Solutions

Bridge E

User Manual

ER-EB 1000M
ER-EB 1000M-2
r24.11

Table of Contents

Disclaimer

All directives, data and requirements mentioned in this document relate to CE certification and use in the EU. The sections of this document regarding the FCC certifications are still work in progress and will be updated in the near future. Conformity and approvals for US/CA are explained in a separate section marked with FCC (Section 3.1.3).

1 General Terms of Use of this Document

It is the user's responsibility to check and ensure they have downloaded the latest version of this manual regularly as R3 may edit, revise, or improve product documentation over time.

The user must ensure the product is used correctly according to this document's guidelines, in particular observing all relevant standards and regulations.

This document, including all diagrams and images, is copyright-protected. Any changes whatsoever violate our Terms of Use.

> **NOTE** — To configure devices running this new release 24.11, please ensure the R3 Configuration Server version is also updated to at least 8.2.x
>
> Devices with older release versions require the previous R3 Configuration Server version for configuration. Note that the new config server can only be used with older release versions to update devices to the latest release and configuration of older versions is not supported in the new software version.

2 Please Observe the Following Notes

Please observe and obey the following note formats and instructions throughout the document:

TIP — Text in this format is information explaining the use of the product.

ATTENTION — Text in this format must be observed to prevent malfunctions and/or even damage, or safety risks.

EXAMPLE/NOTE — Text in this format provides examples or notes.

Solutions

3 Product Information

3.1 General Information

3.1.1 Versions of this Product

- ER-EB 1000M / ER-EB 1000M-2 (EU Version)

- ER-EB 1000M / ER-EB 1000M-2 (US/CA Version)

3.1.2 Conformity/National Approvals – CE (EU)

The device complies with these essential EU directives, which include any modifications:

- 2011/65/EU Restriction of the use of certain hazardous substances (RoHS)

- 2014/53/EU Radio equipment (RED).

Additional information (e.g. declaration of conformity, documents, data sheets, certificates, etc.) can be found at www.r3.group.

3.1.3 Conformity/National Approvals – FCC (US/CA)

Additional information (e.g. declaration of conformity, documents, data sheets, certificates, etc.) can be found at www.r3.group.

FCC 47 CFR 15 Compliance

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference;
2. This device must accept any interference, including interference that may cause undesired operation.

⚠ **ATTENTION** — Changes or modifications made to this equipment not expressly approved by R3 may void the FCC authorization to operate this equipment.

This equipment 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 residential installation.

This equipment 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 equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

> **ATTENTION** — This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. Under normal use condition the user has to keep at least 20cm separation distance between radiator and body of the user.

> **ATTENTION** — This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

> **ATTENTION** — Professional Installation Notice: To comply with FCC Part 15 rules in the United States, the system must be professionally installed to ensure compliance with the Part 15 certification. It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States. The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly forbidden.

RSS-247, Issue 2 of ISED

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference;
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. L'appareil ne doit pas produire de brouillage;
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

> **ATTENTION** — This device has been designed to operate with dipole antennas having a maximum gain of 8.5 dBi. Antennas having a gain greater than that are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication. That the device for the band 5,150-5,250 MHz is only operated indoors to reduce potential for harmful interference to co-channel mobile satellite systems.

3.2 Intended Use of the Product

The Bridge E (device) provides a reliable, time-critical wireless link between Ethernet-based industrial protocol devices. It can be used to:

- Replace cable-based network infrastructure with a wireless connection in machinery, vehicles and devices, providing simplified infrastructure and flexible operations.

- Replace network cables between moving structures or components in machinery, vehicles and devices to reduce weight, size and use of installation space, as well as wear and tear on network infrastructure.

⚠️ **ATTENTION** — Installation must only be performed by qualified specialist personnel.

⚠️ **ATTENTION** — This radio device is designed to transmit wireless data. It is also intended to be used for low latency and/or high reliability data communications. When using the device, keep in mind the general behavior and physics of the wireless channel. Abrupt or predictable changes in the operational environment, such as movement of people or objects, and the presence of interfering devices, can result in reduced wireless signal quality and failed data transmissions. As a result, **intended operations cannot rely solely on this device when used in critical applications, where the result of poor wireless conditions can cause serious injury or economic damage**. A comprehensive system solution, such as an integrated wired fail-safe in the case of poor wireless connectivity, must be installed and tested to the level of intended application's importance.

⚠️ **ATTENTION** — The device emits Radio Frequency (RF) energy in the Industrial, Scientific, Medical (ISM) bands. Make sure that all medical devices used in proximity to this device meet appropriate susceptibility specifications for this type of RF energy.

⚠️ **ATTENTION** — The antennas used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be colocated or operating in conjunction with any other antenna or transmitter.

⚠️ **ATTENTION** — The device is recommended for use in industrial environments. It is mandatory to use a functional ground connection to comply with safety requirements.

⚠️ **ATTENTION** — The device is certified with the enclosed antenna. Any other antenna can exceed the maximum permitted transmission power.

⚠️ **ATTENTION** — The device must not be disassembled. Do not break the seal!

3.3 Equipment Required

ID	Item	Needed to		
		Deploy	Operate	Update
❶	Bridge E	x	x	x
❷	Power Cable M12, 5-pin, A-coded	x*	x*	x*
❸	Ethernet Cable M12/RJ45	x	x	x
❹	Network Switch	x		x
❺	Ethernet Cable RJ45/RJ45	x		x

* Item not needed if Power over Ethernet (PoE) is used.

3.3.1 Requirements for the Equipment

ID	Item	Requirements
❸	Ethernet Cable M12/RJ45	The signal cable for digital input must be routed in the same cable as the power supply and functional ground if the line length exceeds 3 meters.
❹	Switch	Possibility to disable IGMP Snooping; at least as many ports as Bridge E devices should be connected + 1

> **TIP** — Not all switches support IGMP Snooping, we recommend turning it off. For more information check the IGMP section in Troubleshooting.

3.4 Connectors
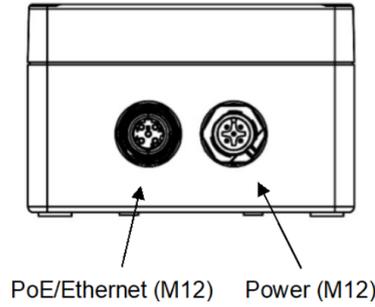
Figure 3-I: Connectors

> 💡 **TIP** — The Ethernet connector is PoE (Power over Ethernet) and can also be used to supply power to the device (48 VDC, PoE 802.3at Type 1).

Figure	Pins	Function
	1	Power supply 24 VDC (+/- 10%)
	2	Ground for digital input
	3	Ground for power supply
	4	Digital input + (9 – 30 VDC)
	5	Functional ground

Table 3-i: Power connector (M12 plug, A coded)

Figure	Pins	Function	Color Mark (T568B)
	1	Send	Orange/white
	2	Receive	Green/white
	3	Send	Orange
	4	Receive	Green

Table 3-ii: PoE/Ethernet connector (M12 plug, D coded)

3.5 LED Indicators

LED	Color/pattern	Meaning
Power	Off	No power.
	● Green	Device is connected to power.
Ethernet	● Green	Ethernet physical layer was able to establish a connection to another device.
Config	Off	Device is in Deployment Mode.
	● Green	Device is in Configuration Mode and a Configuration Server was found.
	● Green blinking (slow)	Device is updating its firmware.

LED	Color/pattern	Meaning
Status	● Green	Device is in active deployment and EchoRing is reporting healthy state.
	● Green blinking (slow)	EchoRing offline.
	● Red	The main station manager task found an unrecoverable error. Device is not working.
	● Red blinking (slow)	EchoRing not in healthy state.
	● Red / ● Green switching (fast)	System initialization experienced a critical failure. The system is most likely offline on all interfaces.
	● Red / ● Green switching (medium)	Failed to start or stop EchoRing and/or the Bridge E or the initialization of the Bridge E failed during bootup.
Config+ Status	● Green flashing Config and Status (very slow)	System is initializing.
	● Green flashing Config and Status (very slow) with ● Orange Status for a short moment at the beginning of a cycle	Waiting to receive a DHCP lease.
	● Green flashing Config (slow) alternating with ● Green blinking Status (fast)	Update successful.
	● Green flashing Config (slow) alternating with ● Red blinking Status (fast)	Update failed.
	● Green flashing Config ● Green Status	The EchoRing network interface has been started or, in the case of a Mobile Station in Deployment Mode, the device is ready to be controlled via ERCI (see Section 8.2).
	● Green Config ● Red flashing Status	Failed to deploy the configuration to flash or failed to verify the written configuration.
All	Off	Inconclusive; a specific mode might have been exited (depending on context).

Table 3-iii: Explanation of LEDs

TIP — There are other LED labels on older versions of the Bridge E: PWR (Power), ETH (Ethernet), CFG (Config), HLT (Status).

Flashing speeds

- Very Slow: 1.6s on - 1.6s off

- Slow: 800ms on - 800ms off

- Medium: 200ms on - 400ms off

- Fast: 200ms on - 200ms off

![R3 Solutions logo]

4 Installation

4.1 Hardware Installation
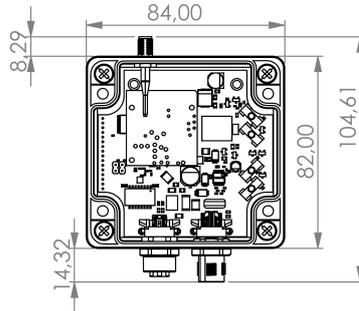
Figure 4-I: Dimensions are in millimeters (mm)

Screw the antenna(s) to the device's SMA connector(s). *Note: antenna is not included in the diagram.*

⚠️ **ATTENTION** — Antennas should only be tightened by hand or with a torque wrench of maximum 0.3 Nm.

4.1.1 DIN Rail Mounting
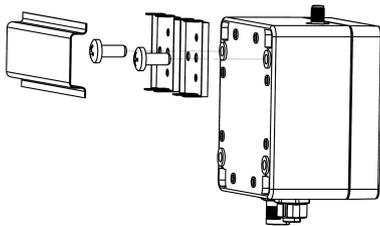
Figure 4-II: DIN rail mounting

Applies to both versions of the Bridge E.

1. Use the provided self-tapping screws to attach the device to DIN rail. Place the self-tapping screws through the small DIN rail-adapter-plates and screw them into their designated position in the device.

2. Place the device that is now attached to the adapter on the top edge of the DIN rail.

3. Push the device downwards so that it snaps into place.

💡 **TIP** — To release device from DIN rail, push the device downwards while pulling outwards.

4.1.2 Wall or Mast Mounting

💡 **TIP** — Attaching wall mounts to a device is irreversible.

1. Place the wall mounts in their desired positions on the device. They can be placed horizontally or vertically.

2. Use adequate force to drive the mount bolt in the device notch. If using a hammer, please ensure you do not accidentally hit and damage the device casing.

3. Repeat with the other mounts.
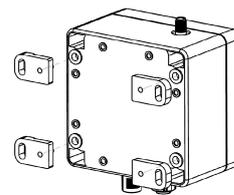
Figure 4-III: Wall or mast mounting

Applies to both versions of the Bridge E.

4.2 Software Installation

4.2.1 R3 Launcher Application

The R3 Launcher is an application provided as a single installer which can be found at www.r3.group/en/support-downloads/ under "Software".
The application allows you to enable Internet Connection Sharing (ICS) and launch the Configuration Server that can be accessed using your browser.

> **NOTE** — For using the installer and the application the following requirements have to be met: the computer needs to run on Windows 10 or 11 and admin rights are needed for starting the installer and the application.

- To install, double-click the R3 Launcher application setup file.

