

Version 2.5.0. Configuring

To move to configuration mode, choose one of the following tab «Network», «VoIP» or «System» depending on the configuration goals:

- «Network» menu is dedicated to implement network settings configuration.
- «VoIP» menu is dedicated to implement the following configuration: SIP settings, accounts settings, codecs installation, VAS and dialplan settings.
- «System» menu is dedicated to configure system time, access to the device via different protocols, change passwords, update firmware.

Configuration mode elements:

- «Network» menu
 - «Internet» submenu
 - «802.1X» submenu
 - «QoS» submenu
 - «MAC management» submenu
 - «Local DNS» submenu
 - «Firewall» submenu
 - «MAC filter» submenu
 - «Static Routes» submenu
- «VoIP» menu
 - «Network settings» submenu (VoIP)
 - «SIP Accounts» submenu
 - «Common SIP settings» submenu
 - «QoS» submenu
 - «Phone Book» submenu
 - «Call history» submenu
- «User interface» menu
 - «Buttons» submenu
 - «Ringtones» submenu
 - «Notifications» submenu
 - «Volume» submenu
- «System» menu
 - «Time» submenu
 - «Access» submenu
 - «Log» submenu
 - «Password» submenu
 - «Configuration Management» submenu
 - «Firmware upgrade» submenu
 - «Reboot» submenu
 - «Autoprovisioning» submenu
 - «Management interface» submenu
 - «Certificates» submenu
 - «Advanced» submenu

«Network» menu

«Network» menu is dedicated to implement network settings configuration.

«Internet» submenu

In the 'Internet' submenu you may configure LAN (via PPPoE, DHCP, and Static).

Network

VoIP

System

Monitoring

Internet

QoS

MAC Management

Local DNS

Firewall

MAC Filter

Static Routes

SNMP

Common Settings

Hostname

Speed and Duplex

Auto

LAN

Protocol

DHCP

Alternative Vendor ID (option 60)

1st DNS Server

2nd DNS Server

MTU

1500

Use VLAN

IPSec Settings

Enable

✓ Apply

✕ Cancel

Common settings

- *Hostname* — device network name.
- *Speed and Duplex* — specify data rate and duplex mode for LAN Ethernet port of the device:
 - *Auto* — automatic speed and duplex negotiation;
 - *100 Half* — 100Mbps data transfer rate with half-duplex mode is supported;
 - *100 Full* — 100Mbps data transfer rate with duplex mode is supported;
 - *10 Half* — 10Mbps data transfer rate with half-duplex mode is supported;
 - *10 Full* — 10Mbps data transfer rate with duplex mode is supported.

LAN

- *Protocol* — select the protocol that will be used for device LAN interface connection to a data network:
 - *Static* — operation mode where IP address and all the necessary parameters for LAN interface are assigned statically;
 - *DHCP* — operation mode where IP address, subnet mask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from DHCP server;
 - *PPPoE* — operation mode when PPP session is established on LAN interface over Ethernet;
 - *No IP* — operation mode when IP address is not assigned to the interface.

Static

When 'Static' type is selected, the following parameters will be available for editing:

- *IP Address* — specify the device LAN interface IP address in the data network;
- *Netmask* — external subnet mask;
- *Default gateway* — address that the packet will be sent to, when route for it is not found in the routing table;
- *1st DNS Server, 2nd DNS Server* — domain name server addresses (allow identifying the IP address of the device by its domain name). You may leave these fields empty, if they are not required;
- *MTU* — maximum size of the data unit transmitted on the network.

DHCP

When 'DHCP' type is selected, the following parameters will be available for editing:

- *Alternative Vendor ID (Option 60)* — when selected, the device transmits Vendor ID (Option 60) field value in Option 60 DHCP messages (Vendor class ID). If the field is empty, Option 60 will not be transmitted in DHCP messages:
[**VENDOR** :device vendor][**DEVICE** :device type][**HW** :hardware version] [**SN** :serial number][**WAN** :WAN interface MAC address][**LAN** :LAN interface MAC address][**VERSION** :firmware version]
Example: [VENDOR:Eltex][DEVICE:VP-12P][HW:1.0][SN:VI23000118] [WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.1.0]
- *Vendor ID (Option 60)* — option 60 value (Vendor class ID) which is transmitted in DHCP messages. When the field is empty, option 60 is not transmitted in DHCP messages.
- *1st DNS Server, 2nd DNS Server* — domain name server addresses (allow identifying the IP address of the device by its domain name. Addresses, which are specified statically, have the higher priority than addresses obtained via DHCP;
- *MTU* — maximum size of the data unit transmitted on the network.

You can manually assign the List of used DHCP options on each network interface (Internet, VoIP, and Management). See Appendix [Version 2.5.0. DHCP client configuration in multiservice mode](#).

PPPoE

When 'PPPoE' type is selected, the following parameters will be available for editing:

- *User Name* — username for authorization on PPP server;
- *Password* — password for authorization;
- *MTU* — maximum size of the data unit transmitted on the network (recommended value — 1492);
- *Service - Name* — service-name tag value in PADI message (this field is optional);
- *Secondary access* — type of access (IPOE) to local area network resources. You may select 2 options:
 - DHCP — dynamic access when IP address and other required parameters are obtained via DHCP;
 - Static — specifying access settings manually: IP address, subnet mask, DNS server, gateway.



When you choose one of the way of IP addresses assignment, the additional parameters will be displayed according to the selected protocol.

- *Use the Secondary Access for VoIP* — this option is available, if there are no dedicated interfaces for VoIP service ('Use Internet settings' checkbox is selected). When the checkbox is not selected (default value), VoIP service uses PPP interface for its operation; when selected, the secondary access interface (IPOE);
- *Alternative Vendor ID (Option 60)* — when selected, the device transmits Vendor ID (Option 60) field value in Option 60 DHCP messages (Vendor class ID). If the field is empty, Option 60 will not be transmitted in DHCP messages:
[**VENDOR** :device vendor][**DEVICE** :device type][**HW** :hardware version] [**SN** :serial number][**WAN** :WAN interface MAC address][**LAN** :LAN interface MAC address][**VERSION** :firmware version]
Example: [VENDOR:Eltex][DEVICE:VP-12P][HW:1.0][SN:VI23000118] [WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.1.0]
 - *Vendor ID (Option 60)* — option 60 value (Vendor class ID) which is transmitted in DHCP messages. When the field is empty, option 60 is not transmitted in DHCP messages.

No IP protocol

When this mode is selected, IP address will not be assigned to the network interface. This mode is used when IP telephony operates in an allocated VLAN.



Be careful when selecting this mode. Before the mode is selected, make sure that VoIP VLAN has been activated (see section «[Network settings](#)» submenu (VoIP)) and there is access for management through the corresponding interface (see section «[Access](#)» submenu).



When using No IP operation mode and acquiring policies through LLDP MED, it is recommended to enable management interface (see section «[Management interface](#)» submenu) and allow access through it (see section «[Access](#)» submenu).

Use VLAN

VLAN — a virtual local area network. VLAN is a group of hosts united in a network not depending on the physical location. The devices grouped to a VLAN have the same identifier VLAN-ID.

- *Use VLAN* — use VLAN identifier specified below to enter the network:
 - *VLAN ID* — VLAN identifier which is used for the device;
 - *802.1P* — 802.1P attribute (also called CoS — Class of Service) is attached to egress Ethernet frames. The value is from 0 (the least priority) to 7 (the highest priority).

IPsec settings

In this section you may configure IPsec encryption (IP Security).

IPsec is a set of protocols used for protection of data transmitted via Internet Protocol that enables authentication, integrity check and/or encryption of IP packets. IPsec also includes secure Internet Key Exchange protocols.

In the current firmware version you may only access the device management interfaces (Web, Telnet) using IPsec.

IPSec Settings

Enable ☒

Interface

Local IP Address

Local Subnet

Local Netmask

Remote Subnet

Remote Netmask

Remote Gateway

NAT-Traversal IPsec

Aggressive Mode ☐

My Identifier Type

My Identifier

Phase 1

Pre-shared Key

IKE Authentication Algorithm

IKE Encryption Algorithm

Diffie Hellman Group

IKE SA Lifetime, s

Phase 2

IKE Authentication Algorithm

IKE Encryption Algorithm

Diffie Hellman Group

IPSec SA Lifetime, s

- **Enable** — enable IPSec protocol utilization for data encryption;
 - **Interface** — this setting takes effect only when PPPoE is selected for the Internet, and defines the interface that will be accessed with IPSec: Ethernet (secondary access interface) or PPP (primary access interface). When DHCP or Static protocol is selected, there is only a single active interface (Ethernet) for the service that may be accessed with IPSec only;
 - **Local IP Address** — device address for IPSec operation;
 - **Local Subnet** together with a **Local Netmask** define a local subnet for creation of network-to-network or network-to-point topologies;
 - **Remote Subnet** together with a **Remote Netmask** define a remote subnet address used for IPSec-encrypted communication. If the mask value is 255.255.255.255, communication is performed with a single host. Mask that differs from 255.255.255.255 allows you to define a whole subnet. Thus, device features allow you to establish 4 network topologies that utilize IPSec traffic encryption: Point-to-Point, Network-to-Point, Point-to-Network, Network-to-Network;
 - **Remote gateway** — gateway used for remote network access;
 - **NAT-Traversal IPsec** — NAT-T mode selection. NAT-T (NAT Traversal) encapsulates IPSec traffic and simultaneously creates UDP packets to be sent correctly by a NAT device. For this purpose, NAT-T adds an additional UDP header before IPSec packet so it would be processed as an ordinary UDP packet and the recipient host would not perform any integrity checks. When the packet arrives to the destination, UDP header is removed and the packet goes further as an encapsulated IPSec packet. With NAT-T technique you may establish communication between IPSec clients in secured networks and public IPSec hosts via firewalls. NAT-T operation modes:
 - **On** — NAT-T mode is activated only when NAT is detected on the way to the destination host;
 - **Force** — use NAT-T in any case;
 - **Off** — disable NAT-T on connection establishment.

The following NAT-T settings are available:

- **NAT-T UDP port** — UDP port for packets for IPSec message encapsulation. Default value is 4500;
- **Interval Between Sending NAT-T Keepalive Packets, s** — periodic message transmission interval for UDP connection keepalive on the device performing NAT functions;

- *Aggressive Mode* — phase 1 operation mode when all the necessary information is exchanged using three unencrypted packets. In the main mode, the exchange process involves six unencrypted packets.
- My Identifier Type — device identifier type: address, fqdn, keyed, user_fqdn, asn1dn;
- My Identifier — device identifier used for identification during phase 1 (fill in, if required). Identifier format depends on the type.

Phase 1

During the first step (phase), two hosts negotiate on the identification method, encryption algorithm, hash algorithm and Diffie Hellman group. Also, they identify each other. For phase 1, there are the following settings:

- *Pre-shared Key* — a secret key used by authentication algorithm in phase 1. It is represented by a string from 8 to 63 characters;
- *IKE Authentication Algorithm* — select an authentication algorithm from the list: MD5, SHA1;
- *IKE Encryption Algorithm* — select an encryption algorithm from the list : DES, 3DES, Blowfish;
- *Diffie Hellman Group* — select an Diffie-Hellman group;
- *IKE SA Lifetime, s* — time that should pass for hosts' mutual re-identification and policy comparison (other name 'IKE SA lifetime'). Default value is 24 hours (86400 seconds).

Phase 2

During the second step, key data is generated; hosts negotiate on the utilized policy. This mode—also called as 'quick mode'—differs from the phase 1 in that it may be established after the first step only, when all the phase 2 packets are encrypted.

- *IKE Authentication Algorithm* — select an authentication algorithm from the list: HMAC - MD5, HMAC-SHA1, DES, 3DES;
- *IKE Encryption Algorithm* — select an encryption algorithm from the list: DES, 3DES, Blowfish;
- *Diffie Hellman Group* — select Diffie-Hellman group;
- *IPSec SA Lifetime, s* — time that should pass for the data encryption key changeover (other name 'IPSec SA lifetime'). Default value is 60 minutes (3600 seconds).



To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button.

