Draft

Nokia ONT

G-0126G-A Product Guide

3TN-0122-AAAA-TCZZA
Issue 1
January 2025

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

Draft

Draft

Draft

List of tables

Draft

List of figures

Draft

Draft

About this document

Purpose

This documentation set provides information about safety, features and functionality, ordering, hardware installation and maintenance, and software installation procedures of this ONT 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 ONTs.

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 ONT 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, please 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, please 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.

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

Select **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 list.

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 25.01

The Product guide is a new guide in BBD Release 25.01, issue 1. In future releases, this chapter will provide tables of the feature and document changes applicable to this guide.

Draft

2 ETSI ONT safety guidelines

This chapter provides information about the mandatory regulations that govern the installation and operation of the optical network terminals (ONTs).

2.1 Safety instructions

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

2.1.1 Safety instruction boxes

The safety instruction boxes are provided in the ONT 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 ONTs. It does not provide safety-related instructions.

2.1.2 Safety-related labels

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

The following table provides sample safety labels on the ONT equipment.

Table 2-1 Safety labels

Description	Label text
ESD warning	Caution: This assembly contains an electrostatic sensitive device.
Laser classification	Class 1 laser product

2.2 Safety standards compliance

This section describes the ONT compliance with the European safety standards.

2.2.1 EMC, EMI, and ESD compliance

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

- EN 300-328 v1.9.1 wide band data transmission standards for 2.4GHz bands
- EN 300-386 V1.5.1: Electromagnetic Compatibility and Radio Spectrum Matters (ERM): Telecommunications Network Equipment; Electromagnetic Compatibility (EMC) requirements; Electrostatic Discharge (ESD) requirements
- EN 55022 (2006): Class B, Information Technology Equipment, Radio Disturbance Characteristics, limits and methods of measurement
- EN 55024 (2010): Information Technology Equipment, Immunity Characteristics, limits and methods of measurement
- European Council Directive 2004/108/EC
- EN 300-386 V1.4.1: 2008

- EN 55022:2006 Class B (ONTs)
- EN 301489-1 and EN 301489-17
- EN 55032: Information Technology Equipment, Immunity Characteristics, limits and methods of measurement
- EN 61000-3-2

2.2.2 Equipment safety standard compliance

The ONT equipment complies with the requirements of EN 60950-1, Safety of Information Technology Equipment for use in a restricted location (per R-269).

2.2.3 Environmental standard compliance

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

2.2.4 Laser product standard compliance

For most ONTs, the ONT equipment complies with EN 60825-1 and IEC 60825-2 for laser products. If there is an exception to this compliance regulation, you can find this information in the standards compliance section of the unit data sheet in this Product Guide.

2.2.5 Resistibility requirements compliance

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

2.2.6 Acoustic noise emission standard compliance

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

2.3 Electrical safety guidelines

This section provides the electrical safety guidelines for the ONT equipment.

Note: The ONTs 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 ONTs comply with BS EN 61140.

2.3.1 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.

2.3.2 Cabling

The following are the guidelines regarding cables used for the ONT equipment:

- All cables must be approved by the relevant national electrical code.
- The cables for outdoor installation of ONTs must be suitable for outdoor use.

- POTS wiring run outside the subscriber premises must comply with the requirements of local electrical codes. In some markets, the maximum allowed length of the outside run is 140 feet (43 m). If the outside run is longer, NEC requires primary protection at both the exit and entry points for the wire.

2.3.3 Protective earth

Earthing and bonding of the ONTs must comply with the requirements of local electrical codes.

2.4 ESD safety guidelines

The ONT equipment is sensitive to ESD. Operations personnel must observe the following ESD instructions when they handle the ONT equipment.

CAUTION

Service Disruption

This equipment is ESD sensitive. Proper ESD protections should be used when you enter the TELCO Access portion of the ONT.

During installation and maintenance, service personnel must wear wrist straps to prevent damage caused by ESD.

2.5 Laser safety guidelines

Observe the following instructions when you perform installation, operations, and maintenance tasks on the ONT equipment.

Only qualified service personnel who are extremely familiar with laser radiation hazards should install or remove the fiber optic cables and units in this system.

DANGER

Hazard

There may be invisible laser radiation at the fiber optic cable when the cable is removed from the connector. Avoid direct exposure to the laser beam.

Observe the following danger for laser hazard. Eyes can be damaged when they are exposed to a laser beam. Take necessary precautions before you plug in the optical modules.

DANGER

Hazard

Possibility of equipment damage. Risk of eye damage by laser radiation.

2.5.1 Laser classification

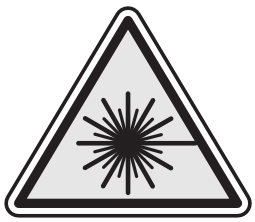
The ONT is classified as a Class 1 laser product based on its transmit optical output.

Laser warning labels

The following figures show the labels related to laser product, classification and warning.

The following figure shows a laser product label.

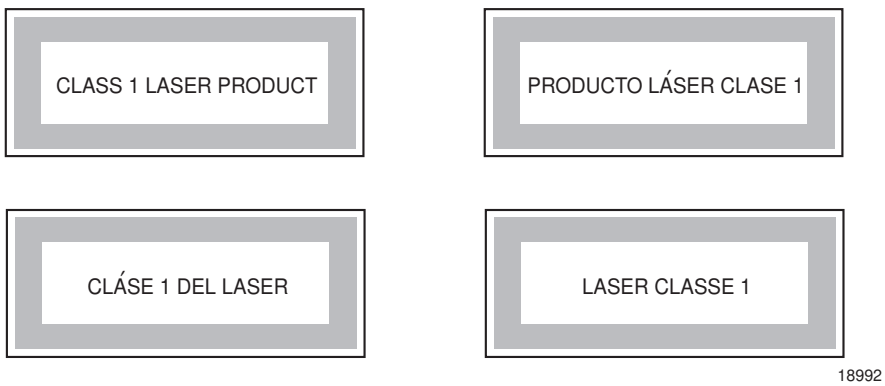
Figure 2-1 Laser product label



18455

Figure 2-2, “Laser classification label” (p. 27) shows a laser classification label. Laser classification labels may be provided in other languages.

Figure 2-2 Laser classification label



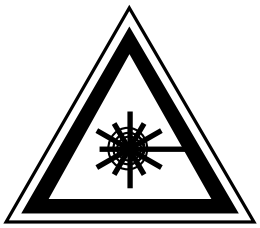
18992

Figure 2-3, “Laser warning labels” (p. 28) shows a laser warning label and an explanatory label for laser products. Labels and warning may be provided in other languages. The explanatory label provides the following information:

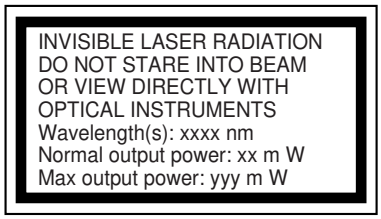
- A warning that calls attention to the invisible laser radiation
- An instruction against staring into the beam or viewing directly with optical instruments
- Wavelength
- Normal output power

- Maximum output power

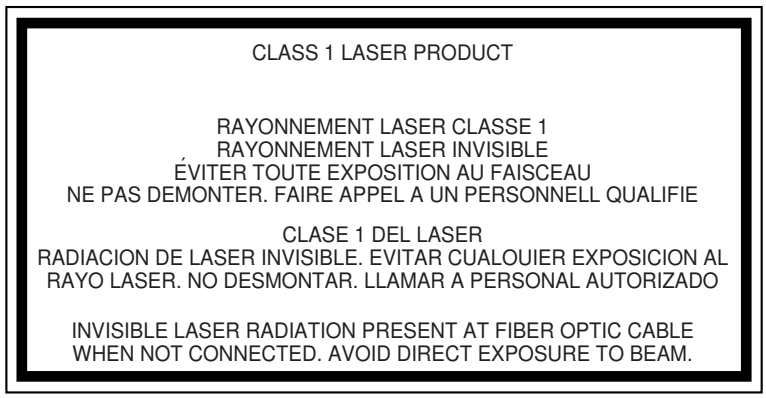
Figure 2-3 Laser warning labels



Laser Warning Label



Laser Warning Label



Laser Warning Label

18993

2.5.2 Transmit optical output

The maximum transmit optical output of an ONT is +5 dBm.

2.5.3 Normal laser operation

In normal operation, fiber cable laser radiation is always off until it receives signal from the line terminal card.

Eyes can be damaged when they exposed to a laser beam. Operating personnel must observe the instructions on the laser explanatory label before plugging in the optical module.

DANGER

Hazard

Risk of eye damage by laser radiation.

2.5.4 Location class

Use cable supports and guides to protect the receptacles from strain.

2.6 Environmental requirements

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

During operation in the supported temperature range, condensation inside the ONT caused by humidity is not an issue. To avoid condensation caused by rapid changes in temperature and humidity, Nokia recommends:

- The door of the ONT not be opened until temperature inside and outside the enclosure has stabilized.
- If the door of the ONT must be opened after a rapid change in temperature or humidity, use a dry cloth to wipe down the metal interior to prevent the risk of condensation.
- When high humidity is present, installation of a cover or tent over the ONT helps prevent condensation when the door is opened.

Draft

3 ETSI environmental and CRoHS guidelines

This chapter provides information about the ETSI environmental China Restriction of Hazardous Substances (CRoHS) regulations that govern the installation and operation of the optical line termination (OLT) and optical network termination (ONT) systems. This chapter also includes environmental operation parameters of general interest.

3.1 Environmental labels

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

3.1.1 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.

3.1.2 Environmental related labels

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

Products below Maximum Concentration Value (MCV) label

Figure 3-1, "Products below MCV value label" (p. 32) 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 3-1 Products below MCV value label

18986

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

Figure 3-2, “Products above MCV value label” (p. 32) 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 3-2 Products above MCV value label

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

Draft

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 3.2 “Hazardous Substances Table (HST)” (p. 32) for more information.

3.2 Hazardous Substances Table (HST)

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

3.3 Other environmental requirements

Observe the following environmental requirements when handling the P-OLT or ONT equipment.

3.3.1 ONT environmental requirements

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

3.3.2 Storage

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

3.3.3 Transportation

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

3.3.4 Stationary use

According to EN 300-019-1-3 - Class 3.1/3.2/3.E, stationary use of ONT equipment must be in a temperature-controlled location, with no rain allowed, and with no condensation allowed.

3.3.5 Material content compliance

European Union (EU) Directive 2002/95/EC, “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. This Directive applies to electrical and electronic products placed on the EU market after 1 July 2006, with various exemptions, including an exemption for lead solder in network infrastructure equipment. Nokia products shipped to the EU after 1 July 2006 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 (RoHS2). With the process equipment is assessed in accordance with the Harmonised Standard EN50581:2012 (CENELEC) on Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances.

3.3.6 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 3-3 Recycling/take back/disposal of product symbol

At the end of their life, the OLT and ONT products are subject to the applicable local legislations that implement the European Directive 2012/19EU on waste electrical and electronic equipment (WEEE).

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 3-3, “Recycling/take back/disposal of product symbol” (p. 34) 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.

4 ANSI ONT safety guidelines

This chapter provides information about the mandatory regulations that govern the installation and operation of the optical network terminals or units (ONTs or ONUs) in the North American or ANSI market.

4.1 Safety instructions

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

4.1.1 Safety instruction boxes in customer documentation

The safety instruction boxes are provided in the ONT 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 ONTs. It does not provide safety-related instructions.

4.1.2 Safety-related labels

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

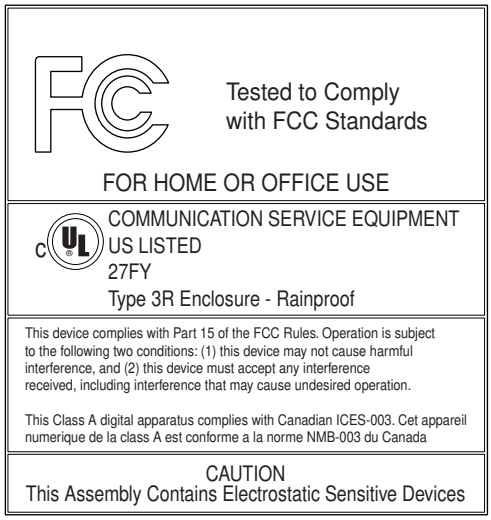
The following table provides examples of the text in the various ONT safety labels.

Table 4-1 Safety labels

Description	Label text
UL compliance	Communication service equipment US listed. Type 3R enclosure - Rainproof.
TUV compliance	Type 3R enclosure - Rainproof.
ESD warning	Caution: This assembly contains electrostatic sensitive device.
Laser classification	Class 1 laser product
Laser product compliance	This laser product conforms to all applicable standards of 21 CFR 1040.10 at date of manufacture.
FCC standards compliance	Tested to comply with FCC standards for home or office use.
CDRH compliance	Complies with 21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007
Operation conditions	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.
Canadian standard compliance (modular ONT)	This Class A digital apparatus complies with Canadian ICES-003.
Canadian standard compliance (outdoor ONT)	This Class B digital apparatus complies with Canadian ICES-003.
CE marking	There are various CE symbols for CE compliance.

The following figure shows a sample safety label on the ONT equipment.

Figure 4-1 Sample safety label on the ONT equipment



18533

4.2 Safety standards compliance

This section describes the ONT 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.

4.2.1 EMC, EMI, and ESD standards compliance

The ONT equipment complies with the Federal Communications Commission (FCC) CFR 47, Part 15, Subpart B, Class A requirements for OLT 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.

4.2.2 Equipment safety standard compliance

The ONT equipment complies with the requirements of UL60950-1, Outdoor ONTs to “Communication Service Equipment” (CSE) and Indoor ONTs to Information Technology Equipment (ITE).

4.2.3 Environmental standards compliance

The ONT equipment complies with the following standards:

- GR-63-CORE (NEBS): requirements related to operating, storage, humidity, altitude, earthquake, office vibration, transportation and handling, fire resistance and spread, airborne contaminants, illumination, and acoustic noise
- GR-487-CORE: requirements related to rain, chemical, sand, and dust
- GR-487 R3-82: requirements related to condensation
- GR-3108: Requirements for Network Equipment in the Outside Plant (OSP)
- TP76200: Common Systems Equipment Interconnections Standards

4.2.4 Laser product standards compliance

The ONT equipment complies with 21 CFR 1040.10 and CFR 1040.11, except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007” or to 21 CFR 1040.10 U.S. Center for Devices and Radiological Health (CDRH) of the Food and Drug Administration (FDA) Laser Notice 42 for ONTs containing Class 1 Laser modules certified by original manufactures.

Per CDRH 21 CFR 10.40.10 (h) (1) (iv) distributors of Class 1 laser products, such as Nokia ONTs shall leave the following Laser Safety cautions with the end user.

a) “Class 1 Laser Product”

b) “Caution – Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.”

Figure 4-2, “Sample laser product label showing CDRH 21 CFR compliance” (p. 39) shows a laser product label.

Figure 4-2 Sample laser product label showing CDRH 21 CFR compliance

4.2.5 Resistibility requirements compliance

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

4.3 Laser safety guidelines

Only qualified service personnel who are extremely familiar with laser radiation hazards should install or remove the fiber optic cables and units in this system.

Observe the following warnings when you perform installation, operations, and maintenance tasks on the ONT equipment.

DANGER

Hazard

There may be invisible laser radiation at the fiber optic cable when the cable is removed from the connector. Avoid direct exposure to beam.

Observe the following danger for a laser hazard. Eyes can be damaged when they are exposed to a laser beam. Take necessary precautions before you plug in the optical modules.

DANGER

Hazard

Possibility of equipment damage. Risk of eye damage by laser radiation.

Per CDRH 21 CFR 10.40.10 (h) (1) (iv) distributors of Class 1 laser products, such as Nokia ONTs shall leave the following Laser Safety cautions with the end user.

a) “Class 1 Laser Product”

b) “Caution – Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.”

4.3.1 Laser warning labels

The following figures show sample labels related to laser product, classification and warning.

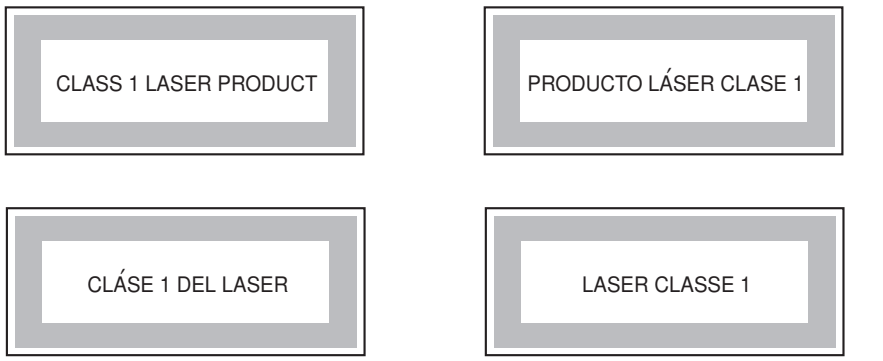
The following figure shows a laser product label.

Figure 4-3 Laser product label

18455

Figure 4-4, “Laser classification label” (p. 40) shows a laser classification label. Laser classification labels may be provided in other languages.

Figure 4-4 Laser classification label

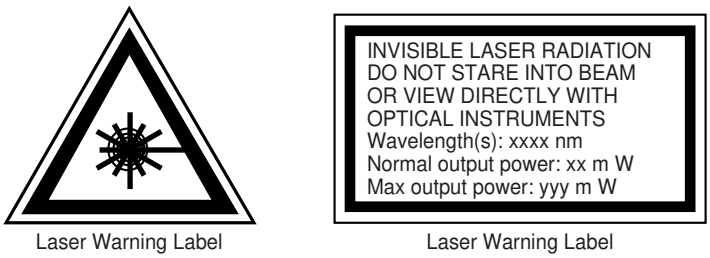


18992

Figure 4-5, “Laser warning labels” (p. 41) shows a laser warning label and an explanatory label for laser products. Explanatory labels may be provided in other languages. The explanatory label provides the following information:

- A warning that calls attention to the invisible laser radiation
- An instruction against staring into the beam or viewing directly with optical instruments
- Wavelength
- Normal output power
- Maximum output power

Figure 4-5 Laser warning labels



4.3.2 Laser classification

The ONT is classified as a Class 1 laser product based on its transmit optical output.

For Class 1 laser products, lasers are safe under reasonably foreseeable conditions of operation, including the use of optical instruments for intrabeam viewing.

Figure 4-6, “Sample laser product safety label on the ONT equipment” (p. 41) shows a sample laser product safety label on the ONT equipment.

Figure 4-6 Sample laser product safety label on the ONT equipment

4.3.3 Transmit optical output

The maximum transmit optical output of an ONT is +5 dBm.

4.3.4 Normal laser operation

In normal operation, fiber cable laser radiation is always off until it receives signal from the line terminal card.

Operating personnel must observe the instructions on the laser explanatory label before plugging in the optical module.

DANGER

Hazard

Risk of eye damage by laser radiation.

4.3.5 Location class

Use cable supports and guides to protect the receptacles from strain.

4.4 Electrical safety guidelines

This section provides the electrical safety guidelines for the ONT equipment.

Note: The ONTs 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.

4.4.1 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.

4.4.2 Cabling

The following are the guidelines regarding cables used for the ONT equipment:

- Use only cables approved by the relevant national electrical code.
- Use cables suitable for outdoor use for outdoor installation of ONTs.
- The ONTs have been evaluated for use with external POTS wiring without primary protection that may not exceed 140 ft (43 m) in reach. However, the power cable must not exceed 100 ft (31 m).

4.4.3 Protective earth

Earthing and bonding of the ONTs must comply with the requirements of NEC article 250 or local electrical codes.

4.5 ESD safety guidelines

The ONT equipment is sensitive to ESD. Operations personnel must observe the following ESD instructions when they handle the ONT equipment.

CAUTION

Service Disruption

This equipment is ESD sensitive. Proper ESD protections should be used when entering the TELCO Access portion of the ONT.

During installation and maintenance, service personnel must wear wrist straps to prevent damage caused by ESD.

Nokia recommends that you prepare the site before you install the ONT equipment. In addition, you must control relative humidity, use static dissipating material for furniture or flooring, and restrict the use of air conditioning.

4.6 Environmental requirements

See the ONT technical specification documentation for temperature ranges for ONTs.

During operation in the supported temperature range, condensation inside the ONT caused by humidity is not an issue. To avoid condensation caused by rapid changes in temperature and humidity, Nokia recommends:

- The door of the ONT not be opened until temperature inside and outside the enclosure has stabilized.
- If the door of the ONT must be opened after a rapid change in temperature or humidity, use a dry cloth to wipe down the metal interior to prevent the risk of condensation.
- When high humidity is present, installation of a cover or tent over the ONT helps prevent condensation when the door is opened.

5 G-0126G-A unit data sheet

5.1 Overview

5.1.1 Purpose

5.1.2 Contents

5.2 G-0126G-A part numbers and identification

Table 5-1, “Identification of G-0126G-A indoor ONTs” (p. 45) provides part numbers and identification information for the G-0126G-A indoor ONT.

Table 5-1 Identification of G-0126G-A indoor ONTs

Ordering kit part number	Provisioning number	Description	CLEI Code	CPR	ECI/ Bar code
3TN01414BA	3TN01415BA	G-0126G-A, GPON ONT supports 6KV, 4xGE UNI, WiFi 6, 2+2, 5dBi external antenna Includes a 12V 1.5A wall-mounted AC/DC power adapter with 2-pin EU input plug.	—	—	—

Table 5-2, “G-0126G-A power supply ordering information” (p. 46) provides the power supply information for the G-0126G-A ONT. For more information on power supplies, see the **G-0126G-A Power Supply and UPS Guide**. The power consumption is less than 18 W.

Table 5-2 G-0126G-A power supply ordering information

ONT part numbers	Power model (Model No./Manufacture Part Number)	Ordering part numbers	Power information	Customer category or country compliance tested for	Notes
Kit: 3TN01148BA EMA: 3TN01222BA	RUIDE:RD1201000-C55-35OGD BC120100-EC6C-LL03 KELI: KL-WE120100-B SW-WB160A	NA	12V/1A wall mounted, AC/DC power adapter with 2-pin EU input plug.	CE/CB	2-pin EU input plug

The following table describes the various plug types used in the ONTs:

Table 5-3 Plug types

Plug type	Icon
2-pin EU plug	
2-pin US plug	
2-pin AU plug	
3-pin UK plug	
3-pin US plug	
3-pin India plug	

Table 5-4, “Hardware parts required for G-0126G-A installations” (p. 47) lists the hardware parts required for mounting an G-0126G-A ONT.

Table 5-4 Hardware parts required for G-0126G-A installations

Part	Description
ONT unit	The G-0126G-A ONT
Wall mount bracket 3TN00658AA	The wall mount bracket is fastened to a wall. The G-0126G-A ONT is seated in the wall mount bracket. Color of the wall mount bracket: White
Mounting screws	Two screws are required to mount the wall mount bracket. The recommended screw is a M4 or #6 screw with a pan head style of screw head.

5.3 G-0126G-A general description

G-0126G-A indoor ONTs provide the subscriber interface for the network by terminating the PON interface and converting it to user interfaces that directly connect to subscriber devices.

The G-0126G-A has built-in concurrent dual-band Wi-Fi® 802.11 b/g/n/ax and 802.11ac/ax networking with triple play capability and can provide triple play services. The G-1426G-A supports Wi-Fi 6 and Wi-Fi EasyMesh™. This coverage can be expanded by installing additional Wi-Fi EasyMesh-capable beacons.

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.

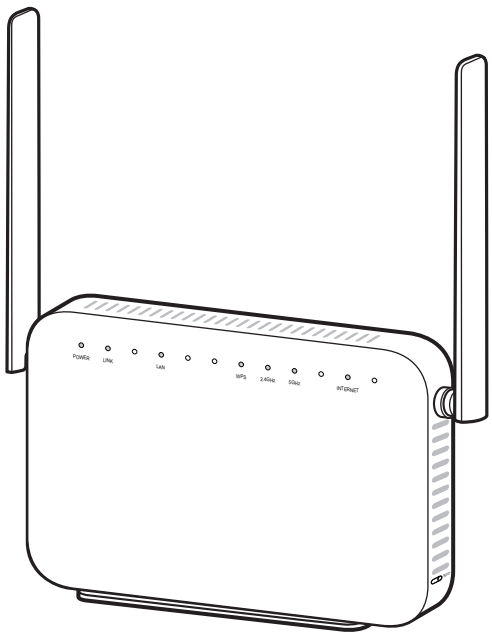
Note: The Nokia WiFi Care Portal can be accessed by the end user and the operator.

The ONT is compatible with all existing subscriber equipment, including analog phones with both tone and rotary dial capabilities, cordless phones, modems, (Type I, Type II, and Type III).

The ONT can be placed on a flat surface, such as a desk or shelf.

Figure 5-1, "G-0126G-A ONT (external antenna)" (p. 48) shows the G-0126G-A ONT.

Figure 5-1 G-0126G-A ONT (external antenna)



40049

G-0126G-A indoor ONTs provide the following functions:

- Dual-band concurrent 2x2 IEEE 802.11 b/g/n/ax 2.4 GHz and 802.11ac/ax MIMO 5 GHz
- Supports 802.11 b/g/n/ax 2x2 Wireless 2.4 GHz MIMO; Channel bandwidth 20, 40, 20/40 MHz
- Supports 802.11ac/ax 2x2 Wireless 5 GHz Mu-MIMO; Channel bandwidth 20, 40, 80, 160 MHz
  Notes:
  - When the channel bandwidth is configured to Auto in the ETSI domain, after boot up, the ONT can take up to 10 minutes (depending on the channel selection by the initial channel selection algorithm) to complete Connection Admission Control (CAC) as required by the regulation. During this time, the 5GHz SSIDs will not be operational and you can be connected to 2.4GHz SSIDs instead. When the 5GHz SSIDs become operational, you can be band-steered to 5GHz, if appropriate.
  - When the ONT is operational and needs to fall back from 160MHz to 80MHz channel bandwidth, it will only attempt to change to 160MHz between 2:00 am and 3:00 am. Hence, the potential 10-minute CAC will create minimal impact. You can change this behavior through the configuration file by either limiting to 80MHz channels only (will limit CAC to 1 minute) or by disabling the expansion from 80MHz to 160MHz between 2:00 am and 3:00 am.
- Four Gigabit standard RJ-45 1000/100/10 Mbps, auto negotiating Ethernet ports and MDI/MDIX auto sensing
- One FXS port for VoIP service with RJ-11 connector
- GPON uplink: G.984 and G.988 series standard compliant

- 256MB NAND Flash with bad block management, 512MB DDR3 RAM, pin2pin compatible design for possible upgrade of RAM/Flash
- WiFi on/off push button
- WPS on/off push button
- Reset button
- USB 2.0 interface (Optional)

  Note: Some variants of G-1426G-A do not support USB.
- Built-in layer 2 switch; Line Rate L2 traffic
- IP video distribution
- Wavelength: 1490 nm downstream; 1310 nm upstream
- Supports WBF filter.The GPON ONTs can co-exist with XGSPON ONTs in the same PON
- PHY rate: 574 Mbps for 2.4 G and 2402 Mbps for 5 G
- External antennas with 5dBi gain for each
- Optics that support received signal strength indication (RSSI)
- G.984.3-compliant Advanced Encryption Standard (AES) in downstream
- WPA, WPA-PSK/TKIP
- WPA2, WPA2-PSK/AES
- WPA3
- VLAN tagging/detagging and marking/remarking of IEEE 802.1p per Ethernet port.
- Dying gasp support
- DTMF dialing
- Echo cancellation (G.168)
- Forward Error Correction (FEC)
- Support for multiple SSIDs (private and public instances); contact your Nokia representative for further details.
- Conductive power: 200 mW/27 dBm (2.4 GHz); 200 mW/30 dBm (5GHz)
- Maximum effective isotropic radiated power (EIRP):
  - 5 dBi external antenna: 100 mW/20 dBm (2.4GHz); 1000 mW/30 dBm (5GHz) for the European variant
  - 5 dBi external antenna: 1995 mW/33 dBm (2.4GHz); 1259 mW/31 dBm (5GHz) for the North American variant
- Bridged mode or routed mode per LAN port
- TR-069 support
- TR-181 support
- TR-157 LXC support
- Ethernet-based Point-to-Point (PPPoE)
- DHCP client/server
- DNS server/client

- DDNS
- Port forwarding
- Network Address Translation (NAT)
- Network Address Port Translation (NAPT)
- UPnP IGD2.0 support
- ALG
- IGMP snooping and proxy (v2/v3)
- Traffic classification and QoS capability
- OMCI/TR-069 Web GUI configuration
- Performance monitoring and alarm reporting
- Remote software image downloading and activation
- IP/MAC/URL filter
- Multi-level firewall and ACL
- SoftGRE supports IPv4 and IPv6 tunnel
- Speed Test support

5.3.1 TR-069 parameter support

The G-0126G-A ONT supports the following TR-069 features:

- Host object
- Port forwarding
- Optical parameters
- Object support for optical parameters
- Statistics and troubleshooting
- Diagnostic parameter
- Component parameter

Host object support

The ONT provides host object support for: InternetGatewayDeviceLANDevice.Hosts.Host.

Port forwarding support

The ONT supports the port forwarding of objects via TR-069:

- Application name
- WAN port
- LAN port
- Internal client
- Protocol
- Enable mapping
- WAN connection list

These port forwarding parameters are also supported in the GUI. For more information, see7.43 “Configuring Port Forwarding” (p. 169) in Chapter 7, “Configure a G-0126G-A indoor ONT”.

Optical parameters support

The ONT supports the reading of optical parameters via TR-069:

- Laser bias current
- Voltage
- Temperature
- Received signal levels
- Lower thresholds

These optical parameters are also supported in the GUI. For more information, see 7.15 “Viewing Optical Module Status” (p. 109) in Chapter 7, “Configure a G-0126G-A indoor ONT”.

Object support for Wi-Fi parameters

The ONT supports the status retrieval and configuration of the following Wi-Fi parameters via TR-069:

- Channel
- SSID
- Password for WPA
- Tx power (transmission rate in percentage of maximum transmit power)
- WPS

These TR-069 object parameters are also supported in the GUI. For more information, see 7.28 “Configuring Wireless 2.4 GHz” (p. 141) and 7.29 “Configuring Wireless 5 GHz” (p. 143) in Chapter 7, “Configure a G-0126G-A indoor ONT”.

Statistics and troubleshooting support

The ONT supports TR-069 statistics and troubleshooting for LAN, WAN, and WiFi.

Diagnostic parameter support

The ONT supports the following TR-069 diagnostic parameters:

- TR-143
- IP ping
- Traceroute

These diagnostic parameters are also supported in the GUI. For more information, see 7.56 “Diagnosing WAN Connections” (p. 184) in Chapter 7, “Configure a G-0126G-A indoor ONT”.

5.3.2 TR-069 authentication using TLS and CA certificates

G-0126G-A ONTs support TLS, as well as ACS authentication using SHA-256 pre-installed certificates.

If the URL is set to the HTTPs format, by default, the connection will use TLS without authentication

mode. The ONT can also authenticate the ACS using a pre-installed CA certificate.

The G-0126G-A ONTs support TLSv1.3 for TR-069. The ONT supports download certification from ACS.

5.3.3 TR-111 support

The G-0126G-A ONT supports TR-111, which extends the WAN Management Protocol defined in TR-069 to enhance the ability to remotely manage LAN devices.

The device-gateway association enables an ACS to identify the associated gateway through which a device is connected.

A connect request via the NAT gateway enables an ACS to initiate a TR-069 session with a device that is operating behind a NAT gateway.

5.3.4 TR-157 support

This ONT can support LXC container for third party software components on ONTs with minimal 512M memory. These software components are managed by ACS with the parameters defined in TR-157.

The TR-157 objects are:

- Manage each software component via SoftwareModules.DeploymentUnit.{i}
- Set software component execution environment via SoftwareModules.ExecEnv.{i}
- Run software component and get the execution status via SoftwareModules.ExecutionUnit.{i}

Note: The device reserves and limits to 36MB RAM and 32MB flash in total for all of the third-party applications. The maximum CPU load created or provided to the third party application is limited to approximately 30%. Underlying non-priority processes may still use the remaining memory on a temporary basis.

Nokia can assist to review specific applications, taking into account the actual memory load of the current hardware, current and projected software evolution over time, and the projected use by a third party application of the software.

5.3.5 TR-181 parameter support

TR-181 and TR-369 parameter support has been introduced or enhanced for the parameter categories and functions listed in the following table.

TR-181 can be enabled (instead of TR-098) by defining the associated TR-181 parameter in a customer specific pre-configuration file downloadable into the ONT.

For details about which parameters are supported, see your Nokia representative.

Table 5-5 Support for TR-181 parameter categories

Parameter category	Functionality
Device info and statistics	Device information
	Optical statistics
	Ethernet statistics
	Wi-Fi statistics
	Bridge statistics
	PPP statistics
	IP statistics
	Periodic statistics
Diagnostics	Wi-Fi diagnostic
	Ping
	Trace route
	TR-143 Speed test
	Self test
	NSLookup diagnostics
Optical configuration	
Forwarding configuration	Ethernet
	Bridge
	PPP
	IP
	Routing
	QoS
	DSlite
	NAT
	Neighbor discovery
Hosts configuration	
Wi-Fi configuration	

Table 5-5 Support for TR-181 parameter categories (continued)

Parameter category	Functionality
Service configuration	
	DDNS
	DNS
	DHCP
	GRE
	IGMP
	NTP timing
Firewall	
WebGUI configuration	
Nokia Wi-Fi configuration	Nokia Wi-Fi cloud service

Note: Due to the internal chipset architecture, the application session time-out is not fully precise and ranges from session timer to session timer + 20 seconds. The applications with a session timer are ICMP connections, TCP sessions, and UDP sessions. The default session time-out of an ICMP connection is 30 seconds. The background of this constraint is that the application session time-out is maintained and refreshed by both the software and hardware session timers maintained separately. The hardware session timer refreshes the software session timer, which results in the deviation of the software timer. The range of application session time is from session timer to session timer + 20 seconds.

5.4 G-0126G-A software and installation feature support

For information on installing or replacing the G-0126G-A see Chapter 6, “Install or replace a G-0126G-A indoor ONT”.

For information on the following topics, see the **G-0126G-A Product Overview Guide**:

- ONT and MDU general descriptions of features and functions
- Ethernet interface specifications
- POTS interface specifications
- RSSI specifications
- Wi-Fi specifications
- ONT optical budget
- SLID entry via Ethernet port
- ONT management using an ONT interface

5.5 G-0126G-A interfaces and interface capacity

The following table describes the supported interfaces and interface capacity for G-0126G-A indoor ONTs.

Table 5-6 G-0126G-A indoor ONT interface connection capacity

ONT type and model	Maximum capacity								
	POTS	100/10 BASE-T	1000/100/10 BASE-T	RF video (CATV)	MoCA	VDSL2	E1/T1	Local craft	GPON SC/APC
G-0126G-A [1]	—	—	1	—	—	—	—	—	1

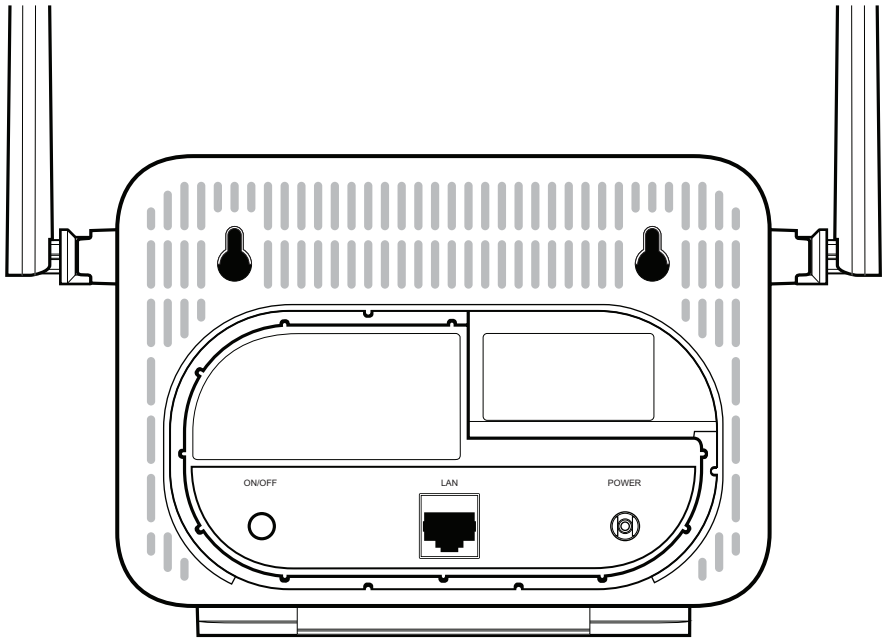
Notes:

1. The G-0126G-A ONTs provide WiFi service that is enabled and disabled using a WiFi on/off switch.

5.5.1 G-0126G-A connections and components

Figure 5-2, “G-0126G-A indoor ONT physical connections (back)” (p. 55) shows the physical connections for G-0126G-A indoor ONTs.

Figure 5-2 G-0126G-A indoor ONT physical connections (back)



40048

Note: Some variants of G-1426G-A do not support USB.

Table 5-7, “G-0126G-A indoor ONT physical connections” (p. 55) describes the physical connections for G-0126G-A indoor ONTs.

Table 5-7 G-0126G-A indoor ONT physical connections

Connection [1]	Print Letters	Description
Ethernet ports	LAN1 to LAN4	This connection is provided through Ethernet RJ-45 connectors. Up to four 1000/100/10 Base-T Ethernet interfaces are supported. The Ethernet ports can support both data and in-band video services on all four interfaces.
Power input	POWER	This connection is provided through the power connector. A power cable fitted with a barrel connector is used to make the connection.
Reset button	RESET	Pressing the Reset button for less than 10 seconds reboots the ONT; pressing the Reset button for 10 seconds resets the ONT to the factory defaults, except for the LOID and SLID. Accessible through a 2mm pin hole.
On/Off button	ON/OFF	This button turns the ONT on or off.
Fiber optic port	-	The SC/APC fiber optic port is located at the back of the ONT and provides the connection for the fiber optic cable.

Notes:

1. The primary path for the earth ground for these ONTs is provided by the 12V return signal in the power connector.

5.6 G-0126G-A LEDs

Figure 5-3, “G-0126G-A indoor ONT LEDs” (p. 56) shows the G-0126G-A indoor ONT LEDs.

