



Pyxis Duo Router Manual

Issue 1.2 –2025

This document contains proprietary information and must not be provided or copied to third parties without express permission from Ubiik Inc.

Ubiik Inc.

Issue 1.2 –2025
Pyxis Duo Product Manual

Disclaimer

While precaution has been taken in the preparation of this literature and it is believed to be correct at the time of issue, Ubiik Inc. assumes no liability for errors or omissions or for any damages resulting from the use of this information. Due to a policy of continuous technical improvement, the contents of this document and any specifications contained therein are subject to revision and may change without notice.

Introduction

Purpose of this Manual

The Pyxis Duo LTE Router User Manual provides comprehensive, detailed instructions for the installation, configuration, operation, and maintenance of your Pyxis Duo LTE Router. It is designed to guide you through each process step-by-step, ensuring successful deployment and operation.

Intended Audience

This manual is written specifically for:

- Field technicians performing hardware installation.
- Network engineers configuring LTE and network settings.
- IT administrators managing network operations and maintenance.

Configuration Scope

This manual covers local GUI configuration capabilities available through the web interface. Advanced features may require:

- SSH/CLI access for complex setups
- goNMS for network-wide management
- Technical support for specialized deployments

For advanced configuration assistance, contact: support@ubiik.com

Regulatory Compliance & Safety

Certification for this product is pending for the following regions:

Region	Certification	Standard
Brazil	ANATEL	ATO 915/2024, ATO 2091/2025, Resolution 680/2017
USA	FCC	Part 15, Part 22, Part 24, Part 27
Canada	ISED	RSS-Gen, RSS-102
Europe	CE/RED	EN 301 489, EN 300 328
Global	Safety	IEC 62368-1

FCC Statement

The Pyxis Duo complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial or industrial installation. This device generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this device does cause harmful interference to radio or television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one of the following measures.

Table 1.1 Approaches to correcting interference

Method	Action
1	Reorient or relocate the receiving antenna
2	Increase the separation between the device and receiver
3	Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
4	Consult the dealer or an experienced RF technician for help

CAUTION!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this device.

RF Exposure Compliance

To comply with applicable international RF exposure regulations (including FCC and ANATEL):

- Maintain at least **25 cm** separation between the antenna and any person during operation.
- Do not exceed the maximum antenna gain or radiated power (EIRP) specified by the regional authority.
- If the Wi-Fi and LTE antennas are co-located (less than 25 cm apart), use the **lower permitted antenna gain**.

For detailed RF exposure guidance, refer to your regulatory region's guidelines, e.g. FCC OET Bulletin 65.

Safety statement

All instructions, warning and caution statements that accompany this device must be strictly followed at all times to ensure its safe use. Observe all warning and caution symbols that are fixed to this device. This device has been designed with the utmost care for the safety of installers and users. However, when using this device, basic safety precautions should always be followed to reduce the risk of injury and electric shock. Do not cover the device or block the airflow to the device with any other objects. This device was qualified under test conditions that included the use of the supplied cables between system components.

To comply with regulations, the user must use the cables supplied with the unit (including power adapter) and follow the installation guide. Place the unit to allow for easy access when disconnecting the power adapter from the main wall outlet. Operate this device only with the type of power source indicated on the marking label. If you are not sure of the type of power supplied to your facility, consult your dealer or local electricity provider.

Do not use this product near water, for example a swimming pool or a bathroom. Keep the device away from excessive heat and humidity and keep the device free from vibration and dust. Wipe the unit with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the unit or use forced air to remove dust.

Avoid installing or using this product during an electrical storm - there may be a remote risk of electric shock from lightning. During electrical storms, for added protection from lightning or power surges we suggest unplugging the unit from the wall outlet and disconnecting all cables. For safety reasons, only authorized service technicians should open the device. If the device is opened the warranty will become void. The device may also affect medical equipment – we recommend checking any potential impact on medical equipment prior to use. This device, like other radio devices, emits radio frequency electromagnetic energy, but operates within the guidelines found in radio frequency safety standards and recommendations. It is recommended that the minimum operating distance from the installed Base Station to person is 19.68 inches (50cm).

Professional installation statement

1. Installation personnel: This device is designed for specific applications and needs to be installed by qualified personnel who have RF and related regulations knowledge. The general user should not attempt to install or change the settings.
2. Installation location: The device should be installed at a location where the radiating antenna can be kept 19.68 inches (50 cm) from any nearby person in normal operating conditions to meet regulatory RF exposure requirements.
3. Installation procedure: Please refer to the procedure for mounting the device to a wall or pole.
4. Warning: Please carefully select the installation position and make sure that the final output power does not exceed the limits set in relevant rules. Violation of rules could lead to serious federal penalties.

General hazard statement

Safety notes are marked with symbols. Ignoring the safety notes may lead to personal injury, damage to the instrument and malfunctions. Signal Words identify the hazard severity level as the following:

Table 1.5 Safety notes

Word	Meaning
DANGER	Indicates an extremely hazardous situation which, if not avoided, will result in death or serious injury, permanent damage to equipment or large fines and penalties
WARNING	Indicates a hazardous situation which, if not avoided, could result in serious injury or damage to equipment and moderate fines or penalties
CAUTION	Indicates a hazardous situation which, if not avoided, could result in minor injury or minor damage to equipment or minor to moderate penalty fees
NOTICE	Indicates a hazardous situation not related to personal injury or damage to equipment

Electrical Safety Guidelines

Follow these guidelines carefully:

- Connect only to power sources within the specified 9-60 VDC range.
- Ensure correct polarity is maintained.
- Securely ground the router using one of the unused mounting screw locations.

Handling and Operational Safety

- Operating temperature: -40°C to +65°C.
- Avoid installation in environments containing explosive materials unless specifically rated.
- Be cautious of heated surfaces during prolonged operation.

Introduction.....	3
Regulatory Compliance & Safety.....	4
1 Product Overview.....	10
1.1. Pyxis Duo Architecture	10
1.2. Cellular Technology Implementation.....	10
1.4. Industrial Interface and Positioning Capabilities	11
1.5. Network Integration and Security.....	11
1.6. Environmental Design	11
1.7. Target Applications	12
1.8. Accessories.....	12
1.9. Connectors & LEDs.....	12
1.9.1 Ethernet 1 and 2.....	12
1.9.2 Serial 1 and 2.....	12
1.9.3 RS232 Full Duplex Pin Out.....	13
1.9.4 RS485 Half Duplex Pin Out.....	13
1.9.5 GPIO	13
1.9.6 GNSS	14
1.9.7 Cellular A & Cellular B	14
1.9.8 Wi-Fi	14
1.9.9 RST	14
1.9.10 LED Behaviour	14
1.10 Basic Network Architecture	15
1.11 Management Capabilities	15
1.12 SIM Installation	17
1.13 Hardware Specifications	17
1.14 Environmental and Mechanical Specifications	20
1.15 Mounting Solutions.....	22
1.16 Enterprise Authentication.....	24
2 Power Requirements & I/O Ports.....	25
2.1 Voltage Range	25
2.2 Power Consumption.....	25
2.3 Supply Polarity	26
2.4 Grounding	26
2.5 Supply Noise.....	27
2.6 Operating from AC Mains	27
3 First Log In	28
3.1 Password Change	28
3.2 Remote Management	28
3.3 Access to local management interface	29
3.4 Set date and time	29
3.5 Logging	31
3.6 - First-Time Security Hardening (MANDATORY)	32
3.7 Installation Commissioning Checklist.....	33
4 Advanced Networking Features - LAN & WAN Configuration	35
4.1 Change LAN IPv4 address.....	35
4.2 DHCP server settings.....	36
4.3 Add static DHCP reservations	38
4.4 Add static host name entries	38
4.5 Add static ARP entries.....	39
4.6 LTE Settings (APN).....	40
4.7 Wi-Fi	40
4.8 Create VLANs.....	44
4.9 Application Layer Gateway (ALG)	47
4.10 GRE Tunnels (VPN) Configuration	47

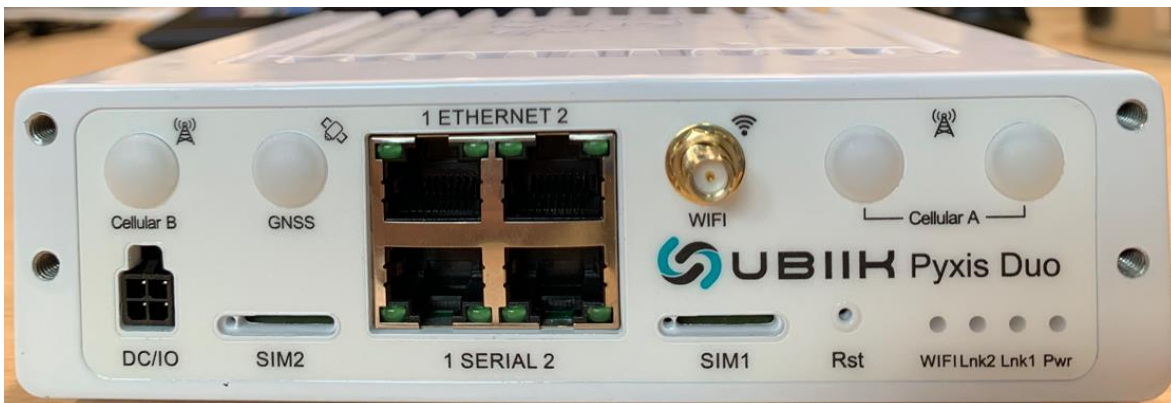
4.11 Routing	49
4.12 Serial Ports	53
4.13 Industrial Protocol Network Configuration	56
4.14 Define Quality of Service (QoS)	57
4.15 Multiple WAN Configuration	59
4.16 Network Architecture Examples	62
4.16.1 goRAN™ with Embedded EPC (Standalone Private Network)	62
4.16.2 goRAN™ with External EPC (Distributed Core Network)	63
4.16.3 Multi-vendor 3GPP Compliant Network	63
5 Firewall & Security	64
5.1 General Settings	64
5.2 Port Forwarding	64
5.3 Port Trigger	65
5.4 Traffic Rules	66
5.5 Denial of Service (DOS) prevention	68
5.6 DMZ Host	69
6 Services Features & Settings	70
6.1 UPnP and NAT-PMP	70
7 Administrator Features	71
7.1 Manage access to local management interface	71
7.2 Create time schedules	72
7.3 Diagnostic tools	74
7.4 Backup and restore configuration settings	78
7.5 Reboot	80
7.6 Reset to factory settings	80
7.7 Ping Watchdog	81
7.8 GPIO Settings	82
7.9 Firmware Management	83
8 Status Features	85
8.1 Status Overview	85
8.2 LTE Status	87
8.3 Real Time Graphs	87
8.4 View routing table and ARP entries	89
8.4.1 Key Performance Indicators (KPI) Monitoring	90
8.5 Logging	92
9 Maintenance & Lifecycle Management	93
9.1 Preventive Maintenance Schedule	93
9.2 Field Deployment Checklist	94
9.3 Performance Monitoring	95
9.4 Performance Optimization Techniques	95
10 How to ... Access Devices Behind Pyxis	96
10.1 WAN Configurations	96
10.2 LAN Configurations	96
10.3 Change Radio Access Technology between NB-IOT & LTE-M	97
10.4 Real-World Application Examples	97
10.4.1 SCADA System Integration over LTE	97
10.4.2 Industrial IoT Gateway with Protocol Conversion	98
10.5 Utility Application Integration	98
11 Troubleshooting & Support	101
11.1 Systematic Troubleshooting Methodology	101
11.1.1 Level 1, Basic Diagnostics (5 minutes)	101
11.1.2 Level 2, Intermediate Diagnostics (15 minutes)	101
11.1.3 Level 3, Advanced Diagnostics (30+ minutes)	102

11.2 Common Issues and Solutions Matrix.....	103
11.3 3GPP Interoperability Troubleshooting	104
11.4 Technical Support	104
11.5 Emergency Recovery Procedures	105
12 Ordering Information	106
12.1 goRAN™-Specific Information:.....	106
Appendix A: Quick Reference Cards	107
Appendix B: Port and Protocol Reference	108
Appendix C: Power Supply Selection	109
Document History	111

1 Product Overview

1.1. Pyxis Duo Architecture

The Pyxis Duo is a Wi-Fi platform for dual-radio edge gateway ready to enable Cat-4/Cat-1 LTE and 5G LPWA technologies including LTE-M, and NB-IoT. The platform supports iSIM and dual physical SIM with eSIM capability, providing comprehensive connectivity to Ubiik's goRAN™ private LTE networks, public cellular networks, and NTN satellite systems. Each LTE module in the Pyxis Duo router is independent, featuring dedicated antennas, SIM slots, and RF pathways. Offers simultaneous operation on separate networks plus automatic failover from primary to secondary LTE modules.



3GPP Standards Compliance & Network Interoperability

The Pyxis Duo is a Wi-Fi router platform, when enabled with Cat-4/Cat-1/Cat-M/Cat-NB connectivity ensures seamless interoperability with:

- Ubiik goRAN™ eNodeB base stations with embedded EPC
- Any 3GPP-compliant eNodeB (Nokia, Ericsson, Huawei, Samsung, etc.)
- Standard EPC/5GC core networks
- Any 3GPP User Equipment (UE) on the same network

This standards-based design enables:

- Vendor-agnostic network deployment
- Future-proof investment protection
- Seamless handover between different base station vendors
- Integration with existing cellular infrastructure

1.2. Cellular Technology Implementation

The dual-module Wi-Fi router architecture is compatible with M.2 & mPCIe modules of the following technologies:

Technology	Band
Cat-NB	B1, B3, B5, B8, B20, B28, B31, B72, B73, B87, B88, B103, Space Data 900 MHz

Cat-M	B1, B2, B3, B4, B5, B6, B8, B9, B10, B12, B13, B14, B15, B16, B17, B18, B19, B20, B23, B25, B26, B28, B31, B66, B72, B73, B85, B87, B88, B106, B107, B111, ISM-FDD, ISM-TDD
NTN	N255, 256
Cat-1 LTE	B1, B3, B5, B8, B18, B19, B26, B28, and Anterix B8
Cat-4 LTE	B2, B48, B54, B66, B54+B48 CA

The implementation complies with ANATEL regulatory requirements including Acts 915, 773/2025, and 16539/2023, with performance operating within regulatory channel bandwidth constraints of 5MHz maximum.

1.4. Industrial Interface and Positioning Capabilities

The platform provides dual Gigabit Ethernet ports and dual RS232/485 serial interfaces for comprehensive industrial connectivity. GPIO functionality supports sensor and control applications, while integrated WiFi 6 capability operates on 2.4GHz for local networking requirements. Built-in GNSS capability provides precise positioning and time synchronization services for location-dependent applications and network synchronization.

The system accepts 9-60 VDC power input for flexible deployment across various power infrastructure environments, with full IPv4 and IPv6 protocol support ensuring compatibility with modern network infrastructures and future-ready connectivity.

1.5. Network Integration and Security

Integration with Ubiik's goRAN™ infrastructure and goNMS management platform enables centralized network control and monitoring. The platform supports automatic failover between private LTE, public cellular, and NTN satellite connectivity, ensuring continuous operation across diverse network conditions.

The system implements comprehensive cybersecurity measures including secure SIM management with iSIM technology, encrypted communications across all network interfaces, and secure management protocols. The 3GPP-compliant design enables operation with any standards-compliant base station technology while maintaining enterprise-grade security standards.

1.6. Environmental Design

Operating temperature: -40°C to +65°C."

The platform operates across extreme temperature ranges from -40°C to +65°C for industrial deployment environments. The compact design measures 123.7 x 151.9 x 41.91 mm and weighs 0.77 kg, enabling flexible mounting options for diverse installation scenarios.

1.7. Target Applications

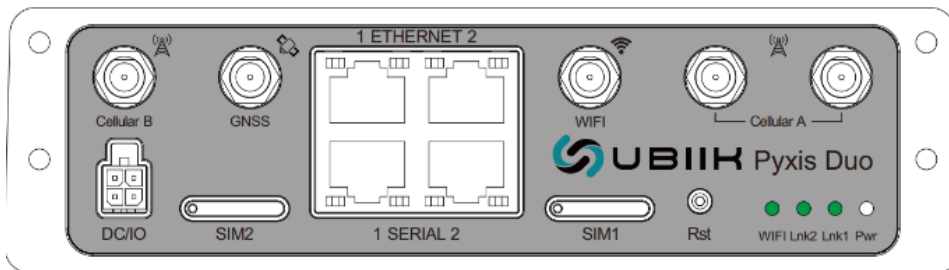
The system is prepared to addresses connectivity requirements for utilities use cases such as SCADA systems, Advanced Metering Infrastructure and Distributed Energy Resources, industrial automation, Smart City applications, Transportation Networks and remote site monitoring. The comprehensive failover architecture and industrial interface capabilities make it suitable for mission-critical applications requiring guaranteed connectivity and integration with existing industrial infrastructure.

1.8. Accessories

Pyxis Duo does not come with any accessory.

1.9. Connectors & LEDs

The diagram below labels each of the different connectors and LEDs.



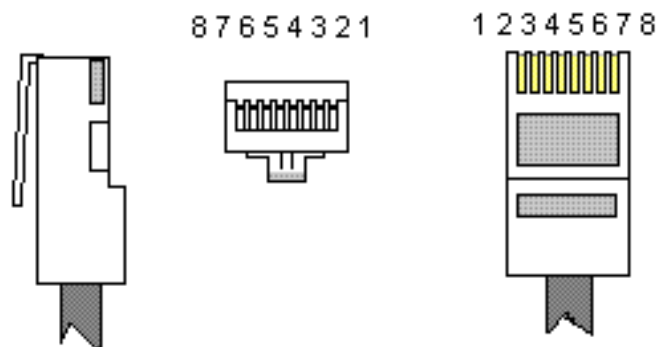
1.9.1 Ethernet 1 and 2

Two shielded RJ45 sockets provide the Ethernet connections to ethernet 1 and 2.

The Ethernet ports are both 10/100/1000 Mbps BASE-T ports.

1.9.2 Serial 1 and 2

Two shielded RJ45 sockets provide the serial port connection. They can be configured via the web GUI to allow data to flow to a TCP server.



1.9.3 RS232 Full Duplex Pin Out

Signal Name	Pin number	Direction
Tx Data	6	Out of radio
Rx Data	5	Into radio
Ground	4	n/a

Note: It is recommended to use Ethernet cable with shielding when connecting peripheral equipment through serial port.

1.9.4 RS485 Half Duplex Pin Out

Signal Name	Pin number	Direction
Data n	6	In/Out of radio
Data p	8	In/Out of Radio
Ground	4	n/a

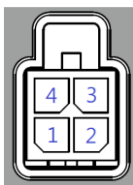
Note: It is recommended to use Ethernet cable with shielding when connecting peripheral equipment through serial port.

1.9.5 GPIO

Two GPIO pins are available on the DC connector. The GPIO modes supported are:

- 1) Digital Push-pull output 5V
- 2) Digital Open Collector output, up to 24V pull up, requires 10k external resister
- 3) 5V Digital input

The GPIO connector is shared with the DC input, the pinout is below.



Pin Number	Name	Description
1	Ground	Ground for DC input
2	Positive	9-60V / 1.5A DC power input (single module)

		9-60V / 2A DC power input (dual-module)
3	Digital GPIO 1	Push-pull output / Open Collector output / Digital input
4	Digital GPIO 2	Push-pull output / Open Collector output / Digital input

1.9.6 GNSS

A GNSS receiver is built in, an external antenna is required and is connected via a SMA connector on the front of the Pyxis DUO.

A passive GNSS antenna with SMA connection is required if GNSS is being used and should be fitted in a location with a view of the sky. Please refer to section 4.6 LTE Setting (APN), point #3 *SIM Binding*.

1.9.7 Cellular A & Cellular B

Cellular A and Cellular B are antenna connectors corresponding to the LTE/LTE-M modules integrated within the Pyxis Duo. Each connector is dedicated to one of the internal cellular modules to ensure proper signal transmission and reception.

1.9.8 Wi-Fi

The Wi-Fi connector is used for the 2.4 GHz Wi-Fi 6 (802.11ax) antenna.

1.9.9 RST

Pressing the Reset button will restore the Pyxis Duo to its factory default settings.

1.9.10 LED Behaviour

The LEDs indicate the following:

Pyxis Duo	Color	Definition
Pwr	White	ON: power on OFF: power off
Link1	Green:	ON: connected OFF: initialization failed Blinking: no connection
Link2	Green	ON: connected OFF: initialization failed Blinking: no connection
Wi-Fi	Green	ON: link OFF: no link

		Blinking: data Tx/Rx
Ethernet port	Green	Left: ON: 1G link OFF: 10/100 link / no link Right: ON: link OFF: no link Blinking: Data Tx/Rx
Serial port	Green	Always OFF

1.10 Basic Network Architecture

The diagram below outlines the basic network architecture to connect Pyxis Duo router with goRAN™ base station when enabled with backhaul connectivity of Cat-4, Cat-1, Cat-M, and Cat-NB type:



1.11 Management Capabilities

The Pyxis Duo can be managed via either goNMS Server (centralized remote management) or the web GUI (local management)

Pyxis Duo

Auto Refresh on

Network

LAN

WAN

Wireless

VLAN

GRE

Firewall

Application

Routing

Serial

QoS

Multiple WAN

Services

Administrator

Status

Log out

LAN

This section allows you to modify the router's LAN IP address interface settings. Typically, the router LAN IP address settings do not need to be changed. In addition, this page allows you to configure the router's LAN DHCP server/relay settings or DHCP reservations/static leases which automatically assigns IP addresses to the wired and wireless devices that connect to your router. The router can also function as a name server and allows you to manually enter customized host names to resolve to the IP addresses of devices on your local network.

