

# Yacht Devices

## User Manual

**NMEA 0183 Wi-Fi Gateway YDWN-02**

Firmware version

1.71

**2024**

© 2018—2024 Yacht Devices Ltd. Document YDWN02-002. April 11, 2024.

Web: <http://www.yachtd.com/>.

NMEA 2000® is a registered trademark of the National Marine Electronics Association. SeaTalk NG is a registered trademark of Raymarine UK Limited. Garmin® is a registered trademark of Garmin Ltd.

## Contents

Introduction .....	4
Warranty and Technical Support .....	6
I. Product Specifications .....	7
II. NMEA 0183 Basics .....	9
III. Device Installation and Connection .....	11
IV. LED Signals .....	13
V. Wi-Fi Settings .....	15
VI. Configuration of Application Protocols .....	20
VII. Settings Reset and Hardware Reset .....	25
VIII. Routing and Data Filters .....	26
IX. NMEA Settings and Data Logging .....	31
X. Web Gauges .....	34
XI. Recording of Diagnostics Data .....	36
XII. Firmware Updates .....	38
APPENDIX A. Troubleshooting .....	39

## Package Contents

Device	1 pc.
Wi-Fi antenna	1 pc.
Screws	2 pcs.
This Manual	1 pc.
Paperclip for reset	1 pc.

## Introduction

The NMEA 0183 Wi-Fi Gateway (hereinafter Gateway or Device) allows you to get and observe data from an NMEA 0183 equipment on a PC or smartphone. With it, you get NMEA 0183 network data including vessel course, speed, position, wind speed and direction, water depth, AIS messages from vessels and aircrafts and other navigation data in popular marine software applications.

The Gateway has two physical NMEA 0183 Ports (two inputs a.k.a. Listeners and two outputs a.k.a. Talkers) with configurable baud rate from 300 to 115200 baud. This makes it possible to organise the exchange of data between two devices with NMEA 0183 ports working on different baud rates.

The Gateway has Wi-Fi interface with three Data Servers, each one can be configured for UDP or TCP network protocols.

Device allows to set up arbitrarily data routing schemes between its NMEA 0183 ports and Data Servers, making it a powerful data router and multiplexer.

Individual Data Filters can be defined for incoming and outgoing NMEA 0183 data at any physical port or network server. This allows reduction of traffic on slow connections. The default NMEA 0183 baud rate is only 4800 baud and that is not enough to transfer AIS data, for example. AIS uses 38400 baud rate.

The Gateway can create its own Wi-Fi network (with range of about 30 meters in open spaces) or it can be connected to an existing Wi-Fi network router or access point. In the second case, coverage depends on the coverage of the base network; To access the Device's web-interface and Data Servers, connect your devices to that router's Wi-Fi network. If your router has Internet access, you can also set up data logging and upload to Yacht Devices Cloud services.

To configure the Gateway, you need any Wi-Fi-capable device (laptop or smartphone) with any web browser. The Device's settings can be reset to factory values using the hidden reset button (a paper clip is required, supplied with the Device).

The Web Gauges pages of the Device's web interface allow real time monitoring of vessel's data using a web browser on PC, laptop, tablet or smartphone. This feature can replace or augment existing instrument displays. No Internet connection or app installation is required.

A pair of Wi-Fi Gateways can act as an NMEA 0183 wireless extender and allows joining of two or more physical networks. To pair the Gateways, you need to set up Data Servers on both with UDP network protocol and set the same network port number.

You can also pair the Device with Yacht Devices NMEA 2000 Ethernet or Wi-Fi gateways/routers in the same way. Configure connection on both using NMEA 0183 data protocol (our NMEA 2000 gateways and routers support bi-directional conversion between NMEA 2000 and NMEA 0183, making a wireless bridge between NMEA 2000 and NMEA 0183 networks.

The Gateway can be set up to automatically record your track data with weather, depth and other data to the internal memory. These data can be exported to GPX (for Garmin MapSource, Google Earth, GPXSee or other cartographic applications) or CSV (spreadsheet) formats.


Thank you for purchasing our product and happy voyages!


## Warranty and Technical Support

1. The Device warranty is valid for two years from the date of purchase. If a Device was purchased in a retail store, the sales receipt may be requested when applying for a warranty claim.
2. The Device warranty is terminated in case of violation of the instructions in this Manual, case integrity breach, or repair or modification of the Device without the manufacturer's written permission.
3. If a warranty request is accepted, the defective Device must be sent to the manufacturer.
4. The warranty liabilities include repair and/or replacement of the goods and do not include the cost of equipment installation and configuration, or shipping of the defective Device to the manufacturer.
5. Responsibility of the manufacturer in case of any damage as a consequence of the Device's operation or installation is limited to the Device cost.
6. The manufacturer is not responsible for any errors and inaccuracies in guides and instructions of other companies.
7. The Device requires no maintenance. The Device's case is non-dismountable.
8. In the event of a failure, please refer to Appendix A before contacting technical support.
9. The manufacturer accepts applications under warranty and provides technical support only via e-mail or through authorized dealers.
10. The contact details of the manufacturer and a list of the authorized dealers are published on the website: <http://www.yachtd.com/>.



<b>Device parameter</b>	<b>Value</b>	<b>Unit</b>
Supply voltage	7..17	V
Average current consumption	47	mA
Wi-Fi module 2.4 GHz	802.11b/g/n	—
Wi-Fi signal range (open space)	30 / 100	m / feet
Wi-Fi connections in Access Point mode (max.)	3	—
TCP connections from applications (max.)	9	—
UDP clients (applications or devices)	Unlimited	—
NMEA 0183 physical ports (inputs / outputs)	2 / 2	—
Device case without antenna (LxWxH)	85x45x28	mm
Total height with the antenna in vertical position	93	mm
Total length with the antenna in horizontal position	192	mm
Weight	80	g
Operating temperature range	-20..55	°C

 Yacht Devices Ltd declares that this product is compliant with the essential requirements of EMC directive 2014/30/EU and radio and TTE directive 1999/5/EC.

 Dispose of this product in compliance with the WEEE Directive or local regulations. Do not dispose of it with household or industrial waste.



## II. NMEA 0183 Basics

The default baud rate of a NMEA 0183 interface is 4800 baud. High-speed interfaces are 38400 baud and were designed especially for AIS, but usually chart plotters and instrument displays allow any data (not only AIS) on a high-speed port. On a chart plotter, port baud rate a.k.a. speed can be configured in the NMEA 0183 interface settings. NMEA 0183 uses different wires for talking (transmitting, TX) and listening (receiving, RX) data.

One Talker can be connected to multiple Listeners, but a Listener can have only one Talker connected. The Gateway can act as a «multiplexer» and join the output of two physical Talkers to a single data stream.

