**Technical Task**

Device Management Server - TR-069 (CWMP) CPEs control and monitoring platform

Content

**Content 2**

**General information 4**

Platform full name 4

Platform conventional symbols 4

Platform ultimate customer (ultimate user) 4

List of abbreviations and terms 4

**Platform development purpose and goals 6**

Platform purpose 6

Platform creating goals 7

**CPE and business process automation characteristics 8**

Provided services 8

Internet access service 8

Bridged services or additional services 8

CPE 8

Subscriber devices CPE 8

Rule-Based Automation 8

Main business process 9

Subscriber CPEs configuring 9

Subscriber CPEs replacing 10

Subscriber CPEs deletion 10

Subscribers requests or technical support process 10

**Approved platform requirements or platform specification 10**

**General requirements**  10

Structural and functional requirements 10

Staff no., time schedule and qualification 11

Reliability requirement 12

Scalability requirement 13

Maintenance requirements 14

Data protection and unauthorized access requirements 14

Data preserve requirements for all emergency contexts 14

Non-infringement quality to the DMS platform 15

Unification requirement 15

Requirements for platform functions and tasks 16

Data storage subsystem requirement 16

Terminal interaction requirement 17

Requirement for CPE search function implementation including subscriber datas 18

Requirement for CPE status management function implementation 19

Requirement for CPE management function implementation 19

Requirement for CPEs class management based on DMS functionality 20

Auto-Based CPE configuration mechanism 20

Requirement to Factory Reset function 21

Rule-Based CPE management 21

DMS and CPE diagnostics 21

CPE software (firmware) and software update process requirements 22

Requirements for interaction with external systems and programs 22

UI requirement 23

Communication support requirement 24

Linguistic support requirement 25

* 1. General information
  2. Platform full name

CPEs management platform on the CWMP protocol, hereunder referred to DMS. Software «DMS».

* 1. Platform conventional symbol

DMS platform

* 1. Platform ultimate CUSTOMER (ultimate USER)

«UCOM», CJSC (ЗАО «ЮКОМ») hereunder referred to ultimate CUSTOMER

* 1. List of abbreviations and terms

**Table 1 List of abbreviations and terms**

|  |  |
| --- | --- |
| **Name** | **Description** |
| ACS | Auto Configuration Server – network terminating equipments management platform general title. |
| BBF | Broadband Forum – non-profit industry organization. The organization provides development and distribution specification for broadband data network protocols.  CWMP protocol specification development is BBF one of the main effort |
| CPE | Customer Premises Equipment – telecommunication equipment connected to a public or private network through a network interface. CPE located in the subscribers apartment or house or flat. |
| CWMP | CPE WAN Management Protocol – CPEs management application level protocol. |
| DB | Database. |
| NBI | North Bound Interface – north interface, interface for interaction in the internal network with IT system of «ultimate CUSTOMER» |
| RPC | Remote Procedure Call – remote procedure call on СРЕ. |
| SBI | South Bound Interface –south interface, interface for interaction with external network and with CPEs. |
| STB | Set Top Box. |
| TR-069 | Technical Report - 069 – CWMP technical specification |
| VoIP | Voice over IP – phone communication through IP data network. |
| Zero Touch Provisioning | Automatic CPE configuration |
| ПО | Software |
| СУБД | Data base system |

1. **Platform development purpose and goals**
   1. Platform purpose

"DMS" is intended for control of subscriber devices (CPE) using TR069 stack protocols. DMS allows to organize a wide range of technological processes associated with subscriber equipment, such as:

* configuration, reconfiguration of subscriber devices;
* adding, deleting subscriber services;
* software update (firmware) of subscriber devices;
* error detection and correction on CPEs;
* Zero Touch provisioning;
* mass configuration and firmware update;
* real time mode technical support ;
* CPE remote management and monitoring.

DMS is the link (middleware) for CPEs management tasks. DMS provides interfaces to the OSS/BSS system to manage applicable CPEs, and completely hides the complexity of device characteristics and enables a service-oriented management model for connected systems.

