NOKIA

7368 Intelligent Services Access Manager ONT

7368 ISAM ONT G-240W-J Product Guide

3FE-48009-AAAA-TCZZA

Issue: 01

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

1 Preface

This preface provides general information about the documentation set for optical network terminals (ONTs).

1.1 Scope

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

1.2 Audience

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

1.3 Required knowledge

The reader must be familiar with general telecommunications principles.

1.4 Acronyms and initialisms

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

1.5 Assistance and ordering phone numbers

Nokia provides global technical support through regional call centers. Phone numbers for the regional call centers are available at the following URL: http://support.alcatel-lucent.com.

For ordering information, contact your Nokia sales representative.

1.6 Nokia quality processes

Nokia’s ONT quality 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

1.7 Safety information

For safety information, see the appropriate safety guidelines chapter.

1.8 Documents

Documents are available using ALED or OLCS.

Procedure 1 To download a ZIP file package of the customer documentation

1 Navigate to http://support.alcatel-lucent.com 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 From the Technical Content for drop-down menu, choose the product.

3 Click on Downloads: Electronic Delivery.

4 Choose Documentation from the drop-down menu and click Next.

5 Select the image from the drop-down menu and click Next.

6 Follow the on-screen directions to download the file.

Procedure 2 To access individual documents

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

1 Navigate to http://support.alcatel-lucent.com 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 From the Technical Content for drop-down menu, choose the product.

3 Click on Manuals and Guides to display a list of customer documents by title and part number. You can filter this list using the Release drop-down menu.

4 Click on the PDF to open or save the file.

1.9 Special information

The following are examples of how special information is presented in this document.

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

Caution — 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.

1.9.1 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.

Procedure 3 Example of options in a procedure

At step 1, you can choose option a or b. At step [1], 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.

Procedure 4 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: **i** This is the first substep. **ii** This is the second substep.

iii This is the third substep.

---

[1] You must perform this step.

1.10 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.

Procedure 5 To search multiple PDF files for a common term

1 Open Adobe Acrobat Reader.

2 Choose Edit→Search from the Acrobat Reader main menu. The Search PDF panel appears.

3 Enter the search criteria.

4 Click on the All PDF Documents In radio button.

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

6 Click on the Search button.

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

Table of contents

List of figures

List of tables

2 ANSI CPE safety guidelines

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

2.1 Safety instructions

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

2.1.1 Safety instruction boxes in customer documentation

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

The following is an example of the Danger box.

Danger — 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 1 — Possibility of equipment damage.

Warning 2 — 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 1 — Possibility of service interruption.

Caution 2 — Service interruption.

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

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

The following is an example of the Note box.

Note — Information of special interest.

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

2.1.2 Safety-related labels

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

Table 1 provides examples of the text in the various CPE safety labels.

Table 1 **Safety labels**

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

Figure 1 shows a sample safety label located on the bottom of the G-240W-J.

Figure 1 **Sample safety label**

2.2 Safety standards compliance

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

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

2.2.1 EMC, EMI, and ESD standards compliance

The customer premises equipment complies with the following requirements:

- Federal Communications Commission (FCC) CFR 47, Part 15, Subpart B, Class A requirements for equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is needed.
- Consult the dealer or an experienced radio/TV technician for help.

2.2.2 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the G-240W-J devices are in compliance with the essential requirements and other relevant provisions of Directive 2009/125/EC together with Commission Regulation (EC) No 1275/2008 and Commission Regulation (EC) No 801/2013.

The G-240W-J devices qualify as high network availability (HiNA) equipment. Since the main purpose of G-240W-J devices is to provide network functionality with HiNA 7 days/24 hours, the modes Off/Standby, Power Management, and Networked Standby are inappropriate.

For information about the type and number of network ports, see "G-240W-J interfaces and interface capacity" in chapter 5.

For information about power consumption, see "G-240W-J detailed specifications" in chapter 5.

2.2.3 FCC statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

2.2.4 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 23 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and consider removing the no-collocation statement.

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

1. this device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

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

2.2.5 Resistibility requirements compliance

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

2.3 Electrical safety guidelines

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

G-240W-J devices are compliant with the following standards

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

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

2.3.1 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 customer premises equipment:

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

3 ETSI ONT safety guidelines

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

3.1 Safety instructions

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

3.1.1 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 — 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 1 — Possibility of equipment damage.

Warning 2 — 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 1 —** Possibility of service interruption.

Caution 2 — 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.

ℹ **Note —** Information of special interest.

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

3.1.2 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.

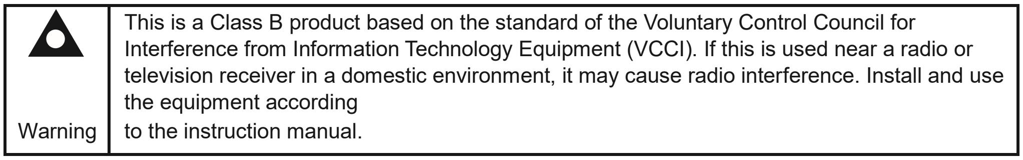
Table 2 provides sample safety labels on the ONT equipment.

Table 2 **Safety labels**

Description	Label text
ESD warning	Caution: This assembly contains an electrostatic sensitive device.
Laser classification	Class 1 laser product
PSE marking	These power supplies are Japan PSE certified and compliant with Japan VCCI emissions standards.

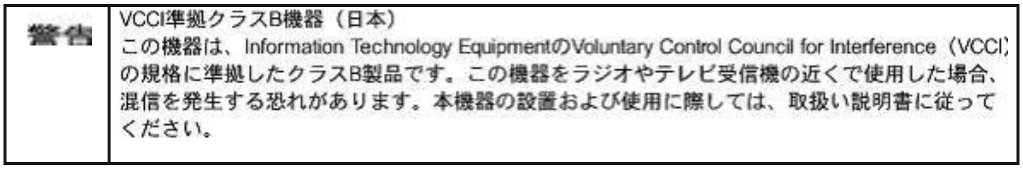
Figure 2 shows the PSE certification.

Figure 2 **PSE certification**



Warning

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according
to the instruction manual.



警告	VCCI準拠クラスB機器（日本） この機器は、Information Technology EquipmentのVoluntary Control Council for Interference（VCCI）の規格に準拠したクラスB製品です。この機器をラジオやテレビ受信機の近くで使用した場合、混信を発生する恐れがあります。本機器の設置および使用に際しては、取扱い説明書に従ってください。

19841

3.2 Safety standards compliance

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

3.2.1 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)

3.2.2 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).

3.2.3 Environmental standard compliance

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

3.2.4 CE RED RF Radiation Exposure Statement

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

3.2.5 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.

3.2.6 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 overcurrents.

3.2.7 Acoustic noise emission standard compliance

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

3.3 Electrical safety guidelines

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

Note 1 — 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.

Note 2 — The ONTs comply with BS EN 61140.

3.3.1 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.

3.3.2 Cabling

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

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

3.3.3 Protective earth

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

3.4 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 —** 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.

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

3.5.1 Laser classification

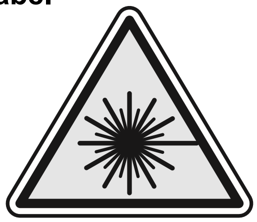
The ONT is classified as a Class 1 laser product based on its transmit optical output.

3.5.1.1 Laser warning labels

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

Figure 3 shows a laser product label.

Figure 3 **Laser product label**



18455

Figure 4 shows a laser classification label. Laser classification labels may be provided in other languages.

Figure 4 **Laser classification label**

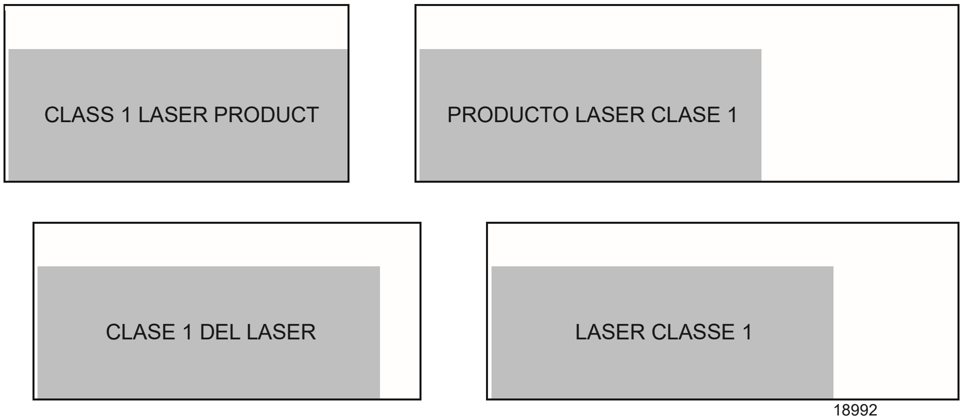
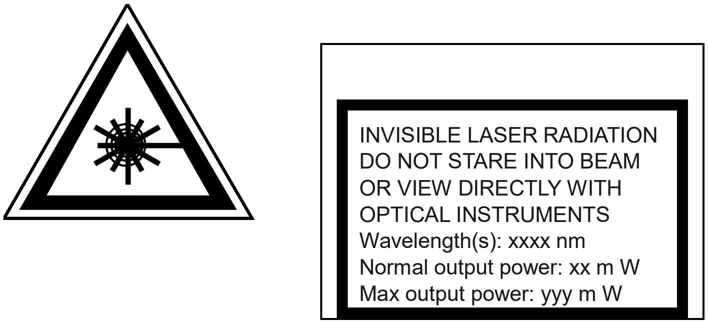


Figure 5 shows a laser warning label and an explanatory label for laser products. Labels and warning may be provided in other languages. The explanatory label provides the following information:

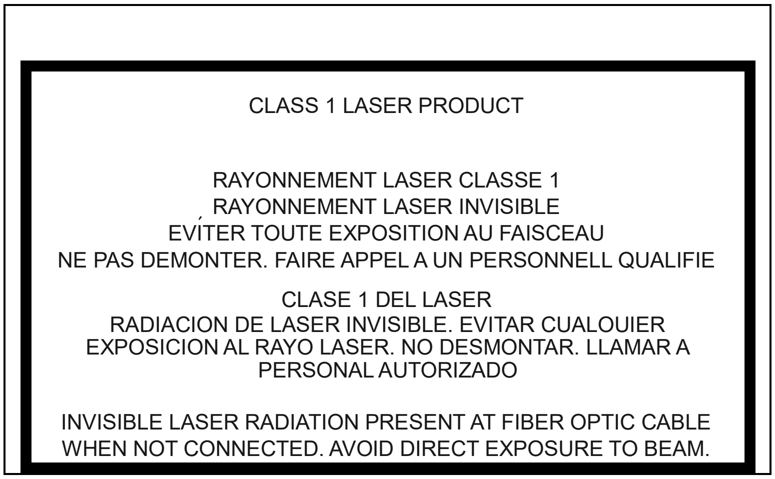
- a warning that calls attention to the invisible laser radiation
- an instruction against staring into the beam or viewing directly with optical instruments
- wavelength
- normal output power
- maximum output power

Figure 5 **Laser warning labels**



INVISIBLE LASER RADIATION
DO NOT STARE INTO BEAM
OR VIEW DIRECTLY WITH
OPTICAL INSTRUMENTS
Wavelength(s): xxxx nm
Normal output power: xx m W
Max output power: yyy m W

Laser Warning Label Laser Warning Label



CLASS 1 LASER PRODUCT

RAYONNEMENT LASER CLASSE 1
RAYONNEMENT LASER INVISIBLE
EVÍTER TOUTE EXPOSITION AU FAISCEAU
NE PAS DEMONTER. FAIRE APPEL A UN PERSONNELL QUALIFIE

CLASE 1 DEL LASER
RADIACION DE LASER INVISIBLE. EVITAR CUALOUIER
EXPOSICION AL RAYO LASER. NO DESMONTAR. LLAMAR A
PERSONAL AUTORIZADO

INVISIBLE LASER RADIATION PRESENT AT FIBER OPTIC CABLE
WHEN NOT CONNECTED. AVOID DIRECT EXPOSURE TO BEAM.

Laser Warning Label

18993

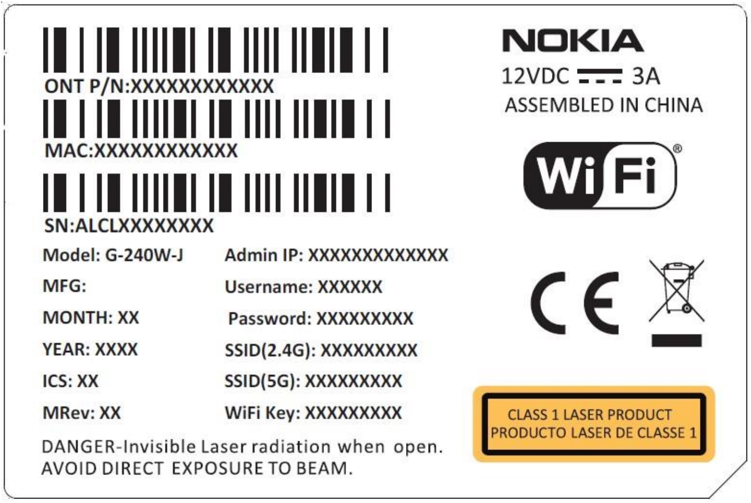
3.5.2 Laser classification

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 6 shows a sample laser product safety label on the ONT equipment.

Figure 6 **Sample laser product safety label on the ONT equipment**



ONT P/N:XXXXXXXXXXXX
MAC:XXXXXXXXXXXX
SN:ALCLXXXXXXXX

NOKIA
12VDC ⎓ 3A
ASSEMBLED IN CHINA

Model: G-240W-J
MFG:
MONTH: XX
YEAR: XXXX
ICS: XX
MRev: XX

Admin IP: XXXXXXXXXXXX
Username: XXXXXX
Password: XXXXXXXXX
SSID(2.4G): XXXXXXXXX
SSID(5G): XXXXXXXXX
WiFi Key: XXXXXXXXX

CLASS 1 LASER PRODUCT
PRODUCTO LASER DE CLASSE 1

DANGER-Invisible Laser radiation when open.
AVOID DIRECT EXPOSURE TO BEAM.

3.5.3 Transmit optical output

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

3.5.4 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 —** Risk of eye damage by laser radiation.

3.5.5 Location class

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

3.6 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.

4 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.

4.1 Environmental labels

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

4.1.1 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.

4.1.2 Environmental related labels

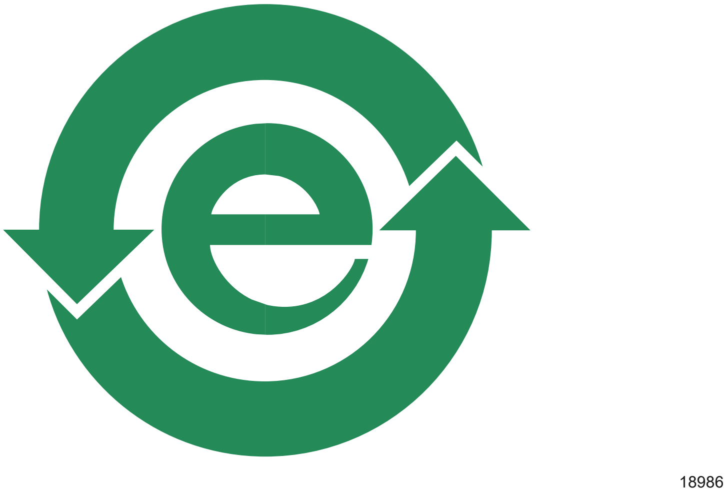
Environmental labels are located on appropriate equipment. The following are sample labels.

4.1.2.1 Products below Maximum Concentration Value (MCV) label

Figure 7 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.

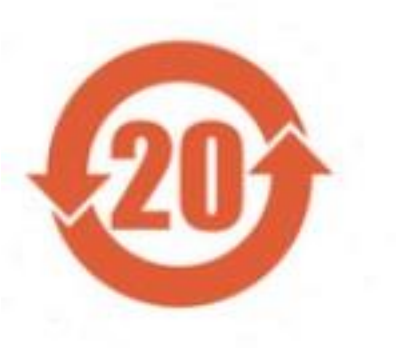
Figure 7 **Products below MCV value label**



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

Figure 8 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 8 **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 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 "Hazardous Substances Table (HST)" for more information.

4.2 Hazardous Substances Table (HST)

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

4.3 Other environmental requirements

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

4.3.1 ONT environmental requirements

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

4.3.2 Storage

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

4.3.3 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.

4.3.4 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.

4.3.5 Thermal limitations

When the ONT is installed in the CO or CEV, install air filters on the OLT. The thermal limitations for ONT operation in a CO or CEV are:

- operating temperature: 5°C to 40°C (41°F to 104°F)
- short-term temperature: –5°C to 50°C (23°F to 122°F)
- operating relative humidity: 5% to 85%
- short-term relative humidity: 5% to 95%, but not to exceed 0.024 kg of water/kg

4.3.6 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.

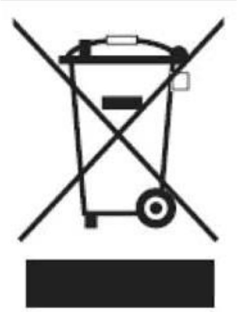
Nokia has implemented a material/substance content management process. The process is described in: Nokia process for ensuring RoHS Compliance (1AA002660031ASZZA). This ensures compliance with the European Union Directive 2011/65/EU on the Restriction of the Use of Certain Hazardous Substances in Electrical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

4.3.7 End-of-life collection and treatment

Electronic products bearing or referencing the symbol shown in Figure 9, 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 9 **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 9 at the end of their useful life, or products displaced by Nokia equipment offers. For information regarding take-back of equipment by Nokia, or for more information regarding the requirements for recycling/disposal of product, contact your Nokia account manager or Nokia take back support at sustainability.global@nokia.com.

5 G-240W-J unit data sheet

5.1 G-240W-J part numbers and identification

Table 3 provides part numbers and identification information for the G-240W-J indoor ONT.

Table 3 **Identification of G-240W-J indoor ONTs**

Ordering kit part number	Provisioning number	Description	CLEI	CPR	ECI/ Bar code
3FE 48008 AA	3FE 48009 AA	GPON indoor ONT, 2 POTS, 4 Gigabit Ethernet, dual-band WiFi 3x3 802.11n + 4x4 802.11ac, SC/APC, US plug (2-pin wall mounted 12V 3A, 6kV) LED	—	—	—
3FE 48008 BA	3FE 48009 BA	GPON indoor ONT, 2 POTS, 4 Gigabit Ethernet, dual-band WiFi 3x3 802.11n + 4x4 802.11ac, SC/APC, EU plug (2-pin wall mounted 12V)	—	—	—
3FE 48008 CA	3FE 48009 BA	GPON indoor ONT, 2 POTS, 4 Gigabit Ethernet, dual-band WiFi 3x3 802.11n + 4x4 802.11ac, SC/APC, UK plug (3-pin wall mounted 12V) Nokia logo,	—	—	—

Table 4 provides the power supply information for the G-240W-J ONT. For more information on power supplies, see the *7368 ISAM ONT Power Supply and UPS Guide*.

Table 4 **G-240W-J power supply**

ONT part numbers	Power model	Power information	Customer category or country compliance tested for	Notes
Kit: 3FE 48008 AA EMA: 3FE 48009 AA	SUN-1200300 RD1203000-C55-20MG	36 Watt AC/DC power adapter	ANSI municipality US, Canada ETSI, IEC 60950-1	2-pin US input plug with LED
Kit: 3FE 48008 BA EMA: 3FE 48009 BA	RD1203000-C55-115OG SOY-1200300EU	36 Watt AC/DC power adapter	CE certified	2-pin EU input plug
Kit: 3FE 48008 CA EMA: 3FE 48009 BA	RD1203000-C55-20YG SOY-1200300GB	36 Watt AC/DC power adapter	CE certified	3-pin UK input plug

5.2 G-240W-J general description

G-240W-J 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 ONT is compatible with all existing subscriber equipment, including analog phones with both tone and rotary dial capabilities, cordless phones, modems, fax machines, and caller ID boxes (Type I, Type II, and Type III).