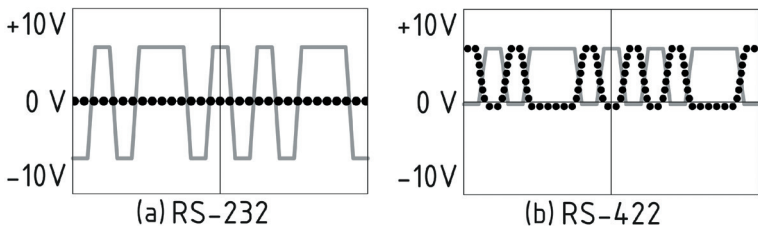


Figure 2. (a) RS-232 and (b) RS-422

NMEA 0183, until version 2.0 (1992), used a «single ended» RS-232 interface with one TX line and one RX signal line (grey at Figure 2.a) and ground line (dotted at Figure 2.a) used as reference for TX and RX signals. Therefore, old devices have only three wires.

Since Version 2.0, NMEA 0183 has been based on a «differential» RS-422 interface, which has two RX lines RX+ (can also be marked as «A») and RX- (or «B»), two TX lines TX+ (or «A», grey at Figure 2.b) and TX-

(or «B», dotted at Figure 2) and a ground (not shown at Figure 2.b). Modern devices use five wires.

Devices of different versions can be connected, but with one cautionary note. TX- («B») is not equal to a ground line. Voltage on the TX- line (dotted on Figure 2.b) changes from 0 to 5V, and connecting this line to ground line can cause a short circuit.

The correct connection schemes are shown in Figure 3.

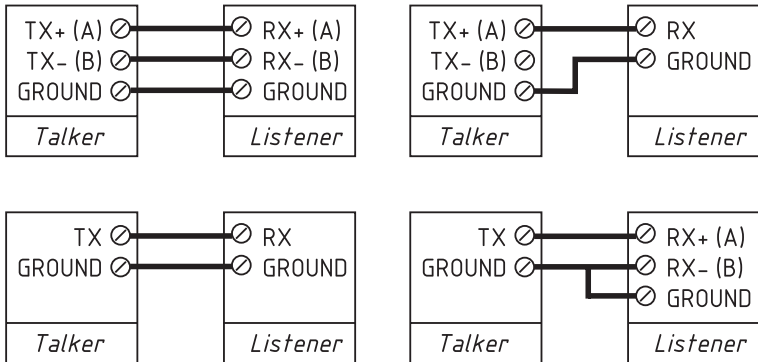


Figure 3. Connection of NMEA 0183 devices

### III. Device Installation and Connection

The Device requires no maintenance. When deciding where to install the Device, choose a dry mounting location. Despite the fact that the Gateway case is waterproof, the terminals are open and fluids can enter the Device and/or cause a short circuit. Do not place the Device where it can be flooded by water, get wet in the rain or be sprayed with any other fluids.

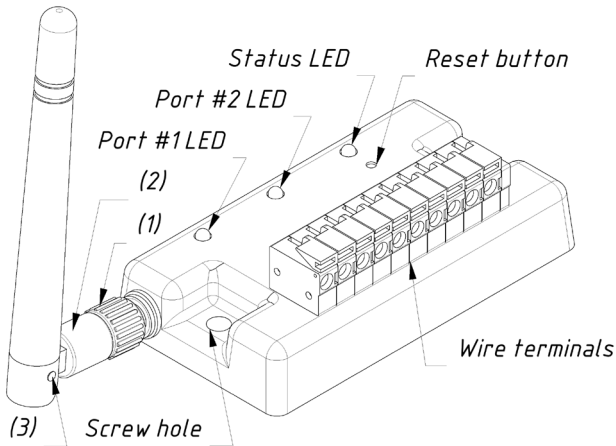


Figure 4. Gateway LEDs and terminals

First, connect the Wi-Fi antenna. Part (2) of the antenna base (see Figure 4) rotates relative to the part (1) with notches. At the point (3), the angle of the antenna can be changed between horizontal and vertical positions. Orient the antenna relative to paired Wi-Fi device(s) to achieve an optimal Wi-Fi signal reception.

The Gateway can be fixed horizontally or vertically using two screw holes (4 mm diameter, 72 mm between centers) and screws supplied. When the holes of wire terminals are pointing down, they are better protected from occasional water spray.

Terminals, from the left to right (Figure 4):

- port #1: RX-, RX+, TX-, TX+;
- port #2: RX-, RX+, TX-, TX+;
- ground (opposite the reset button and Status LED);
- power supply, 7..17 V.



*Connection to the NMEA 0183 equipment varies depending on the equipment's NMEA 0183 ports hardware version. Please, refer to Section II for connection schemas.  
Warning! Incorrect wiring may damage the Device and/or connected equipment ports!*

The Gateway is supplied with NMEA 0183 Ports configured for 4800 baud. If your NMEA 0183 equipment has a different baud rate, configure the corresponding Gateway Port baud rate before connecting to NMEA 0183 equipment (see Section IX.1). If your NMEA 0183 equipment supports configurable baud rates, it is recommended initially to set the highest available baud rate on both the Gateway's Port and target equipment port.

All connections should be made when the power is off. This will protect against accidental short circuits during installation. When the power and ground wires are connected, turn on the power supply and the Device's LEDs will blink (see Section IV).

## IV. LED Signals

The Device is equipped with three bi-color LEDs (refer Figure 4): Status LED, Port #2 LED and Port #1 LED. Upon power-up, the Status LED emit a single long green flash, indicating that the Device firmware was booted successfully. Then LEDs start flashing in normal operation mode.

### *1. Signals during normal operation*

During normal operation, Device produces a series of four flashes of each LED (starting from Status) every five seconds. These flashes indicate the state of Device interfaces over the last five seconds and have the following meaning:

- **Status LED, flash #1: Wi-Fi configuration.** Green, if the Gateway is configured to use its own Wi-Fi network named «YDWN» (SSID), Access Point mode. Red, if the Gateway is configured to use the boat's existing Wi-Fi network, Client mode.
- **Status LED, flash #2: Wi-Fi state.** Red, if the Wi-Fi link is not established yet or some error has happened (cannot connect to existing Wi-Fi network, wrong password, etc.). Otherwise green.
- **Status LED, flash #3: TCP connections.** Green, if some clients are connected to Gateway services by TCP protocol. When the Device's web-interface is browsed, the connection opens only for a short period when web-pages are downloaded from the web server. Red, if no TCP connections are open (but applications can receive data by UDP protocol at the same time).
- **Status LED, flash #4: data received from network.** Green, if data was received by any of the Data Servers (via TCP or UDP network protocol). Otherwise red.
- **Port LED, flash #1: data received.** Green, if any data was received by this Port in the last 5 seconds.
- **Port LED, flash #2: RX errors.** Green, if any data was received and all data was received without errors. NMEA 0183 sentences contain a checksum, so any transmission error will be detected.
- **Port LED, flash #3: data sent.** Green, if data was sent to this Port. As RS-422 does not support confirmation of reception, this signal does not mean that data was received by any Listener. Red means that the Gateway has nothing to send.

- **Port LED, flash #4: TX overflow.** Green, if data was sent without overflow. In case of a red signal, you should increase the Port baud rate (if possible) or filter our unnecessary data, because the selected baud rate is not enough to send all the data. This signal will also be red if flash #3 is red.

