- **X** - interface number is set by default and can not be changed.
- **IP address** - IP-address and network mask can be set manually or be obtained automatically via DHCP.
- **Description** - set the arbitrary interface description (up to 72 characters).

Pseudo Radio Interface (prfX)

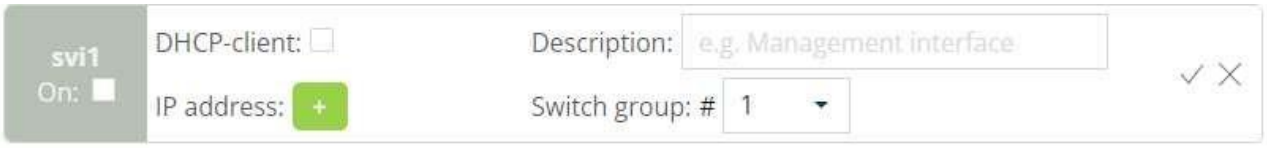
- **X** - interface number is determined by the numerical order for this interface type at the time of creation.
- **IP address** - IP-address and network mask can be set manually or be obtained automatically via DHCP.
- **Description** - set the arbitrary interface description (up to 72 characters).
- **Parent** - set the parent interface to be transmitted the encapsulated packets (assign the PRF interface to the physical Ethernet interface).
- **Channel** - set the channel number (from 0 to 3) on which the frames are sent and received by the parent interface. Both PRF interfaces (of the two units in the link) must have the same channel assigned in order to establish the wireless link.

VLAN interface (vlanX)

- **X** - interface number is set automatically equal to VLAN ID.
- **IP address** - IP-address and network mask can be set manually or be obtained automatically via DHCP.
- **Description** - set the arbitrary interface description (up to 72 characters).
- **Parent** - set the parent interface to be transmitted the encapsulated packets.
- **VLAN-id** - configure the VLAN tag (802.1q) for the current interface (from 1 to 4094).

Switch Virtual Interface (sviX)

- **X** - interface number is set automatically equal to swich group assigned.
- **IP address** - IP-address and network mask can be set manually or be obtained automatically via DHCP. This IP-address is used for the management of the unit via interfaces added to binded switch group.
- **Description** - set the arbitrary interface description (up to 72 characters).
- **Switch group** - set the Switch group number which this interface is assigned to (bind the SVI interface to a switch group).



Link aggregation interface (lagX)

- **X** - interface number is determined by the numerical order for this interface type at the time of creation.
- **IP address** - IP-address and network mask can be set manually or be obtained automatically via DHCP.
- **Description** - set the arbitrary interface description (up to 72 characters).
- **Mode** - set standard or fast operational mode, the fast mode can only be used, if MINT based device is on the other side of connection.
- **Interfaces** - set the parent interfaces to be aggregated.

Default gateway

Default gateway field allows to set an IP-address of nearest router.

Switch groups

Switch configuration

The Switch configuration is based on a set of rules for the switching groups:

- An unique numeric identifier (1-4999) for each group
- Two or more local network interfaces (*ethX, rfX, vlanX, etc*) and a set of rules (filters) which allow placing different types of traffic into different switching groups
- Each node can have several switching groups. The same interfaces or group of interfaces can be used in several groups simultaneously
- Switching groups are activated on different nodes of the MINT network. The nodes that have the same switching group identifier in their configurations represent a "switching zone"
- "Switching zone" exists only within the MINT network segment.

