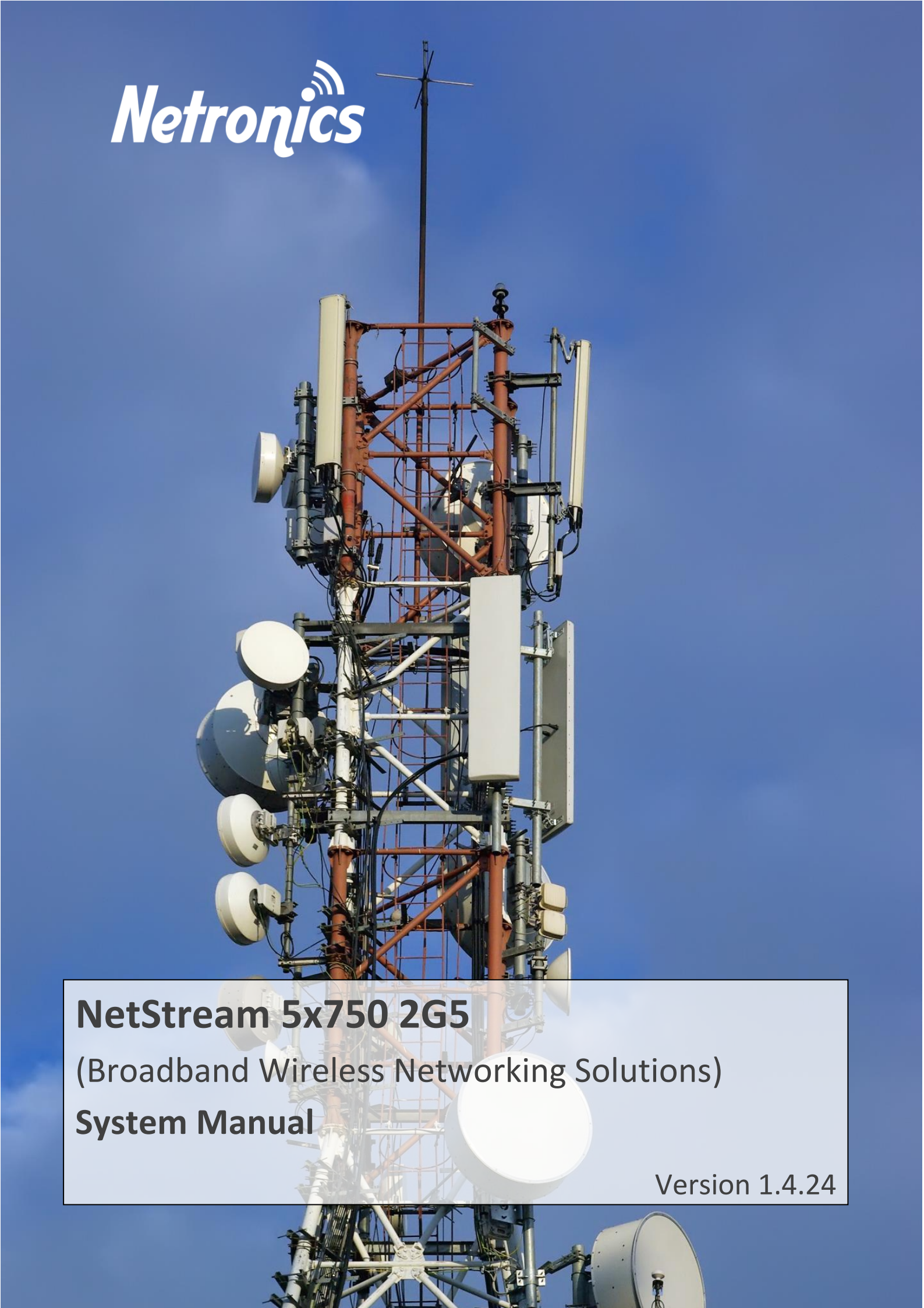


Netronics

NetStream 5x750 2G5

(Broadband Wireless Networking Solutions)

System Manual

Version 1.4.24

Table of Contents

1.Introduction

1.1 Document Scope

This document describes how to configure and manage the Netronics NetStream 5x750 2G5 Outdoor Units (ODUs). It also describes the Wireless E model, concepts of operation, a technology overview, and troubleshooting, as detailed in the following main sections:

•

- Connecting a Laptop to the ODU
- Aligning the Antenna and Starting/Stopping Services
- Viewing Devices & Link Status
- Configuring the Air Interface Parameters
- Configuring ODU Management Parameters
- Configuring Service Parameters

1.2 Revision History

	Date	Document Revision	SW Release	Revision details
1.	Mar. 2024	3.1	6.0.15	First release

1.3 What's New in this release

N/A – first release

1.4 Product Family Overview

The Netronics NetStream 5x750 2G5 Family delivers up to 2.5Gbps (depending on the regulation) in a point-to-point architecture and is the ideal choice for enterprise connectivity and for backhaul.

The Netronics NetStream 5x750 2G5 family includes the following models:

NETRONICS NetStream 5x750 2G5 Family Model Comparisons

Model Name	PN	Max Throughput	Form Factor
ODU NetStream 5x750 2G5D	NCS-NS-5x750-2G5D	2.5Gbps (universal), 1.2Gbps (FCC)	Connectorized
ODU NetStream 5x750 2G5A	NCS-NS-5x750-2G5A	2.5Gbps (universal), 1.2Gbps (FCC)	Integrated

Some options and models may not be available for your regulatory environment.

1.5 Technology Overview

1.5.1 Higher Capacity - Over Longer Distances

Netronics NetStream 5x750 2G5 family products leverage the cutting-edge 802.11ax technology, building on the techniques of the market proven Netronics NetStream 5x750 2G5 PtP family to push performance to a new level.

With the ability to squeeze more bits per frequency channel and uniquely support channels of up to 160MHz and up to 4096QAM modulation, Netronics NetStream 5x750 2G5 offers greater capacity and range than any other unlicensed PtP solution.

1.5.2 AIR Interface Mitigation Techniques

Netronics NetStream 5x750 2G5 employs multiple Air interface mitigation techniques:

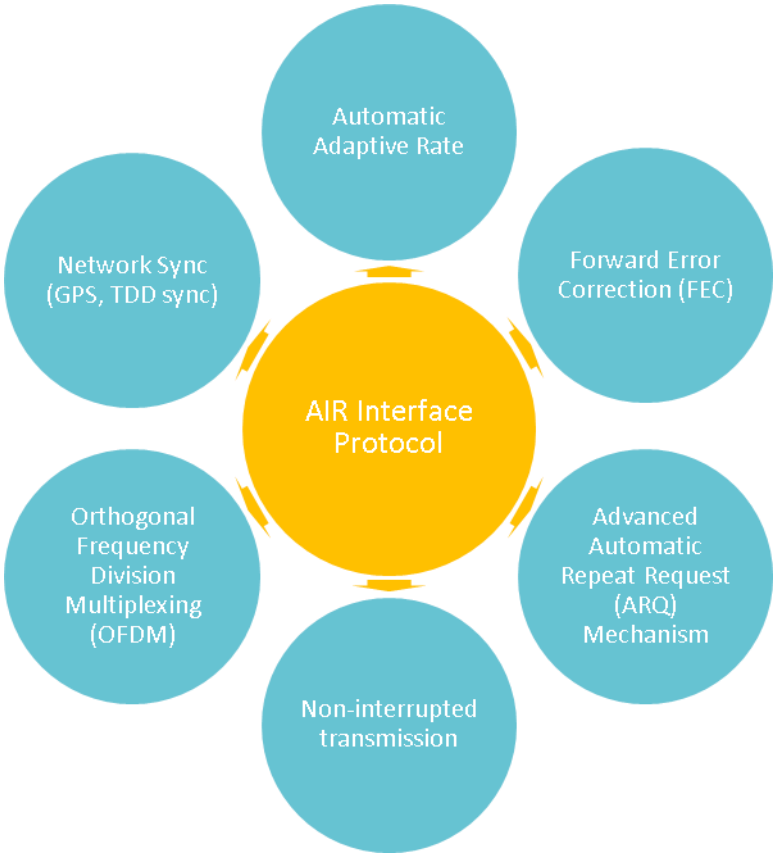


Figure 1: Multiple Air Interface Mitigation Techniques

Orthogonal Frequency Division Multiplexing (OFDM)

Orthogonal Frequency Division Multiplexing, or OFDM, is a modulation technique for effective transmission of large amounts of digital data over a radio link. It is characterized by its low overhead, low latency, and high resiliency to interference.

Selected by standards organizations and leading telecommunications providers, OFDM is the technology of choice for terrestrial radio communications that require high efficiency in difficult environments.

Based on the concept of redundant transmission, OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the

receiver.

By replicating the content signal using multiple narrowband sub-carriers to repeat transmissions over time, OFDM works to ensure that complete content arrives at the transmission destination.

This technique is especially effective for protecting against the effects of multipath fading deriving from the cancellation of carriers under heavy interference conditions.

When a system employing OFDM encounters RF interference, it recovers the affected signal from duplicate carriers that were not affected by the interference.

Based on these considerations, NETRONICS selected OFDM as the core modulation technique for all its radio products.

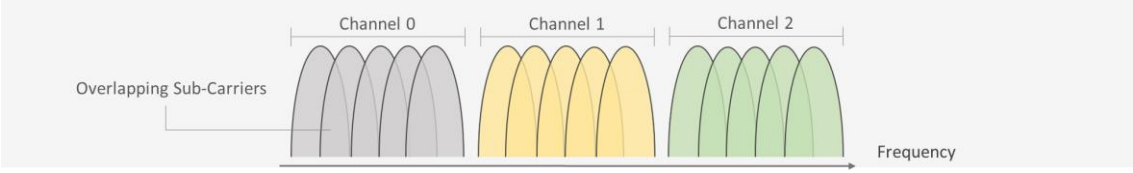


Figure 2:Orthogonal Frequency Division Multiplexing (OFDM)

Automatic Adaptive Rate - BPSK to 4096QAM

Automatic Adaptive Rate works under the NETRONICS proprietary algorithm, adjusting the Modulation and Coding Scheme, and checking potential MCS without affecting the current level of service.

Netronics NetStream 5x750 2G5 product family supports the following modulation schemes: BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM, 4096QAM with the following error correction rate indexes: 1/2, 2/3, 3/4, 5/6.

The automatic adaptive rate maximizes ethernet throughput while ensuring a minimum Error Rate.

The automatic adaptive rate allows enhanced robustness and better performance under interference.

NETRONICS products perform independent automatic adaptive rate at each side of the link, in both the uplink and downlink.

Advanced Automatic Repeat Request (ARQ)

Advanced ARQ error-handling at the physical layer, instead of higher levels, has much lower overhead than other ARQ methods, and in many cases repeat transmission is initiated without having to wait for a request from the Client ODU, minimizing either latency or error rate to optimize performance for the type of services being delivered.

If there are unrecoverable errors in a packet, it requests retransmission automatically. NETRONICS systems ensure error-free service using a proprietary quick ARQ mechanism with super-fast retransmission of errant data.

Advanced Forward Error Correction (FEC)

The Advanced FEC technique uses very little overhead, and algorithms specifically designed for the varying conditions of license-exempt frequency bands. The sender adds redundant data, enabling the receiver to detect and correct errors upon reception. Retransmissions are avoided, thus avoiding the cost of higher bandwidth requirements on average.

Non-Interrupted Transmission

The non-Interrupted transmission technique keeps transmissions regardless of changing conditions in the channel, leaving the on-the-fly corrections to operate while the communication flows remain stable and robust.

Adjustable UL/DL Ratio

Netronics NetStream 5x750 2G5 family links support an adjustable DL/UL ratio between 25%/75% to 75%/25%. This capability allowed the user to optimize the transmission time allocation to the direction that contains the most data.

Adaptive MIMO/Diversity

Based on RSS levels from both paths of the dual-polarization antenna, ODUs can decide to use either MIMO or Diversity.

In most situations, MIMO represents the best option in terms of performance. However, certain conditions can affect the link, forcing the use of Diversity, such as a nearby water mirror (a lake or a bay with dense vegetation), and metal structures.

MIMO - Multiple Input Multiple Output

Multiple Input Multiple Output, or MIMO, is based on using multiple antennas per side, in our case, two antennas with opposite linear polarization. Throughput can be increased using different streams per polarity, doubling capacity over the same channel bandwidth. MIMO needs good isolation (rejection) between both polarities and a similar path performance for all the antennas. MIMO increases spectral efficiency without increasing transmission power and bandwidth. We use MIMO mode, particularly for its Rate Gain.

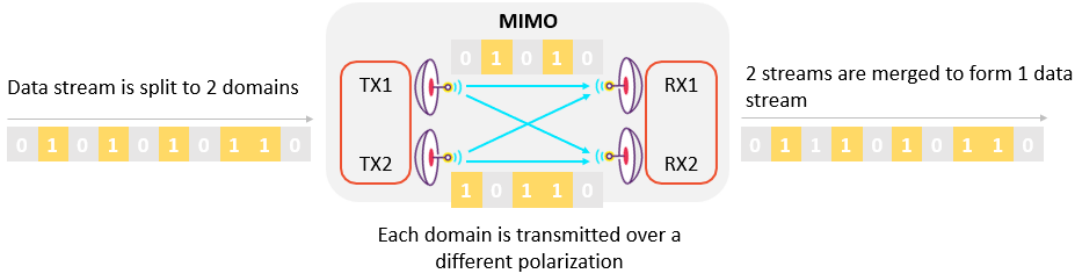


Figure 3: Multiple Input Multiple Output (MIMO)

Diversity

Diversity Mode uses two antennas to improve the quality and reliability of the link. In some scenarios, the signal is reflected along multiple paths. Each such “bounce” can introduce phase shifts, time delays, attenuations and even distortions that can destructively interfere with one another at the receiver. Antenna diversity is especially effective for mitigating multi-path situations because multiple antennas afford a receiver several parts of the same signal. Each antenna will be exposed to a different interference, thus, if one antenna is undergoing a deep fade, it is likely that another has enough signal, and collectively, such a system can provide a better link. Antenna diversity requires antenna separation, which is possible using a dual-polarization antenna or two spatially separated antennas.

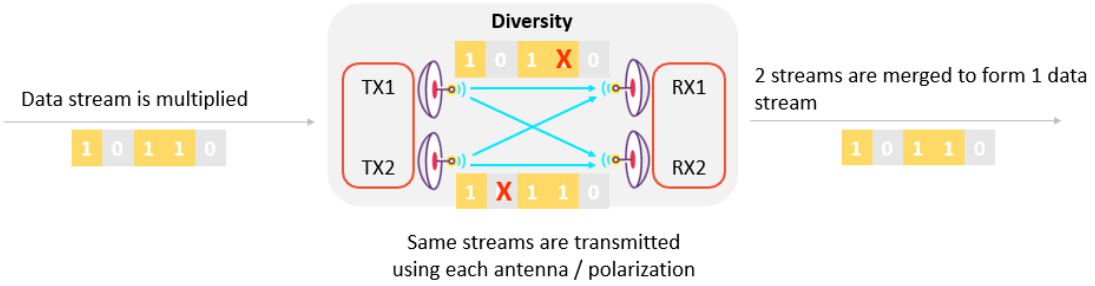


Figure 4: Diversity

1.5.3 Configurable/Adaptive Channel Bandwidth

You can configure the channel bandwidth that will be employed in the link. Supported CBWs are as follows (depending on regulation):

- 20 MHz
- 40 MHz
- 80 MHz
- 160 MHz

With the adaptive channel bandwidth feature, links that are configured to a higher channel bandwidth will automatically transfer to a lower channel bandwidth in case of interference, to optimize the throughput and provide the best service.

1.5.4 Security and Encryption

NETRONICS products conform to high-security standards both in securing access to the management interface of the ODUs and in encrypting the data transmitted over the air interface.

AIR Interface Security

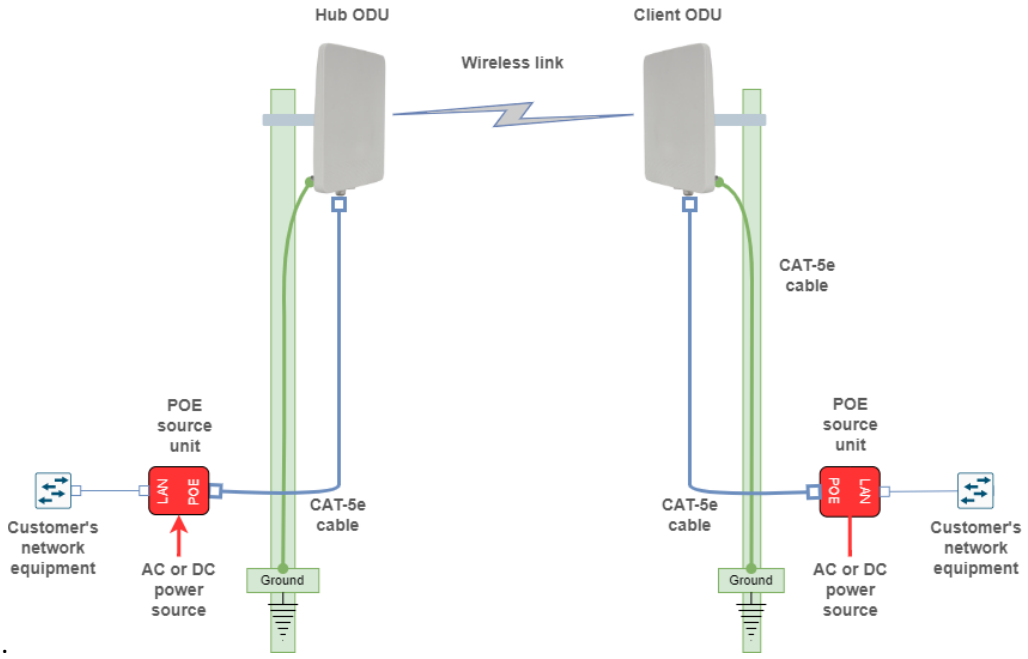
The Netronics NetStream 5x750 2G5 platform provides a proprietary air interface that is not amenable to scanning and penetration attacks from Wi-Fi devices. Netronics NetStream 5x750 2G5 family ODUs offer standard AES 256-bit over-the-air encryption for transmitted data. The encryption is based on a user-defined link password.