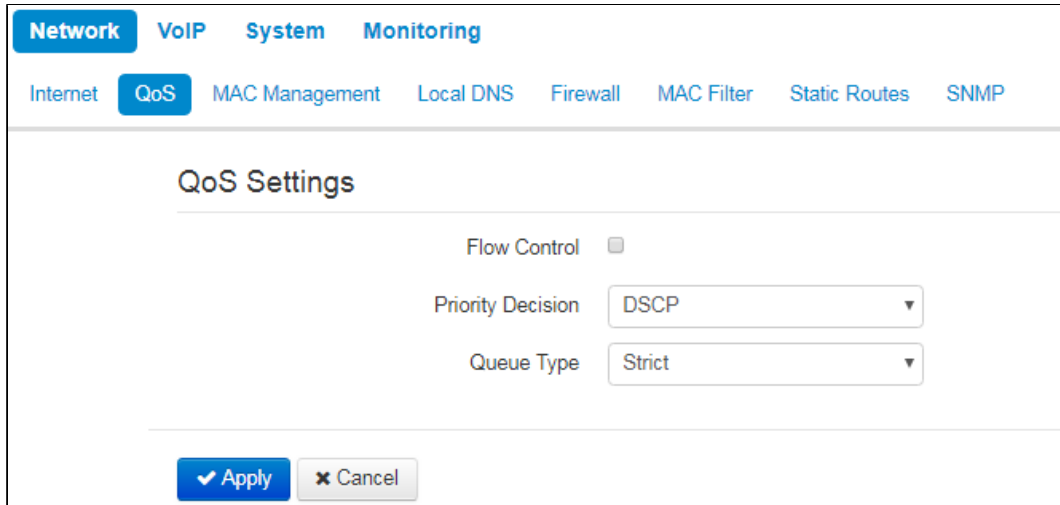
«802.1X» submenu

In «802.1X» submenu, you may configure parameters for authentication in compliance with 802.1X specification.


- Enable — check the box to enable authentication in compliance with 802.1X specification:
 - User Name — a user name which will be used while authentication;
 - Password — a password which is used for authentication;
 - Auth Period — a timer used by the Supplicant PAE to determine how long to wait for a response from the Authenticator before timing it out;
 - Held Period — a timer used by the Supplicant state machine to define periods of time during which it will not attempt to acquire an Authenticator;
 - Max Starts — the maximum number of successive EAPOL-Start messages that will be sent before the Supplicant assumes that there is no Authenticator present.

«QoS» submenu


In the 'QoS' submenu, you may configure traffic processing priority and queue type.



- *Flow control* — enabling/disabling a mechanism of data flow management by using TCP;
- *Priority decision* — select traffic prioritization way:
 - *DSCP* — classification mechanism of traffic control and providing quality of service by priorities;
 - *802.1p* — attribute (*CoS* — *Class of Service*) is attached to egress Ethernet frames. The value is from 0 (the least priority) to 7 (the highest priority).

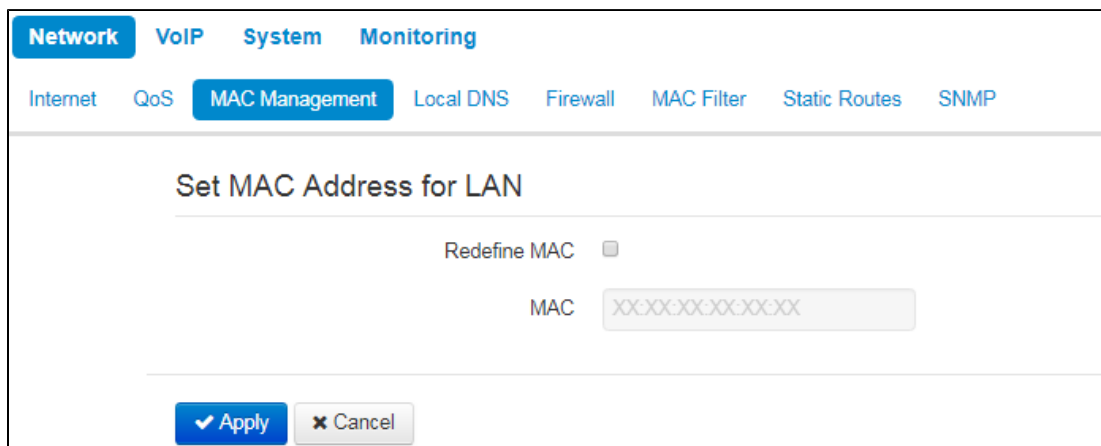
 Settings of the priorities are not available when flow control is enabled.

- *Queue type* — select service procedure of queues:
 - *Strict* — service procedure of queues when traffic with lowest priority is transmitted only after transmitting queues with higher priority;
 - *WRQ* — service procedure of queues, when accessible bandpass is divided among queues in proportion with priority:
 - *Weight 0..5* — define priority weight in the range from 1 to 127. Then weight is higher then traffic is more priority.

 To apply a new configuration and store settings into the non-volatile memory, click '*Apply*' button. To discard changes, click '*Cancel*' button.

«MAC management» submenu

In the 'MAC management' submenu you may change MAC address of the device LAN interface.



- *Redefine* — when selected, MAC address from the MAC field is used on the Internet interface;
- *MAC* — MAC address that will be assigned to the device network interface.

To redefine MAC for 'VoIP' or 'Management VLAN' interface, use sections 'Set MAC address for interface 'VoIP'' or 'Set MAC address for interface 'Management VLAN''.

✔ To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button.

«Local DNS» submenu

In 'Local DNS' submenu you may configure a local DNS server by adding 'IP address — domain name' pairs into the database.

Local DNS allows the gateway to obtain IP address of the communicating device by its domain name. You may use local DNS in cases when DNS server is missing from the network segment that the gateway belongs to, and you need to establish routing using network names, or when you have to use SIP server network name as its address. Although, you have to know the matches between hostnames (domains) and their IP addresses.

NetworkVoIPSystemMonitoring

InternetQoSMAC ManagementLocal DNSFirewallMAC FilterStatic RoutesSNMP

List of Domain Names

	Domain Name	IP Address
<input type="checkbox"/>	test.ru	192.168.12.12

+ Add

Remove

To add the address into the list, click 'Add' button in the 'New domain name' window and fill in the following fields:

New Domain Name

Domain Name

IP Address

✔ Apply

✕ Cancel

- Domain name — host name;
- IP address — host IP address.

✔ Click 'Apply' to create 'IP address—domain name' pair. To discard changes, click 'Cancel' button. To remove the record from the list, select the checkbox next to the respective record and click 'Delete'.

«Firewall» submenu

In the 'Firewall' submenu you may set the rules for the incoming and outgoing traffic transmission. You may restrict transmission of various traffic types (incoming, outgoing, transit) depending on the protocol, source and destination IP addresses, source and destination TCP/UDP ports (for TCP or UDP messages), ICMP message type (for ICMP messages).

Network
VoIP
System
Monitoring

Internet
QoS
MAC Management
Local DNS
Firewall
MAC Filter
Static Routes
SNMP

Rules for Input Traffic

Name	Protocol	Source IP Address	Source Ports	Destination Ports	Action
------	----------	-------------------	--------------	-------------------	--------

Rules for Output Traffic

Name	Protocol	Source Ports	Destination IP Address	Destination Ports	Action
------	----------	--------------	------------------------	-------------------	--------

Add
Remove

To add a new rule, click 'Add' button and fill in the following fields in the 'Add a New Rule' window:

Add a New Rule

Name

Traffic Type

Protocol

Source IP Address

Source Ports

Destination Ports

Action

Apply
Cancel

- *Name* — rule name;
- *Traffic Type* — select traffic type to which this rule will apply:
 - *Input* — incoming device traffic (recipient is one of the device network interfaces);
 - *Output* — outgoing device traffic (traffic generated locally by the device from one of the network interfaces):
 - *Source IP Address* — define starting source IP address. Use '/' symbol to define a mask in 'xxx.xxx.xxx.xxx' or 'xx' format, e.g. 192.168.16.0/24 or 192.168.16.0/255.255.255.0, when you need to specify an address range (/24 mask record corresponds to /255.255.255.0);
 - *Destination IP Address* — define destination IP address. Use '/' symbol to define a subnet mask in 'xxx.xxx.xxx.xxx' or 'xx' format, e.g. 192.168.18.0/24 or 192.168.18.0/255.255.255.0, when you need to highlight an address range.
- *Protocol* — packet protocol to which this rule will apply:
 - TCP;
 - UDP;
 - TCP/UDP;
 - ICMP;
 - Any.
- *Action* — an action to be performed on packets (reject/skip).

When TCP, UDP, TCP/UDP are selected, the following settings will become available for editing:

- *Source ports* — list of source ports with packets falling under the rule (a single port or port range delimited by '-' is permitted);
- *Destination ports* — list of destination ports. The packets of a destination port fall under this rule (a single port or port range delimited by '-' is permitted).

When ICMP protocol is selected, the following setting will be available for editing:

- *Message type* — you may create a rule for the specific ICMP message type only or for all ICMP message types.



Click 'Apply' button to add a new rule. To discard changes, click 'Cancel' button. To remove the record from the list, select the checkbox next to the respective record and click 'Delete'.

«MAC filter» submenu

In the 'MAC filter' submenu, you may configure access filtering by host's MAC address.

Wired Connection Filter Mode — define one of the three filter operation modes depending on the host's MAC address:

- *Disabled* — MAC address filtering is disabled, all clients are allowed to connect to the device;
- *Deny* — in this filter operation mode, hosts with MAC addresses from the 'MAC address list' are denied to connect to the device. Hosts with unlisted MAC addresses are allowed to connect to the device;
- *Allow* — in this filter operation mode, hosts with MAC addresses from the 'MAC address list' are allowed to connect to the device. Hosts with unlisted MAC addresses are denied to connect to the device.

MAC address list

You may enter up to 30 host MAC addresses which may access the device in accordance to the specified filtering mode.

To add a new host to the list, click 'Add' button and enter its MAC address.



To apply a new configuration and store settings into the flash memory, click 'Apply' button. To discard changes, click 'Cancel' button.

«Static Routes» submenu

In the 'Static routes' submenu you may configure device static routes.

Network
VoIP
System
Monitoring

Internet
QoS
MAC Management
Local DNS
Firewall
MAC Filter
Static Routes
SNMP

Static Routes

	Name	Destination IP	Netmask	Gateway
	route1	192.168.23.0	255.255.255.0	192.168.0.254

+ Add
Remove

To add a new route, click 'Add' button and fill in the following fields:

Add Route

Name

Destination IP

Netmask

Gateway

- *Name*— route name, used for human perception convenience. You may leave this field empty;
- *Destination IP*— IP address of destination host or subnet that the route should be established to;
- *Netmask*— subnet mask. Subnet mask for host should be 255.255.255.255, for subnet—depending on its size;
- *Gateway*— gateway IP address that allows for the access to the 'Destination IP'.



To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button.

«VoIP» menu

In the 'VoIP' menu you may configure VoIP (Voice over IP): SIP protocol configuration, account configuration, installation of codecs, VAS and dial plan.

«Network settings» submenu (VoIP)

In the "VoIP" menu — 'Network Settings' submenu you may specify custom network settings for VoIP service.

Network
VoIP
System
Monitoring

Network Settings
SIP Accounts
Common SIP Settings
QoS
Phone Book
Call History

VoIP Network Settings

Use Internet Settings
☐

Use VLAN
☒

VLAN ID

802.1P

Protocol

Alternative Vendor ID (option 60)
☐

1st DNS Server

2nd DNS Server

IPSec Settings

Enable
☐

- *Use Internet Settings* — when selected, use network settings specified in the 'Network' -> 'Internet' menu, otherwise use settings specified in this menu;

VLAN settings

- *Use VLAN* — when selected, VoIP service will use a dedicated interface in a separate VLAN for its operation, with VLAN number specified in 'VLAN ID' field;
- *VLAN ID* — VLAN identifier which is used for the network interface;
- *802.1P* — attribute (CoS — Class of Service) is attached to egress Ethernet frames. The value is from 0 (the least priority) to 7 (the highest priority).

Network settings

- *Protocol* — select protocol assigning address to VoIP service interface:
 - *Static* — operation mode where IP address and all the necessary settings for LAN interface are assigned manually. When 'Static' type is selected, the following parameters will be available for editing;
 - *DHCP* — operation mode where IP address, subnet mask, DNS address and other necessary settings for service operation (e.g. SIP and registration server static routes) are automatically obtained from DHCP server;

Static

When 'Static' type is selected, the following parameters will be available for editing:

- *IP Address* — specify the device LAN interface IP address in the provider network;
- *Netmask* — external subnet mask;
- *Default gateway* — address that the packet will be sent to, when route for it is not found in the routing table;
- *1st DNS Server, 2nd DNS Server* — domain name server addresses (allow identifying the IP address of the device by its domain name). You may leave these fields empty, if they are not required;
- *MTU* — maximum size of the data unit transmitted on the network.

DHCP

When 'DHCP' type is selected, the following parameters will be available for editing:

- *Alternative Vendor ID (Option 60)* — when selected, the device transmits Vendor ID (Option 60) field value in Option 60 DHCP messages (Vendor class ID). If the field is empty, Option 60 will not be transmitted in DHCP messages:
[**VENDOR** :device vendor][**DEVICE** :device type][**HW** :hardware version] [**SN** :serial number][**WAN** :WAN interface MAC address][**LAN** :LAN interface MAC address][**VERSION** :firmware version]
Example: [VENDOR:Eltex][DEVICE:VP-12P][HW:1.0][SN:VI23000118] [WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.1.0]
- *Vendor ID (Option 60)* — option 60 value (Vendor class ID) which is transmitted in DHCP messages. When the field is empty, option 60 is not transmitted in DHCP messages.
- *1st DNS Server, 2nd DNS Server* — domain name server addresses (allow identifying the IP address of the device by its domain name. Addresses, which are specified statically, have the higher priority than addresses obtained via DHCP;
- *MTU* — maximum size of the data unit transmitted on the network.

