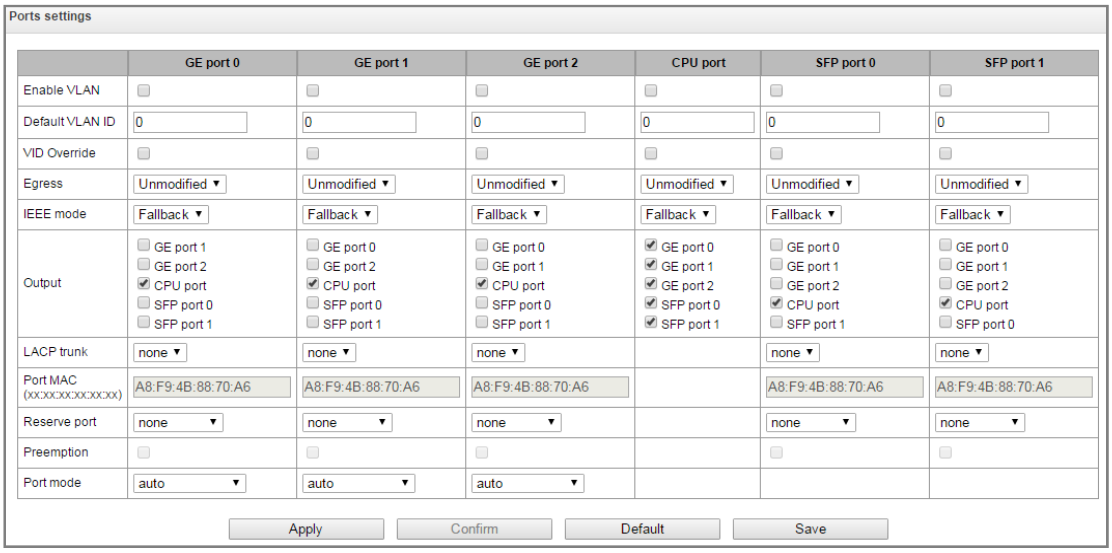
The switch can operate in four modes:

1. ***Without VLAN settings*** — to use this mode, *'Enable VLAN'* checkboxes should be deselected for all ports, *'IEEE Mode'* value should be set to *'Fallback'* for all ports, mutual availability of data ports should be set to *'Output'* with the respective checkboxes. *'802.1q'* routing table in *'802.1q'* tab should not contain any records.

2. ***Port based VLAN*** — to use this mode, *'IEEE Mode'* value should be set to *'Fallback'* for all ports, mutual availability of data ports should be set to *'Output'* with the respective checkboxes. For VLAN operation, use '*Enable VLAN', 'Default VLAN ID', 'Egress'* and *'Override'* settings. *'802.1q'* routing table in *'802.1q'* tab should not contain any records.

3. ***802.1q*** — to use this mode, *'IEEE Mode'* value should be set to '*Check*' or *'Secure'* for all ports*.* For VLAN operation, use *'Enable VLAN', 'Default VLAN ID',* and *'Override'* settings. Also, routing rules described in *'802.1q'* routing table in *'802.1q'* tab will apply.

4. ***802.1q + Port based VLAN.*** 802.1q mode may be used in combination with 'Port based VLAN'. In this case, *'IEEE Mode'* value should be set to *'Fallback'* for all ports, mutual availability of data ports should be set to *'Output'* with the respective checkboxes. For VLAN operation, use *'Enable VLAN', 'Default VLAN ID', 'Egress'* and *'Override'* settings. Also, routing rules described in *'802.1q'* routing table in *'802.1q'* tab will apply.



Ports settings

	GE port 0	GE port 1	GE port 2	CPU port	SFP port 0	SFP port 1
Enable VLAN	□	□	□	□	□	□
Default VLAN ID	0	0	0	0	0	0
VID Override	□	□	□	□	□	□
Egress	Unmodified ▾	Unmodified ▾	Unmodified ▾	Unmodified ▾	Unmodified ▾	Unmodified ▾
IEEE mode	Fallback ▾	Fallback ▾	Fallback ▾	Fallback ▾	Fallback ▾	Fallback ▾
Output	□ GE port 1 □ GE port 2 ☑ CPU port □ SFP port 0 □ SFP port 1	□ GE port 0 □ GE port 2 ☑ CPU port □ SFP port 0 □ SFP port 1	□ GE port 0 □ GE port 1 ☑ CPU port □ SFP port 0 □ SFP port 1	☑ GE port 0 ☑ GE port 1 ☑ GE port 2 ☑ SFP port 0 ☑ SFP port 1	□ GE port 0 □ GE port 1 □ GE port 2 ☑ CPU port □ SFP port 1	□ GE port 0 □ GE port 1 □ GE port 2 ☑ CPU port □ SFP port 0
LACP trunk	none ▾	none ▾	none ▾		none ▾	none ▾
Port MAC (xx:xx:xx:xx:xx:xx)	A8:F9:4B:88:70:A6	A8:F9:4B:88:70:A6	A8:F9:4B:88:70:A6		A8:F9:4B:88:70:A6	A8:F9:4B:88:70:A6
Reserve port	none ▾	none ▾	none ▾		none ▾	none ▾
Preemption	□	□	□		□	□
Port mode	auto ▾	auto ▾	auto ▾			

In factory configuration, switch ports may not access each other.

Device switch is equipped with 3x[1] or 4x[2] electrical Ethernet ports, 2x optical ports and 1x port for CPU interactions:

- *GE port* — electrical Ethernet ports of the device.
- *SFP port* — optical Ethernet ports of the device.
- *CPU* — internal port linked to the device CPU.

Switch Settings

- *Enable VLAN* — when checked, enable 'Default VLAN ID', 'Override' and 'Egress' settings for this port.
- *Default VLAN ID* — when an untagged packet is received at the port, this will be its VID; when a tagged packet is received at that port, its VID is considered to be specified in its VLAN tag.
- VID override — when checked, it is considered that any received packet has a VID, defined in *'default VLAN ID'* row. True for both untagged and tagged packets.
- Egress:
  - *unmodified* — packets will be sent by the port without any changes (i.e. as they came to another switch port).
  - *untagged* — packets will always be sent without VLAN tag by this port.
  - *tagged* — packets will always be sent with VLAN tag by this port.
  - *double tag* — each packet will be sent with two VLAN tags — if received packet was tagged and sent with one VLAN tag — if the received packet was untagged.
- IEEE mode - sets security mode for received tagged frames processing.

[1] For SMG-1016M
[2] For SMG-2016

- *fallback* — frame is received on ingress port regardless whether it has 802.1q tag in '802.1q' routing table or not.
  - If there is no 802.1q tag in '802.1q' routing table and the frame is allowed in 'output' section, the frame will be transmitted to the egress port.
  - Also, the frame will be transmitted to the egress port, if there is 802.1q tag in '802.1q' routing table, the egress port is a member of VLAN included in '802.1q' routing table and the frame is allowed in 'output' section.
- *check* — the frame will be received on ingress port, if its 802.1q tag is kept in '802.1q' routing table (the ingress port is not necessary to be a member of VLAN in '802.1q' routing table)
  - The frame will be transmitted to an egress port if the egress port is a member of VLAN in '802.1q' routing table and allowed in 'output' section of the ingress port settings.
- *secure* – the frame will be received on ingress port, if its 802.1q tag is kept in '802.1q' routing table and the ingress port is a member of VLAN in '802.1q' routing table.
  - The frame will be transmitted to an egress port if the egress port is a member of VLAN in '802.1q' routing table and allowed in 'output' section of the ingress port settings.

- *Output* — mutual availability of data ports. Defines privileges that allow packets received by this port to be transferred to flagged ports.
- *LACP trunk* – select LACP group to which the defined port will belong;
- *Port MAC* – change a MAC address of the port. The option is available when LACP group is selected on the port. Ports which are in the one LACP group should have different MAC addresses.
- *Reserve port* — select the port that will receive the traffic when abnormal situation occurs (i.e. line interruption). This setting is required for provisioning of Dual Homing redundancy.
- *Preemption* — when checked, return to master port when it becomes available.

This firmware version supports the global dual homing only.

- *Port mode* — select port operation mode (auto, 10/100 Mbps Half, 10/100 Mbps Full, 1 Gbps). Mode configuration is possible for electric Ethernet ports only (*GE port 0, GE port 1, GE port 2*).

Click 'Confirm' button in 1 minute interval to confirm settings, or the previous values will be restored.

To apply settings, click *'Apply'* button; to confirm applied settings, click *'Confirm'* button.

Click *'Defaults'* button to set default parameters. (The figure below shows default values.)

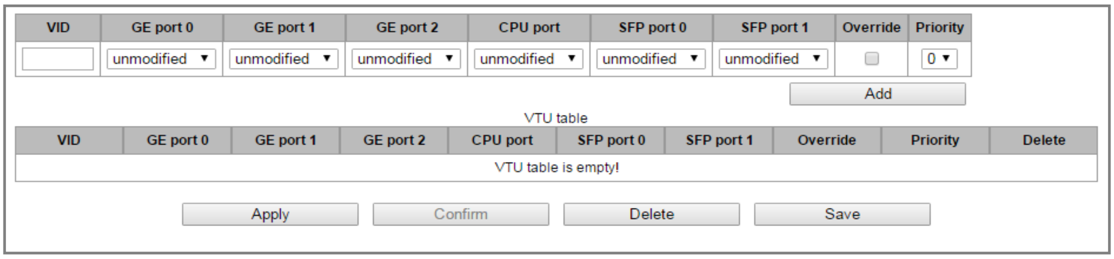
To save settings to the configuration file without applying them, click *'Save'* button.

3.1.12.3 802.1q

In *'802.1q'* submenu, you may define the configuration of packet routing rules for switch operation in 802.1q mode

Gateway switch is equipped with 3x electrical Ethernet ports, 2x optical ports and 1x port for CPU interactions:

- GE port 0, port 1, port 2 — electrical Ethernet ports of the device.
- SFP port 0, SFP port 1 — optical Ethernet port of the device.
- CPU — internal port linked to the device CPU.



VID	GE port 0	GE port 1	GE port 2	CPU port	SFP port 0	SFP port 1	Override	Priority
	unmodified ▼	unmodified ▼	unmodified ▼	unmodified ▼	unmodified ▼	unmodified ▼	□	0 ▼

VTU table

VID	GE port 0	GE port 1	GE port 2	CPU port	SFP port 0	SFP port 1	Override	Priority	Delete
VTU table is empty!									

Adding records to the packet routing table

In 'VID' field, enter an identifier of VLAN group, that the routing rule is created for, and assign actions for each port to be performed during transfer of packets with specified VID.

- *unmodified* — packets will be sent by the port without any changes (i.e. as they have been received).
- *untagged* — packets will always be sent without VLAN tag by this port.
- *tagged* — packets will always be sent with VLAN tag by this port.
- *not member* — packets with specified VID will not be sent by this port, i.e. the port is not the member of VLAN.

- *override* — when checked, override 802.1p priority for this VLAN; otherwise, leave the priority unchanged.
- *priority* — 802.1p priority assigned to packets in this VLAN, if *'override'* checkbox is selected.

Then, click *'Add'* button.

Click "Apply" button to apply the settings than click "Confirm" to confirm the settings.

Click 'Confirm' button in 1 minute interval to confirm settings, or the previous values will be restored.

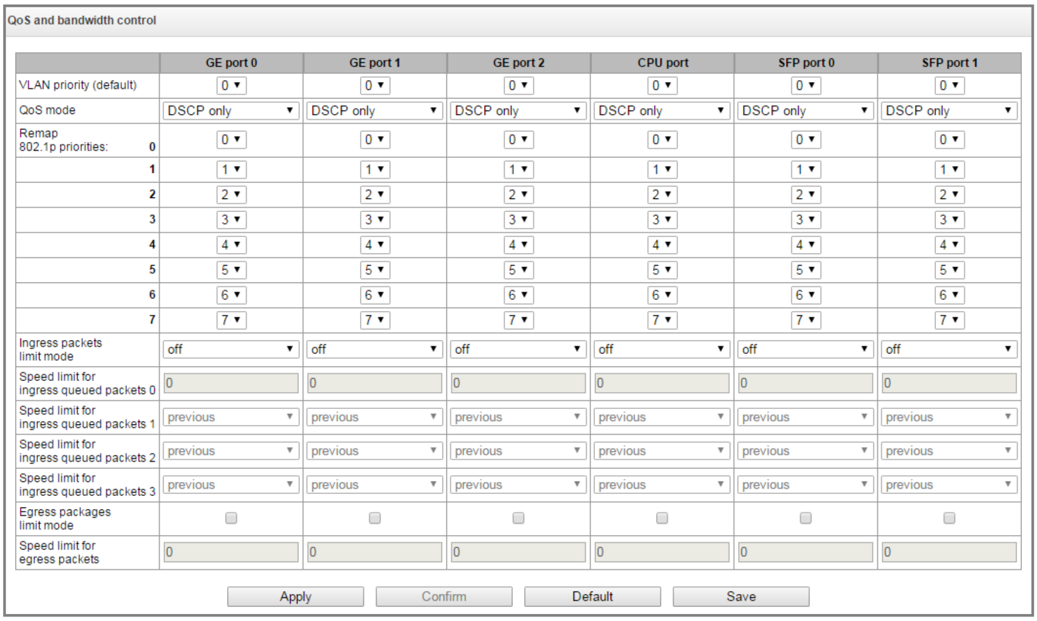
- *Save* — save settings into the device flash memory without applying them.

Removing records from the packet routing table

To remove records, select checkboxes for the rows to be removed and click *'Remove selected'* button.

3.1.12.4 QoS and bandwidth control

In the 'QoS and bandwidth control' section, you may configure Quality of Service functions.



QoS and bandwidth control

	GE port 0	GE port 1	GE port 2	CPU port	SFP port 0	SFP port 1
VLAN priority (default)	0	0	0	0	0	0
QoS mode	DSCP only	DSCP only	DSCP only	DSCP only	DSCP only	DSCP only
Remap 802.1p priorities: 0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	2	2	2	2	2	2
3	3	3	3	3	3	3
4	4	4	4	4	4	4
5	5	5	5	5	5	5
6	6	6	6	6	6	6
7	7	7	7	7	7	7
Ingress packets limit mode	off	off	off	off	off	off
Speed limit for ingress queued packets 0	0	0	0	0	0	0
Speed limit for ingress queued packets 1	previous	previous	previous	previous	previous	previous
Speed limit for ingress queued packets 2	previous	previous	previous	previous	previous	previous
Speed limit for ingress queued packets 3	previous	previous	previous	previous	previous	previous
Egress packages limit mode	□	□	□	□	□	□
Speed limit for egress packets	0	0	0	0	0	0

- *VLAN priority (default)* — 802.1p priority assigned to untagged packets, received by this port. If *802.1p* or *IP Diffserv* is already assigned to the packet, this setting will not be used ('default vlan priority' will not be applied to packets containing IP header, when one of the QoS modes is in use: *DSCP only, DSCP preferred, 802.1p preferred*).

- *QoS mode* — QoS operation mode:

  – *DSCP only* — distribute packets into queues based on IP Diffserv priority only.
  – *802.1p* only — distribute packets into queues based on 802.1p priority only.
  – *DSCP, 802.1p* — distribute packets into queues based on IP Diffserv and 802.1p priorities, if both priorities are present in the packet, IP Diffserv priority is used for queuing purposes.
  – *802.1p, DSCP* — distribute packets into queues based on IP Diffserv and 802.1p priorities, if both priorities are present in the packet, 802.1p priority is used for queuing purposes.

- *Remap 802.1p priorities* — remap 802.1p priorities for untagged packets. Thus, a new value may be assigned for each priority received in VLAN packet.

- *Ingress packets limit mode* — restriction mode for traffic coming to the port.

  – *Off* — no restriction.
  – *All packets* — restrict all traffic.
  – *BroadMultFlood* — multicast, broadcast, and flooded unicast traffic will be restricted.
  – *BroadMult* — multicast and broadcast traffic will be restricted.
  – *Broad* — only broadcast traffic will be restricted.

- *Speed limit for ingress queued packets 0* — bandwidth restriction for traffic incoming to a queue 0 port. Permitted values — from 70 to 250000kbps.

- *Speed limit for ingress queued packets 1* — bandwidth restriction for traffic incoming to a queue 1 port. You can double the bandwidth (prev prio *2) of priority 0, or leave it unchanged (same as prev prio).

- *Speed limit for ingress queued packets 2* — bandwidth restriction for traffic incoming to a queue 2 port. You can double the bandwidth (prev prio *2) of priority 1, or leave it unchanged (same as prev prio).

- *Speed limit for ingress queued packets 3* — bandwidth restriction for traffic incoming to a queue 3 port. You can double the bandwidth (prev prio *2) of priority 2, or leave it unchanged (same as prev prio).

- *Egress packages limit mode* — when checked, enable the bandwidth restriction for outgoing port traffic.

- *Speed limit for egress packets* — bandwidth restriction for outgoing port traffic. Permitted values — from 70 to 250000kbps.

- *Apply* — apply defined settings.

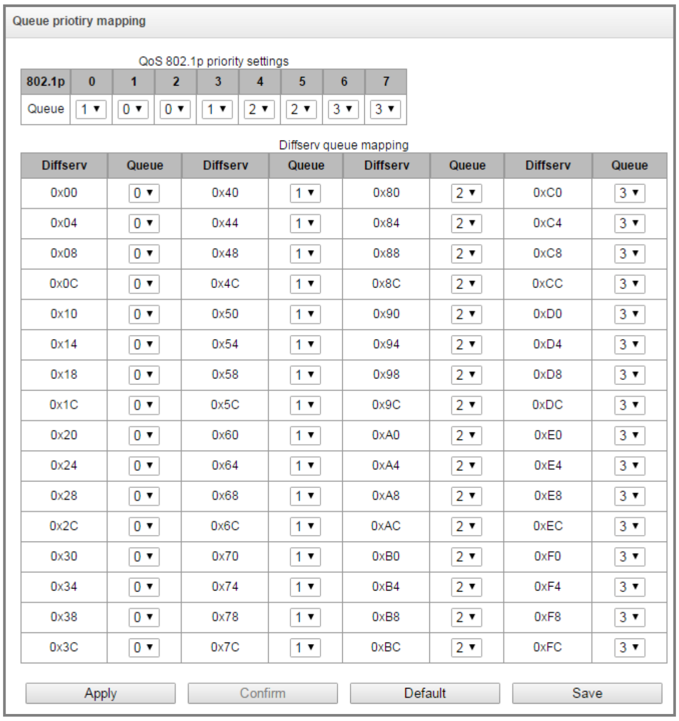
- Confirm — commit modified settings.

Click 'Confirm' button in 1 minute interval to confirm settings, or the previous values will be restored.

- *Default* — set default settings.

- *Save* — save settings into the device flash memory without applying them.

3.1.12.5 Queue priority mapping



Queue priotiry mapping

QoS 802.1p priority settings

802.1p	0	1	2	3	4	5	6	7
Queue	1 ▾	0 ▾	0 ▾	1 ▾	2 ▾	2 ▾	3 ▾	3 ▾

Diffserv queue mapping

Diffserv	Queue	Diffserv	Queue	Diffserv	Queue	Diffserv	Queue
0x00	0 ▾	0x40	1 ▾	0x80	2 ▾	0xC0	3 ▾
0x04	0 ▾	0x44	1 ▾	0x84	2 ▾	0xC4	3 ▾
0x08	0 ▾	0x48	1 ▾	0x88	2 ▾	0xC8	3 ▾
0x0C	0 ▾	0x4C	1 ▾	0x8C	2 ▾	0xCC	3 ▾
0x10	0 ▾	0x50	1 ▾	0x90	2 ▾	0xD0	3 ▾
0x14	0 ▾	0x54	1 ▾	0x94	2 ▾	0xD4	3 ▾
0x18	0 ▾	0x58	1 ▾	0x98	2 ▾	0xD8	3 ▾
0x1C	0 ▾	0x5C	1 ▾	0x9C	2 ▾	0xDC	3 ▾
0x20	0 ▾	0x60	1 ▾	0xA0	2 ▾	0xE0	3 ▾
0x24	0 ▾	0x64	1 ▾	0xA4	2 ▾	0xE4	3 ▾
0x28	0 ▾	0x68	1 ▾	0xA8	2 ▾	0xE8	3 ▾
0x2C	0 ▾	0x6C	1 ▾	0xAC	2 ▾	0xEC	3 ▾
0x30	0 ▾	0x70	1 ▾	0xB0	2 ▾	0xF0	3 ▾
0x34	0 ▾	0x74	1 ▾	0xB4	2 ▾	0xF4	3 ▾
0x38	0 ▾	0x78	1 ▾	0xB8	2 ▾	0xF8	3 ▾
0x3C	0 ▾	0x7C	1 ▾	0xBC	2 ▾	0xFC	3 ▾

- *Queue 802.1p priority settings* — allows to distribute packets into queues depending on the 802.1p priority.
  - *802.1p* — 802.1p priority value.
  - *Queue* — outgoing queue number.

- *Diffserv queue mapping* — allows to distribute packets into queues depending on the IP Diffserv priority.
  - *Diffserv* — IP Diffserv priority value.
  - *Queue* — outgoing queue number.

- *Apply* — apply defined settings.

- Confirm — commit modified settings.

Click 'Confirm' button in 1 minute interval to confirm settings, or the previous values will be restored.

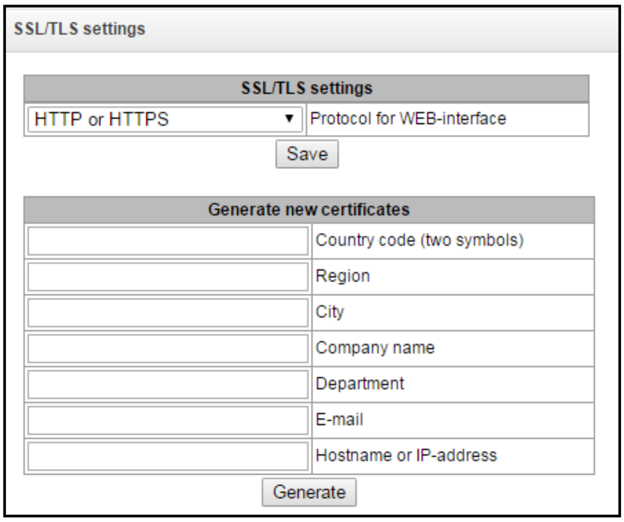
- *Default* — set default settings.

- Save — save settings into the device flash memory without applying them.

Queue 3 has the highest priority, queue 0 — the lowest priority. Weighted packet distribution to outgoing queues 3/2/1/0 is as follows: 8/4/2/1.

3.1.13 Security

3.1.13.1 SSL/TLS settings



SSL/TLS settings

SSL/TLS settings	
HTTP or HTTPS ▾	Protocol for WEB-interface

Generate new certificates	
	Country code (two symbols)
	Region
	City
	Company name
	Department
	E-mail
	Hostname or IP-address

In this section, you may obtain a self-signed certificate which allows you to use an encrypted connection to the gateway via HTTP protocol and configuration file upload/download via FTPS protocol.

- Protocol for WEB-interface — web configurator connection mode:
  - *HTTP or HTTPS* — unencrypted connection — via HTTP — as well as encrypted connection — via HTTPS — is enabled. At that, connection via HTTPS is possible only when generated certificate is present.
  - *HTTPS only* — only encrypted connection via HTTPS is enabled. Connection via HTTPS is possible only when generated certificate is present.

Generate new certificates

These parameters should be entered in Latin character.

- Country code (two symbols) — for Russia — RU
- Region
- City
- Company name
- Department
- E-mail
- Hostname or IP address.

Upload PEM certificate and key

This section allows uploading generated and signed PEM certificate and key. To upload a file, select its type in drop-down menu, click "Browse", select the file and click "Upload".

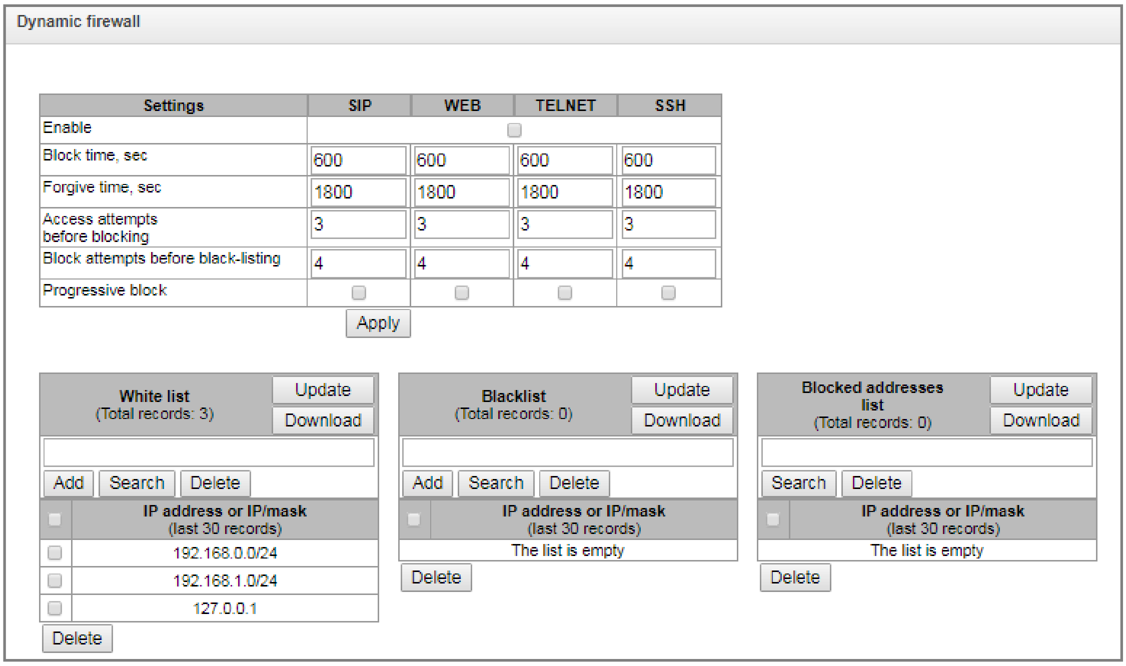
After uploading of the certificate and key, please, restart the web server using "Restart WEB-server" button.

3.1.13.2 Dynamic firewall

Dynamic firewall — is a utility that tracks attempts of access to various services. When constantly repeated unsuccessful access attempts from the same IP address/host are discovered, fail2ban blocks all further access attempts from this IP address/host.

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

- Brute forcing web configurator or SSH authentication data, i.e. attempt to log in to the management interface using wrong login or password.
- Brute forcing authentication data — reception of REGISTER requests from known IP address but containing wrong authentication data.
- Reception of requests (REGISTER, INIVITE, SUBSCRIBE and others) from unknown IP address.
- Reception of unknown requests via SIP port.



Dynamic firewall

Settings	SIP	WEB	TELNET	SSH
Enable	□			
Block time, sec	600	600	600	600
Forgive time, sec	1800	1800	1800	1800
Access attempts before blocking	3	3	3	3
Block attempts before black-listing	4	4	4	4
Progressive block	□	□	□	□

White list (Total records: 3)

□	IP address or IP/mask (last 30 records)
□	192.168.0.0/24
□	192.168.1.0/24
□	127.0.0.1

Blacklist (Total records: 0)

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

Blocked addresses list (Total records: 0)

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

Parameters:

- Enable — launch dynamic firewall utility.
- Block time, seconds — time in seconds during which access from the suspicious address will be banned.

- Forgive time, seconds — time that should pass for the address that originated the suspicious request to be forgotten if it was not banned earlier.
- Access attempts before blocking — maximum quantity of unsuccessful access attempts for a host prior to be banned by dynamic firewall.
- Block attempts before black-listing — quantity of bans after which the suspicious address will be blacklisted.
- Progressive block — when checked, each following address ban will be twice longer than the previous one and twice less access attempts will be used. E.g. for the first time 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 forth.

White list (last 30 records) — list of IP addresses and subnets that dynamic firewall will be unable to ban.

Black list (last 30 records) — list of permanently banned addresses and subnets. A device may have up to 8192 records on SMG-1016M and 16384 records on SMG-2016.

To add/search/remove an address from the list, select it in the entry field and click *'Add'/'Search'/'Delete'* button.

You may enter an IP address as well as a subnet.
To enter the subnet, you should enter the data in the following format:
`AAA.BBB.CCC.DDD`/mask

Example:
192.168.0.0/24 — record corresponds to the network address 192.168.0.0 with mask 255.255.255.0

- Download whole IP address white/black list — web configurator shows only the 30 last records in the file; click this button to download the whole white list and black list to your PC.

Blocked addresses list — list of addresses banned while dynamic firewall operation. Up to 8192 entries are available on SMG-1016M and up to 16384 entries are available on SMG-2016.

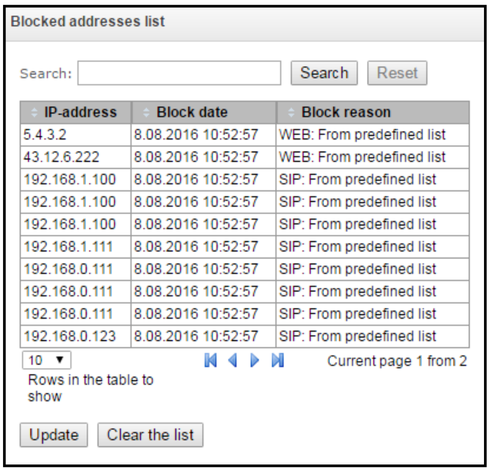
- Download block addresses list — allows you to download the whole list of banned addresses to your PC.

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

Dynamic firewall log information is written into **pbx_sip_bun.log** file.

3.1.13.3 Blocked addresses list

This section contains a list of addresses blocked by fail2ban that allows you to analyze which addresses got banned and when, for all the time from the switch startup.



Blocked addresses list

Search: Search Reset

IP-address	Block date	Block reason
5.4.3.2	8.08.2016 10:52:57	WEB: From predefined list
43.12.6.222	8.08.2016 10:52:57	WEB: From predefined list
192.168.1.100	8.08.2016 10:52:57	SIP: From predefined list
192.168.1.100	8.08.2016 10:52:57	SIP: From predefined list
192.168.1.100	8.08.2016 10:52:57	SIP: From predefined list
192.168.1.111	8.08.2016 10:52:57	SIP: From predefined list
192.168.0.111	8.08.2016 10:52:57	SIP: From predefined list
192.168.0.111	8.08.2016 10:52:57	SIP: From predefined list
192.168.0.111	8.08.2016 10:52:57	SIP: From predefined list
192.168.0.123	8.08.2016 10:52:57	SIP: From predefined list

10 ▼ Rows in the table to show

Current page 1 from 2

Update Clear the list

- *Search* — enter an address to search for it in the blocked address table.
- *IP address* — IP address that was banned.
- *Block date* — date and time of IP address ban.
- *Block reason* – a cause of blocking.
- *Update* — update blocked addresses list.
- *Clear the list* — delete all records from the banned address log.

For the list of banning messages and reasons, see Table below.

Table 24 — Banning messages

Message in pbx_sip_bun.log	***Reason***	***SIP message***
Request error: REGISTER failed : Resource limit overflow	Dynamic user registration limit has been achieved	403 response
Request error: REGISTER failed : Unknown user or registration domain	Registration request from unknown user	403 response
Request error: REGISTER failed : Server doesn’t allow a third party registration	Registration request with different To and From headers	403 response
Request error: REGISTER failed : Authentication is wrong	Wrong login/password	403 response
Request error: REGISTER failed : Wrong de-registration	User attempted to deregister not registered contact	200 response
Request error: REGISTER failed : Request from disallowed IP	Registration attempt from not allowed address	403 response
Request error: INVITE failed : No registration before	Call attempt from known user with not registered contact	403 response
Request error: INVITE failed : Registration is expired	Call attempt from known user with expired contact registration	403 response

Request error: INVITE failed : Authentication is wrong	Incoming call or registration has failed an authentication	403 response
Request error: INVITE failed : Unknown original address	Call from an unknown direction	Call is directed to mgapp where it will be passed through or rejected
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	Dialog for request acceptance has not been found	481 response

3.1.13.4 Static firewall

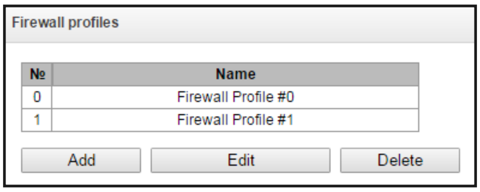
Firewall is a package of software tools that performs control and filtering of transmitted network packets in accordance with the defined rules in order to protect the device from unauthorized access.

The rules of static firewalls will not operate to limit access via HTTP/HTTPS, SSH, Telnet, SNMP, FTP. To limit the access via these protocols, use the white addresses list (section 3.1.13.5) and services activation settings on the network interfaces (section 3.1.10.3).

Firewall profiles

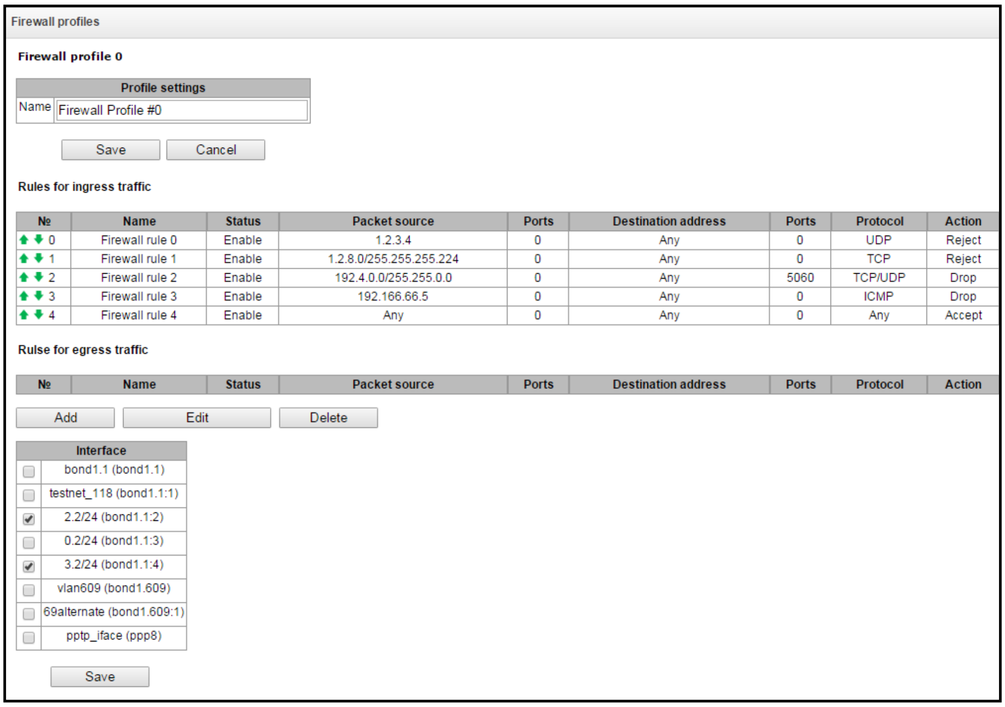
To create, edit or remove firewall profiles, use the following buttons:

Add
Edit
Delete


Firewall profiles

№	Name
0	Firewall Profile #0
1	Firewall Profile #1

Software allows you to configure firewall rules for incoming, outgoing and transit traffic as well as for specific network interfaces.


Firewall profiles

Firewall profile 0

Profile settings

Name: Firewall Profile #0

Rules for ingress traffic

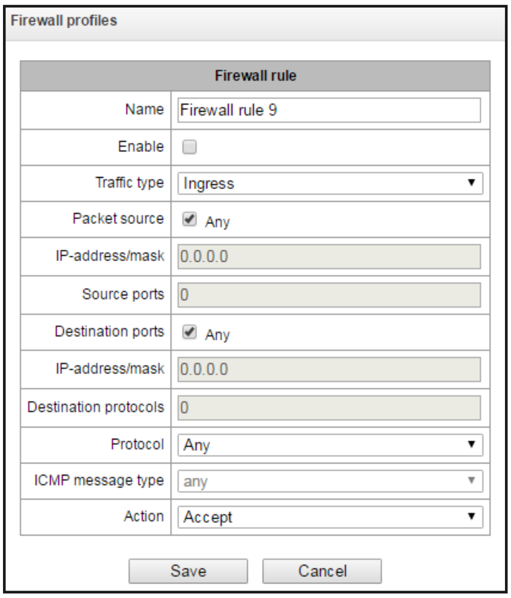
№	Name	Status	Packet source	Ports	Destination address	Ports	Protocol	Action
0	Firewall rule 0	Enable	1.2.3.4	0	Any	0	UDP	Reject
1	Firewall rule 1	Enable	1.2.8.0/255.255.255.224	0	Any	0	TCP	Reject
2	Firewall rule 2	Enable	192.4.0.0/255.255.0.0	0	Any	5060	TCP/UDP	Drop
3	Firewall rule 3	Enable	192.166.66.5	0	Any	0	ICMP	Drop
4	Firewall rule 4	Enable	Any	0	Any	0	Any	Accept

Rulse for egress traffic

№	Name	Status	Packet source	Ports	Destination address	Ports	Protocol	Action

	Interface
□	bond1.1 (bond1.1)
□	testnet_118 (bond1.1:1)
☑	2.2/24 (bond1.1:2)
□	0.2/24 (bond1.1:3)
☑	3.2/24 (bond1.1:4)
□	vlan609 (bond1.609)
□	69alternate (bond1.609:1)
□	pptp_iface (ppp8)

When a rule is created, you should configure the following parameters:



Firewall profiles

Firewall rule

Name	Firewall rule 9
Enable	□
Traffic type	Ingress ▾
Packet source	☑ Any
IP-address/mask	0.0.0.0
Source ports	0
Destination ports	☑ Any
IP-address/mask	0.0.0.0
Destination protocols	0
Protocol	Any ▾
ICMP message type	any ▾
Action	Accept ▾

- *Name* — rule name.
- *Enable* — defines whether the rule will be used. When unchecked, the rule will be inactive.
- *Traffic type* — type of traffic for the rule being created:
  - *ingress* — intended for SMG.
  - *egress* — sent by SMG.
- *Rule type* – might have the following values:
  - *General* – check IP addresses and ports;
  - *GeoIP* – check addresses in GeoIP base;
  - *String* – check the presence of a string in a packet.
- *Country* – select a country to which the address belongs. The field is available only for "GeoIP" rule type.
- *Content* – the string which might be in packets. The case of letters is important. The field is available only for "String" rule type.
- *Packet source* — defines the packet source network address either for all addresses or a particular IP address or network:
  - *any* — for all addresses (checkbox is selected).
- *IP address/mask* — for a particular IP address or network. Field is active when *'any'* checkbox is deselected. For a network, the mask is mandatory; for IP address, the mask is optional.
- *Source ports* — packet source TCP/UDP port or port range (defined with a hyphen '-'). This parameter is used for TCP and UDP only; thus, select UDP, TCP, or TCP/UDP in the field in order to make this field active.
- *Destination address* — defines the packet recipient network address either for all addresses or a particular IP address or network:
  - *any* — for all addresses (checkbox is selected).

- *IP address/mask* — for a particular IP address or network. Field is active when *'any'* checkbox is deselected. For a network, the mask is mandatory; for IP address, the mask is optional.

- *Destination ports* — packet recipient TCP/UDP port or port range (defined with a hyphen '-'). This parameter is used for TCP and UDP only; thus, select UDP, TCP, or TCP/UDP in the field in order to make this field active.

- *Protocol* — protocol that the rule will be used for: any, UDP, TCP, ICMP, or TCP/UDP.

- *ICMP message type* — ICMP message type that the rule will be used for. This field is active, when ICMP is selected in the *'Protocol'* field.

- *Action* — action executed by this rule:

  – *ACCEPT* — packets falling under this rule will be accepted by the firewall.
  – *DROP* — packets falling under this rule will be rejected by the firewall without informing the party that has sent these packets.
  – *REJECT* — packets falling under this rule will be rejected by the firewall. The party that has sent the packet will receive either TCP RST packet or 'ICMP destination unreachable'.

Created rule will be placed into the respective section: *'Incoming traffic rules'*,*'Outgoing traffic rules'* or *'Transit traffic rules'*.

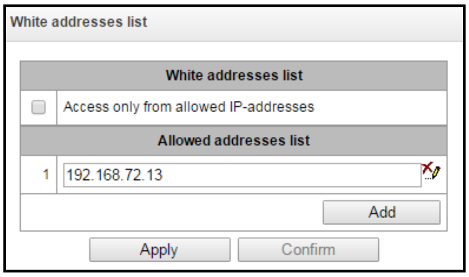
Also, in the firewall profile, you may specify network interfaces that these profile rules will be applied to.

Each network interface may be used only in a single firewall profile at a time. If you attempt to assign a network interface to a new profile, it will be removed from the previous one.

To apply the rules, click 'Apply' button that will appear when the changes are made into the firewall settings.

3.1.13.5 White addresses list

In this section, you may configure the list of allowed IP addresses that the administrator may use for connection to the device via web configurator and Telnet/SSH protocol. By default, all addresses are allowed.



White addresses list

	White addresses list
□	Access only from allowed IP-addresses
	Allowed addresses list
1	192.168.72.13

- *Access only from allowed IP addresses* — when checked, the list of allowed IP addresses will be applied; otherwise, access is allowed from any address.

You may enable access for subnets; to do that, you should specify address in IP/mask format, e.g.: 192.168.0.0/24.

- *Apply* — apply changes.

- *Confirm* — confirm changes.

To create, edit or remove the list allowed addresses, use the following buttons:

— *'Add'*

— *'Edit'*

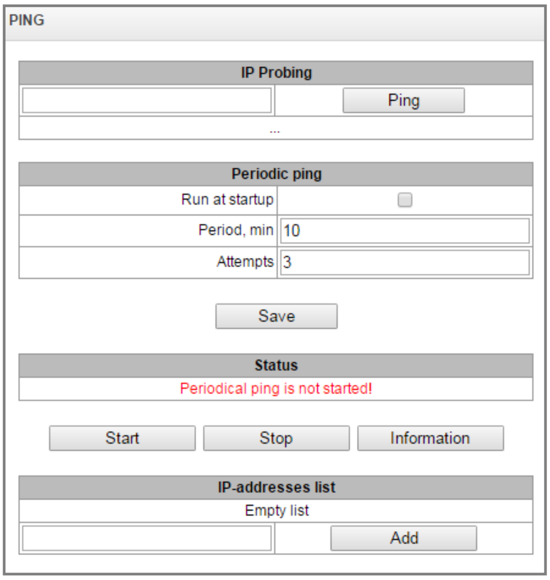
— *'Remove'*

When the address list has been configured, click 'Apply' and 'Confirm' buttons; if you fail to confirm changes in 60 seconds, previous values will be restored — this procedure allows to protect the user from the loss of access to the device.

3.1.14 Network utilities:

3.1.14.1 PING

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



PING

IP Probing

[ ] Ping

...

Periodic ping

Run at startup	□
Period, min	10
Attempts	3

Save

Status

Periodical ping is not started!

Start Stop Information

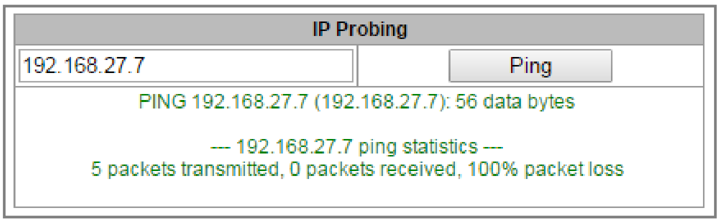
IP-addresses list

Empty list

[ ] Add

IP Probing — used for a single-time device network connection control.

To send *Ping request (ICMP protocol is used)*, you should enter host IP address or network name in the *'IP probing'* field and click *'Ping'* button. Command execution result will be shown in the lower part of the page. The result contains the quantity of transmitted packets, quantity of received responses to those packets, percentage of lost packets, and reception/transmission time (minimum/average/maximum) in milliseconds.



IP Probing

192.168.27.7 Ping

```
PING 192.168.27.7 (192.168.27.7): 56 data bytes

--- 192.168.27.7 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

Periodic ping — used for periodic device network connection control.

- *Run at startup* – when checked, the transmission of ping requests to addresses defined in hosts list will be activated right after the device startup.
- *Period, minutes* — time interval between requests in minutes.

- *Attempts* — number of attempts to send the request to an address.

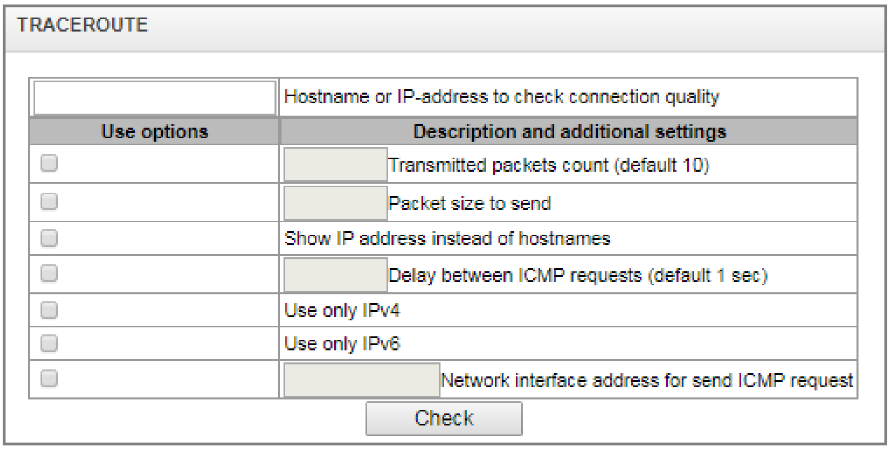
State

- *Start* — launch/restart periodic ping.
- *Stop* — forcedly stop periodic ping.
- *Information* — click this button to view the log file '/tmp/log/hosttest.log'that contains data on the last periodic ping request transmission attempt.

IP addresses list — list of IP addresses that periodic ping requests will be sent to.
To add a new address to the list, select it in the entry field and click *'Add'* button. To remove an address, click *'Remove'* button next to the required address.

3.1.14.2 TRACEROUTE

The **TRACEROUTE** utility performs route tracing functions and echo tests (ping requests transmission) for network operation diagnostics. The function allows to evaluate quality of connection with the node being checked.



TRACEROUTE

	Hostname or IP-address to check connection quality
Use options	**Description and additional settings**
□	Transmitted packets count (default 10)
□	Packet size to send
□	Show IP address instead of hostnames
□	Delay between ICMP requests (default 1 sec)
□	Use only IPv4
□	Use only IPv6
□	Network interface address for send ICMP request

Enter the IP address of the network device, connection to which is going to be checked, in the "Hostname or IP address to check connection quality" field. Check the boxes next to the necessary options to use them.

Options:

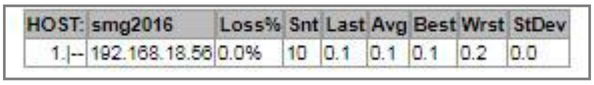
- *Transmitted packets count (default 10)* – the number of ICMP requests transmission cycles.
- *Packet size to send* – the size of ICMP packets in bytes;
- *Show IP address instead of hostnames*– do not use DNS. Display IP addresses without attempts to receive their network names.
- *Delay between ICMP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

After entering an IP address of a network device, the connection to which is going to be evaluated, and checking the boxes next to the necessary options, click "Check".

As a result, the table with the following information is displayed:

- *Number of the node and its IP address* (or network name),
- *The percentage of lost packets (Loss%),*

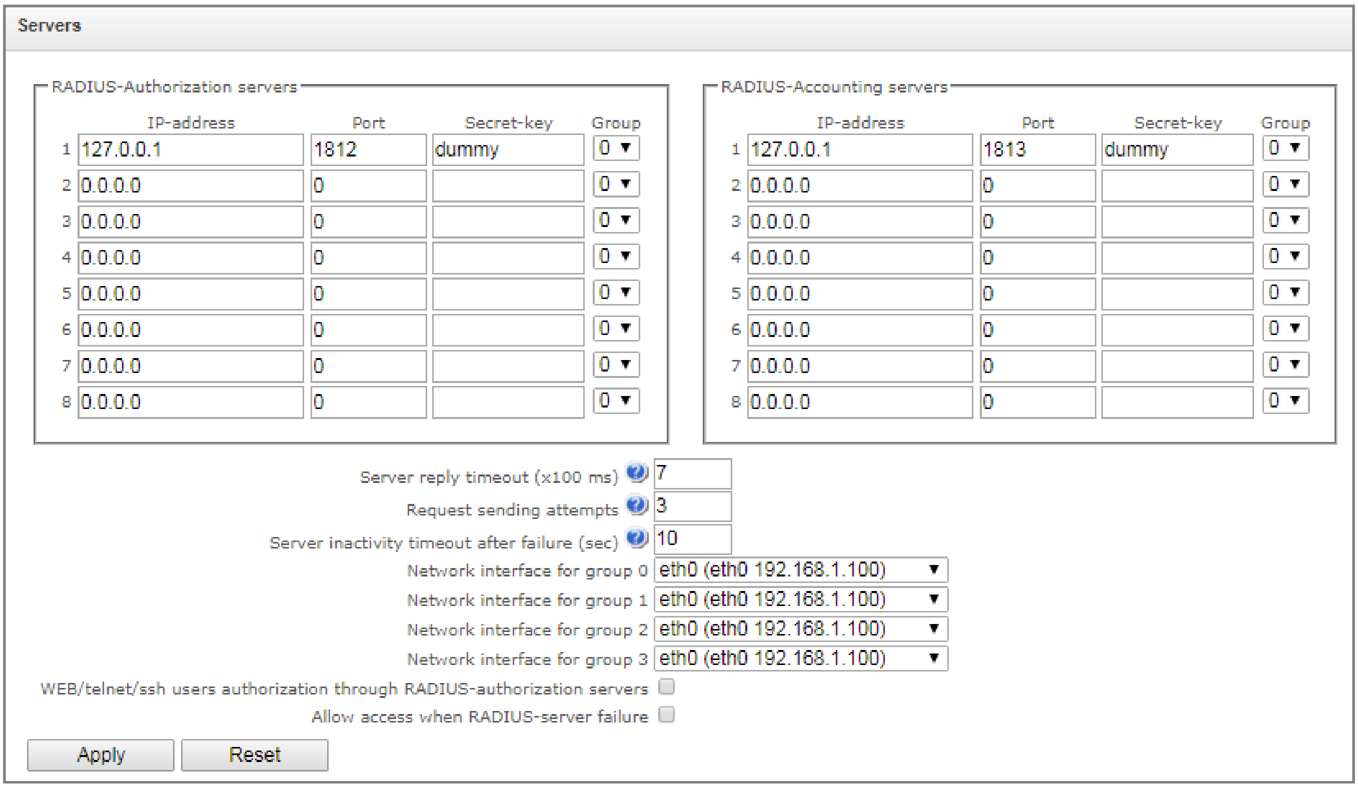
- *The number of transmitted packets (Snt),*
- *The round-trip time of the last packet (Last),*
- *Average round-trop time for packets (Avg),*
- *The best round-trip time for the packets (Best),*
- *The worst round-trip time for the packets (Wrst),*
- *Mean square deviation of delays for each node (StDev).*



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

3.1.15 RADIUS configuration

3.1.15.1 RADIUS servers



Servers

RADIUS-Authorization servers

	IP-address	Port	Secret-key	Group
1	127.0.0.1	1812	dummy	0 ▼
2	0.0.0.0	0		0 ▼
3	0.0.0.0	0		0 ▼
4	0.0.0.0	0		0 ▼
5	0.0.0.0	0		0 ▼
6	0.0.0.0	0		0 ▼
7	0.0.0.0	0		0 ▼
8	0.0.0.0	0		0 ▼

RADIUS-Accounting servers

	IP-address	Port	Secret-key	Group
1	127.0.0.1	1813	dummy	0 ▼
2	0.0.0.0	0		0 ▼
3	0.0.0.0	0		0 ▼
4	0.0.0.0	0		0 ▼
5	0.0.0.0	0		0 ▼
6	0.0.0.0	0		0 ▼
7	0.0.0.0	0		0 ▼
8	0.0.0.0	0		0 ▼

Server reply timeout (x100 ms): 7
Request sending attempts: 3
Server inactivity timeout after failure (sec): 10
Network interface for group 0: eth0 (eth0 192.168.1.100) ▼
Network interface for group 1: eth0 (eth0 192.168.1.100) ▼
Network interface for group 2: eth0 (eth0 192.168.1.100) ▼
Network interface for group 3: eth0 (eth0 192.168.1.100) ▼
WEB/telnet/ssh users authorization through RADIUS-authorization servers ☐
Allow access when RADIUS-server failure ☐

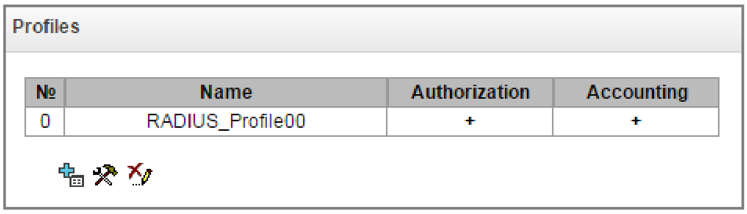
Device supports up to 8 authorization servers and up to 8 accounting servers. The servers might be combined in a group. Then, while RADIUS profiles settings, you may choose the group of servers to transmit requests. Four group are available.

- *Server reply timeout* — amount of time intended for server response.
- *Request sending attempts* — quantity of request retries addressed to a server. When all attempts are used up, the server will be deemed inactive and the request will be forwarded to another server, if it is specified, otherwise the error will be detected.
- *Server inactivity timeout after failure* — amount of time that the server is deemed unavailable (requests will not be sent to it).
- *Network interface for <N> group* — select corresponding group for network interface through which RADIUS requests will be transmitted.

- *WEB/telnet/ssh users authorization through RADIUS-authorization servers* – in case of the access attempt via WEB/telnet/ssh, the authorization will be implemented via RADIUS server. You should register local users with the necessary names and configure access rights in advanced (see section 3.1.25 Setting password for web configurator access).

- *Allow access when RADIUS-server failure* – if authorization via RADIUS is enabled and there is no answer from the RADIUS server, you may use local account of admin.

3.1.15.2 Profile list



Profiles

№	Name	Authorization	Accounting
0	RADIUS_Profile00	+	+

To create, edit and delete profiles from the list use the following buttons:

– «*Add*»;
– «*Edit*»;
– «*Delete*».

Profile parameters:

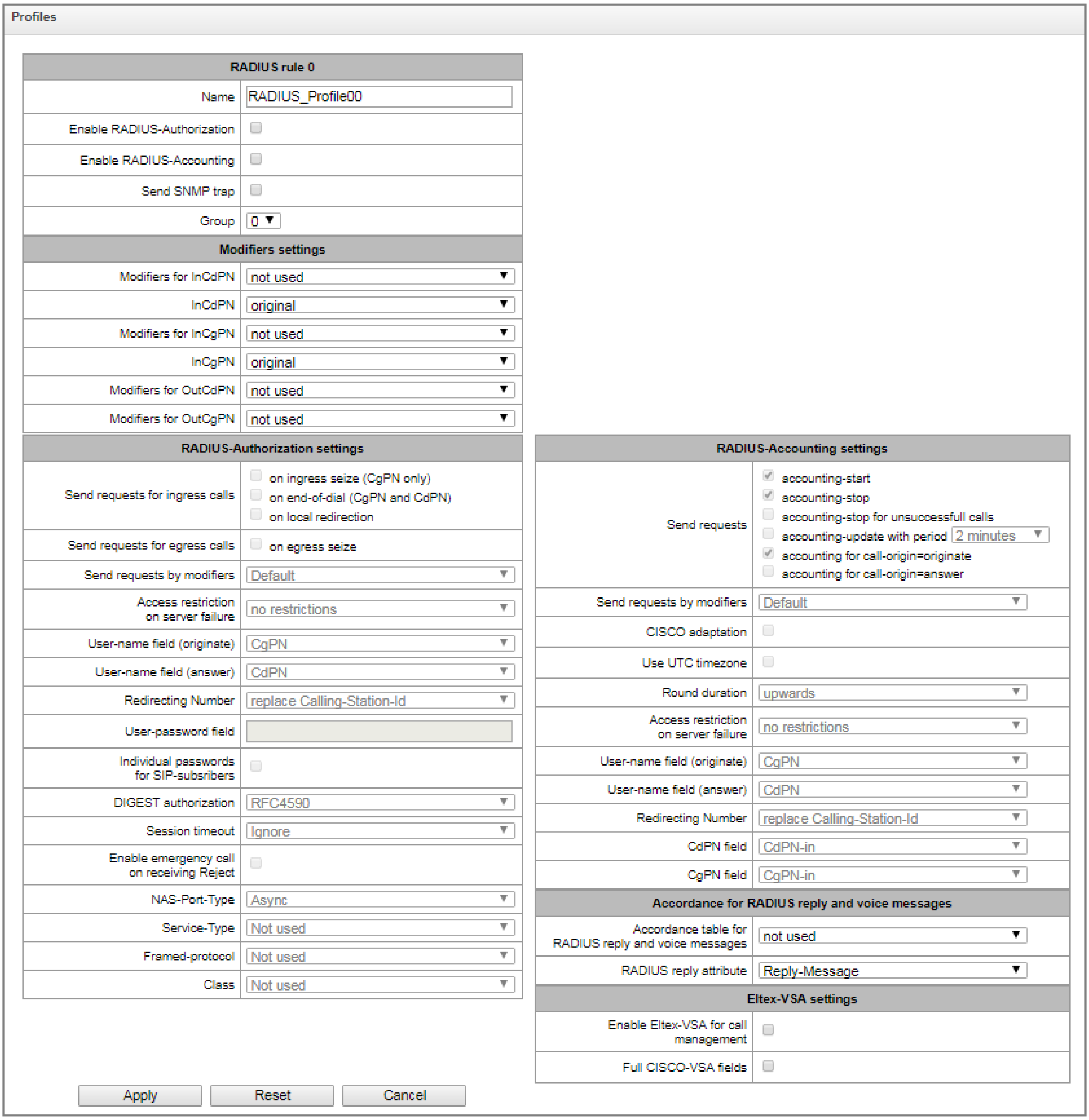
- Name – profile's name;

- Enable RADIUS-Authorization — enable/disable the transmission of authentication/authorization (Access Request) messages to the RADIUS server.

- Enable RADIUS-Accounting — enable/disable the transmission of accounting(Accounting Request) messages to the RADIUS server.

- *Send SNMP trap* – enable SNMP trap sending with every RADIUS request transmission.

- *Group* – the group of RADIUS servers used to transmit requests.



RADIUS rule 0	
Name	RADIUS_Profile00
Enable RADIUS-Authorization	□
Enable RADIUS-Accounting	□
Send SNMP trap	□
Group	0
Modifiers settings	
Modifiers for InCdPN	not used
InCdPN	original
Modifiers for InCgPN	not used
InCgPN	original
Modifiers for OutCdPN	not used
Modifiers for OutCgPN	not used
RADIUS-Authorization settings	
Send requests for ingress calls	□ on ingress seize (CgPN only) □ on end-of-dial (CgPN and CdPN) □ on local redirection
Send requests for egress calls	□ on egress seize
Send requests by modifiers	Default
Access restriction on server failure	no restrictions
User-name field (originate)	CgPN
User-name field (answer)	CdPN
Redirecting Number	replace Calling-Station-Id
User-password field	
Individual passwords for SIP-subsribers	□
DIGEST authorization	RFC4590
Session timeout	Ignore
Enable emergency call on receiving Reject	□
NAS-Port-Type	Async
Service-Type	Not used
Framed-protocol	Not used
Class	Not used

RADIUS-Accounting settings	
Send requests	☑ accounting-start ☑ accounting-stop □ accounting-stop for unsuccessfull calls □ accounting-update with period 2 minutes ☑ accounting for call-origin=originate □ accounting for call-origin=answer
Send requests by modifiers	Default
CISCO adaptation	□
Use UTC timezone	□
Round duration	upwards
Access restriction on server failure	no restrictions
User-name field (originate)	CgPN
User-name field (answer)	CdPN
Redirecting Number	replace Calling-Station-Id
CdPN field	CdPN-in
CgPN field	CgPN-in
Accordance for RADIUS reply and voice messages	
Accordance table for RADIUS reply and voice messages	not used
RADIUS reply attribute	Reply-Message
Eltex-VSA settings	
Enable Eltex-VSA for call management	□
Full CISCO-VSA fields	□

Modifiers settings:

- Modifiers for InCdPN — select callee (CdPN) number modifier for the incoming connection in relation to Called-Station-Id, xpgk-dst-number-in fields of RADIUS-Authorization and RADIUS-Accounting messages.
- InCdPN — select the number transmitted in xpgk-dst-number-in field of RADIUS-Authorization and RADIUS-Accounting messages:
  - *original* — initial number that was received in CdPN field of the incoming call prior to its modification.
  - processed — CdPN number after modification.

- Modifiers for InCgPN — select caller (CgPN) number modifier for the incoming connection in relation to Calling-Station-Id, xpgk-src-number-in fields of RADIUS-Authorization and RADIUS-Accounting messages.

- InCgPN — select the number transmitted in xpgk-dst-number-in field of RADIUS-Authorization and RADIUS-Accounting messages:

  - *original* — initial number that was received in CgPN field of the incoming call prior to its modification.
  - processed — CgPN number after modification.

- Modifiers for OutCdPN — select callee (CdPN) number modifier for the outgoing connection in relation to xpgk-src-number-out field of RADIUS-Authorization and RADIUS-Accounting messages.

- Modifiers for OutCgPN — select caller (CgPN) number modifier for the outgoing connection in relation to xpgk-dst-number-out field of RADIUS-Authorization and RADIUS-Accounting messages.

RADIUS-Authorization settings:

Send requests for ingress calls. Authentication/authorization requests may be transmitted during various call phases:

- on ingress seize (CgPN only);

- on the end-of-dial (CgPN and CdPN)

- on local redirection

Send requests for egress calls. Authentication/authorization requests may be transmitted:

- on egress seize.

The control of calls in RADIUS might be limited on the basis of modifier mask. Select one or more modifiers in "Modifiers settings" and select "Restrict" in the "Send requests by modifiers" field. In this case, a request for authorization will be sent to RADIUS only if the number complies one of the mask in the modifiers table. The modification will be implemented as usual, according to modifiers table rules.

✓ **When "Send requests by modifiers" is set to "Restrict", the calls which numbers is not in the modifier mask wil be considered as automatically authorized.**

*Access restriction on server failure.*During server fault (response non-reception), you may impose restrictions upon the outgoing communications:

- *no restrictions* — allow all calls.

- *local and zone networks only* — allow calls to emergency services, local and zone network.

- *local network only* — allow calls to emergency services and local network.

- *emergency only* — allow calls to emergency services only.

- *deny all (disconnect)* — deny all calls.

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

- User-name field — select User-Name attribute value in the corresponding Access Request authorization packet (RADIUS-Authorization):
  - CgPN — use calling party phone number as the value.
  - CgPN — use called party phone number as the value.
  - IP or E1-stream — use calling party IP address or incoming connection stream number as the value.
  - Trunk name — use incoming connection trunk name as the value.
  - Original CgPN — use non-modified phone number of the caller as the value;
  - Original CdPN — use non-modified phone number of the callee as the value.
- Redirection Number – a mode of RedirPN transmission to RADIUS :
  - replace Calling-Station-Id – RedirPN will be transmitted to the Calling-Station-Id field, replacing the existing value;
  - send as h323-redirect-number – RedirPN will be transmitted to the h323-redirect-number field separately.
- User-password field — specify User-Password attribute value in the corresponding RADIUS-Authorization packet:
- Individual passwords for SIP subscribers — when checked, use custom passwords for authentication/authorization of SIP subscribers instead of the password specified in USER-PASSWORD field.
- DIGEST authorization — select subscriber authorization algorithm with dynamic registration through the RADIUS server. In DIGEST authorization, the password is not transferred in the open as for the basic authentication; it represents a hash code and couldn't be intercepted during traffic scanning:
  - RFC4590 (RFC4590 recommendation complete implementation)
  - RFC4590-no-challenge (operation with a server that does not transfer Access Challenge)
  - Draft-sterman (NetUp, FreeRadius) (operation upon draft that RFC4590 recommendation is based on)
- Session timeout — impose limitation on the maximum call duration:
  - Ignore — do not impose limitation on the maximum call duration.
  - Use Session-Time — limit the maximum call duration on the basis of the Session-Timeout(27) attribute value.
  - Use Cisco h323-credit-time — limit the maximum call duration on the basis of the Cisco VSA (9) h323-credit-time(102) attribute value.
  - Session-Time priority — if both parameters (session-time and Cisco h323-credit-time) are present in the server response, use session-time and ignore Cisco h323-credit-time.
  - Cisco h323-credit-time priority — if both parameters (session-time and Cisco h323-credit-time) are present in the server response, use Cisco h323-credit-time and ignore session-time.

SMG gateway may use *Session-Timeout* or *Cisco VSA h323-credit-time* attribute value from Access-Accept packet in order to impose limitation on the maximum duration of an authorized call.

- *Enable emergency call on receiving reject* — allow calls to emergency services node after Access-Reject reception from the server.

Specifying optional Authentication-Request packet attributes:

- *NAS-Port-Type* — NAS physical port type (server for user authentication), default value is Async.
- *Service-Type* — type of service, not used by default (Not Used).
- *Framed-protocol* — protocol specified for the packet access utilization, not used by default (Not Used).
- *Class* — AV-Pair Class field processing for category change:
  - Not used — do not process AV-Pair Class field.
  - SS7 category — use value of the received AV-Pair Class field as the caller SS7 category.

RADIUS-Accounting settings:

- Send requests:
  - *accounting-start* — send 'accounting' start packet that notifies RADIUS server on the call start.
  - *accounting-stop* — send 'accounting' stop packet that notifies RADIUS server on the call end.
  - *accounting-stop* for unsuccessful calls — send information on unsuccessful calls to RADIUS server.
  - *accounting-update with period* — send 'update' packet during a call to RADUIS server with the definite period, that notifies RADIUS server on the call active state.
  - *accounting for call-origin=originate* — send 'RADIUS-Accounting' messages for incoming connection branch.
  - *accounting for call-origin=answer* — send 'RADIUS-Accounting' messages for outgoing connection branch.

You may limit sending billing information in RADIUS on the basis of the modifier mask. Select one or more modifiers in "Modifiers settings" and select "Restrict" in the "Send requests by modifiers" field. In this case, billing information will be sent to RADIUS only if the number complies one of the mask in the modifiers table. The modification will be implemented as usual, according to modifiers table rules.

When "Send requests by modifiers" is set to "Restrict", billing information will not be sent for the calls which numbers is not in the modifier mask.

- *Cisco adaptation* - swap originate and answer is accounting messages;
- *Use UTC timezone* — send time in 'RADIUS-**Accounting'** messages in UTC format;
- *Round duration* - rounding selection for RADIUS-Accounting messages. Three options are available - rounding up, rounding down and not rounding (transmit milliseconds).
- Access restriction on server failure - during server fault (response non-reception), you may impose restrictions upon the outgoing communications:
  - no restrictions — allow all calls.
  - local and zone networks only — allow calls to emergency services, local and zone network.
  - local network only — allow calls only to emergency services.
  - deny all — deny all calls.

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

- User-name field — select User-Name attribute value in the corresponding Accounting Request authorization packet (RADIUS-Accounting):
  - CgPN — use calling party phone number as a value.
  - CgPN — use called party phone number as a value.
  - IP or E1-stream — use calling party IP address or incoming connection stream number as a value.
  - Trunk name — use incoming connection trunk name as a value.
  - Original CgPN — use non-modified phone number of the caller as the value;
  - Original CdPN — use non-modified phone number of the callee as the value.
- Redirection Number – a mode of RedirPN transmission to RADIUS :
  - replace Calling-Station-Id – RedirPN will be transmitted to the Calling-Station-Id field, replacing the existing value;
  - send as h323-redirect-number – RedirPN will be transmitted to the h323-redirect-number field separately.
- CdPN field — select callee number value used in RADIUS packet generation for specific Attribute-Value pairs (Section 3.1.15.5):
  - CdPN-in — use callee number prior to modification (number received in SETUP/INVITE request).
  - CdPN-out — use callee number after the modification.
- CgPN field — select caller number value used in RADIUS packet generation for specific Attribute-Value pairs (section 3.1.15.5):
  - CgPN-in – use the number of a calling subscriber before modification (the number received in SETUP/INVITE request);
  - CgPN-out – use the number of a calling subscriber after modification.

Accordance for RADIUS rely and voice messages

After *Reject* message reception from the RADIUS server, you may enable output of a standard gateway voice message in order to inform the subscriber on the reason for connection refusal. Voice message output is based on the analysis of the replay-Message field or h-323-return-code field of *Reject* message.

Accordance table for RADIUS reply and voice messages — select correspondence table for RADIUS-reject responses and voice messages.

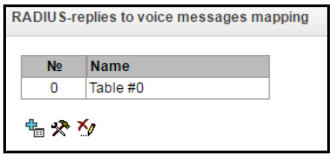
RADIUS response attribute — select an attribute that will be used for RADIUS-reject message analysis.

Eltex-VSA settings

- *Enable Eltex-VSA for call management* — activate Radius call management service (if RCM license is available); for Radius call management service description, see Appendix K.
- *Full CISCO-VSA fields* — complete attribute name transmission in CISCO-VSA fields.

3.1.15.3 RADIUS replies to voice messages mapping

In this section, you may configure the correspondence between RADIUS-reject responses and voice messages output to the subscribers.



RADIUS-replies to voice messages mapping

№	Name
0	Table #0

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

— *'Add table'*

— *'Edit table'*

— *'Remove table'*

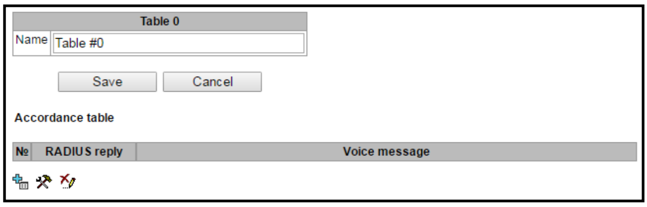
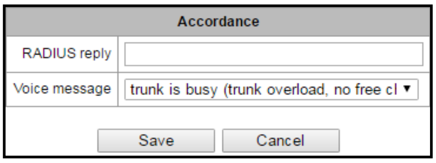


Table 0

Name: Table #0

Accordance table

№	RADIUS reply	Voice message



Accordance

RADIUS reply	
Voice message	trunk is busy (trunk overload, no free cl ▾

- *RADIUS reply* **—** replay-Message or h-323-return-code field value of the Reject message received from the RADIUS server.
- *Voice message* — select a voice message that will be output to the subscriber.

3.1.15.4 RADIUS packet format

Each packet description includes descriptions of every Attribute-Value pair for this packet type. Attributes may be either standard attributes or vendor specific attributes (Vendor-Specific Attribute). If the attribute value is unknown for any reason (e.g. if the outgoing trunk is missing, it is impossible to identify CdPN_OUT variable value that is used as a value for some attributes), then this attribute is not included into the message.

For standard attributes, description will be as follows:

Attribute name (Attribute number): Attribute value

For 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 — vendor number assigned by IANA organization in the “PRIVATE ENTERPRISE NUMBERS” document (http://www.iana.org/assignments/enterprise-numbers);

VSA name — vendor attribute name

VSA number — vendor attribute number

VSA value — vendor attribute value

You may use *<$NAME>* structure as an attribute value, where *NAME* is a name of the variable. For description of variable values, see Section 3.1.15.5Variable description.

Access-Request packet

```
User-Name(1): <$USER_NAME>
User-Password(2): based on password "eltex" (w/o quotation marks)
NAS-IP-Address(4): <$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): <$CgPN_IN>
Acct-Delay-Time(41): acc. to RFC2866
Event-Timestamp(55): acc. to RFC2869
NAS-IP-Address(4): <$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): acc. to RFC2866
Event-Timestamp(55): acc. 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

After the Access-Accept packet is received from the RADIUS server, the call is considered as authorized. Next, the search for an outgoing trunk will be performed and if successful, an attempt to establish the connection will be made.