1.5.5 Low Sidelobes Integrated Antenna

Netronics NetStream 5x750 2G5 family Integrated products include a directional antenna with an exceptionally high side-lobe rejection level (> 22dB). This antenna provides excellent isolation in noisy environments while keeping the ODU compact and easy to install.

1.6 Mode of Operation

Netronics NetStream 5x750 2G5 is a Point to Point (PtP) Outdoor Unit (ODU). The PtP ODUs establish a wireless radio link between them to transmit high-capacity



data.

Figure 5: PtP Connection Scheme

Note

For simplicity, Lightning Protection Units (LPUs) are not shown in the following figure, but are recommended.

1.6.1 Hub / Client

Any Netronics NetStream 5x750 2G5 ODU can be configured either as Hub or as Client.

The method of operation of the Netronics NetStream 5x750 2G5 link requires that one side of the link would be designated as the Hub - which will transmit a beacon, and the other side of the link would be designated as a client which will scan for the beacon and connect to the Hub.

Due to this mode of operation, configuration of the link and service are stored in the Hub, and are transferred to the Client upon link establishment.

Note

NETRONICS recommends that the ODU close to the network operator's main network side will be configured as the Hub, while the ODU at the remote side (closer to the end customer) be configured as Client. This way, if the link between the Hub and Client is lost, you keep the connection to the Hub.

The differences between Hub and Client are summarized in the following table:

Overview of the Differences between Hub and Client

Hub	Client
Transmits beacon, waiting for Client connection	Searches for beacon and establishes a connection to the Hub
Contains some master settings for both devices	Receives settings from the Hub on link establishment
Identifies its location from GNSS and determines the country and applicable regulation	Receives the country and applicable regulation configuration from the Hub

1.6.2 Link Establishment and Starting Service

ODU Activation and Initial Setup

An ODU comes out of the box configured as a client by default. You can change the ODU configuration between Hub and Client through the Quick Setup wizard).

To establish a link between ODUs, you need to activate the ODU by configuring essential parameters such as link ID, password, and antenna parameters for external ODUs, operating band and channels in the Hub).

Link Establishment Process

High-level process of link establishment:

1. When the Hub ODU boots, if it has been activated (essential parameters configured), it will start transmitting a beacon on configured channel and with the configured link ID.
2. When the Client ODU boots, if it has been activated (essential parameters configured), it will start scanning for a beacon.
3. Once the Client detects a beacon, the Client will attempt to connect to the Hub.
4. If the link ID matches the configured security policy, a link will be established.
5. At this point, both Hub and Client will appear in the UI, as being part of the link, but the Client is not registered yet (no service).
6. You can perform antenna alignment at this stage (the MCS is locked to be constant).
7. Once you want to start the service, register the Client to the Hub using the browser user interface.
8. Once the Client is registered, the link is fully active.

Registered/Deregistered Devices

An active link between the Hub and Client can be in either Registered or Unregistered state. When the hub and client are registered, the service is activated, and full user-data is transferred over the active link. When they are not registered, the link will only allow limited communication between the devices during an active link and will not transfer any user-data.

When a client is registered to a Hub, both devices are locked together and won’t accept a connection to any other device if the link is lost. If they are not registered to each other, each device can create a new link with any other device if the link between them is lost.

1.6.3 Browser User Interface for Configuration and Monitoring

The Netronics NetStream 5x750 2G5 browser user interface allows to configure both Hub and Client settings simultaneously in a side-by-side view. The Hub is always displayed on the left side, while the Client is always displayed on the right side.

While a link between both ODUs is active, you can configure and view the status of both ODUs.

If the link is broken, or if there is a mismatch in the link (Client not registered to the Hub, link password not matching, etc.), you will only be able to configure the device to which you are directly connected (local device).

Local Device

Using a (laptop icon), the browser user interface indicates which ODU is the local device (the ODU whose IP address was entered in the browser).

Some configurations in the browser user interface are only possible for the local device (such as SW upgrade, changing user password). To configure the remote device, connect to that device's IP address directly and perform the required operation.

If the link is lost, you will have a connection to only one side of the link. The other ODU becomes inaccessible. For this reason, take care when modifying the configuration that might cause the link to be lost (such as factory reset).

Link Status Indications

The browser user interface shows the status of the link. The following statuses can appear.

Status Name	Description
Not Activated	The ODU hasn't been activated. Complete the quick setup wizard to configure all the essential parameters.
Searching	The ODU is searching for a link. This can happen either if there was a link and it got disconnected, or if no link was yet established.
Not Registered	A link has been established, but the Client Hasn't been registered to the Hub. The service is not active at this link status.
Active	The link is established and is active. Full service is active over this link.
PW Mismatch	The passwords of the hub and client do not match. The service is not active at this link status.
SW Upgrade Required	A software upgrade is required for the system to function.
Spectrum Scanning	Scanning the radio spectrum to detect an optimal frequency. Service is still active during that time.

Status Name	Description
Regulation Mismatch	The regulation settings of the hub and client do not match. Service is inactive at this link status.

TDD (DL/UL) Ratio

TDD ratio determines which part of the radio frame is allocated for DL transmission and which is allocated for UL transmission. This setting is extremely useful when the data capacity is not symmetrical between the UL and the DL directions.

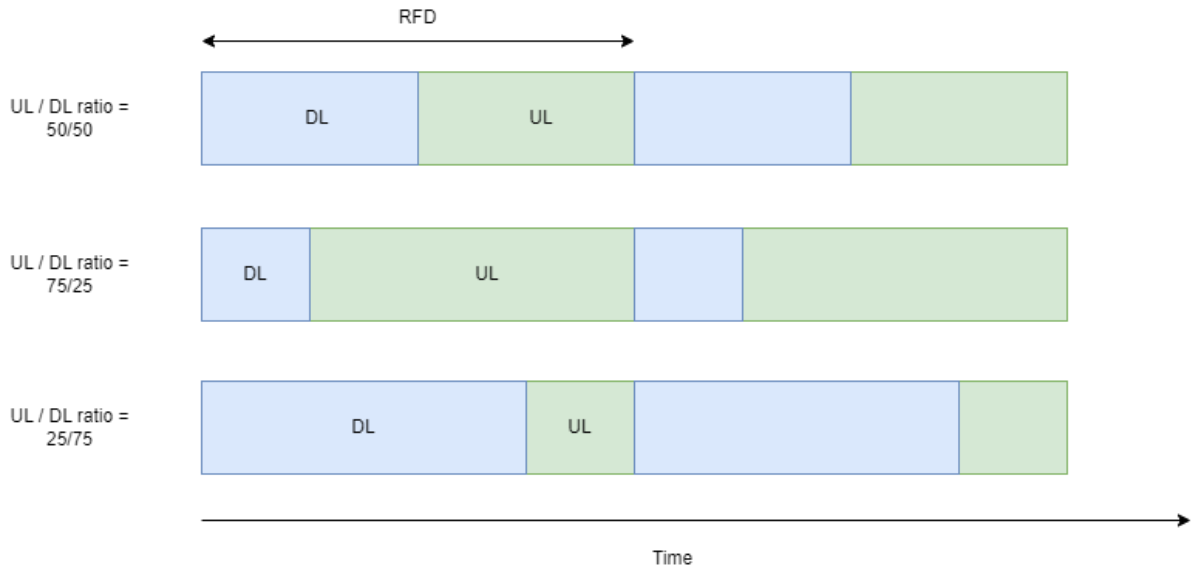


Figure 6: TDD ratio

1.7 Regulation Compliance

1.7.1 Enforcing Regulation Restrictions

Netronics NetStream 5x750 2G5 family of ODUs include a built-in GNSS receiver. The ODUs identify their location from GNSS and determine the country in which they are located and the regulation that applies in that country. Subsequently, a single PN is available for each HW version of the radio, without needing to create multiple PNs (dedicated PN for each regulation). The same radio device can be transferred from one regulation zone to another.

1.7.2 GPS Mode

- When the radio detects a GNSS signal, it will determine the country it is located in and select the applicable regulation.
- User will only be able to select a frequency band that is allowed by the regulation of the detected country.
- When the system could connect to the GNSS Signal, you could see the colored GPS icon on the upper right corner of the WebUI.
- When the GNSS Signal is not reachable, this icon is greyed out.

Figure 7: GNSS Signal acquired

1.7.3 No GPS Mode

If the user wishes to test the device indoors - e.g., inside a warehouse / lab, the device will not detect a GNSS signal. In this case, the device would be in “No GPS” mode, in which the user will be allowed to select the country manually. Once the country is selected, the device will select the allowed regulation for this country, and the available frequencies will adjust to allowed frequency band in this country.

The selected country will be remembered by the device as long as the device doesn’t detect a GNSS signal. Once GNSS signal is detected, the device would update the country to the country detected by GNSS, and would check for regulation mismatch between its previously selected band and the current allowed regulation. This functionality is intended to prevent the device from transmitting in a band forbidden by the local regulation.

The transmission would not be affected in case there is no mismatch between the regulation of the previously selected band and the current detected regulation.

1.8 Management Tools

Currently, the following management tools are enabled:

Tool	Capabilities
EMS - browser UI	• Configure ODU and link parameters. • Monitor ODU and link status. • Inspect the recent events logs. • Perform SW upgrade. • Perform reboot and factory reset.

1.9 Safety and Security

1.9.1 Safety

- Before working on equipment connected to power lines or telecommunication lines, remove jewelry or any other metallic object that may come into contact with energized parts.
- Use extreme care when working at heights.
- All NETRONICS products should be grounded during operation.
- The use of lightning protection is dependent on regulatory and end-user requirements.
- To protect against overexposure to RF energy, all persons should maintain safe distances from radio sources.
  When the system is operational, avoid standing directly in front of the antenna. Strong RF fields are present when the transmitter is on.

1.9.2 Security Recommendations

- Change the default user password and set a new link password
- Use only SNMPv3 for monitoring and disable SNMPv1

2 Connecting a Laptop to the ODU

This section describes how to connect a laptop to an ODU and perform the initial configuration between Hub and Client ODUs using the Quick Setup wizard in the browser user interface.

2.1 Preparing a Laptop

The laptop needs to have the same subnet as the default IP of the ODU. The ODU's default IP address is **10.0.0.120**

Configuration in Windows

Configure the laptop IP address and subnet mask as follows:

1. Control Panel -> Network and Internet -> Network and Sharing Center -> Change Adapter Settings -> click Network Interface Card Name.
2. Properties -> Select Internet Protocol Version 4 (TCP/IPv4) -> Properties -> set the IP address to 10.0.0.x (any other than 120) and Subnet mask to 255.255.255.0.

Configuration in Mac

Configure the laptop IP address and subnet mask as follows:

1. System Settings -> Network -> Select network interface
2. Details -> TCP/IP -> Configure IPv4 -> Select Manually -> set the IP address to 10.0.0.x (any other than 120) and Subnet mask to 255.255.255.0.

2.2 Connecting a Laptop to Netronics NetStream 5x750 2G5 ODUs

1. Connect the PoE (or POE switch) to a power source.
2. Connect an ethernet cable between the laptop and the PoE (or POE switch).
3. Connect an ethernet cable from the POE (or POE switch) to the ODU **PoE IN** socket.

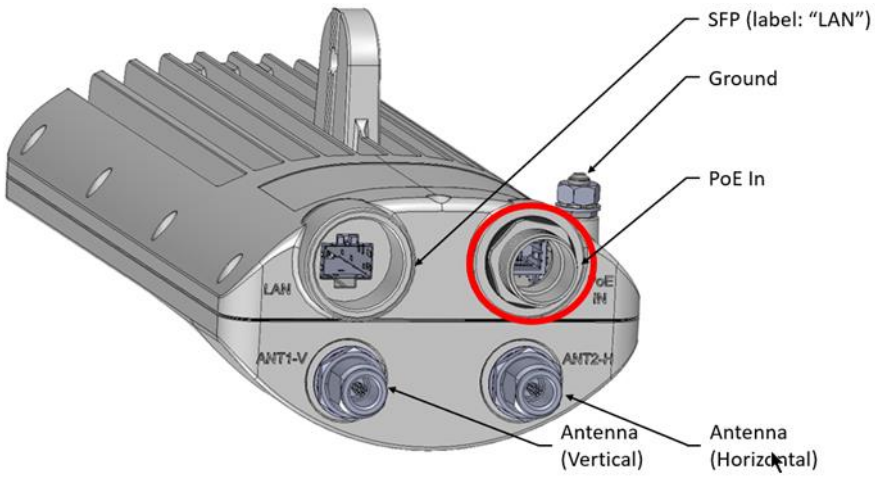


Figure 8: External ODU - POE IN socket

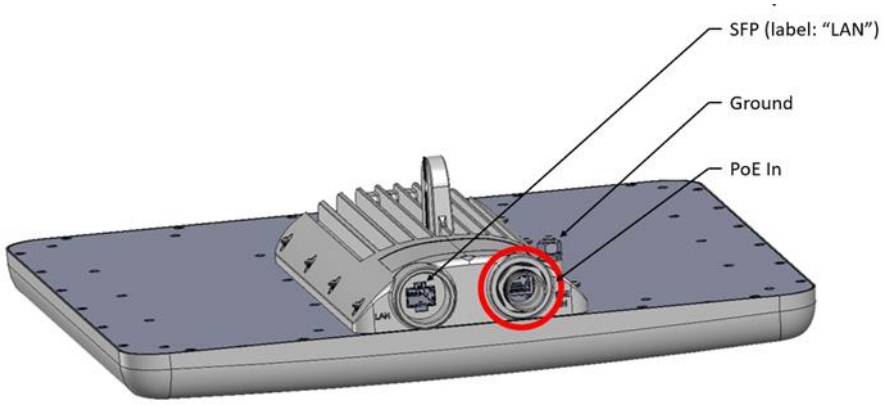


Figure 9: Integrated ODU - POE IN socket

4. In a browser, enter the ODU IP address (default value: 10.0.0.120).
5. In the login page, enter the following default credentials and click **Login**:

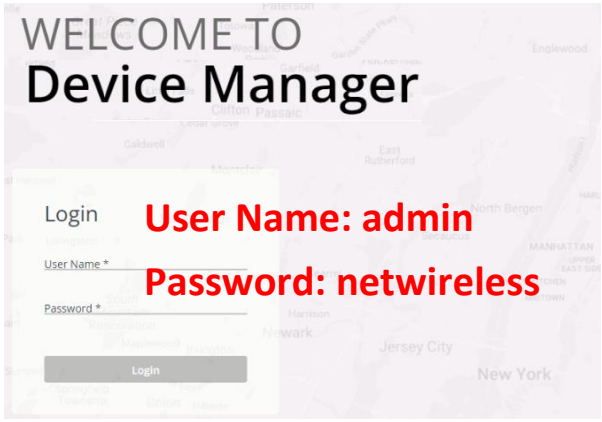


Figure 10: Login

Note

After the first login:

- Run quick setup to configure basic device parameters and activate the device – see Running Quick Setup for ODU Initial Configuration.
- Change the IP address - see
-
-
-
-
-
-
-

-

- Configuring the Management IP.

Change the default user password - see Configuring the Protocols

2.3 Running Quick Setup for ODU Initial Configuration

1. Using a browser, log in to the ODU.
2. If this ODU hasn't yet been activated, the **Quick Setup** wizard starts automatically. Otherwise, the **Home** page appears.
3. If the **Quick Setup** wizard hasn't started, click **Quick Setup.**
   The wizard for configuring the initial device parameters appears:

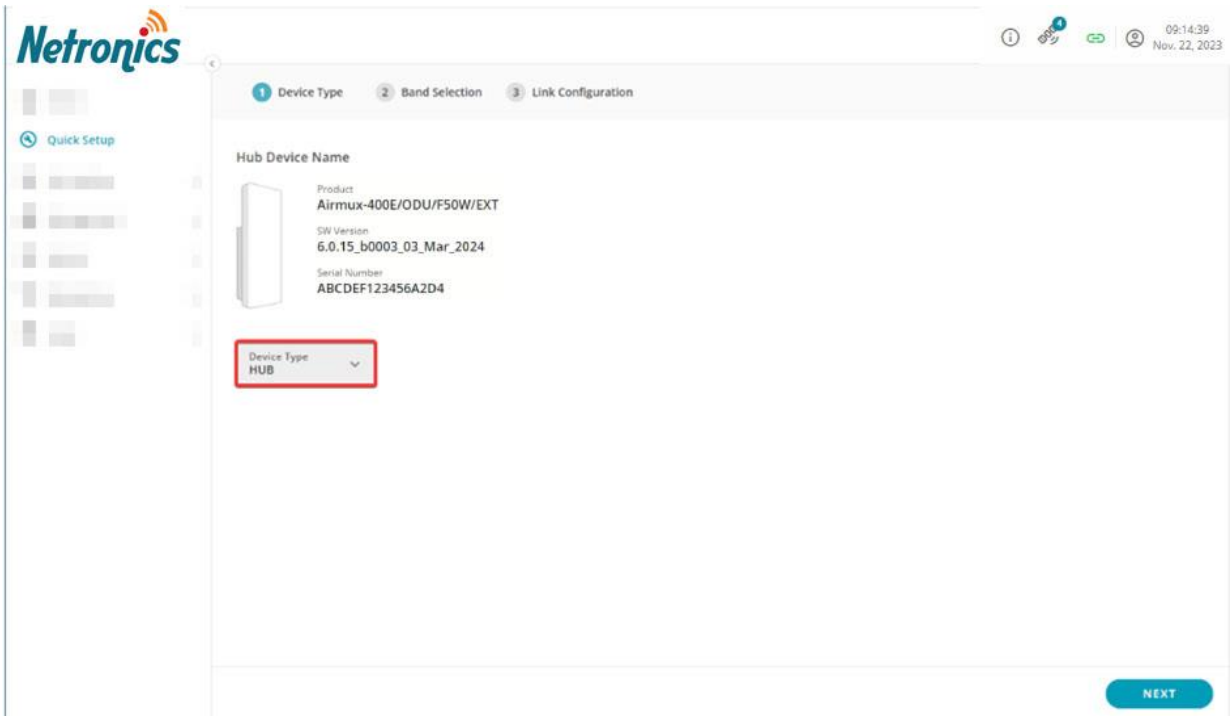


Figure 11: Define the Device Type as Hub or Client

Note

When changing device type, the ODU will perform a reboot.