G-240W-J indoor ONTs provide the following functions:

- Single fiber GPON interface with 1.244Gbit/s upstream and 2.488Gbit/s downstream data rates
- Advanced data features such as VLAN tag manipulation, classification, and filtering.
- Traffic classification and QoS capability
- Analog Telephone Adapter (ATA) function integrated based on SIP (RFC3261), with various CLASS services supported, including Caller ID, Call Waiting, Call Forwarding, and Call Transfer
- 5 REN per line
- Multiple voice Codec
- MDI/MDIX auto-negotiation
- Line Rate L2 traffic
- Internal Switch
- UPnP IGD2.0 support
- Bridged mode or routed mode per LAN port
- Optics that support received signal strength indication (RSSI)

- Internal DHCP server, with configurable DHCP pool and gateway
- WPS on wireless authorization support
- 802.11ac support
- 2.4 GHz and 5 GHz wireless interface
- 450Mbps PHY Rate for 3x3 2.4Ghz, and 2.2Gbps PHY rate for 4x4 5Ghz with QAM1024
- Maximum effective isotropic radiated power (EIRP) on 2.4 GHz up to 500 mW and 5 GHz up to 1 W (as constrained by local regulations)
- antenna gain: 2.4 GHz and 5 GHz Wi-Fi: 3dBi
- Concurrent 802.11n 3x3 MIMO in 2.4 GHz and 802.11ac 4x4MIMO in 5GHz
- Support Beamforming
- Support auto channel selection
- Different hardware variants for different available channel list follows the regional regulatory
- Support MCS0-8 for 802.11n and MCS0-11 for 802.11ac
- support HT20/HT40 for 802.11b/g/n, and HT20/40/80 for 802.11ac
- support for up to 32 simultaneous wireless connections
- 64/128 WEP encryption
- WPA, WPA-PSK/TKIP
- WPA2, WPA2-PSK/AES
- support for multiple SSIDs (private and public instances); contact your Nokia representative for further details.
- WLAN on/off push button
- WPS/PBC button (for 2.4 GHz and 5 GHz)
- Ethernet-based Point-to-Point (PPPoE)
- Network Address Translation (NAT)
- Network Address Port Translation (NAPT)
- ALG and UPnP port forwarding
- DMZ
- IP/MAC filter
- Multi-level firewall
- DNS server
- DHCP client/server
- External USB HD (Hard Drive) support, accessible to all LAN devices

5.2.1 Configuring the G-240W-J to function as a single port ONT

In addition to functioning as a residential gateway, the G-240W-J ONT can be configured to function as a single port ONT.

In the custom configuration, the ONT reports to the OLT as one PPTP port. The physical Ethernet port of the ONT is managed by the RGW using the TR-069 protocol, rather than by the ONT/OMCI.

To enable the ONT to function as a single port ONT, the value of the parameter:

```
InternetGatewayDevice.DeviceInfo.X_ALU-COM_PortReport2OLT.PPTP
```

must be set to

```
PPTP_one
```

A custom pre-configuration file is required to operate the G-240W-J as a single-port ONT. Contact your Nokia support engineer to arrange for a custom pre-configuration file.

5.2.2 Support for CFM over S-tunnel

The G-240W-J ONT supports Connectivity Fault Management (CFM) over S-tunnel. This feature eliminates the need for creating many UP MEPs to handle CFM frames with each inner VLAN tag. The UP MEP can be configured using the CLI. Down MEP over S-tunnel is not supported.

To configure the S-tunnel, type the following commands:

```
configure vlan id stacked:1025:0 mode cross-connect in-qos-prof-name
name:Default_TC0 mac-mcast-ctrl
```

```
configure vlan id stacked:1026:0 mode residential-bridge in-qos-prof-name
name:Default_TC0 mac-mcast-ctrl
```

To configure the UP MEP, type the following commands:

```
configure cfm domain 5 name string:MD1 level 1 configure cfm domain 5

association 1 vlan stacked:1025:0 name string:MA1 configure cfm domain

5 association 1 mep 2 location user:1/1/1/1/1/1/1
```

The current design does not support the propagation of AIS frames with VLAN information from the received packet. As a result, when a downstream AIS frame is received for UP MEP over S-tunnel, the propagated AIS packet will not contain the VLAN information.

5.2.3 TR-069 parameter support

The G-240W-J ONT supports the following TR-069 features:

- Host object
- Port forwarding
- Optical parameters
- Object support for Wi-Fi parameters
- Statistics and troubleshooting
- Diagnostic parameter
- Timing parameter

5.2.3.1 Host object support

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

5.2.3.2 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 are the same port forwarding parameters supported in the GUI. For more information, see Table 46 in the chapter “Configure a G-240W-J indoor ONT”.

5.2.3.3 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 are the same optical parameters supported in the GUI. For more information, see Table 23 in the chapter "Configure a G-240W-J indoor ONT".

5.2.3.4 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 and WEP
- Tx power (transmission rate in percentage of maximum transmit power)
- WPS

These are the same TR-069 object parameters that are supported in the GUI. For more information, see Tables 29 and 30 in the chapter "Configure a G-240W-J indoor ONT".

5.2.3.5 Statistics and troubleshooting support

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

For more information, see the Procedure "Statistics retrieval" in the chapter "Configure a G-240W-J indoor ONT".

5.2.3.6 Diagnostic parameter support

The ONT supports the following TR-069 diagnostic parameters:

- TR-143
- IP ping
- traceroute

These are the same diagnostic parameters supported in the GUI. For more information, see Procedure "Diagnose WAN connections" in the chapter "Configure a G-240W-J indoor ONT".

5.2.3.7 Timing parameter support

The ONT supports TR-069 timing parameters.

5.2.4 TR69 authentication using TLS and CA certificates

G-240W-J 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.

5.2.5 TR-104 parameter extension support for voice service

A proprietary attribute has been added to the TR-104 Voice Service object structure to enable the ACS to configure the name of the embedded GSIP XML file to be selected.

The TR-104 Voice Service Object is:
InternetGatewayDevice.Services.VoiceService.{i}.Capabilities.SIP.

The proprietary attribute is: X_ALU-COM_XML_File_Name_Path.

5.2.6 TR-104 voice-related alarms

The G-240W-J ONT supports the following four TR-104 voice-related alarms on a per FXS port basis.

These alarms all represent SIP registration failures with an alarm level of MAJOR.

- SIPREGDNS: domain name could not be resolved
- SIPREGAUTH: authentication failed
- SIPREGTO: re-transmissions timed out
- SIPREGERFRSP: error response from the registration server

5.2.7 TR-104 parameters for FX line testing

New attributes have been added to the TR-104 Voice Service object structure to enable the ACS to perform line tests. The ONT supports the following electrical line tests:

- hazardous potential
- foreign electrical motive force
- resistive faults
- receiver off-hook test
- ringers test

5.2.8 TR-111 support

The G-240W-J 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.

5.2.9 TR-181 parameter support

TR-181 parameter support has been introduced or enhanced for the parameter categories and functions listed in Table 5.

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

Table 5 **Support for TR-181 parameter categories**

Parameter category	Functionality
Diagnostics	Bulk data: collection, reports, HTTP, and encoding
	DNS
	IP ping
	TR-143 uploading and downloading
	IPv6
	Periodic statistics
	Self test
	WiFi neighboring
End user functional features	Bridging port
	Captive portal
	Device information, including: processor, data model, and vendor log

	Device interface
	DHCPv4 and DCHPv6 client and server
	Ethernet interface
	Firewall
	Hosts
	Interface stack
	IP interface configuration

(1 of 2)

Parameter category	**Functionality**
End user functional features	Management server
	NAT
	Neighbor discovery
	Optical interface
	PPP interface
	QoS classification, QoS queue, and QoS shaper
	Routing and route information
	Timing
	Remote access
	User
	WiFi: AP configuration, radio configuration, and SSID configuration
Statistics and status monitoring	Bridging statistics
	Device information processes
	WiFi radio statistics
WiFi	Access point configuration
	Access point associated device
	Radio configuration
	SSID configuration

(2 of 2)

5.2.10 Mobile offload support

As part of the E2E solution supported by the ISAM 7750 service router, the G-240W-J ONT offers Mobile Offload support using a combination of EAP-SIM and ITU-T 802.11.

EAP-SIM is an authentication method that uses the user credentials on the SIM card and EAP to authenticate the user with the Wi-Fi network, removing the need for user input (username and password).

A dedicated public mobile offload SSID in the ONT enables mobile subscribers to connect to the Internet. Encryption is supported by 802.11, providing seamless Wi-Fi authentication for SIM-based user equipment.

The ONT acts as the RADIUS client and sends the encapsulated EAP messages to the AAA server via the WLAN Gateway, which acts as the RADIUS proxy server. The interaction between the ONT and the AAA server provides subscriber management for authenticated mobile users without adding authentication load to the 3G network.

5.2.11 Support for soft GRE tunnels

This section describes the support for soft GRE tunnels for integration with the 7750 Service Router WLAN gateway. The Nokia 7750 Service Router WLAN GW can accept soft GRE tunnels from any IP Source Address, in a preconfigured Subnet or Access Control List, or MPLS label.

5.2.11.1 GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. GRE provides a secure path for transporting packets through a public network. In essence, GRE creates a private P2P connection, similar to a VPN, between clients and servers. GRE is the preferred transport mechanism between the Carrier Wi-Fi access network and the WLAN GW.

GRE works by encapsulating a payload (an inner packet that needs to be delivered to a destination network) inside an outer IP packet. GRE tunnel endpoints send payloads through GRE tunnels by routing encapsulated packets through intervening IP networks. The inner packets are not parsed along the way; only the outer IP packets are parsed as they are forwarded towards the GRE tunnel endpoint, where the GRE encapsulation is removed, and the payload is forwarded to its final destination.

5.2.11.2 Soft GRE

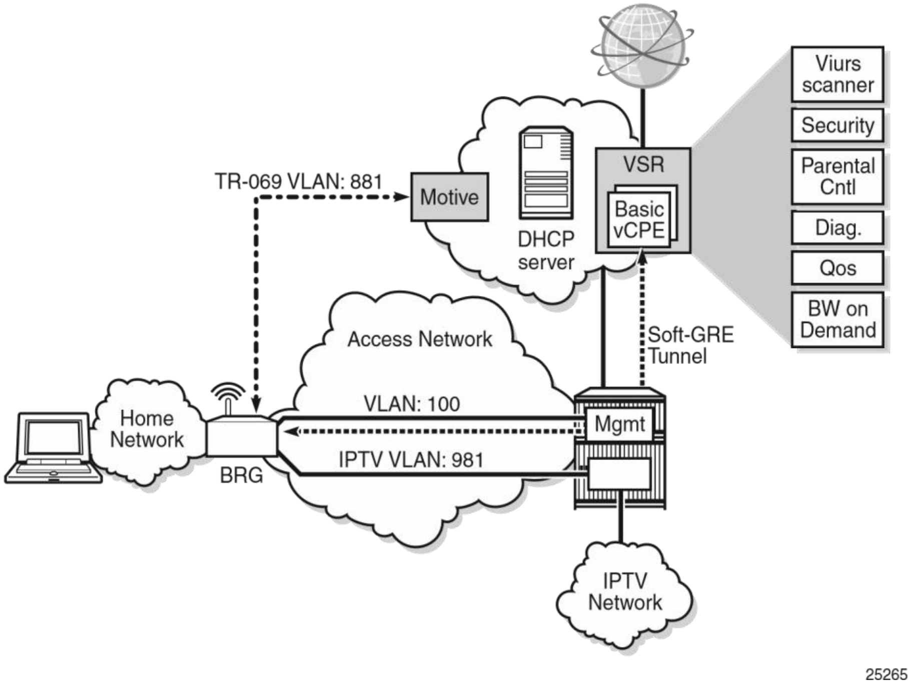
In soft GRE, only one side of the tunnel needs to be configured; the other end learns the remote IP addresses of all remote tunnel endpoints by examining the incoming GRE packets.

GRE tunnels can be automatically created when devices attach to the AP, eliminating the need for each AP to be explicitly provisioned on the WLAN Gateway. Because this soft GRE is stateless and the tunnel contexts are created based on need, the WLAN Gateway does not need to maintain states for unused tunnels, which improves scalability.

The operator can restrict the traffic going through the GRE tunnel based on the SSIDs or LAN ports.

Figure 10 shows the soft GRE architecture.

Figure 10 **Soft GRE-based architecture**



For more information about soft GRE architecture and configuration procedures, see the *7368 Configuration, Management, and Troubleshooting guide*.

5.3 G-240W-J software and installation feature support

For information on installing or replacing the G-240W-J, see:

- Install a G-240W-J indoor ONT
- Replace a G-240W-J indoor ONT

For information on the following topics, see the *7368 ISAM ONT 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

5.4 G-240W-J interfaces and interface capacity

Table 6 describes the supported interfaces and interface capacity for G-240W-J indoor ONTs.

Table 6 **G-240W-J indoor ONT interface connection capacity**

ONT type and model	Maximum capacity								
	POTS	10/ 100 BASE-T	10/ 100/ 1000 BASE-T	RF video (CATV)	MoCA	VDSL2	E1/T1	Local craft	GPON SC/APC
G-240W-J [1]	2	—	4	—	—	—	—	—	1

Note

[1] The G-240W-J ONTs provide Wi-Fi service that is enabled and disabled using a Wi-Fi on/off switch.

5.4.1 G-240W-J connections and components

Figure 11 shows the physical connections for G-240W-J indoor ONTs.

Figure 11 **G-240W-J indoor ONT physical connections**

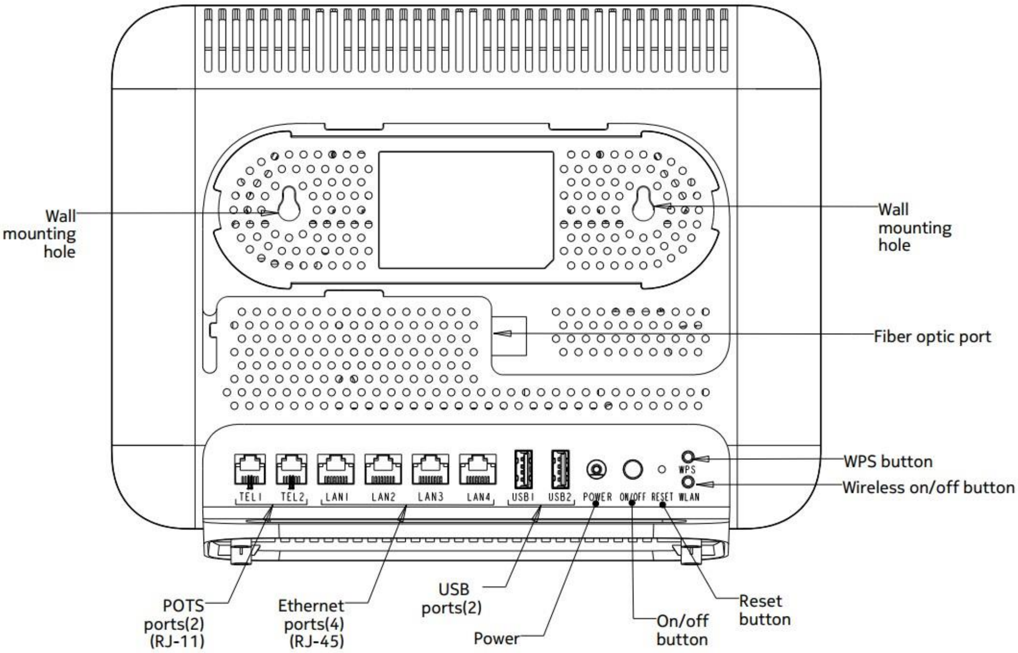


Figure 12 shows the G-240W-J indoor ONT with a fiber optic connector.

Figure 12 **G-240W-J indoor ONT with fiber optic connector**

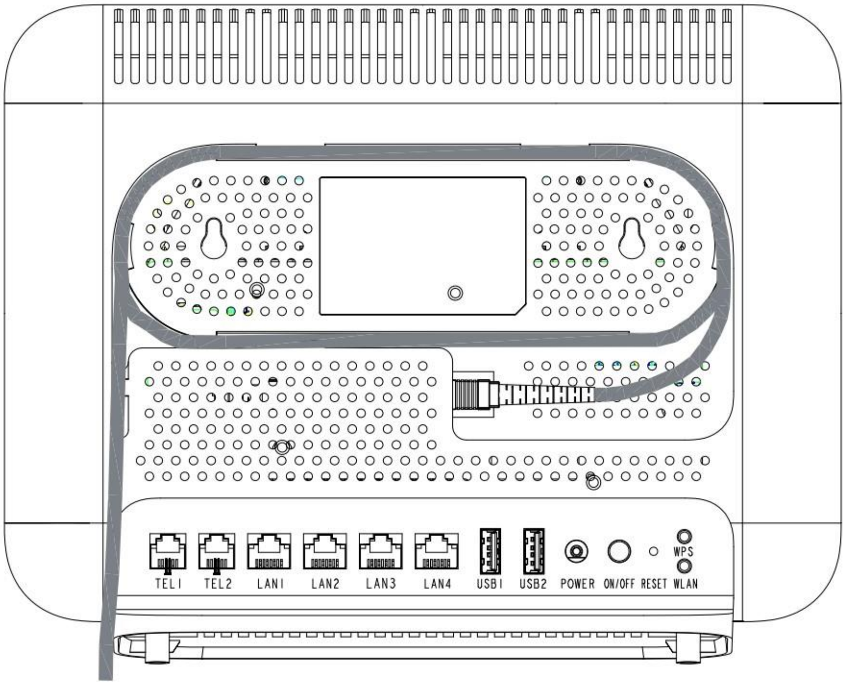


Table 7 describes the physical connections for G-240W-J indoor ONTs.

Table 7 **G-240W-J indoor ONT physical connections**

Connection [1]	Description
POTS ports	This connection is provided through RJ-11 ports. Up to two POTS connections are supported.The POTS ports support voice services.
Ethernet ports	This connection is provided through Ethernet RJ-45 connectors. Up to four 10/100/1000 Base-T Ethernet interfaces are supported.The Ethernet ports can support both data and in-band video services on all four interfaces.
USB ports	This connection is provided through 2 USB ports. The ONT supports external USB hard drives that can be made accessible to all LAN devices.
WPS button	The Wi-Fi Protected Setup button is labeled as WPS. This button enables and disables WPS for 2.4 GHz and 5 GHz bands.
WLAN button	The WLAN button turns the Wi-Fi service on or off. Wi-Fi service is compliant with IEEE 802.11 standards and is enabled or disabled using the WLAN button.
Reset button	Pressing the Reset button for less than 10 seconds reboots the ONT. Pressing the Reset button for 10 seconds resets the ONT to its factory defaults, except for the LOID and SLID.
Power input	This connection is provided through the power connector. A power cable fitted with a barrel connector is used to make the connection.
On/Off button	This button turns the ONT on or off.
Fiber optic port	This port provides the connection for the fiber optic cable.

Note

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

5.5 G-240W-J LEDs

Figure 13 shows the G-240W-J indoor ONT LEDs.

Figure 13 **G-240W-J indoor ONT LEDs**

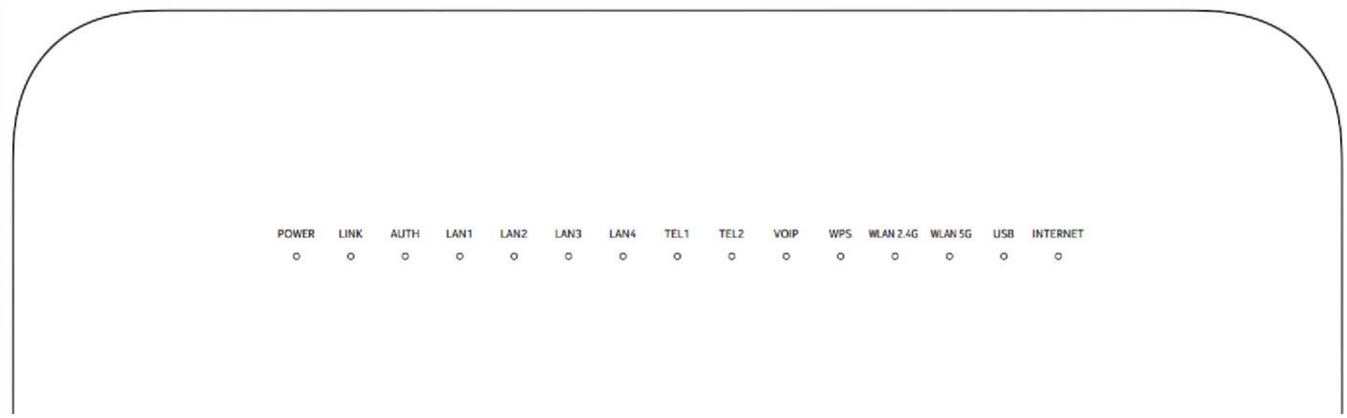


Table 8 provides LED descriptions for G-240W-J indoor ONTs.

