

A solid blue vertical bar with rounded ends, positioned to the left of the main text.

Digital gateways

SMG-1016M, SMG-2016, SMG-3016

Operation manual, firmware version 3.21.5

CONTENT

1	RELEASE NOTES	8
2	CONVENTIONAL SYMBOLS AND AUDIENCE	14
	2.1 Conventional symbols.....	14
	2.2 Tips, notes and warnings	15
	2.3 Audience	15
3	PRODUCT DESCRIPTION	16
	3.1 Introduction.....	16
	3.2 Product Description	16
	3.2.1 Application	16
	3.2.2 Typical Application Diagrams	19
	3.2.2.1 Interfacing of TDM and VoIP network signalling and media streams.....	19
	3.2.2.2 Mini IP-PBX.....	20
	3.2.2.3 Outstation via V5.2	21
	3.2.3 Device Design and Operating Principle	22
	3.2.3.1 SMG-1016M design	22
	3.2.3.2 SMG-2016 design	23
	3.2.3.3 SMG-3016 design	24
	3.2.3.4 SMG operating principle	25
	3.2.4 Main Specifications	26
	3.2.5 Design	29
	3.2.5.1 SMG-1016M.....	29
	3.2.5.2 SMG-2016	30
	3.2.5.3 SMG-3016	32
	3.2.6 LED Indication	34
	3.2.6.1 Device light indication in operation	34
	3.2.6.2 LED indication of E1 stream status	36
	3.2.6.3 Light indication of Ethernet 1000/100 interfaces	37
	3.2.6.4 Light indication during startup and reset to factory defaults	37
	3.2.6.5 Fault LED Indication	39
	3.2.7 'F' button operation	39
	3.2.8 Saving factory configuration	40
	3.2.9 Password recovery	40
	3.2.9.1 CLI password recovery	40
	3.2.9.2 WEB password recovery	41
	3.2.10 Delivery package	43
	3.2.10.1 SMG-1016M.....	43
	3.2.10.2 SMG-2016	43
	3.2.10.3 SMG-3016	43
	3.2.11 Safety instructions.....	44
	3.2.11.1 General Guidelines.....	44
	3.2.11.2 Electrical Safety Requirements	44
	3.2.11.3 Electrostatic Discharge Safety Measures	44
	3.2.11.4 Power Supply Requirements.....	44
	3.2.12 SMG Installation	45
	3.2.12.1 Startup sequence	46
	3.2.12.2 Support brackets mounting	46
	3.2.12.3 Device rack installation	47
	3.2.12.4 Power module installation	47
	3.2.12.5 Removing the housing	48
	3.2.12.6 Submodule Installation	51
	3.2.12.7 Installation of ventilation units	54
	3.2.12.8 SSD installation for SMG-1016M	56
	3.2.12.9 SATA drive installation for SMG-2016, SMG-3016.....	57
	3.2.12.10 RTC battery replacement	58
	3.3 General Switch Operation Guidelines.....	59
4	DEVICE CONFIGURATION	60
	4.1 SMG configuration via web configurator.....	60

4.1.1	System settings	63
4.1.2	Monitoring	68
4.1.2.1	Telemetry	69
4.1.2.2	E1 streams.....	70
4.1.2.3	E1 channel monitoring.....	72
4.1.2.4	CPU utilization chart	76
4.1.2.5	SFP module monitoring	77
4.1.2.6	Front ports monitoring	77
4.1.2.7	VoIP submodule monitoring.....	78
4.1.2.8	Fault alarms. Alarm events list.....	81
4.1.2.9	Network interface monitoring	84
4.1.2.10	Local disk drives	84
4.1.2.11	V5.2 interfaces	85
4.1.2.12	Queue statistics.....	85
4.1.2.13	VNS tasks (section is available with SMG-VNS licence).....	86
4.1.3	E1 streams.....	87
4.1.3.1	Synchronization sources	87
4.1.3.2	Signaling protocol selection	88
4.1.3.3	Physical settings.....	89
4.1.3.4	Signaling protocol settings DSS1/EDSS1 (ISDN PRI Q.931)	90
4.1.3.5	SS7 signaling protocol configuration	94
4.1.3.6	V5.2 signaling protocol configuration.....	96
4.1.3.7	SORM signaling protocol configuration	97
4.1.4	Dial plans.....	99
4.1.4.1	Creating a prefix in the dial plan	101
4.1.4.2	Description of Number Mask and Its Syntax.....	106
4.1.4.3	Mask Operation Examples	107
4.1.4.4	Timer operation examples	108
4.1.4.5	Configuration example of prefix with 'subscribers pool' type.....	108
4.1.5	Call routing.....	109
4.1.5.1	Trunk groups	109
4.1.5.2	SS7 Linkset	114
4.1.5.3	SIP/SIP-T/SIP-I, SIP-profiles	120
4.1.5.4	H323 interfaces	145
4.1.5.5	Trunk directions	155
4.1.5.6	V5.2 interfaces	156
4.1.5.7	SIP-Trunk Registrations	159
4.1.6	Subscribers.....	160
4.1.6.1	SIP Subscribers	160
4.1.6.2	PRI profiles	171
4.1.6.3	Dynamic subscribers groups	172
4.1.6.4	V5.2 subscribers.....	178
4.1.6.5	PRI Subscribers.....	184
4.1.7	Internal resources	187
4.1.7.1	CDR settings	187
4.1.7.2	SS7 Categories.....	198
4.1.7.3	Access categories	199
4.1.7.4	Routing by access category	202
4.1.7.5	PBX profiles	202
4.1.7.6	Modifier tables.....	205
4.1.7.7	Q.931 timers	210
4.1.7.8	SS7 timers	211
4.1.7.9	Q.850-cause and SIP-reply code correspondence table	213
4.1.7.10	Scheduled routing	215
4.1.7.11	Time redirection.....	216
4.1.7.12	Hunt groups	216
4.1.7.13	Pickup groups.....	221
4.1.7.14	Voice messages	222
4.1.7.15	SIP replies list to switch on reserve	223

4.1.7.16	Q.850 release causes list	223
4.1.7.17	Q.850 recovery causes list	224
4.1.8	Voice notification system	224
4.1.8.1	Voice messages	227
4.1.8.2	Notification tasks	228
4.1.8.3	Numbers list	230
4.1.8.4	Reports.....	232
4.1.8.5	Notify records	233
4.1.9	LDAP.....	234
4.1.9.1	LDAP-storage list	234
4.1.10	Voice mail	235
4.1.10.1	Voice mail settings	235
4.1.10.2	Voice messages (only for SMG-2016)	236
4.1.11	IVR	237
4.1.11.1	Scenarios list	237
4.1.11.2	Tones list	247
4.1.11.3	Call records (IVR).....	248
4.1.12	Call recording.....	251
4.1.12.1	Call recording settings.....	251
4.1.12.2	Call records	254
4.1.12.3	Group notification records.....	257
4.1.12.4	Call record settings	258
4.1.13	TCP/IP Settings	261
4.1.13.1	Routing tables	262
4.1.13.2	Network settings.....	263
4.1.13.3	Network interfaces	263
4.1.13.4	RTP ports.....	267
4.1.14	Data transfer	267
4.1.15	Network services	268
4.1.15.1	NTP.....	268
4.1.15.2	SNMP settings	269
4.1.15.3	SNMPv3.....	270
4.1.15.4	SNMP trap settings	270
4.1.15.5	DHCP server settings.....	272
4.1.15.6	FTP server	275
4.1.16	Network utilities.....	276
4.1.16.1	PING	276
4.1.16.2	TRACEROUTE.....	277
4.1.17	Security.....	279
4.1.17.1	SSL/TLS settings	279
4.1.17.2	Dynamic firewall	280
4.1.17.3	Blocked addresses list	282
4.1.17.4	Static firewall	283
4.1.17.5	White addresses list.....	287
4.1.17.6	SMG firewall operation scheme	288
4.1.17.7	Providing SMG firewall tasks	288
4.1.18	RADIUS settings.....	289
4.1.18.1	Servers	289
4.1.18.2	Profiles	290
4.1.18.3	RADIUS replies to voice messages mapping	296
4.1.18.4	RADIUS packet format	297
4.1.18.5	Variable description	299
4.1.18.6	Authorization calls	301
4.1.18.7	Interaction with verification nodes of IS Antifraud.....	303
4.1.19	Traces	307
4.1.19.1	PCAP traces	307
4.1.19.2	PBX traces	311
4.1.19.3	Syslog settings.....	315

4.1.20	Network switch (for SMG-1016M only)	316
4.1.20.1	LACP settings.....	316
4.1.20.2	Configuration of switch ports	318
4.1.20.3	802.1q	320
4.1.20.4	QoS and bandwidth control	321
4.1.20.5	Queue priority mapping.....	323
4.1.21	Working with objects and 'Objects' menu	324
4.1.22	Saving configuration and 'Service' menu	324
4.1.23	Time and date configuration	325
4.1.24	Firmware update via web configurator	325
4.1.25	Licenses	326
4.1.26	'Help' menu	329
4.1.27	'Users: Management' menu	329
4.1.28	View factory settings and system information.....	331
4.1.29	Exit the configurator.....	331
4.2	Command line, list of supported commands and keys (SMG).....	332
4.2.1	Command line in debug mode, list of supported commands and keys.....	332
4.2.1.1	Tracing commands available through the debug port.....	333
4.2.2	SMG configuration via Telnet, SSH, or RS-232	334
4.2.2.1	List of CLI commands	335
4.2.2.2	Change device access password via CLI	337
4.2.2.3	Statistics mode.....	337
4.2.2.4	Management mode	342
4.2.2.5	Port mirroring parameters configuration mode	343
4.2.2.6	General device parameter configuration mode	344
4.2.2.7	CDR parameter configuration mode.....	347
4.2.2.8	CDR field list	349
4.2.2.9	Access categories' configuration mode	350
4.2.2.10	E1 stream configuration mode	351
4.2.2.11	Dynamic firewall's parameters configuration mode.....	355
4.2.2.12	Static firewal's parameters configuration mode	357
4.2.2.13	FTP parameter configuration mode.....	362
4.2.2.14	H.323 protocol parameter configuration mode	363
4.2.2.15	H.323 interface parameter configuration mode.....	364
4.2.2.16	Call group configuration mode	368
4.2.2.17	SS7 link set modification configuration mode	369
4.2.2.18	SS7 timer configuration mode	371
4.2.2.19	Configuration mode of submodule usage.....	372
4.2.2.20	Modifier table configuration mode	373
4.2.2.21	Network parameter configuration mode.....	376
4.2.2.22	Dial plan configuration mode	383
4.2.2.23	Pickup group configuration mode	387
4.2.2.24	PBX profile configuration mode.....	387
4.2.2.25	Q.931 timer configuration mode	388
4.2.2.26	RADIUS configuration mode	389
4.2.2.27	Callback authorization configuration mode.....	396
4.2.2.28	Conversation recording settings configuration mode	397
4.2.2.29	Call records masks configuration modes	398
4.2.2.30	Static route configuration mode.....	399
4.2.2.31	Q.850 release causes list configuration	400
4.2.2.32	SIP/SIP-T general settings editing mode	400
4.2.2.33	SIP/SIP-T interface parameter configuration mode.....	401
4.2.2.34	Interface subscriber registration parameter configuration mode.....	409
4.2.2.35	SIP subscribers parameter configuration mode	410
4.2.2.36	Subscribers group's VAS configuration mode.....	417
4.2.2.37	PRI-subscribers' parameters configuration mode	418
4.2.2.38	VAS configuration mode for PRI subscribers	420
4.2.2.39	PRI profiles configuration mode	421
4.2.2.40	SORM configuration mode	422

4.2.2.41	SS7 category modification configuration mode.....	423
4.2.2.42	Switch parameter configuration mode.....	423
4.2.2.43	Syslog parameter configuration mode	431
4.2.2.44	Voice message file management configuration mode	432
4.2.2.45	IVR function configuration mode.....	433
4.2.2.46	Trunk group configuration mode.....	433
4.2.2.47	Trunk directions configuration mode	435
4.2.3	SMG-2016/SMG-3016 switch configuration	435
4.2.3.1	Switch structure	435
4.2.3.2	SMG 2016/3016 switch interface management commands	437
4.2.3.3	Aggregation group configuration commands	444
4.2.3.4	SMG-2016 board VLAN interface management commands.....	446
4.2.3.5	STP/RSTP configuration commands.....	447
4.2.3.6	MAC table configuration commands	450
4.2.3.7	Port mirroring configuration commands	451
4.2.3.8	SELECTIVE Q-IN-Q configuration commands	454
4.2.3.9	DUAL HOMING protocol configuration.....	456
4.2.3.10	LLDP protocol configuration	459
4.2.3.11	QOS Configuration	465
4.2.3.12	Configuration operation commands.....	468
4.2.3.13	Miscellaneous commands.....	469
5	APPENDIXES (SMG)	471
5.1	Appendix A. Cable contact pin assignment	471
5.1.1	For SMG-2016, SMG-3016	471
5.1.2	For SMG-1016M.....	472
5.1.3	Correspondence tables for wire and pin colors of the E1 Line connector.....	473
5.2	Appendix B. Alternative firmware update method	474
5.2.1	Alternative device firmware update method using RS-232	474
5.2.2	Alternative device firmware update method using USB flash drive	476
5.3	Appendix C. Examples of modifier operation and device configuration via CLI	476
5.3.1	Modifier operation examples	476
5.3.1.1	The procedure for applying modifiers on incoming communications	476
5.3.1.2	The procedure for applying modifiers on outgoing communications	476
5.3.1.3	Objective 1	477
5.3.1.4	Objective 2	478
5.3.2	CLI device configuration example	479
5.3.2.1	Objective	479
5.3.2.2	Source data	479
5.3.2.3	Configuration via CLI	480
5.4	Appendix D. Transmission of VAS settings from RADIUS server for dynamic subscribers	485
5.4.1	Request syntax.....	485
5.4.2	Service activation examples.....	486
5.5	Appendix E. SORM function configuration	487
5.6	Appendix F. Interaction of the device with monitoring systems.....	487
5.7	Appendix G. Voice messages and music on hold (MOH)	490
5.8	Appendix H. Working with VAS services.....	491
5.8.1	Working with 'Call hold', 'Call transfer', 'Three-way conference' services	494
5.8.2	Working with 'Redirection' service	495
5.8.2.1	Call forward unconditional (CF Unconditional):.....	495
5.8.2.2	Call forward on busy (CF Busy):	495
5.8.2.3	Call forward on no reply (CF No reply):	495
5.8.2.4	Call forward on out of service (CF Out Of Service):	496
5.8.2.5	Call forward on time	496
5.8.3	Conference with sequential participant collection (Conference)	497
5.8.4	Call pickup.....	499
5.8.5	Intercom and paging calls	499
5.8.6	Password activation/deactivation, restricted by password.....	500
5.8.7	Change password.....	500

5.8.8	Outgoing calls restriction	500
5.8.9	Do not disturb	501
5.8.10	Blacklist.....	501
5.8.11	Reset all services	501
5.8.12	Follow me	502
5.8.13	Follow me no response	503
5.8.14	Call park to	504
5.8.15	Voice mail	504
5.8.16	One touch record	508
5.8.17	Anonymous call	508
5.8.18	Reject anonymous calls	508
5.8.19	Reminder	509
5.9	Appendix I. Radius call management service	510
5.9.1	CgPN and CdPN number modification request syntax.....	510
5.9.2	Call routing management	512
5.9.3	Call category management	512
5.9.4	Subscriber parameter management	513
5.10	APPENDIX J. MONITORING AND MANAGEMENT VIA SNMP	515
5.10.1	OID description from MIB ELTEX-SMG	516
5.10.2	Monitoring and configuration of SIP subscribers (static subscribers)	536
5.10.2.1	Monitoring	536
5.10.2.2	Example of a search by index.....	537
5.10.2.3	Example of a search by numbering plan and full subscriber's number	537
5.10.2.4	Example of a search by numbering plan and partial subscriber's number	538
5.10.2.5	View information without using a search	539
5.10.2.6	Configuration	539
5.10.2.7	Example of new subscriber creating.....	539
5.10.2.8	Example of settings viewing.....	540
5.10.2.9	Example of settings editing.....	540
5.10.2.10	Example of subscriber removing	540
5.10.3	Monitoring and configuration of dynamic subscriber groups	546
5.10.3.1	Monitoring	546
5.10.3.2	Example of a search by index.....	547
5.10.3.3	Example of a search by subscriber ID	547
5.10.3.4	Example of a search by numbering plan and substring number	547
5.10.3.5	View the information without searching	548
5.10.3.6	Configuration	548
5.10.3.7	Example of group creating	549
5.10.3.8	Example of settings viewing.....	549
5.10.3.9	Example of settings editing.....	549
5.10.3.10	Example of group removing.....	549
5.10.3.11	Out-of-date OID	556
5.10.3.12	OID MIB-2 support (1.3.6.1.2.1).....	557
5.11	Appendix K. SMG Redundancy Function	557
5.12	Appendix L. Safety recommendations	564
5.12.1	Changing passwords on WEB and CLI.....	564
5.12.2	Creating restricted accounts	565
5.12.3	Restricting access to signaling and management interfaces.....	565
5.12.4	Configuring a static firewall	566
5.12.5	Configuring a dynamic firewall	566
5.13	Appendix H. Configuring a software media server	567
5.13.1	Media server settings	569
5.13.2	Media server launch.....	571
5.13.3	Example of setting up MSR with Softswitch	571

1 RELEASE NOTES

Firmware Version: V. 3.21.5			
Document version	Firmware version	Issue date	Revisions
Version 4.9	V.3.21.5	01.11.2023	Changed: <ul style="list-style-type: none"> – Changed the format of messages sent to the verification node RTK-NT, before updating it is necessary to contact RTK-NT to change the software on their equipment.
Version 4.8	V.3.21.1	27.10.2023	Added: <ul style="list-style-type: none"> – Interaction with verification node of IS "Antifrod" by RADIUS protocol for call verification purposes.
Version 4.7	V.3.21.0	27.10.2023	Added: <ul style="list-style-type: none"> – SORM support – VAS: "Anonymous call", "Reject anonymous calls", "Reminder"; – Marking of listened call records. Changed: <ul style="list-style-type: none"> – Improved logic for conferences with sequential collection.
Version 4.6	V.3.20.5	31.03.2023	Added: <ul style="list-style-type: none"> – Option "ISUP Location Number"; – Name transfer method QSIG-NA (Ericsson); – Monitoring of trunk groups via SNMP; – Monitoring of licenses via SNMP; – Monitoring of the number of installed C4E1, SMVP modules via SNMP; – Option "Transfer DisplayName in Remote-Party-ID header". Changed: <ul style="list-style-type: none"> – Expanded the VNS functionality; – Removed the need for a license to record conversations for the VNS work.
Version 4.5	V.3.20.3	14.11.2022	Added: <ul style="list-style-type: none"> – Option "DTE/DCE mode adjustment" for the SORM protocol; – Option "Notify about call completion in (sec)" on prefix in the numbering plan; – Ability to upload cdr files via SCP protocol; – Option "Replace symbol '?' by 'D' in CgPN" for Q.931 protocol; – Option "CISCO 1700 adaptation" for H.323 interfaces. Changed: <ul style="list-style-type: none"> – Removed the option "VAS reset timeout" for dynamic subscribers.
Version 4.4	V.3.20.0	31.07.2022	Added: <ul style="list-style-type: none"> – VAS "One touch record"; – Hang up mode "Silent" for call groups; – Disk monitoring via SNMP; – Modification of RedirPN for RADIUS; – Logic "AND" in the dial plan; – Name transmission method for H323 interfaces; – Ability to clear queue statistics; – Option "Call back the person who rejected the call in a Hunt Group"; – Option "Allow inband DTMF"; – Option "Stream order by SLC"; – SNMP request to obtain the IP address value from the network interface; – RingBack settings for a call group when queues used; – Reset configuration via cli; – Monitoring of web interface active sessions; – Modifiers for outgoing communication in a PRI profile; – Monitoring of KPD1 KPD2 performance during TCP implementation; – Operation of the OOB port on SMG-3016; – Reset counters button for SMG-1016M. Changed: <ul style="list-style-type: none"> – Reworked removal of logs; – Increased the number of consecutive redirects to 10; – Expanded state indication of external synchronization source for Sync ports; – For SMG-1016M, maximum number of subscriptions has been limited to 500; – Expanded the VNS functionality; – The number of accounts in the web interface has been increased to 100 pieces.
Version 4.3	V.3.19.0	13.05.2021	Added: <ul style="list-style-type: none"> – Multiple registration (SIP-forking); – Voice notification system; – Routing by access category; – Transfer "real ip" to RADIUS-Accounting; – Switch settings for SMG-3016;

			<ul style="list-style-type: none"> - SMG-3016 redundancy; - Statistics of Radius requests via SNMP; - Listening to conversation recordings without the possibility of downloading; - Run at startup (automatically enable logging after restarting the gateway); - Transfer of Display name when calling through a call group; - Voice mail. Playing message details; - Access category for the Dial block in IVR; - V5.2-LE. Hotline service. <p>Changed:</p> <ul style="list-style-type: none"> - Changed answer from 502 to 486 busy here when using VAS "DND"; - Operation of OPTIONS messages in a reservation scheme (switching precedence does not stop operation of SIP OPTIONS messages); - Operation of transport mode on SIP interfaces (one mode is allowed on one port).
Version 4.2	V.3.18.0	14.05.2020	<p>Added:</p> <ul style="list-style-type: none"> - Registering a SIP subscriber from a random network interface; - TO instead of RURI for routing (optional); - Option "Transit SIP headers" for SIP profile; - LDAP server (SMG-2016; SMG-3016); - Voice mail. <p>Changed:</p> <ul style="list-style-type: none"> - Increased the service life of the backup device up to 720 hours; - Added extension number to call recordings when calling a call group via IVR; - Display of alarms, all current alarms are in a separate list; - Configuring the transport protocol is now on each SIP-interface; - Fixed defects when assembling a pair of master-slave using LACP.
Version 4.1	V.3.17.0	18.11.2019	<p>Added:</p> <ul style="list-style-type: none"> - Support for working with a remote LDAP server; - VAS "Call Parking"; - E1 stream reservation (SMG-2016); - Advanced sip profile settings; - Ability to use "Login" as "User-Name" during authorization/accounting via RADIUS; - Call group number in the conversation recording if you reached subscriber through this group. <p>Changed:</p> <ul style="list-style-type: none"> - Switching settings in the web interface has been changed from drop-down list to tabs, for convenience; - Added timeout between master- slave pair switching"; - Removed setting of a broadcast address in network interfaces (automatic completion); - Playing the time and position in the queue is divided into two various functions (Call group); - "Modifier" prefix type has been renamed to "Subscriber capacity"; - "Direct Prefix Availability Control" has been renamed to "Block if direct prefix is unavailable".
Version 4.0	V.3.16.0	07.08.2019	<p>Added:</p> <ul style="list-style-type: none"> - NTP server on SMG-1016M; - PRI profile for PRI subscribers; - Support for multiple E1 streams for PRI subscribers; - Limitation on the number of lines for PRI subscribers; - Use of different numbering plans for PRI subscribers; - Calls from PRI subscribers; - SNMP trap about changing E1 stream synchronization sources; - SNMP OID with E1 stream name; - Forwarding by day of the week and time of day; - The names of external drives are binded to the interface ports; - Video stream transmission in Video Offroad mode; - Blocking the trunk if the direct prefix is unavailable. <p>Changed:</p> <ul style="list-style-type: none"> - The size of the pickup group has been increased to 60 participants; - Hunt group timer upper limit has been increased to 3600 seconds; - Settings in the web are sorted – the most used functions are moved up and logically grouped.
Version 3.8	V.3.14.1	16.04.2019	<p>Added:</p> <ul style="list-style-type: none"> - Authorization with a callback when a RADIUS CoA request is received.
Version 3.7	V.3.14.0	28.11.2018	<p>Added:</p> <ul style="list-style-type: none"> - Transmitting the received SIP header X-UniqueTag or forming it from the RADIUS Acct-Session-Id value; - SNMP OID of SIP trunk availability; - Ability to enable call traces by trunk group or by phone number; - Transfer of Connected Name for SIP subscribers; - Transition to local call service when transit registration on the server is absent; - Hang-up mark on the device side in the CDR.

Version 3.6	V.3.12.0	22.10.2018	<p>Added:</p> <ul style="list-style-type: none"> – Operation in light reserve mode according to the 1+1 scheme; – Queues in call groups.
Version 3.5	V.3.10.1	23.07.2018	<p>Added:</p> <ul style="list-style-type: none"> – Edit identifier of the link for V5.2; – Own subscribers via PRI; – RADIUS servers aggregation into groups for different servers usage in RADIUS profiles; – Opportunity to send non-modified CgPN or CdPN in User-Name to RADIUS independent from assigned CgPN and CdPN modifiers; – Option to ignore HOLD indication in SS7 linkset settings; – "Blacklist" VAS (for SMG-2016); – "Do not disturb" VAS (for SMG-2016); – NTP server; – NTP servers advertisement through DHCP.
Version 3.4	V. 3.10.0	06.12.2017	<p>Changed:</p> <ul style="list-style-type: none"> – "fail2ban" section has been renamed to "dynamic firewall"; – "firewall profiles" section has been renamed to "static firewall"; – Rules of blocking in dynamic firewall has been separated for different services. <p>Added:</p> <ul style="list-style-type: none"> – Numbers modification while dial plan changing; – Delayed applying of configuration changes in dial plans; – The "exception" mask when a number is selected; – Opportunity to set the description of a trunk group; – Automatic uploading of configuration via FTP and TFTP protocols; – Transmission of requests to RADIUS according to selection by modifiers tables; – Transmission of subscriber IP address to RADIUS in Framed-IP-Address attribute; – Settings of SNMP notifications on RADIUS requests; – BLF and intercom configuring while subscriber configuration via SNMP; – Access to call records according to call records category; – Automatic uploading of call records to FTP; – Call recording to USB storage; – A name of recorded call contains a dial plan; – Hop counter settings in SS7 linksets; – Location Number modification; – SIP headers transit; – Optional display-name filling when a call without display-name is received; – Automatic gain management; – Notification of subscribers by recorded message; – SIP subscribers authorization only via IP address; – Settings of subscriber displayed name and priority of using configured name; – Traceroute functions.
Version 3.3	V. 3.9.0	31.07.2017	<p>Added</p> <ul style="list-style-type: none"> – New V5.2 LE protocol; – New VAS types: access to intercity calls via password, password activation, outgoing calls restriction (Appendix H. Working with VAS services); – Copying of prefixes among dial plans; – Selection of egress RADIUS profile in SIP interface settings); – Opportunity to change order of SIP interfaces in the list; – Selection of dial plan in Dial block of IVR scenario; – Opportunity to download MIB files from the device; – Local GateKeeper operation description.
Version 3.2	V. 3.8.0	09.01.2017	<p>Added</p> <ul style="list-style-type: none"> – Time rounding selection for RADIUS parameters; – Conversation record file name transmission in RADIUS parameters; – 'Clear All' service management through RADIUS for dynamic subscribers; – # and * usage in IVR select blocks;

			<ul style="list-style-type: none"> - The quantity of numbering plans has been extended to 255 on SMG-2016¹; - Common prefix creation for all pickup groups; - Number modifiers testing; - Selective E1 stream assignment from SS7 linksets to different trunk groups; - SS7 channel continuity testing through the WEB interface; - If SIP RURI and To fields has a distinction, Redirecting and Original Called numbers issuing will be disabled; - Diversion field can be issued in SIP URI format; - + symbol transmission can be disabled for international numbers; - subnet address assignment for incoming calls is available in SIP interface configuration; - DTMF transmission by SIP NOTIFY (Cisco DTMF); - Incoming and outgoing calls restrictions can be configured separately for SIP subscribers; - Language selection and saving based on browser configurations and user selection; - Call hold in incoming trunk with automatic connection via alternative route, in case of connection loss; - INVITE duplication to SMS receiver server; - SMS receiving via SMPP, then transmission via SIP to SMS server. <p>Changed</p> <ul style="list-style-type: none"> - All IVR settings were moved to IVR configuration tab; - 'IVR Caller Info' block keeps initial subscriber's name , if it is out of the number mask (initial name was deleted in previous firmware versions).
Version 3.1	V.3.7.0	26.08.2016	<p>Added:</p> <ul style="list-style-type: none"> - Setting of SM-VP submodule usage; - Customizable set of CDR fields; - List of CDR fields is extended; - Restriction of call duration on prefix; - Optional outgiving a MOH in settings of trunk group; - Setting a BLF monitoring group; - New options of SIP headers for general loudspeaker system (intercom).
Version 3.0	V.3.6.0	14.06.2016	<p>Added:</p> <ul style="list-style-type: none"> - Intercom and paging calls; - Restriction for quantity of calls (CPS) at trunks; - Fault indication for CPS limit exceeded at trunks; - SS7 signal link management via web configurator; - SS7 (CIC) channel management via web configurator; - RADIUS profile selection for outgoing communications in trunk group settings; - 'Local ringback for early-media' option; - QSIG tunneling protocol in SIP (SIP-Q).
Version 2.9	V.3.5.1	04.04.2016	<p>Added:</p> <ul style="list-style-type: none"> - P-Early-Media support (RFC5009).
Version 2.8	V.3.5.0	21/03/2016	<p>Added:</p> <ul style="list-style-type: none"> - Voice notification on conversation recording start; - WEB, TELNET, SSH intrusion protection in Fail2ban; - Configurable Q.850 release causes list for redundant trunk group transition; - Detection of * and # digits as a flash; - Conference assembly with the consequent assembly with re-INVITE with sendonly flag; - RADIUS-acct optional sending to both connection branches; - Dial plan name is displayed in settings tree; - Text description for each modification rule; - Changed mask order in prefix and modifier table; - Caller ID request in trunk group for incoming communication; - Call duration optional rounding up or down in CDR; - Configuration file upload in format <code>cfg_\${dev-name}_YYYYMMDD.yaml</code>; - RFC6432 'Carrying Q.850 Codes in Reason Header Fields in SIP (Session Initiation Protocol) Responses' support; - VLAN configuration on switch for SMG-2016.
Version 2.7	V.3.4.2	06.11.2015	<p>Added:</p> <ul style="list-style-type: none"> - 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	<p>Added:</p> <ul style="list-style-type: none"> - 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;



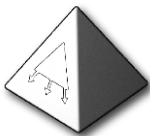



¹ Available only under VAS license.

			<ul style="list-style-type: none"> – Clear Channel override configuration; – Clear Channel-transit configuration; – local direction configuration for trunk; – Caller dial plan and mask configuration for call group.
Version 2.5	V.3.3.0	21.05.2015	<p>Added:</p> <ul style="list-style-type: none"> – Per-core CPU monitoring; – SIP response list for redundant trunk group transition; – 'Redirecting number' usage in call forwarding; – New call group operation modes; – REC and Caller Info blocks in IVR scenarios; – Blocking by fail2ban addresses list; – Original or processed numbers transmission in RADIUS messages; – RADIUS- Authorization transmission during local redirection; – Time transmission in UTC format in RADIUS-Accounting messages; – Playing of standard voice message phrases upon receiving denial message from RADIUS server with a reason for denial.
Version 2.4	V.3.2.1	30.03.2015	<p>Added:</p> <ul style="list-style-type: none"> – 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	<p>Added:</p> <ul style="list-style-type: none"> – Call Group and Pickup Group prefix type; – 'Send up to 15 digits to IAM' and 'Check presence of Redirecting/Original Called in incoming redirection' options in SS7 link set settings; – 'Transitional registration' option in SIP interface; – Configuration of call groups; – Configuration of pickup groups; – Ability to define gateway for network interfaces; – Dynamic subscriber group configuration.
Version 2.2	V.3.0.0	02.09.2014	<p>Added:</p> <ul style="list-style-type: none"> – Global Dual Homing port redundancy; – Ability to select Ethernet port operation mode; – Device firmware update via FTP; – 'NAT keep-alive' option in SIP profile; – https connection option.
Version 2.1	V.2.15.02	02.05.2014	<p>Added:</p> <ul style="list-style-type: none"> – Emergency phasing in case of a single signal link in linkset; – Fault indication when opposite device is not available via SIP; – Caller category transmission via SIP in cpc and cpc-rus fields; – Restriction for optional field transmission in SIP messages; – VAS timeouts; – SS7 timers; – Conversation recording feature.
Version 2.0	V.2.15.01	07.02.2014	<p>Added:</p> <ul style="list-style-type: none"> – VAS configuration; – VAS operation application; – Radius call management configuration.
Version 1.12	V.2.14.02	12.12.2013	<p>Added:</p> <ul style="list-style-type: none"> – LACP settings; – Configuration for dialing digits transmission to IAM during overlap; – Configuration for minimum subscriber registration interval; – DTMF RFC2833 PT transmission.
Version 1.11	V.2.14.01	10.10.2013	<p>Added:</p> <ul style="list-style-type: none"> – H.323 protocol operation support; – Q.850-causes and SIP-replies match table configuration; – Scheduled routing configuration; – RTP port range configuration; – FTP server configuration; – Firewall profile configuration; – Voice message usage configuration; – Device selection for fault logging; – View submodule link connection information; – SMG connection method example for operation in SS7 quasi-associated mode via PBX with STP features; – SMG connection method example for operation in combined mode; – Appendix. Voice messages and music on hold (MOH).
Version 1.10	V.2.12.01	20.05.2013	<p>Added:</p> <ul style="list-style-type: none"> – Appendix. Guidelines for SMG operation in public network'.

Version 1.9	V.2.12.01	1.04.2013	<p>Added:</p> <ul style="list-style-type: none"> – 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	<p>Added:</p> <ul style="list-style-type: none"> – Expanded list of E1 stream monitoring parameters; – SFP module monitoring; – Fault state monitoring; – Alarm events list; – MTP3 (DPC-MTP3) destination point code function support; – ISUP (DPC- ISUP) destination point code function support; – Dial plan wildcard search; – NAT (comedia mode) for SIP operation via NAT; – VPN/PPTP interface configuration; – Creation of list of allowed addresses used for device connection; – Trace filters: restriction on number of simultaneous calls for subscriber.
Version 1.7	V.2.10.04	20.09.2012	<p>Added:</p> <ul style="list-style-type: none"> – 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	<p>Added:</p> <ul style="list-style-type: none"> – Fail2ban settings; – CPU utilization monitoring; – Modifier operation examples; – Configuration of SIP interface registration parameters; – View list of addresses issued via DHCP; – STUN server settings; – Digest authorization settings; – SIP subscribers group editing.
Version 1.5	V.2.9.05	20.03.2012	<p>Added:</p> <ul style="list-style-type: none"> – 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	<p>Added:</p> <ul style="list-style-type: none"> – Maximum number of trunk groups and SIP interfaces increased up to 64; – SNMP trap configuration; – DHCP server management; – IP-MAC address binding; – Apply/confirm switch settings w/o gateway reboot; – Apply/confirm VLAN settings w/o gateway reboot; – Subscriber number availability check against configured SIP subscriber database; – Availability check for routing by number; – Ability to read CDR from local drives; – Reception monitoring for media traffic coming from the specific IP.
Version 1.3	V.2.1.01	3.11.2011	<p>Added:</p> <ul style="list-style-type: none"> – CDR configuration.
Version 1.2	V.2.1.01	21.10.2011	Bug fixes
Version 1.1	V.2.0.10	10.10.2011	<p>Added:</p> <ul style="list-style-type: none"> – DHCP server settings; – Received/transferred signal volume settings.
Version 1.0	V.2.0.10	12.09.2011	First edition.

2 CONVENTIONAL SYMBOLS AND AUDIENCE

2.1 Conventional symbols

Symbol	Description
Calibri	Notes, warnings, chapter headings, titles, table titles are written in bold.
<i>Calibri</i>	Important information is written in italic.
Courier New	Command entry examples, command execution results and program output data are written in Courier New.
<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

2.2 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.

2.3 Audience

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

3 PRODUCT DESCRIPTION

3.1 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 a 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 interfacing of traditional communication networks based on the circuit-switching principle with communication networks used packet-switching data transmission.

This operation manual details main features of SMG-1016M, SMG-2016 and SMG-3016 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.

3.2 Product Description

3.2.1 Application

Digital gateways SMG-1016M, SMG-2016 and SMG-3016 allow 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).

The number of E1 paths supported by SMG can reach 16, the number of conversational (media) channels on the E1 side is up to 495 and on the VoIP side is 768 (when using the G.711 codec with packetization time 20 ms or greater).

The gateway submodular design allows one to flexibly change the capacity, and the minimum number of module types 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.

The gateway allows one to organize one E1 stream per SORM console. E1 stream operating according to the SORM protocol contains 28 conversational channels for listening controlled subscribers. During combined control, the audio traffic from A and B subscribers is mixed to the SORM stream voice channel. Mixing of sound streams is performed using a three-way conference on the VoIP submodule. One VoIP submodule supports 27 three-way conferences. Thus, to ensure the possibility of interception simultaneously on all channels of the E1 stream, it is necessary that at least 2 VoIP submodules were installed on the gateway.

SMG main specifications:

- Number of E1 interfaces: 4 to 16, in increments of 4
- Up to 768 VoIP channels (128 channels in TDM for connecting to a single submodule)
- Number of Ethernet ports for SMG-1016M:
 - 3 × 10/100/1000BASE-T ports;
 - 2 × 1000BASE-X (SFP) ports.
- Number of Ethernet ports for SMG-2016, SMG-3016:
 - 4 × 10/100/1000BASE-T ports;
 - 2 × 1000BASE-X (SFP) combo ports.
- Static address and DHCP support
- DHCP server
- VoIP protocols: SIP, SIP-T, SIP-I, SIP-Q, MGCP¹, MEGACO¹, SIGTRAN¹, H.323²
- TDM protocols: DSS1/EDSS1 (ISDN PRI Q.931), QSIG and CORNET to transmit subscriber name, SS7 (associated and quasi-associated modes operation), V5.2;
- Support for the Q.699 standard — interaction between EDSS1 and SS7;
- SIP subscriber registration support:
 - Up to 2000 for SMG-1016M;
 - Up to 3000 for SMG-2016 and SMG-3016.
- DTMF transmission (SIP INFO, RFC2833, in-band, SIP NOTIFY);
- 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;
- ToS and CoS for RTP and signaling;
- 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.

¹ Not supported in the current firmware version.

² Optionally.

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 and 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).

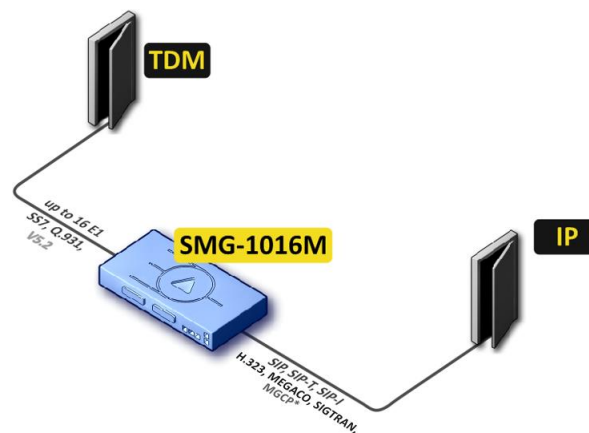
3.2.2 Typical Application Diagrams

This manual covers several SMG device connection methods.

3.2.2.1 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 (SS7, ISDN PRI/QSIG/CORNET, V5.2) and maintenance for up to 768 channels uncompressed (G.711 codec), up to 432 channels compressed (G.729 A/20-80), or 324 T.38 fax channels.

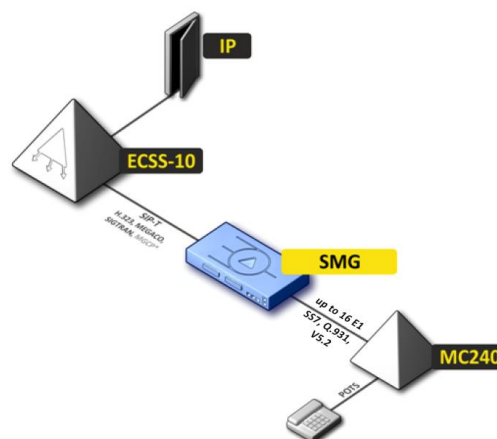
Device connects to the IP network via 10/100/1000BASE-T network interface using H.323/SIP/SIP-T/SIP-I protocols.



* — not supported in the current version

Figure 1 — Interfacing of TDM and VoIP network signalling and media streams

Figure 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

Figure 2 — Interfacing of TDM and VoIP network signalling and media streams

3.2.2.2 Mini IP-PBX

In this configuration, device provides the registration of up to 2000 subscribers for SMG-1016M and up to 3000 for SMG-2016 and SMG-3016 as well as the interaction with PSTN network via 16 E1 streams with various signalling protocols (SS7, ISDN PRI/QSIG/CORNET, V5.2).

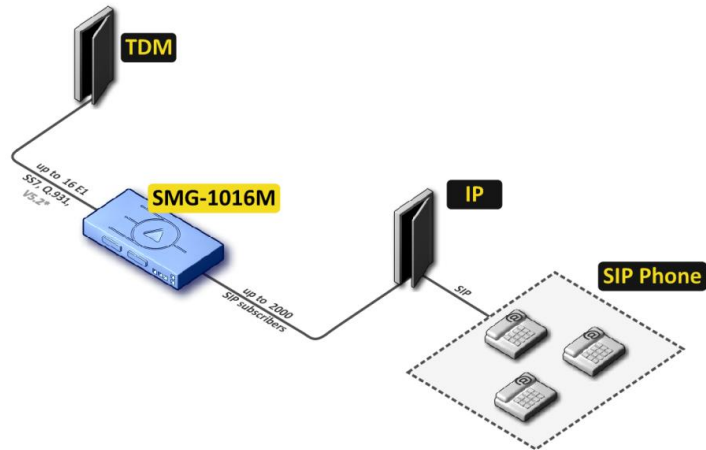


Figure 3 — Mini IP-PBX based on SMG-1016M

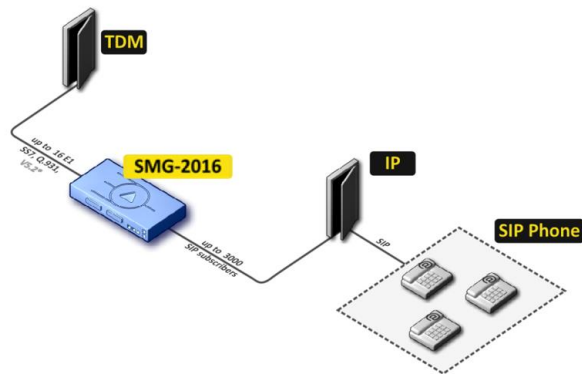


Figure 4 — Mini IP-PBX based on SMG-2016

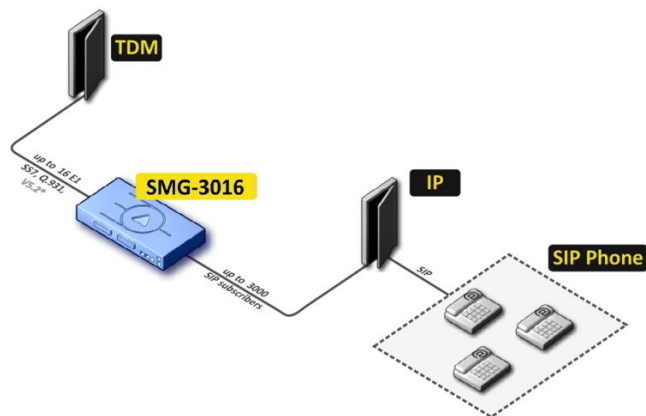


Figure 5 — Mini IP-PBX based on SMG-2016

3.2.2.3 Outstation via V5.2

The activation of additional features of IP PBX ECSS-10 software module allows to arrange outstation via V5.2 protocol and to service up to 2000 subscribers for SMG-1016M and up to 3000 subscribers for SMG-2016 and SMG-3016 with support for wide VAS set. As an outstation, the equipment with V5.2 AN support from any other manufacturer can be used.

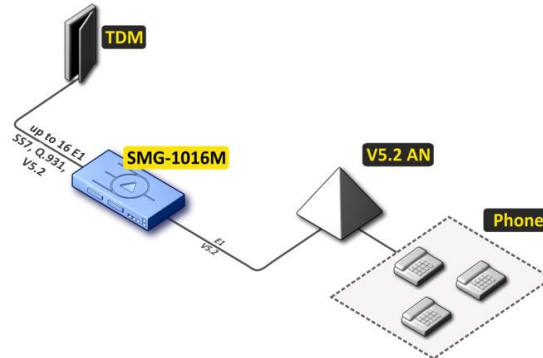


Figure 6 — V5.2 AN outstation based on SMG-1016M

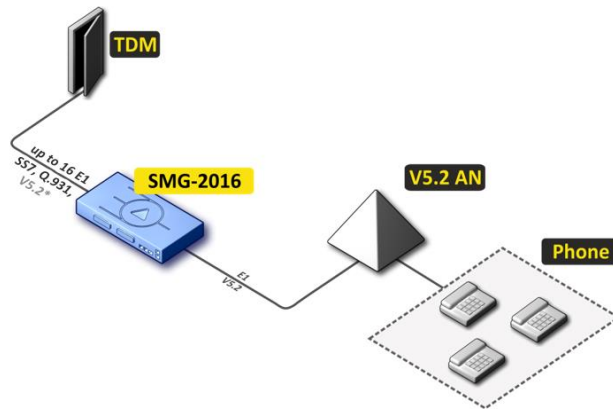


Figure 7 — V5.2 AN outstation based on SMG-2016

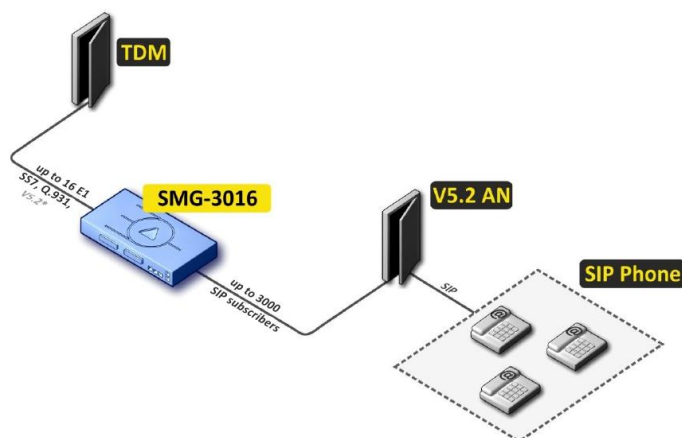


Figure 8 — V5.2 AN outstation based on SMG-2016

3.2.3 Device Design and Operating Principle

3.2.3.1 SMG-1016M design

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

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

The figure below shows SMG-1016M functional diagram.

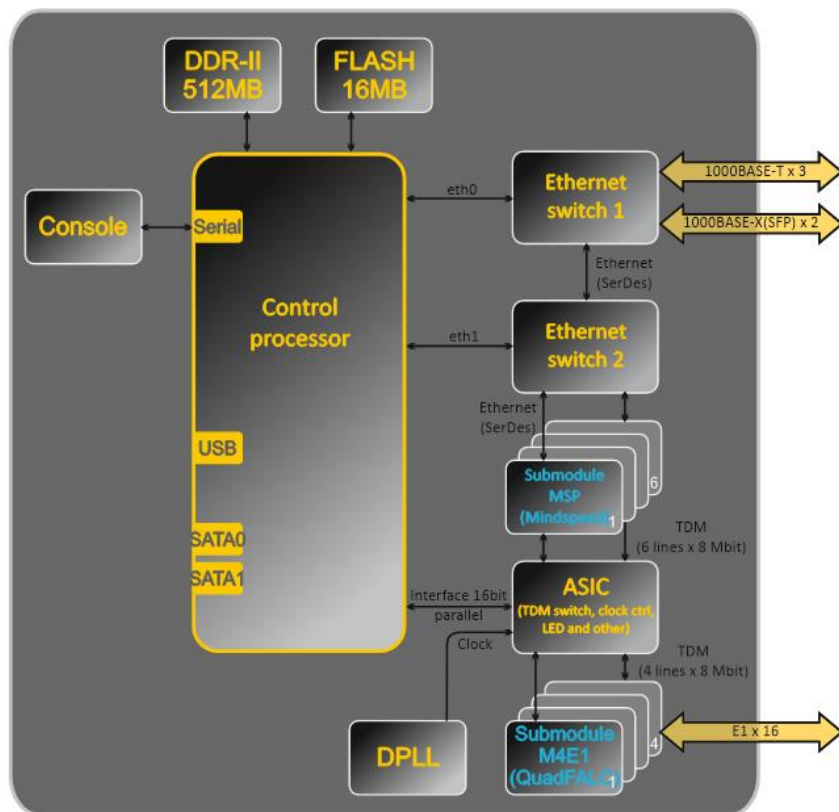


Figure 9 — SMG-1016M functional diagram

3.2.3.2 SMG-2016 design

SMG-2016 has a submodule architecture and contains the following elements:

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

The figure below shows SMG-2016 functional diagram.

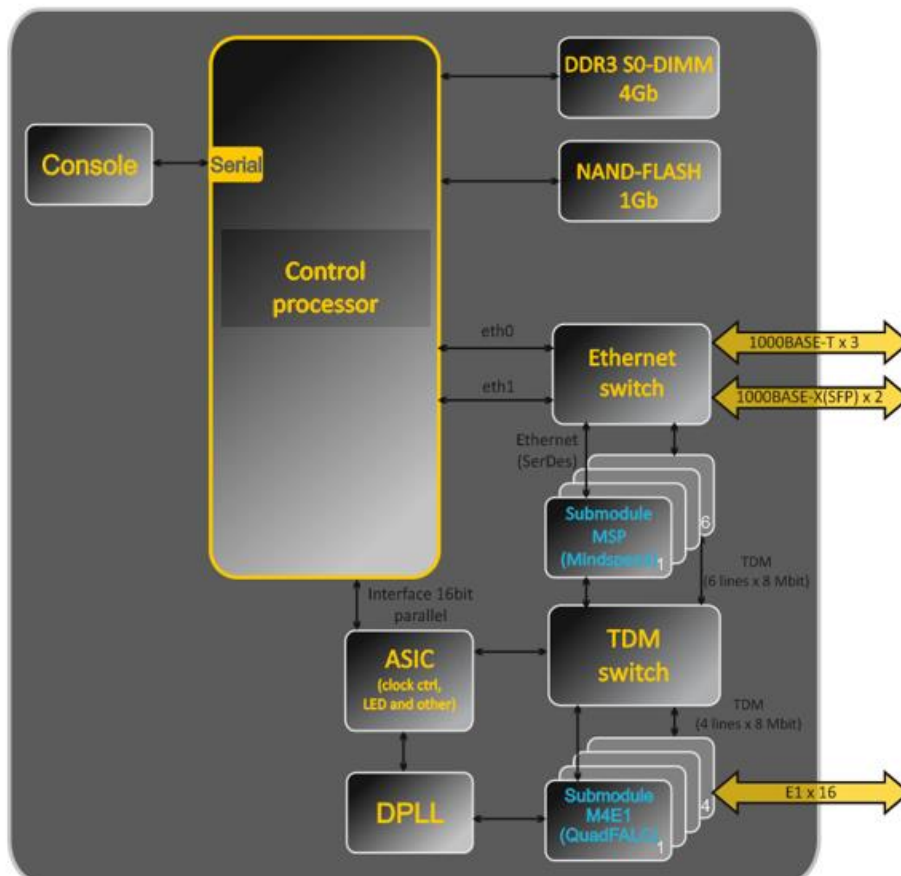


Figure 10 — SMG-2016 functional digram

3.2.3.3 SMG-3016 design

SMG-3016 has a submodule architecture and contains the following elements:

- Controller featuring:
 - Control processor;
 - Flash memory: 8192 MB.
- Up to 4 E1 stream submodules C4E1;
- Up to 6 IP submodules SM-VP-M300;
- Ethernet switch (L2), 4 × 10/100/1000BASE-T ports, 2 × MiniGBIC (SFP) combo ports;
- Switch fabric;
- Out-of-band port (OOB port);
- Phase-lock-loop (PLL) frequency control system.

The figure below shows SMG-3016 functional diagram.

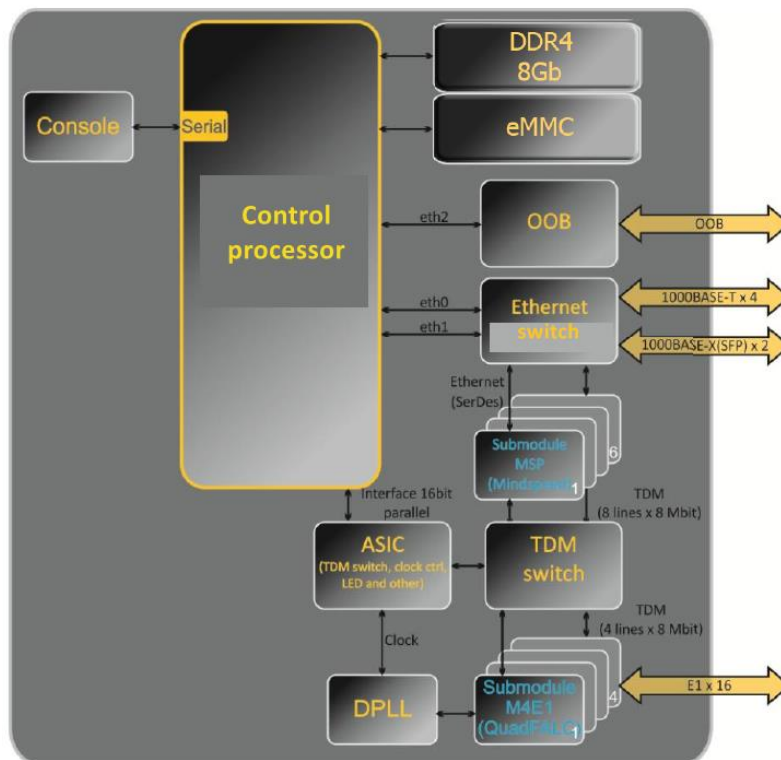


Figure 11 — SMG-3016 functional digram

3.2.3.4 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 trunk 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 trunk.

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

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



For SMG to operate, at least one SM-VP submodule should be installed.

For device firmware architecture, see the figure below.

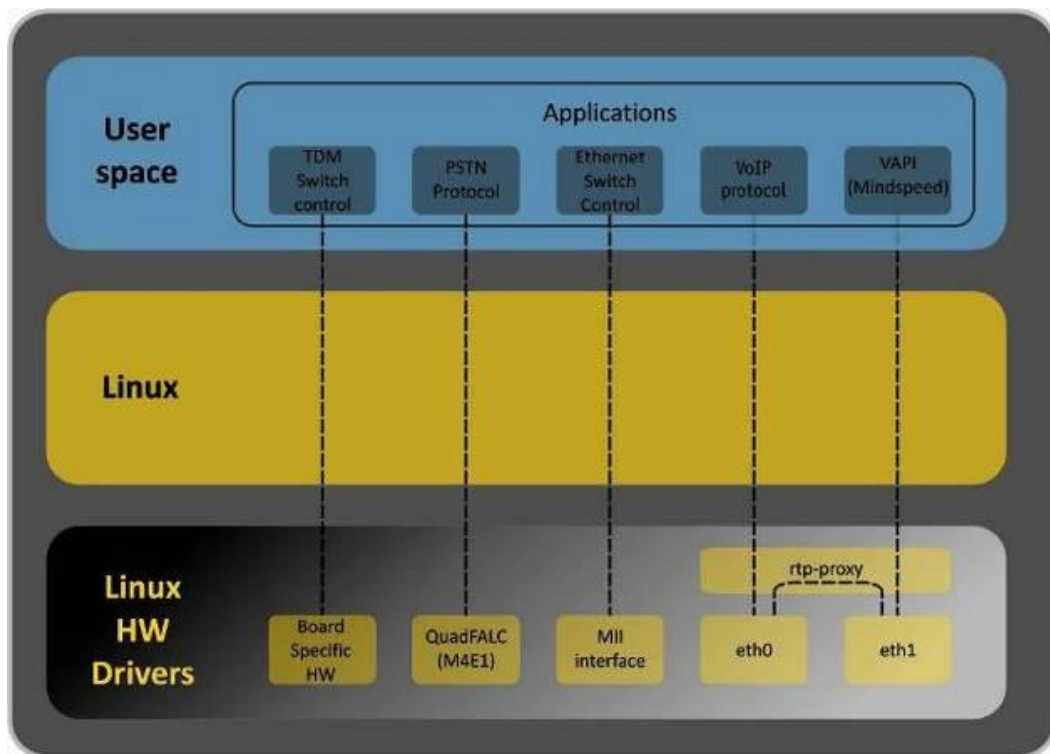


Figure 12 — SMG firmware architecture

3.2.4 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 MGCP ¹ MEGACO ¹ SIGTRAN (M2UA, IUA) ¹ SIGTRAN (M3UA) ¹ H.323v2/v3/v4 ² T.38
---------------------	--

Audio Codecs

Codecs	G.711 a-law (hereinafter G.711A) G.711 μ -law (hereinafter G.711U) G.729 A/B G.723.1 (6.3 Kbps; 5.3 Kbps) G.726 (32 Kbps)
--------	---

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

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

Electrical Ethernet interface specifications

No. of interfaces	SMG-1016M	SMG-2016, SMG-3016
	3	4
Electric port	RJ-45	
Data rate	Auto-detection, 10/100/1000 Mbps duplex	
Supported standards	10/100/1000BASE-T	

Optical Ethernet interface specifications

No. of interfaces	SMG-1016M	SMG-2016, SMG-3016
	2	2 combo ports
Optical port	Mini-Gbic (SFP): 1) duplex, double fiber, wave length 1310 nm (Single-Mode), 1000BASE-LX (LC connector), distance — up to 10 km, supply voltage — 3.3 V 2) duplex, single fiber, reception/transmission wave lengths 1310/1550 nm, 1000BASE-LX (SC connector), distance — up to 10 km, supply voltage — 3.3 V	

¹ Not supported in the current firmware version.

² Optionally.

Data rate	1000 Mbps, duplex
Supported standards	1000BASE-X

Console Parameters

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

E1 Interface Parameters

No. of channels	According to ITU-T G.703,G.704 guidelines
Line data transfer rate	2048 kbps
Line code	HDB3, AMI
Line output signal	3.0 V peak for 120 Ω load 2.37 V peak for 75 Ω load (acc. to CCITT G.703 guidelines)
Input signal from the line	From 0 to -6 dB in relation to the standard output impulse
Elastic buffer	2 frame capacity
Signalling protocols	DSS1/EDSS1 (ISDN PRI Q.931), QSIG and CORNET for subscriber name transmission, SS7, V5.2

Redundancy

Master-Slave redundancy	For SMG-2016 and SMG-3016 only
E1 redundancy	For SMG-2016 and SMG-3016 only

Number of conference participants

SMG-1016	The maximum number of participants for all conferences is 40. There can be no more than 40 participants in one conference. Example: 1 conference of 40 participants; 10 conferences of 4 participants, etc.
SMG-2016	The maximum number of participants for all conferences is 160. There can be no more than 40 participants in one conference. Example: 4 conferences of 40 participants each; 10 conferences of 16 participants each, etc.
SMG-3016	The maximum number of participants for all conferences is 160. There can be no more than 40 participants in one conference. Example: 4 conferences of 40 participants each; 10 conferences of 16 participants each, etc.

Supported file systems for external media

Device	Disk partitions	File systems
SMG-1016	MBR	USB flash – NTFS, FAT32, ext2, ext3, ext4 USB HDD – NTFS, ext2
	GPT	Not supported
SMG-2016	MBR	HDD – NTFS, ext2 USB flash – NTFS, FAT32, ext2, ext3, ext4 USB HDD – NTFS, ext2
	GPT	HDD – NTFS, ext2 USB flash – NTFS, FAT32, ext2, ext3, ext4 USB HDD – NTFS, ext2
SMG-3016	MBR	HDD – NTFS, ext2 USB flash – NTFS, FAT32, ext2, ext3, ext4 USB HDD – NTFS, ext2
	GPT	HDD – NTFS, ext2 USB flash – NTFS, FAT32, ext2, ext3, ext4 USB HDD – NTFS, ext2



The recommended file system for SATA drives is ext2.

Supported interfaces

Device	Interface
SMG-1016M/ SMG-2016	SATA2
SMG-3016	SATA3

External synchronization signal parameters

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

General parameters

Operating temperature range	From 0 to +40 °C		
Relative humidity	Up to 80 %		
Noise level	From 44 to 60 dB		
Power options	<ul style="list-style-type: none"> • Single AC or DC power supply • Two AC or DC hot-swappable power modules 		
Power supply	AC	DC	
	Supply voltage	100–240 V, 47–63 Hz	36–72 V
	PM designation	PM160-220/12	PM100-48/12
	PM rated power	160 W	100 W
Power consumption	No more than 50 W max.		
Dimensions (W × H × D)	SMG-1016M	SMG-2016, SMG-3016	
	430 × 45 × 260 mm	430 × 45 × 340 mm	
Form-factor	19" form-factor, 1U size		
Net weight	Complete device package	SMG-1016M	SMG-2016, SMG-3016
		3.2 kg	5.3 kg
	Power supply	0.5 kg	
	Vent panel	0.1 kg	
	SATA storage device ¹	0.1 kg	
Lifetime	No less than 15 years		

¹ For SMG-2016 and SMG-3016 only.

3.2.5 Design

3.2.5.1 SMG-1016M

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

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

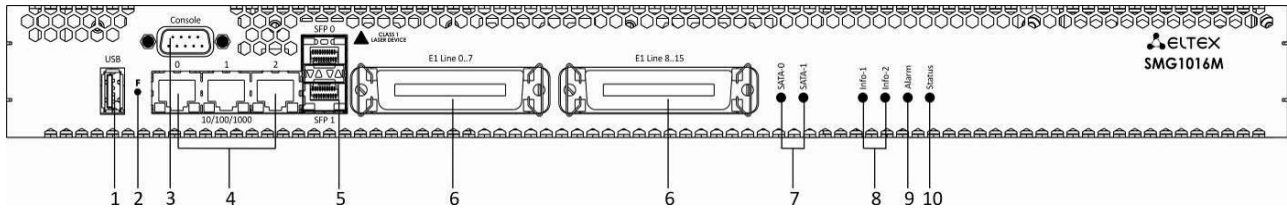


Figure 13 — SMG-1016M front panel layout

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

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

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

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

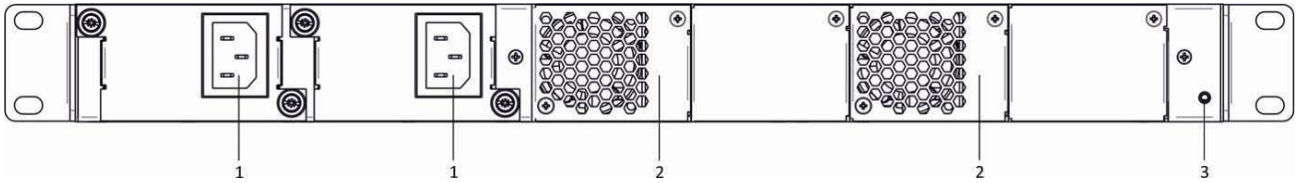



Figure 14 — SMG-1016M rear panel layout

The following table lists rear panel connectors of the switch.

Table 3 — Description of rear panel connectors of the switch

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

3.2.5.2 SMG-2016

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

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

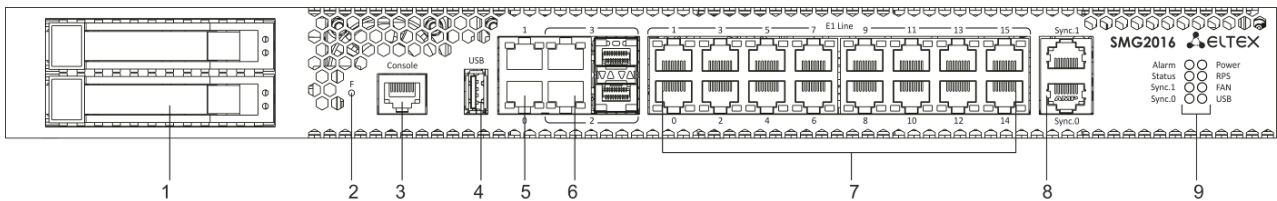


Figure 15 — SMG-2016 front panel layout

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	<i>SATA disk ports</i>	SATA drive trays
2	<i>F</i>	Function button
3	<i>Console</i>	Console port for local device management (see APPENDIXES (SMG) Appendix A. Cable contact pin assignment for connector wiring)
4	<i>USB</i>	USB port for external storage device connection
5	<i>0, 1</i>	2 x 10/100/1000BASE-T Gigabit uplink interface RJ-45 Ethernet connectors used for IP network connection
6	<i>2,3</i>	2 chassis for 1000BASE-X uplink interface SFP modules used for IP network connection

		2 × 10/100/1000BASE-T Gigabit uplink interface RJ-45 connectors used for IP network connection
7	<i>E1 Line 0..15</i>	16 × RJ-48 connectors for E1 streams connection (see APPENDIXES (SMG) Appendix A. Cable contact pin assignment for connector wiring)
8	<i>Sync.0, Sync.1</i>	2 × RJ-45 ports for connection of external synchronization sources
Indicators		
9	<i>Alarm</i>	Device alarm indicator
	<i>Status</i>	Device operation indicator
	<i>Sync.1</i>	<i>Sync.2</i> external synchronization interface operation indicator
	<i>Sync.0</i>	<i>Sync.1</i> external synchronization interface operation indicator
	<i>Power</i>	Device power indicator
	<i>RPS</i>	Device aux power indicator
	<i>FAN</i>	Fan operation indicator
	<i>USB</i>	USB operation indicator

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

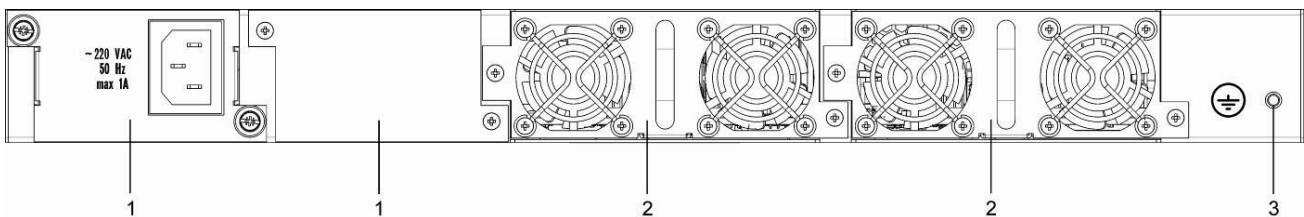



Figure 16 — SMG-2016 rear panel layout

The following table 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	Ground connection point 	Ground connection point of the device

3.2.5.3 SMG-3016

SMG-3016 digital gateway has a metal case available for 19" rack-mount 1U shelf installation. The front panel of the device is shown in the figure below.

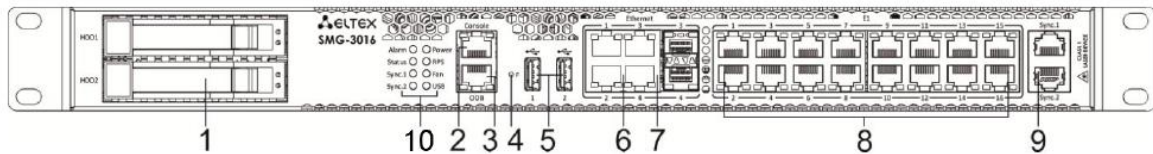


Figure 17 — SMG-3016 front panel layout

Connectors, LEDs and controls located on the front panel of the device are listed in Table 6.

Table 6 — Description of connectors, LEDs, and controls located on the front panel

No	Front panel elements	Description
1	<i>SATA disk ports</i>	SATA drive trays
2	<i>Console</i>	Console port for local device management (see APPENDIXES (SMG) Appendix A. Cable contact pin assignment for connector wiring)
3	<i>OOB</i>	Out-of-band Ethernet port for device configuration. The port does not have the ability to switch with other SMG ports
4	<i>F</i>	Function button
5	<i>USB</i>	USB port for external storage device connection
6	<i>1, 2</i>	2 × 10/100/1000BASE-T Gigabit uplink interface RJ-45 Ethernet connectors used for IP network connection
7	<i>3, 4</i>	2 chassis for 1000BASE-X uplink interface SFP modules used for IP network connection
		2 × 10/100/1000BASE-T Gigabit uplink interface RJ-45 connectors used for IP network connection
8	<i>E1 Line 0..15</i>	16 × RJ-48 connectors for E1 streams connection (see APPENDIXES (SMG) Appendix A. Cable contact pin assignment for connector wiring)
9	<i>Sync.1, Sync.2</i>	2 × RJ-45 ports for connection of external synchronization sources
Indicators		
10	<i>Alarm</i>	Device alarm indicator
	<i>Status</i>	Device operation indicator
	<i>Sync.1</i>	<i>Sync.2</i> external synchronization interface operation indicator
	<i>Sync.0</i>	<i>Sync.1</i> external synchronization interface operation indicator
	<i>Power</i>	Device power indicator
	<i>RPS</i>	Device aux power indicator
	<i>FAN</i>	Fan operation indicator
	<i>USB</i>	USB operation indicator

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

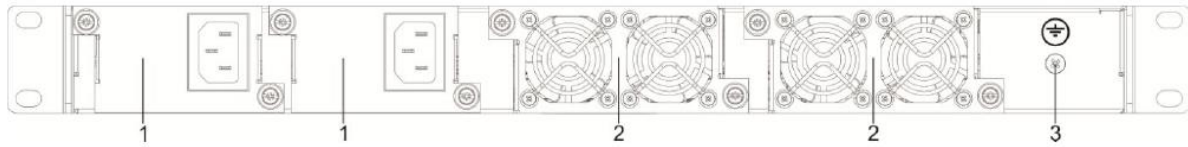



Figure 18 —SMG-3016 rear panel layout

The following table lists rear panel connectors of the switch.

Table 7 — 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	Ground connection point 	Ground connection point of the device

3.2.6 LED Indication

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

3.2.6.1 Device light indication in operation

3.2.6.1.1 SMG-1016M

For device light indication in operation, see the table below.

Table 8 — Light indication of the device status in operation

Indicator	Indicator State	Device State
<i>Info1</i>	Off	SFP0 link lost
	Solid green	SFP0 link in operation
<i>Info2</i>	Off	SFP1 link lost
	Solid green	SFP1 link in operation
	Solid red	Device is loading
<i>Alarm</i>	Flashes red	Critical device failure
	Solid red	Non-critical device failure
	Solid yellow	No failures, there are non-critical warnings
	Solid green	Normal operation
<i>Status</i>	Solid green	Normal operation
	Off	Device power lost

3.2.6.1.2 SMG-2016

For device light indication in operation, see the table below.

Table 9 — Light indication of the device in operation

Indicator	Indicator State	Device State
<i>Alarm</i>	Flashes red	Critical device failure
	Solid red	Non-critical device failure
	Solid yellow	No failures, there are non-critical warnings
	Solid green	Normal operation
<i>Status</i>	Solid green	Normal operation
	Off	Device power lost
<i>Sync.0, Sync.1</i>	Solid green	Synchronization from an external source is active, synchronization is being captured from the source
	Solid red	Synchronization from an external source is active, external source is not connected (no frequency in the range)
	Solid orange	Synchronization from an external source is not active, external source connected (frequency is in the range)
	Flashes orange	Frequency output mode
	Off	Synchronization from an external source is not active, not configured for frequency output, external source is not connected (no frequency in the range)
<i>Power</i>	Solid green	Power from Power supply no.0
	Solid orange	Power supply no.0 is installed, but not energized
<i>RPS</i>	Solid green	Power supply no.1 is installed and energized
	Solid red	Power supply no.1 is installed, but not energized
	Off	Power supply no.1 is not installed
<i>FAN</i>	Solid green	All removable fan modules are installed, all fans are operational
	Solid orange	All removable fan modules are installed, some fans are nonoperating
	Solid red	Single or both removable fan modules are not installed
<i>USB</i>	Solid green	USB flash is installed
	Off	USB flash is not installed

3.2.6.1.3 SMG-3016

For device light indication in operation, see the table below.

Table 10 — Light indication of the device in operation

Indicator	Indicator State	Device State
<i>Alarm</i>	Flashes red	Critical device failure
	Solid red	Non-critical device failure
	Solid yellow	No failures, there are non-critical warnings
	Solid green	Normal operation
<i>Status</i>	Solid green	Normal operation
	Off	Device power lost
<i>Sync.1, Sync.2</i>	Solid green	Synchronization from an external source is active, synchronization is being captured from the source
	Solid red	Synchronization from an external source is active, external source is not connected (no frequency in the range)
	Solid orange	Synchronization from an external source is not active, external source connected (frequency is in the range)
	Flashes orange	Frequency output mode
	Off	External synchronization source is not connected
<i>Power</i>	Solid green	Power from Power supply no.1
	Solid orange	Power supply no.1 is installed, but not energized
<i>RPS</i>	Solid green	Power supply no.2 is installed and energized
	Solid red	Power supply no.2 is installed, but not energized
	Off	Power supply no.2 is not installed
<i>FAN</i>	Solid green	All removable fan modules are installed, all fans are operational
	Solid orange	All removable fan modules are installed, some fans are nonoperating
	Solid red	Single or both removable fan modules are not installed
<i>USB</i>	Solid green	USB flash is installed
	Off	USB flash is not installed

3.2.6.2 LED indication of E1 stream status

For LED indication of E1¹ stream status, see the table below.

Table 11 — Indication of E1 stream status

RJ-48 ports	Indication (flashing period)		
	Red	Yellow	Green
Status	Red	Yellow	Green
E1 is disabled in the gateway configuration	Off	Off	Off
E1 stream failure state	Flashes (200 ms)	Off	Off
Loss of signal (LoS)	On	Off	Off
AIS failure	On	Flashes (200 ms)	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 (200 ms)	Flashes (200 ms)
E1 stream is in operation, there are SLIPs in the stream	Off	Flashes (300 ms)	Flashes (1500 ms)
E1 stream test is being performed	Flashes (200 ms)	Flashes (200 ms)	Flashes (200 ms)

¹ For SMG-2016 and SMG-3016 only.

3.2.6.3 Light indication of Ethernet 1000/100 interfaces

The status of the Ethernet interfaces is indicated by LED indicators built into the 1000/100 connector and is shown in the table below.

Table 12 — Light indication of Ethernet 1000/100 interfaces

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

3.2.6.4 Light indication during startup and reset to factory defaults

3.2.6.4.1 SMG-1016M

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

Table 13 — Light indication during startup and reset to factory defaults

Item	Indication				Reset to factory defaults procedure (device is on)
	Info1	Info2	Alarm	Status	
1	Yellow	Yellow	Yellow	Yellow	Press and hold F button for 1 second until the following pattern appears, then release the button. The device will be rebooted in 3 seconds.
2	Green	Red	Yellow	Red	Reset to factory defaults has been initiated. This LED pattern will appear only when the device startup begins.
3	Yellow	Yellow	Yellow	Yellow	At this step, LED functionality check will be performed — all LEDs will turn on yellow including SATA-0 and SATA-1.
4	Off	Off	Green	Green	At this step, the gateway operating system will be loaded. To change network parameters and restore the device configuration to factory defaults, when the pattern appears press and hold F button for 40–45 seconds. (When you press and hold the button, pattern 2 may appear shortly; ignore it and continue holding the button until the pattern 4 appears.)
5	Yellow	Yellow	Yellow	Yellow	When the pattern appears, release F button. After a while, the following message will be displayed in the console. <<<BOOTING IN SAFE-MODE.RESTORING DEFAULT PARAMETERS>>> Reset to factory settings is complete.



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



Also, the device can be reset to factory configuration during the device startup. In this case, skip the 1st step.

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

Table 14 — Light indication during startup and reset to factory defaults

Item	Indication				Reset to factory defaults procedure (device in operation)
	Alarm	Status	Sync.0	Sync.1	
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 configuration has been initiated. This LED pattern will appear only when the device startup begins.
3	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.
4	Yellow	Yellow	-	-	When the pattern appears, release F button. After a while, the following message will be displayed in the console. <pre><<<BOOTING IN SAFE- MODE . RESTORING DEFAULT PARAMETERS>>></pre> Reset to factory settings is complete.



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

Also, the device can be reset to factory configuration during the device startup. In this case, skip the 1st step.

3.2.6.5 Fault LED Indication

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



CDR file saving indication

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

Table 15 — Fault LED Indication

Alarm LED State	Fault level	Fault description
Flashes red	Critical	Configuration error
		SIP module loss
		SS7 link set fault (when ' <i>Fault indication</i> ' checkbox is selected in ' <i>Routing/SS7 linksets</i> ' menu)
		Stream fault (when ' <i>Alarm indication</i> ' checkbox is selected in ' <i>E1 streams/Physical parameters</i> ' menu)
		FTP server is unavailable, utilization of RAM for CDR file storage exceeds 50 %
Solid red	Non-critical errors	SS7 link fault (when ' <i>Fault indication</i> ' checkbox is selected in ' <i>Routing/SS7 linksets</i> ' menu)
		VoIP submodule (MSP) loss
		Synchronization fault (free-run mode operation)
		FTP server is unavailable, utilization of RAM for CDR file storage is more than 15 %
Solid yellow	Warnings	Remote stream fault
		Synchronization from the lower priority source (the one with the higher priority is not available)
		FTP server is unavailable, utilization of RAM for CDR file storage is more than 5 %
		CPS fault threshold is exceeded for one of the trunk groups
		INVITE duplication failure received from emergency call service node

3.2.7 'F' button operation

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

To perform reset to factory defaults on operating device, see section 3.2.6.4 Light indication during startup and reset to factory defaults: Table 13 and Table 14.

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, it is possible to save the factory configuration, restore password or reboot the device.

3.2.8 Saving factory configuration

To save the factory configuration:

- Reset the device to factory defaults (see section 3.2.6.4 Light indication during startup and reset to factory defaults);
- 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
```

3.2.9 Password recovery

3.2.9.1 CLI password recovery

To recover the password:

- Reset the device to factory defaults (see section 3.2.6.4 Light indication during startup and reset to factory defaults);
- 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
```

3.2.9.2 WEB password recovery

To recover the password:

- Reset the device to factory defaults (see section 3.2.6.4 Light indication during startup and reset to factory defaults);
- 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);
- Connect to the device web interface via the IP address 192.168.1.2;
- Go to the 'Users: Management' section;
- Change the password for 'admin' user;
- Enter **save** command in the console;
- Reboot the device using the **reboot** command.



It is not recommended to save the configuration from the web when recovering a password, because it may lead to the loss of the saved gateway configuration. Use the save command from shell mode.