Figure 5-3 G-0126G-A indoor ONT LEDs

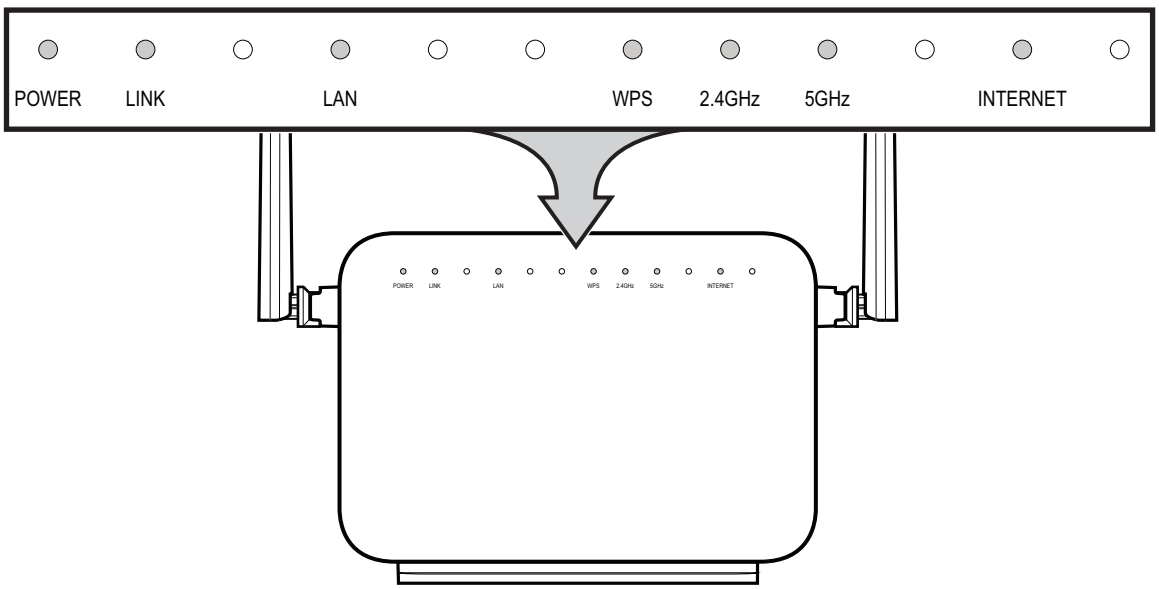


Table 5-8, “G-0126G-A indoor ONT LED descriptions” (p. 57) provides LED descriptions for G-0126G-A indoor ONTs.

Table 5-8 G-0126G-A indoor ONT LED descriptions

Indicator	LED color and behavior	LED behavior description
POWER	Green solid	Power on.
	Fast Green flashing	Software update in progress.
	Slow Green flashing	Failure at startup or loopback detected
	Off	Power off.
LINK	Green solid	ONT is configured on the OLT and is in service (UP) and the OMCI messages are downloaded.
	Fast Green flashing	ONT is attempting to range with OLT and the OMCI messages are downloaded.
	Slow Green flashing	Rouge state is triggered.
	Off	GPON link is down or no link is connected.
LAN 1 to 4	Off	ONT power is off or Ethernet is not connected.
	Green solid	ONT is connected to the associated LAN port (includes devices with wake-on-LAN capability where a slight voltage is supplied to an Ethernet connection).
	Green flashing	LAN activity is present (traffic in either direction).
WPS	Green solid	Wi-Fi protected setup link is up (negotiation and auto-configuration successful).
	Slow Green flashing	Wi-Fi protected setup link activity (negotiation and auto-configuration ongoing).
	Off	Wi-Fi protected setup link down or no link connected (negotiation has not started or has failed). Wi-Fi protected setup processing exception or multiple peers using WPS simultaneously.
	Fast Green flashing [Fast]	WPS session overlap detected.
2.4 GHz	Green solid	WLAN link is enabled in 2.4 GHz.
	Green flashing	Traffic is passing through the WLAN link.
	Off	WLAN link is disabled or no link is connected.
5 GHz	Green solid	WLAN link is enabled in 5 GHz.
	Green flashing	Traffic is passing through the WLAN link.
	Off	WLAN link is disabled or no link is connected.

Table 5-8 G-0126G-A indoor ONT LED descriptions (continued)

Indicator	LED color and behavior	LED behavior description
INTERNET	Green solid	IP connected (the device has a WAN IP address from IPCP/DHCP/Static and Broadband link is up) and no traffic detected. If the IP or PPPoE session is dropped due to an idle timeout, the light will remain green if PON link is still present. If the session is dropped for any other reason, the light is turned off.
	Green flickering	PPPoE or DHCP connection is in progress.
	Off	Broadband physical connection power off, device in bridged mode with no IP address assigned to the device, or Broadband physical interface connection not present.
USB	Green solid	A device is connected to the USB port.
	Green flashing	Traffic is passing through the USB connection.
	Off	No device is connected to the USB port.

Note: Some variants of G-1426G-A do not support USB.

5.7 G-0126G-A detailed specifications

Table 5-9, “G-0126G-A indoor ONT physical specifications” (p. 58) lists the physical specifications for G-0126G-A indoor ONTs.

Table 5-9 G-0126G-A indoor ONT physical specifications

Description	Specification
Depth (with external antenna)	1.5 in. (39 mm)
Length and Depth of the bottom plate (with external antenna)	2.7 in.(68.8 mm)
Width (with external antenna)	7.8 in. (197mm)
Height (including antenna) (without antenna)	5.7 in. (145 mm) 10.8 in. (275 mm)
Weight [within ± 0.5 lb (0.23 kg)] (net weight of ONT) (with external antenna)	1.00 lb (0.46 kg)

Table 5-10, “G-0126G-A indoor ONT power consumption specifications” (p. 58) lists the power consumption specifications for G-0126G-A indoor ONT.

Table 5-10 G-0126G-A indoor ONT power consumption specifications

Mnemonic	Maximum power (Not to exceed)	Condition	Minimum power	Condition
G-0126G-A	18 W	1 POTS off-hook, 4 1000/100/10 Base-T Ethernet, Wi-Fi operational	4.3 W	1 POTS on-hook, other interfaces/services not provisioned

Table 5-11, “G-0126G-A indoor ONT environmental specifications” (p. 59) lists the environmental specifications for G-0126G-A indoor ONT.

Table 5-11 G-0126G-A indoor ONT environmental specifications

Mounting method	Temperature range and humidity	Altitude
On desk or shelf	Operating: 23° F to 113° F (0° C to 40° C) ambient temperature 10% to 90% relative humidity, non-condensing	Contact your Nokia technical support representative for more information
	Storage: -4° F to 158° F (-20° C to 70° C)	

Table 5-12, “G-0126G-A indoor ONT Dimension data specifications” (p. 59) lists the dimension data specifications for G-0126G-A indoor ONT.

Table 5-12 G-0126G-A indoor ONT Dimension data specifications

Dimensions	Specifications
Packet size supported	2000 bytes
Number of IP addresses supported (or ranges)	In LAN network, the supported range is: • IPv4: 192.168.1.1 ~192.168.1.253 • IPv6: No limitation
Number of supported WiFi clients (per radio, per device, per mesh)	64 per radio, 128 per device, 256 per mesh
Number of supported Beacons/APs in a mesh	6 (including the device)
Number of supported WAN interfaces	Supports 8 WAN connections
Number of supported VLANs	Supports 4094 VLANs
Number of priority queues, and overall buffer size	256 priority queues. Max 16MB for WAN and 4MB for LAN, 512KB SRAM buffer in PONMAC
Number of multicast groups (DACL entries)	512

5.8 G-0126G-A GEM ports and T-CONTs

The following table lists the maximum number of supported T-CONTs and GEM ports. See the appropriate release Customer Release Notes for the most accurate list of supported devices.

Table 5-13 G-0126G-A indoor ONT capacity for GEM ports and T-CONTs

ONT or MDU	Maximum	Notes
Package P ONTs		
GEM ports per indoor or outdoor ONT	256	256 are present; 254 are available, and 2 are reserved for multicast and debugging
T-CONTs per indoor or outdoor ONT	32	32 are present; 31 are available, and 1 is reserved for OMCI

5.9 G-0126G-A performance monitoring statistics

The following section identifies the supported performance monitoring statistics for G-0126G-A ONTs. A check mark indicates the statistic is supported on that ONT. An empty cell indicates the statistic is not supported. The following tables are categorized by supported alarm types:

- Table 5-14, “Package S ONTs ONTENET performance monitoring statistics” (p. 59) provides statistics for ONTENET type counters
- Table 5-15, “Package S ONTs ONTL2UNI performance monitoring statistics” (p. 60) provides statistics for ONTL2UNI type counters
- Table 5-16, “Package S ONTs PONONTTC, PONONTMCTC, PONONTTCHSI, PONONTTCCES, PONONTTCFLOW, PONONTTCVOIP performance monitoring statistics” (p. 61) provides statistics for PONONTTC, PONONTMCTC, PONONTTCHSI, PONONTTCCES, PONONTTCFLOW, and PONONTTCVOIP type counters
- Table 5-17, “Package S ONTs PONONTTC aggregate performance monitoring statistics” (p. 61) provides statistics for PONONTTC aggregate type counters

Note: If you have trouble accessing G-0126G-A ONTs performance monitoring statistics using TL1, please contact your Nokia support representative for more information about how to access and retrieve performance monitoring type counters.

The following table provides statistics for ONTENET type counters

Table 5-14 Package S ONTs ONTENET performance monitoring statistics

ONT	ONTENET statistics													
	FCSE	EC	LC	RBO	SCF	MCF	DT	IMTE	CSE	AE	IMRE	FTL	TBO	SQE
G-0126G-A [1]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Notes:

1. A 5 second polling window limitation exists on the ONT, therefore the margin of error for each 15-min window is 5 seconds.

Table 5-15 Package S ONTs ONTL2UNI performance monitoring statistics

ONT	ONTL2UNI statistics									
	FRAMES	BYTES	MCFRAMES	DSDRPDFRMS	USDRPDFRMS	USFRAMES	DSFRAMES	DSBYTES	USMCFRAMES	DSMCFRAMES
G-0126G-A [1]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Notes:

1. A 5 second polling window limitation exists on the ONT, therefore the margin of error for each 15-min window is 5 seconds.

Table 5-16 Package S ONTs PONONTTC, PONONTMCTC, PONONTTCHSI, PONONTTCCES, PONONTTCFLOW, PONONTTCVOIP performance monitoring statistics

ONT	PONONTTC, PONONTMCTC, PONONTTCHSI, PONONTTCCES, PONONTTCFLOW, PONONTTCVOIP statistics					
	TXBLOCKS	TXFRAGS	RXBLOCKS	RXFRAGS	LOSTFRAGS	BADGEMHDRS
G-0126G-A [1]	✓	✓	✓	✓	✓	—

Notes:

1. A 5 second polling window limitation exists on the ONT, therefore the margin of error for each 15-min window is 5 seconds.

Table 5-17 Package S ONTs PONONTTC aggregate performance monitoring statistics

ONT	PONONTTC (aggregate) statistics					
	TXBLOCKS	TXFRAGS	RXBLOCKS	RXFRAGS	LOSTFRAGS	BADGEMHDRS
G-0126G-A [1]	✓	✓	✓	✓	✓	—

Notes:

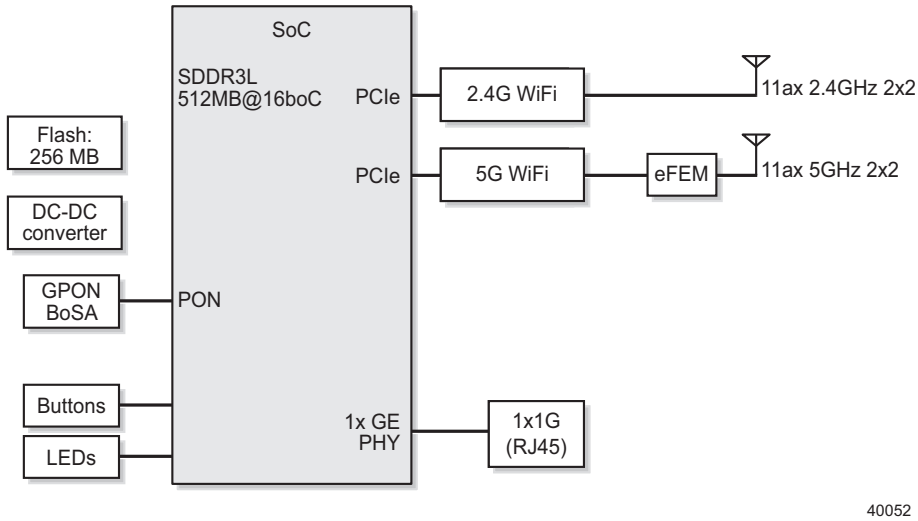
1. A 5 second polling window limitation exists on the ONT, therefore the margin of error for each 15-min window is 5 seconds.

5.10 G-0126G-A functional blocks

G-0126G-A indoor ONTs are single-residence ONTs that support Wireless (Wi-Fi) service. Wi-Fi service on these ONTs is compliant with the IEEE 802.11 standard and enabled or disabled using a WIFI button. In addition to the Wi-Fi service, these ONTs transmit Ethernet packets to four RJ-45 Ethernet ports to one RJ-11 POTS port. These ONTs also feature fiber optic, and power connectors.

The following figure shows the functional blocks for G-0126G-A indoor ONT.

Figure 5-4 G-0126G-A ONT functional block



5.11 G-0126G-A standards compliance

G-0126G-A indoor ONTs are compliant with the following standards:

- CE marking for European standards for health, safety, and environmental protection
- EN 300-328 v1.9.1 wide band data transmission standards for 2.4GHz bands
- G.984 support GPON interface (framing)
- G.984.2 (Amd1, class B+) for GPON
- G.984.3 support for activation and password functions
- G.984.3 support for AES with operator enable/disable on per port-ID level
- G.984.3 support for dynamic bandwidth reporting
- G.984.3 support for FEC in both upstream and downstream directions
- G.984.3 support for multicast using a single GEM port-ID for all video traffic
- G.984.4 and G.983.2 support for ONT management and provisioning
- IEEE 802.1p for traffic prioritization
- IEEE 802.1q for VLANs
- IEEE 802.3 (2012)
- IEEE 802.11 ax/ac/b/g/n for Wi-Fi
- ITU-T G.711 A-law, G.711 µ-law, and G.729A and G.729B, G.723.1
- SIP RFC 3261

5.11.1 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the G-0126G-A ONTs 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 G-0126G-A ONTS qualify as equipment with high network availability (HiNA) functionality. Since the main purpose of G-0126G-A ONTs 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 “G-0126G-A interfaces and interface capacity” (p. 55) in this chapter.

For information about power consumption, see 5.7 “G-0126G-A detailed specifications” (p. 58) in this chapter.

5.11.2 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.

5.11.3 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 20 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.
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.

5.12 G-0126G-A special considerations

G-0126G-A is a package P ONT.

5.12.1 WiFi service

G-0126G-A indoor ONTs feature WiFi service and data services. WiFi is a wireless networking technology that uses radio waves to provide wireless HSI and network connections. This ONT complies with the IEEE 802.11 standards, which the Wi-Fi Alliance defines as the basis for Wi-Fi technology.

Wi-Fi physical features

G-0126G-A indoor ONTs have the following physical features that assist in providing WiFi service:

- 1 WiFi for enabling and disabling WiFi service
- 1 WiFi Protected Setup (WPS) push button for adding WPS-enabled wireless devices
- 4 external antennas: 2 for 2.4G and 2 for 5G

WiFi standards and certifications

The WiFi service on G-0126G-A indoor ONTs supports the following IEEE standards and Wi-Fi Alliance certifications:

- Wi-Fi CERTIFIED 6™
- Wi-Fi CERTIFIED™ a, b, g, n, ac
- WPA™, WPA2™ , WPA3™
- Wi-Fi Agile Multiband™
- WMM®, WMM®-Power Save
- Wi-Fi Protected Setup™
- Easymesh R4

WiFi GUI features

G-0126G-A indoor ONTs have HTML-based WiFi configuration GUIs.

5.12.2 G-0126G-A ONT considerations and limitations

The following table lists the considerations and limitations for Package P G-0126G-A ONTs.

Table 5-18 G-0126G-A ONT considerations and limitations

Considerations and limitations
Call History Data collection (ONTCALLHST) is supported, except for the following parameters: RTP packets (discarded), far-end RTCP and RTCP-XR participation, RTCP average and peak round trip delay, MOS, average jitter, number of jitter-buffer over-runs and under runs.
The maximum value of the ringing AC voltage is 60Vrms, and the ring DC offset voltage is suggested to be 0V.
The following voice features/ GSIP parameters are configurable on a per-Client/ per-ONT basis (not per-Subscriber): • Enable Caller ID and Enable Caller Name ID • Digitmap and the associated Interdigit and Critical timers and Enter key parameters • Warmline timer is enabled per subscriber, but the warmline timer value is configured per ONT and must have a lower value than the permanent time • Miscellaneous timers: Permanent, Timed-release, Reanswer, Error-tone, and CW-alert timers • Features/ functions: Message waiting mode, WMWI refresh interval, DTMF volume level • Service Codes for the following features: CW, Call Hold and Warmline

Draft

6 Install or replace a G-0126G-A indoor ONT

6.1 Overview

6.1.1 Purpose

This chapter provides the steps to:

- Install a G-0126G-A indoor ONT
- Replace a G-0126G-A indoor ONT
- Wall mount an G-0126G-A indoor ONT

6.1.2 Contents

6.2 Prerequisites

Ensure that you have all required cables.

6.3 Recommended tools

You need the following tools:

- #2 Phillips screwdriver
- 1/4 in. (6 mm) flat blade screwdriver
- Wire strippers
- Fiber optic splicing tools
- RJ-45 cable plug crimp tool
- Voltmeter or multimeter
- Optical power meter
- Drill and drill bits
- Paper clip

6.4 Safety information

Read the following safety information before installing or replacing 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.

WARNING

Equipment Damage

This equipment is ESD sensitive. Proper ESD protections should be used when removing the fiber access cover of the indoor ONT.

CAUTION

Service Disruption

Keep indoor ONTs away from 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 indoor ONT should be installed in accordance with the applicable requirements of the NEC or CEC. Local authorities and practices take precedence when there is conflict between the local standard and the NEC or CEC.
- The indoor ONT must be installed by qualified service personnel.
- Indoor ONTs must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the Chapter 5, “G-0126G-A unit data sheet” for the temperature ranges of these ONTs.

6.5 Install a G-0126G-A indoor ONT

1

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

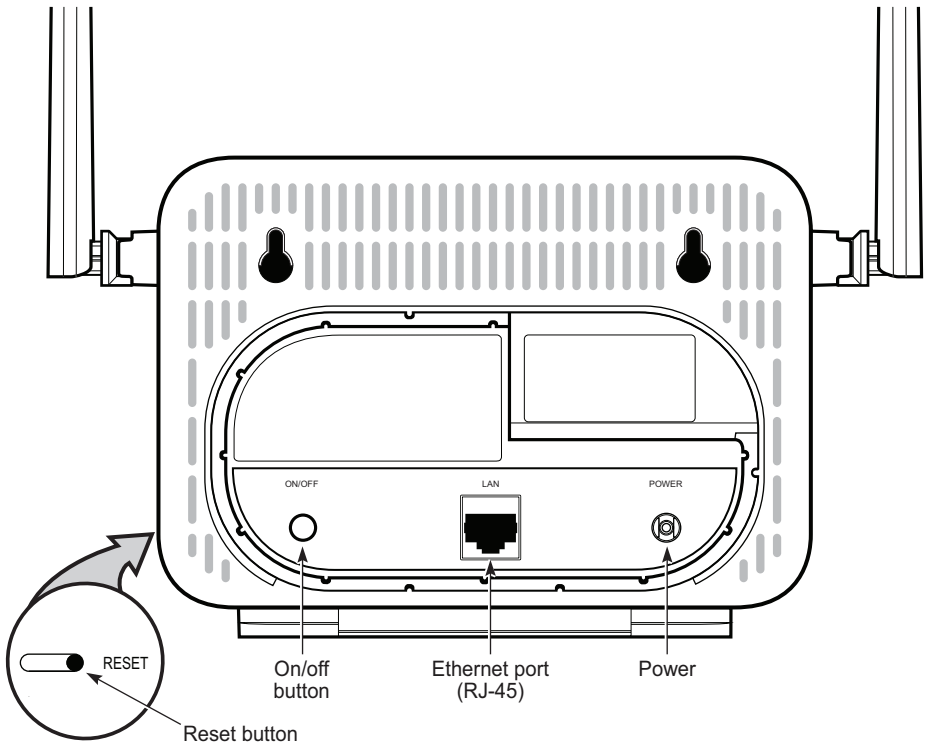
Note: The G-0126G-A cannot be stacked with another ONT or with other equipment. The ONT mounting requirements are:

- 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, “G-0126G-A ONT connections” (p. 68).

Figure 6-1 G-0126G-A ONT connections



40053

3

Connect the Ethernet cables to the RJ-45 ports.

4

Route the POTS cable directly to the RJ-11 port as per local practices.

5

DANGER

Hazard

Fiber cables transmit invisible laser light. To avoid eye damage or blindness, never look directly into fibers, connectors, or adapters.

WARNING

Equipment Damage

Be careful to maintain a bend radius of no less than 1.5 in. (3.8 cm) when connecting the fiber optic cable. A very small bend radius in the cable can result in damage to the optic fiber.

Connect the fiber optic cable with SC/APC adapter to the SC/APC connector on the bottom of the ONT.

Note: Fiber cable preparation varies depending on the type and size of the inside or outside plant fiber cable being spliced to the SC/APC fiber optic pigtail cable.

6

Connect the power cable to the power connector.

7

Power up the ONT unit by using the power switch.

8

By default the WiFi service is enabled.

9

Verify the ONT LEDs, voltage status, and optical signal levels; see the **G-0126G-A Hardware and Cabling Installation Guide**.

10

Activate and test the services; see the **G-0126G-A Hardware and Cabling Installation Guide**.

11

If used, configure the SLID; see the **G-0126G-A Configuration, Management, and Troubleshooting Guide**.

12

If necessary, reset the ONT.

a. Locate the Reset button on a G-0126G-A indoor ONT as shown in Figure 6-1, “G-0126G-A ONT connections” (p. 69).

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

END OF STEPS

6.6 Replace a G-0126G-A indoor ONT

1

Deactivate the ONT services at the P-OLT.

If you are using the SLID feature, this step is not required. The ONT and the services can remain in service (IS).

a. Use the RTRV-ONT command to verify the ONT status and th associated services. Record the serial number or the SLID of the ONT displayed in the command output.

Example:

```
RTRV-ONT::ONT-1-1-1-1-1;
```

b. If the ONT is in service, place the ONT in OOS state.

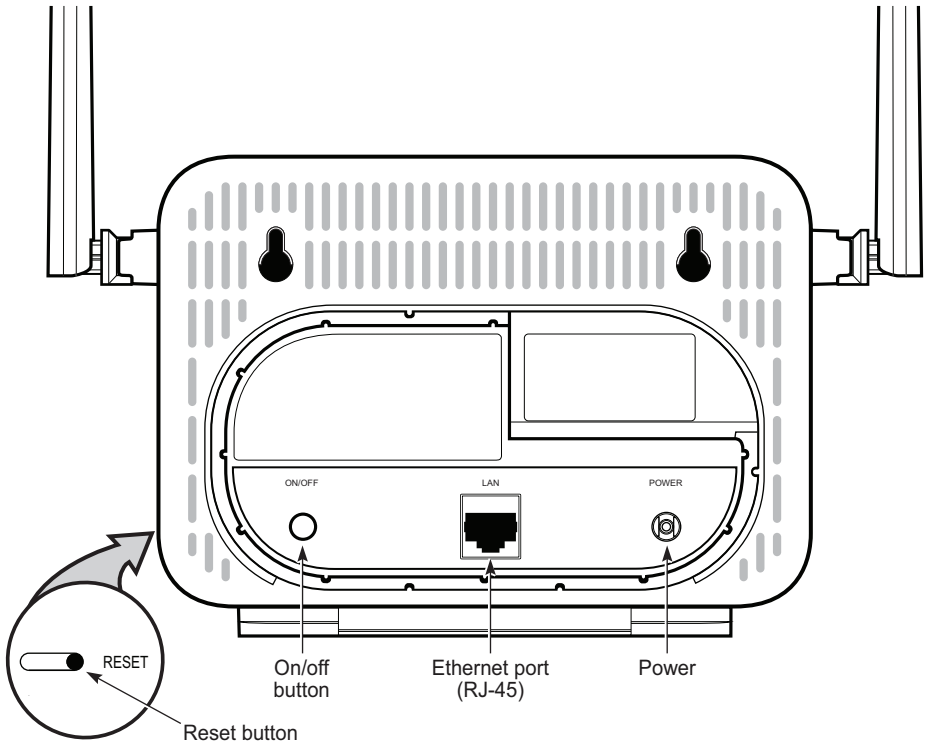
Example:

```
ED-ONT::ONT-1-1-1-1-1;
```

2

By default the WiFi service is enalbed.

Figure 6-2 G-0126G-A indoor ONT connections



3

Power down the unit by using the on/off power switch.

4

Disconnect the POTS, Ethernet, and power cables from the ONT; see Figure 6-2, “G-0126G-A indoor ONT connections” (p. 72) for the connector locations on the G-0126G-A indoor ONT.

5

DANGER

Hazard

Fiber cables transmit invisible laser light. To avoid eye damage or blindness, never look directly into fibers, connectors, or adapters.

Disconnect the fiber optic cables.

a. Unplug the fiber optic cable with SC/APC connector from the bottom of the ONT.

b. Attach a fiber dust cover to the end of the SC/APC connector.

6

Replace the old ONT with a new ONT on a flat surface, such as a desk or shelf.

7

Connect the Ethernet cables directly to the RJ-45 ports; see Figure 6-2, “G-0126G-A indoor ONT connections” (p. 72) for the location of the RJ-45 ports.

8

Connect the POTS cable directly to the RJ-11 port as per local practices; see Figure 6-2, “G-0126G-A indoor ONT connections” (p. 72) for the location of the RJ-11 ports.

9

DANGER

Hazard

Fiber optic cables transmit invisible laser light. To avoid eye damage or blindness, never look directly into fibers, connectors, or adapters.

If required, have approved service personnel who are trained to work with optic fiber clean the fiber optic connection. See the **G-0126G-A Configuration, Management, and Troubleshooting Guide** for more information about fiber optic handling, inspection, and cleaning.

10

DANGER

Hazard

Fiber cables transmit invisible laser light. To avoid eye damage or blindness, never look directly into fibers, connectors, or adapters.

WARNING

Equipment Damage

Be careful to maintain a bend radius of no less than 1.5 in. (3.8 cm) when connecting the fiber optic cable. A very small bend radius in the cable can result in damage to the optic fiber.

Connect the fiber optic cable with SC/APC adapter into the SC/APC connector on the bottom of the ONT.

Note: Fiber cable preparation varies depending on the type and size of the inside or outside plant fiber cable being spliced to the SC/APC fiber optic pigtail cable.

11

Connect the power cable to the power connector.

12

Power up the unit by using the power switch.

13

By default the Wi-Fi service is enabled. .

14

If used, configure the SLID; see the **G-0126G-A Configuration, Management, and Troubleshooting Guide** for more information.

Note: A new SLID or the old SLID may be used with the replacement ONT.
If a new SLID is used, the new SLID must also be programmed at the P-OLT using TL1 or a network manager.
If the old SLID is used, no changes need to be made at the P-OLT; see the operations and maintenance documentation for the OLT for more details.

15

Verify the ONT LEDs, voltage status, and optical signal levels; see the **G-0126G-A Hardware and Cabling Installation Guide**.

16

Activate and test the services; see the **G-0126G-A Hardware and Cabling Installation Guide**.

17

If necessary, reset the ONT.

a. Locate the Reset button on a G-0126G-A indoor ONT as shown in Figure 6-2, “G-0126G-A indoor ONT connections” (p. 72).

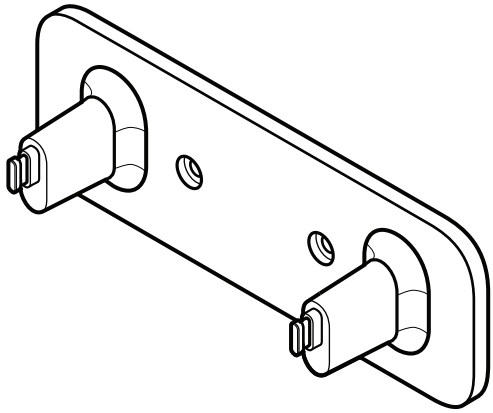
b. Insert the end of a straightened paper clip or other narrow object into the hole in the Reset button to reset the ONT.

END OF STEPS

6.7 Wall mount a G-0126G-A indoor ONT

This chapter provides the steps to mount a G-0126G-A indoor ONT on a wall using a wall mount bracket (3TN00658AA/3TN00658AB). The G-0126G-A indoor ONT is shipped without the wall mount bracket. The wall mount bracket must be ordered separately (3TN00658AA/3TN00658AB).

Figure 6-3 G-0126G-A wall mount bracket



38768

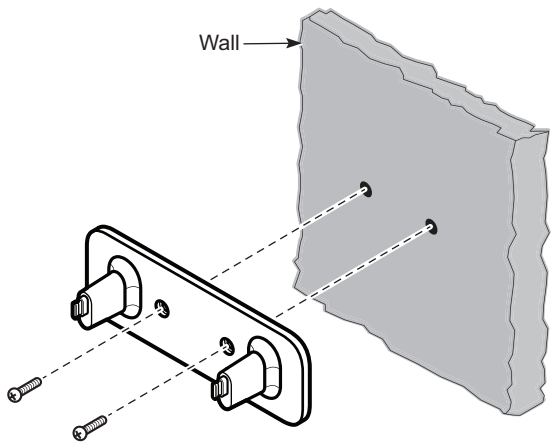
6.7.1 Recommended tools

See section 6.3 “Recommended tools” (p. 67) for the recommended tools.

6.7.2 Procedure

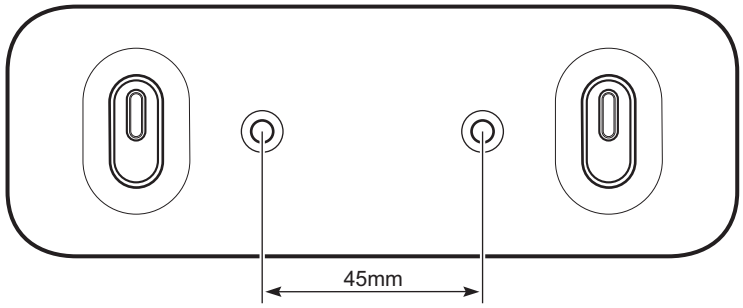
Use this procedure to mount a G-0126G-A ONT on a wall. The G-0126G-A ONT must be mounted in a horizontal position, as indicated by the wall mounting key holes in Figure 6-5, “G-0126G-A - Distance between the mounting holes” (p. 76).

Figure 6-4 G-0126G-A wall mount bracket - mounting holes



38770

Figure 6-5 G-0126G-A - Distance between the mounting holes



1

Mount the bracket to the wall such that the two screws fit into the designated keyholes on the bracket. Tighten the screws to secure the bracket to the wall firmly.

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

2

Connect the power cord and other cables to the G-0126G-A ONT.

3

Hang the unit onto the wall.

Figure 6-6 ONT to wall mount connection

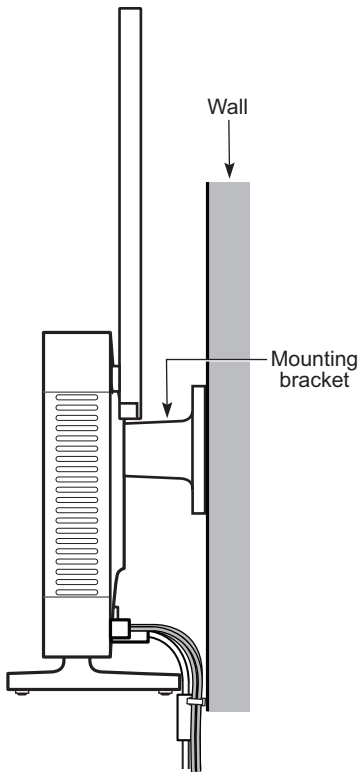
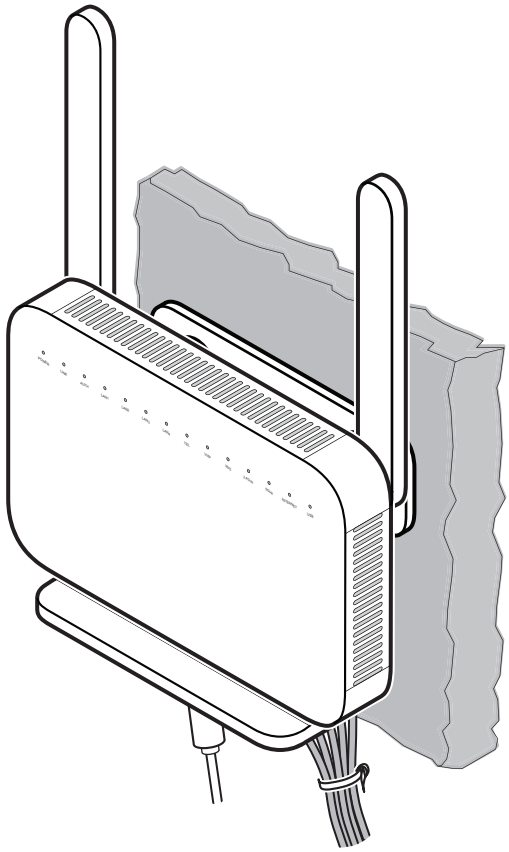


Figure 6-7, “ONT in wall mount bracket—facing the room” (p. 78) shows the cables connected to the wall mount bracket and the ONT facing the room.

Figure 6-7 ONT in wall mount bracket—facing the room



38772

END OF STEPS

7 Configure a G-0126G-A indoor ONT

7.1 Overview

7.1.1 Purpose

This chapter describes the WebGUI configuration procedures.

7.1.2 Contents

Draft

GUI overview

This section provides an overview of the G-0126G-A WebGUI.

7.2 General configuration

For HTTP/HTPPs configuration procedures, refer to the **G-0126G-A Configuration, Management, and Troubleshooting Guide**.

7.3 HGU mode GUI configuration

Use the procedures below to use the web-based GUI for the G-0126G-A in HGU mode. This mode is preset at delivery.

A home gateway unit (HGU) is a home networking device, used as a gateway to connect devices in the home through fiber to the Internet. An HGU provides a variety of features for the home network including routing and firewall capability. By using the HGU, users can connect all smart equipment in their home, including personal computers, set-top boxes, mobile phones, and other consumer electronics devices, to the Internet.

7.4 WAN services overview

This section provides a brief overview of the WAN services in different modes and interactions with ONT.

The following WAN services can be configured.

7.4.1 Forwarding model

WAN ports are broadly grouped into Layer-2 and Layer-3 WAN ports. A Bridging forwarding service uses the Layer-2 WAN port for forwarding packets to WAN side, and a routing forwarding service uses the Layer-3 WAN port for forwarding.

A LAN port is a virtual LAN (VLAN) interface above a physical interface. The LAN ports are broadly grouped into Layer-2 and Layer-3 LAN ports. Bridging forwarding services are attached to the Layer-2 LAN ports whereas Routing forwarding services are attached to the Layer-3 LAN ports. (Layer-2 LAN ports are typically VLAN created over the Ethernet physical interface or SSID mapped to a VLAN. Each WiFi SSID is mapped only to one VLAN, whereas an Ethernet interface can be mapped to multiple VLAN interfaces.

7.4.2 VLAN binding service

In this model, a bridging service can be associated with multiple Ethernet ports. An Ethernet UNI can be a member of multiple VLANs (services), but a WiFi SSID can be associated only to one bridging service.

The VLAN binding service switches packets from LAN port to WAN port and also LAN port to LAN port based on destination MAC address.

7.4.3 Tunnel service

In this model, bridging service can be associated with more than one LAN port and a WAN Port. The traffic from the LAN ports whether its tagged or untagged (traffic from SSID will always be untagged) are received on this interface and the Bridge Tunnel service adds a service VLAN to the received traffic and forwards on the WAN port. It also learns and saves the MAC address on the receiver port. Tunnel service also performs a LAN to LAN switching based on destination MAC address.

7.4.4 Transparent service (Special case of Tunnel mode)

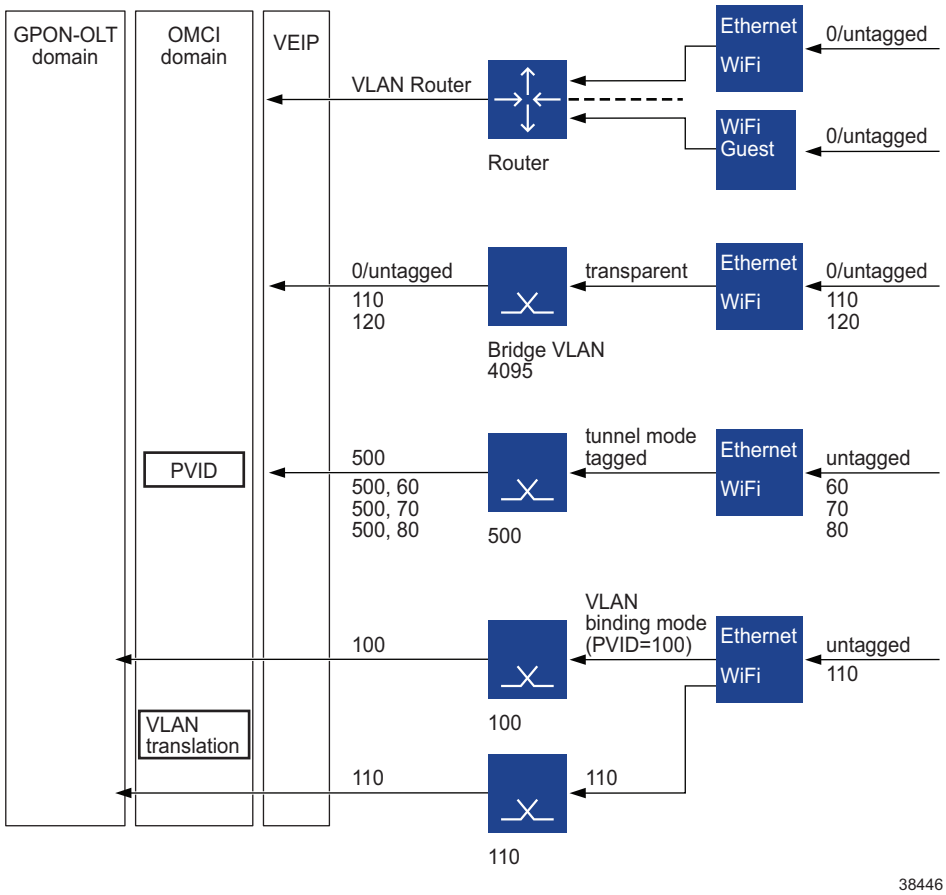
This service is an extension of the bridge tunnel service, where the service VLAN is considered as NULL or empty. This model is applicable only for xPON RGs. The traffic from the LAN side is transmitted on the associated WAN side without adding/stripping a service VLAN. In this service, a PVID is configured through OMCI on xPON , so that all untagged traffic received is tagged with this VLAN on the upstream direction and stripped on the downstream direction. Application of this service model is very limited and recommended only in very specific cases.

