1. Product Description

The use of wireless data communication technologies in automation, data collection, and telemetry systems is a growing trend, especially as a driving force behind the revolutions of Industry 4.0. The advantages of using wireless technology are numerous, and its dissemination is still below its real potential, mainly due to doubts about the security, stability, and reliability of this type of communication. Wireless communication solutions significantly reduce cabling, installation, and commissioning costs. In addition, they also extend to the maintenance stage because this type of communication allows access to data that could not be accessed by wired technologies. Access to this data and its subsequent analysis can prevent unnecessary downtime in processes and systems, which increases the availability, productivity, and safety of the infrastructure provided.

The LoRa (Long Range Communication) standard is the wireless modulation used to create the long-range communication link. LoRa is based on spread spectrum modulation, which maintains the same low-power characteristics as FSK (Frequency-Shift Keying) modulation, but significantly increases the communication range. Spread spectrum has been used in military and space communications for decades due to the long communication distances that can be achieved and robustness to interference, but LoRa is the first low-cost implementation for commercial use.

These features enable the creation of urban or rural networks due to the coverage area that gateways like the GW700 can cover. Due to its Sub-Gigahertz operating band, the penetration of LoRa communications also allows interactions with devices located underground or in the basements of establishments.

In private networks, it is possible to deploy servers without the need for large operating resources or licensed software. Although there are commercial software solutions for these networks, open developments have evolved security aspects over the last few years for professional applications.

The GW700 has been designed for aggressive environments, such as some industrial plants and exposure to the weather, as it has an IP 67 degree of protection and is therefore perfectly suited to urban, rural, or industrial environments. It also has a power supply system with various protections that comply with the main international standards.

In addition to having connectivity with LoRa devices developed by Altus, the GW700 can interact with any LoRa device on the market. Thousands of devices are currently available on the market for monitoring temperature, humidity, and water levels. In addition, the GW700 can be incorporated into any network with other gateways on the market without the need for any adaptation or conversion equipment.

Its main features are:

- LoRaWAN communication standard
- A high-performance gateway operating on 915-928MHz frequencies according to region
- Network security using encryption and security keys that prevent access to the network without using them
- Efficient message publishing algorithm to maximize the use of devices with batteries and/or techniques for powering wireless devices
- Ethernet communication interface
- Enclosure with IP 67 degree of protection for use outdoors
- Removable antenna with the possibility of using an external antenna
- Configuration and monitoring via integrated web server
- Integrated network diagnostics monitoring
- Real-time clock

2. Ordering Information

2.1. Included Itens

The product package has the following items:

- GW700
- Antenna
- Connector

2.2. Product Code

The following code should be used to purchase the product:

Code	Description
GW700	GATEWAY LORA, ETH

Table 1: Product Code

3. Related Products

The following products must be purchased separately when necessary:

Code	Description
NL717	NL717 - DATALOGGER 8DI 8AI LORA
NX9202	RJ45-RJ45 2 m Cable
NX9205	RJ45-RJ45 5 m Cable
NX9210	RJ45-RJ45 10 m Cable

Table 2: Related Products

4. Product Features

4.1. General Features

	GW700
Module Type	GATEWAY LORA, ETH, USB
Nominal Supply Voltage	12/24 Vdc
Power Supply Voltage	10 to 30 Vdc
Maximum Current Consumption	450 mA @ 12 Vdc
Operating Consumption	0.35 A @ 12 Vdc / 0.2 A @ 24 Vdc
Power Dissipation	4.5 W
Real-time Clock	Yes
Time Synchronization	Yes
Configuration	Through integrated web server
Diagnostics	Through integrated web server
Operating Temperature	0 to 60 °C
Storage Temperature	-20 to 70 °C
Operating and Storage Relative Humidity	5% to 96%, non-condensing
Protection Index	IP 67
Standards and Certifications  **RoHS – 2011/65/EU**	Yes
 **ANATEL (16956-22-14445)**	Yes
Product dimensions (W x H x D)	198,0 x 275,0 x 54,0 mm
Product dimensions with antenna (W x H x D)	198,0 x 466,0 x 54,0 mm
Packaging dimensions (W x H x D)	230,0 x 325,0 x 85,0 mm
Weight	1 kg
Weight with package	1,3 kg

Table 3: General Features

Notes:
Ethernet Interface: Category 5 (CAT5) cable is recommended.
Maximum Current Consumption: Maximum consumption considering a supply voltage of 12 Vdc.
Power Dissipation: Power considering a supply voltage of 12 Vdc.
Time Synchronization: Through SNTP protocol, without internal GPS module.