Table 8 **G-240W-J indoor ONT LED descriptions**

Indicator	LED color and behavior	LED behavior description
Power	Green solid Red solid Off	Power on Light failed on startup (for example corrupt flash), or self test failed on startup, or self test failed during regular operation or when executed over OMCI Power off
Link	Green solid Off	GPON link between ONT and OLT is operating normally GPON link is down or no link is connected
Auth	Off Green solid Green flashing	Fiber is not connected or no power is received to the ONT ONT is configured on the OLT and is in service (UP) ONT is in the process of ranging or synchronizing over the OLT ONT is ranged but not configured on the OLT ONT is configured on OLT but admin is down and the ONT is out of service ONT is in service and subsequently un-configured on the OLT ONT is in service while other services are being configured ONT is in service but admin is down and the ONT is out of service
LAN 1 to 4	Green solid Green flashing Off	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) LAN activity is present (traffic in either direction) ONT power is off or Ethernet is not connected
TEL 1 to 2	Green solid Green flashing Off	Phone is off hook. Phone is in 'call in' or 'talking' condition All phones are on hook
VOIP	Green solid Off	VoIP service is built up and can provide service VoIP service is not built up or out of service
WPS	Green solid Green flashing Red solid Off	WiFi protected setup link is up (negotiation and auto-configuration successful) WiFi protected setup link activity (negotiation and auto-configuration ongoing) WiFi protected setup processing exception or multiple peers using WPS simultaneously WiFi protected setup link down or no link connected (negotiation has not started or has failed)
WLAN 2.4 GHz	Green solid Green flashing Off	WLAN link is enabled in 2.4 GHz Traffic is passing through the WLAN link WLAN link is disabled or no link is connected
WLAN 5 GHz	Green solid Green flashing Off	WLAN link is enabled in 5 GHz Traffic is passing through the WLAN link WLAN link is disabled or no link is connected

(1 of 2)

USB	Green solid Green flashing Off	At least one device is connected to the USB port There is traffic activity on at least one device connected to the USB port No device is connected to the USB port
INTERNET	Green solid Green flashing Off	HSI WAN is connected: a) the device has an IP address assigned from IPCP, DHCP, or static, and no traffic has been detected; b) the session is dropped due to idle timeout but the PON link is still present. PPPoE or DHCP connection is in progress, or transmit and receive traffic is ongoing. HSI WAN is not connected: a) there is no physical interface connection; b) the device is in bridged mode without an assigned IP address; c) the session has been dropped for reasons other than idle timeout.

(2 of 2)

5.6 G-240W-J detailed specifications

Table 9 lists the physical specifications for G-240W-J indoor ONTs.

Table 9 **G-240W-J indoor ONT physical specifications**

Description	Specification
Length	9.62 in. (244.31 mm)
Width	1.48 in. (37.54 mm)
Height	7.54 in. (191.48 mm)
Weight [within ± 0.5 lb (0.23 kg)] (net weight of ONT)	1.22 lb (0.553 kg)

Table 10 lists the power consumption specifications for G-240W-J indoor ONT.

Table 10 **G-240W-J indoor ONT power consumption specifications**

Mnemonic	Maximum power (Not to exceed)	Condition	Minimum power	Condition
G-240W-J	16.92W	2 POTS off-hook, 4 10/100/1000 Base-T Ethernet, Wi-Fi operational	3.96W	2 POTS on-hook, other interfaces/services not provisioned

Table 11 lists the environmental specifications for G-240W-J indoor ONT.

Table 11 **G-240W-J indoor ONT environmental specifications**

Mounting method	Temperature range and humidity	Altitude
On desk or wall mounted	Operating: 23°F to 113°F (-5°C to 45°C) ambient temperature 5% to 95% relative humidity, non-condensing	Contact your Nokia technical support representative for more information
	Storage: -4°F to 185°F (-20°C to 85°C)	

5.7 G-240W-J GEM ports and T-CONTs

Table 12 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 12 **G-240W-J indoor ONT capacity for GEM ports and T-CONTs**

ONT or MDU	Maximum	Notes
Package P ONTs		
GEM ports per indoor ONT	124	124 are present; 122 are available, and 2 are reserved for multicast and debugging
T-CONTs per indoor ONT	32	32 are present; 31 are available, and 1 is reserved for OMCI

5.8 G-240W-J performance monitoring statistics

The following section identifies the supported performance monitoring statistics for G-240W-J 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 13 provides statistics for ONTENET type counters
- Table 14 provides statistics for ONTL2UNI type counters
- Table 15 provides statistics for PONONTTC, PONONTMCTC, PONONTTCHSI, PONONTTCCES, PONONTTCFLOW, and PONONTTCVOIP type counters
- Table 16 provides statistics for PONONTTC aggregate type counters

Note — If you have trouble accessing G-240W-J 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.

Table 13 **Package P ONTs ONTENET performance monitoring statistics**

ONT	ONTENET statistics													
	FCSE	EC	LC	RBO	SCF	MCF	DT	IMTE	CSE	AE	IMRE	FTL	TBO	SQE
G-240W-J [(1)]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Note

[(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 14 Package P ONTs ONTL2UNI performance monitoring statistics

ONT	ONTL2UNI statistics										
	FRAMES	BYTES	MCFRAMES	DSDRPDFRMS	USDRPDFRMS	USFRAMES	DSFRAMES	USBYTES	DSBYTES	USMCFRAMES	DSMCFRAMES
G-240W-J [1]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Note

[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 15 Package P 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-240W-J [1]	✓	✓	✓	✓	✓	

Note

[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 16 Package P ONTs PONONTTC aggregate performance monitoring statistics

ONT	PONONTTC (aggregate) statistics					
	TXBLOCKS	TXFRAGS	RXBLOCKS	RXFRAGS	LOSTFRAGS	BADGEMHDRS
G-240W-J [1]	✓	✓	✓	✓	✓	

Note

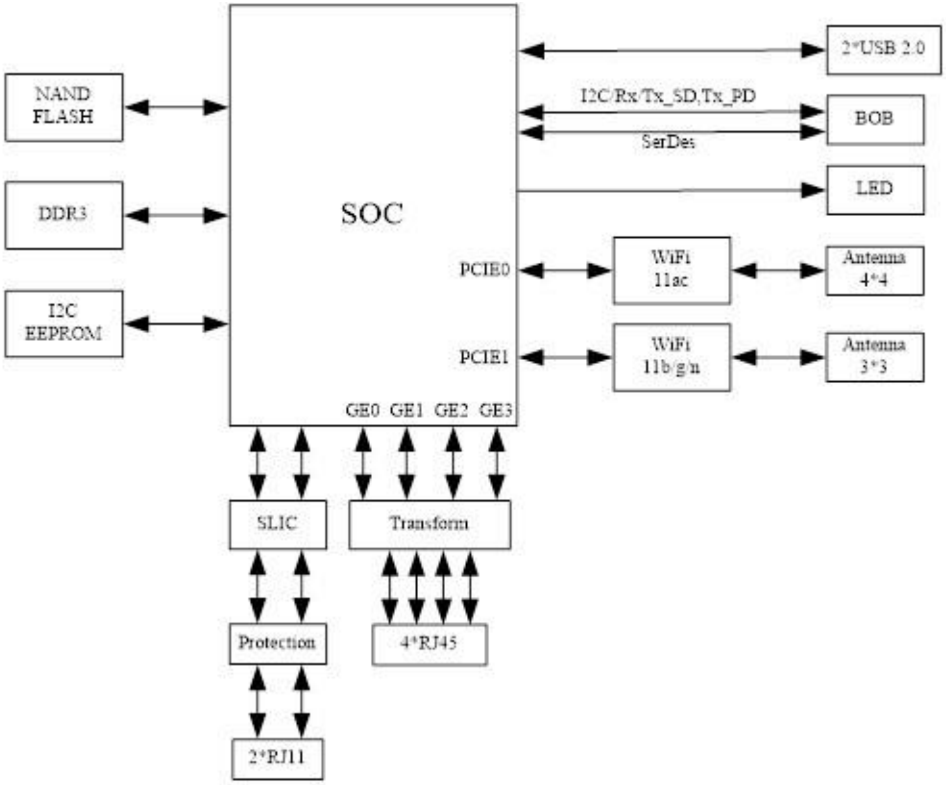
[1] A 5 second polling window limitation exists on the ONT, therefore the margin of error for each 15-min window is 5 seconds

5.9 G-240W-J functional blocks

G-240W-J 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 WLAN button. In addition to the Wi-Fi service, these ONTs transmit Ethernet packets to four RJ-45 Ethernet ports and voice traffic to two RJ-11 POTS ports. These ONTs also feature fiber optic, two USB ports, and power connectors.

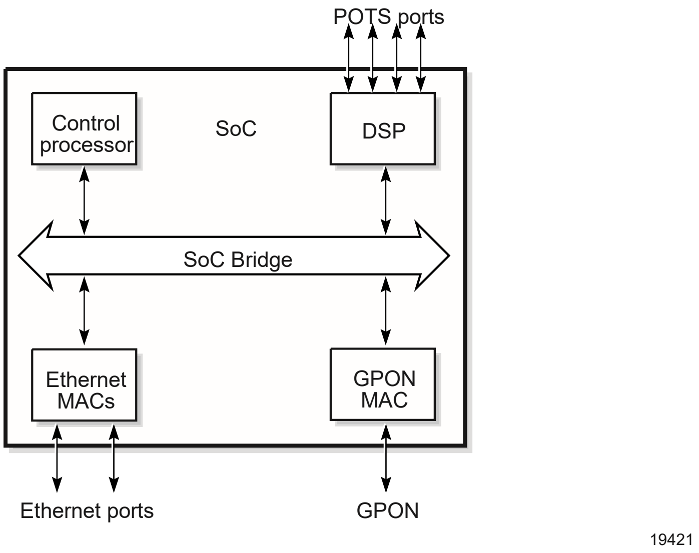
Figure 14 shows the functional blocks for G-240W-J indoor ONT.

Figure 14 **Single-residence Wi-Fi ONT with Gigabit Ethernet and POTS and without RF video**



ONT SoC technology serves as the main hardware block for these ONTs; see Figure 15.

Figure 15 **G-240W-J ONT hardware block**



ONT SoC technology consists of five key elements:

- GPON MAC
  The Gigabit Passive Optical Network Media Access Control (GPON MAC) element on the SoC terminates the GPON interface using an optical diplexer. This interface supports GPON as described in G.984.3 (GPON TC Layer) ITU specification.
- Ethernet MAC
  The SoC provides up to four GE MACs.
- DSP interface
  The Digital Signal Processor (DSP) provides voice processing for 2 POTS lines with 3-way calling. The DSP has a dedicated 64 kbyte instruction cache and shares a 32 kbyte data cache with the Control Processor. It provides up to 4 network processor cores, each at 800MHz.
- Control Processor
  The Control Processor features an integral memory management unit that supports a dedicated 64 kbyte instruction cache and shares a single 32 kbyte data cache with the DSP. The Control Processor and DSP also include a single channel Data Management Application (DMA) controller with a 4 kbyte read ahead low-latency Dynamic Random Access Memory (DRAM) access port.
- Switch matrix
  The Switch matrix provides an integrated data channel between the four GE MACs, the GPON MAC, the DSP, the control processor, and the other integrated elements such as flash memory, DRAM, and the local bus controller.

These ONTs can also interact with additional hardware components to support functionality not provided by the SoC technology.

5.10 G-240W-J standards compliance

G-240W-J indoor ONTs are compliant with the following standards:

- 802.1p marking and VLAN based pbit is supported
- EN 300 328 v2.1.1 wide band data transmission standards for 2.4 GHz bands
- EN 301 893 v2.1.1 5 GHz RLAN: Harmonized Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU
- G.711 support for FAX and modem connection
- G.984 support GPON interface (framing)
- G.984.2 support for Amd1, class B+
- 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 FEC in both upstream and downstream directions
- G.984.3 support for multicast using a single GEM Port-ID for all video traffic
- G984.4 and G.983.2 support for ONT management and provisioning
- CE marking for European standards for health, safety, and environmental protection
- FCC marking for US standards for health, safety, and environmental protection

5.10.1 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the G-240W-J 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-240W-J ONTS qualify as equipment with high network availability (HiNA) functionality. Since the main purpose of G-240W-J 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 “G-240W-J interfaces and interface capacity” in this chapter.

For information about power consumption, see “G-240W-J detailed specifications” in this chapter.

5.10.2 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.

5.10.3 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 23 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and consider removing the no-collocation statement.

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

1 this device may not cause harmful interference, and

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

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

5.11 G-240W-J special considerations

G-240W-J is a package P ONT.

5.11.1 Wi-Fi service

G-240W-J indoor ONTs feature Wi-Fi service as well as voice and data services. Wi-Fi 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.

5.11.1.1 Wi-Fi physical features

G-240W-J indoor ONTs have the following physical features that assist in providing Wi-Fi service:

- WLAN button for enabling and disabling Wi-Fi service
- 7 internal antennas: 3 for 2.4GHz and 4 for 5GHz
- one Wi-Fi Protected Setup (WPS) push button for both 2.4GHz and 5GHz controlling

5.11.1.2 Wi-Fi standards and certifications

The Wi-Fi service on G-240W-J indoor ONTs supports the following IEEE standards and Wi-Fi Alliance certifications:

- certified for IEEE 802.11ac/b/g/n/standards
- WPA support including WPA-PSK
- certified for WPA2-Personal and WPA2-Enterprise

5.11.1.3 Wi-Fi GUI features

G-240W-J indoor ONTs have HTML-based Wi-Fi configuration GUIs.

5.11.2 G-240W-J ONT considerations and limitations

Table 17 lists the considerations and limitations for Package P G-240W-J ONTs.

Table 17 **G-240W-J 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.

(1 of 2)

Considerations and limitations
Some voice features are configurable on a per ONT basis, including Call Waiting, Call Hold, 3-Way Calling, and Call Transfer.
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: CCW, Call Hold and Warmline

(2 of 2)

6 Install a G-240W-J indoor ONT

6.1 Purpose

This chapter provides the steps to install a G-240W-J indoor ONT.

6.2 General

The steps listed in this chapter describe mounting and cabling for G-240W-J indoor ONTs.

6.3 Prerequisites

You need the following items before beginning the installation:

- all required cables

6.4 Recommended tools

You need the following tools for the installation:

- #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

6.5 Safety information

Read the following safety information before installing the unit.

Danger 1 — 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.

Danger 2 — 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.

Danger 3 — Always contact the local utility company before connecting the enclosure to the utilities.

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

Caution — Keep indoor ONTs out of direct sunlight. Prolonged exposure to direct sunlight can damage the unit.

Note 1 — Observe the local and national laws and regulations that may be applicable to this installation.

Note 2 — 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 precedent 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 G-240W-J unit data sheet for the temperature ranges for these ONTs.

6.6 Procedure

Use this procedure to install a G-240W-J indoor ONT.

1 Place the indoor ONT unit:

a On a flat surface, such as a desk; go to step 3.

Note — The G-240W-J 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

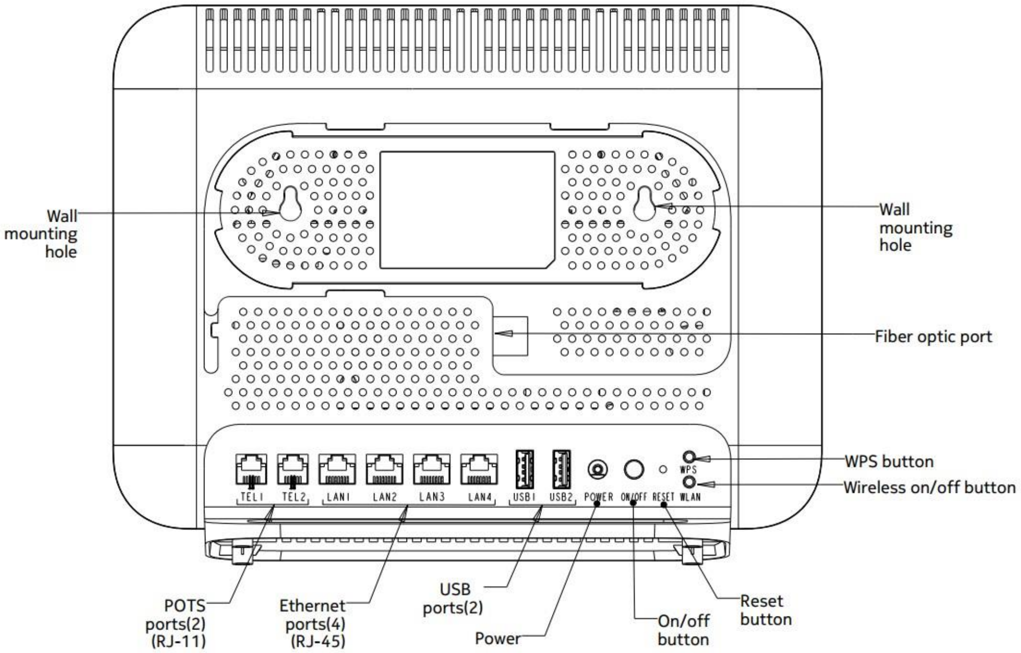
b On a wall; go to step [2].

[2] Mount the G-240W-J indoor ONT to a wall.

The G-240W-J indoor ONT must be mounted in a horizontal position, as indicated by the wall mounting key holes in Figure 16.

Figure 16 shows the ONT with the connections and the key mounting holes.

Figure 16 **G-240W-J ONT with connections and key mounting holes**



i Attach the wall mounting keyholes on the ONT.

ii Drill two holes into the wall where the ONT will be mounted. If possible, mount the ONT on a wall stud.

Do not drive the screw into the wall completely. Leave approximately 1/8 in. (6 mm) between the screw head and the wall surface.

iii Drive the mounting screws into the holes.

The recommended length of the mounting screw is 1.15 in. (3.8 cm).

iv Slide the wall mount keyholes on the ONT enclosure down over the mounting screws until the ONT is securely seated.

---

3 Review the connection locations, as shown in Figure 16.

---

4 Connect the Ethernet cables to the RJ-45 ports; see Figure 16 for the location of the RJ-45 ports.

---

5 Route the POTS cables directly to the RJ-11 ports as per local practices.

The POTS port to the left is labeled 1 for Line 1 while the port on the right is labeled 2 for Line 2, as shown in Figure 16.

6 Connect the fiber optic cable with SC/APC adapter into the SC/APC connector; see Figure 16 for the location of the SC/APC connector.

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

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

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.

7 Install the power supply according to manufacturer specifications.

Note — Observe the following:

- Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 12 VDC, 3 A.

8 Connect the power cable to the power connector.

9 Power up the ONT unit by using the power switch.

10 If used, enable the Wi-Fi service.

i Locate the WLAN button; see Figure 16 for the location of the WLAN button. **ii**

Press the WLAN button to change the status of the Wi-Fi service.

11 If used, enable the WPS.

i Locate the WPS button; see Figure 16 for the location of the WPS button. **ii**

Press the WPS button to change the status of the WPS.

12 Verify the ONT LEDs, voltage status, and optical signal levels; see the *7368 Hardware and Cabling Installation Guide*.

13 Activate and test the services; see the *7368 Hardware and Cabling Installation Guide*.

14 If used, configure the SLID; see the *7368 ISAM ONT Configuration, Management, and Troubleshooting Guide*.

15 If necessary, reset the ONT.

i Locate the Reset button; see Figure [3].

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

[3] STOP. This procedure is complete.

7 Replace a G-240W-J indoor ONT

7.1 Purpose

This chapter provides the steps to replace G-240W-J indoor ONTs.

7.2 General

The steps listed in this chapter describe mounting and cabling for G-240W-J indoor ONTs.

7.3 Prerequisites

You need the following items before beginning the installation:

- all required cables

7.4 Recommended tools

You need the following tools for replacing the ONT:

- #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

7.5 Safety information

Read the following safety information before replacing the unit.

Danger 1 — 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.

Danger 2 — 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.

Danger 3 — Always contact the local utility company before connecting the enclosure to the utilities.

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

Caution — Keep indoor ONTs out of direct sunlight. Prolonged exposure to direct sunlight can damage the unit.

Note 1 — Observe the local and national laws and regulations that may be applicable to this installation.

Note 2 — 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 precedent 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 G-240W-J unit data sheet for the ONT temperature ranges for these ONTs.

