ELTEX

Complete solutions for networking

Digital gateway

SMG-4, SMG-2

Operation manual, version 2.4 (15/06/2017)

Firmware version: 3.1.6.1189

Firmware version	V.3.1.6.1189	
SIP adapter version	V.3.1.6.67	
Document version	Issue date	Revisions
Version 2.4	15/06/2017	Updated: —encoding settings and configuration of methods of subscriber name transmission in Q.931 Added: —insert remote name in Contact header —SS7 channels transit via semi-permanent connection —name transmission using AVAYA, Siemens, Windows-1251 encodings, Translit and Unicode (UTF-8). —name transmission methods: QSIG, Q.931 Display, CorNet and AVAYA Display
Version 2.3	15/08/2016	Time zones updated. New features added: - STUN server parameters, - public IP settings, - Clear Channel (CLEARMODE) settings, - English language.
Version 2.2	05/04/2016	Support added for routing modes configuration during trunk registration for SIP interfaces.
Version 2.1	26/11/2015	SIP interfaces registration added.
Version 2.0	22/06/2015	Second issue.
Version 1.0	12/08/2014	First issue.

EXPLANATION OF THE SYMBOLS USED

Symbol	Description
Calibri	Notes, warnings, chapter headings, titles, and table titles are written in bold.
Calibri	Italic denotes important information that requires special attention.
Courier New	Courier New is used for command entry examples, command execution results, and program output data.
<KEY>	Keyboard keys are written in upper-case and enclosed in angle brackets.
	Analogue phone unit.
	SMG digital gateway.
	Softswitch ECSS-10 software switch.
	Digital subscriber PBX.
	Network connection.
	Optical transmission medium.

Notes and Warnings

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

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

TARGET AUDIENCE

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

TABLE OF CONTENTS

INTRODUCTION

Today, means of communication employing state-of-the-art hardware and software solutions evolve rapidly. New communication devices, which utilise alternative data transmission principles, pose a problem of their integration into existing communication networks. The solution is to use special equipment, which interconnects diverse segments of networks. Currently, such equipment is represented by digital gateways. They allow gradual transition from existing communication networks to more efficient ones with alternative operation principles.

At present, IP networks are considered to be the most efficient when they are weakly dependent from data type and transmission medium and at the same time are flexible and manageable. Designed and manufactured by Eltex, SMG digital gateway is intended for interfacing of traditional communication networks based on the link switching principle with communication networks used for IP network data transmission.

This operation manual details main features of SMG-2 and SMG-4 digital gateways. The document contains technical specifications of the gateway and its components. Also, it provides an overview of operation and maintenance software-based procedures.

1 DEVICE DESCRIPTION

1.1 Purpose

The SMG trunk gateway is designed to interface signalling, PSTN (E1) media streams, and VoIP networks.

SMG is an optimal and robust solution that can be used to upgrade, develop, and migrate telecommunication infrastructures from PSTN to NGN.

SMG Main Specifications

- Number of E1 interfaces:
    - for SMG-2: 1 or 2[1];
    - for SMG-4: 4.
- Number of VoIP channels:
    - for SMG-2: 104;
    - for SMG-4: 128.
- Maximum load intensity—40 cps.
- Number of Ethernet ports:
    - 1 port 10/100/1000BASE-T.
- Static address and DHCP support.
- IP telephony protocols: SIP, SIP-T, SIP-I.
- TDM protocols: ISDN PRI(Q.931), QSIG, and CORNET for subscriber name transmission, SS-7 (quasi-associated mode operation).
- DTMF transmission (SIP INFO, RFC2833, in-band).
- Echo cancellation (G.168 recommendation).
- Voice activity detector (VAD).
- Comfortable noise generator (CNG).
- Adaptive or fixed jitter buffer.
- V.152 data transmission.
- Fax transmission:
    - G.711 pass through;
    - T.38 UDP Real-Time Fax.
- NTP support.
- DNS support.
- SNMP support.
- ToS for RTP and signalling.
- Firmware update: via web interface, CLI (Telnet, SSH, console (RS-232));
- automatic update of firmware and device configuration.
- Configuration and setup (also remotely):
    - web interface;
    - CLI (Telnet, SSH, console (RS-232)).

---

[1] Only one E1 stream is available in an SMG-2 device by default. To activate another one, a special licence is required. For more information about licences, see section **4.1.19**. **Licence Renewal**

- Remote monitoring:
    - web interface;
    - SNMP.

SIP/SIP-T/SIP-I Functions

- RFC 2976 SIP INFO (for DTMF transmission);
- RFC 3204 MIME Media Types for ISUP and QSIG (ISUP support);
- RFC 3261 SIP;
- RFC 3262 Reliability of Provisional Responses in SIP (PRACK);
- RFC 3263 Locating SIP servers for DNS;
- RFC 3264 SDP Offer/Answer Model;
- RFC 3265 SIP Notify;
- RFC 3311 SIP Update;
- RFC 3323 Privacy Header;
- RFC 3325 P-Asserted-Identity;
- RFC 3372 SIP for Telephones (SIP-T);
- RFC 3398 ISUP/SIP Mapping;
- RFC 3515 SIP REFER;
- RFC 3581 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 5806 SIP Diversion Header;
- SIP Enable/Disable 302 Responses;
- Q1912.5 SIP-I;
- SIP/SIP-T/SIP-I interaction;
- Delay offer;
- SIP OPTIONS Keep-Alive (SIP Busy Out).

1.2   Typical Applications

This manual describes several methods of SMG connection.

1.2.1   Interface for TDM and VoIP Network Signalling and Media Streams

In this configuration, the device allows connection of up to 4 E1 streams with various signalling (SS-7, ISDN PRI/QSIG/CORNET) and service protocols for up to 128 uncompressed channels (G.711 codec), for up to 72 compressed channels (G.729 A / 20-80), or for 54 T.38 fax channels; maximum load intensity—40 cps.

The device connects to an IP network via 10/100/1000 BASE-T network interface using SIP/SIP-T/ SIP-I protocols.

Fig. 1.1—Interfacing of TDM and VoIP Network Signalling and Media Streams Using SMG-4

Fig. 1.2—Interfacing of TDM and VoIP Network Signalling and Media Streams Using SMG-2

Fig. 3 shows TDM and VoIP network interfacing and uses interaction between MC240 digital PBX and ECSS-10 software switch as an example.
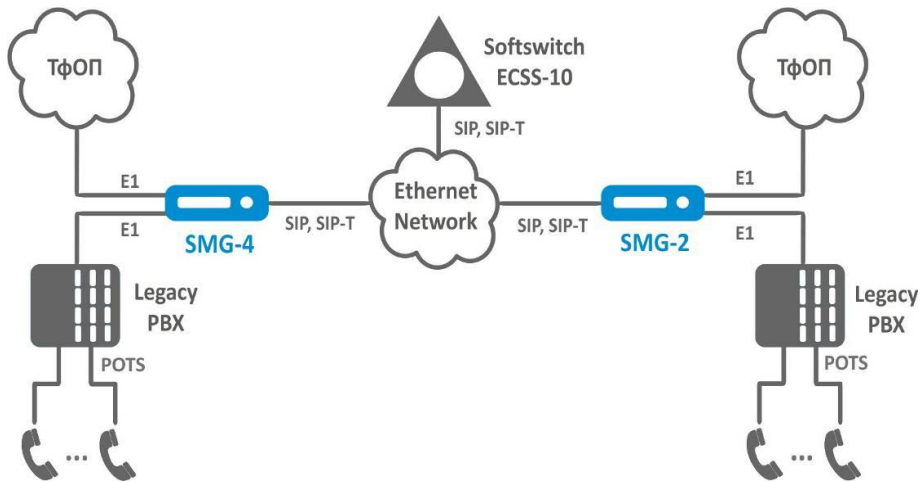
Fig. 1.3—Interfacing of TDM and VoIP Network Signalling and Media Streams

Fig. 4 shows scheme of semi-permanent connection over E1 channels through an Ethernet network.
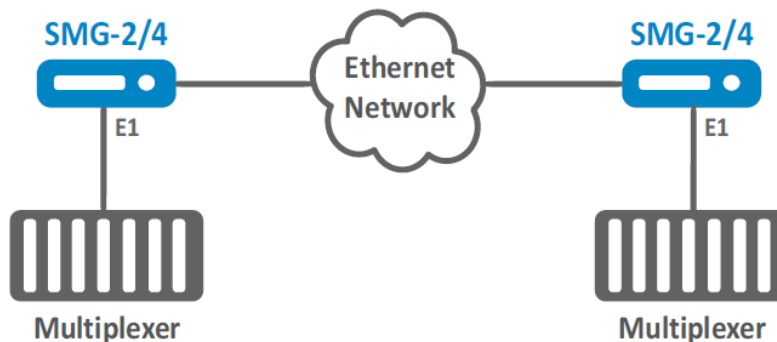
Fig. 1.4 - Semi-permanent connection over E1 channels trough an Ethernet network

1.3   Device Design and Operating Principle

SMG has a submodule architecture and contains the following elements:

- A controller featuring:

- a controlling CPU,

- flash memory of 64 MB,

- 512 MB RAM;

- *M4E1* submodule of E1 streams;

- *SM-VP-M200 IP submodule for SMG-2;*

- *SM-VP-M300 IP submodule for SMG-4;*

- a phase-lock-loop (PLL) frequency control system.

See the SMG functional chart in Fig. 4.
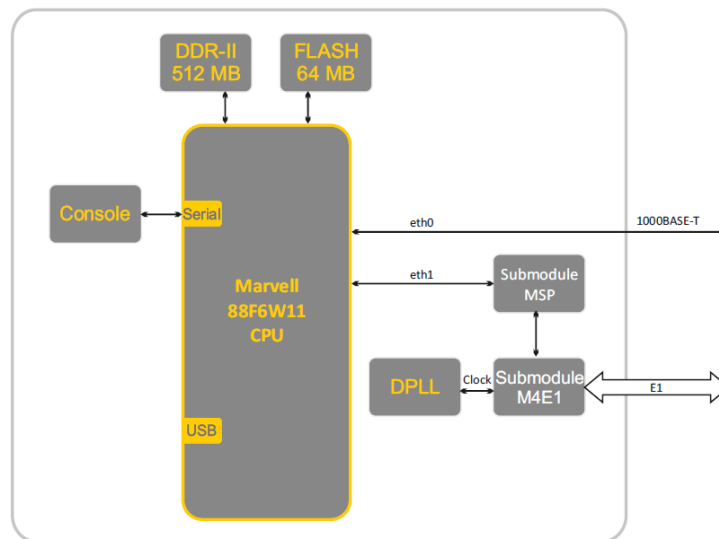
Fig. 1.5—SMG Functional Chart

In the TDM-IP direction, a signal coming to E1 streams is transferred to VoIP submodule audio codecs (a line of 128 TDM channels) via the intrasystem backbone to be encoded using one of the selected standards and further transferred as digital packets to the central processing unit. In the IP-TDM direction, digital packets are transferred to the VoIP submodule to be decoded and further transferred to E1 streams via the intrasystem backbone.

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

See Fig. 5 for device firmware architecture.
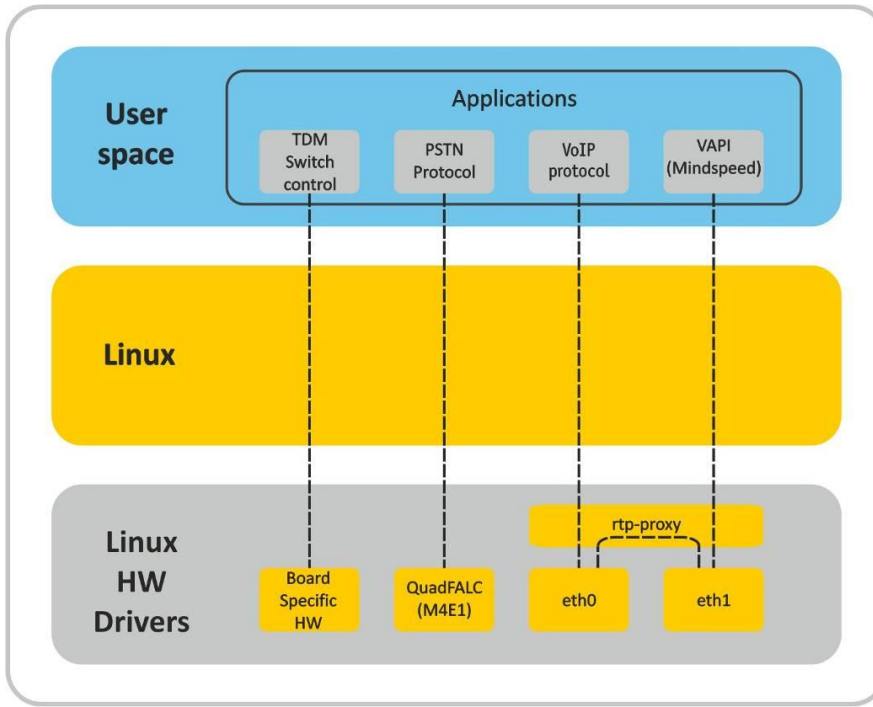
Fig. 1.6—SMG firmware architecture

1.4 Main Specifications

The main specifications of the terminal are provided in the following tables:

Table 1.1 —Main Specifications

VoIP Protocols

Supported protocols	SIP-T/SIP-I
	SIP
	T.38

Audio Codecs

Codecs	G.711 (A/U)
	G.729 AB
	G.723.1 (6.3 Kbps, 5.3 Kbps)
	G.726 (32 Kbps)
	CLEARMODE (RFC 4040)

Number of VoIP Channels Supported by a Submodule Depending on the Codec Type

Codec/packetisation time, ms	Number of channels	
	SMG-2/SMG-4 with SM-VP-M300 submodule	SMG-2 with SM-VP-M200 submodule
G.711 (A/U) / 20-60	128	104
G.711 (A/U) / 10	112	74
G.729 A / 20-80	72	48
G.729 A / 10	62	41
G.723.1 (6.3 Kbps, 5.3 Kbps)	58	39
G.726 / 20	98	65
G.726 / 10	88	59
T.38	54	36

Electrical Ethernet Interface Specifications

No. of interfaces	1
Electric port	RJ-45
Data transfer rate, Mbps	Auto detection, 10/100/1000 Mbps, duplex

Supported standards	10/100/1000BaseT

Console Parameters

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

E1 Interface Parameters

No. of interfaces	SMG-4	SMG-2
	4	1 or 2[2]
Electric port	RJ-48	
No. of channels	Acc. to ITU-T G.703 and G.704 guidelines	
Line data transfer rate	2,048 Mbps	
Line code	HDB3, AMI	
Output signal to the line	3.0 V peak for 120 Ω load 2.37 V peak for 75 Ω load (acc. to CCITT G.703 guidelines)	
Input signal from the line	from 0 to -6 dB in relation to the standard output impulse	
Elastic buffer	2 frame capacity	
Signalling protocol	ISDN PRI (Q.931), QSIG and CorNet to transmit user name, SS-7	

General Parameters

Operating temperature range	from +5°C to 40°C
Relative humidity	up to 80%
Power voltage	12 V DC, 2 A power adapter
Power consumption	not more than 10 W
Dimensions (W x H x D)	187x124x32
Net weight	0.3 kg
Gross weight	0.5 kg

---

[2] Only one E1 stream is available in an SMG-2 device by default. To activate another one, a special licence is required. For more information about licences, see section **4.1.19**. **Licence Renewal**

1.5   Design

SMG trunk gateway is enclosed in 187x124x32 mm plastic casing.

For external view of the device panels, see Fig. 6, 7a, and 7b.
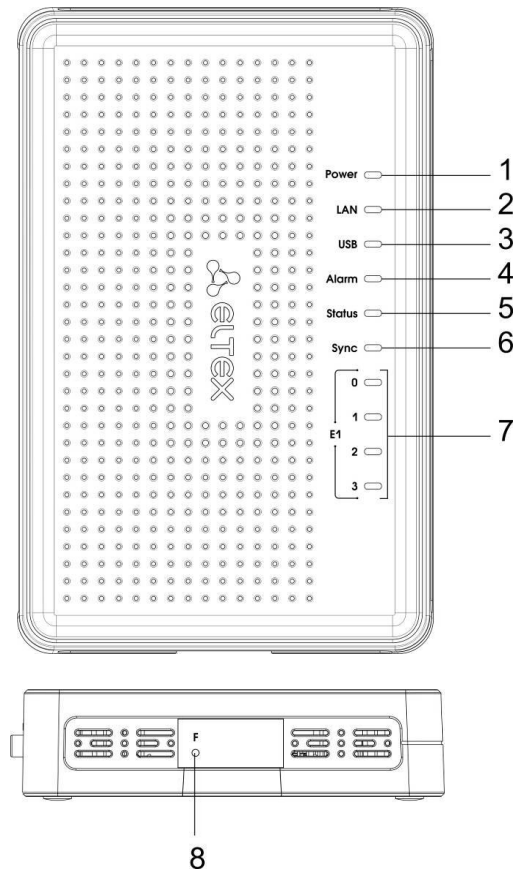
Fig. 1.7—SMG External View. Top and Side Panels
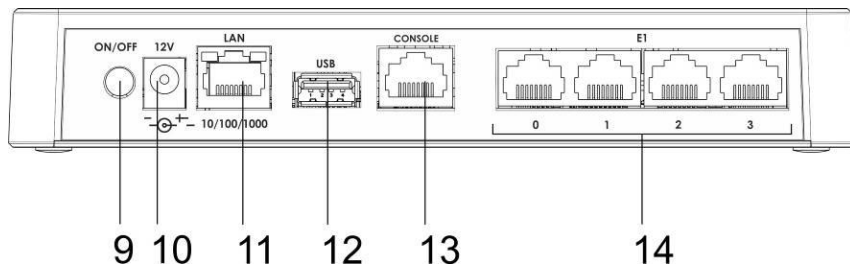
Fig. 1.8—SMG-4 External View. Rear Panel
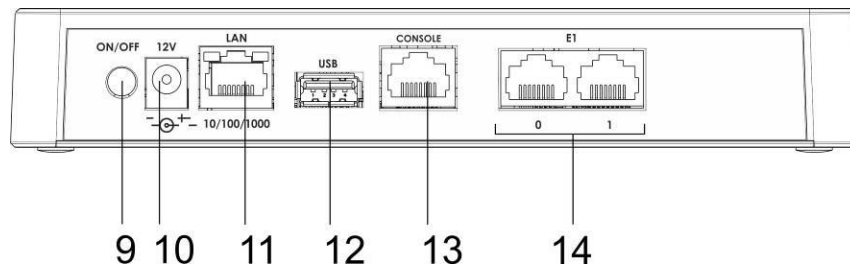
Fig. 1.9—SMG-2 External View. Rear Panel

For ports, LEDs, and controls located on the device, see Table 2.1.

Table 2.1—Description of Ports, LEDs, and Controls Located on the Front Panel

№	Panel Element	Description
Top panel. Operation indicators		
1	*Power*	Power indicator
2	*LAN*	Network activity indicator
3	*USB*	USB operation indicator
4	*Alarm*	Device critical failure indicator
5	*Status*	Device operation indicator
6	*Sync*	Synchronisation indicator
7	*E1 0..3*	E1 stream operation indicator; E1 2 and E1 3 LEDs are inactive for SMG-2
Side panel. Function button		
8	*F*	Function button
Rear panel. Ports and controls		
9	*ON/OFF*	On/off button
10	*12V*	Power socket (for connection to power line via the supplied adapter)
11	*LAN 10/100/1000*	1 RJ-45 port for Ethernet 10/100/1000 Base-T interface
12	*USB*	USB port for external storage device
13	*Console*	RJ-45 console port for local device administration (for connector wiring, see Appendix A)
14	*E1 0..3 (for SMG-4)*	4 x RJ-48 ports for E1 streams (for connector wiring, see Appendix A)
	E1 0..1 (for SMG-2)	2 x RJ-48 ports for E1 streams[3] (for connector wiring, see Appendix A)

1.6   LED Indication

The current status of the device is shown by the ***Power, LAN, USB, Alarm, Status, Sync, and E1*** indicators located on the top panel.

Indicator statuses are listed in Tables 3.1 and 3.2.

Table 3.1—LED Indication of the Device Status in Operation

LED	LED Status	Device Status
Power	Off	No power supply from 12 V adapter
	Solid green	12 V power supplied to the device
LAN	Off	Link lost
	Solid green / blinking green	Port is in the 10/100Base-TX mode
	Solid yellow / blinking yellow	Port is in the 1000Base-T mode
USB	Off	USB device is not connected
	Solid green	A high-speed USB device is connected
	Solid red	A low-speed USB device is connected
Alarm	Blinking red	Critical device failure

---

[3] Only one E1 stream is available in an SMG-2 device by default. To activate another one, a special licence is required. For more information about licences, see section **4.1.19**. **Licence Renewal**

	Solid red	Non-critical device failure
	Solid yellow	Non-critical warnings, no failures
	Solid green	Normal operation
Status	Solid green	Normal operation
	Off	Device power lost
Sync	Off	Synchronisation sources not defined
	Solid green	Synchronisation from source available
	Solid red	Synchronisation from source unavailable

Table 3.2—LED Indication During Device Startup and Reset to Factory Defaults

No.	LED			Reset to Factory Defaults (Device Is On)
	Sync	Alarm	Status	
1	Yellow	Yellow	Yellow	Press the *F* button and hold for 1 second until the following pattern appears, then release the button. The device reboot will start in 3 seconds.
2	Off	Off	Yellow	The device is powered on, the operating system is not loaded.
3	Off	Green	Green	The gateway operating system is being loaded. When the pattern appears, press the *F* button and hold it for 40–45 seconds to change network parameters and restore the device configuration to factory defaults.
4	Off	Yellow	Yellow	When the pattern appears, release the *F* button. After a while, the following message will be displayed in the console. <<<BOOTING IN SAFE-MODE.RESTORING DEFAULT PARAMETERS>>> Reset to factory defaults is complete.

> **The device can also be reset to factory defaults during startup.**
> **Skip step 1 in this case.**

Ethernet interface status is also shown by LED indicators built in the 1000/100 connector.

Table 3.3—LED Indication for Ethernet 1000/100 Interfaces

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

Table 3.4 shows E1 streams indication.

Table 3.4—E1 Indication

Stream Status	E1 Indicator		
	Red	Yellow	Green
E1 is disabled in the gateway configuration	Off	Off	Off
E1 stream failure	Blinking (200 ms)	Off	Off
Loss of signal (LoS)	On	Off	Off
AIS failure	Blinking (200 ms)	Blinking (200 ms)	Off
LOF failure	Blinking (200 ms)	Off	Off
LOMF failure	Blinking (200 ms)	Off	Off
E1 stream normal operation	Off	Off	On
Failure on a remote host (RAI)	Off	On	Off
E1 stream is in operation, the stream has slips	Off	Blinking (500 ms)	Blinking (500 ms)
E1 stream is being tested	Blinking (200 ms)	Off	Blinking (200 ms)

Table 3.5 provides a detailed description of the failures shown by the **Alarm** indicator.

✓ **Indication of CDR Files Saving**
When the FTP server is not available, CDRs will be saved to the device RAM. 30 MB are allocated for storing CDR files. If the memory is full up to a specified value, a fault will be indicated.

Table 3.5—Alarm Indication

Alarm LED Status	Fault Level	Fault Description
Blinking red	Critical failure	Configuration error
		Connection with SIP module lost
		SS-7 line group fault (when the *Fault indication* checkbox is checked in the *Routing/SS line groups* menu)
		E1 stream fault (when the *Alarm indication* checkbox is checked in the *E1 streams/Physical parameters* menu)
		FTP server is unavailable, RAM utilisation for storing CDR files exceeds 50% (15–30 MB)
		CPU temperature exceeds 100 ºC
		Less than 25 MB free RAM (5%)
		Free storage on a connected USB drive is less than - 5% of the total capacity (for drives with less than 5 GB storage), - 256 MB (for drives with more than 5 GB storage)
		Opposing SIP device does not respond to OPTIONS queries, when regular checks by OPTIONS messages are enabled
		setting up of semi-permanent connection over E1 channel failed
Solid red	Non-critical failure (errors)	SS-7 link fault (when the *Fault indication* checkbox is checked in the *Routing/SS line groups* menu)

		Synchronisation fault (free-run mode operation)
		FTP server is unavailable, RAM utilisation for storing CDR files is less than 50% (5–15 MB)
		No connection to one of the SM-VP-300 modules
		CPU temperature reached 90 ºC
		Less than 50 MB free RAM (10%)
		Free storage on a connected USB drive is less than - 10% of the total capacity (for drives with less than 5 GB storage), - 512 MB (for drives with more than 5 GB storage)
		CPU load is about or above 95% during the last 9 seconds
Solid yellow	Warnings	E1 stream remote fault
		E1 stream slipping
		Synchronisation from a lower priority source (a higher priority one is not available)
		FTP server is unavailable, RAM utilisation for storing CDR files is below 5 MB
		CPU temperature reached 85 ºC
		Less than 128 MB free RAM (25%)
		CPU load is about or above 90% during the last 9 seconds
		Free storage on a connected USB drive is less than - 15% of the total capacity (for drives with less than 5 GB storage), - 1,024 MB (for drives with more than 5 GB storage)

1.7   The *F* Function Button

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

For instructions on reset of an operating device to factory defaults, see Table 3.2.

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

    −   via telnet or console: login: **admin**, password: **rootpasswd**;
    −   via web interface: login: **admin**, password: **rootpasswd**.

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

Saving Factory Configuration

To save the factory configuration: connect via telnet or console using **admin** for login and **rootpasswd** for password; enter the *sh* command (the device will switch from the CLI mode to the SHELL mode), enter the *save* command, and restart using the *reboot* command. The gateway will be restarted with the factory configuration.

```
*******************************************
*        Welcome to SMG-4        *
*******************************************


smg login: admin
Password: rootpasswd


*******************************************
*        Welcome to SMG-4        *
*******************************************


Welcome! It is Thu Aug 21 11:40:40 GMT+6 2014
SMG4> sh
```

```
/home/admin # save
tar: removing leading '/' from member names
*Saved successful
New image 1
Restored successful
/home/admin # reboot
```

Password Recovery

To recover a password: connect via telnet, SSH, or console, enter the *sh* command (the device will switch from the CLI mode to the SHELL mode), enter the *restore* command (the current configuration will be restored), enter the *passwd* command (the device will request to enter and confirm a new password), enter the *save* command, and restart using the *reboot* command. The gateway will be restarted with the current configuration and the new password.

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

```
*****************************************
*          Welcome to SMG-4          *
*****************************************


smg login: admin
Password: rootpasswd


*****************************************
*          Welcome to SMG-4          *
*****************************************


Welcome! It is Thu Aug 21 11:40:40 GMT+6 2014
SMG4> sh
/home/admin # restore
Welcome! It is Fri Jul  2 12:57:56 UTC 2010
SMG4> sh
/home/admin # restore
New image 1
Restored successful
/home/admin # passwd admin
Changing password for admin
New password: 1q2w3e4r5t6y
Retype password: 1q2w3e4r5t6y
passwd: password for admin is changed
/home/admin # save
tar: removing leading '/' from member names
*Saved successful
New image 1
Restored successful
/home/admin # reboot
```

1.8   Delivery Package

SMG standard delivery package includes:

- SMG-2 or SMG-4 trunk gateway,
- power adapter,
- operation manual and documentation package.

1.9 Safety Instructions

1.9.1 General Guidelines

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

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

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

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

- The SMG trunk gateway can be used 24/7 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 x 10^4 to 10.7x10^4 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.

1.9.2 Electrical Safety Requirements

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

- Before dismantling and assembling the device, make sure the power supply is disabled.

2 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 the corresponding document, and contact your supplier.

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

2.1 Startup Procedure

1. Connect stream (E1) and Ethernet cables to corresponding gateway connectors.

2. Connect the power adaptor to the device.

3. Turn the device on and check the front panel LEDs to make sure the terminal is in normal operating conditions.

2.2 Opening the Casing

Prior to proceed, disable SMG power supply and disconnect all cables.
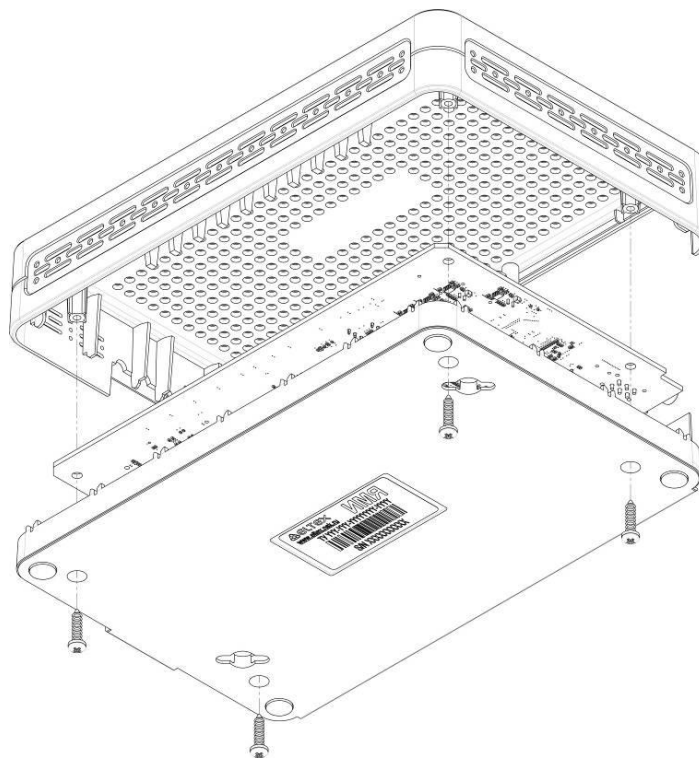
Fig. 2.1—Opening the Casing

1. Use a screwdriver to remove 4 screws holding the bottom panel of the device as shown in the figure.

2. Pull the top panel (cover) of the device to remove it.

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

2.3 RTC Battery Replacement

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

Battery type	Lithium
Form-factor	CR2032 (CR2024 option is possible)
Voltage	3 V
Capacity	225 mA
Diameter	20 mm
Thickness	3.2 mm
Battery life / expiration date	5 years
Storage conditions	-20 to +35 °C
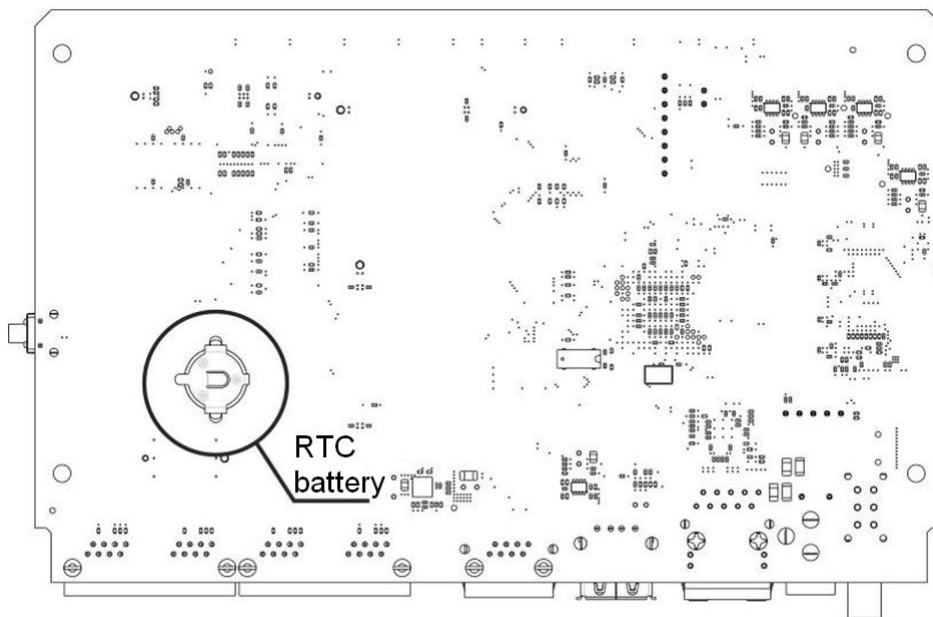
Fig. 2.2—Battery Location in RTC

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

1. Check if the device is energised.

2. If the voltage is present, disconnect the power supply.

3. Open the device casing (see section **2.2 Opening the Casing**).

4. Remove the exhausted battery from the reverse side of the plate (Fig. 17) and install a new one in the same position.

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

> **If NTP synchronisation is disabled, the system date and time will require adjustment after RTC battery replacement.**
> **Used batteries should be recycled according to requirements.**

3   GENERAL GUIDELINES FOR GATEWAY OPERATION

The easiest way to configure and monitor the device is to use the web interface, so it is highly recommended.

To prevent unauthorised access to the device, it is recommended to change the password for telnet and console access (default username: admin, password: rootpasswd) and the administrator password for the web interface. For information on password configuration for telnet and console access, see section **4.3.2 Changing Device Access Password via CLI**. For information on password configuration for web interface access, see section **4.1.21**. It is recommended to write down and store the configured passwords in a safe place, inaccessible for intruders.

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

4   DEVICE CONFIGURATION

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

> ✓ **All settings will take effect without gateway restart. To save configuration changes into the non-volatile memory, use the *Service/Save Configuration into Flash* menu in the web configurator or the COPY RUNNING_TO_STARTUP command in CLI.**
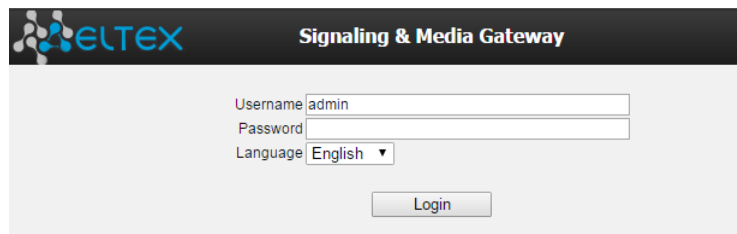
4.1   SMG Configuration via web Interface

To configure the device, establish a connection to the device in a *web browser* (hypertext document viewer), e. g. Firefox, Google Chrome. Enter the device IP address in the address bar of the web browser.

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

As soon as the IP address is entered, the device will request username and password.

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

Upon access to the web configurator, the *System Information* menu opens.

The figure below illustrates navigation in the web configurator.
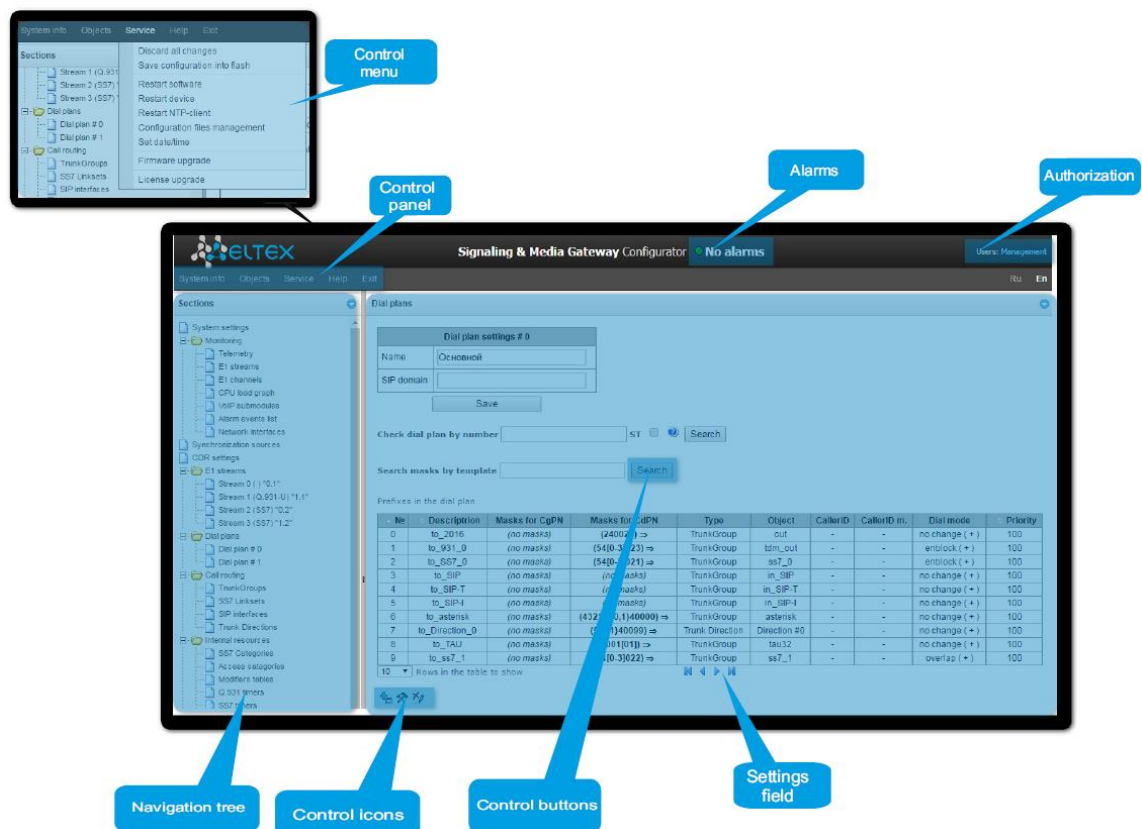
A window in user interface is divided into several areas.

Navigation tree – enables management of the settings field. The navigation tree represents a hierarchy of management sections and nested menus.

Settings field – is defined by user selections. Allows user to view device settings and enter configuration data.

Control panel – a panel to control the settings field and firmware status.

Control menu – drop-down menus in the control panel for the settings field and firmware status.

Alarms – displays the current highest-priority fault and serves as a link to work with the fault events log.

Authorisation – a link to work with passwords, which are used to access the device via web interface.

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

        – *Add Object;*

        — *Edit Object;*

        — *Remove Object;*

        — *View Object.*

Control buttons – controls to work with the settings field.

To prevent unauthorised access to the device during further work, it's recommended to change the password (see section **4.1.21**).

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

4.1.1 System Parameters

System Settings

- *Device name (for web pages only)*—the device name used in the heading of the web configurator.
- *Active dial plan count* —the quantity of simultaneously active numbering schedules; up to 16 independent numbering schedules can be configured with a possibility to add subscribers and create a customised call routing table.

Alarm Indication

- *CPU load* —when checked, the control system will be alerted about high CPU utilisation.
- *RAM usage*—when checked, the control system will be alerted when running out of free RAM.
- *Local disk drive free space*—when checked, the control system will be alerted when running out of free memory on an external drive.

Auto configuration (Automatic Configuration)

- *Active auto-update*—enables automatic updates of firmware and configuration.
- *Source*—a method to receive parameters for automatic updates:
    - *Static*—use automatic update parameters set in the configuration;
    - *DHCP*—select a network interface with the configured DHCP protocol, which will be used to retrieve Options 66 and 67 for automatic updates.

- *Protocol*—a protocol, which will be used for automatic updates (TFTP/FTP/HTTP/HTTPS).
- *Authentication*—setting the flag enables authentication during automatic updates via the selected protocol (FTP/HTTP/HTTPS).
- *Name*—a login to access the automatic update server.
- *Password*—a password to access the automatic update server.
- *Server*—IP address or network name of the automatic update server when the *static* source is selected; *update.local* name is used by default.
- *Update configuration*—specifies to use automatic configuration updates.
- *Configuration file name*—name and path to the configuration file located on the automatic update server; *MAC.cfg* by default, where *MAC* is the MAC address of the device in the xx.xx.xx.xx.xx.xx format.
- *Configuration upgrade period, min*—time interval in minutes between requests for a configuration file sent to the automatic update server.
- *Software update*—enables automatic firmware updates.
- *Software version file name*—name of the manifest file on the automatic update server that contains a description of the firmware version, a path to the firmware file, and time of firmware update.
- *Software upgrade period, min*—time interval in minutes between requests for a manifest file on the automatic update server.

4.1.1.1 Format of Options 66 and 67

Option 66 is required to retrieve the IP address or domain name of the automatic update server.

Syntax:

"<IP address or domain name of the update server>"

Example:

"update.local"

or

"192.168.1.3"

Option 67 is required to retrieve the path to the file with firmware version description (the manifest file) and the path to the configuration file.

