Draft

Nokia WiFi Beacon

Beacon 19

Beacon 19 Product Guide

3TN-00789-AAAA-TCZZA
Issue 1
September 2024

Draft

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Contents

Draft

List of tables

Draft

List of figures

Draft

About this document

Purpose

This documentation set provides information about safety, features and functionality, ordering, hardware installation and maintenance, and software installation procedures for the current release.

Intended audience

This documentation set is intended for planners, administrators, operators, and maintenance personnel involved in installing, upgrading, or maintaining the Nokia WiFi Beacon.

The reader must be familiar with general telecommunications principles.

Safety information

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

Safety Information Examples

DANGER

Hazard

Danger indicates that the described activity or situation may result in serious personal injury or death; for example, high voltage or electric shock hazards.

WARNING

Equipment Damage

Warning indicates that the described activity or situation may, or will, cause equipment damage or serious performance problems.

CAUTION

Service Disruption

Caution indicates that the described activity or situation may, or will, cause service interruption.

Note: A note provides information that is, or may be, of special interest.

Acronyms and initialisms

The expansions and optional descriptions of most acronyms and initialisms appear in the glossary

Nokia quality processes

Nokia's WiFi Beacon manufacturing, testing, and inspecting practices are in compliance with TL 9000 requirements. These requirements are documented in the Fixed Networks Quality Manual 3FQ-30146-6000-QRZZA.

The quality practices adequately ensure that technical requirements and customer end-point requirements are met. The customer or its representatives may be allowed to perform on-site quality surveillance audits, as agreed upon during contract negotiations.

Documents

Documents are available using ALED or OLCS.

To download a ZIP file package of the customer documentation

1. Navigate to http://customer.nokia.com/s/ and enter your user name and password. If you are a new user and require access to this service, contact your Nokia sales representative.
2. Select **Products**.
3. Type your product name in the **Find and select a product** field and click the search icon. Select a product.
4. Click **Downloads: ALED** to go to the Electronic Delivery: Downloads page.
5. Select **Documentation** from the list.
6. Select a release from the list.
7. Follow the on-screen directions to download the file.

END OF STEPS

To access individual documents

Individual PDFs of customer documents are also accessible through the Nokia Support Portal website.

1

Navigate to http://customer.nokia.com/s/ and enter your user name and password. If you are a new user and require access to this service, contact your Nokia sales representative.

2

Select **Products**.

3

Type your product name in the **Find and select a product** field and click the search icon. Select a product.

4

Click **Documentation: Doc Center** to go to the product page in the Doc Center.

5

Select a release from the **Release** list and click **SEARCH**.

6

Click on the PDF icon to open or Save the file.

END OF STEPS

Procedures with options or substeps

When there are options in a procedure, they are identified by letters. When there are required substeps in a procedure, they are identified by roman numerals.

Example of options in a procedure

At Step 1, you can choose option a or b. At Step 2, you must do what the step indicates.

1

This step offers two options. You must choose one of the following:

a. This is one option.

b. This is another option.

2

You must perform this step.

END OF STEPS

Example of required substeps in a procedure

At Step 1, you must perform a series of substeps within a step. At Step 2, you must do what the step indicates.

Draft

1

This step has a series of substeps that you must perform to complete the step. You must perform the following substeps:

a. This is the first substep.

b. This is the second substep.

c. This is the third substep.

2

You must perform this step.

END OF STEPS

Multiple PDF document search

You can use Adobe Reader Release 6.0 and later to search multiple PDF files for a common term. Adobe Reader displays the results in a single display panel. The results are grouped by PDF file, and you can expand the entry for each file.

Note: The PDF files in which you search must be in the same folder.

To search multiple PDF files for a common term

1

Open Adobe Acrobat Reader.

2

Choose **Edit→Search** from the Acrobat Reader main menu. The Search PDF panel displays.

3

Enter the search criteria.

4

Select **All PDF Documents In**.

5

Select the folder in which to search using the drop-down menu.

6

Click **Search**.

Acrobat Reader displays the search results. You can expand the entries for each document by clicking on the + symbol.

END OF STEPS

Technical support

For details, refer to the Nokia Support portal (https://customer.nokia.com/support/s/).

For ordering information, contact your Nokia sales representative.

How to comment

Note to reviewers: The following "How to comment" text will appear in the final document when it is published. However, the feedback method described below is for use only on final documents. Please send your review comments to the author using the process you were given when you received this draft document.

To comment on this document, go to the Online Comment Form (https://documentation.nokia.com/comments/) or e-mail your comments to the Comments Hotline (mailto:comments@nokia.com).

1 What's new

1.1 Overview

1.1.1 Purpose

This chapter provides the details of features and other documentation changes updated in the product guide in each release.

1.1.2 Contents

1.2 What's new in BBD Release 24.03

The Product guide is a new guide in BBD Release 24.03, issue 1. In future releases, this chapter will provide tables of the feature and document changes applicable to this guide.

Draft

2 ANSI CPE safety guidelines

2.1 Overview

2.1.1 Purpose

This chapter provides information about the mandatory regulations that govern the installation and operation of devices in the North American or ANSI market.

2.1.2 Contents

2.2 Safety instructions

This section describes the safety instructions that are provided in the CPE customer documentation and on the equipment.

2.2.1 Safety instruction boxes in customer documentation

The safety instruction boxes are provided in the CPE customer documentation. Observe the instructions to meet safety requirements.

The following is an example of the Danger box.

DANGER

Hazard

Possibility of personal injury.

The Danger box indicates that the described activity or situation may pose a threat to personal safety. It calls attention to a situation or procedure which, if not correctly performed or adhered to, may result in death or serious physical harm.

Do not proceed beyond a Danger box until the indicated conditions are fully understood and met.

The following is an example of the Warning box.

WARNING

Equipment Damage

Possibility of equipment damage.

Possibility of data loss.

The Warning box indicates that the described activity or situation may, or will, cause equipment damage, loss of data, or serious performance problems. It identifies a possible equipment-damaging situation or provides essential information to avoid the degradation of system operations or data.

Do not proceed beyond a warning until the indicated conditions are fully understood and met.

The following is an example of the Caution box.

CAUTION

Service Disruption

Possibility of service interruption.

Service interruption.

The Caution box indicates that the described activity or situation may, or will, cause service interruption.

Do not proceed beyond a caution until the indicated conditions are fully understood and met.

The following is an example of the Note box.

Note: Information of special interest.

The Note box provides information that assists the personnel working with devices. It does not provide safety-related instructions.

2.2.2 Safety-related labels

The customer premises equipment is labeled with specific safety compliance information and instructions that are related to a variant of the CPE. Observe the instructions on the safety labels.

Table 2-1, “Safety labels” (p. 22) provides examples of the text in the various CPE safety labels.

Table 2-1 Safety labels

Label text	Description
ETL compliance	Communication service equipment US listed.
ESD warning	Caution: This assembly contains electrostatic sensitive device.
FCC standards compliance	Tested to comply with FCC standards for home or office use.

Figure 2-1, “Sample safety label” (p. 23) shows a sample safety label located on the bottom of the Beacon 19.

Figure 2-1 Sample safety label

Draft

Figure 2-2 Sample safety label - US

Figure 2-3 Sample safety label - CA

2.3 Safety standards compliance

This section describes the CPE compliance with North American safety standards.

WARNING

Equipment Damage

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

2.3.1 FCC/ ISED warning

This section describes the FCC warning.

WARNING

Equipment Damage

FCC regulations restrict the operation of this device to indoor use only.

The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet in the 5.925-6.425 GHz band.

Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence- 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.

ISED warning

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.

The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Les dispositifs fonctionnan+D9t dans la bande de 5150 à 5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

1. Operation shall be limited to indoor use only.
2. Operation on oil platforms, automobiles, trains, maritime vessels and aircraft shall be prohibited except for on large aircraft flying above 3,048 m (10,000 ft).

1. leur utilisation doit être limitée à l'intérieur seulement;
2. leur utilisation à bord de plateformes de forage pétrolier, d'automobiles, de trains, de navires maritimes et d'aéronefs doit être interdite, sauf à bord d'un gros aéronef volant à plus de 3 048 m (10 000 pi) d'altitude.

This equipment complies with Innovation, Science and Economic Development Canada RF exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated to ensure a minimum of 31cm spacing to any person at all times.

Cet équipement est conforme aux limites d'exposition RF d'Innovation, Science et Développement économique Canada établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé de manière à assurer un espacement d'au moins 31cm avec toute personne en tout temps.

2.3.2 EMC, EMI, and ESD standards compliance

The customer premises equipment complies with the following requirements:

- Federal Communications Commission (FCC) CFR 47, Part 15, Subpart B, Class B requirements for 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 is 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 needed.
- Consult the dealer or an experienced radio/TV technician for help.

2.3.3 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the Beacon 19 devices are in compliance with the essential requirements and other relevant provisions of Directive 2009/125/EC together with Commission Regulation (EC) No 1275/2008 and Commission Regulation (EC) No 801/2013.

The Beacon 19 devices qualify as high network availability (HiNA) equipment. Since the main purpose of Beacon 19 devices is to provide network functionality with HiNA 7 days/24 hours, the modes Off/Standby, Power Management, and Networked Standby are inappropriate.

For information about the type and number of network ports, see 5.5 “Beacon 19 interfaces and interface capacity” (p. 44) in Chapter 5, “Beacon 19 unit data sheet”.

For information about power consumption, see 5.7 “Beacon 19 detailed specifications” (p. 47) in Chapter 5, “Beacon 19 unit data sheet”.

2.3.4 FCC statement

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 is 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.

2.3.5 FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 31 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and consider removing the no-collocation statement.

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, and
2. this device must accept any interference received, including interference that may cause undesired operation.

CAUTION

Service Disruption

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

2.3.6 Resistibility requirements compliance

The customer premises equipment complies with the requirements of ITU Recommendation K.21 for resistibility of telecommunication equipment installed in customer premises to overvoltage and overcurrents.

2.4 Electrical safety guidelines

This section provides the electrical safety guidelines for the customer premises equipment.

Beacon 19 devices are compliant with the following standards

- IEC-62368-1
- UL-62368-1

Note: The devices comply with the U.S. National Electrical Code. However, local electrical authorities have jurisdiction when there are differences between the local and U.S. standards.

2.4.1 Power supplies

The use of any non-Nokia approved power supplies or power adapters is not supported or endorsed by Nokia. Such use will void any warranty or support contract with Nokia. Such use greatly increases the danger of damage to equipment or property.

2.4.2 Cabling

The following are the guidelines regarding cables used for the customer premises equipment:

- Use only cables approved by the relevant national electrical code.

3 ETSI CPE safety guidelines

3.1 Overview

3.1.1 Purpose

This chapter provides information about the mandatory regulations that govern the installation and operation of devices.

3.1.2 Contents

3.2 Safety instructions

This section describes the safety instructions that are provided in the CPE customer documentation and on the equipment.

3.2.1 Safety instructions

The safety instructions are provided in the customer documentation. Observe the instructions to meet safety requirements.

The following is an example of the Danger instruction.

DANGER

Hazard

Possibility of personal injury.

The Danger instruction indicates that the described activity or situation may pose a threat to personal safety. It calls attention to a situation or procedure which, if not correctly performed or adhered to, may result in death or serious physical harm.

Do not proceed beyond a Danger box until the indicated conditions are fully understood and met.

The following is an example of a Warning instruction.

WARNING

Equipment Damage

Possibility of equipment damage.

Possibility of data loss.

The Warning instruction indicates that the described activity or situation may, or will, cause equipment damage, loss of data, or serious performance problems. It identifies a possible equipment-damaging situation or provides essential information to avoid the degradation of system operations or data.

Do not proceed beyond a warning until the indicated conditions are fully understood and met.

The following is an example of the Caution instruction.

CAUTION

Service Disruption

Possibility of service interruption.

Service interruption.

The Caution instruction indicates that the described activity or situation may, or will, cause service interruption.

Do not proceed beyond a caution until the indicated conditions are fully understood and met.

The following is an example of the Note instruction.

Note: Information of special interest.

The Note box provides information that assists the personnel working with devices. It does not provide safety-related instructions.

3.2.2 Safety-related labels

The WiFi Beacon is labeled with the specific safety instructions and compliance information that is related to a variant of the WiFi Beacon. Observe the instructions on the safety labels.

Table 3-1, “Safety labels” (p. 32) provides sample safety labels.

Table 3-1 Safety labels

Label text	Description
CE marking	Indicates compliance to the European Council Directives including EN60950-1 safety
ESD warning	Caution: This assembly contains an electrostatic sensitive device.

3.3 Safety standards compliance

This section describes the WiFi Beacon compliance with the European safety standards.

3.3.1 EMC, EMI, and ESD compliance

The customer premises equipment complies with the following EMC, EMI, and ESD requirements:

- EN 300-386 V1.6.1: Electromagnetic Compatibility and Radio Spectrum Matters (ERM): Telecommunications Network Equipment; Electromagnetic Compatibility (EMC) requirements; Electrostatic Discharge (ESD) requirements
- EN 301489-1: Electromagnetic Compatibility and Radio Spectrum Matters (ERM): Telecommunications Network Equipment; Electromagnetic Compatibility (EMC) Standard for Radio Equipment and Servcies; part 1: Common Technical Requirements
- EN 301489-17: Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Electromagnetic Compatibility (EMC) Standard for Radio Equipment; Part 17: Specific Conditions for Broadband Data Transmission Systems.
- Radio Equipment Directive (RED) 2014/53/EU (applicable from 13 June 2016)
- EN 55032 (2015): Electromagnetic compatibility of multimedia equipment - Emission Requirements
- EN 55024 (2010): Information Technology Equipment, Immunity Characteristics, limits and methods of measurement
- Electromagnetic Compatibility (EMC) directive 2014/30/EU
- European Council Directive 2004/108/EC
- Low Voltage (LVD) directive 2014/35/EC

3.3.2 Equipment safety standard compliance

The customer premises equipment is labeled with specific safety compliance information and instructions that are related to a variant of the CPE. Observe the instructions on the safety labels.

Table 3-2, “Safety labels” (p. 33) provides examples of the text in the various CPE safety labels.

Table 3-2 Safety labels

Label text	Description
TUV compliance	Type 3R enclosure - Rainproof.
ESD warning	Caution: This assembly contains electrostatic sensitive device.
CDRH compliance	Complies with 21 CFR 1040.10 and 1040.11.
CE marking	There are various CE symbols for CE compliance.
UKCA marking	There is UKCA symbol for UKCA compliance.

The customer premises equipment complies with the requirements of EN 60950-1, Safety of Information Technology Equipment for use in a restricted location.

- ETS 300 019-2-1 Storage Class T1.1
- ETS 300 019-2-2 Transport Class T2.3
- ETS 300 019-2-3 Stationary Class T3.2

3.3.3 Environmental standard compliance

The customer premises equipment complies with the EN 300 019 European environmental standards.

3.3.4 CE RED RF Radiation Exposure Statement

This device complies with CE RED radiation exposure limits set forth for an uncontrolled environment. To comply with CE RED RF exposure compliance requirements, this grant is applicable only for mobile configurations. The antennas used for the transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

3.3.5 Resistibility requirements compliance

The customer premises equipment complies with the requirements of ITU Recommendation K.21 for resistibility of telecommunication equipment installed in customer premises to over voltage and overcurrents.

3.3.6 Acoustic noise emission standard compliance

The customer premises equipment complies with EN 300 753 acoustic noise emission limit and test methods.

3.4 Electrical safety guidelines

This section provides the electrical safety guidelines for the customer premises equipment.

Note: The devices comply with the U.S. National Electrical Code. However, local electrical authorities have jurisdiction when there are differences between the local and U.S. standards.

The devices comply with BS EN 61140.

3.4.1 Power supplies

The use of any non-Nokia approved power supplies or power adapters is not supported or endorsed by Nokia. Such use will void any warranty or support contract with Nokia. Such use greatly increases the danger of damage to equipment or property.

3.4.2 Cabling

The following are the guidelines regarding cables used for the customer premises equipment:

- All cables must be approved by the relevant national electrical code.

4 ETSI environmental and CRoHS guidelines

4.1 Overview

4.1.1 Purpose

This chapter provides information about the ETSI environmental China Restriction of Hazardous Substances (CRoHS) regulations that govern the installation and operation of devices. This chapter also includes environmental operation parameters of general interest.

4.1.2 Contents

4.2 Environmental labels

This section describes the environmental instructions that are provided with the customer documentation, equipment, and location where the equipment resides.

4.2.1 Overview

CRoHS is applicable to Electronic Information Products (EIP) manufactured or sold and imported in the territory of the mainland of the People's Republic of China. EIP refers to products and their accessories manufactured by using electronic information technology, including electronic communications products and such subcomponents as batteries and cables.

4.2.2 Environmental labels

Environmental labels are located on appropriate equipment. The following are sample labels.

Products below Maximum Concentration Value (MCV) label

Figure 4-1, "Products below MCV value label" (p. 36) shows the label that indicates a product is below the maximum concentration value, as defined by standard SJ/T11363-2006 (Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products). Products with this label are recyclable. The label may be found in this documentation or on the product.

Figure 4-1 Products below MCV value label

18986

Products containing hazardous substances above Maximum Concentration Value (MCV) label

Figure 4-2, “Products above MCV value label” (p. 36) shows the label that indicates a product is above the maximum concentration value, as defined by standard SJ/T11363-2006 (Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products). The number contained inside the label indicates the Environment-Friendly User Period (EFUP) value. The label may be found in this documentation or on the product.

Figure 4-2 Products above MCV value label

18985

Together with major international telecommunications equipment companies, Nokia has determined it is appropriate to use an EFUP of 50 years for network infrastructure equipment and an EFUP of 20 years for handsets and accessories. These values are based on manufacturers' extensive practical experience of the design, manufacturing, maintenance, usage conditions, operating environments, and physical condition of infrastructure and handsets after years of service. The values reflect minimum values and refer to products operated according to the intended use conditions. See the following section for more information.

4.3 Hazardous Substances Table (HST)

This section describes the compliance of the OLT and CPE to the CRoHS standard when the product and subassemblies contain hazardous substances beyond the MCV value. This information is found in this user documentation where part numbers for the product and subassemblies are listed. It may be referenced in other OLT and CPE documentation.

In accordance with the People’s Republic of China Electronic Industry Standard Marking for the Control of Pollution Caused by Electronic Information Products (SJ/T11364-2006), customers may access the Nokia Hazardous Substance Table, in Chinese, from the following location:

- http://www.nokia-sbell.com/wwwroot/images/upload/private/1/media/ChinaRoHS.pdf

4.4 Other environmental requirements

Observe the following environmental requirements when handling the WiFi Beacon.

4.4.1 WiFi Beacon environmental requirements

See the CPE technical specification documentation for more information about temperature ranges.

4.4.2 Storage

According to ETS 300-019-1-1 - Class 1.1, storage of CPE equipment must be in Class 1.1, weather-protected, temperature-controlled locations.

4.4.3 Transportation

According to EN 300-019-1-2 - Class 2.3, transportation of the equipment must be in packed, public transportation with no rain on packing allowed.

4.4.4 EU RoHS

European Union (EU) Directive 2011/65/EU, “Restriction of the use of certain Hazardous Substances” (RoHS), restricts the use of lead, mercury, cadmium, hexavalent chromium, and certain flame retardants in electrical and electronic equipment. Nokia products shipped to the EU comply with the EU RoHS Directive.

Nokia has implemented a material/substance content management process. The process is described in: Nokia process for ensuring RoHS Compliance (1AA002660031ASZZA). This ensures compliance with the European Union Directive 2011/65/EU on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment.

4.4.5 End-of-life collection and treatment

Electronic products bearing or referencing the symbol shown in the following figure, when put on the market within the European Union (EU), shall be collected and treated at the end of their useful life, in compliance with applicable EU and local legislation. They shall not be disposed of as part of unsorted municipal waste. Due to materials that may be contained in the product, such as heavy metals or batteries, the environment and human health may be negatively impacted as a result of inappropriate disposal.

Note: In the European Union, a solid bar under the symbol for a crossed-out wheeled bin indicates that the product was put on the market after 13 August 2005.

Figure 4-3 Recycling/take back/disposal of product symbol

About mark is used in compliance to European Union WEEE Directive (2012/19/EU).

There can be different requirements for collection and treatment in different member states of the European Union.

In compliance with legal requirements and contractual agreements, where applicable, Nokia will offer to provide for the collection and treatment of Nokia products bearing the logo shown in Figure 4-3, “Recycling/take back/disposal of product symbol” (p. 38) at the end of their useful life, or products displaced by Nokia equipment offers. For information regarding take-back of equipment by Nokia, or for more information regarding the requirements for recycling/disposal of product, contact your Nokia account manager or Nokia take back support at sustainability.global@nokia.com.

5 Beacon 19 unit data sheet

5.1 Overview

5.1.1 Purpose

This chapter describes the Beacon 19 unit data sheet.

5.1.2 Contents

5.2 Beacon 19 part numbers and identification

Table 5-1, “Beacon 19 identification” (p. 39) provides part numbers and identification information for Beacon 19.