Common Configuration

General Setup

Advanced Settings

Status

Uptime: 6h 36m 20s

MAC address: 0E-49-5F-1F-F8-EE

RX: 2.96 MB

TX: 18.34 MB

IPv4: 192.168.10.1/24

Mode

NAT

IPv4 address

192.168.10.1

IPv4 netmask

255.255.255.0

DHCP Server / Relay

General Setup

Advanced Settings

DHCP mode

Enable

DHCP (Dynamic Host Configuration Protocol) disable/enabled relay

Start address

192.168.10.101

DHCP (Dynamic Host Configuration Protocol) start address

End address

192.168.10.199

DHCP (Dynamic Host Configuration Protocol) end address

1.12 SIM Installation

The Pyxis Duo accommodates two standard Nano SIM cards (12.3 × 8.8 mm).

Use the eject pin to remove the SIM1 and SIM2 socket tray, then insert the corresponding SIM cards into their respective slots..

Note: The installed SIMs can be re-assigned to the modules during operation on the WEBGUI, and no physical insertion/removal of the SIMs is needed. Physical SIM installation/removal requires device power-off.

SAFETY: Always power off the device before inserting/removing SIM cards



1.13 Hardware Specifications

Processing and Memory

Component	Specification	Notes
CPU	Quad-core ARM Cortex-A53, 1.2 GHz	Industrial temperature rated
RAM	1 GB DDR3	ECC supported
Flash Storage	8 GB eMMC	Wear-levelling enabled

Wi-Fi 6 (802.11ax) Specifications

Parameter	Specification	Notes
Standard	IEEE 802.11ax (Wi-Fi 6)	2.4 GHz only

Parameter	Specification	Notes
Frequency Range	2400-2483.5 MHz	Global ISM band
Channel Width	20/40 MHz	Configurable
Max PHY Rate	287 Mbps (40 MHz)	With 1024-QAM
MIMO	1x1 SISO	Single spatial stream
Output Power	19 dBm	Regulatory compliant
Rx Sensitivity	-94 dBm @ 6 Mbps	802.11ax rates
Security	WPA3-Personal/Enterprise	Backward compatible WPA2

Ethernet Interface Specifications

Parameter	Port 1	Port 2
Standard	IEEE 802.3ab	IEEE 802.3ab
Speed	10/100/1000 Mbps	10/100/1000 Mbps
Duplex	Full/Half	Full/Half
Auto-negotiation	Yes	Yes
Connector	RJ45 shielded	RJ45 shielded
Isolation	1.5 kV RMS	1.5 kV RMS
Cable Length	Up to 100m Cat5e/6	Up to 100m Cat5e/6

Serial Interface Specifications

Parameter	Serial 1	Serial 2
Standards	RS232/RS485	RS232/RS485
Baud Rates	300-115200 bps	300-115200 bps
Data Bits	7, 8	7, 8

Parameter	Serial 1	Serial 2
Stop Bits	1, 2	1, 2
Parity	None, Even, Odd	None, Even, Odd
Flow Control	NON	NON
Isolation	NA	NA
Connector	RJ45	RJ45

Note: It is recommended to use Ethernet cable with shielding when connecting peripheral equipment through serial port.

Performance Benchmarks

Metric	Specification	Notes
Boot Time	<60 seconds to full operation	Typical startup time
LTE Attach Time	<30 seconds typical	Network dependent
Concurrent Sessions	1000+ simultaneous	Maximum capacity
Throughput	140+ Mbps actual	Under optimal conditions
Latency	<25ms LTE, <5ms Wi-Fi	Typical values
Wi-Fi Standard	IEEE 802.11ax (Wi-Fi 6)	287 Mbps maximum
Power Consumption	3.5W idle, 11.4W peak	Standard operating range
Temperature Range	-40°C to +65°C	Operating specification

1.14 Environmental and Mechanical Specifications

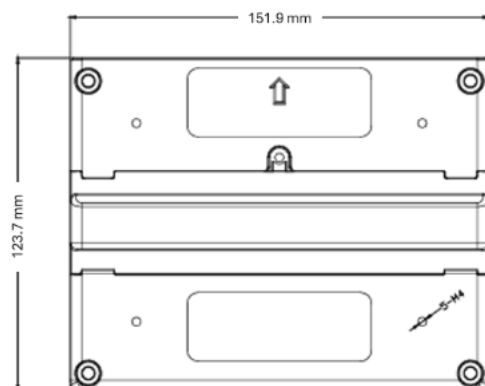
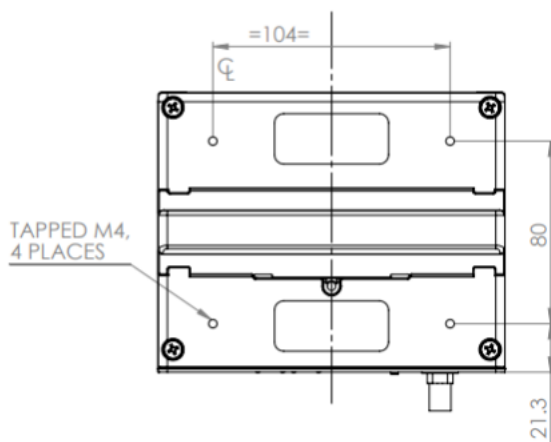
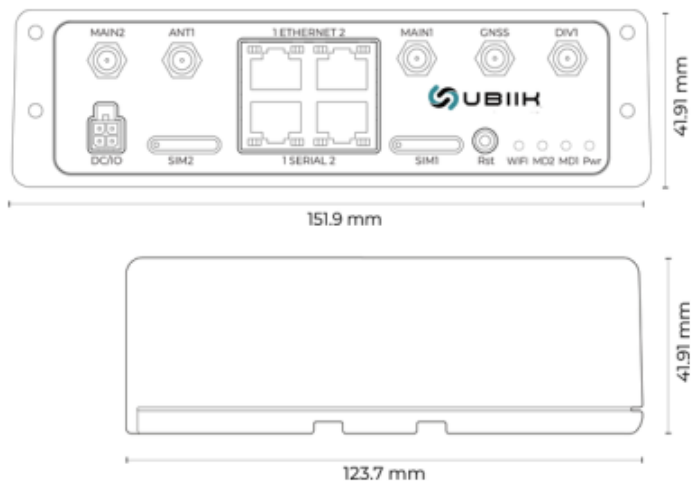
Environmental Operating Conditions

Parameter	Minimum	Maximum	Notes
Operating Temperature	-40°C	+65°C	Full specification range
Storage Temperature	-40°C	+85°C	Non-operating
Relative Humidity	5%	95%	Non-condensing
EMC	EN 301 489	Class B emissions	Industrial environments

Mechanical Specifications

Parameter	Dimension	Tolerance
Length	151.9 mm	±0.5 mm
Width	123.7 mm	±0.5 mm
Height	41.9 mm	±0.5 mm
Weight	0.77 kg	±50g

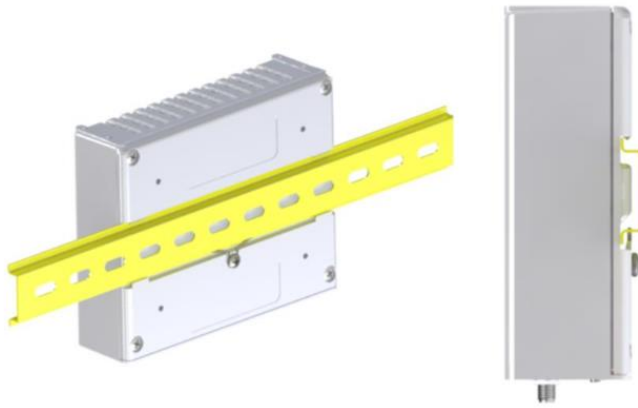
Mechanical Drawings



1.15 Mounting Solutions

Pyxis radios can be mounted in several different ways to meet the customers application. These include:

DIN Rail Mounting



Pyxis mounting on TS35 DIN Rail

Wall/Surface Mounting



1U Rack Mounting



1.16 Enterprise Authentication

SSH authentication via an external RADIUS server is available, and for more details or other enterprise authentication methods please contact technical support.

2 Power Requirements & I/O Ports

2.1 Voltage Range

The Pyxis Duo supports typical utility requirements of 48VDC with a wide operating input voltage range of 9 to 60 VDC.

This means that the voltage must not rise above 60 VDC under idle conditions or fall below 9 VDC at full load.

The input current is 0.19-1.9A depending on voltage and load.

2.2 Power Consumption

Idle (standby)	3.5W
Cat-4 LTE operation	5.2W - 8.1W
Cat-M/NB-IoT operation	4.5W - 6.6W
Peak (maximum operation)	11.4W

* Standard configuration includes GPS and Wi-Fi active

* All measurements with single cellular service active. No external modules required

Power Consumption by Input Voltage

DC Input Voltage	Standby Current	Full Load Current	Power Consumption
9V	0.54A	0.9A	8.1W
12V	0.37A	0.87A	10.44W
24V	0.21A	0.42A	10.08W
48V	0.11A	0.22A	10.56W
56V	0.10A	0.20A	11.2W
60V	0.11A	0.19A	11.4W

2.3 Supply Polarity

The power cable is wired to Pin 1 (Ground) and Pin 2 (Positive). The required connector for the Power supply cable is E.C.I 3016H-04 (2*2) housing and 3016 crimp terminals.

A 2-meter-long pre-connectorized DC cable is included inside each box containing a Pyxis DUO.



2.4 Grounding

The radio unit case must be grounded through an external earth strap – see image below.

Any of the unused mounting screw points can be used with an appropriate star washer. Generally, this is done to the local rack frame, which in turn should be part of a well-designed station grounding system.

This internal grounding is intended for EMC compliance and transient protection.

Grounding Requirements:

- Ground connection: M4 screw point (marked with $\perp$ symbol)
- Ground resistance: <5 ohms to building ground
- Ground wire: Minimum 2.5 mm² copper conductor
- Connection: Star washer required for reliable connection

This grounding is mandatory for ANATEL certification compliance and essential for protection against electrical transients in utility environments.



2.5 Supply Noise

Regardless of the EMC provisions in the equipment, power wiring from the DC source should not be shared with other equipment that may introduce excessive noise. Nor should the power cables to the unit be run alongside cables that connect to other equipment that may produce high current noise or transients, e.g. power relays.

2.6 Operating from AC Mains

AC-DC 'plug pack' power supplies are available from Ubiik with the required power (see Appendix D for recommended Power Supplies).

3 First Log In

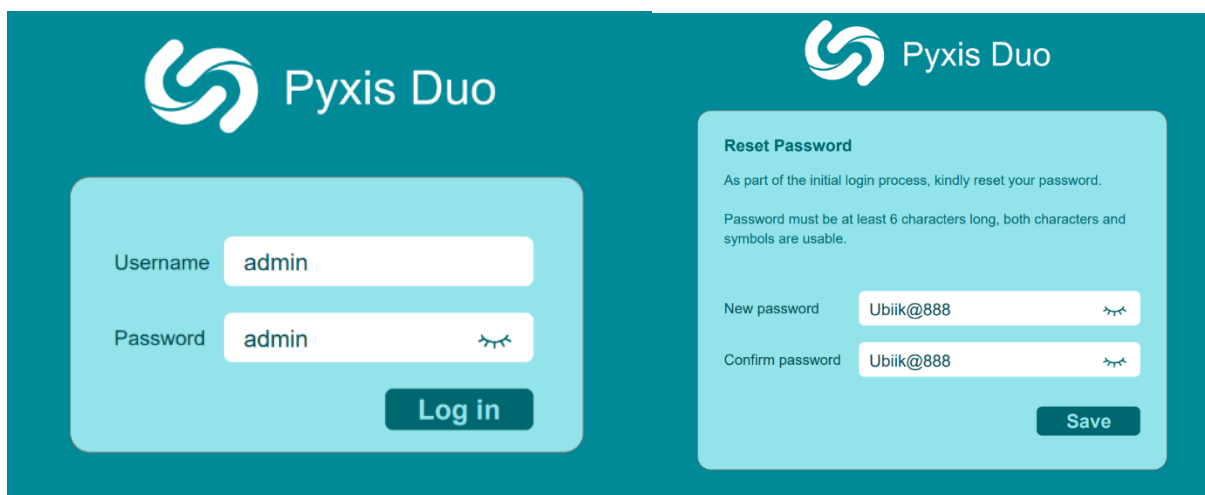
3.1 Password Change

With the first-time log-in to Pyxis Duo's **local web interface**, the user is required to change the password.

1. Log into your router management page
2. Click on **Administrator** and click on **Administration**.

The new password must be at least 6 characters long, and both characters and symbols are usable. After completing the change, the user may log in again with the new password.

Note: If you change the administrator password, you will need to access the router management page using the username "admin" and the new password instead of the pre-configured default password of "admin". If you reset the device to factory defaults, you will need to access the router management page using the pre-configured default settings.

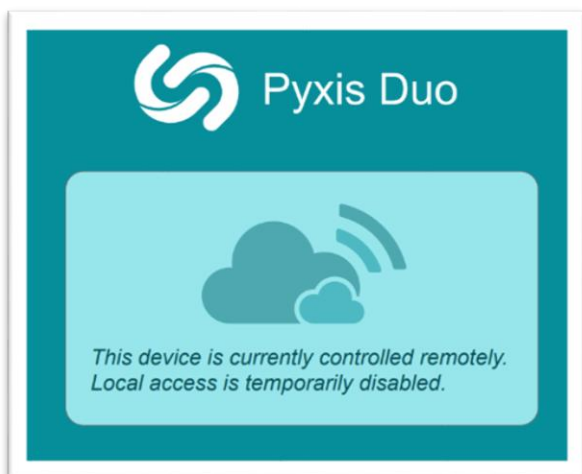


The image displays two side-by-side screenshots of the Pyxis Duo web interface. The left screenshot shows the login page with the Pyxis Duo logo at the top. Below the logo is a light blue box containing two input fields: 'Username' with the value 'admin' and 'Password' with the value 'admin'. A 'Log in' button is located at the bottom right of this box. The right screenshot shows the 'Reset Password' page. It features the Pyxis Duo logo and the title 'Reset Password'. Below the title, there is a message: 'As part of the initial login process, kindly reset your password.' followed by a note: 'Password must be at least 6 characters long, both characters and symbols are usable.' There are two input fields: 'New password' and 'Confirm password', both containing the text 'Ubiik@888'. A 'Save' button is located at the bottom right of this section.

3.2 Remote Management

When accessing the local WEBGUI if the below image is displayed, this means the Pyxis DUO has been configured to allow management via goNMS only.

Therefore, unless configured otherwise, the access to Pyxis Duo via the local WEBGUI has been denied to the user.



3.3 Access to local management interface

1. The default IP address to connect to the local web interface is <https://192.168.10.1>. Note that it might be different if a new IP has been set up – see the Quick Start Guide for further details.

2. The Pyxis router will prompt for a username and password.

The default username and **password** is “admin,” and users are required to change password with first log in. After password change, users can login in with the new password.

Note: Username and Password are case sensitive.

3. Save and apply changes

For new parameters to take effect, the local interface offers all or some of the options below.



Note that some configuration changes may require a device reboot.

- **Apply** – Apply the configuration changes on a specific page which will take effect immediately
- **Save** – Temporarily save the changes on a specific or multiple configuration page(s). Click on the “Unsaved Changes” button on the upper right corner of the web page to check the details and apply all configuration changes at once
- **Cancel** – Discard changes

3.4 Set date and time

Administrator > System

It is recommended to set the router date and time for scheduling functions and logging functions for monitoring and troubleshooting.

1. Log into your router Administrator page
2. Click on **System**.

3. Review the settings below. Click **Apply** to save and commit the changes.

System Properties

- **Local Time** – Displays the current day, date, and time.
- **Hostname** – Modifies the router host name. The host name is the name used to identify the router to other computer or devices on the network. Modifying this setting will modify the hostname used when accessing the router management page using the hostname.
- **Timezone** – Click the drop-down list to select the appropriate time zone.

The screenshot shows the Pyxis Duo web interface. The left sidebar has a menu with 'Network', 'Services', 'Administrator', 'System' (selected), 'Administration', and 'Schedule'. The main content area is titled 'System' and contains a sub-section 'System Properties'. It displays three settings: 'Local Time' showing 'Thu Oct 17 10:26:06 2024', 'Hostname' set to 'PyxisDuo', and 'Timezone' set to 'UTC' with a dropdown arrow.

There is an option to enable or disable the **daylight saving**, configure offset and to schedule the same.

The screenshot shows the 'Daylight Saving Time' configuration section. It features a label 'Daylight Saving Enable' followed by a dropdown menu currently set to 'Disabled'.

Time Synchronization

Clock Mode – Select the method of clock mode

- **Local Time:** Manually input the time

The screenshot shows the 'Date/Time Setting' configuration page. The 'Clock Mode' is set to 'Local Time'. Below this, there are date and time settings: 'Date Settings' with Year (2025), Month (Jul), and Day (16); and 'Time Settings' with Hour (10), Minute (50), and Second (55). Each value is in a dropdown menu.

- **NTP:** Time is grabbed from a designated NTP server

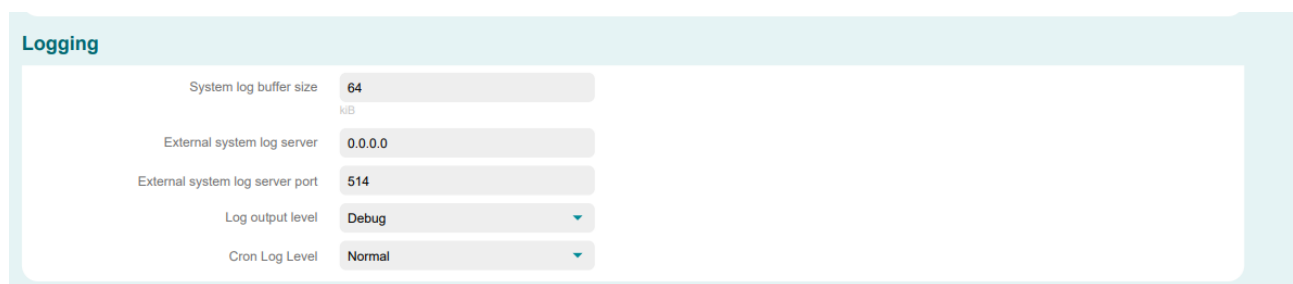
The screenshot shows the 'Date/Time Setting' configuration page with 'Clock Mode' set to 'NTP'. Below this, there is a field for 'NTP server candidates' with the value 'time.ami.ubiik.com' and a small icon to the right.

- **NTP server candidates** – Enter the domain name of the network time server to obtain time and settings. (e.g. pool.ntp.org)
- An optional license is available for Cloud Sync Time which enables the time to be synched with the Ubiik cloud server

Note: You can add multiple time servers by clicking the  icon next to the NTP Server candidate domain name. If one server is not available, your router will try the next available server in the list.

3.5 Logging

- **System log buffer size** – The system log buffer size in 64KB, 128 KB, 256 KB, and 512 KB can be configured.
- **External system log server** – The logs can be redirected to an external syslog server which requires the server IP address configuration.
- **External system log port** – The port number for communication with log server.
- **Log output level** – The system log severity level is defined in below table.
- **Cron log Level** – The log level for cron logs.



System log Severity level

Severity	Description	Condition
Emergency	System is unusable	A panic condition
Alert	Action must be taken immediately	A condition that should be corrected immediately, such as a corrupted system database
Critical	Critical conditions	Hard device errors
Error	Error conditions	
Warning	Warning conditions	
Notice	Normal but significant conditions	Conditions that are not error conditions, but that may require special handling.
Informational	Informational messages	Confirmation that the program is working as expected.
Debug	Debug-level messages	Messages that contain information normally of use only when debugging a program

3.6 - First-Time Security Hardening (MANDATORY)

Immediate Security Actions:

1. **Change Admin Password** - minimum 12 characters with mixed case, numbers, symbols
2. **Enable HTTPS** - disable HTTP in System > Administration > Access Control
3. **Change Wi-Fi Credentials** - new SSID and WPA3 password
4. **Configure Firewall** - enable default-deny policy
5. **Disable Unused Services** - Telnet, unnecessary protocols
6. **Set Time/NTP** - accurate time critical for security

Post-deployment Verification:

- ☐ All LEDs showing normal status
- ☐ Internet connectivity confirmed (ping test)
- ☐ Signal strength acceptable (RSRP > -100 dBm)
- ☐ Security settings applied
- ☐ Configuration backed up
- ☐ Documentation completed

3.7 Installation Commissioning Checklist

Purpose: Professional installation verification to ensure optimal performance and warranty compliance.