Syntax:

"<Path to smg4.manifest (or smg2.manifest) file>;<Path and name of the configuration file>"

Example:

"/smg4/firmware/smg4.manifest;/smg4/conf/<MAC>.cfg"

"/smg2/firmware/smg2.manifest;/smg2/conf/<MAC>.cfg"

If a device receives a configuration file name in the format "*<MAC>.cfg*" from the server, it automatically replaces *<MAC>* with its own MAC address in the format *11.22.33.44.55.66* when addressing the server. This means that the server should contain a configuration file named *11.22.33.44.55.66.cfg*.

Instead of using the expression "*<MAC>.cfg*", the server may send the configuration file name in the following format*: 11.22.33.44.55.66.cfg*, where *11:22:33:44:55:66* is the factory MAC address of the device.

If no Options 66 and 67 are received from the DHCP server, their default values will be used.

For **Option 66**: "update.local".

For **Option 67**: "smg4.manifest;<MAC>.cfg";

"smg2.manifest;<MAC>.cfg".

4.1.1.2 smg4.manifest (smg2.manifest) File Format

smg4.manifest (smg2.manifest) is a text file containing information about the version and the path to the firmware file located on the automatic update server, as well as the time to restart the device after firmware update to a new version.

General format of the file content:

<firmware version>;<path to firmware file>; <time (in hours)>

The *<firmware version>* and *<path to firmware file>* parameters are mandatory. The *<Time>* parameter is optional. If it is not specified, the device will restart as soon as there are no conversation sessions.

Example of a file with time set:
3.1.1.1076;smg4/smg4_firmware_3.1.1.1076.bin;18-21

Example of a file without time set:
3.1.1.1076;smg4/smg4_firmware_3.1.1.1076.bin

4.1.1.3 Algorithm of Automatic Configuration Loading and Checking for a New Configuration File

This procedure is used for automatic download of a new device configuration file from the server. The configuration file contains the date and time of its creation:

```
SMG-config:
 Version: 13
LastUpdate:
 ID: 1
Date: 2015-03-30
Time: 05:59:28
```

While loading, SMG checks for a configuration file in the specified location on the FTP/TFTP/HTTP/HTTPS sever (and authorises on the server if necessary). If it finds the configuration file, the gateway downloads it and compares the creation date and time of the current file and the downloaded one's. If the downloaded file is created later, the device saves and applies the new configuration. Otherwise, the current configuration remains valid.

Thus, to change the gateway configuration, operator simply needs to upload a new configuration file to the server with necessary adjustments and new date and time of creation. The configuration will be updated automatically after the time set in the *Configuration update period* parameter.

```
┌─────────────────────────┐
│      SMG loading        │
└─────────────────────────┘

┌─────────────────────────┐
│      Start timer        │
│ configuration update    │
│      interval           │
└─────────────────────────┘
        │ timer expired
        ▼
┌─────────────────────────┐
│ Download configuration  │
│   file from server      │
└─────────────────────────┘
        │
        ▼
    ◇ Data and time are later ◇ ── No
        │
        │ Yes
        ▼
┌─────────────────────────┐
│ Apply downloaded        │
│   configuration         │
└─────────────────────────┘
```
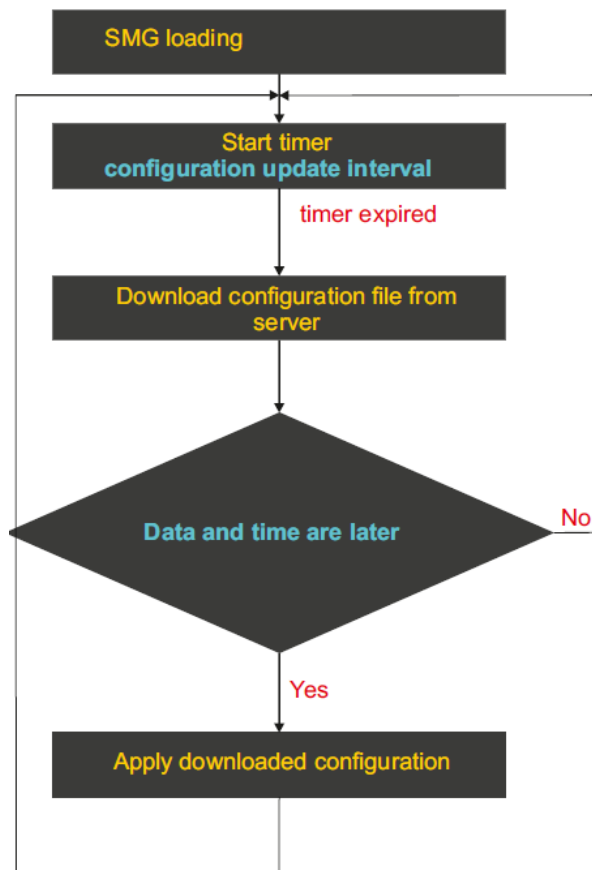
4.1.1.4 Algorithm of Automatic Software Updating and Checking for New Firmware Versions

During SMG loading or after the time set in *Firmware update period* elapses, the gateway checks for a version description file (smg4.manifest/smg2.manifest) in the specified location on the server. If the file is found, SMG downloads it. The file contains information on firmware file versions available on the server, their locations and names, as well as (optional) the time period before device restart after update. If firmware versions on the server differ from the current ones on the gateway, the device checks for active conversation sessions. If there are none, the gateway downloads the firmware image specified in the *smg4.manifest/smg2.manifest* file and updates the firmware. After the firmware update, the gateway checks for active voice sessions and restarts if finds none. Otherwise, a 30 seconds timer starts. When the time runs out, the gateway checks for active conversation sessions again. If the manifest file specifies a time period for restart, a timer starts for this period. For example, if the file specifies 18–21, the device waits till 18:00 to check for active voice sessions. If it finds none, the gateway restarts; otherwise, the 30 seconds timer starts. When the time runs out, the gateway checks for active conversation sessions again.
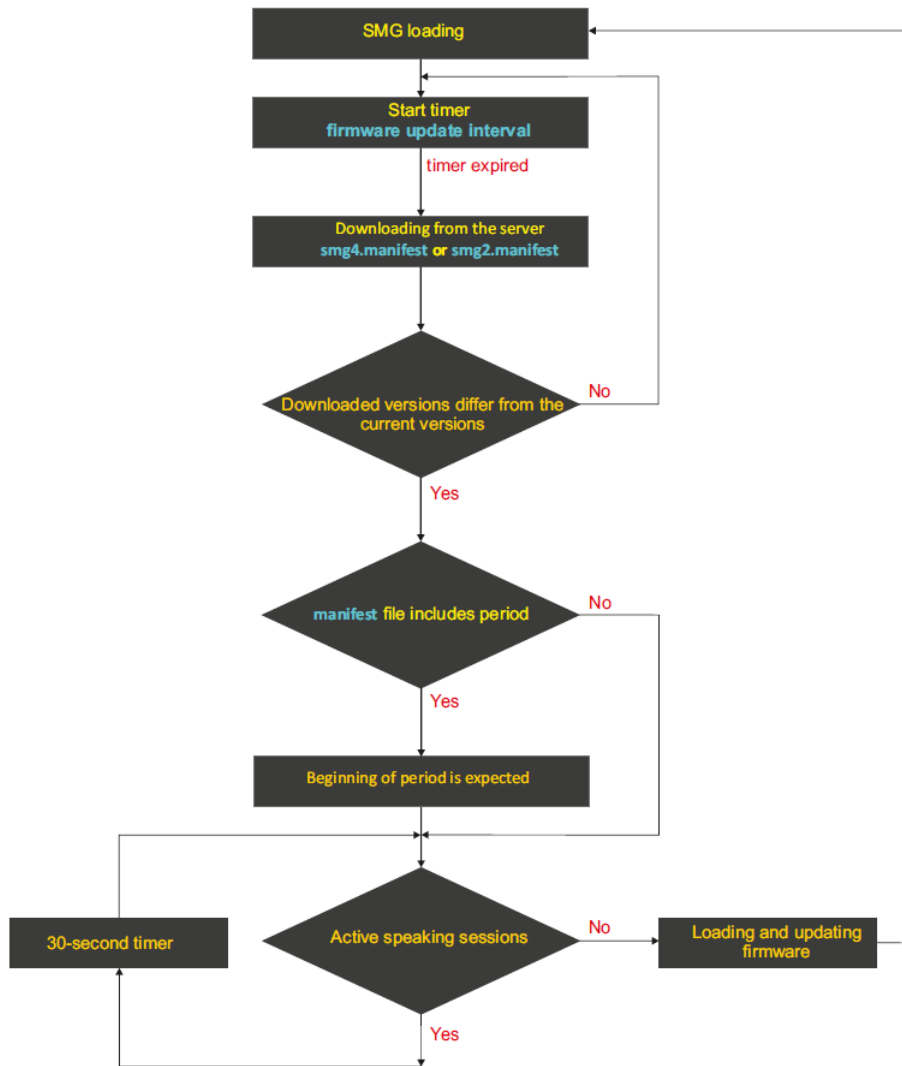
4.1.2 Monitoring

4.1.2.1 Telemetrics

This section contains information on the temperature sensors and CPU utilisation.

Temperature sensors

- *TempSensor #0*—CPU temperature.
- *TempSensor #1*—switch temperature.

Current CPU Utilisation

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

4.1.2.2 E1 Stream Monitoring

This section[4] contains information on the chip installed in the M4E1 submodule, as well as on E1 stream monitoring and statistics.

E1 streams

M4E1 submodule info: QFALC_v3.1, ID=0x20

Stream number	0	1	2	3
State	🟢 WORK	🟢 WORK	🟢 WORK	🟢 WORK
D-channel state	up	up	up	up
Statistics collection time, sec	3386	3386	3386	3386
Slip up	0	0	0	0
Slip down	2	2	5	2
RX bytes	2707	2707	8363	8561
TX bytes	2707	2707	38264	38276
Short packets	0	0	0	0
Big packets	0	0	0	0
RX Overflow	0	0	0	0
CRC errors	0	0	0	0
TX underrun	0	0	0	0
Code violation counter	4	0	0	0
CRC Error Counter / PRBS	0	0	0	0
Bit error rate	0	2	0	0
Select ☐	☐	☐	☐	☐

[Reset counters] [Remote Loop] [PRBS test] [PRBS test with Local Loop] [Stop test]

- *M4E1 Submodule Info*—information about chip name and identifier.

Stream Parameters

- State—stream status:
    - *WORK*—stream in operation;
    - *LOS*—signal lost;
    - *OFF*—stream is disabled in configuration;
    - *NONE*—submodule not installed;
    - *AIS*—alarm state indication signal (signal that contains all units);
    - *LOMF*—multi-frame alarm state indication signal;
    - *RAI*—remote alarm indication;
    - *D channel status*—status 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.

- D-channel state - state of D channel, service management channel
    - *up*- D-channel is in operation
    - *down* - D-channel is not in operation
    - *no*- there is no management channel for the stream
    - *off* - signalling is disabled for the stream

- *Statistics collection time, sec*—time for statistics collection in seconds.

---

[4] Only one E1 stream is available in an SMG-2 device by default. To activate another one, a special licence is required. For more information about licences, see section **4.1.19**. **Licence Renewal**

- *Slip up*—number of positive bit slips for the stream.

- *Slip down*—number of negative bit slips for the stream.

- *RX bytes*—number of bytes received from the stream.

- *TX bytes*—number of bytes sent to the stream.

- *Short packets*—number of received packets of a smaller size than the standard one.

- *Big packets*—number of received packets of a larger size than the standard one.

- *RX Overflow*—buffer overrun error counter.

- *CRC errors*—CRC error counter.

- *TX underrun*—stream transmission failure counter.

- *Code violations counter*—signal code sequence failure counter.

- *CRC Error Counter / PRBS*—number of CRC errors (in the *PRBS test* mode).

- *Bit error rate*—number of bit errors for the stream.

- *Select*—when checked, clicking the *Reset Counters* button will clear the collected statistics.

- *Remote loop*—E1 path test mode, where the signal received by the unit from the connected E1 stream is transmitted directly in the same stream.

- *PRBS test*—enables pseudorandom sequence output to the output port of the unit (transmitted into the connected E1 stream); at that, the 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. The number of errors and analysis time counter will be displayed in the stream information window.

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

- *Stop test*—disables the test mode.

4.1.2.3 E1 Channel Monitoring

This section[5] contains information on E1 stream channel status.

---

[5] Only one E1 stream is available in an SMG-2 device by default. To activate another one, a special licence is required. For more information about licences, see section **4.1.19**. **Licence Renewal**

SMG digital gateway

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	○	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	○	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎
🟢 Stream 1	○	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	○	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎
🟢 Stream 2	○	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	○	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎
🟢 Stream 3	○	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	○	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎

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

Streams state		Channels state	
✖	NONE	○	Off
⚪	OFF	◎	Idle
🔴	ALARM	🔴	Block
🔴	LOS	📞	Incoming dialing
🔴	AIS	➡	Outgoing dialing
🔴	LOF	📞	Incoming alerting
🔴	LOMF	📞	Outgoing alerting
🟡	WORK/RAI	📞	Busy, Release
🔵	WORK/SLIP	📞	Talk, Hold
🟢	WORK	⌛	Waiting
✖	TEST		

Stream State

State—stream status:

- *NONE*—M4E1 submodule is missing;
- *OFF*—stream is disabled in configuration;
- *ALARM*—M4E1 submodule initialisation error;
- *LOS*—signal lost;
- *AIS*—alarm state indication signal (signal that contains all units);
- *LOF*—loss of frame;
- *LOMF*—multi-frame alarm state indication signal;
- *WORK/RAI*—remote alarm indication;
- *WORK/SLIP*—SLIP indication for the stream;
- *WORK*—stream in operation;
- *TEST*—stream test indication (PRBS test, local or remote loop).

Channel State

State—channel status:

- *OFF*—channel is disabled in configuration;
- *Idle*—channel is in initial state;
- *Block*—port is blocked;
- *Incoming dialing*—incoming call dialling;
- *Outgoing dialing*—outgoing call dialling;
- *Incoming alerting*—incoming engagement, callee is disengaged;
- *Outgoing alerting*—outgoing engagement, callee is disengaged;
- *Busy, Release*—channel release, sending the *busy* tone;
- *Talk, Hold*—channel is in the call state, on hold;

- *Waiting*—waiting for response from the opposite party (waiting for engagement acknowledgement, waiting for Caller ID, waiting for call dialling).

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 #: PRI/SS7 channel # or VoIP submodule #: VoIP channel #.

- *Connected Callref*—call identifier for the linked channel.

- *State*—channel status:
    - *Off*—channel is disabled;
    - *Block*—port is blocked;
    - *Init*—channel initialisation;
    - *Idle*—channel is in initial state;
    - *In-Dial/Out-Dial*—incoming/outgoing call dial;
    - *In-Call/Out-Call*—incoming or outgoing engagement;
    - *In-Busy/Out-Busy*—sending the *busy* tone;
    - *Talk*—channel is in call state;
    - *Release*—channel release;
    - *Wait-Ack*—waiting for acknowledgement;
    - *Wait-CID*—waiting for CgPN (Caller ID);
    - *Wait-Num*—waiting for call dial;
    - *Hold*—subscriber is on hold.

- *State timer*—channel last known status duration.

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

- *Incoming CdPN*—callee number before modification.

- *Incoming CgPN*—caller number before modification.

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

- *Outgoing CdPN*—callee number after modification.

- *Outgoing CgPN*—caller number after modification.

    Channel status updates every 5 seconds.

4.1.2.4 CPU Utilisation Chart

This section contains information on CPU utilisation in real time (10-minute interval). Statistics charts are based on average data for each 3-second device operation interval.
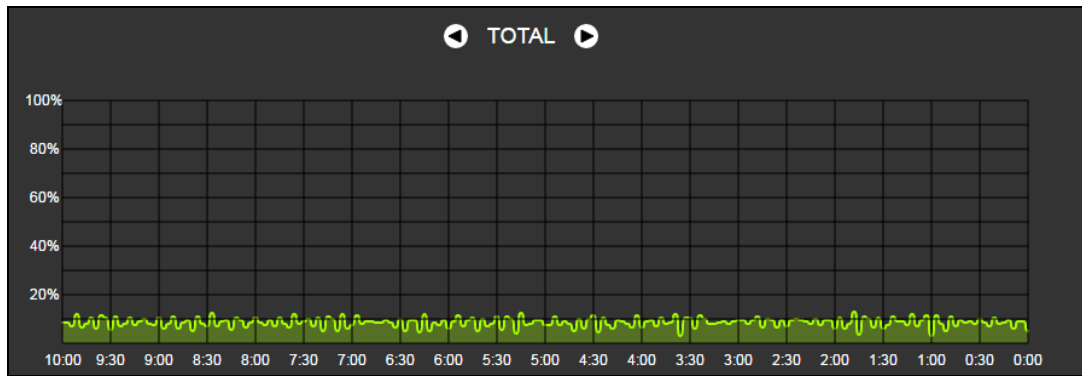
To navigate between specific parameters in monitoring charts, use the ◀ and ▶ buttons. To enhance visual identification, all charts have different colours.

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

4.1.2.5 VoIP Submodule Monitoring

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

- *No*—SM-VP submodule serial number (SMG allows installation of only one VoIP submodule).
- *Type*—installed submodule type.
- State:
  - *Not Present*—not installed;
  - *No init*—not initialised, no initialisation attempts;
  - *Off*—disabled, starting to load submodule;
  - *Wait Ack*—waiting for acknowledgement from CPU after submodule loading;
  - *Failed*—no response from submodule;
  - *Work*—submodule is in normal operation;
  - *Recovery*—no control packets coming from submodule;
- *Active count*—the number of submodule active connections at the given moment;
- Payload—percentage of submodule resource utilisation at the given moment.

To monitor the status of channels, select a submodule in the table and press the *Channel Monitoring* button.

VoIP submodules

VoIP submodule channels monitoring #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

Channel info #		Call IP-info #		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	-				

Cancel

Channel Connection Information

- *Port/channel*—port/channel data:
  - signalling protocol (VoIP);
  - port location: VoIP submodule #: channel #.

- *Callref*—call identifier.

- *Connected port/channel*— data on the linked port/channel:
  - 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 the linked channel.

- *State*—channel status:
  - *Off*—channel is disabled;
  - *Block*—port is blocked;
  - *Init*—channel initialisation;
  - *Idle*—channel is in initial state;
  - In-Dial/Out-Dial—incoming/outgoing call dial;
  - *In-Call/Out-Call*—incoming or outgoing engagement;
  - *In-Busy/Out-Busy*—sending the *busy* tone;
  - *Talk*—channel is in call state;
  - *Release*—channel release;
  - *Wait-Ack*—waiting for acknowledgement;
  - *Wait-CID*—waiting for CgPN (Caller ID);
  - *Wait-Num*—waiting for call dial;
  - *Hold*—subscriber is on hold;

- *State timer*—channel last known status duration.

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

- *Incoming CdPN* —callee number before modification.

- *Incoming CgPN* —caller number before modification.

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

- *Outgoing CdPN* —callee number after modification.

- *Outgoing CgPN* —caller number after modification.

Channel States

- *Idle (grey)*—initial state, the channel is ready to serve a call.
- *Active (green)*—active state, the channel is engaged with an active call.
- *Reserved (yellow)*—the channel is reserved for service needs (sending the *busy*, *ringback*, *PBX response* tones) or for a new call. Channels cannot be reserved in SGM.

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

Information on Channel IP Connection

- *State*—channel state (see description above).
- *Codec*—codec used (Payload Type is specified in square brackets).
- *Status*—media information transmission status:
  – *Good*—channel in operation;
  – *Loss of RTP*—loss of the opposite RTP stream (when the time in *RTP packet timeout* expires);
  – *VBD*—communication is established through the channel in the data transmission mode;
  – *T38*—fax connection using the T.38 protocol is established through the channel.
- *Mode*—media channel operation mode:
  – *sendrecv*—channel operates in the duplex mode (receipt and transmission);
  – *sendonly*—channel operates in the simplex mode, transmission only;
  – *recvonly*—channel operates in the simplex mode, receipt only;
  – *inactive*—channel is not active, receipt and transmission are inactive.
- *SSRC*—the *SSRC* (Synchronisation Source) field value for the RTP stream outgoing from the device.
- *IP:port remote*—remote IP address and port of the RTP stream source.
- *IP:port local*—local IP address and port of the RTP stream source.
- *MAC remote*—remote MAC address of the RTP stream source.
- *MAC local*—local MAC address of the RTP stream source.

4.1.2.6 Alarm log

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

When there are no alarms, the message *"No alarms"* will be displayed.
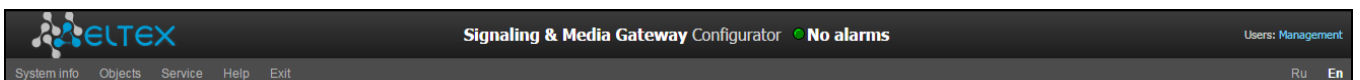
Alarm Message Examples

Alarm Message	Meaning
Configuration has not been read	Configuration file error
No communication with SIP module	Failure of a software module responsible for VoIP operation
No communication with VoIP submodule #	SM-VP-300 submodule failure
SS-7 line group (linkset) No. is not in operation	SS-7 line group failure

E1 stream # failure	E1 stream failure
SS-7 link failure Link set #, E1 stream #	SS-7 link failure
Synchronisation with a local source. All specified sources are inoperable	Synchronisation source is lost
E1 stream # remote fault	E1 stream remote fault
Synchronisation from a lower priority source	Primary synchronisation source is lost, the priority of the current source is lower
Failed to send CDR files via FTP	Failure to send a CDR file to FTP server
Running out of operating memory	One of RAM utilisation limits has been reached
High CPU temperature	One of CPU temperature limits has been reached
High CPU utilisation	One of CPU utilisation limits has been reached
Transit over E1 stream	setting up of semi-permanent connection over E1 channel failed

The *Alarm events list* menu contains a list of alarm events arranged by time and date.

Alarm events list

Clear | Clear the alarm events list

№	Time	Date	Type	State	Parameters
11	10:05:42	05/10/16	SIPT-MODULE	OK	SIP-module connection error
10	10:05:41	05/10/16	High CPU load	OK	
9	10:05:39	05/10/16	LINKSET	OK	SS7 Linkset 1 failed
8	10:05:39	05/10/16	SS7LINK	OK	SS7 link alarm. Linkset 3, E1 stream 1
7	10:05:39	05/10/16	LINKSET	OK	SS7 Linkset 0 failed
6	10:05:39	05/10/16	SS7LINK	OK	SS7 link alarm. Linkset 2, E1 stream 0
5	10:05:37	05/10/16	SM-VP DEVICE	OK	VoIP-submodule 0 connection error
4	10:05:29	05/10/16	High CPU load	Alarm	
3	10:05:29	05/10/16	SIPT-MODULE	Critical alarm	SIP-module connection error
2	10:05:29	05/10/16	Configuration is not read	OK	
1	10:05:29	05/10/16	Software start V.3.1.04.1139	OK	
0	10:05:26	05/10/16	Configuration is not read	Critical alarm	

Alarm Table

- *Clear*—delete the existing fault events table.

- *№*—fault sequential number.

- *Time*—fault occurrence time (HH:MM:SS).

- *Date*—fault occurrence date (DD/MM/YY).

- *Type*—a fault type:

    – *CONFIG*—a critical fault, a configuration file fault;
    – *SIPT-MODULE*—a critical fault, a failure of a program module responsible for VoIP operation;
    – *LINKSET*—a critical fault, an SS-7 line group is not in operation;
    – *STREAM*—a critical fault, an E1 stream is not in operation;
    – *SM-VP DEVICE*—a fault, a SM-VP module failure;
    – *SS7 LINK*—an SS-7 signal channel failure;
    – *SYNC*—a synchronisation fault, a synchronisation source is missing;
    – *STREAM-REMOTE*—a warning, a remote fault of an E1 stream;
    – *CDR-FTP*—a fault or a warning, a failure to send a CDR file to the FTP server.
    – *TRANSIT* – critical alarm, setting up of semi-permanent connection over E1 channel failed.

- *State*—a fault state status:

- *critical alarm, LED blinking red*—the fault requires immediate intervention of the service personnel and affects device operation and provisioning of communication services;

- *alarm, red LED*—non-critical fault, intervention of the service personnel is also required;

- *warning, yellow LED*—the fault does not affect provisioning of communication services;

- *OK, green LED*—the fault is resolved.

- *Parameters*—detailed fault description.

4.1.2.7 Interface Monitoring

This section describes status monitoring for network interfaces and turning VPN/PPTP interfaces on and off.

Network interfaces

№	Ethernet	Network name	VLAN ID	DHCP	IP address	Broadcast	Network mask
0	eth0	eth0	-	-	192.168.1.4	192.168.1.255	255.255.255.0
1	eth0:1	alt_control	-	-	192.168.0.4	192.168.0.255	255.255.255.0
2	eth0.609	vlan	609	+	192.168.69.104	192.168.69.255	255.255.255.0

VPN/pptp interfaces

№	PPP-interface	Network name	PPTPD IP	Username	IP address	P-t-P	Network mask

4.1.3 Synchronisation Sources

To synchronise the device with multiple sources, a priority list algorithm has been implemented. The algorithm is as follows: when a sync signal from the current source is lost, the system looks through the list to find active signals from lower priority sources. When a higher priority signal is restored, the system switches to that signal. Also, there may be multiple sources of the same priority. When a signal of the same priority is restored, the system does not switch to that signal.

Up to 4 synchronisation sources are supported (from any of the 4 E1 streams).

To generate the list, use the following buttons:

—Add Source; —Remove.

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

- *Signal loss timeout, sec*—time interval when the system does not switch to a lower priority synchronisation source in case of a signal loss. If the signal is restored during this interval, the system will not switch to a lower priority source.

- *Signal presence timeout, sec*—time interval when the restored higher priority synchronisation signal should be active for the system to switch to that signal.

If the PRI protocol is configured for the stream, from which the synchronisation signal is received, then the PRI protocol should also be enabled for the connected stream at the other side. Otherwise, the synchronisation signal will not be received from the stream, which will cause slips.

4.1.4 CDR

This section describes parameters configuration to save call detail records.

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

CDR Saving Parameters

- *Enable CDR*—when checked, the gateway will generate CDRs.
- *Saving period: Days, Hours, Minutes*—time period for CDR generation and saving in the device RAM.
- *Add header*—when checked, the following header will be written at the beginning of the CDR file: SMG4. 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.

FTP server settings

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

Settings of Redundant FTP Server

- *Save files on FTP*—when checked, CDRs will be transferred to a redundant FTP server.
- *Server address/hostname*—IP address of the redundant FTP server.
- *Server port*—TCP port of the redundant FTP server.
- *Path on server*—a path to the redundant FTP server directory to store CDRs.
- *Login*—username for access to the redundant FTP server.
- Password—user password for access to the redundant FTP server.

✓ **When the FTP server is not available, CDRs will be saved to the device RAM. 30 MB are allocated for storing CDR files. If the memory is full up to a specified value, a fault will be indicated. For CDR file saving indication, see section 1.6 LED Indication.**

✓ **When a certain alarm level is reached, the system sends the corresponding SNMP trap.**

Other Settings

- *Save unsuccessful calls*—when checked, stores unsuccessful calls (not resulted in conversation) into CDR files.
- *Save empty files*—when checked, saves CDR files containing no records.
- *Write redirecting number*—when checked, an additional field, *Redirecting Number,* is added to CDR; otherwise, the additional *Redirecting Number* field will not be added when a call is redirected, and the number which originated the redirection will be saved into the *Calling Party Number* parameter.
- *Write redirecting mark*—when checked, CDR will contain an additional field, *Redirection Tag*.
- *Write call category*—when checked, CDR will contain an additional field, *Calling Party Category*.

Modifiers for incoming numbers

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

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

Modifiers for outgoing numbers

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

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

4.1.4.1 CDR Format

- A general header for an entire CDR file (this parameter is displayed, if the corresponding setting is selected).
- A discriminant (this parameter is displayed, if the corresponding setting is selected).
- Connection establishment time in the YYYY-MM-DD hh:mm:ss format (in case of unsuccessful calls, this parameter is equal to the disconnection time).
- Call duration, seconds.
- Cause of disconnection according to ITU-T Q.850.
- Connection information.
- Caller information:
  - IP address;
  - source type;
  - subscriber/trunk name (TG).
- Caller number on input.
- Caller number on output.
- Caller category on input.
- Caller category on output.
- Redirecting number (this parameter is displayed, if the corresponding setting is selected).
- Callee information:
  - IP address;
  - destination type;
  - subscriber/trunk name (TG).
- Callee number on input.
- Callee number on output.
- Call received time in the format: YYYY-MM-DD hh:mm:ss.
- Connection termination time in the format: YYYY-MM-DD hh:mm:ss.
- Redirection tag (this parameter is displayed, if the corresponding setting is selected).

Source and Destination Types

- *SIP-user*—SIP subscriber;
- *trunk-SIP*—SIP trunk;
- *trunk-SS7*—SS-7 trunk;

- *trunk-Q931*—ISDN PRI trunk.

Types of Connection Information

- *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;
- *end point equipment out of order*—unsuccessful call, the terminal equipment is not available;
- *unavailable trunk line*—unsuccessful call, the trunk is not available;
- *unavailable v-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;
- *other cause*—unsuccessful call, another reason.

Redirection Tag

- *normal*—a call w/o redirection;
- *redirecting*—a redirected call (a call containing the redirecting number after the redirection);
- *redirected*—the received call that was redirected.

4.1.4.2 CDR File Example

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

SMG4. CDR. File started at '20111024093328'

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

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

4.1.4.3 CDR Structure for Various Settings

By default, a CDR on SMG (checkboxes in *Other Settings* are not checked) contains rows of the following format:

;2013-10-08 15:10:14;2;16;user answer;0.0.0.0;trunk-SS7;TrunkGroup00;650000;650000;0.0.0.0;trunk-SS7;TrunkGroup00;80123456789;80123456789;2013-10-08 15:10:12;2013-10-08 15:10:16;

where

2013-10-08—call start date;
15:10:14—call start time;
2—call duration (in seconds);
16—cause of disconnection according to ITU-T Q.850;
user answer—connection information;
0.0.0.0—IP address where the call originates from (a call from TDM appears as 0.0.0.0);
trunk-SS7—source type;

TrunkGroup00—caller name or incoming trunk name (TG);
650000—caller name on SMG input (before modification on incoming TG);
650000—caller name on SMG output (after modification on incoming and outgoing TG);
0.0.0.0—IP address where the call is directed to (a call to TDM appears as 0.0.0.0);
trunk-SS7—destination type;
TrunkGroup00—callee name or outgoing trunk name (TG);
80123456789—callee number on SMG input (before modification on incoming TG);
80123456789—callee number on SMG output (after modification on incoming and outgoing TG);
2013-10-08 15:10:12—call received time;
2013-10-08 15:10:16—connection termination time.

The caller number will have the following format:

- For normal calls—the number from the *Calling Party Number* field (the PRI and SS-7 protocols) or the *From* field (SIP).

- When an IAM (the SS7 protocol) or SETUP (the PRI protocol) message received with redirection information—the number from the *Redirecting Number* field.

- When message 302 (the SIP protocol) is received—the number from the *To* field.

The callee number will have the following format:

- For normal calls—the number from the *Called Party Number* field (the PRI and SS-7 protocols) or the *To* field (SIP).

- When an IAM (the SS7 protocol) or SETUP (the PRI protocol) message received with redirection information—the number from the *Called Party Number* field.

- When message 302 (the SIP protocol) is received—the number from the *Contact* field.

When the **Save Call Category** checkbox is checked, two additional fields are added to this record:

2013-10-08   15:10:14;2;16;user   answer;0.0.0.0;trunk-SS7;TrunkGroup00;650000;650000;**1;3;**0.0.0.0;trunk-SS7;TrunkGroup00;80123456789;80123456789;2013-10-08 15:10:12;2013-10-08 15:10:16;

where

1—caller category on input (before modification on incoming TG);
3—caller category on output (after modification on incoming and outgoing TG).

When the **Save Redirecting Number** checkbox is checked, two additional fields are added:

;2013-10-08 18:27:13;1;16;user answer;0.0.0.0;trunk-SS7;TrunkGroup00;650000;37650000;1;1;**650016;3835650016;**0.0.0.0;trunk-SS7;TrunkGroup00;80123456789;58123456789;2013-10-08 18:27:09;2013-10-08 18:27:14;

where

650016—the redirecting number (the number that originated the redirection) on SMG input (before modification on incoming TG)—the number from the *Redirecting Number* field (the PRI and SS-7 protocols) or the *To* field (SIP).
3835650016—the redirecting number on SMG output (after modification on incoming and outgoing TG)—the number from the *Redirecting Number* field (the PRI and SS-7 protocols) or the *To* field (SIP).

In this case, the number from the *Calling Party Number* field (the PRI and SS-7 protocols) or the *From* field (SIP) will be specified as a caller number.

SMG digital gateway

- When an IAM (the SS7 protocol) or SETUP (the PRI protocol) message received with redirection information—the number from the *Redirecting Number* field.
- When message 302 (the SIP protocol) is received—the number from the *To* field.

When the **Save Redirection Tag** checkbox is checked, the following field is added for redirected calls:

;2013-10-09 17:58:26;5;16;user answer;192.168.0.2;trunk-SIP;TrunkGroup01;650000;650000;1;1;001;001;0.0.0.0;trunk-SS7;TrunkGroup00;650023;650023;2013-10-09 17:58:24;2013-10-09 17:58:31;**redirecting**;

where

redirecting—a redirection tag.

The redirection tag may have the following values:

- *redirecting*—the caller has redirected the call to the callee;
- *redirected*—the call initiated by the caller has been redirected to another subscriber.

4.1.5 E1 Streams

This section[6] describes configuration of signalling and parameters for each E1 stream.

4.1.5.1 Signalling Protocol Selection

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

The device supports the following signalling protocols:

- Q.931 (User, Network);
- SS7 (OKC-7);
- QSIG for subscriber name transmission;
- CorNet for subscriber name transmission.

4.1.5.2 Configuration of Physical Parameters

Physical settings

- *Enable*—the stream is physically enabled.
- *CRC4 xmit/control*—CRC4 checksum is generated during transmission and checked during reception.
- *Equalizer*—when checked, amplifies the transmitted signal.
- *Alarm indication*—when checked, a local stream fault results in fault indication (the ALARM LED turns on and the alarm is registered in the alarm log).
- *Remote alarm indication*—when checked, a remote stream fault results in fault indication (the

---

[6] Only one E1 stream is available in an SMG-2 device by default. To activate another one, a special licence is required. For more information about licences, see section **4.1.19 Licence Renewal**Licence Renewal.

ALARM LED turns on and the alarm is registered in the alarm log).

- *Line code* —the method of channel information encoding (HDB3, AMI).

- *Slip indication*—when checked, any slips identified in the reception path result is fault indication.

- *Slip detection timeout*—time interval for stream parameters polling on the card; if a slip is detected in the stream, the gateway will indicate an alarm during the timeout.

4.1.5.3 Q.931 Signalling Protocol Configuration

Physical Parameters/Q.931 Tab

Q.931 LAPD—LAPD Channel-Level Parameters of Q.931 Protocol

- *T200*—transmission timer. The timer defines the time period when a frame response should be received, which enables transmission of next frames. The time period should be longer than the time required to transmit a frame and receive its acknowledgement.

- *T203*—the maximum time when the device may have no frames exchange with the opposite device.

- *N200*—the number of frame transmission retries.

Q.931 Signalling Protocol parameters

- *TrunkGroup*—name of the trunk group this E1 stream belongs to.

- *Scheduled routing profile*—the selected scheduled routing profile.

- *Access category*—the selected access category.

- *Dial plan* —defines the numbering schedule that will be used to route calls received from this port (required for coordination of numbering schedules).

- *Numbering plan type*—defines the ISDN numbering schedule type. To use E.164 common numbering schedule, select *ISDN/telephony*.

- *Calling category for incoming calls*—the caller ID category assigned to the calls received from this port.

- *Send calling category* —enables transmission of the caller ID category as the first digit of the number in the CgPN information element of the SETUP message.

> ✓ **Proper operation requires support of this mode by the opposite party.**

- *"End-of-dial" message*—issues the "*Sending Complete*" information element upon the "*End of dial*" event (the event received from a linked channel; the maximum number of digits is achieved according to the prefix; the dialling timeout for the next digit).

- *Do not send RESTART for interface*—when checked, the gateway does not send the RESTART message into the line when a stream is restored (the channel level LAPD is established).

- *Do not send RESTART for channel* —when checked, the gateway does not send the RESTART message into the line upon expiration of T308 timer. The timer activates when the RELEASE message is sent into the channel and resets upon receipt of the RELEASE COMPLETE message in response. If the RELEASE COMPLETE message is not received while T308 timer is active, the RESTART message is transmitted to release the channel.

- *Channels selection order* —defines the order of physical channels provisioning for an outgoing call. Four types are available: sequential forward, sequential back, from the first one and forward, from the last one and back. To minimise the number of communication conflicts with adjacent PBXs, inverse channel engagement types are recommended.

- *DialTone for incoming overlap-seize*—when checked, the gateway sends a *DialTone* into the line in case of an incoming overlap engagement (the *"PBX response"* ready signal). In this case, an *overlap engagement* means that the SETUP message is received without "*sending complete*". To switch between tracts, the SETUP message should have the progress indicator = 8.

- *Process PI 'In-band' in DISCONNECT* — when checked, field *PI In-Band* contained in *DISCONNECT* message will be processed for call clearback IVR voice message transmission otherwise this field is ignored.

Names transmission parameters

In this tab you can configure method of reception/ transmission of subscriber name and type of encoding of receiving/transmitting name.

Name transmission method:

- *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 supplementary information for Hicom PBX;
- *AVAYA DISPLAY* - transmission in Q.931 Display element with Codeset 6;

Name encoding method:

- *Transit* - transcoding is not performed (name received in UTF-8, by default);
- *CP 1251* - Windows-1251 encoding;
- *Siemens adaptation* - Siemens PBX encoding;
- *AVAYA adaptation* - AVAYA PBX encoding;
- *Latin transliteration* - latin transliteration of Russian names.

Using Channels

This menu allows E1 stream channels to be enabled or disabled. Check or uncheck the checkbox next to the corresponding channel. The *Trunk Group* column shows the number of the group where the channels are configured (it is used when a trunk group is set for certain stream channels instead of the entire stream).

4.1.5.4 SS7 Signalling Protocol Configuration

SS-7 Settings

- *SS7 Linkset* —linkset selection (SS-7 line group).

- *Channel ID (SLC)*—identifier of a signal channel in the SS-7 line group.

- *MTP3 opposite code (DPC-MTP3)*—the code of the opposite signalling transition point (STP). It is used when SMG operates in the quasi-associated mode. If the quasi-associated mode is not required, set the value to 0. In this case, the opposite MTP3 code is equal to the *DPC-ISUP* value, which is set in the configuration of SS-7 Line Groups (**section 4.1.7.2**).

- *D-channel*—the number of the channel interval (CI) to be used for signal transmission.

- *Bit D in LSU*—sets "1" to bit D in the status field (SF) of the LSSU signal unit (bits D–F in the status field are reserved).

Channel Settings

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

To adjust automatic numbering of voice links, click the *Set* button.

This will open the following menu:

- *Starting number*—the number of the first voice link.

- *Numbering increment*—the channel numbering increment. Each subsequent channel will be assigned a number, which is greater than the number of the current channel by the numbering increment.

- *Channels range*—this section allows numeration adjustment for all stream channels or for a certain range of channels only.

The *Trunk Group* column shows the number of the group where the channels are configured (it is used when a trunk group is set for certain stream channels instead of the entire stream).

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

Set Clear Stream transit

Apply Cancel

The button for configuration of a channel transit through semi-permanent connection is displayed in 'Transit' column[7]. The example of configuration of the connection is represented in appendix G.

The window where you can set the following parameters is opened after clicking the button:

Configure transit

Stream 2, channel 1

Transit enable: ☐

SIP interface: [0] incoming ▼

Codec: Default ▼

E1 stream: Stream 0 ▼

Channel: 1

Active side: ☐

Apply Cancel

---

[7] Only upon a lisence for transit

- *Transit enable*– When you enable a transit, the channel will be excluded from SS7 stream and will be transmitted directly over semi-permanent connection through a SIP interface;

- *SIP interface* – interface through which transit is implemented;

- *Codec*–voice codec, which will be used for transit. If you chose 'by default', the codecs which were configured on the selected SIP interface will be negotiated;

- *E1 stream* – E1 stream on remote side , to which the channel will be connected;

- *Channel* – channel of E1 stream on remote side to which the channel will be connected;

- *Active side* – if you enable this option, SMG will initiate connection for the channel transit. If you disable the option, SMG will be a receiving side for the channel.