Table 5-1 Beacon 19 identification

Ordering part number	Provisioning number	Description	CLEC	CPR	ECI/ Bar code
3TN00784AA	3TN00789AA	Beacon 19, US Plug,10Gbps WAN/LAN, WiFi 7 4+4+4	BVMNJ10HRA	—	—
3TN00784AB					
3TN00784BA	3TN00789BA	Beacon 19, EU Plug, 10Gbps WAN/LAN, WiFi 7 4+4+4	—	—	—
3TN00784CA	3TN00789CA	Beacon 19, UK Plug, 10Gbps WAN/LAN, WiFi 7 4+4+4	—	—	—

Table 5-2, “Beacon 19 power supply ordering information” (p. 40) provides power supply ordering information for Beacon 19.

Table 5-2 Beacon 19 power supply ordering information

Ordering part number	Manufacturer	Applicable power supply model	Power information	Compliance detail	Notes
Kit: 3TN00784AA EMA: 3TN00789AA	Honor	ADS-40FKJ-12N 12036EPCU/ 9040108111201204R	12V 3A wall mounted DC power adapter	ANSI municipality US, Canada	2-pin US input plug
	Keli	KL-WA120300-A1/SW-WB042N			
Kit: 3TN00784AB EMA: 3TN00789AA	Honor	ADS-40FKJ-12N 12036EPCU/ 9040108111201204R	12V 3A wall mounted DC power adapter	ANSI municipality US, FCC/ETL	2-pin US input plug
	Keli	KL-WA120300-A1/SW-WB042N			
Kit: 3TN00784BA EMA: 3TN00789BA	Honor	ADS-40FKJ-12N 12036EPG/ 9040108111202204R	12V 3A wall mounted DC power adapter	Europe, CE certified	2-pin EU input plug
	Keli	KL-WE120300-Z/SW-WB042NC1	12V 3A wall mounted DC power adapter		
Kit: 3TN00784CA EMA: 3TN00789CA	Honor	ADS-40FKJ-12N 12036EPB/ 9040108111206203R	12V 3A wall mounted, DC power adapter	UK, CE certified	3-pin UK input plug
	Keli	KL-WB120300-Z/SW-WB042NB			

5.3 Beacon 19 general description

WiFi is abundantly deployed in home networks. Users crave a seamless experience at home including effortlessly connecting their wireless devices to the network. Traditional WiFi networks require unique SSIDs for each of the access points or tedious set-up of WiFi extenders, which complicate the user experience. The Nokia WiFi network simplifies the user experience by providing a seamless mesh network with easy device onboarding and automated network optimization.

The overall Nokia WiFi solution is composed of one Nokia WiFi gateway (or Nokia WiFi Beacon) as root AP, one or more Nokia WiFi Beacons, the Nokia WiFi Care Portal for the operator's customer care team, and a mobile application for the end-user's self care.

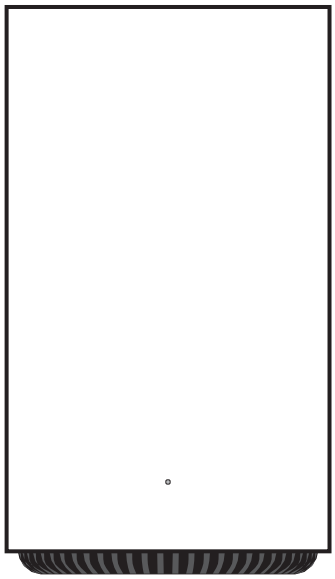
Note: The Nokia WiFi Care Portal can be accessed by the end user and the operator.

Beacon 19 can be deployed as either an Ethernet residential gateway or a WiFi Beacon in the Nokia WiFi solution. The residential gateway is the central point of the mesh network providing access to the broadband network (Internet) while the Beacon aids with extending the WiFi coverage to every corner of the home, providing seamless roaming to wireless connected devices.

The Beacon 19 has built-in concurrent quadband Wi-Fi 802.11 be networking with triple-play capability. Beacon 19 devices can be configured using the Nokia WiFi Mobile App, which can be downloaded on both iOS and Android devices.

The following figure shows the Beacon 19:

Figure 5-1 Beacon 19 WiFi gateway/Beacon



38917

The Beacon 19 provides the following functions and benefits:

- Quad-band WiFi7: concurrent IEEE802.11b/g/n/ax/be 4x4 2.4GHz, IEEE802.11a/n/ac/ax/be 4x4 5GHz, IEEE802.11 a/ax/be 4x4 6GHz
- Automatically decide on wireless router mode and Beacon mode in a mesh network
- One 10Gbase-T interface with RJ-45 connector for WAN, one 10Gbase-T and two 1Gbase-T interfaces with RJ-45 connectors for LAN
- Nokia intelligent EasyMesh
- Embedded edge analytics optimize network performance in real-time

Benefits:

- Latest Wi-Fi 7 technology that supports MLO operation allowing of up to 3 radio links to be assigned to a client enabling both higher speeds and lower latencies. An MLO link with 5GHz + 6 GHz can provide a maximum PHY rate of 23 Gbps
- Additonal features supported: Multiple RUs (MRU) per STA operation to avoid interference and increase efficiency, 320 MHz bandwidth in 6GHz radio, Higher efficiency with 4K QAM waveform, Ready to support AFC
- PHY rate up to 1376 Mb/s for 2.4 GHz, 5765 Mb/s for 5GHz and 11529 Mb/s for 6GHz
- Improves connection speeds throughout the home and provides WiFi where typically there would be none
- Better mesh performance by using 4x4 5GHz High band and 4x4 6GHz band as MLO
- Client steering, channel optimization
- Real-time wireless spectrum scan and analysis

- High quality of service (QoS) video over WiFi
- Ease of setup and user intuitive information

The table below lists additional function detail:

Table 5-3 Beacon 19 function detail

Function	Detail
Installation	Desktop and wall mountable with optional wall mount bracket
Interfaces	• One RJ45 10 Gigabit Ethernet WAN port • One RJ45 10 Gigabit Ethernet LAN port and two RJ45 1 Gigabit Ethernet LAN port • Supports 4x4 802.11b/g/n/ax/be 2.4 GHz wireless LAN (WLAN) interface • Supports 4x4 802.11a/n/ac/ax/be 5 GHz wireless LAN (WLAN) interface • Supports 4x4 802.11 a/ax/be 6 GHz wireless LAN (WLAN) interface • Maximum Effective Isotropic Radiated Power (EIRP) on 2.4 GHz up to 2000 mW, 5 GHz up to 2000 mW, and 6 GHz up to 1000 mW • WPA support including WPA2 and WPA3 Personal encryption • Nokia Design for Security (DFSEC) requirement compliant
Router mode	• IPv4 and IPv6 • Point-to-Point Protocol over Ethernet (PPPoE) and IP over Ethernet (IPoE) • Network Address Translation (NAT), demilitarized zone (DMZ) and firewall • Dynamic Host Configuration Protocol (DHCP) and domain name system (DNS) proxy • Internet Group Management Protocol (IGMP) v2/v3 • LXC container and TR157 Software module management • Supports TR-069 with TR-181 datamodel. Supports USP/TR-369 • Supports virtual private network (VPN) pass- through for Point-to-Point Tunneling protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and IPSec • Port forwarding and DMZ/dynamic domain name system (DDNS) • Flexible video delivery options over Ethernet or wireless • Nokia WiFi mesh middleware
Beacon mode	• Supports IPv4/IPv6 UDP/TCP forwarding • Supports IPv4 for internal management • Supports TR-069 with TR-181 datamodel. Supports USP/TR-369 • Supports VPN pass-through for PPTP, L2TP and IPSec • IGMP v2/v3 snooping • Flexible video delivery options over Ethernet or wireless • Nokia WiFi mesh middleware
LED	• Single multi-color LED for simple and intuitive status indication

Table 5-3 Beacon 19 function detail (continued)

Function	Detail
Regulatory compliance	• ETL • FCC Part 15 • ISED

5.3.1 TR-069 object support for WiFi parameters

The Beacon 19 supports the status retrieval and configuration of the following WiFi parameters via TR-069:

- Channel
- SSID
- Password for WPA and WEP
- Tx power (transmission rate in dBm)

These are the same TR-069 object parameters that are supported in the GUI.

5.3.2 Communication method to Nokia cloud management solution

The Beacon 19 communicates to the Nokia cloud management solution through MQTT and https.

The supported mechanism is specific to a customer deployment and the detailed description is available in the Customer Release Notes (CRN) of each release.

5.3.3 TR-157 Software Module Managements

Beacon 19 can support LXC container for third party software components. Life cycle of these software components are managed by ACS with the parameters defined in TR-157.

The TR-157 objects are:

- Mange each software component via SoftwareModules.DeploymentUnit.
- Set software component execution environment via SoftwareModules.ExecEnv.
- Run software component and get the execution status via SoftwareModules.ExecutionUnit.

Note: The available memory for third party applications needs a detailed study, considering the actual memory load of the current hardware, software, Beacon software evolution over long time and the projected use by a third party application of the software. Therefore, Nokia suggests to review this case by case. Contact your Nokia support representative for more information.

5.3.4 TR-069 authentication using TLS and CA certificates

Beacon 19 devices support encrypted remote TR-069 management using TLS, as well as ACS authentication using SHA-256 pre-installed certificates.

If the ACS URL is set to the https://... format, by default, the connection will use TLS without authentication mode. The Beacon 19 can also authenticate the ACS using a pre-installed CA certificate.

5.4 Beacon 19 software and installation feature support

For information on installing or replacing the Beacon 19, see Chapter 6, “Install or replace a Beacon 19”.

5.5 Beacon 19 interfaces and interface capacity

The table below describes the supported interfaces and interface capacity for Beacon 19 devices.

Table 5-4 Beacon 19 interface connection capacity

Device type and model	Maximum capacity							
	POTS	100/ 10 BASE-T	RF video (CATV)	10GE WAN	1GE LAN	10GE LAN	Local craft	USB3. 1(gen1)
Beacon 19	—	—	—	1	2	1	—	—

5.5.1 Beacon 19 connections and components

Figure 5-2, “Beacon 19 physical connections” (p. 45) shows the physical connections for Beacon 19.

Figure 5-2 Beacon 19 physical connections

The table below describes the physical connections for Beacon 19 devices.

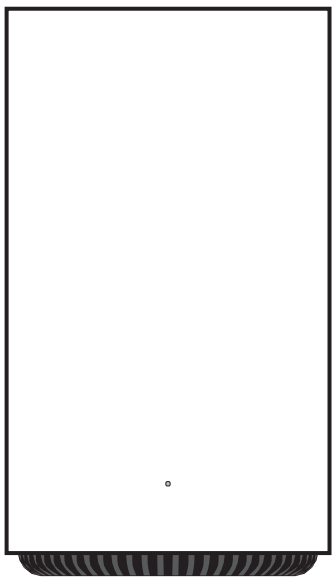
Table 5-5 Beacon 19 physical connections

Connection	Description
On/Off button	This button powers the unit on or off.
LAN 1/ LAN 2/ LAN 3	This connection is provided through Ethernet RJ-45 connectors. Up to one 10Gbase-T and two 1Gbase-T interfaces with RJ45 connector are supported. The Ethernet ports can support both data and in-band video services on all three interfaces.
WAN port	This connection is provided through an 10GE interface.
WPS button	This button is used to start the WiFi Protected Setup (WPS) for new WiFi devices.
Reset button	Pressing the Reset button for less than 10 seconds reboots the Beacon; pressing the Reset button for 10 seconds or more restores the Beacon to its factory defaults.
Power input	This connection is provided through the power connector. A power cable fitted with a barrel connector is used to make the connection.

5.6 Beacon 19 LEDs

The front of the Beacon 19 functions as a multi-color LED indicator. The LED color and pulse rate acts as a signal to the home user, which indicates the state of the Beacon 19 and the quality of its backhaul link.

Figure 5-3 Beacon 19 LEDs



38917

Table 5-6, “Beacon 19 LED indications” (p. 46) provides LED descriptions for the Beacon 19.

Table 5-6 Beacon 19 LED indications

LED color	LED behavior	Router mode	Extender mode	LED behavior description
Off	Off	✓	✓	Power off.
Blue-Green	Solid	✓		Good backhaul connection to the Internet.
	Solid		✓	Good backhaul connection. A link to the next node is available.
	Solid		✓	Backhaul connection is successful but not optimal. A link to the next node is below standard.
Yellow	Solid		✓	Backhaul connection is successful but not optimal. A link to the next node is below standard.
	Slow pulsing	✓	✓	Configuration mode. The unit is waiting to be configured.

Table 5-6 Beacon 19 LED indications (continued)

LED color	LED behavior	Router mode	Extender mode	LED behavior description
Red	Solid	✓		No connection to the Internet
	Solid		✓	Backhaul connection is successful but not optimal. A link to the next node is not operational.
	Fast pulsing	✓	✓	Factory reset.
White	Slow pulsing	✓	✓	WPS enabled.
	Solid	✓	✓	Powering on.
	3 sec quick pulse	✓	✓	WPS successful.

5.7 Beacon 19 detailed specifications

The table below lists the physical specifications for the Beacon 19.

Table 5-7 Beacon 19 physical specifications

Description	Specification
Length	125 mm (4.92 in.)
Width	125 mm (4.92 in.)
Height	237.5 mm (9.35 in.)
Weight [within ± 0.5 lb (0.23 kg)]	1230g (2.71 lb)

Table 5-8, “Beacon 19 dimension data specifications” (p. 47) lists the dimension data specifications for Beacon 19.

Table 5-8 Beacon 19 dimension data specifications

Dimension	Specification
Packet size supported	1518
Number of IP addresses supported (or ranges)	In LAN network, the supported range is: • IPv4: 253 (support the IPv4 private network IP ranges) • IPv6: any allocated Global Unicast Addresses (GUA)
Number of supported WiFi clients (per radio, per device, per mesh)	120 per radio, 120 per device, 256 per mesh
Number of supported beacons /APs in a mesh	4 (including root AP)
Number of supported WAN interfaces	8
Number of supported VLANs	2-4094
Number of LLIDs in the device	-

Table 5-8 Beacon 19 dimension data specifications (continued)

Dimension	Specification
Number of priority queues, and overall buffer size	LAN port queques: 8; total buffer: 4MB WAN port queques: 8; total buffer: 4MB
Number of multicast groups (DACL entries)	256

Table 5-9, “Beacon 19 power consumption specifications” (p. 48) lists the power consumption specifications for the Beacon 19.

Table 5-9 Beacon 19 power consumption specifications

Maximum power (Not to exceed)	Condition	Minimum power	Condition
36W	Ethernet ports and WiFi interfaces running at full load	10.67W	WAN link active and connected to the Internet

Table 5-10, “Beacon 19 environmental specifications” (p. 48) lists the environmental specifications for Beacon 19.

Table 5-10 Beacon 19 environmental specifications

Mounting method	Temperature range and humidity	Altitude
On desk or shelf	Operating: -5°C to 45°C (23°F to 113°F) ambient temperature 95% relative humidity, non-condensing at 40°C	Contact your Nokia technical support representative for more information
	Storage: --20°C to 70°C (-68°F to 185°F)	

5.8 Beacon 19 functional blocks

Beacon 19 devices are single-residence units that support Wireless (WiFi) service. WiFi service on these devices is compliant with the IEEE 802.11 standard. In addition to the WiFi service, these devices transmit Ethernet packets to three RJ-45 Ethernet ports.

5.9 Beacon 19 responsible party

Table 5-11, “Responsible party contact information” (p. 49) lists the party in the US responsible for this device.

Table 5-11 Responsible party contact information

Legal Company name	Nokia Solutions and Networks OY	Nokia of America Corporation
Offices	Offices | Nokia (https://www.nokia.com/contact-us/offices/#north-america)	
Support	Business Support | Nokia (https://www.nokia.com/networks/business-support/)	
Other contacts	Contact us | Nokia (https://www.nokia.com/contact-us/)	

5.10 Beacon 19 special considerations

This section describes the special considerations for Beacon 19 devices.

5.10.1 WiFi service

Beacon 19 devices feature WiFi service as well as data services. WiFi is a wireless networking technology that uses radio waves to provide wireless HSI and network connections. This device complies with the IEEE 802.11 standards, which the WiFi Alliance defines as the basis for WiFi technology.

WiFi standards and certifications

The WiFi service on Beacon 19 devices supports the following IEEE standards and Wi-Fi Alliance certifications (WFA100049 for 2x2, WFA100571 for 4x4):

- Compliant with IEEE 802.11 standards
- Certified for Wi-Fi 7
- Certified for WPA™ – Enterprise, Personal
- Certified for WPA2™ – Enterprise, Personal
- Certified for WPA3™ – Enterprise, Personal (Aug 2019)
- Certified for Protected Management Frames
- Certified for Wi-Fi Agile Multiband™,WMM®, WMM®-Power Save, Wi-Fi Protected Setup™

Nokia WiFi app configuration

The Nokia WiFi mobile app can be used to set up the Beacon 19 and manage the network.

It can be downloaded from the App Store for iOS (https://apps.apple.com/us/app/nokia-wifi/id1345278192) and the Google Play store for Android (https://play.google.com/store/apps/details?id=com.nokia.wifi).

Information about the Nokia WiFi app can be found on the Nokia WiFi Help Center https://wifi-helpcenter.nokia.com

WiFi GUI features

Beacon 19 devices have HTML-based WiFi configuration GUIs.

5.10.2 Beacon 19 considerations and limitations

For details about the considerations and limitations, see the CRN (Customer Release Notes).

6 Install or replace a Beacon 19

6.1 Overview

6.1.1 Purpose

This chapter provides the steps to:

- Install a Beacon 19
- Replace a Beacon 19

6.1.2 Contents

6.2 Prerequisites

Ensure that you have all required cables.

6.3 Recommended tools

You need the following tools:

- RJ-45 cable
- Paper clip

6.4 Safety information

Read the following safety information before installing the unit.

DANGER

Hazard

Hazardous electrical voltages and currents can cause serious physical harm or death. Always use insulated tools and follow proper safety precautions when connecting or disconnecting power circuits.

Make sure all sources of power are turned off and have no live voltages present on feed lines or terminals. Use a voltmeter to measure for voltage before proceeding.

Always contact the local utility company before connecting the enclosure to the utilities.

CAUTION

Service Disruption

Keep indoor devices out of direct sunlight. Prolonged exposure to direct sunlight can damage the unit.

Note: Observe the local and national laws and regulations that may be applicable to this installation.

Observe the following:

- The device should be installed in accordance with the applicable requirements of the NEC or CEC. Local authorities and practices take precedent when there is conflict between the local standard and the NEC or CEC.
- The device must be installed by qualified service personnel.
- Iindoor units must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the Chapter 5, “Beacon 19 unit data sheet” for the temperature ranges for these devices.

6.5 Install a Beacon 19

1

Place the unit on a flat surface, such as a desk or shelf.

Note: The Beacon 19 cannot be stacked with another or with other equipment. The installation requirements are:

- Allow a minimum 100 mm clearance above the top cover.
- Allow a minimum 50 mm clearance from the side vents.
- Do not place any heat source directly above the top cover or below the bottom cover.

2

Review the connection locations, as shown in Figure 6-1, “Beacon 19 connections” (p. 53).

Figure 6-1 Beacon 19 connections

3

Connect the Ethernet cables to the RJ-45 ports; see Figure 6-1, “Beacon 19 connections” (p. 53) for the location of the RJ-45 ports.

4

Connect the WAN cable to the RJ-45 WAN port; see Figure 6-1, “Beacon 19 connections” (p. 53) for the location of the RJ-45 WAN port.

5

Connect the power cable to the power connector.

Note: Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 12 V dc, 4 A. The polarity of the power adapter plug must match the Beacon 19.

6

Power up the unit by using the On/Off power switch.

7

Verify the LED status.

8

Activate and test the services.

9

If necessary, reset the Beacon 19.

Note: Resetting the device will return all settings to factory default values; any configuration customization will be lost.

a. Locate the **Reset** button as shown in Figure 6-1, “Beacon 19 connections” (p. 53).

b. Insert the end of a straightened paper clip or other narrow object into the hole in the Reset button to reset the device.

END OF STEPS

6.6 Replace a Beacon 19

1

Power down the unit by using the on/off power switch. See Figure 6-2, “Beacon 19 connections” (p. 53) for the connections on the Beacon 19.

Draft

Figure 6-2 Beacon 19 connections

2

Disconnect the WAN, Ethernet, and power cables from the Beacon 19; see Figure 6-2, “Beacon 19 connections” (p. 55) for the connector locations on the Beacon 19.

3

Replace the Beacon 19 with the new device. The device can be placed on any flat surface, such as a desk or shelf.

4

Connect the Ethernet cables directly to the RJ-45 ports; see Figure 6-2, “Beacon 19 connections” (p. 55) for the location of the RJ-45 ports.

5

Connect the WAN cable directly to the RJ-45 port; see Figure 6-2, “Beacon 19 connections” (p. 55) for the location of the RJ-45 WAN port.

6

Connect the power cable to the power connector.

Note: Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 12 V dc, 4 A. The polarity of the power adapter plug must match the Beacon 19.

7

Power up the unit by using the On/Off power switch.

8

Verify the LED status.

9

Activate and test the services.

10

If necessary, reset the Beacon 19.

Note: Resetting the device will return all settings to factory default values; any configuration customization will be lost.

a. Locate the Reset button on a Beacon 19 as shown in Figure 6-2, “Beacon 19 connections” (p. 55).