Switch groups

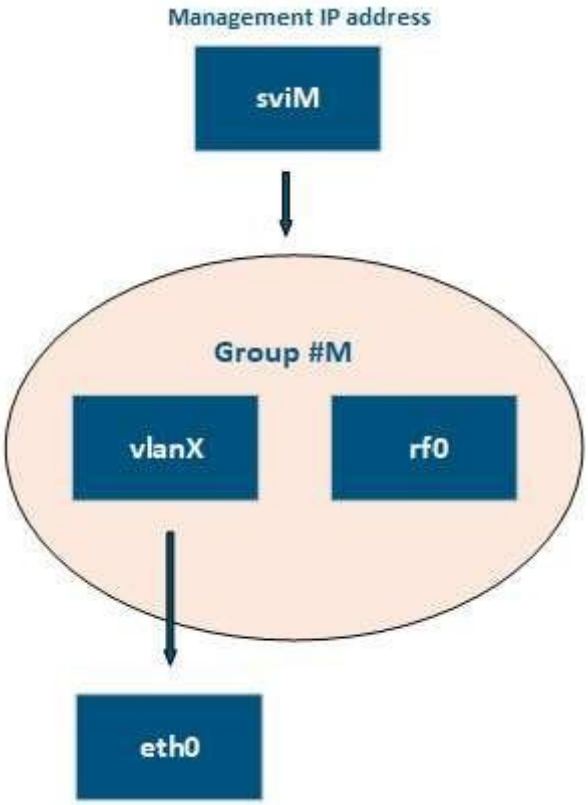
The MINT network can be viewed as one virtual distributed layer-3 switch, where border nodes act as external ports of the virtual switch. The virtual switch task is to transport frames from one external port to another. It is important to understand that switching groups should be created only on the nodes where frames enter from or leave to the "outside" network ("outside" relative to MINT). On the repeater nodes (in mesh topology) there is no need to create switching groups.

Management connection to the unit

For the management purposes, you can create a dedicated Switch Group for all units in the MINT network, attached to the Switch Virtual Interface (SVI). Assign the IP addresses directly on the SVI interface for native management. All packets sent via SVI interface will be distributed only within the assigned switch group.

The universal way to configure Management VLAN via dedicated switch group is presented in the figure below.

You have to assign the Management IP addresses to "*sviM*" interface which is the management interface of Group M and includes "*vlanX*" (with parent interface "*eth0*") and "*rf0*" interface:



Switch Group parameters

«Enable» - this checkbox enables/disables global switch operation.

Parameter	Description
Group #	Displays the Switch Group number. Assign the switch group identifier (must be unique within the MINT network segment).
VLAN-id list	Set the VLAN ID list to be passed via current switch group.
Description	Type a description sentence for the current switch group.
Interfaces	Add Ethernet or/and Radio as Switch Group interface(s) via the «+» button. "*Select*": pass (selected by default), strip or tag for VLAN tag modification for each added interface. The Interfaces section provides the means to control the VLAN tag processing mode, as each local interface supports three different scenarios: • "*Pass*" - transparent mode, traffic remains unchanged. • "*Strip*" - all tags are stripped. • "*Tag*" - all packets are tagged with the specified VLAN tag. Another option in this field is to remove one or both added interfaces.
Repeater	Enable/disable repeater support. The unit acts as a simple switch, relaying packets to all ports, except the source port.

MINT Settings

The "MINT settings" section is intended for the MINT protocol configuration.

"Interfaces list" section allows to configure MINT (radio and pseudo-radio) interfaces parameters. Radio interface is created by default and can not be deleted. To perform settings of the previously created pseudo-radio interface click "Add interface" button and select the desired interface.

Following parameters are available to configure:

Parameter	Description
MINT on	Enable / disable MINT protocol on the interface.
Node name	Interface name will be displayed in neighbour's list of the MINT network.
Role	MINT interface role. In Slave role interface can only set the connection with one Master interface. In Master role interface can set the connections with one or more (for prf) interfaces with roles Master and Slave.
Key	MINT interfaces should authorize each other before link establishment. Access key must be up to 64 characters long, without spaces and must be the same at both ends of the link.