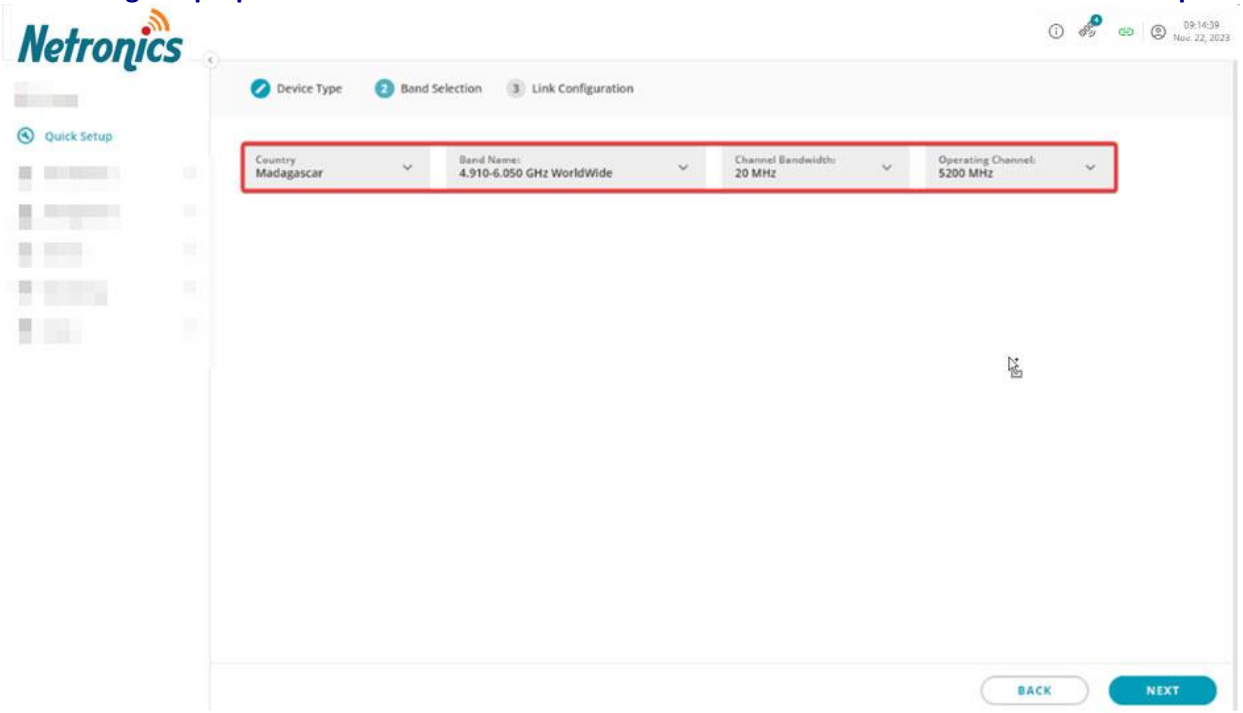


Figure 12: Hub

4. For Hub only: select the required bands.

   For detailed explanation regarding the parameters on this page, see Configuring the Band and Channel:

   - If the ODU has a GNSS/GPS fix, the country is automatically selected by the system.
     If the ODU doesn't have a GNSS/GPS fix, manually select the actual country in which the ODU is installed.

Note

Selection of a different country will result in the link being stopped if the ODU gets a GPS fix and the configured band is not permitted according to the regulation in the detected country.

5. Configure Link Configuration parameters:

For Client:

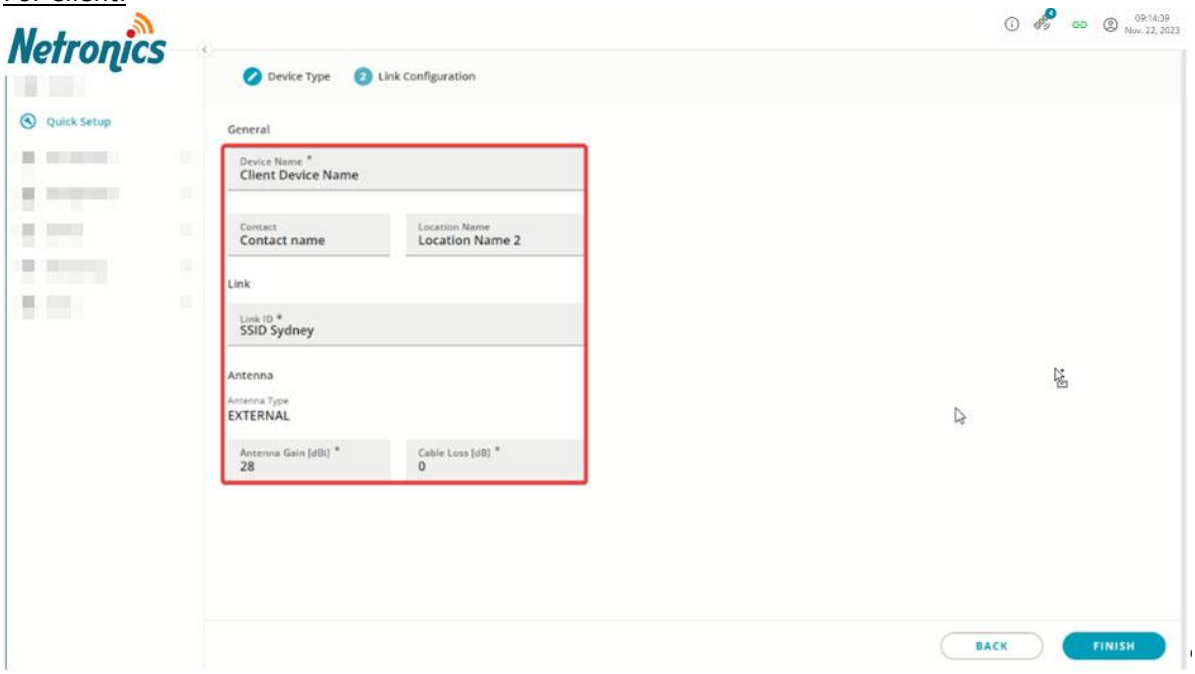


Figure 13: Client Device Name

Parameter	Description	Mandatory
Device Name	See Configuring General ODU Settings.	Yes
Contact	See Configuring General ODU Settings.	No
Location name	See Configuring General ODU Settings.	No
Link ID	See Configuring the Link Security.	Yes
Antenna Gain	See Configuring the Antenna & TX Power.	Yes
Cable loss	See Configuring the Antenna & TX Power.	Yes

For Hub:

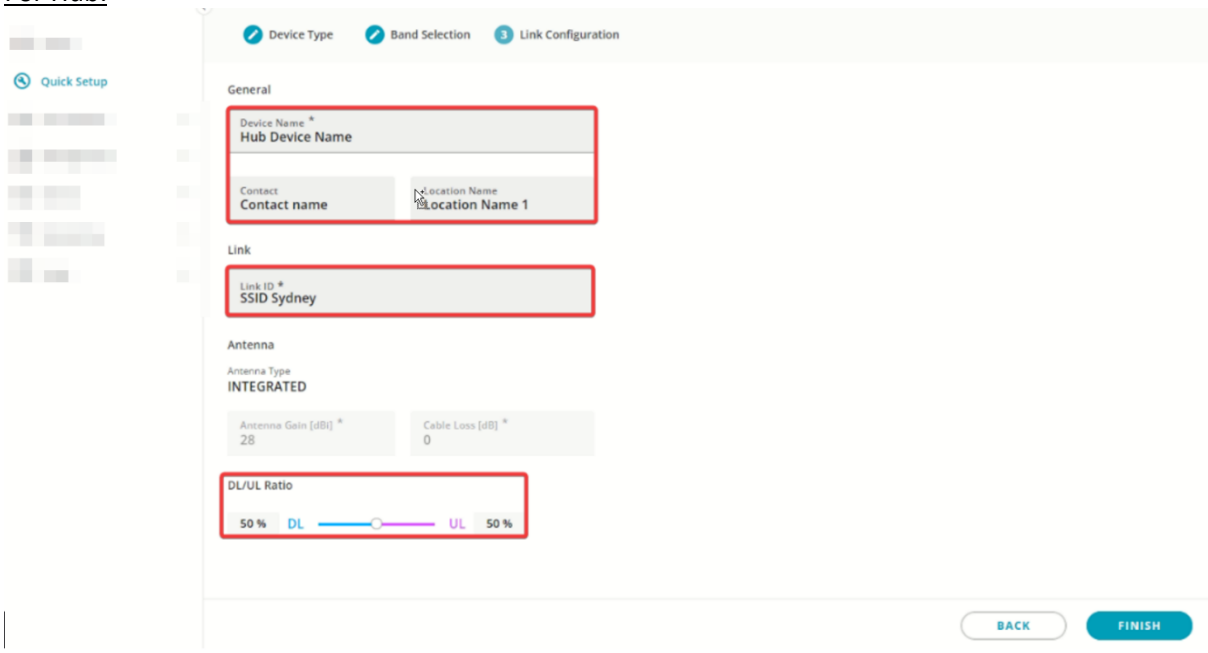


Figure 14: Hub

Parameter	Description	Mandatory
Device Name	See Configuring General ODU Settings.	Yes
Contact	See Configuring General ODU Settings.	No
Location name	See Configuring General ODU Settings.	No
Link ID	See Configuring the Link Security.	Yes
Antenna Gain	See Configuring the Antenna & TX Power.	Yes
Cable loss	See Configuring the Antenna & TX Power.	Yes
DL/UL ratio	See Configuring TDD.	No

After finishing the quick setup, the home page appears.

3 Aligning the Antenna and Starting/Stopping Services

This section describes how to align the antenna between the Hub and Client ODUs.

Aligning the Antenna

Starting and Stopping Service

3.1 Aligning the Antenna

Antenna alignment is performed while the Client is not Registered. In this state, the link MCS and TX power are kept constant, allowing you to evaluate the RSS while adjusting antenna alignment to get the optimal signal
level.

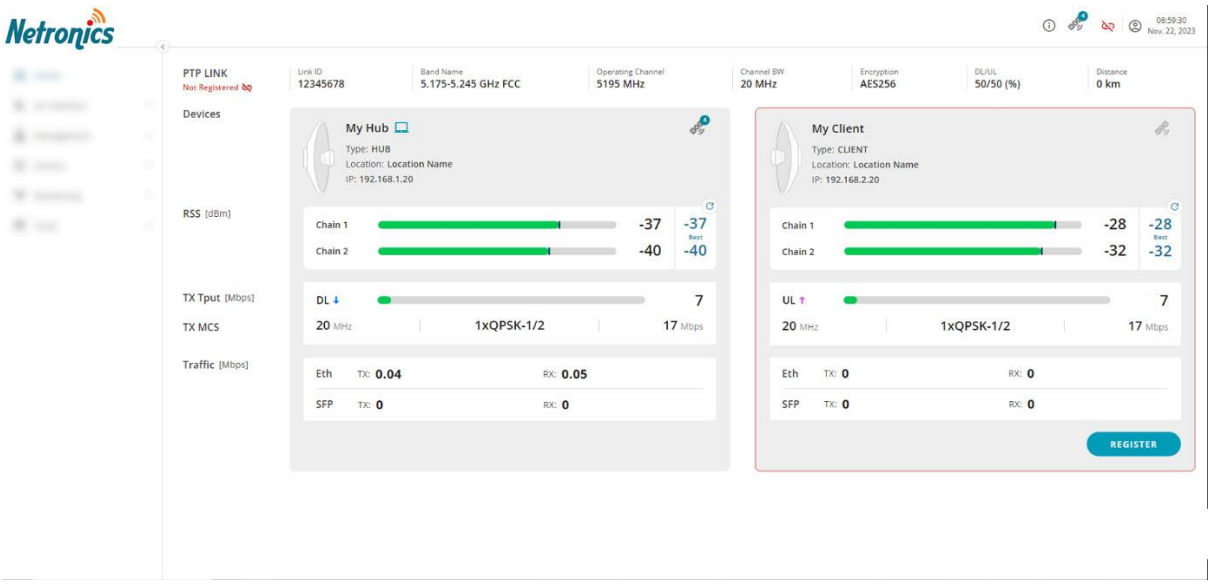


Figure 15: Aligning the Antenna

1. In the browser user interface, if the Home page is not displayed, click **Home**.
2. Start antenna alignment while monitoring the RSS values for both radio units.
3. “Best RSS” is updated each time a new highest RSS value has been recorded, serving as easy-to-use RSS reference point for the alignment process.
4. Continue alignment until highest possible RSS values are achieved.
5. To start the data service between the Hub and the Client, click **Register**.
6. In some cases (depending on TX power and max EIRP allowed by regulation), RSS may drop by several dB as the link reaches highest possible modulation and adjusts TX power.
7. Please refer your link budget calculation in order to validate the achieved RSS of a registered link matches the design prediction.

3.2 Starting and Stopping Service

For a detailed explanation regarding registered/unregistered devices, see Registered/Deregistered Devices.

To stop the service between a Hub/Client pair:

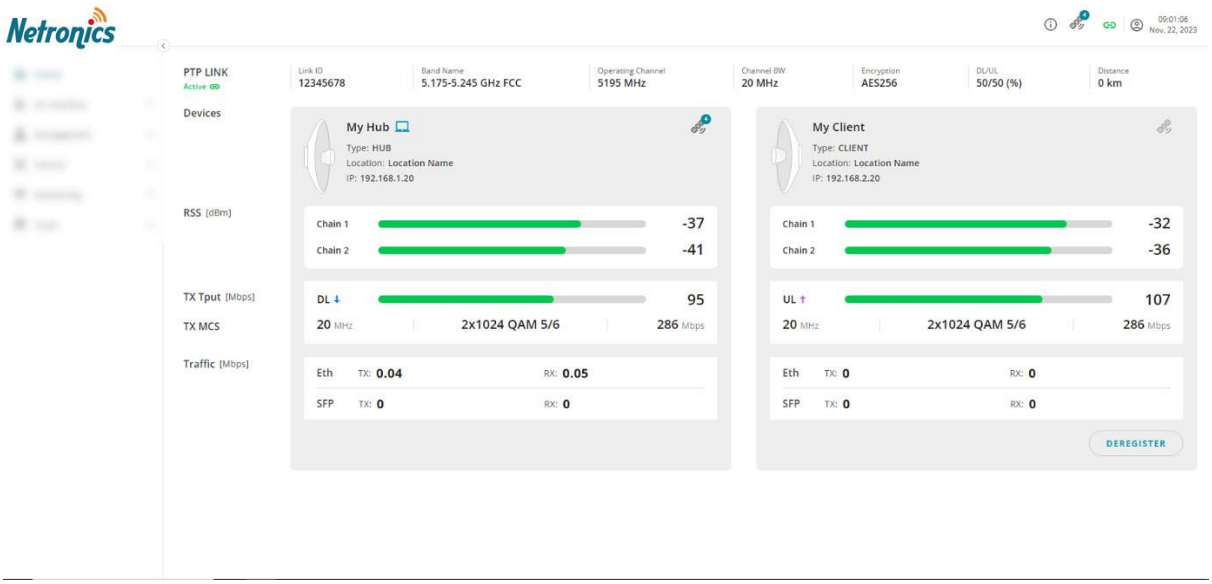


Figure 16: Starting and Stopping Service

1. On the Home page, click **DEREGISTER**.:
2. Click **CONTINUE**.

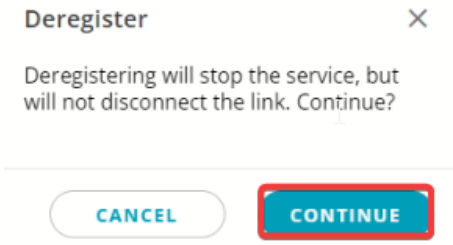


Figure 17: Deregister Client Unit

4 Viewing Devices & Link Status

The home window is the main dashboard of the link and its devices.

