

# **CUSTOM 4G-LTE SIGNAL INDICATOR**

---

## **FUNCTIONAL SPECIFICATIONS DOCUMENT**

## FUNCTIONAL SPECIFICATIONS

### 1. Monitoring System Initial Setup

Starting up the monitoring service consists of configuring and testing first of all the available SNMP agents of routing devices. Every network equipment has its own service and particular characteristics that must be enabled to handle SNMP monitoring.

#### 1.1. SNMP Agent Configuration

##### 1.1.1. Teltonika equipment

Teltonika routers and gateways share the same operating system and a similar proprietary software and WebUI to change the equipment settings and manage their internal services. In this section, it is presented the procedure to enable SNMP agent on a Teltonika RUT241 4G-LTE Industrial Cellular Router, although the following steps can be applied to any other Teltonika Networks device.

SNMP agent is not by default installed on the RUTOS version, so it has to be properly installed using Teltonika Package Manager.

- From a web browser, access to router WebUI using its default gateway address. Administrator PC has to be connected to the LAN of the device.

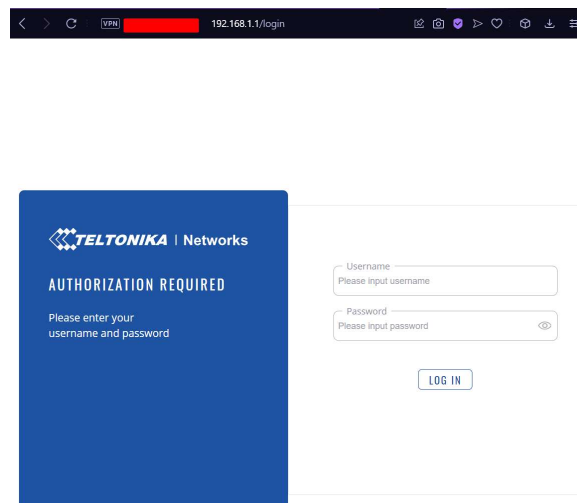


Figure 1. Teltonika Network device login screen.

- After entering user credentials, the WebUI view must be set to “Advanced” on the top right corner. This will allow access to special settings of the device.

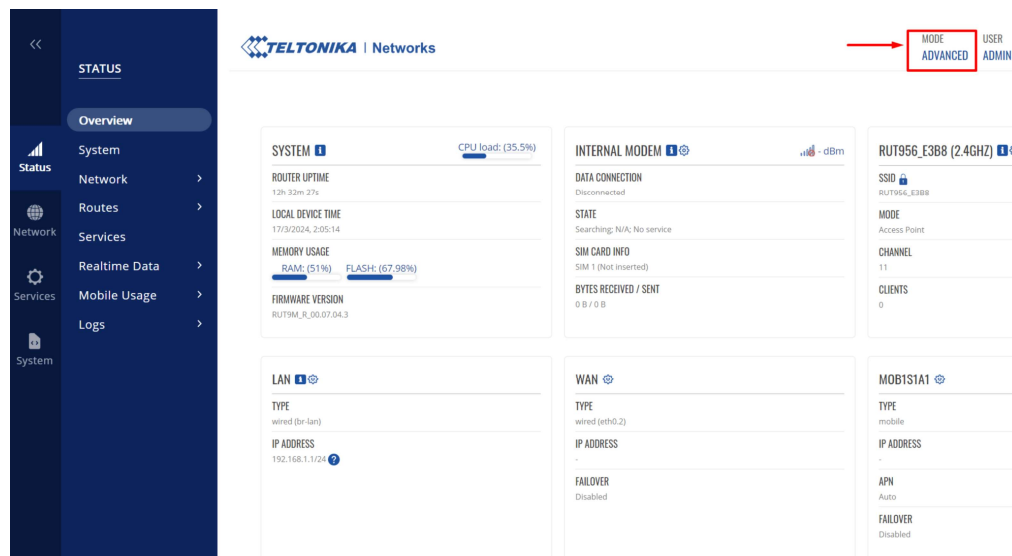


Figure 2. Teltonika WebUI changing to “Advanced” mode.