- It will prompt confirmation to make changes to your system. Click on "Yes".
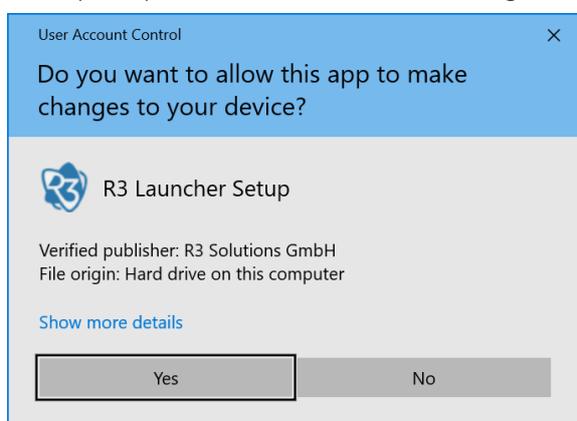
- When the screen below appears, select if you want to create a desktop shortcut and click on "Next".
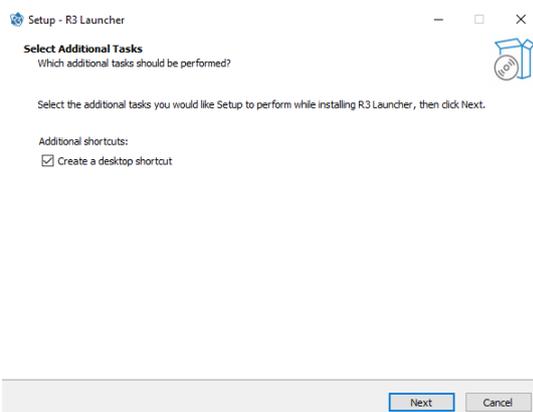
- Click on "Install". This will run the setup file and begin installing the R3 Launcher application on your computer.
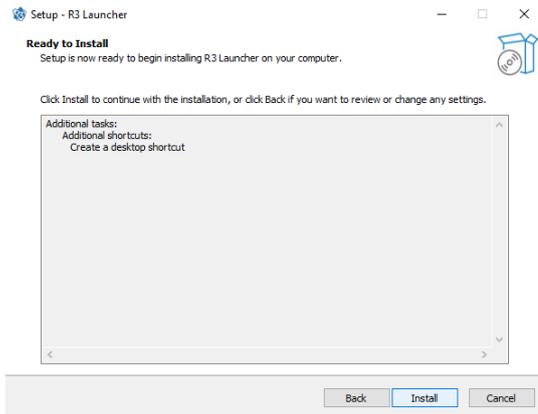
- Wait for R3 Launcher to finish installing. The installation will be completed in a few seconds.
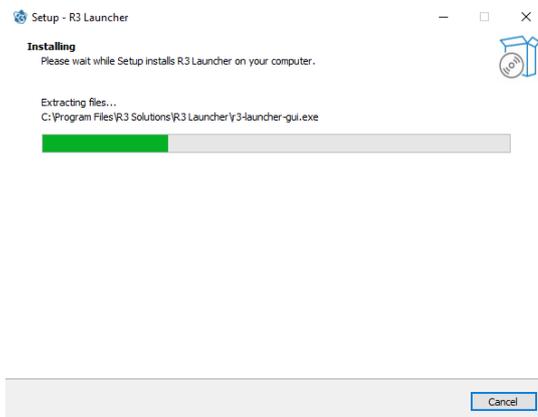
- Click on "Finish" to complete the installation process. The R3 Launcher application is now successfully installed on the system and ready to use.
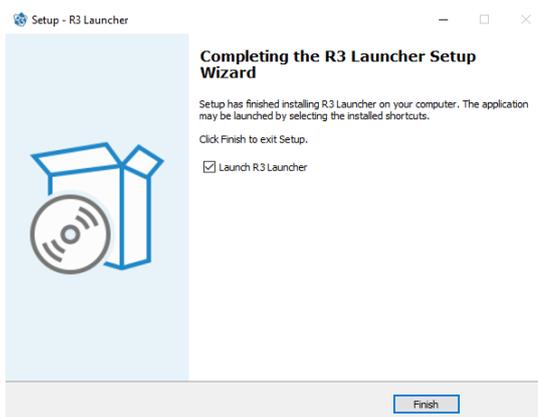
4.2.2 Internet Connection Sharing

An internet connection is required to update the Bridge E. When you operate the Bridge E in a separated network without internet connection, you can use ICS to share the connection from a second network interface (e.g. WiFi). When ICS is activated, it automatically includes a Dynamic Host Configuration Protocol (DHCP) server. To enable ICS in the application, select the interface providing the internet connection ("Internet" interface). Then you can enable ICS using the toggle switch.
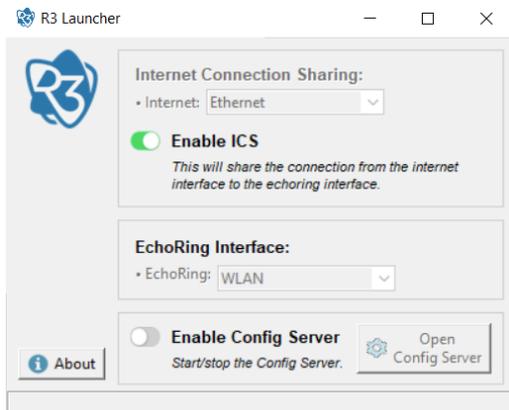
NOTE — Due to a problem with Windows 10, enabling Internet Connection Sharing can interrupt the ability to access the web on the computer sharing the connection.
Suggested courses of action:

- Try connecting to the Internet over Ethernet.

- Try using a WiFi dongle as the problem might be related to certain brands of WiFi cards.

- Install update KB5014669.

- Factory reset the computer.

4.2.3 Configuration Server

The Bridge E is configured and can also be updated using the Configuration Server. The Bridge E is updated using the Configuration Server. By enabling ICS, the Bridge E device will be assigned an IP address via DHCP and there is no manual IP assignment needed. To start the Configuration Server, select the network interface it should be running on ("EchoRing Interface").

⚠️ **ATTENTION** — Do not set-up multiple instances of the Configuration Server on the same physical Ethernet interface.
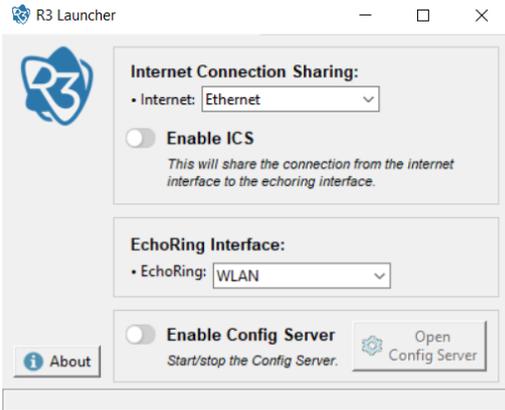
This interface needs an assigned IP address to run the Configuration Server. Start the server by clicking the toggle-switch "Enable Config Server".
Click the "Open Config Server" button to access the web-based user interface.
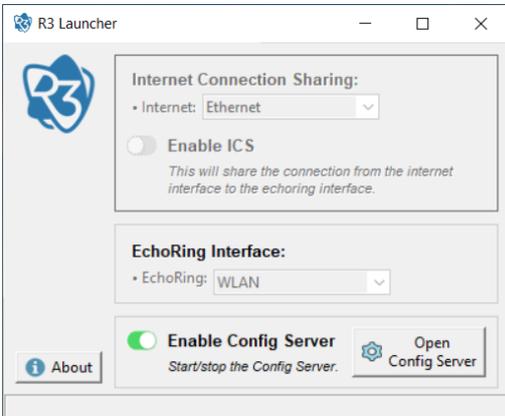
If no IP address is assigned, the following error prompt will appear:

ℹ️ **NOTE** — Alternatively to ICS an external DHCP server can also be used.

4.2.4 Set Up and Access Web User Interface

The web-based configuration interface is used for configuring, deploying and updating devices.

1. Set up and connect a PC running the R3 Configuration Server and the Bridge E devices ①, intended to be in the same network or subnetwork, to the switch ④, according to Figure 4-IV:
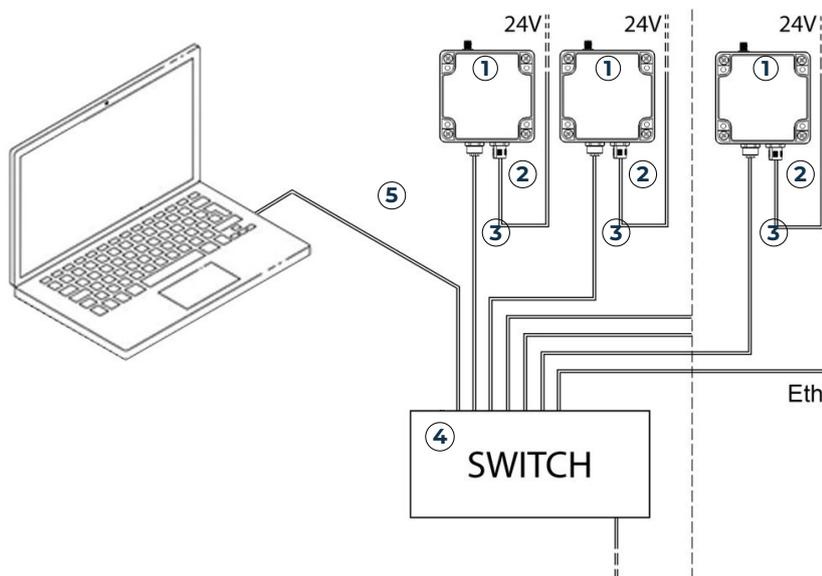
Figure 4-IV: Configuration set-up

2. Turn on the network switch.

3. Start the R3 Launcher application and start the Configuration Server. The Configuration Server needs an IP address on the EchoRing interface (either from ICS, a DHCP server, or assigned manually).

4. Open a web browser and enter the URL `http://localhost:8080`.

> **TIP** — The web-based user interface supports the web browsers Firefox and Chrome version 100 or newer, we recommend using version 114. Other browsers may not support full functions.

5. Turn on the Bridge E devices.

4.2.5 Update Devices

> **TIP** — New devices might require a software update before use. In that case you must register first to have access to an update that you can perform. Please download the registration form here. Typically however, the devices are shipped with running firmware, thus there is often no need for an initial update.

> **NOTE** — To successfully run updates, admin rights and internet connection are required.

New devices are already initialized but might require an update before use. They require an internet connection and a DHCP and Network Time Protocol (NTP) server in the network to perform an update. If you are using ICS, the DHCP and NTP servers are provided by ICS.
Devices will never search or update on their own. This is to assure solution stability.
Updates are assigned on a customer basis. Ask your sales representative about new versions.