DMS translates the stages of a business process into a sequence of specific actions performed on subscriber devices. DMS takes into account the characteristics of devices and allows you to execute complex scripts in relation with many devices.

To work with devices, DMS supports various BBF standards, including TR-069. TR-069 - technical specification (TR - Technical Report), describing the protocol for managing subscriber equipment remotely via an IP network - CWMP (CPE WAN Management Protocol). Any subscriber devices with TR-069 support enabled can be controlled remotely via DMS. Examples of such devices are IAD access devices, IP telephones, STB set-top boxes, VoIP telephone gateways.

To support devices incompatible with TR-069, the functionality of the DMS can be extended with an additional adaptation module to interact with the control protocols contained in these devices.

To provide Zero Touch Provisioning DMS fully support integration with ultimate Customer internal IT systems.

* 1. Platform creating goals

As a result of the creation of the Platform, the following goals should be achieved:

**Increasing customer loyalty:**

* Acceleration of errors diagnostics when contacting a customer is achieved due to quick access to all CPE parameters in a single interface.
* Reducing the time of communication with the client to determine the problem. The client does not need to have deep technical knowledge to describe the problem.
* Making the necessary changes to the CPE configuration at the time of the client's request.
* Reducing clients complaints about CPE performance by being proactive. It is provided by the collection of CPE statistical data and the ACS analytics module, which allows to create alerts about the incorrect operation of some CPE components even before the client calls.
* Automatic configuration of new CPEs when connecting new client, when replacing client devices in case of failure.
* Reduced troubleshooting period of time.
* Reducing number of visits to set up CPE.
* Improving the quality of all services.

**Centralized management of connected applications:**

* Unified and centralized CPE management policy. Bulk operations are performed within the framework of unified campaigns and policies with flexible CPE selection criteria. Campaigns and policies are created by a System user with the Manager role.
* Reducing operating costs, time and resources spent to launch existing and new clients services.

1. **CPE and business process automation characteristics**
   1. Provided services
   2. Internet access service

The connection for Internet access is established by the IPoE client, PPPoE implemented in the CPE. Client identification occurs on the client side and does not require storing additional information about the session and subscriber's access data.

The CPE obtains a dynamic public or private IP address via DHCP for IPoE or via PPP for PPPoE.

Access of client devices (personal computers, laptops, etc.) is performed by means of routing using NAT. Dynamic configuration of the network parameters of these client devices is implemented via the DHCP protocol from the DHCP server implemented on the CPE.

Client equipment can be connected to 1, 2, 3 LAN ports, or via a wireless Wi-Fi interface.

3.3.Bridged services or additional services

Bridge group configuration with the ability to assign an Ethernet port to it.

3.4. CPEs - ultimate Customer CPEs

* Calix 813G-2
* Calix 844G-1
* Calix 814G-1
* ERSN R1B
* ERSN R1A
* ERSN T073G
* TP-Link Archer AX10

3.5.Rule-Based Automation

CPE must obtain DMS details (ACS URL) via three ways (in descending order of priority):

* DHCP Option 43.
* ACS URL by manual.
* ACS URL, fixed in device firmware.
* OMCI subscriber profile.
* In any other way that can be identified in the process of working with the fleet of CPE.

Devices accessing the ACS URL transmit their identification data:

* InternetGatewayDevice.DeviceInfo.SerialNumber
* InternetGatewayDevice.DeviceInfo.ManufacturerOUI
* MAC-address WAN-port

after that they are registered on ACS, after which it becomes possible to receive and change parameters from the TR-069 parameter tree, perform RPC, in accordance with the protocol.

On the ACS side, it is possible to perform both single actions and mass operations across the entire fleet of supported devices or based on campaigns with complex selection conditions.

3.6. Main business process

DMS affects the following business processes of the ultimate Customer:

Subscriber CPEs configuring

DMS does not directly participate in the connection of the subscriber and the organization of access, however, when connecting a new device.