Phase 1: Pre-Installation Verification (5 minutes)

- Signal strength survey completed (minimum -100 dBm RSRP at location)
- Power source verified (stable 9-60 VDC supply within specifications)
- Grounding point identified and accessible
- Environmental conditions within -40°C to +70°C range
- Antenna mounting locations selected with clear line-of-sight
- ANATEL compliance verification: Band 31 antennas ≤ 9 dBi gain

Phase 2: Installation Quality Verification (10 minutes)

- Device securely mounted using appropriate bracket type
- Grounding strap connected to designated ground point (marked $\perp$)
- Ground resistance verified < 5 ohms to building ground
- All antenna connections tight and weatherproofed (outdoor installations)
- Power connection verified: Pin 1 (Ground), Pin 2 (Positive)
- Cable routing provides 50cm minimum clearance for maintenance access
- ERP calculation verified: Module power + Antenna gain ≤ 35 dBm

Phase 3: Functional Testing (15 minutes)

- Power LED solid white (normal operation confirmed)
- LTE LEDs solid green (both modules registered and operational)
- Wi-Fi LED active (wireless functionality confirmed)
- Ethernet link LEDs active (network connectivity established)
- Web interface accessible at configured IP address
- Internet connectivity test passed (ping 8.8.8.8 successful)
- Signal strength meets acceptance criteria (RSRP > -100 dBm)

Phase 4: Security and Configuration (10 minutes)

- Default admin password changed to strong credentials (12+ characters)
- HTTPS enabled and HTTP access disabled
- Wi-Fi security configured (WPA3 preferred, minimum WPA2)
- Firewall rules configured per security requirements
- System time/NTP configured for accurate logging
- Complete configuration backup created and stored

Phase 5: Documentation and Handover (5 minutes)

- Installation parameters documented (signal levels, IP configuration)
- Performance baseline recorded (throughput, latency measurements)
- Customer training completed (basic operation and monitoring)
- Maintenance schedule established and documented
- Warranty registration completed with Ubiik support
- ERP compliance documentation completed and retained

Acceptance Criteria:

- Signal Strength: RSRP >-100 dBm minimum
- Internet Throughput: >80% of carrier specification
- Latency: <50ms to public servers
- System Temperature: Within -40°C to +70°C range
- All configuration items completed per design requirements
- ANATEL Compliance: ERP ≤35 dBm verified and documented

Installation Sign-off:

Installation Technician:	Date:
Customer Representative:	Date:
Installation Quality Verified:	Date:
ANATEL Compliance Verified:	Date:

4 Advanced Networking Features - LAN & WAN Configuration

Note: It is recommended that you configure the wireless router from a computer directly connected to Pyxis Duo.

4.1 Change LAN IPv4 address

Network > LAN

Note: The default LAN interface IPv4 address settings is 192.168.10.1 / 255.255.255.0. If the LAN IPv4 address settings are modified, you will need to log into the router management page with the new IPv4 address settings.

1. Log into your router management page
2. Click on **Network** and click **LAN**.
3. Under the Common Configuration section, you can enter the new LAN interface IP address settings.

- **IPv4 address** – Enter the new LAN IPv4 address. (e.g. 192.168.50.1)
- **IPv4 netmask** – Select or Enter the new LAN IPv4 subnet mask. The drop-down menu will list class A, B, C, or custom which will allow you to manually enter a custom subnet mask. (e.g. 255.255.255.0)

4. Click **Apply**

Below is a reference of the additional LAN settings if you choose to make other configuration changes to these sections.

General Setup

Common Configuration

General Setup | Advanced Settings

Status: Uptime: 6h 36m 20s
 MAC address: 0E:49:5F:1F:F8:EE
 RX: 2.96 MB
 TX: 18.34 MB
 IPv4: 192.168.10.1/24

Mode: NAT

IPv4 address: 192.168.10.1

IPv4 netmask: 255.255.255.0

Status – LAN Interface (br-lan)

- Uptime – Displays the amount time the LAN interface has been up and continuously running. This time will reset if the router is powered off or if the router is rebooted.
- MAC-Address – Displays the current MAC address assigned to the LAN interface.
- Rx – Displays the total amount of data received by the LAN interface in MB (# of packets) since the start of the currently displayed uptime.
- Tx – Displays the total amount of data transmitted by the LAN interface in MB (# of packets) since the start of the currently displayed uptime.
- IPv4: Displays the current IPv4 address settings assigned to the LAN interface.

Mode – Allows you to change the function between NAT mode or Route Only (NAT-less).

- **NAT** – The default router mode which uses network address translation between the local internal (LAN/VLAN) interfaces and external (WAN1/WAN2) interfaces translating public and private IP addressing.
- **Route Only (NAT-less)** – This mode disables the NAT function between internal and external interfaces and may also be known as classical routing mode. This mode should only be used when the router is used for local internal IP routing or GRE tunnels are used over between the Pyxis and the goRAN.

Advanced Settings

Override MAC Address

This parameter allows you to assign a new LAN interface (br-lan) MAC address. Typically, this parameter does not need to be modified. (e.g. AA:BB:CC:DD:EE:FF)

Override MTU

The default MTU (maximum transfer unit) or frame size is set to 1428bytes. This parameter allows you to assign a new MTU size. Typically, this parameter does not need to be modified.

4.2 DHCP server settings

Network > LAN

Note: The internal DHCP server function is enabled by default on the LAN interface to automatically distribute IP address settings to network devices connected to the LAN and wireless LAN interfaces. The internal DHCP server only supports the class C IP address range. The default IP range is 101 – 199 (192.168.10.101 – 192.168.10.199)

1. Log into your router management page
2. Click on **Network** and click **LAN**.
3. Under the DHCP Server/Relay section, you can modify or enter the new DHCP settings and click **Apply** to save and commit the changes.

DHCP mode – Allows you to set the mode to Enable, Disable, or Relay.

- **Enable** – Using this setting enables the DHCP server function on the LAN interface.
- **Disable** - Using this setting disables the DHCP server function on the LAN interface.
- **Relay** – Using this setting allows you to use an external DHCP server instead of your router's internal DHCP server to distribute IP address settings on the LAN interface. If choosing this setting, enter the IP address of your external DHCP relay server.

Start address – Enter the starting value of DHCP IPv4 address range. (e.g. If your LAN IPv4 address is 192.168.50.1, entering 120 will define the first IP address of the DHCP pool is 192.168.50.120)

End address – Enter the ending value of DHCP IPv4 address range. (e.g. If your LAN IPv4 address is 192.168.50.1, entering 200 will define the last IP address of the DHCP pool is 192.168.50.200)

Lease time – Enter the lease time in hours (h) or minutes (m) DHCP clients will hold their IP address settings before automatically requesting a new lease (IP address settings) from the internal DHCP server. (e.g. To specify 24 hours, enter 24h. To specify 480 minutes, enter 480m.)

WINS server (optional) – Enter the IPv4 address of your WINS (Windows Internet Name Server) for internal host name resolution on your local network to be distributed to DHCP clients. The WINS server provides the host name to IP address resolution for the NetBIOS naming service. This parameter is optional. (e.g. 192.168.50.250)

Primary DNS (optional) – Enter the IPv4 address of your primary DNS (Domain Name System) server for Internet domain name resolution to be distributed to DHCP clients. By default, the internal DHCP server uses DNS relay and provides the router LAN IPv4 address as the primary DNS server to DHCP clients. The DNS server provides the Internet domain name to IP address resolution when computers are accessing or browsing Internet websites. This parameter is optional. (e.g. If entering 8.8.8.8, this DNS server will be provided DHCP clients instead of the router's LAN IPv4 address to resolve Internet domain names such as trendnet.com).

Secondary DNS (optional) – Enter the IPv4 address of your secondary DNS (Domain Name System) server for Internet domain name resolution to be distributed to DHCP clients. If the primary DNS server cannot be reached, the secondary DNS server will be used. This parameter is optional. (e.g. 8.8.4.4)

Local domain name – Enter a domain name to distribute to DHCP clients. This parameter is optional. (e.g. trendnet.com)

Below is a reference of the additional DHCP Server/Relay settings if you choose to make other configuration changes to these sections.

DHCP Server/Relay

General Setup **Advanced Settings**

DHCP mode: **Enable** (DHCP (Dynamic Host Configuration Protocol) disable/enable/relay.)

Start address: **192.168.10.101** (DHCP start address.)

End address: **192.168.10.199** (DHCP end address.)

Leasetime: **12h** (Expiry time of leased addresses, range 2m ~ 999999h (m = minutes, h = hours).)

WINS server: (WINS (Windows Internet Name Service) server.)

Primary DNS server: (Primary DNS (Domain Name System) server.)

Secondary DNS server: (Secondary DNS (Domain Name System) server.)

Local domain name: (Local domain name.)

Advanced Settings

- **Dynamic DHCP** – Checking this option enables the DHCP server to distribute IPv4 address settings dynamically to clients. If this option is unchecked, IPv4 address settings will only be assigned to DHCP clients with a static DHCP reservation (see section 4.2.8) Typically, this parameter does not need to be modified.
- **Log Queries** – Checking this option will enable logging to internal or syslog of any DNS queries. Typically, this parameter does not need to be modified.

DHCP Server/Relay

General Setup **Advanced Settings**

Dynamic DHCP (Dynamic Host Configuration Protocol) ☒ Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

Log queries ☐ Write received DNS requests to syslog

4.3 Add static DHCP reservations

Network > LAN

1. Log into your router management page.
2. Click on **Network** and click **LAN**.
3. Under the Static Leases section, click **Add**.
4. Enter the parameters for the static DHCP reservation and click **Apply** to save and commit the changes.

Note: The network device or computer needs to release and renew the IPv4 address settings in order to obtain the new IP address once the reservation has been made.

- **Hostname** – Enter a name for the DHCP reservation. (e.g. trendnetpc)
- **MAC-Address** – Enter the MAC (Media Access Control) address of the computer or network device to assign to the reservation. You can also click the drop-down list to select from a list of network devices detected by the router that have been assigned IPv4 address settings through DHCP. (e.g. AA:BB:CC:DD:EE:FF)
- **IPv4-Address** – Enter the IPv4 address to assign to the computer or network device for the reservation. You can also click the drop-down list to select from list of network devices detected by the router through DHCP. (e.g. 192.168.50.150)

Static Leases

Hostname	MAC address	IPv4 address	
	v	v	Add Delete

4.4 Add static host name entries

Network > LAN

The router can be used for host name to IP address resolution of computers or network devices on your local network, similar to a WINS server. However, entries will not dynamically populate and each entry must be manually entered. For clients to resolve the manually entered static entries, DHCP clients must use the router LAN IPv4 address as the WINS server.

1. Log into your router management page.
 2. Click on **Network** and click **LAN**.
 3. Under the Host Entries section, click **Add**.
 4. Enter the parameters for the static host name entry and click **Apply** to save and commit the changes.
- **Hostname** – Enter the host name. (e.g. trendnetpc)
 - **IP Address** – Enter the IPv4 address to resolve to host name. (e.g. 192.168.50.150)

Host Entries

Hostname	IP address	Add
This section contains no values yet		

4.5 Add static ARP entries

Network > LAN

ARP (Address Resolution Protocol) is the protocol responsible for resolving IP addresses to hardware MAC addresses. Typically, ARP entries are dynamically learned and refreshed in the ARP table however, in the case where your application requires static ARP entries to always be present in the router ARP table, you can manually enter and add them to the router. (ex. applications: WoL (Wake on LAN) or Wake on WAN)

1. Log into your router management page.
2. Click on **Network** and click **LAN**.
3. Under the Static ARP section, click the **MAC-Address** drop-down list to select a MAC address from the list or select custom to manually enter a MAC address (format example: aa:bb:cc:dd:ee:ff).

Static ARP

MAC address	IPv4 address	Add
f0:2f:74:a9:80:27 (169.254.226.197) -- custom --		Delete

Apply Save Cancel

4. Click the **IPv4-Address** drop-down list and select the IPv4 address to assign to the MAC address ARP table entry or select custom to manually enter an IPv4 address (format example: 192.168.10.129)

Static ARP

MAC address	IPv4 address	Add
	192.168.10.139 169.254.226.197 -- custom --	Delete

Apply Save Cancel

5. Click **Apply** to save and commit the changes.

Note: You can specify additional static ARP entries by clicking **Add**. Delete existing entries by clicking the **Delete** button next to the entry to be removed.

4.6 LTE Settings (APN)

Network > WWAN

The default setting for SIM 1 and SIM 2 APN is Internet. The user may choose either combination to bind the SIM to the modules inside Pyxis Duo: SIM 1: Module 1, SIM 2: Module 2 OR SIM 1: Module 2, SIM 2: Module 1..

1. Log into your router management page.
2. Click on **Network** and click **WWAN**.
3. Under the **SIM Setting** section, click the **SIM Binding** drop-down list to select one of binding options.
4. Under **Cellular A Settings** section, enter the frequency band (default 31) to reduce the number of bands scanned to only the one entered. This can reduce the amount of time the module spends scanning before it attaches to the network, and the default value for MTU is of 1428
5. Under **Cellular B Settings** section, enter the frequency band (default 31) to reduce the number of bands scanned to only the one entered. This can reduce the amount of time the module spends scanning before it attaches to the network, and the default value for MTU is of 14286. Click **Apply** to save and commit the changes.

LTE

SIM Settings

SIM 1 APN

internet

SIM 2 APN

internet

PDP

IPv4

SIM Binding

SIM 1: --, SIM 2: Cellular B

Cellular A Settings

Band

31

MTU

1400

Cellular B Settings

Band

31

MTU

1428

Apply

Save

Cancel

4.7 Wi-Fi

Network > Wi-Fi

The router only supports 2.4 GHz Wi-Fi connectivity, with a single antenna (SISO)

1. Log into your router management page.
2. Click on **Network** and click on **Wi-Fi**.
3. Under Wi-Fi settings, review the settings below. When complete, click **Apply** to save and commit your changes.

Primary SSID: "Pyxis Duo"

This section allows you to configure the basic settings required for your primary Wi-Fi network such as your Wi-Fi network name (SSID) and Wi-Fi Password. Additional settings include enabling/disabling the Wi-Fi radio, applying a schedule when the radio should be enabled or disabled, and client MAC address filtering.

Device Configuration

General Setup | Advanced Settings

Status: **Mode:** Access Point
SSID: Pyxis Duo
BSSID: 00:03:7F:12:34:56
Encryption: WPA2 Personal
Channel: 11 (2.462 GHz)
Tx-Power: 21 dBm
Speed: 286.0 Mbit/s

Enable Wi-Fi radio ☒

Turn off Wi-Fi radio by schedule: **Disable time schedule** ▼

Operating frequency (Channel): **Auto** ▼

Interface Configuration

General Setup | Wi-Fi Security | MAC-Filter | Advanced Settings

SSID: **Pyxis Duo**

Hide SSID: ☐

Apply **Save** **Cancel**

Device Configuration

General Setup

Status-it shows the SSID, BSSID, Encryption, Chennel, Tx-Power, and Bitrate of the Wi-Fi network. To enable or disable Wi-Fi network, click on **Enable Wi-Fi radio**, and user can schedule the availability of Wi-Fi network through the drop-down list of **Turn off Wi-Fi radio by schedule**. To assign specific Wi-Fi channel, the user may choose from the drop-down list within **Operating frequency**.

Advanced Settings

Device Configuration

General Setup | **Advanced Settings**

Mode: **802.11b/g/n/ax** ▼

HT mode: **Auto 20/40MHz** ▼

Interface Configuration

General Setup | Wireless Security | MAC-Filter | Advanced Settings

ESSID (Extended Service Set Identifier): **Lemonade_plus_0**

Hide ESSID (Extended Service Set Identifier) ☐

Apply **Save** **Cancel**

For more advanced Wi-Fi setting, user may change the **Mode from the drop-down list** and **HT Mode** of the radio.

Interface Configuration

General Setup

The user may choose to change **SSID (Service Set Identifier)** or **Hide SSID (Service Set Identifier)** in this section of the WebGUI.

Device Configuration

General Setup

Advanced Settings

Status

Mode: Access Point

SSID: Pyxis Duo

BSSID: 00:03:7F:12:34:56

Encryption: WPA2 Personal

Channel: 11 (2.462 GHz)

Tx-Power: 21 dBm

Speed: 286.0 Mbit/s

Enable Wi-Fi radio

☒

Turn off Wi-Fi radio by schedule

Disable time schedule

Operating frequency (Channel)

Auto

Interface Configuration

General Setup

Wi-Fi Security

MAC-Filter

Advanced Settings

SSID

Pyxis Duo

Hide SSID

☐

Apply

Save

Cancel

Wi-Fi Security

Device Configuration

General Setup

Advanced Settings

Mode

HT mode

Encryption

WPA2 Personal

Cipher

Force CCMP (AES)

Key

password

Interface Configuration

General Setup

Wireless Security

MAC-Filter

Encryption

WPA2 Personal

Cipher

Force CCMP (AES)

Key

password

Apply

Save

Cancel

Device Configuration

General Setup
Advanced Settings

Status
Mode: Access Point
SSID: Pyxis Duo
BSSID: 00:03:7F:12:34:56
Encryption: WPA2 Personal
Channel: 11 (2.462 GHz)
Tx-Power: 21 dBm
Speed: 286.0 Mbit/s

Enable Wi-Fi radio ☒

Turn off Wi-Fi radio by schedule
Disable time schedule

Operating frequency (Channel)
Auto

Interface Configuration

General Setup
Wi-Fi Security
MAC-Filter
Advanced Settings

Encryption
WPA2 Personal

Cipher
Force CCMP (AES)

Password
.....

Apply
Save
Cancel

To change the **Encryption**, **Cipher**, and **Password** of the Wi-Fi radio, the user may choose from the drop-down list and change the password accordingly.

MAC-Filter

Interface Configuration

General Setup
Wireless Security
MAC-Filter
Advanced Settings

MAC-Address Filter
Disable

Disable
Allow listed only
Deny listed

Apply
Save
Cancel

To enable MAC-Address Filter option, user may choose from **MAC-Address Filter** drop-down list.

Advanced Settings

Interface Configuration

General Setup
Wireless Security
MAC-Filter
Advanced Settings

Separate Clients ☐
Prevents client-to-client communication

Enable HT20/HT40 coexistence ☐

Protected Management Frames ☐

Apply
Save
Cancel

More advanced setting is available through **Separate Clients**, **Enable HT20/HT40 coexistence**, and **Protected Management Frames** options.

4.8 Create VLANs

Network > VLAN

VLAN Scope and Purpose

VLANs operate on LAN-side interfaces only for local network segmentation. This functionality enables:

- Industrial protocol separation (GOOSE vs DNP3)
- Local device isolation behind the Pyxis
- Network traffic management on Ethernet interfaces

Note: VLANs operate on LAN interfaces only. LTE transmission remains Layer 3 routing and does not support VLAN tagging over the cellular interface.

Advanced VLAN Features: The Pyxis supports advanced VLAN features including trunking and VLAN retagging via SSH/CLI access. Contact technical support for complex VLAN configurations.

Your router supports port-based 802.1Q VLANs in addition to inter-VLAN routing. VLANs can be assigned different IP address interfaces in which the router can route between VLAN IP subnets.

Create a port-based VLAN

1. Log into your router management page.
2. Click on **Network** and click **VLAN**.
3. Before assigning which untagged and tagged VLAN member ports are assigned to a new VLAN, the ports must be set to Off in the default VLAN VID: 1 (LAN).

Also, click the Inter VLAN Routing drop-down list and select **Enabled** to enable communication between the LAN and other VLAN interfaces.

Click **Apply** to save and commit the changes.

Example: Below, we will remove port 3 from the default VLAN VID: 1 (LAN) interface so these ports can be re-assigned as untagged member ports of new VLANs.

VLANs

VID	Ports	Network	DHCP Server	
1	1 Untagged ▼ 2 Untagged ▼	IP address 192.168.10.1 Subnet mask 255.255.255.0	Mode : Enabled Start address 192.168.10.101 End address 192.168.10.199 Leasetime 12h WINS Server Primary DNS Server Secondary DNS Server Local domain name	Add
3	1 Off ▼ 2 Off ▼	IP address : 192.168.55.1 Subnet mask : 255.255.255.0	Mode : Enabled ▼ Start address 192.168.10.101 End address 192.168.10.199 Leasetime 12h WINS Server Primary DNS Server Secondary DNS Server	Delete

4. To create a new 802.1Q VLAN, under the VLANs section, click **Add**.

5. Under **VID**, enter the VLAN ID to assign to the new VLAN and set the untagged VLAN member ports. *Example: In the example below, we will create a new VLAN with VLAN ID: 50 and assign ports 2 as untagged member ports.*

50	1 Off ▼	2 Off ▼
----	-------------------------------	-------------------------------

6. Enter the VLAN IP interface configuration under **IP Address** and **Subnet Mask**.

Example: In the example below, we will enter the VLAN 50 interface IP address as 192.168.50.1 and subnet mask 255.255.255.0.

Network
IP Address 192.168.50.1
Subnet Mask 255.255.255.0

IP address

192.168.50.1

Subnet mask

255.255.255.0

7. Under DHCP Server, click the **Mode** drop-down list and select **Enabled** to enable the DHCP server on the VLAN. Click **Apply** to save and commit the changes.