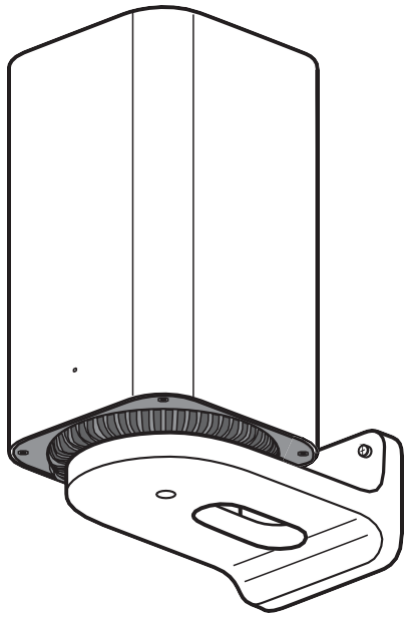
b. Insert the end of a straightened paper clip or other narrow object into the hole in the Reset button to reset the device.

END OF STEPS

6.7 Wall mount a Beacon 19

This section provides the steps to mount a Beacon 19.

Figure 6-3 Beacon 19 wall mounting bracket



38921

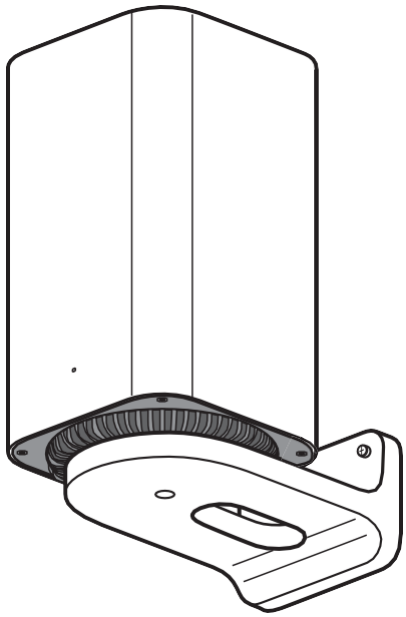
6.7.1 Procedure

Use this procedure to mount a Beacon 19 on a wall.

1

You can wall mount the Beacon 19 as shown in Figure 6-4, “Beacon 19 in wall mount bracket” (p. 58).

Figure 6-4 Beacon 19 in wall mount bracket

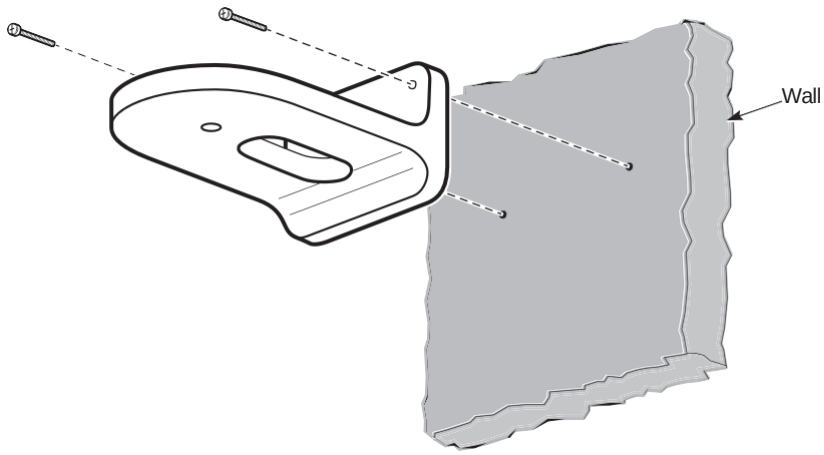


38921

2

Mount the Beacon 19 on a wall using the wall mount bracket as shown in Figure 6-5, “Beacon 19 wall mount bracket” (p. 58).

Figure 6-5 Beacon 19 wall mount bracket



38920

a. Determine the location of the two anchor holes for the wall mount bracket. The bracket can be used as a template for marking and drilling the holes.

   It is recommended to use a level to ensure that the ONT unit is installed horizontally.

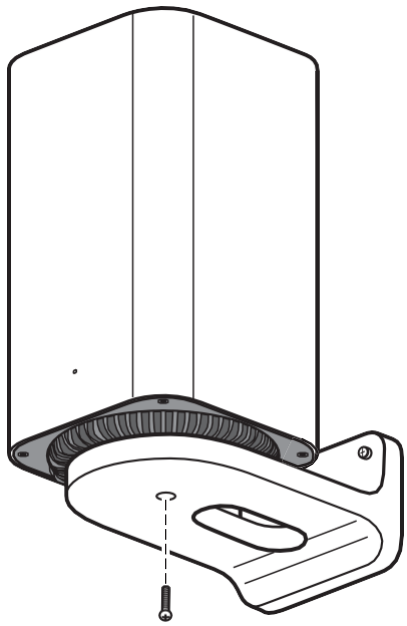
b. Drill two holes into the wall and with the centers spaced 72 mm.

c. Insert the two mounting screws and optional anchors into the holes.

d. At this point, perform a test to ensure that the wall mount bracket fits securely over the screw heads. Mount the bracket flush to the wall so that it does not warp or twist.

e. Install the Beacon 19 onto the wall mount bracket by placing the unit on the edge of the bracket and drill it in place with a screw from below to mount tightly. See Figure 6-6, “Beacon 19 to wall mount connection” (p. 58).

Figure 6-6 Beacon 19 to wall mount connection



38931

f. Connect the power cord and other cables to the Beacon 19.

END OF STEPS

7 Configure Beacon 19

7.1 Overview

7.1.1 Purpose

This chapter describes the WebGUI configuration procedures.

7.1.2 Contents

GUI overview

This section provides an overview of the Beacon 19 WebGUI.

7.2 General configuration

For HTTP/HTPPs configuration procedures, refer to the **Nokia ONT Configuration, Management, and Troubleshooting Guide**.

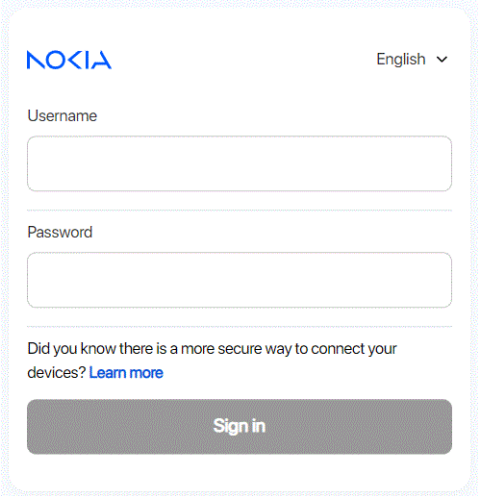
7.3 Logging in to the web-based GUI

1

Open a web browser and enter the IP address of the Beacon in the address bar.

The *Login* page displays.

Figure 7-1 Login page



The default gateway IP address must be same as the one printed on the device label. You can connect to this IP address using your web browser after connecting your PC to one of Ethernet ports of the Beacon or via WiFi connection. The static IP address of your PC must be in the same default gateway subnet as the Beacon.

2

CAUTION

Service Disruption

If you forget the current username and password, press the **Reset** *button for 10 seconds to reset the values to the default username and password provided at startup.*

Pressing the **Reset** *button for less than 10 seconds reboots the device.*

Pressing the **Reset** *button for 10 seconds resets the device to the factory defaults.*

Enter your username and password in the *Login* page, as shown in Figure 7-1, “Login page” (p. 64).

The superadmin account is meant for the operator and the password is unique per device unless specified differently in customer specific pre configuration. Contact your Nokia representative to obtain the superadmin password for device.

The default end-user account name and the default password for this account are printed on the device label.

The superadmin user has access to all WebGUI features while the end-user account has only limited access to WebGUI features. This access for the end-user can be adapted with a WebGUI configuration file. Contact your Nokia representative to know the factory default settings of which WebGUI access is available to your end user or how to get a WebGUI configuration file.

3

Click **Sign in**. The *Overview* page displays.

Note: To help protect the security of your Internet connection, the application displays a pop-up reminder to change both the WiFi password and the Beacon password.
To increase password security, use a minimum of 10 characters, consisting of a mix of numbers and upper and lower case letters.

END OF STEPS

7.4 Beacon 19 WebGUI Menu

The following table lists the main menu and sub-menu options in the Beacon 19 WebGUI:

Table 7-1 Beacon 19 WebGUI Menu

Main Menu	Sub-menu	Procedure Reference
Overview	-	7.5 “Viewing overview information” (p. 67)
WAN	**WAN services**	7.7 “Configuring WAN Services” (p. 70)
WAN	**WAN statistics**	7.8 “Viewing WAN Statistics” (p. 77)
WAN	**TR-069**	7.9 “Configuring TR-069” (p. 79)

Table 7-1 Beacon 19 WebGUI Menu (continued)

Main Menu	Sub-menu	Procedure Reference
WAN	**TR-369**	7.10 “Configuring TR-369” (p. 81)
WAN	**IP routing**	7.11 “Configuring Static routing” (p. 82)
WAN	**Qos config**	7.12 “Configuring QoS” (p. 83)
LAN	**DHCP IPv4**	7.14 “Configuring DHCP IPv4” (p. 86)
LAN	**DHCP IPv6**	7.15 “Configuring DHCP IPv6” (p. 88)
LAN	**DNS**	7.16 “Configuring DNS” (p. 90)
LAN	**LAN statistics**	7.17 “Viewing LAN Statistics” (p. 93)
WiFi	**WiFi networks**	7.19 “Configuring WiFi Network” (p. 96)
WiFi	**Guest network**	7.20 “Configuring Guest Network” (p. 102)
WiFi	**Network map**	7.21 “Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points” (p. 103)
WiFi	**Advanced settings**	7.22 “Configuring Wireless 2.4 GHz” (p. 109)
WiFi	**WiFi statistics**	7.25 “Viewing WiFi Statistics” (p. 114)
Devices	-	7.27 “Viewing Device Information” (p. 116)
Security	**Firewall**	7.29 “Configuring the Firewall” (p. 119)
Security	**MAC filter**	7.30 “Configuring the MAC Filter” (p. 120)
Security	**IP filter**	7.31 “Configuring the IP Filter” (p. 122)
Security	**Family profiles**	7.32 “Configuring Family Profiles” (p. 123)
Security	**DMZ and ALG**	7.33 “Configuring DMZ and ALG” (p. 134)
Security	**Access control**	7.34 “Configuring Access Control” (p. 135)
Advanced settings	**Port forwarding**	7.36 “Configuring Port Forwarding” (p. 138)
Advanced settings	**Port triggering**	7.37 “Configuring Port Triggering” (p. 139)
Advanced settings	**DDNS**	7.38 “Configuring DDNS” (p. 140)
Advanced settings	**NTP**	7.39 “Configuring NTP” (p. 142)
Maintenance	**Change password**	7.41 “Configuring the Password” (p. 144)
Maintenance	**Backup and restore**	7.42 “Backing Up the Configuration” (p. 146) 7.43 “Restoring the Configuration” (p. 146)
Maintenance	**Firmware upgrade**	7.44 “Upgrading Firmware” (p. 148)
Maintenance	**Diagnostics**	7.45 “Diagnosing WAN Connections” (p. 149)
Maintenance	**Log**	7.46 “Viewing Log Files” (p. 153)
Maintenance	**Container management**	7.47 “Viewing Container Management” (p. 154)
Troubleshooting	**Troubleshooting counters**	7.48 “Troubleshooting counters” (p. 155)

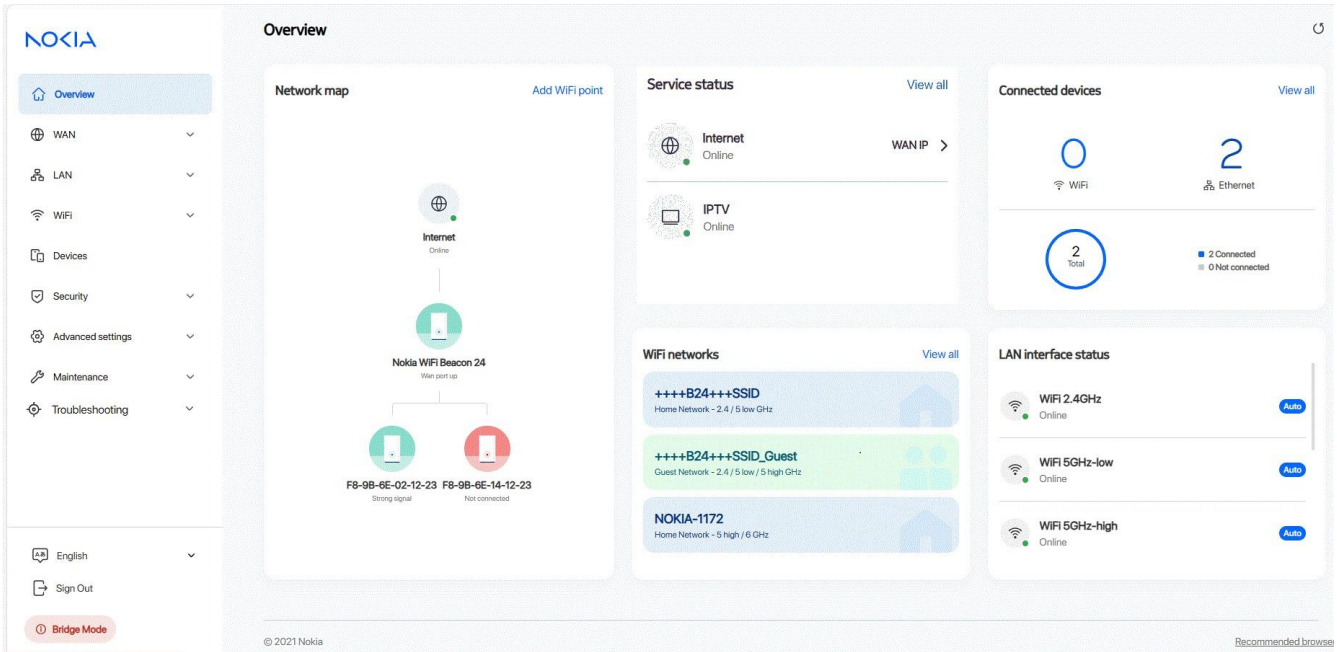
Table 7-1 Beacon 19 WebGUI Menu (continued)

Main Menu	Sub-menu	Procedure Reference
Troubleshooting	**Speed test**	7.49 “Viewing Speed Test” (p. 156)

7.5 Viewing overview information

1

Click **Overview** from the left pane. The Overview page displays the following cards:



END OF STEPS

7.5.1 Network Map

Displays information about the status of the mesh network and connection to the internet. The status of the internet connection is defined by the presence of an IP address on the internet service. *Up* is indicated with green and *Down* is indicated with red.

Root device

Displays the mnemonic of the device. The colored indicator as well as the status under the name reflects the physical status of the WAN connection (4G/5G, PON port, WAN port). *Up* is Green, *Down* is Red.

Extender device

Displays the mnemonic of the device. The colored indicator as well as the status under the name reflects the physical status of the backhaul connection (Strong Signal = Green, Poor Signal = Amber, Not connected = red).

7.5.2 Radio Access

Displays the 4G, 5G or 6G signal connection status when a device is connected to an FWA receiver. Click the button to view the connection details.

7.5.3 Service Status

Displays the active status of the triple-play services.

Internet service

The internet service represents the presence of a WAN IP address for the routed network that has the internet attached to it. The card shows the WAN IP address (IPv4 and/or IPv6).

IPTV service

Shows the status of the IPTV service. If the IPTV flag is enabled on a routed service, the online or offline state is indicated by the presence of a WAN IP address for that routed service. If the IPTV is attached to a bridged service, the online or offline state is defined by the WAN uplink status.

7.5.4 WiFi Networks

Displays a network card per activated single or dual band WiFi network containing the bands supported, the name of the network and the type of network (bridge or routed).

7.5.5 Connected Clients

Displays the total number of online and offline clients connected to this device (single device or mesh system).

7.5.6 LAN Interface Status

Displays information about all the LAN ports of the device.

WiFi 2.4GHz

Shows the status of the 2.4GHz (Up/Down) network and the current band setting. This can either be auto which indicates Radio Resource Management is enabled or in the range 1-13 when manually configured.

WiFi 5GHz low

Shows the status of the 5GHz low network (Up/Down) and the current band setting. This can either be auto which indicates Radio Resource Management is enabled or is in the range 36-64 when manually configured.

WiFi 6GHz

Shows the status of the 6GHz high network (Up/Down) and the current band setting. This can either be auto which indicates Radio Resource Management is enabled or is in the range of 100-165 when manually configured.

Ethernet Port

Shows the status of the Ethernet ports (Up/Down), the sync rate (10Mbps, 100Mbps, 1Gbps, 2.5Gbps, 5Gbps, 10Gbps) and the duplex mode (Half duplex, Full duplex).

WAN Configuration

7.6 Overview

This section describes the WAN configuration procedures that can be performed from the following sub-menu options under the **WAN** menu:

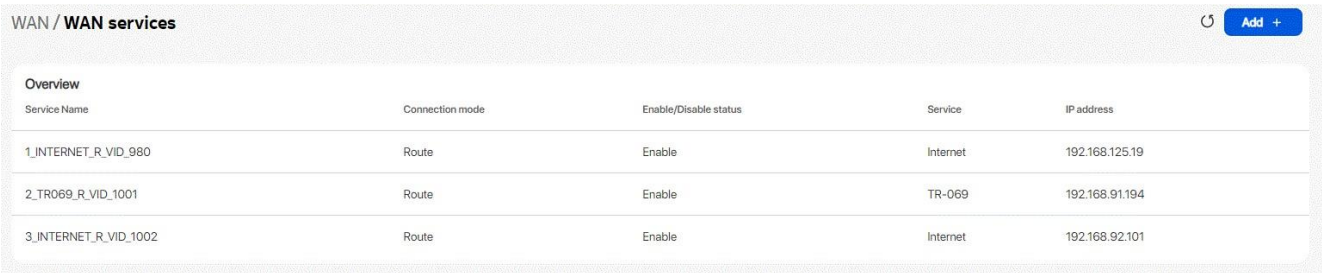
Sub-menu	Procedure
WAN services	7.7 “Configuring WAN Services” (p. 70)
WAN statistics	7.8 “Viewing WAN Statistics” (p. 77)
TR-069	7.9 “Configuring TR-069” (p. 79)
TR-369	7.10 “Configuring TR-369” (p. 81)
IP routing	7.11 “Configuring Static routing” (p. 82)
Qos config	7.12 “Configuring QoS” (p. 83)

7.7 Configuring WAN Services

1

Click **WAN→WAN services** in the left pane. The *WAN services* page displays the existing WAN connections in the *Overview* table. You can click on a connection to modify the connection configuration.

Figure 7-2 Overview table in *WAN services* page



2

Click **Add +** to create a WAN connection. The *Create New Connection* page displays.