You can manually assign the List of used DHCP options on each network interface (Internet, VoIP, and Management). See Appendix [Version 2.5.0. DHCP client configuration in multiservice mode](#).

IPsec settings

In this section you may configure IPsec encryption (IP Security). IPsec is a set of protocols used for protection of data transmitted via Internet Protocol that enables authentication, integrity check and/or encryption of IP packets. IPsec also includes secure Internet Key Exchange protocols.

In the current firmware version you may only access the device management interfaces (Web and Telnet) using IPsec.

For detailed information on IPsec settings see «Internet» submenu section [IPsec settings](#).



To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button.

«SIP Accounts» submenu

Use drop-down 'SIP Accounts' menu to select account for editing.

You can assign own SIP server addresses, registration servers, voice codecs, individualized dialing plan and other parameters for each account.

General settings

Network
VoIP
User Interface
System
Monitoring

Network Settings
SIP Accounts
Common SIP Settings
QoS
Phone Book
Call History

SIP Accounts

Account
Account 1

General Settings
Codecs
Service Settings
Additional Parameters
Dialplan

Enable
☒

Account Name
4804-smg

Phone
4804

User Name

Use Alternative Number
☐

SIP Port
5060

Calling Party Category
Off

Voice Mail Number

- *Enable*— when selected, account is active;
- *Account Name*— an account tag, which will be used for identifying active account or account by default;
- *Phone*— subscriber number assigned to the account;
- *User Name*— user name associated with the account (shown in '*Display-Name*' field of '*From*' header in the outgoing SIP messages);
- *Use Alternative Number*— when selected, an alternative number will be inserted into the '*From*' header of SIP messages sent from this account (particularly, in order to hide the real number from the Caller ID system of the callee):
 - *Use As a Contact Header*— alternative number assigned to a phone port will be changed to specified number and inserted into '*Contact*' header of the SIP message.
- *SIP Port*— UDP port for incoming SIP message reception for this account, and for outgoing SIP message transmission from this account. It may take values from 1 to 65535 (default value: 5060);
- *Calling Party Category*— enables transmission of outgoing messages in the '*From*' header; the last header is transmitted in Tel-URI format (see RFC3966);
- *Voice Mail Number*— a number which a call will be established to when subscriber selects "Call" (to listen voice mail messages) in voice mail menu.

Authentication

Authentication

Login

Password

- *Login* — user name used for subscriber authentication on SIP server (and on registration server);
- *Password*— password used for subscriber authentication on SIP server (and on registration server).

SIP parameters

Use '*SIP Parameters*' section to configure SIP parameters of the account.

SIP Parameters

Proxy Mode	Homing ▼
Proxy Server	smg1016m.test.loc
Registration	<input checked="" type="checkbox"/>
Registration Server	smg1016m.test.loc
Home Server Check Method	Invite ▼
Transport	UDP (preferred), TCP ▼
Invite Initial Timeout, ms	500
Invite Initial Max Timeout, ms	4000
Invite Total Timeout, ms	32000
Subscribe for MWI	<input type="checkbox"/>
Subscription Server	192.168.8.232

- *Proxy Mode* — you can select SIP server operation mode in the drop-down list:
 - Off;
 - Parking — SIP-proxy redundancy mode without main SIP-proxy management;
 - Homing — SIP-proxy redundancy mode with main SIP-proxy management.

The phone may operate with a single main SIP-proxy and up to four redundant SIP-proxies. For exclusive operations with the main SIP-proxy, 'Parking' and 'Homing' modes are identical. In this case, if the main SIP-proxy fails, it will take time to restore its operational status.

For operations with redundant SIP-proxies, 'Parking' and 'Homing' modes will work as follows:

The gateway sends INVITE message to the main SIP-proxy address when performing outgoing call, and REGISTER message when performing registration attempt. If on expiration of 'Invite total timeout' there is no response from the main SIP-proxy or response 408 or 503 is received, the phone sends INVITE (or REGISTER) message to the first redundant SIP-proxy address. If it is not available, the request is forwarded to the next redundant SIP-proxy and so forth. When available redundant SIP-proxy is found, registration will be renewed on that SIP-proxy.

Next, the following actions will be available depending on the selected redundancy mode:

In the 'parking' mode, the main SIP-proxy management is absent, and the phone will continue operation with the redundant SIP-proxy even when the main proxy operation is restored. If the connection to the current SIP-proxy is lost, querying of the subsequent SIP-proxies will be continued using the algorithm described above. If the last redundant SIP-proxy is not available, the querying will continue in a cycle, beginning from the main SIP-proxy.

In the 'homing' mode, three types of the main SIP-proxy management are available: periodic transmission of OPTIONS messages to its address, periodic transmission of REGISTER messages to its address, or transmission of INVITE request when performing outgoing call. First of all, INVITE request is sent to the main SIP-proxy, and if it is unavailable, then the next redundant one, etc. Regardless of the management type, when the main SIP-proxy operation is restored, the gateway will use it to renew its registration. The gateway will begin operation with the main SIP-proxy.

- *Proxy Server* — network address of a SIP server — device that manages access to provider's phone network for all subscribers. You may specify IP address as well as the domain name (specify SIP server UDP port after the colon, default value is 5060);
- *Registration* — when selected, register ports that utilize this profile on registration server;
- *Registration Server* — network address of a device that is used for registration of all phone network subscribers in order to provide them with the communication services (specify registration server UDP port after the colon, default value is 5060). You may specify IP address as well as the domain name (you may specify UDP port of a SIP server after the colon, default value is 5060). As a rule, registration server is physically co-located with SIP proxy server (they have the same address);
- *Home Server Check Method* — select availability control method for the primary SIP server in 'Homing' mode:
 - *Invite* — control via transmission of INVITE request to its address when performing an outgoing call;
 - *Register* — control via periodic transmission of REGISTER messages to its address;
 - *Options* — control via periodic transmission of OPTIONS messages to its address.
- *Home Server Keepalive Timeout, s* — periodic message transmission interval in seconds; used for primary SIP server availability check;
- *Transport* — select protocol for SIP messages transport;
- *Invite Initial Timeout, ms* — a time interval between first INVITE transmission and the second one in case there is no answer on the first INVITE (ms). For the following INVITE requests (third, forth, fifth etc.) the interval will be increased twice (i.e. if the value is 300 ms, the second INVITE will be sent in 300 ms, the third — in 600 ms, the forth — in 1200 ms, etc.);
- *Invite Initial Max Timeout, ms* — the maximum time interval for retransmitting non-INVITE requests and responses on INVITE requests;
- *Invite Total Timeout, ms* — common timeout of INVITE requests transmission (ms). When the timeout is expired, it is defined that the route is not available. INVITE requests retranslation is limited for availability definition as well;

- *Subscribe for MWI*— when checked, the subscription request on "message-summary" events is send. After obtaining such request, subscription server will notify the device on new voice messages through sending NOTIFY requests;
- *Subscription Server*— a network address, to which SUBSCRIBE requests are sent for subscription on "message-summary" and "dialog" events. You may specify IP address as well as domain name (after colon, you may specify a UDP port of SIP server, default value is 5060).



If you use different values of timeouts on different accounts, be sure that SIP port of the accounts are different as well.

Reserved Proxy

Reserved Proxy

Proxy Server	Registration Server
<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>
<input type="button" value="+ Add"/> <input type="button" value="Remove"/>	

To add redundant SIP proxy, click 'Add' button and enter the following settings:

- *Proxy Server*— network address of redundant SIP server. You may specify IP address as well as the domain name (specify SIP server UDP port after the colon, default value is 5060);
- *Registration Server*— network address of redundant registration server (specify UDP port after the colon, default value is 5060). You may specify IP address as well as the domain name. If the '*Registration server*' checkbox is selected, the redundant server registration is enabled.

To remove the redundant SIP proxy, select the checkbox next to the specified address and click '*Delete*' button.

Additional SIP Properties

Additional SIP Properties

SIP Domain	elttest.loc
Use Domain to Register	<input checked="" type="checkbox"/>
Use Domain to Subscribe	<input checked="" type="checkbox"/>
Outbound Mode	Off
Expires, s	1800
Registration Retry Interval, s	30
Subscription Expires, s	1800
Subscription Retry Interval, s	30
STUN Enable	<input type="checkbox"/>
Public IP Address	
Use SIP Display Name in Register	<input type="checkbox"/>
Ringback at 183 Progress	<input type="checkbox"/>
Reliable provisional responses (1xx)	Supported
Timer Enable	<input checked="" type="checkbox"/>
Min SE, s	120
Session Expires, s	1800
Keepalive NAT Sessions Mode	Off
Rejecting SIP Response	480 Temporarily Unavailable
Use Alert-Info Header	<input type="checkbox"/>
Check RURI User Part Only	<input type="checkbox"/>
Send IP Address in Call-ID Header	<input type="checkbox"/>

- *SIP Domain* — domain where the device is located (fill in, if needed);
- *Use Domain to Register* — when selected, apply SIP domain for registration (SIP domain will be inserted into the 'Request-Line' of 'Register' requests);
- *Use Domain to Subscribe* — when checked, apply SIP domain for subscription (SIP domain will be inserted into 'Request-Line' of 'SUBSCRIBE' requests);
- Outbound Mode:
 - *Off* — calls will be routed according to the dialplan;
 - *Outbound* — dialplan is required for outgoing communications; however, all calls will be routed via SIP server; if there is no registration, PBX response will be sent to the subscriber in order to enable subscriber service management (VAS management);
 - *Outbound with «Busy»* — dialplan is required for outgoing communications; however, all calls will be routed via SIP server; if there is no registration, VoIP will be unavailable — error tone will be transmitted to the phone headset.
- *Expires, s* — time for account registration on SIP server. At the average, account registration renewal will be performed after 2/3 of the specified period;
- *Registration Retry Interval, s* — when the registration is unsuccessful, time period between SIP server registration attempts;
- *Subscription Expires, s* — valid time of subscription on events. The subscription renewal is usually performed in 2/3 of the specified period;
- *Subscription Retry Interval, s* — time interval between unsuccessful attempt to subscribe on events and the next try;
- *STUN Enable* — when checked, STUN (Session Traversal Utilities for NAT) protocol is used for public address of the device definition (external NAT address);



If you use different STUN settings on the different accounts, be sure that SIP ports are different as well.

- **Public IP Address**— this parameter is used as an external address of the device when it operates behind the NAT (gateway). As a public address, you may specify an external address (WAN) of a gateway (NAT) that VP-12(P) operates through. At that, on the gateway (NAT), you should forward the corresponding SIP and RTP ports used by the device;
- **Use SIP Display Name in Register**— when selected, use username in 'SIP Display Info' field of the 'Register' message;
- **Ringback at 183 Progress**— when selected, 'ringback' tone will be sent upon receiving '183 Progress' message (w/o enclosed SDP);
- **100rel**— use reliable provisional responses (RFC3262):
 - **Supported**— reliable provisional responses are supported;
 - **Required**— reliable provisional responses are mandatory;
 - **Off**— reliable provisional responses are disabled.

SIP protocol defines two types of responses for connection initiating requests (INVITE)—provisional and final. 2, 3, 4, 5 and 6-class responses are final and their transfer is reliable, with ACK message confirmation. 1-class responses, except for '100 Trying' response, are provisional, without confirmation (RFC3261). These responses contain information on the current INVITE request processing step, therefore loss of these responses is unacceptable. Utilization of reliable provisional responses is also stated in SIP (RFC3262) protocol and defined by '100rel' tag presence in the initiating request. In this case, provisional responses are confirmed with PRACK message.

100rel setting operation for outgoing communications:

- **Supported**— send the following tag in 'INVITE' request — supported:100rel. In this case, communicating gateway may transfer provisional responses reliably or unreliably — as it deems fit;
- **Required**— send the following tags in 'INVITE' request — supported: 100rel and required:100rel. In this case, communicating gateway should perform reliable transfer of provisional replies. If communicating gateway does not support reliable provisional responses, it should reject the request with message 420 and provide the following tag — unsupported: 100rel. In this case, the second INVITE request will be sent without the following tag—required: 100rel;
- **Off**— do not send any of the following tags in INVITE request — supported: 100rel and required: 100rel. In this case, communicating gateway will perform unreliable transfer of provisional replies.