4.2. Radio Features

	Radio
Radio Type	LoRaWAN
Operation Frequency	915MHz to 928MHz
Bandwidths	125kHz / 250kHz / 500kHz
Receiver Noise Figure	7dB
Receiver Sensitivity	-140 dBm
Output Power	27 dBm

Table 4: Radio Features

Notes:

For more information see: www.gov.br/anatel.

This equipment is not entitled to protection against harmful interference and may not cause interference to properly authorized systems.

This product is not suitable for domestic environments usage because it may cause electromagnetic interference that requires the user to take reasonable steps to minimize such interference.

Operation Frequency: The frequency band can be adjusted according to the region through internal settings within the limits between 915MHz and 928MHz (ISM - Industrial, Scientific, and Medical).

4.3. Antenna Features

	Antenna
Antenna Type	Omnidirectional for outdoor environments
Connector	Male SMA-RP
Frequency Band	915MHz to 928MHz
Gain	2 dBi

Table 5: Antenna Features

4.4. Ethernet Interface Features

	Ethernet
Connector	Shielded female RJ45
Auto crossover	Yes
Maximum cable length	100 m
Cable Type	UTP or ScTP, category 5
Transmission rate	10/100 Mbps
Physical layer	10BASE-T/100BASE-TX
Network layer	IP (Internet Protocol)
Transport layer	TCP (Transmission Control Protocol) UDP (User Datagram Protocol)
Isolation **Ethernet interface for logic** **Ethernet interface for protective earth** ⏚	 1500 Vac / 1 minute 1500 Vac / 1 minute
Factory settings **IP address** **Subnet mask** **Gateway address**	 192.168.15.1 255.255.255.0 192.168.15.253

Table 6: Ethernet Interface Features

5. Installation

ATTENTION

Products with broken warranty seal are not covered in warranty.

CAUTION

The device is sensitive to static electricity (ESD). Always touch in a metallic grounded object before handling it.

DANGER

Connect Series can operate with voltage up to 250 Vac. Special care must be taken during the installation, which should only be done by qualified technical personnel. Do not touch on the wiring field when in operation.

5.1. Electrical Installation

5.1.1. Standard Installation

The figure below shows the GW700 connection diagram using an external power supply connected to the POWER connector and the Ethernet interface connected directly to an Ethernet network.

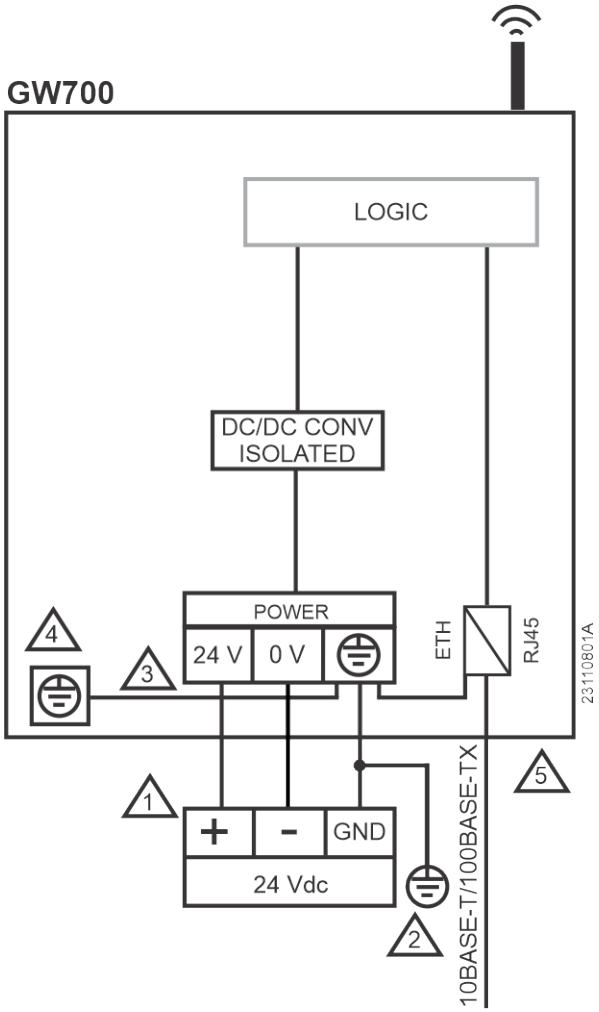

Figure 1: Diagrama de Instalação Convencional

Diagram Notes:

1. The external power supply is connected to the 24V (terminal 1) and 0V (terminal 2) terminals of the POWER connector. This connection must be made using the power connector supplied with the GW700.
2. The ground of the external power supply is connected to the terminal (ground terminal 1) of the POWER connector and must be connected to the external ground and also to the GND of the external power supply. This connection must be made using the power connector supplied with the GW700.
3. The ground terminal of the POWER connector (terminal 1) and the ground screw are connected internally on the GW700.
4. If grounding is done via the ground screw, the ground terminal of the POWER connector must not be used. Similarly, if the ground terminal of the POWER connector (terminal 1) is connected to earth ground, as shown in the diagram in the figure above, the ground screw must not be connected.
5. 10BASE-T/100BASE-TX standard interface.