With the factory settings, the Status LED should flash GREEN-GREEN-RED-RED after the power on; this means that the Gateway is configured for Access Point mode, successfully created the Wi-Fi network with «YDWN» name (SSID) and has no incoming TCP connections from connected software yet.

### *2. Signals during Device reset*

Hardware reset or settings reset is initiated by pressing the hidden reset button. See Section VI for LED signals.

### *3. Signals during firmware update*

Firmware update file can be uploaded via Device's web interface. See Section XII.

## V. Wi-Fi Settings

The Device Wi-Fi module can operate in either Access Point mode — creates its own Wi-Fi network (factory default) or in Client mode — connected to an existing Wi-Fi network. To configure the Gateway, you will need a Wi-Fi-capable device such as a laptop or smartphone with a web browser.



*The Gateway's internal web server has limited capabilities, and it is not advisable to have multiple devices accessing it simultaneously. Updating settings of Data Servers will cause termination of all active TCP data connections.*

### 1. Access Point mode

In Access Point mode the Device creates a 2.4 GHz Wi-Fi network with name (SSID) «YDWN» and passphrase 12345678. To access the Device web interface, connect to this Wi-Fi network and enter <http://192.168.4.1> in a web browser. Use login 'admin' and password 'admin' (without quotes) to log in to the Device web interface.

The Device's web interface includes a navigation menu on the left. In the mobile version, this menu is accessible via the «hamburger» icon in the top left corner.

On the «Wi-Fi Access Point» page, you can change the Wi-Fi network name (SSID) and passphrase, set the Wi-Fi authentication algorithm, select the desired Wi-Fi channel and make the network hidden.

Note that hidden networks will not appear in the list of available Wi-Fi networks on client devices. However, you can still connect to them by manually entering their name (SSID) and passphrase in the Wi-Fi connection settings on the client devices.

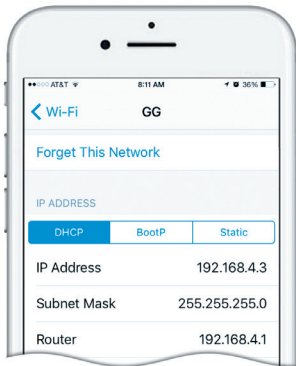
The Device's default Wi-Fi channel is 1. If you experience an unstable Wi-Fi connection in an area with many deployed Wi-Fi networks, such as a marina, try changing the Wi-Fi channel. Connection issue may be caused by congestion or signal interference on the channel. Check nearby Wi-Fi network channels using a Wi-Fi scanner application that shows nearby Wi-Fi channel usage and signal strength and select the most free channel.



*Note that the Device allows you to select from all available 2.4 GHz channels, from 1 to 13. As of 2024 in North America you are allowed to use only channels 1–11. EU, Australia and Japan has no such limitation. Check local laws and regulations with regard to restrictions on the use of Wi-Fi channels.*

The Device's Access Point allows a maximum of 3 Wi-Fi client devices to be connected simultaneously. To bypass this limitation, connect both the Gateway and all Wi-Fi client devices to a generic Wi-Fi router in Client mode.

## *2. Client mode*



*Figure 5. How to get your Wi-Fi network IP settings using mobile device*



In Wi-Fi Client mode, the Device connects to an existing Wi-Fi network. To switch the Device to this mode from the default Access Point mode, use the «Wi-Fi Client» page in the Device's web interface.

To connect to your Wi-Fi network, you can either scan for available networks or manually enter your network name (SSID) and passphrase. Once the scan is complete, select your Wi-Fi network from the list using the radio button and enter its passphrase.

By default, Device will use DHCP to get IPv4 address automatically from the Wi-Fi router. In that case, router will assign IP address randomly from the allowed DHCP address range.

To access the Device you will need to get its new IPv4 address. This can be done by accessing router's Wi-Fi clients list and checking for the Device MAC address — the one which is displayed on the «Wi-Fi Client» page, «Wi-Fi State» section. If your router lacks this feature you can perform Wi-Fi network IPv4 range scan for open ports 80 (default Device web interface port) and 1456 (default Device Server #1 port) using e.g. Zenmap NMAP GUI or similar software.

Many routers support «Static DHCP» aka «DHCP Tethering» feature, which forces router to always give the Device the same fixed IPv4 address over DHCP, Device will be identified by router via its MAC address. Note that the Gateway has two different MAC addresses, one for the Access Point mode and another for Client mode. You should use the MAC address given on «Wi-Fi Client» page, «Wi-Fi State» section for DHCP Tethering.

Of course, you can always avoid messing up with DHCP setup by simply giving the Device a static IP address. For that, select the «Set Static IP» radio button on the «Wi-Fi Client» page, section «IP Address Setup». Then, enter a new IP address for the Device that is not already in use by other nodes on your Wi-Fi network, along with a subnet mask that matches your router's Wi-Fi network IPv4 CIDR subnet range. Also enter the network gateway IPv4 address, which is typically the same as the Router's address.

If you do not remember your router's Wi-Fi network IP settings, you can quickly check them by connecting a mobile device or laptop to the router's Wi-Fi in DHCP mode and then checking the obtained IP settings. Refer to Figure 5 on the previous page and note that the network gateway address is 192.168.4.1, and subnet mask is 255.255.255.0 (CIDR /24 subnet). The smartphone has been assigned the IP address 192.168.4.3. To avoid conflicts, it is recommended to assign the Device IP address from the same subnet but with a different address, such as 192.168.4.100.

Contact your router administrator or refer to your router documentation to get more specific instructions on the Wi-Fi setup.

The «Save» button will save the settings in the EEPROM and the settings will be applied the next time you connect to the Wi-Fi network. The «Save & Apply» button saves settings and immediately attempts to apply them if the Gateway is already in Client mode.

When all necessary settings are entered, click «Connect» button to switch Device to Wi-Fi Client mode and connect to chosen Wi-Fi network. Check the Device's LED indication to make sure the correct Wi-Fi mode is selected and the connection status is OK (refer Section IV).



*If the Gateway was in Access Point mode before, it will shutdown the «YDWN» network after successful connection to a router's Wi-Fi network. Your client device (smartphone, laptop) may still attempt to connect to non-existing «YDWN» network, in that case re-connect to the correct Wi-Fi network manually.*

In our static IP configuration example above we have connected the Device to Wi-Fi network «GG» with manually set IP address 192.168.4.100. To access the Device web interface, connect smartphone or laptop to Wi-Fi network «GG» and enter <http://192.168.1.100> in the web browser address bar.

### 3. *If Device web interface is not accessible*

There are many possible reasons why you may not be able to connect to the Gateway, especially after changing the settings. Please check the following:

- if Device LED flash #1 shows desired Wi-Fi operation mode (Access Point vs Client, refer IV)?
- if Device LED flash #2 shows bad Wi-Fi connection status (refer IV)?
- are you using DHCP or Static IP? If DHCP, have you set up «DHCP Tethering» aka «Static DHCP» on the router correctly?
- have you set correct IP address, mask and gateway (matching your Wi-Fi router settings) before switching to Client mode?
- do your router's security settings block IP connections between Wi-Fi clients, e.g. is «Wi-Fi isolation» enabled?