If *Session-Time (27)* attribute or *Cisco VSA (9) h323-credit-time (102)* attribute has been transferred in a packet, and the corresponding setting was specified in the RADIUS profile, attribute value will be used for the maximum call duration limitation. When this timeout expires, the connection will be terminated by SMG.

3.1.15.5 Variable description

Table 25 — Variable description

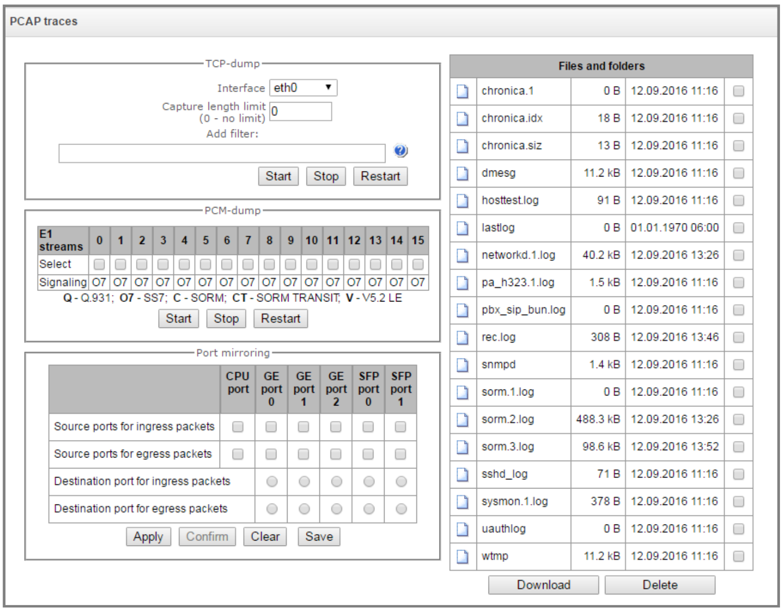
Variable	***Description and possible values***
$CALL_TYPE	defined on the basis of the transmission medium that the outgoing trunk belongs to: • 'Telephony', if the outgoing trunk is PSTN (TDM). • 'VoIP', if the outgoing trunk is VoIP.
$CdPN	determined from SMG settings • $CdPN = $CdPN_IN [by default] • $CdPN = $CdPN_OUT
$CdPN_IN	callee number before modification (received in SETUP/INVITE)
$CdPN_OUT	callee 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 reason for call clearing
$DST_ID	outgoing trunk name for this call
$DST_IP (string)	IP address of the terminating device when if the outgoing trunk is VoIP, e.g.: 192.168.0.1
$USER_IP	IP address of the device intiated the call if the ingress trunk is VoIP or SIP subscriber
$LOCAL_DISCONNECT_CAUSE	local reason for call clearing; values: • 1 — connection to the callee has been established (User-Answer) • 2 — wrong or incomplete number format (Incomplete-Number) • 3 — number does not exist (Unassigned-Number) • 4 — unsuccessful connection attempt, unknown reason (Unsuccessful-Other-Cause) • 5 — callee is busy (User-Busy) • 6 — equipment fault (Out-of-Order) • 7 — no response from the callee (No-Answer) • 8 — outgoing trunk is unavailable (Unavailable-Trunk) • 9 — RADIUS server authorization 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, 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	arrival time of the SETUP/INVITE message in hh:mm:ss.uuu t www MMM dd yyyy format
$TIME_CONNECT	reception time of the CONNECT/200 OK message issued by the called party in hh:mm:ss.uuu t www MMM dd yyyy format
$TIME_DISCONNECT	reception time of DISCONNECT/BYE issued by one of the parties in hh:mm:ss.uuu t www MMM dd yyyy format; if the call is unsuccessful, time of the message is specified upon reception of which SMG begins 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
<$inc_SIP_call_ID>	SIP message Call-ID field value for the incoming connection branch.
<$out_SIP_call_ID>	SIP message Call-ID field value for the outgoing connection branch.
<$inc_RTP_loc_IP>	Local IP address of the device for the incoming connection branch RTP session establishment.
<$inc_RTP_rem_IP>	Remote IP address of the communicating device for the incoming connection branch RTP session establishment.
<$out_RTP_loc_IP>	Local IP address of the device for the outgoing connection branch RTP session establishment.
<$out_RTP_rem_IP>	Remote IP address of the communicating device for the outgoing connection branch RTP session establishment.
<$call_record_file_name>	Conversation record file name. For instance: call_records/2016-12-13-0000/2016-12-13_12-41-45_20000-10000.wav

3.1.16 Tracing

3.1.16.1 PCAP tracings

In this menu, you may configure parameters for network traffic analysis and TDM protocol.



Interface: eth0

Capture length limit (0 - no limit): 0

E1 streams	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Select	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Signaling	O7	O7	O7	O7	O7	O7	O7	O7	O7	O7	O7	O7	O7	O7	O7	O7

Q - Q.931; **O7** - SS7; **C** - SORM; **CT** - SORM TRANSIT; **V** - V5.2 LE

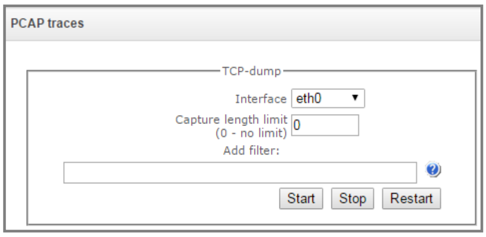
	CPU port	GE port 0	GE port 1	GE port 2	SFP port 0	SFP port 1
Source ports for ingress packets	□	□	□	□	□	□
Source ports for egress packets	□	□	□	□	□	□
Destination port for ingress packets		○	○	○	○	○
Destination port for egress packets		○	○	○	○	○

Files and folders				
🗋	chronica.1	0 B	12.09.2016 11:16	□
🗋	chronica.idx	18 B	12.09.2016 11:16	□
🗋	chronica.siz	13 B	12.09.2016 11:16	□
🗋	dmesg	11.2 kB	12.09.2016 11:16	□
🗋	hosttest.log	91 B	12.09.2016 11:16	□
🗋	lastlog	0 B	01.01.1970 06:00	□
🗋	networkd.1.log	40.2 kB	12.09.2016 13:26	□
🗋	pa_h323.1.log	1.5 kB	12.09.2016 11:16	□
🗋	pbx_sip_bun.log	0 B	12.09.2016 11:16	□
🗋	rec.log	308 B	12.09.2016 13:46	□
🗋	snmpd	1.4 kB	12.09.2016 11:16	□
🗋	sorm.1.log	0 B	12.09.2016 11:16	□
🗋	sorm.2.log	488.3 kB	12.09.2016 13:26	□
🗋	sorm.3.log	98.6 kB	12.09.2016 13:52	□
🗋	sshd_log	71 B	12.09.2016 11:16	□
🗋	sysmon.1.log	378 B	12.09.2016 11:16	□
🗋	uauthlog	0 B	12.09.2016 11:16	□
🗋	wtmp	11.2 kB	12.09.2016 11:16	□

TCP dump — TCP–dump utility settings:

TCP dump is a utility for network traffic interception and analysis.

- *Interface* — interface for the network traffic interception.
- *Capture length limit* — size limit for intercepted packets (0 – no limit), bytes.
- *Add filter* — packet filter for tcpdump utility.



Interface: eth0

Capture length limit (0 - no limit): 0

Structure of filter expressions

Each expression that defines the filter includes a single or multiple primitives containing a single or multiple object identifiers and preceding qualifiers. Object identifier may be represented by its name or number.

Object qualifiers:

1. **type** — indicates the object type specified by identifier. Object type may be represented by the following values:
   host,
   net,
   port.
   If object type is not defined, **host** value will be assumed.

2. **dir** — defines the direction towards the object. For this qualifier, the following values are supported:
   src (object is a source),
   dst (object is a destination),
   src or dst (source or destination),
   src and dst (source and destination).

If dir qualifier is not defined, **src or dst** value will be assumed.
For traffic interception from artificial interface 'any', qualifiers **inbound** and **outbound** may be used.

3. **proto** — defines the protocol that packets should belong to. This qualifier may take up the following values:
ether, **fddi1**, **tr2**, **wlan3**, **ip**, **ip6**, **arp**, **rarp**, **decnet**, **tcp** and **udp**.
If the primitive does not contain protocol qualifier, it is assumed that all protocols compatible with 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 numerous primitives interconnected with logical operators **and**, **or**, and **not**. To reduce the expressions that define the filters, identical qualifier lists may be omitted.

Filter examples:

dst foo — filters packets which IPv4/v6 recipient address field contains foo host address.

src net 128.3.0.0/16 — filters all Ipv4/v6 packets sent from the specific network.

ether broadcast — enables filtering of all Ethernet broadcasting frames. Keyword 'ether' may be omitted.

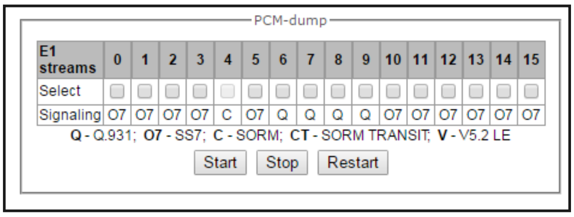
ip6 multicast — filters packets with IPv6 group addresses.

For detailed information on packet filtering, see specialized resources

- *Start* — begin data collection.
- *Finish* — finish data collection.
- *Restart* — restart utility, begin data collection again.

PCM–dump — PCM–dump utility settings.

PCMdump is a utility for E1 stream signaling traffic interception and analysis. The device features PCM-dumping either for a single stream or for multiple streams; for PCM-dumping for multiple streams simultaneously, tracing will be written to a single file that will contain signaling messages from multiple streams; at that, simultaneous PCM-dumping for streams with different signaling protocols is not available.



E1 streams	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Select	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Signaling	O7	O7	O7	O7	C	O7	Q	Q	Q	Q	O7	O7	O7	O7	O7	O7

Q - Q.931; **O7** - SS7; **C** - SORM; **CT** - SORM TRANSIT; **V** - V5.2 LE

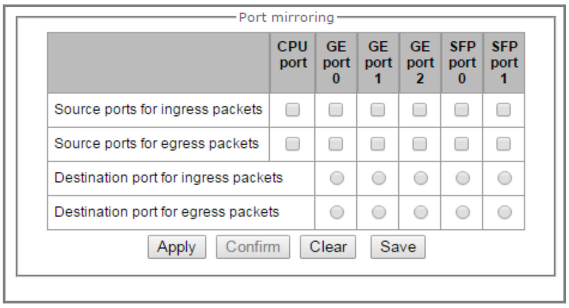
- *Select* — select E1 streams.
- *Signaling* — signaling protocol selected for the stream:
  - SS7

- Q.931-N
- Q.931-U
- V5.2

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

Port mirroring*[1] *— traffic mirroring settings:

Port mirroring enables copying of sent and received frames from the gateway switch ports and their forwarding to another port.



Port mirroring

	CPU port	GE port 0	GE port 1	GE port 2	SFP port 0	SFP port 1
Source ports for ingress packets	□	□	□	□	□	□
Source ports for egress packets	□	□	□	□	□	□
Destination port for ingress packets		○	○	○	○	○
Destination port for egress packets		○	○	○	○	○

For device ports, available operations are as follows:

- *Source ports for ingress packets* — copy frames received from this port (source port).
- *Source ports for egress packets* — copy frames sent by this port (source port).
- *Destination port for ingress packets* — destination port for copied frames received by selected source ports.
- *Destination port for egress packets* — destination port for copied frames sent by selected source ports.
- *Apply* — apply mirroring setting parameters.
- *Confirm* — confirm applied mirroring setting parameters.
- *Clear* — reset mirroring settings.
- *Save* — save mirroring setting parameters.

Click 'Confirm' button in 1 minute interval to confirm settings, or the previous values will be restored.

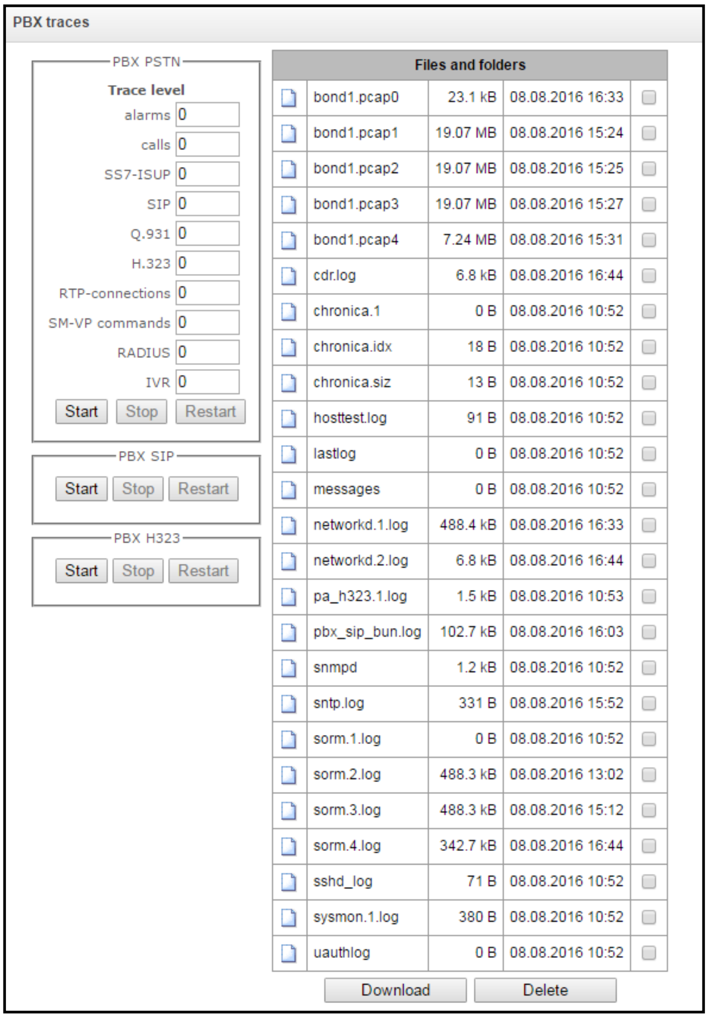
The **'Files and folders in tracing directory'** block features the list of tracing files.

To download it to a local PC, select the checkboxes located next to the required filenames and click *'Download'* button. To delete the specific files from the directory, click 'Delete'.

[1] For SMG-1016M only

3.1.16.2 PBX tracing

Utilization of IP PBX tracing leads to delays in the device operation. This debug mode is RECOMMENDED only when problems in gateway operation occur, and you have to identify the reason.



PBX traces

PBX PSTN

Trace level	
alarms	0
calls	0
SS7-ISUP	0
SIP	0
Q.931	0
H.323	0
RTP-connections	0
SM-VP commands	0
RADIUS	0
IVR	0

Files and folders			
bond1.pcap0	23.1 kB	08.08.2016 16:33	□
bond1.pcap1	19.07 MB	08.08.2016 15:24	□
bond1.pcap2	19.07 MB	08.08.2016 15:25	□
bond1.pcap3	19.07 MB	08.08.2016 15:27	□
bond1.pcap4	7.24 MB	08.08.2016 15:31	□
cdr.log	6.8 kB	08.08.2016 16:44	□
chronica.1	0 B	08.08.2016 10:52	□
chronica.idx	18 B	08.08.2016 10:52	□
chronica.siz	13 B	08.08.2016 10:52	□
hosttest.log	91 B	08.08.2016 10:52	□
lastlog	0 B	08.08.2016 10:52	□
messages	0 B	08.08.2016 10:52	□
networkd.1.log	488.4 kB	08.08.2016 16:33	□
networkd.2.log	6.8 kB	08.08.2016 16:44	□
pa_h323.1.log	1.5 kB	08.08.2016 10:53	□
pbx_sip_bun.log	102.7 kB	08.08.2016 16:03	□
snmpd	1.2 kB	08.08.2016 10:52	□
sntp.log	331 B	08.08.2016 15:52	□
sorm.1.log	0 B	08.08.2016 10:52	□
sorm.2.log	488.3 kB	08.08.2016 13:02	□
sorm.3.log	488.3 kB	08.08.2016 15:12	□
sorm.4.log	342.7 kB	08.08.2016 16:44	□
sshd_log	71 B	08.08.2016 10:52	□
sysmon.1.log	380 B	08.08.2016 10:52	□
uauthlog	0 B	08.08.2016 10:52	□

In **PBX PSTN** block, device components operation and interaction log is recorded and message exchange via various protocols is collected. In PBX PSTN parameters, you may configure tracing level for various events and protocols.

In **PBX IP** block, SIP error and message tracing is collected.

- *Start* — begin data collection.
- *Stop* — finish data collection.
- *Restart* — restart, begin data collection again.

In **PBX H323** block, H323 error and message tracing is collected.

- *Start* — begin data collection.
- *Stop* — finish data collection.
- Restart — restart, begin data collection again.

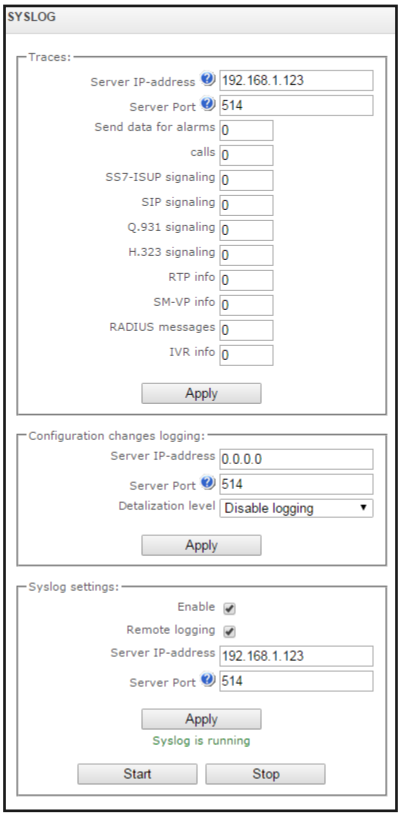
When data collection is stopped, buttons will appear that allow to download tracing files to a local PC.

The **'Files and folders in tracing directory'** block features the list of files in the respective tracing directory.

To download files to a local PC, select the checkboxes located next to the required filenames and click *'Download'* button. To delete the specific files from the directory, click *'Delete'*.

3.1.16.3 Syslog settings

In *'SYSLOG'* menu, you may configure system log settings.


SYSLOG

Traces:

Server IP-address 192.168.1.123
Server Port 514
Send data for alarms 0
calls 0
SS7-ISUP signaling 0
SIP signaling 0
Q.931 signaling 0
H.323 signaling 0
RTP info 0
SM-VP info 0
RADIUS messages 0
IVR info 0

Configuration changes logging:

Server IP-address 0.0.0.0
Server Port 514
Detalization level Disable logging

Syslog settings:

Enable ☑
Remote logging ☑
Server IP-address 192.168.1.123
Server Port 514

Syslog is running

SYSLOG is a protocol, designed for transmission of messages on current system events. Gateway software generates system data logs on operation of system applications and signaling protocols, as well as occurred failures and sends them to SYSLOG server.

High debug levels may cause delays in operation of the device.
IT IS NOT RECOMMENDED to use system log without due cause.

System log should be used only when problems in gateway operation occur, and you have to identify the reason. To define the necessary debug levels, consult an Eltex Service Centre specialists.

Tracings — allows to save the log of device components operation and interaction, as well as message exchange via various protocols.

In tracing parameters, you may configure tracing level for various events and protocols. Possible levels are as follows: 0 — disabled, 1–99 — enabled. 1 — minimum debug level, 99 — maximum debug level.

- *Server IP address* — server address that the tracing will be sent to.
- *Server port* — server port that the tracing will be sent to.

Configuration changes logging — allows to save the history of the gateway setting changes.

- *Server IP address* — server address that the entered commands log will be sent to.
- *Server port* — server port that the entered commands log will be sent to.
- *Detalization level* — verbosity level of the entered commands log:
  - Disable logging — disable entered commands logs generation.
  - Standard — messages contain the name of modified parameter.
  - Extended — messages contain the name of modified parameter as well as parameter values before and after the modification.

Syslog settings — system log configuration settings for transmission of the device access events.

- *Enable* — when checked, device access event history will be saved; when unchecked, logging will be disabled.

- *Remote logging* — when checked, system log will be saved on server located at the specified address.
- *Server IP address* — address of a server for system log storage.
- *Server port* — server port that the system log will be sent to.

3.1.17 Call recording

Use this menu to set conversation recording[1].

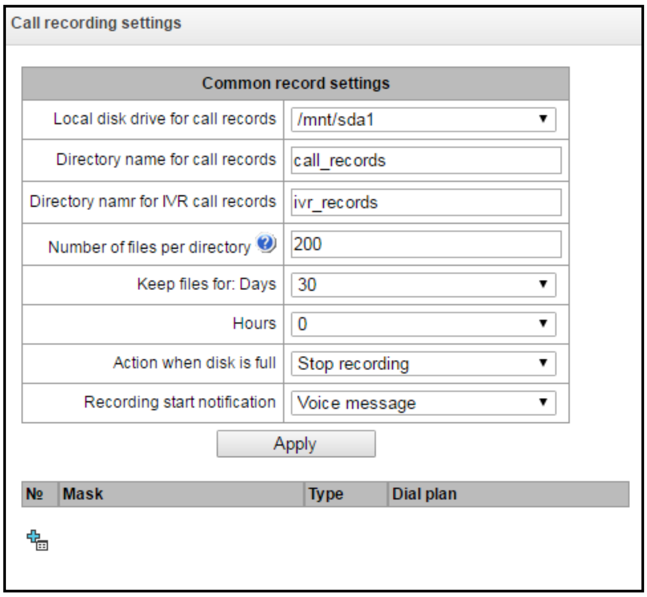
The SMG can record several calls simultaneously. The number of calls which can be recorded simultaneously depends on the type of connections. Check the table below before the configuration:

Type of connection	1 submodule SM-VP-M300	6 sumbodules SM-VP-M300
E1 - E1	27	162
E1 - SIP	22	132
SIP - SIP	20	120

The recorded calls can be uploaded to FTP server. In this case, the records are saved on a local storage and then, by schedule, are sent to FTP server.

We do not recommend to record calls to USB storage when there are a large amount of calls. The bandwidth of the interface is not sufficient for simultaneous record of many calls, it leads to increase in input-output buffers in RAM and may cause the gateway operation problems.

3.1.17.1 Call recording settings



Call recording settings

Common record settings	
Local disk drive for call records	/mnt/sda1 ▾
Directory name for call records	call_records
Directory namr for IVR call records	ivr_records
Number of files per directory	200
Keep files for: Days	30 ▾
Hours	0 ▾
Action when disk is full	Stop recording ▾
Recording start notification	Voice message ▾

[1] The menu is available for the devices with Call-record license. Read more detailed information on licenses in the section 3.1.23 Licenses.

Common record settings:

- *Local disk drive for call records* — select available storage device for saving conversation records.
- *Directory name for call records* — directory name for saving conversation records; if the folder name is not specified, conversation records will be saved to the root directory of the storage device.
- *Directory name for IVR call records* — directory name for saving conversation records, when call comes to REC block in IVR scenario.
- *Number of files per directory* — maximum number of conversation record files in a single directory; when this number is achieved, a new directory will be created.

In the conversation records directory, a new subdirectory will be created each day with 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.

When the 'Number of files per directory' value is achieved, device will create a new directory with NNNN value increases by 1.

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) — time period during which conversation records will be kept on the storage device; when it expires, obsolete files will be removed.
- Action when disk is full — select an action that will be applied to conversation record files when the disk is full:
  - Stop recording — stop generation of new recordings when the disk is full.
  - Delete obsolete records — delete obsolete recordings when the disk is full.

FTP server settings:

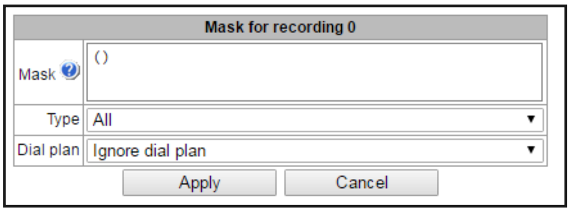
- Store files on FTP – when checked, the records of calls are uploaded to the FTP server automatically according to defined upload mode;
- Upload mode – defines periodicity of files uploading:
  - *once per day* – upload once a day in specified time;
  - *once per hour* – upload once an hour;
  - *once per minute* – upload once a minute.
- *Hours* – available in "once per day" upload mode. Select an hour of uploading the files.
- *Minutes* – available in "once per day" upload mode. Select minutes to upload the files.
- *Server address/hostname* – IP address or domain name of FTP to which recorded calls will be uploaded.
- *Server port* – FTP server port;
- *Path on server* – path to the stored files on an FTP server.
- *Login* – a name (login) for authorization;
- *Password* – a password for authorization;
- *Remove files after upload* – if checked, the files will be deleted from the local storage of SMG after sending to FTP server.

Filter masks for conversation recording:

Device identifies the necessity of conversation recordings for CgPN and CdPN numbers.

- *Mask* — number filtering mask; for mask syntax, see Section 3.1.6.2 Number mask description and its syntax.
- Type — search for mask matches to CdPN or CgPN number.

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



Mask for recording 0

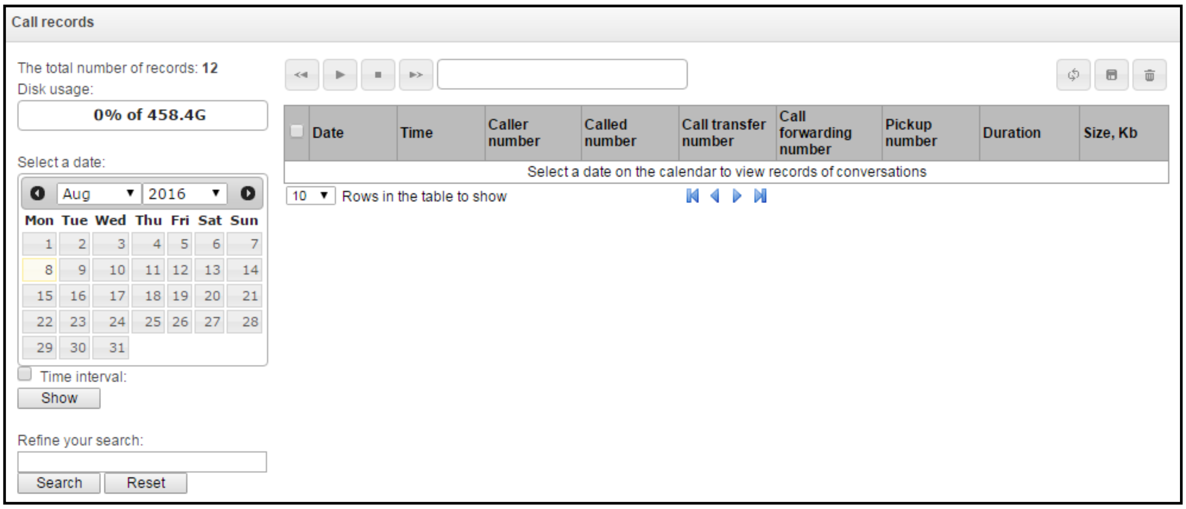
Mask	()
Type	All
Dial plan	Ignore dial plan

  - *All* – search by CgPN and CdPN numbers;
  - *Calling* — search for CgPN number matches only.
  - *Called* — search for CdPN number matches only.
- *Dial plan* – define a dial plan through which the record mask will operate. If you choose "Ignore dial plan", the search will be implemented through all the active dial plans.
- *Recording start notification* – notification on start of recording:
  - *None* – disable notification on start of recording;
  - *Voice message* – notify on start of recording by voice message.

- *Call record category* – a category which will be assigned to a record under the defined mask.

3.1.17.2 Call records

This section enables management of conversation recording files.



Call records

The total number of records: **12**

Disk usage:

0% of 458.4G

Select a date:

Aug ▾ 2016 ▾

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

□ Time interval:

Show

Refine your search:

Search Reset

□	Date	Time	Caller number	Called number	Call transfer number	Call forwarding number	Pickup number	Duration	Size, Kb
Select a date on the calendar to view records of conversations									

10 ▾ Rows in the table to show

- *The total number of records* — total quantity of conversation recording files in the selected directory for conversation recordings.
- *Disk usage* — display used space on disk selected for conversation recording.
- *User record category* – displays a category of call record which the current user has;
- *Select a date* — select a date to display the conversation recording files.
- *Time interval* — select time interval to display the conversation recording files.
- *Search* — search for conversation recording files; search function uses any matches of the entered value to conversation recording file name.

For record control buttons description, see Table below.

Table 26 — Record control buttons

Button	***Function***
◂◂	previous record
▶	begin playback
■	stop playback
▸▸	next record
⟲	repeat record playback
💾	save record
🗑	delete record

The table columns description

– *Date/time* – date and time of record start;

- *Caller number/Called number* – numbers of the subscribers participated in the recorded conversation;
- *Dial plan* – a dial plan in which the record was taken;
- *Category* – call record category;
- *FTP* – shows whether the record was uploaded to FTP;
- *Duration* – conversation duration;
- *Size, KB* – the size of the record in kilobytes.

Conversation recording file format

1. A common call without call redirection 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 — caller name, if it is missing, value 'none' will be used.
CdPN — callee number.
nX – a number of dial plan in which the record was taken;
cX – call record category.
Example:
Subscriber 40010 calls Subscriber 40012, file name should be as follows:
2017-10-23_09-27-26_40010-40012_n0_c0.wav

2. A call that uses call redirection service

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 — caller name, if it is missing, value 'none' will be used.
CdPN — callee number — a number that the call is actually comes to.
cf — marker indicating that call forwarding has taken place.
ct — the call has been forwarded;
cp — the call has been picked up;

SrvNum – a number which used in the value added service. Depending on the meaning of **Srv** tag, SrvNum means number to which the call was forwarded or from which it was transferred or picked up.

nX — a number of dial plan in which the record was taken;
cX — call record category.

Example:
Subscriber 40010 calls Subscriber 40011 that has configured a call redirection to 40012.
2017-10-23_09-28-04_40010-40011_cf_40012_n0_c0.wav

3. A call that uses call transfer service

Call transfer service engages 3 subscribers — call initiating subscriber (Subscriber A), call transferring subscriber (Subscriber B) and transferred call recipient subscriber (Subscriber C).
For call transfer, 3 conversation recording files will be created.
Subscriber A — Subscriber B conversation
Subscriber B — Subscriber C conversation

Subscriber A — Subscriber C conversation after the call transfer

Example:
Subscriber 40012 calls Subscriber 40010 that transfers the call to Subscriber 40000.

The following files will be created:

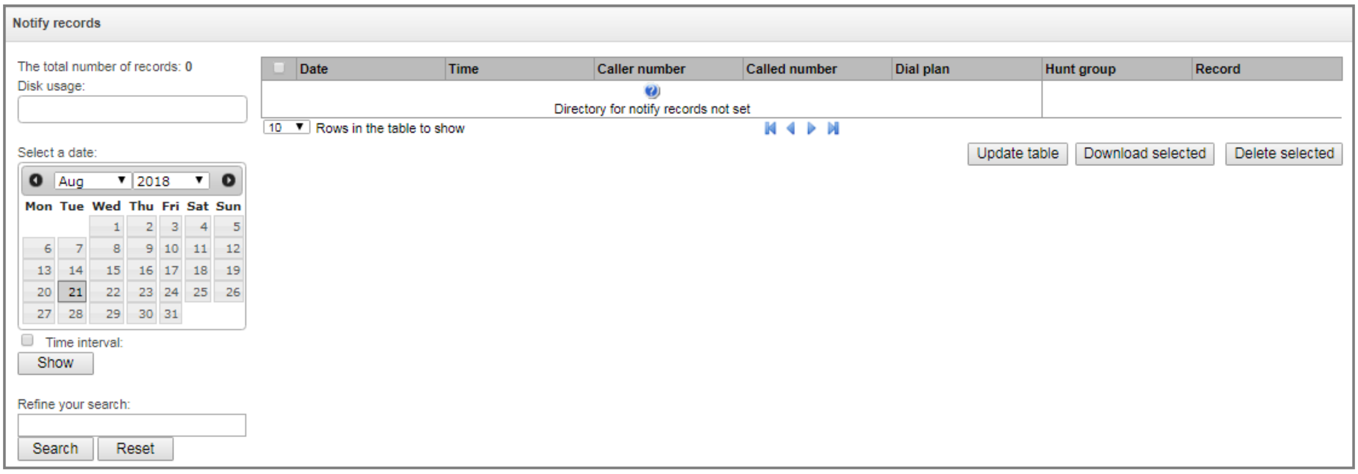
2017-10-23_10-15-19_40012-40010_n0_c0.wav — Subscriber A — Subscriber B conversation.

2017-10-23_10-15-31_40010-40000_n0_c0.wav — Subscriber B — Subscriber C conversation after the Subscriber B has put the Subscriber A on hold.

2017-10-23_10-15-19_40012-40010_ct_40000_n0_c0.wav — Subscriber A — Subscriber C conversation after the call transfer by Subscriber B; ct in the file name is a call transfer marker.

3.1.17.3 Notify records

The section is dedicated to manage recorded notification files.



Notify records

The total number of records: 0
Disk usage:

□	Date	Time	Caller number	Called number	Dial plan	Hunt group	Record

Directory for notify records not set

10 Rows in the table to show

Select a date:

Aug 2018

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

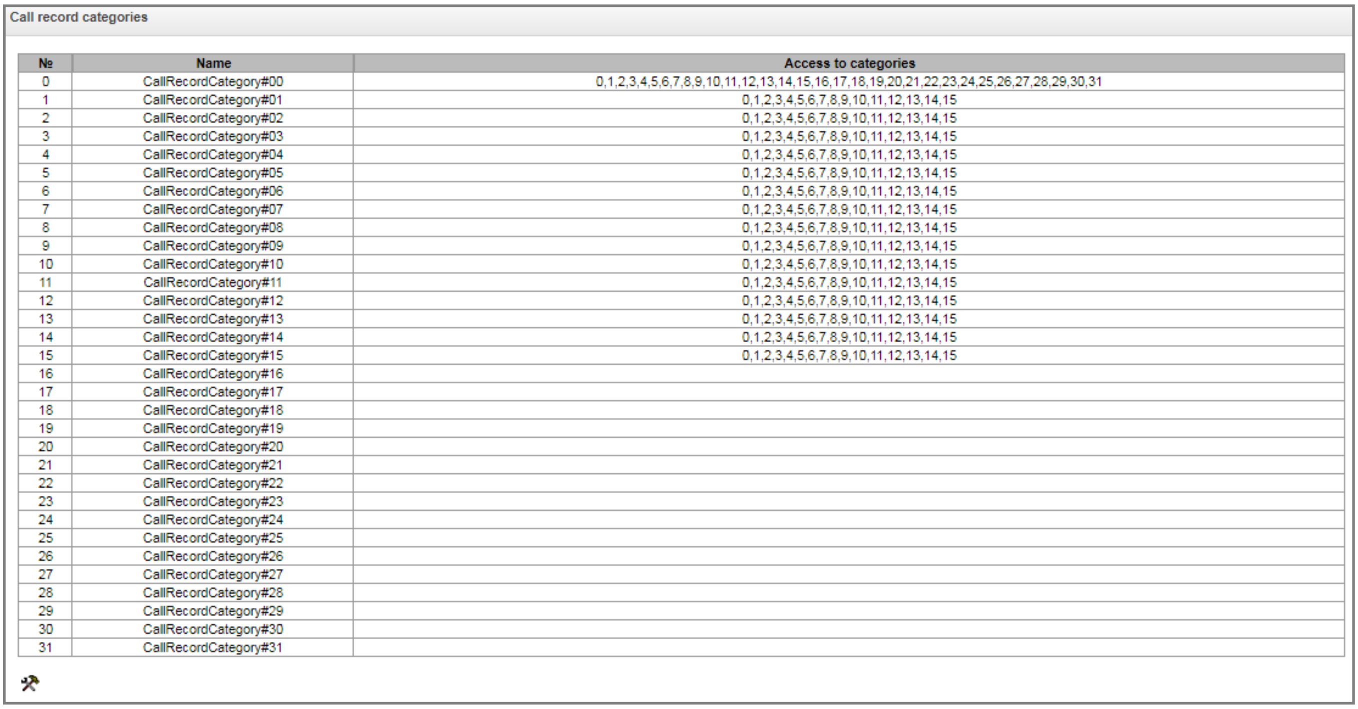
□ Time interval:

Refine your search:

- *The total number of records* – the total number of recorded notifications in the selected call record catalogue.
- *Disk usage* – displays space used on the selected storage for recording of notifications.
- *Select a date* – select a date for displaying notifications files.
- *Time interval* – select a time interval for displaying notifications files .
- *Refine your search* – search files with recorded notifications, the search is implemented by any match of the entered value with the name of the call record file.

Each entry in the "Date" column is a link to a notification log. The log contains the descriprion of notification process and its result. You may listen to the notification by pressing a link in the "Record" column. Here, you may download the record – click the pictogram next to the record.

3.1.17.4 *Call records category*

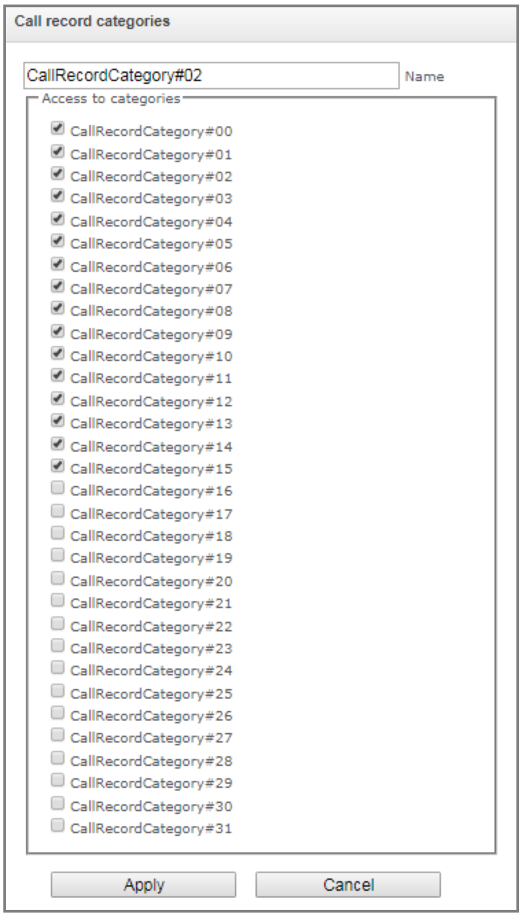


Call record categories

№	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	

The call categories are used to define access rights to the recorded conversations.

If you need to limit access to some records, you should assign them a special category. Define the availability of categories by pressing ⚒ button. Check the boxes to select necessary categories.



Call record categories

Name: CallRecordCategory#02

Access to categories

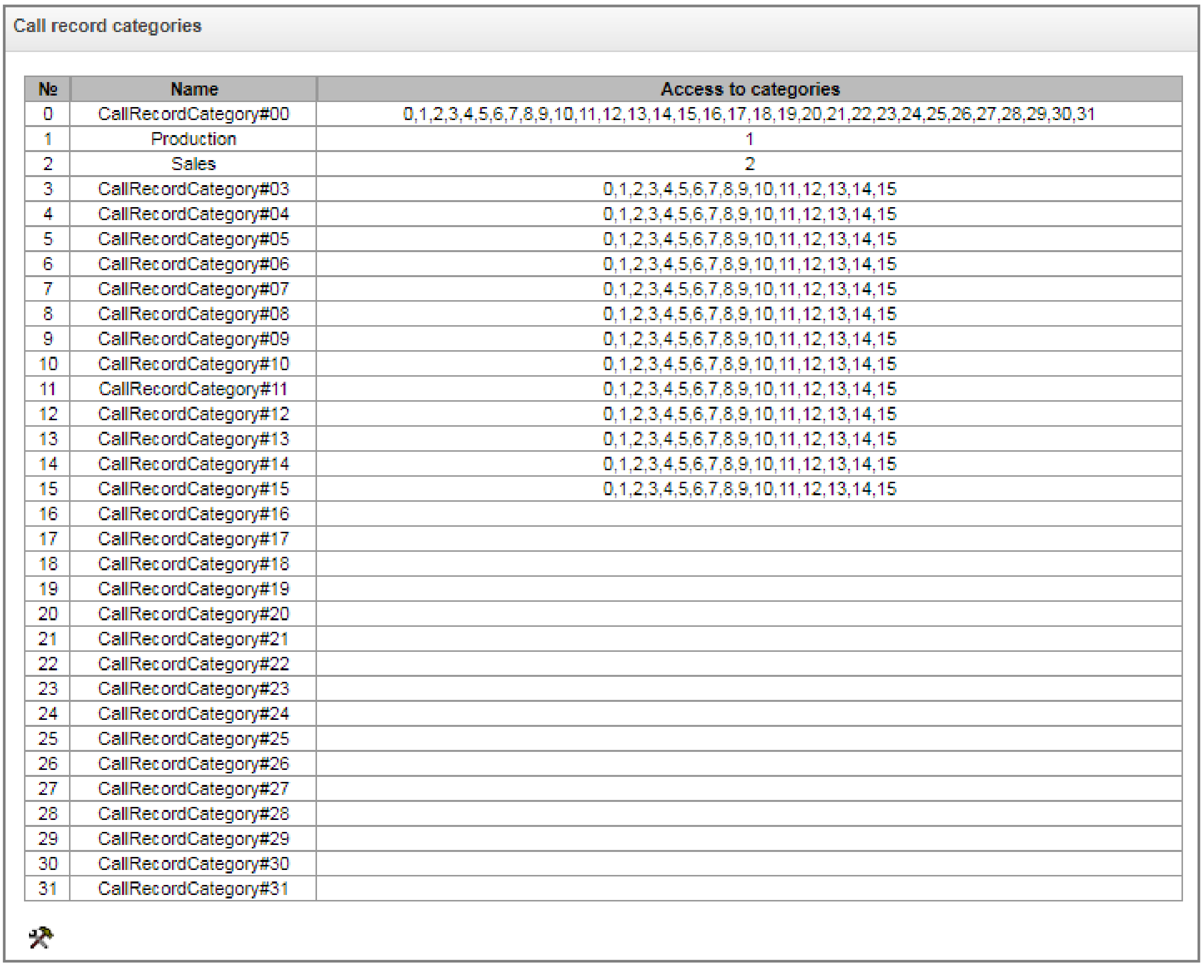
☑ CallRecordCategory#00
☑ CallRecordCategory#01
☑ CallRecordCategory#02
☑ CallRecordCategory#03
☑ CallRecordCategory#04
☑ CallRecordCategory#05
☑ CallRecordCategory#06
☑ CallRecordCategory#07
☑ CallRecordCategory#08
☑ CallRecordCategory#09
☑ CallRecordCategory#10
☑ CallRecordCategory#11
☑ CallRecordCategory#12
☑ CallRecordCategory#13
☑ CallRecordCategory#14
☑ CallRecordCategory#15
☐ CallRecordCategory#16
☐ CallRecordCategory#17
☐ CallRecordCategory#18
☐ CallRecordCategory#19
☐ CallRecordCategory#20
☐ CallRecordCategory#21
☐ CallRecordCategory#22
☐ CallRecordCategory#23
☐ CallRecordCategory#24
☐ CallRecordCategory#25
☐ CallRecordCategory#26
☐ CallRecordCategory#27
☐ CallRecordCategory#28
☐ CallRecordCategory#29
☐ CallRecordCategory#30
☐ CallRecordCategory#31

You may configure 32 record categories. The category 0 has unchangeable access to all the categories by default and dedicated to admin account which has access to all the calls. The other categories have configurable access. The first 15 categories have access to the first 16 categories.

Example of configuring the access to call records

Let us consider the example of access delimitation between production and sales department. Each user must have access only to records made in their department. To limit the access:

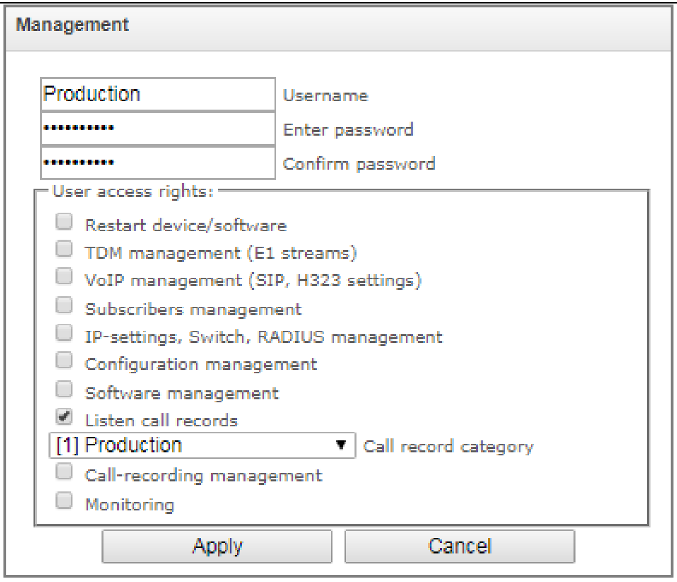
1. Select the call record category from the list. You may rename it as "Production" and "Sales". Set only their own categories to each department:



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	Production	1
2	Sales	2
3	CallRecordCategory#03	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
4	CallRecordCategory#04	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
5	CallRecordCategory#05	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
6	CallRecordCategory#06	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
7	CallRecordCategory#07	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
8	CallRecordCategory#08	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
9	CallRecordCategory#09	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
10	CallRecordCategory#10	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
11	CallRecordCategory#11	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
12	CallRecordCategory#12	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
13	CallRecordCategory#13	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
14	CallRecordCategory#14	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
15	CallRecordCategory#15	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
16	CallRecordCategory#16	
17	CallRecordCategory#17	
18	CallRecordCategory#18	
19	CallRecordCategory#19	
20	CallRecordCategory#20	
21	CallRecordCategory#21	
22	CallRecordCategory#22	
23	CallRecordCategory#23	
24	CallRecordCategory#24	
25	CallRecordCategory#25	
26	CallRecordCategory#26	
27	CallRecordCategory#27	
28	CallRecordCategory#28	
29	CallRecordCategory#29	
30	CallRecordCategory#30	
31	CallRecordCategory#31	

2. Move to accounts management (see section 3.1.25 paragraph "Web interface users"). In the users rights check the "Listen call records" box and set the necessary category ("production" for "production" user and "sales" for "sales" user):

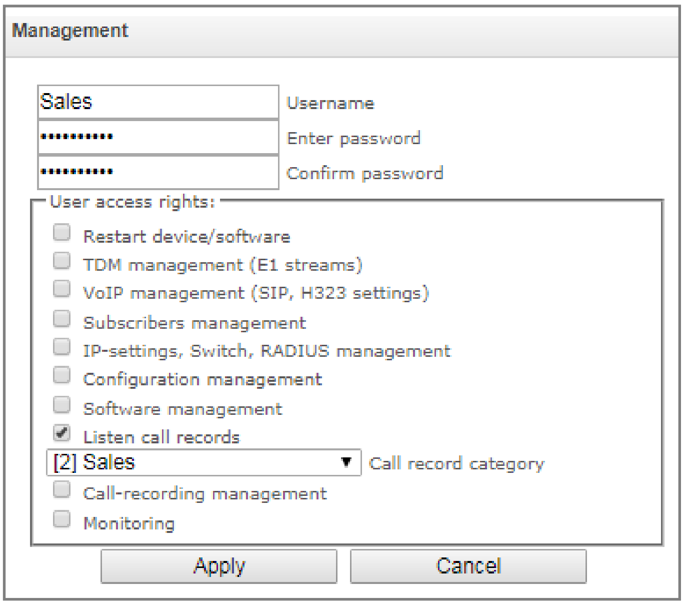


Management

Production	Username
••••••••••	Enter password
••••••••••	Confirm password

User access rights:

□ Restart device/software
□ TDM management (E1 streams)
□ VoIP management (SIP, H323 settings)
□ Subscribers management
□ IP-settings, Switch, RADIUS management
□ Configuration management
□ Software management
☑ Listen call records
[1] Production ▼ Call record category
□ Call-recording management
□ Monitoring



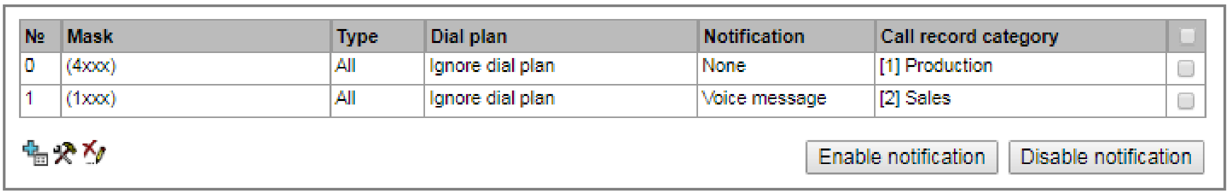
Management

Sales	Username
••••••••••	Enter password
••••••••••	Confirm password

User access rights:

□ Restart device/software
□ TDM management (E1 streams)
□ VoIP management (SIP, H323 settings)
□ Subscribers management
□ IP-settings, Switch, RADIUS management
□ Configuration management
□ Software management
☑ Listen call records
[2] Sales ▼ Call record category
□ Call-recording management
□ Monitoring

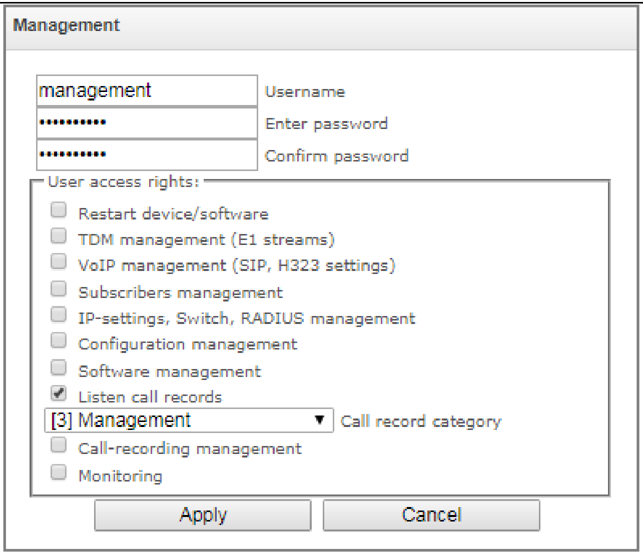
3. In the "Call recording settings" add masks for numbers of production and sales department and set the corresponding call record categories.



№	Mask	Type	Dial plan	Notification	Call record category	□
0	(4xxx)	All	Ignore dial plan	None	[1] Production	□
1	(1xxx)	All	Ignore dial plan	Voice message	[2] Sales	□

4. Now, if a user enter in "Call recording" section, he will see records to which he has the access.

5. If you need to add a user, for example "management", which will have access to all the departments records, add a new category and set access rights to "Production" and "Sales" category. And assign the access to "management" call record category in the "management" tab.



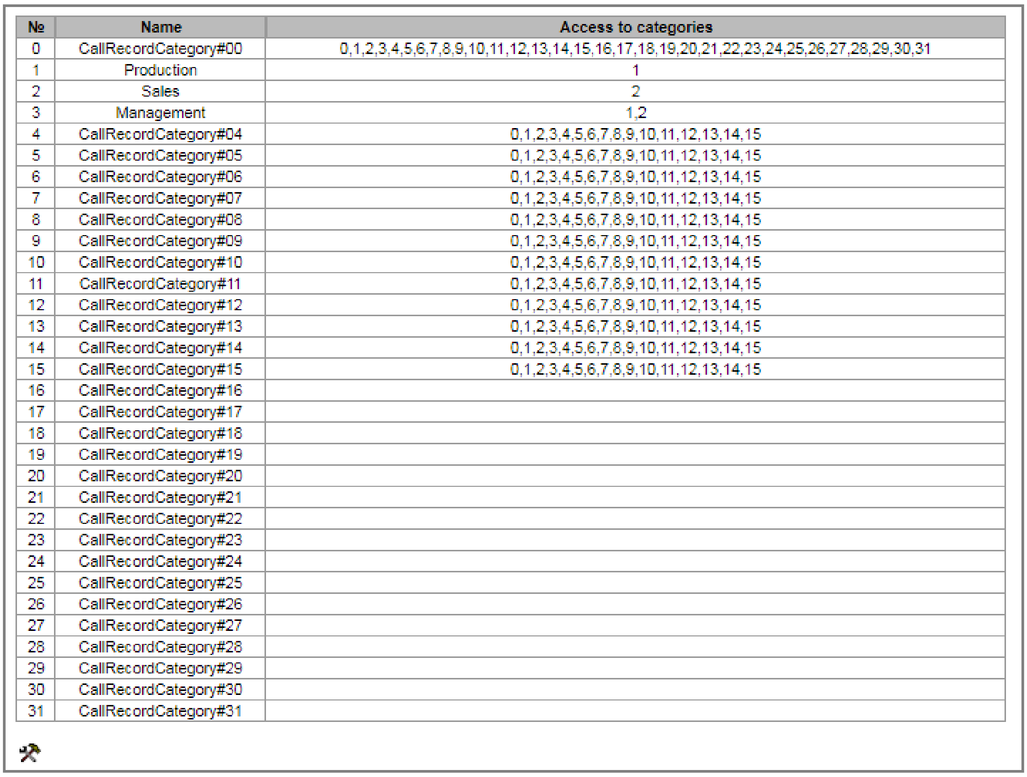
Management

management	Username
••••••••••	Enter password
••••••••••	Confirm password

User access rights:

- □ Restart device/software
- □ TDM management (E1 streams)
- □ VoIP management (SIP, H323 settings)
- □ Subscribers management
- □ IP-settings, Switch, RADIUS management
- □ Configuration management
- □ Software management
- ☑ Listen call records
- [3] Management ▼ Call record category
- □ Call-recording management
- □ Monitoring

As the result, the call record categories table is displayed as follows:



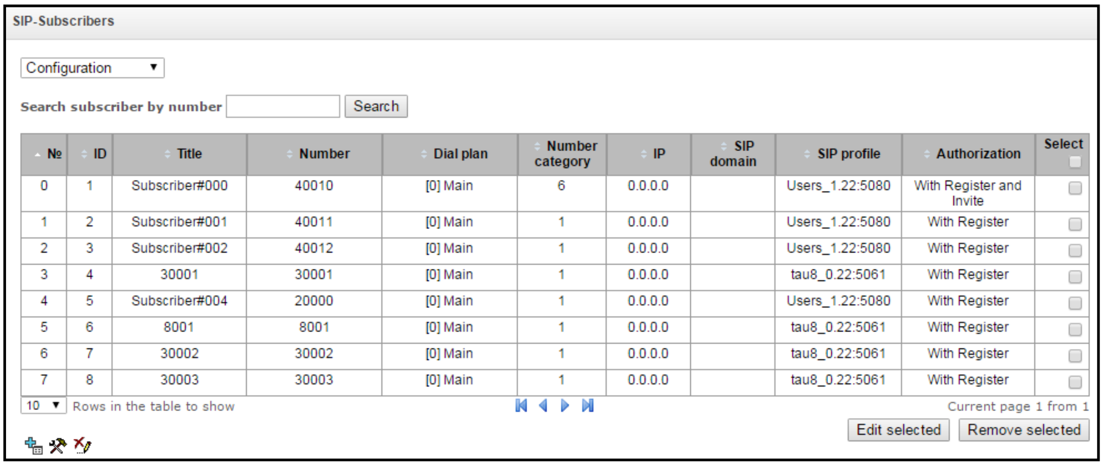
№	Name	Access to categories
0	CallRecordCategory#00	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31
1	Production	1
2	Sales	2
3	Management	1,2
4	CallRecordCategory#04	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
5	CallRecordCategory#05	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
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	

3.1.18 Subscribers

In this menu, you may configure SIP subscribers[1].

3.1.18.1 SIP subscribers

3.1.18.1.1 Subscriber configuration



SIP-Subscribers

Configuration ▾

Search subscriber by number [ ] Search

№	ID	Title	Number	Dial plan	Number category	IP	SIP domain	SIP profile	Authorization	Select □
0	1	Subscriber#000	40010	[0] Main	6	0.0.0.0		Users_1.22:5080	With Register and Invite	□
1	2	Subscriber#001	40011	[0] Main	1	0.0.0.0		Users_1.22:5080	With Register	□
2	3	Subscriber#002	40012	[0] Main	1	0.0.0.0		Users_1.22:5080	With Register	□
3	4	30001	30001	[0] Main	1	0.0.0.0		tau8_0.22:5061	With Register	□
4	5	Subscriber#004	20000	[0] Main	1	0.0.0.0		Users_1.22:5080	With Register	□
5	6	8001	8001	[0] Main	1	0.0.0.0		tau8_0.22:5061	With Register	□
6	7	30002	30002	[0] Main	1	0.0.0.0		tau8_0.22:5061	With Register	□
7	8	30003	30003	[0] Main	1	0.0.0.0		tau8_0.22:5061	With Register	□

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

Edit selected   Remove selected

- *Search subscriber by number* — subscriber number availability check against configured SIP subscriber database.

- *Edit selected* — click this button to enter the group editing menu for the selected subscribers' parameters (with *'Select'* checkbox selected next to them). To enable editing, select *'Modify'* checkbox next to the required parameter. For configuration parameters' description, see below.

- *Remove selected* — click this button to perform the group removal of the selected subscribers.

To create, edit or remove a record of a single subscriber, use *'Objects'* — *'Add object'*, *'Objects'* — *'Edit object'* and *'Objects'* — *'Remove object'* menus and the following buttons:

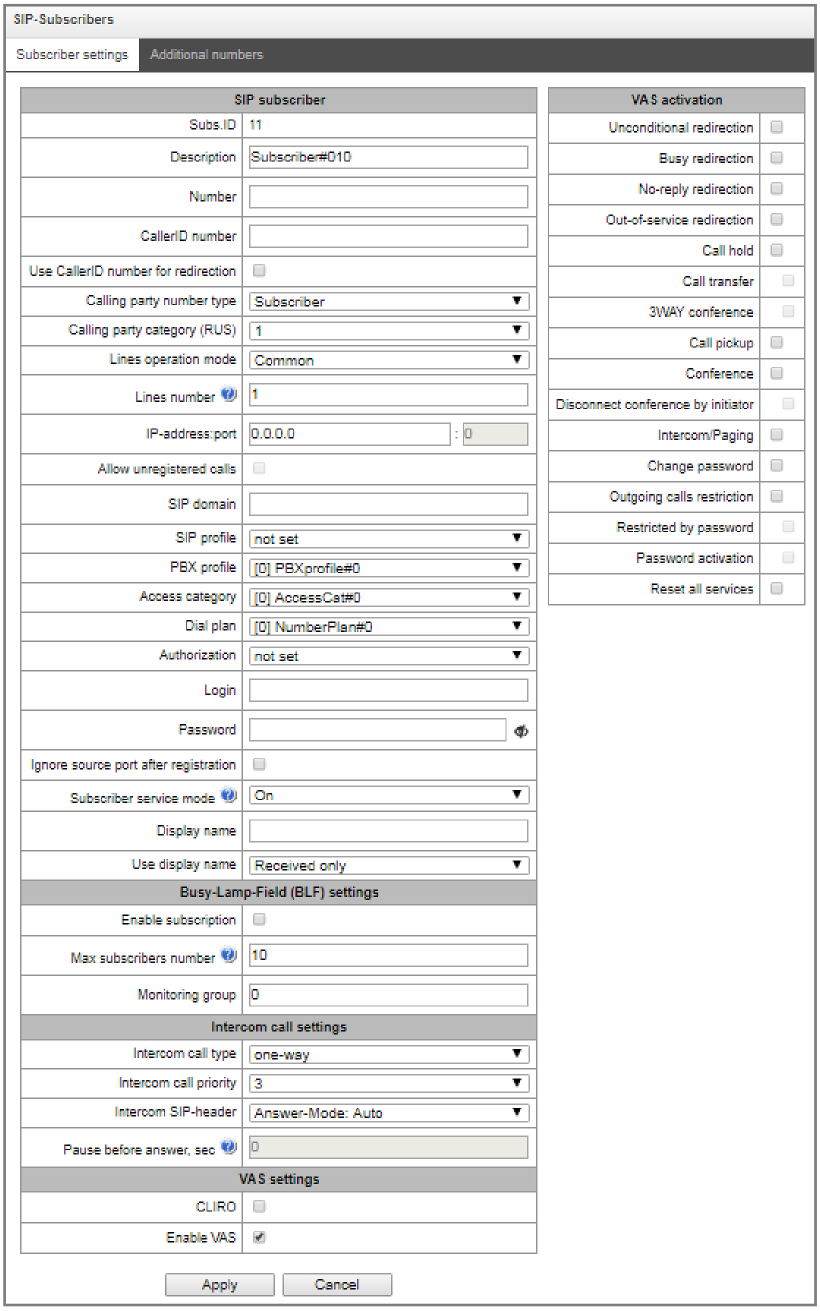
— *'Add subscriber'*

— *'Edit subscriber parameters'*

— *'Remove subscriber'*

[1] The menu is available for the devices with SIP registrar license. Read more detailed information on licenses in the section 3.1.23 Licenses.

3.1.18.1.1.1 Subscriber settings



SIP-Subscribers

Subscriber settings | Additional numbers

SIP subscriber	
Subs.ID	11
Description	Subscriber#010
Number	
CallerID number	
Use CallerID number for redirection	□
Calling party number type	Subscriber
Calling party category (RUS)	1
Lines operation mode	Common
Lines number	1
IP-address:port	0.0.0.0 : 0
Allow unregistered calls	□
SIP domain	
SIP profile	not set
PBX profile	[0] PBXprofile#0
Access category	[0] AccessCat#0
Dial plan	[0] NumberPlan#0
Authorization	not set
Login	
Password	
Ignore source port after registration	□
Subscriber service mode	On
Display name	
Use display name	Received only
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	☑

VAS activation	
Unconditional redirection	□
Busy redirection	□
No-reply redirection	□
Out-of-service redirection	□
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	□
Reset all services	□

- *Subs. ID* — a unique subscriber's identifier.
- *Description* — arbitrary subscriber text description.
- *Number* — subscriber's number; for a group of subscribers, 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* – if checked, the CallerID number will be set instead of a subscriber number in Diversion or Redirecting number.
- *Calling party number type* — subscriber number type.
- *Calling party category (RUS)* — subscriber's Caller ID category.