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

If reboot without performing any actions, the device will be restored to the current configuration without password recovery. The gateway will boot with the current configuration and the 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
```

At this stage, the password is changed from web.

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

3.2.10 Delivery package

3.2.10.1 SMG-1016M

SMG-1016M standard delivery package includes:

- SMG-1016M digital gateway;
- 2 × CENC-36M connectors (if UTP CAT5E 18 pairs cable were not included in order);
- 4 × Latches for CENC-36M connectors (if UTP CAT5E 18 pairs cable were not included in order);
- RS-232 DB9(F)–DB9(F) connection cable;
- A mounting set for 19" rack;
- User manual on a CD disk (optional);
- Technical passport.

3.2.10.2 SMG-2016

SMG-2016 standard delivery package includes:

- SMG-2016 digital gateway;
- A mounting set for 19" rack;
- User manual on a CD disk (optional);
- Technical passport.

3.2.10.3 SMG-3016

SMG-3016 standard delivery package includes:

- SMG-3016 digital gateway;
- A mounting set for 19" rack;
- User manual on a CD disk (optional);
- Technical passport.

3.2.11 Safety instructions

3.2.11.1 General Guidelines

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



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

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

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

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

- Ambient temperature from 0 to +40 °C;
- Relative humidity up to 80 % at +25 °C;
- Atmosphere pressure from $6,0 \times 10^4$ to $10,7 \times 10^4$ Pa (from 450 to 800 mm Hg).

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

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

3.2.11.2 Electrical Safety Requirements

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

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

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

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

Installation and removal of submodules should only be carried out with the power off, following the section 3.2.12.4 Power module installation.

3.2.11.3 Electrostatic Discharge Safety Measures

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

3.2.11.4 Power Supply Requirements

3.2.11.4.1 Power supply type requirements

The device should be powered from 48 V DC power supply with grounded positive potential or from the remote 220 V AC power supply.

3.2.11.4.2 Permissible voltage variation requirements for DC power supply

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

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

3.2.11.4.3 Permissible interference requirements for DC power supply

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

Table 16 — Permissible interference requirements for DC power supply

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

3.2.11.4.4 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 the table below.

Table 17 — Requirements to interference produced by equipment in power supply circuit

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

3.2.11.4.5 AC power supply requirements

AC power supply parameters should be as follows:

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

3.2.12 SMG Installation

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

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

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

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

After installation, ground the device case. This should be done prior to connecting the device to the power supply. An insulated multiconductor wire should be used for grounding. The device grounding and the grounding wire section should comply with Electric Installation Code. The ground connection point is located at the right bottom corner of the rear panel, see Figure 14, Figure 16, Figure 18.

3.2.12.1 Startup sequence

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



To protect digital streams from extraneous voltages, the linear side of the cross-connect should be equipped with integrated protection devices. It is recommended 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 1 mm².
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.

3.2.12.2 Support brackets mounting

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

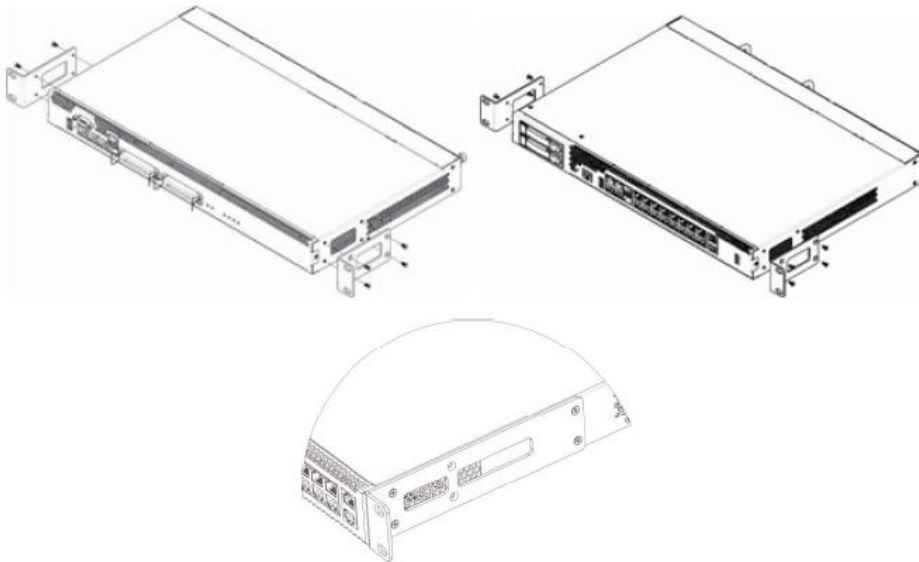


Figure 19 — Attaching support brackets for SMG-1016M (left top), SMG-2016 (right top) and SMG-3016 (bottom)

To attach the support brackets:

1. Align four mounting holes in the support bracket with the corresponding holes in the side panel of the device, Figure 19.
2. Use a screwdriver to screw the support bracket to the case.

Repeat steps 1 and 2 for the second support bracket.

3.2.12.3 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.

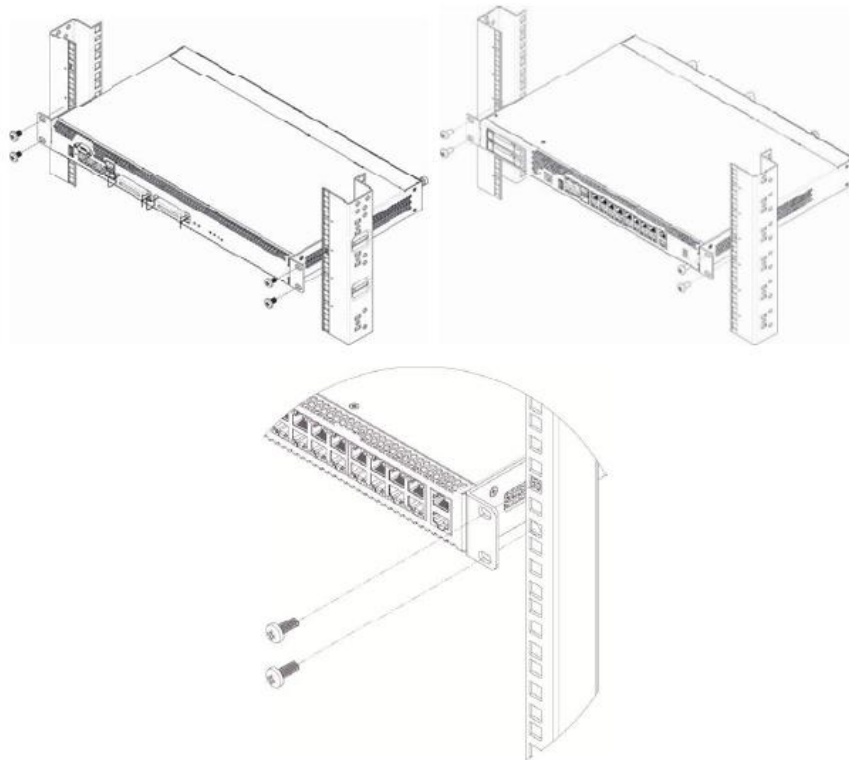


Figure 20 — Device rack installation for SMG-1016M (left), SMG-2016 (right) and SMG-3016 (bottom)

3.2.12.4 Power module installation

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

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

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

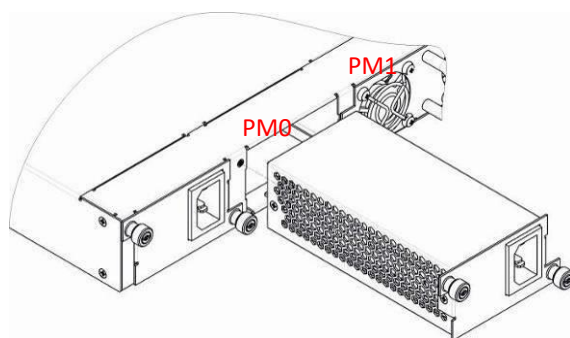


Figure 21— Power module installation

3.2.12.5 Removing the housing

First, disconnect SMG from the power supply, disconnect all the cables and remove the device from rack if necessary (see 3.2.12.3 Device rack installation).

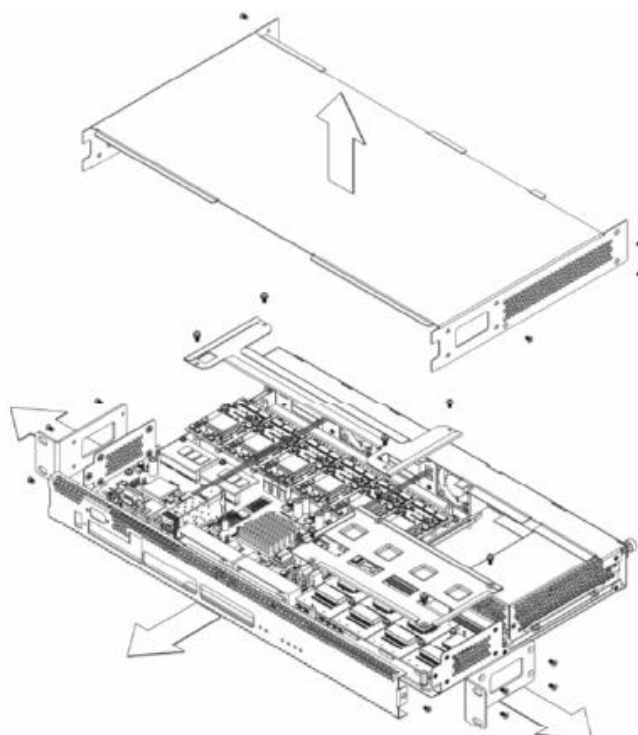


Figure 22 — SMG-1016M housing removal procedure

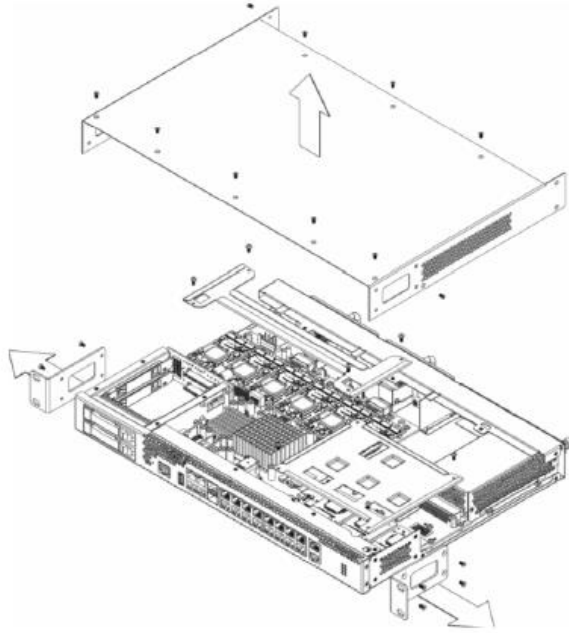


Figure 23 — SMG-2016 housing removal procedure

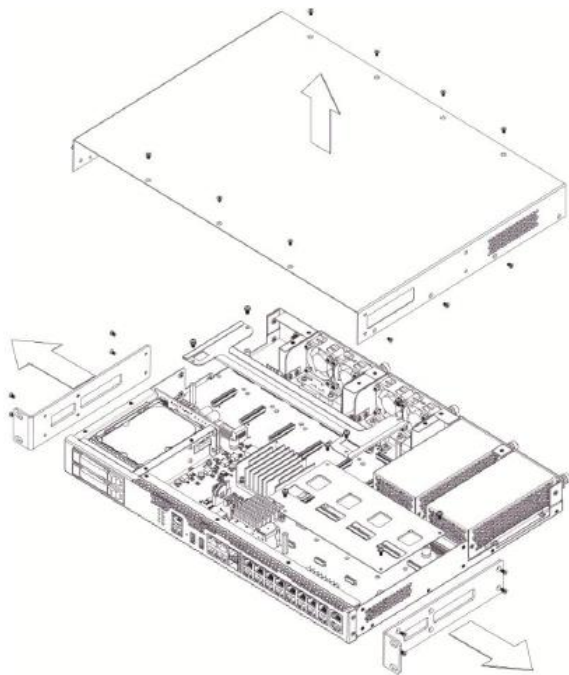


Figure 24 — SMG-3016 housing removal procedure

1. Use a screwdriver to remove support brackets from the device housing.
2. Only for **SMG-1016M**: it is necessary to untwist the fixing screws of the front panel, then pull it until it separates from the top and side panels (Figure 22).
3. Untwist the screws on the top panel.
4. Pull the top panel of the device to remove it.

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

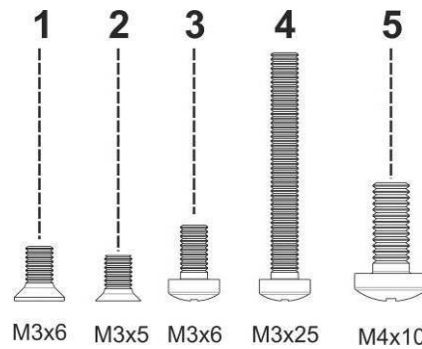


Figure 25 — Types of screws used for SMG assembly

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

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



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

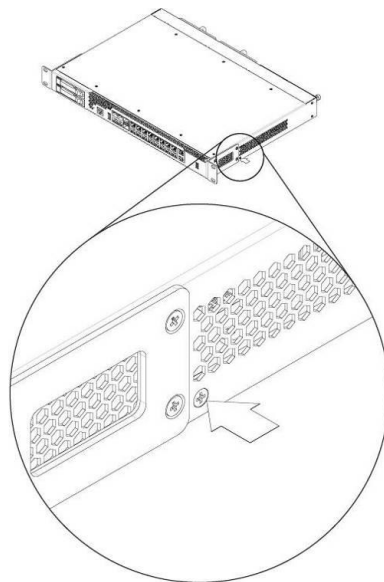


Figure 26 — SMG assembly into housing



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

3.2.12.6 Submodule Installation

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

The device requires at least one SM-VP-M300 module to operate. The required quantity of submodules for full operation of the device is calculated based on the required number of E1 streams, active VoIP channels (taking into account the codecs used) and the presence of SORM.

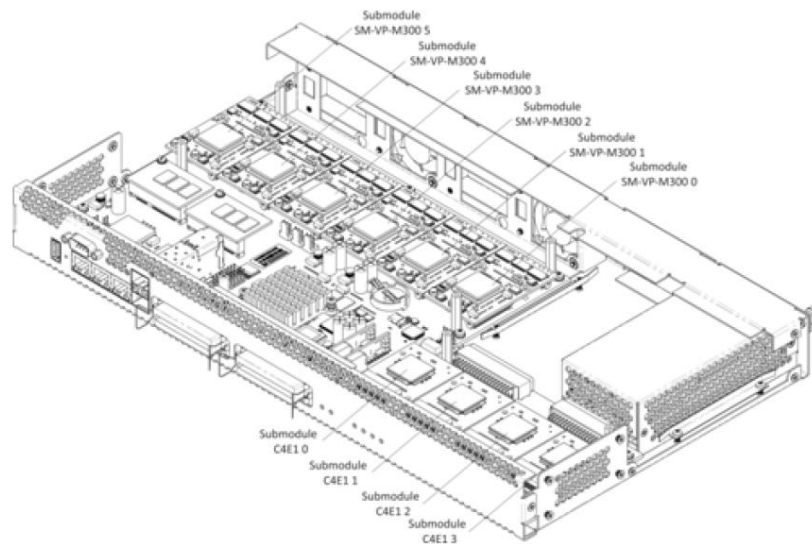


Figure 27 — SMG-1016M submodule location

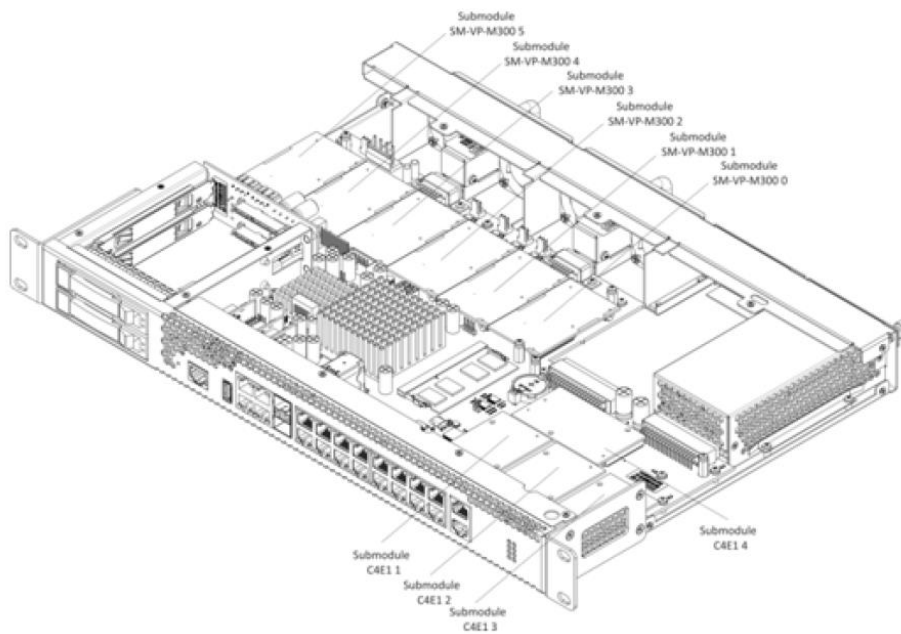


Figure 28 — SMG-2016M submodule location

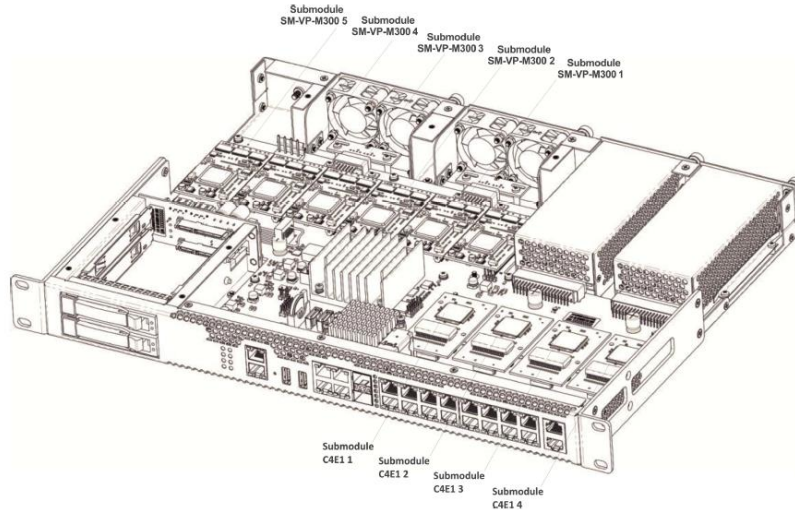


Figure 29 — SMG-3016M submodule location

SMG submodule installation order:

1. Check if the device is powered on.
2. If the voltage is present, disconnect the power supply.
3. Remove the device from the rack if necessary (see section 3.2.12.3 Device rack installation).
4. Remove the device housing (see section 3.2.12.5 Removing the housing).
5. In some hardware revisions, submodules are covered with specially shaped plates to prevent submodules from falling out during transportation (see section 3.2.12.5, Figure 22, Figure 23, Figure 24). In this case, the plate should be removed.
7. Install the module into the empty position (see Figure 27,
8. Figure 28, Figure 29).
 - 8.1 Install washers on the board, install brass standoffs on them.
 - 8.2 Install the submodule onto the brass standoffs, making sure that the connectors are tightly connected to the submodule
 - 8.3 Fix the module using the screws.

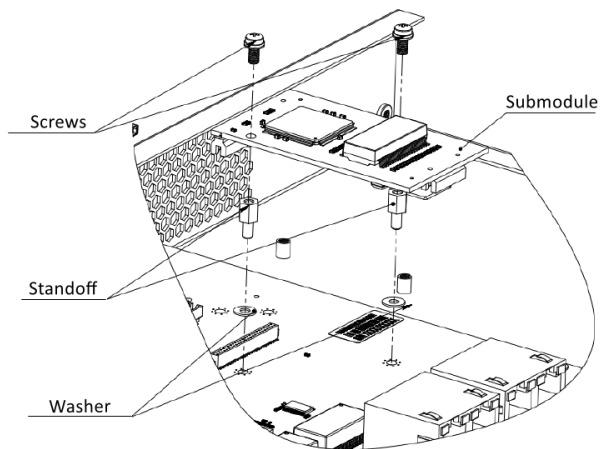


Figure 30 — Submodule installation on the board

- 8.4 Install the module on the board, making sure that the connectors are tightly connected to the submodule.
- 8.5 Secure the submodule using sealant to fix the submodule on the board.

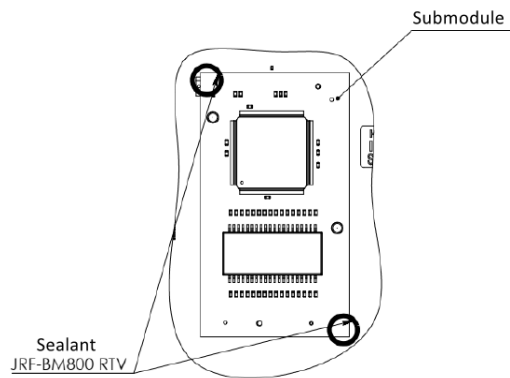


Figure 31 — Submodule installation on the board

9. For the positions of C4E1 submodules, the following correspondence is established with the numbers of E1 streams:

For SMG-1016M

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

For SMG-2016

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

For SMG-3016

- Submodule C4E1 1 — E1 Stream 1-4
- Submodule C4E1 2 — E1 Stream 5-8
- Submodule C4E1 3 — E1 Stream 9-12
- Submodule C4E1 4 — E1 Stream 13-16

10. Remount the restrictor plates above the submodules (if any), assemble the housing, install the device into the rack (if required).

3.2.12.7 Installation of ventilation units

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

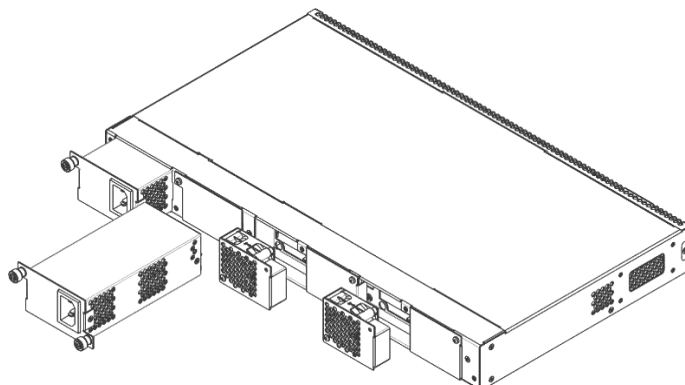


Figure 32 — SMG-1016M ventilation unit. Installation into case

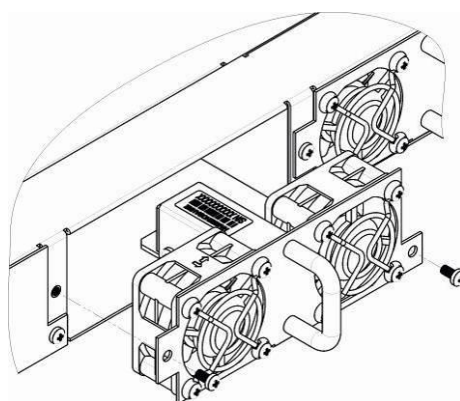


Figure 33 — SMG-2016 ventilation unit. Installation into case

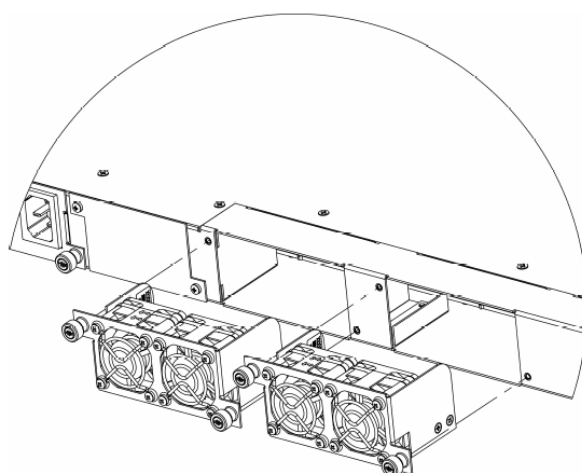


Figure 34 — SMG-2016 rev.B. ventilation unit. Installation into case

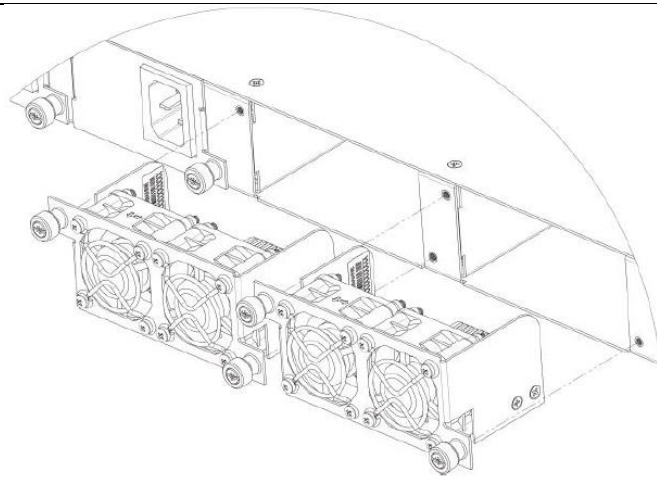


Figure 35 — SMG-3016 ventilation unit. Installation into case

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, Figure 36.

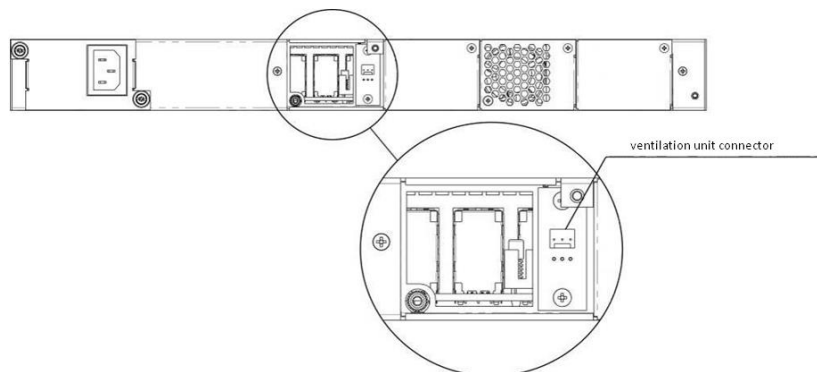


Figure 36 — SMG-1016M ventilation unit connector

To install a ventilation unit, perform the following actions:

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

3.2.12.8 SSD installation for SMG-1016M

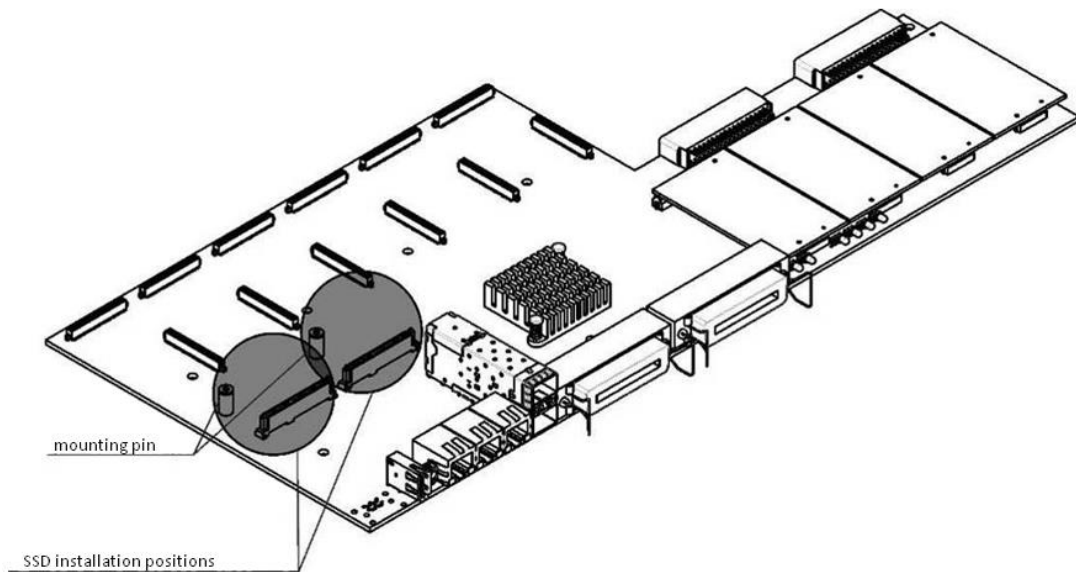


Figure 37 — SSD installation procedure

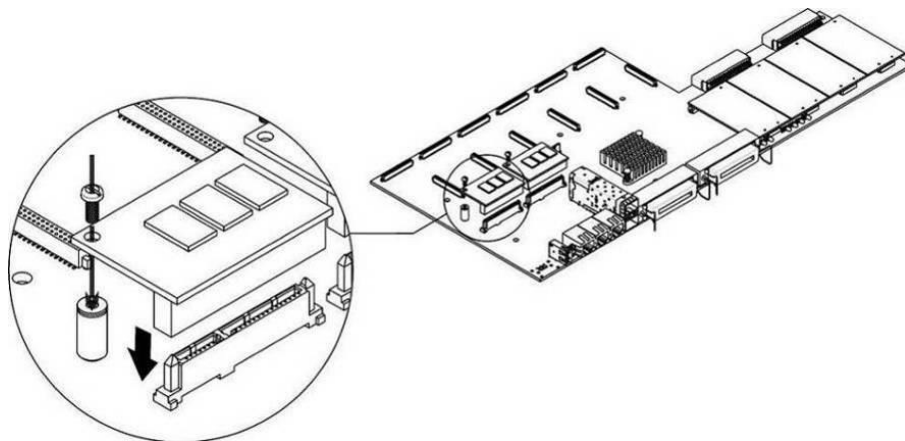


Figure 38 — SSD mounting procedure

1. Check if the device is powered on.
2. If the voltage is present, disconnect the power supply.
3. Remove the device from rack if necessary (see section 3.2.12.3).
4. Remove the device housing (see section 3.2.12.5).
5. If there is no mounting pin (see Figure 37) on 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 Figure 37), and if there is a mounting pin on the board, fasten the drive with a screw (see Figure 38).



To remove the SSD, repeat all mentioned steps in the reverse order.

3.2.12.9 SATA drive installation for SMG-2016, SMG-3016

SATA drives may be additionally included in the device delivery package. Connection slot is designed for 2.5" drives with a thickness of up to 12.5 mm".

Installation of SATA drives:

1. Remove the drive tray from the device housing (Figure 15, Figure 17 Element 1). To do this, press the button on the right until the ejector knob is released, pull the knob to remove the drive tray from the housing.
2. Remove the mounting kit located under the ejector knob, Figure 39.
3. Fix the drive in the tray, Figure 40.
4. Insert the tray with the SATA drive installed back into slot and push the ejector knob until it fits with a click, Figure 41.

To remove the SATA drive, repeat all mentioned steps in the reverse order.

SATA drives can be installed/removed when the device is powered on.

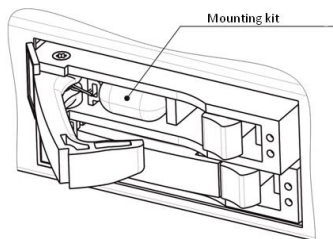


Figure 39 — Mounting kit location

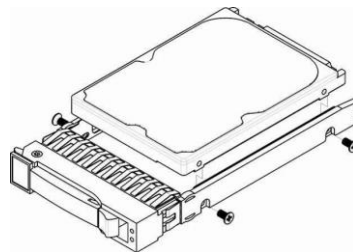


Figure 40 — Mounting SATA drive into drive tray

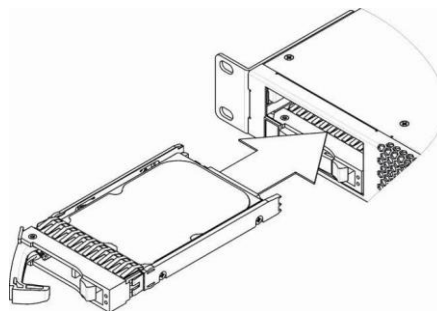


Figure 41 — Installation of SATA drive into device case

3.2.12.10 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 has a battery which specifications are listed in the table below.

Table 18 — RTC battery specifications

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

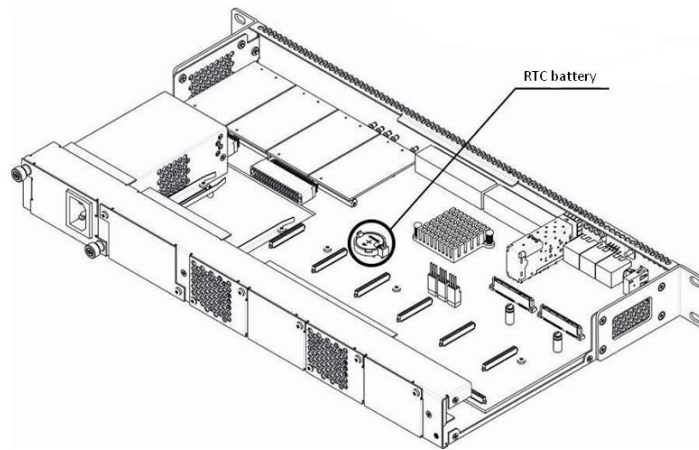


Figure 42 — RTC battery location for SMG-1016M

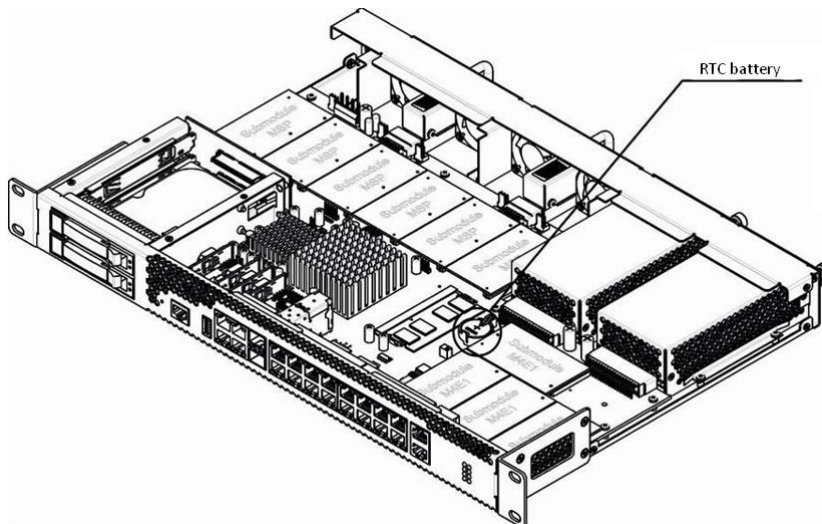


Figure 43 — RTC battery location for SMG-2016

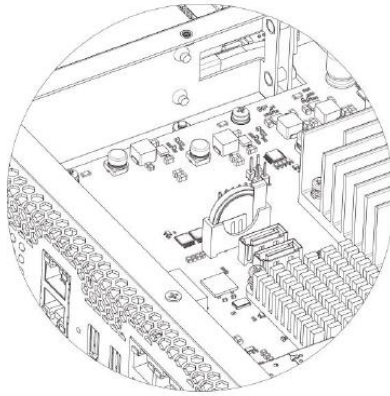


Figure 44 — RTC battery location for SMG-3016

If the battery lifetime 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 powered on.
2. If the voltage is present, disconnect the power supply.
3. Remove the device from rack if necessary (see section 3.2.12.3).
4. Remove the device housing (see section 3.2.12.5).
5. Remove used battery (Figure 42, Figure 43, Figure 44) 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, set the system date and time after RTC battery replacement.



Used batteries should be recycled accordingly.

3.3 General Switch Operation Guidelines

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

In order to prevent an unauthorized access to the device, it is recommended to change 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 0 Changing password for CLI access to device. For setting password for web configurator access, see Section Setting password for web configurator access. It is recommended 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 configuration, it is recommended to make configuration backup copies and store them on a PC each time significant changes are made.



To ensure the device safety, follow the recommendations described in Appendix M. Safety Recommendations.

4 DEVICE CONFIGURATION

Connect to the device using the following methods: via web configurator, via Telnet/SSH protocols, or using RS-232 cable (CLI is used 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.

4.1 SMG configuration via web configurator



The interface appearance may vary.

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



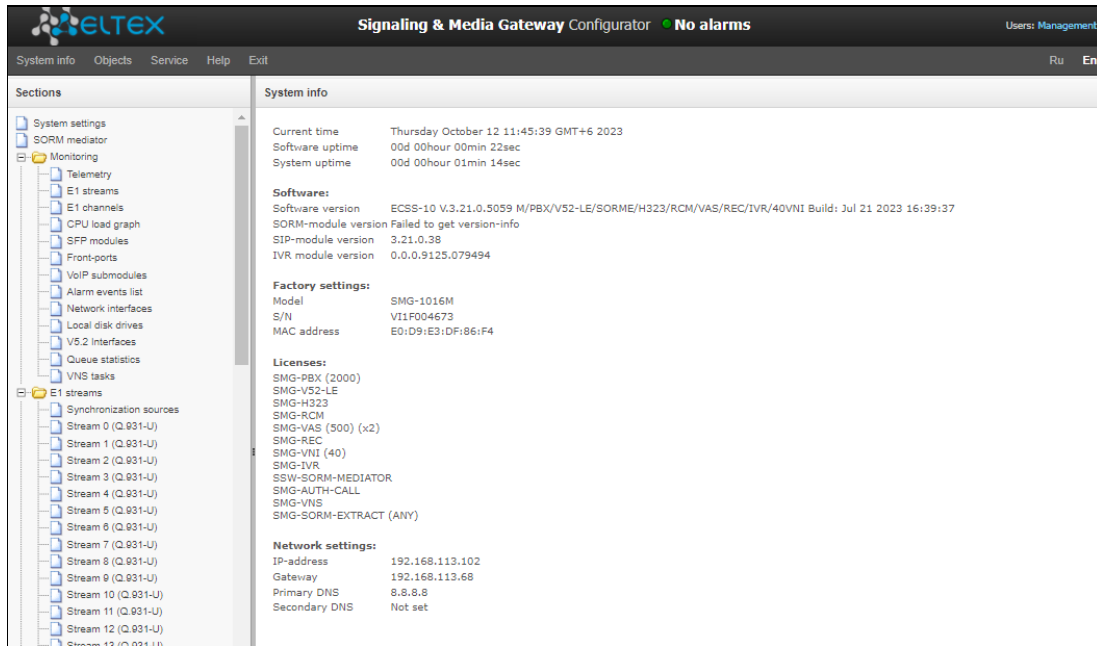
Factory IP address of the SMG device: *192.168.1.2*, network mask: *255.255.255.0*.

Upon entering IP address, the device will request username and password. it is also possible to choose the language that will be used in the interface.

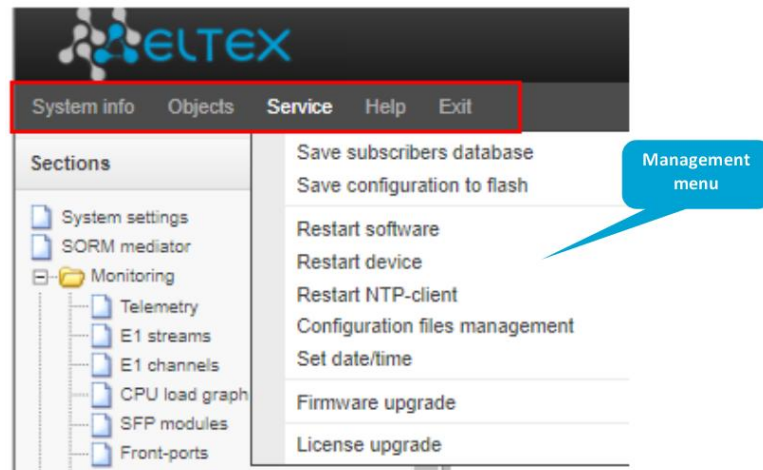


Initial startup username: ***admin***, password: ***rootpasswd***.

When web configurator access is established, the 'System information' page will be displayed.



The figure below shows web configurator navigation elements.



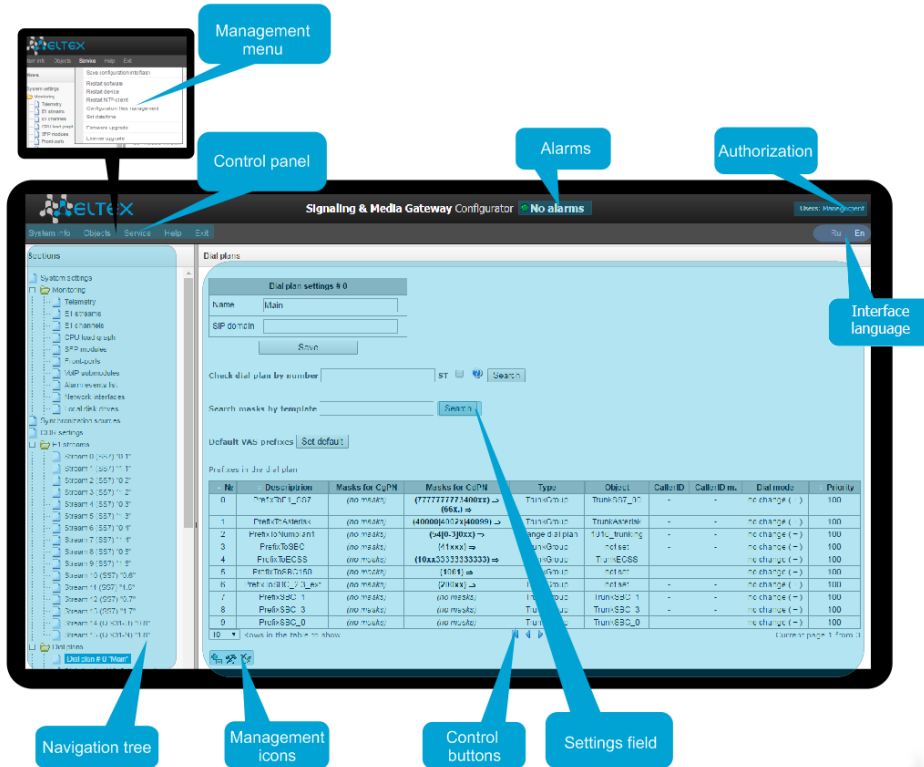







Figure 45 — Web configurator navigation elements

The user interface is divided into several areas.

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


To prevent unauthorized access to device in the future, it is recommended to change password (see 4.1.27 Setting password for web configurator access).



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

4.1.1 System settings

System settings → Basic settings

System settings						
System settings						
Device name	SMG1016M					
Backup unsaved changes 	<input type="checkbox"/>					
Local disk drive for traces	default					
Active dial plan count	1					
Numbering plan wait for applying	<input type="checkbox"/>					
Local disk drive for alarm logging	not set					
SM-VP submodules usage	0	1	2	3	4	5
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- *Device name* — name of the device. This name is used in the device web configurator header;
- *Backup unsaved changes* — if checked, the device creates a backup copy of unsaved configuration changes every 60 seconds for further recovery. For example, there were unsaved changes on the device and the power restarted. If the option was enabled after the device started, the window will be displayed in the web interface asking you to restore unsaved changes;
- *Local disk drive for traces* — the debugging information (traces) can be saved on the device in random access memory (RAM) or on the installed drive:
 - default — debug information is stored in RAM;
 - /mnt/sdX — path to local storage device; setting is displayed when the storage device is installed. When the drive is selected, a logs directory will be created on it, which will contain trace files.
- *Active dial plan count* — quantity of simultaneously active dial plans; up to 16 (up to 255 on SMG-2016 and SMG-3016 if there is a VAS license) independent dial plans can be configured with an ability to add subscribers and create custom call routing table;
- *Numbering plan wait for applying* — if checked, SMG will not apply changes in the numbering plan without confirming. Setting this option helps to operate with long dial plans. It allows avoiding long processing of dial plans after every setting change;
- *Local disk drive for alarm logging* — select the drive used for critical alarm message storage into non-volatile memory. This option may be necessary when finding out the reasons for restarting or equipment failure:
 - /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:

1. 24/09/13 20:03:22. Software started.
2. 24/09/13 20:03:22. state ALARM. Sync from local source, but sync source table not empty
3. 24/09/13 20:03:22. state OK. PowerModule#1. Unit ok! or absent
4. 24/09/13 20:03:31. state OK. MSP-module lost: 1
5. 24/09/13 20:03:34. state OK. MSP-module lost: 2
6. 24/09/13 20:03:38. state OK. MSP-module lost: 3
7. 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 19 — Alarm message examples

Alarm message	Meaning
Configuration error	Configuration file error
SIP module lost	Failure of a software module responsible for VoIP operation
Linkset down	SS7 link set failure
E1 stream alarm	E1 stream failure
SS7 link alarm	SS7 signal channel failure
Synchronization from a lower priority source	Primary synchronization source is lost, current source has lower priority
E1-Line Remote-alarm	E1 stream remote fault
FTP error. CDR-send failed	Failed to send CDR file to remote storage
Software started	Device software startup

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

Alarm Indication

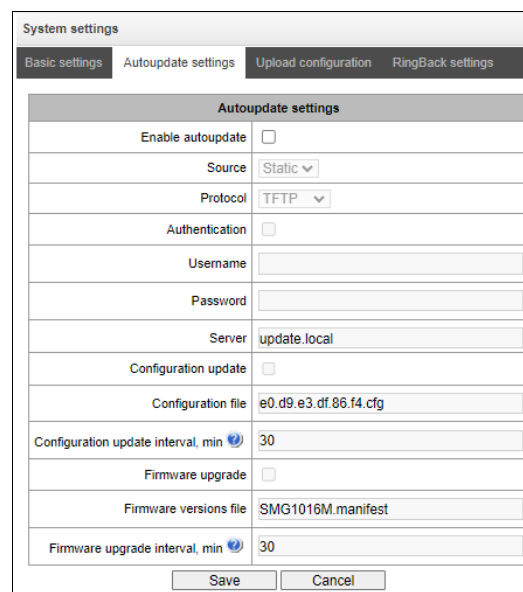
Alarm indication	
Fans operation	<input checked="" type="checkbox"/>
CPU load	<input checked="" type="checkbox"/>
RAM usage	<input checked="" type="checkbox"/>
Local disk drive free space	<input checked="" type="checkbox"/>
Alarms from slave device	<input checked="" type="checkbox"/>
Slave device connection	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

- *Local disk drive free space* — when checked, fault indication will appear, if the utilization of a single external storage device with capacity less than 5GB exceeds 80% (or there is less than 1024MB of free space on an external storage device with capacity exceeding 5GB) (ALARM LED will light up, alarm will be added to alarm log).
 - *Alarms from slave device* — when checked, the main device will receive alarms of the backup device;
 - *Slave device connection* — when checked, in the absence of communication with the slave on a global or local link, there will be an indication of an accident (the device will light up ALARM indicator, the accident will be recorded in the accident log).

Autoupdate settings

System settings → Autoupdate settings



SMG can automatically receive configuration and software version files from the auto-configuration server (hereinafter referred to as the “server”) with a specified period.

After downloading the configuration, SMG will wait for all active calls to end, after which will apply the new configuration or before a reboot.

Firmware version description file contains information about firmware versions on the server: versions and file names. In this file, the time to update can be also set. The file format should be as follows:

<Firmware version>;<Firmware file name>;<Permitted update time, hour>

- Firmware version is specified completely up to the assembly version;
- Firmware file name should have .bin extension;
- The permitted update time can be unspecified. In this case, SMG will be updated in the near future, when there are no active calls. If a time interval is specified, then SMG will be updated only at the specified time interval.

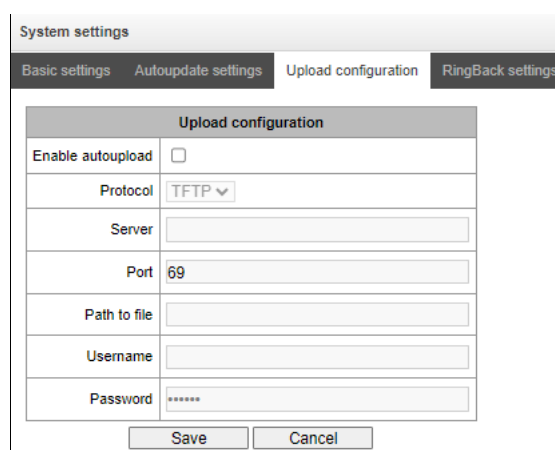
Example of firmware description file:

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

- *Enable autoupdate* — enable automatic firmware and configuration update;
- *Source* — server information source;
 - *Static* — information about server is written and saved on SMG;
 - *DHCP (interface name)* — server information will be received on the selected interface via DHCP protocol from option 66, information about the firmware file name and the configuration file name is obtained via option 67;
- *Protocol* — protocol for connecting to the server;
- *Authentication* — use authentication to get access to the server (for FTP, HTTP, HTTPS);
- *Username* — name (login) for access to the server;
- *Password* — password for access to the server;
- *Server* — IP address or domain name of server. Available if Static Sourcy is selected;
- *Configuration update* — allows configuration update from server;
- *Configuration file* — configuration file name. The name should have .cfg extension and contains up to 64 symbols;
- *Configuration update interval, min* — frequency of server validation for configuration update;
- *Firmware upgrade* — enable firmware upgrade from server;
- *Firmware versions file* — file name with firmware versions. The name should have .manifest extension and contains up to 64 symbols.
- *Firmware upgrade interval, min* — frequency of server validation for firmware upgrade.

Upload configuration

System settings → Upload configuration



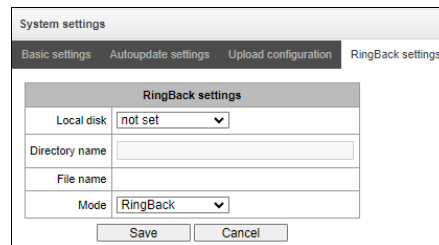
SMG can upload a configuration to FTP/TFTP/SCP-server automatically each time it is saved to non-volatile memory.

- *Enable autoupload* — enable the function of automatic configuration upload;
- *Protocol* — select a protocol for uploading. FTP, TFTP, SCP are supported;
- *Server* — IP address of the server for uploading the configuration;
- *Port* — port of the server through which the uploading will be implemented;
- *Path to file* — directory located on the server where the configuration will be stored;

- *Username* — name for authentication in case of FTP using;
- *Password* — password for authentication in case of FTP using.

Ringback settings

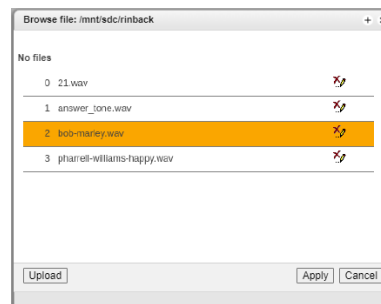
System settings → *Ringback settings*



RingBack settings allow replacing the standard ringing sound with any other one, similarly operation of the “Replace the horn” service.

- *Local disk* — path to the external drive where audio files will be stored;
- *Directory name* — the name of the folder on the external drive where the audio files are stored;
- *File name* — desired file to play;
- *Mode* — operation mode:
 - *RingBack* — standard ringback sound;
 - *Audio file* — a special file selected as audio for RBT.

System settings → *RingBack settings* → *Browse*



- *Upload* — uploading an audio file of a specific format;



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

- *Apply* — selecting the desired audio file;
- *Cancel* — exit from the ‘Browse’ submenu.

When setting up RBT from the ‘System parameters’ item, the audio file is applied to all subscribers and system trunk groups.

There are several levels of settings, each next “more detailed” level has priority over previous:

1. RBT system settings
2. RBT settings for Trunk groups and PBX profiles
3. RBT settings for subscribers

4.1.2 Monitoring

Monitoring → Telemetry

Telemetry	
Temperature sensors:	
CPU temperature	48.000 °C
RAM temperature	38.000 °C
Power supply:	
Power module #0	Installed and powered
Power module #1	Not installed
Fans:	
Fan #0	4620 rpm
Fan #1	4680 rpm
Fan #2	4620 rpm
Fan #3	4680 rpm
Current voltage :	
+12.0 V	12.399 V
+5.0 V	5.132 V
+3.3 V	3.340 V
+2.5 V	2.400 V
+1.8 V	1.782 V
+1.5 V	1.540 V
+1.2 V	1.254 V
+1.0 V	1.018 V
CPU	1.138 V
CPU Vcore	0.938 V
RTC battery	3.168 V
CPU load:	
0.6%	usr
1.0%	sys
0.0%	nic
98.3%	idle
0.0%	io
0.0%	irq
0.0%	sirq

4.1.2.1 Telemetry

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

Temperature sensors

For SMG-1016M:

- *Sensor #0* — CPU temperature;
- *Sensor #1* — RAM module temperature.

For SMG-2016, SMG-3016:

- *Sensor #0* — CPU temperature.

Power supply

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

Possible power supply states:

- *Installed* — power supply is installed;
- *Not installed* — power supply is not installed;
- *In operation* — power supply is energized;
- *Not in operation* — power supply is de-energized.

Fans¹

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

Voltage (for SMG-1016M only)

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

Current voltage (for SMG-2016 and SMG-3016 only)

- *+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 SMG-1016M has 2 fans installed, SMG-2016 and SMG-3016 have 4 fans installed.

- *+1.2V* — 1.2V voltage sensor status details;
- *+1.0V* — 1V voltage sensor status details;
- *CPU* — CPU voltage status details;
- *CPU Vcore* — CPU core voltage status details;
- *RTC battery* — real-time clock battery voltage status details.

CPU load:

- *USR* — percentage of CPU time utilization by user applications;
- *SYS* — percentage of CPU time utilization by core processes;
- *NIC* — percentage of CPU time utilization by applications with modified priority;
- *IDLE* — percentage of unused CPU resources;
- *IO* — percentage of CPU time spent on I/O operations;
- *IRQ* — percentage of CPU time spent on hardware interruptions' processing;
- *SIRQ* — percentage of CPU time spent on software interruptions' processing.

4.1.2.2 E1 streams

The section displays information about installed chips on C4E1 submodules, as well as E1 stream monitoring and statistics.

Monitoring → E1 streams

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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
D-channel state	off	off	off	off	off	off	off	off	off	off	off	off	off	off	off	off
Statistics collection time, sec	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Slip up	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Slip down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RX bytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TX bytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Short packets	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Big packets	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RX Overflow	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CRC errors	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TX underrun	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Code violation counter	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Select <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

For E1 chips, the table indicates the position number in which it is installed (see 3.2.12.6 Submodule 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 ONES);
 - *LOMF* — multi-frame alarm state indication signal;
 - *RAI* — remote alarm indication;
 - *TEST* — stream test indication (PRBS test, local or remote loop).
- *D-channel state* — state of D-channel, service management channel:
 - *UP* — D-channel is in operation;
 - *DOWN* — D-channel is not in operation;
 - *NO* — there is no management channel for the stream;
 - *OFF* — signalling is disabled for the stream;
 - *KPD1/KPD2 down* — KPD1/KPD2 is not in operation.
- *Statistics collection time, sec* — statistics collection period in seconds;
- *Slip up* — number of positive bit slips for the stream;
- *Slip down* — number of negative bit slips for the stream;
- *RX bytes* — number of bytes received from the stream;
- *TX bytes* — number of bytes sent to the stream;
- *Short packets* — number of packets received which size is less than standard;
- *Big packets* — number of packets received which size is bigger than standard;
- *RX Overflow* — buffer overrun error counter;
- *CRC errors* — CRC error counter;
- *TX underrun* — stream transmission failure counter;
- *Code violation counter* — signal code sequence failure counter;
- *CRC Error Counter / PRBS* — CRC error quantity (in 'PRBS test' mode);
- *Bit error rate* — number of bit errors for the stream.

The following buttons are below the table:

- *Reset counters* — when checked, click '*Reset*' button to reset the collected statistics for the selected stream;
- *Remote Loop* — E1 path test mode, where signal received from the connected E1 stream by the unit is transmitted into the same stream;
- *PRBS test* — enables pseudorandom sequence output to the output port of the unit (transmitted into the connected E1 stream); at that, error detection mode will be enabled at the unit input port (E1

stream reception) for this sequence in order to evaluate the signal transmission quality. Number of errors and analysis time counter will be displayed in the stream information window;

- *PRBS test with Local Loop* — E1 path test mode, where external line is disabled and the signal transferred by the unit is transmitted into the input of the same unit. Pseudorandom sequence output will be enabled to the unit output port; input port will operate in the error detection mode;
- *Stop test* — disable test mode.

4.1.2.3 E1 channel monitoring

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

Information tables

Connection information for stream # and channel #:

- *Port/channel* — this section is divided into two parts:
 - Signalling protocol (PRI/SS7);
 - Port location Stream #: Channel #.
- *Connected port/channel* — this section is divided into two parts:
 - Linked port signalling protocol (PRI/SS7/VoIP);
 - Linked port location Stream #: Channel # for PRI/SS7 or VoIP submodule #: VoIP channel #.
- *Connected Callref* — call identifier for linked channel;
- *State* — channel state:
 - *Off* — channel is disabled;
 - *Block* — port is blocked;
 - *Init* — channel initialization;
 - *Idle* — channel is in initial state;
 - *In-Dial/ Out-Dial* — incoming/outgoing call dialing;
 - *In-Call/ Out-Call* — incoming or outgoing occupation;
 - *In-Busy/ Out-Busy* — sending 'busy' tone;
 - *Talk* — channel is in call state;
 - *Release* — channel release;
 - *Wait-Ack* — waiting for acknowledgement;
 - *Wait-CID* — waiting for CgPN (Caller ID);
 - *Wait-Num* — waiting for call dialing;
 - *Hold* — subscriber is on hold.
- *State timer* — channel last known state duration;
- *Incoming SS7 category* — SS7 category of an incoming call before modification;
- *Incoming CdPN* — callee number before modification;
- *Incoming CgPN* — caller number before modification;

-
- *Outgoing SS7 category* — SS7 category of an incoming call after modification;
 - *Outgoing CdPN* — callee number after modification;
 - *Outgoing CgPN* — caller number after modification.

Stream state — information table with matrix symbol interpretations:

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

Channel state — information table with matrix symbol interpretations:

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

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

Channel state updates in 5 seconds interval.

Link management

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

E1 channels

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

Call information on channel #	Streams state	Channels state	Link management
Port/channel	✘ NONE	○ Off	Send LUN
Connected port/channel	○ OFF	○ Idle	Send LIN
Connected Callref	● ALARM	● Block	Send LFU
State	● LOS	☎ Incoming dialing	Set congestion state
State timer	● AIS	➡ Outgoing dialing	Clear congestion state
Incoming SS7 category	● LOF	☎ Incoming alerting	Set local processor outage
Incoming CdPN	● LOMF	☎ Outgoing alerting	Clear local processor outage
Incoming CgPN	● WORK/RAI	☎ Busy, Release	Invoke normal link restart
Outgoing SS7 category	● WORK/SLIP	☎ Talk	Invoke emergency link restart
Outgoing CdPN	● WORK	☎ Hold	Stop link
Outgoing CgPN	● TEST	⌚ Waiting	
		☎ 3way, Conference	
		☎ Service dialing	

SS7 link management — SS7 signal link management table:

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

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 11 in Stream 0 (SS7). Next, in 'SS7 channel management' table, select the field with the required action and left-click it. Pop-up informational message about the command execution will be shown on screen.



Group operations for channels in a stream can be performed. To do this, select the range of channels while holding <SHIFT> key.

E1 channels

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

Call information 0 on channel #11	Streams state	Channels state	SS7 channel management
Port/channel: SS7:0:11	<input checked="" type="checkbox"/> NONE	<input type="checkbox"/> Off	Block channel (send BLO)
Connected port/channel: -	<input type="checkbox"/> OFF	<input type="checkbox"/> Idle	Unblock channel (send UBL)
Connected Callref: -	<input checked="" type="checkbox"/> ALARM	<input checked="" type="checkbox"/> Block	Reset channel (send RSC)
State: Off	<input checked="" type="checkbox"/> LOS	<input checked="" type="checkbox"/> Incoming dialing	Local block
State timer: 0	<input checked="" type="checkbox"/> AIS	<input checked="" type="checkbox"/> Outgoing dialing	Local unblock
Incoming SS7 category: -	<input checked="" type="checkbox"/> LOF	<input checked="" type="checkbox"/> Incoming alerting	Release (send REL)
Incoming CdPN: -	<input checked="" type="checkbox"/> LOMF	<input checked="" type="checkbox"/> Outgoing alerting	Release complete (send RLC)
Incoming CgPN: -	<input type="checkbox"/> WORK/RAI	<input checked="" type="checkbox"/> Busy, Release	Run continuous-check test (send CCR)
Outgoing SS7 category: -	<input type="checkbox"/> WORK/SLIP	<input checked="" type="checkbox"/> Talk	Stop continuous-check test
Outgoing CdPN: -	<input checked="" type="checkbox"/> WORK	<input type="checkbox"/> Hold	Show continuous-check test state
Outgoing CgPN: -	<input checked="" type="checkbox"/> TEST	<input type="checkbox"/> Waiting	
<input type="button" value="Disconnect the call"/>		<input checked="" type="checkbox"/> 3way, Conference	

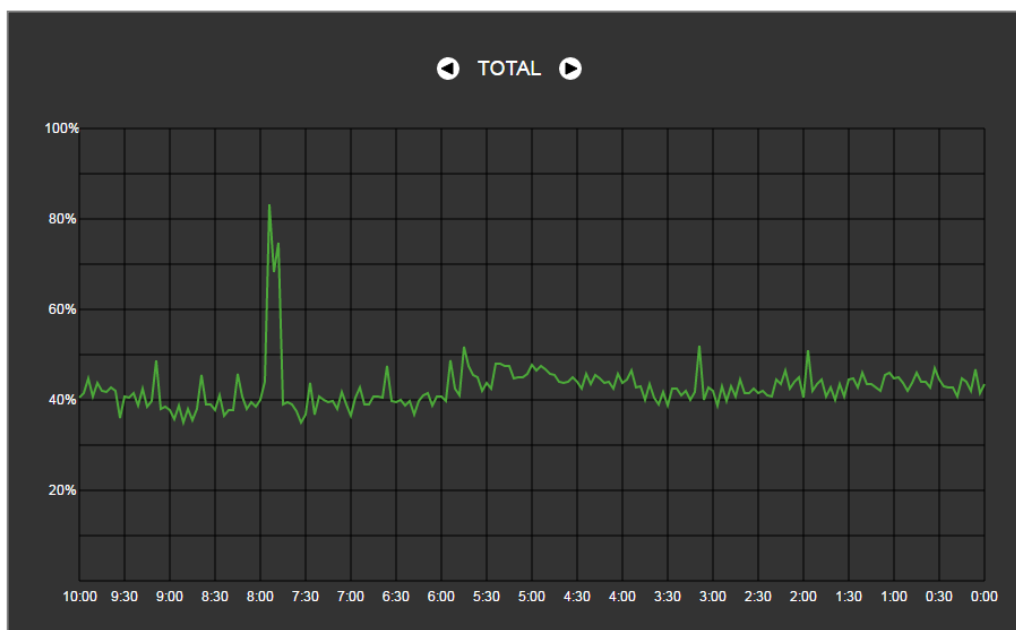
SS7 channel management — SS7 (CIC) channel management table:



- *Block channel (send BLO)* — send BLO message to block channel;
- *Unblock channel (send UBL)* — send UBL message to unblock channel;
- *Reset channel (send RSC)* — send RSC message;
- *Local block* — block channel locally without BLO message transmission;
- *Local unblock* — cancel local block;
- *Release (send REL)* — send REL message;
- *Release complete (send RLC)* — send RLC message;
- *Run continuous-check test (send CCR)* — Run continuous-check test by sending CCR message;
- *Stop continuous-check test* — stop channel continuity test;
- *Show continuous-check test state* — show current continuous-check test state.

4.1.2.4 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.

Monitoring → CPU load graph



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.

4.1.2.5 SFP module monitoring

This section contains status indication and optical line parameters.

Monitoring → SFP modules

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

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

4.1.2.6 Front ports monitoring

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

Monitoring → Front-ports

Front-ports					
	Port 0	Port 1	Port 2	SFP 0	SFP 1
Link	DOWN	UP	DOWN	DOWN	DOWN
Speed	N/A	1000M	N/A	N/A	N/A
Duplex	N/A	full-duplex	N/A	N/A	N/A
LACP group	-	-	-	-	-
LACP state	-	-	-	-	-
RX Bytes	0	19330730 (18.4 MiB)	0	0	0
errors packets	0	0	0	0	0
dropped packets	0	0	0	0	0
unicast packets	0	9892	0	0	0
broadcast packets	0	260023	0	0	0
TX Bytes	0	1707966 (1.6 MiB)	0	7511994 (7.2 MiB)	7511994 (7.2 MiB)
errors packets	0	0	0	0	0
unicast packets	0	9235	0	0	0
broadcast packets	0	88	0	117374	117374




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

4.1.2.7 VoIP submodule monitoring

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

Monitoring → VoIP submodules

VoIP submodules				
No	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 #	Call IP-info # submodule #	Channels state
Port/channel -	State -	 Idle
Callref -	Codec -	 Active
Connected port/channel -	Status -	 Reserved
Connected Callref -	Mode -	
State -	SSRC -	
State timer -	IP:port remote -	
Incoming SS7 category -	IP:port local -	
Incoming CdPN -	MAC remote -	
Incoming CgPN -	MAC local -	
Outgoing SS7 category -		
Outgoing CdPN -		
Outgoing CgPN -		

- *No* — SM-VP submodule sequential number;
- *Type* — installed submodule type;
- *State*:
 - *Not Present* — not installed;
 - *No init* — not initialized, no initialization attempts;
 - *Off* — disabled, no submodule load attempts;
 - *Wait Ack* — waiting for acknowledgement from CPU after submodule load;
 - *Failed* — no response from submodule;
 - *Work* — submodule normal operation;
 - *Recovery* — no control packets coming from submodule;
 - *Reserved* — submodule is reserved for SORM needs;
 - *SSW.Sorm* — submodule is used by SORM agent.
- *Active count* — number of active connections on the submodule at the given moment;
- *Payload* — submodule resource utilization percentage at the given moment.

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

Monitoring → VoIP submodules → Type (M2359)

VoIP submodules																																		
No	Type										State										Active count										Payload			
0	M82359										Work										3										1.89%			
1	M82359										Reserved										0										0.0%			
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63		
	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95		
	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127		
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 #	Call IP-info # submodule #	Channels state
Portchannel	-	State
Callref	-	Codecs
Connected portchannel	-	Status
Connected Callref	-	Mode
State	-	SSRC
State timer	-	IP:port remote
Incoming SS7 category	-	IP:port local
Incoming CdPN	-	MAC remote
Incoming CgPN	-	MAC local
Outgoing SS7 category	-	
Outgoing CdPN	-	
Outgoing CgPN	-	

Channel info#:

- *Port/channel* — port/channel data:
 - Signaling protocol (VoIP);
 - Port location VoIP submodule #: Channel #.
- *Callref* — internal call identifier;
- *Connected port/channel* — linked port/channel data:
 - Linked port signaling protocol (PRI/SS7/VoIP);
 - Linked port location Stream #:Channel # for PRI/SS7 or VoIP submodule #:VoIP channel #.
- *Connected Callref* — call identifier for linked channel;
- *State* — channel state:
 - *Off* — channel is disabled;
 - *Block* — port is blocked;
 - *Init* — channel initialization;
 - *Idle* — channel is in initial state;
 - *In-Dial/ Out-Dial* — incoming/outgoing call dialing;
 - *In-Call/ Out-Call* — incoming or outgoing engagement;
 - *In-Busy/ Out-Busy* — sending 'busy' tone;
 - *Talk* — channel is in conversational state;
 - *Release* — channel release;
 - *Wait-Ack* — waiting for acknowledgement;
 - *Wait-CID* — waiting for CgPN (Caller ID);
 - *Wait-Num* — waiting for call dialing;
 - *Hold* — subscriber is on hold.
- *State timer* — channel last known state duration;
- *Incoming SS7 category* — SS7 category of an incoming call before modification;
- *Incoming CdPN* — callee number before modification;

-
- *Incoming CgPN* — caller number before modification;
 - *Outgoing SS7 category* — SS7 category of an incoming call after modification;
 - *Outgoing CdPN* — callee number after modification;
 - *Outgoing CgPN* — caller number after modification.

Channels state:

- *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.

Call IP info# submodule#:

- *State* — channel state (see description above);
- *Codec* — used codec (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 with T.38 protocol has been established through the channel.
- *Mode* — media channel operating mode:
 - *sendrecv* — channel operates in duplex mode (reception and transmission);
 - *sendonly* — channel operates in simplex mode, transmission only;
 - *recvonly* — channel operates in simplex mode, reception only;
 - *inactive* — channel is not active, reception and transmission are inactive.
- *SSRC* — SSRC (Synchronization Source) field value for outgoing device RTP stream;
- *IP:port remote* — remote IP address and port of RTP stream source;
- *IP:port local* — local IP address and port of RTP stream source;
- *MAC remote* — remote MAC address of RTP stream source;
- *MAC local* — local MAC address of RTP stream source.

There is the '*Disconnect the call*' button below the tables with channel status, which allows one to forcibly terminate the connection.



When using a SORM license, one of the submodules is completely allocated for ensuring combined control (see section 3.2.1 Application and Appendix E. SORM function configuration). In this case, the state of the submodule is displayed as Reserved, channel monitoring this module is not produced.

4.1.2.8 Fault alarms. Alarm events list.

When a failure occurs, related information containing the fault stream number, SS7 link set, signal link or faulty module will be displayed on 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.

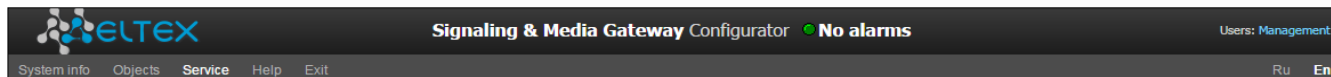


Table 20 — Alarm message examples


Alarm message	Meaning
Configuration is not read	Configuration file error
SIP module connection error	Failure of a software module responsible for SIP operation
SS7 Linkset failed	SS7 link set failure
E1 stream alarm	E1 stream failure
SS7 link alarm	SS7 signal channel failure
Synchronization from low-priority source	Primary synchronization source is lost, priority of the current source is lower
E1 stream remote alarm	E1 stream remote fault
Synchronization from local source. All configured sources are failed	Synchronization from local source. All configured sources are failed
Failed to send CDR files to remote storage	Failed to send CDR file to remote storage
VoIP-submodule connection error	No communication with SM-VP submodule
RAM is almost running out	High RAM utilization alarm
No power on the power module	Primary power main is missing on one of the power modules
H323-module connection error	Failure of a software module responsible for H.323 operation
High CPU temperature	Temperature: 70°C — warning; 85°C — alarm; 100°C — critical alarm
SIP interface is not responding on OPTIONS requests	One of the SIP interfaces is not available
High CPU load	Load: More than 90% — warning; More than 95% — alarm
Fans malfunction	One or multiple fans are inoperable
Low free space on a USB/HDD drive	Low free space on one of the external storage devices
CPS threshold is exceeded for TrunkGroupName	Number of calls coming to one of the trunk groups per second exceeds the value defined by 'Alarm CPS value' option
SIP interface INVITE duplication error	Duplication failures of INVITE received from emergency call service node. Failure might occur if duplication server is not available.
KPD1/KPD2 down	KPD1/KPD2 is not in operation
SIP. different transport type on one receiving port	Incorrect configuration warning — Several SIP interfaces with the same network alarm interface and alarm receiving port are configured, but with a different transport type on these interfaces (TCP/UDP)

The 'Alarm events list' menu displays a list of emergency events, ranked by date, time and events. 'Only active' events show current accidents on the device in this moment. 'All events' display all available alarm information. Also there is a 'Clear' button, which deletes all information from the current log.

Alarm events list

Clear the list











Display events

No	Time	Date	Type	State	Parameters	Description
9	11:53:22	30/01/24	SYNC-SOURCE	 Alarm	Synchronization from local source. All configured sources are failed	

Alarm events list

Clear the list

Display events

No	Time	Date	Type	State	Parameters	Description
9	11:53:22	30/01/24	SYNC-SOURCE	 Alarm	Synchronization from local source. All configured sources are failed	
8	11:53:22	30/01/24	Fans malfunction	 OK	Fans are operating normally	
7	11:53:07	30/01/24	SM-VP DEVICE	 OK	SM-VP submodule 5 active	
6	11:53:03	30/01/24	SM-VP DEVICE	 OK	SM-VP submodule 4 active	
5	11:52:59	30/01/24	SM-VP DEVICE	 OK	SM-VP submodule 3 active	
4	11:52:55	30/01/24	SM-VP DEVICE	 OK	SM-VP submodule 2 active	
3	11:52:51	30/01/24	SM-VP DEVICE	 OK	SM-VP submodule 1 active	
2	11:52:47	30/01/24	SM-VP DEVICE	 OK	SM-VP submodule 0 active	
1	11:52:41	30/01/24	Configuration is successfully read	 OK		
0	11:52:41	30/01/24	Software start V.3.21.5.5195	 OK		

Alarm events list:

- *Clear* — delete the current alarm events table;
- *No* — alarm sequential number;
- *Time* — alarm occurrence time in HH:MM:SS format;
- *Date* — alarm occurrence date in DD/MM/YY format;
- *Type* — alarm type:
 - *CONFIG* — critical fault, configuration file fault;
 - *SIPT-MODULE* — critical fault, failure of a software module responsible for VoIP operation;
 - *LINKSET* — critical fault, SS7 link set is not in operation;
 - *STREAM* — critical fault, E1 stream is not in operation;
 - *SM-VP DEVICE* — fault, SM-VP module failure;
 - *SS7LINK* — SS7 signal channel failure;

-
- *SYNC* — synchronization fault, synchronization source is missing;
 - *STREAM-REMOTE* — warning, E1 stream remote fault;
 - *CDR_UPSERVER* — alarm or warning, error of sending a CDR file to a remote storage;
 - *TRUNK-CPS* — permitted number of calls per second is exceeded for a trunk group;
 - *SORM-KPD* — alarm, KPD1/KPD2 in not in operation;
 - *SIP-DUPLICATE* — duplication failures of INVITE message received from emergency call service node;
 - *SIP-TRANSPORT* — warning, the configuration contains SIP interfaces with different types of transport at one receiving port.
- *State* — fault state status:
 - *Critical fault, flashing red icon* — alarm requires immediate intervention of the service personnel, affects device operation and provisioning of communication services;
 - *Fault, red icon* — non-critical alarm, also requires intervention of the service personnel;
 - *Warning, yellow icon* — alarm does not affect provisioning of communication services;
 - *OK, green icon* — alarm is resolved.
 - *Parameters* — text description of alarm details. Depending on the alarm type, may appear as follows:
 - *CONFIG*
 - *SIPT-MODULE* — no communication with SIP module;
 - *LINKSET* — SS7 link set XX is not in operation, where XX is SS7 link set number;
 - *STREAM* — E1 stream XX failure, where XX is stream number;
 - *SM-VP DEVICE* — no communication with VoIP submodule XX, where XX is SM-VP submodule number;
 - *SS7LINK* — SS7 link failure Linkset XX, E1 stream YY, where XX is SS7 link set number, YY is a signal channel number in SS7 group;
 - *TRUNK-CPS* — 'XX' trunk group exceeds CPS threshold, where XX is a trunk group name;
 - *SORM-KPD* — KPD1/KPD2 stream 'XX' in not in operation, where XX — E1 stream number;
 - *SIP-DUPLICATE* — SIP interface 'XX'. INVITE duplication to the '<YY>' server failure, where XX — SIP interface name, on which failure was occurred; YY — duplication server address, on which failure was occurred.
 - *Description*.
-

4.1.2.9 Network interface monitoring

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

Monitoring → Network interfaces

Network interfaces							
No	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							
No	PPP-interface	Network name	PPTPD IP	Username	IP address	P-t-P	Network mask
8	ppp8 <i>Запущен. Подключен. IP <192.168.20.10></i>	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

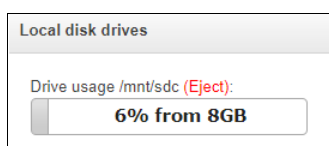
- *PPP interface* — name of the interface;
- *Network name* — name that the current network settings are associated with;
- *PPTPD IP* — PPTP server IP address used for connection;
- *Username* — username identifier;
- *IP address, P-t-P, network mask* — interface network settings.

4.1.2.10 Local disk drives

This section contains information on the connected storage media.

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

Monitoring → Local disk drive



The names of external drives are linked to the interface ports:



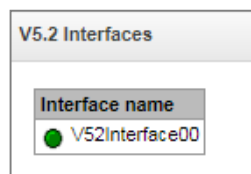
Devices are named according to the /dev/sdX principle.

SMG-1016M	
SSD № 1	/dev/sda*
SSD № 2	/dev/sdb*
USB	/dev/sdc*
SMG-2016	
HDD № 1	/dev/sda*
HDD № 2	/dev/sdb*
USB	/dev/sdc*
SMG-3016	
HDD № 1	/dev/sda*
HDD № 2	/dev/sdb*
USB	/dev/sdc*

4.1.2.11 V5.2 interfaces

The state of V5.2 interfaces is displayed in this section¹.

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



4.1.2.12 Queue statistics

This section displays queue operation statistics.

Queue statistics									
ID queue	Total calls	Answered	Unanswered	Maximum queue length (hour/day/workday)	Callback failure	Queue overflow	Waiting time	Select all	<input type="checkbox"/>
Selected: 0									

- *ID queue* — queue identifier;
- *Total calls*— total number of calls received in the queue;
- *Answered* — number of successful calls ending with an operator response;
- *Unanswered* — number of calls in which the caller hung up without waiting an operator response;
- *Maximum queue length (hour/day/workday)* — maximum queue length per last hour/day/working day. Last hour/day is a periodic time interval, repeating every hour/24 hours respectively, the beginning of the first interval is necessary to count from the moment the software starts. Time intervals of the working day are set in the group settings call;

¹ Available for the devices with V5.2 license.

- *Callback failure* — number of unsuccessful attempts to call back the subscriber, when using the callback option (not supported in the current firmware version 3.21.5);
- *Queue overflow* — number of calls rejected due to queue overflow;
- *Waiting time* — average waiting time for an operator response, a response is generated based on this value.

To clear queue statistics, check 'Select' opposite those queues whose statistics need to be cleared, and click the appeared 'Clear selected' button.

4.1.2.13 VNS tasks (section is available with SMG-VNS licence)

Monitoring → VNS tasks

VNS tasks									
No	Task name	State	Start time	Percent done	Idle	Active	Failed	Done	Stop
There are no running voice notification tasks									
<div style="display: flex; justify-content: space-between; align-items: center;"> 20 Rows in the table to show <input type="button" value="Update"/> </div>									

This section displays the status of running voice notification systems.

- *Task name* — VNS task name;
- *State* — displays the state of a running task for an alert:
 - *Waiting*;
 - *Reserved*;
 - *Prepared*;
 - *Launched*;
 - *Error*;
 - *Requires completion*;
 - *Stopped*;
 - *Completed*.
- *Start time* — time to start the notification task in the format Hours:Minutes:Seconds Day. Month. Year;
- *Percent done* — task procent done (ratio of processed calls number to all calls in this task);
- *Idle* — number of inactive calls in a task. Example: 30(40) – 30 from 40 (total numbers in the task);
- *Active* — number of active calls in a task. Example: 15(40) – 15 from 40 (total numbers in the task);
- *Failed* — number of unsuccessful calls in a task. Example: 5(40) – 5 from 40 (total numbers in the task);
- *Done* — number of completed calls in the task. Example: 35(40) – 35 из 40 (total numbers in the task);
- *Stop* — force completion of a calling task.

4.1.3 E1 streams

The signalling and parameters of each E1 stream are configured in this section.

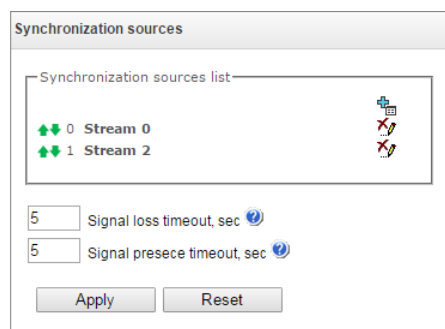
4.1.3.1 Synchronization sources

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.

Up to 16 synchronization sources can be specified (each of 16 E1 streams and 2 external sources).


The ports receiving external signals have the impedance of 120 Ohm. The incoming signal should have the parameters given in ITU-T G.703 recommendation, section 15, 2048 kHz synchronization interface (T12).


E1 streams → Synchronization 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 15.

- *Signal loss timeout, sec* — time interval during which the system does not switch to a lower priority synchronization source when the signal is lost. If the signal is restored during this interval, there will be no switching;
- *Signal presece timeout, sec* — time interval during which the signal restored from a higher priority synchronization source should be active before the system switches to that signal.

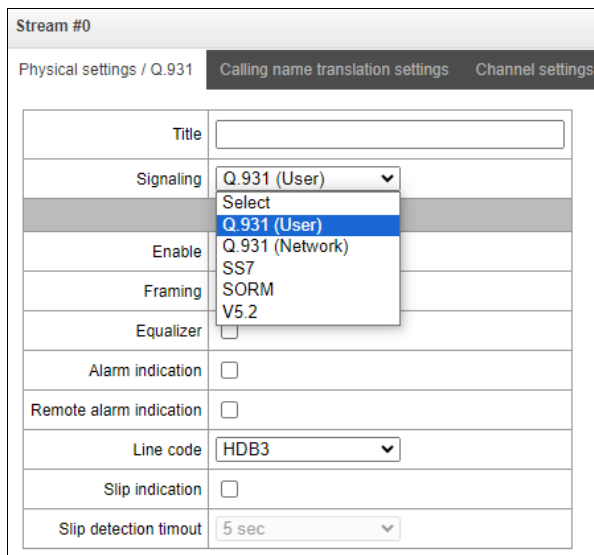


If D-channel is configured for the stream originating the synchronization signal (for SS7 or PRI protocol), make sure that D-channel is in operation, otherwise the synchronization signal will not be captured from the stream that will cause slips.

4.1.3.2 Signaling protocol selection

The signaling protocol used on the stream is selected in the drop-down list 'Signaling protocol'.

E1 streams → Stream 0 (Q.931 User) → Physical settings/ Q.931



Stream #0	
Physical settings / Q.931	
Title	<input type="text"/>
Signaling	Q.931 (User) ▼
	Select
	Q.931 (User)
Enable	Q.931 (Network)
Framing	SS7
	SORM
	V5.2
Equalizer	<input type="checkbox"/>
Alarm indication	<input type="checkbox"/>
Remote alarm indication	<input type="checkbox"/>
Line code	HDB3 ▼
Slip indication	<input type="checkbox"/>
Slip detection timeout	5 sec ▼

The device supports the following signals:

- Q.931 (User);
- Q.931 (Network);
- SS7;
- SORM;
- SORM-TRANSIT¹;
- V5.2 (LE);
- M2UA2¹;
- IUA (User)¹;
- IUA (Network)¹;

V5.2 interfaces:

- Media Gateway¹.

¹ Is not supported in this firmware version for SMG-1016M, SMG-2016, SMG-3016.

4.1.3.3 Physical settings

E1 streams → *Stream 2 (Q.931-U)* → *Physical settings/Q.931*

Stream #2	
Physical settings / Q.931	
Calling name translation settings	
Channel settings	
Title	<input type="text"/>
Signaling	Q.931 (User) ▼
Physical settings	
Enable	<input type="checkbox"/>
Framing	doubleframe ▼
Equalizer	<input type="checkbox"/>
Alarm indication	<input type="checkbox"/>
Remote alarm indication	<input type="checkbox"/>
Line code	HDB3 ▼
Slip indication	<input type="checkbox"/>
Slip detection timeout	15 min ▼

- *Title* — E1 stream name;
- *Enable* — enable the stream;
- *Framing*:
 - *Doubleframe* — CRC4 disabled;
 - *CRC multiframe* — CRC4 checksum generation at transmission and control at the reception.
- *Equalizer* — when checked, transmitted signal is amplified;
- *Alarm indication* — when checked, in case of local alarm an alarm indication will be on the stream (the ALARM indicator will light up, the accident will be recorded in the alarm events list);
- *Remote alarm indication* — when checked, in case of remote alarm an alarm indication will be on the stream (the ALARM indicator will light up, the accident will be recorded in the alarm events list);
- *Line code* — type of information encoding in the channel (HDB3, AMI);
- *Slip indication* — when checked, in case of slip detection in the receiving path, an alarm indication will take place;
- *Slip detection timeout* — the frequency of polling the flow parameters of the board, if the slip is detected in the stream, then during this timeout the gateway will indicate an alarm.

4.1.3.4 Signaling protocol settings DSS1/EDSS1 (ISDN PRI Q.931)

4.1.3.4.1 'Physical settings/Q.931' tab

E1 Streams → *Stream 0 (Q.931-U)* → *Physical settings/Q.931*

Q.931 LAPD	
T200, x100 ms	<input type="text" value="10"/>
T203, x100 ms	<input type="text" value="100"/>
N200	<input type="text" value="3"/>
Q.931 settings	
TrunkGroup	<input type="text" value="not set"/>
PRI profile	<input type="text" value="not set"/>
Scheduled routing profile	<input type="text" value="not set"/>
Access category	<input type="text" value="[0] AccessCat#0"/>
Dial plan	<input type="text" value="[0] NumberPlan#0"/>
Numbering plan type	<input type="text" value="Unknown"/>
Calling party category (RUS)	<input type="text" value="7"/>
Send calling party category (RUS)	<input type="checkbox"/>
'End-of-dial' message	<input type="checkbox"/>
Do not send RESTART for interface	<input type="checkbox"/>
Do not send RESTART for channel	<input type="checkbox"/>
Channels selection order	<input type="text" value="Successive forward"/>
DialTone for incoming overlap-seize	<input type="checkbox"/>
Process PI 'In-band' in DISCONNECT	<input type="checkbox"/>
Handle PROCEEDING as ALERTING	<input type="checkbox"/>
Process PI in SETUP	<input type="text" value="Transit"/>
Replace symbol '?' by 'D' in CgPN	<input type="checkbox"/>
ISUP Location Number transit	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

- *T200, x100 ms* — transmission timer. This timer defines time period for frame response reception that will enable the following frames' transmission. This time period should be greater than the time required for frame transmission and its acknowledgement reception;
- *T203, x100 ms* — maximum time during which the device may not exchange frames with the remote device;
- *N200* — quantity of frame retransmission attempts.

Q.931 settings

- *Trunk group* — name of a trunk group, that includes the E1 stream;
- *PRI profile* — selects a PRI profile for servicing PRI subscribers;
- *Scheduled routing profile* — selects scheduled routing profile from the list of existing profiles;
- *Access category* — selects access category;
- *Dial plan* — defines dial plan that will be used for routing of the call received from this port (necessary for dial plan negotiation);

- *Numbering plan type* — defines ISDN dial plan type. To use common dial plan E.164, select 'ISDN/telephony';
- *Calling party category* — Caller ID category assigned to calls received from this port;
- *Send calling part category* — enables Caller ID category transmission as the first digit of a number in CgPN information element of the SETUP message.



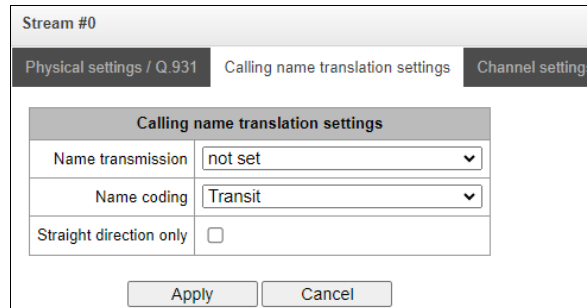
For proper operation, support for this mode on the opposite side is necessary.

- *'End of dial' message* — produces 'Sending Complete' informational element upon 'End of dial' event (such event arrives from the linked channel side, achieved maximum quantity of digits according to prefix, dialing timeout for the next digit);
- *Do not send RESTART for interface* — when checked, gateway will not send RESTART message into the line when the stream is restored (channel level LAPD is established);
- *Do not send RESTART for channel* — when checked, gateway will not send RESTART message upon the expiration of T308 timer. This timer activates when RELEASE message is sent into the channel and resets when it receives RELEASE COMPLETE message as a response. If RELEASE COMPLETE message is not received during T308 timer active state, RESTART message is transmitted in order to release the channel;
- *Channels selection order* — defines the order of the physical channel provisioning when performing outgoing call. You may select one of four types: sequential forward, sequential back, from the first and forward, from the last and back. To minimize conflicts during communication with neighboring PBXes, we recommend to set inverse channel engagement types;
- *DialTone for incoming overlap-seize* — when checked, gateway will send DialTone into the line during incoming overlap seize ('PBX response' ready signal). In this case, overlap seize is a reception of SETUP message without 'sending complete' indication;
- *Process PI 'In-Band' in DISCONNECT* — when checked, field PI In-Band contained in DISCONNECT message will be processed for call release voice message transmission, otherwise this field is ignored;
- *Handle PROCEEDING as ALERTING* — when checked, upon receiving a PROCEEDING message, it will be processed as an ALERTING and a RBT will be issued;
- *Process PI in SETUP* — when checked, adds the ability to change the Progress Indicator in a SETUP message. It is possible to change to:
 - *Transit* — transmit without change;
 - *1* — Not end-to-end ISDN;
 - *2* — Dest addr is non ISDN;
 - *3* — Orig addr is non ISDN;
 - *4* — Return to ISDN;
 - *5* — Interworking occurred;
 - *8* — In-band information.
- *Replace symbol '?' by 'D' in CgPN* — when checked, if a received SETUP message in CgPN receives a '?', it will be replaced by 'D'.
- *ISUP Location Number transit* — when checked, if the Location Number parameter is passed in the incoming message SS7/SIPT, it will be transferred to the Calling Party Number parameter in the outgoing message SETUP Q.931.

4.1.3.4.2 'Calling name translation settings' tab

This tab is used to configure the way of name reception/transmission and coding of received/transmitted name.

E1 Streams → *Stream #0 (Q.931-U)* → *Calling name and translation settings*



Stream #0	
Physical settings / Q.931 Calling name translation settings Channel settings	
Calling name translation settings	
Name transmission	not set
Name coding	Transit
Straight direction only	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- *Name transmission:*
 - *Not set* — name transmission is disabled;
 - *Q.931 DISPLAY* — transmission in Q.931 Display element with Codeset 5;
 - *QSIG-NA* — transmission via QSIG-NA (ECMA-164) protocol;
 - *CORNET* — transmission via Siemens CorNet protocol;
 - *CORNET HICOM-350* — transmission via Siemens CorNet protocol with additional info for Hicom PBX;
 - *AVAYA DISPLAY* — transmission in Q.931 Display element with Codeset 6;
 - *QSIG-NA (Ericsson)* — transmission in facility and user-user information.
- *Name coding:*
 - *Transit* — no recoding is carried out (by default the name is assumed to be accepted in UTF-8);
 - *CP 1251* — coding of Windows-1251;
 - *Siemens adaptation* — coding of Siemens PBX;
 - *AVAYA adaptation* — coding of AVAYA PBX;
 - *Latin transliteration* — Russian names will be transliterated into Latin letters.
- *Straight direction only* — send subscriber name only in forward direction messages.

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

4.1.3.4.3 'Channel settings' tab

E1 Streams → Stream #0 (Q.931-U) → Cannel settings

Stream #0

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

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

This menu is used to enable/disable E1 stream channel. To do that, select/clear checkbox against the corresponding channel. 'Trunk group' column displays number of group where these channels are configured (used only when trunk group is assigned to channels, not to the whole stream).

4.1.3.5 SS7 signaling protocol configuration

4.1.3.5.1 Physical settings/SS7

E1 streams → Stream #0 (SS7) → Physical settings/SS7

Stream #0	
Physical settings / SS7 Channel settings	
Title	<input type="text"/>
Signaling	SS7
Physical settings	
Enable	<input type="checkbox"/>
Framing	doubleframe
Equalizer	<input type="checkbox"/>
Alarm indication	<input type="checkbox"/>
Remote alarm indication	<input type="checkbox"/>
Line code	HDB3
Slip indication	<input type="checkbox"/>
Slip detection timeout	5 sec
SS7 settings	
SS7 Linkset	not set
Channel ID (SLC)	0
DPC-MTP3	0
D-channel	not set
Bit D in LSU	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

SS7 settings:

- *SS7 Linkset* — linkset selection (SS7 linkset);
- *Channel ID (SLC)* — signal line identifier in SS7 linkset;
- *DPC-MTP3* — destination point code of the signaling transition point (STP). It is 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 (see section 4.1.5.2 SS7 Linkset);
- *D-channel* — number of the channel interval that will be used for signaling transmission;



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

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

4.1.3.5.2 'Channel settings' tab

E1 streams → *Stream #0 (SS7)* → *Channel settings*

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

- *ISUP CIC* — channel identifier code — setting conversation channel numbers (CIC).
To automatically number conversation channels, click the 'Set' button.

E1 streams → *Stream #0 (SS7)* → *Channel settings* → *Set*

The following menu will be displayed:

- *Starting value* — number of the first conversation channel;
- *Numbering step* — channel numbering step. Each subsequent channel will be assigned a number with "numbering step" larger relative to the previous channel;
- *Last value* — number of the last conversation channel in the selected range;
- *Channels range* — selecting values in this block allows one to assign numbering for all stream channels or for a specified range of channels.

4.1.3.6 V5.2 signaling protocol configuration

The assignment of a stream to the V5.2 interface is made in the V5.2 interface parameters.

This section displays the current V5.2 interface to which this stream is assigned for reference, as well as the stream identifier inside the V5.2 interface.

E1 streams → Stream #0 → Physical settings/V5.2

Stream #0	
Title	<input type="text"/>
Signaling	V5.2 ▼
Physical settings	
Enable	<input type="checkbox"/>
Framing	doubleframe ▼
Equalizer	<input type="checkbox"/>
Alarm indication	<input type="checkbox"/>
Remote alarm indication	<input type="checkbox"/>
Line code	HDB3 ▼
Slip indication	<input type="checkbox"/>
Slip detection timeout	5 sec ▼
V5.2 settings	
V5.2 interface	not set
Link ID	-
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

4.1.3.7 SORM signaling protocol configuration

E1 streams → Stream #0 → Physical settings/SORM

SORM settings	
Enable command-avaiting timer (10 min)	<input type="checkbox"/>
Activity control	<input checked="" type="checkbox"/>
Link alarm indication	<input checked="" type="checkbox"/>
No VAS-number prefix	<input type="checkbox"/>
No extended error codes	<input type="checkbox"/>
No operator-selection code	<input type="checkbox"/>
Control by Redirecting number	No <input type="text"/>
Skip msg 1.1 for incomplete number	<input type="checkbox"/>
Station type	terminal-transit <input type="text"/>
Protocol	RUS Order 70 <input type="text"/>
Connection mode	X25 <input type="text"/>
Channel 1	
Channel mode	<input checked="" type="radio"/> DTE <input type="radio"/> DCE
Send SABM	<input checked="" type="checkbox"/>
Send RESTART (L3)	<input type="checkbox"/>
Send INITIAL_RESET (L3)	<input type="checkbox"/>
Channel 2	
Channel mode	<input checked="" type="radio"/> DTE <input type="radio"/> DCE
Send SABM	<input checked="" type="checkbox"/>
Send RESTART (L3)	<input type="checkbox"/>
Send INITIAL_RESET (L3)	<input type="checkbox"/>
Frames addresses	
Tx Cmd Addr <input type="text"/>	1 DTE-1 DCE-3
Tx Resp Addr <input type="text"/>	3 DTE-3 DCE-1
DTE/DCE mode adjustment	<input checked="" type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- *Enable command-avaiting timer (10 min)* — enable/disable timeout for receiving commands from the SORM control panel;
- *Activity control* — control of message exchange activity at the L1 level, if within 15 seconds, no packets were received on at least one of the channels, a reset will occur and re-initialization of the E1 stream framer;
- *No VAS-number prefix* — when ordering VAS by the subscriber, VAS-number prefix will be not transmitted to the SORM remote control. For example, when ordering the *'Unconditional forwarding'* service and dialing the number *21*2728331# to the SORM remote control, the message 44 will have the number 2728331 only, which forwarding is assigned to;
- *No extended error codes* — when checked, in response to a command with incorrect parameters, the message will be sent about non-acceptance or non-compliance commands only with the characteristics defined in order No. 268. Otherwise the command non-compliance signs of the manufacturer will be used, allowing to more accurate determine the reason for the command failure. List of standard and manufacturer codes is given in Appendix D;
- *No operator-selection code* — when monitoring a subscriber, the prefix for selecting a telecom operator for long-distance or international calls is not taken into account (more details in Appendix D);
- *Control by Redirecting number* — use the number from the Redirecting number field (or diversion in the SIP protocol) for transmission to the control panel. Upon receiving a call with a Redirecting number (or diversion in the SIP protocol) the number from the Calling Party Number field is initially

compared with the numbers on the control, then, if a match is not found, with the number from Redirecting number fields (or diversion in the SIP protocol). When unchecked, the comparison with Redirecting number (or diversion in the SIP protocol) is not performed;

- *Skip msg 1.1 for incomplete number*;
- *Station type* — communication node type transmitted in the last byte of message 11 (station firmware version);
- *Protocol* — selection of the SORM specification according to which the device will operate:
 - *RUS Order 70* — SORM specification for the order of the State Committee for Communications of Russia dated April 20, 1999 No. 70;
 - *RUS Order 268* — SORM specification for the order of the Ministry of Telecom and Mass Communications of Russia dated November 19, 2012 No. 268;
 - *KZ* — SORM specification for the Republic of Kazakhstan.
- *Connection mode*:
 - *X25* — signal channels are organized via the X25 protocol, using 30-31 channels of E1 stream;
 - *TCP* — signal channels are organized via the TCP protocol. The settings are active only when selecting 'TCP connection mode':
 - *Port 1* — virtual TCP port to organize the signal channel of command and control center 1;
 - *Port 2* — virtual TCP port to organize the signal channel of command and control center 2;
 - *Network interface* — selecting the device network interface.

Channel operation mode

- *Channel 1* — block for setting parameters of the control information transmission channel from the SORM control panel;
- *Channel 2* — block for setting parameters of the channel for transmitting information about the controlled connections from SMG-1016M.

Channel settings

- *Channel mode*:
 - *DTE* — when checked, the device type is DTE (information transmitter);
 - *DCE* — when checked, the device type is DCE (receives the data from DTE devices).
- *Send SABM* — when checked, a message about the beginning of the connection initialization procedure is transmitted to the channel;
- *Send RESTART (L3)* — transmission of 'level 3 restart' message when establishing connections with SORM control panel;
- *Send INITIAL_RESET (L3)* — transmission of a 'level 3 reset' message when establishing connections with SORM control panel.

Frames addresses

- *Tx Cmd Addr* — command frame address;
- *Tx Resp Addr* — response frame address.



It is not allowed to install the SORM protocol on multiple streams.

After selecting the SORM protocol on one of the streams, it is necessary to restart the software. The factory password for SORM is '123456'.

- *DTE/DCE mode adjustment* — option to automatically adjust DTE/DCE mode, by default: enabled. If the device and the remote side are set to the same mode (DTE-DTE or DCE/DCE) and the adjustment option is enabled, the SMG will automatically change the mode to the correct one.



It is not recommended to disable the 'DTE/DCE mode adjustment' option, because this could lead to malfunction of the device.



Modification of numbers on the SORM stream serves only to further configure interaction with SORM remote control in some exceptional configurations and should not be used with normal SORM setup. The need to use modifiers is determined by a qualified specialist. The procedure for setting up SORM is described in the section Appendix E. SORM function configuration.

Modifiers of incoming numbers — selecting a table of modifiers intended for analysis and modification of the subscriber's telephone number in SORM messages received from the console.

Modifiers of outgoing number — selecting a table of modifiers intended for analysis and modification of the subscriber's phone number in SORM messages sent to the remote control.

Always modify B-number — an option required to modify all B-numbers, the outgoing number modifier has been not previously applied for the number dialed by the local subscriber.

Modifiers of controlled numbers — selecting a table of modifiers intended for analysis and modification of the subscriber's phone number before selecting it for sending to the SORM control panel.

4.1.4 Dial plans

This section is used to configure the device dial plan.

The device has up to 16 independent dial plans (up to 255 for SMG-2016 and SMG-3016 with VAS license). Each dial plan can have its own subscribers and prefixes.

The number of active plans is configured in the System settings section.

There are 4 criteria by which calls are routed on the device:

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

Upon entering a call into the dial plan, its routing begins, initially search for a match with CgPN number masks takes place. If there is a prefix with 'AND' logic (masks are specified by CgPN and CdPN, and a match was found for both parameters) and a prefix with the same mask is found according to CgPN, then if the "Priority" parameter is equal, the call will go through the prefix with the 'AND' logic, because this mask is considered to be more accurate. If the priority of the prefix with 'AND' is lower, then the call will go by prefix with 'OR'.

If, when searching by CgPN, two prefixes with 'AND' logic are found, and the CgPN mask is the same, then CdPN is compared and the call is routed using a prefix with a more accurate mask.

Searching and routing a call through the database of configured subscribers is carried out even when the call parameters match the CgPN number masks.

If the call parameters do not match the CgPN masks and the subscriber number, a search occurs across all CdPN masks configured in the dial plan



If masks for CgPN and CdPN numbers are simultaneously configured in the prefix parameters and the logical operator 'OR' is set, then this rule works according to the logic 'OR', i.e. simultaneous analysis by CgPN and CdPN numbers does not occur. If masks for CgPN and CdPN numbers are simultaneously configured in the prefix parameters and the logical operator 'AND' is set, then this rule works according to the 'AND' logic, i.e. for routing a call using this prefix, the CgPN and CdPN masks should match.

Dial plans → Dial plan #0 'NumberPlan#0'

Dial plan # 0 'NumberPlan#0'

Dial plan settings # 0

Name

Check dial plan by number ST

Search mask

Default VAS prefixes

Prefixes in the dial plan

No	Description	Masks for CgPN	Operator	Masks for CdPN	Type	Object	CallerID	CallerID m.	Dial mode	Priority	
0	Prefix#00	(no masks)	or	(x.) ⇒	TrunkGroup	SIPP UAS TG	-	-	no change (+)	100	<input type="checkbox"/>

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

Dial plan settings:

- *Name* — dial plan name;

Check dial plan by number — checks if routing is possible for the number entered into this field. The check is performed by callee and caller masks and through the configured SIP subscriber database.

- *ST* — when checked, the search recognizes the end dial marker.

Search mask — prefix search by number pattern, name, direction, prefix type, trunk direction, trunk group.


The check provides information on routing capability for this number:


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

Copying prefixes to another dial plan

- *Copy all prefixes to the dial plan* — this option allows copying the selected prefixes to another dial plan. It is used similarly to copying dedicated prefixes, but does not require prefix selection;
- *Copy selected prefixes to the dial plan* — this option appears when prefix is selected in the table. It allows copying selected prefixes to another dial plan. For use, select prefixes, target dial plan and click 'Copy'.

4.1.4.1 Creating a prefix in the dial plan

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

Dial plans → Dial plan #0 'NumberingPlan#0' → 

Dial plan # 0 'NumberPlan#0'

Common prefix settings 1	
Title	Prefix#01
Dial plan	[0] NumberPlan#0
Access category	[0] AccessCat#0
Check access category	<input type="checkbox"/>
Prefix type	TrunkGroup
TrunkGroup	not set
Direction	local network
CallerID request	<input type="checkbox"/>
CallerID mandatory	<input type="checkbox"/>
Dial mode	unchanged
Do not send end-of-dial (ST)	<input type="checkbox"/>
Priority	100
Max session time (sec)	0
Session warning time (sec)	0
Logical operator	or
CdPN settings	
Number type	unchanged
Numbering plan type	isdn/telephony
Skip first digits	0
Direct route timers	
Short timer	5
Duration	30

Common prefix settings

- *Title* — prefix name;
- *Dial plan* — selects a dial plan;
- *Access category* — selects an access category;
- *Check access category* — when this option is selected, it checks the possibility of call routing by the prefix based on the rules determined by access categories;
- *Prefix type* — selects the prefix type:
 - *TrunkGroup* — transition to a trunk group;
 - *Trunk Direction* — transition to a trunk direction;
 - *Change dial plan* — this option allows you to enter another dial plan when this prefix is dialed. When this prefix type is selected, the *New Dial plan* option becomes available, where you should specify the dial plan for transition;
 - *Subscribers pool* — enables setting the subscriber capacity of the device. If the number is present in the subscriber capacity but not yet assigned to any subscriber, then a call to such a number will trigger a call release message with the cause code: 1 — Unallocated (unassigned) number;
 - *VAS prefix* — used to manage VAS services from the telephone set;
 - *Pickup group* — used to configure the pickup group transition prefix;
 - *IVR scenario* — used to configure the IVR script transition prefix.

Parameters of the 'Trunk Group and Trunk Direction' Prefix

Common Prefix Parameters:

- *TrunkGroup* — a trunk group to which the call will be routed by this prefix;
- *Direction* — a trunk group access type: local, emergency, zone, department, national, international. The prefix is used when enabling SORM function in the network, as well as to restrict a connection if a failure occurs during the data exchange with the RADIUS server (see section 4.1.18 RADIUS Configuration);
- *Caller ID request* — indicates the need for caller ID information (caller number and category) to access the trunk group specified in the "Trunk group" field. Upon receiving a call from an interacting node and the absence of Caller ID information in this call, a Caller ID request will be sent to the node (INR message via SS7 signaling);
- *Caller ID mandatory* — indicates that Caller ID information is required when accessing the direction. If Caller ID information cannot be obtained from the calling party, then connection establishment process is interrupted;
- *Dial mode* — a method of number transmission:
 - *enblock* — after collection of all address information;
 - *overlap* — without waiting for collection of all address information.
- *Do not send end-of-dial (ST)* — when this option is active, the end dial marker is not sent (ST in SS or sending complete in PRI);
- *Priority* — if there are some overlapping masks in the dial plan, the call will be made into the prefix with a higher priority. The value of 0 is the highest priority, 100 is the lowest priority;
- *Max session time (sec)* — limit duration of calls passed through this prefix;
- *Session warning time (sec)* — activates when using the option 'Max session time (sec)', an audible signal is issued, which warns about the end of the call for a specified number of seconds before the end of the call. If the specified time is more than 60 seconds, an additional warning signal will sound 5 seconds before the end of the call. If the specified time is less than 60 seconds, there will be no additional signal;
- *Logical operator*:
 - OR — if CgPN and CdPN masks are on the prefix, there is no simultaneous analysis by CgPN and CdPN numbers;
 - AND — simultaneous analysis by CgPN and CdPN number is performed.

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

CdPN Settings:

- *Number type* — a callee number type: *unknown, subscriber number, national number, international number, network specific, no change*. The selected number type will be sent in SS7, ISDN PRI, SIP-I/T signaling messages during an outgoing call by a prefix ('no change' means that the number type will not be converted, i. e. it will be sent in the form it has been received from the incoming channel);
- *Numbering plan type* — a callee dial plan type; it may take the following values: *unknown, isdn/telephony, national, private, no change*. The selected dial plan type will be sent in ISDN PRI signaling messages during an outgoing call by a prefix ('no change' means that the number type will not be converted, i. e. it will be sent in the form it has been received from the incoming channel);
- *Skip first digits* — number of digits removed from the callee number, starting from the first.

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

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

- *Short timer* — time interval in seconds when the digital gateway waits for further dialling if a part of address information has already been received. Default value: 5 seconds;

- *Duration* — a timer for number dialing duration. Default value: 30 seconds.

Parameters of the 'Change dial plan' Prefix

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

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

Modifiers when changing the dial plan:

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

Parameters of the 'VAS Prefix'

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

- *VAS type* — selecting the Supplementary Service type to manage it from the subscriber's telephone:
 - *CFU* — Call Forwarding Unconditional;
 - *CFB* — Call Forwarding Busy;
 - *CFNR* — Call Forwarding No Reply;
 - *CFOOS* — Call Forwarding Out of Service;
 - *Call pickup* — call pickup;
 - *Conference* — conference call;
 - *Clear All* — canceling all services;
 - *Intercom* — intercom call (with an automatic answer from party B);
 - *Paging* — similar to Intercom, but with a call to conference numbers;
 - *Password* — setting a password;
 - *Password once* — access by password;
 - *Password access* — password activation;
 - *Restrict out* — restriction of outgoing communication;
 - *DND* — Do Not Disturb feature;
 - *Blacklist* — black list;
 - *Anonymous call*;
 - *Reject anonymous calls*;
 - *Reminder*.
- *Action* — selecting an action for the service:
 - *Configure* — enabling a Supplementary Service;
 - *Cancel* — canceling a Supplementary Service;
 - *Control* — a Supplementary Service activity control;
 - *numberAdd*— add a number;
 - *numberDel* — delete a number.

Parameters of the 'Pickup Group' Prefix

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

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

Direct route timers

- *Short timer* — time in seconds that the digital gateway will wait for further dialing, if the already dialed number matches any pattern in the numbering plan, but there is opportunity to obtain more digits, which will lead to a match with another pattern. Default value: 5 seconds;
- *Duration* — dialing duration timer. Default value: 30 seconds.

Parameters of the 'IVR Scenario' Prefix

- *IVR scenario* — an IVR scenario to which a call will be routed to on the basis of this prefix;
- *CallerID request* — indicates the need for caller ID information (caller number and category subscriber). When a call comes from a collaborating node and there is no Caller ID information, a caller ID request will be sent to the node (INR message via SS7 signaling);
- *CallerID mandatory* — indicates that Caller ID information is mandatory when accessing the direction. If Caller ID information cannot be obtained from the calling party, then connection establishment process is interrupted;
- *Priority* — configuring prefix priority in the range from 0 to 100. Prefix which parameter value is lower has a greater priority (0 — the highest priority, 100 — the lowest priority);
- *Max session time (sec)* — limit duration of calls passed through this prefix;
- *Session warning time (sec)* — activates when using the option 'Max session time (sec)', an audible signal is issued, which warns about the end of the call for a specified number of seconds before the end of the call. If the specified time is more than 60 seconds, an additional warning signal will sound 5 seconds before the end of the call. If the specified time is less than 60 seconds, there will be no additional signal;
- *Logical operator:*
 - *OR* — if CgPN and CdPN masks are on the prefix, there is no simultaneous analysis by CgPN and CdPN numbers;

- **AND** — simultaneous analysis by CgPN and CdPN number is performed.

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

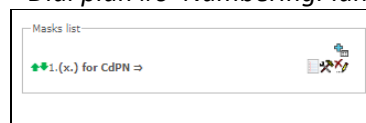
Direct route timers

- **Short timer** — time in seconds that the digital gateway will wait for further dialing, if the already dialed number matches any pattern in the numbering plan, but there is opportunity to obtain more digits, which will lead to a match with another pattern. Default value: 5 seconds;
- **Duration** — dialing duration timer. Default value: 30 seconds.





Masks lists

For created dial plans, the ‘Masks List’ section allows configuring the masks of numbers for routing by this prefix.


Dial plans → Dial plan #0 ‘NumberingPlan#0’ → Object

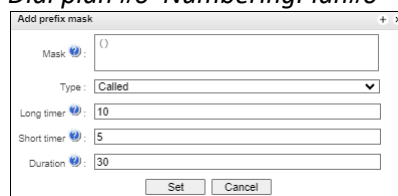


To generate the list, use the following buttons:

-  — Add mask;
-  — Edit mask;
-  — Remove mask;
-  — View mask.

Using green arrows to the left of the created mask, the entries can be moved in the table by prioritizing them.

Dial plans → Dial plan #0 ‘NumberingPlan#0’ → Object → 



- **Mask** — a template or a set of templates, which is compared to the calling or called number received from the incoming channel. It is used for further call routing (for mask syntax, see section 4.1.4.2);
- **Type** — mask type. Defines the number for the call routing – caller number (calling) or callee number (called);
- **Long timer** — the time interval in seconds when the digital gateway will wait for the next digit dialling until a match to a sample from the dial plan is established. Default value: 10 seconds;
- **Short timer** — the time interval in seconds when the digital gateway will wait for further dialling if the dialed number already matches a sample in the dial plan, but additional digits may be also dialed, which will result in a match to another sample. Default value: 5 seconds;
- **Duration** — the timer for number dialling duration. Default value: 30 seconds.

To edit a prefix, double-click the prefix row in the prefix table with the left button or select the prefix

and click the  button below the list.

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

4.1.4.2 Description of Number Mask and Its Syntax

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

Syntax:

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

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

Prefix 1: (2xxxx)

Prefix 2: (23xxx)

When the number '23456' arrives to the dial plan, it will be processed with prefix 2.

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



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

Prefix 2: (23xxx)

When the number '23456' arrives to the dial plan, it will be processed with prefix 2.

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

Prefix 1: (2x.)

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

When the number '23456' arrives to the dial plan, it will be processed with prefix 2.

4.1.4.3 Mask Operation Examples

Example 1

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

The mask contains 9 templates:

1. #XX# — dialling a 4-character number that begins and ends with #; the 2nd and the 3rd digits of the number may take any values from 0 to 9, as well as * and #.

In general, this template disables VAS using a phone set.

2. *#XX# — dialling a 5-character number that begins with *# and ends with #, the 3rd and the 4th digits of the number may take any values from 0 to 9, as well as * and #.

In general, this template is used to control VAS from the phone set.

3. *XX*X.# — dialling an N-character number which begins with * followed by two arbitrary characters of the number (digits from 0 to 9, as well as * and # characters), then followed by *, and then by any number of characters (digits from 0 to 9, or *) until # is met.

In general, this template is used to order VAS using a phone set.

4. 112 – dialling the specific 3-digit number (112).

5. 011 – dialling the specific 3-digit number (011).

6. 0[1-4] – a 2-digit number that begins with 0 and ends with 1, 2, 3, or 4, i. e. 01, 02, 03, or 04.

7. 6[2-9]XXX – a 5-digit number that begins with 6, with the second digit of the number being any digit from 2 to 9, and the last three digits being any digits from 0 to 9, as well as * and #.

8. 5[24]XXXXX – a 7-digit number that begins with 5, with the second digit of the number being 2 or 4, and the last five digits being any digits from 0 to 9, as well as * and #.

9. 810X{11, 15} – a number that begins with 810 followed by 11 to 15 arbitrary digits from 0 to 9, as well as * and #. Taking into account the first three digits, the length of the number according to this rule is from 14 to 18 digits.

Example 2

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

To solve this task, configure the following prefixes:

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

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

Example 3

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

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

4.1.4.4 Timer operation examples

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

L = 10 seconds.

S = 5 seconds.

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

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

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

4.1.4.5 Configuration example of prefix with ‘subscribers pool’ type

Objective

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

Solution

For correct release cause transmission, local numbering should be created — configure a ‘*subscribers pool*’ type prefix.




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

4.1.5 Call routing


4.1.5.1 Trunk groups

Call routing → TrunkGroup

TrunkGroups					
Nº	TrunkGroup	TrunkGroup member	Direct routing prefix	Disable incoming	Disable outgoing
0	TrunkGroup00_500	SIP interfaces [2] "SIP-interface01_500"	not set	-	-
1	SIPP UAS TG	SIP interfaces [3] "SIPP UAS"	not set	-	-
2	SMG500 TG	SIP interfaces [4] "SMG500"	not set	-	-
3	SMG3016 TG	SIP interfaces [5] "SMG3016"	not set	-	-
4	Asterisk TG	SIP interfaces [6] "Asterisk"	not set	-	-

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

the left mouse button or select the group and click the  button below the list.

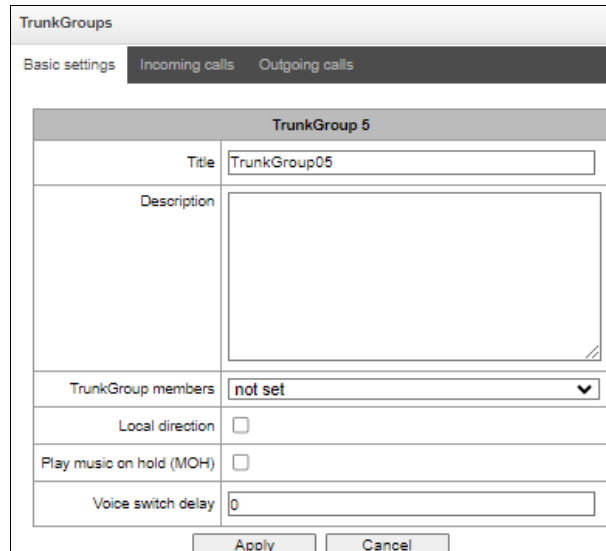
To *delete a trunk group*, select the group and click the  button below the list or open the *Objects* menu and select *Remove Object*.

Up to 255 trunk groups can be created.

4.1.5.1.1 'Basic settings' tab

To add a trunk group click the  button, then fill in the following fields:

Call routing → TrunkGroups → 




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

- *Title* — trunk group name;
- *Description* — trunk group description;
- *TrunkGroup members* — trunk group members:
 - *Stream with Q.931 signaling, SS linkset, SIP or H323 interface*;
 - *E1 stream channels* — E1 stream channels with Q.931, SS7 signaling protocols;
 - *E1 streams from SS7 Linkset*.
- *E1 stream* — E1 stream selection to assign the trunk group to E1 stream channels, this menu is active only when 'E1 channels' value is selected for 'TrunkGroup members' field.

Call routing → TrunkGroups → → Basic settings

TrunkGroups

Basic settings Incoming calls Outgoing calls

TrunkGroup 5

Title:

Description:

TrunkGroup members:

E1 stream:

Channels selection order:

Local direction:

Play music on hold (MOH):

Voice switch delay:

E1 channel number	Select	E1 channel number	Select
0 Sync	<input type="checkbox"/>	16 D-channel	<input type="checkbox"/>
1	<input type="checkbox"/>	17	<input type="checkbox"/>
2	<input type="checkbox"/>	18	<input type="checkbox"/>
3	<input type="checkbox"/>	19	<input type="checkbox"/>
4	<input type="checkbox"/>	20	<input type="checkbox"/>
5	<input type="checkbox"/>	21	<input type="checkbox"/>
6	<input type="checkbox"/>	22	<input type="checkbox"/>
7	<input type="checkbox"/>	23	<input type="checkbox"/>
8	<input type="checkbox"/>	24	<input type="checkbox"/>
9	<input type="checkbox"/>	25	<input type="checkbox"/>
10	<input type="checkbox"/>	26	<input type="checkbox"/>
11	<input type="checkbox"/>	27	<input type="checkbox"/>
12	<input type="checkbox"/>	28	<input type="checkbox"/>
13	<input type="checkbox"/>	29	<input type="checkbox"/>
14	<input type="checkbox"/>	30	<input type="checkbox"/>
15	<input type="checkbox"/>	31	<input type="checkbox"/>




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

- *SS7 Linkset* — SS7 link set for selecting E1 streams. This menu is available only when you choose 'SS7 Linkset lines' in 'TrunkGroup members' menu;
- *Channels selection order* — channel selection order in E1 streams. This menu is available only when 'SS7 Linkset lines' is chosen in 'TrunkGroup members' menu;



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

- *Local direction* — when checked, subscribers of this direction are considered local. Subscribers of this direction are set under SORM control with the type and number sign as 'subscriber of this station';
- *Play music on hold (MOH)* — enabling Music On Hold option;
- *Voice switch delay* — forced voice switching path delay after the subscriber's answer.

Call routing → TrunkGroups →  → Incoming calls


TrunkGroups

Basic settings Incoming calls Outgoing calls

Incoming calls

Disable ingress calls	<input type="checkbox"/>
Direct routing prefix	not set
Use voice messages	<input type="checkbox"/>
No Connected number transit	<input type="checkbox"/>
Copy CgPN into Redirecting number	<input type="checkbox"/>
Use Redirecting number for routing	<input type="checkbox"/>
CallerID request	<input type="checkbox"/>
Alarm CPS value	0
Max CPS value	0
RADIUS profile	not used
List of reasons for call recovery after outbound leg failure	not set

Ingress calls modifiers

Add CgPN 

Apply Cancel


- *Disable ingress calls* — when this option is checked, the incoming calls are prohibited. Setting the call prohibition does not terminate any of the established connections;
- *Direct routing prefix* — the prefix will be used without caller or callee number analysis. It enables switching of all calls in a single trunk group to another group regardless of the dialed number (without mask creation in prefixes). When a number is dialed in the overlap mode, direct dialling timers are used, which are configured in the direct prefix;
- *Use voice messages* — when this option is selected, pre-recorded voice messages stored in the device memory will be played upon the occurrence of specific events. For detailed description, see Appendix G. Voice messages and music on hold (MOH);
- *No Connected number transit* — disable the transmission of the Connected number field;
- *Copy CgPN into Redirecting number* — when this option is checked, if there is no *Redirecting number* in the incoming call, it will be generated from the CgPN number;
- *Use Redirecting number for routing* — when this option is checked, the Redirecting number field is used when using SS7 or Q.931 signaling protocols, the SIP *diversion* field is used to route the incoming call in the dial plan using CgPN number masks;
- *CallerID request* — specify the need of a caller's information (number and category) to call the trunk group. If a call is received from an interacting node and do not contain CallerID information, the CallerID request will be sent to the calling node (INR messages via SS7);
- *Alarm CPS value* — the number of calls per second after which a failure will be indicated in the log. '0' value – the fault indication is turned off. Fault indication time — 5 minutes after exceeding the specified threshold of CPS;
- *Max CPS value* — the maximum number of calls per second that can be received by a trunk group. '0' value – turning off the CPS limit. The CPS value is calculated as the moving average for the last 3 seconds. For example, if 3xCPS calls arrive within the first second, they will be accepted, but if there are any additional calls within the next two seconds, they will be rejected;


- *RADIUS profile* — selecting the RADIUS profile to use (profiles are configured in the RADIUS Configuration/Profile List menu, in section 4.1.18.2);
- *List of reasons for call recovery after outbound leg failure* — selecting the ‘List of reasons to restore the Q.850’ table to configure the reasons for the Q.850 release to restore the call in case of failure of the outgoing leg. If a call received through the trunk group with the enabled option was released not from an incoming side and the cause of the release is present in the selected table, then SMG will try to recover the connection without interrupting the conversation on the A call leg using recall or alternative routes if the main is not unavailable.

Incoming calls modifiers

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

4.1.5.1.3 ‘Outgoing calls’ tab

Call routing → TrunkGroups →  → Outgoing calls

TrunkGroups		
Basic settings	Incoming calls	Outgoing calls
Outgoing calls		
Disable egress calls	<input type="checkbox"/>	
Replace CgPN by Redirecting	<input type="checkbox"/>	
Check access category	<input type="checkbox"/>	
Reserve TrunkGroup	not set	
Q.850 release causes list for switching to reserve TG	not set	
RADIUS profile	not used	
Egress calls modifiers		
Add	CdPN 	
RingBack settings		
Mode	Default	
File name		
Apply		Cancel

- *Disable egress calls* — when this option is active, transmitting outgoing calls is forbidden. Setting the call prohibition does not terminate any of the established connections;
- *Replace CgPN by Redirecting* — when this option is active, the CgPN number is replaced with Redirecting;
- *Check access category* — when this option is active, it checks the possibility of call routing based on the rights determined by access categories;
- *Reserve TrunkGroup* — specifying a trunk group to which a call will be routed when routing to the current trunk group is not possible (all channels are engaged or inoperable);
- *Q.850 release causes list for switching to reserve TG* — selecting the Q.850 release causes table to configure the Q.850 release causes for switching to the reserve trunk group;
- *RADIUS profile* — selecting the RADIUS profile to use (profiles are configured in the RADIUS Configuration/Profile List menu, in section 4.1.18.2).

Outgoing calls modifiers

- *CdPN modifiers* — intended for modifications based on the analysis of the called number received from the incoming channel;
- *CgPN modifiers* — intended for modifications based on the analysis of the calling number received from the incoming channel;
- *Original CdPN* — intended for modifications based on analysis of the original called number transmitted to the outgoing channel;
- *RedirPN modifier* — intended for modifications based on the analysis of the redirecting number transmitted to the outgoing channel;
- *GenericPN* — intended for modifications based on the analysis a special number (generic number) transmitted to the outgoing channel;
- *LocationNumber* — are intended for modifications based on the analysis location number transmitted to the outgoing channel.

To create, edit, or remove groups (as well as other objects), use the 'Objects' — 'Add object', 'Objects' —

'Edit object' and 'Objects' — 'Remove object' menus and the following buttons:



— Add a trunk group;



— Edit trunk group parameters;



— Remove a trunk group.

RingBack settings

Mode:

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

4.1.5.2 SS7 Linkset

Call routing → SS7 Linkset

SS7 Linksets		
Nº	SS7 Linkset	TrunkGroup
	Linkset members	



For SS7 protocol configuration, see E1 streams 4.1.3.5.

SS7 Linkset is a set of signaling links in one direction. To create, edit, or remove linkset, use the 'Objects' — 'Add object', 'Objects' — 'Edit object' and 'Objects' — 'Remove object' menus and the following buttons:



— Add SS7 Linkset;



— Edit SS7 Linkset;



— Remove SS7 Linkset.

SS7 Linksets	
SS7 Linkset 0	
Title	Linkset00
TrunkGroup	not set
Access category	[0] AccessCat#0
Dial plan	[0] NumberPlan#0
Scheduled routing profile	Not set
Toll	<input type="checkbox"/>
Alarm indication	<input type="checkbox"/>
Channel selection	successive forward
Reserve SS7 Linkset	Not set
Combined mode	<input type="checkbox"/>
Primary SS7 Linkset	Not set
Secondary SS7 Linkset	Not set
SS7 Timers profile	Profile 0
Stream order by SLC	<input checked="" type="checkbox"/>
MTP2 layer settings	
Emergency alignment for a single link	<input type="checkbox"/>
Service information (SIO)	
Network ID	00 - international network (DEC)
Routing label	
OPC	0
DPC-ISUP	0

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



To minimize conflicts during communication with neighboring PBXes, it is recommended to set inverse channel engagement types.

- *Reserve SS7 Linkset* — redundant SS7 linkset selection. When the main SS7 linkset is not available, the whole signalling message exchange will be performed through the redundant SS7 linkset;
 - *Combined mode* — Combined Linkset mode that will enable the exclusive utilization of voice streams in the current SS7 link set and signalling transfer through the signal channels of SS7 primary and secondary groups;
 - *Primary SS7 Linkset* — selects SS7 link set, that will perform the exchange of signalling messages related to this particular SS7 link set, by the signal D-channels;
 - *Secondary SS7 Linkset* — selects the second SS7 link set, that will perform the exchange of signaling messages related to this particular SS7 link set, by the signal D-channels;
- In the combined mode operation, the signalling payload will be distributed evenly (50/50) between the primary and secondary SS7 linksets.
- *SS7 Timers profile* — selects the timer profile that will be used for the current SS7 linkset;
 - *Stream order by SLC* — affects the operation of the Order of channel engagement setting. With this option enabled, the order of engaged E1 streams is determined by the SLC number (sorted from a smaller SLC to a larger one), with this option disabled the order is determined by the E1 stream index.

MTP2 Layer settings

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

Service information (SIO)

- *Network ID* — indicates the network type: international, federal, local network or spare (usually on RF networks the value “Local network” is used).

Routing label

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

ISUP subsystem

ISUP subsystem	
Channels initialization mode	remain in block <input type="button" value="v"/>
Send REL on receiving SUS	<input type="checkbox"/>
Add a digit in IAM for overlap	<input type="checkbox"/>
Restrict CdPN in IAM to 15 digits	<input type="checkbox"/>
Control receiving Redirecting/Original Called for incoming redirection	<input checked="" type="checkbox"/>
Ignore HOLD indications	<input type="checkbox"/>
Transmit Global Callref	<input type="checkbox"/>
Hop counter	Decrement <input type="button" value="v"/> 0

- *Channels initialization mode* – device operations during stream recovery:
 - *Remain in block* — channels remain blocked (BLO);
 - *Individual unblock* — sending unblock command for each channel (UBL);
 - *Group unblock* — sending channel group unblock command (CGU);
 - *Group reset* — group reset command (GRS).
- *Send REL on receiving SUS* — sending Release message in response to Suspend message;

- *Add a digit in IAM for overlap* — sending a single digit of the number to Called Party number of IAM message if overlap dialing method is used;
- *Restrict CdPN in IAM to 15 digits* — when active, up to 15 digits of CdPN number will be sent in IAM message, other digits will be sent in SAM message;
- *Control receiving Redirecting/Original Called for incoming redirection* — this checkbox enables controlling the presence of Redirecting/Original Called fields with redirection information in incoming IAM message; when this option is active, the call will be rejected if these fields are absent;
- *Ignore HOLD indication* — when checked, SMG will ignore the CPG messages with remote hold or remote retrieval signs;
- *Transmit Global Callref* — when there is no Global Call Reference (GCR) field in an incoming leg, SMG forms it automatically;
- *Hop counter* — setting rules for operation with hop counter field:
 - *Decrement* — transmission with decreasing value;
 - *No change* — transmission without any changes;
 - *Preset* — transmission with pre-assigned value always;
 - *Don't send* — disable issuing hop counter for outgoing communication or ignore the received parameter for incoming communication.

IAM indicators

IAM indicators	
Transmission medium requirements	transit
Forward call indications	
ISUP preference	unchanged
Interworking indicator	unchanged
Call type indicator	unchanged
Connect type indicators	
Satellite indicator	change to 'no satellite'
Enable continuity check	<input type="checkbox"/>
Continuity check frequency	0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

Forward call indications

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

Connect type indicators

- *Satellite indicator* — identifies the presence of a satellite channel:
 - *Change to 'no satellite'* — changing identifier value to no satellite regardless of the value received from the incoming channel;
 - *Unchanged* — keeping the indicator value unchanged;

- *Add one satellite* — this setting is used if the signal link operates via satellite channel. In this case, a satellite channel parameter transmitted in the nature of connection indicators will be increased by 1.
- *Enable continuity check* — enables integrity check support in the SS7 link set. During the outgoing call, the called party establishes a remote loop in the stream. The SMG sends the frequency value to the channel and then detects it on reception after transmission through the channel. If the frequency is detected, the call will be served at this channel; if it is not detected, the similar attempt will be performed at the next channel. After 3 unsuccessful attempts (for three different channels), call serving will stop;
- *Continuity check frequency* — defines the frequency of channel continuity checks during outgoing calls performed via the SS7 link set. For example, value 3 means that each third outgoing call will be performed with the channel integrity check.

For the gateway, you may assign the correspondence of SS categories to Caller ID categories. For configuration, see section 4.1.7.2.

Examples

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

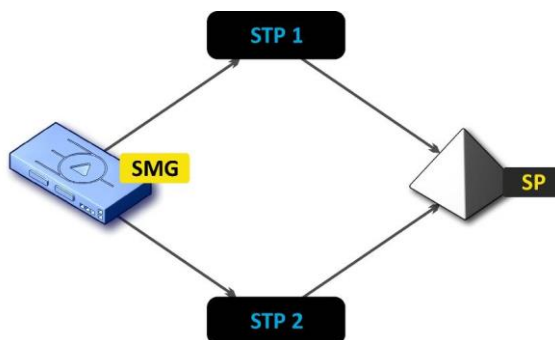


Figure 46 — SMG connection method for operation in SS7 quasi-associated mode via STP

Objective

It is necessary to provide the SMG connection to the remote signalling point (SP) using two signal links. The first signal link should pass through the signalling transition point STP 1 and the second signal link should pass through the STP 2.

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

Solution

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

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

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

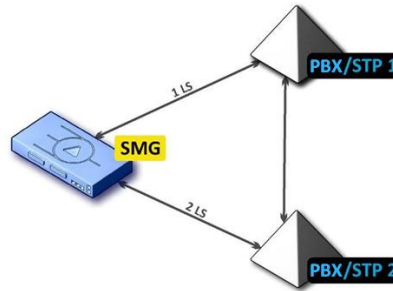


Figure 47 — SMG connection method for operation in SS7 quasi-associated mode via PBX with STP (LS – SS7 Link Set)

Objective

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

Solution

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

SMG connection method example for operation in combined mode:

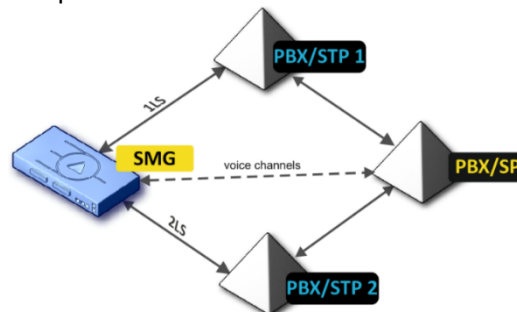


Figure 48 — SMG connection method for operation in combined mode

Objective

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

Solution

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

4.1.5.3 SIP/SIP-T/SIP-I, SIP-profiles

4.1.5.3.1 Configuration

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

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

SIP network addressing is based on the SIP URI scheme:

sip:user@host:port;uri-parameters

user – the number of a SIP subscriber;

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

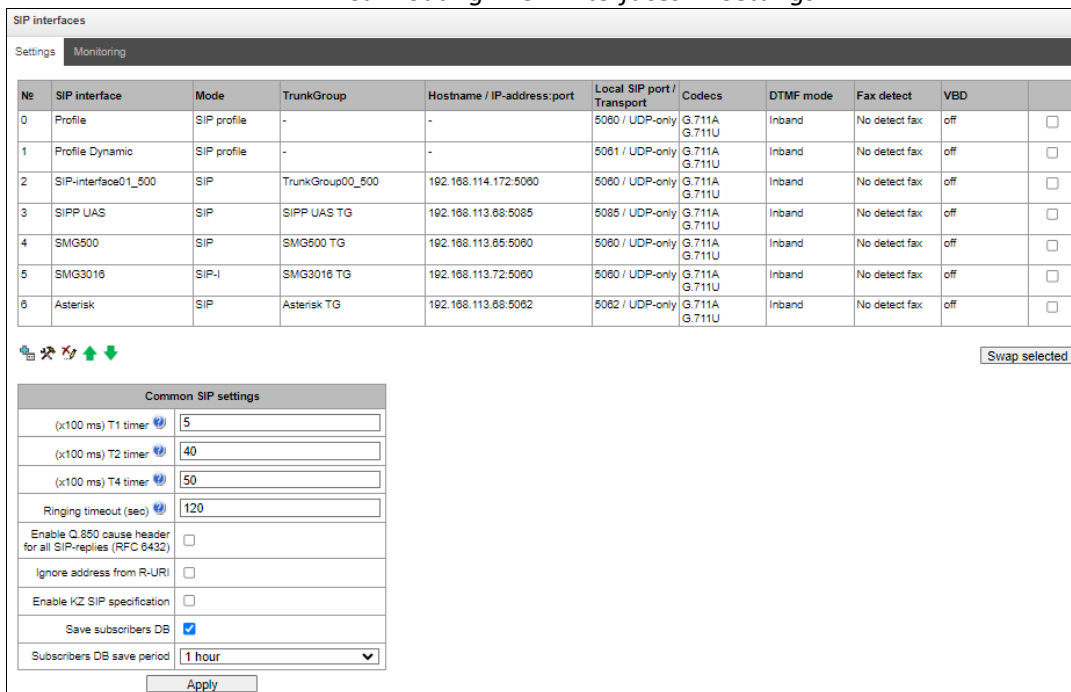
host – domain or IP address of the SIP subscriber;

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

uri-parameters – additional parameters.

One of the additional SIP URI parameters is user=phone. If this parameter is specified, the syntax of the SIP subscriber number (in the user part) should match the TEL URI syntax described in RFC 3966. In this case, SMG PBX will process requests that contain '+', ';', '=', '?' in the SIP subscriber number, and will automatically add '+' before the called number for international calls using the SIP-T protocol.

Call routing → SIP interfaces → Settings



The screenshot shows the 'SIP interfaces' settings page. At the top, there are tabs for 'Settings' and 'Monitoring'. Below the tabs is a table with the following columns: No, SIP interface, Mode, TrunkGroup, Hostname / IP-address:port, Local SIP port / Transport, Codecs, DTMF mode, Fax detect, VBD, and a checkbox. The table contains 6 rows of data. Below the table, there are several icons and a 'Swap selected' button. At the bottom, there is a 'Common SIP settings' section with various configuration options, including timers and checkboxes.

No	SIP interface	Mode	TrunkGroup	Hostname / IP-address:port	Local SIP port / Transport	Codecs	DTMF mode	Fax detect	VBD	
0	Profile	SIP profile	-	-	5080 / UDP-only	G.711A G.711U	Inband	No detect fax	off	<input type="checkbox"/>
1	Profile Dynamic	SIP profile	-	-	5081 / UDP-only	G.711A G.711U	Inband	No detect fax	off	<input type="checkbox"/>
2	SIP-interface01_500	SIP	TrunkGroup00_500	192.168.114.172:5080	5080 / UDP-only	G.711A G.711U	Inband	No detect fax	off	<input type="checkbox"/>
3	SIPP UAS	SIP	SIPP UAS TG	192.168.113.68:5085	5085 / UDP-only	G.711A G.711U	Inband	No detect fax	off	<input type="checkbox"/>
4	SMG500	SIP	SMG500 TG	192.168.113.65:5080	5080 / UDP-only	G.711A G.711U	Inband	No detect fax	off	<input type="checkbox"/>
5	SMG3016	SIP-I	SMG3016 TG	192.168.113.72:5080	5080 / UDP-only	G.711A G.711U	Inband	No detect fax	off	<input type="checkbox"/>
6	Asterisk	SIP	Asterisk TG	192.168.113.68:5082	5082 / UDP-only	G.711A G.711U	Inband	No detect fax	off	<input type="checkbox"/>

Common SIP settings

- (x100 ms) T1 timer: 5
- (x100 ms) T2 timer: 40
- (x100 ms) T4 timer: 50
- Ringling 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

Apply





Common SIP settings

- (x100 ms) T1 timer — timeout for a response to the request, after which the request will be sent again. The maximum retranslation interval for INVITE requests is 64*T1;
- (x100 ms) T2 timer — the maximum retranslation interval for responses to the INVITE request and for all requests except for the INVITE requests;
- (x100 ms) T4 timer — the maximum time for all retranslations of the final response;

- *Ringling timeout, sec* — pre-answering state timeout of the call after reception of 18X message, during which the ringback tone or IVR message is played to the subscriber;
- *Enable Q.850 cause header for all SIP-replies (RFC 6432)* — when this option is active, the device analyses the Q.850 cause field in all final SIP messages. If the option is not active, the Q.850 cause field is only analyzed in BYE and CANCEL messages;
- *Ignore address from R-URI* — when this option is active, address information after the '@' separator in Request-URI is ignored. Otherwise, the gateway checks if the address information matches the device's IP address and host name; if there is no match, the call is rejected;
- *Enable KZ SIP specification* — setting a specification in accordance with the requirements of the Republic of Kazakhstan;
- *Save subscribers DB* — when this option is active, saving details of registered subscribers to the non-volatile memory of the gateway. The option is required to save the database of registered subscribers in case of device reboot due to power loss or failure. If the gateway is rebooted from WEB or CLI, the current database will be saved to non-volatile memory regardless of this setting;
- *Subscriber DB save period* — setting the data update period in the archive database (from 1 to 16 hours).

The SIP protocol defines two types of responses to connection initiating requests (INVITE) — provisional and final. 2xx, 3xx, 4xx, 5xx and 6xx-class responses are final, their transfer is reliable and confirmed by the ACK message. 1xx-class responses, except for the *100 Trying* response, are provisional and do not have a confirmation (RFC3261). These responses contain information on the current INVITE request processing step; in SIP-T/SIP-I protocols, SS-7 messages are encapsulated into 1xx class responses, therefore the loss of these responses is unacceptable. Utilisation of reliable provisional responses is also realised in the SIP protocol (RFC3262) and is defined by the *100rel* tag in the initiating request. In this case, provisional responses are confirmed by a PRACK message.

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

-  – Add interface;
-  – Edit interface parameters;
-  – Remove interface;
-  – Move interfaces up or down.

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

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

G.726 is an ITU-T standard for adaptive pulse code modulation — ADPCM and describes voice transmission with a bandwidth of 16, 24, 32, and 40 kilobits/sec. **G.726-32** replaces G.721, which describes ADPCM voice transmission with a bandwidth of 32 kilobits/sec.


G.723.1 is a codec with speech information compression, provides two operating modes: 6.3 Kbit/s and 5.3 Kbps. The G.723.1 codec has a speech activity detector and provides generation of comfortable noise at the remote end during the silent period (Annex A).

G.729 is also a voice compression codec and provides a bit rate of 8 Kbps. Similar to the G.723.1 codec, the G.729 codec supports speech activity detection and ensures the generation of comfortable noise (Annex B).

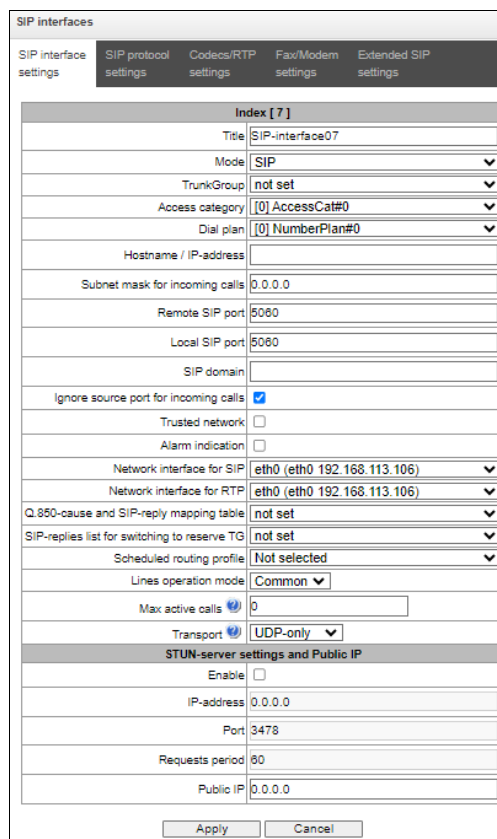
T.38 is a standard that describes the transmission of fax messages in real time over IP networks. Signals and data transmitted by a fax machine are encoded into T.38 protocol packets. In generated packets, redundancy can be introduced — data from previous packets, which allows carrying out reliable fax transmission over unstable channels.

CLEARMODE is a mode in which signal encoding/decoding is not used. Used for transparent transmission of digital information 64 kbit/s (RFC4040).

4.1.5.3.1.1 'SIP interface settings' tab

To create SIP/SIP-T interfaces, use the 'Objects' menu – 'Add object' or the  button, when pressed, the following menu appears:

Call routing → SIP interfaces → Settings →  → SIP interface settings



- **Title** – the interface name;
- **Mode** – selects the interface protocol (*SIP/SIP-T/SIP-I/SIP profile*);
- **Ingress RADIUS profile** – selects the RADIUS profile for the *SIP profile* interface for incoming communication (for other interfaces, the RADIUS profile is assigned in the trunk group);

-
- *Egress RADIUS profile* – selects the RADIUS profile for the *SIP profile* interface for outgoing communication (for other interfaces, the RADIUS profile is assigned in the trunk group);
 - *Trunk group*¹ – name of the trunk group to which the interface belongs;
 - *Access category* – selects an access category;
 - *Dial plan* – defines the dial plan that will be used for dialling from this port (required for coordination of dial plans);
 - *Hostname/IP-address*¹ – IP address or name of the host communicating via the gateway SIP/SIP-T protocol;
 - *Subnet mask for incoming calls* – if the mask is set, SMG will receive calls from the subnet holding the connecting host, specified in the '*Host name/IP address*' field. Note that when using the masks 0.0.0.0 (/0), 255.255.255.255 (/32) or 255.255.255.254 (/31), SMG will only accept calls from the IP address indicated in the '*Host name/IP address*' field, rather than from the subnet;
 - *Remote SIP port*¹ – a UDP/TCP port of the communicating gateway that is used to receive SIP/SIP-T signalling;
 - *Local SIP port*¹ – a local UDP/TCP port of the device used to receive SIP/SIP-T signalling from the device communicating via this interface;
 - *SIP domain* – a domain that is placed into the *from* field when an outgoing call is made through the SIP interface; is used in the SIP interface registration;
 - *Ignore source port for incoming calls* – when this option is checked, the signalling transmission UDP port of the communicating gateway that is specified in the *Port for SIP Signalling Reception* parameter is not checked; otherwise, the port is checked and the call is cleared back if the INVITE request is received from another port. If the INVITE request is received via TCP, the port is not checked regardless of the parameter value;
 - *Trusted network* – means that the interface is connected to a trusted network. This option defines generation of the INVITE request fields for calls with hidden caller number (presentation restricted). When this option is checked, the caller number information is transmitted in the *from* and *P-Asserted-identity* fields together with the information on its hidden state in the *Privacy: id* field; otherwise, the caller number information is not transmitted in any fields;
 - *Alarm indication* – when this option is checked, SMG will indicate a fault when connection to the opposite device is lost. For correct operation of this feature, check the *Opposite party availability control using OPTIONS messages* checkbox in SIP settings;
 - *Network interface for SIP* – network interface selected to receive and transmit signalling SIP messages;
 - *Network interface for RTP* – selects a network interface to receive and transmit voice traffic;
 - *Q.850-cause and SIP-reply mapping table* – table of correspondence between Q.850-cause and SIP-reply codes. To configure correspondence tables, use the '*Internal Resources*' menu;
 - *SIP-replies list for switching to reserve TG* – selects the reply table for SIP 4XX – 6XX classes for transition to a reserve trunk group. The replies list table is configured in Internal resources section;

¹ The field is disabled in the SIP profile mode.

- *Scheduled routing profile* – selects a profile for the Scheduled Routing service configured in the Internal Resources section;
- *Lines operation mode* – setting lines operation mode to limit the number of simultaneous calls via this interface:
 - *Common* – considering the total number of simultaneous calls (incoming and outgoing) via this interface;
 - *Separate* – incoming and outgoing calls are counted separately.
- *Max active calls* – maximum number of simultaneous (incoming and outgoing) connections via this interface. The field is displayed if *Common* operation mode is selected;
- *Ingress lines number* – number of simultaneous incoming calls via this SIP interface. The field is displayed if *Separate* operation mode is selected;
- *Egress lines number* – number of simultaneous outgoing calls via this SIP interface. The field is displayed if *Separate* operation mode is selected;
- *Transport* – selecting a transport level protocol using for reception and transmission of SIP messages:
 - *TCP-prefer* – receiving by UDP and TCP. Sending via TCP. If not connected by TCP, make attempt by UDP;
 - *UDP-prefer* – receiving by UDP and TCP. Transmitting by TCP whenever packet is greater than 1300 bytes, otherwise by UDP;
 - *UDP-only* – receiving and transmitting only by UDP;
 - *TCP-only* – receiving and transmitting only by TCP.
- *Global Callref generation* – if there is no GCR in a call, it will be generated locally. If there is GCR in a call, it will be transmitted further without generating a new one. **The option is only available for SIP-I;**
- *Node ID* – an identifier used for generating a global Callref. The range of allowed values is [0;255]. **The option is only available for SIP-I.**

STUN server settings and Public IP:

STUN-server settings and Public IP	
Enable	<input type="checkbox"/>
IP-address	0.0.0.0
Port	3478
Requests period	60
Public IP	0.0.0.0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

STUN network protocol (RFC 5389) allows applications located behind a network address translation server (NAT) to discover their external IP address and port mapped to an internal port. Used when SMG is located behind a NAT. To identify external device address, use STUN or Public IP (used separately).

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








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

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

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

4.1.5.3.1.2 'SIP protocol setting' tab

Call routing → SIP interfaces → Settings →  → SIP protocol settings

SIP interfaces	
SIP interface settings	SIP protocol settings
Options	
Keep-alive control 	<input type="checkbox"/> 0
Keep-alive mode	SIP-OPTIONS 
Always transmit SDP in provisional responses	<input type="checkbox"/>
'In-band signal' with 183+SDP transmission	<input type="checkbox"/>
Local ring-back instead of early-media	<input type="checkbox"/>
Enable P-Early-Media (RFC5009)	<input type="checkbox"/>
Fill empty Display-Name	<input type="checkbox"/>
Send DisplayName in Remote-Party-ID header	<input checked="" type="checkbox"/>
Ignore RURI and To difference	<input type="checkbox"/>
Do not use plus sign in CdPN and Diversion	<input type="checkbox"/>
Diversion header with SIP URI	<input type="checkbox"/>
Enable redirection (302) processing	<input type="checkbox"/>
Redirection server direction 	<input type="checkbox"/>
Enable REFER processing	<input type="checkbox"/>
Enable Re-INVITE with a=sendonly processing	<input type="checkbox"/>
Send calling category	off 
Reliable provisional responses (1xx) 	off 
DSCP for signaling 	0
Transit SIP header	<input type="checkbox"/>

Setting options for SIP/SIP-T/SIP-I protocols

- *Keep-alive control* – a function that controls direction availability by sending OPTIONS requests; when a direction is not available, the redundant trunk group is used for the call. This function also analyses the received OPTIONS response that allows avoiding the use of the *100rel*, *replaces*, and *timer* features configured in this direction, unless the opposite party supports them. The parameter defines the request transmission period and may take values in the range of 30–3600 seconds;
- *Keep-alive mode*:
 - *SIP-OPTIONS* – at specified opposite party control intervals, the device will send the OPTIONS control message. This message should receive a response from the opposite party; if no response is received, the direction is considered unavailable, and the failure status is registered in the device;
 - *SIP-NOTIFY* – the device will send the NOTIFY control message at specified opposite party control intervals. This message should receive a response from the opposite party; if no response is received, the direction is considered unavailable, and the failure status is registered in the device;
 - *UDP-CRLF* – device will send an empty UDP packet at specified opposite party control intervals; the opposite party response to an empty UDP packet is not applicable; consequently, the failure status will not be initiated on the device.




These methods are also used to maintain the NAT connection.

- *Always transmit SDP in provisional responses* – allows early forwarding of the voice frequency path. For example, when this option is not checked, SMG sends reply 180 without SDP session

description; according to this reply, the outgoing party plays the ringback tone; when this option is checked, SMG sends reply 180 with SDP session description and the ringback is played by the incoming party;

- *'In-band signal' with 183+SDP transmission* – issues SIP-reply 183 with SDP session description for voice frequency path forwarding upon receipt of the CALL PROCEEDING or PROGRESS messages from ISDN PRI that contain the progress indicator = 8 (in-band signal);
- *Local ringback instead of early-media* – when the early media marker is received from the outgoing leg, ringback tone will be played to the caller instead of the inband voice message;
- *Enable P-Early-Media (RFC5009)* – use the P-Early-Media header described in RFC 5009. With outgoing call, the device will transmit the P-Early-Media: supported header in the INVITE. Upon receiving INVITE with P-Early-Media: supported marker, the response 18X messages will contain the P-Early-Media header: sendrecv;
- *Fill empty Display-Name* – when this option is checked, if a call with the missing display-name is received, SMG will fill it with the user name (number) taken from the URI;
- *Send DisplayName in Remote-Party-ID header* – enables/disables substitution of DisplayName in Remote-Party-ID;
- *Ignore RURI and To difference* – disables issuing the Redirecting and Original Called numbers in SS7 calls when the values in SIP RURI and To fields are different;
- *Do not use plus sign in CdPN and Diversion* – disables addition of '+' to a number, for International number type;
- *Diversion header with SIP URI* – uses SIP URI in the Diversion header instead of TEL URI;
- *Enable CCI* – for SIP-I/T, enable transmission of IAM with a Continuity check indication value of 2. **The option is available only for SIP-T and SIP-I protocols;**
- *Enable redirection (302) processing* – when this option is checked, the gateway is allowed to perform forwarding upon receipt of reply 302 from this interface. When unchecked and reply 302 is received, the gateway will reject the call and perform forwarding;
- *Redirection server direction* – this option is available when the redirection 302 processing is enabled. This enables forwarding of the call, which was sent using a public address, to the subscriber's private address received in reply 302 without dial plan routing. The call is routed directly to the address specified in the 'contact' header of reply 302 received from the forwarding server;
- *Enable REFER processing* – a REFER request is sent by the communicating gateway to enable the *Call Transfer* service. When this option is checked, the gateway is allowed to process REFER requests received from this interface. When unchecked, the gateway clears back the call upon receipt of a REFER request and does not provide the *Call Transfer* service;
- *Enable Re-INVITE with a=sendonly processing* – when this option is checked, it allows a call to be put on hold when the Re-INVITE message is received with a=sendonly marker in SDP;
- *Send calling category* – select a method of caller category transmission through SIP. The following methods are implemented:
 - *off* – sending and receiving of Caller ID category are disabled;

- *category* – the caller category is sent/received in a separate *category* field in the INVITE message; in this case, the SS7 category with values 0 – 255 is sent;
 - *cpc* – the caller category is sent/received via the “cpc=” tag transmitted in the *from* field, in this case, the Caller ID category with values 1–10 is sent;
 - *cpc-rus* – the caller category is sent/received via the “cpc-rus=” tag transmitted in the *from* field; in this case, the Caller ID category with values 1–10 is sent.
- *Reliable provisional responses (1xx)* – when this option is checked, the INVITE request and 1xx class provisional responses will contain the *require: 100rel* option, which requires assured confirmation of provisional responses:
 - *off* – reliable delivery of provisional responses is disabled;
 - *support* – the INVITE request and 1xx class provisional responses will contain the *support: 100rel* option;
 - *support+* – duplicate SDP in 200 OK message when using *support: 100rel*;
 - *require* – the INVITE request and 1xx class provisional responses will contain the *require: 100rel* option, which requires assured confirmation of provisional responses;
 - *require+* – duplicating SDP in 200 OK message when using *require: 100rel*.
 - *DSCP for signaling* – a service type (DSCP) for SIP signalling traffic;
-  *DSCP for RTP* and *DSCP for SIP* settings will be ignored when using VLAN for RTP transmission and signaling. To prioritize traffic in this case there will be used Class of Service VLAN.
- *Transit SIP header* – enables transit of the received SIP headers into the outbound leg.

SIP-session timers (RFC 4028)

SIP-session timers (RFC 4028)	
Enable	<input type="checkbox"/>
Session Expires	0
Min SE	0
Refresher side	Client

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

Registration settings (available for SIP mode only)

Registration settings	
Upper registration	no registration ▼
Login	<input type="text"/>
Password	<input type="text"/>
Username/Number	<input type="text"/>
Default CdPN	<input type="text"/>
Replace CgPN on egress call	<input type="checkbox"/>
Registration period (sec)	1800
Registration requests interval (ms)	1000

- *Upper registration* – the selected type of registration on an upstream server:
 - *No registration* – do not perform registration on the upstream server;
 - *Trunk registration* – registration on the upstream server using parameters specified in this section;
 - *User registration* – registration on the upstream server using parameters specified on the 'registration' tab. This registration type allows to define the list of subscribers with enabled access via this interface;
 - *Upper registration* – transit registration of device subscribers on the upstream server; when this option is selected, SMG will transfer subscribers' SIP messages via this SIP interface. When transit registration is selected, you should specify this SIP interface in the settings of SIP profile that requires transit registration.
- *Login* – the name used for authentication;
- *Password* – the password used for authentication;
- *Username/Number* – the user number which is used as a caller number for outgoing trunk calls;
- *Default CdPN* – the default CdPN number that will be used for all calls via this SIP interface;
- *Replace CgPN on egress call* – when this option is checked, the caller number (CgPN) is taken from the *Username/Number* parameter; otherwise, the CgPN number received in the incoming call is used;
- *Registration period (sec)* – the time interval for registration renewal;
- *Registration requests interval (ms)* – the minimum interval between the Register messages that is used to protect from high traffic caused by simultaneous registration of a large number of subscribers.

SIP INVITE duplication settings

SIP INVITE duplication settings	
Enable	<input type="checkbox"/>
Primary server IP-address	0.0.0.0
Primary server port	0
Secondary server IP-address	0.0.0.0
Secondary server port	0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

In this section, one can configure the reception of incoming INVITE requests with SMS text from the equipment of the emergency call service center and duplicating them on SMS receiving servers. The SMPP server parameters can be also configured here for receiving messages via the SMPP protocol and forwarding them to SMS receiving servers via SIP protocol.

Duplication is carried out as follows: after activating the option when receiving INVITE request via SIP interface with SMS text (determined by the presence in the message body with Content-Type: text/plain or Content-Type: multipart/mixed, where the content includes text/plain), SMG will redirect it to the duplication server via TCP protocol. To confirm the delivery, the server should respond the 403 Forbidden message. Any other release from the server will be treated as a duplication failure with issuing a corresponding alarm. After this, the call will end with a 403 Forbidden message.

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

- *Enable* – enable duplication of INVITE requests;



Duplication operates over the TCP protocol, so when enabling the option, it is necessary to configure the “Transport” setting in the General SIP configuration (see Common SIP settings so that operation over TCP is allowed (UDP-prefer, TCP-prefer or TCP-only).

- *Primary server IP-address* – primary server address;
- *Primary server port* – primary server port;
- *Secondary server IP-address* – secondary server address;
- *Secondary server port* – secondary server port;
- *SMS port* – port for receiving SMS via SMPP protocol. When this option is specified, SMG will accept connections via the SMPP protocol to the specified port and forward the received SMS messages to duplication servers via SIP protocol. Encoding of transmitted messages in text/plain will correspond to the encoding of the incoming message, it will be further specified by the Content-Type (charset parameter) and Content-Transfer-Encoding headers in the INVITE message.

Setting options for SIP profile

Call routing → SIP interfaces → Settings → SIP interface #1 → SIP protocol settings

SIP interfaces	
SIP interface settings	SIP protocol settings
Codecs/RTP settings	Fax/Modem settings
Extended SIP settings	
Options	
Keep-alive control	<input type="checkbox"/> 0
Keep-alive mode	SIP-OPTIONS
Register expires, min	300
Register expires, max	3600
Always transmit SDP in provisional responses	<input type="checkbox"/>
'In-band signal' with 183+SDP transmission	<input type="checkbox"/>
Local ring-back instead of early-media	<input type="checkbox"/>
Enable P-Early-Media (RFC5009)	<input type="checkbox"/>
Fill empty Display-Name	<input type="checkbox"/>
Send DisplayName in Remote-Party-ID header	<input checked="" type="checkbox"/>
Ignore RURI and To difference	<input type="checkbox"/>
Do not use plus sign in CdPN and Diversion	<input type="checkbox"/>
Diversion header with SIP URI	<input type="checkbox"/>
Enable redirection (302) processing	<input type="checkbox"/>
Enable REFER processing	<input type="checkbox"/>
Enable Re-INVITE with a=sendonly processing	<input type="checkbox"/>
Reliable provisional responses (1xx)	off
DSCP for signaling	0
Transit SIP header	<input type="checkbox"/>
Max forwarding count between subscribers	5
NAT settings	
NAT (comedia mode)	<input type="checkbox"/>
Transmit SDP in 18x messages	<input type="checkbox"/>
VIA and IP-address match control	<input type="checkbox"/>
SIP-session timers (RFC 4028)	
Enable	<input type="checkbox"/>
Session Expires	0
Min SE	0
Refresher side	Client
Upper registration settings	
Upper registration interface	not set
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	


- *Keep-alive control* – a function that controls the direction availability (NAT keep-alive) using the SIP-OPTIONS, SIP-NOTIFY or empty UDP method. The parameter determines the request transmission period and takes values from the range 30–3600 s;

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



These methods are also used to maintain the NAT connection.

- *Register expires, min* – minimum registration time value of expires;
- *Register expires, max* – maximum registration time value of expires;
- *Always transmit SDP in provisional responses* – allows for early connection of the voice path. For example, if the flag is unchecked, then SMG sends a 180 response without SDP session description, based on this response, the outgoing party plays a ringback, when the flag is checked, SMG sends a 180 response with SDP session description, and the ringback is played by the incoming party;
- *'In-band signal' with 183+SDP transmission* – issues SIP-reply 183 with SDP session description for voice path forwarding upon receipt of the CALL PROCEEDING or PROGRESS messages from ISDN PRI that contain the progress indicator = 8 (in-band signal);
- *Local ringback instead of early-media* – when the early media marker is received from the outgoing leg, ringback tone will be played to the caller instead of the inband voice message;
- *Enable P-Early-Media (RFC5009)* – use the P-Early-Media header described in RFC 5009. With outgoing call, the device will transmit the P-Early-Media: supported header in the INVITE. Upon receiving INVITE with P-Early-Media: supported marker, the response 18X messages will contain the P-Early-Media header: sendrecv;
- *Fill empty Display-Name* – when this option is checked, if a call with the missing display-name is received, SMG will fill it with the user name (number) taken from the URI;
- *Send DisplayName in Remote-Party-ID header* – enables/disables substitution of DisplayName in Remote-Party-ID;
- *Ignore RURI and To difference* – disables issuing the Redirecting and Original Called numbers in SS7 calls when the values in SIP RURI and To fields are different;
- *Do not use plus sign in CdPN and Diversion* – disables addition of '+' to a number, for International number type;
- *Diversion header with SIP URI* – uses SIP URI in the Diversion header instead of TEL URI;
- *Enable redirection (302) processing* – when this option is checked, the gateway is allowed to perform forwarding upon receipt of reply 302 from this interface. When unchecked and reply 302 is received, the gateway will reject the call and perform forwarding;

- *Enable REFER processing* – a REFER request is sent by the communicating gateway to enable the *Call Transfer* service. When this option is checked, the gateway is allowed to process REFER requests received from this interface. When unchecked, the gateway clears back the call upon receipt of a REFER request and does not provide the *Call Transfer* service;
- *Enable Re-INVITE with a=sendonly processing* – when this option is checked, it allows a call to be put on hold when the Re-INVITE message is received with a=sendonly marker in SDP;
- *Reliable provisional responses (1xx)* – when this option is checked, the INVITE request and 1xx class provisional responses will contain the *require: 100rel* option, which requires assured confirmation of provisional responses:
 - *off* – reliable delivery of provisional responses is disabled;
 - *support* – the INVITE request and 1xx class provisional responses will contain the *support: 100rel* option;
 - *require* – the INVITE request and 1xx class provisional responses will contain the *require: 100rel* option, which requires assured confirmation of provisional responses;
- *DSCP for signaling* – a service type (DSCP) for SIP signalling traffic;
 -  *DSCP for RTP and DSCP for SIP* settings will be ignored when using VLAN for RTP transmission and signaling. To prioritize traffic in this case there will be used Class of Service VLAN.
- *Transit SIP header* – enables transit of the received SIP headers into the outbound leg;
- *Max forwarding count between subscribers* – maximum possible number of consecutive forwardings between subscribers, default value is 5.

NAT settings

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

SIP Session Timers (RFC 4028)

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

Upper registration settings (this block of settings is available for SIP profile only):

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

Setting options for SIP-Q

SIP interface settings	SIP protocol settings	Codecs/RTP settings	Fax/Modem settings	Extended SIP settings
Options				
Keep-alive control	<input type="checkbox"/>	0		
Keep-alive mode	SIP-OPTIONS			
DSCP for signaling	<input type="checkbox"/>	0		
Transit SIP header	<input type="checkbox"/>			
SIP-session timers (RFC 4028)				
Enable	<input checked="" type="checkbox"/>			
Session Expires	1800			
Min SE	90			
Refresher side	Client			
SIP INVITE duplication settings				
Enable	<input type="checkbox"/>			
Primary server IP-address	0.0.0.0			
Primary server port	0			
Secondary server IP-address	0.0.0.0			
Secondary server port	0			
Apply		Cancel		

- *Keep-alive control* – a function that controls the direction availability (NAT keep-alive) using the SIP-OPTIONS, SIP-NOTIFY or empty UDP method. The parameter determines the request transmission period and takes values from the range 30–3600 s;
- *Keep-alive mode*:
 - *SIP-OPTIONS* – at specified opposite party control intervals, the device will send the OPTIONS control message. This message should receive a response from the opposite party; if no response is received, the direction is considered unavailable, and the failure status is registered in the device;
 - *SIP-NOTIFY* – the device will send the NOTIFY control message at specified opposite party control intervals. This message should receive a response from the opposite party; if no response is received, the direction is considered unavailable, and the failure status is registered in the device;
 - *UDP-CRLF* – device will send an empty UDP packet at specified opposite party control intervals; the opposite party response to an empty UDP packet is not applicable; consequently, the failure status will not be initiated on the device.



These methods are also used to maintain the NAT connection.

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



DSCP for RTP and DSCP for SIP settings will be ignored when using VLAN for RTP transmission and signaling. To prioritize traffic in this case there will be used *Class of Service VLAN*.

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

SIP-session timers (RFC 4028)

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

SIP INVITE duplication settings

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

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

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

- *Enable* – activate INVITE requests duplication;



Duplication operates over the TCP protocol, so when enabling the option, it is necessary to configure the “Transport” setting in the General SIP configuration (see Common SIP settings so that operation over TCP is allowed (UDP-prefer, TCP-prefer or TCP-only).

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

4.1.5.3.1.3 'Codecs/RTP settings' tab

Call routing → SIP interfaces → Configuration → → Codecs/RTP settings


SIP Interfaces

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

Options	On	Codec	PType	PTE
VAD / CNG <input type="checkbox"/>	<input checked="" type="checkbox"/>	G.711A	8	20
Source IP:Port verification <input type="checkbox"/>	<input checked="" type="checkbox"/>	G.711U	0	20
Echo-cancellation <input type="checkbox"/> off	<input type="checkbox"/>	G.729	18	20
DSCP for RTP <input type="checkbox"/> 0	<input type="checkbox"/>	G.723.1 (5.3 kbps)	4	30
RTP-loss timeout <input type="checkbox"/> 0	<input type="checkbox"/>	G.723.1 (6.3 kbps)	4	30
RTP-loss timeout after Silence-Suppression indication <input type="checkbox"/> X 0	<input type="checkbox"/>	G.726-32	102	20
RTCP period (sec) <input type="checkbox"/> 0	<input type="checkbox"/>	CLEARMODE	103	30
RTCP activity control <input type="checkbox"/> 0	↑ ↓			
Clear Channel override <input type="checkbox"/>				
Clear Channel transit <input type="checkbox"/>				
Video processing <input type="checkbox"/> off				
Digital gain				
Rx gain (0.1 dB) <input type="checkbox"/> 0				
Tx gain (0.1 dB) <input type="checkbox"/> 0				
AGC (Auto Gain Control)				
Compliance with ITU-T G.169 <input type="checkbox"/>				
Rx gain settings				
AGC master enable <input type="checkbox"/>				
Limit gain during doubletalk <input type="checkbox"/>				
Signal Reference Level, dBm0 <input type="checkbox"/> -19				
Signal Maximum Gain, dB <input type="checkbox"/> 40				
Signal Minimum Gain, dB <input type="checkbox"/> -40				
Tx gain settings				
AGC master enable <input type="checkbox"/>				
Limit gain during doubletalk <input type="checkbox"/>				
Signal Reference Level, dBm0 <input type="checkbox"/> -19				
Signal Maximum Gain, dB <input type="checkbox"/> 40				
Signal Minimum Gain, dB <input type="checkbox"/> -40				
Dual-Tone Multi-Frequency signalling settings				
DTMF transport <input type="checkbox"/> inband				
RFC2833 PT <input type="checkbox"/> 101				
RFC2833: same PT <input type="checkbox"/>				
DTMF MIME Type <input type="checkbox"/> application/dtmf				
Jitter buffer settings				
Mode <input type="checkbox"/> Dynamic				
Minimum size, ms <input type="checkbox"/> 0				
Initial size, ms <input type="checkbox"/> 0				
Maximum size, ms <input type="checkbox"/> 200				
Adaptation period, ms <input type="checkbox"/> 10000				
Removal mode <input type="checkbox"/> Soft				
Removal threshold, ms <input type="checkbox"/> 500				
Adjustment mode <input type="checkbox"/> Smooth				
Size for VBD, ms <input type="checkbox"/> 0				

Options

- *Voice activity detector / Comfort noise generator (VAD/CNG)* — when checked, silence detector and comfort noise generator are enabled. Voice activity detector disables transmission of RTP packets during periods of silence, reducing loads in data networks;
- *Source IP: Port verification* — when this setting is checked, control of media traffic received from IP address and UDP port specified in SDP communication session description will be enabled; otherwise the traffic from any IP address and UDP port will be accepted;
- *Echo cancellation* — echo cancellation mode:
 - *voice(default)* — echo cancellers are enabled in the voice data transmission mode.
 - *voice nlp-off* — echo cancellers are enabled in voice mode, non-linear processor (NLP) is disabled. When signal levels on transmission and reception significantly differ, weak signal may become suppressed by the NLP. Use this echo canceller operation mode to prevent the signal suppression.
 - *modem* — echo cancellers are enabled in the modem operation mode (direct component filtering is disabled, NLP control is disabled, CNG is disabled).
 - *voice nlp-option 1* — echo cancellers are enabled in the voice mode, non linear processor NLP is enabled in the mode of less intensive effect on a signal than by default;
 - *voice nlp-option 2* — echo cancellers are enabled in the voice mode, non linear processor NLP is enabled in the mode of more intensive effect on a signal than by default;
 - *off* — do not use echo cancellation (this mode is set by default).
- *DSCP for RTP* — service type (DSCP) for RTP and UDPTL (T.38) packets;



The DSCP setting for RTP and DSCP setting for SIP will be ignored while using VLAN for RTP transmission and signalling. *Class of Service VLAN* is used for prioritization in this case.
- *RTP loss timeout* — voice frequency path status control function that monitors the presence of RTP traffic from the communicating device. Permitted value range is from 10 to 300sec. When unchecked, RTP control is disabled; when checked, it is enabled. Control is performed as follows: if there are no RTP packets coming from the opposite device for the duration of the timeout and the last packet was not a silence suppression packet, the call will be rejected;
- *RTP loss timeout after Silence-Suppression indication* — RTP packet timeout for the silence suppression option utilization. Permitted value range is from 1 to 30. Coefficient is a multiplier that applies to the '*RTP packet timeout*' value. Control is performed as follows: if there are no RTP packets coming from the opposite device for the duration of the timeout and the last packet was a silence suppression packet, the call will be rejected;
- *RTCP period (sec.)* — time period in seconds (5-65535 s), after which the device send control packets via RTCP protocol. When unchecked, RTCP will not be used;
- *RTCP activity control* — voice frequency path status control function, may take up values in the range 2–255. Quantity of time periods (RTCP timer) during which the opposite party will wait for RTCP protocol packets. When there are 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*** seconds. When unchecked, feature will be disabled
 - *Clear Channel* — channel established for the transparent digital data transfer; when this channel is established, the device will not attempt to recode it and will transfer it transparently. To establish

such a connection, reception of '*Transmission Medium Requirement*' field is required with the following values:

- *restricted digital info (Q.931 protocol)*
 - *unrestricted dig.info (Q.931 protocol)*
 - *video (Q.931 protocol)*
 - *64 kbit/s unrestricted (SS7 protocol)*
- *Clear Channel override* — when checked, during 'clear channel' organization, a single codec CLEARMODE will be specified in SDP (if operation via Clear Channel was requested on the first call leg). When unchecked, the complete list of selected codecs will be always transferred to SDP in priority order.
 - *Clear Channel 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.
 - *Video processing* — this mode allows video traffic to pass transparently between clients.

Digital gain

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

AGC (Auto Gain Control)

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


Rx gain settings

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

Tx gain settings

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

Dual-Tone Multi-Frequency signalling settings:

- **DTMF transport** — method of DTMF transmission via IP network:
 - *inband* — in RTP packets, inband.
 - *RFC2833* — in RTP packets according to RFC2833 recommendation.
 - *SIP-INFO* — outband, via SIP, INFO messages are used; at that, DTMF signal appearance will depend on the MIME extension type.
 - *SIP-NOTIFY* — NOTIFY messages are used via SIP protocol and out-of-band. This DTMF transmission is an implementation of the method that is used on Cisco equipment.
 -  In order to be able to use extension dialing during the call, make sure that the similar DTMF tone transmission method is configured on the opposite gateway.
- **Allow inband DTMF** — this option is available for all DTMF transmission methods except *inband*. When this option is unchecked, if SMG receives dtmf in two formats, for example, RFC2833 and inband, then inband will be ignored and RFC2833 will be processed only;
- **Flash signal processing (RFC2833)** — checkbox that governs activation of FLASH signal processing using INFO, RFC2833, and re-invite methods for 'Call transfer' VAS operation;
- **RFC2833 PT** — type of payload used to transfer DTMF packets via RFC2833. Permitted values: 96 to 127. RFC2833 recommendation describes the transmission of DTMF via RTP protocol. This parameter should conform to the similar parameter of a communicating gateway (the most frequently used values: 96, 101);
- **RFC2833: same PT** — when checked, if SMG is the party that sends 'offer SDP', RFC2833 packets are expected for reception with PT value sent in 'answer SDP'; otherwise, RFC2833 packets are expected for reception with the same PT value that SMG has sent in 'offer SDP';
- **DTMF MIME Type** — specify payload type used for DTMF transmission in SIP protocol INFO packets:
 - *application/dtmf-relay* — in SIP INFO application/dtmf-relay packets ('*' and '#' are sent as symbols '*' and '#');
 - *application/dtmf* — in SIP INFO application/dtmf packets ('*' and '#' are sent as digits 10 and 11).

Jitter buffer parameters:

- **Mode** — jitter buffer operation mode: static or dynamic;
- **Minimum size, ms** — size of fixed jitter buffer or lower limit (minimum size) of adaptive jitter buffer. Permitted value range is from 0 to 200 ms;
- **Initial size, ms** — initial value of adaptive jitter buffer. Permitted value range is from 0 to 200 ms;
- **Maximum size, ms** — upper limit (maximum size) of adaptive jitter buffer, in milliseconds. Permitted value range is from 'Minimum size' to 200 ms;
- **Adaptation period, ms** — time of buffer adaptation to the lower limit without faults in packet sequence order;
- **Removal mode** — buffer adjustment mode. Defines the method of packet deletion during buffer adjustment to lower limit.
 - *Soft* — device uses intelligent selection pattern for deletion of packets that exceed the threshold;

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

Codecs

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

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

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



When VAD/CNG are enabled, G.729 codec operates as G.729B, otherwise as G.729A, 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.

4.1.5.3.1.4 Fax/Modem settings tab

Call routing → SIP interfaces → Configuration → → Fax/Modem settings

SIP interface settings	SIP protocol settings	Codecs/RTP settings	Fax/Modem settings	Extended SIP settings
Data transmission				
Enable VBD <input type="checkbox"/>				
VCodec for VBD <input type="text" value="G.711A"/>				
Payload type for VBD <input type="text" value="Static"/>				
Fax settings				
Fax detector mode <input type="text" value="no detect fax"/>				
Fax relay mode <input type="text" value="T.38"/>				
Fax relay max rate (bps) <input type="text" value="no limit"/>				
Fax relay rate management <input type="text" value="transferred TCF"/>				
T.38 data fill bits removal <input type="text" value="Off"/>				
T.38 data redundancy <input type="text" value="0"/>				
T.38 data packetization <input type="text" value="30 ms"/>				
T.38 data transit <input type="text" value="Off"/>				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

Data transmission

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

Fax settings

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



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

- *Fax relay mode* — select protocol for fax transmission;
- *Fax relay max rate (bps)* — maximum transfer rate of fax transmitted via T.38 protocol. This setting affects the ability of a gateway to work with high-speed fax units. If fax units support data transfer at 14400 baud, and the gateway is configured to 9600 baud, the maximum rate of connection between fax units and the gateway will be limited at 9600 baud. And vice versa, if fax units support data transfer at 9600 baud, and the gateway is configured to 14400 baud, this setting will not affect the interaction, maximum rate will be defined by the performance of fax units;
- *Fax relay rate management* — set the data transfer rate management method:
 - *local TCF* — method requires that the TCF tuning signal was generated locally by the recipient gateway. In general, used in T.38 transmission via TCP.
 - *transferred TCF* — method requires that the TCF tuning signal was sent from the sender device to the recipient device. In general, used in T.38 transmission via UDP.
- *T.38 data fill bits removal* — padding bit removals and inserts for data that does not relate to ECM (error correction mode);

- *T.38 data redundancy* — redundancy amount in T.38 data packets (amount of previous packets in the following T.38 packet). Introduction of redundancy allows to restore the transmitted data sequence on reception when packets were lost during transmission;
- *T.38 data packetization* — define T.38 packet generation frequency in milliseconds (ms). This option allows to adjust the size of a transmitted packet. If the communicating gateway is able to receive datagrams with max. size of 72 bytes (maxdatagramSize: 72), packetization time should be set to a minimum on SMG;
- *T.38 data transit* — when the call is performed using two SIP interfaces and T.38 fax transfer protocol is used by both interfaces, this setting allows to transit T.38 packets between interfaces with a minimum delay.

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

- 0 (DSCP 0x00, Diffserv 0x00) – standard forwarding (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 0x0C, Diffserv 0x30) – 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).

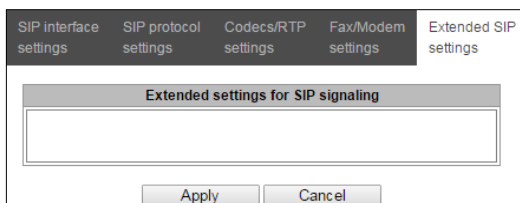
IP Precedence:

- 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).

4.1.5.3.1.5 Extended SIP settings

In this section, extended SIP settings are configured. These settings allow modifying SIP message fields using defined rules.

Call routing → SIP interfaces → Configuration →  → Extended SIP settings



Field entry format

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

where:

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

Modification rules

Modification rules are described by the following characters:

- \$ — keep the text that follows;
- ! — delete the remaining text;
- +(ABC) — add the text specified;
- -(ABC) — delete the text specified.

For implementation examples of operation rules, see Table 21 below.



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

Table 21 — Implementation examples of operation rules

Operation	Initial header	Rule	Result
Do not send the header	Accept: application/SDP	[sipheader:accept=disable]	
Transmit the header from the first leg without changes	Additional headers on the first leg: P-Asserted-Identity: <u>username@domain</u> Subject: Test call	[sipheader:[LIST_OF_MESSAGES]: [HEADER_MASK]=transit] [sipheader:[HEADER_MASK]=transit] In INVITE and 200 messages: [sipheader:INVITE,200:Subject=transit] In any messages: [sipheader:Subject=transit]	The defined header appears on the second leg: Subject: Test call

Transmit the group of headers from the first leg without changes	Additional headers on the first leg: P-Asserted-Identity: sip: username@domain P-Called-Party-ID: sip: username@domain Privacy: id Subject: Test call	[sipheader:P-*=transit] Note, that the following rule: [sipheader:*=transit] will not be operate, as the * character can replace only a part of a name.	The defined headers appear on the second leg: P-Asserted-Identity: sip: username@domain P-Called-Party-ID: sip: username@domain
Insert a header		[sipheader:insert[LIST_OF_HEADERS]: Remotelp=+(TEXT)] In all requests: [sipheader:insert:Remotelp=+(example.SMG)] In INVITE request: [sipheader:insert,INVITE:Remotelp=+(example.SMG)] Only in specified requests (e.g. INVITE and ACK): [sipheader:insert,INVITE,ACK:Remotelp=+(example.SMG)]	Remotelp:example.SMG
Add text at the beginning	Accept: application/SDP	[sipheader:accept=+(application/ISUP,)\$]	Accept: application/ISUP,application/ SDP
Add text at the end	Accept: application/SDP	[sipheader:accept=\$+(,application/ISUP)]	Accept: application/SDP,application / ISUP
Delete text	Accept: application/SDP,application/ISUP	[sipheader:accept=- (application/SDP,)\$]	Accept: application/ISUP
Delete beginning from the specific place	Accept: application/SDP,text/plain	[sipheader:accept=- (text)!]	Accept: application/SDP
Replace text completely	Accept: application/SDP	[sipheader:accept=+(application/ISUP)!]	Accept: application/ISUP
Replace text	Accept: application/SDP,text/plain	[sipheader:accept=- (SDP)+(ISUP)\$]	Accept: application/ISUP,text/plain
Replace text, discarding data at the end	Accept: application/SDP,text/plain	[sipheader:accept=- (SDP)+(ISUP)!]	Accept: application/ISUP,text/plain
Complete the text	To: "Ivanov A.A." <sip:123@eltex>	[sipheader:to=- (eltex)+(eltexdomain.loc)\$]	To: "Ivanov A.A." <sip:123@eltexdomain.loc>
Example of a complex modification	From: <sip:who@host>;tag=aBc	[sipheader:from=+(DISPLAY)-(who)+(12345)- (>)+(;user=phone>)\$+(;line=abc)]	From: DISPLAY <sip:12345@host;user=pho ne>;tag=aBc;line=abc
Do not transmit X-UniqueTag	X-UniqueTag: 12345678 90abcdef 12345678 90abcdef	[unique-tag=disable]	X-UniqueTag header is not transmitted
Transmit X-UniqueTag content in another title	X-UniqueTag: 12345678 90abcdef 12345678 90abcdef	[unique-tag=NewHeader- Name]	NewHeader-Name: 12345678 90abcdef 12345678 90abcdef
The option allows using TO instead of RURI for routing	Get:	[siprequest:cdpn=to]	Send:

	<pre>Request-Line: INVITE sip:558018@10.22.128.36:5060 SIP/2.0 ... To: <sip:73852245673@10.22.1.50;user=phone></pre>		<pre>Request-Line: INVITE sip:73852245673@10.22.120.40:5060 SIP/2.0 ... To: <sip:73852245673@10.22.120.40;user=phone></pre>
Enable sending history-info in the redirected call		[siprequest:history=true]	

Example

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

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



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

4.1.5.3.1.6 Obtaining Display Name from a third-party server via LDAP

To set up receiving Display Name from a third-party server, it is necessary to add a setting in the form line in the menu item 'Extended SIP settings'.

SMG polls the server(s) at a specified interval and stores the current name. When calling, names are requested for the initiator and destination. If there are no current ones in the database, then they are used default configured subscriber names (from SIP subscriber settings).

Configuration string format:

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

- *ID* – record identifier, for several interfaces there may be the same description, in this case the identifier should also be the same; in particular, it solves the issue duplication of records for sip profiles (when all users of the same profile will have the same record);
- *INTERVAL* – database update interval (minutes);
- *DIRECTION* – for which subscriber to use:
 - *sip* – value for From when calling from the SIP side and To when calling to the SIP side;
 - *exchange* – value for To when calling from the SIP side and From when calling to the SIP side;
 - * – both names are requested in one paragraph.
- *IP* – LDAP server address;
- *PORT* – LDAP server address:
 - * – for shortness, it can be specified instead of the usual LDAP port 389.
- *LOGIN* – database username;
- *PASSWORD* – database user password;
- *BASE* – path to the server subscriber database;
- *ATTRPHONE* – attribute describing in the database the number by which the name will be searched. The parameter is optional, may not be specified: default value: telephoneNumber;

- **ATTRDISPLAY** – attribute describing DisplayName in the database. The parameter is optional, may not be specified, default value: displayName.

Configuration string format:

Full entry:

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

Short entry:

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

4.1.5.3.1.7 Using user=phone in RURI

Setting:

```
[siprequest:user=phone]
```

[siprequest:user=ip] (instead of "ip" any value can be used, other than "phone").

Interface type	Setting	In RURI specify ;user=phone
trunk	no	yes
trunk	siprequest:user=phone	yes
trunk	siprequest:user=ip	no
user	no	no
user	siprequest:user=phone	yes
User	siprequest:user=ip	no

4.1.5.4 H323 interfaces

In this section, H.323¹ stack general configuration parameters, custom settings for each direction operating via H.323 protocol.

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

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

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

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

Call routing → H.323 interfaces

H.323 interfaces								
No	Name	Mode	TrunkGroup	Hostname / IP-address	Codecs	DTMF Type	Fax detect	VBD
0	H323-interface00	H323	нет		G.711A G.711U	Inband	No detect fax	off

Common H323 settings	
Device ID (H323 alias)	SMG1016M
GateKeeper settings	
GateKeeper	not used

Apply

Common H323 settings

- *Device ID (H323 Alias)* — gateway name during registration at the Gatekeeper;
- *Port for signaling* – a network interface for H.323 signaling;
- *Signaling Receive Port* – local TCP port for receiving H.323 signaling messages.

GateKeeper settings

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

Settings for 'remote' mode:

Call routing → H.323 interfaces → Remote mode

Common H323 settings	
Device ID (H323 alias)	SMG1016M
GateKeeper settings	
GateKeeper	remote
Network interface for signaling	eth0 (eth0 192.168.113.110)
Port for signaling	1720
Search GateKeeper	<input type="checkbox"/>
GateKeeper IP	0.0.0.0
GateKeeper Port	1719
Registration time	300
Keep-alive timeout	20

Apply

- *Network interface for signaling* – select a network interface for H.323 signaling;
- *Port for signaling* – local TCP port for receiving H.323 signaling messages;
- *Search GateKeeper* — when checked, automatic Gatekeeper discovery method will be used in multicast mode using IP address 224.0.1.41 and UDP port 1718, otherwise this method will not be used and the Gatekeeper will have a specific IP address;
- *GateKeeper IP* — identification of the gatekeeper at the specific IP;
- *GateKeeper Port* — gatekeeper UDP port (port 1719 is used by the majority of gatekeepers by default);

- *Registration time* — time period in seconds, for which the device will keep its registration on a gatekeeper;
- *Keep-alive timeout* — time period in seconds, after which the device will renew its registration on a gatekeeper



To reliably re-register a device to Gatekeeper, the re-registration period value 'Keep Alive Time' should be set to 2/3 of the 'Time To Live' registration period. In this case, it is recommended to configure the 'Time To Live' parameter the same as on Gatekeeper, so that the value of the 'Keep Alive Time' gateway re-registration period was not greater than or equal to the 'Time To Live' value sent in Gatekeeper responses. Otherwise, incorrect configuration may cause Gatekeeper to remove registration from the gateway before the gateway re-registers, which in turn 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 forcibly terminated, also H323-MODULE LOST fault may appear shortly.

Settings for 'local' mode¹:

Call routing → H.323 interfaces → Local mode


Common H323 settings	
Device ID (H323 alias)	SMG2016
GateKeeper settings	
GateKeeper	local
Network interface for signaling	bond1.1 (bond1.1 192.168.1.200)
Port for signaling	1720
Local subscribers	<input checked="" type="checkbox"/>
GateKeeper H.323 ID	myid
Default technology prefix	1#
DSCP for RAS	0
Primary Directory GateKeeper	
H.323 ID	id1
IP address	192.168.1.100
Secondary Directory GateKeeper	
H.323 ID	id2
IP address	192.168.1.101
Apply	

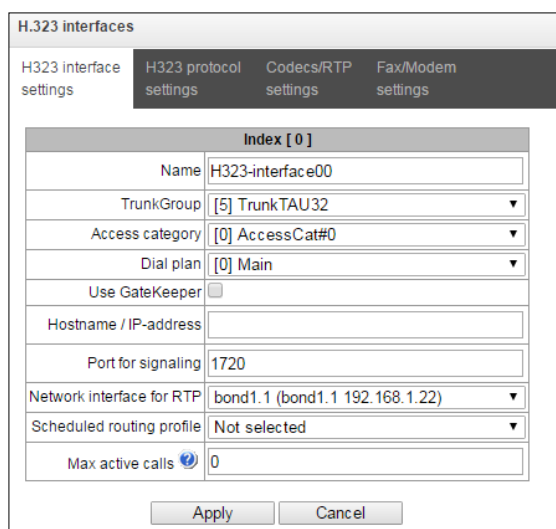
- *GateKeeper* – identifier of local Gatekeeper operating on SMG;
- *Network interface for signaling* – select a network interface for H.323 signaling;
- *Port for signaling* – local TCP port for receiving H.323 signaling messages;
- *Default technology prefix* – defines the default directions to which the GateKeeper will transmit calls returned from Directory GateKeeper and not intended for SMG SIP subscribers. The direction must be registered on a local GateKeeper of SMG;
- *DSCP for RAS* – type of service (DSCP) for signaling traffic (H.323 RAS);
- *Primary Directory Gatekeeper* and *Secondary Directory Gatekeeper* – settings for interaction with a main and redundant Directory Gatekeepers;
- *H.323 ID* – identifier of Directory Gatekeeper;
- *IP address* – IP address of Directory Gatekeeper.

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

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

4.1.5.4.1 H.323 interface settings tab


Call routing → H.323 interfaces →  → H.323 interface settings




H.323 interfaces	
H323 interface settings	H323 protocol settings
Index [0]	
Name	H323-interface00
TrunkGroup	[5] TrunkTAU32
Access category	[0] AccessCat#0
Dial plan	[0] Main
Use GateKeeper	<input type="checkbox"/>
Hostname / IP-address	
Port for signaling	1720
Network interface for RTP	bond1.1 (bond1.1 192.168.1.22)
Scheduled routing profile	Not selected
Max active calls	0


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

4.1.5.4.2 H.323 protocol settings tab


Call routing → H.323 interfaces →  → H323 protocol settings

H.323 interfaces	
H323 interface settings	H323 protocol settings
	<div style="display: flex; justify-content: space-between;"> Codecs/RTP settings Fax/Modem settings </div>
Options	
Device ID (H323 alias)	<input type="text"/>
Fast start	<input type="checkbox"/>
H245-tunnel	<input type="checkbox"/>
CISCO 1700 adaptation	<input type="checkbox"/>
Name coding	Transit ▼
Name transmission	Q931 DISPLAY ▼
DSCP for signaling 	<input type="text" value="0"/>
Number prefixes	
Prefix 1	<input type="text"/>
Prefix 2	<input type="text"/>
Prefix 3	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- *Device ID (H323 alias)* — gateway name during registration at the Gatekeeper;
- *Fast start* — when checked, fast start function is enabled, otherwise it is disabled. When option is used, session description for media channel establishing is performed via H.225 protocol, otherwise via H.245 protocol;
- *H245-tunnel* — when checked, H.245 signaling tunneling is enabled through the Q.931 signal channel, otherwise it is disabled;
- *CISCO 1700 adaption* — when using the option, it works as follows:
 - Bandwidth for Admission Request is set to 64000
 - For an outgoing call, the following is added:
 - remote alias with CgPN value;
 - local alias with H.323 ID Primary Directory Gatekeeper;
 - also local alias with the value 'Device Identifier (Alias)' from the general configuration of H323 is added to the above.
 - For an incoming call, search for an alternative H323 interface is not performed.
- *Name coding:*
 - *Transit* — no recoding is performed (by default, the name is assumed to be accepted in UTF-8);
 - *CP 1251* — coding of Windows-1251;
 - *Siemens adaptation* — coding of ATC Siemens;
 - *AVAYA adaptation* — coding of PBX AVAYA;
 - *Latin transliteration* — Russian names will be transliterated into Latin letters.

- *Name transmission:*
 - *Q931 DISPLAY* — transmission in Q.931 Display element with Codeset 5;
 - *AVAYA DISPLAY* – transmission in Q.931 Display element with Codeset 6;
 - *QSIG-NA* — transmission via QSIG-NA protocol (ECMA-164).
- *DSCP for signaling* — server type (DSCP) for signaling traffic (H.323);
 -  The *DSCP for RTP* and *DSCP for SIP* settings will be ignored while using VLAN for RTP transmission and signalling. *Class of Service VLAN* will be used for traffic prioritization in this case.
- *Number prefixes (Prefix 1, Prefix 2, Prefix 3)* – numbers, which SMG register on a Gatekeeper according to settings – local or remote. The table is filled with the numbers or initial digits of numbers of SIP subscribers registered on SMG in order to gatekeeper could forward calls to SMG (for example, it is sufficient to write the same prefix 10010 for subscribers with numbers 100101 and 100102).

4.1.5.4.3 RTP/codec configuration tab

Call routing → H.232 interfaces →  → Codecs/RTP settings

On	Codec	PType	PTE
<input checked="" type="checkbox"/>	G.711A	8	20
<input checked="" type="checkbox"/>	G.711U	0	20
<input type="checkbox"/>	G.729	18	20
<input type="checkbox"/>	G.723.1 (5.3 kbps)	4	20
<input type="checkbox"/>	G.723.1 (6.3 kbps)	4	30

Options:

- *Voice activity detector / Comfort noise generator (VAD/CNG)* — when checked, silence detector and comfort noise generator are enabled. Voice activity detector disables transmission of RTP packets during periods of silence, reducing loads in data networks.
- *Source IP: Port verification* — when this setting is checked, control of media traffic received from IP address and UDP port specified in SDP communication session description will be enabled; otherwise the traffic from any IP address and UDP port will be accepted;
- *Echo cancellation* — echo cancellation mode:
 - *voice (default)* — echo cancellers are enabled in the voice data transmission mode;
 - *voice nlp-off* — echo cancellers are enabled in voice mode, non-linear processor (NLP) is disabled. When signal levels on transmission and reception significantly differ, weak signal may become suppressed by the NLP. Use this echo canceller operation mode to prevent the signal suppression;
 - *modem* — echo cancellers are enabled in the modem operation mode (direct component filtering is disabled, NLP control is disabled, CNG is disabled);
 - *voice nlp-option 1* — echo cancellers are enabled in the voice mode, non linear processor NLP is enabled in the mode of less intensive effect on a signal than by default;
 - *voice nlp-option 2* — echo cancellers are enabled in the voice mode, non linear processor NLP is enabled in the mode of more intensive effect on a signal than by default;
 - *off* — do not use echo cancellation (this mode is set by default).
- *Rx gain (0.1 dB)* — volume of signal received, gain of the signal received from the communicating gateway;

- *Tx gain (0.1 dB)* — volume of signal transmitted, gain of the signal transmitted to the communicating gateway direction;
- *DSCP for RTP* — service type (DSCP) for RTP and UDPTL (T.38) packets.



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

- *RTP-loss timeout* – the function that controls the presence of RTP traffic from interacting device on a voice-frequency path. The permissible values are from 10 to 300 seconds. When unchecked, RTP control is disabled, when checked – enabled. The control is implemented as follows: if during the set timeout there is no RTP packets received and the last packet was not the packet of pause suppression, the call will be released;
- *RTP-loss timeout after Silence-Suppression indication (coefficient)* – timeout for RTP packets when using the option of pause suppression. The permissible values are from 1 to 30. The coefficient defines how many times this value greater than RTP-loss timeout. The control is implemented as follows: if there is no RTP packets received and the last packet was the packet of pause suppression, the call will be released;
- *RTCP period (sec)* — time period in seconds (5–65535), after which the device sends control packets via RTCP protocol. When unchecked, RTCP will not be used;
- *RTCP activity control* — voice frequency path status control function, may take up values in the range 2–255 seconds. Quantity of time periods (RTCP timer) during which the opposite party will wait for RTCP protocol packets. When there are 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.

Dual-Tone Multi-Frequency signaling settings:

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



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

- *RFC2833 PT* — type of payload used to transfer DTMF packets via RFC2833. Permitted values: 96 to 127. RFC2833 recommendation describes the transmission of DTMF via RTP protocol. This parameter should conform to the similar parameter of a communicating gateway (the most frequently used values: 96, 101).
- *RFC2833: same PT* – when checked, if SMG is an initiating side of connection, RFC2833 packets with PT value which has been transmitted by OpenLogicalChannelAck, are expected to be received.



Otherwise, the RFC2833 with the PT value, which has been transmitted in OpenLogicalChannelAck request by SMG, are expected to be received.

Jitter buffer settings:

- *Mode* — jitter buffer operation mode: static or dynamic;
- *Minimum size, ms* — size of fixed jitter buffer or lower limit (minimum size) of adaptive jitter buffer. Permitted value range is from 0 to 200 ms;
- *Initial size, ms* — initial value of adaptive jitter buffer. Permitted value range is from 0 to 200ms.
- *Maximum size, ms* — upper limit (maximum size) of adaptive jitter buffer, in milliseconds. Permitted value range is from 'Min size' to 200 ms;
- *Adaptation period, ms* — time of buffer adaptation to the lower limit without faults in packet sequence order;
- *Removal mode* — buffer adjustment mode. Defines the method of packet deletion during buffer adjustment to lower limit:
 - *Soft* — device uses intelligent selection pattern for deletion of packets that exceed the threshold;
 - *Hard* — packets which delay exceeds the threshold will be deleted immediately.
- *Removal threshold, ms* — threshold for immediate deletion of a packet, in milliseconds. When buffer size grows and packet delay exceeds this threshold, packets will be deleted immediately. Permitted value range is from 'Max size' to 500 ms.
- *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 200 ms.


Codecs:

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

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

- *On* — when checked, use a codec specified in the adjacent field;
- *Codec* — codec, used for voice data transmission. Supported codecs: G.711A, G.711U, G.729A, G.729B, G.723.1.
 - When VAD/CNG are enabled, G.729 codec operates as G.729B, otherwise as G.729A, 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.

4.1.5.4.4 Fax/Modem settings tab

Call routing → H.232 interfaces →  → Fax/Modem settings

H.323 interfaces	
H323 interface settings	H323 protocol settings
Fax/Modem settings	
Modem settings	
Enable VBD	<input type="checkbox"/>
Codec for VBD	G.711A
Payload type for VBD	Static
Fax settings	
Fax detector mode	no detect fax
Fax relay mode	T.38
Fax relay max rate (bps)	no limit
Fax relay rate management	transferred TCF
T.38 data fill bits removal and insertion	Off
T.38 data redundancy	0
T.38 data packetization	30 ms
T.38 data transit	Off
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Modem settings:

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

Fax settings:

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



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

- *Fax relay mode* — select protocol for fax transmission;
- *Fax relay max rate (bps)* — maximum transfer rate of fax transmitted via T.38 protocol. This setting affects the ability of a gateway to work with high-speed fax units. If fax units support data transfer at 14400 baud, and the gateway is configured to 9600 baud, the maximum speed of connection between fax units and the gateway will be limited at 9600 baud. And vice versa, if fax units support data transfer at 9600 baud, and the gateway is configured to 14400 baud, this setting will not affect the interaction, maximum speed will be defined by the performance of fax units;
- *Fax relay rate management* — set the data transfer speed management method:
 - *local TCF* — method requires that the TCF tuning signal was generated locally by the recipient gateway. In general, used in T.38 transmission via TCP;
 - *transferred TCF* — method requires that the TCF tuning signal was sent from the sender device to the recipient device. In general, used in T.38 transmission via UDP.
- *T.38 data fill bits removal and insertion* — padding bit removals and inserts for data that does not relate to ECM (error correction mode);
- *T.38 data redundancy* — redundancy amount in T.38 data packets (amount of previous packets in the following T.38 packet). Introduction of redundancy allows to restore the transmitted data sequence on reception when packets were lost during transmission;
- *T.38 data packetization* — define T.38 packet generation frequency in milliseconds (ms). This option allows to adjust the size of a transmitted packet. If the communicating gateway is able to receive datagrams with max. size of 72 bytes (maxdatagramSize: 72), packetization time should be set to a minimum on SMG;
- *T.38 data transit* — when the call is performed using two VoIP interfaces and T.38 fax transfer protocol is used by both interfaces, this setting allows to transit T.38 packets between interfaces with a minimum delay.




4.1.5.5 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.

Call routing → Trunk Directions

No	Name	TrunkGroup list	TrunkGroup selection order	Local direction
0	Direction #0	TrunkAsterisk, TrunkSMG1016m_out, TrunkSST_00, 931_out	Starting from first forward	

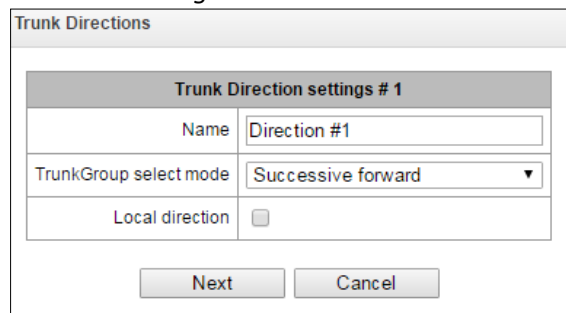
To create, edit or remove trunk directions, use 'Objects' — 'Add object', 'Objects' — 'Edit object' and 'Objects' — 'Remove object' menus and the following buttons:

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



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

Call routing → Trunk Directions → 

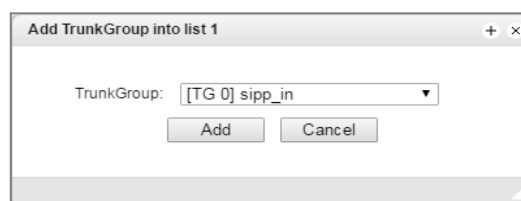


The screenshot shows a dialog box titled "Trunk Directions". Inside, there is a section titled "Trunk Direction settings # 1". It contains three input fields: "Name" with the value "Direction #1", "TrunkGroup select mode" with a dropdown menu set to "Successive forward", and "Local direction" with an unchecked checkbox. At the bottom, there are "Next" and "Cancel" buttons.

- *Name* — trunk direction name;
- *TrunkGroup select mode* — trunk group selection order in the direction:
 - *Successive forward* — all trunk groups comprising the direction are selected in turns beginning from the first in the list;
 - *Successive backward* — all trunk groups comprising the direction are selected in turns beginning from the last in the list;
 - *Starting from first forward* — the first free trunk group comprising the direction is selected beginning from the first in the list;
 - *Starting from last backward* — 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 in this direction are placed under SORM control with the type and sign of the number 'subscriber of this station'.

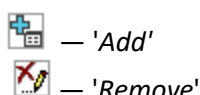
List of trunk groups in direction:



Call routing → Trunk Directions →  → Trunk Direction settings # 0 → 




The screenshot shows a dialog box titled "Add TrunkGroup into list 1". It has a "TrunkGroup:" label followed by a dropdown menu showing "[TG 0] sipp_in". Below the dropdown are "Add" and "Cancel" buttons.

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



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

4.1.5.6 V5.2 interfaces

The menu is dedicated to V5.2 interface parameters configuration. To add a new interface into the configuration, click  in the left screen part with highlighted 'V5.2 Interfaces'. The quantity of created interfaces should be equal to the quantity of outstations.

4.1.5.6.1 Interface settings

Call routing → V5.2 interface → Interface selection → Interface settings

- *Name* — displayed interface name;
- *Primary E1 stream* — primary stream for V5.2 interface;
- *Secondary E1 stream* — secondary stream for V5.2 interface;
- *Interface ID* — interface identifier;
- *Variant ID* — provision option in the initial configuration;
- *C-chan ID* — logical C-channel identifier;
- *PSTN link* — stream number to which the PSTN protocol will be assigned;
- *PSTN ts* — CI number to which the PSTN protocol will be assigned;
- *Link identification* — checking the compliance of E1 ID paths on the LE and AN sides during launching the interface;
- *Accelerated port alignment* — using an accelerated port unlocking mechanism (Accelerated Port Alignment) during interface startup. Possible accelerated port alignment parameters:
 - *PSTN&ISDN* — PSTN and ISDN port alignment;
 - *PSTN* — PSTN port alignment.
- *Alarms* — when checked, the alarm message will be displayed;
- *RADIUS profile* — selection of RADIUS profile for the interface.

— 'Add E1 stream'

When adding a new E1 stream it is necessary to specify its LinkID in the field opposite the drop-down streams list.

To change the order of E1 streams in the list, use the arrows (down, up).

4.1.5.6.2 Subscribers list


This section is intended for binding created V5.2 subscribers to this V5.2 interface. Each cell for a subscriber contains a “Layer 3 address”, which is unique within one interface.

V5.2 Interfaces

Interface settings
Subscribers list

№	L3 Address	Subscriber ID	Subscriber name	Subscriber number	Select
10					<input type="checkbox"/>

10 Rows in the table to show



- *№* — subscriber sequence number;
- *L3 Address* — Layer 3 address required for subscriber identification within V5.2 interface;
- *Subscriber ID* — unique subscriber identifier;
- *Subscriber name* — subscriber name;
- *Subscriber number* — subscriber phone number.

To edit the list, use the buttons:


- *Add* — add V5.2 subscriber;
- *Swap selected* — swap places of two selected subscribers;
- *Clear selected* — delete the number binding (cell content);
- *Delete selected* — delete the subscriber (the cell completely).

4.1.5.7 SIP-Trunk Registrations

4.1.5.7.1 Settings

SIP-Trunk Registrations → Registrations → Settings

SIP-Trunk Registrations			
Settings		Monitoring	
No	Login	Username/Number	SIP-domain
0	200	200	
1	201	201	



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

Registration settings:

- *Login* — name used for authentication;
- *Password* — password for authentication;
- *Username/Number* — user number registered in the SIP domain;
- *SIP-domain* — the domain in which the subscriber is registered on the upstream server.

In the list of SIP interfaces, registration binding to a specific SIP interface is assigned/removed. This allows one to define a list of subscribers who are allowed to make calls via this interface.

4.1.5.7.2 Monitoring

When selecting the '*Monitoring*' item in the drop-down list, a table for monitoring is displayed subscriber registration on the upstream server.

SIP-Trunk Registrations → Registrations → Monitoring

SIP-Trunk Registrations						
Settings		Monitoring				
No	Login	User name/number	SIP interface list	Status	Reason	Expire in
0						
1						

- *Login* — name used for authentication;
- *Username/Number* — user number registered on the upstream server;
- *SIP interface list* — list of interfaces through which the subscriber access is allowed to;
- *Status* — subscriber registration status (registered, not registered, registration expired);
- *Reason* — possible reason for lack of registration;
- *Expire in* — time remaining until registration expires.

4.1.6 Subscribers

The menu is intended to configure the parameters of SIP subscribers (it is available only in the software version with a SIP registrar license, more information about licenses in section Licenses).

4.1.6.1 SIP Subscribers

4.1.6.1.1 Configuration of SIP subscribers

Subscribers → SIP Subscribers → Configuration

SIP Subscribers

Configuration Monitoring VAS management BLF Monitoring

Search subscriber

No	ID	Title	Number	Dial plan	Calling party category (RUS)	IP/Port	SIP domain	SIP profile	Authorization	Select
0	1	Subscriber#000	10	[0] NumberPlan#0	1	0.0.0.0:0		any	Without auth	<input type="checkbox"/>
1	2	Subscriber#001	11	[0] NumberPlan#0	1	0.0.0.0:0		any	Without auth	<input type="checkbox"/>
2	3	Subscriber#002	12	[0] NumberPlan#0	1	0.0.0.0:0		any	Without auth	<input type="checkbox"/>
3	4	Subscriber#003	13	[0] NumberPlan#0	1	0.0.0.0:0		any	Without auth	<input type="checkbox"/>
4	5	Subscriber#004	14	[0] NumberPlan#0	1	0.0.0.0:0		any	Without auth	<input type="checkbox"/>
5	6	Subscriber#005	15	[0] NumberPlan#0	1	0.0.0.0:0		any	Without auth	<input type="checkbox"/>
6	7	Subscriber#006	16	[0] NumberPlan#0	1	0.0.0.0:0		any	Without auth	<input type="checkbox"/>
7	8	Subscriber#007	17	[0] NumberPlan#0	1	0.0.0.0:0		any	Without auth	<input type="checkbox"/>
8	9	Subscriber#008	18	[0] NumberPlan#0	1	0.0.0.0:0		any	Without auth	<input type="checkbox"/>
9	10	Subscriber#009	19	[0] NumberPlan#0	1	0.0.0.0:0		any	Without auth	<input type="checkbox"/>

10 Rows in the table to show Current page 1 from 9

Selected: 0

Search subscriber — checking the presence of a subscriber in the database of configured SIP subscribers, it is possible to check by name, number, callerID, IP address: Port, SIP domain, SIP profile, PBX profile and dial plans;

- *Edit selected* — pressing the button takes you to the group menu editing parameters of selected subscribers (opposite to which the flag is set 'Select'). To be able to edit, set the 'Edit' flag opposite the required parameter. A description of the parameters for configuration is given below;
- *Remove selected* — pressing the button allows to delete a group of selected subscribers.

To create, edit and delete an individual subscriber record, use the 'Objects' menu – 'Add object', 'Objects' – 'Edit object' and 'Objects' – 'Delete object', and also buttons:

- 'Add subscriber'
- 'Edit subscriber parameters'
- 'Remove subscriber'

4.1.6.1.1.1 SIP Subscribers

Subscribers → SIP subscribers → Configuration → 

SIP subscriber	
Subscribers count	1 <small>Max subscribers count 1407.</small>
Starting description	Subscriber#590
Starting number	
Starting CallerID number	
Use CallerID number for redirection	<input type="checkbox"/>
Calling party number type	Subscriber
Calling party category (RUS)	1
Lines operation mode	Common
Lines number	1
Redirecting lines number	0
IP-address:port	0.0.0.0 : 0
Allow unregistered calls	<input type="checkbox"/>
SIP domain	
SIP profile	any
PBX profile	[0] PBXprofile#0
Access category	[0] AccessCat#0
Dial plan	[0] NumberPlan#0
Authorization	not set
Login	
Password	
Ignore source port after registration	<input type="checkbox"/>
Subscriber service mode	On
Display name	
Use display name	Received only

- *Subscribers count* — number of subscribers;
- *Starting description* — free text description of subscribers;
- *Starting number* — subscriber number for a group of subscribers, each subsequent subscriber will be assigned a number increased by one;
- *Starting CallerID number* — subscriber's Caller ID number, for a group of subscribers to each subsequent number increased by one will be assigned;
- *Use CallerID number for redirection* — when using redirections, the caller ID number will be substituted into the Diversion or Redirecting number fields instead of the subscriber number;
- *Calling party number type* — subscriber number type;
- *Calling party category* — CallerID category;

- *Lines operation mode* — operating mode limiting the number of simultaneous calls. It can take two values: 'Combined' and 'Separate'. In the first mode, the total number of simultaneous calls involving the subscriber, in the second mode incoming and outgoing calls are counted separately;
- *Lines number* — number of simultaneous calls involving the subscriber. This field is displayed if the 'Combined' line operation mode is selected. Acceptable values [1;255] or 0 – no restrictions;
- *Ingress lines number* — number of simultaneous incoming calls to a subscriber. The field is displayed if the 'Separate' line operation mode is selected. Acceptable range [1;255] or 0 – no restrictions;
- *Egress lines number* — number of simultaneous outgoing calls from a subscriber. The field is displayed if the 'Separate' line operation mode is selected. Acceptable range [1;255] or 0 – no restrictions;
- *Redirecting lines number* — number of simultaneous calls when redirecting. Acceptable range [1;255] or 0 – no restrictions;
- *IP-address: port* — IP address and port of the subscriber. When setting the value 0.0.0.0, the subscriber is allowed to register from any IP address. Setting the port to zero ignores the port with which registration comes;
- *Allow unregistered calls* — option becomes active only if in the 'IP-address:Port' both the address and port of the subscriber are specified. When the flag is set, the subscriber will be able to do calls without prior registration from the specified IP and port. This option does not work if sip profile 'Any' is selected;
- *SIP domain* — determines whether a subscriber belongs to a specific domain. Sent by the gateway subscriber in the 'host' parameter of the SIP URI scheme of the *from* and *to* fields;
- *SIP profile* — selecting a SIP profile. The SIP profile determines most of the subscriber's settings. If you select the 'Any' profile, this will make it possible to register a SIP subscriber to any from the available SIP profiles in the system (see section 4.1.5.3 SIP/SIP-T/SIP-I, SIP-profiles);
- *PBX profile* — PBX profile selection (see 4.1.7.5 PBX profiles);
- *Access category* — access category selection;
- *Dial plan* — dial plan in which the subscriber will be located;
- *Authorization* — authentication mode for the device:
 - *Not set* — authentication is disabled;
 - *With Register* — authentication is carried out only during registration — upon REGISTER request;
 - *With Register and Invite* — authentication is carried out both during registration and during making outgoing calls – based on REGISTER and INVITE requests.
- *Login* — username for authentication;
- *Password*— password for authentication;
- *Ignore source port after registration* — after registration, the messages from subscribers can come from any port of the registered address;
- *Subscriber service mode* — sets a limit on incoming and outgoing communications to the subscriber:
 - *off*: The subscriber number will be present in the dial plan, but the subscriber's terminal will not be able to register. Respectively incoming calls will be rejected with the 'out of order' reason, outgoing calls will not be able to be initiated;
 - *on*: disabled, all types of communication are available;
 - *off 1*: there is incoming communication, outgoing communication is only to special services;
 - *off 2*: there is no incoming communication, outgoing communication is only to special services;
 - *denied 1*: complete deny on incoming and outgoing traffic. Calls will be routed via dial plan, but will be rejected;
 - *denied 2*: complete deny on incoming and outgoing traffic except for special services;
 - *denied 3*: incoming calls are prohibited, outgoing calls are allowed;
 - *denied 4*: incoming calls are prohibited, outgoing calls are allowed only within local and department networks;

- *denied 5*: incoming calls are allowed, outgoing calls are completely prohibited;
- *denied 6*: incoming calls are allowed, outgoing calls are allowed only to special services;
- *denied 7*: incoming calls are allowed, outgoing calls are allowed for local and department networks;
- *denied 8*: incoming calls are allowed, outgoing calls are allowed only within the local, department and zone networks;
- *ignore*: excluded from numbering. The number is completely excluded from subscriber numbers of a dial plan. When calling this number, the call will be rejected due to no route to destination or will go to a suitable prefix in the dial plan.
- *Display name* — the name that will be passed to display-name. The parameter also affects using display-name as the Connected Name in responses to calls to the subscriber;
- *Use display name* – mode of using display-name (SIP display-name). It can take the values:
 - *Received only* — ‘Display name’ setting will not be used, display-name will always take the value that was in the initiating INVITE;
 - *Received prefer* — if a subscriber receives a call initiation request without a display-name, then the display-name will be filled in with what is configured for SMG. Otherwise, the received display-name will be used;
 - *Configured only* — regardless of what came in the subscriber's request, display-name set to SMG will be used.

Multiple registration (SIP-forking)

Multiple registration (SIP-forking)	
SIP-forking	<input type="checkbox"/>
Max registered contacts number	<input type="text" value="2"/>
Busy-Lamp-Field (BLF) settings	
Enable subscription	<input type="checkbox"/>
Max subscribers number	<input type="text" value="10"/>
Monitoring group	<input type="text" value="0"/>
Intercom call settings	
Intercom call type	<input type="text" value="one-way"/>
Intercom call priority	<input type="text" value="3"/>
Intercom SIP-header	<input type="text" value="Answer-Mode: Auto"/>
Pause before answer, sec	<input type="text" value="0"/>
VAS settings	
CLIRO	<input type="checkbox"/>
Enable VAS	<input type="checkbox"/>
RingBack settings	
Mode	<input type="text" value="Default"/>
File name	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

- *SIP-forking* — enabling multiple registration on a subscriber;
- *Max registered contacts number* — allowed valid registration range on one subscriber (Range of acceptable values [2; 5]).

Busy-Lamp-Field (BLF) settings



Up to 500 subscribers for SMG-1016M.

- *Enable subscription* — allows the subscriber to subscribe to BLF events of other subscribers;
- *Max subscribers number* — quantity of observed numbers with activated BLF service;
- *Monitoring group* — BLF monitoring group, the subscribers included in one monitoring group can perform BLF monitoring between each other.



Directions (local network, special service, zone network, department network, national communication, international communication) are specified when configuring the prefix in the dial plan in Direction field.

Intercom call settings

- *Intercom call type* — type of incoming intercom call (auto answer call of subscriber B):
 - *One-way* — with an incoming intercom call, subscriber B will hear subscriber A, but subscriber A will not hear subscriber B (one-way notification);
 - *Two-way* — with an incoming intercom call, both subscribers will hear each other;
 - *Ordinary call* — incoming intercom call will be made as normal without auto answer of B side;
 - *Ignore* — incoming intercom call will be rejected.
- *Intercom call priority* — priority of incoming intercom call over others calls. Priority controls the allocation of an additional line over the limit for the subscriber, in order to notify the subscriber about the presence of an incoming intercom call:
 - Ordinary call — priority 1;
 - Intercom call can be defined with the priority of 1–5, by default: 3;
 - Notification — 7.


Examples:

- If subscriber A with priority 1 calls an already busy subscriber B (with one line and any priority), then subscriber A will hang up;
- If subscriber A with priority 2 calls already busy subscriber B (with one line and any priority), then 1 more extension line will be allocated for subscriber B and subscriber B will receive a call notification from subscriber A;
- If subscriber A with priority 2 calls already busy subscriber B (with one line and any priority), but subscriber B is already busy with subscriber C with priority 3, then subscriber A will hang up;
- Subscriber A should be notified in any case, because subscriber A has more high priority 7.
- *Intercom SIP-header* — Intercom SIP-header, that will be transmitted to the subscriber in the INVITE message during intercom/paging call:
 - *Answer-Mode: Auto;*
 - *Alert-Info: Auto Answer;*
 - *Alert-Info: info=alert-autoanswer;*
 - *Alert-Info: Ring Answer;*
 - *Alert-Info: info=RingAnswer;*
 - *Alert-Info: Intercom;*
 - *Alert-Info: info=intercom;*
 - *Call-Info: =\;answer-after=0;*
 - *Call-Info: \;answer-after=0;*
 - *Call-Info: ;answer-after=0.*
- *Pause before answer, sec* — transmission of pause time before answering intercom/pagingcall in the “answer-after” parameter.

VAS settings

- *CLIRO* — service to overcome the ban on issuing a caller's number;
- *Enable VAS¹* — connection of VAS services for the subscriber. Upon selecting this item, the table 'VAS activation' will become available.

VAS activation

Subscribers → SIP Subscribers → Configuration →  → Enable VAS

VAS activation	
Call forward (Unconditional)	<input type="checkbox"/>
Call forward (Busy)	<input type="checkbox"/>
Call forward (No-reply)	<input type="checkbox"/>
Call forward (Out of service)	<input type="checkbox"/>
Call forward (Time)	<input type="checkbox"/>
Call hold	<input type="checkbox"/>
Call transfer	<input type="checkbox"/>
3WAY conference	<input type="checkbox"/>
Call pickup	<input type="checkbox"/>
Conference	<input type="checkbox"/>
Disconnect conference by initiator	<input type="checkbox"/>
Interroom/Paging	<input type="checkbox"/>
Change password	<input type="checkbox"/>
Outgoing calls restriction	<input type="checkbox"/>
Restricted by password	<input type="checkbox"/>
Password activation	<input type="checkbox"/>
Follow me	<input type="checkbox"/>
Follow me (no response)	<input type="checkbox"/>
Call Park To	<input type="checkbox"/>
Slot setting	<input type="checkbox"/>
Extraction from slot	<input type="checkbox"/>
Voice mail	<input type="checkbox"/>
One Touch Record	<input type="checkbox"/>
DND	<input type="checkbox"/>
Blacklist	<input type="checkbox"/>
Anonymous call	<input type="checkbox"/>
Reject anonymous calls	<input type="checkbox"/>
Reminder	<input type="checkbox"/>
Reset all services	<input type="checkbox"/>
Voice Notification	<input type="checkbox"/>

- *Call Forward (Unconditional)* – enables the Call Forwarding Unconditional (CF Unconditional) service;
- *Call Forward (Busy)* – enables the Call Forwarding Busy (CF Busy) service;

¹ The menu is available only in the firmware version with the SMG-VAS license, more details about licenses in the section Licenses.

- *Call Forward (No Reply)* – enables the Call Forwarding No Reply (CF No Reply) service;
- *Call Forward (Out of Service)* – enables the Call Forwarding Out of Service (CF Out of Service);
- *Call Forward (Time)* – enables the Call Forwarding by time;
- *Call hold*;
- *Call transfer* – enables the Call Transfer service;
- *3WAY conference*;
- *Call pickup*;
- *Conference*;
- *Disconnect conference by initiator* – when checked, the conference will be over when the initiator leaves the conference. Otherwise, the conference will be saved after the initiator is hung up and will be over only when the last participant leaves the conference;
- *Intercom/Paging* – activation of access to the outgoing intercom or paging call service (call with autoreply of party B);
- *Change password* – changing the password to restrict outgoing communications;
- *Outgoing calls restriction* – use the service ‘restricting outgoing communications by password’;
- *Restricted by password* – allows the subscriber to make a one-time call without restrictions communication by entering the VAS password;
- *Password activation* – allows the subscriber to enter a password once to remove the outgoing communication restriction. Re-entering the password again sets the restrictions;
- *Follow me*;
- *Follow me (no response)*;
- *Call Park To* – allows the subscriber to use the call parking service;
- *Slot setting* (within call parking service);
- *Extraction from slot* (within call parking service);
- *Voice mail* – activation of voice mail service;
- *One Touch Record* – activation of on-demand call recording service;
- *Anonymous call* – allows to make anonymous calls without revealing the call recipient phone number and caller display name;
- *Reject anonymous calls* – allows to reject anonymous calls (without phone number and caller display name);
- *Reminder* – allows to receive an incoming call on your phone at a specified time. Subscriber activates the service and indicates the service activation time. At the appointed time the system establishes a call to the subscriber. When the subscriber picks up the phone, an alarm signal is played;
- *Reset all services*;
- *Voice notification*.



For the ‘Conference’ service to work, create a call group (section 4.1.7.12 Hunt groups) and indicate ‘Conference number’ in it. To include all members of a call group in conference, dial the ‘Conference’ service prefix and the conference number specified in the call group.

For example, the conference number is ‘12345’, the service prefix of VAS Conference is ‘*71*x{1,20}#’, to gather group members into a conference, dial ‘*71*12345#’.

RingBack settings

This block allows to configure the playback of an audio file for the subscriber individually.

Mode:

- *Default* – this setting refers to settings in system parameters;
- *RingBack* – playing standard RBT sound, ignoring settings from system parameters;
- *Audio file* – replacing the standard RBT sound with a randomly selected one that was downloaded at the stage of setting up the RBT in ‘System parameters’ menu item (individual sound for subscriber).

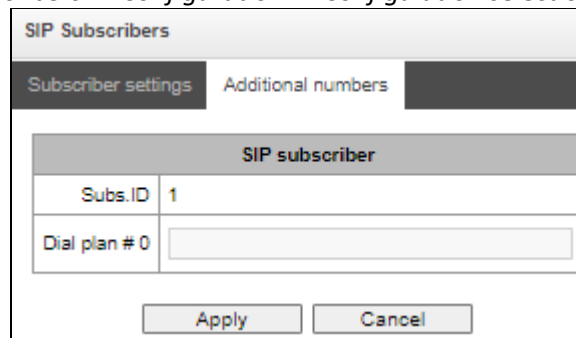
4.1.6.1.1.2 Additional numbers

A subscriber may have different numbers in different dial plans, and when a call is passing through the dial plan change prefix, the subscriber's CgPN number is automatically replaced with the number in the appropriate dial plan, for example:

The subscriber has an internal short numbering; accordingly, it is registered at the gateway under a short number, when accessing an external network, each such subscriber should enter its own number in international format as a CgPN. Access to the external network is via prefix 9.

To solve this problem, it is necessary to activate 2 dial plans in the 'System parameters' section, create a list of subscribers with short numbering on the gateway, indicate its external number in the 'Additional numbers' in the 'Dial plan #1' field for each subscriber. In the dial plan #1, a prefix for accessing the external network should be created; in the 'dial plan #0' a prefix '(9x.)' with 'change dial plan' type should be created, which will switch to the dial plan #1. When a subscriber dials a full number with 9 at the beginning, the call will go through the "Change a dial plan" prefix type, and in the dial plan 1 the CgPN number will be automatically replaced with its external number.

Subscribers → SIP Subscribers → Configuration → Configuration selection → Additional numbers



SIP subscriber	
Subs.ID	1
Dial plan #0	

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

4.1.6.1.2 VAS management

In this section, VAS settings for subscribers are configured.

Each subscriber is provided with VAS services, but to use a specific service it is necessary to active it with an operator. The operator can create a service plan from several VAS functions, to do this, in the Configuration of SIP subscribers section, set the 'Enable VAS' flag and the flags opposite the necessary functions of the VAS.

The subscriber can manage the status of services from the phone. The following functions are available:

- *Service activation* – activation and entry of additional data;
- *Service verification*;
- *Cancel service*.

After entering the activation code or canceling the service, the subscriber can hear either a 'Confirmation' signal (3 short signals), or 'Busy' signal (periodic signal with a duration signal/pause – 0.35/0.35 s). The 'Confirmation' signal indicates that the service has been successfully activated or cancelled, the 'Busy' signal indicates that the subscriber is not connected to this service.



Calling the service through VAS prefixes always ends with a “#” symbol.

After entering the service verification code, the subscriber can hear either the 'Station Answer' signal (continuous signal) or 'Busy' signal. The 'Station Answer' signal indicates that the service is enabled and activated for the subscriber, the 'Busy' signal indicates that either the service is disabled or the subscriber is not connected to this service.

The menu displays only those numbers for which the 'Enable VAS' flag is set in the configuration menu (Configuration of SIP subscribers section).

Subscribers → SIP subscribers → VAS management

SIP Subscribers

Configuration Monitoring VAS management BLF Monitoring

Search subscriber by number Search

No	Description	Number	Parameters
0	Subscriber#590		Intercom; PWD: 1111

10 Rows in the table to show

Current page 1 from 1

Subscribers → SIP subscribers → VAS management → Object

Edit VAS block of Subscriber#590 ()

Numbers Whitelist Blacklist

VAS block for subscriber Subscriber#590

Number for call forward (unconditional)

Number for call forward (busy)

Number for call forward (no-reply)

Number for call forward (out of service)

Number for call forward (time)

Password

Password activation

Restrict out

"Anonymous call" service activation

"Reject Anonymous calls" service activation

Follow me

Follow me activation

Follow me pin

Follow me number

Follow me pin

Follow me number

Follow me (no response)

Follow me activation

Follow me pin

Follow me number

Follow me (no response)pin

Follow me (no response)number

Call forward (Time)

Schedule selection

Voice mail

Voice mail activation

Password

Apply Cancel

- *Number for call forward (unconditional)* – phone number for unconditional forwarding;
- *Number for call forward (busy)* – phone number for call forwarding by busy;
- *Number for call forward (no-reply)* – phone number for call forwarding by no reply;
- *Number for call forward (out of service)* – phone number for call forwarding by out of service;

- *Number for call forward (time)* – phone number for call forwarding by time;
- *Password* – a password of 4 to 8 digits in length to access the ‘outgoing calls restriction’ service;
- *Password activation* – when the flag is set, the password is activated and the restrictions on outgoing calls have been removed;
- *Restrict out* – sets a ban on outgoing calls for certain types of directions with inactive password:
 - *All allowed* – restriction on outgoing calls is not in effect, restriction code is 0;
 - *Only to emergency* – outgoing communication is limited to calls to emergency, restriction code is 1;
 - *Only local and department network* – outgoing communication is limited to calls within local and department networks, restriction code is 2;
 - *Only local, department and zone network* – outgoing communication is limited to calls within local, department and zone networks, restriction code is 3.

‘White List’ tab – on this tab, one can activate ‘Do Not Disturb’ service and set white list of numbers that can call a subscriber, despite the ban.

‘Black List’ tab – on this tab, one can activate the ‘Black List’ service and set a black list of numbers that cannot call a subscriber.

A detailed description of the operation and configuration of VAS services is given in Appendix H. Working with VAS services.

4.1.6.1.3 SIP Subscribers monitoring

Upon selecting the ‘Monitoring’ item in the drop-down list, a table of subscriber states is displayed.

Subscribers → SIP Subscribers → Monitoring

SIP Subscribers

Configuration Monitoring VAS management BLF Monitoring

Number of configured subscribers: 91
Number of registered subscribers: 0

Search subscriber by name Search

No	State	Title	Number	SIP domain	IP/Port	Local IP/Port	Last registration	Expire in	Select
0	Not registered	Subscriber#000	10		0.0.0.0:0	0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>
1	Not registered	Subscriber#001	11		0.0.0.0:0	0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>
2	Not registered	Subscriber#002	12		0.0.0.0:0	0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>
3	Not registered	Subscriber#003	13		0.0.0.0:0	0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>
4	Not registered	Subscriber#004	14		0.0.0.0:0	0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>
5	Not registered	Subscriber#005	15		0.0.0.0:0	0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>
6	Not registered	Subscriber#006	16		0.0.0.0:0	0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>
7	Not registered	Subscriber#007	17		0.0.0.0:0	0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>
8	Not registered	Subscriber#008	18		0.0.0.0:0	0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>
9	Not registered	Subscriber#009	19		0.0.0.0:0	0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>

10 Rows in the table to show

Current page 1 from 10
Selected: 0

- *Search subscriber* – checking the database of configured SIP subscribers, one can check by name, number, status, SIP domain, IP address:Port;
- *State* – subscriber registration status (registration is active, not registered, registration expired);
- *Title* – arbitrary text description of a subscriber;
- *Number* – subscriber number;

- *SIP domain* – domain to which the subscriber belongs;
- *IP/Port* – IP address and port of the subscriber;
- *Last registration* – time of the last registration;
- *Expire in* – time remaining before the registration expiration.

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

4.1.6.1.4 BLF Monitoring

Subscribers → *SIP Subscribers* → *BLF Monitoring*

SIP Subscribers

Configuration Monitoring VAS management **BLF Monitoring**

Search subscriber by number

No	Subs. name	Subs. number	BLF state	Observers number
0	Subscriber#000	10		0
1	Subscriber#001	11		0
2	Subscriber#002	12		0
3	Subscriber#003	13		0
4	Subscriber#004	14		0
5	Subscriber#005	15		0
6	Subscriber#006	16		0
7	Subscriber#007	17		0
8	Subscriber#008	18		0
9	Subscriber#009	19		0

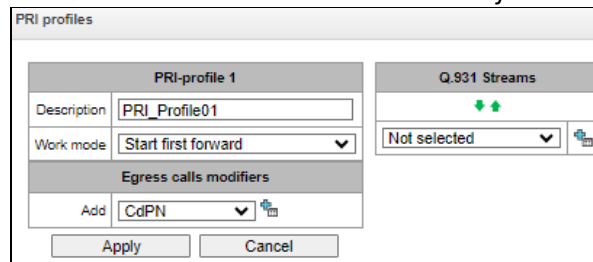
10 Rows in the table to show Current page 1 from 10

By clicking the ‘*Search*’ button, the subscriber with the specified number will be searched among the records.

- *Subs. name* – free text description of the subscriber;
- *Subs.number*;
- *BLF state* – current state of the ‘*Line Seizure Indication*’ service. BLF state can take the following values:
 - *idle* – subscription is inactive (expired);
 - *early* – channel occupation;
 - *alert* – sending a call;
 - *confirmed* – the conversation has been established;
 - *terminated* – the conversation is completed/absent.
- *Observers number* – the current number of subscribers who are observing the state subscriber lines.

4.1.6.2 PRI profiles

Subscribers → SIP Subscribers → Object



PRI profiles are used to configure PRI subscribers:

- *Description* – PRI profile menu;
- *Work mode* – determines the order in which channels are occupied:
 - *Start first forward*;
 - *Start last backward*.
- *Egress calls modifiers*:
 - *CdPN* – intended for modifications based on the analysis of the called subscriber number transmitted to the outgoing channel;
 - *CgPN* – intended for modifications based on the analysis of the calling subscriber number transmitted to the outgoing channel;
 - *Original CdPN* – intended for modifications based on the analysis of the original called party number transmitted to the outgoing channel;
 - *RedirPN* – intended for modifications based on the analysis of the redirecting number transmitted to the outgoing channel.
- *Q.931 Streams* – streams are selected that will be associated with PRI subscribers.

Ingress calls/egress calls modifiers for PRI subscribers work as follows.

For example, on the trunk group of the E1 stream, to which PRI subscribers are attached, for ingress calls the CgPN (Table1) and CdPN (Table0) modifiers are set on the PBX profile to which PRI subscribers are attached, the CgPN (Table3) and CdPN (Table2) modifiers are also set for ingress calls. In all tables the selection mask is set as (x.)

A call comes from E1 stream:

1. The rule for CgPN from the modifier Table1 is applied.
2. The CgPN number is checked for a PRI subscriber.
- 3a. If the call is not from a PRI subscriber, the call is processed as from a regular trunk; the remaining modifiers tied to the trunk group on the incoming connection will be applied.
- 3b. If the call is from a PRI subscriber, the remaining modifiers tied to the trunk group and the PBX profile are applied. The order of modifiers is as follows:
 - The CgPN rule from Table3 is applied
 - The CdPN rule from Table1 is applied
 - The CdPN rule from Table3 is applied
 - The CgPN rule from Table0 is applied
 - The CgPN rule from Table2 is applied
 - The CdPN rule from Table0 is applied
 - The CdPN rule from Table2 is applied

The egress calls modifiers on a PRI profile are triggered if the call is routed to a PRI subscriber associated with this profile.

4.1.6.3 Dynamic subscribers groups

4.1.6.3.1 Configuration of dynamic subscribers group

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

Dynamic registration uses digest authentication on a RADIUS server (RFC 5090, RFC-no-challenge, draft-sterman) for subscribers.

Subscribers → Dynamic subscribers groups → Configuration

Dynamic subscribers groups

Configuration Monitoring VAS management BLF Monitoring

No	ID	Description	Number of subscribers	Dial plan	Calling party category (RUS)	SIP domain	SIP profile	Select
0	1	SubscriberGroup#000	2	[0] NumberPlan#0	1		Profile Dynamic	<input type="checkbox"/>
1	2	SubscriberGroup#001	1	[0] NumberPlan#0	1		any	<input type="checkbox"/>

10 Rows in the table to show

Current page 1 from 1

Selected: 0

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



– Add subscribers;



– Edit subscriber parameters;



– Remove subscriber.

Subscribers → Dynamic subscribes groups → Configuration → Object

Dynamic Subscribers Group 3		VAS activation	
Subscribers number	1 <small>Maximum available subscribers count is 1406.</small>	Call forward (Unconditional)	<input type="checkbox"/>
Description	SubscriberGroup#002	Call forward (Busy)	<input type="checkbox"/>
Calling party number type	Subscriber	Call forward (No-reply)	<input type="checkbox"/>
Calling party category (RUS)	1	Call forward (Out of service)	<input type="checkbox"/>
Lines operation mode	Common	Call forward (Time)	<input type="checkbox"/>
Lines number	1	Call hold	<input type="checkbox"/>
Redirecting lines number	0	Call transfer	<input type="checkbox"/>
SIP domain		3WAY conference	<input type="checkbox"/>
SIP profile	not set	Call pick-up	<input type="checkbox"/>
PBX profile	[0] PBXprofile#0	Conference	<input type="checkbox"/>
Access category	[0] AccessCat#0	Disconnect conference by initiator	<input type="checkbox"/>
Dial plan	[0] NumberPlan#0	Interroom call	<input type="checkbox"/>
Ignore source port after registration	<input type="checkbox"/>	Change password	<input type="checkbox"/>
Subscriber service mode	On	Outgoing calls restriction	<input type="checkbox"/>
Multiple registration (SIP-forking)		Restricted by password	<input type="checkbox"/>
SIP-forking	<input type="checkbox"/>	Password activation	<input type="checkbox"/>
Max registered contacts number	2	DND	<input type="checkbox"/>
Busy-Lamp-Field (BLF) settings		Blacklist	<input type="checkbox"/>
Enable subscription	<input type="checkbox"/>	Follow me	<input type="checkbox"/>
Max subscribers number	0	Follow me (no response)	<input type="checkbox"/>
Monitoring group	0	Call Park To	<input type="checkbox"/>
Interroom call settings		Slot setting	<input type="checkbox"/>
Interroom call type	one-way	Extraction from slot	<input type="checkbox"/>
Interroom call priority	1	Voice mail	<input type="checkbox"/>
Interroom SIP-header	Answer-Mode: Auto	One Touch Record	<input type="checkbox"/>
Pause before answer, sec	0	Clear all services	<input type="checkbox"/>
VAS settings		Voice Notification	<input type="checkbox"/>
CLIR	<input type="checkbox"/>		
VAS management	Individual		
RingBack settings			
Mode	Default		
File name			

Dynamic Subscribers Group

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

- *Egress lines number* – the number of simultaneous outgoing calls from the subscriber. The field appears if the line mode is set to *Separate*. The range of possible values is [1;255] or 0 – no limits;
- *Redirecting lines number* – number of simultaneous calls for redirection. Valid range [1;255] or 0 – no limits;
- *SIP domain* – identifies the domain to which the subscriber belongs. It is sent by the subscriber gateway as the “host” parameter in the SIP URI of the *from* and *to* fields (see section 4.1.4.4 Timer operation examples);
- *SIP profile* – select the SIP profile. The SIP profile defines the most of the subscriber settings. Selecting “Any” profile makes it possible to register a sip subscriber on any of the available sip profiles in the system (see section 4.1.5.3 SIP/ SIP-T/ SIP-I interfaces, SIP profiles);
- *PBX profile* – select the PBX profile (see section PBX profiles);
- *Access category* – select an access category;
- *Dial plan* – define the dial plan for the subscriber;
- *Ignore source port after registration* – after registration, messages from subscribers can arrive from any port;
- *Subscriber service mode* – set a limit on the incoming and outgoing communication for the subscriber:
 - *off* – the port is out of service. The subscriber number is present in the dial plan, but the subscriber terminal cannot be registered. Therefore, incoming calls will be rejected with the *out of order* cause; outgoing calls cannot be initiated;
 - *on* – all types of communication are available;
 - *off 1* – incoming communication is enabled; outgoing communication is to special services only;
 - *off 2* – incoming communication is disabled; outgoing communication is to special services only;
 - *denied 1* – full prohibition for incoming and outgoing calls. Calls will be routed according to the dial plan, but be rejected;
 - *denied 2* – full prohibition for incoming and outgoing calls, except for special services;
 - *denied 3* – incoming calls are prohibited, outgoing calls are allowed;
 - *denied 4* – incoming calls are prohibited, outgoing calls are allowed only for local and department communication;
 - *denied 5* – incoming calls are allowed, outgoing calls are fully prohibited;
 - *denied 6* – incoming calls are allowed, outgoing calls are allowed only for special services;
 - *denied 6* – incoming calls are prohibited, outgoing calls are allowed only for local and private communication;
 - *denied 8* – incoming calls are allowed, outgoing calls are allowed only for local and private and zone communication;
 - *ignore* – the number is excluded from the dial plan. The number is completely excluded from the subscriber number list of the dial plan. If this number is called, the call will be rejected with the *no route to destination* cause, or it will be routed to the appropriate prefix in the dial plan.



Directions (*local network, emergency, zone network, department network, national network, international network*) are specified when configuring the prefix in the *Direction* field of the dial plan.

Multiple registration (SIP forking)

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

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

Busy-Lamp-Field (BLF) settings

- *Enable subscription* – the BLF (*Busy Lamp Field*) function allows monitoring the current status of other subscriber lines in real time;
- *Max subscribers number* – the number of subscribers who can monitor the subscriber line status;
- *Monitoring group* – the BLF monitoring group; BLF monitoring is allowed only between the subscribers belonging to the same monitoring group.

Intercom call settings

- *Intercom call type* – the incoming intercom call type (a call with an automatic answer of subscriber B):
 - *One-way* – with an incoming intercom call, subscriber B will hear subscriber A, but subscriber A will not hear subscriber B (one-way notification);
 - *Two-way* – with an incoming intercom call, both subscribers will hear each other;
 - *Ordinary call* – an incoming intercom call is made as a normal call, without an automatic answer of subscriber B;
 - *Ignore* – an incoming intercom call will be rejected.
- *Intercom call priority* – the priority of an incoming intercom call over other calls:
 - Ordinary call – priority 1;
 - Intercom call can be defined with the priority of 1–5, by default: 3;
 - Notification – 7.

Examples:

- If subscriber A with priority 1 calls an already busy subscriber B (with one line and any priority), then subscriber A will hang up;
 - If subscriber A with priority 2 calls already busy subscriber B (with one line and any priority), then 1 more extension line will be allocated for subscriber B and subscriber B will receive a call notification from subscriber A;
 - If subscriber A with priority 2 calls already busy subscriber B (with one line and any priority), but subscriber B is already busy with subscriber C with priority 3, then subscriber A will hang up;
 - Subscriber A should be notified in any case, because subscriber A has more high priority 7.
- *Intercom SIP-header* – select a SIP header to be sent to the callee in the INVITE message during an intercom/paging call:
 - Answer-Mode: Auto;
 - Alert-Info: Auto Answer;
 - Alert-Info: info=alert-autoanswer;
 - Alert-Info: Ring Answer;
 - Alert-Info: info=RingAnswer;

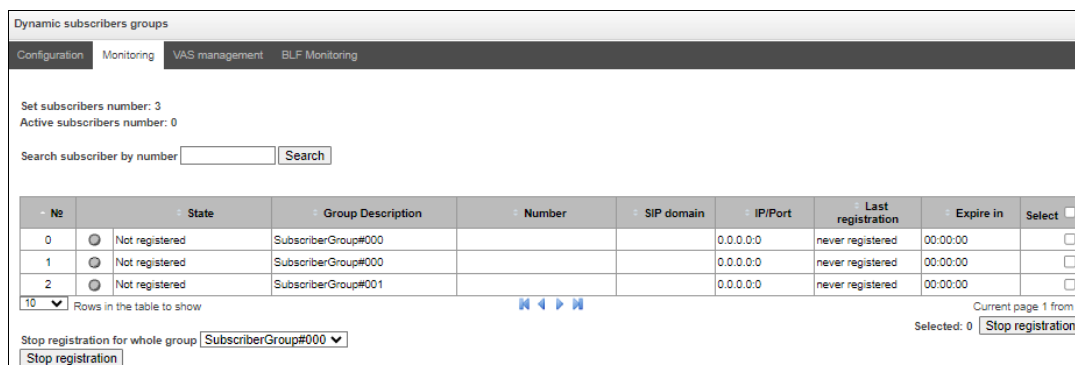
- Alert-Info: Intercom;
 - Alert-Info: info=intercom;
 - Call-Info: =\;answer-after=0;
 - Call-Info: \\;answer-after=0;
 - Call-Info: ;answer-after=0.
- *Pause before answer, sec* – the pause duration before answering an intercom/paging call, which can be transmitted in the ‘answer-after’ header.

VAS settings

- *CLIRO* – a service for overriding the prohibition on caller number identification;
- *VAS management* – selects how VAS services will be activated for dynamic subscribers:
 - *Not used* – do not enable VAS services for dynamic subscribers;
 - *Individual* – VAS services can be configured for each subscriber individually via the gateway configurator. If this option is selected, the *VAS Activation* table will become available (see section 4.1.6.1.1.1 SIP Subscribers);
 - *From RADIUS* – for dynamic subscribers, VAS settings will be sent in the RADIUS server responses. For details, see Appendix D. Transmission of VAS settings from RADIUS server for dynamic subscribers.

4.1.6.3.2 Monitoring of dynamic subscribers group

Subscribers → *Dynamic subscribers groups* → *Monitoring*



Dynamic subscribers groups

Configuration | Monitoring | VAS management | BLF Monitoring

Set subscribers number: 3
Active subscribers number: 0

Search subscriber by number Search

№	State	Group Description	Number	SIP domain	IP/Port	Last registration	Expire in	Select
0	Not registered	SubscriberGroup#000			0.0.0.0:0	never registered	00:00:00	<input type="checkbox"/>
1	Not registered	SubscriberGroup#000			0.0.0.0:0	never registered	00:00:00	<input type="checkbox"/>
2	Not registered	SubscriberGroup#001			0.0.0.0:0	never registered	00:00:00	<input type="checkbox"/>

10 Rows in the table to show

Stop registration for whole group: SubscriberGroup#000

Selected: 0 Stop registration

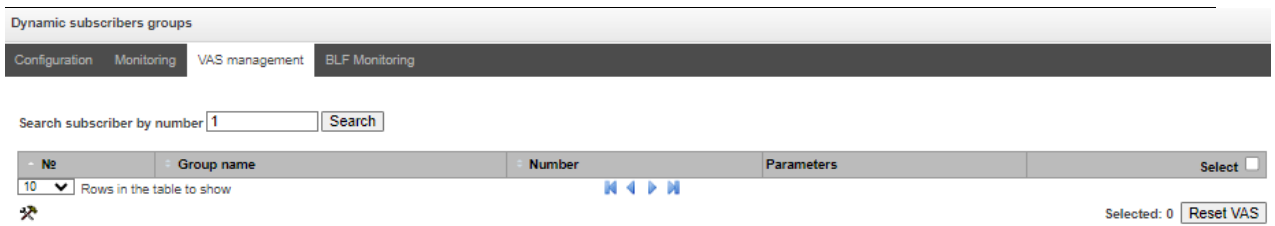
Click the ‘Search’ button to search entries for the subscriber with the specified number.

- *State* – subscriber registration status (registered, not registered, registration expired);
- *Group Description* – arbitrary text description of the group;
- *Number* – the subscriber number;
- *SIP domain* – the domain to which the subscriber belongs;
- *IP/Port* – IP address and port of the subscriber;
- *Last registration* – the time of the last registration;
- *Expire in* – the time remaining before the registration expiration;
- *Select* – when this option is checked, this entry in the table will be processed when you click the *Reset registration* button;
- *Stop registration* – forcibly reset the registration for a selected subscriber.

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

4.1.6.3.3 VAS management of dynamic subscriber groups

Subscribers → Dynamic subscribers groups → VAS management



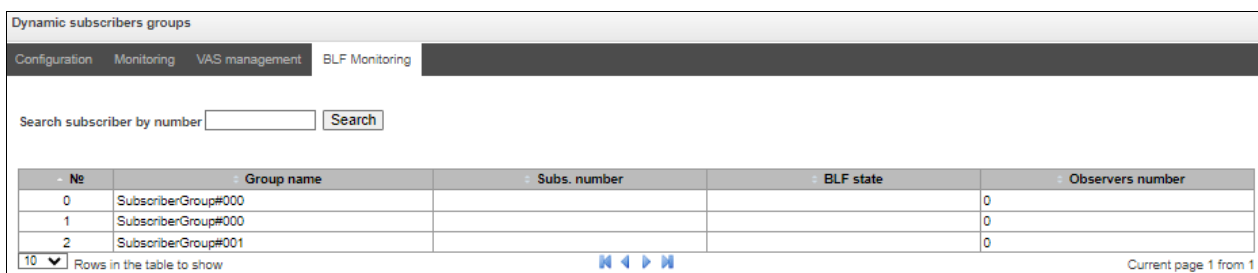
Click the 'Search' button to search entries for the subscriber with the specified number.

- *Group name* – arbitrary text description of the group;
- *Number* – the subscriber number;
- *Parameters* – subscriber VAS parameters;
- *Select* – when this option is checked, this entry in the table will be processed when you click the 'Reset VAS' button.

Click the 'Reset VAS' button to forcibly reset the VAS settings for selected subscribers.

4.1.6.3.4 BLF monitoring of dynamic subscriber groups

Subscribers → Dynamic subscribers groups → BFL monitoring



No	Group name	Subs. number	BLF state	Observers number
0	SubscriberGroup#000			0
1	SubscriberGroup#000			0
2	SubscriberGroup#001			0

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

- *Group name* – arbitrary text description of the group;
- *Subs. number* – the subscriber number;
- *BLF state* – the current status of the *busy lamp field* service:
 - *idle* – subscription is inactive (expired);
 - *early* – channel occupation;
 - *alert* – sending a call;
 - *confirmed* – the conversation has been established;
 - *terminated* – the conversation is completed/absent.
- *Observers number* – the current number of subscribers who monitor the subscriber's line status.

4.1.6.4 V5.2 subscribers

Subscribers → V5.2 Subscribers → Configuration

V5.2 Subscribers

Configuration Monitoring VAS management

Search subscriber by name Search

No	ID	Title	Number	Dial plan	Calling party category (RUS)	V5.2 Interface	Select
0	91	Subscriber#090	0001	[0] NumberPlan#0	1	-	<input type="checkbox"/>
1	92	Subscriber#091	0002	[0] NumberPlan#0	1	-	<input type="checkbox"/>
2	93	Subscriber#092	0003	[0] NumberPlan#0	1	-	<input type="checkbox"/>
3	94	Subscriber#093	0004	[0] NumberPlan#0	1	-	<input type="checkbox"/>
4	95	Subscriber#094	0005	[0] NumberPlan#0	1	-	<input type="checkbox"/>
5	96	Subscriber#095	0006	[0] NumberPlan#0	1	-	<input type="checkbox"/>
6	97	Subscriber#096	0007	[0] NumberPlan#0	1	-	<input type="checkbox"/>
7	98	Subscriber#097	0008	[0] NumberPlan#0	1	-	<input type="checkbox"/>
8	99	Subscriber#098	0009	[0] NumberPlan#0	1	-	<input type="checkbox"/>
9	100	Subscriber#099	0010	[0] NumberPlan#0	1	-	<input type="checkbox"/>

10 Rows in the table to show

Current page 1 from 50

Selected: 0




Attach selected items

V5.2 Interface

Start Layer 3 address

- *Search subscriber* – checking the presence of a subscriber in the database of configured V5.2 subscribers. Can be checked by name, number, caller ID number, PBX profile, dial plans, V5.2 interface;
- *Edit selected* – pressing the button allows going to the group editing menu of selected subscribers (opposite to which the flag is set 'Select'). To be able to edit, set the 'Edit' flag opposite the required parameter. A description of the parameters for configuration is given below;
- *Remove selected* – pressing the button allows group deletion of selected subscribers.

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

-  – Add subscriber;
-  – Edit subscriber parameters;
-  – Remove subscriber.

Attach selected items – add selected subscribers to the V5.2 interface.

V5.2 Subscribers	
V5.2 subscriber	
Subscribers count	1 <small>Max subscribers count 1406.</small>
Starting description	Subscriber#591
Starting number	
Hotline (incoming)	
Hotline delay (incoming), sec	0
Starting CallerID number	
Use CallerID number for redirection	<input type="checkbox"/>
Calling party number type	Subscriber
Calling party category (RUS)	1
PBX profile	[0] PBXprofile#0
Access category	[0] AccessCat#0
Dial plan	[0] NumberPlan#0
CallerID generation	Off
Subscriber service mode	On
VAS settings	
CLIRO	<input type="checkbox"/>
Enable VAS	<input type="checkbox"/>
RingBack settings	
Mode	Default
File name	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Subscriber parameters:

- *Subscribers count* – unique subscriber identifier;
- *Starting description* – arbitrary text description of the subscriber;
- *Starting number* – subscriber number, for a group of subscribers each subsequent one will be assigned a number increased by one;
- *Hotline (incoming)* – hotline number is set. If the number is specified, then the service is activated automatically;
- *Hotline delay (incoming), sec* – allows to set a hotline activation delay. Valid range [0;10];
- *Starting CallerID number* – caller ID number of the subscriber, for a group of subscribers each subsequent one will be assigned a number increased by one;
- *Use CallerID number for redirection* – use the number specified in the ‘Starting CallerID number’ field when performing call forwarding service;
- *Calling party number type* – subscriber number type;
- *Calling party category* – CallerID category;
- *PBX profile* – PBX profile selection;
- *Access category* – access category selection (see PBX profiles);
- *Dial plan* – dial plan in which the subscriber will be located;
- *CallerID generation* – format for CallerID generation;

-
- *Subscriber service mode* – sets a limit on incoming and outgoing communications to the subscriber:
 - *off* – the port is out of service. The subscriber number is present in the dial plan, but the subscriber terminal cannot be registered. Therefore, incoming calls will be rejected with the *out of order* cause; outgoing calls cannot be initiated;
 - *on* – all types of communication are available;
 - *off 1* – incoming communication is enabled; outgoing communication is to special services only;
 - *off 2* – incoming communication is disabled; outgoing communication is to special services only;
 - *denied 1* – full prohibition for incoming and outgoing calls. Calls will be routed according to the dial plan, but be rejected;
 - *denied 2* – full prohibition for incoming and outgoing calls, except for special services;
 - *denied 3* – incoming calls are prohibited, outgoing calls are allowed;
 - *denied 4* – incoming calls are prohibited, outgoing calls are allowed only for local and department communication;
 - *denied 5* – incoming calls are allowed, outgoing calls are fully prohibited;
 - *denied 6* – incoming calls are allowed, outgoing calls are allowed only for special services;
 - *denied 6* – incoming calls are prohibited, outgoing calls are allowed only for local and private communication;
 - *denied 8* – incoming calls are allowed, outgoing calls are allowed only for local, private and zone communication;
 - *ignore* – the number is excluded from the dial plan. The number is completely excluded from the subscriber number list of the dial plan. If this number is called, the call will be rejected with the *no route to destination* cause, or it will be routed to the appropriate prefix in the dial plan.

VAS settings

- *CLIRO* – a service to overcome the ban on issuing a caller's number;
- *Enable VAS*¹ – connection of VAS services for subscriber. When checked, the '*VAS activation*' table is available.

¹ The menu is available only in the firmware version with the SMG-VAS license. Read more detailed information on licenses in the section Licenses.

VAS activation

Subscribers → V5.2 Subscribers → Configuration → Object → Enable VAS

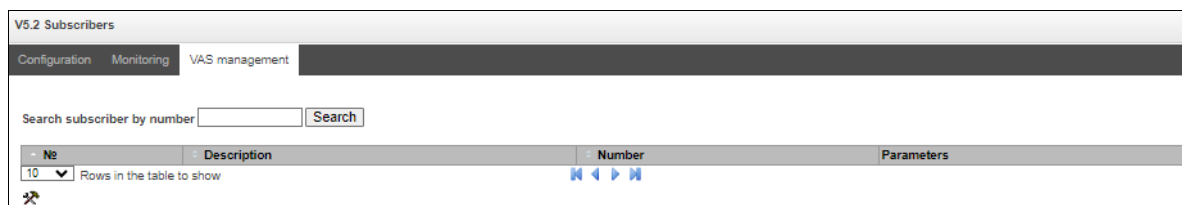
VAS activation	
Call forward (Unconditional)	<input type="checkbox"/>
Call forward (Busy)	<input type="checkbox"/>
Call forward (No-reply)	<input type="checkbox"/>
Call forward (Out of service)	<input type="checkbox"/>
Call forward (Time)	<input type="checkbox"/>
Call hold	<input type="checkbox"/>
Call transfer	<input type="checkbox"/>
3WAY conference	<input type="checkbox"/>
Call pickup	<input type="checkbox"/>
Conference	<input type="checkbox"/>
Disconnect conference by initiator	<input type="checkbox"/>
Change password	<input type="checkbox"/>
Outgoing calls restriction	<input type="checkbox"/>
Restricted by password	<input type="checkbox"/>
Password activation	<input type="checkbox"/>
DND	<input type="checkbox"/>
Blacklist	<input type="checkbox"/>
Follow me	<input type="checkbox"/>
Follow me (no response)	<input type="checkbox"/>
Call Park To	<input type="checkbox"/>
Slot setting	<input type="checkbox"/>
Extraction from slot	<input type="checkbox"/>
Voice mail	<input type="checkbox"/>
Reset all services	<input type="checkbox"/>
Voice Notification	<input type="checkbox"/>

- *Call Forward (Unconditional)* – enables the Call Forwarding Unconditional (CF Unconditional) service;
- *Call Forward (Busy)* – enables the Call Forwarding Busy (CF Busy) service;
- *Call Forward (No Reply)* – enables the Call Forwarding No Reply (CF No Reply) service;
- *Call Forward (Out of Service)* – enables the Call Forwarding Out of Service (CF Out of Service);
- *Call Forward (Time)* – enables the Call Forwarding by Time service (CT Time);
- *Call hold*;
- *Call transfer* – enables the Call Transfer service;
- *3WAY conference*;
- *Call pickup*;
- *Conference*;
- *Disconnect conference by initiator* – when checked, the conference will be over when the initiator leaves the conference. Otherwise, the conference will be saved after the initiator is hung up and will be over only when the last participant leaves the conference;

- *Change password* – changing the password to restrict outgoing communications;
- *Outgoing calls restriction* – use the service ‘restricting outgoing communications by password’;
- *Restricted by password* – allows the subscriber to make a one-time call without restrictions communication by entering the VAS password;
- *Password activation* – allows the subscriber to enter a password once to remove the outgoing communication restriction. Re-entering the password again sets the restrictions;
- *DND* – allows the subscriber to set the ‘Do not disturb’ mode and set several numbers from the white list who will still be able to call the subscriber (the service is available for SMG-2016 and SMG-3016);
- *Blacklist* – allows the subscriber to blacklist numbers so that they cannot call the subscriber (*the service is available for SMG-2016 and SMG-3016*);
- *Follow me* – allows one to forward all calls one’s phone to a remote phone using the remote phone;
- *Follow me (no response)* – allows one to forward all calls coming to ‘local’ number, to the ‘remote’ number in case the local number did not receive a call within the specified time interval;
- *Call Park To* – allows the subscriber to use the call parking service;
- *Slot setting* (within call parking service);
- *Extraction from slot* (within call parking service);
- *Voice mail* – activation of voice mail service;
- *Reset all services* – function required to cancel all configured numbers for forwarding by pressing the service prefix configured in the numbering plan;
- *Voice notification* – activation of the voice notification service (VSS).

VAS management

Subscribers → V5.2 Subscribers → VAS Management



In this section, VAS settings for subscribers are configured.

Each subscriber is provided with VAS services, but to use a specific service it is necessary to activate it with an operator. The operator can create a service plan from several VAS functions, to do this, set the ‘Enable VAS’ flag and the flags opposite the necessary functions of the VAS in the SIP subscribers configuration tab (see 4.1.6.1 SIP Subscribers section).

The subscriber can manage the status of services from the phone. The following functions are available:

- *Service activation* – activation and entry of additional data;
- *Service verification*;
- *Cancel service*.

After entering the activation code or canceling the service, the subscriber can hear either a ‘Confirmation’ signal (3 short signals), or ‘Busy’ signal (periodic signal with a duration signal/pause – 0.35/0.35 s). The ‘Confirmation’ signal indicates that the service has been successfully activated or cancelled, the ‘Busy’ signal indicates that the subscriber is not connected to this service.

After entering the service verification code, the subscriber can hear either the ‘Station Answer’ signal (continuous signal) or ‘Busy’ signal. The ‘Station Answer’ signal indicates that the service is enabled and activated for the subscriber, the ‘Busy’ signal indicates that either the service is disabled or the subscriber is not connected to this service.

The menu displays only those numbers for which the 'Enable VAS' flag is set in the configuration menu (see 4.1.6.1 SIP Subscribers section).

Subscribers → V5.2 Subscribers → VAS Management → 

Edit VAS block of Subscriber#001 ()	
Numbers Whitelist Blacklist	
VAS block for subscriber Subscriber#001	
Number for call forward (unconditional)	<input type="text"/>
Number for call forward (busy)	<input type="text"/>
Number for call forward (no-reply)	<input type="text"/>
Number for call forward (out of service)	<input type="text"/>
Number for call forward (time)	<input type="text"/>
Password	<input type="text" value="1111"/>
Password activation	<input type="checkbox"/>
Restrict out	<input type="text" value="all allowed"/>

- *Number for call forward (unconditional)* – phone number for unconditional forwarding;
- *Number for call forward (busy)* – phone number for call forwarding by busy;
- *Number for call forward (no-reply)* – phone number for call forwarding by no reply;
- *Number for call forward (out of service)* – phone number for call forwarding by out of service;
- *Number of call forward (time)* – phone number for call forwarding by time;
- *Password* – a password of 4 to 8 digits in length to access the 'outgoing calls restriction' service;
- *Password activation* – when the flag is set, the password is activated and the restrictions on outgoing calls have been removed;
- *Restrict out* – sets a ban on outgoing calls for certain types of directions with inactive password:
 - *All allowed* – restriction on outgoing calls is not in effect, restriction code is 0;
 - *Only to emergency* – outgoing communication is limited to calls to emergency, restriction code is 1;
 - *Only local and department network* – outgoing communication is limited to calls within local and department networks, restriction code is 2;
 - *Only local, department and zone network* – outgoing communication is limited to calls within local, department and zone networks, restriction code is 3.

'White List' tab – on this tab, one can activate 'Do Not Disturb' service and set white list of numbers that can call a subscriber, despite the ban.

'Black List' tab – on this tab, one can activate the 'Black List' service and set a black list of numbers that cannot call a subscriber.

A detailed description of the operation and configuration of VAS services is given in Appendix H. Working with VAS services.

4.1.6.5 PRI Subscribers

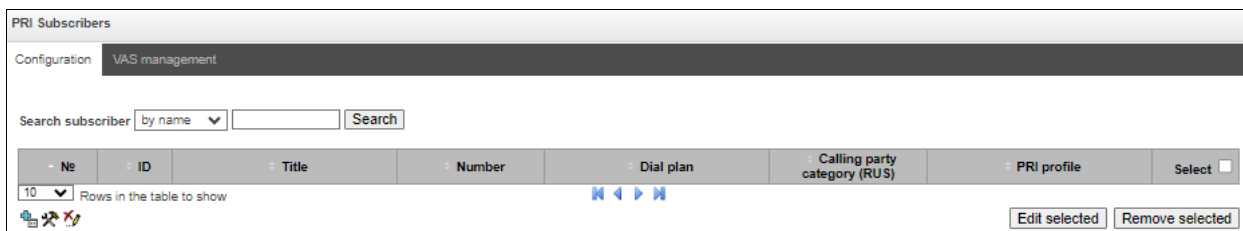
PRI subscribers are numbers that are located behind a PRI trunk (E1 streams with Q.931 signaling) and are perceived by SMG as local subscribers with the provision of some subscriber services.

Routing to such subscribers is carried out without creating additional rules in the dial plan.

Checking whether the calling subscriber is a PRI subscriber is carried out by matching the E1 stream Q.931, from which the call and A-numbers came.

Search subscriber – checking the presence of a subscriber in the database of configured PRI subscribers, possible checking by name, number, PRI profile, PBX profile, dial plans.

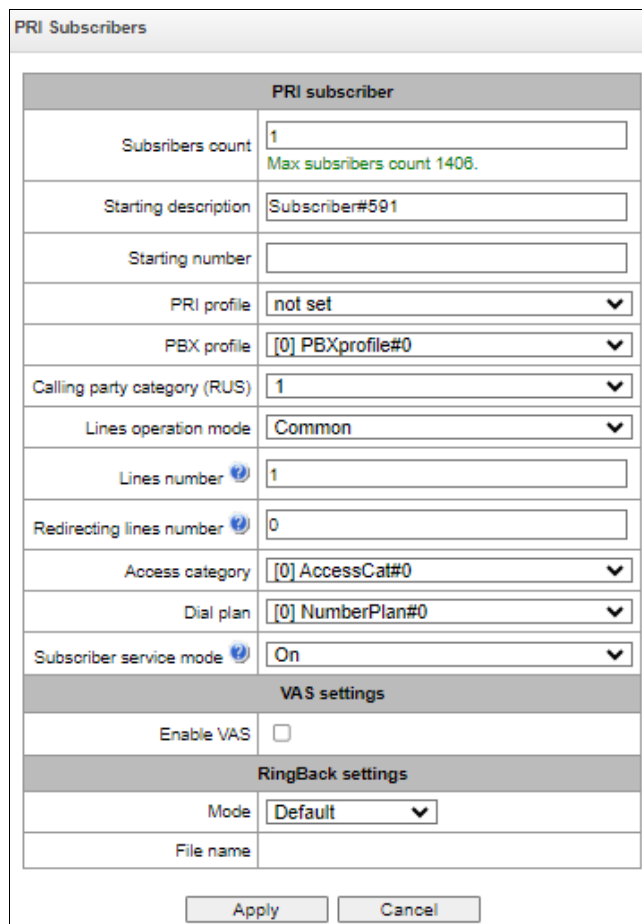
Subscribers → PRI Subscribers → Configuration



The screenshot shows a web interface for managing PRI subscribers. At the top, there's a 'Configuration' tab and a 'VAS management' sub-tab. Below this is a search bar with a dropdown menu set to 'by name' and a 'Search' button. A table with columns for '№', 'ID', 'Title', 'Number', 'Dial plan', 'Calling party category (RUS)', 'PRI profile', and 'Select' is visible. The table currently shows 10 rows. Navigation buttons for the table are present, along with 'Edit selected' and 'Remove selected' buttons at the bottom right.

PRI subscriber parameters

Subscribers → PRI Subscribers → Configuration → Object



The screenshot shows the configuration form for a specific PRI subscriber. The form is titled 'PRI Subscribers' and contains several sections:

- PRI subscriber** section:
 - Subscribers count: 1 (with a note: Max subscribers count 1406.)
 - Starting description: Subscriber#591
 - Starting number: (empty field)
 - PRI profile: not set (dropdown)
 - PBX profile: [0] PBXprofile#0 (dropdown)
 - Calling party category (RUS): 1 (dropdown)
 - Lines operation mode: Common (dropdown)
 - Lines number: 1
 - Redirecting lines number: 0
 - Access category: [0] AccessCat#0 (dropdown)
 - Dial plan: [0] NumberPlan#0 (dropdown)
 - Subscriber service mode: On (dropdown)
- VAS settings** section:
 - Enable VAS:
- RingBack settings** section:
 - Mode: Default (dropdown)
 - File name: (empty field)

At the bottom of the form are 'Apply' and 'Cancel' buttons.

-
- *Subscribers count* – number of subscribers;
 - *Starting description* – arbitrary text description of the subscriber;
 - *Starting number* – subscriber number, for a group of subscribers each subsequent one will be assigned a number increased by one;
 - *PRI profile* – PRI profile selection;
 - *PBX profile* – PBX profile selection (see PBX profiles);
 - *Calling party category (RUS)* – CallerID category;
 - *Lines operation mode* – setting limits on the number of simultaneous calls. Can take two values: *Common* and *Separate*. The *Common* mode takes into account the total number of simultaneous calls in which the subscriber can take part; in the *Separate* mode, incoming and outgoing calls are counted separately;
 - *Lines number* – number of simultaneous calls involving the subscriber. Field is displayed if the *Common* line operation mode is selected. Acceptable range values [1;255] or 0 – no limits;
 - *Ingress lines number* – the number of simultaneous incoming calls to the subscriber. The field appears if the line mode is set to *Separate*. The range of possible values is [1;255] or 0 – no limits;
 - *Egress lines number* – the number of simultaneous outgoing calls from the subscriber. The field appears if the line mode is set to *Separate*. The range of possible values is [1;255] or 0 – no limits;
 - *Redirecting lines number* – number of simultaneous calls for redirection. Valid range [1;255] or 0 – no limits;
 - *Access category* – select an access category;
 - *Dial plan* – define the dial plan for the subscriber;
 - *Subscriber service mode* – set a limit on the incoming and outgoing communication for the subscriber:
 - *off* – the port is out of service. The subscriber number is present in the dial plan, but the subscriber terminal cannot be registered. Therefore, incoming calls will be rejected with the *out of order* cause; outgoing calls cannot be initiated;
 - *on* – all types of communication are available;
 - *off 1* – incoming communication is enabled; outgoing communication is to special services only;
 - *off 2* – incoming communication is disabled; outgoing communication is to special services only;
 - *denied 1* – full prohibition for incoming and outgoing calls. Calls will be routed according to the dial plan, but be rejected;
 - *denied 2* – full prohibition for incoming and outgoing calls, except for special services;
 - *denied 3* – incoming calls are prohibited, outgoing calls are allowed;
 - *denied 4* – incoming calls are prohibited, outgoing calls are allowed only for local and department communication;
 - *denied 5* – incoming calls are allowed, outgoing calls are fully prohibited;
 - *denied 6* – incoming calls are allowed, outgoing calls are allowed only for special services;
 - *denied 6* – incoming calls are prohibited, outgoing calls are allowed only for local and private communication;
 - *denied 8* – incoming calls are allowed, outgoing calls are allowed only for local, private and zone communication;
 - *ignore* – the number is excluded from the dial plan. The number is completely excluded from the subscriber number list of the dial plan. If this number is called, the call will be rejected with the *no route to destination* cause, or it will be routed to the appropriate prefix in the dial plan.
-

VAS settings

- *Enable VAS*¹ – connection of VAS services for subscriber. When checked, the ‘VAS activation’ table is available.

VAS activation

Subscribers → PRI Subscribers → Configuration → Object → Enable VAS

VAS activation	
Call forward (Unconditional)	<input type="checkbox"/>
Call forward (Busy)	<input type="checkbox"/>
Call forward (No-reply)	<input type="checkbox"/>
Call forward (Out of service)	<input type="checkbox"/>
Call forward (Time)	<input type="checkbox"/>

- *Call Forward (Unconditional)* – enables the Call Forwarding Unconditional (CF Unconditional) service;
- *Call Forward (Busy)* – enables the Call Forwarding Busy (CF Busy) service;
- *Call Forward (No Reply)* – enables the Call Forwarding No Reply (CF No Reply) service;
- *Call Forward (Out of Service)* – enables the Call Forwarding Out of Service (CF Out of Service);
- *Call Forward (Time)* – enables the Call Forwarding by time.

A detailed description of the operation and configuration of VAS services is given in Appendix H. Working with VAS services.

RingBack settings

Allows one to configure the playback of an audio file for the subscriber individually.

Mode:

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

¹ The menu is available only in the firmware version with the SMG-VAS license, more details about licenses in the section Licenses.

4.1.7 Internal resources

4.1.7.1 CDR settings

This section describes parameters configuration to save call detail records. CDR is a call detail record, which allows the system to save the history of calls performed through SMG gateway. If the primary server is unavailable, CDR records are sent to the backup server (with appropriate configuration of the backup server) until communication with the primary server is restored. After the connection is restored, the CDR records sent to the backup server, will not be loaded to the primary server. Go to the 'Internal Resources' section and to the 'CDR Records' tab.

Internal resources → CDR settings

CDR settings	
Enable CDR	<input type="checkbox"/>
CDR files settings	
Create files	once per day ▼
Hours	1 ▼
Minutes	0 ▼
Add header	<input type="checkbox"/>
Signature	<input type="text"/>
Local storage settings	
Store files on local disk drive	<input type="checkbox"/>
Path to local disk drive	no path ▼
Directory usage	by date ▼
Keep files for: Days	0 ▼
Hours	0 ▼
Minutes	0 ▼
Remote storing settings	
Protocol	FTP ▼
Remote storage settings	
Store files on server	<input type="checkbox"/>
Server	<input type="text"/>
Server port	21
Path on server	<input type="text"/>
Login	<input type="text"/>
Password	*****
Other settings	
Save unsuccessfull calls	<input type="checkbox"/>
Save empty files	<input type="checkbox"/>
Write redirected call duration	<input type="checkbox"/>
Swap Redirecting number and CgPN	<input type="checkbox"/>
Round duration	upwards ▼
Modifiers for incoming numbers	
CdPN	not used ▼
CgPN	not used ▼
RedirPN	not used ▼
Modifiers for outgoing numbers	
CdPN	not used ▼
CgPN	not used ▼
RedirPN	not used ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

CDR settings

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

CDR files settings

CDR files settings	
Create files	periodically ▼
Days	0 ▼
Hours	1 ▼
Minutes	0 ▼
Add header	<input type="checkbox"/>
Signature	<input type="text"/>
Filename format	Date and time ▼

- *Create files* – select the mode to create CDR files:
 - *periodically* – CDR file is created after the specified period has elapsed since the device boot;
 - *once per day* – CDR file is created once a day at the specified time;
 - *once per hour* – CDR file is created once an hour at the specified time.
- *Saving period: Days, Hours, Minutes* – time period for CDR generation and saving in the device RAM;
- *Add header* – when this option is checked, the following header will be written at the beginning of the CDR file: SMG1016. CDR. File started at “YYYYMMDDhhmmss”, where “YYYYMMDDhhmmss” is the records saving start time;
- *Signature* – specifies a distinctive feature to identify the device, which created the record;
- *Filename format* – changing the CDR file name format. The option is only active when selecting ‘periodically’ file creation mode. The parameter can take the following values:
 - *Date and time* – changes the file name to ‘YYYYMMDDhhmmss.cdr’;
 - *Date only* – changes the file name to ‘YYYYMMDD.cdr’.

Local Storage Settings

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

- *Store files on local disk drive* – when this option is checked, save CDRs onto the local drive;
- *Path to local disk drive* – the path to the local drive. If the local drive path is selected, the menu displays the list of folders and files on that drive. To download data to your computer, select the checkbox for the required records and click *Download*. The folder with records will be moved to the archive, which is recommended to delete after the boot to avoid the disk overflow. To remove the outdated data from your computer, select the checkbox for the required records and click *Remove*;
- *Directory usage* – select the directories for CDR data storage:
 - *by date* – CDRs are saved into separate directories, where the directory name corresponds to the CDR file creation date and the name format is “cdryymmdd”, for example, cdr20150818;
 - *single directory* – all CDRs are saved into a single cdr_all directory located on the selected drive.
- *Keep files for: Days, Hours, Minutes* – the period to keep CDRs on the local drive.



When the the remote server for CDR storage is not available, CDRs will be saved to the device RAM. When the memory is full, a warning message will be generated, followed by a failure alarm. For CDR file saving indication, see section 3.2.6 LED Indication. The thresholds for warning and failure alarms are described in the table of memory thresholds for CDRs saving.



When the failure status is activated, the corresponding SNMP trap is sent.

Table of memory thresholds for CDR saving

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

	SMG-1016M	SMG-2016	SMG-3016
Total memory allocated:	30 MB	512 MB	512 MB
Memory thresholds for alarm messages:			
- warning	512 KB	20 MB	20 MB
- failure	5 MB	85 MB	85 MB
- critical failure	15 MB	255 MB	255 MB

One CDR takes from 200 to 400 bytes. Thus, 1 MB of memory can store from 2600 to 5200 records.

Remote storing settings

Remote storing settings	
Protocol	FTP ▼

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

Remote storage settings

Remote storage settings	
Store files on server	<input type="checkbox"/>
Server	<input type="text"/>
Server port	21
Path on server	<input type="text"/>
Login	<input type="text"/>
Password	*****

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



Remote backup storage settings

Remote backup storage settings	
Store files on server	<input type="checkbox"/>
Only if primary server failed	<input type="checkbox"/>
Server	<input type="text"/>
Server port	21
Path on server	<input type="text"/>
Login	<input type="text"/>
Password	*****

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




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

Other settings

Other settings	
Save unsuccessfull calls	<input type="checkbox"/>
Save empty files	<input type="checkbox"/>
Write redirected call duration	<input type="checkbox"/>
Swap Redirecting number and CgPN 	<input type="checkbox"/>
Round duration	upwards 

- *Save unsuccessful calls* – when this option is checked, unsuccessful calls (not resulted in conversation) will be recorded into CDR files;
- *Save empty files* – when this option is checked, CDR files containing no records are saved;
- *Write redirected call duration* – when this option is checked, the CDR for a call redirected from “discinfo: redirected call;”, will contain actual call duration; when unchecked, the duration will be set to zero;
- *Swap Redirecting number and CgPN* – the option applies to calls redirected in case the CgPN and the Redirecting number fields in the CDR are used simultaneously. If there is no Redirecting number field in the CDR, the CgPN value is automatically replaced with Redirecting number value for redirected calls;
- *Round duration* – this option specifies the mode for the call duration rounding off in CDRs:
 - *upwards* – call duration rounding mode; the call duration is rounded up if it exceeds 330 ms;
 - *downwards* – call duration rounding mode; the call duration is rounded down if it exceeds 850 ms;
 - *without round (use msec)* – in this mode, the call duration is not rounded up or down, and is recorded to the nearest millisecond.

Modifiers for incoming numbers

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

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

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

Modifiers for outgoing numbers

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

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

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

4.1.7.1.1 Lists of fields CDR used

Internal resources → CDR settings

List of fields CDR used	
Added	Available
1. Device Sign	Redirecting mark
2. Connect time	Pickup mark
3. Duration	Release side mark
4. Release cause	Incoming SS7 CIC
5. Call release info	Incoming SIP Call-ID
6. Incoming IP-address	Outgoing SS7 CIC
7. Incoming type	Outgoing SIP Call-ID
8. Incoming description	Incoming SS7 category
9. Incoming CgPN	Incoming Calling party category (RUS)
10. Outgoing CgPN	Outgoing SS7 category
11. Outgoing IP-address	Outgoing Calling party category (RUS)
12. Outgoing type	Incoming E1 stream
13. Outgoing description	Incoming E1 channel
14. Incoming CdPN	Outgoing E1 stream
15. Outgoing CdPN	Outgoing E1 channel
16. Setup time	Sequence number
17. Disconnect time	Incoming redirecting number
18. Rejecting RADIUS server address	Outgoing redirecting number
	RADIUS Accounting-Session-Id
	Global Callref
	Incoming numplan
	Outgoing numplan
	UniqueTag identifier
	Calling NAI
	Called NAI
	Incoming redirecting NAI
	Outgoing redirecting NAI
	Call transfer mark
	Call record path
	IVR call record path

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

The following buttons are located under the list:

- *Add all* – relocate all available fields to the *Added* column;
- *Remove all* – remove all fields from the *Added* column;
- *Default* – the basic set of fields remains in the *Added* column (see the list of fields in 4.1.7.1.2 Default CDR format section).

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

4.1.7.1.2 Default CDR format

- *First line* – a general header for an entire CDR file (this parameter is displayed if the corresponding setting is selected);
- *Next lines* – CDRs in the form of fields separated by semicolons ';'. The basic set of fields is as follows:
 - Device sign;
 - Setup time in YYYY-MM-DD hh:mm:ss format (for unsuccessful calls, this parameter is equal to the disconnect time);
 - Duration, seconds;
 - Release cause, according to ITU-T Q.850;
 - Call release info.

Information about a calling subscriber:

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

Information about a called subscriber:

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

4.1.7.1.3 Description of CDR files

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

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

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

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

Call release info:

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

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

Incoming/outgoing Types

- *SIP-user* – SIP subscriber;
- *v52-user* – V5.2 subscriber;
- *user-service* – use of VAS, only for the source type;
- *trunk-SIP* – SIP trunk;
- *trunk-SS7* – SS7 trunk;
- *trunk-Q.931* – ISDN PRI trunk;
- *trunk-H.323* – H.323 trunk.

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

- *Redirection* – call forwarding;
- *CallTransfer* – call transfer;
- *CallPickup* – call pickup;
- *ServiceManagement* – management of VAS;
- *Conference* – ad-hoc conference;
- *IVR* – call from IVR system;
- *3way* – three-way conference.

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

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

Redirecting mark:

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

Pickup mark:

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

Release side mark:

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

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

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

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

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

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

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

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

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

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

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

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

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

Incoming/outgoing numplan – the number of the dial plan in which the call arrived and left;

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

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

- 0 – Spare;
- 1 – Subscriber number;
- 2 – Unknown;
- 3 – National (significant) number;
- 4 – International number, where:
 - Local – Subscriber;
 - International communications – INTERNATIONAL;
 - Long-distance communications – NATIONAL;
 - Emergency, Zone and Department – unknown.

Call Transmission Label – shows the call transmission label:

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

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

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

4.1.7.1.4 CDR File Example

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

1. Entry sequence number;
2. Device sign;
3. Connect time;
4. Setup time;
5. Disconnect time;
6. Call duration;
7. Release cause Q.850;
8. Call release info;
9. Release side mark;
10. Redirecting mark;
11. Pickup mark;
12. Incoming type;
13. Incoming description;
14. Incoming E1 stream;
15. Incoming IP address;
16. Incoming CgPN;
17. Outgoing CgPN;
18. Outgoing type;
19. Outgoing description;
20. Outgoing E1 stream;
21. Outgoing IP address;
22. Incoming CdPN;
23. Outgoing CdPN.

RADIUS Accounting-Session-Id

SMG2016. CDR. File started at '20161213115258'

```
20161210124301-00000;SMG 2016 ELTZ;2016-12-13 11:52:58.126;2016-12-13 11:52:58.465;2016-12-13
11:52:58.479;0.014;16;user answer;originate;normal;normal;trunk-SIP;sipp_in;;
192.168.0.123;20001;20001;trunk-SS7;TrunkSS7_00;0;0.0.0.0;10001;10001;11000321 584f7eaa 65a813f9
53681e51;
```