Click 'Stream transit' button for enabling transit for all channels on the stream with the same settings. The list of settings will be the same as for single channel, except the 'number of channel' field, which will not be available in this mode, every channel number on the active side will be comply to channel number on remote side.

4.1.6 Dial plan

This section defines transition prefixes to trunk groups.

The device features up to 16 independent numbering schedules. Every numbering schedule may have its own subscribers and prefixes. To set the number of active schedules, see section **4.1.1 System Parameters**.

The device routes calls using 2 criteria:

- Search by caller number—CgPN (Calling Party Number).
- Search by callee number—CdPN (Called Party Number).

When a call arrives to a numbering schedule, its routing begins; first of all, a search for matches to CgPN number masks is performed. If a match is found, the call is routed and further search is stopped.

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

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

Dial plan settings

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

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

The check is performed by caller and callee subscriber masks. The search results determine if call routing is possible for the caller number (CgPN) or the callee number (CdPN) and retrieve the prefix number, if it is.

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

Search masks by template—searches a prefix by the number template.

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

- *Title*—name of the numbering schedule.
- *Dial plan*—the selected numbering schedule.
- *Access category*—the selected access category.
- *Check access category*—when checked, checks the possibility of call routing by the prefix based on the rules determined by access categories.
- *Prefix type*—the selected prefix type:
  - *TrunkGroup*—transition to trunk group;
  - *Trunk Direction*—transition to trunk direction.

- *Change dial plan* —dialling the prefix allows the system to switch to another numbering schedule. When this prefix type is selected, the *New Numbering Schedule* option becomes available which allows selection of the numbering schedule to switch to.

For a trunk group:

- *TrunkGroup*—the trunk group the call will be routed to by this prefix.

- *Direction*—the trunk group access type: local, emergency, zone, private, long-distance, international. It is used to limit communication capabilities if data communication with the RADIUS server fails (see section **4.1.13 RADIUS Configuration**).

- *Caller ID request*—defines if transition to the trunk group specified in the *Trunk Group* field requires caller ID information (caller number and category). When a call arrives from a communication node and the caller ID information is missing, a caller ID request will be sent to the node (an INR message from SS-7 signalling).

- *Caller ID mandatory*—indicates that caller ID information is *mandatory* during the direction transition. If caller ID information cannot be retrieved from the calling party, the connection establishment is cancelled.

- *Dial mode*—the method of number transmission:
    - *enblock*—wait for collection of the entire address information;
    - *overlap*—do not wait for collection of the entire address information.

- *Do not send end-of-dial (ST)*—when checked, the end dial marker is not sent (ST in SS or "*sending complete*" in PRI).

- *Priority*—sets the prefix priority within the range from 0 to 100. A prefix with a smaller value has a higher priority (0 is the highest priority, 100 is the lowest).

For trunk direction:

- *Trunk direction*—a trunk direction (a set of trunk groups united in one direction), in which a call will be routed by this prefix.

- *Direction*—the trunk group access type: local, emergency, zone, private, long-distance, international. It is used to limit communication capabilities if data communication with the RADIUS server fails (see section **4.1.13 RADIUS Configuration**).

- *Caller ID request*—defines if transition to the trunk group specified in the *Trunk Group* field requires caller ID information (caller number and category). When a call arrives from a communication node and the caller ID information is missing, a caller ID request will be sent to the node (an INR message from SS-7 signalling).

- *Caller ID mandatory*—indicates that caller ID information is *mandatory* during the direction transition. If caller ID information cannot be retrieved from the calling party, the connection establishment is cancelled.

- *Dial mode*—the method of number transmission:
    - *enblock*—wait for collection of the entire address information;
    - *overlap*—do not wait for collection of the entire address information.

- *Do not send end-of-dial (ST)*—when checked, the end dial marker is not sent (ST in SS or "*sending complete*" in PRI).

- *Priority*—sets the prefix priority within the range from 0 to 100. A prefix with a smaller value has a higher priority (0 is the highest priority, 100 is the lowest).

To change the numbering schedule:

- *New numbering schedule*—the numbering schedule the call, which is routed by this prefix, will be directed to.

- *New access category*—the access category to be allocated to the caller when the numbering schedule is changed.

- *Priority*—sets the prefix priority within the range from 0 to 100. A prefix with a smaller value has a higher priority (0 is the highest priority, 100 is the lowest).

CdPN settings

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

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

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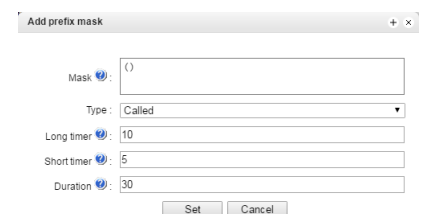
- *Short timer*—time interval in seconds when the digital gateway will wait for further dialling if a part of address information has already been received. The default value: 5 seconds.

- *Duration*—the timer for number dialling duration. The default value: 30 seconds.
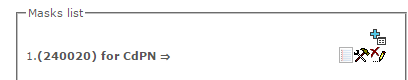
The *Mask List* section allows configuration of number masks for routing by this prefix.

To generate the list, use the following buttons:

— *Add Mask*;

— *Edit Mask;*

— *Remove Mask;*

— *View Mask.*

- *Mask*—a template or a set of templates, which is compared to the caller or callee number received from the incoming channel. It is used for further call routing (for mask syntax, see section **4.1.6.1**).

- *Type*—mask type. Defines the number for the call routing—caller number (calling) or callee number (called).

- *Long timer*—time interval in seconds when the digital gateway will wait for the next digit dialling until a match to a sample from the numbering schedule is established. The default value: 10 seconds.

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

- *Duration*—the timer for number dialling duration. The default value: 30 seconds.

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

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

4.1.6.1 Description of Number Mask and Its Syntax

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

Syntax:

- **X** or **x**—any digit;
- *****—an asterisk (*);
- **#**—a sharp (#);
- **0–9**—digits from 0 to 9;
- **D**—character D.
- **.** —the *dot* is a special symbol which means that the preceding character may be repeated any number of times (30 characters max. for one number), e. g.:
  - **(34x.)** —all possible number combinations which 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 which begin with 1, 2, 3, 4, or 5.
  - the enumeration **([138]xx)**—all 3-digit numbers which 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)**.

- **|**—logical *OR*—separates templates in a mask.
- **(-)**—the mask which is used only in CgPN number modifier tables for calls without a caller number. Allows the caller number to be added if it was missing and also specifies indicators for that number.

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

Prefix 1: (2xxxx)

Prefix 2: (23xxx)

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

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

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

Prefix 2: (23xxx)

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

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

Prefix 1: (2x.)

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

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

4.1.6.2 Mask Operation Examples

Example 1

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

The mask contains 9 templates:

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

Example 2

A numbering schedule configuration is required to allow all numbers, which 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.

4.1.6.3 Timer Operation Examples

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

L = 10 seconds.

S = 5 seconds.

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

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

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

4.1.7 Routing

4.1.7.1 Trunk Groups

№	TrunkGroup	TrunkGroup member	Direct routing prefix	Disable ingress	Disable egress
0	in	SIP interfaces [0]	prefix 1 "to_931_0"	-	-
1	out	SIP interfaces [1]	not installed	-	-
2	tdm_out	Q.931 [0]	not installed	-	-
3	tdm_in		not installed	-	-
4	ss7_0	LinkSet [0]	not installed	-	-
5	ss7_1	LinkSet [1]	not installed	-	-
6	in_SIP	SIP interfaces [4]	not installed	-	-
7	in_SIP-T	SIP interfaces [5]	not installed	-	-
8	in_SIP-I	SIP interfaces [6]	not installed	-	-
9	asterisk	SIP interfaces [7]	not installed	-	-
10	tau32	SIP interfaces [8]	not installed	-	-
11	sipp_in	SIP interfaces [2]	prefix 1 "to_931_0"	-	-
12	sipp_out	SIP interfaces [3]	not installed	-	-

A trunk group is a set of connecting lines (trunks), such as: E1 stream channels, data transmission band (IP channels). E1 stream channels enable Q.931 and SS-7 signalling, while IP channels enable SIP-T interface. To *edit a trunk group,* double-click the corresponding row in the group table with the left 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 64 trunk groups are supported.

Trunk Group Parameters

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

- *Title*—name of the trunk group.

- *TrunkGroup members*—content of the trunk group (E1 stream channels, Q.931 signalling stream, SS line group, or SIP interface) that can be changed when editing the group.

- *E1 stream*—an E1 stream; the parameter is specified if the group includes E1 channels. To include a channel into a trunk group, check the checkbox next to it.

- *Channels selection order*—channel selection order in E1 streams. This menu is available when you chose E1 streams from SS7 Linkset;

- *Direct routing prefix*—transition to the prefix without caller or callee number analysis. It enables switching of all calls in a single trunk group to another group regardless of the dialled number (without mask creation in prefixes). When a number is dialled in the overlap mode, direct dialling timers are used, which are configured in the direct prefix.

Ingress calls

- *Disable ingress calls*—when checked, the incoming calls are barred. Setting the call barring does not terminate any of the established connections.

- *No Connected number transit*—indicates that the *Connected Number* parameter set in the message of the Q.931, the SS-7 protocol is not translated.

- *RADIUS profile*—the selected RADIUS profile (see description in section **4.1.13.2**).

Ingress calls modifiers

- *CdPN*—intended for modifications based on analysis of the callee number received from the incoming channel.

- *CgPN*—intended for modifications based on analysis of the caller number received from the incoming channel.

Egress calls

- *Disable egress calls*—when checked, the outgoing calls are barred. Setting the call barring does not terminate any of the established connections.
- *Reserve TrunkGroup*—specifies the trunk group a call will be routed to when routing to the current trunk group is not possible (all channels are engaged or inoperable).

Egress calls modifiers

- *CdPN*—intended for modifications based on analysis of the callee number sent to the outgoing channel.
- *CgPN*—intended for modifications based on analysis of the caller number sent to the outgoing channel.
- *Original Called Number*—intended for modifications based on analysis of the callee's original number sent to the outgoing channel.
- *Redirecting Number*—intended for modifications based on analysis of the redirecting number sent to the outgoing channel.
- *Generic number*—intended for modifications based on analysis of the generic number sent to the outgoing channel.

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

　　　　— *Add Trunk Group;*

　　　　— *Edit Trunk Group Parameters;*

　　　　— *Remove Trunk Group*.

4.1.7.2 SS7 Linksets

№	SS7 Linkset	Linkset members	TrunkGroup
0	Linkset00	Stream 2 (SS7)	ss7_0
1	Linkset01	Stream 3 (SS7)	ss7_1

For SS7 signalling protocol configuration, see the E1 Streams section (section 4.1.5.4).

An *SS7 line group* is a signal link, which includes a group of signalling channels. To create, edit, or remove line groups, use the *Objects—Add Object, Objects—Edit Object,* or *Objects—Remove Object* menus and the following buttons:

　　　　– *Add SS-7 Line Group (LinkSet);*

　　　　– *Edit SS-7 Line Group (LinkSet);*

　　　　– *Remove SS-7 Line Group (LinkSet).*

SS7 Linksets		

SS7 Linkset 0		
Title	Linkset00	
TrunkGroup	[4] ss7_0	▼
Access category	[0] AccessCat#0	▼
Dial plan	[0] Основной	▼
Scheduled routing profile	Not set	▼
Toll	☐	
Alarm indication	☐	
Channel selection	successive forward	▼
Reserve SS7 Linkset	Not set	▼
Combined mode	☐	
Primary SS7 Linkset	Not set	▼
Secondary SS7 Linkset	Not set	▼
SS7 Timers profile	Profile 0	▼
MTP2 layer settings		
Emergency alignment for a single link	☐	
Service information (SIO)		
Network ID	local network	▼
Routing label		
OPC	40	
DPC-ISUP	42	
ISUP subsystem		
Channels initialization mode	individual unblock	▼
Send REL on receiving SUS	☐	
Add a digit in IAM for overlap	☐	
Restrict CdPN in IAM to 15 digits	☐	
Control receiving Redirecting/Original Called for incoming redirection	☑	
IAM indicators		
Transmission medium requirements	transit	▼
Forward call indications		
ISUP preference	unchanged	▼
Interworking indicator	unchanged	▼
Call type indicator	unchanged	▼
Connect type idicators		
Satellite indicator	change to 'no satellite'	▼
Enable continuity check	☐	
Continuity check frequency ⓘ	0	

Apply   Cancel

SS-7 Line Group Parameters

SS-7 Line Group

- *Title* —name of the SS-7 line group.
- *TrunkGroup*—name of the trunk group the SS-7 line group operates with.
- *Access category*—the selected access category.
- *Dial plan*—defines the numbering schedule that will be used to route calls of this group (required for coordination of numbering schedules).
- *Scheduled routing profile*—the selected scheduled routing profile.

- Toll[8]—means that this signal link is connected to the ALDE. This parameter is used to ensure correct operation with long-distance calls (used in transits to signalling CAS).
- *Alarm indication*—when checked, a fault in SS-7 signal link results in fault indication (the ALARM LED turns on and the fault is registered in the alarm log).
- *Channel selection*—the order of channel engagement for outgoing calls. Available options:
  - sequential forward;
  - sequential back;
  - from the first and forward;
  - from the last and back;
  - sequential forward even;
  - sequential back even;
  - sequential forward odd;
  - sequential back odd.

> **To minimise the number of communication conflicts with adjacent PBXs, inverse channel engagement types are recommended.**

- *Reserve SS7 Linkset*—the selected redundant SS-7 line group. When the main SS-7 line group is not available, the exchange of signalling messages will be entirely performed through the redundant SS7 line group.
- *Combined mode*—the Combined Linkset mode which means that only voice streams are used in this SS-7 line group, while signal channels of the primary and secondary SS-7 groups are used for signalling.
- *Primary SS7 Linkset* —the SS-7 line group selected by signal D-channels that will be used to exchange the signalling messages related to this particular SS-7 line group.
- *Secondary SS7 Linkset* —the second SS7 line group selected by signal D-channels that will be used to exchange the signalling messages related to this particular SS-7 line group.

> **In the combined mode, the signalling load is evenly distributed (50/50) between the primary and secondary SS-7 line groups.**

- *SS7 Timers profile*—the selected timer profile which will be used for this SS-7 line group.

MTP2 Level

- *Emergency alignment for a single signal link*—enables emergency phasing during SS-7 line group commissioning, if this SS-7 line group has a single signal link.

Service Information (SIO)

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

Routing Label

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

---

[8] Not supported in the current version.

ISUP Subsystem

- *Channels initialization mode*—device operations during stream recovery:
    - *leave blocked*—channels remain blocked (BLO);
    - *individual unblock*—the unblock command (UBL) is sent for each channel;
    - *group unblock*—a group command is sent to unblock a group of channels (CGU);
    - *group reset*—the group reset command (GRS) is sent.

- *Send REL on receiving SUS*—sends the REL message in response to the SUS message, which notifies about channel suspension.

- *Add a digit in IAM for overlap*—sends a single digit to the *Called Party Number* field of the IAM message in the overlap dialling mode.

- *Restrict CdPN in IAM to 15 digits* —when checked, limits the number of digits of the CdPN number sent in the IAM message to 15, while other digits are sent in the SAM message.

- *Control receiving Redirecting/Original Called for incoming redirection*—when checked, a call will be cleared back if the IAM message contains the *Redirection Information* parameter, but has no *Redirecting Number* or *Original Called Number*.

IAM Indicators

- *Transmission medium requirements*—specifies the type of information to be delivered by the transmission environment.

Forward call indications

- *ISUP preference* —a rule that governs modification of the ISUP preference indicator. As a rule, these bits should not be changed.

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

- *Call type indicator*—determines whether the call type indicator should change its value to *international* or *national*.

Connect type indicators

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

    - *Override to "no satellite"*—changes the identifier value to "*no satellite*" regardless of the value received from the incoming channel.
    - *Unchanged*—keeps the indicator value unchanged.
    - *Add one*—this setting is used if the signal link operates via a satellite channel. In this case, the satellite channel parameter transmitted in the *Nature of Connection* indicators is increased by 1.

- *Enable continuity check* —enables integrity check support in the SS-7 line group. During an outgoing call, the called party establishes a remote loop in the stream, SMG sends the frequency to the channel that will be detected on receipt after signal transmission through the channel. If the frequency is detected, the call is handled through this channel; otherwise, a similar attempt is performed on the next channel. After 3 unsuccessful attempts (on three different channels), the call service is stopped.

- *Continuity check frequency* —defines the frequency of channel integrity checks during outgoing calls performed through the SS-7 line group. For example, the value of 3 means that every third outgoing call will be checked for channel integrity.

A correspondence between SS and Caller ID categories can be adjusted for the gateway. For configuration, see section **4.1.8.1 SS Category**.

4.1.7.2.1 Examples

An example of SMG connection for operation in the SS-7 quasi-associated mode via signalling transfer points (STP).
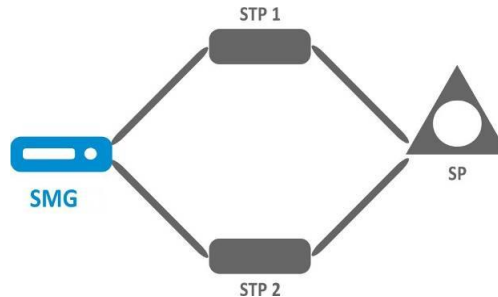
Objective

A connection is required between SMG and the opposite signalling point (SP) using two signal links. The first signal link should pass through STP 1 signalling transition point, while the second one—through STP 2.

Point code: SMG4 = 22, STP 1 = 155, STP 2 = 166, SP = 23.

Solution

In addition to basic settings, set Own Point C*ode (OPC)* = **22** and *ISUP Opposite Code (DPC-ISUP)* = **23** in the *SS-7 Line Groups* menu.

Let us assume that stream 0 is connected to STP 1, while stream 1—to STP 2. Specify the following in the stream settings: SS7 *Signalling protocol*; configure CIC numbering correctly and select the required E1 stream time slot for signalling D-channel; select the pre-created SS-7 line group in *SS-7 Line Group* settings and set *MTP3 Opposite Code (DPC-MTP3)* to **155** for stream 0 and to **166** for stream 1.

An example of SMG connection for operation in the SS-7 quasi-associated mode via PBX with STP features.
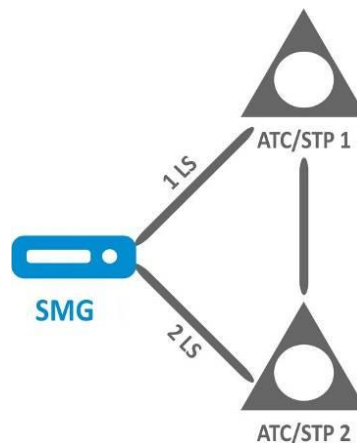
LS— an SS-7 line group (Link Set).

Objective

A connection is required between SMG and two PBXs with STP features (PBX/STP); when the 1LS main circuit group between SMG and PBX/STP 1 fails, signalling messages should be sent via 2LS.

Solution

Let us assume that stream 0 of SMG is connected to PBX/STP 1 and is configured to use the first SS-7 line group, while stream 1 is connected to PBX/STP 2 and is configured to use the second SS-7 line group. Specify the following in the stream settings: **SS7** *Signalling protocol;* configure CIC numbering correctly and select the required E1 stream time slot for signalling D-channel; specify the second SS-7 line group in *Redundant SS-7 Line Group* in configuration of the first SS-7 line group.

An example of SMG connection for operation in the combined mode.
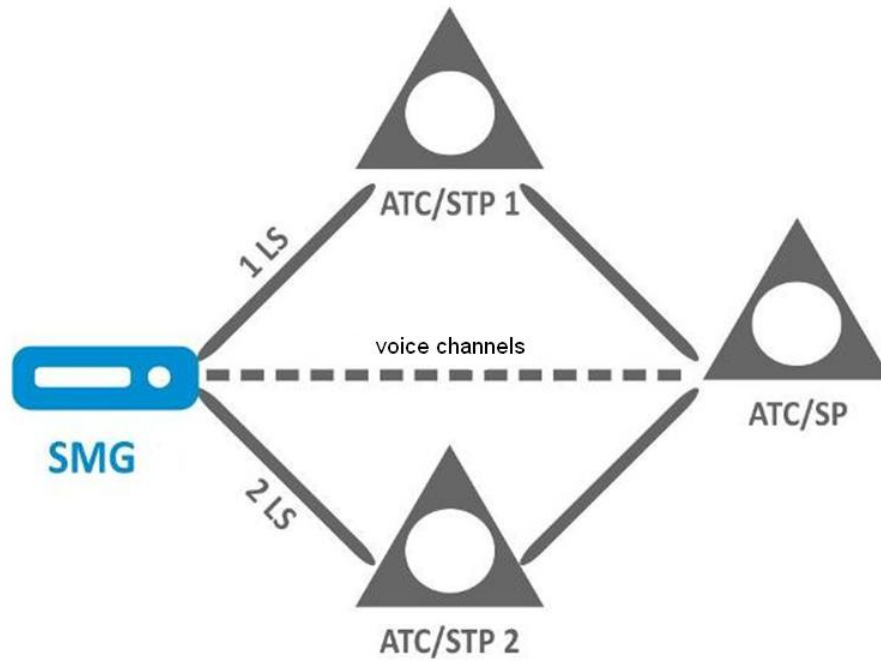
Objective

Only voice channels are used for communication between SMG and PBX/SP; signalling traffic should be transferred via PBX/STP 1 and PBX/STP 2.

Solution

Let us assume that stream 0 of SMG is connected to PBX/STP 1 and is configured to use the first SS-7 line group, while stream 1 is connected to PBX/STP 2 and is configured to use the second SS-7 line group; stream 2 of SMG is connected to PBX/SP and is configured to use the third SS-7 line group. Specify the following in the stream settings: **SS7** *Signalling protocol;* configure CIC numbering correctly and select the required E1 stream time slot for signalling D-channel of streams 0 and 1; specify the **first** SS-7 line group in *Primary SS-7 Line Group* in configuration of the third SS-7 line group; specify the **second** SS-7 line group in *Secondary SS-7 Line Group* in configuration of the third SS-7 line group.

4.1.7.3 SIP/SIP-T/SIP-I Interfaces

4.1.7.3.1 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, the device will process requests, which contain "+", ";", "=", "?" in the SIP subscriber number, and will automatically add "+" before the callee number for international calls using the SIP-T protocol.

SIP interfaces

Settings ▼

№	SIP interface	Mode	TrunkGroup	Hostame / IP-address:port	Codecs	DTMF mode	Fax detect	VBD
0	incoming	SIP	in	192.168.1.22:5151	G.711U G.711A	RFC2833 (101)	No detect fax	dis
1	outgoing	SIP	out	192.168.69.22:5152	G.711A G.711U	RFC2833 (101)	No detect fax	dis
2	sipp_in	SIP	sipp_in	192.168.0.123:5064	CLEARMODE G.711U G.711A	Inband	No detect fax	dis
3	sipp_out	SIP	sipp_out	192.168.1.123:5064	CLEARMODE G.711U G.711A	Inband	No detect fax	dis
4	from_SIP	SIP	in_SIP	192.168.1.22:5081	G.711A G.711U	Inband	No detect fax	dis
5	from_SIP-T	SIP-T	in_SIP-T	192.168.1.22:5082	G.711A G.711U	Inband	No detect fax	dis
6	from_SIP-I	SIP-I	in_SIP-I	192.168.1.22:5083	G.711A G.711U	Inband	No detect fax	dis
7	asterisk	SIP	asterisk	192.168.1.123:5070	G.711A G.711U	Inband	No detect fax	dis
8	TAU32	SIP	tau32	192.168.1.32:5060	G.711A G.711U	Inband	No detect fax	dis

Common SIP settings	
Local SIP port ❷	5060
Transport ❷	UDP-prefer ▼
(x100 ms) T1 timer ❷	5
(x100 ms) T2 timer ❷	40
(x100 ms) T4 timer ❷	50
Ignore address from R-URI	☐

Apply

Common SIP settings

- *Local SIP port*—the UDP port which is used to send and receive SIP messages.

- *Transport*—the selected transport protocol which is used to send and receive SIP messages:

  - *TCP-prefer*—the messages are received via UDP and TCP and sent via TCP. If failed to establish a TCP connection, the messages are sent via UDP.
  - *UDP-prefer*—the messages are received via UDP and TCP. The packets smaller than 1,300 bytes are sent via TCP, while the ones larger than 1,300 bytes—via UDP.
  - *UDP-only*—use the UDP protocol only.
  - TCP-only—use the TCP protocol only.

- *T1 timer*—timeout for a request; upon expiration, the request is re-sent. The maximum retranslation interval for the INVITE requests is equal to 64*T1.

- *T2 timer*—the maximum retranslation interval for responses to the INVITE request and for all requests except for the INVITE ones.

- *T4 timer*—the maximum time allotted for all retranslations of the final response.
- *Ignore address in R-URI*—specifies that only the *user* part of the request URI is analysed.

Up to 64 interfaces are supported. To create, edit, or remove SIP/SIP-T interfaces, use the *Objects—Add Object, Objects—Edit Object,* or *Objects—Remove Object* menus and the following buttons:

 — Add Interface;

 — *Edit Interface Parameters;*

 — *Remove Interface.*

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

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

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

G.729 is a voice data compression codec too; it supports the rate of 8 kbps. By analogy with G.723.1, G.729 supports a voice activity detector and generates comfort noise (Annex B).

T.38 is a standard which describes sending facsimile messages in real time over IP networks. Signals and data sent by a fax unit are copied to T.38 protocol packets. The generated packets may include redundancy data from previous packets that allows reliable fax transmissions through unstable channels.

CLEARMODE—a mode which does not use signals encoding/decoding. It is supported for transparent transmission of digital information at 64 kbps (RFC4040).

The Service Type (IP DSCP) field value for RTP, T.38, and SIP/SIP-T/SIP-I
0 (DSCP 0x00, Diffserv 0x00)—the best effort—the default value.
8 (DSCP 0x08, Diffserv 0x20)—*class 1.*
10 (DSCP 0x0A, Diffserv 0x28)—assured forwarding, low drop precedence (Class1, AF11).
12 (DSCP 0x0A, Diffserv 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).

4.1.7.4 SIP Interface Configuration Tab

- *Title* —the interface name.

- *Mode*—the protocol selected for the interface (*SIP/SIP-T/SIP-I, Transit E1*).

- *TrunkGroup—name of the trunk group the interface in included to.*

- *Access category*—the selected access category.

- *Dial plan*—defines the numbering schedule that will be used for dialling from this port (required for coordination of numbering schedules).

- *Hostname/IP-address*—IP address or name of the host communicating via the gateway's SIP/SIP-T protocol.

- *Remote SIP port[9]*—a UDP/TCP port of the communicating gateway that is used to receive SIP/SIP-T signalling.

- *Local SIP port[9]*—a local UDP/TCP port of the device that is used to receive SIP/SIP-T signalling from the communicating device via this interface.

- *Public IP* —the IP address which is used for outgoing SIP/SDP messages. This helps to ensure correct operation of the device after NAT.

---

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

- *Ignore source port for incoming calls*—when 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 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 checked, SMG will indicate a fault when connection to the opposite device is lost. For correct operation of this feature, check the *Opposite party availability control using OPTIONS messages* checkbox in SIP settings.

- *Network interface for SIP*—the network interface selected to receive and transmit signalling SIP messages.

- *Network interface for RTP*—the network interface selected to receive and transmit voice traffic.

- *Q.850-cause and SIP-reply mapping table*—the selected table of correspondence between Q.850-cause and SIP-reply codes. To configure correspondence tables, use the *Internal Resources* menu.

- *Scheduled routing profile*—the selected profile of the *scheduled routing* service, which is configured in the *Internal Resources* section.

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

Options configurations for 'Transit E1' mode.

Some of the options are not used in this mode. Fields which are not used are not displayed and are not available in 'Transit E1' mode. The rest of the fields are configured as in SIP/SIP-T/SIP-I mode.

SIP interfaces		
SIP interface settings	SIP protocol settings	Codecs/RTP settings

Index [0]	
Title	incoming
Mode	Transit E1 ▼
Hostname / IP-address	192.168.1.22
Remote SIP port	5151
Local SIP port	5151
Public IP	0.0.0.0
Ignore source port for incoming calls	☑
Alarm indication	☐
Network interface for SIP	eth0 (eth0 192.168.6.5) ▼
Network interface for RTP	vlan (eth0.609 192.168.69.104) ▼

Apply   Cancel

SIP/SIP-T/SIP-I Options Configuration

- *Keep-alive control by messages OPTIONS*—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, which are configured in this direction, in case the opposite party does not support them. The parameter defines the request transmission period and may take values in the range of 30–3,600 seconds.

- *Always transmit SDP in provisional responses*—allows early forwarding of voice frequency path. For example, when unchecked, SMG sends reply 180 without SDP session description; according to this reply, the outgoing party plays the ringback tone; when 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).

- *Enable redirection (302) processing*—when checked, the gateway is allowed to perform redirection upon receipt of reply 302 from this interface. When unchecked and reply 302 is received, the gateway will reject the call and perform the redirection.

- *Redirection server direction*—this option is available when reply 302 processing is enabled (*the Enable redirection (302)* parameter). This enables redirection of the call, which was sent using a public address, to the subscriber's private address received in reply 302 without numbering schedule routing. The call is routed directly to the address specified in the "contact" header of reply 302 received from the redirection server.

- *Enable REFER processing*—a REFER request is sent by the communicating gateway to enable the *Call Transfer* service. When 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.

- *Reliable provisional responses (1xx)*—when 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.

  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.

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

> **DSCP settings for RTP** and **SIP** will be ignored when a VLAN is used to transmit RTP and signalling. In this case, *"Class of Service VLAN"* will be used for traffic prioritisation.

- *Remote name in contact header* - insert displayed name in Contact header.

SIP Session Timers (RFC 4028)

- *Enable*—when 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).

Registration Settings[10]
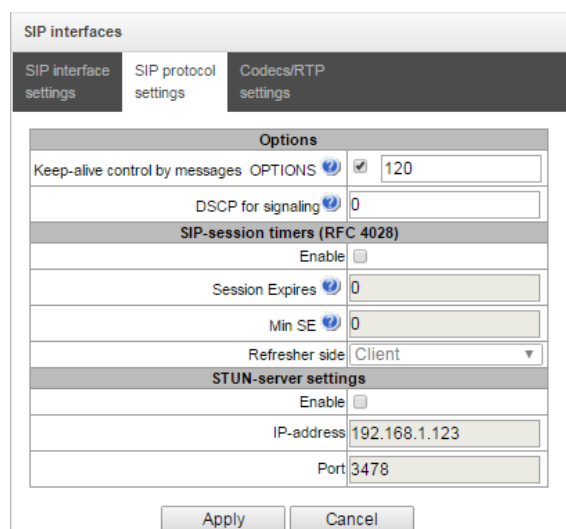
- *Upper registration*—the selected type of registration on an upstream server:
    - *Trunk registration*—registration on the upstream server using parameters specified in this section.
- *Login*—the name used for authentication.
- *Password*—the password used for authentication.
- *Username/Number*—the user number which is used as a caller number for outgoing trunk calls.
- *SIP domain*—the SIP domain to be used for registration and subsequent calls from this interface.
- *Routing mode—the* selected mode for incoming calls routing in case of trunk registration:
    - *by RURI*—routing by request-URI of the INVITE message;
    - *by TO*—routing by the TO field of the INVITE message;
    - *by CdPN by default*—routing by the specified CdPN number regardless of the numbers received in the INVITE message;
- *Default CdPN* —the CdPN number for calls routing in case of the "*by CdPN by default"* mode.
- *Replace CgPN on egress call*—when 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.

STUN Server settings

- *Enable*—when checked, enables requests to the STUN server.
- *IP address—the* IP address of the STUN server.
- *Port*—the port of the STUN server.

Option configuration for 'Transit E1'

Some of the options are not used in this mode. Fields which are not used are not displayed and are not available in 'Transit E1' mode. The rest of the fields are configured as in SIP/SIP-T/SIP-I mode.

---

[10] This block of parameters is available only for the SIP mode.

Options of SIP-session timers (RFC 4028) will be enabled by default in 'Transit E1' mode if the values are not set before.

4.1.7.6 RTP Codec Configuration Tab

Options

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

- *Source IP: Port verification*—when checked, controls media traffic received from the IP address and UDP port specified in the SDP communication session description; otherwise, accepts traffic from any IP address and UDP port.

- *Echo cancellation*—the echo cancellation mode:
  - *voice(default)*—echo cancellers are enabled in the voice data transmission mode;
  - *voice nlp-off*—echo cancellers are enabled in the voice mode; the non-linear processor (NLP) is disabled. When the levels of transmission and reception signals significantly differ, a weak signal may be suppressed by the NLP. This echo canceller mode is used to prevent the signal suppression;
  - *modem*—echo cancellers are enabled in the modem operation mode (direct component filtering is disabled, NLP control is disabled, CNG is disabled);
  - *off*—echo cancellation is disabled (this mode is set by default).

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

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

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

- *RTP-loss timeout*—a function to control voice frequency path status by monitoring the presence of RTP traffic from the communicating device. The range of permitted values is from 10 to 300 seconds. When unchecked, RTP control is disabled; enabled when checked. The following control is performed: if there are no RTP packets coming from the opposite device for the duration of the timeout interval and the last packet was not a silence suppression packet, the call is cleared back.

- *RTP-loss timeout after Silence-Suppression Indication (multiplier)*—the RTP packet timeout for the silence suppression option. The range of permitted values is from 1 to 30. The coefficient is a multiplier that determines how many times the value of this timeout is larger than the *RTP Packet Timeout* value. The following control is performed: if there are no RTP packets coming from the opposite device for the duration of this time interval and the last packet was a silence suppression packet, the call is cleared back.

- *RTCP period (sec.)*—time period in seconds (5–65,535), after which the device sends control packets via the RTCP protocol. When unchecked, RTCP is not used.

- *RTCP activity control*—a function to control voice frequency path status; may take values from 5 to 65,535 seconds. The number of time periods (*RTCP timer*) to wait for RTCP protocol packets from the opposite party. If no packets received during the specified period of time, the established connection is terminated. At that, *"cause 3 no route to destination"* is set as a cause of the disconnection to the TDM and IP protocols. The control period is calculated from the following expression: **RTCP timer * RTCP control period** (seconds). When unchecked, the feature is disabled.

- *Clear Channel* —a channel that is established for transparent transfer of digital data; when the channel is established, the device does not attempt to recode it that ensures transparent transmission. To establish a connection of this kind, the *Transmission Medium Requirement* field is required with the following values:

  – *restricted digital info (Q.931 protocol);*
  – *unrestricted dig.info (Q.931 protocol);*
  – *video (Q.931 protocol);*
  – *64 kbit/s unrestricted (SS-7 protocol).*

- *Clear Channel override*—when checked, only one CLEARMODE codec is specified while establishing a clear channel in SDP if operation via Clear Channel is invoked on the first call leg. When unchecked, the complete list of selected codecs is transferred to SDP in the priority order.

DTMF Transmission

- *DTMF transport* — the method of DTMF transmission via IP network:

  – *inband*—in RTP packets, in-band;
  – *rfc2833*—in RTP packets according to rfc2833 recommendations;
  – *info*—out-of-band. The SIP protocol uses INFO messages; the type of DTMF signals transferred depends on the MIME extension type in this case.

DTMF transport	RFC2833
Flash signal processing (RFC2833)	☐
RFC2833 PT ❓	101
RFC2833: same PT	☐
DTMF MIME Type	application/dtmf-relay

To use extension dialling during a call, make sure the similar DTMF tone transmission method is configured in the opposite gateway.

- *Flash signal processing* (*RFC2833*)—processing of the FLASH signals received according to RFC2833 method.

- *RFC2833 PT*—the type of dynamic load used to transfer DTMF packets via RFC2833. The range of permitted values is from 96 to 127. RFC2833 recommendation defines the transmission of DTMF

via the RTP protocol. This parameter should conform to the similar parameter of the communicating gateway (the most frequently used values are 96, 101).

- *RFC2833: same PT*—when checked, if SMG is the party which sends "*offer SDP*", RFC2833 packets are expected for reception with a PT value sent in "*answer SDP*"; otherwise, RFC2833 packets are expected for reception with the same PT value as sent by SMG "*offer SDP*".

- *DTMF MIME Type*—the load type used for DTMF transmission in SIP protocol INFO packets:

    – *application/dtmf-relay*—in SIP INFO application/dtmf-relay packets ("*" and "#" are sent as symbols "*" and "#");
    – *application/dtmf*—in SIP INFO application/dtmf packets ("*" and "#" are sent as digits 10 and 11).

Jitter Buffer settings

- *Mode*—the mode of jitter buffer operation: fixed or adaptive.

- *Minimum size, ms*—the size of a fixed jitter buffer or the lower limit (minimum size) of an adaptive jitter buffer. The range of permitted values is from 0 to 200 ms.

- *Initial size, ms*—an initial value of the adaptive jitter buffer. The range of permitted values is from 0 to 200 ms.

- Maximum size, ms—the upper limit (maximum size) of the adaptive jitter buffer, in milliseconds. The range of permitted values is from "minimum size" to 200 ms.

Jitter buffer settings	
Mode	Dynamic
Minimum size, ms	0
Initial size, ms	0
Maximum size, ms	200
Adaptation period, ms	10000
Removal mode	Soft
Removal threshold, ms	500
Adjustment mode	Smooth
Size for VBD, ms	0

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

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

    – *Soft*—the device uses an intelligent selection pattern to delete the packets, which exceed the threshold.
    – *Hard*—the packets, which delay exceeds the threshold, are deleted immediately.

- *Removal threshold, ms*—a threshold for immediate deletion of a packet, in milliseconds. When buffer size grows and packets delay exceeds this threshold, the packets are deleted immediately. The range of permitted values is from "Delay max" to 500 ms.

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

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

Options configuration for 'Transit E1' mode

Some of the options are not used in this mode. Fields which are not used are not displayed and are not available in 'Transit E1' mode. The rest of the fields are configured as in SIP/SIP-T/SIP-I mode.

4.1.7.7 Fax and Data Transfer Configuration Tab

Data Transmission

- *Enable VBD*—when checked, creates a VBD channel according to V.152 recommendation for modem transmission. When a CED signal is detected, the device enters *the Voice Band Data* mode. Unchecking the checkbox disables modem tone detection, but does not affect modem

communication (switching to modem codec will not be initiated, but this operation still may be performed by the opposite gateway).

- *VCodec for VBD*—the codec which is used for data transmission in the VBD mode.

- *Payload type for VBD*—the load type which is used for data transmission in the VBD mode.

    – *Static*—uses the standard value of the load type for a codec (8 for G.711A codec, 0 for G.711U codec).
    – 96–127—load types from the dynamic range.

Fax settings

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

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

> **A V.21 signal may also be detected from the transmitting fax.**

- *Fax relay mode*—the protocol selected for fax transmission.

- *Fax relay max rate (bps)*—the maximum transfer rate of a fax transmitted via the T.38 protocol. This setting have influence on the gateway's ability to work with high-speed fax units. If fax units support data transfer at 14,400 bauds and the gateway is configured to 9,600 bauds, the maximum rate of connection between the fax units and the gateway will be limited by 9,600 bauds. And vice versa, if fax units support data transfer at 9,600 bauds and the gateway is configured to 14,400 bauds, this setting does not affect the interaction and the maximum rate is defined by the fax units.

- *Fax relay rate management* —defines the method of data transfer rate management:

    – *local TCF*—the method requires the TCF tuning signal to be locally generated by the recipient gateway. It is generally used for T.38 transmission via TCP;
    – *transferred TCF*—the method requires the TCF tuning signal to be sent from the sender device to the recipient one. It is generally used for T.38 transmission via UDP.

- *T.38 data fill bits removal*—padding bit removals and inserts for the data which is not related to ECM (error correction mode).

- *T.38 data redundancy*—redundancy amount in T.38 data packets (the number of previous packets in the next T.38 packet). Introduction of redundancy allows the transmitted data sequence to be restored upon reception if some packets have been lost during transmission.

