ELTEXALATAU
Complete solutions for networking

SMG-1016M, SMG-2016

Operation manual, version 3.1 (26.08.2016)

Digital gateway

SMG-1016M Firmware Version: V.3.7.0.1928
SMG-2016 Firmware Version: V.3.7.0.1928

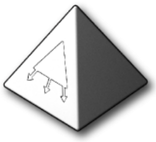
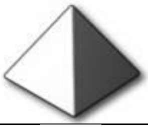
SIP adapter version: 3.7.0.16

Document version	Firmware version	Issue date	Revisions
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 advanced – COPM settings via TCP – Restriction of call duration on prefix – Optional outgiving a MOH in settings of trunk group – Settning a BLF monitoring group – New options of SIP hearders 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 – SS-7 signal link management via web configurator – SS-7 (CIC) channel management via web configurator – Operator selection code analysis option and master station type selection in SORM settings – RADIUS profile selection for outgoing communications in trunk group settings – 'Local ringback for early-media' option QSIG tunnelling protocol in SIP (SIP-Q)
Version 2.9	V.3.5.1	04.04.2016	Added: – New SM-VP submodule state — SSW.Sorm – 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 clearback reason 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 – Numbering schedule name is displayed in tree settings – 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 – Conference with consequent assembly for SORM (Law Enforcement Support System) – Correct SORM operation when operator selection code is dialled during call – VLAN configuration on switch for SMG-2016
Version 2.7	V.3.4.2	06.11.2015	Added: – SORM number modifications – 'Do not transmit VAS prefix' option for SORM protocol – 'Do not use extended error codes' option for SORM protocol – 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 – 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 numbering schedule 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 – Banned address log — fail2ban – Original or processed numbers transmission in RADIUS messages – RADIUS- Authorization transmission during local redirection – Time transmission in UTC format in RADIUS-Accounting messages – Transmission 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 SS-7 line group 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 – SORM configuration sequence by Order 268
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 – SS-7 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 – Addenda of Appendix E. Provisioning of SORM functions – Configuration for dialling 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-cause match table and SIP-reply configuration – Scheduled routing configuration – RTP port range configuration – FTP server configuration – Firewall profile configuration – Voice message usage configuration – Fault logging device selection – View submodule link connection information – L1 tier activity monitoring for SORM – SMG connection method example for operation in SS-7 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 – Fault events log – MTP3 (DPC-MTP3) opposite code function support – ISUP (DPC- ISUP) opposite code function support – Kazakhstan SORM specifications support – Numbering schedule 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 subscriber 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 TG 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	Added: – SORM signalling settings – Appendix E. Provisioning of SORM functions
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 issue

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 link switching principle with communication networks used for IP network 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.

Gateway is able to generate a single E1 stream to SORM panel. E1 stream utilizing SORM protocol contains 28 voice links for wire-tapping of the tracked subscribers. During combined tracking, voice traffic from subscribers A and B is mixed into the SORM stream voice link. Voice stream mixing is performed in a three-way conference on VoIP submodule. A single VoIP submodule supports up to 27 three-way conferences. Thus, to enable the pickup for all E1 stream links simultaneously, at least two VoIP submodules should be installed on the gateway.

SMG main specifications:

- Number of E1 interfaces: 4 to 16, in increments of 4
- Up to 960 VoIP channels (128 channels in TDM for connectingto 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], MEGACO1, SIGTRAN1
- TDM protocols: ISDN PRI(Q.931), QSIG and CORNET for subscriber name transmission, SS-7 (quasi-associated mode operation), V5.21
- SIP subscriber registration support:
  - Up to 2000 for SMG-1016M
  - Up to 3000 for 2016
- DTMF transmission (SIP INFO, RFC2833, in-band)
- Echo cancellation (G.168 recommendation)
- Voice activity detector (VAD)
- 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

[1]Not supported in the current version.

- 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).

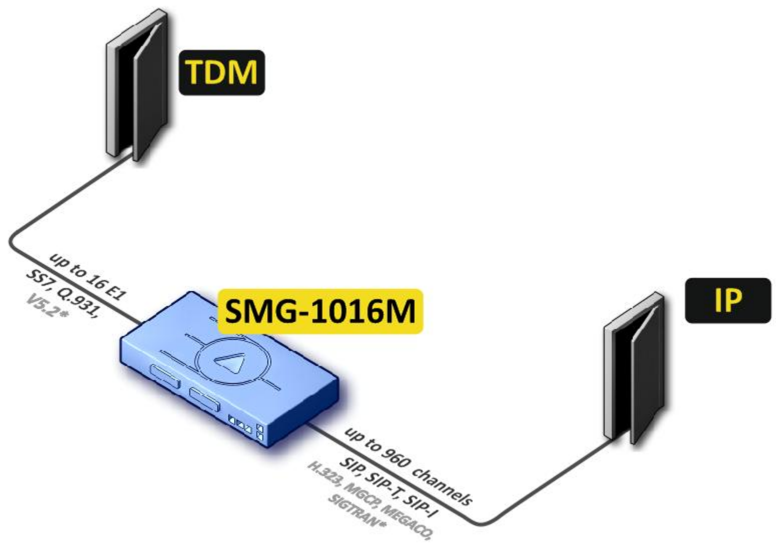
1.2 Typical Application Diagrams

This manual covers several SMG device connection methods:

1.2.1 *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 (SS-7, ISDN PRI/QSIG/CORNET, V5.2[1]) and maintenance for up to 960 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.

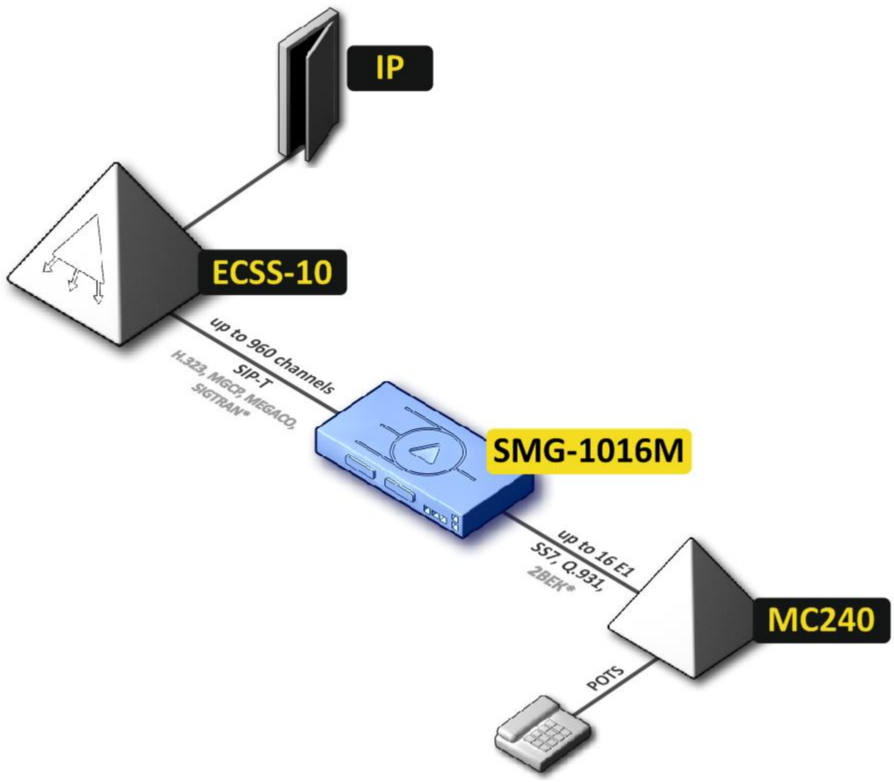


*—Not supported in the current version

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

[1]Not supported in the current version.

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

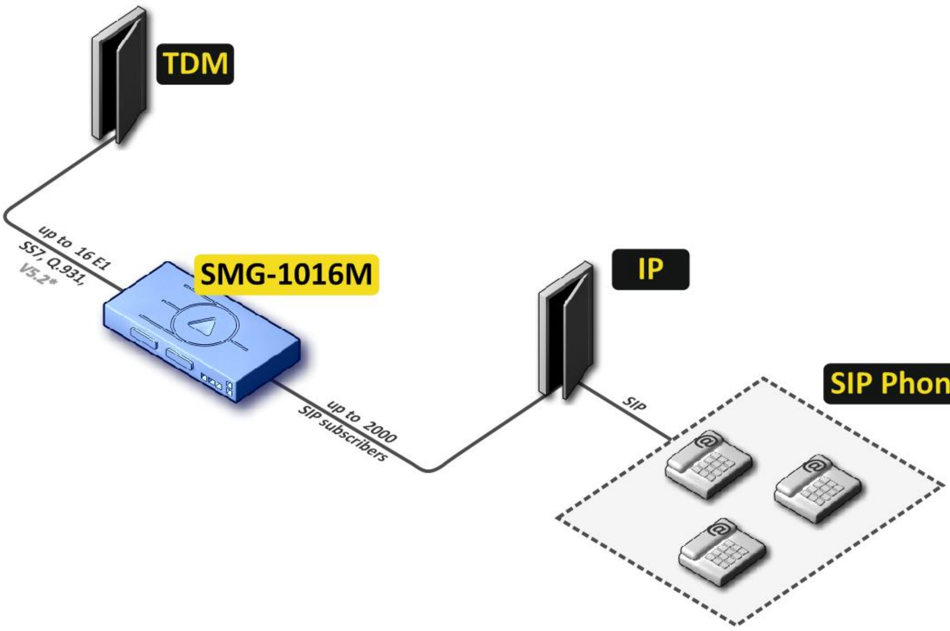


*—Not supported in the current version

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

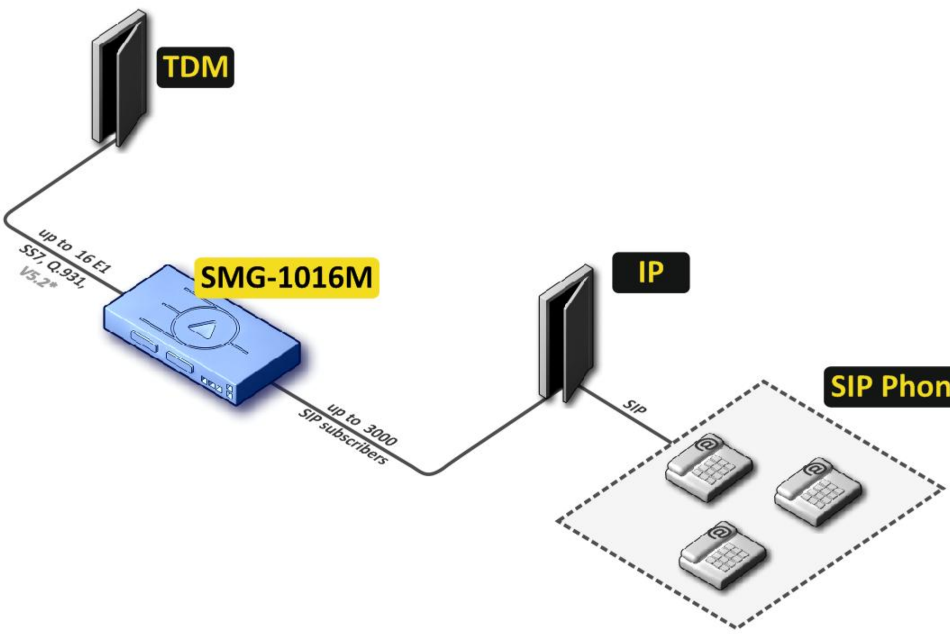
1.2.2 *Mini IP-PBX*

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 (SS-7, ISDN PRI/QSIG/CORNET, V5.2[1]).



*—Not supported in the current version

Fig. 3—Mini IP-PBX based on SMG-1016M



*—Not supported in the current version

Fig. 4—Mini IP-PBX based on SMG-2016

[1] Not supported in the current version

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 *M4E1*
- 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

Fig. below shows SMG-1016M functional chart.

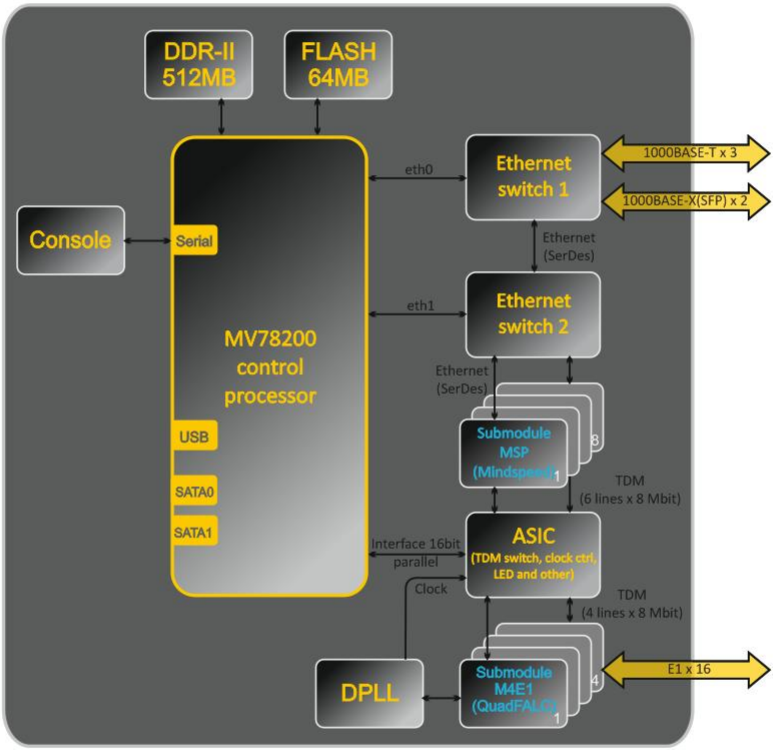


Fig. 5—SMG-1016M functional chart

1.3.2 SMG-2016 Design

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

- Controller featuring:
  - Controlling CPU
  - Flash memory: 1024Mb
  - RAM: 4096Mb
- Up to 4 E1 stream submodules *M4E1*
- 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

Fig. below shows SMG-2016 functional chart.

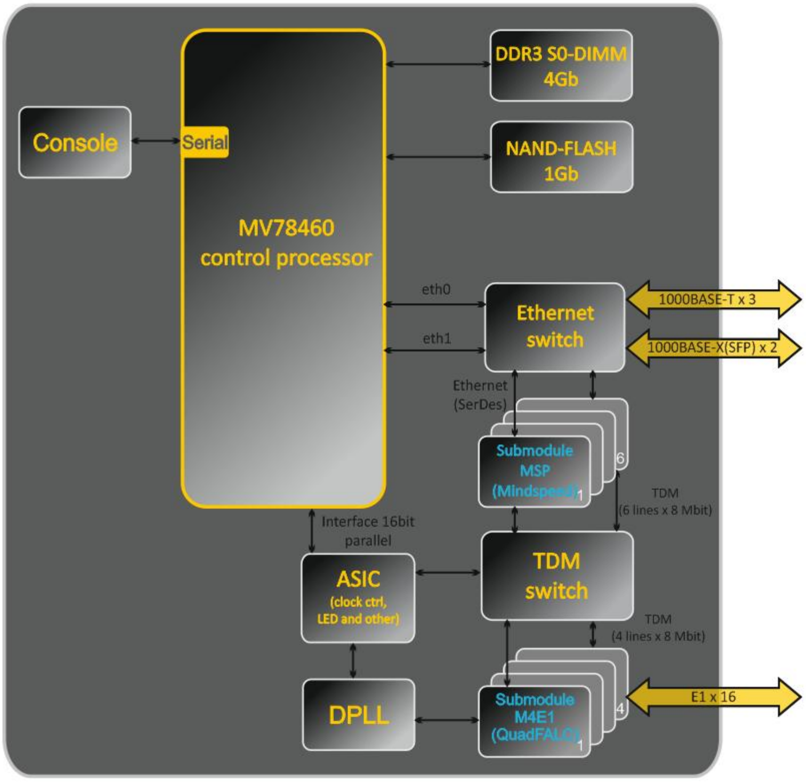


Fig. 6—SMG-2016 functional chart

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 2Mbps 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 (M4E1) and VoIP (SM-VP-M300) submodules.

For device firmware architecture, see Fig. below.

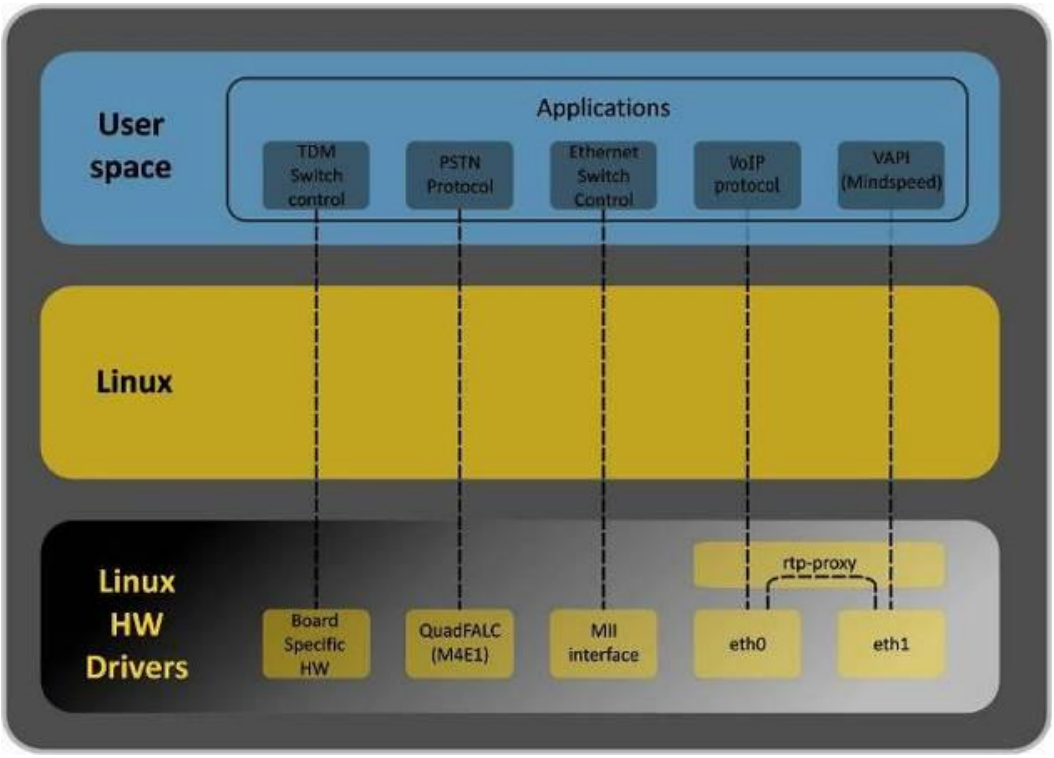


Fig. 7—SMG firmware architecture

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[1] SIGTRAN[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 G.711 (A/U) / 10 G.729 A / 20-80 G.729 A / 10 G.723.1 (6.3 Kbps, 5.3 Kbps) G.726 / 20 G.726 / 10 T.38	160 112 72 62 58 98 88 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 fibre, wave length 1310nm (Single-Mode), 1000BASE-LX (LC connector), distance—up to 10km, supply voltage—3.3V 2) duplex, single fibre, 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 version.

Console Parameters

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

E1 Interface Parameters:

No. of channels	Acc. 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	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, SS-7, V5.2[1]

General parameters

Operating temperature range		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	PM150-220/12	PM75-48/12
	PM rated power	150W	75W
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[2]	0.1kg	

[1] Not supported in the current version.
[2]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 Fig. below.

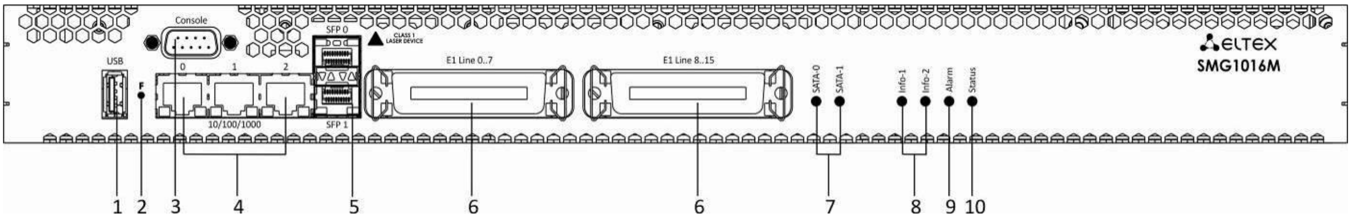


Fig. 8—SMG-1016M front panel layout

Connectors, LEDs and controls located on the front panel of the device are listed in Table 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[1]
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 Fig. below.

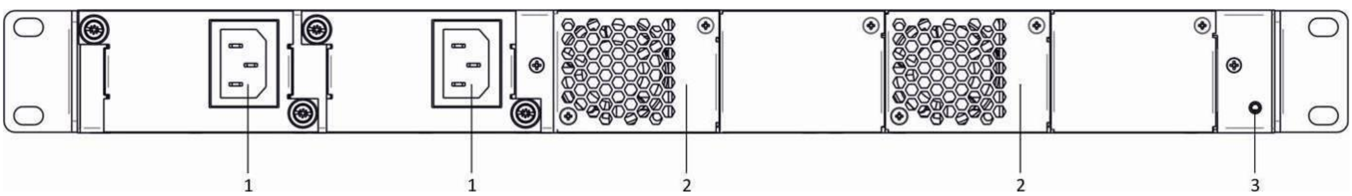


Fig. 9—SMG-1016M rear panel layout

[1]Not used in the current version

Table below 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 Fig. below.

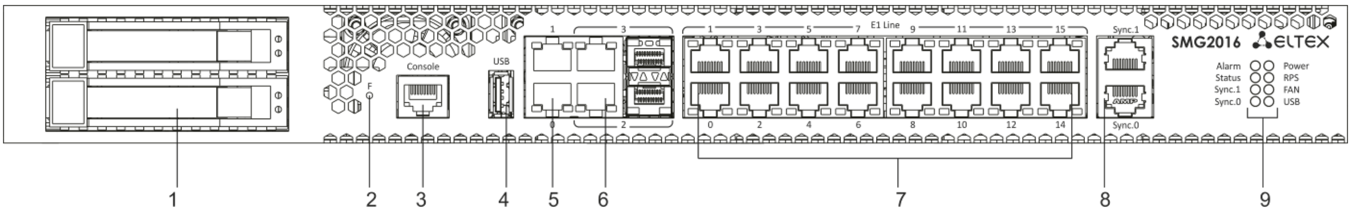


Fig. 10—SMG-2016 front panel layout

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 Fig. below.

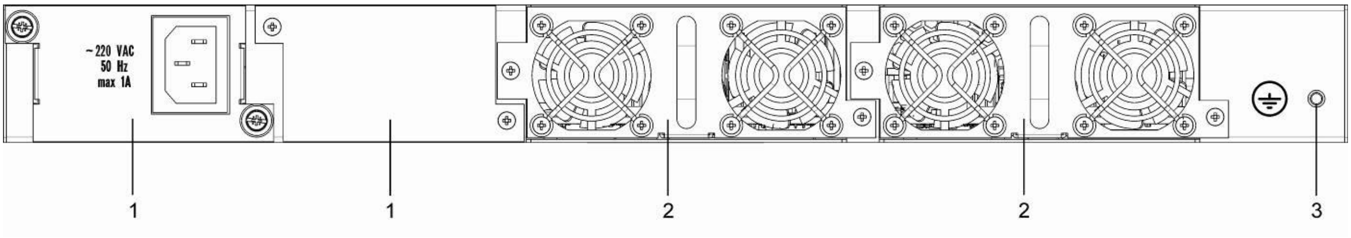


Fig. 11—SMG-2016 rear panel layout

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 below.

Table 6—Light indication of the device status in operation

Indicator	Indicator State	Device State
Info1	Off	SFP0 link lost
	Solid green	SFP0 link in operation
Info2	Off	SFP1 link lost
	Solid green	SFP1 link in operation
	Lights red	Device starts up
Alarm	Flashes red	Critical device failure
	Lights red	Non-critical device failure
	Solid yellow	No failures, non-critical warnings
	Solid green	Normal operation
Status	Solid green	Normal operation
	Off	Device power lost

1.6.1.2 SMG-2016

For device light indication in operation, see Table below.

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
	Solid yellow	No failures, non-critical warnings
	Solid green	Normal operation
Status	Solid green	Normal operation
	Off	Device power lost
Sync.0, Sync.1	Solid green	Synchronization with an external source
	Off	External synchronization source disconnected
Power	Solid green	Powered by Power supply no.1
	Solid orange	Power supply no.1 is installed, but not energized
RPS	Solid 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	Solid green	All removable fan modules are installed, all fans are operational
	Solid orange	All removable fan modules are installed, some fans are down
	Lights red	Single or both removable fan modules are not installed
USB	Solid 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 below.

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)

1.6.3 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	solid on	solid on
Port is in 1000Base-T mode, data transfer	solid on	flashes
Port is in 10/100Base-TX mode, no data transfer	Off	solid 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.

[1] For SMG-2016 only

					(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.

1.6.4.1 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
	Alarm	Status	Sync.1	Sync.2	(device in operation)
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

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 margins, 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
		SS-7 line group fault (when *'Fault indication'* checkbox is selected in *'Routing/SS line groups'* 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% (15–30Mb)
Lights red	Non-critical (errors)	SS-7 link fault (when *'Fault indication'* checkbox is selected in *'Routing/SS line groups'* menu)
		VoIP submodule (MSP) loss
		Synchronization fault (free-run mode operation)
		FTP server is unavailable, utilization of RAM for CDR file storage is below 50% (5–15Mb)
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 below 5Mb
		CPS fault threshold is exceeded for one of the trunk groups

1.7 'F' Function Button Operation

F button allows you 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
– CENC-36M connector—2pcs (if 18 pairs of UTP CAT5E cable were not included in order)
– RS-232 DB9(F)–DB9(F) connection cable
– A mounting set for 19'' rack
– 2 x support brackets
– Operation manual

If ordered, delivery package may also include:

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

1.10.2 SMG-2016

SMG-2016 standard delivery package includes:

– SMG-2016 digital gateway
– A mounting set for 19'' rack
– RJ45-DB9 console port adapter
– 2 x support brackets
– Documentation

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 authorised 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 earthing wire should be securely connected to the earth bonding point. The resistance between the earth bonding point and earthing 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 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 earthing 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 as follows:
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 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 ambient 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 earthing. The device grounding and the earthing wire section should comply with Electric Installation Code. The earth bonding point is located at the right bottom corner of the side panel, Fig. 9, Fig. 11.

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 fix the device case on the brackets.

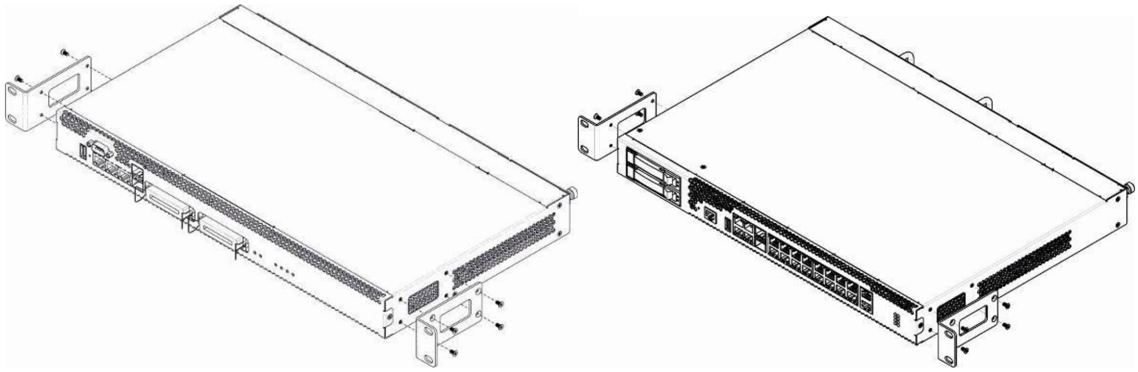


Fig. 12—Support brackets mounting for SMG-1016M (left-hand side) and SMG-2016 (right-hand side)

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. 12.
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.

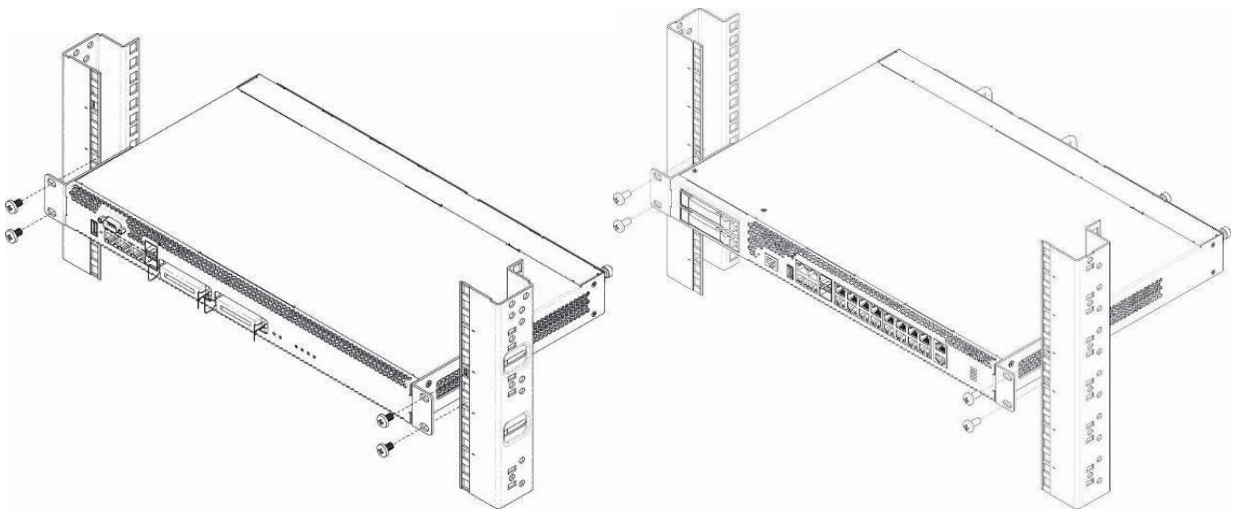


Fig. 13—Device rack installation for SMG-1016M (left-hand side) and SMG-2016 (right-hand side)

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 centre—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 feature 2 power supply circuit breakers with nominal current 3.15A. Circuit breakers are not user-serviceable. They should be replaced by the qualified service specialists in the manufacturer's service center.

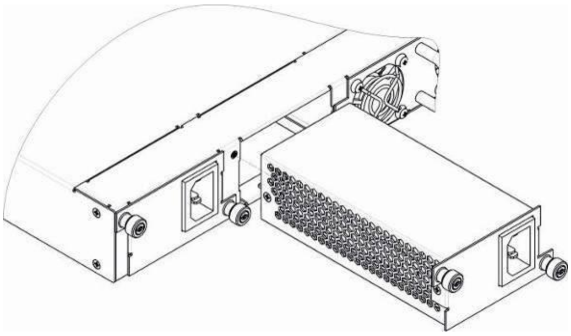


Fig. 14—Power module installation

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**).

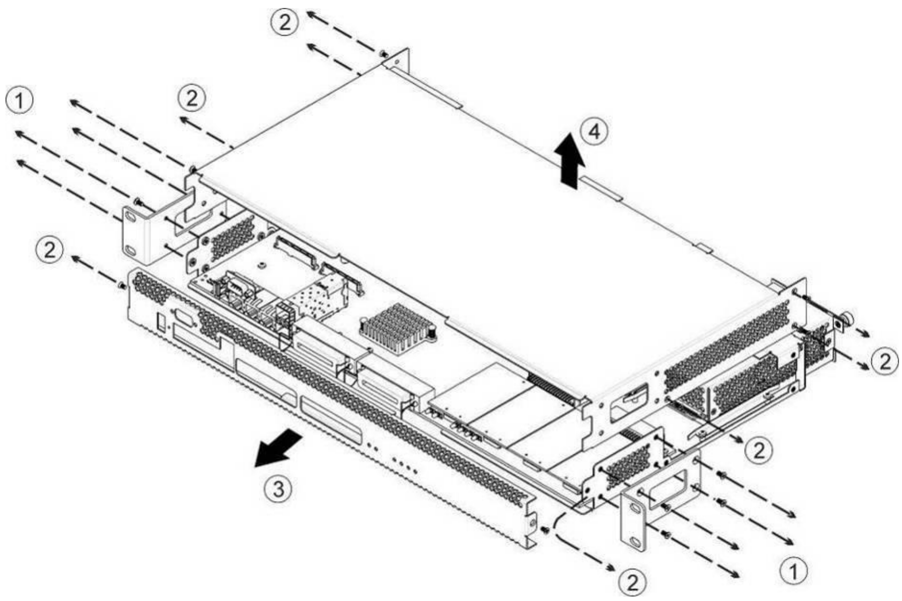


Fig. 15—SMG-1016M housing removal procedure

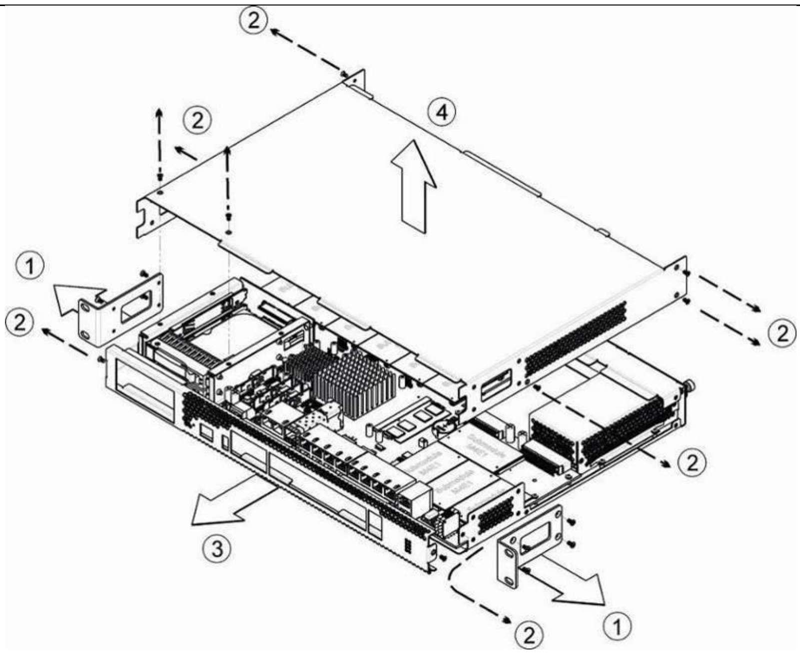


Fig. 16—SMG-2016 housing removal procedure

1. Use a screwdriver to remove support brackets from the device housing.
2. Remove the screws holding the front and top panels of the device with a screwdriver as shown in the Figure.
3. Gently pull the front panel until it separates from the top and side panels.
4. Pull the top panel (cover) of the device to remove it.

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

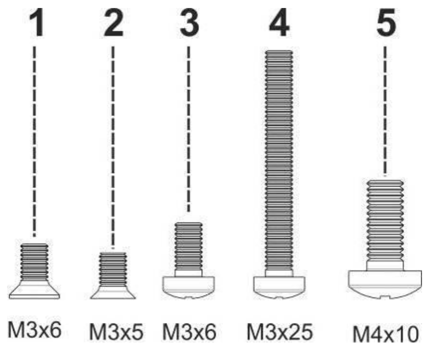


Fig. 17—Types of screws used for SMG assembly

Fig. 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. Earthing screw

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

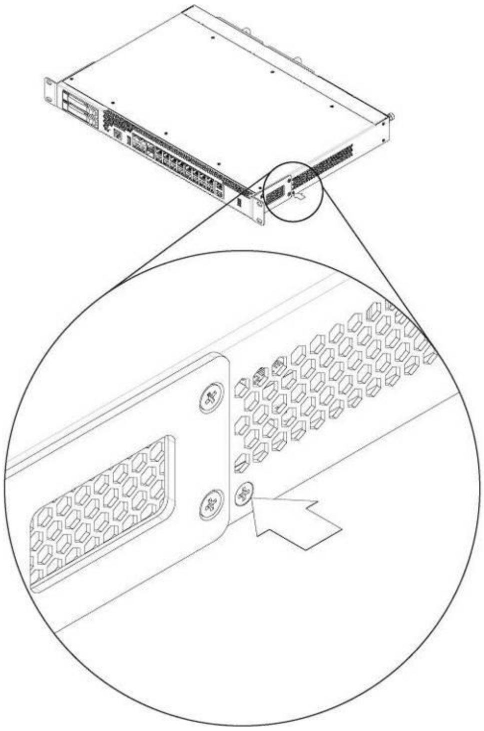


Fig. 18—SMG assembly into housing

During SMG assembly, install the manufacturer-provided screw into place as shown in Fig. 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 M4E1)* in slots shown in Fig. below.

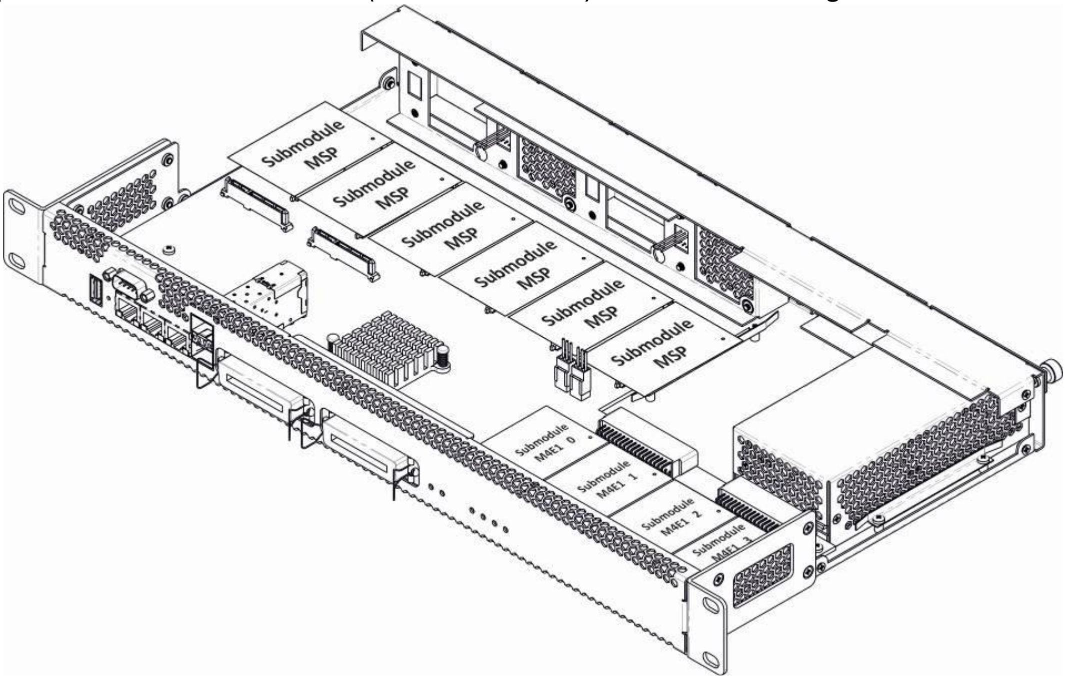


Fig. 19—SMG-1016M submodule location

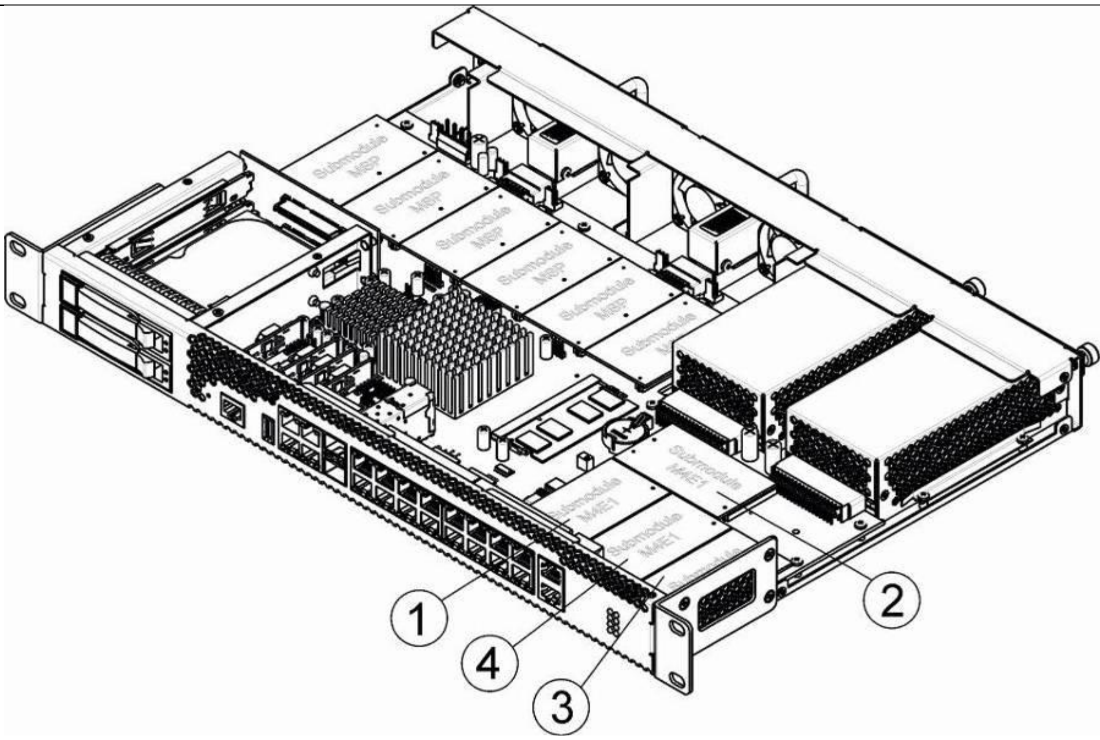


Fig. 20—SMG-2016 submodule location

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. 19, Fig. 20).
6. M4E1 submodule slots are mapped to E1 stream numbers as follows:
   For SMG-1016M

– Submodule M4E1 *0*—E1 Stream *0-3*
– Submodule M4E1 *1*—E1 Stream *4-7*
– Submodule M4E1 *2*—E1 Stream *8-11*
– Submodule M4E1 *3*—E1 Stream *12-15*

For SMG-2016

– Submodule M4E1 *1*—E1 Stream *0-3*
– Submodule M4E1 *2*—E1 Stream *4-7*
– Submodule M4E1 *3*—E1 Stream *8-11*
– Submodule M4E1 *4*—E1 Stream *12-15*

1.12.7 Installation of ventilation units

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

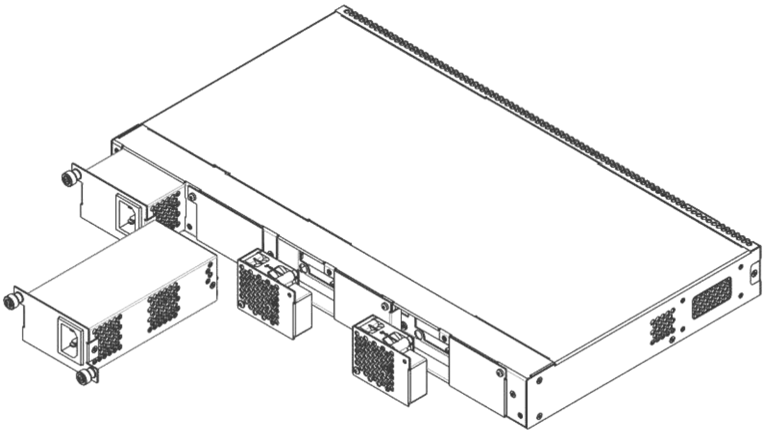


Fig. 21—SMG-1016M ventilation unit Installation into Case

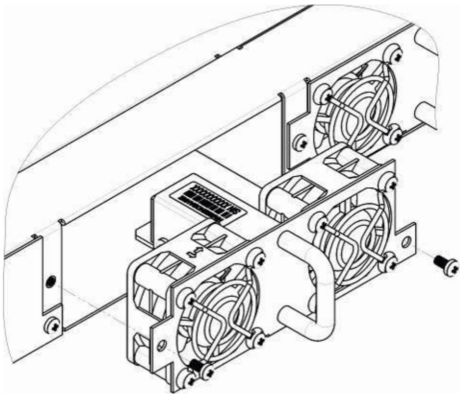


Fig. 22—SMG-2016 ventilation unit Installation into Case

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. 23.

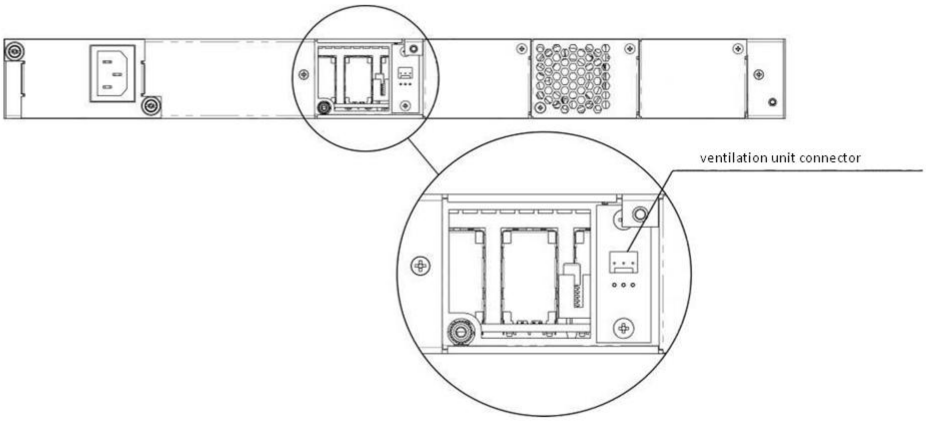


Fig. 23—SMG-1016M ventilation unit connector

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

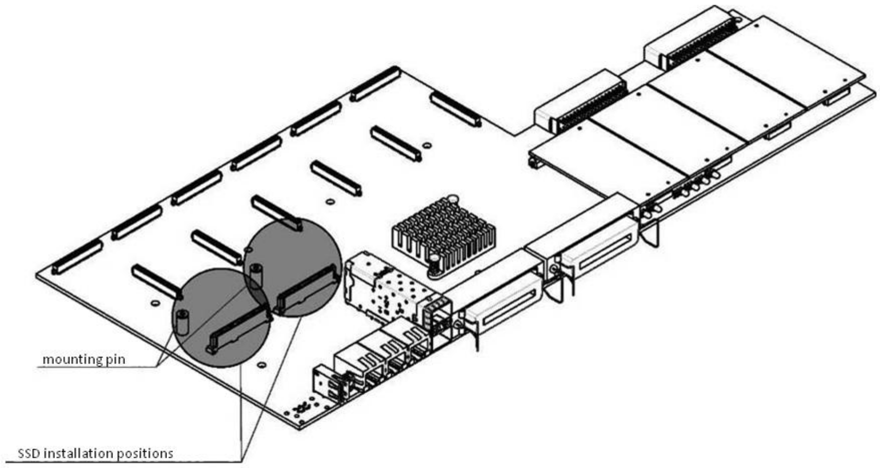


Fig 24—SSD installation procedure

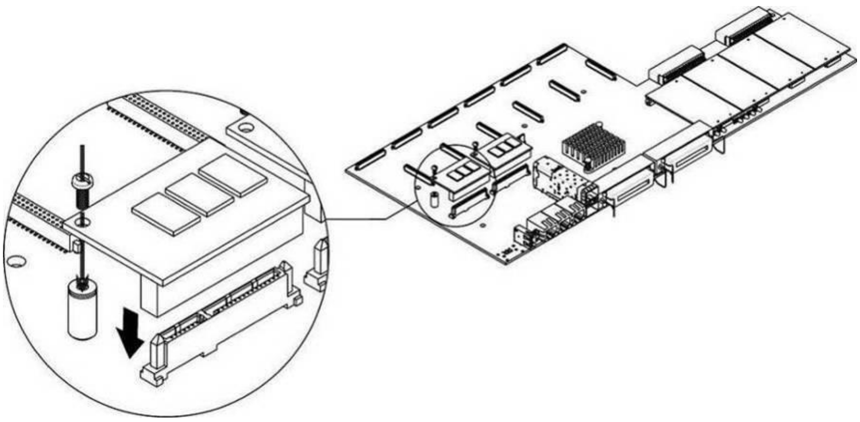


Fig 25—SSD mounting procedure

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 24) 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 24), and if the mounting sleeve is present on the board, fasten the drive with a screw, Fig 25.