```
20161210124301-00001;SMG 2016 ELTZ;2016-12-13 11:52:58.134;2016-12-13 11:52:58.462;2016-12-13
11:52:58.483;0.021;16;user answer;originate;normal;normal;trunk-
SS7;TrunkSS7_01;1;0.0.0.0;20001;20001;trunk-SIP;sipp_out;;192.168.1.123;10001;10001;06000106
584f7eaa
59a880c4 5b369253;
```

20161210124301-00002;SMG 2016 ELTZ;2016-12-13 11:52:58.026;2016-12-13 11:53:00.049;2016-12-13 11:53:00.062;0.013;16;user answer;originate;normal;normal;trunk-SIP;sipp_in;;
192.168.0.123;20000;20000;trunk-SS7;TrunkSS7_00;0;0.0.0.0;10000;10000;11000043 584f7ea9 5068f1a1 418fbc82;

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

4.1.7.1.5 Maximum size of CDR fields

Parameter	Maximum field size
Device Sign	63
Setup time	63
Connect time	63
Disconnect time	63
Duration	15
Release cause	4
Call release info	63
Incoming IP-address	31
Incoming type	63
Incoming description	63
Outgoing IP-address	31
Outgoing type	63
Outgoing description	63
Incoming CgPN	41
Outgoing CgPN	41
Incoming CdPN	41
Outgoing CdPN	41
Incoming redirecting number	41
Outgoing redirecting number	41
Redirecting mark	31
Pickup mark	31
Release side mark	31
Incoming SS7 SIC	15
Incoming SIP Call-ID	255
Outgoing SS7 CIC	15
Outgoing SIP Call-ID	255
Incoming SS7 category	3
Incoming Calling party category (RUS)	3
Outgoing SS7 category	3
Outgoing Calling party category (RUS)	3
Incoming E1 stream	3
Incoming E1 channel	3
Outgoing E1 stream	3
Outgoing E1 channel	3
Sequence number	15
RADIUS Accounting-Session-Id	63
Global Callref	63
Incoming numplan	3
Outgoing numplan	3
UniqueTag	63
NAI	4
Call transfer mark	16

4.1.7.2 SS7 Categories

Internal resources → SS7 categories

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

Apply

In this section, the correspondence between Caller ID categories and SS7 protocol categories can be specified.

Generally accepted correspondence between SS7 categories and Caller ID categories is provided below.

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

4.1.7.3 Access categories


Internal resources → SS7 categories

Access categories		
Nr	Category	Access to categories
0	AccessCat#0	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
1	AccessCat#1	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
2	AccessCat#2	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
3	AccessCat#3	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
4	AccessCat#4	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
5	AccessCat#5	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
6	AccessCat#6	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
7	AccessCat#7	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
8	AccessCat#8	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
9	AccessCat#9	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
10	AccessCat#10	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
11	AccessCat#11	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
12	AccessCat#12	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
13	AccessCat#13	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
14	AccessCat#14	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
15	AccessCat#15	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
16	AccessCat#16	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
17	AccessCat#17	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
18	AccessCat#18	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
19	AccessCat#19	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
20	AccessCat#20	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
21	AccessCat#21	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
22	AccessCat#22	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
23	AccessCat#23	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
24	AccessCat#24	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
25	AccessCat#25	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
26	AccessCat#26	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
27	AccessCat#27	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
28	AccessCat#28	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
29	AccessCat#29	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
30	AccessCat#30	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
31	AccessCat#31	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
32	AccessCat#32	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
33	AccessCat#33	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
34	AccessCat#34	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
35	AccessCat#35	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
36	AccessCat#36	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
37	AccessCat#37	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
38	AccessCat#38	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
39	AccessCat#39	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

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

To restrict an access to an object, you should assign the corresponding category; for other categories, specify accessibility to a category assigned to an object in this menu (deny access — deselect the checkbox next to the corresponding category, allow access — select the checkbox next to the corresponding category).

128 access categories are available for configuration in total. By default, access on each of them is defined for the first 16 categories.

To proceed to category configuration and editing, click  button.

Access restriction configuration example

To restrict the long-distance communication, you should:

1. Select an access category for the long-distance communication. Specify name 'National long-distance call' for convenience.

Internal resources → Access categories → Object

2. Select 2 categories for subscribers: 'Subscriber with long-distance' and 'Subscriber w/o long-distance' and allow/deny an access to 'National long-distance call' category respectively (select/deselect the checkbox next to 'National long-distance call' category).

Internal resources → Access categories → Object

3. For transition to 8 prefix, select 'National long-distance call' category and 'Check access category' checkbox.

Internal resources

4. Assign *'Subscriber with long-distance'* category to subscribers with enabled access to long-distance communication.
5. Assign *'Subscriber w/o long-distance'* category to subscribers with disabled access to long-distance communication.

SIP subscriber 0		SIP subscriber 1	
Subs.ID	1	Subs.ID	2
Description	Subscriber#000	Description	Subscriber#001
Number	774000	Number	774005
CallerID number		CallerID number	
CallerID number type	Subscriber	CallerID number type	Subscriber
CallerID category	1	CallerID category	1
Lines number	1	Lines number	1
IP-address	0.0.0.0	IP-address	0.0.0.0
SIP domain		SIP domain	
SIP profile	not set	SIP profile	not set
PBX profile	[0] PBXprofile#0	PBX profile	[0] PBXprofile#0
Access category	[4] subscriber with long-distance	Access category	[5] subscriber w/o long-distance
Dial plan	[0] Основной	Dial plan	[0] Основной
Authorization	not set	Authorization	not set
Login		Login	
Password	*****	Password	*****
Ignore source port after registration	<input type="checkbox"/>	Ignore source port after registration	<input type="checkbox"/>
Subscriber service mode	On	Subscriber service mode	On
Busy-Lamp-Field (BLF) settings		Busy-Lamp-Field (BLF) settings	
Enable subscription	<input type="checkbox"/>	Enable subscription	<input type="checkbox"/>
Max subscribers number	10	Max subscribers number	10
Monitoring group	0	Monitoring group	0
Intercom call settings		Intercom call settings	
Intercom call type	one-way	Intercom call type	one-way
Intercom call priority	3	Intercom call priority	3
Intercom SIP-header	Answer-Mode: Auto	Intercom SIP-header	Answer-Mode: Auto
Pause before answer, sec	0	Pause before answer, sec	0
VAS settings		VAS settings	
CLIRO	<input type="checkbox"/>	CLIRO	<input type="checkbox"/>
Enable VAS	<input type="checkbox"/>	Enable VAS	<input type="checkbox"/>
Voice mail	not set	Voice mail	not set
Timeout for switching to voice-mail, sec	20	Timeout for switching to voice-mail, sec	20
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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.

4.1.7.4 Routing by access category

When a route is searched by number masks in the numbering plan, there is a check for prefix/call group accessibility by access category. If the *check access category* checkbox is not selected on the prefix/group, the route is considered unconditionally accessible.

Now it is possible to create several completely identical masks leading to different prefixes with different access categories.

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




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

4.1.7.5 PBX profiles




PBX profiles allow for assignment of additional parameters to SIP subscribers.

Subscribers → PBX profiles

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

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

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

Subscribers → PBX profiles → Object

PBX profile 1	
Description	PBX_Profile01
Station prefix	
Direct routing prefix	no prefix
Scheduled routing profile	Not selected
Adding participants to the conference	Auto
Ingress calls	
Use voice messages	<input type="checkbox"/>
No Connected number transit	<input type="checkbox"/>
Copy CgPN into Redirecting number	<input type="checkbox"/>
Use Redirecting number for routing	<input type="checkbox"/>
CdPN modifiers	not used
CgPN modifiers	not used
List of reasons for call recovery after outbound leg failure	not set
Egress calls	
CdPN modifiers	not used For SIP subscribers only
CgPN modifiers	not used For SIP subscribers only
RingBack settings	
Mode	Default
File name	
Timeouts	
First digit timeout, sec	15
Next digit timeout, sec	5
Busy-tone timeout, sec	60
Timeout for call answer, sec (for V5.2 abonents)	90
Timeout for call hold, sec (for V5.2 abonents)	60
VAS timeouts	
CFNR timeout, sec	10
Timeout for call park, sec	300
Flash signal settings	
Flash mode (for V5.2 abonents)	Treat as on-hook
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- *Description* — name of the profile;
- *Station prefix* — prefix added into the beginning of the SIP subscriber number (CgPN);
- *Direct routing prefix* — transition to the prefix without caller or callee number analysis. It enables switching of all calls coming from SIP subscriber to a trunk group configured on the direct prefix regardless of the dialed number (without mask creation in prefixes);
- *Scheduled routing profile* — select 'scheduled routing' service profile, configured in the 'Internal resources' section.

Ingress calls:

- *Use voice messages* — when checked, pre-recorded voice messages stored in the device memory will be played upon the occurrence of specific events; for details, see Appendix I. Voice messages and music on hold (MOH);
- *No Connected number transit* — disable transmission of the Connected number field;
- *Copy CgPN into Redirecting number* — when checked, if there is no Redirecting number in an incoming call, it will be formed from CgPN number;
- *Use Redirecting number for routing* — when checked, the 'Redirecting number' field will be used for SS7 or Q.931 signaling protocols, or SIP protocol 'diversion' field for incoming call routing in the dial plan using CgPN number masks;

- *CdPN modifiers* — designed for modifications based on the analysis of the callee number received from the incoming channel;
- *CgPN modifiers* — designed for modifications based on the analysis of the caller number received from the incoming channel;
- *List of reasons for call recovery after outbound leg failure* — selecting the “List of reasons for Q.850 recovery” table to configure Q.850 Disconnect Reasons for call recovery after outbound leg failure. If a call received through a PBX profile with activated setting, was not rejected by the incoming side, and the reason for rejecting is in the selected table, then SMG will try to restore the conversation on shoulder A without interrupting communication using a repeat call or alternative routes when the main one is unavailable.

Egress calls:

- *CdPN modifiers* are dedicated for modifications based on callee number analysis before sending to an egress channel;
- *CgPN modifiers* are dedicated for modifications based on caller number analysis before sending to an egress channel.

RingBack settings

Allows configuring playback of an audio file for a group of subscribers who belong to specific PBX profile.

Mode:

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

Timeouts:

- *First digit timeout, sec* — dialing timeout for the first digit of a number after the subscriber presses FLASH button during 'call transfer' service. When this timeout expires, busy tone will be played to a subscriber, range is from 5 to 20 seconds;
- *Next digit timeout, sec* — dialing timeout for the digit that follows the first digit of a number during 'call transfer' service. When this timeout expires, end of dial will be detected and the call will be routed, range is from 5 to 20 seconds;
- *Busy-tone timeout, sec* — busy tone timeout for the unsuccessful dialing during 'call transfer' service. When this timeout expires, call will be switched to the subscriber being on hold;
- *Timeout for call answer, sec (for V5.2 abonents)* – timeout for answering a call, when it expires, the call will be released;
- *Timeout for call hold, sec (for V5.2 abonents)* – timeout for subscribers being on hold.

VAS timeouts:

- *CFNR timeout, sec* – when this timeout expires, the VAS ‘Call forward on no response’ will be activated. The range is 5 – 60 seconds;
- *Timeout for call part, sec* – timeout, after which the subscriber will take a callback after installing it in the parking slot, a callback will be triggered to the installation initiator in slot.

Flash signal settings (for V5.2 abonents):

- *Treats as on-hook* – the flash signal is taken as short hangup;
- *Flash1,2,3* – select flash signals parameters block. The block of parameters is configured on AN.





4.1.7.6 Modifier tables

Internal resources → Modifiers table

Modifiers tables						
No	Name	TrunkGroups	PBX profiles	RADIUS profiles	CDR settings	E1 streams (SORM)
0	cdpn_cut_first	Trunk931_1_U smg4_out smg4_in Trunk SMG1016m_in				
1	ModTable#01					
2	ModTable#02					
3	cdpn_E1_normalize	Trunk SS7_00 Trunk SS7_01 Trunk931_1_U Trunk931_2_N 931_out 931_in SS7_2xx_out SS7_2xx_in				
4	fix_cgpn_for_asterisk	TrunkAsterisk Trunk SS7_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'
-  — 'Remove modifier'
-  — 'Add modifier by copying'


Common settings of modifiers table:


Internal resources → Modifiers table → Object

Modifiers tables




Modifiers table 0

Name:

Long timer: 

Short timer: 

Modifiers:

  1. ([35]400xx) 

- *Name* – the displayed name of the table;
- *Long timer* – timeout for number dialing in overlap mode;
- *Short timer* – timeout for digit dialing in overlap mode;
- *Modifiers* – the list of modifiers used in the table.

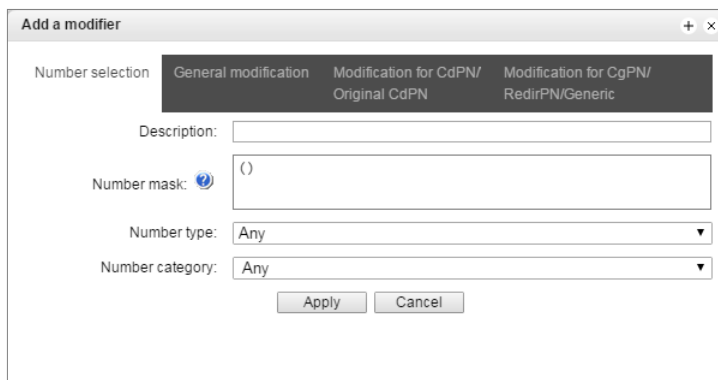
To assign/edit parameters of created modifier, select the respective row and click .

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

Click the link 'Check number' below the modifiers table to check modifiers operation. The description of check procedure is presented in the section 4.1.7.6.4.2 Modifiers check.


4.1.7.6.1 Number selection tab

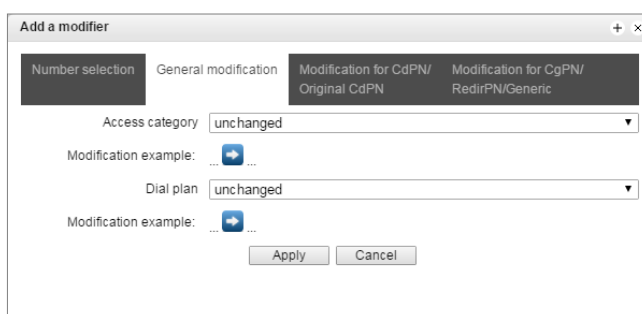
Internal resources → *Modifiers table* → *Object* → 




- *Description* — modifier description;
- *Number mask* — template or set of templates that the subscriber number will be compared with (for mask syntax, see 4.1.4.2 Description of Number Mask and Its Syntax);
- *Number type* — subscriber number type:
 - *Subscriber* — subscriber number (SN) in E.164 format;
 - *National* — national number. Number format: NDC + SN, where NDC — national destination code;
 - *International* — international number. Number format: CC + NDC + SN, where CC — country code for geographic area;
 - *Network specific* — specific network number;
 - *Unknown* — unknown number type;
 - *Any* — modification will be performed for any number type;
 - *Unsupported* — a number type which is not supported on SMG.
- *Number category* — subscriber's Caller ID category.


4.1.7.6.2 General modification tab

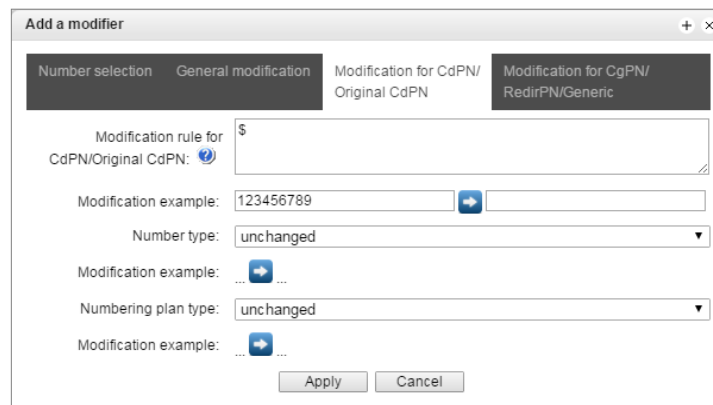
Internal resources → *Modifiers table* → *Object* →  → *General modification*





- *Modification example* — click  button to view the modification summary after application of the modification rules specified;
- *Access category* — allows to modify the access category;
- *Dial plan* — allows to modify dial plan that will be used for further routing (necessary for dial plan negotiation).

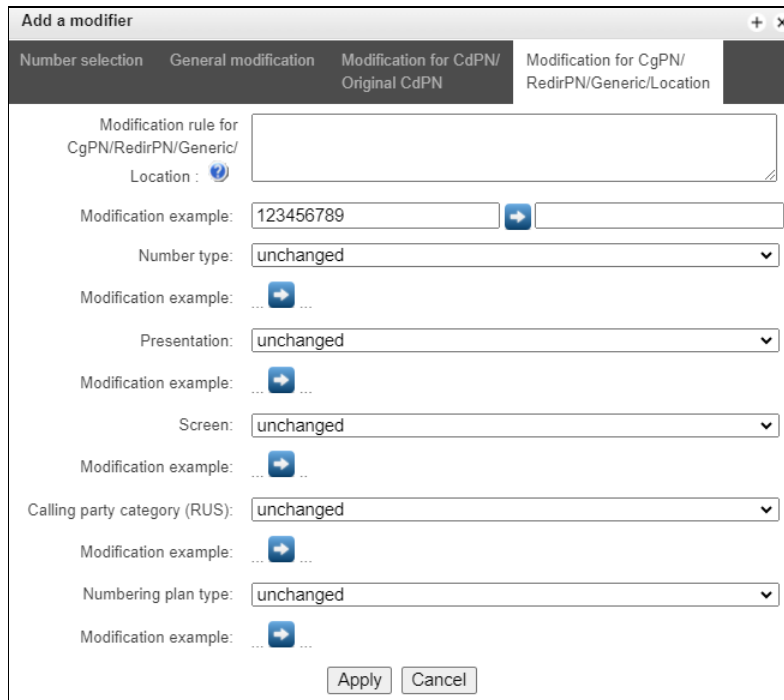
4.1.7.6.3 CdPN/Original CdPN modification tab


Internal resources → Modifiers table → Object →  → Modification for CdPN/Original CdPN



- **Modification rule for CdPN/Original CdPN** — callee number modification rule. For syntax being used, see 4.1.7.6.4.1 Modification rule syntax; for example use, see Appendix C. This rule also applies to modification of the callee initial number (original Called party number) when this modifier table is selected in the 'trunk group' session for Original CdPN modification;
- **Modification example** — click  button to view the modification summary after application of the specified modification rules. We recommend defining a number that will be subject to modification instead of number 123456789 entered in the rule check example;
- **Number type** — callee number type modification rule.
 - *Unknown* – undefined number;
 - *Subscriber* – subscriber number (SN) in E.164 format;
 - *National* – national number. The number has the following format: NDC + SN, where NDC – a geographic zone code;
 - *International* – international number. The number has the following format: CC + NDC + SN, where CC is a country code;
 - *Network specific* – specific network number;
 - *Unchanged* – leave the type of a number unchanged.
- **Numbering plan type** — dial plan type modification rule.
 - *Unchanged*;
 - *Unknown* – unknown type of dial plan;
 - *Isdn/telephony* – a dial plan according to ITU-T E.164 recommendations;
 - *National* – national number. The number has the following format: NDC + SN, where NDC – a geographic zone code;
 - *Private* – a private dial plan.

Internal resources → Modifiers table → Object →  → Modification for CgPN/RedirPN/Generic



- *Modification rule for CgPN/RedirPN/Generic/Location* — callee number modification rule. For syntax being used, see 4.1.7.6.4.1 Modification rule syntax; for example use, see Appendix C. This rule also applies to modification of the callee redirecting number when this modifier table is selected in the 'trunk group' session for Redir PN modification; for Generic Number modification, if the table is selected in GenericPN modification section; for Location Number modification, if the table is selected in LocationNumber modification section;
- *Modification example* — click  button to view the modification summary after application of the modification rules specified. We recommend defining a number that will be subject to modification instead of number 123456789 entered in the rule check example;
- *Number type* — caller number type modification rule;
- *Presentation* — caller presentation modification rule;
- *Screen* — caller screen indicator modification rule;
- *Number category* — caller category modification rule;
- *Numbering plan type* — dial plan type modification rule:
 - *unchanged*;
 - *Unknown* – unknown type of dial plan;
 - *Isdn/telephony* – a dial plan according to ITU-T E.164 recommendations;
 - *National* – national number. The number has the following format: NDC + SN, where NDC – a geographic zone code;
 - *Private* – a private dial plan.

4.1.7.6.4.1 Modification rule syntax

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

'.' and '-.': special characters indicating the removal of digits at the current position and the transposition of digits that follow to a location of that digit.

'X', 'x': special characters indicating that the digit remains unchanged at the current position (the digit is mandatory at the current position).

'?': special character indicating that the digit remains unchanged at the current position (the digit is arbitrary at the current position).

'+' : special character indicating that all characters located between the current position and the next special character (or end of sequence) are inserted at the specified location of the number.

'!': special character indicating the breakdown finish, all other digits of a number are truncated.

'\$': special character indicating the breakdown finish, all other digits of a number remain unchanged.

0-9, D, # and * (without preceding special character '+'): informational characters that substitute the digit at the specified location of the number.

Modification example:

Add the city code 383 to the number 2220123

Modifier: +383

Result: 38322201234

Replace country code with 7 in the number 83832220123

Modifier: 7

Result: 738322201234

Replace the third digit in the number 2220123 with 6

Modifier: xx6\$ or XX6\$

Result: 22601234

Remove the prefix 99# in the number 99#2220123

Modifier: ---\$

Result: 2220123

Remove the last 4 digits in the number 22201239876

Modifier: \$----

Result: 2220123

Select the first seven digits of the number 222012349876

Modifier: xxxxxx!

Result: 2220123

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

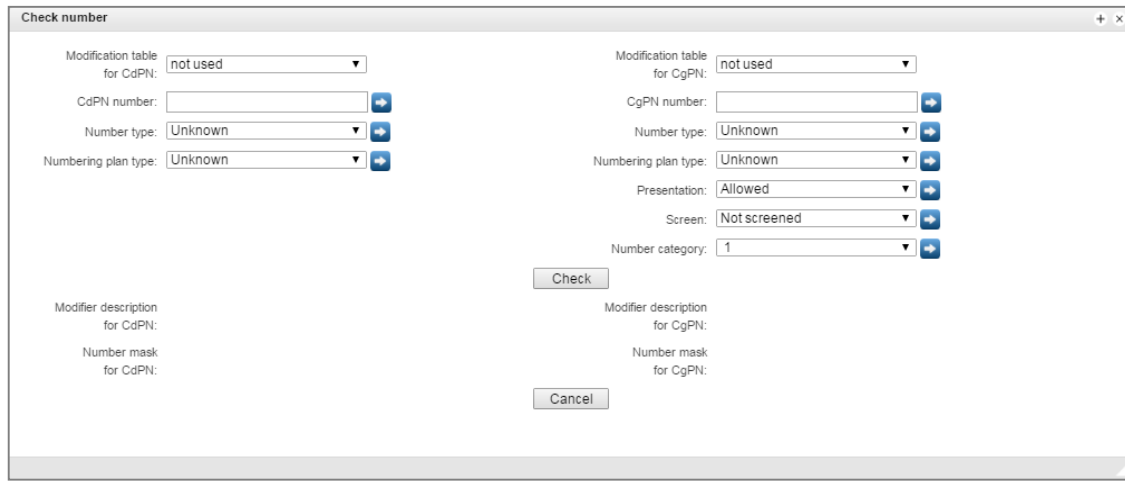
Modifier: +383xx6\$--

Result: 3832260123

4.1.7.6.4.2 Modifiers check

You can check modifiers on a number with parameters specifying, using a 'Check number' button below the table.

Internal resources → Modifiers table → Check number

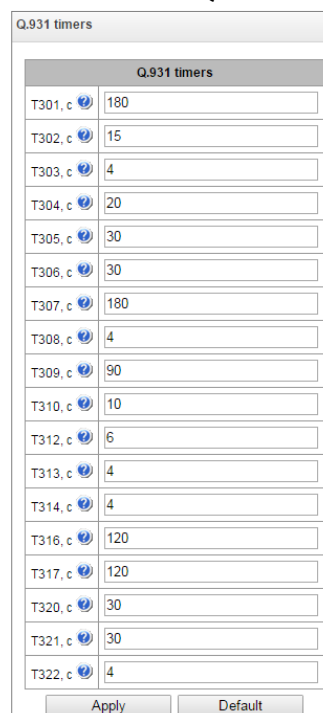


Set CdPN and CgPN numbers, fill 'Number type', 'Numbering plan type', 'Presentation', 'Screen', 'Number category' fields, then choose needed modification table for CgPN and CdPN and click the 'Check' button. The values which will be assigned to the number will be displayed next to the blue arrows. The numbers masks which were investigated and descriptions of modifiers which were included to the modifiers table will be displayed below.

If the modification table contains only SORM modifiers, then this table will not be displayed in the 'Check number' service, because the check does not work for tables with SORM modifiers.

4.1.7.7 Q.931 timers

Internal resources → Q.931 timers



Q.931 timers	
T301, c	180
T302, c	15
T303, c	4
T304, c	20
T305, c	30
T306, c	30
T307, c	180
T308, c	4
T309, c	90
T310, c	10
T312, c	6
T313, c	4
T314, c	4
T316, c	120
T317, c	120
T320, c	30
T321, c	30
T322, c	4

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

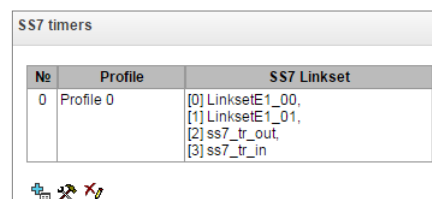
Timer names and default values are described in Q.931 ITU-T recommendation, Paragraph no. 9, List of system parameters.

Name	Default value, seconds	Range, seconds
T301	180	30 – 360
T302	15	10 – 25
T303	4	4 – 10
T304	20	20 -30
T305	30	30 – 40
T306	30	30 -40
T307	180	180 – 240
T308	4	4 – 10
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

4.1.7.8 SS7 timers




In this section, you may configure MTP2, MTP3 and ISUP level timers of SS7 protocol.

Internal resources → SS7 timers



No	Profile	SS7 Linkset
0	Profile 0	[0] LinksetE1_00, [1] LinksetE1_01, [2] ss7_tr_out, [3] ss7_tr_in

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

-  — 'Add profile'
-  — 'Edit profile parameters'
-  — 'Remove profile'

- *No.* — SS7 timer profile sequence number.
- *Profile* — profile name.
- *SS7 Linkset* — list of SS7 link sets that have this profile selected.

Internal resources → SS7 timers → Object

SS7 timers

Profile 0

MTP2 timers	Value	MTP3 timers	Value	ISUP timers	Value
T1, x100ms	400	T2, x100ms	15	T1, x100ms	500
T2, x100ms	110	T4, x100ms	8	T5, x100ms	6000
T3, x100ms	12	T12, x100ms	10	T6, x100ms	300
T4n, x100ms	80	T13, x100ms	10	T7, x100ms	300
T4e, x100ms	6	T14, x100ms	25	T8, x100ms	100
T6, x100ms	45	T17, x100ms	10	T9, x100ms	1800
T7n, x100ms	20	T21, x100ms	630	T12, x100ms	500
		T22, x100ms	1800	T13, x100ms	6000
		T23, x100ms	1850	T14, x100ms	500
				T15, x100ms	6000
				T16, x100ms	500
				T17, x100ms	6000
				T18, x100ms	500
				T19, x100ms	6000
				T20, x100ms	500
				T21, x100ms	6000
				T22, x100ms	500
				T23, x100ms	6000
				T24, x100ms	10
				T25, x100ms	50
				T26, x100ms	600
				T33, x100ms	150
				T34, x100ms	40
				T35, x100ms	200

Apply Cancel Default

Table 21 — MTP2 level timers names and default settings are described in Q.703 ITU-T recommendation, Paragraph 12.3, Timers.

Name	Default value, seconds	Range, seconds
T1	50	40 – 50
T2	50	5 – 150
T3	2	1 – 2
T4n	8.2	7.5 – 9.5
T4e	0.5	0.4 – 0.6
T6	6	3 – 6
T7n	2	0.5 – 2

Table 22 — MTP3 level timers names and default settings are described in Q.704 ITU-T recommendation, Paragraph 16.8, Timers and timer values.

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

Table 23 — ISUP level timer name and default values are described in Q.764 ITU-T recommendation, Appendix A, Table A.1/Q.764 – Timers in the ISDN user part.

Name	Default value, seconds	Range, seconds
T1	60	15 – 60
T5	900	150 – 900
T6	30	10 – 60
T7	30	20 – 30
T8	15	10 – 15
T9	180	30 – 240
T12	60	15 – 60
T13	900	150 – 900
T14	60	15 – 60
T15	900	150 – 900
T16	60	15 – 60
T17	900	150 – 900
T18	60	15 – 60
T19	900	150 – 900
T20	60	15 – 60
T21	900	150 – 900
T22	60	15 – 60
T23	900	150 – 900
T24	2	0 – 2
T25	10	1 – 10
T26	180	60 – 180
T33	15	12 – 15
T34	4	2 – 4
T35	20	15 – 20

Timer values can be reset using the '*Default*' button to the values recommended in ITU-T Q.703, Q.704 and Q.764.




4.1.7.9 Q.850-cause and SIP-reply code correspondence table

In this section, you may establish a correspondence between release causes described in Q.850 recommendations for SS7, PRI protocols and 4xx, 5xx, 6xx class SIP replies.

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

Internal resources → Q.850-cause to SIP-reply mapping

Q.850-cause and SIP-reply mapping table	
No	Name
0	Profile #0

Internal resources → Q.850-cause to SIP-reply mapping → Object

Q.850-cause and SIP-reply mapping table

Profile 0




Name:

Q.850-cause to SIP-reply mapping table




Nz	Cause	Reply
0	15	502
1	46	403

SIP-reply to Q.850-cause mapping table

Nz	Reply	Cause
0	502	4

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

-  — 'Add rule'
-  — 'Edit rule parameters'
-  — 'Remove rule'

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

Profile settings:

Internal resources → Q.850-cause to SIP-reply mapping → Object

Q.850-cause and SIP-reply mapping table

Mapping

Direction:

Q.850-cause:

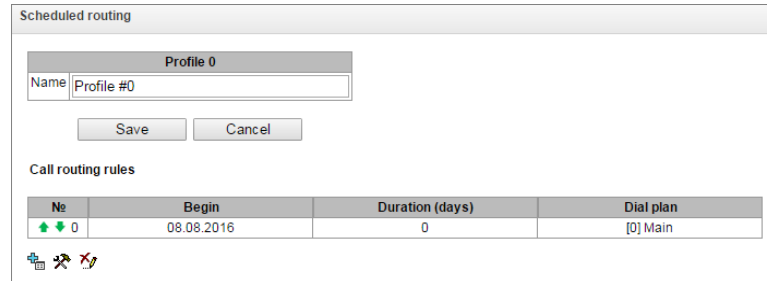
SIP-reply:

- *Direction:*
 - *SIP-reply → Q.850-cause* — direction from SIP side to Q.850 side.
 - *Q.850-cause → SIP-reply* — direction from Q.850 side to SIP side.
- *Q.850-cause* — Q.850 cause value;
- *SIP-reply* — 4xx, 5xx, 6xx class SIP reply value.

4.1.7.10 Scheduled routing


In this section, you may configure scheduled routing function that allows to use different dial plans depending on the time and day of the week.

Internal resources → Scheduled routing



No	Begin	Duration (days)	Dial plan
0	08.08.2016	0	[0] Main


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

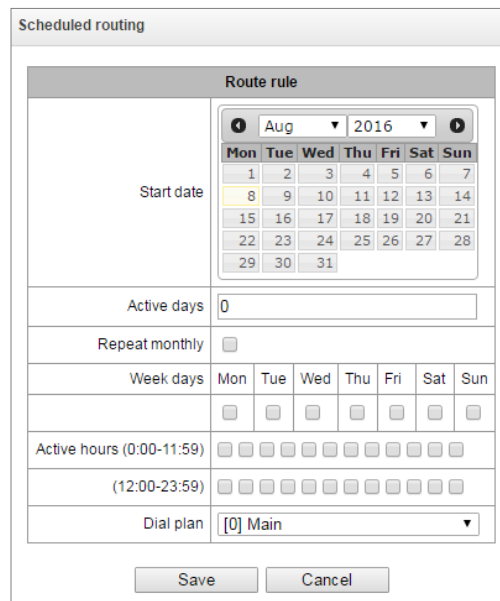
 — 'Add rule'

 — 'Edit rule parameters'

 — 'Remove rule'

Routing rule:

Internal resources → Scheduled routing → 

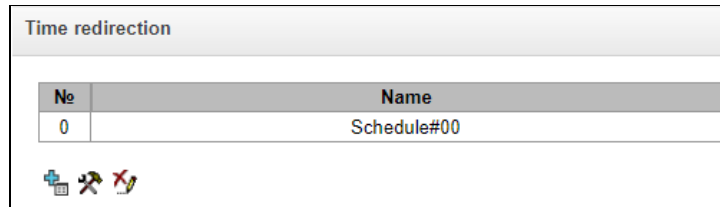


- *Start date* — select start date for scheduled routing rule operation.
- *Active days* — scheduled routing rule operation duration.
- *Repeat monthly* — option that allows you to set the repetition of routing rule operation for each month.
- *Week days* — select days of the week for scheduled routing rule operation.
- *Active hours* — select hours for scheduled routing rule operation
- *Dial plan* — select dial plan that will be used during scheduled routing rule operation.

4.1.7.11 Time redirection

Time redirection allows one to set forwarding schedules for subscribers. To configure forwarding time intervals, you need to create a schedule:

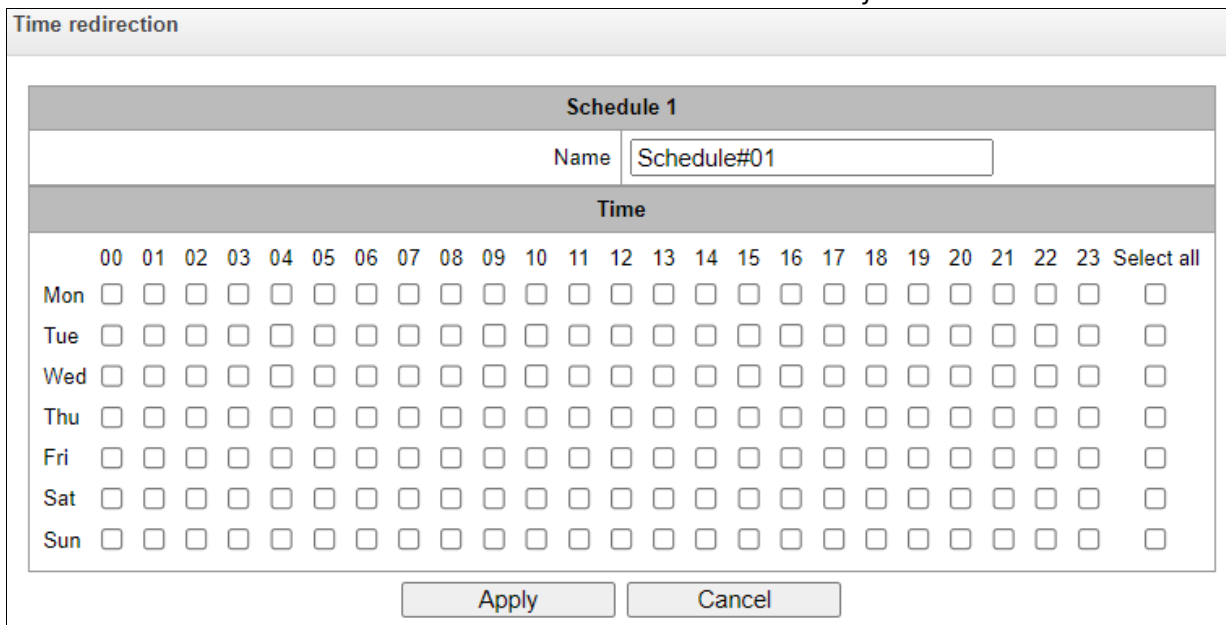
Internal resources → Time redirection



No	Name
0	Schedule#00

Then in the schedules you can select the desired time intervals for forwarding.

Internal resources → Time redirection → Object



Time redirection

Schedule 1

Name:

Time

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Select all
Mon	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tue	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Thu	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fri	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sat	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sun	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

After creating and setting up a schedule, it must be linked to the subscriber through VAS services (see 4.1.6.1.2 VAS management).

4.1.7.12 Hunt groups

Hunt group¹ is a 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.

¹ The option is available for the devices with SMG-VAS license. Read more detailed information on licenses in the section 4.1.25 Licenses.




Internal resources → Hunt groups

Hunt groups						
Search call group <input checked="" type="radio"/> by name <input type="radio"/> by mask <input type="text"/> <input type="button" value="Search"/>						
No	Name	Masks for CdPN	Conference ID	Calling mode	Group members	Select
0	HuntGroup00			simultaneous call		<input type="checkbox"/>

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

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

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

-  — 'Add record'
-  — 'Edit record parameters'
-  — 'Remove record'

Internal resources → Hunt groups → Object

Hunt group 0	
Name	<input type="text" value="HuntGroup00"/>
Dial plan	<input type="text" value="[0] NumberPlan#0"/>
Masks for CdPN	<input type="text"/>
Recording and notification	<input type="checkbox"/>
Calling mode	<input type="text" value="simultaneous call"/>
Conference ID	<input type="text"/>
Participant ringing timeout, sec	<input type="text" value="5"/>
Group ringing timeout, sec	<input type="text" value="30"/>
Group members <input type="button" value="Add"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

- *Name* — call group name.
- *Dial plan* — select dial plan that the call group will belong to.
- *Masks for CdPN* — mask of the caller number that is used for the callee number comparison arrived to the dial plan designed for further call routing (for mask syntax, see 4.1.4.2 Description of Number Mask and Its Syntax).
- *Recording and notification (option is available only with SMG-REC license)* – in this mode group members will hear a notification dictated by the initiator group call. Notification recordings are managed in the Call Recording section → Group notification records.

Operation algorithm:

- The initiator of notification makes a call to a group number;
- SMG answers to a call in 10 seconds and issues a tone signal 1400 Hz for a second, the recording is started;
- Initiator records the message and hangs up;
- In 3 seconds, SMG starts ringing members of the group. When they answer, the SMG plays the recorded notification;
- If a member of the group listened less than 1/3 of the message, the notification is considered to be unsuccessful and there will be one more attempt of notifying in 5 seconds;
- When there is a sequential notification, the next notification attempt will be performed in 3 seconds;
- If the member of the group does not answer before timeout expires, the next attempt will be performed after 60 seconds pause. There will be 5 attempts of notification.
- When there is a sequential notification, the members of the group who was not notified are put at the end of the call queue, and the SMG will ring the next subscriber in a queue.
- *Calling mode* — call group member ringing method:
 - *simultaneous call* — simultaneous call for all call group members;
 - *sequential from first* — method that always dials the first number in the call group number list when a new call comes to this group; when S-timer expires, call addressed to the current group member will be cancelled and the call will be addressed to the next group member;
 - *sequential from next* — method that will enable ringing inside the group, beginning with the number that has ended the previous call to that call group. This method is necessary for load balancing between the group members; when S-timer expires, call addressed to the current group member will be cancelled and the call will be addressed to the next group member;
 - *sequential all from first* — method that always dials the first number in the call group number list when a new call comes to this group; when S-timer expires, call addressed to the current group member will not be cancelled and the call will be addressed to the next group member;
 - *sequential all from next* — method that will enable ringing inside the group, beginning with the number that has ended the previous call to that call group; this method is necessary for load balancing between the group members; when S-timer expires, call addressed to the current group member will not be cancelled and the call will be addressed to the next group member;
 - *serial search from first* — method that will discover the first available subscriber from the beginning of the list; only subscribers of this gateway can be members of this group;
 - *serial search (sequentially)* — a method in which the search for the first available subscriber, starting from the number on which the conversation ended during the previous call, the call to the first available one occurs before the subscriber answers or before hang-ups due to timeout.
- *Hang up mode* – the hang up method for call group members:
 - *by default* – after one of the call group members answers, everyone else A CANCEL message is sent to participants, resulting in a missed call notification appears;
 - *silent* – after one of the call group participants answers, all other participants a CANCEL message is sent with the Reason header: SIP;cause=200, as a result these subscribers' phones will not receive notification of a missed call.
- *Conference ID* — number that when dialed after the service prefix VAS Conference all members of this group will be added to a conference call;

- *Call back the person who Q/52ed the call* – when using this option, repeated calls will be made to group members who rejected the call without picking up the phone. If the called subscriber rejected the call three times, attempts to recall him will stop;
- *Call back a busy person* – when using this option, repeated calls will be made to group members who were busy at the time the group was called (before answering group call or group call timeout expires).










When selecting '*Recording and notification*' option, the operation mode can take the following values:

- *recording and simultaneous notification* – after recording the message, group members will be notified simultaneously;
- *recording and sequential notification* – after recording the message, group members will be notified one by one, starting from the first.
- *Participant ringing timeout, sec* – call timeout for a group member;
- *Group ringing timeout, sec* – general call timeout for the whole call group;
- *Maximum recording time, sec* – the setting is available when '*Recording and notification*' is activated. It sets the maximum duration of the message which can be recorded for the group;
- *Group members* – call group contents, up to 40 members on SMG-1016M and up to 160 members on SMG-2016 and SMG-3016. If the group is used for conference organization, the maximum group size reduces to 40 participants on SMG-1016M, SMG-2016 and SMG-3016. Such conferences can have a maximum of 40 participants (including the initiator) 1 on SMG-1016M and 4 on SMG-2016/3016.

When selecting the operating modes '*simultaneous call*', '*sequential from first*', '*sequential from next*', '*sequential al from first*', '*sequential all from next*', the queue functionality will be available.

The queue functionality is necessary for organizing a call center.

Internal resources → Hunt groups → Object

Queue settings	
Use queue	<input type="checkbox"/>
Queue size 	<input type="text" value="15"/>
Sound path	default 
Advertise	<input type="checkbox"/>
Playing ads every, sec	<input type="text" value="15"/>
Play queue position	<input checked="" type="checkbox"/>
Play queue waiting time	<input checked="" type="checkbox"/>
Position timeout, sec 	<input type="text" value="30"/>
First position timeout, sec 	<input type="text" value="2"/>
Persian numbers 	<input type="checkbox"/>
Answer tone 	<input type="checkbox"/>
Cache calls 	None 
Work day time 	09:00  - 18:00 

- *Queue size* – the maximum number of participants who are in the queue and waiting for an operator response; if the specified number is exceeded, new calls will be rejected;
- *Sound path* – when set to '*off*', the system audio files located in the device file system will be used for queues. If necessary, one can record audio files to an external drive and select the path to the drive with audio files. The files must have specific names given in the table below.



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

Table 24 — Audio files names

File name	Value	By default
queue_position.wav	"Your position in the queue"	Yes
answer_tone.wav	Sound/melody that will be played when the operator answers	No
callback.wav	The phrase played to the operator before calling the subscriber back	No
advertise	Directory with advertising files	no
not_more_2m.wav	"Waiting time no more than 2 minutes"	Yes
not_more_3m.wav	"Waiting time no more than 3 minutes"	Yes
not_more_4m.wav	"Waiting time no more than 4 minutes"	Yes
not_more_5m.wav	"Waiting time no more than 5 minutes"	Yes
more_than_5m.wav	"Waiting time more than 5 minutes"	Yes
1-20.wav, 30.wav	Number in the queue	Yes
callback_operator.wav	The phrase played to the operator before calling the subscriber back	No
callback_abonent.wav	The phrase played to the subscriber when callback option enabled	No

- *Advertise* – when checked, while waiting for the operator respond, the sound files from the advertise directory with a specified advertise timeout will be played to the caller;



Only the first 5 files from the advertise directory will be used. This option is only available when using an external drive to store audio files queues.

- *Playing ads every, sec* – period of time after which the advertisement will be played to the the subscriber;
- *Play queue position* – when using this option, the queue position will be played to the subscriber;
- *Position timeout, sec* – period of time after which the queue position will be played to the subscriber, the beginning of the period is the end time of the last position playing;
- *First position timeout, sec* – period of time after which the queue position will be played to the subscriber for the first time;
- *Persian numbers* – SMG-1016M, SMG-2016 and SMG-3016 support playback of compound Persian numerals. To reproduce numbers greater than 20, use three parts of a numeral, including a linking word;
- *Answer tone* – when checked, after the operator responds, the sound file answer_tone.wav will be played to the caller and the operator;
- *Cache calls* – option required to remember the last operator the caller spoke to. So that when calling back, the caller immediately gets the last operator he/she spoke to:
 - *None* – the cache is disabled;
 - *Strict* – if the operator is busy, the call will not go to other operators, but will wait for the required operator to become available;
 - *Non-strict* – if the required operator is busy, the call will be distributed between other operators in accordance with the specified operating mode.
- *Work day time* – a time period of the working day is specified to calculate statistics of the call group operation;

- **RingBack settings:**
 - *Music on hold* – using music on hold instead of the RBT signal when waiting for a operator’s response;
 - *Delay before music, sec* – the time during which the standard RBT will be played before enabling MoH;
 - *Type* – MOH type selection:
 - *Music on hold* – when selecting this type, the standard MoH of SMG will be played to the subscriber;
 - *Audio file* – when selecting this type, it becomes possible to assign to playing a pre-loaded sound file on the drive. Selecting a drive for downloading sound files is carried out in the section System parameters → RBT settings:
 - *File name* – selecting an audio file to play as RBT.
- **Setting reserve member:**
 - *Reserve number* – number to which the call will be made after triggering ‘group call timeout’;
 - *Reserve ringing timeout, sec* – timeout responsible for the duration of sending a call to a reserve number.
- **Group members** – a list of operators that are part of the call group.

4.1.7.13 Pickup groups




Pickup group¹ is a group of device subscribers. When a call comes to one of the pickup group subscribers, another group member can pick up this call by dialing an exit prefix for this call group.

Internal resources → Pickup groups

No	Name	Numbers list	Select
0	PickupGroup00	345771 Privileged 345773 Ordinary 345774 Ordinary 345775 Ordinary	<input type="checkbox"/>

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

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

-  — 'Add record'
-  — 'Edit record parameters'
-  — 'Remove record'

Group can contain device subscribers only.

Internal resources → Pickup groups → Object

Pickup groups

Pickup group 1

Name:

Number list

1	<input type="text"/>	Ordinary	
---	----------------------	----------	--

¹ The option is available for the devices with SMG-VAS license. Read more detailed information on licenses in the section 4.1.25 Licenses.

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

Pickup group member type:

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

4.1.7.14 Voice messages

The device features 15 standard voice message phrases that are used for provisioning information to subscribers. In this section, you may upload custom voice message files.

File should be in WAV format compressed using codec G.711a, 8bit, 8KHz, mono. File size should not exceed 2Mb.

Internal resources → Voice messages

No	Name	Description
System voice messages		
0	access_restrict.wav	This communication type is not available (access-category restriction)
1	access_temp.wav	Subscriber cannot be called temporarily
2	access_unpaid.wav	Denied for non-payment
3	conf_greeting.wav	Conference greeting
4	conf_switch.wav	The request to switch into conference
5	intercom_announce.wav	Intercom announce
6	music_on_hold.wav	Music on hold
7	number_changed.wav	Number 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 <input type="checkbox"/>		
File is not selected <input type="button" value="Browse"/>		Select description... <input type="button" value="Add"/>
<input type="button" value="Download"/>		

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

You can add your own file to the list of custom voice messages and select for it a description of the event during which this file will be played (use the “Browse” and “Add” buttons).

- *Enable* — enable voice message file playback.




4.1.7.15 SIP replies list to switch on reserve

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

Internal resources → SIP-replies list

No	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'

Internal resources → SIP-replies list → Object

SIP-replies list to switch on reserve

SIP-replies list 0

Name	SipAnswerList#00
1	503 
2	505 

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




4.1.7.16 Q.850 release causes list

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

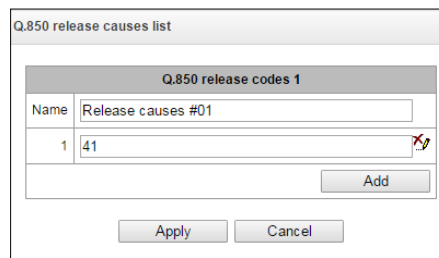
Internal resources → Q.850 release causes list


No	Name	Q.850 release codes
0	Release causes #00	41,27,25

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

-  — 'Add reply list'
-  — 'Edit reply list'
-  — 'Remove reply list'

Internal resources → Q.850 release causes list → Object

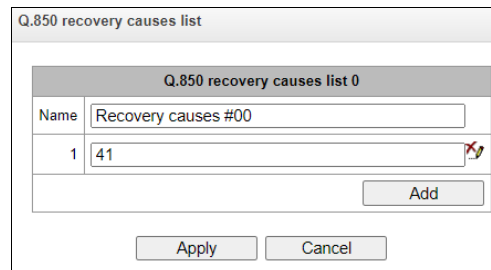


You should specify the list name and generate it by clicking 'Add' and  ('Remove') buttons.




4.1.7.17 Q.850 recovery causes list

In this section, you may configure the list of Q.850 recovery causes for SS7 and Q.931 protocols that will be used to restore the communication if the call is not rejected from the incoming side.

Internal resources → Q.850 recovery causes list → Object



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'

4.1.8 Voice notification system



The functionality is activated with SMG-VNS and SMG-VAS licenses.

The voice notification system (hereinafter referred to as VNS) is designed to implement simultaneous or sequential calling and notification of several subscribers according to pre-created notification task and prepared list of subscriber numbers.



For the VNS to work, you need to connect a drive to the SMG and select it in the 'Call recording' section → 'Call recording settings'. The drive stores voice message files for alerts, alert record files and VNS reports

Capabilities:

1. Ability to create 40 number lists, each of which can contain up to 200 subscriber numbers.
2. Ability to use one phone number simultaneously in several lists.
3. Ability to create 200 notification tasks.
4. Ensuring the simultaneous execution of up to 10 tasks for notifying subscribers groups SMG-2016/3016 and up to 8 tasks for SMG-1016M. Possibilities by total quantity of notified subscribers depend on the number of free channels on the SM-VP submodule and are determined by the following formula:

Number of channels on SM-VP submodules = $(M/S) + S*2$, where:

M – quantity of subscribers in the notification, i.e. quantity of numbers in number lists attached to the notification task;

S – number of simultaneously notified subscribers (the '*Number of notified participants*' parameter in the notification task).

For example, you need to run two notification tasks. In the first task, '*Number of notified participants*' = 20, and there are 200 subscribers in the lists of numbers. In the second task

'*Number of notified participants*' = 10, and there are 40 subscribers in the list of numbers. Then the required number of channels is calculated as follows:

For the first task: $(200/20) + 20*2 = 50$.

For the second task: $(40/10) + 10*2 = 24$.

In total, 74 SM-VP channels are required to simultaneously perform tasks.

Algorithm for working with VNS:

1. Preparing a task for voice notification.
2. Performing a voice notification task.
3. Generating a report on the completed voice notification task.

Description of each stage of the working algorithm for VNS:

1. Preparing a task for voice notification.
 - 1.1. Compiling a list of numbers of notified subscribers.
 - 1.2. Record a voice message.
 - 1.3. Creating a notification task, indicating a list of numbers and a recorded voice messages.
2. Performing a voice notification task:
 - 2.1. The operator issues a command to start a previously prepared task.
 - 2.2. The VNS receives the command and starts the notification task.
 - 2.3. In case of unsuccessful launch of the notification task, the VNS generates a short report with indicating an error.
 - 2.4. Upon successful launch of the notification task, the VNS makes a call and notifies numbers according to the list.
 - 2.5. If the subscriber is busy or unavailable, the call is not answered or there is no listening confirmation, the VNS makes several attempts to notify this subscriber.
 - 2.6. Restarting the same task is possible only after completing the existing one calling process.
3. Generating a report on the results of a completed task.
 - 3.1. Upon completion of the notification, the VNS generates a report, accessible through the web interface, in which indicates:
 - date and time of task launch;
 - date and time of task completion;
 - conditional number of the voice message;
 - a list of notified numbers marked '*notified*'/'*not notified*'.

Detailed description of the actual launch and execution of the voice notification task

1. Start the notification task.
 - 1.1. The operator dials a special number *XX# from the telephone set to access the VNS.
 - 1.2. The VNS receives the call and gives an acoustic signal “Station Answer” (continuous acoustic signal 440 Hz), waiting for additional dialing of the conditional task number NN via DTMF signals.
 - 1.3. Possible alternative option: the operator dials from the telephone set special number *XX*NN# indicating the conditional task number NN.
 - 1.4. The VNS, having received a call and a conditional notification task number, submits:
 - acoustic “confirmation” signal in case of successful launch of the task on notification (dual-frequency signal with frequencies 330 and 440 Hz, duration 100 ms, repeated three times at 100 ms intervals) and then ends the call;
 - acoustic “error” signal in case of error or inability to start the task (three-tone signal with frequencies 950/1400/1800 Hz, the duration of each is 330 ms at 330 ms intervals) and then ends the call.
 - 1.5. The VNS generates a preliminary report on the attempt to launch the task, indicating the date attempt time and task status: started/launch error. In case of startup error indicates the reason in the report.

2. Processing the successful launch of the notification task.
 - 2.1. Upon successful launch of the notification task, the VNS begins calling by telephone numbers specified in the list of notified subscribers.
 - 2.2. After the called subscriber picks up the handset, the VNS plays back the specified task voice message.
 - 2.3. After playing back at least 1/3 of the length of the recorded message, the VNS expects from the subscriber DTMF code confirming the fact of listening (for example, pressing button 1 on phone).
 - 2.4. After receiving the confirmation code, the VNS notes in its database the fact of successful notifying this employee when performing a task.
 - 2.5. If there is no DTMF confirmation code and less than 1/3 of the duration of the message, the VNS believes that the employee did not receive the message and will make further attempts.
 - 2.6. If after 5 notification attempts the VNS still does not receive a DTMF code from the subscriber confirmation, she notes in the database the fact that the notification of this employee failed and stops its notification until the end of this task.
 - 2.7. If there is no answer to the call/the subscriber is unavailable, the VNS repeats attempts dial in accordance with the dialing cycle settings, the following algorithm works:
 - 2.7.1. N dialing attempts are made with a ‘Timeout’ interval of seconds between them.
 - 2.7.2. In case of N failed dialing attempts in a row, the pause timer ‘Between repeats’ sec starts.
 - 2.7.3. Steps 2.7.1-2.7.2 are repeated a specified number of times.

3. Restart the notification task.
 - 3.1. A repeated launch is possible only after the previous launch of this task has completed.
 - 3.2. When you try to restart an unfinished calling task, the VNS will generate an error launch with a corresponding entry in the database.
 - 3.3. A successful repeated launch of an alert task does not take into account the previous result of the task completion and all subscribers from the list will be notified.

The VNS allows one to simultaneously perform up to 20 tasks to notify groups of subscribers with a common total number of notified subscribers up to 500.

Description of the notification report:

Upon completion of the notification task, the VNS generates a report, accessible via the web interface, with the following information:

- date and time of task launch;
- success of task launch;
- date and time of task completion;
- conditional task number;
- task name;
- name of the voice message;
- voice message file name;
- number (and percentage of the total number) of notified participants;
- a list of notified numbers marked “notified”/“not notified”.

4.1.8.1 Voice messages

Voice notification system → Voice messages

Voice messages		
No	Description	File name
0	VNS-VoiceMessage#00	

Voice notification system → Voice messages → Object

Voice messages

Voice message 1

Description:

File name:

Voice notification system → Voice messages → Object → Browse

Browse file

No files

In this section of the menu, a voice message is created (linked) for further use. Where:

- *Path to disk* – indicate the location of the audio files (the disk is selected in the section 'Call recording' – 'Call recording settings');
- *Description* – description of the voice message;
- *File name* – the name of the selected audio file.

In the 'Upload' section it is possible to upload your own audio file of a certain format ("Windows-WAV" file format, audio encoding: PCMA, 64 Kbit, 8 kHz, mono).

You can record a voice message from your telephone, to do this you need to dial *#82# code, dictate a message and hang up. After this, a voice message will be automatically created with this entry. You can also


immediately add a voice message to the already recorded created task, to do this you need to dial *#82*TASK_NUMBER#, dictate the message and hang up, after which the newly recorded message will be attached to the selected task, when the task is launched the next time, it will be played back to subscribers from the list of numbers.

If a task with the specified number does not exist, the message will be added to the general list of voice messages and will not be linked to any task.

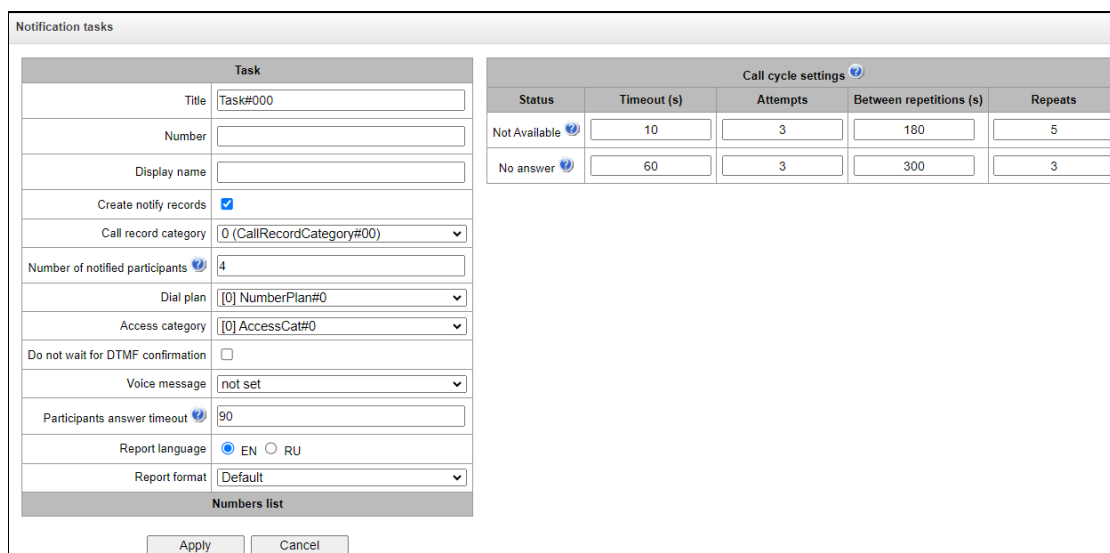
Uploaded audio files and recorded voice messages are saved to the drive in the directory vns_files/audio.

4.1.8.2 Notification tasks

Voice notification system → Notification tasks



Voice notification system → Notification tasks → Object



Status	Timeout (s)	Attempts	Between repetitions (s)	Repeats
Not Available	10	3	180	5
No answer	60	3	300	3

In this menu section, the notification tasks are created with the following parameters:

- **Title** – task name;
- **Number** – the number from which the notification will occur;
- **Display name** – display name when calling subscribers through the public address system;
- **Create notify records** – when this option is activated, records of all notified subscribers will be created. The records are managed in the 'Voice notification system' → 'Notify records';
- **Call record category** (the option is available when the 'Create notify records' is checked) – category that will be assigned to notify records. This option is used to determine user access rights to recorded notifications. A detailed description is given in 4.1.12.4 Call record settings);
- **Number of notified participants** – the number of simultaneously notified participants. Range of acceptable values: for SMG1016M – [4;8], for SMG2016/3016 – [4;40];

- *Dial plan* – dial plan in which the search for the notification system participants specified in the list of numbers will be carried out;
- *Access category* – access category of the notification system (taken into account in the delimitation calls by category);
- *Do not wait for DTMF confirmation* – if this option is activated, the notification system will not wait for confirmation via DTMF from the subscriber (listening to more than 3 seconds);
- *Voice message*;
- *Participants answer timeout* – timeout for a response from the notified subscriber. Range of acceptable values, sec [5; 120]; If the participant being notified does not answer the call within the specified time, then the call is considered unanswered, and then the VNS makes attempts to dial this participant in accordance with the call cycle settings;
- *Report language* – language that will be used when creating the VNS report;
- *Report format* – setting up the report type:
 - *Default* – in the report, the subscribers will be located in the same way as in the lists of numbers,
 - which are added to the notification task;
 - *Unannounced callers at the beginning* – in the report, the unnotified subscribers will be located at the beginning of the list, and notified ones at the end;
 - *Unannounced callers at the end* – in the report, the unnotified subscribers will be located at the end of the list, and notified ones at the beginning;
 - *Only unannounced subscribers* – only unnotified subscribers will be included in the report.
- *Numbers list* – adding lists of numbers to call.



If, in addition to the SMG-VNS license, the SMG-REC license is installed on the SMG, and in the '*Call recording settings*' section the recording masks (for example X.) are used, then when notifying participants numbers falling under this mask, a notify record will be created, even if this option is not active in the task.

Call cycle settings

If the call to the number is unsuccessful, the VNS repeats attempts to call using the following algorithm:

1. N dialing attempts are made (configured in the section '*Attempts*' column) with the '*Timeout*' interval seconds between them.
2. In case of N failed dialing attempts in a row, the pause timer '*Between repetitions*' starts, sec.
3. Steps 1–2 are repeated for a specified number of repetitions.

Example 'Unavailable':

Timeout (s) – 10

Attempts – 3

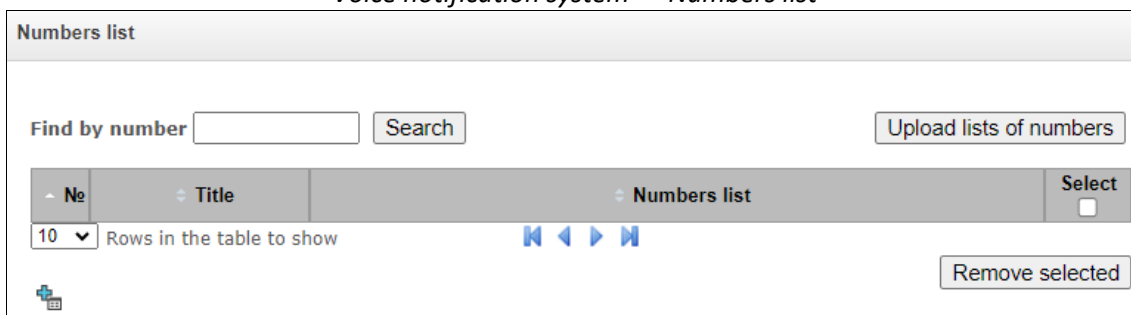
Between repetitions (s) – 180

Repetitions – 5

1. There are 3 dialing attempts with an interval of 10 seconds.
2. In case of 3 unsuccessful calls in a row, there is a pause of 180 seconds.
3. Steps 1–2 are repeated up to 5 times.

4.1.8.3 Numbers list

Voice notification system → Numbers list

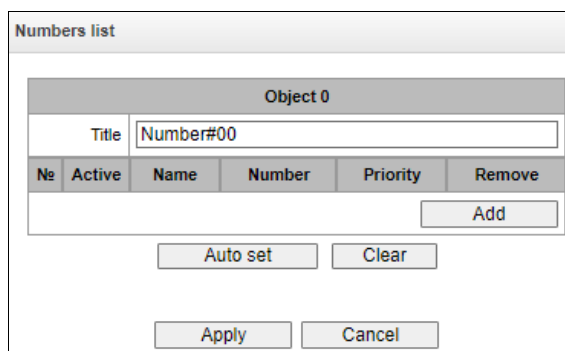


In this menu section, lists are created and loaded, which contains numbers to call through the voice notification system. Up to 40 numbers lists can be created. Each list can contain up to 200 call numbers.



It is prohibited to duplicate a number in one numbers list.
It is allowed to use identical numbers in different numbers lists.

Voice notification system → Numbers list → Object



- *Title* – name of the numbers list;
- *Active* – when this option is activated, the VNS will make a call to the specified number. This option allows you to temporarily disable notification of some participants without deleting numbers from the list. For example, if the subscriber is on vacation, business trip, etc.;
- *Name* – subscriber name that will be used when generating the report;
- *Number* – telephone number of the call participant;
- *Priority* – the order in which the participant is notified when performing a VNS task. This parameter allows one to set priority for notification participants when forming a queue of notifications. Values: from 1 to 5, where 1 is the highest priority (notification participants with this priority will be notified first), 5 is the lowest priority (notification participants with this priority will be notified last).



If the participant with priority 1 is not notified on the first attempt, then this participant is moved to the end of the notification queue.

Upload list of numbers – this option allows uploading numbers lists on the SMG from the prepared .csv file.

File name – this is the name (description) of the numbers list.

File format:

<NAME>;<NUMBER>;<Priority>

<NAME> – participant name. This parameter may be missing.

<NUMBER> – participant number.

<PRIORITY> – priority. This parameter may be missing, and in this case the participant priority will be set to 5.

Example:

Upload the file number_list1.csv filled with the following data:

```
Name1;500;1
Name2;501;2
Name3;502;3
;503;4
;504
```

As a result, the numbers list number_list1 will be created:

Voice notification system → Numbers list → Object

Numbers list

Object 0

Title:

№	Active	Name	Number	Priority	Remove
1	<input checked="" type="checkbox"/>	<input type="text" value="Name1"/>	<input type="text" value="500"/>	1 ▾	
2	<input checked="" type="checkbox"/>	<input type="text" value="Name 2"/>	<input type="text" value="501"/>	2 ▾	
3	<input checked="" type="checkbox"/>	<input type="text" value="Name2"/>	<input type="text" value="502"/>	3 ▾	
4	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text" value="503"/>	4 ▾	
5	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text" value="504"/>	5 ▾	

It is allowed to upload multiple files at the same time. The number of simultaneously uploaded files cannot exceed 40, and if before uploading files, numbers lists have already been created (or uploaded earlier), then the number of simultaneously uploaded files is reduced by the number of already created lists. When uploading a file with content different in format from that described above, a warning will be displayed – ‘Something went wrong during the last operation’. When loading a file containing the duplicate numbers the following warning will be displayed – ‘Failed upload some files: duplicate numbers’.

- If the name of the uploaded file matches the name of an existing list, the following options will be offered:
- *add* – the list will be supplemented with new numbers, the numbers that are already present in list, remain;
 - *overwrite* – the list will be replaced with a new one;
 - *cancel* – the file will not be uploaded; the existing list will remain unchanged.

Find by number – searches for a number across all existing lists of numbers.

Voice notification system → Numbers list

Numbers list

Find by number

Search results:

No	Numbers list	Active	Name	Number	Priority	Select
1	Number#3	+		100	5	<input type="checkbox"/>

No	Title	Numbers list	Select
0	Number#00		<input type="checkbox"/>
1	Number#3	Number1: 345771 : 100	<input checked="" type="checkbox"/>

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

Find by number also allows one to edit and delete the found number in any of the numbers lists. To do this, enter the number in the 'Find by number' field and click the 'Search' button. Then in search results, select an entry from those lists of numbers in which it is necessary to change some parameters of this number and click the 'Edit selected' button. In the appeared table select the fields you need to change, edit them and click the 'Apply' button.

To delete the number from the list, click the 'Remove selected' button. After that, the number will be deleted from the selected lists.

4.1.8.4 Reports

Voice notification system → Reports

Reports

Task name	Task number	Report name	Start of execution	Completion of execution	Size	Select all
-----------	-------------	-------------	--------------------	-------------------------	------	------------

This menu section stores all the reports created while the voice notification system was running. Reports are generated in a .csv file with the ability to upload to a local car. Before uploading, one can select the encoding of the generated report: UTF-8 or WINDOWS-1251. Reports are saved to the drive in the vns_files/reports directory.



Available only for SMG-2016 and SMG-3016, encoding selection is not available for SMG-1016M.

- *Task name* – name of the Task notification task;
- *Task number* – number of the notification task;
- *File name* – name of the report file;
- *Start of execution* – start time of the calling task;
- *Completion of execution* – time of completion of the calling task;
- *Size* – report size in KB.

The report file contains information about the result of the notification task.

Sample report file:

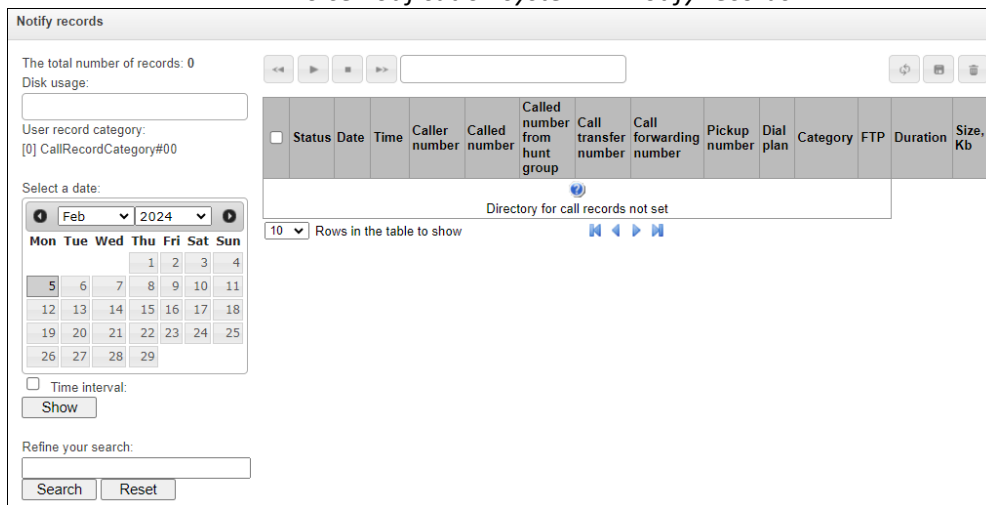
task	0	Notify task number
name	Task#000	Notify task name
message	VNS-VoiceMessage#01	Voice message name
file	priv.wav	Voice message file name
started	2022.09.30 14:38:22	Notify task start time
finished	2022.09.30 14:38:47	Notify task end time
status	Finished	Notify task execution status
total notified 1 (50.00%)		Number (and percentage of total) notified participants
number name last try status		List of participants (number, name, last try, notification status)
701 1 14:38:26 Not notified.		
User not answered		
555 2 14:38:26 OK		

The order in which participants are displayed in the report is configured in the notification task (“Report format” field).

4.1.8.5 Notify records

This menu section is intended for managing notify records files. Recorded notifications are saved into the vns_files/notify_records directory on the drive.

Voice notification system → Notify records



- *The total number of records* – total number of notify records files;
- *Disk Usage*— used storage space of the drive selected for notify records;
- *Select a date* – date to display files with notify records;
- *Time interval* – time interval for displaying files of notify records;
- *Refine your search* – search for files with notify records. The search is carried out for any matches of the entered value with the name of the notify record file.


For a detailed description of the management, see 4.1.11.3 Call Recordings.

4.1.9 LDAP

4.1.9.1 LDAP-storage list

The operation of the local LDAP server is configured in this menu.

LDAP → LDAP-storage list

LDAP-storage list					
ID	State	Name LDAP server	Port	LDAP protocol	
1	Off	LdapServer#00	389	ldap	

LDAP → LDAP-storage list → Edit

Edit LDAP server settings ×

Enable LDAP server

Name

Port 389

LDAP protocol ldap

Base dc=smg,dc=com

User name cn=user,dc=smg,dc=com

Password userpassword

The LDAP storage is formed based on the subscriber capacity of the station (FXS, SIP-station subscribers).

- Displayname = display name. If this field is empty in the settings, then it is substituted
- value "no_name";
- Uid = title;
- Cn = subscriber ID;
- Sn = display name;
- telephoneNumber = subscriber's telephone number.

To connect to the local LDAP server, use the following parameters:

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

4.1.10 Voice mail

4.1.10.1 Voice mail settings

Voice mail → Voice mail settings

Voice mail settings	
Local disk drive for storing mail	off
Directory name for storing mail	voice_mail
Maximum number of message	0
Unheard message storage time, days	0
Listened message storage time, days	0
Minimum message length, sec	3
Maximum message length, sec	60
Apply	

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

4.1.10.2 Voice messages (only for SMG-2016)

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

Voice mail → Voice mail settings

Voice messages

The total number of records: 0





Disk usage:

Select a date:

Enter subscriber number:

Status	Operator	Subscriber	Date	Time	Caller number	Called number	Duration	Size, Kb
Directory for voice mail not set								
<div style="display: flex; justify-content: space-between; align-items: center;"> 10 ▾ Rows in the table to show ⏪ ⏩ </div>								

- **Status** – indicates the message status:
 - **Operator** – web-interface user
 - – message is unheard by the web-interface user;
 - – message is listened by the web-interface user. When hovering over indicator in the Status → Operator column the name of the last user who listened to this message is displayed.
 - **Subscriber** – the subscriber to whom a voice message was left
 - – message is unheard by the subscriber;
 - – message is listened by the subscriber.
- **Date** – date of receiving a voice message;
- **Time** – time of receiving a voice message;
- **Caller number** – the subscriber who made the call to voicemail;
- **Called number** – subscriber number for which the ‘Voice mail’ service is enabled;
- **Duration** – voice message duration;
- **Size, Kb** – voice message recording file size.

-  **Change message status** – changes status from ‘Listen’ to ‘Unheard’ and vice versa;
-  **Refresh table** – updates the table with voice messages;
-  **Download selected** – downloads selected voice messages;
-  **Remove selected** – deletes the selected voice messages.

4.1.11 IVR

IVR (*Interactive Voice Response*) is a system of smart call routing based on the information entered by the client from the phone keypad using DTMF, current time and day of the week, caller and callee number, that enables voice notification of subscribers using voice files uploaded to the device. This function is necessary for call centers, taxi services, technical support, etc.

In this section, you may configure scenario and IVR audio lists and manage recorded conversation files.

4.1.11.1 Scenarios list


In this section, you may create IVR¹ service operation scenarios.

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

 — 'Add record'

 — 'Edit record parameters'




 — 'Remove record'

 — 'Download a scenario' — download selected scenarios from the scenarios list to a user PC.

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

IVR → Scenarios list


Scenarios list		
No	Name	Filename
0	IVRScenario_00	IVRScenario-1

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

The '*System settings*' table contains the '*Local disk drive for IVR scenarios*' setting which defines storage for scenarios.

IVR → System settings

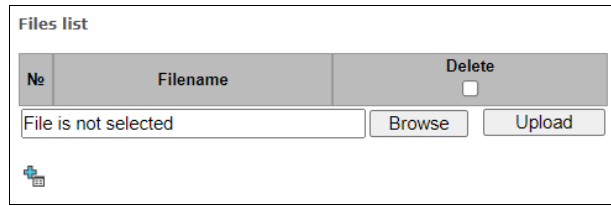
System settings	
Local disk drive for IVR scenarios	default 
<input type="button" value="Save"/>	

The '*Files list*' table contains created IVR scenario files.

¹ The option is available for the devices with SMG-IVR license. Read more detailed information on licenses in the section 4.1.25 Licenses.

Click 'Browse' in a dialog window to select a file and click 'Upload' to add pre-saved IVR file.

IVR → Files list



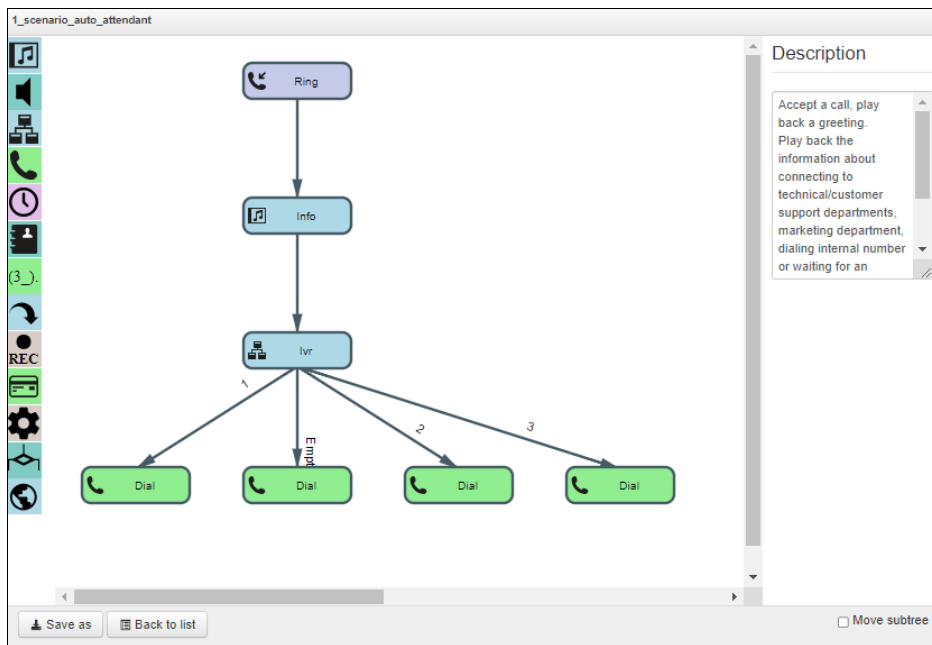
The 'Typical scenarios list' table contains all IVR common scenario files available for editing.

IVR → Typical scenarios list

Typical scenarios list	
No	Filename
0	1_scenario_auto_attendant
1	2_scenario_call_operator
2	3_call_technical_support_department
3	4_call_department
4	4_call_department_2
5	4_call_department_3
6	5_auto_attendant
7	5_auto_attendant_2
8	5_auto_attendant_3
9	5_auto_attendant_4
10	5_auto_attendant_5
11	5_auto_attendant_6

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.

IVR → Scenarios list → Typical scenarios list → Object



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

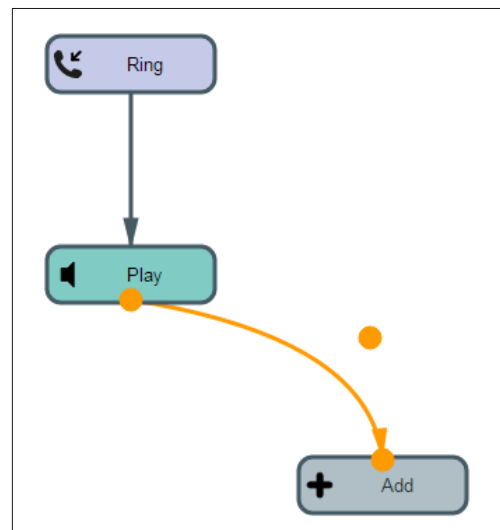
To add a block, select an empty block 'Add' and select the required action from the collection of common blocks by left-clicking it. In the field on the right, configure parameters for created block. Logical connections for a newly created element will be added automatically. Logical connection for 'Goto' 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.

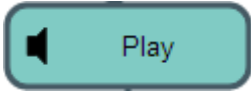

Also, you may left-click the logical connection between blocks, to change its type. Selected line will turn orange and three edit points will appear: for configuration of block exit location, block entry location and line curvature.





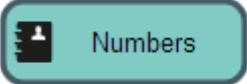

For IVR block description, see the table below.

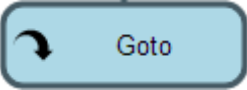
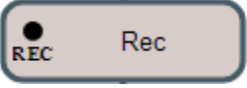
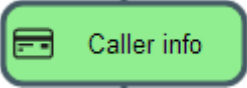
Table 25 — IVR block description

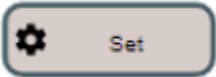

Designation	Name	Description
	Add	Empty unit designed for block addition.
	Ring	<p>Block that enables ringback tone playback for the subscriber; this block is always in the first position in the scenario list. When call arrives to RING block, call state remains unaffected.</p> <p>Parameters</p> <p><i>Ringback playback duration, seconds</i> — select duration of the ringback tone playback or disable it.</p> <p>Connections</p> <p><i>Entry</i> — beginning of the call to IVR.</p> <p><i>Exit</i> — a single exit, incoming call parameter information is available on the block exit (number A, number B).</p> <p>Features</p> <p>Block does not affect the call state.</p>
	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


		<p>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.</p> <p>Parameters</p> <p><i>Messages for playback until the subscriber answers</i> — select a single or multiple voice messages for playback to the caller. For voice message management, see 4.1.7.14 Voice messages. To specify the drive for file storage, see 4.1.1 System settings.</p> <p><i>Looped playback</i> — select the quantity of message playback loops; messages are played in order beginning from the first one.</p> <p>Connections</p> <p><i>Entry</i> — incoming call in the pre-answer state.</p> <p><i>Exit</i> — finish the playback of selected files.</p> <p>Features</p> <p>Info block may be preceded only by blocks that do not affect the call state (Ring, Info, Digitmap, Time, Goto).</p>
	Play	<p>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.</p> <p>Parameters</p> <p><i>Messages for playback until the subscriber answers</i> — select a single or multiple voice messages for playback to the caller. For voice message management, see see 4.1.7.14 Voice messages. To specify the drive for file storage, see 4.1.1 System settings.</p> <p><i>Looped playback</i> — select the quantity of message playback loops. Messages are played in order beginning from the first one.</p> <p>Connections</p> <p><i>Entry</i> — incoming call in the pre-answer or conversation state.</p> <p><i>Exit</i> — finish the playback of selected files.</p>
	IVR	<p>A block that is required for implementation of the interactive voice response function. This block features logical selection of the call path by pressing specific digit combinations, subscriber number extension dialing using internal dial plan and playback of audio files, system sounds (ringback tone, ringing tone, busy tone) and DTMF digits for subscriber notification.</p> <p>Parameters</p> <p><i>Type</i> — type of audio file for playback.</p>

		<p><i>File</i> — audio file uploaded to the device. For IVR audio list configuration, see 4.1.11.2 Tones list.</p> <p><i>Tone</i> — select system sound for playback (DTMF digit, dialtone, busy, ringback).</p> <p><i>Select subscriber</i> — 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.</p> <p><i>Subscriber selection timeout, seconds</i> — additional number dialing timer; when this timer expires, IVR outbound branch will be selected.</p> <p><i>Enable extension dialing</i> — when checked, extension dialing will be enabled followed by the device dial plan routing, e.g. internal subscriber number can be dialed.</p> <p><i>Access category</i> — select access category. Access category allows you to define call barring for the number dialed by the subscriber in IVR block.</p> <p><i>Quantity of digits for extension dialing</i> — maximum quantity of digits that can be dialed in the extension dialing.</p> <p><i>Interdigit delay, seconds</i> — extension number interdigit delay value.</p> <p>Connections</p> <p><i>Entry</i> — incoming call in the pre-answer state or active call phase.</p> <p><i>Exit</i> — quantity of exits is configurable; extension dialing of a subscriber number may also be an exit.</p> <p>Features</p> <p>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.</p>
	Dial	<p>Block required for the specified number dialing, the number routing will be performed according to the device dial plan.</p> <p>Parameters</p> <p><i>Number</i> — specified number.</p> <p>Dial plan:</p> <p><i>Transit</i> — does not change a dial plan.</p> <p><i>Access category</i> — select access category, which will be used after passing the Dial block:</p> <p><i>Transit</i> — does not change a dial plan.</p> <p>Connections</p> <p><i>Entry</i> — incoming call in the pre-answer state or active call phase.</p>

		<p><i>Exit</i> — exit from the block is provided in case of unsuccessful dialing.</p> <p>Reasons for disconnection under which the transition along the Fail branch will be carried out the following:</p> <ul style="list-style-type: none"> • 17 – User busy • 19 – no answer from the user • 21 – call rejected • 27 – destination out of order • 38 – network out of order • 41 – Temporary Failure <p>Features</p> <p>Finishes scenario branch.</p>
	Time	<p>Block required for the selection of call path logic according to the current time and day of the week.</p> <p>Parameters</p> <p><i>Time</i> — select time and day of the week template. Time is defined in 24h format.</p> <p>Connections</p> <p><i>Entry</i> — incoming call in the pre-answer state or active call phase.</p> <p><i>Exit</i> — block has 2 exits, the first one when time matches the defined template ('yes' exit), the second one when the match is not achieved ('no' exit).</p> <p>Features</p> <p>Block does not affect the call state.</p>
	Numbers	<p>Block required for the selection of call path logic according to the caller number.</p> <p>Parameters</p> <p><i>Number</i> — caller number template.</p> <p>Connections</p> <p><i>Entry</i> — incoming call in the pre-answer state or active call phase.</p> <p><i>Exit</i> — block has 2 exits, the first one when caller number matches the defined template ('yes' exit), the second one when the match is not achieved ('no' exit).</p> <p>Features</p> <p>Block does not affect the call state.</p>
	Digitmap	<p>Block required for the selection of call path logic according to the callee number. Callee number is verified at the digitmap block entry phase.</p>

		<p>Parameters</p> <p><i>Mask</i> — callee number mask.</p> <p>Connections</p> <p><i>Entry</i> — incoming call in the pre-answer state or active call phase.</p> <p><i>Exit</i> — block has 2 exits, the first one when callee number matches the defined template ('yes' exit), the second one when the match is not achieved ('no' exit).</p> <p>Features</p> <p>Block does not affect the call state.</p>
	Goto	<p>Block required for call transfer to another arbitrary scenario block.</p> <p>Parameters</p> <p><i>Select block on the flowgraph</i> — click this button to select the block on the flowgraph to perform the transfer.</p> <p><i>Maximum quantity of actuations</i> — select the quantity of passes for a call through this block to ensure the call looping protection.</p> <p>Connections</p> <p><i>Entry</i> — incoming call in the pre-answer state or active call phase.</p> <p><i>Exit</i> — a single exit to the block that the call is being transferred to.</p> <p>Features</p> <p>Block does not affect the call state.</p>
	REC	<p>Block required to begin the conversation recording; when the call logic passes through the block, subscriber conversation will be recorded into the file.</p> <p>Connections</p> <p><i>Entry</i> — incoming call in the active call phase.</p> <p><i>Exit</i> — block has a single exit.</p> <p>Features</p> <p>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 'IVR conversation recording folder name' parameter, 4.1.12.1 Call recording settings. For recording management, see Section 4.1.11.3 Call records.</p>
	Caller Info	<p>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.</p> <p>Parameters</p> <p><i>Number mask</i> — caller number template.</p> <p><i>Subscriber name</i> — new subscriber name.</p>

		<p>Connections</p> <p><i>Entry</i> — incoming call in the pre-answer state or active call phase.</p> <p><i>Exit</i> — block has a single exit.</p> <p>Features</p> <p>Block does not affect the call state.</p>
	Set	<p>The block allows to determine the variable for IVR script:</p> <p>Parameters</p> <p><i>Key</i> — the name of the variable by which you can refer to it in other blocks;</p> <p><i>Value</i> — variable value.</p>
	Condition	<p>The condition block is designed to test Boolean conditions composed of variables and strings. All operations are performed over strings. Up to 10 conditions can be set in a block. Each condition is assigned a corresponding exit branch (from 0 to 9) from a block to another block. In the Condition block, the transition is carried out along the branch of the first true condition (if there are several true conditions, the first one is selected). If none of the conditions in the Condition block turned out to be true, then the transition along the False branch will be performed.</p> <p>The following operators are available to form conditions:</p> <p>Logical operators:</p> <p>!, not - logical NO;</p> <p>&&, and - logical AND;</p> <p> , or - logical OR.</p> <p>Comparison operators:</p> <p>< - less;</p> <p><= - less or equal;</p> <p>= - equal;</p> <p>> - more;</p> <p>>= - more or equal;</p> <p><> - not equal.</p> <p>Logical operators: since the comparison is performed on strings, the comparison is performed character by character.</p> <p>Examples of comparing strings of digits of equal length:</p> <pre>"101" < "102" = true "101" =< "102" = true "101" > "102" = false "101" >= "102" = false</pre> <p>Examples of comparing strings of digits of unequal length:</p> <pre>"101" < "1102" = true "101" =< "1102" = true "101" > "1102" = false "101" >= "1102" = false</pre>

		<p>Examples of comparing strings of numbers and letters of equal length:</p> <pre>"A01" < "102" = false "A01" =< "102" = false "A01" > "102" = true "A01" >= "102" = true</pre> <p>"A01" < "102" = false, since the strings are compared character by character, namely the character code A in the ASCII table is greater than the character code 1.</p> <p>Entry operator in – operator for entering a variable into a list (eg., %%CGPN%% in (710, 711, 712)).</p> <p>Variables: A string enclosed in percent symbols (%). The variable name can contain characters: [A- Za-z 0-9].</p> <p>Constants: Any characters enclosed in single (') or double (") quotes. The slash character (/) is used for escaping. Or any sequence of non-whitespace characters that do not start with a percent sign does not contain single or double quote characters.</p> <p>Predefined variables: CGPN – calling number; CDPN – called number; YEAR, MONTH, DAY, HOUR, MINUTE, SECOND – date and time script execution (UTC+0 time is used); YEAR_LOCAL, MONTH_LOCAL, DAY_LOCAL, HOUR_LOCAL, MINUTE_LOCAL, SECOND_LOCAL – date and time of script execution (local time from the device is used).</p>
	<p>RPC</p>	<p>Block for interacting with an external HTTP server.</p> <p>HTTP request settings:</p> <ul style="list-style-type: none"> • <i>URL</i> – the full URL of the request to the http server. If necessary, you can use the variables of the current IVR scenario in the URL; <p>Example: http://infoUserServer.co/shirts?style=%CDPN%</p> <ul style="list-style-type: none"> • <i>Method</i> – HTTP request method (GET, POST, PUT, TRACE, OPTIONS, DELETE, HEAD); • <i>Request timeout</i> – time to attempt a request to the HTTP server in milliseconds; • <i>Content type</i> – the type of data contained in the request body; • <i>Body content</i> – request body (a string with the possible presence of macro variables); • <i>Headers</i> – HTTP request header; <ul style="list-style-type: none"> • <i>Key</i> – http header key; • <i>Value</i> – a string with a possible value of macro variables; • <i>Response type</i> – the type of data contained in the response body; • <i>json</i> – when this type is selected, if the response body receives data "key:value", then SMG writes this data as variables that can be used later;

		<p><input checked="" type="checkbox"/> If the key in the response body is written in small letters, for example var, then in order to later access this variable, it must be written in capital letters % VAR%.</p> <ul style="list-style-type: none"> • <i>regex</i> – when this type is selected, the ‘Regular expression’ window appears, in which you can write a regexp expression for parsing a response from an HTTP server with the ability to write the parsed data to IVR variables and use them later. <p>Example: Reply in the message body: Hello world The string in the field “Regular expression”: Hello (?<var1>.*) As a result, a variable will be created within the IVR script VAR1=world</p> <ul style="list-style-type: none"> • <i>Max bytes</i> – maximum response size; • <i>Expected encoding</i> – encodings supported in the response; • <i>Codes</i> – expected HTTP server response codes.
--	--	--

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.

4.1.11.2 Tones list

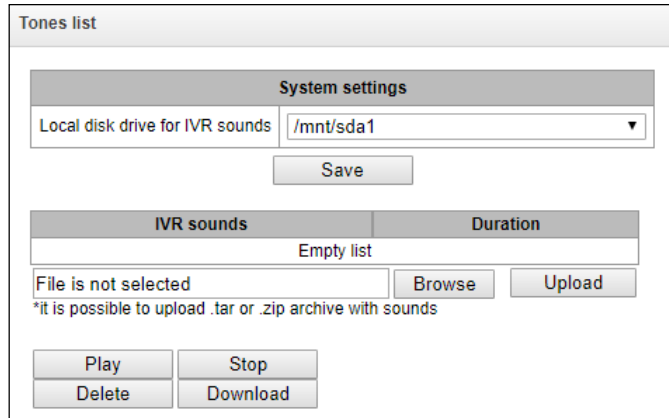
In this section, you may manage audio files required for IVR operation.



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

The 'System settings' table contains 'Local disk drive for IVR sounds' which defines storage for conversation records from IVR.

IVR → Tones list



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



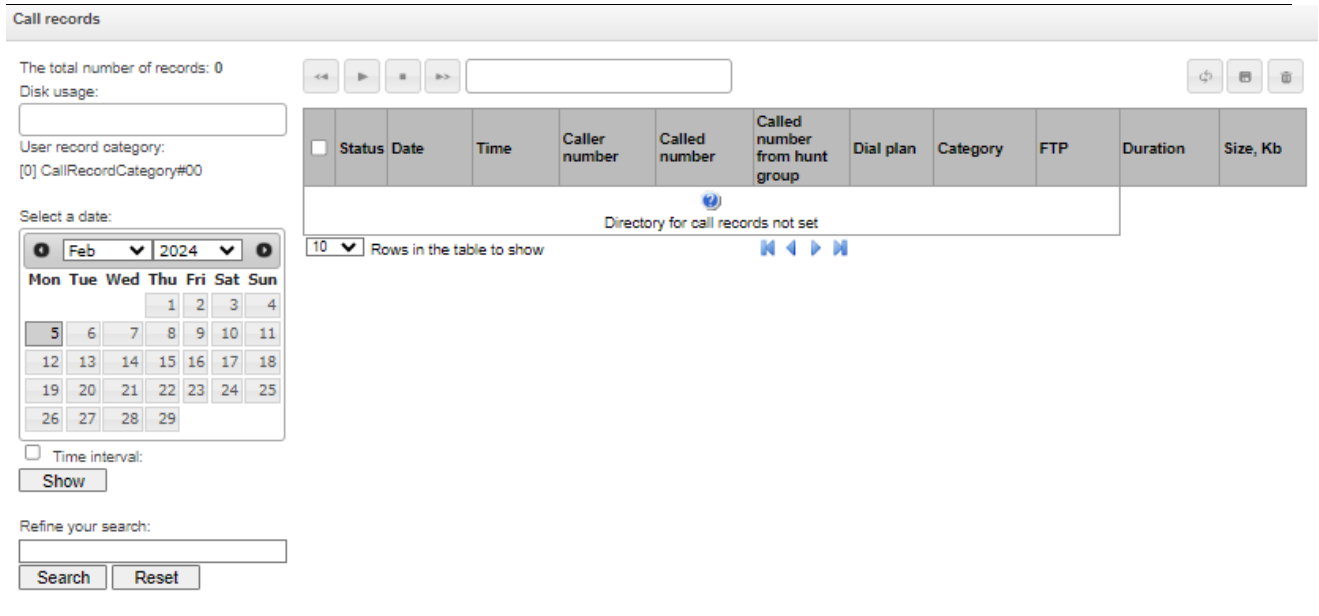
You may upload tar or zip archive file containing multiple audio files; audio files should be in the root directory of the archive.

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

4.1.11.3 Call records (IVR)

This section enables management of IVR conversation recording files. If there is REC block present in IVR scenario, all recorded conversations will be represented in a table.








IVR → Call records



- *The total number of records* — total quantity of conversation recording files in the selected directory for conversation recordings.
- *Disk usage* — display used space on disk selected for conversation recording.
- *Select a date* — select a date to display the conversation recording files.
- *Time interval* — select time interval to display the conversation recording files.
- *Refine your search* — search for conversation recording files; search function uses any matches of the entered value to conversation recording file name.

For record control buttons description, see Table below.

Table 26— Record control buttons

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

Call records table description

- *Status* – indicates the message status:
 - *Operator* – web-interface user
 - – message is listened by the web-interface user. When hovering over indicator in the Status → Operator column the name of the last user who listened to this message is displayed;
 - – message is unheard by the web-interface user.
- *Date/time* – date and time of the recording start;
- *Caller number/called number* – the number of the subscribers participating in the conversation;
- *Dial plan* – a dial plan in which the record is implemented;
- *Category* – conversation record category;
- *FTP* – shows whether the record was uploaded to FTP;
- *Duration* – conversation duration;
- *Size, KB* – the size of the record in kilobytes.

Conversation recording file format

1. A common call without call redirection or transfer:

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

where

YYYY-MM-DD — file creation date, YYYY — year, MM — month, DD — day.
 hh-mm_ss — file creation time, hh — hours, mm — minutes, ss — seconds.
 CgPN — caller name, if it is missing, value 'none' will be used.
 CdPN — callee number.

Example:

Subscriber 7111 calls Subscriber 7222, file name should be as follows:
 2014-05-20_12-05-35_7111_7222.wav

2. A call that uses call redirection service:

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

where

YYYY-MM-DD — file creation date, YYYY — year, MM — month, DD — day.
 hh-mm_ss — file creation time, hh — hours, mm — minutes, ss — seconds.
 CgPN — caller name, if it is missing, value 'none' will be used.
 RdNum — redirecting number — number with configured call redirection service.
 cf — marker indicating that call forwarding has taken place.
 CdPN — callee number — a number that the call is actually comes to.

Example:

Subscriber 7111 calls Subscriber 7222 that has configured a call redirection to 7333.
 2014-05-20_12-05-35_7111_7222cf7333.wav

3. A call that uses call transfer service:

Call transfer service engages 3 subscribers — call initiating subscriber (Subscriber A), call transferring subscriber (Subscriber B) and transferred call recipient subscriber (Subscriber C).

For call transfer, 3 conversation recording files will be created.

- *Subscriber A* — Subscriber B conversation
- *Subscriber B* — Subscriber C conversation
- *Subscriber A* — Subscriber C conversation after the call transfer

Example:

Subscriber 7111 calls Subscriber 7222 that transfers the call to Subscriber 7333.

The following files will be created:

2014-05-20_12-05-35_7111_7222.wav — Subscriber A — Subscriber B conversation.

2014-05-20_12-06-36_7222_7333.wav — Subscriber B — Subscriber C conversation after the Subscriber B has put the Subscriber A on hold.

2014-05-20_12-05-35_7111_7222ct7333.wav — Subscriber A — Subscriber C conversation after the call transfer by Subscriber B; ct in the file name is a call transfer marker.

4. Making a call from the 'Hunt group'

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

YYYY-MM-DD_HH-MM-SS_CgPN - CdPN - CALLEDHG_nPLAN_cCATEGORY.wav

Where:

YYYY-MM-DD – file creation date, YYYY – year, MM – month, DD – day;

hh-mm_ss – file creation time, hh – hours, mm – minutes, ss – seconds;

CgPN – caller number, if absent, set to none;

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

CALLEDHG – hunt group number;

nPLAN – dial plan;

cCATEGORY – call recording category.

5. Calling a subscriber through the 'Hunt group'

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

Where:

YYYY-MM-DD – file creation date, YYYY – year, MM – month, DD – day;

hh-mm_ss – file creation time, hh – hours, mm – minutes, ss – seconds;

CgPN – caller number, if absent, set to none;

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

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

numplan – dial plan;

category – call recording category.

4.1.12 Call recording

This menu is intended for configuring call records.



The menu is only available in software versions with SMG-REC and/or SMG-VNS licenses. Read more detailed information on licenses in the Licenses section.

The SMG can maintain a varying number of simultaneous records depending on the connection type. Please check the table below before setting:

Connection type	1 × SM-VP-M300 submodule	6 × SM-VP-M300 submodules
E1 – E1	27	162
E1 – SIP	22	132
SIP – SIP	20	120



Please note that the call recording feature is designed to record business call conversations.

Call records can be uploaded to an FTP server. In this case, the records are first saved to local drive and then they are sent to the FTP server according to a schedule.



It is not recommended to record to a USB drive if there are a large number of recorded conversations. The interface bandwidth is insufficient to simultaneously record the required number of files, which leads to an increase in I/O buffers in RAM and can disrupt the operation of the gateway.

4.1.12.1 Call recording settings

Call recording → Call recording settings

Call recording settings

Common record settings

Local disk drive for call records	off
Directory name for call records	call_records
Directory name for IVR call records	ivr_records
Number of files per directory	200
Keep files for: Days	30
Hours	0
Action when disk is full	Stop recording

FTP server settings

Store files on FTP	<input type="checkbox"/>
Upload mode	once per day
Hours	0
Minutes	0
Server address/hostname	
Server port	21
Path on server	
Login	
Password	*****
Remove files after upload	<input type="checkbox"/>

Apply

№	Mask	Type	Dial plan	Notification	Call record category
					<input type="checkbox"/>

Common record settings

- *Local disk drive for call records* – selects the available drive for saving conversation records;
- *Directory name for call records* – the name of directory for saving conversation records; if the folder name is not specified, conversation records will be saved to the root directory of the drive;
- *Directory name for IVR call records* – the name of directory name for saving conversation records when a call comes to the REC block in the IVR script;
- *Number of files per directory* – the maximum number of conversation record files in a single directory; if the maximum number of files is reached, a new directory will be created.

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

YYYY-MM-DD-NNNN,

where:

- YYYY – 4 characters – the current year;
- MM – 2 characters – the current month;
- DD – 2 characters – the current date;
- NNNN – 4 characters – number of a directory containing conversation records for the current date.

If the *Number of files per directory* value is reached, the device will create a new directory with the value #### increased by one.

Example of directories created on 2014-02-27:

2014-02-27-0000
2014-02-27-0001
2014-02-27-0002
2014-02-27-0003

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

FTP Server Settings

- *Store files on FTP* – when this option is checked, conversation records will automatically be uploaded to the FTP server, according to the selected upload mode;
- *Upload mode* – determines how often the records will be uploaded to FTP:
 - *once per day* – uploading once a day at a given time;
 - *once per hour* – uploading every hour;
 - *once per minute* – uploading every minute.
- *Hours* – available in the *once a day* uploading mode. Here you can specify the hour for uploading;

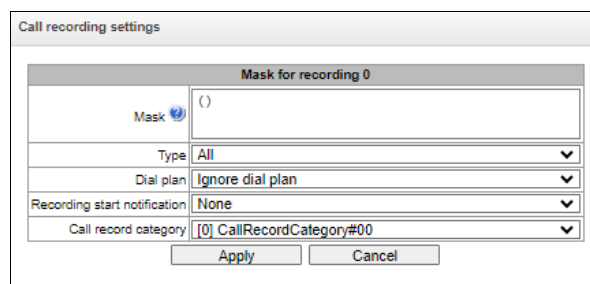
- *Minutes* – available in the *once a day* and *once an hour* uploading modes. Here you can specify the minutes for uploading;
- *Server address/hostname* – the IP address or domain name of the FTP server to which conversation records will be uploaded;
- *Server port* – the FTP server port;
- *Path on server* – the path for saving files on the FTP server;
- *Login* – login for authorization;
- *Password* – password for authorization;
- *Remove files after upload* – if this option is checked, record files will be deleted from the local SMG storage after uploading.



When using only the SMG-VNS license on the SMG, these settings will apply to VNS records. VNS records are saved to disk in the `vns_files/notify_records` directory. When using SMG-REC and SMG-VNS licenses on SMG, the settings are also applied to call recording, and to VNS notify records.

Filter Masks for Conversation Records (option is only available with an SMG-REC license):

Call recording → Call recording settings → Object



The device determines whether a conversation should be recorded for CgPN and CdPN numbers.

- *Mask* – the number filter mask. For mask syntax, see 4.1.4.2 Description of Number Mask and Its Syntax;
- *Type* – search for a mask match by CdPN or CgPN number:



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

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

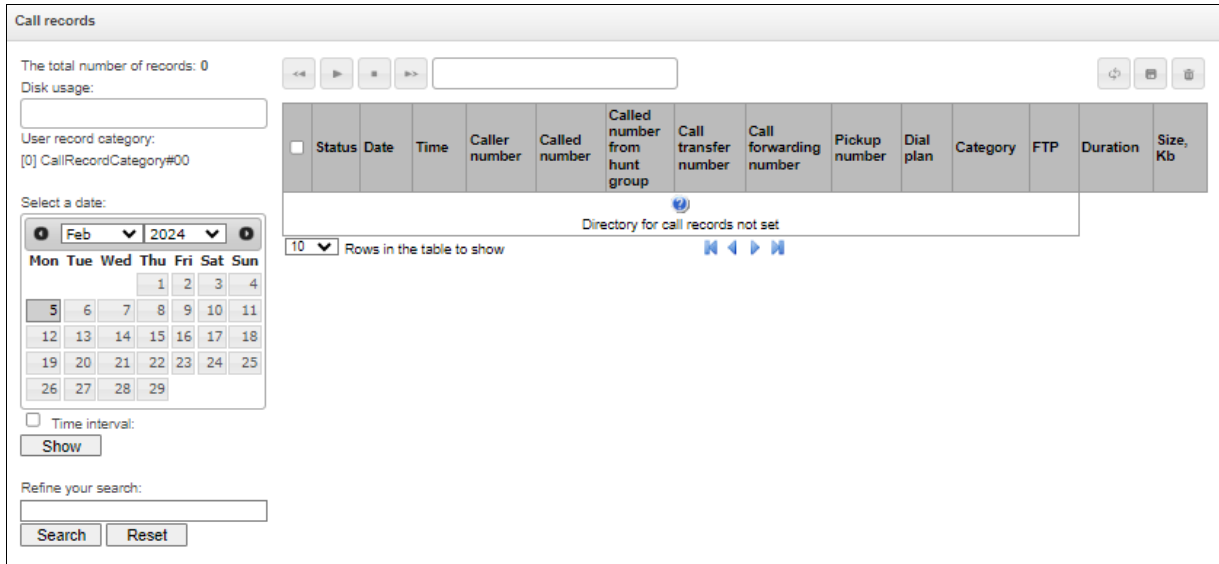
4.1.12.2 Call records



This section is not available when using only the SMG-VNS license.

In this section, conversation record files can be managed.

Call recroding → Call records



- *The total number of records* – total number of conversation record files in the selected directory;
- *Disk usage* – display the used space on the drive selected to store the conversation record files;
- *User record category* – display the conversation record category assigned to the current user of the web interface;
- *Select a date* – select the date to display conversation record files;
- *Time interval* – select the interval to display conversation record files;
- *Refine your search* – search for conversation record files; the search function uses any match of the entered value against the name of a conversation record file.

The record control buttons are described in the table below.

Table 27 – Record Control Buttons

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

Call records table description

- *Status* – indicates the message status:
 - – message is listened by the web-interface user. When hovering over indicator in the Status → Operator column the name of the last user who listened to this message is displayed;
 - – message is unheard by the web-interface user.
- *Date/time* – date and time of the recording start;
- *Caller number/called number* – the number of the subscribers participating in the conversation;
- *Dial plan* – a dial plan in which the record is implemented;
- *Category* – conversation record category;
- *FTP* – shows whether the record was uploaded to FTP;
- *Duration* – conversation duration;
- *Size, KB* – the size of the record in kilobytes.

Format of a conversation record file

1. A common call without call forwarding or transfer

YYYY-MM-DD_hh-mm-ss_CgPN-CdPN_nX_cY.wav

where:

YYYY-MM-DD – file creation date, YYYY – year, MM – month, DD – day;

hh-mm-ss – file creation time, hh – hours, mm – minutes, ss – seconds;

CgPN – the caller number, if absent, set to none;

CdPN – the called number;

nX – the number of the dial plan in which the record was made;

cX – the record category.

Example:

Subscriber 40010 calls to subscriber 40012, the file will look as follows:

2017-10-23_09-27-26_40010-40012_n0_c0.wav

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

YYYY-MM-DD_hh-mm-ss_CgPN-CdPN_Srv_SrvNum_nX_cY.wav

where:

YYYY-MM-DD – file creation date, YYYY – year, MM – month, DD – day;

hh-mm-ss – file creation time, hh – hours, mm – minutes, ss – seconds;

CgPN – the caller number, if absent, set to none;

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

Srv – a label indicating that an additional service was used. The label values:

- cf – the call was forwarded;
- ct – the call was transferred;
- cp – the call was picked up;

SrvNum – the number of the service that provided the additional service. Depending on the label value, Srv is the number, which has received a redirected or transferred call, or the number from which the call has been picked up;

nX – the number of the dial plan in which the record was made;

cX – the record category.

Example:

Subscriber 40010 calls to subscriber 40011 who redirects the call to subscriber 40012.
2017-10-23_09-28-04_40010-40011_cf_40012_n0_c0.wav

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

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

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

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

Example:

Subscriber 40012 calls to subscriber 40010, which transfers the call to subscriber 40000.

The following files are generated:

2017-10-23_10-15-19_40012-40010_n0_c0.wav – conversation of subscribers A and B;

2017-10-23_10-15-31_40010-40000_n0_c0.wav – conversation of B and C, after the subscriber B has put on hold the subscriber A;

2017-10-23_10-15-19_40012-40010_ct_40000_n0_c0.wav – conversation of subscribers A and C after the call was transferred by subscriber B, where *ct* in the file name is the label indicating that the call transfer was made.

4.1.12.3 Group notification records



This section is not available when using only the SMG-VNS license.

In this section, group notification records files can be managed.

Call recording → Group notification records

Group notification records

The total number of records: 0
 Disk usage:

Select a date:

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

Time interval:

Refine your search:

Date	Time	Caller number	Called number	Dial plan	Hunt group	Record
Directory for notify records not set						

10 Rows in the table to show

- *The total number of records* – total number of conversation record files in the selected directory;
- *Disk usage* – display the used space on the drive selected to store the conversation record files;
- *User record category* – display the conversation record category assigned to the current user of the web interface;
- *Select a date* – select the date to display conversation record files;
- *Time interval* – select the interval to display conversation record files;
- *Refine your search* – search for conversation record files; the search function uses any match of the entered value against the name of a conversation record file.

In the 'Date' column, each entry is a link to the notification log. The log shows the progress of the notification and its result. You can listen to the text of the notification by clicking the link in the 'Record' column, in the same column, you can download the record by clicking the icon next to the record.

4.1.12.4 Call record settings

Call recording → Call record categories

Call record categories		
No	Name	Access to categories
0	CallRecordCategory#00	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31
1	CallRecordCategory#01	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
2	CallRecordCategory#02	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
3	CallRecordCategory#03	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
4	CallRecordCategory#04	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
5	CallRecordCategory#05	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
6	CallRecordCategory#06	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
7	CallRecordCategory#07	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
8	CallRecordCategory#08	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
9	CallRecordCategory#09	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
10	CallRecordCategory#10	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
11	CallRecordCategory#11	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
12	CallRecordCategory#12	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
13	CallRecordCategory#13	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
14	CallRecordCategory#14	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
15	CallRecordCategory#15	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
16	CallRecordCategory#16	
17	CallRecordCategory#17	
18	CallRecordCategory#18	
19	CallRecordCategory#19	
20	CallRecordCategory#20	
21	CallRecordCategory#21	
22	CallRecordCategory#22	
23	CallRecordCategory#23	
24	CallRecordCategory#24	
25	CallRecordCategory#25	
26	CallRecordCategory#26	
27	CallRecordCategory#27	
28	CallRecordCategory#28	
29	CallRecordCategory#29	
30	CallRecordCategory#30	
31	CallRecordCategory#31	

Conversation record categories are used to define the user access rights for recorded conversations.

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

In total, up to 32 record categories can be configured. By default, 'Category 0' has a permanent access to all other categories and is used for the administrator account that provides access to all conversations. Other categories have configurable access. By default, the first 15 of them provide access to the first 16 categories.

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

Setup example: restrict access to conversation records

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

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

Call recording → Call record categories

Call record categories		
No	Name	Access to categories
0	Admin	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31
1	production	1
2	sales	2
3	CallRecordCategory#03	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
4	CallRecordCategory#04	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
5	CallRecordCategory#05	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
6	CallRecordCategory#06	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
7	CallRecordCategory#07	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
8	CallRecordCategory#08	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
9	CallRecordCategory#09	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
10	CallRecordCategory#10	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
11	CallRecordCategory#11	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
12	CallRecordCategory#12	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
13	CallRecordCategory#13	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
14	CallRecordCategory#14	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
15	CallRecordCategory#15	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
16	CallRecordCategory#16	
17	CallRecordCategory#17	
18	CallRecordCategory#18	
19	CallRecordCategory#19	
20	CallRecordCategory#20	
21	CallRecordCategory#21	
22	CallRecordCategory#22	
23	CallRecordCategory#23	
24	CallRecordCategory#24	
25	CallRecordCategory#25	
26	CallRecordCategory#26	
27	CallRecordCategory#27	
28	CallRecordCategory#28	
29	CallRecordCategory#29	
30	CallRecordCategory#30	
31	CallRecordCategory#31	

2. Log in to the user account management interface (see 'Users: Management' menu, web-interface users section). In the access rights of the production user, select *Listen to recorded conversations* right and set the available category to *Production*. For the sales user, select the *Listen to recorded conversations* and set the category to *Sales*:

Management → Object

Management

sales Username

..... Enter password

..... Confirm password

User access rights:

- Restart device/software
- VoIP management (SIP)
- Subscribers management
- IP-settings, RADIUS management
- Configuration management
- Software management
- Listen call records

[2] sales Call record category

Call-recording management

Monitoring

Apply Cancel

Management

production Username

..... Enter password

..... Confirm password

User access rights:

- Restart device/software
- VoIP management (SIP)
- Subscribers management
- IP-settings, RADIUS management
- Configuration management
- Software management
- Listen call records

[1] production Call record category

Call-recording management

Monitoring

Apply Cancel

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

Call recording → Call recording settings

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

Enable notification Disable notification

- Now, if the users enter the *Conversation Recording* section, they will only see records of the categories to which they have access.
- In this example, if you need to add a 'management user' with the right to listen records of all departments, then, as in step 1, add a new category, for example, 'Management' and assign the access rights to the 'Production' and 'Sales' categories. Then, in the user management section, assign the access to the 'Management' category to the management user.

Management

management Username

..... Enter password

..... Confirm password

User access rights:

- Restart device/software
- VoIP management (SIP)
- Subscribers management
- IP-settings, RADIUS management
- Configuration management
- Software management
- Listen call records

[3] management Call record category

Call-recording management

Monitoring

Apply Cancel

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

Call recording → Call record categories

Call record categories		
No	Name	Access to categories
0	Admin	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31
1	production	1
2	sales	2
3	management	1,2
4	CallRecordCategory#04	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
5	CallRecordCategory#05	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
6	CallRecordCategory#06	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
7	CallRecordCategory#07	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
8	CallRecordCategory#08	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
9	CallRecordCategory#09	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
10	CallRecordCategory#10	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
11	CallRecordCategory#11	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
12	CallRecordCategory#12	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
13	CallRecordCategory#13	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
14	CallRecordCategory#14	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
15	CallRecordCategory#15	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
16	CallRecordCategory#16	
17	CallRecordCategory#17	
18	CallRecordCategory#18	
19	CallRecordCategory#19	
20	CallRecordCategory#20	
21	CallRecordCategory#21	
22	CallRecordCategory#22	
23	CallRecordCategory#23	
24	CallRecordCategory#24	
25	CallRecordCategory#25	
26	CallRecordCategory#26	
27	CallRecordCategory#27	
28	CallRecordCategory#28	
29	CallRecordCategory#29	
30	CallRecordCategory#30	
31	CallRecordCategory#31	

4.1.13 TCP/IP Settings

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

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

4.1.13.1 Routing tables

This submenu can be used to configure static routes.

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




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

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

TCP/IP settings → Routing table

No	Enable	Status	Destination	Mask	Gateway	Interface	Metric
Automatically generated routes							
0	Yes	Active	192.168.112.0	255.255.240.0	*	eth0	0
1	Yes	Active	default	0.0.0.0	192.168.114.129	eth0	0

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

-  – Add route;
-  – Edit route parameters;
-  – Remove route.

Route Parameters

TCP/IP settings → Routing table →

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

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

4.1.13.2 Network settings

TCP/IP settings → Network settings

Network settings

Hostname:

Use gateway from:

Primary DNS:

Secondary DNS:

Port for SSH:

Port for Telnet:

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

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

4.1.13.3 Network interfaces

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

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

On the SMG-3016 it is possible to configure 2 primary network interfaces eth0 and eth2.

The eth2 interface is of the Management type and is used only to manage the device through the OOB port. The interface supports working with a static address, an address obtained via DHCP, and a VLAN.

There can only be one interface of the Management type on a device.

TCP/IP settings → Network settings

Network interfaces

№	Interface name	Network label	IP-address	Network mask	DHCP	Management services	Telephony services	Firewall profile
0	eth0	eth0	192.168.113.110	255.255.240.0	-	WEB TELNET SSH SNMP	SIP RTP H323 RADIUS	Not selected

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

Network Interface Settings

Common Settings

TCP/IP settings → Network interfaces

Network interfaces	
Network interface 7	
Network label	<input type="text"/>
Firewall profile	Not selected
Type	Untagged
Enable DHCP	<input type="checkbox"/>
IP-address	<input type="text"/>
Network mask	<input type="text"/>
Gateway	<input type="text"/>
Gateway by DHCP	<input type="checkbox"/>
DNS-address by DHCP	<input type="checkbox"/>
NTP-address by DHCP	<input type="checkbox"/>
Services	
Enable Web	<input type="checkbox"/>
Enable Telnet	<input type="checkbox"/>
Enable SSH	<input type="checkbox"/>
Enable SNMP	<input type="checkbox"/>
Enable SIP signaling	<input type="checkbox"/>
Enable RTP transmission	<input type="checkbox"/>
Enable H.323 signaling	<input type="checkbox"/>
Enable RADIUS	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- *Network label* – name of the network;
- *Firewall profile* – show the firewall profile selected for this interface;
- *Type* – interface type (always untagged for eth0 interface):
 - *untagged* – untagged interface (without VLAN);
 - *tagged* – tagged interface (with VLAN);
 - *VPN/pptp client* – client interface for connecting VPN to a remote server via PPTP protocol.
- *VLAN ID* – VLAN identifier (1–4095) (only for tagged type interfaces);
- *Enable DHCP* – dynamically obtain the IP address from the DHCP server (Alias is not supported);
- *IP-address* – network address of the device;
- *Network mask* – the subnet mask of the device;
- *Gateway* – network gateway for the interface (Alias is not supported);
- *Gateway by DHCP* – obtain the IP address of the gateway dynamically from the DHCP server (Alias is not supported);
- *DNS-address by DHCP* – obtain the IP address of the DNS server dynamically from the DHCP server (Alias is not supported);
- *NTP-address by DHCP* – obtain the IP address of the NTP server dynamically from the DHCP server (Alias is not supported).

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

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



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

Front-ports – configuring external front ports (only for SMG-2016)

This setting is available only for tagged VLAN interfaces (in the ‘Type’ parameter set to ‘Tagged’).

TCP/IP settings → Network settings → Tagged

Front-ports				
	0	1	2	3
Default VLAN ID	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Egress mode	tagged ▼	tagged ▼	tagged ▼	tagged ▼

- *Default VLAN ID* – when a packet without a VLAN ID tag arrives on a port, this packet is marked with a VLAN ID tag of the selected network interface; if a packet is received with a VLAN ID tag, then the received tag is not changed;
- *Egress mode* – rules for working with the VLAN tag when sending a packet from a port:
 - *tagged* – send a packet with the VLAN ID of the selected network interface;
 - *untagged* – send a packet without a VLAN ID.

VPN/PPP interface settings:

TCP/IP settings → Network settings → VPN/pptp client

Network interface 1	
Network label	<input type="text"/>
Firewall profile	Not selected
Type	VPN/pptp client <input type="button" value="v"/>
Enable	<input type="checkbox"/>
PPTPD IP	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Options	
Ignore default gateway	<input type="checkbox"/>
Enable MPPE (encryption)	<input type="checkbox"/>
Services	
Enable Web	<input type="checkbox"/>
Enable Telnet	<input type="checkbox"/>
Enable SSH	<input type="checkbox"/>
Enable SNMP	<input type="checkbox"/>

Basic settings:

- *Network label* – name of the network;
- *Firewall profile* – show the firewall profile selected for this interface;
- *Type* – VPN/pptp client;
- *PPTPD IP* – IP address of the PPTP server;
- *Username* – username (login) by which the device connects to the network;
- *Password* – password for VPN connection.

Options:

- *Ignore default gateway* – ignore the gateway setting in the Network section options;
- *Enable encryption* – enables encryption.

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

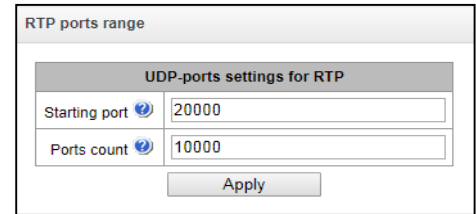
- *Enable Web* – enables access to the configurator via the interface;
- *Enable Telnet* – enables access via the Telnet protocol;
- *Enable SSH* – enables access via the SSH protocol;
- *Enable SNMP* – enables access via the SNMP protocol.

4.1.13.4 RTP ports

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

UDP-ports settings for RTP

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




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

4.1.14 Data transfer



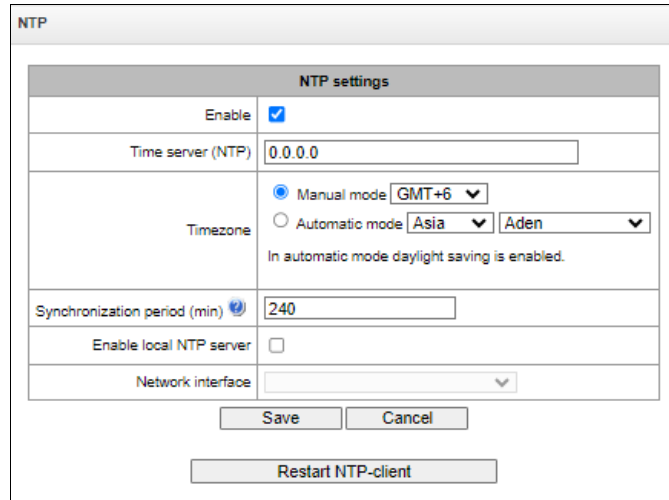
The functionality is activated with the SMG-SORM-374 license; more information about licenses is in the Licenses section (for Russian market only).

4.1.15 Network services

4.1.15.1 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.

Network services → NTP



- *Enable* — enable time synchronization via NTP;
- *Time server (NTP)* — NTP server IP address or host name;
- *Timezone* — timezone and GMT (Greenwich Mean Time) offset configuration:
 - *Manual mode* — define GMT offset.
 - *Automatic mode* — in this mode, you may select the device location, GMT offset will be defined automatically, also this mode enables automatic daylight saving change.
- *Synchronization period, minutes* — time synchronization request transmission period;
- *Enable local NTP server* – activate a local NTP server for time synchronization with external devices. The option is available when '*Enable*' box is checked;
- *Network interface* – select a network interface through which the local NTP-server will answer on requests.

Use '*Save*' button to save the setting and '*Cancel*' to clear the settings. To perform forced time synchronization with the server, click '*Restart NTP client*' button (NTP client will be restarted).

4.1.15.2 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

SNMP settings

Network services → SNMP

SNMP settings	
Sys Name	smg2016 testing
Sys Contact	Eltex VoIP lab
Sys Location	Novosibirsk, O. 29B
ro Community	public
rw Community	private
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

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

Use 'Apply' button to apply settings and 'Reset' to cancel the settings.

4.1.15.3 SNMPv3

SNMPv3 configuration:

Network services → SNMP

SNMPv3 settings	
RW user name	<input type="text"/>
RW user password	<input type="password"/>
<input type="button" value="Delete"/> <input type="button" value="Add"/>	

The system uses a single SNMPv3 user.

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

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

4.1.15.4 SNMP trap settings






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

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

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

Network services → SNMP


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

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

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

-  — 'Add'
-  — 'Edit'
-  — 'Remove'

Network services → SNMP → SNMP traps settings → 

SNMP trap 2	
Type	trapsink ▼
Community	<input type="text"/>
IP-address	0.0.0.0
Port	162
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

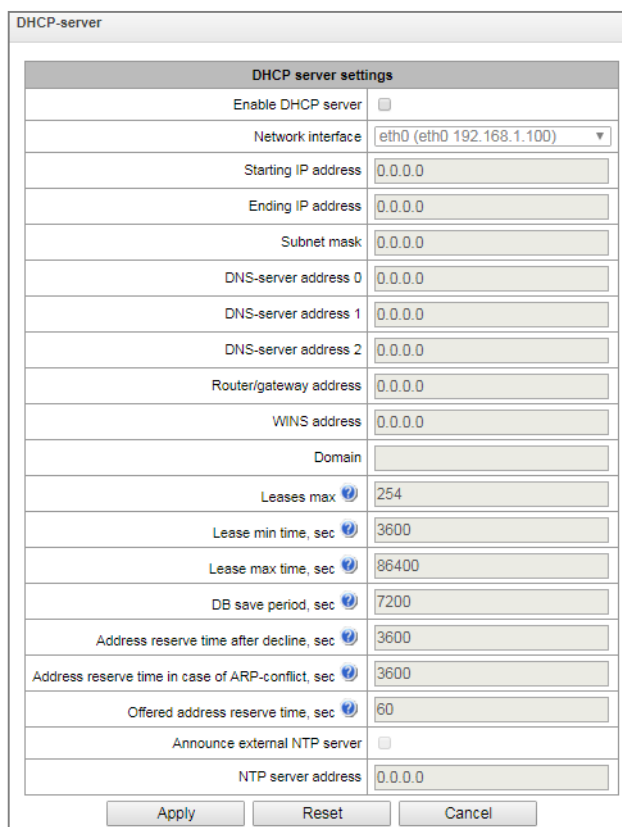
- *Type* — SNMP message type (TRAPv1, TRAPv2, INFORM);
- *Community* — password contained in traps;
- *IP address* — trap recipient IP address;
- *Port* — trap recipient UDP port (default port: 162).

4.1.15.5 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.

Network services → DHCP-server



DHCP server settings	
Enable DHCP server	<input type="checkbox"/>
Network interface	eth0 (eth0 192.168.1.100)
Starting IP address	0.0.0.0
Ending IP address	0.0.0.0
Subnet mask	0.0.0.0
DNS-server address 0	0.0.0.0
DNS-server address 1	0.0.0.0
DNS-server address 2	0.0.0.0
Router/gateway address	0.0.0.0
WINS address	0.0.0.0
Domain	
Leases max	254
Lease min time, sec	3600
Lease max time, sec	86400
DB save period, sec	7200
Address reserve time after decline, sec	3600
Address reserve time in case of ARP-conflict, sec	3600
Offered address reserve time, sec	60
Announce external NTP server	<input type="checkbox"/>
NTP server address	0.0.0.0

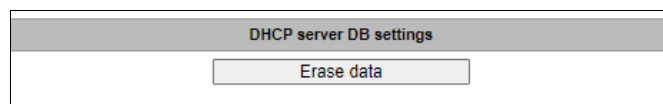
DHCP server parameters:

- *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 address* — DNS server addresses from the operator's networks;
- *Router/gateway address* — default router or gateway address assigned by DHCP server to clients;
- *WINS address* — WINS server IP address in the operator's network;
- *Domain* — network domain name;
- *Leases max, sec* — restrict the number of simultaneously leased addresses;

- *Lease min time, sec* — set the minimum lease time for IP address assigned by DHCP server to the client, 10 seconds or more;
- *Lease max time, sec* — set the maximum lease time for IP address assigned by DHCP server to the client, from 10 to 10,000,000 seconds;
- *DB save period, sec* — time interval for saving information on leased addresses to dhcpd.leases file. Select 'off' to disable saving of the information on the leased addresses;
- *Address reserve time after decline, sec* — time period that the IP address will remain reserved for the client upon the DHCP decline reception, 10 seconds or more;
- *Address reserve time in case of ARP conflict, sec* — time period that the IP address will remain reserved for the client upon MAC address conflict identification, 10 seconds or more;
- *Offered address reserve time, sec* — time period that the IP address requested by client will remain reserved, 10 seconds or more;
- *Announce local NTP server* — the option is available only if local NTP server is activated in 'NTP' section and an interface is defined for the server. When DHCP option is activated, the server will announce the address of the set local NTP server via DHCP option 42;
- *Announce external NTP server* — when DHCP option is activated, the server will announce the address of the NTP servers defined in 'NTP server address' via DHCP option 42;
- *NTP server address* — NTP server address, which SMG will announce via option 42 if 'Announce external NTP server' is enabled.

DHCP server DB settings

Network services → DHCP-server



- *Start server* — launch DHCP server;
- *Stop server* — stop DHCP server operation;
- *Erasa data* — remove established IP-MAC associations from the DHCP server memory.


IP-MAC addresses bonding — assign static associations between IP addresses and MAC addresses.

Network services → DHCP-server

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'

Network services → DHCP-server → IP-MAC addresses bonding → 

DHCP lease 3	
Name	DHCPD lease 3
IP address	0.0.0.0
MAC address	00:00:00:00:00:00
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

Leased IP addresses

Network services → DHCP-server

Leased IP addresses		
MAC address	IP address	Lease ends
a8:aa:bb:cc:dd:ee	16.17.18.4	expired
a8:00:00:00:00:00	16.17.18.5	expired

- *MAC address* — client MAC address;
- *IP address* — address issued from the pool of IP addresses;
- *Lease ends* — remaining time of the address lease:
 - *Expired* — address lease has expired.

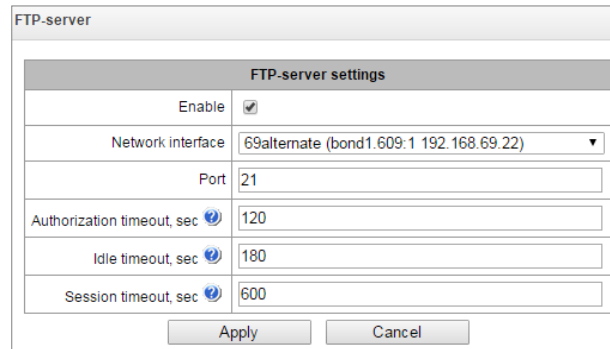
4.1.15.6 FTP server

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

Network services → FTP-server

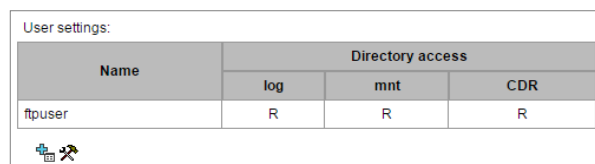


- *Enable* — enable/disable integrated FTP server;
- *Network interface* — select network interface for the FTP server to run on;
- *Port* — select TCP port for the FTP server to run on;
- *Authorization timeout, sec* — data entry timeout for subscriber authorization at FTP server; when this timeout expires, the server will forcibly terminate the connection;
- *Idle timeout, sec* — timeout for the user to be idle at FTP server; when this timeout expires, the server will forcibly terminate the connection;
- *Session timeout, sec* — session duration.

User settings

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

Network services → FTP-server



Name	Directory access		
	log	mnt	CDR
ftpuser	R	R	R

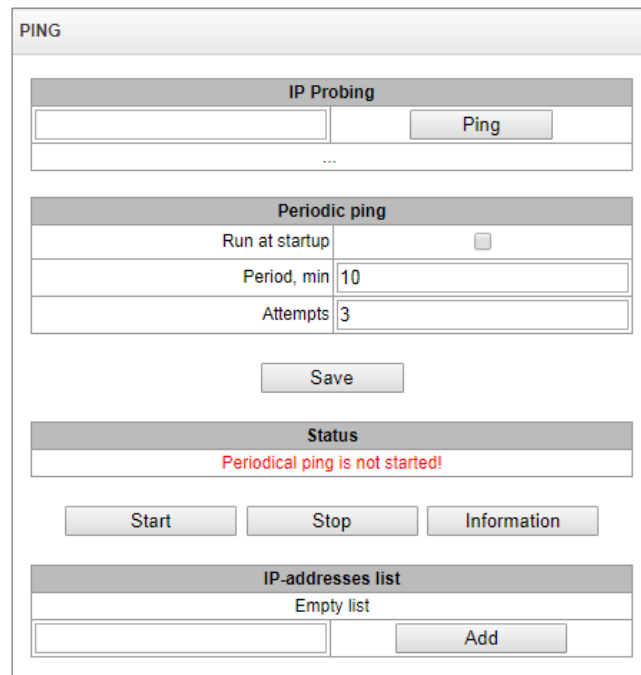
- *Name* — username
- *Password* — user password
- *Access to logs* — log directory access configuration, read/write
- *Access to mounts* — mnt directory access configuration, read/write
- *Access to CDR* — CDR directory access configuration, read/write
- *Access to configuration* — access settings for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

4.1.16 Network utilities

4.1.16.1 PING

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

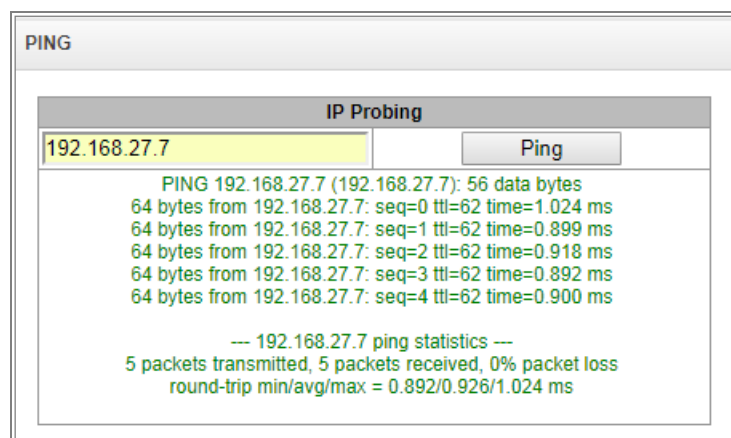
Network utilities → PING



IP Probing – used for a single-time check of the device network connection.

To send a ping request (*the ICMP protocol is used*), enter the host IP address or network name in the *IP Probing* field and click the *Ping* button. The result of the command execution will be shown at the bottom of the page. The result contains information on the number of transmitted packets, the number of responses to the packets, the percent of lost packets, and the time of reception/transmission (minimum/average/maximum) in milliseconds.

Network utilities → PING



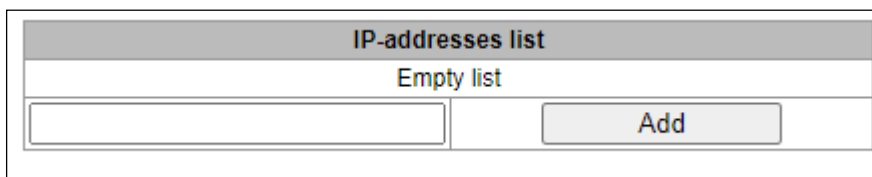
Periodic ping – used for periodic check of device network connection.

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

Status

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

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

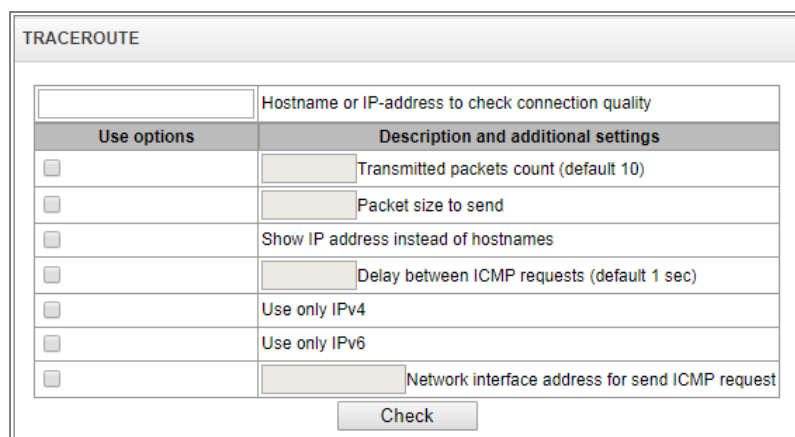


To add a new address to the list, select it in the entry field and click the ‘Add’ button. To remove an address, click the ‘Remove’ button next to the required address.

4.1.16.2 TRACEROUTE

The *TRACEROUTE* utility performs the route tracing function and ping tests to monitor the network health. This function allows you to evaluate the connection quality for the tested node.

Network utilities → *TRACEROUTE*



Use options	Description and additional settings
<input type="checkbox"/>	Transmitted packets count (default 10)
<input type="checkbox"/>	Packet size to send
<input type="checkbox"/>	Show IP address instead of hostnames
<input type="checkbox"/>	Delay between ICMP requests (default 1 sec)
<input type="checkbox"/>	Use only IPv4
<input type="checkbox"/>	Use only IPv6
<input type="checkbox"/>	Network interface address for send ICMP request

In the ‘*Hostname or IP address to check connection quality*’ field, enter the IP address of the network device to test the connection quality. To use the options, select the checkboxes in the corresponding line.

Options:

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

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

As a result, the utility displays a table containing:

- the node number and its IP address (or network name)
- the percentage of packets lost (Loss%)
- the number of packets sent (Snt)
- the round-trip time of the last packet (Last)
- average round-trip time of the packet (Avg)
- the best round-trip time of the packet (Best)
- the worst time round-trip time of the packet (Wrst)
- the standard deviation of delays for each node (StDev)

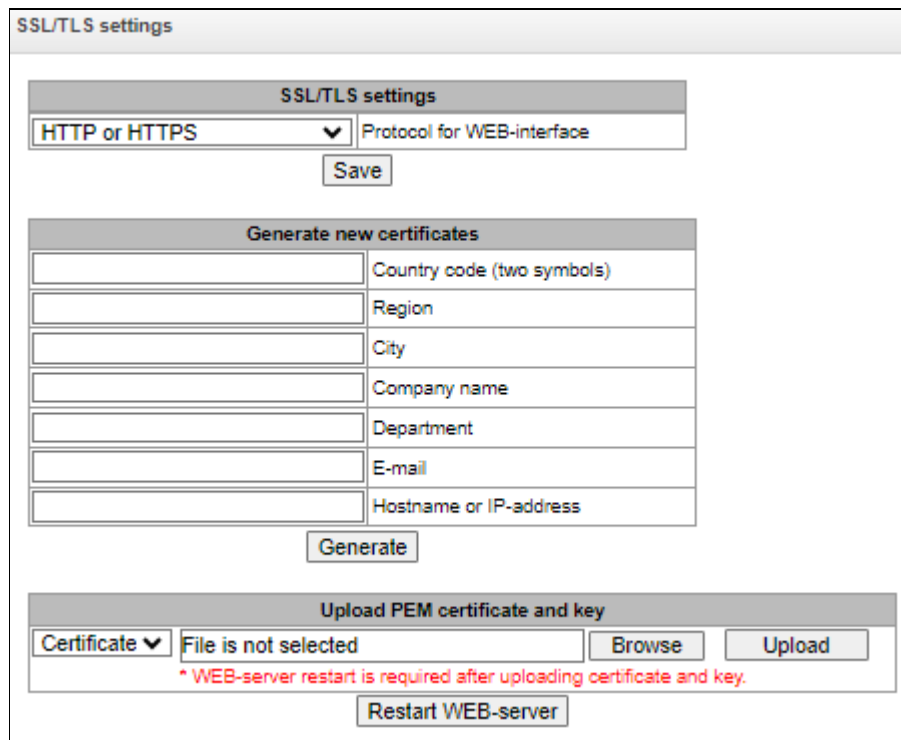
Network utilities → TRACEROUTE → IP address of network device

HOST: smg2016	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. -- 192.168.18.58	0.0%	10	0.1	0.1	0.1	0.2	0.0

4.1.17 Security

4.1.17.1 SSL/TLS settings

Security → SSL/TLS settings



In this section, you may obtain a self-signed certificate which allows you to use an encrypted connection to the gateway via HTTP protocol and configuration file upload/download via FTPS protocol.

- *Protocol for WEB-interface* — web configurator connection mode:
 - *HTTP or HTTPS* — unencrypted connection — via HTTP — as well as encrypted connection — via HTTPS — is enabled. At that, connection via HTTPS is possible only when generated certificate is present.
 - *HTTPS only* — only encrypted connection via HTTPS is enabled. Connection via HTTPS is possible only when generated certificate is present.

Generate new certificates



These parameters should be entered in Latin characters.

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

Upload PEM Certificate and Key

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



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

4.1.17.2 Dynamic firewall

Dynamic firewall — is a utility that tracks attempts of access to various services. When constantly repeated unsuccessful access attempts from the same IP address/host are discovered, fail2ban blocks all further access attempts from this IP address/host.

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

- Brute forcing web configurator or SSH authentication data, i.e. attempt to log in to the management interface using wrong login or password.
- Brute forcing authentication data — reception of REGISTER requests from known IP address but containing wrong authentication data.
- Reception of requests (REGISTER, INVITE, SUBSCRIBE and others) from unknown IP address.
- Reception of unknown requests via SIP port.

Security → Dynamic firewall

Dynamic firewall

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

White list

(Total records: 1)

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

Blacklist

(Total records: 0)

<input type="checkbox"/>	IP address or IP/mask (last 30 records)
The list is empty	

Blocked addresses list

(Total records: 0)

<input type="checkbox"/>	IP address or IP/mask (last 30 records)
The list is empty	

Parameters:

- *Enable* — launch dynamic firewall utility;
- *Block time, sec* — time in seconds during which access from the suspicious address will be banned;
- *Forgive time, sec*— time that should pass for the address that originated the suspicious request to be forgotten if it was not banned earlier;
- *Access attempts before blocking* — maximum quantity of unsuccessful access attempts for a host prior to be banned by dynamic firewall;
- *Block attempts before black-listing* — quantity of bans after which the suspicious address will be blacklisted;
- *Progressive block* — when checked, each following address ban will be twice longer than the previous one and twice less access attempts will be used. E.g. for the first time address was banned for 30 seconds after 16 attempts, for the second time — for 60 seconds after 8 attempts, for the third time — for 120 seconds after 4 attempts and so forth.

White list (last 30 records) — list of IP addresses and subnets that dynamic firewall will be unable to ban.



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

Black list (last 30 records) — list of permanently banned addresses and subnets. A device may have up to 8192 records on SMG-1016M and 16384 records on SMG-2016 and SMG-3016. To add/search/remove an address from the list, select it in the entry field and click 'Add'/'Search'/'Delete' button.

You may enter an IP address as well as a subnet.

To enter the subnet, you should enter the data in the following format:

AAA.BBB.CCC.DDD/mask

Example:

192.168.0.0/24 — record corresponds to the network address 192.168.0.0 with mask 255.255.255.0

Download whole IP address white/black list — web configurator shows only the 30 last records in the file; click this button to download the whole white list and black list to your PC.

Blocked addresses list — list of addresses banned while dynamic firewall operation. Up to 8192 entries are available on SMG-1016M and up to 16384 entries are available on SMG-2016.

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

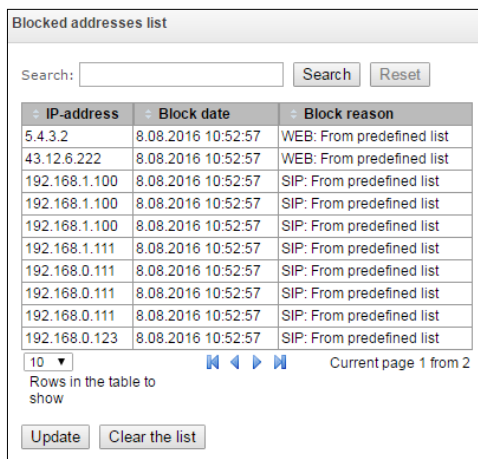
To update the lists, click 'Update' button next to the header.

Dynamic firewall log information is written into **pbx_sip_bun.log** file.

4.1.17.3 Blocked addresses list

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

Security → Blocked addresses list



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 an address to search for it in the blocked address table;
- *IP-address* — IP address that was banned;
- *Block date* — date and time of IP address ban;
- *Block reason* — a cause of blocking;
- *Update* — update blocked addresses list;
- *Clear the list* — delete all records from the banned address log.

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

Table 28 — Banning messages

Message in pbx_sip_bun.log	Reason	SIP message
Request error: REGISTER failed : Resource limit overflow	Dynamic user registration limit has been achieved	403 response
Request error: REGISTER failed : Unknown user or registration domain	Registration request from unknown user	403 response
Request error: REGISTER failed : Server doesn't allow a third party registration	Registration request with different To and From headers	403 response
Request error: REGISTER failed : Authentication is wrong	Wrong login/password	403 response
Request error: REGISTER failed : Wrong de-registration	User attempted to deregister not registered contact	200 response
Request error: REGISTER failed : Request from disallowed IP	Registration attempt from not allowed address	403 response
Request error: INVITE failed : No registration before	Call attempt from known user with not registered contact	403 response

Request error: INVITE failed : Registration is expired	Call attempt from known user with expired contact registration	403 response
Request error: INVITE failed : Authentication is wrong	Incoming call or registration has failed an authentication	403 response
Request error: INVITE failed : Unknown original address	Call from an unknown direction	Call is directed to mgapp where it will be passed through or rejected
Request error: INVITE failed : RURI not for me	Unknown host name or address in RURI	404 response
Request error: BYE failed : Call/Transaction Does Not Exist	Dialog for request acceptance has not been found	481 response

4.1.17.4 Static firewall

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

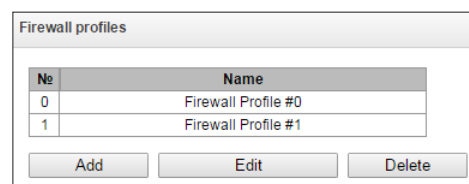


The rules of static firewalls will not operate to limit access via HTTP/HTTPS, SSH, Telnet, SNMP, FTP. To limit the access via these protocols, use the white addresses list (section 4.1.17.5 White addresses list) and services activation settings on the network interfaces (section 4.1.13.3 Network interfaces).

Firewall profiles

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

Security → Static firewall



- *Add*
- *Edit*
- *Delete*

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

Security → Static firewall → Object

Firewall profiles

Firewall profile 0

Profile settings

Name

Rules for ingress traffic

No	Name	Status	Packet source	Ports	Destination address	Ports	Protocol	Action
0	Firewall rule 0	Enable	1.2.3.4	0	Any	0	UDP	Reject
1	Firewall rule 1	Enable	1.2.8.0/255.255.255.224	0	Any	0	TCP	Reject
2	Firewall rule 2	Enable	192.4.0.0/255.255.0.0	0	Any	5060	TCP/UDP	Drop
3	Firewall rule 3	Enable	192.166.66.5	0	Any	0	ICMP	Drop
4	Firewall rule 4	Enable	Any	0	Any	0	Any	Accept

Rule for egress traffic

No	Name	Status	Packet source	Ports	Destination address	Ports	Protocol	Action
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>								

Interface

<input type="checkbox"/>	bond1.1 (bond1.1)
<input type="checkbox"/>	testnet_118 (bond1.1:1)
<input checked="" type="checkbox"/>	2.2/24 (bond1.1:2)
<input type="checkbox"/>	0.2/24 (bond1.1:3)
<input checked="" type="checkbox"/>	3.2/24 (bond1.1:4)
<input type="checkbox"/>	vlan609 (bond1.609)
<input type="checkbox"/>	69alternate (bond1.609:1)
<input type="checkbox"/>	pptp_iface (ppp8)

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:
 - *ingress* — intended for SMG.
 - *egress* — sent by SMG.
- *Rule type* — might have the following values:
 - *General* — check IP addresses and ports;
 - *GeoIP* — check addresses in GeoIP base;
 - *String* — check the presence of a string in a packet.

Security → Static firewall → Object → Rule type (General)

Static firewall	
Firewall rule	
Name	Firewall rule 0
Enable	<input type="checkbox"/>
Traffic type	Ingress
Rule type	General
Packet source	<input checked="" type="checkbox"/> Any
IP-address/mask	0.0.0.0
Source ports	0
Destination address	<input checked="" type="checkbox"/> Any
IP-address/mask	0.0.0.0
Destination ports	0
Protocol	Any
ICMP message type	any
Action	Accept
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Security → Static firewall → Object → Rule type (String)

Static firewall	
Firewall rule	
Name	Firewall rule 0
Enable	<input type="checkbox"/>
Traffic type	Ingress
Rule type	String
Content	
Packet source	<input checked="" type="checkbox"/> any
IP-address/mask	0.0.0.0
Source ports	0
Destination address	<input checked="" type="checkbox"/> any
IP-address/mask	0.0.0.0
Destination ports	0
Protocol	any
ICMP message type	any
Action	Accept
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Firewall rule	
Name	Firewall rule 0
Enable	<input type="checkbox"/>
Traffic type	Ingress
Rule type	GeolIP
Country	Afghanistan (AF)
Source ports	0
Destination ports	0
Protocol	any
ICMP message type	any
Action	Accept

- **Packet source** — defines the packet source network address either for all addresses or a particular IP address or network:
 - *any* — for all addresses (checkbox is selected);
 - *IP address/mask* — for a particular IP address or network. Field is active when '*any*' checkbox is deselected. For a network, the mask is mandatory; for IP address, the mask is optional;
 - *Source ports* — packet source TCP/UDP port or port range (defined with a hyphen '-'). This parameter is used for TCP and UDP only; thus, select UDP, TCP, or TCP/UDP in the field in order to make this field active.
- **Destination address** — defines the packet recipient network address either for all addresses or a particular IP address or network:
 - *any* — for all addresses (checkbox is selected);
 - *IP address/mask* — for a particular IP address or network. Field is active when '*any*' checkbox is deselected. For a network, the mask is mandatory; for IP address, the mask is optional;
 - *Destination ports* — packet recipient TCP/UDP port or port range (defined with a hyphen '-'). This parameter is used for TCP and UDP only; thus, select UDP, TCP, or TCP/UDP in the field in order to make this field active.
- **Protocol** — protocol that the rule will be used for: any, UDP, TCP, ICMP, or TCP/UDP;
- **ICMP message type** — ICMP message type that the rule will be used for. This field is active, when ICMP is selected in the '*Protocol*' field;
- **Action** — action executed by this rule:
 - *ACCEPT* — packets falling under this rule will be accepted by the firewall;
 - *DROP* — packets falling under this rule will be rejected by the firewall without informing the party that has sent these packets;
 - *REJECT* — packets falling under this rule will be rejected by the firewall. The party that has sent the packet will receive either TCP RST packet or 'ICMP destination unreachable'.

- *Country* – select a country to which the address belongs. The field is available only for 'GeoIP' rule type;
- *Content* – the string which might be in packets. The case of letters is important. The field is available only for 'String' rule type.

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.



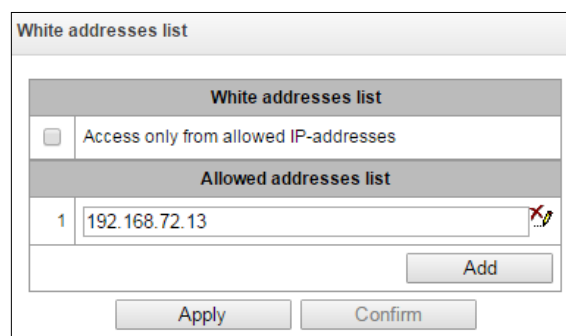
Each network interface may be used only in a single firewall profile at a time. If you attempt to assign a network interface to a new profile, it will be removed from the previous one.

To apply the rules, click '*Apply*' button that will appear when the changes are made into the firewall settings.

4.1.17.5 White addresses list

In this section, you may configure the list of allowed IP addresses that the administrator may use for connection to the device via web configurator and Telnet/SSH protocol. By default, all addresses are allowed.

Security → *White addresses list*



The screenshot shows a web interface window titled "White addresses list". At the top, there is a checkbox labeled "Access only from allowed IP-addresses". Below this is a section titled "Allowed addresses list" containing a table with one row: "1" in the first column and "192.168.72.13" in the second column. To the right of the IP address is a small icon with a red 'X' and a pencil. Below the table is an "Add" button. At the bottom of the window are "Apply" and "Confirm" buttons.

- *Access only from allowed IP addresses* — when checked, the list of allowed IP addresses will be applied; otherwise, access is allowed from any address.

You may enable access for subnets; to do that, you should specify address in IP/mask format, e.g.: 192.168.0.0/24.

- *Apply* — apply changes.
- *Confirm* — confirm changes.

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

-  — '*Add*'
-  — '*Edit*'
-  — '*Remove*'



When the address list has been configured, click '*Apply*' and '*Confirm*' buttons; if you fail to confirm changes in 60 seconds, previous values will be restored — this procedure allows to protect the user from the loss of access to the device

4.1.17.6 SMG firewall operation scheme

The next rule processing procedure is used on SMG for dynamic and static firewall, list of prohibited IP addresses, and access limitation from network interfaces:

1. Rule processing of dynamic firewall (see section 4.1.17.2 Dynamic firewall) is performed. On this stage, requests received from IP addresses located on the blacklist will be dropped.
2. Processing of access limitations (see section 4.1.13.3 Network interfaces -> Services and 4.1.17.5 White addresses list). The rules allowing access to any IP addresses will be created for each service enabled on network interface. The access for other services will be blocked. If the allowed IP address list is activated, the access rules will be updated by control of source IP addresses (connection will be available only for IP address from the list). For each service that is allowed for working on the network interface, rules allowing to access from any IP address are created. Access to other services will be blocked. When the list of allowed IP addresses is activated, the access rules are supplemented with the control of the source IP address. Connection is allowed only from the addresses specified in the list.
3. Access to network interfaces that is not bound with rules of static firewall is allowed.
4. The static firewall rules (see 4.1.17.4 Static firewall) is being processed on the network interfaces to which they are bound.



If one of the rules from the list is processed, remaining rules will not be applied to a request.

4.1.17.7 Providing SMG firewall tasks

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

To restrict the access to management, use 4.1.13.3 Network interfaces -> Services and 4.1.17.5 White addresses list. In the beginning, you should set protocol flags for network interfaces that have to be accessed. Thus, destination address restriction will be applied. After that, the allowed IP addresses list will be created. This list imposes additional restrictions for source IP addresses in accordance with allowed IP addresses.

To restrict the access to SIP/H.323 interfaces by specific addresses and/or geographic locations, configure a static firewall (see section 4.1.17.4 Static firewall).

The example of configuration with such restrictions shown below:

- *Enable the access from Russia;*
- *Enable the access from subnet 34.192.128.128/28;*
- *Restrict the access from other addresses.*

To do that, create tree rules for static firewall in the next order:

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

After that, select the required network interfaces from the list and save settings.

Fully-restricted access to SMG from a specific address or subnet

In order to implement access restriction to SMG from a certain address or subnet, it is necessary to activate the dynamic firewall (see section 4.1.17.2 Dynamic firewall) and enter address or subnet in the black list. Pay attention, if there are too many addresses, it is better to create static firewall rules (see 4.1.17.4 Static firewall) according the next principle: ‘first of all, allow connection to trusted nodes, and then drop all’. Also, use settings for the access restriction by the list of allowed IP addresses (see section 4.1.17.5 White addresses list).

Automatic blocking of failed requests/authorizations

The dynamic firewall (see section 4.1.17.2 Dynamic firewall) automatically blocks failed requests/authorizations. To enable the automatic blocking, you should activate dynamic firewall and configure the trigger conditions. Also, it is recommended to add addresses and subnets that shouldn't fall under the rules of automatic blocking in the white list.

4.1.18 RADIUS settings

4.1.18.1 Servers

RADIUS settings → Servers

Servers

RADIUS-Authorization servers

	IP-address	Port	Secret-key	Group
1	127.0.0.1	1812	dummy	0 ▼
2	0.0.0.0	0		0 ▼
3	0.0.0.0	0		0 ▼
4	0.0.0.0	0		0 ▼
5	0.0.0.0	0		0 ▼
6	0.0.0.0	0		0 ▼
7	0.0.0.0	0		0 ▼
8	0.0.0.0	0		0 ▼

RADIUS-Accounting servers

	IP-address	Port	Secret-key	Group
1	127.0.0.1	1813	dummy	0 ▼
2	0.0.0.0	0		0 ▼
3	0.0.0.0	0		0 ▼
4	0.0.0.0	0		0 ▼
5	0.0.0.0	0		0 ▼
6	0.0.0.0	0		0 ▼
7	0.0.0.0	0		0 ▼
8	0.0.0.0	0		0 ▼

Server reply timeout (x100 ms)

Request sending attempts

Server inactivity timeout after failure (sec)

Network interface for group 0

Network interface for group 1

Network interface for group 2

Network interface for group 3

WEB/telnet/ssh users authorization through RADIUS-authorization servers

Allow access when RADIUS-server failure

Device supports up to 8 authorization servers and up to 8 accounting servers. The servers might be combined in a group. Then, while RADIUS profiles settings, you may choose the group of servers to transmit requests. Four group are available.




- *Server reply timeout* (x100 ms) — amount of time intended for server response;
- *Request sending attempts* — quantity of request retries addressed to a server. When all attempts are used up, the server will be deemed inactive and the request will be forwarded to another server, if it is specified, otherwise the error will be detected;

- *Server inactivity timeout after failure (sec)* — amount of time that the server is deemed unavailable (requests will not be sent to it);
- *Network interface for <N> group* — select corresponding group for network interface through which RADIUS requests will be transmitted;
- *WEB/telnet/ssh users authorization through RADIUS-authorization servers* — in case of the access attempt via WEB/telnet/ssh, the authorization will be implemented via RADIUS server. You should register local users with the necessary names and configure access rights in advanced (see 4.1.27 'Users: Management' menu);
- *Allow access when RADIUS-server failure* — if authorization via RADIUS is enabled and there is no answer from the RADIUS server, you may use local account of admin.

4.1.18.2 Profiles

RADIUS → Profiles

Profiles			
No	Name	Authorization	Accounting
0	RADIUS_Profile00	+	+

To create, edit and delete profiles from the list use the following buttons:

-  — 'Add'
-  — 'Edit'
-  — 'Delete'

RADIUS → Profiles → Object

RADIUS rule 0	
Name	RADIUS_Profile00
Enable RADIUS-Authorization	<input type="checkbox"/>
Enable RADIUS-Accounting	<input type="checkbox"/>
Send SNMP trap	<input type="checkbox"/>
Group	0
Modifiers settings	
Modifiers for InCdPN	not used
InCdPN	original
Modifiers for InCgPN	not used
InCgPN	original
Modifiers for Redirecting	not used
Modifiers for OutCdPN	not used
Modifiers for OutCgPN	not used
RADIUS-Authorization settings	
Send requests for ingress calls	<input type="checkbox"/> on ingress seize (CgPN only) <input type="checkbox"/> on end-of-dial (CgPN and CdPN) <input type="checkbox"/> on local redirection
Send requests for egress calls	<input type="checkbox"/> on egress seize
Send requests by modifiers	Default
Access restriction on server failure	no restrictions
User-name field (originate)	CgPN
User-name field (answer)	CdPN
Redirecting Number	replace Calling-Station-Id
User-password field	
Individual passwords for SIP-subscribers	<input type="checkbox"/>
DIGEST authorization	RFC5090
Session timeout	Ignore
Enable emergency call on receiving Reject	<input type="checkbox"/>
NAS-Port-Type	Async
Service-Type	Not used
Framed-protocol	Not used
Class	Not used
<input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>	
RADIUS-Accounting settings	
Send requests	<input checked="" type="checkbox"/> accounting-start <input checked="" type="checkbox"/> accounting-stop <input type="checkbox"/> accounting-stop for unsuccessful calls <input type="checkbox"/> accounting-update with period 2 minutes <input checked="" type="checkbox"/> accounting for call-origin=originate <input type="checkbox"/> accounting for call-origin=answer
Send requests by modifiers	Default
CISCO adaptation	<input type="checkbox"/>
Use UTC timezone	<input type="checkbox"/>
Round duration	upwards
Access restriction on server failure	no restrictions
User-name field (originate)	CgPN
User-name field (answer)	CdPN
Redirecting Number	replace Calling-Station-Id
CdPN field	CdPN-in
CgPN field	CgPN-in
Accordance for RADIUS reply and voice messages	
Accordance table for RADIUS reply and voice messages	not used
RADIUS reply attribute	Reply-Message
VSA settings	
Enable VSA for call management	<input type="checkbox"/>
Full CISCO-VSA fields	<input type="checkbox"/>

Profile parameters

- *Name* – profile's name;
- *Enable RADIUS-Authorization* — enable/disable the transmission of authentication/authorization (Access Request) messages to the RADIUS server;
- *Enable RADIUS-Accounting* — enable/disable the transmission of accounting (Accounting Request) messages to the RADIUS server;
- *Send SNMP trap* – enable SNMP trap sending with every RADIUS request transmission;
- *Group* – the group of RADIUS servers used to transmit requests.

Modifiers settings

- *Modifiers for InCdPN* — select callee (CdPN) number modifier for the incoming connection in relation to Called-Station-Id, xpgk-dst-number-in in fields of RADIUS-Authorization and RADIUS-Accounting messages;
- *InCdPN* — select the number transmitted in xpgk-dst-number-in in field of RADIUS-Authorization and RADIUS-Accounting messages:
 - *original* — initial number that was received in CdPN field of the incoming call prior to its modification;
 - *processed* — CdPN number after modification.
- *Modifiers for InCgPN* — select caller (CgPN) number modifier for the incoming connection in relation to Calling-Station-Id, xpgk-src-number-in fields of RADIUS-Authorization and RADIUS-Accounting messages;
- *InCgPN* — select the number transmitted in xpgk-dst-number-in field of RADIUS-Authorization and RADIUS-Accounting messages:
 - *original* — initial number that was received in CgPN field of the incoming call prior to its modification;
 - *processed* — CgPN number after modification.
- *Modifiers for Redirecting* — selecting a forwarding number modifier (RedirPN) in the h323-redirect-number field in RADIUS-Authorization and RADIUS-Accounting messages;
- *Modifiers for OutCdPN* — select callee (CdPN) number modifier for the outgoing connection in relation to xpgk-src-number-out field of RADIUS-Authorization and RADIUS-Accounting messages;
- *Modifiers for OutCgPN* — select caller (CgPN) number modifier for the outgoing connection in relation to xpgk-dst-number-out field of RADIUS-Authorization and RADIUS-Accounting messages.

RADIUS-Authorization settings

- *Send requests for ingress calls.* Authentication/authorization requests may be transmitted during various call phases:
 - on ingress seize (CgPN only);
 - on the end-of-dial (CgPN and CdPN) — upon receipt of the complete dialing number;
 - on local redirection.
- *Send requests for egress calls.* Authentication/authorization requests may be transmitted:
 - on egress seize.

The control of calls in RADIUS might be limited on the basis of modifier mask. Select one or more modifiers in 'Modifiers settings' and select 'Restrict' in the 'Send requests by modifiers' field. In this case, a request for authorization will be sent to RADIUS only if the number complies one of the mask in the modifiers table. The modification will be implemented as usual, according to modifiers table rules.



When 'Send requests by modifiers' is set to 'Restrict', the calls which numbers is not in the modifier mask will be considered as automatically authorized.

-
- *Access restriction on server failure.* During server fault (response non-reception), you may impose restrictions upon the outgoing communications:
 - *no restrictions* — allow all calls;
 - *local and zone networks only* — allow calls to emergency services, local and zone network;
 - *local network only* — allow calls to emergency services and local network;
 - *emergency only* — allow calls to emergency services only;
 - *deny all (disconnect)* — deny all calls.

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

- *User-name field* — select User-Name attribute value in the corresponding Access Request authorization packet (RADIUS-Authorization):
 - *CgPN* — use calling party phone number as the value;
 - *CdPN* — use called party phone number as the value;
 - *IP or E1-stream* — use calling party IP address or incoming connection stream number as the value;
 - *Trunk name* — use incoming connection trunk name as the value;
 - *Original CgPN* — use non-modified phone number of the caller as the value;
 - *Original CdPN* — use non-modified phone number of the callee as the value;
 - *Login* — use the login from the sip subscriber authorization as the value.
- *Redirecting Number* — a mode of RedirPN transmission to RADIUS:
 - *replace Calling-Station-Id* — RedirPN will be transmitted to the Calling-Station-Id field, replacing the existing value;
 - *send as h323-redirect-number* — RedirPN will be transmitted to the h323-redirect-number field separately.
- *User-password field* — specify User-Password attribute value in the corresponding RADIUS-Authorization packet;
- *Individual passwords for SIP subscribers* — when checked, use custom passwords for authentication/authorization of SIP subscribers instead of the password specified in USER-PASSWORD field;
- *DIGEST authorization* — select subscriber authorization algorithm with dynamic registration through the RADIUS server. In DIGEST authorization, the password is not transferred in the open as for the basic authentication; it represents a hash code and couldn't be intercepted during traffic scanning:
 - RFC5090 (RFC5090 recommendation complete implementation);
 - RFC5090-no-challenge (operation with a server that does not transfer Access Challenge);
 - Draft-sterman (NetUp, FreeRadius) (operation upon draft that RFC5090 recommendation is based on).
- *Session timeout* — impose limitation on the maximum call duration:
 - *Ignore* — do not impose limitation on the maximum call duration;
 - *Use Session-Time* — limit the maximum call duration on the basis of the Session-Timeout(27) attribute value;
 - *Use Cisco h323-credit-time* — limit the maximum call duration on the basis of the Cisco VSA (9) h323-credit-time(102) attribute value;
 - *Session-Time priority* — if both parameters (session-time and Cisco h323-credit-time) are present in the server response, use session-time and ignore Cisco h323-credit-time;

- *Cisco h323-credit-time priority* — if both parameters (session-time and Cisco h323-credit-time) are present in the server response, use Cisco h323-credit-time and ignore session-time.



SMG gateway may use *Session-Timeout* or *Cisco VSA h323-credit-time* attribute value from Access-Reject packet in order to impose limitation on the maximum duration of an authorized call.

- *Enable emergency call on receiving Reject* — allow calls to emergency services node after Access-Reject reception from the server.

Specifying optional Authentication-Request packet attributes:

- *NAS-Port-Type* — NAS physical port type (server for user authentication), default value is Async;
- *Service-Type* — type of service, not used by default (Not Used);
- *Framed-protocol* — protocol specified for the packet access utilization, not used by default (Not Used);
- *Class* — AV-Pair Class field processing for category change:
 - *Not used* — do not process AV-Pair Class field;
 - *SS7 category* — use value of the received AV-Pair Class field as the caller SS7 category.

RADIUS-Accounting settings

Send requests:

- *accounting-start* — send 'accounting' start packet that notifies RADIUS server on the call start;
- *accounting-stop* — send 'accounting' stop packet that notifies RADIUS server on the call end;
- *accounting-stop* for unsuccessful calls — send information on unsuccessful calls to RADIUS server;
- *accounting-update with period* — send 'update' packet during a call to RADIUS server with the definite period, that notifies RADIUS server on the call active state;
- *accounting for call-origin=originate* — send 'RADIUS-Accounting' messages for incoming connection branch;
- *accounting for call-origin=answer* — send 'RADIUS-Accounting' messages for outgoing connection branch.

You may limit sending billing information in RADIUS on the basis of the modifier mask. Select one or more modifiers in 'Modifiers settings' and select 'Restrict' in the 'Send requests by modifiers' field. In this case, billing information will be sent to RADIUS only if the number complies one of the mask in the modifiers table. The modification will be implemented as usual, according to modifiers table rules.



When 'Send requests by modifiers' is set to 'Restrict', billing information will not be sent for the calls which numbers is not in the modifier mask.

- *Cisco adaptation* — swap originate and answer is accounting messages;
- *Use UTC timezone* — send time in 'RADIUS-Accounting' messages in UTC format;
- *Round duration* — rounding selection for RADIUS-Accounting messages. Three options are available - rounding up, rounding down and not rounding (transmit milliseconds).

Access restriction on server failure. During server fault (response non-reception), you may impose restrictions upon the outgoing communications:

- *no restrictions* — allow all calls.
- *local and zone networks only* — allow calls to emergency services, local and zone network.
- *local network only* — allow calls only to emergency services.
- *deny all* — deny all calls.

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

- *User-name field* — select User-Name attribute value in the corresponding Accounting Request authorization packet (RADIUS-Accounting):
 - *CgPN* — use calling party phone number as a value.
 - *CgPN* — use called party phone number as a value.
 - *IP or E1-stream* — use calling party IP address or incoming connection stream number as a value.
 - *Trunk name* — use incoming connection trunk name as a value.
 - *Original CgPN* — use non-modified phone number of the caller as the value;
 - *Original CdPN* — use non-modified phone number of the callee as the value.
- *Redirection Number* — a mode of RedirPN transmission to RADIUS:
 - *replace Calling-Station-Id* — RedirPN will be transmitted to the Calling-Station-Id field, replacing the existing value;
 - *send as h323-redirect-number* — RedirPN will be transmitted to the h323-redirect-number field separately.
- *CdPN field* — select callee number value used in RADIUS packet generation for specific Attribute-Value pairs (Section 4.1.18.5 Variable description):
 - *CdPN-in* — use callee number prior to modification (number received in SETUP/INVITE request).
 - *CdPN-out* — use callee number after the modification.
- *CgPN field* — select caller number value used in RADIUS packet generation for specific Attribute-Value pairs (section 4.1.18.5 Variable description):
 - *CgPN-in* — use the number of a calling subscriber before modification (the number received in SETUP/INVITE request);
 - *CgPN-out* — use the number of a calling subscriber after modification.

Accordance for RADIUS responses and voice messages

Upon receiving *Reject* message from the RADIUS server, you may enable output of a standard gateway voice message in order to inform the subscriber on the reason for connection refusal. Voice message output is based on the analysis of the replay-Message field or h-323-return-code field of *Reject* message.

- *Accordance table for RADIUS reply and voice messages* — select correspondence table for RADIUS-reject responses and voice messages.
- *RADIUS response attribute* — select an attribute that will be used for RADIUS-reject message analysis.

Eltex-VSA settings

- *Enable Eltex-VSA for call management* — activate Radius call management service (if RCM license is available); for Radius call management service description, see Appendix I. Radius call management service.
- *Full CISCO-VSA fields* — complete attribute name transmission in CISCO-VSA fields.

Transferring "real ip" to RADIUS-Accounting

When receiving an INVITE message in the From field of the real ip parameter, this field is transmitted in Framed-Ip-Address (8) RADIUS-Accounting.




4.1.18.3 RADIUS replies to voice messages mapping

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

RADIUS → RADIUS-replies to voice messages mapping

No	Name
0	Table #0

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

-  — 'Add table'
-  — 'Edit table'
-  — 'Remove table'

RADIUS → RADIUS-replies to voice messages mapping

Table 0		
Name	Table #0	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		
Accordance table		
No	RADIUS reply	Voice message

RADIUS → RADIUS-replies to voice messages mapping →

Accordance	
RADIUS reply	<input type="text"/>
Voice message	trunk is busy (trunk overload, no free c...
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- *RADIUS reply* — replay-Message or h-323-return-code field value of the Reject message received from the RADIUS server;
- *Voice message* — select a voice message that will be output to the subscriber.

4.1.18.4 RADIUS packet format

Each packet description includes descriptions of every Attribute-Value pair for this packet type. Attributes may be either standard attributes or vendor specific attributes (Vendor-Specific Attribute). If the attribute value is unknown for any reason (e.g. if the outgoing trunk is missing, it is impossible to identify CdPN_OUT variable value that is used as a value for some attributes), then this attribute is not included into the message.

For standard attributes, description will be as follows:

Attribute name (Attribute number): Attribute value

For vendor attributes:

Attribute name (Attribute number): Vendor name (Vendor number): VSA name (VSA number): VSA value

where:

Attribute name — always Vendor-Specific;

Attribute number — always 26;

Vendor name — name of the vendor;

Vendor number — vendor number assigned by IANA organization in the “PRIVATE ENTERPRISE NUMBERS” document (<http://www.iana.org/assignments/enterprise-numbers>);

VSA name — vendor attribute name;

VSA number — vendor attribute number;

VS A 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 4.1.18.5 Variable description.

Access-Request packet

User-Name(1): <\$USER_NAME>
 User-Password(2): based on password "eltex" (w/o quotation marks)
 NAS-IP-Address(4): <\$SMG_IP>
 Called-Station-Id(30): <\$CdPN_IN>
 Calling-Station-Id(31): <\$CgPN_IN>
 Acct-Session-Id(44): <\$SESSION_ID>
 NAS-Port(5): <\$NAS_PORT>
 NAS-Port-Type(61): Virtual(5)
 Service-Type(6): Call-Check(10)
 Framed-IP-Address: <\$USER_IP>

Accounting-Request start packet

Acct-Status-Type(40) – Start(1)
 User-Name(1): <\$USER_NAME>
 Called-Station-Id(30): <\$CdPN>
 Calling-Station-Id(31): <\$CgPN_IN>
 Acct-Delay-Time(41): acc. to RFC2866
 Event-Timestamp(55): acc. to RFC2869
 NAS-IP-Address(4): <\$SMG_IP>
 Acct-Session-Id(44): <\$SESSION_ID>
 Framed-IP-Address: <\$USER_IP>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-src-number-in=<\$CgPN_IN>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-src-number-out=<\$CgPN_OUT>