7.6 Procedure

Use this procedure to replace a G-240W-J 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).

i 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;
```

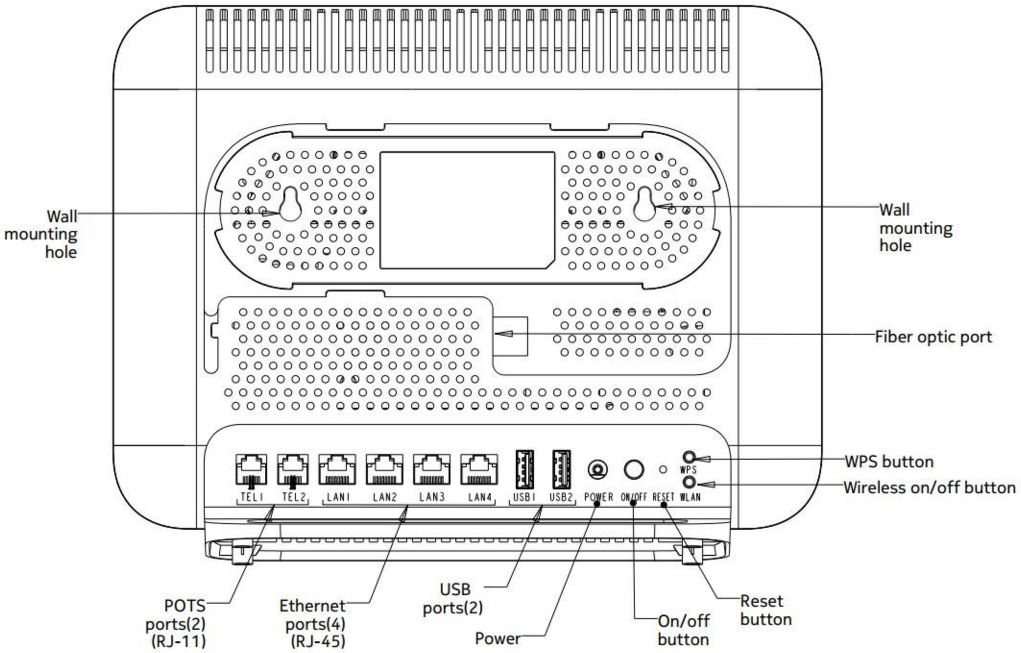
ii If the ONT is in service, place the ONT in OOS state.

Example:

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

2 If used, disable the Wi-Fi service by pressing the WLAN button; see Figure 17 for the location of the WLAN button.

Figure 17 **G-240W-J indoor ONT connections**


Wall mounting hole
Wall mounting hole
Fiber optic port
WPS button
Wireless on/off button
TEL1
TEL2
LAN1
LAN2
LAN3
LAN4
USB1
USB2
POWER
ON/OFF
RESET
WPS
WLAN
POTS ports(2) (RJ-11)
Ethernet ports(4) (RJ-45)
USB ports(2)
Power
On/off button
Reset button

3 Power down the unit by using the on/off power switch; see Figure 17 for the location of the power switch.

4 Disconnect the POTS, Ethernet, and power cables from the ONT; see Figure 17 for the connector locations on the G-240W-J indoor ONT.

5 Disconnect the fiber optic cable.

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

i Unplug the fiber optic cable with SC/APC connector from the ONT; see Figure 17 for the location of the fiber optic port.

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

6 Replace the ONT with a new unit:

a On a flat surface, such as a desk, substitute the new ONT for the old ONT, horizontally resting on its four feet.

b On a wall.

i Slide the old ONT off of the mounting screws until the ONT is free of the wall.

ii Slide the wall mount holes onto the ONT enclosure over the mounting screws until it is securely seated.

7 Connect the Ethernet cables directly to the RJ-45 ports; see Figure 17 for the location of the RJ-45 ports.

8 Connect the POTS cables directly to the RJ-11 ports as per local practices; see Figure 17 for the location of the RJ-11 ports.

The RJ-11 port to the left is labeled 1 for Line 1 while the port on the right is labeled 2 for Line 2.

9 If required, have approved service personnel who are trained to work with optic fiber clean the fiber optic connection. See the *7368 ISAM ONT Configuration, Management, and Troubleshooting Guide* for more information about fiber optic handling, inspection, and cleaning.

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

10 Connect the fiber optic cable with SC/APC adapter into the SC/APC connector. Figure 17 shows the location of the SC/APC connector.

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

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

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 Install the power supply according to manufacturer specifications.

Note — Observe the following:

- Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 12 VDC, 3 A.

12 Connect the power cable to the power connector.

13 Power up the unit by using the power switch.

14 If used, enable the Wi-Fi service by pressing the WLAN button; see Figure 17 for the location of the WLAN button.

15 If used, enable the WPS by pressing the WPS button; see Figure 17 for the location of the WPS button.

16 If used, configure the SLID; see the *7368 ISAM ONT 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.

17 Verify the ONT LEDs, voltage status, and optical signal levels; see the *7368 Hardware and Cabling Installation Guide*.

18 Activate and test the services; see the *7368 Hardware and Cabling Installation Guide*.

19 If necessary, reset the ONT.

i Locate the Reset button; see Figure 17.

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

20 STOP. This procedure is complete.

8 Configure a G-240W-J indoor ONT

8.1 General

Please refer to the configuration information provided with your OLT for the software configuration procedure for a G-240W-J ONT.

For HTTP configuration procedures, please refer to the *7368 ISAM ONT Configuration, Management, and Troubleshooting Guide*.

8.2 HGU mode GUI configuration

Use the procedures below to use the web-based GUI for the G-240W-J 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.

8.2.1 Login

Use the procedure below to login to the web-based GUI for the G-240W-J.

Procedure 6 Login to web-based GUI

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

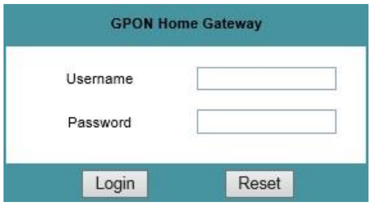
The login window appears.

The default gateway IP address is http://192.168.1.254. You can connect to this IP address using your web browser after connecting your PC to one of Ethernet ports of the ONT. The static IP address of your PC must be in the same 192.168.1.x subnet as the ONT.

2 Enter your username and password in the Log in window, as shown in Figure 18.

The default user name is userAdmin. The default password is a random number, which is included in the ONT kit.

Figure 18 **Web login window**



Caution — 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.

Note — If you forget the current username and password, press the reset button for 5 s and the default values for the username and password will be recovered at startup.

3 Click Login. The Device Information screen appears.

Note — To help protect the security of your Internet connection, the application displays a pop-up reminder to change both the Wi-Fi 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.

4 STOP. This procedure is complete.

8.2.2 Device and connection status

G-240W-J ONTs support the retrieval of a variety of device and connection information, including:

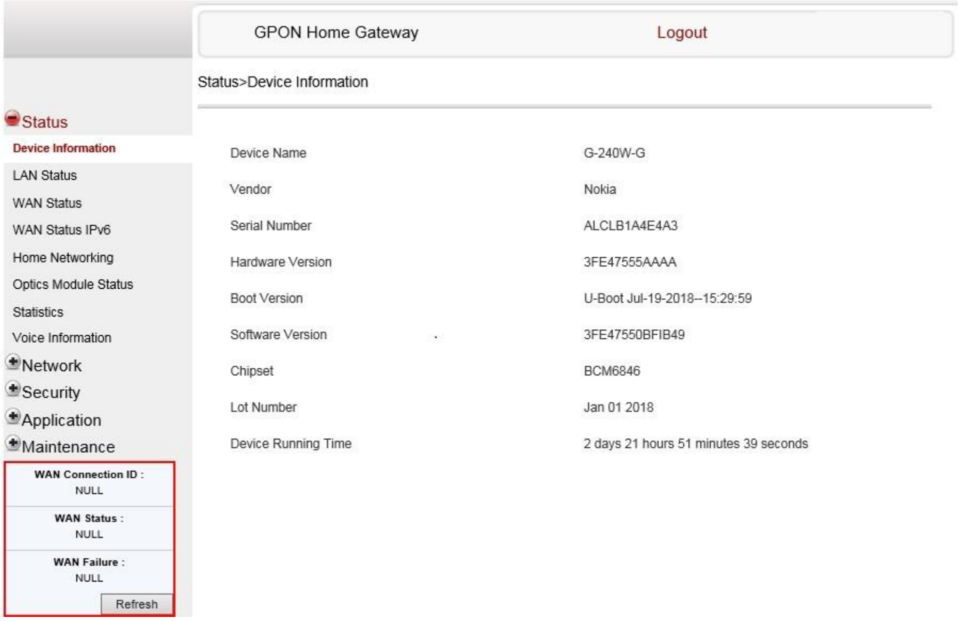
- device information
- LAN status
- WAN status

- WAN status IPv6
- Home networking information
- optics module status
- statistics retrieval
- voice information

Procedure 7 Device information retrieval

1 Select Status > Device Information from the top-level menu in the GPON Home Gateway window, as shown in Figure 19.

Figure 19 **Device Information window**



Device Name	G-240W-G
Vendor	Nokia
Serial Number	ALCLB1A4E4A3
Hardware Version	3FE47555AAAA
Boot Version	U-Boot Jul-19-2018--15:29:59
Software Version	3FE47550BFIB49
Chipset	BCM6846
Lot Number	Jan 01 2018
Device Running Time	2 days 21 hours 51 minutes 39 seconds

WAN Connection ID :
NULL

WAN Status :
NULL

WAN Failure :
NULL

Note — Upon login, the GPON Home Gateway window displays the WAN status block on the bottom left part of each window. This block shows the WAN connection ID, the WAN status, and any WAN errors.

This block is accurate upon login, but it is static; click the Refresh button to update the information.

Table 18 describes the fields in the Device Information window.

Table 18 **Device Information parameters**

Field	Description

Field	Description
Device Name	Name on the ONT
Vendor	Name of the vendor
Serial Number	Serial number of the ONT
Hardware version	Hardware version of the ONT
Boot version	Boot version of the ONT
Software version	Software version of the ONT
Chipset	Chipset of the ONT
Lot Number	Production date of the ONT
Device Running Time	Amount of time the device has run since last reset in hours, minutes, and seconds

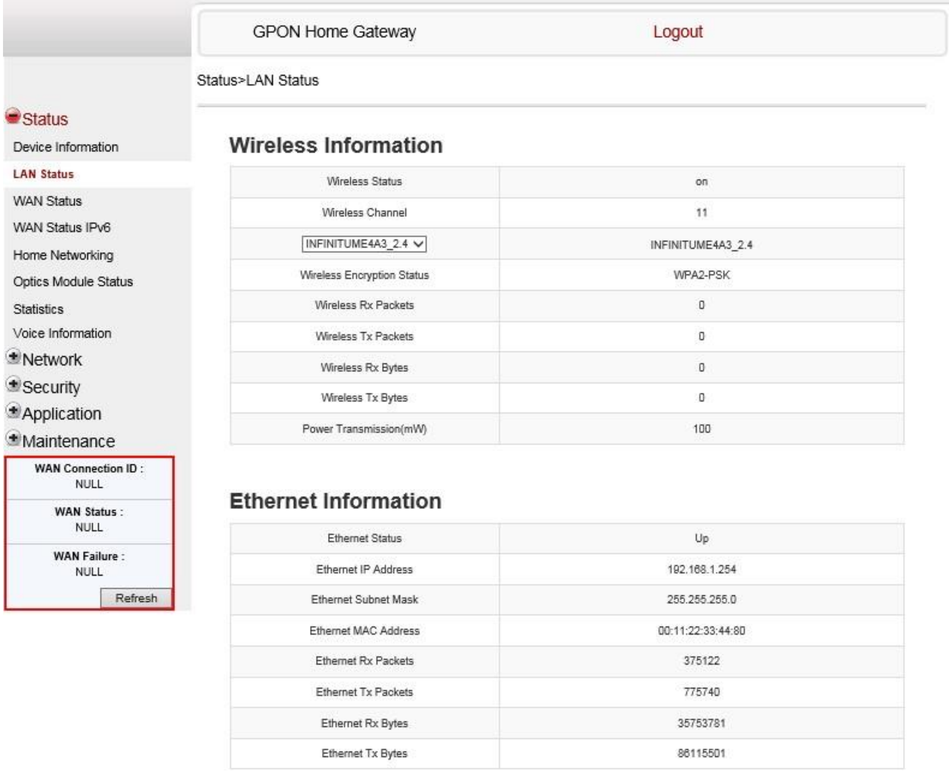
2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

Procedure 8 LAN status retrieval

1 Select Status > LAN Status from the top-level menu in the GPON Home Gateway window, as shown in Figure 20.

Figure 20 **LAN status window**



Status>LAN Status

WAN Connection ID : NULL

WAN Status : NULL

WAN Failure : NULL

Wireless Information

Wireless Status	on
Wireless Channel	11
INFINITUME4A3_2.4	INFINITUME4A3_2.4
Wireless Encryption Status	WPA2-PSK
Wireless Rx Packets	0
Wireless Tx Packets	0
Wireless Rx Bytes	0
Wireless Tx Bytes	0
Power Transmission(mW)	100

Ethernet Information

Ethernet Status	Up
Ethernet IP Address	192.168.1.254
Ethernet Subnet Mask	255.255.255.0
Ethernet MAC Address	00:11:22:33:44:80
Ethernet Rx Packets	375122
Ethernet Tx Packets	775740
Ethernet Rx Bytes	35753781
Ethernet Tx Bytes	86115501

Table 19 describes the fields in the LAN status window.

Table 19 **LAN status parameters**

Field	Description
Wireless Information	
Wireless Status	Indicates whether the wireless is on or off
Wireless Channel	Wireless channel number
SSID Name	Name of each SSID
Wireless Encryption Status	Encryption type used on the wireless connection
Wireless Rx Packets	Number of packets received on the wireless connection

Field	Description
Wireless Tx Packets	Number of packets transmitted on the wireless connection
Wireless Rx Bytes	Number of bytes received on the wireless connection
Wireless Tx Bytes	Number of bytes transmitted on the wireless connection
Power Transmission (mW)	Power of the wireless transmission, in mW
Ethernet Information	
Ethernet Status	Indicates whether the Ethernet connection is on or off
Ethernet IP Address	IP address of the Ethernet connection
Ethernet Subnet Mask	Subnet Mask of the Ethernet connection
Ethernet MAC Address	MAC address of the Ethernet connection
Ethernet Rx Packets	Number of packets received on the Ethernet connection
Ethernet Tx Packets	Number of packets transmitted on the Ethernet connection
Ethernet Rx Bytes	Number of bytes received on the Ethernet connection
Ethernet Tx Bytes	Number of bytes transmitted on the Ethernet connection

(2 of 2)

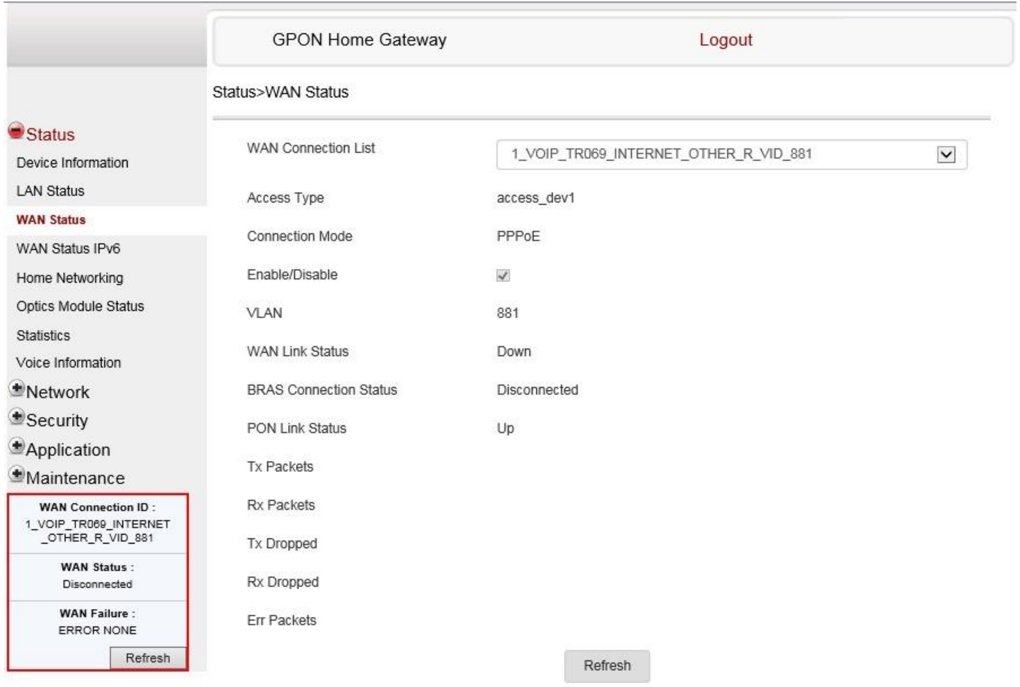
2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

Procedure 9 WAN status retrieval