6. Configuration

The GW700 provides a web page for configuration. It can be accessed via the device's IP address. When accessed, the page displays two tabs: one for device information and the other for device management. The initial tab (information tab) shows relevant device data such as model, IP address, frequency plan, status, etc. The web page can be displayed in two languages: English and Portuguese. To change the language, simply click on the options shown in the top right-hand corner of the screen.

Figure 2: Information Tab of the System Web Page

The management tab has three sections: Firmware Update, Ethernet Configuration and LoRa Configuration. To configure the device, you have to go through an authentication step. In all sections, the default user and password are *"admin"*. The user and password can be changed by clicking on the *"Change password"* button in the bottom right-hand corner of the login screen.

ATTENTION

The system does not allow user and password recovery.

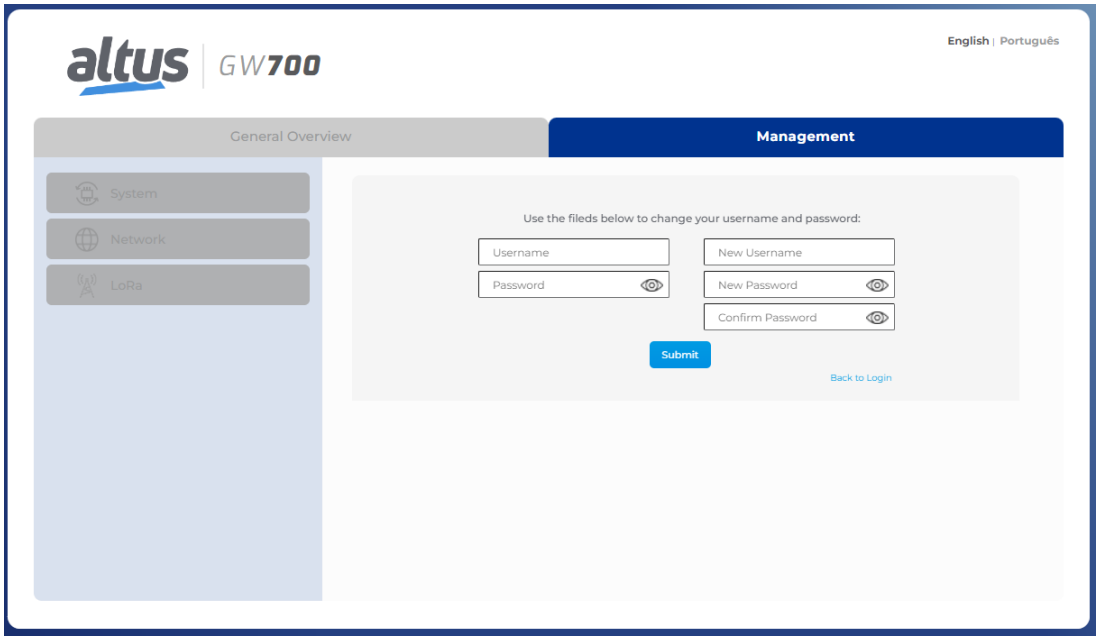

Figure 3: User and Password Configuration

6.1. System Section

To update the gateway's firmware, access the *"System"* section, select the binary file by clicking the *"Choose file"* button, and load it onto the device using the *"Start Update"* button. If an invalid file is selected, the page will prevent the user from uploading it to the gateway.