Example: In the example below, we will enable the DHCP server on VLAN 50 and leave IP address range and lease defaults. This will assign a DHCP IP range of 101-199 to ensure any devices connected to this VLAN obtain IP address information via DHCP.

DHCP Server	
Mode:	Enabled
Start address	192.168.10.101
End address	192.168.10.199
Leasetime	12h
Mode: Enabled ▼	
Start address	192.168.50.101
End address	192.168.50.199
Leasetime	12h
WINS Server	
Primary DNS Server	
Secondary DNS Server	
Local domain name	
Static Leases	

If following the port-based VLAN configuration example, any computers or devices connecting to port 2 will obtain 192.168.50.x/255.255.255.0 address settings and use the VLAN 50 IP interface 192.168.50.1 as the Internet gateway and gateway to other local IP subnets.

VLAN 50

IP address: 192.168.50.1

Mask: 255.255.255.0

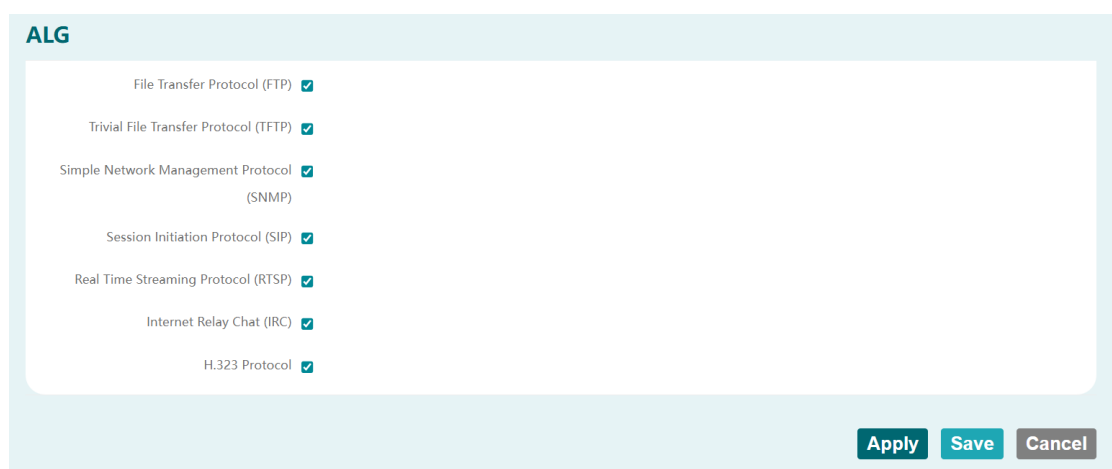
4.9 Application Layer Gateway (ALG)

Network > Application

You may want to configure your router to allow computers the use of specific high layer applications or service sessions to pass through. Application Layer Gateways (ALG) allows you to easily enable or disable these applications to pass through your router.

Note: It is recommended to leave these settings enabled.

1. Log into your router management page.
2. Click on **Network** and click on **Application**.
3. Review the applications. Click **Apply** to save and commit the changes.



The screenshot shows the 'ALG' configuration page. It features a list of protocols with checkboxes indicating they are all enabled:

- File Transfer Protocol (FTP) ☒
- Trivial File Transfer Protocol (TFTP) ☒
- Simple Network Management Protocol (SNMP) ☒
- Session Initiation Protocol (SIP) ☒
- Real Time Streaming Protocol (RTSP) ☒
- Internet Relay Chat (IRC) ☒
- H.323 Protocol ☒

At the bottom right, there are three buttons: 'Apply' (blue), 'Save' (teal), and 'Cancel' (grey).

4.10 GRE Tunnels (VPN) Configuration

Network > GRE

GRE (Generic Routing Encapsulation) encapsulates data inside IP packets and routes it over an IP network through virtual point-to-point links. The GRE allows administrators to create and manage GRE tunnels (VPN), which encapsulate Layer 3 traffic to create point-to-point virtual links between remote networks over an IP network.

1. Go to **GRE**.
2. Enter a unique **Tunnel Name**.
3. Click **Add**.
4. Fill in:
 - a. Source WAN IP
 - b. Destination IP
 - c. Tunnel IP/Netmask
 - d. Remote Network/Netmask
 - e. MTU (e.g., 1476)
 - f. Enable the tunnel.
5. Click **Apply**, then **Save**.

GRE

Generic Routing Encapsulation

GRE tunnels

Add

Tunnel Name	Source WAN IP	Destination IP	Tunnel IP/Netmask	Remote Network/Netmask	MTU	Enabled
This section contains no values yet						

Apply
Save
Cancel

GRE tunnels

Field	Description
New Tunnel Name	Add a unique name to identify the GRE tunnel.
Tunnel Name	The name of the tunnel
Source WAN IP	Specify the IP address on the local WAN interface that initiates the GRE tunnel.
Destination IP	IP address of the remote GRE peer device. This is the endpoint of the tunnel.
Tunnel IP/Netmask	The IP address and subnet mask assigned to the GRE tunnel interface. Used for tunnel-to-tunnel communication.
Remote Network/Netmask	The destination network (and subnet) behind the remote GRE peer that should be reachable through this tunnel.
MTU	Maximum Transmission Unit size for the GRE tunnel. Adjust if fragmentation occurs.
Enabled	Indicates whether the tunnel is currently active (enabled) or disabled.

Notes:

- GRE is a simple tunnelling protocol and does not provide encryption or confidentiality.
- Ensure firewall and routing rules allow GRE traffic (protocol 47).
- You may define multiple tunnels for various peer networks or site-to-site communications.

GRE Tunnel Use Cases

1. Site-to-Site Connectivity

- Connect remote site to headquarters LAN
- Transparent routing of all protocols
- Maintains network topology across LTE

2. Protocol Bridging

- Tunnel industrial protocols (DNP3, Modbus)
- Preserve protocol characteristics
- Support legacy applications without modification

3. Network Extension

- Extend corporate network over LTE
- Seamless integration with existing infrastructure
- Support for broadcast and multicast protocols

Configuration Example:

For SCADA integration, create GRE tunnel between remote substation and control center, allowing transparent DNP3 communication as if devices were on same local network.

Industrial Application: Single GRE tunnel can carry both DNP3 and GOOSE traffic with VLAN separation maintained.

4.11 Routing

Network > Routing

The Routing section allows administrators to manage both static and dynamic routing protocols for IPv4 networks. Supported protocols include Static Routes, RIP, OSPF, and BGP.

Static Routers

Use this section to manually define static routes for directing traffic between network segments.

1. Go to **Routing > Static Routes**.
2. Select the desired **Interface**.
3. Enter the **Target Host-IP or Network** (e.g., 192.168.2.0).
4. Provide the **IPv4-Netmask** (e.g., 255.255.255.0).
5. Input the **IPv4-Gateway**.
6. Set a **Metric** (priority; lower = higher priority).
7. Click **Add** to insert the route.
8. Click **Apply** to preview or **Save** to finalize.

The screenshot shows the 'Routing' configuration page. At the top, there are tabs for 'Static Routes', 'RIP', 'OSPF', and 'BGP'. Below the tabs, a note states: 'Static routes can be configured to allow your router to allow communication between your local IP networks and other IP networks located on neighboring routers.' The main section is titled 'Static IPv4 Routes'. It contains a table with five columns: 'Interface', 'Target Host-IP or Network', 'IPv4-Netmask', 'IPv4-Gateway', and 'Metric'. An 'Add' button is located to the right of the table. Below the table, a message says 'This section contains no values yet'. At the bottom right, there are three buttons: 'Apply', 'Save', and 'Cancel'.

Field	Description
Interface	Select the network interface for the route (e.g., LAN, LTE).
Target Host-IP or Network	Destination IPv4 address or subnet (e.g., 192.168.2.0).
IPv4-Netmask	A netmask is used to divide an IP address into sub-networks (subnets). Combined, the 'Target Host-IP or Network' and

	'Netmask' values define the exact destination network or IP address to which this route applies. Subnet mask for the destination network (e.g., 255.255.255.0).
IPv4-Gateway	Gateway address through which the destination is reachable. This parameter specifies the next hop IP address where packets will be forwarded to a router with this IP address when no other route specification in routing table matches the destination IP address of a packet.
Metric	Route priority. Lower values have higher priority. Router metrics is another value that help the router choose the best route among multiple feasible routes to a destination. The metric value based on information such as path length, bandwidth, load, hop count, path cost, delay that may be used by the different routing protocols. The lowest Metric value has the highest priority route.

RIP

RIP enables automatic exchange of routing information between routers using distance-vector routing.

1. Navigate to **Routing > RIP**.
2. Check **RIP Enable**.
3. In the **Overview** table:
 - a. For each interface, ensure **Enable** is set.
 - b. Set **Send/Receive version** to 1, 2, or both.
 - c. Optionally enable **Authentication**, set **Key**, and select **Key mode** (md5).
4. Click **Edit** to adjust individual interface settings if needed.
5. Click **Apply**, then **Save**.

Routing

Static Routes **RIP** OSPF BGP

RIP (Routing Information Protocol) Configuration

RIP enable ☐

Overview

Interface	Enable	Send version	Receive version	Authentication	Key	Key mode	
LAN	Enable	2	2	Disable	123	md5	Edit
WWAN(Cellular A)	Enable	2	2	Disable	123	md5	Edit
WWAN(Cellular B)	Enable	2	2	Disable	123	md5	Edit

[Apply](#) [Save](#) [Cancel](#)

RIP enable: Check to enable RIP protocol globally.

Field	Description
Interface	Name of the interface (e.g., LAN, LTE).
Enable	Toggle RIP on/off for each interface.
Send version / Receive version	RIP version used (e.g., v2).
Authentication	Optional authentication (Enable/Disable).

Key / Key mode	Password and method (e.g., md5) for authentication.
Edit	Opens editable options for that interface.

OSPF Configuration (Open Shortest Path First)

OSPF is a link-state routing protocol that calculates the shortest path for routing packets.

1. Go to **Routing > OSPF**.
2. Check **OSPF Enable**.
3. Set the **Router ID** (e.g., 192.168.1.1).
4. In the **Overview** table:
 - a. Ensure the correct **Interface** is **Enabled**.
 - b. Choose **Network** type (typically "Broadcast").
 - c. Configure **Authentication**, **Key**, and **Key Mode** if needed.
 - d. Set **Cost**, **Priority**, and **Area** values.
5. Click **Apply**, then **Save**.

Routing

Static Routes RIP **OSPF** BGP

OSPF (Open Shortest Path First) Configuration

OSPF enable ☐

Router ID 192.168.1.1

Overview

Interface	Enable	Network	Authentication	Key	Key mode	Cost	Priority	Area	
LAN	Enable	Broadcast	Disable	123	md5	15	1	0	Edit
WWAN(Cellular A)	Enable	Broadcast	Disable	123	md5	15	1	0	Edit
WWAN(Cellular B)	Enable	Broadcast	Disable	123	md5	15	1	0	Edit

Apply Save Cancel

OSPF enable: Enables or disables OSPF globally.

Router ID: A unique ID for the router (default format: IP address).

Field	Description
Interface	Network interface name.
Enable	Enables OSPF on that interface.
Network	Type of OSPF network (e.g., Broadcast).
Authentication	Optional security (Enable/Disable).
Key / Key mode	Security password and mode (e.g., md5).
Cost	Path cost (lower is preferred).
Priority	Determines designated router (DR) election.
Area	OSPF Area ID (e.g., 0).
Edit	Modify settings for that interface.

BGP Configuration (Border Gateway Protocol)

BGP is a path-vector routing protocol used for inter-domain routing between autonomous systems, enabling High Availability (HA) to the back end.

1. Navigate to **Routing > BGP**.
2. Check **BGP Enable**.
3. Set **Router ID** and **ASN (Autonomous System Number)**.
4. In the **Overview** section, **Enable** BGP for selected interfaces.
5. Under **Neighbor**:
 - a. Enter **Neighbor IP**.
 - b. Check **Key Authentication** if needed.
 - c. Set **Key String** and **Remote AS**.
6. Click **Add**.
7. Click **Apply**, then **Save**.

BGP enable: Enables BGP protocol.

Router ID: Unique router identifier.

ASN: Autonomous System Number assigned to the router.

Overview Table:

Field	Description
Name	Interface name.
Enable	Toggle BGP for each interface.

Neighbor Configuration:

Field	Description
Neighbor	IP address of BGP peer.
Key authentication	Enable/disable BGP session authentication.
Key string	Password for peer authentication.
Remote AS	ASN of the BGP neighbor.

4.12 Serial Ports

Network > serial

This section allows configuration of the router’s onboard serial ports for use with external serial devices or network-to-serial applications. Each serial port has two configuration tabs:

- 1. **Serial:** For physical interface parameters (baud rate, parity, etc.)
- 2. **Serial to Network:** For mapping serial communication to TCP/IP.

Serial

Configuration Fields (Serial Port 1 and Serial Port 2):

- 1. Go to **Serial Port Settings > Serial**.
- 2. For **Serial Port 1/2**, configure:
 - a. **Baud Rate**
 - b. **Data Bits**
 - c. **Parity**
 - d. **Stop Bits**
 - e. **Serial Mode** (e.g., RS-485)
- 3. Click **Apply**, then **Save**.

Serial Port 1

Serial

Serial to Network

Baud Rate

9600

Data bits

8

Parity

None

Stop bits

1

Serial Mode

RS-485

Serial Port 2

Serial

Serial to Network

Virtual COM Type

Disable

Service Mode

Disable

Local Service Port

3021

The protocol to listen to.

Raw

Max of local serial port connections

3

Field	Description
Baud Rate	Transmission speed in bits per second. Typical values: 9600, 19200, 38400, etc.
Data bits	Number of bits per character (usually 7 or 8).

Parity	Error-checking method. Options: None, Even, Odd.
Stop bits	Number of stop bits to mark end of transmission. Common: 1 or 2.
Serial Mode	Electrical interface mode: RS-232, RS-485, or RS-422 (depending on hardware support).

Note: Each serial port can be configured independently for specific equipment needs.

Serial to Network

Used to enable communication between serial devices and TCP/IP networks.

1. Select the **Serial to Network** tab.
2. For each port:
 - a. Set **Virtual COM Type** (e.g., Disable/RFC2217).
 - b. Set **Service Mode** (TCP Server/Client/UDP).
 - c. Enter **Local Service Port** (e.g., 3020).
 - d. Choose **Protocol** (e.g., Raw).
 - e. Set **Max Connections**.
3. Click **Apply**, then **Save**.

Serial Port 1

Serial

Serial to Network

Virtual COM Type

Disable

Service Mode

Disable

Local Service Port

3020

The protocol to listen to.

Raw

Max of local serial port connections

3

Serial Port 2

Serial

Serial to Network

Virtual COM Type

Disable

Service Mode

Disable

Local Service Port

3021

The protocol to listen to.

Raw

Max of local serial port connections

3

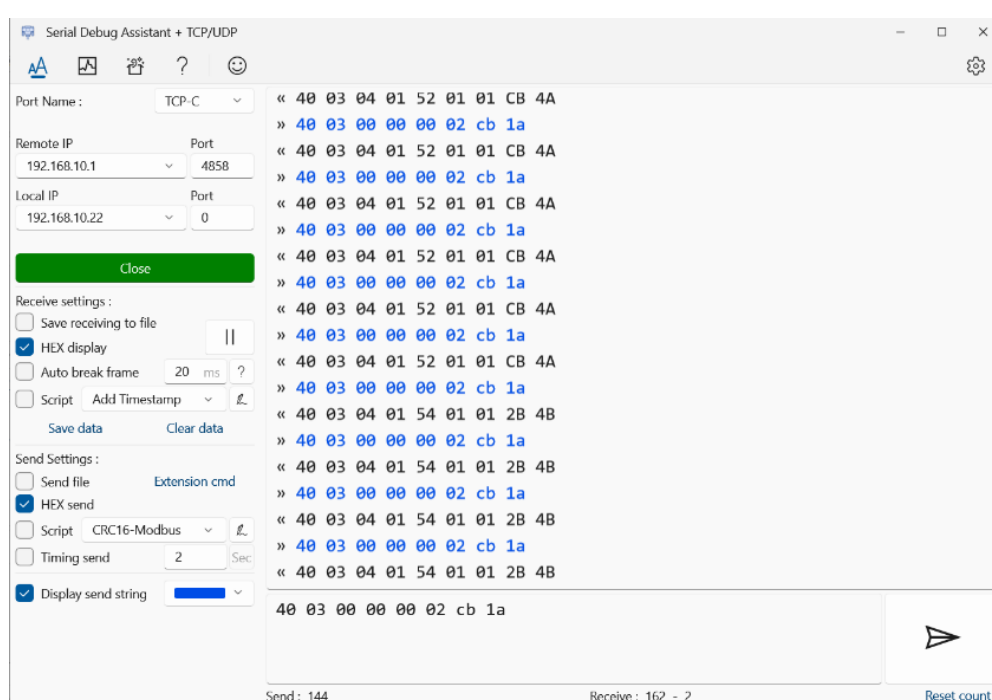
Configuration Fields (Serial Port 1 and Serial Port 2):

Field	Description
Virtual COM Type	Enables mapping to a virtual COM port. Options: Disable, RFC2217, VCOM, etc.
Service Mode	Defines how the serial port communicates: • Disable: No service. • TCP Server: Listens for incoming TCP connections. • TCP Client: Actively connects to a remote host. • UDP: Sends/receives datagrams without connection. Local Service Port TCP/UDP port number used for serial service (e.g., 3020, 3021). The protocol to listen to Specifies data protocol format: Raw, Modbus, etc.

	Max of local serial port connections Limits the number of simultaneous TCP connections (1–4 typical).
--	--

1. Enable the Serial port and choose the "service mode" to TCP Server and specify the Service port and "Virtual COM Type".
2. Apply to save setting.

Use the Serial port access tool that supports TCP client mode, input the IP and port: the IP is the device IP, the port is the service port you configured in the router. Such tool can be found here: <https://apps.microsoft.com/detail/9nblggh43hdm?hl=en-US&gl=US>



If you want to remote connect from the router's WAN IP, you need to configure the traffic rule on the router.

Network > Firewalls – Traffic rules

1. Open the port on router page.
2. Add the External port and apply the setting.

Open Ports on Router

Name

New input rule

Protocol

TCP+UDP

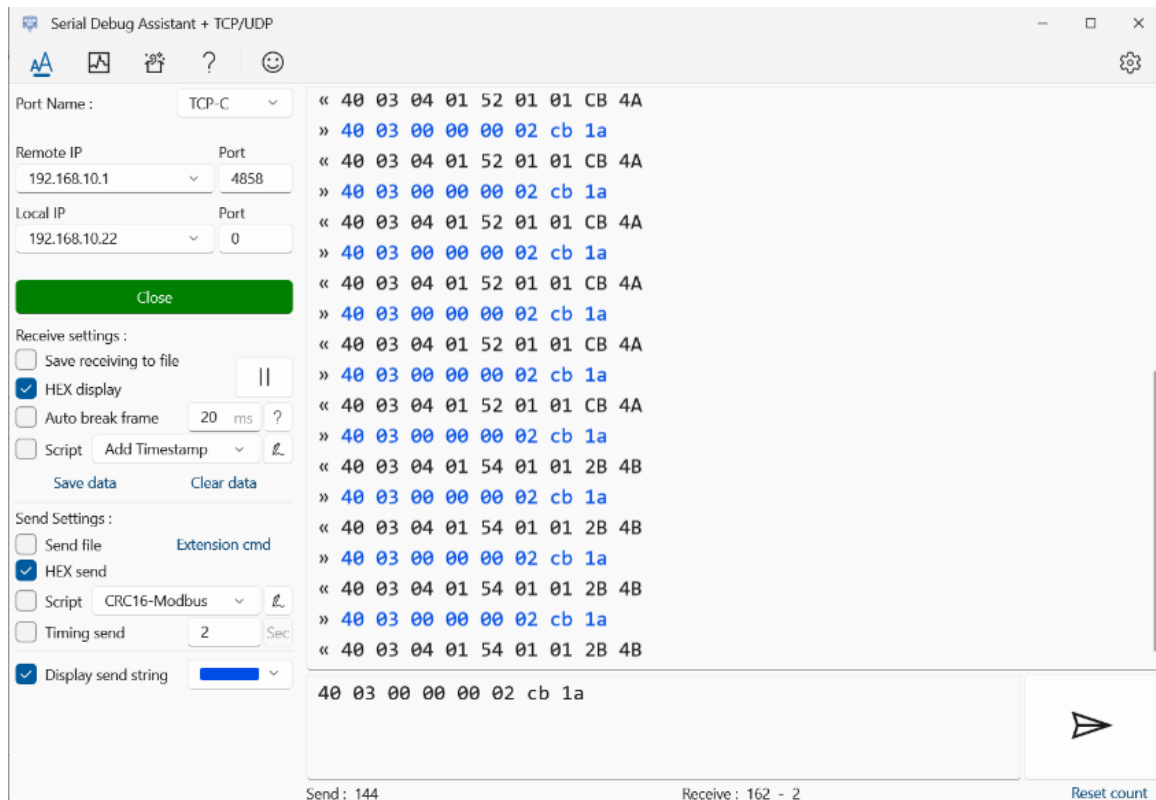
External port

Schedule

Disable time schedule

Add

Check through the debugging tool mentioned above



4.13 Industrial Protocol Network Configuration

The Pyxis Duo provides network-level support for industrial protocols through standard routing and forwarding capabilities.