```

Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-dst-number-in=<$CdPN_IN>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-dst-number-
out=<$CdPN_OUT>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-route-
retries=<$ROUTE_RETRIES>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): h323-remote-
id=<$DST_ID>Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): h323-call-
id=<$CALL_ID>
Vendor-Specific(26): Cisco(9): h323-remote-address(23): h323-remote-
address=<$DST_IP>
Vendor-Specific(26): Cisco(9): h323-conf-id(24): h323-conf-id=<$CALL_ID>
Vendor-Specific(26): Cisco(9): h323-setup-time(25): h323-setup-
time=<$TIME_SETUP>
Vendor-Specific(26): Cisco(9): h323-call-origin(26): h323-call-
origin=originate
Vendor-Specific(26): Cisco(9): h323-call-type(27): h323-call-type=<$CALL_TYPE>
Vendor-Specific(26): Cisco(9): h323-connect-time(28): h323-connect-
time=<$TIME_CONNECT>
Vendor-Specific(26): Cisco(9): h323-gw-id(33): h323-gw-id=<$SMG_IP>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Incoming-SIP-call-id(2):
<$inc_SIP_call_ID>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Outgoing-SIP-call-id(3):
<$out_SIP_call_ID>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Incoming-RTP-local-
address(4): <$inc_RTP_loc_IP>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Incoming-RTP-remote-
address(5): <$inc_RTP_rem_IP>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Outgoing-RTP-local-
address(6): <$out_RTP_loc_IP>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Outgoing-RTP-remote-
address(7): <$out_RTP_rem_IP>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): call-record-
file=<$call_record_file_name>

```

Accounting-Request stop packet

```

Acct-Status-Type(40) - Stop(2)
User-Name(1): <$USER_NAME>
Called-Station-Id(30): <$CdPN>
Calling-Station-Id(31): <$CgPN_IN>
Acct-Delay-Time(41): acc. to RFC2866
Event-Timestamp(55): acc. to RFC2869
NAS-IP-Address(4): <$SMG_IP>
Acct-Session-Id(44): <$SESSION_ID>
Acct-Session-Time(46): <$SESSION_TIME>
Framed-IP-Address: <$USER_IP>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-src-number-in=<$CgPN_IN>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-src-number-
out=<$CgPN_OUT>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-dst-number-in=<$CdPN_IN>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-dst-number-
out=<$CdPN_OUT>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-route-
retries=<$ROUTE_RETRIES>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): h323-remote-id=<$DST_ID>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): h323-call-id=<$CALL_ID>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(30): h323-disconnect-
cause=<$DISCONNECT_CAUSE>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-local-disconnect-
cause=<$LOCAL_DISCONNECT_CAUSE>

```

```

Vendor-Specific(26): Cisco(9): h323-remote-address(23): h323-remote-
address=<$DST_IP
Vendor-Specific(26): Cisco(9): h323-conf-id(24): h323-conf-id=<$CALL_ID>
Vendor-Specific(26): Cisco(9): h323-setup-time(25): h323-setup-
time=<$TIME_SETUP>
Vendor-Specific(26): Cisco(9): h323-call-origin(26): h323-call-
origin=originate
Vendor-Specific(26): Cisco(9): h323-call-type(27): h323-call-type=<$CALL_TYPE>
Vendor-Specific(26): Cisco(9): h323-connect-time(28): h323-connect-
time=<$TIME_CONNECT>
Vendor-Specific(26): Cisco(9): h323-disconnect-time(29): h323-disconnect-
time=<$TIME_DISCONNECT>
Vendor-Specific(26): Cisco(9): h323-gw-id(33): h323-gw-id=<$SMG_IP>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Incoming-SIP-call-id(2):
<$inc_SIP_call_ID>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Outgoing-SIP-call-id(3):
<$out_SIP_call_ID>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Incoming-RTP-local-
address(4): <$inc_RTP_loc_IP>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Incoming-RTP-remote-
address(5): <$inc_RTP_rem_IP>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Outgoing-RTP-local-
address(6): <$out_RTP_loc_IP>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Outgoing-RTP-remote-
address(7): <$out_RTP_rem_IP>
Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): call-record-
file=<$call_record_file_name>

```

Access-Accept packet

After the Access-Accept packet is received from the RADIUS server, the call is considered as authorized. Next, the search for an outgoing trunk will be performed and if successful, an attempt to establish the connection will be made.

If *Session-Time (27)* attribute or *Cisco VSA (9) h323-credit-time (102)* attribute has been transferred in a packet, and the corresponding setting was specified in the RADIUS profile, attribute value will be used for the maximum call duration limitation. When this timeout expires, the connection will be terminated by SMG.

4.1.18.5 Variable description

Table 29 — Variable description

Variable	Description and possible values
\$CALL_TYPE	Defined on the basis of the transmission medium that the outgoing trunk belongs to: <ul style="list-style-type: none"> 'Telephony', if the outgoing trunk is PSTN (TDM) 'VoIP', if the outgoing trunk is VoIP
\$CdPN	Determined from SMG settings <ul style="list-style-type: none"> \$CdPN = \$CdPN_IN [by default] \$CdPN = \$CdPN_OUT
\$CdPN_IN	Callee number before modification (received in SETUP/INVITE)
\$CdPN_OUT	Callee number after modification (sent to the called party in SETUP/INVITE)
\$CgPN_IN	Caller number before modification (received in SETUP/INVITE)
\$CgPN_OUT	Caller number after modification (sent to the called party in SETUP/INVITE)

\$DISCONNECT_CAUSE	Q.850 reason for call clearing
\$DST_ID	Outgoing trunk name for this call
\$DST_IP (string)	IP address of the terminating device when if the outgoing trunk is VoIP, e.g.: 192.168.0.1
\$USER_IP	IP address of the device initiated the call if the ingress trunk is VoIP or SIP subscriber
\$LOCAL_DISCONNECT_CAUSE	Local reason for call clearing; values: <ul style="list-style-type: none"> • 1 — connection to the callee has been established (User-Answer) • 2 — wrong or incomplete number format (Incomplete-Number) • 3 — number does not exist (Unassigned-Number) • 4 — unsuccessful connection attempt, unknown reason (Unsuccessful-Other-Cause) • 5 — callee is busy (User-Busy) • 6 — equipment fault (Out-of-Order) • 7 — no response from the callee (No-Answer) • 8 — outgoing trunk is unavailable (Unavailable-Trunk) • 9 — RADIUS server authorization denied (Access-Denied) • 10 — no free channels for connection establishment (Unavailable-Voice-Channel) • 11 — RADIUS server is unavailable (RADIUS-Server-Unavailable)
\$NAS_PORT	(xport.type<<24) + (xport.slot<<16) + (xport.stream<<8) + (xport.cell)
\$ROUTE_RETRIES	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: <ul style="list-style-type: none"> • <\$CgPN_IN>; • source IP address or E1 stream number [by default] • incoming trunk name
<\$inc_SIP_call_ID>	SIP message Call-ID field value for the incoming connection branch.
<\$out_SIP_call_ID>	SIP message Call-ID field value for the outgoing connection branch.
<\$inc_RTP_loc_IP>	Local IP address of the device for the incoming connection branch RTP session establishment.
<\$inc_RTP_rem_IP>	Remote IP address of the communicating device for the incoming connection branch RTP session establishment.
<\$out_RTP_loc_IP>	Local IP address of the device for the outgoing connection branch RTP session establishment.

<\$out_RTP_rem_IP>	Remote IP address of the communicating device for the outgoing connection branch RTP session establishment.
<\$call_record_file_name>	Conversation record file name. For instance: call_records/2016-12-13-0000/2016-12-13_12-41-45_20000-10000.wav

4.1.18.6 Authorization calls



The functionality is available only with a license, more details in the Licenses section.

The function is used to initiate a call via RADIUS Change-of-Authorization (CoA) request (described in RFC 5176 standard). Used for authorization services for connecting to public networks callback access. The user connects to the network and gets to the web portal, where an access password is requested and you are prompted to enter a password for authorization. After entering the number, the user receives a call on his phone. The caller's number displayed to the user or part of it serves as a password for access to a public access network, which should be entered on the web portal.

To initiate a call, the web portal must send a CoA-Request RADIUS packet to the SMG via the RADIUS protocol, containing the Called-Station-Id attribute with the user's phone number. Example of a CoA-Request:

```
RADIUS Protocol
Code: CoA-Request (43)
Packet identifier: 0xa0 (160)
Length: 33
Authenticator: ac02dd52e3435a2fa46ed7cd2f7f177d
Attribute Value Pairs
  AVP: l=13 t=Called-Station-Id(30): 70123456789
      Type: 30
      Length: 13
      Called-Station-Id: 70123456789
```

In case the number can be called, SMG selects the calling number from the specified pool numbers and sends it in the CoA-ACK response in the Calling-Station-Id attribute. After this, SMG initiates a call from the selected number to the user number. Regardless of the results of the call (reset call, user answer or call end due to no answer timeout), SMG sends information about the completed call in RADIUS Accounting requests. When the user answers, the call will be immediately reset. Example of CoA-ACK response:

```
RADIUS Protocol
Code: CoA-ACK (44)
Packet identifier: 0xa0 (160)
Length: 33
Authenticator: 60363e5d4f742df10316cc05b81a42f6
Attribute Value Pairs
  AVP: l=13 t=Calling-Station-Id(31): 73830019698
      Type: 31
      Length: 13
      Calling-Station-Id: 73830019698
```

In case the number specified by the user cannot be called, SMG will respond with a CoA-NAK message without any attributes and will not initiate a call.


If the CoA-Request came from a RADIUS server that is not linked to the selected RADIUS profile or to a network interface that does not correspond to the selected server, SMG will ignore such a request.

The call is made from a virtual number. Call routing is carried out on a general basis through a numbering plan linked to a virtual number.

Authorization calls

User settings	
PBX profile	not set
RADIUS profile	
Dial plan	[0] NumberPlan#0
Access category	[0] AccessCat#0
Calling party category (RUS)	1
Select mode	sequential

Number pools:

No	First number	Range	
			

Apply Cancel

Virtual number parameters

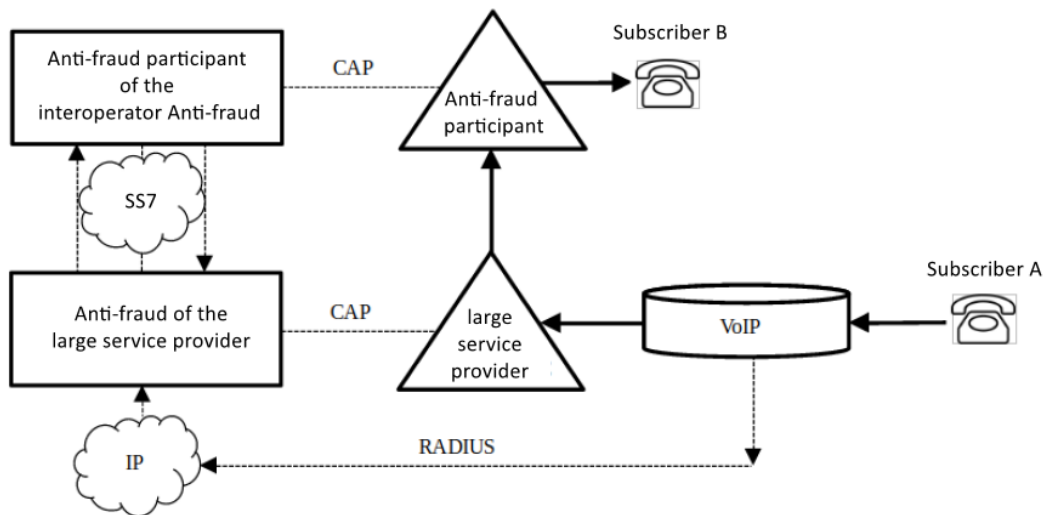
- *PBX profile* – PBX-profile binding;
- *RADIUS profile* – RADIUS profile that will be used to send Accounting requests. RADIUS CoA requests can be accepted from servers associated with this profile;
- *Dial plan* – binding a numbering plan for call routing;
- *Access category* – select an access category;
- *Calling party category* – select the Caller ID category;
- *Select mode* – method of selecting numbers from those specified in the pool of numbers:
 - *random* – numbers will be selected in random order;
 - *sequential* – numbers will be selected in order.
- *Number pools* – pools of numbers from which calls will be made. To organize a pool, you should specify the starting number and range of numbers in the pool. A total of 64 can be set pool.

4.1.18.7 Interaction with verification nodes of IS Antifraud



The functionality is available only with a license, more details in the Licenses section.

The SMG-1016M, SMG2016 and SMG3016 gateways implement functions for connecting to the verification node IS "Antifraud" using the RADIUS protocol. A schematic representation of a RADIUS connection is shown in the picture below. The verification task includes processing two events: registration in the system of outgoing calls and checking the validity of incoming calls.



4.1.18.7.1 Configuration

As a part of the RADIUS connection, it is necessary to perform the following steps in order to generate information about incoming and outgoing calls and to further transmit corresponding requests to the RADIUS server of the IS Anti-fraud verification node.

1. Go to the 'RADIUS' — 'Servers'. In the 'Anti-fraud servers' specify IP address, port, password and server group to which verification requests will be sent;
2. In the same section, select the required operating mode if the installed license involves working in several modes:
 - *OFF* – interaction with the control unit is disabled;
 - *Astarta* – interaction with the iBase-Antifraud verification node produced by Astarta LLC. In this mode, the username and password will be added to the attributes of requests to the verification node, entered in the fields below (for Access-Request User-Name and Password, only User-Name for Accounting-Request:

Anti-fraud parameters

Mode **Astarta**

User

Password

- *Intek* – interaction with the verification node, produced by Hexagon Labs LLC;
- *Custom* – interaction with verification nodes from other manufacturers. When using this mode, the contents of requests to the Anti-fraud verification nodes are configured with the following parameters, located in the Authorization section of the RADIUS profile: *User-name (originate)*, *User-name (answer)*, *Redirecting Number*, *User-password*, option 'Individual

passwords for SIP-subscribers, NAS-Port-Type, Service-Type, Framed-protocol', as well as the parameter 'Full CISCO-VSA fields' in the VSA Settings section;

3. Create a profile in the 'RADIUS' – 'List of Profiles' section, specify the group, activate the option 'Enable anti-fraud mode' and, if necessary, configure modification parameters. For Custom mode, you need to configure the fields listed in step 2.



Changing the Authorization and Accounting parameters is not available in Astarta and Intek modes.

RADIUS rule 0	
Name	RADIUS_Profile00
Enable RADIUS-Authorization	<input type="checkbox"/>
Enable RADIUS-Accounting	<input type="checkbox"/>
Send SNMP trap	<input type="checkbox"/>
Group	0
Enable anti-fraud mode	<input type="checkbox"/>
Modifiers settings	
Modifiers for InCdPN	not used
InCdPN	original
Modifiers for InCgPN	not used
InCgPN	original
Modifiers for Redirecting	not used
Modifiers for OutCdPN	not used
Modifiers for OutCgPN	not used

4. In the parameters of the trunk group for which verification for incoming calls will take place in the Antifraud IS, in the 'Basic settings' tab, select the RADIUS profile for Antifraud created in the previous step:

TrunkGroups	
Basic settings Incoming calls Outgoing calls	
TrunkGroup 3	
Title	Incoming
Description	
TrunkGroup members	[0] Stream 0 (Q.931-U)
Local direction	<input type="checkbox"/>
Play music on hold (MOH)	<input type="checkbox"/>
Voice switch delay	0
Anti-fraud RADIUS profile	[1] RADIUS_Profile01
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

In case there is a need to register transit transit incoming calls to the trunk group, just activate the 'Local direction' option.

5. In the parameters of the SIP profile for which registration will occur in the Antifraud IS of outgoing calls, in the 'SIP Interface Settings' tab, select the appropriate RADIUS-profile in the 'RADIUS profile for antifraud' field:

SIP interfaces	
SIP interface settings	SIP protocol settings
	Codecs/RTP settings
	Fax/Modem settings
	Extended SIP settings
Index [0]	
Title	UAC
Mode	SIP profile
Ingress RADIUS profile	not set
Egress RADIUS profile	not set
Anti-fraud RADIUS profile	[1] RADIUS_Profile01



For outgoing calls, if both on the first and second call legs Anti-fraud RADIUS is selected (for SIP profile and trunk group, respectively), then corresponding settings of the second leg are used. Also, if there are no settings on the first leg, the settings of the second leg are used.

4.1.18.7.2 Request format

- Transmission of information about an outgoing call is carried out by sending from the communication center an Access-Request RADIUS message with the following fields:

Access-Request Packet

User-Name(1): user name, specified in step 2 (for Astarta mode only)
User-Password(2): password, specified in step 2 (for Astarta mode only)
Called-Station-Id(30): <\$CdPN_IN>
Calling-Station-Id(31): <\$CgPN_IN>
Acct-Session-Id(44): <\$SESSION_ID>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-request-type=save_call
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-termination-gateway-ip=\$SMG_IP

- Call verification is ensured by sending from the communication node an Access-Request RADIUS message with the following fields:

Access-Request Packet

User-Name(1): user name, specified in step 2 (for Astarta mode only)
User-Password(2): password, specified in step 2 (for Astarta mode only)
Called-Station-Id(30): <\$CdPN_IN>
Calling-Station-Id(31): <\$CgPN_IN>
Acct-Session-Id(44): <\$SESSION_ID>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-request-type=check_call
Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-termination-gateway-ip=\$SMG_IP

- Ensuring control of call duration and reasons for disconnecting unsuccessful calls carried out by sending from the communication node an Accounting-Request RADIUS message with the following fields:

Accounting-Request Packet

User-Name(1): user name, specified in step 2 (for Astarta mode only)
Called-Station-Id(30): <\$CdPN>
Calling-Station-Id(31): <\$CgPN_IN>
Acct-Delay-Time(41): according to RFC2866
Event-Timestamp(55): according to RFC2869
Acct-Session-Id(44): <\$SESSION_ID>
Acct-Session-Time(46): <\$SESSION_TIME>
Vendor-Specific(26): Cisco(9): Cisco-AVPair(30): h323-disconnect-cause=<\$DISCONNECT_CAUSE>
Vendor-Specific(26): Cisco(9): h323-setup-time(25): h323-setup-time=<\$TIME_SETUP>
Vendor-Specific(26): Cisco(9): h323-connect-time(28): h323-connect-time=<\$TIME_CONNECT>
Vendor-Specific(26): Cisco(9): h323-disconnect-time(29): h323-disconnecttime=<\$TIME_DISCONNECT>

4.1.18.7.3 Response format

As confirmation for receipt of transmitted information about an outgoing call, as well as packets account, a RADIUS Access-Accept message is expected. Regardless of the response and in case of its absence, the call will be completed, since the response to the call registration request is informational and does not affect the progress of the call.

An Access-Accept RADIUS message is expected as confirmation of successful call verification, optionally with additional fields. When an Access-Accept response is received, the call will be continued. If call verification fails, a RADIUS Access-Reject message is expected with additional fields that uniquely identify the error. When receiving Access-Reject the call will be disconnected.

4.1.19 Traces

4.1.19.1 PCAP traces

Traces → PCAP traces

PCAP traces

TCP-dump

Interface: eth0

Capture length limit (0 - no limit): 0

Add filter:

PCM-dump

E1 streams	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Signaling	0.931 U	.	557	557	557	557	557	557	557	557	557	557	557	557	557	557

Port mirroring

	CPU port	GE port 0	GE port 1	GE port 2	SFP port 0	SFP port 1
Source ports for ingress packets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Source ports for egress packets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Destination port for ingress packets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Destination port for egress packets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

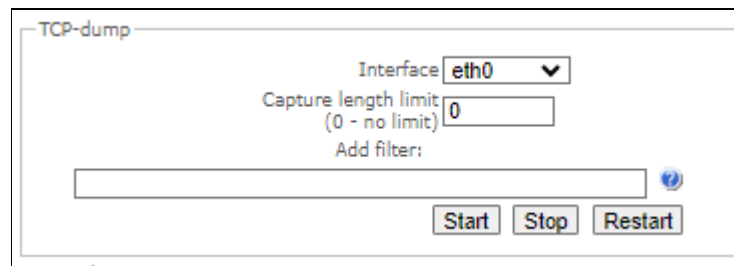
Available 64MB from 64MB

Files and folders			
<input type="checkbox"/>	app_log_20240130_115100.log	2.2 kB	30.01.2024 11:53
<input type="checkbox"/>	chronica.1	0 B	30.01.2024 11:51
<input type="checkbox"/>	chronica.idx	18 B	30.01.2024 11:51
<input type="checkbox"/>	chronica.siz	13 B	30.01.2024 11:51
<input type="checkbox"/>	dmesg	15.4 kB	30.01.2024 11:51
<input type="checkbox"/>	dynamic_firewall.1.log	0 B	08.08.2023 14:42
<input type="checkbox"/>	hosttest.log	91 B	30.01.2024 11:51
<input type="checkbox"/>	lastlog	0 B	01.01.1970 08:00
<input type="checkbox"/>	networkd.1.log	67.3 kB	06.02.2024 17:27
<input type="checkbox"/>	pa_h323.1.log	1.5 kB	31.01.2024 15:50
<input type="checkbox"/>	pbx_sip_bun.log	0 B	30.01.2024 11:51
<input type="checkbox"/>	pbx_sorm_extractor.log	0 B	30.01.2024 11:51
<input type="checkbox"/>	rec.log	787 B	07.02.2024 08:33
<input type="checkbox"/>	smg_logs_dump.tar.gz	122 B	30.01.2024 11:51
<input type="checkbox"/>	snmpd	968 B	30.01.2024 11:51
<input type="checkbox"/>	sorm_extractor.1.log	963 B	30.01.2024 11:51
<input type="checkbox"/>	sorm_extractor_consol_20240130_115101.log	43 B	30.01.2024 11:51
<input type="checkbox"/>	ssh_log0	0 B	30.01.2024 11:51
<input type="checkbox"/>	ssh_log3	0 B	30.01.2024 11:51
<input type="checkbox"/>	sshd_log	1.2 kB	06.02.2024 15:46
<input type="checkbox"/>	sysmon.1.log	1.2 kB	30.01.2024 11:51
<input type="checkbox"/>	uauthlog	0 B	30.01.2024 11:50
<input type="checkbox"/>	voice_mail.log	48.3 kB	07.02.2024 08:23

TCPdump – settings of the TCP-dump utility:

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

Traces → PCAP traces



- *Interface* – an interface for network traffic pickup;
- *Capture length limit (0 – no limit)* – size limit for picked-up packets, bytes (0 — no restrictions);
- *Add filter* – packet filter for the *tcpdump* utility.

Structure of Filter Expressions

Every expression defining a filter includes a single or multiple primitives, which contain a single or multiple object identifiers and preceding qualifiers. An object identifier may be represented by its name or number.

Object Qualifiers:

- 1) **type** – indicates the object type specified by the identifier. An object type may have the following values:
host,
net,
port.
 If an object type is not defined, the host value is assumed.

- 2) **dir** – defines the direction towards the object. This may have the following values:
src (object is a source),
dst (object is a destination),
src or dst (source or destination),
src and dst (source and destination).

If the dir qualifier is not defined, the src or dst value is assumed.

To pick up traffic from the any artificial interface, the inbound and outbound qualifiers can be used.

- 3) **proto** – defines the protocol to which the packets should belong. This qualifier may have the following values:
ether, fddi1, tr2, wlan3, ip, ip6, arp, rarp, decnet, tcp, and udp.
 If a primitive does not contain a protocol qualifier, it is assumed that all protocols compatible with the object type comply with this filter.

In addition to objects and qualifiers, primitives may contain arithmetic expressions and keywords:

gateway,
broadcast,
less,
greater.

Complex filters may contain a set of primitives connected with logical operators **and**, **or**, and **not**. To reduce the expressions which define filters, lists of identical qualifiers may be omitted.

Filter Examples

- dst foo** – filters the packets which IPv4/v6 recipient address field contains address of the foo host;
- src net 128.3.0.0/16** – filters all Ipv4/v6 packets sent from the specified network;
- ether broadcast** – ensures filtering of all Ethernet broadcasting frames. The *ether* keyword may be omitted;
- ip6 multicast** – filters packets with IPv6 group addresses.

For detailed information on packet filtering, see specialized resources.

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

The SMG-1016M equipment has a feature for removing PCAP traces (TCP dump). If you remove traffic from a specific interface (for example, eth0.129), then the resulting dump will not contain outgoing RTP stream. To capture both streams (incoming and outgoing), removing should be done on ANY interface for SMG-1016M and bond1 interface for SMG-2016/3016.

PCM-dump – settings of the PCM-dump utility

PCM-dump is a utility that allows one to pick up and analyze signaling traffic on E1 streams. The device has the ability to remove PCM dump from one stream or from several ones. When removing a PCM dump from several streams at the same time, the trace is written to one file, in which signaling messages from several streams are recorded, while simultaneously removing PCM-dump from streams with different signaling protocols is not possible.

Tracing → PCAP traces

PCM-dump		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
E1 streams																	
Select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Signaling	Q.931-U	.	SS7	SS7	SS7	SS7	SS7	SS7	SS7	SS7	SS7	SS7	SS7	SS7	SS7	SS7	SS7

- *Select* – select E1 stream;
- *Signaling* – signaling protocol, selected on the stream:
 - SS7;
 - Q.931-N;
 - Q.931-U;
 - V5.2.
- *Start* – start data collection;
- *Stop* – finish data collection;
- *Restart* – restart the utility and start collecting data again.

Port mirroring – traffic mirroring settings



Only for SMG-1016M.

Port mirroring allows one to copy from the gateway switch ports received and transmitted frames and route them to another port.

Traces → PCAP traces

Port mirroring

	CPU port	GE port 0	GE port 1	GE port 2	SFP port 0	SFP port 1
Source ports for ingress packets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Source ports for egress packets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Destination port for ingress packets		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Destination port for egress packets		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

The following actions are possible for device ports:

- *Source ports of ingress packets* – copy frames received from this port (port-source);
- *Source ports of egress packets* – copy frames transmitted by this port (port-source);
- *Destination port for ingress packets* – destination port for copied frames received by selected source ports;
- *Destination port for egress packets* – destination port for copied frames, transmitted by selected source ports.

Buttons:

- *Apply* – apply mirroring settings;
- *Confirm* – confirm the applied mirroring settings;
- *Clear* – reset mirroring settings;
- *Save* – save mirroring settings.



If within one minute the settings are not confirmed by pressing the 'Confirm' button, then they return to the previous values.

Tracing Directory Files and Folders block contains a list of tracing files.

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

4.1.19.2 PBX traces

'Basic traces' tab



Using IP PBX tracing causes delays in device operation. This debugging type is recommended to be used only if problems arise in the operation of the gateway to identify their causes.

Traces → PBX traces → Basic traces

PBX traces
Basic traces
Advanced traces
By TrunkGroup
By telephone number

Attention!

Enabling logs can affect system performance!

TRACES START

PBX-PSTN enable

PBX SIP enable

PCAP enable

*The log package will be downloaded automatically after stopped

Available 64MB from 64MB

Files and folders			
	app_log_20240130_115100.log	2.2 kB	30.01.2024 11:53
	chronica.1	0 B	30.01.2024 11:51
	chronica.idx	18 B	30.01.2024 11:51
	chronica.siz	13 B	30.01.2024 11:51
	dmesg	15.4 kB	30.01.2024 11:51
	dynamic_firewall.1.log	0 B	08.08.2023 14:42
	hosttest.log	91 B	30.01.2024 11:51
	lastlog	0 B	01.01.1970 08:00
	networkd.1.log	67.3 kB	06.02.2024 17:27
	pa_h323.1.log	1.5 kB	31.01.2024 15:50
	pbx_sip_bun.log	0 B	30.01.2024 11:51
	pbx_sorm_extractor.log	0 B	30.01.2024 11:51
	rec.log	787 B	07.02.2024 09:13
	smg_logs_dump.tar.gz	122 B	30.01.2024 11:51
	snmpd	968 B	30.01.2024 11:51
	sorm_extractor.1.log	963 B	30.01.2024 11:51
	sorm_extractor_consol_20240130_115101.log	43 B	30.01.2024 11:51
	ssh_log0	0 B	30.01.2024 11:51
	ssh_log3	0 B	30.01.2024 11:51
	sshd_log	1.2 kB	06.02.2024 15:46
	sysmon.1.log	1.2 kB	30.01.2024 11:51
	uauthlog	0 B	30.01.2024 11:50
	voice_mail.log	48.3 kB	07.02.2024 09:13

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

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

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

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

SMG Digital Gateway

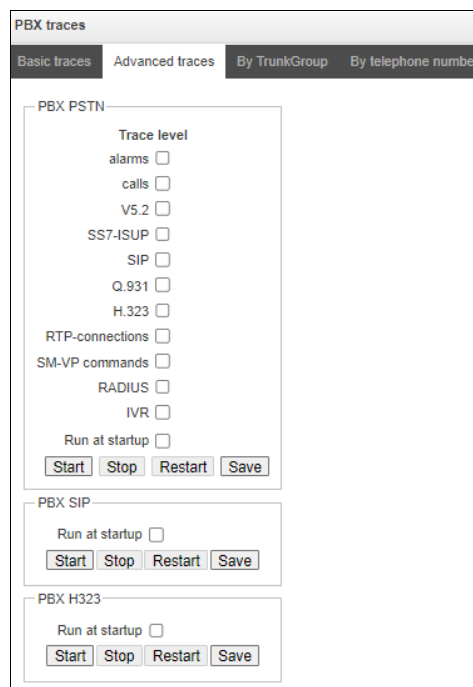
311

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

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

'Advanced traces' tab

Traces → PBX traces → Advanced traces



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

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

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

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

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

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

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

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

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

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



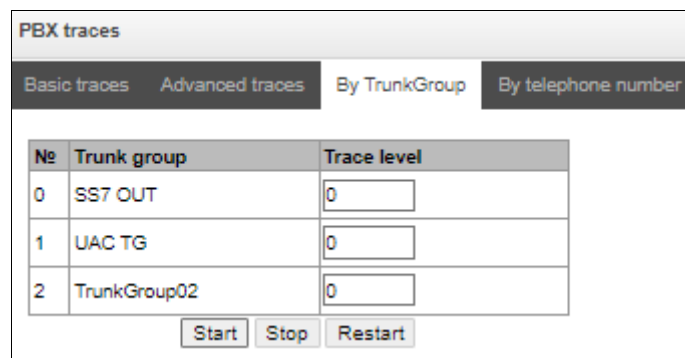
After stopping data collection, buttons will appear allowing one to download trace files to a local computer.

In the *'Tracing Directory Files and Folders'* block, one can download a set of recorded tracing files.

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

'By Trunk Group' tab

Traces → PBX traces → By TrunkGroup



№	Trunk group	Trace level
0	SS7 OUT	0
1	UAC TG	0
2	TrunkGroup02	0

Start Stop Restart

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

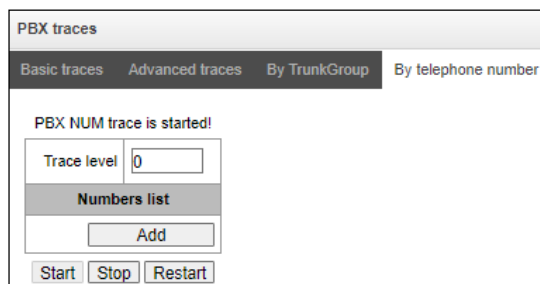
To start the data collection, it is necessary to set non-zero tracing level for required trunk groups, and then click the *'Start'* button.

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

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

'By telephone number' tab

Traces → PBX traces → By telephone number



The screenshot shows a web interface titled "PBX traces". At the top, there are four tabs: "Basic traces", "Advanced traces", "By TrunkGroup", and "By telephone number". The "By telephone number" tab is selected. Below the tabs, a message reads "PBX NUM trace is started!". Underneath, there is a "Trace level" label followed by a text input field containing the number "0". Below that is a section titled "Numbers list" with an "Add" button. At the bottom of the interface, there are three buttons: "Start", "Stop", and "Restart".

Use the menu to start PBX PSTN log collecting on selected phone number. Collection is performed by CdPN as well as CgPN. Tracing levels work similar to PBX PSTN tracing levels (see '*Basic settings*' tab) and differ only by the fact that all protocols have the same specified logging level.

To start data collecting, add phone number in the phone number list, set tracing level, and then click '*Start*' button.

To stop data collecting, click '*Stop*' button. Also, when tracing, you can change the settings and restart data collecting by clicking '*Restart*' button.

4.1.19.3 Syslog settings

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

SYSLOG is a protocol, designed for transmission of messages on current system events. Gateway software generates system data logs on operation of system applications and signaling protocols, as well as occurred failures and sends them to SYSLOG server.



High debug levels may cause delays in operation of the device.
IT IS NOT RECOMMENDED to use system log unnecessarily.

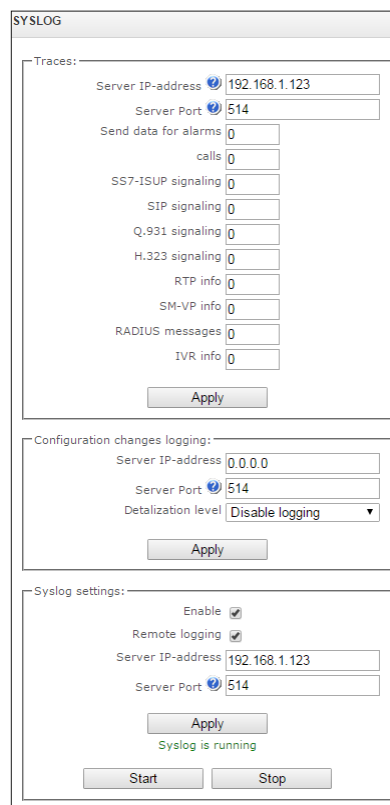


System log should be used only when problems in gateway operation occur, and you have to identify the reason. To define the necessary debug levels, consult an Eltex Service Centre specialists.

Tracings — allows to save the log of device components operation and interaction, as well as message exchange via various protocols.

In tracing parameters, you may configure tracing level for various events and protocols. Possible levels are as follows: 0 — disabled, 1–99 — enabled. 1 — minimum debug level, 99 — maximum debug level.

Traces → SYSLOG



The screenshot shows the 'SYSLOG' configuration window with the following details:

- Traces:**
 - Server IP-address: 192.168.1.123
 - Server Port: 514
 - Send data for alarms: 0
 - calls: 0
 - SS7-ISUP signaling: 0
 - SIP signaling: 0
 - Q.931 signaling: 0
 - H.323 signaling: 0
 - RTP info: 0
 - SM-VP info: 0
 - RADIUS messages: 0
 - IVR info: 0
- Configuration changes logging:**
 - Server IP-address: 0.0.0.0
 - Server Port: 514
 - Detailization level: Disable logging
- Syslog settings:**
 - Enable:
 - Remote logging:
 - Server IP-address: 192.168.1.123
 - Server Port: 514

Buttons: 'Apply' (under Traces), 'Apply' (under Configuration changes logging), 'Apply' (under Syslog settings), 'Start', and 'Stop'.

- *Server IP address* — server address that the tracing will be sent to;
- *Server port* — server port that the tracing will be sent to.

Configuration changes logging — allows to save the history of the gateway setting changes.

- *Server IP-address* — server address that the entered commands log will be sent to;
- *Server port* — server port that the entered commands log will be sent to;
- *Detalization level* — verbosity level of the entered commands log:
 - *Disable logging* — disable entered commands logs generation;
 - *Standard* — messages contain the name of modified parameter;
 - *Extended* — messages contain the name of modified parameter as well as parameter values before and after the modification.

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

- *Enable* — when checked, device access event history will be saved; when unchecked, logging will be disabled;
- *Remote logging* — when checked, system log will be saved on server located at the specified address;
- *Server IP-address* — address of a server for system log storage;
- *Server port* — server port that the system log will be sent to.

4.1.20 Network switch (for SMG-1016M only)

In 'Network switch' menu, you may configure switch ports.

4.1.20.1 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.

Network switch → LACP settings

No	Group description	Enable	Mode	Primary	Updelay	Mimon	Lacp rate
0	LACP trunk 0	+	Active-backup	None	100	100	slow

Apply Confirm Add Edit Delete Save

To create, edit or remove LACP groups, use the following buttons: *Add, Edit, Remove, Apply*.

New LACP	
Group description	LACP trunk 0
Enable	<input type="checkbox"/>
Mode	active-backup
Primary	none
Updelay	100
Miimon	100
LACP rate	slow
Combine interfaces in PortChannel	
GE port 0	
GE port 1	
GE port 2	
CPU port	
SFP port 0	
SFP port 1	
<input type="button" value="Cancel"/> <input type="button" value="Default"/> <input type="button" value="Save"/>	

- *Group description* — LACP group name.
- *Enable* — when checked, LACP will be enabled.
- *Mode* — LACP operation mode:
 - *active-backup* — one interface operates in active mode, while others in standby mode. If an active interface goes out of service, the control will be transferred to one of the standby interfaces. This function doesn't have to be supported by the switch.
 - *balance-xor* — packet transfer is distributed between the aggregated interfaces by the following equation: ((source MAC address) XOR (recipient MAC addresses)) % number of interfaces. A certain interface operates with a specific recipient. This mode allows to balance the load and increase the robustness.
 - *802.3ad* — dynamic port aggregation. This mode enables significant boost of the incoming and outgoing traffic bandwidth through utilization of every single aggregated interface. This function must be supported by the switch, and in some cases it requires an additional switch setting.
- *Primary* — primary interface configuration.
- *Updelay* — interface change time when the primary interface becomes unavailable.
- *Miimon* — MII monitoring time, frequency in milliseconds.
- *LACP rate* — time interval for transmission of LACPDU packets.
 - *fast* — 1 second transmission interval;
 - *slow* — 30 seconds transmission interval.
- *Combine interfaces in PortChannel* — list of ports added to LACP group.

4.1.20.2 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.

Network switch → Ports settings

Ports settings						
	GE port 0	GE port 1	GE port 2	CPU port	SFP port 0	SFP port 1
Enable VLAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Default VLAN ID	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
VID Override	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Egress	<input type="text" value="Unmodified"/>	<input type="text" value="Unmodified"/>	<input type="text" value="Unmodified"/>	<input type="text" value="Unmodified"/>	<input type="text" value="Unmodified"/>	<input type="text" value="Unmodified"/>
IEEE mode	<input type="text" value="Fallback"/>	<input type="text" value="Fallback"/>	<input type="text" value="Fallback"/>	<input type="text" value="Fallback"/>	<input type="text" value="Fallback"/>	<input type="text" value="Fallback"/>
Output	<input type="checkbox"/> GE port 1 <input type="checkbox"/> GE port 2 <input checked="" type="checkbox"/> CPU port <input type="checkbox"/> SFP port 0 <input type="checkbox"/> SFP port 1	<input type="checkbox"/> GE port 0 <input type="checkbox"/> GE port 2 <input checked="" type="checkbox"/> CPU port <input type="checkbox"/> SFP port 0 <input type="checkbox"/> SFP port 1	<input type="checkbox"/> GE port 0 <input type="checkbox"/> GE port 1 <input checked="" type="checkbox"/> CPU port <input type="checkbox"/> SFP port 0 <input type="checkbox"/> SFP port 1	<input checked="" type="checkbox"/> GE port 0 <input checked="" type="checkbox"/> GE port 1 <input checked="" type="checkbox"/> GE port 2 <input checked="" type="checkbox"/> SFP port 0 <input checked="" type="checkbox"/> SFP port 1	<input type="checkbox"/> GE port 0 <input type="checkbox"/> GE port 1 <input type="checkbox"/> GE port 2 <input checked="" type="checkbox"/> CPU port <input type="checkbox"/> SFP port 1	<input type="checkbox"/> GE port 0 <input type="checkbox"/> GE port 1 <input type="checkbox"/> GE port 2 <input checked="" type="checkbox"/> CPU port <input type="checkbox"/> SFP port 0
LACP trunk	<input type="text" value="none"/>	<input type="text" value="none"/>	<input type="text" value="none"/>		<input type="text" value="none"/>	<input type="text" value="none"/>
Port MAC (xxxxxxxxxxxx)	<input type="text" value="A8:F9:4B:88:70:A6"/>	<input type="text" value="A8:F9:4B:88:70:A6"/>	<input type="text" value="A8:F9:4B:88:70:A6"/>		<input type="text" value="A8:F9:4B:88:70:A6"/>	<input type="text" value="A8:F9:4B:88:70:A6"/>
Reserve port	<input type="text" value="none"/>	<input type="text" value="none"/>	<input type="text" value="none"/>		<input type="text" value="none"/>	<input type="text" value="none"/>
Preemption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Port mode	<input type="text" value="auto"/>	<input type="text" value="auto"/>	<input type="text" value="auto"/>			



In factory configuration, switch ports may not access each other.

Device switch is equipped with 3 x (for SMG-1016M) or 4 x (for SMG-2016 and SMG-3016) of electrical Ethernet ports, 2 x optical ports and 1 x port for CPU interactions:

- **GE port** — electrical Ethernet ports of the device.
- **SFP port** — optical Ethernet ports of the device.
- **CPU** — internal port linked to the device CPU.

Switch Settings

- *Enable VLAN* — when checked, enable 'Default VLAN ID', 'Override' and 'Egress' settings for this port;
- *Default VLAN ID* — when an untagged packet is received at the port, this will be its VID; when a tagged packet is received at that port, its VID is considered to be specified in its VLAN tag;
- *VID override* — when checked, it is considered that any received packet has a VID, defined in 'default VLAN ID' row. True for both untagged and tagged packets;
- *Egress:*
 - *unmodified* — packets will be sent by the port without any changes (i.e. as they came to another switch port);
 - *untagged* — packets will always be sent without VLAN tag by this port;
 - *tagged* — packets will always be sent with VLAN tag by this port;
 - *double tag* — each packet will be sent with two VLAN tags — if received packet was tagged and sent with one VLAN tag — if the received packet was untagged.
- *IEEE mode* — sets security mode for received tagged frames processing:
 - *fallback* — frame is received on ingress port regardless whether it has 802.1q tag in '802.1q' routing table or not:
 - If there is no 802.1q tag in '802.1q' routing table and the frame is allowed in 'output' section, the frame will be transmitted to the egress port;
 - Also, the frame will be transmitted to the egress port, if there is 802.1q tag in '802.1q' routing table, the egress port is a member of VLAN included in '802.1q' routing table and the frame is allowed in 'output' section.
 - *check* — the frame will be received on ingress port, if its 802.1q tag is kept in '802.1q' routing table (the ingress port is not necessary to be a member of VLAN in '802.1q' routing table):
 - The frame will be transmitted to an egress port if the egress port is a member of VLAN in '802.1q' routing table and allowed in 'output' section of the ingress port settings.
 - *secure* — the frame will be received on ingress port, if its 802.1q tag is kept in '802.1q' routing table and the ingress port is a member of VLAN in '802.1q' routing table.
 - The frame will be transmitted to an egress port if the egress port is a member of VLAN in '802.1q' routing table and allowed in 'output' section of the ingress port settings.
- *Output* — mutual availability of data ports. Defines privileges that allow packets received by this port to be transferred to flagged ports;
- *LACP trunk* — select LACP group to which the defined port will belong;
- *Port MAC* — change a MAC address of the port. The option is available when LACP group is selected on the port. Ports which are in the one LACP group should have different MAC addresses;
- *Reserve port* — select the port that will receive the traffic when abnormal situation occurs (i.e. line interruption). This setting is required for provisioning of Dual Homing redundancy;
- *Preemption* — when checked, return to master port when it becomes available.



This firmware version supports the global dual homing only.

- *Port mode* — select port operation mode (auto, 10/100 Mbps Half, 10/100 Mbps Full, 1 Gbps). Mode configuration is possible for electric Ethernet ports only (*GE port 0*, *GE port 1*, *GE port 2*).



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

To apply settings, click '*Apply*' button; to confirm applied settings, click '*Confirm*' button.

Click '*Defaults*' button to set default parameters. (The figure shows default values.)

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

4.1.20.3 802.1q

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.

Network switch → 802.1q

VID	GE port 0	GE port 1	GE port 2	CPU port	SFP port 0	SFP port 1	Override	Priority	
<input type="text"/>	unmodified ▼	unmodified ▼	unmodified ▼	unmodified ▼	unmodified ▼	unmodified ▼	<input type="checkbox"/>	0 ▼	
<input type="button" value="Add"/>									
VTU table									
VID	GE port 0	GE port 1	GE port 2	CPU port	SFP port 0	SFP port 1	Override	Priority	Delete
VTU table is empty!									
<input type="button" value="Apply"/>			<input type="button" value="Confirm"/>			<input type="button" value="Delete"/>		<input type="button" value="Save"/>	

Adding records to the packet routing table

- *VID* — enter an identifier of VLAN group, that the routing rule is created for, and assign actions for each port to be performed during transfer of packets with specified VID.
 - *unmodified* — packets will be sent by the port without any changes (i.e. as they have been received);
 - *untagged* — packets will always be sent without VLAN tag by this port;
 - *tagged* — packets will always be sent with VLAN tag by this port;
 - *not member* — packets with specified VID will not be sent by this port, i.e. the port is not the member of VLAN.
- *override* — when checked, override 802.1p priority for this VLAN; otherwise, leave the priority unchanged;
- *priority* — 802.1p priority assigned to packets in this VLAN, if '*override*' checkbox is selected.

Then, click '*Add*' button.

Click '*Apply*' button to apply the settings than click '*Confirm*' to confirm the settings.



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

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

Removing records from the packet routing table

To remove records, select checkboxes for the rows to be removed and click 'Remove selected' button.

4.1.20.4 QoS and bandwidth control

In the 'QoS and bandwidth control' section, you may configure Quality of Service function.

Network switch → QoS and bandwidth control

QoS and bandwidth control						
	GE port 0	GE port 1	GE port 2	CPU port	SFP port 0	SFP port 1
VLAN priority (default)	0 ▼	0 ▼	0 ▼	0 ▼	0 ▼	0 ▼
QoS mode	DSCP only ▼	DSCP only ▼	DSCP only ▼	DSCP only ▼	DSCP only ▼	DSCP only ▼
Remap 802.1p priorities:						
0	0 ▼	0 ▼	0 ▼	0 ▼	0 ▼	0 ▼
1	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼
2	2 ▼	2 ▼	2 ▼	2 ▼	2 ▼	2 ▼
3	3 ▼	3 ▼	3 ▼	3 ▼	3 ▼	3 ▼
4	4 ▼	4 ▼	4 ▼	4 ▼	4 ▼	4 ▼
5	5 ▼	5 ▼	5 ▼	5 ▼	5 ▼	5 ▼
6	6 ▼	6 ▼	6 ▼	6 ▼	6 ▼	6 ▼
7	7 ▼	7 ▼	7 ▼	7 ▼	7 ▼	7 ▼
Ingress packets limit mode	off ▼	off ▼	off ▼	off ▼	off ▼	off ▼
Speed limit for ingress queued packets 0	0	0	0	0	0	0
Speed limit for ingress queued packets 1	previous ▼	previous ▼	previous ▼	previous ▼	previous ▼	previous ▼
Speed limit for ingress queued packets 2	previous ▼	previous ▼	previous ▼	previous ▼	previous ▼	previous ▼
Speed limit for ingress queued packets 3	previous ▼	previous ▼	previous ▼	previous ▼	previous ▼	previous ▼
Egress packages limit mode	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Speed limit for egress packets	0	0	0	0	0	0

- **VLAN priority (default)** — 802.1p priority assigned to untagged packets, received by this port. If 802.1p or IP Diffserv is already assigned to the packet, this setting will not be used ('default vlan priority' will not be applied to packets containing IP header, when one of the QoS modes is in use: DSCP only, DSCP preferred, 802.1p preferred);
- **QoS mode** — QoS operation mode:
 - **DSCP only** — distribute packets into queues based on IP Diffserv priority only;
 - **802.1p only** — distribute packets into queues based on 802.1p priority only;
 - **DSCP, 802.1p** — distribute packets into queues based on IP Diffserv and 802.1p priorities, if both priorities are present in the packet, IP Diffserv priority is used for queuing purposes;
 - **802.1p, DSCP** — distribute packets into queues based on IP Diffserv and 802.1p priorities, if both priorities are present in the packet, 802.1p priority is used for queuing purposes.
- **Remap 802.1p priorities** — remap 802.1p priorities for untagged packets. Thus, a new value may be assigned for each priority received in VLAN packet;
- **Ingress packets limit mode** — restriction mode for traffic coming to the port.
 - **Off** — no restriction;

-
- *All packets* — restrict all traffic;
 - *BroadMultFlood* — multicast, broadcast, and flooded unicast traffic will be restricted;
 - *BroadMult* — multicast and broadcast traffic will be restricted;
 - *Broad* — only broadcast traffic will be restricted.
- *Speed limit for ingress queued packets 0* — bandwidth restriction for traffic incoming to a queue 0 port. Permitted values — from 70 to 250000 kbps;
 - *Speed limit for ingress queued packets 1* — bandwidth restriction for traffic incoming to a queue 1 port. You can double the bandwidth (prev prio *2) of priority 0, or leave it unchanged (same as prev prio);
 - *Speed limit for ingress queued packets 2* — bandwidth restriction for traffic incoming to a queue 2 port. You can double the bandwidth (prev prio *2) of priority 1, or leave it unchanged (same as prev prio);
 - *Speed limit for ingress queued packets 3* — bandwidth restriction for traffic incoming to a queue 3 port. You can double the bandwidth (prev prio *2) of priority 2, or leave it unchanged (same as prev prio);
 - *Egress packages limit mode* — when checked, enable the bandwidth restriction for outgoing port traffic;
 - *Speed limit for egress packets* — bandwidth restriction for outgoing port traffic. Permitted values — from 70 to 250000 kbps.
- *Apply* — apply defined settings.
 - *Confirm* — commit modified settings.



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

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

4.1.20.5 Queue priority mapping

Network switch → Queue priority mapping

Queue priority mapping

QoS 802.1p priority settings

802.1p	0	1	2	3	4	5	6	7
Queue	1 ▼	0 ▼	0 ▼	1 ▼	2 ▼	2 ▼	3 ▼	3 ▼

Diffserv queue mapping

Diffserv	Queue	Diffserv	Queue	Diffserv	Queue	Diffserv	Queue
0x00	0 ▼	0x40	1 ▼	0x80	2 ▼	0xC0	3 ▼
0x04	0 ▼	0x44	1 ▼	0x84	2 ▼	0xC4	3 ▼
0x08	0 ▼	0x48	1 ▼	0x88	2 ▼	0xC8	3 ▼
0x0C	0 ▼	0x4C	1 ▼	0x8C	2 ▼	0xCC	3 ▼
0x10	0 ▼	0x50	1 ▼	0x90	2 ▼	0xD0	3 ▼
0x14	0 ▼	0x54	1 ▼	0x94	2 ▼	0xD4	3 ▼
0x18	0 ▼	0x58	1 ▼	0x98	2 ▼	0xD8	3 ▼
0x1C	0 ▼	0x5C	1 ▼	0x9C	2 ▼	0xDC	3 ▼
0x20	0 ▼	0x60	1 ▼	0xA0	2 ▼	0xE0	3 ▼
0x24	0 ▼	0x64	1 ▼	0xA4	2 ▼	0xE4	3 ▼
0x28	0 ▼	0x68	1 ▼	0xA8	2 ▼	0xE8	3 ▼
0x2C	0 ▼	0x6C	1 ▼	0xAC	2 ▼	0xEC	3 ▼
0x30	0 ▼	0x70	1 ▼	0xB0	2 ▼	0xF0	3 ▼
0x34	0 ▼	0x74	1 ▼	0xB4	2 ▼	0xF4	3 ▼
0x38	0 ▼	0x78	1 ▼	0xB8	2 ▼	0xF8	3 ▼
0x3C	0 ▼	0x7C	1 ▼	0xBC	2 ▼	0xFC	3 ▼

- *Queue 802.1p priority settings* — allows to distribute packets into queues depending on the 802.1p priority.
 - *802.1p* — 802.1p priority value;
 - *Queue* — outgoing queue number.
- *Diffserv queue mapping* — allows to distribute packets into queues depending on the IP Diffserv priority.
 - *Diffserv* — IP Diffserv priority value;
 - *Queue* — outgoing queue number.
- *Apply* — apply defined settings;
- *Confirm* — commit modified settings.



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

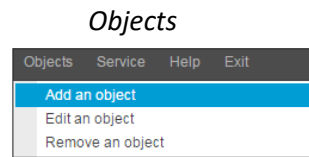
- *Default* — set default settings;
- *Save* — save settings into the device flash memory without applying them.



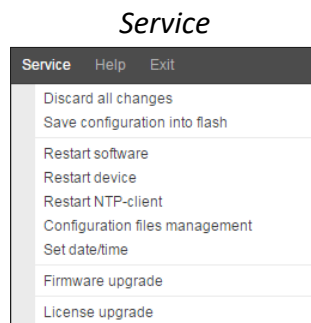
Queue 3 is the highest priority, queue 0 is the least priority.
The weighted distribution of packets across outgoing queues 3/2/1/0 is as follows: 8/4/2/1.

4.1.21 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.



4.1.22 Saving configuration and 'Service' menu



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

To save the base of registered SIP subscribers, select '*Save subscribers database*' in the '*Service*' menu.

To write the current configuration into non-volatile memory of the device, select '*Service*' — '*Save configuration into FLASH*' menu

To restart the device software, select '*Service*' — '*Software restart*' menu.

To restart the device completely, select '*Service*' — '*Device restart*' menu.

To perform forced time re-synchronization with NTP server, select '*Service*' — '*NTP client restart*' menu.

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

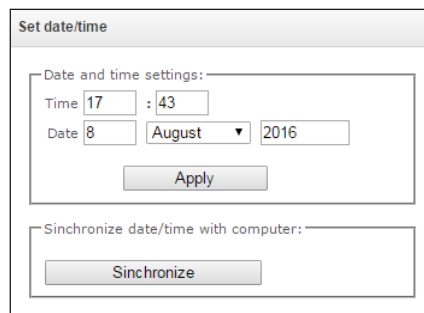
To configure the device local date and time manually, select '*Service*' — '*Date and time configuration*' menu; see Section 4.1.23 Time and date configuration.

To update the firmware via web configurator, select '*Service*' — '*Firmware update*' menu; see Section 4.1.24 Firmware update via web configurator.

To update/add licenses, select '*Service*' — '*License update*' menu; see Section 4.1.25 Licenses.

4.1.23 Time and date configuration

Service → *Set date/time*



The screenshot shows a web interface window titled "Set date/time". Inside, there are two main sections. The first section, "Date and time settings:", contains a "Time" field with "17" and "43" in separate boxes, and a "Date" field with "8", a dropdown menu showing "August", and "2016". Below these fields is an "Apply" button. The second section, "Synchronize date/time with computer:", contains a "Synchronize" button.

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.

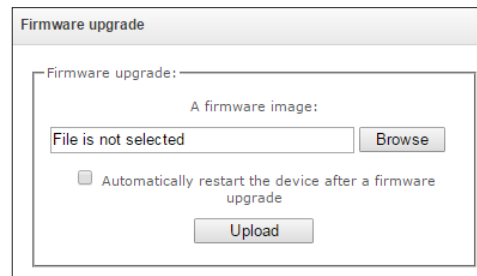
Click '*Synchronize*' button to synchronize the device system time with the current time on a local PC.

4.1.24 Firmware update via web configurator

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

Firmware file upload form will open.

Service → *Firmware upgrade*



The screenshot shows a web interface window titled "Firmware upgrade". Inside, there is a section "Firmware upgrade:" with a sub-section "A firmware image:". Below this, there is a text field containing "File is not selected" and a "Browse" button. Underneath, there is a checkbox labeled "Automatically restart the device after a firmware upgrade" which is currently unchecked. At the bottom of the section is an "Upload" button.

- *Firmware upgrade* — update firmware and/or Linux kernel.

To update the firmware, specify the update file name in '*A firmware image*' field using '*Browse*' button and click '*Upload*'. When the operation is completed, restart the device using '*Service*' — '*Restart device*' menu.

4.1.25 Licenses

SMG-1016M licenses:

- *SMG1-PBX-2000* – registration of up to 2000 SIP subscribers;
- *SMG1-SORM* – activation of SORM functionality;
- *SMG1-VAS-500+IVR* – activation of VAS for 500 subscribers and IVR;
- *SMG1-CORP-500+IVR* – activation of registration feature for up to 500 SIP subscribers, 500 VAS for SIP subscribers and IVR;
- *SMG1-H323* – activation of H.323 protocol;
- *SMG1-RCM* – activation of Radius Call Management;
- *SMG1-REC* – activation of call record functions;
- *SMG1-SRM-1* – activation of SORM agent functionality to provide SORM functions;
- *SMG1-V5.2-LE* – activation of V5.2 LE protocol to provide outstation connection via V5.2 AN;
- *SMG1-VNI-40* – extension of network interfaces quantity for up to 40;
- *SMG1-VNS* – activation of the voice notification system functionality;
- *SMG1-AUTH-CALL* – activation of the ‘Authorization calls’ functionality;
- *SMG1-SORM-374N* – activation of the functionality of the telemetry channel on the agricultural complex produced by JSC Norsi-Trans to implement the requirements of Federal Law No. 374 (‘Yarovaya Package’);
- *SMG1-SORM-374P* – activation of the telemetry channel functionality on the RTK-NT storage system;
- *SMG1-SORM-374T* – activation of the functionality of the telemetry channel on the agricultural complex of the TechArgos company for conducting operational searches for collecting and storing votes;
- *SMG1-SORM-374V* – activation of the telemetry channel functionality on the VAS Experts APC for conducting operational searches for collecting and storing votes;
- *SMG1-SORM-374M* – activation of the functionality of the telemetry channel on the APC of the MFI Soft company for conducting operational searches for collecting and storing votes;
- *SMG1-AF-Astarta* – activation of exchange functionality with the IS ‘Anti-fraud’ verification node produced by LLC ‘Astarta’ via RADIUS protocol;
- *SMG1-AF-Intech* – activation of exchange functionality with IS ‘Anti-fraud’ verification node produced by LLC ‘Hexagon Labs’ via RADIUS protocol;
- *SMG1-AF-Custom* – activation of exchange functionality with the Anti-fraud System Control System of other manufacturers via RADIUS protocol.

SMG-2016 licenses:

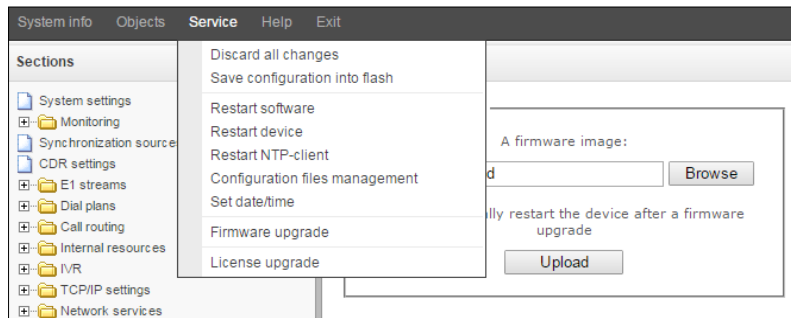
- *SMG2-PBX-3000* – registration of up to 3000 SIP subscribers;
- *SMG2-SORM* – activation of SORM functionality;
- *SMG2-VAS-1000+IVR* – activation of VAS for 1000 subscribers and IVR;
- *SMG2-CORP-1000+IVR* – activation of registration feature for up to 1000 SIP subscribers, 1000 VAS for SIP subscribers and IVR;
- *SMG2-RCM* – activation of Radius Call Management;
- *SMG2-REC* – activation of call record functions;
- *SMG2-SRM-2* – activation of SORM agent functionality to provide SORM functions;
- *SMG2-V5.2-LE* – activation of V5.2 LE protocol to provide outstation connection via V5.2 AN;
- *SMG2-VNI-40* – extension of network interfaces quantity for up to 40;
- *SMG2-RESERVE-SLAVE* – activation of IP reservation in master-slave mode (Total time of device operation without a gateway with an SMG2-RESERVE license is 200 hours);
- *SMG2-RESERVE-E1* – activation of reservation of E1 streams in master-slave mode (required availability of license SMG2-RESERVE (SMG2-RESERVE-SLAVE));
- *SMG2-VNS* – activation of the voice notification system functionality;
- *SMG2-AUTH-CALL* – activation of the ‘Authorization calls’ functionality;
- *SMG1-SORM-374N* – activation of the functionality of the telemetry channel on the agricultural complex produced by JSC Norsi-Trans to implement the requirements of Federal Law No. 374 (‘Yarovaya Package’);
- *SMG2-SORM-374P* – activation of the telemetry channel functionality on the RTK-NT storage system;
- *SMG2-SORM-374T* – activation of the functionality of the telemetry channel on the agricultural complex of the TechArgos company for conducting operational searches for collecting and storing votes;
- *SMG2-SORM-374V* – activation of the telemetry channel functionality on the VAS Experts APC for conducting operational searches for collecting and storing votes;
- *SMG2-SORM-374M* – activation of the functionality of the telemetry channel on the APC of the MFI Soft company for conducting operational searches for collecting and storing votes;
- *SMG2-AF-Astarta* – activation of exchange functionality with the IS ‘Anti-fraud’ verification node produced by LLC ‘Astarta’ via RADIUS protocol;
- *SMG2-AF-Intech* – activation of exchange functionality with IS ‘Anti-fraud’ verification node produced by LLC ‘Hexagon Labs’ via RADIUS protocol;
- *SMG2-AF-Custom* – activation of exchange functionality with the Anti-fraud System Control System of other manufacturers via RADIUS protocol.

SMG-3016 licenses:

- *SMG3-PBX-3000* – registration of up to 3000 SIP subscribers;
- *SMG3-SORM* – activation of SORM functionality;
- *SMG3-VAS-1000+IVR* – activation of VAS for 1000 subscribers and IVR;
- *SMG3-CORP-1000+IVR* – activation of registration feature for up to 1000 SIP subscribers, 1000 VAS for SIP subscribers and IVR;
- *SMG3-RCM* – activation of Radius Call Management;
- *SMG3-REC* – activation of call record functions;
- *SMG3-SRM-2* – activation of SORM agent functionality to provide SORM functions;
- *SMG3-V5.2-LE* – activation of V5.2 LE protocol to provide outstation connection via V5.2 AN;
- *SMG3-VNI-40* – extension of network interfaces quantity for up to 40;
- *SMG3-RESERVE-SLAVE* – activation of IP reservation in master-slave mode (Total time of device operation without a gateway with an SMG2-RESERVE license is 200 hours);
- *SMG3-RESERVE-E1* – activation of reservation of E1 streams in master-slave mode (required availability of license SMG2-RESERVE (SMG2-RESERVE-SLAVE));
- *SMG3-VNS* – activation of the voice notification system functionality;
- *SMG3-AUTH-CALL* – activation of the 'Authorization calls' functionality;
- *SMG3-SORM-374N* – activation of the functionality of the telemetry channel on the agricultural complex produced by JSC Norsis-Trans to implement the requirements of Federal Law No. 374 ('Yarovaya Package');
- *SMG3-SORM-374P* – activation of the telemetry channel functionality on the RTK-NT storage system;
- *SMG3-SORM-374T* – activation of the functionality of the telemetry channel on the agricultural complex of the TechArgos company for conducting operational searches for collecting and storing votes;
- *SMG3-SORM-374V* – activation of the telemetry channel functionality on the VAS Experts APC for conducting operational searches for collecting and storing votes;
- *SMG3-SORM-374M* – activation of the functionality of the telemetry channel on the APC of the MFI Soft company for conducting operational searches for collecting and storing votes;
- *SMG3-MSR* – activation of software media server (MSR) functionality;
- *SMG3-AF-Astarta* – activation of exchange functionality with the IS 'Anti-fraud' verification node produced by LLC 'Astarta' via RADIUS protocol;
- *SMG3-AF-Intech* – activation of exchange functionality with IS 'Anti-fraud' verification node produced by LLC 'Hexagon Labs' via RADIUS protocol;
- *SMG3-AF-Custom* – activation of exchange functionality with the Anti-fraud System Control System of other manufacturers via RADIUS protocol.

To update/add licenses, you should obtain a license file. Contact Eltex marketing department by email eltex@eltex-co.ru or phone +7 (383) 274-48-48 and provide device serial number and MAC address (see 4.1.28 View factory settings and system information).

Next, select *'License upgrade'* 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' — 'Restart device'* menu.

4.1.26 'Help' menu

This menu contains details on the current firmware version and factory settings as well as other system information.

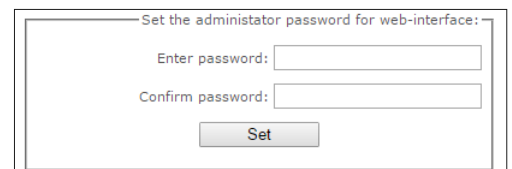


4.1.27 'Users: Management' menu

The link [Users: Management](#) is intended for operations with passwords used in web configurator access.

Specify web interface administrator password

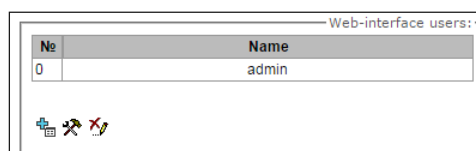
To change administrator password, enter a new password into *'Enter password'* field and re-enter it into *'New password confirmation'* field. To apply the password, click *'Set'* button.



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




Web interface users

Management → Web-interface users



In this block, you may configure web configurator access restrictions at the user level. There is always an administrator for the system, that may add or remove users and assign the access level.

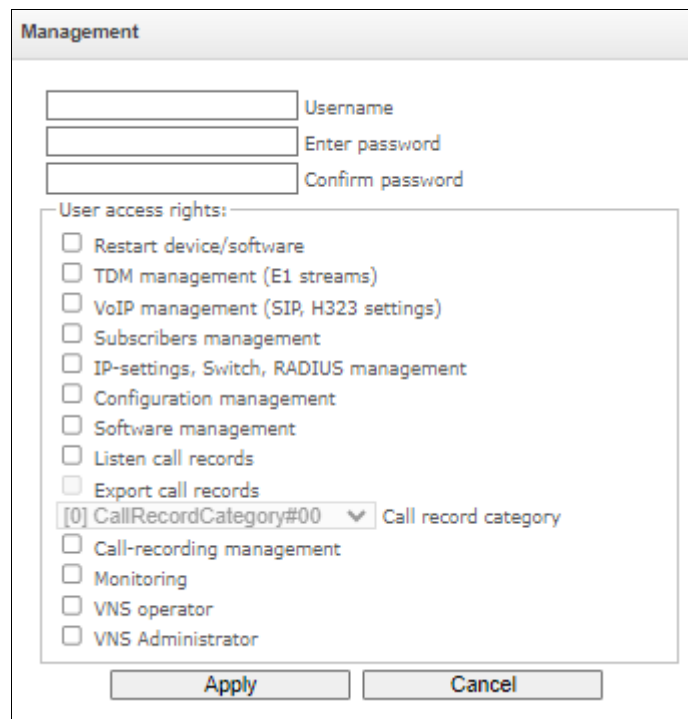
To create, edit or remove users, use the following buttons:

-  — 'Add user'
-  — 'Edit user parameters'
-  — 'Remove user'

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.

Creating a new user:

Management → Web-interface users → Object



The screenshot shows a 'Management' dialog box with the following elements:

- Three text input fields: 'Username', 'Enter password', and 'Confirm password'.
- A section titled 'User access rights:' containing a list of permissions, each with an unchecked checkbox:
 - Restart device/software
 - TDM management (E1 streams)
 - VoIP management (SIP, H323 settings)
 - Subscribers management
 - IP-settings, Switch, RADIUS management
 - Configuration management
 - Software management
 - Listen call records
 - Export call records
 - Call record category (dropdown menu showing '[0] CallRecordCategory#00')
 - Call-recording management
 - Monitoring
 - VNS operator
 - VNS Administrator
- Two buttons at the bottom: 'Apply' and 'Cancel'.

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

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

User access rights:

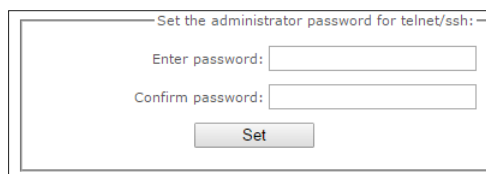
- *Restart device/software* — allows you to restart the device and firmware;
- *TDM management (E1 streams)* — allows you to set up E1 streams;
- *VoIP management (SIP, H323 settings)* — allows you to configure SIP and H323 interfaces;
- *Subscribers management* — provides the ability to configure SMG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

- *Call-recording management* — access to call records and to the settings of call recording;
- *Monitoring* — access to monitoring sections;
- *VNS operator* — access is provided to VNS 'Numbers list' and 'Reports' sections, as well as to 'VNS tasks' of Monitoring;
- *VNS Administrator* — access is provided to the VNS sections 'Voice messages', 'Notification tasks', 'Notify records', as well as to the 'VNS Tasks' of Monitoring. To provide full access to the VNS section, you should use the rights of VNS Operator and Administrator of the VNS jointly.

To save the configuration, click the 'Apply' button, and then use the menu 'Service' – 'Save configuration to flash'.

Set the administrator password for Telnet and SSH

Management → *Web-interface users* → *Set the administrator password for telnet/ssh*

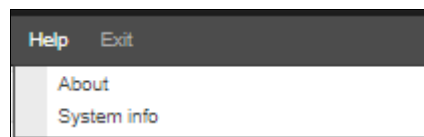


In this block, you may change password for Telnet, SSH and console access.

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.

4.1.28 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.

4.1.29 Exit the configurator

Click 'Exit' link to exit the configurator.

4.2 Command line, list of supported commands and keys (SMG)

4.2.1 Command line in debug mode, list of supported commands and keys

SMG provides several ways to connect to the command line interface:

- *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 30 — Debug mode commands

Command	Description
help	View the list of available commands
quit	Exit debug mode
logout	Exit debug mode
exit	Exit debug mode
history	Show the list of previously entered commands
radact [on/off]	Turn RADIUS on/off
radshow	View the list of requests to RADIUS server
resolve	Check domain name resolution Parameter: domain name
rstat	View RADIUS protocol operation statistics
q931timers	View Q.931 timer values
msspimg [on/off] <idx>	Enable/disable signal processor querying; idx — signal processor name — 0..5
stream [stream]	View E1 stream state or a specific stream state, 'stream' is a stream number (0..15)
e1stat <stream>	View E1 stream counters
alarm	View alarm log information
sync	View synchronization source information
syncfreq	View synchronization frequency information
setsync	Forced synchronization source change Parameter — <stream number>
checkmod	Check number modifier operation for the specific number Parameters: <modifier table><phone number to be checked>
frmtrace	Enable low-level tracing for E1 signal streams Parameters: <level><stream number><usage> – Level: l1, l2, l3 – Usage: 1 — enabled, 0 — disabled
cic <linkset>	View status of channels in the link set, <linkset> is SS7 link set number
checknum	Check the number with the dial plan
cfg_read	Apply the current configuration; this command will reset and re-initialize E1 streams
callref	Show information on active SIP calls
rtpdebug <level>	Enable switch RTP debugging; <level> is a debugging level WARNING! This command may cause the gateway to become unresponsive under load
msspcports	View RTP port state

mshow <device>	View signal processor connection statistics
sipstat	View SIP call statistics
sipclrst	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
mshowreglog	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

4.2.1.1 Tracing commands available through the debug port

4.2.1.1.1 Enable debugging globally

Command syntax: `trace start`

4.2.1.1.2 Disable debugging globally

Command syntax: `trace stop`

4.2.1.1.3 Enable/disable debugging for specific arguments

Command syntax: `trace <POINT>on/off <IDX><LEVEL>`

Parameters:

<POINT>	argument
<IDX>	numeric parameter
<LEVEL>	debug level

Table 31— Possible arguments (<POINT>)

Value <POINT>	Command description	Value <IDX>
<i>hwpkt</i>	Tracing of packet contents at the first level of exchange between the main application and E1 stream driver	0..15
<i>stream</i>	E1 stream tracing	0..15
<i>port</i>	Application operation tracing	Not used
<i>isup</i>	SS7 protocol ISUP subsystem operation tracing	Not used
<i>mtp3</i>	SS7 protocol MTP3 level operation tracing for E1 stream	0..15
<i>sipt</i>	SIP/-T/-I protocol operation tracing	Not used
<i>pril3</i>	DSS1 protocol third level operation tracing for E1 stream	0..15
<i>sw</i>	TDM switch tracing	Not used
<i>mshpc</i>	IP slips tracing	Not used
<i>mshpd</i>	Signal processor operation tracing	0..7
<i>net</i>	2nd layer data network operation tracing	Not used
<i>sync</i>	Synchronization source operation tracing	Not used
<i>erl1</i>	Low-level tracing for the system that transfers messages between the application and SIP module	Not used
<i>erl3</i>	High-level tracing for the system that transfers messages between the application and SIP module	Not used
<i>snmp</i>	SNMP protocol operation tracing	Not used
<i>np</i>	Dial plan (routing) operation tracing	Not used
<i>mod</i>	Modifier operation tracing	Not used
<i>alarm</i>	Gateway alarm state tracing	Not used
<i>radius</i>	RADIUS protocol operation tracing	Not used

4.2.2 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**.

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.

4.2.2.1 List of CLI commands

Table 32 — 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> <MINS>	1-31 1-12 2011-2037 00-23 00-59	Set the device local date and time
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. (<i>License installed</i> — license is installed <i>License NOT installed</i> — license is not installed)
license download	<FILE> <SERVERIP>	License file name	Download licenses from the address specified

		Server IP address in AAA.BBB.CCC.DDD format	
license update			Update the license
license reset	no/yes		Delete all installed licenses
management			Enter SS7 stream management mode
mirroring			Enter mirroring management mode
number check	<NUMPLAN> <NUMBER> <COMPLETE>	0-15/0-255 String, 31 characters max. yes/no	Availability check for routing by this number. Check is performed by caller and callee masks and also in the database of the configured SIP, PRI and V5.2 subscribers. The check provides the routing possibility data for this number in the defined dial plan: <ul style="list-style-type: none"> • <i>calling-table</i> — routing by the caller table. • <i>called-table</i> — routing by the callee table. • <i>NOT found in</i> — routing by this table is not possible. • <i>found in</i> — routing by this table is possible. SIP/PRI/V5.2 abonent ID[11] index [0] — SIP/PRI/V5.2 subscriber [subscriber ID] [database record number for this subscriber] <i>Prefix [6]</i> — 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. <i>STREAM</i> — number of stream for capture <i>FILE</i> — file for writing
quit			Terminate this CLI session
reboot	<YES_NO>	yes/no	Reboot 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 <i>DEVICE</i> — interface for monitoring <i>FILE</i> — file for packet writing <i>SNAPLEN</i> — 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

4.2.2.2 Change device access password via CLI

As it is possible to 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: go to configuration mode by entering the config command, enter the command `copy running_to_startup` and press <Enter>.

4.2.2.3 Statistics mode

In this mode, you may view the statistics data in accordance with Q.752 ITU-T guideline tables.

4.2.2.3.1 Enter the statistics viewing mode

Command syntax: `statistic`

4.2.2.3.2 Enter the MTP (SS7) signaling traffic volume viewing mode

Command syntax: `mtp`

Execution result: Change to MTP statistic mode `SMG-[STAT]-[MTP]>`

Parameters used in MTP traffic statistics viewing commands

<LINK>	E1 stream number
<LINKSET>	SS7 link set number
< TIME1>	amount of time for statistics output (hours)
< TIME2>	amount of time for statistics output (minutes)

4.2.2.3.2.1 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.

4.2.2.3.2.2 View signaling traffic (MTP message accounting)

Q.752 ITU-T guidelines, Table 15

Command syntax: `message accounting<LINK><TIME1><TIME2>`

Example: `SMG-[STAT]-[MTP]> message accounting 8 12 0`

Execution result:

```

+-----+
|      SS7 MTP message accounting.      Link  08      |
+-----+-----+-----+-----+
|      Period:  00:00:00 -  00:00:00 (    0 sec)      |
+-----+-----+-----+-----+
|              |      Messages      |      Octets      |
+-----+-----+-----+-----+
| Received      |              0      |              0      |
+-----+-----+-----+-----+
| Transmitted   |              0      |              0      |
+-----+-----+-----+-----+

```

Meaning: 8th E1 stream MTP signaling traffic volume is shown for 12-hour 00-minute interval.

4.2.2.3.2.3 View MTP signaling link faults and performance counters

Q.752 ITU-T guidelines, Table 1

Command syntax: `signalling link faults_and_performance<LINK><TIME1><TIME2>`

Example: `SMG-[STAT]-[MTP]> signalling link faults_and_performance 8 12 0`

Execution result:

```

+-----+
|      MTP SL faults and performance.      Link  08      |
+-----+-----+-----+-----+
|      Period:  00:00:00 -  00:00:00 (    0 sec)      |
+-----+-----+-----+-----+
| Duration the In-service state |              0 sec |
+-----+-----+-----+-----+
| SL failure events all reasons |              0      |
+-----+-----+-----+-----+
| Number of SU received in error |              0      |
+-----+-----+-----+-----+

```

Meaning: 8th E1 stream signaling link faults and performance counters are shown for 12-hour 00-minute interval.

4.2.2.3.2.4 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.

4.2.2.3.2.5 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.

4.2.2.3.2.6 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 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: Linkset and route set availability metrics are shown for for the 8th Link for 12-hour 00-minute interval.

4.2.2.3.2.7 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.

4.2.2.3.3 Enter the packet traffic viewing mode

Command syntax: `packets`

Execution result: `SMG-[STAT]-[PACKETS]>`

4.2.2.3.3.1 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.

4.2.2.4 Management mode

To enter the SS7 stream management mode, execute 'management' command.