In addition to a summary of general Hub/Client information displayed in other pages, the Home page displays various connection and links metrics as described
below:

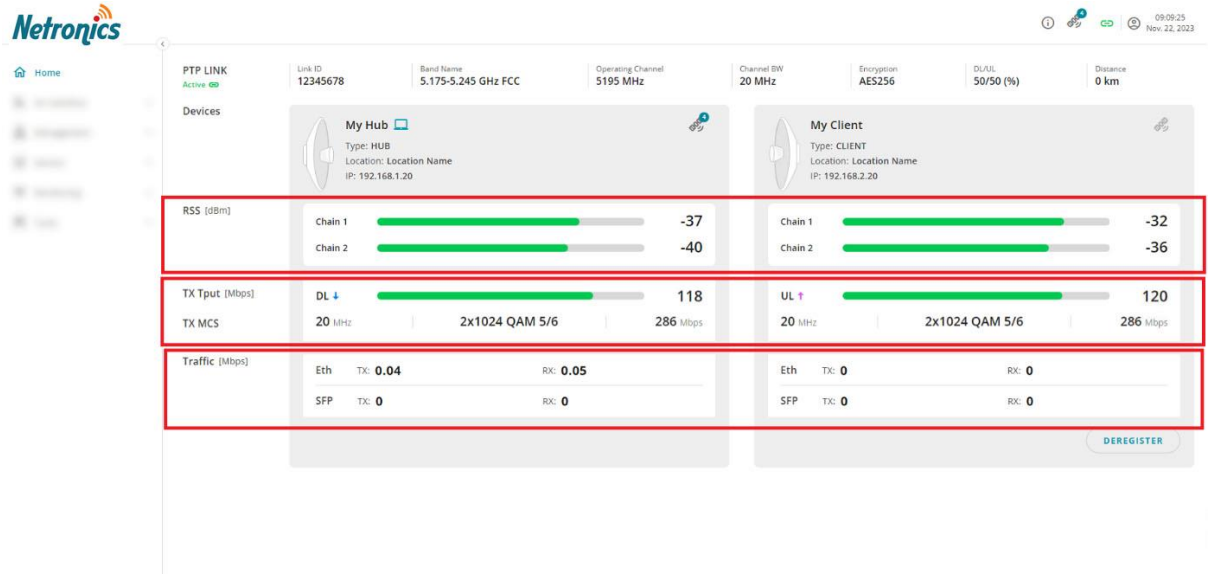


Figure 18: Viewing Devices & Link Status

Parameter	Description
RSS	Current Received Signal Strength for each RF chain (Vertical/Horizontal).
TX Tput	Displays a bar containing 2 values: Gray bar range - maximum throughput that can be achieved under current conditions (distance, CBW, UL/DL ratio) assuming highest MCS. Green bar (and number) - estimated throughput based on actual measured link conditions.
TX MCS	Displays 3 values for the last second (from left to right): Current CBW - changes dynamically according to link quality and interference. This value displays the presently used CBW. Current MCS - changes dynamically according to link quality and interference. This value displays the presently used MCS. Air interface rate - represents the modem speed over the air that corresponds to the current MCS and CBW.
Traffic	The row shows the actual traffic entering / exiting the device over the wired interface. The maximum traffic (going over the air) can reach up to the Tput (green bar) value.

5 Configuring the Air Interface Parameters

5.1 Configuring the Link Security

- In the **Link Security** window, you can:
  - Configure Link ID.
  - Change link password

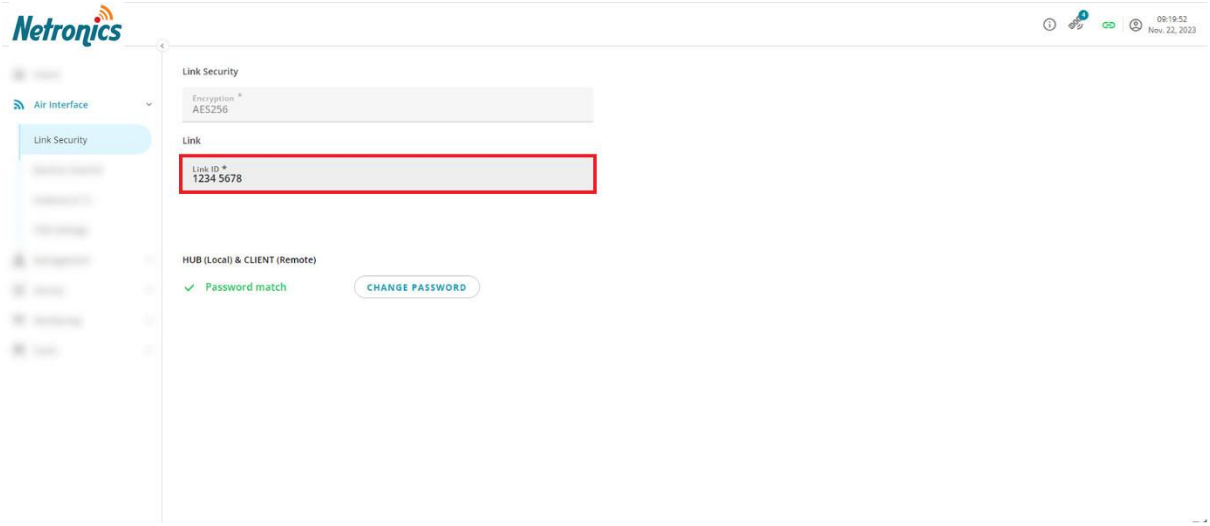


Figure 19: Configuring the Link Security

5.1.1 Changing the Link ID

The following parameters are available in the page:

Parameter	Description	Mandatory
Encryption	Displays the current air interface encryption (Wireless E always uses AES256)	Read only
Link ID	Enter 8-24 characters (English letters, numbers and "_" are allowed)	Yes

Link ID is similar to SSID in WiFi. During link establishment, the Hub's link ID is published in the HUB's beacon. When the Client identifies a beacon, it will attempt to connect to that beacon. The Hub will accept / reject the Client's connection based on the match between the link ID of the Client and the Hub.

If a registered link drops, the Client will only re-connect to a beacon with link ID matching its own link ID.

In case the link ID of either side was changed while the link was down, the link will fail to be reestablished due to link ID mismatch.

Note

When the link is Active (the Client is registered), it is possible to change the link ID only from the Hub side – on the Client side the Link ID field is greyed out. When the Client is not registered or de-registered, you could change the Link ID also on the Client side. When the link is active and you edit the link ID from the Hub side, the link ID of Hub and Client are updated together.

The first 4 characters of the link ID are designated as the “Network ID”.

- When configuring a Client unit, following options are available for Link ID setting:

Client Link ID setting	Client behavior
Empty	Client will connect to any Hub unit
Network ID (first 4 characters)	Client will only connect to Hub unit with matching Network ID
Full link ID	Client will only connect to Hub unit with matching full Link ID

5.1.2 Changing the Link Password

Changing link password will improve link security. All Wireless E units are shipped with a default link password. Once the link password is updated, in order to establish a new link or to replace a unit in the existing link, same link password must be set on both units.

Link password can be updated locally on each unit before installation.On an existing link, from either hub or client unit.

New password should have at least 8 characters, any of the following character types can be used:

English letters

Special characters

Numbers

1. In the Link Security page, click **Change Password**.
2. Enter the old password in **Old Password** field (default password is **Wireless Bridge**)
3. Enter the new password in the **New Password** and **Confirm Password** fields.
4. Click **Change**.

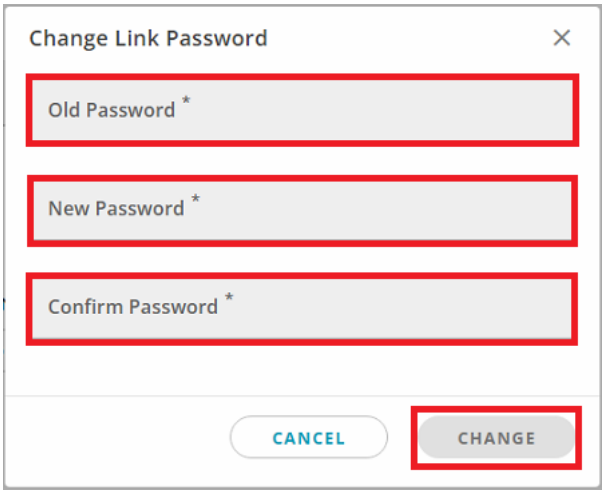


Figure 20: Changing the Link Security Password

5.2 Configuring the Band and Channel

The Band and Channel window enables you to configure the Country, Band Name, Channel Bandwidth, and Operating Channel.

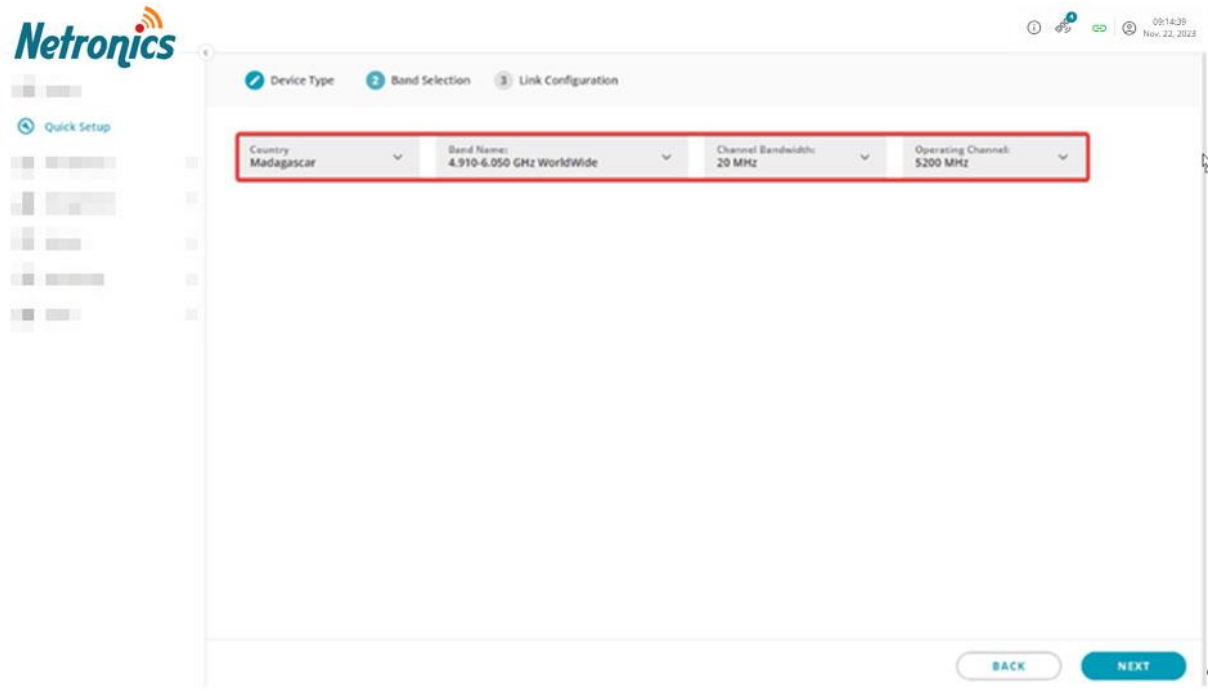


Figure 21: Configuring the Band and Channel

The Band and Channel parameters are described in the following table:

Parameter	Description
Country	This field shows the country in which the Hub is located. The allowed frequency bands and transmission restrictions are derived from the regulation that applies to the set country. The Client receives the operating band and channel from the Hub, and doesn't require its own country setting. See Regulation Compliance for additional explanation regarding country and regulation detection. When the Hub detects a GNSS signal, it determines the country and derives the applicable regulation from that country. In this case, the county selection is disabled for the user. Once the country has been detected once, it is remembered by the Hub regardless of ODU losing GNSS signal afterwards, or of any reboots. If a GNSS signal is not detected during Hub boot, manual country selection is possible. If Hub has been activated already, the previously detected / set country will continue to be applied and service will resume after the device boots with no need for user intervention. If the Hub hasn't been activated yet, select a country to set the frequency band for the link. This allows the Hub to start transmission.

Parameter	Description
	Caution: After manual country selection, when GNSS signal is detected again, the Hub will automatically update the country to the one detected from GNSS. If you configured a band that now becomes not supported in the updated country, the ODU will cease transmission until you select a permitted band. Therefore, always make sure you select the correct country in order to avoid working in non-permitted bands and to avoid having the service interrupted due to contradiction between the manually selected band and the automatically detected regulation
Band Name	Note: The available bands are derived from the applicable regulation of the country in which the Hub is located. Each band includes a range of available channels and regulatory restrictions (TX power, max EIRP).
Channel Bandwidth	This is the required channel bandwidth (CBW) on which the link will operate. The actual CBW is dynamically adapted according to link conditions (Automatic CBW selection). Note: The available CBWs are determined by the selected band, and are derived from the applicable regulation of the country in which the Hub is located.
Operating Channel	This is the actual frequency on which the link with the Client will be established.

5.3 Configuring the Antenna & TX Power

The Antenna and TX window enables you to configure Antenna gain (for external ODU), cable gain, and TX power. Based on the values you enter the system calculates the max TX power allowed that complies with the regulation limit in the selected frequency band.

Current actual TX power, the EIRP limit according to selected band regulation, and the current transmitted EIRP are displayed.

Note: The remote ODU info / settings appear only when the link is active.

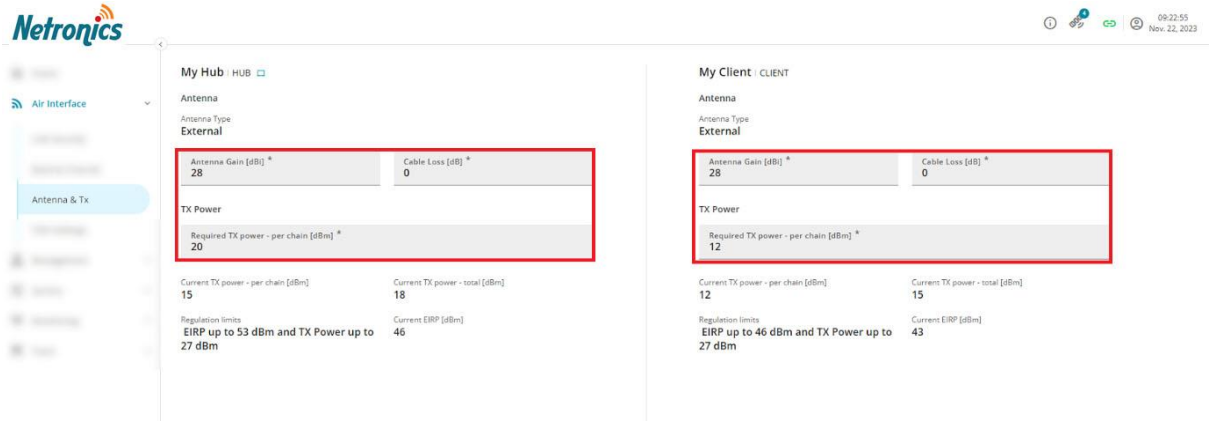


Figure 22: Configuring the Antenna & TX Power

The Antenna and TX parameters are described in the following table:

Parameter	Description	Mandatory
Antenna Type	Integrated or External	Read only
Antenna Gain	Required for External, read only for Integrated antenna	Yes
Cable Loss	For External antenna only	Yes
Max TX Power - per chain	Specify the maximum TX power per antenna chain (0 - 25dBm). The actual TX power is limited by regulation.	Yes
Current TX power - Per chain	The current TX power per chain, adjusted to support both regulation and current modulation.	Read only
Current TX power - Total	The current combined TX power (always 3db > TX power per chain), adjusted to support regulation and modulation.	Read only
Regulation limits	Maximum regulation allowed EIRP and TX power in the selected band	Read only
EIRP	Actual EIRP calculated from the current TX power, antenna gain, cable loss	Read only

5.4 Configuring TDD Settings

The TDD Setting window enables you to configure the ratio allocated for downlink (Hub->Client) and uplink (Client->Hub).

For more information regarding the UL/DL ratio, see

TDD (DL/UL) *Ratio*.

To configure the DL/UL Ratio:

1. Move the slider to select the required ratio from the following options:
   - 75/25
   - 50/50

- 25/75

Figure 23: Configuring the TDD

2. Click **APPLY**.

6 Configuring ODU Management Parameters

6.1 Configuring General ODU Settings

Configure the following parameters for both the Hub and Client ODUs:

Note

The remote ODU info / settings appear only when the link is active.