Connection CPEs with ACS are possible in the two manners:

* Connection without prior activation – a new CPE arrives at ACS and registers in the management network, ACS makes a request to an external information system to establish a connection between the CPE and the subscriber data than request transmits the network data received from the CPE (WAN IP, MAC, etc., specific list is set during integration).
* Connection with pre-activation - using a known serial number, the CPE is connected to the ACS by an engineer when issuing it to a client. A stub device emulator is created on ACS with known subscriber data and settings, when a CPE with the corresponding serial number and entered information appears on the network is associated with ACS.

Subscriber CPEs replacing

Replacing the CPE means replacing identifiers (serial number, MAC address). Replacement can be done both with ACS and via API by external IT systems.

When replacing, all settings associated with the CPE are transferred to the new device, the old CPE is automatically removed from the system.

Subscriber CPEs deletion

Disconnecting the subscriber means that the device is inactive on the network and is not accessing the ACS. Inactive devices can be removed from ACS automatically by timeout or via API by an external system. When the device reappears on the network, it is perceived as new and processed according to the “Subscriber connection” scenario, thus, if the device is transferred to another subscriber, the device will be associated with the subscriber.

Subscribers requests or technical support process

When contacting technical support, a support specialist uses DMS to obtain data and statistics from the CPE, view CPE logs and process previous actions with the CPE, as well as change CPE settings, execute remote scripts (reboot, factory reset, etc.).

A specific list of data and scenarios for display and interaction is determined during the integration of the DMS into the customer's business processes in accordance with the staff responsibilities and the technical readiness of devices.

1. **Approved platform requirements or platform specification**
   1. **General requirements**
      1. Structural and functional requirements
         1. DMS must fulfill the following general requirements for structure and operation::

* DMS should not interfere with the functioning of the ultimate Customer's business applications.
* DMS must be scalable, which means the ability to work with additional monitoring objects by increasing resources without fundamentally restructuring the architecture or implementation model.
* DMS must be expandable to work with 300,000 CPEs.
* DMS should be built on a modular basis with the integration of several subsystems.
  + - 1. DMS must support IPv4, IPv6 and IPv4/IPv6 dual stack for TR-069 operation
      2. DMS vendor (DMS provider) should provide a diagram/diagram explaining the architecture of the ACS solution.
      3. DMS must be built with n+1 redundancy. The DMS vendor (DMS provider) should describe in detail how this is implemented.
      4. DMS must be built in such a way that the output of one of the software and / or hardware components does not affect the performance of the DMS as a whole and does not limit the provision of automatic configuration services.
      5. DMS redundancy solution must operate in both active/active and active/standby modes.
      6. Integration with various IT systems and mandatory multi-protocol support from both IT systems and DMS.
      7. The SBI management interface of the CPE must be isolated (protected by a port filter on the firewall) from the NBI interface. The scalability of the SBI interface should depend on the number of CPEs served, and not depend on other parameters.
      8. It should be possible to obtain data on CPE in the amount necessary for the implementation of all control and configuration functions..
    1. Staff no., time schedule and qualification
       1. DMS users are the ultimate Customer's employees responsible for maintenance of IT infrastructure components.

It is sufficient to allocate the following roles of users (the list can be extended, depending on the needs of the customer), listed in the table below.

**Table 2. Users roles description**

|  |  |
| --- | --- |
| **Роль** | **Описание** |
| Manager | Full access to DMS, configuration, scenario setting, the ability to make changes to the functionality of other roles. |
| Admin | Access to the Administrator portal, full access to the technical support portal |
| Level 2 crew | Extended access to the technical support portal (support engineer). |
| Level 1 crew | Limited access to the technical support portal (support specialist). |

Users with the roles of "Manager", "Admin" must be trained in the use, administration and support of DMS components.

Users with roles of the 1st and 2nd levels must undergo a production briefing on the use of DMS.

The Customer himself determines the required number of personnel serving DMS. Vendor recommendations on the number of personnel with the roles of Managers - 2 specialists, Admin - 2 specialists.