1. Switch power on and set up the devices as described in Section 4.2.4.

2. Click the IP address to update all devices or click the devices that should be updated individually.

3. Click "Update Devices".
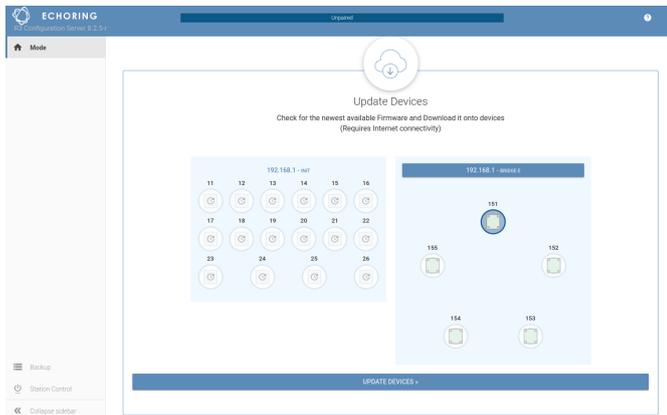
4. Click "Run Update" to install the listed update on each device on the screen. In certain circum-stances it might be the case that no version information is provided.
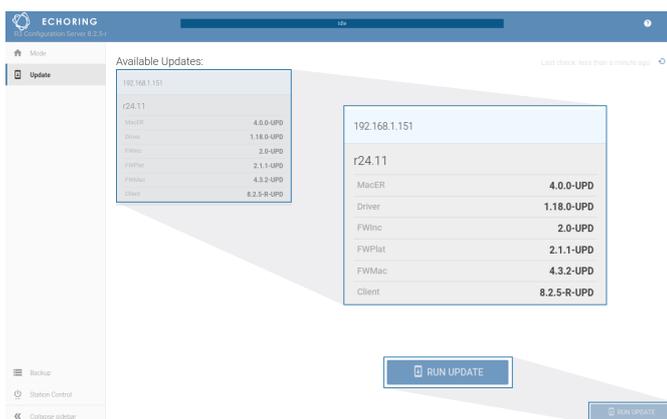
5. Downloading started and the update will be installed right afterwards.
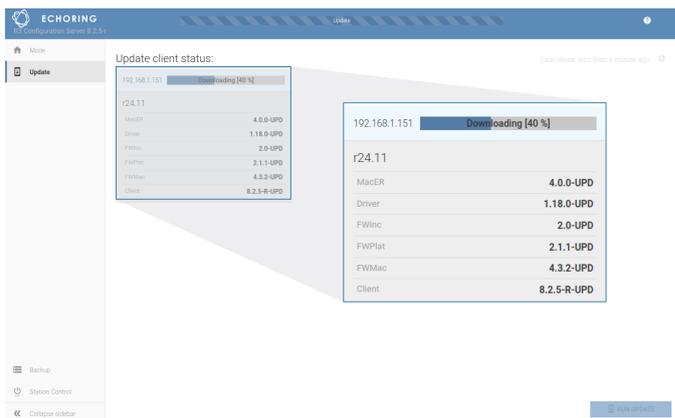
6. The update is complete. Click "Mode" to go back to the main page.
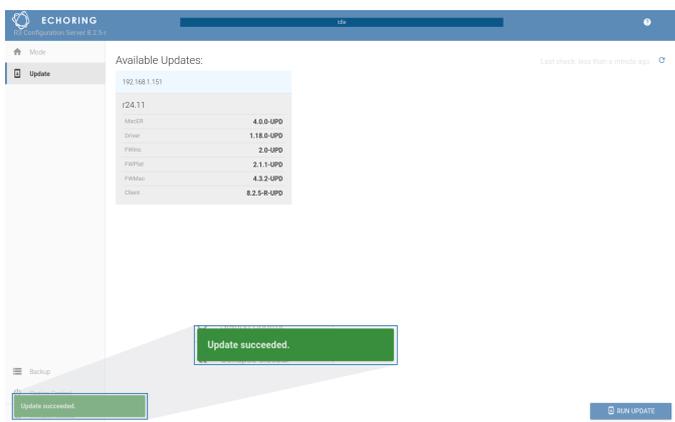
4.3 Configuration and Deployment

There are mainly two modes a device can operate in: Configuration Mode and Deployment Mode.
A device can be configured and updated in Configuration Mode. The device loads the deployed configuration in Deployment Mode.

New devices will be in Configuration Mode. Once a configuration is successfully deployed, the device will go into Deployment Mode after the next reboot.
Devices can be reset to Configuration Mode using the Configuration Server. Open the "Station Control" section, type in the IP address and click on "Select Command" and then "Set Config Flag". Make sure that the IP configuration of the relevant interface needs to be set properly.

Once that command is sent to the device via "Run Command", it will return to Configuration Mode after the next reboot.

The device will go into Fallback Mode if an error occurs during deployment or bootup. In Fallback Mode, the device can be returned to Configuration Mode using the Configuration Server as described above.

5 Using the Device

5.1 Basic Concepts

Subnetwork	A subnetwork is a network of multiple Bridge E devices where all participants can communicate directly with each other. Each subnetwork has its own channel assignment.
Network	A network consists of one or more subnetworks. All subnetworks within a network form a handover domain. If handover is enabled, stations can roam between subnetworks inside the network seamlessly.
Handover	The roaming of Mobile Stations between different subnetworks within one network is called Handover. Mobile Stations do not lose their connection during the Handover process.
Reconfiguration	Mobile Stations can switch between networks (where each network has its own configuration). The Mobile Station is not able to communicate during reconfiguration.
Mobile Station	A Mobile Station can seamlessly roam between subnetworks within one network. Roaming to a new subnetwork needs to be triggered externally. Mobile Stations can be reconfigured to switch to another network.
Static Station	A Static Station is a stationary node in a subnetwork that can be connected to one or more client devices.
Anchor Station	An Anchor Station is a Static Station acting as the central station of a subnetwork for Mobile Stations using Handover. It requires a connection to a shared backbone network between all Anchor Stations of other subnetworks within the same network to support seamless handovers.
Relay Station	A Relay Station is not connected to a network or client device. It is introduced into a subnetwork to increase reliability without consuming any additional resources in the subnetwork. Currently only one Relay Station per subnetwork is supported.

5.1.1 Introduction

The Bridge E devices can be used in multiple application scenarios, for example, in storage, logistics, production or tools.

Let's take lifting platforms as an example in production. Nowadays large workpieces in production lines, such as car chassis, are often carried between workstations by lifting platforms. Complex cable layouts ensure power and real-time data connectivity. Despite their speed and reliability, cables are constantly subject to wear and tear and are frequently prone to failure, resulting in expensive downtimes for diagnosis and repairs.
EchoRing revolutionizes M2M communications, combining speed and reliability with the flexibility of wireless networks. Fewer physical points of failure ensure durable, mobile setups with far fewer maintenance cycles.

But how does this work?

Let's stay with the example of the lifting platforms that are used on a shopfloor.
Lifting platforms are stationary conveyor systems embedded in the floor. They are commonly used for final assembly of vehicles. In this context, lifting platforms are contiguous, similar to a chain, and move forwards in tandem at low speeds.

Let's assume there are Bridge E devices on each workstation and on each platform. For each safety-critical production section there is a separate "configuration zone", which corresponds to a network. A network can consist of several subnetworks.

The Anchor Station is the central station of a subnetwork. There must be one Anchor Station per subnetwork. It is connected to a shared network with all Anchor Stations of other subnetworks to allow signaling.

There can also be Relay Stations in a subnetwork. Relay Stations exist to increase reliability. They do not take part directly in the network, meaning they do not consume or block any (temporal) resources in the subnetwork but can be used as a "relay". Currently only one Relay Stations per subnetwork is supported.

If a platform runs through a production line, then the Bridge E on this platform is called a Mobile Station. Mobile Stations which move through the production line can switch between the subnetworks performing Handovers without interruption.

Each of the sections has its own subnetwork selection and its own channel assignments, which are loaded during downtime between the safety-critical sections. As a result, there is a (Re-)configuration of the Bridge E at the beginning for each "configuration zone".
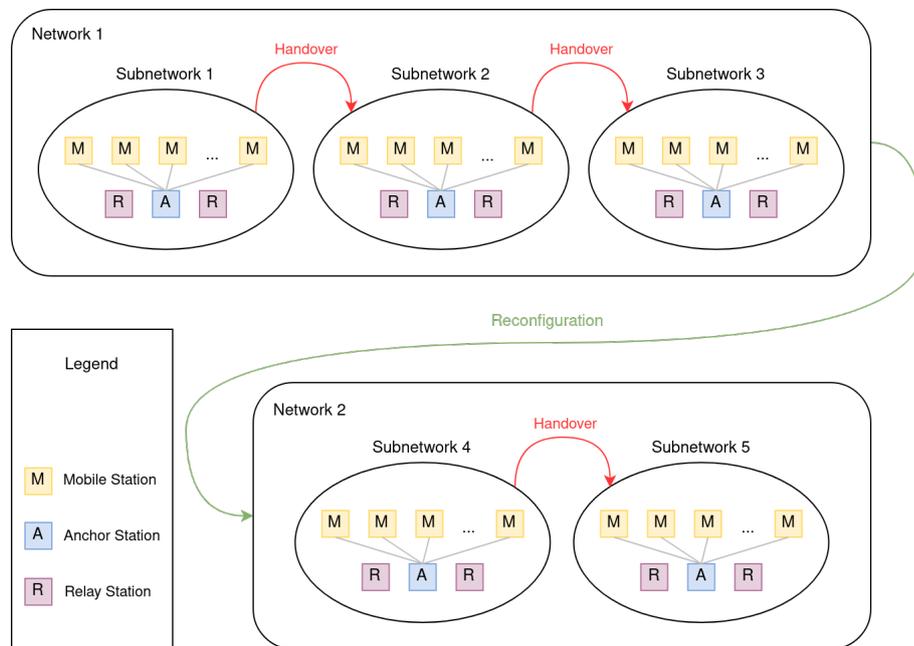
Each network has a defined maximum number of Static and Mobile Stations and a defined number of transmission slots. Aside from that the level of reliability, the maximum frame length, the latency and more parameters can be configured.

For each subnetwork it can be chosen on which channel and with which power the Bridge E devices should operate.

Per Bridge E a capacity factor can be picked (which is limited by the overall network capacity) e.g. to configure asymmetric traffic. Furthermore each Bridge E can be used either as an Anchor or as a Relay Station or neither. The MAC address of network components that should be connected to the Bridge E can be defined as well as if the device should obtain its IP from a DHCP server or use a static IP.

Further information about all parameters and how to configure them will follow in the next sections.

5.2 Configuration

In order to configure devices, they must be set to Configuration Mode before they are booted. Configurations can be created without having actual Bridge E connected, but deploying a configuration to an existing device is only possible if that decvice is set to Configuration Mode.

> **NOTE** — If the configuration on a device has exactly one network and one subnetwork (i.e. Static Stations including Anchor and Relay Stations) then the device will start automatically. Otherwise they are Mobile Stations and need to be started using External Runtime Control Interface (ERCI) commands (see Section 8.2). The command to enable the Configuration Mode on future bootups of the Bridge E can be sent by the Configuration Server (see Section 4.3).

To enter the Configuration, click on "Configure Plant".
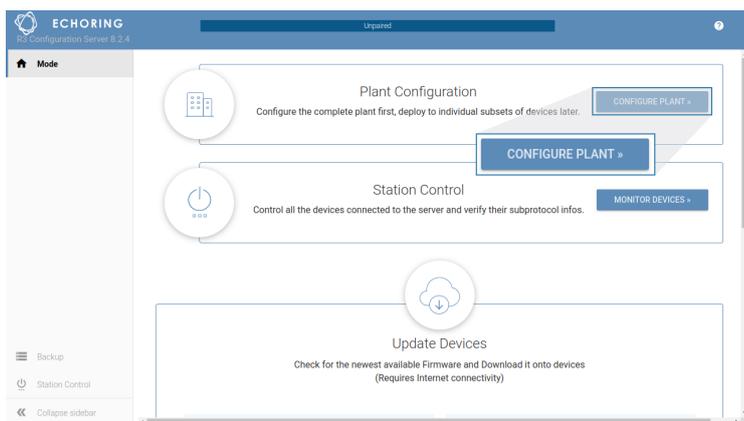
In the top middle you can see the name of the plant which you are currently configuring. Click on it to see the list of plants. You can create new ones, rename existing ones and also copy an existing plant.
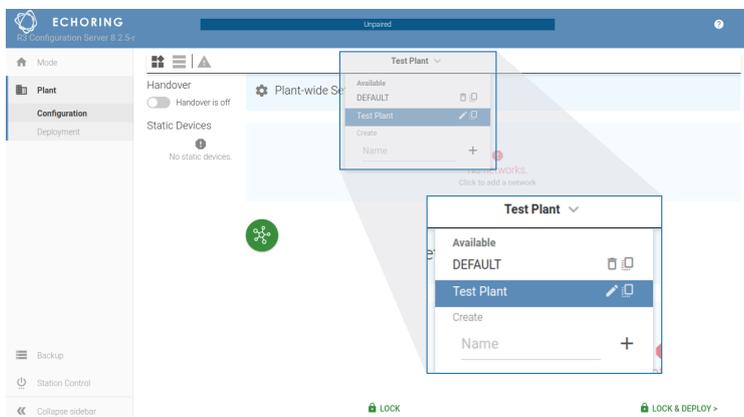
You can add networks and subnets by clicking on the corresponding green button.

> **NOTE** — The maximum number of networks is 20 with no more than 24 subnetworks per network.