If you cannot diagnose what is wrong, you can reset the Device's settings (see Section VII) and the Device will be returned to Access Point mode. You can connect to the «YDWN» network again and try to change the settings one more time.

#### 4. Other important settings



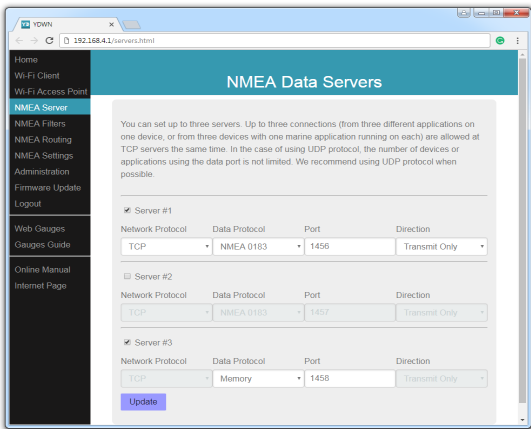
*If you will use the Device in Access Point mode, change the default Access Point Wi-Fi passphrase! Do not forget to write it down in boat's Technical Documentation so you can easily access it later!*



*Change the default web interface access password on the «Administration» page! Do not forget to write it down in boat's Technical Documentation so you can easily access it later!*

In some network configurations, access to network port 80, which is the default HTTP port of the Device web interface, may be limited. Alternatively, you may need to use a different port, say, if you use port forwarding on the router. You can change the Device web interface HTTP port on the Device's «Home» page. For instance, if you set the port to 8080 (alternative HTTP port), you will need to explicitly add that port address to the Device's web interface URL, e.g.: <http://192.168.4.1:8080>

## VI. Configuration of Application Protocols



*Figure 6. Device Data Server page with example settings*

The Device has three Data Servers, each of which can be individually configured. You can enable or disable Servers, select the Network Protocol and Port, and choose the Data Direction for each Server. Note that Server #1 is used by Web Gauges, so if you plan to use Web Gauges, keep Server #1 enabled. Server #3 can also serve special functions such as Data Logging (Memory, see IX.3) and Debug (see XI). Each data Server also has its own Data Filters (see VIII).

Most marine applications support both TCP and UDP network protocols. TCP is a connection-oriented, stateful data exchange protocol. The receiving network node must confirm reception of each data packet before it can get a next data packet, and if reception confirmation is not received, the sender node repeats the transmission after a timeout. Thus TCP roughly doubles the amount of network traffic exchange between two network nodes (and hence, their CPU load), despite the fact that both nodes receive the same data.

Keep in mind that Device has a hardware limitation on maximal number of concurrent TCP connections, not more than 9 TCP connections per Device, not more than 3 TCP connections per each Data Server.

UDP is a connectionless and stateless protocol. If you select the UDP protocol, the corresponding Device Data Server will send local broadcast UDP packets. This means that the number of devices or applications using this data port is not limited. It is recommended to use the UDP protocol whenever possible.

As Device has only NMEA 0183 Ports, the only available Data Protocol you can set on Servers is NMEA 0183 (except special protocols on Server #3). NMEA 0183 Data Protocol is supported by almost all marine applications.

Each Server's data Direction can be configured as «Transmit Only» whenever possible to protect connected NMEA 0183 devices from invalid data which can be sent via Servers. However, if your software needs to send data to NMEA 0183 devices, for example, for Autopilot TRACK/GOTO navigation under control of ECS application, enable either «Receive Only» or «Bidirectional».

In factory settings, Device has Server #1 enabled with TCP Network Protocol on port 1456, with NMEA 0183 Data Protocol and «Transmit Only» Data Direction.

*Example 1: connection to OpenCPN for Autopilot control in TRACK mode (see Figure 7)*

In this example we will show how to connect OpenCPN to the Device in Access Point mode. We will use TCP connection to Server #1 using default port 1456. As OpenCPN will need to send TRACK data (APB, RMB and XTE sentences) to Autopilot we will reconfigure Server #1 to bidirectional mode.

- connect your laptop/PC (with OpenCPN installed) to Device Wi-Fi network;
- check if laptop/PC can access Device's web interface or you can ping the Device by its default IP 192.168.4.1;
- enable bidirectional communications on Server #1 — set Direction = «Bidirectional»;
- create new connection in OpenCPN of type «Network», select TCP protocol, enter Device IP address (192.168.4.1) and Server #1 port (1456);
- enable OpenCPN to receive input on this port (to get data from the Device);
- enable OpenCPN to output on this port (to send TRACK data to the Device);
- click Apply button in OpenCPN connection manager, make sure new connection is present in «Data Connections» list and is enabled;
- tick OpenCPN «Show NMEA Debug Window», make sure you got incoming data stream (marked green) from this new connection;
- to test if OpenCPN can send NMEA 0183 data to Device, start GOTO or TRACK navigation, confirm you got outgoing NMEA 0183 sentences APB, RMB and XTE in the OpenCPN «NMEA Debug Window» marked blue, not red;
- to test if Autopilot receives TRACK data, engage track mode via Pilot Controller and confirm if Autopilot responds correctly.

### *Example 2: connection to Navionics Boating App*

In this example we will show how to connect Navionics to the Device when Device is in Wi-Fi Client mode. Suppose, both Device and tablet/smartphone are connected to the same Wi-Fi network and Device has IP 192.168.1.100. We will use UDP connection to Server #2 using Navionics default UDP port 2000. As Navionics (in year 2023) can not send data, we will configure Server #2 in «Transmit Only» mode.

- connect your tablet/smartphone (with Navionics installed) to Device Wi-Fi network;
- check if tablet/smartphone can access Device's web interface by its IP – 192.168.1.100 in our example;
- enable Server #2;
- set Network Protocol = UDP, Data Protocol = NMEA 0183, port 2000 and Direction = «Transmit Only»;
- in Navionics tap Menu, select Paired Devices, follow the on-screen instructions. Make sure you got incoming NMEA 0183 data stream form the Device.

As of year 2023, Navionics can receive only a limited subset of NMEA 0183 data, so it is recommended to set up Data Filters on Server #2, see example in Section VIII.

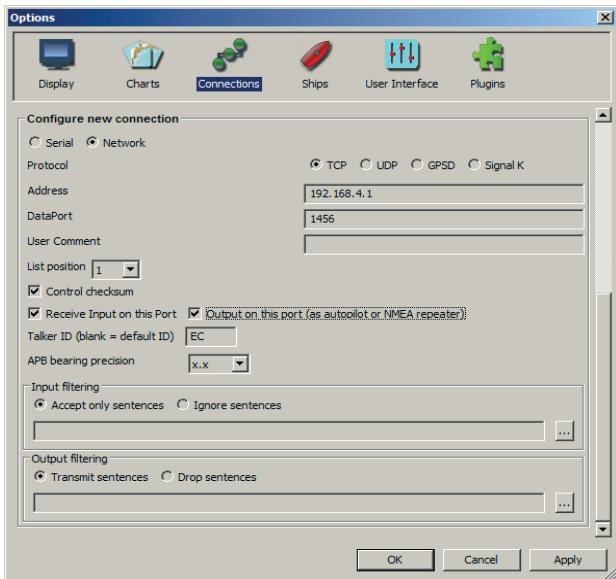


Figure 7. OpenCPN connection example



## VII. Settings Reset and Hardware Reset

Settings reset can be used if Device is configured incorrectly (e.g. if Wi-Fi Client settings were set incorrectly and Device does not connect to router's Wi-Fi network) so you can reconfigure the Device from scratch.