* + 1. Reliability requirement
       1. DMS is implemented on a virtual infrastructure provided by the Customer. The reliability of the infrastructure provided for DMS and the network availability of DMS are the responsibility of the Customer.
       2. The hardware components of the DMS must be connected to an uninterruptible power supply (UPS) to prevent the failure of the System due to a power failure.
       3. DMS must be built with n+1 redundancy.
       4. DMS must be built in such a way that the output of one of the software and / or hardware components does not affect the performance of DMS as a whole and does not limit the provision of automatic configuration services. Deterioration of service characteristics by no more than 30% is allowed. Denial of service is not allowed. DMS vendor (DMS provider) should describe how this mechanism is implemented.
       5. DMS must operate 24 hours a day, 365 days a year and have a functional availability level of at least 99.97%.
       6. DMS redundancy solution must operate in both active/active and active/standby modes.
       7. Reliability of storage of executable and configuration files DMS must be implemented by hardware and use both redundancy and mirroring of information.
       8. Reliability of DMS operation must be ensured by redundancy of software components. The choice of solution should take into account the available technical capabilities of the Customer.
       9. When DMS is put into trial operation (and then into industrial operation), DMS components must be included in the circuit of the corporate data backup system in accordance with the regulations developed by the Contractor.
    2. Scalability requirement
       1. DMS support the possibility of horizontal scaling (increasing the number of servers performing the same function in parallel) and clustering. The application must provide the ability to operate the system in a fault-tolerant mode. The application must allow the use of load balancing features.
       2. DMS vendor (DMS provider) must specify system performance based on the maximum number of managed devices. DMS vendor (DMS provider) should advise what other limitations exist when planning a configuration service.
       3. DMS vendor must provide information on the scalability of all components of the hardware-software complex of the implementation of the DMS (CPU, databases, servers, etc.) and information on the mechanism of the scaling procedure.
       4. DMS vendor (DMS provider) must specify any existing limits on system scalability.

* + 1. Maintenance requirements

DMS should provide the ability to configure and perform routine maintenance of its subsystems and components without interrupting subscriber service and disrupting the operation of the broadband access network.

* + 1. Data protection and unauthorized access requirements
       1. Protection of internal system information from unauthorized access must be provided by the built-in tools of the DMS software.
       2. To protect information from unauthorized access in DMS, mechanisms for domain authorization and authentication should be provided at the level of each subsystem / module.
       3. It should be possible to create, edit and delete user accounts and assign the appropriate rights (privileges) for each.
       4. DMS for assigning user passwords must comply with security regulations in accordance with the length of passwords, the type of characters used, the time passwords are saved, etc..
       5. Authorization and authentication of users in DMS must be carried out:
* Using standard authentication and authorization technologies provided by MS Active Directory.
* With the use of an internal database of users, subject to the use of solutions integrated with IDM. Explicit storage of passwords in the internal database is not allowed.
* All DMS nodes must communicate with each other using standard protocols of the TCP/IP stack.
  + 1. Data preserve requirements for all emergency contexts

Requirements for the safety of information in emergency situations are presented in the table below.

**Table 3 Emergency context**

|  |  |  |
| --- | --- | --- |
| **Setup** | **Ways of dealing** | **Data status after repair** |
| Short term power loss (less than 30 minutes) | Power is supported by an uninterruptible power supply | Actual data |
| Long term power loss (more than 30 minutes) | Automatic shutdown of physical servers of DMS in case of power loss | Up-to-MOMENT data at the time of shutdown |
| Disk subsystem failure | Hardware duplication of information on hard drives is used | Actual data |
| Erroneous actions of personnel or system errors that led to distortion, loss of data in DMS | Restoring intrasystem and relational databases from a backup | Data at the time of the last successful backup operation |
| Failure of DMS component or subsystem | Duplication at the hardware level. | Actual data |

* + 1. Non-infringement quality to the DMS platform

The delivery of DMS must include the licenses necessary for the normal functioning of DMS in accordance with the specification. DMS vendor is obliged to provide the ultimate Customer with DMS patent clearance.