Figure 7-3 Create New Connection page

Figure 7-4 Create New Connection page - PPPoE Configuration

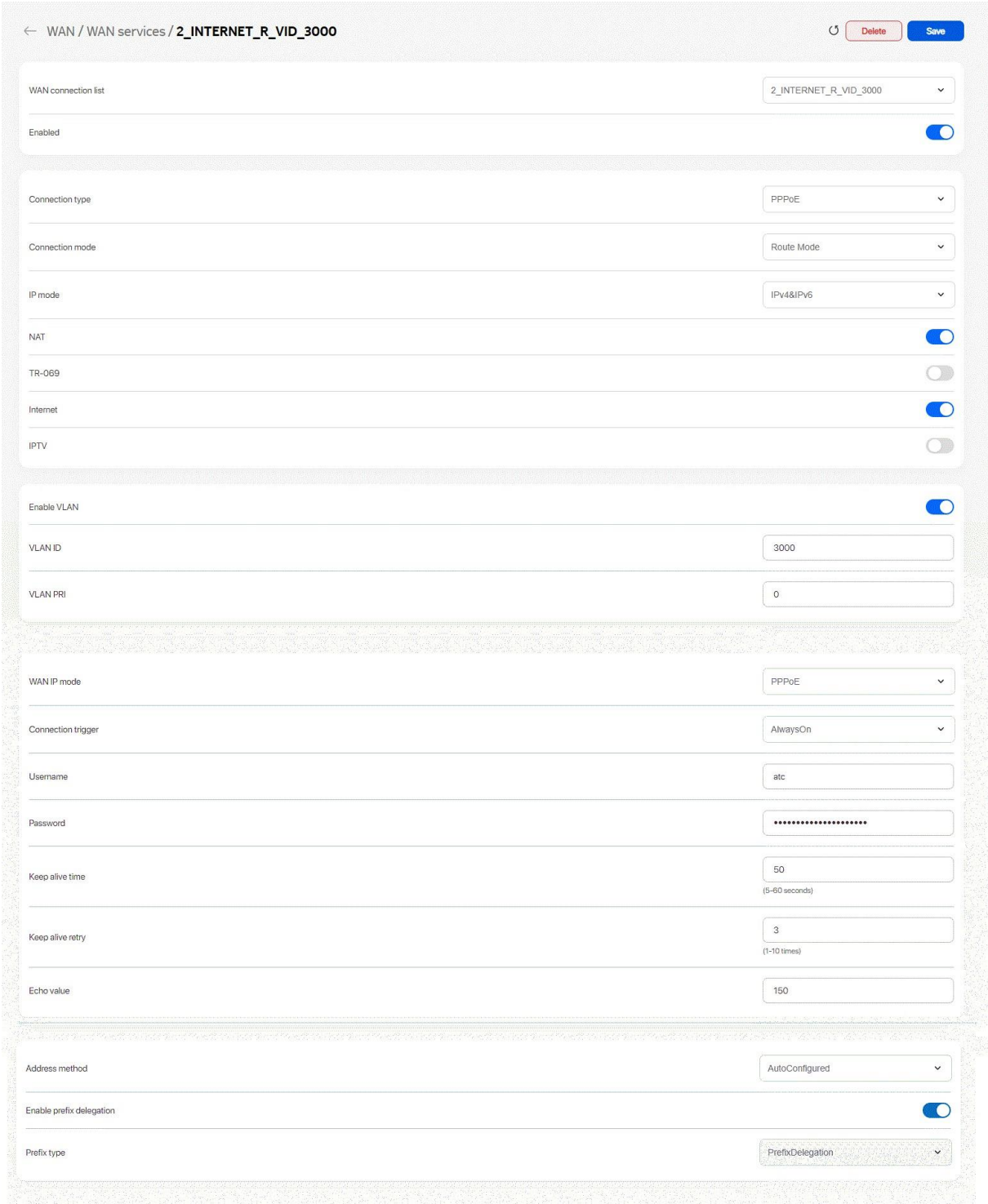


Figure 7-5 Bridge mode - Transparent

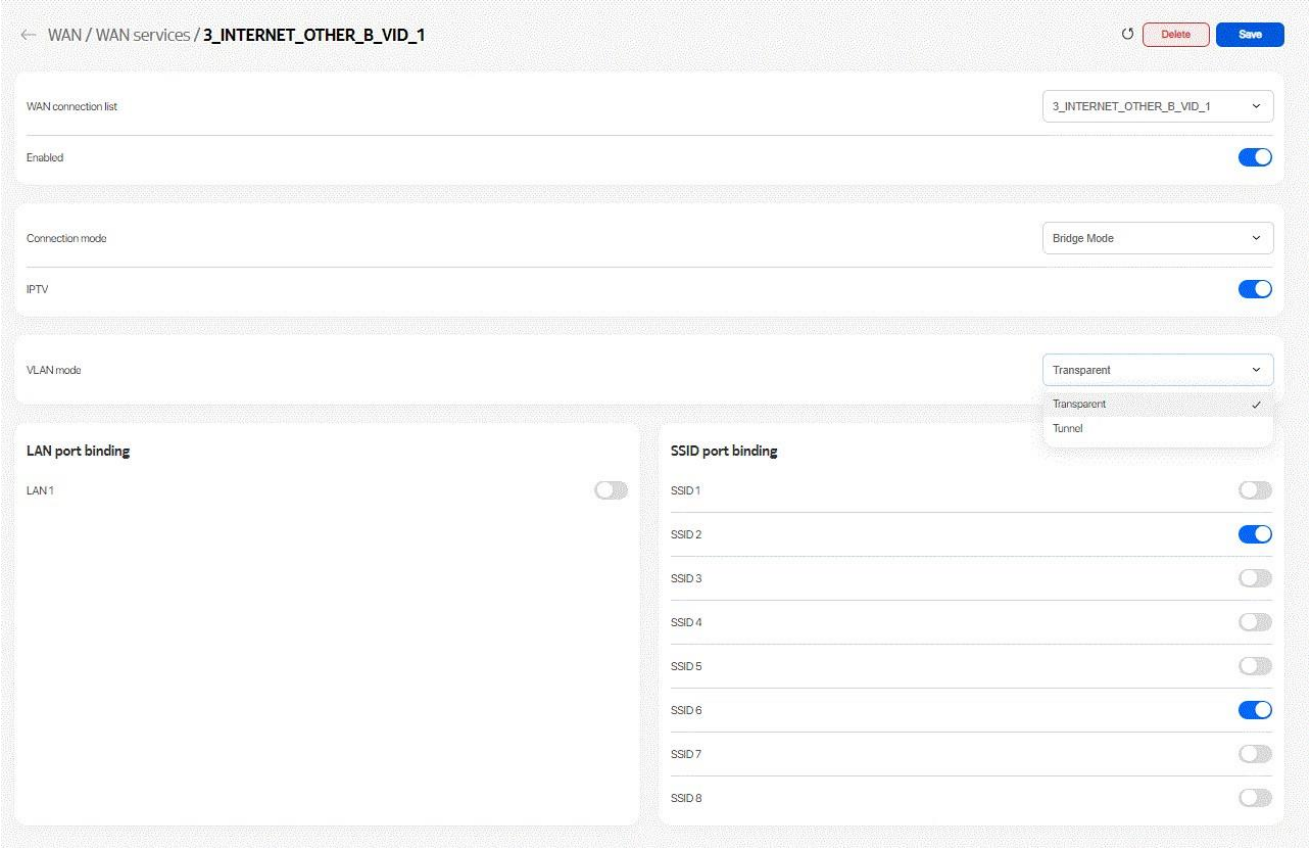
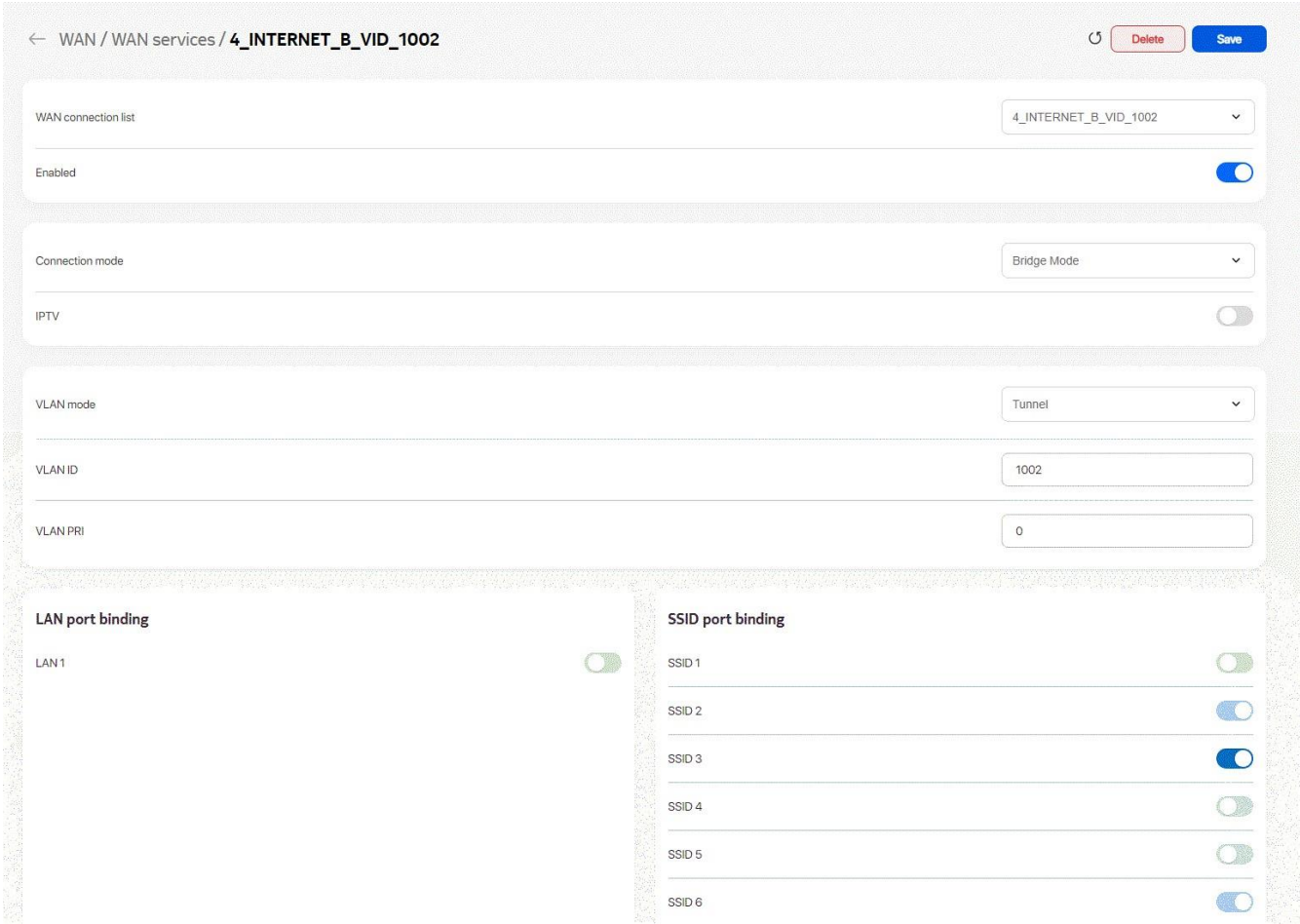


Figure 7-6 Bridge mode - Tunnel



3

Configure the following parameters:

Table 7-2 WAN services parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
Enabled	Select the toggle button to enable the WAN connection.
Connection type	Select a connection type from the list: • **IPoE** • **PPPoE**

Table 7-2 WAN services parameters (continued)

Field	Description
Connection mode	Select the connection mode of the WAN connection from the list: • **Route Mode** • **Bridge Mode**
NAT	Select the toggle button to enable NAT. This option is applicable only if the connection mode is **Route Mode**.
TR-069	Select the toggle button to enable TR-069. This option is applicable only if the connection mode is **Route Mode**.
Internet	Select the toggle button to enable Internet. This option is applicable only if the connection mode is **Route Mode**.
IPTV	Select the toggle button to enable IPTV.
Enable VLAN	Select the toggle button to enable VLAN. This option is applicable only if the connection mode is **Route Mode**.
VLAN mode	Select a VLAN mode from the list: • **Tunnel** • **Transparent** This option is applicable only if the connection mode is **Bridge Mode**.
VLAN ID	Enter the VLAN ID. Allowed values: 2 to 4094 In the bridge mode, this option is applicable only if the VLAN mode is **Tunnel**.
VLAN PRI	Enter the VLAN PRI. VLAN priority allows to assign a priority to outbound packets containing the specified VLAN ID. Allowed values: 0 to 7 In the bridge mode, this option is applicable only if the VLAN mode is **Tunnel** or **Transparent**.
LAN port binding	Select the toggle button next to the LAN to enable it. Select the toggle button next to the PVID to enable it. This option is not applicable if the VLAN mode is **Tunnel**.
SSID port binding	Select the toggle button next to the SSID to enable it. Select the toggle button next to the PVID to enable it. This option is applicable in all VLAN modes.
WAN IP mode	Select an IP mode from the list: • **DHCP** • **PPPoE** This option is visible only if you select PPPoE as the connection type. • **Static**
Manual DNS	If the selected IP mode is **IPv4** and the WAN IP mode is **DHCP**, enter the Domain Name Server (DNS) to be configured manually.
IPv4 Address	If the selected IP mode is **IPv4** or **IPv4&IPv6** and the WAN IP mode is **Static**, enter the static IPv4 address.

Table 7-2 WAN services parameters (continued)

Field	Description
Netmask	If the selected IP mode is **IPv4** or **IPv4&IPv6** and the WAN IP mode is **Static**, enter the netmask.
Gateway	If the selected IP mode is **IPv4** or **IPv4&IPv6** and the WAN IP mode is **Static**, enter the gateway IP address.
Pri DNS	If the selected IP mode is **IPv4** or **IPv4&IPv6** and the WAN IP mode is **Static**, enter the primary Domain Name Server (DNS).
Sec DNS	If the selected IP mode is **IPv4** or **IPv4&IPv6** and the WAN IP mode is **Static**, enter the secondary Domain Name Server (DNS).
Ter DNS	If the selected IP mode is **IPv4** or **IPv4&IPv6** and the WAN IP mode is **Static**, enter the tertiary Domain Name Server (DNS).
Connection trigger	Select the connection trigger type from the list. The default option is **Always On**.
Username	Enter the username to log in to the configuration server. This option is applicable only if the WAN IP mode is **PPPoE**.
Password	Enter the password to log in to the configuration server. Allowed values are limited to numbers, letters and special characters *!* # + , - . / *:* = @ _. This option is applicable only if the WAN IP mode is **PPPoE**.
Keep alive time	The PPPoE connection type triggers one heartbeat each, at the configured time interval to keep the session online. Allowed values: 5 to 60 seconds This option is applicable only if the WAN IP mode is **PPPoE**.
Keep alive retry	Configure the number of retries to check the Keep Alive status of the PPPoE session after time-out. Allowed values: 1 to 10. This option is applicable only if the WAN IP mode is **PPPoE**.
Echo value	Indicates the number of times the device sends messages to the server to check if the IP address is available or not. This option is applicable only if the WAN IP mode is **PPPoE**.
Address method	If the selected IP mode is **IPv6** or **IPv4&IPv6**, select the address method from the list: • **AutoConfigured** • **DHCPv6** • **DHCPv6_PD** • **DHCPv6_NA** • **Static**
Enable prefix delegation	If the selected address method is **AutoConfigured**, select the toggle button to enable inclusion of the Identity Association (IA) for Prefix Delegation option in Solicit messages.
Prefix type	Displays mechanism through which the prefix was assigned or most recently updated.
IP Address (v6)	If the selected address method is **Static**, enter the IPv6 address.
Gateway (v6)	If the selected address method is **Static**, enter the gateway IPv6 address.
IPv6 address prefix	If the selected address method is **Static**, enter the IPv6 address prefix.

Table 7-2 WAN services parameters (continued)

Field	Description
Pri DNS (v6)	If the selected address method is **Static**, enter the primary DNS IP address.
Sec DNS (v6)	If the selected address method is **Static**, enter the secondary DNS IP address.
DHCP option 50 persistent	Select the toggle button to enable DHCP Option 50 persistent.
Enable DHCP option 60	Select the toggle button to enable DHCP Option 60 (vendor class identifier).
Enable DHCP option 61	Select the toggle button to enable DHCP Option 61 (client identifier).
Enable DHCP option 77	Select the toggle button to enable DHCP Option 77 (user class information).
Enable DHCP option 90	Select the toggle button to enable DHCP Option 90 (authentication information).

4

Click **Save**. The connection is listed in the *Overview* table of the *WAN services* page.

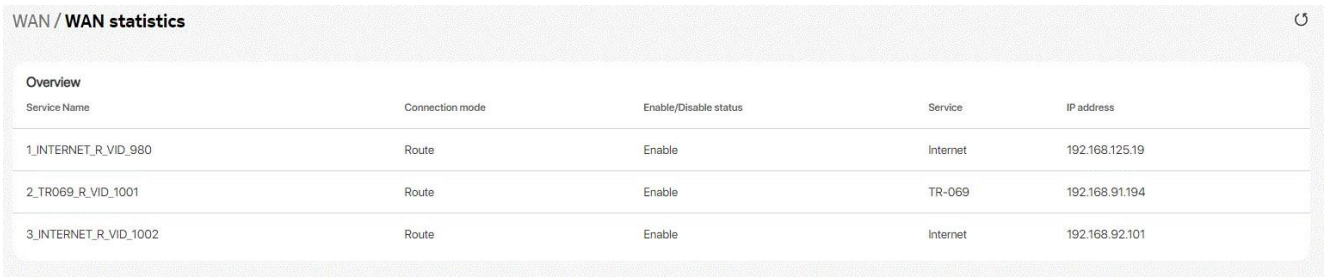
END OF STEPS

7.8 Viewing WAN Statistics

1

Click **WAN→WAN statistics** in the left pane. The *WAN Statistics* page displays the following information for WAN ports.

Figure 7-7 WAN Statistics page



2

Click on the service name to display the WAN statistics details page.

Figure 7-8 WAN Statistics page info

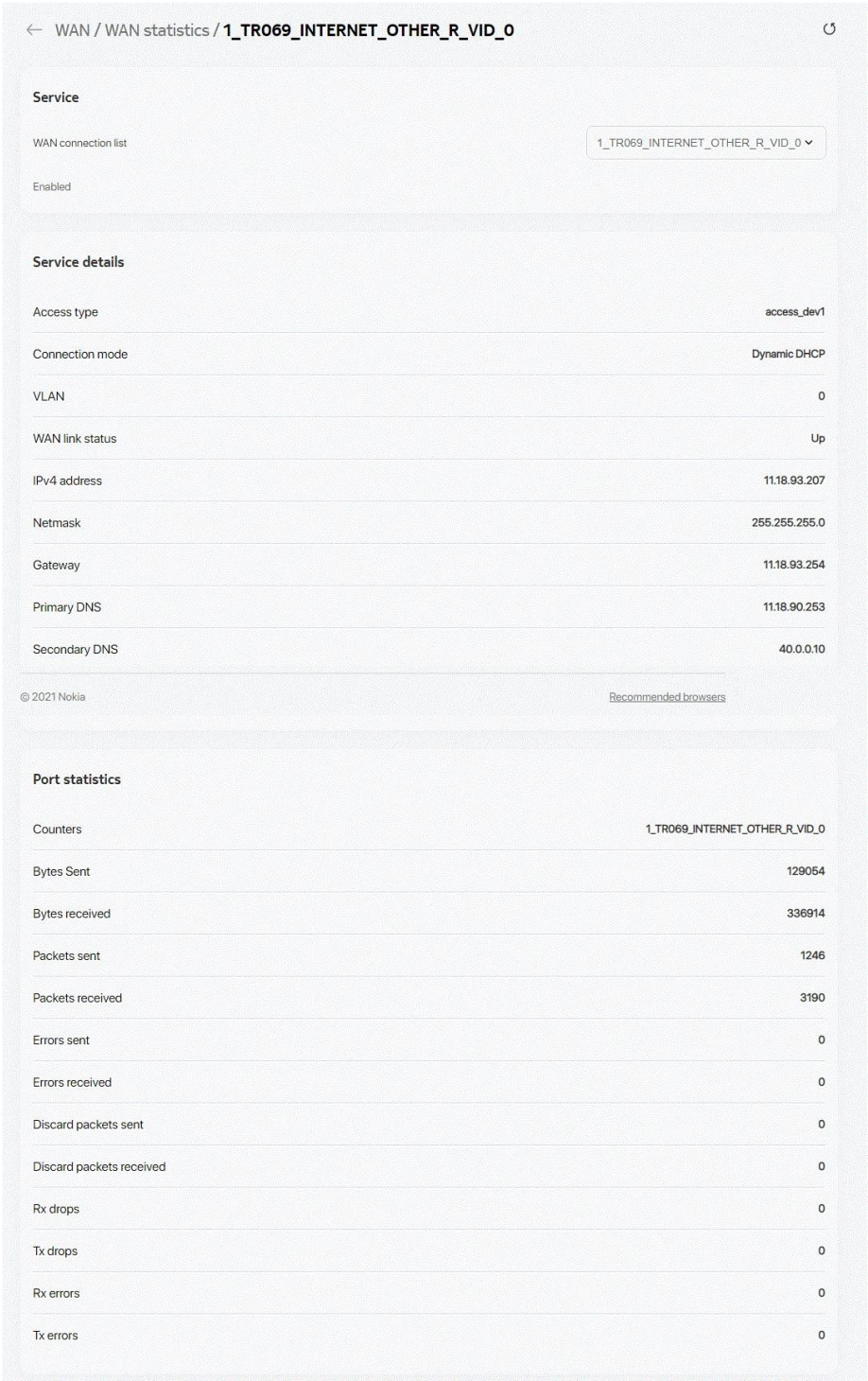


Table 7-3 WAN statistics parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
Enabled	Displays whether WAN connection is either enabled or disabled.
Service details	
Access type	Displays the access type.
Primary DNS	Displays the primary DNS address.
Secondary DNS	Displays the secondary DNS address.
Ethernet link status	Displays the Ethernet status link whether it is Up or Down.
Pri DNS(v6)	Displays the primary DNS address. This option is available when the IP mode is **IPv4 & IPv6** or **IPv6**.
Port statistics	
Counters	Displays the counters details.
Bytes sent/received	Displays the bytes sent and received.
Packets sent/received	Displays the packets sent and received.
Errors sent/received	Displays the errors sent and received.
Unicast packets sent/received	Displays the unicast packets sent and received.
Discard packets sent/received	Displays the discard packets sent and received.
Broadcast packets sent/received	Displays the broadcast packets sent and received.
Unknown proto packets received	Displays the proto packets received.
Rx/Tx drops	Displays the Rx/Tx dropped packets.
Rx/Tx errors	Displays the Rx/Tx error packets.