Hardware reset is normally not required, but it can be used for firmware rollback (e.g. if you are testing beta versions of the firmware and encounter a bug).

To reset the Device settings:

- press and hold the hidden button marked «RST» on the Device label using a paper clip, Device «NET» LED will constantly shine red;
- keep pressing the button until the «NET» LED becomes green, then immediately release the button;
- Device should emit several green flashes on «NET» LED, then reboot and resume normal operation.

After settings reset Device will switch back to Wi-Fi Access Point mode with default SSID = «YDWN» and Wi-Fi passphrase 12345678.

All Routing, Ports and and Data Filters settings will be also reset to factory defaults.

To reset the Device hardware:

- press and hold the hidden button marked «RST» on the Device label using a paper clip, Device «NET» LED will constantly shine red;
- keep pressing the button until the «NET» LED becomes green, keep the button pressed;
- after 2 seconds, «NET» LED becomes red again, keep the button pressed;
- after 5 seconds, «NET» LED becomes green again, immediately release the button;
- within 40 seconds, Device should emit several green and red flashes on «NET» LED (see XII), then reboot and resume normal operation.

During the hardware reset, the Device rolls back the firmware to a default version programmed at the factory (the Device has a copy of the default firmware in EEPROM) and resets all settings to the factory defaults.

Note that neither settings reset not hardware reset will be performed if you release the button when the «NET» LED colour is red.

## VIII. Routing and Data Filters

Data Routing is used to organize the data flows between physical Ports and Data Servers. Factory default settings are shown on Figure 8, observe the Device is set up to send all data from physical Ports to Data Servers and vice versa.

Home

Wi-Fi Client

Wi-Fi Access Point

NMEA Server

NMEA Filters

**NMEA Routing**

NMEA Settings

Administration

Firmware Update

Logout

Web Gauges

Gauges Guide

Online Manual

Internet Page

### NMEA Routing

You can select output ports and servers for each input source. Note that each server has individual filters, and a routed sentence can be filtered out by output filters of the selected server.

Tunnelling allows routing of incorrect sentences from the server or port, including sentences with an invalid checksum. Invalid sentences are not processed by incoming filters of input server/port or outgoing filters of output port/server. Correct sentences are always processed by filters, whether is tunnelling is off or on.

Input	Tunnel	Output				
		NMEA Port		TCP/UDP Server		
Port/Server		1	2	1	2	3
Port #1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Port #2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Server #1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Server #2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Server #3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Update](#)

Figure 8. Default «Data Routing» settings

## Data Routing

Routing matrix allows you to select which data received on Gateway's Ports and Data Servers «Input» will be forwarded to which Device Ports and Data Servers «Output».

You can set complex routing rules, for example, if two different NMEA 0183 devices are connected to the same NMEA 0183 port, say port #1 (one device is Talker, another is Listener) you can enable to forward data received from Listener on port #1 to Talker on the same port #1 – enable route from port #1 «Input» to the port #1 «Output».

Note that Device's Web Gauges (see X) use data routed to Server #1 «Output». Observe that in default routing settings shown on Figure 8, Server #1 receives data only from physical NMEA 0183 Ports #1 and #2. Suppose your application also sends data to Server #1 and you need to observe those data on Web Gauges as well – enable route from Server #1 «Input» to the Server #1 «Output».

## Tunnel settings

According to the Standard, an NMEA 0183 sentence starts with a «\$» or «!» symbol, followed by a 2-character «Talker ID» and a 3-character «Sentence Formatter» followed by several data fields separated by commas. The sentence ends with a checksum separated from data fields section by «\*» (asterisk) symbol.

Device will check each received NMEA 0183 sentence before routing, sentences with incorrect format or invalid checksum will be dropped.

Some NMEA 0183 devices (e.g. NMEA 0183 Standard version 1 compliant) may send sentences with incorrect checksum. You may also need to forward non-NMEA 0183 data «as is», like data from Navtex equipment. In that case, enable «Tunnel» setting on the corresponding «Input» – to receive and forward such data «as is», with no checks.

Device can also fix invalid NMEA 0183 sentences, see IX.

## Data Filters

Device's web interface «NMEA Filters» page can be used to set up Data Filters — e.g. to filter out unwanted sentences or pass only those sentences that application needs. Each Device interface (Server or physical Port) has its own filter set. Choose target Server or Port, then select «Source» identification algorithm (by Sentence or Talker ID) and Filter «direction» («Transmit or Receive»). Then you set «Filter Type» which can be either BLACK to block, or WHITE to pass) and edit the «Filter Settings» strings — matching the desired Source identification algorithm.

Each filter list has a switchable type: WHITE or BLACK. A message is passed through the WHITE filter if it contains a record matching a message. And the reverse for BLACK. In the factory settings, all filter lists are empty and are of BLACK type, so all messages are passed through the filters.

### *Example 1*

Suppose you have AIS transceiver Talker connected to Device port #1 and NMEA 0183 autopilot Listener connected to port #2. AIS sends a lot of data and thus both AIS and port #1 baud rate is set to 38400, but Autopilot uses standard baud rate 4800.

Your AIS unit also sends both AIS data (VDM and VDO sentences), GPS data (GLL sentence with GP «Talker ID») and GLONASS data (GLL sentence with GN «Talker ID»), for example:

```
$GPGLL,4146.5894,N,07029.6952,W,173412.02,A*15
```

```
$GNGLL,4146.5894,N,07029.6952,W,173412.02,A*0B
```

```
!AIVDM,1,1,,B,ENk`smq71h@@@@@@@@@@@@@@@@=MeR6< 7rpP00003v f400,4*5F
```

As autopilot does not need AIS data, we need to block all outgoing AIS sentences on port #2, this can be done with the filter settings shown on Figure 9:

Choose Filter:		
Server	Source	Filter
Port #2	Sentence	Transmit

Define Filter Settings:	
Filter Type	Filter Settings
Black	VDM VDO

*Figure 9. AIS data filter example*

### *Example 2*

Suppose you have the same setup as above, with an extra NMEA 0183 data source Talker connected to Device's Listener on port #1 and Navionics application connected to Device's Server #2.