100rel setting operation for incoming communications :

- **Supported, Required**— when the following tag is received in 'INVITE' request—supported: 100rel, or required: 100rel — perform reliable transfer of provisional replies. If there is no supported: 100rel tag in INVITE request, the gateway will perform unreliable transfer of provisional replies;
- **Off**— when the following tag is received in 'INVITE' request—required: 100rel, reject the request with message 420 and provide the following tag — unsupported: 100rel. Otherwise, perform unreliable transfer of provisional replies.
- **Timer Enable**— when selected, the 'timer' (RFC 4028) extension support is enabled. When connection is established, and both sides support 'timer' extension, one of them periodically sends re-INVITE requests for connection monitoring purposes (if both sides support UPDATE method, wherefore it should be specified in the 'Allow' header, the session update is performed by periodic transmission of UPDATE messages);
- **Min SE, s**— minimal time interval for connection health checks (90 to 1800s, 120s by default);
- **Session Expires, s**— period of time in seconds that should pass before the forced session termination if the session is not renewed in time (90 to 80000s, recommended value—1800s, 0—unlimited session);
- **Keepalive NAT Sessions Mode**— select SIP server polling method:
 - **Off**— SIP server will not be polled;
 - **Options**— SIP server polling with OPTIONS message;
 - **Notify**— SIP server polling with NOTIFY message;
 - **CLRF**— SIP server polling with an empty UDP packet.
- **Keepalive Timeout, s**— SIP server polling time period, in seconds;
- **Rejecting SIP Response**— select SIP response on incoming call rejection;
- **Use Alert-Info Header**— process INVITE request 'Alert-Info' header to send a non-standard ringing to the subscriber port;
- **Check RURI User Part Only**— when selected, only subscriber number (user) will be analyzed, and if the number matches, the call will be assigned to the subscriber port. When unselected, all URI elements (user, host and port—subscriber number, IP address and UDP/TCP port) will be analyzed upon receiving an incoming call. If all URI elements match, the call will be assigned to the subscriber port;
- **Send IP Address in CallID Header**— when selected, during outgoing communications, device custom IP address will be used in 'Call-ID' header in 'localid@host' format.



To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button.

Codecs

SIP Accounts

Account Account 1

General Settings

Codecs

Service Settings

Additional Parameters

Dialplan

Codecs Priority

Codec 1 G.711a

Codec 2 G.729

Codec 3 G.711u

Codec 4 G.723

Codec 5 G.726-24

Codec 6 G.726-32

Codec 7 Off

Packet Time

G.711 Packet Time, ms 20

G.729 Packet Time, ms 20

G.723 Packet Time, ms 30

G.726-24 Packet Time, ms 20

G.726-32 Packet Time, ms 20

Payload Type

G.726-24 Payload Type 103

G.726-32 Payload Type 104

✓ Apply

✕ Cancel

- *Codec 1..7*— you may select a codec and an order of their usage. The highest priority codec should be specified in the 'Codec 1' field. For operation, you should specify at least one codec:
 - *Off* — codec will not be used;
 - G.711a — use G.711A codec;
 - G.711u — use G.711U codec;
 - G.723 — use G.723.1 codec;
 - G.729 — use G.729 codec;
 - G.726-24 — use G.726 codec with the rate of 24 kbps;
 - G.726-32 — use G.726 with the rate of 32 kbps.
- *Packet time* — amount of voice data in milliseconds (ms) transmitted in a single RTP packet for the corresponding codec G.711, G.729, G.723 and G.726;
- *Payload Type* — payload type of G.726-24 or G.726-32 codec (acceptable values are in the range from 96 to 127).



To apply a new configuration and store settings into the non-volatile memory, click '*Apply*' button. To discard changes, click '*Cancel*' button.

Service settings

Network
VoIP
User Interface
System
Monitoring

Network Settings
SIP Accounts
Common SIP Settings
QoS
Phone Book
Call History

SIP Accounts

Account
Account 1

General Settings
Codecs
Service Settings
Additional Parameters
Dialplan

Call Waiting ☒
DND ☐
Stop Dial At # ☐
CLIR Off
Hotline ☐

Allow Receiving Intercom Call ☒
Generate Tone ☒
Intercom Call Priority ☐

Allow Auto Call Answering ☒
Notify Me Before Auto Answer ☐
Auto Call Answering Priority ☐
Auto Call Answering Delay, s 0

- **Call Waiting** — when checked, the subscriber will accept incoming calls while being in a call state, otherwise '484 Busy here' reply will be sent;
- **DND** — when checked, temporary restriction is placed for incoming calls (DND service — Don't Disturb);
- **Stop Dial At #** — when checked, use '#' button on the phone unit to end the dialing, otherwise '#' will be recognized as a part of the number;
- **CLIR** — limitation of caller number identification:
 - **Off** — CLIR service is disabled;
 - **SIP : From** — *Anonymous sip:anonymous@unknown.host* will be transmitted in the 'From' header of SIP messages;
 - **SIP:From and SIP:Contact** — *Anonymous sip:anonymous@unknown.host* will be sent in the 'From' and 'Contact' headers of SIP messages.
- **Hotline** — when checked, 'Hotline' service is enabled. This service enables an outgoing connection automatically without dialling the number after the phone handset is picked up with the defined delay (in seconds). When checked, fill in the following fields:
 - **Hot Number** — phone number that will be used for connection establishment upon 'Delay timeout' expiration after the phone handset is picked up (in SIP profile being used, a prefix for this direction should be defined in the dialplan);
 - **Hot Timeout, s** — time interval that will be used for connection establishment with the opposite subscriber, in seconds.
- **Allow Receiving Intercom Call** — when unchecked, incoming intercom calls are declined automatically;
- **Generate Tone** — short sound signal is played before automatic answering to an incoming intercom call;
- **Intercom all Priority** — when checked, an incoming intercom call has higher priority than an active call. Before answering to incoming intercom call, an active call is put on hold. When the option is disabled, the function of automatic answering to intercom calls during active call is disabled;
- **Allow Auto Call Answering** — when the option is enabled all incoming calls will be answered automatically;
- **Notify Me Before Auto Answer** — short audio signal is played before automatic answering;
- **Auto Call Answering Priority** — when checked, an incoming call has higher priority than an active call. Before answering to incoming call, an active call is put on hold. When the option is disabled, the function of automatic answering to incoming calls during active call is disabled;
- **Auto Call Answering Delay, s** — time interval in seconds between the incoming call and the automatic answer to it.



To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button.

Redirection parameters

Call Forwarding

CFU ☒

CFU Number

CFB ☒

CFB Number

CFNR ☒

CFNR Number

CFNR Timeout

- *CFU*— when selected, CFU (Call Forward Unconditional) service is enabled — all incoming calls will be forwarded to the specified call forward unconditional number:
 - *CFU Number*— number that all incoming calls will be forwarded to when Call forward unconditional service is enabled (in SIP profile being used, a prefix for this direction should be defined in the dialplan).
- *CFB*— when selected, CFB (Call Forward on Busy) service is enabled—forward the call to the specified number, when the subscriber is busy:
 - *CFB Number*— number that incoming calls will be forwarded to when the subscriber is busy and Call forward on busy service is enabled (in SIP profile being used, a prefix for this direction should be defined in the dialplan).
- *CFNR*— when selected, CFNA (Call Forward on No Answer) service is enabled—forward the call, when there is no answer from the subscriber:
 - *CFNR Number*— number that incoming calls will be forwarded to when there is no answer from the subscriber and 'Call forward on no answer' service is enabled (in SIP profile being used, a prefix for this direction should be defined in the dialplan);
 - *CFNR Timeout* — time interval that will be used for call forwarding when there is no answer from the subscriber, in seconds.

When multiple services are enabled simultaneously, the priority will be as follows (in the descending order):

- CFU;
- DND;
- CFB, CFNA.

Three-party conference

Three-party Conference

Mode

Conference Server

- *Mode*— operation mode of three-party conference. Two modes are possible:
 - *Local*— conference assembly is performed locally by the device after pressing 'CONF';
 - *Remote (RFC 4579)*— conference assembly is performed at the remote server; after pressing 'CONF', 'Invite' message will be sent to the server using number specified in the 'Conference server' field. In this case, conference operation complies with the algorithm described in RFC4579.
- *Conference Server* — in general, address of the server that establishes conference using algorithm described in RFC4579. Address is specified in the following format SIP-URI: user@address:port. You may specify the 'user' URI part only—in this case, 'Invite' message will be sent to the SIP proxy address.

Additional Parameters

Network

VoIP

User Interface

System

Monitoring

Network Settings

SIP Accounts

Common SIP Settings

QoS

Phone Book

Call History

SIP Accounts

Account

Account 1

General Settings

Codecs

Service Settings

Additional Parameters

Dialplan

DTMF Transfer

RFC 2833

RFC2833 Payload Type

96

Use the Same PT Both for Transmission and Reception

☐

Silencedetector

☐

Echocanceller

☒

RTCP

☐

Allow Call Pickup

☒

Call Pickup Mode

Replaces

RTP

Min RTP Port

23000

Max RTP Port

26000

DTMF Transfer— mode of DTMF signal transmission:

- *Inband*— inband transmission;
- *RFC2833*— according to RFC2833 recommendation as a dedicated payload in RTP voice packets;
- *SIP info*— transfer messages via SIP in INFO requests.
- *RFC2833 Payload Type*— payload type for packet transmission via RFC2833 (permitted values: from 96 to 127);
- *Use the Same PT Both for Transmission and Reception*— option is used in outgoing calls for payload type negotiation of events sent via RFC2833 (DTMF signals). When selected, event transmission and reception via RFC2833 is performed using the payload from 200Ok message sent by the opposite side. When unselected, event transmission is performed via RFC2833 using the payload from 200Ok being received, and reception—using the payload type from its own configuration (specified in the outgoing Invite);
- *Silencedetector*— when selected, enable voice activity detector;
- *Echocanceller*— when selected, use echo cancellation;
- *Dispersion Time, ms*— parameter that cancels an echo caused by the voice signal dispersion. Parameter values may be specified in the interval from 2ms to 128ms;
- *RTCP*— when selected, use RTCP for voice link monitoring:
 - *Sending Interval*— RTCP packet transmission period, in seconds;
 - *Receiving Period*— RTCP message reception period measured in transmission period units; if there is not a single RTCP packet received until the reception period expires, VP-12(P) will terminate the connection;
 - *RTCP - XR*— when selected, RTCP Extended Reports will be sent according to RFC 3611.
- *Allow Call Pickup*— when the flag is set, pressing the BLF key will initiate the interception of the incoming call to the subscriber on which the BLF key is configured;
- *Call Pickup Mode*— the way the call is intercepted:
 - *Replaces*— call pickup using the Replaces header;
 - *Feature Code*— call pickup using the prefix added to the number of the subscriber on which the BLF key is configured.
- *Call Pickup Code*— prefix which will be added to the number of the subscriber to which the BLF key is configured;
- *Sign '#' terminates the number*— adding the '#' symbol when intercepting a call after the number of the subscriber to which the BLF key is configured.

RTP

- *Min RTP Port*— lower limit of the RTP ports range used for voice traffic transmission;
- *Max RTP Port*— upper limit of the RTP ports range used for voice traffic transmission.

SRTP

SRTP

Enable ☐

Crypto Suite 1

AES_80

Crypto Suite 2

AES_32

- *Enable* — when selected, RTP flow encryption is used. Thus, the RTP/SAVP profile will be specified in SDP of outgoing INVITE requests. Also, the SDP of incoming requests will be scanned for the RTP/SAVP profile. If the RTP/SAVP profile is not found, the call will be rejected;
- Crypto Suite 1-2 — allows to choose encryption and hashing algorithms to be used. A suite with the highest priority should be specified in “Crypto Suite 1” field. You have to specify at least one crypto suit:
 - AES_80 — according to AES_CM_128_HMAC_SHA1_80;
 - AES_32 — according to AES_CM_128_HMAC_SHA1_32.

Jitter Buffer

Jitter Buffer

Min Delay, ms

40

Max Delay, ms

130

Deletion Threshold (DT)

500

Jitter Factor

7

Jitter is a deviation of time periods dedicated to packet delivery. Packet delivery delay and jitter are measured in milliseconds. Jitter value is higher for real time data transfers (e.g. voice or video data).

In RTP, there is a field for precision transmission time tag related to the whole RTP stream. Receiving device uses these time tags to learn when to expect the packet and whether the packet order has been observed. On the basis of this information, the receiving side will learn how to configure its settings in order to evade potential network problems such as delays and jitter. If the expected time for packet delivery from the source to the destination for the whole call period corresponds to the defined value, e.g. 50ms, it is fair to say that there is no jitter in such a network. But packets are delayed in the network frequently, and the delivery time period may fluctuate significantly (in the context of time-critical traffic). If the audio or video recipient application will play packets in the order of their reception time, voice (or video) quality will deteriorate significantly. For example, if the voice data is being transferred, there will be interruptions and interference in the voice.

The device features the following jitter buffer settings:

- *Min Delay, ms* — minimum expected IP package network propagation delay;
- *Max Delay, ms* — maximum expected IP package network propagation delay;
- *Deletion Threshold (DT)* — maximum time for voice package removal from the buffer. The parameter value should be greater or equal to maximum delay;
- *Jitter Factor* — parameter used for jitter buffer size optimization. The recommended value is 0.