- Then, on the left panel, locate the *System > Package Manager > Packages* option. This section allows the user to install additional services on Teltonika devices. For this application, it is desired to locate the *SNMP* package. All available and downloadable packages will be displayed on screen. It is important that the device has an active Internet connection to synchronize with the Teltonika update server. The package can be located browsing through the menu or writing down its name on the search text box on the top right corner.

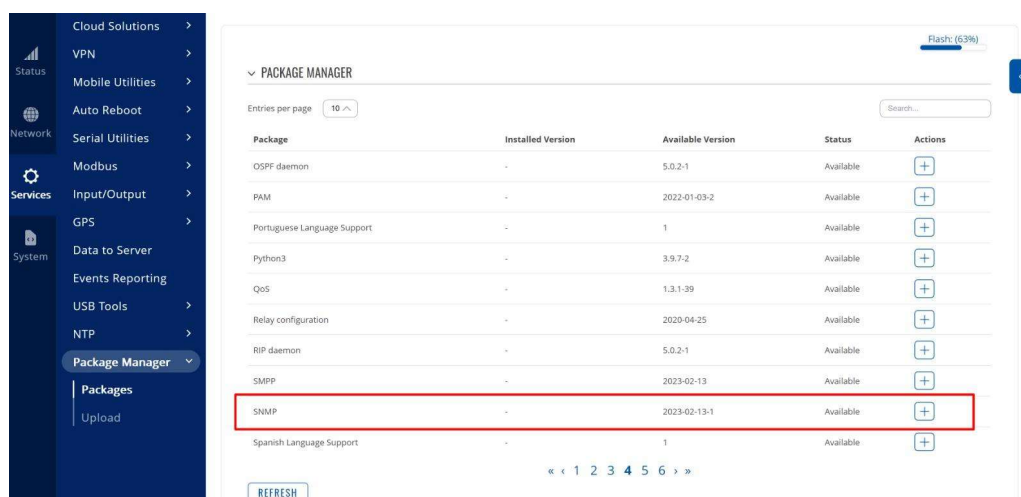


Figure 3. SNMP package installation.

- Click the plus (+) button on the package name, and installation will begin. Do not turn off your device during the installation process. If installation is completed successfully, the package will appear at the top of the packages list with its

corresponding version identifier. Also, the *SNMP* option will be from now on available as a part of the router *Services* menu as long as the respective package remains installed on the device. This package can be removed manually later from the same package manager, if desired, or performing a factory reset to the router.

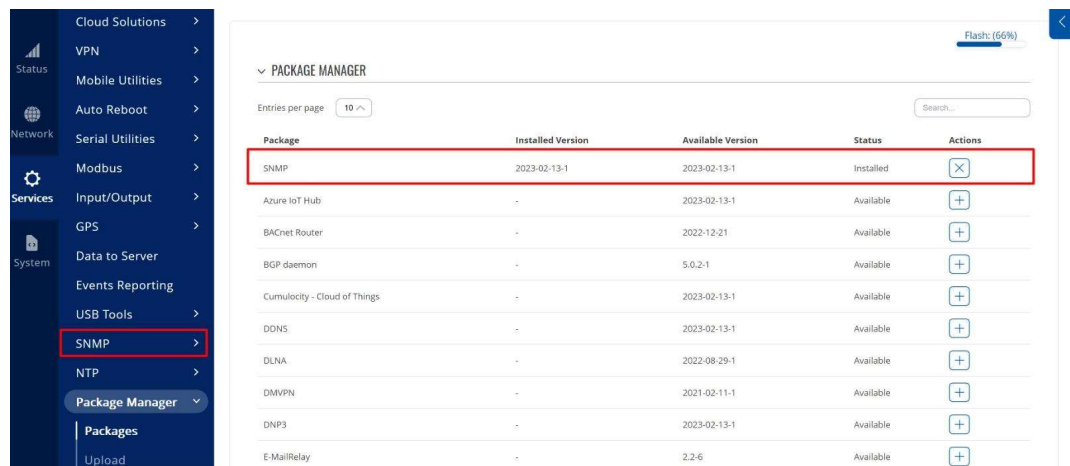


Figure 4. SNMP package after successful installation.