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

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

Options configuration for 'Transit E1' mode

Options of modem and fax detection are not used in 'Transit E1' mode. The tab is not available in this mode.

4.1.7.8 Trunk Directions

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

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

    — *Add Direction*;

    — *Edit Direction Parameters;*

    — *Remove Direction.*

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

- *Name*—name of the trunk direction.

- *TrunkGroup select mode*—order of trunk group selection in the direction:
    - *Sequential forward*—all trunk groups of the direction are selected in turns beginning from the first one in the list;
    - *Sequential back*—all trunk groups of the direction are selected in turns beginning from the last one in the list;
    - *From the first and forward*—the first free trunk group of the direction is selected beginning from the first one in the list;
    - *From the last and back*—the first free trunk group of the direction is selected beginning from the last one in the list.

A list of trunk groups in the direction:

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

 — *Add*;

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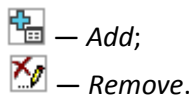
Use the arrow buttons (up, down) to change the trunk group order in the list.

4.1.8 Internal Resources

4.1.8.1 SS7 Categories

This section specifies correspondence between Caller ID categories and SS7 protocol categories.

The generally accepted correspondence between SS7 categories and Caller ID categories is provided below.

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

SS7 Categories

SS7 categories

№	AON category	SS7 category
0	1	10
1	2	225
2	3	228
3	4	11
4	5	226
5	6	15
6	7	227
7	8	12
8	9	229
9	10	224
10	7	0
11	7	240
12	0	0
13	0	0
14	0	0
15	0	0

Apply

Access categories

№	Category	Access to categories
0	AccessCat#0	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
1	AccessCat#1	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
2	AccessCat#2	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
3	AccessCat#3	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
4	AccessCat#4	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
5	AccessCat#5	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
6	AccessCat#6	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
7	AccessCat#7	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
8	AccessCat#8	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
9	AccessCat#9	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
10	AccessCat#10	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
11	AccessCat#11	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
12	AccessCat#12	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
13	AccessCat#13	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
14	AccessCat#14	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
15	AccessCat#15	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
16	AccessCat#16	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
17	AccessCat#17	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
18	AccessCat#18	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
19	AccessCat#19	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

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

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

In total, up to 64 access categories can be configured. Access to the first 16 categories is provided by default in each of the access categories.

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

4.1.8.3 Modifier Tables

Modifiers tables

№	Name	TrunkGroups	RADIUS profiles	CDR settings
0	ModTable#00	out tdm_out tdm_in ss7_1 tau32		
1	ModTable#01			CDR settings

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

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

⊞ — *Add Modifier*;

⚒ — *Edit Modifier Parameters;*

✗ —*Remove Modifier.*

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

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

Number Selection Tab

- *Number mask*—a template or a set of templates which is compared to the subscriber number (for mask syntax, see section 4.1.6.1).

- *Number type*—type of the subscriber number:
    - *Subscriber*—subscriber number (SN) in E.164 format;
    - *National*—national number. The format: NDC + SN, where NDC—a geographical area code;
    - *International*—international number. The format: CC + NDC + SN, where CC—a country code;
    - *Network specific*—specific network number;
    - *Unknown*—unknown type of the number;
    - *Any*—modification will be performed for any number type.

- *Number category*—subscriber's Caller ID category.
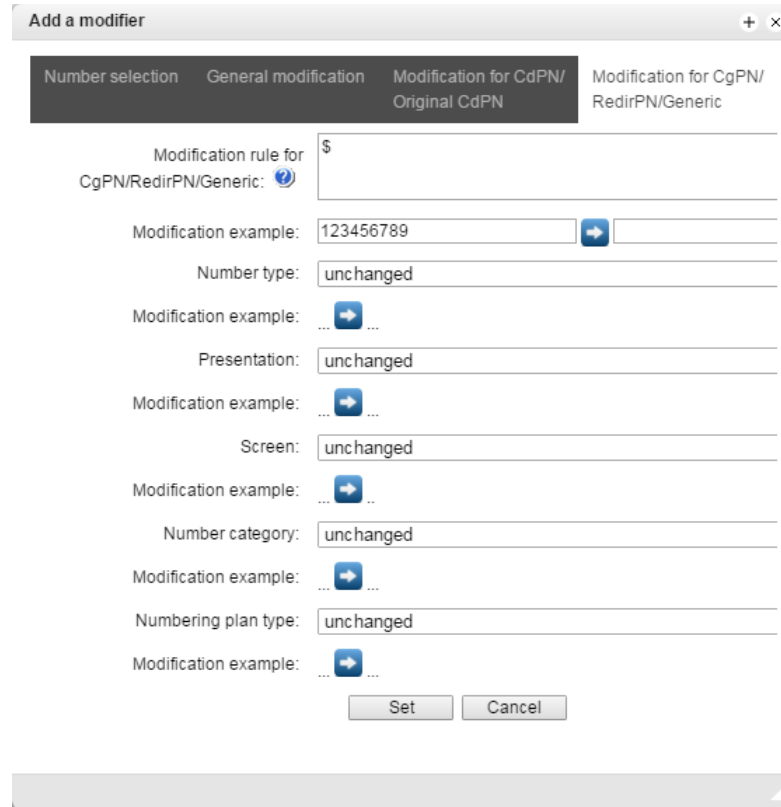
General Modification Tab

- *Modification example*—click the ➡ button to view modification summary after application of the modification rules specified.

- *Access category*—allows modification of access categories.

- *Dial plan* —allows modification of the numbering schedule to be used for further routing (required for coordination of numbering schedules).

CdPN/Original CdPN Modification Tab

- *Modification example*—click the ➡ button to view modification summary after application of the modification rules specified. It is recommended to define a number to be modified instead of number 123456789, which is entered in the rule check example.

- *Modification rule for CdPN/Original CdPN*—callee number modification rule. For syntax, see section **4.1.8.3.1**; for examples, see Appendix C. This rule also applies to modification of the callee original number (original Called party number) when this modifier table is chosen in the *Trunk Group* section for *Original CdPN* modification.

- *Number type*—modification rule for callee number types (no change—do not modify).

- *Numbering plan type*—modification rule for numbering schedule types (no change—do not modify).

CgPN/RedirPN Modification Tab

- *Modification example*—click the button to view modification summary after application of the modification rules specified. It is recommended to define a number to be modified instead of number 123456789, which is entered in the rule check example.

- *Modification rule CgPN/Redir PN*—callee number modification rule. For syntax, see section **4.1.8.3.1**; for examples, see Appendix C. This rule also applies to modification of the redirecting number when this modifier table is chosen in the *Trunk Group* section for *Redir PN* modification.

- *Number type*—modification rule for caller number types (no change—do not modify).

- *Presentation*—modification rule for presentation of the caller (no change—do not modify).

- *Screen*— modification rule for caller screen indicators (no change—do not modify).

- Number *category*—modification rule for caller category (no change—do not modify).

- *Numbering plan type*—modification rule for numbering schedule types (no change—do not modify).

4.1.8.3.1   Modification Rule Syntax

Modification rule is a set of special characters which govern number modifications.

- **'.'** and **'-'**: special characters indicating that a digits is removed in the current position and other digits, which followed the removed one, are shifted to its position.

- **'X'**, **'x'**: special characters indicating that a digit in the current position remains unchanged (the position must contain a digit).

- **'?'**: a special character indicating that a digit in the current position remains unchanged(the position may contain no digits).

- **'+'**: a special character indicating that all characters located between the current position and the next special character (or the end of the sequence) are inserted at the specified location of the number.

- **'!'**: a special character indicating a breakdown finish; all other digits of the number are truncated.

- **'$'**: a special character indicating a breakdown finish; all other digits of the number remain unchanged.

- **0–9, D, #, and *** (not preceded by "+"): informational characters that substitute a digit in the specified position of the number.

4.1.8.4 Q.931 Timers

This section defines configuration of the third level timers required for Q.931 signalling protocol operation.

Timer names and default values are described in Q.931 ITU-T recommendation, §9 *List of System Parameters*.

Name	Default Value, seconds	Range, seconds
T301	180	180 – 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 not less than T316
T320	30	30 – 60
T321	30	30 – 60
T322	4	4 – 10

Q.931 timers

4.1.8.5 SS7 Timers

This section defines configuration of MTP2, MTP3, and ISUP level timers of the SS-7 protocol.

SS7 timers

№	Profile	SS7 Linkset
0	Profile 0	[0] Linkset00, [1] Linkset01

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

— *Add Profile*;

— *Edit Profile Parameters*;

— *Remove Profile.*

SMG digital gateway

- *No.*—the sequence number of the SS-7 timer profile.

- *Profile*—profile name.

- *SS7 Linkset*—a list of SS-7 line groups which have this profile selected.

Profile Settings

Names of MTP2 level timers and their default settings are described in Q.703 ITU-T recommendation, §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

Names of MTP3 level timers and their default settings are described in Q.704 ITU-T recommendation, §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

Names of ISUP level timers and their default settings 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	$15 - 20$

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

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

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

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

— Add Rule;

— *Edit Rule Parameters;*

— *Remove Rule.*

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

Q.850-cause and SIP-reply mapping table

Profile Settings

- Direction:
    - *SIP reply -> Q.850 cause*—direction from SIP to Q.850.
    - *Q.850 cause -> SIP reply*—direction from Q.850 to SIP.
- *Q.850-cause—value of* a Q.850 cause.
- *SIP-reply*—value of a 4xx, 5xx, 6xx class SIP reply.

4.1.8.7 Scheduled Routing

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

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

 — Add Rule;

 — *Edit Rule Parameters;*

 — *Remove Rule.*

Routing Rule

- *Start date*—the selected start date for a scheduled routing rule operation.
- *Active days*—duration of the scheduled routing rule operation.
- *Repeat monthly*—allows monthly repetition of the routing rule.
- *Week days* —the selected days of the week when the scheduled routing rule operates.

- *Active hours* —the selected hours of the scheduled routing rule operation.
- *Dial plan*—the selected routing schedule which will be used during the scheduled routing rule operation.

4.1.8.8 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.

4.1.8.9 Routing Table

This submenu can be used to configure static routes.

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

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

The automatically created routes cannot be changed as they are created automatically when the network

and VPN/PPTP interfaces are established. These routes are required for normal operation of the interfaces.

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

 — Add Route;

 — *Edit Route Parameters;*

 — Remove Route.

Route Parameters

- *Enable*—when checked, enables the route.

- *Destination*—an IP network, an IP address or the *default* value (to set a default gateway).

- *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*—the selected network transmission interface.

- *Metric*—route metrics.

4.1.8.10 Network Settings

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

Device Network Parameters

- *Hostname*—device network name.

- *Use gateway from*—network gateway address for 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.

4.1.8.11 Network Interfaces

The device allows configuration of 1 basic eth0 network interface, up to 8 additional eth0.XX VLAN interfaces, and up to 5 additional pppX VLAN/PPP interfaces.

№	Interface name	Network label	IP-address	Network mask	DHCP	Management services				Telephony services			Firewall profile
0	eth0	eth0	192.168.1.4	255.255.255.0	-	WEB	TELNET	SSH	SNMP	SIP RTP	RADIUS		Firewall Profile #0
1	eth0:1	alt_control	192.168.0.4	255.255.255.0	-	WEB	TELNET	SSH	SNMP	SIP RTP	RADIUS		Not selected
2	eth0.609	vlan	-	-	+	WEB	TELNET	SSH	SNMP	SIP RTP	RADIUS		Not selected

Add   Edit   Delete

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

Network Interface Settings

Basic Settings

- *Network label*—name of the network.

- *Firewall profile*—shows the firewall profile selected for this interface.

- *Type*—interface type (always untagged for eth0 interface).

- *VLAN ID*—VLAN identifier (1–4,095) (only for tagged type interfaces).

- *Enable DHCP*—specifies that an IP address is to dynamically obtained from the DHCP server.

- *IP-address*—network address of the device.

- *Network mask*—subnet mask of the device.

- *Broadcast*—address for packets broadcasting.

- *Gateway*—do not obtain the IP address of the gateway dynamically from the DHCP server.

- *DNS-address by DHCP*—obtain the IP address of the DNS server dynamically from the DHCP server.

Network interface 0	
Network label	eth0
Firewall profile	Firewall Profile #0
Type	Untagged
Enable DHCP	☐
IP-address	192.168.1.4
Network mask	255.255.255.0
Broadcast	192.168.1.255
Gateway	192.168.1.123
DNS-address by DHCP	☐
NTP-address by DHCP	☐
Services	
Enable Web	☑
Enable Telnet	☑
Enable SSH	☑
Enable SNMP	☑
Enable SIP signaling	☑
Enable RTP transmission	☑
Enable RADIUS	☑

- *NTP-address by DHCP*—obtain the IP address of the NTP server dynamically from the DHCP server.

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

- *Enable Web*—enables access via web interface.

- *Enable Telnet*—enables access via the Telnet protocol.

- *Enable SSH*—enables access via the SSH protocol.

- *Enable SNMP*—enables SNMP.

- *Enable SIP signalling*—enables reception and transmission of the SIP signalling information through the network interface configured in this section.

SMG digital gateway

- *Enable RTP transmission*—enables reception and transmission of the voice traffic through the network interface configured in this section.

- *Enable RADIUS*—enables the RADIUS protocol.

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

VPN/PPP Interface Settings

Basic Settings

- *Network label*—name of the network.

- PPTPD IP—IP address of the PPTP server.

- User name—the username (login) used by the device for network connection.

- Password—VPN connection password.

Options

- *Launch at startup*—launches the interface at device startup.

- *Ignore default gateway*—ignores the gateway setting in the *Network Parameters* section.

- *Enable encryption*—enables encryption.

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

- *Enable Web*—enables access via web interface.

- *Enable Telnet*—enables access via the Telnet protocol.

- *Enable SSH*—enables access via the SSH protocol.

- *Enable SNMP*—enables SNMP.

- *Enable RADIUS*—enables the RADIUS protocol.

4.1.8.12 RTP Port Range

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

UDP Port Parameters

- *Starting port*—the number of the UPD starting port for voice traffic (RTP) and data transmission via the T.38 protocol.

- *Ports count*—a range (quantity) of UPD ports 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).

4.1.9 Network Services

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

- *Enable*—enables time synchronisation via NTP.
- *Time server (NTP)*—the IP address or host name of the NTP server.
- *Timezone*—configuration of the time zone and GMT (Greenwich Mean Time) offset:
  - *Manual mode*—defines the GMT offset.
  - *Automatic mode*—this mode allows selection of device location; the GMT offset will be determined automatically. This mode also enables automatic switch to daylight saving time.
- *Synchronisation period (min)*—an interval between synchronisation requests.

- *Save*—saves changes.
- *Cancel*—discards changes.

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

4.1.9.1 SNMP Settings

SMG firmware enables device status monitoring via SNMP. The SNMP submenu allows configuration of SNMP agent settings.

SNMP monitoring allows the following parameters to be requested from the gateway:
- *gateway name;*
- *device type;*
- *firmware version;*
- *IP address;*
- *E1 streams statistics;*
- *IP submodules statistics;*
- *linksets state;*
- *E1 stream channels state;*

- *IP channels state (statistics for the current calls via IP).*

Statistics of the current calls performed via IP channels includes the following data:

- *channel number;*
- *channel state;*
- *call identifier;*
- *caller MAC address;*
- *caller IP address;*
- *caller number;*
- *callee MAC address;*
- *callee IP address;*
- *callee number;*
- *channel engagement duration.*

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

- – *Apply*—applies the changes.
- – Reset—discards the settings.

4.1.9.2 SNMP Trap Configuration

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

The SNMP agent sends an SNMPv2-trap message in case of the following events:

- *configuration error;*
- *SIP module failure;*
- *IP submodule failure;*
- *linkset failure;*
- *SS-7 signal channel failure;*
- *synchronisation loss or synchronisation from a lower priority source;*
- *E1 stream failure;*
- *remote stream failure;*
- *configuration error fixed;*
- *SIP-T module restored after a failure;*
- *IP submodule restored after a failure;*
- *linkset restored after a failure;*
- *SS-7 signal channel restored after a failure;*
- *synchronisation from a higher priority source restored;*
- *no stream failure (after a failure or remote failure);*

- FTP server is unavailable, RAM utilisation for storing CDR files exceeds 50% (15–30 MB);

- *FTP server is unavailable, RAM utilisation for storing CDR files is less than 50% (5–15 MB);*

- *FTP server is unavailable, RAM utilisation for storing CDR files is below 5 MB;*

- *firmware update or configuration file upload/download status.*

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

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

- — *Add;*
- — *Edit;*
- — *Remove.*

- *Type*—type of the SNMP message (TRAPv1, TRAPv2, INFORM).

- *Community*—the password contained in traps.

- *IP address*—IP address of the trap recipient.

- *Port*—UDP port of the trap recipient (default port: 162).

4.1.9.3 FTP Server

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

- *cdr*—a directory with CDR files.

- *log*—a directory with tracing files and other debug data.

- *mnt*—a directory with files located on external storage devices (SSD drives, USB flash drives).

4.1.9.4 FTP Server Settings

- *Enable*—enables/disables the local FTP server.

- *Network interface*—the network interface selected for the FTP server.

- *Port*—the TCP port selected for the FTP server.

SMG digital gateway

- *Authorization timeout, sec*—a timeout for subscriber authorisation on the FTP server; when the timeout expires, the server forces connection termination.
- *Idle timeout, sec*—a timeout for user idle status on the FTP server; when the timeout expires, the server forces connection termination.
- *Session timeout, sec*—duration of a session.

4.1.10 User Configuration

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

- *Name*—username.
- *Password*—user password.
- *Access to log*—log directory access configuration, read/write.
- *Access to mounts*—mnt directory access configuration, read/write.
- *Access to CDR*—CDR directory access configuration, read/write.

4.1.11 Security

4.1.11.1 SSL/TLS Configuration

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

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

Generate New Certificates

☑ **These parameters should be entered in Latin characters.**

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

4.1.11.2   Fail2ban

Fail2ban—a utility that monitors logs files for attempts to access various services. When fail2ban discovers repeated unsuccessful access attempts from the same IP address/host, it blocks all further access attempts from this IP address/host.

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

- Brute forcing authentication data—reception of REGISTER requests from a known IP address but containing wrong authentication data.
- Reception of requests (REGISTER, INIVITE, SUBSCRIBE, and others) from an unknown IP address.
- Reception of unknown requests via SIP port.

Fail2ban Parameters

- Enable—launches Fail2ban utility.
- Block time, seconds—time in seconds during which access from a suspicious address will be banned.
- Access attempts before blocking—the maximum number of host's unsuccessful access attempts to a server before the host is banned by fail2ban.

White list (the last 30 records)—a list of IP addresses that cannot be banned by fail2ban.
Black list (the last 30 records)—a list of permanently banned addresses. A device may have up to **8,192** records in total.

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

An IP address or a subnet can be specified.

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

AAA.BBB.CCC.DDD/mask

Example

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

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

List of banned addresses—a list of addresses banned by fail2ban.

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

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

4.1.11.3 Firewall Profiles

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

Firewall Profiles

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

     Add;
     Edit;
     Delete.

Firewall profiles

№	Name
0	Firewall Profile #0
1	Firewall Profile #1

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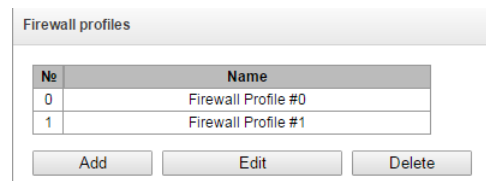
The software allows configuration of firewall rules for incoming, outgoing and transit traffic, as well as for specific network interfaces.

Firewall profiles

Firewall profile 0

Profile settings	
Name	Firewall Profile #0

Save	Cancel

Rules for ingress traffic

№	Name	Status	Packet source	Ports	Destination address	Ports	Protocol	Action
0	Firewall rule 0	Enable	45.45.45.45	0	Any	0	Any	Drop
1	Firewall rule 1	Enable	8.8.8.8	0	Any	0	Any	Reject
2	Firewall rule 2	Enable	Any	8000-9000	Any	0	TCP/UDP	Drop

Rulse for egress traffic

№	Name	Status	Packet source	Ports	Destination address	Ports	Protocol	Action
0	Firewall rule 3	Enable	6.8.9.9	0	4.5.6.7	0	Any	Reject

Add	Edit	Delete

Interface
☑ eth0 (eth0)
☐ alt_control (eth0:1)
☐ vlan (eth0.609)

Save

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

- *Name*—rule name.

- *Enable*—defines whether the rule is used. When unchecked, the rule is inactive.

- *Traffic type*—type of traffic for the rule being created:
    - *egress*—intended for SMG;
    - *ingress*—sent by SMG.

- *Packet source*—defines the network address of the packet source either for all addresses or for a particular IP address or network:
    - *any*—for all addresses (the checkbox is checked);
    - *IP address/mask*—for a particular IP address or network. The field is active when the *any* checkbox is unchecked. The mask is mandatory for a network, but optional for an IP address.

Firewall profiles

Firewall rule	
Name	Firewall rule 3
Enable	☐
Traffic type	Egress ▼
Packet source	☑ Any
IP-address/mask	6.8.9.9
Source ports	0
Destination ports	☑ Any
IP-address/mask	4.5.6.7
Destination protocols	0
Protocol	Any ▼
ICMP message type	any ▼
Action	Accept ▼

Save   Cancel

- *Source ports*—a TCP/UDP port or port range (defined with a hyphen "-") of the packet source. This parameter is used for TCP and UDP only; thus, select UDP, TCP, or TCP/UDP in this field to make it active.

- *Destination address*—defines the network address of the packet recipient either for all addresses or for a particular IP address or network:
    - *any*—for all addresses (the checkbox is checked);
    - *IP address/mask*—for a particular IP address or network. The field is active when the *any* checkbox is unchecked. The mask is mandatory for a network, but optional for an IP address.

- *Destination ports*—a TCP/UDP port or port range (defined with a hyphen "-") of the packet recipient. This parameter is used for TCP and UDP only; thus, select UDP, TCP, or TCP/UDP in this field to make it active.

- *Protocol*—the protocol the rule will be used for: UDP, TCP, ICMP, or TCP/UDP.

- *ICMP Message type*—the ICMP message type the rule will be used for. This field is active, when ICMP is selected in the *Protocol* field.

- *Action*—an action executed by the rule:
    - *ACCEPT*—the packets corresponding this rule will be accepted by the firewall.
    - DROP—the packets corresponding this rule will be rejected by the firewall without informing the party that has sent them.
    - REJECT—the packets corresponding this rule will be rejected by the firewall. The party that has sent the packet will receive either a TCP RST packet or "*ICMP destination unreachable*".

A created rule is placed into the corresponding section: "*Incoming traffic rules*", "*Outgoing traffic rules*" or "*Transit traffic rules*".

Also, the firewall profile allows specification of the network interfaces the rules of the profile will be applied to.

Every network interface can be used only in a single firewall profile at a time. As soon as a network interface is assigned to a new profile, it is removed from the old one.

To apply the rules, click the *Apply* button that appears when changes are made into the firewall settings.

4.1.11.4 List of Allowed IP Addresses

This section allows configuration of the list of IP addresses allowed to be used by administrator to connect to the device via web interface and the Telnet/SSH protocols. By default, all addresses are allowed.

White addresses list
White addresses list
☐ Access only from allowed IP-addresses
Allowed addresses list
Add
Apply	Confirm

- *Access only for allowed IP addresses*—when checked, the list of allowed IP addresses is used; otherwise, access is allowed from any address.

- Apply—applies changes.
- Confirm—commits changes.

To create or remove a list of allowed addresses, use the following buttons:
- *Add*;
- — *Remove*.
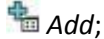
Upon configuration of a list of addresses, click the *Apply* and *Commit* buttons; failing to confirm the changes in 60 seconds restores the previous values. This allows user protection from loss of access to the device.

4.1.12 Network Utilities

4.1.12.1 PING

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

PING
IP Probing
	Ping
...
Periodic ping
Run at startup	☐
Period, min	10
Attempts	3
Save
Status
Periodical ping is not started!
Start	Stop	Information
IP-addresses list
Empty list
	Add

IP Probing—used for a single-time check of 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 the 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.

IP Probing
192.168.27.7	Ping
PING 192.168.27.7 (192.168.27.7): 56 data bytes
--- 192.168.27.7 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
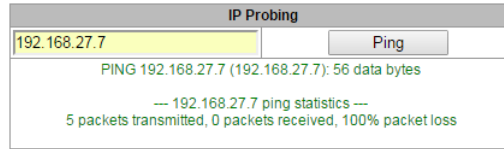
Periodic ping—used for periodic check of device network connection.

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

Status

- *Start—launches/restarts periodic ping.*
- *Stop—forcedly stops periodic ping.*
- *Information—click this button to view the /tmp/log/hosttest.log log file which contains data on the last attempt of periodic ping request transmission.*

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

To add a new address to the list, select it in the entry field and click the Add button. To remove an address, click the Remove button next to the required address.

4.1.13 RADIUS Configuration

4.1.13.1 RADIUS Servers
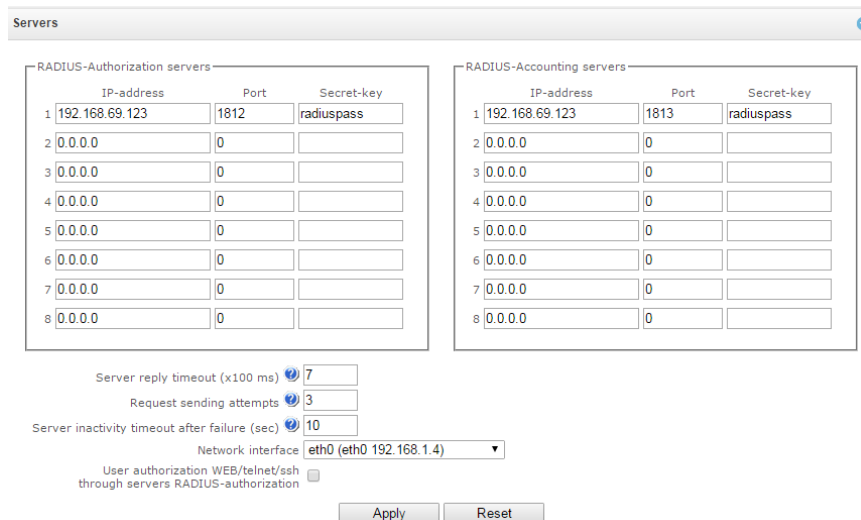
The device supports up to 8 authorisation servers and up to 8 accounting servers.

- *Server reply timeout—amount of time to wait for a server response.*

- *Request sending attempts*—the number of request retries to a server. When all attempts are used, the server will be deemed inactive and the request will be forwarded to another server if it is specified; otherwise, an error will be detected.

- *Server inactivity timeout after failure (sec)*—amount of time when a server is deemed unavailable (requests will not be sent to it).

- *Network interface*—the selected network interface to send RADIUS packets from.

- *User authorisation WEB/telnet/ssh through servers RADIUS-authorization*—enables authorisation on the RADIUS server when a user tries to access the device via web interface, Telnet, or SSH. When login/password are entered, an Access-Request packet is sent to the RADIUS server. In case of success authorisation, the server replies with Access-Accept and the user is allowed to access the device; otherwise, access is denied*.

4.1.13.2 Profile List

Profile Parameters

- Enable RADIUS-Authorization—enables/disables transmission of authentication/authorisation (Access Request) messages to the RADIUS server.

- Enable RADIUS-Accounting—enables/disables transmission of accounting (Accounting Request) messages to the RADIUS server.

Modification Parameters

- Modifiers for InCdPN—*the selected callee (CdPN) number modifier for the incoming connection in relation to the* Called-Station-Id, xpgk-dst-number-in *fields of RADIUS-Authorization and RADIUS-Accounting messages.*

- Modifiers for InCgPN—*the selected caller (CgPN) number modifier for the incoming connection in relation to the* Calling-Station-Id, xpgk-src-number-in *fields of RADIUS-Authorization and RADIUS-Accounting messages.*

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

- Modifiers for OutCgPN modifiers—*the selected caller (CgPN) number modifier for the outgoing connection in relation to the* xpgk-dst-number-out *field of RADIUS-Authorization and RADIUS-Accounting messages.*

RADIUS-Authorization settings

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

- on ingress seize;
- on end-of-dial (full number dial reception).

In case of a server fault (no response from the server), the outgoing communications can be restricted:

- no restrictions—allows all calls;
- local and zone networks only—allows calls to special services, local and zone network;
- local network only—allows calls to special services and local network;
- emergency only—allows calls to special services only;
- deny all—denies all calls.

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

- USER-NAME field—the selected value of the User-Name attribute in the corresponding Access Request authorisation packet (RADIUS-Authorization):
  - CgPN—uses the calling party phone number as the value;
  - IP or E1-stream—uses the calling party IP address or incoming connection stream number as the value;
  - Trunk name—uses incoming connection trunk name as the value.

- USER-PASSWORD field—specifies the value of the User-Password attribute in the corresponding RADIUS-Authorization packet.

- Session time—*limits the maximum call duration*:
  - Ignore—*the maximum call duration is not limited*;
  - Consider Session-Time—*uses the* Session-Timeout(27) *value to limit the maximum call duration*;
  - Consider Cisco h323-credit-time—*uses the* Cisco VSA (9) h323-credit-time(102) value *to limit the maximum call duration*;
  - Session-Time priority—*if the server response has both parameters specified* (session-time *and* Cisco h323-credit-time), session-time *is used and* Cisco h323-credit-time *is ignored*.
  - Cisco h323-credit-time priority—*if the server response has both parameters specified* (session-time *and* Cisco h323-credit-time), Cisco h323-credit-time *is used and* session-time *is ignored*.

The SMG gateway can use the *Session-Timeout* or *Cisco VSA h323-credit-time* values from the Access-Accept packet in order to limit the maximum duration of an authorised call.

- *Enable emergency call on receiving Reject* — when Access-Reject is received from the server, calls to the special services node are allowed.

Optional Attributes of Authentication-Request Packets

- *NAS-Port-Type*—NAS physical port type (a server for user authentication), the default value is Async.
- *Service-Type*—type of the service, not used by default (Not Used).
- *Framed-protocol*—the protocol specified for packet access utilisation, not used by default (Not Used).

RADIUS-Accounting settings

Send Requests

- *accounting-start*—sends an *accounting* start packet that notifies the RADIUS server on call start.
- *accounting-stop*—sends an *accounting* stop packet that notifies the RADIUS server on call end.
- *accounting-stop for unsuccessful calls*—sends information on unsuccessful calls to the RADIUS server.
- *accounting-update with period*—during a call, periodically sends an *update* packet to the RADUIS server to notify the RADIUS server on active state of the call.
- *accounting for call-origin=answer*—sends information about the outgoing part of a call to the RADIUS server.

The *Call Origin* field in case of CISCO—sends "*answer"* for the incoming part of a call, and "*originate*" for the outgoing part.

In case of a server fault (no response from the server), the outgoing communications can be restricted:

- no restrictions—allows all calls;
- local and zone networks only—allows calls to special services, local and zone network;
- local network only—allows calls to special services and local network;
- emergency only—allows calls to special services only;
- deny all—denies all calls.

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

- *USERNAME field—the* selected User-Name value in an Accounting Request packet (RADIUS-Accounting):
    - CgPN—*uses the calling party phone number as the value;*
    - IP or E1-stream—*uses the calling party IP address or incoming connection stream number as the value;*
    - Trunk name—*uses incoming connection trunk name as the value.*
- *CdPN field*—the selected value of the callee number used for RADIUS packet generation for specific Attribute-Value pairs (see section 4.1.13.3):
    - CdPN-in—*uses the callee number prior to modification (the number received in the SETUP/INVITE packet);*
    - CdPN-out—*uses the callee number after modification.*
- CgPN field—the selected value of the caller number to be used for RADIUS packet generation for certain Attribute-Value pairs (see section 4.1.13.3):
    - CgPN-in—*uses the caller number prior to modification (the number received in the SETUP/INVITE packet).*
    - CgPN-out—*uses the caller number after modification.*

4.1.13.2.1 RADIUS Packet Format

Each packet description includes descriptions of every Attribute-Value pair for this packet type. Attributes may be either standard or vendor specific. If the attribute value is unknown for any reason (e. g. if the outgoing trunk is missing, it is impossible to identify the CdPN_OUT variable value, which is used as a value for some attributes), then the attribute is not included into the message.

Standard attributes have the following description:

Attribute name (attribute number): attribute value

Vendor attributes:

Attribute name (attribute number): vendor name (vendor number): VSA name (VSA number): VSA value

where:

> **Attribute name**—always Vendor-Specific;
> **Attribute number**—always 26;
> **Vendor name**—name of the vendor;
> **Vendor number**—the vendor number assigned by IANA in the PRIVATE ENTERPRISE NUMBERS document (http://www.iana.org/assignments/enterprise-numbers);
> **VSA name**—vendor attribute name;
> **VSA value**—vendor attribute value.

> ✔ *<$NAME> can be used* as an attribute value, where *NAME* is a variable name. **For description of variable values, see section 4.1.13.3.**

Access-Request Packet
> User-Name(1): <$USER_NAME>
> User-Password(2): based on the "eltex" password (without quotation marks)
> NAS-IP-Address(4): <$SMG_IP>
> Called-Station-Id(30): <$CdPN_IN>
> Calling-Station-Id(31): <$CgPN_IN>
> Acct-Session-Id(44): <$SESSION_ID>
> NAS-Port(5): <$NAS_PORT>
> NAS-Port-Type(61): Virtual(5)
> Service-Type(6): Call-Check(10)

Accounting-Request Start Packet
> Acct-Status-Type(40) – Start(1)
> User-Name(1): <$USER_NAME>
> Called-Station-Id(30): <$CdPN>
> Calling-Station-Id(31): <$CgPN_IN>
> Acct-Delay-Time(41): according to RFC2866
> Event-Timestamp(55): according to RFC2869
> NAS-IP-Address(4): <$SMG_IP>
> Acct-Session-Id(44): <$SESSION_ID>
> Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-src-number-in=<$CgPN_IN>
> Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-src-number-out=<$CgPN_OUT>
> Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-dst-number-in=<$CdPN_IN>
> Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-dst-number-out=<$CdPN_OUT>
> Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-route-retries=<$ROUTE_RETRIES>
> Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): h323-remote-id=<$DST_ID>Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): h323-call-id=<$CALL_ID>
> Vendor-Specific(26): Cisco(9): h323-remote-address(23): h323-remote-address=<$DST_IP>
> Vendor-Specific(26): Cisco(9): h323-conf-id(24): h323-conf-id=<$CALL_ID>
> Vendor-Specific(26): Cisco(9): h323-setup-time(25): h323-setup-time=<$TIME_SETUP>
> Vendor-Specific(26): Cisco(9): h323-call-origin(26): h323-call-origin=originate
> Vendor-Specific(26): Cisco(9): h323-call-type(27): h323-call-type=<$CALL_TYPE>

Vendor-Specific(26): Cisco(9): h323-connect-time(28): h323-connect-time=<$TIME_CONNECT>
Vendor-Specific(26): Cisco(9): h323-gw-id(33): h323-gw-id=<$SMG_IP>

Accounting-Request Stop Packet

Acct-Status-Type(40) – Stop(2)
User-Name(1): <$USER_NAME>
Called-Station-Id(30): <$CdPN>
Calling-Station-Id(31): <$CgPN_IN>
Acct-Delay-Time(41): according to RFC2866
Event-Timestamp(55): according to RFC2869
NAS-IP-Address(4): <$SMG_IP>
Acct-Session-Id(44): <$SESSION_ID>
Acct-Session-Time(46): <$SESSION_TIME>
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>

Access-Accept Packet

When an Access-Accept packet is received from the RADIUS server, the call is considered as authorised. Then, a search for an outgoing trunk is performed and, if successful, an attempt to establish the connection is made.

If the *Session-Time(27)* attribute or the *Cisco VSA (9) h323-credit-time(102)* attribute has been transferred in a packet and the corresponding setting is specified in the RADIUS profile, the attribute value is used to limit the maximum call duration. When this timeout expires, SMG will terminate the connection.

4.1.13.3 Variable Description

Variable	Description and Possible Values
$CALL_TYPE	Is defined depending on the transmission medium the outgoing trunk belongs to: • *Telephony*, if the outgoing trunk is PSTN (TDM); • *VoIP*, if the outgoing trunk is VoIP.
$CdPN	Is determined based on SMG settings: • $CdPN = $CdPN_IN [by default]; • $CdPN = $CdPN_OUT
$CdPN_IN	Callee number before modification (received in SETUP/INVITE)
$CdPN_OUT	Caller number after modification (sent to the called party in
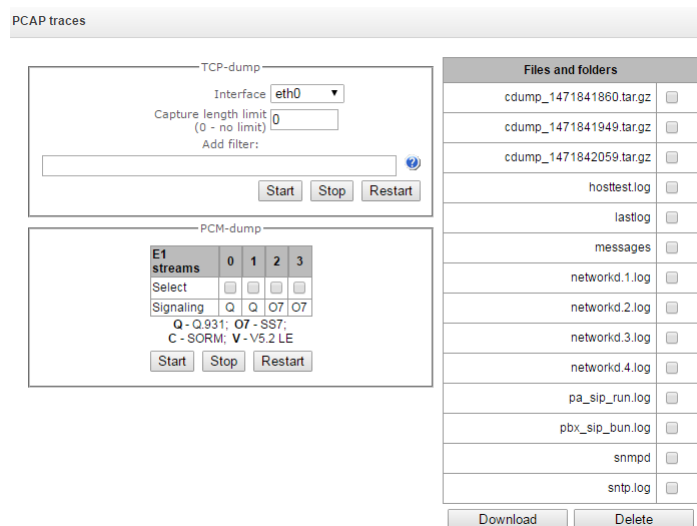
	SETUP/INVITE)
$CgPN_IN	Caller number before modification (received in SETUP/INVITE)
$CgPN_OUT	Caller number after modification (sent to the called party in SETUP/INVITE)
$DISCONNECT_CAUSE	Q.850 cause for call clearing
$DST_ID	Outgoing trunk name for this call
$DST_IP (string)	IP address of the terminating device if the outgoing trunk is VoIP, e. g.: 192.168.0.1
$LOCAL_DISCONNECT_ CAUSE	A local reason for call clearing; values: • 1—connection to the callee has been established (User-Answer); • 2—wrong or incomplete number format (Incomplete-Number); • 3—the number does not exist (Unassigned-Number); • 4—unsuccessful connection attempt, unknown reason (Unsuccesfull-Other-Cause); • 5—the callee is busy (User-Busy); • 6—equipment fault (Out-of-Order); • 7—no response from the callee (No-Answer); • 8—outgoing trunk is unavailable (Unavailable-Trunk); • 9—RADIUS server authorisation denied (Access-Denied); • 10—no free channels for connection establishment (Unavailable-Voice-Channel); • 11—RADIUS server is unavailable (RADIUS-Server-Unavailable).
$NAS_PORT	(xport.type<<24) + (xport.slot<<16) + (xport.stream<<8) + (xport.cell)
$ROUTE_RETRIES	The current number of the attempt, the count begins with 1 (for the first attempt, respectively)
$SESSION_ID	Session identifier
$SESSION_TIME	Call duration
$SMG_IP	SMG IP address
$SRC_ID	Incoming trunk name for this call
$TIME_SETUP	The time of SETUP/INVITE message arrival in the hh:mm:ss.uuu t www MMM dd yyyy format
$TIME_CONNECT	The reception time of the CONNECT/200 OK message issued by the called party in the hh:mm:ss.uuu t www MMM dd yyyy format
$TIME_DISCONNECT	The reception time of the DISCONNECT/BYE message issued by one of the parties in the hh:mm:ss.uuu t www MMM dd yyyy

	format; if the call is unsuccessful, the time of the message is specified upon reception of which SMG begins the call termination procedure (CANCEL, other)
$USER_NAME	Determined from incoming trunk settings: • <$CgPN_IN>; • source IP address or E1 stream number [by default]; • incoming trunk name.

4.1.14 Tracing

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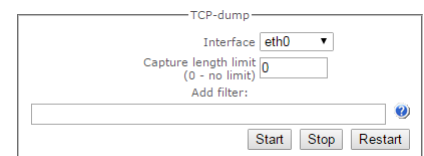
This menu allows configuration of network traffic analysis and the TDM protocol.