Input Gain Control

Input Gain Control

Speakerphone

0 dB

Headset

0 dB

Handset

0 dB

✓ Apply

✕ Cancel

- *Speakerphone* — specifies the value by which a signal from the speakerphone will be amplified (valid values -9, ... 9 dB, at a pitch of 1.5 dB);
- *Headset* — specifies the value by which a signal from the headset will be amplified (valid values -9, ... 9 dB, at a pitch of 1.5 dB);
- *Handset* — specifies the value by which a signal from the handset will be amplified (valid values -9, ... 9 dB, at a pitch of 1.5 dB).



To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button.

Dialplan

The screenshot shows the 'SIP Accounts' configuration interface. At the top, there are tabs for 'Network', 'VoIP', 'System', and 'Monitoring'. Under 'VoIP', there are sub-tabs: 'Network Settings', 'SIP Accounts' (selected), 'Common SIP Settings', 'QoS', 'Phone Book', and 'Call History'. The 'SIP Accounts' section has a dropdown menu for 'Account' currently showing 'Account 1'. Below this are tabs for 'General Settings', 'Codecs', 'Service Settings', 'Additional Parameters', and 'Dialplan' (selected). The 'Dialplan Configuration' text area contains the regular expression 'S4,L8([*#x].)'. At the bottom, there are 'Apply' and 'Cancel' buttons.

To define a dialplan, use regular expressions in the 'Dial plan configuration' field. The structure and format of regular expressions that enable different dialling features are listed below.

Structure of regular expressions:

S xx , L xx (Rule1 | Rule2 | ... | RuleN)

where:

- — arbitrary values of S and L timers;
- **()** — dialplan margins;
- **|** — delimiter for dialplan rules;
- **Rule1, Rule 2, Rule N** — numbers templates which are allowed or forbidden to be called.

Routing rules structure:

Sxx Lxx prefix@optional(parameters)

where:

- — arbitrary value of S and L timer. Timers inside rules could be dropped; in this case, global timer values, defined before the parentheses, will be used.
- **prefix** — prefix part of the rule;
- **@optional** — optional part of the rule (might be skipped);
- **(parameters)** — additional options (might be skipped).

Timers

- *Interdigit Long Timer* (« L » character in a dialplan record) — entry timeout for the next digit, if there are no templates that correspond to the dialled combination.
- *Interdigit Short Timer* (« S » character in a dialplan record) — entry timeout for the next digit, if the dialled combination fully matches at least one template and if there is at least one template that requires an extension dialling for the full match.

The timers values might be assigned either for the whole dialplan or for a certain rule. The timers values specified before round brackets is applied for the whole dialplan.


Example: S4 (8XXX.) or S4, L8 (XXX)

If the value of timers are specified in a rule, they are applied to this rule. The value might be located at any position in a template.

Example: (S4 8XXX. | XXX) or ([1-5] XX S0) — an entry requests instantaneous call transmission when 3-digit number dialing; a number should begin with 1,2, ... ,5.

Prefix part of the rule

Prefix part might consist of the following elements:

Prefix part elements	Description
X or	Any digit from 0 to 9, equivalent to [0-9] range
0 - 9	Digits from 0 to 9
*	Symbol *
#	Symbol # <div> The use of # in a dialplan can cause blocking of dial completion with the help of # key!</div>
[]	<p>Specify a range (using dash), enumeration (without gaps, commas and other symbols between digits) or combination of range and enumeration.</p> <p><u>Example of a range:</u> ([1-5]) — any digit from 1 to 5.</p> <p><u>Example of enumeration:</u> ([1239]) — any digit out of 1, 2, 3 or 9.</p> <p><u>Example of a range and enumeration combination:</u> ([1-39]) — the same as in the previous example but in another form. The entry corresponds to any digit from 1 to 3 and 9.</p>
{a,b}	<p>Specify the number of reiteration of the symbol placed before round brackets, range or *# symbols.</p> <p>The following entries are possible:</p> <ul style="list-style-type: none">• {,max} — equal to {0,max},• {min,} — equal to {min,}. <p>Where:</p> <ul style="list-style-type: none">• min — minimum number of reiteration,• max — maximum. <p><u>Example 1:</u> 6{2,5} — 6 might be dialed from 2 to 5 times. The entry equals to the followings 66 666 6666 66666</p> <p><u>Example 2:</u> 8{2,} — 8 might be dialed 2 and more times. The entry equals to the followings 88 888 8888 88888 888888 ...</p> <p><u>Example 3:</u> 2{,4} — 2 might be dialed up to 4 times. The entry equals to the followings 2 22 222 2222.</p>
.	<p>Special symbol «dot» defines the possibility of reiteration of the previous digit, range or *# symbols for from 0 ad infinitum times. It is equal to {0,} entry.</p> <p><u>Example:</u> 5.* — you may do not use in an entry or use it as many times as needed. It is equal to 5* 5* 5xx* 5xxx* ...</p>
+	<p>Special symbol «plus» — repeat the previous digit, range or *# symbols from 1 ad infinitum times. It is equal to {1,} entry.</p> <p><u>Example:</u> 7+ — is supposed to present in the rule at least 1 time. It is equal to 7 7xx 7xxx 7xxxx ...</p>
<arg1:arg2>	<p>Replace dialed sequence. The dialed sequence (arg1) in SIP request to SIP server is changed to another one (arg2). The modification allows deleting — <:, adding — <:, or replacing — <: of digits and symbols.</p> <p><u>Example 1:</u> (<9:8383>XXXXXXX) — the entry corresponds the following dialed digits 9XXXXXXX, but in the transmitted request to SIP server, 9 digit will be replaced to 8383 sequence.</p> <p><u>Example 2:</u> (<83812:>XXXXXX) — the entry corresponds the following dialed digits 83812XXXXXX, but the sequence 83812 will be omitted and will not be transmitted to a SIP server.</p>
,	<p>Paste tone to dialing. When ringing to intercity numbers (or to city number using an office phone) usually, you may hear a dial tone. The dial tone can be realized by putting comma at the needed position in a sequence.</p> <p><u>Example:</u> (8, 770) — while dialing 8770 sequence you will hear a continuous dial tone (station response) after dialing 8 digit.</p>
!	

Forbid number dialing. If you put '!' symbol at the end of the number template, dialling of numbers corresponding to the template will be blocked.

Example: (8 10X xxxxxxx ! | 8 xxx xxxxxxx) — expression allows long-distance dialling only and denies outgoing international calls.



Attention! Prohibition rules must be written first.

Optional part of rules (could be omitted)

The optional part of a rule might be omitted. This part might consist the following elements:

Optional part of rules element	Description
@host:[port]	Direct address dialing (IP Dialing). «@»placed after the number defines that the dialled call will be sent to the subsequent server address. Also, IP Dialling address format may be used for numbers intended for the call forwarding. If @host:port is not specified, calls are routed via SIP-proxy. <u>Example</u> : (1xxxx@192.168.16.13:5062) — all five-digit dials, beginning with 1, will be routed to 192.168.16.13 IP address to 5062 port.

Additional parameters

Format: (param1: value1, ..., valueN; .. ;paramN: value1, ..., valueN)

- *param* — parameter name; several parameters are semicolon-separated and all parameters are enclosed in parentheses;
- *value* — parameter value; several values of one parameter are comma-separated.

Valid parameters and their values:

Parameter	Description
line	Account. Placing a call via the account, possible values 0 and 1. The value 0 corresponds to the first account, the value 1 corresponds to the second account. <u>Example</u> : 12x(line:1) — call to 3-digit numbers beginning with 12 will be performed via the second account.

Examples

Example 1: (8 xxx xxxxxxx) — 11-digit number beginning with 8.

Example 2: (8 xxx xxxxxxx | <:8495> xxxxxxx) — 11-digit number beginning with 8; if 7-digit number is dialled, add 8495 to the number being sent.

Example 3: (0[123] | 8 [2-9]xx [2-9]xxxxxx) — dialling of emergency call numbers and unusual sets of long-distance numbers.

Example 4: (S0 <:82125551234>) — quickly dial the specified number, similar to 'Hotline' mode.

Example 5: (S5 <:1000> | xxxx) — this dialplan allows you to dial any number that contains digits, and if there was no entry in 5 seconds, dial number '1000' (for example, it belongs to a secretary).

Example 6: (8, 10x.|1xx@10.110.60.51:5060) — this dialplan allows you to dial any number beginning with 810 and containing at least one digit after '810' (after entering '8', 'station reply' tone will be generated) as well as 3-digit numbers beginning with 1. Subscriber calls with 3-digit numbers beginning with 1 will be sent to IP address 10.110.60.51 and port 5060.

Example 7: (S3 *xx#|#xx#|#xx#|*xx*x+#+) — management and usage of VAS.



To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button

«Common SIP settings» submenu

- *STUN Server Address* — STUN server IP address or domain name; you may specify an alternative server port after the colon (default value is 3478);
- *STUN Request Sending Interval, s* — time period that defines transmission of a request to STUN server. The less the polling period, the faster the response to the public address changes;
- *Tones Specification* — selecting country to determine tone specification used.



To apply new configuration and save settings into non-volatile memory of the device, click '*Apply*' button. To discard changes, click '*Cancel*' button.

«QoS» submenu

In the «QoS» submenu you may configure Quality of Service functions.

DSCP Configuration for SIP:

- *Account 1* — DSCP field value of IP packet header for signalling SIP traffic of the first line;
- *Account 2* — DSCP field value of IP packet header for signalling SIP traffic of the second line.

DSCP Configuration for RTP:

- *Account 1* — DSCP field value of IP packet header for voice traffic of the first line;
- *Account 2* — DSCP field value of IP packet header for voice traffic of the first line.



To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button.

«Phone Book» submenu

Local phonebook management

The screenshot shows the 'Phone Book' configuration page. At the top, there are tabs for 'Network', 'VoIP', 'System', and 'Monitoring'. Below these are sub-tabs for 'Network Settings', 'SIP Accounts', 'Common SIP Settings', 'QoS', 'Phone Book', and 'Call History'. The 'Phone Book' sub-tab is active. Under the 'Phone Book' sub-tab, there are two main sections: 'Local' and 'LDAP'. The 'Local' section is currently selected. It contains three main areas: 'Download Phone Book From Device', 'Upload Phone Book To Device', and 'Clear Phone Book File'. The 'Download' section has a 'File Format' dropdown with 'csv' and 'xml' (selected) and a 'Download' button. The 'Upload' section has a 'Phone Book File' input field with a 'Выберите файл' button and 'Файл не выбран' text, a 'File Format' dropdown with 'csv' and 'xml' (selected), an 'Add Mode' checkbox, and an 'Upload' button. The 'Clear' section has a 'Clear' button.

Download Phone Book From Device

Use the section to download a phonebook stored on the device.

- *File Format* — select a format of the file you want to download. The following formats are available:
 - *csv* — text file format where all the contacts are written in the table. The values in the table are separated by the selected separator;
 - *xml* — an eXtensible Markup Language.
- *Separator* — the symbol for separating data in the table in csv format;
- *Add Header* — when the option is selected, downloaded csv file will have a header — the first line;



If 'Add Header' box is not checked, contacts from the loaded file will replace the existing one.

Upload Phone Book To Device

This section is used to configure parameters of restoring a phonebook from the backup copy.

- *File Format* — select a format of the file you want to upload. The following formats are available:
 - *csv* — text file format where all the contacts are written in the table. The values in the table are separated by the selected separator;
 - *xml* — an eXtensible Markup Language.
- *Exist Header* — the option is available only when csv format is selected. When checked, it means that the uploaded file has a header — the first line — while import the first line will be ignored;
- *Add Mode* — when checked, the contacts from the uploaded file will be added to existing ones. **If the box is unchecked, all the contacts from uploaded file will replace the existing ones.**

LDAP. Remote Phonebook management

In the 'Phone book' submenu, you may set up the connection to LDAP server and search parameters.

The screenshot shows the 'Phone Book' configuration interface. The 'VoIP' tab is selected, and within it, the 'Phone Book' sub-tab is active. The 'LDAP' sub-tab is chosen for configuration. Key settings include enabling LDAP, selecting LDAPS for TLS mode, and setting the LDAP server address and port (636). There are also fields for base, login, password, and protocol version. Search filters for names and numbers are provided, along with a 'Max Hits' limit. The 'Lookup For Incoming Call' option is also checked.

- **Enable LDAP**— when selected, the phone book is accessible via display menu;
- **TLS mode**— TLS usage mode. The following modes are available:
 - **Off**— do not use TLS;
 - **StartTLS**— after establishing an unencrypted LDAP connection, the client issues a STARTTLS command to upgrade the connection to an encrypted. After that, the communication between both endpoints is encrypted;
 - **LDAPS**— TLS is used since the start of the LDAP connection.
- **Check Certificate**— server certificate check mode;
- **Interface**— selecting the network interface used to send requests to the LDAP server;
- **LDAP Server Address**— domain name or IP address of LDAP server;
- **LDAP Server Port**— port of LDAP server transport protocol;
- **Base**— indicates the location of base directory, that contains the phone book, and from which the search begins, in the LDAP directory;
- **Login**— username that will be used when authorizing on LDAP server;
- **Password**— password that will be used when authorizing on LDAP server;
- **Protocol Version**— LDAP protocol version of formed requests;
- **Max Hits**— the parameter indicating the maximum amount of search results that will be returned by LDAP server;



Too big 'Hit limit' value reduces the LDAP search rate, that is why the parameter is to be configured according to the available bandwidth.