- *Lines operation mode* – limit the number of simultaneous calls. Two options are available: «Common» and «Separate». In «Common» mode all simultaneous calls are taken into account, in «Separate» mode incoming and outgoing calls are counted separately.
- *Ingress lines number*[1] – the number of simultaneous incoming calls. The field is available only in the «Separate» mode. Permitted value range is [1;255] or 0 — unlimited.
- *Egress lines number*[1] – the number of simultaneous outgoing calls. The field is available only in the «Separate» mode. Permitted value range is [1;255] or 0 — unlimited.
- *Lines number* — quantity of calls that the subscriber may take part in simultaneously. Field is available only in the «Common» mode. Permitted value range is [1;255] or 0 — unlimited.
- *IP address:Port* — subscriber IP address and port. When value 0.0.0.0 is defined, subscriber is allowed to register using any IP address.
- *Allow unregistered calls* – the option is available if an IP address and a port are set in the previous field. If checked, a subscriber can hold a call through specified IP address and port without registration in advance.
- *SIP domain* — identifies the subscriber inherence to a specific domain. Sent by the subscriber's gateway in *from* and *to* fields of the *'host'* parameter of SIP URI scheme.
- *SIP profile* — select SIP profile. SIP profile defines the majority of subscriber's settings (see 3.1.7.3 SIP/SIP-T/SIP-I interfaces, SIP profiles).
- *PBX profile* — select PBX profile (see Section 3.1.8.3 PBX profiles).
- *Access category* — select access category.
- *Dial plan* — defines the dial plan that the subscriber will belong to.
- *Authorization* — defines authentication mode for the device*:*
  - Not set — authentication is disabled.
  - With REGISTER — authentication is performed on registration only — using REGISTER request.
  - With REGISTER and INVITE — authentication is performed on registration as well as when performing outgoing calls — using REGISTER and INVITE requests.
- *Login* — username for authentication.
- *Password* — password for authentication.
- *Ignore source port after registration* — after registration, subscriber messages might be transmitted through any port of registered address.
- *Subscriber service mode* — defines restrictions on the incoming and outgoing communication for the subscriber:
  - off: out of service. Number of a subscriber is in a dial plan, but subscriber terminal cannot be registered. Thus, incoming calls will be barred with 'out of order' cause and egress calls cannot be initiated.
  - on: all communication types are available.

[1] The settings are available when "separate" line operation mode is set

- off 1: incoming communication is enabled, outgoing communication is available only for calls to emergency services.
- off 2: incoming communication is disabled, outgoing communication is available only for calls to emergency services.
- denied 1: full barring for incoming and outgoing calls. Calls will be routed according to dial plans, but will be rejected;
- denied 2: full barring for incoming and outgoing calls except for the calls to emergency services.
- denied 3: incoming calls are barred, outgoing calls are permitted.
- denied 4: incoming calls are barred, outgoing calls are permitted only for local and private communication.
- denied 5: incoming calls are permitted, full barring for outgoing calls.
- denied 6: incoming calls are permitted, outgoing calls are permitted to emergency services only.
- denied 7: incoming calls are permitted, outgoing calls are permitted only for local and private communication.
- denied 8: incoming calls are permitted, outgoing calls are permitted only for local, private and zone communication.
- ignore: excluded from the numbering. The number is completely excluded from the subscriber numbers of the dial plan. The ingress calls are barred with 'no route to destination' cause or transmitted to appropriate prefix in a dial plan.

- *Display name* – a name which will be transmitted in display-name.

- *Use display name* – display-name operation mode (SIP display-name):

  - *Received only* – the display-name setting will not be used, the display-name will have the value which was in an initiated INVITE request.
  - *Received prefer* – if the request on initiation of a call is received without display-name, the display-name will be set as it is defined on SMG. Otherwise, the name received in the INVITE will be used.
  - *Configured only* – the display-name configured on SMG will always be used in spite of the display-name value in an INVITE request.

Busy-Lamp-Field (BLF) settings

- *Enable subscription* – allows client to subscribes itself for BLF events of another clients;

- *Max subscribers number* – quantity of observable numbers when BLF service is enabled;

- *Monitoring group* –BLF monitoring group, clients incoming in the same monitoring group can realize monitoring between each other.

Directions (*local network, special service, zone network, private network, long-distance network, international network*) are specified during prefix configuration in the dial plan, *'Direction'* field.

Intercom call settings

- *Intercom call type* — incoming intercom call type (with the Subscriber B automatic reply):

  - *One-way* — during incoming intercom call, Subscriber B will hear the Subscriber A, but Subscriber A will not hear a Subscriber B (one-way notification).
  - *Two-way* — during incoming intercom call, both subscribers will hear each other.
  - *Ordinary call* — incoming intercom call will be performed as a common call without the Subscriber B automatic reply.

  - *Ignore* — incoming intercom call will be rejected.

- *Intercom call priority* — incoming intercom call priority for other calls.

- Intercom SIP-header – select SIP header, which will be transmitted to caller in INVITE message while 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;

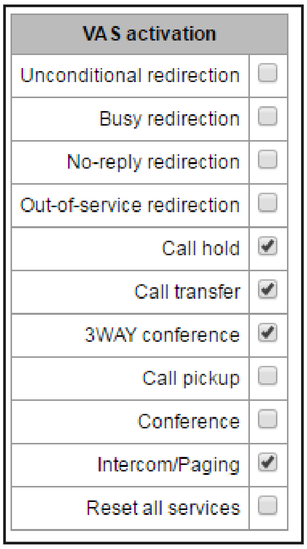
- Pause before answer, sec – transmit pause time before answering on an intercom/paging call in "answer-after" parameter.

VAS settings

- *CLIRO* – calling line identification restriction override service;

- Enable VAS[1] — allow the subscriber to use VAS. When checked, the "VAS activation" table will be available:

VAS activation



VAS activation	
Unconditional redirection	□
Busy redirection	□
No-reply redirection	□
Out-of-service redirection	□
Call hold	☑
Call transfer	☑
3WAY conference	☑
Call pickup	□
Conference	□
Intercom/Paging	☑
Reset all services	□

- *Unconditional redirection* — activate call forward unconditional (CF Unconditional) service.

- *Busy redirection* — activate call forward on busy (CF Busy) service.

- *No-reply redirection* — activate call forward on no reply (CF No reply) service.

- *Out of service redirection* — activate call forward on out of service (CF Out Of Service) service.

- *Call hold* — activate call hold (Call hold) service.

- *Call transfer* — activate call transfer (Call Transfer) service.

- *3WAY conference* — activate 3-way conference (3WAY) service.

- *Call pickup* — activate call pickup (Call Pickup) service.

- *Conference* — activate conference with consequent assembly service.

- *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.

[1] The menu is available for the devices with SMG-VAS license. Read more detailed information on licenses in the section 3.1.23 Licenses.

- *Intercom/paging* — activate access to outgoing intercom or paging call service (with the Subscriber B automatic reply).
- *Change password* – change password for egress calls restriction;
- *Outgoing calls restriction* – use the password-based service "outgoing calls restriction";
- *Restricted by password* – allows a subscriber to hold a call once without restrictions using a password;
- *Password activation* – allows a subscriber enter a password once to eliminate restrictions on egress calls. The second entering of the password will set the restrictions.
- *Do not disturb* – allows a subscriber to set the "Do not disturb" service and define several numbers from the white list which were able to call the subscriber even in "do not disturb" mode[1];
- *Black list* – allows a subscriber to add numbers to black list so that they will not be able to call the subscriber[1];
- *Reset all services* — feature required for cancellation of all numbers configured for redirection by dialing a service prefix configured in the dial plan.

For *'Conference by list'* service operation, you should create a call group (see Section 3.1.8.9 Hunt groups**) and specify the *'Conference number'* for it. To include all of the call group members into the conference, you should dial a service prefix with the 'Conference' type and the conference number specified for the call group.**
For example, conference number '12345', VAS Conference service prefix '*71*x{1,20}#', to gather the group members into the conference, dial '*71*12345#'.

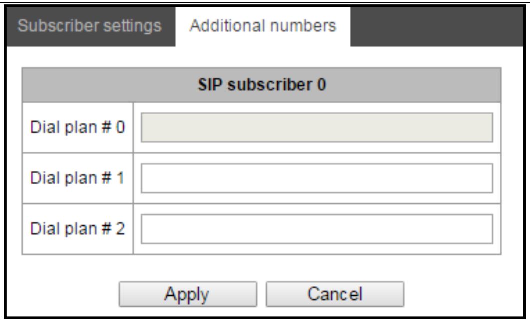
3.1.18.1.1.2 Additional numbers

A subscriber may have different numbers in different dial plans; at that, when a call comes through the dial plan change prefix, subscriber CgPN number is automatically substituted to their number in the corresponding dial plan, e.g.:

Subscriber has an internal short numbering; consequently, they register at the gateway with the short number, upon transition to external network, CgPN should be substituted with a number in the international format for such a subscriber. Transition to an external network is performed by the prefix 9.

To solve this task, activate two dial plans in the 'System parameters' section, create a list of users with the short numbering at the gateway, specify an external number for each subscriber in the 'dial plan #1' field of the 'Additional numbers' setting. In the dial plan #1, an external network exit prefix should be created; in the dial plan #0, prefix '(9x.)' should be created with the 'dial plan change' type that should perform a transfer to the dial plan #1. When the subscriber dials a complete number that begins with 9, the call will transfer through the 'dial plan change' prefix; when it arrives to dial plan #1, their CgPN number will be automatically substituted to their external number.

[1] The service is available on SMG-2016



SIP subscriber 0	
Dial plan # 0	
Dial plan # 1	
Dial plan # 2	

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

3.1.18.1.2 VAS management

In this section, you may configure VAS settings for subscribers.

Supplementary services are provided to each subscriber, but in order to use a specific service, the subscriber must enable it first at the service provider. Operator may create a service plan from multiple

VAS functions; for that, select *'Enable VAS'* checkbox and other checkboxes for corresponding VAS functions in Section 3.1.18.1.1 Subscriber configuration.

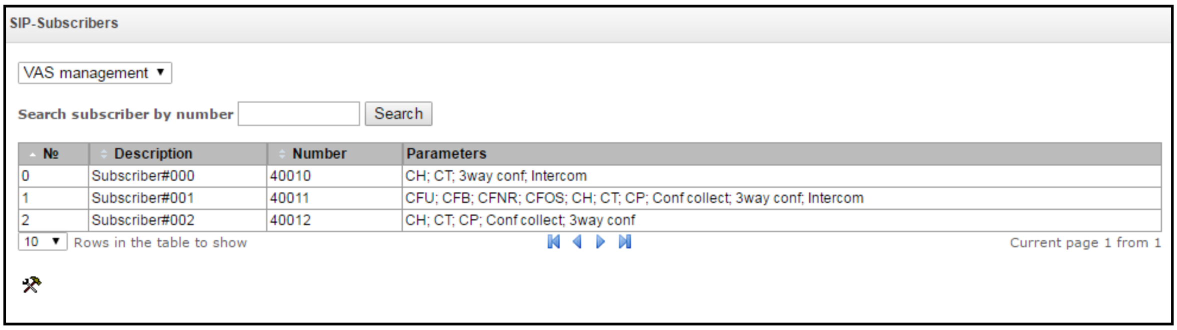
Subscribers may manage state of services from their phone units. The following functions are available:

- Service activation — activation and additional data input.
- Service verification
- Service cancellation — deactivation of a service.

When the activation code is entered or the service is cancelled, subscribers may hear either a 'confirmation' tone (3 short tones), or a 'busy' tone (intermittent tone with tone/pause duration — 0.35/0.35s.) 'Confirmation' tone means that the service has been activated or cancelled successfully, 'busy' tone — that this service is not enabled for this subscriber.

After service confirmation code entry, the subscriber may hear either 'PBX response' tone (continuous) or a 'busy' tone. 'PBX response' tone means that the service has been enabled and activated for the subscriber, 'busy' tone — that this service is not enabled for the subscriber.

The menu only shows numbers with the selected 'Enable VAS' checkbox in the configuration menu (see Section 3.1.18.1.1 Subscriber configuration).



SIP-Subscribers

VAS management ▼

Search subscriber by number

№	Description	Number	Parameters
0	Subscriber#000	40010	CH; CT; 3way conf; Intercom
1	Subscriber#001	40011	CFU; CFB; CFNR; CFOS; CH; CT; CP; Conf collect; 3way conf; Intercom
2	Subscriber#002	40012	CH; CT; CP; Conf collect; 3way conf

10 ▼ Rows in the table to show

Current page 1 from 1

- *Number for unconditional redirection* — phone number for 'Call forward unconditional' service.
- *Number for busy redirection* — phone number for 'Call forward on busy' service.

- *Number for no reply redirection* — phone number for 'Call forward on no reply' service.

- *Number for out of service redirection* — phone number for 'Call forward on out of service' service.

- *Password* – the password of 4 to 8 digits for access to password-based outgoing calls restrictions service;

- *Password activation* – if checked the password is activated and restrictions are not valid.

- *Restrict out* – set prohibitions for some directions of egress calls when the password is inactive:

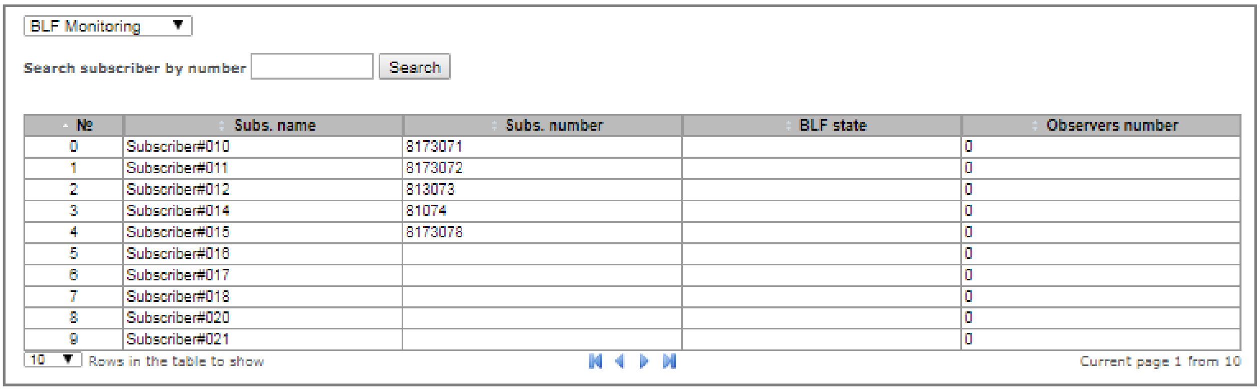
  - *all allowed* – all the restrictions are not valid, restriction code – 0;
  - *only to emergency* – egress communication is restricted, only emergency calls are available, restriction code – 1;
  - *only local and department network* – egress communication is restricted, it is available to call only to local numbers and departmental numbers, restriction code – 2;
  - *only local, department and zone network* – egress communication is restricted, it is available to call only to local and zone numbers and departmental numbers, restriction code – 3.

- *«White list» tab* – you may activate the "do not disturb" service and define white number list containing the numbers which can call the subscriber even in "do not disturb" mode.

- *«Black list» tab* – you may activate the "black list" service and set black list of numbers which can not call the subscriber.

For VAS service detailed operation and configuration description, see Appendix J. Working with VAS services.

3.1.18.1.3 BLF Monitoring



BLF Monitoring ▼

Search subscriber by number [ ] Search

№	Subs. name	Subs. number	BLF state	Observers number
0	Subscriber#010	8173071		0
1	Subscriber#011	8173072		0
2	Subscriber#012	813073		0
3	Subscriber#014	81074		0
4	Subscriber#015	8173078		0
5	Subscriber#016			0
6	Subscriber#017			0
7	Subscriber#018			0
8	Subscriber#020			0
9	Subscriber#021			0

10 ▼ Rows in the table to show

Current page 1 from 10

Click "Search" button to launch search of the subscriber by specified number.

- *Subs. name* – text description of the subscriber;

- *Subs. number* – a number of the subscriber;

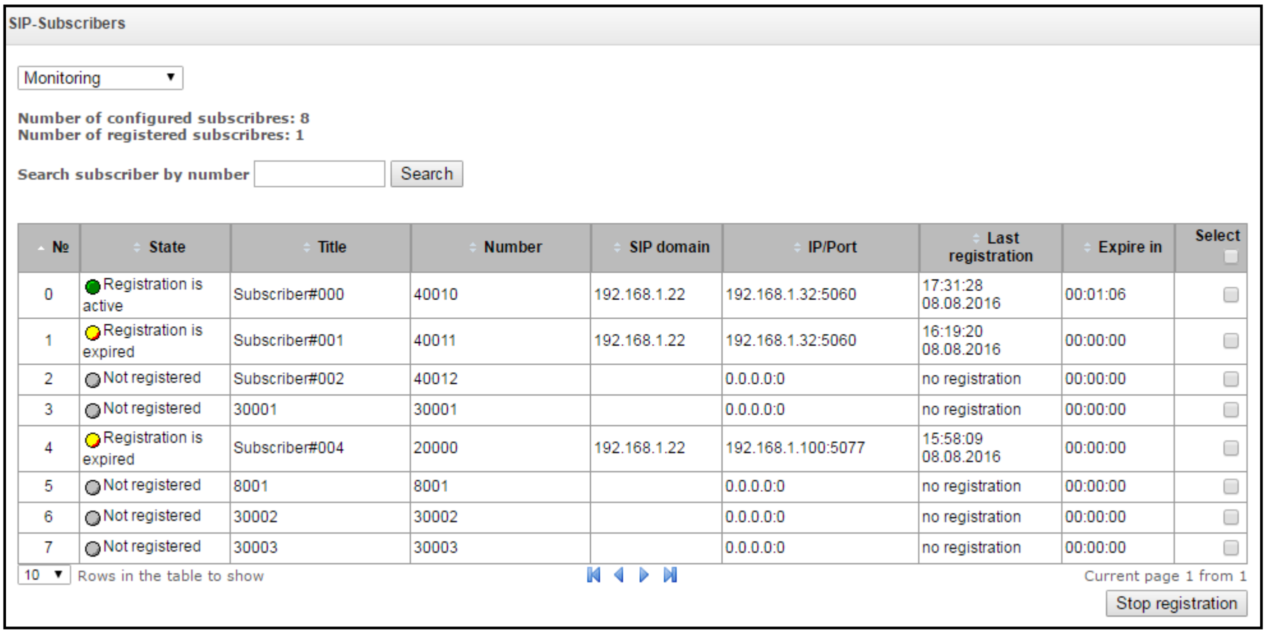
- *BLF state* – the current state of «Busy Lamp Field» service:

  - *idle* – subscribtion is inactive (expired);
  - *early* – channel engagement;
  - *alert* – ringing;
  - *confirmed* – the call is established;
  - *terminated* – the call was ended/there is no call on the line.

- *Observes number* – the current number of subscribers which monitor the subscriber line state.

3.1.18.1.4 Subscriber monitoring

When you choose *'Monitoring'* item from the drop down list, a subscriber status table will be shown.



SIP-Subscribers

Monitoring ▾

Number of configured subscribres: 8
Number of registered subscribres: 1

Search subscriber by number [ ] Search

№	State	Title	Number	SIP domain	IP/Port	Last registration	Expire in	Select □
0	● Registration is active	Subscriber#000	40010	192.168.1.22	192.168.1.32:5060	17:31:28 08.08.2016	00:01:06	□
1	● Registration is expired	Subscriber#001	40011	192.168.1.22	192.168.1.32:5060	16:19:20 08.08.2016	00:00:00	□
2	● Not registered	Subscriber#002	40012		0.0.0.0:0	no registration	00:00:00	□
3	● Not registered	30001	30001		0.0.0.0:0	no registration	00:00:00	□
4	● Registration is expired	Subscriber#004	20000	192.168.1.22	192.168.1.100:5077	15:58:09 08.08.2016	00:00:00	□
5	● Not registered	8001	8001		0.0.0.0:0	no registration	00:00:00	□
6	● Not registered	30002	30002		0.0.0.0:0	no registration	00:00:00	□
7	● Not registered	30003	30003		0.0.0.0:0	no registration	00:00:00	□

10 ▾ Rows in the table to show

Current page 1 from 1

Stop registration

- *State* — subscriber registration status (registered, not registered, registration expired).
- *Title* — arbitrary subscriber text description.
- *Number* — subscriber's number.
- *SIP domain* — domain that the subscriber belongs to.
- *IP/Port* — subscriber IP address and port.
- *Last registration* — last known registration time.
- *Expire in* — remaining time until the registration expiration.
- *Select* — when checked, the current record will be processed when you click *'Stop registration'* button.

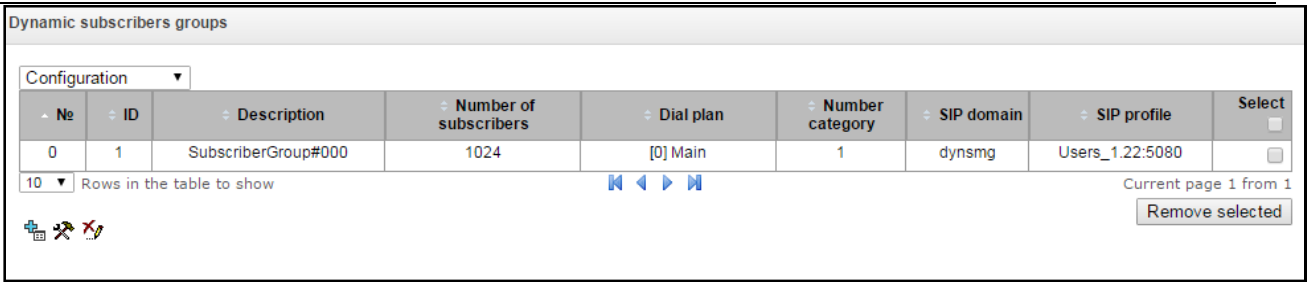
Click *'Stop registration'* button to forcibly stop the registration for selected subscribers.

3.1.18.2 Dynamic subscriber groups

3.1.18.2.1 Dynamic subscriber group configuration

In this section, you may configure dynamic subscriber groups.

In the dynamic registration, digest authentication is used for subscribers at the RADIUS server (RFC4590, RFC4590-no-challenge, draft-sterman).



Dynamic subscribers groups

Configuration ▼

№	ID	Description	Number of subscribers	Dial plan	Number category	SIP domain	SIP profile	Select □
0	1	SubscriberGroup#000	1024	[0] Main	1	dynsmg	Users_1.22:5080	□

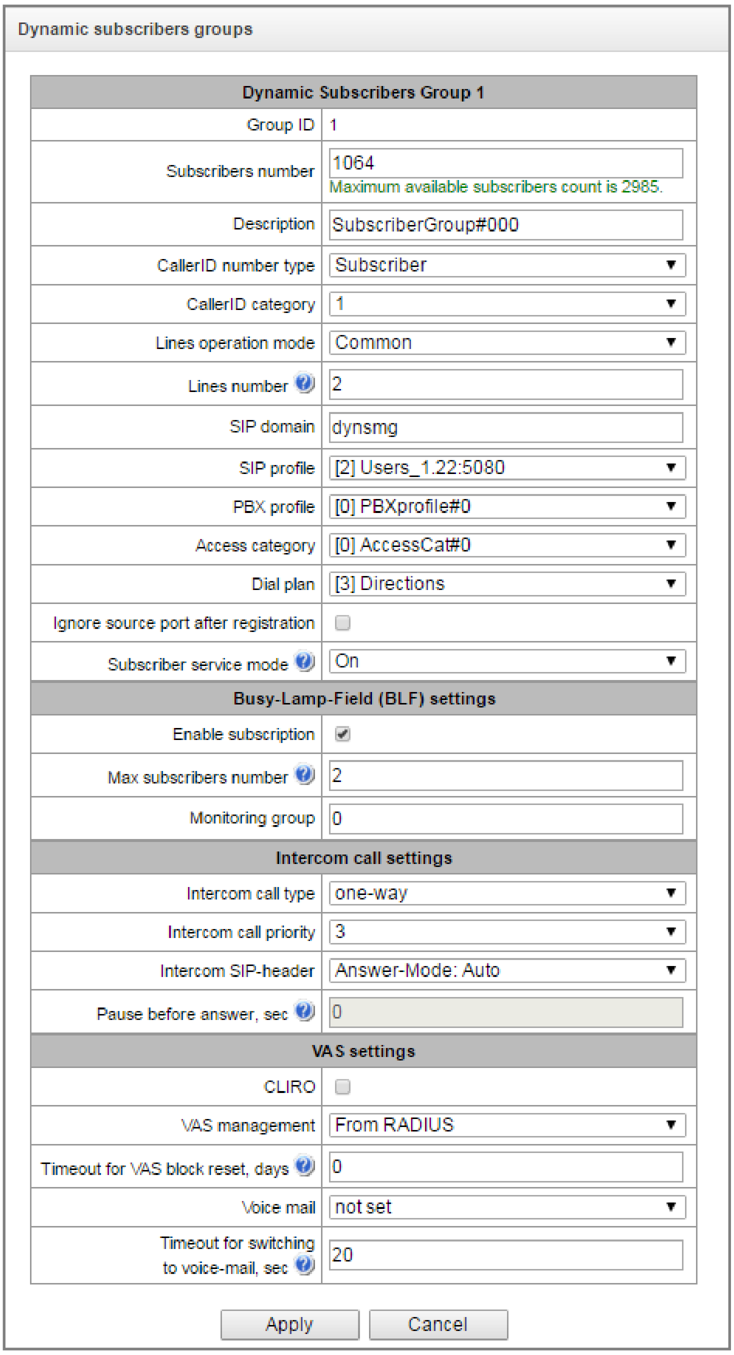
10 ▼ Rows in the table to show

Current page 1 from 1

Remove selected

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

- — *'Add subscriber'*
- — *'Edit subscriber parameters'*
- — *'Remove subscriber'*



Dynamic subscribers groups

Dynamic Subscribers Group 1	
Group ID	1
Subscribers number	1064 Maximum available subscribers count is 2985.
Description	SubscriberGroup#000
CallerID number type	Subscriber ▼
CallerID category	1 ▼
Lines operation mode	Common ▼
Lines number	2
SIP domain	dynsmg
SIP profile	[2] Users_1.22:5080 ▼
PBX profile	[0] PBXprofile#0 ▼
Access category	[0] AccessCat#0 ▼
Dial plan	[3] Directions ▼
Ignore source port after registration	□
Subscriber service mode	On ▼
Busy-Lamp-Field (BLF) settings	
Enable subscription	☑
Max subscribers number	2
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	□
VAS management	From RADIUS ▼
Timeout for VAS block reset, days	0
Voice mail	not set ▼
Timeout for switching to voice-mail, sec	20

- Group of dynamic subscribers:

  - *Subscriber number* — quantity of subscribers in a group.
  - *Description* — name of the group of dynamic objects.
  - *Caller ID number type* — subscriber number type:
  - *Caller ID category* — subscriber's Caller ID category.
  - *Lines operation mode* – limit the number of simultaneous calls. Two options are available: «Common» and «Separate». In «Common» mode all simultaneous calls are taken into account, in «Separate» mode incoming and outgoing calls limits are configured separately;
  - *Lines number* — quantity of calls that the subscriber may take part in simultaneously. Field is available only in the «Common» mode. Permitted value range is [1;255] or 0 — unlimited.
  - *Ingress lines number*[1] – the number of simultaneous incoming calls. The field is available only in the «Separate» mode. Permitted value range is [1;255] or 0 — unlimited.
  - *Egress lines number*[1] – the number of simultaneous outgoing calls. The field is available only in the «Separate» mode. Permitted value range is [1;255] or 0 — unlimited.;
  - *SIP domain* — identifies the subscriber inherence to a specific domain. Sent by the subscriber's gateway in *from* and *to* fields of the *'host'* parameter of SIP URI scheme (see Section 3.1.6.4).
  - *SIP profile* — select SIP profile. SIP profile defines the majority of subscriber's settings (see Section **3.1.7.3** SIP/SIP-T/SIP-I interfaces, SIP profiles).
  - *PBX profile* — select PBX profile (see Section 3.1.8.3).
  - *Access category* — select access category.
  - *Dial plan* — defines the dial plan that the subscriber will belong to.
  - *Ignore source port after registration* — after registration, subscriber messages may come from any port.
  - *Subscriber service mode* — defines restrictions on the incoming and outgoing communication for the subscriber:

    - off: out of service. Number of a subscriber is in a numbering plan, but subscriber terminal cannot be registered. Thus, incoming calls will be barred with 'out of order' cause and egress calls cannot be initiated;
    - on: all communication types available.
    - off 1: incoming communication is enabled, outgoing communication to the special service only.
    - off 2: incoming communication is disabled, outgoing communication to the special service only.
    - denied 1: full barring for incoming and outgoing calls. Calls will be routed by numbering plan, but will be rejected;
    - denied 2: full barring for incoming and outgoing calls except for the emergency services.
    - denied 3: incoming calls are barred, outgoing calls are allowed.
    - denied 4: incoming calls are barred, outgoing calls are allowed only for local and private communication.
    - denied 5: incoming calls are allowed, full barring for outgoing calls.
    - denied 6: incoming calls are allowed, outgoing calls are allowed to emergency services only.
    - 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, private and zone communication.

[1] The settings are available when "separate" line operation mode is set

- ignore: excluded from the numbering. The number is totally excluded from the numbering plan. The ingress calls are barred with 'no route to destination' cause or transmitted to appropriate prefix in numbering plan.

✓ **Directions (*local network, special service, zone network, private network, long-distance network, international network*) are specified during prefix configuration in the dial plan, *'Direction'* field*.***

- Configuration of busy line functions (BLF):
  - *Permit event subscription* –BLF (Busy Lamp Field) function allows you to monitor current line status of another subscribers in real time;
  - *Subscriber number* – quantity of subscribers which can monitor subscriber line status*;*
  - *Monitoring group* – BFL monitoring group, subscribers from the same monitoring group can perform BFL monitoring between each other.
- Intercom configuration:
  - *Type of intercom call* — type of incoming intercom call (autoansmer call of B subscriber):
    - *One way call* — in case of incoming intercom call, B subscriber will hear subscriber A but subscriber A will not hear subscriber B (one-way notification);
    - *Two-way call* — in case of incoming intercom call, both subscribers will hear each other;
    - *Normal call* — incoming intercom call will be performed as normal without B subscriber autoanswer;
    - *Decline* — incoming intercom call will be declined;
  - Intercom call priority — incoming intercom call priority over another calls;
  - *Intercom SIP header* — select SIP header, that will be transmitted to callee by INVITE message during 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;

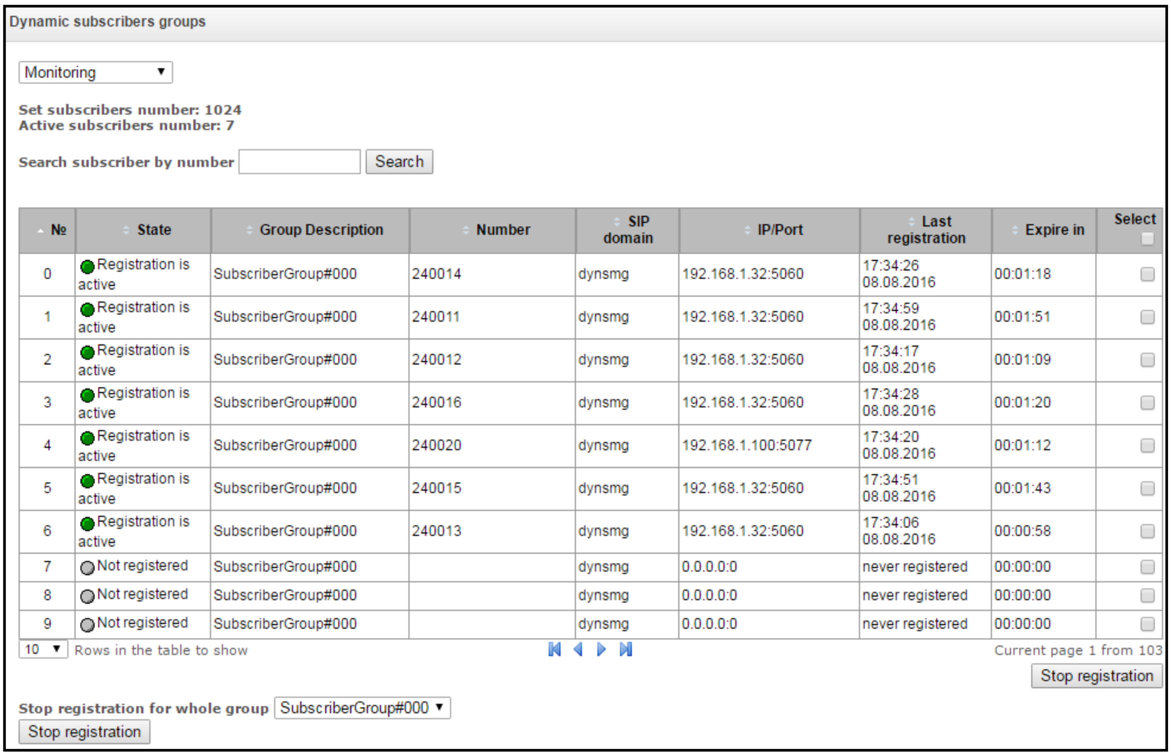
– Pause before answer (sec) — transmission of pause time in ‘answer-after’ headers before taking a intercom/paging call.

- VAS configuration:
  - CLIRO –service for over riding a calling line identification restriction.
  - *VAS activation* — select the VAS activation method for dynamic subscribers.
    - *Do not activate* — do not activate VAS to dynamic subscribers.
    - *Custom selection* — VAS configuration through the gateway configurator individually for each subscriber. When this item is selected, *'VAS activation'* table will become available (for details, see Section 3.1.18.1.1.1 Subscriber settings).

- *Via RADIUS* — transmission of VAS settings in RADIUS server responses is available to dynamic subscribers; for details, see Appendix D.VAS settings transmission from RADIUS server for dynamic subscribers.

- *VAS reset timeout (days)* — when the subscriber goes missing, i.e. if the subscriber no longer registers at the gateway, activated VAS for this subscriber (e.g. redirection service) will continue operation for the duration of this timeout.

3.1.18.2.2 Dynamic subscriber group monitoring



Dynamic subscribers groups

Monitoring ▼

Set subscribers number: 1024
Active subscribers number: 7

Search subscriber by number [ ] Search

№	State	Group Description	Number	SIP domain	IP/Port	Last registration	Expire in	Select □
0	● Registration is active	SubscriberGroup#000	240014	dynsmg	192.168.1.32:5060	17:34:26 08.08.2016	00:01:18	□
1	● Registration is active	SubscriberGroup#000	240011	dynsmg	192.168.1.32:5060	17:34:59 08.08.2016	00:01:51	□
2	● Registration is active	SubscriberGroup#000	240012	dynsmg	192.168.1.32:5060	17:34:17 08.08.2016	00:01:09	□
3	● Registration is active	SubscriberGroup#000	240016	dynsmg	192.168.1.32:5060	17:34:28 08.08.2016	00:01:20	□
4	● Registration is active	SubscriberGroup#000	240020	dynsmg	192.168.1.100:5077	17:34:20 08.08.2016	00:01:12	□
5	● Registration is active	SubscriberGroup#000	240015	dynsmg	192.168.1.32:5060	17:34:51 08.08.2016	00:01:43	□
6	● Registration is active	SubscriberGroup#000	240013	dynsmg	192.168.1.32:5060	17:34:06 08.08.2016	00:00:58	□
7	○ Not registered	SubscriberGroup#000		dynsmg	0.0.0.0:0	never registered	00:00:00	□
8	○ Not registered	SubscriberGroup#000		dynsmg	0.0.0.0:0	never registered	00:00:00	□
9	○ Not registered	SubscriberGroup#000		dynsmg	0.0.0.0:0	never registered	00:00:00	□

10 ▼ Rows in the table to show

Current page 1 from 103

Stop registration

Stop registration for whole group SubscriberGroup#000 ▼

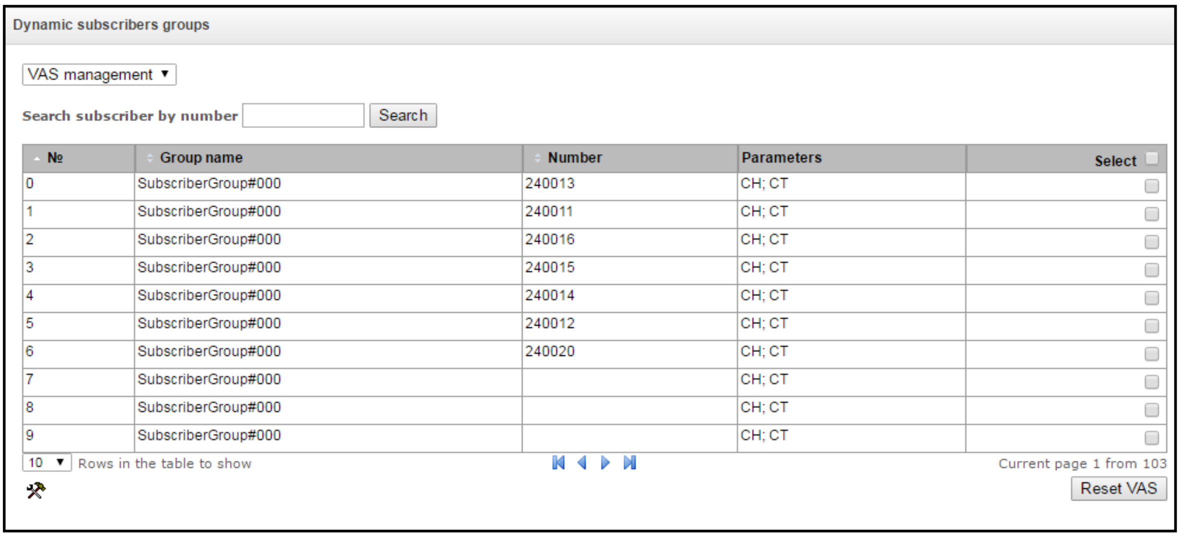
Stop registration

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

- *State* — subscriber registration status (registered, not registered, registration expired).
- *Group description* — arbitrary group text description.
- *Number* — subscriber's number.
- *SIP domain* — domain that the subscriber belongs to.
- *IP/Port* — subscriber IP address and port.
- *Last registration* — last known registration time.
- *Registration expires* — remaining time until the registration expiration.
- *Expire in* — remaining time until the registration expiration.
- *Select* — when checked, the current record will be processed when you click *'Stop registration'* button.
- *Stop registration* — forcedly reset the registration for a selected subscriber.

Click *'Reset'* button to reset the registration for all subscribers in the specified group. To select the group, use the drop-down list.

3.1.18.2.3 Dynamic subscriber group VAS management



Dynamic subscribers groups

VAS management ▾

Search subscriber by number [ ] Search

№	Group name	Number	Parameters	Select □
0	SubscriberGroup#000	240013	CH; CT	□
1	SubscriberGroup#000	240011	CH; CT	□
2	SubscriberGroup#000	240016	CH; CT	□
3	SubscriberGroup#000	240015	CH; CT	□
4	SubscriberGroup#000	240014	CH; CT	□
5	SubscriberGroup#000	240012	CH; CT	□
6	SubscriberGroup#000	240020	CH; CT	□
7	SubscriberGroup#000		CH; CT	□
8	SubscriberGroup#000		CH; CT	□
9	SubscriberGroup#000		CH; CT	□

10 ▾ Rows in the table to show

Current page 1 from 103

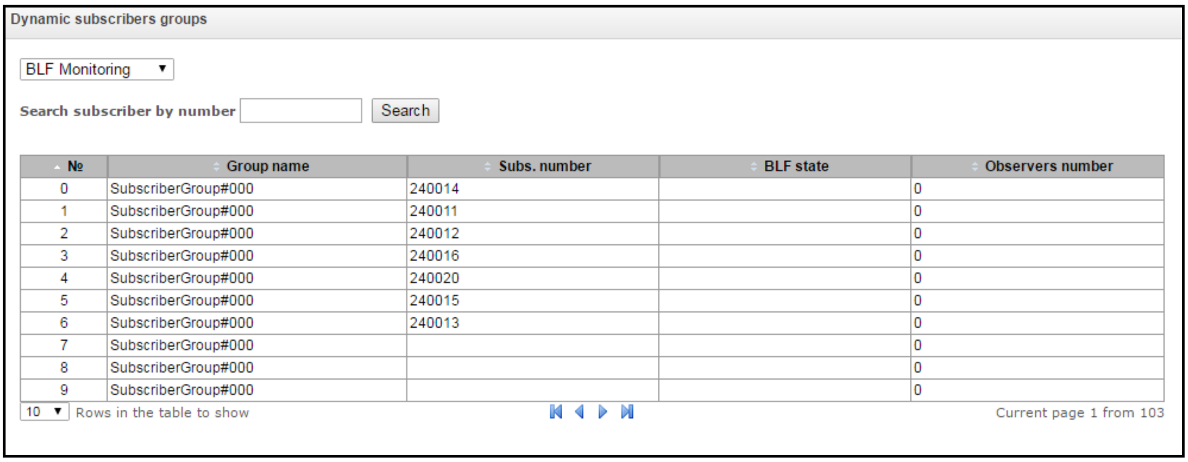
Reset VAS

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

- *Group name* — arbitrary group text description.
- *Number* — subscriber's number.
- *Parameters* — subscriber VAS parameters.
- *Select* — when checked, the current record will be processed when you click *'Reset VAS'* button.

Click *'Reset VAS'* button to reset the VAS settings for selected subscribers.

3.1.18.2.4 Dynamic subscriber group BLF monitoring



Dynamic subscribers groups

BLF Monitoring ▾

Search subscriber by number [ ] Search

№	Group name	Subs. number	BLF state	Observers number
0	SubscriberGroup#000	240014		0
1	SubscriberGroup#000	240011		0
2	SubscriberGroup#000	240012		0
3	SubscriberGroup#000	240016		0
4	SubscriberGroup#000	240020		0
5	SubscriberGroup#000	240015		0
6	SubscriberGroup#000	240013		0
7	SubscriberGroup#000			0
8	SubscriberGroup#000			0
9	SubscriberGroup#000			0

10 ▾ Rows in the table to show

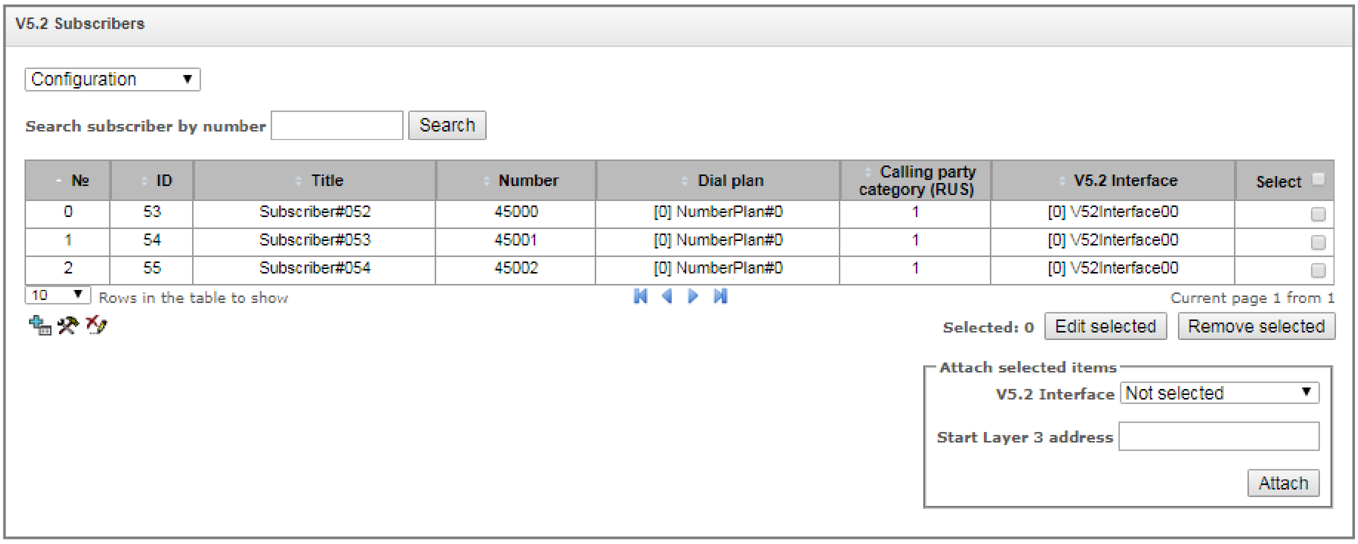
Current page 1 from 103

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

- *Group name* — arbitrary group text description.
- Subscriber number

- *BLF status* — current state of the *'busy lamp field'* service:
  - *idle* – subscribtion is inactive (expired);
  - *early* – channel engagement;
  - *alert* – ringing;
  - *confirmed* – the call is established;
  - *terminated* – the call was ended/there is no call on the line.
- *Viewer quantity* — the current number of subscribers that monitor the subscriber line status.

3.1.18.3 V5.2 subscribers



V5.2 Subscribers

Configuration ▼

Search subscriber by number [ ] Search

№	ID	Title	Number	Dial plan	Calling party category (RUS)	V5.2 Interface	Select ☐
0	53	Subscriber#052	45000	[0] NumberPlan#0	1	[0] V52Interface00	☐
1	54	Subscriber#053	45001	[0] NumberPlan#0	1	[0] V52Interface00	☐
2	55	Subscriber#054	45002	[0] NumberPlan#0	1	[0] V52Interface00	☐

10 ▼ Rows in the table to show

Current page 1 from 1

Selected: 0 Edit selected Remove selected

Attach selected items

V5.2 Interface: Not selected ▼

Start Layer 3 address: [ ]

Attach

- *Search subscriber by number* – check the presence of a subscriber number in the base of configured SIP subscribers;
- *Edit selected* – click the button to edit selected subscribers (subscribers with checked "Select" box). The description of the menu for editing is presented below;
- *Remove selectes* – select subscribers which you want to remove, and click the button "Remove selected".

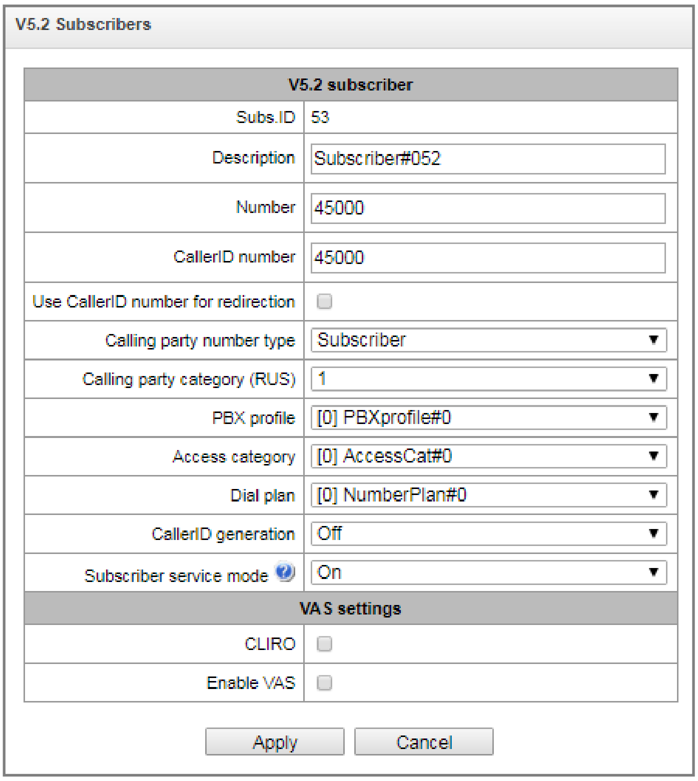
To create, edit and remove subscribers, use the "Objects" menu: "Add an oblect", "Edit an object", "Remove an object". Also you may use the following buttons:

– *«Add a subscriber»;*

– *«Edit subscriber parameters»;*

– *«Delete a subscriber».*

Attach selected items – add selected subscribers to V5.2 interface.



V5.2 Subscribers

V5.2 subscriber	
Subs.ID	53
Description	Subscriber#052
Number	45000
CallerID number	45000
Use CallerID number for redirection	□
Calling party number type	Subscriber
Calling party category (RUS)	1
PBX profile	[0] PBXprofile#0
Access category	[0] AccessCat#0
Dial plan	[0] NumberPlan#0
CallerID generation	Off
Subscriber service mode	On
VAS settings	
CLIRO	□
Enable VAS	□

Subscriber parameters

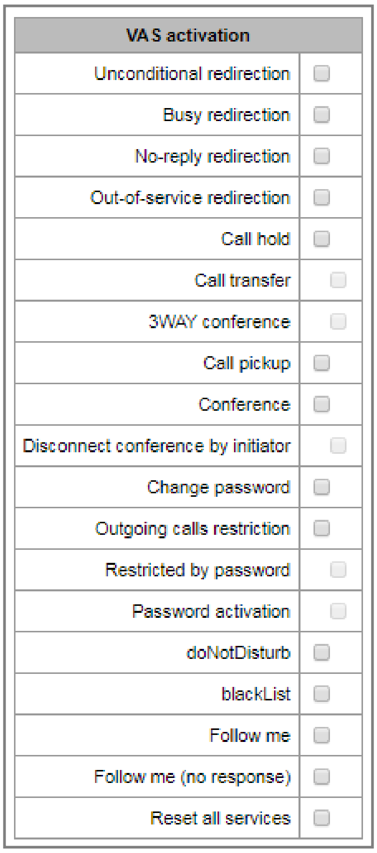
- *Subs. ID* – a unique subscriber identifier
- *Description –text description of the subscriber*;
- *Number* – subscriber's number; for a group of subscribers, number of each following subscriber will be increased by 1.
- *Caller ID number* – subscriber's Caller ID number; for a group of subscribers, number of each following subscriber will be increased by 1;
- *Use CallerID number for redirection* – use the number set in the "CallerID number" when redirecting service is being implemented.
- *Calling party number type* – subscriber number type;
- *Callling party category (RUS)* – CallerID category;
- *PBX profile – select PBX profile* (see section 3.1.8.3 PBX profiles);
- *Access category* – select the access category;
- *Dial plan* – defines the dial plan that the subscriber will belong to*;*
- *CallerID generation – select the format of the Caller ID issuing;*
- *Subscriber service mode* – set restrictions on ingress and egress connection for the subscriber:
  - *off:* out of service. Number of a subscriber is in a dial plan, but subscriber terminal cannot be registered. Thus, incoming calls will be barred with 'out of order' cause and egress calls cannot be initiated.
  - *on:* all communication types are available.
  - *off 1:* incoming communication is enabled, outgoing communication is available only for calls to emergency services.
  - *off 2:* incoming communication is disabled, outgoing communication is available only for calls to emergency services.
  - *denied 1:* full barring for incoming and outgoing calls. Calls will be routed according to dial plans, but will be rejected;
  - *denied 2:* full barring for incoming and outgoing calls except for the calls to emergency services.
  - *denied 3:* incoming calls are barred, outgoing calls are permitted.

- *denied 4:* incoming calls are barred, outgoing calls are permitted only for local and private communication.
- *denied 5:* incoming calls are permitted, full barring for outgoing calls.
- *denied 6:* incoming calls are permitted, outgoing calls are permitted to emergency services only.
- *denied 7:* incoming calls are permitted, outgoing calls are permitted only for local and private communication.
- *denied 8:* incoming calls are permitted, outgoing calls are permitted only for local, private and zone communication.
- *ignore:* excluded from the numbering. The number is completely excluded from the subscriber numbers of the dial plan. The ingress calls are barred with 'no route to destination' cause or transmitted to appropriate prefix in a dial plan.

VAS settings

- *CLIRO* – calling line identification restriction override service;
- Enable VAS[1] — allow the subscriber to use VAS. When checked, the "VAS activation" table will be available:

VAS activation



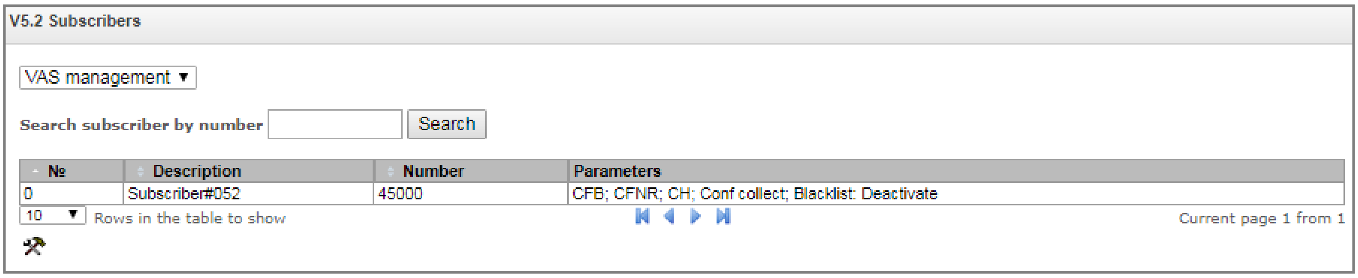
VAS activation	
Unconditional redirection	☐
Busy redirection	☐
No-reply redirection	☐
Out-of-service redirection	☐
Call hold	☐
Call transfer	☐
3WAY conference	☐
Call pickup	☐
Conference	☐
Disconnect conference by initiator	☐
Change password	☐
Outgoing calls restriction	☐
Restricted by password	☐
Password activation	☐
doNotDisturb	☐
blackList	☐
Follow me	☐
Follow me (no response)	☐
Reset all services	☐

- *Unconditional redirection* — activate call forward unconditional (CF Unconditional) service.
- *Busy redirection* — activate call forward on busy (CF Busy) service.
- *No-reply redirection* — activate call forward on no reply (CF No reply) service.
- *Out of service redirection* — activate call forward on out of service (CF Out Of Service) service.
- *Call hold* — activate call hold (Call hold) service.
- *Call transfer* — activate call transfer (Call Transfer) service.
- *3WAY conference* — activate 3-way conference (3WAY) service.
- *Call pickup* — activate call pickup (Call Pickup) service.
- *Conference* — activate conference with consequent assembly service.
- *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* – change password for egress calls restriction;
- *Outgoing calls restriction* – use the password-based service "outgoing calls restriction";

[1] The menu is available for the devices with SMG-VAS license. Read more detailed information on licenses in the section 3.1.23 Licenses.

- *Restricted by password* – allows a subscriber to hold a call once without restrictions using a password;
- *Password activation* – allows a subscriber enter a password once to eliminate restrictions on egress calls. The second entering of the password will set the restrictions.
- *Do not disturb* – allows a subscriber to set the "Do not disturb" service and define several numbers from the white list which were able to call the subscriber even in "do not disturb" mode[1];
- *Black list* – allows a subscriber to add numbers to black list so that they will not be able to call the subscriber[1];
- *Reset all services* — feature required for cancellation of all numbers configured for redirection by dialing a service prefix configured in the dial plan.

VAS management



V5.2 Subscribers

VAS management ▼

Search subscriber by number [ ] Search

№	Description	Number	Parameters
0	Subscriber#052	45000	CFB; CFNR; CH; Conf collect; Blacklist: Deactivate

10 ▼ Rows in the table to show

Current page 1 from 1

You may configure VAS settings for subscribers in this section.

Each subscriber is provided with VAS services, but to use a service, you need to configure it through the operator. The operator may create a service plan with several available services. Check the box "Enable VAS" and check the boxes next to necessary services in the displayed menu (see section 3.1.18.1.1 Subscriber configuration).

The subscriber can manage the services using their phone. The following options are available:

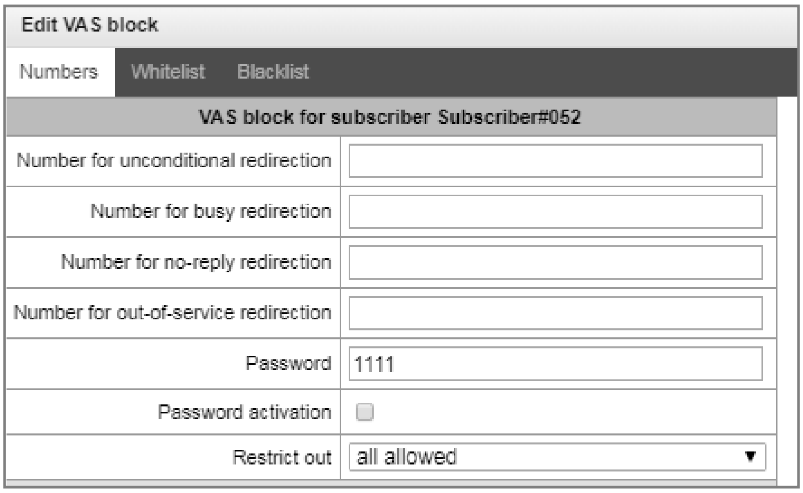
– *service activation* – activation and entering additional information;
– *check the service*;
– *cancel the service* – disable the srevice;

After entering an activation or cancelling code, the susbscriber will hear the "confirm" signal (3 short tones) or "busy" signal (periodic signal with signal/pause duration – 0.35/0.35 seconds). The "confirm" signal means that the service has been successfuly activated or disabled. The "busy" signal means that the service is not enabled to the subscriber.

After entering a check code, the subscriber will hear whether "Station response" signal or "busy" signal. The "Station response" signal means that the service is enabled and activated. The "busy" signal means that the service is disabled or not activated.

The menu displayes the numbers to which "Enable VAS" box is checked in the configuration mode (see section 3.1.18.1.1 Subscriber settings).

[1] The service is available on SMG-2016



Edit VAS block

VAS block for subscriber Subscriber#052	
Number for unconditional redirection	
Number for busy redirection	
Number for no-reply redirection	
Number for out-of-service redirection	
Password	1111
Password activation	□
Restrict out	all allowed ▼

- *Number for unconditional redirection* – a phone number for unconditional redirection service;
- *Number for busy redirection* – a phone number for busy redirection service;
- *Number for no-reply redirection* – a phone number for no-reply redirection service;
- *Number for out of service redirection* – a phone number for out-of-service redirection service;
- *Password* – a password of 4-8 digits for access to password-based outgoing calls restriction service;
- *Password activation* – if checked, the password is activated and the restrictions of egress calls are disabled;
- *Restrict out* – set the restrictions n outgoing communication for certain types of directions if the password is inactive:
  - *all allowed* – the outgoing restrictions are disabled, restriction code – 0;
  - *only to emergency* – outgoing communication is permitted only for calls to emergency services, restriction code - 1;
  - *only local and department network* – outgoing communication is permitted only for local and departmental calls, restriction code - 2;
  - *only local, department and zone network* – outgoing communication is permitted only for local, departmental and zone calls, restriction code - 3;

«Whitelist» tab – you can activate the "do not disturb" service on this tab and set the whitelist of numbers which can call this subscriber even in "do not disturb" mode.

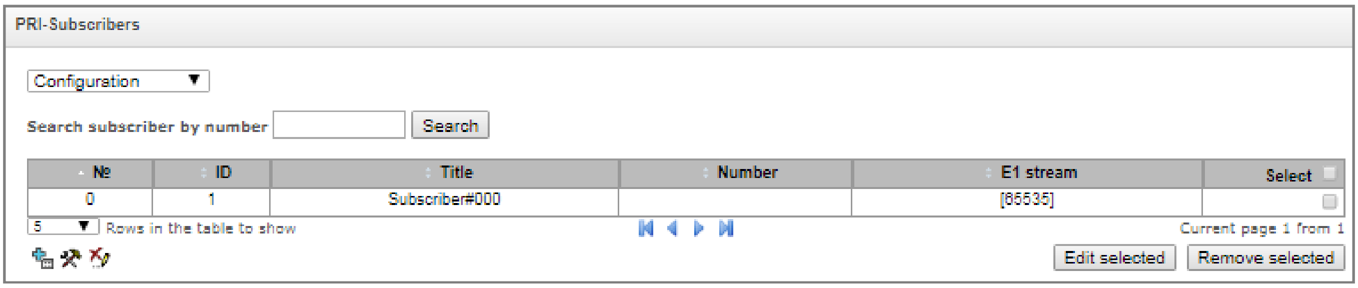
«Blacklist» tab – you can activate the "blacklist" service on this tab and set numbers which cannot call the subscriber.

The detailed information on operation and configuration of VAS is given in Appendix I. Working with VAS services.

3.1.18.4 PRI-susbcribers

PRI-subscribers – numbers which are located behind PRI trunk (E1 streams with Q.931 signalling) and are taken as local subscribers with some services provision. The routing to such subscribers is implemented without additional rules in dial plan.

The check whether the calling subscriber is a PRI subscriber or not is implemented by matching of A number and E1 stream Q.931 from which the call was received.



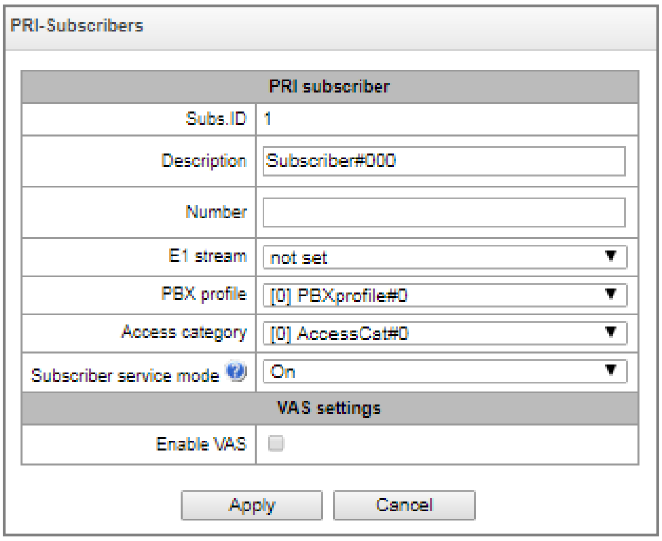
Search subscriber by number

№	ID	Title	Number	E1 stream	Select □
0	1	Subscriber#000		[65535]	□

5 Rows in the table to show

Current page 1 from 1

Subscriber parameters



PRI subscriber	
Subs.ID	1
Description	Subscriber#000
Number	
E1 stream	not set
PBX profile	[0] PBXprofile#0
Access category	[0] AccessCat#0
Subscriber service mode	On
VAS settings	
Enable VAS	□

- *Subs. ID* – a unique identifier of the subscriber.
- *Name* – the description of the subscriber;
- *Number* – a number of the subscriber in the group, the following subscribers will have the number increased by one.
- *E1 stream* – E1 stream, where a call will be routed if the subscriber is called;
- *PBX profile* – select PBX profile (see section 3.1.8.3 PBX profiles);
- *Access category* – select an access category;
- *Subscriber service mode* – set restrictions for egress and ingress communication:
  - off: out of service. The number of the subscriber 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 allowed, only emergency calls are available to be initiated;
  - off 2: no ingress communication, only emergency calls are available to be initiated;
  - denied 1: ingress and egress communication is prohibited. Calls are routed according to a dial plan but rejected;
  - denied 2: ingress and egress communication is prohibited except for emergency services;
  - denied 3: ingress calls are prohibited, egress calls are available;
  - denied 4: ingress calls are prohibited, egress calls are communication only for local and departmental calls;
  - denied 5: ingress calls are available, egress calls are prohibited;
  - denied 6: ingress calls are available, egress communication is available only for emergency calls;
  - denied 7: ingress calls are available, egress communication is available only for local and departmental calls;
  - denied 8: ingress calls are available, egress communication is available only for local, zone and departmental calls;

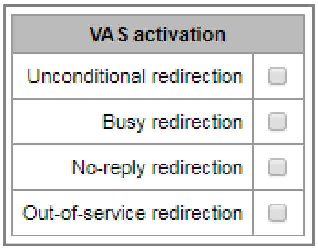
- ignore: excluded from a dial plan. The number is excluded from all the subscriber dial plans. In case of ringing this number, the call will be rejected with "no route destination" cause or will be send to a corresponding prefix in the dial plan.

VAS settings

– *Enable VAS*[1] – allow the subscriber to use VAS. When checked, the "VAS activation" table will be available:

VAS activation

– *Unconditional redirection* – activate call forwarding unconditional service (CF Unconditional);
– *Busy redirection* – activate call forwarding on busy service (CF Busy);
– *No-reply redirection* – activate call forwarding on no reply service (CF No reply);
– *Out-of service redirection* – activate call forwarding on out of order service (CF Out Of Service).

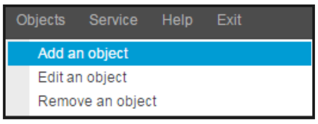


VAS activation	
Unconditional redirection	□
Busy redirection	□
No-reply redirection	□
Out-of-service redirection	□

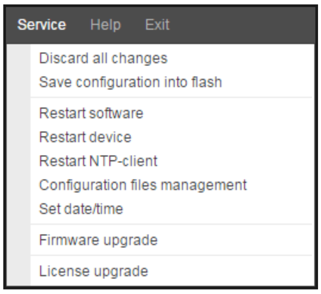
The detailed description of VAS configuring and operating is presented in Appendix I. Working with VAS services.

3.1.19 Working with objects and 'Objects' menu

In addition to create, edit and remove icons, you may use the corresponding 'Objects' menu items to perform different operations with objects.



3.1.20 Saving configuration and 'Service' menu



To discard all changes, select *'Service'* — *'Discard all changes'* menu.

To save the base of registered SIP subscribers, select *'Save subscribers database'* in the *'Service'* menu.

To write the current configuration into non-volatile memory of the device, select *'Service'* — *'Save configuration into FLASH'* menu

To restart the device software, select *'Service'* — *'Software restart'* menu.

To restart the device completely, select *'Service'* — *'Device restart'* menu.

To perform forced time re-synchronization with NTP server, select *'Service'* — *'NTP client restart'* menu.

To read/write the main device configuration file, select *'Service'* — *'Configuration file management'* menu.

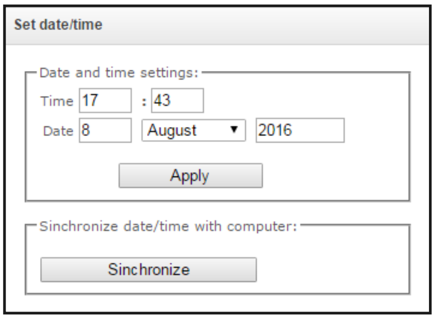
To configure the device local date and time manually, select *'Service'* — *'Date and time configuration'* menu; see Section 3.1.21**.**

[1] The menu is available for the devices with SMG-VAS license. Read more detailed information on licenses in the section 3.1.23 Licenses.

To update the firmware via web configurator, select *'Service'* — *'Firmware update'* menu; see Section 3.1.22**.**

To update/add licenses, select *'Service'* — *'License update'* menu; see Section 3.1.23.

3.1.21 Time and date configuration



Time 17 : 43

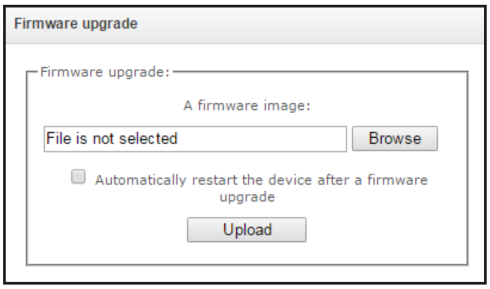
Date 8 August 2016

In the respective fields, you may define the system time in HH:MM format and the date in DD.month.YYYY format.

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

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

3.1.22 Firmware update via web configurator



File is not selected

□ Automatically restart the device after a firmware upgrade

To update the device firmware, use *'Service'* — *'Firmware update'* menu.

Firmware file upload form will open.

- *Update firmware* — update firmware and/or Linux kernel.

To update the firmware, specify the update file name in *'Firmware file'* field using *'Browse'* button and click *'Upload'*. When the operation is completed, restart the device using *'Service'* — *'Device restart'* menu.

3.1.23 Licenses

SMG-1016M licenses:

- *SMG1-PBX-2000* – registration of up to 2000 SIP subscribers;
- *SMG1-VAS-500+IVR* – activation of VAS for 500 subscribers and IVR;
- *SMG1-CORP-500+IVR* – activation of registration feature for up to 500 SIP subscribers, 500 VAS for SIP subsribers and IVR;
- *SMG1-H323* – activation of H.323 protocol;
- *SMG1-RCM* – activation of Radius Call Managment;
- *SMG1-REC* – activation of call record functions *SMG1-SIGTRAN*;
- *SMG1-V5.2-LE* – activation of V5.2 LE protocol to provide outstation connection via V5.2 AN;
- *SMG1-VNI-40* – extension of network interfaces quantity for up to 40.

SMG-2016 licenses:

- *SMG2-PBX-3000* – registration of up to 3000 SIP subscribers;

- *SMG2-VAS-1000+IVR* – activation of VAS for 1000 subscribers and IVR;

- *SMG2-CORP-1000+IVR* – activation of registration feature for up to 1000 SIP subscribers, 1000 VAS for SIP subsribers and IVR.