7.4.5 Routing service

On the home network (LAN side) the routing traffic can be segregated to multiple groups for traffic isolation (for example, a Home network and a guest network). Each group is identified with a unique VLAN ID and referred as a Routing Slice. A Routing slice for xPON and Ethernet RGs, the LAN port associated with a routing slice can receive only untagged frames. A Routing service operates above one or more routing slices on LAN side and routes packets to one or more WAN(s) based on routing policies. In a RG, only one routing service is supported.

The following figure provides common forwarding model for routed services and bridging services.

Figure 7-1 Common forwarding model



7.4.6 Supported combinations

The following table describes the applicable and supported combinations of OMCI and ACS/WebGUI configurations.

Table 7-1 Supported combinations of OMCI and ACS/WebGUI

Service Type	Operation	Untagged traffic at LAN	Tagged traffic at LAN
Untagged Routed WAN	Set PVID, P-bit	OMCI (ACS/WebGUI with VLAN Disabled)	NA (only untagged in for routed)

Table 7-1 Supported combinations of OMCI and ACS/WebGUI (continued)

Service Type	Operation	Untagged traffic at LAN	Tagged traffic at LAN
Tagged Routed WAN	Set WAN P-bit	ACS/WebGUI	NA (only untagged in for routed)
	SET WAN-VID	ACS/WebGUI	NA (only untagged in for routed)
	Remark P-bit per VLAN (single P-bit)	For future development (OMCI)	NA (only untagged in for routed)
	DSCP to P-bit for untagged LAN traffic	L3 QoS + DSCP to P-bit ACS/WebGUI. DSCP_ classicifcation ACS_only Policy based routing for future development	NA (only untagged in for routed)
	DSCP to P-bit for untagged LAN traffic	OMCI not supported	NA (only untagged in for routed)
	Translate VLAN (OMCI domain)	Supported (no N:1 support, each forwarder different VLAN)	NA (only untagged in for routed)
	L2 QoS (Port, MAC)	ACS/ WebGUI	NA (only untagged in for routed)
	P-bit to P-bit (VLAN regeneration profile)	NA	NA (only untagged in for routed)
Bridged WAN (transparent Tunnel)	Set WAN P-bit	OMCI supported from BBDR2302 (Fixed value 0 in BBDR2301)	P-bit same as incoming packet at LAN
	SET WAN-VID	OMCI (PVID)	VLAN_ID same as incoming packet at LAN
	Remark P-bit per VLAN (single P Bit)	NA	NA
	Remap P-bit per protocol	Not supported	Not supported
	DSCP to P-bit for untagged LAN traffic	L3 QoS + DSCP to P-bit ACS/WebGUI. DSCP_ classicifcation ACS_only. Policy based routing is not applicable.	ACS/WebGUI is not applicable
	DSCP to P-bit for untagged LAN traffic	OMCI - NA	OMCI - NA
	Translate VLAN (OMCI domain)	NA	For future development
	L2 QoS (Port, MAC)	ACS/WebGUI	ACS/WebGUI
	P-bit to P-bit (VLAN regeneration profile)	NA	Not supported

Table 7-1 Supported combinations of OMCI and ACS/WebGUI (continued)

Service Type	Operation	Untagged traffic at LAN	Tagged traffic at LAN
Bridge (VLAN binding, Tunnel)	Set WAN P-bit	ACS/WebGUI	ACS/WebGUI (take recent P-bit)
	Set WAN-VID	ACS/WebGUI	ACS/WebGUI
	Remark P-bit per VLAN (single P-bit)	Not supported (OMCI) (no PVID configured)	Not supported (OMCI)
	Remap P-bit per protocol	Not supported	Not supported
	DSCP to P-bit for untagged LAN traffic	L3 QoS + DSCP to P-bit ACS/WebGUI. DSCP_ classicifcation ACS_only. Policy based routing is not applicable.	NA (not supported)
	DSCP to P-bit for untagged LAN traffic	OMCI - NA	NA (not supported)
	Translate VLAN (OMCI domain)	VLAN Binding - Supported Tunnel - Supported N:1 - Not supported	VLAN Binding - Supported Tunnel - Supported N:1 - Not supported
	L2 QoS (Port, MAC)	ACS/WebGUI	ACS/WebGUI
	P-bit to P-bit (VLAN regeneration profile)	For future development	For future development

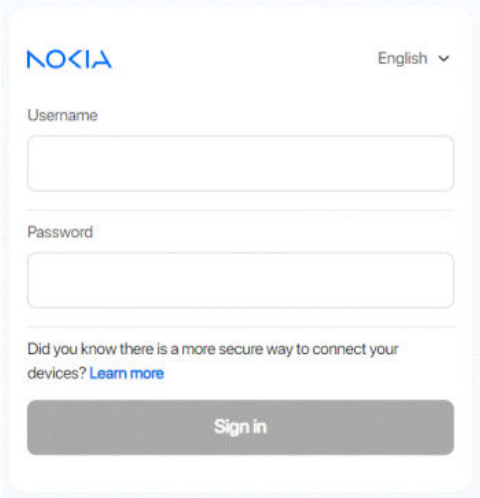
7.5 Logging in to the web-based GUI

1

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

The *Login* page displays.

Figure 7-2 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 ONT or via WiFi connection. The static IP address of your PC must be in the same default gateway subnet as the ONT. You can also access the login page via "https://www.webgui.nokiawifi.com/" and " http://www.webgui.nokiawifi.com/'.

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.*

Enter your username and password in the *Login* page, as shown in Figure 7-2, “Login page” (p. 87).

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.

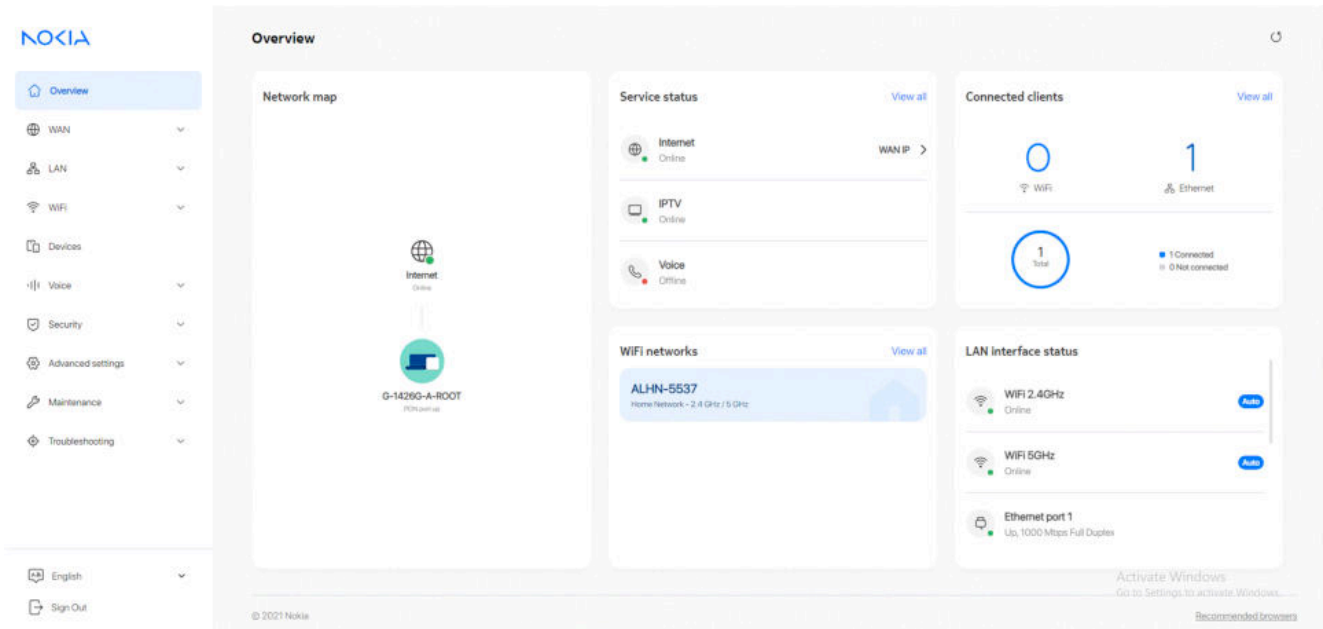
Note: To help protect the security of your Internet connection, the application displays a pop-up reminder to change both the WiFi password and the ONT password.
To increase password security, use a minimum of 10 characters, consisting of a mix of numbers and upper and lower case letters.

END OF STEPS

7.6 Viewing overview information

1

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



END OF STEPS

7.6.1 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).

7.6.2 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.

7.6.3 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).

7.6.4 Connected Clients

Displays the total number of online and offline clients connected to this device .

7.6.5 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

Shows the status of the 5GHz network (Up/Down) and the current band setting. This can either be auto, which indicates Radio Resource Management is enabled or in the range of 36-161 when manually configured.

Ethernet Port

Draft

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).

7.7 G-0126G-A WebGUI Menu

The following table lists the main menu and sub-menu options in the G-0126G-A WebGUI:

Table 7-2 G-0126G-A WebGUI Menu

Main Menu	Sub-menu	Procedure Reference
Overview	-	7.6 “Viewing overview information” (p. 88)
WAN	**WAN services**	7.9 “Configuring WAN Services” (p. 92)
WAN	**WAN statistics**	7.10 “Viewing WAN Statistics” (p. 100)
WAN	**TR-069**	7.11 “Configuring TR-069” (p. 104)
WAN	**TR-369**	7.12 “Configuring TR-369” (p. 105)
WAN	**IP routing**	7.14 “Configuring Static routing” (p. 108)
WAN	**Qos config**	7.16 “Configuring QoS” (p. 111)
WAN	**GRE tunnel**	7.13 “Configuring GRE tunnel” (p. 106)
LAN	**DHCP IPv4**	7.19 “Configuring DHCP IPv4” (p. 121)
LAN	**DHCP IPv6**	7.20 “Configuring DHCP IPv6” (p. 123)
LAN	**DNS**	7.21 “Configuring DNS” (p. 125)
LAN	**LAN statistics**	7.22 “Viewing LAN Statistics” (p. 128)
WiFi	**WiFi networks**	7.24 “Configuring WiFi Network” (p. 130)
WiFi	**Network map**	7.27 “Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points” (p. 137)
WiFi	**Advanced settings**	7.28 “Configuring Wireless 2.4 GHz” (p. 141) 7.29 “Configuring Wireless 5 GHz” (p. 143)
WiFi	**Wireless schedule**	7.30 “Configuring Wireless Schedules” (p. 145)
WiFi	**WiFi statistics**	7.31 “Viewing WiFi Statistics” (p. 146)
Devices	-	7.33 “Viewing Device Information” (p. 148)
Security	**Firewall**	7.35 “Configuring the Firewall” (p. 151)
Security	**MAC filter**	7.36 “Configuring the MAC Filter” (p. 152)
Security	**IP filter**	7.37 “Configuring the IP Filter” (p. 154)
Security	**Family profiles**	7.39 “Configuring Family Profiles” (p. 158)
Security	**DMZ and ALG**	7.40 “Configuring DMZ and ALG” (p. 164)
Security	**Access control**	7.41 “Configuring Access Control” (p. 166)
Advanced settings	**Port forwarding**	7.43 “Configuring Port Forwarding” (p. 169)

Table 7-2 G-0126G-A WebGUI Menu (continued)

Main Menu	Sub-menu	Procedure Reference
Advanced settings	**Port triggering**	7.44 “Configuring Port Triggering” (p. 170)
Advanced settings	**DDNS**	7.45 “Configuring DDNS” (p. 171)
Advanced settings	**NTP**	7.46 “Configuring NTP” (p. 172)
Advanced settings	**UPNP and DLNA**	7.48 “Configuring UPNP and DLNA” (p. 175)
Maintenance	**Change password**	7.50 “Configuring the Password” (p. 177)
Maintenance	**Backup and restore**	7.51 “Backing Up the Configuration” (p. 178) 7.52 “Restoring the Configuration” (p. 179)
Maintenance	**Firmware upgrade**	7.53 “Upgrading Firmware” (p. 180)
Maintenance	**Diagnostics**	7.56 “Diagnosing WAN Connections” (p. 184)
Maintenance	**Log**	7.57 “Viewing Log Files” (p. 186)
Maintenance	**Delta CFG tool**	7.58 “Generating a delta configuration file” (p. 187)
Troubleshooting	-	7.59 “Troubleshooting counters” (p. 190)

WAN Configuration

7.8 Overview

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

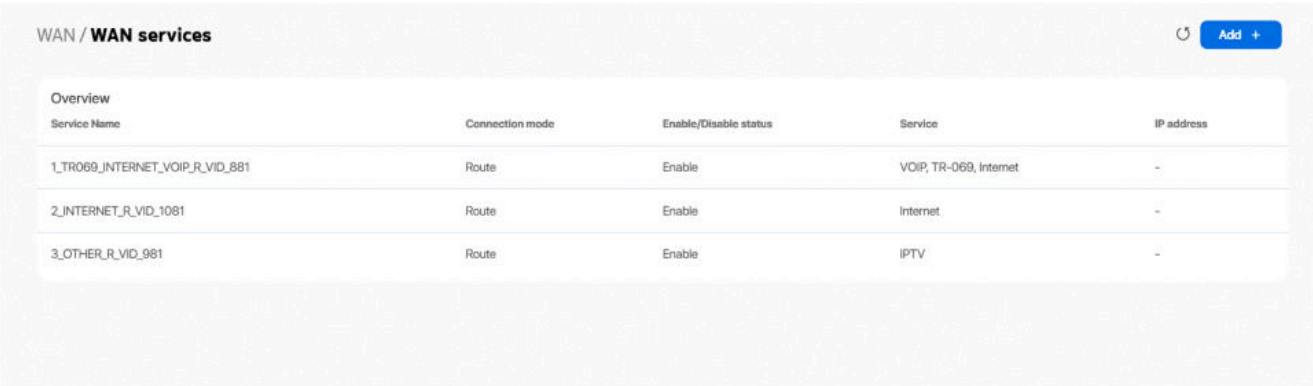
Sub-menu	Procedure
WAN services	7.9 “Configuring WAN Services” (p. 92)
WAN statistics	7.10 “Viewing WAN Statistics” (p. 100)
TR-069	7.11 “Configuring TR-069” (p. 104)
TR-369	7.12 “Configuring TR-369” (p. 105)
IP routing	7.14 “Configuring Static routing” (p. 108)
Optical module status	7.15 “Viewing Optical Module Status” (p. 109)
Qos config	7.16 “Configuring QoS” (p. 111)
GRE tunnel	7.13 “Configuring GRE tunnel” (p. 106)
US classifier	7.17 “Configuring Upstream (US) Classifier ” (p. 114)

7.9 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 7-3 Overview table in *WAN services* page



2

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

Figure 7-4 Create New Connection page

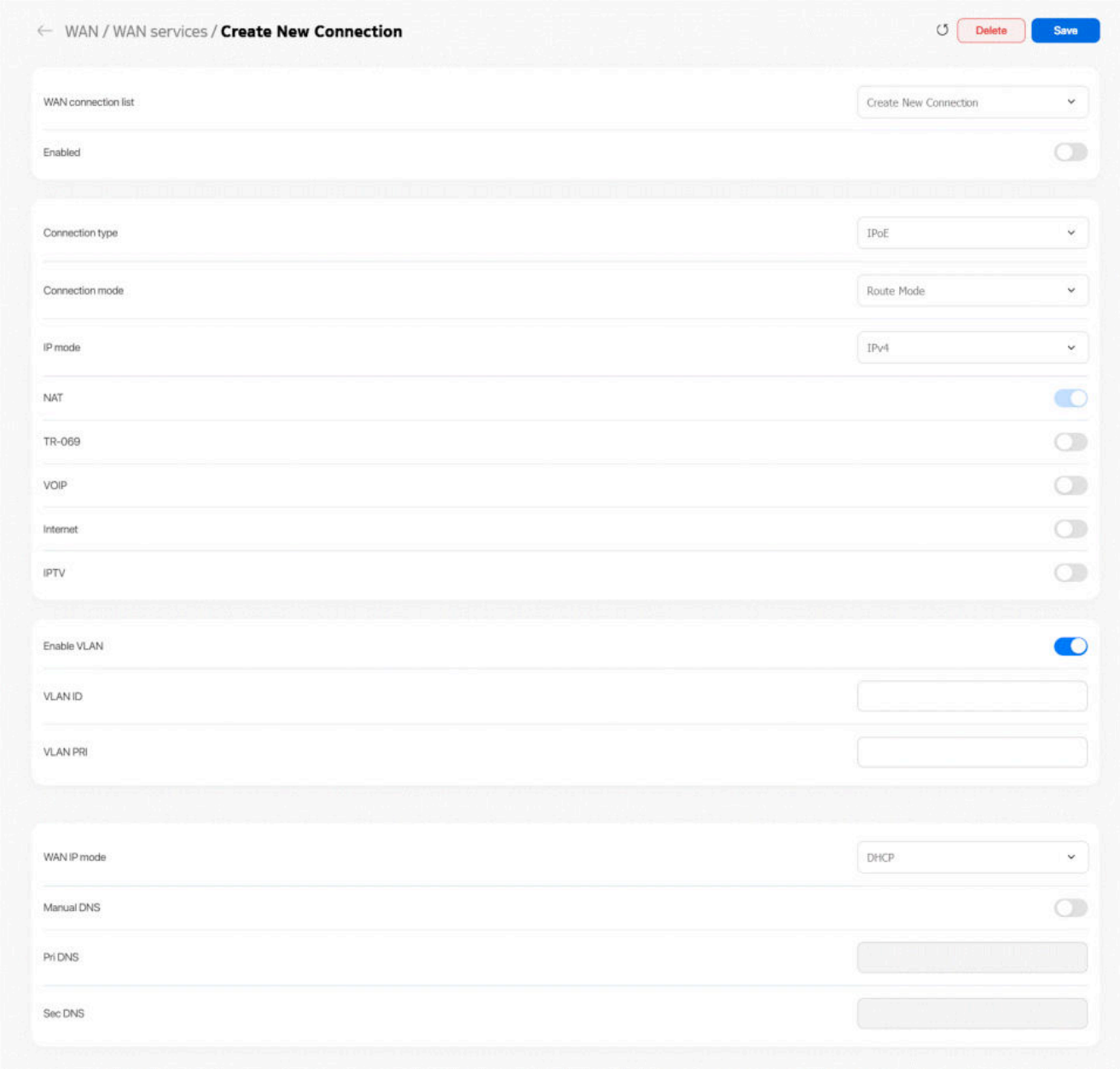


Figure 7-5 Create New Connection page - PPPoE Configuration

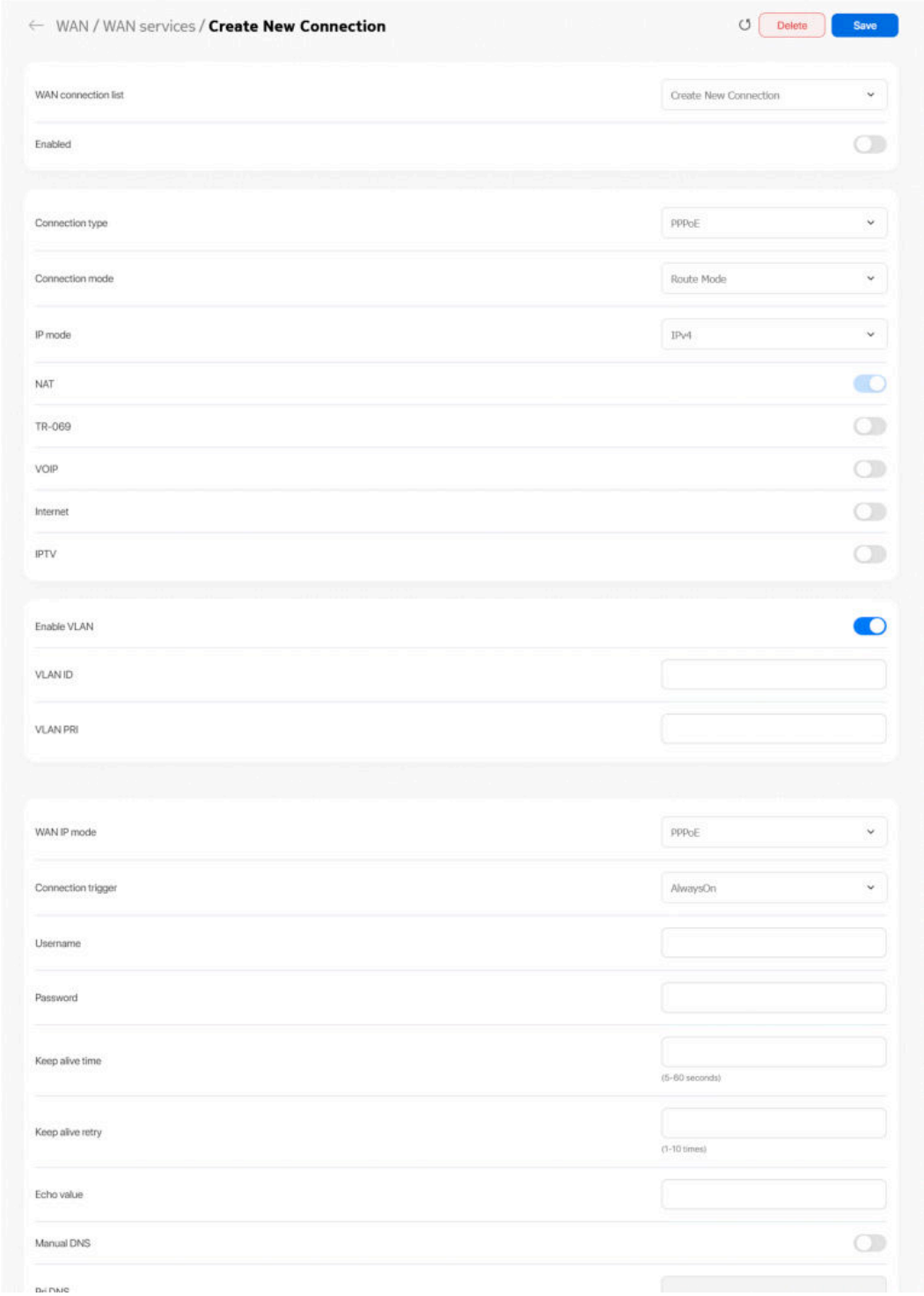


Figure 7-6 VLAN mode - VLAN Binding

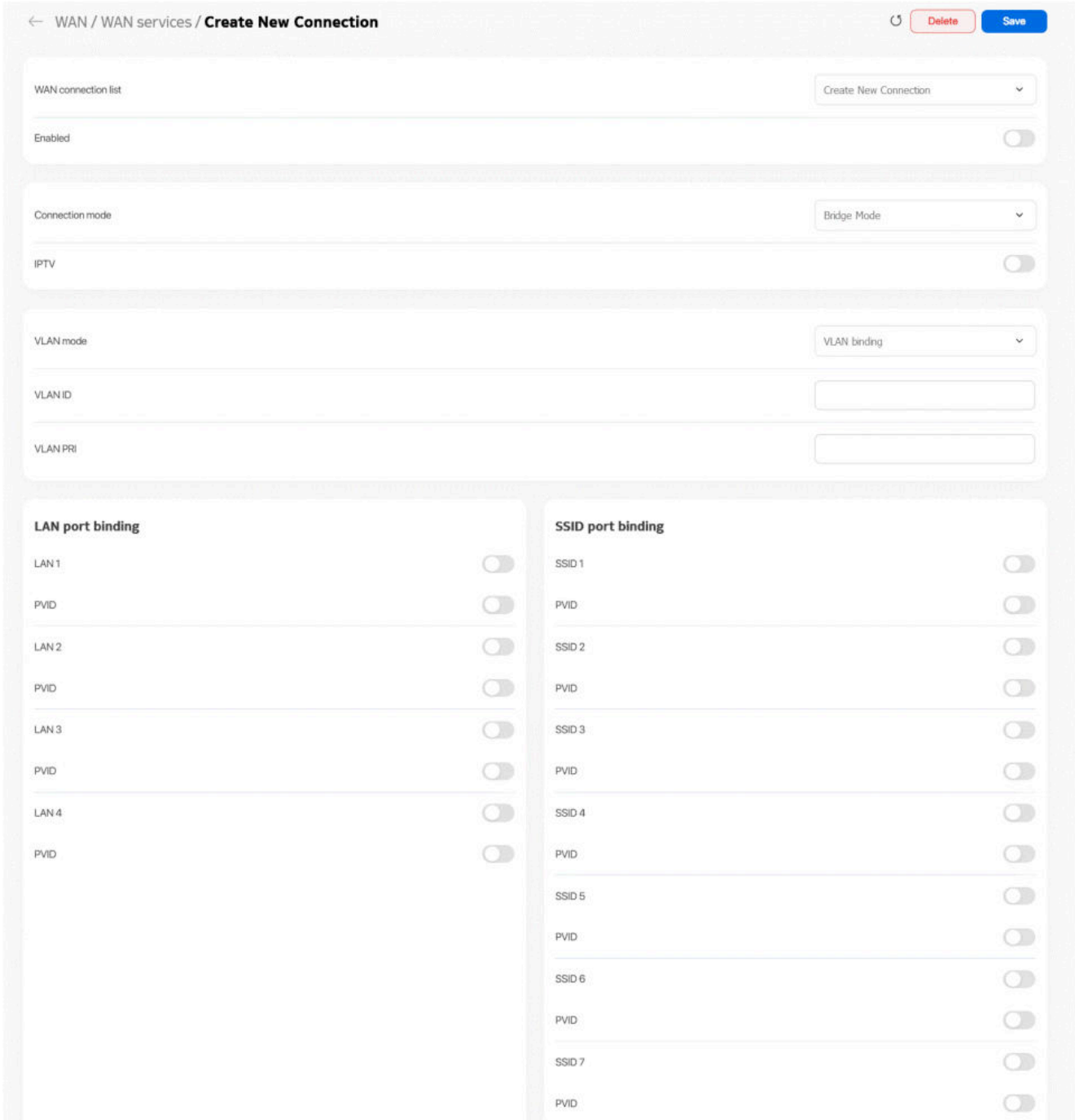


Figure 7-7 Bridge mode - Transparent

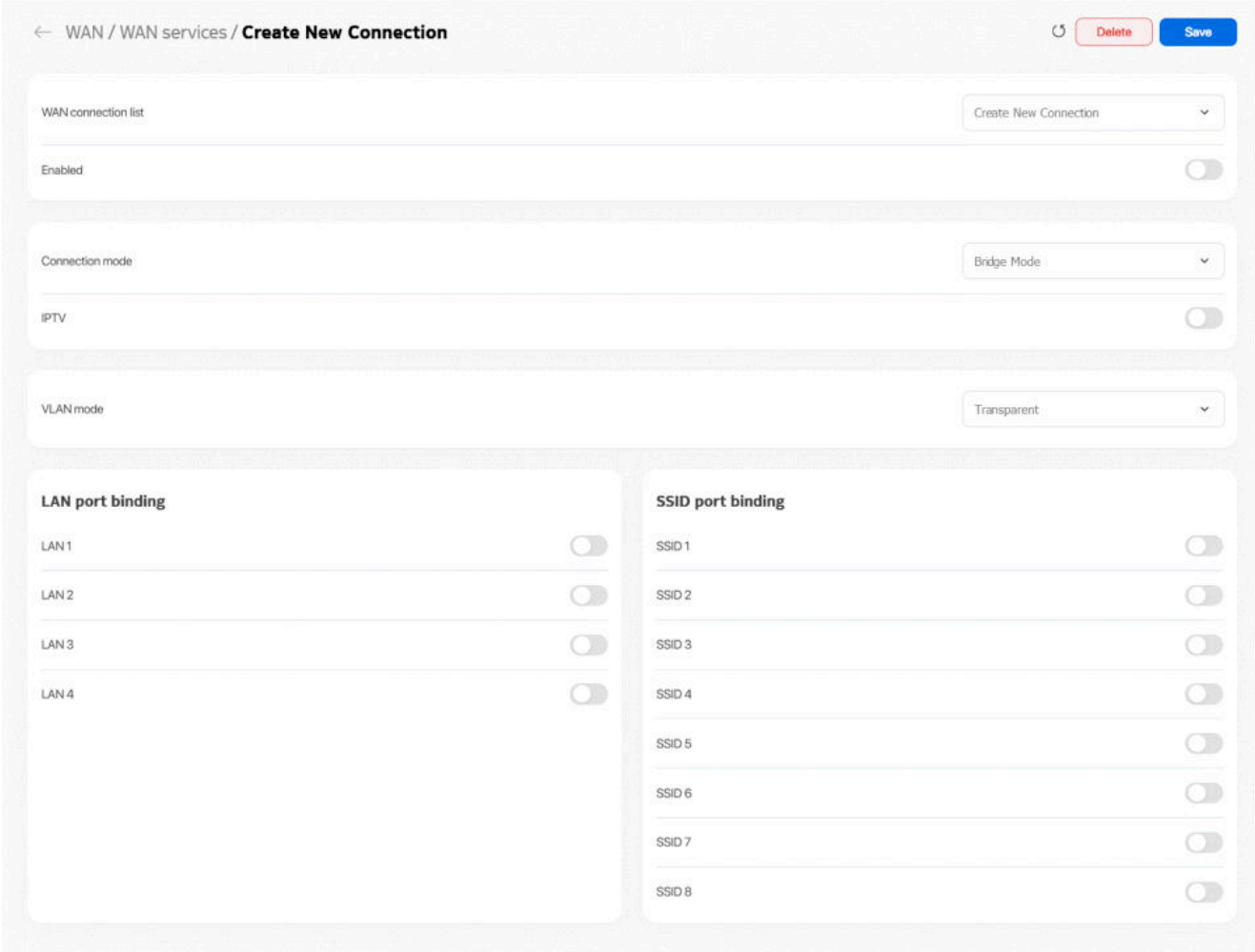
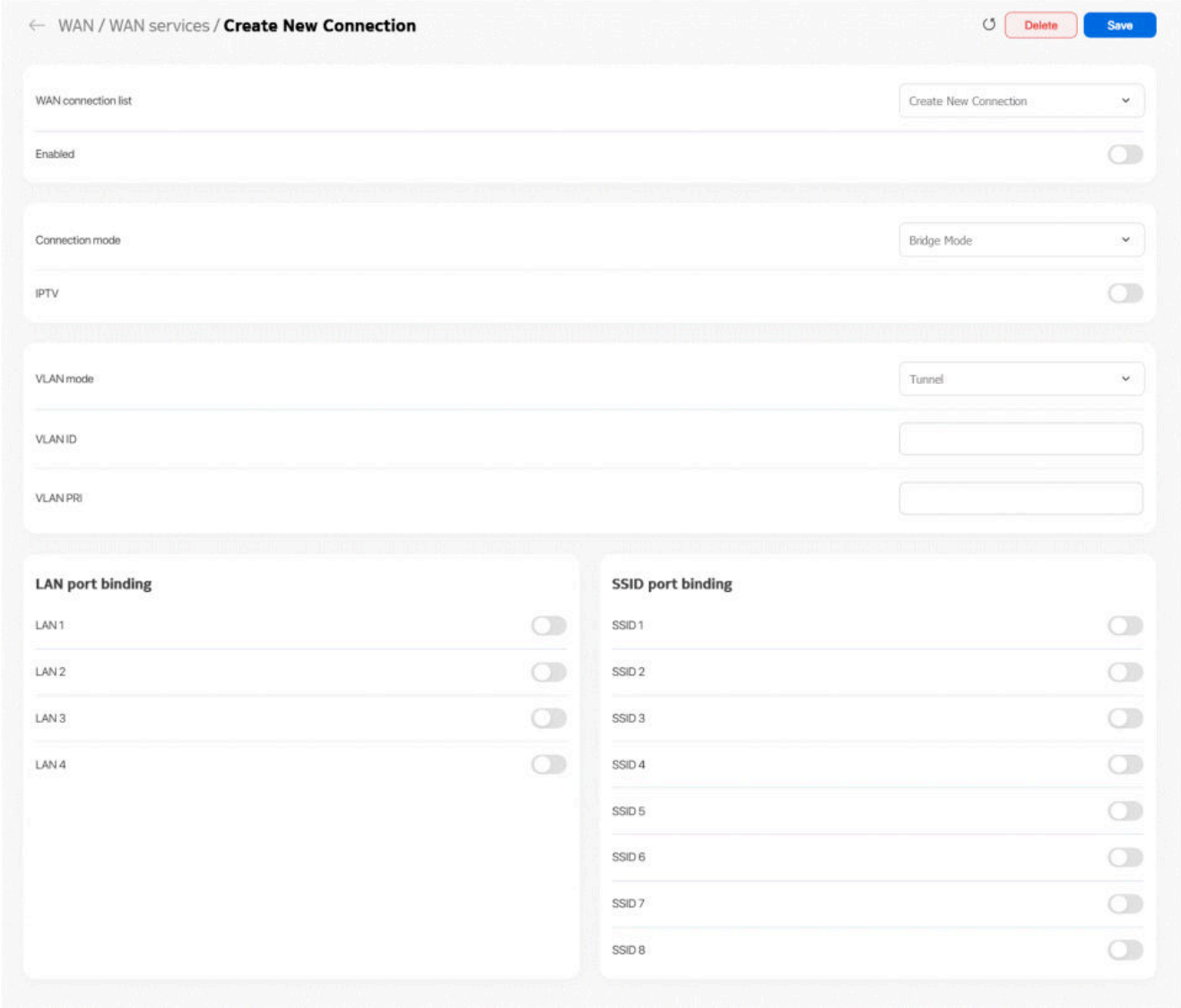


Figure 7-8 Bridge mode - Tunnel



3

Configure the following parameters:

Table 7-3 WAN services parameters

Field	Description
WAN connection list	Select a WAN connection from the list.

Table 7-3 WAN services parameters (continued)

Field	Description
Enabled	Select the toggle button to enable the WAN connection.
Connection type	Select a connection type from the list: • **IPoE** • **PPPoE**
Connection mode	Select the connection mode of the WAN connection from the list: • **Route Mode** • **Bridge Mode**
IP mode	This field is applicable only if the connection mode is **Route Mode**. Select an IP mode from the list: • **IPv4** • **IPv4 & IPv6** • **IPv6** When the IP mode **IPv4 & IPv6** or **IPv6** is selected, you need to configure **Address method**, **Enabled prefix delegation** and **Prefix type**.
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**.
VOIP	Select the toggle button to enable VoIP. This option is applicable only if the connection type is **IPoE** and 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: • **VLAN binding** • **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 **VLAN binding** and **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 **VLAN binding** or **Tunnel**.

Table 7-3 WAN services parameters (continued)

Field	Description
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 applicable in all VLAN modes.
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. You can also enter the Domain Name Server (DNS) to be configured manually if the selected IP mode is **IPv4** and the connection type is **PPPoE**.
IPv4 Address	If the selected IP mode is **IPv4** or **IPv4&IPv6** and the WAN IP mode is **Static**, enter the static IPv4 address.
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). Also, if the selected IP mode is **IPv4** and the Connection type is **PPPoE**, 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). Also, if the selected IP mode is **IPv4** and the Connection type is **PPPoE**, 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**.

Table 7-3 WAN services parameters (continued)

Field	Description
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.
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

7.10 Viewing WAN Statistics

1

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

Figure 7-9 WAN Statistics page

2

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

Figure 7-10 WAN Statistics page info

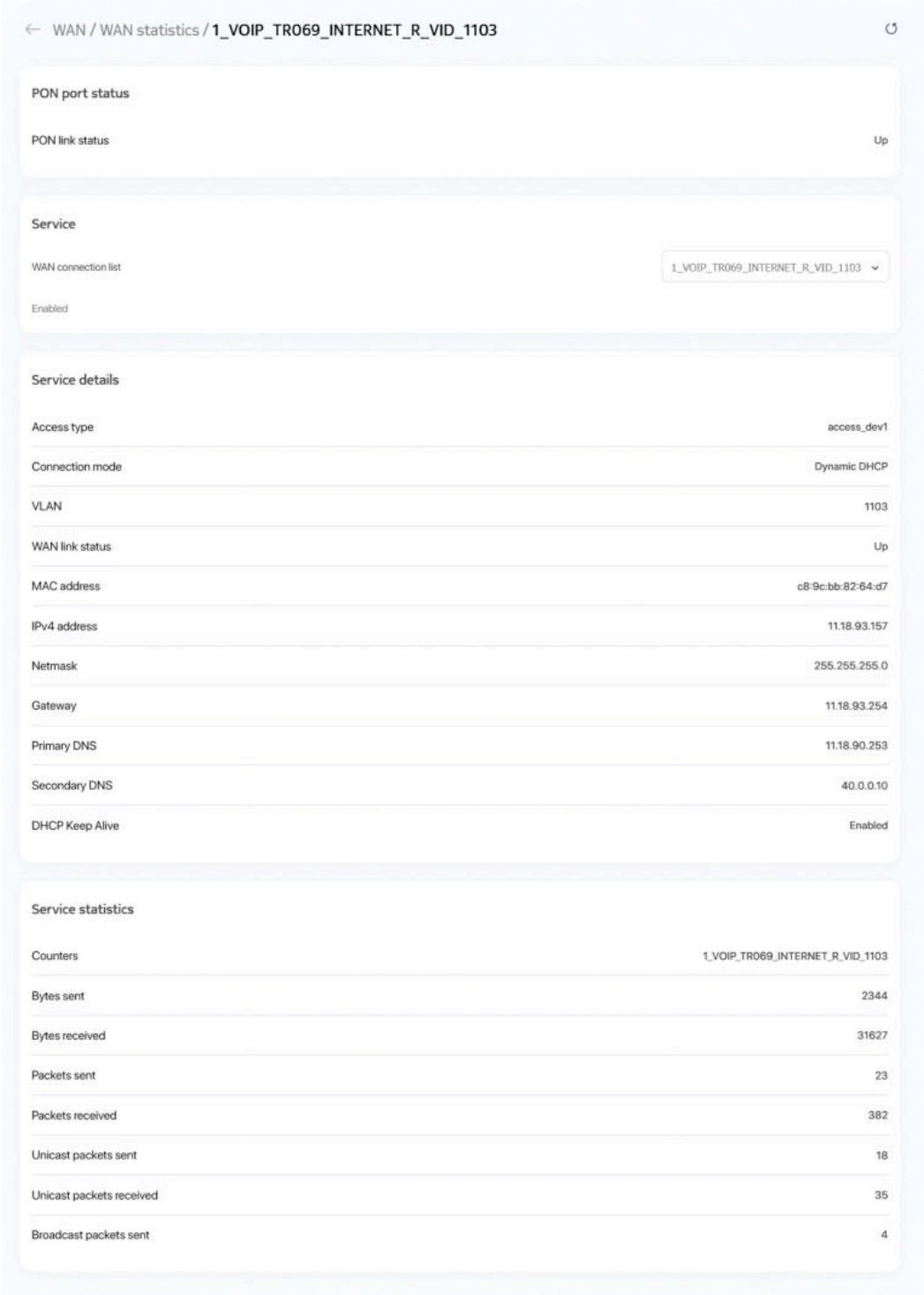


Table 7-4 WAN statistics parameters

Field	Description
PON port status	
PON link status	Displays the PON link status whether it is Up or Down.
Service	
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.
Connection mode	Displays the connection mode of the WAN connection.
VLAN	Displays the VLAN mode based on WAN connection mode.
WAN link status	Displays the WAN status link whether it is Up or Down. This option is available when the IP mode is **IPv4 & IPv6** or **IPv6**.
DHCP Keep Alive	Displays whether the DHCP Keep Alive is enabled or Disabled. This parameter is applicable to Beacon 3.1, Beacon 3.2, Beacon 19, G-1426G-A, G-1426G-B, G-1426G-D, and XS-2437X-B.
PON link status	Displays whether the PON link status is Up or Down. This parameter is applicable to Beacon 3.1, Beacon 3.2, Beacon 19, G-1426G-A, G-1426G-B, G-1426G-D, and XS-2437X-B.
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**.
Service 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.