Network Configuration Options:

1. Port Forwarding

- Direct port mapping (e.g., DNP3 port 20000 → internal device)
- Protocol-specific port ranges
- See Section 5.2 for configuration details

2. DMZ Configuration

- Full network access to single SCADA server
- Simplified setup for legacy systems
- See Section 5.6 for configuration details

3. GRE Tunneling

- Transparent protocol bridging
- Preserves Layer 2 characteristics when needed
- See Section 4.10 for configuration details

Industrial Protocol Examples:

- DNP3: TCP port 20000, UDP port 20000
- Modbus TCP: Port 502
- IEC 61850 GOOSE: Requires GRE tunneling for Layer 2 transparency
- IEC 60870-5-104: Port 2404

For specialized protocol implementations, contact technical support.

Layer 2 Protocol Bridging: GRE tunnels transparently pass both DNP3 and GOOSE messages simultaneously, supporting multiple VLAN sub-interfaces.

4.14 Define Quality of Service (QoS)

Network > QoS

The router supports up to four QoS priority queues for traffic classification and priority.

1. Log into your router management page.
2. Click on **Network** and click on **QoS**.
3. Under QoS settings, review the settings below. When complete, click **Apply** to save and commit your changes.

QoS Settings

- **Enable:** Check the enable option to **Enable** QoS.
- **Download speed (kbit/s):** Enter the maximum download speed provided by your ISP in kilobits per sec. It is important to set this value accurately.
- **Upload speed (kbit/s):** Enter the maximum upload speed provided by your ISP in kilobits per sec. It is important to set this value accurately.
- **Note:** *If your multiple mode is set to load balancing, you can combine the total upload bandwidth of both WAN connections.*
- **Calculate overhead** – Typically, when this option is unchecked/disabled, the overhead value will not be added to the upload and download speeds entered in the fields. When this option is checked/enabled, the total overhead calculation is included in the total upload/download speed specified to ensure the values entered are the absolute maximum value limits entered.
- **Default class** – When QoS is enabled, select the default priority class used for all other traffic after all specific QoS classification rules have been applied. You can typically set this to **Low**, **Medium**, **High** and **Highest**.

QoS Settings

Enable ☐

Download speed (kbit/s)

Upload speed (kbit/s)

Calculate overhead ☐

Default class

Classes – The QoS priority classes define the bandwidth maximum limits of total bandwidth that can be used and total bandwidth that can be shared for a particular class.

Note: Typically, you do not need to modify the QoS priority class percentage settings.

- **Download link share bandwidth (%)** – This defines the guaranteed bandwidth % from the total download speed defined in the QoS settings. The class setting will attempt to guarantee this bandwidth % minimum limit is allocated.
- **Download max bandwidth (%)** – This defines the maximum bandwidth % allowable from the total download speed defined in the QoS settings. This class setting is the maximum bandwidth % limit that can be allocated above the link share bandwidth %.
- **Upload link share bandwidth (%)** – This defines the guaranteed bandwidth % from the total upload speed defined in the QoS settings. The class setting will attempt to guarantee this bandwidth % minimum limit is allocated.
- **Upload max bandwidth (%)** – This defines the maximum bandwidth % allowable from the total upload speed defined in the QoS settings. This class setting is the maximum bandwidth % limit that can be allocated above the link share bandwidth %.

Classes Sum of all four upload/download link share bandwidth cannot exceed 100%.

HIGHEST

Download link share bandwidth (%)	60
Download max bandwidth (%)	90
Upload link share bandwidth (%)	60
Upload max bandwidth (%)	90

Classification Rules

Click Add to create a new QoS classification rule. When complete, click Apply to save and commit your changes.

- **Target** – Select the QoS priority class to apply to the rule.
- **Direction** – Select the direction of traffic in which to apply the QoS classification, Download (Inbound Traffic) or Upload (Outbound Traffic).
- **Source Host** – Click the drop-down list to select All (any IP address), a specific source host IP address from the list or select Custom to define a particular source IP address not listed.
- **Destination Host** – Click the drop-down list to select All (any IP address), a specific destination host IP address from the list or select Custom to define a particular destination IP address not listed.
- **Protocol** – Click the drop-down to select the type of traffic to apply the QoS classification rule. All/TCP/UDP/ICMP or custom to specify a particular protocol not listed.
- **Source Port** (range) – Enter source port range to apply the QoS classification rule.

- **Destination Port** (range) – Enter destination port range to apply the QoS classification rule.

Classification Rules

Target	Direction	Source host	Destination host	Protocol	Source Port (range)	Destination Port (range)	Comment	Sort	
Highest ▾	Download ▾	All ▾	All ▾	All ▾	All ▾	All ▾		^ ▾	Add Delete

Enhanced QoS for Industrial Applications

Industrial Protocol QoS Rules:

Protocol	Priority	Bandwidth Allocation	Latency Requirement
IEC 61850 GOOSE	Highest	10% guaranteed	<4ms
DNP3	High	15% guaranteed	<100ms
Modbus	High	10% guaranteed	<100ms
SCADA HMI	Medium	20% guaranteed	<200ms
Video Surveillance	Medium	30% guaranteed	<500ms
File Transfer	Low	15% guaranteed	Best effort

4.15 Multiple WAN Configuration

Network > Multiple WAN

The Multiple WAN (MWAN) settings allow the router to manage multiple WAN interfaces for load balancing, failover, or using a dedicated primary WAN without backup. There are two configuration tabs: Basic and Advanced.

Basic Tab

1. Navigate to **Multiple WAN > Basic**.
2. View live status under **Status**.
3. Under **Settings**, select:
 - a. **Primary Interface**
 - b. **Policy** (Failover, Load Balancing, etc.)
4. Under **Link Tracking**:
 - a. Check **Enable Tracking** for desired WANs.
 - b. Enter a public **IP/hostname** (e.g., 8.8.8.8).
 - c. Set **Ping Interval** (e.g., 5s).
5. Click **Apply**, then **Save**.

Multiple WAN

Basic

Advanced

This section allows you to set up the mode and traffic rules of the router WAN interfaces. WAN modes include load balancing, failover, or using primary interface without backup.

Status

Interface Live Status

Selected Primary: WWAN (Cellular A)

Interface: WWAN (Cellular A)
Status: Online

Interface: WWAN (Cellular B)
Status: Offline

Settings

Primary Interface

WWAN (Cellular A)

Policy

Load Balance

Load Balance Weighting

50% : 50%

WWAN (Cellular A) : WWAN (Cellular B)

Link Tracking

Link Tracking is used to check if the link is up or down by ping the tracking IP.

WWAN (Cellular A)

Enable Tracking

☒

Tracking hostname or IP address

8.8.8.8

This hostname or IP address will be pinged to determine if the link is up or down. Leave blank to assume interface is always online.

Ping interval

1 second

WWAN (Cellular B)

Enable Tracking

☒

Tracking hostname or IP address

8.8.8.8

This hostname or IP address will be pinged to determine if the link is up or down. Leave blank to assume interface is always online.

Ping interval

1 second

Status

Displays the live status of WAN interfaces:

1. Selected Primary: The currently selected main WAN interface.
2. Interface Status: Shows if a WAN is Online, Offline, or Disabled, and whether link tracking is active.

Status

Interface Live Status

Selected Primary: WWAN (Cellular A)

Interface: WWAN (Cellular A)
Status: Online

Interface: WWAN (Cellular B)
Status: Offline

Settings

Field	Description
Primary Interface	Select the WAN interface to act as the main route for outbound traffic.
Policy	Determines how WAN interfaces behave: • Failover: Uses the primary interface until it fails, then switches. • Load Balance: Distributes traffic across WANs. • Default (Main Routing Table)

Settings

Primary Interface	WWAN (Cellular A)	
Policy	Load Balance	
Load Balance Weighting	50% : 50%	WWAN (Cellular A) : WWAN (Cellular B)

Link Tracking

Link tracking verifies WAN availability by pinging a designated IP.

For each WAN interface:

Field	Description
Enable Tracking	Checkbox to enable/disable link monitoring.
Tracking Hostname/IP	Destination IP (e.g., 8.8.8.8) to ping. If left blank, the link is assumed always online.
Ping Interval	How often (e.g., every 5 seconds) the ping is sent to verify the link.

Link Tracking

Link Tracking is used to check if the link is up or down by ping the tracking IP.

WWAN (Cellular A)

Enable Tracking ☒

Tracking hostname or IP address 



This hostname or IP address will be pinged to determine if the link is up or down. Leave blank to assume interface is always online.

Ping interval

WWAN (Cellular B)

Enable Tracking ☒

Tracking hostname or IP address 



This hostname or IP address will be pinged to determine if the link is up or down. Leave blank to assume interface is always online.

Ping interval

Advanced

The Advanced section allows you to define custom traffic rules to control routing behaviour on each WAN interface.

- Go to Multiple WAN > Advanced.
- Enter a name in the Rule field.
- Click Add.
- Define:
 - Source/Destination IP and Ports
 - Protocol (TCP/UDP)
 - Policy Assigned (e.g., Use WAN1)
 - Sort Order
- Click **Apply**, then **Save**.

Traffic Rules Table:

Field	Description
Rule	Name or label for the custom rule.
Source Address	Originating IP address for the traffic.
Source Port	Port on the source device (optional).
Destination Address	Target IP address for the traffic.
Destination Port	Destination service port (e.g., 80 for HTTP).
Protocol	Select TCP, UDP, or other protocols.
Policy Assigned	Specify which WAN policy (e.g., use WAN1, failover, etc.) applies to this rule.
Sort	Rule priority/order. Lower values are evaluated first.

Traffic Rules

Rule	Source address	Source port	Destination address	Destination port	Protocol	Policy assigned	Sort
------	----------------	-------------	---------------------	------------------	----------	-----------------	------

This section contains no values yet

4.16 Network Architecture Examples

4.16.1 goRAN™ with Embedded EPC (Standalone Private Network)

Network Flow:

End Devices → Pyxis Duo → LTE (Band 31/87) → goRAN™ eNodeB → Embedded EPC → Local Network/Internet

Architecture Benefits:

- Single unit deployment: eNodeB + EPC in one outdoor enclosure
- Local traffic processing: No external core network required
- Reduced backhaul: Only management traffic needs external connectivity
- Edge computing: Applications can run directly on embedded EPC

Deployment Scenario:

- Remote industrial sites with limited backhaul
- Utility substations requiring local control
- Mining operations in remote locations
- Construction sites with temporary networks

4.16.2 goRAN™ with External EPC (Distributed Core Network)

Network Flow:

End Devices → Pyxis Duo → LTE → goRAN eNodeB → S1 Interface → External EPC → Corporate Network

When to use external EPC:

- Multi-site deployments requiring centralized management
- Integration with existing EPC infrastructure
- Roaming between multiple base stations
- Advanced core network features (IMS, policy control)

4.16.3 Multi-vendor 3GPP Compliant Network

Network Flow:

End Devices → Pyxis Duo → 3GPP LTE Interface → Any Vendor eNodeB → Standard EPC → Internet/Private Network

Supported Vendors:

- Base Stations: Nokia, Ericsson, Huawei, Samsung, or any 3GPP-compliant eNodeB
- Core Networks: Any standard EPC
- Management: Standard SNMP

5 Firewall & Security

5.1 General Settings

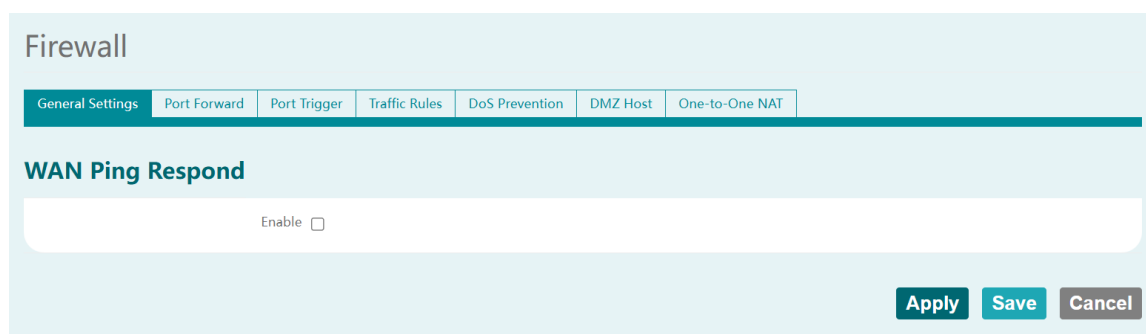
Network > Firewall > General Settings

1. Log into your router management page.
2. Click on **Network**, click on **Firewall**, and click on the **General Settings** tab.
3. Review the settings below. When complete, click **Apply** to save and commit your changes.

General Settings

WAN Ping Respond

- **Enable** – By default, this function is disabled to prevent the WAN port interfaces from responding to ping/ICMP requests. Enabling this option will set your WAN port interfaces to respond ping/ICMP requests from the Internet.



The screenshot shows the 'Firewall' configuration page with the 'General Settings' tab selected. Under the 'WAN Ping Respond' section, there is a single setting: 'Enable' with an unchecked checkbox. At the bottom right of the page, there are three buttons: 'Apply' (blue), 'Save' (teal), and 'Cancel' (grey).

5.2 Port Forwarding

Network > Firewall > Port Forward

Port forwarding rules allow to create inbound rules from the WAN interfaces/Internet to your internal computers or devices for specific services/protocols such as a file server (FTP), IP camera, web server (HTTP/HTTPS), or remote access, etc.

1. Log into your router management page.
2. Click on **Network**, click on **Firewall**, and click on the **Port Forward** tab.
3. Review the settings below. When complete, click **Add** to add the new entry to the list and **Apply** to save and commit your changes.

Add New Port Forward Rule

Name:

Protocol:

External interface:

External port:

Internal IP address:

Internal port:

Schedule:

- **Name** – Enter a name for the new port forwarding rule.
- **Protocol** – Click the drop-down list to select the protocol for the service to allow: **TCP**, **UDP**, **TCP+UDP**, or **Other**.
- **External Port** – Enter the external port number for the service to allow.

Note: You can also enter a consecutive range of ports in the following format: 80-90

- **Internal IP address** – Click the drop-down list to select a device from the list or enter the local/internal IP address of the device to forward the port/protocol service.
- **Internal Port** – Enter the internal port number for the service to allow.

Note: You can also enter a consecutive range of ports in the following format: 80-90. Typically, the internal port or port range is same as the external port or port range.

- **Schedule** – Allows you to select a schedule when the port forwarding rule should be enabled or disabled.

Note: To restrict access to source IP address, after you have created the port forward rule, click **Edit** on the port forwarding entry in the list and enter the IP address in **Source IP address** field, then click **Apply**.

Port Forward Rules

Name	Match	Forward to	Schedule	Enable	Sort	
Port-forwarding	IPv4-tcp From <i>WWAN (GCM4701NA)</i> Via <i>any router IP</i> at port 22	IP <i>192.168.10.139</i> port 22 in <i>LAN</i>	No Schedule Entry	☒	^ v	Edit Delete

5.3 Port Trigger

Network > Firewall > Port Trigger

Port triggering is typically used for applications that require a range of ports to be dynamically opened on request to an internal device on your network. The router will wait for a request on a specific port or range of ports (trigger port) from a device on your network and once a request is detected by your router, the router will forward a port or range of ports (match port) to the device on your network.

1. Log into your router management page.
2. Click on **Network**, click on **Firewall**, and click on the **Port Trigger** tab.

3. Review the settings below. When complete, click **Add** to add the new entry to the list, **Save** to save the settings, and **Apply** to save and commit your changes. The **Cancel** button will delete any unsaved changes and refresh the page.

4. After being added, the new port trigger rule will appear in the 'Port Trigger Rules' section. The port trigger rule can be enabled or disabled by clicking on the checkbox labelled 'Enable'.

Port Trigger Rules

Name	Interface	Match port	Trigger port	Schedule	Enable	Sort	
PortTriggerRule 1	WWAN (Cellular A)	IPv4-TCP, UDP Via ?	IPv4-TCP, UDP To ?	No Schedule Entry	☐	^ v	Edit Delete

Add New Port Trigger Rule

Name:

Interface:

Match protocol:

Match port:

Trigger protocol:

Trigger port:

Schedule:

[Add](#)

- **Name** – Enter a name for the new port trigger rule.
- **Match Protocol** – Click the drop-down list to select the match port protocol for the service to allow: **TCP, UDP, or TCP+UDP**.
- **Match Port** – Enter the match port number for the service to allow.

Note: You can also enter a consecutive range of ports in the following format: 80-90

- **Trigger Protocol** – Click the drop-down list to select the trigger port protocol for the service to allow: **TCP, UDP, or TCP+UDP**.
- **Trigger Port** – Enter the trigger port number for the service to allow.

Note: You can also enter a consecutive range of ports in the following format: 80-90

- **Schedule** – Allows you to select a schedule when the port trigger rule should be enabled or disabled. Instructions for creating time schedules are in Section 3.5.

5.4 Traffic Rules

Network > Firewalls – Traffic rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

1. Log into your router management page.
2. Click on Network, click on Firewall, and click on the Traffic Rules tab.
3. Review the settings below. When complete, click **Save** to save the settings and **Apply** to save and commit your changes. The **Cancel** button will delete any unsaved changes and refresh the page.

Added Traffic Rules will appear in the Traffic Rules list. The traffic rules can be enabled/disabled using the 'Enable' checkbox, reordered using the 'Sort' up and down arrows, and edited or deleted using the correspondingly labelled buttons.

Name	Match	Action	Schedule	Enable	Sort	
Drop-WtoL-Ping	IPv4-icmp with type <i>echo-request</i> From <i>any host</i> in <i>WAN</i> To IP <i>192.168.10.1</i> on <i>this device</i>	<i>Discard input</i>	No Schedule Entry	☒	^ v	Edit Delete
Allow-IGMP	IPv4-igmp From <i>any host</i> in <i>WAN</i> To <i>any router IP</i> on <i>this device</i>	<i>Accept input</i>	No Schedule Entry	☒	^ v	Edit Delete
Allow-DNSv6	IPv6-traffic From <i>any host</i> in <i>WAN</i> with source port <i>53</i> To <i>any router IP</i> on <i>this device</i>	<i>Accept input</i>	No Schedule Entry	☒	^ v	Edit Delete
Allow-DHCPv6	IPv6-udp From IP range <i>fe80::/10</i> in <i>WAN</i> with source port <i>547</i> To IP range <i>fe80::/10</i> at port <i>546</i> on <i>this device</i>	<i>Accept input</i>	No Schedule Entry	☒	^ v	Edit Delete
Allow-MLD	IPv6-icmp with types <i>130/0, 131/0, 132/0, 143/0</i> From IP range <i>fe80::/10</i> in <i>WAN</i> To <i>any router IP</i> on <i>this device</i>	<i>Accept input</i>	No Schedule Entry	☒	^ v	Edit Delete
Allow-ICMPv6-Input	IPv6-icmp with types <i>echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement</i> From <i>any host</i> in <i>WAN</i> To <i>any router IP</i> on <i>this device</i>	<i>Accept input</i> and limit to <i>1000</i> pkts. per <i>second</i>	No Schedule Entry	☒	^ v	Edit Delete
Allow-ICMPv6-Forward	IPv6-icmp with types <i>echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type</i> From <i>any host</i> in <i>WAN</i> To <i>any host</i> on <i>any zone</i>	<i>Accept forward</i> and limit to <i>1000</i> pkts. per <i>second</i>	No Schedule Entry	☒	^ v	Edit Delete

If it is required to allow traffic with certain custom port number/(s), the ports can be opened on the router via "Open ports on router". After clicking 'Add' the rule will appear in the Traffic Rules list.

Open ports on router

Name

New input rule

Protocol

TCP+UDP

External port

Schedule

Disable time schedule

Add

A new forward rule can be added from the New forward rule section. After clicking 'Add and edit...' an edit menu will pop up.

New forward rule

Name

New forward rule

Source interface

LAN

Destination interface

WAN

Schedule

Disable time schedule

Add and edit...

After inputting the correct settings in the editing menu, click on **Save** and **Apply**. The **Cancel** button will delete any edits made to the traffic rule and refresh the editing menu.

5.5 Denial of Service (DOS) prevention

Network > Firewall > DoS Prevention

The router supports prevention against common denial of service (DoS) attacks. Malicious users use denial of service attacks to temporarily or permanently disrupt the availability of services from network resources such as your router. Typically, DoS attacks are achieved by flooding a specific network resource by excessively sending unnecessary requests which can cause the network device or resource to stop functioning.

1. Log into your router management page.
2. Click on Network, click on Firewall, and click on the DoS Prevention tab.

Review the settings below. When complete, click Add to add the new entry to the list, Save to save the settings, and Apply to save and commit your changes. The Cancel button will delete any unsaved changes and refresh the page. Choose the DoS prevention type to enable, TCP SYN flood, UDP flood, or ICMP flood.

- Enable – Check this option to enable DoS prevention.
- Rate (times per second) – This value limits the number of packets that can be received by the router per second for a specific session.
- Burst – This value limits the total number of packets that can be received and stored in buffer memory for a specific session.