Navionics (in year 2023) can only understand AIS, GPS and depth data sentences – VDM, VDO, RMC, DBT and DPT and sometimes can hang if fed with invalid NMEA 0183 sentences. So we will create WHITE filter for Server #2, shown on Figure 10:

Choose Filter:

Server	Source	Filter
Server #2	Sentence	Transmit

Define Filter Settings:

Filter Type	Filter Settings
White	VDM VDO RMC DBT DPT

Update

*Figure 10. Navionics data filter example (by «sentence formatters» list)*

### Example 3

Suppose in addition to Example 2 we also need to block GLONASS data, we can add a second filter to Server #2 blocking all data with GN «Talker ID», shown on Figure 11:

Choose Filter:

Server	Source	Filter
Server #2	Talker ID	Transmit

Define Filter Settings:

Filter Type	Filter Settings
Black	GN

Update

*Figure 11. GLONASS data filter example (by «Talker ID»)*

## IX. NMEA Settings and Data Logging

This Section describes settings available on the Device's web interface «NMEA Settings» page.

### 1. Port Speed

NMEA 0183 standard baud rate is 4800 bits/second. AIS uses 38400 (NMEA High Speed) and Navtex uses non-standard baud rate of 9600. You can change each Device's NEMA 0183 port baud rate by selecting from the list of standard serial port baud rates. For example, you can connect Device to PC's serial port using the highest available rate of 115200.

Some NMEA 0183 equipment allows to change Talker/Listener baud rate. Make sure that all connected NMEA 0183 equipment Talkers/Listeners have baud rates set matching Device's port baud rate.

Note that each individual Device's NMEA 0183 port output (Talker) and input (Listener) can work only on the same baud rate.

### 2. NMEA 0183 Output

You can set any desired valid 2-character «Talker ID» for sentences generated by Device itself. The only sentence that Device can generate is MWV sentence with calculated Theoretical Wind data.

The wind sensor always measures Apparent Wind (AWA). Theoretical (sometimes erroneously called «True») Wind data (speed and angle) can be calculated using various vessel speeds (SOG or STW) and angles (COG or Heading). You can select «Any» for automatic calculations based on available data, choose from one of the calculation algorithms explicitly or disable calculations.

Generated MWV sentence with calculated Theoretical Wind wind be sent to the Device's output Port/Server immediately after the MWV sentence with Apparent Wind — but only if no Theoretical Wind data from another source(s) was received on any Port or Server in last 5 seconds.

### 3. NMEA 0183 Output

«Replace the substring» setting allows you to perform a basic string substitution on incoming NMEA 0183 sentence. This feature can be used to correct incorrectly formed sentences or rename «sensor names» in

XDR sentences, etc. All occurrences of the first string will be replaced with the second string. String length is limited to 16 characters. Modified messages will have a checksum corrected or added to them. You can select on which Ports/Servers this feature should work or disable it. Substitutions will be applied before the sentence is processed further by Device's Data Filters and Routing Matrix.

«Fix or add the checksum» setting allows to add missing checksum or correct invalid checksum of incoming NMEA 0183 sentences. You can select on which Ports/Servers this feature should work or disable it.

#### *4. Data Logging*

The Device can log the most important boat data to its internal non-volatile memory: position, course and speed, wind speed and direction, heading, STW and depth. Valid GPS position and time data are essential for the logging function to work properly. If you want to log the data even when the boat is stationary, uncheck the «Do not record points closer than 5 metres» check box. You can set the logging interval, disable logging or clear all logged data.

The shortest interval is 30 seconds and the Device's non-volatile storage can hold 32000 data points, which is equivalent to approximately 11 days of sailing. Old data is automatically overwritten.

To access the logged data, open the Device's «Data Export» page (see below) and download a GPX file (for cartographic applications such as Google Earth, Garmin MapSource, GPXSee, GPSBabel) or a CSV file (for processing the data with spreadsheet applications).



## Data Export

You can export the data to a GPX (for Google Earth, Garmin MapSource and other cartographic applications) or CSV (spreadsheet) file. Export may not work properly on the iPad and iPhone.

If the number of waypoints below is zero, it possible means that logging is turned off at the NMEA Settings page.

Number of waypoints: 1934

First waypoint date: 3/18/2018, 10:38:16 AM

Last waypoint date: 4/11/2018, 1:04:56 PM

Output file format:

CSV Format     GPX Format   

New track when:  Save only this:

Total tracks: 15    For export: 3 tracks, 1912 waypoints

Preferred units:

Speed	Depth
<input style="width: 100px;" type="text" value="Knots"/>	<input style="width: 100px;" type="text" value="Feet"/>

*Figure 12. Data export page*

The Device's «Data Export» page is a special page that can only be accessed via Server #3.

Configure Server #3 and set the «Data Protocol» to «Memory», then open the page via a browser using URL <http://192.168.4.1:1458/> where 192.168.4.1 is your current Device IP address and 1458 is the Server #3 port.

First, «Loading Data» message will appear, wait until a browser loads all logged data and shows «Data Export» page (Figure 12).

Choose the desired file format, set the file format options (XML schema for GPX file, column separator for CSV file, preferred units and so on) and download the file containing the data.

Note that data export may not work properly on some mobile device browsers.

For example, iPhone/iPad may open the file in the browser window instead of allowing the user to save the file or open it in applications.

You can copy and paste this data from a browser into a text file, but for maximum convenience we recommend using a PC/laptop instead.

## X. Web Gauges

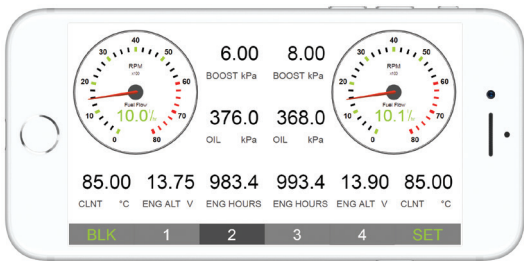


Figure 13. Web Gauges on a mobile device

Device web interface also has a dedicated Web Gauges (WG) page that allows real-time viewing of vessel data using a web browser on a PC, laptop, tablet or smartphone and can replace or enrich the functionality of instrument displays. Web Gauges is a HTML application, so no Internet connection or app installation is required to use it. However, you need a full-fledged modern browser which supports HTML5 canvas, JavaScript, WebSockets and Local Storage technologies (some primitive browsers, such as default Samsung smartphone or Kindle browsers, will not work properly).

No authentication is required to access Web Gauges, you can open it:

- via «Web Gauges» URL given on the Device's «Login» page;
- if you are already logged into the Device's web interface you can use «Web Gauges» menu entry;
- access directly via URL <http://192.168.4.1/g.html> where 192.168.4.1 is your current Device's IP address.

Web Gauges has 5 fully customizable data pages. On mobile devices, you can scroll the pages or use the numeric keys at the bottom to select the active page. On an iPhone, iPad and Android devices, the browser's address bar and/or menu bar can overlap with the WG menu and reduce the visible area, both in horizontal or vertical screen orientation. In that case add WG URL to the browser Home Screen (see browser menu) and open it using the corresponding icon via the browser Home Screen, WG should open in «full screen» mode without browser menus or address bars.

First 3 WG pages are populated with default layout and gauges set, page 4 is blank and page 5 is for autopilot control. You can edit each WG data page, to edit current page click SET button, in OVERALL SETTINGS section set «Edit Gadgets» to «On» and click «Apply». An extra popup «Edit Mode Enabled» should appear on the top of the page. Click any gauge and «Gauge Edit» page opens, where you can choose new gauge type and/or change the gauge settings, you can also add or remove gauges here.