TCPdump—settings of the TCP–dump utility:

TCP-dump—a utility to intercept and analyse network traffic.

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

Structure of Filter Expressions

Every expression defining a filter includes a single or multiple primitives, which contain a single or multiple object identifiers and preceding qualifiers. An object identifier may be represented by its name or number.

Object Qualifiers

1. **type**—indicates the object type specified by the identifier. An object type may have the following values:
   host,
   net,
   port.

If an object type is not defined, the **host** value is assumed.

2. **dir**—defines the direction towards the object. This may have the following values:
   src (object is a source),
   dst (object is a destination),
   src or dst (source or destination),
   src and dst (source and destination).

   If the dir qualifier is not defined, the **src or dst** value is assumed.
   To intercept traffic from the **any** artificial interface, the **inbound** and **outbound** qualifiers can be used.

3. **proto**—defines the protocol the packets should belong to. 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 specialised resources.

- *Launch*—begins data collection.
- *Finish*—finishes data collection.
- *Restart*—restarts the utility and begins data collection again.

The Files and Folders section in /tmp/log contains a list of files in the corresponding /tmp/log directory.

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.*

PCM–dump Utility Settings

PCMdump—a utility to intercept and analyse signal traffic via E1 streams. The device enables PCM-dumping either for a single or for multiple streams; for a simultaneous PCM-dumping for multiple streams,

tracing is written to a single file which contains signalling messages from multiple streams; at that, simultaneous PCM-dumping is not available for streams with different signalling protocols.

- *Select*—selects E1 streams.
- *Signalling*—the signalling protocol selected for the stream:
- O7—SS-7;
- Q—Q.931.
- *Start*—begins data collection.
- *Stop*—finishes data collection.
- *Restart*—restarts the utility and begins data collection again.
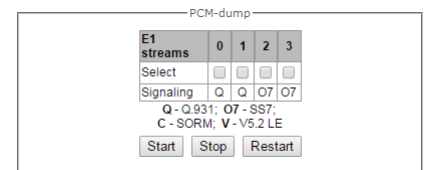
The Files and Folders section in /tmp/log contains a list of files in the corresponding /tmp/log directory.

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*.

4.1.14.2   PBX Tracing

> **Utilisation of IP PBX tracing leads to delays in device operation. This debug mode is RECOMMENDED only if problems in gateway operation occur and their reason should be identified.**
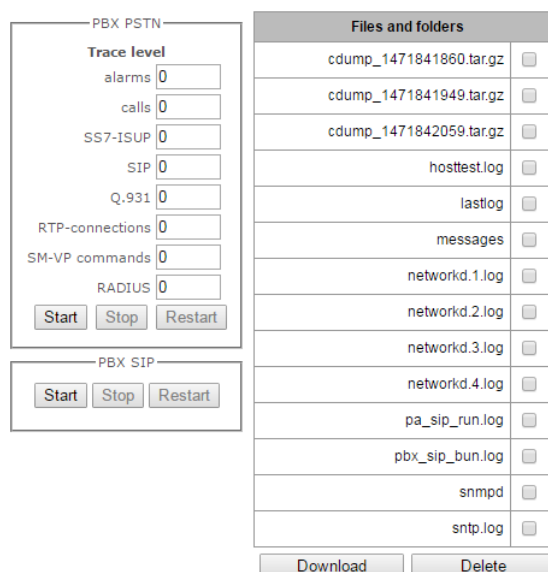
The PBX PSTN section registers operations and interaction in a log, as well as message exchange via various protocols. PBX PSTN parameters allow configuration of tracing levels for various events and protocols.

The PBX IP section registers SIP errors and messages tracing.

- *Start*—begins data collection.
- *Stop*—finishes data collection.
- *Restart*—restarts and begins data collection again.

> **When data collection is stopped, buttons are displayed that allow download of tracing files to a local PC.**

The Files and Folders section in /tmp/log contains a list of files in the corresponding /tmp/log directory.

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*.

4.1.14.3 Syslog Settings

The *SYSLOG* menu allows configuration of system log settings.

SYSLOG is a protocol designed for transmission of messages on current system events. The gateway firmware generates system data logs on operation of system applications and signalling protocols, as well as occurred failures, and sends them to the SYSLOG server.

> **High debug levels may cause delays in device operation.**
> **IT IS NOT RECOMMENDED to use the system log without a due reason.**

> **The system log should be used only when problems in gateway operation occur and their reason should be identified. To determine the necessary debug levels, please contact Eltex Service Centre.**

syslog parameters specify IP address of the syslog server, the UDP port used to receive the syslog server messages, and debug levels according to events and protocols.

Possible levels are as follows: 0—disabled, 1–99—enabled; 1—minimum debug level, 99—maximum debug level.

Output the history of entered commands—saves the history of changes in gateway settings.

- *Server IP address*—the server address where the log of entered commands is sent.

- *Server port*—the server port where the log of entered commands is sent.

- *Detalization level*—verbosity level of the entered commands log:

  - *Disable logging*—disable generation of the entered commands log.
  - *Standard*—messages contain the name of the modified parameter.
  - *Extended*—messages contain the name of the modified parameter as well as parameter values before and after modification.

Syslog settings—configuration settings of the system log.

- *Enable*—when checked, saves events log; otherwise, logging is disabled.

- *Remote logging*—when checked, the system log is stored on a server at the specified address.

- *Server IP address*—address of the server where the system log is stored.

SYSLOG

Traces:
Server IP-address ❓ 192.168.1.123
Server Port ❓ 514
Send data for alarms 0
calls 0
SS7-ISUP signaling 0
SIP signaling 0
Q.931 signaling 0
RTP info 0
SM-VP info 0
RADIUS messages 0
[Apply]

Configuration changes logging:
Server IP-address 0.0.0.0
Server Port ❓ 514
Detalization level [Disable logging ▼]
[Apply]

Syslog settings:
Enable ☑
Remote logging ☑
Server IP-address 192.168.1.123
Server Port ❓ 514
[Apply]
Syslog is not running
[Start] [Stop]

- *Server port*—the server port the system log will be sent to.

4.1.15 Working with Objects and the **Objects** *menu*

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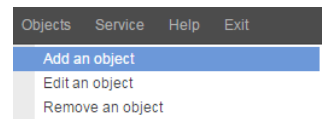
4.1.16 Saving Configuration and the **Service** *menu*

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

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

To restart the device firmware, select the *Service—Firmware Restart* menu item.

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

To perform forced time re-synchronisation with the NTP server, select the *Service— Restart NTP Client* menu item.
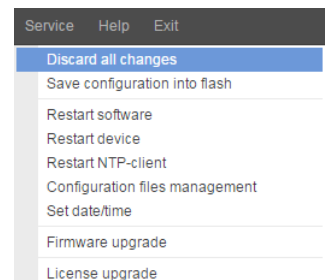
To read/write the main device configuration file, select the *Service— Configuration Files Management* menu item.

To configure the local date and time manually, select the *Service—Date and Time Configuration* menu item; see section **4.1.17.**

To update the firmware via web interface, select the *Service—Firmware Update* menu item; see section **4.1.18.**

To update/add licences, select the *Service—Licence Update* menu item; see section **4.1.19.**

4.1.17 Time and Date Settings

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

To save settings, use the *Apply* button.

Click the *Synchronise* button to synchronise the device system time with the current time on a local PC.
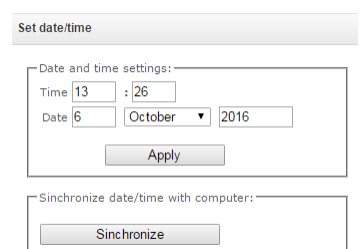
4.1.18 Firmware Upgrade via Web Interface

To upgrade the device firmware, use the *Service—Firmware Upgrade* menu item.

The firmware file upload form opens.

- Firmware upgrade—updates firmware of the control program and/or Linux kernel.

To update the firmware, use the *Browse* button to specify the
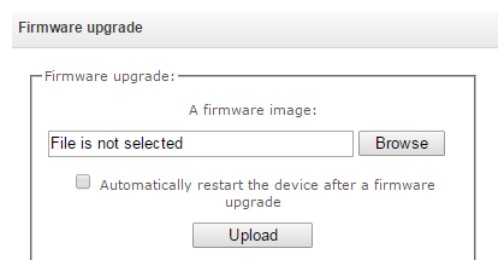
update file name in the *Firmware File* field and click *Upload*. When the operation is completed, restart the device using the *Service—Device Restart* menu item.

4.1.19 Licence Renewal

To update/add licences, contact Eltex Marketing Department by email eltex@eltex.nsk.ru or phone +7 (383) 274-48-48 to obtain a licence file. Specify the serial number and MAC address of your device (see section **4.1.22**).

Next, select the *Licence Update* parameter from the *Service* menu.
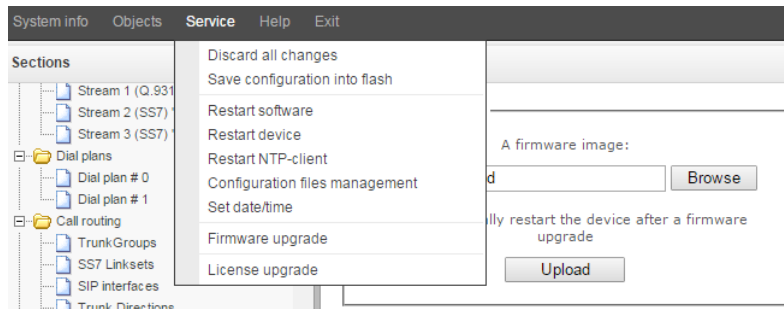
Use the *Select File* button to specify the path to the licence file obtained from the manufacturer and update it by clicking *Update*.

Licence file update requires confirmation.
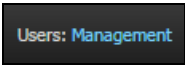
When the operation is complete, the system prompts you to restart the device. This can also be done manually in the *Service—Device Restart* menu.

4.1.20 Help Menu

The menu provides data on the current versions of the web configurator *(About)* and firmware, factory settings, and other system information *(System Information)*.
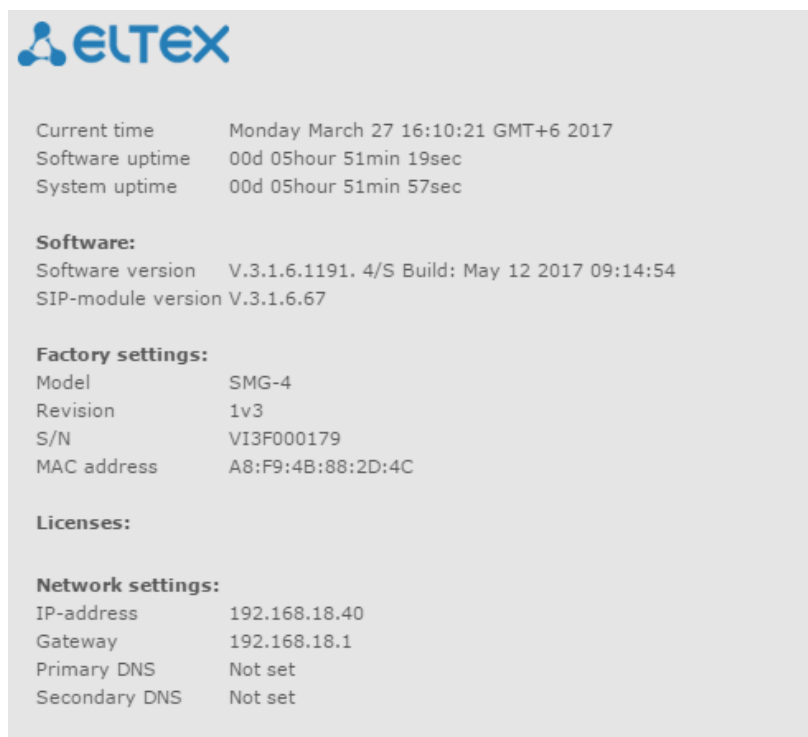
4.1.21 Password Configuration for Web Configurator Access

The link ![Users: Management] is intended for handling the passwords which are used in the web configurator to access the device.

Configuration of Web Interface Administrator Password

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

To save the configuration, use the *Service—Save Configuration* menu item.
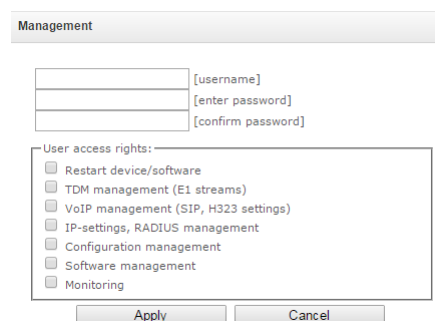
Web Interface Users

This section allows configuration of web interface access restrictions for users. A system administrator can always add or remove users and define their access level.

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

- ![icon] — *Add User*;
- ![icon] — *Edit User Parameters*;
- ![icon] — *Remove User*.

The program allows neither modification of administrator permissions nor his removal from the user list that ensures access to the program for system administrators at any time.

- [*username*]—the username to log in the web interface.
- [*enter password*]—the password to access the web interface.
- [*confirm password*]—used to confirm the password to access the web interface.

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

Configuration of Administrator Password for Telnet and SSH

This section is used to change the password for Telnet, SSH, and console access.

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

4.1.22 View Factory Settings and System Information

To view factory settings and system information, use the *Help—System Information* menu item.

The factory settings are also specified on the label located in the lower part of the device casing.

To view the detailed system information (factory settings, SIP adapter version, current date and time, uptime, network settings, internal temperature), click the *System Information* link in the control panel.

4.1.23 Configurator Exit

Click the *Exit* link to exit the configurator; the following window will open in your browser:
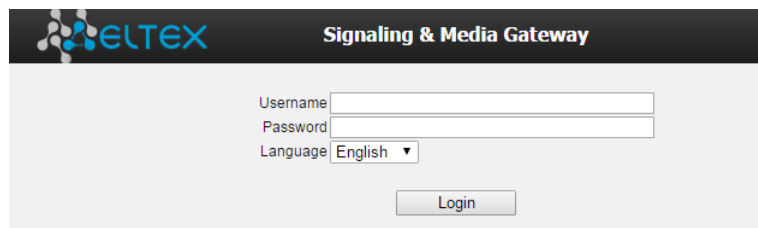
To resume access, specify the defined username and password and click the *Sign In* button. To exit the configurator, click the *Cancel* button.

4.2 Command Line, List of Supported Commands and Keys

SMG features several debug terminals with specific functions:

- *Terminal (com port)*—enables device configuration and firmware update via CLI (command line interface).
- *Telnet port 23*—terminal duplicate (com port).
- *SSH port 22*—terminal duplicate (com port).

4.2.1 System of Commands for SMG Gateway Operation in the Debug Mode

To enter the debug mode, connect to CLI and enter the *tracemode* command.

help	Show the list of available commands
quit	Exit the debug mode
logout	Exit the debug mode
exit	Exit the debug mode
history	Show the list of previously entered commands
radact [on/off]	Turn RADIUS on/off

SMG digital gateway

radshow	Show the list of requests to the RADIUS server
rstat	Show the RADIUS protocol operation statistics
msploopext	Set traffic loop on the VoIP submodule to test packets passing through it; the packets are generated by an external device
msploopint	Set traffic loop on the VoIP submodule to test packets passing through it; the packets are locally generated on SMG
msploopstop	Cancel traffic loop on the VoIP submodule
q931timers	Show Q.931 timer values
resolve	Check domain name resolution. Parameter: domain name
route	Show information on network routes processed by telephony
netiface	Information about network interface
showcall	Show information on currently active calls
licence	Show information on currently active licences
mspping [on/off] <idx>	Enable/disable signal processor querying; idx—signal processor number—0
stream [stream]	Show the status of E1 streams or a specific stream, *stream* is the stream number (0–3)
e1stat <stream>	Show E1 stream counters
e1chip	Version and type of the chip processing E1 streams
alarm	Show alarm log information
sync	Show information on synchronisation sources
syncfreq	Show information on synchronisation frequency
setsync	Forced synchronisation source change. Parameter: <stream number>
checkmod	Check the number modifier operation for a specific number. Parameters: <modifier table> <the phone number to be checked>
cic <linkset>	Show the status of channels in the line group, <linkset> is the number of SS-7 line group
checknum	Check the number with the numbering schedule
cfg_read	Apply the current configuration; this command resets and re-initialises E1 streams
callref	Show information on active SIP calls
rtpdebug <level>	Enable switch RTP debugging; <level> is a debug level **WARNING!** This command may cause the switch to become unresponsive under load
mspcports	Show RTP port status
mspshow/mspcshow	Show signal processor connection statistics
mspreglog	Enable signal processor command tracing
mspunreglog	Disable signal processor command tracing
talk	Show call statistics

frmtrace	Enable low-level tracing for E1 signal streams. Parameters: <level> <stream number> <usage>
	   – level: l1, l2, l3;
	   – usage: 1—enabled, 0—disabled.

sys	Show system information, firmware version
trace	Tracing functions
regcon	This command returns to normal operation after the *unregcon* command (if the application has not terminated abnormally)
unregcon	This command is used in extreme cases to identify the accurate location of the application abnormal termination
stop	Restart the firmware

4.2.2   *Tracing Commands Available Through the Debug Port*

4.2.2.1 Enable Debugging Globally

Command syntax: **trace start**

4.2.2.2 Disable Debugging Globally

Command syntax: **trace stop**

4.2.2.3 Enable/Disable Debugging for Specific Arguments

Command syntax: **trace** <POINT> **on/off** <IDX> <LEVEL>

Parameters:

 <POINT>   argument;
<IDX>   numeric parameter;
<LEVEL>   debug level.

Acceptable arguments (*<POINT>*):

<POINT> Value	*Command Description*	*<IDX> Value*
hwpkt	Tracing of packet contents at the first level of exchange between the main application and the E1 stream driver	0..3
stream	E1 stream tracing	0..3
port	Application operation tracing	Not used
isup	ISUP subsystem operation tracing in the SS-7 protocol	Not used
mtp3	MTP3 level operation tracing in the SS-7 protocol for an E1 stream	0..3
sipt	SIP/-T/-I protocol operation tracing	Not used
pril3	DSS1 protocol third level operation tracing for an E1 stream	0..3
sw	Switch network operation tracing	Not used
mspc	IP forwarding tracing	Not used
mspd	Signal processor operation tracing	0
net	Tracing of the 2nd layer data network operation	Not used
sync	Tracing of synchronisation sources operation	Not used
erl1	Low-level tracing of the system which transfers messages between the application and the SIP module	Not used
erl3	High-level tracing of the system which transfers messages between the application and the SIP module	Not used
snmp	SNMP protocol operation tracing	Not used
np	Numbering (routing) schedule operation tracing	Not used
mod	Modifier operation tracing	Not used
alarm	Gateway fault state tracing	Not used
radius	RADIUS protocol operation tracing	Not used

4.3   **SMG Configuration via Telnet, SSH, or RS-232**

To configure the device, connect to it via the Telnet or SSH protocol, or by the RS-232 cable (for access via CLI). Factory settings for IP address: **192.168.1.2**; mask: **255.255.255.0**.

The device configuration is stored in text files located in the **/etc/config** directory. The files can be edited in the *joe* integrated text editor (the changes will take effect after device restart).

Modifications made to configuration via CLI (command line interface) or the web configurator will be applied immediately.

To save the configuration into the non-volatile memory of the device, execute the **save** command.

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

Given below is a complete list of commands sorted in the alphabetic order.

4.3.1   List of CLI Commands

Command	Parameter	Value	Action
?			Show the list of available commands
alarm global			Show information on the current faults
alarm list clear			Clear the fault events log
alarm list show			Show the fault events log with fault type and status, occurrence time, and localisation parameters.
Config			Enter the device configuration mode
CPU load statistic			Show CPU load for the last minute
date	<DAY>	1-31	Set the device local date and time
	<MONTH>	1-12	
	<YEAR>	2011-2037	
	<HOURS>	00-23	
	<MINS>	00-59	
exit			Terminate this CLI session
firmware update tftp	<FILE>	firmware file name	Firmware update without automatic gateway restart *FILE*—firmware file name *SERVERIP*—IP address of the TFTP server:
	<SERVERIP>	IP address in the AAA.BBB.CCC.DDD format	
firmware update ftp	<FILE>	firmware file name	Firmware update without automatic gateway restart *FILE*—firmware file name *SERVERIP*—IP address of the FTP server
	<SERVERIP>	IP address in the AAA.BBB.CCC.DDD format	
firmware update usb	<FILE>	firmware file name	Firmware update without automatic gateway restart *FILE*—firmware file name
firmware update_and_reboot tftp	<FILE>	firmware file name	Firmware update with automatic gateway restart *FILE*—firmware file name

	<SERVERIP>	IP address in the AAA.BBB.CCC.DDD format	*SERVERIP*—IP address of the TFTP server:
firmware update_and_reboot ftp	<FILE> <SERVERIP>	firmware file name IP address in the AAA.BBB.CCC.DDD format	Firmware update with automatic gateway restart *FILE*—firmware file name *SERVERIP*—IP address of the FTP server
firmware update_and_reboot usb	<FILE>	firmware file name	Firmware update with automatic gateway restart *FILE*—firmware file name
History			Show the history of entered commands
license demo	<ON OFF>	SIP-Registrar/SORM on/off	Check the licence availability for the device (*License installed*—licence is installed; *License NOT installed*—licence is not installed) Activate demo-license.
license download	<FILE> <SERVERIP>	License file name Server IP address in the AAA.BBB.CCC.DDD format	Download a licence file from the specified address
license reset	<YES_NO>	no/yes	Reset the license
license update			Update the licence
management			Enter the SS-7 stream management mode
md5sum	<FILE>	file name	Calculate MD5sum for file from the */tmp/log* folder
number check	<NUMPLAN> <NUMBER> <COMPLETE>	0-15 String, 31 characters max. yes/no	Check routing capability for this number The check is performed by the caller and callee masks and also in the configured SIP subscriber database. The check provides information on routing capability for this number in the specified numbering schedule: *calling-table*—routing by the caller table; *called-table*—routing by the callee table; *NOT found in*—routing by this table is not possible; *found in*—routing by this table is possible; *Prefix [6]*—routing by a prefix [the prefix number in the list].
password			Change access password via CLI
pcmdump	<STREAM>	0-15	Collect packets from the specified E1 stream.

SMG digital gateway

	<FILE>	string	
			STREAM—the number of the stream for capture
			FILE—file for writing
quit			Terminate this CLI session
reboot	<YES_NO>	yes/no	Reboot the device
save			Write the current configuration into the non-volatile memory of the device
sh			Go to Linux Shell from CLI
show system info			Show system information
show environment			Show data from temperature sensors
sntp retry			Send an SNTP request to the server for time synchronisation
statistic			Enter the statistics view mode
tcpdump	<DEVICE> <FILE> <SNAPLEN>	eth0/eth1/local string 0-65535	Capture packets from the Ethernet device DEVICE—an interface for monitoring FILE—a file for packet writing SNAPLEN—the number of bytes captured from each packet (0— the entire packet is captured).
tftp put	<LOCAL_FILE> <REMOTE_FILE> <SERVERIP>	string string IP address in the AAA.BBB.CCC.DDD format	Get a file via TFTP. This command is used to download the tracings made by the tcpdump and pcmdump commands
timezone set	<TIMEZONE>	GMT/ GMT+1/GMT-1/ GMT+2/GMT-2/ GMT+3/GMT-3/ GMT+4GMT-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)	Set the time zone with respect to UTC TIMEZONE—time shift with respect to UTC
tracemode			Enter the tracing mode

4.3.2 Changing Device Access Password via CLI

Since the gateway allows remote connection via Telnet, it is recommended to change the admin password to avoid unauthorised access.

To do this:

1) Connect to the gateway via CLI, authorise using login/password, enter the *password* command,

and press <Enter>.

2) Enter a new password:

New password:

3) Confirm the entered password:

Retype password:

Password changed (Password for admin changed by root)

4) Save the configuration into Flash: enter the *save* command and press <Enter>.

4.3.3 Statistics Mode

This mode is used to view statistics in accordance with Q.752 ITU-T guideline tables.

4.3.3.1 Entering the Statistics View Mode

Command syntax: **statistic**

4.3.3.2 Entering the MTP (SS-7) Signalling Traffic Viewing Mode

Command syntax: **mtp**

Execution result: Change to MTP statistic mode
                                    SMG4-[STAT]-[MTP]>

4.3.3.3 Parameters of the MTP Traffic Statistics View Commands

<LINK>	E1 stream number;
<LINKSET>	SS-7 line group number;
< TIME1>	time span represented in statistics (hours);
< TIME2>	time span represented in statistics (minutes).

4.3.3.4 View the MTP Traffic General Status

Command syntax: **signalling link allstat** <LINK> <TIME1> <TIME2>

Example: SMG4-[STAT]-[MTP]> signalling link allstat 8 12 0

Meaning: The executed command shows statistics for the 8th E1 stream from all tables in the 12-hours 00-minutes interval.

4.3.3.5 View Signalling Traffic (MTP Message Accounting)

Q.752 ITU-T guidelines, Table 15

Command syntax: **message accounting** <LINK> <TIME1> <TIME2>

Example: SMG4-[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: The executed command shows the MTP signalling traffic volume for the
                                    8th E1 stream in the 12-hours 00-minutes interval.

4.3.3.6 View MTP Signalling Link Faults and Performance Counters

Q.752 ITU-T guidelines, Table 1

Command syntax: **signalling link faults_and_performance** <LINK> <TIME1> <TIME2>

Example: SMG4-[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: The executed command shows signalling link faults and performance
                                    counters for the 8th E1 stream in the 12-hours 00-minutes interval.

4.3.3.7 View the Availability Time of MTP Signalling Link

Q.752 ITU-T guidelines, Table 2

Command syntax: **signalling link availablility** <LINK> <TIME1> <TIME2>

Example: SMG4-[STAT]-[MTP]> signalling link availablility 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: The executed command shows the availability time of signalling link of
                                    the 8th E1 stream in the 12-hours 00-minutes interval.

4.3.3.8 View MTP Signalling Link Utilisation Metrics

Q.752 ITU-T guidelines, Table 3

Command syntax: **signalling link utilization** <LINK> <TIME1> <TIME2>

Example: SMG4-[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: The executed command shows utilisation metrics for the 8th E1 stream in the 12-hours 00-minutes interval.

4.3.3.9 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: SMG4-[STAT]-[MTP]> signalling link availability 0 12 0

Execution result:

```
+-------------------------------------------------------+
|           MTP SL utilization.       Link   08         |
+-------------------------------------------------------+
|      Period:   00:00:00 -  00:00:00 (     0 sec)      |
+-------------------------------------+-----------------+
|  SIF and SIO octets transmitted     |         0       |
+-------------------------------------+-----------------+
|  SIF and SIO octets received        |         0       |
+-------------------------------------+-----------------+
|  MSUs discarded due congestion      |         0       |
+-------------------------------------+-----------------+
```

Meaning: The executed command shows availability metrics for the line group (linkset) and signalling routes for Linkset 0 in the 12-hours 00-minutes interval.

4.3.3.10 View MTP Signalling Point Status

Q.752 ITU-T guidelines, Table 5

Command syntax: **signalling point status** <LINK> <TIME1> <TIME2>

Example: SMG4-[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: The executed command shows signalling point metrics for the 8th E1 stream in the 12-hours 00-minutes interval.

4.3.3.11 Enter the Packet Traffic View Mode

Command syntax: **packets**

Execution result: SMG4-[STAT]-[PACKETS]>

4.3.3.12 View QoS Statistics for Packet Traffic

Command syntax: **show** <TIME1> <TIME2>

Parameters:
<TIME1>   time span represented in statistics (hours);
<TIME2>   time span represented in statistics (minutes).

Example: SMG4-[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: The executed command shows QoS statistics for packet traffic in the 12-hours 00-minutes interval.

4.3.4 Management Mode

To switch to the E1 stream management mode, execute the *management* command.

SMG-4 supports up to 4 E1 streams. Only one E1 stream is available in an SMG-2 device by default. To activate another one, a special licence is required. For more information about licences, see section **4.1.19 Licence Renewal**.

```
SMG4> management
Entering management mode.
SMG4-[MGMT]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
exit			Move to a higher menu level
history			Show the history of entered commands
nslookup	<HOST>	string	Request IP address of the host with the specified name *HOST*—the address to be requested
ping host	<HOST>		Send a PING request to the specified host
ping ip	<IP>	IP address in the AAA.BBB.CCC.DDD format	Send a PING request to the specified IP address
e1 stat clear	<STREAM>	0-3	Reset statistics for the specified E1 stream
e1 stat show	<STREAM>	0-3	Show statistics for the specified E1 stream
e1 test remote_loop	<STREAM>	0-3	Set a remote loop on the specified E1 stream
e1 test prbs	<STREAM>	0-3	Transmit a PRBS sequence to the specified E1 stream
e1 test prbs_local_loop	<STREAM>	0-3	Set a local loop and transmit a PRBS sequence to the specified E1 stream
e1 test off	<STREAM>	0-3	Disable a test/loop on the specified E1 stream
ss7link	<SS7_LINK>	0-3	Proceed to management of parameters of the specified E1 stream
quit			Terminate this CLI session

4.3.4.1 SS-7 Stream Management Mode

To enter this mode, execute the *ss7link <Link>* command in the SS-7 stream configuration mode, where *<Link>* is an SS-7 stream number and may take values in the range of 0–15.

```
SMG4-[MGMT]> ss7link 0
E1[0]. Signaling is SS7
SMG4-[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 group block	<CHAN_INDEX_START> <CHAN_COUNT>	1-31 2-31	Block a group of channels CHAN_INDEX_START the number of the starting E1 channel in the group; CHAN_COUNT the number of channels in the group.
chan group reset	<CHAN_INDEX_START> <CHAN_COUNT>	1-31 2-31	Reset a channel group CHAN_INDEX_START the number of

			the starting E1 channel in the group; CHAN_COUNT the number of channels in the group.
chan group unblock	<CHAN_INDEX_START>	1-31	Unblock a group of channels
	<CHAN_COUNT>	2-31	CHAN_INDEX_START the number of the starting E1 channel in the group; CHAN_COUNT the number of channels in the group.
chan rel	<CHAN_INDEX>	1-31	Terminate connection in the specified channel
chan reset	<CHAN_INDEX>	1-31	Reset the specified channel
chan rlc	<CHAN_INDEX>	1-31	Confirm disconnection in the specified channel
chan unblock	<CHAN_INDEX>	1-31	Unblock the specified channel
exit			Return from this configuration submenu to an upper level
link clr outage			Clear the *CPU local failure* status for a channel
link send LFU			Send the *link forced uninhibit* message to a stream
link send LIN			Send the *link inhibit* message to a stream
link send LUN			Send the *link uninhibit* message to a stream
link set congestion			Set the *overload* status for a stream
link set outage			Set the *CPU local failure* status for a stream
link start emergency			Initiate emergency stream startup
link start normal			Initiate normal stream startup
link stop			Stop a stream
quit			Terminate this CLI session
show info chan			Show information on channel status in a stream
show info link			Show information on stream status

4.3.5 General Device Configuration Mode

To proceed to device parameter configuration/monitoring, execute the *config* command.

SMG4> config
Entering configuration mode.
SMG4-[CONFIG]>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
access category			Enter the access categories configuration mode
alarm set cpu	yes/no		The control system will be alerted about a high load on the CPU
alarm set ram	yes/no		The control system will be alerted about running out of free RAM

alarm set drive	yes/no		The control system will be alerted about external device running out of free RAM
cdr			Enter the CDR record configuration mode
copy running_to_startup			Write the current configuration into the non-volatile memory of the device (into the initial configuration)
copy startup_to_running			Restore the current configuration from the initial configuration
count linkset			Show the number of SS-7 line groups
count trunk			Show the number of trunk groups
count trunk-direction			Show the number of trunk directions
count sipt-interface			Show the number of SIP interfaces
count radius-profile			Show the number of RADIUS profiles
count modifiers-profile			Show the number of modifier profiles
count sipcause-profile			Show the number of profiles with Q.850 causes matching SIP replies
count routing-profile			Show the number of scheduled routing profiles
count ss7timers			Show the number of SS-7 timer profiles
delete linkset	<OBJECT_INDEX>	existing number of the line group	Delete an SS-7 line group
delete trunk	<OBJECT_INDEX>	Existing trunk group number	Delete a trunk group
delete trunk-direction	<OBJECT_INDEX>	Existing trunk direction number	Delete a trunk direction
delete sipt-interface	<OBJECT_INDEX>	Existing SIP interface number	Delete a SIP interface
delete radius-profile	<OBJECT_INDEX>	Existing RADIUS profile number	Delete a RADIUS profile
delete modifiers-table	<OBJECT_INDEX>	Existing modifier table number	Delete a modifier table
delete sipcause-profile	<OBJECT_INDEX>	existing number of a profile with Q.850 causes matching SIP replies	Remove a profile with Q.850 causes matching SIP replies
delete routing-profile	<OBJECT_INDEX>	existing scheduled routing profile number	Delete a scheduled routing table
delete ss7timers	<OBJECT_INDEX>	Existing SS-7 timer profile number	Delete an SS-7 timer profile
e1	<E1_INDEX>	0-3	Enter the selected E1 stream configuration mode
exit			Move to a higher menu level
fail2ban			Enter the Fail2ban configuration mode
firewall			Enter the firewall configuration mode
ftpd			Enter the ftp server

			configuration mode
history			Show the history of entered commands
hostping			Enter the regular ping configuration mode
linkset	<LINKSET_INDEX>	0-3	Enter the SS-7 line group configuration mode
modifiers table	<MODTBL_INDEX>	0-255	Enter the modifier table configuration mode
network			Enter the network configuration mode
new linkset			Create a new SS-7 line group
new trunk			Create a new trunk group
new prefix			Create a new prefix
new sipt-interface			Create a new SIP-T interface
new radius-profile			Create a new RADIUS profile
new **modifiers-table**			Create a new modifier table
new sipcause-profile			Create a correspondence table for q.850 and sip-replies
new routing-profile			Create a scheduled routing table
new ss7timers			Create an SS-7 timer profile
numplan			Enter the numbering schedule configuration mode
ports range	<RANGE_PORT>	1-65535	Define a range of UDP ports used for voice traffic (RTP) and data transmission via the T.38 protocol
ports show			Show UDP ports configuration
ports start	<START_PORT>	1024-65535	Define the starting UDP port used for voice traffic (RTP) and data transmission via the T.38 protocol
q931-timers			Enter the Q.931 timer configuration mode
quit			Terminate this CLI session
radius			Enter the RADIUS configuration mode
route			Enter the static route configuration mode
routing			Enter the scheduled routing configuration mode
show running main by_step			Show the current main configuration by steps
show running main whole			Show the current main configuration in full
show running network			Show the current network configuration
show running radius_servers			Show the current RADIUS server configuration
show running snmp			Show the current SNMP configuration
show startup main by_step			Show the initial main configuration by steps
show startup main whole			Show the initial main configuration in full
show startup network			Show the initial network configuration

			Show the initial RADIUS server configuration
show startup radius_servers			Show the initial RADIUS server configuration
show startup snmp			Show the initial SNMP configuration
sip configuration			Enter the SIP/SIP-T configuration mode
sip interface	<SIPT_INDEX>	0-63	Enter the SIP/SIP-T interface configuration mode
sip cause profile	<PROFILE_INDEX>	0-63	Enter the configuration mode of profiles with Q.850 causes matching SIP replies
ss7cat			Enter the SS-7 category configuration mode
ss7timers	<SS7_TIMERS_INDEX>	0-3	
sync			Enter the configuration mode for synchronisation 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

4.3.6 CDR Configuration Mode

To enter this mode, execute the *cdr* command in the configuration mode.

SMG4-[CONFIG]> cdr
Entering CDR-info mode.
SMG4-[CONFIG]-[CDR]>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
archive	<all>	String, 31 characters max.	Archive CDR data
	<directory>	String, 31 characters max.	
category	save	yes/no	Save /do not save subscriber category in CDR files
config			Return to the *Configuration* menu
emptysave	<CDR_EMPTY>	yes/no	Save / do not save empty CDR files
enabled	<CDR>	yes/no	Generate / do not generate CDRs
exit			Return from this configuration submenu to an upper level
ftp enabled	<CDR_FTP_RES>	yes/no	Transfer / do not transfer CDRs to the FRP server
ftp login	<CDR_FTPLOGIN_RES>	String, 31 characters max.	Specify a username for access to the FTP server
ftp passwd	<CDR_PASSWD_RES>	String, 31 characters max.	Specify a password for access to the FTP server
ftp path	<CDR_FTPPATH_RES>	String, 63 characters max.	Set a path to the CDR storage folder on the FTP server
ftp port	<CDR_FTPPORT_RES>	1-65,535	Specify a TCP port for the FTP server
ftp server	<CDR_FTPSERVER_RES>	String, 63 characters	Specify IP address of the FTP server

SMG digital gateway

		max.	
header	<CDR_HEADER>	yes/no	Write / do not write the following header at the beginning of a CDR file: SMG4. CDR. File started at "YYYYMMDDhhmmss", where "YYYYMMDDhhmmss" is the records saving start time.
history			Show the history of entered commands
localdisk	<set> <show>	/mnt/sd[abc][1-7]*	A path to CDR data storage on a USB drive. Show the settings of the CDR data storage path
localkeep period	<day> <hour> < min>	0-30 0-23 0-59	A period of CDR data storage on a USB drive
localsave	<no> <yes>		Save CDR data on a USB drive
modifiers table outgoing called	<MODTBL_INDEX>	0-255	Set a modifier table for callee number for outgoing communication
modifiers table outgoing calling	<MODTBL_INDEX>	0-255	Set a modifier table for caller number for outgoing communication
modifiers table outgoing redirecting	<MODTBL_INDEX>	0-255	Set a modifier table for redirecting number for outgoing communication
modifiers table incoming called	<MODTBL_INDEX>	0-255	Set a modifier table for callee number for incoming communication
modifiers table incoming calling	<MODTBL_INDEX>	0-255	Set a modifier table for caller number for incoming communication
modifiers table incoming redirecting	<MODTBL_INDEX>	0-255	Set a modifier table for redirecting number for incoming communication
period day	<CDR_DAY>	0-30	Set a period for CDR generation and saving in the device RAM, days
period hour	<CDR_HOUR>	0-23	Set a period for CDR generation and saving in the device RAM, hours
period min	<CDR_MIN>	0-59	Set a period for CDR generation and saving in the device RAM, minutes
quit			Terminate this CLI session
redirect mark	<CDR_REDIRECT_MARK>	yes/no	Add / do not add the *Redirection Tag* additional field to CDR
redirect save	<CDR_REDIRECT>	yes/no	Add the *Redirecting Number* additional field to CDR; otherwise, the redirecting number will replace the calling party number in redirected calls
reserved ftp enabled	<CDR_FTP_RES>	yes/no	Transfer / do not transfer CDRs to the redundant FTP server
reserved ftp login	<CDR_FTPLOGIN_RES>	String, 31 characters max.	Specify a username for access to the redundant FTP server
reserved ftp passwd	<CDR_PASSWD_RES>	String, 31 characters max.	Specify a password for access to the redundant FTP server
reserved ftp path	<CDR_FTPPATH_RES>	String, 63 characters max.	Set a path to the CDR storage folder on the redundant FTP server
reserved ftp port	<CDR_FTPPORT_RES>	1-65535	Specify a TCP port for the redundant FTP server
reserved ftp server	<CDR_FTPSERVER_RES>	String, 63 characters max.	Specify IP address of the redundant FTP server
show			Show CDR settings

Command	Parameter	Value	Action
show_dirs			Show a path to the FTP server access directory
signature	<CDR_SIGNATURE>	String, 63 characters max.	Specify a discriminant that will facilitate identification of the device which 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 an archive to the FTP/TFTP server

4.3.7 Access Categories Configuration Mode

To enter this mode, execute the *access category* command in the configuration mode.