Table 7-4 WAN statistics parameters (continued)

Field	Description
Rx/Tx errors	Displays the Rx/Tx error packets.

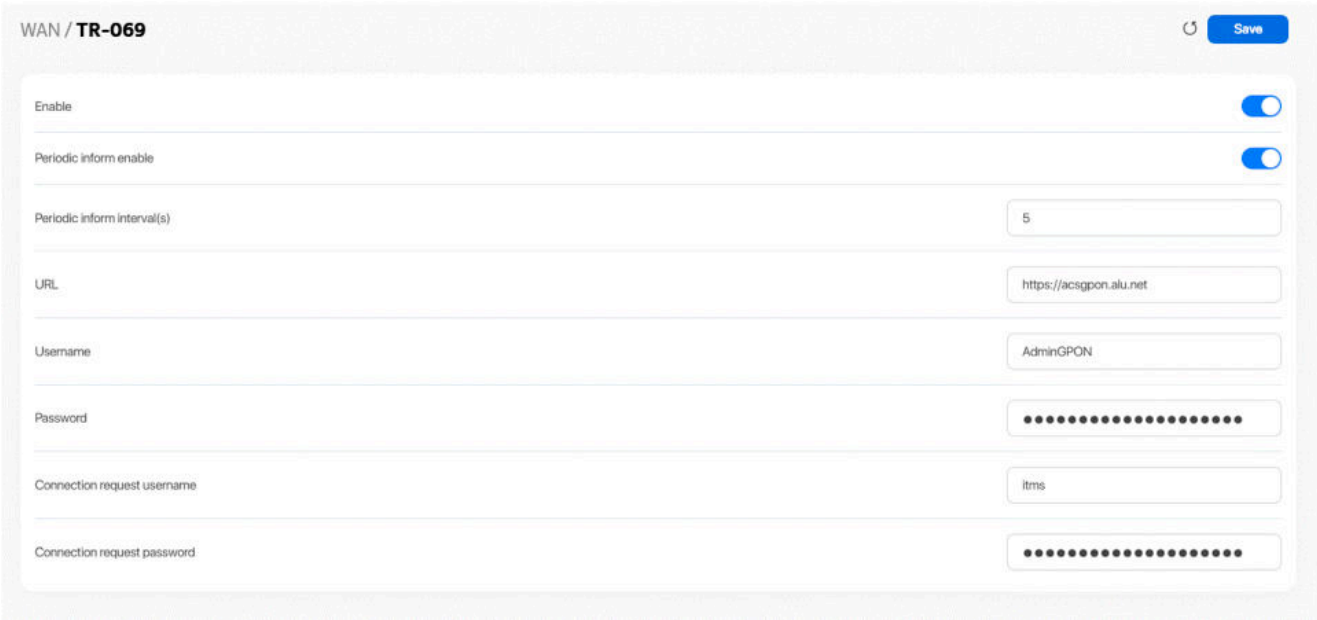
END OF STEPS

7.11 Configuring TR-069

1

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

Figure 7-11 TR-069 page



2

Configure the following parameters:

Table 7-5 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.

Table 7-5 TR-069 parameters (continued)

Field	Description
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 ONT.
Password	Enter the password to log in to the ONT.
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

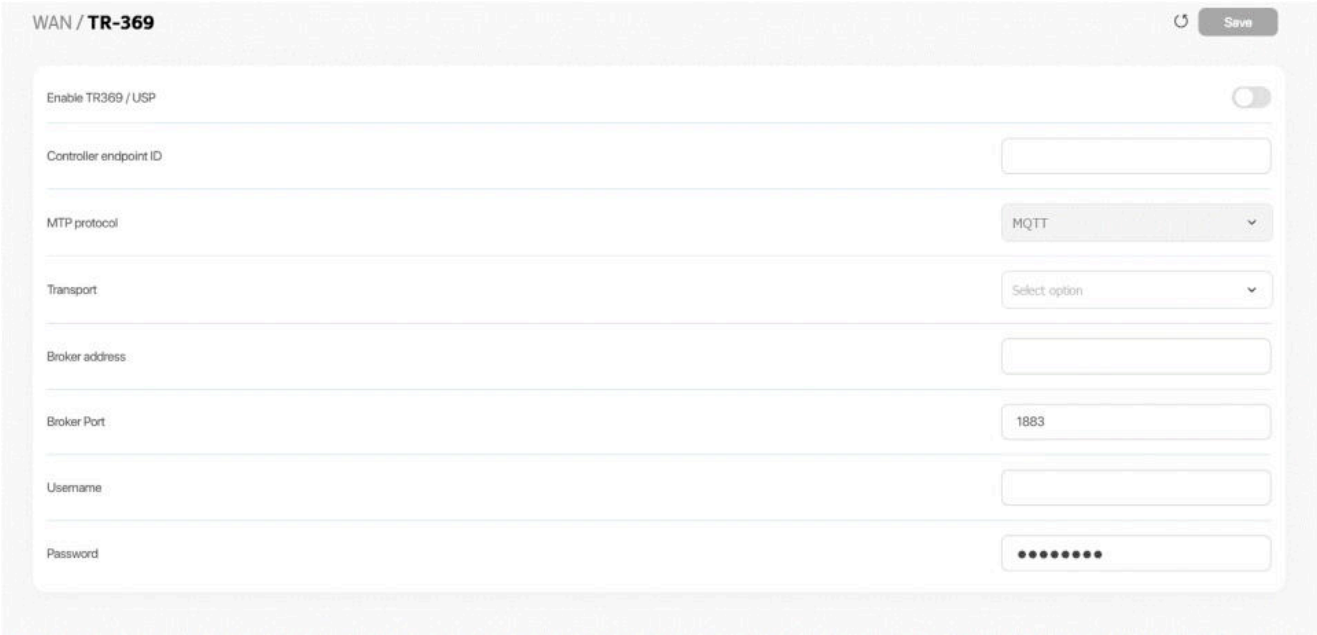
7.12 Configuring TR-369

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 7-12 TR-369 page



2

Configure the following parameters:

Table 7-6 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.
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**.

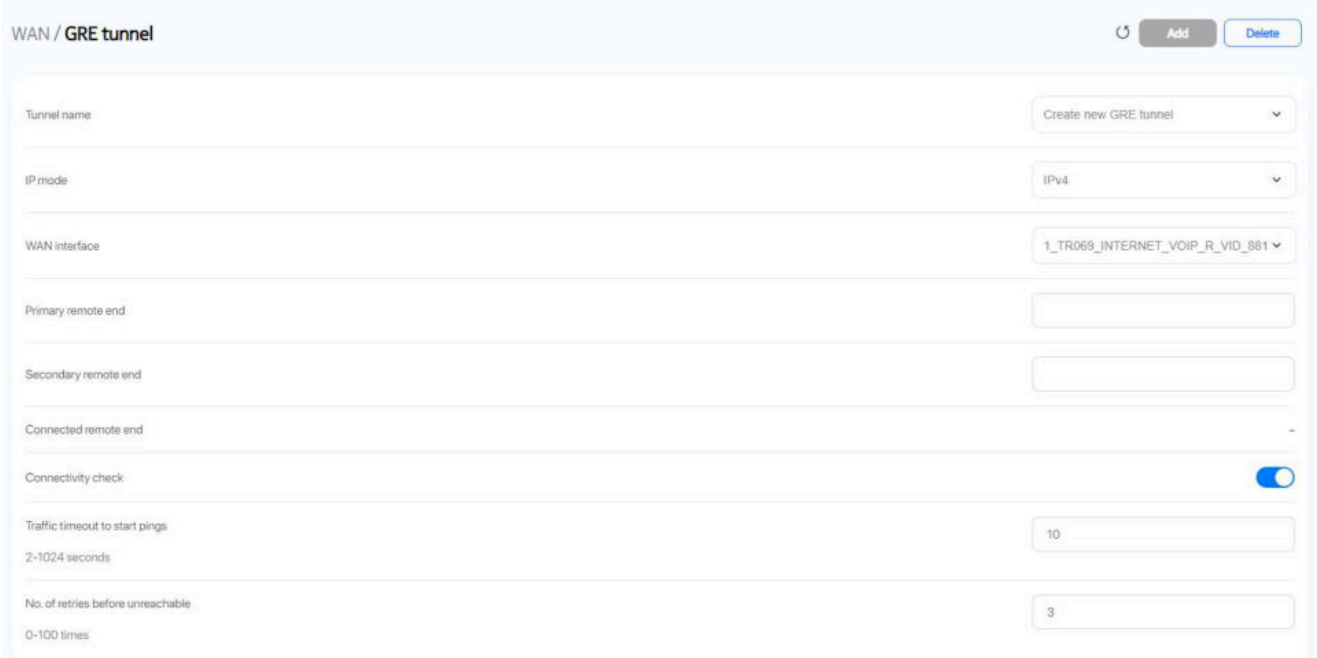
END OF STEPS

7.13 Configuring GRE tunnel

1

Click **WAN→GRE Tunnel** from the left pane in the GPON Home Gateway page. The GRE Tunnel page displays.

Figure 7-13 GRE Tunnel page



2

Configure the following parameters:

Table 7-7 GRE Tunnel parameters

Field	Description
Tunnel Name	Select **Create new GRE Tunnel** or select an existing tunnel from the list. The tunnel name is automatically assigned by the system. Up to 3 GRE tunnels are supported.
IP mode	Select an IP mode from the drop-down list.
WAN Interface	Select a WAN interface from the list. GRE tunnels can only be created on HSI-enabled WAN interfaces.
Primary Remote End Secondary Remote End (optional)	Enter an IP address or FQDN that is unique in the system. If the primary remote endpoint is down or unreachable, the secondary remote endpoint becomes active, if configured. The secondary remote endpoint remains active until it becomes unreachable, in which case the primary remote endpoint becomes active again. Revertive mode is not supported. If both endpoints are unreachable, the GRE tunnel is declared down.
Connected Remote End	This field displays the current data traffic path for the GRE tunnel.
Connectivity check	This feature is automatically selected by the system.

Draft

Table 7-7 GRE Tunnel parameters (continued)

Field	Description
Traffic timeout to start pings	Enter the traffic timeout in seconds (2 to 1024).
No. of retries before unreachable	Enter the number of retries before the tunnel is declared down (0 to 100).

3

Click **Save**.

Note: To delete the entries, click **Delete**.

END OF STEPS

7.14 Configuring Static routing

1

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

Figure 7-14 IP routing page

2

Configure the following parameters:

Table 7-8 IP routing parameters

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

7.15 Viewing Optical Module Status

1

Click **WAN→Optical module status** in the left pane. The *Optical module status* page displays the following information.

Figure 7-15 Optical module status page

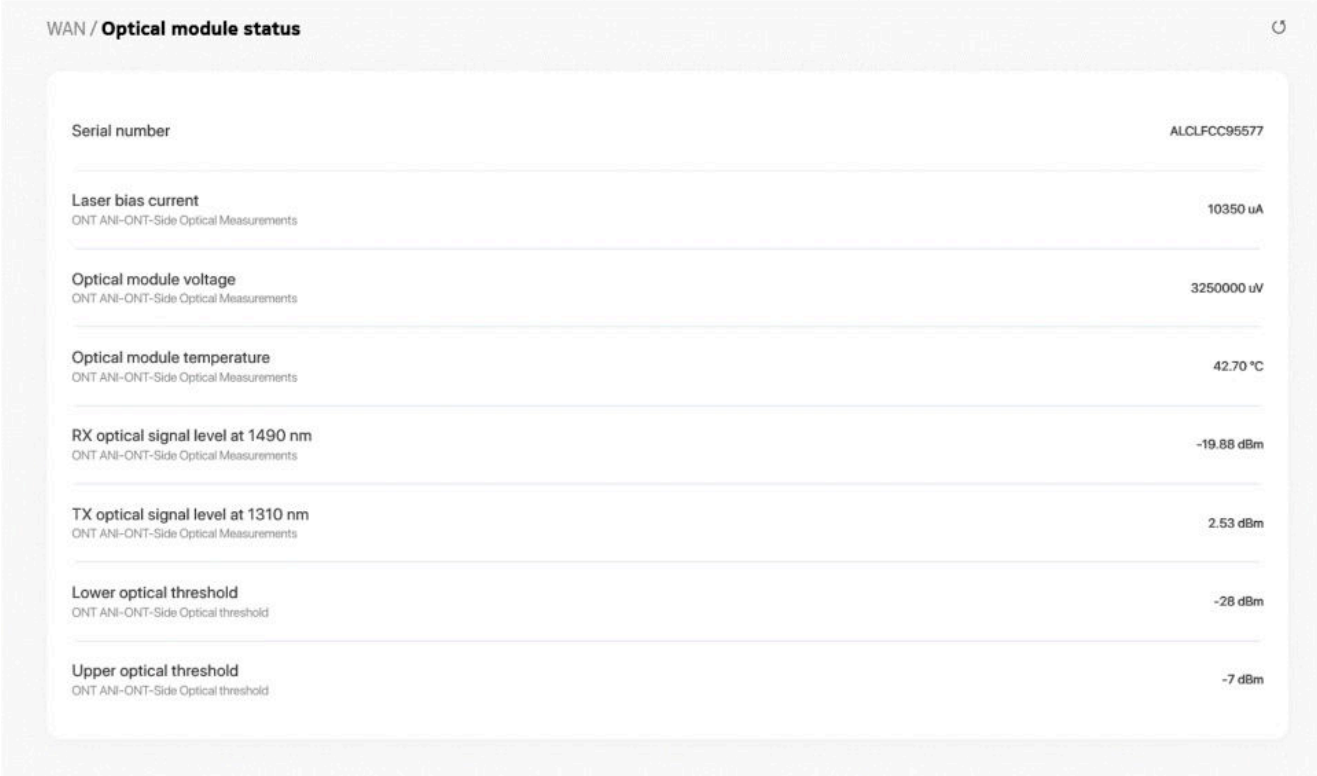


Table 7-9 Optical module status parameters

Field	Description
Serial Number	Indicates the serial number.
Laser bias current (ONT ANI-ONT-Side Optical Measurements)	Laser bias current, measured in uA.
Optics module voltage (ONT ANI-ONT-Side Optical Measurements)	Optics module voltage, measured in V.
Optics module temperature (ONT ANI-ONT-Side Optical Measurements)	Optics module temperature, measured in C.
Rx optics signal level at 1490 nm (ONT ANI-ONT-Side Optical Measurements)	Received optics signal level at 1490 nm, measured in dBm.
Rx optics signal level at 1310 nm (ONT ANI-ONT-Side Optical Measurements)	Transmitted optics signal level at 1310 nm, measured in dBm.
Lower (ONT ANI-ONT-Side Optical Threshold)	Lower optical threshold, measured in dBm.
Upper (ONT ANI-ONT-Side Optical Threshold)	Upper optical threshold, measured in dBm.

END OF STEPS

7.16 Configuring QoS

1

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

Figure 7-16 QoS config page (L2 Criteria)

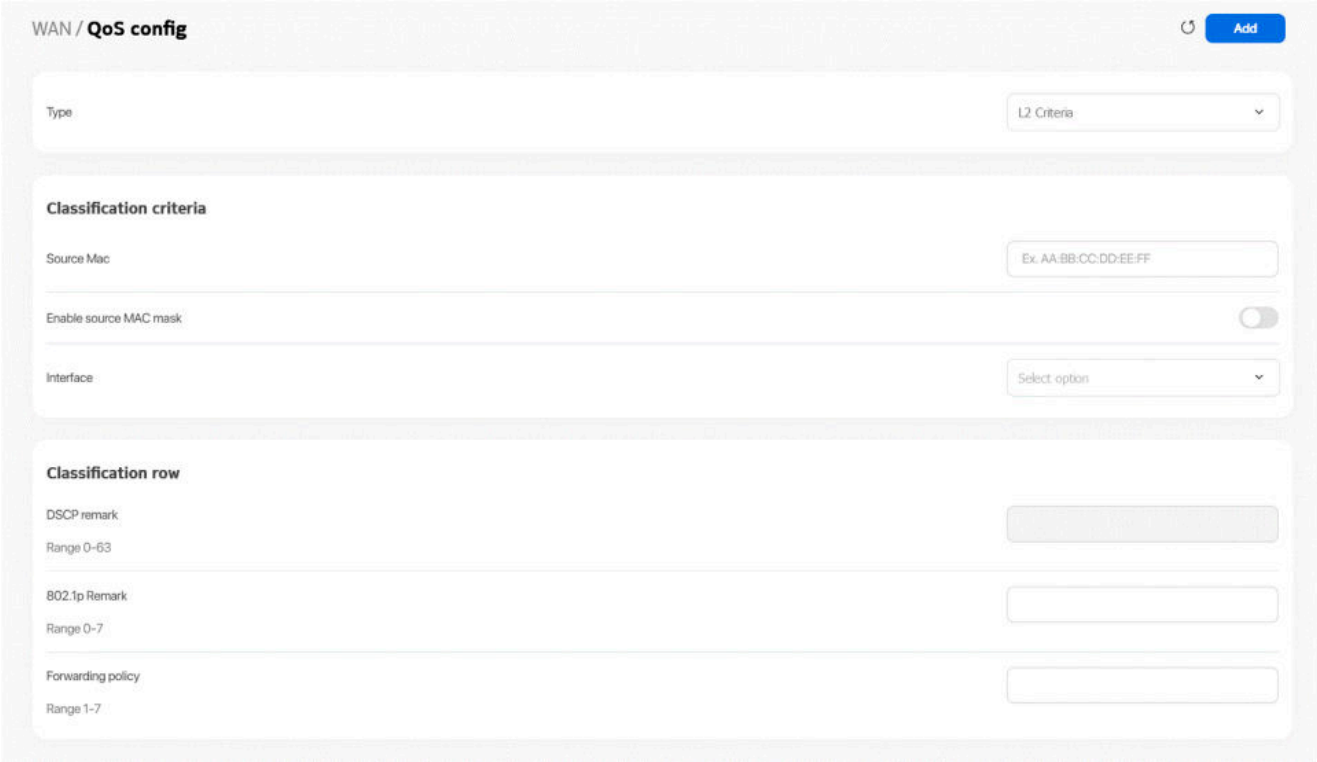
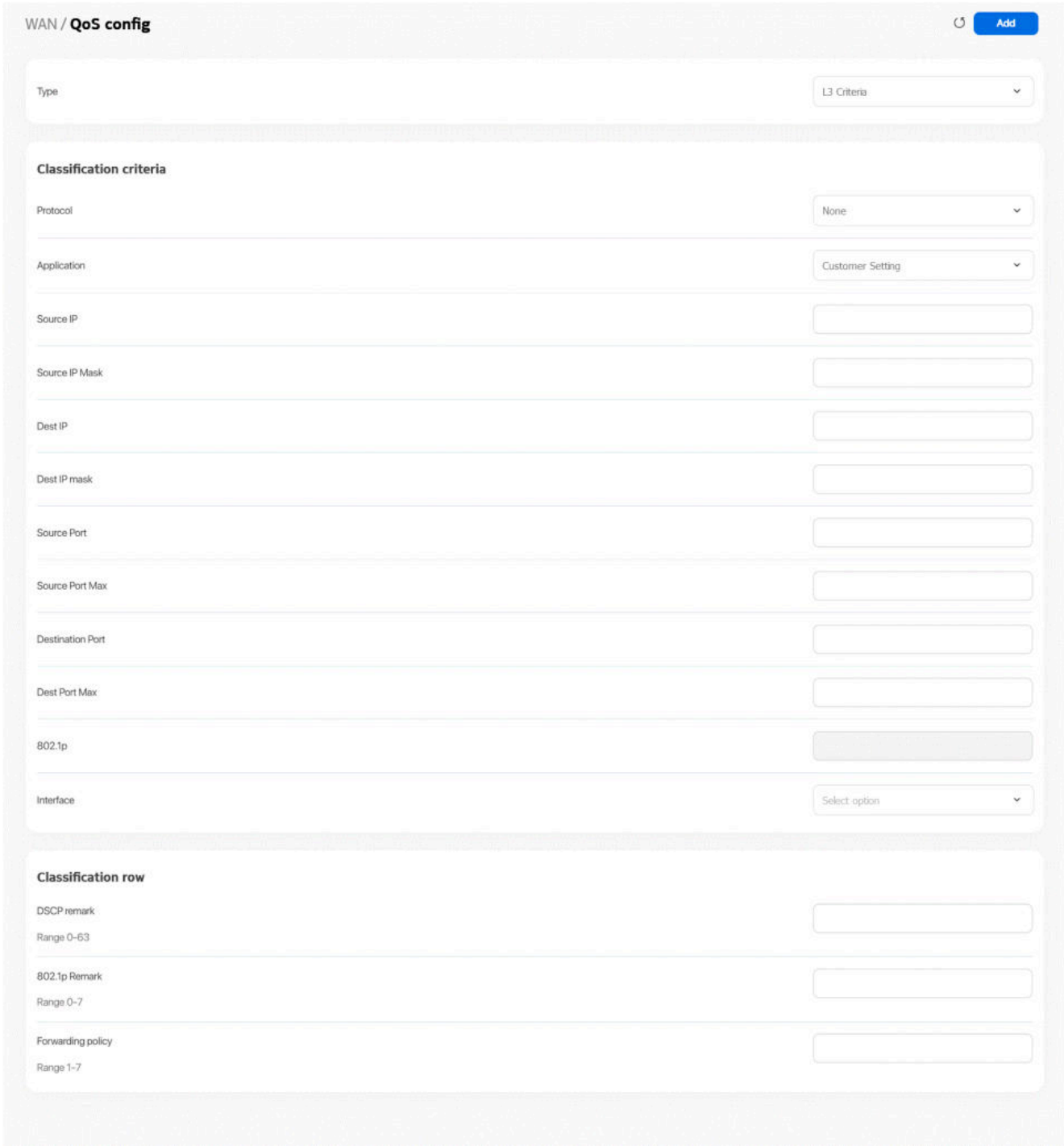


Figure 7-17 QoS config page (L3 Criteria)



2

Configure the following parameters:

Table 7-10 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.
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

7.17 Configuring Upstream (US) Classifier

The US Classifier feature is used to create policies, classifiers, and classifier rules for upstream traffic handling. This feature is available to admin users (super users) only.

A policy defines an action to be performed on a set of LAN or WAN packets. A policy can be created at any time and then subsequently assigned to one or more classifiers.

A classifier is used to select key fields for which the classifier rules will be written. A classifier can be created at any time and then subsequently assigned to one or more classifier rules.

A classifier rule is used to assign actions to a group of packets based on a set of parameters. A classification rule must be created against a pre-defined classifier.

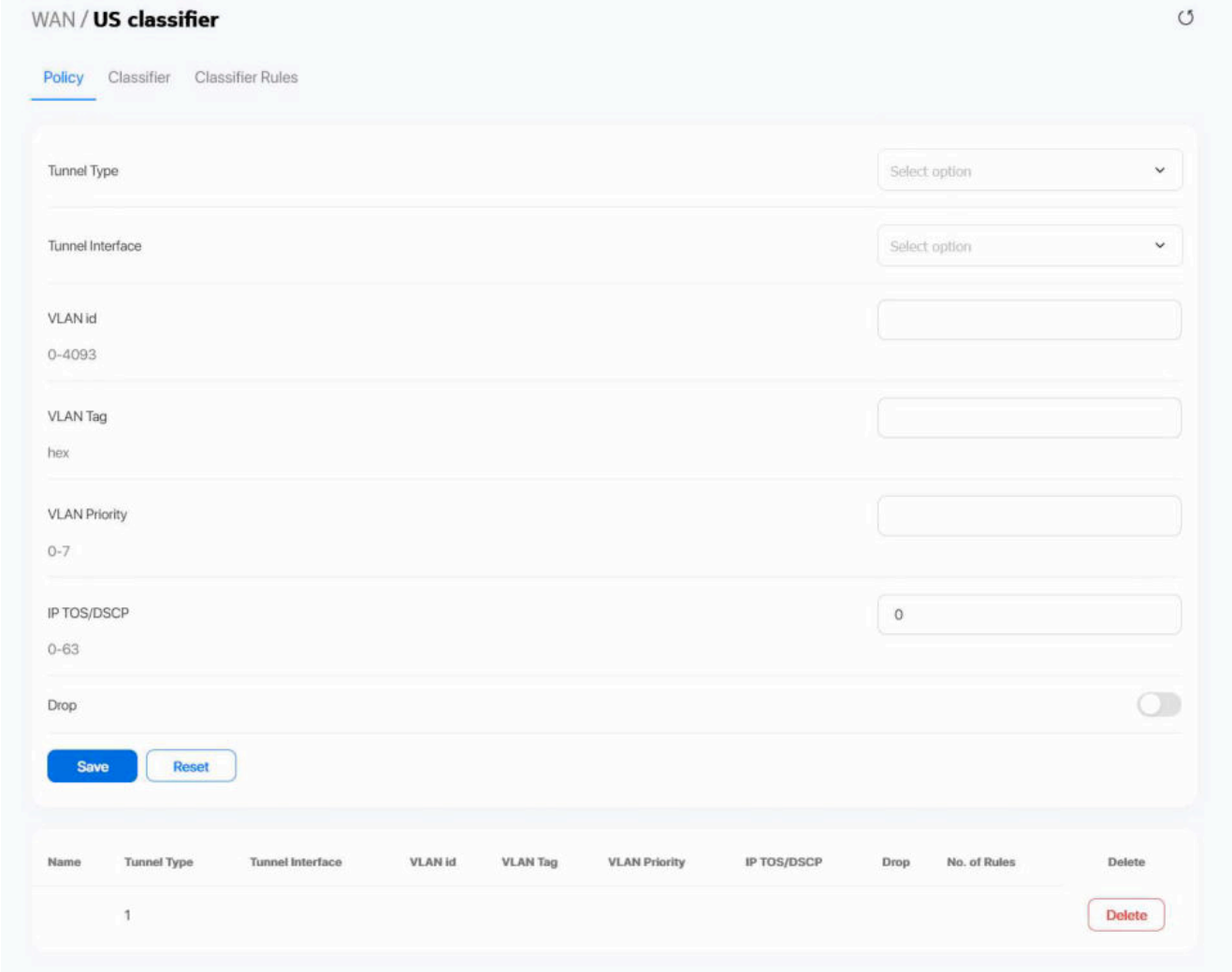
Up to 16 policies can be created, with up to 8 classifiers and 32 classifier rules.

1

Click **WAN→US Classifier** in the left pane and select the **Policy** tab.

All classifier policies are displayed in the policy table in the page.

Figure 7-18 US Classifier - Policy page



2

Configure the following parameters:

Table 7-11 US Classifier - Policy parameters

Field	Description
Tunnel Type	The tunnel type is set to GRE and cannot be modified.

Table 7-11 US Classifier - Policy parameters (continued)

Field	Description
Tunnel Interface	Select a tunnel interface from the list: • **No Tunnel** • The tunnel interface values **No Tunnel**, **GRE Tunnel**, and **LAN traffic** are applicable to: G-1425G-E, G-1425G-H, XS-2426X-A, XS-2426G-B, • The tunnel interface value **No Tunnel** is applicable to: G-1426G-A, G-1426G-B, G-1426G-D, XS-2437X-B
VLAN ID	Enter a VLAN ID. Allowed values: 0 to 4093
VLAN Tag	This field is not configurable. The VLAN tag is set to 8100 (hexadecimal). Determines the VLAN tag used inside the GRE tunnel.
VLAN Priority	Enter a VLAN priority level. A lower number indicates a higher priority. Allowed values: 0 to 7
IP TOS/DSCP	This field is not configurable. All tunnel packets are generated with a default DSCP value (usually 0). Allowed values: 0 to 63
Drop	Select the toggle button to enable dropping of the packets.

3

Click **Save**. The policy is added to the policies table.

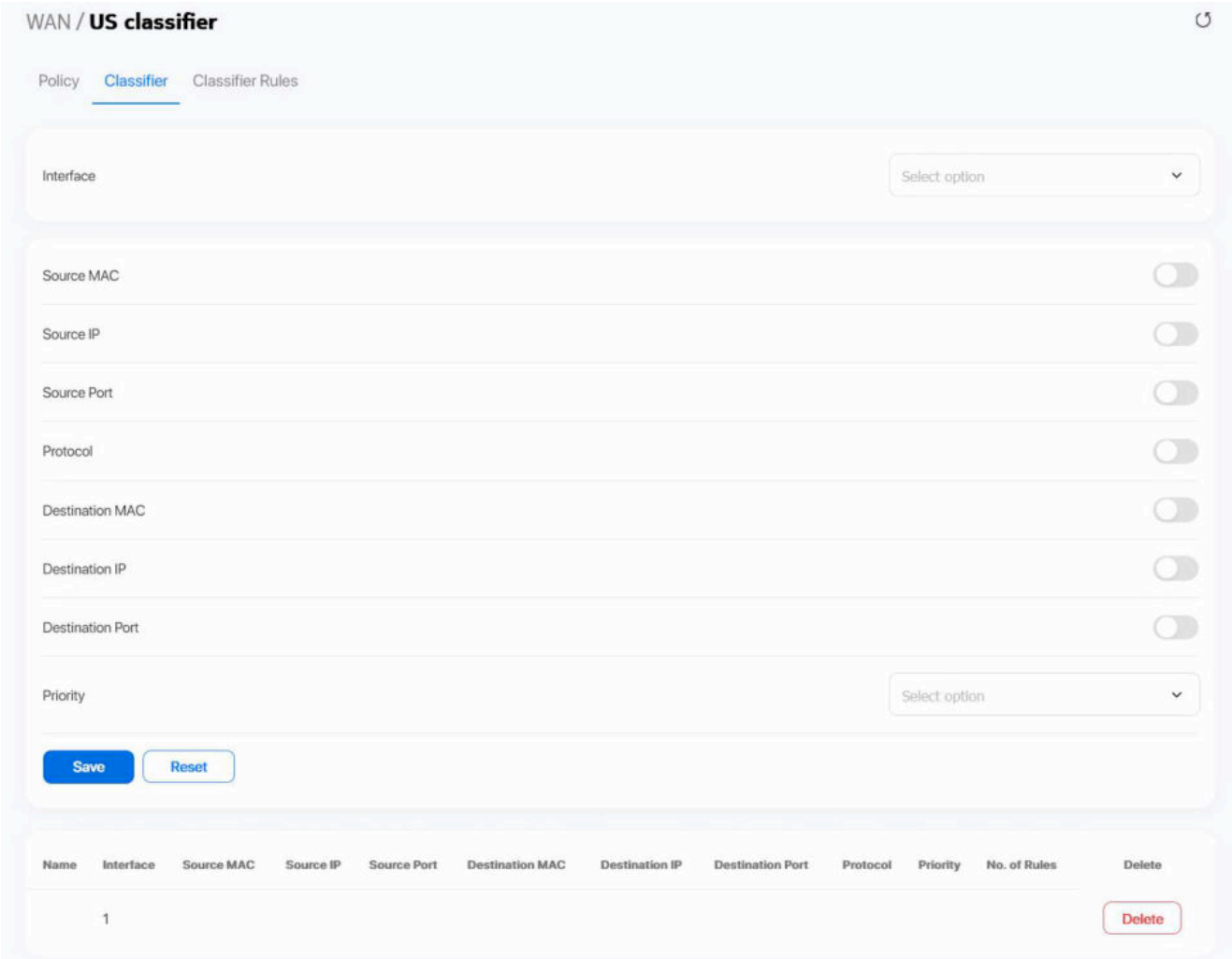
To delete a policy, click **Delete** next to the policy entry in the table. A policy can only be deleted if it is not associated with any classifier rules.

4

Select the **Classifier** tab.

All classifiers are displayed in the classifier table in the page.

Figure 7-19 US Classifier - Classifier page



5

Configure the following parameters:

Table 7-12 US Classifier - Classifier parameters

Field	Description
Interface	Select an interface from the list; for example, None, LAN, 2.4G SSID, or 5G SSID. The option **None** indicates that all interfaces are selected.
Source MAC	Select the toggle button to enter a source MAC address.
Source IP	Select the toggle button to enter a source IP address.

Draft

Table 7-12 US Classifier - Classifier parameters (continued)

Field	Description
Source Port	Select the toggle button to enter a source port.
Protocol	Select the toggle button to enter a protocol.
Destination MAC	Select the toggle button to enter a destination MAC address.
Destination IP	Select the toggle button to enter a destination IP address.
Destination Port	Select the toggle button to enter a destination port.
Priority	Select a priority level from 1 to 8. The lower the number, the higher the priority. Only one classifier can be created with the same priority.

6

Click **Save**. The US classifier is listed in the classifiers table.

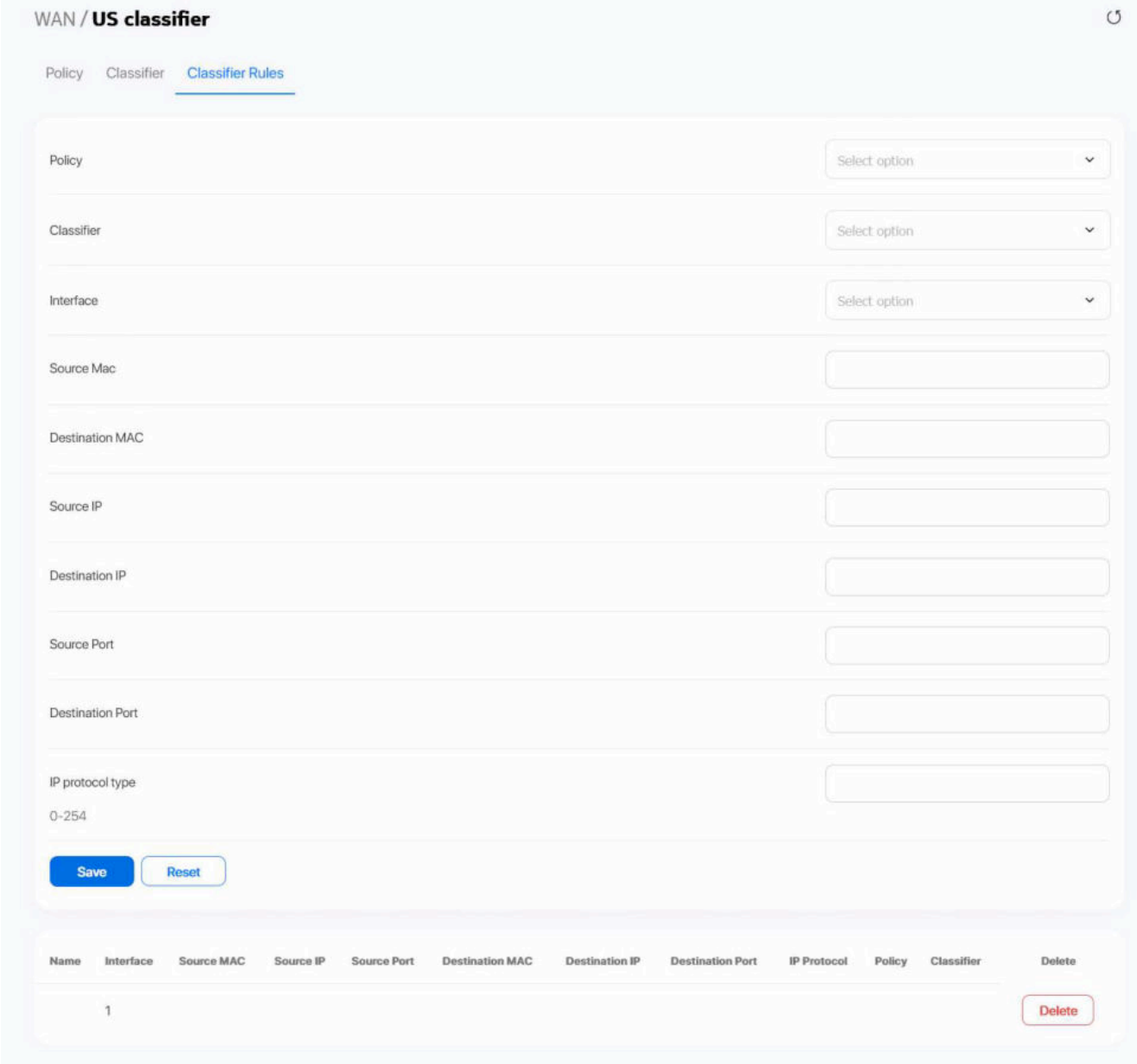
To delete a classifier, click **Delete** next to the classifier entry in the table. A classifier can only be deleted if it is not associated with any classifier rules.

7

Select the **Classifier Rules** tab.

All classifier rules are displayed in the classifier rules table in the page.

Figure 7-20 US Classifier - Classifier Rules page



8

Configure the following parameters:

Table 7-13 US Classifier - Classifier Rules parameters

Field	Description
Policy	Select a policy from the list.
Classifier	Select a classifier from the list.
Interface	Select an interface from the list; for example, None, LAN, 2.4G SSID, 5G SSID.
Source MAC	Enter a source MAC address.
Destination MAC	Enter a destination MAC address.
Source IP	Enter a source IP address.
Destination IP	Enter a destination IP address.
Source Port	Enter a source port.
Destination Port	Enter a destination port.
IP Protocol Type	Enter a value between 0 and 254.

9

Click **Save**. The rule is added to the classifier rules table.

To delete a classifier rule, click **Delete** next to the classifier rule entry in the table.