```
SMG> management
Entering management mode.
SMG-[MGMT]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
exit			Move to a higher menu level
history			View history of entered commands
nslookup	<HOST>	string	Request IP address for host with the name specified <i>HOST</i> — address for request
ping host	<HOST>		Send PING request to the host specified
ping ip	<IP>	IP address in AAA.BBB.CCC.DDD format	Send PING request to the IP address specified
e1 stat clear	<STREAM>	0-15	Reset statistics for the E1 stream specified
e1 stat show	<STREAM>	0-15	View statistics for the E1 stream specified
ss7link	<SS7_LINK>	0-15	Proceed to the specified SS7 stream parameter management
quit			Terminate this CLI session

4.2.2.4.1 SS7 stream management mode

To enter this mode, execute 'ss7link <Link>' command in the SS7 stream configuration mode, where <Link> is SS7 stream number that may take values in the range from 0 to 15.

```
SMG-[MGMT]> ss7link 0
E1[0]. Signaling is SS7
SMG-[MGMT]-[SS7LINK][0]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
chan block	<CHAN_INDEX>	1-31	Block the specified channel (BLO)
chan ccr	<CHAN_INDEX> start state stop	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 <i>CHAN_INDEX_START</i> — starting E1 channel number in a group <i>CHAN_COUNT</i> — quantity of channels in a group
chan group reset	<CHAN_INDEX_START> <CHAN_COUNT>	1-31 2-31	Reset channel group <i>CHAN_INDEX_START</i> — starting E1 channel number in a group <i>CHAN_COUNT</i> — quantity of channels in a group
chan group unblock	<CHAN_INDEX_START> <CHAN_COUNT>	1-31 2-31	Unblock a group of channels <i>CHAN_INDEX_START</i> — starting E1 channel number in a group <i>CHAN_COUNT</i> — 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

4.2.2.5 Port mirroring parameters configuration mode

In the mode of configuring port mirroring parameters (only for SMG-1016M) to enter this mode, you must execute the '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>	CPU/ GE_PORT0/ GE_PORT1/ GE_PORT2/ SFP0/ SFP1	Configure port mirroring: PORT — port type
	<NAME>	src_in/ src_out/ dst_in/ dst_out	NAME — port designation <i>src_in</i> — incoming packet source port — copy frames received from this port (source port) <i>src_out</i> — outgoing packet source ports — copy frames sent by this port (source port). <i>dst_in</i> — incoming packet destination port — destination port for copied frames received by selected source ports. <i>dst_out</i> — outgoing packet destination port — destination port for copied frames sent by selected source ports.
	<ACT>	on/off	
show			Configure port mirroring

4.2.2.6 General device parameter configuration mode

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

For each configuration mode 'do' and 'top' commands are available. The 'do' command allows you to execute a command of root CLI menu when being in any configuration submenu. The 'top' command allows going to root CLI menu.

```
SMG> config
Entering configuration mode.
SMG-[CONFIG]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
alarm path	<set>	off or /mnt/sd[abc][1-7]*	Select an external storage device for alarm message storage Off — disabled /mnt/sd[abc][1-7]* — path to storage device for tracing storage
access category			Enter access categories' configuration mode
cdr			Enter CDR record parameter configuration mode
copy running_to_startup			Write the current configuration into non-volatile memory of the device (into start configuration)
copy startup_to_running			Restore the current configuration from the start configuration
count linkset			Show the number of SS7 link sets
count trunk			Show the number of trunk groups
count trunk_direction			Show the number of trunk directions
count sipt-interface			Show the number of SIP interfaces
count radius-profile			Show the number of RADIUS profiles
delete modifiers-table			Show the number of modifier table profiles
count sipcause-profile			Show the number of Q.850 and sip-reply compliance profiles
count routing-profile			Show the number of scheduled routing profiles
count h323-interface			Show the number of h.323 profiles
count ss7timers			Show the number of SS7 timer profiles
delete linkset	<OBJECT_INDEX>	existing number of the link set	Delete SS7 link set
delete trunk	<OBJECT_INDEX>	Existing trunk group number	Delete trunk group
delete trunk direction	<OBJECT_INDEX>	Existing trunk direction number	Delete trunk direction
delete sipt-interface	<OBJECT_INDEX>	Existing SIP interface number	Delete SIP interface

new hunt-group			Create call group
new pickup-group			Create pickup group
numplan			Enter the dial plan configuration mode
pbx_profiles			Enter the PBX profile configuration mode
ports range	<RANGE_PORT>	1-65535	Define the range of UDP ports used for voice traffic (RTP) and data transmission via T.38 protocol
ports show			Show UDP port configuration
ports start	<START_PORT>	1024-65535	Define the starting UDP port used for voice traffic (RTP) and data transmission via T.38 protocol
q931-timers			Enter Q.931 timer configuration mode
quit			Terminate this CLI session
radius			Enter RADIUS configuration mode
record			Enter the conversation recording configuration mode
reset_config			Reset configuration
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
sorm-data-extractor			Go to SORM configuration mode
ss7cat			Enter SS7 category configuration mode
ss7timers	<SS7_TIMERS_INDEX>	0-15	Enter SS7 timer configuration mode
submodule-usage			Enter the configuration mode of SM-VP submodule usage
switch_port			Enter the internal switch configuration mode

sync			Enter the configuration mode for synchronization parameters
syslog			Enter the system log parameters configuration mode
trunk	<TRUNK_INDEX>	0-63	Enter the trunk group configuration mode
trunk_direction	<DIRECTION_INDEX>	0-31	Enter the trunk direction configuration mode
v52			Enter the configuration mode for V5.2 parameters for the current E1 stream

4.2.2.7 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.	CDR data archiving
category	save	yes/no	Save/do not save subscriber category in CDR files
config			Return to Configuration menu
duration count mode	<CDR_COUNT_MODE>	round-up/round-down/not-round	Rounding up/down or not rounding (write with milliseconds)
emptysave	<CDR_EMPTY>	yes/no	Save/do no save empty CDR files
enabled	<CDR>	yes/no	Generate/do not generate CDRs
exit			Return from this configuration submenu to the upper level
fields add <field>			Add specified field in the end of field list (see 4.2.2.8 CDR field list)
fields default			Set basic set of fields
fields flush			Clear list of used fields
fields set <field>	<FIELD_INDEX>	0-39	Substitute field on corresponding position with specified field (see 4.2.2.8 CDR field list)
file create mode	<CDR_FILE>	periodically/ once-a-day/ once-an-hour	CDR file creation mode <i>periodically</i> — with defined period <i>once-a-day</i> — daily <i>once-an-hour</i> — hourly
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> <show>	/mnt/sd[abc] [1-7]*	Path to CDR data storage on local drives View CDR data storage path setting
localkeep period	<day> <hour> <min>	0-30 0-23 0-59	Time of CDR data storage on a local drive
localsave	<no> <yes>		Save CDR data on a local drive
period day	<CDR_DAY>	0-30	Set the time period for CDR generation and saving in the device RAM, days
period hour	<CDR_HOUR>	0-23	Set the time period for CDR generation and saving in the device RAM, hours

period min	<CDR_MIN>	0-59	Set the time period for CDR generation and saving in the device RAM, minutes
pickup mark	<CDR_pickup_MARK>	yes/no	Add/do not add additional field 'pickup tag' to CDR
quit			Terminate this CLI session
redirectmark	<CDR_REDIRECT_MARK>	yes/no	Add/do not add additional field 'redirection tag' to CDR
redirectsave	<CDR_REDIRECT>	yes/no	Add additional field 'Redirecting number' to CDR, otherwise redirecting number will replace calling party number in redirected calls
redirected duration	<CDR_REDIR_DURATION>	yes/no	Specify redirected call duration
release initiator mark	<CDR_RELEASE>	yes/no	Save disconnection initiator tag
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
upserver enabled	<CDR_UPLOAD>	yes/no	Transfer/do not transfer CDRs to the server
upserver ipaddr	<CDR_SERVER_IPADDR>	String, 63 characters max.	Set server IP address
upserver login	<CDR_SERVER_LOGIN>	String, 63 characters max.	Set a username to access server
upserver passwd	<CDR_SERVER_PASSWD>	String, 63 characters max.	Set a user password to access server
upserver path	<CDR_SERVER_PATH>	String, 63 characters max.	Set the path to the folder on the server, in which CDR records will be saved
upserver port	<CDR_SERVER_PORT>	1-65535	Set server TCP port
upserver protocol	<CDR_VIA_PROTO>	FTP/SCP	Set the protocol by which CDRs will be go to the server
upserver_reserve enabled	<CDR_RESERV_ENA>	yes/no	Transfer/do not transfer CDRs to the backup server
upserver_reserve ipaddr	<CDR_RESERV_IPADDR>	String, 63 characters max.	Set the IP address of the backup server
upserver_reserve login	<CDR_RESERV_LOGIN>	String, 63 characters max.	Set a username to access backup server
upserver_reserve only_fail	<CDR_RESERV_ONLY_FAIL>	yes/no	Enable/disable saving CDR files to the backup server only if an error occurs when writing to the main one
upserver_reserve passwd	<CDR_RESERV_PASSWD>	String, 63 characters max.	Set a user password to access the backup server
upserver_reserve path	<CDR_RESERV_PATH>	String, 63 characters max.	Set the path to the folder on the backup server where CDR records will be saved
upserver_reserve port	<CDR_RESERV_PORT>	1-65535	Set the TCP port of the backup server

4.2.2.8 CDR field list

The CDR fields 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 output (after all modifications)
device sign	Distinguishing feature
disc code	Code of disconnection via Q.850
disc info	Call status in case of disconnection
duration	Call duration
global-callref	Global Call Reference (GCR) field
incoming CID category	CID category on input (before modification)
incoming description	Caller description–subscriber/trunk (TG) name
incoming E1 chan	Number of incoming E1 channel
incoming E1 stream	Number of incoming E1 stream
incoming ipaddr	Caller IP address
incoming SIP call id	SIP Call-ID of incoming call
incoming SS7 category	SS7 category on input (before modification)
incoming SS7 CIC	CIC number of incoming call
incoming type	Caller type
mark pickup	Call pickup mark
mark redir	Call redirection mark
mark release side	Mark of disconnection initiator
numplan in	Dial plan after that call will be received
numplan out	Dial plan after that call will be transmitted
outgoing CID category	CID category on input (after modification)
outgoing description	Callee description–subscriber/trunk (TG)
outgoing E1 chan	Number of outgoing E1 channel
outgoing E1 stream	Number of outgoing E1 stream

outgoing ipaddr	IP address of callee
outgoing SIP call id	SIP Call-ID of outgoing call
outgoing SS7 category	SS7 category on output (after modification)
outgoing SS7 CIC	CIC number of outgoing call
outgoing type	Callee type
radius-rejected	Blocking RADIUS server address
redirecting in	Number of forwarding party on input (before modification)
redirecting out	Number of forwarding party on output (after modification)
sequential number	Sequential record number
time connect	Connection time
time disconnect	Call disconnection time
time setup	Time of call receipt

4.2.2.9 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

4.2.2.10 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 V5.2LE SORM-TRANSIT	Set the signalling type for the stream Possible signalling types: Q931_USR, Q931_NET, SS7, SORM, V5.2LE, SORM-TRANSIT
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 SORM configuration mode for the current E1 stream
ss7			Enter the configuration mode for SS7 signalling parameters of the current E1 stream

4.2.2.10.1 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

4.2.2.10.2 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: <i>up_ring</i> — sequential forward. <i>down_ring</i> — sequential back <i>up_start</i> — from the first and forward <i>down_start</i> — 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 Disconnect	in <on_off>	on/off	Enable 'Process PI In-Band in DISCONNECT' option
invokeID	<INVOKE_ID>	1024-65535	Set operation call initial identifier (used as a reference number for unique operation call identification)
numplan	<CLD_PLAN_ID>	unknown/ISDN/ telephony/National/ Privat	Specify dial plan type To use common dial plan E.164, select 'ISDN/telephony'
qsig	<ON_OFF>	on/off	Enable/disable QSIG signalling
quit			Terminate this CLI session
RestartChannel	<SEND>	send/don't_send	Send/do not send channel RESTART
RestartInterface	<SEND>	send/don't_send	Send/do not send interface RESTART
RoutingProfile	<PROF Number>	[0-127] or none	Select scheduled routing profile
SendCataAON	<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
transit location number	<ON_OFF>	on/off	Allow/disable shifting of the Location Number parameter from incoming SS7/SIP-T message to Calling Party Number parameter of outgoing message SETUP Q931
trunk	<trunk_index>	0-31	Define the trunk group number for the current stream

4.2.2.10.3 SORM configuration mode for the current E1 stream

This mode is available only for SORM signaling (set by the '*signaling*' command). To enter this mode, execute the *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 messaging activity control on L1
chan1(2) mode	<SORM_MODE>	DCE/DTE	Set mode for chan1 (2). Acceptable modes: DCE, DTE
chan1(2) send L3 Reset	<ON_OFF>	on/off	Allow/deny sending L3 reset command to channel1(2)
chan1(2) send L3 Restart	<ON_OFF>	on/off	Allow/deny sending L3 restart command to channel1(2)
chan1(2) send SABME	<ON_OFF>	on/off	Enable/disable balanced asynchronous extended mode (SABME) on channel 1(2)
cmd	<CMD_ADDR>	1/3	Set 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	Select the signal operating mode of KSL channels
protocol specification	<SPECIFICATION>	order_70/ KZ_specification/ order_268	Select the SORM specification
quit			Terminate this CLI session
resp	<RESP_ADDR>	1/3	Set response frame address
show			Show SORM configuration
tcp interface	<IFACE_NAME>		Select a network interface for organizing a TCP connection
tcp port1		10000-65535	
tcp port2		10000-65535	
timer 10min	<ON_OFF>	on/off	Enable/disable timeout for receiving commands from the SORM control unit

4.2.2.10.4 SS7 signalling parameters configuration mode for the current E1 stream

This mode is available for SS7 signalling only (set by 'signaling' command). To enter this mode, execute 'ss7' command in the E1 stream configuration mode.

```
SMG-[CONFIG]-E1[0]> ss7
E1[0]. Signaling is SS7
SMG-[CONFIG]-E1[0]-[SS7]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
CIC fill	<CIC> <step>	0-65535 0-255	Define CIC value for all time slots beginning from 0 CIC — CIC starting number step — numbering increment
CIC set	<TIMESLOT> <CIC>	0-31 0-65535	Define CIC value for a single timeslot TIMESLOT — timeslot number CIC — CIC value
config			Return to Configuration menu
Dchan	<D_CHAN>	0-31	Set D-channel number for a line 0 — do not use D-channel (voice stream)
DPC MTP3		0-16383	Define DPC MTP3 value for the current stream
exit			Return from this configuration submenu to the upper level
history			View history of entered commands
linkset	<linkset_index>	0-15	Assign SS7 link set for the current stream
quit			Terminate this CLI session
show			Show SS7 signalling parameter configuration
SLC	<slc>	0-15	Set the signal channel identifier in SS7 link set

4.2.2.11 Dynamic firewall's parameters configuration mode

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

```
SMG-[CONFIG]> firewall dynamic
Entering dynamic firewallmode.
SMG-[CONFIG]-[DYN-FIREWALL ]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
blacklist add	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Add an address to the blacklist
blacklist remove by addr	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Remove an address from the blacklist
blacklist remove by pos	<POSITION>	0-65635	Remove an address from the blacklist using its position in the list
blacklist show all			Show the blacklist
blacklist show count			Show the number of entries in the list of addresses blocked by dynamic firewall

blacklist show address	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Find the specified address in the blacklist
blacklist show first	<COUNT>	0-4095	Show the defined quantity of addresses from the blacklists starting from the first
blacklist show last	<COUNT>	0-4095	Show the defined quantity of addresses from the blacklists starting from the last
blacklist show position	<POSITION>	0-65635	Show the entry stored in the defined position in the blacklist
block history show all			View the history of the blacklist
block show count			Show the number of entries in the blacklist history
block show address	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Find the defined address in the blacklist history
block show first	<COUNT>	0-4095	Show the defined quantity of addresses from the blacklists history starting from the first
block show last	<COUNT>	0-4095	Show the defined quantity of addresses from the blacklists history starting from the last
block show position	<POSITION>	0-65635	Show the entry stored in the defined position in the blacklist history
blocklist remove by addr	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Remove the address from the list of automatically blocked addresses
blocklist remove by pos	<POSITION>	0-65635	Remove the address from the list of automatically blocked addresses using its position in the list
blocklist show all			Show the list of automatically blocked addresses
blocklist show count			Show the number of entries in the automatically blocked addresses list
blocklist show address	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Find the defined address in the automatically blocked addresses list
blocklist show first	<COUNT>	0-4095	Show the defined number of entries in the automatically blocked addresses list starting from the first
blocklist show last	<COUNT>	0-4095	Show the defined number of entries in the automatically blocked addresses list starting from the last
blocklist show position	<POSITION>	0-65635	Show the entry stored in the defined position in the automatically blocked addresses list
exit			Exit from this configuration submenu to the upper level.
history			View the history of entered commands
quit			Quit the CLI session
set block_time	<SERVICE> <BLCKTIME>	SIP/WEB/TELNET/SSH /OTHER 60-352800	Set time (in seconds) during which the access from a suspicious address will be blocked
set enable	<ENA>	on/off	Enable/disable the dynamic firewall
set tries	<SERVICE> <TRIES>	SIP/WEB/TELNET/SSH /OTHER 1-10	Set the maximum number of access attempts to the service before blocking the host

set forgive_time	<SERVICE> <FORGIVETIME>	SIP/WEB/TELNET/SSH /OTHER 60-352800	Set forgive time for the service
set increment	<SERVICE> <INCREMENT FLG>	SIP/WEB/TELNET/SSH /OTHER no/yes	Enable progressing blocking for the service
show			Show the dynamic firewall settings
whitelist add	<WHITEIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Add an IP address to the list of addresses denied for automatic blocking
whitelist remove by addr	<WHITEIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Remove an IP address from the list of addresses denied for automatic blocking
whitelist remove by pos	<POSITION>	0-65635	Remove an IP address from the list of addresses denied for automatic blocking using its position in the list
whitelist show all			Show the list of addresses denied for automatic blocking
whitelist show count			Show the number of entries in the list of addresses denied for automatic blocking
whitelist show address	<WHITEIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Find the defined address in the list of addresses denied for automatic blocking
whitelist show first	<COUNT>	0-4095	Show the defined number of entries in the list of addresses denied for automatic blocking startinf from the first
whitelist show last	<COUNT>	0-4095	Show the defined number of entries in the list of addresses denied for automatic blocking startinf from the last
whitelist show position	<POSITION>	0-65635	Show the entry stored in the defined position in the list of addresses denied for automatic blocking

4.2.2.12 Static firewall's parameters configuration mode

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

```
SMG-[CONFIG]> firewall static
Entering static firewall mode
SMG-[CONFIG]-[firewall]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
add profile	<PROF_NAME>	you may use letters, numbers, '_' character, 63 characters max.	Add firewall profile
add rule	<direction>	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

			sent the packet will receive either TCP RST packet or 'ICMP destination unreachable'.
	<P_IDX>	1-65535	Firewall profile number
add rule geoip	<direction>	input output	Add firewall GeoIP rule The direction of the rule operation
	<ENABLE>	enable/disable	Enable/disable the rule
	<RULE_NAME>	Text, max 63 characters	Rule name
	<COUNTRY>	Country name	Country to which the address is belong
	<PROTO>	any tcp udp icmp tcp+udp	Protocol type
	<S_PORT_START>	1-65535	Initial source port
	<S_PORT_END>	1-65535	Last source port
	<D_PORT_START>	1-65535	Initial destination port
	<D_PORT_END>	1-65535	Last destination port
	<ICMP_TYPE>	none 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	any ICMP packet type

	<ACTION>	accept, drop, reject	Action – an action implemented according to the rule: <ul style="list-style-type: none"> – <i>ACCEPT</i> – packets which match the rule will be forwarded by the firewall; – <i>DROP</i> – packets which match the rule will be dropped by the firewall without informing of the transmitted party; – <i>REJECT</i> – packets which match the rule will be dropped by the firewall, and the party transmitted the packet will receive a TCP RST packet or ICMP destination unreachable
	<P_IDX>	1-65535	Firewall profile number
add rule string	<direction>	input output	Add firewall rule – check strings. The direction of the rule operation
	<ENABLE>	enable/disable	Enable/disable the rule
	<RULE_NAME>	Text, max 63 characters	Name of the rule
	<CONTENT>	Text, max 127 characters	Text string which should be in a packet
	<S_IP>	AAA.BBB.CCC.DDD	Source IP address
	<S_MASK>	AAA.BBB.CCC.DDD	Source subnet mask
	<R_IP>	AAA.BBB.CCC.DDD	Destination IP address
	<R_MASK>	AAA.BBB.CCC.DDD	Destination subnet mask
	<PROTO>	any tcp udp icmp tcp+udp	Protocol type
	<S_PORT_START>	1-65535	Start source port
	<S_PORT_END>	1-65535	End source port
	<D_PORT_START>	1-65535	Start destination port
	<D_PORT_END>	1-65535	End destination port
	<ICMP_TYPE>	none any echo-reply destination-unreachable network-unreachable host-unreachable protocol-unreachable port-unreachable fragmentation-needed source-route-failed network-unknown host-unknown network-prohibited host-prohibited	ICMP packet type

	<ACTION>	<p>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</p> <p>accept, drop, reject</p>	<p>Action – an action implemented according to the rule:</p> <ul style="list-style-type: none"> – ACCEPT – packets which match the rule will be forwarded by the firewall; – DROP – packets which match the rule will be dropped by the firewall without informing of the transmitted party; – REJECT – packets which match the rule will be dropped by the firewall, and the party transmitted the packet will receive a TCP RST packet or ICMP destination unreachable
	<P_IDX>	1-65535	Firewall profile number
apply			Apply firewall settings
config			Return to Configuration menu.
del profile	<ID>	1-65535	Remove firewall profile
del rule	<ID>	1-65535	Remove firewall rule
exit			Exit from this configuration submenu to the upper level
modify profile	<ID> <NAME>	1-65535 you may use letters, numbers, '_' character 63 characters max.	Firewall profile index Enter a new name for the device
modify rule	<Type>	<p>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</p>	Modify the firewall rule specified (one of the parameters)

	<ID> <param>	1-65535 New value according to this parameter type	
move down	<ID>	1-65535	Move the rule one position down
move up	<ID>	1-65535	Move the rule one position up
quit			Terminate this CLI session
set eth	<PROFILE ID>	0-65535	Assign the rule to the network interface PROFILE ID = 0 means that profile will not be used
set pptp	<PPP_IDX> <PROFILE ID>	0-5 0-65535	Assign the rule to the interface PROFILE ID = 0 means that profile will not be used
set vlan	<VLAN_IDX> <PROFILE ID>	VLAN1...VLAN8 0-65535	Assign the rule to the VLAN PROFILE ID = 0 means that profile will not be used
show config			Show configuration
show interfaces			Show interface parameters
show system			Show system parameters

4.2.2.13 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/r no_access r/w/r no_access r/w/r	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 (external storages)

	<CFG_ACCESS>	no_access r/w/r	Set rights for access to CFG catalogue (configuration files)
user del	<IDX>	1-4	Remove user
user modify access	<IDX> <CDR_ACCESS> <LOG_ACCESS> <MNT_ACCESS> <CFG_ACCESS>	0-4 no_access/r/w/r no_access/r/w/r no_access/r/w/r no_access/r/w/r	Modify access permissions of the selected user: – Configure CDR directory access configuration, read/write – Configure log directory access configuration, read/write – Configure mnt directory access configuration, read/write – Configure access to cfg catalogue, read/write
user modify password	<IDX> <PASSWD>	0-4	Modify password of the selected user

4.2.2.14 H.323 protocol parameter configuration mode

To enter this mode, execute 'h323 configuration' command in the configuration mode.

```
SMG-[CONFIG]> h323 configuration
Entering H323Config-mode.
SMG-[CONFIG]-H323(config)>
```

Command	Parameter	Value	Action
?			Show the list of available commands
alias H323ID	<IDX>	String, max 63 characters	Set the gateway name used while registration on the Gatekeeper
cisco1700_adaptation	<ON_OFF>	on/off	Enable/disable Cisco1700 adaptation
config			Return to Configuration menu
exit			Exit from this configuration submenu to the upper level
gatekeeper discover	<ON_OFF>	on/off	Enable/disable GK search mode
gatekeeper DSCP	<GK_DSCP_RAS>	0-63	Assign the IP diffserv priority for RAS messages
gatekeeper H323ID	<GK_H323ID>	String, max 63 characters or none	Set GateKeeper ID. The 'none' value removes the ID
gatekeeper local subscribers	<ON_OFF>	on/off	Allow registration of local users on the local GK
gatekeeper mode	<GK_MODE>	none/ local/ remote	GK operation mode: – none – do not use; – local; – remote
gatekeeper ipaddr	<IPADDR>	AAA.BBB.CCC.DDD	Set a GK IP address
gatekeeper keepalive	<KEEPAL>	10-86400	Set registration time on the GK
gatekeeper port	<PORT>	1-65535	Set port for the GK
gatekeeper tech-prefix	<GK_TECH_PREFIX>	String, max 255 characters or none	Set technological prefix for the GK. The value 'none' removes the prefix.
gatekeeper ttl	<TTL>	90-86400	Set time for re-registration on the GK
gatekeeper use	<ON_OFF>	on/off	Enable/disable GK usage
history			View the command history
iface	<IFACE_NAME>	String, max 255 characters	Set a network interface for H.323
port	<PORT>	1-65535	Set local TCP port number for signalling H.323 messages receiving.

primary DGK H323ID	<DGK_H323ID>	String, max 63 characters or none	Set a main ID for Directory GateKeeper. The 'none' value removes the ID.
primary DGK ipaddr	<DGK_IPADDR>	AAA.BBB.CCC.DDD	Set a main IP address for Directory GateKeeper.
secondary DGK H323ID	<DGK_H323ID>	String, max 63 characters or none	Set an additional ID for Directory GateKeeper. The 'none' value removes the ID
secondary DGK ipaddr	<DGK_IPADDR>	AAA.BBB.CCC.DDD	Set an additional IP addresses for Directory GateKeeper
quit			Quit the CLI session
show			Show the settings

4.2.2.15 H.323 interface parameter configuration mode

To enter this mode, execute 'h323 interface <H323_INDEX>' command in the configuration mode, where <H323_INDEX> is a number of direction operating via H.323 protocol.

```
SMG-[CONFIG]> h323 interface 0
Entering H323-mode.
SMG-[CONFIG]-H323-INTERFACE [0]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
access category	<CAT_IDX>	0-31	Define the access category
alias H323ID clear	<H323ID>	String, 63 characters max.	Remove the gateway name during registration at the Gatekeeper
alias H323ID set	<H323ID>	String, 63 characters max.	Add the gateway name during registration at the Gatekeeper
codec disable	<CODEC_IDX>	0-3	Disable the defined codec. Codecs are numbered by priority – from 0 (the highest) to 3 (the lowest)
codec pte	<CODEC_IDX> <PTE>	0-3 10/20/30/40/50/ 60/70/80/90	Define payload time
codec ptype	<CODEC_IDX> <PTYPE>	0-3 0-127 or static	Define payload type. The 'static' value sets the value by default according to the defined codec
codec set	<CODEC_IDX> <CODEC>	0-3 G.711-U/ G.711-A/ G.729/ G.723.1_5.3/ G.723.1_6.3	Define used codec
config			Back to Configuration menu
destination clear			Remove interface destination
destination set	<HOSTNAME>	String, 63 characters max.	Define interface destination
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	<DTMF_c>	0-255	Define SIP-INFO level
DTMF mode	<DTMF_m>	inband/ RFC2833/ SIP-INFO	DTMF mode for the current interface
DTMF payload	<DTMF_p>	96-127	Define payload type for RFC2833
ecan	<CANCELLATION>	voice/ nlp-off-voice/	Set echo cancellation mode: Voice — echo cancellers are enabled.

		modem/ off	<p><i>Nlp-off-voice</i> — 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</p> <p><i>Modem</i> — echo cancellers are enabled in the modem operation mode (direct component filtering is disabled, NLP control is disabled, CNG is disabled)</p> <p><i>Off</i> — do not use echo cancellation (this mode is set by default)</p>
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	<p>Set the fax detection mode:</p> <p><i>no</i> — disable fax tone detection</p> <p><i>callee</i> — for the receiving party only</p> <p><i>caller</i> — for the transmitting party only</p> <p><i>callee_and_caller</i> — for both receiving and transmitting parties</p>
gain rx	<GAIN>		Set the volume of voice reception (gain of the signal received from the communicating gateway and output to the speaker of the phone unit connected to SMG gateway)
gain tx	<GAIN>		Volume of voice transmission (gain of the signal received from the microphone of the phone unit connected to SMG gateway and transmitted to the communicating gateway)
gatekeeper	<ON_OFF>	on/off	Enable/disable GK
h245tunneling	<ON_OFF>	on/off	Enable/disable tunneling
history			View history of entered commands
interface rtp	<IFACE_NAME>	String, 255 characters max.	Select network interface for RTP transfer
jitter adaptation period	<JT_AP>	1000-65535	Define the time of jitter-buffer adaptation to the lower limit, in milliseconds
jitter adjust mode	<JT_AM>	non-immediate/ immediately	<p>Specify the jitter buffer adjustment mode:</p> <p><i>non-immediate</i> — gradual</p> <p><i>immediately</i> — instant</p>
jitter deletion mode	<JT_DM>	soft/hard	<p>Specify buffer adjustment mode. Defines the method of packet deletion during buffer adjustment to lower limit.</p> <p><i>soft</i> — device uses intelligent selection pattern for deletion of packets that exceed the threshold</p> <p><i>hard</i> — packets which delay exceeds the threshold will be deleted immediately</p>
jitter deletion threshold	<JT_DT>	0-500	<p>Set the threshold for immediate deletion of a packet, in milliseconds</p> <p>When buffer size grows and packet</p>

			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: <i>adaptive</i> — adaptive <i>non-adaptive</i> — fixed
jitter vbd	<JT_VBD>	0-200	Define fixed buffer size for data transmission in VBD mode
max_active	<MAX_ACTIVE>	0-65535	Define the maximum number of active connection for an interface
name	<s_name>	you may use letters, numbers, '_' character 31 characters max.	Define a name for H.323 interface
nat	<NAT>	enable/disable	Enable/disable NAT
numbering plan	<NUMPLAN>	0-15/0-255	Select dial plan
port	<PORT>	1-65535	Define TCP port of the communicating gateway used for SIP signalling reception
quit			Terminate this CLI session
routing profile	<prof>	0-127	Select scheduled routing profile
RTCP control	<RTCP_c>	2-255	Define the quantity of time periods (RTCP period) during which the opposite party will wait for RTCP protocol packets
RTCP period	<RTCP_p>	5-255	Define the time period in seconds after which the device send control packets via RTCP protocol
show config			Show H323 interface information
src verify	<ON_OFF>	on/off	Enable/disable control of media traffic received from IP address and UDP port specified in SDP communication session description; otherwise the traffic from any IP address and UDP port will be accepted
t38 bitrate	<BITRATE>	nolimit/2400/4800/ 7200/9600/12000/ 14400	Specify the maximum transfer rate of fax transmitted via T.38 protocol
t38 disable			Disable fax reception via T.38 protocol
t38 enable			Enable fax reception via T.38 protocol
t38 fillbitremoval	<ON_OFF>	on/off	Enable/disable padding bit removals and inserts for data that does not relate to ECM
t38 pte	<T38_PTE>	10/20/30/40	Define T.38 packet generation frequency in milliseconds
t38 ratemgmt	<T38_RATE_MGMT>	localTCF/ transferredTCF	Set the data transfer speed management method <i>local TCF</i> — method requires that the TCF tuning signal was generated locally by the recipient gateway <i>transferred TCF</i> — 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

4.2.2.16 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		start End position	Move the number into the beginning of the list Move the number into the end of the list Move the number to the specific position
quit			Terminate this CLI session
set conference number		*,#,D,0-9. Or 'none' for blank(delete) number	Specify conference number
set ltimer		Number in the range 5-255	Define L-timer of a group call
set mode		(all/seqFisrt/seqNext/seqAllFirst/seqAllNextr)	Define group operation mode
set name		letter or number or '_', '.', '-'. Max 63 symbols	Specify call group name
set number			Define call group member number
set record-and-notify mode	<MODE>	simultaneous-notification/sequential-notification	Set 'record and notification' operation mode – simultaneous/separate.
set record-and-notify duration	<DURATION>	15-120	Set the maximum time for notification record
set stimer		Number in the range 5-255	Set S timer of a one group member call
set number-mask		Max 255 symbols	Set a mask for the call group
set recall-busy		yes/no	Enable/disable the 'Call back a busy person' option
set recall-declined		yes/no	Enable/disable the 'Call back the person who rejected the call' option
set release-mode	<MODE>	default/silent	Set release mode for a group call – default/silent

4.2.2.17 SS7 link set modification configuration mode

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

```
SMG-[CONFIG]> linkset 0
Entering Linkset-mode.
SMG-[CONFIG]-LINKSET[0]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
access category	<CAT_IDX>	0-31	Define the access category for the link set
alarm_ind	<ON_OFF>	on/off	Enable/disable fault indication for the specific SS7 link set
CCI	<ON_OFF>	on/off	Enable support for the SS7 link set channel integrity check
CCI frequency	<FREQ>	0-127	Define the frequency of channel integrity checks during outgoing calls performed through the SS7 link set
cdpn digit in IAM	<ON_OFF>	on/off	Transmission of the first digit of CdPN number in IAM message for overlap dialing method
chan_order	<CHAN_SELECT>	up_ring/ down_ring/ up_start/ down_start/ odd_up_ring/ odd_down_ring/ even_up_ring/ even_down_ring	Define the channel engagement order for the current SS7 link set <i>up_ring</i> — sequential forward <i>down_ring</i> — sequential back <i>up_start</i> — from the first and forward <i>down_start</i> — from the first and back <i>odd_up_ring</i> — sequential forward odd <i>odd_down_ring</i> — sequential back odd <i>even_up_ring</i> — sequential forward even <i>even_down_ring</i> — sequential back even
china	<ON_OFF>	on/off	Enable/disable Chinese SS7 protocol specification support
combined	<ON_OFF>	on/off	Enable/disable combined mode
config			Return to Configuration menu
DPC	<DPC_ID>	0-16383	Define destination point code — DPC
emergency alignment	<ON_OFF>	on/off	Emergency phasing in case of a single signal link in linkset
exit			Return from this configuration submenu to the upper level
history			View history of entered commands
ignore hold	<ON_OFF>	off/on	Ignore the received CPG with remote hold or remote retrieval features
init	<INIT_MODE>	blocked/ individual-ublock/ group-unblock/ group-reset	Define initialization type for the current link set
interworking	<INTERWORK>	no_change/ no_encountered/ encountered	Configure extraneous signalling systems interaction indicator: <i>no_change</i> — transfer value from the incoming call without any changes <i>no_encountered</i> — do not report interaction with a network that does not support the majority of services provided by ISDN network

			<i>encountered</i> — 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, characters max. 31	Define the current link set name
net_ind	<NET_IND>	international/ reserved/federal/ national	Set the network identifier: <i>international</i> — international network <i>reserved</i> — reserved network <i>federal</i> — federal network <i>national</i> — local network
numbering plan		0-15	Select dial plan for a LinkSet
OPC	<OPC_ID>	0-16383	Define the origination point code for the current SS7 link set
primary linkset	<PRI_LINKSET>	0-15	Select the primary SS7 link set for the combined mode operation
quit			Terminate this CLI session
release on suspend	<ON_OFF>	on/off	Enable/disable disconnection message output after suspend message reception
reserv linkset	<RES_LINKSET>	0-15	Select redundant SS7 link set
routing_profile	<prof>	0-127	Select scheduled routing profile
satellite	<SATELLITE>	override_no_satellite /transit/ add_one	Identifies the presence of the satellite channel in operation through this SS7 link set
secondary linkset	<SEC_LINKSET>	0-15	Select the secondary SS7 link set for the combined mode operation
show			Show configuration of the current SS7 link set
ss7timers	<index>	0-15	Select SS7 timer profile
stream SLC	<ON_OFF>	off/on	Enable/disable "Streams order by SLC"
TMR	<TMR>	speech/ 64kb_unrestricted/ 3.1KHz_audio/transit	Define the Transmission Medium Requirement for the current SS7 link set
trunk	<trunk_index>	0-31	Define the trunk group number for the current SS7 link set

4.2.2.18 SS7 timer configuration mode

To enter this mode, execute 'ss7timers <SS7_TIMERS_INDEX>' command in the configuration mode, where <SS7_TIMERS_INDEX> is a profile number.

```
SMG-[CONFIG]> ss7timers 0
Entering SS7Timers-mode.
SMG-[CONFIG]-SS7-TIMERS[0]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
config			Return to Configuration menu
exit			Return from this configuration submenu to the upper level
history			View history of entered commands
quit			Terminate this CLI session
set mtp2 T1	<TIMER>	400-500	Define MTP2 T1 level timer value (x100ms)
set mtp2 T2	<TIMER>	50-500	Define MTP2 T2 level timer value (x100ms)
set mtp2 T3	<TIMER>	10-20	Define MTP2 T3 level timer value (x100ms)
set mtp2 T4 normal	<TIMER>	75-95	Define MTP2 T4 normal level timer value (x100ms)
set mtp2 T4 emergency	<TIMER>	4-6	Define MTP2 T4 emergency level timer value (x100ms)
set mtp2 T6	<TIMER>	30-60	Define MTP2 T6 level timer value (x100ms)
set mtp2 T7 normal	<TIMER>	5-20	Define MTP2 T7 normal level timer value (x100ms)
set mtp3 T2	<TIMER>	7-20	Define MTP3 T2 level timer value (x100ms)
set mtp3 T4	<TIMER>	5-12	Define MTP3 T4 level timer value (x100ms)
set mtp3 T12	<TIMER>	8-15	Define MTP3 T12 level timer value (x100ms)
set mtp3 T13	<TIMER>	8-15	Define MTP3 T13 level timer value (x100ms)
set mtp3 T14	<TIMER>	20-30	Define MTP3 T14 level timer value (x100ms)
set mtp3 T17	<TIMER>	8-15	Define MTP3 T17 level timer value (x100ms)
set mtp3 T22	<TIMER>	1800-3600	Define MTP3 T22 level timer value (x100ms)
set mtp3 T23	<TIMER>	1800-3600	Define MTP3 T23 level timer value (x100ms)
set isup T1	<TIMER>	150-600	Define ISUP T1 level timer value (x100ms)
set isup T5	<TIMER>	3000-9000	Define ISUP T5 level timer value (x100ms)
set isup T6	<TIMER>	100-600	Define ISUP T6 level timer value (x100ms)
set isup T7	<TIMER>	200-300	Define ISUP T7 level timer value (x100ms)
set isup T8	<TIMER>	150-600	Define ISUP T1 level timer value (x100ms)
set isup T9	<TIMER>	300-2400	Define ISUP T9 level timer value (x100ms)
set isup T12	<TIMER>	150-600	Define ISUP T12 level timer value (x100ms)
set isup T13	<TIMER>	3000-9000	Define ISUP T13 level timer value (x100ms)

set isup T14	<TIMER>	150-600	Define ISUP T14 level timer value (x100ms)
set isup T15	<TIMER>	3000-9000	Define ISUP T15 level timer value (x100ms)
set isup T16	<TIMER>	150-600	Define ISUP T16 level timer value (x100ms)
set isup T17	<TIMER>	3000-9000	Define ISUP T17 level timer value (x100ms)
set isup T18	<TIMER>	150-600	Define ISUP T18 level timer value (x100ms)
set isup T19	<TIMER>	3000-9000	Define ISUP T19 level timer value (x100ms)
set isup T20	<TIMER>	150-600	Define ISUP T20 level timer value (x100ms)
set isup T21	<TIMER>	3000-9000	Define ISUP T21 level timer value (x100ms)
set isup T22	<TIMER>	150-600	Define ISUP T22 level timer value (x100ms)
set isup T23	<TIMER>	3000-9000	Define ISUP T23 level timer value (x100ms)
set isup T24	<TIMER>	1-20	Define ISUP T24 level timer value (x100ms)
set isup T25	<TIMER>	10-100	Define ISUP T25 level timer value (x100ms)
set isup T26	<TIMER>	600-1800	Define ISUP T26 level timer value (x100ms)
set isup T33	<TIMER>	120-150	Define ISUP T33 level timer value (x100ms)
set isup T34	<TIMER>	20-40	Define ISUP T34 level timer value (x100ms)
set isup T35	<TIMER>	150-200	Define ISUP T35 level timer value (x100ms)
show			Show configuration

4.2.2.19 Configuration mode of submodule usage

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

```
SMG2016-[CONFIG]> submodule-usage
SMG2016-[CONFIG]-[SUBMODULE-USAGE]>
```

Command	Parameter	Value	Action
?			Show list of the available commands
config			Return to the Configuration menu
history			View a history of the entered commands
quit			Complete CLI session
set msp	<INDEX> 0-5	On/off	Enable/disable submodule SM-VP with selected index
show			Show table of submodule usage

4.2.2.20 Modifier table configuration mode

To enter this mode, execute 'modifiers table <MODTBL_INDEX>' command in the configuration mode, where < MODTBL_INDEX> is a table number.

```
SMG-[CONFIG]-TRUNK[0]> modifiers table
Entering TRUNK-Modifiers mode.
SMG-[CONFIG]-TRUNK[0]-MODIFIER>
```

Command	Parameter	Value	Action
?			Show the list of available commands
add	<MODIFIER_MASK> [CLD_RULE] [CLG_RULE]	modifier mask, 255 characters max., should be enclosed in parentheses '(' and ')' modifier rule, 30 characters max. should be enclosed in quotation marks modifier rule, 30 characters max. 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 dial plan type for the callee number: MODIFIER_INDEX — modifier number CALLED_NP_TYPE — dial plan type
change called rule	<MODIFIER_INDEX> <CALLED_RULE>	0-8191 modifier rule, 30 characters max. should be enclosed in quotation marks	Edit callee number modification rule for the modifier MODIFIER_INDEX — modifier number CALLED_RULE — callee number modification rule
change called type	<MODIFIER_INDEX> <CALLED_TYPE>	0-8191 unknown/ subscriber/ national/ international/ network_specific/ nochange	Edit callee number type for the modifier: MODIFIER_INDEX — modifier number NUM_TYPE — subscriber number type: - <i>Subscriber</i> — used in local call and incoming long-distance call processing

			<ul style="list-style-type: none"> - <i>National</i> — used in outgoing long-distance call or local call and incoming long-distance call processing instead of the 'Subscriber' - <i>International</i> — used in long-distance calls and recording-completing circuits for outgoing international call processing - <i>network_specific</i> — specific network number - <i>unknown</i> — unknown number type - <i>nochange</i> — 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 dial plan type for the caller number: MODIFIER_INDEX — modifier number CALLING_NP_TYPE — dial plan type
change calling presentation	<MODIFIER_INDEX> <CALLING_PRESENT>	0-8191 allowed/ restricted/ not_available/ spare/ nochange	Edit caller presentation modification rule
change calling rule	<MODIFIER_INDEX> <CALLING_RULE>	0-8191 modifier rule, 30 characters max., should be enclosed in quotation marks	Edit caller number modification rule for the modifier MODIFIER_INDEX — modifier number CALLING_RULE — caller number modification rule
change calling screen	<MODIFIER_INDEX> <CALLING_SCREEN>	0-8191 not_screened/ user_passed/ user_failed/ network/nochange	Edit caller screen indicator modification rule
change calling type	<MODIFIER_INDEX> <CALLING_TYPE>	0-8191 unknown/ subscriber/ national/ international/ network_specific/ nochange	Edit caller number type for the modifier: MODIFIER_INDEX — modifier number NUM_TYPE — subscriber number type: - <i>Subscriber</i> — used in local call and incoming long-distance call processing

			<ul style="list-style-type: none"> - <i>National</i> — used in outgoing long-distance call or local call and incoming long-distance call processing instead of the 'Subscriber' - <i>International</i> — used in long-distance calls and recording-completing circuits for outgoing international call processing - <i>network_specific</i> — specific network number - <i>unknown</i> — unknown number type - <i>nochange</i> — keep number type unchanged
change general access-cat	<MODIFIER_INDEX> <ACCESS>	0-8191 0-31/nochange	Edit modifier access general category
change general numplan	<MODIFIER_INDEX> <NUMPLAN>	0-8191 0-15/nochange	Edit modifier general dial plan
change mask	<MODIFIER_INDEX> <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: <ul style="list-style-type: none"> - <i>Subscriber</i> — used in local call and incoming long-distance call processing - <i>National</i> — used in outgoing long-distance call or local call and incoming long-distance call processing instead of the 'Subscriber' - <i>International</i> — used in long distance calls and recording-completing circuits for outgoing international call processing - <i>network_specific</i> — specific network number - <i>any</i> — any number type
change type	<MODIFIER_INDEX>	0-8191	Change subscriber type for a modifier (caller/callee)

	<MODIFIER_TYPE>	calling/called	
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

4.2.2.21 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 ptpVPNclient	<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	Specify PPTP server IP address

		IP address in AAA.BBB.CCC.DDD format	
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 interface user_name	<NET_IFACE_IDX> <USER>	0-39 you may use letters, numbers, '_', '.', '-', ':' characters, 63 characters max.	Define user name (for VPN interface only)
set interface user_pass	<NET_IFACE_IDX> <PASS>	0-39 you may use letters, numbers, '_', '.', '-', ':' characters, 63 characters max.	Define password (for VPN interface only)
set interface VID	<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 settings dns primary	<IPADDR>	IP address in AAA.BBB.CCC.DDD format	Define primary DNS server IP address
set settings dns secondary	<IPADDR>	IP address in AAA.BBB.CCC.DDD format	Define secondary DNS server address
set settings gateway_iface	<NET_IFACE_NAME>		Name of an interface which gateway should be considered as a primary by default
set settings hostname	<HOSTNAME>	you may use letters, numbers, '_', '.', '-', ':' characters, 63 characters max.	Specify host name
set settings ssh	<PORT>	1-65535	Define TCP port for the device access via SSH protocol, default value is 22
set settings telnet	<PORT>	1-65535	Define TCP port for the device access via Telnet protocol, default value is 23
set settings use_ip_list	<ON_OFF>	on/off	Enable/disable IP whitelist utilization
set settings web	<PORT>	1-65535	Define TCP port for web configurator, default is 80
show interface by_index			Show settings of the specific network interface
show interface list			Show the list of available network interfaces
show settings			Show network parameters
snmp			Enter SNMP configuration mode
ssh restart			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.

4.2.2.21.1 DHCP server parameters configuration mode

To enter this mode, execute 'dhcp server' command in the network parameter configuration mode.

```
SMG-[CONFIG]-NETWORK> dhcp server
Entering Network mode.
SMG-[CONFIG]-[NETWORK]-[DHCPD]>
```

Command	Parameter	Value	Action
?			Show the list of available commands.
conflicttime	<CONFLICT>	10-10000000	Set the time period during which the IP address will remain reserved upon MAC address conflict identification, 10 seconds or more
declinetime	<DECLINE>	10-10000000	Time period during which the IP address will remain reserved upon the DHCP decline reception, 10 seconds or more
dhcpd start			Launch DHCP server
dhcpd stop			Stop DHCP server
dns 0/1/2/3	<DNS>	IP address in AAA.BBB.CCC.DDD format	Obtain DNS server addresses from the operator's networks
domain	<DOMAIN>	String, 31 characters max.	Define the domain name used for DHCP clients by default
enabled	<ENABLE>	no/yes	Enable/disable DHCP server upon the gateway startup
exit			Exit from this configuration submenu to the upper level.
gateway	<GW>	IP address in AAA.BBB.CCC.DDD format	Define default router or gateway address assigned to DHCP server clients
interface	<IFACE_NAME>	String, 255 characters max.	Select network interface for DHCP server
ipaddr end	<IPADDR>	IP address in AAA.BBB.CCC.DDD format	Define an ending address in the range of assigned IP addresses
ipaddr start	<IPADDR>	IP address in AAA.BBB.CCC.DDD format	Define a starting address in the range of assigned IP addresses
max_lease	<MAX_LEASE>	10-10000000 sec	Define the maximum lease time for IP address assigned by DHCP server, 10 seconds or more
maxleases	<MAXLEASES>	1-65535	Restrict the number of leased addresses
min_lease	<MIN_LEASE>	10-10000000 sec	Define the minimum lease time for IP address assigned by DHCP server, 10 seconds or more
netmask	<NETMASK>	IP address in AAA.BBB.CCC.DDD format	Define the network mask
ntp announce external server address	<NTP_SERVER>	IP address in AAA.BBB.CCC.DDD format	Define the external NTP server address for announcing via option 42
ntp announce external server enable	<ANNOUNCE_EXT>	no/yes	Allow the announcing of external NTP server via option 42
ntp announce local	<ANNOUNCE_LOCAL>	no/yes	Allow the announcing of local NTP server via option 42
offertime	<OFFER>	10-10000000	Set the time period during which the requested IP address will remain reserved, 10 seconds or more
quit			Terminate this CLI session
savetime	<SAVE>	7200-10000000/off	Set the time interval for saving information on leased addresses to dhcpd.leases file off — do not save the database

show config				Show DHCP configuration: usage status, network mask, default gateway, domain addresses, Wins-servers, number of leased addresses, request timeouts
static_lease add	<NAME> <IPADDR> <MAC>	String, characters max. IP address AAA.BBB.CCC.DDD format MAC address in XX:XX:XX:XX:XX:XX format	63 in	Assign IP and MAC address static matches: <i>NAME</i> — match name <i>IPADDR</i> — IP address <i>MAC</i> — 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 AAA.BBB.CCC.DDD format	in	Define the primary WINS server IP address for DHCP client usage

4.2.2.21.2 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, characters max. String, characters max. IP address AAA.BBB.CCC.DDD format; string, characters max. On/off On/off	31 31 in 31 31	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 password server_ip startup username	String, characters max. On/off String, characters max. IP address AAA.BBB.CCC.DDD format On/off String, characters max.	31 31 in 31	Modify PPTP parameters Modify tag Modify encryption activity Modify password Modify PPTP server IP address Modify automatic PPTP startup Modify username
show			Show PPTP settings	
start interface	<IDX_INERFACE>	0-16	Launch PPTP interface immediately	
status interface	<IDX_INERFACE>	0-16	View the state of the specific interface	
stop interface	<IDX_INERFACE>	0-16	Stop PPTP interface immediately	

4.2.2.21.3 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	NET_IFACE_IDX ON_OFF	Network interface index Off/on	Obtain NTP settings via DHCP
set ntp local server enable	ON_OFF	Off/on	Activate local NTP server to get time from SMG
set ntp local server interface	NET_IFACE_IDX	Network interface index	Set up a network interface, on which local NTP server will work
set ntp period	NTP_PERIOD	10-1440	Set synchronization period time
set ntp server	NTP	String, 63 characters max.	Specify the NTP server address with which SMG will synchronize
set ntp usage	ON_OFF	off/on	Enable NTP client
show config			Show configuration
timezone set		GMT/GMT+1/GMT-1/ GMT+2/GMT-2/GMT+3/ GMT-3/GMT+4/GMT-4/ GMT+5/GMT-5/GMT+6/ GMT-6/GMT+7/GMT-7/ GMT+8/GMT-8/GMT+9/ GMT-9/GMT+10/GMT- 10/ GMT+11/GMT- 11/GMT+12 Asia Europe	Specify a timezone in reference to UTC Select location city in Asia Select location city in Europe

4.2.2.1.4 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: <i>TYPE</i> — SNMP message type <i>IP</i> — trap recipient IP address <i>COMM</i> — password contained in traps <i>PORT</i> — 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

4.2.2.22 Dial plan configuration mode

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

```
SMG-[CONFIG]> numplan
Entering Numbering-plan mode.
SMG-[CONFIG]-[NUMPLAN]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
config			Return to Configuration menu
create prefix	<IDX_Numplan>	0-15/0-255	Create prefix in the specified dial plan
delete prefix	<IDX Prefix>		Remove the specified prefix
exit			Exit from this configuration submenu to the upper level
history			View history of entered commands
prefix			Enter prefix configuration mode
quit			Terminate this CLI session
set active		0-15/0-255	Define the number of active dial plans
set domain	<IDX> <DOMAIN>	0-15/0-255 String, 15 characters max.	Specify domain for registration
set name	<IDX> <NAME>	0-15/0-255 String, 15 characters max.	Define the dial plan name
show active count			Show the number of active dial plans
show active list			Show the list of active dial plans
show list			Show the list of dial plans
show prefixes	<IDX>	0-15/0-255 no/yes	Show dial plan prefixes with the specific number

4.2.2.22.1 Prefix configuration mode

To enter this mode, execute 'prefix <PREFIX_INDEX>' command in the configuration mode, where <PREFIX_INDEX> is a prefix number.

```
SMG-[CONFIG]-[NUMPLAN]> prefix 0
Entering Prefix-mode.
SMG-[CONFIG]-[NUMPLAN]-PREFIX[0]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
access category	<CAT_IDX>	0-31	Define the access category
access check	<ON_OFF>	on/off	Check/do not check the access category
called np1	<PFX_CLD_NPI>	transit/ unknown/ isdn/ telephony/ national/ private	Modify callee number type (transit — keep unchanged)
called type	<PFX_CLD_TYPE>	unknown/ subscriber/ national/ international/ specific_net/ transit	Callee number type modification (transit — keep unchanged) <i>Subscriber number</i> — used in local call and incoming long-distance call processing. At that, transmitted number

			<p>should be as follows: abxxxxx, or bxxxxx, or xxxxx</p> <p><i>National number</i> — 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></p> <p><i>International number</i> — 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')</p> <p><i>Transit</i> — keep unchanged</p>
command	<PFX_COMMAND>	set/ clear/ control	<p>Select action for a service</p> <p><i>set</i> — set VAS service</p> <p><i>clear</i> — cancel VAS service</p> <p><i>control</i> — VAS service activity control</p>
config			Return to Configuration menu
dial mode	<MODE>	nochange/ enblock/ overlap	<p>Define the prefix dialling mode:</p> <p><i>nochange</i> — callee number will be sent as it was received from the incoming channel</p> <p><i>enblock</i> — callee number will be sent as a block</p> <p><i>overlap</i> — callee number will be sent with an overlap (by a single digit)</p>
direction	<PFX_DIRECTION>	local/ emergency/ zone/ vedomst/ toll/ international	<p>Define the type of access to the trunk group or direction:</p> <p><i>local</i> — local network</p> <p><i>emergency</i> — emergency services</p> <p><i>zone</i> — zone network</p> <p><i>vedomst</i> — department network</p> <p><i>toll</i> — long-distance network</p> <p><i>international</i> — international network</p>
duration	<PFX_DURATION>	0-255	Specify number dialling duration timer, in seconds
exit			Exit from this configuration submenu to the upper level
getCID	<ON_OFF>	on/off	Enable/disable Caller ID request for the prefix routing
history			View history of entered commands
ivr	<IVR_INDEX>	0-255	Define IVR scenario for ivr-type prefix
mask edit			Enter the prefix mask editing mode
mask show			Show prefix masks
modifiers table called	<MODTBL_INDEX>	0-255 or none	Called number modification table which is used while dial plan changing
modifiers table calling	<MODTBL_INDEX>	0-255 or none	Calling number modification table which is used while dial plan changing

name	<s_name>	string, max 31 characters (letters, digits and '_' sign are allowed to be used)	Define a name/description for prefix
needCID	<ON_OFF>	on/off	Enable/disable CallerID mandatory information request
new access category	<CAT_IDX>	0-127	Select new access category for prefix with 'change-numplan' type.
new numplan	<PLAN_IDX>	0-15/0-255	Select new numbering plan for prefix with 'change-numplan' type.
numplan	<PLAN_IDX>	0-15	Define dial plan that the prefix belongs to
notdial ST	<USE_ST>	yes/no	Disable/enable end dial marker transmission (ST in SS or 'sending complete' in PRI)
operator	<OPERATOR>	or/and	Select the logical operator "or/and"
pickup-group	<PICKUP_GROUP_INDEX>	0-254/any	Select group for prefix with 'pickup group' type. Defines certain group or mode in which any group which includes subscriber's number is selected
quit			Terminate this CLI session
service	<PFX_USER_SERVICE>	cf-unconditional/ cf-busy/ cf-no-reply/ cf-out-of-order/ call-pickup/ conference/ clear-all/ intercom/ paging	VAS service type <i>cf-unconditional</i> — call forward unconditional <i>cf-busy</i> — call forward on busy <i>cf-no-reply</i> — call forward on no reply <i>cf-out-of-order</i> — call forward on out of service <i>call-pickup</i> — call pickup <i>conference</i> — conference with sequential collection <i>clear-all</i> — clear all services <i>intercom</i> — intercom <i>paging</i> — paging
show			Show prefix configuration
session time	<PFX_SESSION_TIME>	5-64800 off — no limits	Set the time in seconds by which the duration of a call passing through a prefix is limited
session warning time	<PFX_SESSION_TIME_WARN>	1-300 off — no warn	An option that enables the sound signal warning about the call ending within a specified number of seconds before the end of the call
trunk	<TRUNK>	0-31	Specify trunk group number or direction
type	<PFX_TYPE>	trunk/ trunk-direction/ change-numplan/ modifier/ user_service pickup-group/ ivr	Define prefix type: <i>trunk</i> — transition to trunk group <i>trunk direction</i> — transition to trunk direction change-numplan — change dial plan <i>modifier</i> — modifier prefix type <i>user_service</i> — VAS prefix <i>pickup-group</i> — pickup group <i>ivr</i> — select IVR scenario

4.2.2.2.2 Prefix mask configuration mode

To enter this mode, execute 'mask edit' command in the prefix configuration mode.

```
SMG-[CONFIG]-PREFIX[0]> mask edit
Entering Prefix-Mask mode.
SMG-[CONFIG]-PREFIX[0]-MASK>
```

Command	Parameter	Value	Action
?			Show the list of available commands
add	<PREFIX_MASK> [PFX_MASK_TYPE]	prefix mask. 255 characters max., should be enclosed in parentheses '(' and ')' calling/called [called]	Add a new mask into the prefix. You may specify the mask type — for a caller ('calling') or callee ('called'); default mask type is always 'called'
config			Return to Configuration menu
history			View history of entered commands
exit			Exit from this configuration submenu to the upper level
modify duration	<PREFIX_MASK_INDEX> <DURATION>	0-1024 0-255	Specify number dialling duration timer <i>PREFIX_MASK_INDEX</i> — mask number <i>DURATION</i> — timer
modify Ltimer	<PREFIX_MASK_INDEX> <LONG_TIMER>	0-1024 0-255	Define the long timer <i>PREFIX_MASK_INDEX</i> — mask number <i>LONG_TIMER</i> — timer
modify mask	<PREFIX_MASK_INDEX> <PREFIX_MASK>	0-1024 prefix mask. 255 characters max., should be enclosed in parentheses '(' and ')'	Modify mask <i>PREFIX_MASK_INDEX</i> — mask number <i>PREFIX_MASK</i> — mask
modify prefix	<PREFIX_MASK_INDEX> <PFX_INDEX>	0-1024 0-255	Transfer mask to another prefix <i>PREFIX_MASK_INDEX</i> — mask number to be transferred <i>PFX_INDEX</i> — prefix that the mask is being transferred to
modify stimer	<PREFIX_MASK_INDEX> <SHORT_TIMER>	0-1024 [0-255]	Define the short timer <i>PREFIX_MASK_INDEX</i> — mask number <i>DURATION</i> — timer
modify type	<PREFIX_MASK_INDEX> <PFX_MASK_TYPE>	0-1024 calling/called	Define the mask type — caller or callee number analysis: <i>PREFIX_MASK_INDEX</i> — mask number to be transferred <i>PFX_MASK_TYPE</i> — mask type: – <i>calling</i> — caller number analysis – <i>called</i> — callee number analysis
quit			Terminate this CLI session
remove	<PREFIX_MASK_INDEX>	0-1024	Remove mask
show			Show mask information

4.2.2.23 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(no more than 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

4.2.2.24 PBX profile configuration mode

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

```
SMG-[CONFIG]> pbx_profiles
Entering PBX profiles mode.
SMG-[CONFIG]-PBX_PROFILES>
```

Command	Parameter	Value	Action
?			Show the list of available commands
add pbx	<NAME> <PREFIX> <PFX>	String, 63 characters max. 1-15 0-255/none	Add PBX profile with the specified name, prefix number and direct prefix number
config			Return to Configuration menu
exit			Exit from this configuration submenu to the upper level
flash mode	<PROFILE_INDEX> <FLASH>	0-31 none/ flash1/ flash2/ flash3	Flash signal transmission mode
history			View 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

4.2.2.25 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

4.2.2.26 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. <i>IP_ADDR</i> — IP address <i>SRV_IDX</i> — server number
acct port	<PORT> <SRV_IDX>	0-65535 0-8	Define the account server (Accounting) port <i>PORT</i> — port number <i>SRV_IDX</i> — server number
acct secret	<SECRET> <SRV_IDX>	String, 31 characters max. 0-8	Define the account server (Accounting) password <i>SECRET</i> — password <i>SRV_IDX</i> — server number
acct server_group	<SRV_GROUP_ID> <SRV_IDX>	0-3 0-7	Set the group for accounting server <i>SRV_GROUP_ID</i> — group number <i>SRV_IDX</i> — server number
antifraud ipaddr	<IP_ADDR> <SRV_IDX>	IP address in AAA.BBB.CCC.DDD format 0-8	Set IP address for verification node RADIUS server (Antifraud) <i>IP_ADDR</i> — IP address <i>SRV_IDX</i> — server number
antifraud port	<PORT> <SRV_IDX>	0-65535 0-8	<i>PORT</i> — port number <i>SRV_IDX</i> — server number
antifraud secret	<SECRET> <SRV_IDX>	string, 31 characters max. 0-8	Set a password for verification node RADIUS server (Antifraud) <i>SECRET</i> — password <i>SRV_IDX</i> — server number
antifraud server_group	<SRV_GROUP_ID> <SRV_IDX>	0-3 0-7	<i>SRV_GROUP_ID</i> — group number <i>SRV_IDX</i> — server number
antifraud mode	<RADIUS_ANTIFRAUD _MODE>	Off Astarta Intek Custom	Interaction disabled Interaction with verification node produced by LLC "Astarta" Interaction with verification node produced by LLC "Hexagon Labs" Interaction with third-party verification nodes
antifraud user	<RADIUS_ANTIFRAUD _USER>	string, 63 characters max.	Set the User-name attribute for Access- Request and Accounting-Request in Astarta mode
antifraud password	<RADIUS_ANTIFRAUD _PASSWORD>	string, 127 characters max.	Set the User-name attribute for Access- Request in Astarta mode

auth ipaddr	<IP_ADDR> <SRV_IDX>	IP address in AAA.BBB.CCC.DDD format 0-8	Set an IP address of authorization server <i>IP_ADDR</i> – IP address <i>SRV_IDX</i> – server number
auth local	<AUTH_LOCAL>	no/yes	Allow access to local administrator in case of RADIUS server deny
auth port	<PORT> <SRV_IDX>	0-65535 0-8	Set a port of authorization server <i>PORT</i> – port number <i>SRV_IDX</i> – server number
auth secret	<SECRET> <SRV_IDX>	string, 31 characters max. 0-8	Set a password for authorization server <i>SECRET</i> – password <i>SRV_IDX</i> – server number
auth server_group	<SRV_GROUP_ID> <SRV_IDX>	0-3 0-7	Set a group for authorization server <i>SRV_GROUP_ID</i> – group number <i>SRV_IDX</i> – server number
auth user	<AUTH_USER>	no/yes	web/telnet/ssh users authorization via RADIUS
config			Return to Configuration menu
deadtime	<DEADTIME>	5-60	Server unavailability time during failure — amount of time that the server is deemed unavailable (requests will not be sent to it)
exit			Exit from this configuration submenu to the upper level
history			View history of entered commands
iface	<IFACE_NAME>	String, 255 characters max.	Specify RADIUS network interface
profile	<PROFILE_INDEX>	0-31	Proceed to RADIUS profile parameters configuration
quit			Terminate this CLI session
retries	<RETRIES>	2-5	Specify the number of request transmission attempts
show config			Show the RADIUS server configuration information
timeout	<TIMEOUT>	3-10	Define the amount of time intended for server response (x100ms)
voice-msg-table	<TABLE_INDEX>	0-31	Select RADIUS responses to voice messages correspondence tables

4.2.2.26.1 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: <i>CdPN-IN</i> — use callee number prior to modification (received in SETUP/INVITE packet). <i>CdPN-OUT</i> — use callee number after the modification
acct CgPN	<CGPN_MODE>	CgPN-IN/CgPN-OUT	Define the caller number for Accounting-Request packets: <i>CgPN-IN</i> — use caller number prior to modification (received in SETUP/INVITE packet) <i>CgPN-OUT</i> — use caller number after the modification
acct duration count mode	<RADIUS_COUNT_MODE>	round-up/round-down/not-round	Time rounding parameters: up, down, not rounding (transmit milliseconds)
acct originate	<ON/OFF>	off/on	Enable/disable acct message transmission for call-orig=originate
acct restrict	<RESTRICT>	none/zone/local/emergency/restrict-all	Define the outgoing communications restriction during the server fault (server response non-reception): <i>none</i> — allow all calls <i>zone</i> — allow calls to emergency services, local and zone network <i>local</i> — allow calls to emergency services and local network <i>emergency</i> — allow calls to emergency services only <i>restrict</i> — deny all calls
acct start	<ON_OFF>	on/off	Enable/disable acct. start message transmission
acct stop	<ON_OFF>	on/off	Enable/disable acct. stop message transmission
acct update	<ON_OFF>	on/off	Enable/disable acct. update message transmission
acct update_period	<PERIOD>	10sec/20sec/30sec/45sec/1min/2min/3min/5min/10min/15min/30min/1hour	Acct. update message transmission period
acct unsuccessfull	<ON_OFF>	on/off	Enable/disable transmission of information on unsuccessful calls to RADIUS server

acct user-name answer	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk/cdpn/initial_cgpn/ initial_cdpn	<p>Set a User-Name attribute value in Accounting-Request packets for 'answer' party:</p> <p><i>cgpn</i> – use a caller phone number as the value</p> <p><i>ip_or_stream</i> – use a caller IP address or number of the stream via which the connection is implemented</p> <p><i>trunk</i> – use a name of the trunk, via which the connection is implemented, as the value</p> <p><i>cdpn</i> – use a callee number as the value</p> <p><i>initial_cgpn</i> – use the non-modified phone number of the calling number</p> <p><i>initial_cdpn</i> – use a non-modified phone number of the callee number</p>
acct user-name originate	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk/cdpn/initial_cgpn/ initial_cdpn	<p>Set a User-Name attribute value in Accounting-Request for originate party:</p> <p><i>cgpn</i> – use a caller phone number as the value</p> <p><i>ip_or_stream</i> – use a caller IP address or number of the stream via which the connection is implemented</p> <p><i>trunk</i> – use a name of the trunk, via which the connection is implemented, as the value</p> <p><i>cdpn</i> – use a callee number as the value</p> <p><i>initial_cgpn</i> – use a non-modified phone number of the calling number</p> <p><i>initial_cdpn</i> – use a non-modified phone number of the callee number</p>
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>	Rfc5090/ Rfc5090-no-challenge/ draft-sterman	Select subscriber authorization algorithm with dynamic registration through the RADIUS server. In DIGEST authorization, the password is transferred as a hash code; thus, it cannot be intercepted during traffic scanning

auth emergency-on-REJ	<PERMIT>	not-allow/allow	Enable/disable access to emergency services after reception of connection refuse from server
auth framedprotocol	<FRAMED_PROTOCOL>	none/PPP/ SLIP/ARAP/ Gandalf/Xylogics/ X75_Sync	Assign protocol during packet access utilization for RADIUS authentication requests <i>none</i> — packet access will be disabled
auth nas port type	<PORT_TYPE>	Async/ Sync/ ISDN_Sync/ ISDN_Async_v120/ ISDN_Async_v110/ Virtual/ PIAFS/ HDLC_Channel/ X25/ X75/ G3_Fax/ SDSL/ ADSL_CAP/ ADSL_DMT/ IDSL/ Ethernet/ xDSL/ Cable/ Wireless/ Wireless IEEE 802.1	Define NAS physical port type (server for user authentication), default value is Async
auth pass	<PASSWD>	Password, 15 characters max.	Specify User-Password attribute value in the corresponding RADIUS-Authorization packet
auth restrict	<RESTRICT>	none/zone/ local/emergency/ restrict-all	Define the outgoing communications restriction during the server fault (server response non-reception): <i>none</i> — allow all calls <i>zone</i> — allow calls to emergency services, local and zone network <i>local</i> — allow calls to emergency services and local network <i>emergency</i> — allow calls to emergency services only <i>restrict all</i> — deny all calls
auth service type	<SERVICE_TYPE>	none/ Login/ Framed/ Callback_Login/ Callback_Framed/ Outbound/ Administrative/ NAS_Prompt/ 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. <i>ignore</i> — ignore the limitation of the maximum call duration

			<p><i>use_rfc_session_timeout</i> — use Session-Timeout attribute value as the maximum call duration timeout</p> <p><i>use_cisco_h323_credit_time</i> — use Session-Time or Cisco VSA h323-credit-time attribute value as the maximum call duration timeout</p>
auth user-name answer	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk/cdpn/initial_cgpn/ initial_cdpn	<p>Set User-Name attribute value in Access-Request packets for answer party:</p> <p><i>cgpn</i> — use a caller phone number as the value</p> <p><i>ip_or_stream</i> — use a caller IP address or number of the stream via which the connection is implemented</p> <p><i>trunk</i> — use a name of the trunk, via which the connection is implemented, as the value</p> <p><i>cdpn</i> — use a callee number as the value</p> <p><i>initial_cgpn</i> — use a non-modified phone number of the calling number</p> <p><i>initial_cdpn</i> — use a non-modified phone number of the callee number</p>
auth user-name originate	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk/cdpn/initial_cgpn/ initial_cdpn	<p>Set User-Name attribute value in Access-Request packets for originate party:</p> <p><i>cgpn</i> — use a caller phone number as the value</p> <p><i>ip_or_stream</i> — use a caller IP address or number of the stream via which the connection is implemented</p> <p><i>trunk</i> — use a name of the trunk, via which the connection is implemented, as the value</p> <p><i>cdpn</i> — use a callee number as the value</p> <p><i>initial_cgpn</i> — use a non-modified phone number of the calling number</p> <p><i>initial_cdpn</i> — use a non-modified phone number of the callee number</p>
auth userpasswd	<ON_OFF>	on/off	Enable/disable custom passwords for SIP subscribers during authorization
modifiers table auth mode	MODTABLE_MODE	default/restricted	<p>An authorization mode of a number in RADIUS.</p> <p>restricted — only numbers, which match masks in the modifiers table, are authorized</p>

modifiers table acct mode	MODTABLE_MODE	default/restricted	A number accounting mode in RADIUS restricted – accounting is available only for numbers, which match masks in the modifiers table
modifiers table incoming called	<MODTBL_INDEX>	0-255/none	Define callee (CdPN) number modifier for the incoming connection in relation to Called-Station-Id, xpgk-dst-number-in fields of RADIUS-Authorization and RADIUS-Accounting messages
modifiers table incoming calling	<MODTBL_INDEX>	0-255/none	Define caller (CgPN) number modifier for the incoming connection in relation to Calling-Station-Id, xpgk-src-number-in fields of RADIUS-Authorization and RADIUS-Accounting messages
modifiers table incoming redirecting	<MODTBL_INDEX>	0-255/none	Set the redirection number modifier (RedirPN) in the h323-redirect-number field in the RADIUS-Authorization and RADIUS-Accounting messages
modifiers table outgoing called	<MODTBL_INDEX>	0-255/none	Define callee (CdPN) number modifier for the outgoing connection in relation to xpgk-src-number-out field of RADIUS-Authorization and RADIUS-Accounting messages
modifiers table outgoing calling	<MODTBL_INDEX>	0-255/none	Define caller (CgPN) number modifier for the outgoing connection in relation to xpgk-dst-number-out field of RADIUS-Authorization and RADIUS-Accounting messages
config			Return to Configuration menu
exit			Exit from this configuration submenu to the upper level
history			View history of entered commands
quit			Terminate this CLI session
reset voice- msg-table			Do not use RADIUS responses to voice messages correspondence tables
server_group	<SRV_GROUP>	0-3	A number of a group of RADIUS servers which will be used by the profile
set vmt-reply- attribute		h323-return-code/Reply- Message	Select an attribute that will be used for RADIUS-reject message analysis
set voice-msg- table	<TABLE_IDX>	[0-31]	Select RADIUS responses to voice messages correspondence tables
show			Show RADIUS profile configuration
use acct	<ON_OFF>	on/off	Enable/disable Accounting request transmission to the RADIUS server
use auth	<ON_OFF>	on/off	Enable/disable Authorization request transmission to the RADIUS server
use antifraud	<ON_OFF>	on/off	Enable/disable Antifraud request transmission to the RADIUS server of the verification node
use class as ss7cat	<ON_OFF>	on/off	Use AV-Pair Class for SS7 subscriber category transmission
use eltex-vsa	<ON_OFF>	on/off	Enable RCM service
use full cisco-vsa	<ON_OFF>	on/off	Use a full Cisco-VAS value for RCM service
use porta billing	<ON_OFF>	on/off	Enable/disable PortaBilling
use porta routing	<ON_OFF>	on/off	Enable/disable PortaRouting

use incoming called		original/processed	Define CdPN number transmitted in <i>xpgk-dst-number-in</i> field of RADIUS-Authorization and RADIUS-Accounting messages
use incoming calling		original/processed	Define CgPN number transmitted in <i>xpgk-dst-number-in</i> field of RADIUS-Authorization and RADIUS-Accounting messages
use snmp	<ON_OFF>	on/off	Send SNMP trap when applying the RADIUS server
use utc time	<ON_OFF>	on/off	Use time in UTC format

4.2.2.27 Callback authorization configuration mode

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

```
SMG1016M-[CONFIG]> auth calls
Entering Auth Calls mode.
SMG1016M-[CONFIG]-AUTH_CALLS>
```

Command	Parameter	Value	Action
?			Show the list of available commands
add number_pool	FIRST_NUMBER RANGE	phone number 1-65535	Add a pool of numbers – starting number and range
config			Return to Configuration menu
exit			Exit from this configuration submenu to the upper level
remove number_pool	INDEX	0-63	Delete a pool of numbers by its index
remove by id number_pool	POOL_ID	1-65535	Delete a pool of numbers by its identifier
set access category	CAT_IDX	0-127	Set access category
set category	CATEGORY	0-9	Set caller ID category
set number_pool first_number	INDEX NUMBER	0-63 phone number	Change the starting phone number in a pool of numbers
set number_pool range	INDEX RANGE	0-63 1-65535	Change a range in a pool of numbers by its index
set by id *	POOL_ID	1-65535	The commands work similarly to the set number_pool * commands, but by identifier
set numplan	PLAN_IDX	0-15 or none	Set a dial plan <i>none</i> – remove a dial plan
set pbx_profile	PROFILE	0-15 or none	Set a PBX profile <i>none</i> – remove a PBX profile
set radius_profile	RADIUS_PROFILE	0-31 or no	Set a RADIUS profile <i>none</i> – remove a RADIUS profile
set select_mode	SELECT_MODE	sequential/ random	Set the mode for selecting numbers from the pool <i>sequential</i> <i>random</i>
show number_pool all			Show all configured pools of numbers
show number_pool by id	POOL_ID	1-65534	Show a pool of numbers by its identifier

show number_pool by index	INDEX	0-63	Show a pool of numbers by its number
show user			Show virtual subscriber settings

4.2.2.28 Conversation recording settings configuration mode

To enter this mode¹, 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
ftp enabled	REC_FTP	no/yes	Save call records on the FTP server
ftp login	REC_FTPLOGIN	string of up to 63 characters	Login to access to FTP
ftp mode recording	REC_MODE	once-a-day/ once-an-hour/ once-an-minute	Upload mode – once a day, once an hour, once a minute
ftp passwd	REC_PASSWD	string of up to 63 characters	Password to access to FTP
ftp path	REC_FTPPATH	string of up to 63 characters	Path to the files on FTP
ftp period day	REC_HOUR REC_MINUTE	0-23 0-59	Set hours and minutes of uploading files to FTP for 'once a day' mode
ftp period hour	REC_MINUTE	0-59	Set minutes of uploading files to FTP for 'once an hour' mode
ftp port	REC_FTPPORT	1-65535	FTP server port
ftp remove-after-upload	REC_FTP_REMOVE	no/yes	Delete records from the local storage after uploading to FTP
ftp server	REC_FTPSERVER	string of up to 63 characters	An address or domain name of the FTP server
set action on full disk		stop-recording/remove-old-files	Select an action for full disk: Stop recording/Delete obsolete
set dirname		none or string, 63 characters max.	Define the name of directory for conversation recording files
set dirname_IVR		none or string, 63 characters max.	Define the name of directory for IVR conversation recording files
set files count per dir	FILECOUNT	100-65535 or unlimited	The quantity of record files in a single directory
set files keep period day	KEEP_DAY	0-90	The quantity of days of storing records on the local storage
set files keep period hour	KEEP_HOUR	0-23	The quantity of hours of storing records on the local storage
set notification	<NOTIFY_TYPE >	None voice_message	Notification on conversation recording start
set path		off/mnt/sd[abc][1-7]*	Define the path to conversation recording files storage

¹The menu is available for the devices with Call-record license. Read more detailed information on licenses in the section 4.1.25 Licenses.

4.2.2.29 Call records masks configuration modes

To enter this mode¹, execute 'mask' command in the configuration mode of call recording settings.

```
SMG2016-[CONFIG]-[RECORD]> mask
Entering Record-Mask mode.
SMG2016-[CONFIG]-[RECORD]-MASK>
```

Command	Parameter	Value	Action
?			Show the list of available command
exit			Exit from this configuration submenu to the upper level
add	REC_MASK_NUMPLAN RECORD_MASK REC_MASK_TYPE	0-255 or all String, max. 255 characters all/ calling/ called	Add a new record mask Parameters: <i>dial plan (all – any dial plan)</i> <i>record mask</i> which should be taken in brackets – (“ and “)” <i>number type</i> – any, calling, called
modify category	RECORD_MASK_INDEX CAT_IDX	0-4095 0-31	Change call record category for a mask
modify direction	RECORD_MASK_INDEX REC_MASK_TYPE	0-4095 all/ calling/ called	Change mask number type to a defined one
modify mask	RECORD_MASK_INDEX PREFIX_MASK	0-4095 String, max. 255 characters	Change mask value The mask must be taken in brackets (“ and “)”
modify notification	RECORD_MASK_INDEX NOTIFY_TYPE	0-4095 none/voice_message	Notification on a record start <i>none</i> – do not notify <i>voice_message</i> – notify by voice message
modify numplan	RECORD_MASK_INDEX REC_MASK_NUMPLAN	0-4095 or none/ voice_message 0-255 or all	Change a dial plan
remove	RECORD_MASK_INDEX	0-4095	Delete a mask
show			Show all the masks

¹ The menu is available for the devices with Call-record license. Read more detailed information on licenses in the section 4.1.25 Licenses.

4.2.2.30 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: <i>DESTINATION</i> — destination IP address <i>MASK</i> — network mask for the specified IP address <i>GATEWAY</i> — gateway IP address <i>METRIC</i> — metrics <i>IFACE_NAME</i> — network interface <i>ENABLE</i> — enable/disable network route
route del	<IDX>	0-4095	Remove route: <i>IDX</i> — network route index
show			Show the route configuration information

4.2.2.31 Q.850 release causes list configuration

To enter this mode, execute 'release cause list' <LIST_INDEX> command in the configuration mode, where <LIST_INDEX> is a number of Q.850 release cause list.

```
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

4.2.2.32 SIP/SIP-T general settings editing mode

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

```
SMG-[CONFIG]> sip configuration
Entering SIP/SIP-T/SIP-I/SIP-profile config mode.
SMG-[CONFIG]-SIP(general)>
```

Command	Parameter	Value	Action
?			Show the list of available commands
cause codes KZ	<ON_OFF>	on/off	Enable/disable the specification in accordance with the requirements of the Republic of Kazakhstan
config			Return to Configuration menu
dynamic route profile	<PROFILE>	0-63	SIP profile for dynamic routing
exit			Exit from this configuration submenu to the upper level
history			View history of entered commands
ignore_RURI		no/yes	Ignore/do not ignore address in R-URI. Address information after '@' separator in Request-URI will be ignored; otherwise, the gateway will check if the address information matches to the device IP address and host name, and if there is no match, the call will be rejected
port destination	<PORT>	1-65535	Define the server port for syslog messages receiving and transmission
port source	<PORT>	1-65535	Define SMG port for messages receiving and transmission
quit			Terminate this CLI session
ringing timeout	<RING_TIMER>	10-255	Call response timeout
save_database	on/off		Save/do not save the information on registered subscribers into the gateway non-volatile memory. It allows you to keep the registered subscribers' database

			in case of device reboot due to power loss or failure. In case of reboot from the WEB or CLI, the gateway will store the current database into the non-volatile memory regardless of this setting
show			Show SIP-T general configuration
T1	<T1_TIMER>	0-255	Define SIP timer T1
T2	<T2_TIMER>	0-255	Define SIP timer T2
T4	<T4_TIMER>	0-255	Define SIP timer T4
transport	<TRANSPORT>	UDP-only/ UDP-prefer/ TCP-prefer/ TCP-only	Define transport layer protocol used for SIP message transmission and reception: <i>TCP-prefer</i> — reception via UDP and TCP. Transmission via TCP. If TCP connection was not established, transmission will be performed via UDP <i>UDP-prefer</i> — reception via UDP and TCP. Packets exceeding 1300 bytes will be sent via TCP, under 1300 bytes — via UDP <i>UDP-only</i> — use UDP protocol only <i>TCP-only</i> — use TCP protocol only
write_timeout	<TIMEOUT>	1hour/ 2hours/ 4hours/ 6hours/ 8hours/ 12hours/ 16hours	Define archive database update period (from 1 to 16 hours)

4.2.2.33 SIP/SIP-T interface parameter configuration mode

To enter this mode, execute 'sip interface <SIPT_INDEX>' command in the configuration mode, where <SIPT_INDEX> is SIP/SIP-T interface number.

```
SMG-[CONFIG]> sip interface 0
Entering SIPT-mode.
SMG-[CONFIG]-SIP/SIPT-INTERFACE[0]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
access category	<CAT_IDX>	0-31	Define the access category
alarm indication	<on/off>		Enable interface unavailability fault indication
category mode	<MODE>	none category cpc cpc-rus	Do not transfer Caller ID category to SIP. Transfer Caller ID category in the specified field, 'none' — do not transfer Caller ID category to SIP
CCI	<on/off>	on/off	Enable support for the channel integrity check
cdpn default	<CDPN>	Up to 30 digits or 'none'	cgpn by default, in case of calls implemented through the interface with trunk registration
cdpn plus sign	<YES/NO>	no/yes	"+" (plus) symbol transmission in international calls. Enables by default

cgpn replace	<YES_NO>	no/yes	Take CgPN from the 'Username/Number' parameter; when disabled, use CgPN number received in the incoming call
clearchan override	<on/off>	<on/off>	Set 'clear channel override' option – announce CLEARMOD codec to second leg when first leg operates in 'clear channel' operation mode
clearchan transit	<on/off>	<on/off>	Set 'clear channel transit' option – transmitted RTP should be exactly the same with the RTP transmitted to the first leg (including packetization time)
codec disable	<CODEC_IDX>	0-5	Enable defined codec. Codecs are numbered by priority – from 0 (the highest) to 5 (the lowest)
codec pte	<CODEC_IDX> <PTE>	0-5 10/20/30/40/50/ 60/70/80/90	Set payload time
codec ptype	<CODEC_IDX> <PTYPE>	0-5 0-127 or static	Set payload type. The static value sets the default value according to defined codec
codec set	<CODEC_IDX> <CODEC>	0-5 G.711-U/ G.711-A/ G.729/ G.723.1_5.3/ G.723.1_6.3	Set codec which is used
command line	<command>	Allowed symbols: [0-9a-zA-Z-_.!~*'();:=\$,%#] always inside []. For clearing use 'none'	SIP advanced settings
config			Return to Configuration menu
diversion use sip-uri	<YES_NO>	no/yes	When the option is enabled, the number in the Diversion header will always be transmitted as SIPURI
dname_rpid	<YES_NO>	no/yes	Enable/disable the 'Send DisplayName in the Remote-Party-ID header' option
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 allow_inband_DTMF	<DTMF_ALLOW_INBAND>	no/yes	Allow inband DTMF
DTMF mime type	<MIME_TYPE>	application/dtmf application/dtmf-relay	Specify payload type used for DTMF transmission in SIP protocol INFO packets application/dtmf — in SIP INFO application/dtmf packets ('*' and '#' are sent as digits 10 and 11) application/dtmf-relay — in SIP INFO application/dtmf-relay packets ('*' and '#' are sent as symbols '*' and '#')
DTMF mode	<DTMF_m>	inband/ RFC2833/ SIP-INFO/ SIP-NOTIFY	DTMF mode for the current interface
DTMF payload	<DTMF_p>	96-127	Define payload type for RFC2833

DTMF payload-equal	<DTMF_PT_EQ>	(off/on)	Enable/disable option 'Same RFC2833 PT'
duplicate enable	<YES_NO>	no/yes	Enable incoming INVITE redundancy mode
duplicate primary host	<REM_IPADDR> <REM_PORT>	IP address in AAA.BBB.CCC.DDD format 0-65535	Define address and port of primary duplicate server
duplicate secondary host	<REM_IPADDR> <REM_PORT>	IP address in AAA.BBB.CCC.DDD format 0-65535	Define address and port of back-up duplicate server
early media header	<early media header>	(off/on)	Enable P-Early-Media support (RFC5009)
ecan	<CANCELLATION>	voice/ nlp-off-voice/ modem/ off	Set echo cancellation mode: <i>Voice</i> — echo cancellers are enabled (this mode is set by default) <i>Nlp-off-voice</i> — 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 <i>Modem</i> — echo cancellers are enabled in the modem operation mode (direct component filtering is disabled, NLP control is disabled, CNG is disabled) <i>Off</i> — disable echo cancellation
exit			Exit from this configuration submenu to the upper level
egress_lines	<COUNT>	0-65535	Set the number of outgoing lines per SIP interface 0 — no restrictions
history			View history of entered commands
fax detection	<DETECTION>	no/callee/caller/ callee_and_caller	Set the fax detection mode: <i>no</i> — disable fax detection <i>callee</i> — for the receiving party only <i>caller</i> — for the transmitting party only <i>callee_and_caller</i> — for both receiving and transmitting parties
fax mode	<MODE>	T38_only/ G.711_only/ T38 and G.711	Select fax transmission mode
fill empty display-name	FILL_DNAME	on/off	Fill display-name when the call without display-name is received
gain rx	<GAIN>	-140 - 60	Set the volume of voice reception (gain of the signal received from the communicating gateway and output to the speaker of the phone unit connected to SMG gateway)
gain tx	<GAIN>	-140 - 60	Volume of voice transmission (gain of the signal received from the

			microphone of the phone unit connected to SMG gateway and transmitted to the communicating gateway)
history			View history of entered commands
hold mode		flash/ flash/star flash/hash flash/star/hash	Call hold by pressing: — flash — flash or * — flash or # — flash, * or #
hostname clear			Remove host name of the communicating gateway
hostname set	<HOSTNAME>	string, 63 characters max.	Define host name of the communicating gateway
ignore RURI/To diff	<IGNORE_RURI_TO_DIFF>	off/on	When enabled, the option will not transmit Redirecting and Original Called numbers to SS7 if there are differences in the SIP RURI and To fields
inband_signal_with_183_and_sdp	on/off		Issue reply 183/SDP to SIP answer for voice channel forwarding after reception of CALL PROCEEDING or PROGRESS messages from ISDN PRI containing progress indicator=8 (In-band signal)
ingress_lines	<COUNT>	0-65535	Set the number of incoming lines per SIP interface 0 — no restrictions
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: <i>non-immediate</i> — gradual <i>immediately</i> — instant
jitter deletion mode	<JT_DM>	soft/hard	Specify buffer adjustment mode. Defines the method of packet deletion during buffer adjustment to lower limit: <i>soft</i> — device uses intelligent selection pattern for deletion of packets that exceed the threshold <i>hard</i> — 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: <i>adaptive</i> — adaptive <i>non-adaptive</i> — 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. <i>SIP-OPTIONS</i> — direction availability control that utilizes OPTIONS requests <i>SIP-NOTIFY</i> — direction availability control that utilizes NOTIFY requests <i>UDP-CRLF</i> — direction availability control that utilizes empty UDP packet transmission
keep-alive period	<KEEP_ALIVE_PERIOD>	30-3600	Request transmission period
lines_mode	<LINES_MODE>	common/ separate	Line operating mode: combined/ separated
local ringback	<on/off>	on/off	Enable 'Local ringback for early-media' option
login	<LOGIN>	string, 15 characters max.	Specify the name used for authentication
max_active	<MAX_ACTIVE>	0-65535	Define the maximum number of active connection for an interface
mode	<mode>	profile/ SIP/ SIP-T/ SIP-I/ SIP-Q	Define interface operation mode (SIP profile is assigned to SIP subscribers)
name	<s_name>	you may use letters, numbers, '_' character, 31 characters max.	Define the interface name
nat	<NAT>	enable/disable	Enable/disable NAT
net-interface rtp	<IFACE_NAME>	string, 255 characters max.	Specify RTP network interface
net-interface sig	<IFACE_NAME>	string, 255 characters max.	Specify SIP network interface
numbering plan	<NUMPLAN>	0-15/0-255	Select dial plan
options	<OPTIONS>	enable/disable	Enable direction availability control function that utilizes OPTIONS requests; when the direction is not available, the call will be performed through the redundant trunk group. Also, this function analyzes received OPTIONS message responses, that allows to avoid usage of 100rel, replaces and timer features configured in this direction if the opposite party supports them
options period	<OPTIONS_PERIOD>	30-3600	Define the time in seconds that should pass for the call to be performed through the redundant trunk group when the direction is not available
password	<PASSWD>	string, 15 characters max.	Specify the password used for authentication

port	<PORT>	1-65535	Define UDP port of the communicating gateway used for SIP signalling reception
quit			Terminate this CLI session
radius profile	<RADIUS_PROFILE>	number [0-31] or 'no'	Define RADIUS profile for the SIP profile interface <i>no</i> — do not use the profile for an interface
Re-INVITE a=sendonly		on/off	Enable Re-INVITE processing with a=sendonly
redirection 302	<REDIRECTION>	on/off	Enable/disable redirection (302) utilization
redirection server	<REDIRECT_SERV>	on/off	Redirect/do not redirect the call sent using the public address to the subscriber's private address without the dial plan routing. The routing will be performed directly to the address contained in the reply 302 'contact' header received from the redirection server. You should configure redirection 302 first (<i>redirection 302</i> 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	<i>Off</i> —100rel tag transmission disabled When <i>support</i> option is enabled, INVITE request and 1xx class provisional responses will contain the support: 100rel tag that requires assured confirmation of provisional responses When <i>require</i> option is enabled, INVITE request and 1xx class provisional responses will contain the require: 100rel tag that requires assured confirmation of provisional responses
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 sends control packets via RTCP protocol
RTP loss silence	<RTP_TIMEOUT_SILENCE>	1-30	Define the RTP packet timeout for the silence suppression option utilization. Coefficient is a multiplier that applies to the 'RTP-loss timeout' value
RTP loss timeout	<RTP_TIMEOUT>	10-300/ off	Define the RTP packet timeout

sdp_in_18x	<ON_OFF>	on/off	Always send SDP in provisional replies
sipdomain	<SIPDOMAIN>	IP address in AAA.BBB.CCC.DDD format	Define the registration domain address
show config			Show the interface information
sipcause profile	<SIPCAUSE>	[0-63]/none	Select Q.850 and sip-reply compliance profile
sms port	<PORT>	0-65535	Port for SMS receiving via SMPP and redirecting them to duplication server
src verify	<ON_OFF>	on/off	Control the media traffic reception from IP address and UDP port specified in SDP(on) communication session description; otherwise the traffic from any IP address and UDP port will be accepted
STUN ip	<IPADDR>	IP address in AAA.BBB.CCC.DDD format	Define STUN server IP address
STUN period	<PERIOD>	10-1800/0	Define the time interval between requests
STUN port	<PORT>	1-65535	Define STUN server port for request transmission (default value is 3478)
STUN use	<YES_NO>	yes/no	Enable/disable STUN
subnet mask clear			Delete subnet mask for incoming calls
subnet mask set	<SUBNET>	a string of up to 63 characters in the form of subnet mask: AAA.BBB.CCC.DDD	Set subnet mask for incoming calls
subscribers max_forwardings	<MAX_FORWARDINGS>	5/10	Maximum number of redirects between subscribers
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: <i>local TCF</i> — method requires that the TCF tuning signal was generated locally by the recipient gateway <i>transferred TCF</i> — 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, <i>off</i> — 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 ' <i>timer sessions expires</i> '
timer session expires	<EXPIRES>	90-64800	Define the time in seconds that should pass before the forced session termination, if the session is not renewed in time
transit sip header	YES_NO	no/yes	Allow transit of SIP headers from this call leg to another
trunk	<TRUNK>	0-31	Define the trunk group number for an interface
trusted network	<YES_NO>	yes/no	Select 'trusted network' option
username	<USERNAME>	String, 15 characters max.	Specify username for authentication
VAD_CNG	<ON_OFF >	on/off	Enable/disable voice activity detector/ Comfort noise generator for an interface
vbd codec	<CODEC>	G.711-U, G.711-A	Codec used for VBD data transmission
vbd enable			Enable V.152
vbd disable			Disable V.152
vbd payload type	<VBD_p>	Static, 96-127	Payload type used for VBD codec
flash processing		on/off	Process flash signal

4.2.2.34 Interface subscriber registration parameter configuration mode

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

```
SMG-[CONFIG]> sip registration
Entering sip-registration mode.
SMG-[CONFIG]-SIP-REGISTRATION>
```

Command	Parameter	Value	Action
?			Show the list of available commands
add one			Add a new account
count			Show the number of created accounts
exit			Exit from this configuration submenu to the upper level
history			View history of entered commands
config			Return to Configuration menu
quit			Terminate this CLI session
remove	<INDEX>	0-3000	Remove the specified account
set authname	<INDEX> <NAME>	0-3000 String, 63 characters max.	Specify the name used for authentication
set authpass	<INDEX> <NAME>	0-3000 String, 63 characters max.	Specify the password used for authentication
set sipdomain	<INDEX> <NAME>	0-3000 String, 63 characters max.	Define the registration domain
set username	<INDEX> <NAME>	0-3000 String, 63 characters max.	Define the user name for registration
show all			Show the information on all created accounts
show one	<ONE_INDEX>	0-3000	Show the information on account with the specified number

4.2.2.35 SIP subscribers parameter configuration mode¹

To enter this mode¹, 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>	0-1999/0-2999	Remove the current user
savedb			Save the information on registered subscribers in the gateway non-volatile memory. It allows you to keep the registered subscribers' database in case of device reboot due to power loss or failure. In case of reboot from the WEB or CLI, the gateway will store the current database into the non-volatile memory regardless of this setting
service user	<INDEX>	0-1999/0-2999	Switch to the VAS configuration mode for the specified subscriber
service group	<INDEX>	0-63	Switch to the VAS configuration mode for the specified group
set authorization	<INDEX> <AUTHMODE>	0-1999/0-2999 none/register/ register_and_invite	Set user authorization mode <i>INDEX</i> – SIP subscriber index; <i>AUTHMODE</i> – authorization mode: <i>None</i> – do not ask for authorization, <i>register</i> – ask while registration, <i>register_and_invite</i> – ask while registration and egress calls ringing
set user allow unregistered	<INDEX> <ON_OFF>	0-1999/0-2999 off/on	Allow calls without registration
set user access category	<INDEX> <CAT_IDX>	0-1999/0-2999 0-31	Assign the category for the specified subscriber
set user access mode	<INDEX> <ACCESS>	0-1999/0-2999 Off/On/Off_1/ Off_2/Denied_1/ Denied_2/Denied_3/ Denied_4/Denied_5/ Denied_6/Denied_7/ Denied_8/Exclude	Define the service mode for the specified subscriber
set user blf groupID	<INDEX> <GROUP_ID>	0-1999/0-2999 0-15	Set a monitoring group (BLF subscription group)

¹ The menu is only available in the software version that supports the SIP registrator.

set user blf subscribers	<INDEX> <BLF_SUBS>	0-1999/0-2999 0-200	Set the maximum number of BLF subscribers for the party (subscriber)
set user blf usage	<INDEX> <ON_OFF>	0-1999/0-2999 off/on	Permit BLF subscription to a subscriber
set user category	<INDEX> <CATEGORY>	0-1999/0-2999 0-9	Set a CallerID category for the specified subscriber <i>INDEX</i> – SIP subscriber index <i>CATEGORY</i> – CallerID category
set user cliro	<INDEX> <ON_OFF>	0-1999/0-2999 off/on	Enable CLIRO service (define a hidden number)
set user display name rule	<INDEX> <USE_DISPLAY_NAME>	0-1999/0-2999 received_only/ received_prefer/ configured_only	Displayed name utilization mode: <i>received_only</i> – always use only received name <i>received_prefer</i> – if there is no a received displayed name, use a configured displayed name <i>configured_only</i> – always use a configured displayed name
set user display name value	<INDEX> <DISPLAY_NAME>	0-1999/0-2999 string, max 40 characters or none	Subscriber displayed name <i>none</i> – clear the displayed name
set user domain	<INDEX> <DOMAIN>	0-1999/0-2999 string of up to 15 characters	Set a SIP domain for a subscriber <i>INDEX</i> – SIP subscriber index <i>DOMAIN</i> – domain name
set user egress lines	<INDEX> <COUNT>	0-1999/0-2999 1-255 or 0	Set the number of simultaneous egress calls, in which the subscriber participates, for lines separate operation mode. The range of available values [1;255] or 0 – no limit
set user ingress lines	<INDEX> <COUNT>	0-1999/0-2999 1-255 or 0	Set the number of simultaneous ingress calls, in which the subscriber participates, for lines separate operation mode. The range of available values [1;255] or 0 – no limit
set user intercom header	<HEADER> <INDEX>	AIAA/AII/AIIAA/AIII/AIIRA/AIRA/AMO/CIAA/CIESAA/CISSAA 0-1999/0-2999	Set a SIP header for intercom: AIAA – Alert-Info: Auto Answer AII – Alert-Info: Intercom' for user AIIAA – Alert-Info: info=alert-autoanswer AIII – Alert-Info: info=intercom AIIRA – Alert-Info: info=RingAnswer AIRA – Alert-Info: Ring Answer AMO – Answer-Mode: Auto CIAA – Call-Info: ;answer-after=0 CIESAA – Call-Info: =\;answer-after=0 CISSAA – Call-Info: \\\;answer-after=0
set user intercom mode	<INDEX>	0-1999/0-2999	Intercom operation mode: <i>sendonly</i> – one-sided

	<MODE>	sendonly/ sendrecv/ ordinary/ reject	<i>sendrecv</i> – double-sided <i>ordinary</i> – a common call (without intercom headers transmission) <i>reject</i> – do not use intercom
set user intercom priority	<INDEX> <PRIORITY>	0-1999/0-2999 1-5	Set the priority for intercom operation
set user intercom timer	<INDEX> <TIMER>	0-1999/0-2999 0-255	A pause before answer. It is used while SIP headers transmission with <i>answer-auto</i> parameter
set user ipaddr	<INDEX> <IPADDR>	0-1999/0-2999 IP address in AAA.BBB.CCC.DDD format	Set an IP address for the specified subscriber
set user lines	<INDEX> <COUNT>	0-1999/0-2999 1-255 or 0	Set the number of simultaneous calls, in which the subscriber participates, for lines common operation mode. The range of available values [1;255] or 0 – no limit
set user lines- mode	<INDEX> <LINES_MODE>	0-1999/0-2999 common/separate	The mode of simultaneous calls limiting. <i>common</i> – common limiting of ingress and egress calls <i>separate</i> – separate limiting of ingress and egress calls
set login	<INDEX> <LOGIN> <PASSWORD>	0-1999/0-2999 string, max 63 characters string, max 63 characters	Set user name and password for authentication
set user name	<INDEX> <NAME>	0-1999/0-2999 string, max 31 characters	Set SIP subscriber name
set user no- source-port- control	<INDEX> <ON_OFF>	0-1999/0-2999 off/on	Do not consider source-port after registration
set user number	<INDEX> <NUMBER>	0-1999/0-2999 subscriber number	Set SIP subscriber number
set user numberAON	<INDEX> <NUMBER>	0-1999/0-2999 subscriber number	Set CallerID number for the specified subscriber
set user numberAON-for- redirection	<INDEX> <NUMBER>	0-1999/0-2999 subscriber number	Use CallerID while redirection
set user numberList	<INDEX> <NUM_IDX> <NUMBER>	0-1999/0-2999 0-15/0-255 [number]/none	Set additional subscriber number in a specified dial plan <i>none</i> – clear the number
set user numplan	<INDEX> <PLAN_IDX>	0-1999/0-2999 0-15/0-255	Set dial plan for the subscriber
set user pbx_profile	<INDEX> <PROFILE>	0-1999/0-2999 0-31	Set PBX profile for SIP subscriber
set user Re- INVITE a=sendonly	<INDEX> <HOLD>	0-63 off/on	Enable hold service when re-invite with a=sendonly feature is received

set user redirection	<INDEX> <REDIRECTION>	0-63 off/on	Permit/deny redirection (302) from a subscriber
set group access category	<INDEX> <CAT_IDX>	0-63 0-31	Set access category for subscribers group
set group blf groupID	<INDEX> <GROUP_ID>	0-63 0-15	Set BLF monitoring group (BLF subscribers group)
set group blf subscribers	<INDEX> <BLF_SUBS>	0-63 0-200	Set the maximum number of blf subscribers for the party (subscriber)
set group blf usage	<INDEX> <ON_OFF>	0-63 off/on	Enable subscription on events
set group category	<INDEX> <CATEGORY>	0-63 0-9	Set Caller ID category for the specified group <i>INDEX</i> – SIP subscriber index <i>CATEGORY</i> – CallerID category
set group cliro	<INDEX> <ON_OFF>	0-63 off/on	Enable CLIRO service (hidden number identification).
set group domain	<INDEX> <DOMAIN>	0-63 string, max 15 characters	Set SIP-domain for a group <i>INDEX</i> – SIP subscriber index <i>DOMAIN</i> – domain name
set group egress lines	<INDEX> <COUNT>	0-63 1-255 or 0	Set the quantity of simultaneous egress calls, in which a subscriber of the group participates, for separate line mode. The range of available values [1;255] or 0 – no limit
set group ingress lines	<INDEX> <COUNT>	0-63 1-255 or 0	Set the quantity of simultaneous ingress calls, in which a subscriber of the group participates, for separate line mode. The range of available values [1;255] or 0 – no limit
set group intercom header	<HEADER> <INDEX>	AIAA/AII/AIIAA/AIII/AIIRA/AIRA/AMO/CIAA/CISSAA 0-63	Set a SIP header for intercom: AIAA – Alert-Info: Auto Answer AII – Alert-Info: Intercom' for user AIIAA – Alert-Info: info=alert-autoanswer AIII – Alert-Info: info=intercom AIIRA – Alert-Info: info=RingAnswer AIRA – Alert-Info: Ring Answer AMO – Answer-Mode: Auto CIAA – Call-Info: ;answer-after=0 CISSAA – Call-Info: =\;answer-after=0 CISSAA – Call-Info: \\;answer-after=0
set group intercom mode	<INDEX> <MODE>	0-63 sendonly/ sendrecv/ ordinary/ reject	Intercom operation mode: <i>sendonly</i> – one-sided <i>sendrecv</i> – double-sided <i>ordinary</i> – an ordinary call (without intercom headers transmission) <i>reject</i> – do not use intercom
set group intercom priority	<INDEX> <PRIORITY>	0-63 1-5	Set the priority for intercom operation
set group intercom timer	<INDEX> <TIMER>	0-63 0-255	A pause before answer. It is used while SIP headers transmission with answer-auto parameter
set group lines	<INDEX> <COUNT>	0-63 1-255 or 0	Set the number of simultaneous calls in which a subscriber of the group

			participates for lines common operation mode. The range of available values [1;255] or 0 – no limit
set group lines-mode	<INDEX> <LINES_MODE>	0-63 common/separate	The mode of simultaneous calls limiting. <i>common</i> – common limiting of ingress and egress calls <i>separate</i> – separate limiting of ingress and egress calls
set group max	<INDEX> <MAX_REG>	0-63 0-1999/0-2999	Set the quantity of subscribers in the group
set group name	<INDEX> <NAME>	0-63 string, max 31 characters	Set the group name
set group numplan	<INDEX> <PLAN_IDX>	0-63 0-15/0-255	Set the group dial plan
set group no-source-port-control	<INDEX> <ON OFF>	0-63 off/on	Do not consider source-port after registration
set group pbx_profile	<INDEX> <PROFILE>	0-63 0-31	Set a PBX profile for the group
set group profile	<INDEX> <PROFILE>	0-63 0-31	Set a SIP profile for the group
set group Re-INVITE a=sendonly	<INDEX> <HOLD>	0-63 off/on	Enable hold service when re-invite with a=sendonly feature is received
set group redirection	<INDEX> <REDIRECTION>	0-63 off/on	Permit/deny redirection (302) from a group
set group refer	<INDEX> <REFER>	0-63 off/on	Enable call transfer with the help of REFER message
show count			Show the quantity of SIP subscribers
show list			Show the list of SIP subscribers
show user	<INDEX>	0-1999/0-2999	Display information on a SIP subscriber
show group	<INDEX>	0-63	Display information on a group

4.2.2.35.1 Subscriber VAS configuration mode

To enter this mode, execute 'service <USER_INDEX>' command in the RADIUS configuration mode, where USER_INDEX is a SIP subscriber index.

```
SMG-[CONFIG]-SIP-USERS> service 0
Entering User-Service mode for user 0
SMG-[CONFIG]-[SIP-USERS][0]-SERVICE>
```

Command	Parameter	Value	Action
?			Show the list of available commands
attach service block			Enable VAS for subscriber
detach service block			Disable VAS for subscriber
exit			Exit from this configuration submenu to the upper level
quit			Terminate this CLI session
set call-pickup enable	<ON_OFF>	off/on	Enable 'call pickup' service
set cfb enable	<ON_OFF>	off/on	Enable 'call forwarding on busy' service
set cfb number	<Number>	number of up to 30 characters or none	Set a number for 'call forwarding on busy', none – disable the service.
set sfnr enable	<ON_OFF>	off/on	Enable 'call forwarding on no-reply' service
set sfnr number	<Number>	number of up to 30 characters or none	Set a number for 'call forwarding on no-reply', none – disable the service
set cfos enable	<ON_OFF>	off/on	Enable 'call forwarding on out of service' service
set cfos number	<Number>	number of up to 30 characters or none	Set a number for 'call forwarding on out-of-service', none – disable the service
set cfu enable	<ON_OFF>	off/on	Enable 'call forwarding unconditional' service
set cfu number	<Number>	number of up to 30 characters or none	Set a number for 'call forwarding unconditional', none – disable the service
set clear-all enable	<ON_OFF>	off/on	Enable 'reset all services'
set conf-3way enable	<ON_OFF>	off/on	Enable '3-way conference' service. The 'call hold' service must be activated
set conference enable	<ON_OFF>	off/on	Enable 'conference add-on' service
set ct enable	<ON_OFF>	off/on	Enable 'call transfer' service. The 'call hold' service must be activated.
set hold enable	<ON_OFF>	off/on	Enable 'call hold' service
set intercom enable	<ON_OFF>	off/on	Enable 'intercom' service
set one_touch_record enable	<ON_OFF>	off/on	Enable 'one touch record' service
set password change enable	<ON_OFF>	off/on	Enable 'change password' service
set password restrict out access active	<ON_OFF>	off/on	Activate a password for 'password activation' service. The 'on' value makes the password active and call restrictions get invalid
set password restrict out access enable	<ON_OFF>	off/on	Enable 'password activation' service. The 'outgoing calls restriction' service must be activated

set password restrict out once enable	<ON_OFF>	off/on	Enable 'restricted by password' service. The 'outgoing calls restriction' service must be activated first
set password value	<VALUE>	string of 4 characters	Set a password for 'outgoing calls restriction' service
set restrict out enable	<ON_OFF>	off/on	Enable 'outgoing calls restriction' service
set restrict out value	<ACCESS_MODE>	On/ Denied_6/ Denied_7/ Denied_8	Outgoing calls restriction mode: On – all calls are permitted Denied_6 – only calls to emergency services are permitted Denied_7 – only local, department and emergency calls are permitted Denied_8 – only local, department, zone and emergency calls are permitted
set anonymous_call enable	<ON_OFF>	off/on	Enable 'anonymous call' service
set anonymous_call active	<ON_OFF>	off/on	Activate 'anonymous call' service
Set reject_anonymous_calls enable	<ON_OFF>	off/on	Enable 'reject anonymous calls' service
set reject_anonymous_calls active	<ON_OFF>	off/on	Activate 'reject anonymous calls' service
set reminder enable	<ON_OFF>	off/on	Enable 'reminder' service
show			Show the current VAS settings
show count			Show the quantity of free VAS blocks

4.2.2.36 Subscribers group's VAS configuration mode

To enter this mode, execute 'service group <USER_INDEX>' command (where USER_INDEX is a SIP subscriber index) in the SIP subscriber configuration mode.

```
SMG2016-[CONFIG]-SIP-USERS> service group 0
Entering UserGroup-Service mode for user-group 0
SMG2016-[CONFIG]-[SIP-USERS][0]-GROUP-SERVICE>
```

Command	Parameter	Value	Action
?			Show the list of available commands
attach service blocks manual			The mode of VAS activation for the subscribers group is manual
attach service blocks radius			The mode of VAS activation for the subscribers is through the RADIUS
detach service block			Disable VAS for the group
exit			Exit this configuration submenu to the menu on the upper level
quit			Terminate the current CLI session
set call-pickup enable	<ON_OFF>	off/on	Enable 'call pick-up' service
set cfb enable	<ON_OFF>	off/on	Enable 'call forwarding on busy' service
set cfb number	<Number>	a number of 30 characters or none	Set a number for call forwarding on busy. None – disable call forwarding
set sfnr enable	<ON_OFF>	off/on	Enable 'call forwarding on no-reply' service
set sfnr number	<Number>	a number of 30 characters or none	Set a number for 'call forwarding on no-reply' service. None – disable call forwarding
set cfos enable	<ON_OFF>	off/on	Enable 'call forwarding on out-of-service' service
set cfos number	<Number>	a number of 30 characters or none	Set a number for 'call forwarding on out-of-service' service. None – disable call forwarding
set cfu enable	<ON_OFF>	off/on	Enable 'call forwarding unconditional' service
set cfu number	<Number>	a number of 30 characters or none	Set a number for 'call forwarding unconditional' service. None – disable call forwarding
set clear-all enable	<ON_OFF>	off/on	Enable 'reset all services'
set conf-3way enable	<ON_OFF>	off/on	Enable '3-way conference' service. The 'call hold' service must be activated
set conference enable	<ON_OFF>	off/on	Enable 'conference add-on' service
set ct enable	<ON_OFF>	off/on	Enable 'call transfer' service. The 'call hold' service should be activated first
set hold enable	<ON_OFF>	off/on	Enable 'call hold' service
set intercom enable	<ON_OFF>	off/on	Enable 'intercom' service
set password change enable	<ON_OFF>	off/on	Enable 'change password' service

set password restrict out access active	<ON_OFF>	off/on	Activate a password for 'password activation' service. The 'on' value makes the password active and call restrictions get invalid
set password restrict out access enable	<ON_OFF>	off/on	Enable 'password activation' service. The 'outgoing calls restriction' service should be activated first
set password restrict out once enable	<ON_OFF>	off/on	Enable 'restricted by password' service. The 'outgoing calls restriction' service should be activated first
set password value	<VALUE>	a string of 4 characters	Set a password for 'outgoing calls restriction' service
set restrict out enable	<ON_OFF>	off/on	Enable 'outgoing calls restriction' service
set restrict out value	<ACCESS_MODE>	On/ Denied_6/ Denied_7/ Denied_8	Outgoing calls restriction mode: <i>On</i> – all calls are permitted; <i>Denied_6</i> – only calls to emergency services are permitted <i>Denied_7</i> – only local, department and emergency calls are permitted <i>Denied_8</i> – only local, department, zone and emergency calls are permitted
show			Show the current VAS settings
show count			Show the quantity of free VAS blocks

4.2.2.37 PRI-subscribers' parameters configuration mode

To enter this mode, execute the 'pri-users' command in configuration mode.

```
SMG2016-[CONFIG]> pri-users
Entering SIP-Users mode.
SMG2016-[CONFIG]-[PRI-USERS]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
add user	<NUMBER> <STREAM>	subscriber number a number of E1 stream 0-15	Create a new subscriber
remove by id	<USER_ID>	removed subscriber ID	Remove a subscriber using their ID
remove by index	<INDEX>	removed subscriber index	Remove a subscriber using their index
service	<USER_INDEX>	subscriber index	Move to subscriber VAS management menu
set by id access category	<USER_ID> <CAT_IDX>	subscriber ID 0-127	Assign an access category using ID

set by id access_mode	<USER_ID> <ACCESS>	subscriber ID Off/On/Off_1/Off_2 /Denied_1/Denied_2 /Denied_3/Denied_4 /Denied_5/Denied_6 /Denied_7/Denied_8 /Exclude	Assign a service mode using ID
set by id name	<USER_ID> <USER_NAME>	subscriber ID a string of 63 characters	Set a name for a subscriber using ID
set by id number	<USER_ID> <NUMBER>	subscriber ID subscriber phone number	Set a number for a subscriber using ID
set by id pbx_profile	<USER_ID> <PROFILE>	subscriber ID 0-15	Specify PBX profile using subscriber ID
set by id stream	<USER_ID> <STREAM>	subscriber ID 0-15	Set E1 stream, where subscriber is located, using subscriber ID
set by index access category	<INDEX> <CAT_IDX>	subscriber index 0-127	Assign an access category using subscriber index
set by index access_mode	<INDEX> <ACCESS>	subscriber index Off/On/Off_1/Off_2 /Denied_1/Denied_2 /Denied_3/Denied_4 /Denied_5/Denied_6 /Denied_7/Denied_8 /Exclude	Assign an service mode using subscriber index
set by index name	<INDEX> <USER_NAME>	subscriber index a string of 63 characters	Set a name for a subscriber using subscriber index
set by index number	<INDEX> <NUMBER>	subscriber index subscriber phone number	Set a number using subscriber index
set by index pbx_profile	<INDEX> <PROFILE>	subscriber index 0-15	Specify PBX profile using subscriber index
set by index stream	<INDEX> <STREAM>	subscriber index 0-15	Set E1 stream, where subscriber is located, using subscriber index
show all			Show settings for all PRI subscribers
show by id	<USER_ID>	subscriber ID	Show subscriber setting using subscriber ID
show by index	<INDEX>	subscriber index	Show subscriber setting using subscriber index
show count			Show the total quantity of PRI subscribers
show list users			Show the list of PRI subscribers

4.2.2.38 VAS configuration mode for PRI subscribers

To enter this mode, execute 'service <USER_INDEX>' command (where USER_INDEX is a PRI subscriber index) in PRI subscriber configuration mode.