1 Select Status > WAN Status from the top-level menu in the GPON Home Gateway window, as shown in Figure 21.

Figure 21 **WAN status window**



WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

WAN Connection List	1_VOIP_TR069_INTERNET_OTHER_R_VID_881
Access Type	access_dev1
Connection Mode	PPPoE
Enable/Disable	☑
VLAN	881
WAN Link Status	Down
BRAS Connection Status	Disconnected
PON Link Status	Up
Tx Packets	
Rx Packets	
Tx Dropped	
Rx Dropped	
Err Packets	

Table 20 describes the fields in the WAN status window.

Table 20 **WAN status parameters**

Field	Description
WAN connection list	Drop-down menu listing all WAN connections. The connection shown is the connection for which WAN status will be shown.
Connection Mode	Connection mode of the WAN connection
Enable/Disable	Select this checkbox to enable the WAN connection
VLAN	VLAN ID
WAN Link Status	Whether the WAN link is up or down
BRAS Connection Status	Whether the BRAS connection is connecting or disconnected
PON Link Status	Whether the PON link is up or down
Tx Packets	Number of packets transmitted on the WAN connection
Rx Packets	Number of packets received on the WAN connection

(1 of 2)

Tx Dropped	Number of packets dropped on the transmit WAN connection
Rx Dropped	Number of packets dropped on the receive WAN connection
Err Packets	Number of errored packets on the WAN connection

(2 of 2)

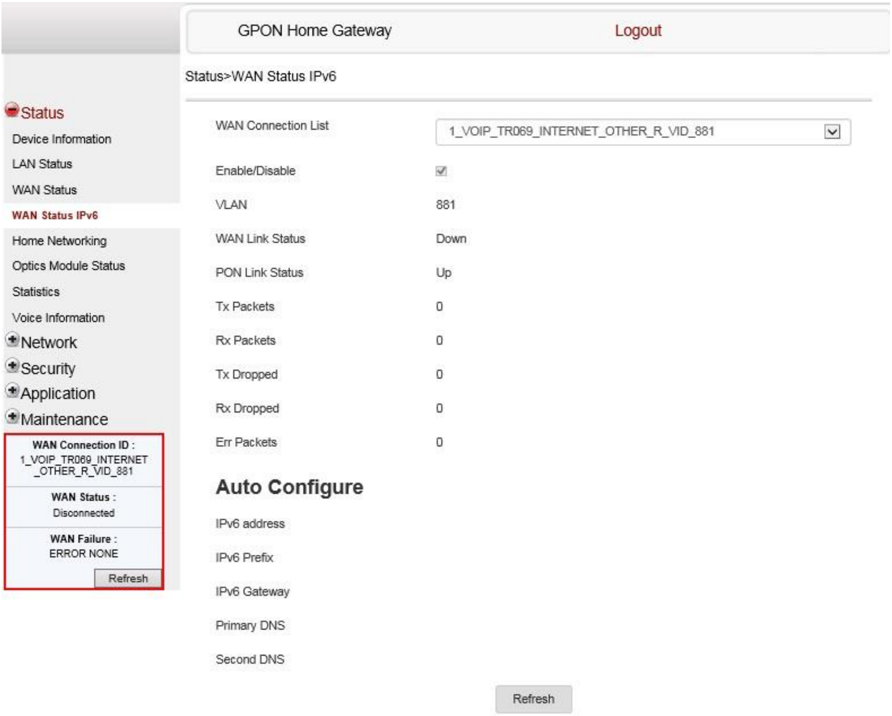
2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

Procedure 10 WAN status IPv6 retrieval

1 Select Status > WAN Status IPv6 from the top-level menu in the GPON Home Gateway window, as shown in Figure 22.

Figure 22 **WAN status IPv6 window**



WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

WAN Connection List	1_VOIP_TR069_INTERNET_OTHER_R_VID_881
Enable/Disable	☑
VLAN	881
WAN Link Status	Down
PON Link Status	Up
Tx Packets	0
Rx Packets	0
Tx Dropped	0
Rx Dropped	0
Err Packets	0

Auto Configure

IPv6 address	
IPv6 Prefix	
IPv6 Gateway	
Primary DNS	
Second DNS	

Table 21 describes the fields in the WAN status IPv6 window.

Table 21 **WAN status IPv6 parameters**

Field	Description
WAN connection list	Drop-down menu listing all WAN connections. The connection shown is the connection for which WAN status will be shown.
Enable/Disable	Select this checkbox to enable the WAN connection
VLAN	VLAN ID
WAN Link Status	Whether the WAN link is up or down
PON Link Status	Whether the PON link is up or down
Tx Packets	Number of packets transmitted on the WAN connection
Rx Packets	Number of packets received on the WAN connection
Tx Dropped	Number of packets dropped on the transmit WAN connection
Rx Dropped	Number of packets dropped on the receive WAN connection
Err Packets	Number of errored packets on the WAN connection
Auto Configure	
IPv6 address	IPv6 address that identifies the device and its location
IPv6 Prefix	IPv6 prefix
IPv6 Gateway	IPv6 gateway address
Netmask	Network mask
Gateway	Gateway address
Primary DNS	Primary Domain Name Server
Second DNS	Secondary Domain Name Server

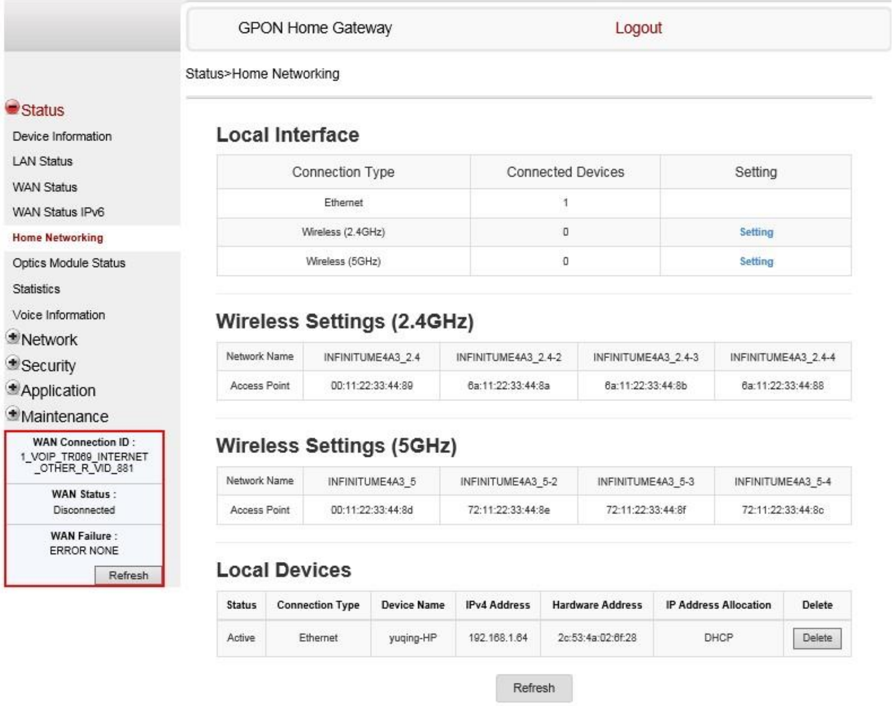
2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

Procedure 11 Home networking information retrieval

1 Select Status > Home Networking from the top-level menu in the GPON Home Gateway window, as shown in Figure 23.

Figure 23 Home networking information window



WAN Connection ID :
1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Local Interface

Connection Type	Connected Devices	Setting
Ethernet	1	
Wireless (2.4GHz)	0	Setting
Wireless (5GHz)	0	Setting

Wireless Settings (2.4GHz)

Network Name	INFINITUME4A3_2.4	INFINITUME4A3_2.4-2	INFINITUME4A3_2.4-3	INFINITUME4A3_2.4-4
Access Point	00:11:22:33:44:89	6a:11:22:33:44:8a	6a:11:22:33:44:8b	6a:11:22:33:44:88

Wireless Settings (5GHz)

Network Name	INFINITUME4A3_5	INFINITUME4A3_5-2	INFINITUME4A3_5-3	INFINITUME4A3_5-4
Access Point	00:11:22:33:44:8d	72:11:22:33:44:8e	72:11:22:33:44:8f	72:11:22:33:44:8c

Local Devices

Status	Connection Type	Device Name	IPv4 Address	Hardware Address	IP Address Allocation	Delete
Active	Ethernet	yuqing-HP	192.168.1.64	2c:53:4a:02:6f:28	DHCP	Delete

Table 22 describes the fields in the Home networking window.

Table 22 Home networking parameters

Field	Description
Local Interface	
Ethernet	Table displays the number of Ethernet connections and their settings
Wireless (2.4GHz)	Table displays the number of wireless connections and their settings
Wireless (5GHz)	
Wireless Settings (2.4GHz)	
Network Name	Name of the wireless network
Access Point	Hexadecimal address of the wireless access point
Wireless Settings (5GHz)	
Network Name	Name of the wireless network

(1 of 2)

Access Point	Hexadecimal address of the wireless access point
Local Devices	
Table entry	Each entry indicates the status (active or inactive), connection type, device name, IP address, hardware address, and IP address allocation of each connected local device.

(2 of 2)

2 Click Delete to delete a particular local device connection.

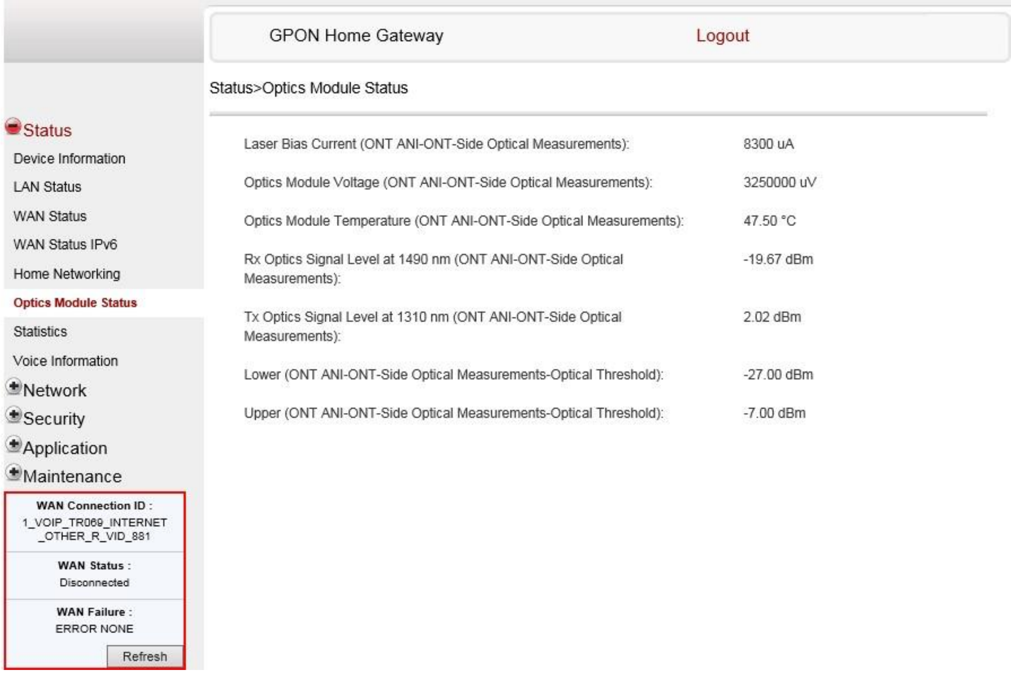
3 Click Refresh to update the displayed information.

4 STOP. This procedure is complete.

Procedure 12 Optics module status retrieval

1 Select Status > Optics Module Status from the top-level menu in the GPON Home Gateway window, as shown in Figure 24.

Figure 24 Optics module status window



Status>Optics Module Status

Laser Bias Current (ONT ANI-ONT-Side Optical Measurements):	8300 uA
Optics Module Voltage (ONT ANI-ONT-Side Optical Measurements):	3250000 uV
Optics Module Temperature (ONT ANI-ONT-Side Optical Measurements):	47.50 °C
Rx Optics Signal Level at 1490 nm (ONT ANI-ONT-Side Optical Measurements):	-19.67 dBm
Tx Optics Signal Level at 1310 nm (ONT ANI-ONT-Side Optical Measurements):	2.02 dBm
Lower (ONT ANI-ONT-Side Optical Measurements-Optical Threshold):	-27.00 dBm
Upper (ONT ANI-ONT-Side Optical Measurements-Optical Threshold):	-7.00 dBm

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 23 describes the fields in the Optics module status window.

Table 23 **Optics module status parameters**

Field	Description
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
Tx 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 Measurements-Optical Threshold)	Lower optical threshold, measured in dBm
Upper (ONT ANI-ONT-Side Optical Measurements-Optical Threshold)	Upper optical threshold, measured in dBm

2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

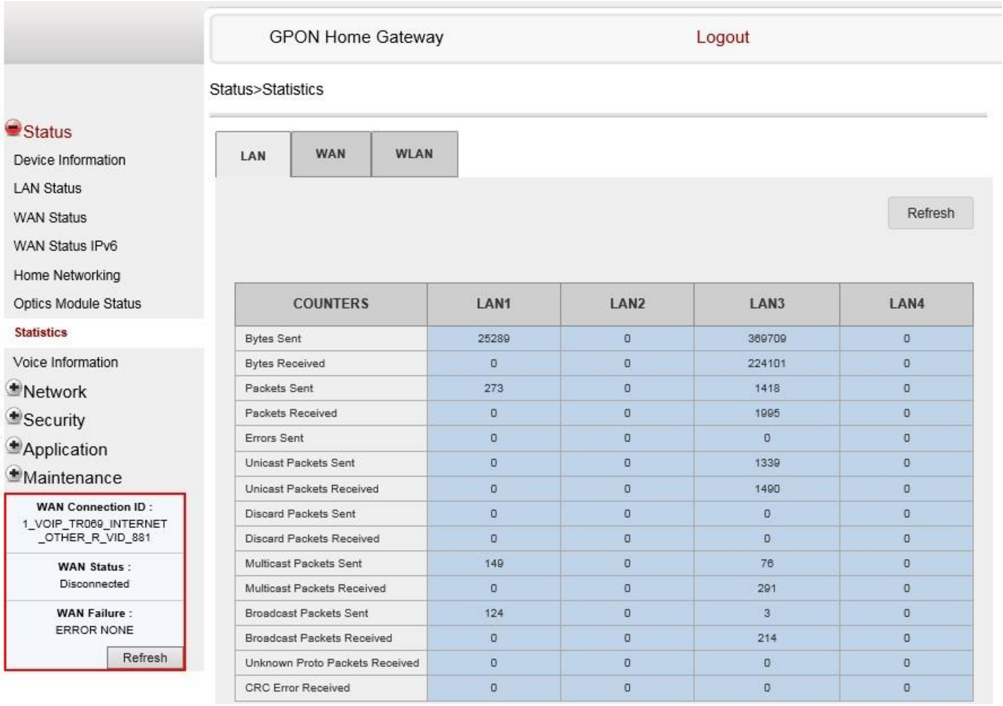
Procedure 13 Statistics retrieval

1 Select Status > Statistics from the top-level menu in the GPON Home Gateway window.

Statistics are available for LAN ports, WAN ports, and WLAN ports.

Figure 25 shows the statistics for the LAN ports.

Figure 25 **LAN ports Statistics window**



WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

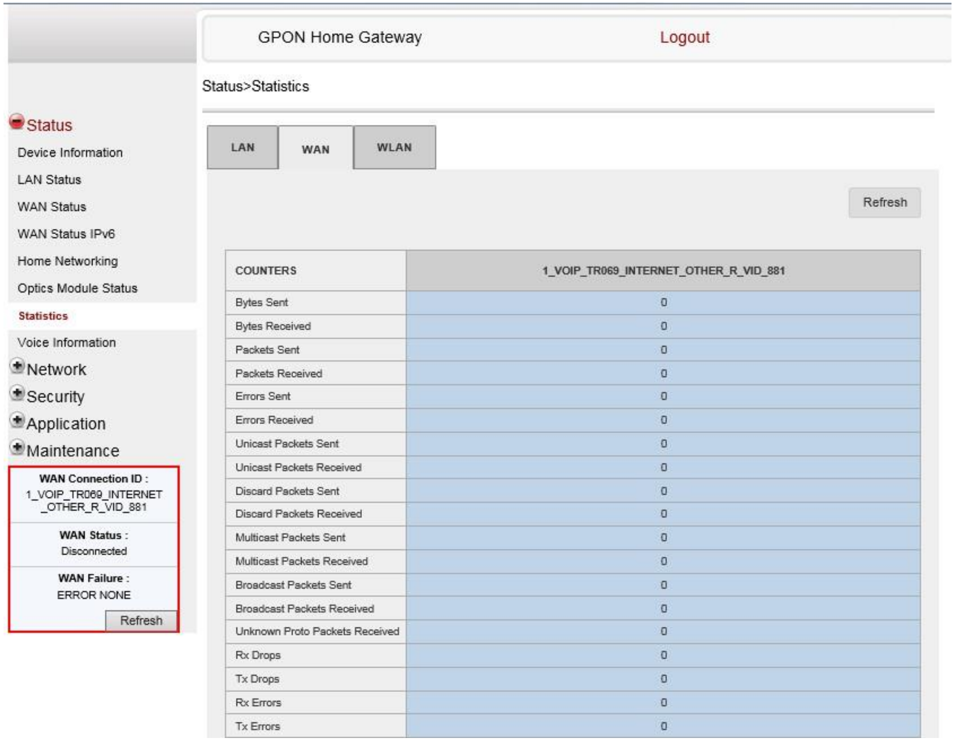
WAN Failure : ERROR NONE

Refresh

COUNTERS	LAN1	LAN2	LAN3	LAN4
Bytes Sent	25289	0	369709	0
Bytes Received	0	0	224101	0
Packets Sent	273	0	1418	0
Packets Received	0	0	1995	0
Errors Sent	0	0	0	0
Unicast Packets Sent	0	0	1339	0
Unicast Packets Received	0	0	1490	0
Discard Packets Sent	0	0	0	0
Discard Packets Received	0	0	0	0
Multicast Packets Sent	149	0	76	0
Multicast Packets Received	0	0	291	0
Broadcast Packets Sent	124	0	3	0
Broadcast Packets Received	0	0	214	0
Unknown Proto Packets Received	0	0	0	0
CRC Error Received	0	0	0	0

Figure 26 shows the statistics for the WAN ports.

Figure 26 WAN ports statistics window



WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

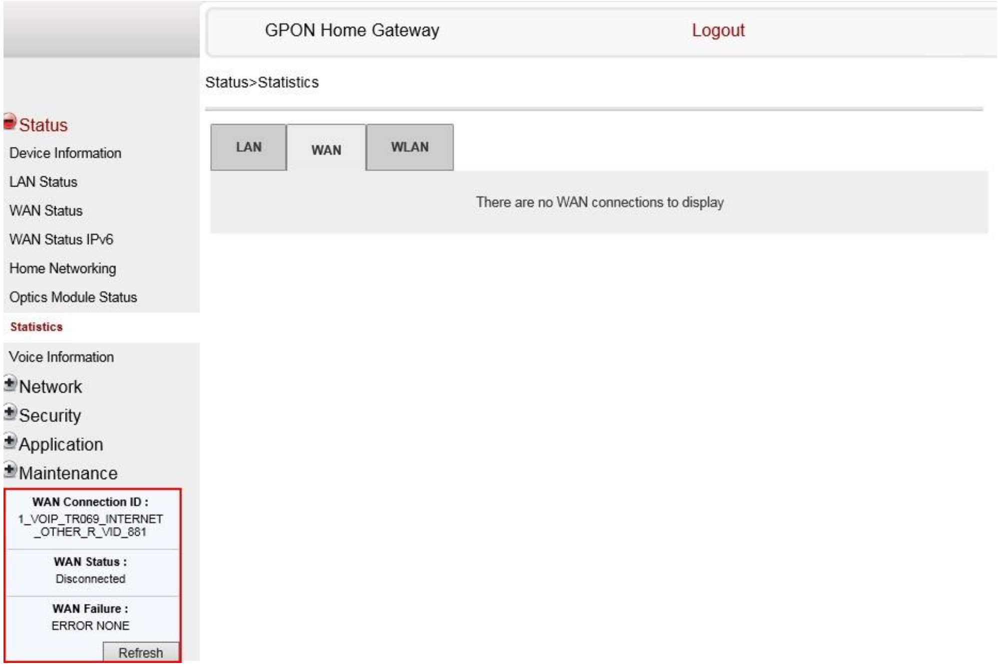
WAN Failure : ERROR NONE

Refresh

COUNTERS	1_VOIP_TR069_INTERNET_OTHER_R_VID_881
Bytes Sent	0
Bytes Received	0
Packets Sent	0
Packets Received	0
Errors Sent	0
Errors Received	0
Unicast Packets Sent	0
Unicast Packets Received	0
Discard Packets Sent	0
Discard Packets Received	0
Multicast Packets Sent	0
Multicast Packets Received	0
Broadcast Packets Sent	0
Broadcast Packets Received	0
Unknown Proto Packets Received	0
Rx Drops	0
Tx Drops	0
Rx Errors	0
Tx Errors	0

If there are no WAN connections to display, the system displays a message, as shown in Figure 27.

Figure 27 WAN ports statistics message



There are no WAN connections to display

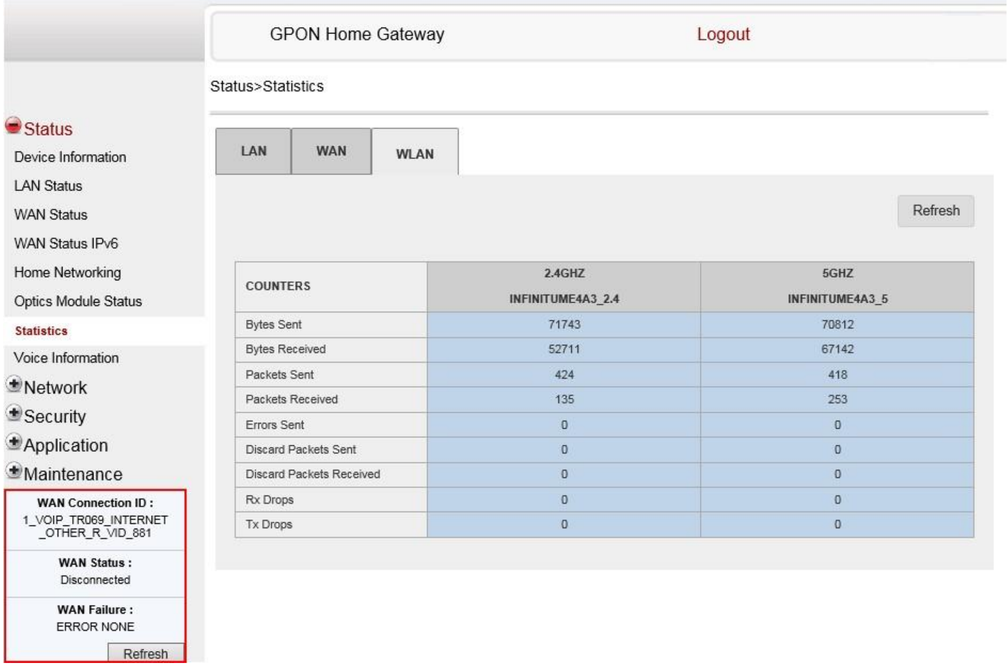
WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Figure 28 shows the statistics for the WLAN ports.

Figure 28 WLAN ports statistics window



COUNTERS	2.4GHZ INFINITUME4A3_2.4	5GHZ INFINITUME4A3_5
Bytes Sent	71743	70812
Bytes Received	52711	67142
Packets Sent	424	418
Packets Received	135	253
Errors Sent	0	0
Discard Packets Sent	0	0
Discard Packets Received	0	0
Rx Drops	0	0
Tx Drops	0	0

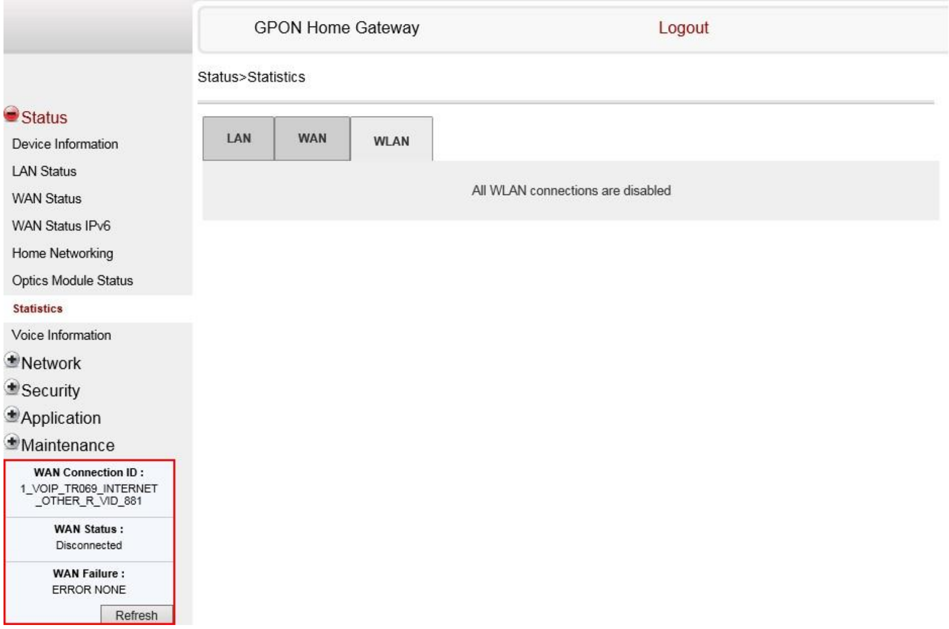
WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

If there are no WLAN connections to display, the system displays a message, as shown in Figure 29.

Figure 29 **WLAN ports statistics message**



All WLAN connections are disabled

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

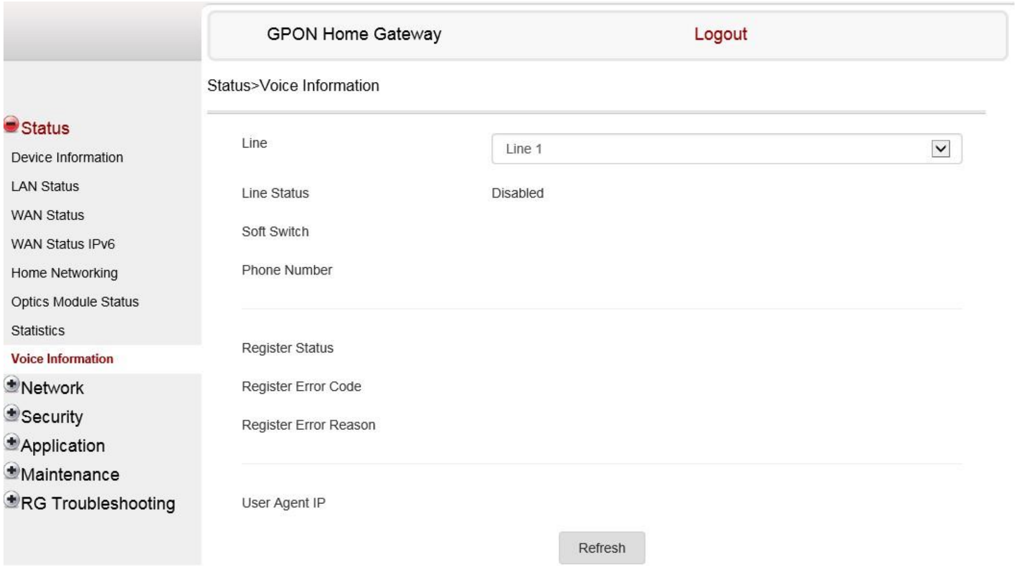
2 STOP. This procedure is complete.

1

Procedure 14 Voice information retrieval

Select Status > Voice Information from the top-level menu in the GPON Home Gateway window, as shown in Figure 30.

Figure 30 **Voice Information window**



Status>Voice Information

Line: Line 1

Line Status: Disabled

Soft Switch

Phone Number

Register Status

Register Error Code

Register Error Reason