END OF STEPS

LAN Configuration

7.18 Overview

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

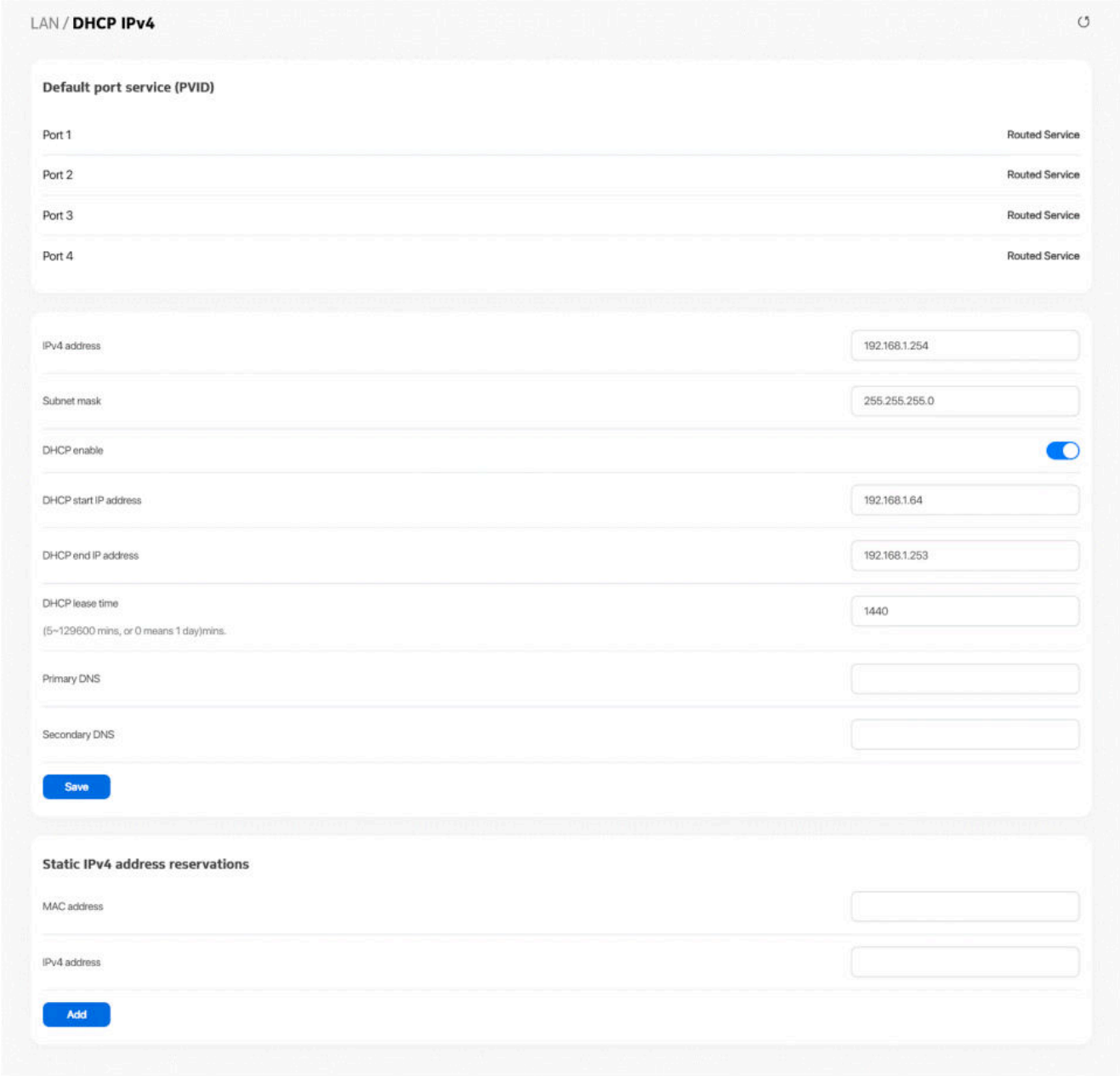
Sub-menu	Procedure
DHCP IPv4	7.19 “Configuring DHCP IPv4” (p. 121)
DHCP IPv6	7.20 “Configuring DHCP IPv6” (p. 123)
DNS	7.21 “Configuring DNS” (p. 125)
LAN statistics	7.22 “Viewing LAN Statistics” (p. 128)

7.19 Configuring DHCP IPv4

1

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

Figure 7-21 DHCP IPv4 page



2

Configure the following LAN parameters:

Table 7-14 DHCP IPv4 parameters

Field	Description
IPv4 address	Enter the IPv4 address of the ONT.
Subnet mask	Enter the subnet mask of the ONT.
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.
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 7-15 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

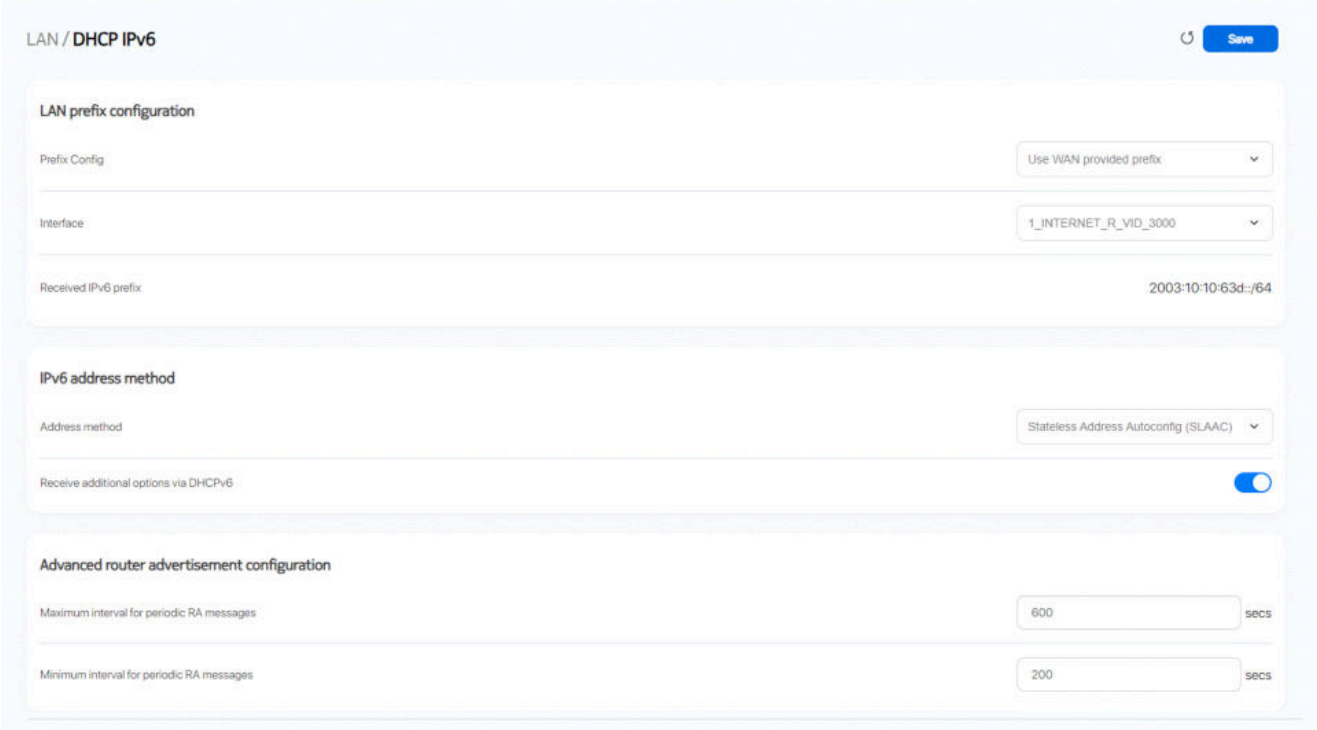
Click **Add**. Repeat steps 4 and 5 for all MAC addresses to be bound.

END OF STEPS

7.20 Configuring DHCP IPv6

1

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



2

Configure the following parameters:

Table 7-16 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	

Table 7-16 DHCP IPv6 parameters (continued)

Field	Description
Address method	Select a address method option from the list: • **Stateless Address Autoconfig (SLAAC)** • **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)**.
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

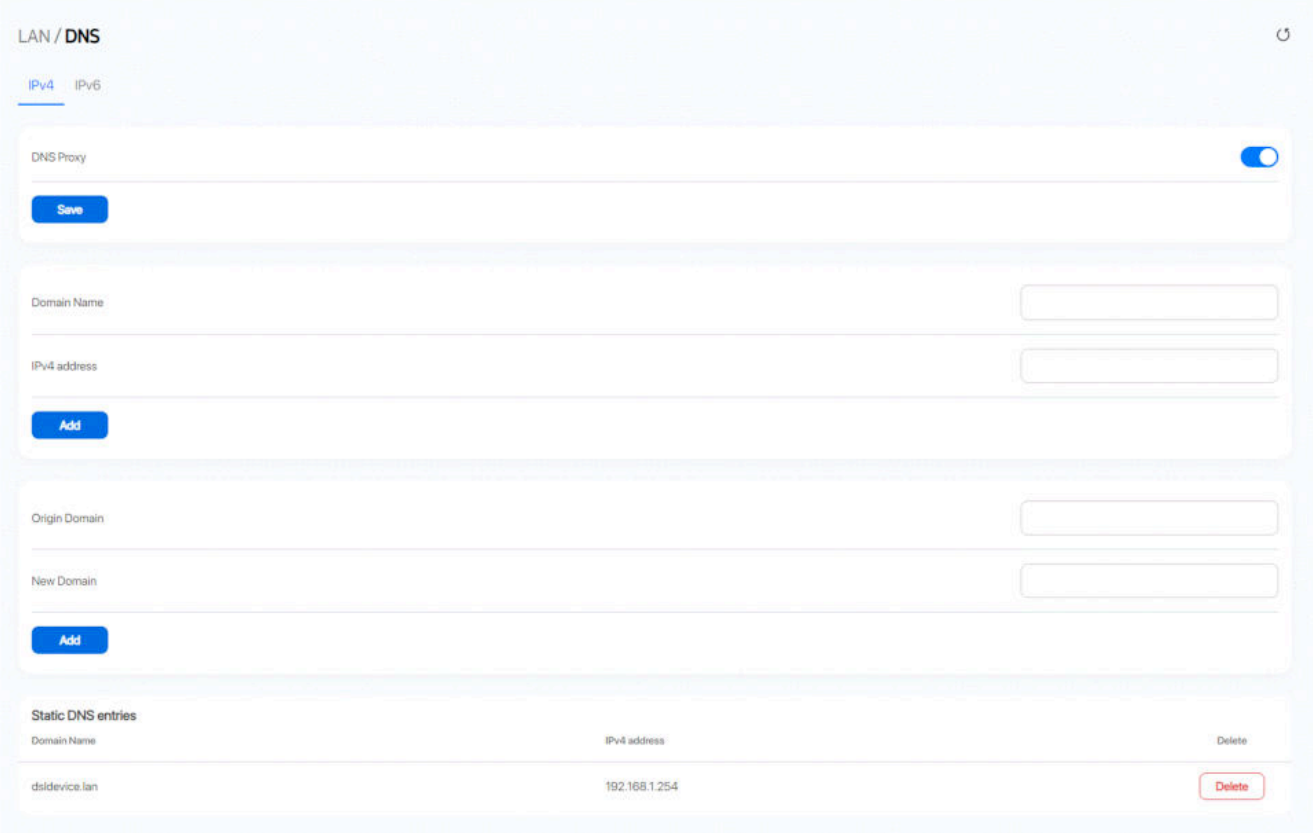
7.21 Configuring DNS

7.21.1 IPv4 DNS configuration

1

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

Figure 7-22 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.

Draft

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

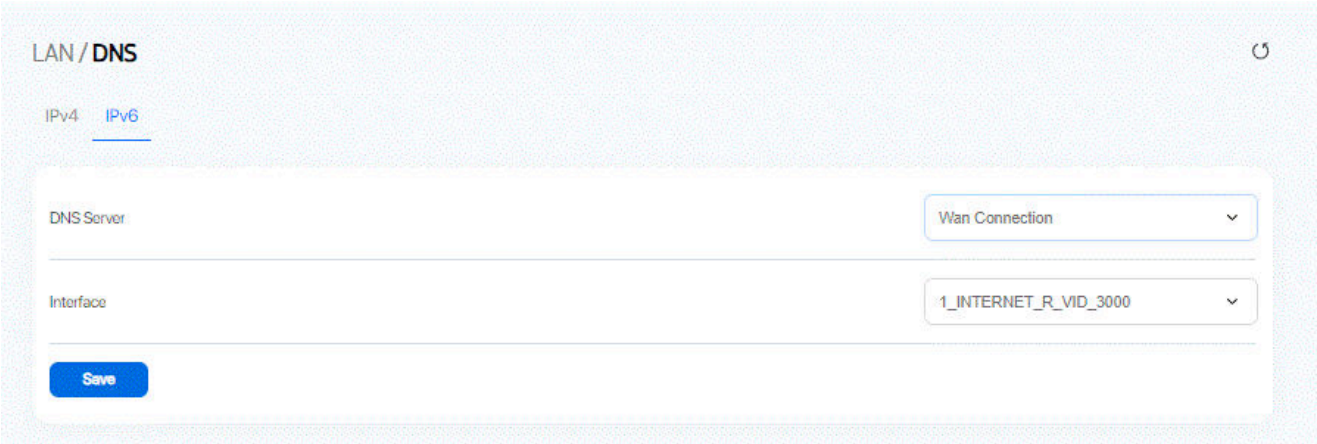
END OF STEPS

7.21.2 IPv6 DNS configuration

1

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

Figure 7-23 DNS page (IPv6)



2

Configure the following parameters

Table 7-17 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.

3

Click **Save**.

END OF STEPS

7.22 Viewing LAN Statistics

1

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

Figure 7-24 LAN statistics page

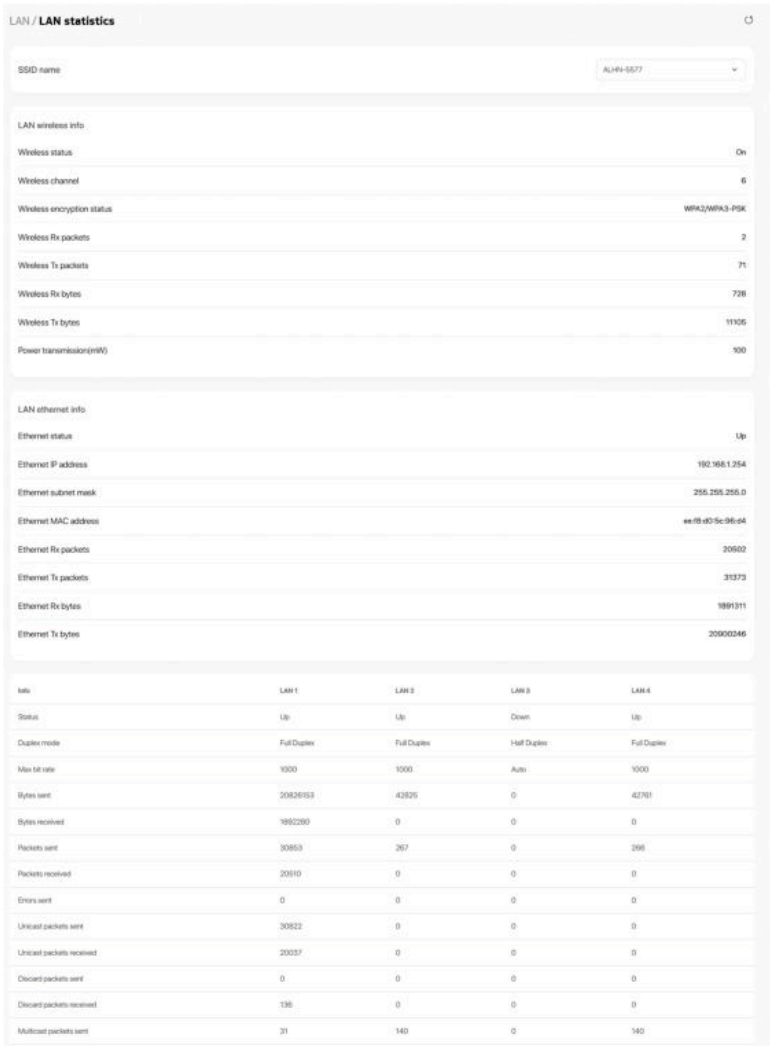


Table 7-18 LAN statistics parameters

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

7.23 Overview

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

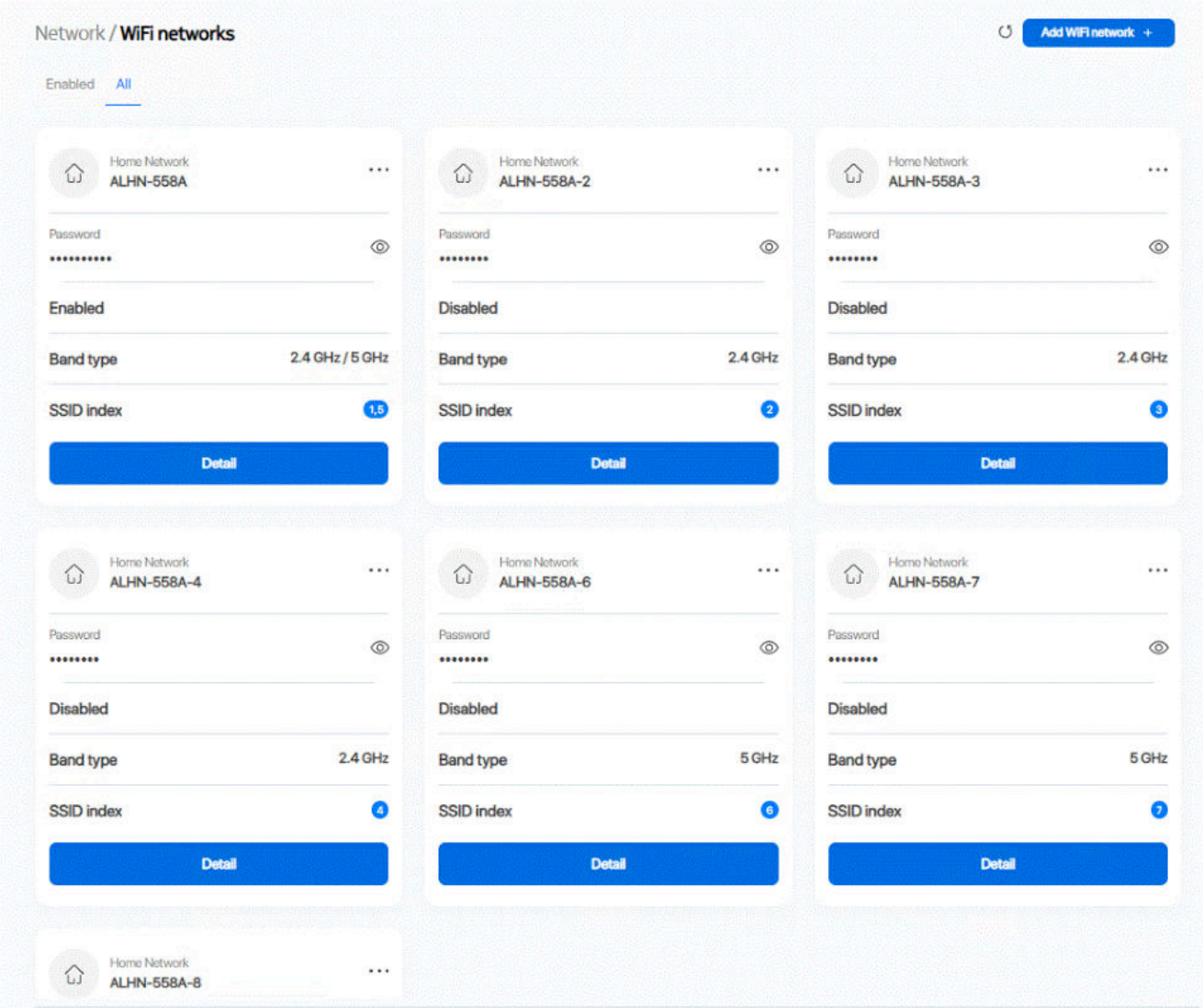
Sub-menu	Procedure
WiFi networks	7.24 “Configuring WiFi Network” (p. 130)
Network map	7.27 “Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points” (p. 137)
Advanced settings	7.28 “Configuring Wireless 2.4 GHz” (p. 141) 7.29 “Configuring Wireless 5 GHz” (p. 143)
Wireless schedule	7.30 “Configuring Wireless Schedules” (p. 145)
WiFi statistics	7.31 “Viewing WiFi Statistics” (p. 146)

7.24 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 7-25 WiFi network page

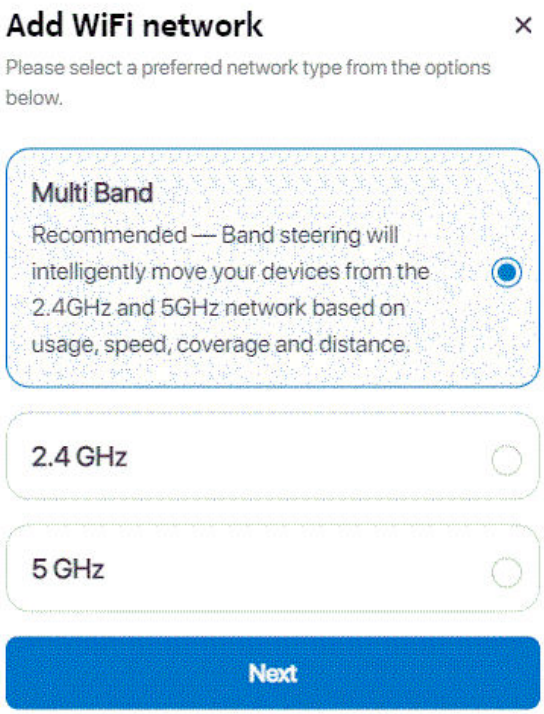


2

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 7-26 Add WiFi network page



3

Configure the following parameters:

Table 7-19 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.

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**.

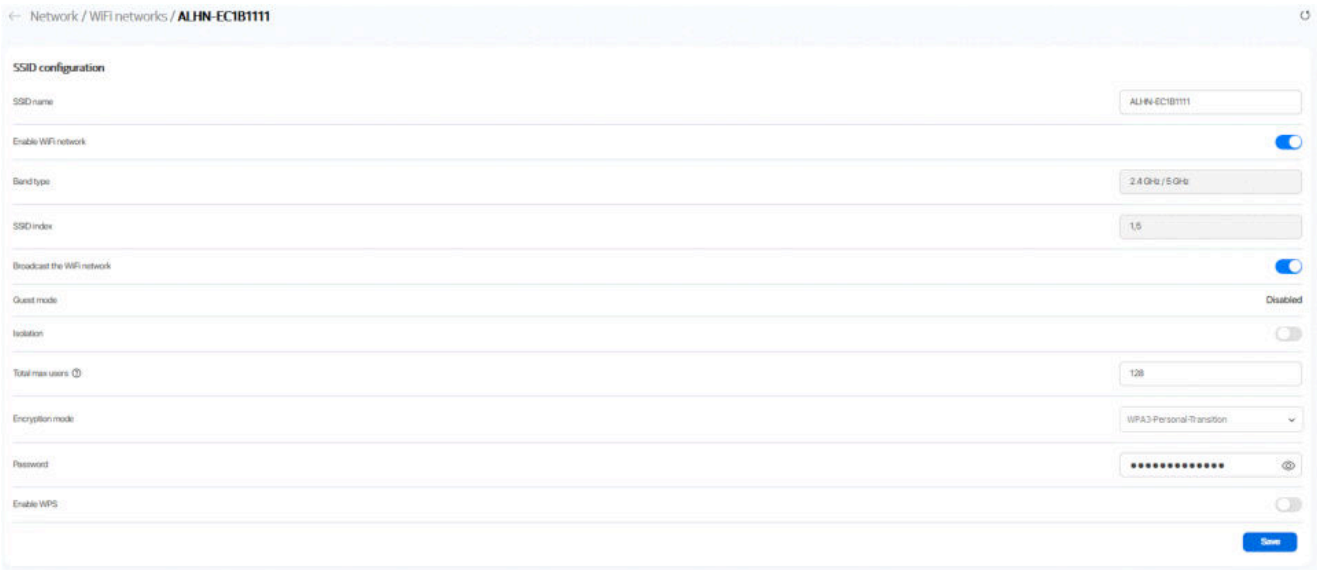
The WiFi network is created and is displayed as a card in the **Enabled** tab of the *WiFi networks* page.

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 7-27 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.

Field	Description
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.
Isolation	Select the toggle button to enable isolation.
Total MAX users	Enter the maximum number of users.
Encryption Mode	Select an encryption mode from the list: • **None** • **WPA2-Personal** • **WPA3-Personal** • **WPA-WPA2-Personal** • **WPA3-Personal-Transition** • **WPA3-Enterprise** • **WPA-WPA2-Enterprise**
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.
WiFi Key	Enter the WiFi key.
Enable WPS	Select the toggle button to enable WPS. **Note:** When you select Enable, a security warning is displayed. Click **OK** to continue.
WPS Mode	Select the required WPS mode from the list: • **PBC** • **STA PIN** • **AP PIN** Select a WPS mode from the list: PBC (Push Button Connect) or STA PIN (Personal Identification Number) or AP PIN (Access Point Personal Identification Number). If the WPS mode is AP PIN, Click **Get PIN Number**. A PIN Code Number is generated. Then, the end user must click **WPS Connect** and enter the generated PIN Code Number into the station, so that the station can connect to the selected SSID. If the WPS mode is STA PIN, the PIN Code Number will be generated by the station. Then, the end user must enter this PIN Code Number into the PIN Code Number field and click **WPS Connect**, so that the station can connect to the selected SSID.
Domain Grouping	Select the toggle button to enable domain grouping.

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

7.25 Configuring the WiFi Password

A password must adhere to the following password rules:

- The password must consist of uppercase letters, lowercase letters, digital numbers, and the following special characters ! # + , -. / : =@_
- The password length must be from 8 to 63 characters.
- The first character must be a digital number or a letter.
- The password must contain all three types of characters: numbers, letters, or special characters.
- The same character must not appear more than 8 times in a row.
- The password cannot be a dictionary password (for example:12345678).

When the password meets the password rules, the application displays the message “Your password has been changed successfully”.

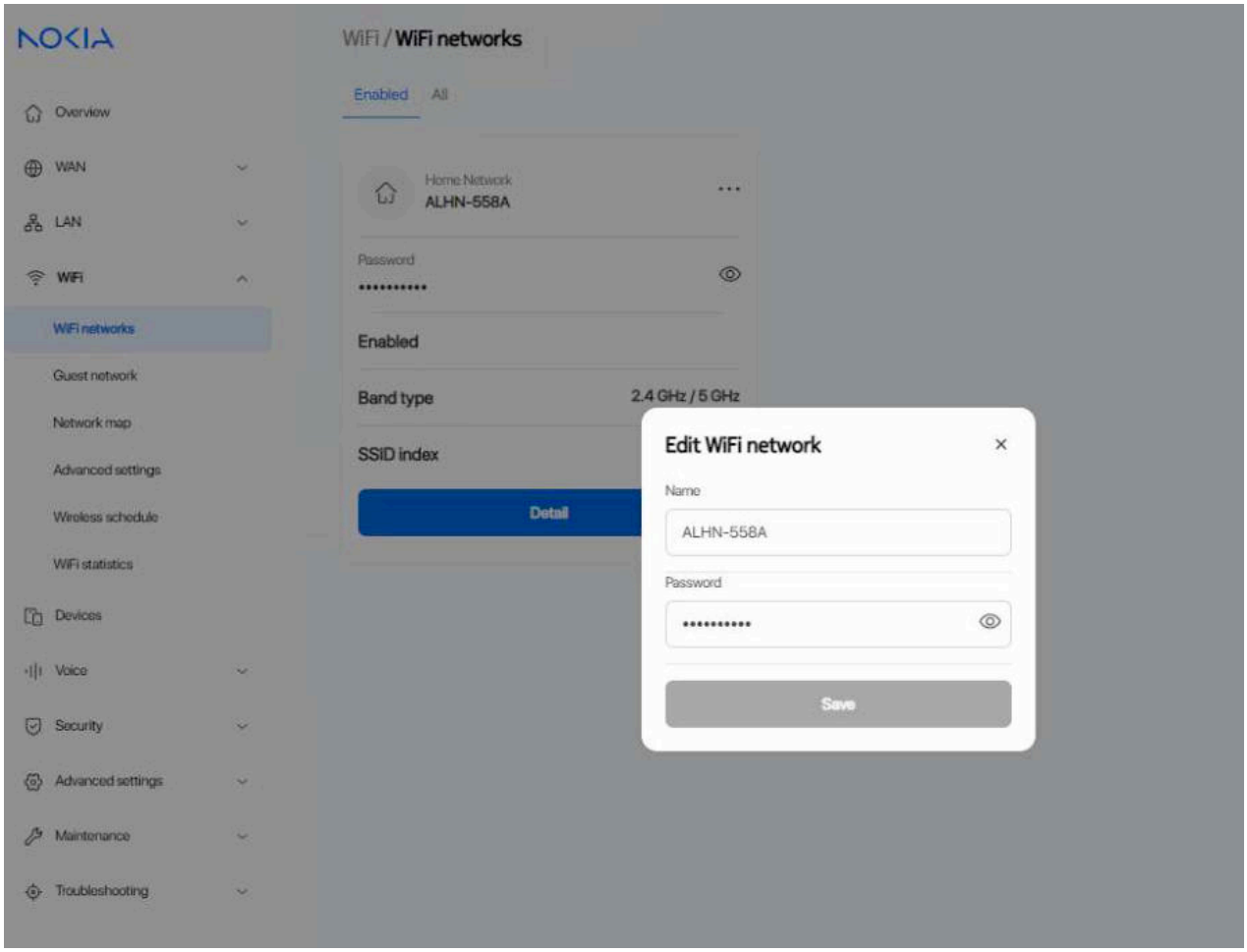
When the password does not meet the password rules, the application displays a message to indicate which password rule has not been followed, for example:

- The password is too short
- The password is too long
- The first character cannot be a special character
- There are not enough character classes

1

Click **WiFi** → **Wi-Fi networks** →**3 dots to edit** →**Change password** in the left pane. The *Edit Wi-Fi network* page displays.

Figure 7-28 Edit Wi-Fi network page



2

Enter the new password.

3

Click **Save**.

END OF STEPS

7.26 Optimizing WiFi Network

The **Optimize** button can be clicked by the user to initiate an immediate network assessment. If a more suitable channel is available, the system initiates a channel switch.

With Channel Selection set to **Auto**, to minimize frequent disconnections of client devices, the radio resource management (RRM) algorithms are designed to change the wireless channel only when internal thresholds are reached or because of regulatory reasons.

In some cases, the system could possibly run on a more suitable channel, but it does not change the channel to avoid interrupting ongoing client traffic.

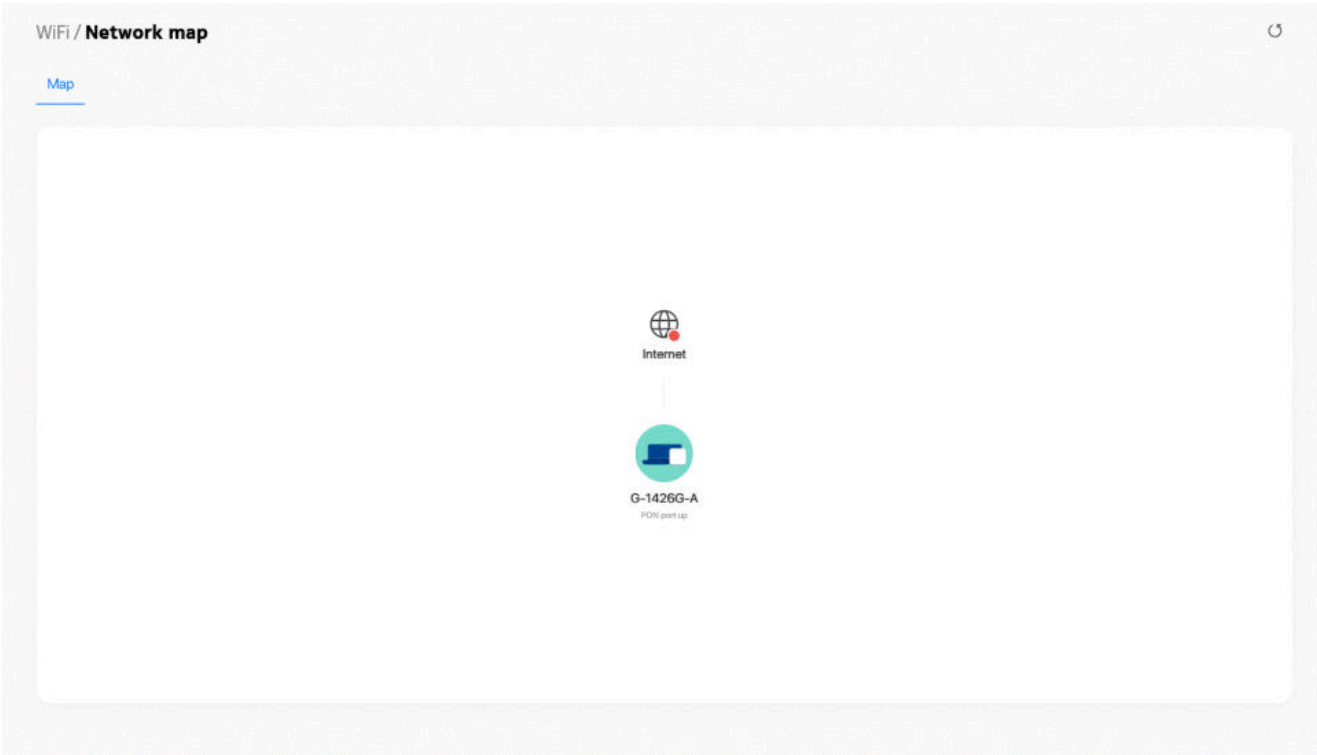
Note that this action may cause a brief downtime of the wireless network during the channel transition.

7.27 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 7-29 Network map page

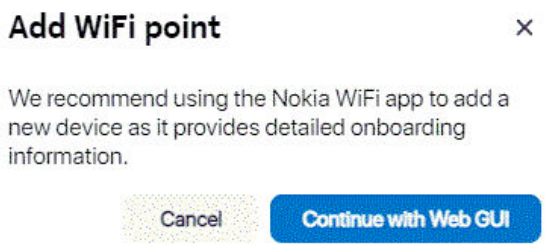


2

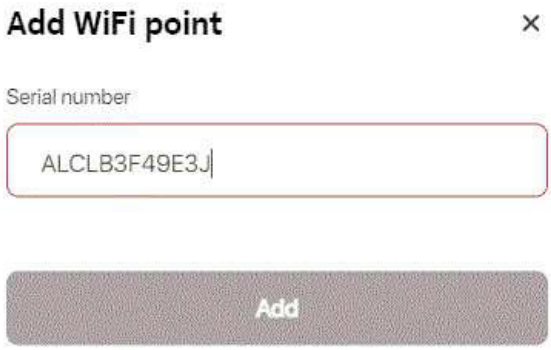
Perform the following steps to add a WiFi point:

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**.



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

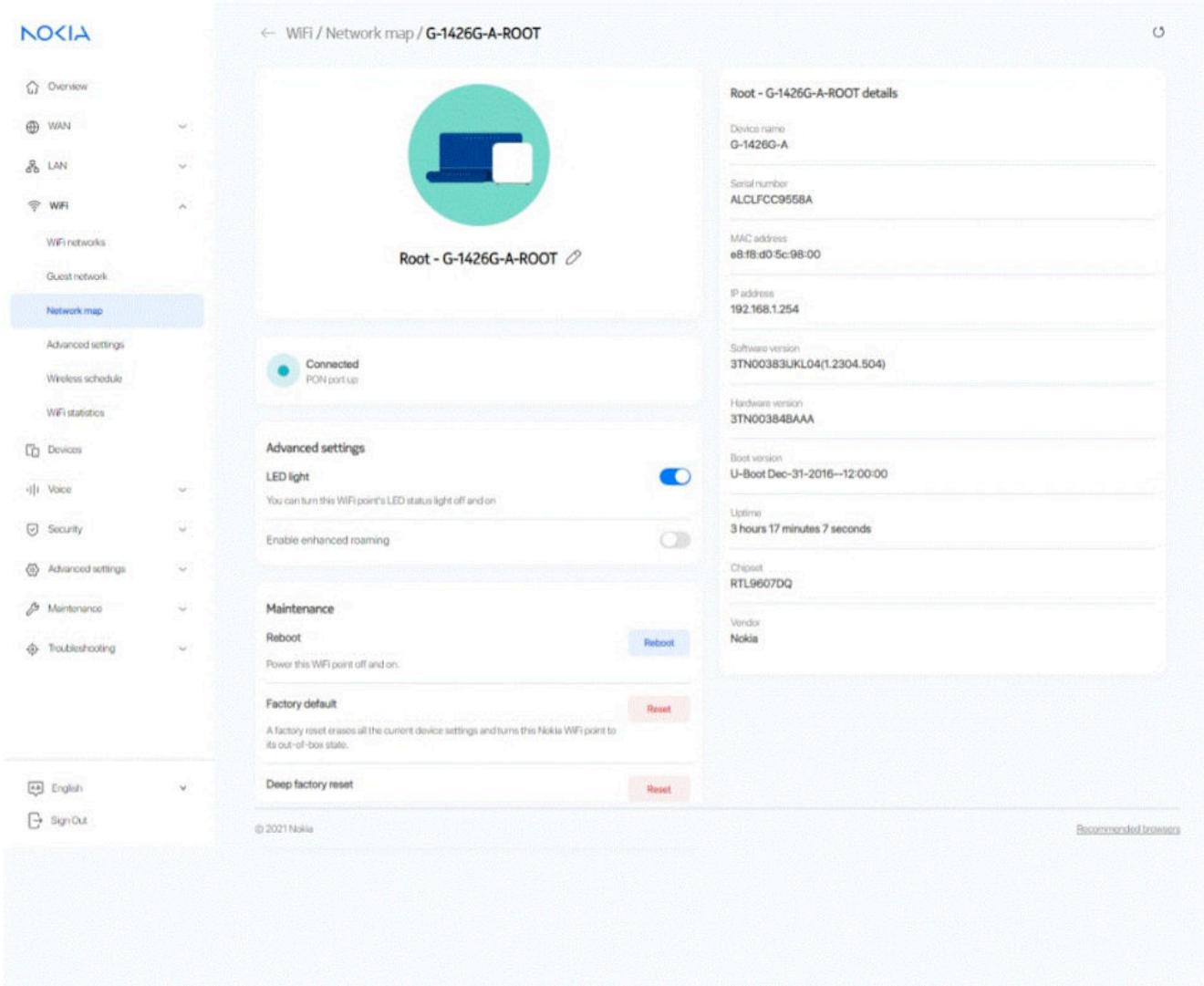


The WiFi point is displayed in the *Detected* or *Not detected* list of the *Onboarding Status* panel in the *Device Info* page.