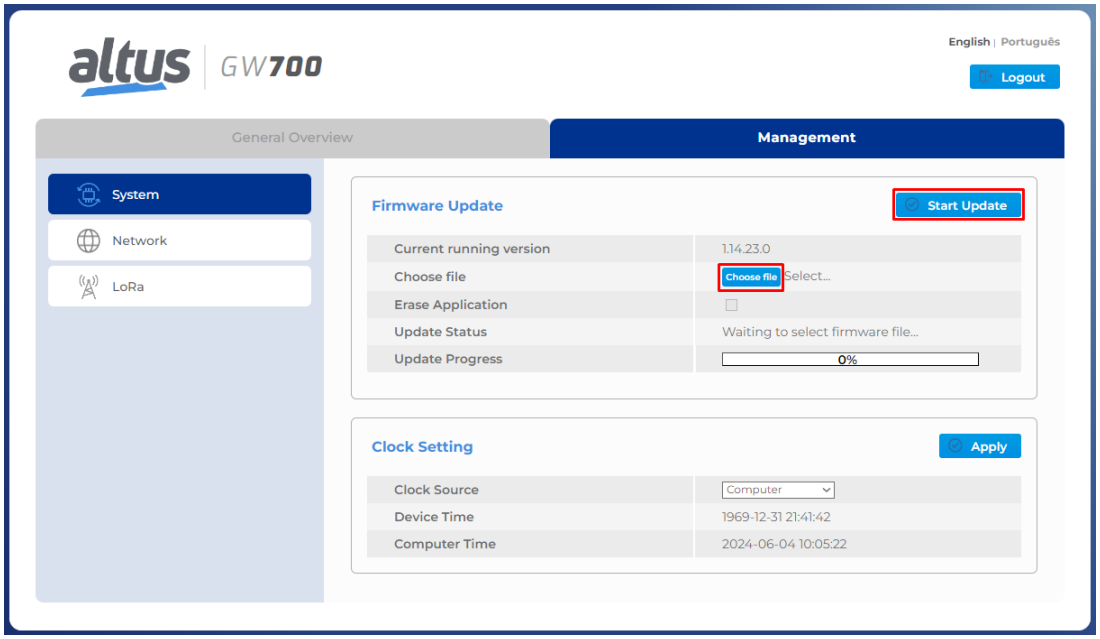

Figure 4: Firmware Update Section

6.1.1. Clock Setting

On the System Web Page, it is possible to adjust the gateway's clock, which is found in the *System* section of the Management tab. The date and time format follows the ISO 8601 standard for date and time sampling (YYYY/MM/DD hh:mm:ss), as shown in the image below:

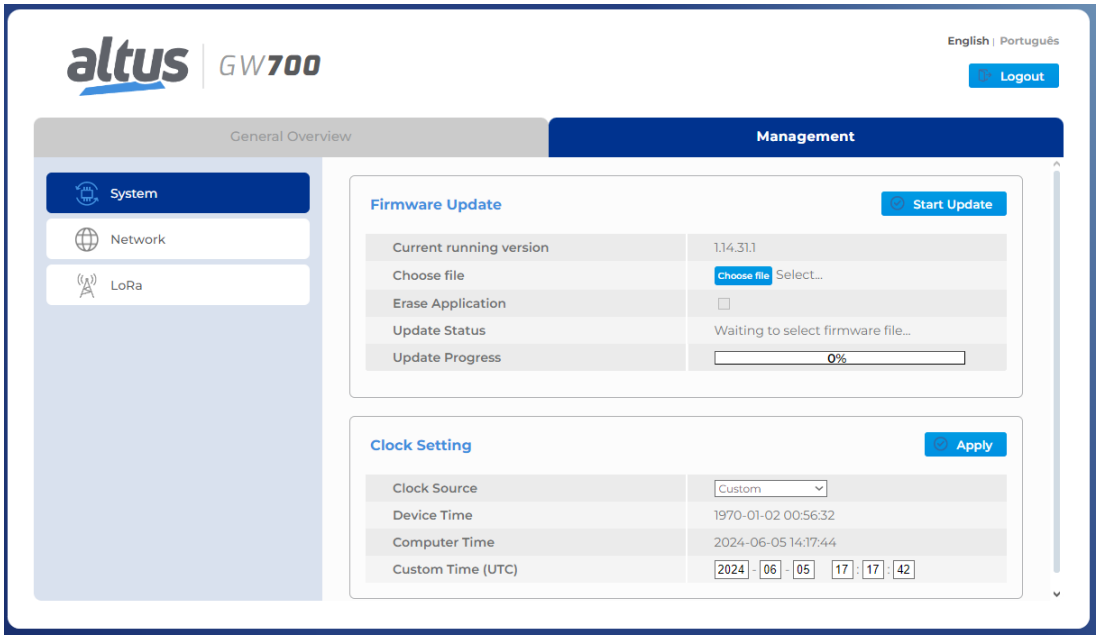

Figure 5: Clock Setting

This feature has two modes for adjusting the device's time, which can be selected in the item "Clock Source", providing the user with two options for synchronizing the clock.

6.2. Network Section

To configure the device's IP, go to the *"Network"* section and click on the *"NET1"* button. From there you can edit the fields. The section allows you to configure the IPv4 address, netmask, and gateway fields.