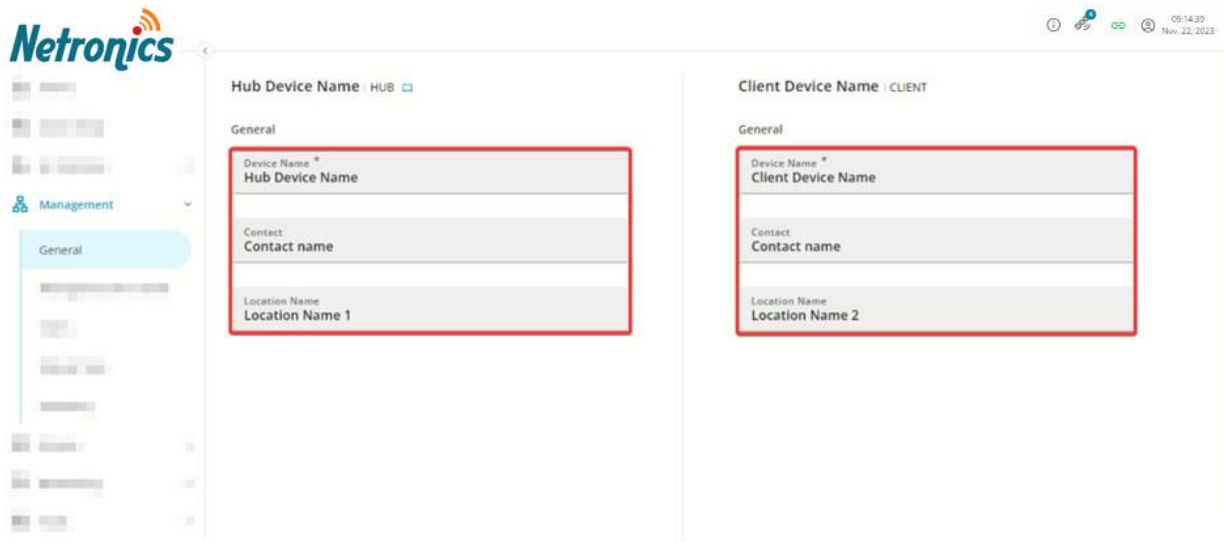


Figure 24: Configuring General ODU Settings

Parameter	Description	Mandatory
Device Name	Descriptive name to identify the device	Yes
Contact	Description to identify the person to be contacted (customer, maintenance contact etc.)	No
Location Name	Description to identify the physical location	No

6.2 Configuring the Management IP and VLAN

Configure the following parameters for both the Hub and Client ODUs:

Note

The remote ODU info / settings appear only when the link is active

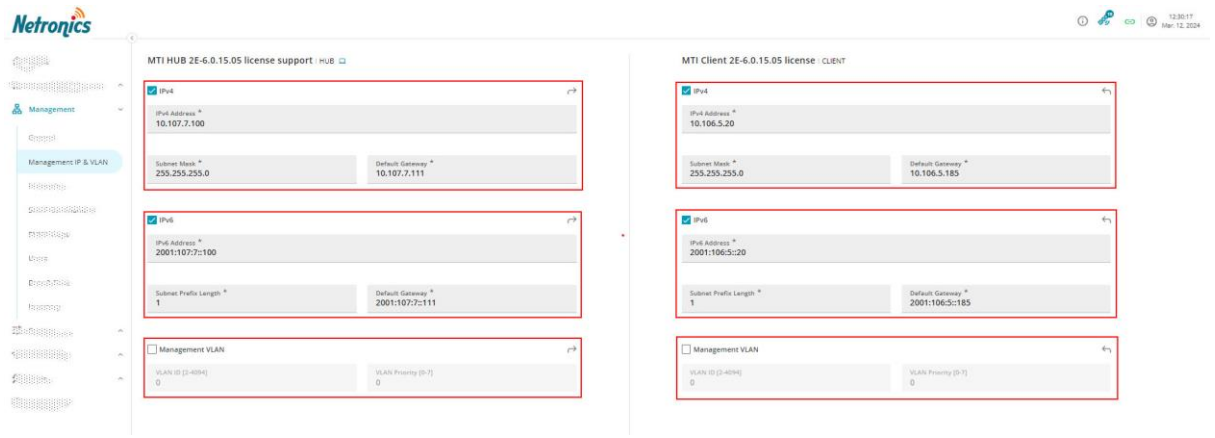


Figure 25: Configuring the Management IP and VLAN

Parameter	Description	Mandatory	Default value
IPv4 Section			
IPv4 Address	IPv4 address for management interface	Yes	**10.0.0.120**
Subnet Mask	IPv4 subnet mask for management interface	Yes	**255.255.255.0**
Default Gateway	IPv4 address default gateway for management interface	Yes	**0.0.0.0**
IPv6 Section			
IPv6 Address	IPv6 Address for management interface	No	**::a**
Subnet Prefix Length	Number of bits used by the prefix	No	**64**
Default Gateway	IPv6 address default gateway for management interface	No	**::b**
Management VLAN	Enable/disable VLAN tagging for management traffic	No	**Disabled**
VLAN ID	Supported values: 2-4094	Parameter	
VLAN Priority	Supported values: 0-7	Parameter	

Note

You can copy IPv4, IPv6 and/or VLAN values from one side of the link to the other side by clicking the Copy arrow button. Make sure you don't configure the same IP address for both devices

6.3 Configuring the Protocols

Configure the following parameters for both the Hub and Client ODUs:

Note

The remote ODU info / settings appear only when the link is active

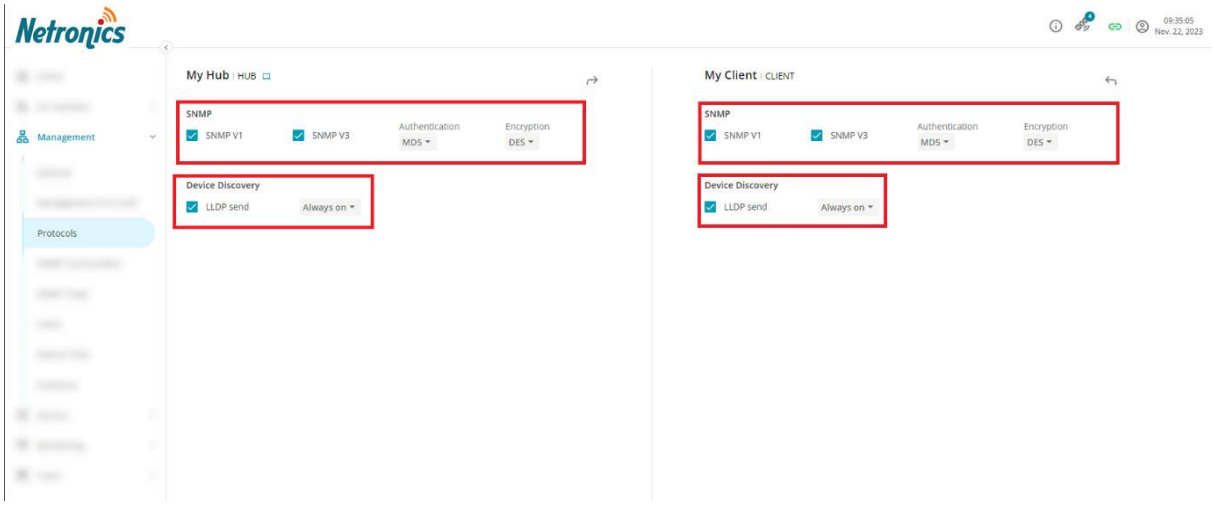


Figure 26: Configuring the Protocols

Parameter	Description	Mandatory	Default value
SNMP	**Control SNMP version and parameters**		
SNMPv1	Enable SNMPv1 for polling	No	**Enabled**
SNMPv3	Enable SNMPv3 for polling	No	**Disabled**
Authentication	SNMPv3 Authentication method (**MD5** / **SHA1**) Only visible when SNMPv3 is selected	Parameter	**MD5**
Encryption	SNMPv3 Encryption method (**DES** / **AES**) Only visible when SNMPv3 is selected	Parameter	**DES**
Device Discovery	**Control LLDP device discovery parameters**		

Parameter	Description	Mandatory	Default value
LLDP send	Enable/disable sending LLDP packets for discovery	No	**Enabled**
	Time limit for LLDP (**Always on** / **Off 5 min after boot**)	Parameter	**Off 5 min after boot**

6.3.1 SNMP implementation

Netronics NetStream 5x750 2G5 supports RFC1213 MIB-II as well as private MIB – see details in the table below.

Root OID	MIB	MIB subtree name	Description
.1.3.6.1.2.1.1	RFC1213-MIB	system	System uptime, system OID, system Name/ Contact/Location
.1.3.6.1.2.1.2	RFC1213-MIB	interfaces	Interface table for POE, SFP and wireless interfaces
.1.3.6.1.4.1.29612.1000.1.1	private	NetronicsOduAdmin	Inventory info, management IP / VLAN settings
.1.3.6.1.4.1.29612.1000.1.2	private	NetronicsOduService	QOS parameters
.1.3.6.1.4.1.29612.1000.1.5	private	NetronicsOduAir	Air interface parameters
.1.3.6.1.4.1.29612.1000.7	private	NetronicsGenesis	New subtree for optimized PTP link monitoring. Presents key LAN and air interface metrics for both local and remote units

6.3.2 LLDP implementation

LLDP is a standard protocol for local discovery of network topology and devices.

Netronics NetStream 5x750 2G5 implementation of LLDP:

- Each unit sends LLDP frames to Ethernet ports to advertise itself to connected devices
- Link is transparent for LLDP frames sent by connected devices
-

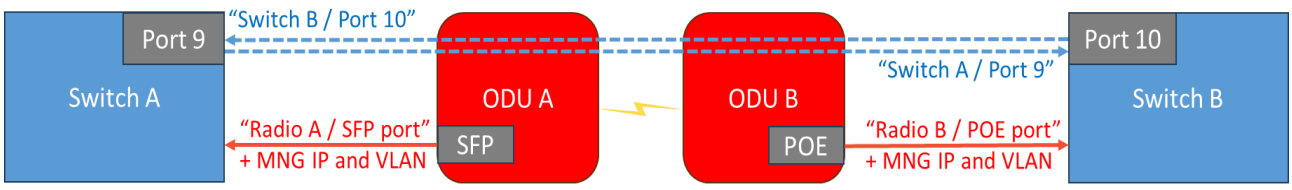


Figure 27: LLDP flow

The following information is advertised by Wireless E via LLDP:

LLDP TLV	Description
Chassis ID	Ethernet MAC address
Port Subtype	Interface name such as **Two_FiveGigabitEthernet0**
Port Description	Port description such as **2.5Gbps_Ethernet_VID_201** to identify the connected port and management VLAN ID (if management VLAN is configured)
System name	Device name set in General configuration screen
Management Address	Management IP address

6.4 Configuring the SNMP Communities

Configure the following parameters for both the Hub and Client ODUs:

Note

The remote ODU info / settings appear only when the link is active

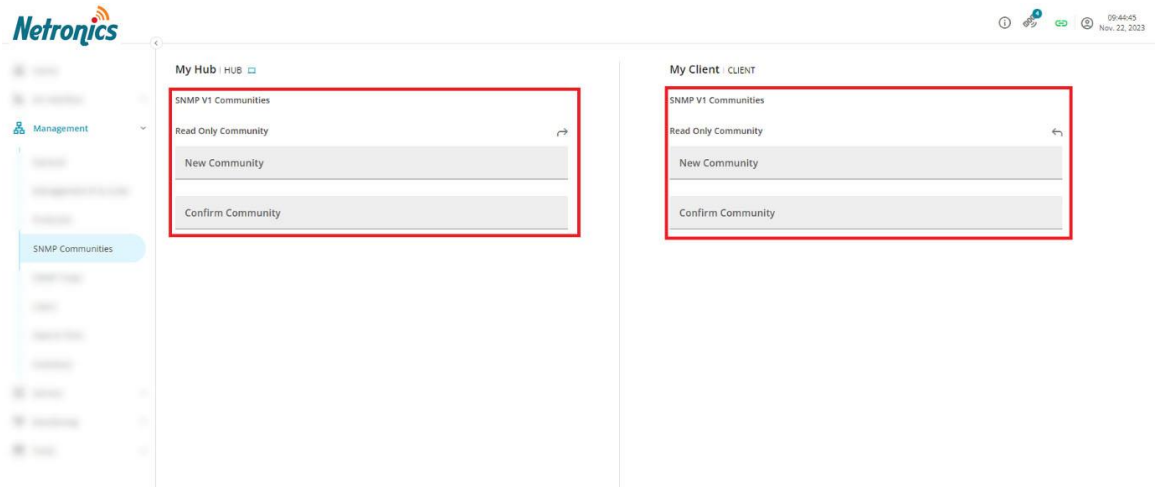


Figure 28: Configuring the SNMP Communities

Parameter	Description	Mandatory	Default value
Read Only Community	**Change the SNMPv1 read only community**	No	**public**
- New Community	Enter the new value	Parameter	
- Confirm Community	Enter the same value again	Parameter	

Note

When using SNMPv3, the admin user credentials are used.

6.5 Configuring the SNMP Traps

Configure the following parameters for both the Hub and Client ODUs:

Note

The remote ODU info / settings appear only when the link is active

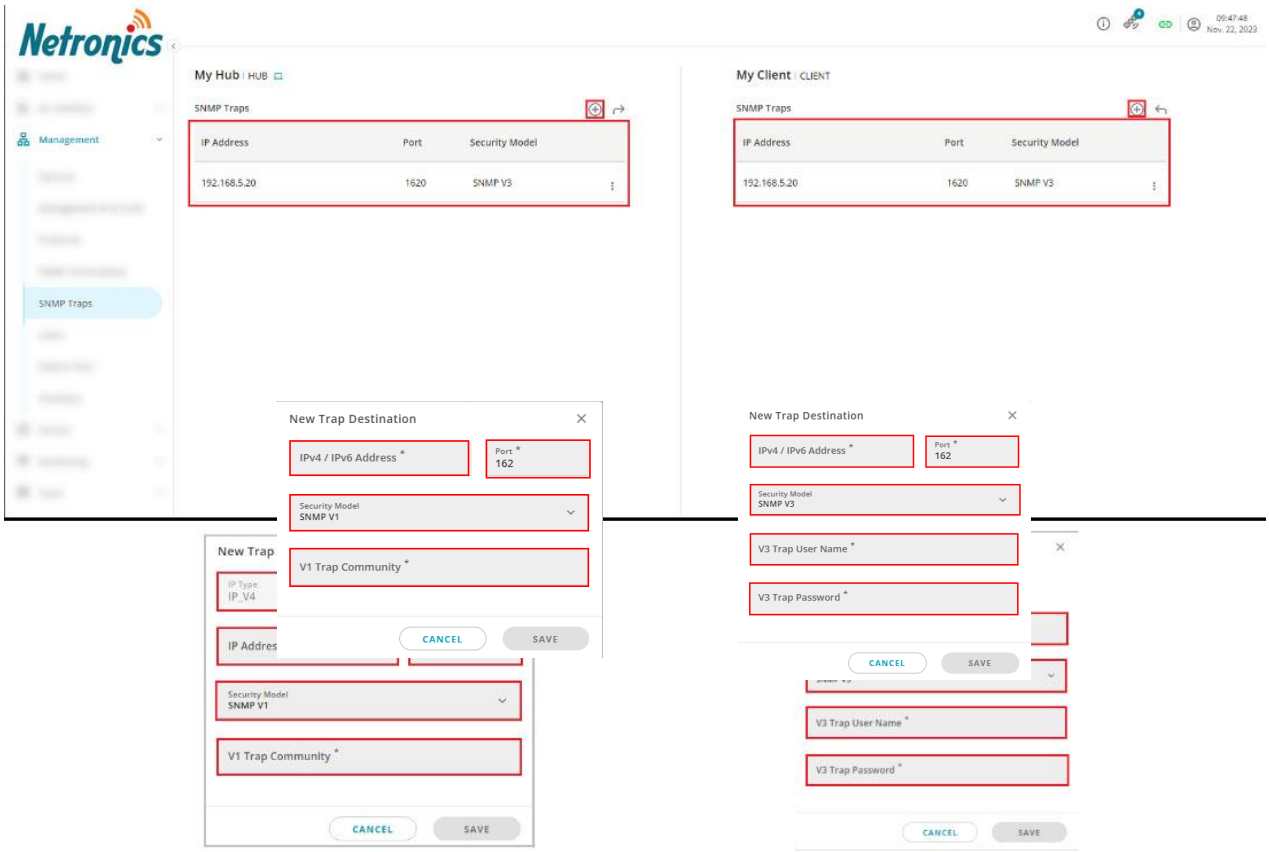


Figure 29: Configuring the SNMP Traps

The following page displays a list of the available trap destinations and enables creating additional destinations using the **+** button.

Parameter	Description	Mandatory	Default value
IP Address	**IPv4 or IPv6** destination IP address	Yes	
Port	Destination UDP port	Yes	**162**
Security Model	The security model (**SNMPv1 / SNMPv3**)	Yes	**SNMPv1**
V1 Trap Community	The community to be used for SNMPv1 traps *Only visible when SNMPv1 security model is selected*	Yes – for V1	

Parameter	Description	Mandatory	Default value
V3 Trap User Name	The username to be used for SNMPv3 traps *Only visible when SNMPv3 security model is selected*	Yes – for V3	
V3 Trap Password	The password to be used for SNMPv3 traps *Only visible when SNMPv3 security model is selected*	Yes – for V3	

6.6 Modifying User Passwords

On the local ODU to which you are connected, you can change the local user credentials for WEB UI access and SNMPv3 polling.

Note

To change a user password on the remote ODU, connect directly to the remote ODU IP address through the browser interface.