TCP SYN Flood Prevention

Enable ☒

Rate (times per second) 25

Burst 50

UDP Flood Prevention

Enable ☐

ICMP Flood Prevention

Enable ☐

Apply

Save

Cancel

5.6 DMZ Host

Network > Firewall > DMZ Host

You may want to expose a specific computer or device on your network to the Internet to allow anyone to access it. Your router includes the DMZ (Demilitarized Zone) feature that makes all the ports and services available on the WAN/Internet side of the router and forwards all ports to a single IP address (computer or network device) on your network. The DMZ feature is an easy way of allowing access from the Internet, however, it is a very insecure method and will open your local area network to greater threats from Internet attacks. It is recommended to use port forwarding instead to limit rules to specific ports/services only.

1. Log into your router management page.
2. Click on **Network**, click on **Firewall**, and click on the **DMZ Host** tab.
3. Review the settings below. When complete, click **Save** to save the settings, and **Apply** to save and commit your changes. The **Cancel** button will delete any unsaved changes and refresh the page.
 - **Enable** – Check this option to enable DMZ host.
 - **DMZ Host IP Address** - Enter the IP address you assigned to the computer or network device to expose to the Internet. (e.g. 192.168.10.250)

DMZ Host

Enable ☒

DMZ Host IP Address

Apply

Save

Cancel

6 Services Features & Settings

6.1 UPnP and NAT-PMP

Services > UPnP

UPnP (Universal Plug and Play) and NAT-PMP (NAT Port Mapping Protocol) allows devices connected to a network to discover each other and automatically open the connections or services for specific applications (e.g. instant messenger, online gaming applications, etc.) UPnP and NAT-PMP is disabled on your router by default and should only be enabled to allow specific applications required by your computers or devices to allow connections through your router as they are needed.

1. Log into your router management page.
2. Click on **Services** and click on **UPnP**.
3. Under the **UPnP** section, check the **Enable UPnP / NAT-PMP functionality** option. Click **Apply** to save and commit the changes.

UPnP / NAT-PMP settings

Enable UPnP / NAT-PMP functionality ☒

Note: When UPnP/NAT-PMP is enabled, you can check the currently open connections in the UPnP/NAT-PMP entries table.

NAT Port Mapping Protocol (NAT-PMP)

Protocol	External Port	Client Address	Client Port
There are no active redirects.			

7 Administrator Features

7.1 Manage access to local management interface

Administrator > Access Management

This section will allow you to restrict access router management access to specific interfaces. By default, management access to the web interface (HTTP) is restricted only to the LAN interface.

1. Log into your router management page.
2. Click on **Administrator** and click on **Access Management**.
3. Review the settings below. When complete, click **Save** to save the settings, and **Apply** to save and commit your changes. The Cancel button will delete any unsaved changes and refresh the page.

The screenshot displays the 'Access Management' configuration page in the Pyxis Duo web interface. The left sidebar shows the navigation menu with 'Administrator' selected. The main content area is titled 'Access Management' and includes a description: 'This section allows you to configure your local and remote access management.' Below this, there are two sections: 'Local Access Management' and 'Remote Access Management'.

Local Access Management:

- Limit access by interface:** ☒
- Allowed interfaces:** ☒ LAN
- Enable HTTP:** ☐
- Enable HTTPS:** ☐
- Enable Telnet:** ☐
- Enable SSH:** ☒
- Port:** 22
- Password authentication:** ☐
- SSH Keys:** [Download Private Key](#)
- Re-generate SSH Keys:** [Generate New Key](#)

Remote Access Management:

- Limit access by interface:** ☐
- Enable HTTP:** ☐
- Enable HTTPS:** ☒
- Port:** 8443

Local Access Management

- **Limit access by interface** – Checking this option will allow you to select specific local interfaces (e.g. LAN, VLAN) that are allowed access to the router management interface.
- **Allowed interfaces** – The available local interfaces will be in this section. (e.g. Selecting LAN will only allow management access from the LAN and all other VLAN interfaces will be denied.)
- **Enable HTTPS** – Checking this option will enable secure HTTPS (SSL) access to the router management page on the selected local interfaces.
- **Enable Telnet** – Checking this option will enable command line interface access via Telnet on the selected local interfaces.
- **Enable SSH** – Checking this option will enable secure command line interface access via SSH (Secure Shell) on the selected local interfaces.

Local Access Management

Limit access by interface ☒

Allowed interfaces ☒ LAN

Enable HTTP ☐

Enable HTTPS ☐

Enable Telnet ☐

Enable SSH ☒

Port

Password authentication ☐

SSH Keys [Download Private Key](#)

Re-generate SSH Keys [Generate New Key](#)

Remote Access Management

- **Limit access by interface** – Checking this option will allow you to select specific local interfaces (e.g. LAN, VLAN) that are allowed access to the router management interface.
- **Enable HTTPS** – Checking this option will enable secure HTTPS (SSL) access to the router management page on the selected WAN interfaces.
- **Enable SSH** – Checking this option will enable secure command line interface access via SSH (Secure Shell) on the selected WAN interfaces.

7.2 Create time schedules

Administrator > Schedule

Your router allows you to create schedules to specify a time period when a feature should be activated and deactivated. Before you use the scheduling feature on your router, ensure that your router system time and date settings are configured correctly.

1. Log into your router management page
2. Click on **Administrator** and click **Schedule**.
3. Review the settings below. Click **Add** to add the new schedule to the list and **Apply** to save and commit the changes.
 - **Name** – Enter a name for the new schedule rule.
 - **Days** – Choosing **Daily** will set the schedule rule to occur at the specified time every day. Choosing **Select Day(s)** will allow the user to manually select specific days for the schedule.
 - **All Day – 24 Hrs** – Checking this option will set the schedule to run all 24 hours instead of a manually specified period.
 - **Start Time / End Time** – Manually define a-period for the schedule.

Notes:

- The time is specified in 24-hour format.
- After adding a new schedule on this page, a corresponding selection shows in the dropdown list on the *Network>Firewall>Port Forward* page.

Schedule Rules

Name	Days	Start Time	End Time	
Always	Every day	00:00	24:00	Edit Delete

Add New Schedule Rule

Name

Days ☒ Daily ☐ Select Day(s)

☐ Sunday
 ☒ Monday
 ☒ Tuesday
 ☒ Wednesday
 ☒ Thursday
 ☒ Friday
 ☒ Saturday

All Day - 24 Hrs ☐

Start Time

End Time

[Add](#)

[Apply](#)
[Save](#)
[Cancel](#)

Schedule Rules

Name	Days	Start Time	End Time	
Always	Every day	00:00	24:00	Edit Delete
test	Every day	00:00	06:20	Edit Delete

Add New Schedule Rule

Name

Days ☒ Daily ☐ Select Day(s)

☐ Sunday
 ☒ Monday
 ☐ Tuesday
 ☒ Wednesday
 ☐ Thursday
 ☒ Friday
 ☒ Saturday

All Day - 24 Hrs ☐

Start Time

End Time

[Add](#)

[Apply](#)
[Save](#)
[Cancel](#)

Port Forward Rules

Name	Match	Forward to	Schedule	Enable	Sort
This section contains no values yet					

Add New Port Forward Rule

Name

Protocol

External interface

External port

Internal IP address

Internal port

Schedule

[Apply](#)
[Save](#)
[Cancel](#)

7.3 Diagnostic tools

Administrator > Diagnostics

This section includes network tools and utilities for testing connectivity and troubleshooting.

1. Log into your router management page.
2. Click on **Administrator** and click on **Diagnostics**.
3. Review the settings below.

The screenshot displays the Pyxis Duo web management interface. On the left is a sidebar menu with categories: Network, Services, and Administrator. The Administrator section is expanded, showing options like System, Administration, Schedule, Access Management, Diagnostics (which is highlighted), Ping Watchdog, Firmware Update, Reboot, GPIO, and Status. The main content area is titled 'Diagnostics' and contains a 'Network Utilities' section. Under 'Utilities', several options are listed: Ping (selected with a radio button), Traceroute, Nslookup, Speed Test, and MWAN Interface Diagnostics. Below this is the 'Ping' configuration section, which includes a dropdown for 'Interface' set to 'Default', a radio button for 'Protocol' set to 'IPv4' (with 'IPv6' as an option), a text input field for 'Host', and a 'Ping' button at the bottom.

Network Utilities

Ping

This tool conducts a basic ping/connectivity test to a host IP address or domain name. After selecting and entering all the required parameters, click **Ping** to start the connectivity test and the results will appear at the bottom of the page.

- **Interface**
- **Protocol** – Select the IP protocol version for the connectivity test, IPv4 or IPv6.
- **Host** – Enter the host IP address or domain name to test connectivity.

Network Utilities

Utilities
☒ Ping
☐ Traceroute
☐ Nslookup

Ping

Protocol
☒ IPv4
☐ IPv6

Host
8.8.8.8

Ping

Result

```

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=57 time=34.866 ms
64 bytes from 8.8.8.8: seq=1 ttl=57 time=33.583 ms
64 bytes from 8.8.8.8: seq=2 ttl=57 time=33.287 ms
64 bytes from 8.8.8.8: seq=3 ttl=57 time=33.114 ms
64 bytes from 8.8.8.8: seq=4 ttl=57 time=32.650 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet
loss
round-trip min/avg/max = 32.650/33.500/34.866 ms

```

Traceroute

This tool conducts a test to check the routing path taken to reach a specific destination host IP address or domain name. After selecting and entering all of the required parameters, click **Traceroute** to start the connectivity test and the results will appear at the bottom of the page.

- **Protocol** – Select the IP protocol version for the connectivity test, IPv4 or IPv6.
- **Host** – Enter the host IP address or domain name to test connectivity.

The screenshot shows the Pyxis Duo web interface. On the left is a sidebar with a teal header containing the Pyxis Duo logo. The sidebar has three main sections: 'Network' (with a network icon), 'Services' (with a gear icon), and 'Administrator' (with a person icon). Under 'Administrator', there is a list of items: System, Administration, Schedule, Access Management, **Diagnostics** (highlighted with a teal bar), Ping Watchdog, Firmware Update, Reboot, and GPIO. Below this is a 'Status' section with a status icon and a 'Log out' button. The main content area has a teal header with the Pyxis Duo logo and the word 'Diagnostics'. Below this is a section titled 'Network Utilities' containing a list of utilities: Ping, **Traceroute** (selected with a teal circle), Nslookup, Speed Test, and MWAN Interface Diagnostics. Below this list is a section titled 'Traceroute' containing a form with the following fields: 'Interface' (a dropdown menu set to 'Default'), 'Protocol' (radio buttons for 'IPv4' (selected) and 'IPv6'), and 'Host' (a text input field). At the bottom of the form is a teal button labeled 'Traceroute'.

Nslookup

This tool conducts a test to check domain name resolution to an IP address. After entering in the domain name to resolve, click **Nslookup** to start the resolution test and the results will appear at the bottom of the page.

- **Host** – Enter the host IP address or domain name to test resolution.

The screenshot shows the Pyxis Duo web interface. On the left is a sidebar with a teal header containing the Pyxis Duo logo. The sidebar has three main sections: 'Network' (with a network icon), 'Services' (with a gear icon), and 'Administrator' (with a person icon). Under 'Administrator', there is a list of items: System, Administration, Schedule, Access Management, **Diagnostics** (highlighted with a teal bar), Ping Watchdog, Firmware Update, Reboot, and GPIO. Below this is a 'Status' section with a status icon and a 'Log out' button. The main content area has a teal header with the Pyxis Duo logo and the word 'Diagnostics'. Below this is a section titled 'Network Utilities' containing a list of utilities: Ping, Traceroute, **Nslookup** (selected with a teal circle), Speed Test, and MWAN Interface Diagnostics. Below this list is a section titled 'Nslookup' containing a form with the following fields: 'Host' (a text input field). At the bottom of the form is a teal button labeled 'Nslookup'.

Speed Test

Diagnostics

Network Utilities

Utilities
☐ Ping
☐ Traceroute
☐ Nslookup
☒ Speed Test
☐ MWAN Interface Diagnostics

Speed Test

Interface
Default
Format
☒ Simple
☐ Verbose
Speedtest

Speed Test

Interface
WWAN (C16QS-AN)
Format
☐ Simple
☒ Verbose
SpeedTest

MWAN Interface Diagnostics

MWAN Interface Diagnostics
Check the interface status via Multiple WAN Management (MWAN). IPv4 Only.

Interface
WWAN (C16QS-AN)

Ping default gateway
Ping tracking IP
Check IP rules
Check routing table

MWAN Diagnostic Results

Command:

```
ping -I 'wwan2' -c 5 -W 1 '8.8.8.8' 2>&1
```

Result:

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=114 time=66.978 ms
64 bytes from 8.8.8.8: seq=1 ttl=114 time=25.630 ms
64 bytes from 8.8.8.8: seq=2 ttl=114 time=31.073 ms
64 bytes from 8.8.8.8: seq=3 ttl=114 time=66.016 ms
64 bytes from 8.8.8.8: seq=4 ttl=114 time=24.710 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 24.710/42.881/66.978 ms
```

7.4 Backup and restore configuration settings

Administrator>Firmware Update

1. Log into your router management page.
2. Click on **Administrator**, then click on **Firmware Update**

Firmware Update

Backup / Restore

Download backup **Generate Archive**
Click "Generate archive" to download a tar archive of the current configuration files.

Restore backup **Choose File** **No file chosen** **Upload Archive**
To restore configuration files, you can upload a previously generated backup archive here.

Reset to defaults **Perform Reset**
To reset the firmware to its initial state, click "Perform reset".

Router Firmware Update Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration.

Keep settings ☒

Image **Choose File** **No file chosen** **Flash Image**

Cellular A Firmware Information and Updates

Module Cat-4

Current Version --

Image **Choose File** **No file chosen** **Flash Image**
Upload a cellular module image here to replace the running firmware.

Cellular B Firmware Information and Updates

Module --

Current Version --

Image **Choose File** **No file chosen** **Flash Image**
Upload a cellular module image here to replace the running firmware.

You may have added many customized settings to your router and in the case that you need to reset your router to factory defaults, all your customized settings will be lost. This will require you to manually reconfigure all of your router settings instead of simply restoring from a backed-up router configuration file.

Backup / Restore

To backup your router configuration:

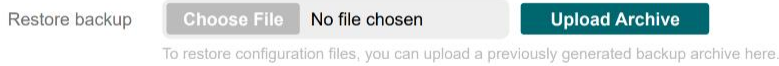
Next to Download backup, click **Generate Archive**.

Download backup **Generate Archive**
Click "Generate archive" to download a tar archive of the current configuration files.

Depending on your web browser settings, you may be prompted to save the configuration file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: backup- **PyxisDuo** -YYYY-MM-DD.dat)

To restore your router configuration:

Next to Restore backup, click **Choose File**.



1. A separate file navigation window should open.
2. Select the router configuration file to restore and click **Upload Archive** (Default Filename: backup- **PyxisDuo** -YYYY-MM-DD.dat). If prompted, click **Yes** or **OK**.
3. Wait for the router to restore settings.

To reset the firmware to its initial state (factory default):

- Click "Perform reset"

Router Firmware Update

To flash new router firmware image:

1. Check on Keep setting checkbox to retain current configuration. If unchecked, the configuration will be reset to default settings.
2. Next to 'Image', click **Choose File**, then select the FW file you want to use.
3. Click **Flash Image** and proceed with the firmware update.

Cellular A Firmware Information and Updates

The cellular module 1 category and firmware version is displayed. The cellular image can be flashed to replace the running firmware.

To flash new firmware image:

1. Next to 'Image', click **Choose File**, then select the FW file you want to use.
2. Click **Flash Image** and proceed with the cellular module firmware update.

Cellular B Firmware Information and Updates

The cellular module 2 category and firmware version is displayed. The cellular image can be flashed to replace the running firmware.

To flash new firmware image:

1. Next to 'Image', click **Choose File**, then select the FW file you want to use.
2. Click **Flash Image** and proceed with the cellular module firmware update.

7.5 Reboot

Administrator > Reboot

You may want to restart your router if you are encountering difficulties with your router and have attempted all other troubleshooting.

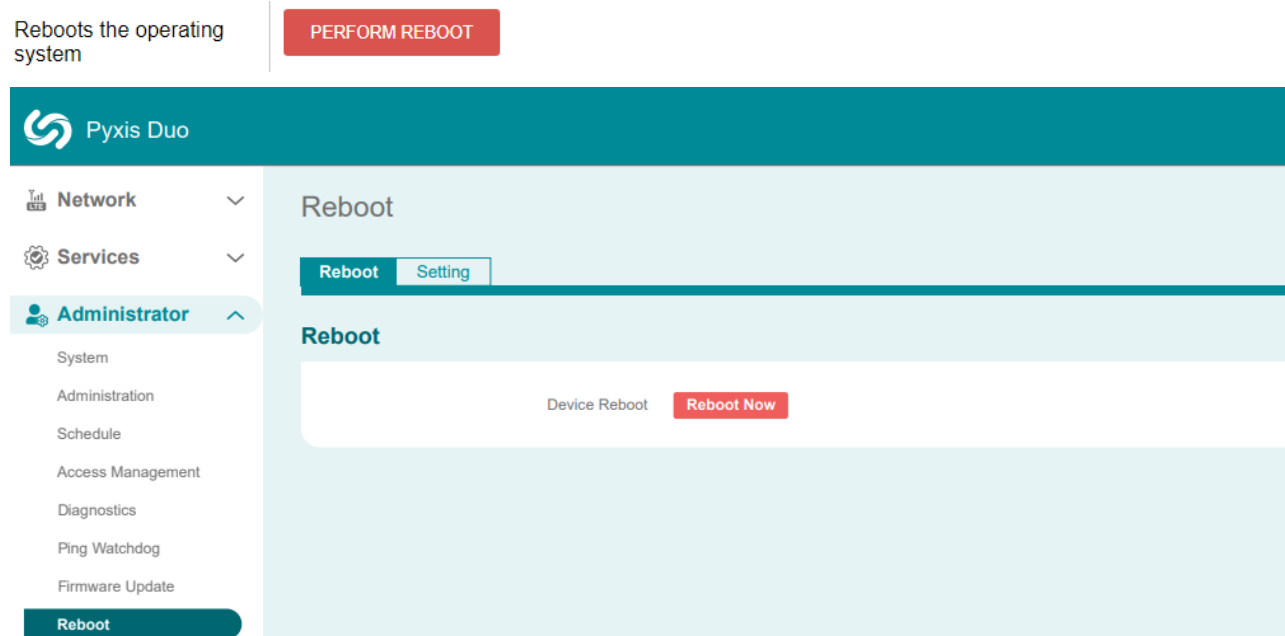
There are two methods that can be used to restart your router.

- 1) **Turn the router** off and wait for 10 seconds. Use this method if you are encountering difficulties with accessing your router management page. This is also known as a hard reboot or power cycle.

OR

2. **Router Management Page** – This is also known as a soft reboot.

1. Log into your router management page.
2. Click on **Administrator**, then click on **Reboot**.
3. Next to Reboot, click **Device Reboot**.



4. Wait for the device to reboot.

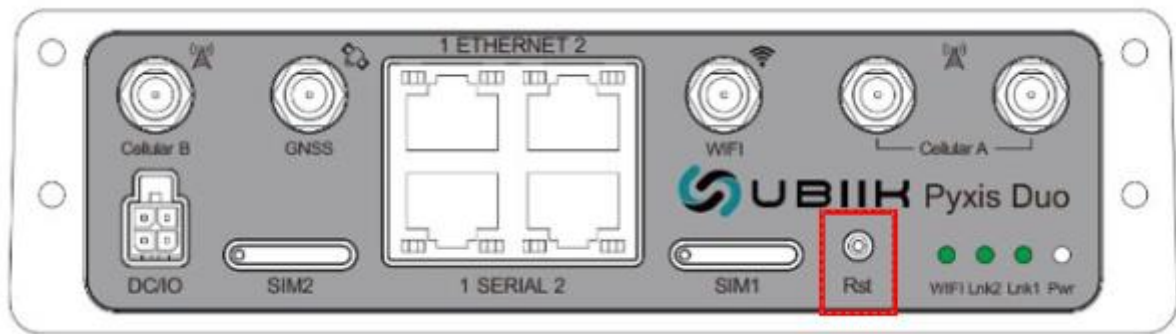
7.6 Reset to factory settings

Administrator > Firmware Update

You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting.

There are two methods that can be used to reset your router to factory defaults.

- **Reset Button** – Located on the front panel of your router. Use this method if you are encountering difficulties with accessing your router management page. Press the Rst for 10 seconds using a pin.



OR

• Router Administrator Page

1. Log into your router management page.
2. Click on **Administrator**, then click on **Firmware Update**
3. Next to Reset to defaults, click **Perform Reset**. When prompted to confirm this action, click **OK**.

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset".

Download backup	Generate Archive
Restore backup	Choose File No file chosen Upload Archive
Reset to defaults	Perform Reset

4. Wait for the router settings to revert to factory default.

7.7 Ping Watchdog

Administrator > Ping Watchdog

The Ping Watchdog feature allows you to configure your router to monitor connectivity to a specific host IP address. If connectivity is lost to the specified host IP address, the router will automatically initiate a device reboot in an automatic attempt to re-establish previously lost connectivity.

1. Log into your router management page.
2. Click on **Administrator** and click on **Ping Watchdog**.
3. Review the settings below. When complete, click **Apply** to save and commit your changes.

Local Access Management

- **Enable** – Check this option to enable the ping watchdog feature.
- **Ping Host / Interface** – Enter the IP address to monitor and send ping requests to check connectivity.

Note: You can add additional host IP address entries to monitor by clicking .

- **ALL** – Check all local and WAN interfaces for the specified host IP address.
- **LTE** – Check the WAN interface for the specified host IP address.

- **Import Default Gateway** – Clicking this option will automatically attempt to copy WAN interfaces default IP gateway to an available entry.
- **Ping Interval** – Enter interval time for the router to send ping and connectivity check. Example: Setting the interval to 5 Minutes will configure to send a ping and check connectivity every 5 minutes.
- **Fail Count to Perform Reboot** – Once ping/connectivity check fails, this sets the maximum number of attempts the router will attempt to check connectivity before initiating an automatic reboot.

Ping Watchdog

Enable ☒

Ping Host / Interface

Import Default Gateway

/ ALL

ALL

WWAN

Ping Interval

5

Minutes

?

 Range: 5~1440 minutes or 1~24 hours

Fail Count To Perform Reboot

1

?

 Range: 1~100

7.8 GPIO Settings

Administrator > GPIO

The GPIO Settings page allows configuration of the router's digital input/output pins for integration with external sensors, relays, alarms, or other control systems.

Each GPIO channel (Digital I/O 1 and Digital I/O 2) can be independently configured as an input or one of two output types.

1. Go to **GPIO Settings**.
2. For each **Digital I/O**:
 - a. Set **Direction**:
 - i. Input
 - ii. Push-Pull Output
 - iii. Open Collector Output
3. Set **Value** (High/Low) if using Output.
4. Click **Apply**, then **Save**.

GPIO Settings

DIGITAL I/O 1

Direction

Value

DIGITAL I/O 2

Direction

Value

Configuration Options:

Field	Description
Direction	Defines the mode of operation for the GPIO pin: Input: Used to read digital signals (e.g., sensor status). Push-Pull Output: Drives high or low voltage actively for controlling external devices. Open Collector Output: Provides an open-drain output, typically used with external pull-up resistors. Value Current or default logic level: Low: 0V / logic 0 High: 3.3V or 5V depending on hardware (logic 1) (Note: Value is only configurable when Direction is set to an output type.)

Use Cases:

- Input Mode: Monitor door sensors, motion detectors, or push buttons.
- Push-Pull Output: Control LEDs, relays, or buzzers.
- Open Collector Output: Interface with industrial control systems requiring isolated switching.

7.9 Firmware Management

Local Update Methods

1. Web GUI Update

- Navigate to Administrator > Firmware Update
- Select firmware file using "Choose File"
- Check "Keep settings" to preserve configuration
- Click "Flash Image" and wait for completion

2. SSH/CLI Update

- Upload firmware via SCP to /tmp directory
- Use sysupgrade command with appropriate flags

- Requires technical knowledge of OpenWrt procedures

Note: Pyxis Duo has dual-image, and in case of FW upgrade failure or file corruption the device will automatically switch to another image to bootup again.

Remote Update Capability

- goNMS Managed Updates: Centralized firmware management (when available)
- Scheduled Maintenance: Plan updates during off-peak hours
- Configuration Preservation: Automatic backup before updates

Update Verification Checklist:

- ☐ Backup current configuration before update
- ☐ Verify firmware file integrity and compatibility
- ☐ Test connectivity after update completion
- ☐ Document firmware version and date
- ☐ Verify all services operational post-update

Firmware File Naming Convention:

- Router firmware: pyxis-duo-[version]-[date].bin
- Cellular Module A: cellular-a-[version].bin
- Cellular Module B: cellular-b-[version].bin

For firmware updates and technical support, contact: support@ubiik.com

8 Status Features

8.1 Status Overview

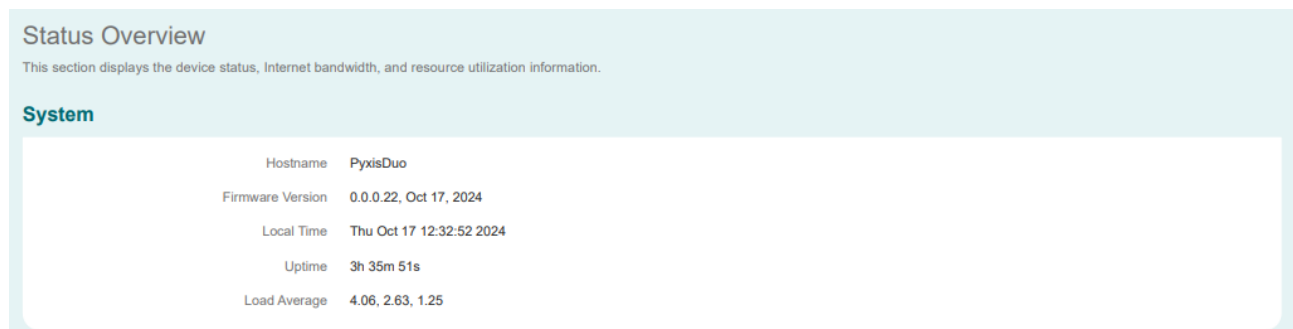
Status > Overview

You may want to check the system information of your router firmware, S/N, uptime, available memory, active connection, WAN interface information, wireless interface information, DHCP clients, connected wireless clients, dynamic DNS and active UPnP entries.

1. Log into your router management page.
2. Click on **Status** and click on **Overview**.

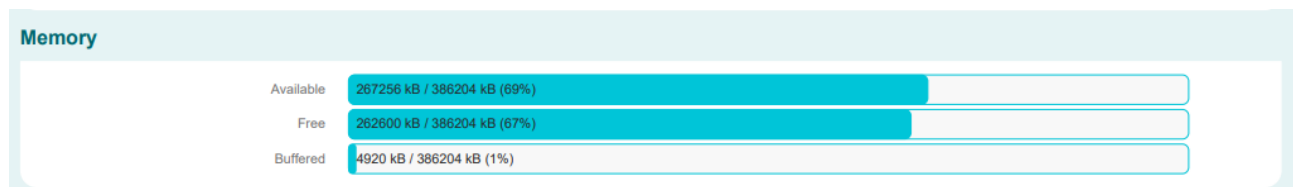
System

- **Hostname** – Displays the currently assigned hostname of the router. This is the name other network devices identify the router by on the network.
- **Firmware Version** – Displays the currently loaded firmware version and date.
- **Local Time** – Displays the current device time and date.
- **Uptime** – Displays the total amount of time the router has been up and running without reboot.



Memory

Displays the available, free and buffered memory status.



Network

- **LTE (Cellular A) IPv4 Status** – Displays the current IPv4 status
- **LTE (Cellular B) IPv4 Status** – Displays the current IPv4 status

Network

WWAN (Cellular A)

IPv4 Status

Type: DHCP client
Address: 192.168.10.32
Netmask: 255.255.255.0
Gateway: 192.168.10.254
DNS 1: 8.8.8.8
Connected: 3h 35m 51s

WWAN (Cellular B)

IPv4 Status

Type:
Address:
Netmask:
Gateway:
DNS 1:
DNS 2:
Connected:

Active Connections

95 / 8192 (1%)

DHCP Leases

This displays the current valid DHCP leases along with their remaining time.

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
There are no active leases.			

Wi-Fi

This displays the status of 2.4GHz Wi-Fi Network.

Wi-Fi

Wi-Fi 2.4GHz

SSID: [Pyxis Duo](#)
Mode: Access Point
Channel: 1 (2.412 GHz)
Speed: 286 Mbit/s
BSSID: 00:03:7F:12:34:56
Encryption: WPA2 Personal

Associated Stations

Associated Stations

MAC Address	Band	Network	Signal	RX Rate	TX Rate
No information available					

MWAN Interfaces

MWAN Interfaces

Selected Primary: WWAN (Cellular A)

Interface: WWAN (Cellular A)
Status: Online

Interface: WWAN (Cellular B)
Status: --

8.2 LTE Status

Status > LTE

This section displays the LTE module and firmware information as well as its network and connection status. If the status is connected, it displays the connection KPIs RSSI, RSRP and RSRQ.

WWAN Status	
Cellular A	
Module	Cat-4
Firmware Version	Cellular_A_v0.2.3
Connection Status	Connected
Connection Type	4G
Network	FL1
IPv4 Address	192.168.3.3
Current Radio Band	8
RSRP	-63 dBm
RSRQ	-3 dBm
RSSI	-59 dBm
IMEI	35470000058875
IMSI	99970000072699
ICCID	123456789012345678901
Cellular B	
Module	Cat-1
Firmware Version	Cellular_B_v1.5.1
Connection Status	Connected
Connection Type	4G
Network	00101
IPv4 Address	192.168.3.2
Current Radio Band	8
RSRP	-63 dBm
RSRQ	-3 dBm
RSSI	-59 dBm
IMEI	QCLC110050E
IMSI	99970000072699
ICCID	123456789012345678901

8.3 Real Time Graphs

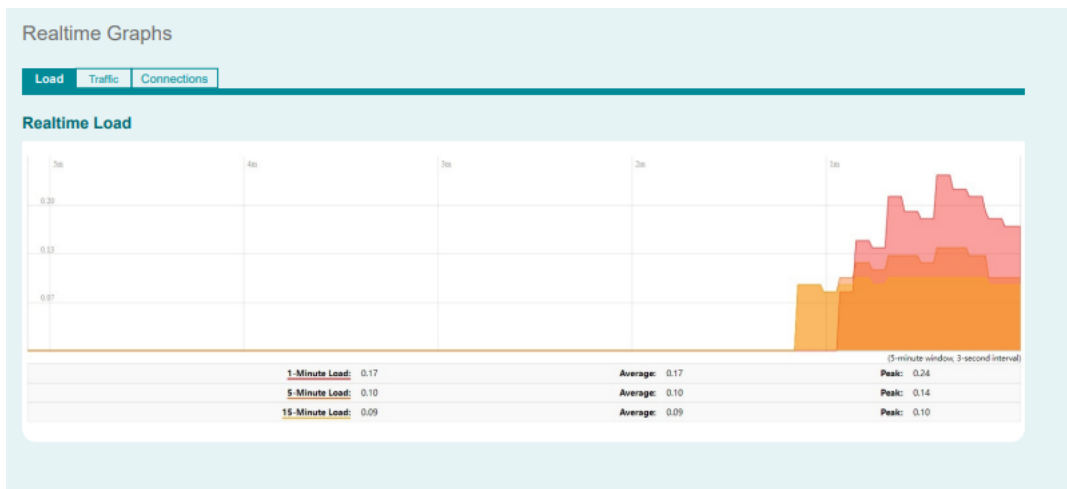
Status > Realtime Graphs

This section displays the device real-time CPU load, traffic load, and connection/session information.

CPU Load

This chart shows the load of the CPU in 1 minute, 5 minutes, and 15 minutes intervals.

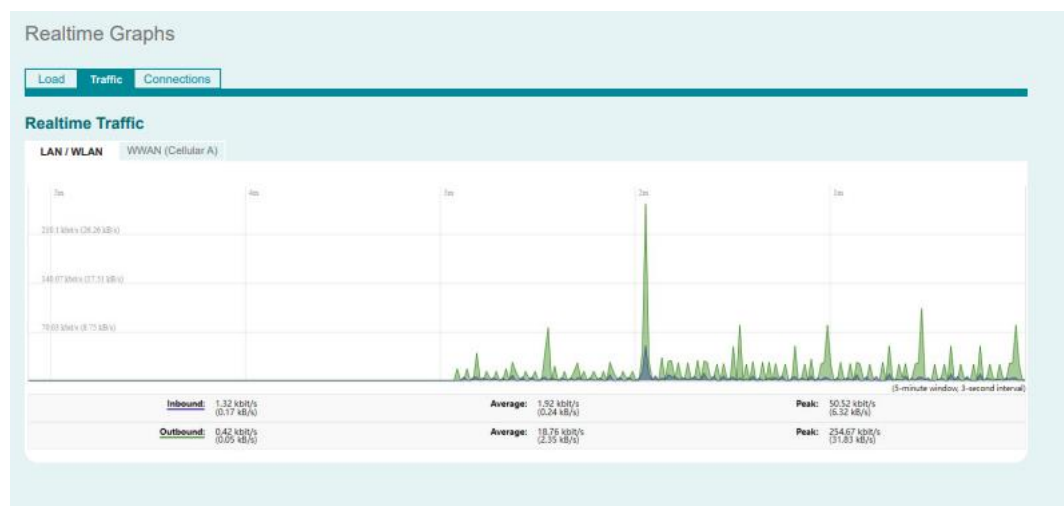
- Red graph: Displays the CPU load in the last 1 minute
- Orange graph: Displays the CPU load in the last 5 minutes
- Yellow graph: Displays the CPU load in the last 15 minutes



Traffic Load

This chart shows the real-time traffic load

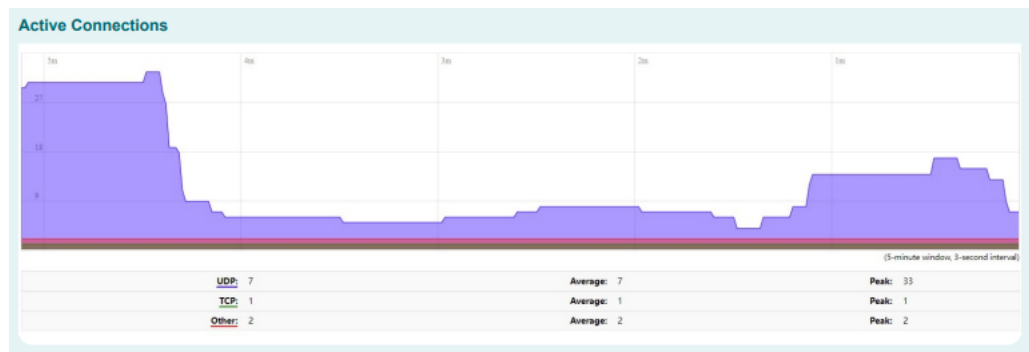
- Blue graph: Displays the inbound traffic
- Green graph: Displays the outbound traffic



Connections

This chart shows the connection and session information

- Blue graph: Displays the connections with UDP protocol
- Green graph: Displays the connections with TCP protocol
- Red graph: Displays the connections that do not use UDP or TCP protocol



8.4 View routing table and ARP entries

Status > Routes

You may want to check the current routing table and ARP entry information for troubleshooting or monitoring purposes.

1. Log into your router management page.
2. Click on **Status** and click on **Routes**.

ARP

Displays the router ARP table.

ARP		
Network	IPv4 address	MAC address
LAN	192.168.10.136	D8:CB:8A:F2:44:C5

Active IPv4-Routes

Displays the current IPv4 active routing table.

Active IPv4 Routes				
Network	Target	IPv4 gateway	Metric	Table
LAN	192.168.10.0/24		0	main
VLAN3	192.168.55.0/24		0	main

Active IPv6-Routes

Displays the current IPv6 active routing table.

Active IPv6 Routes				
Network	Target	Source	Metric	Table
(eth1)	ff00::/8		256	local
VLAN3	ff00::/8		256	local
(eth1)	ff00::/8		256	local
VLAN3	ff00::/8		256	local

IPv6 Neighbors

Displays currently discovered/detected IPv6 neighbor devices.

IPv6 Neighbours

Network

IPv6 address

MAC address

<< This section contains no values yet >>

8.4.1 Key Performance Indicators (KPI) Monitoring

Purpose: Real-time performance monitoring reference for optimal operation and proactive issue identification.

Cellular Network KPIs

Access via Status > LTE for real-time monitoring:

Metric	Optimal Range	Action Required If Outside Range
RSRP (Signal Strength)	>-90 dBm (Excellent)	<-110 dBm: Check antenna positioning
	-90 to -100 dBm (Good)	<-120 dBm: Relocate or improve antennas
	-100 to -110 dBm (Fair)	
RSRQ (Signal Quality)	>-10 dB (Excellent)	<-20 dB: Network congestion
	-10 to -15 dB (Good)	Contact carrier for optimization
	-15 to -20 dB (Fair)	
SINR (Signal-to-Noise)	>20 dB (Excellent)	<0 dB: Check antenna isolation
	13-20 dB (Good)	Investigate interference sources
	0-13 dB (Fair)	
Throughput	>80% of carrier specification	<50%: Optimization required
Latency	<30ms (Real-time applications)	>100ms: Network investigation
	<50ms (General use)	required
Packet Loss	<0.1% (Optimal)	>1%: Immediate investigation
	<1% (Acceptable)	required

System Health KPIs

Access via Status > System Log and Status > Realtime Graphs:

Metric	Optimal Range	Action Required If Outside Range
CPU Utilization	<70% average load	>90%: Reduce QoS complexity
Memory Usage	<80% of available	>95%: Clear logs, restart if needed
Operating Temperature	-40°C to +70°C	>70°C: Improve ventilation
System Uptime	>99.9% monthly target	<99%: Investigate failure patterns
Power Consumption	3.5W idle, <11.4W peak	>12W: Check for system issues

Performance Optimization Actions

For Signal Quality Issues:

1. Navigate to Status > LTE to check real-time signal metrics
2. If RSRP <-100 dBm: Adjust antenna positioning using real-time feedback
3. If RSRQ <-15 dB: Check for network congestion during off-peak hours
4. If SINR <10 dB: Verify antenna separation and check for interference

For System Performance Issues:

1. Navigate to Status > Realtime Graphs for trend analysis
2. High CPU: Review QoS configuration complexity in Network > QoS
3. High Memory: Check log file sizes in Status > System Log
4. High Temperature: Verify adequate ventilation and ambient conditions below +70°C

Weekly Performance Review Checklist:

- Review signal quality trends for degradation patterns
- Check system resource utilization for capacity planning
- Verify uptime targets are being met consistently
- Monitor throughput performance against baseline measurements
- Review error logs for recurring issues requiring attention

Monthly Optimization Review:

- Compare current month's performance to previous month's baseline
- Identify peak usage patterns and optimize resource allocation
- Update performance baselines based on usage growth
- Schedule preventive maintenance based on environmental conditions
- Plan capacity upgrades if performance trends indicate future needs

8.5 Logging

Status > System Log

Your router system log can be used to obtain activity information on the functionality of your router or for troubleshooting purposes.

1. Log into your router management page.
2. Click on **Status** and click on **System Log**.

Note: The router system log will display the most recent entries in the list.

Time	Level	Source	Message
Fri Oct 18 03:28:04 2024	daemon.notice	easycwmpd	sending Inform failed
Fri Oct 18 03:28:04 2024	daemon.notice	easycwmpd	external: execute apply service
Fri Oct 18 03:28:04 2024	daemon.notice	easycwmpd	external script exit
Fri Oct 18 03:28:04 2024	daemon.notice	easycwmpd	end session failed
Fri Oct 18 03:28:04 2024	daemon.notice	easycwmpd	retry session in 3840 sec, RetryCount = 53
Fri Oct 18 03:28:11 2024	daemon.notice	netifd	Interface 'wwan' is now down
Fri Oct 18 03:28:11 2024	daemon.notice	netifd	Interface 'wwan' is setting up now
Fri Oct 18 03:28:11 2024	user.notice	root	qmi bringup failed, retry in 10s
Fri Oct 18 03:28:11 2024	daemon.notice	netifd	Interface 'wwan2' is now down
Fri Oct 18 03:28:11 2024	daemon.notice	netifd	Interface 'wwan2' is setting up now
Fri Oct 18 03:28:11 2024	user.notice	root	qmi bringup failed, retry in 10s
Fri Oct 18 03:28:21 2024	daemon.notice	netifd	Interface 'wwan' is now down
Fri Oct 18 03:28:21 2024	daemon.notice	netifd	Interface 'wwan' is setting up now
Fri Oct 18 03:28:21 2024	user.notice	root	qmi bringup failed, retry in 10s
Fri Oct 18 03:28:21 2024	daemon.notice	netifd	Interface 'wwan2' is now down
Fri Oct 18 03:28:21 2024	daemon.notice	netifd	Interface 'wwan2' is setting up now
Fri Oct 18 03:28:22 2024	user.notice	root	qmi bringup failed, retry in 10s
Fri Oct 18 03:28:31 2024	daemon.notice	netifd	Interface 'wwan' is now down
Fri Oct 18 03:28:31 2024	daemon.notice	netifd	Interface 'wwan' is setting up now
Fri Oct 18 03:28:31 2024	user.notice	root	qmi bringup failed, retry in 10s
Fri Oct 18 03:28:32 2024	daemon.notice	netifd	Interface 'wwan2' is now down
Fri Oct 18 03:28:32 2024	daemon.notice	netifd	Interface 'wwan2' is setting up now
Fri Oct 18 03:28:32 2024	user.notice	root	qmi bringup failed, retry in 10s
Fri Oct 18 03:28:42 2024	daemon.notice	netifd	Interface 'wwan' is now down
Fri Oct 18 03:28:42 2024	daemon.notice	netifd	Interface 'wwan' is setting up now

9 Maintenance & Lifecycle Management

9.1 Preventive Maintenance Schedule

To ensure the health of your Ubiik network, we recommend carrying out regular monitoring and inspections. Below are some suggested checks for performance on a daily, weekly, monthly and quarterly basis.

Daily Checks (Automated Monitoring)

- **Signal Strength Monitoring:** RSRP/RSRQ thresholds
- **Temperature Monitoring:** Operating within -40°C to +70°C
- **Power Supply Monitoring:** Voltage stability
- **Memory Usage:** RAM and flash utilization

Weekly Checks (5 minutes)

- LED status verification
- Log file review for errors
- Configuration backup verification
- Performance metrics review

Monthly Checks (15 minutes)

- Antenna connection inspection
- Cable condition assessment
- Grounding verification
- Enclosure condition check
- Firmware update availability

Quarterly Checks (30 minutes)

- Full configuration audit
- Security patch assessment
- Performance baseline update
- Documentation update
- Spare parts inventory

9.2 Field Deployment Checklist