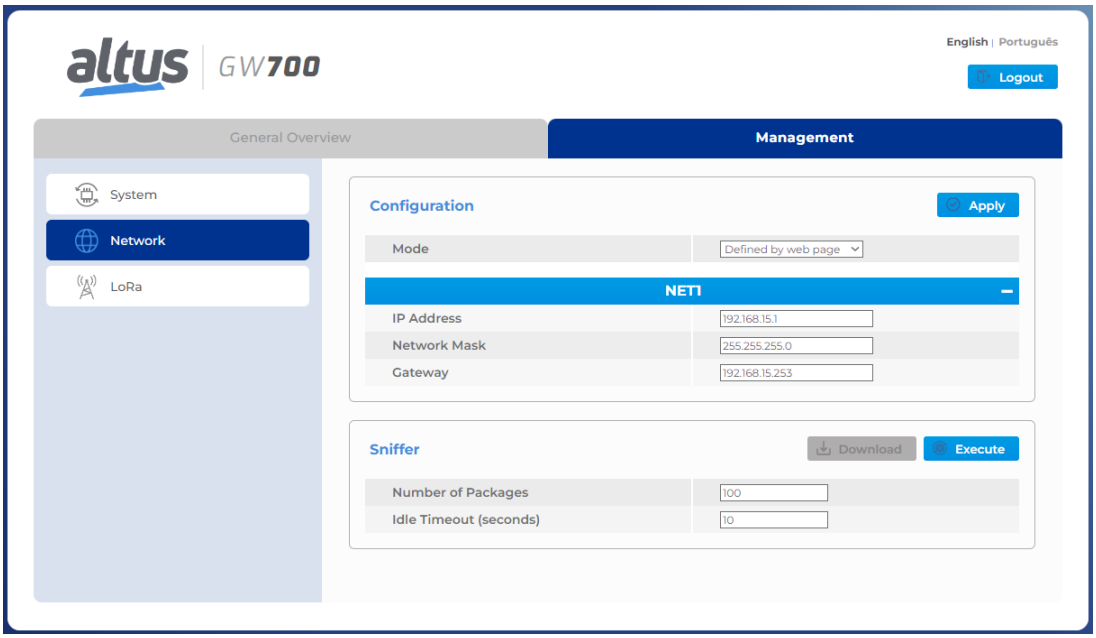

Figure 6: Network Section

6.2.1. Network Sniffer

The network sniffer, shown in the figure below, can be used to observe traffic on physical interfaces, except for USB devices such as modems and wifi adapters. It has two basic settings:

Number of Packets: This is the number of packets you want to capture. The configured value of this parameter must be within the range of 100 to 25000 packets;

Idle Timeout (seconds): If there is no packet traffic on the interface after this configured timeout, the Sniffer execution is terminated. It can be configured with values between 1 and 3600 seconds.

Using the *Interfaces* table, you can select which interfaces you want the Sniffer to run on, i.e., perform network analysis. You can select all available interfaces and run them on all simultaneously. For disabled interfaces, it is not possible to run Sniffer. If the selected option is disabled, an error will be displayed in the browser.

Only a few moments after the screen opens will the *Execute* button, which starts Sniffer's execution, become available. The *Download* button will only be unlocked if there is a Sniffer related file available for download. If the Sniffer has never been run or the file is deleted, the button will not be available.

When running the Network Sniffer, the page will disable the edit fields, the *Download* button will be locked, and the *Execute* button will become the *Stop* button, as shown in the figure below.