- Now, click on the *SNMP* service to access the SNMP agent settings. Then, enable the SNMP service and select the protocol versions that will be available for communication. As SNMP authentication will not be required on this project, SNMP v1 and SNMP v2c will be used instead. Verify the port number to establish the SNMP connection with the agent. By default, this protocol uses port 161. Finally, click on *Save & Apply* to preserve current configuration. SNMP service is now running and listening on port 161 for incoming requests..

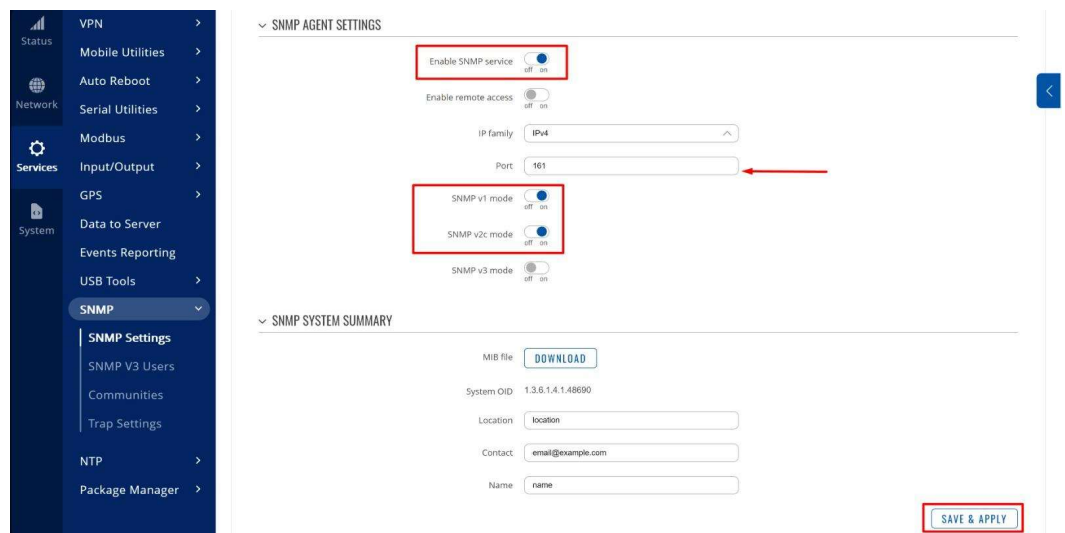


Figure 5. SNMP service settings.

### 1.1.2. Peplink equipment

Peplink routers share a similar WebUI to enable their SNMP agent service.

- From a web browser, access to router WebUI using its default gateway address. Administrator PC has to be connected to the LAN of the device.
- Access to the SNMP settings menu on *System > SNMP* option. SNMP configuration screen should appear as shown below.

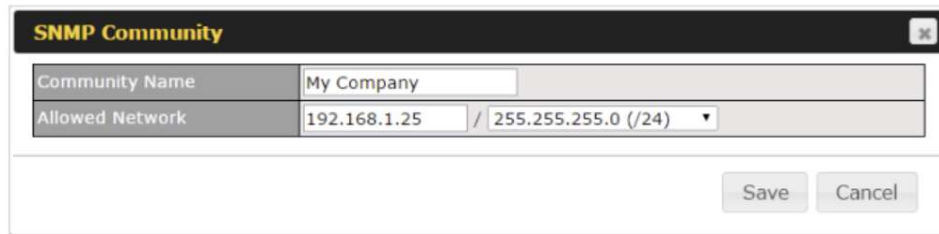
SNMP Settings	
SNMP Device Name	MAX_TST_3D8B
Location	<input type="text"/>
SNMP Port	<input type="text" value="161"/> <input type="button" value="Default"/>
SNMPv1	<input type="checkbox"/> Enable
SNMPv2c	<input type="checkbox"/> Enable
SNMPv3	<input type="checkbox"/> Enable
SNMP Trap	<input checked="" type="checkbox"/> Enable
SNMP Trap Community	<input type="text"/>
SNMP Trap Server	<input type="text"/>
SNMP Trap Port	<input type="text" value="162"/>
SNMP Trap Server Heartbeat	<input type="checkbox"/>
<input type="button" value="Save"/>	