To change the view, click on the ≡ symbol in the top bar. An overview of all networks, subnetworks, etc. is then displayed in a list. As before, you can click on networks, subnetworks or individual devices to change the settings.
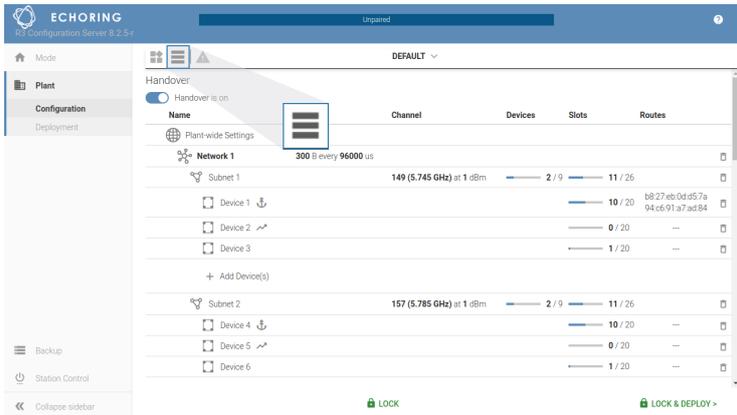
The configuration is split into Plant-wide, Mobile-wide, Network, Subnetwork and Device settings.

5.2.1 Plant-wide Settings

Plant-wide settings affect the entire plant and are the highest level of settings.

(A) Handover Toggle:
The handover functionality can be turned on/off explicitly for the whole plant by toggling the button. Disabling handover deletes all mobile devices after confirming.
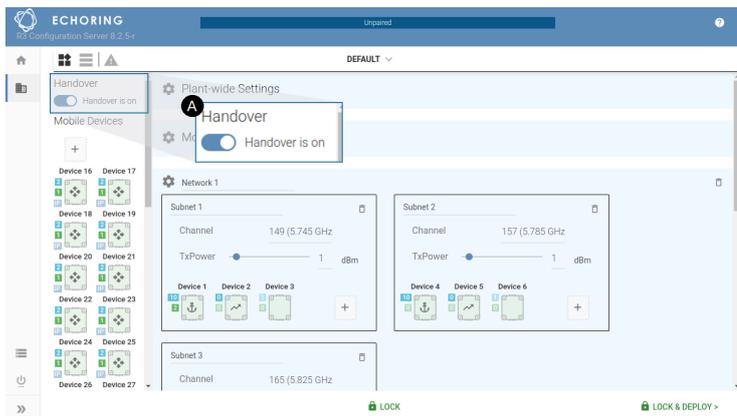
(B) Backbone IP and Backbone Port:
Backbone IP is a multicast IP mask specifying the first 3 common bytes of the multicast IP that the Anchor Stations subscribe to. The range for valid IPs is 224.0.0.0 to 239.255.255.255. This information along with the Backbone Port is collectively used by Anchor Stations on the backbone to subscribe to a multicast address made up of a multicast port equal to the Backbone Port and a multicast IP equal to the Backbone IP appended with subnet ID. It enables Anchor Stations to communicate with each other using a multicast address formed by appending the Target subnet ID to Backbone IP.
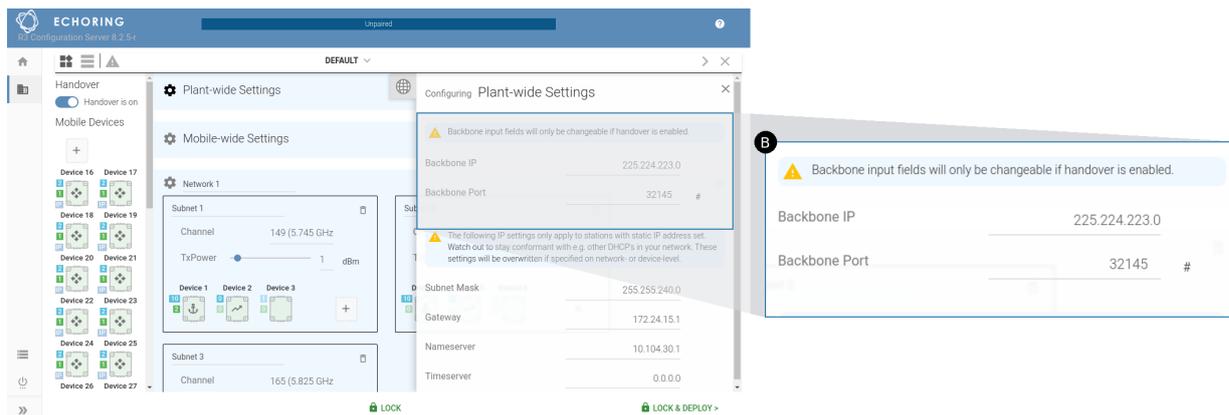
C Subnet Mask, Gateway, Nameserver, Timeserver:
These settings are specified per plant. If necessary, they can be overwritten on a network and device level or for all Mobile Stations. The most specific setting takes precedence.
An IP address needs to be entered to configure the Subnet Mask, Gateway, Nameserver or Time-server. It is not possible to use an URL to configure it.
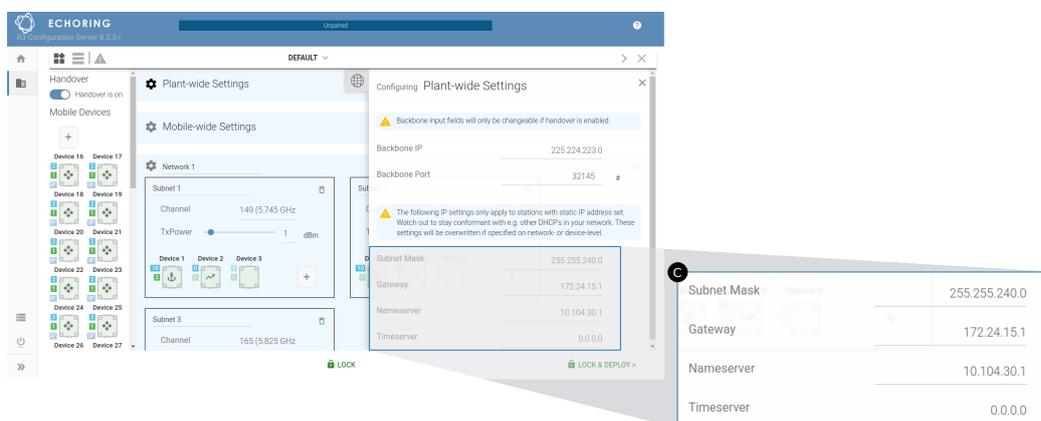
5.2.2 Mobile-wide Settings

Mobile-wide setting only affect the Mobile Stations.

> **NOTE** — When the (A) Handover Setting (as described in Plant-wide Settings) is disabled, all mobile stations will be deleted and this section will not be shown.

A Subnet Mask, Gateway, Nameserver, Timeserver:
If these settings are specified on mobile-wide level, they override those from plant-wide settings. If necessary, they can be overwritten on a network and device level. The most specific setting takes precedence.
An IP address needs to be entered to configure the Subnet Mask, Gateway, Nameserver or Time-server. It is not possible to use an URL to configure it.
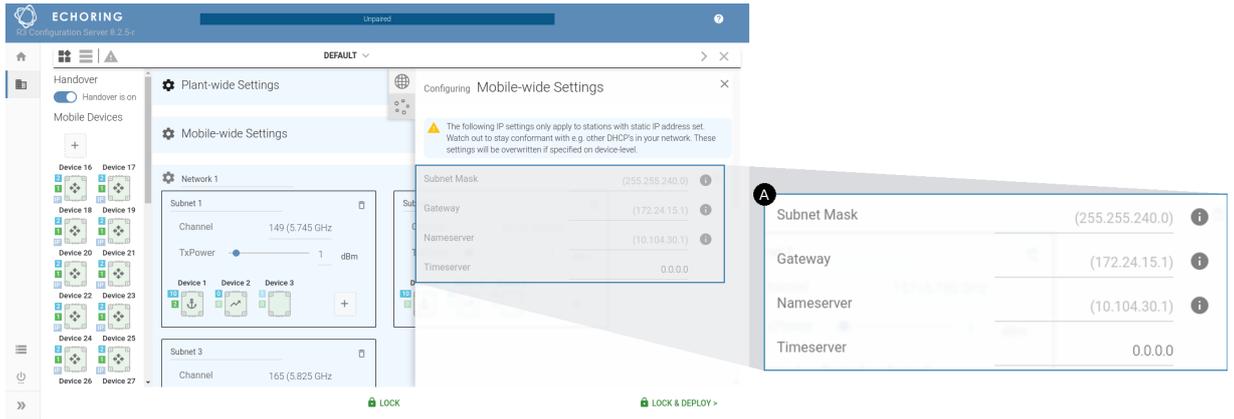
Mobile Stations are listed on the left. To add more, click on the "+"-symbol. Left-click to add one station, right-click to add several stations at once.
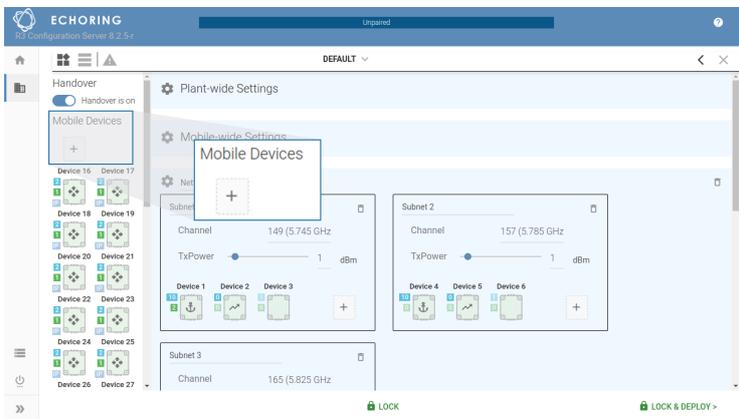
i **NOTE** — The maximum number of all devices in a plant is 239.

5.2.3 Network Settings

The networks can be renamed. The configuration for the different networks can be changed by clicking on the gear icon next to the name. All configurable parameters are defined as follows:

Basic Settings
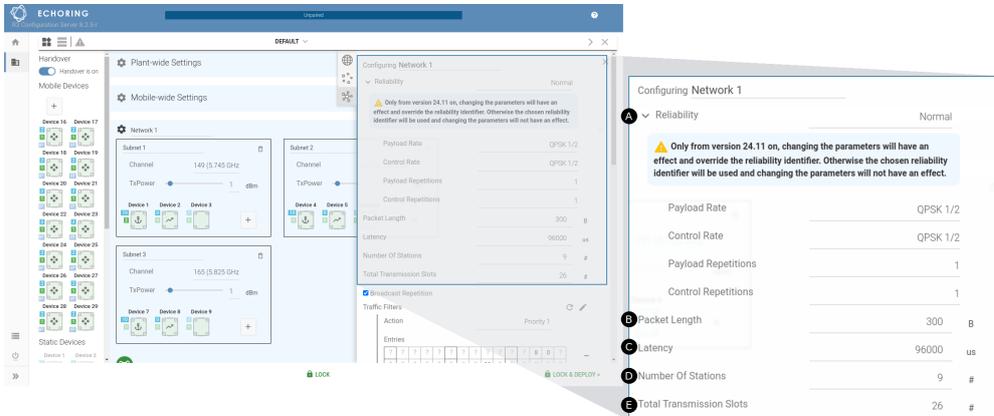
(A) Reliability: defines the Modulation Coding Scheme and the number of scheduled frame repetitions for the EchoRing protocol. By clicking on the setting, more detailed options will be displayed. Reliability can be split into Payload Rate, Control Rate, Payload Repetitions, and Control Repetitions, all of which can be set individually. See Table.

- Payload Rate: Shows the current MCS for payload packets.

- Control Rate: Shows the current MCS for control packets.

- Payload Repetitions: Specifies the number of times a payload packet is retransmitted if the direct link fails. With n repetitions, there will be a total of n+1 transmissions.