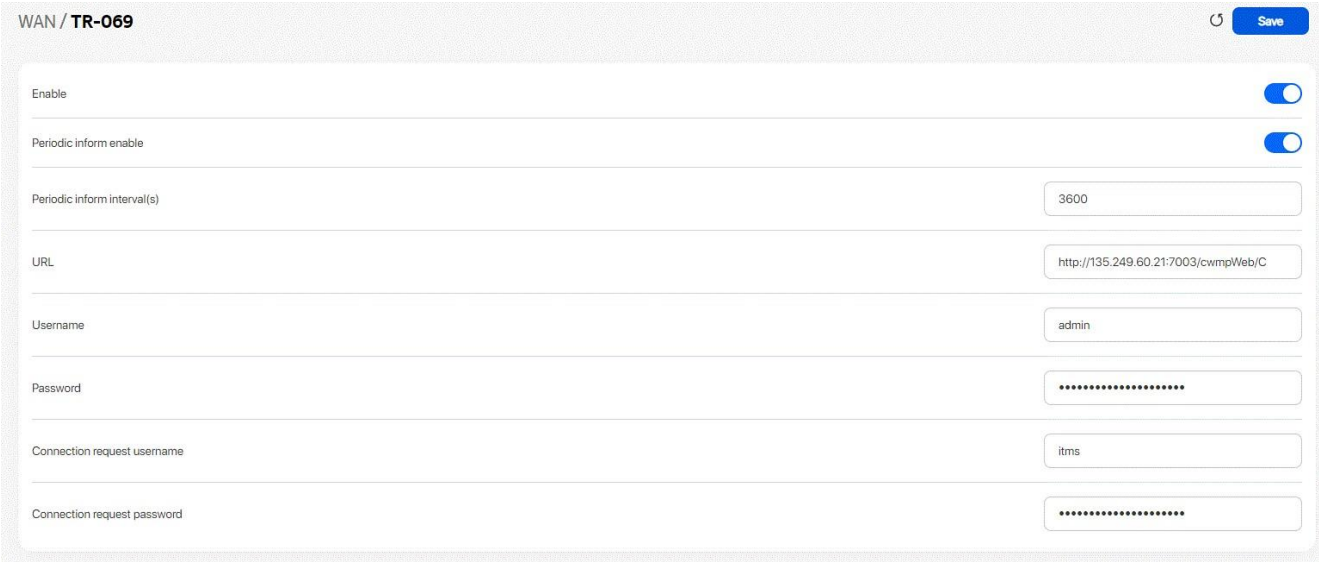
END OF STEPS

7.9 Configuring TR-069

1

Click **WAN→TR-069** in the left pane. The *TR-069* page displays.

Figure 7-9 TR-069 page



2

Configure the following parameters:

Table 7-4 TR-069 parameters

Field	Description
Enable	Select the toggle button to enable CWMP function.
Periodic inform enable	Select the toggle button to enable periodic inform updates.
Periodic inform interval(s)	Enter the time between periodic inform updates, in seconds.
URL	Enter the URL of the auto-configuration server. **Note:** When you enter a HTTP URL, a security warning is displayed that a HTTPS URL is recommended. Click **OK** to continue.
Username	Enter the username to log in to the Beacon.
Password	Enter the password to log in to the Beacon.
Connect request username	Enter the username to log in to the auto-configuration server.
Connect request password	Enter the password to log in to the auto-configuration server.

3

Click **Save**.

END OF STEPS

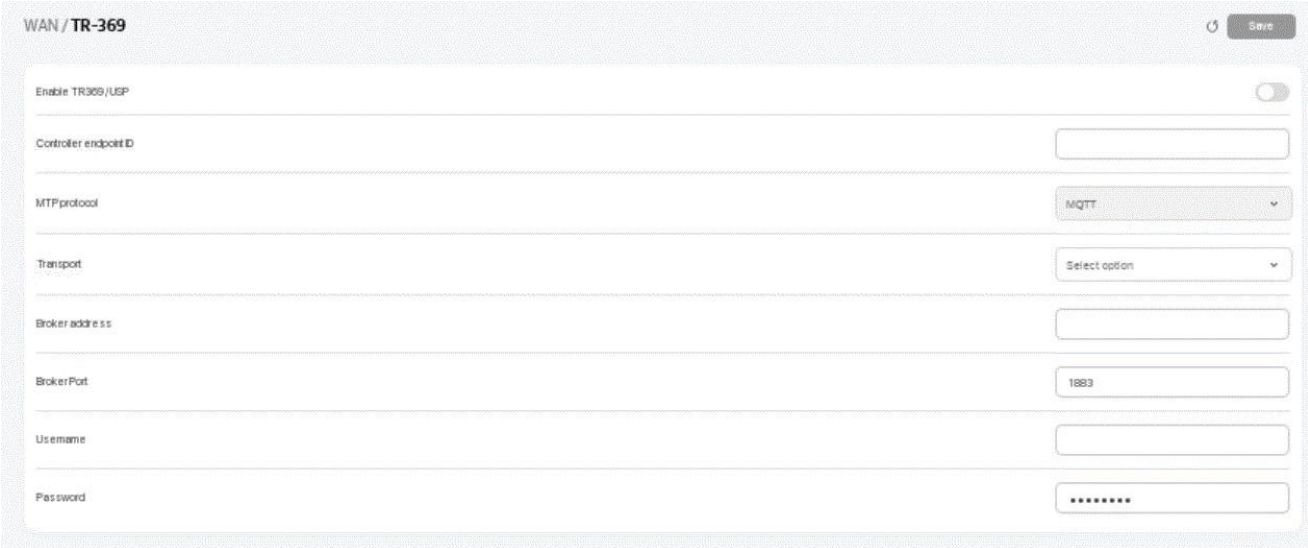
7.10 Configuring TR-369

Note: The TR-369 configuration option is available only if the TR-181 data model is active.

1

Click **WAN**→**TR-369** in the left pane. The *TR-369* page displays.

Figure 7-10 TR-369 page



2

Configure the following parameters:

Table 7-5 TR-369 parameters

Field	Description
Enable TR369/USP	Select the toggle button to enable TR-369/USP and click **Save**.
Controller endpoint ID	Enter the controller endpoint ID.
MTP Protocol	Select the MTP protocol from the list (currently only **MQTT** is supported).
Transport	Select the transport option from the list: • **TCP/IP** • **TLS** **Note:** If you attempt to change the configuration from TLS to TCP/IP, a security warning is displayed that this option poses security risks. Click **OK** to continue.
Broker address	Enter the broker IP address.

Table 7-5 TR-369 parameters (continued)

Field	Description
Broker port	Enter the broker port number.
Username	Enter the username to authenticate with MQTT broker.
Password	Enter the password to authenticate with MQTT broker.

3

Click **Save**.

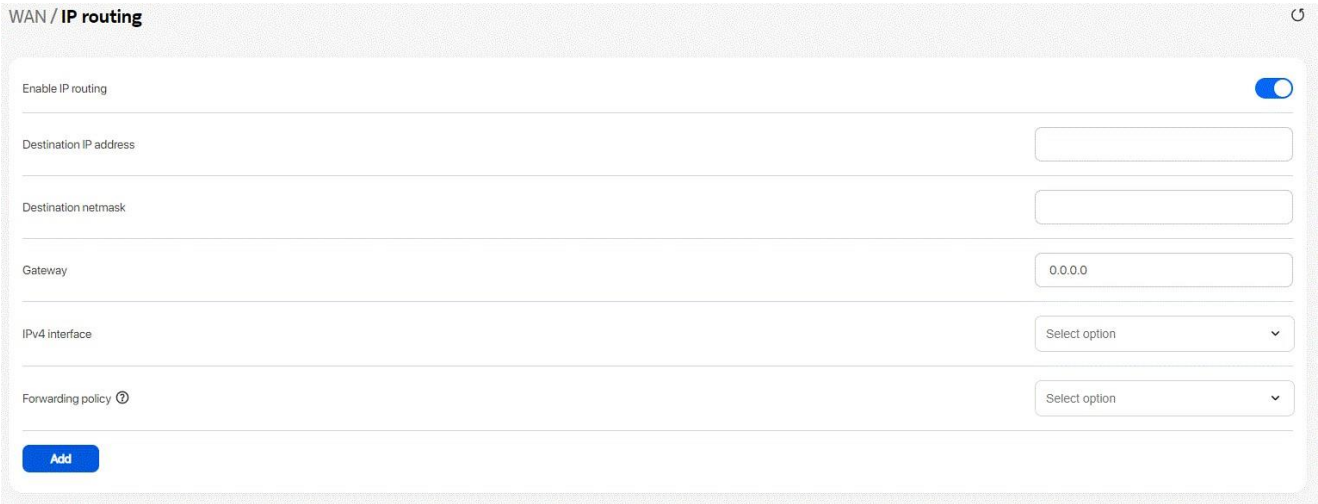
END OF STEPS

7.11 Configuring Static routing

1

Click **WAN→Static routing** in the left pane. The *IP routing* page displays.

Figure 7-11 IP routing page



2

Configure the following parameters:

Table 7-6 IP routing parameters

Field	Description
Enable IP routing	Select the toggle button to enable IP routing.

Table 7-6 IP routing parameters (continued)

Field	Description
Destination IP address	Enter the destination IP address.
Destination netmask	Enter the destination netmask.
Gateway	Enter the gateway IP address.
IPv4 interface	Select an IPv4 interface from the list.
Forwarding policy	Select a forwarding policy from the list.

3

Click **Add**. The IP route is added to the *IP routing table*.

END OF STEPS

7.12 Configuring QoS

1

Click **WAN→QoS config** in the left pane. The *QoS config* page displays.

Figure 7-12 QoS config page (L2 Criteria)

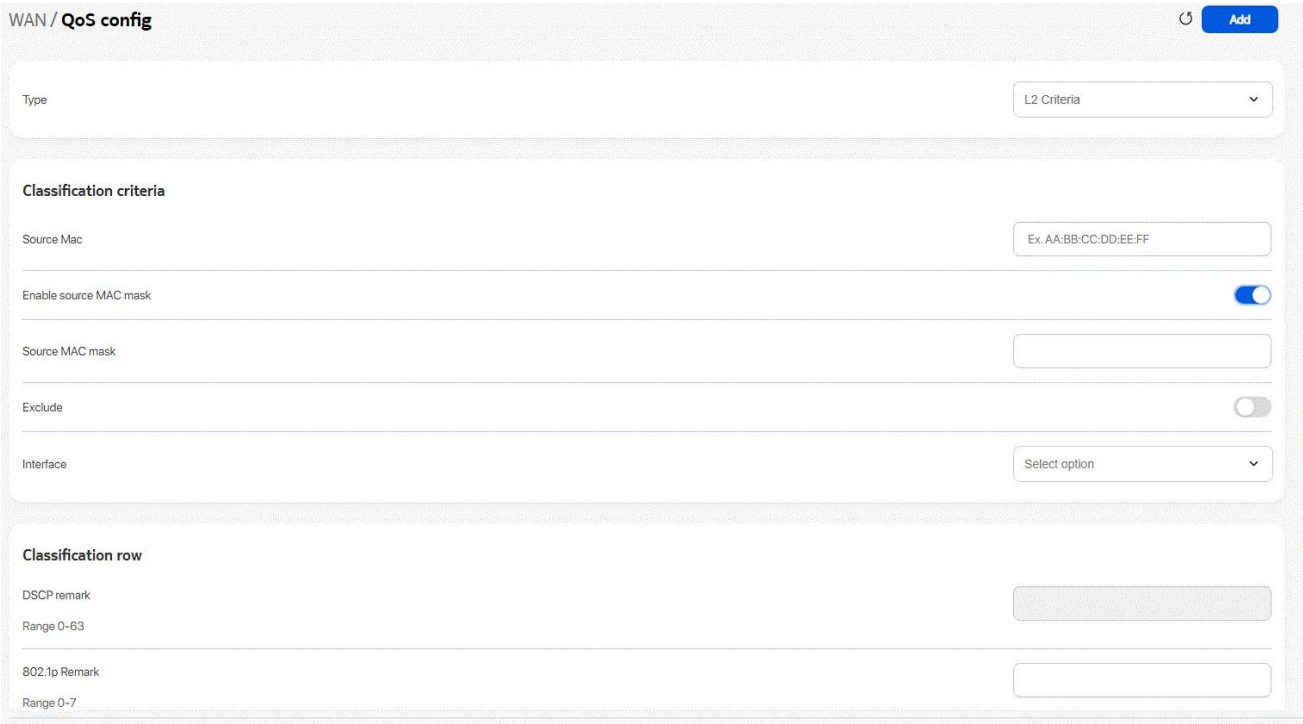
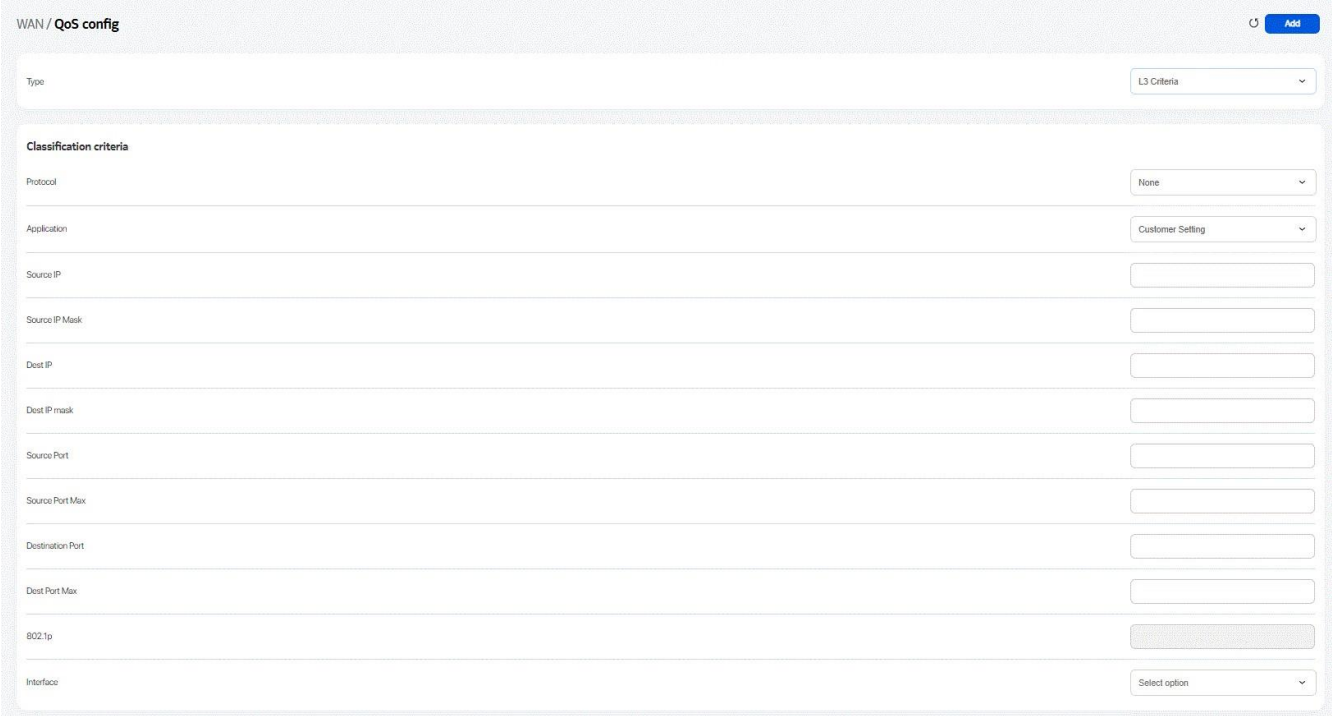


Figure 7-13 QoS config page (L3 Criteria)



2

Configure the following parameters:

Table 7-7 QoS config parameters

Field	Description
Type	Select a QoS service layer type from the list: • **L2 Criteria** • **L3 Criteria**
Classification criteria (L2)	
Source MAC	Enter the source MAC address.
Enable source MAC mask	Select the toggle button to enable the source MAC mask. This button is disabled by default.
Source MAC mask	Enter the source MAC mask address. The syntax is for example: FF:FF:FF:00:00:00 which must be a continuous bit mask pattern on this device. This field is visible only if the **Enable source MAC mask** button is enabled.
Interface	Select an interface from the list.

Table 7-7 QoS config parameters (continued)

Field	Description
Classification criteria (L3)	
Protocol	Select a protocol from the list.
Application	Select an application from the list or select **Custom Settings** and enter an application name.
Source IP	Enter the source IP address.
Source IP mask	Enter the source IP address netmask.
Destination IP	Enter the destination IP address.
Destination IP mask	Enter the destination IP address netmask.
Source port	Enter the source port number.
Source port max	Enter the values for the source port max (highest port number)
Destination port	Enter the destination port number.
Destination port max	Enter the values for the destination port max (highest port number)
802.1p	Indicates whether 802.1p is enabled.
Interface	Select an interface from the list.
Classification row	
DSCP remark	Enter the value for the DSCP remark (applicable only for L3 criteria). Allowed values: 0 to 63
802.1p Remark	Enter the value for the 802.1p remark. Allowed values: 0 to 7
Forwarding policy	Enter the number for the forwarding policy. Allowed values: 1 to 7

3

Click **Add** to add a QoS policy.

END OF STEPS

LAN Configuration

7.13 Overview

This section describes the LAN configuration procedures that can be performed from the following sub-menu options under the **LAN** menu:

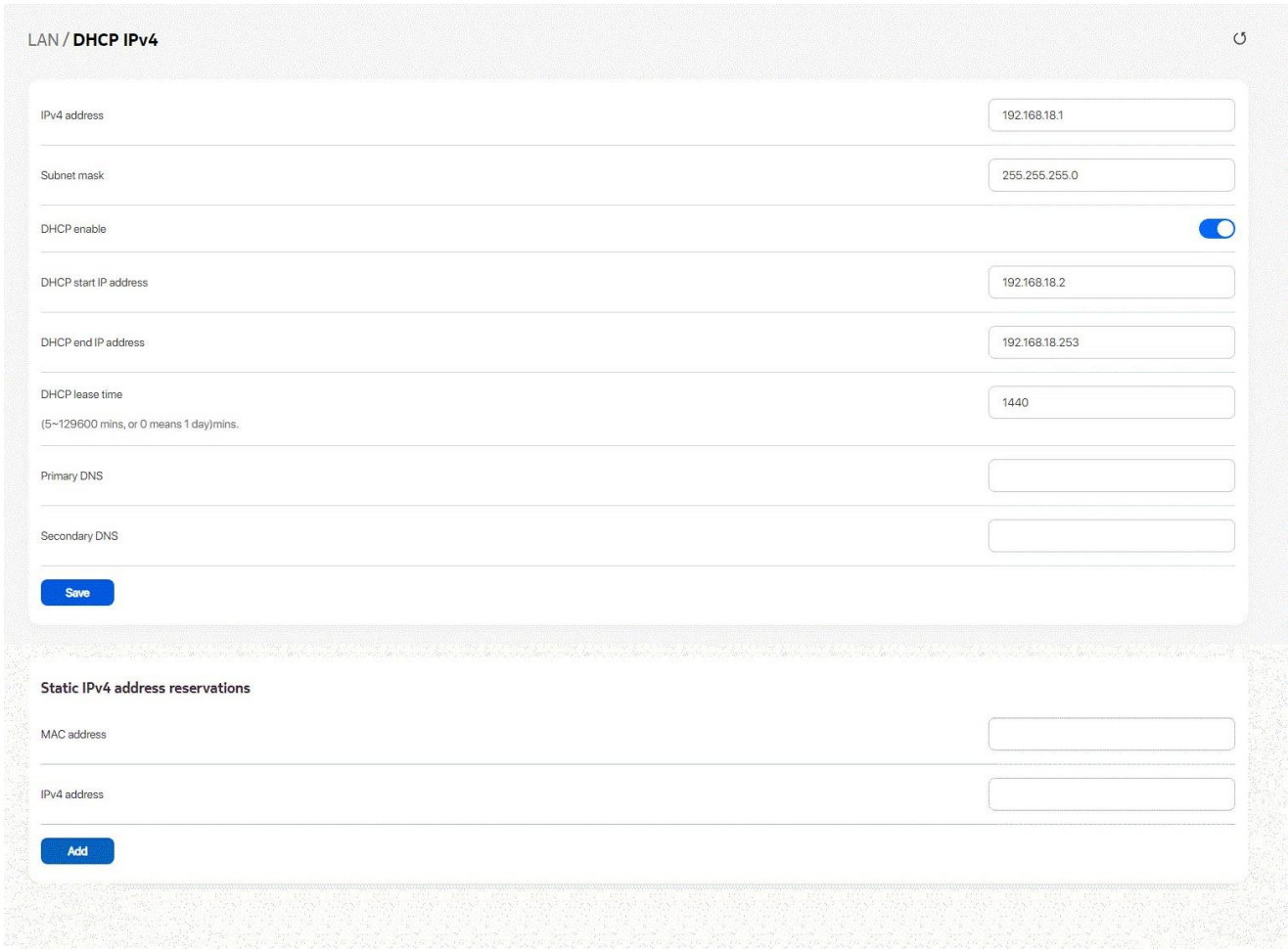
Sub-menu	Procedure
DHCP IPv4	7.14 “Configuring DHCP IPv4” (p. 86)
DHCP IPv6	7.15 “Configuring DHCP IPv6” (p. 88)
DNS	7.16 “Configuring DNS” (p. 90)
LAN statistics	7.17 “Viewing LAN Statistics” (p. 93)

7.14 Configuring DHCP IPv4

1

Click **LAN→DHCP IPv4** in the left pane. The *DHCP IPv4* page displays.

Figure 7-14 DHCP IPv4 page



2

Configure the following LAN parameters:

Table 7-8 DHCP IPv4 parameters

Field	Description
IPv4 address	Enter the IPv4 address of the Beacon.
Subnet mask	Enter the subnet mask of the Beacon.
DHCP enable	Select the toggle button to enable DHCP. If this toggle button is not enabled, the DHCP functionality cannot be used. you need not configure DHCP start IP address, DHCP end IP address and DHCP lease time if this toggle button is not enabled.

Draft

Table 7-8 DHCP IPv4 parameters (continued)

Field	Description
DHCP start IP address	Enter the starting range of the DHCP IP address.
DHCP end IP address	Enter the ending range of the DHCP IP address.
DHCP lease time	Enter the DHCP lease time (in minutes). Allowed values: 5 to 129600 minutes or 0 for 1 day
Primary DNS	Enter the primary DNS IP address.
Secondary DNS	Enter the secondary DNS IP address.