* + 1. Unification requirement
       1. DMS must use standard, unified methods for implementing the functions (tasks) of DMS.
       2. The user interface of DMS must fully support the latest versions of modern web browsers. For Support Portal: Microsoft Edge, Safari, Chrome, Opera, Firefox.
       3. DMS must provide control of CPEs from different manufacturers operating on TR-069 protocols.
       4. DMS must provide management of CPEs of various manufacturers operating via telnet, http protocols.
       5. DMS must provide full support for TR-069 CPEs certified to BBF TR069 by Inter Operability Laboratory.
       6. The implementation of DMS must comply with the recommendations of BBF TR-069 amendment 6.
       7. DMS must support TR-181, TR-157, TR-104 and TR-098 data models for CPE management.
  1. Requirements for platform functions and tasks

This section presents the requirements for the functions of each subsystem

* + 1. Data storage subsystem requirement

DMS must provide storage of CPE parameters, script execution history

* + - 1. Storage of CPE parameters
      2. DMS must store the data received from the CPE in the database for 3 months.
      3. DMS must store the following minimum set of parameters:
* InternetGatewayDevice.ManagementServer.URL
* InternetGatewayDevice.ManagementServer.Username
* InternetGatewayDevice.ManagementServer.Password
* InternetGatewayDevice.ManagementServer.ConnectionRequestURL
* InternetGatewayDevice.ManagementServer.ConnectionRequestUsername
* InternetGatewayDevice.ManagementServer.ConnectionRequestPassword
* InternetGatewayDevice.DeviceInfo.Manufacturer
* InternetGatewayDevice.DeviceInfo.SerialNumber
* InternetGatewayDevice.DeviceInfo.SpecVersion
* InternetGatewayDevice.DeviceInfo.ManufacturerOUI
* InternetGatewayDevice.DeviceInfo.HardwareVersion
* InternetGatewayDevice.DeviceInfo.SoftwareVersion
* MAC-address WAN-port
  + - 1. Depending on the implementation of process configuration options, ACS can store other parameters.
      2. DMS should keep a history of interaction with the CPE.
      3. DMS should automatically save the history of interaction with the CPE in accordance with the configured level of detail.
      4. DMS should be able to change the log verbosity level individually for a specific CPE.
    1. Terminal interaction requirement
       1. The CPE management interface must be isolated (firewalled) from the NBI interface. The scalability of the SBI interface should depend on the number of CPEs served, and not depend on other parameters.
       2. When bootstrapping the auto-configuration script that the ACS must support, the CPE must be identified and authorized. DMS should automatically configure this device based on device type and subscriber profile.
       3. Automatic configuration scripts do not require an operator to scan the CPE's MAC address or serial number, nor does it require a specific CPE to be granted to a specific user.
       4. DMS must support the following scenarios for automatic configuration and initial connection to the CPE network:
* when ACS first identifies and authorizes the CPE based on its unique Device ID (OUI, product class, serial number) and its TR-069 unique login/password combination;
* when ACS uses any available parameters (IP address, MAC address, serial number, etc.) to identify and authorize this CPE;
  + - 1. DMS must have geographically dependent flexible settings for scenarios and types of activation tied to geography and various service models, IP addressing and geography-specific service settings.
    1. Requirement for CPE search function implementation including subscriber datas
       1. DMS must contain a database of devices that are controlled by this system and allow the operator to display through the graphical interface all subscriber devices that are controlled by the system.
       2. DMS must support flexible search mechanisms that allow the operator to quickly find any subscriber devices.
       3. The search must be carried out in accordance with a certain set of parameters. The search mechanism should allow the operator:
* Combine different search parameters into one search rule that the device must match, there should be no limit on the number of criteria that can be combined into one search rule.
* Should allow combining search rules using the logical operators "AND", "OR", etc.
* Use wildcards ("\*") when specifying parameters to be found.
* Find devices using both device information (CPE) and subscriber information..
  + - 1. The search mechanism should allow the ACS operator to define values (or using "\*") for the following sets of CPE or subscriber parameters (a complete list of parameters should be available at the stage of integration with various OSS / BSS systems):
* Subscriber Information
* personal account
* Device values
* Manufacturer/vendor
* CPE model
* OUI
* MAC address
* Serial number
* Firmware version
* Hardware version
* IP
  + - 1. Information to be provided as a result of a completed search:
* CPE serial number.
* Type of CPE.
* IP.
* Current device control state.
* Time when CPE last contacted ACS.
  + - 1. The form for displaying the results of the performed search should be able to be manually configured by the system admin (by the list, the amount of data displayed).
    1. Requirement for CPE status management function implementation
       1. DMS must store, manage and respond to changes in CPE status.
       2. DMS shall store a configurable number of successful CPE status configurations and software versions. There should be a mechanism for comparing versions of stored configurations indicating changes.
    2. Requirement for CPE management function implementation
       1. The ACS system must allow the operator to control one device in real time through a dedicated device control interface.
       2. There must be a mechanism for caching TR tree parameters.