SNMP settings

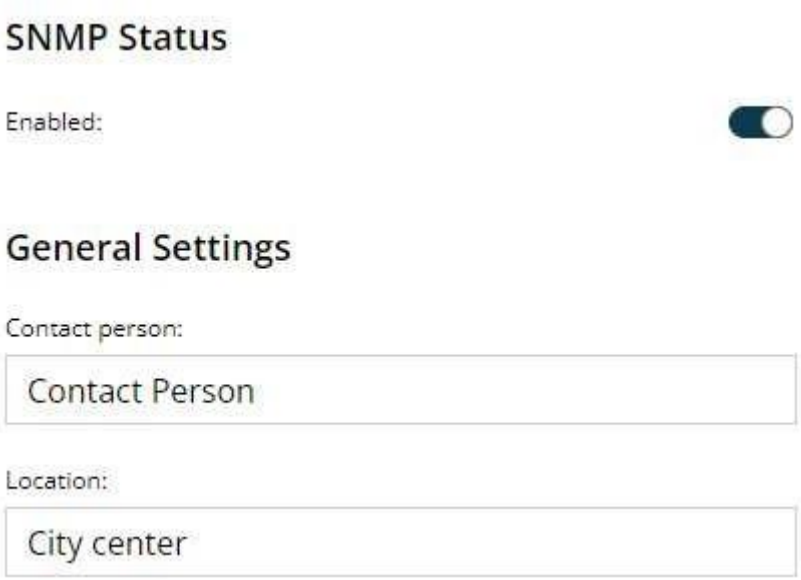
SNMP allows the administrator to gather information about key device parameters and wireless links, including information about changes. The use of any monitoring system helps to timely receive information about the network infrastructure state using Astra devices. Currently, the devices family supports SNMP protocol versions v1 v2c and v3.

The SNMP Protocol has two branches, the agent and the management stations:

- The agent sends data to the management station. Monitoring system - provides data gathering from all agents in the network.
- The monitoring system receives and processes events.
- The information is passed through requests and replies with the use of the MIB.
- The management station or monitoring system is responsible for decoding the SNMP packets and providing an interface to the administrator.

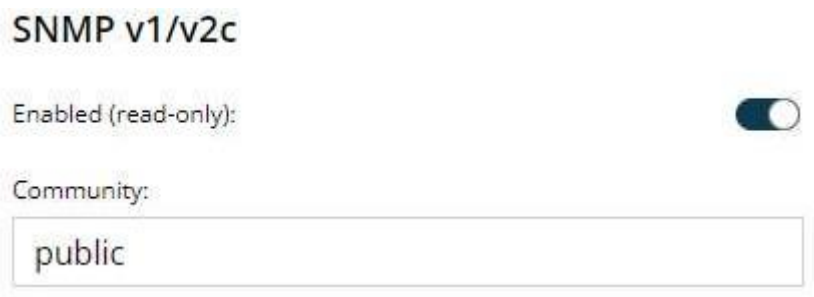
General settings

This section allow to enable/disable SNMP protocol support.



Parameter	Description
Location	The geographical location where the unit is installed, used as a reference information about the physical device's location.
Enabled	Enable/disable the SNMP service in the device.
Contact person	A reference information about the device owner.

SNMP v1/v2c



Parameter	Description
Enabled	Enable/disable the SNMP v.1 and v.2c support. The first version of the SNMP protocol lacks security, that hinders its use for network management, so SNMP v.1 and v.2c operates in read-only mode. Enabled by default.
Community	Set the community name for read-only mode of SNMP v.1 and v.2c, by default: "*public*". The community name passes along with the data packet in clear text.

SNMP v3

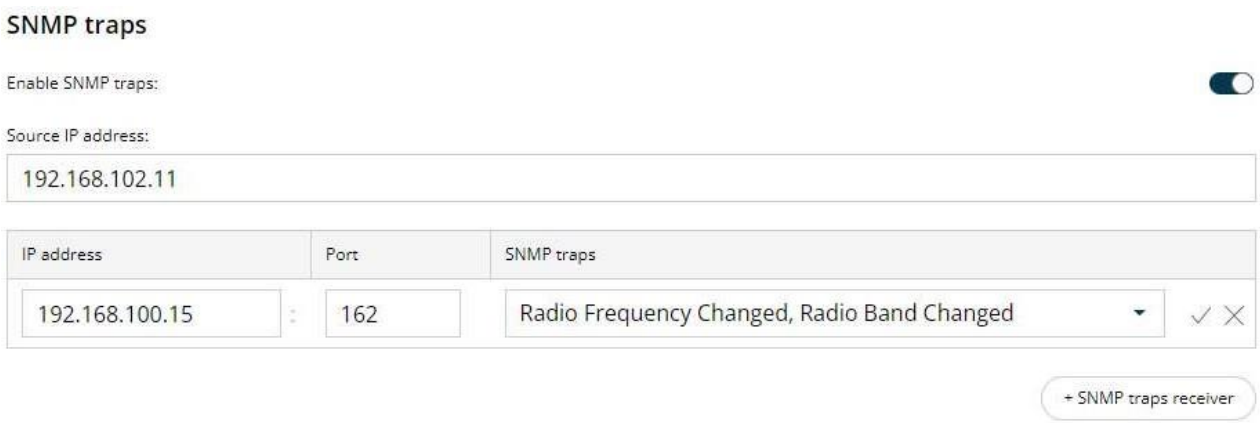
Due to the security level of SNMP v.3 is higher than of SNMP v.1 and v.2c, it allows not only the data collection but also to manage devices. Detailed information about the devices management via the monitoring system is available in the corresponding article.