3

Click **Save**.

4

Configure the Static DHCP parameters.

Table 7-9 Static DHCP parameters

Field	Description
MAC address	Enter the hexadecimal MAC address to associate with the LAN.
IPv4 address	Enter the IPv4 address to associate with the bound MAC address.

5

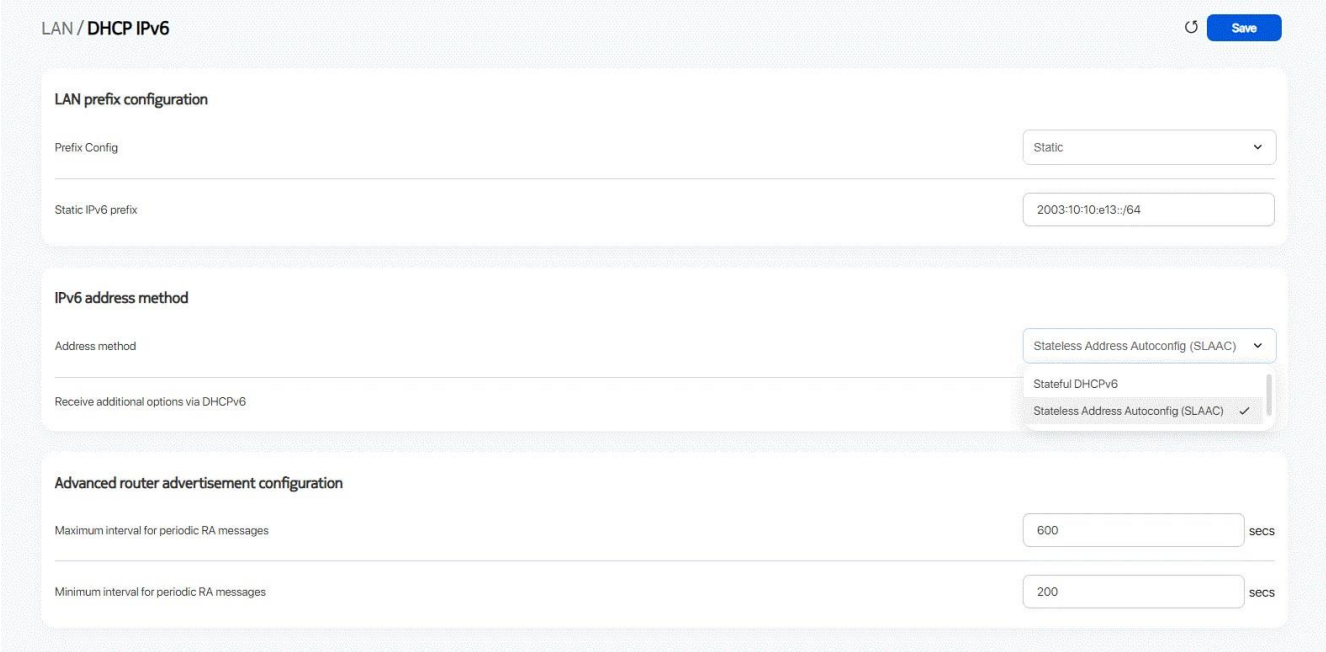
Click **Add**. Repeat steps 4 and 5 for all MAC addresses to be bound.

END OF STEPS

7.15 Configuring DHCP IPv6

1

Click **LAN→DHCP IPv6** in the left pane. The *DHCP IPv6* page displays.



2

Configure the following parameters:

Table 7-10 DHCP IPv6 parameters

Field	Description
LAN prefix configuration	
Prefix Config	Select a prefix configuration option from the list: • **Use WAN provided prefix** (prefix is obtained from the WAN) • **Static** (enables you to enter the prefix)
Interface	This field displays if you select the **Use WAN provided prefix** option from the Prefix Config list. Select a WAN connection interface from the list.
Received IPv6 prefix	This field displays the received IPv6 prefix. This field is displayed only when **Prefix Config** is set to **Use WAN provided prefix**.
Static IPv6 prefix	This field displays the static IPv6 prefix. This field is displayed only when **Prefix Config** is set to **Static**.
IPv6 address method	
Address method	Select a address method option from the list: • **Stateless Address Autoconfig (SLAAC)** • **Stateful DHCPv6**

Table 7-10 DHCP IPv6 parameters (continued)

Field	Description
DHCP Start IP Address	Enter the starting range of the DHCP IP address. This parameter is visible only if the address method is **Stateful DHCPv6**.
DHCP End IP Address	Enter the ending range of the DHCP IP address. This parameter is visible only if the address method is **Stateful DHCPv6**.
Enable stateless and stateful DHCPv6 simultaneously	Select the toggle button to enable stateless or stateful DHCPv6 simultaneously. This parameter is visible only if the address method is **Stateful DHCPv6**.
Received additional options via DHCPv6	Select the toggle button to enable additional options via DHCPv6. This field is displayed only when **Address method** is set to **Stateless Address Autoconfig (SLAAC)**.
Enable stateless and stateful DHCPv6 simultaneously	Select the toggle button to enable stateless and stateful DHCPv6 simultaneously. This field is displayed only when **Address method** is set to **Stateful DHCPv6**.
Advanced router advertisement configuration	
Maximum interval for periodic RA messages	Enter the maximum interval (in seconds) for periodic Router Advertisement messages. Allowed values: 4 to 1800 seconds
Minimum interval for periodic RA messages	Enter the minimum interval (in seconds) for periodic Router Advertisement messages. Allowed values: 4 to 1800 seconds

3

Click **Save**.

END OF STEPS

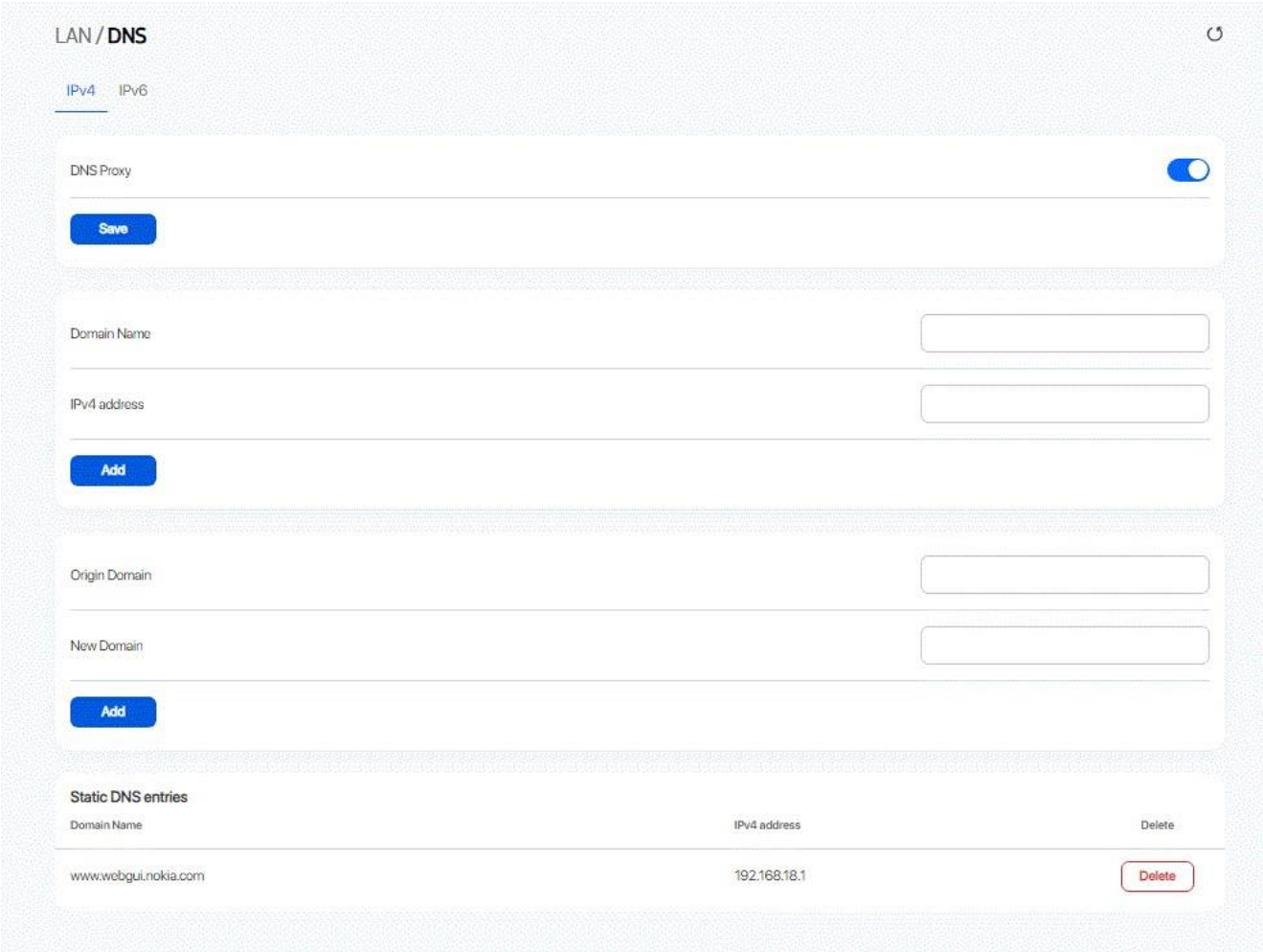
7.16 Configuring DNS

7.16.1 IPv4 DNS configuration

1

Click **LAN→DNS→IPv4** in the left pane. The *DNS* page displays.

Figure 7-15 DNS page (IPv4)



2

Configure the following parameters:

a. Select the **DNS proxy** toggle button to enable the DNS proxy and click **Save**.

b. Configure the following:

   1. Enter the domain name in the Domain Name field.
   2. Enter the domain IP address in the IPv4 Address field.
   3. Click **Add**.

c. Configure the following:

   1. Enter the origin domain name in the Origin Domain field.
   2. Enter the new domain name in the New Domain field.

3. Click **Add** to associate an origin domain with a new domain.

The *DNS* table displays the configured domain names and the associated IPv4 address. Click **Delete** to delete the table entries.

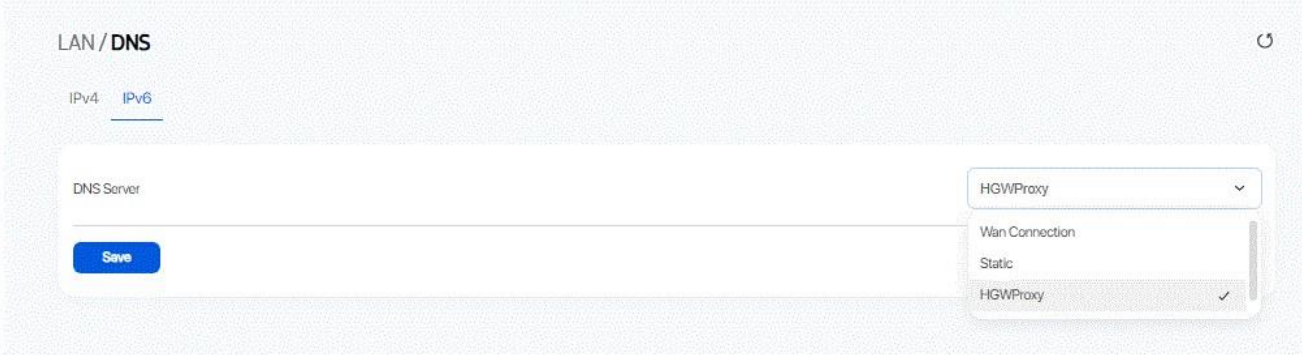
END OF STEPS

7.16.2 IPv6 DNS configuration

1

Click **LAN→DNS→IPv6** in the left pane. The *DNS* page displays.

Figure 7-16 DNS page (IPv6)



2

Configure the following parameters

Table 7-11 DNS parameters

Field	Description
DNS Server	Select DNS server option from the list: • **Wan Connection** (Server address is obtained from the WAN.) • **Static** (enables you to enter the address.) • **HGWProxy** (The Home Gateway acts as DNS Proxy).
Preferred DNS	Enter the preferred IPv6 address. This parameter is visible only if the DNS Server is **Static**.
Alternate DNS	Enter the Alternate IPv6 address. This parameter is visible only if the DNS Server is **Static**.
Interface	This field is displayed if you select the **Wan Connection** option from the DNS Server list.

Draft

3

Click **Save**.

END OF STEPS

7.17 Viewing LAN Statistics

1

Click **LAN→LAN statistics** in the left pane. The *LAN statistics* page displays the following information.

Figure 7-17 LAN statistics page

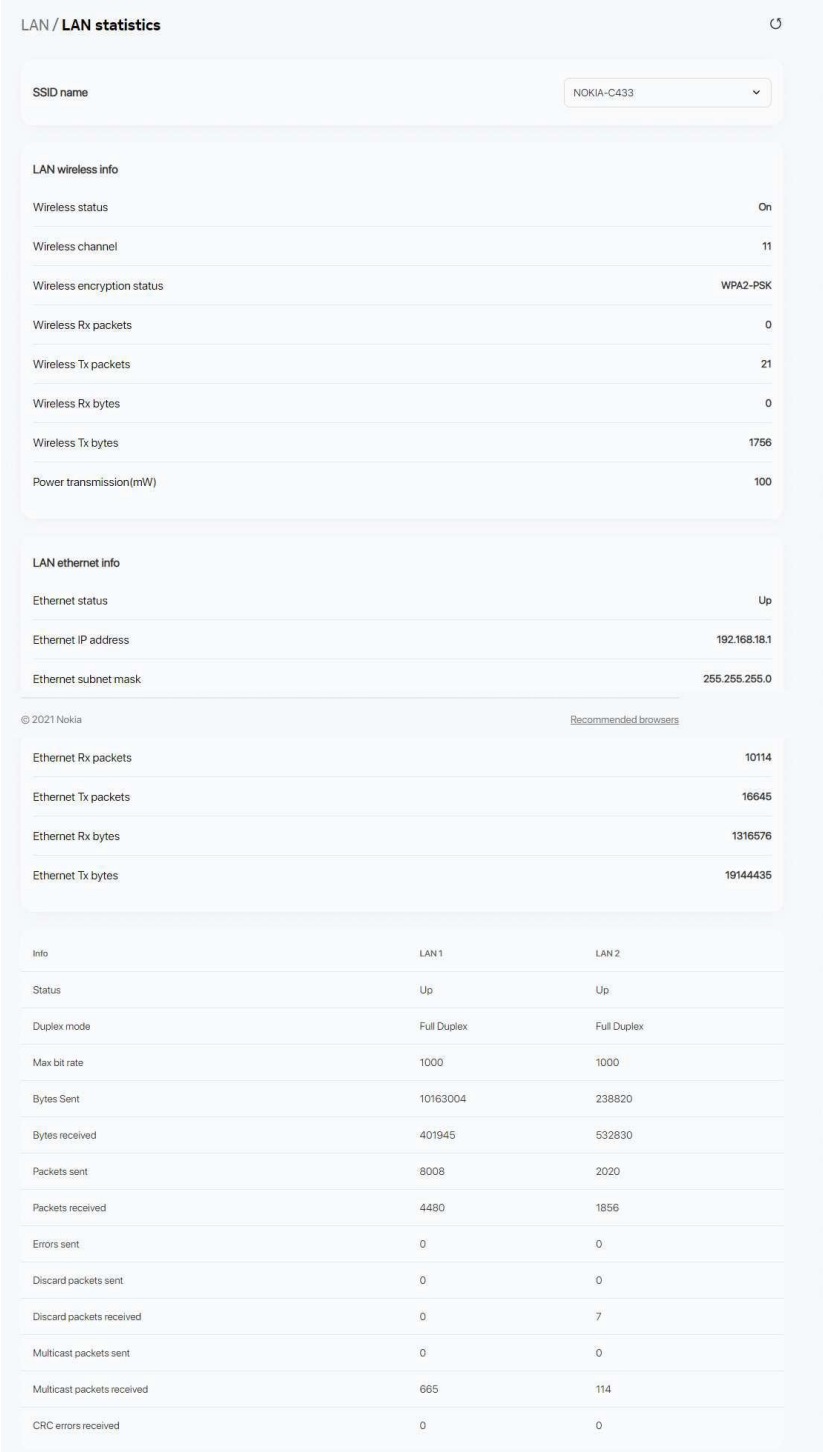


Table 7-12 LAN statistics parameters

Field	Description
SSID name	Select an SSID from the list.
LAN Wireless info	Displays the wireless status, wireless channel, encryption status, received and transmitted bytes and packets and power transmission in mW.
LAN Ethernet info	Displays the Ethernet status IP address, subnet mask, MAC address, received and transmitted bytes and packets.
Info	Displays the information of each such as status, duplex mode, maximum bit rate, packets received and sent, CRC errors, and so on.

END OF STEPS

WiFi Configuration

7.18 Overview

This section describes the WiFi configuration procedures that can be performed from the following sub-menu options under the **WiFi** menu:

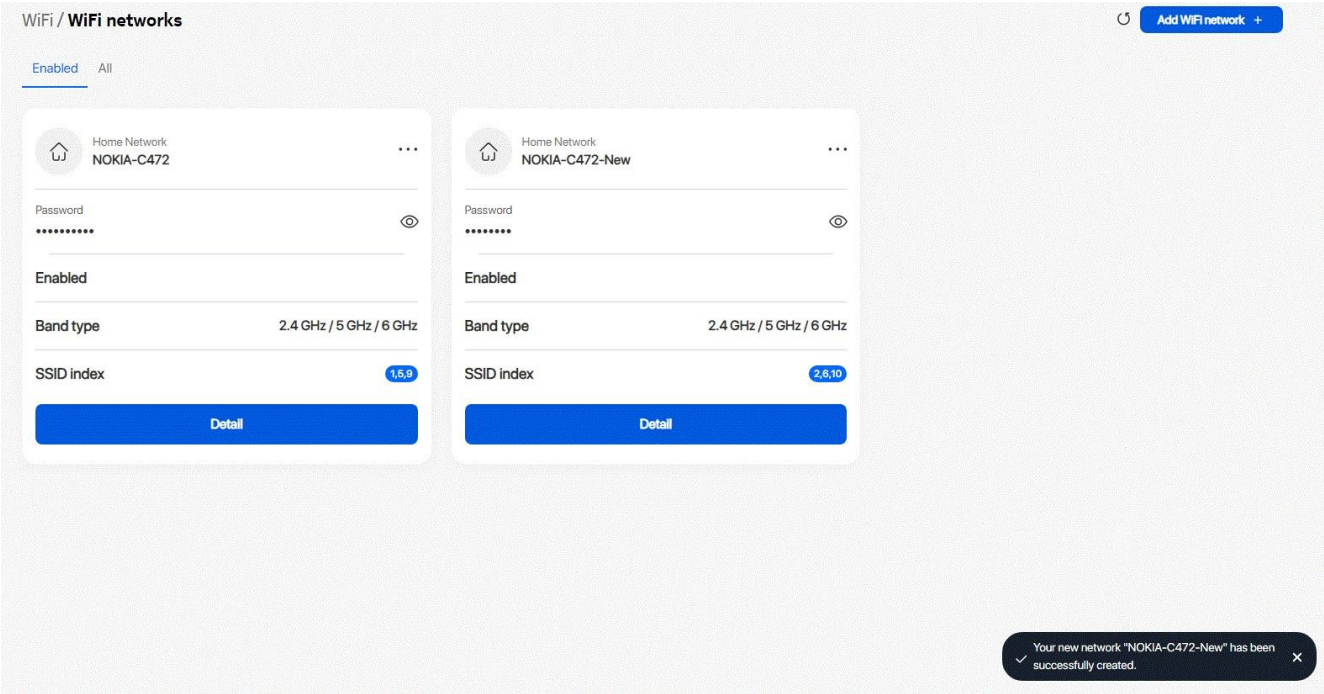
Sub-menu	Procedure
WiFi networks	7.19 “Configuring WiFi Network” (p. 96)
Guest network	7.20 “Configuring Guest Network” (p. 102)
Network map	7.21 “Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points” (p. 103)
Advanced settings	7.22 “Configuring Wireless 2.4 GHz” (p. 109)
WiFi statistics	7.25 “Viewing WiFi Statistics” (p. 114)

7.19 Configuring WiFi Network

1

Click **WiFi→WiFi network** in the left pane. The *WiFi network* page displays the existing WiFi networks. You can click **Detail** on a network to view the network details.