Community Name	Allowed Source Network	Access Mode
No SNMPv1 / SNMPv2c Communities Defined		
<input type="button" value="Add SNMP Community"/>		

SNMPv3 User Name	Authentication / Privacy	Access Mode
No SNMPv3 Users Defined		
<input type="button" value="Add SNMP User"/>		

Figure 6. Peplink SNMP settings menu.

- In a similar way as explained before, select SNMP v1 and SNMP v2c as the allowed protocol versions (SNMP communication with no authentication). Port number must be verified as well. Then click on *Save* to keep selected options.
- A community name should also be configured clicking on the *Add SNMP Community* option. A community name must be chosen, as well as an allowed source subnet address with an appropriate subnet mask. By default, SNMP agents use the “*public*” community name. Click on *Save* to keep current changes.



The image shows a web-based configuration window titled "SNMP Community". It contains two input fields: "Community Name" with the value "My Company" and "Allowed Network" with the value "192.168.1.25 / 255.255.255.0 (/24)". At the bottom right, there are "Save" and "Cancel" buttons.

Community Name	My Company
Allowed Network	192.168.1.25 / 255.255.255.0 (/24)

Figure 7. SNMP community string settings for Peplink routers.

- The SNMP will be running and waiting for incoming requests.

### 1.1.3. Grandstream HT801/HT802 ATA

Finally, SNMP agent must also be enabled on the Grandstream HT801/HT802 ATA to retrieve device information using the telemetry service.

- Just like before, access the Grandstream ATA WebUI through its IP address using your preferred web browser.
- Locate the *ADVANCED SETTINGS* menu, and click on it.



Figure 8. Advanced settings menu on Grandstream device.

- Enable SNMP daemon clicking on the corresponding option, and then choose the desired settings. SNMP daemon configuration has to be consistent with the specifications indicated in previous subsections (SNMP version, listening port, and community string).

## 1.2. SNMP GET Test Script

When the SNMP agents of the equipment that make up the entire solution are properly configured, they are ready to be tested. To validate the status of each SNMP daemon, a simple Python file will be executed to perform a simple SNMP GET operation to retrieve some data registers from each device.

- The required network scheme to run the test is shown below. The ATA device and the administrator PC have to be connected to one of the routing devices LAN interfaces so that the SNMP agents can be accessible from the PC that will be running the test script.