To add an SNMP v3 user, click the corresponding button and fill in the following fields:

Parameter	Description
Login	SNMP v3 user name.
Password	SNMP v3 password.
Security	Security level: • "**No auth / No privacy**" – the lowest security level without authentication and privacy, only Username needs to be set. This level of protection does not allow management via the monitoring system. • "**Auth / No privacy**" – middle level with authentication but without privacy, Username and Password are required. • "**Auth / Privacy**" – highest level with authentication and privacy, Username, Password, Privacy Password and Privacy Protocol should be set.
Readonly	Enable/disable the read-only mode, readonly is set by defaut.
Admin	Enable/disable the full access to all parameters, for example, the ability to reboot the device. By default an access is limited.
Security key	Set the privacy password, it is necessary when privacy is enabled for the required security level.
Security standard	Data encryption standard DES or AES 128

SNMP traps

The devices polling cycle of the monitoring system is 5 minutes. To speed up the process of detecting incidents on devices, SNMP traps can be send each time an incident occurs, regardless of the polling process.



Parameter	Description
Enable SNMP traps	Enable/disable SNMP traps sending.
Source IP address	Set the IP address of the device which sends traps

To create a new record, click the "+**SNMP traps receiver**" button.

Fill in the following parameters:

Parameter	Description
Destination address	Set the monitoring system server IP address.
Port	Set the monitoring system UDP port.
SNMP traps	The traps type to send.

Services

Maintenance

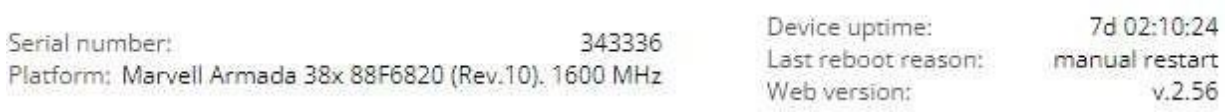
This section is used for firmware updates, operations with licenses and configuration. Allows to view extended information about the device, to reboot the device, reset factory settings, show system log and download diagnostic card in the bottom part of the screen.

The diagnostic card is necessary tool which helps to detect and solve an issue faster and more effective in situation then helps of Astra Wireless technical support team is required.

Device information

The following information is displayed on information panel:

- Part number.
- Device serial number.
- Hardware platform version.
- Time since last reboot.
- Last reboot reason, following values are possible:
  - Software fault.
  - Unexpected restart.
  - Manual restart.
  - Manual delayed restart.
  - Firmware upgrade.
  - SNMP managed restart.
  - Test firmware loaded.
  - Watchdog.
  - Panic.
- Web version.



Firmware

This section allows to view current firmware version and the build date, upload and download firmware file.

To update the firmware, a new version should be downloaded to your PC. Click on "Upload firmware" button and choose a firmware file. Or you can drag and drop a file from your file manager into the dotted area.

To download current firmware version from the device click the "Save" button.