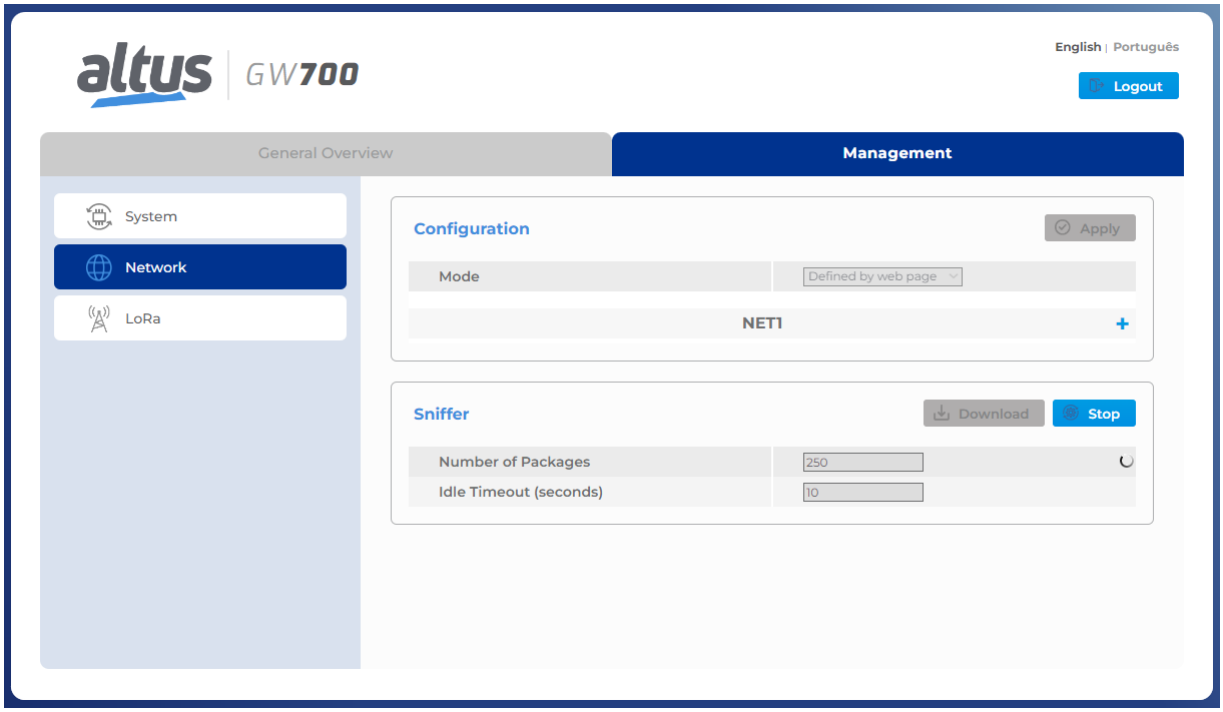

Figure 7: Network Sniffer Running

The *Stop* button can be used to end the sniffer execution at any time after it has been started.

For each of the interfaces on which Sniffer runs, it generates a **.pcap** file. These files are named according to the name of the gateway and the interface that was analyzed, for example, **GW700_NET1.pcap**. These files are found inside a **.zip** file, also named according to the name of the gateway, for example, **GW700_capture.zip**.

At the end of the sniffer execution, a message is displayed asking whether or not to automatically download the generated files. The downloaded file is always in the **.zip** extension, which groups the other files.

If any problems occur related to insufficient memory due to the generation of sniffer files, it will be indicated to the user. It is recommended to try running the analyzer again with a smaller *Number of Packets* configuration.

The network sniffer can terminate its execution for three reasons: insufficient memory, idle time limit of interfaces exceeded, and manual cancellation.

6.3. LoRa Section

To configure the device's LoRa, you need to access the *LoRa* section. This section configures the two main parameters related to LoRa communication that pertain to the LoRa Gateway. The first is the Gateway's communication address protocol with the LoRaWAN server.

At the top of the page, in the *Communication Protocol* section, there is a checkbox for selecting the communication protocol which contains two options, UDP and MQTT. The default protocol is UDP, which is used, for example, in The Things Network's LoRaWAN server services, while the MQTT protocol is used by the ChirpStack private servers. The Things Network (or TTN) is a collaborative ecosystem (IoT) that uses LoRaWAN. Its technology is used as a network server for the Gateway. TTN uses the UDP protocol to establish communication. In addition to TTN, ChirpStack is an IoT solution that provides private network server technology. One of its components is the ChirpStack Gateway Bridge, which is a service responsible for converting the protocols of the so-called *"LoRa Packet Forwarders"* into a data standard common to the ChirpStack Network Server. The ChirpStack Gateway Bridge component communicates with Gateway devices using the MQTT protocol.

Below, you can enter the address of the server with which the device is communicating. By default, it is configured as *"nam1.cloud.thethings.network"*, in this field you must enter the IP address of the server used.