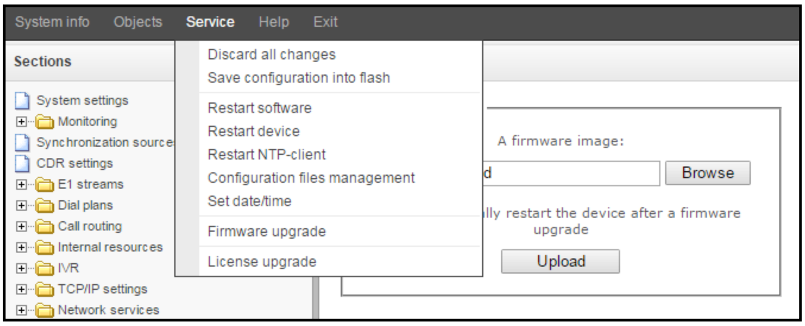
- *SMG2-H323* – activation of H.323 protocol;

- *SMG2-RCM* – activation of Radius Call Managment;

- *SMG2-REC* – activation af call record functions.

To update/add licenses, you should obtain a license file. Contact Eltex marketing department by email eltex@eltex-co.ru or phone +7 (383) 274-48-48 and provide device serial number and MAC address (see Section 3.1.26).

Next, select *'License update'* parameter from the *'Service'* menu.



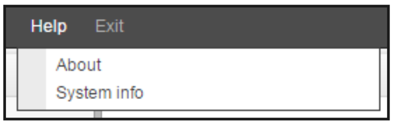
Specify path to the license file obtained from the manufacturer using *'Select file'* button, and update it by clicking *'Update'*.

Confirmation is required for the license file update.

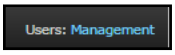
When the operation is completed, you will be prompted to restart the device, or you should do this manually using *'Service'* — *'Device restart'* menu.

3.1.24 'Help' menu

This menu contains details on the current firmware version and factory settings as well as other system information.

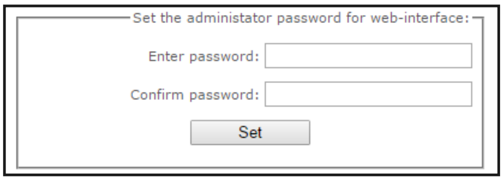


3.1.25 Setting password for web configurator access

The link  is intended for operations with passwords used in web configurator access.

Specify web interface administrator password

To change administrator password, enter a new password into *'Enter password'* field and re-enter it into *'New password confirmation'* field. To apply the password, click 'Set' button.



To save the configuration, use *'Service'* — *'Save configuration'* menu.

Web interface users

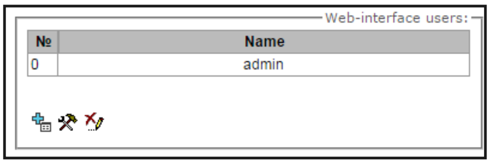
In this block, you may configure web configurator access restrictions at the user level. There is always an administrator for the system, that may add or remove users and assign the access level.

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

— *'Add user'*

— *'Edit user parameters'*

— *'Remove user'*



Web-interface users:

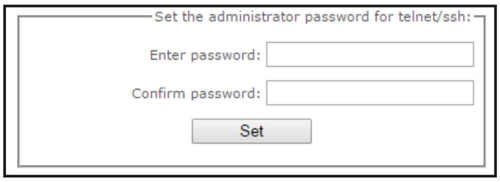
№	Name
0	admin

The program denies modifications of administrator permissions and his removal from the user list, so the system administrators may have an assured access to the program.

- *[username]* — username for web configurator log in.
- *[group]* — user group type. This parameter should have 'webs' parameter.
- *[enter password]* — password for web configurator access.
- *[confirm password]* — confirm password for web configurator access.

To save the configuration, use *'Service'* — *'Save configuration'* menu.

Setting administrator password for Telnet and SSH



Set the administrator password for telnet/ssh:

Enter password:

Confirm password:

In this block, you may change password for Telnet, SSH and console access.

To change the password, enter a new password into *'Enter password'* field and re-enter it into *'New password confirmation'* field. To apply the password, click 'Set' button.

3.1.26 View factory settings and system information

For viewing, use *'Help'* — *'System information'* menu.

Also, factory settings are listed on the label located in the lower part of the device housing.

To view the detailed system information (factory settings, SIP adapter version, current date and time, uptime, network settings, internal temperature), click Home link in the control panel.

3.1.27 Exit the configurator

Click 'Exit' link to exit the configurator.

3.2 Command line, list of supported commands and keys

SMG features several debug terminals, each of them is designed for a specific function:

- *Terminal (COM port)* — enables device configuration and firmware update via CLI (command line interface).
- *Telnet port 23* — terminal (COM port) duplicate.
- *SSH port 22* — terminal (COM port) duplicate.

System of commands for SMG gateway operation in the debug mode

To enter the debug mode, connect to the CLI and enter '`tracemode`' command.

Table 27 — Debug mode commands

Command	Description
help	View the list of available commands
quit	Exit debug mode
logout	Exit debug mode
exit	Exit debug mode
history	Show the list of previously entered commands
radact [on/off]	Turn RADIUS on/off
radshow	View the list of requests to RADIUS server
resolve	Check domain name resolution Parameter: domain name
rstat	View RADIUS protocol operation statistics
q931timers	View Q.931 timer values
mspping [on/off] <idx>	Enable/disable signal processor querying; idx — signal processor name — 0..5
stream [stream]	View E1 stream state or a specific stream state, 'stream' is a stream number (0..15)
e1stat <stream>	View E1 stream counters
alarm	View alarm log information
sync	View synchronization source information
syncfreq	View synchronization frequency information
setsync	Forced synchronization source change Parameter — <stream number>
checkmod	Check number modifier operation for the specific number Parameters: <modifier table><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>	View status of channels in the link set, <linkset> is SS7 link set number
checknum	Check the number with the dial plan
cfg_read	Apply the current configuration; this command will reset and re-initialize E1 streams
callref	Show information on active SIP calls
rtpdebug <level>	Enable switch RTP debugging; <level> is a debugging level **WARNING! This command may cause the gateway to become unresponsive under load**
mspcports	View RTP port state
mspcshow <device>	View signal processor connection statistics
sipstat	View SIP call statistics
sipclrstat	Reset SIP statistics counters
sipreg	View information on the subscriber or trunk registration Parameters: <user>, <trunk <self|user>>
sipreg user	View the list of registered subscribers (similar to 'reginfo' command)
sipreg trunk self	View information on SIP interface trunk registration on the upstream server
sipreg trunk user	View information on SIP interface subscriber registration on the upstream server.
route	View information on network routes processed by VoIP

showcall	View information on currently active calls
license	View information on currently active licenses
mspreglog	Enable signal processor command tracing
mspunreglog	Disable signal processor command tracing
talk	View call statistics
trunk cps	Information on the current quantity of calls per second for the trunk group Parameters: <idx> — trunk group number
trunk stat	Information on the current calls for the trunk group Parameters: <idx> — trunk group number
sys	View system information, firmware version
hwreboot	Rebooting device
trace	Tracing functions
reginfo	Enter information on the registered subscribers
regcon	This command allows you to return to normal mode after 'unregcon' command execution (if application was not terminated abnormally)
unregcon	This command is used in extreme cases to identify the accurate location of the application abnormal termination
stop	Restart the software

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 28 — Possible arguments (*<POINT>*)

Value <POINT>	***Command description***	***Value <IDX>***
hwpkt	Tracing of packet contents at the first level of exchange between the main application and E1 stream driver	0..15
stream	E1 stream tracing	0..15
port	Application operation tracing	Not used
isup	SS7 protocol ISUP subsystem operation tracing	Not used
mtp3	SS7 protocol MTP3 level operation tracing for E1 stream	0..15
sipt	SIP/-T/-I protocol operation tracing	Not used
pril3	DSS1 protocol third level operation tracing for E1 stream	0..15
sw	Switching network operation tracing	Not used

mspc	IP forwarding tracing	Not used
mspd	Signal processor operation tracing	0..7
net	2nd layer data network operation tracing	Not used
sync	Synchronization source operation tracing	Not used
erl1	Low-level tracing for the system that transfers messages between the application and SIP module	Not used
erl3	High-level tracing for the system that transfers messages between the application and SIP module	Not used
snmp	SNMP protocol operation tracing	Not used
np	Dial plan (routing) operation tracing	Not used
mod	Modifier operation tracing	Not used
alarm	Gateway alarm 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, you should connect to it via Telnet or SSH protocol, or by the RS-232 cable (for access via CLI). Default IP address: **192.168.1.2**, mask: **255.255.255.0**.

Configuration is stored in text files located in the ***'/etc/config'*** directory that you can edit with the integrated text editor 'joe' (these changes will take effect after the device is restarted).

Modifications made to configuration via CLI (command line interface) or web configurator will be applied immediately.

To save the configuration into the non-volatile memory of the device, execute **'copy running_to_startup'** command**.**

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

Given below is a complete list of commands sorted in alphabetic order

3.3.1 List of CLI commands

Table 29 — CLI commands

Command	***Parameter***	***Value***	***Action***
`?`			Show the list of available commands.
`alarm global`			Show the current alarm information
`alarm list clear`			Clear fault events log
`alarm list show`			Show fault events log with identification of fault type and status, occurrence time and localization parameters.
`config`			Enter the device parameter configuration mode
`CPU load statistic`			Show CPU load for the last minute

`date`	`<DAY>`
	`<MONTH>`
	`<YEAR>`
	`<HOURS>`
		`1-31`
		`1-12`
		`2011-2037`
		`00-23`
			Set the device local date and time

	<MINS>	00-59	
dhcp start			Launch DHCP server
dhcp stop			Stop DHCP server
exit			Terminate this CLI session
firmware update tftp	<FILE> <SERVERIP>	firmware file name IP address in AAA.BBB.CCC.DDD format	Firmware update without gateway restart FILE — firmware file name SERVERIP — TFTP server IP address:
firmware update ftp	<FILE> <SERVERIP>	firmware file name IP address in AAA.BBB.CCC.DDD format	Firmware update without gateway restart FILE — firmware file name SERVERIP — FTP server IP address
firmware update usb	<FILE>	firmware file name	Firmware update without gateway restart FILE — firmware file name
firmware update_and_reboot tftp	<FILE> <SERVERIP>	firmware file name IP address in AAA.BBB.CCC.DDD format	Firmware update with gateway restart FILE — firmware file name SERVERIP — TFTP server IP address:
firmware update_and_reboot ftp	<FILE> <SERVERIP>	firmware file name IP address in AAA.BBB.CCC.DDD format	Firmware update with gateway restart FILE — firmware file name SERVERIP — FTP server IP address
firmware update_and_reboot usb	<FILE>	firmware file name	Firmware update with gateway restart FILE — firmware file name
history			View history of entered commands.
license check	<LICENSE>	SMG-PBX-2000/ SIP-PBX-Demo/ SMG-PBX-3000/ SMG-H323/ SMG-RCM/ SMG-VAS-500/ SMG-DEMO	Check the license availability for the device. (*License installed* — license is installed *License NOT installed* — license is not installed)
license download	<FILE> <SERVERIP>	License file name Server IP address in AAA.BBB.CCC.DDD format	Download licenses from the address specified
license update			Update the license
license reset	no/yes		Delete all installed licenses
management			Enter SS7 stream management mode
mirroring			Enter mirroring management mode
number check	<NUMPLAN> <NUMBER> <COMPLETE>	0-15/0-255 String, 31 characters max. yes/no	Availability check for routing by this number. Check is performed by caller and callee masks and also in the configured SIP subscriber database. The check provides the routing possibility data for this number in the defined dial plan: *calling-table* — routing by the caller table.

			called-table — routing by the callee table. *NOT found in* — routing by this table is not possible. *found in* — routing by this table is possible. *Abonent 'SIP' idx[4]* — SIP subscriber [database record number for this subscriber]. *Prefix [6]* — routing by prefix [prefix number in the list].
`mirroring`			Ethernet port mirroring configuration
`password`			Change access password via CLI

`pcmdump`	`<STREAM>`
	`<FILE>`
		`0-15`
		`string`
			Collect packets from the specified E1 stream.
			STREAM — number of stream for capture
			FILE — file for writing

`quit`			Terminate this CLI session
`reboot`	`<YES_NO>`	`yes/no`	Reboot device
`save`			Write the current configuration into non-volatile memory of the device
`sh`			Go to Linux Shell from CLI
`sntp retry`			Send SNTP request to the server for time synchronization
`statistic`			Enter the statistics viewing mode

`tcpdump`	`<DEVICE>`
	`<FILE>`
	`<SNAPLEN>`
		`eth0/eth1/local`
		`string`
		`0-65535`
			Capture packets from the Ethernet device
			DEVICE — interface for monitoring
			FILE — file for packet writing
			SNAPLEN — byte quantity captured from each packet (0 — full packet capture)

`tftp put`	`<LOCAL_FILE>`
	`<REMOTE_FILE>`
	`<SERVERIP>`
		`string`
		`string`
		`IP address in AAA.BBB.CCC.DDD format`
			Get file via TFTP. This command allows to download the tracings made by tcpdump and pcmdump commands

`tracemode`			Enter the tracing mode

3.3.2 Change device access password via CLI

Given that you may connect to the gateway remotely via Telnet, we recommend changing the password for *admin* user in order to avoid unauthorized access.

To do this, you should do as follows:

1) Connect to the gateway via CLI, authorize using login/password, enter 'password' command and press <Enter>

2) Enter a new password:

New password:

3) Retype entered password:

```
  Retype password:
  Password changed (Password for admin changed by root)
```

4) Save the configuration into Flash: enter *save* command and press <Enter>

3.3.3 Statistics mode

In this mode, you may view the statistics data in accordance with Q.752 ITU-T guideline tables.

3.3.3.1 Enter the statistics viewing mode

Command syntax: **statistic**

3.3.3.2 Enter the MTP (SS7) signaling traffic volume viewing mode

Command syntax: **mtp**

Execution result: Change to MTP statistic mode
SMG-[STAT]-[MTP]>

3.3.3.2.1 Parameters used in MTP traffic statistics viewing commands

<LINK>	E1 stream number
<LINKSET>	SS7 link set number
< TIME1>	amount of time for statistics output (hours)
< TIME2>	amount of time for statistics output (minutes)

3.3.3.2.2 View MTP traffic general state

Command syntax: **signalling link allstat**<LINK><TIME1><TIME2>

Example: `SMG-[STAT]-[MTP]> signalling link allstat 8 12 0`

Meaning: 8th E1 stream statistics is shown from all tables for 12-hour 00-minute interval.

3.3.3.2.3 View signaling traffic (MTP message accounting)

Q.752 ITU-T guidelines, Table 15

Command syntax: **message accounting**<LINK><TIME1><TIME2>

Example: `SMG-[STAT]-[MTP]> message accounting 8 12 0`

Execution result:

```
+----------------------------------------------------+
|      SS7 MTP message accounting.    Link   08      |
+---------------+-----------------+------------------+
|     Period:  00:00:00 -  00:00:00 (    0 sec)      |
+---------------------------------+------------------+
|               |     Messages    |      Octets      |
+---------------+-----------------+------------------+
|  Received     |               0 |               0  |
+---------------+-----------------+------------------+
|  Transmitted  |               0 |               0  |
+---------------+-----------------+------------------+
```

Meaning: 8th E1 stream MTP signaling traffic volume is shown for 12-hour 00-minute interval.

3.3.3.2.4 View MTP signaling link faults and performance counters

Q.752 ITU-T guidelines, Table 1

Command syntax: **signalling link faults_and_performance**<LINK><TIME1><TIME2>

Example:

```
SMG-[STAT]-[MTP]> signalling link faults_and_performance 8 12 0
```

Execution result:

```
+----------------------------------------------------+
|     MTP SL faults and performance.   Link  08      |
+----------------------------------------------------+
|     Period:  00:00:00 -  00:00:00 (    0 sec)      |
+---------------------------------+------------------+
|  Duration the In-service state  |          0 sec   |
+---------------------------------+------------------+
|  SL failure events all reasons  |          0       |
+---------------------------------+------------------+
|  Number of SU received in error |          0       |
+---------------------------------+------------------+
```

Meaning: 8th E1 stream signaling link faults and performance counters are shown for 12-hour 00-minute interval.

3.3.3.2.5 View MTP signalling link unavailability duration

Q.752 ITU-T guidelines, Table 2

Command syntax: **signalling link availability**<LINK><TIME1><TIME2>

Example:

```
SMG-[STAT]-[MTP]> signalling link availability 8 12 0
```

Execution result:

```
+----------------------------------------------------+
|         MTP SL availability.      Link  08         |
+----------------------------------------------------+
|     Period:  00:00:00 -  00:00:00 (    0 sec)      |
+---------------------------------+------------------+
|  Duration of SL unavailability  |          0 sec   |
+---------------------------------+------------------+
```

Meaning: 8th E1 stream signalling link unavailability duration is shown for 12-hour 00-minute interval.

3.3.3.2.6 View MTP signalling link utilization metrics

Q.752 ITU-T guidelines, Table 3

Command syntax: **signalling link utilization**<LINK><TIME1><TIME2>

Example:

```
SMG-[STAT]-[MTP]> signalling link utilization 8 12 0
```

Execution result:

```
+----------------------------------------------------+
|          MTP SL utilization.      Link  08          |
+----------------------------------------------------+
|      Period:  00:00:00 -  00:00:00 (    0 sec)      |
+----------------------------------+-----------------+
|  SIF and SIO octets transmitted |          0      |
+----------------------------------+-----------------+
|  SIF and SIO octets received    |          0      |
+----------------------------------+-----------------+
|  MSUs discarded due congestion  |          0      |
+----------------------------------+-----------------+
```

Meaning: 8th E1 stream utilization metrics are shown for 12-hour 00-minute interval.

3.3.3.2.7 View MTP signalling link set and route set availability

Q.752 ITU-T guidelines, Table 4

Command syntax: **signalling link availability**<LINKSET><TIME1><TIME2>

Example:

```
SMG-[STAT]-[MTP]> signalling link availability 0 12 0
```

Execution result:

```
+----------------------------------------------------+
|          MTP SL utilization.      Link  08          |
+----------------------------------------------------+
|      Period:  00:00:00 -  00:00:00 (    0 sec)      |
+----------------------------------+-----------------+
|  SIF and SIO octets transmitted |          0      |
+----------------------------------+-----------------+
|  SIF and SIO octets received    |          0      |
+----------------------------------+-----------------+
|  MSUs discarded due congestion  |          0      |
+----------------------------------+-----------------+
```

Meaning: Linkset 0 and route set availability metrics are shown for 12-hour 00-minute interval.

3.3.3.2.8 View MTP signalling point status

Q.752 ITU-T guidelines, Table 5

Command syntax: **signalling point status**<LINK><TIME1><TIME2>

Example: `SMG-[STAT]-[MTP]> signalling point status 8 12 0`

Execution result:

```
+--------------------------------------------------+
|      MTP signalling point status.   Link  08      |
+--------------------------------------------------+
|     Period:  00:00:00 -  00:00:00 (    0 sec)     |
+--------------------------------+-----------------+
|  Adjacent SP inaccessible      |         0       |
+--------------------------------+-----------------+
|  Duration of SP inaccessible   |         0 sec   |
+--------------------------------+-----------------+
|  MSUs discarded due error      |         0       |
+--------------------------------+-----------------+
```

Meaning: 8th E1 stream signalling point metrics are shown for 12-hour 00-minute interval.

3.3.3.3 Enter the packet traffic viewing mode

Command syntax: **packets**

Execution result: `SMG-[STAT]-[PACKETS]>`

3.3.3.3.1 View QoS statistics for packet traffic

Command syntax: **show**<TIME1><TIME2>

Parameters:

< TIME1> amount of time for statistics output (hours)

< TIME2> amount of time for statistics output (minutes)

Example: `SMG-[STAT]-[PACKETS]> show 12 0`

Execution result:

```
+--------------------------------------------------+
|                 Packet statistic                 |
+--------------------------------------------------+
|     Period:  12:00:17 -  13:22:32 ( 4935 sec)     |
+-----------------------------+--------------------+
|  Packets received           |          0         |
+-----------------------------+--------------------+
|  Packets transmitted        |          0         |
+-----------------------------+--------------------+
|  Packets lost               |          0         |
+-----------------------------+--------------------+
|  Packets lost (percentage)  |      0.000000      |
+-----------------------------+--------------------+
|  Packets bad                |          0         |
+-----------------------------+--------------------+
|  Packets bad (percentage)   |      0.000000      |
+-----------------------------+--------------------+
|  Packets trip-time average  |          0 ms      |
+-----------------------------+--------------------+
|  Packets trip-time min      |          0 ms      |
+-----------------------------+--------------------+
|  Packets trip-time max      |          0 ms      |
+-----------------------------+--------------------+
```

Meaning: QoS statistics for packet traffic data is shown for 12-hour 00-minute interval.

3.3.4 Management mode

To enter the SS7 stream management mode, execute 'management' command.

```
SMG> management
Entering management mode.
SMG-[MGMT]>
```

Command	***Parameter***	***Value***	***Action***
`?`			Show the list of available commands.
`exit`			Move to a higher menu level.
`history`			View history of entered commands.
`nslookup`	`<HOST>`	`string`	Request IP address for host with the name specified *HOST* — address for request
`ping host`	`<HOST>`		Send PING request to the host specified
`ping ip`	`<IP>`	`IP address in AAA.BBB.CCC.DDD format`	Send PING request to the IP address specified
`e1 stat clear`	`<STREAM>`	`0-15`	Reset statistics for the E1 stream specified
`e1 stat show`	`<STREAM>`	`0-15`	View statistics for the E1 stream specified
`ss7link`	`<SS7_LINK>`	`0-15`	Proceed to the specified SS7 stream parameter management
`quit`			Terminate this CLI session

3.3.4.1 SS7 stream management mode

To enter this mode, execute 'ss7link <Link>' command in the SS7 stream configuration mode, where <Link> is SS7 stream number that may take values in the range from 0 to 15.

```
SMG-[MGMT]> ss7link 0
E1[0]. Signaling is SS7
SMG-[MGMT]-[SS7LINK][0]>
```

Command	***Parameter***	***Value***	***Action***
`?`			Show the list of available commands.
`chan block`	`<CHAN_INDEX>`	`1-31`	Block the specified channel (BLO)

`chan ccr`	`start`
	`state`
	`stop`
		`<CHAN_INDEX>`
		`1-31`
			Send CCR message and check the channel integrity with this message

`chan group block`	`<CHAN_INDEX_START>`
	`<CHAN_COUNT>`
		`1-31`
		`2-31`
			Block a group of channels
			CHAN_INDEX_START — starting E1 channel number in a group
			CHAN_COUNT — quantity of channels in a group

`chan group reset`	`<CHAN_INDEX_START>`
	`<CHAN_COUNT>`
		`1-31`
		`2-31`
			Reset channel group
			CHAN_INDEX_START — starting E1 channel number in a group
			CHAN_COUNT — quantity of channels in a group

`chan group unblock`	`<CHAN_INDEX_START>`	`1-31`	Unblock a group of channels

	`<CHAN_COUNT>`	2-31	CHAN_INDEX_START — starting E1 channel number in a group CHAN_COUNT — quantity of channels in a group
`chan rel`	`<CHAN_INDEX>`	1-31	Disconnection in the specified channel
`chan reset`	`<CHAN_INDEX>`	1-31	Reset specified channel
`chan rlc`	`<CHAN_INDEX>`	1-31	Confirm disconnection in the specified channel
`chan unblock`	`<CHAN_INDEX>`	1-31	Unblock specified channel
`exit`			Return from this configuration submenu to the upper level.
`link clr outage`			Clear 'CPU local failure' state for a channel
`link send LFU`			Send 'link forced uninhibit' message to stream
`link send LIN`			Send 'link forced inhibit' message to stream
`link send LUN`			Send 'link uninhibit' message to stream
`link set congestion`			Set 'overload' state for a stream
`link set outage`			Set 'CPU local failure' state for a stream
`link start emergency`			Initiate emergency stream startup
`link start normal`			Initiate normal stream startup
`link stop`			Stop stream
`quit`			Terminate this CLI session
`show info chan`			Show information on the channel state in a stream
`show info link`			Show information on the stream state

3.3.5 Port mirroring parameters configuration mode

To enter this mode[1], execute 'mirroring' command.

SMG> mirroring
Change to the mirroring mode
SMG-[MIRRORING]>

Command	Parameter	Value	Action
`?`			Show the list of available commands.
`apply`	`yes/no`		Apply settings
`exit`			Return from this configuration submenu to the upper level.
`quit`			Terminate this CLI session

`set`	`<PORT>`
	
	`<NAME>`
	
	`<ACT>`
		`CPU/ GE_PORT0/ GE_PORT1/ GE_PORT2/ SFP0/ SFP1`
		
		`src_in/ src_out/ dst_in/ dst_out`
		
		`on/off`
			Configure port mirroring:
			
			PORT — port type.
			
			NAME — port designation.
			src_in — incoming packet source port — copy frames received from this port (source port).
			src_out — outgoing packet source ports — copy frames sent by this port (source port).
			dst_in — incoming packet destination port — destination port for copied frames received by selected source ports.
			dst_out — outgoing packet destination

[1] For SMG-1016M only

			port — destination port for copied frames sent by selected source ports.
show			Configure port mirroring:

3.3.6 General device parameter configuration mode

To proceed to device parameter configurations/monitoring, execute 'config' command.

For each configuration mode 'do' and 'top' commands are available. The 'do' command allows you to execute command of CLI menu from any configuration submenu. The 'top' command allows going to CLI 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 alarm message storage Off — disabled /mnt/sd[abc][1-7]* — path to storage device for tracing storage
access category			Enter access categories' configuration mode
cdr			Enter CDR record parameter configuration mode
copy running_to_startup			Write the current configuration into non-volatile memory of the device (into start configuration)
copy startup_to_running			Restore the current configuration from the start configuration
count linkset			Show the number of SS7 link sets
count trunk			Show the number of trunk groups
count trunk_direction			Show the number of trunk directions
count sipt-interface			Show the number of SIP interfaces
count radius-profile			Show the number of RADIUS profiles
delete modifiers-table			Show the number of modifier table profiles
count sipcause-profile			Show the number of Q.850 and sip-reply compliance profiles
count routing-profile			Show the number of scheduled routing profiles
count h323-interface			Show the number of h.323 profiles
count ss7timers			Show the number of SS7 timer profiles
delete linkset	<OBJECT_INDEX>	existing number of the link set	Delete SS7 link set
delete trunk	<OBJECT_INDEX>	Existing trunk group number	Delete trunk group
delete	<OBJECT_INDEX>	Existing trunk	Delete trunk direction

trunk_direction		direction number	
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 modifier table
delete sipcause-profile	<OBJECT_INDEX>	Existing q.850 and sip-reply compliance table number	Delete q.850 and sip-reply compliance table
delete routing-profile	<OBJECT_INDEX>	Existing scheduled routing table number	Delete scheduled routing table
delete h323-interface	<OBJECT_INDEX>	Existing H.323 interface number	Delete H.323 interface
delete ss7timers	<OBJECT_INDEX>	Existing SS7 timer profile number	Delete SS7 timer profile
delete hunt-group	<OBJECT_INDEX>	Existing call group	Delete call group
delete pickup-group	<OBJECT_INDEX>	Existing pickup group	Delete pickup group
e1	<E1_INDEX>	0-15	Enter the selected E1 stream configuration mode
exit			Move to a higher menu level.
firewall dynamic			Enter dynamic firewall configuration mode
firewall static			Enter static firewall configuration mode
ftpd			Enter ftp server configuration mode
h323 configuration			Enter H.323 protocol configuration mode
h323 interface	<H323_INDEX>	0-63	Enter the configuration mode for the specific interface H.323 protocol operation
history			View history of entered commands.
hunt-group	<hunt-group_INDEX>	0-31	Enter the configuration mode for the specific call group operation
log path	<apply>		Apply path settings for tracing storage
	<set>	local /mnt/sd[abc][1-7]*	Configure path for tracing storage: local — local storage in RAM /mnt/sd[abc][1-7]* — path to storage device for tracing storage
	<show>		View path settings for tracing storage
linkset	<LINKSET_INDEX>	0-15	Enter the SS7 link set configuration mode
modifiers table	<MODTBL_INDEX>	0-255	Enter the modifier table configuration mode
network			Enter the network parameter configuration mode
new linkset			Create a new SS7 link set
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 q.850 and sip-reply compliance table

new routing-profile			Create scheduled routing table
new h323-interface			Create H.323 interface
new ss7timers			Create SS7 timer profile
new hunt-group			Create call group
new pickup-group			Create pickup group
numplan			Enter the dial plan configuration mode
pbx_profiles			Enter the PBX profile configuration mode
ports range	<RANGE_PORT>	1-65535	Define the range of UDP ports used for voice traffic (RTP) and data transmission via T.38 protocol
ports show			Show UDP port configuration
ports start	<START_PORT>	1024-65535	Define the starting UDP port used for voice traffic (RTP) and data transmission via T.38 protocol
q931-timers			Enter Q.931 timer configuration mode
quit			Terminate this CLI session
radius			Enter RADIUS configuration mode
record			Enter the conversation recording configuration mode
route			Enter the static route configuration mode
routing			Enter the scheduled routing configuration mode
show running main by_step			Show the current main configuration by steps
show running main whole			Show the current main configuration in full
show running network			Show the current network configuration
show running radius_servers			Show the current RADIUS server configuration
show running snmp			Show the current SNMP configuration
show startup main by_step			Show the initial main configuration by steps
show startup main whole			Show the initial main configuration in full
show startup network			Show the initial network configuration
show startup radius_servers			Show the initial RADIUS server configuration
show startup snmp			Show the initial SNMP configuration
sip configuration			Enter SIP/SIP-T parameter configuration mode
sip interface	<SIPT_INDEX>	0-63	Enter SIP/SIP-T interface parameter configuration mode
sip users			Enter SIP/SIP-T subscriber parameter configuration mode
ss7cat			Enter SS7 category configuration mode
ss7timers	<SS7_TIMERS_INDEX>	0-15	Enter SS7 timer configuration mode
submodule-usage			Enter the configuration mode of SM-VP submodule usage
switch_port			Enter the internal switch configuration mode

Sync/			Enter the configuration mode for synchronization parameters
syslog			Enter the system log parameters configuration mode
trunk	<TRUNK_INDEX>	0-63	Enter the trunk group configuration mode
trunk_direction	<DIRECTION_INDEX>	0-31	Enter the trunk direction configuration mode
v52[1]			Enter the configuration mode for V5.2 parameters for the current E1 stream.

3.3.7 CDR parameter configuration mode

To enter this mode, execute cdr command in the configuration mode.

```
SMG-[CONFIG]> cdr
Entering CDR-info mode.
SMG-[CONFIG]-[CDR]>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
archive	<all> <directory>	String, 31 characters max. String, 31 characters max.	CDR data archiving
category	save	yes/no	Save/do no save subscriber category in CDR files
config			Return to Configuration menu.
duration count mode	<CDR_COUNT_MODE>	round-up/round-down/not-round	Rounding up/down or not rounding (write with milliseconds)
emptysave	<CDR_EMPTY>	yes/no	Save/do no save empty CDR files
enabled	<CDR>	yes/no	Generate/do not generate CDRs
exit			Return from this configuration submenu to the upper level.
fields add <field>			Add specified field in the end of field list (see section3.3.8CDR field list)
fields default			Set basic set of fields
fields flush			Clear list of used fields
fields set <field>	<FIELD_INDEX>	0-39	Substitute field on corresponding position with specified field (see section 3.3.8 CDR field list)
file create mode	<CDR_FILE>	periodically/ once-a-day/ once-an-hour	CDR file creation mode *periodically* — with defined period *once-a-day* — daily *once-an-hour* — hourly
ftp enabled	<CDR_FTP_RES>	yes/no	Transfer/do not transfer CDRs to FRP server
ftp login	<CDR_FTPLOGIN_RES>	String, 31 characters max.	Specify username for FTP server access
ftp passwd	<CDR_PASSWD_RES>	String, 31 characters max.	Specify password for FTP server access
ftp path	<CDR_FTPPATH_RES>	String, 63 characters max.	Set the path to FTP server folder for CDR storage
ftp port	<CDR_FTPPORT_RES>	1-65535	Specify FTP server TCP port
ftp server	<CDR_FTPSERVER_RES>	String, 63 characters max.	Specify FTP server IP address.
header	<CDR_HEADER>	yes/no	Write/do not write the following header

[1] Not supported in the current firmware version.

			into the beginning of CDR file: SMG. CDR. File started at 'YYYYMMDDhhmmss', where 'YYYYMMDDhhmmss' is the record saving start time.
history			View history of entered commands.
localdisk	<set> <show>	/mnt/sd[abc][1-7]*	Path to CDR data storage on local drives View CDR data storage path setting
localkeep period	<day> <hour> <min>	0-30 0-23 0-59	Time of CDR data storage on a local drive
localsave	<no> <yes>		Save CDR data on a local drive
period day	<CDR_DAY>	0-30	Set the time period for CDR generation and saving in the device RAM, days
period hour	<CDR_HOUR>	0-23	Set the time period for CDR generation and saving in the device RAM, hours
period min	<CDR_MIN>	0-59	Set the time period for CDR generation and saving in the device RAM, minutes
pickup mark	<CDR_ pickup _MARK>	yes/no	Add/do not add additional field 'pickup tag' to CDR
quit			Terminate this CLI session
redirectmark	<CDR_REDIRECT_MARK>	yes/no	Add/do not add additional field 'redirection tag' to CDR
redirectsave	<CDR_REDIRECT>	yes/no	Add additional field 'Redirecting number' to CDR, otherwise redirecting number will replace calling party number in redirected calls
redirected duration	<CDR_REDIR_DURATION>	yes/no	specify redirected call duration
release initiator mark	<CDR_RELEASE>	yes/no	Save disconnection initiator tag
reserved ftp enabled	<CDR_FTP_RES>	yes/no	Transfer/do not transfer CDRs to FRP server
reserved ftp login	<CDR_FTPLOGIN_RES>	String, 31 characters max.	Specify username for redundant FTP server access
reserved ftp passwd	<CDR_PASSWD_RES>	String, 31 characters max.	Specify password for redundant FTP server access
reserved ftp path	<CDR_FTPPATH_RES>	String, 63 characters max.	Set the path to redundant FTP server folder for CDR storage
reserved ftp port	<CDR_FTPPORT_RES>	1-65535	Specify redundant FTP server TCP port
reserved ftp server	<CDR_FTPSERVER_RES>	String, 63 characters max.	Specify redundant FTP server address.
show			Show CDR settings
show_dirs			Show path to the FTP server access directory
signature	<CDR_SIGNATURE>	String, 63 characters max.	Specify distinctive feature that will facilitate identification of the device that created the record
unsuccess	<CDR_UNSUCC>	yes/no	Store/do not store unsuccessful calls (not resulted in conversation) into CDR files
upload archive ftp/tftp	<ARCHIVE_NAME> <FTP/TFTP_server>	String, 63 characters max. IP – address	Send archive to FTP/TFTP server

3.3.8 CDR field list

The CDR field list is used in 'fieldsadd<field>' and 'fieldsset<field><n>' commands.

<field>	*Value*
`acct-session-id`	RADIUS Account-Session-Id, value of 'Acct-Session-Id' field that is transmitted to RADIUS by packet of accounting
`called in`	Called number on input (before modification)
`called out`	Called number on output (after modification)
`calling in`	Calling number on input (before modification)
`calling out`	Calling number on input (after all modifications)
`device sign`	Distinguishing feature
`disc code`	Code of disconnection via Q.850
`disc info`	Call status in case of disconnection
`duration`	Call duration
`global-callref`	Global Call Reference (GCR) field
`incoming CID category`	CID category on input (before modification)
`incoming description`	Caller description–subscriber/trunk (TG) name
`incoming E1 chan`	Number of incoming E1 channel
`incoming E1 stream`	Number of incoming E1 flow
`incoming ipaddr`	Caller IP address
`incoming SIP call id`	SIP Call-ID of incoming call
`incoming SS7 category`	SS7 category on input (before modification)
`incoming SS7 CIC`	CIC number of incoming call
`incoming type`	Caller type
`mark pickup`	Call pickup mark
`mark redir`	Call redirection mark
`mark release side`	Mark of disconnection initiator
`numplan in`	Dial plan after that call will be received
`numplan out`	Dial plan after that call will be transmitted
`outgoing CID category`	CID category on input (after modification)
`outgoing description`	Callee description–subscriber/trunk (TG)
`outgoing E1 chan`	Number of outgoing E1 channel

`outgoing E1 stream`	Number of outgoing E1 flow
`outgoing ipaddr`	IP address of callee
`outgoing SIP call id`	SIP Call-ID of outgoing call
`outgoing SS7 category`	SS7 category on output (after modification)
`outgoing SS7 CIC`	CIC number of outgoing call
`outgoing type`	Callee type
`redirecting in`	Number of forwarding party on input (before modification)
`redirecting out`	Number of forwarding party on output (after modification)
`sequential number`	Sequential record number
`time connect`	Connection time
`time disconnect`	Call disconnection time
`time setup`	Time of call receipt

3.3.9 Access categories' configuration mode

To enter this mode, execute 'access category' command in the configuration mode.

```
SMG-[CONFIG]> access category
Entering Access-Category mode.
SMG-[CONFIG]-[ACCESS-CAT]>
```

Command	***Parameter***	***Value***	***Action***
`?`			Show the list of available commands.
`config`			Return to Configuration menu.
`exit`			Return from this configuration submenu to the upper level.
`quit`			Terminate this CLI session

`set access`	`<CAT_IDX>`
	`<ACCESS_IDX>`
	`<ACCESSIBLE>`
		`0-63`
		`0-63`
		`enable/disable`
			Define category mutual access permissions:
			CAT_IDX — configured access category index.
			ACCESS_IDX — category the access to be configured for
			ACCESSIBLE — category access status (available, not available)

`set name`	`<CAT_IDX>`
	`<NAME>`
		`0-63`
		`Access category name, 31 character max. (letters, numbers, underscore character '_')`
			Change access category name
			CAT_IDX — configured access category index.
			NAME — access category name

`show`	`<CAT_IDX>`	`0-63`	Show this access category configuration
`showall`			Show all access categories' configuration

3.3.10 E1 stream configuration mode

To enter this mode, execute 'e1 <E1_INDEX>' command in the configuration mode, where <E1_INDEX> is

E1 stream number.

```
SMG-[CONFIG]> e1 0
Entering E1-stream mode.
SMG-[CONFIG]-E1[0]>
```

Command	***Parameter***	***Value***	***Action***
`?`			Show the list of available commands.
`alarm`	`<ON_OFF>`	`on/off`	Enable/disable fault indication for the current E1 stream
`config`			Return to Configuration menu.
`crc4`	`<ON_OFF>`	`on/off`	Enable/disable CRC4 control for the current E1 stream
`disabled`			Disable the stream operation
`enabled`			Enable the stream operation
`equalizer`	`<ON_OFF>`	`on/off`	Enable/disable E1 stream signal attenuation
`exit`			Return from this configuration submenu to the upper level.
`history`			View history of entered commands.
`lapd`			Enter LAPD parameters configuration mode for the current E1 stream
`linecode AMI`			Set the AMI linear encoding type for the current stream
`linecode HDB3`			Set the HDB3 linear encoding type for the current stream
`name`		`letter or number or '_', '.', '-'. Max 63 symbols`	E1 stream name
`q931`			Enter Q.931 signalling configuration mode for the current E1 stream
`quit`			Terminate this CLI session
`remalarm`	`<ON_OFF>`	`on/off`	Enable/disable remote fault indication for the current stream
`show`			Show the current stream configuration

`signaling`	`<Signaling type>`	`Q931_USR`
		`Q931_NET`
		`SS7`
		`V5.2LE`
			Set the signalling type for the stream
			Possible signalling types: Q931_USR, Q931_NET, SS7, V5.2LE

`slipIND`	`<ON_OFF>`	`on/off`	Enable fault indication when slips are identified in the reception path
`slipTO`	`<TIMEOUT>`	`5sec/10sec/ 20sec/30sec/ 45sec/1min/ 2min/3min/ 5min/10min/ 15min/30min/ 1hour/2hour/6hour`	Specify stream parameter polling frequency; if the slip is detected in that stream, PBX will indicate an alarm for the duration of this timeout.
`ss7`			Enter the configuration mode for SS7 signalling parameters of the current E1 stream.

3.3.10.1 LAPD parameters configuration mode for the current E1 stream

This mode is available for Q.931 signalling only (set by *'signaling'* command).To enter this mode, execute 'lapd' command in the E1 stream configuration mode.

```
SMG-[CONFIG]-E1[0]> lapd
E1[0]. Signaling is Q931
SMG-[CONFIG]-E1[0]-[LAPD]>
```

Command	Parameter	Value	Action
`?`			Show the list of available commands.
`config`			Return to Configuration menu.
`exit`			Return from this configuration submenu to the upper level.
`history`			View history of entered commands.
`N200`	`<N200>`	`0-255`	Specify the number of connection establishment attempts
`quit`			Terminate this CLI session
`show`			Show LAPD configuration
`t200`	`<T200>`	`0-255`	Set T200 timer value, x100ms
`t203`	`<T203>`	`0-255`	Set T203 timer value, x100ms

3.3.10.2 Q.931 signalling configuration mode for the current E1 stream

This mode is available for Q.931 signalling only (set by *'signaling'* command). To enter this mode, execute 'q931' command in the E1 stream configuration mode.

```
SMG-[CONFIG]-E1[0]> q931
E1[0]. Signaling is Q931
SMG-[CONFIG]-E1[0]-[Q931]>
```

Command	Parameter	Value	Action
`?`			Show the list of available commands.
`access category`	`<CAT_IDX>`	`0-31`	Set the access category for a stream
`categoryAON`	`<CAT_AON>`	`0-15`	Define Caller ID category for the incoming call

`channel`	`<CHAN_NUM>`
	`<on_off>`
		`[0-31] or 'all'`
		`on/off`
			Enable/disable specified channel

`chanorder`	`<CHAN_ORDER>`	`up_ring/down_ring/ up_start/down_start`	Specify the channel engagement order: *up_ring* — sequential forward. *down_ring* — sequential back *up_start* — from the first and forward *down_start* — from the first and back
`config`			Return to Configuration menu.
`exit`			Return from this configuration submenu to the upper level.
`history`			View history of entered commands.
`InBand in Disconnect`	`<on_off>`	`on/off`	Enable 'Process PI In-Band in DISCONNECT' option
`invokeID`	`<INVOKE_ID>`	`1024-65535`	Set operation call initial identifier (used as a reference number for unique operation call identification)
`numplan`	`<CLD_PLAN_ID>`	`unknown/ISDN/ telephony/National/ Privat`	Specify dial plan type **To use common dial plan E.164, select 'ISDN/telephony'**
`qsig`	`<ON_OFF>`	`on/off`	Enable/disable QSIG signalling
`quit`			Terminate this CLI session
`RestartChannel`	`<SEND>`	`send/don't_send`	Send/do not send channel RESTART
`RestartInterface`	`<SEND>`	`send/don't_send`	Send/do not send interface RESTART
`RoutingProfile`	`<PROF Number>`	`[0-127] or none`	Select scheduled routing profile
`SendCatAON`	`<ON_OFF>`	`on/off`	Enable/disable Caller ID category transmission as the first digit of a number in the SETUP message **Proper operation requires that this mode is supported by the opposite party**

SendDialTone	<ON_OFF>	on/off	Send/do not send the DialTone ready signal into the line during incoming overlap engagement
SendEndOfDial	<ON_OFF>	on/off	Enable/disable 'End of dial' message transmission
show			Show Q.931 signalling parameter configuration
trunk	<trunk_index>	0-31	Define the trunk group number for the current stream

3.3.10.3 SS7 signalling parameters configuration mode for the current E1 stream

This mode is available for SS7 signalling only (set by *'signaling'* command). To enter this mode, execute 'ss7' command in the E1 stream configuration mode.

```
SMG-[CONFIG]-E1[0]> ss7
E1[0]. Signaling is SS7
SMG-[CONFIG]-E1[0]-[SS7]>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
CIC fill	<CIC> <step>	0-65535 0-255	Define CIC value for all time slots beginning from 0 CIC — CIC starting number step — numbering increment
CIC set	<TIMESLOT> <CIC>	0-31 0-65535	Define CIC value for a single timeslot TIMESLOT — timeslot number CIC — CIC value
config			Return to Configuration menu.
Dchan	<D_CHAN>	0-31	Set D-channel number for a line. 0 — do not use D-channel (voice stream)
DPC MTP3		0-16383	Define DPC MTP3 value for the current stream
exit			Return from this configuration submenu to the upper level.
history			View history of entered commands.
linkset	<linkset_index>	0-15	Assign SS7 link set for the current stream
quit			Terminate this CLI session
show			Show SS7 signalling parameter configuration
SLC	<slc>	0-15	Set the signal channel identifier in SS7 link set

3.3.11 Dynamic firewall's parameters configuration mode

To enter this mode, execute 'firewall dynamic' command in the configuration mode.

```
    SMG-[CONFIG]> firewall dynamic
    Entering dynamic firewallmode.
    SMG-[CONFIG]-[DYN-FIREWALL ]>
```

Command	**Parameter**	**Value**	**Action**
?			Show the 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 blacklist
blacklist remove by addr	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet	Remove an address from the blacklist

		in CIDR notation AAA.BBB.CCC.DDD/FF	
blacklist remove by pos	<POSITION>	0-65635	Remove an address from the blacklist using its position in the list
blacklist show all			Show the blacklist
blacklist show count			Show the number of entries in the list of addresses blocked by 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 blacklist
blacklist show first	<COUNT>	0-4095	Show the defined quantity of addresses from the blacklists starting from the first
blacklist show last	<COUNT>	0-4095	Show the defined quantity of addresses from the blacklists starting from the last
blacklist show position	<POSITION>	0-65635	Show the entry stored in the defined position in the blacklist
block history show all			View the history of the blacklist
block show count			Show the number of entries in the blacklist history
block show address	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Find the defined address in the blacklist history
block show first	<COUNT>	0-4095	Show the defined quantity of addresses from the blacklists history starting from the first
block show last	<COUNT>	0-4095	Show the defined quantity of addresses from the blacklists history starting from the last
block show position	<POSITION>	0-65635	Show the entry stored in the defined position in the blacklist history
blocklist remove by addr	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Remove the address from the list of automatically blocked addresses
blocklist remove by pos	<POSITION>	0-65635	Remove the address from the list of automatically blocked addresses using its position in the list
blocklist show all			Show the list of automatically blocked addresses
blocklist show count			Show the number of entries in the automatically blocked addresses list
blocklist show address	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Find the defined address in the automatically blocked addresses list
blocklist show first	<COUNT>	0-4095	Show the defined number of entries in the automatically blocked addresses list starting from the first
blocklist show last	<COUNT>	0-4095	Show the defined number of entries in the automatically blocked addresses list starting from the last
blocklist show position	<POSITION>	0-65635	Show the entry stored in the defined position in the automatically blocked addresses list
exit			Exit from this configuration submenu to the upper level.
history			View the history of entered commands
quit			Quit the CLI session
set block_time	<SERVICE>	SIP/WEB/TELNET/SSH /OTHER	Set time (in seconds) during which the

	<BLCKTIME>	60-352800	access from a suspicious address will be blocked
set enable	<ENA>	on/off	Enable/disable the dynamic firewall
set tries	<SERVICE> <TRIES>	SIP/WEB/TELNET/SSH /OTHER 1-10	Set the maximum number of access attempts to the service before blocking the host
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 progressing blocking for the service
show			Show the 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 denied 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 denied for automatic blocking
whitelist remove by pos	<POSITION>	0-65635	Remove an IP address from the list of addresses denied for automatic blocking using its position in the list
whitelist show all			Show the list of addresses denied for automatic blocking
whitelist show count			Show the number of entries in the list of addresses denied for 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 the defined address in the list of addresses denied for automatic blocking
whitelist show first	<COUNT>	0-4095	Show the defined number of entries in the list of addresses denied for automatic blocking startinf from the first
whitelist show last	<COUNT>	0-4095	Show the defined number of entries in the list of addresses denied for automatic blocking startinf from the last
whitelist show position	<POSITION>	0-65635	Show the entry stored in the defined position in the list of addresses denied for automatic blocking

3.3.12 Static firewal's parameters configuration mode

To enter this mode, execute 'firewall' command in the configuration mode.

```
SMG-[CONFIG]> firewall static
Entering static firewall mode
SMG-[CONFIG]-[firewall]>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
add profile	<PROF_NAME>	you may use letters, numbers, '_' character, 63 characters max.	Add firewall profile
add rule	<direction> <ENABLE>	forward input output enable/disable	Add firewall rule Rule direction Enable/disable rule

	<RULE_NAME>	Text, 63 characters max.	Rule name
	<S_IP>	AAA.BBB.CCC.DDD	Source IP address
	<S_MASK>	AAA.BBB.CCC.DDD	Source subnet mask
	<R_IP>	AAA.BBB.CCC.DDD	Destination IP address
	<R_MASK>	AAA.BBB.CCC.DDD	Destination 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 timestamp-reply address-mask-request address-mask-reply	ICMP packet type
	<ACTION>	accept, drop, reject 1-65535	Action — action executed by this rule: ACCEPT — packets falling under this rule will

	<P_IDX>		be accepted by the firewall. DROP — packets falling under this rule will be rejected by the firewall without informing the party that has sent these packets. DROP — packets falling under this rule will be rejected by the firewall; the party that has sent the packet will receive either TCP RST packet or 'ICMP destination unreachable'. Firewall profile number
add rule geoip	<direction>	input output	Add firewall GeoIP rule The direction of the rule operation
	<ENABLE>	enable/disable	Enable/disable the rule
	<RULE_NAME>	Text, max 63 characters	Rule name
	<COUNTRY>	Country name	Country to which the address is belong
	<PROTO>	any tcp udp icmp tcp+udp	Protocol type
	<S_PORT_START>	1-65535	Initial source port
	<S_PORT_END>	1-65535	Last source port
	<D_PORT_START>	1-65535	Initial destination port
	<D_PORT_END>	1-65535	Last destination 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	ICMP packet type

		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 – an action implemented according to the rule: — *ACCEPT* – packets which match the rule will be forwarded by the firewall; — *DROP* – packets which match the rule will be dropped by the firewall without informing of the transmitted party; — *REJECT* – packets which match the rule will be dropped by the firewall, and the party transmitted the packet will receive a TCP RST packet or ICMP destination unreachable
	<P_IDX>	1-65535	Firewall profile number
add rule string	<direction>	input output	Add firewall rule – check strings. The direction of the rule operation
	<ENABLE>	enable/disable	Enable/disable the rule
	<RULE_NAME>	Text, max 63 characters	Name of the rule
	<CONTENT>	Text, max 127 characters	Text string which should be in a packet
	<S_IP>	AAA.BBB.CCC.DDD	Source IP address
	<S_MASK>	AAA.BBB.CCC.DDD	Source subnet mask
	<R_IP>	AAA.BBB.CCC.DDD	Destination IP address
	<R_MASK>	AAA.BBB.CCC.DDD	Destination subnet mask
	<PROTO>	any tcp udp icmp tcp+udp	Protocol type
	<S_PORT_START>	1-65535	Initial source port
	<S_PORT_END>	1-65535	Last source port
	<D_PORT_START>	1-65535	Initial destination port
	<D_PORT_END>	1-65535	Last destination port
	<ICMP_TYPE>	none any echo-reply destination-unreachable	ICMP packet type

		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	
	<ACTION>	accept, drop, reject	Action – an action implemented according to the rule: – ACCEPT – packets which match the rule will be forwarded by the firewall; – DROP – packets which match the rule will be dropped by the firewall without informing of the transmitted party; – REJECT – packets which match the rule will be dropped by the firewall, and the party transmitted the packet will receive a TCP RST packet or ICMP destination unreachable
	<P_IDX>	1-65535	Firewall profile number
apply			Apply firewall settings
config			Return to Configuration menu.
del profile	<ID>	1-65535	Remove firewall profile
del rule	<ID>	1-65535	Remove firewall rule
exit			Exit from this configuration submenu to the upper level.
modify profile	<ID> <NAME>	1-65535 you may use letters, numbers, '_' character 63 characters max.	Firewall profile index Enter a new name for the device
modify rule	<Type>	action dport_end dport_start enable icmp-type name prof_id	Modify the firewall rule specified (one of the parameters)

	<ID> <param>	proto r_ip r_mask s_ip s_mask sport_end sport_start traffic-type 1-65535 New value according to this parameter type	
move down	<ID>	1-65535	Move the rule one position down
move up	<ID>	1-65535	Move the rule one position up
quit			Terminate this CLI session
set eth	<PROFILE ID>	0-65535	Assign the rule to the network interface PROFILE ID = 0 means that profile will not be used
set pptp	<PPP_IDX> <PROFILE ID>	0-5 0-65535	Assign the rule to the interface PROFILE ID = 0 means that profile will not be used
set vlan	<VLAN_IDX> <PROFILE ID>	VLAN1…VLAN8 0-65535	Assign the rule to the VLAN PROFILE ID = 0 means that profile will not be used
show config			Show configuration
show interfaces			Show interface parameters:
show system			Show system parameters

3.3.13 FTP parameter configuration mode

To enter this mode, execute 'ftpd' command in the configuration mode.

```
SMG-[CONFIG]> ftpd
Entering ftpd mode.
SMG-[CONFIG]-[FTPd]>
```

Command	**Parameter**	**Value**	**Action**
?			Show the list of available commands
config			Return to Configuration menu.
exit			Exit from this configuration submenu to the upper level.
quit			Terminate this CLI session
set enable	<EN>	on/off	Enable/disable FTP server
set port	<PORT>	1-65535	Specify FTP server port
set interface	<IFACE_NAME>	String, 255 characters max.	Specify FTP server network interface
set timeout idle	<TIME>	0-600	Define idle timeout, in seconds
set timeout login	<TIME>	0-600	Define authorization timeout, in seconds
set timeout session	<TIME>	0-600	Define session timeout, in seconds
show config			Show FTP server configuration
show user			Show user configuration
user add	<USER_NAME> <PASSWD>		Add user Specify name for a new user Specify password for a new 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	Define CDR directory access permissions Define LOG directory access permissions Define MNT directory access permissions (external storages) Set rights for access to CFG catalogue (configuration files)
user del	<IDX>	1-4	Remove user
user modify access	<IDX> <CDR_ACCESS> <LOG_ACCESS> <MNT_ACCESS> <CFG_ACCESS>	0-4 no_access/r/w/r no_access/r/w/r no_access/r/w/r no_access/r/w/r	Modify access permissions of the selected user: - Configure CDR directory access configuration, read/write - Configure log directory access configuration, read/write - Configure mnt directory access configuration, read/write – Configure access to cfg catalogue, read/write
user modify password	<IDX> <PASSWD>	0-4	Modify password of the selected user.

3.3.14 H.323 protocol parameter configuration mode

To enter this mode, execute 'h323 configuration' command in the configuration mode.

```
    SMG-[CONFIG]> h323 configuration
    Entering H323Config-mode.
    SMG-[CONFIG]-H323(config)>
```

Command	Parameter	Value	Action
?			Show the list of available commands
alias H323ID	<IDX>	String, max 63 characters	Set the gateway name used while registration on the Gatekeeper
config			Return to Configuration menu
exit			Exit from this configuration submenu to the upper level.
gatekeeper discover	<ON_OFF>	on/off	Enable/disable GK search mode
gatekeeper DSCP	<GK_DSCP_RAS>	0-63	Assign the IP diffserv priority for RAS messages
gatekeeper H323ID	<GK_H323ID>	String, max 63 characters or none	Set GateKeeper ID. The "none" value removes the ID.
gatekeeper local subscribers	<ON_OFF>	on/off	Allow registration of local users on the local GK
gatekeeper mode	<GK_MODE>	none/ local/ remote	GK operation mode: – *none* - do not use; – *local*; – *remote*.
gatekeeper ipaddr	<IPADDR>	AAA.BBB.CCC.DDD	Set a GK IP address
gatekeeper keepalive	<KEEPAL>	10-86400	Set registration time on the GK
gatekeeper port	<PORT>	1-65535	Set port for the GK
gatekeeper tech-prefix	<GK_TECH_PREFIX>	String, max 255 characters or none	Set technological prefix for the GK. The value "none" removes the prefix.

gatekeeper ttl	<TTL>	90-86400	Set time for re-registration on the GK
gatekeeper use	<ON_OFF>	on/off	Enable/disable GK usage
history			View the command history
iface	<IFACE_NAME>	String, max 255 characters	Set a network interface for H.323
port	<PORT>	1-65535	Set local TCP port number for signalling H.323 messages receiving.
primary DGK H323ID	<DGK_H323ID>	String, max 63 characters or none	Set a main ID for Directory GateKeeper. The "none" value removes the ID.
primary DGK ipaddr	<DGK_IPADDR>	AAA.BBB.CCC.DDD	Set a main IP address for Directory GateKeeper.
secondary DGK H323ID	<DGK_H323ID>	String, max 63 characters or none	Set an additional ID for Directory GateKeeper. The "none" value removes the ID.
secondary DGK ipaddr	<DGK_IPADDR>	AAA.BBB.CCC.DDD	Set an additional IP addresses for Directory GateKeeper.
quit			Quit the CLI session
show			Show the settings

3.3.15 H.323 interface parameter configuration mode

To enter this mode, execute 'h323 interface <H323_INDEX>' command in the configuration mode, where <H323_INDEX> is a number of direction operating via H.323 protocol.

```
    SMG-[CONFIG]> h323 interface 0
    Entering H323-mode.
    SMG-[CONFIG]-H323-INTERFACE[0]>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
access category	<CAT_IDX>	0-31	Define the access category
alias H323ID clear	<H323ID>	String, 63 characters max.	Remove the gateway name during registration at the Gatekeeper
alias H323ID set	<H323ID>	String, 63 characters max.	Add the gateway name during registration at the Gatekeeper
codec disable	<CODEC IDX>	0-3	Disable the defined codec. Codecs are numbered by priority – from 0 (the highest) to 3 (the lowest).
codec pte	<CODEC_IDX> <PTE>	0-3 10/20/30/40/50/ 60/70/80/90	Define payload time
codec ptype	<CODEC_IDX> <PTYPE>	0-3 0-127 or static	Define payload type. The "static" value sets the value by default according to the defined codec.
codec set	<CODEC_IDX> <CODEC>	0-3 G.711-U/ G.711-A/ G.729/ G.723.1_5.3/ G.723.1_6.3	Define used codec
config			Back to Configuration menu.
destination clear			Remove interface destination
destination set	<HOSTNAME>	String, 63 characters max.	Define interface destination
RTP	<DSCP_RTP>	0-255	Define DSCP identifier for RTP traffic
DSCP SIG	<DSCP_SIG>	0-255	Define DSCP identifier for SIG traffic
DTMF mime	<DTMF_c>	0-255	Define SIP-INFO level
DTMF mode	<DTMF_m>	inband/ RFC2833/ SIP-INFO	DTMF mode for the current interface
DTMF payload	<DTMF_p>	96-127	Define payload type for RFC2833
ecan	<CANCELLATION>	voice/ nlp-off-voice/	Set echo cancellation mode:

		modem/ off	*Voice* — echo cancellers are enabled. *Nlp-off-voice* — echo cancellers are enabled in voice mode, non-linear processor (NLP) is disabled. When signal levels on transmission and reception significantly differ, weak signal may become suppressed by the NLP. To avoid this, use this echo canceller operation mode. *Modem* — echo cancellers are enabled in the modem operation mode (direct component filtering is disabled, NLP control is disabled, CNG is disabled). *Off* — do not use echo cancellation (this mode is set by default).
exit			Exit from this configuration submenu to the upper level.
faststart	<ON_OFF>	on/off	Enable/disable faststart
fax detection	<DETECTION>	no/callee/caller/ callee_and_caller	Set the fax detection mode: *no* — disable fax tone detection *callee* — for the receiving party only *caller* — for the transmitting party only *callee_and_caller* — for both receiving and transmitting parties
gain rx	<GAIN>		Set the volume of voice reception (gain of the signal received from the communicating gateway and output to the speaker of the phone unit connected to SMG gateway).
gain tx	<GAIN>		Volume of voice transmission (gain of the signal received from the microphone of the phone unit connected to SMG gateway and transmitted to the communicating gateway).
gatekeeper	<ON_OFF>	on/off	Enable/disable GK
h245tunneling	<ON_OFF>	on/off	Enable/disable tunneling
history			View history of entered commands.
interface rtp	<IFACE_NAME>	String, 255 characters max.	Select network interface for RTP transfer
jitter adaptation period	<JT_AP>	1000-65535	Define the time of jitter-buffer adaptation to the lower limit, in milliseconds
jitter adjust mode	<JT_AM>	non-immediate/ immediately	Specify the jitter buffer adjustment mode: *non-immediate* — gradual *immediately* — instant
jitter deletion mode	<JT_DM>	soft/hard	Specify buffer adjustment mode. Defines the method of packet deletion during buffer adjustment to lower limit. *soft* — device uses intelligent selection pattern for deletion of packets that exceed the threshold. *hard* — packets which delay exceeds the threshold will be deleted immediately.

jitter deletion threshold	<JT_DT>	0-500	Set the threshold for immediate deletion of a packet, in milliseconds When buffer size grows and packet delay exceeds this threshold, packets will be deleted immediately
jitter init	<JT_INIT>	0-200	Specify an initial value of adaptive jitter buffer, in milliseconds
jitter max	<JT_MAX>	0-200	Define the upper limit (maximum size) of adaptive jitter buffer, in milliseconds
jitter min	<JT_MIN>	0-200	Define the size of fixed jitter buffer or lower limit (minimum size) of adaptive jitter buffer
jitter mode	<JT_MODE>	adaptive/non-adaptive	Jitter buffer operation mode: *adaptive* — adaptive *non-adaptive* — fixed
jitter vbd	<JT_VBD>	0-200	Define fixed buffer size for data transmission in VBD mode
max_active	<MAX_ACTIVE>	0-65535	Define the maximum number of active connection for an interface
name	<s_name>	you may use letters, numbers, '_' character 31 characters max.	Define a name for H.323 interface
nat	<NAT>	enable/disable	Enable/disable NAT
numbering plan	<NUMPLAN>	0-15/0-255	Select dial plan
port	<PORT>	1-65535	Define TCP port of the communicating gateway used for SIP signalling reception
quit			Terminate this CLI session
routing_profile	<prof>	0-127	Select scheduled routing profile
RTCP control	<RTCP_c>	2-255	Define the quantity of time periods (RTCP period) during which the opposite party will wait for RTCP protocol packets.
RTCP period	<RTCP_p>	5-255	Define the time period in seconds after which the device send control packets via RTCP protocol.
show config			Show H323 interface information
src verify	<ON_OFF>	on/off	Enable/disable control of media traffic received from IP address and UDP port specified in SDP communication session description; otherwise the traffic from any IP address and UDP port will be accepted.
t38 bitrate	<BITRATE>	nolimit/2400/4800/ 7200/9600/12000/ 14400	Specify the maximum transfer rate of fax transmitted via T.38 protocol
t38 disable			Disable fax reception via T.38 protocol
t38 enable			Enable fax reception via T.38 protocol
t38 fillbitremoval	<ON_OFF>	on/off	Enable/disable padding bit removals and inserts for data that does not relate to ECM
t38 pte	<T38_PTE>	10/20/30/40	Define T.38 packet generation frequency in milliseconds
t38 ratemgmt	<T38_RATE_MGMT>	localTCF/ transferredTCF	Set the data transfer speed management method *local TCF* — method requires that the TCF tuning signal was generated locally by the recipient gateway *transferred TCF* — method requires that the TCF tuning signal was sent

			from the sender device to the recipient device
t38 redundancy	<T38_REDUNDANCY>	off/1/2/3	Enable redundant frames utilization for error control, off — disable
trunk	<TRUNK>	0-31	Define the trunk group number for an interface
VAD_CNG	<ON_OFF >	on/off	Enable/disable voice activity detector / Comfort noise generator for an interface
vbd codec	<CODEC>	G.711-U, G.711-A	Codec used for VBD data transmission
vbd enable			Enable V.152
vbd disable			Disable V.152
vbd payload type	<VBD_p>	Static,96-127	Payload type used for VBD codec

3.3.16 Call group configuration mode

To enter this mode, execute 'hunt-group < hunt-group_INDEX>' command in the configuration mode, where < hunt-group _INDEX> is a pickup group number.

```
SMG-[CONFIG]> hunt-group 0
Entering HuntGroup-mode.
SMG-[CONFIG]-HUNT-GROUP[0]>
```

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands.
config			Return to Configuration menu.
exit			Return from this configuration submenu to the upper level.
history			View history of entered commands.
move number to		End position start	Move the number into the end of the list. Move the number to the specific position. Move the number into the beginning of the list.
quit			Terminate this CLI session
set conference number		*,#,D,0-9. Or 'none' for blank(delete) number	Specify conference number
set ltimer		Number in the range 5-255	Define L-timer of a group call
set mode		(all/seqFisrt/ seqNext/seqAllFirst/ seqAllNextr)	Define group operation mode
set name		letter or number or '_', '.', '-'. Max 63 symbols	Specify call group name
set number			Define call group member number
set record-and-notify mode	<MODE>	simultaneous-notification/ sequential-notification	Set "record and notification" operation mode – simultaneous/separate.
set record-and-notify duration	<DURATION>	15-120	Set the maximum time for notification record.
set stimer		Number in the range 5-255	Set S timer of a one group member call
set number-mask		Max 255 symbols	Set a mask for the call group

3.3.17 SS7 link set modification configuration mode

To enter this mode, execute 'linkset <LINKSET_INDEX>' command in the configuration mode, where <LINKSET_INDEX> is a link set number.

```
SMG-[CONFIG]> linkset 0
Entering Linkset-mode.
SMG-[CONFIG]-LINKSET[0]>
```

Command	***Parameter***	***Value***	***Action***
`?`			Show the list of available commands.
`access category`	`<CAT_IDX>`	`0-31`	Define the access category for the link set
`alarm_ind`	`<ON_OFF>`	`on/off`	Enable/disable fault indication for the specific SS7 link set
`CCI`	`<ON_OFF>`	`on/off`	Enable support for the SS7 link set channel integrity check
`CCI frequency`	`<FREQ>`	`0-127`	Define the frequency of channel integrity checks during outgoing calls performed through the SS7 link set
`cdpn digit in IAM`	`<ON_OFF>`	`on/off`	Transmission of the first digit of CdPN number in IAM message for overlap dialing 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`
			Define the channel engagement order for the current SS7 link set
			up_ring — sequential forward
			down_ring — sequential back
			up_start — from the first and forward
			down_start — from the first and back
			odd_up_ring — sequential forward odd
			odd_down_ring — sequential back odd
			even_up_ring — sequential forward even
			even_down_ring — sequential back even

`china`	`<ON_OFF>`	`on/off`	Enable/disable Chinese SS7 protocol specification support
`combined`	`<ON_OFF>`	`on/off`	Enable/disable combined mode
`config`			Return to Configuration menu.
`DPC`	`<DPC_ID>`	`0-16383`	Define destination point code — DPC
`emergency alignment`	`<ON_OFF>`	`on/off`	Emergency phasing in case of a single signal link in linkset
`exit`			Return from this configuration submenu to the upper level.
`history`			View history of entered commands.
`ignore hold`	`<ON_OFF>`	`off/on`	Ignore the received CPG with remote hold or remote retrieval features

`init`	`<INIT_MODE>`	`blocked/`
		`individual-ublock/`
		`group-unblock/`
		`group-reset`
			Define initialization type for the current link set

`interworking`	`<INTERWORK>`	`no_change/`
		`no_encountered/`
		`encountered`
			Configure extraneous signalling systems interaction indicator:
			no_change — transfer value from the incoming call without any changes
			no_encountered — do not report interaction with a network that does not support the majority of services

			provided by ISDN network. *encountered* — report interaction at selected locations (ISDN network interacts with the network that does not support the majority of services provided by ISDN network and is unable to use commonly used features)
name	<s_name>	you may use letters, numbers, '_' character, 31 characters max.	Define the current link set name
net_ind	<NET_IND>	international/ reserved/federal/ national	Set the network identifier: *international* — international network *reserved* — reserved network *federal* — federal network *national* — local network
numbering plan		0-15	Select dial plan for a LinkSet
OPC	<OPC_ID>	0-16383	Define the origination point code for the current SS7 link set
primary linkset	<PRI_LINKSET>	0-15	Select the primary SS7 link set for the combined mode operation
quit			Terminate this CLI session
release on suspend	<ON_OFF>	on/off	Enable/disable disconnection message output after suspend message reception
reserv linkset	<RES_LINKSET>	0-15	Select redundant SS7 link set
routing_profile	<prof>	0-127	Select scheduled routing profile
satellite	<SATELLITE>	override_no_satellite /transit/ add_one	Identifies the presence of the satellite channel in operation through this SS7 link set
secondary linkset	<SEC_LINKSET>	0-15	Select the secondary SS7 link set for the combined mode operation
show			Show configuration of the current SS7 link set
ss7timers	<index>	0-15	Select SS7 timer profile
TMR	<TMR>	speech/ 64kb_unrestricted/ 3.1KHz_audio/transit	Define the Transmission Medium Requirement for the current SS7 link set
trunk	<trunk_index>	0-31	Define the trunk group number for the current SS7 link set

3.3.18 SS7 timer configuration mode

To enter this mode, execute 'ss7timers <SS7_TIMERS_INDEX>' command in the configuration mode, where <SS7_TIMERS_INDEX> is a profile number.

```
SMG-[CONFIG]> ss7timers 0
Entering SS7Timers-mode.
SMG-[CONFIG]-SS7-TIMERS[0]>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
config			Return to Configuration menu.
exit			Return from this configuration submenu to the upper level.
history			View history of entered commands.
quit			Terminate this CLI session

set mtp2 T1	<TIMER>	400-500	Define MTP2 T1 level timer value (x100ms)
set mtp2 T2	<TIMER>	50-500	Define MTP2 T2 level timer value (x100ms)
set mtp2 T3	<TIMER>	10-20	Define MTP2 T3 level timer value (x100ms)
set mtp2 T4 normal	<TIMER>	75-95	Define MTP2 T4 normal level timer value (x100ms)
set mtp2 T4 emergency	<TIMER>	4-6	Define MTP2 T4 emergency level timer value (x100ms)
set mtp2 T6	<TIMER>	30-60	Define MTP2 T6 level timer value (x100ms)
set mtp2 T7 normal	<TIMER>	5-20	Define MTP2 T7 normal level timer value (x100ms)
set mtp3 T2	<TIMER>	7-20	Define MTP3 T2 level timer value (x100ms)
set mtp3 T4	<TIMER>	5-12	Define MTP3 T4 level timer value (x100ms)
set mtp3 T12	<TIMER>	8-15	Define MTP3 T12 level timer value (x100ms)
set mtp3 T13	<TIMER>	8-15	Define MTP3 T13 level timer value (x100ms)
set mtp3 T14	<TIMER>	20-30	Define MTP3 T14 level timer value (x100ms)
set mtp3 T17	<TIMER>	8-15	Define MTP3 T17 level timer value (x100ms)
set mtp3 T22	<TIMER>	1800-3600	Define MTP3 T22 level timer value (x100ms)
set mtp3 T23	<TIMER>	1800-3600	Define MTP3 T23 level timer value (x100ms)
set isup T1	<TIMER>	150-600	Define ISUP T1 level timer value (x100ms)
set isup T5	<TIMER>	3000-9000	Define ISUP T5 level timer value (x100ms)
set isup T6	<TIMER>	100-600	Define ISUP T6 level timer value (x100ms)
set isup T7	<TIMER>	200-300	Define ISUP T7 level timer value (x100ms)
set isup T8	<TIMER>	150-600	Define ISUP T1 level timer value (x100ms)
set isup T9	<TIMER>	300-2400	Define ISUP T9 level timer value (x100ms)
set isup T12	<TIMER>	150-600	Define ISUP T12 level timer value (x100ms)
set isup T13	<TIMER>	3000-9000	Define ISUP T13 level timer value (x100ms)
set isup T14	<TIMER>	150-600	Define ISUP T14 level timer value (x100ms)
set isup T15	<TIMER>	3000-9000	Define ISUP T15 level timer value (x100ms)
set isup T16	<TIMER>	150-600	Define ISUP T16 level timer value (x100ms)
set isup T17	<TIMER>	3000-9000	Define ISUP T17 level timer value (x100ms)
set isup T18	<TIMER>	150-600	Define ISUP T18 level timer value (x100ms)
set isup T19	<TIMER>	3000-9000	Define ISUP T19 level timer value (x100ms)
set isup T20	<TIMER>	150-600	Define ISUP T20 level timer value (x100ms)
set isup T21	<TIMER>	3000-9000	Define ISUP T21 level timer value (x100ms)
set isup T22	<TIMER>	150-600	Define ISUP T22 level timer value (x100ms)

set isup T23	<TIMER>	3000-9000	Define ISUP T23 level timer value (x100ms)
set isup T24	<TIMER>	1-20	Define ISUP T24 level timer value (x100ms)
set isup T25	<TIMER>	10-100	Define ISUP T25 level timer value (x100ms)
set isup T26	<TIMER>	600-1800	Define ISUP T26 level timer value (x100ms)
set isup T33	<TIMER>	120-150	Define ISUP T33 level timer value (x100ms)
set isup T34	<TIMER>	20-40	Define ISUP T34 level timer value (x100ms)
set isup T35	<TIMER>	150-200	Define ISUP T35 level timer value (x100ms)
show			Show configuration

3.3.19 Configuration mode of submodule usage

To go to this mode you should execute ‘submodule usage’ command in the configuration mode.