To finish editing, click «Edit Mode Enabled» popup.

OVERALL SETTINGS section also allows to set up measurement units for some data types, set WG timezone, enable Autopilot control from WG and view live NMEA 0183 data sent from Device Server #1.

For more information on WG, refer built-in help available:

- via «Gauges Guide» URL given on the Device's «Login» page;
- if you are already logged into the Device's web interface you can use «Gauges Guide» menu entry and online article at: [http://www.yachtd.com/products/web\\_gauges.html](http://www.yachtd.com/products/web_gauges.html).

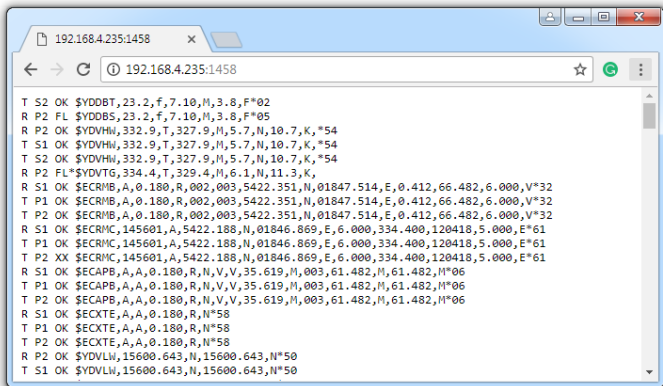
Please, note, that:

- WG uses data only from Server #1, so Server #1 should be enabled;
- WG uses NMEA 0183 data protocol, so Server #1 should set up with «Data Protocol» = NMEA 0183;
- Autopilot mode switching control requires bidirectional communications with Server #1, set «Direction» = Both.

## XI. Recording of Diagnostics Data

Diagnostic procedures are used for troubleshooting connected hardware and software applications. The Device can log all data sent and received by Servers and physical Ports.

Configure Server #3 and set the data protocol to Debug (TCP network protocol will be used automatically) and connect a browser or terminal application to the Server #3 port. For example, if the Device has an IP address of 192.168.4.1 and the Server #3 port has been set to 1458 (default), enter <http://192.168.4.1:1458> in the browser address bar (or connect a terminal application such as PUTTY to this IP and port in «raw TCP» mode). On success, you should observe a simple text web page with growing data log.



```
T S2 OK $YDDBT,23.2,f,7.10,M,3.8,F*02
R P2 FL $YDDBS,23.2,f,7.10,M,3.8,F*05
R P2 OK $YDVHJ,332.9,T,327.9,M,5.7,N,10.7,K,*54
T S1 OK $YDVHJ,332.9,T,327.9,M,5.7,N,10.7,K,*54
T S2 OK $YDVHJ,332.9,T,327.9,M,5.7,N,10.7,K,*54
R P2 FL*$YDVTG,334.4,T,329.4,M,6.1,N,11.3,K,
R S1 OK $ECRMB,A,0.180,R,002,003,5422.351,N,01847.514,E,0.412,66.482,6.000,V*32
T P1 OK $ECRMB,A,0.180,R,002,003,5422.351,N,01847.514,E,0.412,66.482,6.000,V*32
T P2 OK $ECRMB,A,0.180,R,002,003,5422.351,N,01847.514,E,0.412,66.482,6.000,V*32
R S1 OK $ECRMC,145601,A,5422.188,N,01846.869,E,6.000,334.400,120418,5.000,E*61
T P1 OK $ECRMC,145601,A,5422.188,N,01846.869,E,6.000,334.400,120418,5.000,E*61
T P2 XX $ECRMC,145601,A,5422.188,N,01846.869,E,6.000,334.400,120418,5.000,E*61
R S1 OK $ECAPB,A,A,0.180,R,N,V,V,35.619,M,003,61.482,M,61.482,M*06
T P1 OK $ECAPB,A,A,0.180,R,N,V,V,35.619,M,003,61.482,M,61.482,M*06
T P2 OK $ECAPB,A,A,0.180,R,N,V,V,35.619,M,003,61.482,M,61.482,M*06
R S1 OK $EXCTE,A,A,0.180,R,N*58
T P1 OK $EXCTE,A,A,0.180,R,N*58
T P2 OK $EXCTE,A,A,0.180,R,N*58
R P2 OK $YDVLH,15600.643,N,15600.643,N*50
T S1 OK $YDVLH,15600.643,N,15600.643,N*50
```

Figure 13. Web page showing the diagnostic log

When enough data has been logged, stop logging by pressing the 'Stop' button on the browser. Some mobile browsers do not allow you to save files and we recommend that you use a laptop or PC to record diagnostic data. Some web browsers may try to reload the web page while saving, in this case, you can use the clipboard (operating system Copy All and Paste commands) and a text editor to paste and save the log data to a file.

The first character in the log line (see Figure 13) indicates whether the record was received «R» or sent «T». The next group of characters indicates the port «P» or Server «S» with its number, e.g. «P2» means physical port #2 and «S1» means server #1. «XX» indicates a data output overflow on this port (these NMEA sentences have been dropped), «FL» indicates that the sentence was filtered out by one of the Data Filters. An asterisk «\*» after «FL» indicates that the sentence is invalid.

## XII. Firmware Updates

The current firmware version of the Device can be checked either via the NMEA 2000 display device (chartplotter/MFD) «NMEA 2000 Device List» feature or via the Device's web interface on the Login or Home pages. Always ensure that you are running the latest firmware version.

You can download the latest firmware version from our website at: <https://www.yachtd.com/downloads/>.

First, open the downloaded .ZIP archive containing a firmware update and extract the MUPDATE.BIN file to a location on your hard disk where you can easily find it. Also check the README.TXT file included in the archive, it may contain important information regarding the update procedure.

To upload an update file to the Device:

- log into the Device web interface;
- open the «Firmware Update» page via main menu;
- click «Choose File» button, locate and select the MUPDATE.BIN file;
- click «Update the firmware» button.

Uploading the firmware file takes 20–40 seconds. When the file is uploaded, you'll get a message that the update has started. You will also see chaotic flashing of the Status LED for another 40–60 seconds. The unit will reboot when the update process is complete.

The firmware update will not cause any damage to the Device. For instance, if the update process is interrupted, such as by a power failure, after the file has been uploaded, the update will resume automatically upon the next power on. Generally, all Device settings will remain unchanged, unless otherwise specified in the README.TXT file accompanying the update.

If it turns out that the new firmware has bugs or causes issues, or if you need to test firmware beta versions with the same build number you can always roll back to a factory default firmware using Hardware Reset procedure (see Section VII).