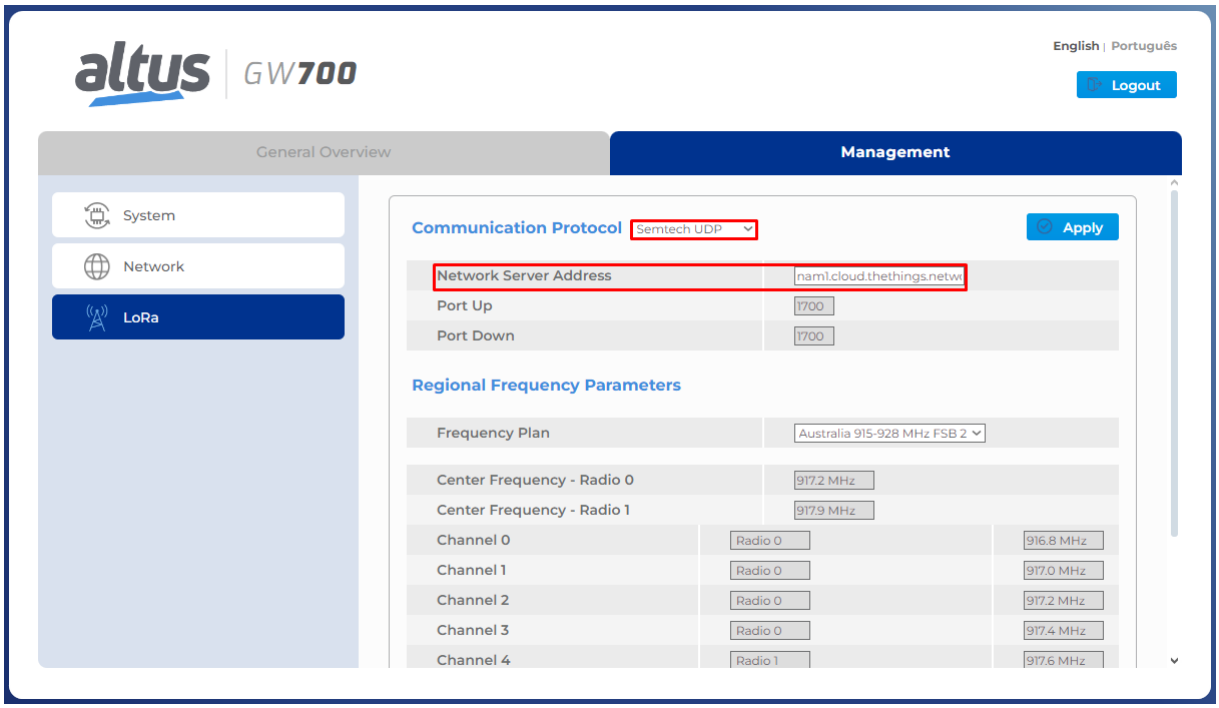

Figure 8: LoRa Section

The second configuration parameter relates to the frequency bands used for LoRa communication between the Gateway and the LoRa device (also known as END NODES). This configuration is performed through the *Regional Frequency Parameters* section, where the user chooses the frequency plan and communication sub-band from those listed.