1. Click the options icon and click Change password.

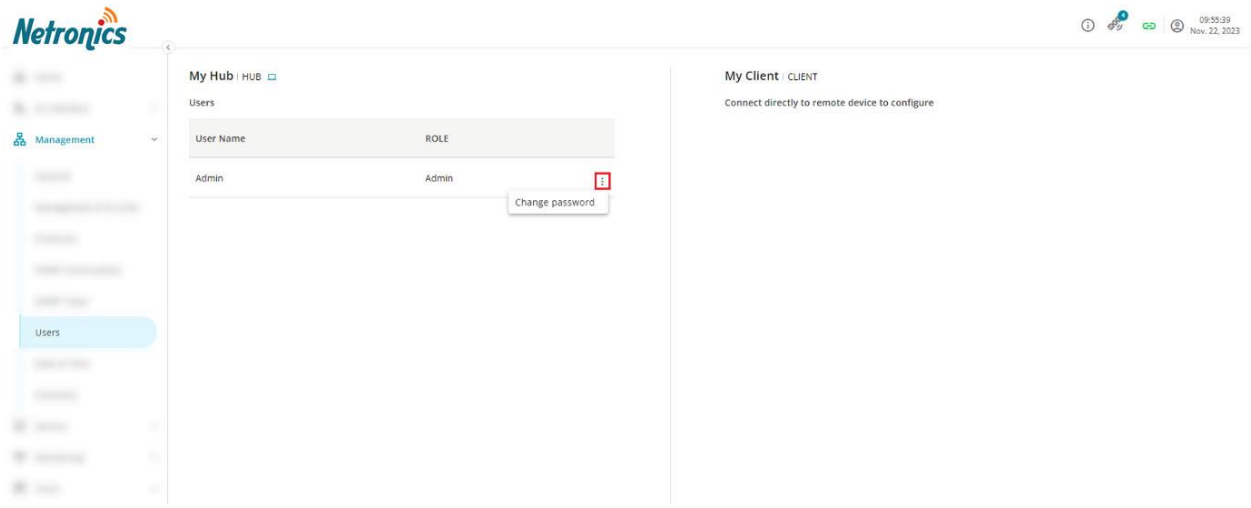


Figure 30: Modifying Passwords

Note

Password update requires current password confirmation

Note

SNMPv3 trap user name and password are set per each SNMPv3 trap destination (see **Configuring the SNMP Traps**)

6.7 Viewing the Date and Time

You can view the time source, as well as current date and time of the ODU in the **Date and Time** window.

Note

The remote ODU appears only when the link is active.

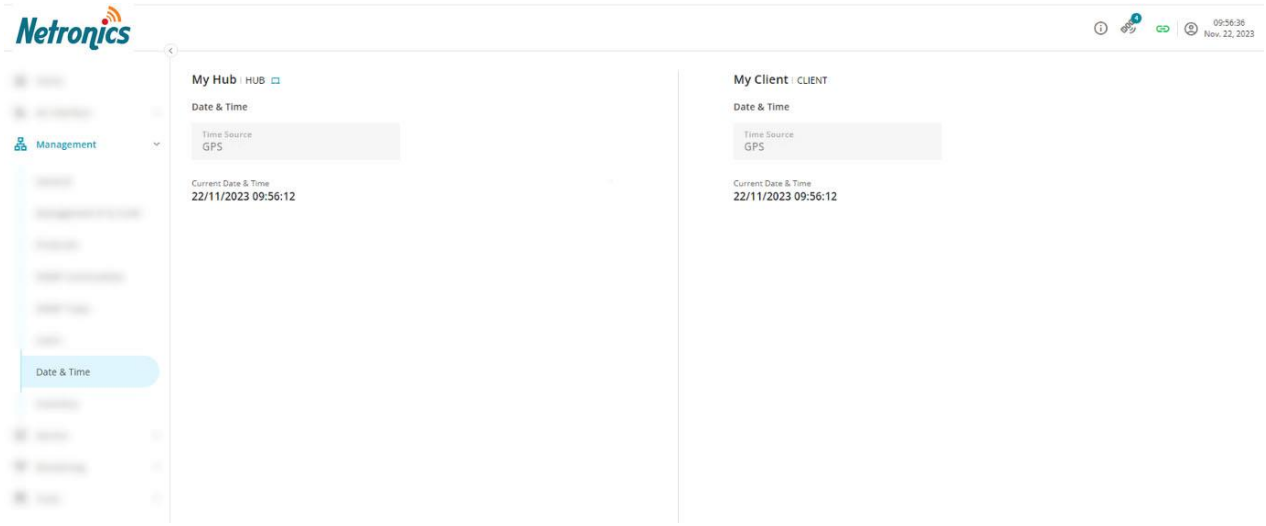


Figure 31: Viewing the Date and Time

Parameter	Description
Time Source	Time data source (**Internal / GPS**) *Note: Internal time source will only be used for several minutes after boot, until GPS signal is acquired.*
Current Date and Time	Shows the Date and Time The format is **DD/MM/YYYY HH:MM:SS** *Note: Time zone is detected automatically based on GPS location data and internal database*

6.8 Viewing the ODU Inventory

Displays information for Hub and Client ODU inventory parameters:

- Product Name
- Part Number
- HW Version
- SW Version
- MAC address
- Serial Number
- Supported Encryptions

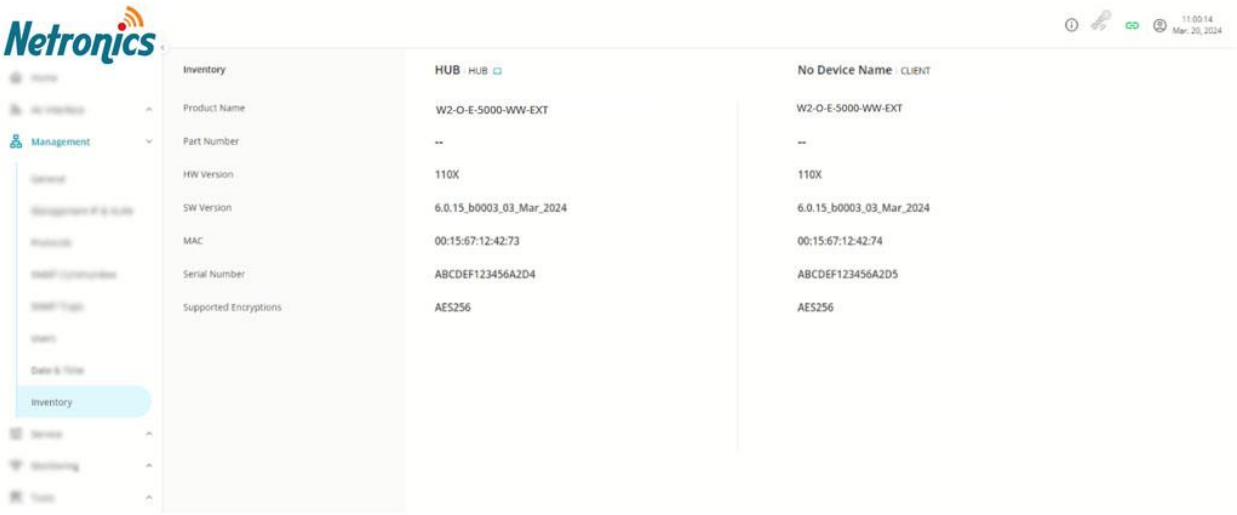


Figure 32: Viewing the ODU Inventory

7 Configuring Service Parameters

7.1 Viewing the LAN Ports Parameters

Displays the port parameters for both the Hub and Client ODUs:

Note

The remote ODU info / settings appear only when the link is active.

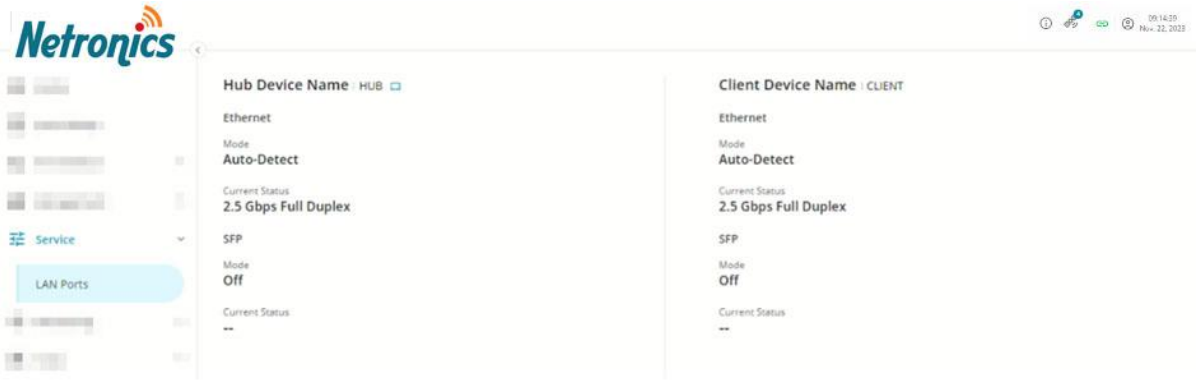


Figure 33: Viewing LAN Ports Parameters

Parameter	Description	Mandatory
Mode (Ethernet)	Only **Auto-Detect** is currently supported	Read only
Current Status (Ethernet)	Displays the current Ethernet speed and duplex mode **(100 Mbps Full Duplex / 1000 Mbps Full Duplex / 2.5 Gbps Full Duplex)**	Read only
Mode (SFP)	**Off**: no SFP module detected **Auto-Detect:** SFP module is present	Read only
Current Status (SFP)	Displays the Ethernet speed and duplex mode of the internal SFP slot interface. Only 1Gbps SFPs are supported, and **1000 Mbps Full Duplex** should be displayed. *Note: fiber / copper link status is not reflected currently*	Read only

7.2 Modifying the QOS Mode and Priority

Netronics NetStream 5x750 2G5 supports QoS classification based on either 802.1p VLAN or Diffserv DSCP values. Ingress traffic is classified into up to 8 priority queues.

The QoS Mode and Priority screen enables the following operations:

- QoS mode selection
- Enable / disable queues
- Rename queues
- Set QoS priority mapping for each enabled queue

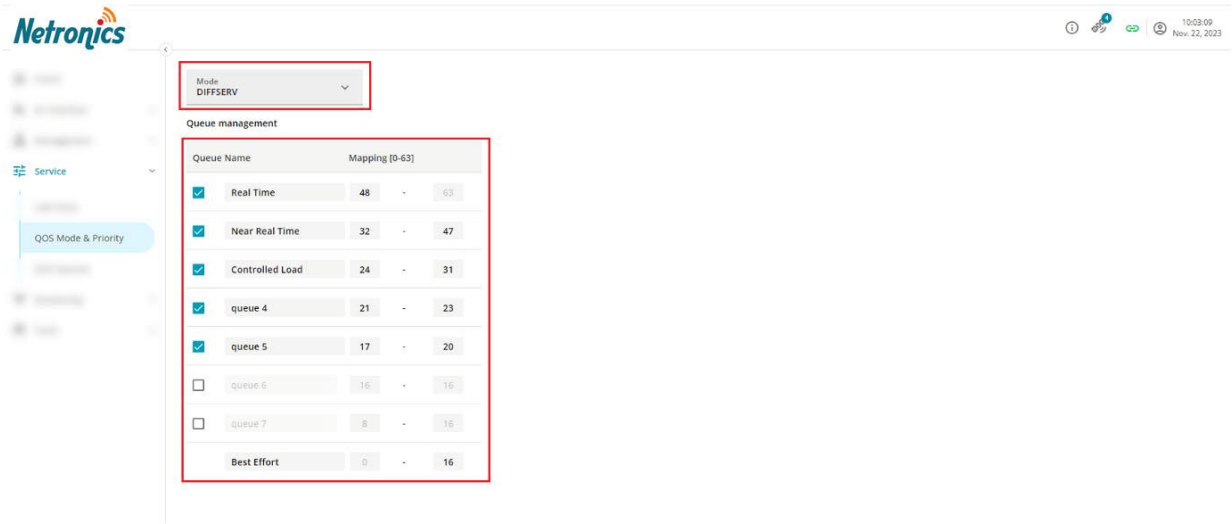


Figure 34: Modifying QOS Mode and Priority

Parameter	Description	Mandatory	Default value
Mode	**Selects the QOS mode (VLAN / DIFFSERV / Disabled) for the link**	**Yes**	**Disabled**
VLAN	801.p COS value of ingress 802.1Q frames will be used for classification	Parameter	
Diffserv	Diffserv DSCP value of ingress packets will be used for classification	Parameter	
Disabled	Traffic classification is disabled	Parameter	
Queue Management	**Enable/disable, set name and priority range**	**Yes**	
Enable / disable	Enabling and disabling the queue will affect the visible queues in the QoS Queue screen. Up to 8 queues can be enabled.	Yes	**See table below**

Parameter	Description	Mandatory	Default value
Queue name	Set a custom name as needed (such as **Video**)	No	**See table below**
Mapping	Set priority range for each queue. Available value ranges depend on the QoS mode selected: • QoS Disabled: N/A • VLAN: 0 – 7 • DIFFSERV: 0 – 63	Yes	**See table below**

If a queue is disabled/enabled, the user must adjust the mapping, so it adheres to the validation rules. Priority range mapping values must be monotonic and must cover the entire range. When enabling a queue, the WFQ proportions between the queues are changed and the user must go to the Queues screen to make sure the new proportions are correctly configured.

Queue	Queue default name	Default Priority	
		Diffserv	VLAN
1	**Real time**	48-63	6-7
2	**Near real time**	32-47	4-5
3	**Controlled load**	16-31	2-3
4	**Queue 4**	Off	Off
5	**Queue 5**	Off	Off
6	**Queue 6**	Off	Off
7	**Queue 7**	Off	Off
8	**Best effort**	0-15	0-1

Further configuration for queue settings is available in the QoS Queues window, as described below. The QoS configuration data is stored in the hub and sent to the client when link is established.

7.3 Modifying the QOS Queues

The QoS Queues screen controls the following:

- Strict / WFQ queue mode (per each link direction)
- Set Weight for WFQ (per each link direction)
- Set MIR mode and MIR value (per each link direction)

Link directions are as follows (also indicated by arrows on the UI):

Downlink (DL, ↓) – settings for Ethernet ingress queues of the **Hub** radio (left side panel)

Uplink (UL, ↑) – settings for Ethernet ingress queues of the **Client** radio (right side panel)

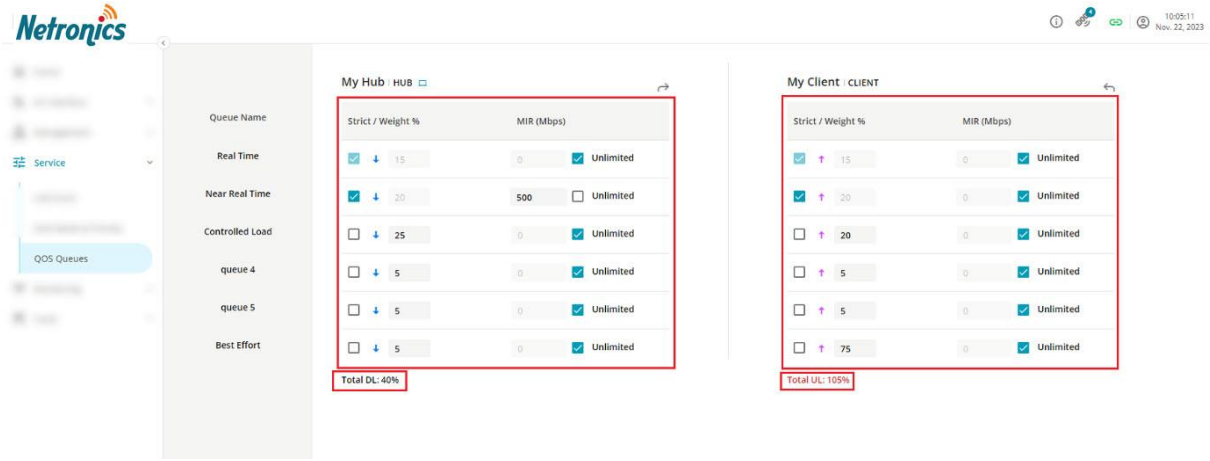


Figure 35: QoS Queues

Parameter	Description	Mandatory
Strict	• "Strict" priority packets will always be transmitted first, up to the defined MIR level. • When there are no more strict priority packets (either due to reaching the MIR or no user data available), the remaining bandwidth will be allocated to other priorities according to the WFQ • In case there are more Strict priority packets than available space in the air-frame, packets from lower priority queues will not enter this air-frame. • This ensures that high-priority traffic gets a guaranteed share of the available bandwidth and is not impacted by lower-priority traffic.	No
Weight %	• WFQ (Weighted Fair Queueing) - percent of the remaining air-frame capacity, assigned to this queue (after Strict priority packets filled the air-frame) • When the data channel is full, the packets of each priority transmitted in the air will be allocated according to the percent allotted for each priority	No

Parameter	Description	Mandatory
	• if a certain priority data channel has less data than its allotted percentage, its extra capacity will be split among the other channels corresponding to their percentage • When the data channel is not full, all packets will be transmitted without waiting The WFQ total percentage is displayed at the bottom row for the hub and client, and must be equal to 100% before you can click **APPLY**.	
MIR (Mbps) / Unlimited	• MIR - Maximum Information Rate ○ This is the maximum throughput limit for this queue ○ Note: actual MIR is limited by the selected channel bandwidth. If you modify the CBW, you might need to adjust the MIR. • Unlimited MIR. ○ No upper limit is set on the traffic for this queue	No

The remote ODU info / settings appear only when the link is active.

8 Viewing Monitoring Information

8.1 Counters View

The Counters window displays various statistics for traffic. The statistics are displayed for both the Hub and for the Client.

Note

The statistics are displayed only if there is an active link.

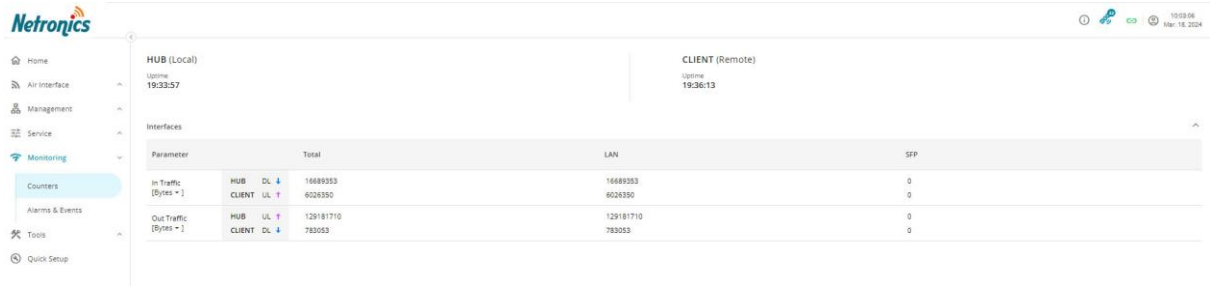


Figure 36: Counters View

The following table describes the Traffic parameters:

Parameter	Description
Uptime	Time elapsed since the reboot of the system.
In Traffic	Traffic entering the device over the wired port. The information can be displayed in bytes or in packets. The table displays values for LAN, SFP and total traffic.
Out Traffic	Traffic exiting the device over the wired port. The information can be displayed in bytes or in packets. The table displays values for LAN, SFP and total traffic.