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. 10, 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. 26.
3. Secure the drive in the cradle tray, Fig. 27.
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.

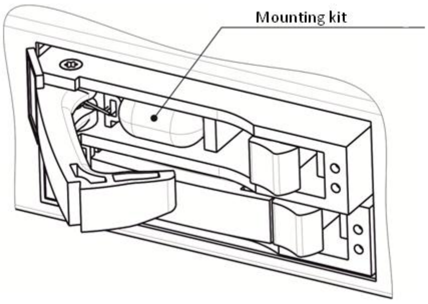


Fig. 26—Mounting kit location in shipping

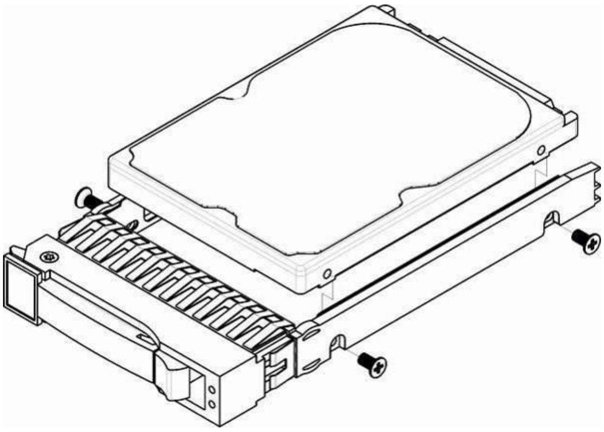


Fig. 27—Mounting SATA drive into cradle tray

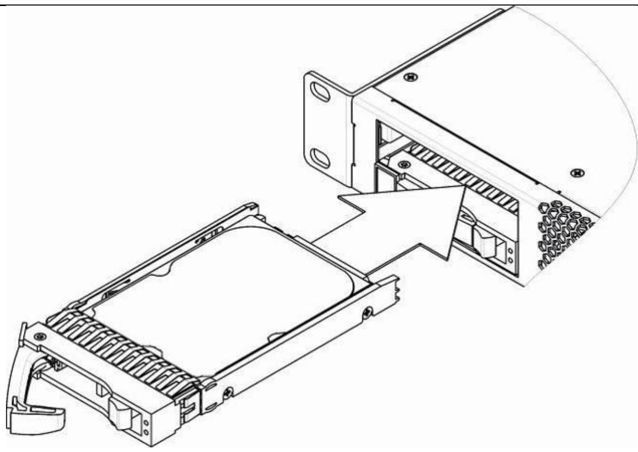


Fig. 28—Installation of SATA drive into device housing

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	225mA
Diameter	20mm
Thickness	3.2mm
Shelf life / expiration date	5 years
Storage conditions	-20 to +35°C

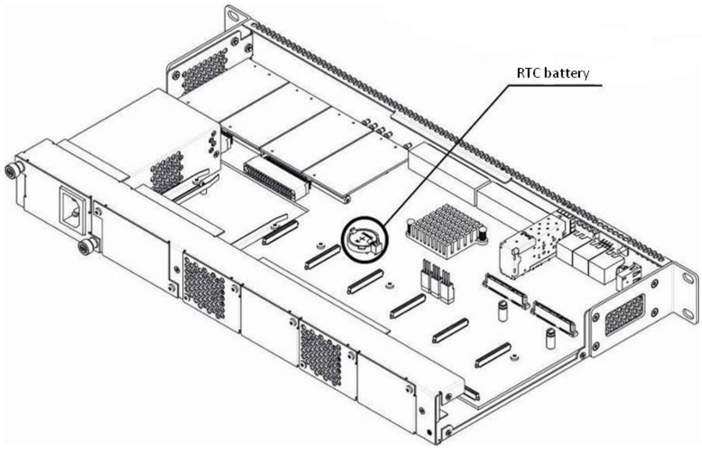


Fig. 29—RTC battery location for SMG-1016M

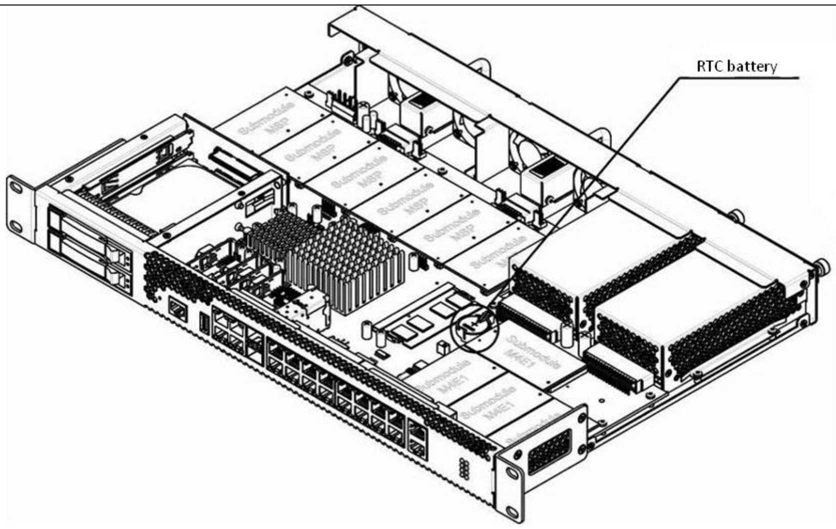


Fig. 30—RTC battery location for SMG-2016

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. 29, Fig. 30) 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 **3.1.25Setting 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.)

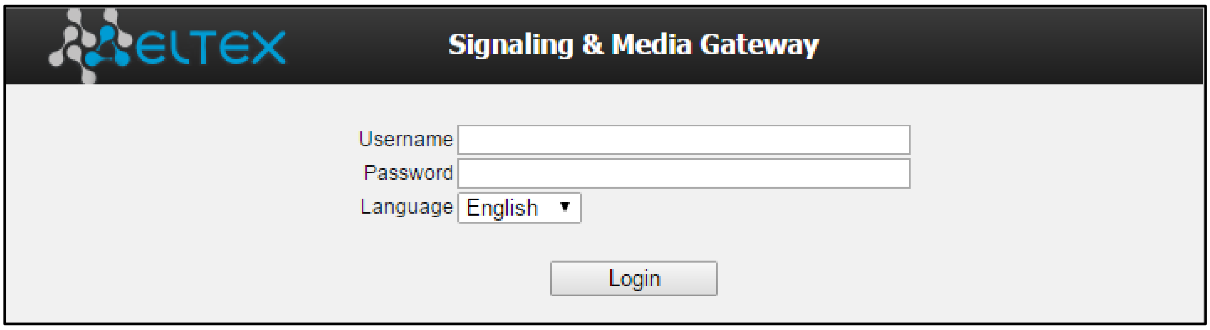
All settings will take effect without gateway restart. To save changes made to configuration into the non-volatile memory, use 'Service/Save configuration into Flash' menu in the web configurator or 'copy running_to_startup' command in CLI.

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.

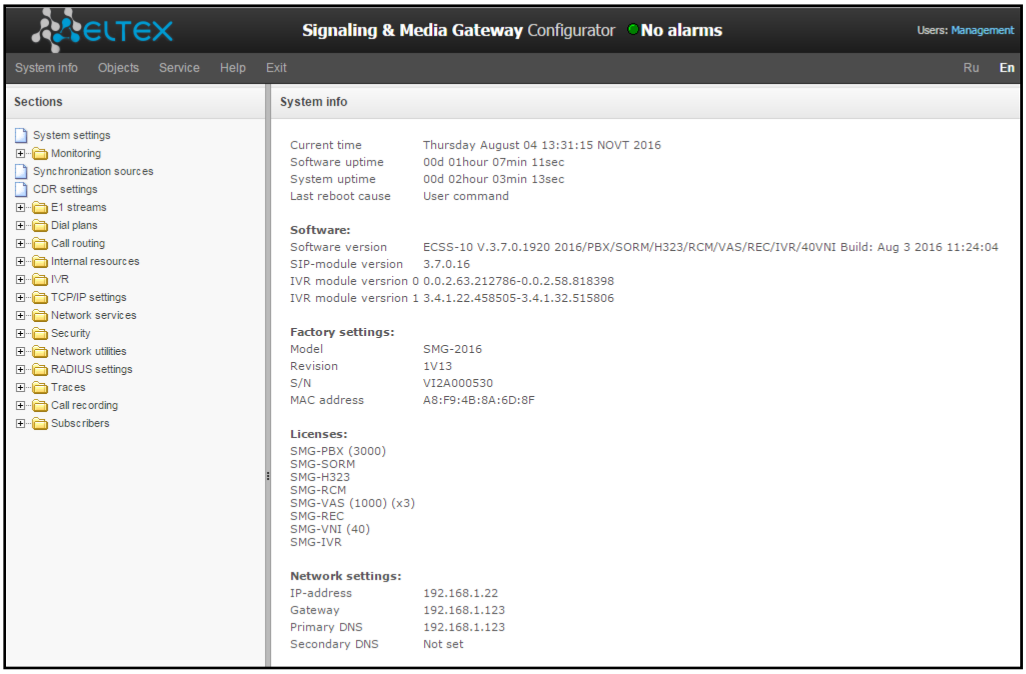


Fig. below shows web configurator navigation elements.

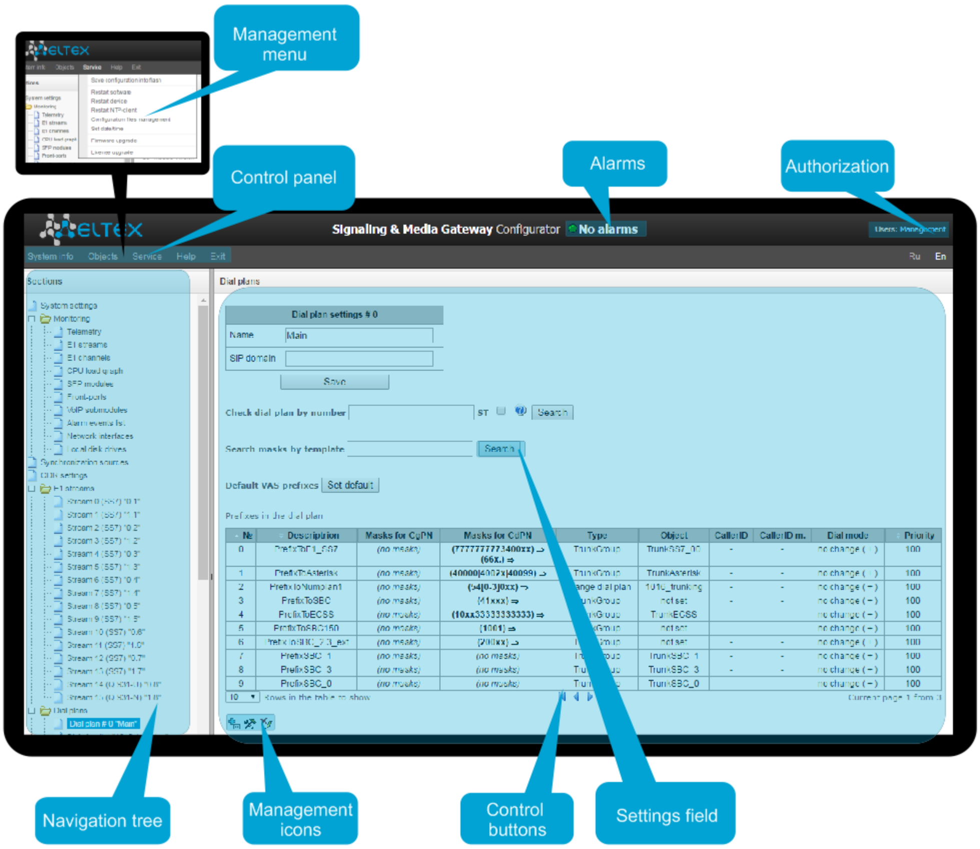


Fig. 31—Web configurator navigation elements

User interface window is divided into several areas.

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

—*Add object*

—*Edit object*

—*Delete object*

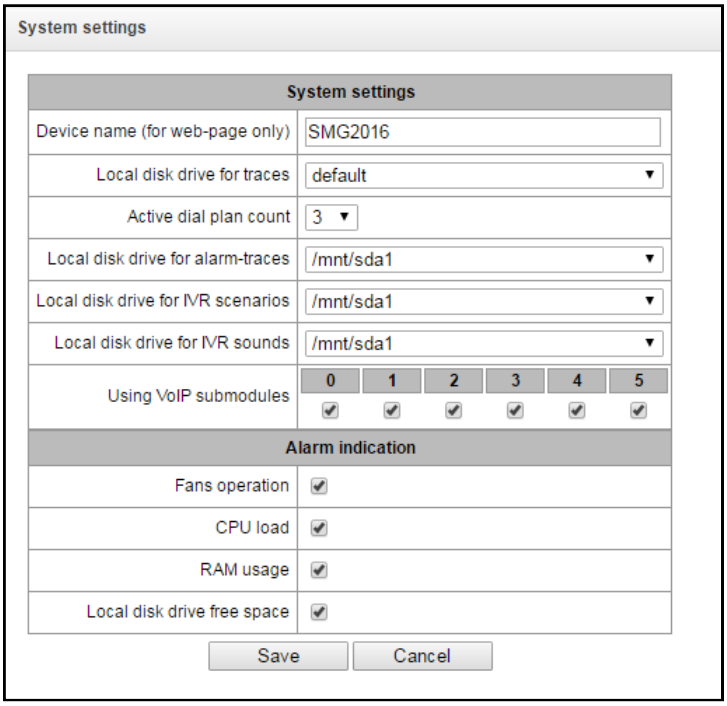
—*View object*

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 parameters



- *Device name*—name of the device. This name is used in the device web configurator header.
- *Path to tracing storage device*—device allows for the debug information (tracing) storage in RAM or on the installed storage device:
  - *default*—debug information is stored in RAM
  - */mnt/sdX*—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.

Tracing file storage is available for SSD/SATA drives only; this function is not available for USB storage devices.

- *Quantity of active numbering schedules*—quantity of simultaneously active numbering schedules; you may configure up to 16 independent numbering schedules with an ability to add subscribers and create custom call routing table.
- *Fault logging device*—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/sdX*—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 (OK—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	SS-7 line group failure
E1-Line alarmed	E1 stream failure
SS7-Link alarmed	SS-7 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, priority of the current source is lower
FTP error. CDR-send failed	Failed to send CDR file to FTP server
Software started	Device software startup

Fault Indication

- *Fan 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 utilization*—when checked, fault indication will appear in case of high CPU utilization (ALARM LED will light up, alarm will be added to alarm log).

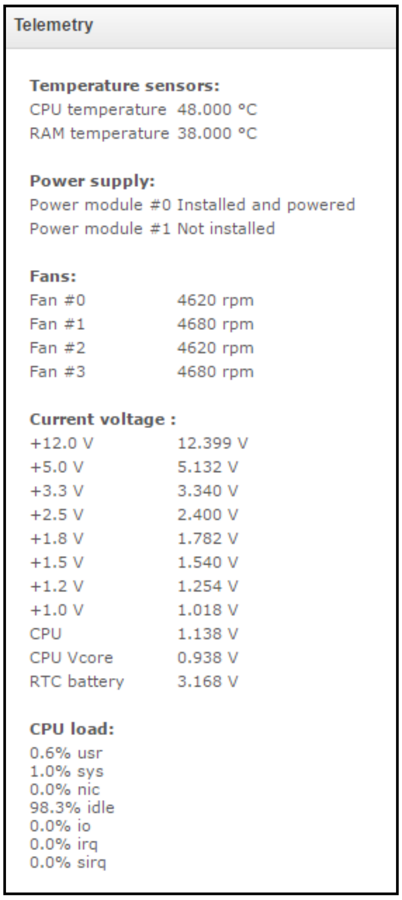
- *RAM utilization*—when checked, fault indication will appear in case of high RAM utilization (more than 75% of the total RAM amount) (ALARM LED will light up, alarm will be added to alarm log).

- *External storage device utilization*—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).

3.1.2 Monitoring

3.1.2.1 Telemetrics

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



Temperature sensors

- *Sensor #0*—CPU temperature sensor readings
- *Sensor #1*—RAM temperature sensor readings

Power supplies

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

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

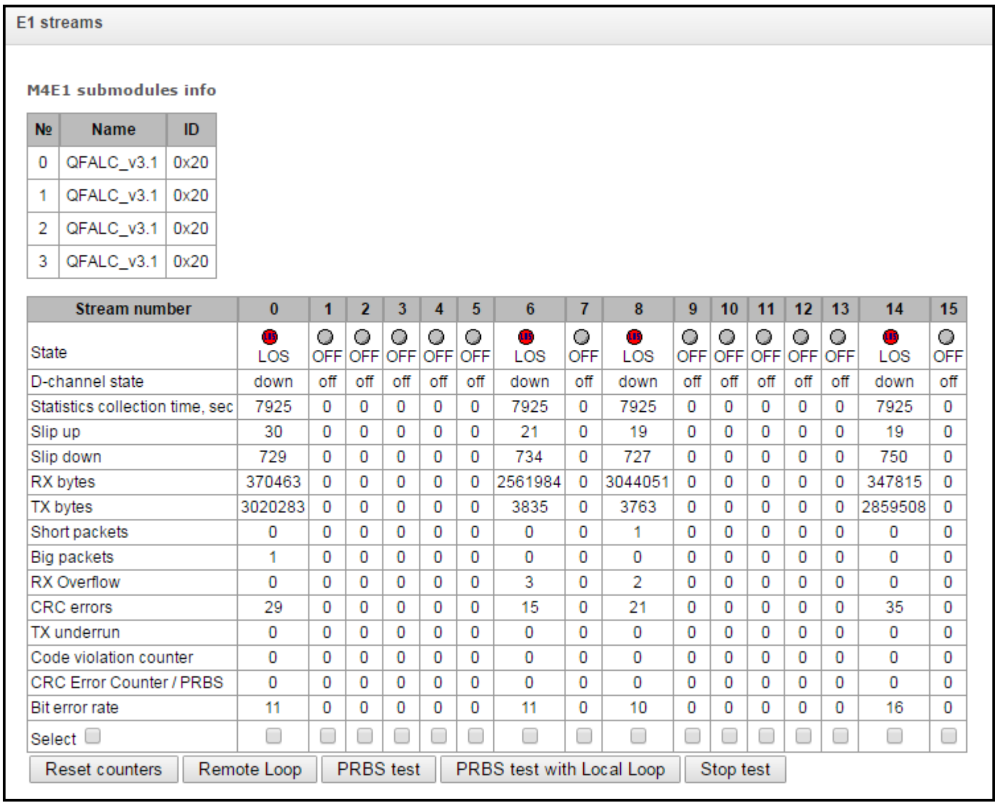
[1] For SMG-1016M only
[2] For SMG-2016 only

Current CPU utilization:

- *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
- *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.


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																

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

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 units)
  - *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)*—time for statistics collection in seconds
- *Positive slips*—number of positive bit slips for the stream
- *Negative slips*—number of negative bit slips for the stream
- *Bytes received*—number of bytes received from the stream
- *Bytes sent*—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
- *Overruns*—buffer overrun error counter
- *CRC errors*—CRC error counter
- *Transmission failures*—stream transmission failure counter
- *Code violations counter*—signal code sequence failure counter
- *CRC Error Counter / PRBS*—CRC error quantity (in 'PRBS test' mode)
- *Bit error rate*—number of bit errors for the stream

- *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 and 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.
- *Disable 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 #
- *Linked 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 #*
- *Linked 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 dial
  - *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 dial
  - *Hold*—subscriber is on hold
- *State timer*—channel last known state duration
- *Incoming SS7 category*—SS7 category of an incoming call before modification
- *CdPN incoming number*—callee number before modification
- *CgPN incoming number*—caller number before modification
- *Outgoing SS7 category*—SS7 category of an incoming call after modification
- *CdPN outgoing number*—callee number after modification
- *CgPN outgoing number*—caller number after modification

Stream state—information table with matrix symbol interpretations

- *State*—stream status:
  - *NONE*—missing M4E1 submodule
  - *OFF*—stream is disabled in configuration
  - *ALARM*—M4E1 submodule initialization error
  - *LOS*—signal is lost
  - *AIS*—alarm state indication signal (signal that contains all units)
  - *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

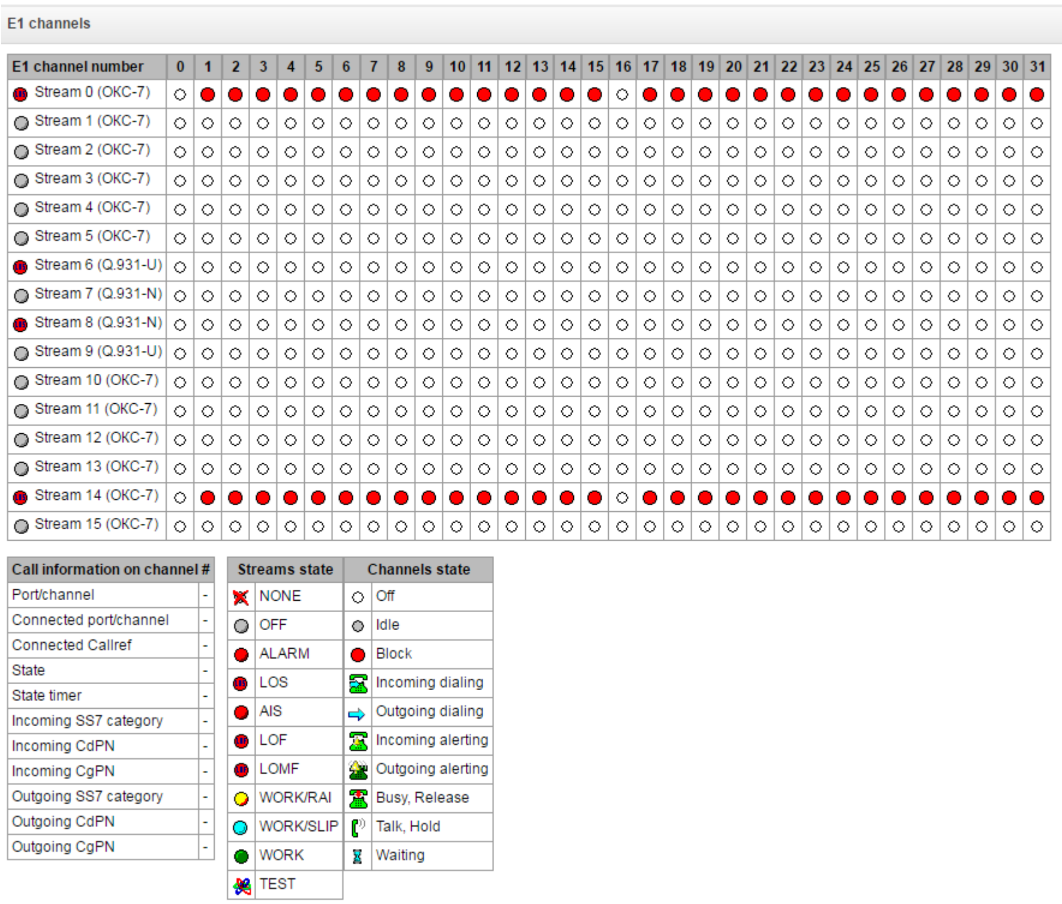
- *State*—channel status:
  - *OFF*—channel is disabled in configuration
  - *Idle*—channel is in initial state
  - *Block*—channel is blocked
  - *Incoming dialing*—incoming call dialling
  - *Outgoing dialing*—outgoing call dialling
  - *Incoming alerting*—incoming occupation, callee is disengaged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

If one of the M4E1 submodules is missing, the message *'M4E1 submodule is not installed, channel monitoring is unavailable'* will be generated.

Channel state updates in 5 seconds interval.

Stream 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 (SS-7). Next, in 'SS-7 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.



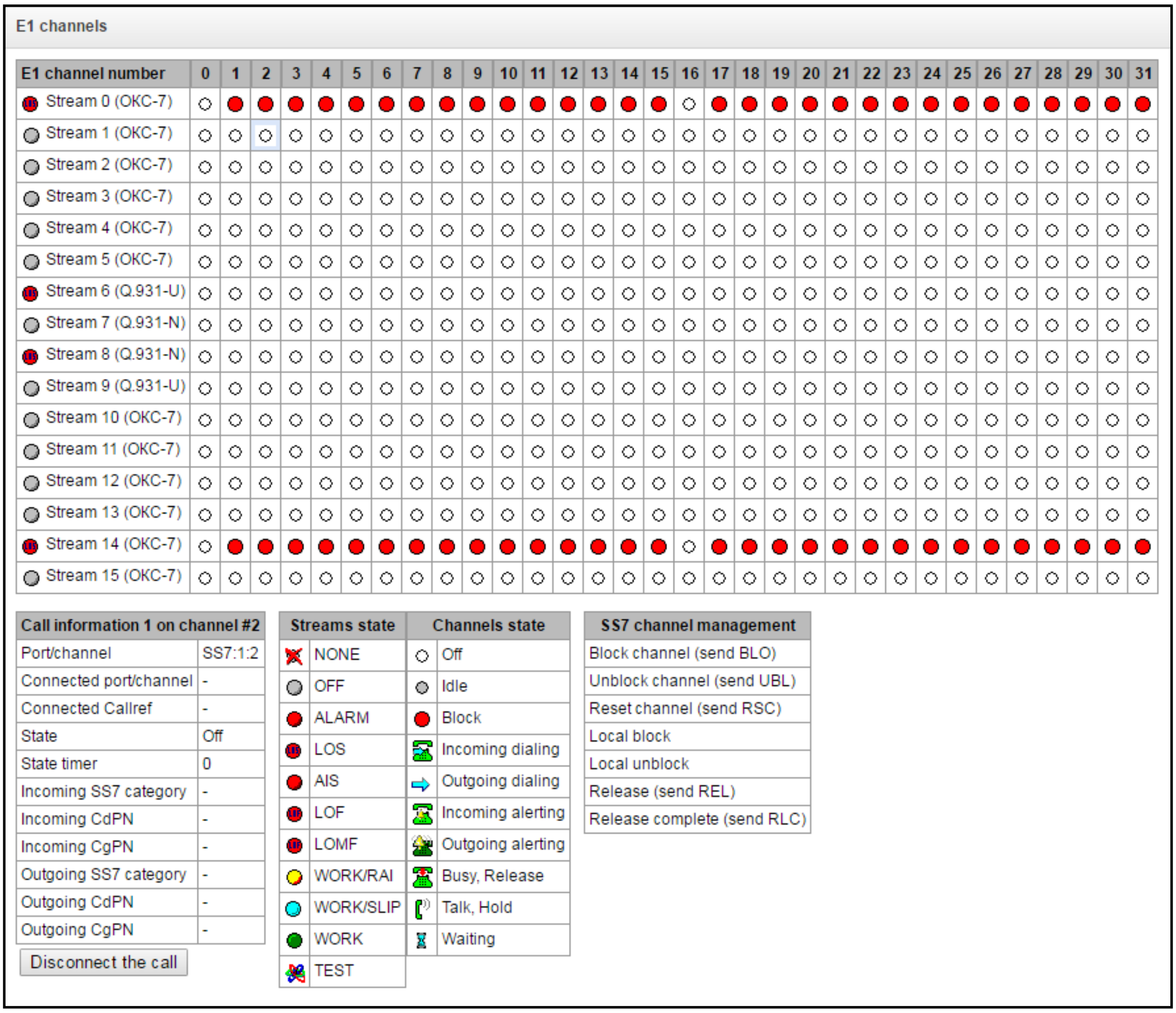
SS-7 link management—SS-7 signal link management table

- *Send LUN*—send link uninhibit signal
- *Send LIN*—send link inhibit signal
- *Send LFU*—send link forced uninhibit signal
- *Set 'Overload' state*—set signal link overload state
- *Cancel 'Overload' state*—cancel signal link overload state
- *Set 'CPU local failure' state*
- *Cancel 'CPU local failure' state*
- *Initiate normal signal link startup*
- *Initiate emergency signal link startup*
- *Shutdown signal link*

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 (SS-7). Next, in 'SS-7 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.

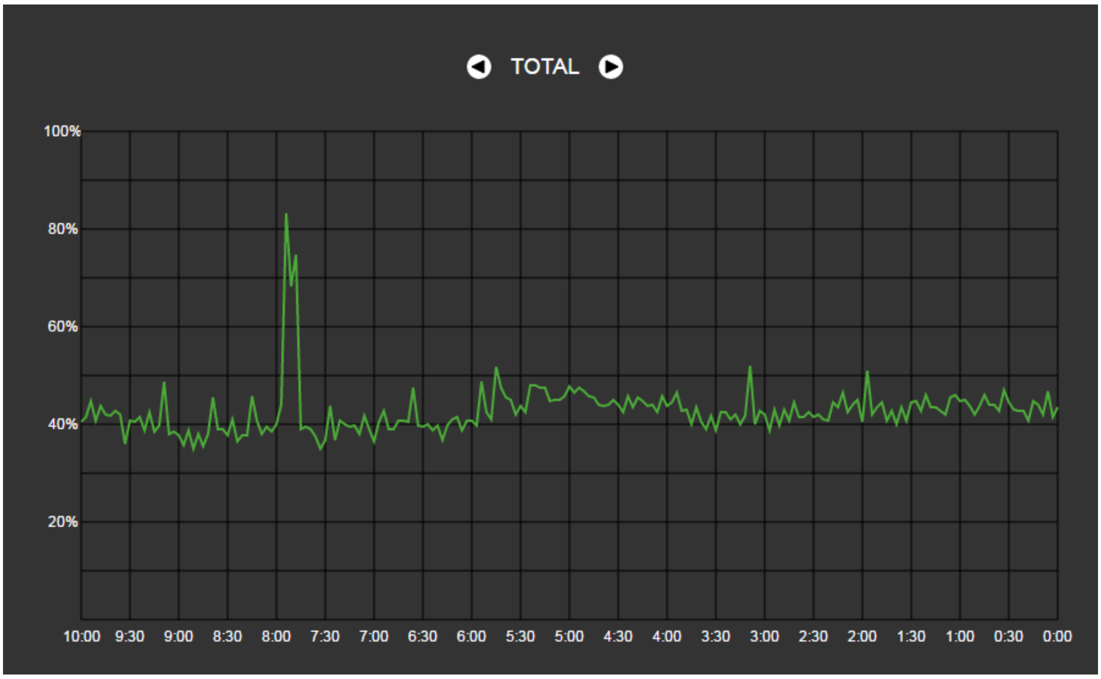


SS-7 channel management—SS-7 (CIC) channel management table:

– *Block channel (send BLO)*—send BLO message to block channel
– *Unblock channel (send UBL)*—send UBL message to unblock channel
– *Reset to initial (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 acknowledgement (send RLC*)—send RLC message

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.

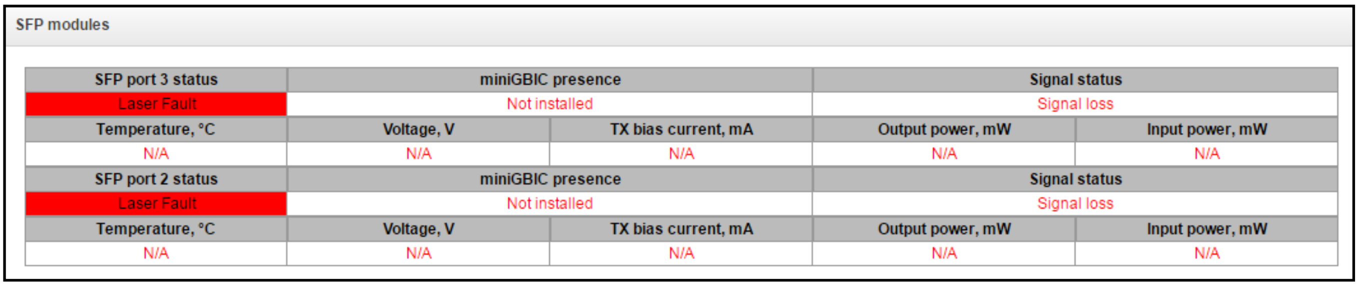


To navigate between specific parameters in monitoring charts, use buttons ◀ and ▶. To facilitate visual identification, all charts have different colors.

– *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.



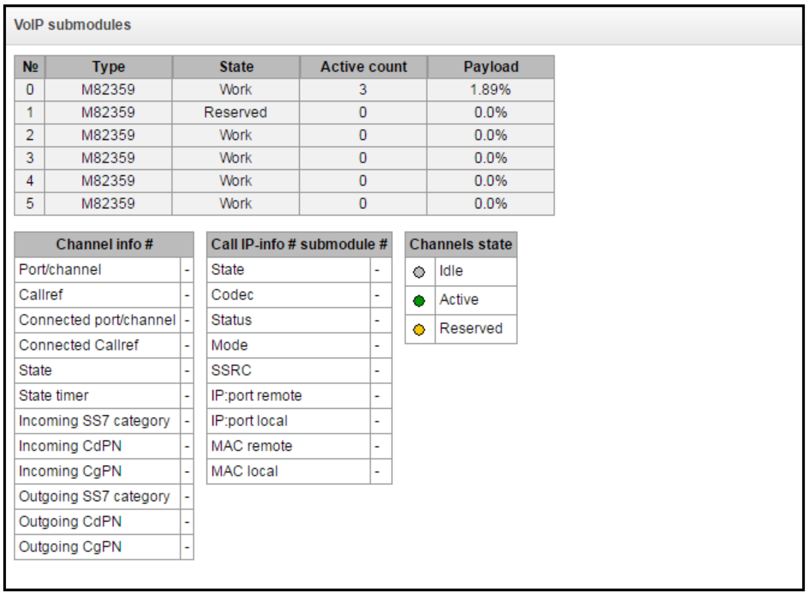
SFP modules

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:
  - *SFP module installed*—indication of module installation (module is installed, module is not installed)
  - *Signal state*—signal loss indication (signal is lost, in operation)
  - *Temperature, °C*—optical module temperature
  - *Power, 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 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	-

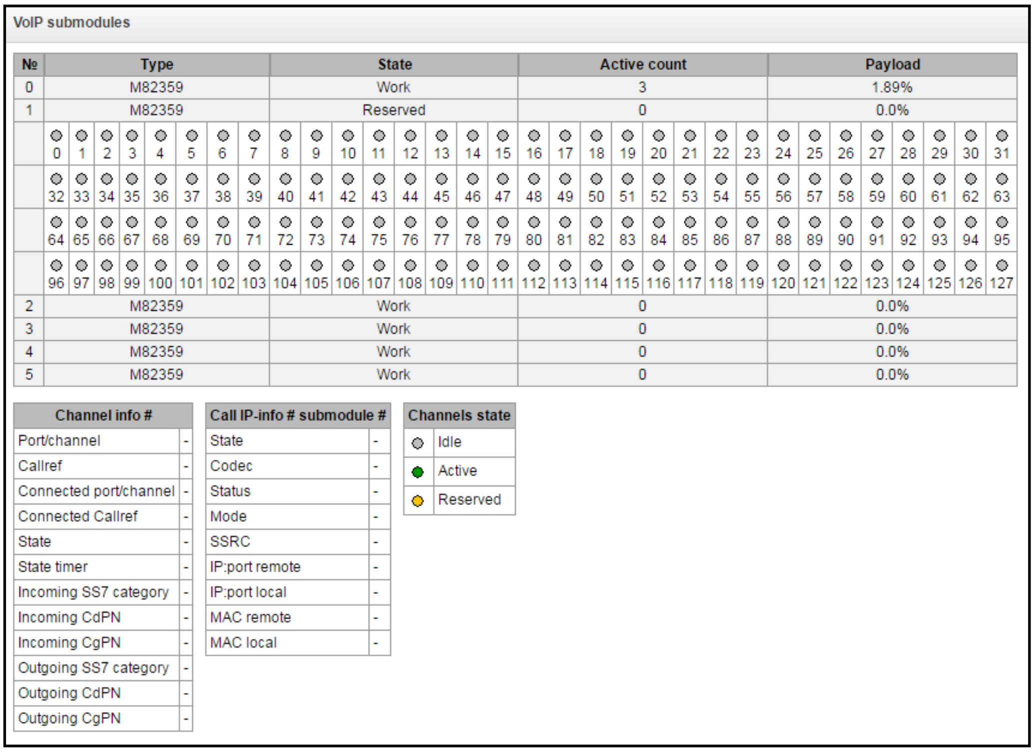
Call IP-info # submodule #	
State	-
Codec	-
Status	-
Mode	-
SSRC	-
IP:port remote	-
IP:port local	-
MAC remote	-
MAC local	-

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 form CPU after submodule load
  - *Failed*—no response from submodule
  - *Work*—submodule normal operation
  - *Recovery*—no control packets coming from submodule

  – *Reserved*—submodule is reserved for SORM
  – *SSW.Sorm*—submodule is used by SORM agent
- *Active connections*—number of active connections on the submodule at the given moment
- *Load*—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%
2	M82359	Work	0	0.0%
3	M82359	Work	0	0.0%
4	M82359	Work	0	0.0%
5	M82359	Work	0	0.0%

Channels of submodule 1: 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

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:
  – Signalling protocol (VoIP)
  – Port location VoIP submodule #/Channel #
- *Callref*—internal call identifier
- *Linked port/channel*—linked port/channel data:
  – Linked port signalling protocol (PRI/SS7/VoIP)
  – Linked port location Stream #:Channel # for PRI/SS7 or VoIP submodule #:VoIP channel #
- *Linked 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 dial
  – *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 dial
  – *Hold*—subscriber is on hold
- *State timer*—channel last known state duration
- *Incoming SS7 category*—SS7 category of an incoming call before modification

– *CdPN incoming number*—callee number before modification
– *CgPN incoming number*—caller number before modification
– *Outgoing SS7 category*—SS7 category of an incoming call after modification
– *CdPN outgoing number*—callee number after modification
– *CgPN outgoing number*—caller number after modification

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

If SORM license is used, one of the submodules will be dedicated for combined tracking provisioning (see Section 1.1Application and Appendix E. Provisioning of SORM functions). At that, the submodule state will be 'Reserved', channel monitoring of this module will not be performed in accordance with requirements of the Order no. 268 dated 19.11.2012 issued by the Ministry of Communications and Mass Media (MinComSvyaz) of the Russian Federation.

3.1.2.7 Fault alarms Fault events log

When a failure occurs, related information containing the fault stream number, SS-7 line group, 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.

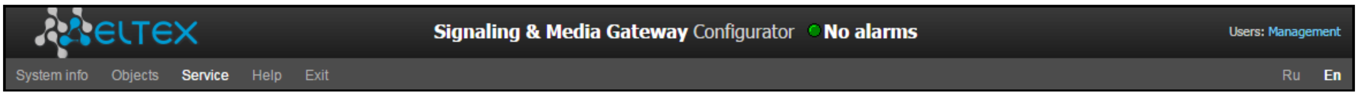


Table 17—Alarm message examples

Alarm message	Meaning
Configuration has not been read	Configuration file error

No communication with SIP module	Failure of a software module responsible for SIP operation
SS-7 line group (linkset) is not in operation	SS-7 line group failure
E1 stream failure	E1 stream failure
SS-7 link failure	SS-7 signal channel failure
Synchronization from the lower priority source	Synchronization with a local source All defined sources are inoperable
E1 stream remote fault	E1 stream remote fault
Synchronization from the lower priority source	Primary synchronization source is lost, priority of the current source is lower
Failed to send CDR files via FTP	Failed to send CDR file to FTP server
No communication with VoIP submodule	No communication with SM-VP submodule
Operating memory is low	High RAM utilization alarm
No power from power supply	Primary main is missing on one of the power supply units
No communication with H323 module	Failure of a software module responsible for H.323 operation
High CPU temperature	Fault state—high CPU temperature
SIP interface does not respond to OPTIONS requests	One of the SIP interfaces is not available
High CPU utilization	Fault state—high CPU utilization
Fan operation problem	One or multiple fans are inoperable
Low free space on disk	Low free space on one of the external storage devices
'TrunkGroupName' exceeds CPS threshold	Number of calls coming to one of the trunk groups per second exceeds the value defined by 'Alarm CPS value' option

In 'Fault events log' menu, you may find the list of alarm events arranged by time or date.

Local alarm-events list

Clear Clear the alarm events list

№	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

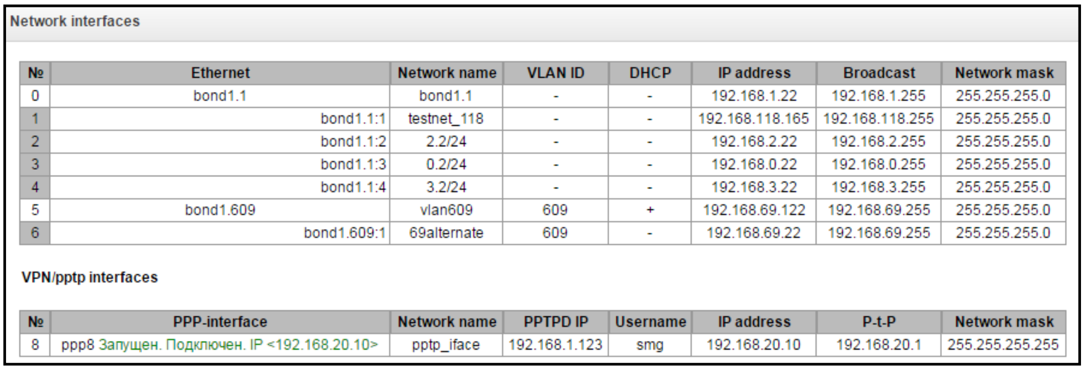
Alarm table:

- *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, SS-7 line group is not in operation
  - *STREAM*—critical fault, E1 stream is in operation
  - *SM-VP DEVICE*—fault, SM-VP module failure
  - *SS7LINK*—SS-7 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
- *State*—fault state status:
  - *critical fault, flashing red LED*—fault requires immediate intervention of the service personnel, affects device operation and provisioning of communication services
  - *fault, red LED*—non-critical fault, also requires intervention of the service personnel
  - *warning, yellow LED*—fault does not affect provisioning of communication services
  - *OK, green LED*—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*—SS-7 line group (linkset) XX is not in operation, where XX is SS-7 line group 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*—SS-7 link failure Linkset XX, E1 stream YY, where XX is SS-7 line group number, YY is a signal channel number in SS-7 group

– *TRUNK-CPS*—'XX' trunk group exceeds CPS threshold, where XX is a trunk group name

3.1.2.8 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

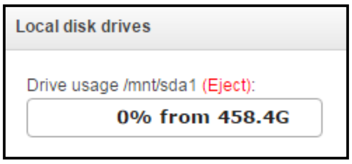
– *Ethernet*—Ethernet interface name
– *Network name*—name that the current network settings are associated with
– *VLAN ID*—virtual network identifier (for tagged interface)
– *DHCP*—DHCP usage status, allows to obtain network settings automatically (DHCP server is required in the operator network)
– *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

3.1.2.9 Storage media information

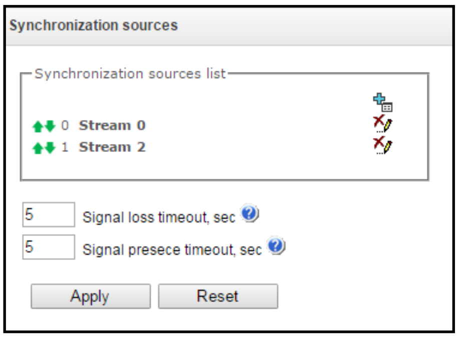
This section contains information on the connected storage media.



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

3.1.3 Synchronization sources

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).

To generate the list, use the following buttons:
—*'Add source'*; —*'Remove'*.

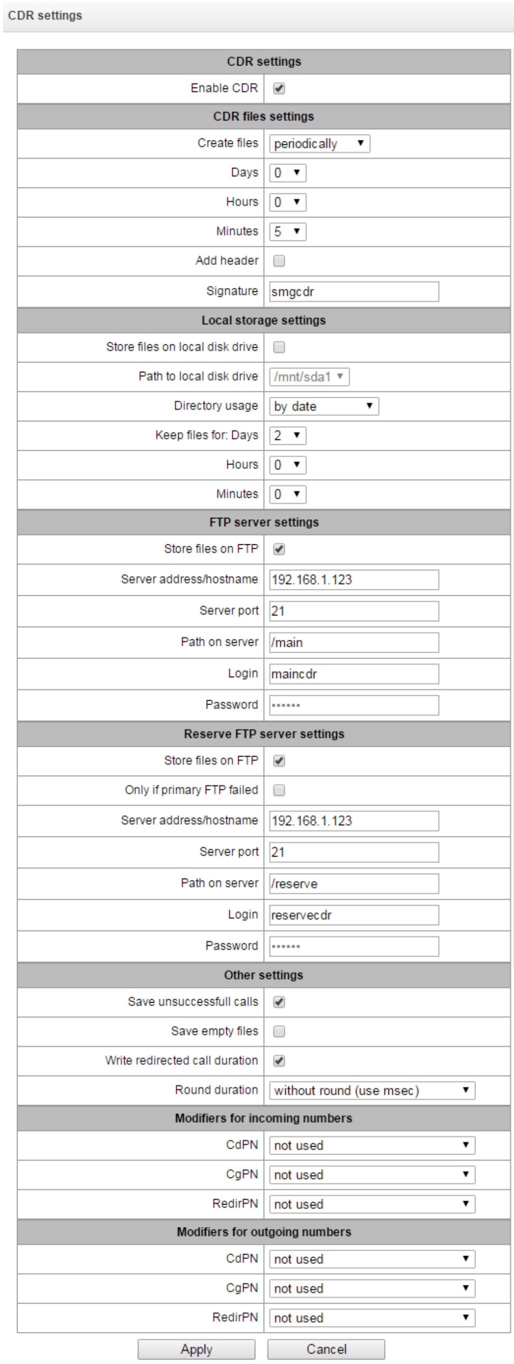
To change the source priority, use *'Up/Down'* buttons located next to each source. The highest priority value is 0, the lowest priority value is 14.

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

If D-channel is configured for the stream originating the synchronization signal (for SS-7 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

In this section, you may configure saving parameters for call detail records.