## APPENDIX A. Troubleshooting

Issue	Possible causes and solutions
All Device's LEDs are OFF.	<p><b>1. No power.</b> Check the voltage supplied to Device's «12V» and «GND» terminals, «12V» input should have +7..+17 Volt potential in respect to «GND».</p> <p><b>2. Incorrect power source polarity.</b> Make sure voltage is applied with correct polarity.</p>
Device's Wi-Fi network is not visible on a client device (laptop, tablet, smartphone).	<p><b>1. Device Wi-Fi module is operating in wrong mode.</b> Make sure the Device is in Access Point mode — check if the first «NET» LED flash is green (see IV).</p> <p><b>2. Device Wi-Fi module failure.</b> Check if the Device reports it has created Wi-Fi network successfully — check if the second «NET» LED flash is green. If you got first two LED flashes green-red, reset the Device settings (see VII). If you still got first two LED flashes green-red after reset, contact Technical Support.</p> <p><b>3. 2.4 GHz Wi-Fi transceiver is not enabled on Wi-Fi client device.</b> Check if you have 2.4 GHz Wi-Fi mode enabled on target client device.</p> <p><b>4. Device's WiFi network was made hidden via Wi-Fi Access Point settings.</b> Manually connect to Device's hidden Wi-Fi network by entering the WiFi SSID explicitly.</p>

Issue	Possible causes and solutions
<p>Device's WiFi network is visible on client device (laptop, tablet, smartphone) but I can not connect to it's Wi-Fi network.</p>	<p><b>1. Bad Wi-Fi network authorization credentials.</b> Make sure you enter Wi-Fi connection details on client device (SSID, passphrase) correctly.</p> <p><b>2. Too many Wi-Fi clients connected.</b> Make sure no more than 3 Wi-Fi client devices are connected to Device's Wi-Fi network. Reboot the Device (e.g. power-cycle) to drop all Wi-Fi connections.</p> <p><b>3. Device Wi-Fi module failure.</b> Check if the Device created Wi-Fi network successfully — first two «NET» LED flashes are green-green. If you got first two LED flashes green-red, reset the Device settings (see VII). If you still got first two LED flashes green-red after reset, contact Technical Support.</p>
<p>I can connect a client device (laptop, tablet, smartphone) to the Device's Wi-Fi network, but got periodic disconnects (Wi-Fi connection unstable). Device «NET» LED indication shows first two LED flashes green-green.</p>	<p><b>1. Bad Device placement or antenna orientation affects Wi-Fi signal reception on client devices.</b> Make sure device is not installed near EMI sources (high-power cables, VHF antennae and feeders, engines, gensets, DC motors, fluorescent lamps, etc.). Make sure there is no large conductive obstacle between the Device and Wi-Fi clients (glass, metal, carbon fiber or wet wood objects). Reposition the Device, re-orient its antenna and find an optimal Wi-Fi reception spot.</p> <p><b>2. Wi-Fi interference due to channel clogging.</b> Usually observed in places with a lot of Wi-Fi networks deployed, like in a marina. Check the Wi-Fi channel usage using any Wi-Fi monitoring software that can show nearby networks signal strength and channel usage, then force the Device's Access Point to use the most free Wi-Fi channel (see V).</p>



Issue	Possible causes and solutions
<p>I can not connect the Device to an existing Wi-Fi network in «WiFi Client» mode. Device «NET» LED indication shows first LED flash red, second LED flash is also red.</p>	<p><b>1. 2.4 GHz Wi-Fi is not enabled on Wi-Fi router.</b> Make sure you are connecting to router's 2.4 GHz network (not to a 5 GHz network).</p> <p><b>2. Wi-Fi signal issues.</b> Confirm if target Wi-Fi network is visible in the list when you perform scanning for Wi-Fi networks.</p> <p><b>3. Bad Wi-Fi network authorization credentials.</b> Double-check if you have entered correct existing Wi-Fi network connection details (SSID and passphrase). Reset the Device settings and try again.</p>
<p>I can not access the Device's web interface or Web Gauges page. Wi-Fi connection status («NET» LED) shows correct Wi-Fi module operation mode (first LED flash matches desired mode, Access Point vs Wi-Fi Client and second LED flash is green, indication connection status OK).</p>	<p><b>1. Bad IP settings.</b> Check if you can ping the device by its IP address. If not, check the network connection status (first two «NET» LED flashes, see IV) and IP settings:</p> <ul style="list-style-type: none"> <li>• if Device is in Access Point mode, enable DHCP on Wi-Fi client device</li> <li>• if Device is in Wi-Fi Client mode, try Static IP or DHCP tethering, (see V.2).</li> </ul> <p>Also make sure your Router does not block IP connections between Wi-Fi clients (turn «Wi-Fi isolation» feature off or create a «guest» Wi-Fi network, connect the Device to this «guest» Wi-Fi network and enable routing between «guest» and «main» WiFi networks). Check also if your Wi-Fi Router does not block or redirect HTTP traffic on port 80 (Device's default port for HTTP requests), change Device's HTTP port if necessary (see 5.3).</p>

Issue	Possible causes and solutions
	<p><b>2. More than 3 TCP connections are opened to the Device simultaneously.</b> Close all excessive connections, use UDP network protocol on Device's Servers. Reboot the Device to drop all active connections.</p>
<p>I can not open TCP Server port in an application. Wi-Fi connection status («NET» LED) shows correct Wi-Fi module operation mode (first LED flash matches desired mode, Access Point vs Wi-Fi Client and second LED flash is green, indication connection status OK).</p>	<p><b>1. Exceeded the number of TCP connections (3) to that Server.</b> Configure application to use another Device's Server or try connecting to Server using UDP network protocol.</p> <p><b>2. IP address of Gateway have changed when Device is in Wi-Fi Client mode.</b> Set static IP address or set up «DHCP Tethering» on your Wi-Fi router (see V.2). Make sure that you can ping the Device and/or open the Device's web interface in a browser.</p>
<p>I can not log into the device web-interface or I have forgotten the web-interface password. Device's NMEA 0183 Port LED indicates an overflow (LED flash #4 is red).</p>	<p><b>1. Wrong administrator password.</b> Reset the device settings (see VII).</p> <p><b>2. Too much data to fit into the outgoing data stream on the selected NMEA 0183 Port baud rate.</b> If target NMEA 0183 equipment supports NMEA 0183 HS baud rate of 38400, set both equipment Listener port and Device's Port baud rate to 38400. Alternatively, exclude unnecessary sentences on this Port «Output» (Talker) using Data Filers (see VIII).</p>

<b>Issue</b>	<b>Possible causes and solutions</b>
<p>Device does not receive (rejects) Navtex messages or NMEA 0183 messages with incorrect/missing checksum. When target equipment sends data, Device's NMEA 0183 Port LED indicates correct baud rate, but reception error (Port LED flash #1 is green, but flash #2 is red).</p>	<p><b>1. Navtex messages are not NMEA 0183 sentences.</b> Turn on «Tunnel» on target Port (see VIII) to pass-through Navtex messages.</p> <p><b>2. Bad NMEA 0183 sentences are sent by connected 0183 equipment Talker (old version of the Standard, missing checksum).</b> Record diagnostics log (see XI) and check incoming (received) NMEA 0183 data stream on target Port for incorrectly formed sentences (see II). If you observe sentences with bad or missing checksum, enable Device to «Fix or add the checksum»; if sentence is malformed try «Replace the substring» feature (see IX.3).</p>