- **Name Attributes**— the parameter that indicates the name attribute of each record returned by the LDAP server;
- **Number Attributes**— the parameter that indicates the number attribute of each record returned by the LDAP server;
- **Display Name Attributes**— the parameter that indicates the display name attribute of each record returned by the LDAP server;
- **Name Filter**— the filter used to lookup for the names. The "*" character in the filter indicates any character. The "%" character in the filter indicates the input string used as the filter condition prefix;
- **Number Filter**— the filter used to lookup for the number. The "*" character in the filter indicates any character. The "%" character in the filter indicates the input string used as the filter condition prefix;

- *Lookup For Incoming Call*— lookup for a name using a number during incoming calls.



To apply a new configuration and store settings into the non-volatile memory, click '*Apply*' button. To discard changes, click '*Cancel*' button.

Remote phonebook management

Network
VoIP
User Interface
System
Monitoring

Network Settings
SIP Accounts
Common SIP Settings
QoS
Phone Book
Call History

Local
LDAP
Remote

Enable Remote PhoneBook ☒

PhoneBook URL

(http: / ftp: / https://download.server.loc/phonebook.file)

User Name

Password

Provisioning Mode
Periodically ▼

PhoneBook Update Interval, s

- *Enable Remote PhoneBook*— when checked, remote phonebook is loaded automatically;
- *PhoneBook URL* —a full path to the remote phonebook — is set in URL format (the following protocols are available to be used for phonebook loading through: TFTP, FTP, HTTP and HTTPS);
- *User Name* —a name which is used for authentication on FTP/HTTP/HTTPS server for phonebook loading;
- *Password* — a password which is used for authentication on FTP/HTTP/HTTPS server for phonebook loading;
- *Provisioning Mode* —select a mode for phonebook loading: periodically or scheduled;
- *PhoneBook Update Interval, s* —time interval between phonebook updates. If the parameter is set to 0, the phonebook is updated once — right after device loading;
- *Days Of PhoneBook Update* —weekdays when the phonebook will be automatically updated;
- *Time Of PhoneBook Update* —time in 24-hours format, when the phonebook will be automatically updated.



To apply a new configuration and store settings into the non-volatile memory, click '*Apply*' button. To discard changes, click '*Cancel*' button.

«Call history» submenu

In the «Call History» submenu you may configure call history logging.

Network

VoIP

System

Monitoring

Network Settings

SIP Accounts

Common SIP Settings

QoS

Phone Book

Call History

Call History

Call History Size

0

Download Call History File

Download

Clear Call History

Clear

View "Call History"

Apply

Cancel

- *Call History Size* — maximum number of log records, may take values from 0 to 10,000 strings. Enter '0' value to disable call history logging. When the defined log limit is reached, each consequent record will delete the oldest record in the beginning of the log;
- *Download Call History File* — to save 'voip_history' file on a local PC, click 'Download' button;
- *Clear Call History* — to clear call history, click 'Clear' button.

To view the call history, follow the «View «Call History» link. For parameter monitoring description, see section [View call history](#) .

✔ To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button.

«User interface» menu

«Buttons» submenu

Network
VolP
User Interface
System
Monitoring

Buttons
Ringtones

Key Customization

F1	Screen	Label	Call History
F2	Switchline	Label	
F3	Screen	Label	Local Contacts
F4	Screen	Label	Menu
F5	No Action Selector		
F6	No Action Selector		
F7	No Action Selector		
F8	Line	Label	Account 1
F9	Line	Label	Account 2
F10	No Action Selector		
OK	No Action Selector		
▲	No Action Selector		
▼	No Action Selector		
◀	No Action Selector		
▶	No Action Selector		
✕	No Action Selector		

Apply
Cancel

You may choose actions for each button to be performed on pressing. The settings are presented as a table with the folloing columns:

- Buttons;
- Action — select action to be performed on the button pressing. The followings are available:
 - No action selected — pressing on this button will not be processed;
 - Screen — open a screen selected in the additional parameters;
 - Call — call the number selected in the additional parameters;
 - Switchline — change the account by default;
 - BLF — only for buttons with LED indicator. LED indicates line status of the subscriber selected in the additional settings. Pressing the button in stand-by mode initiates a call. In conversation mode, pressing the button redirects the call to the selected subscriber.
- Label — button's label, which is displayed on the screen next to the button;
- Additional settings — select additional parameters for the button (options depend on the action selected).

! To BLF function activation, you should specify subscribtion server in SIP account settings.

! The «Buttons» tab is available only for VP-15 and VP-15P.

✓ To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button.

«Ringtones» submenu

In «Ringtones» submenu, you may upload audio files and set them as ring-tone. You may assign different ring-tones for different accounts.

Network VoIP **User Interface** System Monitoring

Buttons **Ringtones**

Ringtone Settings

Upload Ringtone File No file chosen

Using 0% of available space for ringtones (0 KiB of 384 KiB)

Ringtones

Ringtone Name	Account 1	Account 2	Size	Actions
default_ringtone.wav	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	20.0 K (20 513 B)	<input type="button" value="Play"/>

This tab consists of 3 parts:

- a block for audio file uploading;
- drive free space indicator and total drive memory size for audio files storing;
- list of uploaded audio files.

✔ Before being upload to the storage, audio files are compressed. The indicator shows the size of compressed files.

The list of uploaded audio files is shown in a table with the following columns:

- *Ringtone Name* — name of the audio file;
- *Account 1* — assignment of the ringtone to the Account 1;
- *Account 2* — assignment of the ringtone to the Account 2;
- *Size* — the size of the file before being compressing;
- *Actions* — a button to play/pause audio file on the device.

✔ Check and uncheck audio files in the list to select the necessary files and click «Remove» button below the table to delete them from the storage.

⚠ An audio file should satisfy the following requirements to be played correctly:

- Sampling frequency — 8000 Hz;
- Number of channels — 1 (Mono);
- Code size — 8 bit;
- Codec — a-law.

The example of preparing an audio file is presented in the application [Preparing an audio file to be uploaded as a ringtone](#).

«Notificatoins» submenu

In the 'Notifications' submenu you can manage the notifications that are displayed on the device screen.

Network **VoIP** **User Interface** **System** **Monitoring**

Buttons Ringtones **Notifications**

Notifications Settings

Notify of Missed Calls ☒

Notify of Forwarded Calls ☒

Notify of Unread Messages ☒

Notify of Unheard Voice Messages ☒

- *Notify of Missed Calls*— when checked, the display shows notifications of missed calls;
- *Notify of Forwarded Calls*— when checked, the display shows notifications of forwarded calls;
- *Notify of Unread Messages*— when checked, the display shows notifications of unread text messages;
- *Notify of Unheard Voice Messages*— when checked, the display shows notifications of unheard voice messages.

«Volume» submenu

In the 'Volume' submenu you can configure the volume in various device operation modes.

Network **VoIP** **User Interface** **System** **Monitoring**

Buttons Ringtones Notifications **Volume**

Volume Settings

Speakerphone 9

Ring Volume 9

Headset 9

Handset 9

- *Speakerphone*— speakerphone volume;
- *Ring volume*— ring volume;
- *Headset*— headset volume;
- *Handset*— handset volume.

«System» menu

In the 'System' menu you may configure settings for system, time and access to the device via various protocols, change the device password and update the device firmware.

«Time» submenu

In the 'Time Settings' submenu you may configure time synchronization protocol (NTP).

The screenshot shows the 'Time Settings' configuration page. At the top, there are tabs for 'Network', 'VoIP', 'System' (which is active), and 'Monitoring'. Below these, there are sub-tabs: 'Time' (active), 'Access', 'Log', 'Passwords', 'Configuration Management', 'Firmware Upgrade', 'Reboot', 'Autoprovisioning', 'Management Interface', and 'Certificates'. Under the 'Time' sub-tab, there is an 'Advanced' link. The main content area is titled 'Time Settings' and contains the following fields: 'Time Zone' (a dropdown menu set to 'Moscow'), 'Daylight Saving Time Enable' (an unchecked checkbox), 'Enable NTP' (a checked checkbox), 'NTP Server' (a dropdown menu set to 'pool.ntp.org'), and 'NTP Interface' (a dropdown menu set to 'Internet'). At the bottom of the form are two buttons: 'Apply' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

- *Time Zone* — allows you to set a timezone from the list according to the nearest city in your region;
- *Daylight Saving Time Enable* — when selected, automatic daylight saving change will be performed automatically within the defined time period:
 - *DST Start* — daylight saving change starting day;
 - *DST End* — daylight saving change ending day.
- *DST Offset (minutes)* — time shift in minutes;
- *Enable NTP* — select this checkbox to enable device system time synchronization with the particular NTP server;
- *NTP Server* — time synchronization server IP address/domain name;
- *NTP Interface* — select network interface used for sending requests of NTP synchronization.



To apply a new configuration and store settings into the non-volatile memory, click '*Apply*' button. To discard changes, click '*Cancel*' button.

«Access» submenu

In the 'Access' submenu you may configure the device access via WEB interface, Telnet and SSH protocols.

Network
VoIP
System
Monitoring

Time
Access
Log
Passwords
Configuration Management
Firmware Upgrade
Reboot
Autoprovisioning
Management Interface
Certificates
Advanced

Access Ports

HTTP Port

80

HTTPS Port

443

Telnet Port

23

SSH Port

22

Access to "Internet" Service

Web

☒ HTTP
☒ HTTPS

Telnet

☒

SSH

☒

Access to "VoIP" Service

Web

☐ HTTP
☐ HTTPS

Telnet

☐

SSH

☐

Access to "Management Interface" Service

Web

☐ HTTP
☐ HTTPS

Telnet

☐

SSH

☐

Access to Menu Items

Manage Supplementary Services

do not disturb
call waiting
hot line
anonymous calls
stop dial at #
call forward on busy
call forward unconditional
call forward on no answer

Device Settings

autoprovision
network
language
display
accounts
sound
date/time

Device Management

clearing history
reset settings
adding contacts
deleting contacts
reboot
edit contacts

✓ Apply

✕ Cancel

Access ports

In this section you may configure TCP ports for the device access via HTTP, HTTPS, Telnet , and SSH.

- *HTTP port*— number of the port that allows for the device web interface access via HTTP, default value is 80;
- *HTTPS ports*— number of the port that allows for the device WEB interface access via HTTPS (HTTP secure connection), default value is 443;
- *Telnet port*— number of the port that allows for the device access via Telnet, default value is 23;
- *SSH port*— number of the port that allows for the device access via SSH, default value is 22.

You may use Telnet and SSH protocols in order to access the command line (Linux console). Username/password for console connection: **admin** /**password**.

Access to the Internet service

To get device access from the Internet service interfaces, set the following permissions :

Web

- *HTTP*— when selected, connection to the device web configurator is enabled via HTTP (insecure connection);
- *HTTPS* —when selected, connection to the device web configurator is enabled via HTTPS (secure connection).

T elnet — a protocol that allows you to establish mechanisms of control over the network. Allows you to remotely connect to the gateway from a computer for configuration and management purposes. To enable the device access via Telmet protocol , select the appropriate checkboxes.

SSH — is a secure device remote control protocol. However, as opposed to Telnet, SSH encrypts all traffic, including passwords being transferred. To enable the device access via SSH protocol , select the appropriate checkboxes.

Access to VoIP Service

In this section you may configure access to VoIP service interface (to configure VoIP service interface, use VoIP—Network configuration) through the web (HTTP or HTTPS), and also via Telnet and SSH protocols. To enable access to any protocols listed above, select the appropriate checkboxes

Access to Management Interface Service

Use this section to configure access for the device management via HTTP, HTTPS, Telnet and SSH. To configure the interface, use **System—Management VLAN** page. To enable access to any protocols listed above, select the appropriate checkboxes.

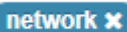


For Telnet and SSH protocol authorization, you may use default username *admin* and password *password*. After authorization, Linux console will become available that supports basic commands of the 'shell' command interpreter.

Access to the menu elements

This block includes 3 groups of items, access to which can be denied for a user. If one or another item is specified in the list, then access to it is allowed.

You can deny access by clicking



to the right of menu item name. To allow access to a previously denied menu item, you should click on



the button and select the required item from the drop-down list.

To provide the administrator with access to all menu items, including hidden from the user, you should switch to the admin mode.



For access to hidden menu items the same password is used as for the access to web interface.



To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

«Log» submenu

In the «Log» submenu you may configure output for various debug messages intended for device troubleshooting. Debug information is provided by the following device firmware modules:

- VoIP Log — deals with VoIP functions operations;
- Networkd Log — deals with the device configuration according to the configuration file;
- Configd Log — deals with the configuration file operations (config file reads and writes from various sources) and the device monitoring data collection;
- Interface Manager Log — deals with the device's user interface operation (such as keyboard, display, speaker phone, handset and etc.).