SMG4-[CONFIG]> access category
Entering Access-Category mode.
SMG4-[CONFIG]-[ACCESS-CAT]>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
config			Return to the *Configuration* menu
exit			Return from this configuration submenu to an upper level
quit			Terminate this CLI session
set access	<CAT_IDX> <ACCESS_IDX> <ACCESSIBLE>	0-63 0-63 enable/disable	Define mutual access permissions for categories: - *CAT_IDX*—index of the access category being configured; - ACCESS_IDX—the category the access is configured to; - ACCESSIBLE—category access status (available, not available).
set name	<CAT_IDX> <NAME>	0-63 Access category name, 31 character max. (letters, numbers, "_")	Set Access-Category parameters: - *CAT_IDX*—index of the access category being configured; - NAME—access category name.
show category	<CAT_IDX>	0-63	Show this access category configuration
show list			Show all access categories configuration

4.3.8 E1 Stream Configuration Mode

To enter this mode, execute the *e1 <E1_INDEX>* command in the configuration mode, where *<E1_INDEX>* is the number of an E1 stream.

SMG4-[CONFIG]> e1 0
Entering E1-stream mode.
SMG4-[CONFIG]- E1[0]>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
alarm	<ON_OFF>	on/off	Enable/disable fault indication for this E1 stream
config			Return to the *Configuration* menu
crc4	<ON_OFF>	on/off	Enable/disable CRC4 control for this E1 stream
disabled			Disable the stream operation
enabled			Enable the stream operation
equalizer	<ON_OFF>	on/off	Enable/disable E1 stream signal amplification
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
lapd			Enter the LAPD parameters configuration mode for this E1 stream
linecode AMI			Set the AMI linear encoding type for this stream
linecode HDB3			Set the HDB3 linear encoding type for this stream
name	<NAME>	63 characters max. (numbers, letters, "_")	E1 stream name
q931			Enter the 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 this stream
show			Show this stream configuration
signaling	Signaling type	Q931_USR Q931_NET SS7 SORM	Set the signalling type for a stream Possible signalling types: Q931_USR, Q931_NET, SS7, SORM
slipIND	<ON_OFF>	on/off	Enable fault indication when slips are identified in the reception path
slipTO	<TIMEOUT>	5sec/10sec/ 20sec/30sec/ 45sec/1min/ 2min/3min/ 5min/10min/ 15min/30min/ 1hour/2hour/6hour	Specify time interval for stream parameters polling on the card; if a slip is detected in the stream, PBX will indicate an alarm during the timeout
ss7			Enter the configuration mode for SS-7 signalling parameters of the current E1 stream

4.3.8.1 LAPD Parameters Configuration Mode for the Current E1 Stream

This mode is available only for Q.931 signalling (set by the *signaling* command). To enter this mode, execute the *lapd* command in the E1 stream configuration mode.

    SMG4-[CONFIG]-E1[0]> lapd
    E1[0]. Signaling is Q931
    SMG4-[CONFIG]- E1[0]-[LAPD]>

Command	Parameter	Value	Action
?			Show the list of available commands
config			Return to the *Configuration* menu
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
N200	<N200>	0-255	Specify the number of connection establishment attempts
quit			Terminate this CLI session
show			Show the LAPD configuration
t200	<T200>	0-255	Set T200 timer value, x100 ms
t203	<T203>	0-255	Set T203 timer value, x100 ms

4.3.8.2 Q.931 Signalling Configuration Mode for the Current E1 Stream

This mode is available only for Q.931 signalling (set by the *signaling* command). To enter this mode, execute the *q931* command in the E1 stream configuration mode.

    SMG4-[CONFIG]-E1[0]> q931
    E1[0]. Signaling is Q931
    SMG4-[CONFIG]- E1[0]-[Q931]>

Command	Parameter	Value	Action
?			Show the list of available commands
access category	<CAT_IDX>	0-31	Set access category for a stream
categoryAON	<CAT_AON>	0-15	Set a Caller ID category for the incoming call
channel	<CHAN_NUM> <on_off>	[0-31] or 'all' on/off	Enable/disable the specified channel
chanorder	<CHAN_ORDER>	up_ring/down_ring/ up_start/down_start	Specify the channel engagement order: *up_ring*—sequential forward; *down_ring*—sequential back; *up_start*—from the first and forward; *down_start*—from the first and back.
config			Return to the *Configuration* menu
exit			Return from this configuration submenu to an upper level
history			
invokeID	<INVOKE_ID>	1024-65535	Set an initial call identifier for an operation (used as a reference which enables unique call identification for operations)
name coding	<NAME_CODING>	transit cp1251 siemens avaya translit	Name encoding: *transit – transcoding is not performed* (name received in UTF-8, by defualt); *cp1251* –Windows-1251 encoding; *siemens* –Siemens PBX encoding; *avaya* –AVAYA PBX encoding; *translit* – roman transliteration of Russian names.
name transmission	<NAME_TRANS>	none Q931-DISPLAY QSIG-NA	Set the subscriber name transmission method.

Command	Parameter	Value	Action

		`CORNET`
		`HICOM-350`
		`AVAYA-DISPLAY`
			none - name transmission is disabled;
			Q931-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;
			HICOM-350 – transmission via Siemens CorNet protocol with supplementary information for Hicom PBX;
			AVAYA-DISPLAY – transmission in Q.931 Display element with Codeset 6;

numbering plan	<PLAN>	0-15	The numbering schedule to be used for accepted calls routing
numplan	<CLD_PLAN_ID>	unknown/ISDN/ telephony/National/ Privat	Set a numbering schedule type **To use the E.164 common numbering schedule, select ISDN/telephony**
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_NUM>	0-127	Set a scheduled routing profile
SendCatAON	<ON_OFF>	on/off	Enable/disable Caller ID category transmission as the first digit of a number in the SETUP message **Proper operation requires support of this mode 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 the "*End of dial"* message transmission
show			Show Q.931 signalling configuration
trunk	<trunk_index>	0-31	Define the trunk group number for this stream

4.3.8.3 SS-7 Signalling Configuration Mode for the Current E1 Stream

This mode is available only for SS7 signalling (set by the *signaling* command). To enter this mode, execute the *ss7* command in the E1 stream configuration mode.

SMG4-[CONFIG]-E1[0]> ss7
E1[0]. Signaling is SS7
SMG4-[CONFIG]-E1[0]-[SS7]>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
CIC fill	<CIC> <step>	0-65535 0-255	Set a CIC value for all time slots beginning from 0 *CIC*—CIC starting number; *step*—step number.
CIC set	<TIMESLOT> <CIC>	0-31 0-65535	Set a CIC value for a single timeslot *TIMESLOT*—timeslot number;

			CIC—CIC value.
config			Return to the *Configuration* menu
Dchan	<D_CHAN>	0-31	Set the number of a D-channel for a line. *0*—do not use a D-channel (voice stream)
DPC MTP3		0-16383	Set a DPC MTP3 value for this stream
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
linkset	<linkset_index>	0-15	Assign an SS-7 line group to this stream
quit			Terminate this CLI session
show			Show SS-7 signalling configuration
slc	<slc>	0-15	Set a signal channel identifier in an SS-7 line group
transit set active	<TIMESLOT> <YES/NO>	0-31 yes/no	Set active mode of transit. In this mode SMG initiate connections.
transit set codec	<TIMESLOT> <CODEC>	0-31 NONE/G.711-U/G.711-A/G.729/G.723.1_5.3/G.723.1_6.3/G.726/CLEARMODE	Select codec, which will be used for transit. *NONE* –by default, the codecs assigned on a transit SIP interface are negotiated.
transit set remote_channel	<TIMESLOT> <R_CHANNEL>	0-31 0-31	Select a remote channel
transit set remote_stream	<TIMESLOT> <R_STREAM>	0-31 0-1/0-3	Select a remote stream
transit set sip_interface	<TIMESLOT> <SIP_IFACE_IDX>	0-31 0-63	Select SIP interface, from which transit will be implemented
transit set usage	<TIMESLOT> <YES_NO>	0-31 yes/no	Enable transit on selected channel

4.3.9 Fail2ban Configuration Mode

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

SMG4-[CONFIG]> fail2ban
Entering fail2ban mode.
SMG4-[CONFIG]-[FAIL2BAN]>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
blacklist_ip add	<BLACKIP>	IP address in the AAA.BBB.CCC.DDD format	Add an IP address to the Fail2ban blacklist
blacklist_ip remove	<BLACKIP>	IP address in the AAA.BBB.CCC.DDD format	Remove an IP address from the Fail2ban blacklist
blacklist_ip show all			Show the Fail2ban blacklist
blacklist_ip show first	<COUNT>	0-4095	Show the specified number of addresses at the beginning of the Fail2ban blacklist
blacklist_ip show ip	<BLACKIP>	IP address in the AAA.BBB.CCC.DDD	Find the specified address in the Fail2ban blacklist

			format	
blacklist_ip show last	<COUNT>	0-4095	Show the specified number of addresses at the end of the Fail2ban blacklist
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
quit			Terminate this CLI session
restart			Restart the fail2ban process
set block_time	<BLCKTIME>	60-352800	Set the time in seconds during which access from a suspicious address will be banned
set enable	<ENA>	on/off	Enable/disable the Fail2ban utility
set tries	<TRIES>	1-10	Set the maximum number of unsuccessful access attempts to a service before the host is banned by fail2ban
show			Show the fail2ban settings
start			Start fail2ban
stop			Stop fail2ban
whitelist_ip add	<WHITEIP>	IP address in the AAA.BBB.CCC.DDD format	Add an IP address to the Fail2ban whitelist
whitelist_ip remove	<WHITEIP>	IP address in the AAA.BBB.CCC.DDD format	Remove an IP address from the Fail2ban whitelist
whitelist _ip show all			Show the Fail2ban whitelist
whitelist _ip show first	<COUNT>	0-4095	Show the specified number of addresses at the beginning of the Fail2ban whitelist
whitelist _ip show ip	<BLACKIP>	IP address in the AAA.BBB.CCC.DDD format	Find the specified address in the Fail2ban whitelist
whitelist _ip show last	<COUNT>	0-4095	Show the specified number of addresses at the end of the Fail2ban whitelist

4.3.10 Firewall Configuration Mode

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

SMG4-[CONFIG]> firewall
Entering firewall mode
SMG4-[CONFIG]-[firewall]>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
add profile	<PROF_NAME>	Allowed characters: letters, numbers, "_"; 63 characters max.	Add a firewall profile
add rule	<direction>	input output	Add a firewall rule Rule direction
	<ENABLE>	enable/disable	Enable/disable a rule
	<RULE_NAME>	Text, 63 characters max.	Rule name
	<S_IP>	AAA.BBB.CCC.DDD	Source IP address

	<S_MASK>	AAA.BBB.CCC.DDD	Source subnet mask
	<R_IP>	AAA.BBB.CCC.DDD	Destination IP address
	<R_MASK>	AAA.BBB.CCC.DDD	Destination subnet mask
	<PROTO>	any tcp udp icmp tcp+udp	Protocol type
	<S_PORT_START>	1-65535	Source starting port
	<S_PORT_END>	1-65535	Source ending port
	<D_PORT_START>	1-65535	Destination starting port
	<D_PORT_END>	1-65535	Destination ending port
	<ICMP_TYPE>	none any echo-reply destination-unreachable network-unreachable host-unreachable protocol-unreachable port-unreachable fragmentation-needed source-route-failed network-unknown host-unknown network-prohibited host-prohibited TOS-network-unreachable TOS-host-unreachable communication-prohibited host-precedence-violation precedence-cutoff source-quench redirect network-redirect host-redirect TOS-network-redirect TOS-host-redirect echo-request router-advertisement router-solicitation time-exceeded ttl-zero-during-transit ttl-zero-during-reassembly parameter-problem ip-header-bad required-option-missing	ICMP packet type

		timestamp-request timestamp-reply address-mask-request address-mask-reply	
	<ACTION>	accept, drop, reject	Action—an action executed by this rule: *ACCEPT*—the packets corresponding this rule will be accepted by the firewall. *DROP*—the packets corresponding this rule will be rejected by the firewall without informing the party that has sent them. *REJECT*—the packets corresponding this rule will be rejected by the firewall. The party that has sent the packet will receive either a TCP RST packet or "ICMP destination unreachable".
	<P_IDX>	1-65535	Firewall profile number
apply			Apply firewall settings
config			Return to the *Configuration* menu
del profile	<ID>	1-65535	Remove a firewall profile
del rule	<ID>	1-65535	Remove a firewall rule
exit			Return from this configuration submenu to an upper level
modify profile	<ID>	1-65535	Firewall profile index
	<NAME>	Allowed characters: letters, numbers, "_"; 63 characters max.	Enter a new name for the device
modify rule	<Type>	action dport_end dport_start enable icmp-type name prof_id proto r_ip r_mask s_ip s_mask sport_end sport_start traffic-type

1-65535

A new value according to this parameter type | Modify the specified firewall rule (one of the parameters) |
	<ID>		
	<param>		
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 a rule to a network interface *PROFILE ID = 0* means that the profile is not used
set pptp	<PPP_IDX>	0-5	Assign a rule to an interface

	<PROFILE ID>	0-65535	*PROFILE ID = 0* means that the profile is not used
set vlan	<VLAN_IDX>	VLAN1...VLAN8	Assign a rule to a VLAN
	<PROFILE ID>	0-65535	*PROFILE ID = 0* means that the profile is not used
show config			Show configuration
show interfaces			Show interface parameters
show system			Show system parameters

4.3.10.1 FTP Configuration Mode

To enter this mode, execute the *ftpd* command in the configuration mode.

SMG4-[CONFIG]> ftpd
Entering ftpd mode.
SMG4-[CONFIG]-[FTPd]>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
config			Return to the *Configuration* menu
exit			Return from this configuration submenu to an upper level
quit			Terminate this CLI session
set enable	<EN>	on/off	Enable/disable the FTP server
set port	<PORT>	1-65535	Specify a port for the FTP server
set interface	<IFACE_NAME>	String, 255 characters max.	Specify a network interface for the FTP server
set timeout idle	<TIME>	0-600	Set an idle timeout, in seconds
set timeout login	<TIME>	0-600	Set an authorisation timeout, in seconds
set timeout session	<TIME>	0-600	Set a session timeout, in seconds
show config			Show FTP server configuration
show user			Show user configuration
user add	<USER_NAME>		Add a user Specify a name for the new user
	<PASSWD>		Specify a password for the new user
	<CDR_ACCESS>	no_access r w rw	Set access permissions for the CDR directory
	<LOG_ACCESS>	no_access r w rw	Set access permissions for the LOG directory
	<MNT_ACCESS>	no_access r w rw	Set access permissions for the MNT directory
user del	<IDX>	1-4	Remove a user
user modify access	<IDX>	0-4	Modify access permissions for the

			selected user:
	<CDR_ACCESS>	no_access/r/w/r	- configure access to the CDR directory, read/write;
	<LOG_ACCESS>	no_access/r/w/r	- configure access to the LOG directory, read/write;
	<MNT_ACCESS>	no_access/r/w/r	- configure access to the MNT directory, read/write
user modify password	<IDX>	0-4	Change the password for the selected user
	<PASSWD>		

4.3.11 SS7 Line Group Configuration Mode

To enter this mode, execute the *linkset <LINKSET_INDEX>* command in the configuration mode, where *<LINKSET_INDEX>* is the number of a line group.

SMG4-[CONFIG]> linkset 0
Entering Linkset-mode.
SMG4-[CONFIG]-LINKSET[0]>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
access category	<CAT_IDX>	0-31	Define an access category for the line group
alarm_ind	<ON_OFF>	on/off	Enable/disable fault indication for this SS-7 line group
cci	<ON_OFF>	on/off	Enable channel integrity check for the SS-7 line group
cci frequency	<FREQ>	0-127	Define the frequency of channel integrity checks during outgoing calls performed through the SS-7 line group
cdpn digit in IAM	<ON_OFF>	on/off	Send the first digit of the CdPN number in the IAM message in the overlap dialling mode
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 this SS-7 line group *up_ring*—sequential forward; *down_ring*—sequential back; *up_start*—from the first and forward; *down_start*—from the first and back; *odd_up_ring*—sequential forward odd; *odd_down_ring*—sequentially back odd; *even_up_ring*—sequential forward even; *even_down_ring*—sequential back even.
china	<ON_OFF>	on/off	Enable/disable Chinese SS-7 protocol specification support
combined	<ON_OFF>	on/off	Enable/disable the combined mode
config			Return to the *Configuration* menu
DPC	<DPC_ID>	0-16383	Define a code for the opposite signalling point—DPC
emergency alignment	<ON_OFF>	on/off	Emergency phasing in case of a single signal link in a linkset
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands

init	<INIT_MODE>	blocked/ individual-ublock/ group-unblock/ group-reset	Define initialisation type for this line group
interworking	<INTERWORK>	no_change/ no_encountered/ encountered	Configure the indicator of interaction with other signalling systems: *no_change*—transfer a value from the incoming call without any changes; *no_encountered*—do not report on interaction with a network which does not support the majority of services provided by the ISDN network; *encountered*—report on interaction at selected locations (the ISDN network interacts with a network which does not support the majority of services provided by the ISDN network and is unable to use the commonly used features).
name	<s_name>	Allowed characters: letters, numbers, "_"; 31 characters max.	Set a name of the line group
net_ind	<NET_IND>	international/ reserved/federal/ national	Set a network identifier: *international*—an international network; *reserved*—a reserved network; *federal*—a federal network; *national*—a local network.
numbering plan		0-15	Select a numbering schedule for a linkset
OPC	<OPC_ID>	0-16383	Set a code for the SS-7 line group's own signalling point
primary linkset	<PRI_LINKSET>	0-3	Select the primary SS-7 line group for the combined mode
quit			Terminate this CLI session
redirection check	<ON_OFF>	on/off	Check for Redirecting and Original Called numbers in IAM if the *Redirection Information* parameter is set
release on suspend	<ON_OFF>	on/off	Notify / do not notify about disconnection when the *suspend* message is received
reserv linkset	<RES_LINKSET>	0-3	Select a redundant SS-7 line group
routing_profile	<prof>	0-127	Select a scheduled routing profile
satellite	<ON_OFF>	on/off	Identify availability of a satellite channel while operating through this SS-7 line group
secondary linkset	<SEC_LINKSET>	0-3	Select the secondary SS-7 line group for the combined mode
show			Show configuration of this SS-7 line group
ss7timers	<index>	0-3	Select an SS-7 timer profile
TMR	<TMR>	speech/ 64kb_unrestricted/ 3.1KHz_audio	Define the Transmission Medium Requirement for this SS-7 line group

trunk	<trunk_index>	0-31	Define the trunk group number for this SS-7 line group

4.3.12 Modifier Table Configuration Mode

To enter this mode, execute the *modifiers table <MODTBL_INDEX>* command in the configuration mode, where *<MODTBL_INDEX>* is a table number.

SMG4-[CONFIG]-TRUNK[0]> modifiers table
Entering TRUNK-Modifiers mode.
SMG4-[CONFIG]-TRUNK[0]-MODIFIER>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
add	<MODIFIER_MASK>	a modifier mask, 255 characters max., should be enclosed in parentheses "(" and ")";	Add a modifier: MODIFIER_MASK— modifier mask; CLD_RULE—callee number modification rule; CLG_RULE—caller number modification rule;
	[CLD_RULE]	a modifier rule, 30 characters max., should be enclosed in quotation marks;	
	[CLG_RULE]	a modifier rule, 30 characters max., should be enclosed in quotation marks	
change aoncat	<MODIFIER_INDEX> <AONCAT>	0-512 0-9/any	Edit the 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 the modifier's numbering schedule type for the callee number: MODIFIER_INDEX— modifier number; CALLED_NP_TYPE— numbering schedule type.
change called rule	<MODIFIER_INDEX> <CALLED_RULE>	0-8191 a modifier rule, 30 characters max., should be enclosed in quotation marks	Edit a callee number modification rule for the modifier: MODIFIER_INDEX— modifier number; CALLED_RULE—callee number modification rule.
change called type	<MODIFIER_INDEX>	0-8191	Edit a callee number type for the modifier:

	<CALLED_TYPE>	unknown/ subscriber/ national/ international/ network_specific/ nochange	*MODIFIER_INDEX*— modifier number; *NUM_TYPE*—subscriber number type: - *Subscriber*—used for local calls and incoming long-distance calls; - *National*—used in outgoing long-distance calls or in local calls and incoming long-distance calls instead of the "*Subscriber*"; - *International*—used in LD and CLR lines for outgoing international calls; - *network_specific*—a specific network number; - *unknown*—an unknown number type; - *nochange*—keep the number type unchanged.
change calling category	<MODIFIER_INDEX> <CALLING_CAT_AON>	0-8191 0-9/nochange	Edit the Caller ID category number of the calling party for the modifier:
change calling numbering plan type	<MODIFIER_INDEX> <CALLING_NP_TYPE>	0-8191 nochange/ unknown/ isdn/ telephony/ national/ private	Edit the modifier's numbering schedule type for the caller number: *MODIFIER_INDEX*— modifier number; *CALLING_NP_TYPE*— numbering schedule type.
change calling presentation	<MODIFIER_INDEX> <CALLING_PRESENT>	0-8191 allowed/ restricted/ not_available/ spare/ nochange	Edit a caller presentation modification rule
change calling rule	<MODIFIER_INDEX> <CALLING_RULE>	0-8191 a modifier rule, 30 characters max., should be enclosed in quotation marks	Edit a caller number modification rule for the modifier: *MODIFIER_INDEX*— modifier number; *CALLING_RULE*—caller number modification rule.
change calling screen	<MODIFIER_INDEX>	0-8191	Edit a caller screen

SMG digital gateway

			indicator modification rule
	<CALLING_SCREEN>	not_screened/ user_passed/ user_failed/ network/nochange	
change calling type	<MODIFIER_INDEX> <CALLING_TYPE>	0-8191 unknown/ subscriber/ national/ international/ network_specific/ nochange	Edit a caller number type for the modifier: *MODIFIER_INDEX*— modifier number; *CALLING_TYPE*—subscriber number type: - *Subscriber*—used for local calls and incoming long-distance calls; - *National*—used in outgoing long-distance calls or in local calls and incoming long-distance calls instead of the "*Subscriber*"; - *International*—used in LD and CLR lines for outgoing international calls; - *network_specific*—a specific network number; - *unknown*—an unknown number type; - *nochange*—keep the number type unchanged.
change general access-cat	<MODIFIER_INDEX> <ACCESS>	0-8191 0-31/nochange	Edit the modifier's general access category
change general numplan	<MODIFIER_INDEX> <NUMPLAN>	0-8191 0-15/nochange	Edit the modifier's general numbering schedule
change mask	<MODIFIER_INDEX> <MODIFIER_MASK>	0-8191 a modifier mask, 255 characters max., should be enclosed in parentheses "(" and ")"	Edit a modifier mask *MODIFIER_INDEX*— modifier number; *MODIFIER_MASK*—mask.
change modtable	<MODIFIER_INDEX> <NEW_MODTBL_INDEX >	0-8191 0-255	Move the modifier into the table with the specified number
change numtype	<MODIFIER_INDEX> <NUM_TYPE>	0-8191 unknown/ subscriber/ national/ international/ network_specific/ any	Edit the modifier's number type: *MODIFIER_INDEX*— modifier number; *NUM_TYPE*—subscriber number type:

			- *Subscriber*—used for local calls and incoming long-distance calls; - *National*—used in outgoing long-distance calls or in local calls and incoming long-distance calls instead of the "*Subscriber*"; - *International*—used in LD and CLR lines for outgoing international calls; - *network_specific*—a specific network number; - *unknown*—an unknown number type; - *any*—any number type.
change type	<MODIFIER_INDEX> <MODIFIER_TYPE>	0-8191 calling/called	Change the modifier's subscriber type (caller/callee)
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
quit			Terminate this CLI session
remove	<MODIFIER_INDEX>	0-8191	Remove the specified modifier
show	<MODIFIER_INDEX>	0-8191	Show modifier configuration

4.3.13 Network Parameter Configuration Mode

To enter this mode, execute the *network* command in the configuration mode.

SMG4-[CONFIG]> network
Entering Network mode.
SMG4-[CONFIG]-NETWORK>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
add interface pptpVPNclient	<LABEL> <IPADDR>	Allowed characters: letters, numbers, "_", ".", "-", ":"; 255 characters max. IP address in the AAA.BBB.CCC.DDD format Allowed characters: letters, numbers, "_", ".", "-";	Add a new VPN/PPTP client *LABEL*—interface name; *IPADDR*—IP address of the PPTP server; *USER*—username;

		63 characters max. Allowed characters: letters, numbers, "_", ".", "-"; 63 characters max.	PASS—password.
	<USER> *<PASS>*		
add interface tagged	dynamic/static <LABEL> <VID> <IPADDR> <NETMASK>	Allowed characters: letters, numbers, "_", ".", "-", ":"; 255 characters max. 1-4,095 IP address in the AAA.BBB.CCC.DDD format network mask in the AAA.BBB.CCC.DDD format	Add a new network interface *LABEL*—interface name; VID—VLAN ID; *IPADDR*—IP address of the PPTP server; *NETMASK*—network mask.
add interface untagged	dynamic/static <LABEL> <IPADDR> <NETMASK>	Allowed characters: letters, numbers, "_", ".", "-", ":"; 255 characters max. IP address in the AAA.BBB.CCC.DDD format network mask in the AAA.BBB.CCC.DDD format	Add a new network interface *LABEL*—interface name; *IPADDR*—IP address of the PPTP server; *NETMASK*—network mask.
available ip add	<IPADDR>	IP address in the AAA.BBB.CCC.DDD format	Add an address to the list of allowed addresses
available ip delete	<INDEX>	0-255	Remove an address from the list of allowed addresses
available ip show			Show the list of allowed addresses
config			Return to the *Configuration* menu
confirm			Confirm modified network settings and VLAN settings without gateway restart. If the network settings are not confirmed within 1 minute, the previous values are restored.
dhcp server			Enter the DHCP server configuration mode
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
ntp			Enter the NTP configuration mode
pptp start	<NET_IFACE_IDX>	0-39	Run the specified interface
pptp status	<NET_IFACE_IDX>	0-39	Show the status of the specified interface
pptp stop	<NET_IFACE_IDX>	0-39	Stop the specified interface
quit			Terminate this CLI session

remove interface	<NET_IFACE_IDX>	0-39	Remove the specified interface
rollback			Cancel the changes
set interface broadcast	<NET_IFACE_IDX>	0-39	Define an address for packets broadcasting for the specified interface
	<BROADCAST>		
set interface COS	<NET_IFACE_IDX>	0-39	Define 802.1p priority for the specified interface
	<COS>	0-7	
set interface dhcp	<NET_IFACE_IDX>	0-39	Obtain network settings dynamically from the DHCP server for the specified interface
	<ON_OFF>	on/off	
set interface dhcp_dns	<NET_IFACE_IDX>	0-39	Obtain IP address of the DNS server dynamically from the DHCP server for the specified interface
	<ON_OFF>	on/off	
set interface dhcp_no_gw	<NET_IFACE_IDX>	0-39	Do not obtain gateway settings dynamically from the DHCP server for the specified interface
	<ON_OFF>	on/off	
set interface dhcp_ntp	<NET_IFACE_IDX>	0-39	Obtain NTP settings dynamically from the DHCP server for the specified interface
	<ON_OFF>	on/off	
set interface gw_ignore	<NET_IFACE_IDX>	0-39	Ignore gateway configuration for the specified interface
	<ON_OFF>	on/off	
set interface h323	<NET_IFACE_IDX>	0-39	Enable H323 signalling exchange for the specified interface
	<ON_OFF>	on/off	
set interface ipaddr	<NET_IFACE_IDX>	0-39	Define an IP address and a network mask for the specified interface
	<IPADDR>	IP address in the AAA.BBB.CCC.DDD format	
	<NETMASK>	network mask in the AAA.BBB.CCC.DDD format	
set interface network-label	<NET_IFACE_IDX>	0-39	Define a name for the specified interface
	<LABEL>	letters, numbers, "_", ".", "-", ":"; 255 characters max.	
set interface radius	<NET_IFACE_IDX>	0-39	Enable RADIUS message transmission through the interface
	<ON_OFF>	on/off	
set interface rtp	<NET_IFACE_IDX>	0-39	Enable RTP packet transmission through the interface
	<ON_OFF>	on/off	
set interface run_at_startup	<NET_IFACE_IDX>	0-39	Launch the interface automatically upon startup (for the VPN interface only)
	<STARTUP>	on/off	
set interface serverip	<NET_IFACE_IDX>	0-39	Specify IP address of the FTP server
	<IPADDR>	IP address in the AAA.BBB.CCC.DDD format	
set interface signaling	<NET_IFACE_IDX>	0-39	Enable SIP message transmission through the interface
	<ON_OFF>	on/off	
set interface snmp	<NET_IFACE_IDX>	0-39	Enable SNMP packet transmission through the interface
	<ON_OFF>	on/off	
set interface ssh	<NET_IFACE_IDX>	0-39	Enable ssh session through the interface

	<ON_OFF>	on/off	
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 the VPN interface only)
set interface user_name	<NET_IFACE_IDX> <USER>	0-39 Allowed characters: letters, numbers, "_", ".", "-"; 63 characters max.	Set a user name (for the VPN interface only)
set interface user_pass	<NET_IFACE_IDX> <PASS>	0-39 Allowed characters: letters, numbers, "_", ".", "-"; 63 characters max.	Set a password (for the VPN interface only)
set interface VID	<NET_IFACE_IDX> <VID>	0-39 1-4095	Define a 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 the AAA.BBB.CCC.DDD format	Specify IP address of the primary DNS server
set settings dns secondary	<IPADDR>	IP address in the AAA.BBB.CCC.DDD format	Specify IP address of the redundant DNS server
set settings gateway	<GATEWAY>	network gateway address in the AAA.BBB.CCC.DDD format	Specify IP address of the network gateway
set settings hostname	<HOSTNAME>	Allowed characters: letters, numbers, "_", ".", "-"; 63 characters max.	Specify a host name
set settings ssh	<PORT>	1-65535	Set a TCP port for device access via the SSH protocol, the default value is 22
set settings telnet	<PORT>	1-65535	Set a TCP port for device access via the Telnet protocol, the default value is 23
set settings use_ip_list	<ON_OFF>	on/off	Enable/disable IP whitelist
set settings web	<PORT>	1-65535	Set a TCP port for the web configurator, the default value is 80
show interface by_index			Show settings of the specified network interface
show interface list			Show the list of available network interfaces
show settings			Show network parameters
snmp			Enter the SNMP configuration mode
ssh restart			Restart the SSH process

If an IP address or network mask has been changed or web configurator management has been disabled for the network interface, confirm these settings using the *confirm* command; otherwise, the previous configuration will be restored in two minutes.

4.3.13.1 NTP Configuration Mode

To enter this mode, execute the *ntp* command in the network configuration mode.

SMG4-[CONFIG]-NETWORK> ntp
Entering NTP mode.
SMG4-[CONFIG]-[NETWORK]-NTP>

Command	Parameter	Value	Action
?			Show the list of available commands
apply		no/yes	Apply NTP settings
config			Return to the *Configuration* menu
exit			Return from this configuration submenu to an upper level
quit			Terminate this CLI session
restart ntp		no/yes	Restart the NTP process
set ntp	dhcp period server usage	off/on 10-1,440 IP address in the AAA.BBB.CCC.DDD format off/on	Obtain NTP settings via DHCP Set the synchronisation period Set an NTP server Enable/disable NTP usage
show config			Show configuration
set timezone		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	Specify a time zone with respect to UTC

4.3.13.2 SNMP Configuration Mode

To enter this mode, execute the *snmp* command in the configuration mode.

SMG4-[CONFIG]-NETWORK> snmp
Entering SNMP mode.
SMG4-[CONFIG]-SNMP>

Command	Parameter	Value	Action
?			Show the list of available commands
add	<TYPE> <IP> <COMM>	trapsink/ trap2sink/ informsink IP address in the AAA.BBB.CCC.DDD format String, 31 characters max.	Add a rule for SNMP trap transmission: *TYPE*—SNMP message type; *IP*—IP address of the trap recipient; *COMM*—the password contained in traps; *PORT*—UDP port of the trap recipient.

Command	Parameter	Value	Action
	<PORT>	1-65535	
config			Return to the *Configuration* menu
create user	<LOGIN>	String, 31 characters max.	Create a user (define an access login and a password)
	<PASSWD>	A password, from 8 to 31 characters	
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
modify community	<IDX>	0-15	Modify a rule for SNMP trap transmission (the password contained in traps)
	<COMM>	String, 31 characters max.	
modify ip	<IDX>	0-15	Modify a rule for SNMP trap transmission (the trap recipient address)
	<IP>	IP address in the AAA.BBB.CCC.DDD format	
modify port	<IDX>	0-15	Modify a rule for SNMP trap transmission (the trap recipient port)
	<PORT>	1-65535	
modify type	<IDX>	0-15	Modify a rule for SNMP trap transmission (the SNMP message type)
	<TYPE>	trapsink/ trap2sink/ informsink	
quit			Terminate this CLI session
remove	<IDX>	0-15	Remove a rule for SNMP trap transmission:
restart snmpd	Yes/no		Restart the SNMP client
ro	<RO>	String, 63 characters max.	Set a password for parameters reading
rw	<RW>	String, 63 characters max.	Set a password for parameters 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

4.3.14 Numbering Schedule Configuration Mode

To enter this mode, execute the *numplan* command in the configuration mode.

SMG4-[CONFIG]> numplan
Entering Numbering-plan mode.
SMG4-[CONFIG]-[NUMPLAN]>

Command	Parameter	Value	Action
?			Show the list of available commands
config			Return to the *Configuration* menu
create prefix	<IDX_Numplan>	0-15	Create a prefix in the specified numbering schedule

delete prefix	<IDX Prefix>		Remove the specified prefix
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
prefix			Enter the prefix configuration mode
quit			Terminate this CLI session
set active		0-15	Define the number of active numbering schedules
set domain	<IDX> <DOMAIN>	0-15 String, 15 characters max.	Specify a domain for registration
set name	<IDX> <NAME>	0-15 String, 15 characters max.	Define a numbering schedule name
show active count			Show the number of active numbering schedules
show active list			Show the list of active numbering schedules
show list			Show the list of numbering schedules
show prefixes	<IDX>	0-15 no/yes	Show numbering schedule prefixes with the specified number

4.3.14.1 Prefix Configuration Mode

To enter this mode, execute the *prefix <PREFIX_INDEX>* command in the configuration mode, where *<PREFIX_INDEX>* is a prefix number.

SMG4-[CONFIG]-[NUMPLAN]> prefix 0
Entering Prefix-mode.
SMG4-[CONFIG]-[NUMPLAN]-PREFIX[0]>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
access category	<CAT_IDX>	0-31	Define an access category for the line group
access check	<ON_OFF>	on/off	Check / do not check the access category
called npi	<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). *Subscriber number*—used for local calls and incoming long-distance calls. At that, the transmitted number should be as follows: abxxxxx, or bxxxxx, or xxxxx. *National number*—used in outgoing long-distance calls or in local calls and

| | | | incoming long-distance calls instead of the "*Subscriber*". At that, the transmitted number should be as follows: ABCabxxxxx, or 2abxxxxx, or 10 <international number>.

International umber—used in LD and CLR lines for outgoing international calls. At that, the transmitted number should be as follows: <international number> (without the international network exit prefix—"10"). |
|---|---|---|---|
| config | | | Return to the *Configuration* menu |
| dial mode | <MODE> | nochange/enblock/ overlap | Define the prefix dialling mode:

- *enblock*—the callee number is sent as a block;
- *overlap*—the callee number is sent with an overlap (by a single digit);
- *nochange*—the callee number is sent in the form it has been received from the incoming channel. |
| direction | <PFX_DIRECTION> | local/ Emergency/ zone/ vedomst/ toll/ international | Define the type of access to the trunk group:

local—local;
emergency—emergency call;
zone—zone access;
vedomst—to a private network;
toll—to a long-distance network;
international—to an international network. |
| duration | <PFX_DURATION> | 0-255 | Set the number dialling duration timer, in seconds |
| exit | | | Return from this configuration submenu to an upper level |
| getCID | <ON_OFF> | on/off | Enable/disable Caller ID request for prefix routing |
| history | | | Show the history of entered commands |
| mask edit | | | Enter the prefix mask editing mode |
| mask show | | | Show prefix masks |
| name | <s_name> | String, 31 characters max. (allowed characters: letters, numbers, and "_") | Set prefix name/designation |
| needCID | <ON_OFF> | on/off | Enable/disable CallerID mandatory information request |
| numplan | <PLAN_IDX> | 0-15 | Define the numbering schedule the prefix belongs to |
| notdial ST | <USE_ST> | yes/no | Disable/enable transmission of the end dial marker (ST in SS or "*sending complete*" in PRI) |
| priority | <PRIORITY> | 0-100 | Set prefix priority:

0—the highest priority;
100—the lowest priority. |
| quit | | | Terminate this CLI session |

Command	Parameter	Value	Action
show			Show prefix configuration
stimer	<PFX_LTIMER>	0-255	Set time interval in seconds when the trunk gateway will wait for further dialling if the dialled number already matches a sample in the numbering schedule, but additional digits may be also dialled, which will result in a match to another sample. The default value: 5 seconds.
trunk	<TRUNK>	0-31	Set a trunk group number
type	<PFX_TYPE>	trunk/trunk-direction/change-numplan	Set a prefix type: *trunk*—transition to a trunk group; *trunk direction*—transition to a trunk direction; *change-numplan*—change the numbering schedule.

4.3.14.2 Prefix Mask Configuration Mode

To enter this mode, execute the *mask edit* command in the prefix configuration mode.

```
SMG4-[CONFIG]-PREFIX[0]> mask edit
Entering Prefix-Mask mode.
SMG4-[CONFIG]-PREFIX[0]-MASK>
```

Command	Parameter	Value	Action
?			Show the list of available commands
add	<PREFIX_MASK> [PFX_MASK_TYPE]	A prefix mask. 255 characters max., should be enclosed in parentheses "(" and ")" calling/called [called]	Add a new mask into the prefix. A mask can be specified—for a caller ("calling") or a callee ("called"); the default mask type is always "called".
config			Return to the *Configuration* menu
history			Show the history of entered commands
exit			Return from this configuration submenu to an upper level
modify duration	<PREFIX_MASK_INDEX> <DURATION>	0-1024 0-255	Set a timer for number dialling duration: *PREFIX_MASK_INDEX*—mask number; *DURATION*—the timer.
modify Ltimer	<PREFIX_MASK_INDEX> <LONG_TIMER>	0-1024 0-255	Set a long timer: *PREFIX_MASK_INDEX*—mask number; *LONG_TIMER*—the timer.
modify mask	<PREFIX_MASK_INDEX>	0-1024	Modify a mask:

	<PREFIX_MASK>	A prefix mask. 255 characters max., should be enclosed in parentheses "(" and ")"	*PREFIX_MASK_INDEX*—mask number; *PREFIX_MASK*—the mask.
modify prefix	<PREFIX_MASK_INDEX> <PFX_INDEX>	0-1024 0-255	Transfer a mask to another prefix: *PREFIX_MASK_INDEX*—number of the mask to be transferred; *PFX_INDEX*—the prefix the mask is transferred to.
modify stimer	<PREFIX_MASK_INDEX> <SHORT_TIMER>	0-1024 [0-255]	Set a short timer: *PREFIX_MASK_INDEX*—mask number; *DURATION*—the timer.
modify type	<PREFIX_MASK_INDEX> <PFX_MASK_TYPE>	0-1024 calling/called	Define the mask type—caller or callee number analysis: *PREFIX_MASK_INDEX*—number of the mask to be transferred; *PFX_MASK_TYPE*—mask type: – *calling*—caller number analysis; – *called*—callee number analysis.
quit			Terminate this CLI session
remove	<PREFIX_MASK_INDEX>	0-1024	Remove a mask
show			Show mask information

4.3.15 Q.931 Timer Configuration Mode

To enter this mode, execute the *q931-timers* command in the configuration mode.

SMG4-[CONFIG]> q931-timers
Entering q931-timers mode.
SMG4-[CONFIG]-[q931-T]>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
config			Return to the *Configuration* menu
exit			Return from this configuration submenu to an upper level
quit			Terminate this CLI session
set	t301	180-360	Define the t301 timer value
	t302	10-25	Define the t302 timer value
	t303	4-10	Define the t303 timer value
	t304	20-30	Define the t304 timer value
	t305	30-40	Define the t305 timer value
	t306	30-40	Define the t306 timer value
	t307	180-240	Define the t307 timer value
	t308	4-10	Define the t308 timer value
	t309	6-90	Define the t309 timer value
	t310	10-20	Define the t310 timer value
	t312	6-12	Define the t312 timer value
	t313	4-10	Define the t313 timer value
	t314	4-10	Define the t314 timer value

Command	Parameter	Value	Action
	t316	120-240	Define the t316 timer value
	t317	120-240	Define the t317 timer value
	t320	30-60	Define the t320 timer value
	t321	30-60	Define the t321 timer value
	t322	4-10	Define the t322 timer value
show			Show Q.931 timer configuration

4.3.16 RADIUS Configuration Mode

To enter this mode, execute the *radius* command in the configuration mode.