User Agent IP

Table 24 describes the fields in the Voice Information window.

Table 24 **Voice Information parameters**

Field	Description
Line	Choose a line from the drop-down menu. The default is Line 1.
Line Status	Depending on the line chosen, the line options are: • Up • Initializing • Registering • Unregistering • Error • Testing • Quiescent • Disabled The default is Disabled

Soft Switch[1]	Proxy IP address; blank if the line is not registered
Phone Number[1]	Phone number configured for a telephone line 1; +13290611266

(1 of 2)

Field	**Description**
Register Status	The default is Registered Blank if no voice service is provisioned
Register Error Code	SIP standard error code for the register status; for example, 401, 403, 503 This field is blank if the register is set to OK
Register Error Reason	SIP standard error reason for the register status This field is blank if the register is set to OK
User Agent IP	IP address of the user agent ExternalIPAddress in WANIPConnection or WANPPPConnection

(2 of 2)

Note

[1] This field is only visible at the adminGPON level; it is not visible at the userAdmin level.

2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

8.2.3 Network configuration

G-240W-J ONTs support network configuration, including:

- LAN
- LAN IPv6
- WAN
- WAN DHCP
- WiFi 2.4G
- WiFi 5G
- Wireless schedule
- Routing

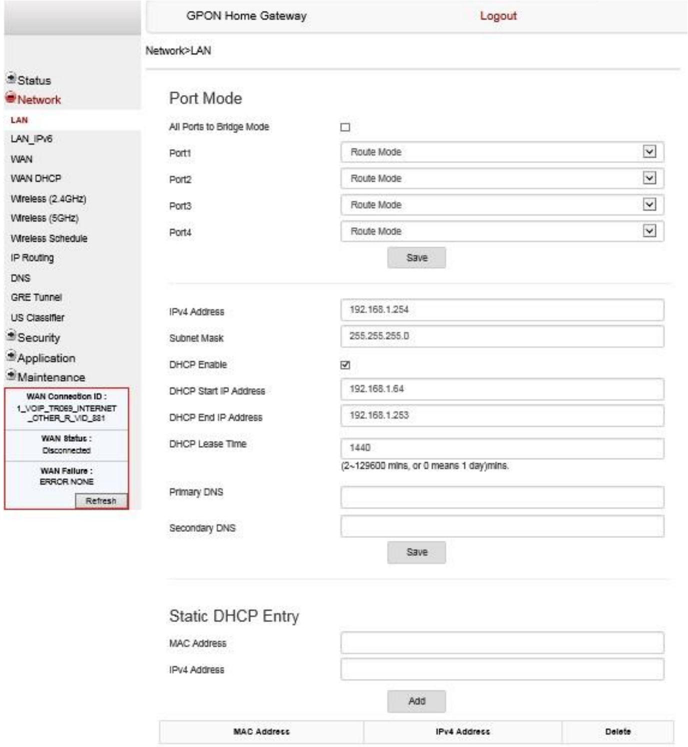
1

- DNS
- TR-069
- GRE tunnel
- QoS
- US (upstream) classification

Procedure 15 LAN networking configuration

Select Network > LAN from the top-level menu in the GPON Home Gateway window, as shown in Figure 31.

Figure 31 LAN network window



Network>LAN

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Port Mode

All Ports to Bridge Mode □

Port1 Route Mode

Port2 Route Mode

Port3 Route Mode

Port4 Route Mode

IPv4 Address 192.168.1.254

Subnet Mask 255.255.255.0

DHCP Enable ☑

DHCP Start IP Address 192.168.1.64

DHCP End IP Address 192.168.1.253

DHCP Lease Time 1440

(2~129600 mins, or 0 means 1 day)mins.

Primary DNS

Secondary DNS

Static DHCP Entry

MAC Address

IPv4 Address

MAC Address	IPv4 Address	Delete

Table 25 describes the fields in the LAN network window.

Table 25 LAN network parameters

Field	Description

Field	Description
Port Mode	
All Ports to Bridge Mode	Select this checkbox to set all ports to Bridge mode
Port 1 - 4	Drop-down port mode for each port: Route mode or Bridge mode
IPv4 Address	IP Address of the ONT
Subnet Mask	Subnet mask of the ONT
DHCP Enable	Select this checkbox to enable DHCP
DHCP Start IP Address	Starting DHCP IP address
DHCP End IP Address	Ending DHCP IP address
DHCP Lease Time	DHCP lease time (in min)
Primary DNS	Primary DNS identifier
Secondary DNS	Secondary DNS identifier
Static DHCP Entry	
MAC Address	MAC address for the static DHCP
IPv4 Address	IPv4 address for the static DHCP

(1 of 2)

(2 of 2)

2 Select the mode for each port.

3 Click Save.

4 Enter the DHCP configuration information.

5 Click Save.

6 Enter the Static DHCP information.

7 Click Add.

You can also use this panel to delete a Static DHCP MAC address or IPv4 address.

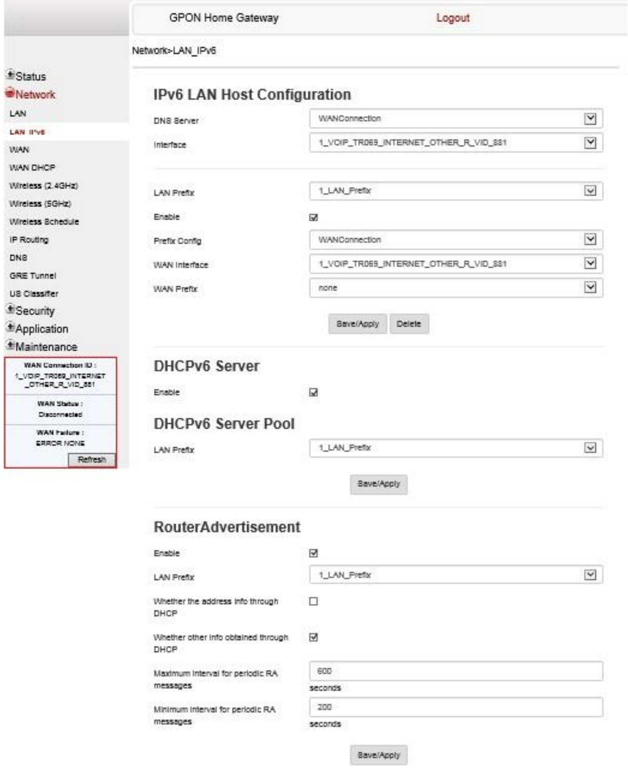
8 STOP. This procedure is complete.

1

Procedure 16 LAN IPv6 networking configuration

Select Network > LAN_IPv6 from the top-level menu in the GPON Home Gateway window, as shown in Figure 32.

Figure 32 LAN IPv6 network window



Network>LAN_IPv6

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881
WAN Status : Disconnected
WAN Failure : ERROR NONE

IPv6 LAN Host Configuration

DNS Server: WANConnection
Interface: 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

LAN Prefix: 1_LAN_Prefix
Enable: ☑
Prefix Config: WANConnection
WAN Interface: 1_VOIP_TR069_INTERNET_OTHER_R_VID_881
WAN Prefix: none

DHCPv6 Server

Enable: ☑

DHCPv6 Server Pool

LAN Prefix: 1_LAN_Prefix

RouterAdvertisement

Enable: ☑
LAN Prefix: 1_LAN_Prefix
Whether the address info through DHCP: □
Whether other info obtained through DHCP: ☑
Maximum interval for periodic RA messages: 600 seconds
Minimum interval for periodic RA messages: 200 seconds

Table 26 describes the fields in the LAN IPv6 network window.

Table 26 LAN IPv6 network parameters

Field	Description
IPv6 LAN Host Configuration	
DNS Server	Choose a DNS server from the drop-down menu.
Interface	This field appears if you selected the Wan Connection option for the “prefix config” field. Choose a WAN connection interface from the drop-down menu.

LAN Prefix	This field appears if you selected the “Static” option for the “prefix config” field. Type a connection.
Enable	Select this checkbox to enable the LAN connection

(1 of 2)

Field	Description
Prefix Config	Choose a prefix config option from the drop-down menu, either WANConnection (prefix will be obtained from the WAN) or Static (enables you to enter the prefix).
WAN Interface	Choose a WAN interface from the drop-down menu
WAN Prefix	Choose a WAN prefix from the drop-down menu
DHCPv6 Server	
Enable	Select this checkbox to enable the DHCPv6 Server connection
DHCPv6 Server Pool	
LAN Prefix	This field appears if you selected the “Static” option for the “prefix config” field. Type a connection.
RouterAdvertisement	
LAN Prefix	This field appears if you selected the “Static” option for the “prefix config” field. Type a connection.
Whether the address info through DCHP	Select this checkbox to enable address information retrieval through DHCP.
Whether other info obtained through DHCP	Select this checkbox to enable retrieval of other information through DHCP.
Maximum interval for periodic RA messages	Enter the maximum interval (in seconds) for periodic Router Advertisement messages. The interval range is from 4 to 1800.
Minimum interval for periodic RA messages	Enter the minimum interval (in seconds) for periodic Router Advertisement messages. The interval range is from 4 to 1800.

(2 of 2)

2 Choose a DNS server, prefix config, and interface.

3 Select or enter the DHCP configuration information.

4 Enter the maximum and minimum intervals for RA messages.

5 Click Save/Apply.

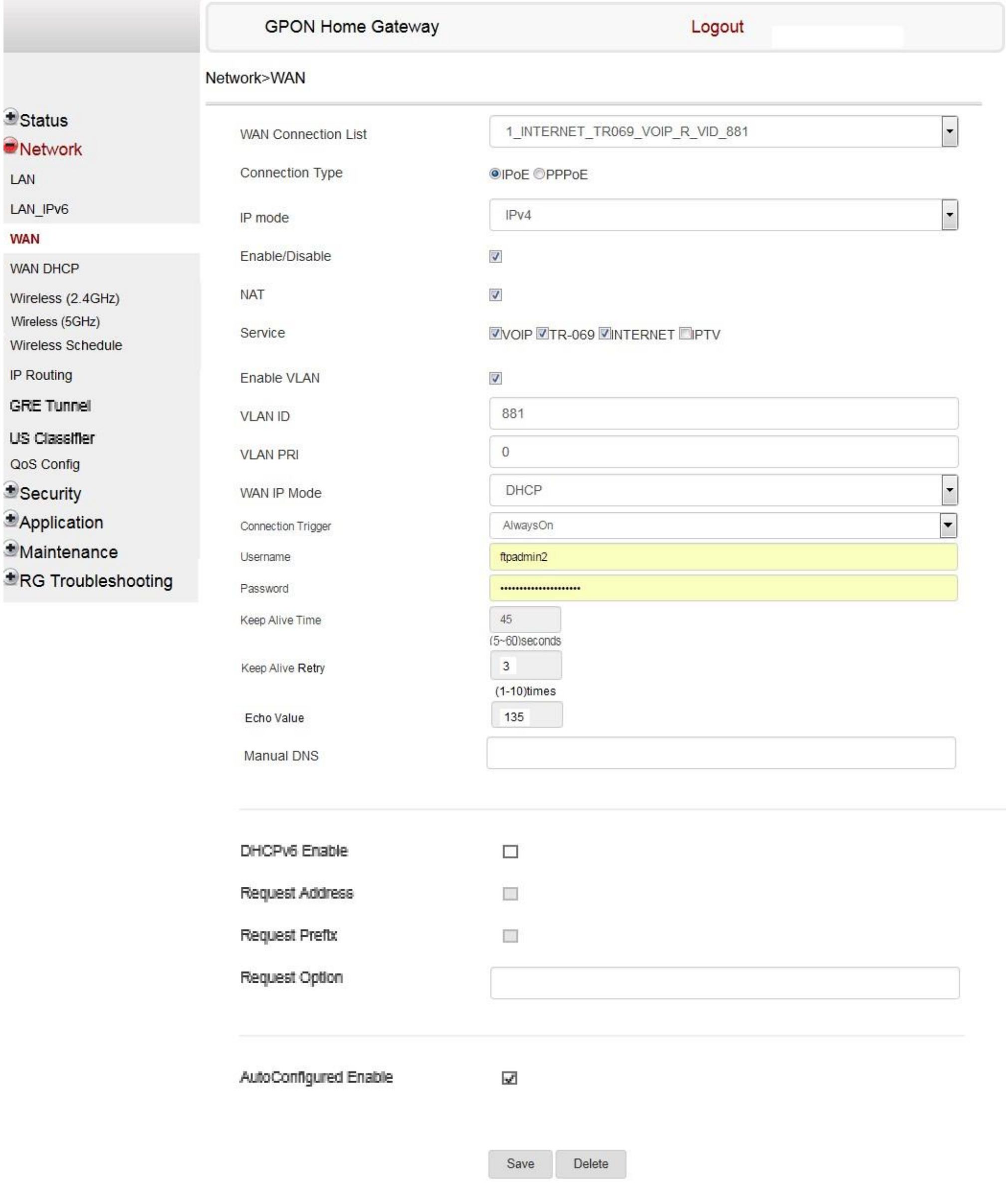
6 STOP. This procedure is complete.

1

Procedure 17 WAN networking configuration

Select Network > WAN from the top-level menu in the GPON Home Gateway window, as shown in Figure 33.

Figure 33 WAN network window



WAN Connection List	1_INTERNET_TR069_VOIP_R_VID_881
Connection Type	● IPoE ○ PPPoE
IP mode	IPv4
Enable/Disable	☑
NAT	☑
Service	☑ VOIP ☑ TR-069 ☑ INTERNET □ IPTV
Enable VLAN	☑
VLAN ID	881
VLAN PRI	0
WAN IP Mode	DHCP
Connection Trigger	AlwaysOn
Username	ftpadmin2
Password	••••••••••••••••••••
Keep Alive Time	45 (5~60)seconds
Keep Alive Retry	3 (1-10)times
Echo Value	135
Manual DNS	
DHCPv6 Enable	□
Request Address	□
Request Prefix	□
Request Option	
AutoConfigured Enable	☑

Table 27 describes the fields in the WAN network window.

Table 27 WAN network parameters

Field	Description
WAN Connection List	Choose a WAN connection from the drop-down menu to set the connection parameters

1

Connection Type	Choose a connection type: IPoE or PPPoE
IP mode	Choose an IP mode from the drop-down menu: IPv4 or IPv6
Enable/Disable	Select this checkbox to enable the WAN connection
NAT	Select this checkbox to enable NAT
Service	Select the checkboxes to enable service types for this connection
Enable VLAN	Select this checkbox to enable VLAN
VLAN ID	Enter the VLAN ID
VLAN PRI	Enter the VLAN PRI
WAN IP Mode	Choose an IP mode from the drop-down menu
Connection Trigger	Choose a connection trigger from the drop-down menu; for example, AlwaysOn The Connection Trigger field is visible when the IP mode is set to IPv6 or IPv4&IPv6.
Username	Enter the username
Password	Enter the password
Keep Alive Time	Enter the Keep Alive Time (from 5 to 60 seconds)
Keep Alive Retry	The number of keep alive time retires (1 to 10); this field cannot be modified in regular user mode
Echo Value	The echo value: the keep alive time value multiplied by the number of retries; this field cannot be modified in regular user mode
Manual DNS	If desired, enter a manual DNS
DHCPv6 Enable	Select this checkbox to enable the DHCPv6 function on this WAN interface
Request Address	Select this checkbox to enable the DHCPv6 option to request the Address from the DHCPv6 Server
Request Prefix	Select this checkbox to enable the DHCPv6 option to request the Prefix from the DHCPv6 server
Request Option	Enter the custom DHCPv6 option send to the DHCPv6 server
Auto Configured Enable	Select this checkbox to enable the Auto Configuration function on this WAN interface

2 Configure a specific WAN connection.

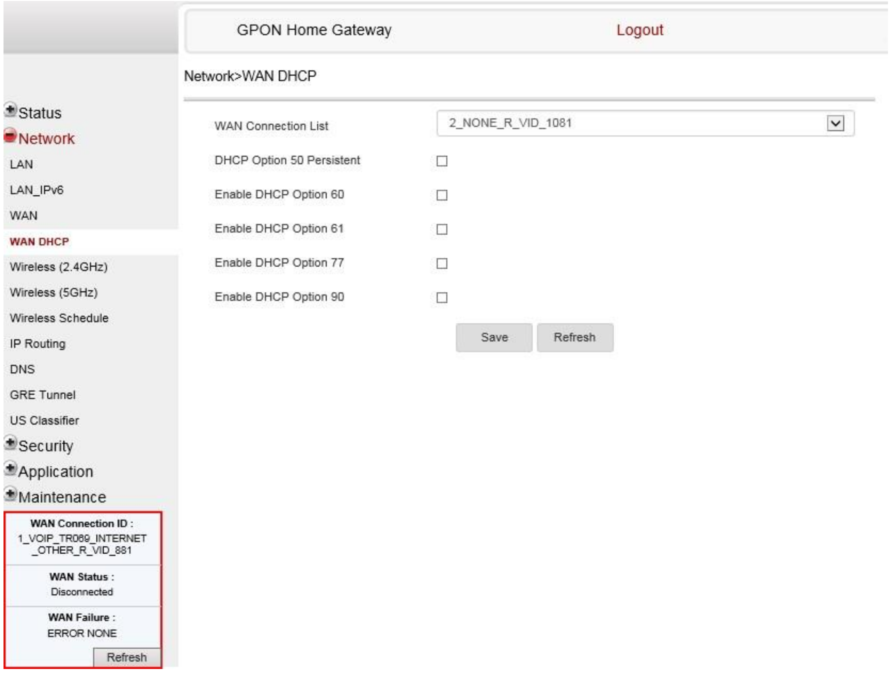
3 Click Save.

4 STOP. This procedure is complete.

Procedure 18 WAN DHCP configuration

Select Network > WAN DHCP from the top-level menu in the GPON Home Gateway window, as shown in Figure 34.

Figure 34 **WAN DHCP window**



WAN Connection List: 2_NONE_R_VID_1081

DHCP Option 50 Persistent ☐

Enable DHCP Option 60 ☐

Enable DHCP Option 61 ☐

Enable DHCP Option 77 ☐

Enable DHCP Option 90 ☐

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 28 describes the fields in the WAN DHCP window.

Table 28 **WAN DHCP parameters**

Field	Description
WAN Connection List	Choose a WAN connection from the drop-down menu
DHCP Option 50 Persistent	Select this checkbox to enable DHCP Option 50 persistent