Network

VoIP

System

Monitoring

Time

Access

Log

Passwords

Configuration Management

Firmware Upgrade

Reboot

Autoprovisioning

Management Interface

Certificates

Advanced

VoIP Log

Log Output

Disabled

Error☐

Warning☐

Debug☐

Info☐

SIP Trace Level

0

Networkd Log

Log Output

Disabled

Error☐

Warning☐

Debug☐

Info☐

Configd Log

Log Output

Disabled

Error☐

Warning☐

Debug☐

Info☐

Interface Manager Log

Log Output

Disabled

Error☐

Warning☐

Debug☐

Info☐

Syslog Settings

Enable☐

Mode

Server

Syslog Server Address

syslog.server

Syslog Server Port

514

✔ Apply

✕ Cancel

VoIP log

- *Log output* — log message output direction:
 - *Disabled* — log is disabled;
 - *Syslog* — messages are output to remote server or local file via syslog protocol (for protocol configuration, see below);
 - *Console* — messages are output to the device console (requires connection via COM port adapter);
 - *Telnet* — messages are output to the telnet session; create telnet protocol connection first.
- *Error* — select this checkbox, if you want to collect «Error» type messages;
- *Warnings* — select this checkbox, if you want to collect «Warning» type;
- *Debug* — select this checkbox, if you want to collect debug messages;
- *Info* — select this checkbox, if you want to collect information messages;
- *SIP trace level* — defines output level of VoIP SIP manager stack messages.

Network log, configure log, interface manager log

- *Log output* — log message output direction:
 - *Disabled* — log is disabled;
 - *Syslog* — messages are output to remote server or local file via syslog protocol (for protocol configuration, see below);
 - *Console* — messages are output to the device console (requires connection via COM port adapter);
 - *Telnet* — messages are output to the telnet session; create telnet protocol connection first.
- *Error* — select this checkbox, if you want to collect «Error» type messages;
- *Warning* — select this checkbox, if you want to collect «Warning» type messages;
- *Debug* — select this checkbox, if you want to collect debug messages;
- *Info* — select this checkbox, if you want to collect information messages.

Syslog Settings

If there is at least a single log (VoIP manager, system manager or configuration manager) is configured for Syslog output, you should enable Syslog agent that will intercept debug messages from the respective manager and send them to remote server or save them to a local file in Syslog format.

- *Enable* — when selected, user Syslog agent is launched;
- *Mode* — Syslog agent operation mode:
 - *Server* — log information will be sent to the remote Syslog server (this is the 'remote log' mode);
 - *Local file* — log information will be saved to the local file;
 - *Server and file* — log information will be sent to the remote Syslog server and saved to the local file.
- *Syslog server address* — Syslog server IP address or domain name (required for 'Server' mode);
- *Syslog server port* — port for Syslog server incoming messages (default value is 514; required for 'Server' mode);
- *File name* — name of the file to store log in Syslog format (required for 'File' mode);
- *File size, KB* — maximum log file size (required for 'File' mode).



To apply a new configuration and store settings into the non-volatile memory, click '*Apply*' button. To discard changes, click '*Cancel*' button.

«Password» submenu

In the 'Passwords' submenu you may define passwords for administrator, non-privileged user, and viewer access.

Defined passwords allow for the device access via WEB interface and also via Telnet protocol.

When signing into WEB interface, administrator (default password: **password**) has the full access to the device: read/write any settings, full device status monitoring.



Administrator login — admin

Network
VoIP
System
Monitoring

Time
Access
Log
Passwords
Configuration Management
Firmware Upgrade
Reboot
Autoprovisioning
Management Interface
Certificates
Advanced

Administrator Password

Password

Confirm

- *Administrator password* — enter administrator password in the respective fields and confirm it.





To apply a new configuration and store settings into the non-volatile memory, click '*Apply*' button. To discard changes, click '*Cancel*' button.

«Configuration Management» submenu

In the «Configuration management» submenu you may save and update the current configuration.

The screenshot shows the 'Configuration Management' submenu within the 'System' tab. The top navigation bar includes 'Network', 'VoIP', 'System' (selected), and 'Monitoring'. Below this, a secondary bar contains 'Time', 'Access', 'Log', 'Passwords', 'Configuration Management' (selected), 'Firmware Upgrade', 'Reboot', 'Autoprovisioning', 'Management Interface', 'Certificates', and 'Advanced'. The main content area is titled 'Configuration Files' and contains three sections: 'Backup Configuration' with a 'Download' button; 'Restore Configuration' with a file selection button labeled 'Выберите файл' (Select file) and 'Файл не выбран' (File not selected), followed by an 'Upload' button; and 'Reset to Default Configuration' with a 'Reset' button.

Backup Configuration

To save the current device configuration to a local PC, click «Download» button..

Restore Configuration

Select configuration file stored on a local PC. To update the device configuration, click «*Select file*» button, specify a file (in .tar.gz format) and click «*Upload*» button. Uploaded configuration will be applied automatically and does not require device reboot.

Reset to Default Configuration

To reset the device to default settings, click «*Reset*» button.



When you reset the device configuration, the followings will be also reset:

- contacts
- call history
- text messages


«Firmware upgrade» submenu

In «Firmware upgrade» submenu you may update the firmware of the device.

The screenshot shows the 'Firmware Upgrade' submenu within the 'System' tab. The top navigation bar is the same as the previous screenshot. The secondary bar includes 'Time', 'Access', 'Log', 'Passwords', 'Configuration Management', 'Firmware Upgrade' (selected), 'Reboot', 'Autoprovisioning', 'Management Interface', 'Certificates', and 'Advanced'. The main content area is titled 'Firmware Upgrade' and contains: 'Active Version of Firmware' (1.5.0.134) with a 'Check for Upgrade' button; 'Firmware Backup Version' (1.5.0.127) with a 'Set Active' button; a note that 'Firmware upgrade is also available at: <http://elitex-co.ru/support/downloads/>'; and 'Firmware Image' with a file selection button labeled 'Выберите файл' (Select file) and 'Файл не выбран' (File not selected), followed by an 'Upload File' button.


- *Active Version of Firmware* — installed firmware version;
- *Check for upgrade* — click this button to check the availability of the latest firmware version. With this function, you may quickly check the latest firmware version and update the firmware, if necessary;
- *Firmware backup version* — installed firmware version which can be used in case of problems with the current active firmware version;

- *Activate* — button allowing you to make a backup of the active firmware version. In order to get that done reboot the device.

 Firmware update check function requires Internet access.

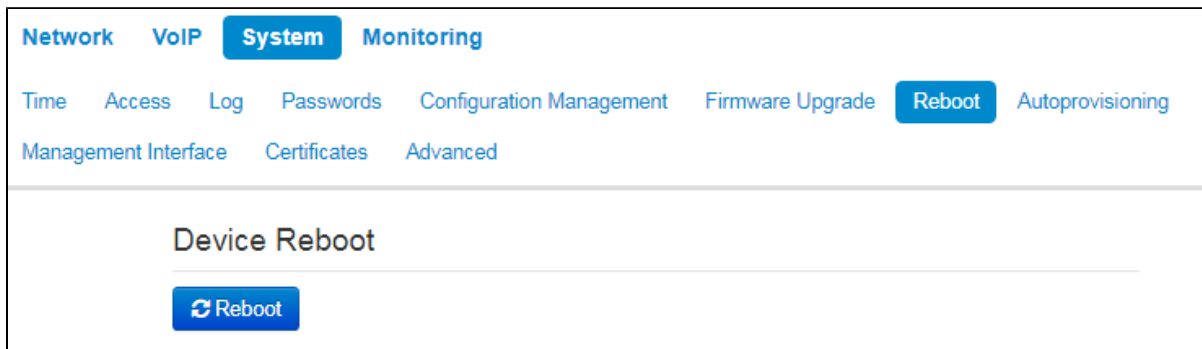
You may update the device firmware manually by downloading the firmware file from the web site <http://eltex-co.ru/support/downloads/> and saving it on the computer. To do this, click the 'Select file' button in the '*Firmware update file*' field, and specify path to firmware .tar.gz format file.

To launch the update process, click '*Upload file*' button. The process may take several minutes (its current status will be shown on the page). The device will be automatically rebooted when the update is completed

 Do not switch off or reboot the device during the software update.

«Reboot» submenu

In the «Reboot» submenu you may reboot the device.

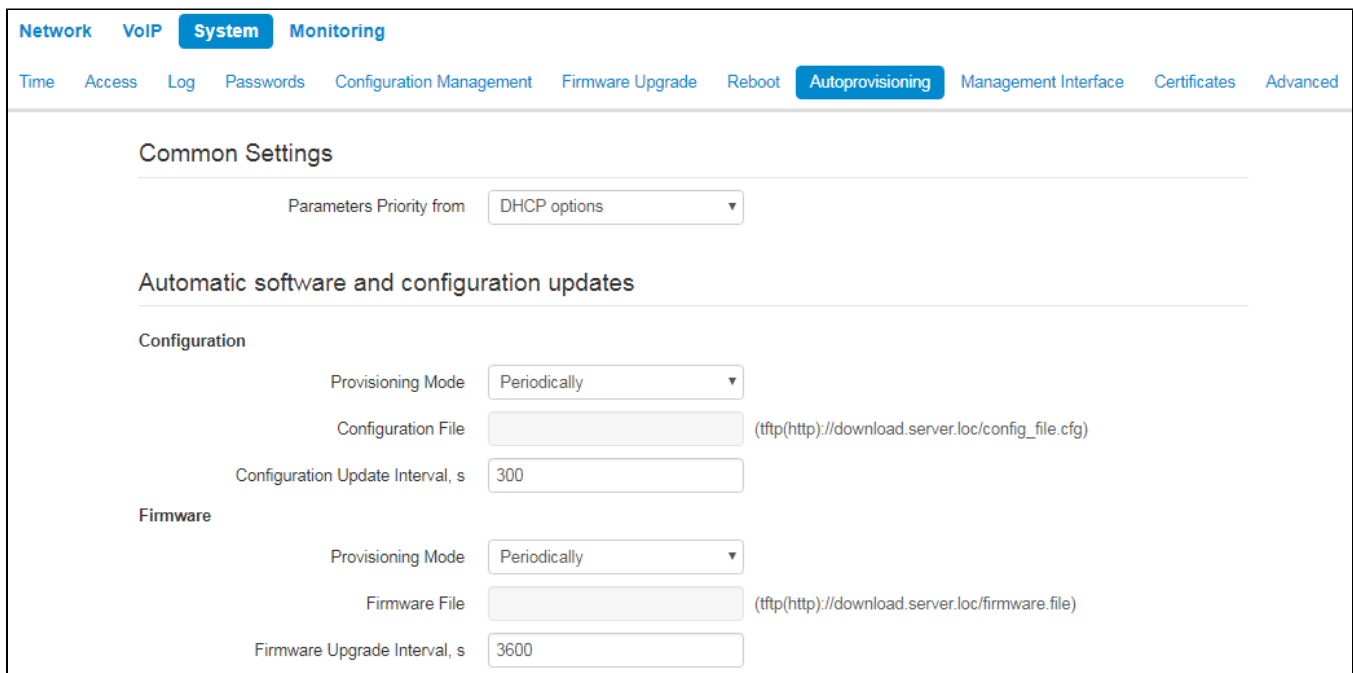


The screenshot shows the «Reboot» submenu. At the top, there are tabs for Network, VoIP, System (selected), and Monitoring. Below these are sub-tabs: Time, Access, Log, Passwords, Configuration Management, Firmware Upgrade, Reboot (selected), and Autoprovisioning. The main content area is titled «Device Reboot» and contains a single blue button with a circular arrow icon and the text «Reboot».

Click the «Reboot» button to reboot the device. Device reboot process takes approximately 1 minute to complete.

«Autoprovisioning» submenu

In the «Autoprovisioning» submenu you may configure DHCP-based autoprovisioning algorithm and TR-069 subscriber device automatic configuration protocol.



The screenshot shows the «Autoprovisioning» submenu. At the top, there are tabs for Network, VoIP, System (selected), and Monitoring. Below these are sub-tabs: Time, Access, Log, Passwords, Configuration Management, Firmware Upgrade, Reboot, Autoprovisioning (selected), Management Interface, Certificates, and Advanced. The main content area is titled «Common Settings» and contains a dropdown menu for «Parameters Priority from» set to «DHCP options». Below this is a section titled «Automatic software and configuration updates». Under «Configuration», there is a «Provisioning Mode» dropdown set to «Periodically», a «Configuration File» text field with a placeholder path (tftp(http://download.server.loc/config_file.cfg)), and a «Configuration Update Interval, s» text field set to 300. Under «Firmware», there is a «Provisioning Mode» dropdown set to «Periodically», a «Firmware File» text field with a placeholder path (tftp(http://download.server.loc/firmware.file)), and a «Firmware Upgrade Interval, s» text field set to 3600.