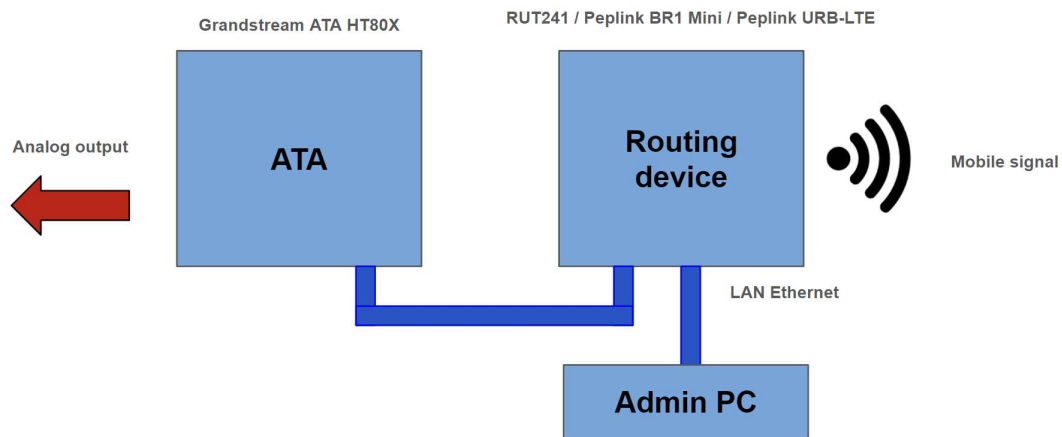


Figure 9. SNMP agents testing setup.

- To execute the test script, a Python interpreter must be installed on the administrator PC. Go to the official Python downloads website and download **Python v3.11.7**. Any version newer than **Python v3.11.0** is suitable for the test.

The screenshot shows the Python.org website's download page. The header includes the Python logo, navigation links (About, Downloads, Documentation, Community, Success Stories, News, Events), and a search bar. The main content area features a large banner for downloading the latest version of Python for Windows, with a button for 'Download Python 3.12.2'. Below this, there is a section titled 'Active Python Releases' with a table of releases. The table lists Python versions from 3.8 to 3.13, their maintenance status, first release date, end of support, and release schedule. The 'Python 3.11.7' row is highlighted with a red border. Below the table, there is a section titled 'Looking for a specific release?' with a table of releases by version number. The 'Python 3.11.7' row is also highlighted with a red border.

Python version	Maintenance status	First released	End of support	Release schedule
3.13	prerelease	2024-10-01 (planned)	2029-10	PEP 719
3.12	bugfix	2023-10-02	2028-10	PEP 693
3.11	bugfix	2022-10-24	2027-10	PEP 664
3.10	security	2021-10-04	2026-10	PEP 619
3.9	security	2020-10-05	2025-10	PEP 596
3.8	security	2019-10-14	2024-10	PEP 569

Release version	Release date	Click for more
Python 3.11.8	Feb. 6, 2024	<a href="#">Download</a> <a href="#">Release Notes</a>
Python 3.12.2	Feb. 6, 2024	<a href="#">Download</a> <a href="#">Release Notes</a>
Python 3.12.1	Dec. 8, 2023	<a href="#">Download</a> <a href="#">Release Notes</a>
Python 3.11.7	Dec. 4, 2023	<a href="#">Download</a> <a href="#">Release Notes</a>
Python 3.12.0	Oct. 2, 2023	<a href="#">Download</a> <a href="#">Release Notes</a>

Figure 10. Downloading Python v3.11.7 interpreter.

- When download is finished, execute the installation file, and mark the two indicated check boxes. Then, click on *Install now*. Admin permissions will be necessary.

