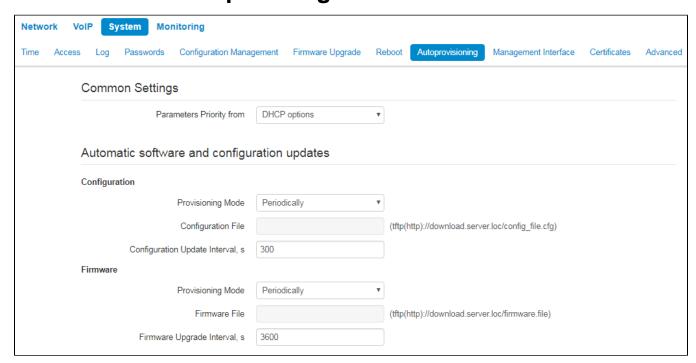# Device automatic update algorithm based on DHCP

Device automatic update algorithm is defined by the "*Parameters Priority from"* value.

If the "Static settings" value is selected, then the full path (including access protocol and server address) to configuration file and firmware file will be defined by 'Configuration file' and 'Firmware file' parameters. Full path should be specified in URL format (TFTP, HTTP, HTTPS and FTP are supported):

<protocol>://<server address>/<path to file>, where

- <protocol> – protocol used for downloading corresponding files from the server (TFTP, HTTP, HTTPS and FTP are supported);
- <server address> – address of the server with a file to be downloaded (domain name or IPv4);
- <path to file> – path to file on the server, the file must be in tar.gz extension.

You may use the following macro in URL (reserved words substituted with the specific values):

- *$MA* – MAC address – this macro in file URL is substituted by the native device MAC address;
- *$SN* – Serial number – this macro in file URL is substituted by the native device serial number;
- *$PN* – Product name – this macro in file URL is substituted by the model name (e.g, VP-12P);
- *$SWVER* – Software version – this macro in file URL is substituted by the firmware version number;
- *$HWVER* – Hardware version – this macro in file URL is substituted by the device hardware version number.

For MAC address, serial number and model name, see "Device" section on the monitoring page.

URL examples:

tftp://download.server.loc/firmware.tar.gz,

http://192.168.25.34/configs/vp-12(p)/mycfg.tar.gz,

tftp://server.tftp/$PN/config/$SN.tar.gz,

http://server.http/$PN/firmware/$MA. tar.gz etc.

At that, some URL parameters might be omitted. For example, configuration file may be specified in the following format:

http://192.168.18.6/ or config_vp12.tar.gz

If the system is unable to extract the necessary file downloading parameters (protocol, server address or path to file on server) from configuration file or firmware file URL, it will attempt to extract an unknown parameter from DHCP Option 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name), when address obtaining via DHCP is enabled for the Internet service (DHCP option format and analysis will be provided below). If the system is unable to extract missing parameter from DHCP options, default value will be used:

- protocol: tftp;
- server address: update.local;
- configuration file name: $MAC.cfg;
- firmware file name: vp 12.fw.

Thus, if you leave *'Configuration file'* and *'Firmware file'* fields empty, and Options 43 or 66, 67 with file locations are not obtained via DHCP, configuration file URL will be as follows:

tftp://update.local/A8.F9.4B.00.11.22.cfg ,

and the firmware file URL:

*tftp://update.local/*vp12*.fw* .

If 'DHCP options' value is selected, configuration file and firmware file URLs will be extracted from DHCP Option 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name), wherefore address obtaining via DHCP should be enabled for the Internet service (DHCP option format and analysis will be provided below). If DHCP options fail to provide some of the URL parameters, default parameter value will be used:

- protocol: tftp;
- server address: update.local;
- configuration file name: $MAC.cfg;
- firmware file name: vp12.fw.

⊘
1. Inspite of the filename $MAC.cfg , the file format should be in .tar.gz extension
2. Inspite of the firmware name vp12.fw , the file format should be in .tar.gz extension
3. You may upload a text file of configuration, the format of the text file must be .yaml

Option 43 format (Vendor specific info)

1|<acs_url>|2|<pcode>|3|<username>|4|<password>|5|<server_url>|6|<config.file>|7|<firmware.file>

1 – TR-069 autoconfiguration server address code;

2 – 'Provisioning code' parameter specification code;

3 – code of the username for TR-069 server authorization;

4 – code of the password for TR-069 server authorization;

5 – server address code; server address URL should be specified in the following format: tftp://address or http://address. The first version represents TFTP server address, the second version – HTTP server address;

6 – configuration file name code;

7 – firmware file name code;

"|" – mandatory separator used between codes and suboption values.

⊘
For autoconfiguration via TR-069, suboptions 1, 3 and 4 will be applied when in the autoconfiguration section the priority is selected from DHCP options on the basis of DHCP.

Algorithm of identification for configuration file and firmware file URL parameters from DHCP Options 43 and 66

1. DHCP exchange initialization.
   Device initializes DHCP exchange after the startup.

2. Option 43 analysis.
   When Option 43 is received, codes 5, 6 and 7 suboptions are analyzed in order to identify the server address and the configuration and firmware file names.

3. Option 66 analysis.
   If Option 43 is not received from DHCP server or it is received but the system fails to extract the server address, Option 66 will be discovered. If the system fails to obtain the firmware file name, Option 67 will be discovered. They are used for TFTP server address and the firmware file path extraction respectively. Next, configuration and firmware files will be downloaded from Option 66 address via TFTP.

Special aspects of configuration updates

Configuration file should be in **.tar.gz** format (this format is used when configuration is saved from the web interface in the "System" "Configuration management" tab). Configuration downloaded from the server will be applied automatically and does not require device reboot.

Special aspects of firmware updates

Firmware file should be in **.tar.gz** format. When the firmware file is loaded, the device unpacks it and checks its version (using 'version' file in **tar.gz** archive).

If the current firmware version matches the version of the file obtained via DHCP, firmware will not be updated. Update is performed only when firmware versions are mismatched. When the firmware image is written into the device flash memory, the Power indicator will flash green, orange and red in succession.

> ⊖ Do not power off or reboot the device, when the firmware image is written into the flash memory. These actions will interrupt the firmware update that will lead to the device boot partition corruption. The device will become inoperable. To restore the device operation, use the instruction provided in System recovery after firmware update failure