Note

To select the units in which the data is displayed (bytes/packets), click the down arrow next to the current display unit:

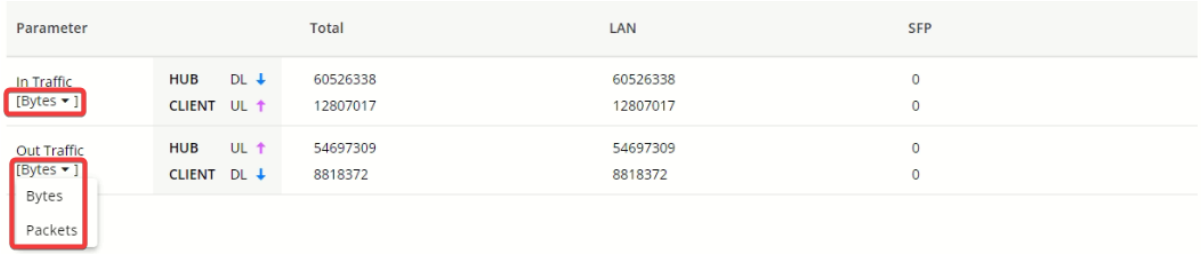


Figure 37: Traffic Parameters

8.2 Alarms and Events

The events list displays events that occurred in the system, sorted by their time of occurrence. Information provided includes:

- Date
- Time
- Type of event
- Device name
- Message

You can search for an event by text, scroll the list or skip to a specific page.

Note

For list of all supported events, see Web UI Events Table.

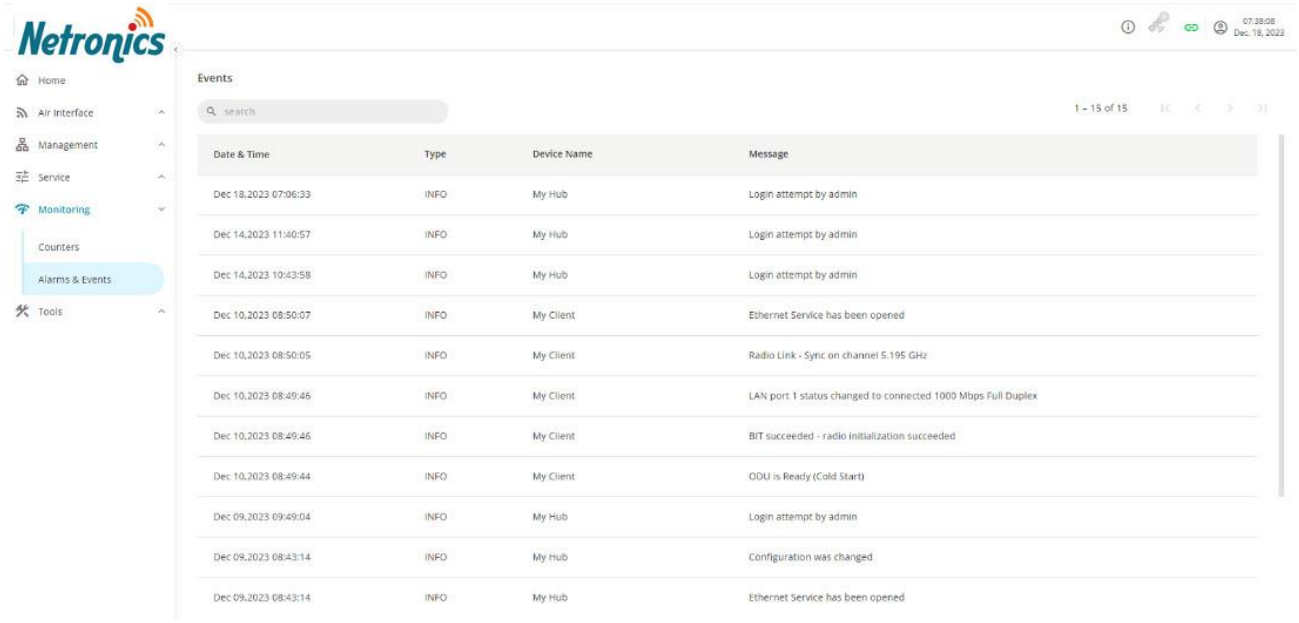


Figure 38: Alarms and Events

9 Applying Tools and Maintenance

9.1 Performing a Software Upgrade

Note

- This operation can only be performed on the local unit to which the browser is connected. To perform this operation on the remote ODU, you must connect to its own UI.
- Upgrading the software does not affect the ODU configuration.

To upgrade the software:

1. Select the device to upgrade.

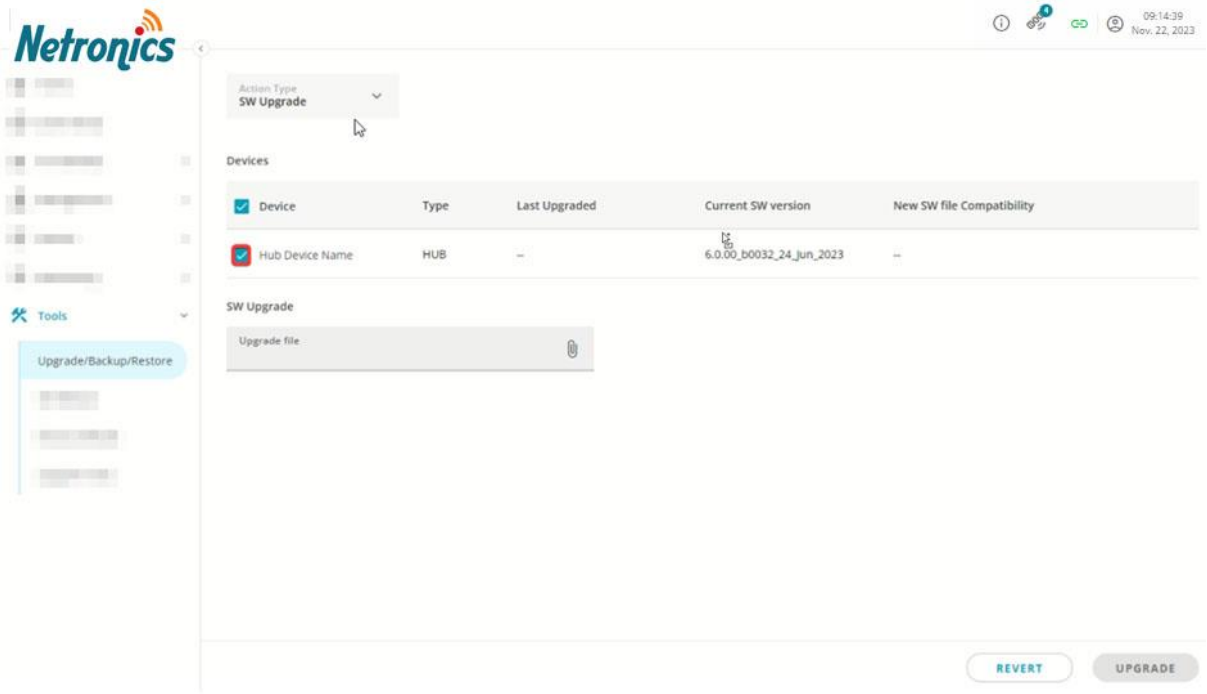


Figure 39: Performing a Software Upgrade

2. Click the **SW Upgrade** paper clip.

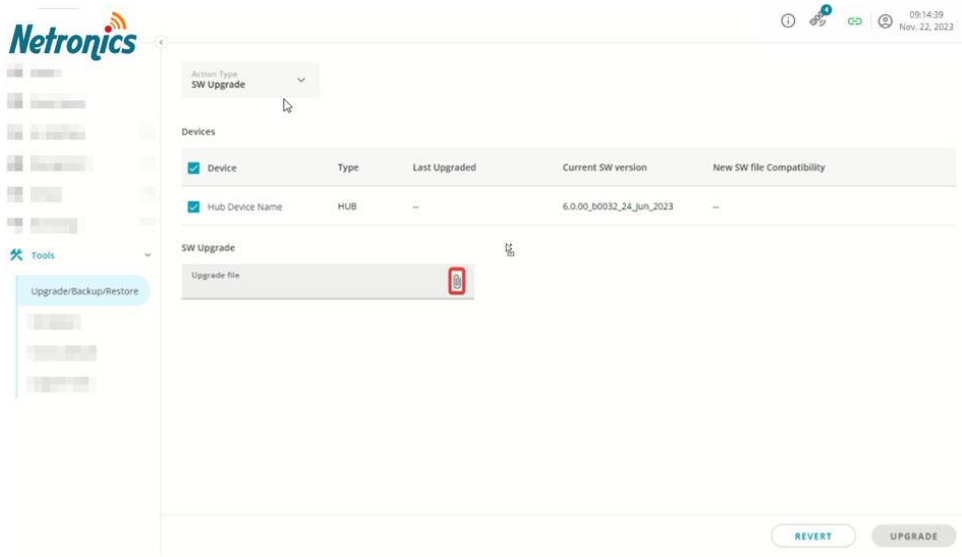


Figure 40: Software Update Paper Clip

3. Navigate to the required file, click **Open** and click **UPLOAD**.

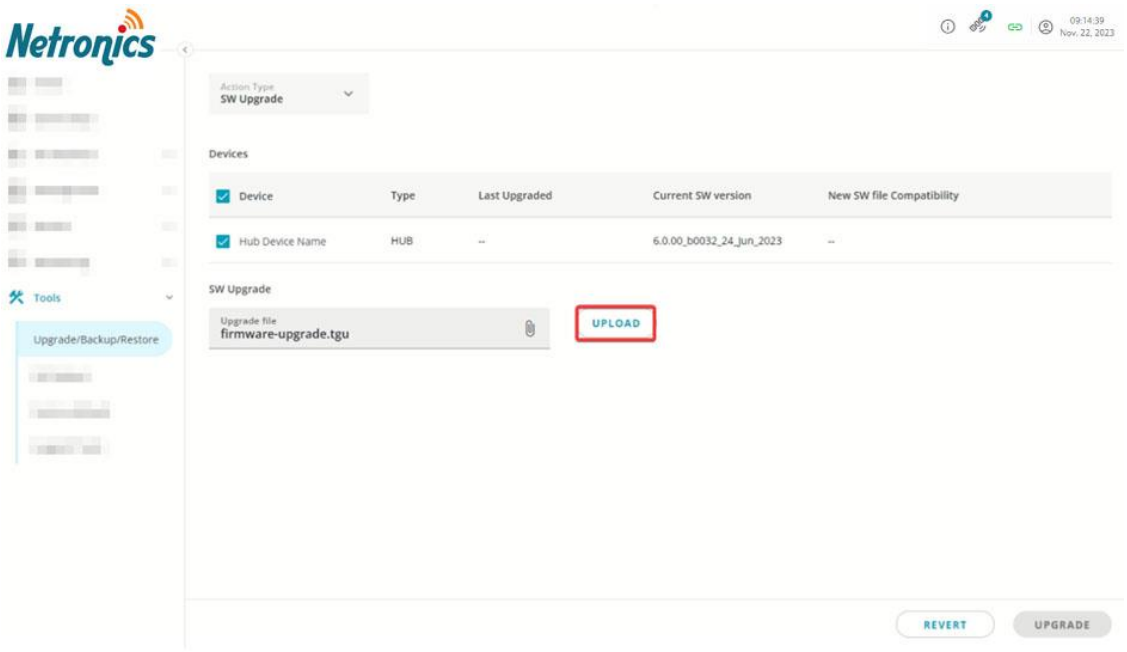


Figure 41: Navigate File

4. The file is uploaded, and its contents are validated and tested for compatibility.

   If validated, the SW version of the upgrade file is displayed, and if it is compatible with the ODU, a green checkmark is displayed.

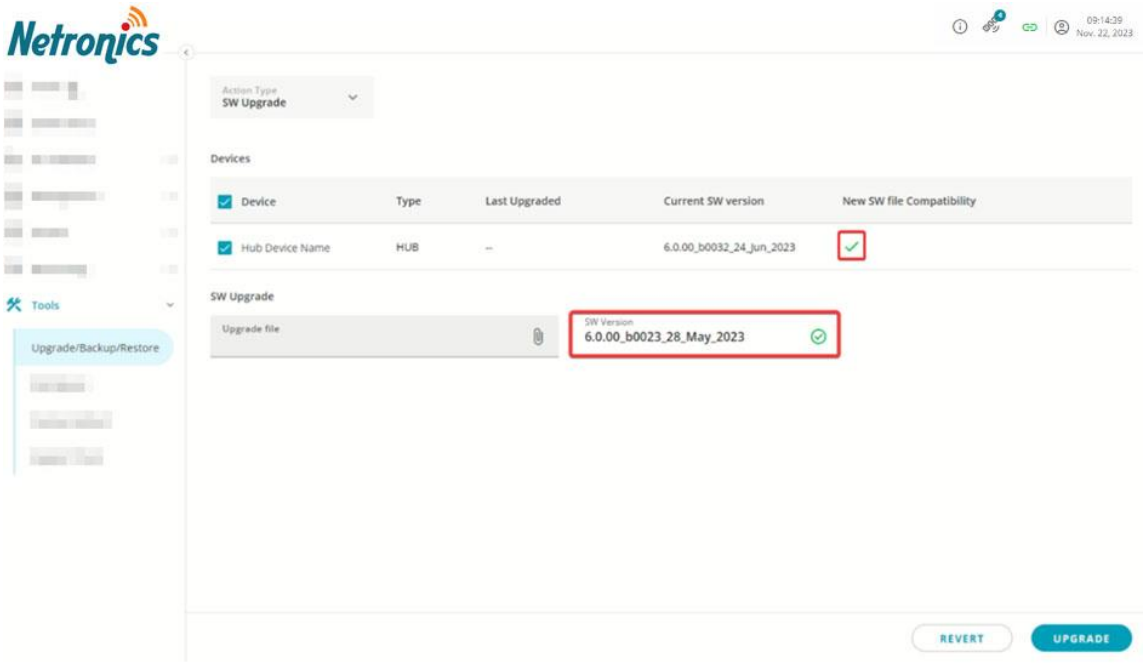


Figure 42: File Upload

Note

If the uploaded file cannot be validated or if it is not compatible with the ODU, a notification is displayed, and the upgrade cannot continue.

5. Click **UPGRADE**.

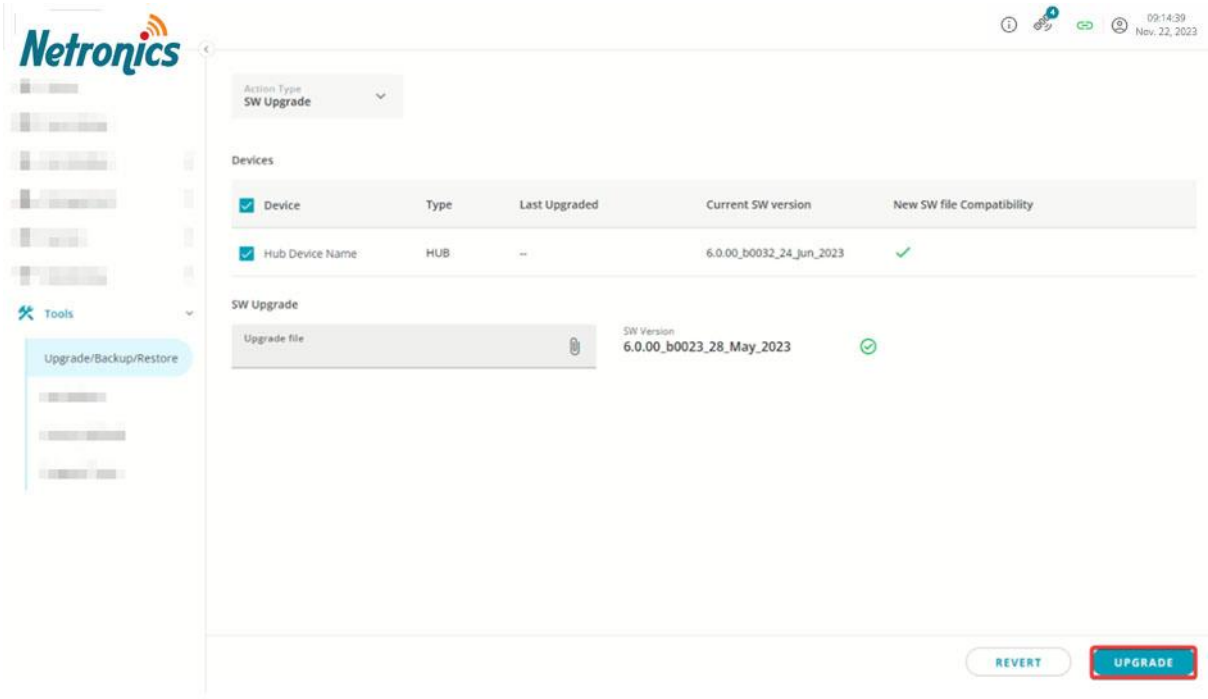


Figure 43: Upgrade

During the upgrade process, all ODU activity is frozen. Progress bars show the progress of the software upgrade and ODU restart.