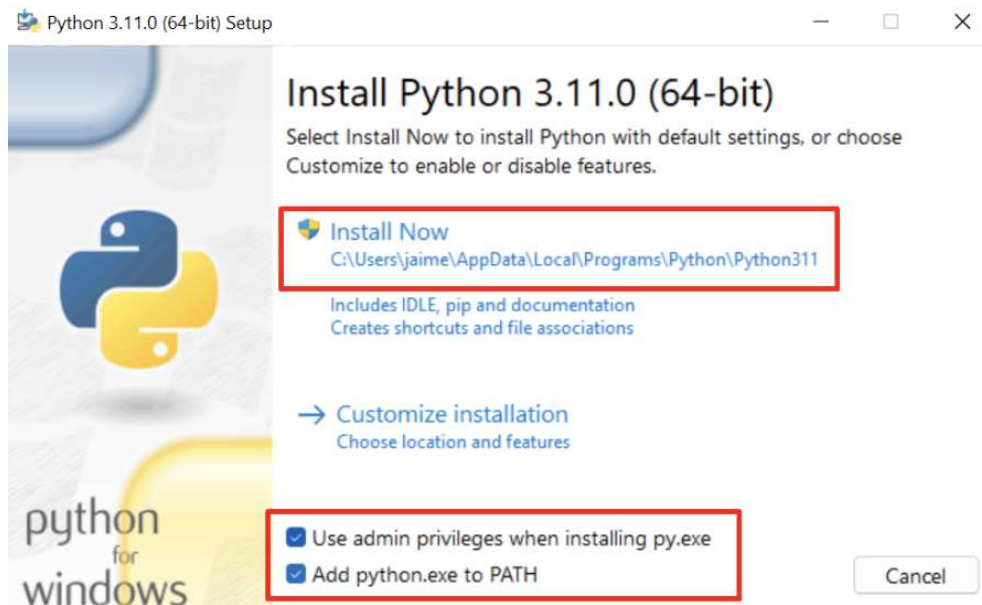


Figure 11. Python installation screen.

- After finishing Python installation, open a command prompt as an administrator, and verify the current Python version typing ***python --version***. Interpreter current version should be displayed on screen.

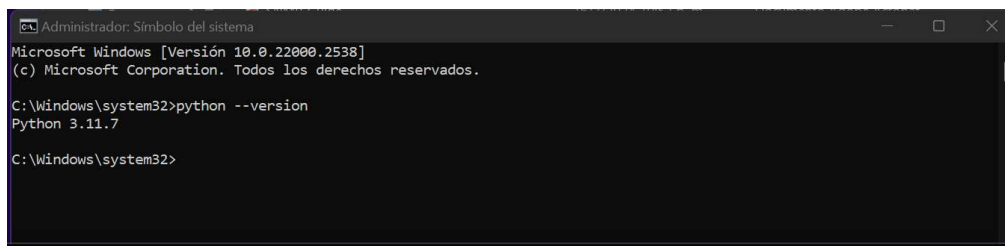


Figure 12. Current Python interpreter version command output.

- Then, the SNMP package for Python has to be added to the local packages library. On the same command prompt, execute ***pip install pysnmp***. PySNMP constitutes the core library of test script for SNMP communication. The PIP manager will download and install PySNMP packages and its corresponding missing dependencies automatically. A message with the current package version will be displayed.



```
Installing collected packages: pysnmp
Successfully installed pysnmp-4.4.12

C:\Windows\system32>
```

Figure 13. PySNMP package successfully installed.

- Now, open the provided test script identified as *snmp-test.py*. A generic text editor can be used to modify the file. This script will perform a series of SNMP GET operations to read some data registers from a selected device through its SNMP running daemon. To indicate the device the data is going to be extracted from, locate the device selection, then introduce the target device.

```
129 # Device selection
130 # (1): Teltonika
131 # (2): Peplink
132 # (3): Grandstream
133
134 selected_device = 1
```

Figure 14. SNMP test script device selection.

- Some settings can be modified using the local scripted variables. User has to make sure that declared information in the test script matches the saved settings of the corresponding device SNMP daemon. The script allows to change the community string and the SNMP agent IP address as shown below.

```
#####
#                               TELTONIKA                               #
#####

# Target device configuration
teltonika_agent_ip = "192.168.1.1" # Device IP address
teltonika_community = "public"     # Community string
```

Figure 15. Teltonika SNMP agent parameters.

```
#####
#                               PEPLINK                                #
#####

# Target device configuration
peplink_agent_ip = "192.168.1.1" # Device IP address
peplink_community = "public"     # Community string
```

Figure 16. Peplink routers SNMP agent parameters.

```
#####
#                                #
#####

# Target device configuration
grandstream_agent_ip  = "192.168.1.1" # Device IP address
grandstream_community = "public"      # Community string
```

Figure 17. Grandstream ATA HT801/HT802 SNMP agent parameters.

- Right after making the necessary changes on the script, save it, and open a new command prompt as administrator. Then, move to the directory where the test file is located using the `cd` command.

```
C:\Windows\system32>cd C:\Users\jaime\4G-LTE-Signal-Indicator\resources
```

Figure 18. Test script directory.