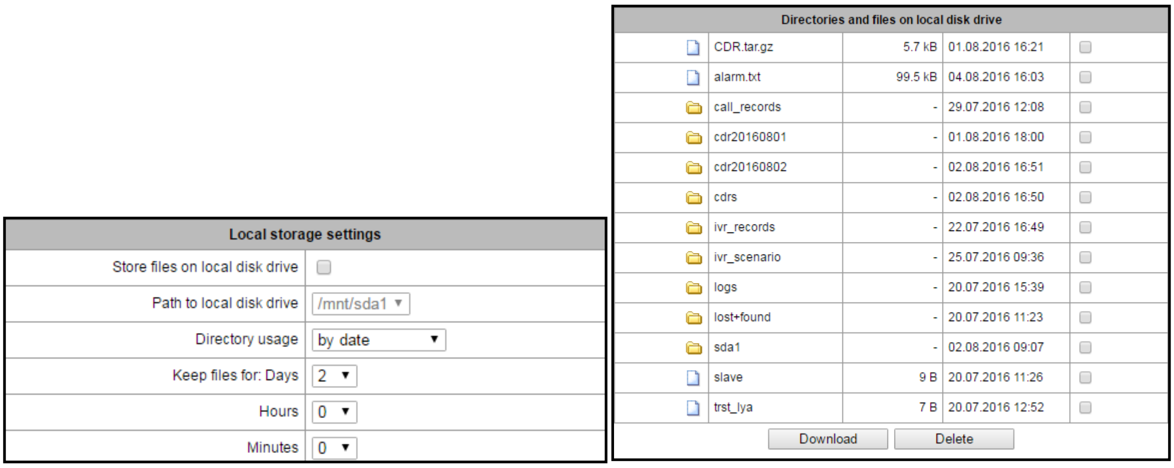
CDR is a detailed call record that enables saving history of calls performed through SMG.

CDR saving parameters

- *Enable saving CDR*—when checked, the gateway will generate CDRs
- *Generation mode*—CDR file creation mode:
  - *defined period*—CDR file will be created upon the expiry of the specific period from the device startup
  - *daily*—CDR file will be created once a day at the defined time
  - *hourly*—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.
- *Discriminant*—specify distinctive feature that will facilitate identification of the device that created the record.

Local storage settings

- *Save on local disk*—when checked, save CDRs on local storage media.
- *Path to local disk*—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'*.



- *Directory utilization*—select directories for CDR data storage
  - *directories 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.
- *Data storage time*: *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. Storage space for CDR files amounts to 30Mb. When the memory is filled within the specific margins, the fault will be indicated. For CDR file saving indication, see Section 1.5.2.

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

FTP server settings

- *Save to FTP*—when checked, CDRs will be transferred to FTP server
- *FTP server*—FTP server IP address
- *FTP port*—FTP server TCP port
- *Path to file*—defines path to FTP server folder for CDR storage
- *FTP login*—username for FTP server access
- *FTP password*—user password for FTP server access

Redundant 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.

- *Save to FTP*—when checked, CDRs will be transferred to a redundant FTP server
- *FTP server*—redundant FTP server IP address
- *FTP port*—redundant FTP server TCP port
- *Path to file*—defines path to a redundant FTP server folder for CDR storage
- *FTP login*—username for redundant FTP server access
- *FTP password*—user password for redundant FTP server access

Miscellaneous 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.
- *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.
- *Duration rounding*—this option specifies duration rounding mode in CDRs:
  - *Rounding up*—call duration rounding mode; call duration value will be rounded up when it exceeds 330ms;
  - *Rounding down*—call duration rounding mode; call duration value will be rounded down when it exceed 850ms.
  - *Without rounding (track of ms)* —in the mode, call duration will be not rounded and it will be recorded within the accuracy of milliseconds.

Incoming number modifiers

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

- *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.

Outgoing number modifiers

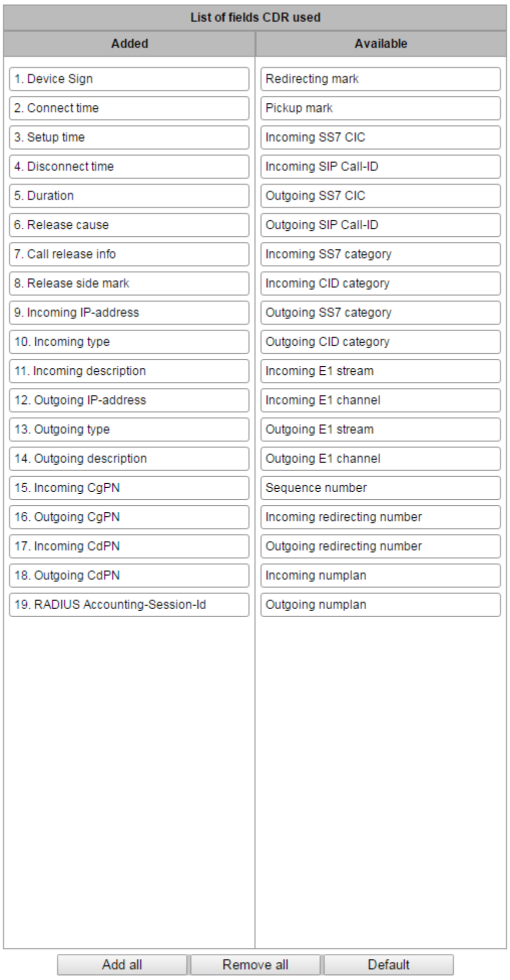
Outgoing number modifiers—modifiers that modify CDR fields containing subscriber numbers and apply to these fields after a call proceeds through the numbering schedule.

- *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 used CDR fields

You may select fields that will be written in CDR files and you may configure their order. All available for adding fields are displayed in 'Available' column. Fields and their CDR filing order are displayed in 'Added' column.



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;
– By default – basic set of the fields stays in added fields (the list of fields see in 3.1.4.2**Ошибка! Источник ссылки не найден.**section).

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

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).
– Nextline - CDRrecords in the form of fields separated by ';'. Basicsetoffieldsisfollowing:
  – Discriminant;
  1. Connection establishment time in YYYY-MM-DD hh:mm:ss format (for unsuccessful calls, this parameter is equal to the disconnection time).
  2. Call duration, seconds
  3. Cause of disconnection according to ITU-T Q.850
  4. Call statuse in case of disconnection

– Caller information:
  5. IP address
  6. Source type
  7. Description - subscriber/trunk name (TG)
  8. Caller number on input
  9. Caller number on output
– Callee information:
  10. IP address
  11. Destination type
  12. Subscriber/trunk name (TG)
  13. Callee number on input
  14. Callee number on output
  15. Call received time in format: YYYY-MM-DD hh:mm:ss;
  16. Connection termination time in format: YYYY-MM-DD hh:mm:ss.

Source and destination types

– *SIP-user*—SIP subscriber
– *trunk-SIP*—SIP trunk
– *trunk-SS7*—SS-7 trunk
– *trunk-Q931*—ISDN PRI trunk
– *trunk-H.323*—H.323 trunk

Call status types 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.

Redirection tag
– *normal*—call w/o redirection
– *redirecting*—redirected call (call containing the redirecting number after the redirection)
– *redirected*—received call that was redirected

3.1.4.3 CDR file example

Example of CDR file containing 2 records (header saving and discriminant are enabled):

SMG1016. CDR. File started at '20111024093328'

27;2011-10-24 09:33:37;2;16;user answer;192.168.16.200;sip-user; undef;520001;520001;
192.168.16.200;sip-user;undef;520000;520000;2011-10-24 09:33:35;2011-10-24 09:33:39;

27;2011-10-24 09:38:56;242;16;user answer;192.168.16.202;sip-user;undef;7000000;7000000;
192.168.16.200;sip-user;undef;520000;520000;2011-10-24 09:38:45;2011-10-24 09:42:58;

3.1.4.4 CDR structure for various settings

Redirection tag value may be as follows:
– redirecting—the caller has redirected a call to the callee
– redirected—call initiated by the caller has been redirected to another subscriber.

Pick up tag

Tagofdisconnectioninitiator–sidewhere 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/outgoingSS7 CIC - numberCICfor incoming/outgoing call. Ifacallwasn’tperformedvia SS7 interface field will be empty;
Incoming/outcomingSIPCall-ID - Call-IDof incoming/outcoming call. If a call wasn’t performed via SIP field will be empty;

Incoming/outcomingSS7 category - category ofSS7 calleroninput (before modification on incoming TG) or on output (after modifications of incoming and outgoing TG);

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

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

Incoming/outcomingE1 channel– number of incoming/outgoing E1 channel. If a call wasn't performed via E1 field will be empty;

Serial number of record–two numbers separated by hyphen. First is time taggen erated during the device start, the second – sequence number of the CDR record.

Incoming/outcoming number off or warder – for warder number on input (up to modification on incoming TG) or on output (after all modifications in incoming and outgoing TG;

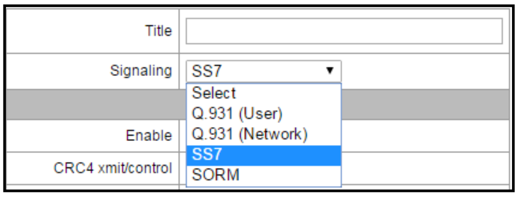
RADIUS Accounting-Session-Id - 'Acct-Session-Id' attribute value transmitted to RADIUS.

Incoming/outcomingdialplan– dial plan through which call was transmitted and received.

3.1.5 E1 streams

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

3.1.5.1 Signalling protocol selection

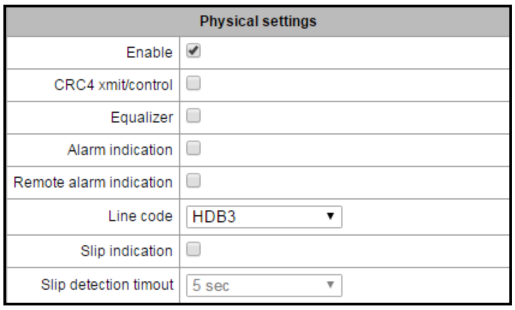


To select signalling protocol for a stream, use the *'Signalling protocol'* drop-down list.

Device supports the following signalling protocols:
- Q.931 (User, Network);
- SS7 (ОКС-7);
- QSIG for subscriber name transmission;
- СОРМ;
- V5.2 LE[1].

3.1.5.2 Configuration of physical parameters

Physical parameters:



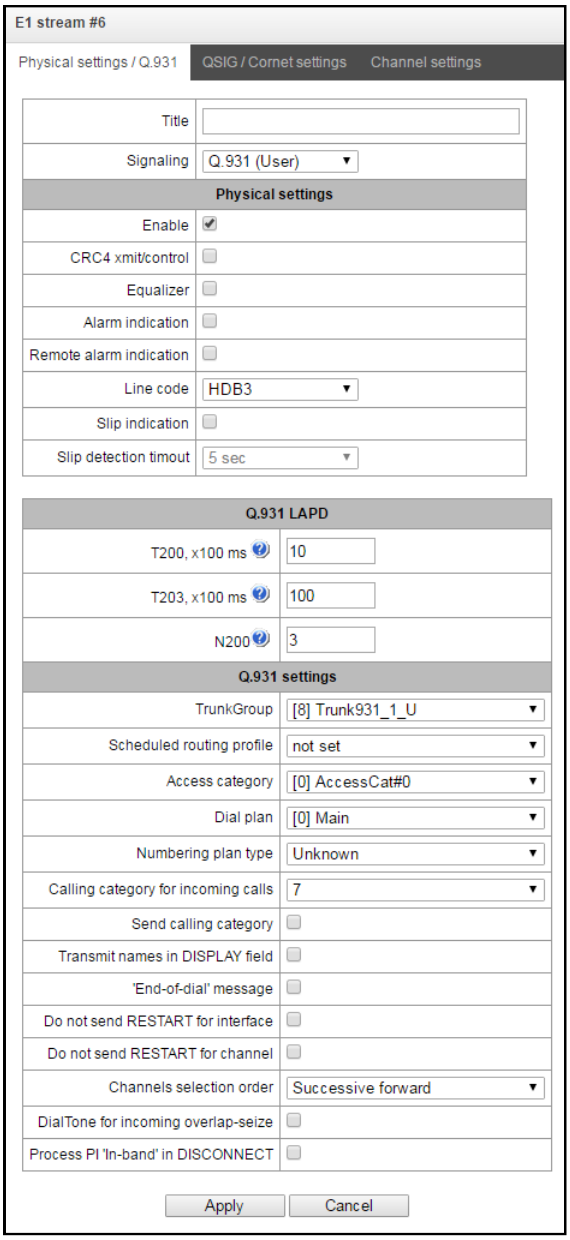
- *Name*—E1 stream name.
- *Enabled*—physically enable stream.
- *CRC4 transmission/control*—CRC4 check sum generation during transmission and control during reception.
- *Equalizer*—when checked, transmitted signal will be amplified.
- *Alarm indication*—when checked, fault indication will appear in 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).
  - *Linear code type*—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.

[1] Not supported in the current firmware version.

– *Slip detection timeout*—stream parameter polling frequency; if the slip is detected in that stream, the gateway will indicate an alarm for the duration of this timeout.

3.1.5.3 Q.931 signalling protocol configuration

3.1.5.3.1. '*Physical parameters/Q.931*' tab



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

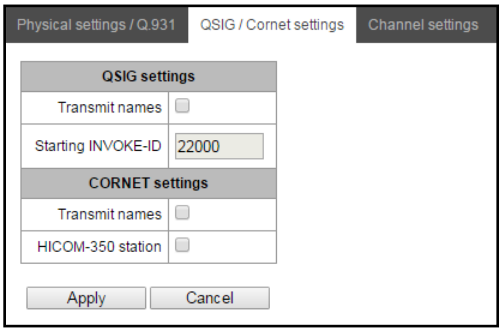
– *Trunk group* — name of a trunk group, that E1 stream belongs to.
– *Scheduled routing profile* — select scheduled routing profile from the list of existing profiles.
– *Access category* — select access category.
– *Numbering schedule* — define numbering schedule that will be used for routing of the call received from this port (necessary for numbering schedule negotiation).

- *Numbering schedule type* — define ISDN numbering schedule type. To use common numbering schedule E.164, select *'ISDN/telephony*'.
- *Caller ID category for incoming calls* — Caller ID category assigned to calls received from this port.
- *Caller ID category transmission* — 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.

- *Send/receive subscriber name in DISPLAY* — when Q.931 (Network) signalling protocol is selected, this field will be sent or received. Field value for transmission is taken from the incoming field 'display' during Q.931 incoming call or from field 'user name' during SIP incoming call. During reception, this field is transferred to *user name* field during SIP incoming call or to *display* field, when Q.931 (Network) protocol is selected.
  If Q.931 (User) protocol is selected, this field will be received only. During reception, this field is transferred to *user name* field during SIP incoming call or to *display* field, when Q.931 (Network) protocol is selected.
- *'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, dialling timeout for the next digit).
- *Do not issue interface RESTART* — when checked, gateway will not send RESTART message into the line when the stream is restored (channel level LAPD is established).
- *Do not issue channel RESTART* — 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.
- *Channel* engagement — 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 neighbouring PBXes, we recommend to set inverse channel engagement types.
- *Issue DialTone during incoming overlap engagement* — 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 clearback IVR voice message transmission, otherwise this field is ignored.

3.1.5.3.2. *QSIG parameters/Cornet* tab



QSIG parameters — QSIG signalling protocol parameters

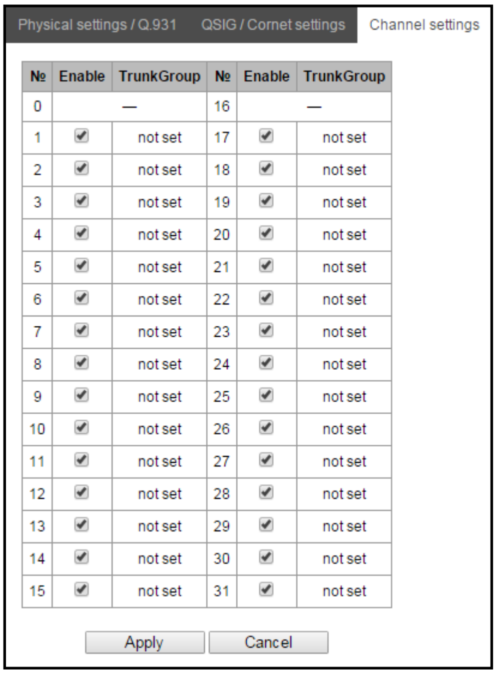
- *Send subscriber name*—when checked, send subscriber name via QSIG protocol during a call.
- *Initial INVOKE-ID*—setting operation call initial identifier (used as a reference number for unique operation call identification).

CORNET parameters — CORNET signalling protocol parameters

- *Send subscriber name* — when checked, send subscriber name via CORNET protocol during a call.
- *ATC HICOM-350* — define name transmission mode via CorNet protocol with adjustments for PBXHICOM-350.

3.1.5.3.3. *Channel usage* tab

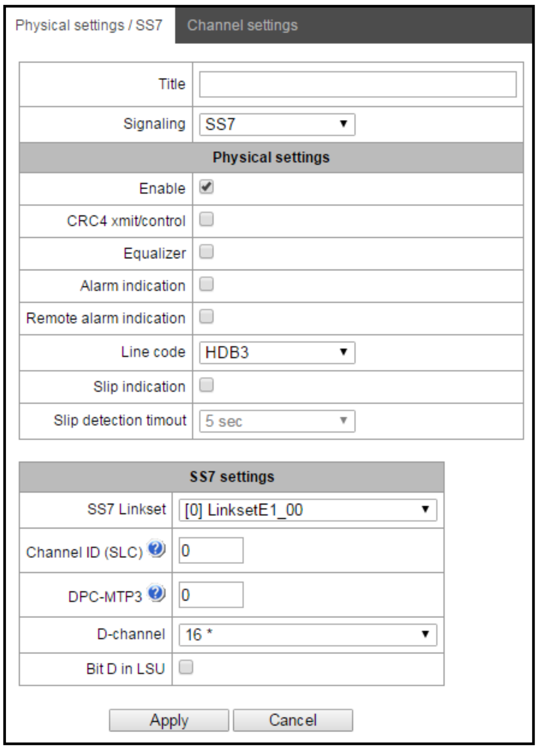
Use this tab to configure channel usage—select the checkbox next to the used channel number.



№	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

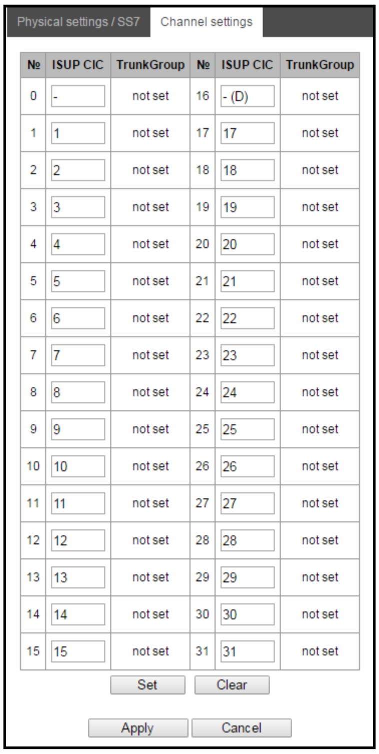
3.1.5.4 SS-7 signalling protocol configuration

3.1.5.4.1. *Physical parameters/SS7* tab



SS-7 parameters

- *SS-7 line group*—linkset selection (SS-7 line group).
- *Channel identifier (SLC)*—signal line identifier in SS-7 line group.
- *MTP3 opposite code (DPC-MTP3)*—code of the opposite 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**).
- *CI for D-channel*—number of the channel interval that will be used for signalling transmission.
- *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).

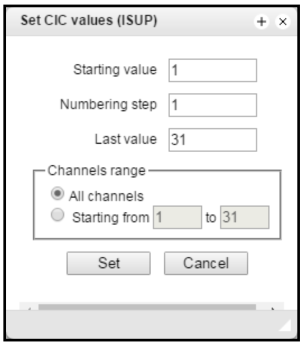


3.1.5.4.2. ***Channel settings*** tab

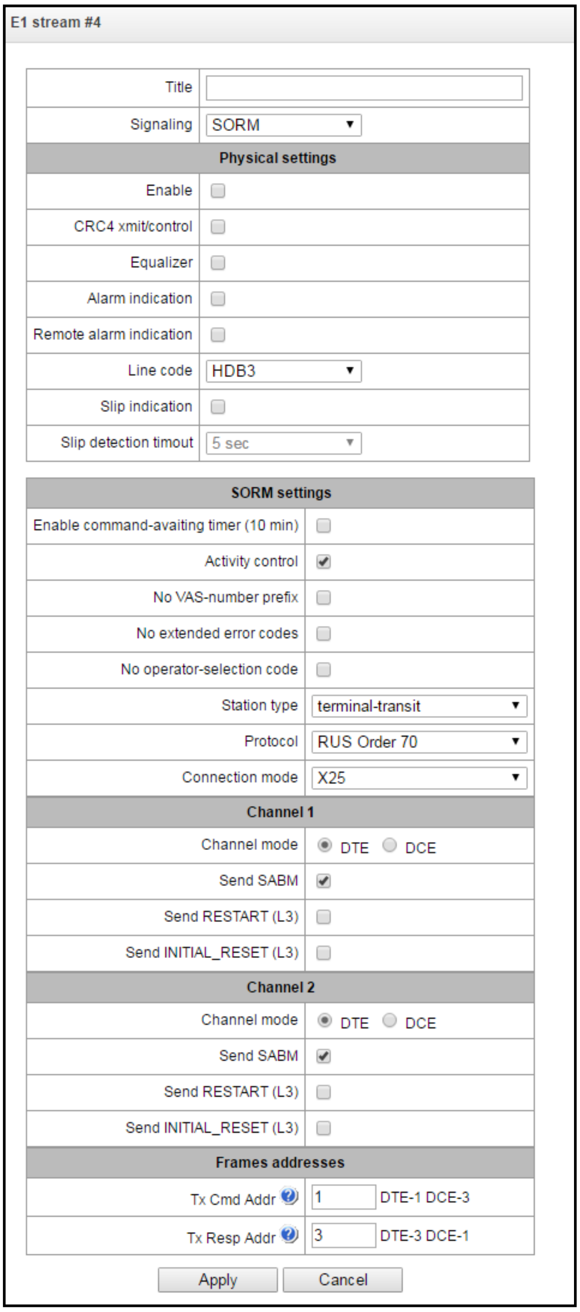
- *ISUP CIC—channel identifier code*—setting voice link numbers(CIC).

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

At that, the following menu will open:
- *Initial number*—number of the first voice link.
- *Numbering increment*—channel numbering increment. A number will be assigned to each of the subsequent channels that is greater by the numbering increment than of the previous channel.
- *CI range*—select values in this block to assign numbering for all stream channels or for specific channel range.



3.1.5.5 SORM signalling protocol configuration



– *Enable 10min command waiting timer* — enable/disable timeout for command reception from SORMCP (implemented according to Paragraph 1.5, Order no. 70 issued by GosComSvyaz RF on 20.04.1999).
– *Activity monitoring* — activity monitoring of L1 level message exchange process; if there are no packets received in 15 second interval through at least one of the channels, E1 stream framer will be reset and reinitialized.
– *Do not send VAS prefix* — when subscriber orders VAS, its prefix will not be sent to SORMcontrol panel. For example, when 'Call forward unconditional' service is ordered and the subscriber dials the number *21*2728331#, message 44 sent to SORM control panel will contain only the number 2728331 used for redirection.
– *Do not use extended error codes* — when checked, only command non-reception or non-execution messages with criteria specified in the Order no.268 will be sent in response to the command with invalid parameters. Otherwise, manufacturer non-execution command criteria will be used that allow for more detailed review the cause of command failure. For list of common codes and manufacturer codes, see Appendix E.

- *Operator selection code analysis* — during subscriber control, operator selection prefix dialled by a subscriber for long-distance or international call will not be registered (for details, see Appendix E).
- *Master station type* — master station type sent in the last byte of message no. 11 (PBX firmware version).
- *Protocol specification* — select SORM specification that will be used during device operation:
  - *RUS Order 70* — SORM specification for Order no. 70 dated 20.04.1999 issued by GosComSvyaz RF.
  - *RUS Order 268* — SORM specification for Order no. 268 dated 19.11.2012 issued by MinComSvyaz RF.
  - *KZ*—SORM specification for Kazakhstan.

Channel operation mode

- *Channel 1*—channel configuration block for management data received from SORMCP.
- *Channel 2*—channel configuration block for controlled connection data received from SMG-1016M.
- Connection mode
  - *X25* –signal channelsof data link control (DLC) become organized via X25 protocol by using 30-31 channal of E1 flow.
  - *TCP*–DLCsignal channelsbecome organized via TCP.
- TCP (the setting is active only when TCP connection mode is enabled)
  - *Port 1* – virtual TCP port to organize DLC-1 signal channel.
  - *Port 2* – virtual TCP port to organize DLC-2 signal channel.
  - *Interface* – select network interface of the device.

Channel settings

- *Channel operation mode:*
  - *DTE*—when checked, DTE is a device type (data transmitter).
  - *DCE*—when checked, DCE is a device type (receives data from DTE devices).
- *Send SABM*—when checked, a message on connection initialization startup will be sent into the channel.
- *Send RESTART (L3)*—send 'level 3 restart' message upon SORM CP connection establishment.
- *Send INITIAL_RESET (L3)*—send 'level 3 reset' message upon SORM CP connection establishment.

- *TxCmd Addr*—command frame address.
- *TxResp Addr*—response frame address.

SORM protocol setup on multiple streams is not allowed.

After SORM protocol selection for one of the streams, restart the software.

SORM default factory password is "123456".

Incoming number modifiers—select modifier table used for subscriber phone number analysis and modification located in messages received from SORM CP.

Outgoing number modifiers—select modifier table used for subscriber phone number analysis and modification located in messages sent to SORM CP.

Always modify B-number– option is required to modify all ‘B’ numbers. In the past, modificator of outgoing numbers aren’t applied for number dialed by local subscriber.

Modificator of controlled numbers – selection of modificator table specified to analize and modify subscriber phone number before it will be sampled for transmitting to SORM CP.

3.1.6 Numbering schedule

In this section, you may configure the device numbering schedule.

The device features up to 16 independent numbering schedules. Each numbering schedule may have its own subscribers and prefixes. To set the quantity of active schedules, see Section **3.1.1 System Parameters**.

Call routing on the device is performed using 3 criteria:

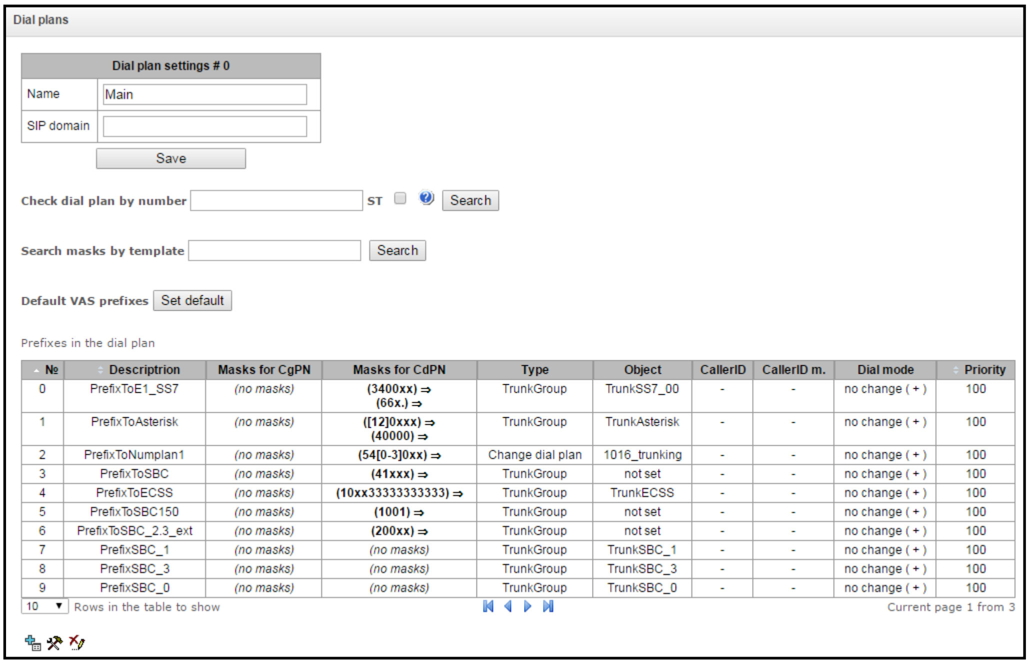
- Search by caller number—CgPN (Calling Party Number).
- Search by callee number—CdPN (Called Party Number).
- Search in a database containing subscribers configured on the device.

When the call arrives to the numbering schedule, 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 numbering schedule 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.



№	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

Numbering schedule parameters:

- *Name*—numbering schedule name.
- *SIP domain*—domain name for registration.

Numbering check 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.

Wildcard masks search—search prefix by the number template.

The check provides the routing possibility data for this number:

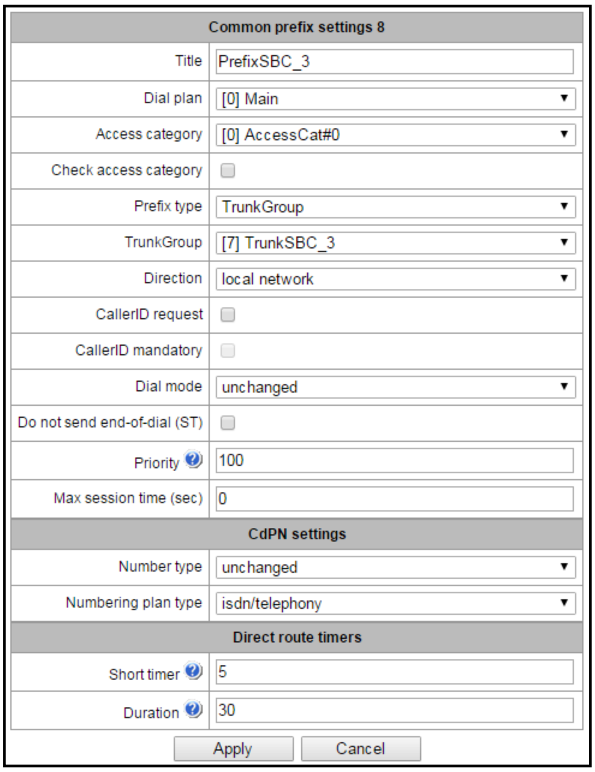
- *calling-table*—routing by the caller table.
- *called-table*—routing by the callee table.
- *NOT found in*—routing by this table is not possible.
- *found in*—routing by this table is possible.
- *Abonent 'SIP' idx[4]*—SIP subscriber [database record number for this subscriber].
- *Prefix [6]*—routing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

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:

- *Name*—numbering schedule name.
- *Numbering schedule*—select numbering schedule.
- *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 numbering schedule*—allows to enter another numbering schedule when this prefix is dialled. When this prefix type is selected, 'new numbering schedule' option will become available where you should specify the numbering schedule 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 clearback 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.

'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 call SORMing and communication restriction during RADIUS server data exchange failure (see Section **3.1.15 RADIUS configuration**).
- *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 SS-7 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.
- *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 dial (ST)*—when checked, do not send end dial marker (ST in SS or 'sending complete' in PRI).

CdPN parameters:
- *Number type*—callee number type: unknown, subscriber number, national number, international number, no change. Selected number type will be sent in SS-77, 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 schedule type*—callee numbering schedule type, may take the following values: unknown, isdn/telephony, national, privat, no change. Selected numbering schedule type will be sent in SS-77, 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).

Timers during direct out (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 dialling if the part of an address information has already been received. Default value—5sec.
- *Duration*—number dial duration timer. Default value—30sec.

'Numbering schedule change' prefix parameters

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

'VAS prefix' parameters

- *VAS service 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
  - *CFOOS*—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

- *Action*—select action for the service:
  - *Set*—set VAS service.
  - *Clear*—cancel VAS service
  - *Control*—VAS service activity control

'Pickup group' prefix parameters

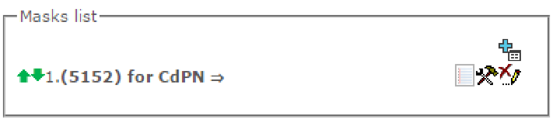
- Pickup group—pickup group that will be used for call pickup when this prefix is dialled.
- *Caller ID request*—defines Caller ID information necessity (caller number and category) for transition to the trunk group specified in *'Trunk group'* field. When the call arrives from the communication node and the Caller ID information is missing in that call, Caller ID request will be directed to that node (INR message from SS-7 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).
  - *Short timer*—time in seconds during which the digital gateway will wait for further dialling if the dialled number matches some sample in the numbering schedule, but the dialling of additional digits is possible at the same time that will cause a match with another sample. Default value—5sec.
  - *Duration*—number dial duration timer. Default value—30sec.

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 SS-7 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).
  - *Short timer*—time in seconds during which the digital gateway will wait for further dialling if the dialled number matches some sample in the numbering schedule, but the dialling of additional digits is possible at the same time that will cause a match with another sample. Default value—5sec.
  - *Duration*—number dial duration timer. Default value—30sec.

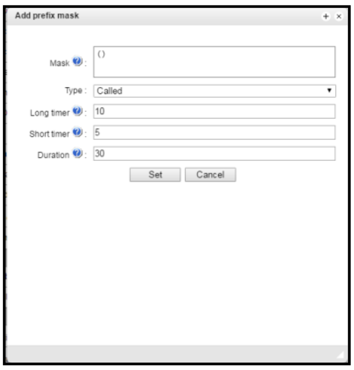
Mask list

For numbering schedules 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.

- *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 dialling until a match to some sample from the numbering schedule is established. Default value—10sec.
  - *Short timer*—time in seconds during which the digital gateway will wait for further dialling if the dialled number matches some sample in the numbering schedule, but the dialling of additional digits is possible at the same time that will cause a match with another sample. Default value—5sec.
  - *Duration*—number dial duration timer. Default value—30sec.

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)**.

- **|—**logical **OR**—enables separation of templates in a mask.

– **(-)**—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 numbering schedule, during number processing in the numbering schedule, 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 numbering schedule, 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 numbering schedule, 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 numbering schedule, 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 dialled 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 dialled 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 dialled 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 dialling 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 dialled 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 dialled 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 dialled 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 numbering schedule 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.

3.1.6.4 Timer operation examples

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

L=10sec.

S=5sec.

*First digit reception—0.*There are 2 rules in a mask for such a dialling: 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 dialling 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.

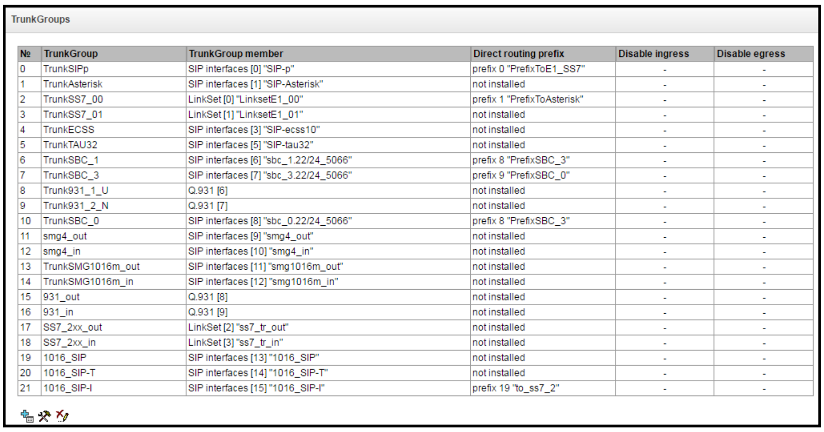
Solution

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

To do this, add a new prefix in the 'Numbering schedule' 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 Routing

3.1.7.1 Trunk groups

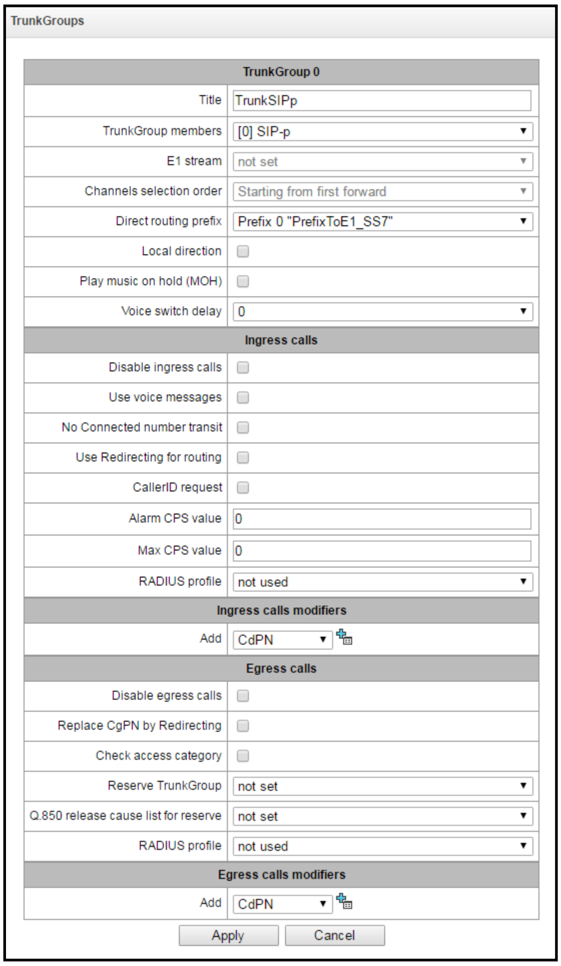


TrunkGroups

№	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, SS-7 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.



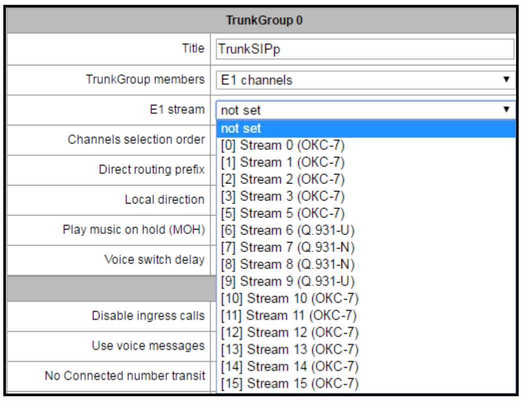
You may create up to 255 trunk groups.

Trunk group parameters:

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

- *Name*—trunk group name.
- *Group contents*—trunk group contents:
  - *Stream with Q.931 signalling, SS line group or SIP interface*
  - *E1 stream channels*—E1 stream channels with Q.931, SS7 signalling protocols

– *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'.*



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

– *Direct 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 dialled number (without mask creation in prefixes). When the dialling is performed in the overlap mode, direct dialling timers are used, configured in the direct prefix.

– *Local direction*—when checked, subscribers of this direction are considered as local. Subscribers of this direction are configured to SORM tracking with the number type and marker 'subscriber of the current PBX'.

– *Musiconhold (MOH)* – option 'MusicOnHold' isenabled, whenyou get hold party attribute.

– *Voice frequency path forwarding delay*—forced voice frequency path delay after the subscriber's answer.

Incoming communication:

– *Incoming call barring*—when checked, the incoming call reception will be barred. Setting call barring will not disrupt any of the established connections.

– *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).

– *Block Connected number transmission*—disable transmission of the *Connected number* field.

– *Use Redirecting 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 numbering schedule using CgPN number masks.

– *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 SS-7 signalling).

– *CPS emergency 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.

– *CPS threshold 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**).

Incoming communication 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.

Outgoing communication:

– *Outgoing call barring*—when checked, the outgoing call transmission will be barred. Setting call barring will not disrupt any of the established connections.

– *Substitute 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.

– *Redundant 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 clearback reason list for transition to redundant group*—select *'Q.850 clearback reason list'* table to configure Q.850 clearback reasons 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**).

Outgoing communication 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.

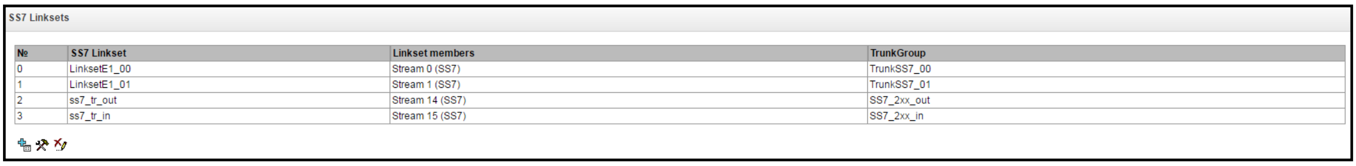
To create, edit or remove groups (as well as other objects), use *'Objects' — 'Add object', 'Objects' — 'Edit object'* and *'Objects' — 'Remove object'* menus and the following buttons:

—*'Add trunk group'*

—*'Edit trunk group parameters'*

—*'Delete trunk group'*

3.1.7.2 SS-7 line groups

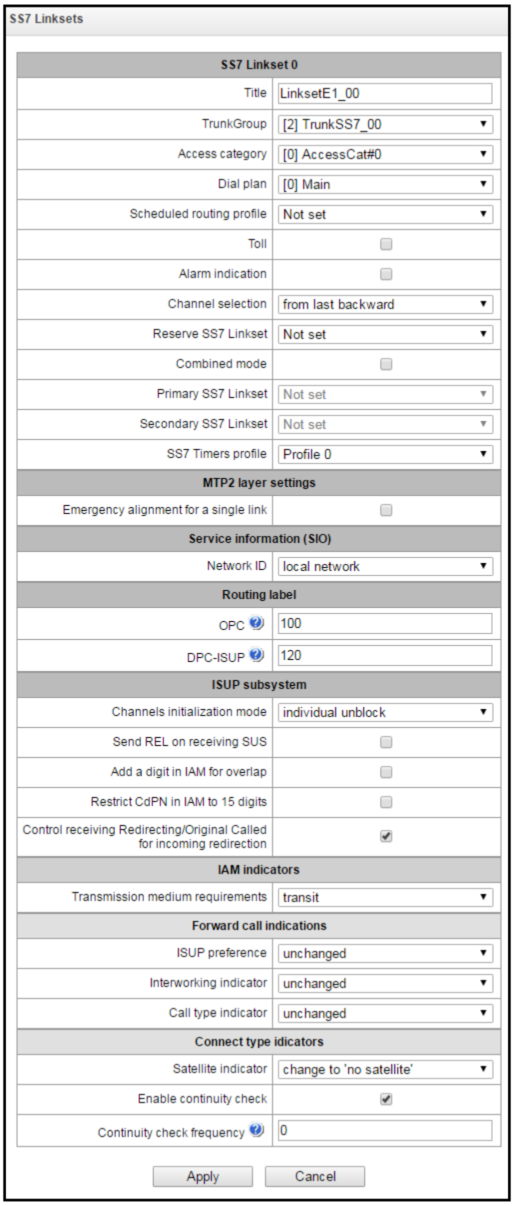

SS7 Linksets

№	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 SS-7 signalling protocol configuration, see 'E1 streams' (Section 3.1.5.4).

'SS-7 line group' is a set of signal loops of a single direction. To create, edit or remove line groups, use *'Objects' — 'Add object', 'Objects' — 'Edit object'* and *'Objects' — 'Remove object'* menus and the following buttons:

– *'Add SS-7 line group (LinkSet)'*
– *'Edit SS-7 line group (LinkSet)'*
– *'Delete SS-7 line group (LinkSet)'*



SS-7 line group parameters

- *Name*—SS-7 line group name.
- *Trunk group*—name of a trunk group that SS-7 line group operates with.
- *Access category*—select access category.
- *Numbering schedule*—define numbering schedule that will be used for routing in this group (necessary for numbering schedule negotiation).
- *Scheduled routing profile*—select 'scheduled routing' service profile, configured in the 'Internal resources' section.
- *Long-distance*[1]—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 to signalling CAS).
- *Fault indication*—when checked, fault indication will appear in case of SS-7 signal link fault (ALARM LED will light up, alarm will be added to alarm log).
- *Channel engagement order*—channel engagement order for the outgoing calls. Available options:
  - *Sequential forward*
  - *Sequential back*
  - *From the first and forward*
  - *From the last and back*
  - *Sequential forward even*
  - *Sequential back even*
  - *Sequential forward odd*
  - *Sequential back odd*

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

- *Redundant SS-7 line group*—redundant SS-7 line group selection. When the main SS-7 line group is not available, the whole signalling message exchange will be performed through the redundant SS-7 line group.
- *Combined mode*—Combined Linkset mode that will enable the exclusive utilization of voice streams in the current SS-7 line group and signalling transfer through the signal channels of SS-7 primary and secondary groups.
- *Primary SS-7 line group*—select SS-7 line group, that will perform the exchange of signalling messages related to this particular SS-7 line group, by the signal D-channels.
- *Secondary SS-7 line group*—select the second SS-7 line group, that will perform the exchange of signalling messages related to this particular SS-7 line group, by the signal D-channels.

In the combined mode operation, the signalling payload will be distributed evenly (50/50) between the primary and secondary SS-7 line groups.

- *SS-7 timer profile*—select the timer profile that will be used for the current SS-7 line group.

MTP2 level

- *Emergency phasing in case of a single signal link in linkset*—enable emergency phasing procedure during SS-7 line group commissioning, if this SS-7 line group has a single signal link.

Service information (SIO)

- *Network identifier*—indicates the network type: international, national, local network or reserve (usually, the value 'Local network' is used in the Russian Federation).

Routing label

- *Proprietary code (OPC)*—signalling point proprietary code.
- *ISUP opposite code (DPC-ISUP)*—code of the communicating signalling point of the ISUP subsystem.

[1]Not supported in the current version.

ISUP subsystem

- *Initialization*—device operations during stream recovery:
  - *Leave blocked*—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.
- *REL in response to SUS*—Release message is sent in response to Suspend message.
- *Send dialling digits to IAM during overlap*—send a single digit to *Called Party number* field of IAM message during overlap dialling method.
- *Send up to 15 digits to IAM*—when checked, up to 15 digits of CdPN number will be sent in IAM message, other digits will be sent in SAM message.
- *Check presence of Redirecting/Original Called in 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.

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 direction call indicators

- *Forward direction call indicators*—rule that governs ISUP preference indicator modification. In normal situation, these bits should not be changed.
- *Interaction indicator*—defines whether the interaction indicator should be modified (defines whether the interaction with non-ISDN network has occurred).
- *Call type identifier—'National/international call indicator'* parameter modifications inFCI.

'Nature of connection' indicators

- *Satellite channel identifier*—identifies the presence of the satellite channel.
  - *Override to "no satellite"*—change identifier value to *'no satellite'* regardless of the value received from the incoming channel.
  - *Transit*—keep the indicator value unchanged.
  - *Add one*—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 channel integrity check support*—enables integrity check support in the SS-7 line group. 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.
- *Frequency of channel integrity checks*—define the frequency of channel integrity checks during outgoing calls performed through the SS-7 line group. 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 **3.1.8.1SS category**.

Examples

1. SMG connection method example for operation in SS-7 quasi-associated mode via signalling transition points (STP).

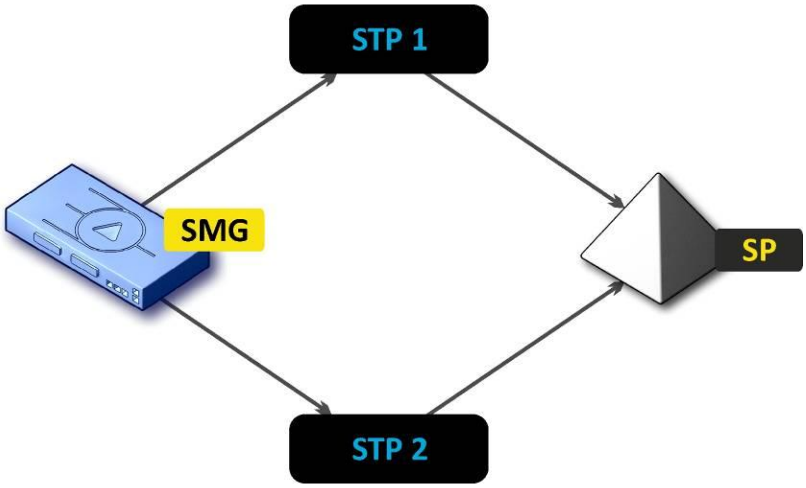


Fig. 32—SMG connection method for operation in SS-7 quasi-associated mode via STP

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 *'Proprietary code (OPC)'* = **22** and ISUP opposite code(DPC-ISUP) = **23** in 'SS-7 line groups' 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 SS-7 line group in *'SS-7 line group'* settings and define the parameter *'MTP3 opposite code (DPC-MTP3)'* equal to **155** for stream 0, and **166** for stream 1.