       3. DMS must be able to automatically create NAT, port translation on a managed subscriber device (CPE) for each TR-069-enabled LAN device located behind the CPE.
       4. It should be possible to import vendor-specific TR-069 parameters for CPE.
       5. It should be possible to perform operations in any combination of these operations through a graphical interface:
* Reset device configuration to factory settings;
* Upgrade/Rollback to an earlier version of the software (SW);
* Uploading a configuration file to a device;
* Uploading a configuration file from a device;
* Comparison of current and loaded configurations;
* Calling an RPC method on a device;
* Device availability check (online/offline);
* Displays the type of equipment connection (PPPoE, IPoE, for routers and Wi-Fi/LAN for IPTV).
  + - 1. Scenarios for interacting with the CPE must support multiple sessions with the CPE.
    1. Requirement for CPEs class management based on DMS functionality
       1. DMS must be able to manage groups of subscriber devices.
       2. DMS must support a flexible and powerful grouping mechanism that gives the operator the ability to easily group all subscriber devices managed by DMS that meet a specific set of criteria.
       3. The grouping mechanism should allow the operator:
* Combine various search criteria into one general rule that the desired subscriber devices must comply with. There should be no restrictions on the number of criteria combined into one rule.
* Should allow combining rules using logical operators such as “AND”, “OR”, etc.
* Combine managed subscriber devices based on any information about the device itself and the subscriber available in the ACS database.
  + 1. Auto-Based CPE configuration mechanism
       1. DMS must support various CPE automatic configuration mechanisms: pre-provisioning and fully automatic (zero-touch).
    2. Requirement to Factory Reset function
       1. DMS must be able to return the subscriber device to its factory settings.
       2. DMS should allow the subscriber device to be reset to factory settings by means of a specific command via the graphical and NBI interfaces.
    3. Rule-Based CPE management
       1. DMS should allow creating rules for automatic control of subscriber devices.
       2. DMS must be able to initiate TR-069 operations based on the following events:
* BOOTSTRAP
* BOOT
* PERIODIC
* SCHEDULED
* VALUE CHANGE
* TRANSFER COMPLETE
* DIAGNOSTICS COMPLETE
* CONNECTION REQUEST
  + 1. DMS and CPE diagnostics
       1. The graphical user interface must be able to be used for diagnostic purposes.
       2. It should be possible to implement diagnostic tests on the CPE using DMS.
       3. It should be possible to modify the parameters and characteristics of tests.
       4. Any available tests of DMS must be able to run them through the NBI interface, and the results of the tests must be returned through the NBI interface as well.
    2. CPE software (firmware) and software update process requirements
       1. DMS must support software upgrades for a single device or for a group of at least 140,000.
       2. It should be possible to perform software upgrades via graphical or NBI interfaces.
       3. DMS must be able to upgrade the software as part of the first activation of one CPE.
       4. When performing a software upgrade, DMS must be able to verify that the current CPE hardware and the software version being installed are compatible.
       5. It should be possible at any time to determine the status of the CPE software upgrade, the status of the process, in what state it is: completed successfully, awaiting the end of the process, unsuccessful end for each CPE.
       6. DMS must support automatic reloading of software on the CPE.
    3. Requirements for interaction with external systems and programs
       1. Integration with the customer's IT systems and mandatory multi-protocol support from both IT systems and ACS. This service should be scalable depending on the load.
       2. DMS must act as a server and receive commands from OSS / BSS via the SOAP / OpenAPI protocol.
       3. DMS should act as a client and send commands to OSS/BSS via SOAP/OpenAPI protocols.
       4. DMS must have connectors to various external databases (subscriber information) to ensure the search and selection of CPE for group operations by parameters from an external database.
       5. A complete list of systems is determined at the design and integration stage.
       6. All functionality of the ACS, which is available through the graphical interface, must also be available through the NBI interface.
    4. UI requirement
       1. The presence of an adaptive graphical user interface with customizable functionality (the composition of the displayed functionality depends on the user account) based on the WEB, which allows you to create both an interface for technical specialists and an interface for support staff to manage, configure, diagnose both a single device and groups of at least 1 million subscriber devices.
       2. The technical support portal for the availability of functionality should be in two versions. Portal for first line technical support and second line technical support. The portal option is determined by the user's role.
       3. The Help Desk Portal should provide the following CPE information:
* Status of interaction with CPE.
* Area with images of equipment.
* Area with images of equipment.
* Status of LAN/Wi-Fi interfaces indicating transmission and reception errors. Connection type.
* Ability to diagnose and configure Bridge on LAN interfaces.
* Wi-Fi configuration for 2.4 GHz and 5 GHz bands.
* Perform actions to turn Wi-Fi on and off.
* Perform actions to change the SSID.
* Follow the steps to change the Wi-Fi password.
* Network map.
* Download, upload, ping diagnostic tests;