```
SMG2016-[CONFIG]-[PRI-USERS]> service 0
Entering User-Service mode for user 0
SMG2016-[CONFIG]-[PRI-USERS][0]-SERVICE>
```

Command	Parameter	Value	Action
?			Show the list of available commands
attach service block			Enable VAS for a subscriber
detach service block			Disable VAS for a subscriber
set cfb enable	<ON_OFF>	off/on	Enable 'call forwarding on busy' service
set cfb number	<NUMBER>	a number of 30 characters or none	Set a number for 'call forwarding on busy' service. None – disable call forwarding
set sfnr enable	<ON_OFF>	off/on	Enable 'call forwarding on no-reply' service
set sfnr number	<NUMBER>	a number of 30 characters or none	Set a number for 'call forwarding on no-reply' service. None – disable call forwarding
set cfos enable	<ON_OFF>	off/on	Enable 'call forwarding on out-of-service' service
set cfos number	<NUMBER>	a number of 30 characters or none	Set a number for 'call forwarding on out-of-service' service. None – disable call forwarding
set cfu enable	<ON_OFF>	off/on	Enable 'call forwarding unconditional' service
set cfu number	<NUMBER>	a number of 30 characters or none	Set a number for 'call forwarding unconditional' service. None – disable call forwarding
show			Show the current VAS settings
show count			Show the quantity of free VAS blocks

4.2.2.39 PRI profiles configuration mode

To enter this mode, execute the `pri_profiles` command in the configuration mode.

```
SMG-[CONFIG]> pri_profiles
Entering PRI profiles mode.
SMG-[CONFIG]-PRI_PROFILES>
```

Command	Parameter	Value	Action
?			Show the list of available commands
add pri_profile	<NAME>	string, max 63 characters	Create a PRI profile
config			Return to the Configuration menu
exit			Exit from this configuration submenu to the upper level
quit			Terminate this CLI session
remove pri_profile	<PROFILE_INDEX>	0-31	Delete a PRO profile
set mode	<PROFILE_INDEX> <PROFILE_MODE>	0-31 start_first_forward/ start_last_backward	Set the pri profile operating mode (From first forward/From last backward)
set modifiers_table outgoing called	<PROFILE_INDEX> <MODTBL_INDEX>	0-31 0-255/none	Set a modifier for a PRI profile based on the analysis of the called subscriber number transmitted to the outgoing channel
set modifiers_table outgoing calling	<PROFILE_INDEX> <MODTBL_INDEX>	0-31 0-255/none	Set a modifier for a PRI profile based on the analysis of the calling subscriber number transmitted to the outgoing channel
set modifiers_table outgoing original_called	<PROFILE_INDEX> <MODTBL_INDEX>	0-31 0-255/none	Set a modifier for a PRI profile based on the analysis of the original Called party number transmitted to the outgoing channel
set modifiers_table outgoing redirecting	<PROFILE_INDEX> <MODTBL_INDEX>	0-31 0-255/none	Set a modifier for a PRI profile based on the analysis of the redirecting number transmitted to the outgoing channel
set name	<PROFILE_INDEX> <NAME>	0-31 string, max 63 characters	Set PRI profile name
show			Show PRI profile settings
stream_list add	<PROFILE_INDEX> <STREAM>	0-31 1-16	Add E1(Q.931) stream to PRI profile
stream_list remove	<PROFILE_INDEX> <STREAM>	0-31 1-4	Remove E1(Q.931) stream from PRI profile

4.2.2.40 SORM configuration mode

To enter this mode, execute the 'sorm-data-extractor' command in the configuration mode.

```
SMG-[CONFIG]> sorm-data-extractor
Entering SORM-Extractor mode.
SMG-[CONFIG]-[SORM-DATA-EXTRACTOR]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
config			Return to the Configuration menu
enable		on/off	Enable/disable SORM
exit			Exit from this configuration submenu to the upper level
history			View the history of entered commands
modifiers table called	<MODTBL_INDEX>	0-255/ none	Set the ITEM_VOIP_CALLEE_E164[0] field modifier for Norsis-Trans mode or CdPN, forwardedTo, transferredTo, dstNr fields for RTK-NT/ Tehargos /VAS-Experts/MFI-Soft modes
modifiers table calling	<MODTBL_INDEX>	0-255/ none	Set the ITEM_VOIP_CALLER_E164[0] field modifier for Norsis-Trans mode, or CgPN, subscriber fields for modes RTK-NT/Tehargos/VAS-Experts/MFI-Soft
modifiers table original_called	<MODTBL_INDEX>	0-255/ none	Set the ITEM_PHONE_NUMBER field modifier for Norsis-Trans mode or dialedNr fields for RTK-NT/Tehargos/VAS-Experts/MFI-Soft modes
modifiers table original_calling	<MODTBL_INDEX>	0-255/ none	Set the ITEM_PHONE_RCV field modifier for Norsis-Trans mode
modifiers table redirecting	<MODTBL_INDEX>	0-255/ none	Set the ITEM_VOIP_CALLER_E164[0] field modifier to Forwarding message for Norsis-Trans mode
modifiers table connected	<MODTBL_INDEX>	0-255/ none	Set the CnPN field modifier for RTK-NT/Tehargos/VAS-Experts/MFI-Soft modes
quit			Terminate the current CLI session
set interface name	<IFACE_NAME>	string, max 255 characters	Select a network interface
set interface sig port	<IFACE_SIG_PORT>	1-65535	Selecting a port for sending signal information
set remote ip	<IP>	IP address in AAA.BBB.CCC.DDD format	Set IP address to receive signaling
set remote port	<REMOTE_PORT>	1-65535	Set port to receive signaling
set remote rtp start port	<REMOTE_RTP_STAR T_PORT>	1024-65535	Set a starting port to receive RTP
set remote rtp end port	<REMOTE_RTP_END_ PORT>	1024-6553 5	Set an end port to receive RTP

set switch_name	<SWITCH_NAME>	string, max 63 characters	Set device identification name
--------------------	---------------	------------------------------	--------------------------------

4.2.2.41 SS7 category modification configuration mode

To enter this mode, execute 'ss7cat' command in the configuration mode.

```
SMG-[CONFIG]> ss7cat
Entering SS7-categories mode.
SMG-[CONFIG]-SS7-CAT>
```

Command	Parameter	Value	Action
?			Show the list of available commands
config			Return to Configuration menu
exit			Exit from this configuration submenu to the upper level
quit			Terminate this CLI session
set	<CAT_IDX> <PBX_CAT> <SS7_CAT>	0-15 0-255 0-255	Set data category: CAT_IDX — category index PBX_CAT — Caller ID category SS7_CAT — SS7 category
show			Show information on SS7 data category

4.2.2.42 Switch parameter configuration mode¹

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

```
SMG-[CONFIG]> switch
Entering switch control mode.
SMG-[CONFIG]-[SWITCH]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
802.1q			Enter the 802.1q configuration mode
apply mirroring settings		no/yes	Apply mirroring settings
apply port settings		no/yes	Apply port settings
confirm mirroring settings			Confirm mirroring settings. If you fail to confirm settings in 1 minute interval, the previous values will be restored
confirm port settings			Confirm port settings. If you fail to confirm settings in 1 minute interval, the previous values will be restored
exit			Exit from this configuration submenu to the upper level.
history			View history of entered commands.
LACP ²			Enter LACP parameter configuration mode
QoS_control			Enter the QoS parameter configuration mode
quit			Terminate this CLI session
save mirroring			Save mirroring settings without applying
save vlan			Save VLAN settings without applying

¹ For SMG-1016M only. It is not supported in the current firmware version.

² Not supported in the current firmware version.

<p>set mirroring</p>	<p><PORT></p> <p><NAME></p> <p><ACT></p>	<p>GE_PORT0 (0) / GE_PORT1 (1) / GE_PORT2 (2) / CPU (4) / SFP0 (6) / SFP1 (7)</p> <p>src_in/ src_out/ dst_in/ dst_out</p> <p>on/off</p>	<p>Configure port mirroring:</p> <p><i>PORT</i> — port type</p> <p><i>NAME</i> — port designation</p> <p><i>src_in</i> — incoming packet source port — copy frames received from this port (source port)</p> <p><i>src_out</i> — outgoing packet source ports — copy frames sent by this port (source port)</p> <p><i>dst_in</i> — incoming packet destination port — destination port for copied frames received by selected source ports</p> <p><i>dst_out</i> — outgoing packet destination port — destination port for copied frames sent by selected source ports</p>
<p>set port backup</p>	<p><ON_OFF></p> <p><B_MASTER></p> <p>B_SLAVE</p> <p>PREEMPTION</p>	<p>on/off</p> <p>GE_PORT0/ GE_PORT1/ GE_PORT2/ SFP0/SFP1</p> <p>GE_PORT0/ GE_PORT1/ GE_PORT2/ SFP0/SFP1</p>	<p>Enable Dual Homing redundancy</p> <p><i>B_MASTER</i> — master port</p> <p><i>B_SLAVE</i> — slave port</p> <p><i>PREEMPTION</i> — enable/disable return to master port when it becomes available</p>
<p>set port default vlan id</p>	<p><PORT></p> <p><VLANID></p>	<p>GE_PORT0 (0) / GE_PORT1 (1) / GE_PORT2 (2) / CPU (4) / SFP0 (6) / SFP1 (7)</p> <p>0-4095</p>	<p>Define VLAN ID for this port</p>
<p>set port egress</p>	<p><PORT></p> <p><EGRESS></p>	<p>GE_PORT0 (0) / GE_PORT1 (1) / GE_PORT2 (2) / CPU (4) / SFP0 (6) / SFP1 (7)</p> <p>unmodified/ untagged/ tagged/ double-tag</p>	<p>Configure packet transmission mode for the current port.</p> <p><i>EGRESS</i> — packet transmission mode:</p> <p><i>unmodified</i> — packets will be sent by the port without any changes (i.e. as they came to another switch port)</p> <p><i>untagged</i> — packets will always be sent without VLAN tag by this port</p> <p><i>tagged</i> — packets will always be sent with VLAN tag by this port</p> <p><i>double tag</i> — each packet will be sent with two VLAN tags — if received packet was</p>

			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: <i>Fallback</i> — 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 <i>Check</i> — 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 <i>Secure</i> — if a packet with VID is received through the port, and there is a record in '802.1q' routing table for this packet, then it falls within a scope of routing rules, specified in the current record of this table; otherwise, it is rejected. Routing rules specified in 'egress' and 'output' will not apply to this port
set port LACP_trunk ¹	<PORT> <LACP>	CPU/ GE_PORT0/ GE_PORT1/ GE_PORT2/ SFP0/ SFP1 0-4	Assign LACP trunk for the port specified
set port MAC GE_PORT0	<MACADDR>	MAC address in XX:XX:XX:XX:XX:XX format	Specify MAC address for port
set port output	<PORT> <P_DEST> <ENABLE>	GE_PORT0/ GE_PORT1/ GE_PORT2/ CPU/ SFP0/ SFP1 GE_PORT0/ GE_PORT1/ GE_PORT2/ CPU/ SFP0/ SFP1 on/off	Specify allowed ports for packet transfer: <i>PORT</i> — port being configured <i>P_DEST</i> — allowed transmission ports
set port speed	<SPEED>	1000M 100M (full-duplex/ half-duplex) 10M (full-duplex/ half-duplex) auto	Specify port operation mode

¹ For SMG-1016M only. It is not supported in the current firmware version.

	<PORT>	GE_PORT0/GE_PORT1/ GE_PORT2	
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

4.2.2.42.1 802.1q parameter configuration mode

To enter this mode, execute '802.1q' command in the switch configuration mode.

```
SMG-[CONFIG]-[SWITCH]> 802.1q
Entering 802.1q_control mode.
SMG-[CONFIG]-[SWITCH]-[802.1q]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
add VTU element	<VID> <PRIO> <OVER> <GE_PORT0> <GE_PORT1> <GE_PORT2> <CPU> <SFP0>	0-4095 0-7 on/off unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member unmodified/ untagged/ tagged/ not_member	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. <i>Unmodified</i> — packets will be sent by the port without any changes <i>Untagged</i> — packets will always be sent without VLAN tag by this port <i>Tagged</i> — packets will always be sent with VLAN tag by this port <i>Not_member</i> — packets with specified VID will not be sent by this port, i. e. the port is not the member of VLAN

	<SFP1>	not_member unmodified/ untagged/ tagged/ not_member	
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. <i>Unmodified</i> — packets will be sent by the port without any changes <i>Untagged</i> — packets will always be sent without VLAN tag by this port <i>Tagged</i> — packets will always be sent with VLAN tag by this port <i>Not_member</i> — 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. <i>Unmodified</i> — packets will be sent by the port without any changes <i>Untagged</i> — packets will always be sent without VLAN tag by this port <i>Tagged</i> — packets will always be sent with VLAN tag by this port <i>Not_member</i> — 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. <i>Unmodified</i> — packets will be sent by the port without any changes <i>Untagged</i> — packets will always be sent without VLAN tag by this port <i>Tagged</i> — packets will always be sent with VLAN tag by this port

			<i>Not_member</i> — 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. <i>Unmodified</i> — packets will be sent by the port without any changes <i>Untagged</i> — packets will always be sent without VLAN tag by this port <i>Tagged</i> — packets will always be sent with VLAN tag by this port <i>Not_member</i> — 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. <i>Unmodified</i> — packets will be sent by the port without any changes <i>Untagged</i> — packets will always be sent without VLAN tag by this port <i>Tagged</i> — packets will always be sent with VLAN tag by this port <i>Not_member</i> — 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. <i>Unmodified</i> — packets will be sent by the port without any changes <i>Untagged</i> — packets will always be sent without VLAN tag by this port <i>Tagged</i> — packets will always be sent with VLAN tag by this port <i>Not_member</i> — 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

4.2.2.42.2 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>	GE_PORT0 (0) / GE_PORT1 (1) / GE_PORT2 (2) / CPU (4) / SFP0 (6) / SFP1 (7)	Enable restriction mode for traffic coming to the current port. INGRMODE — restriction mode: - off — no restriction

	<INGRMODE>	off/ all/ mult_flood_broad/ mult_broad/ broad	<p>- <i>all</i> — restrict all traffic</p> <p>- <i>mult_flood_broad</i> — multicast, broadcast, and flooded unicast traffic will be restricted</p> <p>- <i>mult_broad</i> — multicast and broadcast traffic will be restricted</p> <p>- <i>broad</i> — only broadcast traffic will be restricted</p>
set ingress_rate_prio_0/1/2/3	<PORT>	GE_PORT0 (0) / GE_PORT1 (1) / GE_PORT2 (2) / CPU (4) / SFP0 (6) / SFP1 (7)	Define the bandwidth restriction (in kbps) for incoming port traffic for queue 0/1/2/3
	<INGPRIO>	0-250000	
set QoS_mode	<PORT>	GE_PORT0 (0) / GE_PORT1 (1) / GE_PORT2 (2) / CPU (4) / SFP0 (6) / SFP1 (7)	Set the QoS utilization mode
	<QOSMODE>	DSCP_only/ 802.1p_only/ DSCP_preferred/ 802.1p_preferred	<p><i>QOSMODE</i> — utilization mode:</p> <p><i>DSCP only</i> — distribute packets into queues based on IP diffserv priority only</p> <p><i>802.1p only</i> — distribute packets into queues based on 802.1p priority only</p> <p><i>DSCP preferred</i> — 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</p> <p><i>802.1p preferred</i> — 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</p>
set remapping_priority	<PORT>	GE_PORT0 (0) / GE_PORT1 (1) / GE_PORT2 (2) / CPU (4) / SFP0 (6) / SFP1 (7)	Remap 802.1p priorities for untagged packets.
	<NUM>	0-7	PORT — port being configured
	<REMAP>	0-7	NUM — the current priority 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

4.2.2.43 Syslog parameter configuration mode

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

```
SMG-[CONFIG]> syslog
Entering syslog mode.
SMG-[CONFIG]-SYSLOG>
```

Command	Parameter	Value	Action
?			Show the list of available commands
alarm	<ALARM>	0-99	Send the data on the defined priority level faults, 0 — disable data transfer
apply	yes/no		Apply system log settings
authlog set	IP PORT ONOFF LOCREM	IP address in AAA.BBB.CCC.DDD format 1-65535 off/on local/remote	Set server address for syslog messages transmission and operation mode. <i>on/off</i> – enable/disable logging <i>local/remote</i> – 'remote' means transmit logs to syslog server
authlog show			Show current parameters of logging
calls	<CALLS>	0-99	Enable tracing of calls with the defined debug level, 0 — disable data transfer
config			Return to Configuration menu
exit			Return from this configuration submenu to the upper level
h323	<H323>	0-99	Enable H.323 signaling tracing with defined debug level, 0 – data will not be transmitted
hw	<E1> <HW>	0-15 0-99	Send E1 stream hardware data with the defined debug level, 0 — disable data transfer. E1 — E1 stream name HW — priority level
ipaddr	<IPADDR>	IP address in AAA.BBB.CCC.DDD format	Define syslog server IP address
isup	<ISUP>	0-99	Enable tracing of ISUP subsystem with the defined debug level, 0 — disable data transfer
msp	<MSP>	0-99	Enable tracing of MSP signal processor resources with the defined debug level, 0 — disable data transfer
port	<PORT>	1-65535	Define a local port number
Q931	<Q931>	0-99	Enable tracing of Q.931 signalling with the defined debug level, 0 — disable data transfer
quit			Terminate this CLI session
radius	<RADIUS>	0-99	Enable tracing of RADIUS protocol with the defined debug level, 0 — disable data transfer
rtp-create	<RTP>	0-99	Enable tracing of RTP forwarding creation with the defined debug level, 0 — disable data transfer
show			Show Syslog configuration information
sipt	<SIPT>	0-99	Enable tracing of SIP-T signalling with the defined debug level, 0 — disable data transfer
start			Enable data transmission to a syslog server
stop			Disable data transmission to a syslog server

userlog	<p><IPADDR></p> <p><PORT></p> <p><MODE></p>	<p>IP address in AAA.BBB.CCC.DDD format</p> <p>1-65535</p> <p>off/standart/full</p>	<p>Enable the output of history of entered commands</p> <p>IPADDR — syslog server IP address</p> <p>PORT — syslog server port</p> <p>MODE — verbosity level of the entered commands log: <i>off</i> — disable entered commands logs generation</p> <p><i>standart</i> — messages contain the name of modified parameter</p> <p><i>full</i> — messages contain the name of modified parameter as well as parameter values before and after the modification</p>
---------	---	---	--

4.2.2.44 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

4.2.2.45 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

4.2.2.46 Trunk group configuration mode

To enter the trunk group configuration mode, execute 'trunk group <TRUNK_INDEX>' command in the configuration mode, where <TRUNK_INDEX> is a trunk group number.

```
SMG-[CONFIG]> trunk group 0
Entering trunk-mode.
SMG-[CONFIG]-TRUNK[0]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
channel add	CHAN_INDEX	0-31	Add a channel from selected E1 stream to trunk group 'E1-channels'
channel order	CHAN_ORDER	successive_forward/ successive_backward/ start_first_forward/ start_last_backward	Select channel order for 'E1 channels' trunk groups or Linkset-Line
channel remove	CHAN_INDEX	0-31	Remove E1 channel from trunk group 'E1 channels'
config			Return to Configuration menu
cps max	<CPS_MAX>	0-255	CPS threshold value that may pass through the trunk group
cps warn	<CPS_WARN>	0-255	CPS emergency value that when exceeded, will output the warning into the alarm log
destination	<TG_ENTRY>	Q.931/SS7/SIPT/ E1-channels/ Linkset-Line	Assign the trunk group to the Q931 interface, SS7, SIP-T, specified E1 channels or specified SS7 linkset streams

	<ENTRY_INDEX>	Unsigned integer value	TG_ENTRY — interface type ENTRY_INDEX — object index (number of Q931/SS7 signalling stream, link set, SIP-T interface)
direct prefix	<IDX>	0-255/none	Define the direct call forwarding from the current trunk group to the specified prefix without caller and callee number analysis
disable all	<YES_NO>	yes/no	Enable/disable all incoming and outgoing calls for the current trunk group
disable in			Disable all incoming calls for the current trunk group
disable out			Disable all outgoing calls for the current trunk group
exit			Exit from this configuration submenu to the upper level
history			View history of entered commands
linkset-line add	<LINE_INDEX>	0-15	Add E1 stream from selected SS7 Linkset to 'Linkset-Line' trunk group
linkset-line remove	<LINE_INDEX>	0-15	Remove E1 stream from 'Linkset-Line' trunk group
local	<YES_NO>	yes/no	When enable means that the subscriber is local
modifiers table incoming called	<MODTBL_INDEX>	0-255/none	Define trunk group modifier for modifications based on the analysis of the callee number received from the incoming channel
modifiers table incoming calling	<MODTBL_INDEX>	0-255/none	Define trunk group modifier for modifications based on the analysis of the caller number sent to the outgoing channel
modifiers table outgoing called	<MODTBL_INDEX>	0-255/none	Define trunk group modifier for modifications based on the analysis of the callee number sent to the outgoing channel
modifiers table outgoing original	<MODTBL_INDEX>	0-255/none	Define trunk group modifier for modifications based on the analysis of the initial callee number sent to the outgoing channel
modifiers table incoming redirecting	<MODTBL_INDEX>	0-255/none	Define trunk group modifier for modifications based on the analysis of the redirecting subscriber number sent to the outgoing channel
modifiers table outgoing calling	<MODTBL_INDEX>	0-255/none	Define trunk group modifier for modifications based on the analysis of the caller number received from the incoming channel
name	<s_name>	you may use letters, numbers, ' ' character 31 characters max.	Define trunk group name
quit			Terminate this CLI session
radius profile incoming	<IDX>	0-31/no	RADIUS profile selection for incoming communications
radius profile outgoing	<IDX>	0-31/no	RADIUS profile selection for outgoing communications
recover on egress failure	<RECOVER>	no/yes	Recover calls after failure on incoming leg
reserv	<TG_RSV_IDX>	0-31	Define the redundant trunk group number
show			Show the trunk group configuration

4.2.2.47 Trunk directions configuration mode

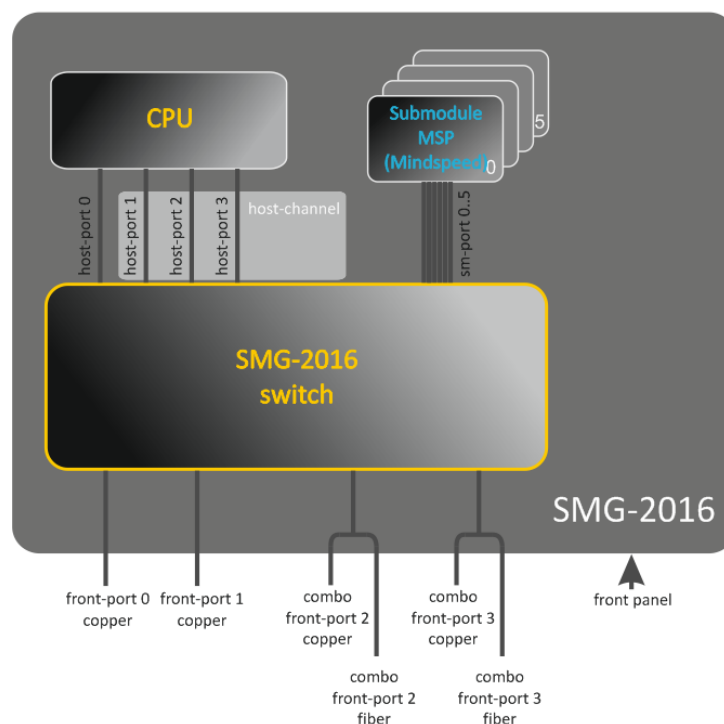
To enter the trunk direction configuration mode, execute 'trunk direction <DIRECTION_INDEX>' command in the configuration mode, where < DIRECTION_INDEX> is a trunk group number.

```
SMG-[CONFIG]> trunk direction 0
Entering trunk-mode.
SMG-[CONFIG] - TRUNK_DIRECTION[0]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
config			Return to Configuration menu
exit			Return from this configuration submenu to the upper level
history			View history of entered commands
list add	<TD_TRUNK>	0-63	Add the trunk group with the specified index into direction
list remove	<TD_TRUNK>	0-63	Remove the trunk group with the specified index from direction
mode		successive_forward/ successive_backward/ first_forward/ last_backward	Define trunk group selection method for a direction <i>Sequential forward</i> <i>Sequential back</i> <i>From the first and forward</i> <i>From the last and back</i>
name	<s_name >	string, 63 characters max.	Define trunk direction name
quit			Terminate this CLI session
show			Show the trunk direction settings

4.2.3 SMG-2016/SMG-3016 switch configuration

4.2.3.1 Switch structure



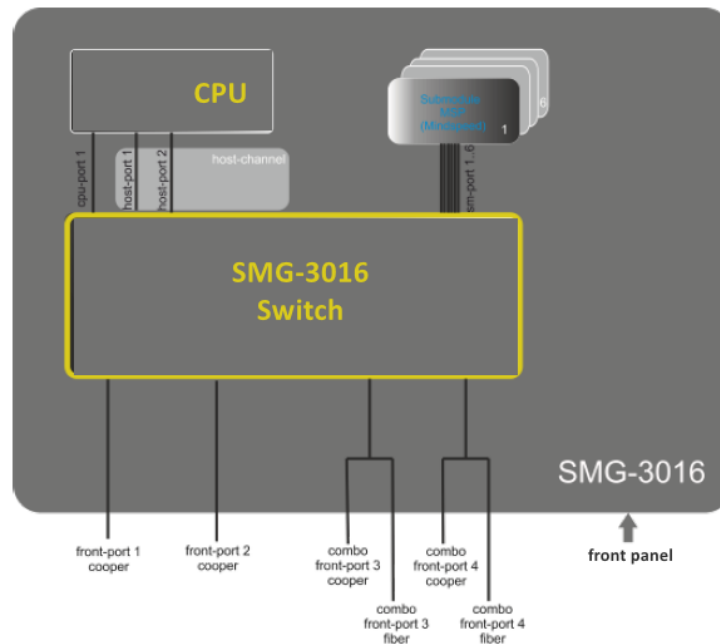


Figure 49 — Switch structure

SMG-2016 switch is equipped with the following interfaces:

- *front-port* — external switch Ethernet ports located on the front panel.
Possible values: 0 — 3.
 - ports 0.. 1 — copper-wire ports
 - ports 2.. 3 — optical/copper-wire combo ports.
- *port-channel* — LAG aggregation groups of front-port interfaces of the switch used for combining multiple front-ports into a single LACP group.
Possible values: 1 — 4.
- *cpu-port* — inner port of the switch for SMG-2016 management.
Possible value: 0.
- *host-port* — SMG-2016 switch internal ports designed for the SMG-2016 CPU communication.
Possible values: 0 — 2.
- *host-channel* — LAG host-channel aggregation group of the switch interfaces, this group is always active.
Possible value: 1.
- *sm-port* — SMG-2016 switch internal ports designed for the SM-VP submodule communication.
Possible values: 0 — 5.

SMG-3016 switch is equipped with the following interfaces:

- *front-port* — external switch Ethernet ports located on the front panel.
Possible values: 1 — 4.
 - ports 1.. 2 — copper-wire ports
 - ports 3.. 4 — optical/copper-wire combo ports.

- *port-channel* — LAG aggregation groups of front-port interfaces of the switch used for combining multiple front-ports into a single LACP group.
Possible values: 1 – 4.
- *cpu-port* — inner port of the switch for SMG-3016 management.
Possible value: 1.
- *host-port* — SMG-3016 switch internal ports designed for the SMG-3016 CPU communication.
Possible values: 1 – 2.
- *host-channel* — LAG host-channel aggregation group of the switch interfaces, this group is always active.
Possible value: 1.
- *sm-port* — SMG-3016 switch internal ports designed for the SM-VP submodule communication.
Possible values: 1 – 6.

During the switch operation, *unit number* value equal to 1 will be used.

4.2.3.2 SMG 2016/3016 switch interface management commands



For SMG-3016, it is necessary to take into account that the port numbering has been changed, the initial front-port= 1.

4.2.3.2.1 interface

This command allows you to enter the SMG-2016/ SMG-3016 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/SMG-301 module number, the value is always 1.
 - port — port number; possible values [0 .. 3] (or 1 .. 3 for SMG-3016).
- 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.

4.2.3.2.2 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.

4.2.3.2.3 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>;
- 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/port>, where:
 - unit — module number; possible value [1],
 - port — port number; possible values [0 .. 2].
- for port-channel: [0 .. 4].
- for sm-port: [0 .. 15]: <unit/port>, where:
 - unit — module number; possible value [1],
 - port — port number; possible values [0 .. 5].

Example

```
SMG2016-[CONFIG]-[SWITCH]-[if]> bridging to front-port all
```

4.2.3.2.4 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
```

4.2.3.2.5 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.

4.2.3.2.6 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.

4.2.3.2.7 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.

4.2.3.2.8 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
                   -----  -----  -----  -----  -----
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]>
```

4.2.3.2.9 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
-----
-----
front-port     1/0       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      Down     N/A
SMG2016-[CONFIG]-[SWITCH]>
```

4.2.3.2.10 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
```

4.2.3.3 Aggregation group configuration commands

4.2.3.3.1 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.

4.2.3.3.2 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.

4.2.3.3.3 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]> interface port-channel 1
SMG2016-[CONFIG]-[SWITCH]-[if]> mode lacp
```

Link aggregation mode is enabled for the configured interface.

4.2.3.3.4 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.

4.2.3.3.5 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.

4.2.3.4 SMG-2016 board VLAN interface management commands

4.2.3.4.1 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 PVID 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.

4.2.3.5 STP/RSTP configuration commands



Settings are available only for SMG-2016/3016. The SMG-1016M does not support the spanning-tree protocol.

4.2.3.5.1 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.

4.2.3.5.2 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.

4.2.3.5.3 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.

4.2.3.5.4 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.

4.2.3.5.5 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.

4.2.3.5.6 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.

4.2.3.6 MAC table configuration commands

4.2.3.6.1 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
```

4.2.3.6.2 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
```

4.2.3.6.3 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

4.2.3.7 Port mirroring configuration commands

4.2.3.7.1 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 incoming traffic going 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.

4.2.3.7.2 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.

4.2.3.7.3 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
```

4.2.3.7.4 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
```

4.2.3.7.5 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
```

4.2.3.8 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).

4.2.3.8.1 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
```

4.2.3.8.2 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
```

4.2.3.8.3 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
```

4.2.3.8.4 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
```

4.2.3.8.5 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
```

4.2.3.8.6 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

4.2.3.8.7 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

4.2.3.9 DUAL HOMING protocol configuration

4.2.3.9.1 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
```

4.2.3.9.2 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
```

4.2.3.9.3 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
```

4.2.3.9.4 backup-interface preemption

Use this command to specify the traffic switchover to the main interface when the connection is restored. If the configuration allows 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
```

4.2.3.9.5 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

4.2.3.10 LLDP protocol configuration

4.2.3.10.1 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
```

4.2.3.10.2 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
```

4.2.3.10.3 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
```

4.2.3.10.4 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
```

4.2.3.10.5 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
```

4.2.3.10.6 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
```

4.2.3.10.7 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
```

4.2.3.10.8 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]>
```

4.2.3.10.9 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

4.2.3.10.10 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          0
front-port 1/1 6134       6159       0          0          0          0          0          0
front-port 1/2 6141       6136       0          0          0          0          0          0
front-port 1/3 0          0          0          0          0          0          0          0
```

4.2.3.10.11 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
```

4.2.3.11 QOS Configuration

4.2.3.11.1 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.

4.2.3.11.2 qos type

Use this command to define the rule that will be used for the packet priority field selection.

The traffic prioritization method will be chosen depending on the configured system rules (IEEE 802.1p/DSCP).

The traffic prioritization methods featured by the system are as follows:

- All priorities are equal
- Packet selection is based on IEEE 802.1p standard
- Packet selection is based on IP ToS (type of service) at the level 3 only — Differentiated Services Code point (DSCP) support
- Interactions based on 802.1p or DSCP/TOS

Syntax

qos type <type>

Parameters

<type> — traffic prioritization method:

- 0 — all priorities are equal
- 1 — packet selection by 802.1p only (Priority field in 802.1Q tag)
- 2 — packet selection by DSCP/TOS only (Differentiated Services field of the IP packet header, 6 high bits)
- 3 — interaction based on either 802.1p or DSCP/TOS

Default value

All priorities are equal by default.

Command mode

CONFIG SWITCH

Example

```
qos type 2
```

Traffic prioritization will be performed by DSCP/TOS only.

4.2.3.11.3 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> = 1, *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.

4.2.3.11.4 cuntrset

Use this command to map the queue statistics collector to queues with the defined criteria.

Syntax

```
cuntrset <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

```
cuntrset sm-port 1/2 1 22 2 1
```

4.2.3.11.5 show cuntrset

Use this command to view the queue collector information.

Syntax

```
show cuntrset <SET>
```

Parameters

<SET> — counter number [0 .. 1]

Command mode

CONFIG – SWITCH

4.2.3.11.6 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

4.2.3.12 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.

4.2.3.12.1 View configuration

4.2.3.12.1.1 running-config viewing command

Syntax

```
show running-config
```

Parameters

There are no parameters for this command.

Command mode

CONFIG – SWITCH

4.2.3.12.1.2 candidate-config viewing command

Syntax

```
show candidate-config
```

Parameters

There are no parameters for this command.

Command mode

CONFIG – SWITCH

4.2.3.12.2 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.

4.2.3.12.2.1 Configuration application command

Syntax

apply

Parameters

There are no parameters for this command.

Command mode

CONFIG – SWITCH

4.2.3.12.2.2 Confirmation command

Syntax

confirm

Parameters

There are no parameters for this command.

Command mode

CONFIG – SWITCH

4.2.3.13 Miscellaneous commands

4.2.3.13.1 config

Use this command to return to Configuration menu.

Syntax

config

Parameters

There are no parameters for this command.

Command mode

CONFIG – SWITCH

4.2.3.13.2 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

4.2.3.13.3 history

Use this command to view history of entered commands.

Syntax

history

Parameters

There are no parameters for this command.

Command mode

CONFIG – SWITCH

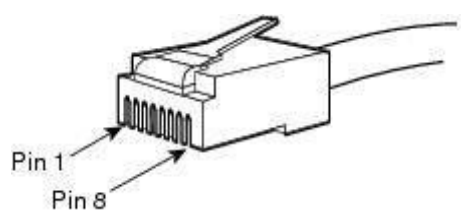
5 APPENDIXES (SMG)

5.1 Appendix A. Cable contact pin assignment

5.1.1 For SMG-2016, SMG-3016

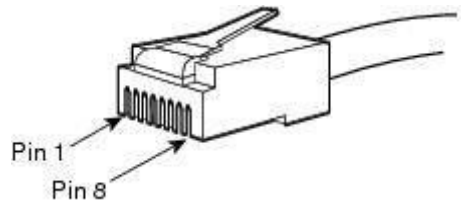
Assignment of the RJ-48 connector pins for connection of *E1 Line 0..15* streams is ISO/IEC 10173 compliant and provided in the table below.

Table A1 — Assignment of RJ-48 connector pins for E1 stream connection

Contact pin no. (Pin)	Purpose	Contact pin numbering
1	RCV tip (receive data)	
2	RCV ring (receive data)	
3	RCV shield (receiver shield)	
4	XMT tip (transmit data)	
5	XMT ring (transmit data)	
6	XMT shield (transmitter shield)	
7	Not used	
8	Not used	

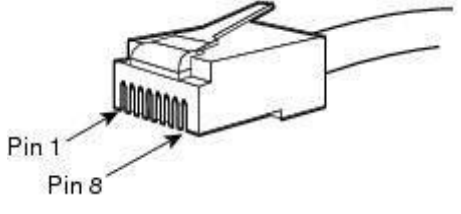
Assignment of the *Console* port RJ-45 connector pins is provided in the table below.

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

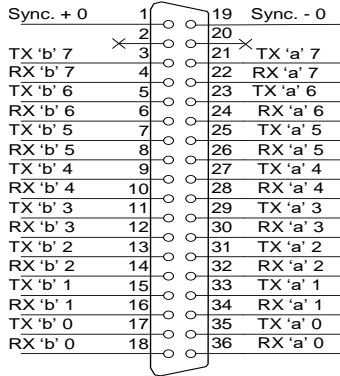
Contact pin no. (Pin)	Purpose	Contact pin numbering
1	Sync A ¹	
2	Sync B ²	
3	Not used	
4	Sync A	
5	Sync B	
6	Not used	
7	Not used	
8	Not used	

¹ Pins 1 and 4 are electrically interconnected inside the device

² Pins 2 and 5 are electrically interconnected inside the device

5.1.2 For SMG-1016M

E1 Line 0..7



E1 Line 8..15

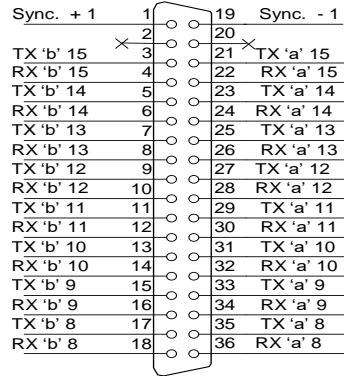


Figure 50 — Assignment of E1 Line contact pins

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

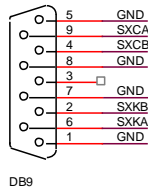


Figure 51— Assignment of Console port contact pins

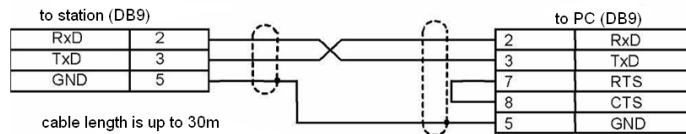


Figure 52— Cable wiring diagram for PORT1, PORT2 connection

5.1.3 Correspondence tables for wire and pin colors of the E1 Line connector

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

5.2 Appendix B. Alternative firmware update method

5.2.1 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: 8 bit 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!
=>
```

5.2.2 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 usb <file-name>
```

If CLI mode is not available, you may update in shell mode; to do this, enter in shell mode:

```
/usr/local/scripts/get_firmware usb <file-name>
```

where <file-name> is the firmware file name.

8. Wait until firmware update procedure is completed and restart the device.

5.3 Appendix C. Examples of modifier operation and device configuration via CLI

5.3.1 Modifier operation examples

5.3.1.1 The procedure for applying modifiers on incoming communications

- from a trunk group or PBX profile by CgPN number – you can change CgPN and CdPN;
- from a trunk group or PBX profile by CdPN number – you can change CgPN and CdPN (CdPN number is used modified in paragraph 1);
- from RADIUS by CgPNin – only CgPN can be changed (the CgPN number changed in step 1,2);
- from RADIUS via CdPNin – only CdPN can be changed (the CdPN number changed in step 1,2).

5.3.1.2 The procedure for applying modifiers on outgoing communications

- from a trunk group or PBX profile by CgPN number – you can change CgPN and CdPN (CgPN number is used after all higher steps);
- from a trunk group or PBX profile by CdPN number – you can change CgPN and CdPN (CdPN number is used after all higher steps);
- from RADIUS by CgPNout – only CgPN can be changed (the CgPN number is used after all higher steps);
- from RADIUS by CdPNout – only CdPN can be changed (the CdPN number is used after all higher steps).

5.3.1.3 Objective 1

In the *trunk group 0*, perform the following modification for outgoing dialling matching with the mask (1x{4,6}) — remove the first digit, replace it with 34, leave other digits unchanged.

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
Mdfier. 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

```

5.3.1.4 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

```

5.3.2 CLI device configuration example

5.3.2.1 Objective

Configure SS7-SIPT transit.

5.3.2.2 Source data

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

SS7 signalling parameters:

- OPC=67;
- DPC=32;
- signalling channel SLC=1 in the channel interval 1;
- CIC numbering from 2 to 31 for channels from 2 to 31 respectively;
- channel engagement order — 'Sequential forward even' (respectively, to exclude the mutual channel engagement, the channel engagement order should be assigned on the opposite side, e. g. 'Sequential back odd').

SIP-T signalling parameters:

- IP address of the communicating gateway — 192.168.16.7;
- UDP port for SIP-T signalling reception of the communicating gateway — 5060;
- Quantity of simultaneously allowed sessions — 25;
- Packetization time for G.711 codec — 30 ms;
- DTMF signal transmission performed during the established session according to RFC2833, payload type for RFC2833 packets — 101.

Routing:

- Route to SS7 by trunk group 0;
- Route to SIP-T by trunk group 1;
- Transition to SS7 is performed by 7-digit numbers beginning from 6, 7, 91, 92, 93;
- Transition to SIP-T is performed by 7-digit numbers beginning from 1, 2, 3;
- All SS7 signalling messages are transferred by transit.

5.3.2.3 Configuration via CLI

5.3.2.3.1 SS7 signalling parameters configuration:

```

SMG>config // Enter the configuration mode
SMG-[CONFIG]>new linkset // Create a new link set
NEW 'LINKSET' [00]: successfully created
SMG-[CONFIG]>linkset0 // Enter the linkset configuration mode
Entering Linkset-mode.
SMG-[CONFIG]-LINKSET[0]>chan_order even_successive_forward
// Select the channel engagement order — sequential forward even
Linkset[0]. Set chan_order '6'
SMG-[CONFIG]-LINKSET[0]>DPC 32 // Define destination point code
Linkset[0]. Set DPC '32'
SMG-[CONFIG]-LINKSET[0]>OPC 67 // Define the originating point code
Linkset[0]. Set OPC '67'
SMG-[CONFIG]-LINKSET[0]>init group-reset
// Select channel initialization mode during signalling channel establishment
Linkset[0]. Set init '7'
SMG-[CONFIG]-LINKSET[0]>net_ind national // Define the network identifier — local network
Linkset[0]. Set net_ind '3'
'LINKSET' [00]:

                Name:          Linkset00
                Trunk:          1
                Access cat:     0
                OPC:            67
                DPC:            32
                init:           'group reset'
                china:          n
                chan_order:     'even_successive_forward'
                netw_ind:       national
                satellite:      override_no_satellite
                interwork:      no change
                TMR:            speech
                alarm ind:      no
                CCI:            off
                CCI_freq:       3

SMG-[CONFIG]-LINKSET[0]>exit // Exit the linkset configuration mode
Leaving Linkset mode
SMG-[CONFIG]>e10 // Enter the E1 stream 0 configuration mode
Entering E1-stream mode
SMG-[CONFIG]-E1[0]>enabled // Put E1 stream into operation
E1[0]. Set line 'on'
SMG-[CONFIG]-E1[0]>signalingSS7 // Select SS7 signalling protocol for a stream
E1[0]. Set Signaling 3
'E1: PHYS' [00]:

                line           'on'
                code           'hdb3'
                eq              'off'
                crc             'off'
                sig              'SIG_SS7' (3)
                alarm_ind       'off'
                rem_alarm_ind   'off'

SMG-[CONFIG]-E1[0]>ss7 // Enter the SS7 protocol configuration mode
E1[0]. Signaling is SS7
SMG-[CONFIG]-E1[0]-[SS7]>CIC fill0 1 // Assign channel numbering from 0 in increments of 1
E1-SS7[0]. Fill CIC: start [0], step [1]
SMG-[CONFIG]-E1[0]-[SS7]>dchan1 // Select channel 1 as a signal channel
E1-SS7[0]. Set Dchan 1
SMG-[CONFIG]-E1[0]-[SS7]>SLC1 // Assign code 1 for the created signalling channel
E1-SS7[0]. Set SLC 1

```



```
SMG-[CONFIG]-E1[0]-[SS7]>linkset0// Assign linkset 0 for a stream
```

```
E1-SS7[0]. Set Linkset 0
```

```
'E1: SS7' [00]:
```

```

        stream:      0
linkset:      0
SLC:         1

```

```
CICs:
```

```

00: --- | 01: -D- | 02: 002 | 03: 003 |
04: 004 | 05: 005 | 06: 006 | 07: 007 |
08: 008 | 09: 009 | 10: 010 | 11: 011 |
12: 012 | 13: 013 | 14: 014 | 15: 015 |
16: 016 | 17: 017 | 18: 018 | 19: 019 |
20: 020 | 21: 021 | 22: 022 | 23: 023 |
24: 024 | 25: 025 | 26: 026 | 27: 027 |
28: 028 | 29: 029 | 30: 030 | 31: 031 |

```

```
SMG-[CONFIG]-E1[0]-[SS7]>exit// Exit the SS7 protocol configuration mode
```

```
Leaving SS7-signaling mode
```

```
SMG-[CONFIG]-E1[0]>exit// Exit the E1 stream 0 configuration mode
```

```
Leaving E1-stream mode
```

5.3.2.3.2 SIP-T signalling parameters configuration (session continued)

```
SMG-[CONFIG]>new sip-t-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]>ipaddr 192.168.16.7
```

```
// Define IP address of the communicating gateway
```

```
SIPT-Interface[0]. Set ipaddr '192.168.16.7'
```

```
SMG-[CONFIG]-SIPT-INTERFACE[0]>port 5060
```

```
// 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_active 25// Define the quantity of simultaneous sessions
```

```
SIPT-Interface[0]. Set max_active '25'
```

```
SMG-[CONFIG]-SIPT-INTERFACE[0]>DTMF mode RFC2833
```

```
// Select DTMF – RFC2833 transmission method
```

```
SIPT-Interface[0]. Set DTMF_type '1'
```

```
SMG-[CONFIG]-SIPT-INTERFACE[0]>DTMF payload 101// 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

```

5.3.2.3.3 Routing configuration (session continued)

```

SMG-[CONFIG]>new trunk// Create the trunk group for SS7 link set
NEW 'TRUNK GROUP' [00]: successfully created
SMG-[CONFIG]>new trunk// Create the trunk group for operation via SIP-T interface
NEW 'TRUNK GROUP' [01]: successfully created
SMG-[CONFIG]>new prefix// Create the prefix for transition to SS7 direction
NEW 'PREFIX' [00]: successfully created
SMG-[CONFIG]>new prefix// Create the prefix for transition to SIP-T direction
NEW 'PREFIX' [01]: successfully created
SMG-[CONFIG]>trunk 0// Enter the trunk group configuration mode for SS7 link set
Entering trunk-mode
SMG-[CONFIG]-TRUNK [0]>destination SS7 0// Associate the trunk group 0 with SS7 link set 0
Trunk[0]. Set destination '2'
Trunk[0]. Same destination
'TRUNK GROUP' [00]:
      name:          TrunkGroup00
      disable out:   no
      disable in:    no
      reserv trunk:  none
      direct_pfx:    none
      RADIUS-profile: none
      destination:   Linkset [0]
SMG-[CONFIG]-TRUNK [0]>exit// Exit the trunk group configuration mode for SS7 link set
Leaving TRUNK mode
SMG-[CONFIG]>trunk 1// Enter the trunk group configuration mode for SIP-T interface
Entering trunk-mode

```

```
SMG- [CONFIG]-TRUNK[1]>destination SIPT 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]>prefix 0// Enter the prefix configuration mode for transition to trunk group 0
```

```
Entering Prefix-mode
```

```
SMG- [CONFIG]-PREFIX[0]>type trunk// Define the prefix type — 'transition to trunk group'
```

```
Prefix[0]. Set type '1'
```

```
SMG- [CONFIG]-PREFIX[0]>trunk 0// 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]>prefix 1// 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]>trunk 1// 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]>called transit// 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

```

5.3.2.3.4 Saving configuration and device restart (session continued)



Continuation of the session described above.

```

SMG- [CONFIG]> copy running_to_startup// Save the configuration
tar: removing leading '/' from member names
*****
*****Saved successful
SMG- [CONFIG]> exit // Leaving configuration mode
SMG>reboot yes// Restart device

```

5.4 Appendix D. Transmission of VAS settings from RADIUS server for dynamic subscribers



Available with SMG-PBX and SMG-VAS licenses.

The gateway allows to configure VAS settings to dynamic subscribers using the RADIUS server commands sent in response to RADIUS-Authorization requests during registration. Commands are transferred in the text format using Vendor-Specific attribute (see Section 4.1.18.3 RADIUS replies to voice messages mapping) 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

5.4.1 Request syntax

Command consists of the initial text identifier of a command, VAS activation/deactivation identifier for VAS configuration and configuration commands.

- 'UserService:' is a text identifier defining that this attribute contains the VAS management command.
- 'CFU=', 'CFB=', 'CFNR=', 'CFOS=', 'CT=', 'CallPickup=', 'BLF=', 'Intercom=', 'Conf=', '3PTY=', 'ClearAll=' — VAS activation/deactivation indicator, may take up values 'yes' or 'no', enables or disables VAS respectively.
 - CFU — call forward unconditional
 - CFB — call forward on busy
 - CFNR — call forward on no reply
 - CFOOS — call forward on out of service
 - CT — call transfer
 - CallPickup — call pickup
 - Hold — call holding
 - BLF — busy lamp field (BLF)
 - Intercom — access to intercom and paging calls
 - Conf — conference connection, add-on;
 - 3PTY — 3-way conference;
 - ClearAll — cancel all services.
- 'numCFU=', 'numCFB=', 'numCFNR=', 'numCFOS=' — 'Call forward' VAS configuration command; subscriber's listed directory phone number used for call forwarding may be passed as a value.
- 'limitBLF=' — 'Busy lamp field (BLF)' VAS configuration command; quantity of subscribers may be passed as a value.
- 'CT=', 'CallPickup=', 'Intercom=', 'Conf=', '3PTY=', 'ClearAll=' — do not have 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.

5.4.2 Service activation examples

Objective 1

Activate 'Call forward unconditional' to 12345, 'Call forward on no reply' to 56789 and 'Call pickup' service for a subscriber.

Actions

You should pass the following request:

```
UserService:CFU=yes;numCFU=12345;CFNR=yes;numCFNF=56789;CallPickup=yes"
```

Objective 2

Deactivate 'Call forward unconditional' and 'Call pickup' services, and activate 'BLF for 10 subscribers' and 'Call transfer' services for a subscriber.

Actions

You should pass the following request:

```
UserService:CFU=no;CallPickup=no;CT=yes;BLF=yes;limitBLF=10;
```

5.5 Appendix E. SORM function configuration

Related materials:

The firmware of the SMG-1016M, SMG-2016 and SMG-3016 devices allows you to perform technical requirements for the system of technical means to ensure operational functions investigative activities on electronic automatic telephone exchanges, approved by order of the State Committee for Communications of Russia dated 04/20/1999 No. 70 and by order of the Ministry of Telecom and Mass Communications of Russia No. 268 dated 11/19/2012.

5.6 Appendix F. Interaction of the device with monitoring systems

To be able to monitor in real time emergency situations occurring on the device it is necessary to configure work with the monitoring system.

The absence of any accidents is considered normal operation; when an emergency event occurs, the device state changes to emergency, and when all current alarms are normalized normal operating condition is restored.

Possible device status indications:

- light indication on the front panel – Alarm LED (indication of the Alarm LED is described in the 3.2.6.1 Device light indication in operation),
- indication of the most critical accident in the header of the web configurator (more detailed information is provided in the operation log),
- transmission of accident events to the monitoring system via the SNMP protocol (trap, inform).

Events for which emergency conditions are generated are divided into unconditional and optional:

- *Unconditional* – accidents, the issuance of indications about which is not configurable, these include:
 - *CONFIG* – critical error, configuration file error;
 - *SIPT-MODULE* – critical accident, failure of the software module responsible for the operation IP telephony;
 - *SM-VP DEVICE* – accident, malfunction of the SM-VP IP submodule;
 - *SYNC* – an accident when the synchronization source is lost, or a warning during operation from a low-priority synchronization source;
 - *CDR-FTP* – critical alarm, alarm or warning, occurs when there is an error transferring CDR data to an FTP server, the level of failure is determined by the volume of CDR data awaiting transmission to the server;
 - *PM-POWER-STATE* – warning about the lack of voltage at the output of one of the installed power supplies.
- *Optional* – accidents, the indication of which is configured by the corresponding settings, these include:
 - *STREAM* – critical accident, E1 stream is not working;
 - *STREAM-REMOTE* – warning, remote E1 stream failure;
 - *STREAM-SLIP* – warning on slip stream;

These alarms are configured in the setting of the physical parameters of E1 stream (section 4.1.3.3 Physical settings).

- *LINKSET* – critical accident, SS7 linkset is not in operation;
- *SS7LINK* – accident, problems on the SS7 signal channel;
- *TRUNK-CPS* – exceeding the specified number of calls per second on a trunk group.

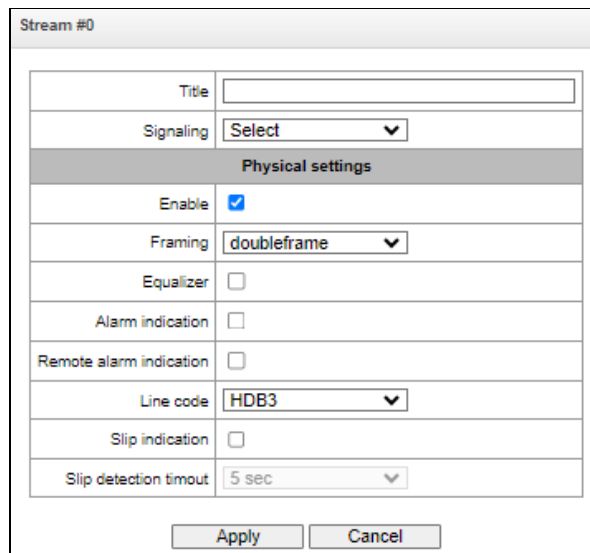
These accidents are configured in the settings of SS7 linkset (section 4.1.5.2 SS7 Linkset).

By default, indication of optional alarms is disabled, i. e. when interacting with monitoring systems, it is necessary to configure alarm indication for all active E1 streams and SS7 Linksets.

To interact with the monitoring system via SNMP protocol, you must enable SNMP protocol and configure the retrieval of SNMP TRAP or INFORM messages to the IP address of the monitoring server.

Setting parameters via the web configurator

1. Configuring the indication of optional alarms when configuring the E1 stream ('E1 streams/Physical parameters' menu, see 4.1.3.3 Physical settings).



Stream #0	
Title	<input type="text"/>
Signaling	Select ▼
Physical settings	
Enable	<input checked="" type="checkbox"/>
Framing	doubleframe ▼
Equalizer	<input type="checkbox"/>
Alarm indication	<input type="checkbox"/>
Remote alarm indication	<input type="checkbox"/>
Line code	HDB3 ▼
Slip indication	<input type="checkbox"/>
Slip detection timeout	5 sec ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

To indicate LOS and AIS failures on the E1 stream, you must set the 'Alarm Indication' flag.

To indicate an RAI failure, you must set the 'Remote Alarm Indication' flag.

To indicate slippage (SLIP) on a stream, you must set the 'Indication SLIP' and configure the SLIP detection timeout.

2. Configuring the indication of optional alarms when configuring SS7 Linkset ('Call routing/SS7 Linkset' menu, see 4.1.5.2 SS7 Linksets).

SS7 Linksets	
SS7 Linkset 1	
Title	Linkset01
TrunkGroup	not set
Access category	[0] AccessCat#0
Dial plan	[0] NumberPlan#0
Scheduled routing profile	Not set
Toll	<input type="checkbox"/>
Alarm indication	<input type="checkbox"/>
Channel selection	successive forward
Reserve SS7 Linkset	Not set
Combined mode	<input type="checkbox"/>
Primary SS7 Linkset	Not set
Secondary SS7 Linkset	Not set
SS7 Timers profile	Profile 0
Stream order by SLC	<input checked="" type="checkbox"/>

To indicate an alarm about SS7 Linkset failure, set the 'Alarm Indication' flag.

3. The SNMP protocol is enabled in the 'TCP/IP Settings/Network interfaces' menu (section 4.1.13.3 Network interfaces).

Services	
Enable Web	<input type="checkbox"/>
Enable Telnet	<input type="checkbox"/>
Enable SSH	<input type="checkbox"/>
Enable SNMP	<input type="checkbox"/>
Enable SIP signaling	<input type="checkbox"/>
Enable RTP transmission	<input type="checkbox"/>
Enable H.323 signaling	<input type="checkbox"/>
Enable RADIUS	<input type="checkbox"/>

To configure, set the 'Use SNMP' flag.

4. SNMP traps are configured in the 'Network Services/SNMP' menu (section 4.1.15.2 SNMP settings).

SNMP	
SNMP trap 1	
Type	trapsink
Community	
IP-address	0.0.0.0
Port	162
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

To configure, specify the type of SNMP message (TRAPv1, TRAPv2, INFORM), password (Community), IP address and port of the SNMP trap receiver.

After setting up and applying the configuration, restart the SNMP agent by clicking 'Restart SNMPd' button.

5.7 Appendix G. Voice messages and music on hold (MOH)

By default, the device features pre-recorded voice message phrases and music to be played on hold. Message playback corresponds to a specific event; the table below contains the list of messages and their correspondence to events.

Table G1 — 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.

Voice messages configured in a trunk group may not work in some cases if the protocol does not allow for it. For example, as with Q.931, in which only the Network side is involved in sending messages, such functionality is not provided for User.

MOH message playback is unconditional and does not depend on the settings.

5.8 Appendix H. 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 transfer* — activate call transfer service (Call Transfer).
- *3Way conference.*
- *Call pickup* (Call pickup).
- *Conference* (CONF, add-on).
- *Disconnect conference by initiator* — when checked, the conference will be disabled when an initiator leaves the conference. Otherwise, the conference will be saved even when the initiator leaves and will be over only when all the participants leave.
- *Intercom* — call service with the Subscriber B automatic reply.
- *Paging* — service is similar to Intercom but with a call performed to the conference number.
- *Change password* (PWD).
- *Outgoing calls restriction.*
- *Restricted by password.*
- *Password activation* (RBP);
- *Do not disturb.*
- *Black list.*
- *Follow me.*
- *Follow me (no response).*
- *Call Park To.*
- *Slot setting.*
- *Extraction from slot.*
- *Voice mail.*
- *Reset all services.*

Starting from firmware version 3.20.10 the following VAS were added:

- *Anonymous call.*
- *Reject anonymous calls.*
- *Reminder.*

VAS functionality becomes available only when additional SMG-VAS license is installed.

For VAS utilization by a subscriber, select the '*Enable VAS*' checkbox in the subscriber settings.

To activate a specific VAS, select the checkbox next to the required service in the 'VAS activation' menu of the subscriber settings.

SIP Subscribers

SIP subscriber		VAS activation	
Subscribers count	<input type="text" value="1"/> <small>Max subscribers count 1998.</small>	Call forward (Unconditional)	<input type="checkbox"/>
Starting description	<input type="text" value="Subscriber#004"/>	Call forward (Busy)	<input type="checkbox"/>
Starting number	<input type="text"/>	Call forward (No-reply)	<input type="checkbox"/>
Starting CallerID number	<input type="text"/>	Call forward (Out of service)	<input type="checkbox"/>
Use CallerID number for redirection	<input type="checkbox"/>	Call forward (Time)	<input type="checkbox"/>
Calling party number type	<input type="text" value="Subscriber"/>	Call hold	<input type="checkbox"/>
Calling party category (RUS)	<input type="text" value="1"/>	Call transfer	<input type="checkbox"/>
Lines operation mode	<input type="text" value="Common"/>	3WAY conference	<input type="checkbox"/>
Lines number	<input type="text" value="1"/>	Call pickup	<input type="checkbox"/>
Redirecting lines number	<input type="text" value="0"/>	Conference	<input type="checkbox"/>
IP-address:port	<input type="text" value="0.0.0.0"/> : <input type="text" value="0"/>	Disconnect conference by initiator	<input type="checkbox"/>
Allow unregistered calls	<input type="checkbox"/>	Intercom/Paging	<input type="checkbox"/>
SIP domain	<input type="text"/>	Change password	<input type="checkbox"/>
SIP profile	<input type="text" value="any"/>	Outgoing calls restriction	<input type="checkbox"/>
PBX profile	<input type="text" value="[0] PBXprofile#0"/>	Restricted by password	<input type="checkbox"/>
Access category	<input type="text" value="[0] AccessCat#0"/>	Password activation	<input type="checkbox"/>
Dial plan	<input type="text" value="[0] NumberPlan#0"/>	Follow me	<input type="checkbox"/>
Authorization	<input type="text" value="not set"/>	Follow me (no response)	<input type="checkbox"/>
Login	<input type="text"/>	Call Park To	<input type="checkbox"/>
Password	<input type="password"/>	Slot setting	<input type="checkbox"/>
Ignore source port after registration	<input type="checkbox"/>	Extraction from slot	<input type="checkbox"/>
Subscriber service mode	<input type="text" value="On"/>	Voice mail	<input type="checkbox"/>
Display name	<input type="text"/>	One Touch Record	<input type="checkbox"/>
Use display name	<input type="text" value="Received only"/>	DND	<input type="checkbox"/>
Multiple registration (SIP-forking)		Blacklist	<input type="checkbox"/>
SIP-forking	<input type="checkbox"/>	Anonymous call	<input type="checkbox"/>
Max registered contacts number	<input type="text" value="2"/>	Reject anonymous calls	<input type="checkbox"/>
Busy-Lamp-Field (BLF) settings		Reminder	<input type="checkbox"/>
Enable subscription	<input type="checkbox"/>	Reset all services	<input type="checkbox"/>
Max subscribers number	<input type="text" value="10"/>	Voice Notification	<input type="checkbox"/>
Monitoring group	<input type="text" value="0"/>		
Intercom call settings			
Intercom call type	<input type="text" value="one-way"/>		
Intercom call priority	<input type="text" value="3"/>		
Intercom SIP-header	<input type="text" value="Answer-Mode: Auto"/>		
Pause before answer, sec	<input type="text" value="0"/>		
VAS settings			
CLIRO	<input type="checkbox"/>		
Enable VAS	<input checked="" type="checkbox"/>		
RingBack settings			
Mode	<input type="text" value="Default"/>		
File name	<input type="text"/>		

5.8.1 Working with 'Call hold', 'Call transfer', 'Three-way conference' services

'Call transfer' service operation requires that the subscriber terminal party supports FLASH transmission via SIP using SIP-INFO, RFC2833 methods. Also, the subscriber terminal party should have an inband, SIP-INFO or RFC2833 DTMF signal transmission methods configured; make sure that the similar method is selected in the subscriber SIP profile configuration.

'Call transfer' service configuration example

Subscriber A calls Subscriber B; Subscriber B may press FLASH during conversation to put the Subscriber A on hold, at that time, 'Music on hold' will be played to the subscriber A, and Subscriber B will hear 'PBX response' tone; at that, timeouts for dialling the Subscriber C number will be activated, their values are provided below. After the number dial and Subscriber C reply, the options are as follows:

While being in a call state with a Subscriber A, put him on hold with hook flash (R), wait for 'PBX response' tone and dial a Subscriber C number. When Subscriber C answers, the following operations will be possible:

- R 0 — disconnect a subscriber on hold, connect to online subscriber.
- R 1 — disconnect an online subscriber, connect to subscriber on hold.
- R 2 — switch to another subscriber (change a subscriber).
- R 3 — three-way conference.
- R 4 — call transfer. Voice connection will be established between Subscribers A and C.
- Hangup — call transfer; voice connection will be established between Subscribers A and C.

'Call transfer' service timeouts — at the moment, these timeouts are at their default values; their configuration will be implemented in future firmware versions.

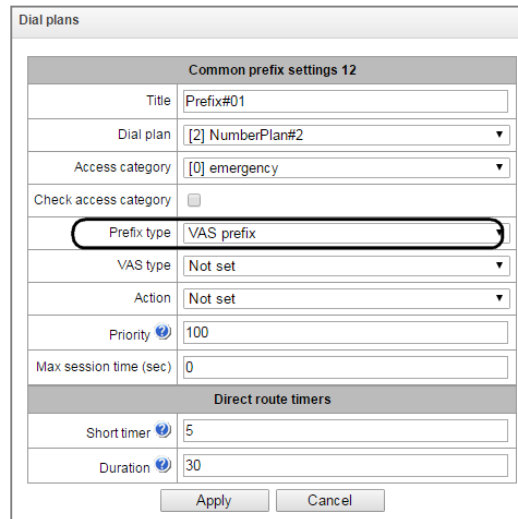
- First digit dial timeout: 15 seconds.
- Next digit dial timeout: 5 seconds.
- Busy tone timeout: 60 seconds.

5.8.2 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 4.1.6.1.2 VAS management) or using VAS management from the phone unit (according to RD-45), this method is described below.

VAS configuration from the phone unit (according to GOST 45.49-96)

The subscriber may activate or deactivate the service themselves by dialling specific prefixes on their phone unit. Redirection service prefixes are configured in the dial plan (4.1.4 Dial plans) add a new prefix with the 'Prefix type'/'VAS prefix' value.



Common prefix settings 12	
Title	Prefix#01
Dial plan	[2] NumberPlan#2
Access category	[0] emergency
Check access category	<input type="checkbox"/>
Prefix type	VAS prefix
VAS type	Not set
Action	Not set
Priority	100
Max session time (sec)	0
Direct route timers	
Short timer	5
Duration	30

For VAS, it is recommended to use the following prefix values:

5.8.2.1 Call forward unconditional (CF Unconditional):

- Activation (*21*|*21*x.#);
- Deactivation (#21#);
- Control (*#21*|#21*x.#).

5.8.2.2 Call forward on busy (CF Busy):

- Activation (*22*|*22*x.#);
- Deactivation (#22#);
- Control (*#22*|#22*x.#).

5.8.2.3 Call forward on no reply (CF No reply):

- Activation (*27*|*27*x.#);
- Deactivation (#27#);
- Control (*#27*|#27*x.#).

5.8.2.4 Call forward on out of service (CF Out Of Service):

- Activation (*62*|*62*x.#);
- Deactivation (#62#);
- Control (*#62*|#62*x.#).

5.8.2.5 Call forward on time

- Activation (*28*x.#);
- Deactivation (#28#);
- Control (*#28#|#28*x.#).

Digits 21, 22, 27, 62, 28 may take up any arbitrary value; these examples feature recommended values.



In the subscriber terminal dial plan, you should define VAS management prefixes. Operation with VAS at the gateway is performed after reception of the INVITE message with the required combination of digits from the subscriber terminal.

'Call transfer' service timeouts are at their default values at the moment; their configuration will be implemented in future firmware versions:

- Call forward on no reply (CF No reply) timeout: 10 seconds
- Call forward on out of service (CF Out Of Service) timeout: 10 seconds

Example of VAS configuration from the phone unit

Objective

The subscriber should configure unconditional forwarding 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#.

Example of VAS configuration for Call forward on time

Objective

The subscriber should schedule time forwarding from 12 to 2 p.m. from Mon to Fri to the phone number

222333444.

Actions

1. In the Internal Resources → Scheduled routing section, create and/or edit the schedule by checking the boxes for those hours and days of the week when redirection should work, for this example these are columns 12, 13, 14 for the lines Mon, Tue, Wed, Thu, Fri.
2. In the settings of SIP subscriber on which you want to configure forwarding, enable call forward on time.
3. The subscriber sets the number for forwarding and the schedule configured in step 1 by dialing *28*

<number> * <shedule_idx> #, where:

<number> – number to which the call will be forwarded

<shedule_idx> – schedule index according to which redirection will be performed

for this example, the dial will look like this: *28*222333444*0#

4. You can check that the service is activated by dialing *#28# or *#28*222333444*0#. If the service is activated, the dialed number and the schedule coincide with the previously specified one, then the subscriber will hear a dial tone. If the service is not activated or the dialed number and schedule do not coincide with the previously set one, the subscriber will hear a busy signal. To deactivate the service, the subscriber should dial #28#.

5.8.3 Conference with sequential participant collection (Conference)

This service allows the initiator to establish the conference by consequently adding participants using subscriber hold feature.

Upon the initiator hanging up, participants will hear the busy tone.

When the initiating subscriber hangs up, the rest of the participants receive a 'Busy' signal if the initiating subscriber has 'Disconnect conference by initiator' option enabled. If VAS is disabled, then when the initiating subscriber hangs up, the conference will continue to work. The maximum number of participants for all collected conferences for SMG-1016M is 40, for SMG-2016/3016 – 160. One conference can have no more than 40 participants. For example: on the SMG-1016M you can gather one conference for 40 participants, 10 conferences for 4 participants, etc. On SMG-2016/3016 you can gather 4 conferences of 40 participants, 10 conferences of 16 participants, etc.

This functionality can be activated both on analog phones using the R key (short hang up (FLASH)) and on SIP phones using the CONF&TRANSFER/HOLD keys).

Access to the service is managed by the "Conference" checkbox.

Usage	* 71# <CONF> R <RS> <NUMBER 1> <CONF> R <RS> <NUMBER 2> < CONF> ...
-------	--

where:

<NUMBER N> — number of the subscriber participating in a conference.

<CONF> — conference call state

<RS> — station response signal, waiting for dialing of the subscriber who needs to be added to the conference;

R — short hang up (FLASH), if your telephone does not have a FLASH button, you can use the * or # buttons. To do this, you need to set the option 'HOLD by' flash/*/# in the sip profile in the DTMF reception/transmission section.

- For the service to work, the presence of the VAS 'Conference' prefix in the dial plan is required.
- For the service to work, the 'Call Hold' and 'Conference' options should be enabled in the VAS block in the SIP subscriber settings.

An example of using a conference call with sequential dialing, when subscriber A gather subscribers B and C into a conference:

Subscriber A makes a call to *71# and hears the welcome message "Welcome to conference", then puts the conference on hold <R> and dials the number of subscriber B, when subscriber B accepts the call, the connection between A and B is disconnected and they are both added to conference, subscriber B hears a welcome message, after which the subscribers A, B are in the conference.

Subscriber A puts the conference on hold again <R> and dials subscriber C number, when subscriber C accepts the call, the connection between A and C is disconnected and they are both added to a conference, subscriber C hears a welcome message, after which subscribers A, B, C are in the conference.

Functionality description for SIP telephones:

Usage	CONF TRANSFER <NUMBER 1> TRANSFER < NUMBER 2> CONF < STATE >...
Usage	* 71# HOLD < NUMBER 1> < STATE > < NUMBER 2> < STATE > HOLD < STATE > ...

Where:

<NUMBER N> – subscriber number – participant in the conference call;

< STATE > – conference call status;

CONF – conference (should comply with RFC 4579 and the conference number should be identical to 'Conference' prefix in the dial plan);

HOLD – call on hold;

TRANSFER – call transfer.

- For the service to work, the presence of the VAS 'Conference' prefix in the dial plan is required.
- For the service to work via 'HOLD', the 'Call Hold' and 'Conference' options should be enabled in the VAS block in the SIP subscriber settings. In addition, enable 'Call Transfer' in the SIP subscriber settings, increase the number of lines to 2, for the initiating subscriber for the conference collection scenario via CONF&TRANSFER.

An example of collecting a conference for a SIP phone via CONF&TRANSFER:

Collection from the conversation:

- A makes a call to B, B answers.
- A presses the CONF button on the phone.
- Both numbers are included in the conference, the conference is gathered.
- Adding subsequent participants:
 - A presses TRANSFER, dials C, C answers and gets into the conference;
 - The station hangs up the A-C call;

- A releases the conference from hold (CONF) – now all subscribers are in the conference.
- Or A does not release the conference from hold and immediately makes a transfer (TRANSFER) to the next subscriber D (adds to the conference) and so on.

Collection with CONF button:

- A presses CONF, thereby making a call to *71# and hears the welcome message 'Welcome to the conference';
- Adding subsequent participants:
 - A presses TRANSFER, dials B's number, B answers and gets into the conference;
 - The station hangs up the A-B call;
 - A releases the conference from hold (CONF) — now all subscribers are in the conference
 - Or A does not release the conference from hold and immediately transfers it to the next subscriber C (adds to the conference) and so on.

5.8.4 Call pickup

This service allows to answer the call directed to another subscriber. Access to service is managed by the VAS 'Call pickup' checkbox.

Usage	* 66 *<NUMBER>#
-------	-----------------

where:

<NUMBER> — number of the subscriber for call pickup.

5.8.5 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 used phone units should support Answer-Mode: Auto for RFC 5373. Access to service is managed by the VAS 'Intercom' checkbox.

Usage	*80*<NUMBER>#
-------	---------------

where:

<NUMBER> — number of the intercom call subscriber.

Paging call service operates in the similar way to the intercom call but it enables calls to subscriber groups using the conference number. For that, define the call group with the conference number in call group section (Section 4.1.7.12 Hunt groups) and add all subscribers using this service into it.

Usage	*81*<NUMBER>#
-------	---------------

<NUMBER> — conference number of the paging call.

5.8.6 Password activation/deactivation, restricted by password

These services provide the opportunity to override restrictions on access to outgoing calls (controlled by 'Outgoing calls restriction' service).

For example, if a restriction is set on outgoing communication, then the 'Restricted by password' service makes it possible to cancel the access restriction only for the next attempt to establish an outgoing connection. The 'Password Activation' service cancels/sets a restriction on outgoing communication for all subsequent outgoing communication attempts.

The access to the service is managed by checking the 'Password activation' box in VAS activation window.

The access to the 'Restricted by password' service is managed by checking corresponding box in VAS activation window.

Password activation	* 29 * <PASSWORD> #
Password deactivation	# 29 #
Restricted by password	* 32 * <PASSWORD> #

Where:

<PASSWORD> – private subscriber password.

5.8.7 Change password

This service allows a subscriber to change a password assigned by PBX service personnel. The access to the service is managed by checking the 'Change password' box in VAS activation window.

Change password	* 30 * <PASSWORD1> * <PASSWORD2> * <PASSWORD2> #
-----------------	--

where:

<PASSWORD1> – current password;

<PASSWORD2> – a new password, which you need to enter twice. The password must contain 4 characters.

5.8.8 Outgoing calls restriction

The service allows to establish restriction on outgoing communication for phone calls to some directions. The following groups of communication types are defined:

Group 1 – only calls to emergency services;

Group 2 – only local and emergency calls;

Group 3 – communication types of group 1 and group 2 and zone communication.

The type of communication is set in prefix parameters.

To override restrictions set by this service, you may use 'Restrict by password' and 'Password activation' services. To reestablish the restrictions, use 'Password deactivation' service.

The access to the service is managed by checking the 'Outgoing calls restriction' box in VAS activation window.

Activate the service	* 34 * <PASSWORD> * N #
Cancel the service	# 34 * <PASSWORD> #
Control	* # 34 * <PASSWORD> #

<N> – a number of a group of permitted outgoing communication.

5.8.9 Do not disturb

The service allows to restrict calls on a subscriber and set a whitelist of numbers which are permitted to call the subscriber even in 'Do Not Disturb' mode.

The access to the service is managed by checking the 'Do not disturb' box in VAS activation window.

Activate the service	* 26 #
Cancel the service	# 26 #
Control	* # 26 #
Add a number to whitelist	* 26 * <NUMBER >#
Remove a number from whitelist	# 26 * <NUMBER>#
Remove all numbers from blacklist	# 26 * 0 # # 26 * 00 #

5.8.10 Blacklist

The service allows to forbid certain numbers to implement calls to a subscriber.

The access to the service is managed by checking the 'Blacklist' box in VAS activation window

Activate the service	* 61 * <PASSWORD> #
Cancel the service	# 61 * <PASSWORD> #
Control	* # 61 * <PASSWORD> #
Add a number to blacklist	* 61 * <PASSWORD> * <NUMBER>
Remove a number from blacklist	# 61 * <PASSWORD> * <NUMBER>
Remove all numbers from blacklist	# 61 * <PASSWORD> * 0 # # 61 * <PASSWORD> * 00 #

5.8.11 Reset all services

This service allows the subscriber to cancel all activated services from their phone unit using a single cancelling procedure. Cancelling procedure includes the service code and password code.

Access to service is managed by checking the 'Reset all services' box in VAS category checkbox.

Usage	* 50#
-------	-------

5.8.12 Follow me

Description

With the 'Follow me' service, you can enable call forwarding for all calls from your telephone set to a remote one, using the remote phone. Service use example: a subscriber located outside their workplace wants to activate call forwarding for all calls from their work telephone set to a telephone set which is now 'at hand'.

Use case

Service activation:

The service involves two telephone sets: local and remote. The subscriber wants to forward all calls from the local telephone set to the remote telephone set.

To do this, first of all, the subscriber should activate the service with or without PIN on the local telephone set

(i. e. while being in the workplace the subscriber should enable the use of the service). After that, the subscriber, using their remote phone, can enable call forwarding from the local telephone set to the remote telephone set (if the service activation involved a PIN code, then you will have to enter the PIN; otherwise, the PIN is not needed).

Service deactivation:

Remote call forwarding can be turned off from both remote and local telephone sets. You can deactivate the service only from the local telephone set, with or without a PIN-code.

Service management from the telephone set

The service activation with a temporary PIN code is performed on the local number	*23*PIN#
The service activation without a PIN code is performed on the local number	*23#
Call forwarding from the local to the remote telephone set with a temporary PIN is performed on the remote number	* 23 * PIN * LOCAL_PHONE #
Call forwarding from the local to the remote telephone set without a PIN code is performed on the remote number	* 23 ** LOCAL_PHONE#
Cancelling call forwarding from the local to the remote telephone set without a temporary PIN code is performed on the remote number	#23**LOCAL_PHONE#
Cancelling call forwarding from the local to the remote telephone set with a temporary PIN code is performed on the remote number	#23*PIN*LOCAL_PHONE#
Deactivation, is performed on the local number	#23#
Status view, is performed on the local number	*#23#

Where:

- PIN – a secret digital code consisting of 4 characters;
- LOCAL_PHONE – the phone number from which the calls will be forwarded.

5.8.13 Follow me no response

Description

Using the 'Follow me (no response)' service, you can forward all calls from the local number to the remote number, if a call to the local number has not been answered within the specified time interval.

Use case

The service involves two telephone sets: local and remote. The subscriber wants all calls that come to the local phone and have not been answered within the specified time interval, to be forwarded to the remote telephone set. Activation/deactivation of the service is performed only on the local phone number. Request for call forwarding is performed on the remote phone.

Service management from the telephone set

The service activation with a temporary PIN code is performed on the local number	*25*PIN#
The service activation without a PIN code is performed on the local number	*25#
Call forwarding from the local to the remote telephone set with a temporary PIN is performed on the remote number	* 25 * PIN * LOCAL_PHONE #
Call forwarding from the local to the remote telephone set without a PIN code is performed on the remote number	* 25 ** LOCAL_PHONE#
Cancelling call forwarding from the local to the remote telephone set without a temporary PIN code is performed on the remote number	#25**LOCAL_PHONE#
Cancelling call forwarding from the local to the remote telephone set with a temporary PIN code is performed on the remote number	#25*PIN*LOCAL_PHONE#
Deactivation, is performed on the local number	#25#
Status view, is performed on the local number	*#25#

Where:

- PIN – a secret digital code consisting of 4 characters;
- LOCAL_PHONE – the phone number from which the calls will be forwarded.

5.8.14 Call park to

Description

The 'Call Park to' service is intended for placing a call on hold by one subscriber and removing it from hold by another subscriber.

Placing a call into a parking slot is done by performing an unattended transfer during a conversation to the number of the code for placing a call in the slot.

Use case

It is necessary to put the subscriber on hold in parking slot number 15.

- During the call, a transfer is made to the number *57*15#.
- Another subscriber can remove the subscriber from this parking slot number 15 by calling *58*15#.

Service management from the telephone set

Slot setting	* 57*<PARKING_SLOT_NUMBER>#
Extraction from slot	* 58*< PARKING_SLOT_NUMBER >#

Where:

PARKING_SLOT_NUMBER – number of the parking slot in which the subscriber should be placed.

If you dial *57# on your telephone, then PARKING_SLOT_NUMBER = number of the initiating subscriber placing into the slot.

5.8.15 Voice mail

Description

The 'Voice Mail' service allows subscriber A to leave a message to subscriber B (call from A to B) in case subscriber B is unavailable/does not answer.

After fully listening to a new message, it is marked as old. Also, a message is marked as old if the user presses the digit 3 (go to the next message).

Upon activation, the following voice mail options are available to the subscriber:

- Unconditional – unconditionally forwarding an incoming call to the subscriber's voice mail;
- No-reply – forwarding an incoming call to voice mail if the subscriber does not answer;
- Busy – forwarding the incoming call to voice mail when the subscriber is busy;
- Out of service – forwarding an incoming call to voice mail when the subscriber is unavailable;
- DND – forwarding an incoming call to voice mail if the Do Not Disturb service is activated.

Edit VAS block of Subscriber#006 ()	
Numbers Whitelist Blacklist	
VAS block for subscriber Subscriber#006	
Number for call forward (unconditional)	<input type="text"/>
Number for call forward (busy)	<input type="text"/>
Number for call forward (no-reply)	<input type="text"/>
Number for call forward (out of service)	<input type="text"/>
Number for call forward (time)	<input type="text"/>
Password	<input type="text" value="1111"/>
Password activation	<input type="checkbox"/>
Restrict out	<input type="text" value="all allowed"/>
"Anonymous call" service activation	<input type="checkbox"/>
"Reject Anonymous calls" service activation	<input type="checkbox"/>
Follow me	
Follow me activation	<input type="checkbox"/>
Follow me pin	<input type="checkbox"/>
Follow me number	<input type="checkbox"/>
Follow me pin	<input type="text"/>
Follow me number	<input type="text"/>
Follow me (no response)	
Follow me activation	<input type="checkbox"/>
Follow me pin	<input type="checkbox"/>
Follow me number	<input type="checkbox"/>
Follow me (no response)pin	<input type="text"/>
Follow me (no response)number	<input type="text"/>
Call forward (Time)	
Schedule selection	<input type="text" value="not set"/>
Voice mail	
Voice mail activation	<input type="text" value="not set"/>
Password	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	



At the moment, the voice mailbox subscription mode (MWI (RFC3842)) is not implemented, thus the subscriber will not be able to find out whether a new voice message has been left or not. To inform about the presence of messages, you need to use the voice menu (*90# or *91*Subscriber number with voicemail#).



The mail from a remote phone can be listened to only if the remote subscriber has a voicemail password set.



When changing the password through the voice menu, if the old password is not set, just press the hash key.

Message playing:

To play voice messages, the subscriber dials the code *90# from his/her own phone, dials the code *91# or *91*NUMBER# from someone else's phone, and then enters the voice menu.

Use case

To activate voice mail, it is necessary to enable the Voice Mail of the VAS for the subscriber.

VAS activation	
Call forward (Unconditional)	<input type="checkbox"/>
Call forward (Busy)	<input type="checkbox"/>
Call forward (No-reply)	<input type="checkbox"/>
Call forward (Out of service)	<input type="checkbox"/>
Call forward (Time)	<input type="checkbox"/>
Call hold	<input type="checkbox"/>
Call transfer	<input type="checkbox"/>
3WAY conference	<input type="checkbox"/>
Call pickup	<input type="checkbox"/>
Conference	<input type="checkbox"/>
Disconnect conference by initiator	<input type="checkbox"/>
Intercom/Paging	<input type="checkbox"/>
Change password	<input type="checkbox"/>
Outgoing calls restriction	<input type="checkbox"/>
Restricted by password	<input type="checkbox"/>
Password activation	<input type="checkbox"/>
Follow me	<input type="checkbox"/>
Follow me (no response)	<input type="checkbox"/>
Call Park To	<input type="checkbox"/>
Slot setting	<input type="checkbox"/>
Extraction from slot	<input type="checkbox"/>
Voice mail	<input type="checkbox"/>
One Touch Record	<input type="checkbox"/>
DND	<input type="checkbox"/>
Blacklist	<input type="checkbox"/>
Anonymous call	<input type="checkbox"/>
Reject anonymous calls	<input type="checkbox"/>
Reminder	<input type="checkbox"/>
Reset all services	<input type="checkbox"/>
Voice Notification	<input type="checkbox"/>

Next, in the 'VAS Management' set the desired mode of operation:

Edit VAS block of Subscriber#006 ()	
Numbers Whitelist Blacklist	
VAS block for subscriber Subscriber#006	
Number for call forward (unconditional)	<input type="text"/>
Number for call forward (busy)	<input type="text"/>
Number for call forward (no-reply)	<input type="text"/>
Number for call forward (out of service)	<input type="text"/>
Number for call forward (time)	<input type="text"/>
Password	<input type="text" value="1111"/>
Password activation	<input type="checkbox"/>
Restrict out	<input type="text" value="all allowed"/>
"Anonymous call" service activation	<input type="checkbox"/>
"Reject Anonymous calls" service activation	<input type="checkbox"/>
Follow me	
Follow me activation	<input type="checkbox"/>
Follow me pin	<input type="checkbox"/>
Follow me number	<input type="checkbox"/>
Follow me pin	<input type="text"/>
Follow me number	<input type="text"/>
Follow me (no response)	
Follow me activation	<input type="checkbox"/>
Follow me pin	<input type="checkbox"/>
Follow me number	<input type="checkbox"/>
Follow me (no response)pin	<input type="text"/>
Follow me (no response)number	<input type="text"/>
Call forward (Time)	
Schedule selection	<input type="text" value="not set"/>
Voice mail	
Voice mail activation	<input type="text" value="not set"/>
Password	<input type="text" value="not set"/> <ul style="list-style-type: none"> Unconditional No-reply Busy Out of service DND
<input type="button" value="Apply"/>	

Now, when a call is received by this subscriber, messages will go to voice mail, and the subscriber will be able to listen to them by dialing *90# on their telephone and following the prompts of the voice menu.

The subscriber can also set up the voice mail operating mode, using the voice menu and following its prompts.

From the voice menu, the subscriber can:

- Listen to voice messages
- Delete voice messages
- Change the voice mail mode
- Set a password for voice mail

5.8.16 One touch record

Description

The service allows the subscriber to start recording a conversation during a conversation.

Use case:

Subscribers A and B are talking, and A has the 'One touch record' service enabled. When during the dialogue, the subscriber A dials code 99, a sound signal is played, and the recording of the conversation begins. The recording of the conversation stops when the dialogue ends or if the subscriber A dials code 99 again during the dialogue.

If the device is configured to record a conversation by a mask that the talking parties match, and one of them tries to start one touch record, an audio signal will be played, but a new conversation recording will not start. If one touch record is activated for both subscribers who are in a dialogue, and both subscribers dial code 99 to start recording, then the sound signal will be played for both subscribers A and B, but the recording will start only once — after the subscriber's command, who dialed the code first.

5.8.17 Anonymous call

Description

The 'Anonymous Call' service allows you to make anonymous calls by hiding the phone number and display name of the caller from the call recipient.

The service is configured on SMG in the SIP subscriber settings. The 'Anonymous call' option is set in the VAS block.

After this, in the 'VAS Management' tab, you can activate and deactivate the service for the subscriber. The subscriber can also control the activation of the service from the telephone.

Service management from the telephone set

Service activation	*31#
Service deactivation	#31#
Control	*#31#

- To activate the service from a telephone set, the presence of the 'Anonymous Call' prefix in the dial plan is required.
- Control: short beeps – activated, busy signal – deactivated.

5.8.18 Reject anonymous calls

Description

The 'Reject anonymous calls' service rejects incoming calls if the caller hides from the call recipient's phone number and display name.

The service is configured on SMG in the SIP subscriber settings. In the VAS block, set the option 'Reject anonymous calls'.

After this, in the 'VAS Management' tab, you can activate and deactivate the service for the subscriber. The subscriber can also control the activation of the service from the telephone.

Service management from the telephone set

Service activation	*16#
Service deactivation	#16#
Control	*#16#

- To activate the service from a telephone set, the presence of the 'Reject anonymous calls' prefix in the dial plan is required.
- Control: short beeps – activated, busy signal – deactivated.

5.8.19 Reminder

Description

The 'Reminder' service allows you to receive an incoming call to the phone on which you activated this service at a given time. The subscriber, when activating the service, indicates the time of its activation. At the appointed time, the system makes a call to the subscriber. When the subscriber answers the call, an alarm tone is played.

The service is configured on SMG in the SIP subscriber settings. The 'Reminder' option is set in the VAS block. After this, the subscriber can control the activation of the service from the telephone.

Service management from the telephone set

Service activation	*55*<HHMM>#
Service deactivation	#55#
Control	*#55#

- <HHMM> – call at the appointed hour (HH) and minute (MM), in 24-hour format.
- To activate the service from a telephone set, the presence of the 'Reminder' prefix in the dial plan is required.
- Control: short beeps – activated, busy signal – deactivated, error signal – the time was entered incorrectly.

5.9 Appendix I. Radius call management service¹

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 4.1.18.3 RADIUS replies to voice messages mapping) with vendor number assigned to Eltex and equal to 35265 and Eltex-AVPair attribute name with the number 1.

In general, Eltex-AVPair attribute format will be as follows:

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1):<${COMMAND-STRING}>
```

By transferring various commands in `${COMMAND-STRING}`, you may manage the following parameters:

- CgPN and CdPN number modification:

Number modification may be performed at two stages during call processing:

- For the incoming communication, before the call passes through the dial plan, i.e. before its routing. For that purpose, CgPNin and CdPNin values are used for Calling and Called numbers respectively.
- For the outgoing communication, after the call passes through the dial plan and after its routing. For that purpose, CgPNout and CdPNout values are used for Calling and Called numbers respectively.

For CgPN numbers, you may modify the following parameters in addition to the number itself:

- *numtype* — CgPN number type
- *plantype* — CgPN dial plan type
- *presentation* — CgPN 'presentation' field value

For CdPN numbers, you may modify the following parameters in addition to the number itself:

- *numtype* — CdPN number type
- *plantype* — CdPN dial plan type

5.9.1 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).

¹ Available only under RCM license.

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=<$plantype>;presentation=<$presentation>
```

Where:

'CallManagement:CgPNin=<\$modify-mask>';' — required part.

'numtype=<\$numtype>;plantype=<\$plantype>;presentation=<\$presentation>' — optional part.

```
2. CallManagement:CdPNin=;numtype=<$numtype>;plantype=<$plantype>
```

Where:

'CallManagement:CgPNin=;' — required part with an empty modification mask.

'numtype=<\$numtype>;plantype=<\$plantype>' — optional part.

```
3. CallManagement:CgPNin=<$modify-mask>;
```

Where:

'CallManagement:CgPNin=<\$modify-mask>';' — required part. Optional part is absent.

Values of parameters used in commands are as follows:

- *\$modify-mask* — number modification rule (for rule modification syntax, see Section 4.1.7.6.4.1 Modification rule syntax).
- *\$numtype* — represents one of the values: international, national, network-specific, subscriber, unknown.
- *\$plantype* — represents one of the values: isdn, national, private, unknown.
- *\$presentation* — represents one of the values: allowed, restricted, not-available, spare.

The gateway allows to pass the number modification command parameters in multiple attributes. Thus, a set of commands:

```
'CallManagement:CgPNin=<$modify-mask>'
'CallManagement:CgPNin=;numtype=<$numtype>'
'CallManagement:CgPNin=;presentation=<$presentation>'
```

is equivalent to a single command:

```
'CallManagement:CgPNin=<$modify-mask>;numtype=<$numtype>;presentation=<$presentation>'
```



If one of the optional parameters (*numtype*, *plantype*, *presentation*) should remain unchanged, do not include it in the request, but you must specify the number type

(CgPNin, CdPNin, CgPNout, CdPNout) that passed fields belong to in the beginning of the request.

Example:

For incoming communication, add prefix +7383 to CgPN, change its number type to national and define presentation restricted.

To do that, it is sufficient to pass the attribute with the following value in Access-Accept reply from the RADIUS server:

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1):  
CallManagement:CgPNin=+7383;numtype=national;presentation=restricted
```

That is also equivalent to three attributes with the following values:

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): CallManagement:CgPNin=+7383  
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): CallManagement:CgPNin=;numtype=national  
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): CallManagement:CgPNin=;presentation=restricted
```

5.9.2 Call routing management

Using RADIUS server commands, you may manage the call routing process, i.e. to transfer it to another dial plan of the gateway and unconditionally forward it to a prefix created in the configuration (equivalent to the 'direct prefix' parameter described in Section 4.1.5.1 Trunk groups)

Routing management command consists of the required part only:

'CallManagement:' is a text identifier defining that this attribute contains the call management command.

'NumberingPlan' — identifier that indicates the dial plan change command.

'DirectRoutePrefix' — identifier that indicates the direct routing prefix selection command.

In general, command format will be as follows:

```
CallManagement:NumberingPlan=<${numplan_idx}>  
CallManagement:DirectRoutePrefix=<${prefix_index}>
```

where

`${numplan_idx}` — dial plan sequential number.

`${prefix_index}` — ID of a prefix created in the dial plan.

Example:

Change the call dial plan to the 3rd one.

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): CallManagement:NumberingPlan=3
```

5.9.3 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.

The priority of changing the AON category depends on the type of subscriber.

The dynamic subscriber:

1. Modification via RADIUS;
2. Modification via modification tables on the incoming leg;
3. Modification via modification tables on the outgoing arm.

The other subscribers:

1. Modification via modification tables on the incoming leg;
2. Modification via RADIUS;
3. Modification via modification tables on the outgoing arm.

Example:

Define subscriber category (calling party category) equal to 7.

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): CallManagement:AONCategory=7
```

5.9.4 Subscriber parameter management¹

For dynamic subscribers, you may define the 'Line quantity' and line operation mode parameter at the subscriber registration phase.

Subscriber parameter management command consists of the required part only:

- 'UserManagement:' is a text identifier defining that this attribute contains the subscriber record management command.
- 'MaxActiveLines' is an identifier indicating the quantity of active lines that are available to the current subscriber in common mode. The line operation mode will be set as common (even if separate mode has been specified), if the parameter 'MaxActiveLines' is specified.
- 'MaxEgressLines' - identifier, which indicates the number of egress lines that are available for subscriber in separate mode. The parameter can be combined with the 'MaxIngressLines';
- 'MaxIngressLines' - identifier, which indicates the number of ingress lines that are available in separate mode. The parameter can be combined with the 'MaxEgressLines';

¹ Available with SMG-PBX and SMG-VAS licenses, SMG-RCM license is not required.

In general, command format will be as follows:

```
"UserManagement:MaxActiveLines=<$line_count>"  
"UserManagement:MaxEgressLines=<$egress>;MaxIngressLines=<$ingress>;"  
"UserManagement:MaxEgressLines=<$egress>"  
"UserManagement:MaxIngressLines=<$ingress>"
```

Where:

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

\$egress — the number of egress connections that are available to the subscriber;

\$ingress — the number of ingress connections that are available to the subscriber.

Examples:

Define common line mode and three active lines for a subscriber.

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

Set the separate line mode: 3 egress and 2 ingress lines

```
Vendor-Specific(26):                               Eltex(35265):                               Eltex-AVPair(1):  
UserManagement:MaxEgressLines=3;MaxIngressLines=2
```

Set the common line mode: 2 active lines. (MaxActiveLines has unconditional priority over MaxEgressLines and MaxIngressLines)

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1):  
UserManagement:MaxEgressLines=6;MaxActiveLines=2;MaxIngressLines=5
```

5.10 APPENDIX J. MONITORING AND MANAGEMENT VIA SNMP

The gateway supports configuration and monitoring via **Simple Network Management Protocol (SNMP)**.

Monitoring functions:

- collection of general information about the device, sensor readings, installed firmware
- E1 streams and channels state
- VoIP submodules and channels state
- SS7 Linksets state
- SIP interfaces state

Management functions:

- firmware version updating
- current configuration saving
- device reboot
- SIP subscriber management
- management of dynamic SIP subscriber groups

The following format will be accepted for 'Inquiry description' column in the tables of OID description:

- Get – an object or tree value can be displayed by sending 'GetRequest'.
- Set – set an object value by sending 'SetRequest' (Please pay attention that if you set value by SET inquiry, you need OID in 'OID.0' form).
- {} – object name or OID;
- N – integer type numeric parameter is used in the command;
- U – unsigned integer numeric parameter is used in the command;
- S – string parameter is used in the command;
- A – IP address is used in the command (some commands using IP address as an argument has string type of data - 's').

Table J1 – Command examples

Inquiry description	Command
Get {}	snmpwalk -v2c -c public -m +ELTEX-SMG \$ip_smg activeCallCount
Get {}.x	snmpwalk -v2c -c public -m +ELTEX-SMG \$ip_smg pmExist.1 snmpwalk -v2c -c public -m +ELTEX-SMG \$ip_smg pmExist.2 etc.
Set {} N	snmpset -v2c -c public -m +ELTEX-SMG \$ip_smg \ smgSyslogTracesCalls.0 i 60
Set {} 1	snmpset -v2c -c private -m +ELTEX-SMG \$ip_smg smgReboot.0 i 1
Set {} U	snmpset -v2c -c public -m +ELTEX-SMG \$ip_smg \ getGroupUserByID.0 u 2
Set {} S	snmpset -v2c -c private -m +ELTEX-SMG \$ip_smg \ smgUpdateFw.0 s "smg1016m_firmware_3.8.0.1966.bin 192.0.2.2"
Set {} "NULL"	snmpset -v2c -c private -m +ELTEX-SMG \$ip_smg \ getUserByNumber.0 s "NULL"
Set {} A	snmpset -v2c -c private -m +ELTEX-SMG \$ip_smg \ smgSyslogTracesAddress.0 a 192.0.2.44

Examples of requests execution:

The inquiries which are shown below are equivalent. For instance, different types of requests for activeCallsCount object, that displays a number of current calls on SMG, are shown below.

```
$ snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 activeCallCount
ELTEX-SMG::activeCallCount.0 = INTEGER: 22
```

```
$ snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 smg.42.1
ELTEX-SMG::activeCallCount.0 = INTEGER: 22
```

```
$ snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 1.3.6.1.4.1.35265.1.29.42.1
ELTEX-SMG::activeCallCount.0 = INTEGER: 22
```