2. SMG connection method example for operation in SS-7 quasi-associated mode via PBX with STP features.

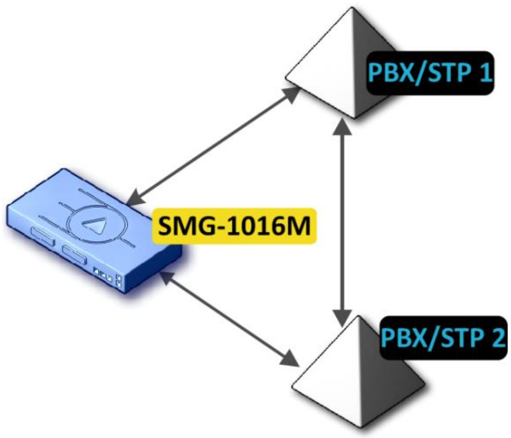


Fig. 33—SMG connection method for operation in SS-7 quasi-associated mode via PBX with STP.

LS—SS-7 line group (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 SS-7 line group configuration, stream 1 is connected to PBX/STP 2 and used for the second SS-7 line group 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 SS-7 line group in the *'Redundant SS-7 line group'* setting in the first SS-7 line group configuration.

3. SMG connection method example for operation in combined mode

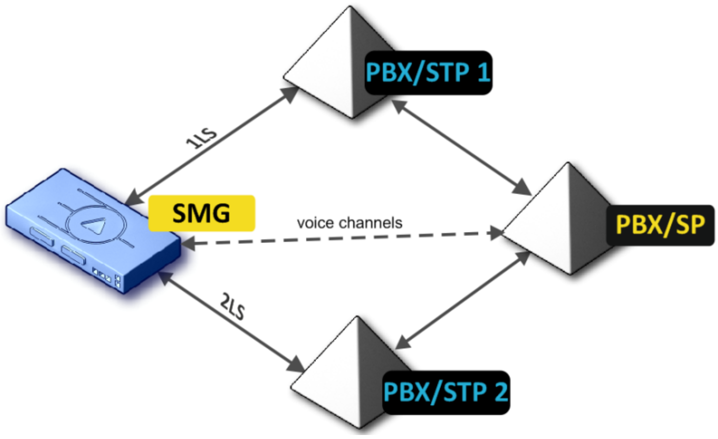


Fig. 34—SMG connection method for operation in combined mode

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 SS-7 line group configuration, stream 1 is connected to PBX/STP 2 and used for the second SS-7 line group configuration, SMG stream 2 is connected to PBX/SP and used for the third SS-7 line group 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** SS-7 line group in the *'Primary SS-7 line group'* setting and the **second** SS-7 line group in the *'Secondary SS-7 line group'* setting in the third SS-7 line group configuration.

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

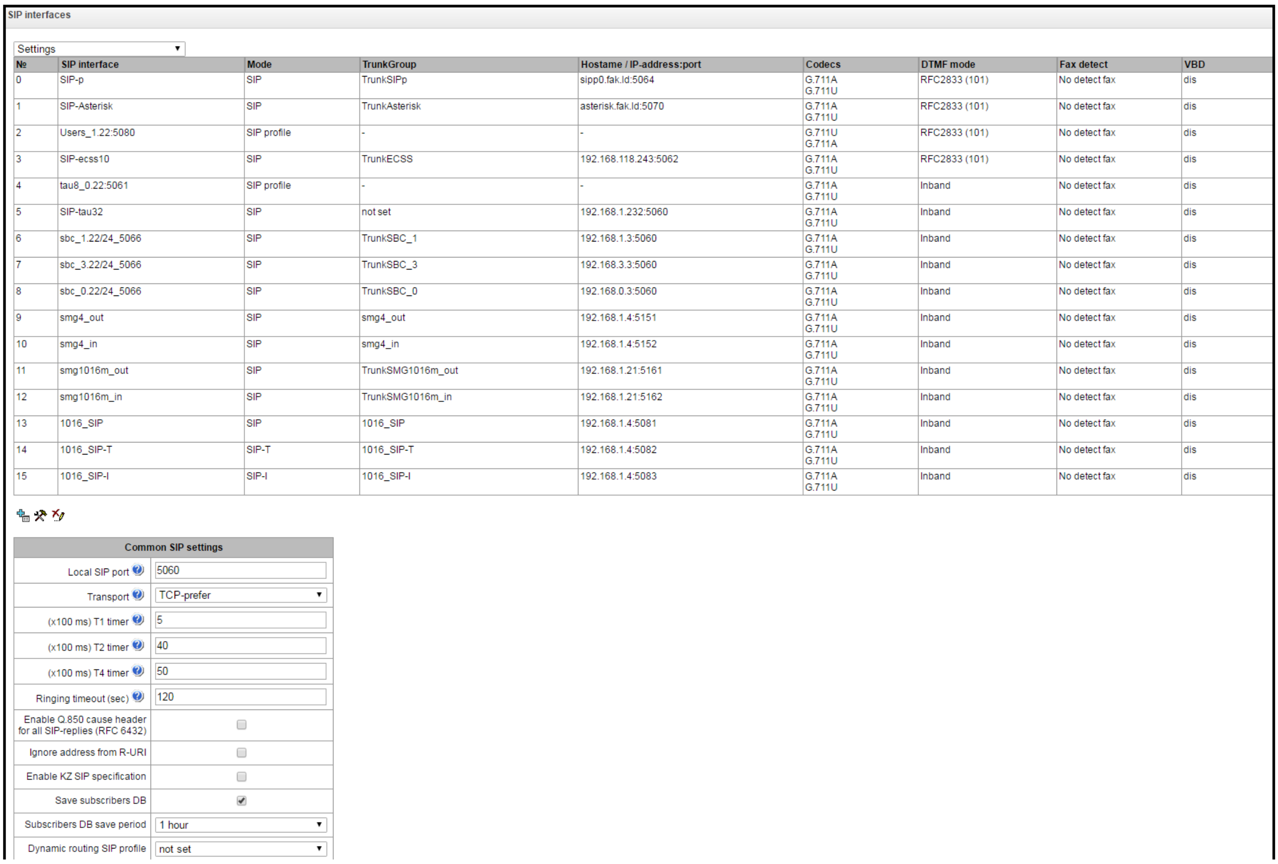
3.1.7.3.1 Configuration

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 located 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 interfaces

Settings

№	SIP interface	Mode	TrunkGroup	Hostame / IP-address:port	Codecs	DTMF mode	Fax detect	VBD
0	SIP-p	SIP	TrunkSIPp	sipp0.fak.ld:5064	G.711A G.711U	RFC2833 (101)	No detect fax	dis
1	SIP-Asterisk	SIP	TrunkAsterisk	asterisk.fak.ld:5070	G.711A G.711U	RFC2833 (101)	No detect fax	dis
2	Users_1.22:5080	SIP profile	-	-	G.711U G.711A	RFC2833 (101)	No detect fax	dis
3	SIP-ecss10	SIP	TrunkECSS	192.168.118.243:5062	G.711A G.711U	RFC2833 (101)	No detect fax	dis
4	tau8_0.22:5061	SIP profile	-	-	G.711A G.711U	Inband	No detect fax	dis
5	SIP-tau32	SIP	not set	192.168.1.232:5060	G.711A G.711U	Inband	No detect fax	dis
6	sbc_1.22/24_5066	SIP	TrunkSBC_1	192.168.1.3:5060	G.711A G.711U	Inband	No detect fax	dis
7	sbc_3.22/24_5066	SIP	TrunkSBC_3	192.168.3.3:5060	G.711A G.711U	Inband	No detect fax	dis
8	sbc_0.22/24_5066	SIP	TrunkSBC_0	192.168.0.3:5060	G.711A G.711U	Inband	No detect fax	dis
9	smg4_out	SIP	smg4_out	192.168.1.4:5151	G.711A G.711U	Inband	No detect fax	dis
10	smg4_in	SIP	smg4_in	192.168.1.4:5152	G.711A G.711U	Inband	No detect fax	dis
11	smg1016m_out	SIP	TrunkSMG1016m_out	192.168.1.21:5161	G.711A G.711U	Inband	No detect fax	dis
12	smg1016m_in	SIP	TrunkSMG1016m_in	192.168.1.21:5162	G.711A G.711U	Inband	No detect fax	dis
13	1016_SIP	SIP	1016_SIP	192.168.1.4:5081	G.711A G.711U	Inband	No detect fax	dis
14	1016_SIP-T	SIP-T	1016_SIP-T	192.168.1.4:5082	G.711A G.711U	Inband	No detect fax	dis
15	1016_SIP-I	SIP-I	1016_SIP-I	192.168.1.4:5083	G.711A G.711U	Inband	No detect fax	dis

Common SIP settings	
Local SIP port	5060
Transport	TCP-prefer
(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

SIP general configuration:

- *Port for SIP signalling* reception—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.
  - *USP-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.
- *Set the specification in accordance with the requirements of the Republic of Kazakhstan.*
- *Ignore address in 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.
- *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.
- *Use Q.850 cause header for all response SIP codes(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.
- *Store subscribers' database*—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.
- *Database saving 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 и 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, SS-7 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*'*

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, and T.38 protocol.

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.

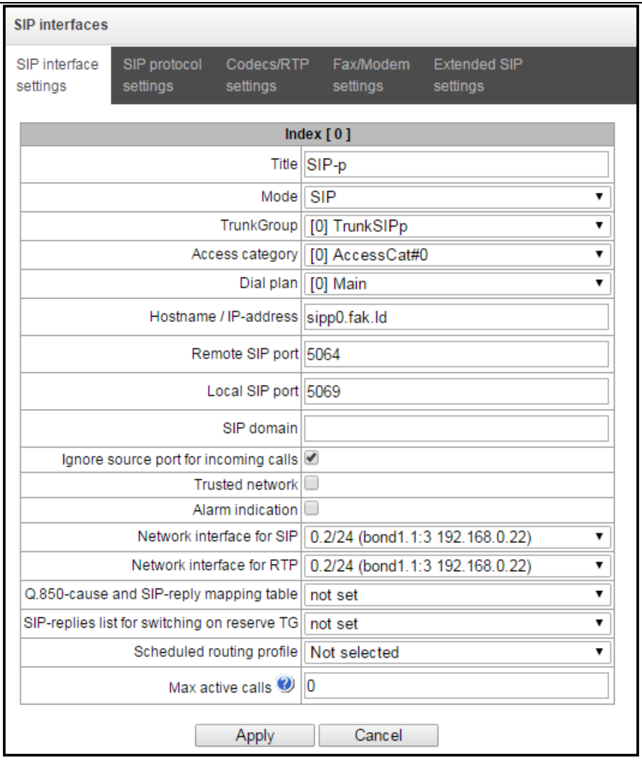
G.726 is an ADPCM ITU-T standard that describes voice data transmission using 16, 24, 32, and 40kbps bands. **G.726-32** substitutes G.721 that describes ADPCM voice data transmission using 32kbps band.

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).

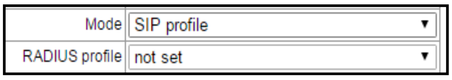
G.729 is also a voice data compression codec with the rate of 8kbps. As with G.723.1, G.729 codec supports voice activity detector and performs comfort noise generation (Annex B).

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.

3.1.7.3.1.1. SIP interface configuration tab



- *Name*—interface name.
- *Mode*—select protocol for the interface (*SIP/SIP-T/SIP-I/SIP profile*).
- *RADIUS profile*—select RADIUS profile for the *SIP profile* interface (for the rest of interfaces, RADIUS profile is assigned in the trunk group).

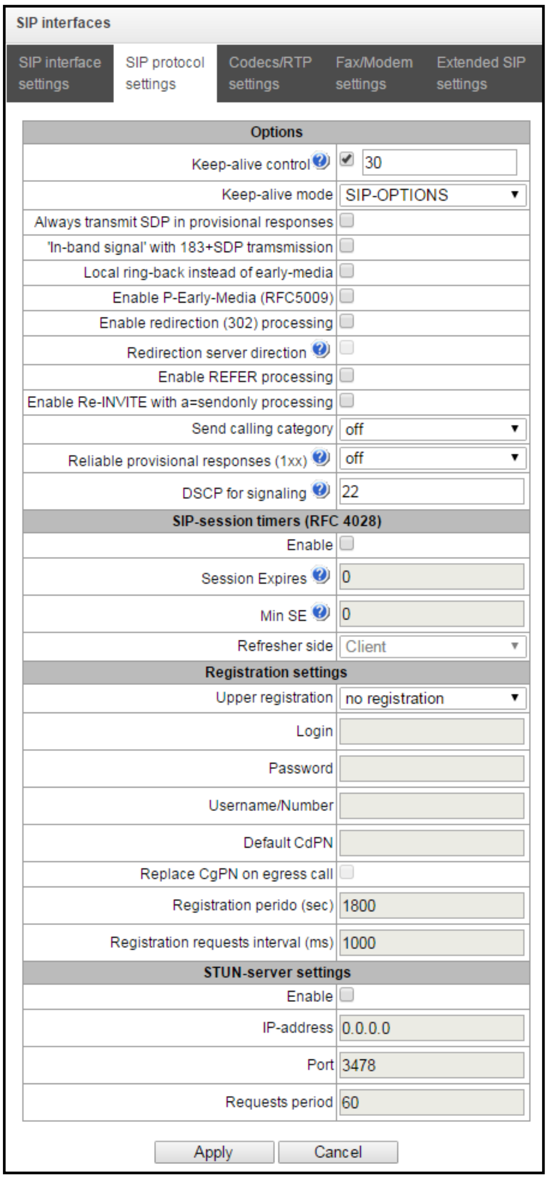


- *Trunk group*[1]—name of a trunk group, that the interface belongs to.
- *Access category*—select access category.
- *Numbering schedule*—define numbering schedule that will be used for dialling from this port (necessary for numbering schedule negotiation).
- *Host name/IP address*—IP address or name of the host communicating via gateway SIP/SIP-T protocol.
- *SIP signalling destination port*[1]—UDP/TCP port of the communicating gateway used for SIP/SIP-T signalling reception.
- *Port for SIP signalling reception*[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 address registration.
- *Ignore source port during 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.
- *Fault 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.
- *Signalling network interface*—select network interface for signalling SIP message transmission and reception.

[1]Field is not active in SIP profile mode.

- *RTP network interface*—select network interface for voice traffic transmission and reception.
- *Q.850-cause and SIP-reply correspondence table*—select correspondence table for Q.850-cause and SIP-reply codes. To configure correspondence tables, use 'Internal resources' menu.
- *CSIP response list for redundant TG transition*—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, configured in the 'Internal resources' section.
- *Active connections*—maximum number of simultaneous (incoming and outgoing) connection through the interface specified.

3.1.7.3.1.2. SIP protocol configuration tab



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

- *Opposite party availability control using OPTIONS messages*—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.
- *Opposite party availability control 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 send SDP in provisional replies*—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 ringback for 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.
- *Use 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.
- *CCI Enable*—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)*—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 perform the redirection.
- *Redirection server*—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 numbering schedule routing. The routing will be performed directly to the address contained in the reply 302 'contact' header received from the redirection server.
- *Enable REFER message 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 clearback the call and will not perform 'Call transfer' service.
- *Enable Re-INVITE processing with a=sendonly*—checkbox that allows to put the call on hold when Re-INVITE message is received with a=sendonly marker in SDP.
- *Caller category transmission*—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, SS-7 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 delivery of 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 Signaling*—service (DSCP) type for SIP signalling traffic.

SIP session timers (RFC 4028)

- *Enable timer support*—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*'.
- *Session renewal party*—defines the party that will perform session renewal (client (uac)—client (caller) party, server (uas)—server (callee) party).

Registration parameters[1]:

- *Registration on upstream server*—select type of registration on the upstream server:
  - *Without registration*—do not register on the upstream server.
  - *Trunk registration*—registration on the upstream server using parameters specified in this section.
  - *Subscriber 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.
  - *Transit registration (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.
- *CgPN substitution in outgoing 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 time*—registration renewal time period.
- *Registration request interval (ms)*—minimum 'Register' message transmission interval designed for protection from high traffic caused by simultaneous registration of large number of subscribers.

STUN server parameters:

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

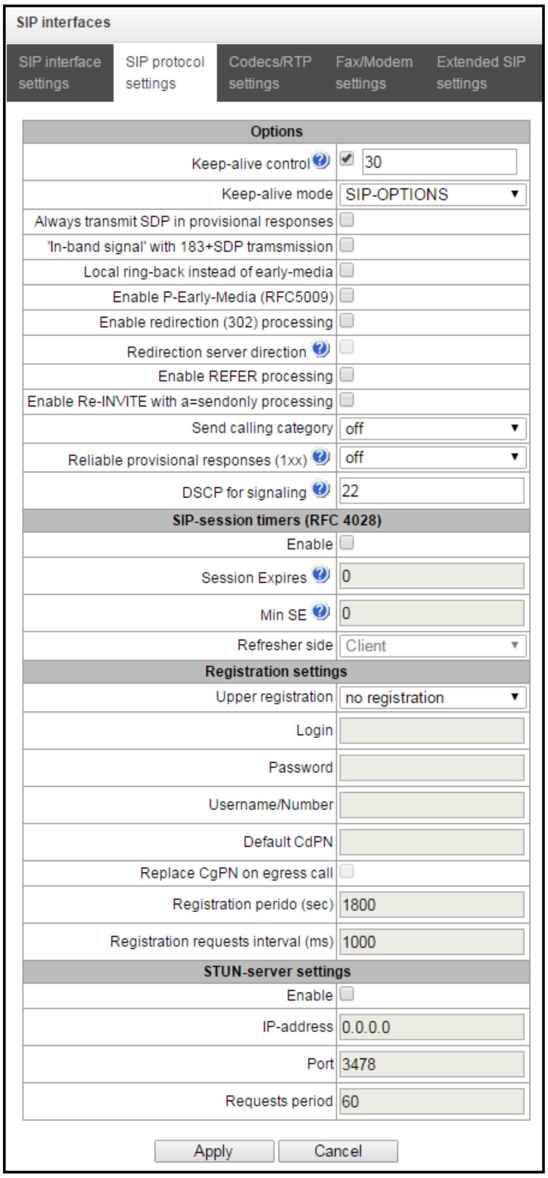
[1]Parameter block is available for SIP mode only.

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.**

Configuration of options for SIP profile mode:



- *Opposite party availability 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.
- *Opposite party availability control 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 send SDP in provisional replies*—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).
- *Enable redirection (302)*—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 perform the redirection.
- *Redirection server*—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 numbering schedule routing. The routing will be performed directly to the address contained in the reply 302 'contact' header received from the redirection server.
- *Enable REFER message 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 processing with a=sendonly—checkbox that allows to put the call on hold when Re-INVITE message is received with a=sendonly marker in SDP.
- *Reliable delivery of 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.
- *DSCPдляSignaling* – service type (DSCP) for SIPsignaling traffic.

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.
- *NAT: send 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.

SIP session timers (RFC 4028)

- *Enable timer support*—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*'.
- *Session renewal party*—defines the party that will perform session renewal (client (uac)—client (caller) party, server (uas)—server (callee) party).

Transit registration parameters[1]: (Parameter block is available for SIP profile mode only.)

- *Transit registration interface*—select SIP interface for transit registration.

STUN server parameters:

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

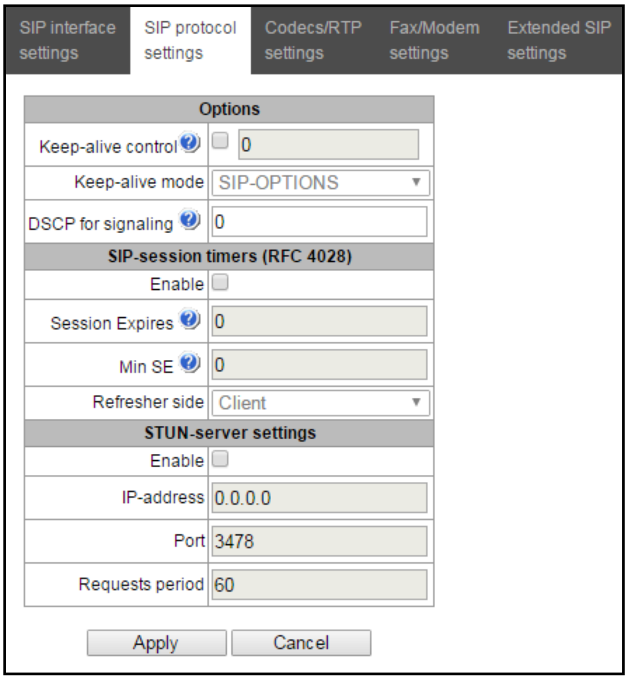
STUN network protocol (RFC 5389) allows applications located behind a network address translation server (NAT) to discover their external IP address and port mapped to an internal port. Used when SMG is located behind a NAT.

- *Enable STUN*—when checked, enable STUN.
- *STUN server IP address*—STUN server IP address
- *STUN server port*—server port for request transmission (default value is 3478).
- *Request 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:



- *Opposite party availability 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.
- *Opposite party availability control 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 Signaling*—service (DSCP) type for SIP signalling traffic.

SIP session timers (RFC 4028)

- *Enable timer support*—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*'.
- *Session renewal party*—defines the party that will perform session renewal (client (uac)—client (caller) party, server (uas)—server (callee) party).

STUN server parameters:

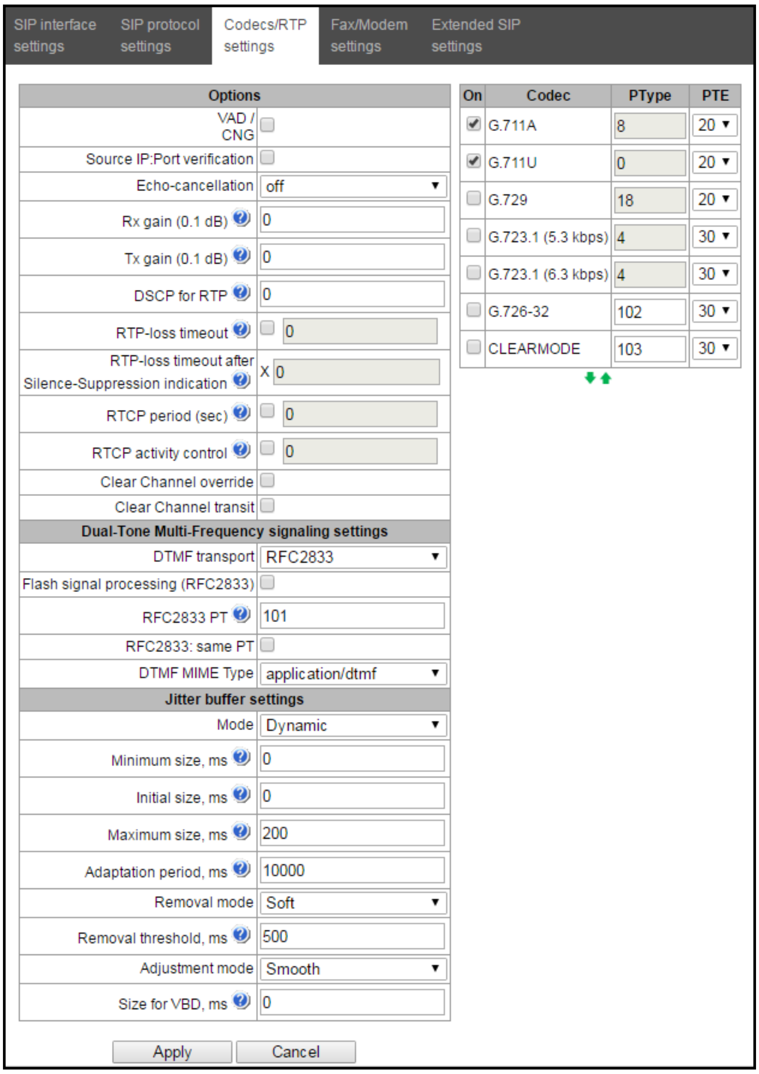
STUN network protocol (RFC 5389) allows applications located behind a network address translation server (NAT) to discover their external IP address and port mapped to an internal port. Used when SMG is located behind a NAT.

- *Enable STUN*—when checked, enable STUN.
- *STUN server IP address*—STUN server IP address
- *STUN server port*—server port for request transmission (default value is 3478).
- *Request 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.

3.1.7.3.1.3. RTP codec configuration tab



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 control*—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).
  - *off*—do not use echo cancellation (this mode is set by default).
- *Gain receive (0.1 dB)*—volume of signal received, gain of the signal received from the communicating gateway.
- *Gain transmit (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.

- *RTP packet 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 packet timeout after reception of Silence-Suppression (multiplier)*—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 packet transmission 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.
- *Session activity monitoring via RTCP*—voice frequency path status control function, may take up values in the range 5–65535. 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 (SS-7 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.

DTMF transmission:

- *DTMF transmission method*—method of DTMF transmission via IP network.
  - *inband*—in RTP packets, inband.
  - *RFC2833*—in RTP packets according to rfc2833 recommendation.
  - *INFO*—outband, via SIP, INFO messages are used; at that, DTMF signal appearance will depend on the MIME extension type.

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

- *Flash(RFC2833) signal processing*—checkbox that governs activation of FLASH signal processing using INFO, frc2833, and re-invite methods for *'Call transfer'* VAS operation.
- *HOLD put on/release by*—select a signal that will be used for subscriber put on/remove from hold:
  - *flash*—by flash signal only.
  - *flash/**—by flash signal or on '*' key press.
  - *flash/#*—by flash signal or on '#' key press.
  - *flash/*/#*—by flash signal or on '*' key press, or on '#' key press.
- *RFC2833 PT*—type of payload used to transfer DTMF packets via КАС2833. 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).

- *Same RFC2833 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: 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.

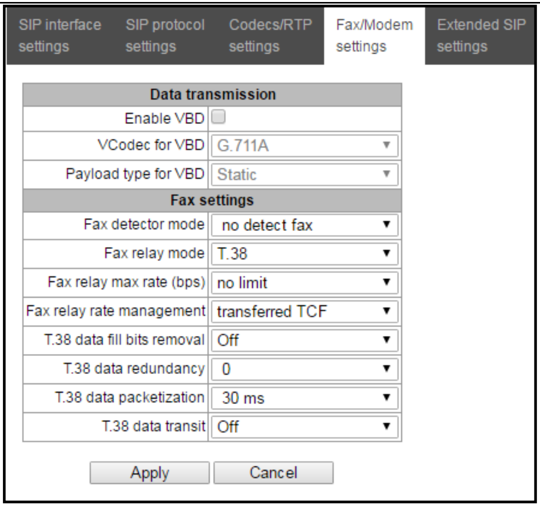
Click the left mouse button to highlight the row with the selected codec. Use arrow buttons (up, down) to change the codec priority.

- *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, 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 and data transfer configurationtab



Data transfer:

- *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).
- *VBD codec*—codec, used for data transmission in VBD mode
- *VBD payload type*—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 transmission:

- *Detection 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.

- *Transmission mode*—select protocol for fax transmission.
- *T.38 fax maximum speed*—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.
- *Speed management method for T.38 protocol data transfer*—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.
- *Bit removals and inserts for T.38 data*—padding bit removals and inserts for data that does not relate to ECM (error correction mode).
- *Redundancy amount in T.38 data packets*—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.
- *Packetization time for T.38 protocol*—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 packet 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.

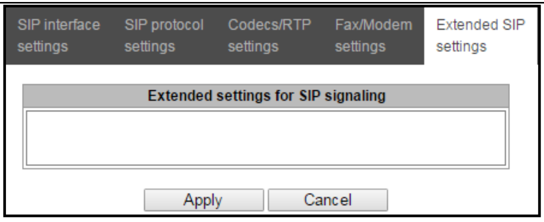
'Service type' (IP DSCP) field value for RTP, T.38 and SIP/SIP-T/SIP-I:

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:

- *Operations*—disable 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.

Table 18—Implementation examples of operation rules

Operation	**Initial header**	**Rule**	**Result**
Do not send the header	Accept: application/SDP	[sipheader:accept=disable]	
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)$]	Accept: application/ISUP,text/plain
Replace text truncating data at the end	Accept: application/SDP,text/plain	[sipheader:accept=-(SDP)+(ISUP)!]	Accept: application/ISUP,text/plain
Complex modification example	From: <sip:who@host>;tag=aBc	[sipheader:from=+(DISPLAY)-(who)+(12345)-(>)+(;user=phone>)$+(;line=abc)]	From: DISPLAY <sip:12345@host;user=phone>;tag=aBc;line=abc

Example

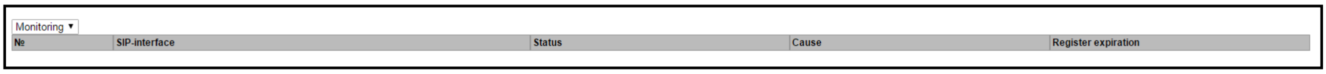
```
[sipheader:Accept=disable,user-agent=disable]
```

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

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

3.1.7.3.2 Monitoring

When you choose 'Monitoring' item from the drop down list, a table will be shown that enables monitoring of the trunk registration on the upstream server.



- *Login*—name used for authentication.
- *User number/Number*—user number utilized for outgoing trunk calls.
- *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.

3.1.7.4 H323 interfaces

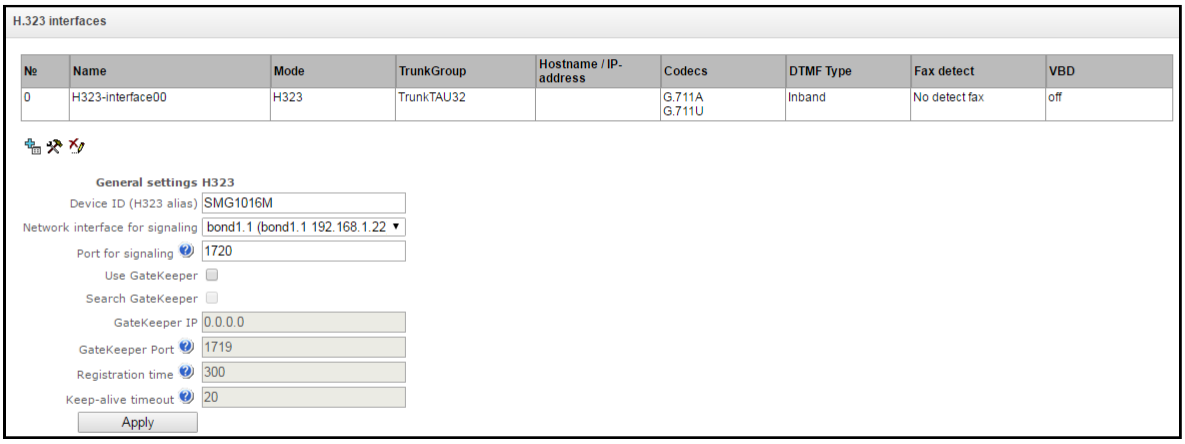
In this section, you may configure H.323[1] stack general configuration parameters, custom settings for each direction operating via H.323 protocol.

H.323 protocol is a signalling 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 signalling is a stack of protocols based on the**Q.931** recommendation implemented inISDN. Recommendations utilized by the gateway as follows:**H.225.0**and**H.245.**

SMG may operate within a method that may or may not feature the **Gatekeeper**.

H.323 general configuration



- *Device identifier (Alias)*—gateway name during registration at the Gatekeeper.
- *Signalling network interface*—select the network interface for H.323 signalling.
- *Signalling reception port*—local TCP port for H.323 signalling message reception.
- *Enable GateKeeper*—when checked, the Gatekeeper will be used, otherwise it will not be used.
- *GateKeeper discovery*—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).
- *Time To Live*—time period in seconds, for which the device will keep its registration on a gatekeeper.

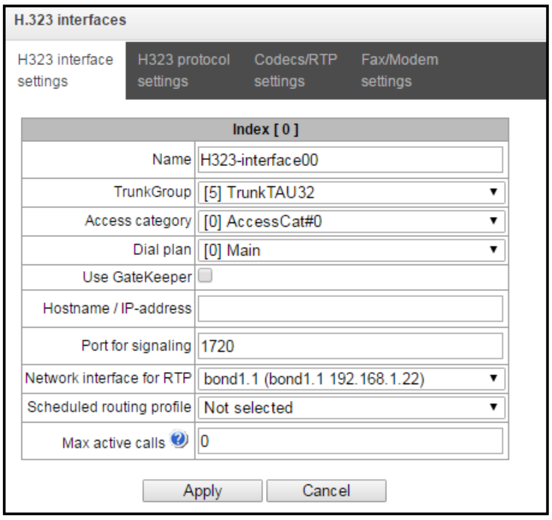
[1]This menu is available in the firmware version with H.323 license only, for license details, see Section **3.1.23.Licences**

– *Keep Alive Time*—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 *'Time To Live'* registration period. At that, for *'Time To Live'* 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 *'Time To Live'* 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.

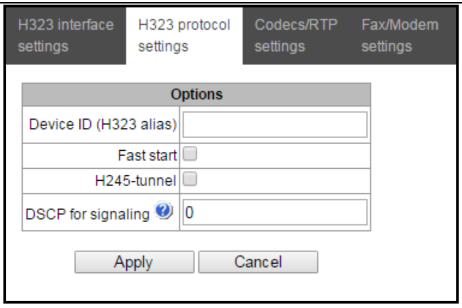
When settings are applied in this section, H.323 will be restarted and all established H.323 voice connections will be forcedly terminated, also H323-MODULE LOST fault may appear shortly.

3.1.7.4.1 ***H.323 interface settings*** tab



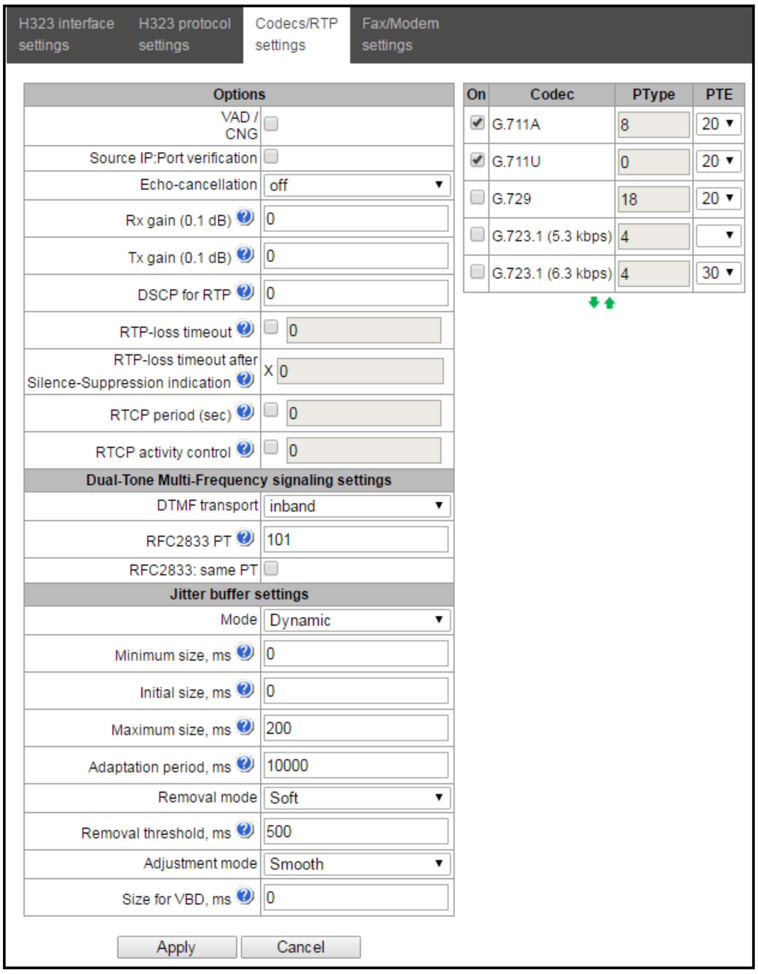
– *Name*—interface name.
– *Trunk group*—select a trunk group, that the interface belongs to.
– *Access category*—select access category.
– *Numbering schedule*—define numbering schedule that will be used for dialling from this interface (necessary for numbering schedule negotiation).
– *Enable GateKeeper* —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.
– *H323 signalling destination port*—signalling TCP port of the communicating gateway used for H323 signalling reception.
– *RTP network interface*—select network interface for voice traffic transmission and reception.
– *Scheduled routing profile*—select 'Scheduled routing' service profile, configured in the 'Internal resources' section.
– *Active connections*—maximum number of simultaneous (incoming and outgoing) connection through the interface specified.

3.1.7.4.2 ***H.323 protocol settings*** tab



- *Device identifier (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 signalling tunnelling is enabled through the Q.931 signal channel, otherwise it is disabled.
- *RTP packet 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 cleared back.
- *RTP packet timeout after reception of Silence-Suppression (multiplier)*—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 cleared back.
- *DSCP for signaling*—service (DSCP) type for SIP signalling traffic (H.323).

3.1.7.4.3 ***RTP/ codec configuration*** tab



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 control*—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).
  - *off*—do not use echo cancellation (this mode is set by default).
- *Gain receive (0.1 dB)*—volume of signal received, gain of the signal received from the communicating gateway.
- *Gain transmit (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.
- *RTCP packet transmission 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.

- *Session activity monitoring via RTCP*—voice frequency path status control function, may take up values in the range 5–65535 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 transmission method*—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 Alphanumeric*—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 IE—*outband; Keypad information element is used for DTMF transmission in Q.931 INFORMATION message.*

In order to be able to use extension dialling 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 KAC2833. 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).

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:

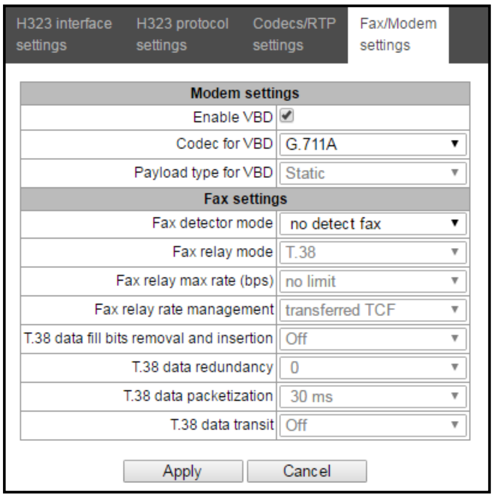
In this section, you may select codecs for an interface and an order of their usage on connection establishment. Codec with the highest priority should be placed in top position.

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



Data transfer:

- *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).
- *VBD codec*—codec, used for data transmission in VBD mode
- *VBD payload type*—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 transmission:

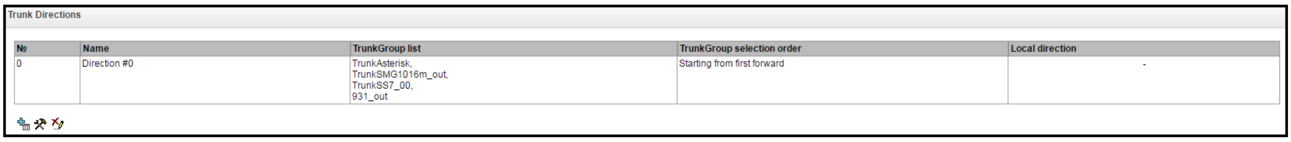
- *Detection mode*—detects transmission direction for fax tone detection and subsequent switching to fax codec:
  - *no detect fax*—disables fax tone detection, but will not affect fax transmission (switching to fax codec will not be initiated, but such operation still may be performed by the opposite 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.

- *Transmission mode*—select protocol for fax transmission.
- *T.38 fax maximum speed*—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.
- *Speed management method for T.38 protocol data transfer*—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.
- *Bit removals and inserts for T.38 data*—padding bit removals and inserts for data that does not relate to ECM (error correction mode).
- *Redundancy amount in T.38 data packets*—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.
- *Packetization time for T.38 protocol*—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 packet 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

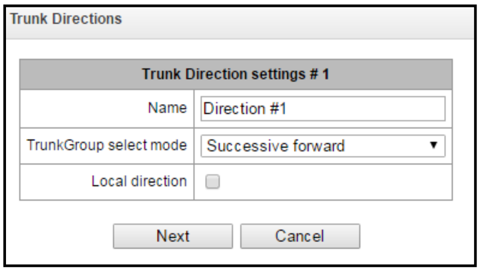
Trunk direction is a set of trunk groups. For a call to a trunk direction, you may specify the selection order for trunk groups comprising this direction.



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

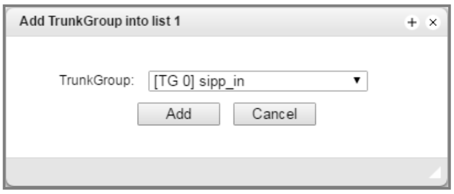
—*'Add direction'*
—*'Edit direction parameters'*
—*'Removedirection'*

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



- *Name*—trunk direction name.
- *Trunk group selection 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. Subscribers of this direction are configured to SORM tracking with the number type and marker 'subscriber of the current PBX'.

List of trunk groups in direction



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 Registration

3.1.7.6.1 Configuration

Subscriber registration and authentication parameters for interfaces with the subscriber registration type.

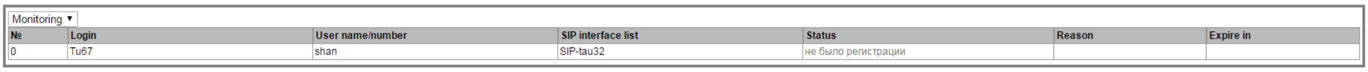
Registration parameters:

– *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.

3.1.7.6.2 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.

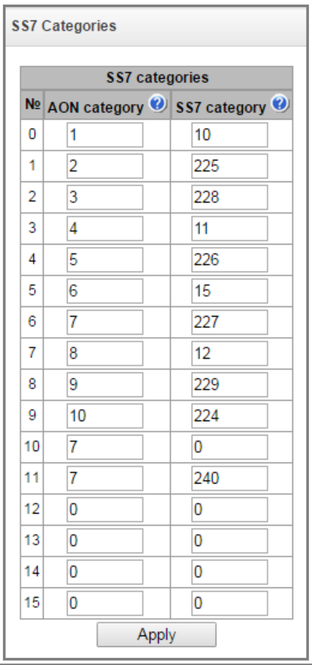


– *Login*—name used for authentication.
– *Username/Number*—number of the user registered on the upstream server.
– *SIP interface list*—list of interfaces with enabled access for the current subscriber.
– *Status*—subscriber registration status (registered, not registered, registration expired).
– *Reason*—possible 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 SS-7 protocol 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

Apply

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

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

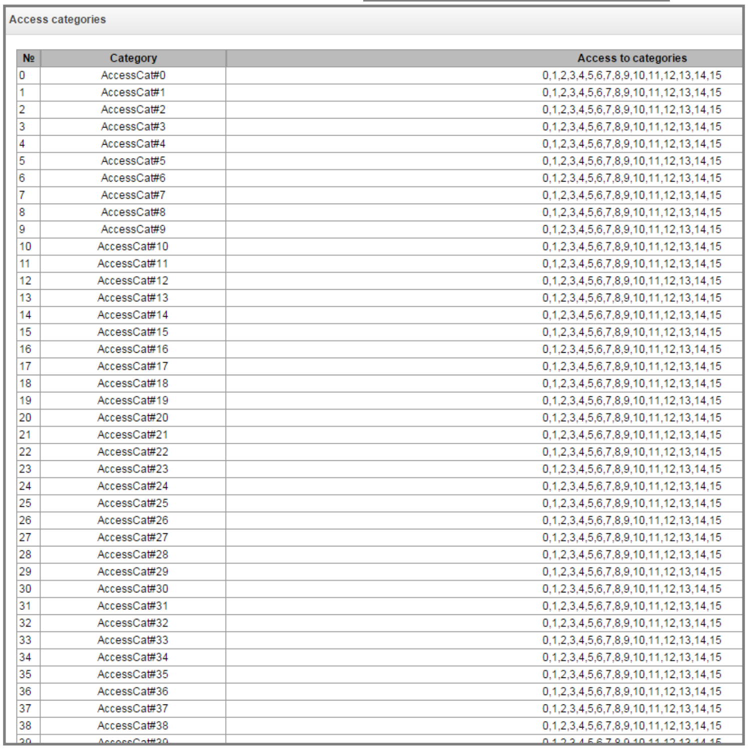
3.1.8.2 Access categories

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).

128access 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.



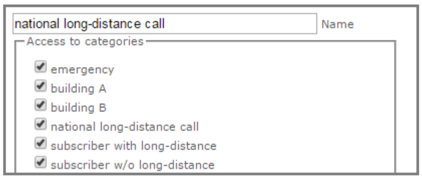
Access categories

№	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

Access restriction configuration example

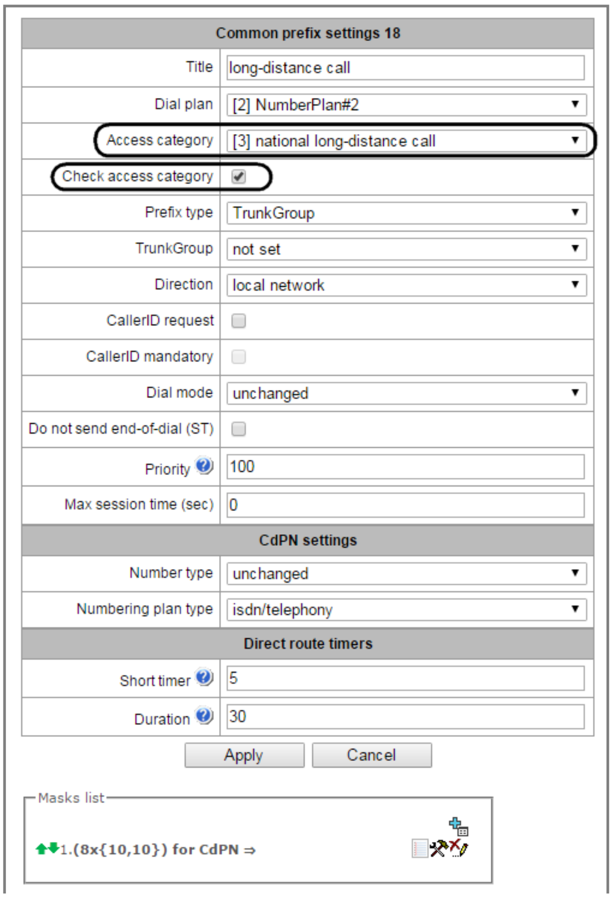
To restrict the long-distance communication, you should:

1. Select an access category for the long-distance communication. Specify name 'Long-distance' or *'Transition to 8'* for convenience.