```
SMG2016-[CONFIG]> submodule-usage
SMG2016-[CONFIG]-[SUBMODULE-USAGE]>
```

Command	*Parameter*	*Value*	*Action*
?			Show list of the available commands
config			Return to the Configuration menu
history			View a history of the entered commands
quit			Complete CLI session
set msp	<INDEX> 0-5	On/off	Enable/disable submodule SM-VP with selected index
show			Show table of submodule usage.

3.3.20 Modifier table configuration mode

To enter this mode, execute 'modifiers table <MODTBL_INDEX>' command in the configuration mode, where < MODTBL_INDEX> is a table number.

```
SMG-[CONFIG]-TRUNK[0]> modifiers table
Entering TRUNK-Modifiers mode.
SMG-[CONFIG]-TRUNK[0]-MODIFIER>
```

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands.
add	<MODIFIER_MASK> [CLD_RULE] [CLG_RULE]	modifier mask, 255 characters max., should be enclosed in parentheses '(' and ')' modifier rule, 30 characters max. should be enclosed in quotation marks modifier rule, 30 characters max.	Add modifier: MODIFIER_MASK — modifier mask. CLD_RULE — callee number modification rule. CLG_RULE — caller number modification rule.

		should be enclosed in quotation marks	
caller ID request	<YES_NO>	no/yes	Caller ID request
change aoncat	<MODIFIER_INDEX> <AONCAT>	0-512 0-9/any	Edit Caller ID category number for the modifier: MODIFIER_INDEX — modifier number. AONCAT — Caller ID 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 the callee number:
			MODIFIER_INDEX — modifier number.
			CALLED_NP_TYPE — dial plan type.

change called rule	<MODIFIER_INDEX> <CALLED_RULE>	0-8191 modifier rule, 30 characters max. should be enclosed in quotation marks	Edit callee number modification rule for the modifier MODIFIER_INDEX — modifier number. CALLED_RULE — callee number modification rule.
change called type	<MODIFIER_INDEX> <CALLED_TYPE>	0-8191 unknown/ subscriber/ national/ international/ network_specific/ nochange	Edit callee number type for the modifier: MODIFIER_INDEX — modifier number. NUM_TYPE — subscriber number type: - *Subscriber* — used in local call and incoming long-distance call processing. - *National* — used in outgoing long-distance call or local call and incoming long-distance call processing instead of the 'Subscriber'. - *International* — used in long-distance calls and recording-completing circuits for outgoing international call processing. - *network_specific* — specific network number. - *unknown* — unknown number type. *nochange* — keep number type unchanged.
change calling category	<MODIFIER_INDEX> <CALLING_CAT_AON>	0-8191 0-9/nochange	Edit Caller ID category number of a calling party for the modifier:
change calling numbering plan type	<MODIFIER_INDEX> <CALLING_NP_TYPE>	0-8191 nochange/ unknown/	Edit modifier dial plan type for the caller number: MODIFIER_INDEX — modifier

		isdn/ telephony/ national/ private	number. CALLING_NP_TYPE — dial plan type.
change calling presentation	<MODIFIER_INDEX> <CALLING_PRESENT>	0-8191 allowed/ restricted/ not_available/ spare/ nochange	Edit caller presentation modification rule
change calling rule	<MODIFIER_INDEX> <CALLING_RULE>	0-8191 modifier rule, 30 characters max., should be enclosed in quotation marks	Edit caller number modification rule for the modifier MODIFIER_INDEX — modifier number. CALLING_RULE — caller number modification rule.
change calling screen	<MODIFIER_INDEX> <CALLING_SCREEN>	0-8191 not_screened/ user_passed/ user_failed/ network/nochange	Edit caller screen indicator modification rule
change calling type	<MODIFIER_INDEX> <CALLING_TYPE>	0-8191 unknown/ subscriber/ national/ international/ network_specific/ nochange	Edit caller number type for the modifier: MODIFIER_INDEX — modifier number. NUM_TYPE — subscriber number type: - *Subscriber* — used in local call and incoming long-distance call processing. - *National* — used in outgoing long-distance call or local call and incoming long-distance call processing instead of the 'Subscriber'. - *International* — used in long-distance calls and recording-completing circuits for outgoing international call processing. - *network_specific* — specific network number. - *unknown* — unknown number type. *nochange* — keep number type unchanged.
change general access-cat	<MODIFIER_INDEX> <ACCESS>	0-8191 0-31/nochange	Edit modifier access general category
change general numplan	<MODIFIER_INDEX> <NUMPLAN>	0-8191 0-15/nochange	Edit modifier general dial plan
change mask	<MODIFIER_INDEX>	0-8191	Edit modifier mask

	<MODIFIER_MASK>	modifier mask, 255 characters max., should be enclosed in parentheses '(' and ')'	MODIFIER_INDEX — modifier number. MODIFIER_MASK — mask.
change modtable	<MODIFIER_INDEX> <NEW_MODTBL_INDEX>	0-8191 0-255	Move modifier into a table with the specified number
change numtype	<MODIFIER_INDEX> <NUM_TYPE>	0-8191 unknown/ subscriber/ national/ international/ network_specific/ any	Edit number modifier type MODIFIER_INDEX — modifier number. NUM_TYPE — subscriber number type: - *Subscriber* — used in local call and incoming long-distance call processing. - *National* — used in outgoing long-distance call or local call and incoming long-distance call processing instead of the 'Subscriber'. - *International* — used in long distance calls and recording-completing circuits for outgoing international call processing. - *network_specific* — specific network number. - *unknown* — unknown number type. - *any* — any number type.
change type	<MODIFIER_INDEX> <MODIFIER_TYPE>	0-8191 calling/called	Change subscriber type for a modifier (caller/callee)
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
quit			Terminate this CLI session
remove	<MODIFIER_INDEX>	0-8191	Remove the specific modifier
show	<MODIFIER_INDEX>	0-8191	Show modifier configuration
voice channel setup delay	<DELAY>	0-7	Voice frequency path forwarding delay.

3.3.21 Network parameter configuration mode

To enter this mode, execute 'network' command in the configuration mode.

```
SMG-[CONFIG]> network
Entering Network mode.
SMG-[CONFIG]-NETWORK>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
add interface	<LABEL>	you may use letters,	Add a new VPN/PPTP client

pptpVPNclient	<IPADDR> <USER> <PASS>	numbers, '_', '.', '-', ':' characters, 255 characters max. IP address in AAA.BBB.CCC.DDD format you may use letters, numbers, '_', '.', '-', ':' characters, 63 characters max. you may use letters, numbers, '_', '.', '-', ':' characters, 63 characters max.	LABEL — interface name IPADDR — PPTP server IP address USER — username PASS — password
add interface tagged	dynamic/static <LABEL> <VID> <IPADDR> <NETMASK>	you may use letters, numbers, '_', '.', '-', ':' characters, 255 characters max. 1-4095 IP address in AAA.BBB.CCC.DDD format network mask in AAA.BBB.CCC.DDD format	Add a new network interface LABEL — interface name VID — VLAN ID IPADDR — PPTP server IP address NETMASK — network mask
add interface untagged	dynamic/static <LABEL> <IPADDR> <NETMASK>	you may use letters, numbers, '_', '.', '-', ':' characters, 255 characters max. IP address in AAA.BBB.CCC.DDD format network mask in AAA.BBB.CCC.DDD format	Add a new network interface LABEL — interface name IPADDR — PPTP server IP address NETMASK — network
config			Return to Configuration menu.
confirm			Confirm modified network settings and VLAN settings without gateway restart. If you fail to confirm network settings in 1 minute interval, the previous values will be restored.
dhcp server			Enter DHCP server parameter configuration mode
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
ntp			Enter NTP configuration mode
quit			Terminate this CLI session
remove interface	<NET_IFACE_IDX>	0-39	Remove the specific interface
rollback			Rollback changes
set interface broadcast	<NET_IFACE_IDX> <BROADCAST>	0-39 IP address in AAA.BBB.CCC.DDD format	Define broadcast packets address for the specific interface
set interface COS	<NET_IFACE_IDX> <COS>	0-39 0-7	Define 802.1p priority for the specific interface
set interface dhcp	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Obtain network settings dynamically from DHCP server for the specific interface

set interface dhcp_dns	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Obtain DNS server IP address dynamically from DHCP server for the specific interface
set interface dhcp_no_gw	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Do not obtain gateway settings dynamically from DHCP server for the specific interface
set interface gateway	<NET_IFACE_IDX> <IPADDR>	0-39 IP address in AAA.BBB.CCC.DDD format	Define default gateway for the interface
set interface dhcp_ntp	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Obtain NTP settings dynamically from DHCP server for the specific interface
set interface gw_ignore	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Ignore gateway configuration for the specific interface
set interface h323	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Enable H323 signalling exchange for the specific interface
set interface ipaddr	<NET_IFACE_IDX> <IPADDR> <NETMASK>	0-39 IP address in AAA.BBB.CCC.DDD format network mask in AAA.BBB.CCC.DDD format	Define IP address and network mask for the specific interface
set interface network-label	<NET_IFACE_IDX> <LABEL>	0-39 letters, numbers, '_', '.', '-', ':' characters, 255 characters max.	Define a name for the specific interface
set interface radius	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Enable RADIUS message transmission through the interface
set interface rtp	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Enable RTP packet transmission through the interface
set interface run_at_startup	<NET_IFACE_IDX> <STARTUP>	0-39 on/off	Launch the interface automatically upon startup (for VPN interface only)
set interface serverip	<NET_IFACE_IDX> <IPADDR>	0-39 IP address in AAA.BBB.CCC.DDD format	Specify PPTP server IP address
set interface signaling	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Enable SIP message transmission through the interface
set interface snmp	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Enable SNMP packet transmission through the interface
set interface ssh	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Enable ssh session through the interface
set interface telnet	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Enable telnet session through the interface
set interface use_mppe	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Enable/disable encryption (for VPN interface only)
set interfaceuser_name	<NET_IFACE_IDX> <USER>	0-39 you may use letters, numbers, '_', '.', '-', ':' characters, 63 characters max.	Define user name (for VPN interface only)
set interfaceuser_pass	<NET_IFACE_IDX> <PASS>	0-39 you may use letters,	Define password (for VPN interface only)

		numbers, '_', '.', '-', ':' characters, 63 characters max.	
set interfaceVID	<NET_IFACE_IDX> <VID>	0-39 1-4095	Define VID for the interface
set interface web	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Enable web access through the interface
set settingsdns primary	<IPADDR>	IP address in AAA.BBB.CCC.DDD format	Define primary DNS server IP address
set settings dns secondary	<IPADDR>	IP address in AAA.BBB.CCC.DDD format	Define secondary DNS server address.
set settings gateway_iface	<NET_IFACE_NAME>		Name of an interface which gateway should be considered as a primary by default
set settings hostname	<HOSTNAME>	you may use letters, numbers, '_', '.', '-', ':' characters, 63 characters max.	Specify host name
set settings ssh	<PORT>	1-65535	Define TCP port for the device access via SSH protocol, default value is 22
set settings telnet	<PORT>	1-65535	Define TCP port for the device access via Telnet protocol, default value is 23
set settings use_ip_list	<ON_OFF>	on/off	Enable/disable IP whitelist utilization
set settings web	<PORT>	1-65535	Define TCP port for web configurator, default is 80
show interface by_index			Show settings of the specific network interface
show interface list			Show the list of available network interfaces
show settings			Show network parameters
snmp			Enter SNMP configuration mode
sshrestart			Restart SSH process

If IP address or network mask has been changed or web configurator management has been disabled for the network interface, confirm these settings using '*confirm*' command; otherwise the previous configuration will be restored when two minute timeout expires.

3.3.21.1 DHCP server parameters configuration mode

To enter this mode, execute 'dhcp server' command in the network parameter configuration mode.

```
SMG-[CONFIG]-NETWORK> dhcp server
Entering Network mode.
SMG-[CONFIG]-[NETWORK]-[DHCPD]>
```

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands.
conflicttime	<CONFLICT>	10-10000000	Set the time period during which the IP address will remain reserved upon MAC address conflict identification, 10 seconds or more.
declinetime	<DECLINE>	10-10000000	Time period during which the IP address will remain reserved upon the DHCP decline reception, 10 seconds or more.
dhcpd start			Launch DHCP server
dhcpd stop			Stop DHCP server
dns 0/1/2/3	<DNS>	IP address in AAA.BBB.CCC.DDD format	Obtain DNS server addresses from the operator's networks

domain	<DOMAIN>	String, 31 characters max.	Define the domain name used for DHCP clients by default
enabled	<ENABLE>	no/yes	Enable/disable DHCP server upon the gateway startup
exit			Exit from this configuration submenu to the upper level.
gateway	<GW>	IP address in AAA.BBB.CCC.DDD format	Define default router or gateway address assigned to DHCP server clients
interface	<IFACE_NAME>	String, 255 characters max.	Select network interface for DHCP server
ipaddr end	<IPADDR>	IP address in AAA.BBB.CCC.DDD format	Define an ending address in the range of assigned IP addresses
ipaddr start	<IPADDR>	IP address in AAA.BBB.CCC.DDD format	Define a starting address in the range of assigned IP addresses
max_lease	<MAX_LEASE>	10-10000000 sec	Define the maximum lease time for IP address assigned by DHCP server, 10 seconds or more
maxleases	<MAXLEASES>	1-65535	Restrict the number of leased addresses
min_lease	<MIN_LEASE>	10-10000000 sec	Define the minimum lease time for IP address assigned by DHCP server, 10 seconds or more
netmask	<NETMASK>	IP address in AAA.BBB.CCC.DDD format	Define the network mask
ntp announce external server address	<NTP_SERVER>	IP address in AAA.BBB.CCC.DDD format	Define the external NTP server address for announcing via option 42.
ntp announce external server enable	<ANNOUNCE_EXT>	no/yes	Allow the announcing of external NTP server via option 42.
ntp announce local	<ANNOUNCE_LOCAL>	no/yes	Allow the announcing of local NTP server via option 42.
offertime	<OFFER>	10-10000000	Set the time period during which the requested IP address will remain reserved, 10 seconds or more
quit			Terminate this CLI session
savetime	<SAVE>	7200-10000000/off	Set the time interval for saving information on leased addresses to dhcpd.leases file off — do not save the database
show config			Show DHCP configuration: usage status, network mask, default gateway, domain addresses, Wins-servers, number of leased addresses, request timeouts
static_lease add	<NAME> <IPADDR> <MAC>	String, 63 characters max. IP address in AAA.BBB.CCC.DDD format MAC address in XX:XX:XX:XX:XX:XX format	Assign IP and MAC address static matches: *NAME* — match name *IPADDR* — IP address *MAC* — MAC address
static_lease remove	<INDEX>	0-4095	Remove the specified rule from the static IP and MAC address match table
static_lease show			Show static IP and MAC address match table:
wins	<WINS>	IP address in AAA.BBB.CCC.DDD format	Define the primary WINS server IP address for DHCP client usage

3.3.21.2 PPTP client configuration mode

SMG-[CONFIG]-NETWORK> pptp
Entering PPTP mode.
SMG-[CONFIG]-[NETWORK]-PPTP>

Command	Parameter	Value	Action
?			Show the list of available commands.
add interface	<USER> <PASS> <IP_SRV> <LABEL> <MPPE> <STARTUP>	String, 31 characters max. String, 31 characters max. IP address in AAA.BBB.CCC.DDD format; string, 31 characters max. On/off On/off	Specify username Specify password Specify PPTP server IP address Specify tag Enable/disable encryption Run at startup
config			Return to Configuration menu.
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
modify interface	label mppe pssword server_ip startup username	String, 31 characters max. On/off String, 31 characters max. IP address in AAA.BBB.CCC.DDD format On/off String, 31 characters max.	Modify PPTP parameters Modify tag Modify encryption activity Modify password Modify PPTP server IP address Modify automatic PPTP startup Modify username
show			Show PPTP settings
start interface	<IDX_INERFACE>	0-16	Launch PPTP interface immediately
status interface	<IDX_INERFACE>	0-16	View the state of the specific interface
stop interface	<IDX_INERFACE>	0-16	Stop PPTP interface immediately

3.3.21.3 NTP configuration mode

To enter this mode, execute 'ntp' command in the network parameter configuration mode.

SMG-[CONFIG]-NETWORK> ntp
Entering NTP mode.
SMG-[CONFIG]-[NETWORK]-NTP>

Command	Parameter	Value	Action
?			Show the list of available commands.
apply		no/yes	Apply NTP settings
config			Return to Configuration menu.
exit			Exit from this configuration submenu to the upper level.
quit			Terminate this CLI session
restart ntp		no/yes	Restart NTP process

set ntp	dhcp period server usage	off/on 10-1440 IP address in AAA.BBB.CCC.DDD format off/on	Obtain NTP settings via DHCP Define synchronization period Define NTP server Enable/disable NTP usage
show config			Show
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	Specify a timezone in reference to UTC Select location city in Asia Select location city in Europe

3.3.21.4 SNMP configuration mode

To enter this mode, execute 'snmp' command in the configuration mode.

```
SMG-[CONFIG]-NETWORK> snmp
Entering SNMP mode.
SMG-[CONFIG]-SNMP>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
add	<TYPE> <IP> <COMM> <PORT>	trapsink/ trap2sink/ informsink IP address in AAA.BBB.CCC.DDD format String, 31 characters max. 1-65535	Add SNMP trap transmission rule: TYPE — SNMP message type IP — trap recipient IP address COMM — password contained in traps PORT — trap recipient UDP port
config			Return to Configuration menu.
create user	<LOGIN> <PASSWD>	String, 31 characters max. Password, 8 to 31 characters	Create user (define access login and password)
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
modify community	<IDX> <COMM>	0-15 String, 31 characters max.	Modify SNMP trap transmission rule (password contained in traps)
modify ip	<IDX> <IP>	0-15 IP address in AAA.BBB.CCC.DDD format	Modify SNMP trap transmission rule (trap recipient address)
modify port	<IDX> <PORT>	0-15 1-65535	Modify SNMP trap transmission rule (trap recipient port)

modify type	<IDX> <TYPE>	0-15 trapsink/ trap2sink/ informsink	Modify SNMP trap transmission rule (SNMP message type)
quit			Terminate this CLI session
remove	<IDX>	0-15	Remove SNMP trap transmission rule:
restart snmpd	Yes/no		Restart SNMP client
ro	<RO>	String, 63 characters max.	Set the password for parameter reading
rw	<RW>	String, 63 characters max.	Set the password for parameter reading and writing
show			Show SNMP configuration
syscontact	<SYSCONTACT>	String, 63 characters max.	Specify contact information
syslocation	<SYSLOC>	String, 63 characters max.	Specify device location
sysname	<SYSNAME>	String, 63 characters max.	Specify device name

3.3.22 Dial plan configuration mode

To enter this mode, execute 'numplan' command in the configuration mode.

```
SMG-[CONFIG]> numplan
Entering Numbering-plan mode.
SMG-[CONFIG]-[NUMPLAN]>
```

Command	Parameter	Value	Action
?			Show the list of available commands.
config			Return to Configuration menu.
create prefix	<IDX_Numplan>	0-15/0-255	Create prefix in the specified dial plan
delete prefix	<IDX Prefix>		Remove the specified prefix
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
prefix			Enter prefix configuration mode
quit			Terminate this CLI session
set active		0-15/0-255	Define the number of active dial plans
set domain	<IDX> <DOMAIN>	0-15/0-255 String, 15 characters max.	Specify domain for registration
set name	<IDX> <NAME>	0-15/0-255 String, 15 characters max.	Define the dial plan name
show active count			Show the number of active dial plans
show active list			Show the list of active dial plans
show list			Show the list of dial plans
show prefixes	<IDX>	0-15/0-255 no/yes	Show dial plan prefixes with the specific number

3.3.22.1 Prefix configuration mode

To enter this mode, execute 'prefix <PREFIX_INDEX>' command in the configuration mode, where<PREFIX_INDEX> is a prefix number.

```
SMG-[CONFIG]-[NUMPLAN]> prefix 0
Entering Prefix-mode.
SMG-[CONFIG]-[NUMPLAN]-PREFIX[0]>
```

Command	***Parameter***	***Value***	***Action***
`?`			Show the list of available commands.
`access category`	`<CAT_IDX>`	`0-31`	Define the access category
`access check`	`<ON_OFF>`	`on/off`	Check/do not check the access category

`callednpi`	`<PFX_CLD_NPI>`	`transit/`
		`unknown/`
		`isdn/`
		`telephony/`
		`national/`
		`private`
			Modify callee number type (transit — keep unchanged).

`calledtype`	`<PFX_CLD_TYPE>`	`unknown/`
		`subscriber/`
		`national/`
		`international/`
		`specific_net/`
		`transit`
			Callee number type modification (transit — keep unchanged).
			Subscriber number — used in local call and incoming long-distance call processing. At that, transmitted number should be as follows: abxxxxx, or bxxxxx, or xxxxx.
			National number — used in outgoing long-distance call or local call and incoming long-distance call processing instead of the 'Subscriber'. At that, transmitted number should be as follows: ABCabxxxxx, or 2abxxxxx, or 10 <international number>.
			International number — used in LD lines and CLR lines for outgoing international call processing. At that, transmitted number should be as follows: <international number> (without the international network exit prefix '10').

`command`	`<PFX_COMMAND>`	`set/`
		`clear/`
		`control`
			Select action for a service
			set — set VAS service
			clear — cancel VAS service
			control — VAS service activity control

`config`			Return to Configuration menu.

`dial mode`	`<MODE>`	`nochange/`
		`enblock/`
		`overlap`
			Define the prefix dialling mode:
			enblock — callee number will be sent as a block
			overlap — callee number will be sent with an overlap (by a single digit)
			nochange — callee number will be sent as it was received from the incoming channel

`direction`	`<PFX_DIRECTION>`	`local/`
		`emergency/`
		`zone/`
		`vedomst/`
		`toll/`
		`international`
			Define the type of access to the trunk group or direction:
			local — local network;
			emergency — emergency services;

			zone — zone network;
			vedomst — departmental network;
			toll — long-distance network;
			international — international network

duration	<PFX_DURATION>	0-255	Specify number dialling duration timer, in seconds
exit			Exit from this configuration submenu to the upper level.
getCID	<ON_OFF>	on/off	Enable/disable Caller ID request for the prefix routing
history			View history of entered commands.
ivr	<IVR_INDEX>	0-255	Define IVR scenario for ivr-type prefix
mask edit			Enter the prefix mask editing mode
mask show			Show prefix masks
modifiers table called	<MODTBL_INDEX>	0-255 or none	Called number modification table which is used while dial plan changing
modifiers table calling	<MODTBL_INDEX>	0-255 or none	Calling number modification table which is used while dial plan changing
name	<s_name>	string, max 31 characters (letters, digits and '_' sign are allowed to be used)	Define a name/description for prefix
name	<s_name>	String, 31 characters max. (you may use letters, numbers, '_' character)	Specify prefix name/designation
needCID	<ON_OFF>	on/off	Enable/disable CallerID mandatory information request
new access category	<CAT_IDX>	0-127	Select new access category for prefix with 'change-numplan' type.
new numplan	<PLAN_IDX>	0-15/0-255	Select new numbering plan for prefix with 'change-numplan' type.
numplan	<PLAN_IDX>	0-15	Define dial plan that the prefix belongs to
notdial ST	<USE_ST>	yes/no	Disable/enable end dial marker transmission (ST in SS or 'sending complete' in PRI)
pickup-group	<PICKUP_GROUP_INDEX>	0-254/any	Select group for prefix with 'pickup group' type. Defines certain group or mode in which any group which includes subscriber's number is selected.
quit			Terminate 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	VAS service type *cf-unconditional* — call forward unconditional *cf-busy* — call forward on busy *cf-no-reply* — call forward on no reply *cf-out-of-order* — call forward on out of service
show			Show prefix configuration
stimer	<PFX_LTIMER>	0-255	Specify time in seconds during which the digital gateway will wait for further dialling if the dialled number matches some sample in the dial plan, but the

			dialling of additional digits is possible at the same time that will cause a match with another sample. Default value — 5 seconds.
trunk	<TRUNK>	0-31	Specify trunk group number or direction
type	<PFX_TYPE>	trunk/ trunk-direction/ change-numplan/ modifier/ user_service pickup-group/ ivr	Define prefix type: *trunk* — transition to trunk group *trunk direction* — transition to trunk direction change-numplan — change dial plan *modifier* — modifier prefix type *user_service* — VAS prefix *pickup-group* — pickup group *ivr* — select IVR scenario

3.3.22.2 Prefix mask configuration mode

To enter this mode, execute 'mask edit' command in the prefix configuration mode.

```
SMG-[CONFIG]-PREFIX[0]> mask edit
Entering Prefix-Mask mode.
SMG-[CONFIG]-PREFIX[0]-MASK>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
add	<PREFIX_MASK> [PFX_MASK_TYPE]	prefix mask. 255 characters max., should be enclosed in parentheses '(' and ')' calling/called [called]	Add a new mask into the prefix. You may specify the mask type — for a caller ('calling') or callee ('called'); default mask type is always 'called'.
config			Return to Configuration menu.
history			View history of entered commands.
exit			Exit from this configuration submenu to the upper level.
modify duration	<PREFIX_MASK_INDEX> <DURATION>	0-1024 0-255	Specify number dialling duration timer. PREFIX_MASK_INDEX — mask number DURATION — timer
modify Ltimer	<PREFIX_MASK_INDEX> <LONG_TIMER>	0-1024 0-255	Define the long timer PREFIX_MASK_INDEX — mask number LONG_TIMER — timer
modify mask	<PREFIX_MASK_INDEX> <PREFIX_MASK>	0-1024 prefix mask. 255 characters max., should be enclosed in parentheses '(' and ')'	Modify mask PREFIX_MASK_INDEX — mask number PREFIX_MASK — mask

modify prefix	<PREFIX_MASK_INDEX> <PFX_INDEX>	0-1024 0-255	Transfer mask to another prefix PREFIX_MASK_INDEX — mask number to be transferred PFX_INDEX — prefix that the mask is being transferred to
modify stimer	<PREFIX_MASK_INDEX> <SHORT_TIMER>	0-1024 [0-255]	Define the short timer PREFIX_MASK_INDEX — mask number DURATION — timer
modify type	<PREFIX_MASK_INDEX> <PFX_MASK_TYPE>	0-1024 calling/called	Define the mask type — caller or callee number analysis: PREFIX_MASK_INDEX — mask number to be transferred PFX_MASK_TYPE — mask type: – calling — caller number analysis. – called — callee number analysis.
quit			Terminate this CLI session
remove	<PREFIX_MASK_INDEX>	0-1024	Remove mask
show			Show mask information

3.3.23 Pickup group configuration mode

To enter this mode, execute 'pickup-group <pickup-group_INDEX>' command in the configuration mode, 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 the list of available commands.
exit			Return from this configuration submenu to the upper level.
history			View history of entered commands.
member add	<CALL_NUMBER >	symbols(not more then 30): *,#,D,0-9. Or 'none' for blank(delete) number.	Add pickup group member
member remove	<GROUP_MEMBER_INDEX>	[0-19]	Remove pickup group member
member set number	<GROUP_MEMBER_INDEX>	[0-19]	Define pickup group member number
member set user-type	<GROUP_MEMBER_INDEX> <USER_TYPE>	[0-19] 0 - 'restricted', 1 - 'ordinary', 2 - 'privileged'	Define call group member type 0 — limited 1 — common 2 — privileged
show			Show the pickup group settings

3.3.24 PBX profile configuration mode

To enter this mode, execute 'pbx_profiles' command in the configuration mode.

```
SMG-[CONFIG]> pbx_profiles
Entering PBX profiles mode.
SMG-[CONFIG]-PBX_PROFILES>
```

Command	***Parameter***	***Value***	***Action***
`?`			Show the list of available commands.

`add pbx`	`<NAME>`
	`<PREFIX>`
	`<PFX>`
		`String, 63 characters max.`
		`1-15`
		`0-255/none`
			Add PBX profile with the specified name, prefix number and direct prefix number

`config`			Return to Configuration menu.
`exit`			Exit from this configuration submenu to the upper level.

`flash mode`	`<PROFILE_INDEX>`
	`<FLASH>`
		`0-31`
		`none/`
		`flash1/`
		`flash2/`
		`flash3`
			Flash signal transmission mode

`history`			View the command history
`history`			View history of entered commands.

`modifiers table incoming called`	`<PROFILE_INDEX>`
	`<MODTBL_INDEX>`
		`0-31`
		`0-255/none`
			Define PBX profile modifier based on the analysis of the callee number received from the incoming channel.

`modifiers table incoming calling`	`<PROFILE_INDEX>`
	`<MODTBL_INDEX>`
		`0-31`
		`0-255/none`
			Define PBX profile modifier based on the analysis of the caller number received from the incoming channel.

`modify pbx connected number transit`	`<CONNNUM>`	`normal/block`	Deny 'Connected number' field transmission

`modify pbx direct_pfx`	`<PROFILE_INDEX>`
	`<PFX>`
		`0-31`
		`0-255/none`
			Transition to the prefix without caller or callee number analysis. It enables switching of all calls coming from SIP subscriber to a trunk group regardless of the dialled number (without mask creation in prefixes).

`modify pbx inband messages`	`<PROFILE_INDEX>`
	`<YES/no>`
		`0-31`	Transmission of voice message phrases

`modify pbx name`	`<IDX>`
	`<NAME>`
		`0-31`
		`String, 63 characters max.`
			Rename the specific profile

`modify pbx prefix`	`<IDX>`
	`<PREFIX>`
		`0-31`
		`Up to 15 digits or 'none'`
			Redefine the PBX prefix for the specified profile

`modify pbx routing_profile`	`<IDX>`	`0-127`	Select scheduled routing profile
`timeout busy-signal`	`<TIMER>`	`0-31`	Busy tone timeout for call transfer service
`timeout cfnr`	`<TIMER>`	`0-31`	Call forward on no reply (CFNR) timeout
`timeout cfoos`	`<TIMER>`	`0-31`	Call forward on out of service (CFOOS) timeout
`timeout first-digit`	`<TIMER>`	`0-31`	First digit dial timeout for call transfer service
`timeout next-digit`	`<TIMER>`	`0-31`	Next digit dial timeout for call transfer service
`quit`			Terminate this CLI session
`remove pbx`	`<IDX>`	`0-31`	Remove PBX profile with the specific number
`show pbx`			Show the PBX profile list

3.3.25 Q.931 timer configuration mode

To enter this mode, execute 'q931-timers' command in the configuration mode.

```
SMG-[CONFIG]> q931-timers
Entering q931-timers mode.
SMG-[CONFIG]-[q931-T]>
```

Command	Parameter	Value	Action
?			Show the list of available commands.
config			Return to Configuration menu.
exit			Exit from this configuration submenu to the upper level.
quit			Terminate 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	Define t301 timer value Define t302 timer value Define t303 timer value Define t304 timer value Define t305 timer value Define t306 timer value Define t307 timer value Define t308 timer value Define t309 timer value Define t310 timer value Define t312 timer value Define t313 timer value Define t314 timer value Define t316 timer value Define t317 timer value Define t320 timer value Define t321 timer value Define t322 timer value
show			Show Q.931 timer configuration

3.3.26 RADIUS configuration mode

To enter this mode, execute 'radius' command in the configuration mode.

```
SMG-[CONFIG]> radius
Entering RADIUS mode.
SMG-[CONFIG]-RADIUS>
```

Command	Parameter	Value	Action
?			Show the list of available commands.
acct ipaddr	<IP_ADDR> <SRV_IDX>	IP address in AAA.BBB.CCC.DDD format 0-8	Define the account server (Accounting) IP address. IP_ADDR — IP address SRV_IDX — server number
acct port	<PORT> <SRV_IDX>	0-65535 0-8	Define the account server (Accounting) port. PORT — port number SRV_IDX — server number
acct secret	<SECRET> <SRV_IDX>	String, 31 characters max. 0-8	Define the account server (Accounting) password. SECRET — password SRV_IDX — server number

acct server_group	<SRV_GROUP_ID> <SRV_IDX>	0-3 0-7	Set the group for accounting server *SRV_GROUP_ID* – group number *SRV_IDX* – server number
auth ipaddr	<IP_ADDR> <SRV_IDX>	IP address in AAA.BBB.CCC.DDD format 0-8	Set an IP address of authorization server *IP_ADDR* – IP address; *SRV_IDX* – server number
auth local	<AUTH_LOCAL>	no/yes	Allow access to local administrator in case of RADIUS server deny
auth port	<PORT> <SRV_IDX>	0-65535 0-8	Set a port of authorization server *PORT* – port number; *SRV_IDX* – server number
auth secret	<SECRET> <SRV_IDX>	string, max. 31 character 0-8	Set a password for authorization server SECRET – password; SRV_IDX – server number
auth server_group	<SRV_GROUP_ID> <SRV_IDX>	0-3 0-7	Set a group for authorization server *SRV_GROUP_ID* – group number *SRV_IDX* – server number
auth user	<AUTH_USER>	no/yes	web/telnet/ssh users authorization via RADIUS
config			Return to Configuration menu.
deadtime	<DEADTIME>	5-60	Server unavailability time during failure — amount of time that the server is deemed unavailable (requests will not be sent to it).
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
iface	<IFACE_NAME>	String, 255 characters max.	Specify RADIUS network interface
profile	<PROFILE_INDEX>	0-31	Proceed to RADIUS profile parameters configuration
quit			Terminate this CLI session
retries	<RETRIES>	2-5	Specify the number of request transmission attempts
show config			Show the RADIUS server configuration information
timeout	<TIMEOUT>	3-10	Define the amount of time intended for server response (x100ms)
voice-msg-table	<TABLE_INDEX>	0-31	Select RADIUS responses to voice messages correspondence tables

3.3.26.1 RADIUS profile parameter configuration mode

To enter this mode, execute 'profile <PROFILE_INDEX>' command in the RADIUS configuration mode, where <PROFILE_INDEX> is a RADIUS profile number.

```
SMG-[CONFIG]-RADIUS> profile 0
Entering RADIUS-Profile-mode.
SMG-[CONFIG]-RADIUS-PROFILE[0]>
```

Command	***Parameter***	***Value***	***Action***
`?`			Show the list of available commands.
`acct answer`	`<ON/OFF>`	`off/on`	Enable/disable acct message transmission for call-orig=answer
`acct CdPN`	`<CDPN_MODE>`	`CdPN-IN/CdPN-OUT`	Define the callee number for Accounting-Request packets: CdPN-IN — use callee number prior to modification (received in SETUP/INVITE packet). CdPN-OUT — use callee number after the modification.
`acct CgPN`	`<CGPN_MODE>`	`CgPN-IN/CgPN-OUT`	Define the caller number for Accounting-Request packets: CdPN-IN — use caller number prior to modification (received in SETUP/INVITE packet). CdPN-OUT — use caller number after the modification.
`acct duration count mode`	`<RADIUS_COUNT_MODE>`	`round-up/round-down/not-round`	Time rounding parameters: up, down, not rounding (transmit milliseconds)
`acct originate`	`<ON/OFF>`	`off/on`	Enable/disable acct message transmission for call-orig= `originate`
`acct restrict`	`<RESTRICT>`	`none/zone/ local/emergency/ restrict-all`	Define the outgoing communications restriction during the server fault (server response non-reception): *none* — allow all calls. *zone* — allow calls to emergency services, local and zone network. *local* — allow calls to emergency services and local network. *emergency* — allow calls to emergency services only. *restrict* — deny all calls.
`acct start`	`<ON_OFF>`	`on/off`	Enable/disable acct. start message transmission
`acct stop`	`<ON_OFF>`	`on/off`	Enable/disable acct. stop message transmission
`acct update`	`<ON_OFF>`	`on/off`	Enable/disable acct. update message transmission
`acct update_period`	`<PERIOD>`	`10sec/20sec/30sec/ 45sec/1min/2min/ 3min/5min/10min/ 15min/30min/1hour`	Acct. update message transmission period
`acct unsuccessfull`	`<ON_OFF>`	`on/off`	Enable/disable transmission of information on unsuccessful calls to RADIUS server
`acct user-name answer`	`<USERNAME_MODE>`	`cgpn/ ip_or_stream/ trunk/cdpn/initial_cgpn/ initial_cdpn`	Set a User-Name attribute value in Accounting-Request packets for 'answer' party: *cgpn* – use a caller phone number as the value; *ip_or_stream* – use a caller IP address or number of the stream via which the connection is

			implemented; *trunk* – use a name of the trunk, via which the connection is implemented, as the value; *cdpn* - use a callee number as the value ; *initial_cgpn* - use the non-modified phone number of the calling number; *initial_cdpn* - use a non-modified phone number of the callee number.
acct user-name originate	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk/cdpn/initial_cgpn/ initial_cdpn	Set a User-Name attribute value in Accounting-Request for originate party: *cgpn* – use a caller phone number as the value; *ip_or_stream* – use a caller IP address or number of the stream via which the connection is implemented; *trunk* – use a name of the trunk, via which the connection is implemented, as the value; *cdpn* - use a callee number as the value; *initial_cgpn* - use a non-modified phone number of the calling number; *initial_cdpn* - use a non-modified phone number of the callee number
auth check on seize	<ON_OFF>	on/off	Enable/disable authorization (Authorization) request transmission during the incoming engagement
auth check on stop-dial	<ON_OFF>	on/off	Enable/disable authorization (Authorization) request transmission during the end of dial
auth check on local-redir	<ON_OFF>	on/off	Enable/disable authorization (Authorization) request transmission during the local redirection
auth digestauth	<DIGESTAUTH>	rfc4590/ rfc4590-no-challenge/ draft-sterman	Select subscriber authorization algorithm with dynamic registration through the RADIUS server. In DIGEST authorization, the password is transferred as a hash code; thus, it cannot be intercepted during traffic scanning
auth emergency-on-REJ	<PERMIT>	not-allow/allow	Enable/disable access to emergency services after reception of connection refuse from server
auth framedprotocol	<FRAMED_PROTOCOL>	none/PPP/ SLIP/ARAP/ Gandalf/Xylogics/ X75_Sync	Assign protocol during packet access utilization for RADIUS authentication requests

			none — packet access will be disabled
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	Define NAS physical port type (server for user authentication), default value is Async.
auth pass	<PASSWD>	Password, 15 characters max.	Specify User-Password attribute value in the corresponding RADIUS-Authorization packet
auth restrict	<RESTRICT>	none/zone/ local/emergency/ restrict-all	Define the outgoing communications restriction during the server fault (server response non-reception): *none* — allow all calls. *zone* — allow calls to emergency services, local and zone network. *local* — allow calls to emergency services and local network. *emergency* — allow calls to emergency services only. *restrict all* — deny all calls.
auth service type	<SERVICE_TYPE>	none/ Login/ Framed/ Callback_Login/ Callback_Framed/ Outbound/ Administrative/ NAS_Promt/ Authenticate_Only/ Callback_NAS_Prompt/ Call_Check/ Callback_Administrative	Type of service, not used by default (none)
auth session time	<SESSION_TIME_MODE>	ignore/ use_RFC_Session_timeout/ use_CISCO_h323_ credit_time	Define the maximum call duration limit on the basis of an attribute value transmitted in Access-Accept from the RADIUS server. *ignore* — ignore the limitation of the maximum call duration. *use_rfc_session_timeout* — use Session-Timeout attribute value as the maximum call duration timeout. *use_cisco_h323_credit_time* — use Session-Time or Cisco VSA h323-credit-time attribute value as the maximum call duration timeout.

auth user-name answer	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk/cdpn/initial_cgpn/ initial_cdpn	Set User-Name attribute value in Access–Request packets for answer party: *cgpn* – use a caller phone number as the value; *ip_or_stream* – use a caller IP address or number of the stream via which the connection is implemented; *trunk* – use a name of the trunk, via which the connection is implemented, as the value; *cdpn* - use a callee number as the value; *initial_cgpn* - use a non-modified phone number of the calling number; *initial_cdpn* - use a non-modified phone number of the callee number
auth user-name originate	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk/cdpn/initial_cgpn/ initial_cdpn	Set User-Name attribute value in Access–Request packets for originate party: *cgpn* – use a caller phone number as the value; *ip_or_stream* – use a caller IP address or number of the stream via which the connection is implemented; *trunk* – use a name of the trunk, via which the connection is implemented, as the value; *cdpn* - use a callee number as the value; *initial_cgpn* - use a non-modified phone number of the calling number; *initial_cdpn* - use a non-modified phone number of the callee number
auth userpasswd	<ON_OFF>	on/off	Enable/disable custom passwords for SIP subscribers during authorization
modifiers table auth mode	MODTABLE_MODE	default/restricted	An authorization mode of a number in RADIUS. restricted - only numbers, which match masks in the modifiers table, are authorized.
modifiers table acct mode	MODTABLE_MODE	default/restricted	A number accounting mode in RADIUS. restricted - accounting is available only for numbers, which match masks in the modifiers table.

modifiers table incoming called	<MODTBL_INDEX>	0-255/none	Define callee (CdPN) number modifier for the incoming connection in relation to Called-Station-Id, xpgk-dst-number-in fields of RADIUS-Authorization and RADIUS-Accounting messages
modifiers table incoming calling	<MODTBL_INDEX>	0-255/none	Define caller (CgPN) number modifier for the incoming connection in relation to Calling-Station-Id, xpgk-src-number-in fields of RADIUS-Authorization and RADIUS-Accounting messages
modifiers table outgoing called	<MODTBL_INDEX>	0-255/none	Define callee (CdPN) number modifier for the outgoing connection in relation to xpgk-src-number-out field of RADIUS-Authorization and RADIUS-Accounting messages
modifiers table outgoing calling	<MODTBL_INDEX>	0-255/none	Define caller (CgPN) number modifier for the outgoing connection in relation to xpgk-dst-number-out field of RADIUS-Authorization and RADIUS-Accounting messages.
config			Return to Configuration menu.
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
quit			Terminate this CLI session
reset voice-msg-table			Do not use RADIUS responses to voice messages correspondence tables
server_group	<SRV_GROUP>	0-3	A number of a group of RADIUS servers which will be used by the profile
set vmt-reply-attribute		h323-return-code/Reply-Message	Select an attribute that will be used for RADIUS-reject message analysis
set voice-msg-table	<TABLE_IDX>	[0-31]	Select RADIUS responses to voice messages correspondence tables
show			Show RADIUS profile configuration
use acct	<ON_OFF>	on/off	Enable/disable Accounting request transmission to the RADIUS server
use auth	<ON_OFF>	on/off	Enable/disable Authorization request transmission to the RADIUS server
use class as ss7cat	<ON_OFF>	on/off	Use AV-Pair Class for SS7 subscriber category transmission
use eltex-vsa	<ON_OFF>	on/off	Enable RCM service
use full cisco-vsa	<ON_OFF>	on/off	Use a full Cisco-VAS value for RCM service
use porta billing	<ON_OFF>	on/off	Enable/disable PortaBilling
use porta routing	<ON_OFF>	on/off	Enable/disable PortaRouting
use incoming called		original/processed	Define CdPN number transmitted in *xpgk-dst-number-in* field of RADIUS-Authorization and RADIUS-Accounting messages
use incoming calling		original/processed	Define CgPN number transmitted in xpgk-dst-number-in field of RADIUS-Authorization and RADIUS-Accounting messages
use snmp	<ON_OFF>	on/off	Send SNMP trap when applying the RADIUS server
use utc time	<ON_OFF>	on/off	Use time in UTC format

3.3.27 Conversation recording settings configuration mode

To enter this mode[1], execute 'record' command in the configuration mode.

```
SMG-[CONFIG]> record
Entering Record-setup mode.
SMG-[CONFIG]-[RECORD]>
```

Command	Parameter	Value	Action
?			Show the list of available commands.
ftp enabled	REC_FTP	no/yes	Save call records on the FTP server
ftp login	REC_FTPLOGIN	string of up to 63 characters	Login to access to FTP
ftp mode recording	REC_MODE	once-a-day/ once-an-hour/ once-an-minute	Upload mode – once a day, once an hour, once a minute
ftp passwd	REC_PASSWD	string of up to 63 characters	Password to access to FTP
ftp path	REC_FTPPATH	string of up to 63 characters	Path to the files on FTP
ftp period day	REC_HOUR REC_MINUTE	0-23 0-59	Set time of uploading files to FTP for 'once a day' mode
ftp period hour	REC_MINUTE	0-59	Set minutes of uploading files to FTP for 'once an hour' mode
ftp port	REC_FTPPORT	1-65535	FTP server port
ftp remove-after-upload	REC_FTP_REMOVE	no/yes	Delete records from the local storage after uploading to FTP
ftp server	REC_FTPSERVER	string of up to 63 characters	An address or domain name of the FTP server
ftp enabled	REC_FTP	no/yes	Save call records on the FTP server
set action on full disk		stop-recording/remove-old-files	Select an action for full disk: Stop recording/Delete obsolete
set dirname		none or string, 63 characters max.	Define the name of directory for conversation recording files
set dirname_IVR		none or string, 63 characters max.	Define the name of directory for IVR conversation recording files
set files count per dir	FILECOUNT	100-65535 or unlimited	The quantity of record files in a single directory
set files keep period day	KEEP_DAY	0-90	The quantity of days of storing records on the local storage
set files keep period hour	KEEP_HOUR	0-23	The quantity of hours of storing records on the local storage
set notification	<NOTIFY_TYPE >	None voiceless	Notification on conversation recording start
set path		off/mnt/sd[abc][1-7]*	Define the path to conversation recording files storage

3.3.28 Call records masks configuration modes

Imply the **mask** command in configuration mode to move to this mode[2].

```
SMG2016-[CONFIG]-[RECORD]> mask
Entering Record-Mask mode.
SMG2016-[CONFIG]-[RECORD]-MASK>
```

Command	Parameter	Value	Action
?			Show the list of available command

[1] The menu is available for the devices with Call-record license. Read more detailed information on licenses in the section 3.1.23 Licenses.

[2] This menu is available in the firmware version with Call-record license only, for license details, see Section 3.1.23.Licenses

exit			Exit from this configuration submenu to the upper 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 taken in brackets – «(» and «)»; *number type* - any, calling, called
modify category	RECORD_MASK_INDEX CAT_IDX	0-4095 0-31	Change call record categoty for a mask
modify direction	RECORD_MASK_INDEX REC_MASK_TYPE	0-4095 all/ calling/ called	Change mask number type to a defined one
modify mask	RECORD_MASK_INDEX PREFIX_MASK	0-4095 String, max. 255 characters	Change mask value The mask must be taken in brackets «(» and «)».
modify notification	RECORD_MASK_INDEX NOTIFY_TYPE	0-4095 none/voice_message	Notification on a record start none - do not notify voice_message - notify by 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	Delete a mask
show			Show all the masks

3.3.29 Static route configuration mode

To enter this mode, execute 'route' command in the configuration mode.

```
SMG-[CONFIG]> route
Entering route mode.
SMG-[CONFIG]-ROUTE>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
config			Return to Configuration menu.
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
quit			Terminate this CLI session
route add	<DESTINATION> <MASK> <GATEWAY> <METRIC> <IFACE_NAME>	IP address in AAA.BBB.CCC.DDD format Mask in AAA.BBB.CCC.DDD format Gateway in AAA.BBB.CCC.DDD format Unsigned integer value	Add 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 route

	`<ENABLE>`	`String, 255 characters max. disable/enable`	
`route del`	`<IDX>`	`0-4095`	Remove route: `IDX` — network route index
`show`			Show the route configuration information

3.3.30 Q.850 release causes list configuration

To enter this mode, execute 'record' command in the configuration mode.

```
SMG1016M-[CONFIG]> release cause list 0
Entering RelCauseList-mode.
SMG1016M-[CONFIG]-REL-CAUSE-LIST[0]>
```

Command	***Parameter***	***Value***	***Action***
`?`			Show the list of available commands.
`add cause`	`<CAUSE>`	`1-127`	Add q.850 reason into table
`config`			Return to Configuration menu.
`exit`			Exit from this configuration submenu to the upper level.
`history`			View history of entered commands.
`quit`			Terminate this CLI session
`remove cause`	`<CAUSE>`	`1-127`	Remove q.850 reason from table
`set name`	`<LIST_NAME>`	`letter or number or '_', '.', '-'. Max 63 symbols`	Specify table name
`show`			Show table configuration

3.3.31 SIP/SIP-T general settings editing mode

To enter this mode, execute 'sip configuration' command in the configuration mode.

```
SMG-[CONFIG]> sip configuration
Entering SIP/SIP-T/SIP-I/SIP-profile config mode.
SMG-[CONFIG]-SIP(general)>
```

Command	***Parameter***	***Value***	***Action***
`?`			Show the list of available commands.
`cause codes KZ`	`<ON_OFF>`	`on/off`	Enable/disable the specification in accordance with the requirements of the Republic of Kazakhstan
`config`			Return to Configuration menu.
`dynamic route profile`	`<PROFILE>`	`0-63`	SIP profile for dynamic routing
`exit`			Exit from this configuration submenu to the upper level.
`history`			View history of entered commands.
`ignore_RURI`		`no/yes`	Ignore/do not ignore address in R-URI.Address information after '@' separator in Request-URI will be ignored; otherwise, the gateway will check if the address information matches to the device IP address and host name, and if there is no match, the call will be rejected.
`port destination`	`<PORT>`	`1-65535`	Define the server port for syslog messages receiving and transmission.
`port source`	`<PORT>`	`1-65535`	Define SMG port for messages receiving and transmission.

quit			Terminate this CLI session
ringing timeout	<RING_TIMER>	10-255	Call response timeout
save_database	on/off		Save/do not save the information on registered subscribers into the gateway non-volatile memory. It allows you to keep the registered subscribers' database in case of device reboot due to power loss or failure. In case of reboot from the WEB or CLI, the gateway will store the current database into the non-volatile memory regardless of this setting.
show			Show SIP-T general configuration
T1	<T1_TIMER>	0-255	Define SIP timer T1
T2	<T2_TIMER>	0-255	Define SIP timer T2
T4	<T4_TIMER>	0-255	Define SIP timer T4
transport	<TRANSPORT>	UDP-only/ UDP-prefer/ TCP-prefer/ TCP-only	Define transport layer protocol used for SIP message transmission and reception: *TCP-prefer* — reception via UDP and TCP. Transmission via TCP. If TCP connection was not established, transmission will be performed via UDP. *UDP-prefer* — reception via UDP and TCP. Packets exceeding 1300 bytes will be sent via TCP, under 1300 bytes — via UDP. *USP-only* — use UDP protocol only. *TCP-only* — use TCP protocol only.
write_timeout	<TIMEOUT>	1hour/ 2hours/ 4hours/ 6hours/ 8hours/ 12hours/ 16hours	Define archive database update period (from 1 to 16 hours)

3.3.32 SIP/SIP-T interface parameter configuration mode

To enter this mode, execute 'sip interface <SIPT_INDEX>' command in the configuration mode, where <SIPT_INDEX> is SIP/SIP–T interface number.

```
SMG-[CONFIG]> sip interface 0
Entering SIPT-mode.
SMG-[CONFIG]-SIP/SIPT-INTERFACE[0]>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
access category	<CAT_IDX>	0-31	Define the access category
alarm indication	<on/off>		Enable interface unavailability fault indication.
category mode	<MODE>	none category cpc cpc-rus	Do not transfer Caller ID category to SIP. Transfer Caller ID category in the specified field, 'none' — do not transfer Caller ID category to SIP.
CCI	<on/off>	on/off	Enable support for the channel integrity check
cdpn default	<CDPN>	Up to 30 digits or	cgpn by default, in case of calls

		'none'	implemented through the interface with trunk registration.
cdpn plus sign	<YES/NO>	no/yes	"+" (plus) symbol transmission in international calls. Enables by default.
cgpn replace	<YES_NO>	no/yes	Take CgPN from the 'Username/Number' parameter; when disabled, use CgPN number received in the incoming call
clearchan override	<on/off>	<on/off>	Set ‘clear channel override’ option – announce CLEARMOD codec to second leg when first leg operates in ‘clear channel’ operation mode
clearchan transit	<on/off>	<on/off>	Set ‘clear channel transit’ option– transmitted RTP should be exactly the same with the RTP transmitted to the first leg (including packetization time).
codec disable	<CODEC IDX>	0-5	Enable defined codec. Codecs are numbered by priority – from 0 (the highest) to 5 (the 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. The static value sets the default value according to defined codec.
codec set	<CODEC_IDX> <CODEC>	0-5 G.711-U/ G.711-A/ G.729/ G.723.1_5.3/ G.723.1_6.3	Set codec which is used.
command line	<command>	Allowed symbols: [0-9a-zA-Z-_.!~*'();:=+$,%#] always inside []. For clearing use 'none'	SIP advanced settings
config			Return to Configuration menu.
DSCP RTP	<DSCP_RTP>	0-255	Define DSCP identifier for RTP traffic
DSCP SIG	<DSCP_SIG>	0-255	Define DSCP identifier for SIG traffic
DTMF mime type	<MIME_TYPE>	application/dtmf or application/ dtmf-relay	Specify payload 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).
DTMF mode	<DTMF_m>	inband/ RFC2833/ SIP-INFO/ SIP-NOTIFY	DTMF mode for the current interface
DTMF payload	<DTMF_p>	96-127	Define payload type for RFC2833
DTMF payload-equal	<DTMF_PT_EQ>	(off/on)	Enable/disable option 'Same RFC2833 PT'
duplicate enable	<YES_NO>	no/yes	Enable incoming INVITE redundancy mode.
duplicate primary host	<REM_IPADDR> <REM_PORT>	IP address in AAA.BBB.CCC.DDD format 0-65535	Define address and port of primary duplicate server.
duplicate secondary host	<REM_IPADDR>	IP address in AAA.BBB.CCC.DDD	Define address and port of secondary duplicate server

	<REM_PORT>	format 0-65535	
early media header	<early media header>	(off/on)	Enable P-Early-Media support (RFC5009)
ecan	<CANCELLATION>	voice/ nlp-off-voice/ modem/ 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 processor (NLP) is disabled. When signal levels on transmission and reception significantly differ, weak signal may become suppressed by the NLP. To avoid this, use this echo canceller operation mode. *Modem* — echo cancellers are enabled in the modem operation mode (direct component filtering is disabled, NLP control is disabled, CNG is disabled). *Off* — disable echo cancellation.
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
fax detection	<DETECTION>	no/callee/caller/ callee_and_caller	Set the fax detection mode: *no* — disable fax detection *callee* — for the receiving party only *caller* — for the transmitting party only *callee_and_caller* — for both receiving and transmitting parties
fax mode	<MODE>	T38_only/G.711_only/ T38_and_G.711	Select fax transmission mode
fill empty display-name	FILL_DNAME	on/off	Fill display-name when the call without display-name is received
gain rx	<GAIN>	-140 – 60	Set the volume of voice reception (gain of the signal received from the communicating gateway and output to the speaker of the phone unit connected to SMG gateway).
gain tx	<GAIN>	-140 – 60	Volume of voice transmission (gain of the signal received from the microphone of the phone unit connected to SMG gateway and transmitted to the communicating gateway).
history			View history of entered commands.
hold mode		flash/ flash/star flash/hash flash/star/hash	Call hold by pressing: — flash — flash or * — flash or # — flash, * or #
hostname clear			Remove host name of the communicating gateway
hostname set	<HOSTNAME>	String, 63 characters max.	Define host name of the communicating gateway

ignore RURI/To diff	<IGNORE_RURI_TO_DIFF>	off/on	If option is enabled and there is a difference between SIP RURI and To fields, 'redirecting' and 'Original called' numbers will not be transmitted to SS7.
inband_signal_ with_183_and_sdp	on/off		Issue reply 183/SDP to SIP answer for voice channel forwarding after reception of CALL PROCEEDING or PROGRESS messages from ISDN PRI containing progress indicator=8 (In-band signal).
jitter adaptation period	<JT_AP>	1000-65535	Define the time of jitter-buffer adaptation to the lower limit, in milliseconds
jitter adjust mode	<JT_AM>	non-immediate/ immediately	Specify the jitter buffer adjustment mode: non-immediate — gradual immediately — instant
jitter deletion mode	<JT_DM>	soft/hard	Specify buffer adjustment mode. Defines the method of packet deletion during buffer adjustment to lower limit. *soft* — device uses intelligent selection pattern for deletion of packets that exceed the threshold. *hard* — packets which delay exceeds the threshold will be deleted immediately.
jitter deletion threshold	<JT_DT>	0-500	Set the threshold for immediate deletion of a packet, in milliseconds When buffer size grows and packet delay exceeds this threshold, packets will be deleted immediately
jitter init	<JT_INIT>	0-200	Specify an initial value of adaptive jitter buffer, in milliseconds
jitter max	<JT_MAX>	0-200	Define the upper limit (maximum size) of adaptive jitter buffer, in milliseconds
jitter min	JT_MIN>	0-200	Define the size of fixed jitter buffer or lower limit (minimum size) of adaptive jitter buffer
jitter mode	<JT_MODE>	adaptive/non-adaptive	Jitter buffer operation mode: *Adaptive* — adaptive *non-adaptive* — fixed
jitter vbd	<JT_VBD>	0-200	Define fixed buffer size for data transmission in VBD mode
keep-alive enable			Enable direction availability control (NAT keep-alive) (for SIP profile only)
keep-alive disable			Disable direction availability control (NAT keep-alive) (for SIP profile only)
keep-alive mode	<KEEP_ALIVE_MODE>	SIP-OPTIONS/ SIP-NOTIFY/UDP-CRLF	Opposite party availability control mode. SIP-OPTIONS — direction availability control that utilizes OPTIONS requests. SIP-NOTIFY — direction availability

			control that utilizes NOTIFY requests. UDP-CRLF — direction availability control that utilizes empty UDP packet transmission.
keep-alive period	<KEEP_ALIVE_PERIOD>	30-3600	Request transmission period
local ringback	<on/off>	on/off	Enable 'Local ringback for early-media' option
login	<LOGIN>	String, 15 characters max.	Specify the name used for authentication
max_active	<MAX_ACTIVE>	0-65535	Define the maximum number of active connection for an interface
mode	<mode>	profile/ SIP/ SIP-T/ SIP-I/ SIP-Q	Define interface operation mode (SIP profile is assigned to SIP subscribers)
name	<s_name>	you may use letters, numbers, '_' character 31 characters max.	Define the interface name
nat	<NAT>	enable/disable	Enable/disable NAT
net-interface rtp	<IFACE_NAME>	String, 255 characters max.	Specify RTP network interface
net-interface sig	<IFACE_NAME>	String, 255 characters max.	Specify SIP network interface
numbering plan	<NUMPLAN>	0-15/0-255	Select dial plan
options	<OPTIONS>	enable/disable	Enable direction availability control function that utilizes OPTIONS requests; when the direction is not available, the call will be performed through the redundant trunk group. Also, this function analyzes received OPTIONS message responses, that allows to avoid usage of 100rel, replaces and timer features configured in this direction if the opposite party supports them.
options period	<OPTIONS_PERIOD>	30-3600	Define the time in seconds that should pass for the call to be performed through the redundant trunk group when the direction is not available.
password	<PASSWD>	String, 15 characters max.	Specify the password used for authentication
port	<PORT>	1-65535	Define UDP port of the communicating gateway used for SIP signalling reception
quit			Terminate this CLI session
radius profile	<RADIUS_PROFILE>	number [0-31] or 'no'	Define RADIUS profile for the SIP profile interface no — do not use the profile for an interface.
Re-INVITE a=sendonly		on/off	Enable Re-INVITE processing with a=sendonly
redirection 302	<REDIRECTION>	on/off	Enable/disable redirection (302) utilization
redirection server	<REDIRECT_SERV>	on/off	Redirect/do not redirect the call sent using the public address to the subscriber's private address without the dial plan routing. The routing will be performed directly to the address contained in the reply 302 'contact' header received from the redirection

			server. You should configure redirection 302 first (`redirection 302` command)
refer	<REFER>	enable/disable	Enable/disable call transfer with REFER
register delay	<REGEXP>	500-5000	Minimum 'Register' message transmission interval designed for protection from high traffic caused by simultaneous registration of large number of subscribers
register expires	<REGEXP>	90-64800	Define the registration renewal time period
regmode	<REGMODE>	none/ trunk-mode/ user-mode	Define the type of registration on the upstream server.
reliable_1xx_ response	<ON_OFF>	Off/ Support/ support-plus/ require/ require-plus	When *support* option is enabled, INVITE request and 1xx class provisional responses will contain the tag support : 100rel that requires assured confirmation of provisional responses. When *require* option is enabled, INVITE request and 1xx class provisional responses will contain the tag require: 100rel that requires assured confirmation of provisional responses. *Off* — 100rel tag transmission is disabled.
routing_profile	<prof>	0-127	Select scheduled routing profile
RTCP control	<RTCP_c>	2-255	Define the quantity of time periods (RTCP period) during which the opposite party will wait for RTCP protocol packets.
RTCP period	<RTCP_p>	5-255	Define the time period in seconds after which the device send control packets via RTCP protocol.
RTP loss silence	<RTP_TIMEOUT_SILENCE>	1-30	Define the RTP packet timeout for the silence suppression option utilization. Coefficient is a multiplier that applies to the 'RTP-loss timeout' value.
RTP loss timeout	<RTP_TIMEOUT>	10-300/ off	Define the RTP packet timeout
sdp_in_18x	<ON_OFF>	on/off	Always send SDP in provisional replies
sipdomain	<SIPDOMAIN>	IP address in AAA.BBB.CCC.DDD format	Define the registration domain address
show config			Show the interface information
sipcause profile	<SIPCAUSE>	[0-63]/ none	Select Q.850 and sip-reply compliance profile
sms port	<PORT>	0-65535	Port for SMS receiving via SMPP and redirecting them to duplication server
src verify	<ON_OFF>	on/off	Control the media traffic reception from IP address and UDP port specified in SDP(on) communication session description; otherwise the traffic from any IP address and UDP port will be accepted.
STUN ip	<IPADDR>	IP address in AAA.BBB.CCC.DDD format	Define STUN server IP address
STUN period	<PERIOD>	10-1800/0	Define the time interval between requests

STUN port	<PORT>	1-65535	Define STUN server port for request transmission (default value is 3478)
STUN use	<YES_NO>	yes/no	Enable/disable STUN
subnet mask clear			Delete subnet mask for incoming calls
subnet mask set	<SUBNET>	A string of up to 63 characters in the form of subnet mask: AAA.BBB.CCC.DDD	Set subnet mask for incoming calls
t38 bitrate	<BITRATE>	nolimit/2400/4800/ 7200/9600/12000/ 14400	Specify the maximum transfer rate of fax transmitted via T.38 protocol
t38 disable			Disable fax reception via T.38 protocol
t38 enable			Enable fax reception via T.38 protocol
t38 fillbitremoval	<T38_FBR>	on/off	Enable/disable padding bit removals and inserts for data that does not relate to ECM
t38 pte	<T38_PTE>	10/20/30/40	Define T.38 packet generation frequency in milliseconds
t38 ratemgmt	<T38_RATE_MGMT>	localTCF/ transferredTCF	Set the data transfer speed management method local TCF — method requires that the TCF tuning signal was generated locally by the recipient gateway. transferred TCF — method requires that the TCF tuning signal was sent from the sender device to the recipient device.
t38 redundancy	<T38_REDUNDANCY>	off/1/2/3	Enable redundant frames utilization for error control, off — disable
timer enable	<YES_NO>	no/yes	Enable/disable RFC4028 SIP session timers
timer refresher	<REFRESHER>	uac/uas	Define the party that will perform session renewal
timer session Min-SE	<MIN_SE>	90-32000	Define the minimum session state control period, in seconds. This period should not exceed session forced termination timeout '*timer sessions expires*'.
timer session expires	<EXPIRES>	90-64800	Define the time in seconds that should pass before the forced session termination, if the session is not renewed in time
transit sip header	YES_NO	no/yes	Allow transit of SIP headers from this call leg to another
trunk	<TRUNK>	0-31	Define the trunk group number for an interface
trusted network	<YES_NO>	yes/no	Select 'trusted network' option
username	<USERNAME>	String, 15 characters max.	Specify username for authentication
VAD_CNG	<ON_OFF >	on/off	Enable/disable voice activity detector / Comfort noise generator for an interface
vbd codec	<CODEC>	G.711-U, G.711-A	Codec used for VBD data transmission
vbd enable			Enable V.152
vbd disable			Disable V.152
vbd payload type	<VBD_p>	Static,96-127	Payload type used for VBD codec
flash processing		on/off	Process flash signal

3.3.33 Interface subscriber registration parameter configuration mode

To enter this mode, execute 'sip registration' command in the configuration mode.

```
SMG-[CONFIG]> sip registration
Entering sip-registration mode.
SMG-[CONFIG]-SIP-REGISTRATION>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
add one			Add a new account
count			Show the number of created accounts
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
config			Return to Configuration menu.
quit			Terminate this CLI session
remove	<INDEX>	0-3000	Remove the specified account
set authname	<INDEX> <NAME>	0-3000 String, 63 characters max.	Specify the name used for authentication
set authpass	<INDEX> <NAME>	0-3000 String, 63 characters max.	Specify the password used for authentication
set sipdomain	<INDEX> <NAME>	0-3000 String, 63 characters max.	Define the registration domain
set username	<INDEX> <NAME>	0-3000 String, 63 characters max.	Define the user name for registration
show all			Show the information on all created accounts
show one	<ONE_INDEX>	0-3000	Show the information on account with the specified number

3.3.34 SIP subscribers parameter configuration mode[1]

To enter this mode[1], execute 'sip users' command in the configuration mode.