```
$ snmpwalk -v2c -c public 192.0.2.1 1.3.6.1.4.1.35265.1.29.42.1
SNMPv2-SMI::enterprises.35265.1.29.42.1.0 = INTEGER: 22
```

5.10.1 OID description from MIB ELTEX-SMG

Table J2 – Common information and sensors

Name	OID	Inquiry	Description
smg	1.3.6.1.4.1.35265.1.29	Get {}	Root object for OID tree
smgDevName	1.3.6.1.4.1.35265.1.29.1	Get {}	Device's name
smgDevType	1.3.6.1.4.1.35265.1.29.2	Get {}	Type of the device (always 29)
smgFwVersion	1.3.6.1.4.1.35265.1.29.3	Get {}	Firmware version
smgEth0	1.3.6.1.4.1.35265.1.29.4	Get {}	IP address of primary interface
smgUptime	1.3.6.1.4.1.35265.1.29.5	Get {}	Firmware operating time
smgUpdateFw	1.3.6.1.4.1.35265.1.29.25	Set {} S	Firmware updating. Send a Set inquiry with parameters (separate with spaces): <ul style="list-style-type: none"> name of firmware without spaces; TFTP server's address
smgReboot	1.3.6.1.4.1.35265.1.29.27	Set {} 1	Reboot of the device
smgSave	1.3.6.1.4.1.35265.1.29.29	Set {} 1	Configuration saving
smgFreeSpace	1.3.6.1.4.1.35265.1.29.32	Get {}	Free space on embedded flash memory
smgFreeRam	1.3.6.1.4.1.35265.1.29.33	Get {}	The value of free RAM
smgMonitoring	1.3.6.1.4.1.35265.1.29.35	Get {}	Display temperature sensors and fan rate, root object
smgTemperature 1	1.3.6.1.4.1.35265.1.29.35.1	Get {}	Temperature sensor 1
smgTemperature 2	1.3.6.1.4.1.35265.1.29.35.2	Get {}	Temperature sensor 2
smgFan0	1.3.6.1.4.1.35265.1.29.35.3	Get {}	Fan speed sensor 1
smgFan1	1.3.6.1.4.1.35265.1.29.35.4	Get {}	Fan speed sensor 2
smgFan2	1.3.6.1.4.1.35265.1.29.35.5	Get {}	Fan speed sensor 3
smgFan3	1.3.6.1.4.1.35265.1.29.35.6	Get {}	Fan speed sensor 4
smgPowerModule Table	1.3.6.1.4.1.35265.1.29.36	Get {}	Information on power supply state, root object. Number of

			power unit is specified for subordinate objects: 0 or 1.
smgPowerModuleEntry	1.3.6.1.4.1.35265.1.29.36.1	Get {}	see smgPowerModuleTable
pmExist	1.3.6.1.4.1.35265.1.29.36.1.2.x	Get {}.x	Power unit <ul style="list-style-type: none"> • 1 – installed • 2 – not installed
pmPower	1.3.6.1.4.1.35265.1.29.36.1.3.x	Get {}.x	Power units are <ul style="list-style-type: none"> • 1 – supplied with electric energy • 2 – not supplied with electric energy
pmType	1.3.6.1.4.1.35265.1.29.36.1.4.x	Get {}.x	Type of installed power unit <ul style="list-style-type: none"> • 1 – PM48/12 • 2 – PM220/12 • 3 – PM220/12V • 4 – PM150-220/12
smgCpuLoadTable	1.3.6.1.4.1.35265.1.29.37	Get {}	CPU load, root object. Shows CPU load in per cents for different types of tasks. The number of processor is specified for subordinate objects. SMG1016M - 1 SMG2016 - 1..4
smgCpuLoadEntry	1.3.6.1.4.1.35265.1.29.37.1	Get {}	see smgCpuLoadTable
cpuUsr	1.3.6.1.4.1.35265.1.29.37.1.2.x	Get {}.x	% CPU, user applications
cpuSys	1.3.6.1.4.1.35265.1.29.37.1.3.x	Get {}.x	% CPU, core applications
cpuNic	1.3.6.1.4.1.35265.1.29.37.1.4.x	Get {}.x	% CPU, applications with changed priority
cpuidle	1.3.6.1.4.1.35265.1.29.37.1.5.x	Get {}.x	% CPU, Idle
cpulo	1.3.6.1.4.1.35265.1.29.37.1.6.x	Get {}.x	% CPU, input-output operations
cpulrq	1.3.6.1.4.1.35265.1.29.37.1.7.x	Get {}.x	% CPU, hardware interrupts processing
cpuSirq	1.3.6.1.4.1.35265.1.29.37.1.8.x	Get {}.x	% CPU, software interrupts processing
cpuUsage	1.3.6.1.4.1.35265.1.29.37.1.9.x	Get {}.x	% CPU, common usage
smgSubscribersInfo	1.3.6.1.4.1.35265.1.29.42	Get {}	General information on active calls and registration quantity
activeCallCount	1.3.6.1.4.1.35265.1.29.42.1	Get {}	Current number of active calls
registrationCount	1.3.6.1.4.1.35265.1.29.42.2	Get {}	Current number of registrations

Table J3 – Syslog settings

Name	OID	Inquiry	Description
smgSyslog	1.3.6.1.4.1.35265.1.29.34	Get {}	Syslog settings, root object
smgSyslogTraces	1.3.6.1.4.1.35265.1.29.34.1	Get {}	Trace settings in syslog, root object
smgSyslogTracesAddress	1.3.6.1.4.1.35265.1.29.34.1.1	Get {} Set {} S	IP address of syslog server for trace receiving
smgSyslogTracesPort	1.3.6.1.4.1.35265.1.29.34.1.2	Get {} Set {} N	Syslog server port for trace receiving
smgSyslogTracesAlarms	1.3.6.1.4.1.35265.1.29.34.1.3	Get {} Set {} N	Alarm trace level: <ul style="list-style-type: none"> • 1-99 – enable trace; • 0 – disable trace.
smgSyslogTracesCalls	1.3.6.1.4.1.35265.1.29.34.1.4	Get {} Set {} N	Calls trace level: <ul style="list-style-type: none"> • 1-99 – enable trace; • 0 – disable trace.
smgSyslogTracesISUP	1.3.6.1.4.1.35265.1.29.34.1.5	Get {} Set {} N	SS7/ISUP trace level: <ul style="list-style-type: none"> • 1-99 – enable trace; • 0 – disable trace.
smgSyslogTracesSIPT	1.3.6.1.4.1.35265.1.29.34.1.6	Get {} Set {} N	SIPT trace level: <ul style="list-style-type: none"> • 1-99 – enable trace; • 0 – disable trace.
smgSyslogTracesQ931	1.3.6.1.4.1.35265.1.29.34.1.7	Get {} Set {} N	Q.931 trace level: <ul style="list-style-type: none"> • 1-99 – enable trace; • 0 – disable trace.
smgSyslogTracesRTP	1.3.6.1.4.1.35265.1.29.34.1.8	Get {} Set {} N	RTP trace level: <ul style="list-style-type: none"> • 1-99 – enable trace; • 0 – disable trace.
smgSyslogTracesMSP	1.3.6.1.4.1.35265.1.29.34.1.9	Get {} Set {} N	Voice submodule commands trace level: <ul style="list-style-type: none"> • 1-99 – enable trace; • 0 – disable trace.
smgSyslogTracesRadius	1.3.6.1.4.1.35265.1.29.34.1.10	Get {} Set {} N	RADIUS trace level: <ul style="list-style-type: none"> • 1-99 – enable trace; • 0 – disable trace.
smgSyslogTracesRowStatus	1.3.6.1.4.1.35265.1.29.34.1.11	Get {} Set {} i 1	Apply trace configuration changes
smgSyslogHistory	1.3.6.1.4.1.35265.1.29.34.2	Get {}	Settings of command logging in syslog, root object
smgSyslogHistoryAddress	1.3.6.1.4.1.35265.1.29.34.2.1	Get {} Set {} S	IP address of syslog server for command history receiving
smgSyslogHistoryPort	1.3.6.1.4.1.35265.1.29.34.2.2	Get {} Set {} N	Port of syslog server for command history receiving
smgSyslogHistoryLevel	1.3.6.1.4.1.35265.1.29.34.2.3	Get {} Set {} N	Level of log detalization: <ul style="list-style-type: none"> • 0 – disable logging; • 1 – standard; • 2 – full
smgSyslogHistoryRowStatus	1.3.6.1.4.1.35265.1.29.34.2.4	Get {} Set {} i 1	Apply changes in command history logging

smgSyslogConfig	1.3.6.1.4.1.35265.1.29.34.3	Get {}	Syslog settings
smgSyslogConfigLogsEnabled	1.3.6.1.4.1.35265.1.29.34.3.1	Get {} Set {} N	Enable logging <ul style="list-style-type: none"> • 1 – enable; • 2 – disable
smgSyslogConfigSendToServer	1.3.6.1.4.1.35265.1.29.34.3.2	Get {} Set {} N	Send messages to syslog server: <ul style="list-style-type: none"> • 1 – enable; • 2 – disable
smgSyslogConfigAddress	1.3.6.1.4.1.35265.1.29.34.3.3	Get {} Set {} S	IP address of syslog server
smgSyslogConfigPort	1.3.6.1.4.1.35265.1.29.34.3.4	Get {} Set {} N	Port of syslog server
smgSyslogConfigRowStatus	1.3.6.1.4.1.35265.1.29.34.3.5	Get {} Set {} i 1	Apply changes in syslog settings

Table J4 –E1 streams monitoring

Name	OID	Inquiry	Description
smgEOneTable	1.3.6.1.4.1.35265.1.29.7	Get {}	Table which shows physical state of E1 streams.
eOneLineInfoPhyState	1.3.6.1.4.1.35265.1.29.7.1.2 1.3.6.1.4.1.35265.1.29.7.1.2.x	Get {} Get {}.x	Physical state of E1 stream. Complete OID with a number of certain stream (0..15) in order to obtain information on the stream. State of a stream: 0 – stream is disabled; 1 – ALARM; 2 – LOS; 3 – AIS; 4 – LOM; 5 – LOMF; 6 – stream is in operation; 7 – the PRBS test has been launched on the stream
eOneLineInfoRemAlarm	1.3.6.1.4.1.35265.1.29.7.1.3 1.3.6.1.4.1.35265.1.29.7.1.3.x	Get {} Get {}.x	Presence of RAI signal on the stream – error on the remote side. Add a stream number (0..15) to OID for obtaining information on its status. <ul style="list-style-type: none"> • 0 – normal state; • 1 – RAI signal received
eOneLineInfoRemAlarmT S16	1.3.6.1.4.1.35265.1.29.7.1.4 1.3.6.1.4.1.35265.1.29.7.1.4.x	Get {} Get {}.x	Presence of RAI16 signal on the stream means an error on the remote side over a 16-channel interval. Add a stream number (0..15) to OID for obtaining information on its status. <ul style="list-style-type: none"> • 0 – normal state; • 1 – RAI16 signal received
eOneLineStateAlarm	1.3.6.1.4.1.35265.1.29.7.1.5 1.3.6.1.4.1.35265.1.29.7.1.5.x	Get {} Get {}.x	Alarms status on the stream. Add a stream number (0..15) to OID for obtaining information on its status. <ul style="list-style-type: none"> • 0 – no alarms or stream is disabled; • 1 – critical alarm, the stream is out of work; • 2 – alarm, errors occurred; • 3 – code is not used; • 4 – alarm, RAI error
eOneLineStatePhyWork	1.3.6.1.4.1.35265.1.29.7.1.6 1.3.6.1.4.1.35265.1.29.7.1.6.x	Get {} Get {}.x	Physical link state on the stream (signal reception). Add a stream number (0..15) to OID for obtaining information on its status.

			<ul style="list-style-type: none"> • 0 – no link; • 1 – link
eOneLinkState	1.3.6.1.4.1.35265.1.29.7.1.7 1.3.6.1.4.1.35265.1.29.7.1.7.x	Get {} Get {}.x	D-channel status. Add a stream number (0..15) to OID for obtaining information on a particular stream state: <ul style="list-style-type: none"> • 0 – does not work/ off/ • both KPDs do not work • 1 – work / both KPDs work • 4 – KPD1 does not work • 8 – KPD2 does not work
eOneStatistTimer	1.3.6.1.4.1.35265.1.29.7.1.9 1.3.6.1.4.1.35265.1.29.7.1.9.x	Get {} Get {}.x	Time of statistics gathering, in seconds. Add a stream number (0..15) to OID for obtaining information on its status
eOneSlipUp	1.3.6.1.4.1.35265.1.29.7.1.10 1.3.6.1.4.1.35265.1.29.7.1.10. x	Get {} Get {}.x	Frame slip (frame repeat). Add a stream number (0..15) to OID for obtaining information on its status
eOneSlipDown	1.3.6.1.4.1.35265.1.29.7.1.11 1.3.6.1.4.1.35265.1.29.7.1.11. x	Get {} Get {}.x	Frame slip (frame loss). Add a stream number (0..15) to OID for obtaining information on its status
eOneBERCount	1.3.6.1.4.1.35265.1.29.7.1.12 1.3.6.1.4.1.35265.1.29.7.1.12. x	Get {} Get {}.x	Bit errors. Add a stream number (0..15) to OID for obtaining information on its status
eOneCVC	1.3.6.1.4.1.35265.1.29.7.1.13 1.3.6.1.4.1.35265.1.29.7.1.13. x	Get {} Get {}.x	Code Violation Counter. Add a stream number (0..15) to OID for obtaining information on its status
eOneCEC	1.3.6.1.4.1.35265.1.29.7.1.14 1.3.6.1.4.1.35265.1.29.7.1.14. x	Get {} Get {}.x	CRC/PRBS Errors Counter. Add a stream number (0..15) to OID for obtaining information on its status
eOneRxCount	1.3.6.1.4.1.35265.1.29.7.1.16 1.3.6.1.4.1.35265.1.29.7.1.16. x	Get {} Get {}.x	A byte has been received. Add a stream number (0..15) to OID for obtaining information on its status
eOneTxCount	1.3.6.1.4.1.35265.1.29.7.1.17 1.3.6.1.4.1.35265.1.29.7.1.17. x	Get {} Get {}.x	A byte has been transmitted. Add a stream number (0..15) to OID for obtaining information on its status
eOneRxLow	1.3.6.1.4.1.35265.1.29.7.1.18 1.3.6.1.4.1.35265.1.29.7.1.18. x	Get {} Get {}.x	Short data packets have been received. Add a stream number (0..15) to OID for obtaining information on its status
eOneRxBig	1.3.6.1.4.1.35265.1.29.7.1.19 1.3.6.1.4.1.35265.1.29.7.1.19. x	Get {} Get {}.x	Big data packets have been received. Add a stream number (0..15) to OID for obtaining information on its status
eOneRxOvfl	1.3.6.1.4.1.35265.1.29.7.1.20 1.3.6.1.4.1.35265.1.29.7.1.20. x	Get {} Get {}.x	Overload of receiving. Add a stream number (0..15) to OID for

			obtaining information on its status
eOneRxCRC	1.3.6.1.4.1.35265.1.29.7.1.21	Get {} Get {}.x	CRC errors. Add a stream number (0..15) to OID for obtaining information on its status
eOneTxUrun	1.3.6.1.4.1.35265.1.29.7.1.22	Get {} Get {}.x	Transmission failure. Add a stream number (0..15) to OID for obtaining information on its status
eOneName	1.3.6.1.4.1.35265.1.29.7.1.23	Get {} Get {}.x	Display information about the name of the E1 stream
smgEOneChannelTable	1.3.6.1.4.1.35265.1.29.13	Get {}	Table of E1 channels states, root object
smgEOneChannelEntry	1.3.6.1.4.1.35265.1.29.13.1	Get {}	see smgEOneChannelTable
channelEOneState	1.3.6.1.4.1.35265.1.29.13.1.2 1.3.6.1.4.1.35265.1.29.13.1.2.x 1.3.6.1.4.1.35265.1.29.13.1.2.x.x	Get {} Get {}.x Get {}.x.x	E1 channel state. Add a stream number (0..15) to OID for obtaining information on its status. Add a stream number (0..15) and channel number (0..31) to OID for obtaining information on its status
smgEOneBusyChannelsCounters	1.3.6.1.4.1.35265.1.29.31	Get {}	Quantity of busy E1 channels, root object
smgEOneInstantCounters	1.3.6.1.4.1.35265.1.29.31.1	Get {}	see smgEOneBusyChannelsCounters
smgEOneStream0BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.0	Get {}	Quantity of busy 0 E1 channels
smgEOneStream1BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.1	Get {}	Quantity of busy 1 E1 channels
smgEOneStream2BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.2	Get {}	Quantity of busy 2 E1 channels
smgEOneStream3BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.3	Get {}	Quantity of busy 3 E1 channels
smgEOneStream4BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.4	Get {}	Quantity of busy 4 E1 channels
smgEOneStream5BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.5	Get {}	Quantity of busy 5 E1 channels
smgEOneStream6BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.6	Get {}	Quantity of busy 6 E1 channels
smgEOneStream7BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.7	Get {}	Quantity of busy 7 E1 channels
smgEOneStream8BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.8	Get {}	Quantity of busy 8 E1 channels
smgEOneStream9BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.9	Get {}	Quantity of busy 9 E1 channels
smgEOneStream10BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.10	Get {}	Quantity of busy 10 E1 channels
smgEOneStream11BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.11	Get {}	Quantity of busy 11 E1 channels
smgEOneStream12BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.12	Get {}	Quantity of busy 12 E1 channels

smgEOneStream13BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.13	Get {}	Quantity of busy 13 E1 channels
smgEOneStream14BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.14	Get {}	Quantity of busy 14 E1 channels
smgEOneStream15BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.15	Get {}	Quantity of busy 15 E1 channels
smgEOnePeriodicCounter s	1.3.6.1.4.1.35265.1.29.31.2	Get {}	Quantity of busy E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream0BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.0	Get {}	Quantity of busy 0 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream1BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.1	Get {}	Quantity of busy 1 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream2BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.2	Get {}	Quantity of busy 2 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream3BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.3	Get {}	Quantity of busy 3 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream4BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.4	Get {}	Quantity of busy 4 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream5BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.5	Get {}	Quantity of busy 5 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream6BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.6	Get {}	Quantity of busy 6 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream7BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.7	Get {}	Quantity of busy 7 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream8BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.8	Get {}	Quantity of busy 8 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream9BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.9	Get {}	Quantity of busy 9 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream10BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.10	Get {}	Quantity of busy 10 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream11BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.11	Get {}	Quantity of busy 11 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream12BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.12	Get {}	Quantity of busy 12 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream13BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.13	Get {}	Quantity of busy 13 E1 channels in specified period (see smgEOneCounterPeriod)

smgEOneStream14BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.14	Get {}	Quantity of busy 14 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream15BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.15	Get {}	Quantity of busy 15 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneCounterPeriod	1.3.6.1.4.1.35265.1.29.31.2.16	Get {} Set {} N	Frequency (period) of statistics collection, in minutes. Statistics will accumulate in periodic counters, while the counter will display the value for the previous period
smgChannelsE1free	1.3.6.1.4.1.35265.1.29.41	Get {}	Quantity of free E1 channels, root object
e1freeS0channels	1.3.6.1.4.1.35265.1.29.41.1	Get {}	Quantity of free 0 E1 channels
e1freeS1channels	1.3.6.1.4.1.35265.1.29.41.2	Get {}	Quantity of free 1 E1 channels
e1freeS2channels	1.3.6.1.4.1.35265.1.29.41.3	Get {}	Quantity of free 2 E1 channels
e1freeS3channels	1.3.6.1.4.1.35265.1.29.41.4	Get {}	Quantity of free 3 E1 channels
e1freeS4channels	1.3.6.1.4.1.35265.1.29.41.5	Get {}	Quantity of free 4 E1 channels
e1freeS5channels	1.3.6.1.4.1.35265.1.29.41.6	Get {}	Quantity of free 5 E1 channels
e1freeS6channels	1.3.6.1.4.1.35265.1.29.41.7	Get {}	Quantity of free 6 E1 channels
e1freeS7channels	1.3.6.1.4.1.35265.1.29.41.8	Get {}	Quantity of free 7 E1 channels
e1freeS8channels	1.3.6.1.4.1.35265.1.29.41.9	Get {}	Quantity of free 8 E1 channels
e1freeS9channels	1.3.6.1.4.1.35265.1.29.41.10	Get {}	Quantity of free 9 E1 channels
e1freeS10channels	1.3.6.1.4.1.35265.1.29.41.11	Get {}	Quantity of free 10 E1 channels
e1freeS11channels	1.3.6.1.4.1.35265.1.29.41.12	Get {}	Quantity of free 11 E1 channels
e1freeS12channels	1.3.6.1.4.1.35265.1.29.41.13	Get {}	Quantity of free 12 E1 channels
e1freeS13channels	1.3.6.1.4.1.35265.1.29.41.14	Get {}	Quantity of free 13 E1 channels
e1freeS14channels	1.3.6.1.4.1.35265.1.29.41.15	Get {}	Quantity of free 14 E1 channels
e1freeS15channels	1.3.6.1.4.1.35265.1.29.41.16	Get {}	Quantity of free 15 E1 channels

Table J5 – SS7 Linkset monitoring

Name	OID	Inquiry	Description
smgLinkSetTable	1.3.6.1.4.1.35265.1.29.11	Get {}	SS7 Linkset states, root object
linkSetEntry	1.3.6.1.4.1.35265.1.29.11.1	Get {}	see smgLinkSetTable
linkSetState	1.3.6.1.4.1.35265.1.29.11.1.2	Get {} Get {}.x	SS7 Linkset states. Add Linkset's index (0..15) to OID for obtaining information on its status
linkSetName	1.3.6.1.4.1.35265.1.29.11.1.3	Get {} Get {}.x	The name of the SS7 linksets. To get the name of a specific linkset, supplement the OID with its index (0..3)

Table J6 – SM-VP submodules monitoring (VoIP submodules)

Name	OID	Inquiry	Description
smgMspTable	1.3.6.1.4.1.35265.1.29.9	Get {}	Statistics of the status of the VoIP submodules, root object.
mspEntry	1.3.6.1.4.1.35265.1.29.9.1	Get {}	see smgMspTable.
mspState	1.3.6.1.4.1.35265.1.29.9.1.2 1.3.6.1.4.1.35265.1.29.9.1.2.x	Get {} Get {}.x	Operation mode of VoIP submodule. Add submodule's number (0..5) to OID for obtaining information on its status
mspUsedConn	1.3.6.1.4.1.35265.1.29.9.1.3 1.3.6.1.4.1.35265.1.29.9.1.3.x	Get {} Get {}.x	Quantity of used submodule's channels. Add submodule's number (0..5) to OID for obtaining information on its status
mspCreateReq	1.3.6.1.4.1.35265.1.29.9.1.4 1.3.6.1.4.1.35265.1.29.9.1.4.x	Get {} Get {}.x	Cumulative counter of inquiries to the module for link creation. Add submodule's number (0..5) to OID for obtaining information on its status
mspCreated	1.3.6.1.4.1.35265.1.29.9.1.5 1.3.6.1.4.1.35265.1.29.9.1.5.x	Get {} Get {}.x	Cumulative counters of executed inquiries to the module for link creation. Add submodule's number (0..5) to OID for obtaining information on its status
mspDestroyReq	1.3.6.1.4.1.35265.1.29.9.1.6 1.3.6.1.4.1.35265.1.29.9.1.6.x	Get {} Get {}.x	Cumulative counters of inquiries to the module for link removing. Add submodule's number (0..5) to OID for obtaining information on its status
mspDestroyed	1.3.6.1.4.1.35265.1.29.9.1.7 1.3.6.1.4.1.35265.1.29.9.1.7.x	Get {} Get {}.x	Cumulative counters of executed inquiries to the module for link removing. Add submodule's number (0..5) to OID for obtaining information on its status
mspPayload	1.3.6.1.4.1.35265.1.29.9.1.8 1.3.6.1.4.1.35265.1.29.9.1.8.x	Get {} Get {}.x	Load of submodules measured in % of total channels number. Add submodule's number (0..5) to OID for obtaining information on its status
smgIpMspChannelTable	1.3.6.1.4.1.35265.1.29.15	Get {}	Statistics of active channels state of VoIP submodules, root object
smgMspIpChannelEntry	1.3.6.1.4.1.35265.1.29.15.1	Get {}	see smgIpMspChannelTable
ipMspChannelState	1.3.6.1.4.1.35265.1.29.15.1.2 1.3.6.1.4.1.35265.1.29.15.1.2.x 1.3.6.1.4.1.35265.1.29.15.1.2.x.x	Get {} Get {}.x Get {}.x.x	Active channels' state. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for

			<p>obtaining information on the channel's status.</p> <ul style="list-style-type: none"> • 0 – free; • 1 – channel allocation; • 2 – inquiry for channel allocation; • 3 – inquiry for channel allocation has been processed; • 4 – inquiry for channel discharging; • 5 – inquiry for channel discharging has been processed; • 6 – inquiry for channel disabling; • 7 – inquiry for channel activating; • 8 – in operation; • 9 – activated; • 10 – inquiry for connection to a conference; • 11 – conference is active
ipMspChannelSiptCallref	<p>1.3.6.1.4.1.35265.1.29.15.1.3 1.3.6.1.4.1.35265.1.29.15.1.3.x 1.3.6.1.4.1.35265.1.29.15.1.3.x.x</p>	<p>Get {} Get {}.x Get {}.x.x</p>	<p>Local call identifier, which connected to an active channel. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status</p>
ipMspChannelSrcIp	<p>1.3.6.1.4.1.35265.1.29.15.1.4 1.3.6.1.4.1.35265.1.29.15.1.4.x 1.3.6.1.4.1.35265.1.29.15.1.4.x.x</p>	<p>Get {} Get {}.x Get {}.x.x</p>	<p>Local IP address of a media stream. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status</p>
ipMspChannelSrcPort	<p>1.3.6.1.4.1.35265.1.29.15.1.5 1.3.6.1.4.1.35265.1.29.15.1.5.x 1.3.6.1.4.1.35265.1.29.15.1.5.x.x</p>	<p>Get {} Get {}.x Get {}.x.x</p>	<p>Local port of a media stream. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status</p>
ipMspChannelSrcMac	<p>1.3.6.1.4.1.35265.1.29.15.1.6 1.3.6.1.4.1.35265.1.29.15.1.6.x 1.3.6.1.4.1.35265.1.29.15.1.6.x.x</p>	<p>Get {} Get {}.x Get {}.x.x</p>	<p>Local MAC address of a media stream. Add submodule's number (0..5) to OID for</p>

			obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status
ipMspChannelDstIp	1.3.6.1.4.1.35265.1.29.15.1.7 1.3.6.1.4.1.35265.1.29.15.1.7.x 1.3.6.1.4.1.35265.1.29.15.1.7.x.x	Get {} Get {}.x Get {}.x.x	Remote IP address of a media stream. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status
ipMspChannelDstPort	1.3.6.1.4.1.35265.1.29.15.1.8 1.3.6.1.4.1.35265.1.29.15.1.8.x 1.3.6.1.4.1.35265.1.29.15.1.8.x.x	Get {} Get {}.x Get {}.x.x	Remote port of a media stream. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status
ipMspChannelDstMac	1.3.6.1.4.1.35265.1.29.15.1.9 1.3.6.1.4.1.35265.1.29.15.1.9.x 1.3.6.1.4.1.35265.1.29.15.1.9.x.x	Get {} Get {}.x Get {}.x.x	Remote MAC address of a media stream. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status
ipMspChannelCallingPartyNumber	1.3.6.1.4.1.35265.1.29.15.1.10 1.3.6.1.4.1.35265.1.29.15.1.10.x 1.3.6.1.4.1.35265.1.29.15.1.10.x.x	Get {} Get {}.x Get {}.x.x	Number of a caller. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status
ipMspChannelCalledPartyNumber	1.3.6.1.4.1.35265.1.29.15.1.11 1.3.6.1.4.1.35265.1.29.15.1.11.x 1.3.6.1.4.1.35265.1.29.15.1.11.x.x	Get {} Get {}.x Get {}.x.x	Number of a callee. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for obtaining information on the channel's status
ipMspChannelOccupiedTime	1.3.6.1.4.1.35265.1.29.15.1.12 1.3.6.1.4.1.35265.1.29.15.1.12.x 1.3.6.1.4.1.35265.1.29.15.1.12.x.x	Get {} Get {}.x Get {}.x.x	Call duration. Add submodule's number (0..5) to OID for obtaining information on its status. Add submodule's number (0..5) and channel's number (0..127) to OID for

			obtaining information on the channel's status
smgChannelsVoip	1.3.6.1.4.1.35265.1.29.40	Get {}	Quantity of busy channels on VoIP submodules, root object
voip0busyChannels	1.3.6.1.4.1.35265.1.29.40.1	Get {}	Quantity of busy channels on 0 VoIP submodule
voip1busyChannels	1.3.6.1.4.1.35265.1.29.40.2	Get {}	Quantity of busy channels on 1 VoIP submodule
voip2busyChannels	1.3.6.1.4.1.35265.1.29.40.3	Get {}	Quantity of busy channels on 2 VoIP submodule
voip3busyChannels	1.3.6.1.4.1.35265.1.29.40.4	Get {}	Quantity of busy channels on 3 VoIP submodule
voip4busyChannels	1.3.6.1.4.1.35265.1.29.40.5	Get {}	Quantity of busy channels on 4 VoIP submodule
voip5busyChannels	1.3.6.1.4.1.35265.1.29.40.6	Get {}	Quantity of busy channels on 5 VoIP submodule
voip0freeChannels	1.3.6.1.4.1.35265.1.29.40.7	Get {}	Quantity of free channels on 0 VoIP submodule
voip1freeChannels	1.3.6.1.4.1.35265.1.29.40.8	Get {}	Quantity of free channels on 1 VoIP submodule
voip2freeChannels	1.3.6.1.4.1.35265.1.29.40.9	Get {}	Quantity of free channels on 2 VoIP submodule
voip3freeChannels	1.3.6.1.4.1.35265.1.29.40.10	Get {}	Quantity of free channels on 3 VoIP submodule.
voip4freeChannels	1.3.6.1.4.1.35265.1.29.40.11	Get {}	Quantity of free channels on 4 VoIP submodule
voip5freeChannels	1.3.6.1.4.1.35265.1.29.40.12	Get {}	Quantity of free channels on 5 VoIP submodule

Table J7 – SIP interfaces monitoring

Name	OID	Inquiry	Description
smgSipIntrfCallInfo	1.3.6.1.4.1.35265.1.29.43	Get {}	Information on calls on SIP interfaces, root object
sipIntrfCount	1.3.6.1.4.1.35265.1.29.43.1	Get {}	Quantity of SIP interfaces
sipIntrfActiveCallTable	1.3.6.1.4.1.35265.1.29.43.2	Get {}	Call table. (table will not be displayed if there is not any SIP interfaces)
sipIntrfActiveCallTableEntry	1.3.6.1.4.1.35265.1.29.43.2.1	Get {}	see 1.3.6.1.4.1.35265.1.29.43.2
sipIntrfID	1.3.6.1.4.1.35265.1.29.43.2.1.2 1.3.6.1.4.1.35265.1.29.43.2.1.2.x	Get {} Get {}.x	ID of a SIP interface. Add interface index to OID for obtaining information on its status.
sipIntrfName	1.3.6.1.4.1.35265.1.29.43.2.1.3 1.3.6.1.4.1.35265.1.29.43.2.1.3.x	Get {} Get {}.x	SIP interface name. Add interface index to OID for obtaining information on its status.
sipIntrfMode	1.3.6.1.4.1.35265.1.29.43.2.1.4 1.3.6.1.4.1.35265.1.29.43.2.1.4.x	Get {} Get {}.x	Operation mode. Add interface index to OID for obtaining information on its status. 0 – SIP; 1 – SIP-T;

			2 – SIP-I; 3 – SIP-Q; 4 – SIP-profile
sipIntrfCallCount	1.3.6.1.4.1.35265.1.29.43.2.1.5 1.3.6.1.4.1.35265.1.29.43.2.1.5.x	Get {} Get {}.x	Quantity of active calls on the interface. Add interface index to OID for obtaining information on its status
sipIntrfMaxCallCount	1.3.6.1.4.1.35265.1.29.43.2.1.6 1.3.6.1.4.1.35265.1.29.43.2.1.6.x	Get {} Get {}.x	Maximum quantity of calls on the interface. Add interface index to OID for obtaining information on its status. 0 – no limit; 1..65535 – limit of calls

Table J8 — Statistics of Radius requests

Name	OID	Request	Description
radiusTotal	1.3.6.1.4.1.35265.1.29.47.1	Get {}	General requests statistics
radiusTotalSent	1.3.6.1.4.1.35265.1.29.47.2	Get {}	Sent requests statistics
radiusAccsReq	1.3.6.1.4.1.35265.1.29.47.3	Get {}	General Statistics of Access Requests
radiusAccsReqSent	1.3.6.1.4.1.35265.1.29.47.4	Get {}	Statistics of sent Access Requests
radiusAccsRsp	1.3.6.1.4.1.35265.1.29.47.5	Get {}	General Statistics of Access Responses
radiusAccsAccept	1.3.6.1.4.1.35265.1.29.47.6	Get {}	Statistics of Access Accepts
radiusAccsReject	1.3.6.1.4.1.35265.1.29.47.7	Get {}	Statistics of Access Rejects
radiusAcctReq	1.3.6.1.4.1.35265.1.29.47.8	Get {}	General Statistics of Accounting Requests
radiusAcctReqSent	1.3.6.1.4.1.35265.1.29.47.9	Get {}	Statistics of sent Accounting Requests
radiusAcctRsp	1.3.6.1.4.1.35265.1.29.47.10	Get {}	General Statistics of Accounting Responses
radiusAcctRspSuccess	1.3.6.1.4.1.35265.1.29.47.11	Get {}	Statistics of Accounting Responses Success
radiusDiscReq	1.3.6.1.4.1.35265.1.29.47.12	Get {}	General Statistics of Disconnect Requests
radiusDiscReqSent	1.3.6.1.4.1.35265.1.29.47.13	Get {}	Statistics of sent Disconnect Requests
radiusRspTimeout	1.3.6.1.4.1.35265.1.29.47.14	Get {}	Timeouts while waiting for responses from the RADIUS server
radiusTimeoutExhst	1.3.6.1.4.1.35265.1.29.47.15	Get {}	Retransmission end timeout
radiusProcTimeout	1.3.6.1.4.1.35265.1.29.47.16	Get {}	Timeouts while processing the response. Usually it is '0'
radiusTimeThreshold	1.3.6.1.4.1.35265.1.29.47.17	Get {} Set {}	Getting / setting the time threshold for the received statistics. 0 – statistics for all time, 5 – for the last 5 minutes, 60 – for the last 60 minutes
radiusClearStat	1.3.6.1.4.1.35265.1.29.47.18	Set {}	Clear statistics: 0 – clear permanent statistics

Table J9 — Information about the network interfaces

Name	OID	Requests	Description
iftType	1.3.6.1.4.1.35265.1.29.19.1.2 1.3.6.1.4.1.35265.1.29.19.1.2.x	Get {} Get {}.x	Network interface type. To obtain information about the type of a particular interface, supplement the OID with its number
iftLabel	1.3.6.1.4.1.35265.1.29.19.1.3	Get {} Get {}.x	The name of the network interface. To get information about the name of a specific interface, supplement the OID with its number
iftIaddr	1.3.6.1.4.1.35265.1.29.19.1.4	Get {} Get {}.x	IP address of the network interface. To get information about the IP address of a specific interface, supplement the OID with its number
iftNetmask	1.3.6.1.4.1.35265.1.29.19.1.5	Get {} Get {}.x	Network interface mask. To get information about the mask of a particular interface, supplement the OID with its number
iftGateway	1.3.6.1.4.1.35265.1.29.19.1.6 1.3.6.1.4.1.35265.1.29.19.1.6.x	Get {} Get {}.x	Network interface gateway. To obtain information about the gateway of a particular interface, supplement the OID with its number
iftBroadcast	1.3.6.1.4.1.35265.1.29.19.1.7 1.3.6.1.4.1.35265.1.29.19.1.7.x	Get {} Get {}.x	The broadcast address of the interface. To get information about the broadcast address of a particular interface, supplement the OID with its number
iftWeb	1.3.6.1.4.1.35265.1.29.19.1.8 1.3.6.1.4.1.35265.1.29.19.1.8.x	Get {} Get {}.x	Access to the device via the web through the network interface: <ul style="list-style-type: none"> • 0 – no access; • 1 – access is available
iftSsh	1.3.6.1.4.1.35265.1.29.19.1.9 1.3.6.1.4.1.35265.1.29.19.1.9.x	Get {} Get {}.x	Access to the device via ssh through the network interface: <ul style="list-style-type: none"> • 0 – no access; • 1 – access is available

IftTelnet	1.3.6.1.4.1.35265.1.29.19.1.10 1.3.6.1.4.1.35265.1.29.19.1.10. x	Get {} Get {}.x	Access to the device via telnet through the network interface: • 0 – no access; • 1 – access is available
iftSnmp	1.3.6.1.4.1.35265.1.29.19.1.11 1.3.6.1.4.1.35265.1.29.19.1.11. x	Get {} Get {}.x	Using the SNMP protocol through the network interface: • 0 – denied; • 1 – allowed
IftRtp	1.3.6.1.4.1.35265.1.29.19.1.12 1.3.6.1.4.1.35265.1.29.19.1.12. x	Get {} Get {}.x	Ability to receive / transmit RTP traffic through the network interface: • 0 – denied; • 1 – allowed
IftRadius	1.3.6.1.4.1.35265.1.29.19.1.13 1.3.6.1.4.1.35265.1.29.19.1.13. x	Get {} Get {}.x	Using the RADIUS protocol through the network interface: • 0 – denied; • 1 – allowed
IftH323	1.3.6.1.4.1.35265.1.29.19.1.14 1.3.6.1.4.1.35265.1.29.19.1.14. x	Get {} Get {}.x	Using the H.323 protocol through the network interface: • 0 – denied; • 1 – allowed
iftDhcp	1.3.6.1.4.1.35265.1.29.19.1.16 1.3.6.1.4.1.35265.1.29.19.1.16. x	Get {} Get {}.x	Using DHCP on the network interface: • 0 – DHCP is off; • 1 – DHCP is on
iftDhcpNoGw	1.3.6.1.4.1.35265.1.29.19.1.17 1.3.6.1.4.1.35265.1.29.19.1.17. x	Get {} Get {}.x	Using the 'Obtain Gateway Automatically' option on a network interface with DHCP: • 0 – option is disabled; • 1 – option is enabled
iftDhcpDns	1.3.6.1.4.1.35265.1.29.19.1.18 1.3.6.1.4.1.35265.1.29.19.1.18. x	Get {} Get {}.x	Using the 'Obtain DNS Automatically' option on a network interface with DHCP: • 0 – option is disabled; • 1 – option is enabled
iftDhcpNtp	1.3.6.1.4.1.35265.1.29.19.1.19 1.3.6.1.4.1.35265.1.29.19.1.19. x	Get {} Get {}.x	Using the 'Obtain NTP Automatically' option on a network interface with DHCP: • 0 – option is disabled; • 1 – option is enabled
IftSip	1.3.6.1.4.1.35265.1.29.19.1.20 1.3.6.1.4.1.35265.1.29.19.1.20. x	Get {} Get {}.x	Using the SIP protocol through the network interface: • 0 – denied; • 1 – allowed

IftServerIp	1.3.6.1.4.1.35265.1.29.19.1.21 1.3.6.1.4.1.35265.1.29.19.1.21.x	Get {} Get {}.x	IP address of the PPTP server. To obtain information about the address of the PPTP server of a specific network interface, supplement the OID with its number
IftRunStup	1.3.6.1.4.1.35265.1.29.19.1.22 1.3.6.1.4.1.35265.1.29.19.1.22.x	Get {} Get {}.x	Using the 'Enable' option on the VPN/pptp interface: <ul style="list-style-type: none"> • 0 – interface is disabled; • 1 – interface is enabled
IftGwIgnore	1.3.6.1.4.1.35265.1.29.19.1.23 1.3.6.1.4.1.35265.1.29.19.1.23.x	Get {} Get {}.x	Using the 'Ignore Default Gateway' option on the VPN/pptp interface: <ul style="list-style-type: none"> • 0 – option is disabled; • 1 – option is enabled
IftUseMppe	1.3.6.1.4.1.35265.1.29.19.1.24 1.3.6.1.4.1.35265.1.29.19.1.24.x	Get {} Get {}.x	Using the 'Encryption' option on the VPN/pptp interface: <ul style="list-style-type: none"> • 0 – option is disabled; • 1 – option is enabled
IftUserIp	1.3.6.1.4.1.35265.1.29.19.1.25 1.3.6.1.4.1.35265.1.29.19.1.25.x	Get {} Get {}.x	VPN user IP address
IftVid	1.3.6.1.4.1.35265.1.29.19.1.27	Get {}	VID of the network interface.
	1.3.6.1.4.1.35265.1.29.19.1.27.x	Get {}.x	To obtain information about the VID of a specific network interface, supplement the OID with its number
IftCos	1.3.6.1.4.1.35265.1.29.19.1.28	Get {}	COS of the network interface.
	1.3.6.1.4.1.35265.1.29.19.1.28.x	Get {}.x	To obtain information about the COS of a specific network interface, supplement the OID with its number
IftFwProfile	1.3.6.1.4.1.35265.1.29.19.1.29 1.3.6.1.4.1.35265.1.29.19.1.29.x	Get {} Get {}.x	Network interface firewall profile. To obtain information about the firewall profile of a specific network interface, supplement the OID with its number

Table J10 – Monitoring of trunk groups

Name	OID	Requests	Description
trunkName	1.3.6.1.4.1.35265.1.29.46.1.1.2 1.3.6.1.4.1.35265.1.29.46.1.1.2.x	Get {} Get {}.x	Trunk group name. To obtain information about the name of a specific trunk group, supplement the OID with its number
trunkEntryType	1.3.6.1.4.1.35265.1.29.46.1.1.3 1.3.6.1.4.1.35265.1.29.46.1.1.3.x	Get {} Get {}.x	<p>Type of trunk group: 0 – CAS 1 – PRI 2 – SS7 3 – SIP 4 – E1 stream channels 5 – H323 6 –E1 streams from SS7 linkset 7 – IPNET 8 – CSPG 9 – fxo</p> <p>To obtain information about the type of a particular trunk group, supplement the OID with its number.</p>
trunkEnable	1.3.6.1.4.1.35265.1.29.46.1.1.4 1.3.6.1.4.1.35265.1.29.46.1.1.4.x	Get {} Get {}.x	<p>The status of the E1 stream, which is associated with the trunk group, is used for trunk group types CAS, PRI, SS7, E1 stream channels, E1 streams from the SS7 linkset:</p> <p>0 – stream is disabled; 1 – stream is enabled</p>
trunkCapacity	1.3.6.1.4.1.35265.1.29.46.1.1.5 1.3.6.1.4.1.35265.1.29.46.1.1.5.x	Get {} Get {}.x	<p>The total number of channels in the trunk group, used for trunk group types CAS, PRI, SS7, channels of the E1 stream, E1 streams from the SS7 linkset.</p> <p>To obtain information about the number of channels of a particular trunk group, supplement the OID with its number</p>

trunkCurrentIngressCalls	1.3.6.1.4.1.35265.1.29.46.1.1.6 1.3.6.1.4.1.35265.1.29.46.1.1.6.x	Get {} Get {}.x	The number of incoming calls in the trunk group. To obtain information about the number of channels of a particular trunk group, supplement the OID with its number
trunkCurrentEgressCalls	1.3.6.1.4.1.35265.1.29.46.1.1.7 1.3.6.1.4.1.35265.1.29.46.1.1.7.x	Get {} Get {}.x	The number of outgoing calls in the trunk group. To obtain information about the number of outgoing calls of a specific trunk group, supplement the OID with its number
trunkCurrentTotalCalls	1.3.6.1.4.1.35265.1.29.46.1.1.8 1.3.6.1.4.1.35265.1.29.46.1.1.8.x	Get {} Get {}.x	The total number of calls in the trunk group. To obtain information about the number of calls to a specific trunk group, supplement the OID with its number
trunkCurrentCps	1.3.6.1.4.1.35265.1.29.46.1.1.9 1.3.6.1.4.1.35265.1.29.46.1.1.9.x	Get {} Get {}.x	Current cps in the trunk group. To obtain information about the cps of a specific trunk group, supplement the OID with its number
trunkStatus	1.3.6.1.4.1.35265.1.29.46.1.1.10 1.3.6.1.4.1.35265.1.29.46.1.1.10.x	Get {} Get {}.x	Trunk group status. For trunk groups containing E1 streams: 0 – stream is not in operation 1 – stream is in operation; 2 – no D-channel. For trunk groups that include SIP interfaces: 0 – interface is not available; 1 – interface is in operation; 2 – interface status is unknown (options control disabled). To obtain information about the status of a specific trunk group, supplement the OID with its number

trunkUnavailableCicCount	1.3.6.1.4.1.35265.1.29.46.1.1.11 1.3.6.1.4.1.35265.1.29.46.1.1.11.x	Get {} Get {}.x	The number of non-working channels (blocked / unavailable/disabled), used for trunk group types CAS, PRI, SS7, E1 stream channels, E1 streams from SS7 linkset
			To obtain information about the number of non-working channels of a specific trunk group, supplement the OID with its number
trunkCPSMax	1.3.6.1.4.1.35265.1.29.46.1.1.12 1.3.6.1.4.1.35265.1.29.46.1.1.12.x	Get {} Get {}.x	CPS limit value in trunk group. To obtain information about the CPS limit value of a specific trunk group, supplement the OID with its number
trunkCPSAlarm	1.3.6.1.4.1.35265.1.29.46.1.1.13 1.3.6.1.4.1.35265.1.29.46.1.1.13.x	Get {} Get {}.x	CPS alarm value in trunk group. To obtain information about the CPS alarm value of a specific trunk group, supplement the OID with its number
trunkChansFree	1.3.6.1.4.1.35265.1.29.46.1.1.14 1.3.6.1.4.1.35265.1.29.46.1.1.14.x	Get {} Get {}.x	The number of free channels in the trunk group. If the trunk group contains a SIP/H323 interface and the limit on the number of active connections is not configured, the value 65535 will be returned (without restrictions) To obtain information about the number of free channels of a specific trunk group, supplement the OID with its number

trunkChansBusyc	1.3.6.1.4.1.35265.1.29.46.1.1.15 1.3.6.1.4.1.35265.1.29.46.1.1.15.x	Get {} Get {}.x	Number of busy channels in the trunk group To obtain information about the number of busy channels of a specific trunk group, supplement the OID with its number
-----------------	--	--------------------	---

5.10.2 Monitoring and configuration of SIP subscribers (static subscribers).

The commands for SNMP utilities call are represented in description of monitoring and configuration functions as follows:

swalk script, which implements reading of values:

```
#!/bin/bash
/usr/bin/snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 "$@"
```

sset script, which implements setting of values:

```
#!/bin/bash
/usr/bin/snmpset -v2c -c private -m +ELTEX-SMG 192.0.2.1 "$@"
```

5.10.2.1 Monitoring

Monitoring of subscriber or static group of subscriber can be implemented by several means:

- 1) By index or ID of a subscriber;
- 2) By numbering plan and full subscriber's number;
- 3) By numbering plan and partial subscriber's number.

To monitor:

- 1) Clear search status;
- 2) Define search criteria (optionally);
- 3) Display the information.

5.10.2.2 Example of a search by index

```
sset staticResetCheck.0 i 1          # reset search status
sset getUserByIndex.0 i 4          # setting search by index 4
swalk tableOfUsers                 # inquiry of a table with subscriber information
```

Result:

```
ELTEX-SMG::StaticResetCheck.0 = INTEGER: 0
ELTEX-SMG::getUserByIndex.0 = INTEGER: 4
ELTEX-SMG::UserID.4 = INTEGER: 5
ELTEX-SMG::RegState.4 = INTEGER: 2
ELTEX-SMG::Numplan.4 = INTEGER: 0
ELTEX-SMG::Number.4 = STRING: 20000
ELTEX-SMG::Ip.4 = IpAddress: 192.0.2.123
ELTEX-SMG::Port.4 = Gauge32: 5063
ELTEX-SMG::Domain.4 = STRING: 192.0.2.1
ELTEX-SMG::MaxActiveLines.4 = INTEGER: 3
ELTEX-SMG::ActiveCallCount.4 = INTEGER: 0
ELTEX-SMG::RegExpires.4 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.12.4 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.13.4 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.14.4 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.15.4 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.16.4 = INTEGER: -1
```

5.10.2.3 Example of a search by numbering plan and full subscriber's number

```
sset staticResetCheck.0 i 1          # search status reset
sset getUserByNumplan.0 i 2          # set second numbering plan
sset getUserByNumber.0 s 20001      # set subscriber number
swalk tableOfUsers                 # inquiry of a table with subscriber information
```

Result:

```
ELTEX-SMG::UserID.9 = INTEGER: 10
ELTEX-SMG::RegState.9 = INTEGER: 0
ELTEX-SMG::Numplan.9 = INTEGER: 2
ELTEX-SMG::Number.9 = STRING: 20001
ELTEX-SMG::Ip.9 = IpAddress: 0.0.0.0
ELTEX-SMG::Port.9 = Gauge32: 0
ELTEX-SMG::Domain.9 = STRING: sipp.domain
ELTEX-SMG::MaxActiveLines.9 = INTEGER: 0
ELTEX-SMG::ActiveCallCount.9 = INTEGER: 0
ELTEX-SMG::RegExpires.9 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.12.9 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.13.9 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.14.9 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.15.9 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.16.9 = INTEGER: -1
```

5.10.2.4 Example of a search by numbering plan and partial subscriber's number

```
sset ttaticResetCheck.0 i 1          # search status reset
sset getUserByNumplan.0 i 0          # set zero numbering plan
sset getUserBySubNumber.0 s 400      # set part of the subscriber number
swalk tableOfUsers                   # inquiry of a table with subscriber information
```

Result:

```
ELTEX-SMG::UserID.0 = INTEGER: 1
ELTEX-SMG::UserID.1 = INTEGER: 2
ELTEX-SMG::UserID.2 = INTEGER: 3
ELTEX-SMG::RegState.0 = INTEGER: 1
ELTEX-SMG::RegState.1 = INTEGER: 1
ELTEX-SMG::RegState.2 = INTEGER: 0
ELTEX-SMG::Numplan.0 = INTEGER: 0
ELTEX-SMG::Numplan.1 = INTEGER: 0
ELTEX-SMG::Numplan.2 = INTEGER: 0
ELTEX-SMG::Number.0 = STRING: 40010
ELTEX-SMG::Number.1 = STRING: 40011
ELTEX-SMG::Number.2 = STRING: 40012
ELTEX-SMG::Ip.0 = IpAddress: 192.0.2.21
ELTEX-SMG::Ip.1 = IpAddress: 192.0.2.21
ELTEX-SMG::Ip.2 = IpAddress: 0.0.0.0
ELTEX-SMG::Port.0 = Gauge32: 23943
ELTEX-SMG::Port.1 = Gauge32: 23943
ELTEX-SMG::Port.2 = Gauge32: 0
ELTEX-SMG::Domain.0 = STRING: 192.0.2.1
ELTEX-SMG::Domain.1 = STRING: 192.0.2.1
ELTEX-SMG::Domain.2 = STRING:
ELTEX-SMG::MaxActiveLines.0 = INTEGER: -1
ELTEX-SMG::MaxActiveLines.1 = INTEGER: 4
ELTEX-SMG::MaxActiveLines.2 = INTEGER: 6
ELTEX-SMG::ActiveCallCount.0 = INTEGER: -1
ELTEX-SMG::ActiveCallCount.1 = INTEGER: 0
ELTEX-SMG::ActiveCallCount.2 = INTEGER: 0
ELTEX-SMG::RegExpires.0 = INTEGER: 118
ELTEX-SMG::RegExpires.1 = INTEGER: 91
ELTEX-SMG::RegExpires.2 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.12.0 = INTEGER: 1
ELTEX-SMG::TableOfUsersEntry.12.1 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.12.2 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.13.0 = INTEGER: 2
ELTEX-SMG::TableOfUsersEntry.13.1 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.13.2 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.14.0 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.14.1 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.14.2 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.15.0 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.15.1 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.15.2 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.16.0 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.16.1 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.16.2 = INTEGER: -1
```

5.10.2.5 View information without using a search

```
sset staticResetCheck.0 i 1      # search status reset
swalk tableOfUsers              # display all subscribers
swalk regState.3                # display subscriber registration status
                                # with index 3
swalk ip.4                      # display IP address of subscriber with index 4
swalk activeCallCount           # display quantity of active calls of all subscribers
```

5.10.2.6 Configuration

Configuration involves the following operations on subscribers:

- 1) Settings viewing;
- 2) Settings editing;
- 3) Creation of a new subscriber;
- 4) Removing.

To view the settings:

- 1) Select subscriber through the search;
- 2) Select configuration mode - view;
- 3) Display the necessary data.

To edit the settings:

- 1) Select subscriber through the search;
- 2) Select configuration mode - edit;
- 3) Define necessary settings;
- 4) Apply the settings.

To create a new subscriber:

- 1) Select configuration mode - creation;
- 2) Define necessary settings of the subscriber (at least number);
- 3) Apply the settings.

To remove a subscriber:

- 4) Select subscriber through the search;
- 5) Select configuration mode - removing;
- 6) Apply the settings.

You can cancel changes that were not applied only in 'Add new subscriber' and 'Edit a subscriber' modes.



Undo group remove is not possible. Only a complete configuration restore via WEB or CLI is available.

5.10.2.7 Example of new subscriber creating

```
sset staticResetCheck.0 i 1      # search status reset
sset staticSetMode.0 i 3        # set the 'add' mode
sset stSetNumber.0 s 71234567890 # set the subscriber number
sset staticSetApply.0 i 1      # apply the settings
sset staticSetMode.0 i 0      # set the 'none' mode
```

5.10.2.8 Example of settings viewing

```
sset staticResetCheck.0 i 1          # search status reset
sset getUserByIndex.0 i 4           # set search by index 4
sset staticSetMode.0 i 1           # set the 'show' mode
swalk tableOfStSetUser              # view the settings table or
swalk stSetAuth                     # separate registration mode or
swalk stSetAccessMode               # separate maintenance mode, etc
```

5.10.2.9 Example of settings editing

```
sset staticResetCheck.0 i 1          # search status reset
sset getUserByNumplan.0 i 0         # set zero numbering plan
sset getUserByNumber.0 s 71234567890 # set the subscriber number
sset staticSetMode.0 i 2           # set 'set' mode
sset stSetNumplan.0 i 1            # change numbering plan to the first one
sset stSetCliro.0 i 1              # activate the 'CLIRO' service
sset stSetAONtypeName.0 i 2       # set 'National' automatic calling line identification
type
sset staticSetApply.0 i 1          # apply the settings
sset staticSetMode.0 i 0           # set the 'none' mode
```

5.10.2.10 Example of subscriber removing

```
sset staticResetCheck.0 i 1          # search status reset
sset getUserByID.0 i 15             # set search by ID 15
sset staticSetMode.0 i 4           # set the 'del' mode
sset staticSetApply.0 i 1          # apply the settings
# it is not required to set the 'none' mode manually
```

Table J11 – Monitoring and configuration of SIP subscribers (static subscribers)

Name	OID	Inquiry	Description
smgSipUser	1.3.6.1.4.1.35265.1.29.38	Get {}	Static subscribers list, root object.
staticCheckStatus	1.3.6.1.4.1.35265.1.29.38.1	Get {}	Status of the search by criteria. None – without a search, display all static subscribers; Find user by index; Find user by ID; Find users by numplan; Find user by numplan and number; Find users by numplan and substring number – search by partial number and numbering plan
staticResetCheck	1.3.6.1.4.1.35265.1.29.38.2	Set {} N	Search reset. Any value sets status of search to 'None'
numActiveUsers	1.3.6.1.4.1.35265.1.29.38.3	Get {}	Quantity of active (authorized) subscribers
numAllUsers	1.3.6.1.4.1.35265.1.29.38.4	Get {}	Quantity of subscribers in the system

getUserByIndex	1.3.6.1.4.1.35265.1.29.38.5	Set {} N Set {} -1	Set subscriber's index for the search. The values in a range of [0:numAllUsers) set search in 'Find user by index' state. The '-1' value corresponds to 'None' state of the search
getUserByID	1.3.6.1.4.1.35265.1.29.38.6	Set {} N Set {} -1	Set user ID for the search. The values from 1 and further complies 'Find user by ID' mode of search. The '-1' value corresponds to 'None' state of the search
getUserByNumplan	1.3.6.1.4.1.35265.1.29.38.7	Set {} N Set {} -1	Set a dial plan for searching subscribers. Setting the value to 1, if the search status was 'Find users by numplan', 'Find user by numplan and number' or 'Find users by numplan and substring number', the '-1' value sets 'None' status. If the value is '0' or over, the priority of search mode setting is as follows: <ul style="list-style-type: none"> - If 'getUserByNumber' is defined, the 'Find user by numplan and number' mode will be activated; If 'getUserBySubNumber' is defined, the 'Find users by numplan and substring number' mode will be activated; - If 'getUserByNumber' and 'getUserBySubNumber' are not defined, the 'Find users by numplan' mode will be activated
getUserByNumber	1.3.6.1.4.1.35265.1.29.38.8	Set {} S Set {} "NULL"	Set the number to search for a subscriber in conjunction with the numplan. Number length should be from 1 to 32 digits. When the numbering plan is set, the status of search will set to 'Find user by numplan and number', otherwise the search status will not change. Set 'NULL' value to reset the number. However, if the search status was 'Find user by numplan and number' the search status will be changed to 'None'
getUserBySubNumber	1.3.6.1.4.1.35265.1.29.38.9	Set {} S Set {} "NULL"	Set a partial number to search for subscribers in conjunction with the numbering plan

			<p>Number length should be from 1 to 32 digits.</p> <p>When the numbering plan is set, the status of search will be set to 'Find users by numplan and substring number', otherwise the search status will not be changed. Set 'NULL' value to reset the number. However, if the search status was 'Find users by numplan and substring number', the search status will be changed to 'None'</p>
tableOfUsers	1.3.6.1.4.1.35265.1.29.38.10	Get {}	Static subscriber table, root object
tableOfUsersEntry	1.3.6.1.4.1.35265.1.29.38.10.1	Get {}	see TableOfUsers
userID	1.3.6.1.4.1.35265.1.29.38.10.1.2 1.3.6.1.4.1.35265.1.29.38.10.1.2.x	Get {} Get {}.x	Subscriber ID. Add subscriber index to OID to obtain information on the subscriber
userRegState	1.3.6.1.4.1.35265.1.29.38.10.1.3 1.3.6.1.4.1.35265.1.29.38.10.1.3.x	Get {} Get {}.x	State of subscriber registration. Add subscriber index to OID to obtain information on the subscriber. 0 – not registered; 1 – registered
userNumplan	1.3.6.1.4.1.35265.1.29.38.10.1.4 1.3.6.1.4.1.35265.1.29.38.10.1.4.x	Get {} Get {}.x	Subscriber numbering plan. Add subscriber index to OID to obtain information on the subscriber
userNumber	1.3.6.1.4.1.35265.1.29.38.10.1.5 1.3.6.1.4.1.35265.1.29.38.10.1.5.x	Get {} Get {}.x	Number of a subscriber. Add subscriber index to OID to obtain information on the subscriber
userIp	1.3.6.1.4.1.35265.1.29.38.10.1.6 1.3.6.1.4.1.35265.1.29.38.10.1.6.x	Get {} Get {}.x	Subscriber IP address. Add subscriber index to OID to obtain information on the subscriber. If the address is unknown, the '0.0.0.0' value will be set
userPort	1.3.6.1.4.1.35265.1.29.38.10.1.7 1.3.6.1.4.1.35265.1.29.38.10.1.7.x	Get {} Get {}.x	Subscriber port. Add subscriber index to OID to obtain information on the subscriber
userDomain	1.3.6.1.4.1.35265.1.29.38.10.1.8 1.3.6.1.4.1.35265.1.29.38.10.1.8.x	Get {} Get {}.x	Subscriber SIP domain. Add subscriber index to OID to obtain information on the subscriber
userMaxActiveLines	1.3.6.1.4.1.35265.1.29.38.10.1.9 1.3.6.1.4.1.35265.1.29.38.10.1.9.x	Get {} Get {}.x	The quantity of ingress/egress lines while operation in common line mode.

			Add subscriber index to OID to obtain information on the subscriber
userActiveCallCount	1.3.6.1.4.1.35265.1.29.38.10 .1.10 1.3.6.1.4.1.35265.1.29.38.10 .1.10.x	Get {} Get {}.x	The quantity of active calls while operation in common line mode. Add subscriber index to OID to obtain information on the subscriber
userRegExpires	1.3.6.1.4.1.35265.1.29.38.10 .1.11 1.3.6.1.4.1.35265.1.29.38.10 .1.11.x	Get {} Get {}.x	Time to registration expiry, in seconds. Add subscriber index to OID to obtain information on the subscriber
userLinesMode	1.3.6.1.4.1.35265.1.29.38.10 .1.12 1.3.6.1.4.1.35265.1.29.38.10 .1.12.x	Get {} Get {}.x	Lines operation modes. Add subscriber index to OID to obtain information on the subscriber. 0 – common; 1 – separate
userMaxIngressLines	1.3.6.1.4.1.35265.1.29.38.10 .1.13 1.3.6.1.4.1.35265.1.29.38.10 .1.13.x	Get {} Get {}.x	The quantity of ingress lines while operation in separate mode. Add subscriber index to OID to obtain information on the subscriber
userMaxEgressLines	1.3.6.1.4.1.35265.1.29.38.10 .1.14 1.3.6.1.4.1.35265.1.29.38.10 .1.14.x	Get {} Get {}.x	The quantity of egress lines while operation in separate mode. Add subscriber index to OID to obtain information on the subscriber
userActiveIngressCount	1.3.6.1.4.1.35265.1.29.38.10 .1.15 1.3.6.1.4.1.35265.1.29.38.10 .1.15.x	Get {} Get {}.x	The quantity of active ingress calls while operation in separate mode. Add subscriber index to OID to obtain information on the subscriber
userActiveEgressCount	1.3.6.1.4.1.35265.1.29.38.10 .1.16 1.3.6.1.4.1.35265.1.29.38.10 .1.16.x	Get {} Get {}.x	The quantity of active egress calls while operation in separate mode. Add subscriber index to OID to obtain information on the subscriber
stSetAuthLog	1.3.6.1.4.1.35265.1.29.38.15 .1.14	Get {} Set {} S	A name for authorization (login)
staticModeSetings	1.3.6.1.4.1.35265.1.29.38.11	Get {}	Operation mode with subscriber settings. None – operation with subscriber settings is disabled; Show – show the settings; Set – change settings; Add – add a subscriber; Del – remove a subscriber; The 'Show', 'Set', and 'Del' status display settings only if the search status does not equal to 'None'
staticSetMode	1.3.6.1.4.1.35265.1.29.38.12	Set {} N	Set subscriber settings operation mode 0 – None mode; 1 – Show mode; 2 – Set mode;

			3 – Add mode; 4 – Del mode
staticSetReset	1.3.6.1.4.1.35265.1.29.38.13	Set {} N	Reset setting changes (before applying) in 'Set' and 'Add' modes, in other modes this command will be ignored
staticSetApply	1.3.6.1.4.1.35265.1.29.38.14	Set {} N	Apply settings, add and removing of groups. New settings are activated in 'Set' mode; In 'Add' mode new subscriber is created and index for subscriber search is set equal to the created subscriber index, status of the search changes to 'Find user by index' and settings operation mode sets to 'Show'. In 'Del' mode user is deleted, search status and settings operation mode set to 'None'. The inquiry is ignored in 'None' and 'Show' modes
tableOfStSetUser	1.3.6.1.4.1.35265.1.29.38.15	Get {}	Table of static subscribers settings, root object
tableOfStSetUserEntry	1.3.6.1.4.1.35265.1.29.38.15 .1	Get {}	see TableOfStSetUser
stSetId	1.3.6.1.4.1.35265.1.29.38.15 .1.2	Get {}	Subscriber ID
stSetName	1.3.6.1.4.1.35265.1.29.38.15 .1.3	Get {} Set {} S	Displayed name of a subscriber
stSetIpAddr	1.3.6.1.4.1.35265.1.29.38.15 .1.4	Get {} Set {} A	Subscriber IP address
stSetSIPdomain	1.3.6.1.4.1.35265.1.29.38.15 .1.5	Get {} Set {} S	SIP domain
stSetNumber	1.3.6.1.4.1.35265.1.29.38.15 .1.6	Get {} Set {} S	Phone number
stSetNumplan	1.3.6.1.4.1.35265.1.29.38.15 .1.7	Get {} Set {} N	Dial plan
stSetAONnumber	1.3.6.1.4.1.35265.1.29.38.15 .1.8	Get {} Set {} S	Caller ID number
stSetAONtypeNumber	1.3.6.1.4.1.35265.1.29.38.15 .1.9	Get {} Set {} N	Caller ID number type 0 – Unknown; 1 – Subscriber; 2 – National; 3 – International; 4 – Network specific; 5 – No change (from call)
stSetProfile	1.3.6.1.4.1.35265.1.29.38.15 .1.10	Get {} Set {} N	SIP profile
stSetCategory	1.3.6.1.4.1.35265.1.29.38.15 .1.11	Get {} Set {} N	Caller ID category: 0 – No change (from call); 1..10 – Category selection

stSetAccessCat	1.3.6.1.4.1.35265.1.29.38.15 .1.12	Get {} Set {} N	Access category
stSetAuth	1.3.6.1.4.1.35265.1.29.38.15 .1.13	Get {} Set {} S	Authorization type: none – without authorization; register – REGISTER authorization; register_and_invite – REGISTER and INVITE authorization
stSetAuthLog	1.3.6.1.4.1.35265.1.29.38.15 .1.14	Get {} Set {} S	Authorization login
stSetAuthPass	1.3.6.1.4.1.35265.1.29.38.15 .1.15	Get {} Set {} S	Authorization password
stSetCliro	1.3.6.1.4.1.35265.1.29.38.15 .1.16	Get {} Set {} N	CLIRO service 0 – not installed; 1 – installed
stSetPbxProfile	1.3.6.1.4.1.35265.1.29.38.15 .1.17	Get {} Set {} N	PBX profile
stSetAccessMode	1.3.6.1.4.1.35265.1.29.38.15 .1.18	Get {} Set {} N	Customer service mode 0 – Enabled; 1 – Disabled 1; 2 – Disabled 2; 3 – ban 1; 4 – ban 2; 5 – ban 3; 6 – ban 4; 7 – ban 5; 8 – ban 6; 9 – ban 7; 10 – ban 8; 11 – excluded; 12 – disabled
stSetLines	1.3.6.1.4.1.35265.1.29.38.15 .1.19	Get {} Set {} N	The number of lines in common mode operation
stSetNoSRCportControl	1.3.6.1.4.1.35265.1.29.38.15 .1.20	Get {} Set {} N	Do not consider the source port after registration 0 – consider; 1 – do not consider
stSetBLFusage	1.3.6.1.4.1.35265.1.29.38.15 .1.21	Get {} Set {} N	Event subscription (BLF) 0 – disable; 1 – enable
stSetBLFsubscribers	1.3.6.1.4.1.35265.1.29.38.15 .1.22	Get {} Set {} N	The quantity of event subscribers.
stSetIntercomMode	1.3.6.1.4.1.35265.1.29.38.15 .1.23	Get {} Set {} N	Intercom call type 0 – One-sided; 1 – Two-sided; 2 – Regular call; 3 – Reject
stSetIntercomPriority	1.3.6.1.4.1.35265.1.29.38.15 .1.24	Get {} Set {} N	Intercom call priority (1..5)
stSetLinesMode	1.3.6.1.4.1.35265.1.29.38.15 .1.25	Get {} Set {} N	Lines operation mode 0 – Common; 1 – Separate

stSetIngressLines	1.3.6.1.4.1.35265.1.29.38.15 .1.26	Get {} Set {} N	The quantity of ingress lines in separate mode. 0 – no limit.
stSetEgressLines	1.3.6.1.4.1.35265.1.29.38.15 .1.27	Get {} Set {} N	The quantity of egress lines in separate mode. 0 – no limit
stSetMonitoringGroup	1.3.6.1.4.1.35265.1.29.38.15 .1.28	Get {} Set {} N	BLF monitoring group
stSetIntercomHeader	1.3.6.1.4.1.35265.1.29.38.15 .1.29	Get {} Set {} N	Set SIP-header for intercom: 0 – Answer-Mode: Auto 1 – Alert-Info: Auto Answer 2 – Alert-Info: info=alert-autoanswer 3 – Alert-Info: Ring Answer 4 – Alert-Info: info=RingAnswer 5 – Alert-Info: Intercom 6 – Alert-Info: info=intercom 7 – Call-Info: =\;answer-after=0 8 – Call-Info: \;answer-after=0 9 – Call-Info: ;answer-after=0
stSetIntercomTimer	1.3.6.1.4.1.35265.1.29.38.15 .1.30	Get {} Set {} N	Set preanswering pause which will be transmitted in answer-after parameter

5.10.3 Monitoring and configuration of dynamic subscriber groups

In the description of monitoring and configuration functions, commands for calling SNMP utilities will be presented in the following scripts for brevity and clarity of presentation:

Script **swalk**, realizing reading of values:

```
#!/bin/bash
/usr/bin/snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 "$@"
```

Script **sset**, realizing setting of values:

```
#!/bin/bash
/usr/bin/snmpset -v2c -c private -m +ELTEX-SMG 192.0.2.1 "$@"
```

5.10.3.1 Monitoring



Only authorized subscribers will be displayed while searchщтп dynamic subscribers.

The dynamic subscriber can be monitored using the following ways:

- 1) By group and subscriber index;
- 2) By subscriber ID;
- 3) By numbering plan and full subscriber number;
- 4) By numbering plan and part of a subscriber number.

To monitor:

- 1) Reset the search status;
- 2) Define search criteria (optionally);
- 3) Show the information.

5.10.3.2 Example of a search by index

```
sset groupResetCheck.0 i 1          # reset status of the search
sset getGroupByIndex.0 i 0          # select the zero group
sset getGroupUserByIndex.0 i 4      # set the search by index 4
swalk tableOfGroupUsers             # request for table with information on a subscriber
```

Result:

```
ELTEX-SMG::GroupUserID.0.4 = INTEGER: 4
ELTEX-SMG::RegState.0.4 = INTEGER: 1
ELTEX-SMG::Numplan.0.4 = INTEGER: 0
ELTEX-SMG::Number.0.4 = STRING: 240011
ELTEX-SMG::Ip.0.4 = IpAddress: 192.0.2.32
ELTEX-SMG::Port.0.4 = Gauge32: 5060
ELTEX-SMG::Domain.0.4 = STRING: dynsmg
ELTEX-SMG::MaxActiveLines.0.4 = INTEGER: -1
ELTEX-SMG::ActiveCallCount.0.4 = INTEGER: -1
ELTEX-SMG::RegExpires.0.4 = INTEGER: 55
ELTEX-SMG::TableOfGroupUsersEntry.13.0.4 = INTEGER: 1
ELTEX-SMG::TableOfGroupUsersEntry.14.0.4 = INTEGER: 3
ELTEX-SMG::TableOfGroupUsersEntry.15.0.4 = INTEGER: 4
ELTEX-SMG::TableOfGroupUsersEntry.16.0.4 = INTEGER: 0
ELTEX-SMG::TableOfGroupUsersEntry.17.0.4 = INTEGER: 0
```

5.10.3.3 Example of a search by subscriber ID

```
sset groupResetCheck.0 i 1          # reset status of the search
sset getGroupUserByID.0 i 2          # set subscriber ID
swalk tableOfGroupUsers             # request for table with information on a
subscriber
```

5.10.3.4 Example of a search by numbering plan and substring number

```
sset groupResetCheck.0 i 1          # reset status of the search
sset getGroupUserByNumplan.0 i 0     # set the zero numbering plan
sset getGroupUserBySubNumber.0 s 24001 # set a part of a number
swalk tableOfGroupUsers             # request for table with information on a subscriber
```

Result:

```
ELTEX-SMG::GroupUserID.0.0 = INTEGER: 0
ELTEX-SMG::GroupUserID.0.1 = INTEGER: 1
ELTEX-SMG::RegState.0.0 = INTEGER: 1
ELTEX-SMG::RegState.0.1 = INTEGER: 1
ELTEX-SMG::Numplan.0.0 = INTEGER: 0
ELTEX-SMG::Numplan.0.1 = INTEGER: 0
ELTEX-SMG::Number.0.0 = STRING: 240015
```

```

ELTEX-SMG::Number.0.1 = STRING: 240014
ELTEX-SMG::Ip.0.0 = IpAddress: 192.0.2.32
ELTEX-SMG::Ip.0.1 = IpAddress: 192.0.2.32
ELTEX-SMG::Port.0.0 = Gauge32: 5060
ELTEX-SMG::Port.0.1 = Gauge32: 5060
ELTEX-SMG::Domain.0.0 = STRING: dynsmg
ELTEX-SMG::Domain.0.1 = STRING: dynsmg
ELTEX-SMG::MaxActiveLines.0.0 = INTEGER: -1
ELTEX-SMG::MaxActiveLines.0.1 = INTEGER: -1
ELTEX-SMG::ActiveCallCount.0.0 = INTEGER: -1
ELTEX-SMG::ActiveCallCount.0.1 = INTEGER: -1
ELTEX-SMG::RegExpires.0.0 = INTEGER: 98
ELTEX-SMG::RegExpires.0.1 = INTEGER: 100
ELTEX-SMG::TableOfGroupUsersEntry.13.0.0 = INTEGER: 1
ELTEX-SMG::TableOfGroupUsersEntry.13.0.1 = INTEGER: 1
ELTEX-SMG::TableOfGroupUsersEntry.14.0.0 = INTEGER: 3
ELTEX-SMG::TableOfGroupUsersEntry.14.0.1 = INTEGER: 3
ELTEX-SMG::TableOfGroupUsersEntry.15.0.0 = INTEGER: 4
ELTEX-SMG::TableOfGroupUsersEntry.15.0.1 = INTEGER: 4
ELTEX-SMG::TableOfGroupUsersEntry.16.0.0 = INTEGER: 0
ELTEX-SMG::TableOfGroupUsersEntry.16.0.1 = INTEGER: 0
ELTEX-SMG::TableOfGroupUsersEntry.17.0.0 = INTEGER: 0
ELTEX-SMG::TableOfGroupUsersEntry.17.0.1 = INTEGER: 0

```

5.10.3.5 View the information without searching

```

sset groupResetCheck.0 i 1          # reset status of the search
swalk tableOfGroupUsers             # display all subscribers

```

5.10.3.6 Configuration

Configuration involves the following operations on dynamic subscribers' groups:

- 1) Settings viewing;
- 2) Settings editing;
- 3) Creation of a new subscriber;
- 4) Removing.

To view the settings:

- 4) Select subscriber group by index or ID;
- 5) Select configuration mode - view;
- 6) Display the necessary data.

To edit the settings:

- 5) Select subscriber group by index or ID;
- 6) Select configuration mode – edit;
- 7) Define necessary settings;
- 8) Apply the settings.

To create a new group:

- 4) Select configuration mode - creation;
- 5) Define necessary settings of a new group
- 6) Apply the settings.

To remove a group:

- 7) Select subscriber group by index or ID;
- 8) Select configuration mode - removing;
- 9) Apply the settings.

You can cancel changes that were not applied only in 'Add new group' and 'Edit a group' modes.



Undo group remove is not possible. Only a complete configuration restore via WEB or CLI is available.

5.10.3.7 Example of group creating

```
sset groupSetMode.0 i 3      # set the 'add' mode
sset groupSetApply.0 i 1    # apply the settings
sset groupSetMode.0 i 0    # set the 'none' mode
```

5.10.3.8 Example of settings viewing

```
sset groupByIndex.0 i 2     # select group by index - second
sset groupSetMode.0 i 1    # set the 'show' mode
swalk tableOfGroupSet      # view the settings table, or
swalk groupSetMaxReg       # maximum number of subscribers in the group, or
swalk groupSetName         # the name of the group, etc.
```

5.10.3.9 Example of settings editing

```
sset groupByID.0 i 3       # select group by index - third
sset groupSetMode.0 i 2    # set the 'set' mode
sset groupSetCliro.0 i 1   # activate the 'CLIRO' service
sset groupSetNumplan.0 i 3 # set the third numbering plan
sset groupSetIntercomMode.0 i 3 # forbid intercom calls
sset groupSetApply.0 i 1   # apply the settings
sset groupSetMode.0 i 0    # set the 'none' mode
```

5.10.3.10 Example of group removing

```
sset groupByID.0 i 3       # select group by ID - third
sset groupSetMode.0 i 4    # set the 'del' mode
sset groupSetApply.0 i 1   # apply the settings
# you do not need to set the 'none' mode manually
```

Table J12– Monitoring and configuration of dynamic subscriber groups

Name	OID	Inquiry	Description
smgSipUserGroup	1.3.6.1.4.1.35265.1.29.39	Get {}	The list of dynamic subscriber groups, root object.
groupCheckStatus	1.3.6.1.4.1.35265.1.29.39 .1	Get {}	Status of search by criteria None – without a search, displays all dynamic subscribers; Find user by group and user index; Find user by ID; Find user by numplan and number; Find user by numplan and number
groupResetCheck	1.3.6.1.4.1.35265.1.29.39 .2	Set {} N	Reset search status to 'None'. Set any value to reset
numGroups	1.3.6.1.4.1.35265.1.29.39 .3	Get {}	The quantity of subscriber groups
numInGroup	1.3.6.1.4.1.35265.1.29.39 .4	Set {} N	The quantity of subscribers in a group. Set a group number, and you will receive the number of subscribers. If you receive '-1' in reply, it means that the group with this number does not exist
numActiveInGroup	1.3.6.1.4.1.35265.1.29.39 .5	Set {} N	The quantity of active (authorized) subscribers in the group. Set a group number, and you will receive the number of subscribers. If you receive '-1' in reply, it means that the group with this number does not exist
getGroupByIndex	1.3.6.1.4.1.35265.1.29.39 .6	Set {} N	Setting the subscriber's index in the group for searching a subscriber by the group index. Setting a value from zero or more sets the group index and sets the search status to 'Find user by numplan and number'. Setting the value to '-1' – when the search status is active, "Find user by group and user index" sets the status to 'None'. When setting a group index that does not exist, the search status is reset to 'None'
getGroupUserByIndex	1.3.6.1.4.1.35265.1.29.39 .7	Set {} N	Setting the subscriber's index in the group for searching a subscriber by the group index. Set index of the group before start. (see GetGroupByIndex). The status of the search will be

			set to 'Find user by numplan and number'. Setting '-1' value make search status changed from 'Find user by group and user index' to 'None'
getGroupUserByID	1.3.6.1.4.1.35265.1.29.39.8	Set {} U	Set ID in order to search a subscriber. Setting '1' and greater numbers makes search status changed to 'Find user by ID'. If you set '0' value, the status will be changed from 'Find user by ID' to 'None'
getGroupUserByNumplan	1.3.6.1.4.1.35265.1.29.39.9	Set {} N	Set a dial plan in order to search subscriber by the number and dial plan. If you set '-1' value, the status of search will be changed to 'None'. If the value is greater than 0, the status will be set to ' Find user by numplan and number' (see getGroupUserByNumber). Otherwise, the status of search will not be changed
getGroupUserByNumber	1.3.6.1.4.1.35265.1.29.39.10	Set {} S Set {} "NULL"	Set a number in order to search subscriber by the number and numbering plan. The length of a number should be from 1 to 32 characters. If you set '0' or greater, the search status will be changed to 'Find user by numplan and number', otherwise, the status will not be changed. Set 'NULL' to reset a number, the search status will be changed to 'None' in this case
getGroupUserBySubNumber	1.3.6.1.4.1.35265.1.29.39.11	Set {} S	Set part of a number and numbering plan for subscriber search. The length of a number from 1 to 32 characters. If you set '0' or greater, the status of the search will be set to 'Find user by numplan and substring number', otherwise the status will not change. Set 'NULL' to reset a number, the search status will be changed to 'None' in this case
tableOfGroupUsers	1.3.6.1.4.1.35265.1.29.39.12	Get {}	Dynamic subscriber table, root object
tableOfGroupUsersEntry	1.3.6.1.4.1.35265.1.29.39.12.1	Get {}	see TableOfGroupUsers

groupUserID	1.3.6.1.4.1.35265.1.29.39 .12.1.3 1.3.6.1.4.1.35265.1.29.39 .12.1.3.x.x	Get {} Get {}.x.x	Subscriber's ID Add a group index and subscriber's ID to OID for obtaining information on the subscriber
groupUserRegState	1.3.6.1.4.1.35265.1.29.39 .12.1.4 1.3.6.1.4.1.35265.1.29.39 .12.1.4.x.x	Get {} Get {}.x.x	Subscriber's registration state. Add a group index and subscriber's ID to OID for obtaining information on the subscriber. 0 – unregistered; 1 – registered
groupUserNumplan	1.3.6.1.4.1.35265.1.29.39 .12.1.5 1.3.6.1.4.1.35265.1.29.39 .12.1.5.x.x	Get {} Get {}.x.x	Subscriber's numbering plan. Add a group index and subscriber's ID to OID for obtaining information on the subscriber
groupUserNumber	1.3.6.1.4.1.35265.1.29.39 .12.1.6 1.3.6.1.4.1.35265.1.29.39 .12.1.6.x.x	Get {} Get {}.x.x	Number of a subscriber. Add a group index and subscriber's ID to OID for obtaining information on the subscriber
groupUserIp	1.3.6.1.4.1.35265.1.29.39 .12.1.7 1.3.6.1.4.1.35265.1.29.39 .12.1.7.x.x	Get {} Get {}.x.x	Subscriber's IP address Add a group index and subscriber's ID to OID for obtaining information on the subscriber. If the IP address is unknown, the value will set to 0.0.0.0
groupUserPort	1.3.6.1.4.1.35265.1.29.39 .12.1.8 1.3.6.1.4.1.35265.1.29.39 .12.1.8.x.x	Get {} Get {}.x.x	Subscriber's port Add a group index and subscriber's ID to OID for obtaining information on the subscriber
groupUserDomain	1.3.6.1.4.1.35265.1.29.39 .12.1.9 1.3.6.1.4.1.35265.1.29.39 .12.1.9.x.x	Get {} Get {}.x.x	SIP domain of a subscriber. Add a group index and subscriber's ID to OID for obtaining information on the subscriber
groupUserMaxActiveLines	1.3.6.1.4.1.35265.1.29.39 .12.1.10 1.3.6.1.4.1.35265.1.29.39 .12.1.10.x.x	Get {} Get {}.x.x	The quantity of ingress/egress lines in 'common' mode. Add a group index and subscriber's ID to OID for obtaining information on the subscriber
groupUserActiveCallCount	1.3.6.1.4.1.35265.1.29.39 .12.1.11 1.3.6.1.4.1.35265.1.29.39 .12.1.11.x.x	Get {} Get {}.x.x	The quantity of active calls in 'common' line mode. Add a group index and subscriber's ID to OID for obtaining information on the subscriber
groupUserRegExpires	1.3.6.1.4.1.35265.1.29.39 .12.1.12	Get {} Get {}.x.x	Time to registration expiry, in seconds. Add a group index and

	1.3.6.1.4.1.35265.1.29.39 .12.1.12.x.x		subscriber's ID to OID for obtaining information on the subscriber
groupUserLinesMode	1.3.6.1.4.1.35265.1.29.39 .12.1.13 1.3.6.1.4.1.35265.1.29.39 .12.1.13.x.x	Get {} Get {}.x.x	Lines operation mode. Add a group index and subscriber's ID to OID for obtaining information on the subscriber. 0 – common; 1 – separate
groupUserMaxIngressLines	1.3.6.1.4.1.35265.1.29.39 .12.1.14 1.3.6.1.4.1.35265.1.29.39 .12.1.14.x.x	Get {} Get {}.x.x	The quantity of ingress lines in 'separate' mode. Add a group index and subscriber's ID to OID for obtaining information on the subscriber
groupUserMaxEgressLines	1.3.6.1.4.1.35265.1.29.39 .12.1.15 1.3.6.1.4.1.35265.1.29.39 .12.1.15.x.x	Get {} Get {}.x.x	The quantity of egress lines in 'separate' mode. Add a group index and subscriber's ID to OID for obtaining information on the subscriber
groupUserActiveIngressCount	1.3.6.1.4.1.35265.1.29.39 .12.1.16 1.3.6.1.4.1.35265.1.29.39 .12.1.16.x.x	Get {} Get {}.x.x	The quantity of active incoming calls in 'separate' line mode. Add a group index and subscriber's ID to OID for obtaining information on the subscriber
groupUserActiveEgressCount	1.3.6.1.4.1.35265.1.29.39 .12.1.17 1.3.6.1.4.1.35265.1.29.39 .12.1.17.x.x	Get {} Get {}.x.x	The quantity of active outgoing calls in 'separate' line mode. Add a group index and subscriber's ID to OID for obtaining information on the subscriber
groupUserGroupModeSettings	1.3.6.1.4.1.35265.1.29.39 .13	Get {}	Dynamic subscriber group operation settings modes: None – settings operation is disabled; Show – show group settings; Set – change group settings; Add – add a group; Del – remove a group
groupUserGroupSetMode	1.3.6.1.4.1.35265.1.29.39 .14	Set {} N	Set a mode for subscriber group operation 0 – None; 1 – Show; 2 – Set; 3 – Add; 4 – Del
groupUserGroupSetReset	1.3.6.1.4.1.35265.1.29.39 .15	Set {} N	Reset setting changes (before applying) in 'Set' and 'Add' modes, in other modes this command will be ignored
groupUserGroupSetApply	1.3.6.1.4.1.35265.1.29.39 .16	Set {} N	Apply settings, add and removing of groups

			<p>New settings are activated in 'Set' mode;</p> <p>In 'Add' mode new group is created and index for group search is set equal to the created group index, status of the search changes to 'Find group settings by index' and settings operation mode sets to 'Show'.</p> <p>In 'Del' mode group is deleted, search status and settings operation mode set to 'None'.</p> <p>The inquiry is ignored in 'None' and 'Show' modes</p>
groupUserGroupFindStatus	1.3.6.1.4.1.35265.1.29.39.17	Get {}	<p>Status of settings search by criteria:</p> <p>Without search;</p> <p>Find group settings by Index;</p> <p>Find group settings by ID</p>
groupResetFindStatus	1.3.6.1.4.1.35265.1.29.39.18	Set {} N	Reset status of search to 'without search' status. Set any value to reset
groupByIndex	1.3.6.1.4.1.35265.1.29.39.19	Set {} N	<p>Set group index and status of the search as 'Find group settings by index'.</p> <p>If you set '-1', the status will change from 'Find group settings by index' to 'Without search'</p>
groupByID	1.3.6.1.4.1.35265.1.29.39.20	Set {} N	<p>Set the group ID (from 1 and greater) and status of the search as 'Find group settings by ID'.</p> <p>If you set '-1', the status will change from 'Find group settings by ID' to 'Without search'.</p>
tableOfGroupSet	1.3.6.1.4.1.35265.1.29.39.21	Get {}	Table of dynamic subscriber group settings
tableOfGroupSetEntry	1.3.6.1.4.1.35265.1.29.39.21.1	Get {}	see TableOfGroupSet
groupSetId	1.3.6.1.4.1.35265.1.29.39.21.1.2	Get {}	Group ID
groupSetName	1.3.6.1.4.1.35265.1.29.39.21.1.3	Get {} Set {} S	Group name
groupSetSIPdomain	1.3.6.1.4.1.35265.1.29.39.21.1.4	Get {} Set {} S	SIP domain
groupSetMaxReg	1.3.6.1.4.1.35265.1.29.39.21.1.5	Get {} Set {} N	The maximum number of subscribers in a group
groupSetProfile	1.3.6.1.4.1.35265.1.29.39.21.1.6	Get {} Set {} S	SIP profile
groupSetCategory	1.3.6.1.4.1.35265.1.29.39.21.1.7	Get {} Set {} N	<p>Automatic calling line identification category</p> <p>0 – No change (from call);</p> <p>1..10 – Category selection</p>

groupSetAccessCat	1.3.6.1.4.1.35265.1.29.39 .21.1.8	Get {} Set {} N	Access category
groupSetCliro	1.3.6.1.4.1.35265.1.29.39 .21.1.9	Get {} Set {} N	CLIRO service 0 – not installed; 1 – installed
GroupSetPbxProfile	1.3.6.1.4.1.35265.1.29.39 .21.1.10	Get {} Set {} N	PBX profile
groupSetAccessMode	1.3.6.1.4.1.35265.1.29.39 .21.1.11	Get {} Set {} N	Customer service mode 0 – Enabled; 1 – Disabled 1; 2 – Disabled 2; 3 – ban 1; 4 – ban 2; 5 – ban 3; 6 – ban 4; 7 – ban 5; 8 – ban 6; 9 – ban 7; 10 – ban 8; 11 – excluded; 12 – disabled
groupSetLines	1.3.6.1.4.1.35265.1.29.39 .21.1.12	Get {} Set {} N	The quantity of lines in common mode
groupSetNumplan	1.3.6.1.4.1.35265.1.29.39 .21.1.13	Get {} Set {} N	Numbering plan
groupSetNoSRCportControl	1.3.6.1.4.1.35265.1.29.39 .21.1.14	Get {} Set {} N	Do not consider the source port after registration 0 – consider; 1 – do not consider
groupSetBLFusage	1.3.6.1.4.1.35265.1.29.39 .21.1.15	Get {} Set {} N	Event subscription (BLF) 0 – disable; 1 – enable.
groupSetBLFsubscribers	1.3.6.1.4.1.35265.1.29.39 .21.1.16	Get {} Set {} N	The quantity of subscribers to events
groupSetIntercomMode	1.3.6.1.4.1.35265.1.29.39 .21.1.17	Get {} Set {} N	Intercom call type 0 – One-sided; 1 – Two-sided; 2 – Regular call; 3 – Reject
groupSetIntercomPriority	1.3.6.1.4.1.35265.1.29.39 .21.1.18	Get {} Set {} N	Intercom call priority (1..5).
groupSetLinesMode	1.3.6.1.4.1.35265.1.29.39 .21.1.19	Get {} Set {} N	Lines operation mode: 0 – Common; 1 – Separate
groupSetIngressLines	1.3.6.1.4.1.35265.1.29.39 .21.1.20	Get {} Set {} N	The quantity of ingress lines in separate mode.
groupSetEgressLines	1.3.6.1.4.1.35265.1.29.39 .21.1.21	Get {} Set {} N	The quantity of egress lines in separate mode
groupSetAONtypeNumber	1.3.6.1.4.1.35265.1.29.39 .21.1.22	Get {} Set {} N	Caller ID type: 0 – Unknown; 1 – Subscriber; 2 – National; 3 – International;

			4 – Network specific; 5 – No change (from call)
groupSetMonitoringGroup	1.3.6.1.4.1.35265.1.29.39 .21.1.23	Get {} Set {} N	BLF monitoring group
groupSetIntercomHeader	1.3.6.1.4.1.35265.1.29.39 .21.1.24	Get {} Set {} N	Define SIP header for intercom: 0 – Answer-Mode: Auto 1 – Alert-Info: Auto Answer 2 – Alert-Info: info=alert- autoanswer 3 – Alert-Info: Ring Answer 4 – Alert-Info: info=RingAnswer 5 – Alert-Info: Intercom 6 – Alert-Info: info=intercom 7 – Call-Info: =\;answer-after=0 8 – Call-Info: \;answer-after=0 9 – Call-Info: ;answer-after=0
groupSetIntercomTimer	1.3.6.1.4.1.35265.1.29.39 .21.1.25	Get {} Set {} N	Set preanswering pause which will be transmitted in answer- after parameter

5.10.3.11 Out-of-date OID

Some of OIDs were changed and some branches might have been removed or changed to new values in subsequent releases. We recommend you to re-configure monitoring system and scripts to new OID usage.

Table J13 – Out-of-date OID

Name	OID	Inquiry	Description
eOneRSV	1.3.6.1.4.1.35265.1.29.7.1.8 1.3.6.1.4.1.35265.1.29.7.1.8.x	Get {} Get {}.x	Not used
eOneRxEqualizer	1.3.6.1.4.1.35265.1.29.7.1.15 1.3.6.1.4.1.35265.1.29.7.1.15.x	Get {} Get {}.x	Is not supported in new hardware versions, always –1
smgCpuLoad	1.3.6.1.4.1.35265.1.29.17	Get {}	Changed to smgCpuLoadTable (1.3.6.1.4.1.35265.1.29.37)
smgTopCpuUsr	1.3.6.1.4.1.35265.1.29.17.1.x	Get {}	Changed to cpuUsr (1.3.6.1.4.1.35265.1.29.37.1.2.x)
smgTopCpuSys	1.3.6.1.4.1.35265.1.29.17.2.x	Get {}	Changed to cpuSys (1.3.6.1.4.1.35265.1.29.37.1.3.x)
smgTopCpuNic	1.3.6.1.4.1.35265.1.29.17.3.x	Get {}	Changed to cpuNic (1.3.6.1.4.1.35265.1.29.37.1.4.x)
smgTopCpuIdle	1.3.6.1.4.1.35265.1.29.17.4.x	Get {}	Changed to cpuidle (1.3.6.1.4.1.35265.1.29.37.1.5.x)
smgTopCpuLo	1.3.6.1.4.1.35265.1.29.17.5.x	Get {}	Changed to cpulo (1.3.6.1.4.1.35265.1.29.37.1.6.x)
smgTopCpuIrq	1.3.6.1.4.1.35265.1.29.17.6.x	Get {}	Changed to cpulrq (1.3.6.1.4.1.35265.1.29.37.1.7.x)
smgTopCpuSirq	1.3.6.1.4.1.35265.1.29.17.7.x	Get {}	Changed to cpuSirq (1.3.6.1.4.1.35265.1.29.37.1.8.x)
smgTopCpuUsage	1.3.6.1.4.1.35265.1.29.17.8.x	Get {}	Changed to cpuUsage (1.3.6.1.4.1.35265.1.29.37.1.9.x)

5.10.3.12 OID MIB-2 support (1.3.6.1.2.1)

SMG supports the following MIB-2 branches:

- system (1.3.6.1.2.1.1) – common information on the system;
- interfaces (1.3.6.1.2.1.2) – information on network interfaces;
- snmp (1.3.6.1.2.1.11) – information on SNMP operation.

5.11 Appendix K. SMG Redundancy Function



Available only for SMG-2016/3016.

Starting from version 3.14.0, the redundancy function is implemented on SMG. This function is enabled automatically by installing an additional SMG-RESERVE license on the master device and SMG-RESERVE-SLAVE on the redundant one. The principle of operation is that the slave device is in sleep mode (SLAVE), it performs no functions and has no IP address on the network, monitors the main device (MASTER) constantly and, as soon as the MASTER fails, the SLAVE takes over all functions, completely replacing the failed MASTER device. To completely duplicate the functions, the slave device constantly updates the current configuration and other necessary files from the main device.

The SLAVE device activation occurs after connecting it to the MASTER device by creating a LAN and WAN connection between them. As soon as the two devices see each other via these links, the lifetime of the SLAVE device will be updated to 720 hours. This is the time of full operation of the SLAVE device without MASTER (in case MASTER failed for some reason and was disconnected from the SLAVE device). If the pair is assembled successfully and the gateway with the SMG-RESERVE license performs the MASTER role, the time on the gateway with the SMG-RESERVE-SLAVE license is restored to 720 hours.



To restore the lifetime on the SLAVE device, there must be two connections, both via LAN and WAN links. The recovery time is 5 minutes.

If the lifetime of the SLAVE device ends:

- If there is a connected gateway with the SMG-RESERVE license — switchover will be made (a gateway with the SMG-RESERVE license will become a MASTER device);
- If there is no connected gateway with the SMG-RESERVE license — termination of active connections and operation (similar to the completion of the "demo" operation mode) will occur.



To provide redundancy functions, use only the same type of SMG-2016 devices.

The typical connection schemes are below:

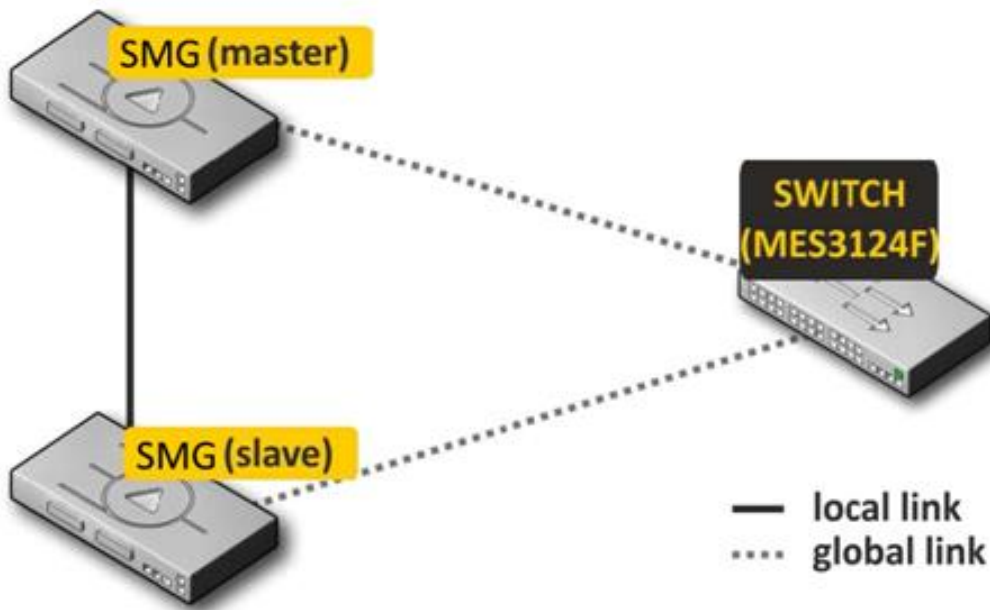


Figure 53 – Redundancy scheme with one switch

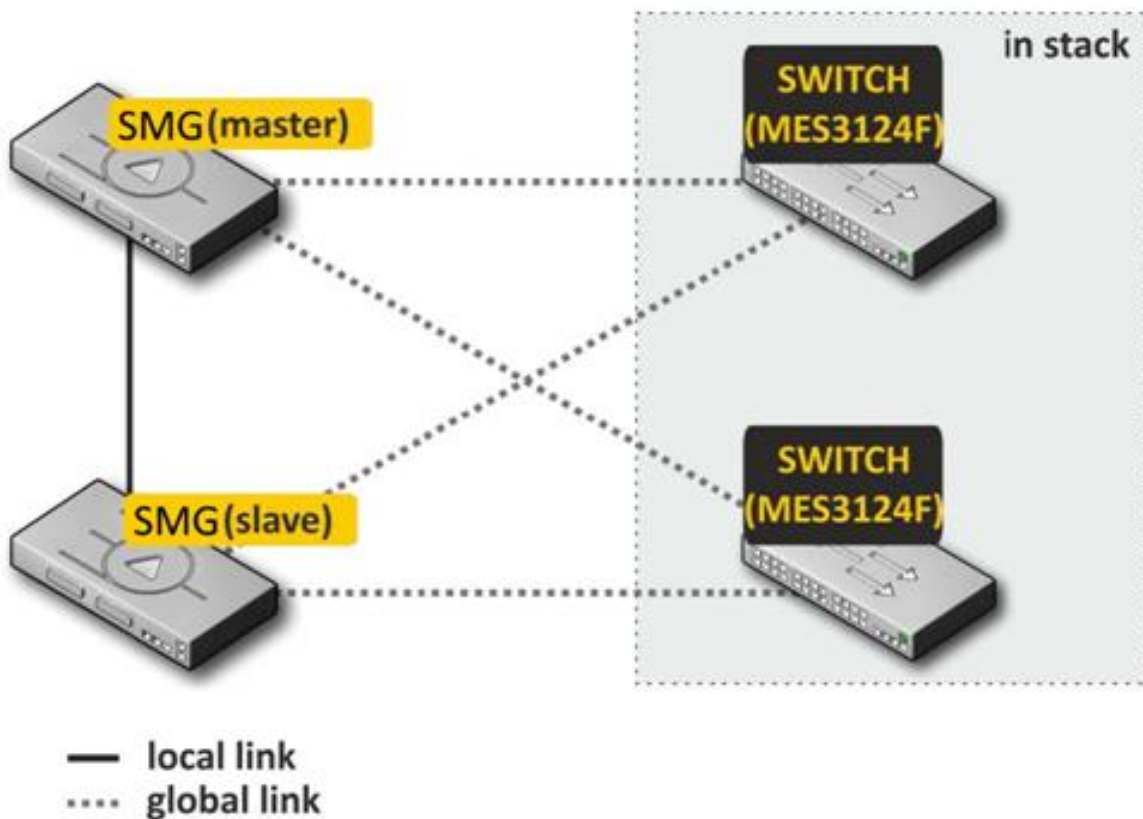


Figure 54 – Redundancy scheme with two switches in stack

There are 2 types of front ports for redundancy at the device — local and global ones. For SMG-2016 ports 0 and 1 can be used as local, and 2, 3 as global ports (for SMG-3016 local ports are 1 and 2, and the global ones are 3 and 4 respectively). When connecting devices, communication is required via local and global link simultaneously. The redundancy scheme works via IPv6 protocol, devices exchange configuration and other

necessary files to keep information up-to-date periodically during operation. VLAN 4091 is used for communication via the local link, and VLAN 4092 is used via the global one. In case of an interruption of the local link, the devices exchange files via the global link.

If one of the links connection is broken, the device initiates an alarm.

Procedure for redundancy connection and configuring

The case of connecting to two MES switches in stack will be considered (Figure 54). Initial state: two SMG of the same type with the reserve license, two MES switches in stack. The stack configuration on the switches is performed in accordance with operation manuals for these switches.

Firstly, it's necessary to configure service VLANs at the switches. VLAN 4092 must be allowed on the ports where global SMG links will be connected. The ports must also pass traffic of other VLANs configured on the SMG. Also, the ports to which SMG will be connected must be combined into a port-channel. The final scheme at this stage will look like this:

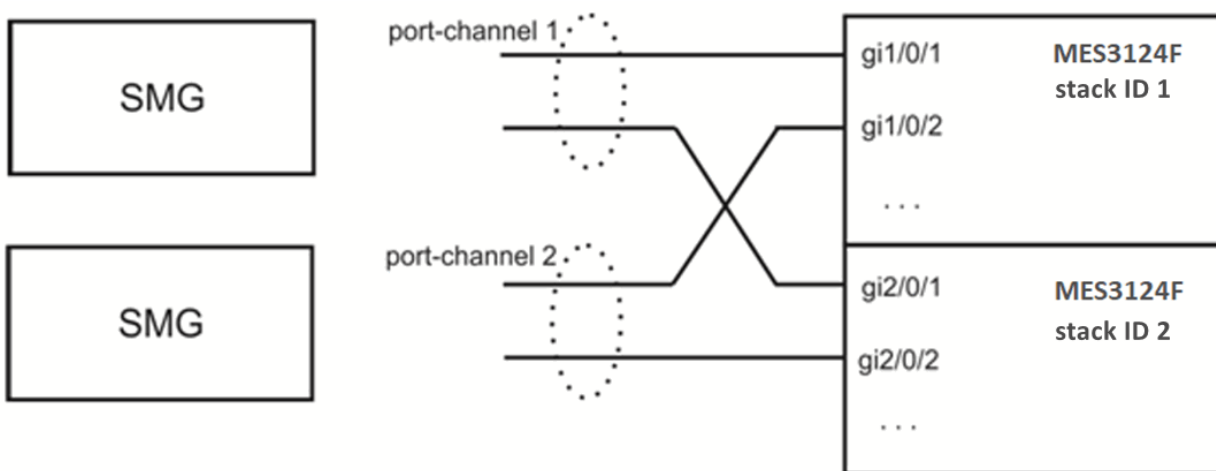


Figure 55 – The scheme of combining ports in port-channel

Next, the master SMG should be connected. At this stage, only global links are connected. After that, SMG is put into operation and becomes the master. The scheme at this stage will look like this:

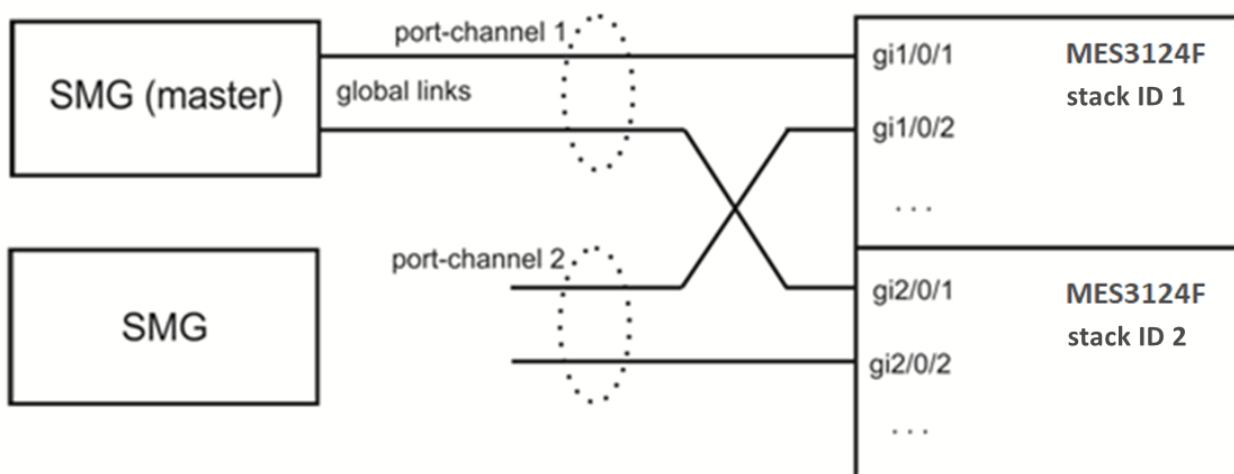


Figure 56 – Connection scheme of the master SMG

After that, a slave SMG is connected to the master one via local link. It takes some time for devices to detect each other and start to work as a slave-master pair (see the Monitoring – Reservation section). The scheme at this stage will look like this:

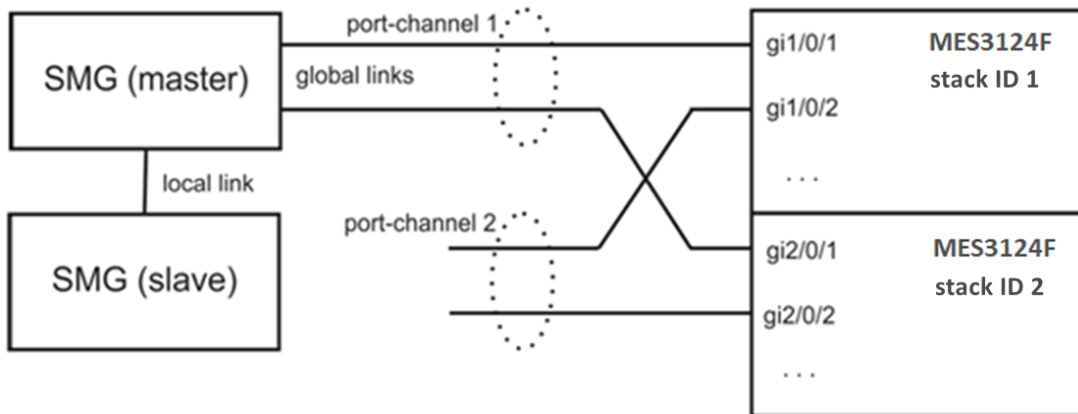


Figure 57 – Connection scheme of the slave SMG

After the master-slave pair has been formed, global links can be connected to the slave device:

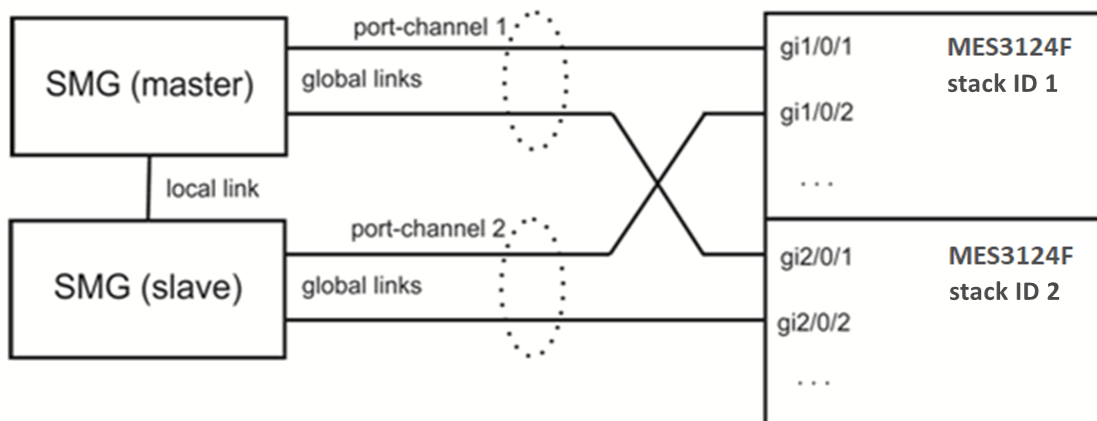


Figure 58 – Global links connection scheme

At this step, redundancy scheme is completely assembled. It's necessary to ensure in “monitoring” web section that SMGs see each other both via the local and via the global link.

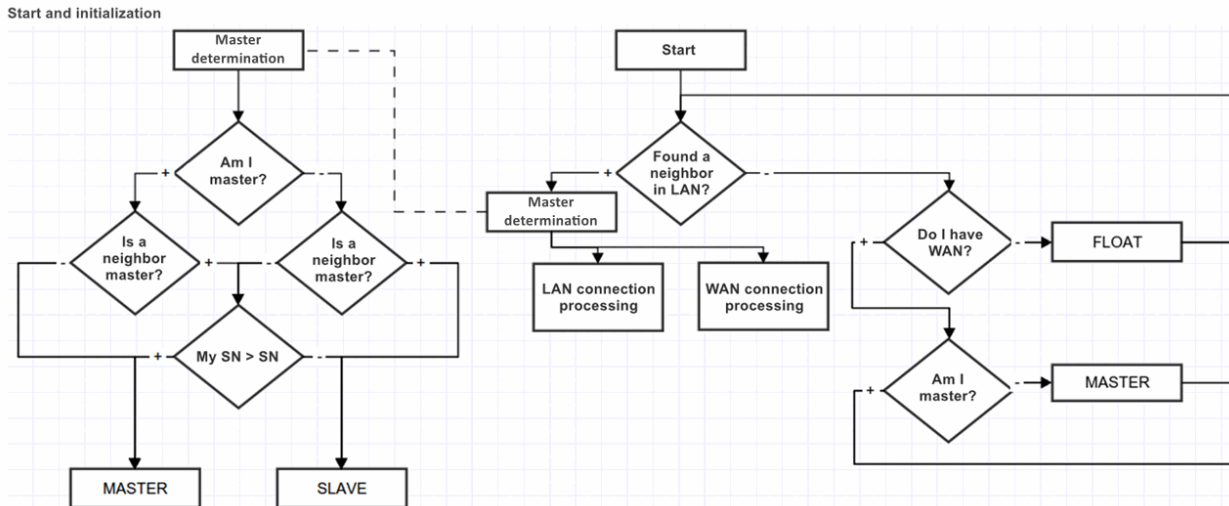
If problems occur with establishing a master-slave relationship, or lack of visibility on local and global links, please check that all configuration steps were performed correctly.

Master determination

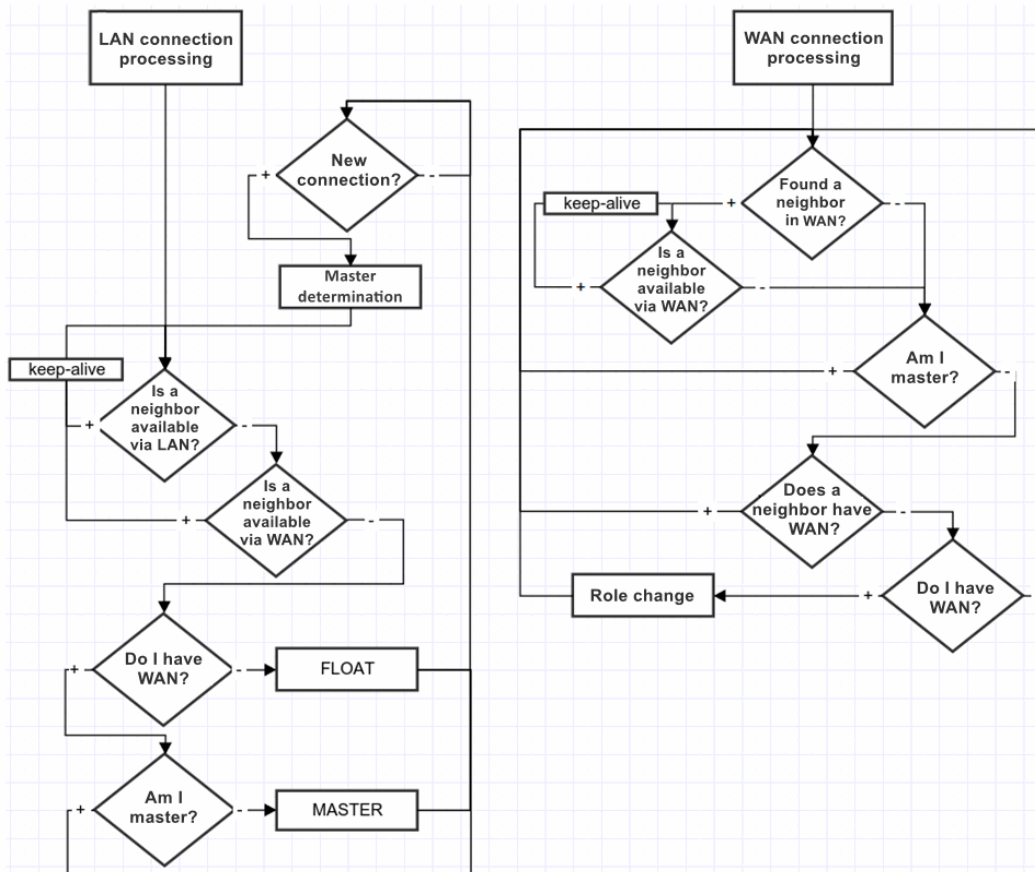
The following algorithm is used to determine which of the devices will be MASTER or SLAVE:

1. If local links are not active when the device is turned on, then the device becomes MASTER;
2. If global links are not active when the device is turned on, then the device becomes SLAVE;
3. If a SLAVE is connected to a MASTER device during operation, there will be no switchover;
4. If you connect a MASTER to another MASTER device during operation, then MASTER will be determined based on the serial number: whoever has a larger serial number will become a MASTER.

Block diagrams for master determination:



Processing connection via global or local link:



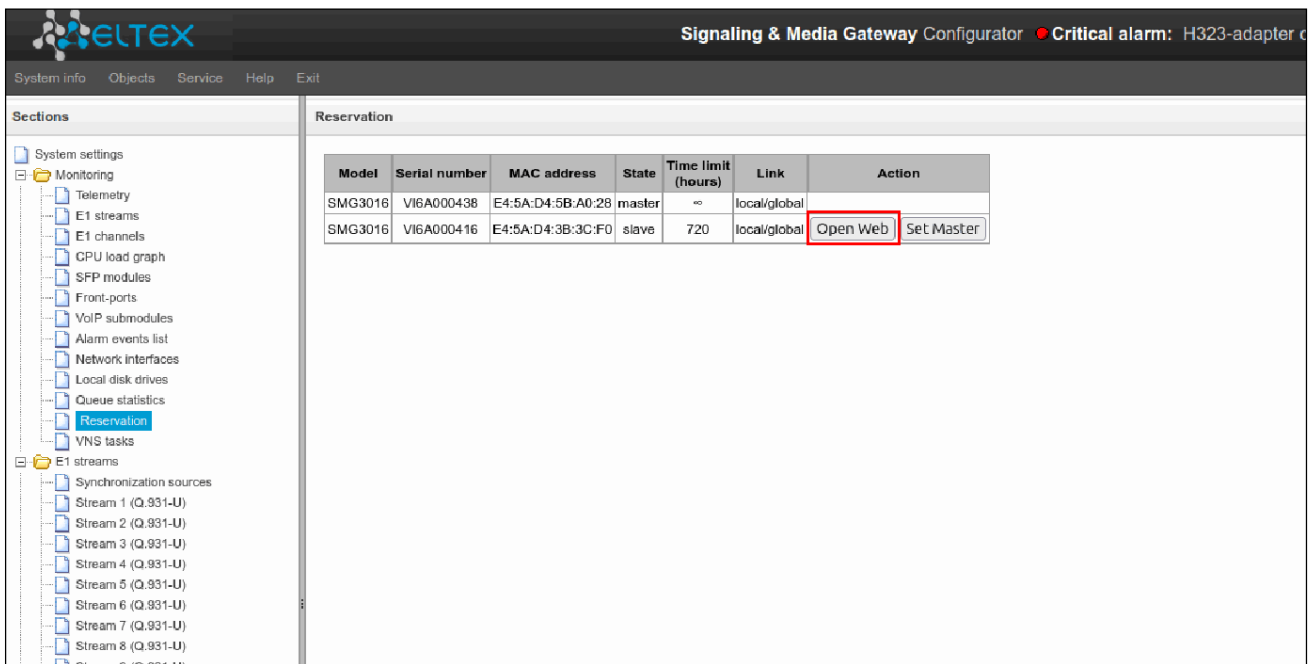
When connecting a device to already operating one, it is necessary to disconnect all WAN links on the connected device, connect the LAN link to the operating (MASTER) SMG, wait for approval, then connect the WAN links to the SLAVE (otherwise the newly connected device may be identified as a MASTER and transfer its outdated working files).

Working files are transferred immediately after connecting to the MASTER, every time when saving the configuration on flash, 10 seconds after each configuration change and periodically every 180 seconds.

List of files to be transferred between devices:

1. configuration file recorded in flash;
2. current running configuration file;
3. crypto keys for creating ssh tunnels;
4. database of registered subscribers;
5. linux users files;
6. user password files for web interface and CLI;
7. all dynamic firewall access lists;
8. keys and certificates for the https protocol.

During operation, a user can access SLAVE web interface. To do this go to the tab 'Monitoring' — 'Reservation' — 'open Web', or follow the link <http://<MASTER IP-address>:8080/login>, where instead of 192.168.0.100 enter the MASTER IP address.



The screenshot shows the ELTEX Signaling & Media Gateway Configurator interface. The top bar includes the ELTEX logo, the title "Signaling & Media Gateway Configurator", and a "Critical alarm: H323-adapter" indicator. The main interface is divided into a left sidebar with a tree view of sections and a main content area. The "Reservation" section is selected in the sidebar and is displayed in the main content area. It contains a table with the following data:

Model	Serial number	MAC address	State	Time limit (hours)	Link	Action
SMG3016	V16A000438	E4:5A:D4:5B:A0:28	master	∞	local/global	
SMG3016	V16A000416	E4:5A:D4:3B:3C:F0	slave	720	local/global	Open Web Set Master

The "Open Web" button in the second row of the table is highlighted with a red box.

Redundancy of E1 streams

Starting from version 3.17.0, the E1 streams redundancy function is implemented on SMG. This function is activated automatically by installing an additional SMG-RESERVE-E1 license (SMG-RESERVE or SMG-RESERVE-SLAVE license is required). The principle of operation is the following: E1 streams stay turned off on the slave device, thereby eliminating the influence of PDCs “connected in parallel”. It allows to connect the streams from the master and slave devices in parallel at the patch panel, without affecting each other.

After device switchover, respective streams are switched between master and slave gateways. Active connections are destroyed during switchover.

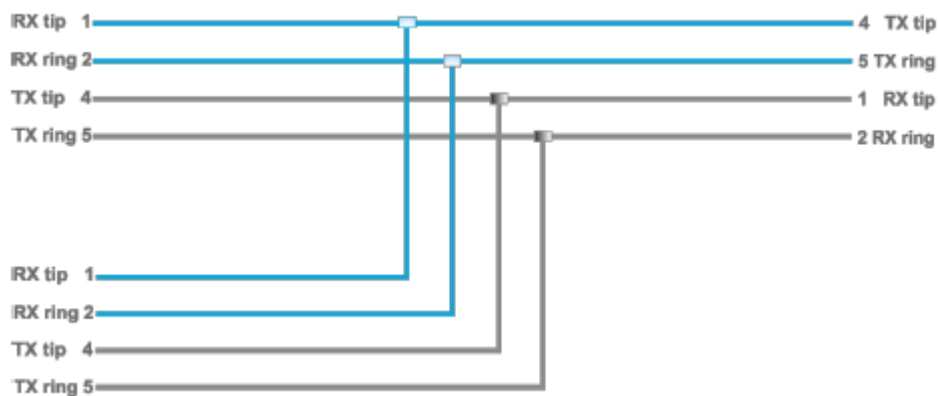
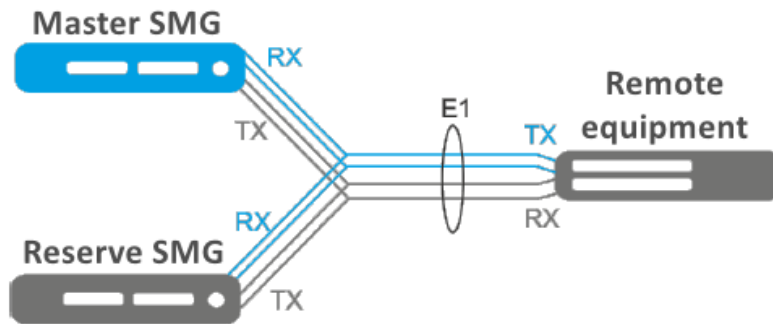


Figure 59 – The scheme of cable pinout for E1 redundancy

5.12 Appendix L. Safety recommendations

When installing and configuring SMG, you should pay attention to security settings – access organization to PBX management and monitoring, as well as call processing security. You should also pay attention to configuration backup.

Organization of access implies:

- changing standard passwords for WEB and CLI;
- creating limited accounts for certain types of settings and monitoring;
- setting restrictions on IP addresses and/or subnets from which configuration and monitoring can be made;
- setting up a static firewall that restricts access to signaling interfaces and manage only trusted nodes;
- setting up a dynamic firewall, which will automatically cut off unwanted access attempts for public interfaces.



Using SMG on a public network is undesirable without the use of additional security measures, such as a session border controller (SBC), a firewall, etc.

5.12.1 Changing passwords on WEB and CLI



Changing passwords for admin/root accounts is mandatory to ensure device security.

Passwords are changed via the 'Users: Management' menu.

Changing the WEB password for the admin account is done in the 'Set the administrator password for web-interface'.

Changing the CLI password for the admin account is done in the 'Set the administrator password for telnet/ssh'. More detailed information on setting can be found in the 'Users: Management' menu.

Changing the password for the root account is done through the shell. In order to change the password you need connect to SMG via ssh/console and run the following commands:

```
SMG2016>
SMG2016> sh (exit cli mode to shell mode)
/home/admin #
/home/admin #
/home/admin # passwd root (command to change root password)
Changing password for root
New password: (enter a new password)
Retype password: (repeat new password)
Password for root changed by root
/home/admin #
/home/admin #
/home/admin#save
tar: removing leading '/' from member names
***Saved successful
New image 0
Restored successful
/home/admin #
```

5.12.2 Creating restricted accounts

Creation of limited accounts for the web is done through the *'Users:Management'* menu.

- In the *'Web-interface users'* block, click *'Add'*;
- Set the user name and password;
- Select access permissions.

Creating restricted accounts is not supported for the CLI. More information on settings can be found in the *'Users: Management'* section.

5.12.3 Restricting access to signaling and management interfaces

Restrictions are configured in the *'TCP/IP Settings' → 'Network Interfaces'* menu.

- Go to the network interface settings.
- In the *'Services'* block, disable all management protocols and alarms not used on the interface.
- For the management interface, it is recommended to allow access only to the web interface and ssh.

More detailed configuration information can be found in the Network interfaces section.

Telnet access to the device should be prohibited via the public IP address.

Management should be allowed NOT via public addresses. If it is still used management via public IP, then it is necessary to use a list of allowed IP addresses – you need to add to the white list the address from which connections will be allowed. For all the rest, the access should be denied.

CHANGING STANDARD PORTS FOR ACCESS TO THE DEVICE

The setting is made in the menu *'TCP/IP Settings' → 'Network Settings'*

- Change the standard (22 for ssh and 23 for telnet) access ports to the device via ssh/ telnet protocols
- The standard port for accessing the device via the web (via the http protocol) can be changed via

CLI. To do this, connect to SMG via ssh/console and do the following commands:

```
SMG2016>
SMG2016> config
Entering configuration mode.
SMG2016-[CONFIG]> network
Entering Network mode.
SMG2016-[CONFIG]-NETWORK>
PORT Number in the range 1-65535
SMG2016-[CONFIG]-NETWORK> set settings web (specify the necessary port in the 1–65535 range)
```

It is recommended to use the HTTPS protocol to access the web interface.

It can be configured in the *'Security' → 'SSL/TLS settings'* section. The *'HTTPS only'* should be selected as the *'Protocol for WEB-interface'* in the SSL/TLS settings. It is also possible to use authorization via PAM/RADIUS. More detailed information on setup can be found in the SSL/TLS settings section.

CONFIGURING A LIST OF ALLOWED IP ADDRESSES

The setting is made in the *'Security' → 'White addresses list'* menu.

- Add to the white list addresses, from which access to the device is allowed via the web configurator and via telnet/ssh protocols;
- Enable the option *'Access only from allowed IP-addresses'*;
- Click the *'Apply'* and *'Confirm'* buttons.

More detailed configuration information can be found in White addresses list section.

5.12.4 Configuring a static firewall

A static firewall is used to restrict access to network interfaces according to a list of pre-defined rules.

The settings can be made in the *'Security' -> 'Static Firewall'* menu.

- Go to the firewall settings;
- Create a firewall profile by clicking the *'Add'* button;
- Set the profile name, click *'Next'*;
- Set filtering rules for incoming and outgoing traffic. At the same time, remember that if an incoming or outgoing packet did not fall under any filtering rule, then the *'Accept'* action is applied for it (allow the packet to pass through). Therefore, if access should be allowed only to some nodes and denied to all others, then it is necessary to configure the firewall profile so that the last rule is a rule with source type and destination *'Any'* and action *'Reject'* or *'Drop'* (drop a packet with notification via ICMP or discard without notification);
- In the *'Interface'* block, select the network interfaces for which filtering will be applied;
- Click the *'Save'* button located under the list of interfaces;
- Click the *'Apply'* button located at the top of the page;
- Click the *'Save'* button located above the filter tables.

More detailed configuration information can be found in the Static firewall section.

5.12.5 Configuring a dynamic firewall

A dynamic firewall is used to restrict access to network interfaces based on analysis of requests to various services. If repeated unsuccessful attempts to access service from the same IP address are detected, the dynamic firewall temporarily blocks it.

If an address is temporarily blocked several times, it is permanently blocked in the black list of addresses.

The settings can be made in the *'Security' -> 'Dynamic Firewall'* menu.

- Go to the firewall settings;
- Add addresses of trusted hosts and subnets to the white list;
- Check the *'Enable'* checkbox;
- Click the *'Apply'* button.

More detailed configuration information can be found in the Dynamic firewall section.

It is not recommended to use standard port 5060 for SIP signaling.

It is necessary to periodically check the information in the *'Security' -> 'Blocked addresses list'* section. It displays a list of addresses blocked by the dynamic firewall from which an unsuccessful attempt was made to gain access to the device.

It is recommended to periodically change passwords for accessing the device via web/ssh. The Policy of shifting passwords should be determined by your security team.



It is recommended to use the latest software version: <https://eltex-co.ru/support/downloads/>

5.13 Appendix H. Configuring a software media server



Available for SMG-3016 only.

In the transit scheme of interaction with the geographical separation of SMG from SSW, signaling as well as the media is processed on the server with softswitch (by default, msr is installed on the host with ssw). As a result, when calling within one SMG, all media had to be sent through SSW (Figure H1).

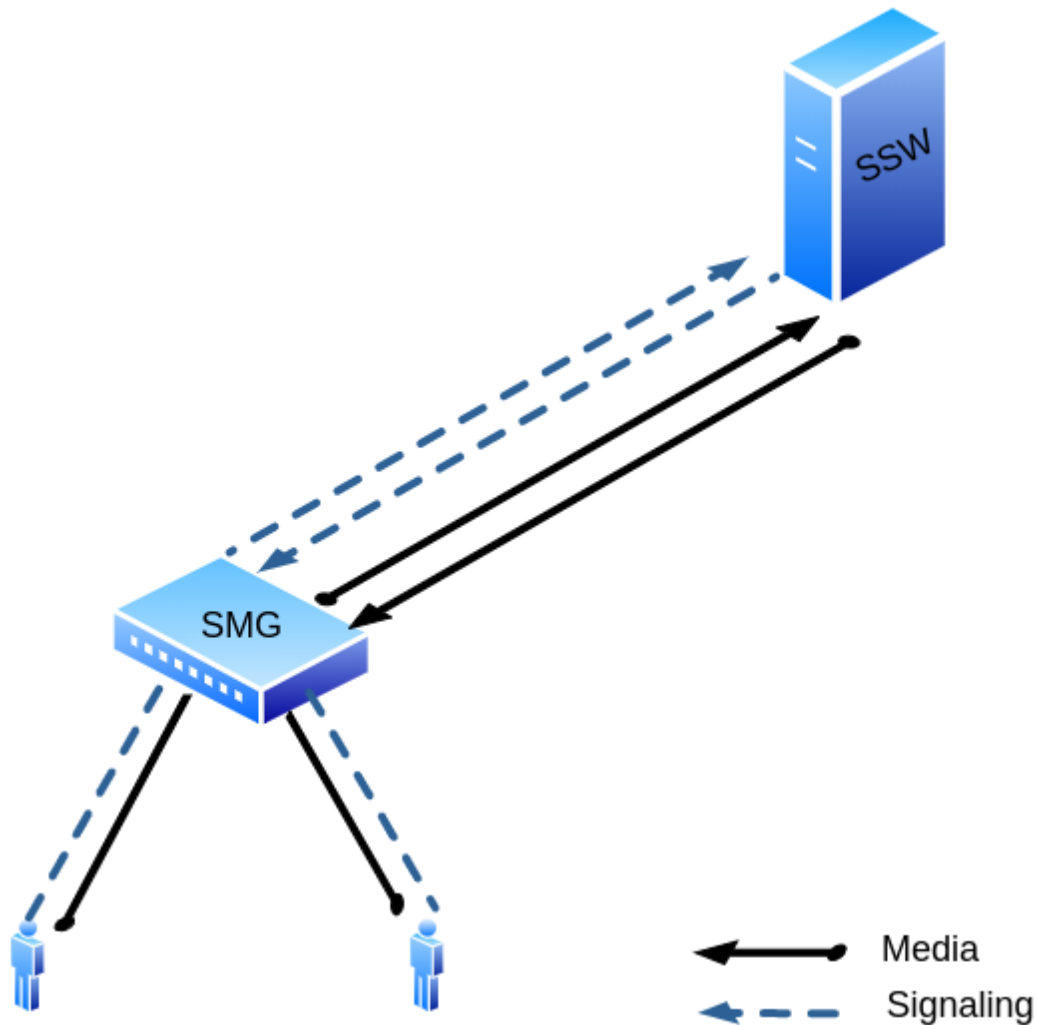


Figure 60 – MSR in on the SSW

For such cases, a media server was installed on the SMG. When a connection is established, SSW indicates MSR on SMG as a media processor, as a result of which rtp does not go to the upstream server, but processed locally on the SMG (Figure H2 below).

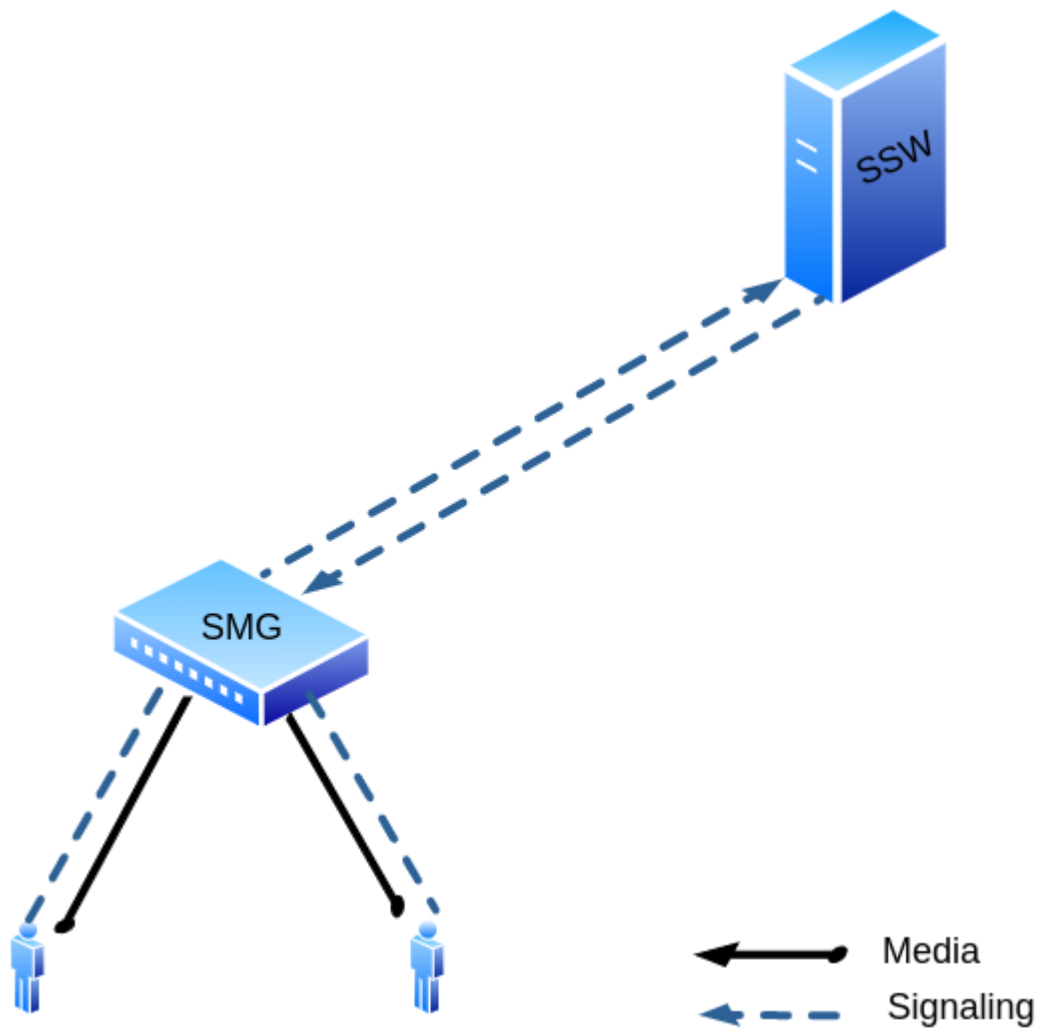


Figure 61 – MSR in on the SSW

5.13.1 Media server settings



The media server activation is only available with an SMG-MSR license, more details about licenses see in the Licenses section.

In the configuration file, which is located at the path `/etc/config/ecss_msr_ena`, the line `ECSS_MSR_ENA=no` should be replaced with `ECSS_MSR_ENA=yes`.

The whole setup comes down to changing the configuration file located at `/etc/config/config.xml`

To edit the file, you can use the vi. editor on the SMG (`vi /etc/config/config.xml`).

Default file example

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <general log-level="3" max-calls="1000" max-in-group="3"
  tread-cnt="2" syslog="no"/>
  <transport bind-addr="127.0.0.1" port="5080" transport="udp" />
  <media use-vad="no" port-start="15000" port-range="5000" rtcp-timeout="15" />
  <codec pcma="1" pcmu="2" g729="3" ilbc="4" gsm="5" g722="6" />
  <accounts>
    <dynamic msr_name="msr.smg" realm="sip:127.0.0.1:5000" dtmf_mode="rfc+inband+info"
    auth_name="user" auth_password="password" />
  </accounts>
  <pbyte>
    <mcc bind-addr="127.0.0.1" port="51000" />
  </pbyte>
</config>
```

Where:

- general – general settings of media server:
 - log-level – logs level. The larger the value, the more information is in the logs (by default: "3");
 - max-calls – the maximum number of calls simultaneously served by the media server;
 - max-in-group – maximum number of subscribers in a group within a conference;



If the Conference Call service is used with a large number of participants, then it is necessary to increase the value of this parameter. The maximum value is 4000.

- transport — transport settings:
 - bind-addr — IP address that the media server will use for SIP signaling (by default: "127.0.0.1"). This parameter should be configured in accordance with the network host settings;
 - port — port number for SIP (by default: "5080"). If 5040 port is already busy on the host where the media server is installed, then the value of this parameter should be changed;
 - transport — transport type (by default: "udp"), takes values: "udp", "tcp", "udp+tcp". This parameter does not require changes.
- media – media parameters:
 - use-vad — enable Voice Activity Detection (by default: "no"). This parameter does not require changes;
 - rtcp-timeout - if RTCP does not arrive to the media server during this period of time, then you can assume that the client is inactive (by default: "0" – not used). When using the

-
- control function, the control is enabled only after receiving one RTCP packet from the opposite side;
 - rtp-timeout — RTP traffic timeout, similar to the previous parameter (by default: "0" – not used);
 - port-start — the beginning of the range of ports that will be used for RTP streams (by default: "12000");
 - port-range — range size (by default: "1024");
 - thread-cnt — number of working streams for processing media data (dtmf-to-total-energy, by default: "2");
 - codec — priority of codecs (1 – maximum, 255 – minimum, 0 – the codec is disabled). Supported codecs:
 - pcma
 - pcmu
 - ilbc
 - gsm
 - g722
 - g729
 - t38
 - accounts — all accounts for registering the media server. Can contain up to 32 acc elements;
 - dynamic — separate account with parameters:
 - msr_name — the MSR name as displayed on ECSS;
 - realm — registration server in the sip:domain format. Specify the SIP server address for media server registration;
 - dtmf_mode — DTMF detection mode ("rfc", "inband", "info"). This parameter should be configured in accordance with the DTMF sending settings on the subscriber device.
 - auth_name — user name used for authorization;
 - auth_password — password for authorization.
 - pbyte — setting up pbyte connections;
 - mcc — setting up the control connection of the media control channel;
 - bind-addr — IP address where the connection will be expected;
 - port — port for incoming connections (by default: 5700).
 - conf_dir path — path to the folder that will contain the MSR configurations. These configurations will override the default configuration config.xml



Separately, you need to pay attention to the media section; the **port-start** and **port-range** parameters should not overlap with the parameters used on the SMG.

The settings of configuration files can be changed in the directory: `/etc/ecss/ecss-media-server/conf.d` for the `config.xml` file



This PAC is not designed for a large number of simultaneous calls and has performance limitations.

For the G711 codec, it is strongly recommended to make no more than 150 simultaneous calls. For G729 codec, it is strongly recommended to make no more than 25 simultaneous calls in case of using one thread-cnt (see default file example), in case of using two thread-cnt, the number of calls is increased up to 50.

5.13.2 Media server launch

The media server starts automatically when the system starts.
To operate, the service uses the configuration from the file

```
/etc/config/config.xml
```

When changing the configuration, you should restart the ecss-media-server service.
To do this, terminate the ecss-media-server process and it will start with a new configuration.

```
pkill -2 ecss-media-server
```

5.13.3 Example of setting up MSR with Softswitch



The necessary MSR settings on the SMG are made in the **shell** command string.

Changing the configuration is done by changing the **config.xml file**

```
vi /etc/config/config.xml
```

In our case it will look like this:

```
<config>
  <general log-level="3" max-calls="1000" max-in-group="3"
  tread-cnt="2" syslog="no"/>
  <transport bind-addr="192.168.114.79" port="5080" transport="udp" />
  <media use-vad="no" port-start="15000" port-range="5000" rtcp-timeout="15" />
  <codec pcma="1" pcmu="2" g729="3" ilbc="4" gsm="5" g722="6"/>
  <accounts>
    <dynamic msr_name="msr.smg" realm="sip:192.168.114.90:5000" dtmf_mode="rfc+inband+info
    " auth_name="user" auth_password="password" />
  </accounts>
  <pbyte>
    <mcc bind-addr="192.168.114.79" port="51000" />
  </pbyte>
  <conf_dir path="/etc/config/conf.d"/>
</config>
```

Where:

- 192.168.114.79 – IP address of SMG,
- 192.168.114.90 – IP address of SSW.

You should restart MSR for the changes to take effect.

```
pkill -2 ecss-media-server
```

If the configuration is correct, the MSR will send the registration to the IP address of SSW:

```
REGISTER sip:192.168.114.90:5000 SIP/2.0
Via: SIP/2.0/UDP 192.168.114.79:5080;rport;branch=z9hG4bKPjuUBlvIWbH0rgYXYLRVCBkWRCJvNmZX4w
Max-Forwards: 70
From: <sip:bond1.1@msr.smg>;tag=ruTwS9WQ7HaSalkcdz9J9NJBpCntQUGL
To: <sip:bond1.1@msr.smg>
Call-ID: Nm96ZyfgH9ND8ZFDXhUzsQcDrYnw7hRq
CSeq: 1 REGISTER
P-Eltex-MSR-Iface-Name: bond1.1
P-Eltex-MSR-Iface-Addr: 192.168.114.79
P-Eltex-MSR-CC-Addr: 192.168.114.79
P-Eltex-MSR-CC-Port: 51000
P-Eltex-MSR-Name: msr.smg
P-Eltex-Max-Calls: 1000
User-Agent: Eltex media-server 3.14.11.1
Contact: <sip:bond1.1@192.168.114.79:5080>
Expires: 3600
Allow: PRACK, INVITE, ACK, BYE, CANCEL, UPDATE, INFO, SUBSCRIBE, NOTIFY, REFER, MESSAGE,
OPTIONS
Content-Length: 0
```

On the softswitch side, this MSR should be declared (the command is executed in **cocon**):

```
system/media/resource/declare core1@ecss1 contact bond1.1@msr.smg default local true
```

To check the status, use the command:

```
system/media/resource/list
```

TECHNICAL SUPPORT

For technical assistance in issues related to handling Eltex Ltd. equipment, please, address to Service Center of the company:

<http://www.eltex-co.com/support>

You are welcome to visit Eltex official website to get the relevant technical documentation and software, to use our knowledge base or consult a Service Center Specialist:

<http://www.eltex-co.com/>

<http://www.eltex-co.com/support/downloads/>