Figure 7-18 WiFi network page

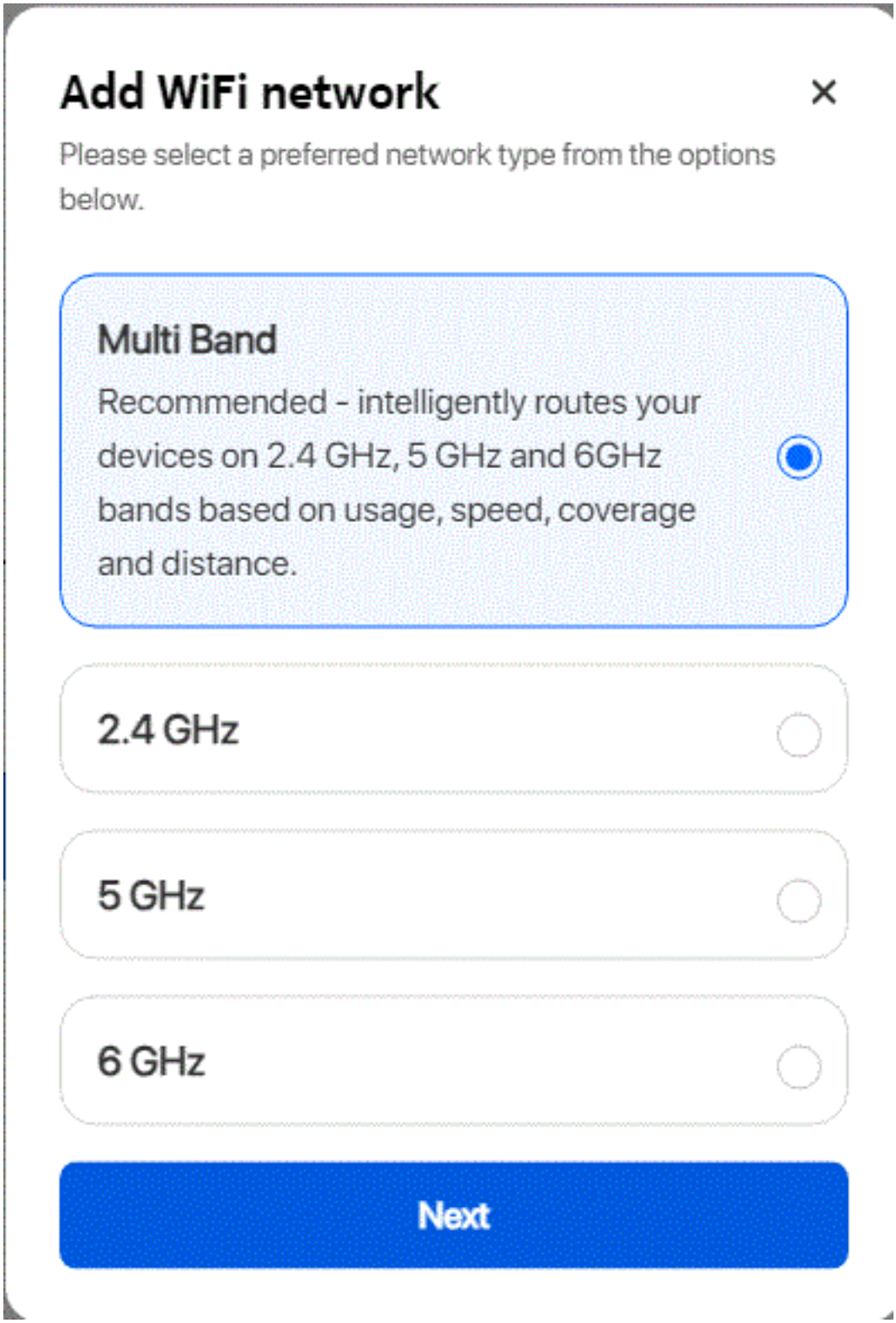


2

Click **Add WiFi network +** to create a WiFi network. The *Add WiFi network* page displays.

Note: The **Add WiFi point** option is displayed only when the mesh feature is enabled.

Figure 7-19 Add WiFi network page



3

Configure the following parameters:

Table 7-13 Add WiFi network parameters

Field	Description
Multiband	Select this option to configure a multiband wireless network. This option is recommended your devices on 2.4 GHz or 5 GHz bands based on usage, speed, coverage and distance.
2.4 GHz	Select this option to configure a 2.4 GHz wireless network.
5 GHz	Select this option to configure a 5 GHz wireless network.
6 GHz	Select this option to configure a 6 GHz wireless network.

4

Click **Next**.

5

Enter the name of your network in the Name field and click **Save**.

6

Enter the password for the network in the Password field and click **Save**.

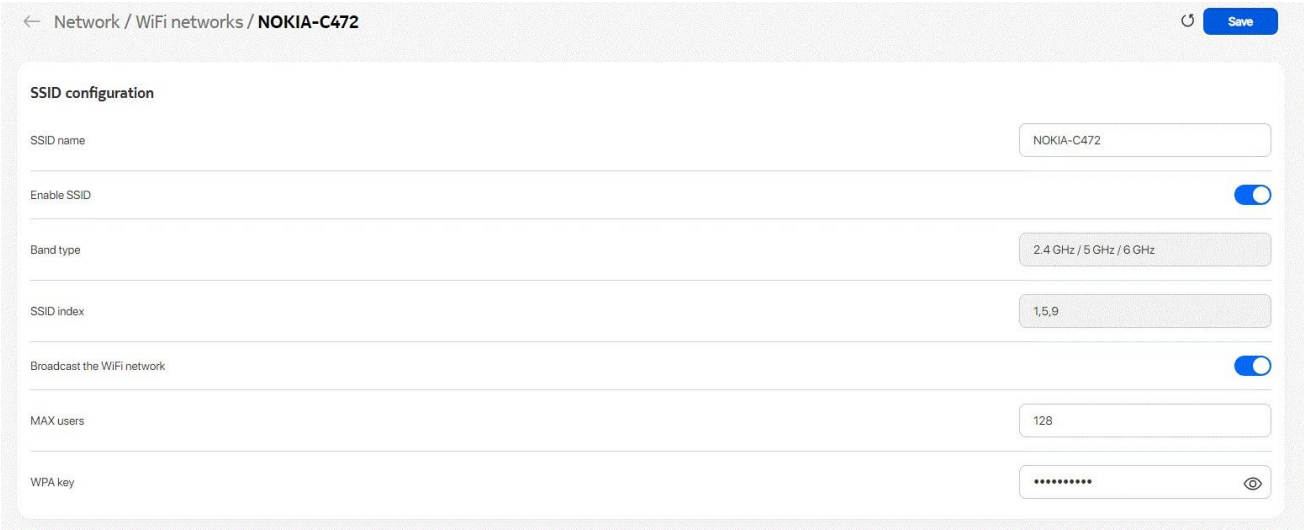
The WiFi network is created and is displayed as a card in the **Enabled** tab of the *WiFi networks* page.

Note: You can click the ellipsis icon on the card of your WiFi network and select **Edit** to edit and save the network name and password.

7

Click **Detail** to view and edit the SSID configuration for your network.

Figure 7-20 WiFi network - example of SSID Configuration page



8

Configure the following parameters:

Field	Description
SSID name	Displays the SSID name.
Enable SSID	Select the toggle button to enable SSID.
Band type	Displays the band type.
SSID index	Displays the SSID index.
Broadcast the WiFi network	Select the toggle button to enable broadcasting of the WiFi network.
Guest Mode	Indicates whether guest mode is enabled or disabled. When a particular SSID is enabled with Guest Mode, LAN devices connected to the SSID can only connect to the Internet. Such devices cannot see or communicate with other LAN devices.
MAX users	Enter the maximum number of users.

Field	Description
Encryption Mode	In case of 2.4 GHz band type, select an encryption mode from the list: • **WPA2 Personal** • **WPA/WPA2 Personal** • **WPA3 Personal** • **WPA2/WPA3 Personal** • **WPA/WPA2 Enterprise** • **Open** In case of 5 GHz band type, select an encryption mode from the list: • **WPA2-AES** • **WPA2+WPA** • **WPA/WPA2 Enterprise** • **WPA3+WPA2** • **WPA3** • **NONE-OPEN** In case of 6 GHz band type, select an encryption mode from the list: • **WPA3** **Notes:** • If you select OPEN, a security warning is displayed that this option poses a security risk. Click **OK** to continue. • When you select WPA/WPA2 Personal, WPA/WPA2 Enterprise for 2.4Ghz and WPA2+WPA, WPA/WPA2 Enterprise for 5Ghz, a security warning is displayed that WPA is an outdated encryption mechanism, and that WPA2 or WPA3 is recommended. • If you select WPA3, a warning is displayed as follows, 'Enabling WPA3 encryption on your wireless network enhances security, but it may not be compatible with all devices. Some older devices may not connect unless updated, so be prepared for possible compatibility issues. Ensure you have a strong, memorable password for WPA3 and consider using a legacy encryption method for older devices to ensure they can connect to your network securely. Are you sure you want to proceed?'.
WPA version	WPA version is displayed when the encryption mode is selected: • **WPA2** • **WPA/WPA2** • **WPA3** • **WPA2/WPA3** This parameter is visible only if the band type is 2.4 GHz.
WPA Encryption Mode	Select a WPA encryption mode from the list: • **AES** • **TKIP/AES** This parameter is visible only if the band type is 2.4 GHz.
WPA Key	Enter the WPA key.
Enable WPS	Select the toggle button to enable WPS. **Note:** When you select Enable, a security warning is displayed. Click **OK** to continue.

Notes:

1. When Encryption Mode is set to “WPA/WPA2 Enterprise”, the following options are no longer available: WPA encryption mode, WPA key, Enable WPS, WPS mode.
2. When Encryption Mode is set to “WPA/WPA2 Enterprise”, the following options become available: Primary RADIUS server, port and password; RADIUS accounting port.
3. The EasyMesh standard does not support synchronizing WPA3-only mode to the other nodes that participate in the mesh. For this reason, the WPA3 (only) mode should not be used on devices that participate in an EasyMesh mesh. Instead, WPA2/WPA3 mode should be used, as is also mentioned in the EasyMesh standard.

9

Click **Save**.

END OF STEPS

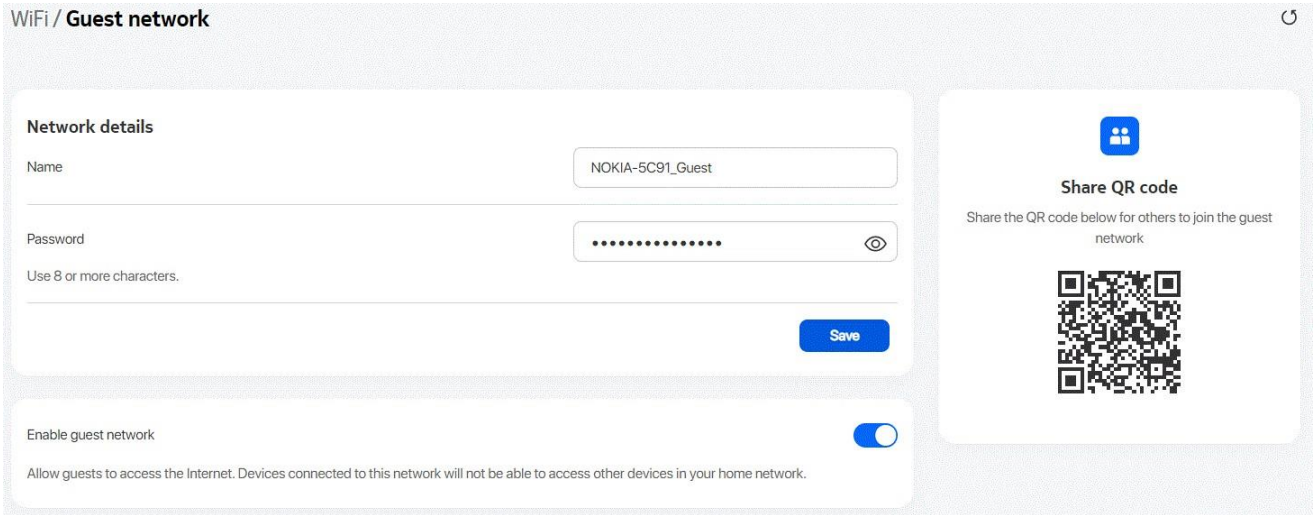
7.20 Configuring Guest Network

Note: Guest WiFi function is not supported.

1

Click **WiFi→Guest network** in the left pane. The *Guest network* page displays the network details.

Figure 7-21 Guest network page



2

Configure the following parameters:

Table 7-14 Guest network parameters

Field	Description
Name	Enter the name for guest network.
Password	Enter a password for guest network. Click **Save**.
Enable guest network	Select this toggle button to enable guest WiFi. Enabling the Guest SSID creates a multiband network (2.4GHz and 5GHz). Atleast one 2.4GHz and one 5GHz SSID index must be available to enable Guest network. After enabling the Guest Network a new WiFi card can be seen in WiFi networks page and Overview page with Guest SSID details.

3

Share the QR code for others to join the guest network.

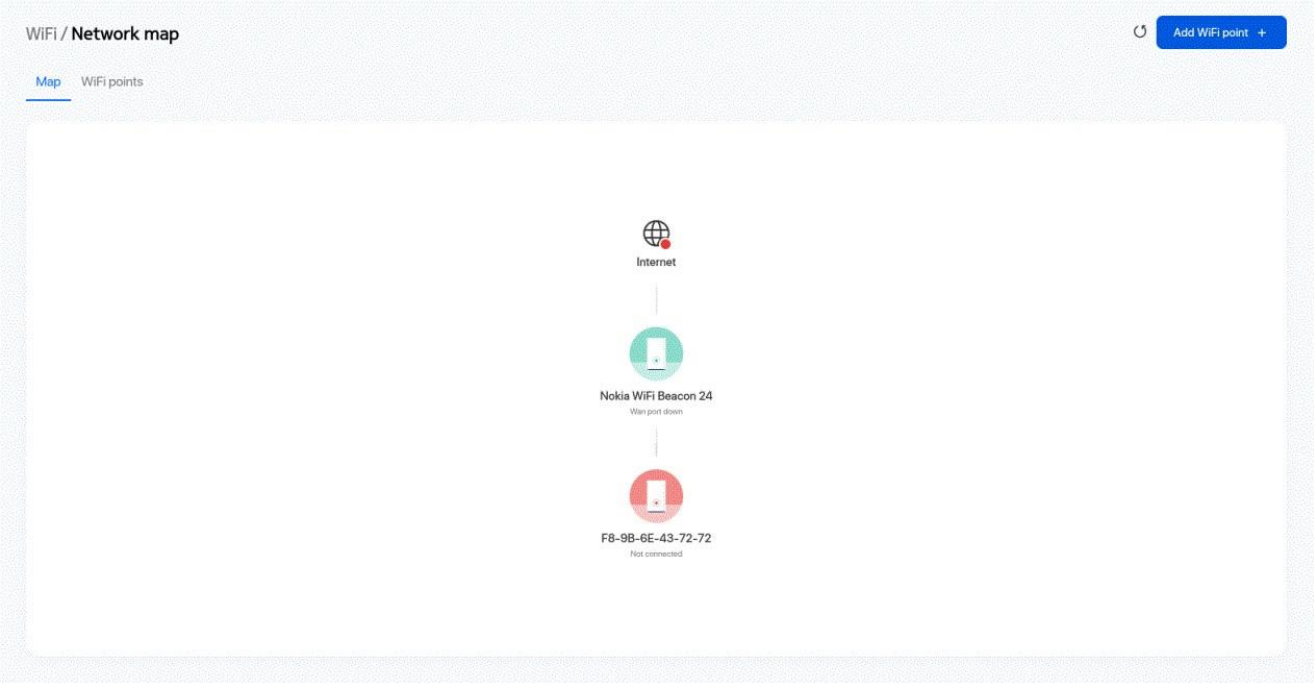
END OF STEPS

7.21 Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points

1

Click **WiFi→Network map** in the left pane. The *Network map* page displays the WiFi points added to the network.

Figure 7-22 Network map page



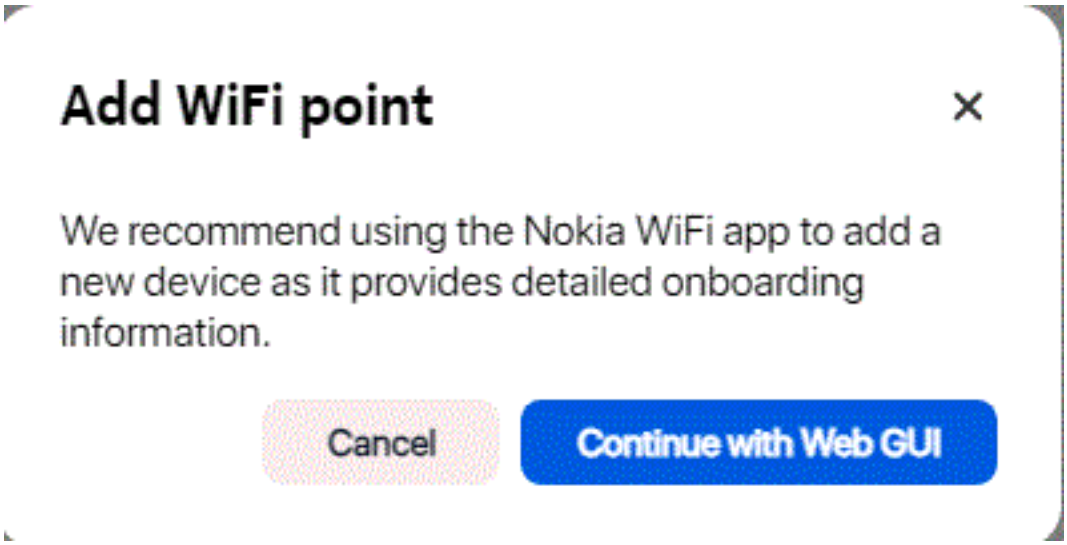
2

Perform the following steps to add a WiFi point:

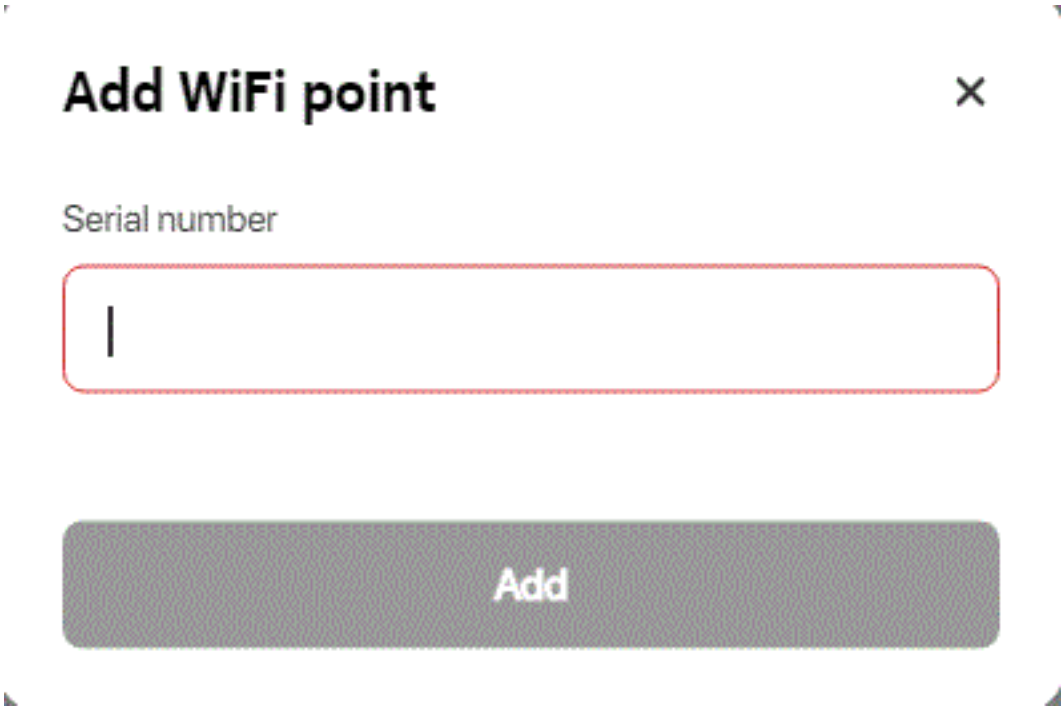
a. Click **Add WiFi point** at the top right corner of the *Device Info* page. A message displays that it is recommended to use the Nokia WiFi mobile app to add a WiFi point.

b. To add a WiFi point using the WebGUI, click **Continue with WebGUI**.

Draft



c. In the *Add WiFi point* page, enter the serial number and click **Add**.