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 7-30 <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 7-31 Change the name of your WiFi point page

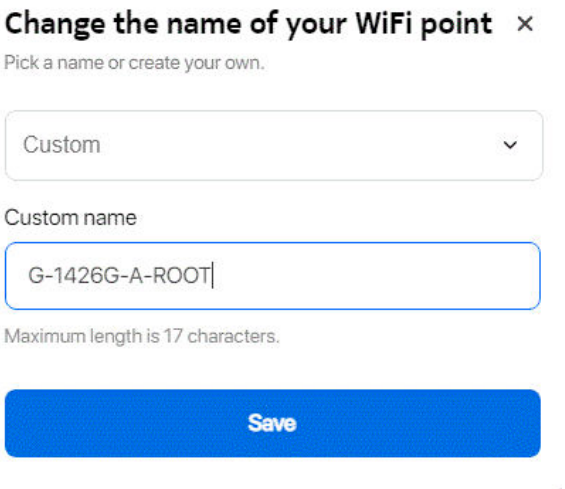


Table 7-20 <*Device*> parameters

Field	Description
Device name	Name on the device
Serial number	Serial number 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)
CPU usage	Displays percentage of CPU used.
Memory usage	Displays percentage of Memory used.
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 ONT. 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 ONT 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

7.28 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 7-32 Advanced settings - 2.4 GHz tab

3

Configure the following parameters:

Table 7-21 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** • **802.11b/g/n** • **802.11b** • **802.11g** • **802.11n** • **802.11b/g** • **802.11g/n** • **802.11n/ax**
Channel Selection	Select a channel from the list: • **Auto** • **Manual** **Note**: When changing from automatic to manual channel management, depending on the channel, channel bandwidth, and region, it can take several minutes for the changes to take into effect and for the wireless network to be functional again. Also, after a reboot, this same delay is observed. It is recommended to set this value to “Auto”.
Channel bandwidth	Select the bandwidth range from the list: • **20 MHz** • **40 MHz** This parameter is visible only if the Channel Selection is **Manual**.
Channel	Select a channel from the list or select **Auto** to auto-assign the channel. This parameter is visible only if the Channel Selection is **Manual**.
Transmit power	Select a percentage for the transmitting power from the list: • **25%** • **50%** • **75%** • **100%**
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. This parameter is visible only if the Channel Selection is **Manual**.

4

Click **Save**.

END OF STEPS

For optimizing WiFi network, see 7.26 “Optimizing WiFi Network” (p. 136).

7.29 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 7-33 Advanced settings - 5 GHz tab

3

Configure the following parameters:

Table 7-22 Wireless 5 GHz parameters

Field	Description
Enable	Select this toggle button to enable WiFi.

Table 7-22 Wireless 5 GHz parameters (continued)

Field	Description
Mode	Select the mode from the list: • **802.11a/n/ac** • **802.11a/n/ac/ax** • **802.11n/ac/ax**
Channel Selection	Select a channel from the list: • **Auto** • **Manual** **Note**: When changing from automatic to manual channel management, depending on the channel, channel bandwidth, and region, it can take several minutes for the changes to take into effect and for the wireless network to be functional again. Also, after a reboot, this same delay is observed. It is recommended to set this value to “Auto”.
Channel bandwidth	Select the bandwidth range from the list: • **20 MHz** • **40 MHz** • **80 MHz** • **160 MHz** This parameter is visible only if the Channel Selection is **Manual**.
Channel	Select a channel from the list or select **Auto** to auto-assign the channel. This parameter is visible only if the Channel Selection is **Manual**.
Transmit power	Select a percentage for the transmitting power from the list: • **25%** • **50%** • **75%** • **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 64. This parameter is visible only if the Channel Selection is **Manual**.

4

Click **Save**.

END OF STEPS

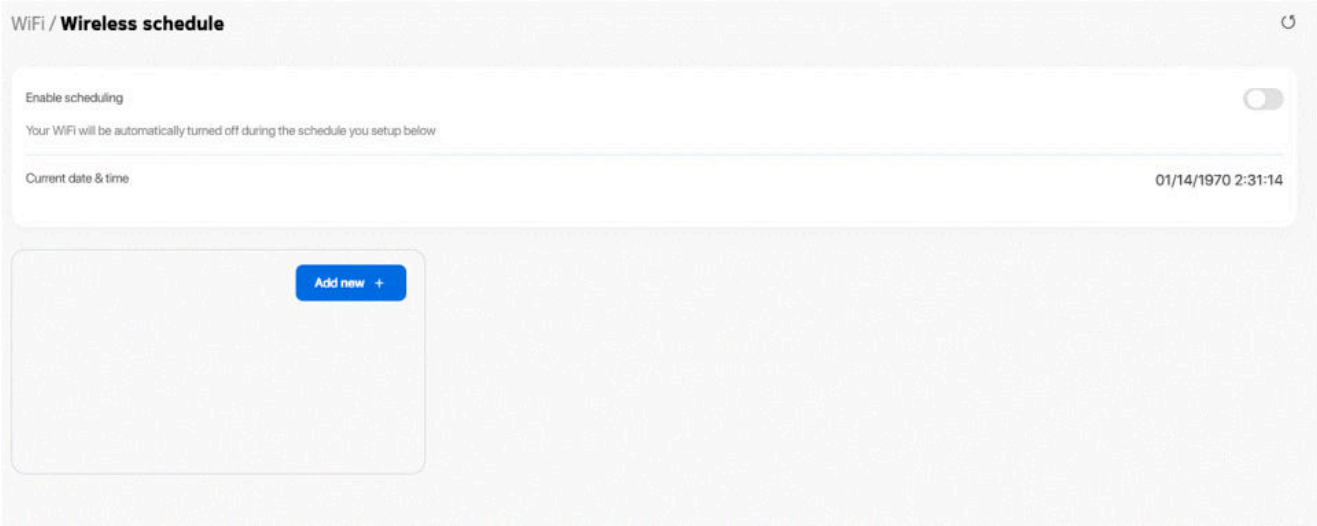
For optimizing the WiFi network, see 7.26 “Optimizing WiFi Network” (p. 136).

7.30 Configuring Wireless Schedules

1

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

Figure 7-34 Wireless schedule page



2

Select the **Enable Scheduling** toggle button to turn off the wireless signal for the configured period.

Note: The ONT stores the settings of the current wireless signal and restores with the same settings when WiFi is enabled or disabled until the programmed wireless signal rule is triggered. The stored value is restored if the active wireless signal schedule rule is deleted.

3

Click **Add new +** to add a scheduling rule.

4

Enter a start time and end time for the period during which you want to turn off the wireless signal.

5

Select **Everyday** or **Individual Days** from the list.

6

If you select **Individual Days**, select the checkboxes for the desired days.

The Recurrence Pattern shows the rules created to date.

7

If required, click **Add new +** to add more rules.

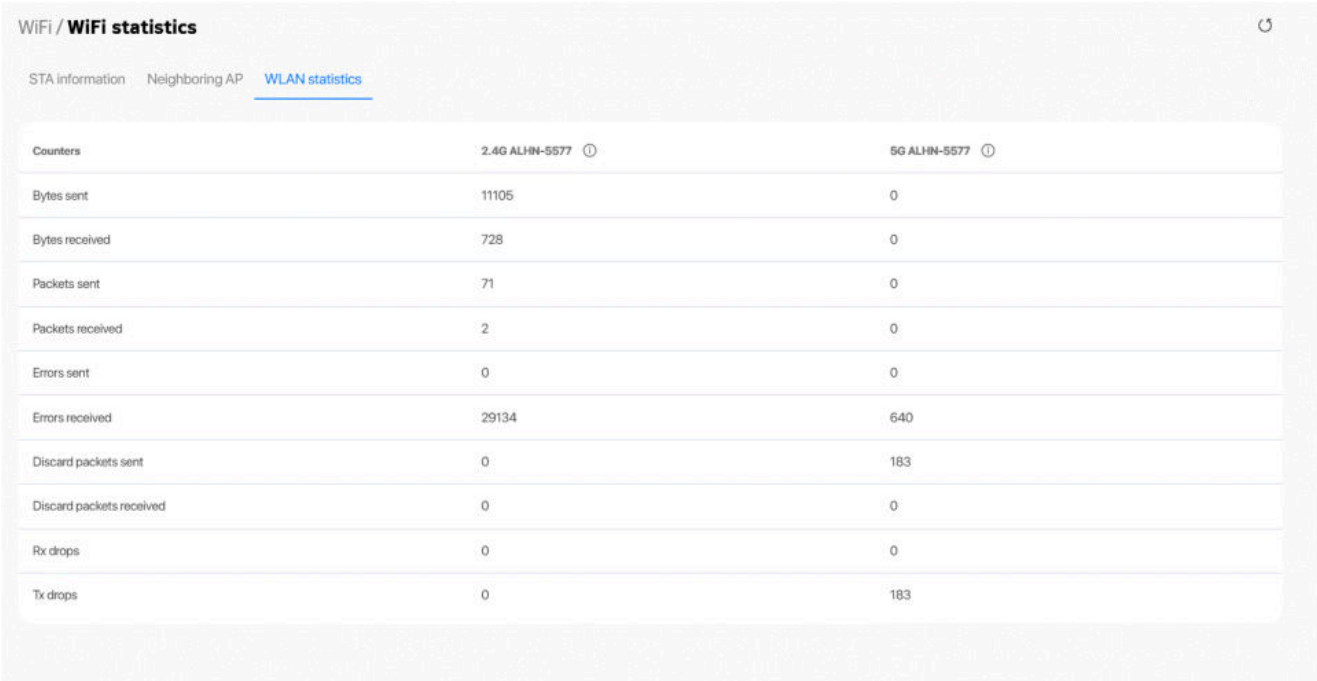
END OF STEPS

7.31 Viewing WiFi Statistics

1

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

Figure 7-35 WiFi statistics page



2

Select the **WLAN statistics** tab to display WLAN statistics.

Table 7-23 WLAN statistics parameters

Field	Description
Bytes sent	Displays the bytes sent.
Bytes received	Displays the bytes received.
Packets sent	Displays the packets sent.
Packets received	Displays the packets received.
Errors sent	Displays the errors sent.
Errors received	Displays the errors received.
Discard packets sent	Displays the discard packets sent.
Discard packets received	Displays the broadcast packets received.
Rx drops	Displays the Rx dropped packets.
Tx errors	Displays the Tx dropped packets.

END OF STEPS

Devices

7.32 Overview

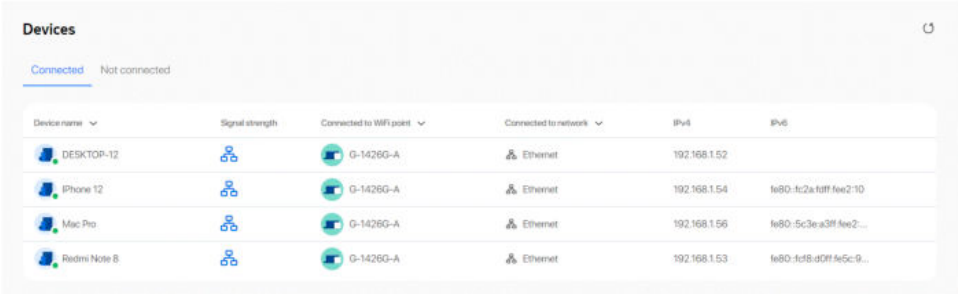
This section describes how to view device information from the **Device** menu.

7.33 Viewing Device Information

1

Click **Devices** in the left pane. The *Devices* page displays the devices.

Figure 7-36 Devices page

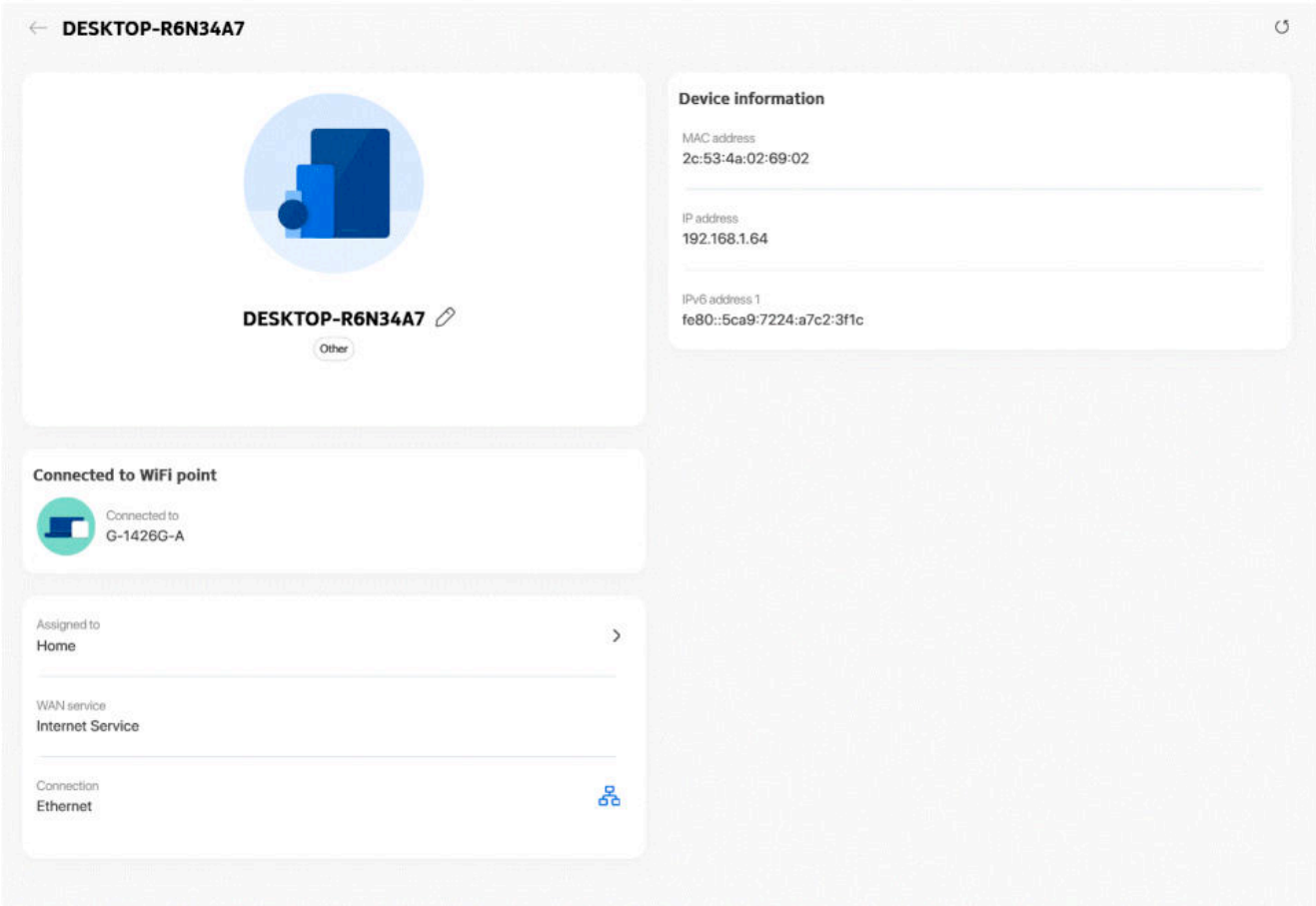


2

The Devices page lists the devices. Click on a Device to view the respective device Info page.

The *Device Info* page displays the details of the selected device in a network.

Figure 7-37 Device information page - L3 devices



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

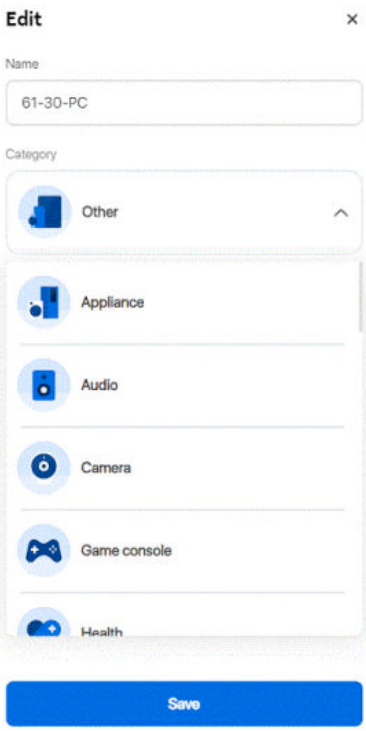
Perform the following steps to rename the client device:

a. To rename the client device, click the Edit icon . The **Edit** page displays.

b. On the **Edit** page, enter the name to create your own customized name or select a category listed in the drop-down menu.

c. Click **Save**.

Figure 7-38 Device Rename page



END OF STEPS

Draft

Security Configuration

7.34 Overview

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

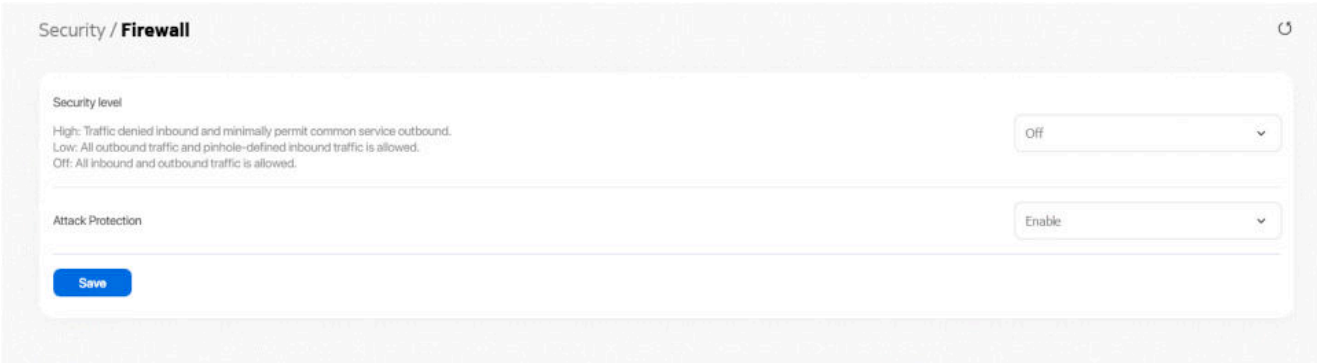
Sub-menu	Procedure
Firewall	7.35 “Configuring the Firewall” (p. 151)
MAC filter	7.36 “Configuring the MAC Filter” (p. 152)
IP filter	7.37 “Configuring the IP Filter” (p. 154)
URL filter	7.38 “Configuring the URL Filter” (p. 156)
Family profiles	7.39 “Configuring Family Profiles” (p. 158)
DMZ and ALG	7.40 “Configuring DMZ and ALG” (p. 164)
Access control	7.41 “Configuring Access Control” (p. 166)

7.35 Configuring the Firewall

1

Click **Security→Firewall** in the left pane. The *Firewall* page displays.

Figure 7-39 Firewall page



2

Configure the following parameters.

Table 7-24 Firewall parameters

Field	Description
Security level	Select the security level from the list: • **High**: Pre-routing and application services are not supported. UDP Port 8000 can be used to access the services. For example, FTP can use 8021 and Telnet can use 8023. Regular UDP cannot be used. RG access is permitted via the LAN side but not via the WAN side. • **Low**: All outbound traffic and pinhole-defined inbound traffic is allowed. Pre-routing is supported: port forwarding, DMZ, host application, and host drop. Also supported are application services: DDNS, DHCP, DNS, H248, IGMP, NTP client, SSH, Telnet, TFTP, TR-069, and VoIP. The following types of ICMP messages are permitted: echo request and reply, destination unreachable, and TTL exceeded. Other types of ICMP messages are blocked. DNS proxy is supported from LAN to WAN but not from WAN to LAN. • **Off**: All inbound and outbound traffic is allowed. No firewall security is in effect.
Attack Protection	Select **Enable** or **Disable** from the list to enable or disable protection against DoS or DDoS attacks. Default value: **Enable**. **Note:** If you select Disable, a security warning is displayed that this option poses security risks. Click **OK** to continue.

3

Click **Save**.

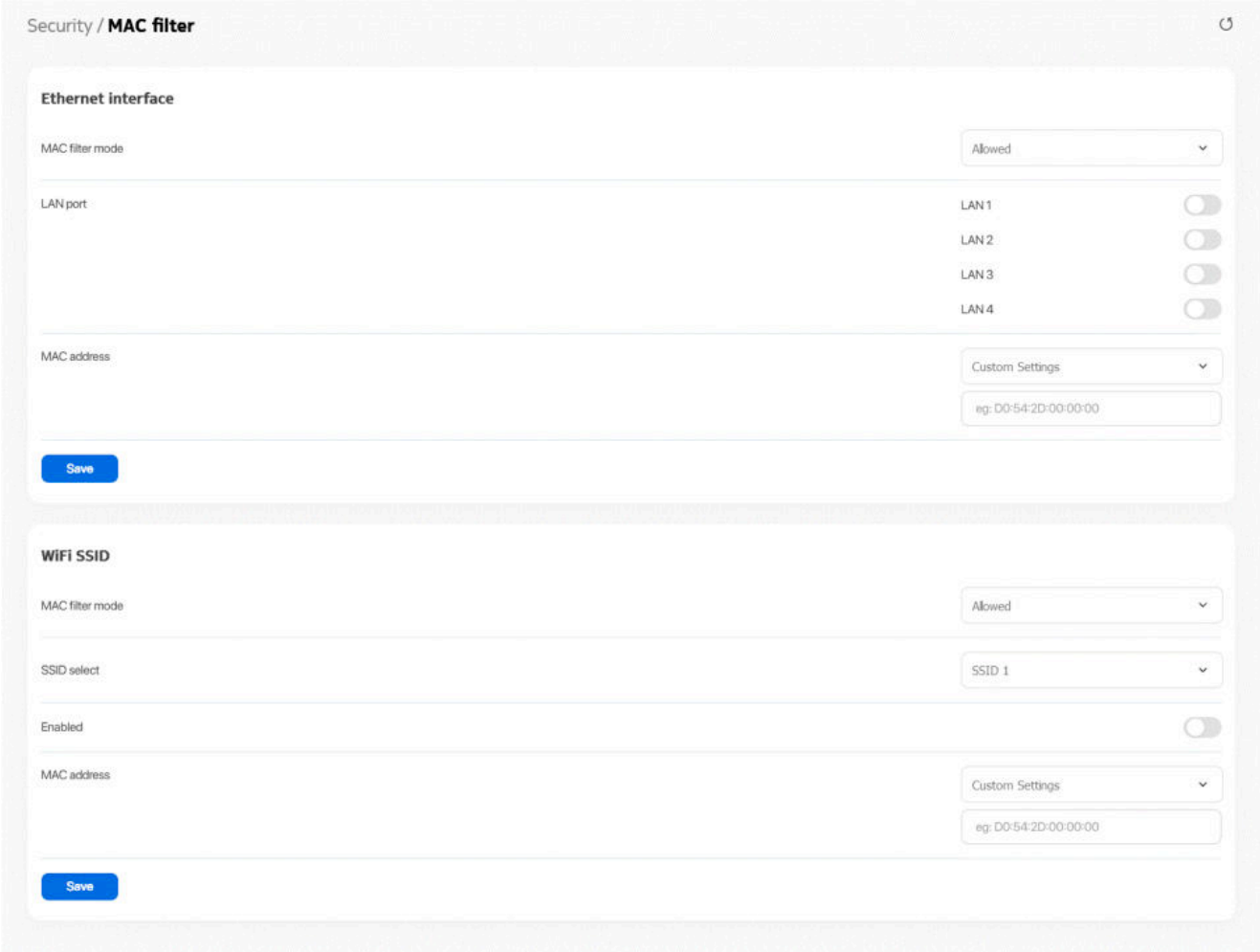
END OF STEPS

7.36 Configuring the MAC Filter

1

Click **Security→MAC filter** in the left pane. The *MAC filter* page displays.

Figure 7-40 MAC filter page



2

Configure the following parameters:

Table 7-25 MAC filter - Ethernet Interface parameters

Field	Description
Ethernet Interface	
MAC filter mode	Select the MAC filter mode from the list: • **Blocked** • **Allowed**

Table 7-25 MAC filter - Ethernet Interface parameters (continued)

Field	Description
LAN port	Select the toggle button to enable any of the LAN ports.
MAC address	Select a MAC address from the list or enter the MAC address in the text field.

3

Click **Save**.

4

Configure the following parameters:

Table 7-26 MAC filter - WiFi SSID parameters

Field	Description
WiFi SSID	
MAC filter mode	Select the MAC filter mode from the list: • **Blocked** • **Allowed**
SSID select	Select the SSID from the list.
Enabled	Select the toggle button to enable the MAC filter.
MAC address	Select a MAC address from the list or enter the MAC address in the text field.

5

Click **Save**.

END OF STEPS

7.37 Configuring the IP Filter

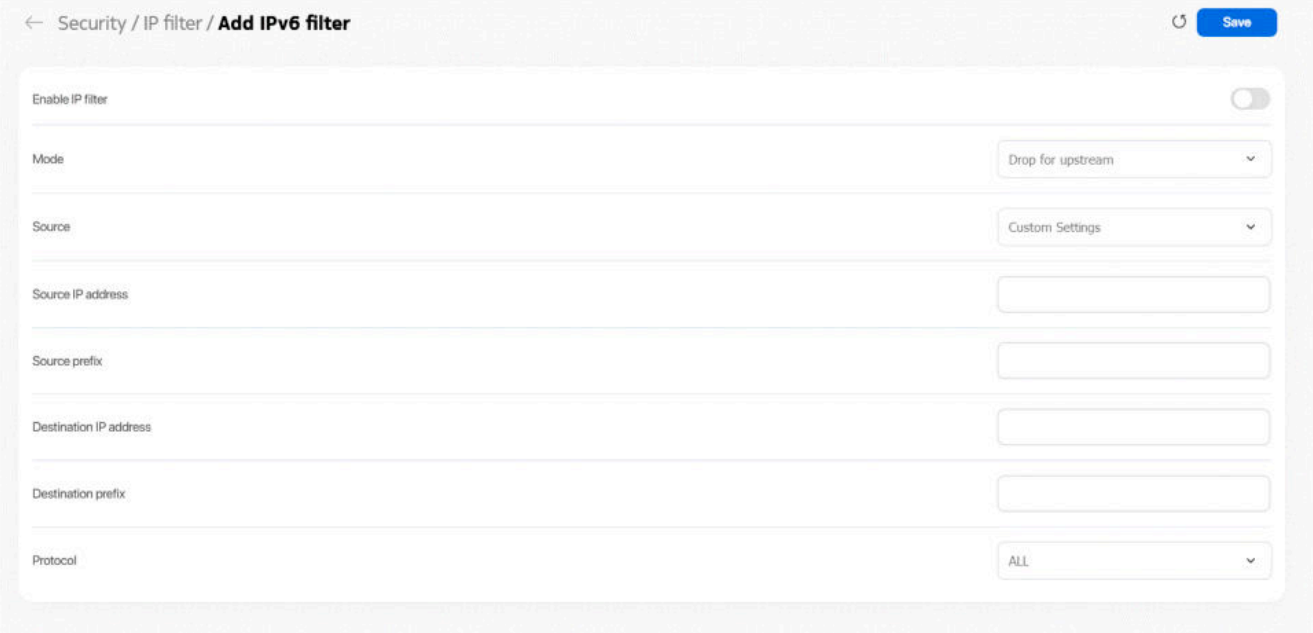
1

Click **Security→IP filter** in the left pane.

2

Click **Add Filter** to add a IPv4 or IPv6 filter. The *Add IP filter* page displays.

Figure 7-41 IP filter page



3

Configure the following parameters:

Table 7-27 IP filter parameters

Field	Description
Add IPv4 filter or **Add IPv6 filter** parameters	
Enable IP filter	Select the toggle button to enable an IP filter.
Mode	Select an IP filter mode from the list: • **Drop for upstream** • **Drop for downstream** • **Accept for upstream** • **Accept for downstream**
Source	Select an internal client from the list: • **Custom Settings**: uses the IP address input below • **IP**: uses the connecting devices' IP to the ONT
Add IPv4 filter parameters	
Local IP address	Enter the local IP address.
Local subnet mask	Enter the local subnet mask.

Table 7-27 IP filter parameters (continued)

Field	Description
Destination IP address	Enter the destination IP address.
Destination subnet mask	Enter the destination subnet mask.
Protocol	Select an application protocol or select **ALL** from the list.
Add IPv6 filter parameters	
Source IP address	Enter the source IP address.
Source Prefix	Enter the source prefix.
Destination IP address	Enter the destination IP address.
Destination prefix	Enter the destination prefix.
Protocol	Select an application protocol or select **ALL** from the list.

4

Click **Save**.

END OF STEPS

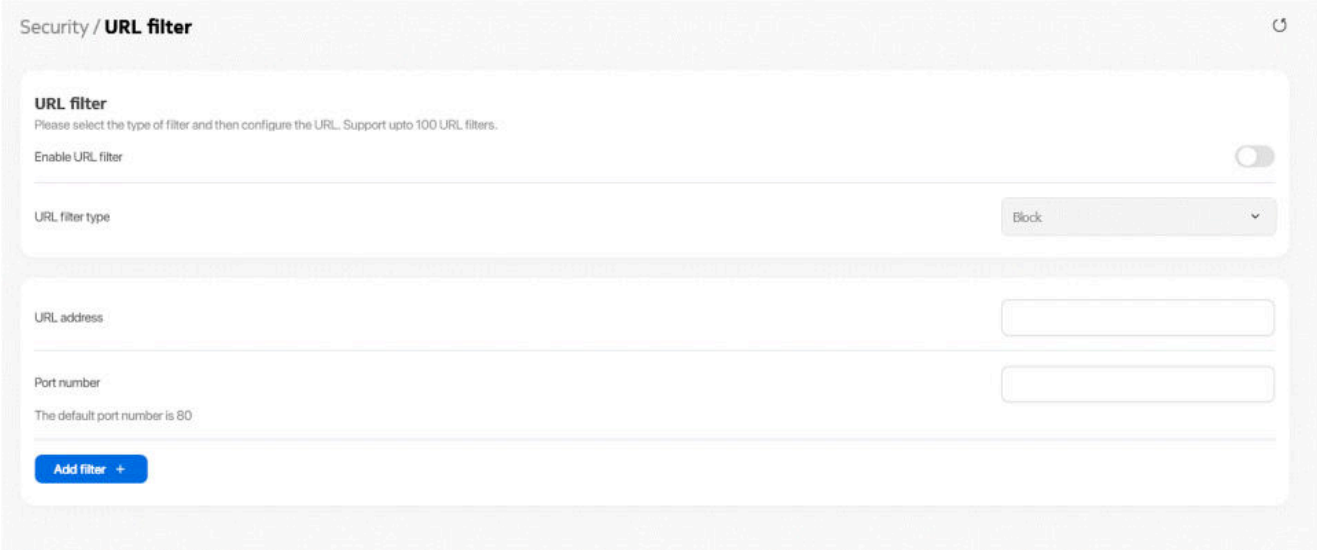
7.38 Configuring the URL Filter

Note: You can add up to 100 URL filters.

1

Click **Security→URL filter** in the left pane. The *URL filter* page displays.

Figure 7-42 URL filter page



Note: You cannot use URL filtering for HTTPS. The URL is encrypted when using HTTPS.

2

Configure the following parameters:

Table 7-28 URL filter parameters

Field	Description
Enable URL filter	Select the toggle button to enable the URL filter.
URL filter type	Select a URL filter type from the list: • **Block** • **Allow**
URL address	Enter the URL address.
Port number	Enter the port number. Default value: 80

3

Click **Add filter +** to add the URL filter.

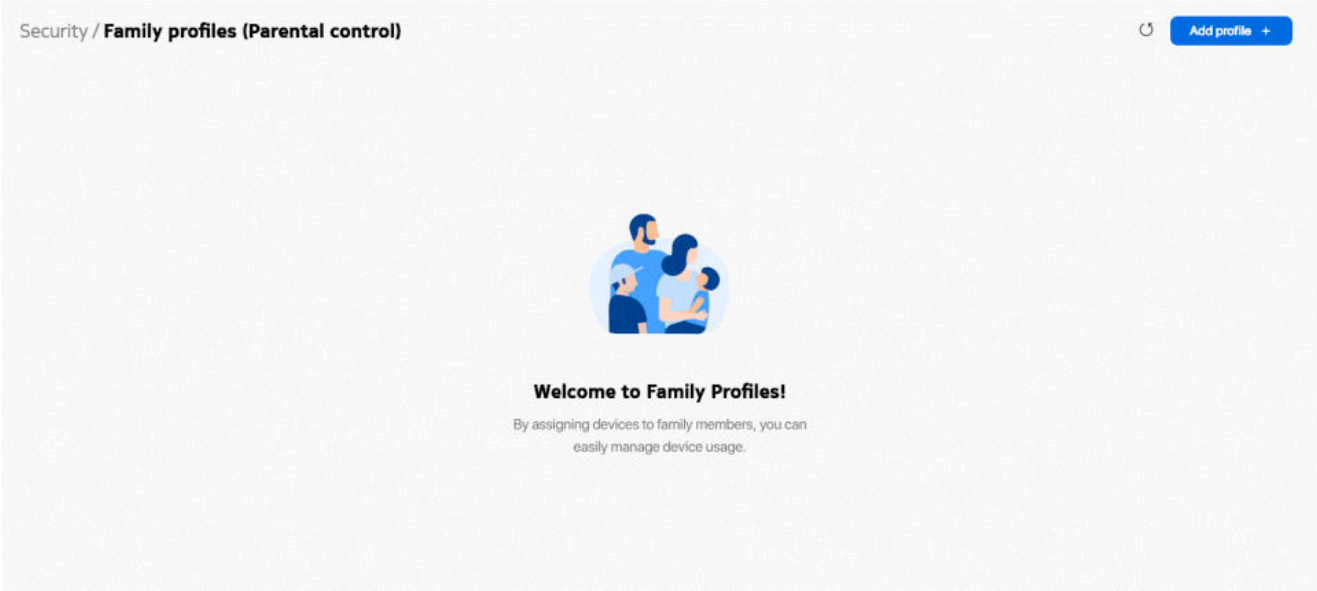
END OF STEPS

7.39 Configuring Family Profiles

1

Click **Security→Family profiles (Parental control)** from the left pane. The *Family profiles (Parental control)* page displays.

Figure 7-43 Family profiles (Parental control) page



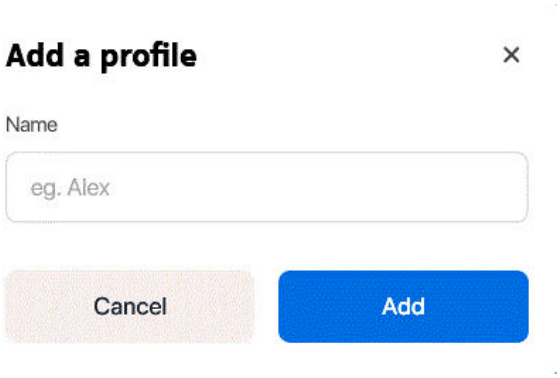
2

Click **Add profile +** to add a profile with parental controls.

3

In the *Add a profile* page, enter a name for the profile and click **Add**.

Figure 7-44 Add a profile page

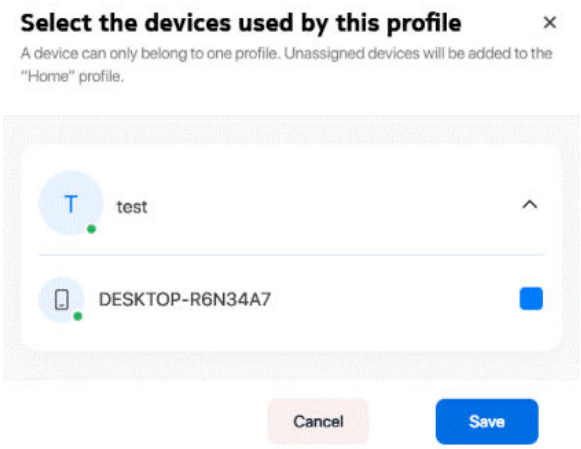


4

In the *Select the devices used by <profile>* page, select the check box next to the device name and click **Save** to assign the device to the profile.

Note: A device can be assigned to only one profile. Unassigned devices are added to the *Home* profile.

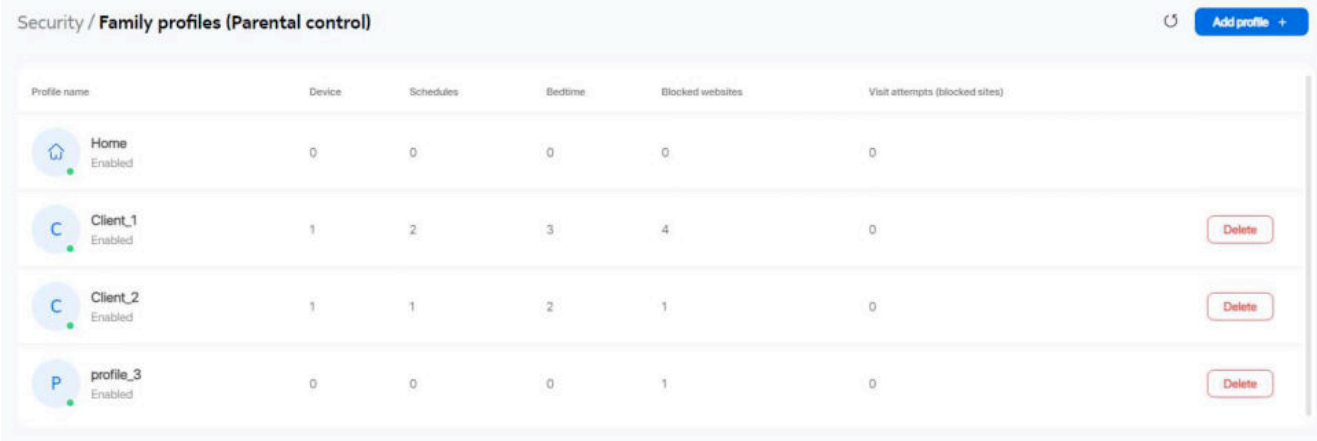
Figure 7-45 Assign devices to family profile



The new profile name is listed in the table in the *Family profiles (Parental control)* page.

Draft

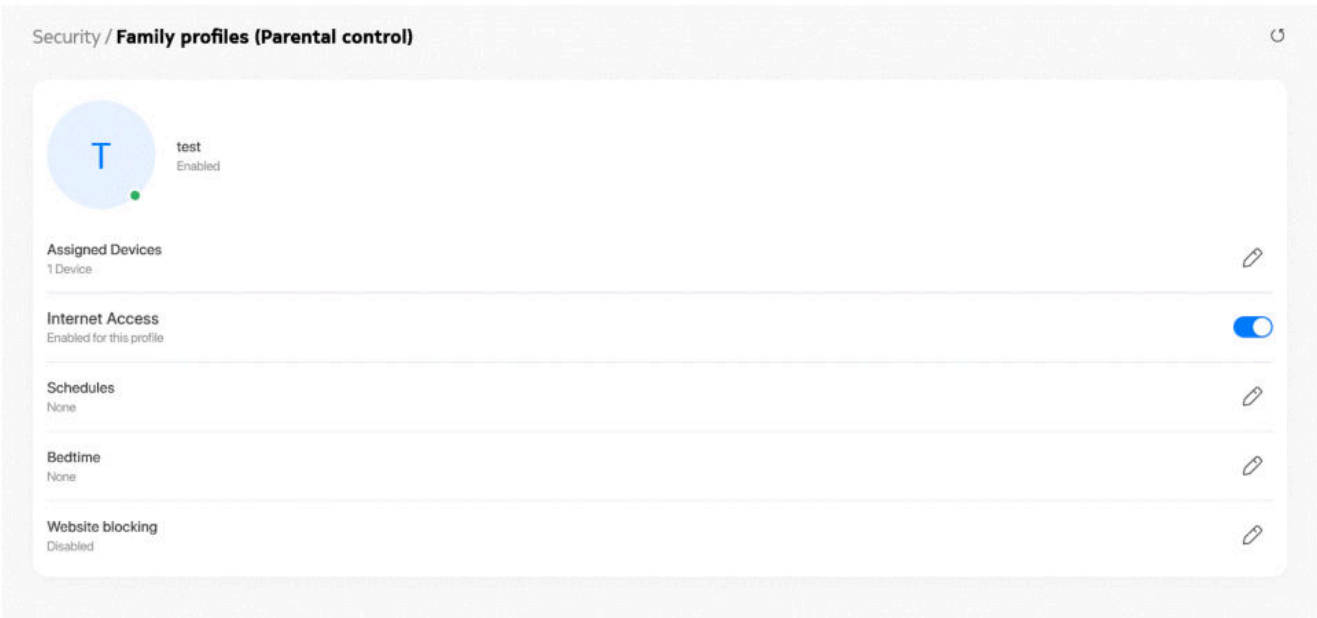
Figure 7-46 Family profiles table



5

Click a profile to configure parental control for the profile. A page displays the profile parameters.