Configuration

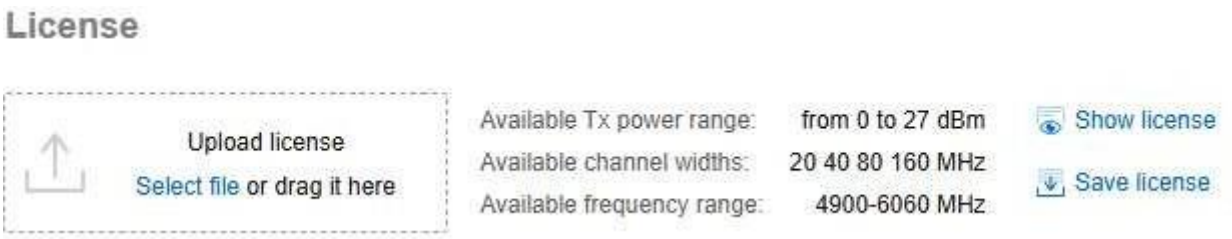
The device allows to upload, download and view current configuration in text form. To view the configuration, click the "Show configuration" button, the file will open in new window. To download the configuration, click the "Save configuration" button, the configuration can be loaded by clicking the "Upload configuration" button, or you can drag and drop a file from your file manager into the dotted area.

To upload and apply the configuration file that has beenmodified, please follow these steps:

- Change the "check_sum <VALUE>" command to "check_sum off" in the configuration file.
- Upload the configuration file to the device.
- Refresh the web page by pressing F5.
- To apply the settings, click "Changes" in the upper right corner and click "Apply" in the window that opens.

License

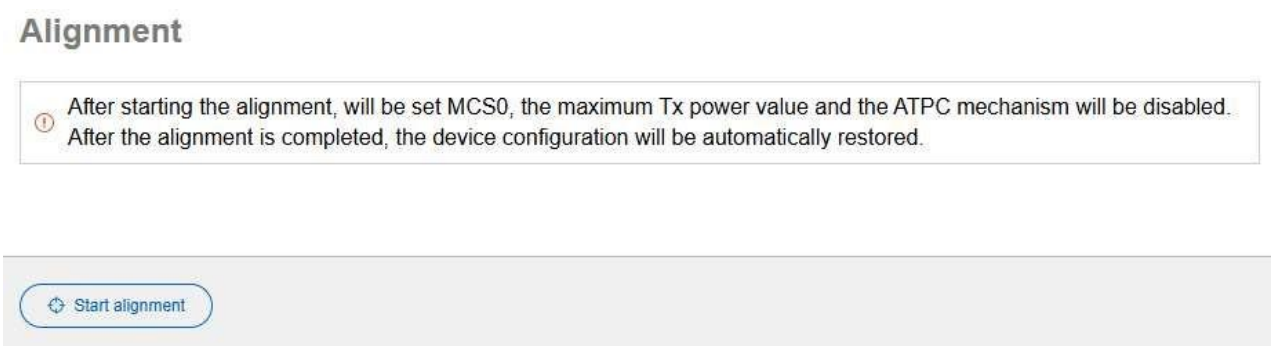
License contains information about allowed frequencies, channel width and power limit. This section allows to view the current license and upload a new one. To upload a license on device, click the "Upload license" button drag and drop a file from your file manager into the dotted area.



Alignment

The graphical antenna alignment tool allows to visualize the signal characteristics on both sides of the link in order to make the antenna alignment process more accurate and easier. It helps to find the best antenna position via comparing the actual received signal level with the calculated reference value. The accuracy of the antenna alignment at the neighbor device is very important for the link quality.

Antenna alignment tool operates online and does not break the wireless connection, but switch the devices to the alignment mode, which set MCS0, the maximum Tx power value and disable the ATPC mechanism.



Click the "Start alignment" button to begin.

Each side of the link (local and remote) has two similar test indicator sets, corresponding to each antenna polarization. This allows controlling the alignment process for each antenna polarization for the local and for the remote device simultaneously.

On the left edge of the graph there is a RSSI scale, below is a time scale (exact, if a connection to the SNTP server is performed or the time from the device being turned on). Red squares indicates break of the connection. Optimal RSSI values for operation at the highest modulations are -60...-40 dBm.

Click the "Stop alignment" button to finish a test. To download picture of current alignment state click the "Save as PNG" button.