SMG4-[CONFIG]> radius
Entering RADIUS mode.
SMG4-[CONFIG]-RADIUS>

Command	Parameter	Value	Action
?			Show the list of available commands
acct ipaddr	<IP_ADDR>	IP address in the AAA.BBB.CCC.DDD format	Set an IP address of the accounting server: *IP_ADDR*—IP address;
	<SRV_IDX>	0-8	*SRV_IDX*—server number.
acct port	<PORT>	0-65535	Set a port for the accounting server: *PORT*—port number;
	<SRV_IDX>	0-8	*SRV_IDX*—server number.
acct secret	<SECRET>	String, 31 characters max.	Set a password for the accounting server: *SECRET*—password;
	<SRV_IDX>	0-8	*SRV_IDX*—server number.
auth ipaddr	<IP_ADDR>	IP address in the AAA.BBB.CCC.DDD format	Set an IP address of the authorisation server: *IP_ADDR*—IP address;
	<SRV_IDX>	0-8	*SRV_IDX*—server number.
auth port	<PORT>	0-65535	Set a port for the authorisation server: *PORT*—port number;
	<SRV_IDX>	0-8	*SRV_IDX*—server number.
auth secret	<SECRET>	String, 31 characters max.	Set a password for the authorisation server: *SECRET*—password;
	<SRV_IDX>	0-8	*SRV_IDX*—server number.
auth user		no/yes	Enable authorisation of Web, Telnet, or SSH users on the RADIUS server
config			Return to the *Configuration* menu
deadtime	<DEADTIME>	0-255	Server unavailability time during failure—amount of time when a server is deemed unavailable
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
iface	<IFACE_NAME>	String, 255 characters max.	Set a RADIUS network interface
profile	<PROFILE_INDEX>	0-31	Proceed to RADIUS profile configuration

			Terminate this CLI session
quit			Terminate this CLI session
retries	<RETRIES>	0-255	Set the number of request transmission attempts
show config			Show information on RADIUS server configuration
timeout	<TIMEOUT>	0-255	Set the amount of time to wait for a server response (x100 ms)

4.3.16.1 RADIUS Profile Configuration Mode

To enter this mode, execute the *profile <PROFILE_INDEX>* command in the RADIUS configuration mode, where *<PROFILE_INDEX>* is a RADIUS profile number.

SMG4-[CONFIG]-RADIUS> profile 0
Entering RADIUS-Profile-mode.
SMG4-[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	Set a callee number for Accounting-Request packets: *CdPN-IN*—use the callee number prior to modification (the number received in the SETUP/INVITE packet); *CdPN-OUT*—use the callee number after modification.
acct CgPN	<CGPN_MODE>	CgPN-IN/CgPN-OUT	Set a caller number for Accounting-Request packets: *CdPN-IN*—use the caller number prior to modification (the number received in the SETUP/INVITE packet); *CdPN-OUT*—use the caller number after modification.
acct name	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk	Define the User-Name attribute for Accounting-Request packets: *cgpn*—use the calling party phone number as the value; *ip_or_stream*—use the calling party IP address or incoming connection stream number as the value;

			trunk—use incoming connection trunk name as the value.
acct restrict	<RESTRICT>	none/zone/ local/emergency/ restrict-all	Restrict the outgoing communications in case of a server fault (no response from the server): *none*—allow all calls; *zone*—allow calls to special services, local and zone networks; *local*—allow calls to special services and local networks; *emergency*—allow calls to special services only; *restrict*—deny all calls.
acct start	<ON_OFF>	on/off	Enable/disable *acct. start* message transmission
acct stop	<ON_OFF>	on/off	Enable/disable *acct. stop* message transmission
acct update	<ON_OFF>	on/off	Enable/disable *acct. update* message transmission
acct update_period	<PERIOD>	10sec/20sec/30sec/ 45sec/1min/2min/ 3min/5min/10min/ 15min/30min/1hour	*Acct. update* message transmission period
acct unsuccessfull	<ON_OFF>	on/off	Enable/disable transmission of information on unsuccessful calls to the RADIUS server
auth check on seize	<ON_OFF>	on/off	Enable/disable authorisation request transmission during incoming engagement
auth check on stop-dial	<ON_OFF>	on/off	Enable/disable authorisation request transmission during the end of dial
auth emergency-on-REJ	<PERMIT>	not-allow/allow	Enable/disable access to special services after connection denial from server
auth framed protocol	<FRAMED_PROTOCOL>	none/PPP/ SLIP/ARAP/ Gandalf/Xylogics/ X75_Sync	Assign a packet access protocol for RADIUS authentication requests: *none*—packet access is disabled.
auth name	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk	Define the User-Name attribute for Access-Request packets: *cgpn*—use the calling party phone number as the value; *ip_or_stream*—use the calling party IP address or incoming connection stream number as the value; trunk—use incoming

			connection trunk name as the value.
auth nas port type	<PORT_TYPE>	Async/ Sync/ ISDN_Sync/ ISDN_Async_v120/ ISDN_Async_v110/ Virtual/ PIAFS/ HDLC_Channel/ X25/ X75/ G3_Fax/ SDSL/ ADSL_CAP/ ADSL_DMT/ IDSL/ Ethernet/ xDSL/ Cable/ Wireless/ Wireless_IEEE_802.1	Define a NAS physical port type (a server for user authentication), the default value is *Async*
auth pass	<PASSWD>	A password, 15 characters max.	Set the *User-Password* attribute values in the corresponding RADIUS-Authorization packet
auth restrict	<RESTRICT>	none/zone/ local/emergency/ restrict-all	Restrict the outgoing communications in case of a server fault (no response from the server): *none*—allow all calls; *zone*—allow calls to special services, local and zone networks; *local*—allow calls to special services and local networks; *emergency*—allow calls to special services only; *restrict all*—deny all calls.
auth service type	<SERVICE_TYPE>	none/ Login/ Framed/ Callback_Login/ Callback_Framed/ Outbound/ Administrative/ NAS_Promt/ Authenticate_Only/ Callback_NAS_Prompt/ Call_Check/ Callback_Administrative	Set a type of service; not used by default (none)
auth session time	<SESSION_TIME_MODE>	ignore/ use_RFC_ Session_timeout/ use_CISCO_h323_ credit_time	Set the maximum call duration based on a value of the attribute transmitted in Access-Accept from the RADIUS server:

			ignore—ignore the maximum call duration limit; *use_rfc_session_timeout*—use the value of the Session-Timeout attribute as the maximum call duration timeout; *use_cicso_h323_credit_time*—use the value of the Session-Time or the Cisco VSA h323-credit-time attribute as the maximum call duration timeout.
config			Return to the *Configuration* menu
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
modifiers table incoming called	<MODTBL_INDEX>	0-255/none	Set a callee (CdPN) number modifier for the incoming connection in relation to the *Called-Station-Id*, *xpgk-dst-number-in* fields of RADIUS-Authorization and RADIUS-Accounting messages.
modifiers table incoming calling	<MODTBL_INDEX>	0-255/none	Set a caller (CgPN) number modifier for the incoming connection in relation to Calling-Station-Id, xpgk-src-number-in fields of RADIUS-Authorization and RADIUS-Accounting messages.
modifiers table outgoing called	<MODTBL_INDEX>	0-255/none	Set a callee (CdPN) number modifier for the outgoing connection in relation to the *xpgk-src-number-out* field of RADIUS-Authorization and RADIUS-Accounting messages.
modifiers table outgoing calling	<MODTBL_INDEX>	0-255/none	Set a caller (CgPN) number modifier for the outgoing connection in relation to the *xpgk-dst-number-out* field of RADIUS-Authorization and RADIUS-Accounting messages.
quit			Terminate this CLI session
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

4.3.17 Static Route Configuration Mode

To enter this mode, execute the *route* command in the configuration mode.

SMG4-[CONFIG]> route
Entering route mode.
SMG4-[CONFIG]-ROUTE>

Command	Parameter	Value	Action
?			Show the list of available commands
config			Return to the *Configuration* menu
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
quit			Terminate this CLI session
route add			Add a route:
	<DESTINATION>	IP address in the AAA.BBB.CCC.DDD format	*DESTINATION*—destination IP address;
	<MASK>	Mask in the AAA.BBB.CCC.DDD format	*MASK*—network mask for the specified IP address;
	<GATEWAY>	Gateway in the AAA.BBB.CCC.DDD format	*GATEWAY*—gateway IP address;
	<METRIC>	Unsigned integer	*METRIC*—metrics;
	<IFACE_NAME>	String, 255 characters max.	*IFACE_NAME*—network interface;
	<ENABLE>	disable/enable	*ENABLE*—enable/disable the network route.
route del	<IDX>	0-4095	Remove a route: *IDX*—network route index.
show			Show route configuration information

4.3.18 SIP/SIP-T General Configuration Mode

To enter this mode, execute the *sip configuration* command in the configuration mode.

SMG4-[CONFIG]> sip configuration
Entering SIP/SIP-T/SIP-I/SIP-profile config mode.
SMG4-[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 the *Configuration* menu
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
ignore_RURI		no/yes	Ignore / do not ignore address in R-URI. Address information after the "@" separator in Request-URI is ignored; otherwise, the gateway checks if the address information matches the device IP address and host name, and if there is no match, the call is rejected.
port	<PORT>	1-65535	A port to receive SIP protocol messages
quit			Terminate this CLI session
show			Show SIP general configuration
T1	<T1_TIMER>	0-255	Set T1 SIP timer
T2	<T2_TIMER>	0-255	Set T2 SIP timer
T4	<T4_TIMER>	0-255	Set T4 SIP timer
transport	<TRANSPORT>	UDP-only/ UDP-prefer/ TCP-prefer/ TCP-only	Define the transport layer protocol to be used to send and receive SIP messages: *TCP-prefer*—the messages are received via UDP and TCP. Transmission via TCP. If failed to establish a TCP connection, the messages are sent via UDP; *UDP-prefer*—the messages are received via UDP and TCP. The packets smaller than 1,300 bytes are sent via TCP, while the ones larger than 1,300 bytes—via UDP; *UDP-only*—use the UDP protocol only; *TCP-only*—use the TCP protocol only.

4.3.19 SIP/SIP-T Interface Configuration Mode

To enter this mode, execute the *sip interface <SIPT_INDEX>* command in the configuration mode, where *<SIPT_INDEX>* is the number of SIP/SIP–T interface.

SMG4-[CONFIG]> sip interface 0
Entering SIPT-mode.
SMG4-[CONFIG]-SIP/SIPT-INTERFACE[0]>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
access category	<CAT_IDX>	0-31	Define an access category for the line group
alarm indication	<on/off>		Enable fault indication for interface unavailability
cci	<on/off>	on/off	Enable support of channel integrity checks
cgpn replace	<YES_NO>	no/yes	Take CgPN from the *Username/Number* parameter; when disabled, use the CgPN number received in the incoming call
clearchan override	<on/off>	on/off	Enable the *clear channel override*

			option—only the CLEARMODE codec is specified for the second leg call when the first leg is operating in the *clear channel* mode
clearchan transit	<on/off>	on/off	Enable the *clear channel transit* option—transfer RTP in the same form it has been received on the first leg (including the packetisation time)
codec	<CODEC>	G.711-A	Set the codec to be used for voice data transmission
config			Return to the *Configuration* menu
DSCP RTP	<DSCP_RTP>	0-255	Set a DSCP identifier for RTP traffic
DSCP SIG	<DSCP_SIG>	0-255	Set a DSCP identifier for SIG traffic
DTMF mime type	< MIME_TYPE>	application/dtmf or application/ dtmf-relay	Set the load type used for DTMF transmission in SIP protocol INFO packets: *application/dtmf-relay*—in SIP INFO application/dtmf-relay packets ("*" and "#" are sent as symbols "*" and "#"); *application/dtmf*—in SIP INFO application/dtmf packets ("*" and "#" are sent as digits 10 and 11).
DTMF mode	<DTMF_m>	inband/ RFC2833/ SIP-INFO	The DTMF mode for this interface
DTMF payload	<DTMF_p>	96-127	Set a payload type for RFC2833
DTMF payload-equal	<DTMF_PT_EQ>	(off/on)	Enable/disable the *Same RFC2833 PT* option
ecan	<CANCELLATION>	voice/ nlp-off-voice/ modem/ off	Set the echo cancellation mode: *Voice*—echo cancellers are enabled (this mode is set by default); *Nlp-off-voice*—echo cancellers are enabled in the voice mode; the non-linear processor (NLP) is disabled. When the levels of transmission and reception signals significantly differ, a weak signal may be suppressed by the NLP. This echo canceller mode is used to prevent the signal suppression; *modem*—echo cancellers are enabled in the modem operation mode (direct component filtering is disabled, NLP control is disabled, CNG is disabled); *Off*—echo cancellation is disabled.
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
fax detection	<DETECTION>	no/callee/caller/ callee_and_caller	Set the fax detection mode: *no*—disable fax tone detection;

			callee—for the receiving party only; *caller*—for the transmitting party only; *callee_and_caller*—for both receiving and transmitting parties.
fax mode	<MODE>	T38_only/G.711_only/ T38_and_G.711	Select the fax transmission mode
gain rx	<GAIN>	-140 – 60	Set the volume of voice reception (gain of the signal received from the communicating gateway and output to the speaker of the phone unit connected to the SMG gateway)
gain tx	<GAIN>	-140 – 60	The volume of voice transmission (gain of the signal received from the microphone of the phone unit connected to the SMG gateway and transmitted to the communicating gateway)
history			Show the history of entered commands
hostname clear			Remove a host name of the communicating gateway
hostname set	<HOSTNAME>	String, 63 characters max.	Define a host name of the communicating gateway
inband_signal_with_183_and_sdp	on/off		Issue SIP-reply 183/SDP for voice frequency path forwarding upon receipt of the CALL PROCEEDING or PROGRESS messages from PRI that contain the progress indicator = 8 (in-band signal)
jitter adaptation period	<JT_AP>	1000-65535	Set the time of jitter-buffer adaptation to the lower limit, in milliseconds
jitter adjust mode	<JT_AM>	non-immediate/ immediately	Set the jitter buffer adaptation mode: *non-immediate*—gradual; *immediately*—instant.
jitter deletion mode	<JT_DM>	soft/hard	Set the buffer adaptation mode. Defines the method of packet deletion during buffer adaptation to the lower limit. *soft*—the device uses an intelligent selection pattern to delete the packets, which exceed the threshold; *hard*—the packets, which delay exceeds the threshold, are deleted immediately.
jitter deletion threshold	<JT_DT>	0-500	Set a threshold for immediate deletion of a packet, in milliseconds. When buffer size grows and packets delay exceeds this threshold, the packets are deleted immediately.
jitter init	<JT_INIT>	0-200	Specify an initial value of an adaptive jitter buffer, in milliseconds
jitter max	<JT_MAX>	0-200	Set the upper limit (maximum size) of

SMG digital gateway

			an adaptive jitter buffer, in milliseconds
jitter min	<JT_MIN>	0-200	Set the size of a fixed jitter buffer or the lower limit (the minimum size) of an adaptive jitter buffer
jitter mode	<JT_MODE>	adaptive/non-adaptive	The mode of jitter buffer operation: *Adaptive*—adaptive; *non-adaptive*—fixed.
jitter vbd	<JT_VBD>	0-200	Set a fixed buffer size for data transmission in the VBD mode
max_active	<MAX_ACTIVE>	0-65535	Set the maximum number of active connections for an interface
mode	<mode>	SIP/ SIP-T/ SIP-I/E1-TRANSIT	Set the interface operation mode (SIP profile is assigned to SIP subscribers)
name	<s_name>	Allowed characters: letters, numbers, "_"; 31 characters max.	Set a name for SIP interface
net-interface rtp	<IFACE_NAME>	String, 255 characters max.	Set an RTP network interface
net-interface sig	<IFACE_NAME>	String, 255 characters max.	Set a SIP network interface
numbering plan	<NUMPLAN>	0-15	Select a numbering schedule
password	<PASSWD>	String, 15 characters max.	Set an authentication password
options	<OPTIONS>	enable/disable	Enable the function that controls direction availability by sending OPTIONS messages; when a direction is not available, the redundant trunk group is used for the call. This function also analyses the received OPTIONS message that allows avoiding the use of the *100rel, replaces,* and *timer* features, which are configured in this direction, in case the opposite party does not support them.
options period	<OPTIONS_PERIOD>	30-3600	Set the time in seconds after which the redundant trunk group will be used for a call if the direction is not available.
port	<PORT>	1-65535	Set a UDP port of the communicating gateway that is used for SIP signalling reception
public_ip clear			Remove a public IP
public_ip set	<PUBLIC_IP>	IP address in the AAA.BBB.CCC.DDD format	Set a public IP to be used in SIP/SDP messages
quit			Terminate this CLI session
redirection 302	<REDIRECTION>	on/off	Enable/disable redirection (302)
redirection server	<REDIRECT_SERV>	on/off	Redirect / do not redirect the call, which was sent using a public address, to the subscriber's private

			address without numbering schedule routing. The call is routed directly to the address specified in the "contact" header of reply 302 received from the redirection server. First, redirection 302 should be configured (the *redirection 302* command).
refer	<REFER>	enable/disable	Enable/disable call transfer with REFER
register delay	<REGEXP>	500-5000	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
register expires	<REGEXP>	90-64800	Set the time interval for registration
regmode	<REGMODE>	none/ trunk-mode/	Set the type of registration on an upstream server
reliable_1xx_ response	<ON_OFF>	on/off	When the option is enabled, the INVITE request and 1xx class provisional responses will contain the *require: 100rel* option, which requires assured confirmation of provisional responses
remote name in contact header	<ON_OFF>	on/off	insert displayed name in Contact header
route_mode	<ROUTE_MODE>	RURI/ TO/ defaultCdPN	Set a routing mode: by RURI, by the TO field, CdPN by default
routing_profile	<prof>	0-127	Select a scheduled routing profile
RTCP control	<RTCP_c>	2-255	Set the number of time periods (*RTCP period*) to wait for RTCP protocol packets from the opposite party
RTCP period	<RTCP_p>	5-255	Set the time period in seconds, after which the device sends control packets via the RTCP protocol.
RTP loss silence	<RTP_TIMEOUT_SILENCE>	1-30	Set the RTP packet timeout for the silence suppression option. The coefficient determines how many times the value of this timeout is larger than *RTP-loss timeout*
RTP loss timeout	<RTP_TIMEOUT>	10-300/ off	Set an RTP packet timeout
sdp_in_18x	<ON_OFF>	on/off	Always send SDP in provisional replies
show			Show SIP-T interface information
sipcause profile	<SIPCAUSE>	[0-63]/ none	Select a compliance profile for Q.850 causes and sip-replies
sipdomain	<SIPDOMAIN>	String, 63 characters max. IP address in the AAA.BBB.CCC.DDD format	Set an address of the registration domain
source port check	<ON_OFF>	on/off	Control reception of signalling traffic from the UDP port specified in the *port* setting

src verify	<ON_OFF>	on/off	Control media traffic reception from the IP address and UDP port specified in the SDP communication session description (on); otherwise, accept traffic from any IP address and UDP port (off)
STUN ip	<IPADDR>	IP address in the AAA.BBB.CCC.DDD format	Set an address of the STUN server the requests will be sent to
STUN port	<PORT>	1-65535	Set a port of the STUN server the requests will be sent to
STUN use	<YES_NO>	no/yes	Use the STUN server to determine the public IP
t38 bitrate	<BITRATE>	nolimit/2400/4800 / 7200/9600/12000/ 14400	Set the maximum transfer rate of a fax transmitted via the T.38 protocol
t38 disable			Disable fax reception via the T.38 protocol
t38 enable			Enable fax reception via the T.38 protocol
t38 fillbitremoval	<T38_FBR>	on/off	Enable/disable padding bit removals and inserts for the data which is not related to ECM
t38 pte	<T38_PTE>	10/20/30/40	Set the frequency of T.38 packet generation, in milliseconds
t38 ratemgmt	<T38_RATE_MGMT>	localTCF/ transferredTCF	Set a rate management method: *local TCF*—the method requires the TCF tuning signal to be locally generated by the recipient gateway; *transferred TCF*—the method requires the TCF tuning signal to be sent from the sender device to the recipient one;
t38 redundancy	<T38_REDUNDANCY>	off/1/2/3	Enable redundant frames for error control, off—disable
timer enable	<YES_NO>	no/yes	Enable/disable RFC4028 SIP session timers
timer refresher	<REFRESHER>	uac/uas	Set the party that performs session renewal
timer session Min-SE	<MIN_SE>	90-32000	Set the minimum session state control period, in seconds. This value should not exceed the *timer session expires* forced termination timeout
timer session expires	<EXPIRES>	90-64800	Set a period of time in seconds before a forced session termination if the session is not renewed in time
trunk	<TRUNK>	0-31	Set a trunk group number for an interface
trusted network	<YES_NO>	yes/no	Enable the *trusted network* option
username	<USERNAME>	String, 15 characters max.	Specify a 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	The codec which is used for VBD data transmission

vbd enable			Enable V.152
vbd disable			Disable V.152
vbd payload type	<VBD_p>	Static,96-127	The payload type which is used for the VBD codec

4.3.20 SS-7 Category Modification Configuration Mode

To enter this mode, execute the *ss7cat* command in the configuration mode.

SMG4-[CONFIG]> ss7cat
Entering SS7-categories mode.
SMG4-[CONFIG]-SS7-CAT>

Command	Parameter	Value	Action
?			Show the list of available commands
config			Return to the *Configuration* menu
exit			Return from this configuration submenu to an upper level
quit			Terminate this CLI session
set	<CAT_IDX>	0-15	Set a data category:
	<PBX_CAT>	0-255	*CAT_IDX*—category index;
	<SS7_CAT>	0-255	*PBX_CAT*—Caller ID category;
			SS7_CAT—SS-7 category.
show			Show information on SS-7 data category

4.3.21 SS-7 Timer Configuration Mode

To enter this mode, execute the *ss7timers <SS7_TIMERS_INDEX>* command in the configuration mode, where *<SS7_TIMERS_INDEX>* is a profile number.

SMG4-[CONFIG]> ss7timers 0
Entering SS7Timers-mode.
SMG4-[CONFIG]-SS7-TIMERS[0]>

Command	Parameter	Value	Action
?			Show the list of available commands
config			Return to the *Configuration* menu
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
quit			Terminate this CLI session
set mtp2 T1	<TIMER>	400-500	Set a value of MTP2 T1 level timer (x100 ms)
set mtp2 T2	<TIMER>	50-500	Set a value of MTP2 T2 level timer (x100 ms)
set mtp2 T3	<TIMER>	10-20	Set a value of MTP2 T3 level timer (x100 ms)
set mtp2 T4	<TIMER>	75-95	Set a value of MTP2 T4 normal

normal			level timer (x100 ms)
set mtp2 T4 emergency	<TIMER>	4-6	Set a value of MTP2 T4 emergency level timer (x100 ms)
set mtp2 T6	<TIMER>	30-60	Set a value of MTP2 T6 level timer (x100 ms)
set mtp2 T7 normal	<TIMER>	5-20	Set a value of MTP2 T7 normal level timer (x100 ms)
set mtp3 T2	<TIMER>	7-20	Set a value of MTP3 T2 level timer (x100 ms)
set mtp3 T4	<TIMER>	5-12	Set a value of MTP3 T4 level timer (x100 ms)
set mtp3 T12	<TIMER>	8-15	Set a value of MTP3 T12 level timer (x100 ms)
set mtp3 T13	<TIMER>	8-15	Set a value of MTP3 T13 level timer (x100 ms)
set mtp3 T14	<TIMER>	20-30	Set a value of MTP3 T14 level timer (x100 ms)
set mtp3 T17	<TIMER>	8-15	Set a value of MTP3 T17 level timer (x100 ms)
set mtp3 T22	<TIMER>	1800-3600	Set a value of MTP3 T22 level timer (x100 ms)
set mtp3 T23	<TIMER>	1800-3600	Set a value of MTP3 T23 level timer (x100 ms)
set isup T1	<TIMER>	150-600	Set a value of ISUP T1 level timer (x100 ms)
set isup T5	<TIMER>	3000-9000	Set a value of ISUP T5 level timer (x100 ms)
set isup T6	<TIMER>	100-600	Set a value of ISUP T6 level timer (x100 ms)
set isup T7	<TIMER>	200-300	Set a value of ISUP T7 level timer (x100 ms)
set isup T8	<TIMER>	150-600	Set a value of ISUP T1 level timer (x100 ms)
set isup T9	<TIMER>	300-2400	Set a value of ISUP T9 level timer (x100 ms)
set isup T12	<TIMER>	150-600	Set a value of ISUP T12 level timer (x100 ms)
set isup T13	<TIMER>	3000-9000	Set a value of ISUP T13 level timer (x100 ms)
set isup T14	<TIMER>	150-600	Set a value of ISUP T14 level timer (x100 ms)
set isup T15	<TIMER>	3000-9000	Set a value of ISUP T15 level timer (x100 ms)
set isup T16	<TIMER>	150-600	Set a value of ISUP T16 level timer (x100 ms)
set isup T17	<TIMER>	3000-9000	Set a value of ISUP T17 level timer (x100 ms)
set isup T18	<TIMER>	150-600	Set a value of ISUP T18 level timer (x100 ms)
set isup T19	<TIMER>	3000-9000	Set a value of ISUP T19 level timer (x100 ms)
set isup T20	<TIMER>	150-600	Set a value of ISUP T20 level timer (x100 ms)
set isup T21	<TIMER>	3000-9000	Set a value of ISUP T21 level timer (x100 ms)
set isup T22	<TIMER>	150-600	Set a value of ISUP T22 level timer (x100 ms)
set isup T23	<TIMER>	3000-9000	Set a value of ISUP T23 level

			timer (x100 ms)
set isup T24	<TIMER>	1-20	Set a value of ISUP T24 level timer (x100 ms)
set isup T25	<TIMER>	10-100	Set a value of ISUP T25 level timer (x100 ms)
set isup T26	<TIMER>	600-1800	Set a value of ISUP T26 level timer (x100 ms)
set isup T33	<TIMER>	120-150	Set a value of ISUP T33 level timer (x100 ms)
set isup T34	<TIMER>	20-40	Set a value of ISUP T34 level timer (x100 ms)
set isup T35	<TIMER>	150-200	Set a value of ISUP T35 level timer (x100 ms)
show			Show configuration

4.3.22 Sync Configuration Mode

To enter this mode, execute the *sync* command in the configuration mode.

SMG4-[CONFIG]> sync
Entering sync mode.
SMG4-[CONFIG]-SYNC>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
config			Return to the *Configuration* menu
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
new stream	<E1>	0-3	Set a synchronisation source from an E1 stream *E1*—E1 stream number.
quit			Terminate this CLI session
remove	<SOURCE>	0-3	Remove a synchronisation source (specify the source number, but not the number of the E1 stream)
show			Show information on synchronisation sources configuration
timeout down	<TIMEOUT>	0-255	A time interval when the system does not switch to a lower priority synchronisation source in case of a signal loss. If the signal is restored during this interval, the system will not switch to a lower priority source.
timeout up	<TIMEOUT>	0-255	A time interval when the restored higher priority synchronisation signal should be active for the system to switch to that signal

4.3.23 Syslog Configuration Mode

To enter this mode, execute the syslog command in the configuration mode.

SMG4-[CONFIG]> syslog

Entering syslog mode.
SMG4-[CONFIG]-SYSLOG>

Command	Parameter	Value	Action
?			Show the list of available commands
alarm	<ALARM>	0-99	Send information on faults with the specified priority; 0—disable data transfer
apply	yes/no		Apply system log settings
authlog set	<IPADDR>

<PORT>

<MODE>

<TYPE> | IP address in the AAA.BBB.CCC.DDD format

1-65535

off/on

local/remote | Enable registration of device access operations:

IPADDR—IP address of the syslog server;

PORT—port of the syslog server;

MODE—enable/disable log registration;

TYPE—defines whether the log is stored locally or sent to the Syslog server |
authlog show			Show settings for registration of device access operations
calls	<CALLS>	0-99	Enable tracing of calls with the specified debug level; 0—disable data transfer
config			Return to the *Configuration* menu
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
hw	<E1>

<HW> | 0-15

0-99 | Send E1 stream hardware data with the specified debug level, 0—disable data transfer
E1—E1 stream number;
HW—priority level. |
ipaddr	<IPADDR>	IP address in the AAA.BBB.CCC.DDD format	Set an IP address of the PPTP server
isup	<ISUP>	0-99	Enable tracing of the ISUP subsystem with the specified debug level; 0—disable data transfer
msp	<MSP>	0-99	Enable tracing of MSP signal processor resources with the specified debug level; 0—disable data transfer
port	<PORT>	1-65535	Set the number of the local UDP port for operations via the SIP-T protocol
Q931	<Q931>	0-99	Enable tracing of Q.931 signalling with the specified debug level; 0—disable data transfer
quit			Terminate this CLI session
radius	<RADIUS>	0-99	Enable tracing of the RADIUS protocol with the specified debug level; 0—disable data transfer

rtp-create	<RTP>	0-99	Enable tracing of RTP forwarding creation with the specified debug level; 0—disable data transfer
show			Show Syslog configuration information
sipt	<SIPT>	0-99	Enable tracing of SIP-T signalling with the specified debug level; 0—disable data transfer
start			Enable data transmission to the syslog server
stop			Disable data transmission to the syslog server
userlog	<IPADDR> ial<PORT> <MODE>	IP address in the AAA.BBB.CCC.DDD format 1-65535 off/standart/full	Enable history registration for the entered commands *IPADDR*—IP address of the syslog server; *PORT*—port of the syslog server; *MODE*—verbosity level of the entered commands log; 　*off*—disable generation of the entered commands log; 　*standard*—messages contain the name of the modified parameter; 　*full*—messages contain the name of the modified parameter as well as parameter values before and after modification.

4.3.24 Trunk Group and Trunk Direction Configuration Mode

To enter the trunk group configuration mode, execute the *trunk group <TRUNK_INDEX>* command in the configuration mode, where *<TRUNK_INDEX>* is a trunk group number.

    SMG1016M-[CONFIG]> trunk group 0
    Entering trunk-mode.
    SMG1016M-[CONFIG]-TRUNK[0]>

Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
channel add	<TimeSlot>	1-31	Add a channel into the trunk group. It is used when destination = E1-channels
channel order	<VALUE>	first_forward/ successive_forward	The order of channel engagement in the trunk group first_forward—from the first and forward; successive_forward—sequential forward;
channel remove	<TimeSlot>	1-31	Remove a channel from the trunk group. It is used when destination = E1-channels
config			Return to the *Configuration* menu

connected number transit	<VALUE>	normal/block	Define whether the *connected number* parameter is transferred by transit: normal—transfer; block—do not transfer.
destination	<TG_ENTRY> <ENTRY_INDEX>	Q.931/SS7/SIPT/ E1-channels Unsigned integer	Assign the trunk group to the Q931, SS-7, or SIP-T interface or to E1 channels *TG_ENTRY*—interface type; *ENTRY_INDEX*—object index (the number of Q931 signalling stream, line group, SIP-T interface)
direct prefix	<IDX>	0-255/none	Set direct call forwarding from this trunk group to the specified prefix without caller and callee number analysis
disable all	<YES_NO>	yes/no	Enable/disable incoming and outgoing calls for this trunk group
disable in			Disable all incoming calls for this trunk group
disable out			Disable all outgoing calls for this trunk group
exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
modifiers table incoming called	<MODTBL_INDEX>	0-255/none	Set a trunk group modifier intended for modifications based on analysis of the callee number received from the incoming channel
modifiers table incoming calling	<MODTBL_INDEX>	0-255/none	Set a trunk group modifier intended for modifications based on analysis of the caller number sent to the outgoing channel
modifiers table outgoing called	<MODTBL_INDEX>	0-255/none	Set a trunk group modifier intended for modifications based on analysis of the callee number sent to the outgoing channel
modifiers table outgoing original	<MODTBL_INDEX>	0-255/none	Set a trunk group modifier intended for modifications based on analysis of the caller original number sent to the outgoing channel
modifiers table incoming redirecting	<MODTBL_INDEX>	0-255/none	Set a trunk group modifier intended for modifications based on analysis of the redirecting subscriber sent to the outgoing channel
modifiers table outgoing calling	<MODTBL_INDEX>	0-255/none	Set a trunk group modifier intended for modifications

			based on analysis of the caller number received from the incoming channel
name	<s_name>	Allowed characters: letters, numbers, "_"; 31 characters max.	Set a trunk group name
quit			Terminate this CLI session
radius profile	<IDX>	0-31/ no	Set a RADIUS profile
reserv	<TG_RSV_IDX>	0-31	Set the number of the redundant trunk group
show			Show trunk group configuration
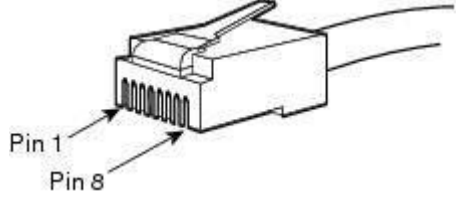
To enter the trunk direction configuration mode, execute the *trunk direction <DIRECTION_INDEX>* command in the configuration mode, where *<DIRECTION _INDEX>* is a trunk group number.

    SMG4-[CONFIG]> trunk direction 0
    Entering trunk-mode.
    SMG4-[CONFIG]- TRUNK_DIRECTION[0]>
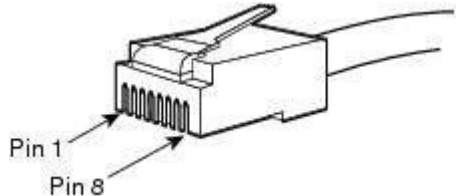
Command	*Parameter*	*Value*	*Action*
?			Show the list of available commands
config			Return to the *Configuration* menu
Exit			Return from this configuration submenu to an upper level
history			Show the history of entered commands
list add	<TD_TRUNK>	0-63	Add the trunk group with the specified index into the direction
list remove	<TD_TRUNK>	0-63	Remove the trunk group with the specified index from the direction
mode		successive_forward/ successive_backward/ first_forward/ last_backward	Define the method of trunk group selection for the direction: sequential forward; sequential back; from the first and forward; from the last and back.
name	<s_name >	String, 63 characters max.	Set a name of the trunk direction
quit			Terminate this CLI session
show			Show trunk direction configuration

SMG digital gateway

5   APPENDIX A. CABLE CONTACT PIN ASSIGNMENT

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

Contact Pin No. (Pin)	Assignment	Contact Pin Numbering
1	RCV from network (tip)	
2	RCV from network (ring)	
3	RCV shield	
4	XMT tip	
5	XMT ring	
6	XMT shield	
7	Not used	
8	Not used	

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

Contact Pin No. (Pin)	Assignment	Contact Pin Numbering
1	Not used	
2	Not used	
3	TX	
4	Not used	
5	GND	
6	RX	
7	Not used	
8	Not used	

6 APPENDIX B. ALTERNATIVE METHOD OF DEVICE FIRMWARE UPDATE

In case firmware update via web interface or console (Telnet, RS-232) is not possible, an alternative firmware update method via RS-232 can be used.

To update the device firmware, the following programs are required:

- Terminal program (for example, TERATERM);
- TFTP server program.

Firmware update procedure:

1. Connect to the Ethernet port of the device.

2. Connect the PC COM port to the device console port using a crossed cable.

3. Run the terminal program.

4. Configure data transmission rate: 115200, data format: 8 bit w/o parity, 1 stop bit, w/o flow control.

5. Run the tftp server program on the PC and specify the path to the *smg_files* folder. Create the *smg4* subfolder in the folder and place there the *smg4_kernel, smg4_initrd* files (the computer that runs the TFTP server and the device should be located in the same network).

6. Turn the device on and stop the startup sequence by entering the *stop* command in the terminal program window:

```
BootROM 1.08
Booting from SPI flash
General initialization – Version: 1.0.0

High speed PHY – Version: 2.1.4 (COM-PHY-V20)
Update PEX Device ID 0x67100
High speed PHY – Ended Successfully
DDR3 Training Sequence – Ver 5.5.0
DDR3 Training Sequence – Run without PBS.
DDR3 Training Sequence – Ended Successfully
BootROM: Image checksum verification PASSED


   __  \/ __  |  __ _ _ _____    _____ _ | _ |
  |   |\/|  |/ _` |  '_\ \ / /  / _ \ | |
  | |   | | (_| | |  \ v /  __/ | |
  |_|   |_|\__,_|_|     \_/ \___|_|_|

        |  |  |  |  |____ )           |   |
        | | |  |  |___|  __  \ /  _ \ /  _ \|  __|
        | |_|  |___|  |_) | (_) | (_) | |_
         \___/       |____/ \___/ \___/ \__|
  ** LOADER **


U-Boot 2011.12 (Jul 22 2014 – 16:26:55) Marvell version: v2011.12 2013_Q3.1

Board: RD-88F6W11
SoC:  MV6710 A1
CPU:  Marvell PJ4B v7 UP (Rev 1) LE
```

```
    CPU    @ 800 [MHz]
    L2     @ 533 [MHz]
    TClock @ 200 [MHz]
    DDR    @ 533 [MHz]
    DDR 16Bit Width, FastPath Memory Access
DRAM:  512 MiB

Initialize PHY on port1

Map:  Code:        0x1fefb000:0x1ff8f9c0
    BSS:        0x1ffefaf8
    Stack:       0x1f9eaef8
    Heap:        0x1f9eb000:0x1fefb000

NAND:  Using Hamming 1-bit ECC for NAND device
1024 MiB
MMC:   MRVL_MMC: 0
SF: Detected MX25L12805D with page size 64 KiB, total 16 MiB
*** Warning – bad CRC, using default environment

PCI:
Initialize and scan all PCI interfaces
PEX unit.port(active IF[-first bus]):
-----------------------------------------
PEX 0.0(0): Detected No Link.
PEX 0.1(1): Detected No Link.
ready
FPU not initialized
USB 0: Host Mode
USB 1: Host Mode


SF: Detected MX25L12805D with page size 64 KiB, total 16 MiB
Factory settings:
 MODEL :  <SMG-4>
 S/N :   <VI3F000026>
 HW :     <1v1>
 WAN MAC : <A8:F9:4B:88:29:93>
 LAN MAC : <02:00:04:88:29:93>


Net:   egiga0, egiga1 [PRIME]
Type 'stop' to stop autoboot:  0
SMG4>>
```

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 the computer which runs the TFTP server> <ENTER>*.

- Example: set serverip 192.168.2.5

10.   Enter *mii si <ENTER>* to activate the network interface:

```
=> mii si
Init switch 0: ..Ok!
Init switch 1: ..Ok!
Init phy 1: ..Ok!
Init phy 2: ..Ok!
=>
```

11. Update the Linux kernel using the *run flash_kern* command:

```
SMG4>> run flash_kern
Using egiga1 device
TFTP from server 192.168.2.5; our IP address is 192.168.2.2
Filename 'smg4/smg4_kernel'.
Load address: 0x2000000
Loading: #################################################################
       #############
done
Bytes transferred = 3220040 (312248 hex)

NAND erase: device 0 offset 0x0, size 0xa00000
Erasing at 0x9e0000 -- 100% complete.
OK

NAND write: device 0 offset 0x0, size 0x312248
 3220040 bytes written: OK
SMG4>>
```

12. Update the file system using the *run flash_initrd* command:

```
SMG4>> run flash_initrd
Using egiga1 device
TFTP from server 192.168.2.5; our IP address is 192.168.2.2
Filename 'smg4/smg4_initrd'.
Load address: 0x2880000
Loading: #################################################################
       #################################################################
       #################################################################
       #################################################################
       ###################################################
done
Bytes transferred = 12727152 (c23370 hex)

NAND erase: device 0 offset 0xa00000, size 0x4000000
Erasing at 0x49e0000 -- 100% complete.
OK

NAND write: device 0 offset 0xa00000, size 0xc23370
 12727152 bytes written: OK
SMG4>>
```

13. Startup the device using the *run bootcmd* command.

7 APPENDIX C. EXAMPLES OF MODIFIER OPERATION AND DEVICE CONFIGURATION VIA CLI

Modifier Operation Examples

Objective 1

Implement a modification corresponding to the mask (1x{4,6}) in *trunk group* 0: remove the first digit, replace it with "34", and leave the other digits unchanged.