Enable DHCP Option 60	Select this checkbox to enable DHCP Option 60 (vendor class identifier)
Enable DHCP Option 61	Select this checkbox to enable DHCP Option 61 (client identifier)
Enable DHCP Option 77	Select this checkbox to enable DHCP Option 77
Enable DHCP Option 90	Select this checkbox to enable DHCP Option 90

1

2 Configure a WAN DHCP option.

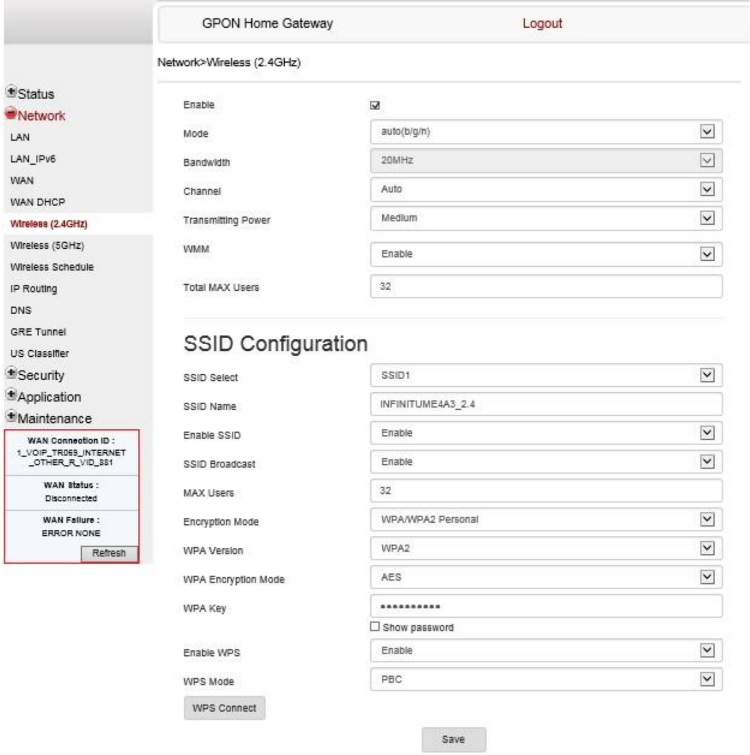
3 Click Save.

4 STOP. This procedure is complete.

Procedure 19 WiFi 2.4G networking configuration

1 Select Network > WiFi 2.4G from the top-level menu in the GPON Home Gateway window, as shown in Figure 35.

Figure 35 **WiFi 2.4G network window**



Network>Wireless (2.4GHz)

Enable	☑
Mode	auto(b/g/n)
Bandwidth	20MHz
Channel	Auto
Transmitting Power	Medium
WMM	Enable
Total MAX Users	32

SSID Configuration

SSID Select	SSID1
SSID Name	INFINITUME4A3_2.4
Enable SSID	Enable
SSID Broadcast	Enable
MAX Users	32
Encryption Mode	WPA/WPA2 Personal
WPA Version	WPA2
WPA Encryption Mode	AES
WPA Key	•••••••••• ☐ Show password
Enable WPS	Enable
WPS Mode	PBC

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 29 describes the fields in the WiFi 2.4G network window.

Table 29 **WiFi 2.4G network parameters**

Field	Description
Enable	Select this checkbox to enable WiFi

(1 of 3)

Field	Description
Mode	Choose a Wi-Fi mode from the drop-down menu: • auto (b/g/n) • b • g • n • b/g
Bandwidth	Choose from: • 20 MHz • 40 MHz • 20/40 MHz
Channel	Choose a channel from the drop-down menu or choose Auto to have the channel automatically assigned
Transmitting Power	Choose a percentage for the transmitting power from the drop-down menu: • Low (25%) • Medium (50%) • High (75%) • Maximum (100%)
WMM	Choose Enable or Disable from the drop-down menu to enable or disable WiFi multi-media
Total MAX Users	Enter the number of total MAX users
SSID Configuration	
SSID Select	Choose the SSID from the drop-down menu
SSID Name	Enter the SSID name
Enable SSID	Enable or disable SSID from this drop-down menu
SSID Broadcast	Enable or disable SSID broadcast from this drop-down menu
MAX Users	Enter the number of MAX users
Encryption Mode	Choose an encryption mode from the drop-down menu: • OPEN • WEP • WPA/WPA2 Personal • WPA/WPA2 Enterprise (1) (2)
WPA Version	Choose a WPA version from the drop-down menu: • WPA1 • WPA2 • WPA1/WPA2

WPA Encryption Mode	Choose a WPA encryption mode from the drop-down menu: • TKIP • AES • TKIP/AES
WPA Key	Enter the WPA key
Enable WPS	Enable or disable WPS from this drop-down menu

(2 of 3)

Field	Description
WPS Mode	Choose a WPS mode from the drop-down menu: PBC (Push Button Connect) or PIN (Personal Identification Number)

(3 of 3)

Notes

[1] When Encryption Mode is set to “WPA/WPA2 Enterprise”, the following options are no longer available: WPA version, 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; Secondary RADIUS server, port, and password; RADIUS accounting port.

2 Configure the WiFi connection.

3 If you have enabled and configured WPS, click WPS connect.

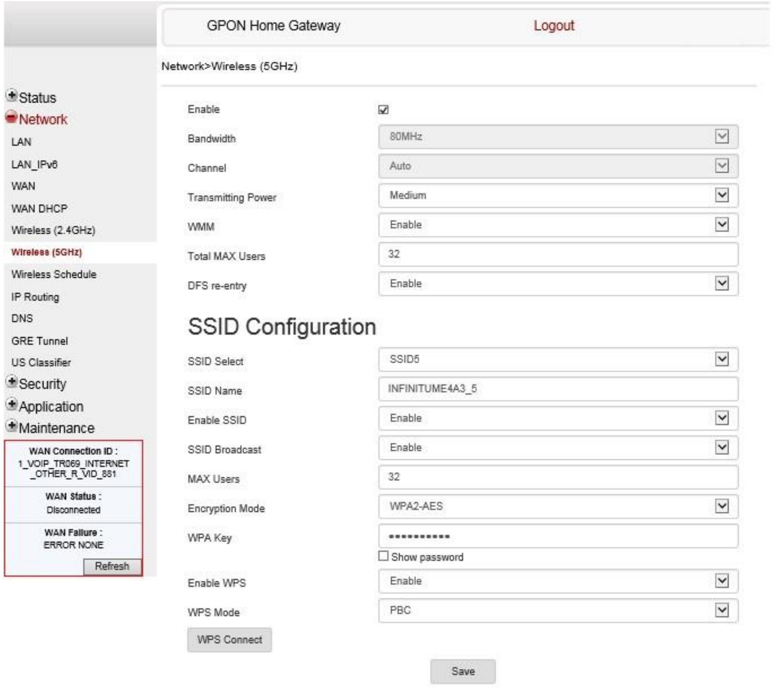
4 Click Save.

5 STOP. This procedure is complete.

Procedure 20 WiFi 5G networking configuration

1 Select Network > WiFi 5G from the top-level menu in the GPON Home Gateway window, as shown in Figure 36.

Figure 36 **WiFi 5G network window**



Network>Wireless (5GHz)

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Enable ☑

Bandwidth 80MHz

Channel Auto

Transmitting Power Medium

WMM Enable

Total MAX Users 32

DFS re-entry Enable

SSID Configuration

SSID Select SSID5

SSID Name INFINITUME4A3_5

Enable SSID Enable

SSID Broadcast Enable

MAX Users 32

Encryption Mode WPA2-AES

WPA Key ••••••••••

□ Show password

Enable WPS Enable

WPS Mode PBC

Table 30 describes the fields in the WiFi 5G network window.

Table 30 **WiFi 5G network parameters**

Field	**Description**
Enable	Select this checkbox to enable WiFi
Bandwidth	Choose from: • 20 MHz • 40 MHz • 80 MHz
Channel	Choose a channel from the drop-down menu or choose Auto to have the channel automatically assigned

(1 of 2)

Field	**Description**

Transmitting Power	Choose a percentage for the transmitting power from the drop-down menu: • Low (20%) • Medium (40%) • High (60%) • Maximum (100%)
WMM	Choose Enable or Disable from the drop-down menu to enable or disable WiFi multi-media
Total MAX Users	Enter the total number of MAX users
DFS re-entry	Choose Enable or Disable from the drop-down menu to enable or disable DFS re-entry
SSID Configuration	
SSID Select	Choose the SSID from the drop-down menu
SSID Name	Change the name of the selected SSID
Enable SSID	Choose Enable or disable SSID from this drop-down menu
SSID Broadcast	Choose Enable or disable SSID broadcast from this drop-down menu
MAX Users	Enter the number of MAX users
Encryption Mode	Choose an encryption mode from the drop-down menu: • OPEN • WEP • WPA/WPA2 Personal • WPA/WPA2 Enterprise [(1)] [(2)]
WPA Key	Enter the WPA key
Enable WPS	Choose Enable or disable WPS from this drop-down menu
WPS Mode	Choose a WPS mode from the drop-down menu: PBC (Push Button Connect) or PIN (Personal Identification Number)

(2 of 2)

Notes

[(1)] When Encryption Mode is set to “WPA/WPA2 Enterprise”, the following options are no longer available: WPA version, 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; Secondary RADIUS server, port, and password; RADIUS accounting port.

2 Configure the WiFi connection.

3 If you have enabled and configured WPS, click WPS connect.

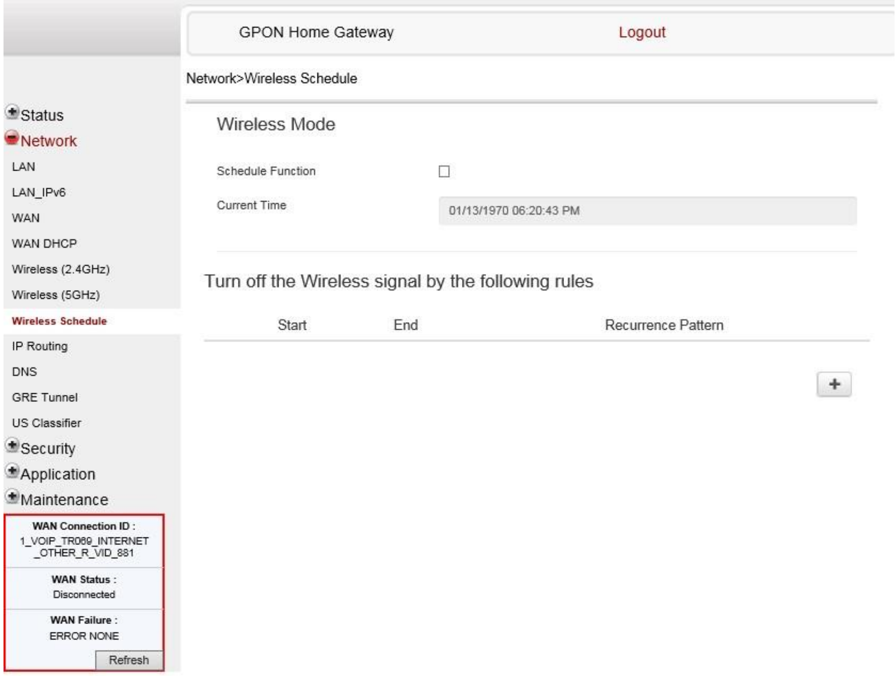
4 Click Save.

5 STOP. This procedure is complete.

Procedure 21 Wireless scheduling

1 Select Network > Wireless Schedule from the top-level menu in the GPON Gateway window, as shown in Figure 37.

Figure 37 **Wireless Schedule window**



Network>Wireless Schedule

Wireless Mode

Schedule Function □

Current Time 01/13/1970 06:20:43 PM

Turn off the Wireless signal by the following rules

Start	End	Recurrence Pattern

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

2 Select the Schedule Function checkbox to turn the wireless signal off for the configured period.

3 Click the plus sign (+) to add a scheduling rule.

A separate panel displays for configuring wireless schedule rules.

4 Enter a start time and end time for the period in which you want the wireless signal off.

5 Choose Everyday or Individual Days from the drop-down menu.

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

The Recurrence Pattern shows the rules created to date.

7 If desired, click the plus sign (+) to add more rules.

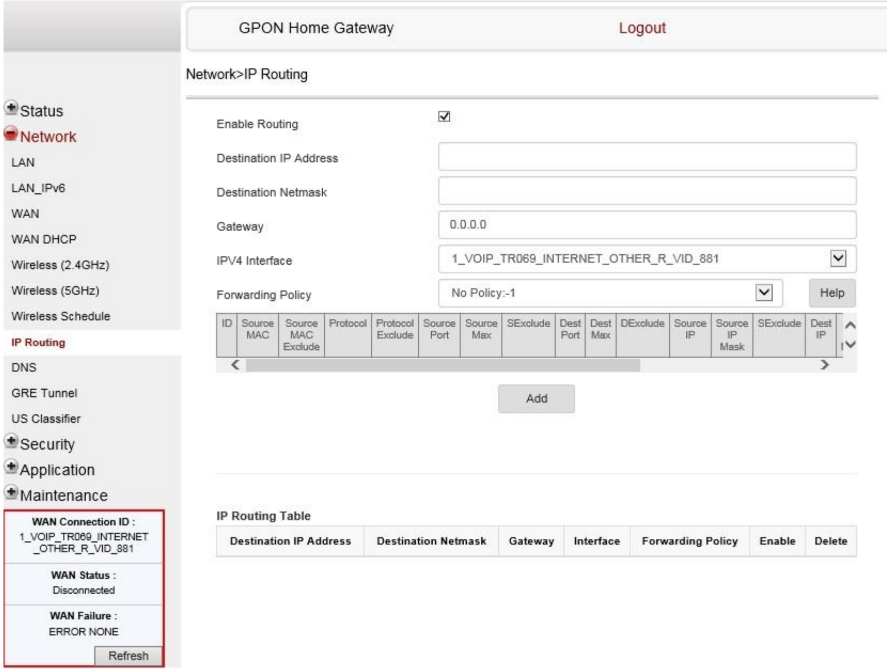
8 Click Save Changes.

9 STOP. This procedure is complete.

Procedure 22 Routing configuration

1 Select Network > Routing from the top-level menu in the GPON Home Gateway window, as shown in Figure 38.

Figure 38 **Routing network window**



Network>IP Routing

Enable Routing ☑

Destination IP Address

Destination Netmask

Gateway 0.0.0.0

IPV4 Interface 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

Forwarding Policy No Policy:-1

ID	Source MAC	Source MAC Exclude	Protocol	Protocol Exclude	Source Port	Source Max	SExclude	Dest Port	Dest Max	DExclude	Source IP	Source IP Mask	SExclude	Dest IP

IP Routing Table

Destination IP Address	Destination Netmask	Gateway	Interface	Forwarding Policy	Enable	Delete

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 31 describes the fields in the Routing network window.

Table 31 **Routing network parameters**

Field	Description
Enable Routing	Select this checkbox to enable routing
Destination IP Address	Enter the destination IP address
Destination Netmask	Enter the destination network mask
Gateway	Enter the gateway address
IPv4 Interface	Choose a WAN connection previously created in the WAN network window from the drop-down menu
Forwarding Policy	Choose a forwarding policy from the drop-down menu

(1 of 2) **(2 of 2)**

2 Enter the routing information.

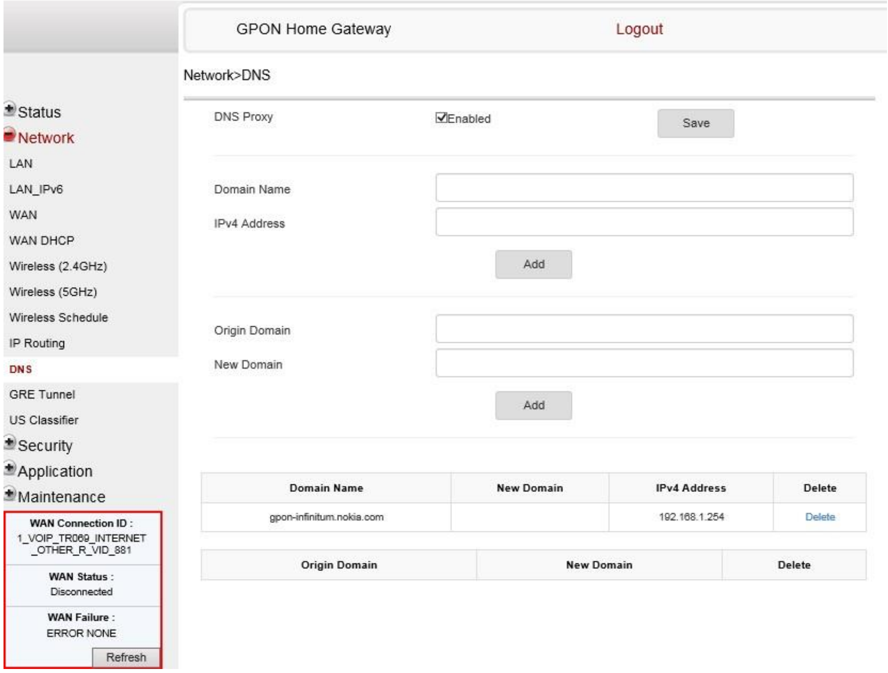
3 Click Add.

4 STOP. This procedure is complete.

Procedure 23 DNS configuration

1 Select Network > DNS from the top-level menu in the GPON Home Gateway window, as shown in Figure 39.

Figure 39 DNS network window



DNS Proxy ☑Enabled

Domain Name

IPv4 Address

Origin Domain

New Domain

Domain Name	New Domain	IPv4 Address	Delete
gpon-infinitum.nokia.com		192.168.1.254	Delete

Origin Domain	New Domain	Delete

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 32 describes the fields in the DNS network window.

Table 32 DNS network parameters

Field	Description
DNS Proxy	Select the Enabled checkbox to enable the DNS proxy
Domain Name	Domain name
IPv4 Address	Domain IP address
Origin Domain	Origin domain name
New Domain	New domain name

2 Select the Enabled checkbox and click Save to enable the DNS proxy.

3 Enter the domain name and IPv4 address and click Add.

4 If required, associate an origin domain with a new domain, click Add.

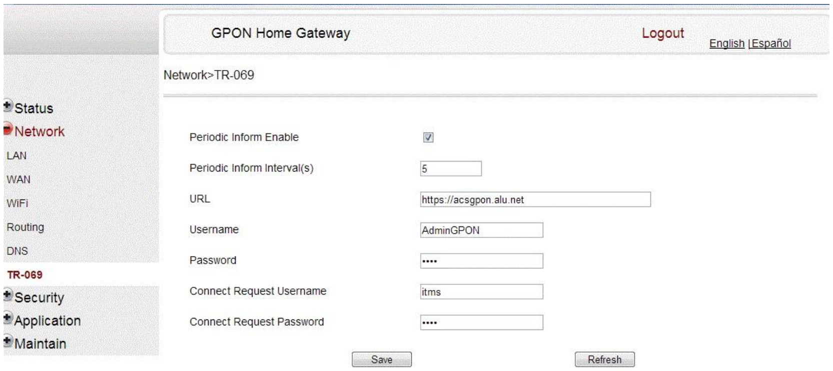
5 STOP. This procedure is complete.

Procedure 24 TR-069 configuration

Note — You need to have administrator (SuperAdmin) account privileges for TR-069 configuration; a user account (userAdmin) does not provide access to this procedure.

1 Select Network > TR-069 from the top-level menu in the GPON Home Gateway window, as shown in Figure 40.

Figure 40 **TR-069 network window**



Network>TR-069

Periodic Inform Enable ☑