Pre-Installation Checklist

- [] Site survey completed (signal strength >-100 dBm RSRP)
- [] Power source verified (9-60 VDC, stable supply)
- [] SIM cards activated and tested in mobile device
- [] Antenna mounting locations selected (clear line-of-sight)
- [] Grounding point identified and prepared
- [] Configuration laptop prepared with Ethernet capability

15-Minute Field Deployment Procedure:

Step 1: Physical Installation (5 minutes)

1. **Mount Device** using DIN rail or wall bracket
2. **Connect Grounding** strap to unused mounting screw
3. **Install Antennas:**
 - o LTE antennas → Cellular A & B ports
 - o Wi-Fi antenna → Wi-Fi port
 - o GNSS antenna → GNSS port (if required)
4. **Insert SIM Cards** (power OFF device first)

Step 2: Power and Initial Connection (3 minutes)

1. **Connect Power** (verify polarity: Pin 1=Ground, Pin 2=Positive)
2. **Power ON** - verify Power LED goes solid white
3. **Connect Ethernet** from laptop to any LAN port
4. **Wait for Boot** - LTE LEDs will progress: OFF → Flashing → Solid Green (2-5 minutes)

Step 3: Local Configuration Access (2 minutes)

1. **Configure Laptop** network adapter:
 - o IP: 192.168.10.50
 - o Subnet: 255.255.255.0
 - o Gateway: 192.168.10.1
2. **Access Web Interface:** <https://192.168.10.1>
3. **Login** with admin/admin credentials
4. **IMMEDIATE SECURITY:** Change password to strong 12+ character password

Step 4: Network Configuration (5 minutes)

1. **Navigate to Network > LTE**
2. **Configure APN** settings for your carrier
3. **Verify Signal Strength** in Status > LTE (target RSRP >-100 dBm)
4. **Test Connectivity** using Diagnostics > Ping (ping 8.8.8.8)
5. **Save Configuration** via System > Backup

9.3 Performance Monitoring

Performance of your Ubiik equipment can be monitored against standard Key Performance Indicators (KPIs). Some suggested KPIs are listed below:

1. **Signal Quality Metrics:**

- RSRP: Target >-100 dBm
- RSRQ: Target >-15 dB
- SINR: Target >0 dB

2. **Network Performance:**

- Throughput: Monitor vs. carrier specifications
- Latency: <200 ms for real-time applications
- Packet Loss: $<1\%$ under normal conditions

3. **System Health:**

- CPU Utilization: $<80\%$ average
- Memory Usage: $<85\%$ of available
- Temperature: Within operational range

9.4 Performance Optimization Techniques

To optimize the performance of your Ubiik network/equipment, we would recommend the following optimization techniques:

1. **Antenna Optimization:**

- Regular VSWR measurements
- Optimal positioning for signal strength
- Periodic cleaning and inspection

2. **Network Configuration:**

- QoS tuning based on traffic patterns
- Route optimization
- Bandwidth allocation adjustment

3. **Power Management:**

- Sleep mode configuration for battery operation
- Power profile optimization
- Voltage monitoring and regulation

10 How to ... Access Devices Behind Pyxis

The follow section summarizes the different methods to enable remote connection to devices located behind the pyxis router, on the LAN side.

10.1 WAN Configurations

For any of the options outlined below, the Pyxis DUO router WAN IP needs to be known by the computer initiating the connection.

For that purpose, customers should consider the following goRAN™ configurations

- Disable NAT on goRAN™ so the Pyxis router is on the same subnet as the computer on the WAN side
- Or allocate a fixed IP to Pyxis (aka disable DHCP on goRAN™ – similar to a fixed public IP on commercial LTE network)
- Or leveraging dynamic DNS for each Pyxis, so that router hostname could be used (vs IP)

10.2 LAN Configurations

All the options below can use for DHCP or static /manual addressing but NAT set up breaks if a DHCP address change.

Please refer to the corresponding sections above of the document for details on the configuration parameters.

10.2.1 NAT-LESS

The devices behind the Pyxis router are on the same subnet – configuration not recommended.

Configure DHCP Relay to get devices IP from the goRAN™ DHCP Server or set up manual addressing scheme.

10.2.2 NAT

Enable DMZ host to a single LAN device, irrespective of any protocol or port. Configuration not recommended.

Or

Enable port forwarding to route the traffic to different end-points based on the service type – configuration recommended.

Or

One to One static NAT when all public traffic is required to be NATed to a single internal device/end point on the LAN – configuration recommended.

10.3 Change Radio Access Technology between NB-IOT & LTE-M

To switch between NB-IoT and LTE-M the user must:

- Login to the device through SSH with the 'tech' account (default IP is 192.168.10.1 and port is 22; default password is Ubiik123!)
- Open the file `/root/ccm.conf`, e.g. `vi /root/ccm.conf`
i (to edit the file)
wq! (to write and quit)
- The variable `USE_NB` controls the RAT (Radio Access Technology)
USE_NB 0 - Radio module will use LTE-M
USE_NB 1 - Radio module will use NB-IoT
- After changing the file `/root/ccm.conf`, user needs to reboot the unit by unplugging and replugging the unit to power

10.4 Real-World Application Examples

10.4.1 SCADA System Integration over LTE

Scenario:

Remote substation connects to central SCADA server via secure LTE tunnel

Network Topology:

[Remote RTU] ↔ [Pyxis Duo] ↔ [goRAN] ↔ [Embedded EPC] ↔ [SCADA Master] ↓ [Local HMI via Wi-Fi]

Configuration Steps:

Step 1: Basic Network Setup

1. **LAN Configuration:**
 - Navigate to Network > LAN
 - Set IP: 192.168.100.1/24 (avoid conflicts with SCADA network)
 - DHCP Range: 192.168.100.100-150

Step 2: VPN Tunnel for Security

1. **Navigate to VPN > IPsec**
2. **Create Site-to-Site Tunnel:**
 - Tunnel Name: "SCADA-HQ"
 - Remote Gateway: [SCADA server public IP]

- Local Subnet: 192.168.100.0/24
- Remote Subnet: [SCADA network range]
- Encryption: AES-256
- Authentication: SHA-256
- IKE Version: IKEv2

10.4.2 Industrial IoT Gateway with Protocol Conversion

Upstream Flow:

Legacy Devices → Serial (Modbus RTU) → Pyxis Duo → Protocol Gateway → Modbus TCP → LTE → Cloud Platform

Protocol Support:

- Serial Protocols: Modbus RTU, DNP3, IEC 60870-5
- Ethernet Protocols: Modbus TCP, DNP3 over TCP, IEC 61850
- IoT Protocols: MQTT, CoAP, HTTP/HTTPS
- Network Protocols: IPv4/IPv6, VLAN, QoS

10.5 Utility Application Integration

The Pyxis Duo supports comprehensive integration with utility infrastructure including electrical substations, distribution automation systems, and advanced metering infrastructure. Understanding these applications helps optimize configuration for specific utility use cases.

Electrical Substation Integration

Electrical substation integration utilizes IEC 61850 communication standards for integration with protection and control equipment. The Pyxis Duo connects to substation LANs providing cellular connectivity to remote control centers and system operations facilities.

Configure the device for process bus integration when connecting to protection IEDs (Intelligent Electronic Devices) such as protective relays, digital fault recorders, and power quality monitoring equipment. Station bus integration provides connectivity to substation automation systems and SCADA networks for real-time monitoring and control.

Time synchronization is critical for substation applications requiring coordinated operations across multiple devices. Configure IEEE 1588 Precision Time Protocol (PTP) for microsecond-level accuracy needed for synchronized measurements and protection coordination. GPS time synchronization provides an alternative time reference for installations without PTP infrastructure.

GOOSE messaging configuration enables peer-to-peer communication between protection devices for fast fault clearing and automatic switching operations. Configure GOOSE transmission timing to meet protection system speed requirements, typically requiring transmission within 4 milliseconds for critical protection functions.

Distribution Automation Applications

Distribution automation systems utilize the Pyxis Duo for communication with field devices including automatic reclosers, sectionalizing switches, voltage regulators, and capacitor banks. These applications improve system reliability through automated fault location, isolation, and service restoration.

Configure DNP3 protocol for supervisory control of automatic reclosers and switches. Set up appropriate data point mapping for status monitoring, control operations, and metering functions. Configure event reporting for real-time notification of equipment operation and fault conditions.

Voltage regulation applications require communication with voltage regulator controls and capacitor bank controllers. Configure analog measurement reporting for voltage, current, and power factor monitoring. Set up control point configuration for automatic voltage regulation based on system conditions.

Load management applications utilize cellular communication for demand response programs and peak load reduction. Configure load control interfaces for remotely controllable loads such as water heaters, air conditioning systems, and industrial processes. Implement appropriate security measures for load control operations to prevent unauthorized access.

Advanced Metering Infrastructure

AMI (Advanced Metering Infrastructure) applications utilize the Pyxis Duo as a communication gateway for smart meter networks. The device provides cellular backhaul for meter data collection and remote disconnect/reconnect operations.

Configure mesh network interfaces for communication with smart meter networks using protocols such as IEEE 802.15.4 or proprietary mesh networking protocols. Set up data collection parameters for regular meter reading intervals and on-demand reading capabilities.

Implement security measures appropriate for customer billing data including encryption and authentication. Configure data retention policies and backup procedures to ensure billing data integrity. Set up alarm reporting for meter tampering detection and power outage notifications.

Configure remote disconnect/reconnect capabilities for customer service applications. Implement appropriate authorization and logging procedures for service disconnection operations. Set up real-time notification systems for successful operation confirmation.

Network Architecture Planning

Design cellular network architecture to support utility communication requirements including redundancy, security, and performance. Primary communication paths typically utilize 450MHz private LTE networks for dedicated utility use. Secondary communication paths may use public cellular networks for backup connectivity.

Configure automatic failover between primary and secondary communication paths based on signal quality, network availability, and application requirements. Implement appropriate failover timing to minimize service interruption while avoiding unnecessary switching due to temporary signal variations.

Security architecture should implement defense-in-depth principles with multiple layers of protection including network firewalls, VPN encryption, and application-level authentication. Configure monitoring and logging systems to detect unauthorized access attempts and security violations.

Plan network capacity and Quality of Service configuration to support multiple applications with different performance requirements. Real-time protection and control applications require priority handling and guaranteed bandwidth allocation. Routine data collection and monitoring applications can utilize best-effort service levels.

11 Troubleshooting & Support

11.1 Systematic Troubleshooting Methodology

11.1.1 Level 1, Basic Diagnostics (5 minutes)

Ubiik recommends the following actions as your initial troubleshooting steps:

Power and LED Analysis

1. **Power LED Status Check:**
 - OFF: Check power supply, cable connections, fuse
 - Flashing: Firmware issue, attempt recovery
 - Solid: Normal operation
2. **LTE LED Diagnosis:**
 - OFF → No power to module or module failure
 - Slow Flash → Searching for network
 - Fast Flash → Registering with network
 - Solid Green → Connected and operational
3. **Signal Strength Assessment:**
 - Navigate to Status > LTE
 - Target Values: RSRP > -100 dBm, RSRQ > -15 dB
 - If poor signal: Check antenna connections, positioning

Basic Connectivity Tests

- **Local Network Test:**
- ping 192.168.10.1 # Device management interface
- **Internet Connectivity Test:**
 - ping 8.8.8.8 # Google DNS (IPv4)
 - ping 2001:4860:4860::8888 # Google DNS (IPv6)
- **DNS Resolution Test:**
 - nslookup google.com

11.1.2 Level 2, Intermediate Diagnostics (15 minutes)

Network Configuration Verification

1. **APN Settings Validation:**
 - Verify APN matches carrier requirements
 - Check authentication method (PAP/CHAP/None)

- Validate username/password if required

2. **Routing Table Analysis:**

- Navigate to Status > Routes
- Verify default route present
- Check for routing conflicts

3. **Interface Status Check:**

- All interfaces UP and configured
- IP addresses correctly assigned
- No duplicate IP conflicts

Advanced Signal Analysis

1. **Cell Tower Information:**

- Cell ID and tracking area
- Serving vs. neighbor cells
- Handover frequency

2. **Band Lock Testing:**

- Force specific LTE band
- Test signal strength per band
- Identify optimal band for location

11.1.3 Level 3, Advanced Diagnostics (30+ minutes)

Packet Capture and Analysis

1. **Enable Packet Capture:**

- Navigate to Diagnostics > Packet Capture
- Capture interface traffic
- Analyze for errors, retransmissions

2. **Log Analysis:**

- System logs for error patterns
- Authentication failures
- Network registration issues

Factory Reset and Recovery

1. **Configuration Backup:**

- Always backup before reset
- Document current settings

2. **Reset Procedure:**

- Hardware reset: Hold reset button 10 seconds
- Software reset: System > Administration > Factory Reset

11.2 Common Issues and Solutions Matrix

Symptom	Possible Causes	Solution Steps	Prevention
No LTE Connection	Weak signal, incorrect APN, SIM issue	1. Check signal strength 2. Verify APN settings 3. Test SIM in phone 4. Reposition antennas	Use external antennas, verify carrier settings
Slow Internet	Network congestion, antenna placement	1. Test at different timest 2. Check antenna VSWR 3. Enable QoS 4. Consider antenna upgrade	Monitor usage patterns, optimize QoS
VPN Won't Connect	Firewall blocking, key mismatch	1. Check firewall rules 2. Verify certificates 3. Test with different encryption	Use standard ports, maintain certificates
Wi-Fi Issues	Interference, configuration	1. Change channel 2. Check antenna 3. Verify settings	Regular site surveys, proper antenna selection
Device Unresponsive	CPU overload, memory leak	1. Power cycle 2. Check logs 3. Firmware update	
Configuration Lost	Power interruption during config changes, firmware corruption	1. Check for backup files 2. Restore from goNMS 3. Factory reset if needed	Regular configuration backups, UPS power protection

Symptom	Possible Causes	Solution Steps	Prevention
		4. Reconfigure from documented settings	
Poor LTE Performance	Network congestion, antenna issues, carrier limitations	1. Check signal strength at different times 2. Test with different carriers 3. Verify antenna VSWR 4. Consider external antennas	Site survey before deployment, carrier performance testing

11.3 3GPP Interoperability Troubleshooting

Issue	Cause	Solution
Attach Failure to Non-Ubiik eNodeB	Band mismatch, PLMN config	Verify supported bands, check PLMN settings
Poor Performance with 3rd Party eNodeB	Non-optimized parameters	Use standard 3GPP settings, disable proprietary features
Handover Issues	Vendor-specific configurations	Ensure standard X2/S1 handover parameters
QoS Not Working	EPC policy mismatch	Verify QCI mappings, check bearer configurations

11.4 Technical Support

For advanced configuration, technical support:

- **Email:** support@ubiik.com
- **Website:** Visit Ubiik support portal for documentation and firmware updates

11.5 Emergency Recovery Procedures

Serial Console Recovery

1. **Hardware Requirements:**
 - USB-to-Serial adapter
 - Terminal software (PuTTY, TeraTerm)
 - Serial settings: 115200, 8N1
2. **Recovery Process:**
 - Connect to serial console
 - Boot into recovery mode
 - Restore firmware from backup
 - Reconfigure basic settings

Firmware Recovery

1. **TFTP Recovery Mode:**
 - Hold reset during power-on
 - Device enters TFTP recovery
 - Upload firmware via TFTP

12 Ordering Information

Product Name	Model Number	SKU Number	Frequency Band
Pyxis Duo	Pyxis Duo	PLN-LMN00017	Wi-Fi only

12.1 goRAN™-Specific Information:

goRAN™ Integration Specifications

goRAN™-Specific Configuration

Embedded EPC Mode Detection: The Pyxis Duo automatically detects goRAN deployment mode:

- Embedded EPC: Local APN resolution and traffic processing
- External EPC: Standard S1 interface procedures
- Hybrid Mode: Local processing with external connectivity

Optimized Parameters for goRAN™:

- Frequency Bands: ALL
- Power Class: Normal power (23 dBm) supported
- Bandwidth: 5MHz, 3MHz, 1.4MHz auto-selection
- QoS: Enhanced QCI support for industrial applications

goNMS Integration:

- Automatic device discovery and provisioning
- Centralized configuration management
- Performance monitoring and analytics
- Firmware update management
- Alarm correlation between Pyxis and goRAN

Appendix A: Quick Reference Cards

A.1 Default Settings Quick Reference

- Default IP Address: 192.168.10.1
- Default Username: admin
- Default Password: admin (CHANGE IMMEDIATELY)
- Default DHCP Range: 192.168.10.100-199
- Default Wi-Fi SSID: Lemonade_plus_0
- Default Wi-Fi Password: password (CHANGE IMMEDIATELY)
- SSH Port: 22
- HTTP Port: 80 (disable after setup)
- HTTPS Port: 443

A.2 LED Status Quick Reference

Power LED:

- Solid White = Normal operation
- Off = No power
- Flashing = Boot/firmware issue

LTE LEDs:

- Solid Green = Connected
- Flashing Green = Searching
- Off = No module/SIM

Wi-Fi LED:

- Solid Green = Active
- Flashing = Data transfer
- Off = Disabled

A.3 Emergency Recovery Quick Reference

- Hardware Reset: Hold reset button 10 seconds
- Factory Reset: System > Administration > Factory Reset
- Firmware Recovery: TFTP mode (hold reset during power-on)
- Serial Console: 115200, 8N1
- Default Recovery IP: 192.168.1.1

Appendix B: Port and Protocol Reference

B.1 Network Ports

Port	Protocol	Service	Direction
22	TCP	SSH	Inbound
53	UDP	DNS	Outbound
80	TCP	HTTP (disable)	Inbound
123	UDP	NTP	Outbound
161	UDP	SNMP	Inbound
162	UDP	SNMP Traps	Outbound
443	TCP	HTTPS	Inbound
502	TCP	Modbus	Both
514	UDP	Syslog	Outbound
1194	UDP	OpenVPN	Both
20000	TCP	DNP3	Both

B.2 Industrial Protocol Reference

- Modbus RTU: Serial, 1-115200 bps, 8N1/8E1/8O1
- Modbus TCP: Port 502, TCP/IP
- DNP3 Serial: Serial, 1200-115200 bps, 8N1
- DNP3 TCP: Port 20000, TCP/IP
- IEC 61850: Ethernet, multiple ports
- IEC 60870-5-104: Port 2404, TCP/IP

Appendix C: Power Supply Selection

The user may choose from the market power supply of choice, provided that it meets below specifications:

Input	
Rated Input Voltage	100-240Vac
Operating Range	90-264Vac
Rated Input Frequency	50/60Hz +/-3Hz and 400Hz
Rated input current	1.0A max. @Full load&115Vac input
Power consumption (no-loading)	0.1W max
Primary current protection	An adequate internal fuse on the AC input line is provided
Configuration	2 Conductor

Output	
Nominal DC output voltage	+12.0V
Minimum load current	0.0A
Rating load current	3.0A
Peak load current	/
Rating output power	36.0W
Ripple and noise	150 mVp-p
Average efficiency	87.4% minimum

In addition, the chosen power supply unit should comply with safety, EMC, and ESD requirements from local authority.

Recommended Power Supply Models

For 9-60 VDC input range compliance:

1. Industrial DIN Rail Supplies

- Mean Well DR-60-12: 12V/5A output, wide input range
- Phoenix Contact QUINT4: Industrial grade, monitoring capabilities

- Siemens SITOP Smart: Integrated diagnostics

2. Outdoor/Weather-Resistant Options

- Mean Well LPV-60-12: IP67 rated, 12V/5A
- Mornsun LO60-12B12: Compact design, surge protection

3. Utility Substation Applications (48VDC Input)

- Custom DC-DC converters for 48V battery systems
- Contact technical support for substation power requirements

Note: All power supplies must comply with local electrical codes and utility standards. Ubiik does not supply power supplies with the Pyxis Duo unit.

Document History

Issue No.	Date	Description
1	06/2025	Initial version
1.1	07/2025	Updated version taking into account Brazil specifics
1.2	08/2025	Mandatory regulatory compliance update: • ANATEL ATO 915/2024 and ATO 2091/2025 compliance • Band 31 ERP limits (35 dBm max, 9 dBi antenna max) • Temperature specification correction (-40°C to +70°C) • SIM installation procedure clarification • Antenna/power supply compliance notes • All units converted to metric system