```
SMG-[CONFIG]> sip users
Entering SIP-Users mode.
SMG-[CONFIG]-SIP-USERS>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
add		group/user	Add a new user/dynamic subscribers group
config			Return to Configuration menu.
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
quit			Terminate this CLI session

[1] This menu is available for the devices with SIP registar license. Read more detailed information on licenses in the section 3.1.23 Licenses.

remove	<INDEX>	0-1999/0-2999	Remove the current user
savedb			Save the information on registered subscribers in the gateway non-volatile memory. It allows you to keep the registered subscribers' database in case of device reboot due to power loss or failure. In case of reboot from the WEB or CLI, the gateway will store the current database into the non-volatile memory regardless of this setting.
service user	<INDEX>	0-1999/0-2999	Switch to the VAS configuration mode for the specified subscriber.
service group	<INDEX>	0-63	Switch to the VAS configuration mode for the specified 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 while registration, *register_and_invite* – ask while registration and egress calls ringing
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 the category for the specified 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/ Denied_8/Exclude	Define the service mode for the specified subscriber
set user blf groupID	<INDEX> <GROUP_ID>	0-1999/0-2999 0-15	Set a monitoring group (BLF subscription group)
set user blf subscribers	<INDEX> <BLF_SUBS>	0-1999/0-2999 0-200	Set the maximum number of BLF subscribers for the party (subscriber)
set user blf usage	<INDEX> <BLF>	0-1999/0-2999 off/on	Permit BLF subscribtion to a subscriber.
set user category	<INDEX> <CATEGORY>	0-1999/0-2999 0-9	Set a CallerID category for the specified subscriber *INDEX* – SIP subscriber index; *CATEGORY* – CallerID category
set user cliro	<INDEX> <ON_OFF>	0-1999/0-2999 off/on	Enable CLIRO service (define a hidden number)

set user display name rule	<INDEX> <USE_DISPLAY_NAME>	0-1999/0-2999 received_only/ received_prefer/ configured_only	Displayed name utilization mode: *received_only* - always use only received name; *received_prefer* - if there is no a received displayed name, use a configured displayed name; *configured_only* - always use a configured displayed name.
set user display name value	<INDEX> <DISPLAY_NAME>	0-1999/0-2999 string, max 40 characters or none	Subscriber displayed name. none - clear the displayed name.
set user domain	<INDEX> <DOMAIN>	0-1999/0-2999 string of 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 egress calls, in which the subscriber participates, for lines separate operation mode. The range of available values [1;255] or 0 – no limit.
set user ingress lines	<INDEX> <COUNT>	0-1999/0-2999 1-255 or 0	Set the number of simultaneous ingress calls, in which the subscriber participates, for lines separate operation mode. The range of available values [1;255] or 0 – no limit.
set user intercom header	<HEADER> <INDEX>	AIAA/AII/AIIAA/ AIII/AIIRA/AIRA/ AMO/CIAA/CIESAA/ CISSAA 0-1999/0-2999	Set a 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-sided; *sendrecv* - double-sided; *ordinary* - a common call (without intercom headers transmission)); *reject* - do not use intercom.
set user intercom priority	<INDEX> <PRIORITY>	0-1999/0-2999 1-5	Set the priority for intercom operation
set user intercom timer	<INDEX> <TIMER>	0-1999/0-2999 0-255	A pause before answer. It is used while SIP headers transmission with answer-auto parameter.
set user ipaddr	<INDEX> <IPADDR>	0-1999/0-2999 IP address in AAA.BBB.CCC.DDD format	Set an IP address for the specified subscriber.
set user lines	<INDEX> <COUNT>	0-1999/0-2999 1-255 or 0	Set the number of simultaneous calls, in which the subscriber

			participates, for lines common operation mode. The range of available values [1;255] or 0 – no limit.
set user lines-mode	<INDEX> <LINES_MODE>	0-1999/0-2999 common/separate	The mode of simultaneous calls limiting. *common* – common limiting of ingress and egress calls; *separate* – separate limiting of ingress and egress calls.
set login	<INDEX> <LOGIN> <PASSWORD>	0-1999/0-2999 string of up to 63 characters string of up to 63 characters	Set user name and password 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	Do not consider source-port after registration
set user number	<INDEX> <NUMBER>	0-1999/0-2999 subscriber number	Set SIP subscriber number
set user numberAON	<INDEX> <NUMBER>	0-1999/0-2999 subscriber number	Set CallerID number for the specified subscriber
set user numberAON-for-redirection	<INDEX> <NUMBER>	0-1999/0-2999 subscriber number	Use CallerID while redirection
set user numberList	<INDEX> <NUM_IDX> <NUMBER>	0-1999/0-2999 0-15/0-255 [number]/none	Set additional subscriber number in a specified dial plan. none - clear the number.
set user numplan	<INDEX> <PLAN_IDX>	0-1999/0-2999 0-15/0-255	Set dial plan for the 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	Enable hold service when re-invite with a=sendonly feature is received
set user redirection	<INDEX> <REDIRECTION>	0-63 off/on	Permit/deny redirection (302) from a subscriber
set group access category	<INDEX> <CAT_IDX>	0-63 0-31	Set access category for subscribers group
set group blf groupID	<INDEX> <GROUP_ID>	0-63 0-15	Set BLF monitoring group (BLF susbcribers group)
set group blf subscribers	<INDEX> <BLF_SUBS>	0-63 0-200	Set the maximum number of blf subscribers for the party (subscriber)
set group blf usage	<INDEX> <ON_OFF>	0-63 off/on	Enable subscription on events

set group category	<INDEX> <CATEGORY>	0-63 0-9	Set Caller ID category for the specified group *INDEX* – SIP subscriber index; *CATEGORY* – CallerID category
set group clear service timeout	<INDEX> <CLEAR_TIMEOUT>	0-63 1-255/off	The VAS reset timer for a subscriber. When the time (days) expires, all the VAS attached to the account will be reset.
set group cliro	<INDEX> <ON_OFF>	0-63 off/on	Enable CLIRO service (hidden number identification).
set group domain	<INDEX> <DOMAIN>	0-63 string of 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 quantity of simultaneous egress calls, in which a subscriber of the group participates, for separate line mode. The range of available values [1;255] or 0 – no limit.
set group ingress lines	<INDEX> <COUNT>	0-63 1-255 or 0	Set the quantity of simultaneous ingress calls, in which a subscriber of the group participates, for separate line mode. The range of available values [1;255] or 0 – no limit.
set group intercom header	<HEADER> <INDEX>	AIAA/AII/AIIAA/ AIII/AIIRA/AIRA/ AMO/CIAA/CIESAA/ CISSAA 0-63	Set a 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/ ordinary/ reject	Intercom operation mode: *sendonly* - one-sided; *sendrecv* - double-sided; *ordinary* - an ordinary call (without intercom headers transmission); *reject* - do not use intercom.
set group intercom priority	<INDEX> <PRIORITY>	0-63 1-5	Set the priority for intercom operation
set group intercom timer	<INDEX> <TIMER>	0-63 0-255	A pause before answer. It is used while SIP headers transmission with answer-auto parameter.
set group lines	<INDEX> <COUNT>	0-63 1-255 or 0	Set the number of simultaneous calls in which a subscriber of the group participates for lines common operation mode. The range of available values [1;255] or 0 – no limit
set group lines-mode	<INDEX> <LINES_MODE>	0-63 common/separate	The mode of simultaneous calls limiting. *common* – common limiting of ingress and egress calls; *separate* – separate limiting of ingress and egress calls.

set group max	<INDEX> <MAX_REG>	0-63 0-1999/0-2999	Set the quantity of subscribers in the group
set group name	<INDEX> <NAME>	0-63 string,max 31 characters	Set the group name
set group numplan	<INDEX> <PLAN_IDX>	0-63 0-15/0-255	Set the group dial plan
set group no-source-port-control	<INDEX> <ON_OFF>	0-63 off/on	Do not consider source-port after registration
set group pbx_profile	<INDEX> <PROFILE>	0-63 0-31	Set a PBX profile for the group
set group profile	<INDEX> <PROFILE>	0-63 0-31	Set a SIP profile for the group
set group Re-INVITE a=sendonly	<INDEX> <HOLD>	0-63 off/on	Enable hold service when re-invite with a=sendonly feature is received
set group redirection	<INDEX> <REDIRECTION>	0-63 off/on	Permit/deny redirection (302) from a group
set group refer	<INDEX> <REFER>	0-63 off/on	Enable call transfer with the help of REFER message
show count			Show the quantity of SIP subscribers
show list			Show the list of SIP subscribers
show user	<INDEX>	0-1999/0-2999	Display information on a SIP subscriber

3.3.34.1 Subscriber VAS configuration mode

To enter this mode, execute 'service <USER_INDEX>' command in the RADIUS configuration mode, where USER_INDEX is a SIP subscriber index.

```
SMG-[CONFIG]-SIP-USERS> service 0
Entering User-Service mode for user 0
SMG-[CONFIG]-[SIP-USERS][0]-SERVICE>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
attach service block			Enable VAS for subscriber
detach service block			Disable VAS for subscriber
exit			Exit from this configuration submenu to the upper level.
quit			Terminate this CLI session
set call-pickup enable	<ON_OFF>	off/on	Enable "call pickup" service
set cfb enable	<ON_OFF>	off/on	Enable "call forwarding on busy" service
set cfb number	<ON_OFF>	number of up to 30 characters or none	Set a number for " call forwarding on busy", none – disable the service.
set sfnr enable	<ON_OFF>	off/on	Enable "call forwarding on no-reply" service

set sfnr number	<ON_OFF>	number of up to 30 characters or none	Set a number for " call forwarding on no-reply", none – disable the service
set cfos enable	<ON_OFF>	off/on	Enable "call forwarding on out of service" service
set cfos number	<ON_OFF>	number of up to 30 characters or none	Set a number for "call forwarding on out-of-service", none – disable the service
set cfu enable	<ON_OFF>	off/on	Enable "call forwarding unconditional" service
set cfu number	<ON_OFF>	number of up to 30 characters or none	Set a number for " call forwarding unconditional", none – disable the service
set clear-all enable	<ON_OFF>	off/on	Enable "reset all services"
set conf-3way enable	<ON_OFF>	off/on	Enable "3-way conference" service. The "call hold" service must be activated.
set conference enable	<ON_OFF>	off/on	Enable "conference add-on" service
set ct enable	<ON_OFF>	off/on	Enable "call transfer" service. The "call hold" service must be activated.
set hold enable	<ON_OFF>	off/on	Enable "call hold" service
set intercom enable	<ON_OFF>	off/on	Enable "intercom" service
set password change enable	<ON_OFF>	off/on	Enable "password change" service
set password restrict out access active	<ON_OFF>	off/on	Activate a password for "password activation" service. The "on" value makes the password active and call restrictions get invalid.
set password restrict out access enable	<ON_OFF>	off/on	Enable "password activation" service. The "outgoing calls restriction" service must be activated.
set password restrict out once enable	<ON_OFF>	off/on	Enable "password-based outgoing calls restriction" service. The "outgoing calls restriction" service must be activated.
set password value	<VALUE>	string of 4 characters	Set a password for "outgoing calls restriction" service
set restrict out enable	<ON_OFF>	off/on	Enable "outgoing calls restriction" service
set restrict out value	<ACCESS_MODE>	On/ Denied_6/ Denied_7/ Denied_8	Outgoing calls restriction mode: On - all calls are permitted; Denied_6 - only calls to emergency services are permitted; Denied_7 - only local, departmental and emergency calls are permitted; Denied_8 - only local, departmental, zone and emergency calls are permitted.
show			Show the current VAS settings
show count			Show the quantity of free VAS blocks

3.3.35 Subscribers group's VAS configuration mode

To enter this mode, perform the command **service <USER_INDEX>** (where USER_INDEX is a SIP susbcriber index) in the SIP subscriber configuration mode.

```
    SMG2016-[CONFIG]-SIP-USERS> service group 0
    Entering UserGroup-Service mode for user-group 0
    SMG2016-[CONFIG]-[SIP-USERS][0]-GROUP-SERVICE>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands
attach service blocks manual			The mode of VAS activation for the subscribers is manual.
attach service blocks radius			The mode of VAS activation for the subscribers is through the RADIUS.
detach service block			Disable VAS for the group
exit			Exit this configuration submenu to the menu on the upper level
quit			Quit the current CLI session
set call-pickup enable	<ON_OFF>	off/on	Enable "call pick-up" service
set cfb enable	<ON_OFF>	off/on	Enable "call forwarding on busy" service.
set cfb number	<ON_OFF>	a number of 30 characters or none	Set the number for call forwarding on busy. None – disable call forwarding.
set sfnr enable	<ON_OFF>	off/on	Enable "call forwarding on no-reply" service
set sfnr number	<ON_OFF>	a number of 30 characters or none	Set the number for "call forwarding on no-reply" service. None – disable call forwarding.
set cfos enable	<ON_OFF>	off/on	Enable "call forwarding on out-of-service" service
set cfos number	<ON_OFF>	a number of 30 characters or none	Set the number for "call forwarding on out-of-service" service. None – disable call forwarding.
set cfu enable	<ON_OFF>	off/on	Enable "call forwarding unconditional" service
set cfu number	<ON_OFF>	a number of 30 characters or none	Set the number for "call forwarding unconditional" service. None – disable call forwarding.
set clear-all enable	<ON_OFF>	off/on	Enable "reset all services"
set conf-3way enable	<ON_OFF>	off/on	Enable "3-way conference" service. The "call hold" service must be activated.
set conference enable	<ON_OFF>	off/on	Enable "conference add-on" service.
set ct enable	<ON_OFF>	off/on	Enable "call transfer" service. The "call hold" service must be activated.
set hold enable	<ON_OFF>	off/on	Enable "call hold" service.
set intercom enable	<ON_OFF>	off/on	Enable "intercom" service.
set password change enable	<ON_OFF>	off/on	Enable "password change" service
set password restrict out access active	<ON_OFF>	off/on	Activate a password for "password activation" service. The "on" value makes the password active and call restrictions get invalid.
set password restrict out access enable	<ON_OFF>	off/on	Enable "password activation" service. The "outgoing calls restriction" service must be activated.
set password restrict out once enable	<ON_OFF>	off/on	Enable "password-based outgoing calls restriction" service. The "outgoing calls restriction" service must be activated.
set password value	<VALUE>	a string of 4 characters	Set a password for "outgoing calls restriction" service
set restrict out enable	<ON_OFF>	off/on	Enable "outgoing calls restriction" service
set restrict out value	<ACCESS_MODE>	On/ Denied_6/ Denied_7/ Denied_8	Outgoing calls restriction mode: On - all calls are permitted; Denied_6 - only calls to emergency services are permitted; Denied_7 - only local, departmental and emergency calls are permitted; Denied_8 - only local, departmental, zone and emergency calls are permitted.

show			Show the current VAS settings
show count			Show the quantity of free VAS blocks

3.3.36 PRI-subscribers parameters configuration mode

To enter this mode, implement the **`pri-users`** command in configuration mode.

```
    SMG2016-[CONFIG]> pri-users
    Entering SIP-Users mode.
    SMG2016-[CONFIG]-[PRI-USERS]>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands
add user	<NUMBER> <STREAM>	subscriber number a number of E1 stream 0-15	Create a new susbcriber
remove by id	<USER_ID>	subscriber ID	Remove a subscriber using their ID
remove by index	<INDEX>	Subscriber index	Remove a subscriber using their index
service	<USER_INDEX>	Subscriber index	Move to subscriber VAS management menu
set by id access category	<USER_ID> <CAT_IDX>	Subscriber ID 0-127	Assign an access category using 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	Assign a service mode using ID
set by id name	<USER_ID> <USER_NAME>	Subscriber ID a string of 63 characters	Set a name for a subscriber using ID
set by id number	<USER_ID> <NUMBER>	Subscriber ID subscriber phone number	Set a number for a subscriber using ID
set by id pbx_profile	<USER_ID> <PROFILE>	Subscriber ID 0-15	Specify PBX profile using subscriber ID
set by id stream	<USER_ID> <STREAM>	Subscriber ID 0-15	Set E1 stream, where subscriber is located, using subscriber ID
set by index access category	<INDEX> <CAT_IDX>	Subscriber index 0-127	Assign an access category using 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 /Denied_7/Denied_8 /Exclude	Assign an service mode using subscriber index
set by index name	<INDEX> <USER_NAME>	Subscriber index a string of 63 characters	Set a name for a subscriber using subscriber index
set by index number	<INDEX>	Subscriber index	Set a number using subscriber index

	<NUMBER>	subscriber phone number	
set by index pbx_profile	<INDEX> <PROFILE>	Subscriber index 0-15	Specify PBX profile using subscriber index
set by index stream	<INDEX> <STREAM>	Subscriber index 0-15	Set E1 stream, where subscriber is located, using subscriber index
show all			Show settings for all PRI subscribers
show by id	<USER_ID>	Subscriber ID	Show subscriber setting using subscriber ID
show by index	<INDEX>	Subscriber index	Show subscriber setting using subscriber index
show count			Show the total quantity of PRI subscribers
show list users			Show the list of PRI subscribers

3.3.37 VAS configuration mode for PRI subscribers

To enter this mode, implement the command **`service <USER_INDEX>`** (where USER_INDEX is a PRI susbcriber index) in PRI subscriber configuration mode.

```
SMG2016-[CONFIG]-[PRI-USERS]> service 0
Entering User-Service mode for user 0
SMG2016-[CONFIG]-[PRI-USERS][0]-SERVICE>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands
attach service block			Enable VAS for a subscriber
detach service block			Disable VAS for a subscriber
set cfb enable	<ON_OFF>	off/on	Enable "call forwarding on busy" service
set cfb number	<ON_OFF>	a number of 30 characters or none	Set a number for "call forwarding on busy" service. None – disable call forwarding.
set sfnr enable	<ON_OFF>	off/on	Enable "call forwarding on no-reply" service
set sfnr number	<ON_OFF>	a number of 30 characters or none	Set a number for "call forwarding on no-reply" service. None – disable call forwarding.
set cfos enable	<ON_OFF>	off/on	Enable "call forwarding on out-of-service" service
set cfos number	<ON_OFF>	a number of 30 characters or none	Set a number for "call forwarding on out-of-service" service. None – disable call forwarding.
set cfu enable	<ON_OFF>	off/on	Enable "call forwarding unconditional" service
set cfu number	<ON_OFF>	a number of 30 characters or none	Set a number for "call forwarding unconditional" service. None – disable call forwarding.
show			Show the current VAS settings
show count			Show the quantity of free VAS blocks

3.3.38 SS7 category modification configuration mode

To enter this mode, execute 'ss7cat' command in the configuration mode.

SMG-[CONFIG]> ss7cat

Entering SS7-categories mode.
SMG-[CONFIG]-SS7-CAT>

Command	Parameter	Value	Action
?			Show the list of available commands.
config			Return to Configuration menu.
exit			Exit from this configuration submenu to the upper level.
quit			Terminate this CLI session
set	<CAT_IDX> <PBX_CAT> <SS7_CAT>	0-15 0-255 0-255	Set data category: CAT_IDX — category index PBX_CAT — Caller ID category SS7_CAT — SS7 category
show			Show information on SS7 data category.

3.3.39 *Switch parameter configuration mode*[1]

To enter this mode, execute switch command in the configuration mode.

SMG-[CONFIG]> switch
Entering switch control mode.
SMG-[CONFIG]-[SWITCH]>

Command	Parameter	Value	Action
?			Show the list of available commands.
802.1q			Enter the 802.1q configuration mode
apply mirroring settings		no/yes	Apply mirroring settings.
apply port settings		no/yes	Apply port settings.
confirm mirroring settings			Confirm mirroring settings. If you fail to confirm settings in 1 minute interval, the previous values will be restored.
confirm port settings			Confirm port settings. If you fail to confirm settings in 1 minute interval, the previous values will be restored.
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
LACP[2]			Enter LACP parameter configuration mode
QoS_control			Enter the QoS parameter configuration mode
quit			Terminate this CLI session
save mirroring			Save mirroring settings without applying
save vlan			Save VLAN settings without applying
set mirroring	<PORT> <NAME>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) src_in/ src_out/	Configure port mirroring: PORT — port type. NAME — port designation. - *src_in* — incoming packet source port — copy frames received from this port

[1] For SMG-1016M only

[2] Not supported in the current firmware version.

	<ACT>	dst_in/ dst_out on/off	(source port). - *src_out* — outgoing packet source ports — copy frames sent by this port (source port). - *dst_in* — incoming packet destination port — destination port for copied frames received by selected source ports. - *dst_out* — outgoing packet destination port — destination port for copied frames sent by selected source ports.
set port backup	<ON_OFF> <B_MASTER> B_SLAVE	on/off GE_PORT0/GE_PORT1/ GE_PORT2/SFP0/SFP1 GE_PORT0/GE_PORT1/ GE_PORT2/SFP0/SFP1	Enable Dual Homing redundancy B_MASTER — master port B_SLAVE — slave port PREEMPTION — enable/disable return to master port when it becomes available
set port default vlan id	<PORT> <VLANID>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) 0-4095	Define VLAN ID for this port
set port egress	<PORT> <EGRESS>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) unmodified/ untagged/ tagged/ double-tag	Configure packet transmission mode for the current port. EGRESS — packet transmission mode: - *unmodified* — packets will be sent by the port without any changes (i.e. as they came to another switch port). - *untagged* — packets will always be sent without VLAN tag by this port. - *tagged* — packets will always be sent with VLAN tag by this port. - *double tag* — each packet will be sent with two VLAN tags — if received packet was tagged and came with one VLAN tag — if the received packet was untagged.
set port ieee mode	<PORT> <IEEE>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) fallback/ check/ secure	Define the management mode for the tagged packets received at the current port IEEE — packet management mode: - *Fallback* — if a packet with VLAN tag is received through this port, and there are records in'802.1q' routing table for this packet, then it falls within a scope of routing rules, specified in the record of this table; otherwise, routing rules specified in 'egress' and 'output' will be applied to it. - *Check* — if a packet with VID is

			received through the port, and there is a record in '802.1q' routing table for this packet, then it falls within a scope of routing rules, specified in the current record of this table, even if this port does not belong to the group of this VID. Routing rules specified in 'egress' and 'output' will not apply to this port. - *Secure* – if a packet with VID is received through the port, and there is a record in '802.1q' routing table for this packet, then it falls within a scope of routing rules, specified in the current record of this table; otherwise, it is rejected. Routing rules specified in 'egress' and 'output' will not apply to this port.
set port LACP_trunk[1]	<PORT> <LACP>	CPU/ GE_PORT0/ GE_PORT1/ GE_PORT2/ SFP0/ SFP1 0-4	Assign LACP trunk for the port specified.
set port MAC GE_PORT0	<MACADDR>	MAC address in XX:XX:XX:XX:XX:XX format	Specify MAC address for port.
set port output	<PORT> <P_DEST> <ENABLE>	GE_PORT0/ GE_PORT1/ GE_PORT2/ CPU/ SFP0/ SFP1 GE_PORT0/ GE_PORT1/ GE_PORT2/ CPU/ SFP0/ SFP1 on/off	Specify allowed ports for packet transfer: PORT — port being configured P_DEST — allowed transmission ports
set port speed	<SPEED> <PORT>	1000M 100M (full-duplex/ half-duplex) 10M(full-duplex/ half-duplex) auto GE_PORT0/GE_PORT1/ GE_PORT2	Specify port operation mode
set port vlan enabling	<PORT> <ENABLE>	CPU/ GE_PORT0/ GE_PORT1/ GE_PORT2/ SFP0/ SFP1 on/off	Enable/disable VLAN for this port
set port vlan override	<PORT>	CPU/ GE_PORT0/ GE_PORT1/ GE_PORT2/ SFP0/	Set the mode for VLAN ID redefinition to a standard one for the current port

[1] Not supported in the current firmware version.

	<OVER>	SFP1 on/off	
show mirror settings			Show port mirroring parameters
show port settings			Show port configuration parameters

3.3.39.1 802.1q parameter configuration mode

To enter this mode, execute '802.1q' command in the switch configuration mode.

```
SMG-[CONFIG]-[SWITCH]> 802.1q
Entering 802.1q_control mode.
SMG-[CONFIG]-[SWITCH]-[802.1q]>
```

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands.
add VTU element	<VID> <PRIO> <OVER> <GE_PORT0> <GE_PORT1> <GE_PORT2> <CPU> <SFP0> <SFP1>	0-4095 0-7 on/off unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member	Add a new element to VTU table: VID — VLAN identifier. PRIO — 802.1p priority assigned to packets in this VLAN, when *OVER* parameter is active (on). OVER — override 802.1p priority for this VLAN (yes/no). PORT — assign actions performed by this port during transfer of a packet with specified VID. - *Unmodified* — packets will be sent by the port without any changes. - *Untagged* — packets will always be sent without VLAN tag by this port. - *Tagged* — packets will always be sent with VLAN tag by this port. - *Tagged* — packets with specified VID will not be sent by this port, i.e. the port is not the member of VLAN.
apply	<YES_NO>	yes/no	Apply VTU settings
confirm			Confirm VTU settings If you fail to confirm settings in 1 minute interval, the previous values will be restored.
exit			Return from this configuration submenu to the upper level.
QoS_control			Enter the QoS configuration mode
quit			Terminate this CLI session
remove VTU element	<NUMBER>	0-4095	Delete the current VTU table element

save			Save VTU settings without applying
set VTU override	<NUMBER> <OVER>	0-4095 on/off	Override/do not override 802.1p priority for this VLAN (yes/no)
set VTU priority	<NUMBER> <PRIO>	0-4095 0-7	Define 802.1p priority assigned to packets in this VLAN, if 'set VTU override' parameter is activated
set VTU settings_CPU	<NUMBER> <CPU>	0-4095 unmodified/ untagged/ tagged/ not_member	Assign actions performed by this port during transfer of a packet with specified VID. - *Unmodified* — packets will be sent by the port without any changes. - *Untagged* — packets will always be sent without VLAN tag by this port. - *Tagged* — packets will always be sent with VLAN tag by this port. - *Tagged* — packets with specified VID will not be sent by this port, i.e. the port is not the member of VLAN.
settings_GE_PORT0	<NUMBER> <CPU>	0-4095 unmodified/ untagged/ tagged/ not_member	Assign actions performed by this port during transfer of a packet with specified VID. - *Unmodified* — packets will be sent by the port without any changes. - *Untagged* — packets will always be sent without VLAN tag by this port. - *Tagged* — packets will always be sent with VLAN tag by this port. - *Tagged* — packets with specified VID will not be sent by this port, i.e. the port is not the member of VLAN.
settings_GE_PORT1	<NUMBER> <CPU>	0-4095 unmodified/ untagged/ tagged/ not_member	Assign actions performed by this port during transfer of a packet with specified VID. - *Unmodified* — packets will be sent by the port without any changes. - *Untagged* — packets will always be sent without VLAN tag by this port. - *Tagged* — packets will always be sent with VLAN tag by this port. - *Tagged* — packets with specified VID will not be sent by this port, i.e. the port is not the member of VLAN.
settings_GE_PORT2	<NUMBER> <CPU>	0-4095 unmodified/ untagged/ tagged/ not_member	Assign actions performed by this port during transfer of a packet with specified VID. - *Unmodified* — packets will be sent by the port without any changes. - *Untagged* — packets will always be sent without VLAN tag by this port.

			- *Tagged* — packets will always be sent with VLAN tag by this port. - *Tagged* — packets with specified VID will not be sent by this port, i.e. the port is not the member of VLAN.

`settings_SFP0`	`<NUMBER>`
	`<CPU>`
		`0-4095`
		`unmodified/ untagged/ tagged/ not_member`
			Assign actions performed by this port during transfer of a packet with specified VID.
			- *Unmodified* — packets will be sent by the port without any changes.
			- *Untagged* — packets will always be sent without VLAN tag by this port.
			- *Tagged* — packets will always be sent with VLAN tag by this port.
			- *Tagged* — packets with specified VID will not be sent by this port, i.e. the port is not the member of VLAN.

`settings_SFP1`	`<NUMBER>`
	`<CPU>`
		`0-4095`
		`unmodified/ untagged/ tagged/ not_member`
			Assign actions performed by this port during transfer of a packet with specified VID.
			- *Unmodified* — packets will be sent by the port without any changes.
			- *Untagged* — packets will always be sent without VLAN tag by this port.
			- *Tagged* — packets will always be sent with VLAN tag by this port.
			- *Tagged* — packets with specified VID will not be sent by this port, i.e. the port is not the member of VLAN.

`show list`			Show element list in VTU table
`show one`	`<NUMBER>`	`0-4095`	Show information on the current VTU table element
`show table`			Show VTU table

3.3.39.2 QoS parameter configuration mode

To enter this mode, execute 'QoS_control' command in the switch or 802.1q configuration mode.

```
SMG-[CONFIG]-[SWITCH]> QoS_control
Entering QoS_control mode.
SMG-[CONFIG]-[SWITCH]-[QoS]>
```

Command	***Parameter***	***Value***	***Action***
`?`			Show the list of available commands.
`802.1q`			Return to 802.1q parameter configuration mode
`apply`	`<YES_NO>`	`yes/no`	Apply QoS settings.
`confirm`			Confirm QoS settings. If you fail to confirm settings in 1 minute interval, the previous values will be restored.
`exit`			Return from this configuration submenu to the upper level.

quit			Terminate this CLI session
save			Save QoS settings without applying
set 802.1p_prio_mapping	<PRIO> <QUEUE>	0-7 0-3	Distribute packets into queues depending on the 802.1p priority PRIO — 802.1p priority number QUEUE — queue number
set default_VLAN_priority	<PORT> <DEFPRIO>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) 0-7	Define 802.1p priority to untagged packets received by this port. If 802.1p or IP diffserv priority is already assigned to the packet, this setting will not be used ('default vlan priority' will not be applied to packets containing IP header, when one of the QoS modes is in use: DSCP only, DSCP preferred, 802.1p preferred, and also to untagged packets.
set diffserv_prio_mapping	<NUMBER> <QUEUE>	*1 0-3	Distribute packets into queues depending on the IP diffserv priority NUMBER — IP diffserv priority number QUEUE — queue number
set egress_limit	<PORT> <EGRLIM>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) on/off	Enable/disable the bandwidth restriction for outgoing port traffic
set egress_rate_limit	<PORT> <EGRRATE>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) 0-250000	Enable the bandwidth restriction (in kbps) for outgoing port traffic
set ingress_limit_mode	<PORT> <INGRMODE>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) off/ all/ mult_flood_broad/ mult_broad/ broad	Enable restriction mode for traffic coming to the current port. INGRMODE — restriction mode: - *off* — no restriction. - *all* — restrict all traffic. - *mult_flood_broad* — multicast, broadcast, and flooded unicast traffic will be restricted. - *mult_broad* — multicast and broadcast traffic will be restricted. - *broad* — only broadcast traffic will be restricted.
set ingress_rate_ prio_0/1/2/3	<PORT> <INGPRIO>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) 0-250000	Define the bandwidth restriction (in kbps) for incoming port traffic for queue 0/1/2/3.

set QoS_mode	<PORT> <QOSMODE>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) DSCP_only/ 802.1p_only/ DSCP_preferred/ 802.1p_preferred	Set the QoS utilization mode QOSMODE — utilization mode: - *DSCP only* — distribute packets into queues based on IP diffserv priority only. - *802.1p* only — distribute packets into queues based on 802.1p priority only. - *DSCP preferred* — distribute packets into queues based on IP diffserv and 802.1p priorities, if both priorities are present in the packet, IP diffserv priority is used for queuing purposes. - *802.1p preferred* — distribute packets into queues based on IP diffserv and 802.1p priorities, if both priorities are present in the packet, 802.1p priority is used for queuing purposes.
set remapping_priority	<PORT> <NUM> <REMAP>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) 0-7 0-7	Remap 802.1p priorities for untagged packets. PORT — port being configured NUM — the current priority value REMAP — new value
show QOS	<PORT>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/SFP0(6)/ SFP1(7)	Show QoS configuration parameters for this port
show QOS_diffserv			Show parameters of packets distribution into queues depending on the IP diffserv priority
show QOS_priomap			Show parameters of packets distribution into queues depending on the 802.1p priority

3.3.40 Syslog parameter configuration mode

To enter this mode, execute 'syslog' command in the configuration mode.

```
SMG-[CONFIG]> syslog
Entering syslog mode.
SMG-[CONFIG]-SYSLOG>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
alarm	<ALARM>	0-99	Send the data on the defined priority level faults, 0 — disable data transfer.
apply	yes/no		Apply system log settings
authlog set	IP PORT	IP address in AAA.BBB.CCC.DDD format	Set server address for syslog messages transmission and operation mode.

	ONOFF LOCREM	1-65535 off/on local/remote	on/off - enable/disable logging; local/remote - 'remote' means transmit logs to syslog server
authlog show			Show current parameters of logging
calls	<CALLS>	0-99	Enable tracing of calls with the defined debug level, 0 — disable data transfer.
config			Return to Configuration menu.
exit			Return from this configuration submenu to the upper level.
h323	<H323>	0-99	Enable H.323 signaling tracing with defined debug level, 0 – data will not be transmitted
hw	<E1> <HW>	0-15 0-99	Send E1 stream hardware data with the defined debug level, 0 — disable data transfer. E1 — E1 stream name. HW — priority level.
ipaddr	<IPADDR>	IP address in AAA.BBB.CCC.DDD format	Define syslog server IP address
isup	<ISUP>	0-99	Enable tracing of ISUP subsystem with the defined debug level, 0 — disable data transfer.
msp	<MSP>	0-99	Enable tracing of MSP signal processor resources with the defined debug level, 0 — disable data transfer.
port	<PORT>	1-65535	Define a local port number
Q931	<Q931>	0-99	Enable tracing of Q.931 signalling with the defined debug level, 0 — disable data transfer.
quit			Terminate this CLI session
radius	<RADIUS>	0-99	Enable tracing of RADIUS protocol with the defined debug level, 0 — disable data transfer.
rtp-create	<RTP>	0-99	Enable tracing of RTP forwarding creation with the defined debug level, 0 — disable data transfer.
show			Show Syslog configuration information
sipt	<SIPT>	0-99	Enable tracing of SIP-T signalling with the defined debug level, 0 — disable data transfer.
start			Enable data transmission to a syslog server
stop			Disable data transmission to a syslog server
userlog	<IPADDR> <PORT> <MODE>	IP address in AAA.BBB.CCC.DDD format 1-65535 off/standart/full	Enable the output of history of entered commands IPADDR — syslog server IP address PORT — syslog server port MODE — verbosity level of the entered commands log *off* — disable entered commands logs generation. standart — messages contain the name of modified parameter. *full* — messages contain the name of modified parameter as well as parameter values before and after the modification.

3.3.41 Voice message file management configuration mode

To enter the trunk group configuration mode, execute 'user-voice-files' command in the configuration mode.

```
SMG-[CONFIG]> user-voice-files
Entering User voice-files setup mode.
SMG-[CONFIG]-USER_VOICE_FILES>
```

Command	Parameter	Value	Action
?			Show the list of available commands.
exit			Return from this configuration submenu to the upper level.
quit			Terminate 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	Delete a custom file of the defined 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	Enable the utilization of a custom file of the defined type.
show files			Show uploaded user files
show usage			Show user files utilization

3.3.42 IVR function configuration mode

To enter the trunk group configuration mode, execute 'ivr' command in the configuration mode.

```
SMG-[CONFIG]> ivr
Entering IVR-setup mode
SMG-[CONFIG]-IVR>
```

Command	Parameter	Value	Action
?			Show the list of available commands.
add scenario			Add a new IVR scenario file.
config			Return to Configuration menu.
delete scenario			Remove IVR scenario file
download scenario		<SRC_PATH_AND_FILE_NAME><DST_FILE_NAME><SERVER_IP>	Download scenario from the device via FTP

exit			Return from this configuration submenu to the upper level.
quit			Terminate this CLI session
remove scenario		Index [0-255]	Delete IVR scenario
set scenario filename		Index [0-255]	Define IVR scenario file name
set scenario name		Index [0-255]	Define IVR scenario name
set scenario path		default or /mnt/sd[abc][1-7]	Define the IVR scenario storage path
show list scenarios			Show all IVR scenario files
show path scenario			Show the IVR scenario file storage path
show scenario		Index [0-255]	Show IVR scenario

3.3.43 Trunk group configuration mode

To enter the trunk group configuration mode, execute 'trunk group <TRUNK_INDEX>' command in the configuration mode, where <TRUNK_INDEX> is a trunk group number.

```
SMG-[CONFIG]> trunk group 0
Entering trunk-mode.
SMG-[CONFIG]-TRUNK[0]>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
channel add	CHAN_INDEX	0-31	Add a channel from selected E1 stream to trunk group 'E1-channels'
channel order	CHAN_ORDER	successive_forward/ successive_backward/ start_first_forward/ start_last_backward	Select channel order for 'E1 channels' trunk groups or Linkset-Line
channel remove	CHAN_INDEX	0-31	Remove E1 channel from trunk group 'E1 channels'
config			Return to Configuration menu.
cps max	<CPS_MAX>	0-255	CPS threshold value that may pass through the trunk group
cps warn	<CPS_WARN>	0-255	CPS emergency value that when exceeded, will output the warning into the alarm log
destination	<TG_ENTRY> <ENTRY_INDEX>	Q.931/SS7/SIPT/ E1-channels/ Linkset-Line Unsigned integer value	Assign the trunk group to the Q931 interface, SS7, SIP-T, specified E1 channels or specified SS7 linkset streams TG_ENTRY — interface type ENTRY_INDEX — object index (number of Q931 signalling stream, link set, SIP-T interface)
direct prefix	<IDX>	0-255/none	Define the direct call forwarding from the current trunk group to the specified prefix without caller and callee number analysis
disable all	<YES_NO>	yes/no	Enable/disable all incoming and outgoing calls for the current trunk group
disable in			Disable all incoming calls for the current trunk group

disable out			Disable all outgoing calls for the current trunk group
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
linkset-line add	<LINE_INDEX>	0-15	Add E1 stream from selected SS7 Linkset to 'Linkset-Line' trunk group.
linkset-line remove	<LINE_INDEX>	0-15	Remove E1 stream from 'Linkset-Line' trunk group
local	<YES_NO>	yes/no	When enable means that the subscriber is local.
modifiers table incoming called	<MODTBL_INDEX>	0-255/none	Define trunk group modifier for modifications based on the analysis of the callee number received from the incoming channel.
modifiers table incoming calling	<MODTBL_INDEX>	0-255/none	Define trunk group modifier for modifications based on the analysis of the caller number sent to the outgoing channel.
modifiers table outgoing called	<MODTBL_INDEX>	0-255/none	Define trunk group modifier for modifications based on the analysis of the callee number sent to the outgoing channel.
modifiers table outgoing original	<MODTBL_INDEX>	0-255/none	Define trunk group modifier for modifications based on the analysis of the initial callee number sent to the outgoing channel.
modifiers table incoming redirecting	<MODTBL_INDEX>	0-255/none	Define trunk group modifier for modifications based on the analysis of the redirecting subscriber number sent to the outgoing channel.
modifiers table outgoing calling	<MODTBL_INDEX>	0-255/none	Define trunk group modifier for modifications based on the analysis of the caller number received from the incoming channel.
name	<s_name>	you may use letters, numbers, '_' character 31 characters max.	Define trunk group name
quit			Terminate this CLI session
radius profile incoming	<IDX>	0-31/no	RADIUS profile selection for incoming communications
radius profile outgoing	<IDX>	0-31/no	RADIUS profile selection for outgoing communications
recover on egress failure	<RECOVER>	no/yes	Recover calls after failure on incoming leg
reserv	<TG_RSV_IDX>	0-31	Define the redundant trunk group number
show			Show the trunk group configuration

3.3.44 Trunk directions configuration mode

To enter the trunk direction configuration mode, execute 'trunk direction <DIRECTION_INDEX>' command in the configuration mode, where < DIRECTION _INDEX> is a trunk group number.

```
SMG-[CONFIG]> trunk direction 0
Entering trunk-mode.
SMG-[CONFIG] – TRUNK_DIRECTION[0]>
```

Command	***Parameter***	***Value***	***Action***
?			Show the list of available commands.
config			Return to Configuration menu.
exit			Return from this configuration submenu to the upper level.
history			View history of entered commands.
list add	<TD_TRUNK>	0-63	Add the trunk group with the specified index into direction
list remove	<TD_TRUNK>	0-63	Remove the trunk group with the specified index from direction
mode		successive_forward/ successive_backward/ first_forward/ last_backward	Define trunk group selection method for a direction Sequential forward Sequential back From the first and forward From the last and back
name	<s_name >	String, 63 characters max.	Define trunk direction name
quit			Terminate this CLI session
show			Show the trunk direction settings

3.4 SMG-2016 switch configuration

3.4.1 Switch structure

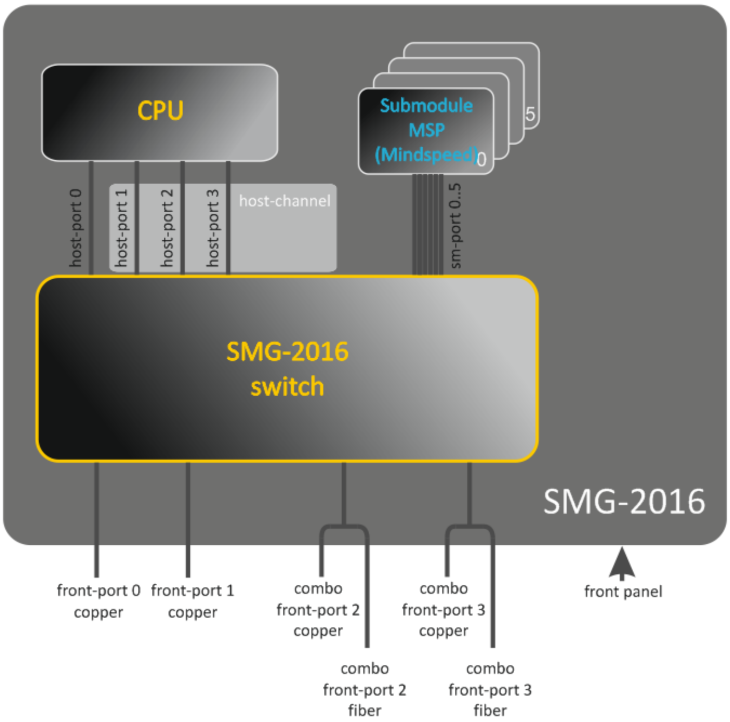


Fig. 37 — Switch structure

SMG-2016 switch is equipped with the following interfaces:

- *front-port* — switch external Ethernet ports located on the front panel.
- Possible values: 0 — 3.

- ports 0.. 1 — copper-wire ports
- ports 2.. 3 — optical/copper-wire combo ports.

- *port-channel* — LAG aggregation groups of front-port interfaces of the switch used for combining multiple front-ports into a single LACP group.
- Possible values: 1 – 4.
- *cpu-port* – inner port of the switch for SMG-2016 management. Possible value: 0.
- *host-port* — SMG-2016 switch internal ports designed for the SMG-2016 CPU communication.
- Possible values: 0 – 2.
- *host-channel* — LAG host-channel aggregation group of the switch interfaces, this group is always active.
- Possible value: 1.
- *sm-port* — SMG-2016 switch internal ports designed for the SM-VP submodule communication.
- Possible values: 0 – 5.

During the switch operation, unit number value equal to 1 will be used.

3.4.2 SMG 2016 switch interface management commands

interface

This command allows you to enter the SMG-2016 switch interface configuration mode.

Syntax

interface <interface><number>

Parameters

<interface> — interface type:

- front-port — external interfaces of the switch.
- host-channel — LAG host-channel aggregation groups of the switch interfaces.
- port-channel — LAG aggregation groups of external interfaces of the switch.

<number> — port number:

- for front-port: <unit/port>, where
  - unit — SMG-2016 module number, the value is always 1.
  - port — port number; possible values [0 .. 3].
- for host-channel: 1;
- for port-channel: [1 .. 4].

For configuration of all ports for a single interface type, use 'all' as the <number> parameter value.

shutdown

This command disables the interface being configured.

The command in negative form enables the interface being configured.

Syntax

[no] shutdown

Parameters

There are no parameters for this command.

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> shutdown
```

Configured interface is disabled.

bridging to

This command defines the permission for the traffic exchange between the interfaces.

The command in negative form denies the traffic exchange between the interfaces.

Syntax

[no] bridging to <interface><range>

Parameters

<interface> — interface type:

- cpu-port;
- front-port — external uplink interfaces.
- host-channel;
- host-port;
- port-channel — LAG aggregation groups of uplink interfaces.
- sm-port.

<range> — port number(s) that are allowed to exchange traffic:

- for cpu-port: <1/0>, where:
- for front-port: <unit/port>, where:
  - unit — module number; possible value [1],
  - port — port number; possible values [0 .. 3].
- for host-channel: [1];
- for host-port:
  - unit — module number; possible value [1],
  - port — port number; possible values [0 .. 2].
- for port-channel: [0 .. 4].
- for sm-port: [0 .. 15].
  - unit — module number; possible value [1],
  - port — port number; possible values [0 .. 5].

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> bridging to front-port all
```

flow-control

This command enables/disables data flow control mechanism for the interface being configured. Flow control mechanism allows to compensate the transfer rate difference of the transmitter and receiver. If the traffic volume exceeds the specific level, the receiver will send frames informing the transmitter on the necessity to lower the traffic volume and reduce the amount of lost frames. Implementation of this mechanism requires that the remote device also supports this function.

Syntax

flow-control <act>

Parameters

<act> — assigned action:

- on — enable
- off — disable

Default value

off

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> flow-control on
```

frame-types

The command assigns the specific packet reception rules to the interface:

- Receive both tagged and untagged packets
- Receive packets with VLAN tag only

Syntax

frame-types <act>

Parameters

<act> — assigned action:

- all — receive both tagged and untagged packets
- tagged — receive packets with VLAN tag only

Default value

All packets are accepted (both tagged and untagged)

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> frame-types all
```

Untagged traffic reception is enabled for the configured ports.

speed

This command specifies transfer rate value for the configured interface.

Defined modes are as follows: 10Mbps, 100Mbps, 1000Mbps. For 10Mbps or 100Mbps, you should specify the transceiver operation mode: duplex or half-duplex.

Syntax

speed <rate> [<mode>]

Parameters

<rate> — transfer rate value: 10M; 100M; 1000Mbps; 10Gbps

<mode> — transceiver operation mode:

- full-duplex
- half-duplex

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> speed 10M full-duplex
```

'10Mbps, duplex' interface speed mode is configured.

speed auto

This command specifies transfer rate value for the configured interface automatically.

Syntax

speed auto

Parameters

There are no parameters for this command.

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> speed auto
```

Transfer rate for the port will be configured automatically.

show interfaces configuration

This command allows you to view the SMG-2016 switch interface configuration.

Syntax

show interfaces configuration <interface><number>

Parameters

<interface> — interface type:

- front-port — external uplink interfaces.
- host-channel.
- host-port.
- port-channel — LAG aggregation groups of external uplink interfaces.
- sm-port.

<number> — port number:

- all — all ports of the selected interface.
- for front port: <unit/port>, where:
  - unit — module number; possible values [1],
  - port — port number; possible values [0 .. 3].
- for host-channel: [1];
- for host-port:
  - unit — module number; possible value [1],
  - port — port number; possible values [0 .. 2].

- for port-channel: [0 .. 4].
- for sm-port: [0 .. 15].
  - unit — module number; possible value [1],
  - port — port number; possible values [0 .. 5].

Example

```
SMG2016-[CONFIG]-[SWITCH]> show interfaces configuration front-port all
Port                 Duplex   Speed      Neg        Flow      Admin
                                                    control   State
------------------   ------   --------   --------   -------   -----
front-port   1/0     Full     10 Mbps    Enabled    Off       Up
front-port   1/1     Full     10 Mbps    Disabled   Off       Up
front-port   1/2     Full     10 Mbps    Enabled    Off       Up
front-port   1/3     Full     10 Mbps    Enabled    Off       Up
SMG2016-[CONFIG]-[SWITCH]>
```

show interfaces status

This command allows you to view the interface or interface group status.

Syntax

show interfaces status <interface><number>

Parameters

<interface> — interface type:

- front-port — external uplink interfaces.
- host-channel
- host-port ;
- port-channel — LAG aggregation groups of external uplink interfaces.
- sm-port

<number> — port number:

- all — all ports of the selected interface.
- for front port: <unit/port>, where:
  - unit — module number; possible values [1],
  - port — port number; possible values [0 .. 3].
- for host-channel: [1];
- for host-port:
  - unit — module number; possible value [1],
  - port — port number; possible values [0 .. 2].
- for port-channel: [0 .. 4].
- for sm-port:
  - unit — module number; possible value [1],
  - port — port number; possible values [0 .. 5].

Example

```
SMG2016-[CONFIG]-[SWITCH]> show interfaces status front-port all
Port                 Media     Duplex   Speed      Neg        Flow      Link    Back
                                                              control   State   Pressure
------------------   -------   ------   --------   --------   -------   -----   --------
front-port   1/0     N/A       N/A      N/A        N/A        N/A       Down    N/A
front-port   1/1     copper    Full     10 Mbps    Disabled   Off       Up      Disabled
front-port   1/2     copper    Full     100 Mbps   Enabled    Off       Up      Disabled
front-port   1/3     N/A       N/A      N/A        N/A        N/A       Down    N/A
SMG2016-[CONFIG]-[SWITCH]>
```

show interfaces counters

This command allows you to view the interface or interface group counters.

Syntax

show interfaces counters <interface><number>

Parameters

<interface> — interface type:

- cpu-port.
- front-port — external uplink interfaces.
- host-channel.
- host-port.
- port-channel — LAG aggregation groups of uplink interfaces.
- sm-port.

<range> — port number(s) that are allowed to exchange traffic:

- for cpu-port: <1/0>, where:
- for front-port: <unit/port>, where:
  - unit — module number; possible value [1],
  - port — port number, possible values [0 .. 3].
- for host-channel: [1];
- for host-port:
  - unit — module number, possible value [1],
  - port — port number, possible values [0 .. 2].
- for port-channel: [0 .. 4].
- for sm-port:
  - unit — module number; possible value [1],
  - port — port number; possible values [0 .. 5].

Example

```
SMG2016-[CONFIG]-[SWITCH]> show interfaces counters front-port all

   MAC MIB counters receive
   ~~~~~~~~~~~~~~~~~~~~~~~~
Port            UC recv           MC recv          BC recv           Octets recv
---------------------------------------------------------------------------------
front-port 1/0        0                0                0                      0
front-port 1/1    436940            6297             9289               65685375
```

```
front-port 1/2   1422764           6077           41999             210652881
front-port 1/3         0              0               0                     0

   MAC MIB counters sent
   ~~~~~~~~~~~~~~~~~~~~~
Port            UC sent           MC sent           BC sent           Octets sent
----------------------------------------------------------------------------------
front-port 1/0        0                 0                 0                   0
front-port 1/1   455819              6087             42006            96955149
front-port 1/2   148842              6280              9296            17450454
front-port 1/3        0                 0                 0                   0
```

3.4.3 Aggregation group configuration commands

channel-group

Use this command to add FRONT-PORT interfaces into the aggregation group.

The command in negative form (no) removes FRONT-PORT interfaces from the aggregation group.

Syntax

channel-group <id> [force]

no channel-group

Parameters

<id> — sequential number of an aggregation group for the port to be added into, possible values [1 .. 4].

- [force] — optional parameter, possible values
- force — means to be compatible with the rest of the group members.

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> channel-group 1
```

All uplink ports are combined into groups 1.

lacp mode

This command allows you to select the channel aggregation mode:

- Passive — in this mode, the switch will not initiate creation of a logical link, but will process incoming LACP packets.
- Active — in this mode, the switch should establish the aggregated communication link and initialize the negotiation.

Communication links are aggregated when the other party operates in LACP active or passive mode.

The command in negative form (no) defines the default link aggregation mode.

Syntax

lacp mode <name>

no lacp mode

Parameters

<name> — mode:

- active.

- passive.

Default value

active

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> lacp mode active
```

'Active' link aggregation mode is enabled for configured channels.

mode

Use this command to define the channel aggregation mode:

- Use LACP link aggregation protocol
- Disable link aggregation

Syntax

mode <act>

Parameters

<act> — mode:

- lacp — enable LACP
- static — disable link aggregation protocol

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> mode lacp
```

Link aggregation mode is enabled for the configured interface.

lacp port-priority

Use this command to define the priority of the configured port. Priority will be specified in the range of [1 .. 65535]. 1 is the highest priority value.

The command in negative form (no) defines the default priority value.

Syntax

lacp port-priority <priority>

no lacp port-priority

Parameters

<priority> — priority for the current port; possible values [0 .. 65535].

Default value

Priority 32768 is specified for all ports

Command mode

INTERFACE FRONT-PORT

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> lacp port-priority 256
```

Port priority 256 is specified for all configured ports.

lacp rate

Use this command to define the time interval for transmission of LACPDU control packets.

The command in negative form (no) defines the default time interval for transmission of LACPDU control packets.

Syntax

lacp rate <rate>

no lacp rate

Parameters

<rate> — transmission interval:

- fast — 1-sec transmission interval.
- slow — 30-sec transmission interval.

Default value

1 second (fast)

Command mode

INTERFACE FRONT-PORT

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> lacp rate slow
```

30-second time interval is defined for transmission of LACPDU packets.

3.4.4 SMG-2016 board VLAN interface management commands

pvid

Use this command to define the default VID value for packets received by this port.

When an untagged packet or packet with VLAN tag VID value equal to 0 is received, VID value equal to PID will be defined for such a packet.

Syntax

pvid <num> Parameters

<num> — VLAN port ID, specified in the range of [1 .. 4094].

Default value

PVID = 1

Command mode

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> pvid 5
```

PVID 5 is defined for the configured port.

3.4.5 STP/RSTP configuration commands

spanning-tree enable

Use this command to enable the STP function for the configured interface.

The command in negative form (no) disables the STP utilization for the interface.

Syntax

[no] spanning-tree enable

Parameters

There are no parameters for this command.

Command mode

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> spanning-tree enable
```

STP function is enabled for all front ports.

spanning-tree pathcost

Use this command to specify the STP operation path cost for the configured interface.

The command in negative form (no) defines the default path cost.

0 is set by default.

Syntax

spanning-tree pathcost <pathcost>

no spanning-tree pathcost

Parameters

<pathcost> — path cost, permitted value range is [0..200000000].

Default value

Path cost value = 0

Command mode

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> spanning-tree pathcost 1
```

Defined path cost value is 1.

spanning-tree priority

Use this command to specify the STP operation priority for the configured interface.

The command in negative form (no) defines the default STP operation priority value. 128 is set by default.

Syntax

spanning-tree priority <priority>

no spanning-tree priority

Parameters

<priority> — priority, may take up values divisible by 16 [0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240].

Default value

128

Command mode

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> spanning-tree priority 144
```

Defined priority is 144.

spanning-tree admin-edge

Use this command to define the connection type as the edge link to the host. In this case, data transmission is enabled automatically for the interface, when the link is established.

The command in negative form (no) restores the default value.

Syntax

[no] spanning-tree admin-edge

Parameters

There are no parameters for this command.

Default value

off

Command mode

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> spanning-tree admin-edge
```

Edge-link connection type is enabled for the configured port.

spanning-tree admin-p2p

Use this command to define the p2p connection identification type.

The command in negative form (no) defines the default p2p connection identification type.

Syntax

spanning-tree admin-p2p <type>
no spanning-tree admin-p2p

Parameters

<type> — connection identification type:

- auto — identification is based on BPDU.
- force-false — forcedly set link as non-p2p.
- force-true — forcedly set link as p2p.

Default value

p2p connection type identification is based on BPDU

Command mode

INTERFACE FRONT-PORT
INTERFACE PORT-CHANNEL

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> spanning-tree admin-p2p auto
```

For the configured port, p2p connection type identification is based on BPDU.

spanning-tree auto-edge

Use this command to set the automatic bridge detection on the configured interface.

The command in negative form (no) disables automatic bridge detection on the configured interface.

Automatic bridge detection function is enabled by default.

Syntax

[no] spanning-tree auto-edge

Parameters

There are no parameters for this command.

Command mode

INTERFACE FRONT-PORT
INTERFACE PORT-CHANNEL

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> spanning-tree auto-edge
```

'Automatic bridge detection' function is enabled.

3.4.6 MAC table configuration commands

mac-address-table aging-time

Use this command to set the MAC address lifetime globally in a table.

The command in negative form (no) defines the default MAC address lifetime.

Syntax

[no] mac-address-table aging time <aging time>

no mac-address-table aging time

Parameters

<aging time> — MAC address lifetime, possible values [10 .. 630] seconds.

Default value

300 seconds

Command mode

CONFIG-SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> mac-address-table aging-time 100
```

show mac address-table count

Use this command to view the quantity of MAC address records for all front-port, port-channel and slot-channel interfaces.

Syntax

show mac address-table count

Parameters

There are no parameters for this command.

Command mode

CONFIG-SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> show mac address-table count
17 valid mac entries
```

show mac address-table include/exclude interface

Use this command to view the MAC address table for the specific interface.

Syntax

show mac address-table include/exclude interface <interface><number>

Parameters

<interface> — interface type:

- front-port — external uplink interfaces.
- host-channel;
- port-channel — LAG aggregation groups of external uplink interfaces.

<number> — port number:

- all — all ports of the selected interface.
- for front port: <unit/port>, where:

- unit — module number; possible values [1],
- port — port number; possible values [0 .. 3].

- for host-channel: [1];
- for port-channel: [0 .. 4].

Command mode

CONFIG-SWITCH

3.4.7 Port mirroring configuration commands

mirror <rx|tx> interface

Use this command to enable mirroring operation at the switch ports for incoming/outgoing traffic.

Port mirroring allows to copy the traffic coming from one port to another in order to perform an external analysis.

The command in negative form (no) disables the mirroring operation.

Syntax

[no] mirror <rx|tx> interface <port><num>

Parameters

<rx|tx> — traffic type:

- rx — incoming
- tx — outgoing

<port> — interface type:

- front-port — external uplink interfaces.
- host-channel — interfaces for interface modules connection.
- host-port.
- port-channel — logical aggregation of external uplink interfaces.
- sm-port.

<num> — sequential number of the specified group port (you may specify multiple ports separated by ',' or the port range separated by '-'):

- 'all' — all ports of the current group.

<interface> — interface type:

- front-port — external uplink interfaces.
- host-channel.
- host-port.
- port-channel — LAG aggregation groups of external uplink interfaces.
- sm-port.

<number> — port number:

- all — all ports of the selected interface.
- for front port: <unit/port>, where:

  - unit — module number; possible values [1],
  - port — port number; possible values [0 .. 3].

- for host-channel: [1];
- for host-port:

        - unit — module number; possible value [1],
        - port — port number, possible values [0 .. 2].

    - for port-channel: [0 .. 4].
    - for sm-port:

        - unit — module number; possible value [1],
        - port — port number; possible values [0 .. 5].

Command mode

CONFIG-SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> mirror rx interface front-port 1/3
```

For traffic incoming to front-port 1/3 interfaces, the

'port mirroring' operation is enabled. Traffic is copied from slot-ports to analyzer port defined with 'mirror rx analyzer' command.

mirror <rx|tx> analyzer

Use this command to specify a port, that the packets for analysis of traffic incoming/outgoing from/to ports defined with 'mirror rx port/ mirror tx port' command will be copied to.

The command in negative form (no) disables analysis of transferred incoming/outgoing traffic.

Syntax

[no] mirror <rx|tx> analyzer <interface><port>

Parameters

<rx|tx> — traffic type:

- rx — incoming
- tx — outgoing

<interface> — interface type. As an analyzer port, you may use front-port, port-channel interfaces only.

<port> — sequential number of the front-port group port in <unit/port> format, where:

- for front port: <unit/port>, where:

    - unit — module number; possible values [1],
    - port — port number; possible values [0 .. 3].

- for port-channel: [0 .. 4].

Command mode

CONFIG-SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> mirror rx analyzer front-port 1/2
```

Data for an external analysis will be mirrored to the front-port 1/2 from the port(s) that have 'incoming traffic mirroring' enabled.

mirror add-tag

Use this command to add 802.1q tag for the analyzed traffic. For tag value configuration, use **'mirror <rx/tx> added-tag-config'** command.

The command in negative form (no) deletes the tag.

Syntax

[no] mirror add-tag

Parameters

There are no parameters for this command.

Command mode

CONFIG-SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> mirror add-tag
```

mirror <rx|tx> added-tag-config

Use this command to specify the tag value, that may be added to the analyzed incoming/outgoing traffic.

Syntax

mirror <rx|tx> added-tag-config vlan <vid> [user-prio <user-prio>]

Parameters

<vid> — VLAN ID; possible values [1 .. 4094].

<user-prio> — COS priority; possible values [0 .. 7].

Command mode

CONFIG-SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> mirror rx added-tag-config vlan 77 user-prio 5
```

mirror <rx|tx> vlan

This command specifies VLAN ID that will be used in mirroring operation during incoming/outgoing traffic transmission.

Syntax

[no] mirror <rx|tx> vlan <vid>

Parameters

<rx|tx> — traffic type:

- rx — incoming
- tx — outgoing

<vid> — VLAN ID; possible values [1..4094].

Command mode

CONFIG-SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> mirror rx vlan 56
```

3.4.8 SELECTIVE Q-IN-Q configuration commands

To perform Selective Q-in-Q general configuration, you may use **SELECTIVE Q-IN-Q COMMON** command mode. To define Selective Q-in-Q rule list, you may use **SELECTIVE Q-IN-Q LIST** command mode.

SELECTIVE Q-IN-Q function allows to assign external SPVLAN (Service Provider's VLAN), substitute Customer VLAN, and block the transmission of traffic based on configured filtering rules by internal VLAN numbers (Customer VLAN).

add-tag

Use this command to add an external tag based on the internal tag.

The command in negative form (no) removes the defined rule.

Syntax

[no] add-tag svlan <s-vlan> cvlan <c-vlan>

Parameters

<s-vlan> — external tag number; possible values [1..4095].

<c-vlan> — internal tag number(s); possible values 1-4094. C-VLAN list values should be separated by ','.

Command mode

SELECTIVE Q-IN-Q

overwrite-tag

This command enables VLAN substitution in the required direction.

The command in negative form (no) removes the defined rule.

Syntax

[no] overwrite-tag new-vlan <new-vlan> old-vlan <old-vlan><rule_direction>

Parameters

<new-vlan> — new VLAN number; possible values [1..4095].

<old-vlan> — VLAN number that should be substituted; possible values [1 .. 4094].

<rule_direction> — traffic direction:

- Ingress — incoming
- Egress — outgoing

Command mode

SELECTIVE Q-IN-Q

remove

Use this command to delete Selective Q-in-Q rule by the defined number.

Syntax

```
remove <rule_index>
```

Parameters

<rule_index> — rule number; possible values [0 .. 511].

Command mode

SELECTIVE Q-IN-Q

clear

Use this command to delete all Selective Q-in-Q rules.

Syntax

```
clear
```

Parameters

There are no parameters for this command.

Command mode

SELECTIVE Q-IN-Q

selective-qinq enable

Use this command to enable Selective Q-in-Q for the configured interface of SMG-2016 switch. The command in negative form (no) disables Selective Q-in-Q on the configured interface.

Syntax

```
[no] selective-qinq enable
```

Parameters

There are no parameters for this command.

Command mode

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

selective-qinq list

Use this command to assign Selective Q-in-Q rule list to the configured interface of SMG-2016 switch.

The command in negative form (no) deletes the assignment.

Syntax

```
selective-qinq list <name>
no selective-qinq list
```

Parameters

<name> — name of the Selective Q-in-Q rule list

Command mode

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

show interfaces selective-qinq lists

Use this command to view the information on Selective Q-in-Q status on the switch interfaces.

Syntax

show interfaces selective-qinq lists

3.4.9 DUAL HOMING protocol configuration

backup interface

Use this command to specify the backup interface, that will be used for communication fallback, when the main connection is lost. You can enable backup only for those interfaces where SPANNING TREE protocol is disabled.

The command in negative form (no) removes the setting from the interface.

Syntax

[no] backup interface <INTERFACE><INDEX> vlan <VLAN_ID_RANGE>

Parameters

<INTERFACE> — interface type:

- front-port — external interfaces.
- port-channel — LAG aggregation groups of external uplink interfaces.
-

<INDEX> — port number.

- for front port: <unit/port>, where:
  - unit — SMG-2016 board number, possible value is 1.
  - port — port number; possible values [0 .. 3].
- for port-channel: [1 .. 4].

<VLAN_ID_RANGE> — possible values:

- [1..4094] — specific VLAN ID (of VLAN range) to enable the backup for.
- ignore — enable backup regardless of the existing VLANs for the port.

Command mode

INTERFACE FRONT-PORT

INTERFACE PORT-CHANNEL

Example

Global backup

```
SMG2016-[CONFIG]-[SWITCH]-[if]> no backup interface vlan ignore
SMG2016-[CONFIG]-[SWITCH]-[if]> backup interface front-port 1/1 vlan ignore
```

Backup in a specific VLAN

```
SMG2016-[CONFIG]-[SWITCH]-[if]> no backup interface vlan 10
SMG2016-[CONFIG]-[SWITCH]-[if]> backup interface port-channel 1 vlan 10
```

backup-interface mac-per-second

Use this command to specify the packet quantity per second, that will be sent into the active interface during the fallback:

The command in negative form (no) restores the default value (400 packets).

Syntax

[no] backup-interface mac-per-second <COUNT>

Parameters

<COUNT> — quantity of MAC addresses per second, possible value [50..400].

Default value

400 packets

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> backup-interface mac-per-second 200
```

backup-interface mac-duplicate

Use this command to specify the quantity of packet copies with the same MAC address, that will be sent into the active interface during the fallback:

The command in negative form (no) restores the default value (1 packet).