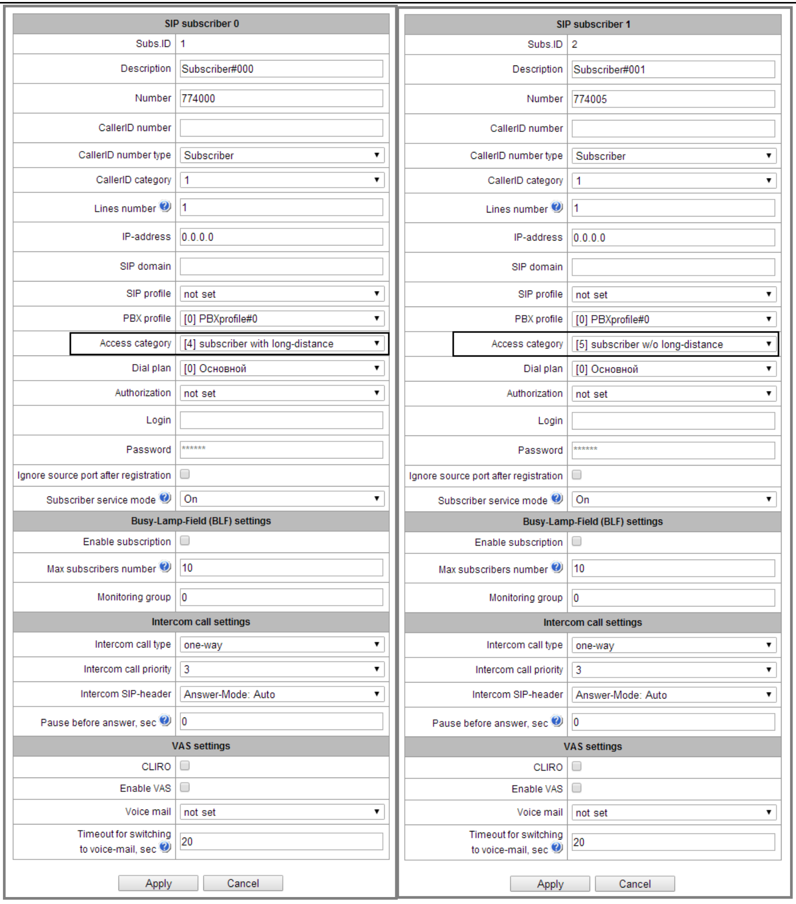
2. Select 2 categories for subscribers: *«Subscriber with LD»* and *«Subscriber without LD»* and allow/deny an access to *'Long-distance'* category respectively (select/deselect the checkbox next to *'Long-distance'* category).

3. For transition to 8 prefix, select *'Long-distance'* category and *'Check access category'* checkbox.



4. Assign *«Subscriber with LD»* category to subscribers with enabled access to long-distance communication.

5. Assign *«Subscriber without LD»* category to subscribers with disabled access to long-distance communication.

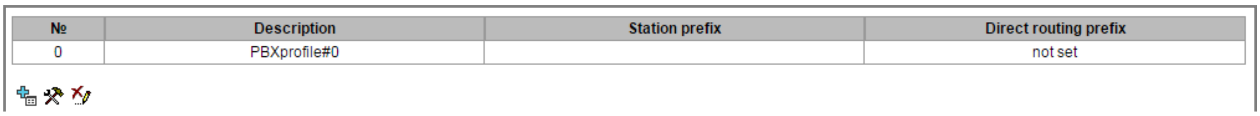


Items 4 and 5 may be performed via subscriber group editing:

- **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 profiles allow for assignment of additional parameters to SIP subscribers.



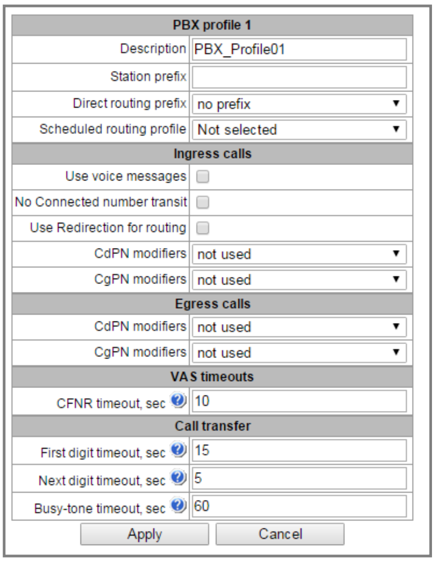
№	Description	Station prefix	Direct routing prefix
0	PBXprofile#0		not set

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'*

—*'Removeprofile'*



PBX profile:

- *Profile name*—name of the profile.
- *PBX prefix*—prefix added into the beginning of the SIP subscriber number (CgPN).
- *Direct 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 dialled number (without mask creation in prefixes).

- *Scheduled routing profile*—select 'scheduled routing' service profile, configured in the 'Internal resources' section.

Incoming communication:

- *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).
- *Block Connected number transmission*—disable transmission of the *Connected number* field.
- *Use Redirecting 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 numbering schedule 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.

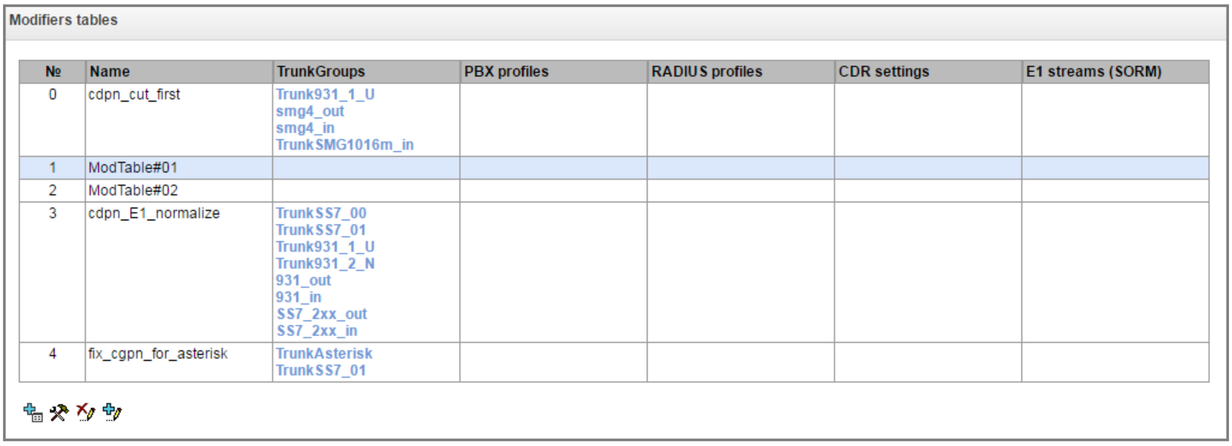
VAS timers:

- *Call forward on no reply (CFNR) timeout, seconds*—timeout upon the expiration of which the call forward on no reply VAS will be activated when the call comes to the subscriber, range is from 5 to 60 seconds.

Call transfer:

- *First digit dial timeout, seconds*—dialling 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 dial timeout, seconds*—dialling 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, seconds*—busy tone timeout for the unsuccessful dialling during 'call transfer' service. When this timeout expires, call will be switched to the subscriber being on hold.

3.1.8.4 Modifier tables

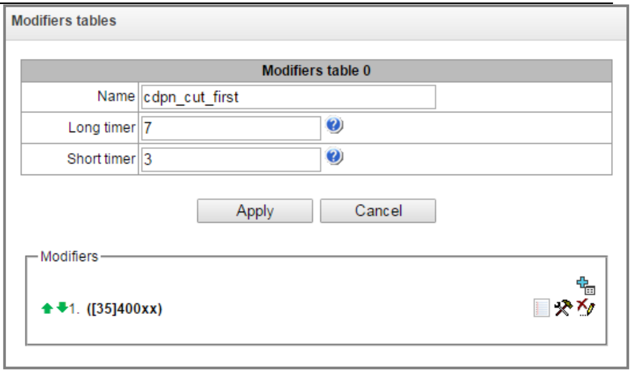


Modifiers tables

№	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:



— *'Add modifier'*

— *'Edit modifier parameters'*

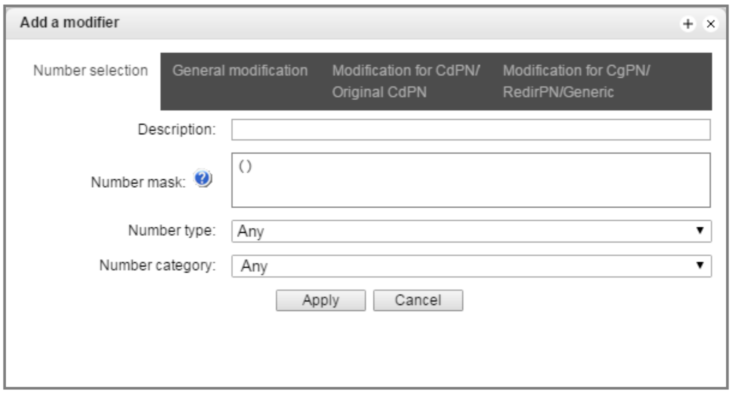
— *'Removemodifier'*

— *'Add modifier by copying'*

To assign/edit parameters of created modifier, select the respective row and click .

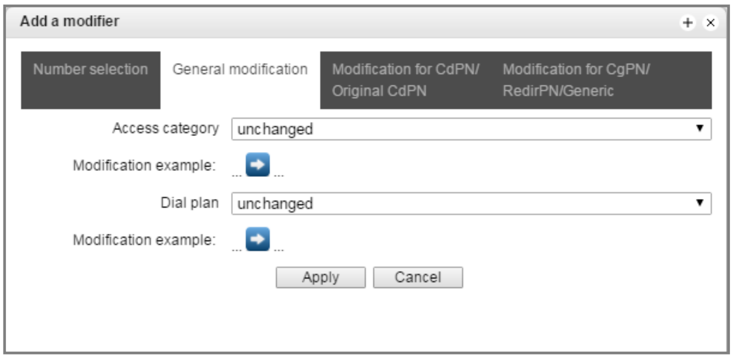
To confirm changes of the modifier parameters, click *'Set'* button; or click *'Cancel'* to exit without saving changes.

3.1.8.4.1 *Number selection* tab



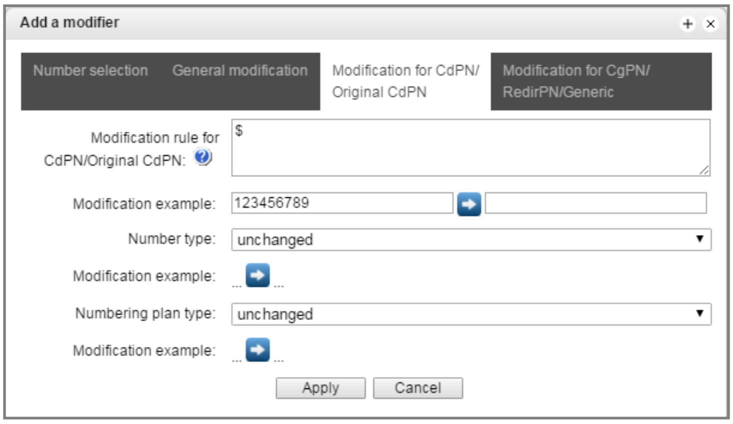
- *Description*—modifier description.
- *Number mask*—template or set of templates that the subscriber number will be compared with (for mask syntax, see Section 3.1.6.21).
- *Number type*—subscriber number type:
  - *Subscriber*—subscriber number (SN) in E.164 format.
  - *National*—national number. Number format: NDC + SN, where NDC—geographical area code.
  - *International*—international number. Number format: CC + NDC + SN, where CC—country code.
  - *Network specific*—specific network number.
  - *Unknown*—unknown number type.
  - *Any*—modification will be performed for any number type.
- *Caller ID category*—subscriber's Caller ID category.

3.1.8.4.2 *General modification* tab



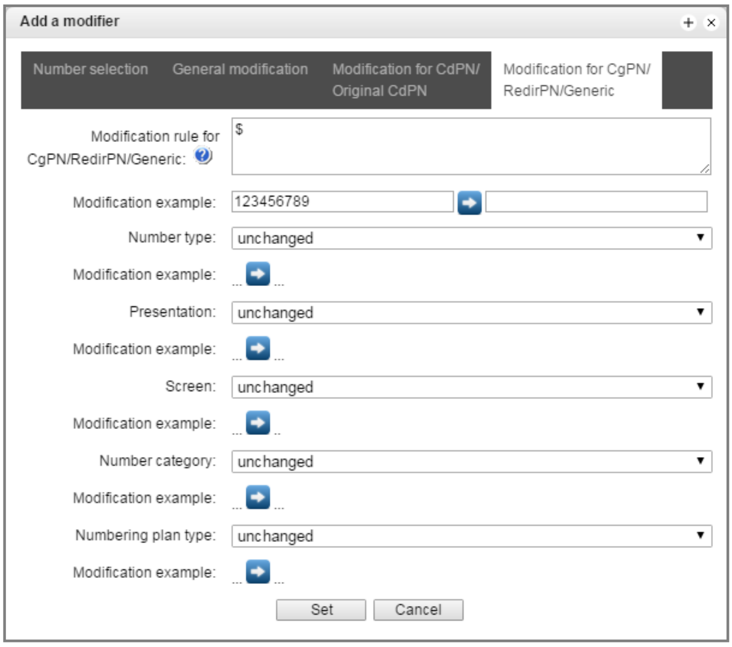
– *Modification example*—click button to view the modification summary after application of the modification rules specified.
  – *Access category*—allows to modify the access category.
  – *Numbering schedule*—allows to modify numbering schedule that will be used for further routing (necessary for numbering schedule negotiation).

3.1.8.4.3 ***CdPN/Original CdPN modification*** tab



– *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.
– *CdPN/Original CdPN modification rule*—callee number modification rule. For syntax being used, see Section **3.1.8.4.5**; 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.
– *Called number type*—callee number type modification rule.
– *Numbering schedule type*—numbering schedule type modification rule.

3.1.8.4.4 ***CgPN/RedirPN modification*** tab



– *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.

– *CgPN/RedirPN modification rule*—callee number modification rule. For syntax being used, see Section **3.1.8.4.5**; 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.
– *Calling number type*—caller number type modification rule.
– *Calling presentation*—caller presentation modification rule.
– *Calling screen*—caller screen indicator modification rule.
– *Caller ID*—caller category modification rule.
– *Numbering schedule type*—numbering schedule type modification rule.

3.1.8.4.5 Modification rule syntax

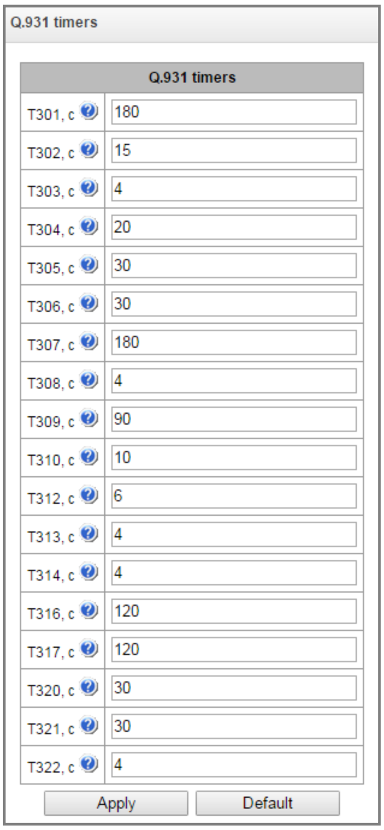
Modification rule is a set of special characters that govern number modifications:
– **'.'** and **'-'**: special characters indicating the removal of digits at the current position and the transposition of digits that follow to a location of that digit.
– **'X'**, **'x'**: special characters indicating 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.

3.1.8.5 Q.931 timers

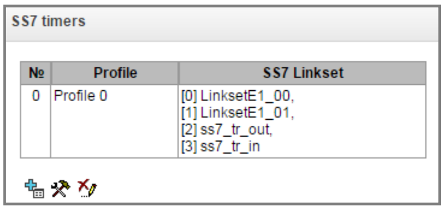
In this section, you may configure third level timers required for Q.931 signalling protocol operation.

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
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



3.1.8.6 SS-7 timers



In this section, you may configure MTP2, MTP3 and ISUP level timers of SS-7 protocol.

To create, edit or remove a profile, use the following buttons:

—*'Add profile'*

—*'Edit profile parameters'*

—*'Removeprofile'*

- *No.*—SS-7 timer profile sequence number.
- *Profile*—profile name.
- *SS-7 line group*—list of SS-7 line groups that have this profile selected.

Profile settings:

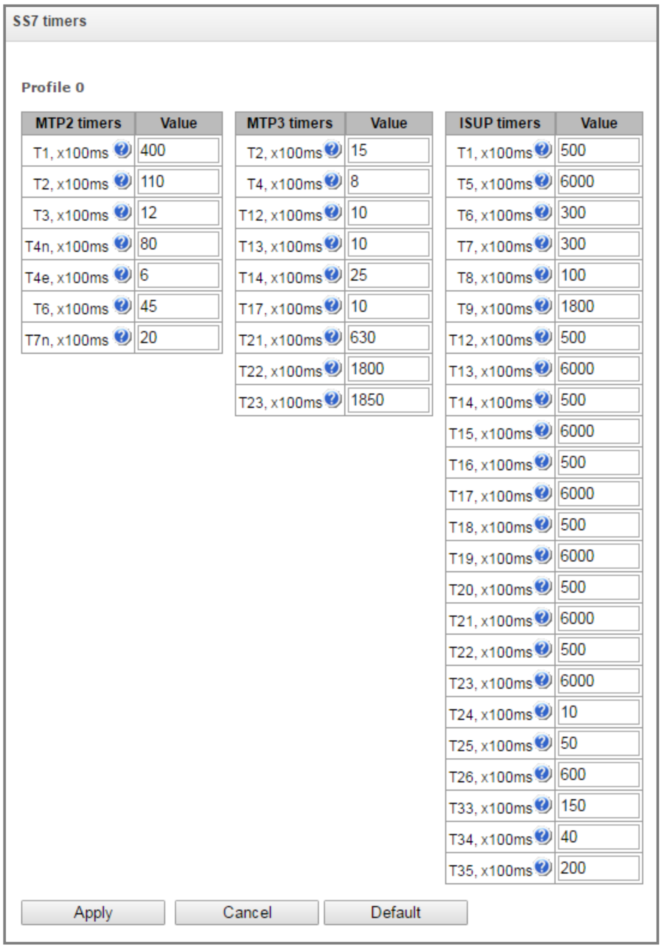


Table 19—For MTP2 level timers name and default settings, see Q.703 ITU-T recommendation, Paragraph 12.3, Timers.

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—For MTP3 level timers name and default settings, see Q.704 ITU-T recommendation, Paragraph 16.8, Timers and timer values.

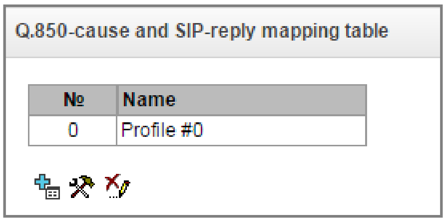
Name	Default value, seconds	Range, seconds
T2	2	0.7 – 2
T4	1.2	0.5 – 1.2
T12	1.5	0.8 – 1.5
T13	1.5	0.8 – 1.5
T14	3	2 – 3
T17	1.5	0.8 – 1.5
T22	180	180 – 360
T23	180	180 – 360

Table 21—For ISUP level timer name and default values, see 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 clearback reasons described in Q.850 recommendations for SS-7, PRI protocols and 4xx, 5xx, 6xx class SIP replies.



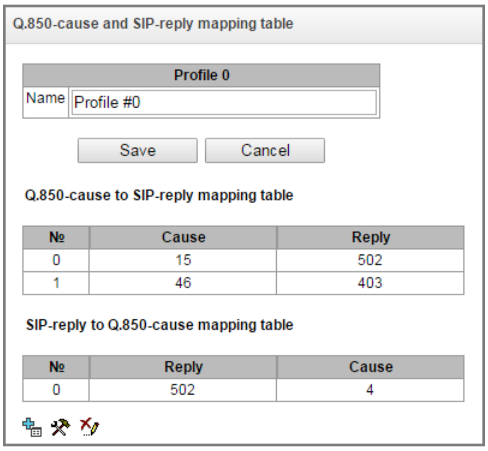
By default, the correspondence is used described in the Order no.10 dated 27.01.2009 issued by Ministry of Communications and Mass Media (MinComSvyaz) of the Russian Federation; for reasons not described in this Order, correspondence described in Q.1912.5 recommendation for SIP-I and RFC3398 for SIP/SIP-T is used.

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

—*'Add rule'*

—*'Edit rule parameters'*

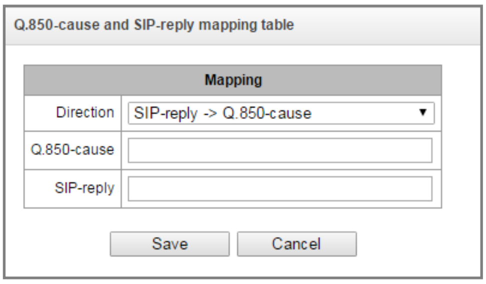
—*'Removerule'*



– *Name*—Q.850-cause and SIP-reply correspondence table name.

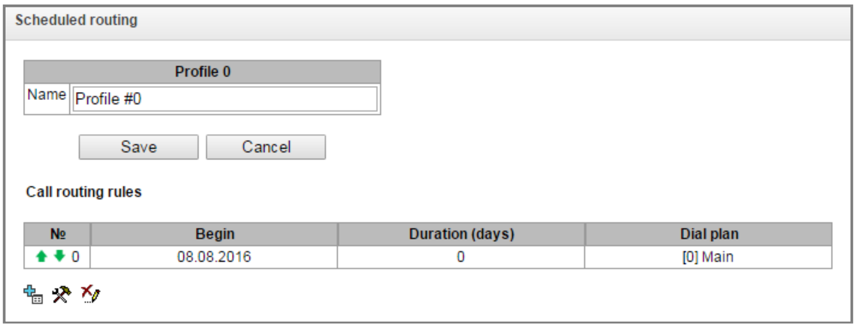
Profile settings:

- *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 numbering schedules depending on the time and day of the week.



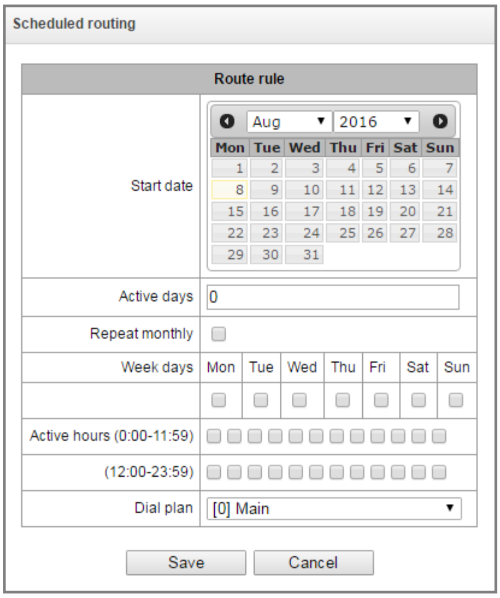
To create, edit or remove rules, use the following buttons:

—*'Add rule'*

—*'Edit rule parameters'*

—*'Removerule'*

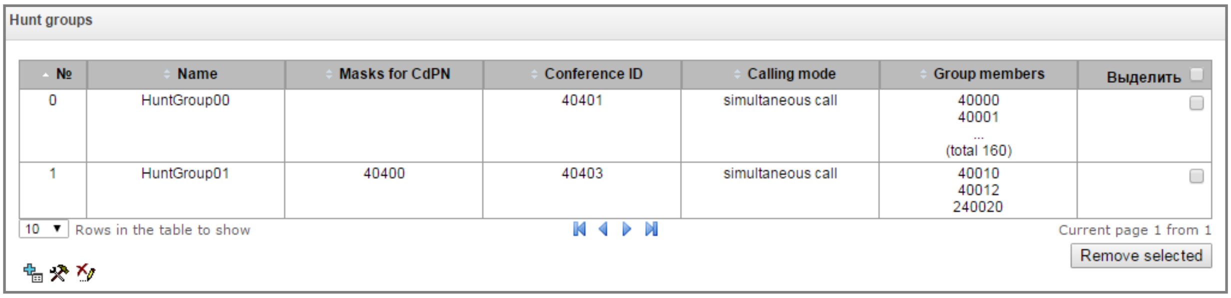
Routing rule:



- *Operation period start date*—select start date for scheduled routing rule operation.
- *Operation duration (days)*—scheduled routing rule operation duration.
- *Repeat each month*—option that allows you to set the repetition of routing rule operation for each month.
- *Days of the week*—select days of the week for scheduled routing rule operation.
- *Hours of operation*—select hours for scheduled routing rule operation
- *Numbering schedule*—select routing schedule 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

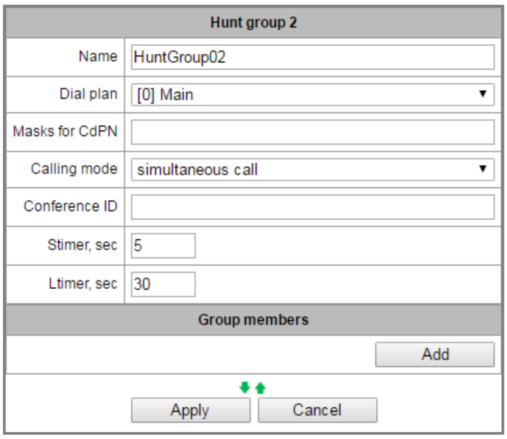
To create, edit or remove table records, use the following buttons:

—*'Add record'*

—*'Edit record parameters'*

—*'Removerecord'*

The call group may contain numbers of device subscribers as well as the external numbers.



- *Name*—call group name.
- *Numbering schedule*—select numbering schedule 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 numbering schedule designed for further call routing (for mask syntax, see Section 3.1.6.2).
- *Operation mode*—call group member ringing method:
  - *simultaneous call*—simultaneous call for all call group members.
  - *from first by one*—method that always dials the first number in the call group number list when

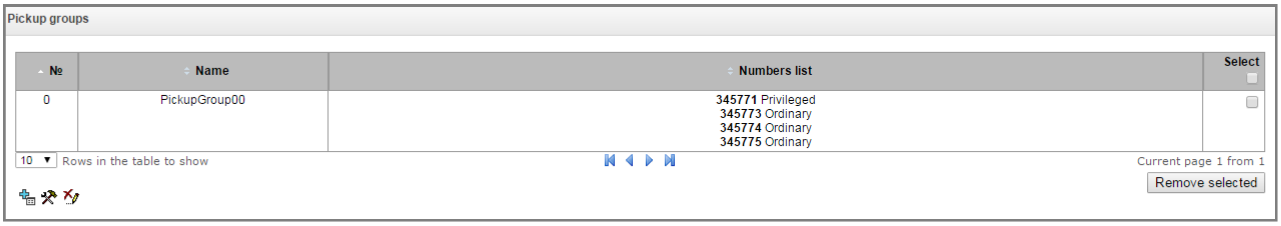
[1]This option is available only when SMG-VAS license is available; for license details, see Section **3.1.23 Licenses**

a new call comes to this group; when Stimer expires, call addressed to the current group member will be cancelled and the call will be addressed to the next group member.

  - *sequentially by one*—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 payload balancing between the group members; when Stimer expires, call addressed to the current group member will be cancelled and the call will be addressed to the next group member.
  - *from first adding next*—method that always dials the first number in the call group number list when a new call comes to this group; when Stimer expires, call addressed to the current group member will not be cancelled and the call will be addressed to the next group member.
  - *sequentially adding 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 payload balancing between the group members; when Stimer expires, call addressed to the current group member will not be cancelled and the call will be addressed to the next group member.
  - *serial discovery (from first)*—method that will discover the first available subscriber from the beginning of the list; members of this group may only include the subscribers of this gateway.
  - *serial discovery (from last)*—method that will discover the first available subscriber from the end of the list; members of this group may only include the subscribers of this gateway.
- *Conference number*—number that when dialled after the service prefix VAS Conference all members of this group will be added to a conference call.
- *Stimer, seconds*—call timeout for a single call group member.
- *Ltimer, seconds*—general call timeout for the whole call group.
- *Number list*—call group contents, up to 20 members.

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 dialling an exit prefix for this call group.



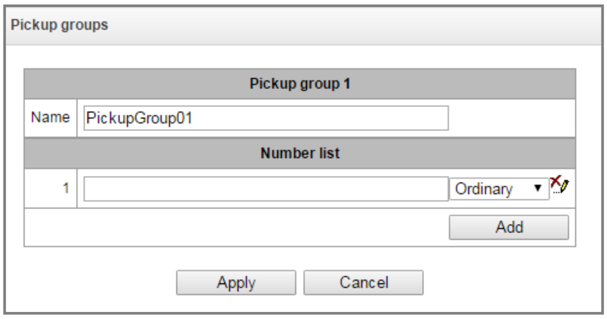
To create, edit or remove table records, use the following buttons:

— *'Add record'*

— *'Edit record parameters'*

— *'Removerecord'*

Group may contain device subscribers only.



– *Name*—pickup group name.
– *Number list*—pickup group contents.

Pickup group member type

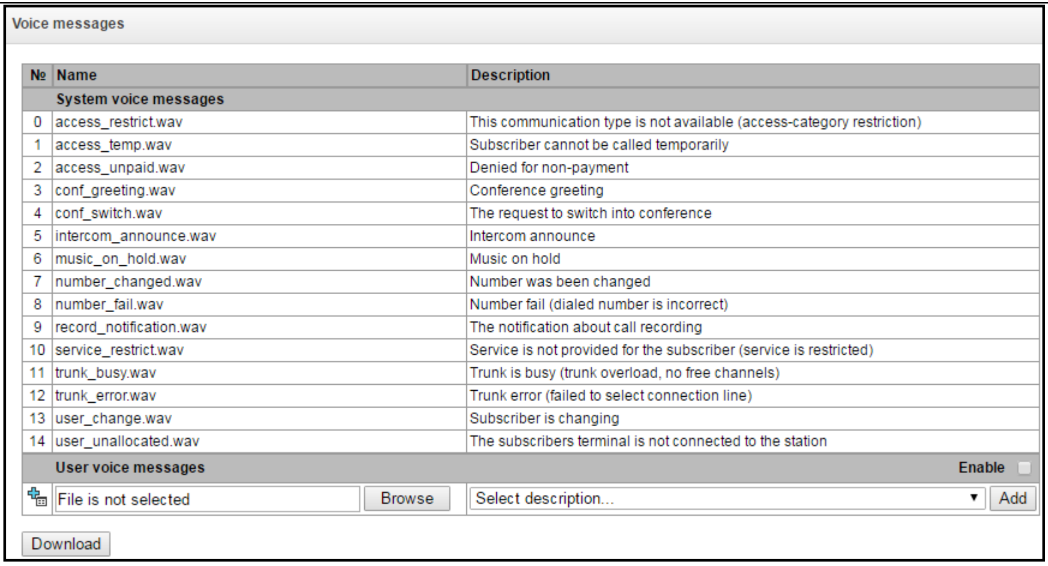
– *limited*—cannot perform the pickup, but the call directed at that member may be picked up by another group member.
– *common*—may pickup calls directed at common and limited members, but cannot pickup calls directed at privileged group member.
– *privileged*—may pickup calls directed at any pickup group member.

3.1.8.11 Voice messages

The device features 11 standard voice message phrases that are used for information provisioning 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.

[1]This option is available only when SMG-VAS license is available; for license details, see Section **3.1.23Licences**



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

Download

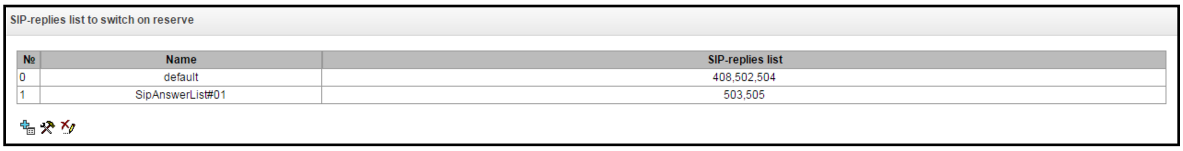
– *No.*—voice message file sequential number.
– *Name*—voice message file name.
– *Description*—voice message file description.

To add a custom file and select description of an event for this file to be played, click *'Select file'* and *'Add'* buttons.

– *Enable*—enable voice message file playback.

3.1.8.12 SIP response list for redundant trunk group transition

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.

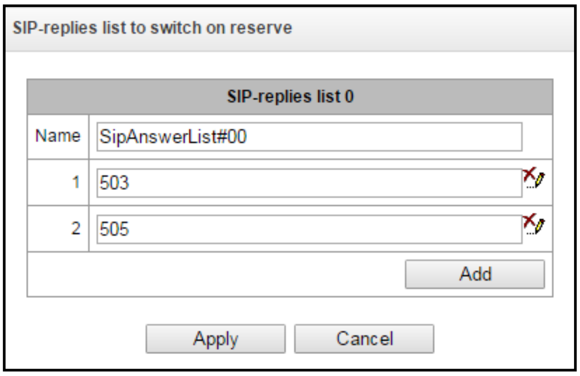


SIP-replies list to switch on reserve

№	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:

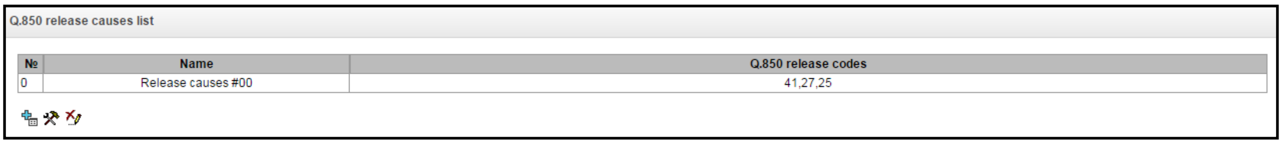
– *'Add reply list'*
– *'Edit reply list'*
– *'Remove reply list'*



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

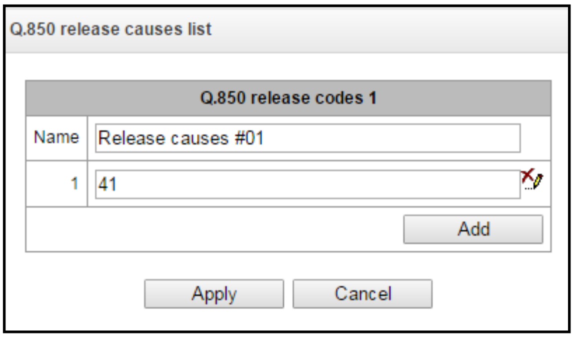
3.1.8.13 Q.850 release causes list

In this section, you may configure the list of Q.850 clearback reasons for SS-7 and Q.931 protocols that will be used for transition to the redundant trunk group or the next trunk of the trunk direction.



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'*



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 a must for call centres, 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 IVR scenario list

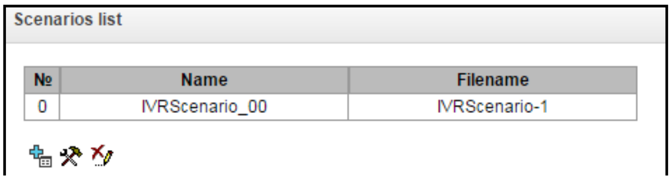
In this section, you may create IVR[1] service operation scenarios.

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

—*'Add record'*
—*'Edit record parameters'*
—*'Removerecord'*

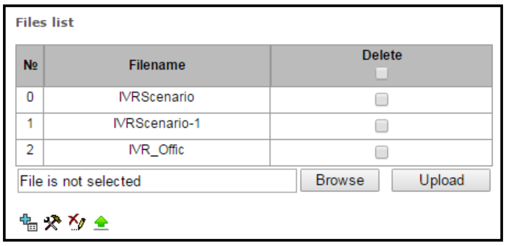
The table **'Scenario list'—**this table contains all created IVR scenarios.

[1]This option is available only when SMG-IVR license is available; for license details, see Section **3.1.23 Licenses**



– *Name*—IVR scenario name.
– *File name*—select IVR scenario file from the list of files created on the device.

The table **'Common scenario list'**—this table contains all IVR common scenario files available for editing.



The table **'File list'**—this table contains created IVR scenario files.

To specify the drive for scenario file storage, see Section **3.1.1 System parameters**.

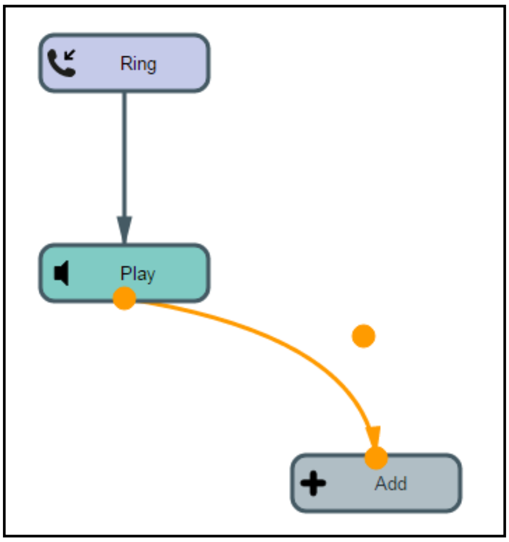
- *'Download scenario'*—download selected scenarios to the user PC.

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.

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.



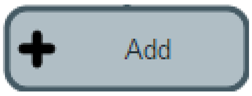
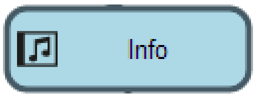
To remove the selected block from the flowgraph, click *'Remove block'* button.If this block has any lower-level logical connections, the whole branch of its child objects will be removed.

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.

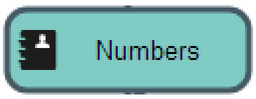
Also, you may left-click the logical connection between blocks, to change its type. Selected line will turn orange and three edit points will appear: for configuration of block exit location, block entry location and line curvature.

For IVR block description, see 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 **3.1.8.11Voice messages**. To specify the drive for file storage, see Section **3.1.1System parameters.** *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 parameters.** *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 dialling using internal numbering schedule 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 **3.1.9.2IVR audio 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 dialling timer; when this timer expires, IVR outbound branch will be selected. *Enable extension dialling*—when checked, extension dialling will be enabled followed by the device numbering schedule routing, e.g. internal subscriber number can be dialled. *Access category*—select access category. Access category allows you to define call barring for the number dialled by the subscriber in IVR block. *Quantity of digits for extension dialling*—maximum quantity of digits that can be dialled in the extension dialling. *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 dialling 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 dialling, the number routing will be performed according to the device numbering schedule. **Parameters** *Number*—specified number. **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 onewhen 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 onewhen 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 onewhen 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 **3.1.17.1Recording parameters**, 'IVR conversation recording folder name' parameter. For recording management, see Section **3.1.9.3Conversation recordings**.
	**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 IVR audio list

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

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

- *IVR audio*—list of uploaded files.
- *Duration*—uploaded file length.
- *Select file*—select the audio file to be uploaded to the device.
- *Upload*—command to upload the selected file.

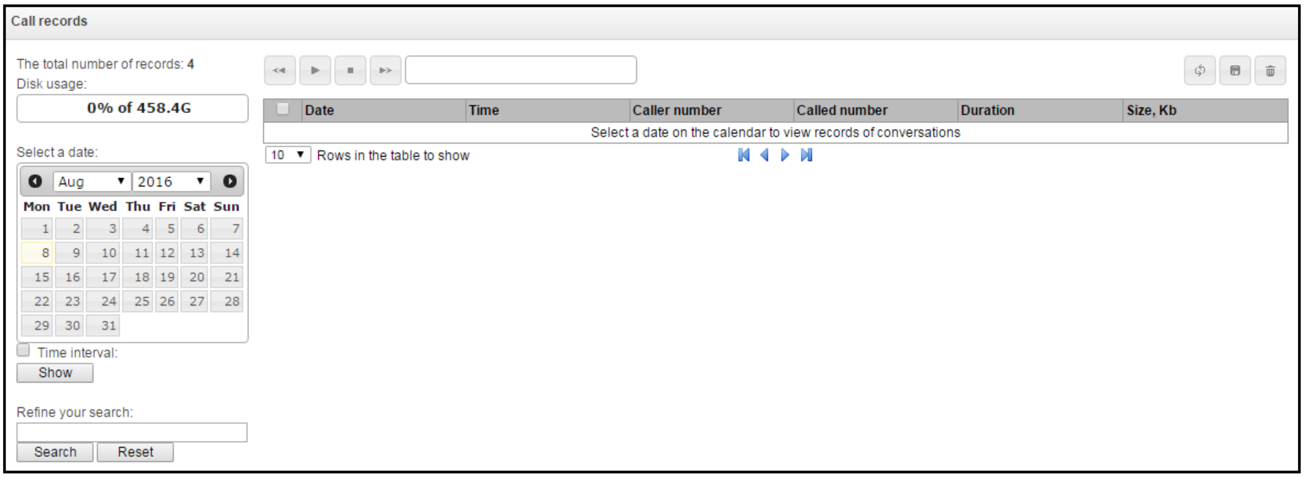
You may upload tar or zip archive file containing multiple audio files; audio files should be in the root directory of the archive.

– *Play*—listen to the selected file.
– *Stop*—stop the file playback.
– *Remove*—delete the selected file.
– *Download*—download the selected file from the device.

To specify the drive for file storage, see Section **3.1.1 System parameters**.

3.1.9.3 Conversation recordings

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.



– *Total record count*—total quantity of conversation recording files in the selected directory for conversation recordings.
– *Disk utilization*—display used space on disk selected for conversation recording.
– *Select 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 23—Record control buttons

Button	Function
	previous record
	begin playback
	stop playback
	next record
	repeat record playback
	save record
	delete record

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.

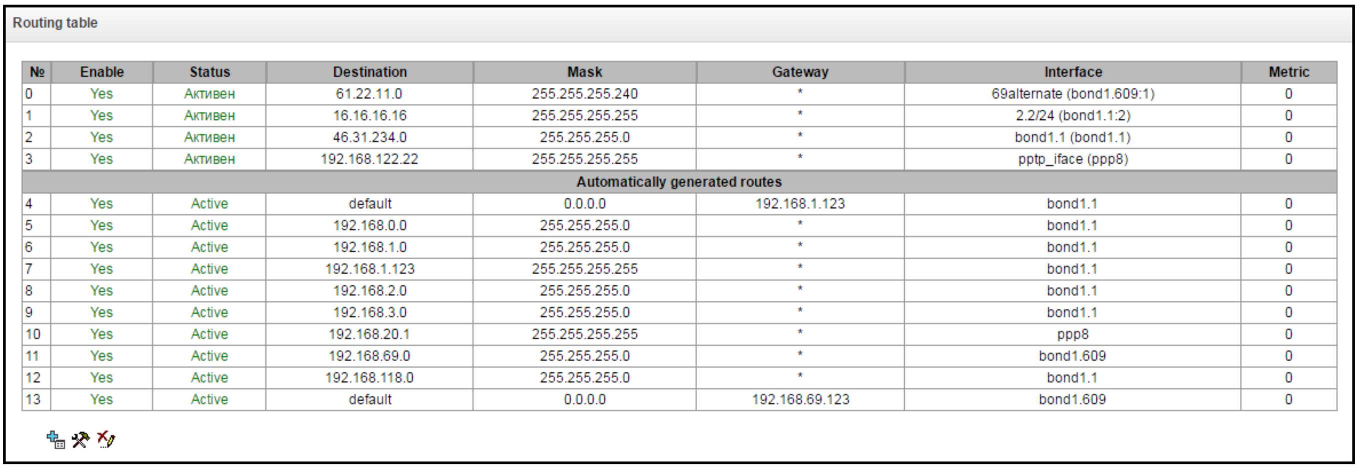
3.1.10.1 Routing table

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

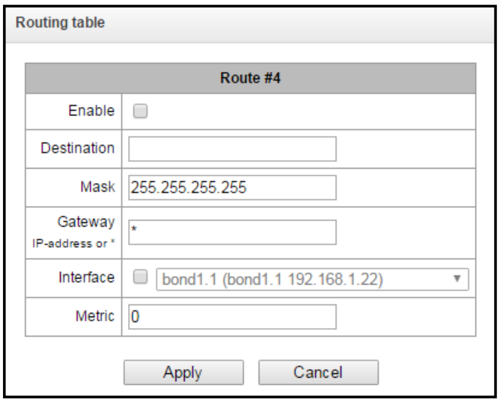
№	Enable	Status	Destination	Mask	Gateway	Interface	Metric
0	Yes	Активен	61.22.11.0	255.255.255.240	*	69alternate (bond1.609:1)	0
1	Yes	Активен	16.16.16.16	255.255.255.255	*	2.2/24 (bond1.1:2)	0
2	Yes	Активен	46.31.234.0	255.255.255.0	*	bond1.1 (bond1.1)	0
3	Yes	Активен	192.168.122.22	255.255.255.255	*	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:

— *'Add route'*

— *'Edit route parameters'*

— *'Removeroute'*

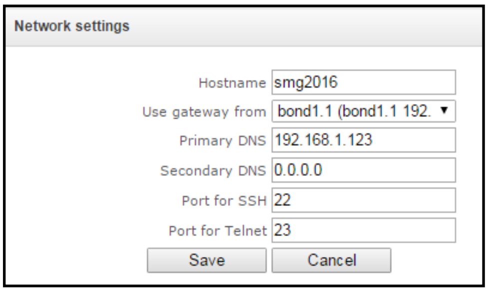


Route parameters:

- *Enable*—when checked, the route is enabled.
- *Direction*—IP network.
- *Mask*—specify a network mask for the defined IP network (use mask 255.255.255.255 for IP address).
- *Interface*—select network transfer interface.
- *Gateway*—define IP address of route gateway.
- *Metrics*—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.



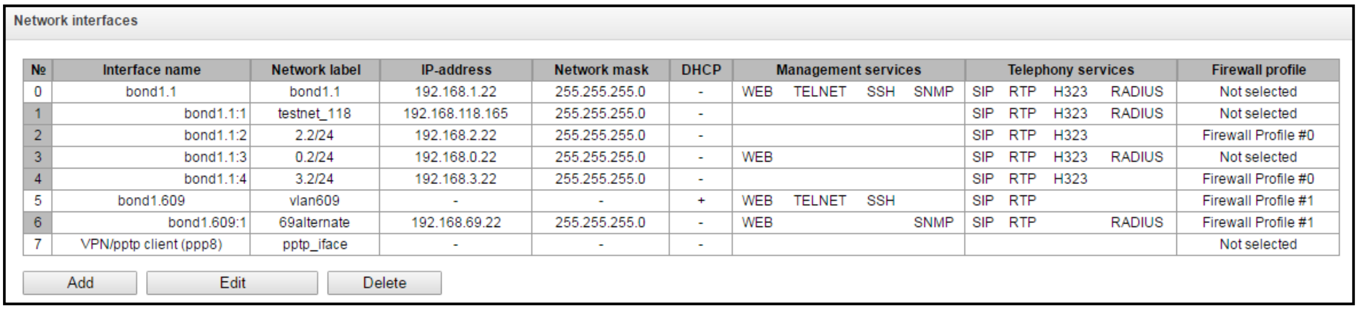
- *Hostname*—device network name.
- *Use interface gateway*—select network interface that the gateway will consider as a primary for the device.
- *DNS primary*—primary DNS server.
- *DNS secondary*—secondary DNS server.

- *ssh access port*—TCP port for the device access via SSH protocol, default value is 22.
- *Telnet access port*—TCP port for the device access via Telnet protocol, default value is 23.

3.1.10.3 Network interfaces

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 VLAN interface.

Alias is an additional network interface based on the existing primary network interface eth0 or VLAN interface.