- Control Repetitions: Specifies the number of times a control packet is retransmitted if the direct link fails. With n repetitions, there will be a total of n+1 transmissions.

> **NOTE** — The split settings are only available from version 24.11 on. Older versions will only use the reliability identifier.
>
> (i)

(B) Packet Length: the maximum length of priority packets to be conveyed over EchoRing (Ethernet frame size including headers). The Bridge E traffic may be fragmented.

(C) Latency: the maximum time limit for a priority packet to be queued for transmission in EchoRing before it is dropped. An infeasible latency might cause the configuration not being accepted by the bridge.

(D) Number of Stations: the maximum number of Static and Mobile Stations in each subnetwork in this network. Relay Stations do not count into the Number of Stations. Maximum is 20.

(E) Total Transmission Slots: configures the number of available transmission slots available in each subnetwork, allowing for greater data throughput or asymmetric traffic per device in relation to overall network capacity.

Advanced Settings

(F) Broadcast Repetition:
EchoRing uses cooperative communication to increase reliability. A suitable Relay Station is selected for each frame to repeat the frame if the direct link fails.
Broadcast traffic is sent to all stations in the network, and thus has no clear destination, which makes it difficult to determine a single suitable Relay Station for all possible destinations. As a result, broadcast frames are only sent once by default.
The Broadcast Repetition setting enables repetition of broadcast frames to increase reliability. This setting only applies to Priority 1 frames. If enabled, all Priority 1 broadcast frames are repeated once. Deduplication in cases where both frames are received is performed on the receiving station. The Broadcast Repetition will only take place once all other Priority 1 frames not yet sent have been sent.

> **TIP** — The repetition of the broadcast frame will take up a transmission slot. Please include this in your capacity calculation. All priority will be dropped after the configured maximum latency. This applies to broadcast repetitions as well.

(G) Traffic Filters:

EchoRing allows you to distinguish five priority classes. Datatraffic can be assigned to a priority class using a bytemask. It is possible to assign different priorities to different filters. It is also possible to drop unwanted traffic using a drop rule.

Priority filters are evaluated in the listed order, starting from the top. Only the first match is applied, with one filter per packet. The filter transmission order can be rearranged via drag and drop.

To enable prioritization, choose a priority action in the Traffic Filter section from the dropdown menu.

To select the bytes of the frames which should be filtered, type in the byte value in the box for the corresponding byte index.

All traffic that does not match the filter is treated as "Best Effort" and thus will be sent after all priority traffic. The latency drop rule is not applied to "Best Effort" traffic.

> (i) **NOTE** — Data to be transmitted is buffered in a queue and transmitted when its device's transmission slot is available. If the application has multiple traffic types, such as critical control/safety frames or best-effort frames, the critical frames can be prioritized via a filter. Frames matching the filter will be buffered in the corresponding priority queue and sent prior to frames in the "Best Effort" queue. If no prioritized traffic is set, all data is treated as "Best Effort".

> (i) **NOTE** — If Handover is enabled, drop rule for anchor multicast traffic is automatically added based on "Backbone IP" setting (see (B)). This rule will not be added automatically if it is already manually entered.

H Queue Sizes:

> ⚠ **ATTENTION** — This setting needs changes only in very specific scenarios. Proceed with caution!

The queues in EchoRing are equally sized by default. In special cases, e.g. with very high traffic load in one priority class compared to the others, it may be necessary to customize the queue sizes to ensure no frames are lost.

EchoRing will allocate the queue sizes automatically by default, or if the entries are not specified (all entries 0).

To customize queue sizes, queue sizes need to be configured for all priorities that have been assigned in the Traffic Filter section. If possible, the available buffers will be assigned as specified, any additional buffers will be distributed equally among all queues.
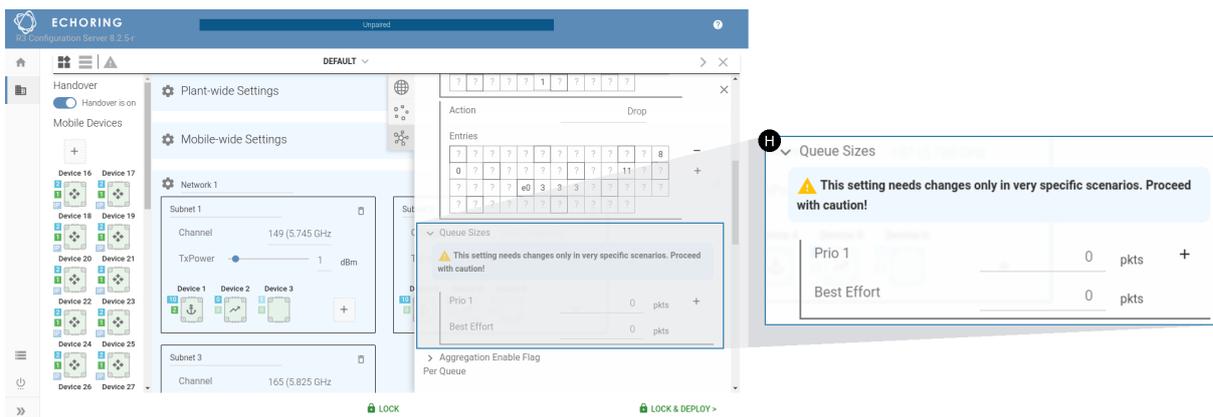
I Aggregation:

The aggregation feature for a queue allows multiple smaller packets to be combined before transmission. Packets are aggregated without fragmentation until either the payload limit is reached or the specified timeout expires. This feature can be enabled or disabled individually for each queue by checking or unchecking the corresponding box. The aggregation timeout, adjustable as a percentage, has to correspond to the desired latency.
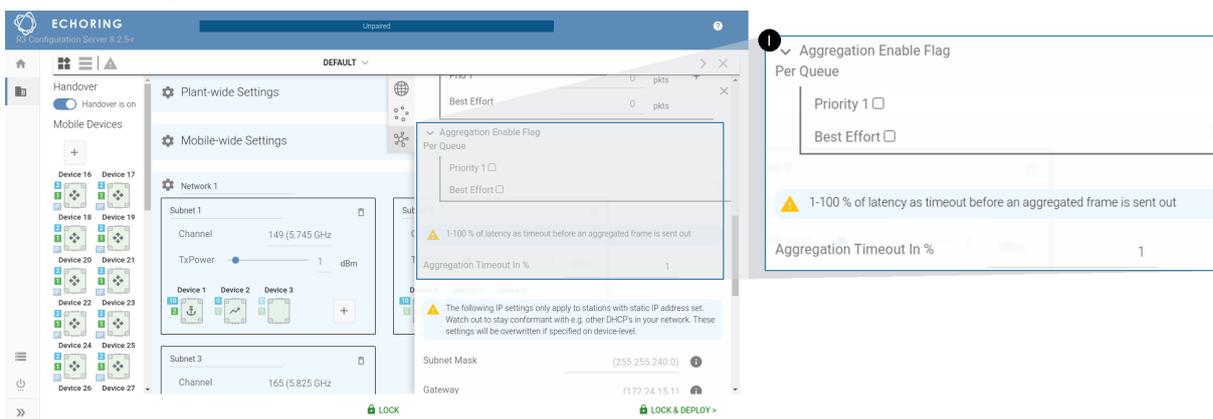
J Subnet Mask, Gateway, Nameserver, Timeserver:

If these settings are specified on network level, they override those from plant-wide settings. If necessary, they can be overwritten on device level. The most specific setting takes precedence.

An IP address needs to be entered to configure the Subnet Mask, Gateway, Nameserver or Timeserver. It is not possible to use an URL to configure it.

Calculated Settings

Given the configured parameters (A) - (E), the timings are calculated and the resulting Target Token Rotation Time and Data Rate are displayed. For explanations of the parameters (A) - (E) check section Basic Settings.

> **i**
>
> **NOTE** — In case the parameters are not feasible, an error message will appear instead of the calculated values. This can be fixed, for example, by increasing the latency to ensure the calculation works and successful deployment can be guaranteed.
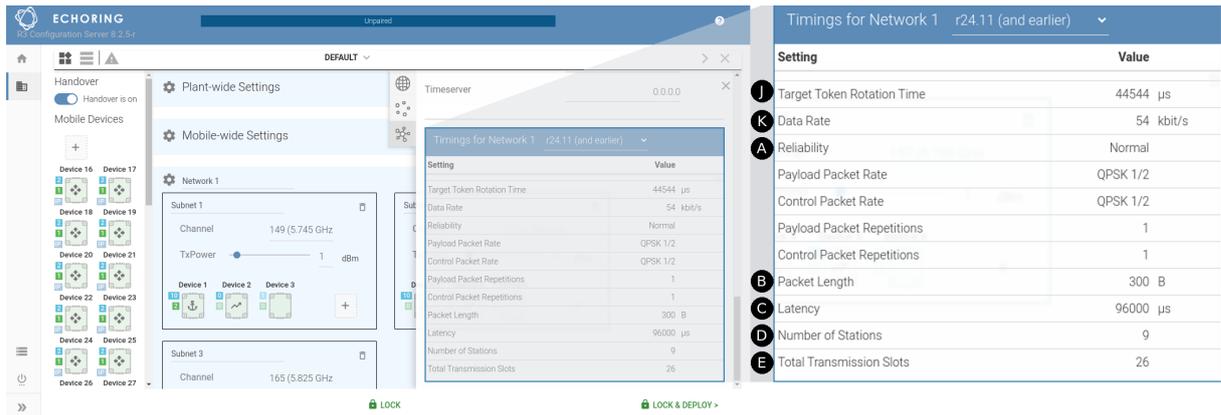
(J) Target Token Rotation Time: the timespan for a station that has transmitted a packet to be allowed to transmit once more.

> **i**
>
> **EXAMPLE** — If the application traffic has a cycle time of 16 ms (whereas packets received later than this may result in an application shutdown), the system should ideally be configured with a Target Token Rotation Time of just below 8ms, allowing for jitter leeway.

> **i**
>
> **NOTE** — For more background information on EchoRing, please visit our website.

(K) Data Rate: Shows the System Data Rate in kbit/s (provided above the MAC layer) achieved by the configuration. This is the minimum, deterministically assigned, guaranteed data rate at maximum utilization of the system.

5.2.4 Subnetwork Settings

The different subnetworks can be configured.
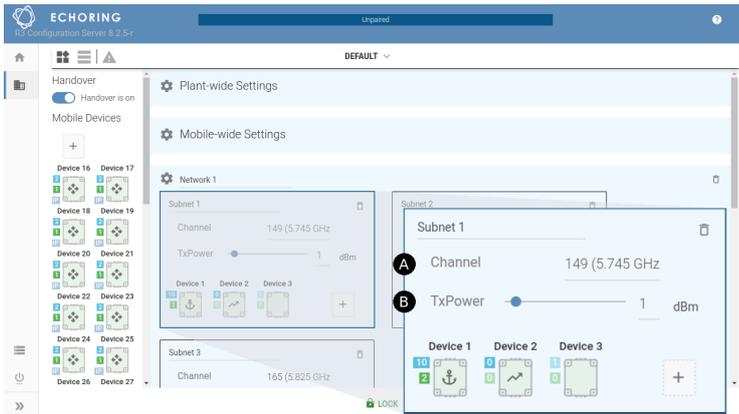
> **TIP** — To prevent interference, please ensure that other/external radio transmitting devices in the vicinity of the network are not operating on the selected frequency.

(A) Channel: the network's radio frequency to operate on.

(B) TxPower: each device's transmitting power.