Spectrum analyzer

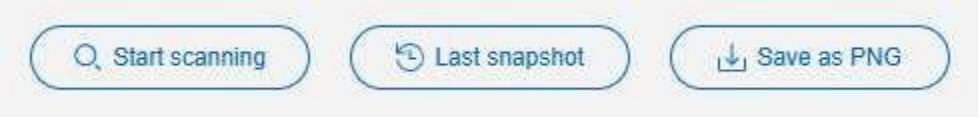
In the "Spectrum Analyzer" menu, you can perform a deep analysis of the radio emissions in the environment where the unit is placed. The unit scans the radio spectrum on all available frequencies. In order to obtain the information as accurate as possible, the scanning process may take a while.

The following parameters are available in order to operate the Spectrum Analyzer:

Parameter	Description
Start Frequency	Set the first frequency for scanning (in MHz).
End Frequency	Set the last frequency for scanning (in MHz).
Scan step	Set the scanning frequency step (in MHz). It is recommended to set 1 MHz "*step*" value to get more precise scanning results.
Channel width	Set the bandwidth (in MHz).

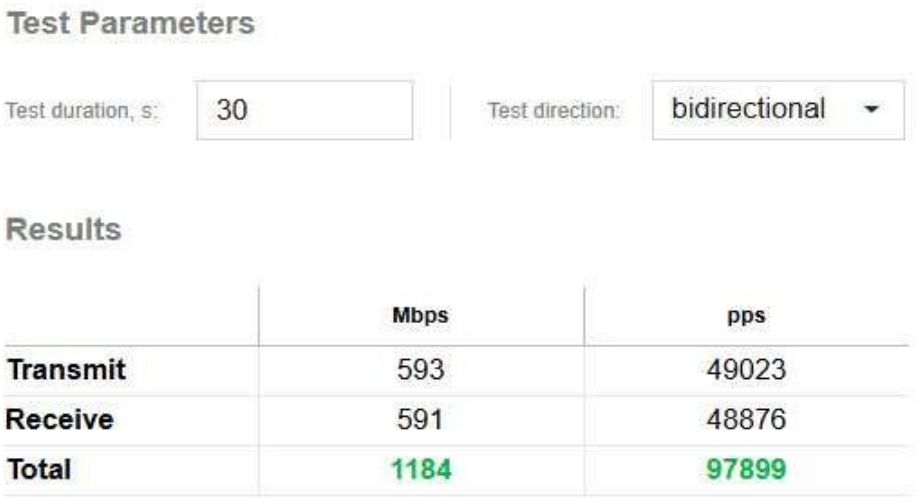
Click on "Start scanning" button to start scanning. You may stop scanning by clicking on appropriate button.

By clicking the "Last Snapshot" button, you get the final scanning results. The most common usage of this feature is when you perform a spectrum scan at the remote unit on the other side of the wireless link. When running a spectrum scan at such a unit (accessible via the RF interface), connection to this unit will be lost for a scan time. "*Last Snapshot*" option allows viewing scan results when the connection gets up again. To download picture of last scanning result click the "Save as PNG" button.



Speed test

The "Speed test" tool performs link throughput tests for the configured channel width and on the current frequency, without radio link interruption. The "Speed test" tool displays the values of the full channel throughput which is available under the current settings, for current bitrate, in Mbps ang packets per second.



By clicking the "Start Tests"/"Stop Tests" buttons at the bottom of the page, you can start/stop the performance tests.

- "Test duration" parameter allows setting the duration (in seconds) of the test.
- "Test direction" parameter allows choosing between bi-directional and unidirectional performance test.

The device is tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses,and can radiate radio frequency energy. The equipment may cause harmful interference to radio communications, if the installation is not followed in accordance with the provided instructions.
However, there is no guarantee that interference will not occur in a particular installation. If these equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on. Additionally, the user is encouraged to try and correct the interference by following any one of the listed measures:
• Reorient or relocate the receiving antenna.
• Minimum 1.5-meter horizontal and vertical separation from the nearest radio.

FCC Caution

To assure continued compliance, any changes or modifications not expressly approved by the party Responsible for compliance could avoid the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

• This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
• This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
• This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
• The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.
• These devices complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- These devices may not cause harmful interference.
- These devices must accept any interference received, including interference that may cause undesired operation.