Network interfaces

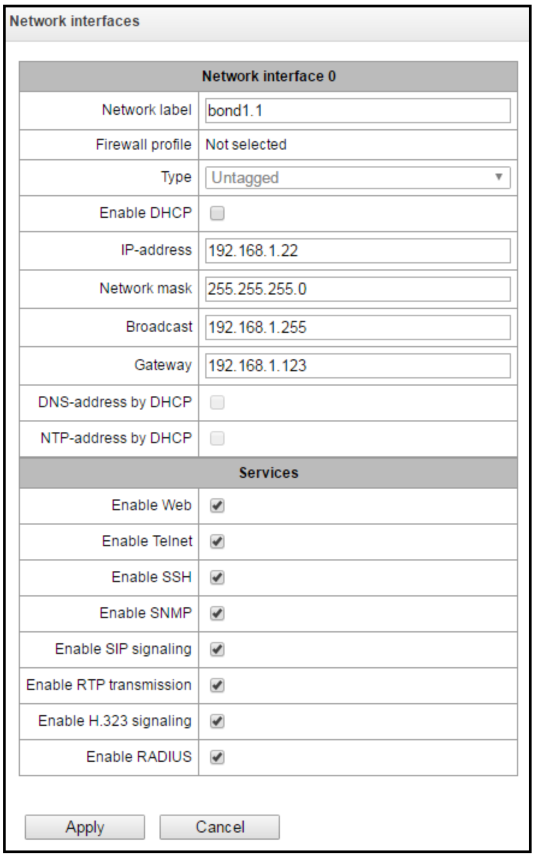
№	Interface name	Network label	IP-address	Network mask	DHCP	Management services	Telephony services	Firewall profile
0	bond1.1	bond1.1	192.168.1.22	255.255.255.0	-	WEB TELNET SSH SNMP	SIP RTP H323 RADIUS	Not selected
1	bond1.1:1	testnet_118	192.168.118.165	255.255.255.0	-		SIP RTP H323 RADIUS	Not selected
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

Add Edit Delete

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

Add
Edit
Remove

Network interface settings:



<u>*Basic settings:*</u>

- *Network name*—network name.
- *Firewall profile*—show the selected firewall profile for the current interface.
- *Type*—interface type (always untagged for eth0 interface).
- *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.
- *Subnet mask*—device network address.
- *Broadcast*—address for broadcasting packets.
- *Gateway*—network gateway for the current interface (not supported for aliases).
- *Obtain DNS automatically*—obtain DNS server IP address dynamically from DHCP server (not supported for aliases).
- *Obtain NTP automatically*—obtain NTP server IP address dynamically from DHCP server (not supported for aliases).

<u>*Services*</u>—configuration menu for services that are enabled the current interface:

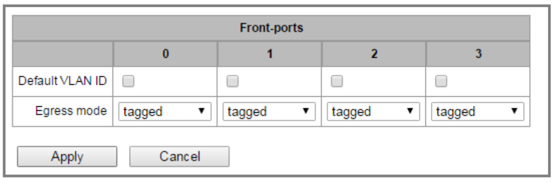
- *Management via Web*—enables access to configurator through the interface
- *Management via Telnet*—enables access via telnet protocol through the interface.
- *Management via SSH*—enables access via ssh protocol through the interface.
- *Enable SNMP*—enables SNMP utilization through the interface.

- *Send RTP*—enables voice traffic reception and transmission through the network interface configured in this section.
- *SIP signalling*—enables SIP signalling information reception and transmission through the network interface configured in this section.
- *RTP signalling*—enables RTP signalling information reception and transmission through the network interface configured in this section.
- *H.323 signalling*—enables H.323 signalling information reception and transmission through the network interface configured in this section.
- *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 for *'Type'* parameter).

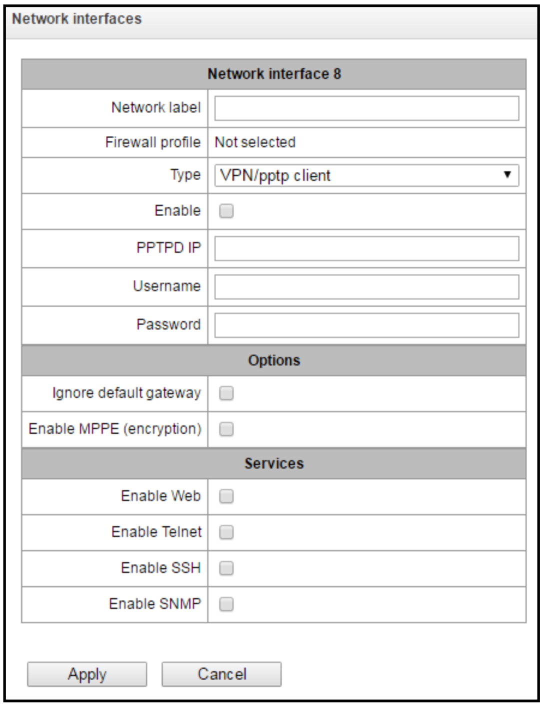


- *Default VLAN ID*—when a packet without VLAN ID tag comes to the port, this packet will be tagged with VLAN ID tag of the selected network interface, if the packet is received with VLAN ID tag, this tag remains unchanged.
- *Egress mode*—VLAN tag operation rules during packet transfer from the port:
  - *tagget*—send packet with the selected interface VLAN ID.
  - *untagget*—send packet without VLAN ID.

VPN/PPP interface settings:

Basic settings:

- *Network name*—network name.
- *Enable*—enable VPN/PPP interface.
- *Firewall profile*—show the selected firewall profile for the current interface.
- *Type*—VPN/pptp client.
- *PPTPD IP*—PPTP server IP address.
- *User name*—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.
- *Enable encryption*—enable encryption.

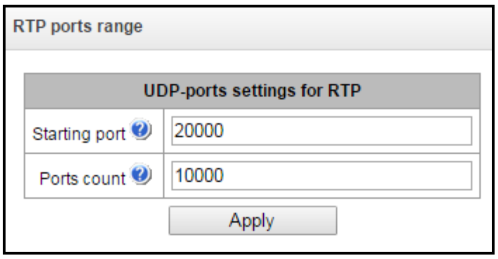
Services—configuration menu for services enabled the current interface:

[1]For SMG-2016 only

- *Management via Web*—enables access to configurator through the interface
- *Management via Telnet*—enables access via telnet protocol through the interface.
- *Management via SSH*—enables access via ssh protocol through the interface.
- *Enable SNMP*—enables SNMP utilization through the interface.
- *Enable RADIUS*—enables RADIUS protocol utilization through the interface.

3.1.10.4 RTP port range

In this section, you may configure UDP port range for voice RTP packets transmission.



UDP port parameters:

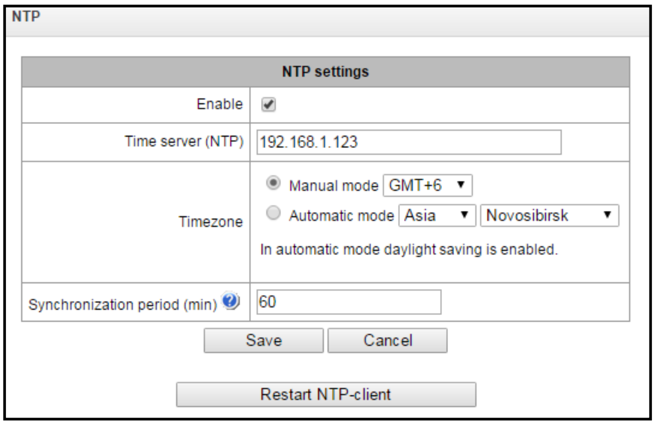
- *Starting port*—starting UPD port number used for voice traffic (RTP) and data transmission via T.38 protocol.
- *Port range*—range (quantity) of UPD ports used for voice traffic (RTP) and data transmission via T.38 protocol.

To avoid conflicts, ports used for RTP and T.38 transmission should not overlap the ports used for SIP signalling (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.



- *Use NTP*—enable time synchronization via NTP.
- *Obtain settings automatically*—when checked, use NTP server address obtained via DHCP.
- *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.
- *NTP synchronization period, minutes*—time synchronization request transmission period.

- *Save*—save changes.
- *Discard*—discard changes.

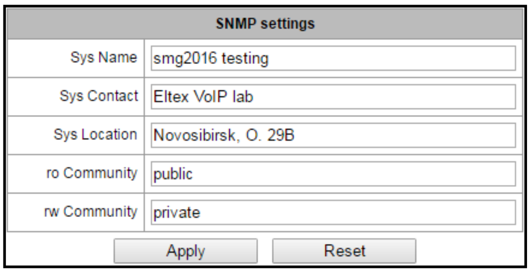
To perform forced time synchronization with the server, click *'Restart NTP client'* button (NTP client will be restarted).

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
- Callee IP address
- Callee number
- Channel engagement duration



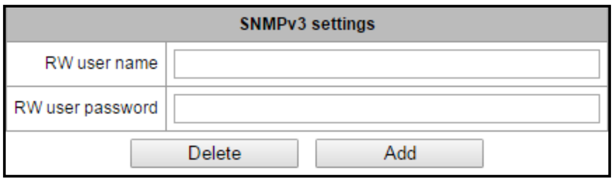
- *Sys Name*—device name.
- *Sys Contact*—contact information.
- *Sys Location*—device location.
- *ro Community*—parameter read password/community.
- *rw Community*—parameter write password/community.

- *Apply*—apply changes.
- *Discard*—discard settings.

3.1.11.3 SNMPv3

SNMPv3 configuration:

The system uses a single SNMPv3 user. SNMPv3 user is used for SORM commands transmission to SMG gateway.



- *RW User name*—username.
- *RW User password*—password (password should contain 8 characters or more).

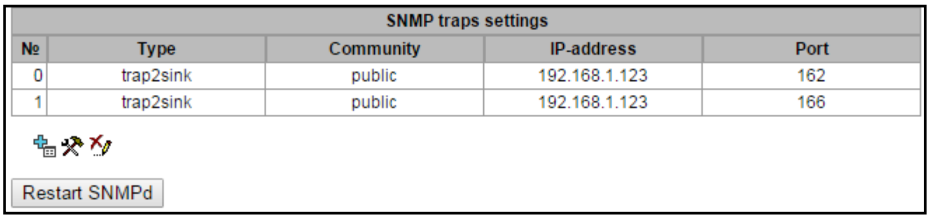
To apply SNMPv3 user configuration, click *'Add'* button (settings will be applied immediately). To remove a record, click *'Remove'* button.

3.1.11.4 SNMP trap configuration

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
– SS-7 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
– SS-7 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

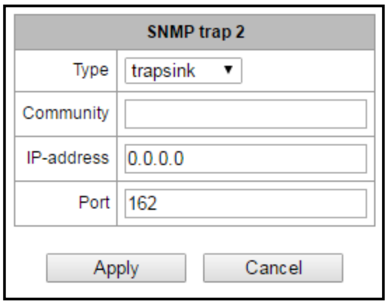


SNMP traps settings				
№	Type	Community	IP-address	Port
0	trap2sink	public	192.168.1.123	162
1	trap2sink	public	192.168.1.123	166

– Restart SNMPd—*click the button to restart SNMP client.*

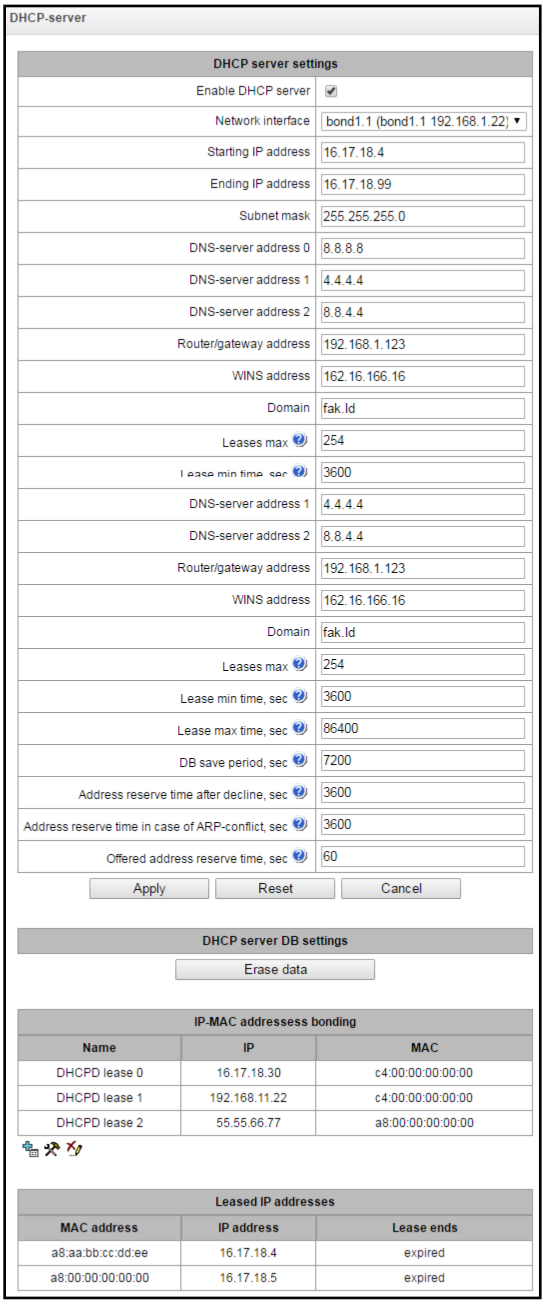
To create, edit or remove trap parameters, use the following buttons:

—*'Add'*
—*'Edit'*
—*'Remove'*



– *Type*—SNMP message type (TRAPv1, TRAPv2, INFORM).
– *Community*—password contained in traps.
– *IP address*—trap 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:

— *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 0/1/2/3 address*—DNS server addresses from the operator's networks.
— *Gateway/router address*—default router or gateway address assigned by DHCP server to clients.
— *Wins address*—WINS server IP address in the operator's network.
— *Domain name*—network domain name.
— *Number of leased addresses*—restrict the number of simultaneously leased addresses.
— *Minimum address lease time, seconds*—set the minimum lease time for IP address assigned by DHCP server to the client, 10 seconds or more.
— *Maximum address lease 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 saving 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 reservation time upon decline reception*—time period that the IP address will remain reserved for the client upon the DHCP decline reception, 10 seconds or more.
— *Address reservation time upon ARP conflict*—time period that the IP address will remain reserved for the client upon MAC address conflict identification, 10 seconds or more.
— *Leased address reservation time, seconds*—time period that the IP address requested by client will remain reserved, 10 seconds or more.

DHCP server management

— *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 address binding—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'*

- *Name*—name of the mapping
- *IP address*—client IP address
- *MAC address*—client MAC address

DHCP lease 3	
Name	DHCPD lease 3
IP address	0.0.0.0
MAC address	00:00:00:00:00:00
Apply	Cancel

Issued IP addresses:

- *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*

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

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

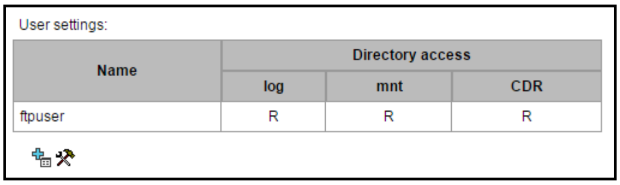
FTP-server settings	
Enable	☑
Network interface	69alternate (bond1.609:1 192.168.69.22)
Port	21
Authorization timeout, sec	120
Idle timeout, sec	180
Session timeout, sec	600
Apply	Cancel

- *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 configuration:

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 log*—log directory access configuration, read/write
– *Access to mnt*—mnt directory access configuration, read/write
– *Access to CDR*—CDR directory access configuration, read/write

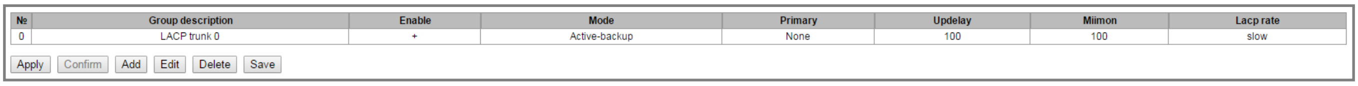
3.1.12 Switch[1]

In *'Switch'* menu, you may configure switch ports.

3.1.12.1 LACP settings

In this section, you may configure LACP groups.

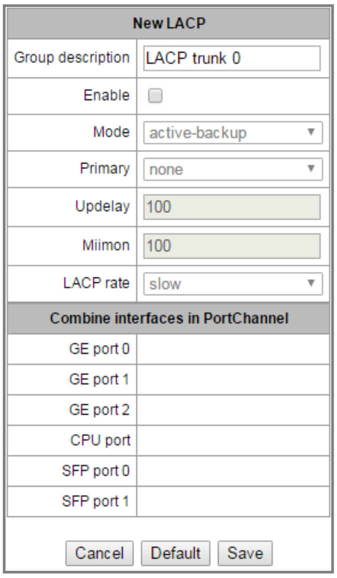
Link Aggregation Control Protocol (LACP) is a protocol, designed for combining multiple physical channels into one logical channel.



№	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



– *Name*—LACP group name
– *Enable LACP*—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.
  – *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

[1]For SMG-1016M only

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-second transmission interval).
- *Combine interfaces in PortChannel*—list of ports added to LACP group.

3.1.12.2 Configuration of switch ports

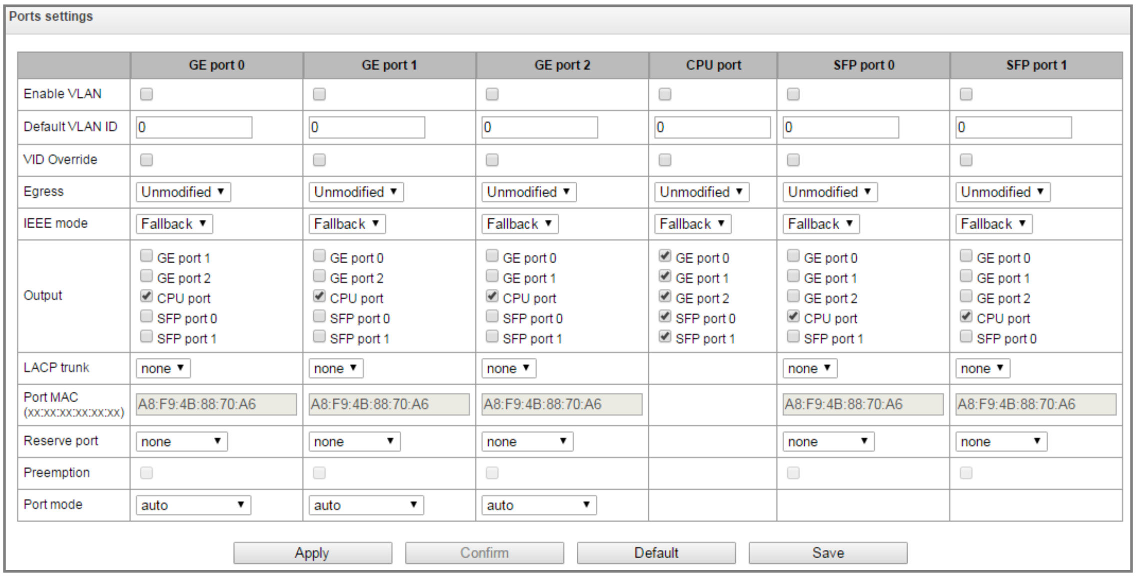
The switch can operate in four modes:

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			

Apply | Confirm | Default | Save

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*—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.
- 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 came with one VLAN tag—if the received packet was untagged.
- *IEEE mode:*
  - *disabled*—for a packet received by this port, routing rules described in the 'output' section of the table will be applied.
  - *fallback*—if a packet with VLAN tag is received through this port, and there is a record in a '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 a '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 a '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.
- *Output*—mutual availability of data ports. Defines privileges that allow packets received by this port to be transferred to flagged ports.
- *Backup 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.
- *Return to master-port*—when checked, return to master port when it becomes available.

This firmware version supports the global dual homing only.

- *Port operation 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 'Commit' 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.)

[1]For SMG-1016M
[2]For SMG-2016

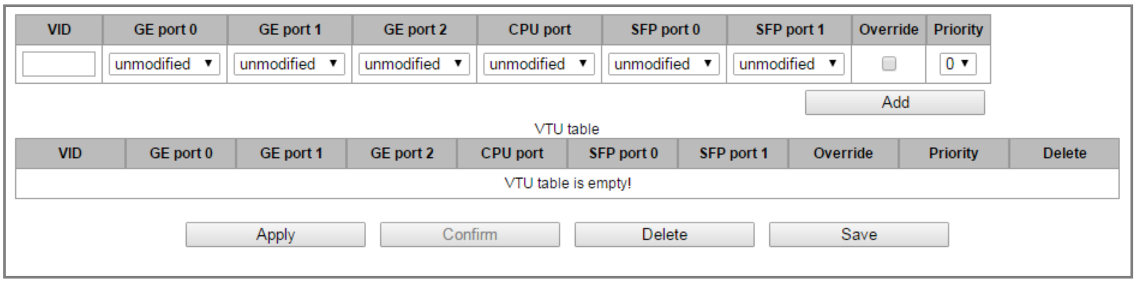
To save settings to the configuration file without applying them, click *'Save'* button.

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.



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.

- *Apply*—apply defined settings.
- *Commit*—commit modified settings.

Click 'Commit' button in 1 minute interval to confirm settings, or the previous values will be restored.

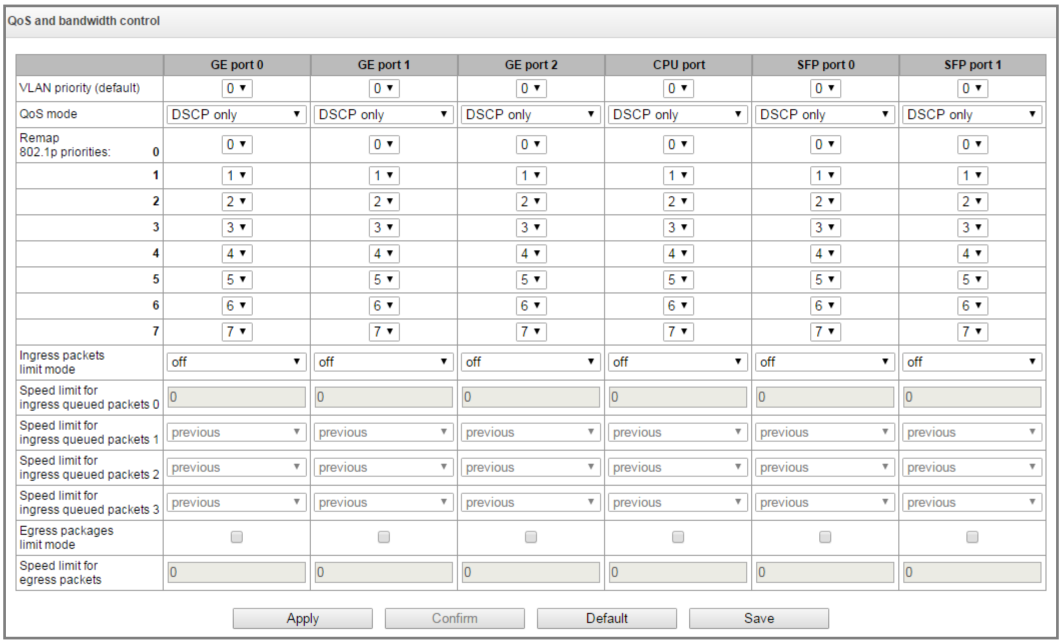
- *Save*—save settings into the device flash memory without applying them.

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.



- *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 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.

- *Remapping 802.1p priority*—remap 802.1p priorities for untagged packets. Thus, a new value may be assigned for each priority received in VLAN packet.
- *Ingress limit mode*—restriction mode for traffic coming to the port.
  - *Off*—no restriction.
  - *All packets*—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.
- *Ingress rate prio 0*—bandwidth restriction for traffic incoming to a queue 0 port. Permitted values—from 70 to 250000kbps.
- *Ingress rate prio 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).
- *Ingress rate prio 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).
- *Ingress rate prio 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 limit on*—when checked, enable the bandwidth restriction for outgoing port traffic.
- *Egress rate limit*—bandwidth restriction for outgoing port traffic. Permitted values—from 70 to 250000kbps.

- *Apply*—apply defined settings.
- *Commit*—commit modified settings.

Click 'Commit' button in 1 minute interval to confirm settings, or the previous values will be restored.

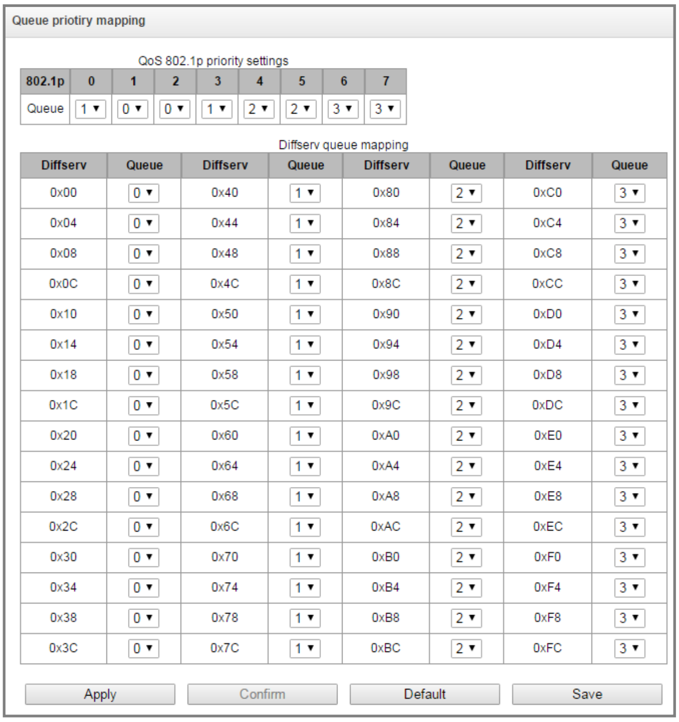
– *Default*—set default settings.
– *Save*—save settings into the device flash memory without applying them.

3.1.12.5 Priority mapping

– *802.1p priorities mapping*—allows to distribute packets into queues depending on the 802.1p priority.
  – *802.1p*—802.1p priority value.
  – *Queue*—outgoing queue number.
– *IP diffserv priorities 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.
– *Commit*—commit modified settings.

Click 'Commit' 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 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

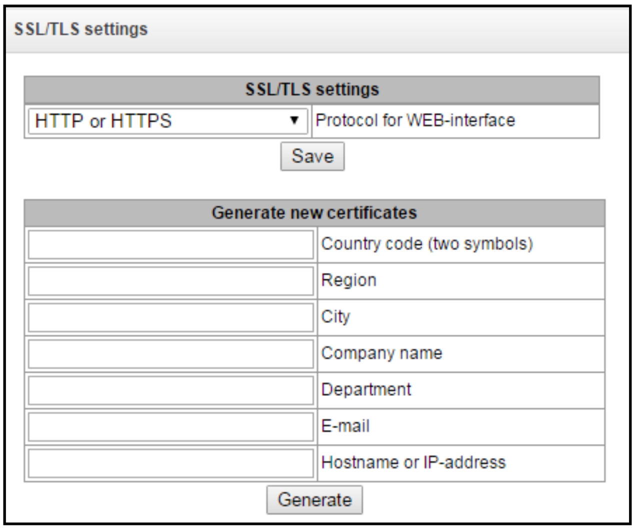
Diffserv	Queue	Diffserv	Queue	Diffserv	Queue	Diffserv	Queue
0x00	0	0x40	1	0x80	2	0xC0	3
0x04	0	0x44	1	0x84	2	0xC4	3
0x08	0	0x48	1	0x88	2	0xC8	3
0x0C	0	0x4C	1	0x8C	2	0xCC	3
0x10	0	0x50	1	0x90	2	0xD0	3
0x14	0	0x54	1	0x94	2	0xD4	3
0x18	0	0x58	1	0x98	2	0xD8	3
0x1C	0	0x5C	1	0x9C	2	0xDC	3
0x20	0	0x60	1	0xA0	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

Apply Confirm Default Save

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 configuration



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.

– *Web configurator interaction protocol*—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

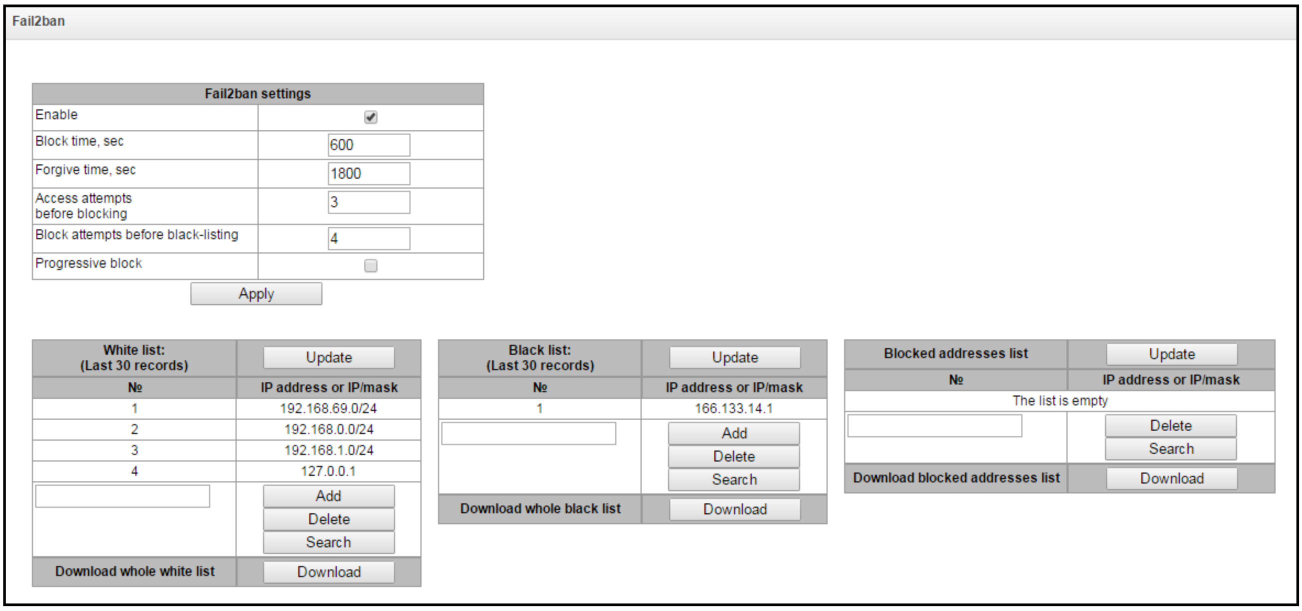
These parameters should be entered in Latin character.

- *2-Digit country code*—country code (for Russia—RU).
- *Region*—region name.
- *City*—city name.
- *Organization*—organization name.
- *Organization unit*—organization unit or division name.
- *Contact e-mail*—e-mail address.
- *Device name (or IP address)*—gateway IP address.

3.1.13.2 Fail2ban

Fail2ban—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:
- Bruteforcing web configurator or SSH authentication data, i.e. attempt to log in to the management interface using wrong login or password.
- Bruteforcing 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.



Fail2ban parameters:
- *Enable*—launch Fail2ban utility.
- *Ban time, seconds*—time in seconds during which access from the suspicious address will be banned.
- *Remission 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 count*—maximum quantity of unsuccessful access attempts for a host prior to be banned by fail2ban.
- *Temporary bans count*—quantity of bans after which the suspicious address will be blacklisted.

- *Progressive ban*—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 fail2ban will be unable to ban.

Black list (last 30 records)—list of permanently banned addresses and subnets. A device may have up to 131072records on SMG-1016M and 1048576 records on SMG-2016.

To add/search/remove an address from the list, select it in the entry field and click *'Add'/'Search'/'Remove'* 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.

Banned address list—list of addresses banned by fail2ban.

- *Download whole banned IP address list*—allows you to download the whole list of banned addresses to your PC.

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

fail2ban log information is written into **pbx_sip_bun.log** file.

For the list of banning messages and reasons, see Table below.

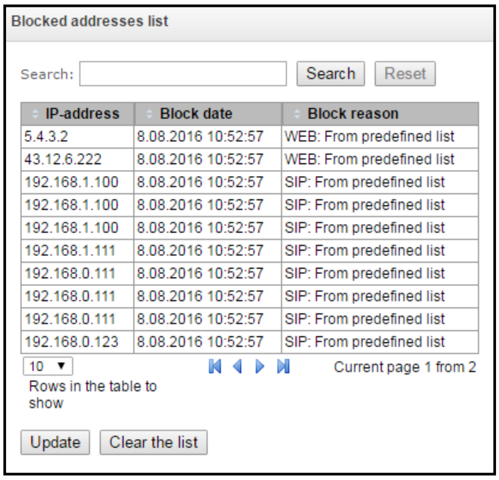
Table 24—Banning messages

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

Message in pbx_sip_bun.log	Reason	SIP message
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

3.1.13.3 Banned address log

This section contains a log of addresses banned by fail2ban that allows you to analyze which addresses have got banned and when, for all the time from the switch startup.



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

– *Search*—enter address to search for in the blocked address table.
– *IP address*—IP address that was banned.
– *Ban date*—date and time of IP address ban.
– *Refresh*—update banned address log.
– *Clear log*—delete all records from the banned address log.

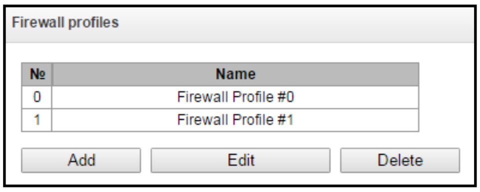
3.1.13.4 Firewall profiles

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

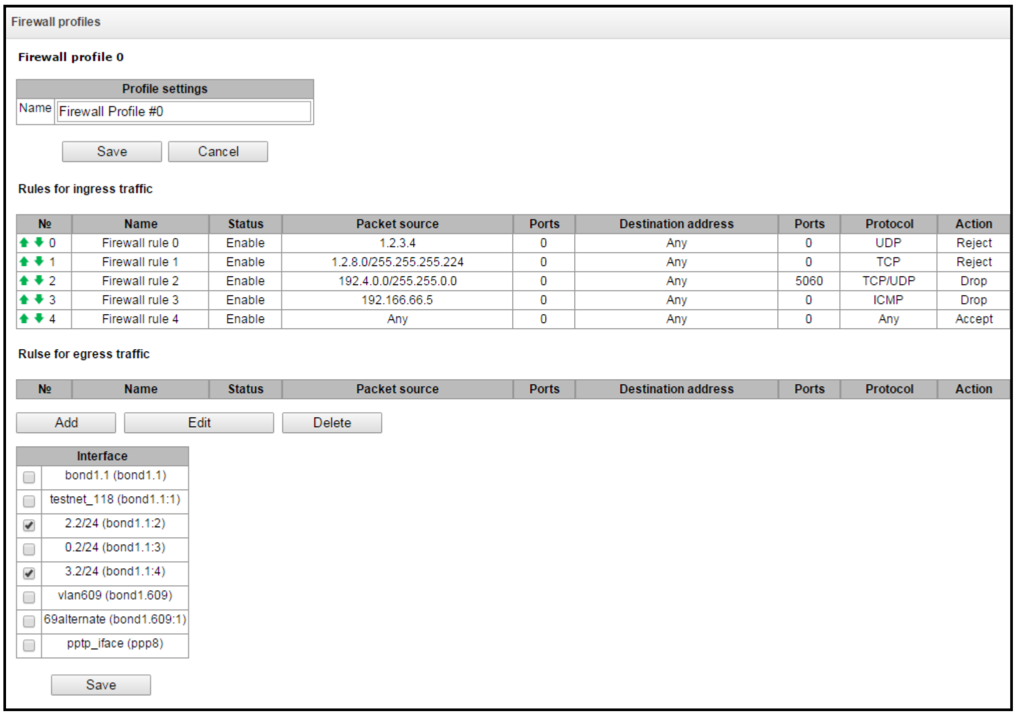
Firewall profiles

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

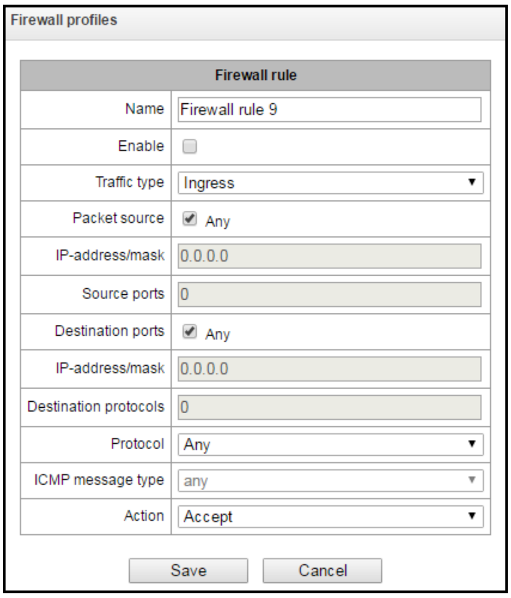
Add
Edit
Remove



Software allows you to configure firewall rules for incoming, outgoing and transit traffic as well as for specific network interfaces.



When a rule is created, you should configure the following parameters:



- *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:
  - *incoming*—intended for SMG.
  - *outgoing*—sent by SMG.
- *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: UDP, TCP, ICMP, or TCP/UDP.
- *Message type (ICMP)*—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'*.

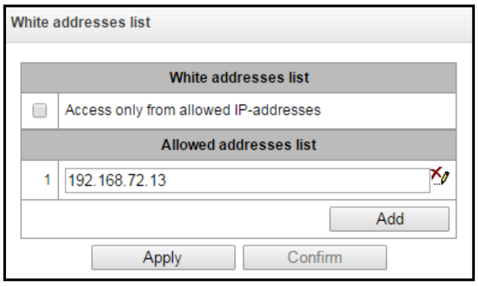
Also, in the firewall profile, you may specify network interfaces that these profile rules will be applied to.

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 List of allowed IP addresses

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.



- *Access for allowed IP addresses only*—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.
- *Save*—save access settings into the configuration file without applying them.

To create, edit or remove the list allowed addresses, use the following buttons:

—*'Add'*

—*'Edit'*

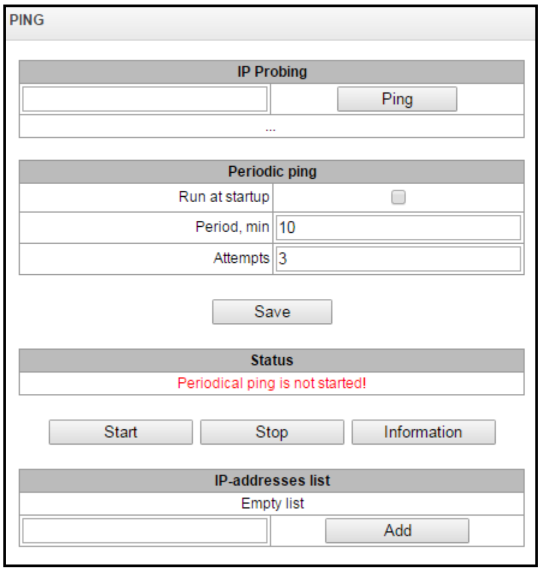
—*'Remove'*

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:

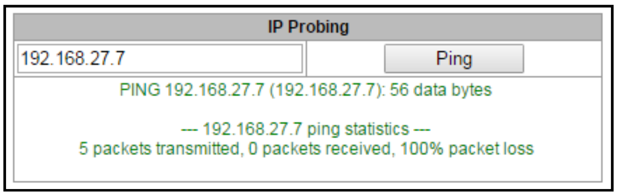
3.1.14.1 PING

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



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.



Periodic ping—used for periodic device network connection control.

– *Enable*—when checked, send ping requests to addresses specified in host list.
– *Period, minutes*—time interval between requests in minutes.
– *Attempts count*—number of attempts to send the request to an address.

State

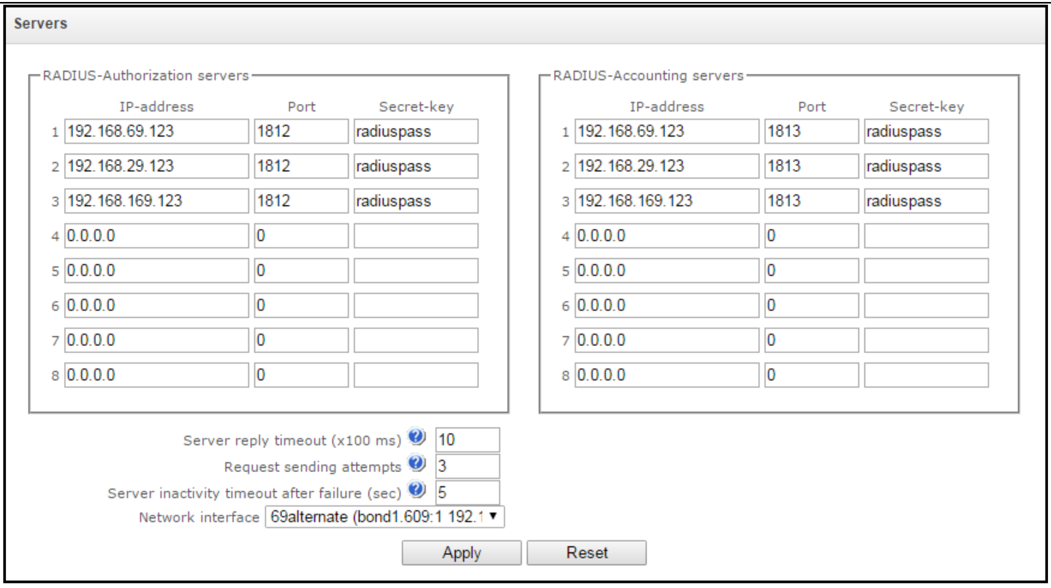
– *Restart*—launch/restart periodic ping.
– *Stop*—forcedly stop periodic ping.
– *Information*—click this button to view the log file '/tmp/log/hosttest.log'that contains data on the last periodic ping request transmission attempt.

Host 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.

3.1.15 RADIUS configuration

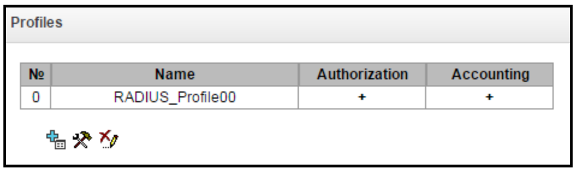
3.1.15.1 RADIUS servers



Device supports up to 8 authorization servers and up to 8 accounting servers.

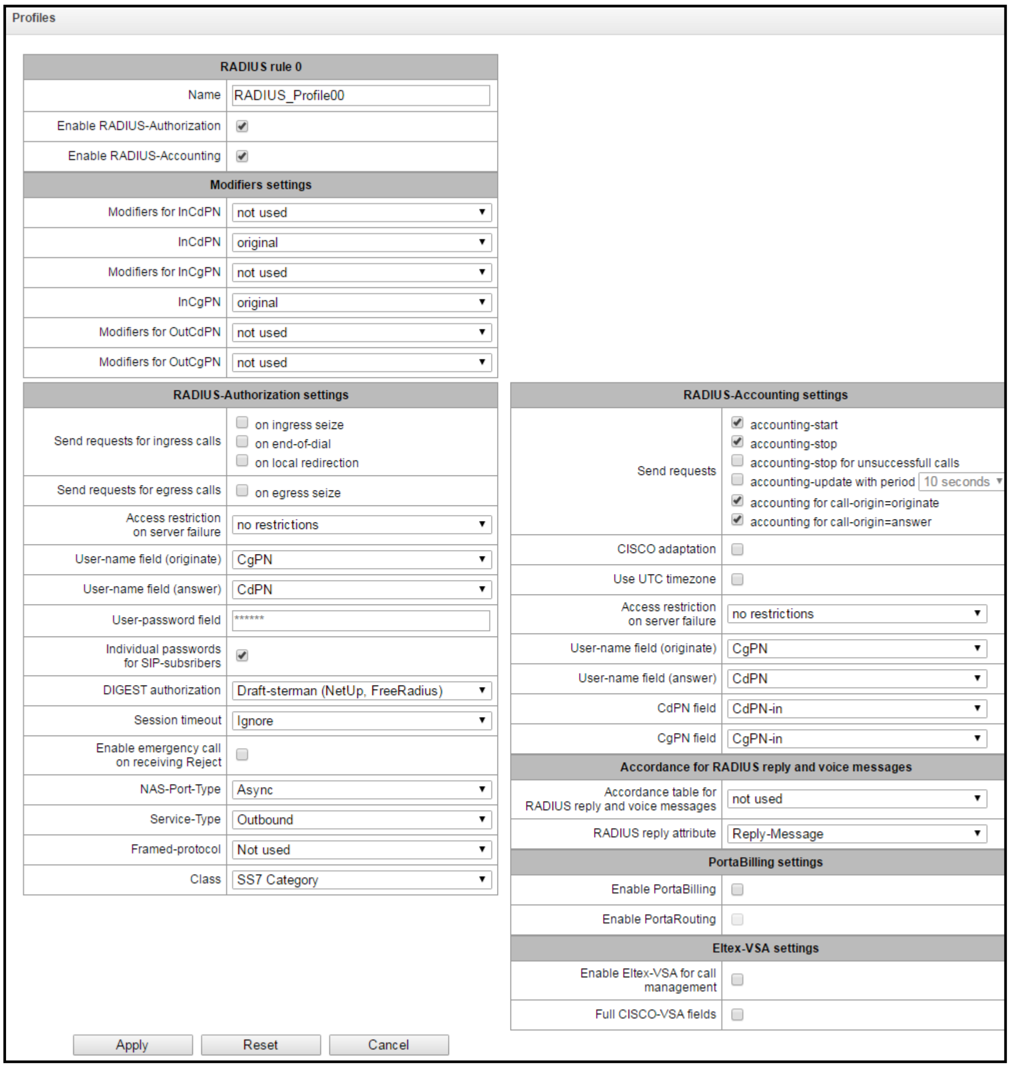
– *Server response timeout*—amount of time intended for server response.
– *Number of request transmission attempts*—quantity of request retries addressed to a server. When all attempts are used up, the server will be deemed inactive and the request will be forwarded to another server, if it is specified, otherwise the error will be detected.
– *Server unavailability time during failure*—amount of time that the server is deemed unavailable (requests will not be sent to it).
– *Network interface*—select network interface for the RADIUS protocol operation.

3.1.15.2 Profile list



Profile parameters:

– *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.



Modification parameters:

– *InCdPN modifiers*—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 number*—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.

– *InCgPN modifiers*—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 number*—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.

– *OutCdPN modifiers*—select callee (CdPN) number modifier for the outgoing connection in relation to *xpgk-src-number-out* field of RADIUS-Authorization and RADIUS-Accounting messages.

– *OutCgPN modifiers*—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 parameters:

Authentication/authorization requests may be transmitted during various call phases:
– During incoming engagement
– During the end of dial (full number dial reception)
– During local redirection

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 special services, local and zone network.
– *local network only*—allow calls to special services and local network.
– *special services only*—allow calls to special services only.
– *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 Access Request authorization packet (RADIUS-Authorization):
  – *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.
– *USER-PASSWORD field*—specify *User-Password* attribute value in the corresponding RADIUS-Authorization packet:

– *Custom 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) (operation upon draft that RFC4590 recommendation is based on).*

– *Session time*—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.

- *Allow access to special services after reception of connection refuse from server*—allow calls to special 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 SS-7 category.

RADIUS-Accounting parameters:

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.

- *Send time in UTC format*—send time in 'RADIUS-**Accounting'** messages in UTC format.

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 special services, local and zone network.
- *local network only*—allow calls to special services and local network.
- *special services only*—allow calls to special services only.
- *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.
- *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 packet).
  - *CdPN-out*—use callee number after the modification.

Correspondence between RADIUS responses 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.

RADIUS responses to voice messages correspondence table—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.

PortaBilling parameters

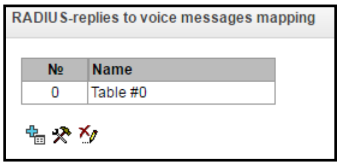
Enable PortaBilling—when checked, enable *PortaBilling*.
Enable PortaRouting—when checked, enable *PortaRouting*.

Eltex-VSA parameters

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.
Use complete CISCO-VSA value—complete attribute name transmission in CISCO-VSA fields.

3.1.15.3 RADIUS replaies to voice messages mapping

In this section, you may configure the correspondence between RADIUS-reject responses and voice messages output to the subscribers.