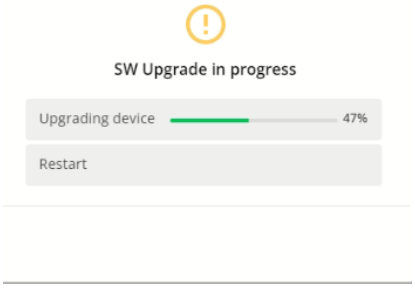


Figure 44: Upgrade in Progress

6. After the device restarts, the UI automatically will redirect to the login page.

9.2 Rebooting the ODU

You can reboot the ODU by clicking **REBOOT** for the Hub or Client ODU as required.

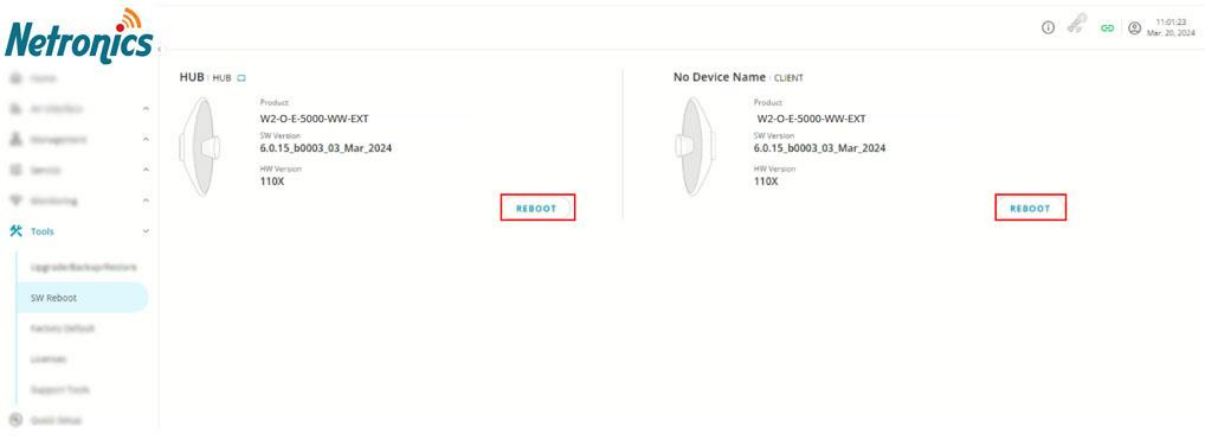


Figure 45: Rebooting the ODU

- During the reboot, a timer appears. When the ODU reboots, you will need to login again.

9.3 Resetting the ODU to Factory Defaults

You can restore the ODU to factory defaults by clicking **RESET TO FACTORY DEFAULT** for the Hub or Client ODU as required.

The IP and VLAN settings can be preserved after a factory reset by checking the **Preserve IP and VLAN** checkmark.

Note

The IP address is kept unchanged after a factory reset.

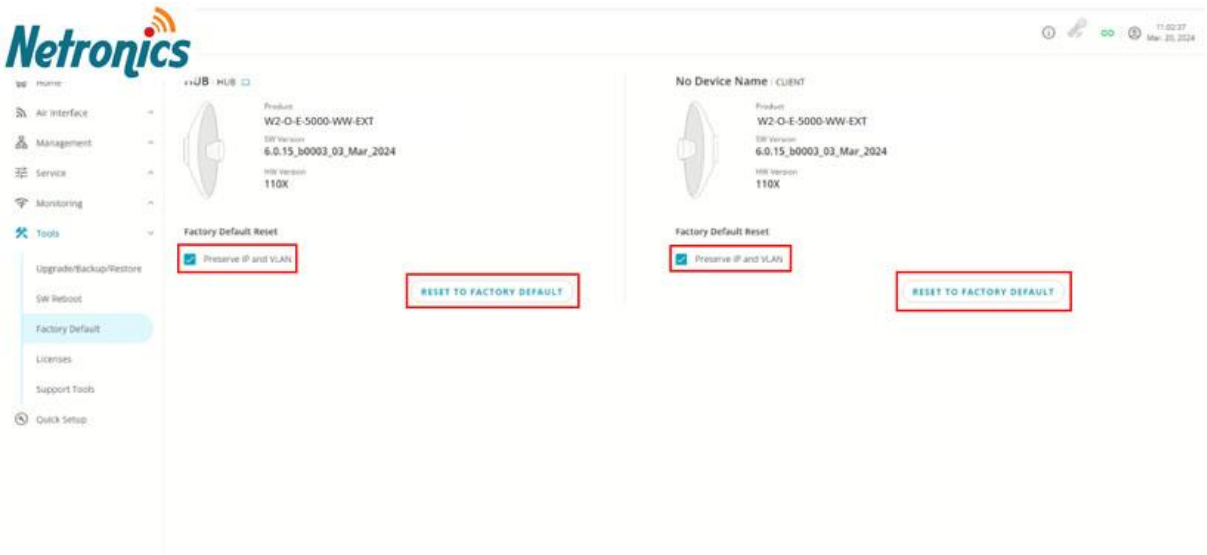


Figure 46: Resetting the ODU to Factory Defaults

Warning

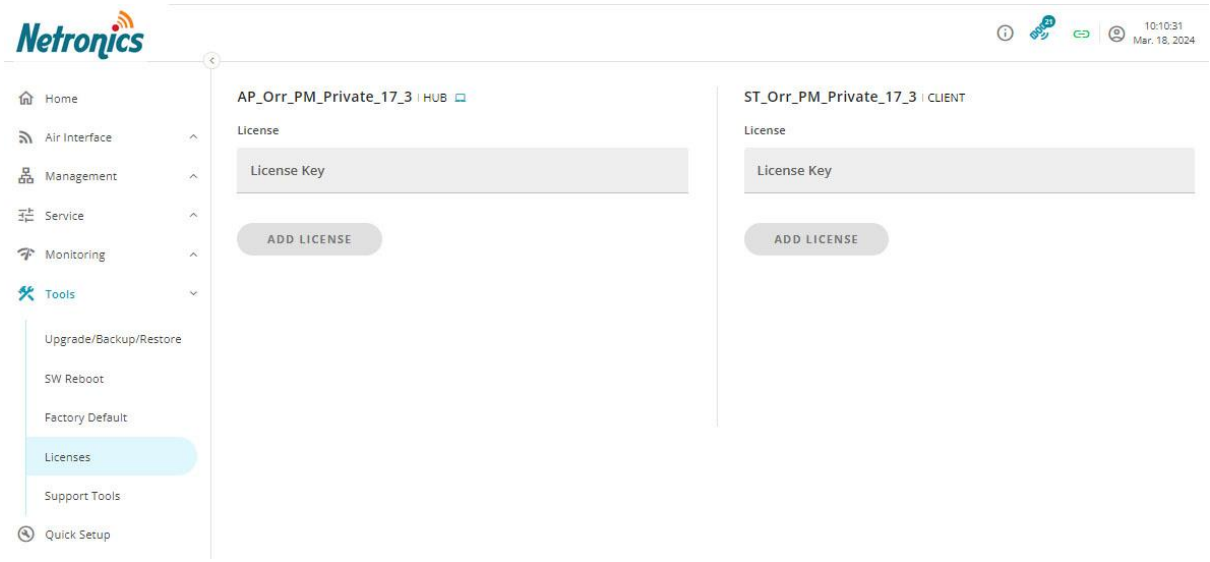
Resetting the ODU to factory default will erase all the device configuration, including Air interface parameters and user passwords. You need to make sure you will be able to connect to the device after you perform the factory reset.

9.4 Licenses

By default, bands are restricted based on GPS location according to local regulation. In some cases, such as for military or other government bodies, operator may have an authorization to operate on licensed bands.

In such a case, a band license can be obtained via your local NETRONICS partner who will provide license keys.

Paste the license keys for both hub and client to License Key fields and click **Add License.**



Note

In case of SW upgrade or restore factory default, the license is kept.

9.5 Support Tools

Note

These operations can only be performed on the local unit to which the browser is connected. To perform these operations on the remote ODU, you must connect to its own UI.

The following tool can be used to assist you when dealing with tech support:

- **Download Logs** - download the logs that have been collected in the ODU.

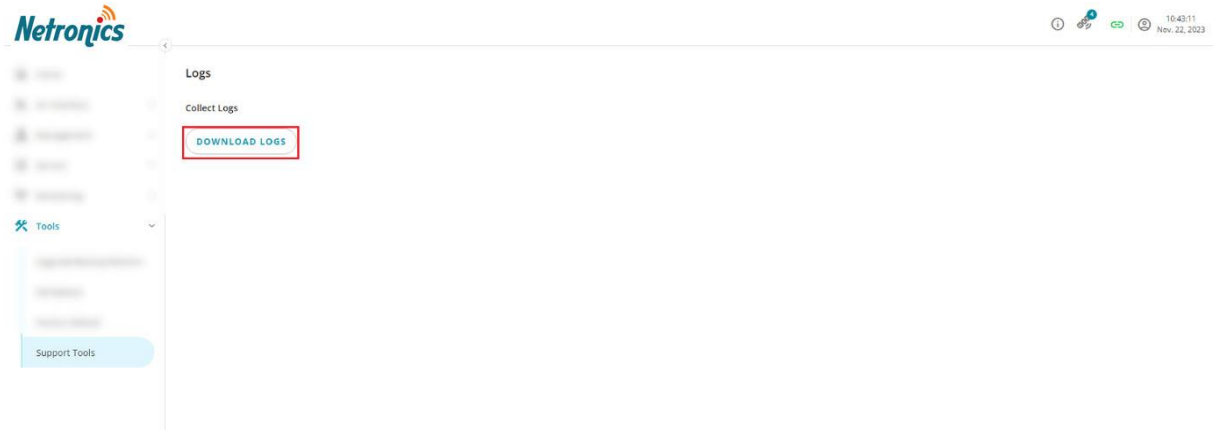


Figure 47: Supporting Tools

10 Troubleshooting

10.1 ODU Discovery via LLDP

Note

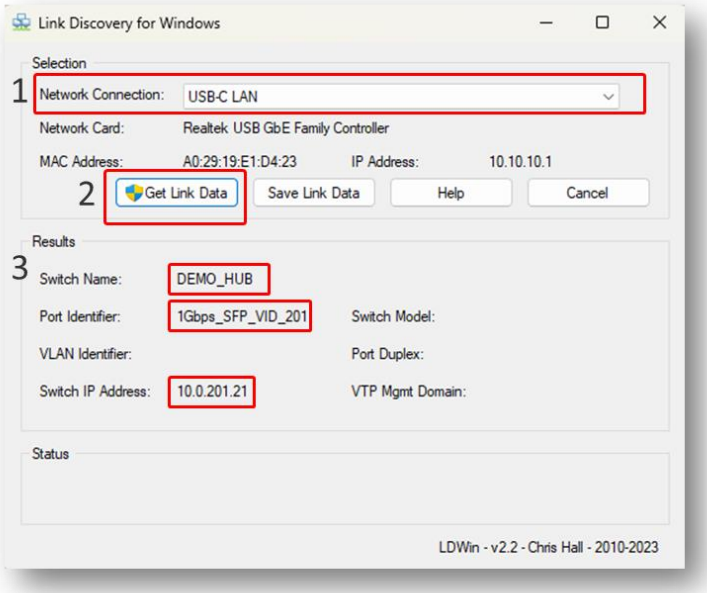
By default, LLDP discovery is enabled for 5 minutes after boot (see Protocols screen). We recommend not to change this setting in order to facilitate device discovery in any scenario.

10.1.1 Discovery on local PC using Wireshark

- Select your network interface and run capture
- Set capture filter for LLDP
- Connect the Wireless E ODU via POE injector directly to your PC
- After up to 30 seconds, LLDP frame should appear (NETRONICS MAC starts with **00:1E:48**)
- See Protocols section for details on LLDP TLVs

10.1.2 Discovery on local PC using LDWin

- **Download and run the open-source LDWin tool (https://github.com/chall32/LDWin)**
- Connect the Wireless E ODU via POE injector directly to your PC
- Select your Network Connection (1)
- Press the Get Link Data button (2)
- After up to 30 seconds, the following data is shown (3)
    - Device name (as “Switch name”)
    - Port name and Management VID (as “Port ID)
    - Management IP (as “Switch IP Address”)



10.1.3 Remote discovery via managed network device

- Enable LLDP receive on a connected device with LLDP support
- Power cycle the Wireless E unit (if the unit is powered by a managed POE switch, this can be done remotely by disabling and re-enabling enabling POE output on the relevant port)
- Check LLDP Neighbor Information for Chassis ID with NETRONICS MAC (starts with **00:1E:48)**

10.2 ODU Discovery via ARP

1. In a command line, arp –a | findstr 00:1E:48 to filter IP addresses by the MAC address. if running Linux or Mac, use grep instead of findstr.
2. The IP address of the unit is displayed.

10.3 Replacing a Device in the Link

You can substitute a different Hub or Client in a linked pair.

The devices must be in a deregistered state in order for them to be able to connect to a different device. For more information see Registered/Deregistered Devices.

To substitute a Hub or Client for a different one:

1. Switch ON the alternate ODU
2. Make sure the ODU is configured to be Hub / Client - according to its intended role in the link (same role as the ODU being replaced)
3. Make sure the link ID of the 2 devices between which you wish to establish a link - is identical.
4. Reset the Hub or Client that you want to replace (from tools->SW reboot->click “**REBOOT**”).
5. While the device is being reset, enter the browser user interface of the other ODU in the link, and deregister the link (Home-> click “**DEREGISTER**”).
6. The alternate ODU and the current ODU will now establish a link and synchronize.
7. When a link is established between the ODUs, register the link (Home -> click “**REGISTER”)**.

11 Appendixes

11.1 Web UI Events Table

The following events are supported in the system and displayed in the browser user interface.

Event text	Comments
Login attempt by <username> failed / succeeded	Login attempt to browser user interface
Ethernet Service was opened / closed	Link is active (non-active), and traffic is enabled (disabled)
Link is up	Link between Hub and Client established
Link is down due to <reason>	Link between Hub and Client dropped Possible reasons: Bad quality: link disconnected due to weak signal or high interference User request: link disconnected due to user changing air interface configuration (e.g., CBW, Channel, Tx Ratio)
Link state changed to <new state>	
LAN / SFP disconnected	LAN / SFP Cable was disconnected
LAN / SFP connected	LAN / SFP Cable was connected
Configuration was changed	
BIT succeeded - radio initialization succeeded	Internal device built-in-test on boot succeeded
ODU is Ready (Cold Start)	Device boot completed
GPS detected country is different than the user defined	User manually selected a country. The device GPS identified a different country than user selected. The new country has same regulation as previous country. Service was not interrupted.
GPS detected regulation is different than user defined	User manually selected a country. The device GPS identified a different country than user selected. The new country has a different regulation than previous country. Service was stopped. User must select a band supported by the regulation of the detected country.
SW upgrade was finished successfully to unit	
Failed to upgrade unit	

11.2 Terminology

ACRONYM	DEFINITION
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ARQ	Automatic Repeat Request
BPSK	Binary Phase-shift Keying
DIFFSERV	Differentiated Services
DL	Download
EIRP	Effective Isotropic Radiated Power
FEC	Forward Error Correction
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IP	Internet Protocol
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MCS	Modulation Coding Scheme
MIMO	Multiple Input Multiple Output
MIR	Maximum Information Rate
ODU	Outdoor Unit
OFDM	Orthogonal Frequency Division Multiplexing
POE	Power Over Ethernet
QOS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RSS	Receive Signal Strength
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier

TCP	Transmission Control Protocol
TDD	Time-Division Duplex
TX	Transmit
UL	Upload
VLAN	Virtual Local Area Network
WFQ	Weighted Fair Queueing

11.3 User Handbook Notice

11.3.1 Netronics NetStream 5x750 2G5-Plus Family

- This handbook contains information that is proprietary to NETRONICS. No part of this publication may be reproduced in any form whatsoever without prior written approval by NETRONICS.
- Right, title and interest, all information, copyrights, patents, know-how, trade secrets and other intellectual property or other proprietary rights relating to this handbook and to the NETRONICS products and any software components contained therein are proprietary products of NETRONICS protected under international copyright law and shall be and remain solely with NETRONICS.
- The NETRONICS name is a registered trademark of NETRONICS. No right, license, or interest to such trademark is granted hereunder, and you agree that no such right, license, or interest shall be asserted by you with respect to such trademark.
- You shall not copy, reverse compile or reverse assemble all or any portion of the Configuration Guide or any other NETRONICS documentation or products. You are prohibited from, and shall not, directly, or indirectly, develop, market, distribute, license, or sell any product that supports substantially similar functionality based or derived in any way from NETRONICS products. Your undertaking in this paragraph shall survive the termination of this Agreement.
- This Agreement is effective upon your opening of a NETRONICS product package and shall continue until terminated. NETRONICS may terminate this Agreement upon the breach by you of any term thereof. Upon such termination by NETRONICS, you agree to return to NETRONICS any NETRONICS products and documentation and all copies and portions thereof.
- For further information contact NETRONICS or contact your local distributor.

11.3.2 Disclaimer

The parameters quoted in this document must be specifically confirmed in writing before they become applicable to any order or contract. NETRONICS reserves the right to make alterations or amendments to the detail specification at its discretion. The publication of information in this document does not imply freedom from patent or other rights of NETRONICS, or others.

11.3.3 Trademarks

- Netronics NetStream 5x750 2G5 is a trademark of NETRONICS