The availability of this information depends on the CPE firmware.

* + - 1. The portal for the second line of technical support, in addition to the functionality of the first line portal, must provide information on CPE:
* Perform actions to reset CPE to factory settings.
* Device overview section containing CPE version, serial number, MAC address, network time, subscriber information.
* Perform actions for configuring WAN, LAN, Wi-Fi interfaces.
* Working with CPE configuration files.
* Working with CPE logs.

The availability of this information depends on the CPE firmware.

* + - 1. The portal for the second line of technical support must perform the following actions for configuring the WAN interface: DNS, Default Gateway, MTU size.   
         The availability of this information depends on the CPE firmware.
      2. The portal for the second line of technical support must perform the following steps to configure the mode of operation of bridge or router, DHCP, NAT. The availability of this information depends on the CPE firmware.
      3. The portal for the second line of technical support must perform the following actions for configuring Wi-Fi interfaces for the 2.4 GHz and 5 GHz bands: access point (SSID), setting or changing the access point password, encryption method, setting the channel, signal strength, communication standard.

The availability of this information depends on the CPE firmware.

* + - 1. The portal for the second line of technical support must perform the following actions for working with the CPE configuration: download and upload the configuration to the CPE, edit and delete the CPE configuration saved on the ACS.
    1. Communication support requirement

The composition, structure and methods of organizing and transferring data to the DMS must be determined at the stage of technical design.

The level of data storage in DMS should be built on the basis of modern relational DBS. Built-in DBS mechanisms should be used to ensure data integrity.

Information compatibility with adjacent systems should be achieved in the following ways::

* Use of standard integration adapters provided by the vendor.
* Using integration adapters developed by the vendor using open information exchange protocols (HTTP, API, REST, SOAP and others).
* Ability to connect to DBS via open ODBC/JDBC interfaces.
  + 1. Linguistic support requirement

Users must interact with the DMS at the level of the graphical user interface. ACS must support naming of logical objects and filling fields with event information in UTF-8 format.