- Now, execute the test script calling Python interpreter using the command ***python snmp-test.py***. If all the steps explained above were correctly done, a list of OIDs and their corresponding polled values will be displayed on screen.

```
C:\Users\jaime\4G-LTE-Signal-Indicator\resources>python snmp-test.py
OID: 1.3.6.1.4.1.48690.1.1.0 = 6000670471
OID: 1.3.6.1.4.1.48690.1.2.0 = RUT956
OID: 1.3.6.1.4.1.48690.1.5.0 = 0404
OID: 1.3.6.1.4.1.48690.1.6.0 = RUT9M_R_00.07.04.3
OID: 1.3.6.1.4.1.48690.1.7.0 =
OID: 1.3.6.1.4.1.48690.2.2.1.3.1 = 862708043630230
OID: 1.3.6.1.4.1.48690.2.2.1.6.1 = EC25AUXGAR08A07M1G_01.001.01.001
OID: 1.3.6.1.4.1.48690.2.2.1.8.1 =
OID: 1.3.6.1.4.1.48690.2.2.1.9.1 = not inserted
OID: 1.3.6.1.4.1.48690.2.2.1.10.1 = SIM not inserted
OID: 1.3.6.1.4.1.48690.2.2.1.11.1 = Searching
OID: 1.3.6.1.4.1.48690.2.2.1.12.1 = -109
OID: 1.3.6.1.4.1.48690.2.2.1.13.1 =
OID: 1.3.6.1.4.1.48690.2.2.1.14.1 = 0
OID: 1.3.6.1.4.1.48690.2.2.1.15.1 = Disconnected
OID: 1.3.6.1.4.1.48690.2.2.1.16.1 = No service
OID: 1.3.6.1.4.1.48690.2.2.1.22.1 = 0
OID: 1.3.6.1.4.1.48690.2.2.1.23.1 = 0
OID: 1.3.6.1.4.1.48690.2.2.1.24.1 = N/A
OID: 1.3.6.1.4.1.48690.2.2.1.25.1 = 0
OID: 1.3.6.1.4.1.48690.2.2.1.26.1 = 0
OID: 1.3.6.1.4.1.48690.2.2.1.27.1 = N/A
OID: 1.3.6.1.4.1.48690.2.2.1.28.1 =
OID: 1.3.6.1.4.1.48690.2.2.1.29.1 =
OID: 1.3.6.1.4.1.48690.2.2.1.30.1 =
OID: 1.3.6.1.4.1.48690.2.2.1.31.1 =
OID: 1.3.6.1.4.1.48690.2.3.0.1 =
```

Figure 19. SNMP test result.

- If SNMP GET operation fails, an error message will be displayed on screen. SNMP daemon settings and running status must be then checked, as well as the devices network configurations.

## REFERENCES

Grandstream Networks Inc. "SNMP Guide". [Online product documentation]  
[https://www.grandstream.com/hubfs/Product\\_Documentation/SNMP\\_Guide.pdf](https://www.grandstream.com/hubfs/Product_Documentation/SNMP_Guide.pdf)

Grandstream Networks Inc. (2022). "HT801/HT802 Analog Telephone Adaptors. Administration Guide. Version 1.0.35.4". [Online product documentation].  
[https://www.grandstream.com/hubfs/Product\\_Documentation/ht80x\\_administration\\_guide.pdf](https://www.grandstream.com/hubfs/Product_Documentation/ht80x_administration_guide.pdf)

Pepwave. "Pepwave MAX User manual" [Online product documentation].  
<https://manual.peplink.com/pepwave-max-user-manual/>.

Teltonika Wiki Knowledge Base. "RUT 241" [Online product documentation]  
[https://wiki.teltonika-networks.com/view/RUT241\\_SNMP](https://wiki.teltonika-networks.com/view/RUT241_SNMP).

Python Software Foundation (2024). <https://www.python.org/downloads/>