Static Stations can be added to a subnetwork by clicking on the "+"-symbol. Left-click to add one station, right-click to add several stations at once.
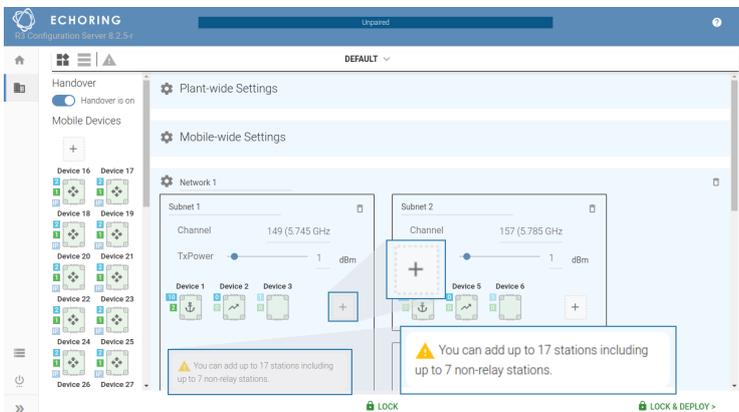
> **NOTE** — The maximum number of Channels is 3 for all subnetworks in a network.
> The maximum number of devices in a subnetwork is 20.
> The maximum number of all devices in a plant is 239.

Added devices can be deleted by hovering over the device and clicking the trash bin twice. The trash bin will turn red after the first click. Same applies to deleting subnetworks and networks.

When a subnetwork containing devices is deleted, the outcome depends on the handover toggle. If handover is enabled, the devices are transferred to the Mobile Devices. If handover is disabled, the devices are permanently deleted after confirmation.
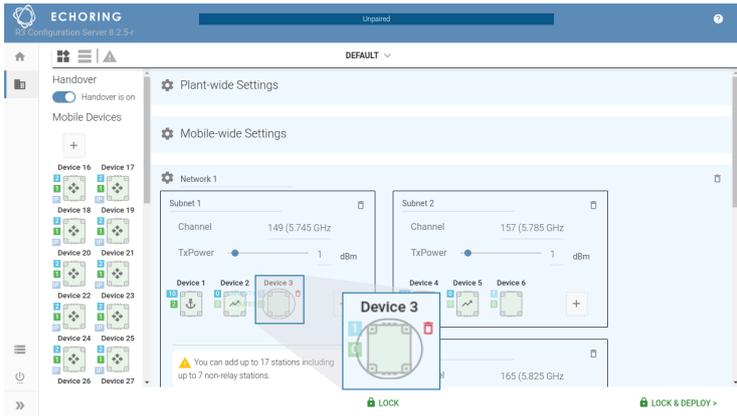
5.2.5 Device Settings

Click on a specific device to configure it individually.
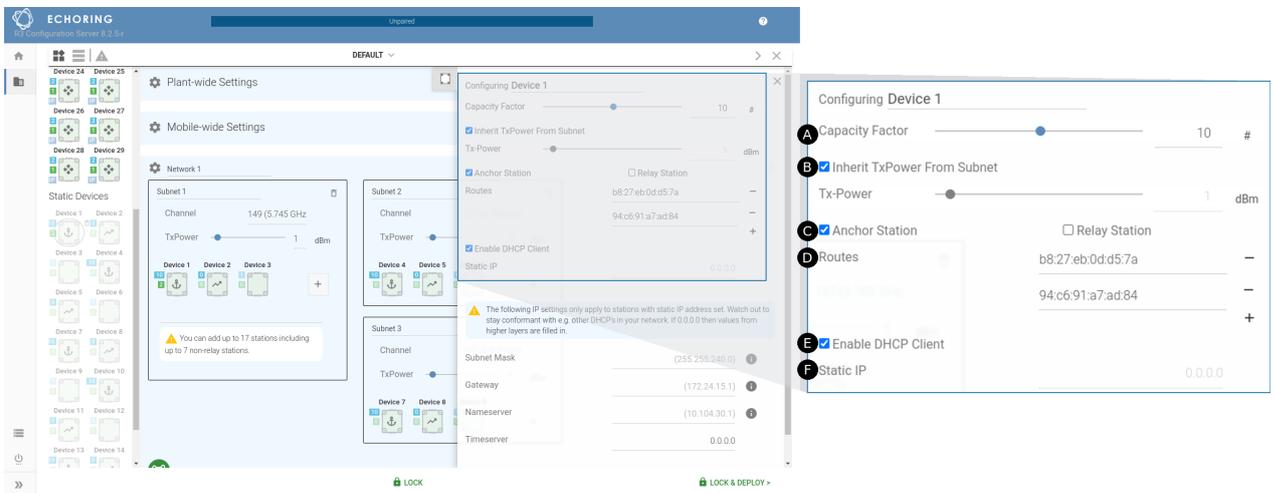
(A) Capacity Factor: configures the number of transmission slots used for the selected device, allowing for greater data throughput or asymmetric traffic per device. The sum for all devices in this subnetwork is limited by the overall subnetwork capacity (see (E) Total Transmission Slots).

> 💡 **TIP** — To determine the required capacity factor for each device, analyze the traffic and corresponding data rate that each device transmits, in relation to all devices in the subnetwork. Then distribute the capacity factors accordingly.

(B) Inherit TxPower From Subnet: if checkbox is selected, TxPower is inherited from the subnetwork settings. If the box is deselected, the value initially remains that of the subnetwork, but can be changed individually for the respective device using the slider.

(C) Anchor Station or Relay Station (or neither):

- An Anchor Station is the central station for a subnetwork. It is connected to a shared network with all Anchor Stations of other subnetworks within the network for signaling.

- External Relay Stations increase the reliability. They do not consume or block (temporal) resources in the subnetwork, but support data exchange between other Bridge E devices. Thus they have a capacity factor of zero. Currently only one Relay Station per subnetwork is supported.

D Routes: Allows to statically assign the MAC address of one or more customer network components that are to be connected to the Bridge E.

The introduction of the MAC learning feature in r24.05 enhances this process by dynamically learning and storing MAC addresses, thereby automating part of the routing management. The system initially broadcasts the first few packets to discover the MAC addresses of connected devices. Once a MAC address is captured, it is stored in a table, enabling the system to directly route packets to these addresses in future communications.

> **NOTE** — Be aware of the table's capacity, which can hold a maximum of 200 entries. This includes both manually set routes and dynamically learned addresses.

E Enable DHCP Client: The device should obtain its IP from a DHCP server.

F Static IP: If DHCP is disabled, this static IP will be the device's IP address.

> **TIP** — When using static IP, other settings such as Subnet Mask, Gateway, Nameserver and Timeserver should also be configured.

> **NOTE** — If **D** DHCP is enabled, **E** Static IP is automatically disabled and vice versa.

G Subnet Mask, Gateway, Nameserver, Timeserver:

If these settings are specified on device level, they override those from network and -wide settings. If not, they are inherited from higher level(s).

An IP address needs to be entered to configure the Subnet Mask, Gateway, Nameserver or Timeserver. It is not possible to use an URL to configure it.

5.2.6 Make Configuration Deployable

> **NOTE** — Applying a configuration with warnings is possible, but errors must be solved first.

Click on the warning sign in the top bar to display warnings and errors. Click on a warning or error to open the settings where the warning originates.

When getting a warning, yet confident that the actions taken are correct and intentional, one may choose to dismiss the warning to prevent distraction. This can be accomplished by clicking on the "x" icon next to the warning. Once dismissed, these warnings are relocated to the "dismissed" tab. From there, they can be reinstated by clicking the eye icon causing them to reappear in the error/warning list.

> **TIP** — How to avoid warnings:
> If there is more than one subnetwork per network or Mobile Stations are required, Handover is needed. In that case, there has to be an Anchor Station configured in each subnetwork!
> The number of stations must be lower than configured in Step 5.2.3.
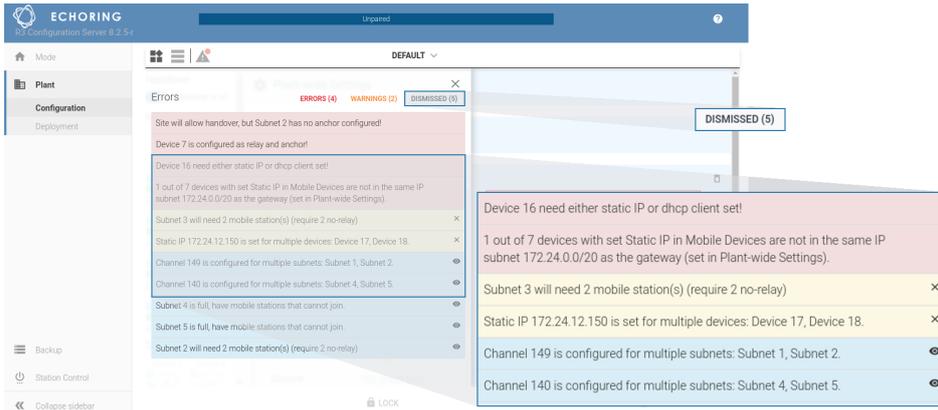
When there are no errors displayed, the "Lock & Deploy" button on the bottom right will be green.
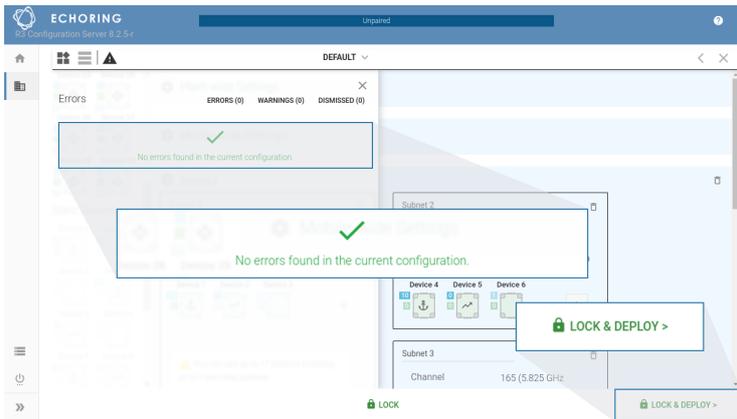
5.3 Deployment

1. Click on "Lock & Deploy" to access the "Deployment" page.
   All the deployable devices are listed on the right. Use the dropdown menu to select a searching/-sorting criteria (MAC/IP/Name).
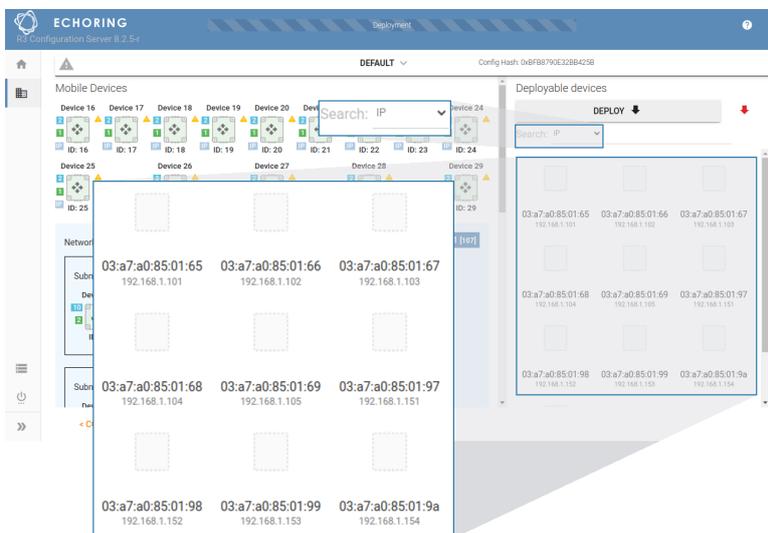
> **NOTE** — If the target latency cannot be met, an error message 'failed to validate MAC setting' will be raised.

2. When the configuration changed, outdated devices will have a yellow update symbol next to them. Click "Deploy" or drag and drop the device to the MAC/IP on the right. The updated devices will have a green check mark.
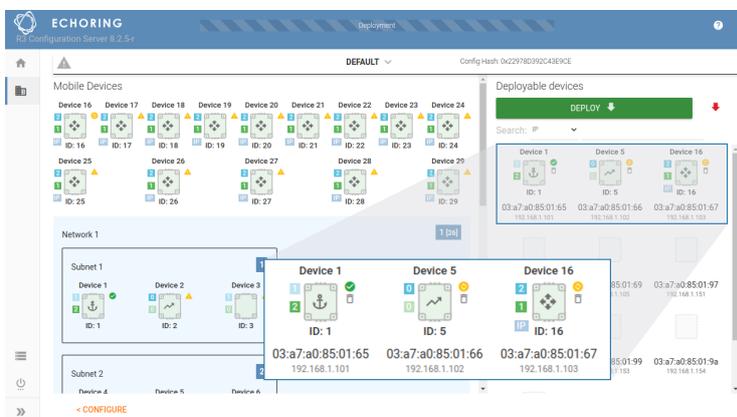
> **TIP** — When you click "Deploy", only devices with a yellow symbol will be updated. When you click the green button next to deploy, the configuration will be sent to all devices, including the ones that already have a green check mark.