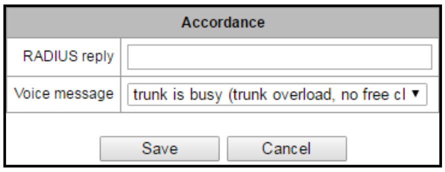


To create, edit or remove tables, use *'Objects' — 'Add object'*, *'Objects' — 'Edit object'* and *'Objects' — 'Remove object'* menus and the following buttons:

*—'Add table'*

*—'Edit table'*

*—'Removetable'*



– *RADIUS resply***—**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 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)
```

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): <$SESSION_ID>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-src-number-in=<$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>
```

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>
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>
```

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

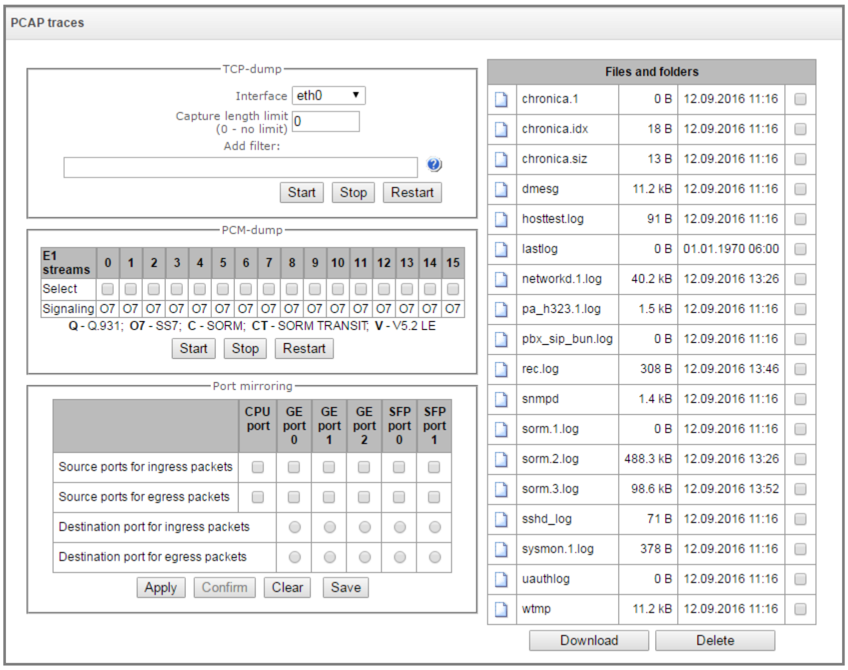
Variable	Description and possible values
$CALL_TYPE	defined on the basis of the transmission medium that the outgoing trunk belongs to: • 'Telephony', if the outgoing trunk is PSTN (TDM). • 'VoIP', if the outgoing trunk is VoIP.
$CdPN	determined from SMG settings • $CdPN = $CdPN_IN [by default] • $CdPN = $CdPN_OUT
$CdPN_IN	callee number before modification (received in SETUP/INVITE)
$CdPN_OUT	caller number after modification (sent to the called party in SETUP/INVITE)
$CgPN_IN	caller number before modification (received in SETUP/INVITE)
$CgPN_OUT	caller number after modification (sent to the called party in SETUP/INVITE)
$DISCONNECT_CAUSE	Q.850 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
$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 (Unsuccesfull-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.

3.1.16 Tracing

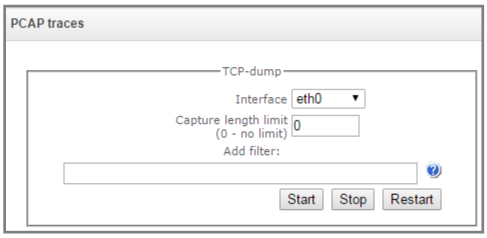
3.1.16.1 PCAP tracings

In this menu, you may configure parameters for network traffic analysis and TDM protocol.



TCP dump—TCP–dump utility settings:

TCP dump is a utility for network traffic interception and analysis.



– *Interface*—interface for the network traffic interception.
– *Packet length limit*—size limit for intercepted packets, bytes.
– *Add filter*—packet filter for tcpdump utility.

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

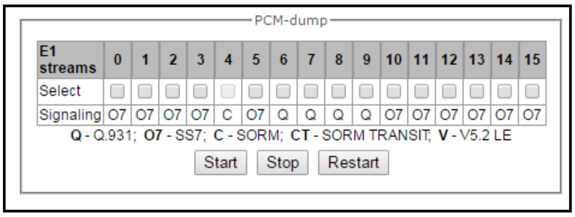
- *Launch*—begin data collection.
- *Finish*—finish data collection.
- *Restart*—restart utility, begin data collection again.

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'.

PCM–dump—PCM–dump utility settings.

PCMdump is a utility for E1 stream signalling 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 signalling messages from multiple streams; at that, simultaneous PCM-dumping for streams with different signalling protocols is not available.



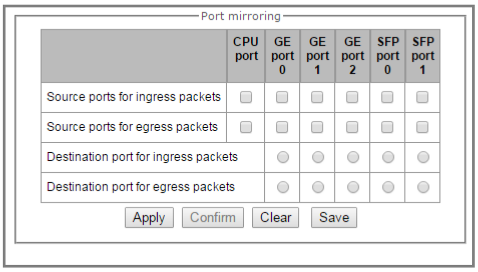
- *Select*—select E1 streams.
- *Signalling*—signalling protocol selected for the stream:
- O7 – SS-7
- Q – Q.931
- *Launch*—begin data collection.
- *Finish*—finish data collection.
- *Restart*—restart the utility and begin data collection again.

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'.

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.



For device ports, available operations are as follows:

- *Ports of incoming packet source*—copy frames received from this port (source port).
- *Ports of outgoing packet source*—copy frames sent by this port (source port).
- *Incoming packet destination port*—destination port for copied frames received by selected source ports.
- *Outgoing packet destination port*—destination port for copied frames sent by selected source ports.

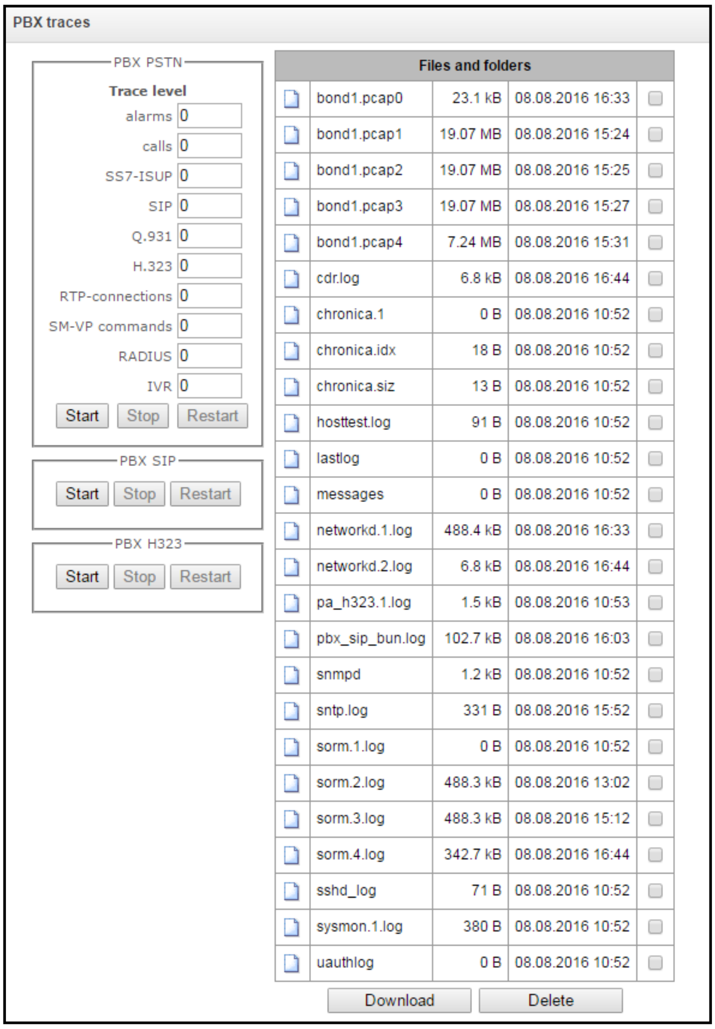
- *Apply*—apply mirroring setting parameters.
- *Confirm*—confirm applied mirroring setting parameters.
- *Clear*—reset mirroring settings.
- *Save*—save mirroring setting parameters.

Click 'Commit' button in 1 minute interval to confirm settings, or the previous values will be restored.

[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.



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.

– *Launch*—begin data collection.
– *Finish*—finish data collection.
– *Restart*—restart, begin data collection again.

In **PBX H323** block, H323 error and message tracing is collected.

– *Launch*—begin data collection.
– *Finish*—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 /tmp/log directory'** block features the list of files in the respective /tmp/log directory.

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'*.

3.1.16.3 Syslog settings

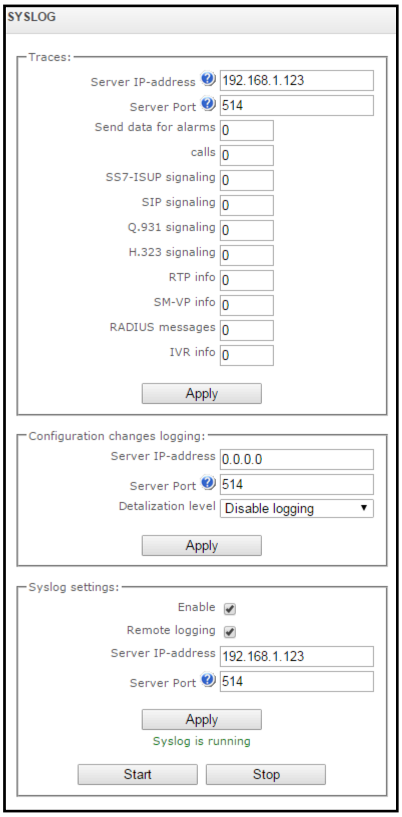
In *'SYSLOG'* menu, you may configure system log settings.

SYSLOGis a protocol, designed for transmission of messages on current system events. Gateway software generates system data logs on operation of system applications and signalling 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 a Eltex Service Centre Specialist.

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.

Output the history of entered commands—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.
- *Verbosity level*—verbosity level of the entered commands log:
  - *Disable logs*—disable entered commands logs generation.
  - *Standard*—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.

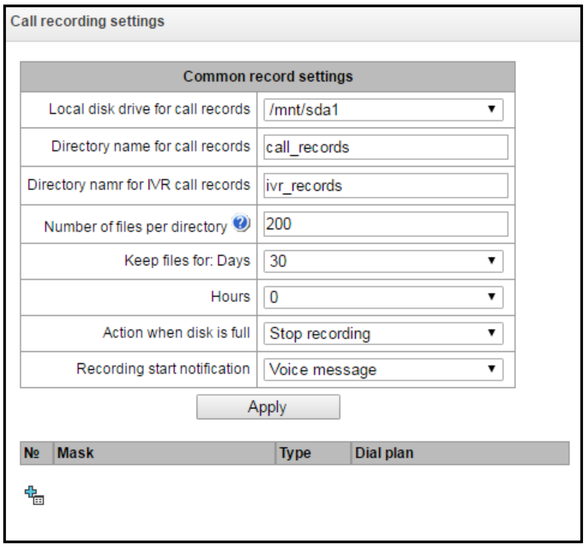
System log configuration—system log configuration settings for transmission of the device access events.

- *Enable logging*—when checked, device access event history will be saved; when unchecked, logging will be disabled.
- *Send to server*—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 Conversation recording

Use this menu to set conversation recording[1].

3.1.17.1 Recording parameters



General recording parameters:

– *Local disk drive for callrecords*—select available storage device for saving conversation records.
– *Directory namefor callrecords*—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 callrecords*—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

– *Data storage time (days/hours)—time period during which conversation records will be kept on the storage device; when it expires, obsolete files will be removed.*
– *Action for full disk—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.*

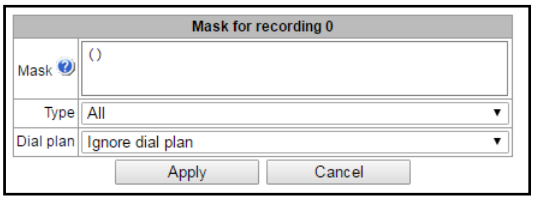
[1]This menu is available in the firmware version with Call-record license only, for license details, see Section 3.1.22 **Licenses**.

– *Notify on record start — notify the callee on conversation recording start:*
  – *Do not notify — disable notification on conversation recording start.*
  – *Voice message — play voice notification on conversation recording start.*

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.

  – *Calling*—search for CgPN number matches only.
  – *Called*—search for CdPN number matches only.

3.1.17.2 Conversation recordings

This section enables management of conversation recording files.

– *Total record count*—total quantity of conversation recording files in the selected directory for conversation recordings.
– *Disk utilization*—display used space on disk selected for conversation recording.
– *Select 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

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.

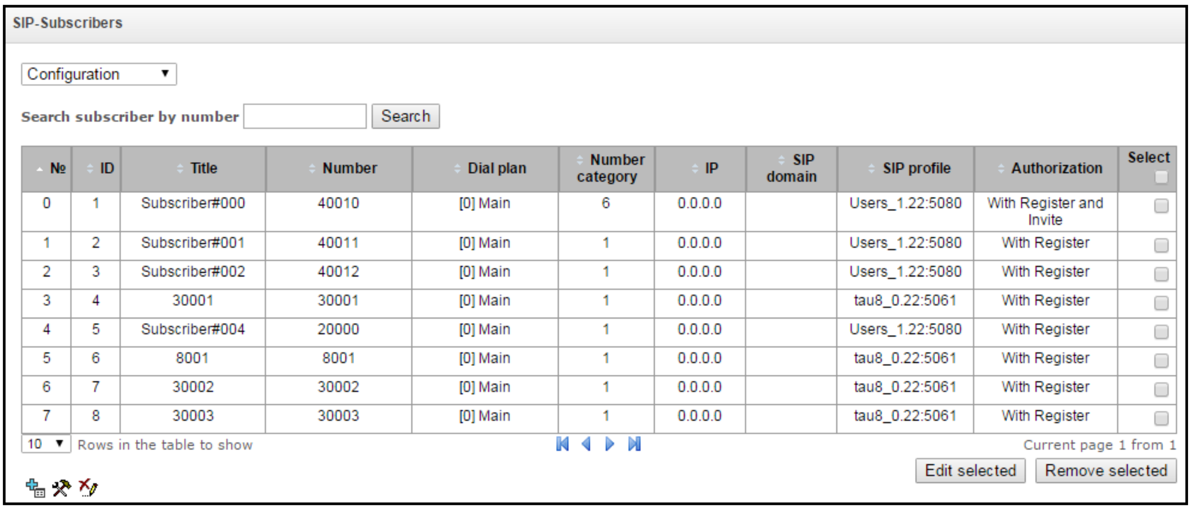
3.1.18 Subscribers

In this menu, you may configure SIP subscribers[1].

[1]This menu is available in the firmware version with SIP registrar license only, for license details, see Section **3.1.23. Licenses**

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 for 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.

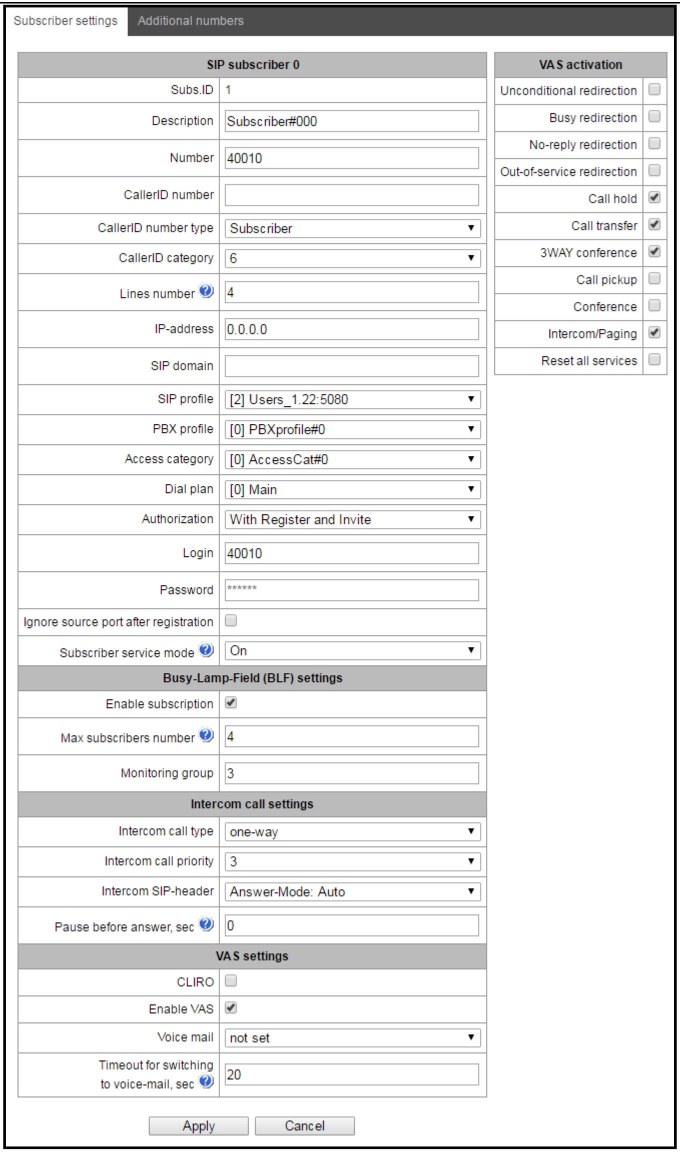
To create, edit or remove a record of a single subscriber, use *'Objects'* — *'Add object', 'Objects'* — *'Edit object'* and *'Objects'* — *'Remove object'* menus and the following buttons:

— *'Add subscriber'*

— *'Edit subscriber parameters'*

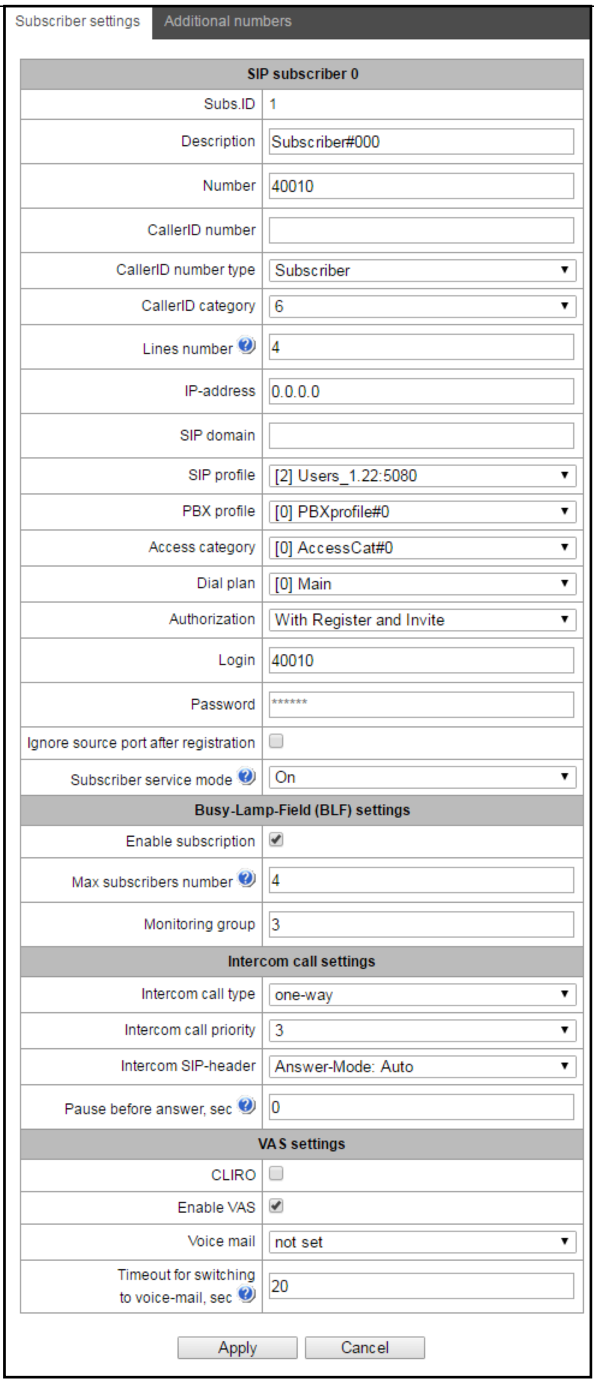
— *'Removesubscriber'*

3.1.18.1.1.1. Subscriber settings



- *Subscriber ID* —quantity of subscribers being created.
- *Name*—arbitrary subscriber text description.
- *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.
- *Caller ID number type*—subscriber number type:
- *Caller ID category*—subscriber's Caller ID category.
- *Line quantity*—quantity of calls that the subscriber may take part in simultaneously. Permitted value range is [1;255] or 0—unlimited.
- *IP address*—subscriber IP address. When value 0.0.0.0 is defined, subscriber is allowed to register using any IP address.
- *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 **3.1.6.4Timer operation example**).
- *SIP profile*—select SIP profile. SIP profile defines the majority of subscriber's settings (see Section **3.1.7.3SIP/SIP-T/SIP-I interfaces, SIP profiles**).
- *PBX profile*—select PBX profile (see Section **3.1.8.3PBX profiles**).
- *Access category*—select access category.

- *Numbering schedule*—defines the numbering schedule that the subscriber will belong to.
- *Authorization*—defines authentication mode for the device*:*
  - *None*—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 may come from any port.
- *Subscriber service mode*—defines restrictions on the incoming and outgoing communication for the subscriber:
  - *disabled:* out of service.
  - *enabled:* all communication types available.
  - *disabled 1:* incoming communication is enabled, outgoing communication to the special service only.
  - *disabled 2:* incoming communication is disabled, outgoing communication to the special service only.
  - *barring 1:* full barring for incoming and outgoing calls.
  - *barring 2:* full barring for incoming and outgoing calls except for the special services.
  - *barring 3:* incoming calls are barred, outgoing calls are allowed.
  - *barring 4:* incoming calls are barred, outgoing calls are allowed only for local and private communication.
  - *barring 5:* incoming calls are allowed, full barring for outgoing calls.
  - *barring 6:* incoming calls are allowed, outgoing calls are allowed to special services only.
  - *barring 7:* incoming calls are allowed, outgoing calls are allowed only for local and private communication.
  - *barring 8:* incoming calls are allowed, outgoing calls are allowed only for local, private and zone communication.
  - *excluded:* excluded from the numbering.



Configuring busy lamp field (BLF)

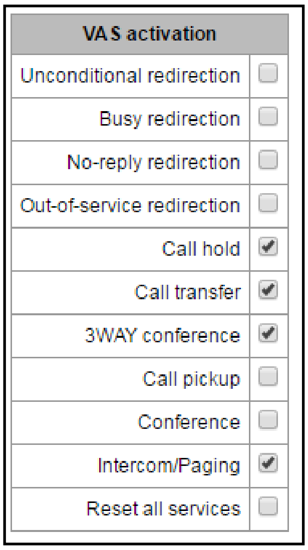
- *Permitevent subscription* – allowsclienttosubscribes itself for BLF events of another clients;
- *Numberofsubscribers* – quantity of observable numbers when BLF service is enabled;
- *Monitoringgroup* –BLF monitoring group, clients incoming in the same monitoring group can realize monitoring between each other.

Directions (*local network, special service, zone network, private network, long-distance network, international network*) are specified during prefix configuration in

the numbering schedule, *'Direction'* field.

- *Intercom call*—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.
  - *Common call*—incoming intercom call will be performed as a common call without the Subscriber B automatic reply.
  - *Reject*—incoming intercom call will be rejected.
- *Intercom call priority*—incoming intercom call priority for other calls.
- *Voice mail*
- *No answer timeout for voicemail (seconds).*
- *Enable VAS*[1]—allow the subscriber to use VAS.

VAS activation



- *Call forward unconditional*—activate call forward unconditional (CF Unconditional) service.
- *Call forward on busy*—activate call forward on busy (CF Busy) service.
- *Call forward on no reply*—activate call forward on no reply (CF No reply) service.
- *Call forward on out of service*—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.
- *3-way conference*—activate 3-way conference (3WAY) service.
- *Call pickup*—activate call pickup (Call Pickup) service.
- *Conference with consequent assembly*—activate conference with consequent assembly service.
- *Intercom call*—activate access to outgoing intercom or paging call service (with the Subscriber B automatic reply).
- *Cancel all services*—feature required for cancellation of all numbers configured for redirection by dialling a service prefix configured in the numbering schedule.

- *Voice mail;*
- *Noanswertimeoutforswitchingtovoicemail (sec)* –time interval (in seconds) from start of call, after that call will be switched to voice mail. Therangeofavailablevaluesis [5;255].

For *'Conference by list'* service operation, you should create a call group (see Section 3.1.8.9Hunt 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#'.

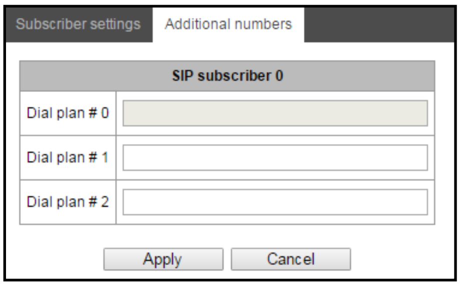
3.1.18.1.1.2. Additional numbers

A subscriber may have different numbers in different numbering schedules; at that, when a call comes trough the numbering schedule change prefix, subscriber CgPN number is automatically substituted to their number in the corresponding numbering schedule, e.g.:

[1]This menu is available in the firmware version with SMG-VAS license only, for license details, see Section **3.1.22 Licenses**.

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 numbering schedules 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 'Numbering Schedule #1' field of the 'Additional numbers' setting. In the numbering schedule #1, an external network exit prefix should be created; in the numbering schedule #0, prefix '(9x.)' should be created with the 'numbering schedule change' type that should perform a transfer to the numbering schedule #1. When the subscriber dials a complete number that begins with 9, the call will transfer through the 'Numbering schedule change' prefix; when it arrives to numbering schedule #1, their CgPN number will be automatically substituted to their external number.



Numbering schedule #0-16—additional subscriber number in the corresponding numbering schedule.

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 **3.1.18.1.1Subscriber configuration**.

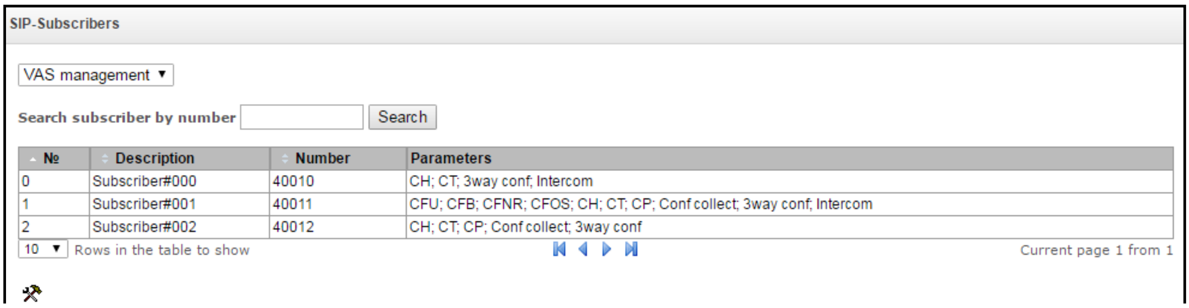
Subscribers may manage state of services from their phone units. The following functions are available:

– 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**).



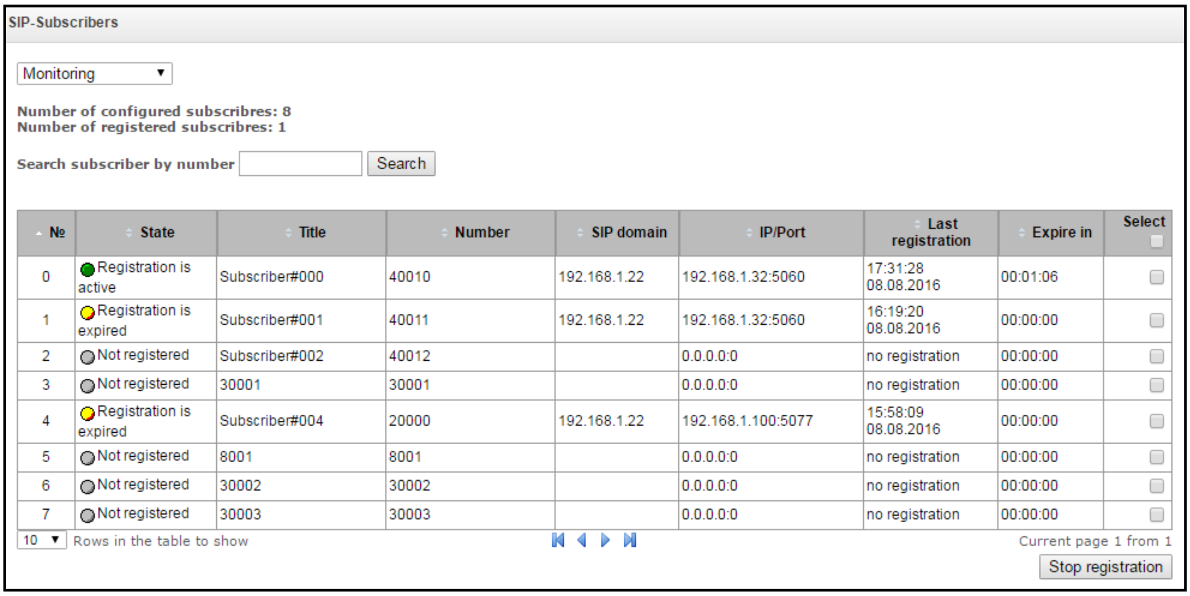
№	Description	Number	Parameters
0	Subscriber#000	40010	CH; CT; 3way conf; Intercom
1	Subscriber#001	40011	CFU; CFB; CFNR; CFOS; CH; CT; CP; Conf collect; 3way conf; Intercom
2	Subscriber#002	40012	CH; CT; CP; Conf collect; 3way conf

– *Number for call forward unconditional*—phone number for 'Call forward unconditional' service.
– *Number for call forward on busy*—phone number for 'Call forward on busy' service.
– *Number for call forward on no reply*—phone number for 'Call forward on no reply' service.
– *Number for call forward on out of service*—phone number for 'Call forward on out of service' service.

For VAS service detailed operation and configuration description, see Appendix J. Working with VAS services

3.1.18.1.3 Subscriber monitoring

When you choose *'Monitoring'* item from the drop down list, a subscriber status table will be shown.



№	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	

– *Status*—subscriber registration status (registered, not registered, registration expired).
– *Name*—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.
– *Registration expires*—remaining time until the registration expiration.

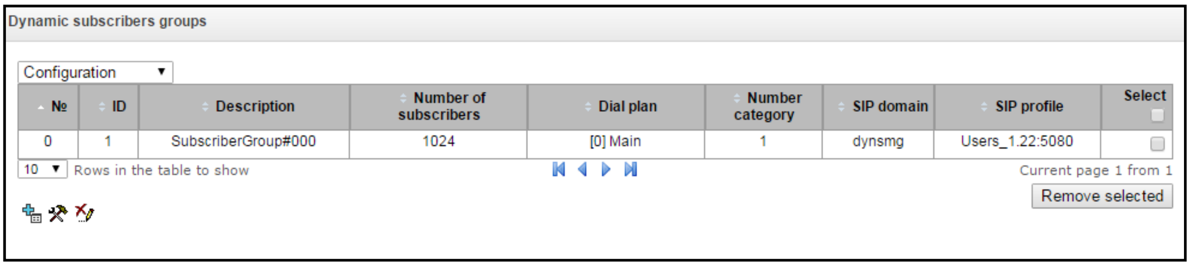
Click *'Reset registration'* button to forcedly reset the registration for selected subscribers.

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 (rfc 4590, rfc4590-no-challenge, draft-sterman).

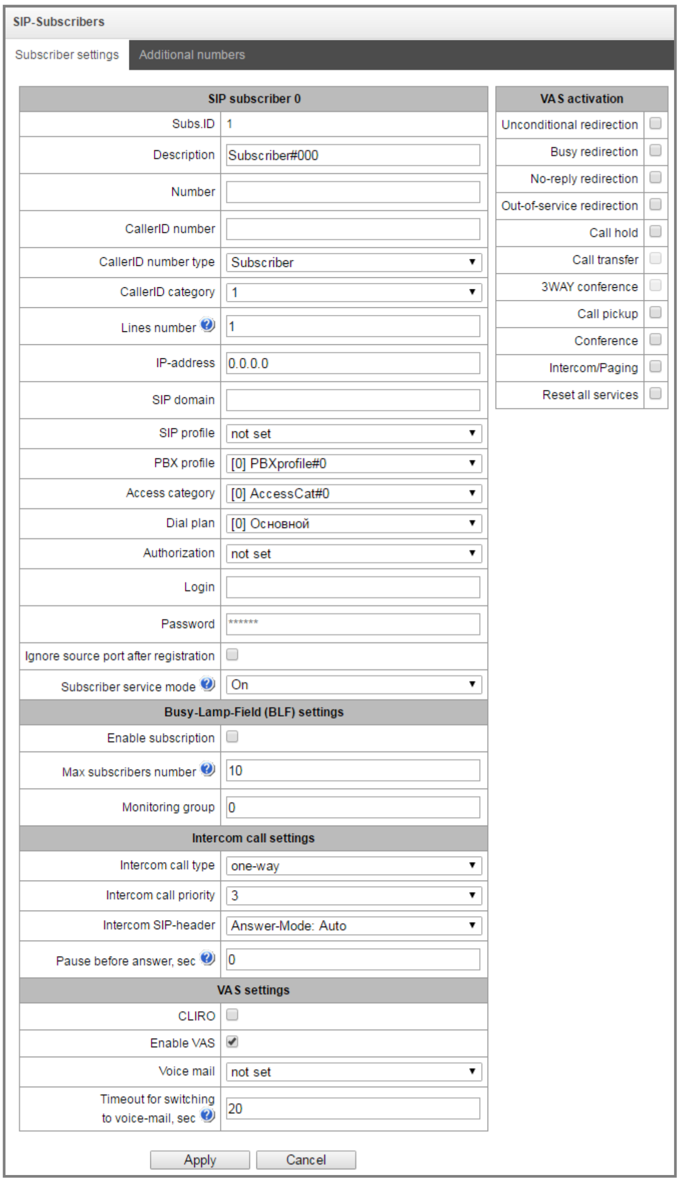


To create, edit or remove a record, use *'Objects'* — *'Add object'*, *'Objects'* — *'Edit object'* and *'Objects'* — *'Remove object'* menus and the following buttons:

— *'Add subscriber'*

— *'Edit subscriber parameters'*

— *'Removesubscriber'*



- ***Group of dynamic subscribers:***
  - *Subscriber quantity*—quantity of subscribers in a group.
  - *Name*—name of the group of dynamic objects.
  - *Caller ID number type*—subscriber number type:
  - *Caller ID category*—subscriber's Caller ID category.

- *Line quantity*—quantity of calls that the subscriber may take part in simultaneously. 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.
- *Numbering schedule*—defines the numbering schedule 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:
  - **disabled:** out of service.
  - **enabled:** all communication types available.
  - **disabled 1:** incoming communication is enabled, outgoing communication to the special service only.
  - **disabled 2:** incoming communication is disabled, outgoing communication to the special service only.
  - **barring 1:** full barring for incoming and outgoing calls.
  - **barring 2:** full barring for incoming and outgoing calls except for the special services.
  - **barring 3:** incoming calls are barred, outgoing calls are allowed.
  - **barring 4:** incoming calls are barred, outgoing calls are allowed only for local and private communication.
  - **barring 5:** incoming calls are allowed, full barring for outgoing calls.
  - **barring 6:** incoming calls are allowed, outgoing calls are allowed to special services only.
  - **barring 7:** incoming calls are allowed, outgoing calls are allowed only for local and private communication.
  - **barring 8:** incoming calls are allowed, outgoing calls are allowed only for local, private and zone communication.
  - **excluded:** excluded from the numbering.

Directions (*local network, special service, zone network, private network, long-distance network, international network*) are specified during prefix configuration in the numbering schedule, *'Direction'* field.

- ***Configuration of busy line functions (BLF):***
  - *Permit event subscription* –BLF (Busy Lamp Field) functionallows 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 performBFL monitoring between each other.

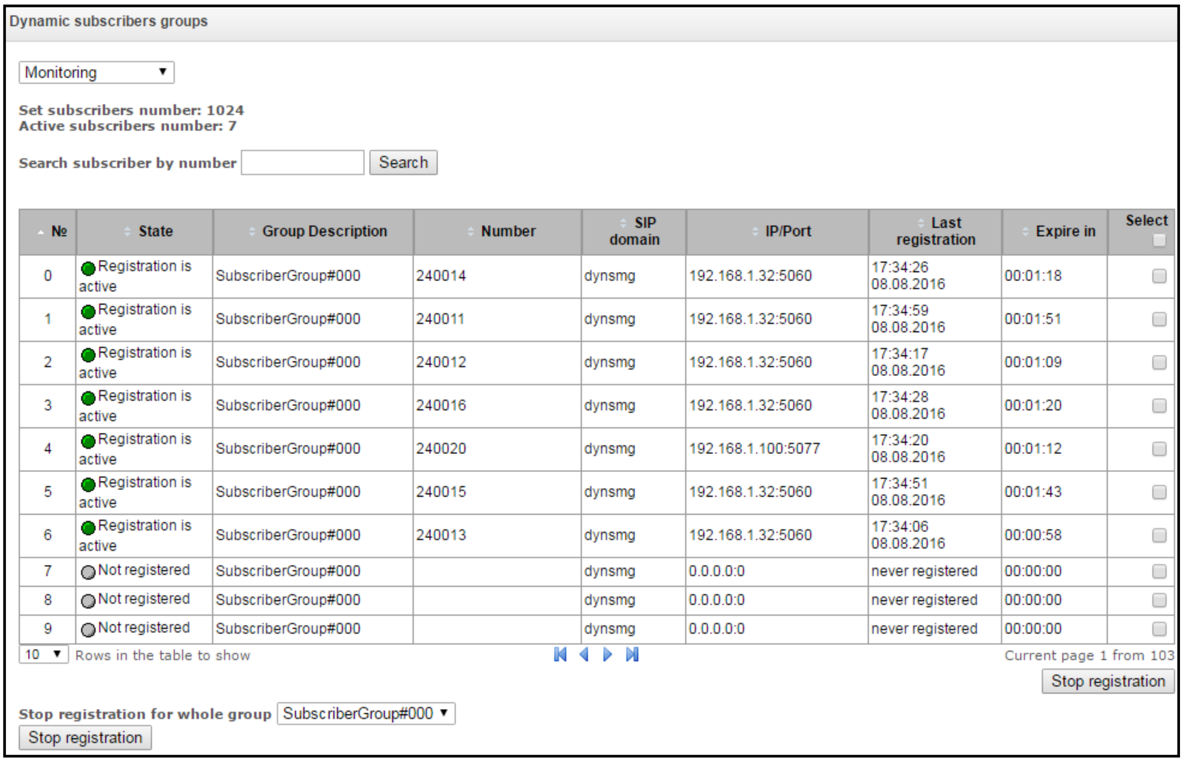
- ***Intercom configuration:***
  - *Type of intercom call* — type of incoming intercom call(autoansmer call of B subscriber):
    - *One way call* — in case ofincomingintercomcall, B subscriber will hear subscriber A but subscriber A will not hear subscriber B (oneway notification);
    - *Two-way call* — 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 hearder*—select SIP hearder, 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;

– Pausebeforeanswer (sec) — transmission of pause time in 'answer-auto' hearders before taking a intercom/paging call.

– ***VAS configuration:***
  – CLIRO –service foroverriding 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.
    – *Voice mail;*
    – *Noanswer timeout for switching to voice mail (sec)* – time interval (in seconds) from start of call, after that call will be switched to voice mail. The range of available values is [5;255].

3.1.18.2.2 Dynamic subscriber group monitoring



№	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	

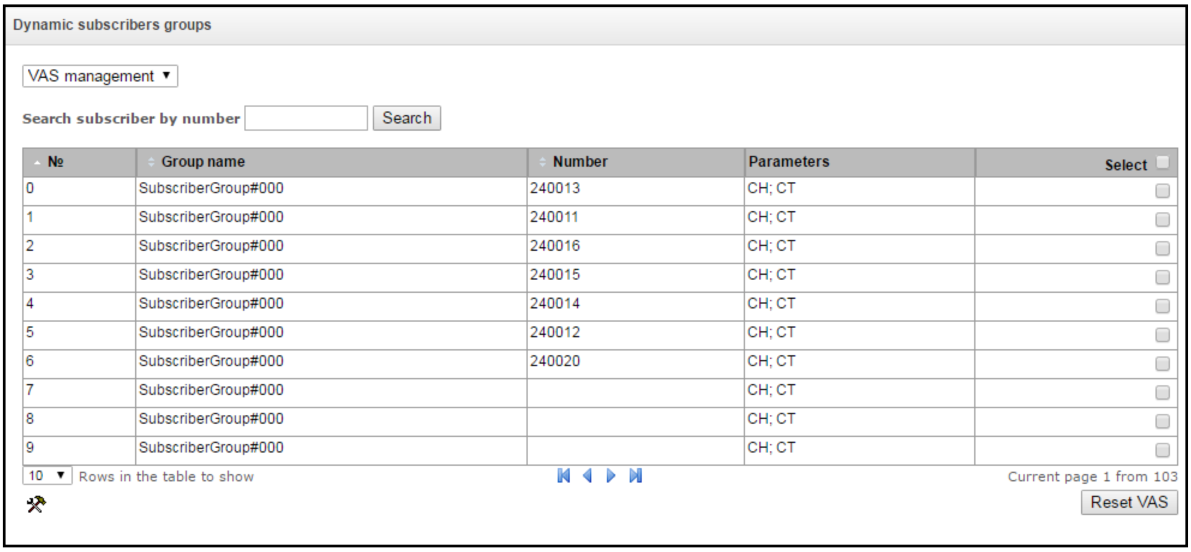
Click *'Search'* button to search the records for the subscriber with the specified number.

– *Status*—subscriber registration status (registered, not registered, registration expired).

- *Group name*—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.
- *Select*—when checked, the current record will be processed when you click *'Reset registration'* button.
- *Reset 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

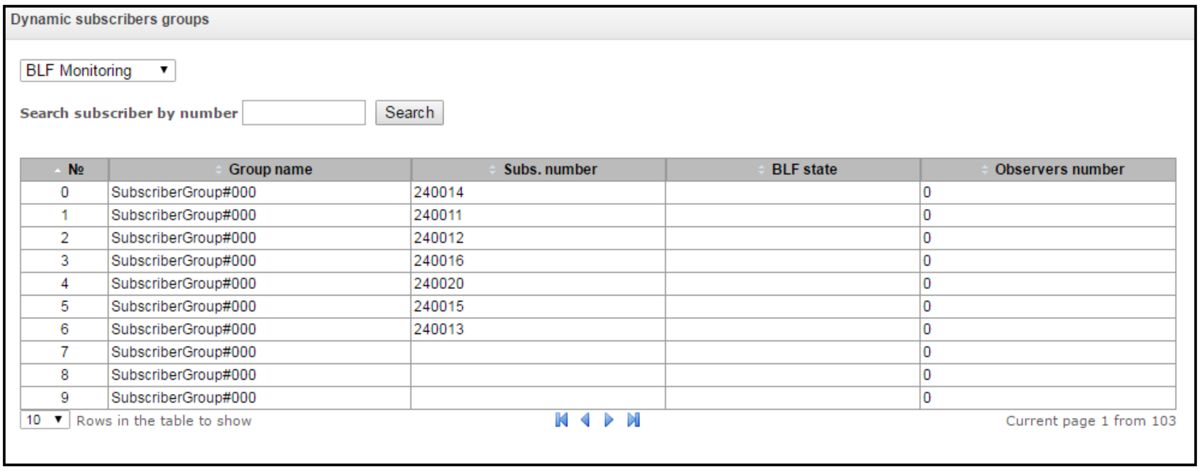


Click *'Search'* button to search the records for the subscriber with the specified number.

– *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

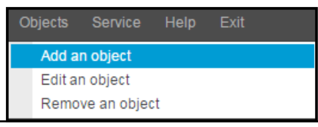


Click *'Search'* button to search the records for the subscriber with the specified number.

– *Group name*—arbitrary group text description.
– *Subscriber number*
– *BLF status*—current state of the *'busy lamp field'* service.
– *Viewer quantity*—the current number of subscribers that monitor the subscriber line status.

3.1.19 Working with objects and 'Objects' menu

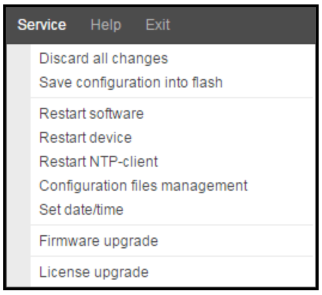
In addition to create, edit and remove icons, you may use the corresponding 'Objects' menu items to perform different operations with objects.



3.1.20 Saving configuration and 'Service' menu

To discard all changes, select *'Service'—'Discard all changes'* menu.

To write the current configuration into non-volatile memory of the 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 perform forced SSHD client restart, select *'Service'—'SSHD restart'* menu.

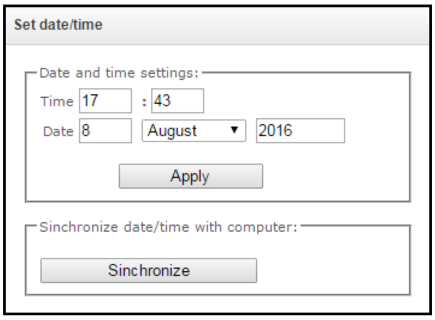
To read/write the main device configuration file, select *'Service'—'Configuration file management'* menu.

To configure the device local date and time manually, select *'Service'—'Date and time configuration'* menu; see Section **3.1.21.**

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

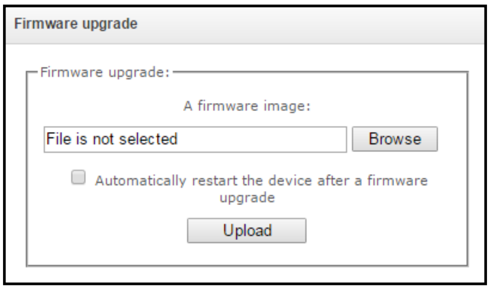


In the respective fields, you may define the system time in HH:MM format and the date in DD.month.YYYY format.

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



To update the device firmware, use *'Service'—'Firmware update'* menu.

Firmware file upload form will open.

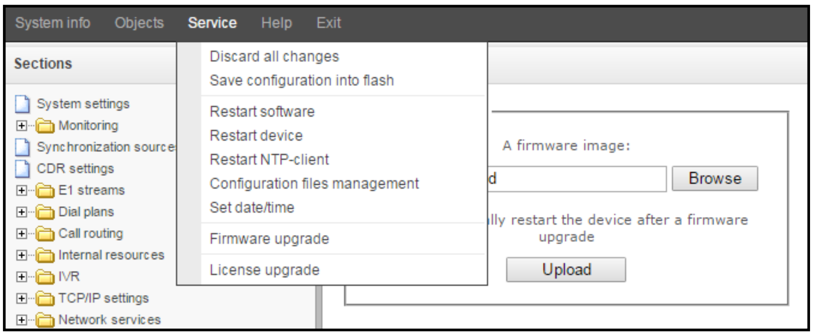
– *Update firmware*—update firmware and/or Linux kernel.

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

To update/add licenses, you should obtain a license file. Contact Eltex marketing department by email eltex@eltex.nsk.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.



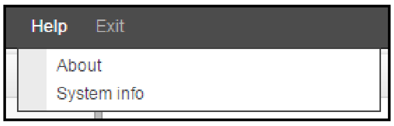
Specify path to the license file obtained from the manufacturer using *'Select file'* button, and update it by clicking *'Update'*.

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.



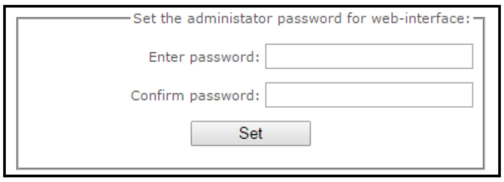
3.1.25 Setting password for web configurator access

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.

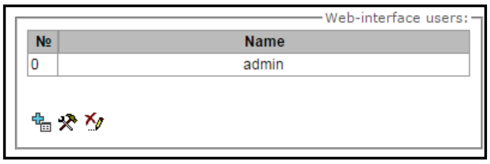
To create, edit or remove users, use the following buttons:

—*'Add user'*

—*'Edit user parameters'*

—*'Removeuser'*

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.

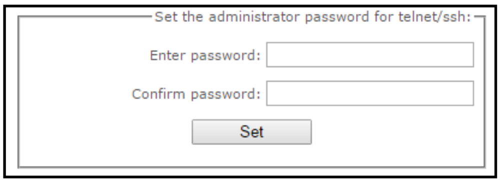


- *[username]*—username for web configurator log in.
- *[group]*—user group type. This parameter should have 'webs' parameter.
- *[enter password]*—password for web configurator access.
- *[confirm password]*—confirm password for web configurator access.

To save the configuration, use *'Service'—'Save configuration'* menu.

Setting administrator password for Telnet and SSH

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; in the browser, the following screen will be shown next:

To resume the access, you should specify the defined username and password and click *'Sign In'* button. To exit the configuration program, click *'Cancel'* button.

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

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 line group, <linkset> is SS-7 line group number
checknum	Check the number with the numbering schedule
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 debug level **WARNING!This command may cause the switch 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	SS-7 protocol ISUP subsystem operation tracing	Not used

mtp3	SS-7 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	Switch 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	Numbering schedule (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/ SMG-SORM/ 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 licence
license reset	no/yes		Delete all installed licenses
management			Enter SS-7 stream management mode
mirroring			Enter mirroring management mode
number check	<NUMPLAN> <NUMBER> <COMPLETE>	0-15 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 numbering schedule: *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 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 (SS-7) signalling 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> SS-7 line group 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 signalling 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 signalling traffic volume is shown for 12-hour 00-minute interval.

3.3.3.2.4 *View MTP signalling 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 signalling 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 SS-7 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 SS-7 stream parameter management
quit			Terminate this CLI session

3.3.4.1 SS-7 stream management mode

To enter this mode, execute 'ss7link <Link>' command in the SS-7 stream configuration mode, where <Link> is SS-7 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> <CHAN_COUNT>	1-31 2-31	Unblock a group of channels 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

Toenterthismode[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 port*—destination port for copied frames sent by selected source ports.
show			Configure port mirroring:

[1]For SMG-1016M only

3.3.6 General device parameter configuration mode

To proceed to device parameter configurations/monitoring, execute 'config' command.

Foreachconfigurationmode ‘do’ and ‘top’ commandsareavailable. The ‘do’ command allows you to execute command of CLI menu from any configuration submenu. The ‘top’ commandallowsgoingtoCLImenu.

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 the device (into start configuration)
copy startup_to_running			Restore the current configuration from the start configuration
count linkset			Show the number of SS-7 line groups
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 SS-7 timer profiles
delete linkset	<OBJECT_INDEX>	existing number of the line group	Delete SS-7 line group
delete trunk	<OBJECT_INDEX>	Existing trunk group number	Delete trunk group
delete trunk_direction	<OBJECT_INDEX>	Existing trunk direction number	Delete trunk direction
delete sipt-interface	<OBJECT_INDEX>	Existing SIP interface number	Delete SIP interface
delete radius-profile	<OBJECT_INDEX>	Existing RADIUS profile number	Delete RADIUS profile
delete modifiers-table	<OBJECT_INDEX>	Existing modifier table number	Delete 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 SS-7 timer profile number	Delete SS-7 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.
fail2ban			Enter Fail2ban configuration mode
firewall			Enter Fail2ban 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> <set> <show>	 local /mnt/sd[abc][1-7]*	Apply path settings for tracing storage Configure path for tracing storage: local—local storage in RAM /mnt/sd[abc][1-7]*—path to storage device for tracing storage View path settings for tracing storage
linkset	<LINKSET_INDEX>	0-15	Enter the SS-7 line group 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 SS-7 line group
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 SS-7 timer profile
new hunt-group			Create call group
new pickup-group			Create pickup group
numplan			Enter the numbering schedule 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 SS-7 category configuration mode
ss7timers	<SS7_TIMERS_INDEX>	0-15	Enter SS-7 timer configuration mode
submodule-usage			Enter theconfigurationmodeofSM-VPsubmodule 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	Rounding up or down
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>			Addspecifiedfieldintheendoffield 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 fieldoncorrespondingpositionwith specified field (see section3.3.8CDR 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 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>	/mnt/sd[abc][1-	Path to CDR data storage on local drives

[1]Not supported in the current firmware version.

	<show>	7]*	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
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	SIPCall-IDof incoming call
incoming SS7 category	SS7 categoryon 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 cannal
outgoing E1 stream	Number of outgoing E1 flow
outgoing ipaddr	IP address of callee
outgoing SIP call id	SIPCall-IDof outgoing call
outgoing SS7 category	SS7 categoryonoutput (after modification)
outgoing SS7 CIC	CIC number of outgoing call
outgoing type	Callee type
redirecting in	Numberof forwarding party on input (before modification)
redirecting out	Numberof 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 SORM	Set the signalling type for the stream Possible signalling types: Q931_USR, Q931_NET, SS7, SORM
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.
sorm			Enter the configuration mode for SORM for the current E1 stream.
ss7			Enter the configuration mode for SS-7 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 numbering schedule type **To use common numbering schedule 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 SORM parameters configuration mode for the current E1 stream

This mode is available for SORM signalling only (set by *'signaling'* command). To enter this mode, execute 'sorm' command in the E1 stream configuration mode.

SMG-[CONFIG]-E1[0]> sorm
E1[0]. Signaling is SORM
SMG-[CONFIG]-E1[0]-[SORM]>

Command	Parameter	Value	Action
?			Show the list of available commands.
activity	<ON_OFF>	on/off	Enable/disable activity monitoring of L1 level message exchange process
chan1(2) mode	<SORM_MODE>	DCE/DTE	Set mode for chan1 (2). Permitted modes: DCE, DTE
chan1(2) send L3 Reset	<ON_OFF>	on/off	Allow/deny channel1(2) to send the L3 restart command
chan1(2) send L3 Restart	<ON_OFF>	on/off	Allow/deny channel 1 to send the L3 settings reset command
chan1(2) send SABME	<ON_OFF>	on/off	Enable/disable Asynchronous Balanced Mode Extended (SABME) for channel 1(2)
cmd	<CMD_ADDR>	1/3	Set the command frame address
config			Return to Configuration menu.
exit			Return from this configuration submenu to the upper level.
history			View history of entered commands
mode		Tcp/x25	Selectoperationmodeofcontrol connection lines
protocol specification	<SPECIFICATION>	order_70/ KZ_specification/ order_268	SORM specification selection
quit			Terminate this CLI session
resp	<RESP_ADDR>	1/ 3	Set the response frame address
show			Show SORM configuration
tcp interface	<IFACE_NAME>		Select network interface to organize TCP connection
tcp port1		10000-65535	Select virtual TCP port to organize DLC-1
tcp port2		10000-65535	Select virtual TCP port to organize DLC-2
timer 10min	<ON_OFF>	on/off	Enable/disable timeout for command reception from SORM CP

3.3.10.4 SS-7 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 SS-7 line group for the current stream
quit			Terminate this CLI session
show			Show SS-7 signalling parameter configuration
SLC	<slc>	0-15	Set the signal channel identifier in SS-7 line group

3.3.11 Fail2ban parameter configuration mode

To enter this mode, execute 'fail2ban' command in the configuration mode.

SMG-[CONFIG]> fail2ban
Entering fail2ban mode.
SMG-[CONFIG]-[FAIL2BAN]>

Command	Parameter	Value	Action
?			Show the list of available commands.
blacklist_ip add	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format	Add IP address to the Fail2ban blacklist
blacklist_ip remove	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format	Remove IP address from the Fail2ban blacklist
blacklist_ip show all			Show the Fail2ban blacklist
blacklist_ip show first	<COUNT>	0-4095	Show the specified amount of addresses from the beginning of the Fail2ban blacklist
blacklist_ip show ip	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format	Find specified address in the Fail2ban blacklist
blacklist_ip show last	<COUNT>	0-4095	Show the specified amount of addresses from the end of the Fail2ban blacklist
exit			Return from this configuration submenu to the upper level.
history			View history of entered commands.

quit			Terminate this CLI session
restart			Restart fail2ban process
set block_time	<BLCKTIME>	60-352800	Set the time in seconds during which access from the suspicious address will be banned
set enable	<ENA>	on/off	Enable/disable Fail2ban utility
set tries	<TRIES>	1-10	Define the maximum quantity of unsuccessful service access attempts for a host prior to be banned by fail2ban
set forgive_time	<FORGIVETIME>	60-352800	Define the remission time
set increment	<INCREMENT_FLG>	no/yes	Enable progressive ban
show			Show fail2ban settings
whitelist_ip add	<WHITEIP>	IP address in AAA.BBB.CCC.DDD format	Add IP address to the Fail2ban whitelist
whitelist_ip remove	<WHITEIP>	IP address in AAA.BBB.CCC.DDD format	Remove IP address from the Fail2ban whitelist
whitelist _ip show all			Show the Fail2ban whitelist
whitelist _ip show first	<COUNT>	0-4095	Show the specified amount of addresses from the beginning of the Fail2ban whitelist
whitelist _ip show ip	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format	Find the specified address in the Fail2ban whitelist
whitelist _ip show last	<COUNT>	0-4095	Show the specified amount of addresses from the end of the Fail2ban whitelist

3.3.12 Firewall parameter configuration mode

To enter this mode, execute 'firewall' command in the configuration mode.

SMG-[CONFIG]> firewall
Entering 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>	forward input output	Add firewall rule Rule direction
	<ENABLE>	enable/disable	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	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. 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

	<P_IDX>	1-65535	
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> <ID> <param>	action dport_end dport_start enable icmp-type name prof_id proto r_ip r_mask s_ip s_mask sport_end sport_start traffic-type 1-65535 New value according to this parameter type	Modify the firewall rule specified (one of the parameters)
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> <CDR_ACCESS> <LOG_ACCESS> <MNT_ACCESS>	 no_access r w rw no_access r w rw no_access r w rw	Add user Specify name for a new user Specify password for a new user Define CDR directory access permissions Define LOG directory access permissions Define MNT directory access permissions
user del	<IDX>	1-4	Remove user
user modify access	<IDX> <CDR_ACCESS> <LOG_ACCESS> <MNT_ACCESS>	0-4 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
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, 63 characters max.	Define the gateway name during registration at the Gatekeeper
config			Return to Configuration menu.
exit			Exit from this configuration submenu to the upper level.
gk_discover	<ON_OFF>	on/off	Enable/disable GK search mode
gk_ip	<IPADDR>	AAA.BBB.CCC.DDD	Specify GK IP address
gk_keepalive	<KEEPAL>	10-86400	Specify the time for registration at the GK
gk_port	<PORT>	1-65535	Specify GK port
gk_ttl	<TTL>	90-86400	Specify the time for registration renewal at the GK
gk_use	<ON_OFF>	on/off	Enable/disable GK
history			View history of entered commands.
iface	<IFACE_NAME>	String, 255 characters max.	Specify H.323 network interface
port	<PORT>	1-65535	Define the number of a local TCP port for H.323 signalling message reception
quit			Terminate this CLI session
show			Show 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	<CODEC>	G.711-A	Define codec, used for voice data transmission.
config			Return 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/ modem/ off	Set echo cancellation mode: *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 tunnelling
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	Select numbering schedule
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
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 stimer		Number in the range 5-255	Define S-timer
set number-mask		Max 255 symbols	Define call group mask

3.3.17 SS7 line group modification configuration mode

To enter this mode, execute 'linkset <LINKSET_INDEX>' command in the configuration mode, where <LINKSET_INDEX> is a line group 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 line group

alarm_ind	<ON_OFF>	on/off	Enable/disable fault indication for the specific SS-7 line group
CCI	<ON_OFF>	on/off	Enable support for the SS-7 line group channel integrity check
CCI frequency	<FREQ>	0-127	Define the frequency of channel integrity checks during outgoing calls performed through the SS-7 line group
cdpn digit in IAM	<ON_OFF>	on/off	Transmission of the first digit of CdPN number in IAM message for overlap dialling 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 SS-7 line group *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 SS-7 protocol specification support
combined	<ON_OFF>	on/off	Enable/disable combined mode
config			Return to Configuration menu.
DPC	<DPC_ID>	0-16383	Define opposite signalling 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.
init	<INIT_MODE>	blocked/ individual-ublock/ group-unblock/ group-reset	Define initialization type for the current line group
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 line group 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 numbering schedule for a LinkSet
OPC	<OPC_ID>	0-16383	Define the signalling point proprietary code for the current SS-7 line group
primary linkset	<PRI_LINKSET>	0-15	Select the primary SS-7 line group 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 SS-7 line group
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 SS-7 line group
secondary linkset	<SEC_LINKSET>	0-15	Select the secondary SS-7 line group for the combined mode operation
show			Show configuration of the current SS-7 line group
ss7timers	<index>	0-15	Select SS-7 timer profile
TMR	<TMR>	speech/ 64kb_unrestricted/ 3.1KHz_audio/transit	Define the Transmission Medium Requirement for the current SS-7 line group
trunk	<trunk_index>	0-31	Define the trunk group number for the current SS-7 line group

3.3.18 SS-7 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

Togotothismodeyoushould 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 theConfiguration menu
history			Veiw a history of the entered commands
quit			CompletreCLI session
set msp	<INDEX> 0-5	On/off	Enable/disable submoduleSM-VPwith selected index
show			Showtableofsubmoduleusage.

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
Entring 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. should be enclosed in quotation marks	Add modifier: MODIFIER_MASK—modifier mask. CLD_RULE—callee number modification rule. CLG_RULE—caller number modification rule.
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 numbering schedule type for the callee number: MODIFIER_INDEX—modifier number. CALLED_NP_TYPE—numbering schedule type.
change called rule	<MODIFIER_INDEX> <CALLED_RULE>	0-8191 modifier rule, 30 characters max.	Edit callee number modification rule for the modifier

		should be enclosed in quotation marks	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 LD lines and CLR lines 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/ isdn/ telephony/ national/ private	Edit modifier numbering schedule type for the caller number: MODIFIER_INDEX—modifier number. CALLING_NP_TYPE—numbering schedule 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/	Edit caller screen indicator modification rule

		network/nochange	
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. CALLING_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 LD lines and CLR lines 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 numbering schedule
change mask	<MODIFIER_INDEX> <MODIFIER_MASK>	0-8191 modifier mask, 255 characters max., should be enclosed in parentheses '(' and ')'	Edit modifier mask MODIFIER_INDEX—modifier number. MODIFIER_MASK—mask.
change modtable	<MODIFIER_INDEX> <NEW_MODTBL_INDEX>	0-8191 0-255	Move 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 LD lines and CLR lines 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 pptpVPNclient	<LABEL> <IPADDR> <USER> <PASS>	you may use letters, 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.	Add a new VPN/PPTP client 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, numbers, '_', '.', '-', ':' characters, 63 characters max.	Define password (for VPN interface only)
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	<PORT>	1-65535	Define TCP port for the device

telnet			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 parameter 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	Define the network mask

		format	
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	Modify PPTP parameters Modify tag Modify encryption activity Modify password Modify PPTP server IP address Modify automatic PPTP startup Modify username

		characters max.	
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 Numbering schedule 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	Create prefix in the specified numbering schedule
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	Define the number of active numbering schedules
set domain	<IDX> <DOMAIN>	0-15 String, 15 characters max.	Specify domain for registration
set name	<IDX> <NAME>	0-15 String, 15 characters max.	Define the numbering schedule name
show active count			Show the number of active numbering schedules
show active list			Show the list of active numbering schedules
show list			Show the list of numbering schedules
show prefixes	<IDX>	0-15 no/yes	Show numbering schedule 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 for the line group
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: *local*—local *emergency*—special service

			zone—zone network *vedomst*—to private 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.
mask edit			Enter the prefix mask editing mode
mask show			Show prefix masks
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
numplan	<PLAN_IDX>	0-15	Define numbering schedule 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)
quit			Terminate this CLI session
service	<PFX_USER_SERVICE>	cf-unconditional/ cf-busy/ cf-no-reply/ cf-out-of-order	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 numbering schedule, but the dialling of additional digits is possible at the same time that will cause a match with another sample. Default value—5sec.
trunk	<TRUNK>	0-31	Specify trunk group number
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—numbering schedule change *modifier*—modifier prefix type *user_service*—VAS prefix *pickup-group*—pickup group

			ivr—select IVR scenario

3.3.22.1 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.
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
auth ipaddr	<IP_ADDR> <SRV_IDX>	IP address in AAA.BBB.CCC.DDD format 0-8	Define the authorization server (Authorization) IP address. IP_ADDR—IP address SRV_IDX—server number
auth port	<PORT> <SRV_IDX>	0-65535 0-8	Define the authorization server (Authorization) port. PORT—port number SRV_IDX—server number
auth secret	<SECRET> <SRV_IDX>	String, 31 characters max. 0-8	Define the authorization server (Authorization) password. SECRET—password SRV_IDX—server number
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 name	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk	Define the User-Name attribute for Accounting-Request packets: *cgpn*—use calling party phone number as a value. *ip_or_stream*—use calling party IP address or incoming connection stream number as a value. *trunk*—use incoming connection trunk name as a value.
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 special services, local and zone network. *local*—allow calls to special services and local network. *emergency*—allow calls to special 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
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 special 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 name	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk	Define the User-Name attribute for Access-Request packets: *cgpn*—use calling party phone number as a value. *ip_or_stream*—use calling party IP address or incoming connection stream number as a value. *trunk*——use incoming connection trunk name as a value.
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/	Define NAS physical port type (server for user authentication), default value is Async.

		Ethernet/ xDSL/ Cable/ Wireless/ Wireless_IEEE_802.1	
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 special services, local and zone network. *local*—allow calls to special services and local network. *emergency*—allow calls to special 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_cicso_h323_credit_time*— use Session-Time or Cisco VSA h323-credit-time attribute value as the maximum call duration timeout.
auth userpasswd	<ON_OFF>	on/off	Enable/disable custom passwords for SIP subscribers during authorization
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
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 SS-7 subscriber category transmission
use eltex-vsa	<ON_OFF>	on/off	Enable 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 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.
exit			Exit from this configuration submenu to the upper level.
mask add	<PREFIX_MASK>	prefix mask. 255 characters max., should be enclosed in	Add a new mask

[1]This menu is available in the firmware version with Call-record license only, for license details, see Section **3.1.23. Licenses**

		parentheses '(' and ')'	
mask modify direction	<TYPE>	all/ calling/ called	Change the mask type to the specified one
mask modify mask	<PREFIX_MASK>	prefix mask. 255 characters max., should be enclosed in parentheses '(' and ')'	Modify mask value
mask remove	<IDX>	0-4095	Remove mask
mask show			Show all masks
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 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 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> <ENABLE>	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 String, 255 characters max. disable/enable	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
route del	<IDX>	0-4095	Remove route: IDX—network route index
show			Show the route configuration information

3.3.29 Q.850 clearback reason 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

3.3.30 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	<PORT>	1-65535	Define the server port that syslog messages will be sent to
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)

3.3.31 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 for the line group
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
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'clearchanneloverride' option – announce CLEARMOD codec to second leg when first leg operates in 'clear channel' operation mode
clearchan transit	<on/off>	<on/off>	Set 'clearchanneltransit' option– transmittedRTPshould be exactly the same with the RTP transmitted to the first leg (including packetization time).
codec	<CODEC>	G.711-A	Define codec, used for voice data transmission.
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	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'
early media header	<early media header>	(off/on)	Enable P-Early-Media support (RFC5009)
ecan	<CANCELLATION>	voice/ nlp-off-voice/ modem/	Set echo cancellation mode: *Voice*—echo cancellers are enabled

		off	(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
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
inband_signal_ with_183_and_sdp	on/off		Issue reply 183/SDP to SIP for voice frequency path 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, '_'	Define the interface name

		character 31 characters max.	
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	Select numbering schedule
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 numbering schedule 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
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
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
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

3.3.32 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	<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

3.3.33 SIP subscribers parameter configuration mode[1]

To enter this mode, 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
remove	<INDEX>	0-1999	Remove the current user
savedb			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.
service	<INDEX>	0-1999	Switch to the VAS configuration mode for the specified subscriber.
set access category	<INDEX> <CAT_IDX>	0-1999 0-31	Define the access category for the specific subscriber
set user access mode	<INDEX> <ACCESS>	0-1999 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 specific subscriber
set user blf			Define blf settings
set authorization	<INDEX> <AUTHMODE>	0-1999 none/register/ register_and_invite	Define the user authorization mode INDEX—SIP subscriber index AUTHMODE—authorization mode: *None*—do not request authorization *register*—request authorization on registration *register_and_invite*—request authorization on registration as well as when performing outgoing calls
set user category	<INDEX> <CATEGORY>	0-1999 0-9	Specify Caller ID category for the selected subscriber INDEX—SIP subscriber index CATEGORY—subscriber's Caller ID category.

[1]This menu is available in the firmware version with SIP registrar support

Set user domain	<INDEX> <DOMAIN>	0-1999 String, 15 characters max.	Set the SIP domain for a subscriber INDEX—SIP subscriber index DOMAIN—domain name
set user ipaddr	<INDEX> <IPADDR>	0-1999 IP address in AAA.BBB.CCC.DDD format	Define IP address for the selected subscriber
Set user lines	<INDEX> <COUNT>	0-1999 1-255 or 0	Define the quantity of calls that the subscriber may take part in simultaneously. Permitted value range is [1;255] or 0—unlimited.
set login	<INDEX> <LOGIN> <PASSWORD>	0-1999 String, 15 characters max. String, 15 characters max.	Define authentication username and password for this subscriber.
set user name	<INDEX> <NAME>	0-1999 String, 31 characters max.	Define SIP subscriber name
set user number	<INDEX> <NUMBER>	0-1999 Subscriber number	Define SIP subscriber number
set user numberAON	<INDEX> <NUMBER>	0-1999 Subscriber number	Specify Caller ID number for the current subscriber
set user numplan	<INDEX> <PLAN_IDX>	0-1999 0-15	Specify the numbering schedule for the subscriber
set user pbx_profile	<INDEX> <PROFILE>	0-1999 0-31	Define PBX profile for SIP subscriber
Set user profile	<INDEX> <PROFILE>	0-1999 0-31	Define SIP profile for SIP subscriber
Set user redirection	<INDEX> <REDIRECTION>	0-1999 enable/disable	Enable/disable redirection (302) utilization for SIP subscriber
set registration	<INDEX> <ON_OFF>	0-1999 on/off	Enable/disable complete digest authentication (rfc 5090) for subscribers with dynamic registration. In DIGEST authentication, 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. If the digest is not used, authentication will be partial—authentication parameters will be generated by the gateway itself.
set user typeAON	<INDEX> <TYPE>	0-1999 unknown/ subscriber/ national/ international/ network_specific/ nochange	Specify Caller ID number type for the current subscriber TYPE—Caller ID 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 LD lines and CLR lines for outgoing international call processing.
set user numberList	<NumPlan Index>	0-15	Define an additional number
set group access category	<INDEX> <CAT_IDX>	0-63 0-31	Define the access category for the subscriber group
set group access mode	<INDEX> <ACCESS>	0-63 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 specific group
set group blf subscribers usage		Disable/enable	Enable BLF service
set group category	<INDEX> <CATEGORY>	0-63 0-9	Specify Caller ID category for the selected group INDEX—SIP subscriber index CATEGORY—subscriber's Caller ID category.
set group domain	<INDEX> <DOMAIN>	0-63 String, 15 characters max.	Set the SIP domain for a group INDEX—SIP subscriber index DOMAIN—domain name
set group lines	<INDEX> <COUNT>	0-63 1-255 or 0	Define the quantity of calls that the group may take part in simultaneously. Permitted value range is [1;255] or 0—unlimited.
set group max	<MAX_REG>	0-63	Define number of subscribers in a group
set group name	<INDEX> <NAME>	0-63 String, 31 characters max.	Specify group name
set group numplan	<INDEX> <PLAN_IDX>	0-63 0-15	Define the group numbering schedule
set group pbx_profile	<INDEX> <PROFILE>	0-63 0-31	Define group PBX profile
set group profile	<INDEX> <PROFILE>	0-63 0-31	Define group SIP profile
set group Re-INVITE a=sendonly		enable/disable	Enable hold service upon re-invite message reception with a=sendonly marker
set group redirection	<INDEX> <REDIRECTION>	0-63 enable/disable	Enable/disable redirection (302) utilization for uheggs
set group refer		disable/enable	Enable call transfer with the 'refer' message
show count			Show SIP subscriber quantity
show list			Show SIP subscriber list
show user	<INDEX>	0-1999	Show SIP subscriber information
show group	<INDEX>	0-63	Show group information

3.3.33.1 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	<TYPE>	blf-usage call-pickup cfb cfnr cfoos cfu ct clear-all conf-3way conference hold intercom	Enable BLF Call pickup Specify cfb service parameters Specify cfnr service parameters Specify cfoos service parameters Specify cfu service parameters Specify ct service parameters Specify clear-all service parameters Specify 3WAY service parameters Specify 3WAY service parameters Specify hold service parameters Specify intercom service parameters

3.3.34 SS-7 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—SS-7 category
show			Show information on SS-7 data category.

3.3.35 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.

[1]For SMG-1016M only

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[1]			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> <ACT>	GE_PORT0(0)/ GE_PORT1(1)/ GE_PORT2(2)/ CPU(4)/ SFP0(6)/ SFP1(7) 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 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/	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).

[1]Not supported in the current firmware version.

		untagged/ tagged/ double-tag	- *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>	GE_PORT0/ GE_PORT1/ GE_PORT2/ CPU/ SFP0/ SFP1 GE_PORT0/	Specify allowed ports for packet transfer: PORT—port being configured P_DEST—allowed transmission ports

[1]Not supported in the current firmware version.

	<ENABLE>	GE_PORT1/ GE_PORT2/ CPU/ SFP0/ SFP1 on/off	
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> <OVER>	CPU/ GE_PORT0/ GE_PORT1/ GE_PORT2/ SFP0/ SFP1 on/off	Set the mode for VLAN ID redefinition to a standard one for the current port
show mirror settings			Show port mirroring parameters
show port settings			Show port configuration parameters

3.3.35.1 802.1q 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>	0-4095 0-7 on/off unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/	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

	 <SFP0> <SFP1>	not_member unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member	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

3.3.35.2 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

3.3.36 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
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.
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 UDP port number for operation via SIP-T protocol
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.

3.3.37 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

3.3.38 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

3.3.39 Trunk group and trunk direction 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.
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 Unsigned integer value	Assign the trunk group to the Q931, SS-7 or SIP-T interface TG_ENTRY—interface type ENTRY_INDEX—object index (number of Q931 signalling stream, line group, 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.
local	<YES_NO>	yes/no	Configure/Do not configure SORM tracking for subscribers of this direction with the number type and marker 'subscriber of the current PBX'.
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
reserv	<TG_RSV_IDX>	0-31	Define the redundant trunk group number
show			Show the trunk group configuration

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 design

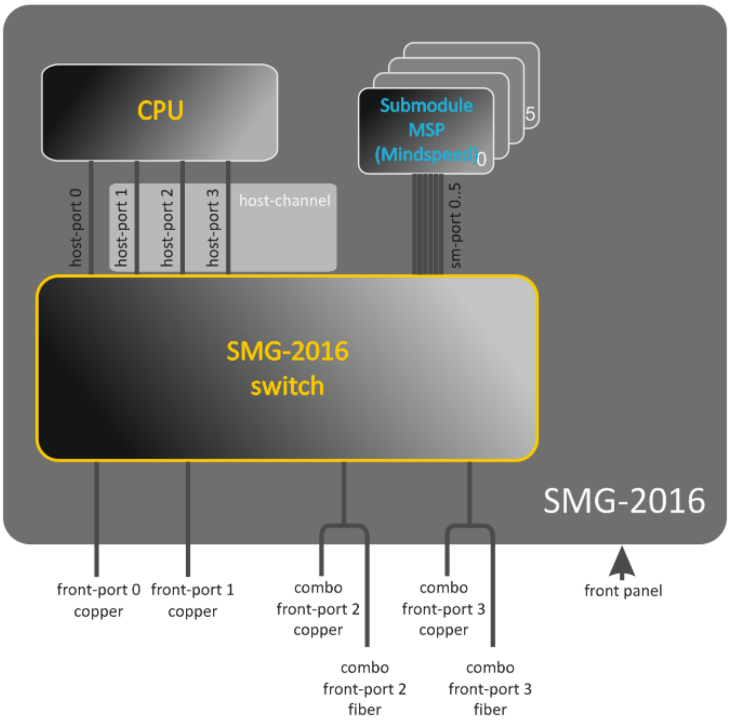


Fig. 35—Switch structure

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.

– *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 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 Codepoint (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

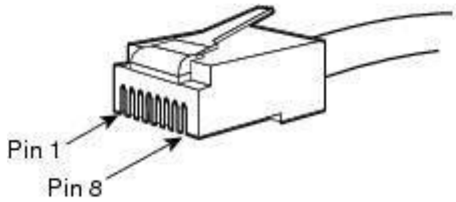
CONFIG – SWITCH

APPENDIX A. CABLE CONTACT PIN ASSIGNMENT

For SMG-2016

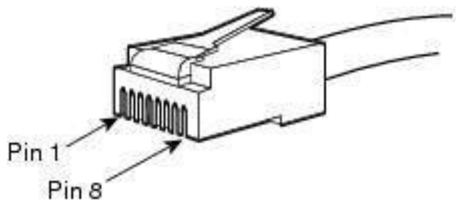
Assignment of the **RJ-48** connector pins for connection of ***E1 Line 0..15*** streams is ISO/IEC 10173 compliant and provided in the table below.

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	

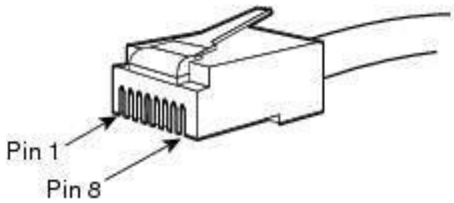
Assignment of the ***Console*** port **RJ-45** connector pins is provided in the table below.

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***

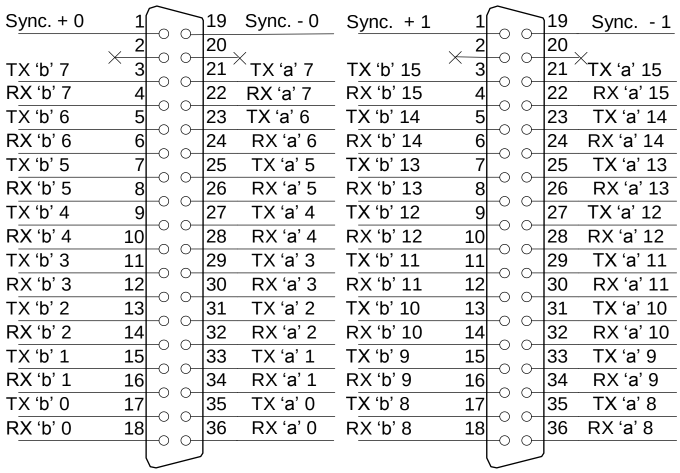


Fig. 36—Assignment of *E1 Line* contact pins

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

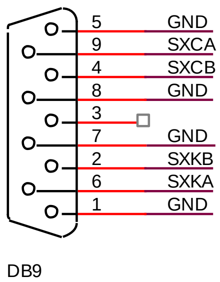


Fig. 37—Assignment of *Console* port contact pins

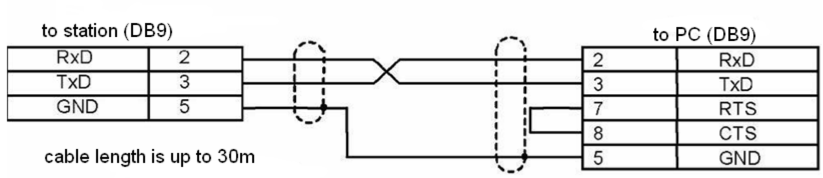


Fig. 38—Cable wiring diagram for PORT1, PORT2 connection

E1 Line wire colour and terminal contact correspondence table

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

1. 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.

2. 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 modification—remove the first digit, replace it with 34, leave other digits as is—for outgoing dialling matching with the mask (1x{4,6}).

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 SS-7-SIPT transit

Source data:
Stream from the opposite PBX is physically connected to the E1 stream 0 at the SMG connector.

SS-7 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 SS-7 by trunk group 0
- Route to SIP-T by trunk group 1
- Transition to SS-7 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 SS-7 signalling messages are transferred by transit

Configuration via CLI:

SS-7 signalling parameters configuration:

```
SMG>config // Enter the configuration mode
SMG-[CONFIG]>new linkset// Create a new line group (linkset)
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 opposite signalling point code
Linkset[0]. Set DPC '32'
SMG-[CONFIG]-LINKSET[0]>OPC67// Define the proprietary signalling 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 SS-7 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 SS-7 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 SS-7 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 SS-7 line group
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 SS-7 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 SS-7 line group
Entering trunk-mode
SMG-[CONFIG]-TRUNK[0]>destinationSS7 0// Associate the trunk group 0 with SS line group 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 SS-7 line group
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. VAS SETTINGS TRANSMISSION FROM RADIUS SERVER FOR DYNAMIC SUBSCRIBERS.

The gateway allows to transfer 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='—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 forwardon out of service
  - CT—call transfer
  - CallPickup—call pickup
  - BLF—busy lamp field (BLF)
  - Intercom—access to intercom and paging calls

- '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='—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=5;
```

APPENDIX E. ROUTING, SUBSCRIBERS AND SIGNAL LINK PARAMETERS CORRELATION

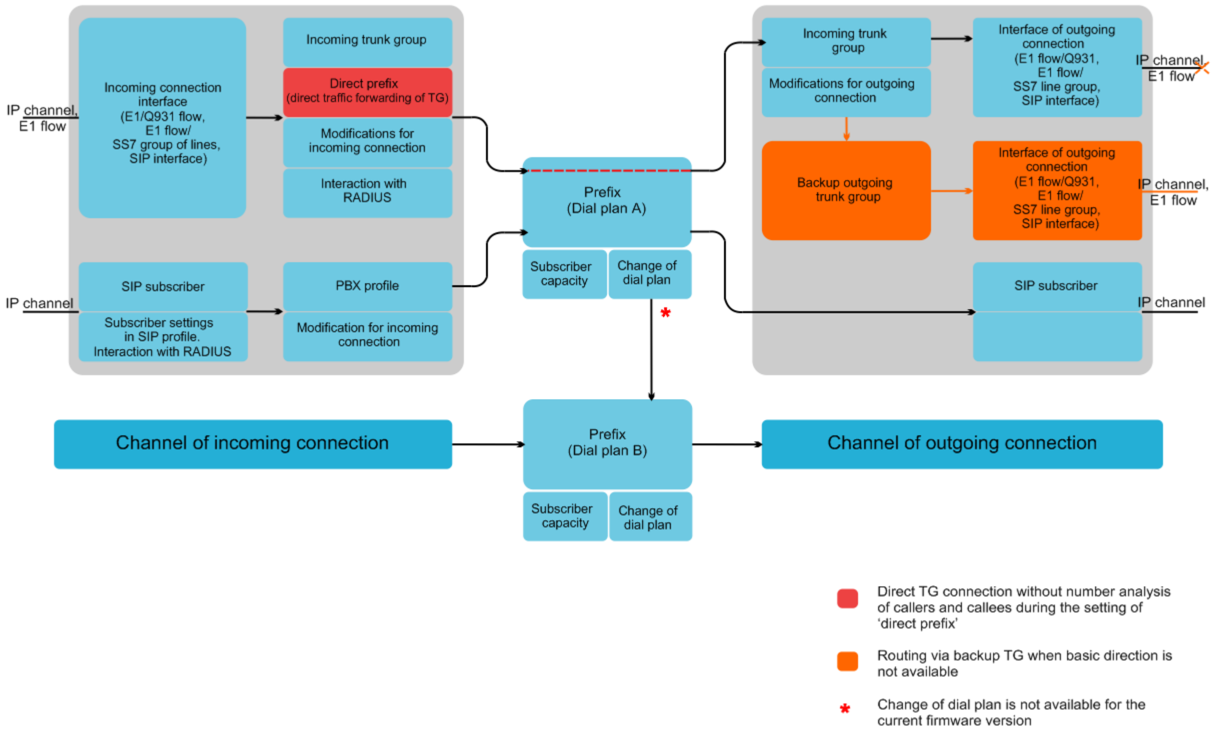


Fig. 39—Routing, subscribers and signal link parameters correlation

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 bruteforcing, 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 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 fail2ban utility.

Fail2ban 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**.

[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, SS-7 line group is not in operation
  - *SS7LINK*—SS-7 signal channel failure
  - *TRUNK-CPS*—permitted number of calls per second is exceeded for a trunk group

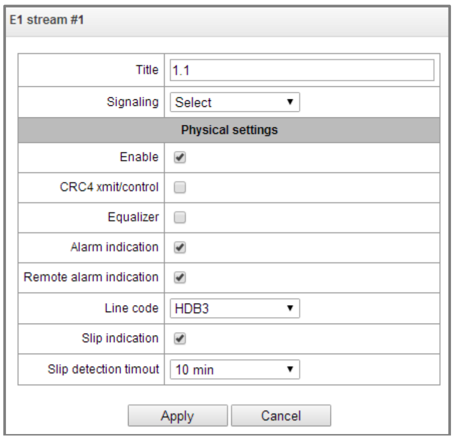
These alarms are configured in SS-7 line group configuration (Section **3.1.7.2**).

By default, optional fault indication is disabled, i.e. for monitoring systems interactions, you should configure fault indication for all E1 streams and SS-7 line groups (linksets) 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.

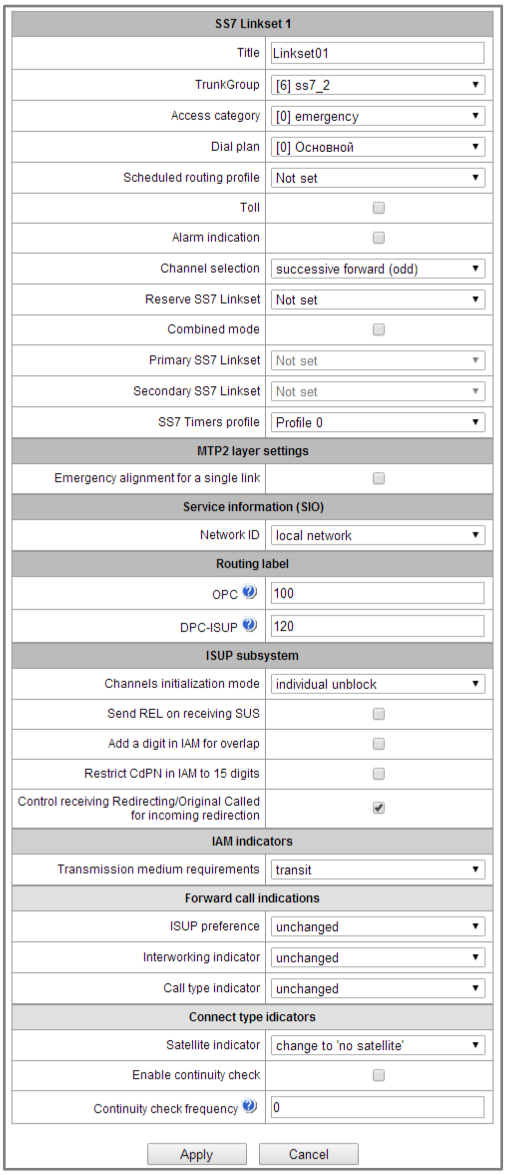
Parameter configuration via web configurator

1) Optional fault indication configuration for E1 stream configuration (*'E1 stream/Physical parameters'* menu, see Section **3.1.5.2Configuration of physical parameters**).

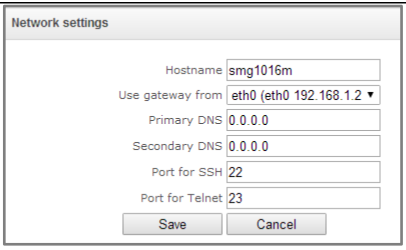


For LOS and AIS fault indication, select the *'Alarm indication'* checkbox for the E1 stream.
For RAI fault indication, select the *'Remote alarm indication'* checkbox.
For slips indication for a stream, select *'SLIP indication'* checkbox and configure SLIP detection timer.

2) Optional fault indication configuration for SS-7 line group configuration (*'E1 streams/SS7 linkset'*, see Section **3.1.5.4**).

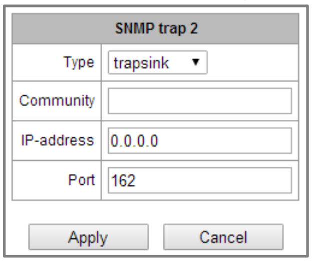


For SS-7 signal link fault indication, select the *'Fault indication'* flag.
3) To enable SNMP, go to *'TCP settings/IP/Network parameters'* menu (Section**3.1.10.2Network Settings***)*.



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**).



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 oh 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

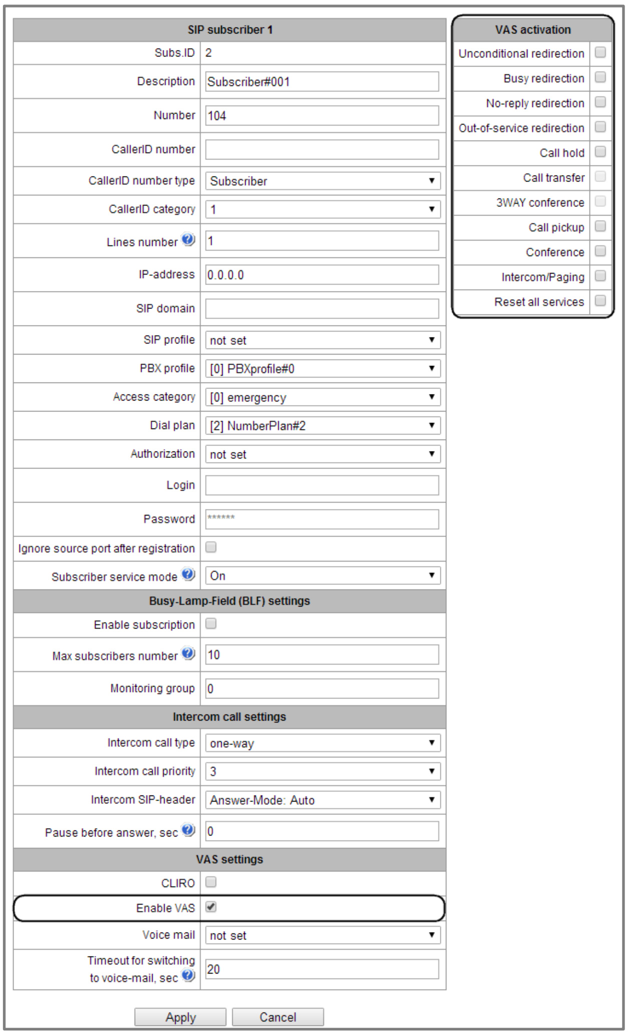
Beginning from the firmware version 2.15.01, the device features the following VAS:

- *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).*
- *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.
- *Cancel 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.



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 short clearback 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.
- Clearback—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 RD-45)

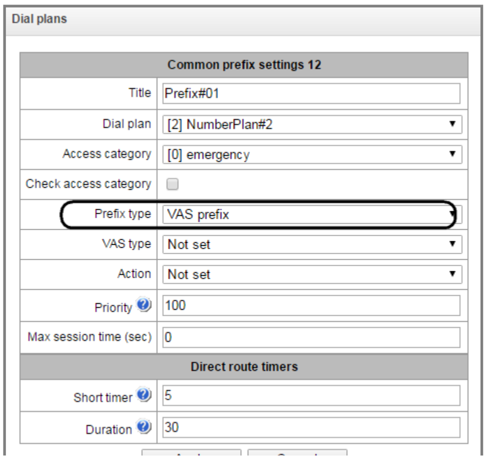
The subscriber may activate or deactivate the service themselves by dialling specific prefixes on their phone unit. Redirection service prefixes are configured in the numbering schedule (Section 0**Incoming number modifiers**—select modifier table used for subscriber phone number analysis and modification located in messages received from SORM CP.

Outgoing **number modifiers**—select modifier table used for subscriber phone number analysis and modification located in messages sent to SORM CP.

Always modify B-number– option is required to modify all ‘B’ numbers. In the past, modificator of outgoing numbers aren’t applied for number dialed by local subscriber.

Modificator of controlled numbers – selection of modificator table specified to analize and modify subscriber phone number before it will be sampled for transmitting to SORM CP.

Numbering schedule); for that, add a new prefix with the *'Prefix type'/'VAS prefix'* value.



For VAS, we recommend using 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 numbering schedule, 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

This service allows the initiator to establish the conference by consequently adding participants using subscriber hold feature.
Upon the initiator clearback, participants will hear the busy tone. Maximum number of conference participants—10.
Access to service is governed by the 'Conference with consequent assembly' VAS category checkbox.

Usage	* 71# <NUMBER 1><CONF> R<NUMBER 2><CONF> …

<NUMBER N>—number of the subscriber participating in a conference.
<CONF>—conference call state
R—short clearback (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>#

<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>#

<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. Cancelling 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 'Cancel all services' VAS category checkbox.

Usage	* 50#

APPENDIX J. RADIUS CALL MANAGEMENT SERVICE

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 numbering schedule, 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 numbering schedule 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 numbering schedule 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 numbering schedule 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.

Possible optional part parameters:

- numtype.
- plantype.
- presentation.

In general, command format will be as follows:

1.CallManagement:CgPNin=<$modifymask>;numtype=<$numtype>;plantype=<$plantype>;presentation=<$pres entation>

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 **3.1.8.4.5Modification 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 numbering schedule of the gateway and unconditionally forward it to a prefix created in the configuration (equivalent to the 'direct prefix' parameter described in Section **3.1.7.1Trunk 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 numbering schedule 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—numbering schedule sequential number.
$prefix_index—ID of a prefix created in the numbering schedule.

Example

Change the call numbering schedule 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' 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 available to the current subscriber.

In general, command format will be as follows:

```
"UserManagement:MaxActiveLines=<$line_count>
```

where
$line_count—quantity of active connections available to the subscriber simultaneously.

Example

Define three active lines for a subscriber.

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): UserManagement:MaxActiveLines=3
```

TECHNICAL SUPPORT

For technical assistance in issues related to handling of EltexAlatau Ltd. equipment please address to Service Centre of the company:

9 Ibragimova street, Almaty, Republic of Kazakhstan, 050032,
Phone:
+7(727) 320-18-40
+7(727) 320-18-38
E-mail: info@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:

http://www.eltexalatau.kz/en