Creating a Modification Rule

This mask covers all 5-, 6- and 7-digit numbers beginning with 1. According to the syntax, the modification rule will be as follows: **".+34xxxx??"** (the "." character at the first position means that the first digit is deleted; "+34" means that "34" is inserted after it; "xxxx"—the next 4 digits are always present and are not 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 present at these positions and is not modified).

Commands Used

SMG4> **config** *// Enter the configuration mode*
Entering configuration mode
SMG4-[CONFIG]> **new modifiers-table** *// Create a new modifier table*
NEW 'MOD-TABLE' [01]: successfully created *// Table 1 has been created*
SMG4-[CONFIG]> **modifiers table** 1 *// Enter the configuration mode for table 1*
Entering modifiers-table mode.
SMG4-[CONFIG]-MODTABLE[1]> **add** (1x{4,6}) ".+34xxxx??" *// Add a modifier: a number mask and a modification rule*
Modifier. 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: 1
                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
SMG4-[CONFIG]-MODTABLE[1]> **exit** *// Exit the modifier table configuration mode*
Back to configuration mode.
SMG4-[CONFIG]> **trunk group** 0 *// Enter the trunk group configuration mode*
Entering trunk-mode
SMG4-[CONFIG]-TRUNK[0]> **modifiers table outgoing called** 1 *// Add the created modification table for modification of the CdPN number in outgoing communications*
Trunk[0]. Set oModCld '1'
'TRUNK GROUP' [00]:
                name: TrunkGroup00
                disable out: no

```
                disable in:        no
                reserv trunk:       none
                direct_pfx:        none
                RADIUS-profile:      none
                destination:       Linkset [0]
                local:            no


                Modifiers:
                 incoming calling:   none
                 incoming called:    none
                 outgoing calling:   none
                 outgoing called:    1
                 outgoing redir:     none
                 outgoing orig-cld:  none
                 outgoing generic num:none


                use in-band message:  no
                connected-num transit: normal
```

Objective 2

Remove the area code from the caller number, which is received in the national format with area code 383, of *trunk group 0* and change the number type to *subscriber*.

Creating a Modification Rule

A number in national format contains 10 digits and begins with 383. Since the remaining 7 digits may take any values, "xxxxxxx" should be specified for them. The resulting mask is **(383xxxxxxx)**. The area code, i. e. the first 3 digits, should be removed, while the remaining digits remain unchanged. The resulting modification rule is as follows: **"…xxxxxxx"**. Use the *change* command for category modification (the *add* command in the command example below adds an incoming modifier number 8; thus, the *change* category modification command should be used for modifier 8).

Commands Used

SMG4> **config** // *Enter the configuration mode*
Entering configuration mode
SMG4-[CONFIG]> **new modifiers-table** // *Create a new modifier table*
NEW 'MOD-TABLE' [02]: successfully created // *Table 2 has been created*
SMG4-[CONFIG]> **modifiers table** 2 // *Enter the configuration mode for table 2*
Entering modifiers-table mode.
SMG4-[CONFIG]-MODTABLE[2]> **add (383xxxxxxx) "$" "...xxxxxxx"** // *Add a modifier: a number mask and a modification rule which removes the first three digits from the caller number. Modifier 8 has been created*
Modifier. add
Modifier. Create: mask <(383xxxxxxx)>, cld-rule <$>, clg-rule <...xxxxxxx>
NEW 'MODIFIER' [08]: successfully created
Modifier. Created with index [8].
'MODIFIER'   [08]:
                table: 2
                mask: (383xxxxxxx)
                numtype: any
                AONcat: any
                general-access: no change
                general-numplan: no change

                called-rule: $
                called-type: <no-change>
                called-numplan: no change

```
            calling-rule:    ...xxxxxxx
            calling-type:    <no-change>
            calling-numplan:  no change
            calling-present:  no change
            calling-screen:   no change
            calling-catAON:   no change
```

SMG4-[CONFIG]-MODTABLE[2]> **change calling type 8 subscriber** *// Change the type of the caller number to "subscriber"*

```
Modifier. change_clg_type
'MODIFIER'   [08]:
            table:         2
            mask:          (383xxxxxxx)
            numtype:        any
            AONcat:         any
            general-access:  no change
            general-numplan:  no change

            called-rule:    $
            called-type:    <no-change>
            called-numplan:   no change

            calling-rule:    ...xxxxxxx
            calling-type:    <subscriber>
            calling-numplan:  no change
            calling-present:  no change
            calling-screen:   no change
            calling-catAON:   no change
```

SMG4-[CONFIG]-MODTABLE[2]> **exit** *// Exit the modifier table configuration mode*

Back to configuration mode.

SMG4-[CONFIG]> **trunk group 0** *// Enter the trunk group configuration mode*

Entering trunk-mode

SMG4-[CONFIG]-TRUNK[0]> **modifiers table incoming calling** 2 *// Add the created modification table for modification of the CgPN number in incoming communications*

```
Trunk[0]. Set iModCld '7'
'TRUNK GROUP' [00]:
            name:           TrunkGroup00
            disable out:       no
            disable in:        no
            reserv trunk:       none
            direct_pfx:        none
            RADIUS-profile:      none
            destination:       Linkset [0]
            local:           no

            Modifiers:
             incoming calling:   2
             incoming called:    none
             outgoing calling:   none
             outgoing called:    none
             outgoing redir:     none
             outgoing orig-cld:   none
             outgoing generic num:none

            use in-band message:   no
            connected-num transit: normal
```

Device Configuration Example via CLI

Objective

Configure SS7-SIPT transit.

Source Data

A stream from the opposite PBX is physically connected to E1 stream 0 at SMG4.

<u>SS7 Signalling Parameters</u>

- OPC=67;
- DPC=32;
- associated signalling mode, i. e. the same DPC for both MTP3 and ISUP;
- 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 mutual channel engagement, the channel engagement order should be assigned on the opposite side, e. g. *sequential back odd*).

<u>SIP-T Signalling Parameters</u>

- IP address of the communicating gateway—192.168.16.7;
- UDP port for SIP-T signalling reception of the communicating gateway—5060;
- number of simultaneously allowed sessions—25;
- packetisation time for G.711 codec—30 ms;
- DTMF signal transmission during the established session according to RFC2833, payload type for RFC2833 packets—101.

<u>Routing</u>

- route to SS-7 by trunk group 0;
- route to SIP-T by trunk group 1;
- transition to SS-7 is performed by 7-digit numbers beginning from 6, 7, 91, 92, 93;
- transition to SIP-T is performed by 7-digit numbers beginning from 1, 2, 3;
- all SS-7 signalling messages are transferred by transit.

Configuration via CLI

SS-7 Signalling Configuration

```
SMG4> config // Enter the configuration mode
SMG4-[CONFIG]> new linkset // Create a new line group (linkset)
NEW 'LINKSET' [00]: successfully created
SMG4-[CONFIG]> linkset 0 // Enter the linkset configuration mode
Entering Linkset-mode.
SMG4-[CONFIG]-LINKSET[0]> chan_order even_successive_forward
// Select the channel engagement order—sequential forward even
Linkset[0]. Set chan_order '6'
SMG4-[CONFIG]-LINKSET[0]> DPC ISUP 32 // Define a code for opposite ISUP signalling point
Linkset[0]. Set DPC '32'
SMG4-[CONFIG]-LINKSET[0]> OPC 67 // Define a code for own signalling point
```

Linkset[0]. Set OPC '67'

SMG4-[CONFIG]-LINKSET[0]> **init group-reset**

// Select a channel initialisation mode which is used in signalling channel establishment

Linkset[0]. Set init '7'

SMG4-[CONFIG]-LINKSET[0]> **net_ind national** *// Set 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
```

SMG4-[CONFIG]-LINKSET[0]> **exit** *// Exit the linkset configuration mode*

Leaving Linkset mode

SMG4-[CONFIG]> **e1 0** *// Enter the E1 stream 0 configuration mode*

Entering E1-stream mode

SMG4-[CONFIG]-E1[0]> **enabled** *// Put E1 stream into operation*

E1[0]. Set line 'on'

SMG4-[CONFIG]-E1[0]> **signaling SS7** *// Select an SS-7 signalling protocol for the 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'
```

SMG4-[CONFIG]-E1[0]> **ss7** *// Enter the SS-7 protocol configuration mode*

E1[0]. Signaling is SS7

SMG4-[CONFIG]-E1[0]-[SS7]> **DPC MTP3 32**// *Define a code for opposite MTP3 signalling point*

E1-SS7[0]. Fill CIC: start [0], step [1]

SMG4-[CONFIG]-E1[0]-[SS7]> **CIC fill 0 1**// *Assign channel numbering from 0 in increments of 1*

E1-SS7[0]. Fill CIC: start [0], step [1]

SMG4-[CONFIG]-E1[0]-[SS7]> **Dchan 1** *// Select channel 1 as a signal channel*

E1-SS7[0]. Set Dchan 1

SMG4-[CONFIG]-E1[0]-[SS7]> **SLC 1** *// Assign code 1 to the created signalling channel*

E1-SS7[0]. Set SLC 1

SMG4-[CONFIG]-E1[0]-[SS7]> **linkset 0** *// Assign linkset 0 for the stream*

E1-SS7[0]. Set Linkset 0

'E1: SS7' [00]:

```
            stream:    0
        linkset:   0
        SLC:       1
        DPC-MTP3:  32

        CICs:
      00: --- [TG: --] | 01: -D- [TG: --] | 02: 002 [TG: --] | 03: 003 [TG: --] |
      04: 004 [TG: --] | 05: 005 [TG: --] | 06: 006 [TG: --] | 07: 007 [TG: --] |
      08: 008 [TG: --] | 09: 009 [TG: --] | 10: 010 [TG: --] | 11: 011 [TG: --] |
      12: 012 [TG: --] | 13: 013 [TG: --] | 14: 014 [TG: --] | 15: 015 [TG: --] |
```

```
        16: 016 [TG: --] | 17: 017 [TG: --] | 18: 018 [TG: --] | 19: 019 [TG: --] |
        20: 020 [TG: --] | 21: 021 [TG: --] | 22: 022 [TG: --] | 23: 023 [TG: --] |
        24: 024 [TG: --] | 25: 025 [TG: --] | 26: 026 [TG: --] | 27: 027 [TG: --] |
        28: 028 [TG: --] | 29: 029 [TG: --] | 30: 030 [TG: --] | 31: 031 [TG: --] |
```

SMG4-[CONFIG]-E1[0]-[SS7]> **exit** *// Exit the SS-7 protocol configuration mode*

Leaving SS7-signaling mode

SMG4-[CONFIG]-E1[0]> **exit***// Exit the E1 stream 0 configuration mode*

Leaving E1-stream mode

SIP-T Signalling Configuration (the above session continued)

SMG4-[CONFIG]> **new sipt-interface** *// Create a new SIP-T interface*

NEW 'SIPT INTERFACE' [00]: successfully created

SMG4-[CONFIG]> **sip interface 0***// Enter the configuration mode for the created SIP-T interface*

Entering SIPT-mode.

SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[0]> **hostname set 192.168.16.7**

// Set an IP address of the communicating gateway

SIPT-Interface[0]. Set ipaddr '192.168.16.7'

SMG4-[CONFIG]-SIPT-INTERFACE[0]> **port destination 5060**

// Set a UDP port of the communicating gateway that is used for SIP signalling

SIPT-Interface[0]. Set port '5060'

SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[0]> **codec set 0 G.711-a***// Set a codec*

SIPT-Interface[0]. Set codec '0'

SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[0]> **codec pte 0 30***// Set packetisation time of 30 ms for the G.711 codec*

SIPT-Interface[0]. Set pte '30'

SMG4-[CONFIG]-SIPT-INTERFACE[0]> **max_active 25***// Define the number of simultaneous sessions*

SIPT-Interface[0]. Set max_active '25'

SMG4-[CONFIG]-SIPT-INTERFACE[0]> **DTMF mode RFC2833**

// Select a method of DTMF–RFC2833 transmission

SIPT-Interface[0]. Set DTMF_type '1'

SMG4-[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
```

SMG4-[CONFIG]-SIPT-INTERFACE[0]> **exit** *// Exit the SIP-T interface configuration mode*

Leaving SIPT mode

Routing Configuration (the above session continued)

SMG4-[CONFIG]> **new trunk** *// Create a trunk group for the SS-7 line group*

NEW 'TRUNK GROUP' [00]: successfully created

SMG4-[CONFIG]> **new trunk** *// Create a trunk group to work via the SIP-T interface*

NEW 'TRUNK GROUP' [01]: successfully created

SMG4-[CONFIG]> **numplan** *// Switch to the numbering schedule configuration mode*

NEW 'PREFIX' [00]: successfully created

SMG4-[CONFIG]-[NUMPLAN]> **create prefix 0** *// Create a prefix to transit in the SS-7 direction in numbering schedule 0*

NEW 'PREFIX' [00]: successfully created

SMG4-[CONFIG]-[NUMPLAN]> **create prefix 0** *// Create a prefix to transit in the SIP-T direction in numbering schedule 0*

NEW 'PREFIX' [01]: successfully created

SMG4-[CONFIG]-[NUMPLAN]> **exit** *// Exit the numbering schedule configuration mode*

SMG4-[CONFIG]> **trunk group 0** *// Switch to the trunk group configuration mode for the SS-7 line group*

Entering trunk-mode

SMG4-[CONFIG]-TRUNK[0]> **destination SS7 0**// *Associate trunk group 0 with SS line group 0*

```
Trunk[0]. Set destination '2'
'TRUNK GROUP' [00]:
          name:      TrunkGroup00
          disable out:   no
          disable in:    no
          reserv trunk:  none
          direct_pfx:    none
          RADIUS-profile: none
          destination:   Linkset [0]

          Modifiers:
           incoming calling:   none
           incoming called:    none
           outgoing calling:   0
           outgoing called:    0
           outgoing redirecting:none
           outgoing orig-called:none
           outgoing generic num:none

          use in-band message:   no
          connected-num transit: normal
```

SMG4-[CONFIG]-TRUNK[0]> **exit**
// Exit the trunk group configuration mode for the SS-7 line group
Leaving TRUNK mode
SMG4-[CONFIG]> **trunk group 1** *// Enter the trunk group configuration mode for the SIP-T interface*
Entering trunk-mode
SMG4-[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]

       Modifiers:
        incoming calling: none
        incoming called: none
        outgoing calling: 0
        outgoing called: 0
        outgoing redirecting:none
        outgoing orig-called:none
        outgoing generic num:none

       use in-band message: no
       connected-num transit: normal
SMG4-[CONFIG]-TRUNK[1]> **exit**
// Exit the trunk group configuration mode for the SIP-T interface
Leaving TRUNK mode
SMG4-[CONFIG]> **numplan**
SMG4-[CONFIG]-[NUMPLAN]> **prefix 0**
// Enter the prefix configuration mode for transition to trunk group 0
Entering Prefix-mode
SMG4-[CONFIG]-[NUMPLAN]-PREFIX[0]> **type trunk** *// Set the prefix type—'transition to trunk group"*
Prefix[0]. Set type '1'
SMG4-[CONFIG]-[NUMPLAN]-PREFIX[0]> **trunk 0** *// Assign transition to trunk group 0 by prefix*
Prefix[0]. Set idx '0'
SMG4-[CONFIG]-[NUMPLAN]-PREFIX[0]> **mask edit**
// Enter the mode which allows configuration of dialling masks and analysis of caller numbers
Entering Prefix-Mask mode
SMG4-[CONFIG]-[NUMPLAN]-PREFIX[0]-MASK> **add ([67]xxxxxx|9[1-3]xxxxx)**
// Add a 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
SMG4-[CONFIG]-[NUMPLAN]-PREFIX[0]-MASK> **exit**
// Exit the mode which allows configuration of dialling masks and analysis of caller numbers
Leaving Prefix-Mask mode
SMG4-[CONFIG]-[NUMPLAN]-PREFIX[0]> **called type transit**
// Define a transit for caller number type
Prefix[0]. Set cdpn_type '5'

```
'PREFIX' [00]:
                name:        'Prefix#00'
                type:        'trunk'
                idx:         0
                access cat:   0 [no check]
                direction:   'local'
                CdPN type:   '<no-change>'
                CdPN npi:    'isdn/telephony'
                get  CID:    n
                need CID:    n
                dial mode:    no change
                not dial ST:  no
                priority:    100
                Stimer:      5
                duration:    30
                PLAN:        0
                Mask for prefix [00]:
                [000]  −   [called]
                  Mask:    ([67]xxxxxx|9[1-3]xxxxx)
                  Ltimer:  10
                  Stimer:  5
                  Duration: 30
```

SMG4-[CONFIG]-[NUMPLAN]-PREFIX[0]> **exit** *// Exit the prefix configuration mode*

Leaving Prefix mode

SMG4-[CONFIG]-[NUMPLAN]> **prefix 1**

// Enter the prefix configuration mode for transition to trunk group 1

 Entering Prefix-mode

SMG4-[CONFIG]-[NUMPLAN]-PREFIX[1]> **type trunk** *// Set the prefix type—"transition to trunk group"*

Prefix[1]. Set type '1'

SMG4-[CONFIG]-[NUMPLAN]-PREFIX[1]> **trunk 1** *// Assign transition to trunk group 1 by prefix*

Prefix[1]. Set idx '1'

SMG4-[CONFIG]-[NUMPLAN]-PREFIX[1]> **mask edit** *// Enter the mode which allows configuration of dialling masks and analysis of caller numbers*

Entering Prefix-Mask mode

SMG4-[CONFIG]-[NUMPLAN]-PREFIX[1]-MASK> **add ([1-3]xxxxxx)**

// Add a 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
```

SMG4-[CONFIG]-[NUMPLAN]-PREFIX[1]-MASK> **exit** *// Exit the mode which allows configuration of dialling masks and analysis of caller numbers*

Leaving Prefix-Mask mode

SMG4-[CONFIG]-[NUMPLAN]-PREFIX[1]> **called transit** *// Set a transit for callee number type*

```
Prefix[1]. Set called '5'
'PREFIX' [01]:
                name:        'Prefix#01'
                type:        'trunk'
                idx:         0
                access cat:   0 [no check]
                direction:   'local'
                CdPN type:   '<no-change>'
                CdPN npi:    'isdn/telephony'
                get  CID:    n
                need CID:    n
                dial mode:    no change
                not dial ST:  no
```

```
        priority:    100
        Stimer:      5
        Ltimer:      10
        duration:    30
        PLAN:        0
        Mask for prefix [01]:
        [001]  –   [called]
          mask:    ([1-3]xxxxxx)
          Ltimer:  10
          Stimer:  5
          Duration: 30
```

SMG4-[CONFIG]-[NUMPLAN]-PREFIX[1]> **exit**// *Exit the prefix configuration mode*

Leaving Prefix mode

SMG4-[CONFIG]-[NUMPLAN]> **exit** // *Exit the numbering schedule configuration mode*

SMG4-[CONFIG]> exit

Leaving configuration mode.

Saving Configuration and Device Restart (the above session continued)
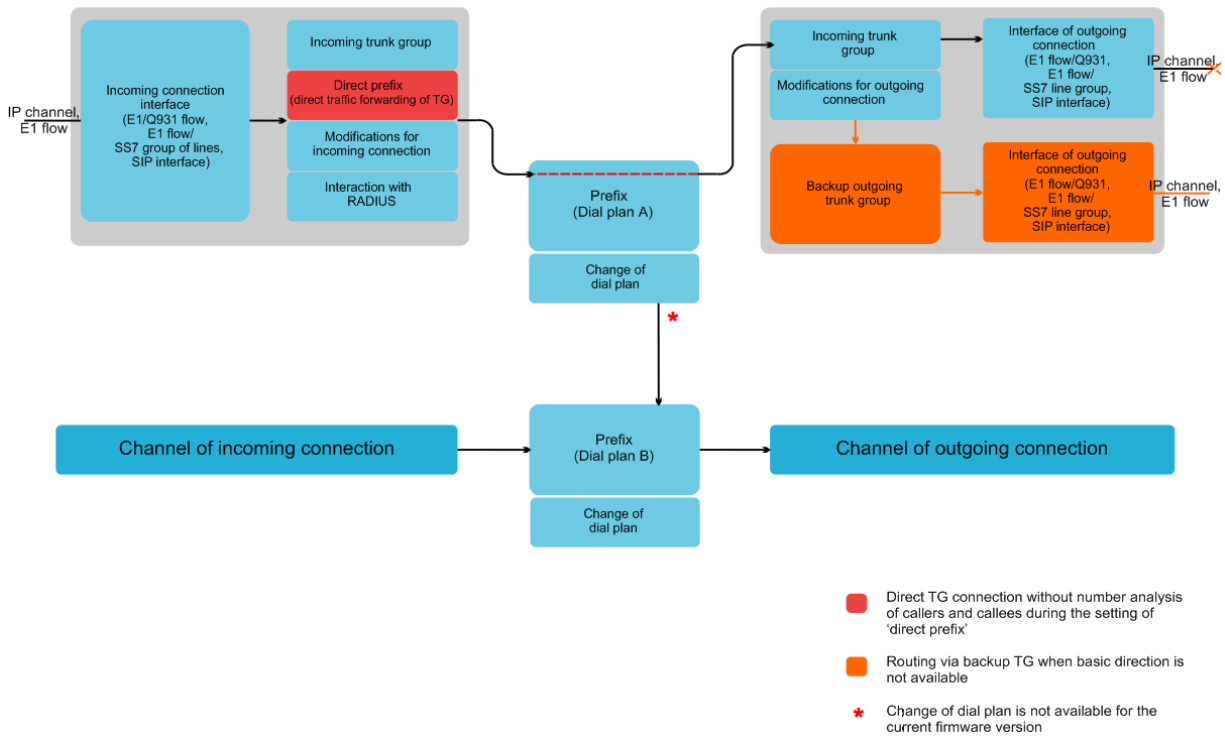

SMG4> **save** // *Save the configuration*

tar: removing leading '/' from member names
****
*****Saved successful

SMG4> **reboot yes** // *Restart the device*

8 APPENDIX D. CORRELATION BETWEEN ROUTING, SUBSCRIBERS, AND SIGNAL LINK PARAMETERS

An incoming call from an IP or TDM channel arrives to the incoming interface, then the call further routing is determined by a trunk group (TG) using the RADIUS protocol (if applicable). The TG performs number modifications for incoming communication. After that, the call is routed by prefix into the outgoing channel or to a SIP subscriber. If a "direct prefix" is configured in the incoming TG, the call is routed to the outgoing TG configured in the prefix parameters without caller and callee number analysis. The outgoing TG performs number modifications. After that, the call arrives to the outgoing interface/channel. If the outgoing direction in not available, the call will be directed to the backup direction (if configured).

9 APPENDIX E. GUIDELINES FOR SMG OPERATION IN A PUBLIC NETWORK

SMG operation in a public network requires to take all security measures in order to avoid the device password brute forcing, DoS (DDoS) attacks, and other intrusive actions which may lead to unstable operation, subscriber data theft, attempts to perform calls at the expense of other subscribers, and consequently to damages to the service provider as well as subscribers.

Avoid using SMG in a public network without additional protective measures like session border controller (SBC), firewall, etc.

Guidelines for SMG Operation in a Public Network

- Operation in a public network with the default SIP signalling port 5060 is not recommended. To change this, modify the *Port for SIP signalling reception* parameter in the *SIP interfaces* settings in SIP general configuration and SIP interface settings. This setting will not ensure complete protection as the signalling port may be discovered during port scanning.
- If IP addresses of all devices communicating with SMG are known, use the *iptables* utility to configure rules allowing access from these addresses and denying access from all other ones.

Also, you should configure the *fail2ban* utility.

Fail2ban stores unsuccessful SIP protocol access attempts in a log file (/tmp/log/pbx_sip_bun.log), and if the number of such attempts exceeds a defined value, the IP address, which has originated them, will be banned for the specified time. The utility also allows generation of lists for trusted and untrusted addresses. For detailed description, see section **4.1.11.1**.

10   APPENDIX F. DEVICE INTERACTION WITH MONITORING SYSTEMS

To enable real-time fault monitoring for the device, configure device interaction with a monitoring system.

Absence of faults means device normal operation; when a fault event occurs, the normal state turns to the alarm state, when all the current faults are resolved, the normal operation state is restored.

Possible indications of device status:

- front panel light indication—*Alarm* LED (for Alarm LED indication, see section **1.6 LED Indication**);
- indication of the most critical failure in the header of web interface (see operation log for more details);
- transmission of the fault events to the monitoring system via the SNMP protocol (trap, inform).

Events for the fault state generation are divided into unconditional and optional:

- *Unconditional*—faults with non-configurable indication; they include:
    - *CONFIG*—a critical fault, a configuration file fault;
    - *SIPT-MODULE*—a critical fault, a failure of a software module responsible for VoIP operation;
    - *SM-VP DEVICE*—a fault, an SM-VP IP submodule failure;
    - *SYNC*—a fault indicating that a synchronisation source is missing or a warning indicating that synchronisation is performed with a low-priority synchronisation source;
    - *CDR-FTP*—a critical fault or a warning indicating an error during CDR data transfer to the FTP server; the fault level is determined by the amount of CDR data awaiting transfer to the server;
    - TRANSIT – critical alarm, which occurs in case of error while semi-permanent connection establishment for E1 channel transit.

- *Optional*—faults with configurable indication; they include:
    - *STREAM*—a critical fault, an E1 stream is not in operation;
    - *STREAM-REMOTE*—a warning, a remote fault of an E1 stream;
    - *STREAM-SLIP*—a warning, SLIPs in a stream;
    - These faults are configured in physical parameters of E1 streams (see section **4.1.2.2**).
    - *LINKSET*—a critical fault, an SS-7 line group is not in operation;
    - *SS7LINK*—an SS-7 signal channel failure;
    - *SIP-ACCESS*—an availability fault of an opposite gateway via the SIP interface;
    - *CPU-OVERLOAD*—a CPU load failure;
    - *MEMORY-LIMIT*—a failure, no free RAM;
    - *DRIVE-LIMIT*—a failure, no free space on an external drive.

By default, optional fault indication is disabled, i. e. interaction with monitoring systems requires configuration of failure indication for all necessary objects.

To configure interactions with monitoring systems via SNMP, enable SNMP on the device and configure SNMP TRAP or INFORM message transmission to the monitoring server IP address.

Configuration via Web Configurator

1) Configuration of optional failure indication for an E1 stream (the *E1 Stream/Physical Parameters* menu, see section **4.1.5.2 Configuration of Physical Parameters).**

To configure LOS and AIS fault indication for an E1 stream, check the *Alarm Indication* checkbox.

To configure RAI fault indication, check the *Remote Alarm Indication* checkbox.

To configure slips indication for a stream, check the *SLIP Indication* checkbox and configure the SLIP detection timer.

2) Configuration of optional failure indication for an SS-7 line group (the *E1 Streams/SS-7 Line Group* menu, see section **4.1.5.4 SS-7 Signalling Protocol Configuration**)**.**

To configure SS-7 signal link fault indication, check the *Fault Indication* checkbox.

3) To enable SNMP, use the *TCP/IP Settings/Network Interfaces* menu (section **4.1.8.11 Network interfaces**)*.*

Network interface 0	
Network label	eth0
Firewall profile	Firewall Profile #0
Type	Untagged ▼
Enable DHCP	☐
IP-address	192.168.1.4
Network mask	255.255.255.0
Broadcast	192.168.1.255
Gateway	192.168.1.123
DNS-address by DHCP	☐
NTP-address by DHCP	☐
Services	
Enable Web	☑
Enable Telnet	☑
Enable SSH	☑
Enable SNMP	☑
Enable SIP signaling	☑
Enable RTP transmission	☑
Enable RADIUS	☑

To perform the configuration, check the *Enable SNMP* checkbox.

4) To configure SNMP trap output, use the *Network Services/SNMP* menu (section **4.1.9.2 SNMP Traps Settings).**

SNMP	
SNMP trap 0	
Type	trap2sink ▼
Community	public
IP-address	192.168.1.123
Port	166

Apply   Cancel

To perform the configuration, specify an SNMP message type (TRAPv1, TRAPv2, INFORM), a password (Community), an IP address and an SNMP trap recipient port.

When the configuration is set up and applied, restart the SNMP agent by clicking the *Restart SNMPd* button.

11 APPENDIX G: CONFIGURATION OF E1 CHANNELS TRANSIT THROUGH A SEMIPERMANENT CONNECTION

Work principle

The channels for transit through a SIP interface are selected from E1 stream which is connected to SMG. SMG transmit request via SIP interface for establishment of connections with remote SMG. Remote SMG receives the request and connects voice tract with appropriate E1 channel. Then, all the voice data which comes to the timeslot will be transmitted to the remote side (and from remote side to the active).

After establishment of connection SMG will control its status and tries to recover connection in case of a failure. The connection integrity and availability of remote side is controlled by following means:

- OPTIONS requests transmission;
- session timers updating via RFC4028;
- session activity control via RTCP;
- control of presence of RTP-packets from remote side.

Objective
Configure connection between two geographically remote phones.

Initial conditions

- Two remote objects connected through an Ethernet network;
- On the first object the phone is connected through the subscriber line of Makom-MX multiplexer and multiplexed to channel 1. The stream is connected to SMG via 0 E1 port;
- IP address of SMG on the first object is 192.0.2.1;
- On the second object the phone is connected through the subscriber line of Makom-MX multiplexer and multiplexed to channel 4. The stream is connected to SMG via 1 E1 port;
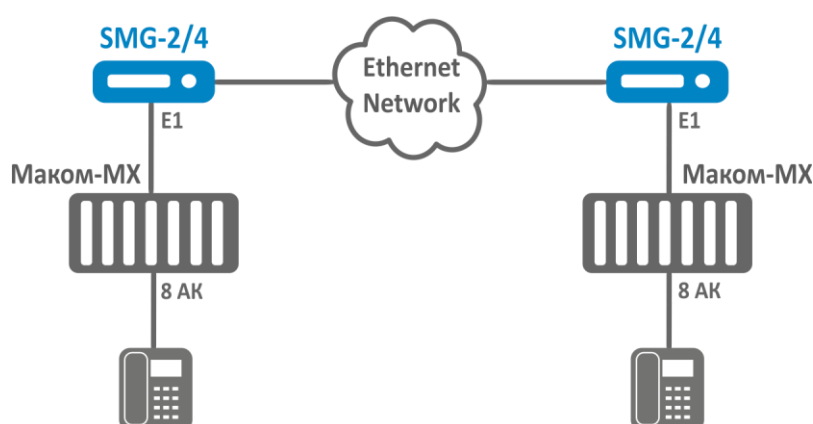- IP address of SMG on the second object is 192.0.2.2.

Fig. 11 - Objects' connection scheme

On the receiving SMG the following actions must be performed:

1. Create a new interface in 'Routing -> SIP interfaces' section:
   1.1. Set 'Transit E1' mode on the interface;
   1.2. Set IP address of the remote side;
   1.3. Set signalling destination port on the remote side;
   1.4. Set signalling receive port;
   1.5. Select network signalling interfaces and RTP;
   1.6. Select appropriate codecs in 'Codecs configuration/RTP' tab, if it is necessary;
   1.7. Click 'Apply'

2. Select a stream in 'E1 streams' section and perform the following settings:
   2.1. Signalling protocol - SS7;
   2.2. Physical parameters - Enabled;
   2.3. Move to 'Channel settings' tab;
   2.4. Click 'Edit' in 'Transit' column of the channel which will be configured;
   2.5. Check 'Enable transit';
   2.6. Select codec which will be used for connection. If you select 'by default', the codecs which were set on the selected SIP interface will be used.
   2.7. Select SIP interface which were configured in 1 step;
   2.8. Define E1 stream and number of a channel on remote side to which connection will be implemented;
   2.9. Click 'Apply' in transit configuration window;
   2.10. Click 'Apply' in 'Channel configuration' section.

On the SMG which establishes the connection 1 and 2 steps must be performed as for receiving SMG, but check the box 'Active side' before 2.9 step. SMG will start to establish the connection immediately.

You can check the status of the connection in section 'Monitoring - E1 channels monitoring'.

The example of connection configuration via CLI

On the first object

```
// SIP interface configuration
// Enter to configuration mode
SMG4> config
Entering configuration mode.
// Creation of SIP interface for transit
SMG4-[CONFIG]> new sipt-interface
NEW 'SIP/SIPT INTERFACE' [11]: successfully created
// Enter to SIP interface configuration mode
SMG4-[CONFIG]> sip interface 11
Entering SIPT-mode.
// Set E1 channels transit mode
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[11]> mode E1-TRANSIT
SIPT-Interface[11]. Set SIP_mode '4'
// Set address of remote side
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[11]> hostname set 192.0.2.2
SIPT-Interface[11]. Set hostname '192.0.2.2'
// Set port on remote side
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[11]> port destination 5060
SIPT-Interface[11]. Set dstport '5060'
// Set a local port
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[11]> port source 5060
SIPT-Interface[11]. Set srcport '5060'
// Set an interface for signalling
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[11]> net-interface sig eth0
```

```
SIPT-Interface[11]. Set netiface_sig 'eth0'
```
// Set an interface for media
```
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[11]> net-interface rtp eth0
SIPT-Interface[11]. Set netiface_rtp 'eth0'
```
// Complete configuration of SIP interface
```
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[11]> exit
Leaving SIPT mode.
```

// Configuration of E1 stream and channel for transit
// Enter to E1 stream configuration mode
```
SMG4-[CONFIG]> e1 0
Entering E1-stream mode
```
// Set SS7
```
SMG4-[CONFIG]-E1[0]> signaling ss7
E1[0]. Set Signaling 3
```
// Enable stream
```
SMG4-[CONFIG]-E1[0]> enabled
E1[0]. Set line 'on'
```
// Enter to SS7 configuration mode
```
SMG4-[CONFIG]-E1[0]> ss7
E1[0]. Signaling is SS7
```
// Enable transit mode
```
SMG4-[CONFIG]-E1[0]-[SS7]> transit set usage 1 yes
Transit:
01: remote stream [   0] remote channel [   1] role 'passive' codec '.............
NONE' SIP Inteface [00] 'incoming'
```
// Set SIP interface for transit
```
SMG4-[CONFIG]-E1[0]-[SS7]> transit set sip_interface 1 11
Transit:
01: remote stream [   0] remote channel [   1] role 'passive' codec '.............
NONE' SIP Inteface [11] 'SIP-interface11'
```
// Set channel number on the remote side
```
SMG4-[CONFIG]-E1[0]-[SS7]> transit set remote_channel 1 4
Transit:
01: remote stream [   0] remote channel [   4] role 'passive' codec '.............
NONE' SIP Inteface [11] 'SIP-interface11'
```
// Set stream number on remote side
```
SMG4-[CONFIG]-E1[0]-[SS7]> transit set remote_stream 1 1
Transit:
01: remote stream [   1] remote channel [   4] role 'passive' codec '.............
NONE' SIP Inteface [11] 'SIP-interface11'
```
// Quit SS7 configuration mode
```
SMG4-[CONFIG]-E1[0]-[SS7]> exit
Leaving SS7-signaling mode.
```
// Quit E1 stream configuration mode
```
SMG4-[CONFIG]-E1[0]> exit
Leaving E1-stream mode.
```
// Quit configuration mode
```
SMG4-[CONFIG]> exit
Leaving configuration mode.
```

On the second object

// SIP interface configuration
// Enter to configuration mode
```
SMG4> config
Entering configuration mode.
```
// Create SIP interface for transit
```
SMG4-[CONFIG]> new sipt-interface
NEW 'SIP/SIPT INTERFACE' [2]: successfully created
```
//Enter to SIP interface configuration mode
```
SMG4-[CONFIG]> sip interface 2
```

SMG digital gateway

```
Entering SIPT-mode.
// Set transit mode for E1 channels
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[2]> mode E1-TRANSIT
SIPT-Interface[2]. Set SIP_mode '4'
// Set address of the remote side
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[2]> hostname set 192.0.2.1
SIPT-Interface[2]. Set hostname '192.0.2.2'
// Set a port on the remote side
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[2]> port destination 5060
SIPT-Interface[2]. Set dstport '5060'
// Set a local port
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[2]> port source 5060
SIPT-Interface[2]. Set srcport '5060'
// Set an interface for signalling
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[2]> net-interface sig eth0
SIPT-Interface[2]. Set netiface_sig 'eth0'
// Set an interface for media
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[2]> net-interface rtp eth0
SIPT-Interface[2]. Set netiface_rtp 'eth0'
// Complete configuration of SIP interface
SMG4-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[2]> exit
Leaving SIPT mode.


// E1 stream and channel configuration for the transit
// Enter to an E1 stream configuration mode
SMG4-[CONFIG]> e1 1
Entering E1-stream mode
// Set SS7
SMG4-[CONFIG]-E1[1]> signaling ss7
E1[1]. Set Signaling 3
// Enable the stream
SMG4-[CONFIG]-E1[1]> enabled
E1[1]. Set line 'on'
// Enter to SS7 configuration mode
SMG4-[CONFIG]-E1[1]> ss7
E1[1]. Signaling is SS7
// Enable transit mode
SMG4-[CONFIG]-E1[1]-[SS7]> transit set usage 4 yes
Transit:
04: remote stream [  0] remote channel [  1] role 'passive' codec '............
NONE' SIP Inteface [00] 'test'
// Set SIP interface for transit
SMG4-[CONFIG]-E1[1]-[SS7]> transit set sip_interface 4 2
Transit:
04: remote stream [  0] remote channel [  1] role 'passive' codec '............
NONE' SIP Inteface [02] 'SIP-interface2'
// Set a channel number on the remote side
SMG4-[CONFIG]-E1[1]-[SS7]> transit set remote_channel 4 1
Transit:
04: remote stream [  0] remote channel [  1] role 'passive' codec '............
NONE' SIP Inteface [02] 'SIP-interface2'
// Set a stream number on the remote side
SMG4-[CONFIG]-E1[1]-[SS7]> transit set remote_stream 4 0
Transit:
04: remote stream [  0] remote channel [  1] role 'passive' codec '............
NONE' SIP Inteface [02] 'SIP-interface2'
// Set active mode for transit
SMG4-[CONFIG]-E1[1]-[SS7]> transit set active 1 yes
 Transit:
04: remote stream [  0] remote channel [  1] role 'active ' codec '............
NONE' SIP Inteface [02] 'SIP-interface2'
//Quit SS7 configuration mode
```

```
SMG4-[CONFIG]-E1[1]-[SS7]> exit
```
Leaving SS7-signaling mode.

// Quit E1 stream configuration mode
```
SMG4-[CONFIG]-E1[1]> exit
```
Leaving E1-stream mode.

// Quit configuration mode
```
SMG4-[CONFIG]> exit
```
Leaving configuration mode.

12 TECHNICAL SUPPORT

Contact Eltex Service Centre to receive technical support on operation of our products:

29B Okruzhnaya Str., Novosibirsk, 630020, Russian Federation
Tel.:
+7(383)274-47-88
+7(383)274-47-87
+7(383)272-83-31
E-mail: techsupp@eltex.nsk.ru

Visit Eltex official website to get relevant technical documentation and software for Eltex products, benefit from our knowledge base, or consult a Service Centre Specialist on our technical forum:

http://eltex.nsk.ru
http://eltex.nsk.ru/downloads
http://eltex.nsk.ru/forum
http://eltex.nsk.ru/eltex_kb
http://eltex.nsk.ru/interaktivnyi-zapros

13 ACCEPTANCE CERTIFICATE AND WARRANTY

The SMG-_____ trunk gateway, serial No. _____, complies with technical specifications TU6650-107-33433783-2014 and is qualified for operation.

The manufacturer, LLC *Eltex*, guarantees that the trunk gateway meets the requirements of technical specifications TU6650-107-33433783-2014 provided its operation conditions correspond to the ones set forth in this Manual.

Warranty period—1 year.

The device does not contain precious materials.

Director _____ A. N. Chernikov
  signature full name

Quality Control Director _____ S. I. Igonin
  signature full name