Figure 7-47 Family profile configuration page



6

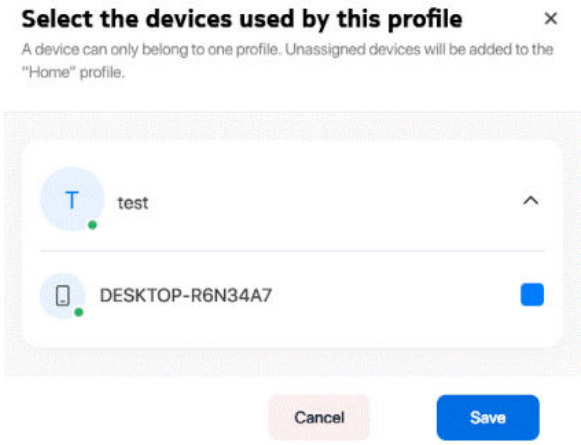
Select the **Internet Access** toggle button to enable internet access.

Assign more devices

7

Assign more devices to the profile, if required:

a. In the profile page, click the edit icon next to **Assigned Devices** to assign devices to the profile. The *Select the devices used by <profile>* page displays.



b. Select the check box next to the device to assign to the profile.

c. Click **Save**.

Configure and enable schedules

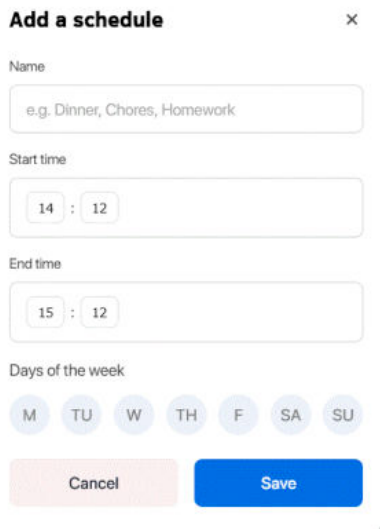
8

Configure schedules for the profile:

a. In the profile page, click the edit icon next to **Schedules** to create one or more schedules for the profile to set specific days and time slots when the Internet should be turned off.

b. Click **Create Schedule**.

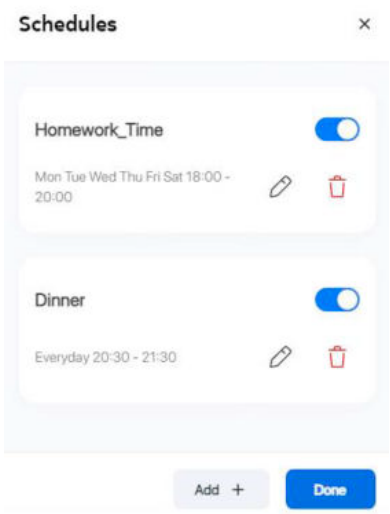
c. In the *Add a schedule* page, configure the following:



1. Enter the name of the schedule in the Name field.
2. Select the start time, end time, and select the days of the week on which the schedule will be in effect.
3. Click **Save**. The schedule is created and listed in the Schedules page.

9

In the *Schedules* page, select the toggle button to enable the schedule and click **Done**. To add more schedules, you can click **Add +**.



Configure and enable bedtime

10

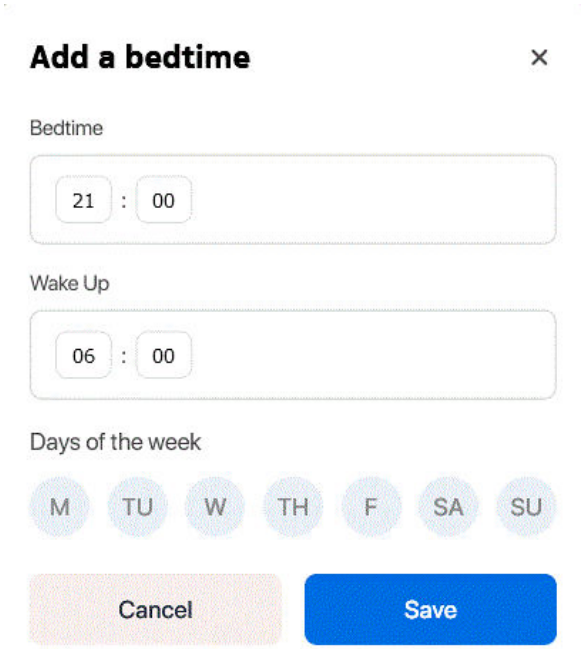
Configure bedtime for the profile:

a. In the profile page, click the edit icon next to **Bedtime** to configure bedtime for the profile to automatically pause internet access at this time.

Only one bedtime can be assigned per day.

b. Click **Create Bedtime**.

c. In the *Add a bedtime* page, configure the following:



1. Select the Bedtime, Wake Up time, and select the days of the week on which the bedtime will be in effect.
2. Click **Save**. The bedtime is created and listed in the *Bedtime* page.

d. In the *Bedtime* page, select the toggle button to enable the bedtime and click **Done**.

Configure website blocking

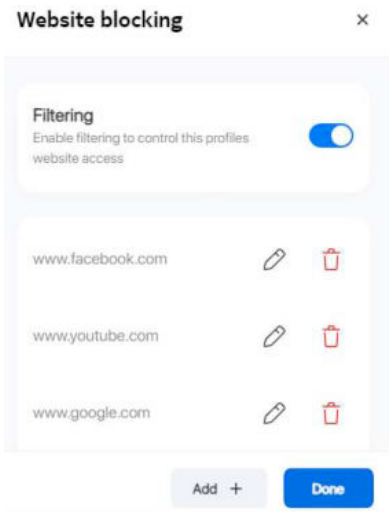
11

Configure website blocking for the profile:

a. In the profile page, click the edit icon next to **Website blocking** to control websites and services that devices assigned to the profile can access.

b. Click **Continue**.

c. In the *Website blocking* page, perform the following:



1. Select the toggle button next to **Filtering** to enable filtering to control the profile's website access.
2. Click **Add +** to add a website URL to be blocked.
3. Enter the URL in the Website URL field and click **Save**.
4. Click **Add +** to add more website URLs to be blocked or click **Done**.

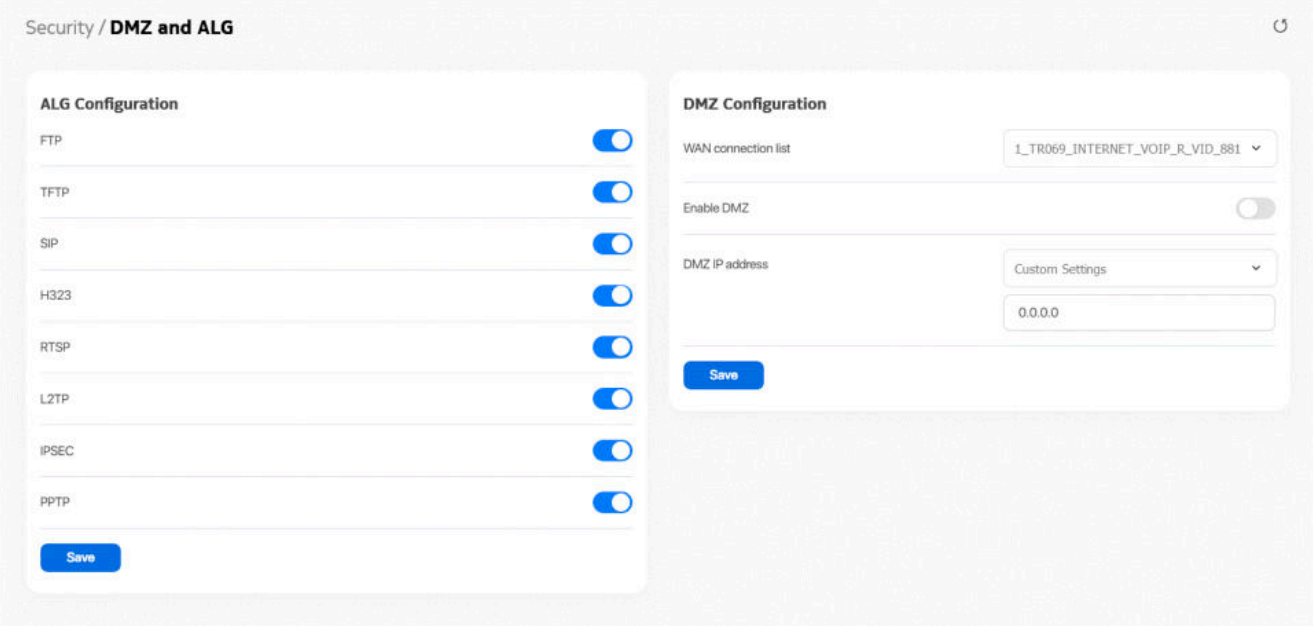
END OF STEPS

7.40 Configuring DMZ and ALG

1

Click **Security→DMZ and ALG** in the left pane. The *DMZ and ALG* page displays.

Figure 7-48 DMZ and ALG page



2

Configure the following parameters:

Table 7-29 ALG Configuration parameters

Field	Description
ALG Configuration	Select the toggle button next to the protocol name to enable the protocols to be supported by ALG: • FTP • TFTP • SIP • H323 • RTSP • L2TP • PPTP • IPSEC

3

Click **Save**.

4

Configure the following parameters:

Draft

Table 7-30 DMZ Configuration parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
Enable DMZ	Select the toggle button to enable DMZ on the WAN connection.
DMZ IP address	Select **Custom Settings** and enter the DMZ IP address or select the IP address of a connected device from the list.

5

Click **Save**.

END OF STEPS

7.41 Configuring Access Control

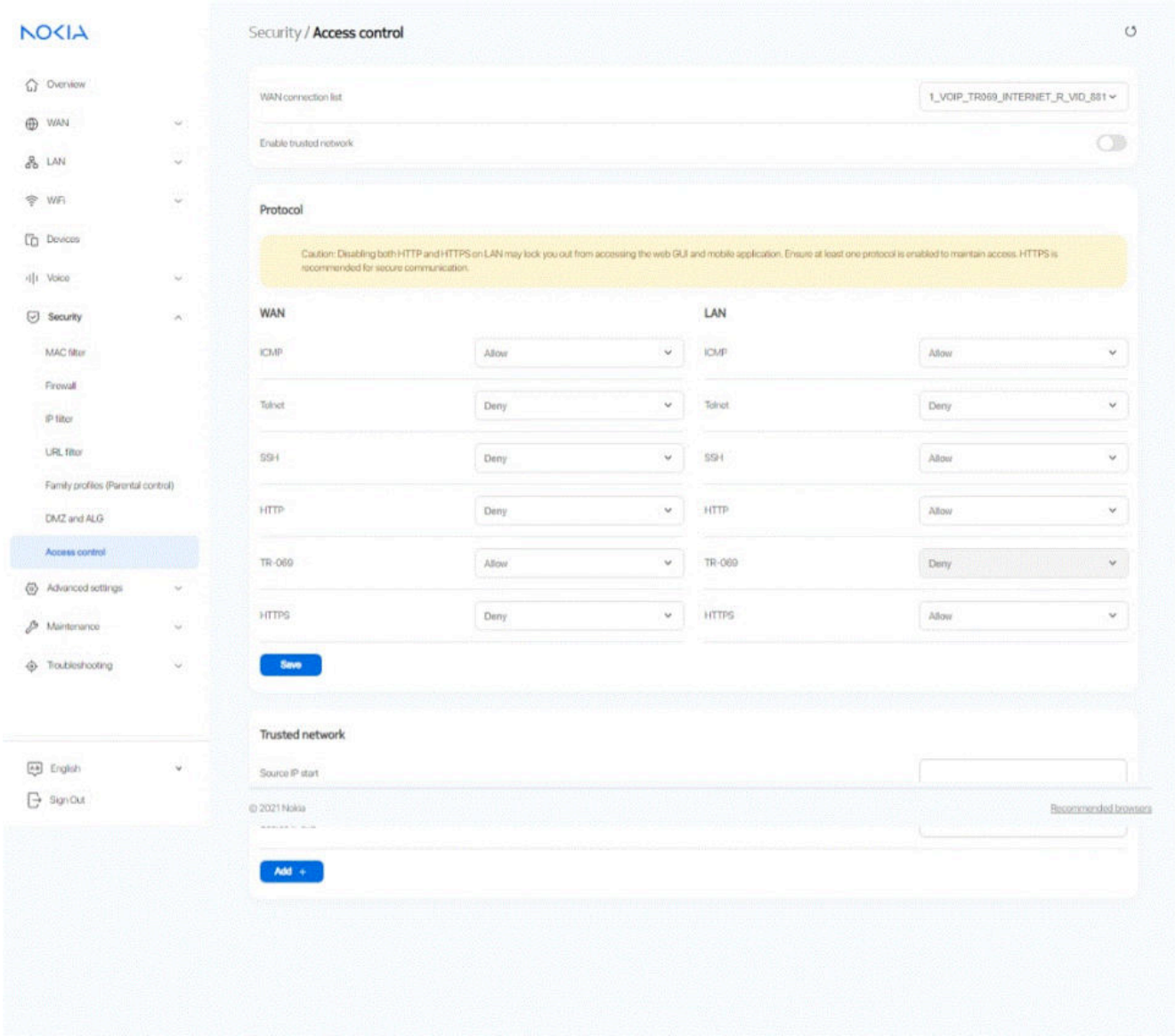
This procedure describes how to configure the access control level (ACL).

Note: ACL takes precedence over the firewall policy.
The trusted network will be shared for all WAN connections; it is not applied individually to a WAN connection.

1

Click **Security→Access control** in the left pane. The *Access control* page displays.

Figure 7-49 Access control page



2

Configure the following parameters:

Draft

Table 7-31 Access control parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
Enable trusted network	Select the toggle button to enable a trusted network.
WAN	The following protocols are supported: ICMP, Telnet, SSH, HTTP, TR-069, HTTPS, SFTP. Select an access control level for each protocol: **Allow**, **Deny**, or **Trusted Network Only** LAN side: **Allow** or **Deny** **Note:** If you allow SSH/Telnet/HTTP/HTTPS on WAN, a security warning is displayed. Click **OK** to continue.
LAN	The following protocols are supported: ICMP, Telnet, SSH, HTTP, TR-069, HTTPS, SFTP. Select an access control level for each protocol: LAN side: **Allow** or **Deny** **Notes:** • If you allow Telnet or HTTP on LAN, a security warning is displayed. Click **OK** to continue. • If you **Deny** HTTP and HTTPS on LAN at same time, the following warning message is displayed, 'Disabling both HTTP and HTTPS on LAN may lock you out from accessing the web GUI and mobile application. Atleast one of them should be enabled.' Click **OK** to continue.

3

Click **Save** to save the ACL configuration.

4

If the **Enable trusted network** option is enabled, add one or more subnet trusted networks. You can add up to 32 trusted networks.

Table 7-32 Trusted Network parameters

Field	Description
Source IP start	Enter a start IP address range for the new subnet trusted network.
Source IP end	Enter an end IP address range for the new subnet trusted network.

5

Click **Add +**.

END OF STEPS

Advanced Settings

7.42 Overview

This section describes the advanced settings that can be performed from the following sub-menu options under the **Advanced settings** menu:

Sub-menu	Procedure
Port forwarding	7.43 “Configuring Port Forwarding” (p. 169)
Port triggering	7.44 “Configuring Port Triggering” (p. 170)
DDNS	7.45 “Configuring DDNS” (p. 171)
NTP	7.46 “Configuring NTP” (p. 172)
USB	7.47 “Configuring USB” (p. 174)
UPNP and DLNA	7.48 “Configuring UPNP and DLNA” (p. 175)

7.43 Configuring Port Forwarding

1

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

Figure 7-50 Port forwarding page

2

Configure the following parameters:

Table 7-33 Port forwarding parameters

Field	Description
WAN port	Enter the WAN port range.
LAN port	Enter the LAN port range.
Internal client	Select a connected device from the list and enter the associated IP address. The default is **Custom Settings**.
Protocol	Select the port forwarding protocol from the list: • **TCP** • **UDP** • **TCP/UDP**
WAN connection list	Select a WAN connection from the list. Only active devices are displayed in the list.

3

Click **Save**.

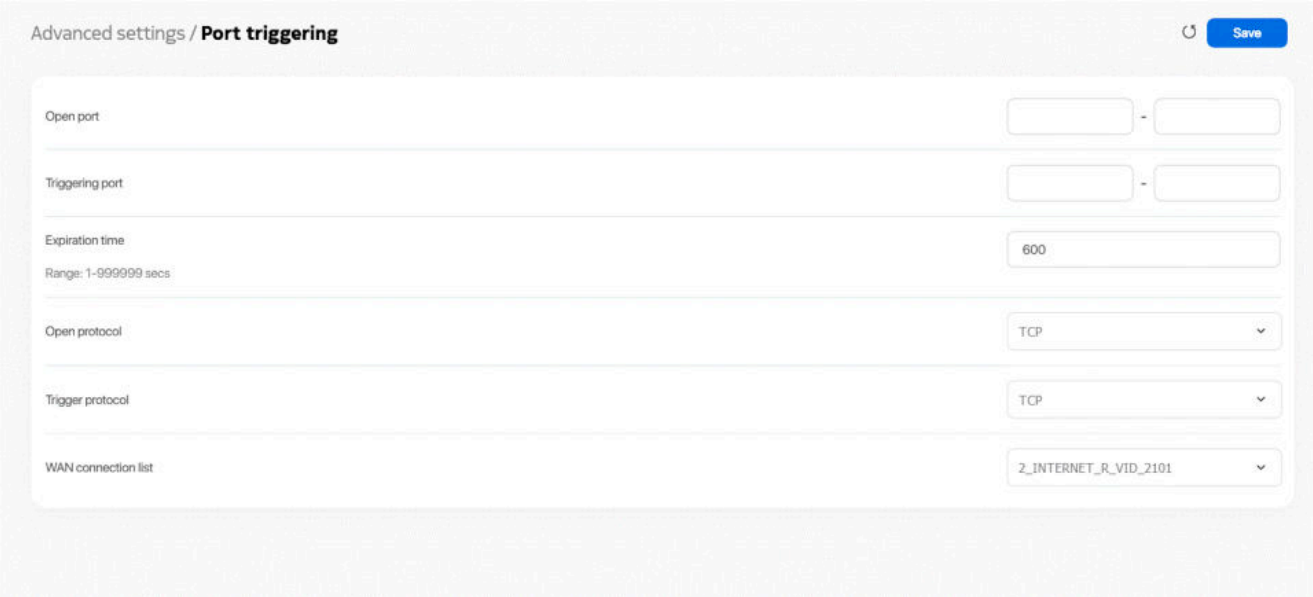
END OF STEPS

7.44 Configuring Port Triggering

1

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

Figure 7-51 Port triggering page



2

Configure the following parameters:

Table 7-34 Port triggering parameters

Field	Description
Open port	Enter the open port range.
Triggering port	Enter the triggering port range.
Expiration time	Enter the expiration time in seconds. Allowed range: 1 to 999999 seconds
Open protocol	Select the open port protocol from the list: • **TCP** • **UDP** • **TCP/UDP**
Trigger protocol	Select the triggering port protocol from the list: • **TCP** • **UDP** • **TCP/UDP**
WAN connection list	Select a WAN connection from the list. Only active devices are displayed in the list.

3

Click **Save**.

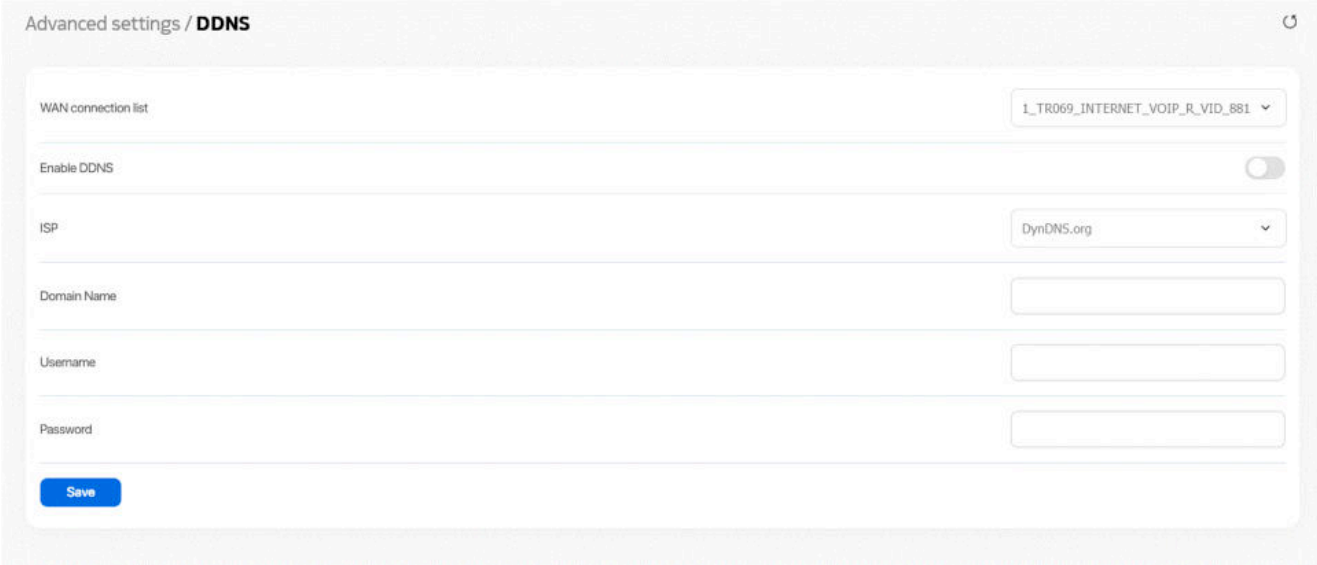
END OF STEPS

7.45 Configuring DDNS

1

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

Figure 7-52 DDNS page



2

Configure the following parameters:

Table 7-35 DDNS parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
Enable DDNS	Select the toggle button to enable DDNS on the WAN connection.
ISP	Select an ISP from the list.
Domain Name	Enter the domain name of the DDNS server.
Username	Enter the username.
Password	Enter the password.

3

Click **Save**.

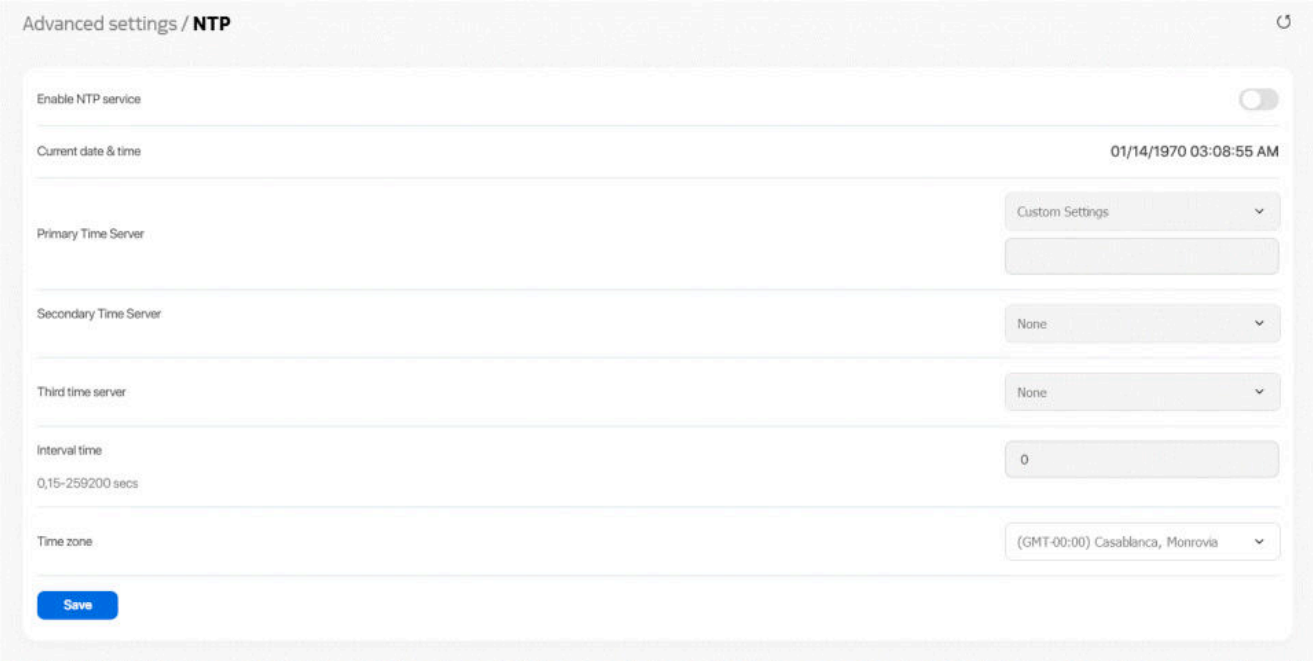
END OF STEPS

7.46 Configuring NTP

1

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

Figure 7-53 NTP page



2

Configure the following parameters:

Table 7-36 NTP parameters

Field	Description
Enable NTP service	Select the toggle button to enable the NTP service.
Current date & time	Displays the current local date and time.
Primary Time Server Secondary Time Server Third Time Server	Select a time server from the list or select **Custom Settings** and enter the IP address of the time server. You can select **None** if you do not want configure a secondary or tertiary time server.
Interval time	Enter the interval at which to get the time from the time server, in seconds. Allowed values: 0 to 259200 seconds
Time zone	Select the local time zone from the list.

3

Click **Save**.

END OF STEPS

7.47 Configuring USB

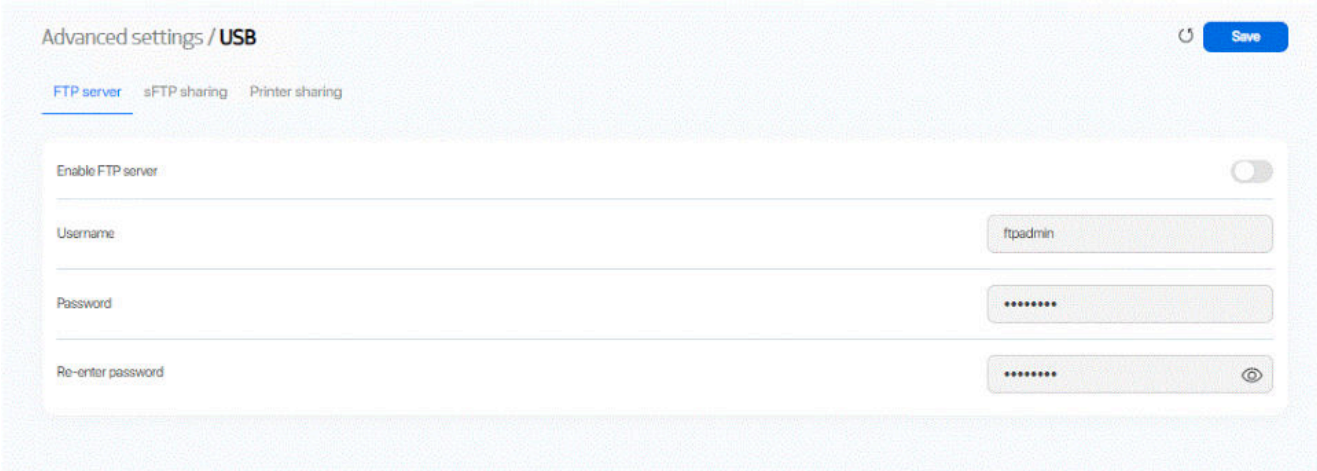
You can connect USB storage devices and USB printers to the USB ports of the device. The USB menu enables you to configure FTP and SFTP for your USB storage devices.

The USB connected devices are shown in a table at the bottom of the *USB* page.

1

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

Figure 7-54 USB page



2

Configure the following parameters:

Table 7-37 USB parameters

Field	Description
FTP server parameters	
Enable FTP server	Select the toggle button to enable an FTP server. By default, FTP server is disabled.
Username	Enter the username of the FTP server.
Password	Enter the password of the FTP server.
Re-enter password	Re-enter the password of the FTP server.
sFTP sharing parameters	
Enable SFTP Server	Select the toggle button to enable an SFTP server. By default, SFTP server is disabled.
Enable SFTP for Remote Access	Select the toggle button to enable SFTP for remote access. By default, SFTP is disabled.

Table 7-37 USB parameters (continued)

Field	Description
Username	Enter the username of the SFTP server.
Password	Enter the password of the SFTP server.
Re-enter password	Re-enter the password of the SFTP server.
Printer sharing parameters	
Enable printer sharing	Select the toggle button to enable printer sharing. By default, printer sharing is disabled.
Username	Enter the username of the printer.
Password	Enter the password of the printer.
Re-enter password	Re-enter the password of the printer.

3

Click **Save**.

A table displays the following information for each server or printer that is connected to the device through a USB port:

- Host Number: For example, Printer1, Printer2
- Device Name: Name or identifier of the device
- Format: Storage format (applies only to a USB storage device)
- Total space (applies only to a USB storage device)
- Free space (applies only to a USB storage device)

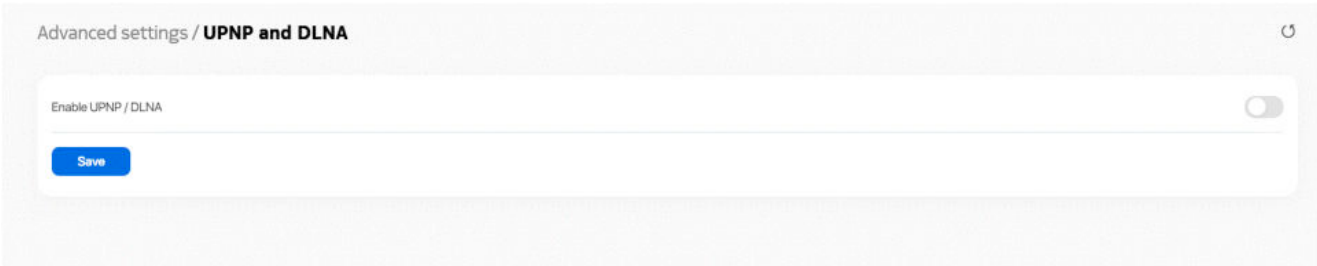
END OF STEPS

7.48 Configuring UPNP and DLNA

1

Click **Advanced settings→UPNP and DLNA** from the left pane. The *UPNP and DLNA* page displays.

Figure 7-55 UPNP and DLNA page



2

Select the **Enable UPNP/DLNA** toggle button to enable UPNP/DLNA. If this toggle button is not enabled, the UPNP and DLNA process will not start.

3

Click **Save**.

END OF STEPS

Maintenance

7.49 Overview

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

Sub-menu	Procedure
Change password	7.50 “Configuring the Password” (p. 177)
Backup and restore	7.51 “Backing Up the Configuration” (p. 178) 7.52 “Restoring the Configuration” (p. 179)
Firmware upgrade	7.53 “Upgrading Firmware” (p. 180)
LOID config	7.54 “Configuring LOID” (p. 182)
SLID configuration	7.55 “Configuring SLID” (p. 183)
Diagnostics	7.56 “Diagnosing WAN Connections” (p. 184)
Log	7.57 “Viewing Log Files” (p. 186)
Delta CFG tool	7.58 “Generating a delta configuration file” (p. 187)

7.50 Configuring the Password

A password must adhere to the following password rules:

- The password may consist of uppercase letters, lowercase letters, digital numbers, and the following special characters ! # + , -. / : =@_
- The password length must be from 8 to 24 characters
- The first character must be a digital number or a letter
- The password must contain at least two types of characters: numbers, letters, or special characters
- The same character must not appear more than 8 times in a row
- The password cannot be a dictionary password (for example:12345678).

When the password meets the password rules, the application displays the message “Your password has been changed successfully”.

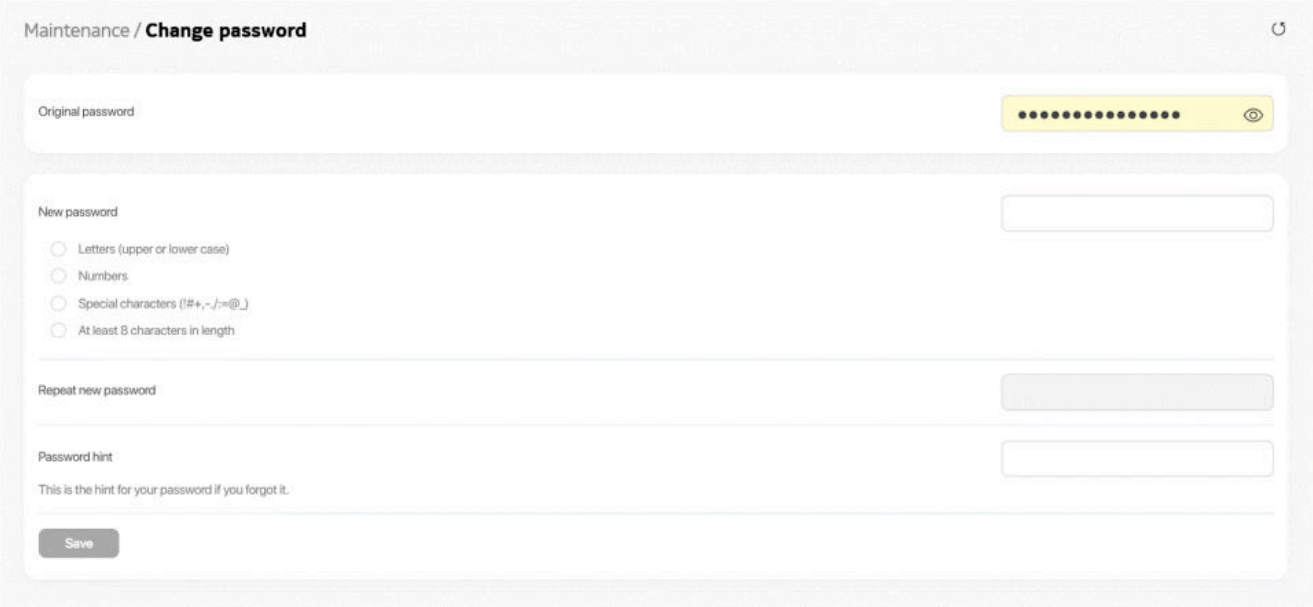
When the password does not meet the password rules, the application displays a message to indicate which password rule has not been followed, for example:

- The password is too short
- The password is too long
- The first character cannot be a special character
- There are not enough character classes

1

Click **Maintenance→Change password** in the left pane. The *Change password* page displays.

Figure 7-56 Change password page



2

Configure the following parameters:

Table 7-38 Change password parameters

Field	Description
Original password	Enter the current password.
New password	Enter the new password as per the password rules.
Repeat new password	Re-enter the new password (must match the password entered above).

3

Click **Save**.

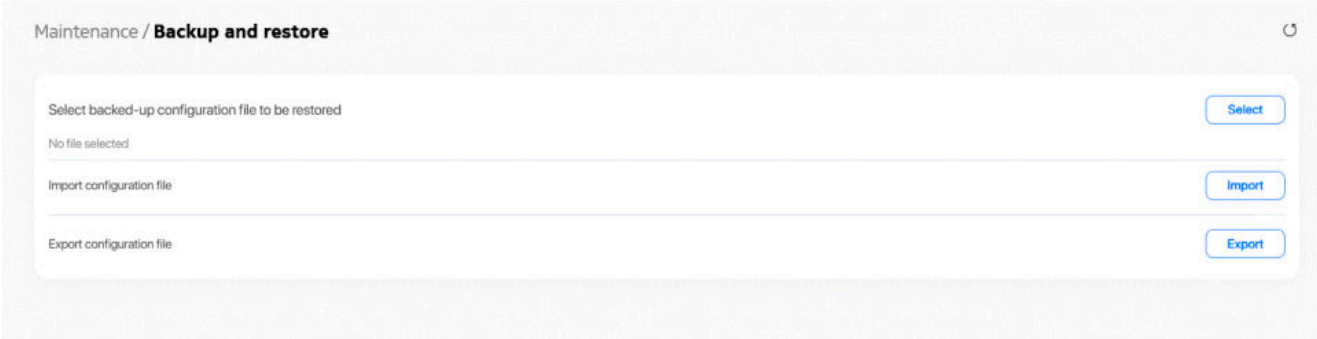
END OF STEPS

7.51 Backing Up the Configuration

1

Click **Maintenance→Backup and restore** in the left pane. The *Backup and restore* page displays.

Figure 7-57 Backup and restore page



2

Click **Export** to export the current ONT configuration to your PC. The configuration filename is *config.cfg*.

END OF STEPS

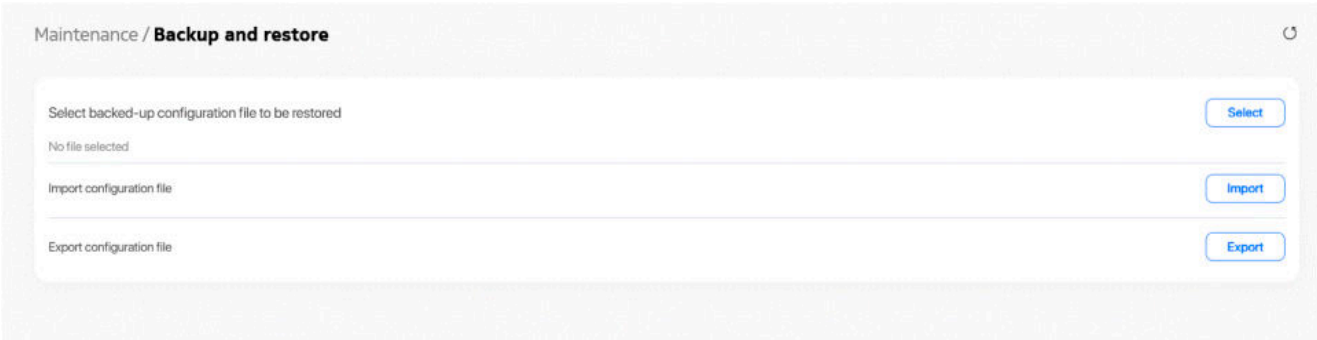
7.52 Restoring the Configuration

Note: Ensure that you have a previously backed-up configuration file.