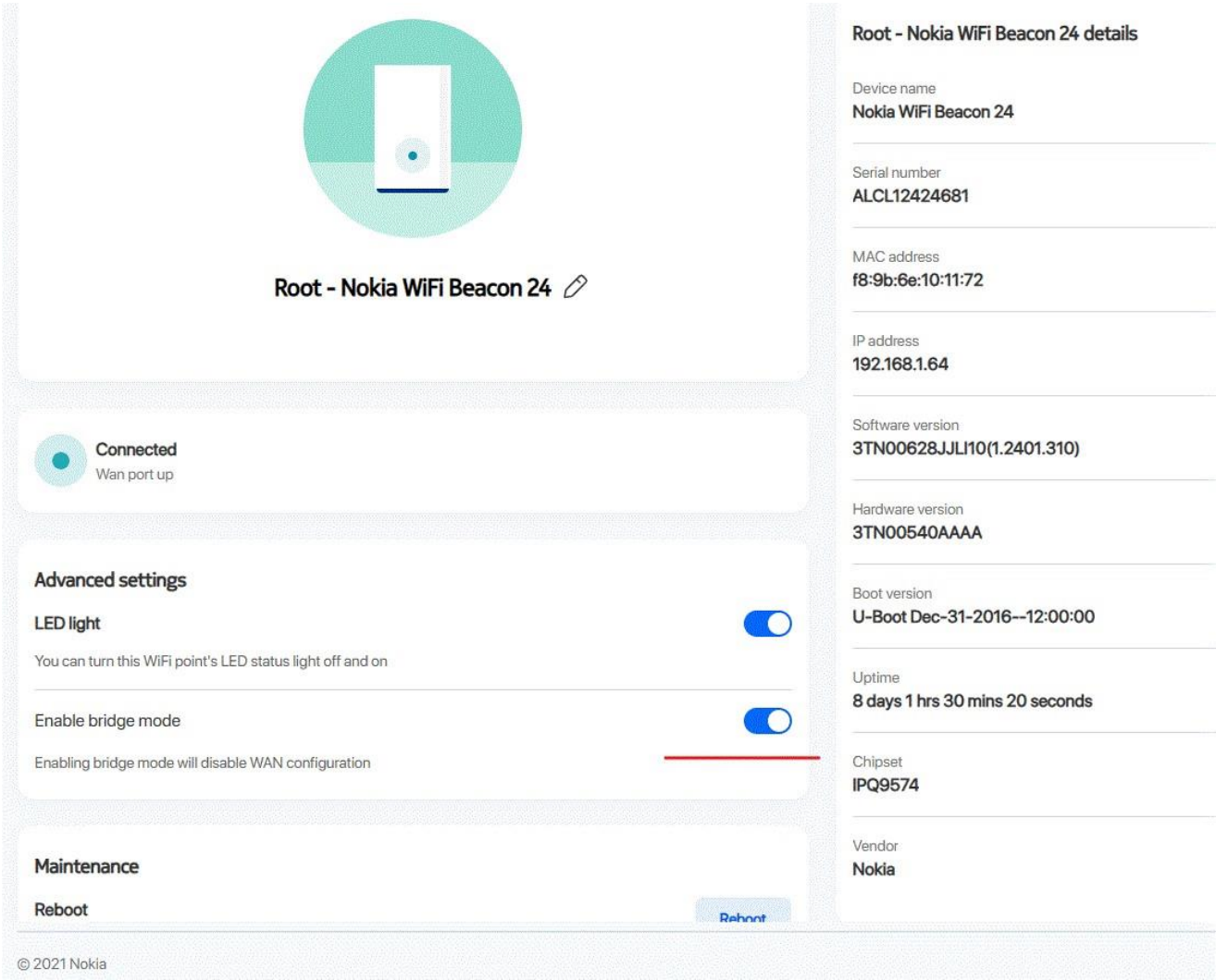


The WiFi point is displayed in the *Detected* or *Not detected* list of the *Onboarding Status* panel in the *Device Info* page.

3

Click on a WiFi point to view the device details. The <*Device*> page displays the details of the selected device in the network, including connection status.

Figure 7-23 <Device> page



4

The WiFi point name can be edited by clicking the edit icon .

Perform the following steps to change the name of your WiFi point:

a. To edit the name of the WiFi point, click the Edit icon . The **Change the name of your WiFi point** page displays.

b. On the page **Change the name of your WiFi point**, click the drop-down menu to select a name for the WiFi point, or enter a **Custom name** to create your own customized name.

c. Click **Save**.

Figure 7-24 Change the name of your WiFi point page

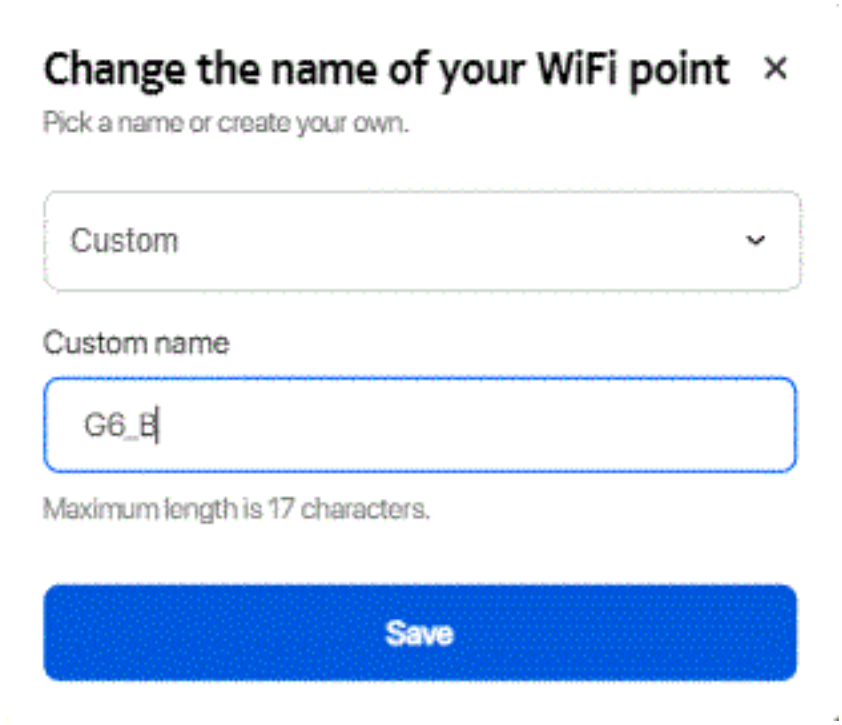


Table 7-15 <*Device*> parameters

Field	Description
Device name	Name on the device
Serial number	Serial number of the device
MAC address	MAC address of the device
IP address	IP address of the device
Software version	Software version of the device (displays only for a root device)
Hardware version	Hardware version of the device (displays only for a root device)
Boot version	Boot version of the device (displays only for a root device)
Uptime	Amount of time the device has run since last reset in hours, minutes, and seconds (displays only for a root device)
Chipset	Chipset of the device (displays only for a root device)

Table 7-15 <*Device*> parameters (continued)

Field	Description
Vendor	Name of the vendor (displays only for a root device)
Onboarding status	Onboarding status of the device in the WiFi network (displays only for an extender device)
Backhaul status	Backhaul status of the device (displays only for an extender device)
Location nickname	Name of the location of the device (displays only for an extender device)

5

Click **LED Light** to enable the LED light on the device.

6

Perform any of the following, as applicable:

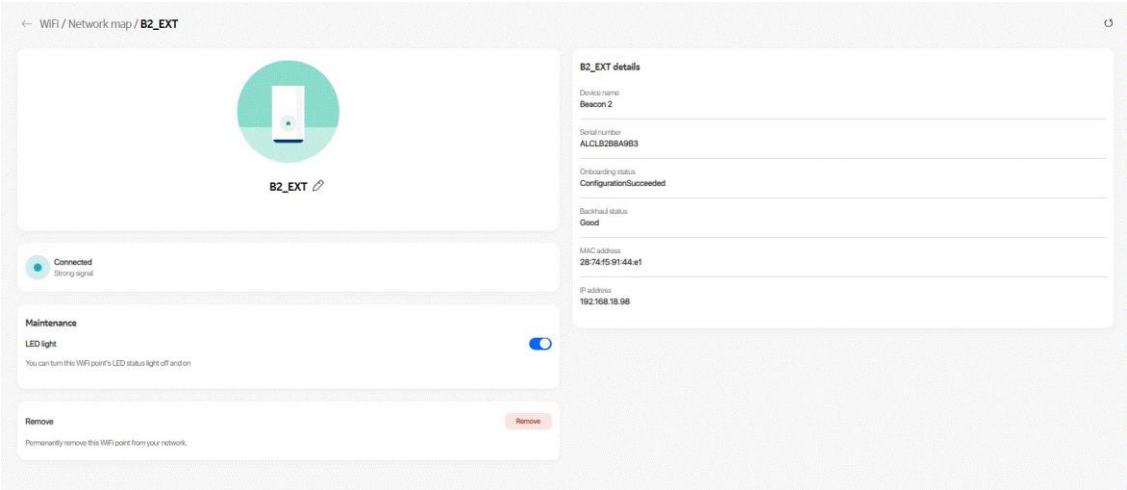
- **Reboot the device:**
  1. Click **Reboot**. A message displays asking if you want reboot the device.
  2. Click **OK** to reboot the Beacon. The device reboots and displays the login page.
- **Reset the device to factory default settings:**
  1. Click **Factory default**. A message displays asking if you want to reset the system configuration to the factory default settings.
  2. Click **OK** to reset the Beacon to the factory default settings.
- **Reset the device to deep factory default settings:**
  1. Click **Deep factory reset**. A message displays asking if you want to reset the system configuration to the factory default settings.
  2. Click **OK** to reset the ONT so that all the downloaded configuration files such as Web customization, delta-config, voice XML, certification file and so on will be removed.

END OF STEPS

7.21.1 Remove WiFi points

To remove WiFi points, perform the following:

1. Click any extender device and the following *Network map* page is displayed.



   The device name can be renamed by clicking the edit icon .

2. Ensure to power off the extender and wait for a few minutes to get the extender in offline status and click **Remove** to permanently remove the WiFi point from your network.

   When the extender is in powered on state, a message is displayed to power off the extender and then remove it permanently.

The WiFi point is removed from your network. If you want to use the WiFi point on a different network, factory reset it first.

7.22 Configuring Wireless 2.4 GHz

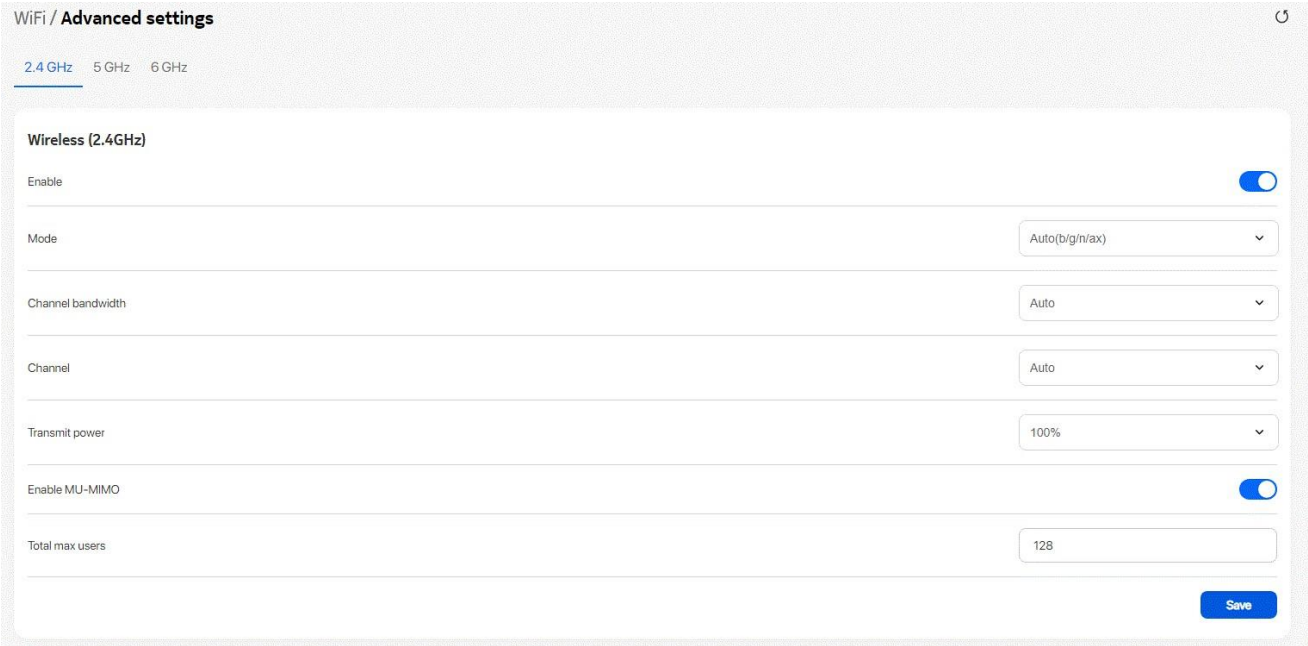
1

Click **WiFi→Advanced settings** in the left pane. The *Advanced settings* page displays.

2

Select the **2.4 GHz** tab to configure the wireless 2.4 GHz parameters.

Figure 7-25 Advanced settings - 2.4 GHz tab



3

Configure the following parameters:

Table 7-16 Wireless 2.4 GHz parameters

Field	Description
Enable	Select the toggle button to enable Wireless (2.4 GHz).
Mode	Select a wireless mode from the list: • **802.11b/g/n/ax/be**
Channel bandwidth	Select the bandwidth range from the list: • **Auto** (auto-assigns the bandwidth range) • **20 MHz** • **40 MHz**
Channel	Select a channel from the list or select **Auto** to auto-assign the channel.
Transmit power	Select a percentage for the transmitting power from the list: • **12%** • **25%** • **50%** • **100%**

Draft

Table 7-16 Wireless 2.4 GHz parameters (continued)

Field	Description
Enable MU-MIMO	Select an option from the list to enable or disable MU-MIMO: • **Enable** • **Disable**
Total max users	Enter the maximum number of users.

4

Click **Save**.

END OF STEPS

7.23 Configuring Wireless 5 GHz

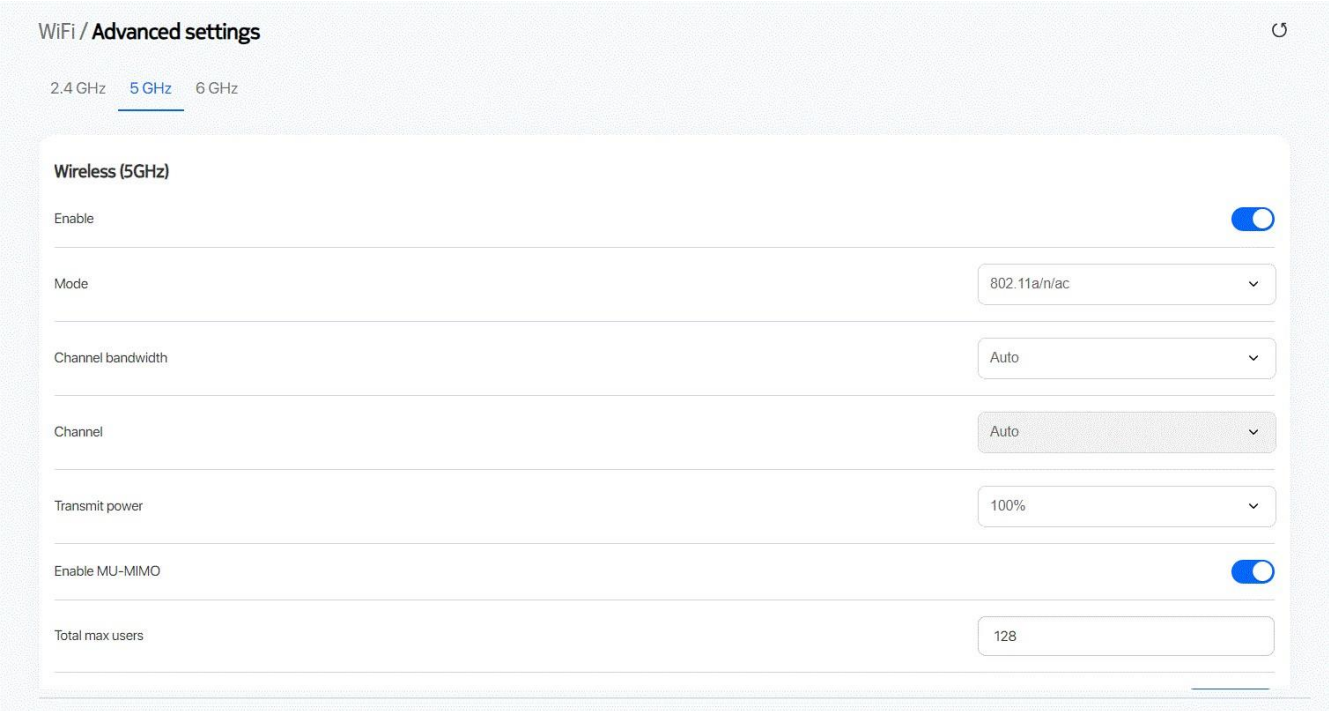
1

Click **WiFi→Advanced settings** in the left pane. The *Advanced settings* page displays.

2

Select the **5 GHz** tab to configure the wireless 5 GHz parameters.

Figure 7-26 Advanced settings - 5 GHz tab



3

Configure the following parameters:

Table 7-17 Wireless 5 GHz parameters

Field	Description
Enable	Select this toggle button to enable WiFi.
Mode	Select the mode from the list: • **802.11a/n/ac** • **802.11a/n/ac/ax** • **802.11n/ac/ax**
Channel bandwidth	Select the bandwidth range from the list: • **20 MHz** • **40 MHz** • **80 MHz** • **160 MHz** • **Auto**
Channel	Select a channel from the list or select **Auto** to auto-assign the channel.
Transmit power	Select a percentage for the transmitting power from the list: • **12%** • **25%** • **50%** • **100%**
Enable MU-MIMO	Select the toggle button to enable MU-MIMO. This can be enabled when multiple users are trying to access the wireless network. When this parameter is enabled, multiple users can access router functions without the congestion.
Total max users	Enter the total number of MAX users. The maximum users allowed is 128.

4

Click **Save**.

END OF STEPS

7.24 Configuring Wireless 6GHz

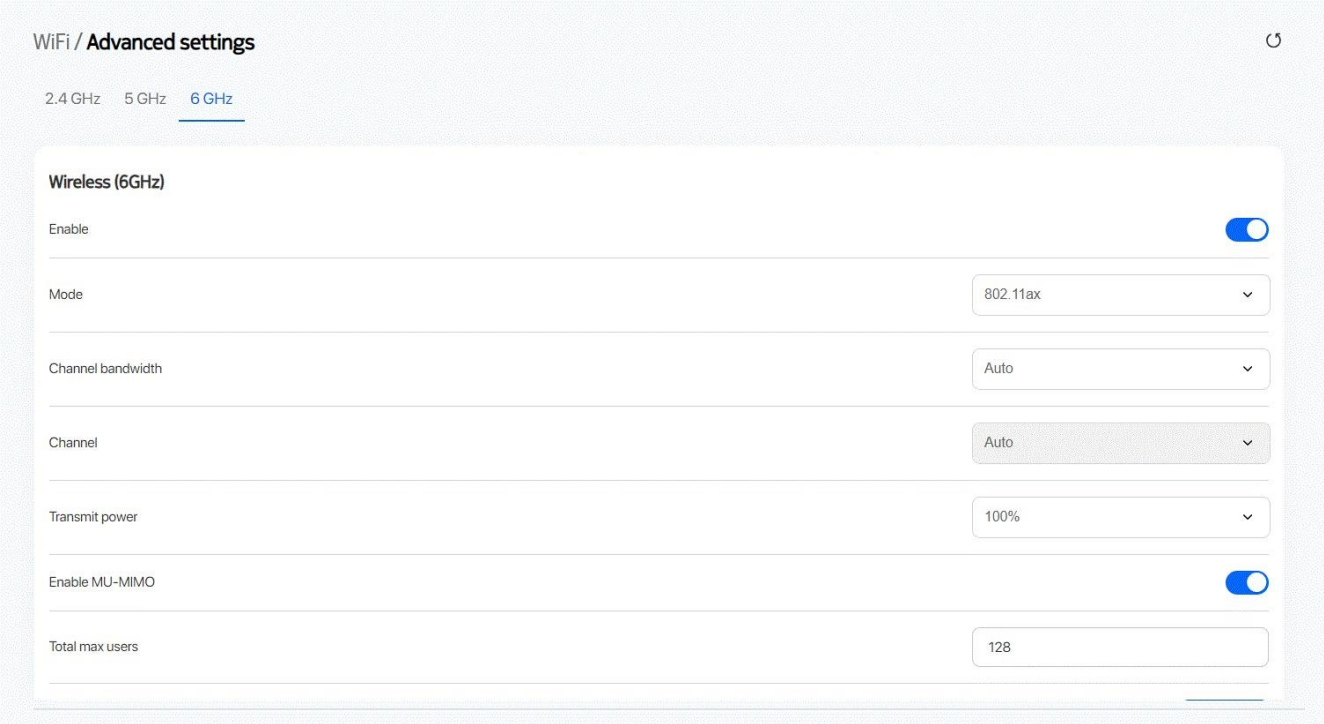
1

Click **WiFi→Advanced settings** in the left pane. The *Advanced settings* page displays.

2

Select the 6 GHz tab to configure the wireless 6 GHz parameters

Figure 7-27 Wireless 6 GHz page



3

Configure the following parameters:

Table 7-18 Wireless 6 GHz

Field	Description
Enable	Select this toggle button to enable WiFi.
Mode	Select the mode from the list: • **802.11ax/be**

Table 7-18 Wireless 6 GHz (continued)

Field	Description
Channel bandwidth	Select an option from the list: • **20 MHz** • **40 MHz** • **80 MHz** • **160 MHz** • **320 MHz-1** • **320 MHz-2** • **Auto**
Channel	Select a channel from the list or select **Auto** to auto-assign the channel.
Transmit power	Select a percentage for the transmitting power from the list: • **12%** • **25%** • **50%** • **100%**
Enable MU-MMO	Select the toggle button to enable MU-MMO. This can be enabled when multiple users are trying to access the wireless network. When this parameter is enabled, multiple users can access router functions without the congestion.
Total max users	Enter the total number of MAX users. The maximum users allowed is 128.

4

Click **Save**.

END OF STEPS

7.25 Viewing WiFi Statistics

1

Click **WiFi→WiFi statistics** in the left pane. The *WiFi statistics* page displays.