3. Click on a device in the list of deployable devices to open its settings.

> **TIP** — If the application's data rate exceeds the maximum throughput limited by the other set configuration parameters, the system overloads and the packets risk being dropped, leading to packet losses. If application has combined traffic of both critical and best-effort, the setting Prioritized Traffic filter ((F)) allows a type of traffic to be prioritized and the other to be transmitted secondly (bearing eventual packet losses).
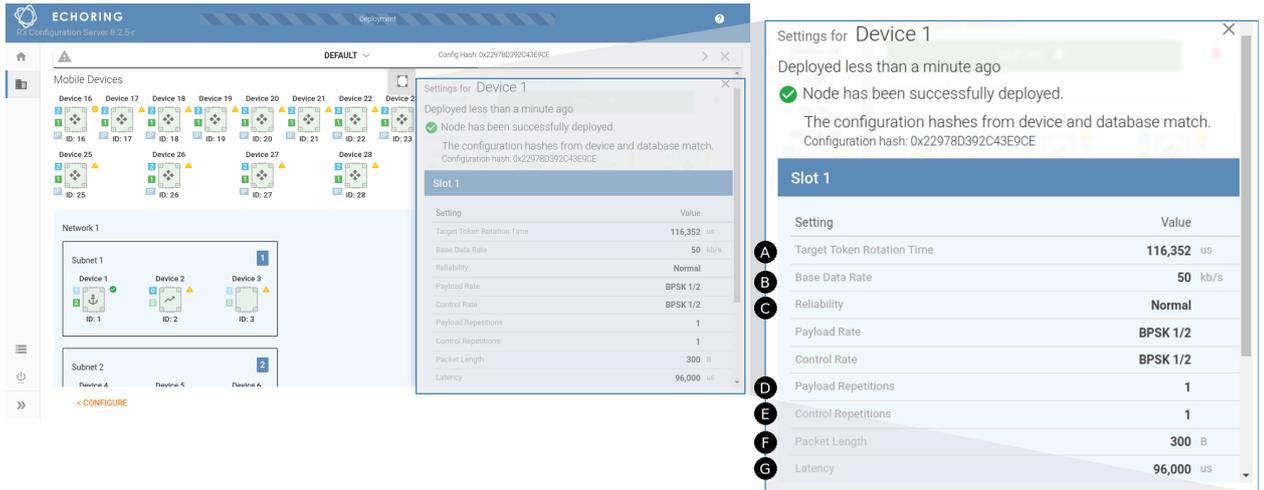
4. The configuration is locked during deployment to prevent corruption of the configuration data set.
   Choose either to continue the deployment or to unlock the configuration.

> ℹ️ **NOTE** — If you choose to unlock the configuration, the configuration deployment will stop.

> ℹ️ **NOTE** — Note that by choosing to change the configuration parameters, the entire network (including stations that were deployed earlier) will need to be redeployed.

5. The deployment process cannot be started while the configuration is unlocked, so finish modifying the configuration first. Then click on "Lock" and redeploy all devices.

6. After deployment, the Bridge E should be disconnected from the common switch to avoid creating a bridging loop.

5.3.1 Control Device during Runtime

To control the device during runtime, the "Station Control" offers a range of ERCI commands. A detailed description of those commands can be found in Section 8.2.
For example, to change the configuration of a device in Deployment Mode, the device needs to return to Configuration Mode first.
To do so, open "Station Control", type in the IP address of the device, click "Select Command", choose "Set Config Flag" and then click "Run Command". The device will go into Configuration Mode when booting the next time.

5.4 Save and Restore Database

The left-hand menu contains the "Backup" section, where the database can be saved and restored. The database contains all adjustments made in the Plant Configuration.
The current database can be downloaded using "Export".
A previously saved database can be uploaded using "Import".

> **ATTENTION** — All previous settings will be **overwritten** when you import a database. ⚠️
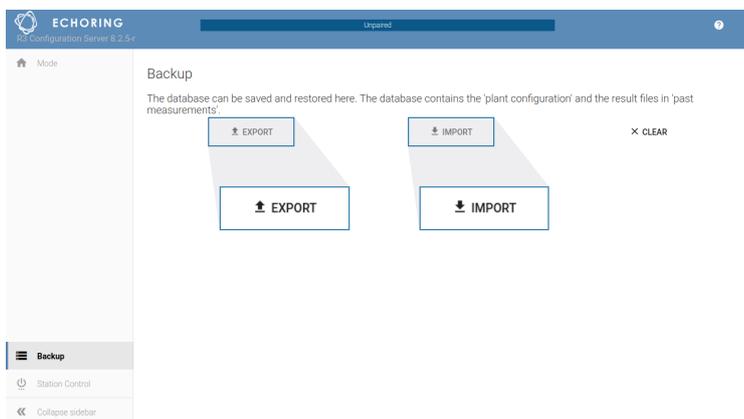
6 Troubleshooting

6.1 Device Not Showing Up

If the devices do not show up on the web user interface, one of the following messages may be displayed under the "Update Devices" box:

- Unreachable Testbeds: These devices could not be discovered by the Configuration Server for roughly 20 seconds.

- Elsewhere Paired Testbeds: The devices shown in this section are reporting that they are already paired.

- Mismatching Testbeds: These devices are not compatible with the Configuration Server in any of the core functions (Configuration or Update).
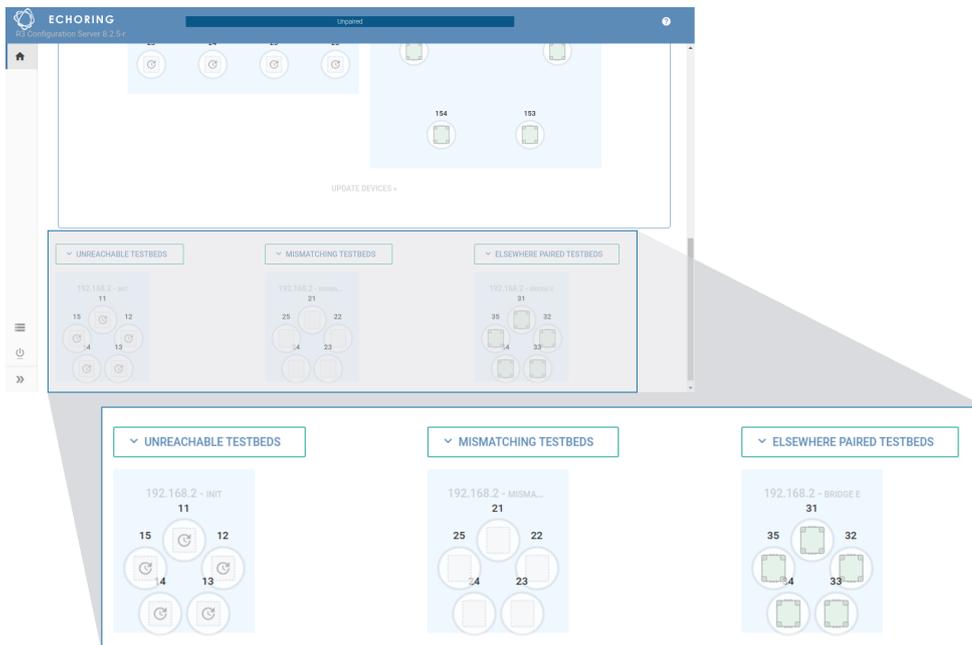
Mismatching Testbeds

If none of the subprotcols are compatible with the corresponding Configuration Server subprotocol versions for a device, the device will be shown in the "Mismatching Testbeds".
To check the exact version numbers of the subprotocols, go to "Station Control" in the bottom left-hand corner and click on the speech bubbles icon in the upper-hand right corner.
The subprotocol version numbers from both server (first line) and stations (more below) will be shown.
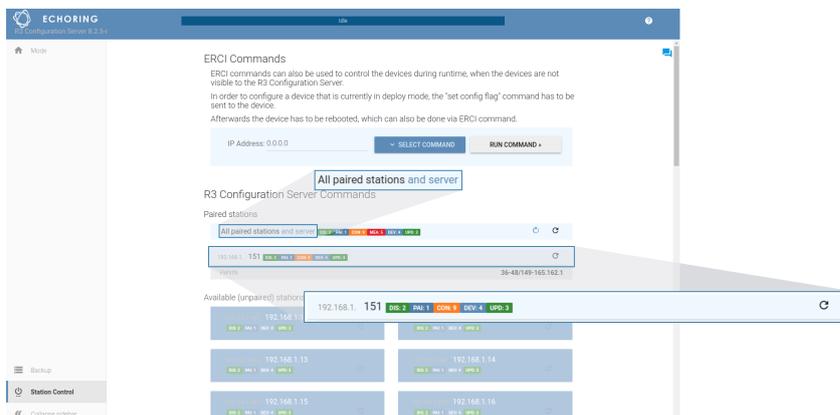
The version numbers on the labels must be the same, so that the Configuration Server and the devices can communicate in the domain concerned.

> **EXAMPLE** — If the server displays "CON: 8" then only Bridge E devices that have the same subprotocol version numbers, also indicated with "CON: 8", can be configured.

If the subprotocol version from the device is not compatible with the Configuration Server, the information is grayed out, so here "CON: 5" would appear with gray background.

> **INFO** — To configure an Bridge E, it needs to use the same configuration subprotocol (CON) version as the Configuration Server.
> To update an Bridge E, it needs to use the same update subprotocol (UPD) version as the Configuration Server.

IGMP Snooping Problem

If no devices are discovered and the network is working properly, try checking if multicast is working as intended. Not all switches support IGMP Snooping, so turning it off on all switches may solve the issue.

> **TIP** — We recommend to use the Netgear GS308E-100PES switch as it has been tested and works with it. The use of other switches is at your own risk.

6.2 Different Regularity Domains

The regulatory domain is used to indicate the area where Bridge E devices are used, and to enforce the regulatories for that domain because different laws apply in different parts of the world.

If you see the error message "The used regulatory domain of the R3 Configuration Server and the database do not match", this means that the Configuration Server and the database file are from different regulatory domains.

This problem can be solved by changing either the regulatory domain of the Configuration Server or of the database. Please contact your Application Engineering representative.

7 Customer Service and Addresses

Customer Service

For technical inquiries, our service is available.

R3 Customer Service
Contact form: www.r3.group/contact
Email: service@r3.group

R3 Solutions GmbH
Kurfürstendamm 21
D-10719 Berlin
Phone: +49 30 800 936 75
Email: contact@r3.group

Further addresses for sales and service locations can be found at:
www.r3.group

8 Appendix

8.1 Reliability/MCS Table

The reliability influences the chosen Modulation Coding Scheme (MCS) as well as how many repetitions for data (Payload Repetitions) and token (Control Repetitions) are being used.

Reliability Level	Payload Rate	Control Rate	Payload Repetitions	Control Repetitions
None	QAM16 3/4	QAM16 3/4	1	1
Low	QAM16 1/2	QAM16 1/2	1	1
Moderate	QPSK 3/4	QPSK 3/4	1	1
Normal	QPSK 1/2	QPSK 1/2 1	1	1
Advanced	BPSK 3/4	BPSK 3/4	1	1
High	BPSK 1/2	BPSK 1/2	1	1
Critical	BPSK 1/2	BPSK 1/2	2	1
Extreme	BPSK 1/2	BPSK 1/2	2	2

8.2 ERCI Specification

ERCI is the control interface for the Bridge E during runtime.