Syntax

[no] backup-interface mac-duplicate <COUNT>

Parameters

<COUNT> — quantity of packet copies, possible value [1..4].

Default value

1 packet

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> backup-interface mac-duplicate 4
```

backup-interface preemption

Use this command to specify the traffic switchover to the main interface when the connection is restored. If the configuration allow the main interface restoration during the backup interface active state, the traffic will be switched to the main interface when the link is established on it. The command in negative form (no) restores the default setting.

Syntax

[no] backup-interface preemption

Parameters

There are no parameters for this command.

Default value

Switchover is disabled.

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> backup-interface preemption
```

show interfaces backup

Use this command to view the interface backup configuration.

Syntax

show interfaces backup

Parameters

There are no parameters for this command.

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> show interfaces backup
   Backup Interface Options:
      Preemption is disabled.
      MAC recovery packets rate 400 pps.
      Recovery packets repeats count 1.

   Backup Interface Pairs
   ~~~~~~~~~~~~~~~~~~~~~~
```

```
VID    Master Interface           Backup Interface           State
----   -------------------------  -------------------------  ------------------------------
30     front-port 1/0             front-port 2/0             Master Up/Backup Standby
----   -------------------------  -------------------------  ------------------------------
150    front-port 1/0             front-port 2/0             Master Up/Backup Standby
```

3.4.10 LLDP protocol configuration

lldp enable

This command enables the switch operation via LLDP protocol.

The command in negative form (no) disables LLDP utilization by the switch.

Syntax

[no] lldp enable

Parameters

There are no parameters for this command.

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> lldp enable
```

lldp hold-multiplier

Use this command to define the amount of time for the receiving device to keep LLDP packets before dropping them.

This value will be transmitted to the receiving party in LLDP update packets; is a divisibility for LLDP timer. Thus, LLDP packet lifetime is calculated by the equation: TTL = min(65535, LLDP-Timer * LLDP-HoldMultiplier).

The command in negative form (no) restores the default value.

Syntax

lldp hold-multiplier <hold>

no lldp hold-multiplier

Parameters

<hold> — time, possible value [2 .. 10] seconds.

Default value

The default value is 4 seconds.

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> lldp hold-multiplier 5
```

lldp reinit

Use this command to define the minimum amount of time that LLDP port will wait before LLDP reinitialization.

The command in negative form (no) restores the default value.

Syntax

lldp reinit <reinit>

no lldp reinit

Parameters

<reinit> — time, possible value [1 .. 10] seconds.

Default value

The default value is 2 seconds.

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> lldp reinit 3
```

lldp timer

Use this command to define the frequency of LLDP information updates transmission by the device.

The command in negative form (no) restores the default value.

Syntax

lldp timer <timer>

no lldp timer

Parameters

<timer> — time, possible value [5..32768] seconds.

Default value

The default value is 30 seconds.

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> lldp timer 60
```

lldp tx-delay

Use this command to define the delay between the subsequent LLDP packet transmissions, initiated by changes of values or status in local LLDP MIB database.

We recommend setting this delay less than 0.25* LLDP-Timer.

The command in negative form (no) restores the default value.

Syntax

lldp tx-delay <txdelay>

no lldp tx-delay

Parameters

<txdelay> — time, possible value [1..8192] seconds.

Default value

The default value is 2 seconds.

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> lldp tx-delay 3
```

lldp lldpdu

Use this command to define the LLDP packet processing mode, when LLDP is disabled.

The command in negative form (no) restores the default value (filtering).

Syntax

lldp lldpdu [mode]

no lldp lldpdu

Parameters

[mode] — LLDP packet processing mode:

- filtering — LLDP packets are filtered, if LLDP is disabled on the switch
- flooding — LLDP packets are transmitted, if LLDP is disabled on the switch

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> lldp lldpdu flooding
```

show lldp configuration

Use this command to view LLDP configuration on all device physical interfaces, or on specified interfaces only.

Syntax

show lldp configuration [<interface>< number >]

Parameters

Optional parameters; if omitted, information for all ports will be shown on display.

[interface] — interface type:

- front-port — external uplink interfaces.
- port-channel — LAG aggregation groups of external uplink interfaces.

[number] — number of the port (you may specify multiple ports separated by ',' or the port range separated by '-'):

- for front port: <unit/port>, where:
  - unit — module number; possible values [1],
  - port — port number; possible values [0 .. 3].
- for port-channel: [0 .. 4].

Default value

Information for all ports will be shown on display.

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> show lldp configuration

   LLDP configuration
   ~~~~~~~~~~~~~~~~~~
Interface        Status              Timer (sec)  Hold multiplier  Reinit delay (sec)  Tx delay (sec)
-------------  ----------------- ------    ----------    -------------    ----------
front-port 1/0  transmit-receive   30          4             2               2
front-port 1/1  transmit-receive   30          4             2               2
front-port 1/2  transmit-receive   30          4             2               2
front-port 1/3  transmit-receive   30          4             2               2
```

show lldp neighbor

Use this command to view the information on the neighbouring devices with the active LLDP protocol.

Syntax

show lldp neighbor [<interface>< number >]

Parameters

Optional parameters; if omitted, information for all ports will be shown on display.

[interface] — interface type:

- front-port — external uplink interfaces.
- port-channel — LAG aggregation groups of external uplink interfaces.

[number] — number of the port (you may specify multiple ports separated by ',' or the port range separated by '-'):

for front port: <unit/port>, where:
- unit — module number; possible values [1],
- port — port number; possible values [0 .. 3].

for port-channel: [0 .. 4].

Default value

Information for all ports will be shown on display.

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> show lldp neighbor

   LLDP neighbors
   ~~~~~~~~~~~~~~
Interface           Device ID                Port ID                   TTL
----------------   ----------------------   -----------------------   ----------
front-port 1/1     02:00:2a:00:07:15           g15                    115/120
front-port 1/2     02:00:04:88:7e:             front-port 1/3         105/120
SMG2016-[CONFIG]-[SWITCH]>
```

show lldp local

Use this command to view LLDP information announced by this port.

Syntax

show lldp local [<interface>< number >]

Parameters

Optional parameters; if omitted, information for all ports will be shown on display.

[interface] — interface type:

- front-port — external uplink interfaces.
- port-channel — LAG aggregation groups of external uplink interfaces.

[number] — number of the port (you may specify multiple ports separated by ',' or the port range separated by '-'):

- for front port: <unit/port>, where:
  - unit — module number; possible values [1],
  - port — port number; possible values [0 .. 3].
- for port-channel: [0 .. 4].

Default value

Information for all ports will be shown on display.

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> show lldp local

   LLDP local TLVs
   ~~~~~~~~~~~~~~~
Interface           Device ID                Port ID                   TTL
----------------   ----------------------   -----------------------   ----------
front-port 1/1     02:00:04:88:7c:0a        front-port 1/1             120
front-port 1/2     02:00:04:88:7c:0a        front-port 1/2             120
```

show lldp statistics

Use this command to view LLDP statistics for front-port, port-channel interfaces.

Syntax

show lldp statistics [<interface>< number >]

Parameters

Optional parameters; if omitted, information for all ports will be shown on display.

[interface] — interface type:

- front-port — external uplink interfaces.
- port-channel — LAG aggregation groups of external uplink interfaces.

[number] — number of the port (you may specify multiple ports separated by ',' or the port range separated by '-'):

- for front port: <unit/port>, where:
  - unit — module number; possible values [1],
  - port — port number; possible values [0 .. 3].
- for port-channel: [0 .. 4].
- for slot-channel: [0 .. 15].

Default value

Information for all ports will be shown on display.

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> show lldp statistics

Tables Last Change Time: 0:0:4:28
Tables Inserts: 3
Tables Deletes: 1
Tables Dropped: 0
Tables Ageouts: 0

   LLDP statistics
   ~~~~~~~~~~~~~~~
Interface         Tx total Rx total Rx errors Rx discarded TLVs discarded TLVs unrecognized Agouts total
front-port 1/0     0         0        0          0             0              0              0
front-port 1/1    6134      6159      0          0             0              0              0
front-port 1/2    6141      6136      0          0             0              0              0
front-port 1/3     0         0        0          0             0              0              0
```

show lldp lldpdu

Use this command to view LLDPDU packet processing method for interfaces where LLDP function is disabled.

Syntax

show lldp lldpdu

Parameters

There are no parameters for this command.

Command mode

CONFIG SWITCH

Example

```
SMG2016-[CONFIG]-[SWITCH]> show lldp lldpdu
Global: flooding
```

3.4.11 QOS Configuration

qos default

Use this command to define the priority queue that will be used for packets without any preconfigured rules. Queue with value 7 has the highest priority.

Syntax

qos default <queue>

Parameters

< queue > — priority queue number; possible values [0 .. 7].

Default value

Queue 0 is used by default.

Command mode

CONFIG SWITCH

Example

```
qos default 6
```

Packets without any other specified rules will come to the queue with priority 6.

qos type

Use this command to define the rule that will be used for the packet priority field selection.

The traffic prioritization method will be chosen depending on the configured system rules (IEEE 802.1p/DSCP).

- The traffic prioritization methods featured by the system are as follows:
- All priorities are equal
- Packet selection is based on IEEE 802.1p standard
- Packet selection is based on IP ToS (type of service) at the level 3 only — Differentiated Services Code point (DSCP) support
- Interactions based on 802.1p or DSCP/TOS

Syntax

qos type <type>

Parameters

<type> — traffic prioritization method:

- 0 — all priorities are equal
- 1 — packet selection by 802.1p only (Priority field in 802.1Q tag)
- 2 — packet selection by DSCP/TOS only (Differentiated Services field of the IP packet header, 6 high bits)
- 3 — interaction based on either 802.1p or DSCP/TOS

Default value

All priorities are equal by default.

Command mode

CONFIG SWITCH

Example

```
qos type 2
```

Traffic prioritization will be performed by DSCP/TOS only.

qos map

Use this command to define the priority queue parameters:

- Specify Differentiated Services field values of the IP packet header, 6 high bits,
- Priority field value in 802.1Q tag.

Packets will be selected to this priority value based on rules defined by 'qos type' command and specified priority values.

The command in negative form (no) removes the record from the queue configuration table.

Syntax

no] qos map <type><field values> to <queue>

Parameters

<type> — traffic prioritization method:

- 0 — according to 802.1p standard (used on 2nd layer)
- 1 — according to DSCP/TOS standard (used on 3rd layer)

<field values > — field value used for packet selection, defined depending on the <parameter 1> (field values entered should be comma-separated or represent the range delimited by '-'):

- if <type> = 0, Priority field value in 802.1Q tag should be specified: [0 .. 7].
- if <type> = 0, *Differentiated Services* field values of the IP packet header, 6 high bits should be specified. Values should be entered in a decimal format: [0 .. 63].

<queue > — priority queue number; possible values [0 .. 7].

Command mode

CONFIG SWITCH

Example

```
qos map 0 7 7
```

For 7th priority queue, priority field value =7 in 802.1Q tag.

cntrset

Use this command to map the queue statistics collector to queues with the defined criteria.

Syntax

cntrset <PORT><UNIT><SET><VLAN><QUEUE><DROP PRECEDENCE>

Parameters

< PORT > — accounting port type may take up the following values:

- all — all ports.
- cpu — CPU port.
- front-port — counting front-port.
- host-port.
- sm-port.

< UNIT > — sequential number of the port:

- for cpu: possible value is [1]
- for front port: <unit/port>, where:
  - unit — module number; possible values [1]
  - port — port number; possible values [0 .. 3].
- for host-port: <unit/port>, where:
  - unit — module number; possible values [1]
  - port — port number, possible values [0 .. 2].
- for sm-port: <unit/port>, where:
  - unit — module number; possible values [1]
  - port — port number, possible values [0 .. 5].
- < SET > — statistics collector number, possible values [0 .. 1].
- < VLAN > — VLAN ID; possible values [1 .. 4094] or all
- < QUEUE > — priority queue number; possible values [0 .. 7] or all
- < DROP PRECEDENCE > — drop precedence value [0 .. 1] or all

Command mode

CONFIG – SWITCH

Example

```
cntrset sm-port 1/2 1 22 2 1
```

show cntrset

Use this command to view the queue collector information.

Syntax

show cntrset <SET>

Parameters

<SET> — counter number [0 .. 1].

Command mode

CONFIG – SWITCH

show qos

Use this command to view the assigned queue priorities. The queue priority equals 0 by default. Queue priority value is specified in the range of [0 .. 7]; queue with value 7 has the highest priority.

Syntax

show qos

Parameters

There are no parameters for this command.

Command mode

CONFIG – SWITCH

3.4.12 Configuration operation commands

SMG-2016 switch features 2 types of configuration:

- running-config — configuration that is currently active for the device.
- candidate-config — configuration with any pending changes; it will become 'running-config' after it is applied with the 'apply' command.

3.4.12.1 View configuration

running-config *viewing command*

Syntax

show running-config

Parameters

There are no parameters for this command.

Command mode

CONFIG – SWITCH

candidate-config *viewing command*

Syntax

show candidate-config

Parameters

There are no parameters for this command.

Command mode

CONFIG – SWITCH

3.4.12.2 Configuration application and confirmation commands

When the SMG-2016 switch configuration is completed, you should apply the configuration in order for it to become active on the device and confirm it in order to avoid the loss of access to the device due to these configuration edits. If you fail to confirm the configuration in 60 seconds, it will be rolled back to the previous running-config.

Configuration application command

Syntax

apply

Parameters

There are no parameters for this command.

Command mode

CONFIG – SWITCH

Confirmation command

Syntax

confirm

Parameters

There are no parameters for this command.

Command mode

CONFIG – SWITCH

3.4.13 Miscellaneous commands

config

Use this command to return to Configuration menu.

Syntax

config

Parameters

There are no parameters for this command.

Command mode

CONFIG – SWITCH

exit

Use this command to exit from this configuration submenu to the upper level.

Syntax

exit

Parameters

There are no parameters for this command.

Command mode

CONFIG – SWITCH

history

Use this command to view history of entered commands.

Syntax

history

Parameters

There are no parameters for this command.

Command mode

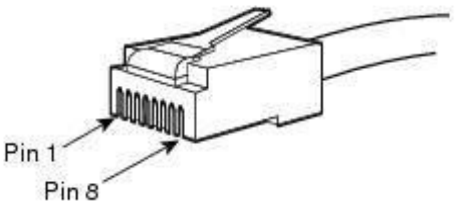
CONFIG – SWITCH

APPENDIX A. CABLE CONTACT PIN ASSIGNMENT

For SMG-2016

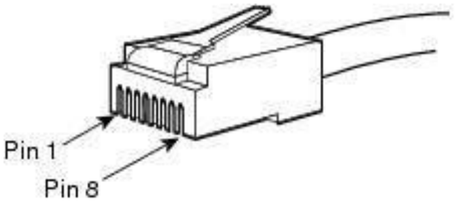
Assignment of the **RJ-48** connector pins for connection of ***E1 Line 0..15*** streams is ISO/IEC 10173 compliant and provided in the table below.

Table A1 — Assignment of **RJ-48** connector pins for E1 stream connection

Contact pin no. (Pin)	*Purpose*	*Contact pin numbering*
1	RCV from network (tip)	
2	RCV from network (ring)	
3	RCV shield	
4	XMT tip	
5	XMT ring	
6	XMT shield	
7	Not used	
8	Not used	

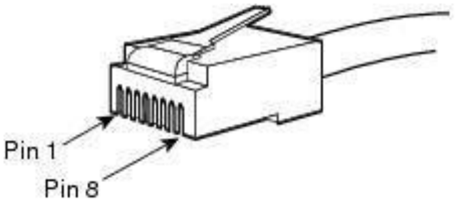
Assignment of the ***Console*** port **RJ-45** connector pins is provided in the table below.

Table A2 — Assignment of the console port **RJ-45** connector pins

Contact pin no. (Pin)	*Purpose*	*Contact pin numbering*
1	Not used	
2	Not used	
3	TX	
4	Not used	
5	GND	
6	RX	
7	Not used	
8	Not used	

Assignment of the **RJ-45** connector pins for external synchronization source ***Sync.0/Sync.1*** connection is provided in the table below.

Table A3 — Assignment of **RJ-45** connector pins for external synchronization source connection

Contact pin no. (Pin)	*Purpose*	*Contact pin numbering*
1	Sync A[1]	
2	Sync B[2]	
3	Not used	
4	Sync A	
5	Sync B	
6	Not used	
7	Not used	
8	Not used	

[1] Pins 1 and 4 are electrically interconnected inside the device

[2] Pins 2 and 5 are electrically interconnected inside the device

For SMG-1016M

E1 Line 0..7 ***E1 Line 8..15***

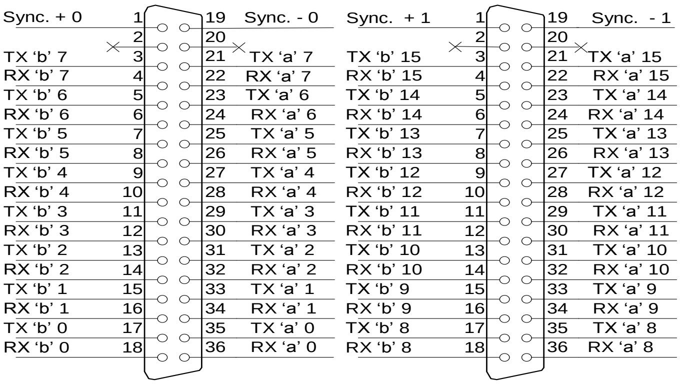

Sync. + 0 1 | 19 Sync. - 0
2 | 20
TX 'b' 7 3 | 21 TX 'a' 7
RX 'b' 7 4 | 22 RX 'a' 7
TX 'b' 6 5 | 23 TX 'a' 6
RX 'b' 6 6 | 24 RX 'a' 6
TX 'b' 5 7 | 25 TX 'a' 5
RX 'b' 5 8 | 26 RX 'a' 5
TX 'b' 4 9 | 27 TX 'a' 4
RX 'b' 4 10 | 28 RX 'a' 4
TX 'b' 3 11 | 29 TX 'a' 3
RX 'b' 3 12 | 30 RX 'a' 3
TX 'b' 2 13 | 31 TX 'a' 2
RX 'b' 2 14 | 32 RX 'a' 2
TX 'b' 1 15 | 33 TX 'a' 1
RX 'b' 1 16 | 34 RX 'a' 1
TX 'b' 0 17 | 35 TX 'a' 0
RX 'b' 0 18 | 36 RX 'a' 0
Sync. + 1 1 | 19 Sync. - 1
2 | 20
TX 'b' 15 3 | 21 TX 'a' 15
RX 'b' 15 4 | 22 RX 'a' 15
TX 'b' 14 5 | 23 TX 'a' 14
RX 'b' 14 6 | 24 RX 'a' 14
TX 'b' 13 7 | 25 TX 'a' 13
RX 'b' 13 8 | 26 RX 'a' 13
TX 'b' 12 9 | 27 TX 'a' 12
RX 'b' 12 10 | 28 RX 'a' 12
TX 'b' 11 11 | 29 TX 'a' 11
RX 'b' 11 12 | 30 RX 'a' 11
TX 'b' 10 13 | 31 TX 'a' 10
RX 'b' 10 14 | 32 RX 'a' 10
TX 'b' 9 15 | 33 TX 'a' 9
RX 'b' 9 16 | 34 RX 'a' 9
TX 'b' 8 17 | 35 TX 'a' 8
RX 'b' 8 18 | 36 RX 'a' 8

Fig. 38 — Assignment of *E1 Line* contact pins

RX contact pins are designed for the signal reception from the channel.

TX contact pins are designed for the signal transmission into the channel.

Sync contact pins are designed for the device synchronization with external sources (input impedance is 120Ω).

Console

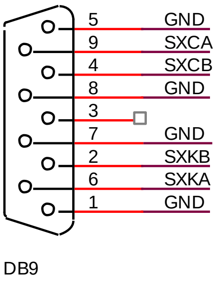


Fig. 39 — Assignment of *Console* port contact pins

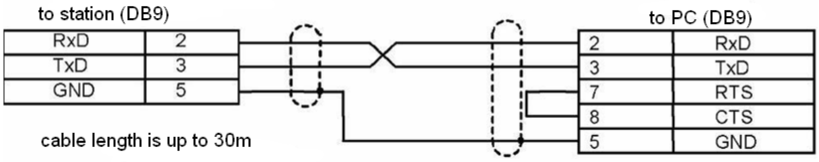


Fig. 40 — Cable wiring diagram for PORT1, PORT2 connection

Table A4 — E1 Line wire colour and terminal contact correspondence table (NENSHI NSPC-7019-18 cable)

Wire colour	***Terminal contact***	***Wire colour***	***Terminal contact***
White-blue	1	**Black-blue**	10

Blue	19	Blue	28
White-orange	2	**Black-orange**	11
Orange	20	Orange	29
White-green	3	**Black-green**	12
Green	21	Green	30
White-brown	4	**Black-brown**	13
Brown	22	Brown	31
Purple	5	**Yellow-blue**	14
Grey	23	Blue	32
Red-blue	6	**Yellow-orange**	15
Blue	24	Orange	33
Red-orange	7	**Yellow-green**	16
Orange	25	Green	34
Red-green	8	**Yellow-brown**	17
Green	26	Brown	35
Red-brown	9	**Yellow-grey**	18
Brown	27	Grey	36

Table A5 — E1 Line wire colour and terminal contact correspondence (HANDIAN UTP 18PR cable)

Wire colour	***Terminal contact***	***Wire colour***	***Terminal contact***
White-blue	1	**Red-grey**	10
Blue	19	Grey	28
White-orange	2	**Black-blue**	11
Orange	20	Blue	29
White-green	3	**Black-orange**	12
Green	21	Orange	30
White-brown	4	**Black-green**	13
Brown	22	Green	31
Purple-grey	5	**Black-brown**	14
Grey	23	Brown	32
Red-blue	6	**Black-grey**	15
Blue	24	Grey	33
Red-orange	7	**Yellow-blue**	16
Orange	25	Blue	34
Red-green	8	**Yellow-orange**	17
Green	26	Orange	35
Red-brown	9	**Yellow-green**	18
Brown	27	Green	36

APPENDIX B. ALTERNATIVE FIRMWARE UPDATE METHOD

I. Alternative device firmware update method using RS-232

When you cannot update the firmware via web configurator or the console (Telnet, SSH), you may use an alternative firmware update method via RS-232.

To update the device firmware, you will need the following programs:

- Terminal program (for example, TERATERM).
- TFTP server program.

Firmware update procedure:

1. Connect to Ethernet port of the device.
2. Connect PC COM port to the device console port using a crossed cable.
3. Run the terminal application.
4. Configure data rate: 115200, data format: 8bit w/o parity, 1 stop bit, w/o flow control:
5. Run *tftp* server program and specify the path to *smg_files* folder. In this folder, create *smg* subfolder, and place *SMG_kernel, SMG_initrd* files in it (computer that runs TFTP server and the device should be located in the same network.)
6. Turn the device on and stop the startup sequence by entering 'stop' command in the terminal program window:

```
U-Boot 2009.06 (Feb 09 2010 - 20:57:21)

CPU:   AMCC PowerPC 460GT Rev. A at 800 MHz (PLB=200, OPB=100, EBC=100 MHz)
       Security/Kasumi support
       Bootstrap Option B - Boot ROM Location EBC (16 bits)
       32 kB I-Cache 32 kB D-Cache
Board: SMG-1016Mv2 board, AMCC PPC460GT Glacier based, 2*PCIe, Rev. FF
I2C:   ready
DRAM:  512 MB
SDRAM test phase 1:
SDRAM test phase 2:
SDRAM test passed. Ok!
FLASH: 64 MB
NAND:  128 MiB
DTT:   1 FAILED INIT
Net:   ppc_4xx_eth0, ppc_4xx_eth1

Type run flash_nfs to mount root filesystem over NFS

Autobooting in 3 seconds, press 'stop' for stop
=>
```

7. Enter *set ipaddr* <device ip address><ENTER>

Example: `set ipaddr 192.168.2.2`

8. Enter *set netmask*<device network mask><ENTER>

Example: `set netmask 255.255.255.0`

9. Enter *set serverip* <IP address of a computer, that runs TFTP server><ENTER>

Example: `set serverip 192.168.2.5`

10. Enter mii si <ENTER> to activate the network interface:

```
=> mii si
Init switch 0: ..Ok!
Init switch 1: ..Ok!
Init phy 1: ..Ok!
Init phy 2: ..Ok!
=>
```

11. Update the Linux kernel using *run flash_kern* command:

```
=> run flash_kern
About preceeding transfer (eth0):
- Sent packet number 0
- Received packet number 0
- Handled packet number 0
ENET Speed is 1000 Mbps – FULL duplex connection (EMAC0)
Using ppc_4xx_eth0 device
TFTP from server 192.168.2.5; our IP address is 192.168.2.2
Filename 'smg/SMG_kernel'.
Load address: 0x400000
Loading: #################################################################
         ###################################
done
Bytes transferred = 1455525 (1635a5 hex)
Un-Protected 15 sectors

............... done
Erased 15 sectors
Copy to Flash... 9....8....7....6....5....4....3....2....1....done
=>
```

12. Update the file system using *run flash_initrd* command:

```
=> run flash_initrd
Using ppc_4xx_eth0 device
TFTP from server 192.168.2.5; our IP address is 192.168.2.2
Filename 'smg/SMG_initrd'.
Load address: 0x400000
Loading: #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         ####################
done
Bytes transferred = 25430113 (1840861 hex)
Erase Flash Sectors 56-183 in Bank # 2
Un-Protected 256 sectors
........................................................... done
Erased 256 sectors
Copy to Flash... 9....8....7....6....5....4....3....2....1....done
=>
```

13. Start up the device using 'run bootcmd' command.

II. Alternative device firmware update method using USB flash drive

When all other firmware update methods are unavailable, you may update the firmware using USB flash drive.

To update the device firmware using USB flash drive, you will need the following:

- USB flash drive.
- Terminal program (for example, TERATERM).

Firmware update procedure:

1. Copy the firmware file into the USB flash drive root directory.
2. Connect PC COM port to the device console port using a crossed cable or establish a connection with the device via Telnet/SSH protocol.
3. Run the terminal application.
4. Configure data rate: 115200, data format: 8bit w/o parity, 1 stop bit, w/o flow control (for connection via RS-232).
5. Turn the device on, wait until it boots up completely.
6. After the startup, connect in the terminal mode via Telnet/SSH or RS-323.
7. Enter the following command in CLI mode:

```
firmware update <file-name> usb
```

If CLI mode is not available, you may update in shell mode; to do this, enter in shell mode:

```
/usr/local/scripts/get_firmware <file-name> usb
```

where <file-name> is the firmware file name.

8. Wait until firmware update procedure is completed and restart the device.

APPENDIX C. EXAMPLES OF MODIFIER OPERATION AND DEVICE CONFIGURATION VIA CLI

Modifier operation examples

Objective 1:

In the *trunk group 0*, perform the following modification for outgoing dialling matching with the mask (1x{4,6}) — remove the first digit, replace it with 34, leave other digits as is.

Modification rule composition

This mask covers all 5-, 6- and 7-digit numbers beginning with 1. According to syntax, modification rule will be as follows: **'.+34xxxx??'** ('.' character at the first position — deletion of the first digit, '+34' — insert digits 34 after it, 'xxxx' — the next 4 digits will be always present and will not be modified, '??' — the last 2 digits may be missing for a 5-digit number, but if the number consists of 6 or 7 digits, one of the digits will be present at these positions and they will not be modified).

Utilized commands:

```
SMG>config// Enter the configuration mode
Entering configuration mode
SMG-[CONFIG]>new modifiers-table// Create a new modifier table
NEW 'MOD-TABLE' [07]: successfully created   // Table no.7 has been created
SMG-[CONFIG]>modifiers table7// Enter table no.7 configuration mode
Entering modifiers-table mode.
SMG-[CONFIG]-MODTABLE[7]>add(1x{4,6}) ".+34xxxx??"// Add number mask and modification rule
Mdifier. add
Modifier. Create: mask <(1x{4,6})>, cld-rule <.+34xxxx\?\?>, clg-rule <$>
NEW 'MODIFIER' [07]: successfully created
Modifier. Created with index [7].
'MODIFIER'    [07]:
                          table:             7
                          mask:              (1x{4,6})
                          numtype:           any
                          AONcat:            any
                          general-access:    no change
                          general-numplan:   no change

                          called-rule:       .+34xxxx??
                          called-type:       no change
                          called-numplan:    no change

                          calling-rule:      $
                          calling-type:      no change
                          calling-numplan:   no change
                          calling-present:   no change
                          calling-screen:    no change
                          calling-catAON:    no change
SMG-[CONFIG]-MODTABLE[7]>exit// Exit modifier table configuration mode
Back to configuration mode.
SMG-[CONFIG]>trunk0// Enter the trunk group configuration mode
Entering trunk-mode
SMG-[CONFIG]-TRUNK[0]>modifiers tableoutgoing called 7 // Add created modification table for CdPN
number modification in the outgoing communications
Trunk[0]. Set oModCld '7'
'TRUNK GROUP' [00]:
                         name:                TrunkGroup00
                         disable out:         no
                         disable in:          no
                         reserv trunk:        none
                         direct_pfx:          none
                         RADIUS-profile:      none
                         destination:         SIPT-Interface [3]
                         local:               no

                         Modifiers:
                           incoming calling:  none
                           incoming called:   none
                           outgoing calling:  none
                           outgoing called:   7
```

Objective 2:

In the *trunk group 0*, for the caller number received in the national format with area code 383, remove the area code and change the number type to *'subscriber'*.

Modification rule composition

Number in national format is 10-digit and begins with 383; given that values of the remaining 7 digits may vary, you should specify 'xxxxxxx' for them. Resulting mask is **(383xxxxxxx).** To remove the area code, i.e. the first 3 digits, remaining digits will be left unchanged, resulting modification rule as follows: '**...xxxxxxx**'. For category modification, use *change* command (in command example below, *add* command adds incoming modifier with the number 2, thus in *change* category modification command you should use modifier 2).

Utilized commands:

```
SMG>config// Enter the configuration mode
SMG-[CONFIG]>trunk 0// Enter the trunk group configuration mode
SMG-[CONFIG]-TRUNK[0]>modifiers // Enter the modifier configuration mode
SMG-[CONFIG]-TRUNK[0]-MODIFIER>addincoming calling(383xxxxxxx) "...xxxxxxx"
// Add caller number modification rule in the incoming communication
InModifier. Create: mask <(383xxxxxxx)>, rule <...xxxxxxx>
NEW 'TRUNK: IN-MODIFIER' [02]: successfully created
InModifier. Created with index [2].
'TRUNK: IN-MODIFIER' [02]:
                          trunk:          0
                          type:           calling
                          mask:           (383xxxxxxx)
                          rule:           ...xxxxxxx
                          calling-type:   no change
                          calling-pres:   no change
                          calling-scrn:   no change
                          calling-catAON: no change
SMG-[CONFIG]-TRUNK[0]-MODIFIER>change incoming clg_type 2 subscriber
// Change the caller number type in the modifier created by the previous command
'TRUNK: IN-MODIFIER' [02]:
                          trunk:          0
                          type:           calling
                          mask:           (383xxxxxxx)
                          rule:           ...xxxxxxx
                          calling-type:   subscriber
                          calling-pres:   no change
                          calling-scrn:   no change
                          calling-catAON: no change
```

CLI device configuration example

Objective:
Configure SS7-SIPT transit

Source data:
Stream from the opposite PBX is physically connected to the E1 stream 0 at the SMG connector.

SS7 signalling parameters:
- OPC=67;
- DPC=32;
- signalling channel SLC=1 in the channel interval 1;
- CIC numbering from 2 to 31 for channels from 2 to 31 respectively;

-channel engagement order — 'Sequential forward even' (respectively, to exclude the mutual channel engagement, the channel engagement order should be assigned on the opposite side, e.g. 'Sequential back odd').

SIP-T signalling parameters:
- IP address of the communicating gateway — 192.168.16.7
- UDP port for SIP-T signalling reception of the communicating gateway — 5060
- Quantity of simultaneously allowed sessions — 25
- Packetization time for G.711 codec — 30ms
- DTMF signal transmission performed during the established session according to RFC2833, payload type for RFC2833 packets — 101

Routing:
- Route to SS7 by trunk group 0
- Route to SIP-T by trunk group 1
- Transition to SS7 is performed by 7-digit numbers beginning from 6, 7, 91, 92, 93
- Transition to SIP-T is performed by 7-digit numbers beginning from 1, 2, 3
- All SS7 signalling messages are transferred by transit

Configuration via CLI:

SS7 signalling parameters configuration:

```
SMG>config // Enter the configuration mode
SMG-[CONFIG]>new linkset// Create a new link set
NEW 'LINKSET' [00]: successfully created
SMG-[CONFIG]>linkset0// Enter the linkset configuration mode
Entering Linkset-mode.
SMG-[CONFIG]-LINKSET[0]>chan_ordereven_successive_forward
// Select the channel engagement order — sequential forward even
Linkset[0]. Set chan_order '6'
SMG-[CONFIG]-LINKSET[0]>DPC32// Define destination point code
Linkset[0]. Set DPC '32'
SMG-[CONFIG]-LINKSET[0]>OPC67// Define the originating point code
Linkset[0]. Set OPC '67'
SMG-[CONFIG]-LINKSET[0]>init group-reset
// Select channel initialization mode during signalling channel establishment
Linkset[0]. Set init '7'
SMG-[CONFIG]-LINKSET[0]>net_ind national// Define the network identifier — local network
Linkset[0]. Set net_ind '3'
'LINKSET' [00]:

                      Name:        Linkset00
```

```
                       Trunk:        1
                       Access cat:   0
                       OPC:          67
                       DPC:          32
                       init:        'group reset'
                       china:        n
                       chan_order:  'even_successive_forward'
                       netw_ind:     national
                       satellite:    override_no_satellite
                       interwork:    no change
                       TMR:          speech
                       alarm ind:    no
                       CCI:          off
                       CCI_freq:     3
SMG-[CONFIG]-LINKSET[0]>exit// Exit the linkset configuration mode
Leaving Linkset mode
SMG-[CONFIG]>e10//Enter the E1 stream 0 configuration mode
Entering E1-stream mode
SMG-[CONFIG]-E1[0]>enabled// Put E1 stream into operation
E1[0]. Set line 'on'
SMG-[CONFIG]-E1[0]>signalingSS7// Select SS7 signalling protocol for a stream
E1[0]. Set Signaling 3
'E1: PHYS' [00]:
                          line          'on'
                          code          'hdb3'
                          eq            'off'
                          crc           'off'
                          sig           'SIG_SS7' (3)
                          alarm_ind     'off'
                          rem_alarm_ind 'off'
SMG-[CONFIG]-E1[0]>ss7// Enter the SS7 protocol configuration mode
E1[0]. Signaling is SS7
SMG-[CONFIG]-E1[0]-[SS7]>CIC fill0 1// Assign channel numbering from 0 in increments of 1
E1-SS7[0]. Fill CIC: start [0], step [1]
SMG-[CONFIG]-E1[0]-[SS7]>Dchan1// Select channel 1 as a signal channel
E1-SS7[0]. Set Dchan 1
SMG-[CONFIG]-E1[0]-[SS7]>SLC1// Assign code 1 for the created signalling channel
E1-SS7[0]. Set SLC 1
SMG-[CONFIG]-E1[0]-[SS7]>linkset0// Assign linkset 0 for a stream
E1-SS7[0]. Set Linkset 0
'E1: SS7' [00]:
           stream:     0
    linkset:     0
    SLC:         1


                       CICs:
                      00: --- | 01: -D- | 02: 002 | 03: 003 |
                      04: 004 | 05: 005 | 06: 006 | 07: 007 |
                      08: 008 | 09: 009 | 10: 010 | 11: 011 |
                      12: 012 | 13: 013 | 14: 014 | 15: 015 |
                      16: 016 | 17: 017 | 18: 018 | 19: 019 |
                      20: 020 | 21: 021 | 22: 022 | 23: 023 |
                      24: 024 | 25: 025 | 26: 026 | 27: 027 |
                      28: 028 | 29: 029 | 30: 030 | 31: 031 |
SMG-[CONFIG]-E1[0]-[SS7]>exit// Exit the SS7 protocol configuration mode
Leaving SS7-signaling mode
SMG-[CONFIG]-E1[0]>exit// Exit the E1 stream 0 configuration mode
Leaving E1-stream mode
```

SIP-T signalling parameters configuration (session continued):

```
SMG-[CONFIG]>new sipt-interface// Create a new SIP-T interface
NEW 'SIPT INTERFACE' [00]: successfully created
SMG-[CONFIG]>sip interface0// Enter the created SIP-T interface configuration mode
```

```
Entering SIPT-mode.
SMG-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[0]>ipaddr192.168.16.7
// Define IP address of the communicating gateway
SIPT-Interface[0]. Set ipaddr '192.168.16.7'
SMG-[CONFIG]-SIPT-INTERFACE[0]>port5060
// Define UDP port of the communicating gateway used for SIP signalling operation
SIPT-Interface[0]. Set port '5060'
SMG-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[0]>codec set0 G.711-a// Define the codec
SIPT-Interface[0]. Set codec '0'
SMG-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[0]>codec pte0 30// Define packetization time 30ms for G.711
codec
SIPT-Interface[0]. Set pte '30'
SMG-[CONFIG]-SIPT-INTERFACE[0]>max_active25// Define the quantity of simultaneous sessions
SIPT-Interface[0]. Set max_active '25'
SMG-[CONFIG]-SIPT-INTERFACE[0]>DTMF modeRFC2833
// Select DTMF – RFC2833 transmission method
SIPT-Interface[0]. Set DTMF_type '1'
SMG-[CONFIG]-SIPT-INTERFACE[0]>DTMF payload101// Select payload type 101 for RFC2833
SIPT-Interface[0]. Set DTMF_PT '101'
'SIP/SIPT INTERFACE' [00]:   id[00]
                          name:             SIP-interface00
                          mode:             SIP-T
                          trunk:            0
                          access category:  0
                          ip:port:          192.168.16.7:5060
                          login / password:   <not set> / <not set>

                          codecs:
                                 0 :
                                     codec:   G.711-A
                                     ptype:   8
                                     pte:     30

                          max active:       25

                          VAD/CNG:          no
                          Echo cancel:      voice (default)

                          DSCP RTP:         0
                          DSCP SIG:         0
                          RTCP period:      0
                          RTCP control:     0
                          RTP loss timeout: off

                          DTMF MODE:        RFC2833
                          DTMF PType:       101
                          DTMF MIMETYPE:    application/dtmf


                          CCI:              off
                          Redirect (302):   disabled
                          REFER:            disabled
                          Session Expires:  1800
                          Min SE:           90
                          Refresher:        uac
                          Rport:            disabled
                          Options:          disabled:0

                          FAX-detect:       no detecting
                          FAX-mode:         none

                          VBD:              disabled

                          Jitter buffer adaptive mode
                            minimum size:          0 ms
                            initial size:          0 ms
                            maximum size:          200 ms
```

```
                                deletion mode:          soft
                                deletion threshold:     500 ms
                                adaptation period:      10000 ms
                                adjustment mode:        non-immediate
                                size for VBD:           0

SMG-[CONFIG]-SIPT-INTERFACE[0]>exit// Exit the SIP-T interface configuration mode
Leaving SIPT mode
```

Routing configuration (session continued):

```
SMG-[CONFIG]>new trunk// Create the trunk group for SS7 link set
NEW 'TRUNK GROUP' [00]: successfully created
SMG-[CONFIG]>new trunk// Create the trunk group for operation via SIP-T interface
NEW 'TRUNK GROUP' [01]: successfully created
SMG-[CONFIG]>new prefix// Create the prefix for transition to SS7 direction
NEW 'PREFIX' [00]: successfully created
SMG-[CONFIG]>new prefix// Create the prefix for transition to SIP-T direction
NEW 'PREFIX' [01]: successfully created
SMG-[CONFIG]>trunk0// Enter the trunk group configuration mode for SS7 link set
Entering trunk-mode
SMG-[CONFIG]-TRUNK[0]>destinationSS7 0// Associate the trunk group 0 with SS7 link set 0
Trunk[0]. Set destination '2'
Trunk[0]. Same destination
'TRUNK GROUP' [00]:
                         name:           TrunkGroup00
                         disable out:    no
                         disable in:     no
                         reserv trunk:   none
                         direct_pfx:     none
                         RADIUS-profile: none
                         destination:    Linkset [0]
SMG-[CONFIG]-TRUNK[0]>exit
// Exit the trunk group configuration mode for SS7 link set
Leaving TRUNK mode
SMG-[CONFIG]>trunk1// Enter the trunk group configuration mode for SIP-T interface
Entering trunk-mode
SMG-[CONFIG]-TRUNK[1]>destinationSIPT 0
// Associate trunk group 1 with SIP-T interface 0
Trunk[1]. Set destination '3'
Trunk[1]. Same destination
'TRUNK GROUP' [01]:
                          name:          TrunkGroup01
                         disable out:    no
                         disable in:     no
                         reserv trunk:   none
                         direct_pfx:     none
                         RADIUS-profile: none
                         destination:    SIPT-Interface [0]
SMG-[CONFIG]-TRUNK[1]>exit
// Exit the trunk group configuration mode for SIP-T interface
Leaving TRUNK mode
SMG-[CONFIG]>prefix0
// Enter the prefix configuration mode for transition to trunk group 0
Entering Prefix-mode
SMG-[CONFIG]-PREFIX[0]>typetrunk// Define the prefix type — 'transition to trunk group'
Prefix[0]. Set type '1'
SMG-[CONFIG]-PREFIX[0]>trunk0// Define the transition to the trunk group 0 by prefix
Prefix[0]. Set idx '0'
SMG-[CONFIG]-PREFIX[0]>mask edit
// Enter the dialling mask editing and caller number analysis mode
Entering Prefix-Mask mode
SMG-[CONFIG]-PREFIX[0]-MASK>add ([67]xxxxxx|9[1-3]xxxxx)
```

// Add dialling mask according to the objective

```
PrefixMask. add
NEW 'PREFIX-MASK' [00]: successfully created
PrefixMask. Created with index [00].
'PREFIX-MASK' [00]:
                          mask:         ([67]xxxxxx|9[1-3]xxxxx)
                          prefix:       0
                          type:         called
                          Ltimer:       10
                          Stimer:       5
                          Duration:     30
SMG-[CONFIG]-PREFIX[0]-MASK>exit
```

// Exit the dialling mask editing and caller number analysis mode

```
Leaving Prefix-Mask mode
SMG-[CONFIG]-PREFIX[0]>called transit
```

// Define the transit for caller number type

```
Prefix[0]. Set called '5'
'PREFIX' [00]:
                            type:          'to trunk'
                            idx:            1
                            access cat:     0 [no check]
                            direction:     'local'
                            called type:   'transit'
                            getCID:         n
                            needCID:        n
                            dial_mode:      enblock
                            priority:       100
                            Stimer:         5
                            duration:       30
         Mask for prefix [00]:
                           [000]  -    ([67]xxxxxx|9[1-3]xxxxx)  [called]
                              Ltimer:   10
                              Stimer:   5
                              Duration: 30
SMG-[CONFIG]-PREFIX[0]>exit// Exit the prefix configuration mode
Leaving Prefix mode
SMG-[CONFIG]>prefix1
```

// Enter the prefix configuration mode for transition to trunk group 1

```
 Entering Prefix-mode
SMG-[CONFIG]-PREFIX[1]>type trunk// Define the prefix type — 'transition to trunk group'
Prefix[1]. Set type '1'
SMG-[CONFIG]-PREFIX[1]>trunk1// Define the transition to the trunk group 1 by prefix
Prefix[1]. Set idx '1'
SMG-[CONFIG]-PREFIX[1]>mask edit// Enter the dialling mask editing and caller number analysis mode
Entering Prefix-Mask mode
SMG-[CONFIG]-PREFIX[1]-MASK>add ([1-3]xxxxxx)
```

// Add dialling mask according to the objective

```
PrefixMask. add
NEW 'PREFIX-MASK' [01]: successfully created
PrefixMask. Created with index [01].
'PREFIX-MASK' [01]:
                          mask:         ([1-3]xxxxxx)
                          prefix:       1
                          type:         called
                          Ltimer:       10
                          Stimer:       5
                          Duration:     30
SMG-[CONFIG]-PREFIX[1]-MASK>exit// Exit the dialling mask editing and caller number analysis mode
Leaving Prefix-Mask mode
SMG-[CONFIG]-PREFIX[1]>calledtransit// Define the transit for caller number type
Prefix[1]. Set called '5'
'PREFIX' [01]:
                            type:          'to trunk'
                            idx:            1
                          access cat:    0  [no check]
                          direction:    'local'
                          called type:  'transit'
                          getCID:        n
                          needCID:       n
                          dial_mode:     enblock
                          priority:      100
                          Stimer:        5
                          duration:      30
         Mask for prefix [01]:
                         [001]  -    ([1-3]xxxxxx)  [called]
                            Ltimer:   10
                            Stimer:   5
                            Duration: 30
SMG-[CONFIG]-PREFIX[1]>exit// Exit the prefix configuration mode
Leaving Prefix mode
SMG-[CONFIG]>exit
Leaving configuration mode.
```

Saving configuration and device restart (session continued):

```
SMG>save// Save configuration
tar: removing leading '/' from member names
**********
*****Saved successful
SMG>rebootyes// Restart device
```

APPENDIX D. TRANSMISSION OF VAS SETTINGS FROM RADIUS SERVER FOR DYNAMIC SUBSCRIBERS.

The gateway allows to configure VAS settings to dynamic subscribers using the RADIUS server commands sent in response to RADIUS-Authorization requests during registration. Commands are transferred in the text format using Vendor-Specific attribute (see Section 3.1.15.3) with vendor number assigned to Eltex and equal to 35265 and Eltex-AVPair attribute name with the number 1.

In general, Eltex-AVPair attribute format will be as follows:

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1):<$COMMAND-STRING>
```

By transferring various commands in $COMMAND-STRING, you may send the following parameters:

- Enable/disable VAS for dynamic subscribers
- Settings for activated services (redirection numbers, BLF subscribers count)
- Disable all VAS for a subscriber

Request syntax

Command consists of the initial text identifier of a command, VAS activation/deactivation identifier for VAS configuration and configuration commands.

- 'UserService:' is a text identifier defining that this attribute contains the VAS management command.
- 'CFU=', 'CFB=', 'CFNR=', 'CFOS=', 'CT=', 'CallPickup=', 'BLF=', 'Intercom=', 'Conf=', '3PTY=', 'ClearAll=' — VAS activation/deactivation indicator, may take up values 'yes' or 'no', enables or disables VAS respectively.
  - CFU — call forward unconditional
  - CFB — call forward on busy
  - CFNR — call forward on no reply
  - CFOOS — call forward on out of service
  - CT — call transfer
  - CallPickup — call pickup
  - BLF — busy lamp field (BLF)
  - Intercom — access to intercom and paging calls
  - Conf – conference connection, add-on;
  - 3PTY – 3-way conference;
  - ClearAll – cancel all services.
- 'numCFU=', 'numCFB=', 'numCFNR=', 'numCFOS=' — *'Call forward'* VAS configuration command; subscriber's listed directory phone number used for call forwarding may be passed as a value.
- 'limitBLF=' — *'Busy lamp field (BLF)'* VAS configuration command; quantity of subscribers may be passed as a value.
- 'CT=', 'CallPickup=', 'Intercom=', 'Conf=', '3PTY=', 'ClearAll=' — does not feature any additional settings.
- 'UserService:none' — command that allows to disable VAS for a subscriber.

If the subscriber has VAS services active, i.e. the VAS activation/deactivation indicator with 'yes' value has been passed, pass 'no' value for this subscriber in order to disable this service. If after VAS activation there was no information transmitted on the activated VAS in the subsequent RADIUS server messages, the service is considered to be active until 'no' parameter is transmitted.

If some VAS were activated for the subscriber and it became inactive later (device registration timeout has expired), its VAS are considered to be active until 'UserService:none' parameter is transmitted for the current subscriber.

After the device reboot, VAS activated for the subscriber remain active.

Service activation examples

Objective 1

Activate *'Call forward unconditional'* to 12345, *'Call forward on no reply'* to 56789 and *'Call pickup'* service for a subscriber.

Actions

You should pass the following request:

```
UserService:CFU=yes;numCFU=12345;CFNR=yes;numCFNF=56789;CallPickup=yes"
```

Objective 2

Deactivate *'Call forward unconditional'* and *'Call pickup'* services, and activate *'BLF for 10 subscribers'* and *'Call transfer'* services for a subscriber.

Actions

You should pass the following request:

```
UserService:CFU=no;CallPickup=no;CT=yes;BLF=yes;limitBLF=10;
```

APPENDIX E. ROUTING, SUBSCRIBERS AND SIGNAL LINK PARAMETERS CORRELATION

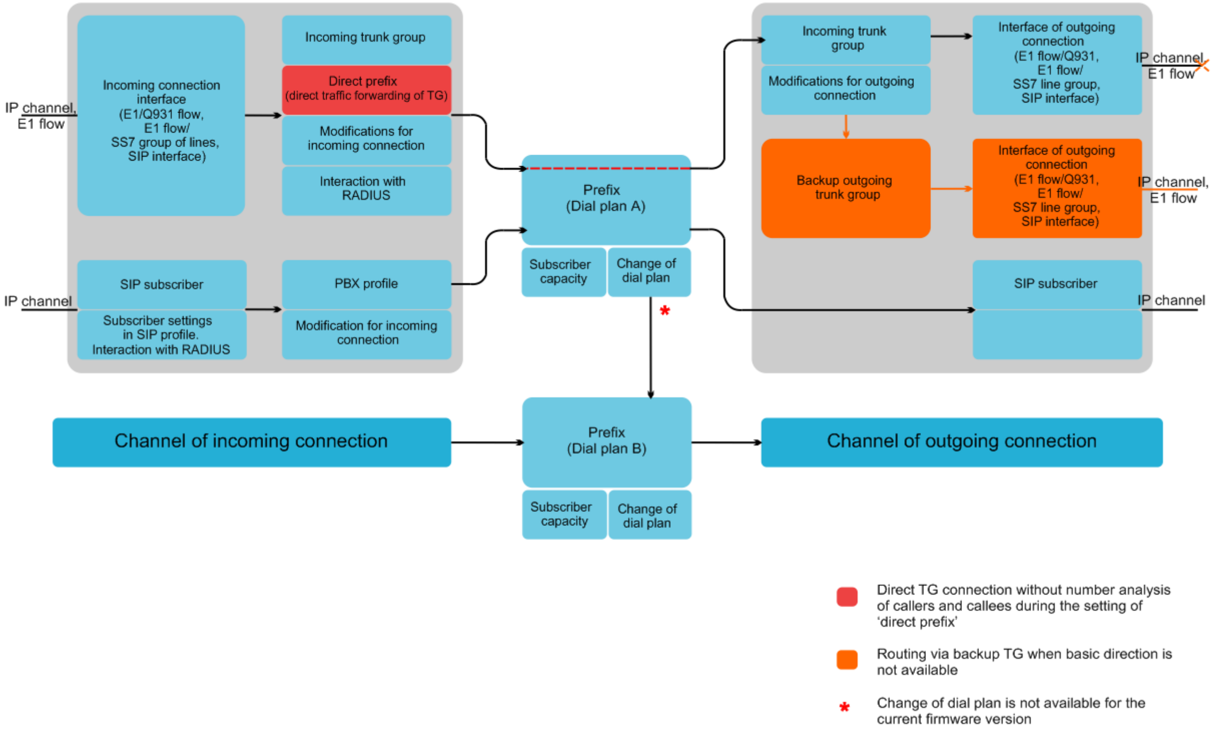

IP channel,
E1 flow
Incoming connection interface (E1/Q931 flow, E1 flow/ SS7 group of lines, SIP interface)
Incoming trunk group
Direct prefix (direct traffic forwarding of TG)
Modifications for incoming connection
Interaction with RADIUS
IP channel
SIP subscriber
Subscriber settings in SIP profile. Interaction with RADIUS
PBX profile
Modification for incoming connection
Prefix (Dial plan A)
Subscriber capacity
Change of dial plan
*
Incoming trunk group
Modifications for outgoing connection
Interface of outgoing connection (E1 flow/Q931, E1 flow/ SS7 line group, SIP interface)
IP channel,
E1 flow
Backup outgoing trunk group
Interface of outgoing connection (E1 flow/Q931, E1 flow/ SS7 line group, SIP interface)
IP channel,
E1 flow
SIP subscriber
IP channel
Channel of incoming connection
Prefix (Dial plan B)
Subscriber capacity
Change of dial plan
Channel of outgoing connection
🟥 Direct TG connection without number analysis of callers and callees during the setting of 'direct prefix'
🟧 Routing via backup TG when basic direction is not available
* Change of dial plan is not available for the current firmware version

Fig. 41 — Routing, subscribers and signal link parameters correlation

Incoming call from IP or TDM channel arrives to the incoming interface, then the further call routing is determined in the trunk group (TG) using 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 SIP subscriber. If the 'direct prefix' is configured in the incoming TG, the call is routed into 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 direction in not available, the call will be directed to the backup direction (if configured).

Incoming call from SIP subscriber arrives to the incoming SIP interface (SIP profile), then the further call routing is determined in the profile using RADIUS protocol (if applicable). Call is routed by prefix into the outgoing channel or to 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 direction in not available, the call will be directed to the backup direction (provided that such direction has been configured).

For SMG gateway numbering capacity definition, 'numbering capacity' modifier is used for the prefix. These numbers will belong to the gateway, although they are may not be assigned to subscribers.

APPENDIX F. GUIDELINES FOR SMG OPERATION IN PUBLIC NETWORK

During SMG operation in a public network, you should take all security measures in order to avoid the device password brute forcing, DoS (DDoS) attacks and other intrusive actions that may lead to unstable operation, subscriber data theft, attempts to perform calls at the expense of other subscribers and consequently to damages to the service provider as well as subscribers.

Avoid using SMG in a public network without additional protective measures like session border controller (SBC), firewall, etc.

Guidelines for SMG operation in public network:

- Operation in a public network with default SIP signalling port 5060 is not recommended. To change this parameter, modify the 'Port for SIP signalling reception' parameter value in 'SIP interfaces' settings for general SIP configuration and SIP interface settings[1]. This setting will not ensure the complete protection as the signalling port may be discovered during port scanning.
- If IP addresses of all devices communicating with SMG are known, use the embedded firewall (static firewall) to configure the allowing rules for them and deny the access from all the other addresses. Allowing rules should be placed first in the rule list.
- Also, you should configure dynamic firewall.

Dynamic firewall stores unsuccessful SIP protocol access attempts in a log file (/tmp/log/pbx_sip_bun.log) and if the amount of such attempts exceeds the defined value, the IP address that has originated them will be banned for the specified time. This utility also allows to create lists of trusted and untrusted addresses. For detailed description, see Section 3.1.13.2 Dynamic firewall.

[1] This function is available in version RC14 and later

APPENDIX G. MONITORING SYSTEM INTERACTIONS

To establish the device fault monitoring in real time, you should configure the monitoring system.

Absence of faults means normal operation; when the fault event occurs, the normal state turns to alarm state, when all the current faults are resolved, the normal operation state will be restored.

Possible device status indications:

- Front panel light indication — *Alarm* LED (for *Alarm* LED indication, see Section 1.6)
- Indication of the most critical failure in the web configurator header (see operation log for more details)
- Transmission of the fault information to the monitoring system via SNMP protocol (trap, inform)

Events for the fault state generation are subdivided into unconditional and optional:

- *Unconditional* — faults with non-configurable indication; they include:
  - *CONFIG* — critical fault, configuration file fault
  - *SIPT-MODULE* — critical fault, failure of a software module responsible for VoIP operation
  - *SM-VP DEVICE* — fault, SM-VP IP submodule failure
  - *SYNC* — fault indicating that synchronization source is missing or a warning indicating that synchronization is performed with the low-priority synchronization source.
  - *CDR-FTP* — critical fault or warning indicating the error during CDR data transfer to FTP server; fault level is determined by the amount of CDR data awaiting transfer to server.
  - *PM-POWER-STATE* — warning indicating the output power loss for one of the power supplies installed.
- *Optional* — faults with configurable indication; they include:
  - *STREAM* — critical fault, E1 stream is in operation
  - *STREAM-REMOTE* — warning, E1 stream remote fault
  - *STREAM-SLIP* — warning, there are SLIPs in the stream
  - These faults are configured in the E1 stream physical parameter configuration (see Section 3.1.5.2)
  - *LINKSET* — critical fault, SS7 link set is not in operation
  - *SS7LINK* — SS7 signal channel failure
  - *TRUNK-CPS* — permitted number of calls per second is exceeded for a trunk group

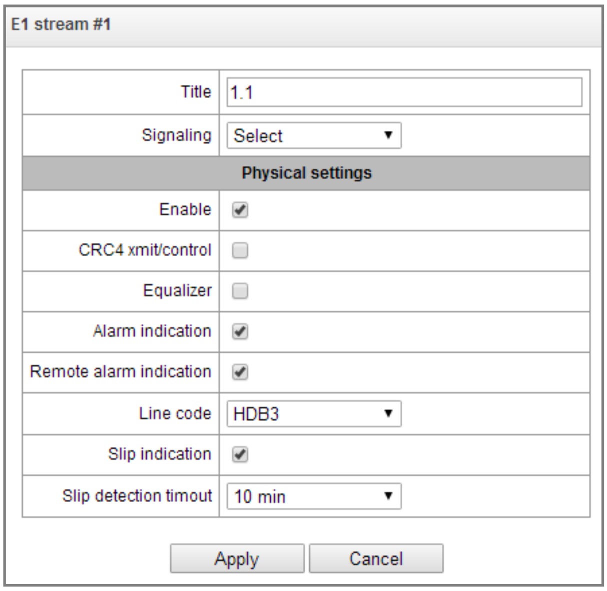
  These alarms are configured in SS7 link set configuration (Section 3.1.7.2).

By default, optional fault indication is disabled, i.e. for monitoring systems interactions, you should configure fault indication for all E1 streams and SS7 link sets put in operation.

For interactions with the monitoring system via SNMP, you should enable SNMP on the device and configure SNMP TRAP or INFORM message transmission to the monitoring server IP address.

Parameter configuration via web configurator

1) Optional fault indication configuration for E1 stream configuration (*'E1 stream/Physical parameters'* menu, see Section 3.1.5.2 Configuration of physical parameters).



E1 stream #1

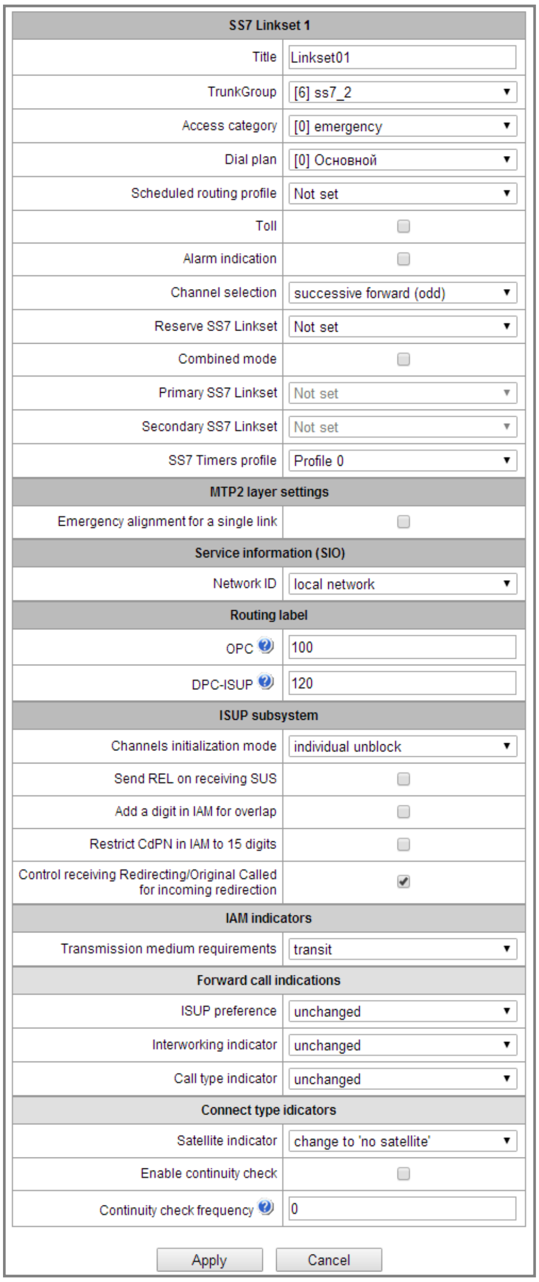
Title	1.1
Signaling	Select ▾
Physical settings	
Enable	☑
CRC4 xmit/control	□
Equalizer	□
Alarm indication	☑
Remote alarm indication	☑
Line code	HDB3 ▾
Slip indication	☑
Slip detection timout	10 min ▾

For LOS and AIS fault indication, select the *'Alarm indication'* checkbox for the E1 stream.

For RAI fault indication, select the *'Remote alarm indication'* checkbox.

For slips indication for a stream, select *'SLIP indication'* checkbox and configure SLIP detection timer.

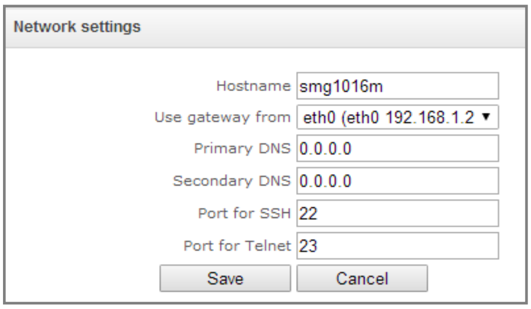
2) Optional fault indication configuration for SS7 link set configuration (*'E1 streams/SS7 linkset'*, see Section 3.1.5.4).



SS7 Linkset 1	
Title	Linkset01
TrunkGroup	[6] ss7_2 ▼
Access category	[0] emergency ▼
Dial plan	[0] Основной ▼
Scheduled routing profile	Not set ▼
Toll	□
Alarm indication	□
Channel selection	successive forward (odd) ▼
Reserve SS7 Linkset	Not set ▼
Combined mode	□
Primary SS7 Linkset	Not set ▼
Secondary SS7 Linkset	Not set ▼
SS7 Timers profile	Profile 0 ▼
MTP2 layer settings	
Emergency alignment for a single link	□
Service information (SIO)	
Network ID	local network ▼
Routing label	
OPC	100
DPC-ISUP	120
ISUP subsystem	
Channels initialization mode	individual unblock ▼
Send REL on receiving SUS	□
Add a digit in IAM for overlap	□
Restrict CdPN in IAM to 15 digits	□
Control receiving Redirecting/Original Called for incoming redirection	☑
IAM indicators	
Transmission medium requirements	transit ▼
Forward call indications	
ISUP preference	unchanged ▼
Interworking indicator	unchanged ▼
Call type indicator	unchanged ▼
Connect type idicators	
Satellite indicator	change to 'no satellite' ▼
Enable continuity check	□
Continuity check frequency	0

For SS7 signal link fault indication, select the *'Fault indication'* flag.

3) To enable SNMP, go to *'TCP settings/IP/Network parameters'* menu (Section 3.1.10.2 Network Settings*).*

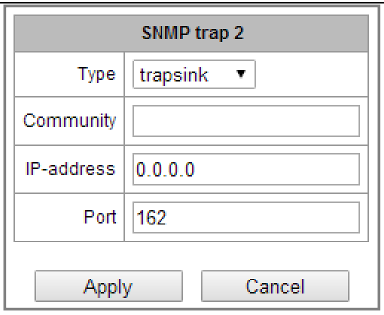


Network settings

Hostname	smg1016m
Use gateway from	eth0 (eth0 192.168.1.2 ▼
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Port for SSH	22
Port for Telnet	23

To perform the configuration, select the *'Enable SNMP'* checkbox.

4) For SNMP trap output, go to *'Network services/SNMP'* menu (Section 3.1.11.2 SNMP settings).



SNMP trap 2

Type	trapsink ▼
Community	
IP-address	0.0.0.0
Port	162

To perform the configuration, specify SNMP message type (TRAPv1, TRAPv2, INFORM), password (Community), IP address and SNMP trap recipient port.

When configuration is set up and applied, restart SNMP agent by clicking *'Restart SNMPd'* button.

APPENDIX H. VOICE MESSAGES AND MUSIC ON HOLD (MOH)

By default, the device features pre-recorded voice message phrases and music to be played on hold. Message playback corresponds to a specific event; the table below contains the list of messages and their correspondence to events.

Table I1 — MOH messages and events

Name	*Meaning*	*Event*
TRUNK_BUSY	'Direction is overloaded'	No free channels for outgoing direction. Outgoing channels are blocked or inoperable. When Q.850 cause = 34 is received
NUMBER_FAIL	'Invalid number is dialled'	When non-existent prefix is dialled When Q.850 cause =3, 28 are received
ACCS_DENIED_TEMP	'Number is temporarily unavailable'	When unregistered subscriber is dialled When Q.850 cause = 27 is received
ACCESS_RESTRICT	'This type of communication is missing from the service list for your phone unit'	Incoming communication restriction for a subscriber Call restriction by access categories When Q.850 cause = 21 is received
USER_UNALLOCATED	'Subscriber unit is not connected to PBX'	For calls to 'modifier' type prefix When Q.850 cause = 1 is received
USER_CHANGE	'Subscriber has switched the number'	When Q.850 cause = 22 is received
MOH	Music on hold	When subscriber has been put on hold

Voice message playback management is located in the trunk group configuration and PBX profile settings for subscribers.

MOH message playback is unconditional and does not depend on the settings.

APPENDIX I. WORKING WITH VAS SERVICES

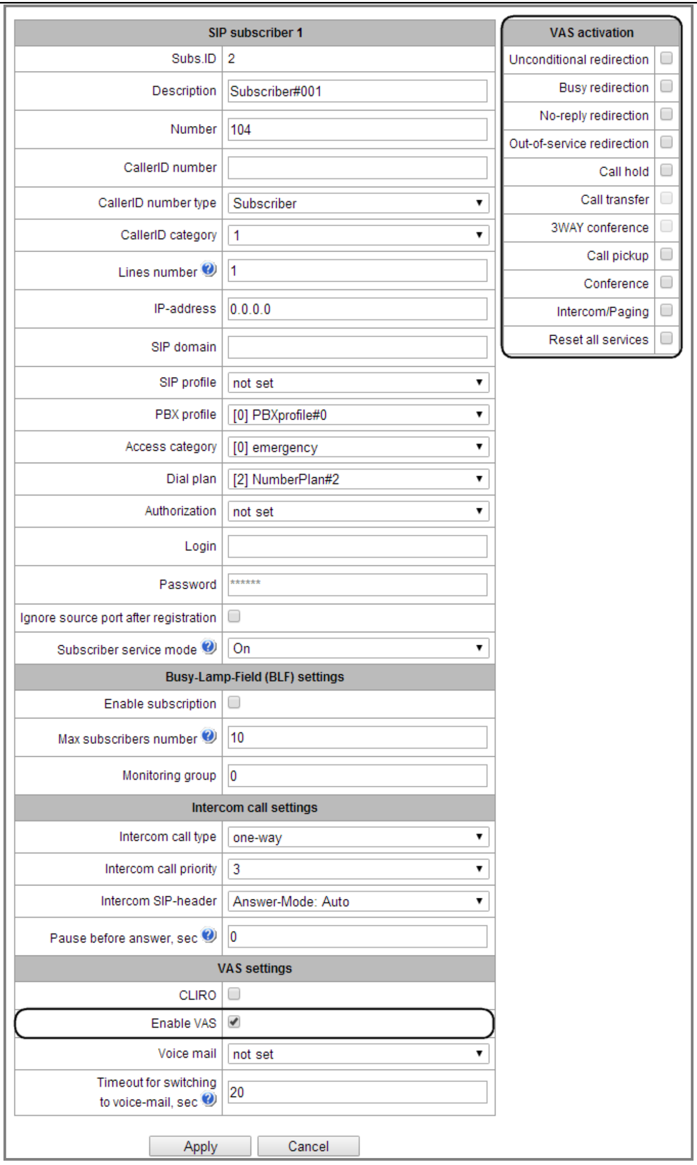
Beginning from the firmware version 2.15.01, the device features the following VAS:

- Call forward unconditional — activate call forward unconditional service (CF Unconditional).
- Call forward on busy — activate call forward on busy service (CF Busy).
- Call forward on no reply — activate call forward on no reply service (CF No reply).
- Call forward on out of service — activate call forward on out of service (CF Out Of Service).
- Call hold (Call hold).
- Call transfer — activate call transfer service (Call Transfer).
- Three-way conference (3Way). Call pickup (Call pickup).
- Conference with consequent assembly (CONF).
- *Disable conference when an initiator leaves the conference* – when checked, the conference will be disabled when an initiator leaves the conference. Otherwise, the conference will be saved even when the initiator leaves and will be over only when all the participants leave.
- Intercom call — call service with the Subscriber B automatic reply.
- Paging call — service is similar to Intercom but with a call performed to the conference number.
- Password change (PWD);
- Out calls restriction;
- Egress connection via password (PWD ACT);
- Password activation (RBP);
- Do not disturb (only for SMG-2016);
- Black list (only for SMG-2016);
- Reset all services.

VAS functionality becomes available only when additional SMG-VAS license is installed.

For VAS utilization by a subscriber, select the *'Enable VAS'* checkbox in the subscriber settings.

To activate a specific VAS, select the checkbox next to the required service in the 'VAS activation' menu of the subscriber settings.



SIP subscriber 1	
Subs.ID	2
Description	Subscriber#001
Number	104
CallerID number	
CallerID number type	Subscriber
CallerID category	1
Lines number	1
IP-address	0.0.0.0
SIP domain	
SIP profile	not set
PBX profile	[0] PBXprofile#0
Access category	[0] emergency
Dial plan	[2] NumberPlan#2
Authorization	not set
Login	
Password	******
Ignore source port after registration	☐
Subscriber service mode	On
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	☑
Voice mail	not set
Timeout for switching to voice-mail, sec	20

VAS activation	
Unconditional redirection	☐
Busy redirection	☐
No-reply redirection	☐
Out-of-service redirection	☐
Call hold	☐
Call transfer	☐
3WAY conference	☐
Call pickup	☐
Conference	☐
Intercom/Paging	☐
Reset all services	☐

1. Working with 'Call hold', 'Call transfer', 'Three-way conference' services

'Call transfer' service operation requires that the subscriber terminal party supports FLASH transmission via SIP using SIP-INFO, RFC2833 methods. Also, the subscriber terminal party should have an inband, SIP-INFO or RFC2833 DTMF signal transmission methods configured; make sure that the similar method is selected in the subscriber SIP profile configuration.

'Call transfer' service configuration example

Subscriber A calls Subscriber B; Subscriber B may press FLASH during conversation to put the Subscriber A on hold, at that time, 'Music on hold' will be played to the subscriber A, and Subscriber B will hear 'PBX response' tone; at that, timeouts for dialling the Subscriber C number will be activated, their values are provided below. After the number dial and Subscriber C reply, the options are as follows:

While being in a call state with a Subscriber A, put him on hold with hook flash (R), wait for 'PBX response' tone and dial a Subscriber C number. When Subscriber C answers, the following operations will be possible:

- R 0 — disconnect a subscriber on hold, connect to online subscriber.
- R 1 — disconnect an online subscriber, connect to subscriber on hold.
- R 2 — switch to another subscriber (change a subscriber).

- R 3 — three-way conference.
- R 4 — call transfer. Voice connection will be established between Subscribers A and C.
- Hangup — call transfer; voice connection will be established between Subscribers A and C.

'Call transfer' service timeouts — at the moment, these timeouts are at their default values; their configuration will be implemented in future firmware versions.

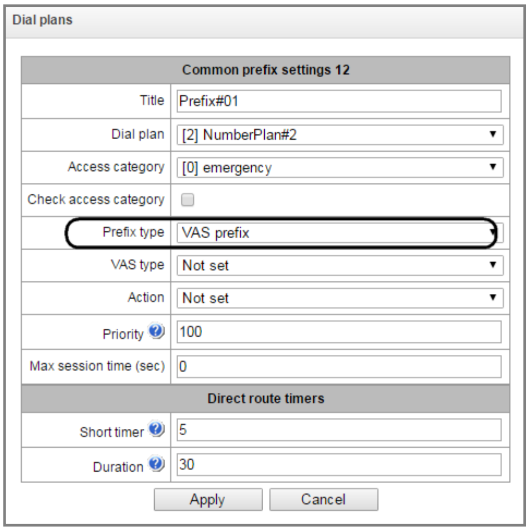
- First digit dial timeout: 15 seconds
- Next digit dial timeout: 5 seconds
- Busy tone timeout: 60 seconds

2. Working with 'Redirection' service

'Redirection' service configuration may be performed using the corresponding setting in *'SIP subscribers'/'VAS management'/'Required subscriber selection'* menu of the web configurator (Section 3.1.18.1.2) or using VAS management from the phone unit (according to RD-45), this method is described below.

VAS configuration from the phone unit (according to GOST 45.49-96)

The subscriber may activate or deactivate the service themselves by dialling specific prefixes on their phone unit. Redirection service prefixes are configured in the dial plan (3.1.6 Dial plans) add a new prefix with the *'Prefix type'/'VAS prefix'* value.



Dial plans

Common prefix settings 12	
Title	Prefix#01
Dial plan	[2] NumberPlan#2
Access category	[0] emergency
Check access category	□
Prefix type	VAS prefix
VAS type	Not set
Action	Not set
Priority	100
Max session time (sec)	0
Direct route timers	
Short timer	5
Duration	30

For VAS, we recommend to use the following prefix values:

Call forward unconditional (CF Unconditional):

- Activation (*21*|*21*x.#);
- Deactivation (#21#);
- Control (*#21*|*#21*x.#).

Call forward on busy (CF Busy):

- Activation (*22*|*22*x.#);

- Deactivation (#22#);
- Control (*#22*|*#22*x.#).

Call forward on no reply (CF No reply):

- Activation (*61*|*61*x.#);
- Deactivation (#61#);
- Control (*#61*|*#61*x.#).

Call forward on 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 arbitrary value; these examples feature recommended values.

✓ **In the subscriber terminal dial plan, you should define VAS management prefixes. Operation with VAS at the gateway is performed after reception of the INVITE message with the required combination of digits from the subscriber terminal.**

'Call transfer' service timeouts are at their default values at the moment; their configuration will be implemented in future firmware versions:

- Call forward on no reply (CF No reply) timeout: 10 seconds
- Call forward on out of service (CF Out Of Service) timeout: 10 seconds

Example of VAS configuration from the phone unit

Objective

Subscriber should configure call forward unconditional to the number 222333444.

Actions

1. To activate the service, the subscriber should dial *21* and hear the 'PBX response' tone in response.
2. To check the service activation, the subscriber should dial *#21*. If the service is active, the subscriber will hear the 'PBX response' tone. If the service is inactive, the subscriber will hear the 'busy' tone.
3. To define the forwarding number, the subscriber should dial *21*222333444# and hear the 'PBX response' tone.
4. To check whether the service has been activated for the specific number, the subscriber should dial *#21*222333444#. If the service is active and the dialled number matches the previously defined number, the subscriber will hear the 'PBX response' tone. If the service is inactive or the dialled number does not match the previously defined number, the subscriber will hear the 'busy' tone.

   To deactivate the service, the subscriber should dial #21#.

3. Conference with consequent participant assembly (Conference Add-on)

This service allows the initiator to establish the conference by consequently adding participants using subscriber hold feature.

Upon the initiator hanging up, participants will hear the busy tone. The maximum number of conference participants for SMG-1016M – 30, for SMG-2016 – 120.

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 — hook flash (FLASH).

4. Call pickup

This service allows to answer the call directed to another subscriber.
Access to service is governed by the 'Call pickup' VAS category checkbox.

Usage	* 66 *<NUMBER>#

where:

<NUMBER> — number of the subscriber for call pickup.

5. Intercom and paging calls

This service allows the subscriber to perform the call with automatic phone unit response at the call party B. Note, that utilized phone units should support Answer-Mode: Auto for RFC 5373.

Access to service is governed by the 'Intercom call' VAS category checkbox.

Usage	*80*<NUMBER>#

where:

<NUMBER> — number of the intercom call subscriber.

Paging call service operates in the similar way to the intercom call but it enables calls to subscriber groups using the conference number. For that, define the call group with the conference number in call group section (Section 3.1.8.9) and add all subscribers using this service into it.

Usage	*81*<NUMBER>#

<NUMBER> — conference number of the paging call.

6. Activation/deactivation of a password, egress communication via password

These services provide the opportunity to override restrictions on access to outgoing calls (restriction set by outgoing calls restriction service).

For example, if outgoing communication is limited by "outgoing calls restriction", the "restricted by password" service gives an opportunity to inactivate restrictions only for the next outgoing connection establishment. "Activation/deactivation of a password" disable/enable restrictions on outgoing communication for the next outgoing connection establishment.

The access to the service is managed by checking the "Password activation" box in VAS activation window.

The access to the "restricted by password" service is managed by checking corresponding box in VAS activation window.

Pa ssword activation	* 29 * <PASSWORD> #
Password deactivation	# 29 #
Rassword-based outgoing calls restrictions ("restricted by password")	* 32 * <PASSWORD> #

Where:
<PASSWORD> – private subscriber password.

7. Change password

This service allows a subscriber to change a password assigned by PBX service personnel. The access to the service is managed by checking the "Change password" box in VAS activation window.

Change password	* 30 * <PASSWORD1> * <PASSWORD2> * <PASSWORD2> #

where:
<PASSWORD1> –current password;
<PASSWORD2> – a new password, which you need to enter twice. The password must contain 4 characters.

8. Outgoing calls restriction

The service allows to establish restriction on outgoing communication for phone calls to some directions. The following groups of communication types are defined:

Group 1 – only calls to emergency services;

Group 2 – only local and emergency calls;

Group 3 – communication types of group 1 and group 2 and zone communication.

The type of communication is set in prefix parameters.

To override restrictions set by this service, you may use "restrict by password" and "password activation" services. To reestablish the restrictions, use "password deactivation" service.

The access to the service is managed by "Outgoing calls restriction" box in VAS activation window.

Activate the service	* 34 * <PASSWORD> * N #
Cancel the service	# 34 * <PASSWORD> #
Control	* # 34 * <PASSWORD> #

<N> – a number of a group of permitted outgoing communication.

9. Do not disturb

The service allows to restrict calls on a subscriber and set a whitelist of numbers which are permitted to call the subscriber even in "do not disturb" mode.

The access to the service is managed by checking the "do not disturb" box in VAS activation window.

Activate the service	* 26 #
Cancel the service	# 26 #
Control	* # 26 #
Add a number to whitelist	* 26 * <NUMBER>
Remove a number from whitelist	# 26 * <NUMBER>

10. Blacklist

The service allows to forbid certain numbers to implement calls to a subscriber.

The access to the service is managed by "Blacklist" box in VAS activation window

Activate the service	* 61 * <PASSWORD> #
Cancel the service	# 61 * <PASSWORD> #
Control	* # 61 * <PASSWORD> #
Add a number to blacklist	* 61 * <PASSWORD> * <NUMBER>
Remove a number from blacklist	# 61 * <PASSWORD> * <NUMBER>

11. Reset all services

This service allows the subscriber to cancel all activated services from their phone unit using a single cancelling procedure. Cancelling procedure includes the service code and password code.

Access to service is governed by the "Reset all services" VAS category checkbox.

Usage	* 50#

APPENDIX J. RADIUS CALL MANAGEMENT SERVICE[1]

The gateway allows to change the passing call parameters using the RADIUS server commands sent in response to RADIUS-Authorization requests. Commands are transferred in the text format using Vendor-Specific attribute (see Section 3.1.15.3) with vendor number assigned to Eltex and equal to 35265 and Eltex-AVPair attribute name with the number 1.

In general, Eltex-AVPair attribute format will be as follows:
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): <$COMMAND-STRING>

By transferring various commands in $COMMAND-STRING, you may manage the following parameters:

- CgPN and CdPN number modification:

Number modification may be performed at two stages during call processing:

- For the incoming communication, before the call passes through the dial plan, i.e. before its routing. For that purpose, CgPNin and CdPNin values are used for Calling and Called numbers respectively.
- For the outgoing communication, after the call passes through the dial plan and after its routing. For that purpose, CgPNout and CdPNout values are used for Calling and Called numbers respectively.

For CgPN numbers, you may 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 may modify the following parameters in addition to the number itself:

- *numtype* — CdPN number type
- *plantype* — CdPN dial plan type

CgPN and CdPN number modification request syntax

The command consists of the required part and optional parts. Required part contains an initial text identifier of the command, modified number identifier and modification mask.

- 'CallManagement:' is a text identifier defining that this attribute contains the call management command.
- 'CgPNin=', 'CdPNin=', 'CgPNout=', 'CdPNout=' — number identifiers, indicate the number that the modification should be applied to.
- 'Modifier mask' parameter — modification rule for number digits (may be empty).

Optional part may contain a single or multiple parameters delimited by semicolons. If an optional part of the command is present, required and optional parts are also should be delimited by the semicolon.

[1] Available only under RCM license

Possible optional part parameters:

- numtype.
- plantype.
- presentation.

In general, command format will be as follows:

1.CallManagement:CgPNin=<$modifymask>;numtype=<$numtype>;plantype=<$plantype>;presentation=<$presentation>

where
'CallManagement:CgPNin=<$modify-mask>;' — required part.
'numtype=<$numtype>;plantype=<$plantype>;presentation=<$presentation>' — optional part.

2. CallManagement:CdPNin=;numtype=<$numtype>;plantype=<$plantype>

where
'CallManagement:CgPNin=;' — required part with an empty modification mask.
«numtype=<$numtype>;plantype=<$plantype>» — optional part.

3. CallManagement:CgPNin=<$modify-mask>;

where

«CallManagement:CgPNin=<$modify-mask>;» — required part.
Optional part is absent.

Values of parameters used in commands are as follows:

- $modify-mask — number modification rule (for rule modification syntax, see Section 3.1.8.4.4.1 Modification rule syntax).
- $numtype — represents one of the values: international, national, network-specific, subscriber, unknown.
- $plantype — represents one of the values: isdn, national, private, unknown.
- $presentation — represents one of the values: allowed, restricted, not-available, spare.

The gateway allows to 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>»
```