1

Click **Maintenance→Backup and restore** in the left pane. The *Backup and restore* page displays.

Figure 7-58 Backup and restore page



2

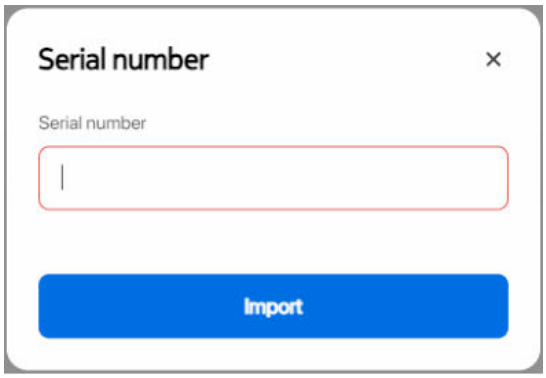
Click **Select** and select the previously backed-up configuration file.

3

Click **Import** to import the configuration file created in 7.51 “Backing Up the Configuration” (p. 178) and restore the ONT to the backed-up configuration.

a. If the configuration file is from the same ONT variant with a different serial number, you will be prompted to enter the serial number of the original device.

Figure 7-59 Backup and restore: Serial number



b. If you enter an invalid serial number, the back up fails and an error message is displayed.

c. The backup cannot be restored for the configuration files from a different ONT variant, OPID, or different release prior to Release 2402.

A confirmation message displays after successful restore and the ONT reboots.

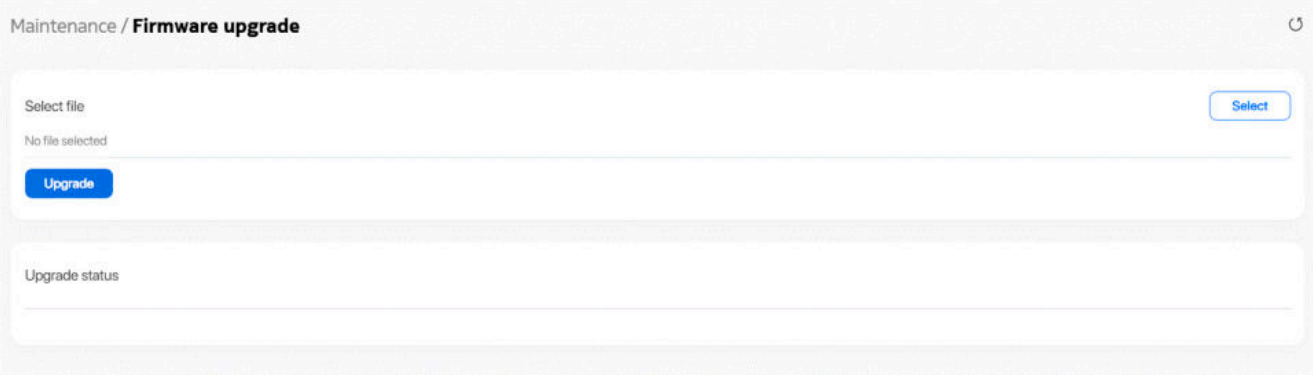
END OF STEPS

7.53 Upgrading Firmware

1

Click **Maintenance→Firmware upgrade** in the left pane. The *Firmware upgrade* page displays.

Figure 7-60 Firmware upgrade page



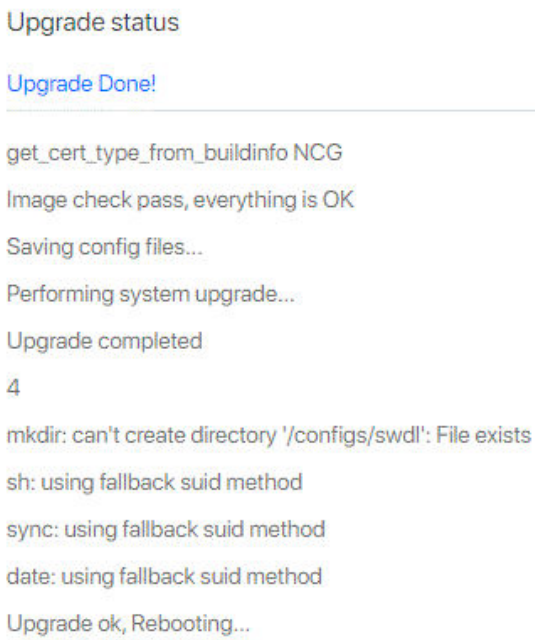
2

Click **Select** and select the file for firmware upgrade.

3

Click **Upgrade** to upgrade the firmware. The status displays in the *Upgrade status* panel. The device reboots after firmware upgrade and displays the login page.

Figure 7-61 Example of upgrade status messages



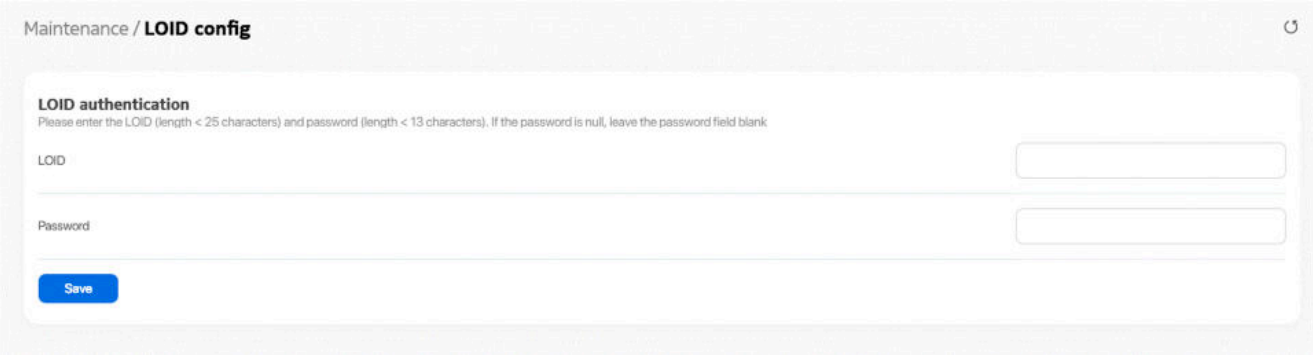
END OF STEPS

7.54 Configuring LOID

1

Click **Maintenance→LOID config** in the left pane. The *LOID config* page displays.

Figure 7-62 LOID config page



2

Configure the following parameters:

Table 7-39 LOID config parameters

Field	Description
LOID authentication	
LOID	Enter the LOID. Maximum number of characters: 24
Password	Enter the password. If the password is null, leave this field blank. Maximum number of characters: 12

3

Click **Save**.

END OF STEPS

7.55 Configuring SLID

1

Click **Maintenance→SLID configuration** in the left pane. The *SLID configuration* page displays.

Figure 7-63 SLID configuration page

2

Configure the following parameters:

Table 7-40 SLID configuration parameters

Field	Description
Current SLID	Displays the current SLID.
Enter new SLID	Enter the new SLID.
SLID mode	Select a SLID mode from the list. The default is HEX Mode. • ASCII Mode • HEX Mode In ASCII Mode, the allowed characters are 0-9, a-z and the maximum number of characters is 10. Special character is not allowed. In HEX Mode, the allowed characters are 0-9, a-f, A-F and the maximum number of characters is 20. Special character is not allowed.

3

Click **Save**.

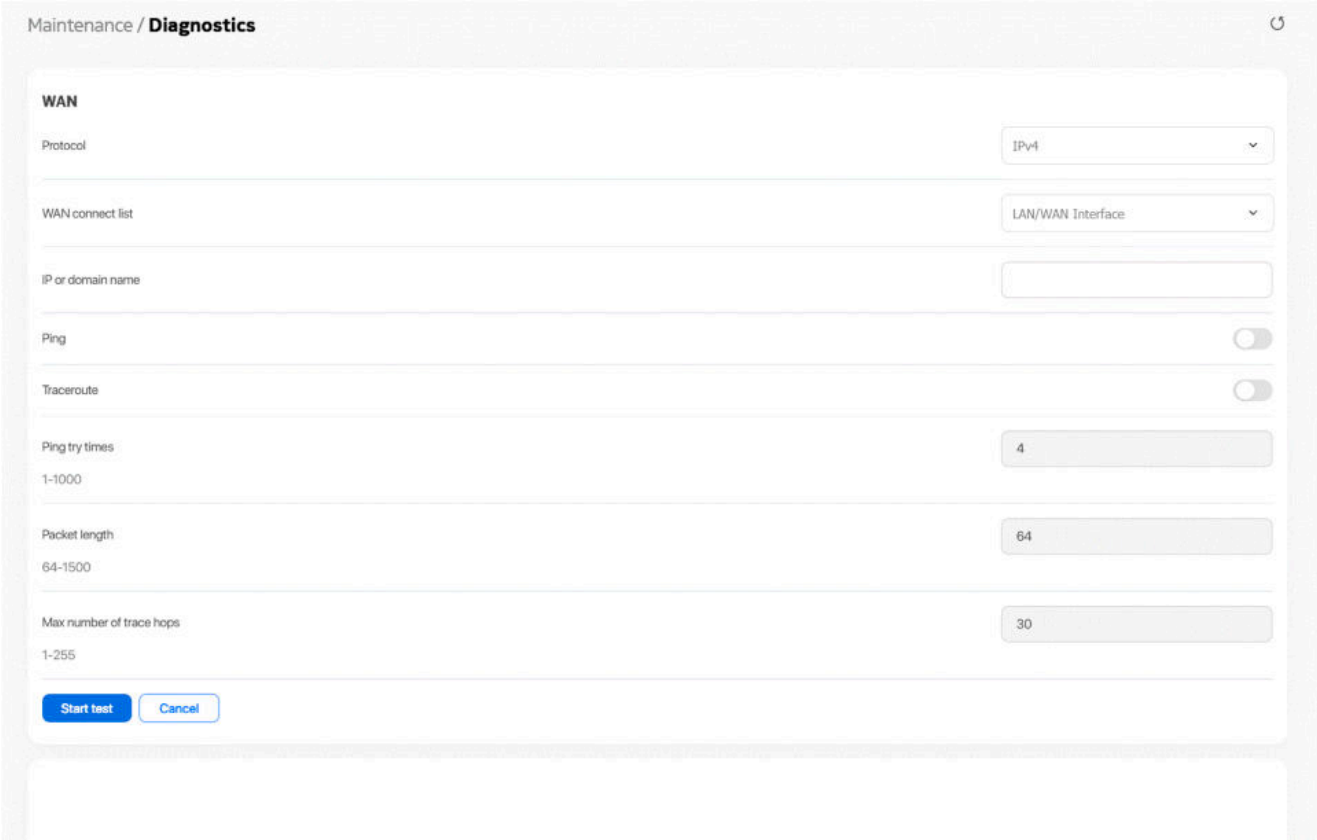
END OF STEPS

7.56 Diagnosing WAN Connections

1

Click **Maintenance→Diagnostics** in the left pane. The *Diagnostics* page displays.

Figure 7-64 Diagnostics page



2

Configure the following parameters.

Table 7-41 Diagnostics parameters

Field	Description
Protocol	Select a protocol from the list: • **IPv4** • **IPv6**

Table 7-41 Diagnostics parameters (continued)

Field	Description
WAN connect list	Select a WAN connection to diagnose from the list.
IP or domain name	Enter the IP address or domain name.
Ping	Select this toggle button to enable ping.
Traceroute	Select this toggle button to enable traceroute.
Ping try times	Enter the number of ping attempts. This field is enabled only if you select the **Ping** toggle button. Allowed values: 1 to 1000 Default value: 4
Packet length	Enter a packet length. Allowed values: 64 to 1500 Default value: 64
Max number of trace hops	Enter the maximum number of trace hops. This field is enabled only if you select the **Traceroute** toggle button. Allowed values: 1 to 255 Default value: 30

3

Click **Start test** to start the test. Results are displayed at the bottom of the page.

Figure 7-65 Example of ping results

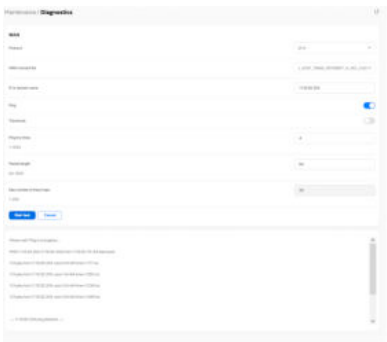


Figure 7-66 Example of traceroute results

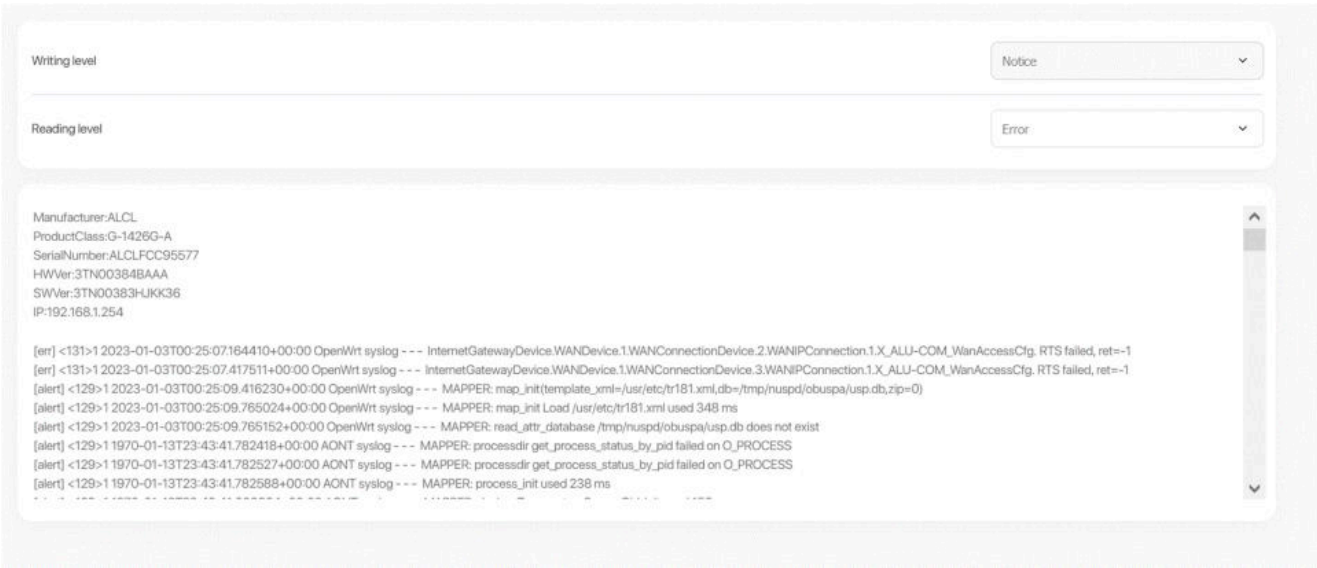
END OF STEPS

7.57 Viewing Log Files

1

Click **Maintenance→Log** in the left pane. The *Log* page displays.

Figure 7-67 *Log* page



2

Configure the following parameters:

Table 7-42 Log parameters

Field	Description
Writing level	Select a writing level from the list to determine the event types recorded in the log file: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**
Reading level	Select a reading level from the list to determine the event types displayed in the log file: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**

3

Click **Save**. The log file is displayed at the bottom of the page.

4

Click **Export log** to download the log file to your PC. The filename of the log is *onu_info.log*.

END OF STEPS

7.58 Generating a delta configuration file

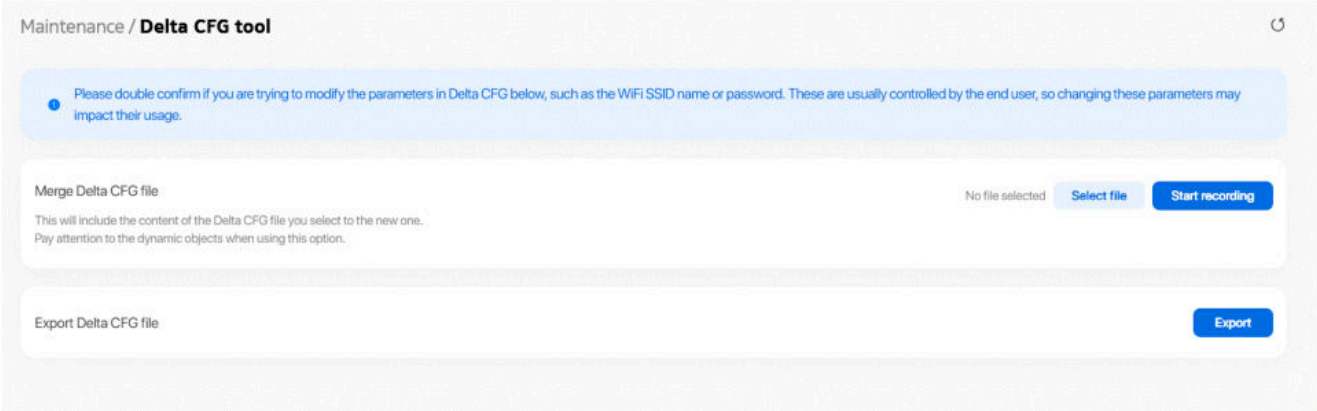
The delta CFG tool is used to generate a delta CFG file which records the parameter changes on the WebGUI. The tool also allows to merge the generated delta configuration file with a previously existing delta config file.

1

Click **Maintenance→Delta CFG tool** from the left pane. The Delta CFG tool page displays.

- To generate a delta CFG file without merging with a previous CFG file, go to Step 2.
- To merge delta CFG file, go to Step 3.

Figure 7-68 Delta CFG Tool page



2

Generating a delta CFG file without merging with a previous delta CFG file

a. Click **Start recording**.

b. Perform the required configuration such as adding/deleting WAN connection, changing WAN connection VLAN ID, changing ACS URL and so on. If reboot is needed after modifying a parameter, for example, disabling the DNS Proxy in the DNS page, wait until the ONT is rebooted and continue with the configuration.

c. Click **Stop recording** to stop recording.

d. Click **Export** to download the delta CFG file to the local computer. The delta CFG file is in plain text format with the filename *delta_config_result file*. If required, rename the file and convert the file to .tar format before downloading it to the ONT.

Note: For merging the downloaded delta config, the previously downloaded delta file must be renamed by adding “CFG” at the start of the filename and *.cfg* extension to be added to the delta config file (CFG_*.cfg) to upload the file successfully in Delta CFG tool page.

3

Generating a delta CFG file and merging the file with a previously generated file

This option allows a user to select a delta CFG file from the local computer which will be merged with the recorded commands. The generated delta CFG file will include the content of the selected delta CFG file and the new modifications.

a. Click **Select file** and select an existing delta CFG file from the local computer to merge with the recorded commands.

Note: Choose the delta CFG file before clicking **Start recording**. The delta CFG file chosen needs to be in plain text format and not in the .tar format.

b. Click **Start recording**.

c. Perform the required configuration such as adding/deleting WAN connection, changing WAN connection VLAN ID, changing ACS URL and so on. If reboot is needed after modifying a parameter, for example, disabling the DNS Proxy in the DNS page, wait until the ONT is rebooted and continue with the configuration.

d. Click **Stop recoding** to stop recording.

e. Click **Export** to download the delta CFG file to the local computer. The delta CFG file is in plain text format with the filename *delta_config_result file*. If required, rename the file and convert the file to .tar format before downloading it to the ONT.

Note: For merging the downloaded delta config, the previously downloaded delta file must be renamed by adding “CFG” at the start of the filename and *.cfg* extension to be added to the delta config file (CFG_*.cfg) to upload the file successfully in Delta CFG tool page.

END OF STEPS

Troubleshooting

7.59 Troubleshooting counters

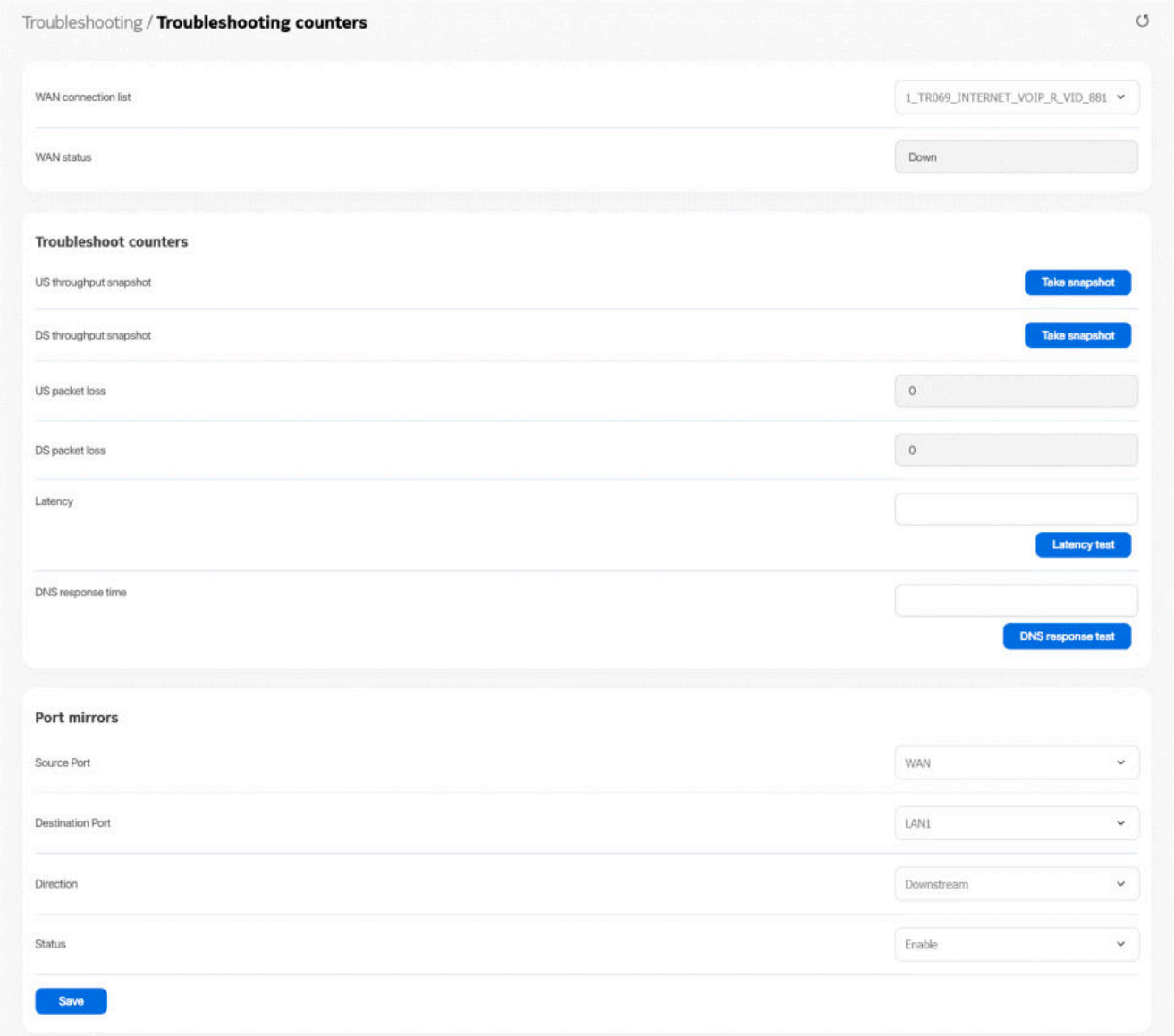
The Troubleshooting counters feature enables service providers and end users to monitor the performance of their broadband connection for about 10 seconds from the time the test is triggered.

Tests are run to retrieve upstream and downstream throughput, latency, and DNS response time. The Troubleshooting counters page also displays upstream and downstream packet loss and Internet status.

1

Click **Troubleshooting→Troubleshooting counters** in the left pane. The *Troubleshooting counters* page displays.

Figure 7-69 Troubleshooting counters page



2

Configure the following parameters:

Table 7-43 Troubleshooting counters parameters

Field	Description
WAN Connection List	Select a WAN connection from the list.
WAN Status	Displays the WAN status: • Up • Down
Troubleshoot counters	
US throughput snapshot	This test is used to determine the upstream throughput/speed. Click **Take snapshot** to take a snapshot of the time for the upstream test.
DS throughput snapshot	This test is used to determine the downstream throughput/speed. Click **Take snapshot** to take a snapshot of the time for the downstream test.
US packet loss	Displays the number of upstream packages lost.
DS packet loss	Displays the number of downstream packages lost.
Latency	This test is used to determine the lowest round-trip time in milliseconds by pinging the target server multiple times. Click **Latency test** to specify the time for the test.
DNS response time	This test is used to determine the lowest round-trip time in milliseconds by sending a request to the target DNS server. Click **DNS response test** to specify the time for the test.

3

Click **Save**.

END OF STEPS

7.60 Speed Test

1

Click **Troubleshooting→Speed test** in the left pane. The *Speed test* page displays.

Figure 7-70 Speed test page

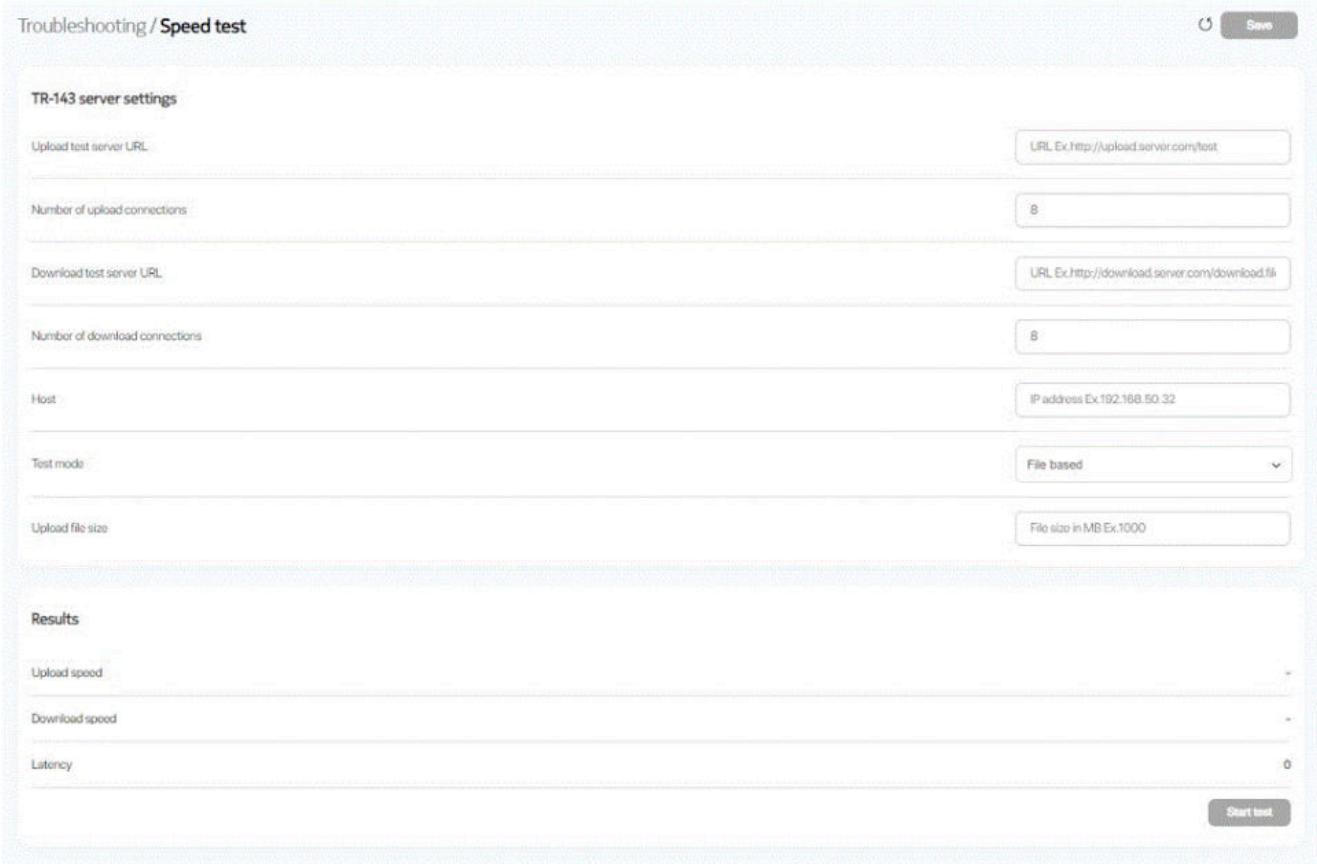


Table 7-44 Speed test parameters

Field	Description
TR-143 server settings	
Upload test server URL	Enter the Upload test server URL.
Number of upload connections	Enter the Number of upload connections.
Download test server URL	Enter the Download test server URL.
Number of download connections	Enter the Number of download connections.
Host	Enter Host.
Test mode	Select a Test mode: • Time based • File based

Table 7-44 Speed test parameters (continued)

Field	Description
Upload file size	Displays the file size in MB. This parameter is visible only if the Test mode is **File Based**.
Duration	Displays the time duration is sec. This parameter is visible only if the Test mode is **Time Based**.
Results	
Upload speed	Displays the upload speed.
Download speed	Displays the download speed.
Latency	Displays the latency.

2

Click **Save** to save the TR-143 settings.

3

Click **Start test** to start the speed test.

END OF STEPS

8 ONT configuration file over OMCI

8.1 Overview

8.1.1 Purpose

8.1.2 Contents

8.2 Purpose

This procedure describes how to use configuration files over OMCI to configure ONTs. Some advantages include:

- Flexibility to change the ONT default behavior by downloading configuration file
- Flexibility to update a deployed ONT by downloading updated parameters
- Ability to securely download any configuration file to an ONT
- Ability to avoid using embedded configuration files in ONT software

Note: This feature is supported for use with the 7360 ISAM FX and the 7342 ISAM FTTU.

8.3 Supported configuration file types

Table 8-1, “Supported configuration files” (p. 196) describes the configuration file types that are supported from G-0126G-A R05.02.00 and later.

Table 8-1 Supported configuration files

File Index	Description	Details	Supported ONTs/DPU
PRE	ONT pre-configuration file	The XML-based PRECONFIG file controls the working mechanics of the ONT for various services. The default behavior of different ONTs may vary based on the factory settings. The pre-configuration file includes the factory default value for the residential gateway. Note: The pre-configuration file does not work with SFU ONTs; therefore, this feature applies only to Residential Gateway ONTs. The pre-configuration file can be used as is, but Nokia provides its customers with the flexibility to customize the pre-configuration file. This pre-configuration file enables operators to change the default behavior by downloading a customized pre-configuration based on customer inputs. This PRE XML file includes a custom OPERID. The Nokia defined index for the PRECONFIG file is: "PRE"	All Nokia GPON and 10 GPON ONT.
CFG	ONT configuration delta file	The XML-based CFG file updates the configurable parameters (the PRE settings) in the existing PRE file of a deployed ONT, where required. This configuration file enables operators to change the deployed behavior by downloading customized updates in the CFG file. This file is used only to modify the parameters in the PRE file; it is not used for service provisioning. No OPERID is required, because the update is based on the OPERID used for the PRE file. The Nokia defined index for the PRECONFIG DELTA file is: "CFG"	All Nokia GPON and 10GPON ONT.
GFT	G.fast-related configuration file	This text-based json script file controls the default behavior of the G.Fast ONT. This file includes the provisioning parameters of the G.fast transports layer; it does not include VLAN or QoS provisioning. While the ONT functions well with the default values; they can optionally be customized. While default values can work in VDSL mode, a download file is required for the device to function as a G.fast ONT. The Nokia defined index for the G.fast file is: "GFT"	Nokia G.fast.

8.3.1 Filename conventions

Nokia provides the raw configuration files, which must be saved by the operator in a TAR file to be uploaded. TAR file names must be unique.

The filenames of the raw configuration files may not adhere to the naming conventions outlined below. In this case, the files must be renamed to adhere to the naming conventions before the operator generates the TAR file. Filenames are not case-sensitive.

ABCXXXXVER

where

ABC is the file index type (PRE, CFG, XML, GFT)

XXXX is the operator ID

For PRE and CFG, a valid operator ID is required

For XML and GFT, any characters may be used

VER is the file version (from 001 to 999)

Note: You cannot update the configuration using two files with the same name.

8.3.2 Download configuration file

The following table provides the supported download options for ONT pre-configuration file and configuration file.

Table 8-2 Download configuration files

ONT type	Legacy method download		Zero management download	
	PRE file	CFG file	PRE file	CFG file
Broadlight(eg.I240WA-3FE54869AFGA80)	—	✓	—	✓
Broadcom(eg.G240WB-3FE56773BFGA07)	—	✓	✓	✓
MTK(eg.G240WF)	—	✓	✓	✓

8.4 ONT configuration file over OMCI

WARNING

Equipment Damage

Executing the following procedure will trigger the ONT to reboot, which will impact ongoing services.

Use this procedures to configure ONTs using configuration files via legacy method and OMCI.

8.4.1 Configuring an ONT using a configuration file via legacy method

1

Upload the ABCXXXXVER TAR file to the /ONT/ directory in the OLT.

A maximum of 250 files can be kept in the OLT file system.

2

Using OLT commands, download the TAR file to the ONT.

For OLT commands, refer to the *7360 ISAM FX CLI Command Guide for 100_320Gbps FD NT and FX NT*, or the **7342 ISAM FTTU Operation and Maintenance Using TL1 and CLI**.

Please note:

- **pri-cfgfile-pland/dnload** or **sec-cfgfile-pland/dnload** can be 1 to 14 characters.
- **pri-cfgfile-pland** and **pri-cfgfile-dnload** should be the same name.

Examples

Note: X can be 1 or 2 unless specified:

a. If **pland-cfgfileX= Disabled** and **dnload-cfgfileX= Disabled**,

no file is downloaded to the ONT.

b. If **pland-cfgfileX=FILENAME1** and **dnload-cfgfileX= Disabled**,

FILENAME1 is downloaded and FILENAME1 is made active. An ONT reboot is required.

c. If **pland-cfgfileX=Disabled** and **dnload-cfgfileX= FILENAME2**,

FILENAME2 is downloaded and FILENAME2 is made passive. An ONT reboot is not required.

d. If **pland-cfgfileX=FILENAME3** and **dnload-cfgfileX= FILENAME4**, the OLT reports an error because the filenames are not the same.

e. Configure equipment interface **pland-cfgfile1=XMLXXXXXX1** and **dnload-cfgfile1 XMLXXXXXX1**

Configure equipment interface **pland-cfgfile2=XMLXXXXXX2** and **dnload-cfgfile2 XMLXXXXXX2**

Although the OLT permits the above two steps without reporting an error, Nokia does not recommend executing them, because the ONT may exhibit unexpected behavior.

f. If **pland-cfgfileX=Auto** and **dnload-cfgfileX= Auto**

The OLT will download the XML file from "sw-ctr-list" (**configure equipment ont sw-ctrl**)

END OF STEPS

The ONT will distribute the configuration files to the different services based on the active indication from the OLT and on the Nokia defined index.

The ONT automatically reboots to apply the configuration files. After the ONT reboots and reports the active version, the OLT completes the file download procedure.

Operators must check the committed file from the OLT to verify whether the corresponding file has been applied. If an error occurs, contact Nokia for support.

8.4.2 Configuring an ONT using a configuration file via OMCI

1

Generate the TAR file to be uploaded to the OLT.

Using the raw configuration file(s) provided by Nokia, generate the TAR file as follows:

a. On a Linux platform, rename the raw configuration file to adhere to the naming convention, as described in section 8.3 “Supported configuration file types” (p. 195).

b. Tar the **ABCXXXXVER** raw configuration file:

`tar -cf ABCXXXXVER.tar ABCXXXXVER`

Where

ABCXXXXVER

Is the name of the file created in step i.

This creates two files: **ABCXXXXVER** and **ABCXXXXVER**.tar.

c. Rename **ABCXXXXVER** to **ABCXXXXVER**.org

d. Remove the “.tar” extension from **ABCXXXXVER**.tar file.

2

Upload the ABCXXXXVER TAR file to the /ONT/ directory in the OLT.

A maximum of 250 files can be kept in the OLT file system.

3

Using OLT commands, download the TAR file to the ONT.

For OLT commands, refer to the *7360 ISAM FX CLI Command Guide for 100_320Gbps FD NT and FX NT*, or the **7342 ISAM FTTU Operation and Maintenance Using TL1 and CLI**.

Please note:

- **pri-cfgfile-pland/dnload** or **sec-cfgfile-pland/dnload** can be 1 to 14 characters.
- **pri-cfgfile-pland** and **pri-cfgfile-dnload** should be the same name.

Examples

Note: Note: X can be 1 or 2 unless specified:

a. If **pland-cfgfileX= Disabled** and **dnload-cfgfileX= Disabled**,

no file is downloaded to the ONT.

b. If **pland-cfgfileX=FILENAME1** and **dnload-cfgfileX= Disabled**,

FILENAME1 is downloaded and FILENAME1 is made active. An ONT reboot is required.

c. If **pland-cfgfileX=Disabled** and **dnload-cfgfileX= FILENAME2**,

FILENAME2 is downloaded and FILENAME2 is made passive. An ONT reboot is not required.

d. If **pland-cfgfileX=FILENAME3** and **dnload-cfgfileX= FILENAME4**, the OLT reports an error because the filenames are not the same.

e. Configure equipment interface **pland-cfgfile1=XMLXXXXXX1** and **dnload-cfgfile1 XMLXXXXXX1**

Configure equipment interface **pland-cfgfile2=XMLXXXXXX2** and **dnload-cfgfile2 XMLXXXXXX2**

Although the OLT permits the above two steps without reporting an error, Nokia does not recommend executing them, because the ONT may exhibit unexpected behavior.

f. If **pland-cfgfileX=Auto** and **dnload-cfgfileX= Auto**,

the OLT will download the XML file from "sw-ctr-list" (**configure equipment ont sw-ctrl**)

END OF STEPS

The ONT will distribute the configuration files to the different services based on the active indication from the OLT and on the Nokia defined index.

The ONT automatically reboots to apply the configuration files. After the ONT reboots and reports the active version, the OLT completes the file download procedure.

Operators must check the committed file from the OLT to verify whether the corresponding file has been applied. If an error occurs, contact Nokia for support.

8.4.3 Configuring ONT using a Combined Customized Software Package

ONT supports a combined customized software package which includes a new software-version and one or more configuration files (Config, Delta Config, and WebGUI config), allowing to download and install it as a single package into the ONT. This is specially useful in deployment scenarios with third party OLTs, which do not support Nokia configuration files download via OMCI.

Note:

1. If the ONT exist on your OLT system, and before configuring the ONT using customized firmware, the **pri-cfgfile-pland** and **pri-cfgfile-dnload** files must be disabled.
2. The pre-config, delta config, and/or WebGUI configuration files as well as the required firmware version file must be shared with Nokia representatives in order to create the customized combined firmware.
3. Nokia will generate the combined customized firmware file and share with the operator.

1

The customer must upload the customized firmware file to the OLT.

2

Using OLT commands, the combined customized firmware file is downloaded.

3

The ONT automatically reboots to apply the configuration files. After the ONT reboots and reports the active version, the OLT completes the file download procedure.

END OF STEPS