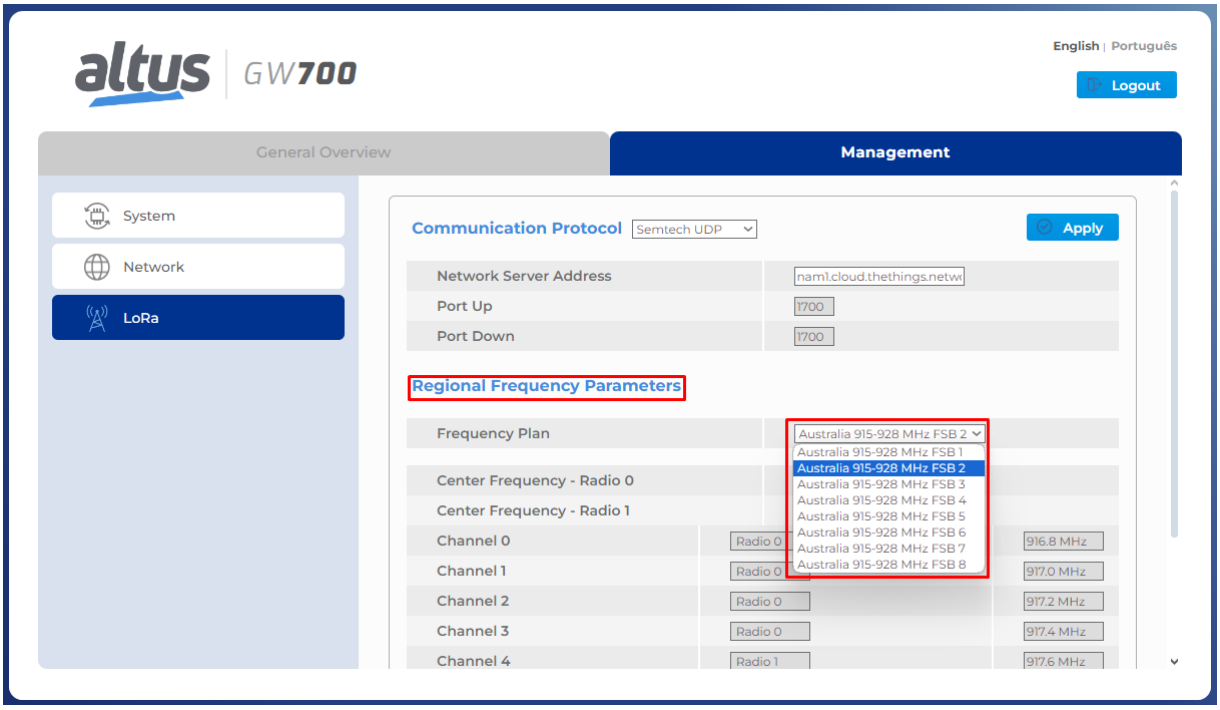

Figure 9: LoRa - Regional Frequency Parameters

Once the communication protocol, the server address and the frequency plan have been defined, the settings can be saved by clicking on the *Apply* button. Once configured and applied, the new radio frequency parameters are updated and can be viewed below on the same page, as shown in the figure below.

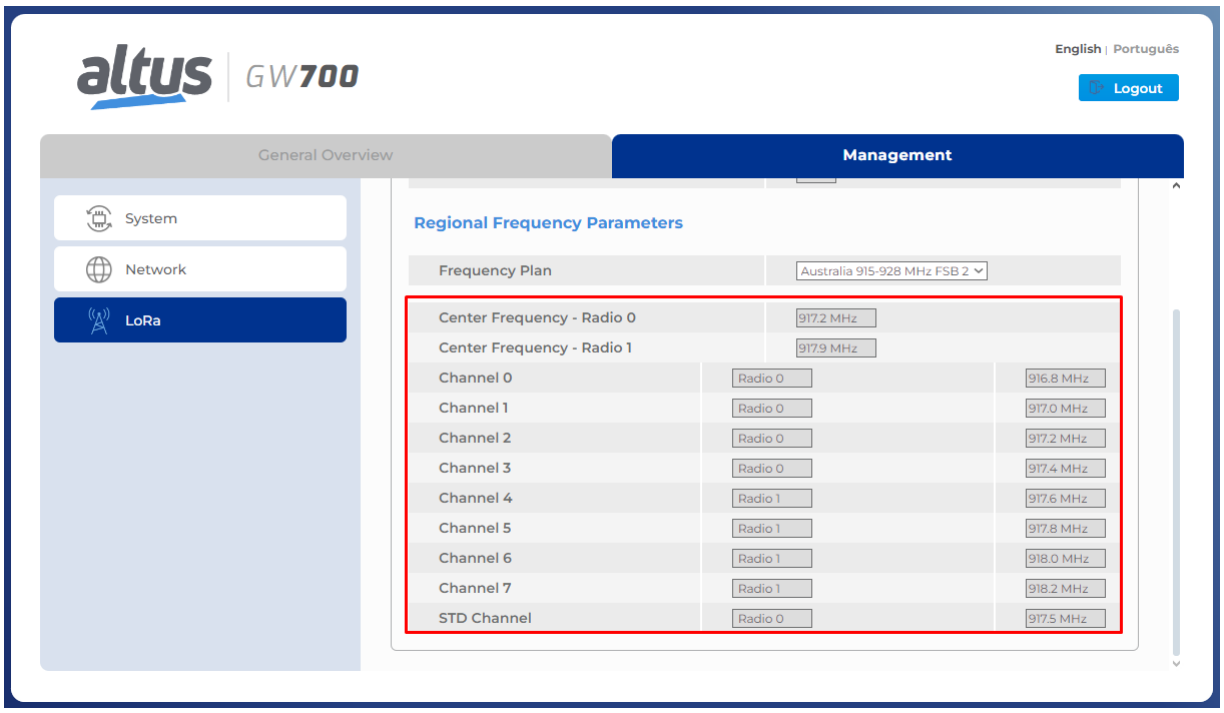

Figure 10: Radio Settings Applied

7. Maintenance

7.1. LED Diagnostics

The GW700 has a power LED (PWR). The following table shows the meaning of each state and its description:

PWR	Description	Causes	Priority
Off	Not used	No power supply or Hardware problem	-
On	Device is powered	-	-

Table 7: Description of the Diagnostic LEDs States

Note:
The *DG* and *LoRa* LEDs have no functionality implemented.

8. Manuals

For further technical details, configuration, installation and programming, the table below should be consulted.

The table below is only a guide of some relevant documents that can be useful during the use, maintenance, and programming of this product.

Code	Description	Language
CE117100	NL717 Technical Characteristics	English
CT117100	Características Técnicas NL717	Portuguese

Table 8: Related Documents