is equivalent to a single command:

```
«CallManagement:CgPNin=<$modify-mask>;numtype=<$numtype>;presentation=<$presentation>»
```

✓ **If one of the optional parameters (numtype, plantype, presentation) should remain unchanged, do not include it in the request, but you must specify the number type**

(CgPNin, CdPNin, CgPNout, CdPNout) that passed fields belong to in the beginning of the request.

Example:

For incoming communication, add prefix +7383 to CgPN, change its number type to national and define presentation restricted.

To do that, it is sufficient to pass the attribute with the following value in Access-Accept reply from the RADIUS server:

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1):
CallManagement:CgPNin=+7383;numtype=national;presentation=restricted

That 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 RADIUS server commands, you may manage the call routing process, i.e. to transfer it to another dial plan of the gateway and unconditionally forward it to a prefix created in the configuration (equivalent to the 'direct prefix' parameter described in Section 3.1.7.1 Trunk groups).

Routing management command consists of the required part only:

- 'CallManagement:' is a text identifier defining that this attribute contains the call management command.
- 'NumberingPlan' — identifier that indicates the dial plan change command.
- 'DirectRoutePrefix' — identifier that indicates the direct routing prefix selection command.

In general, command format will be as follows:

```
CallManagement:NumberingPlan=<$numplan_idx>
CallManagement:DirectRoutePrefix=<$prefix_index>
```

where
$numplan_idx — dial plan sequential number.
$prefix_index — ID of a prefix created in the dial plan.

Example

Change the call dial plan to the 3rd one.

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): CallManagement:NumberingPlan=3
```

Call category management

Using RADIUS server commands, you may modify access category and subscriber's Caller ID category (equivalent to the 'calling party category'). To do this, use the following fields:

Category changing command consists of the required part only:

- 'CallManagement:' is a text identifier defining that this attribute contains the call management command.

- 'AccessCategory' — identifier that indicates the access category change command.

- 'AONCategory' — identifier that indicates the calling party category change command.

In general, command format will be as follows:

```
CallManagement:AccessCategory=<$category_idx>
CallManagement:AONCategory=<$category_value>
```

where

```
$category_idx — access category index.
$category_value — Caller ID category index.
```

Example

Define subscriber category (calling party category) equal to 7.

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): CallManagement:AONCategory=7
```

Subscriber parameter management

For dynamic subscribers, you may define the 'Line quantity' and line operation mode parameter at the subscriber registration phase.

Subscriber parameter management command consists of the required part only:

- *'UserManagement:'* is a text identifier defining that this attribute contains the subscriber record management command.

- *'MaxActiveLines'* is an identifier indicating the quantity of active lines that are available to the current subscriber in common mode. The line operation mode will be set as common (even if separate mode has been specified), if the parameter 'MaxActiveLines' is specified.

- 'MaxEgressLines' - identifier, which indicates the number of egress lines that are available for subscriber in separate mode. The parameter can be combined with the 'MaxIngressLines';

- 'MaxIngressLines' - identifier, which indicates the number of ingress lines that are available in separate mode. The parameter can be combined with the 'MaxEgressLines';

In general, command format will be as follows:

```
"UserManagement:MaxActiveLines=<$line_count>"

"UserManagement:MaxEgressLines=<$egress>;MaxIngressLines=<$ingress>;”
"UserManagement:MaxEgressLines=<$egress>”
"UserManagement:MaxIngressLines=<$ingress>”
```

where
$line_count — quantity of active connections available to the subscriber simultaneously
$egress - the number of egress connections that are available to the subscriber;
$ingress - the number of ingress connections that are available to the subscriber.

Example

Define common line mode and three active lines for a subscriber.

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): UserManagement:MaxActiveLines=3
```

Set the separate line mode: 3 egress and 2 ingress lines

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1):      UserManagement:MaxEgressLines=3;MaxIngressLines=2
```

Set the common line mode: 2 active lines. (MaxActiveLines has unconditional priority over MaxEgressLines and MaxIngressLines)

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1):
        UserManagement:MaxEgressLines=6;MaxActiveLines=2;MaxIngressLines=5
```

APPENDIX K. MONITORING AND MANAGEMENT VIA SNMP

The gateway supports configuration and monitoring via Simple Network Management Protocol (SNMP).

Monitoring functions:

- Collection data on device, established sensors and software
- E1 streams and channels state
- VoIP submodules and channels state
- SS7 Linksets state
- SIP interfaces state

Management functions:

- firmware version updating
- current configuration saving
- device reboot
- SIP subscriber management
- management of dynamic SIP subscriber groups

The following format will be accepted for 'Inquiry description' column in the tables of OID description:

- Get – an object or tree value can be displayed by sending 'GetRequest'.
- Set – set an object value by sending 'SetRequest' (Please pay attention that if you set value by SET inquiry, you need OID in 'OID.0' form).
- {} – object name or OID;
- N – integer type numeric parameter is used in the command;
- U – unsigned integer numeric parameter is used in the command;
- S – string parameter is used in the command;
- A –IP address is used in the command (some commands using IP address as an argument has string type of data - 's'.

Inquiry 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

Examples of requests execution:

The inquiries which are shown below are equivalent. For instance, different types of requests for activeCallsCount object, that displays a number of current calls on SMG, are shown below.

```
$ 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 description from MIB ELTEX-SMG

Table K.2 – Common information and sensors

Name	***OID***	***Inquiry***	***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's name
smgDevType	1.3.6.1.4.1.35265.1.29.2	Get {}	Type of the device (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 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 parameters (separate with spaces): - name of firmware without spaces; - TFTP server's 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
smgTemperature 1	1.3.6.1.4.1.35265.1.29.35.1	Get {}	Temperature sensor 1
smgTemperature	1.3.6.1.4.1.35265.1.29.35.2	Get {}	Temperature sensor 2

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
smgPowerModuleTable	1.3.6.1.4.1.35265.1.29.36	Get {}	Information on power supply state, root object. Number of power unit is specified for subordinate objects: 1 or 2.
smgPowerModuleEntry	1.3.6.1.4.1.35265.1.29.36.1	Get {}	see smgPowerModuleTable
pmExist	1.3.6.1.4.1.35265.1.29.36.1.2.x	Get {}.x	Power unit 1 - installed 2 - not installed
pmPower	1.3.6.1.4.1.35265.1.29.36.1.3.x	Get {}.x	Power units are 1 - supplied with electric energy 2 - not supplied with electric energy
pmType	1.3.6.1.4.1.35265.1.29.36.1.4.x	Get {}.x	Type of installed power 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 CPU load in per cents for different types of tasks. The number of processor is specified for subordinate objects. SMG1016M - 1 SMG2016 - 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, user applications
cpuSys	1.3.6.1.4.1.35265.1.29.37.1.3.x	Get {}.x	% CPU, core applications
cpuNic	1.3.6.1.4.1.35265.1.29.37.1.4.x	Get {}.x	% CPU, applications with changed 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, input-output operations
cpuIrq	1.3.6.1.4.1.35265.1.29.37.1.7.x	Get {}.x	% CPU, hardware interrupts processing
cpuSirq	1.3.6.1.4.1.35265.1.29.37.1.8.x	Get {}.x	% CPU, software interrupts processing
cpuUsage	1.3.6.1.4.1.35265.1.29.37.1.9.x	Get {}.x	% CPU, common usage
smgSubscribersInfo	1.3.6.1.4.1.35265.1.29.42	Get {}	General information on active calls and registration quantity
activeCallCount	1.3.6.1.4.1.35265.1.29.42.1	Get {}	Current number of active calls
registrationCount	1.3.6.1.4.1.35265.1.29.42.2	Get {}	Current number of registrations

Table K.3 – Syslog settings

Name	***OID***	***Inquiry***	***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 {}	Trace settings in syslog, 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 trace receiving
smgSyslogTracesAlarms	1.3.6.1.4.1.35265.1.29.34.1.3	Get {} Set {} N	Alarm trace level: 1-99 - enable trace; 0 - disable trace.
smgSyslogTracesCalls	1.3.6.1.4.1.35265.1.29.34.1.4	Get {} Set {} N	Calls trace level: 1-99 - enable trace; 0 - disable trace.
smgSyslogTracesISUP	1.3.6.1.4.1.35265.1.29.34.1.5	Get {} Set {} N	SS7/ISUP trace level: 1-99 - enable trace; 0 - disable trace.
smgSyslogTracesSIPT	1.3.6.1.4.1.35265.1.29.34.1.6	Get {} Set {} N	SIPT trace level: 1-99 - enable trace; 0 - disable trace.
smgSyslogTracesQ931	1.3.6.1.4.1.35265.1.29.34.1.7	Get {} Set {} N	Q.931 trace level: 1-99 - enable trace; 0 - disable trace.
smgSyslogTracesRTP	1.3.6.1.4.1.35265.1.29.34.1.8	Get {} Set {} N	RTP trace level: 1-99 - enable trace; 0 - disable trace.
smgSyslogTracesMSP	1.3.6.1.4.1.35265.1.29.34.1.9	Get {} Set {} N	Voice submodule commands trace level: 1-99 - enable trace; 0 - disable trace.
smgSyslogTracesRadius	1.3.6.1.4.1.35265.1.29.34.1.10	Get {} Set {} N	RADIUS trace level: 1-99 - enable trace; 0 - disable trace.
smgSyslogTracesRowStatus	1.3.6.1.4.1.35265.1.29.34.1.11	Get {} Set {} i 1	Apply trace configuration changes
smgSyslogHistory	1.3.6.1.4.1.35265.1.29.34.2	Get {}	Settings of command 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 - full

smgSyslogHistoryRowStatus	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 {}	Syslog settings
smgSyslogConfigLogsEnabled	1.3.6.1.4.1.35265.1.29.34.3.1	Get {} Set {} N	Enable logging 1 - enable; 2 - disable
smgSyslogConfigSendToServer	1.3.6.1.4.1.35265.1.29.34.3.2	Get {} Set {} N	Send messages to syslog server: 1 - enable; 2 - disable
smgSyslogConfigAddres	1.3.6.1.4.1.35265.1.29.34.3.3	Get {}	IP address of syslog server

s		Set {} S	
smgSyslogConfigPort	1.3.6.1.4.1.35265.1.29.34.3.4	Get {} Set {} N	Port of syslog server
smgSyslogConfigRowStatus	1.3.6.1.4.1.35265.1.29.34.3.5	Get {} Set {} i 1	Apply changes in syslog settings

Table K.4 –E1 streams monitoring

Name	***OID***	***Inquiry***	***Description***
smgEOneTable	1.3.6.1.4.1.35265.1.29.7	Get {}	Table which shows physical state 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
			Physical state of E1 stream. Complete OID with a number of certain stream (0..15) in order to obtain information on the stream.
			State of a stream:
			0 - stream is disabled;
			1 - ALARM;
			2 - LOS;
			3 - AIS;
			4 - LOM;
			5 - LOMF;
			6 - stream is in operation;
			7 - the PRBS test has been launched on the stream

eOneLineInfoRemAlarm	1.3.6.1.4.1.35265.1.29.7.1.3 1.3.6.1.4.1.35265.1.29.7.1.3.x	Get {} Get {}.x	Presence of RAI signal on the stream - error on the remote side. Add a stream number (0..15) to OID for obtaining information on its status. 0 - normal state; 1 - RAI signal 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..15) to OID for obtaining information on its status. 0 - normal state; 1 - RAI16 signal 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	Alarms status on the stream. Add a stream number (0..15) 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, errors occured; 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..15) to OID for obtaining information on its status. 0 - no link; 1 - link
eOneLinkState	1.3.6.1.4.1.35265.1.29.7.1.7 1.3.6.1.4.1.35265.1.29.7.1.7.x	Get {} Get {}.x	Common state of the link. Add a stream number (0..15) 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..15) to OID for obtaining information on its status.
eOneSlipUp	1.3.6.1.4.1.35265.1.29.7.1.10 1.3.6.1.4.1.35265.1.29.7.1.10.x	Get {} Get {}.x	Frame slip (frame repeat). Add a stream number (0..15) to OID for obtaining information on its status.
eOneSlipDown	1.3.6.1.4.1.35265.1.29.7.1.11 1.3.6.1.4.1.35265.1.29.7.1.11.x	Get {} Get {}.x	Frame slip (frame loss). Add a stream number (0..15) to OID for obtaining information on its status.
eOneBERCount	1.3.6.1.4.1.35265.1.29.7.1.12 1.3.6.1.4.1.35265.1.29.7.1.12.x	Get {} Get {}.x	Bit errors. Add a stream number (0..15) to OID for obtaining information on its status.
eOneCVC	1.3.6.1.4.1.35265.1.29.7.1.13 1.3.6.1.4.1.35265.1.29.7.1.13.x	Get {} Get {}.x	Code Violation Counter. Add a stream number (0..15) 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 Errors Counter. Add a stream number (0..15) 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	A byte has been received. Add a stream number (0..15) 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	A byte has been transmitted. Add a stream number (0..15) 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 data packets have been received. Add a stream number (0..15) 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	Big data packets have been received. Add a stream number (0..15) to OID for obtaining information on its status.
eOneRxOvfl	1.3.6.1.4.1.35265.1.29.7.1.20	Get {}	Overload of receiving. Add a

	1.3.6.1.4.1.35265.1.29.7.1.20.x	Get {}.x	stream number (0..15) 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..15) 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 failure. Add a stream number (0..15) to OID for obtaining information on its status.
smgEOneChannelTable	1.3.6.1.4.1.35265.1.29.13	Get {}	Table of E1 channels states, root object.
smgEOneChannelEntry	1.3.6.1.4.1.35265.1.29.13.1	Get {}	see smgEOneChannelTable
channelEOneState	1.3.6.1.4.1.35265.1.29.13.1.2 1.3.6.1.4.1.35265.1.29.13.1.2.x 1.3.6.1.4.1.35265.1.29.13.1.2.x.x	Get {} Get {}.x Get {}.x.x	E1 channel state. Add a stream number (0..15) to OID for obtaining information on its status. Add a stream number (0..15) and channel number (0..31) to OID for obtaining information on its status.
smgEOneBusyChannelsCounters	1.3.6.1.4.1.35265.1.29.31	Get {}	Quantity of busy E1 channels, root object.
smgEOneInstantCounters	1.3.6.1.4.1.35265.1.29.31.1	Get {}	see smgEOneBusyChannelsCounters
smgEOneStream0BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.0	Get {}	Quantity of busy 0 E1 channels.
smgEOneStream1BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.1	Get {}	Quantity of busy 1 E1 channels
smgEOneStream2BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.2	Get {}	Quantity of busy 2 E1 channels
smgEOneStream3BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.3	Get {}	Quantity of busy 3 E1 channels
smgEOneStream4BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.4	Get {}	Quantity of busy 4 E1 channels
smgEOneStream5BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.5	Get {}	Quantity of busy 5 E1 channels
smgEOneStream6BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.6	Get {}	Quantity of busy 6 E1 channels
smgEOneStream7BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.7	Get {}	Quantity of busy 7 E1 channels
smgEOneStream8BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.8	Get {}	Quantity of busy 8 E1 channels
smgEOneStream9BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.9	Get {}	Quantity of busy 9 E1 channels
smgEOneStream10BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.10	Get {}	Quantity of busy 10 E1 channels
smgEOneStream11BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.11	Get {}	Quantity of busy 11 E1 channels
smgEOneStream12BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.12	Get {}	Quantity of busy 12 E1 channels

smgEOneStream13BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.13	Get {}	Quantity of busy 13 E1 channels
smgEOneStream14BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.14	Get {}	Quantity of busy 14 E1 channels
smgEOneStream15BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.15	Get {}	Quantity of busy 15 E1 channels
smgEOnePeriodicCounters	1.3.6.1.4.1.35265.1.29.31.2	Get {}	Quantity of busy E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream0BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.0	Get {}	Quantity of busy 0 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream1BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.1	Get {}	Quantity of busy 1 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream2BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.2	Get {}	Quantity of busy 2 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream3BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.3	Get {}	Quantity of busy 3 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream4BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.4	Get {}	Quantity of busy 4 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream5BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.5	Get {}	Quantity of busy 5 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream6BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.6	Get {}	Quantity of busy 6 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream7BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.7	Get {}	Quantity of busy 7 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream8BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.8	Get {}	Quantity of busy 8 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream9BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.9	Get {}	Quantity of busy 9 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream10BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.10	Get {}	Quantity of busy 10 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream11BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.11	Get {}	Quantity of busy 11 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream12BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.12	Get {}	Quantity of busy 12 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream13BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.13	Get {}	Quantity of busy 13 E1 channels in specified period (see smgEOneCounterPeriod)

smgEOneStream14BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.14	Get {}	Quantity of busy 14 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream15BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.15	Get {}	Quantity of busy 15 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneCounterPeriod	1.3.6.1.4.1.35265.1.29.31.2.16	Get {} Set {} N	Frequency (period) of statistics collection, in minutes. Statistics will accumulate in periodic counters, while the counter will display the value for the previous period.
smgChannelsE1free	1.3.6.1.4.1.35265.1.29.41	Get {}	Quantity of free E1 channels, root object.
e1freeS0channels	1.3.6.1.4.1.35265.1.29.41.1	Get {}	Quantity of free 0 E1 channels
e1freeS1channels	1.3.6.1.4.1.35265.1.29.41.2	Get {}	Quantity of free 1 E1 channels
e1freeS2channels	1.3.6.1.4.1.35265.1.29.41.3	Get {}	Quantity of free 2 E1 channels
e1freeS3channels	1.3.6.1.4.1.35265.1.29.41.4	Get {}	Quantity of free 3 E1 channels
e1freeS4channels	1.3.6.1.4.1.35265.1.29.41.5	Get {}	Quantity of free 4 E1 channels
e1freeS5channels	1.3.6.1.4.1.35265.1.29.41.6	Get {}	Quantity of free 5 E1 channels
e1freeS6channels	1.3.6.1.4.1.35265.1.29.41.7	Get {}	Quantity of free 6 E1 channels
e1freeS7channels	1.3.6.1.4.1.35265.1.29.41.8	Get {}	Quantity of free 7 E1 channels
e1freeS8channels	1.3.6.1.4.1.35265.1.29.41.9	Get {}	Quantity of free 8 E1 channels
e1freeS9channels	1.3.6.1.4.1.35265.1.29.41.10	Get {}	Quantity of free 9 E1 channels
e1freeS10channels	1.3.6.1.4.1.35265.1.29.41.11	Get {}	Quantity of free 10 E1 channels
e1freeS11channels	1.3.6.1.4.1.35265.1.29.41.12	Get {}	Quantity of free 11 E1 channels
e1freeS12channels	1.3.6.1.4.1.35265.1.29.41.13	Get {}	Quantity of free 12 E1 channels
e1freeS13channels	1.3.6.1.4.1.35265.1.29.41.14	Get {}	Quantity of free 13 E1 channels
e1freeS14channels	1.3.6.1.4.1.35265.1.29.41.15	Get {}	Quantity of free 14 E1 channels
e1freeS15channels	1.3.6.1.4.1.35265.1.29.41.16	Get {}	Quantity of free 15 E1 channels

Table K.5 – SS7 Linkset monitoring

Name	***OID***	***Inquiry***	***Description***
smgLinkSetTable	1.3.6.1.4.1.35265.1.29.11	Get {}	SS7 Linkset states, 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 states. Add Linkset's index (0..15) to OID for obtaining information on its status.

Table K.6 –SM-VP submodules monitoring (VoIP submodules)

Name	***OID***	***Inquiry***	***Description***
smgMspTable	1.3.6.1.4.1.35265.1.29.9	Get {}	Statistics of the status of the VoIP submodules, root object.
mspEntry	1.3.6.1.4.1.35265.1.29.9.1	Get {}	see smgMspTable
mspState	1.3.6.1.4.1.35265.1.29.9.1.2 1.3.6.1.4.1.35265.1.29.9.1.2.x	Get {} Get {}.x	Operation mode of VoIP submodule. Add submodule's number (0..5) to OID for obtaining information on its status

mspUsedConn	1.3.6.1.4.1.35265.1.29.9.1.3 1.3.6.1.4.1.35265.1.29.9.1.3.x	Get {} Get {}.x	Quantity of used submodule's channels. Add submodule's number (0..5) to OID for obtaining information on its status.
mspCreateReq	1.3.6.1.4.1.35265.1.29.9.1.4 1.3.6.1.4.1.35265.1.29.9.1.4.x	Get {} Get {}.x	Cumulative counter of inquiries to the module for link creation. Add submodule's number (0..5) to OID for obtaining information on its status.
mspCreated	1.3.6.1.4.1.35265.1.29.9.1.5 1.3.6.1.4.1.35265.1.29.9.1.5.x	Get {} Get {}.x	Cumulative counters of executed inquiries to the module for link creation. Add submodule's number (0..5) to OID for obtaining information on its status.
mspDestroyReq	1.3.6.1.4.1.35265.1.29.9.1.6 1.3.6.1.4.1.35265.1.29.9.1.6.x	Get {} Get {}.x	Cumulative counters of inquiries to the module for link removing. Add submodule's number (0..5) to OID for obtaining information on its status
mspDestroyed	1.3.6.1.4.1.35265.1.29.9.1.7 1.3.6.1.4.1.35265.1.29.9.1.7.x	Get {} Get {}.x	Cumulative counters of executed inquiries to the module for link removing . Add submodule's number (0..5) to OID for obtaining information on its status.
mspPayload	1.3.6.1.4.1.35265.1.29.9.1.8 1.3.6.1.4.1.35265.1.29.9.1.8.x	Get {} Get {}.x	Load of submodules measured in % of total channels number. Add submodule's number (0..5) to OID for obtaining information on its status.
smgIpMspChannelTable	1.3.6.1.4.1.35265.1.29.15	Get {}	Statistics of active channels state of VoIP submodules, root object.
smgMspIpChannelEntry	1.3.6.1.4.1.35265.1.29.15.1	Get {}	see smgIpMspChannelTable
ipMspChannelState	1.3.6.1.4.1.35265.1.29.15.1.2 1.3.6.1.4.1.35265.1.29.15.1.2.x 1.3.6.1.4.1.35265.1.29.15.1.2.x.x	Get {} Get {}.x Get {}.x.x	Active channels' state. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status. 0 - free; 1 - channel allocation; 2 - inquiry for channel allocation; 3 - inquiry for channel allocation has been processed; 4 - inquiry for channel

			discharging; 5 - inquiry for channel discharging has been processed; 6 - inquiry for channel disabling; 7 - inquiry for channel activating; 8 - in operation; 9 - activated; 10 - inquiry for connection to a conference; 11 - conference is active.
ipMspChannelSiptCallref	1.3.6.1.4.1.35265.1.29.15.1.3 1.3.6.1.4.1.35265.1.29.15.1.3.x 1.3.6.1.4.1.35265.1.29.15.1.3.x.x	Get {} Get {}.x Get {}.x.x	Local call identifier, which connected to an active channel. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status.
ipMspChannelSrcIp	1.3.6.1.4.1.35265.1.29.15.1.4 1.3.6.1.4.1.35265.1.29.15.1.4.x 1.3.6.1.4.1.35265.1.29.15.1.4.x.x	Get {} Get {}.x Get {}.x.x	Local IP address of a media stream. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status.
ipMspChannelSrcPort	1.3.6.1.4.1.35265.1.29.15.1.5 1.3.6.1.4.1.35265.1.29.15.1.5.x 1.3.6.1.4.1.35265.1.29.15.1.5.x.x	Get {} Get {}.x Get {}.x.x	Local port of a media stream. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status.
ipMspChannelSrcMac	1.3.6.1.4.1.35265.1.29.15.1.6 1.3.6.1.4.1.35265.1.29.15.1.6.x 1.3.6.1.4.1.35265.1.29.15.1.6.x.x	Get {} Get {}.x Get {}.x.x	Local MAC address of a media stream. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status.
ipMspChannelDstIp	1.3.6.1.4.1.35265.1.29.15.1.7 1.3.6.1.4.1.35265.1.29.15.1.7.x 1.3.6.1.4.1.35265.1.29.15.1.7.x.x	Get {} Get {}.x Get {}.x.x	Remote IP address of a media stream. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's

			number (0..127) to OID for obtaining information on the channel's status.
ipMspChannelDstPort	1.3.6.1.4.1.35265.1.29.15.1.8 1.3.6.1.4.1.35265.1.29.15.1.8.x 1.3.6.1.4.1.35265.1.29.15.1.8.x.x	Get {} Get {}.x Get {}.x.x	Remote port of a media stream. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status.
ipMspChannelDstMac	1.3.6.1.4.1.35265.1.29.15.1.9 1.3.6.1.4.1.35265.1.29.15.1.9.x 1.3.6.1.4.1.35265.1.29.15.1.9.x.x	Get {} Get {}.x Get {}.x.x	Remote MAC address of a media stream. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status.
ipMspChannelCallingPartyNumber	1.3.6.1.4.1.35265.1.29.15.1.10 1.3.6.1.4.1.35265.1.29.15.1.10.x 1.3.6.1.4.1.35265.1.29.15.1.10.x.x	Get {} Get {}.x Get {}.x.x	Number of a caller. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status.
ipMspChannelCalledPartyNumber	1.3.6.1.4.1.35265.1.29.15.1.11 1.3.6.1.4.1.35265.1.29.15.1.11.x 1.3.6.1.4.1.35265.1.29.15.1.11.x.x	Get {} Get {}.x Get {}.x.x	Number of a callee. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status.
ipMspChannelOccupiedTime	1.3.6.1.4.1.35265.1.29.15.1.12 1.3.6.1.4.1.35265.1.29.15.1.12.x 1.3.6.1.4.1.35265.1.29.15.1.12.x.x	Get {} Get {}.x Get {}.x.x	Call duration. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status.
smgChannelsVoip	1.3.6.1.4.1.35265.1.29.40	Get {}	Quantity of busy channels on VoIP submodules, root object.
voip0busyChannels	1.3.6.1.4.1.35265.1.29.40.1	Get {}	Quantity of busy channels on 0 VoIP submodule
voip1busyChannels	1.3.6.1.4.1.35265.1.29.40.2	Get {}	Quantity of busy channels on 1 VoIP submodule
voip2busyChannels	1.3.6.1.4.1.35265.1.29.40.3	Get {}	Quantity of busy channels on 2 VoIP submodule
voip3busyChannels	1.3.6.1.4.1.35265.1.29.40.4	Get {}	Quantity of busy channels on 3

			VoIP submodule
voip4busyChannels	1.3.6.1.4.1.35265.1.29.40.5	Get {}	Quantity of busy channels on 4 VoIP submodule
voip5busyChannels	1.3.6.1.4.1.35265.1.29.40.6	Get {}	Quantity of busy channels on 5 VoIP submodule
voip0freeChannels	1.3.6.1.4.1.35265.1.29.40.7	Get {}	Quantity of free channels on 0 VoIP submodule
voip1freeChannels	1.3.6.1.4.1.35265.1.29.40.8	Get {}	Quantity of free channels on 1 VoIP submodule
voip2freeChannels	1.3.6.1.4.1.35265.1.29.40.9	Get {}	Quantity of free channels on 2 VoIP submodule
voip3freeChannels	1.3.6.1.4.1.35265.1.29.40.10	Get {}	Quantity of free channels on 3 VoIP submodule
voip4freeChannels	1.3.6.1.4.1.35265.1.29.40.11	Get {}	Quantity of free channels on 4 VoIP submodule
voip5freeChannels	1.3.6.1.4.1.35265.1.29.40.12	Get {}	Quantity of free channels on 5 VoIP submodule

Table K.7 – SIP interfaces monitoring

Name	***OID***	***Inquiry***	***Description***
smgSipIntrfCallInfo	1.3.6.1.4.1.35265.1.29.43	Get {}	Information on calls on SIP interfaces, root object
sipIntrfCount	1.3.6.1.4.1.35265.1.29.43.1	Get {}	Quantity of SIP interfaces
sipIntrfActiveCallTable	1.3.6.1.4.1.35265.1.29.43.2	Get {}	Call table. (table will not be displayed if there is not any SIP interfaces)
sipIntrfActiveCallTableEntry	1.3.6.1.4.1.35265.1.29.43.2.1	Get {}	see 1.3.6.1.4.1.35265.1.29.43.2
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 of a SIP interface. Add interface index to OID for obtaining information on its status.
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 for obtaining information on its status.

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 for obtaining information on its status.
			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	Quantity of active calls on the interface. Add interface index to OID for obtaining information on its status.
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	Maximum quantity of calls on the interface. Add interface index to OID for obtaining

			information on its status. 0 - no limit; 1..65535 - limit of calls.

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, which implements reading of values:

```
#!/bin/bash
/usr/bin/snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 "$@"
```

sset script, which implements setting of values:

```
#!/bin/bash
/usr/bin/snmpset -v2c -c private -m +ELTEX-SMG 192.0.2.1 "$@"
```

Monitoring

Monitoring of subscriber or static group of subscriber can be implemented by several means:

5) By index or ID of a subscriber;
6) By numbering plan and full subscriber's number;
7) By numbering plan and partial subscriber's number.

To monitor:

1) Clear search status;
2) Define search criteria (optionally);
3) Display the information.

Example of a search by index

```
sset staticResetCheck.0 i 1             # reset search status
sset getUserByIndex.0 i 4       # setting search by index 4
swalk tableOfUsers          # inquiry of a table with 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 a search by numbering plan and full subscriber's number

```
sset staticResetCheck.0 i 1       # search status reset
sset getUserByNumplan.0 i 2          # set second numbering plan
sset getUserByNumber.0 s 20001          # set subscriber number
swalk tableOfUsers                  # inquiry of a table with subscriber information
```

Result:

```
ELTEX-SMG::UserID.9 = INTEGER: 10
ELTEX-SMG::RegState.9 = INTEGER: 0
ELTEX-SMG::Numplan.9 = INTEGER: 2
ELTEX-SMG::Number.9 = STRING: 20001
ELTEX-SMG::Ip.9 = IpAddress: 0.0.0.0
ELTEX-SMG::Port.9 = Gauge32: 0
ELTEX-SMG::Domain.9 = STRING: sipp.domain
ELTEX-SMG::MaxActiveLines.9 = INTEGER: 0
ELTEX-SMG::ActiveCallCount.9 = INTEGER: 0
ELTEX-SMG::RegExpires.9 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.12.9 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.13.9 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.14.9 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.15.9 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.16.9 = INTEGER: -1
```

Example of a search by numbering plan and partial subscriber's number

```
sset ttaticResetCheck.0 i 1       # search status reset
sset getUserByNumplan.0 i 0          # set zero numbering plan
sset getUserBySubNumber.0 s 400# set part of the subscriber number
swalk tableOfUsers                  # inquiry of a table with 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 a search

```
sset staticResetCheck.0 i 1         # search status reset
swalk tableOfUsers        # display all subscribers
swalk regState.3                    # display subscriber registration status
                          # with index 3
swalk ip.4                # display IP address of subscriber with index 4
swalk activeCallCount               # display quantity of active calls
                          # of all subscribers
```

Configuration

Configuration involves the following operations on subscribers:

1) Settings viewing;
2) Settings editing;
3) Creation of a new subscriber;
4) Removing.

To view the settings:

1) Select subscriber through the search;
2) Select configuration mode - view;
3) Display the necessary data.

To edit the settings:

1) Select subscriber through the search;
2) Select configuration mode - edit;
3) Define necessary settings;
4) Apply the settings.

To create a new subscriber:

1) Select configuration mode - creation;
2) Define necessary settings of the subscriber (at least number);
3) Apply the settings.

To remove a subscriber:

1) Select subscriber through the search;
2) Select configuration mode - removing;
3) Apply the settings.

You can cancel changes that were not applied only in 'Add new subscriber' and 'Edit a subscriber' modes.

Undo group remove is not possible. Only a complete configuration restore via WEB or CLI is available.

Example of new subscriber creation

```
sset staticResetCheck.0 i 1                # search status reset
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                     # search status reset
sset getUserByIndex.0 i 4             # set 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                # search status reset
sset getUserByNumplan.0 i 0           # set zero numbering plan
sset getUserByNumber.0 s 71234567890            # set the subscriber number
sset staticSetMode.0 i 2                        # set 'set' mode
sset stSetNumplan.0 i 1                    # change numbering plan to the first one
    sset stSetCliro.0 i 1                  # activate the 'CLIRO' service
    sset stSetAONtypeNumber.0 i 2                   # set 'National' automatic calling line identification type
sset staticSetApply.0 i 1                       # apply the settings
sset staticSetMode.0 i 0                   # set the 'none' mode
```

Example of removing of subscriber

```
sset staticResetCheck.0 i 1                # search status reset
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
                                   # you do not need to set the 'none' mode manually
```

Table M.8 – Monitoring and configuration of SIP subscribers (static subscribers)

Name	*OID*	*Inquiry*	*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; Find users by numplan; Find user by numplan and number; Find users by numplan and substring number - search by partial number and numbering plan;
staticResetCheck	1.3.6.1.4.1.35265.1.29.38.2	Set {} N	Search reset. Any value sets status of search to 'None'.
numActiveUsers	1.3.6.1.4.1.35265.1.29.38.3	Get {}	Quantity of active (authorized) subscribers.
numAllUsers	1.3.6.1.4.1.35265.1.29.38.4	Get {}	Quantity of subscribers in the system.
getUserByIndex	1.3.6.1.4.1.35265.1.29.38.5	Set {} N Set {} -1	Set subscriber's index for the search. The values in a range of [0:numAllUsers) set search in 'Find user by index' state. The '-1' value corresponds to 'None' state of the search.
getUserByID	1.3.6.1.4.1.35265.1.29.38.6	Set {} N Set {} -1	Set user ID for the search. 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 numbering plan for subscribers search. The -1 value automatically set search in 'None' status. If the value equals '0' or more, the priority of mode setting 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 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 a number for search of subscriber by numbering plan and a number. The length of the number should be from 1 to 32 digits. If you set a numbering plan, the status of search will be set to 'Find user by numplan and number', otherwise the status will not be changed. Set 'NULL' value to reset the number. In this case the status will be changed to

			'None'.
getUserBySubNumber	1.3.6.1.4.1.35265.1.29.38.9	Set {} S Set {} "NULL"	Set part of a number for search of subscriber by numbering plan and part of a number. The length of the number should be from 1 to 32 digits. If you set a numbering plan, the status of search will be set to 'Find user by numplan and substring number', otherwise the status will not be changed. Set 'NULL' value to reset the number. In this case the status will be changed to 'None'.
tableOfUsers	1.3.6.1.4.1.35265.1.29.38.10	Get {}	Static subscriber table, root object
tableOfUsersEntry	1.3.6.1.4.1.35265.1.29.38.10.1	Get {}	see TableOfUsers
userID	1.3.6.1.4.1.35265.1.29.38.10.1.2 1.3.6.1.4.1.35265.1.29.38.10.1.2.x	Get {} Get {}.x	Subscriber ID. Add subscriber index to OID to obtain information on the subscriber.
userRegState	1.3.6.1.4.1.35265.1.29.38.10.1.3 1.3.6.1.4.1.35265.1.29.38.10.1.3.x	Get {} Get {}.x	State of subscriber registration. Add subscriber index to OID to obtain information on the subscriber. 0 - not registered; 1 - registered
userNumplan	1.3.6.1.4.1.35265.1.29.38.10.1.4 1.3.6.1.4.1.35265.1.29.38.10.1.4.x	Get {} Get {}.x	Subscriber numbering plan. 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	Number of a subscriber. Add subscriber index to OID to obtain information on the subscriber.
userIp	1.3.6.1.4.1.35265.1.29.38.10.1.6 1.3.6.1.4.1.35265.1.29.38.10.1.6.x	Get {} Get {}.x	Subscriber IP address Add subscriber index to OID to obtain information on the subscriber. If the address is unknown, the '0.0.0.0' value will be set.
userPort	1.3.6.1.4.1.35265.1.29.38.10.1.7 1.3.6.1.4.1.35265.1.29.38.10.1.7.x	Get {} Get {}.x	Subscriber port. Add subscriber index to OID to obtain information on the subscriber.
userDomain	1.3.6.1.4.1.35265.1.29.38.10.1.8 1.3.6.1.4.1.35265.1.29.38.10.1.8.x	Get {} Get {}.x	Subscriber SIP domain Add subscriber index to OID to obtain information on the subscriber.
userMaxActiveLines	1.3.6.1.4.1.35265.1.29.38.10.1.9 1.3.6.1.4.1.35265.1.29.38.10.1.9.x	Get {} Get {}.x	The quantity of ingress/egress lines while operation in common line mode. Add subscriber index to OID to obtain information on the 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 common line mode. Add subscriber index to OID to obtain information on the subscriber.
userRegExpires	1.3.6.1.4.1.35265.1.29.38.10.1.11 1.3.6.1.4.1.35265.1.29.38.10.1.11.x	Get {} Get {}.x	Time to registration expiry, in seconds. Add subscriber index to OID to obtain information on the subscriber.
userLinesMode	1.3.6.1.4.1.35265.1.29.38.10.1.12 1.3.6.1.4.1.35265.1.29.38.10.1.12.x	Get {} Get {}.x	Lines operation modes. Add subscriber index to OID to obtain information on the subscriber. 0 - common; 1 - separate.
userMaxIngressLines	1.3.6.1.4.1.35265.1.29.38.10.1.13 1.3.6.1.4.1.35265.1.29.38.10.1.13.x	Get {} Get {}.x	The quantity of ingress lines while operation in separate mode. Add subscriber index to OID to obtain information on the subscriber.
userMaxEgressLines	1.3.6.1.4.1.35265.1.29.38.10.1.14 1.3.6.1.4.1.35265.1.29.38.10.1.14.x	Get {} Get {}.x	The quantity of egress lines while operation in separate mode. Add subscriber index to OID to obtain information on the subscriber.
userActiveIngressCount	1.3.6.1.4.1.35265.1.29.38.10.1.15 1.3.6.1.4.1.35265.1.29.38.10.1.15.x	Get {} Get {}.x	The quantity of active ingress calls while operation in separate mode. Add subscriber index to OID to obtain information on the subscriber.
userActiveEgressCount	1.3.6.1.4.1.35265.1.29.38.10.1.16 1.3.6.1.4.1.35265.1.29.38.10.1.16.x	Get {} Get {}.x	The quantity of active egress calls while operation in separate mode. Add subscriber index to OID to obtain information on the subscriber.
stSetAuthLog	1.3.6.1.4.1.35265.1.29.38.15.1.14	Get {} Set {} S	A name for authorization (login)

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;
			Del – remove a subscriber;
			The 'Show', 'Set', and 'Del' status 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 (before applying) in 'Set' and 'Add' modes, in other modes this command will be ignored.
staticSetApply	1.3.6.1.4.1.35265.1.29.38.14	Set {} N	Apply settings, add and removing of groups. New settings are activated in 'Set' mode; In '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 '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	Displayed name of a subscriber
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 {} Set {} S	Caller ID number

stSetAONtypeNumber	1.3.6.1.4.1.35265.1.29.38.15.1.9	Get {}
		Set {} N
			Caller ID number type
			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 - Category selection
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 {}	Authorization type

		Set {} S	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	Authorization login
stSetAuthPass	1.3.6.1.4.1.35265.1.29.38.15.1.15	Get {} Set {} S	Authorization password
stSetCliro	1.3.6.1.4.1.35265.1.29.38.15.1.16	Get {} Set {} N	CLIRO service 0 - not installed; 1 - installed
stSetPbxProfile	1.3.6.1.4.1.35265.1.29.38.15.1.17	Get {} Set {} N	PBX profile

stSetAccessMode	1.3.6.1.4.1.35265.1.29.38.15.1.18	Get {}
		Set {} N
			Customer service mode
			0 - Enabled;
			1 - Disabled 1;
			2 - Disabled 2;
			3 - ban 1;
			4 - ban 2;
			5 - ban 3;
			6 - ban 4;
			7 - ban 5;
			8 - ban 6;
			9 - ban 7;
			10 - ban 8;
			11 - excluded;
			12 - disabled

stSetLines	1.3.6.1.4.1.35265.1.29.38.15.1.19	Get {} Set {} N	The number of lines in common 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 - disable; 1 - enable
stSetBLFsubScribers	1.3.6.1.4.1.35265.1.29.38.15.1.22	Get {} Set {} N	The quantity of event subscribers

stSetIntercomMode	1.3.6.1.4.1.35265.1.29.38.15.1.23	Get {}
		Set {} N
			Intercom call type
			0 - One-sided;
			1 - Two-sided;
			2 - Regular call;
			3 - Reject.

stSetIntercomPriority	1.3.6.1.4.1.35265.1.29.38.15.1.24	Get {} Set {} N	Intercom call priority (1..5)
stSetLinesMode	1.3.6.1.4.1.35265.1.29.38.15.1.25	Get {} Set {} N	Lines operation mode 0 - Common; 1 - Separate
stSetIngressLines	1.3.6.1.4.1.35265.1.29.38.15.1.26	Get {} Set {} N	The quantity of ingress lines in separate mode. 0 - no limit
stSetEgressLines	1.3.6.1.4.1.35265.1.29.38.15.1.27	Get {} Set {} N	The quantity of egress lines in separate mode.

			0 - no limit
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 preanswering pause which will be transmitted in answer-after parameter

Monitoring and configuration of dynamic subscriber groups

The commands of SNMP utilities fetching will be implemented as following scripts in description of monitoring and configuration functions in order to achieve brevity and clarity of presentation:

Script **swalk**, realizing reading of values:

```
#!/bin/bash
/usr/bin/snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 "$@"
```

Script **sset**, realizing setting of values:

```
#!/bin/bash
/usr/bin/snmpset -v2c -c private -m +ELTEX-SMG 192.0.2.1 "$@"
```

Monitoring

Only authorized subscribers will be displayed while dynamic subscriber search.

Monitoring of a dynamic subscriber can be implemented by several means:

- By group and subscriber index;
- By subscriber ID;
- By numbering plan and full subscriber number;
- By numbering plan and part of a subscriber number.

To monitor:

1) Reset status of a search;
2) Define search criteria (optionally);
3) Show the information.

Example of a search by index

```
sset groupResetCheck.0 i 1                # reset status of the search
sset getGroupByIndex.0 i 0             # select the zero group
sset getGroupUserByIndex.0 i 4                # set the search by index 4
```

```
swalk tableOfGroupUsers              # request for table with information on a subscriber
```

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 table with information on a subscriber
```

Example of a search by numbering plan and partial number

```
sset groupResetCheck.0 i 1           # reset status of the search
sset getGroupUserByNumplan.0 i 0             # set the zero numbering plan
sset getGroupUserBySubNumber.0 s 24001 # set a part of a number
swalk tableOfGroupUsers              # request for table with information on a subscriber
```

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 the information without searching

```
sset groupResetCheck.0 i 1          # reset status of the search
swalk tableOfGroupUsers        # display all subscribers
```

Configuration

Configuration involves the following operations on dynamic subscribers groups:

1) Settings viewing;
2) Settings editing;
3) Creation of a new subscriber;
4) Removing.

To view the settings:

4) Select subscriber group by index or ID;
5) Select configuration mode - view;
6) Display the necessary data.

To edit the settings:

5) Select subscriber group by index or ID;
6) Select configuration mode - edit;
7) Define necessary settings;
8) Apply the settings.

To create a new group:

4) Select configuration mode - creation;
5) Define necessary settings of a new group
6) Apply the settings.

To remove a group:

4) Select subscriber group by index or ID;
5) Select configuration mode - removing;
6) Apply the settings.

You can cancel changes that were not applied only in 'Add new group' and 'Edit a group' modes.

Undo group remove is not possible. Only a complete configuration restore via WEB or CLI is available.

Example of 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                # activate 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 K.9 – Monitoring and configuration of dynamic subscriber groups

Name	*OID*	*Inquiry*	*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 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 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 {}	The quantity of subscriber groups.
numInGroup	1.3.6.1.4.1.35265.1.29.39.4	Set {} N	The quantity of subscribers in a group. Set a group number, and you will receive the number of subscribers. If you receive '-1' in reply, it means that the group with this number does not exist.
numActiveInGroup	1.3.6.1.4.1.35265.1.29.39.5	Set {} N	The quantity of active (authorized) subscribers in the group. Set a group number, and you will receive the number of subscribers. If you receive '-1' in reply, it means that the group

			with this number does not exist.
getGroupByIndex	1.3.6.1.4.1.35265.1.29.39.6	Set {} N	Set subscriber index for searching of by group index. The search status will be changed to 'Find user by numplan and number', if you set '1' or greater as a group index. If you set '-1' value, the status of search will be changed to 'None'. If you set group index which does not exist, the status of search will be reset to 'None'.
getGroupUserByIndex	1.3.6.1.4.1.35265.1.29.39.7	Set {} N	Set subscriber index in a group for search by group index. Set index of the group before start. (see GetGroupByIndex). The status of the search will be set to 'Find user by numplan and number'. Setting '-1' value make search status changed from ' Find user by group and user index' to 'None'.
getGroupUserByID	1.3.6.1.4.1.35265.1.29.39.8	Set {} U	Set ID in order to search a subscriber. Setting '1' and greater numbers makes search status changed to 'Find user by ID'. If you set '0' value, the status will be changed from 'Find user by ID' to 'None'.
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 changed. Set 'NULL' to reset a number, the search status will be changed to 'None' in this case.
tableOfGroupUsers	1.3.6.1.4.1.35265.1.29.39.12	Get {}	Dynamic subscriber table, root object
tableOfGroupUsersEntry	1.3.6.1.4.1.35265.1.29.39.12.1	Get {}	see TableOfGroupUsers
groupUserID	1.3.6.1.4.1.35265.1.29.39.12.1.3 1.3.6.1.4.1.35265.1.29.39.12.1.3.x.x	Get {} Get {}.x.x	Subscriber's ID. Add a group index and subscriber's ID to OID for obtaining information on the 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	Subscriber's registration state. Add a group index and subscriber's ID to OID for obtaining information on the subscriber. 0 - unregistered; 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	Subscriber's numbering plan. Add a group index and subscriber's ID to OID for obtaining information on the 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	Number of a subscriber. Add a group index and subscriber's ID to OID for obtaining information on the 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's IP address Add a group index and subscriber's ID to OID for obtaining information on the subscriber. If the IP address is unknown, the value will set to 0.0.0.0.
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 's port Add a group index and subscriber's ID to OID for obtaining information on the

			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 a subscriber. Add a group index and subscriber's ID to OID for obtaining information on the 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 in 'common' mode. Add a group index and subscriber's ID to OID for obtaining information on the 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 in 'common' line mode. Add a group index and subscriber's ID to OID for obtaining information on the 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 a group index and subscriber's ID to OID for obtaining information on the 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	Lines operation mode. Add a group index and subscriber's ID to OID for obtaining information on the subscriber. 0 - common; 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 in 'separate' mode. Add a group index and subscriber's ID to OID for obtaining information on the 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 in 'separate' mode. Add a group index and subscriber's ID to OID for obtaining information on the 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 incoming calls in 'separate' line mode. Add a group index and subscriber's ID to OID for obtaining information on the 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 outgoing calls in 'separate' line mode. Add a group index and subscriber's ID to OID for obtaining information on the subscriber.

groupUserGroupModeSetings	1.3.6.1.4.1.35265.1.29.39.13	Get {}	Dynamic subscriber group operation settings modes:
			None - settings operation is disabled;
			Show - show group settings;
			Set - change group settings;
			Add - add a group;
			Del - remove 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 (before applying) in 'Set' and 'Add' modes, in other modes this command will be ignored.
groupUserGroupSetApply	1.3.6.1.4.1.35265.1.29.39.16	Set {} N	Apply settings, add and removing of groups. New settings are activated in 'Set' mode; In '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.
groupUserGroupFindStatus	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'. 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	Automatic calling line identification category 0 - No change (from call); 1..10 - Category selection
groupSetAccessCat	1.3.6.1.4.1.35265.1.29.39.21.1.8	Get {} Set {} N	Access category
groupSetCliro	1.3.6.1.4.1.35265.1.29.39.21.1.9	Get {} Set {} N	CLIRO service 0 - not installed; 1 - installed
GroupSetPbxProfile	1.3.6.1.4.1.35265.1.29.39.21.1.10	Get {} Set {} N	PBX profile

groupSetAccessMode	1.3.6.1.4.1.35265.1.29.39.21.1.11	Get {}
		Set {} N
			Customer service mode
			0 - Enabled;
			1 - Disabled 1;
			2 - Disabled 2;
			3 - ban 1;
			4 - ban 2;
			5 - ban 3;
			6 - ban 4;
			7 - ban 5;
			8 - ban 6;
			9 - ban 7;
			10 - ban 8;
			11 - excluded;
			12 - disabled

groupSetLines	1.3.6.1.4.1.35265.1.29.39.21.1.12	Get {} Set {} N	The quantity of lines in common mode
groupSetNumplan	1.3.6.1.4.1.35265.1.29.39.21.1.13	Get {} Set {} N	Numbering 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 - disable; 1 - enable

groupSetBLFsubScribers	1.3.6.1.4.1.35265.1.29.39.21.1.16	Get {} Set {} N	The quantity of subscribers to events

groupSetIntercomMode	1.3.6.1.4.1.35265.1.29.39.21.1.17	Get {}
		Set {} N
			Intercom call type
			0 - One-sided;
			1 - Two-sided;
			2 - Regular call;
			3 - Reject.

groupSetIntercomPriority	1.3.6.1.4.1.35265.1.29.39.21.1.18	Get {} Set {} N	Intercom call priority (1..5)
groupSetLinesMode	1.3.6.1.4.1.35265.1.29.39.21.1.19	Get {} Set {} N	Lines operation mode: 0 - Common; 1 - Separate
groupSetIngressLines	1.3.6.1.4.1.35265.1.29.39.21.1.20	Get {} Set {} N	The quantity of ingress lines 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 in separate mode.

groupSetAONtypeNumber	1.3.6.1.4.1.35265.1.29.39.21.1.22	Get {}
		Set {} N
			Caller ID type:
			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	Define 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
groupSetIntercomTimer	1.3.6.1.4.1.35265.1.29.39.21.1.25	Get {} Set {} N	Set preanswering pause which will be tramsmitted in answer-after parameter

Out-of-date OID

Some of OIDs were changed and some branches might have been removed or changed to new values in subsequent releases. We recommend you to re-configure monitoring system and scripts to new OID usage.

Table M.10 – Out-of-date OID

Name	*OID*	*Inquiry*	*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	Is not supported in new hardware versions, always -1.

smgCpuLoad	1.3.6.1.4.1.35265.1.29.17	Get {}	Changed to 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 {}	Changed to 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 {}	Changed to 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 {}	Changed to 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 {}	Changed to 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 {}	Changed to 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 {}	Changed to 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 {}	Changed to 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 {}	Changed to cpuUsage (1.3.6.1.4.1.35265.1.29.37.1.9.x)

OID MIB-2 support (1.3.6.1.2.1)

SMG supports the following MIB-2 branches:

- system (1.3.6.1.2.1.1) – common information on the system;
- interfaces (1.3.6.1.2.1.2) – information on network interfaces;
- snmp (1.3.6.1.2.1.11) – information on SNMP operation.

TECHNICAL SUPPORT

For technical assistance in issues related to handling of ELTEXALATAU Ltd. equipment please address to Service Centre of the company:

Republic of Kazakhstan, 050032, Medeu district, microdistrict Alatau, 9 st. Ibragimova, 9
Phone:
+7(727) 220-76-10
+7(727) 220-76-07
E-mail: post@eltexalatau.kz

In official website of the ELTEXALATAU Ltd. you can find technical documentation and software for products, refer to knowledge base, consult with engineers of Service center in our technical forum:

http://www.eltexalatau.kz/en/