- *Parameter priority from* — this parameter manages names and locations of configuration and firmware files:
 - *Static settings* — paths to configuration and firmware files are defined by the '*Configuration file*' and '*Firmware file*' settings correspondingly;

- DHCP options — paths to configuration and firmware files are defined by the DHCP Option 43, 66, and 67 (to do this, you should select DHCP for the Internet service).

For detailed algorithm operation, see section [«Internet» submenu](#).

DHCP-based autoprovisioning

- *FTP User Name* — a user name used for authorization on FTP server when loading configuration or firmware;
- *FTP Password* — a password used for authorization on FTP server when loading configuration or firmware.

Configuration

- *Provisioning Mode* — to update configuration, you may separately specify one of the several update modes:
 - *Disabled* — autoupdate of the device configuration is disabled;
 - *Periodically* — the device configuration will be automatically updated after defined period of time;
 - *Scheduled* — the device configuration will be automatically updated at specific times and on specific days.
- *Configuration File* — full path to configuration file—defined in URL format (at this time you may upload configuration files via TFTP and HTTP)

```
tftp://<server address>/<full path to cfg file>
http://<server address>/<full path to cfg file>
ftp://<server address>/<full path to cfg file>
```

where <server address> — HTTP, TFTP or FTP server address (domain name or IPv4), < full path to cfg file > — full path to configuration file on server;

- *Configuration Update Interval, s* — time period in seconds that will be used for periodic device configuration update; if 0 is selected, device will be updated only once — immediately after startup;
- *Time of Configuration Update* — time on 24-hour format that will be used for configuration autoupdate;
- *Days of Configuration Update* — week days with defined time that will be used for configuration autoupdate.

Firmware

- *Provisioning Mode* — to update firmware, you may separately specify one of the several update modes:
 - *Disabled* — autoupdate of the device configuration or firmware is disabled;
 - *Periodically* — the device configuration or firmware will be automatically updated after defined period of time;
 - *Scheduled* — the device configuration or firmware will be automatically updated at specific times and on specific days.
- *Firmware File* — full path to firmware file — defined in URL format (at this time you may upload firmware files via TFTP and HTTP):

```
tftp://<server address>/<full path to firmware file>
http://<server address>/<full path to firmware file>
ftp://<server address>/<full path to firmware file>
```

where <server address> — HTTP, TFTP or FTP server address (domain name or IPv4), < full path to firmware file > — full path to firmware file on server;

- *Firmware Upgrade Interval, s* — time period in seconds that will be used for periodic device firmware update; if 0 is selected, device will be updated only once — immediately after startup;
- *Time of Firmware Upgrade* — time on 24-hour format that will be used for firmware autoupdate;
- *Days of Firmware Upgrade* — week days with defined time that will be used for firmware autoupdate.

For detailed DHCP-based automatic update algorithm, see Appendix [Device automatic update algorithm based on DHCP](#).

TR-069 protocol autoconfiguration

Via TR-069, you may perform full device configuration, firmware update, view device information (firmware version, model, serial number, etc.), upload and download the configuration file and reboot the device remotely.

TR-069 Autoconfiguration

Common

Enable TR-069 Client

☒

Interface

Internet

ACS Server Address

http://update.local:9595/

Enable Periodic Inform

☒

Periodic Inform Interval, s

60

ACS Connection Request

User Name

acs

Password

.....

Client Connection Request

User Name

admin

Password

.....

NAT Settings

NAT Mode

STUN

STUN Server Address

stun.local

STUN Server Port

3478

Minimum Keep Alive Period, s

30

Maximum Keep Alive Period, s

60

✓ Apply

✕ Cancel

Common

- *Enable TR-069 Client* — when selected, integrated TR-069 protocol client will be enabled;
- *Interface* — select the interface for TR-069 protocol operation. If *'Management VLAN'* interface is enabled on the gateway, this VLAN will be used for TR-069 protocol operation automatically. Interface selection setting will be disabled;
- *ACS Server Address* — autoconfiguration server address. Enter address in the following format: http://<address>:<port> or https://<address>:<port> (<address> — ACS server IP address or domain name, <port> — ACS server port, default value is 80). Alternatively, the client will exchange the data with ACS server via the secure protocol—HTTPS. By default, ACS server produced by Eltex utilizes port 9595 for communication;
- *Enable Periodic Inform* — when selected, integrated TR-069 client performs periodic ACS server polling at intervals equal to *«Periodic Inform Interval»* value, in seconds. Goal of the polling is to identify possible changes in the device configuration.

ACS connection request

- *User Name, Password* — username and password used by client to ACS.

Client Connection Request

- *User Name, Password* — username and password used by TR-069 client to access ACS.

NAT Settings

If there is a NAT (network address translation) between the client and ACS, ACS may not be able to establish the connection to client without specific technologies intended to prevent such situations. These technologies allow the client to identify its so called public address (NAT address or in other words external address of a gateway that covers the client). When public address is identified, the client reports it to the server that uses this public address for establishing connection to the client in the future..

- **NAT Mode** — identifies the method, that will be used by a client for obtaining its public address information. The following modes are possible:
 - *STUN*— use STUN protocol for public NAT address discovery;
 - *Manual*— manual mode, when public address is explicit in configuration; in this mode, you should add a forwarding rule on a device that acts as a NAT for TCP port used by TR-069 client;
 - *Off*— NAT is not used —this mode is recommended only when the device is directly connected to ACS without network address translation. In this case public address will match local client address.

When choosing STUN mode, you should define the following settings:

- *STUN Server Address* — IP address or domain name of STUN server;
- *STUN Server Port* — UDP port of STUN server (3478, by default);
- *Minimum Keep Alive Period and Maximum Keep Alive Period* — define the time interval in seconds for periodic transmission of messages to STUN server in order to identify public address modification.



For correct ACS operation behind NAT, STUN server minimum polling period should be less than maximum session time provided by NAT device.



To apply a new configuration and store settings into the flash memory, click '*Apply*' button. To discard changes, click '*Cancel*' button.

«Management interface» submenu

Use this menu to configure the network interface and establish the device network management via HTTP, HTTPS, and Telnet.

- *Enable Management Interface* — when checked, device management will be performed via this interface:
 - *Access Type* — defines interface operation mode:
 - *Tagged* — data is transferred by the interface with the defined VLAN ID;
 - *Untagged* — data is transferred by the interface without VLAN.
 - *VLAN ID* — identifier for interface extract into virtual local area network;
 - *802.1 P* — 802.1P attribute (another name: CoS — Class of Service), assigned to the outgoing Ethernet frames from this interface. It may take values from 0 (the lowest priority) to 7 (the highest priority);
 - *Protocol* — select address assigning protocol for the interface:
 - *Static*— operation mode where IP address and all the necessary settings for LAN interface are assigned manually;
 - *DHCP*— operation mode where IP address, subnet mask, DNS address and other necessary settings for the interface operation (e.g. static routes) are automatically obtained from DHCP server.

Static

When «Static» type is selected, the following parameters will be available for editing:

- *IP address* — specify the IP address for the management interface;
- *Netmask* — subnet mask for the management interface;
- *Default Gateway* — default gateway IP address for the management interface;
- *1st DNS Server, 2nd DNS Server* — DNS IP addresses required for the gateway autoconfiguration protocols' operation; to configure protocols, use **System — Autoprovisioning** page.

DHCP

When «DHCP» type is selected, the following parameters will be available for editing:

- *Alternative Vendor ID (option 60)* — when selected, the device transmits Vendor ID (Option 60) field value in Option 60 DHCP messages (Vendor class ID). If the *Alternative Vendor ID (Option 60)* checkbox is not selected, the default value will be transmitted in Option 60 in the following format:
[**VENDOR** :vendor][**DEVICE** :device type][**HW** :hardware version] [**SN** :serial number][**WAN** :WAN interface MAC address][**LAN** :LAN interface MAC address][**VERSION** :firmware version]
Example: [VENDOR:Eltex][DEVICE:VP-12P][HW:1.0][SN:VI23000118] [WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.1.0]
- *Vendor ID (option 60)* — Option 60 value (Vendor class ID) transmitted in DHCP messages. If the field is empty, Option 60 will not be transmitted in DHCP messages;
- *1st DNS Server, 2nd DNS Server* — addresses of domain names servers (it is used for IP address defining with the help if domain name). Manually defined addresses will have a priority over DNS addresses obtained via DHCP.

The list of DHCP options used on each network interface (Internet, VoIP and Management) can be assigned manually. For detailed setting information, see section [DHCP client configuration in multiservice mode](#).



To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button

«Certificates» submenu

Network	VoIP	System	Monitoring
Time	Access	Log	Passwords
Configuration Management	Firmware Upgrade	Reboot	Autoprovisioning
Management Interface	Certificates	Advanced	

Certificates		
Type	Common name	Organization
<input checked="" type="checkbox"/> Root certificate	192.168.1.1	Eltex
<input type="checkbox"/> Client certificate	<no certificate>	
<input type="checkbox"/> Web certificate	192.168.1.1	Eltex Ent

Remove

'Certificates' submenu allows to view, download and upload certificates for using in protected TLS connections.

Root certificate

A root certificate is used to authenticate certificates with incoming connections. This certificate must be signed by the certification authority.

NetworkVoIPSystemMonitoring

TimeAccessLogPasswordsConfiguration ManagementFirmware UpgradeRebootAutoprovisioningManagement InterfaceCertificatesAdvanced

Root certificate

Certificate

Serial Number

81:72:83:DD:0D:F4:26:C7

Not valid before

01.01.1970

Not valid after

31.12.1975

Subject

Common name

192.168.1.1

Organization

Eltex

Subject alternative name

—

Name of the certification authority

Common name

192.168.1.1

Organization

Eltex

Operation with certificate

Download certificate

Download

Upload certificate

Выберите файлФайл не выбран

Upload

Back

- *Serial Number*— serial number of the selected certificate;
- *Not valid before* — valid-from date;
- *Not valid after*— valid-to date;
- *Subject*— information about the certificate recipient (common name, organization, subject alternative name);
- *Name of the certification authority*— information about the certification authority (common name, organization).

Client certificate

Client certificate is used with outbound connections via SIP with use of TLS.

Network
VoIP
System
Monitoring

Time
Access
Log
Passwords
Configuration Management
Firmware Upgrade
Reboot
Autoprovisioning
Management Interface

Certificates
Advanced

Client Certificate

Certificate

Serial Number

Not valid before29.03.2018

Not valid after29.03.2019

Subject

Common NameEltex

OrganizationEltex

Subject Alternative Name—

Name of the certification authority (self-signed certificate)

Common NameEltex

OrganizationEltex

Operation With Certificate

Download Certificate

Download

Upload Certificate

Выберите файл

Файл не выбран

Upload

Back

- *Serial Number*— serial number of the selected certificate;
- *Not valid before*— valid-from date;
- *Not valid after*— valid-to date;
- *Subject*— information about the certificate recipient (common name, organization, subject alternative name);
- *Name of the certification authority*— information about the certification authority (common name, organization).

Web certificate

Web certificate is used when accessing to the device Web configurator via HTTPS.

NetworkVoIPSystemMonitoring

TimeAccessLogPasswordsConfiguration ManagementFirmware UpgradeRebootAutoprovisioningManagement InterfaceCertificatesAdvanced

Web certificate

Certificate

Serial Number

CD:02:8E:EE:3F:25:3F:B8

Not valid before

01.10.2018

Not valid after

18.10.2086

Subject

Common name

192.168.1.1

Organization

Eltex Ent

Subject alternative name

—

Name of the certification authority (self-signed certificate)

Common name

192.168.1.1

Organization

Eltex Ent

Operation with certificate

Download certificate

Download

Upload certificate

Выберите файлФайл не выбран

Upload

Back

- *Serial Number*— serial number of the selected certificate;
- *Not valid before* — valid-from date;
- *Not valid after* — valid-to date;
- *Subject*— information about the certificate recipient (common name, organization, subject alternative name);
- *Name of the certification authority*— information about the certification authority (common name, organization).

«Advanced» submenu

Use the menu to configure additional device settings.

NetworkVoIPUser InterfaceSystemMonitoring

TimeAccessLogPasswordsConfiguration ManagementFirmware UpgradeRebootAutoprovisioning

Management InterfaceCertificatesAdvanced

Reserved VLAN ID

Start VLAN ID

1

End VLAN ID

6

Settings LLDP

Enable LLDP

☒

LLDP transmit interval

30

✓ Apply

✕ Cancel

Reserved VLAN ID

Reserved VLAN IDs are required for solving intrasystem tasks of the gateway and may be changed depending on the VLAN ID being used for the network:

- *Start VLAN ID*— starting VLAN ID value in the reserved range, may take values in range [1-4090];
- *End VLAN ID*— ending VLAN ID value in the reserved range. This setting is unavailable for editing and calculated automatically.

Setting LLDP

- Enable LLDP — use LLDP when checked;
- LLDP transmit interval — time interval for messages transmission through LLDP. Default value is 30 seconds.



To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.