> **INFO** — The Application Engineering Team can provide 'function block' examples to integrate ERCI functionality to different automation environments. See here for the contact information. ⓘ

Mode of Operation

The devices communicate using the User Datagram Protocol (UDP).
All configuration data will be pre-deployed using the Configuration Server.
Until EchoRing is started, all "Switch Ring" and "Switch Antenna" commands are invalid and an error will be returned.

Initialization

If the configuration of a Bridge E only consists of a single network with a single subnetwork, the configuration is auto deployed and the Medium Access Control (MAC) started for Static Stations. This is not the case for Mobile Stations.
Otherwise the Bridge E waits for input via ERCI to select the active configuration and another ERCI command to start the MAC. The ERCI client listens on port 12200.

Message Header

Field	Size (B)	Comment
-	1	[Reserved] Value: 0
Protocol Version	1	Value: 3
Type	1	
Sequence number	1	
Payload	n	

Messages

Byte Index	0	1	2	3
	0x00	Version	Type	Payload

| fixed | **Version**
0x03 fix | **Type**
0x00: Invalid
0x01: Select Configuration
0x02: Switch Ring
0x03: Start
0x04: Stop
0x05: Command Result

0x06: State Query
0x07: State Response

0x08: Diagnostic Description Query
0x09: Diagnostic Description Response

0xA: Switch Antenna
0xB: Set Config Mode

0xC: Query Passport
0xD: Query Passport Response

0xE-0x7F: Not used
0x80-0xFF: Reserved | **Payload**
depends on message type, see message table |

Value	Message Type	Payload	Response	Command Result Code	Comment
0	Invalid				
1	Select Con-figuration	1B Config ID, 1B Ring ID, 1B Antenna ID	Command Result	Success → Config applied Invalid Message Received → Wrong format Wrong State → Not in READY or CONFIGURED No Config Available → No configs at all are stored Invalid Data Received → Invalid config, ring and/or antenna id Generic Error → Error in processing request	Only in READY or CONFIGURED state. If provided config is invalid or unknown, (config ID and/or ring ID and/or antenna ID) will reset any loaded config (if present) and go to READY
2	Switch Ring	1B Ring ID, 1B Antenna ID	Command Result	Success → Switch ring executed Invalid Message Received → Wrong format Wrong State → Not in RUNNING Invalid Data Received → Invalid ring and/or antenna ID Generic Error → Error in processing request	Only in RUNNING state
3	Start	1B Ring ID	Command Result	Success → Start executed Invalid Message Received → Wrong format Wrong State → Not in CONFIGURED Generic Error → Error in processing request	Only in CONFIGURED state
4	Stop		Command Result	Success → Stop executed Invalid Message Received → Wrong format Wrong State → Not in RUNNING Generic Error → Error in processing request	Only in RUNNING state, resets Config ID, Ring ID and Antenna ID to 0 (=invalid)
5	Command Result	1B Command Result Code, NULL terminated result description	-		

Value	Message Type	Payload	Response	Command Result Code	Comment
6	State Query		State Response		Allowed in any state
7	State Response	1B State, 1B Config ID, 1B Ring ID, 1B Antenna ID	-		Returns State, Configuration ID, and Ring ID
8	Diagnostic Description Query		Diagnostic Description Response		Allowed in any state request ASCII system diagnostics
9	Diagnostic Description Response	NULL terminated diagnostic description			ASCII text representation of system diagnostics
10	Switch Antenna	1B Antenna ID	Command Result	Success → Switch antenna executed Invalid Message Received → Wrong format Wrong State → Not in RUNNING Invalid Data Received → Invalid antenna ID Generic Error → Error in processing request	Only in RUNNING state
11	Set Config Mode	1B 0: disabled 1: enabled other: invalid	Command Result	Success → Config flag set or cleared Invalid Message Received → Wrong format Generic Error → Error in processing request	
12	Query Passport	6B assumed MAC of device, 26B assumed Serial Number (SN) of device	Query Passport Response		Allowed in any state
13	Query Passport Response	1B Command Result, 6B MAC address stored in passport (PP), 26B Serial Number stored in passport		Success → Provided SN & PP MAC matches stored information in bootloader, query was successful Invalid Data Received → Provided SN and/or PP MAC do NOT match stored information in bootloader Invalid Msg Received → "Query Passport" message wrong size → Failed to parse "Query Passport" message Generic Error → Provided SN & PP MAC matches stored information in bootloader, query was NOT successful	
14..127					Not used yet
128..255					Reserved

Command Result Codes

Value	Result
0..64	[Reserved]
65	Success
66..69	[Reserved]
70	Generic Error
71	Wrong State
72	Invalid Message Received
73	Invalid Data Received
74	No Config Available

State Machine

State	Value	Description
INVALID	0	Values of zero are invalid.
STARTUP	1	The device is still booting up.
READY	2	The device is ready to be configured.
RUNNING	3	Bridging over EchoRing is operational.
RECONFIGURING	4	The device is reconfiguring.
FAULT	5	The device is in an unrecoverable fault state and needs to be reset.
MAINTENANCE	6	The device is busy with other activities (i.e. updating, Configuration Mode, ...).
CONFIGURED	7	The device has been configured and is ready to be started (or reconfigured).

State Diagram
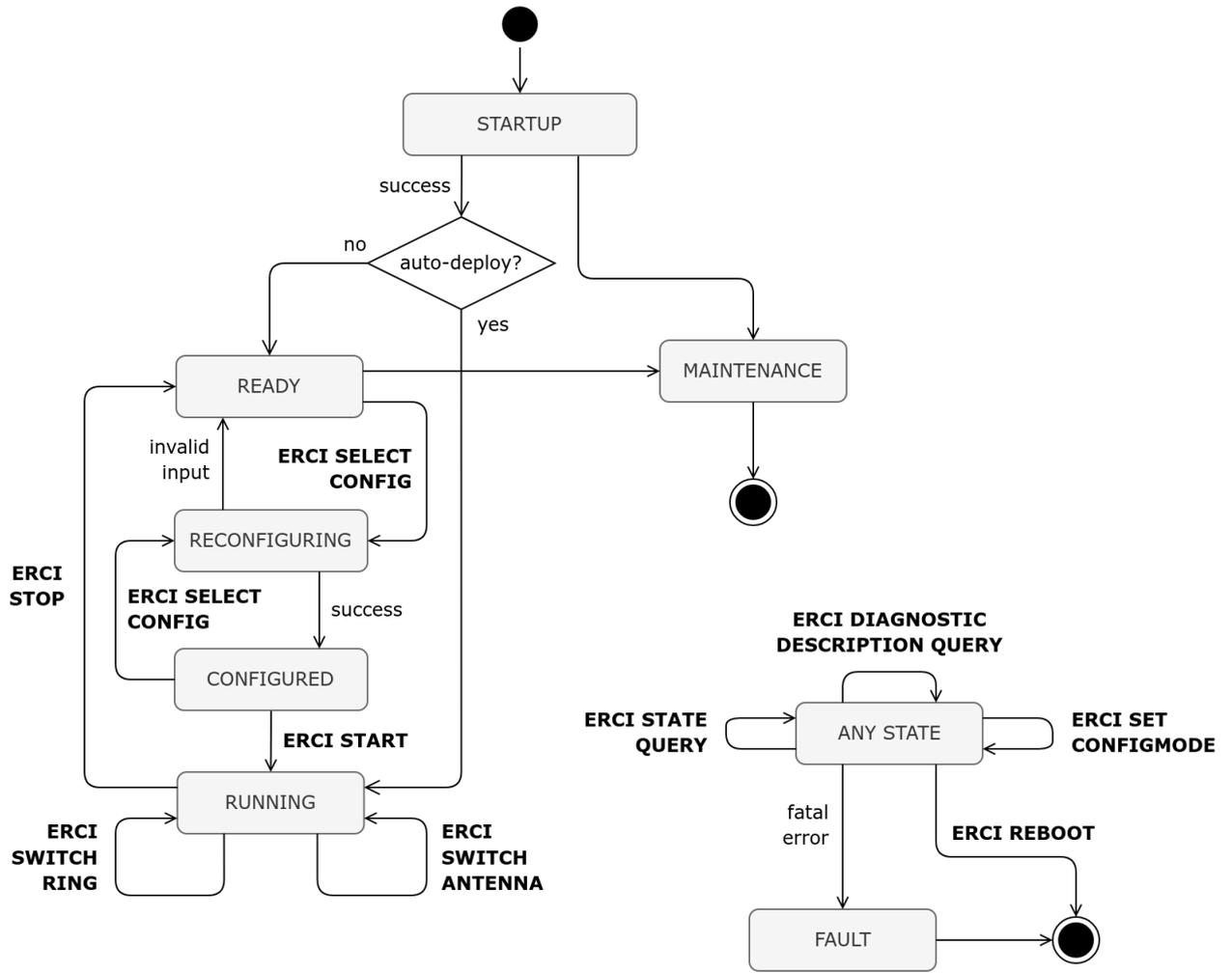
8.3 Product Change Notification
Product Change Notification Form 1

PN #: PCN-E-001	**Rev:** 1.0	**Issue Date:** 18-Aug-2022

Type of Change

☒ minor   ☐ major

Detailed description of change

Product name changes to Bridge E.

Resulting changes in code marking and changes in its face plate label are documented in Exhibit 1.

Exhibit 2 summarizes all code marketings for this product that are still valid.

Quality Impact

☐ minor   ☐ major   ☒ none

Reliability Impact

☐ minor   ☐ major   ☒ none

Reason for change

As the product portfolio of R3 Solutions grows, new product names are necessary to differentiate product families better.

Implementation date

18-AUG-2022

Contact details

R3 Customer Service

service@r3.group

Affected part number(s)

ER-EB 1000M

PCN-E-001 Exhibit 1

New Code Marking (Label)
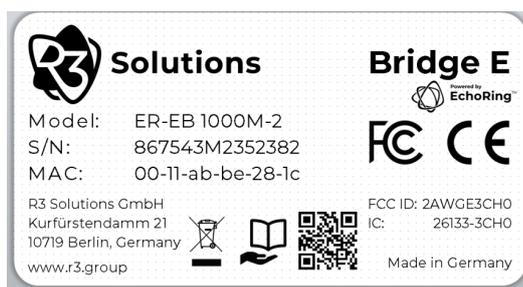
Face Plant Print
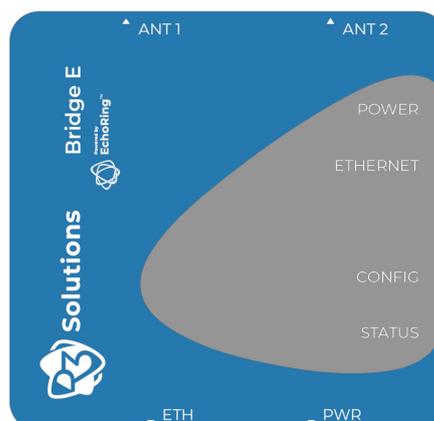
PCN-E-001 Exhibit 2

Existing Code Marking 1

Existing Code Marking 2

Existing Code Marking 3

Existing Code Marking 4

Product Change Notification Form 2

PN #: PCN-E-002	**Rev:** 1.0	**Issue Date:** 20-Aug-2022

Type of Change

☒ minor   ☐ major

Detailed description of change

The product is now equipped with an additional antenna port. The product uses only one of the two ports at any given time and can be operated either with only one antenna connected or two antennas connected.

The product package now includes one Bridge E device, one antenna, and one IP65-compatible lid to seal an antenna port if not in use.

Code marking and label changes are documented in the appendix.

Quality Impact

☒ minor   ☐ major   ☐ none

Reliability Impact

☒ minor   ☐ major   ☐ none

Reason for change

The extra antenna port on the product now supports roaming between different channels.

Implementation date

20-AUG-2022

Contact details

R3 Customer Service

service@r3.group

Affected part number(s)

ER-EB 1000M-2 (formerly ER-EB 1000M)

PCN-E-002 Exhibit 1

New Code Marking (Label)

Face Plant Print

List of Acronyms

UM-ER-EB1000M-r24.11