Periodic Inform Interval(s) 5

URL https://acsgpon.alu.net

Username AdminGPON

Password ••••

Connect Request Username itms

Connect Request Password ••••

Table 33 describes the fields in the TR-069 network window.

Table 33 **TR-069 network parameters**

Field	Description
Periodic Inform Enable	Select this checkbox to enable periodic inform updates
Periodic Inform Interval(s)	Time between periodic inform updates, in seconds
URL	URL of the auto-configuration server
Username	Username used to log in to the auto-configuration server
Password	Password used to log in to the auto-configuration server
Connect Request Username	Username used to log in to the ONT
Connect Request Password	Password used to log in to the ONT

2 Configure TR-069 by entering the required information.

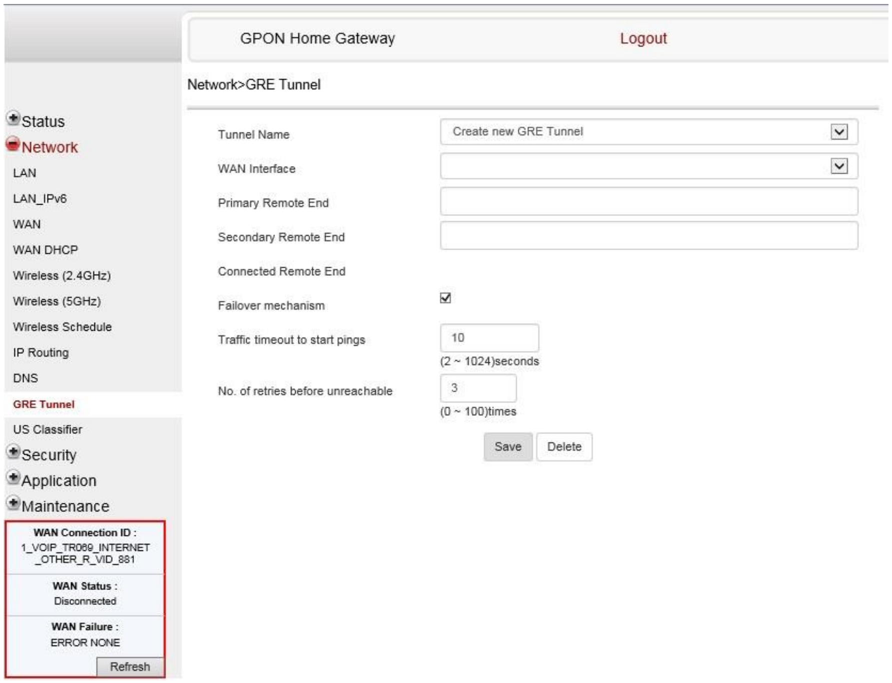
3 Click Save.

4 STOP. This procedure is complete.

Procedure 25 GRE Tunnel configuration

1 Select Network > GRE Tunnel from the top-level menu in the GPON Home Gateway window, as shown in Figure 41.

Figure 41 **GRE Tunnel window**



Tunnel Name: Create new GRE Tunnel

WAN Interface:

Primary Remote End:

Secondary Remote End:

Connected Remote End

Failover mechanism ☑

Traffic timeout to start pings: 10 (2 ~ 1024)seconds

No. of retries before unreachable: 3 (0 ~ 100)times

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 34 describes the fields in the GRE Tunnel window.

Table 34 **GRE Tunnel parameters**

Field	Description
Tunnel Name	Choose Create new GRE Tunnel, or Choose an existing tunnel from the drop-down menu. The tunnel name is automatically assigned by the system. Up to 3 GRE tunnels are supported.

(1 of 2)

Field	Description

WAN Interface	Choose a WAN interface from the drop-down menu. 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.
Failover mechanism	This feature is automatically selected by the system.
Traffic timeout to start pings	Enter the traffic timeout in seconds (0 to 100).
No. of retries before unreachable	Enter the number of retries before the tunnel is declared down (2 to 1024).

(2 of 2)

2 Configure the GRE tunnel by entering or selecting the required information.

3 Click Save.

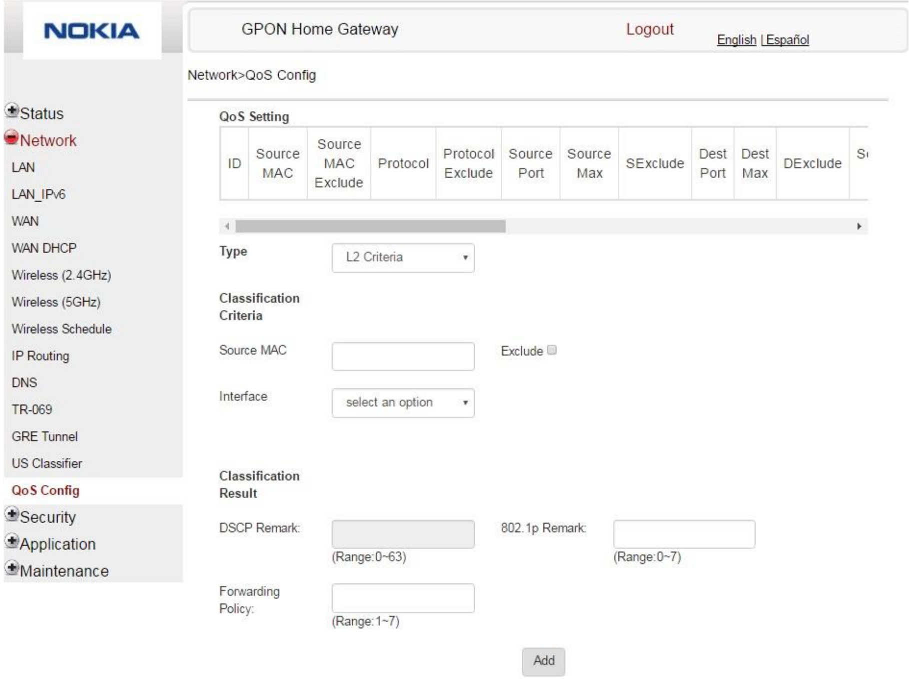
4 STOP. This procedure is complete.

Procedure 26 QoS configuration

1 Select Network > QoS Config from the top-level menu in the Home Gateway window.

Figure 42 shows the window for configuring QoS L2 (Layer 2 packet sizes).

Figure 42 **QoS Config window (L2)**



QoS Setting

ID	Source MAC	Source MAC Exclude	Protocol	Protocol Exclude	Source Port	Source Max	SExclude	Dest Port	Dest Max	DExclude	S

Type L2 Criteria

Classification Criteria

Source MAC Exclude □

Interface select an option

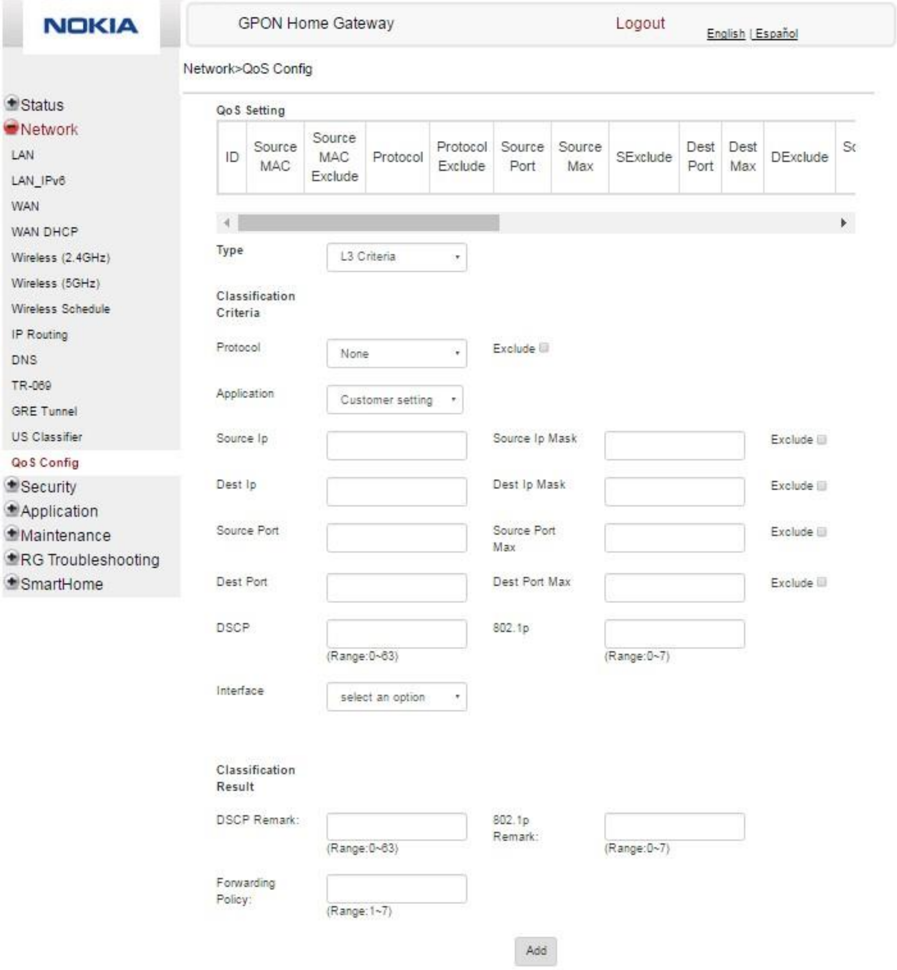
Classification Result

DSCP Remark: (Range:0~63) 802.1p Remark: (Range:0~7)

Forwarding Policy: (Range:1~7)

Figure 43 shows the window for configuring QoS L3 (Layer 3 packet sizes).

Figure 43 **QoS Config window (L3)**



QoS Setting

ID	Source MAC	Source MAC Exclude	Protocol	Protocol Exclude	Source Port	Source Max	SExclude	Dest Port	Dest Max	DExclude	Sc

Type: L3 Criteria

Classification Criteria

Protocol: None Exclude □

Application: Customer setting

Source Ip: Source Ip Mask: Exclude □

Dest Ip: Dest Ip Mask: Exclude □

Source Port: Source Port Max: Exclude □

Dest Port: Dest Port Max: Exclude □

DSCP: (Range:0~63) 802.1p: (Range:0~7)

Interface: select an option

Classification Result

DSCP Remark: (Range:0~63) 802.1p Remark: (Range:0~7)

Forwarding Policy: (Range:1~7)

Table 35 describes the fields in the QoS Config window.

Table 35 **QoS Config parameters**

Field	Description
Type	Choose a QoS service layer type from the drop-down menu L2 or L3.
Source MAC	Enter the source MAC Select the Exclude checkbox to exclude the source MAC
Interface	Choose an interface from the drop-down menu
DSCP Mark	Enter the value for the DSCP mark (range: 0-63); valid only for L3 Criteria
802.1p Mark	Enter the value for the 802.1p (range: 0-7)

(1 of 2)

Field	Description
Forwarding Policy	Enter the number for the forwarding policy (range: 1-7)
Additional fields for L3	
Protocol	Choose a protocol from the drop-down menu, or select the Exclude checkbox
Application	Choose an application from the drop-down menu
Source IP and Source IP Mask	Enter the values for the source IP and IP mask, or select the Exclude checkbox
Destination IP and Destination IP Mask	Enter the values for the destination IP and IP mask, or select the Exclude checkbox
Source Port and Source Port Max	Enter the values for the source port and port max (highest port number) or select the Exclude checkbox
Destination Port and Destination Port Max	Enter the values for the destination port and port max (highest port number), or select the Exclude checkbox

(2 of 2)

2 Choose a QoS type from the drop-down menu: L2 or L3.

3 Configure a QoS policy.

4 Click Add to add a QoS policy.

5 STOP. This procedure is complete.

Procedure 27 Upstream (US) Classifier configuration

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.

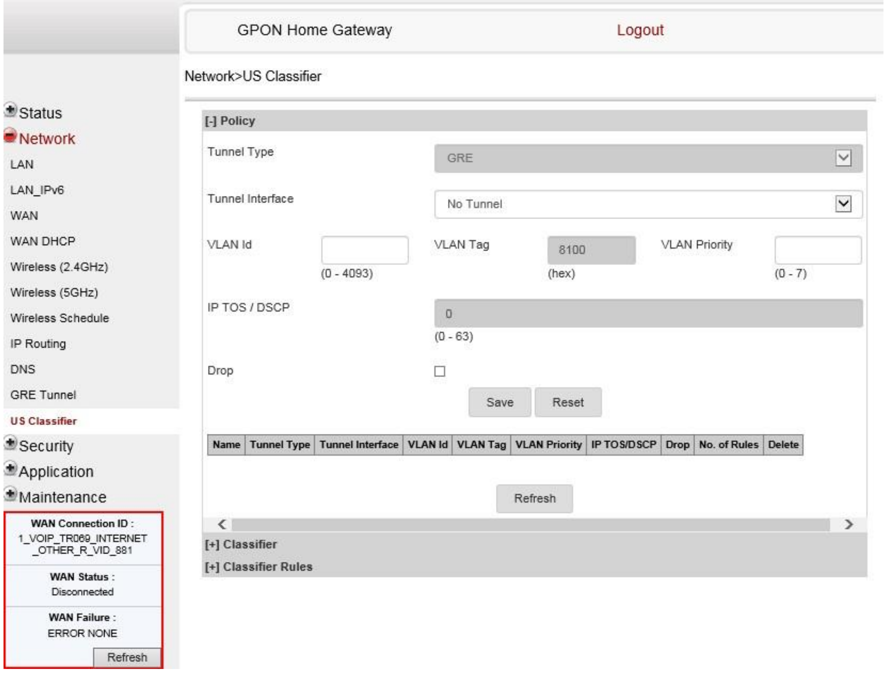
A classifier rule is used to assign actions to a group of packets based on a set of parameters. A classification rule must be created against a pre-defined classifier.

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

1 Select Network > US Classifier from the top-level menu in the GPON Home Gateway window, and select the Policy tab, as shown in Figure 44.

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

Figure 44 US Classifier Policy window



Tunnel Type: GRE

Tunnel Interface: No Tunnel

VLAN Id: (0 - 4093)

VLAN Tag: 8100 (hex)

VLAN Priority: (0 - 7)

IP TOS / DSCP: 0 (0 - 63)

Drop: □

Name	Tunnel Type	Tunnel Interface	VLAN Id	VLAN Tag	VLAN Priority	IP TOS/DSCP	Drop	No. of Rules	Delete

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Refresh

Table 36 describes the fields in the US Classifier Policy window.

Table 36 US Classifier Policy parameters

Field	Description
Tunnel Type	The tunnel type is set to GRE and cannot be modified.
Tunnel Interface	Choose a tunnel interface from the drop-down menu: No Tunnel, GRE Tunnel, or LAN traffic.
VLAN ID	Enter a VLAN ID (0-4094).
VLAN Tag	This field is not configurable. The VLAN tag is set to 8100 (hexadecimal).
VLAN Priority	Enter a VLAN priority level (0 to 7). A lower number indicates a higher priority.
IP TOS/DSCP	This field is not configurable. All tunnel packets are generated with a default DSCP value (usually 0).
Drop	Select this checkbox to drop the packets

2 Select a tunnel interface.

3 Enter a VLAN ID and priority level.

4 Click Save.

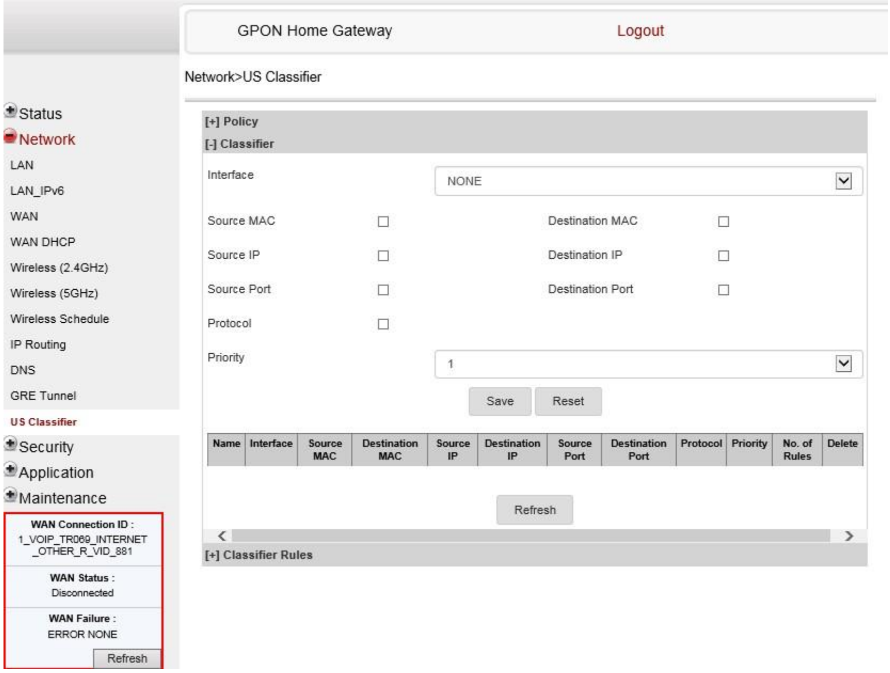
5 To delete a policy, click the Delete option for the applicable policy in the policy table.

A policy can only be deleted if it is not associated with any classifier rules.

6 Select Network > US Classifier from the top-level menu in the GPON Home Gateway window, and select the Classifier tab, as shown in Figure 45.

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

Figure 45 US Classifier window



Network>US Classifier

Interface NONE

Source MAC □ Destination MAC □

Source IP □ Destination IP □

Source Port □ Destination Port □

Protocol □

Priority 1

Name	Interface	Source MAC	Destination MAC	Source IP	Destination IP	Source Port	Destination Port	Protocol	Priority	No. of Rules	Delete

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 37 describes the fields in the US Classifier window.

Table 37 US Classifier parameters

Field	Description
Interface	Choose an interface from the drop-down menu; for example, None, LAN, 2.4G SSID, or 5G SSID.

Field	Description
Source MAC	Click to enter a source MAC
Destination MAC	Click to enter a destination MAC
Source IP	Click to enter a source IP
Destination IP	Click to enter a destination IP
Source Port	Click to enter a source port
Destination Port	Click to enter a destination port
Protocol	Click to enter a protocol
Priority	Choose a priority level from 1 to 8. The lower the number, the higher the priority. No more than 1 classifier can be created with the same priority.

(1 of 2)

(2 of 2)

7 Configure the US classifier.

At least one field must be selected to create a classifier. A maximum of four fields may be selected to create a classifier; this includes the interface field.

8 Click Save.

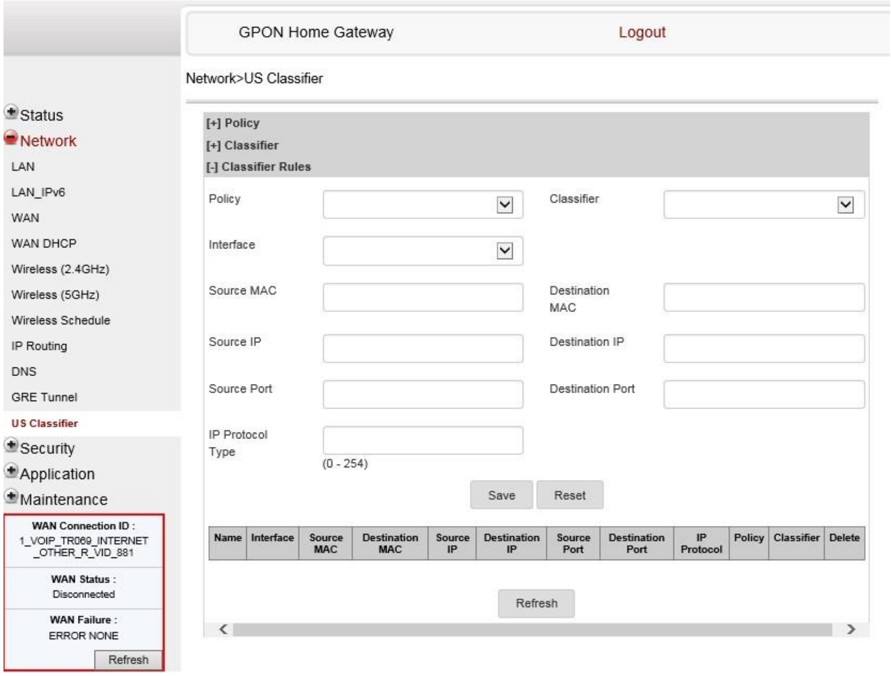
9 To delete a classifier, click the Delete option for the applicable classifier in the classifier table.

A classifier can only be deleted if it is not associated with any classifier rules.

10 Select the Classifier Rules tab, as shown in Figure 46.

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

Figure 46 **US Classifier Rules window**



WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Name	Interface	Source MAC	Destination MAC	Source IP	Destination IP	Source Port	Destination Port	IP Protocol	Policy	Classifier	Delete

Table 38 describes the fields in the US Classifier Rules window.

Table 38 **US Classifier Rules parameters**

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

11 Configure the classifier rule.

12 Click Save.

13 To delete a classifier rule, click the Delete option for the applicable classifier rule in the classifier rules table.

14 STOP. This procedure is complete.

8.2.4 Security configuration

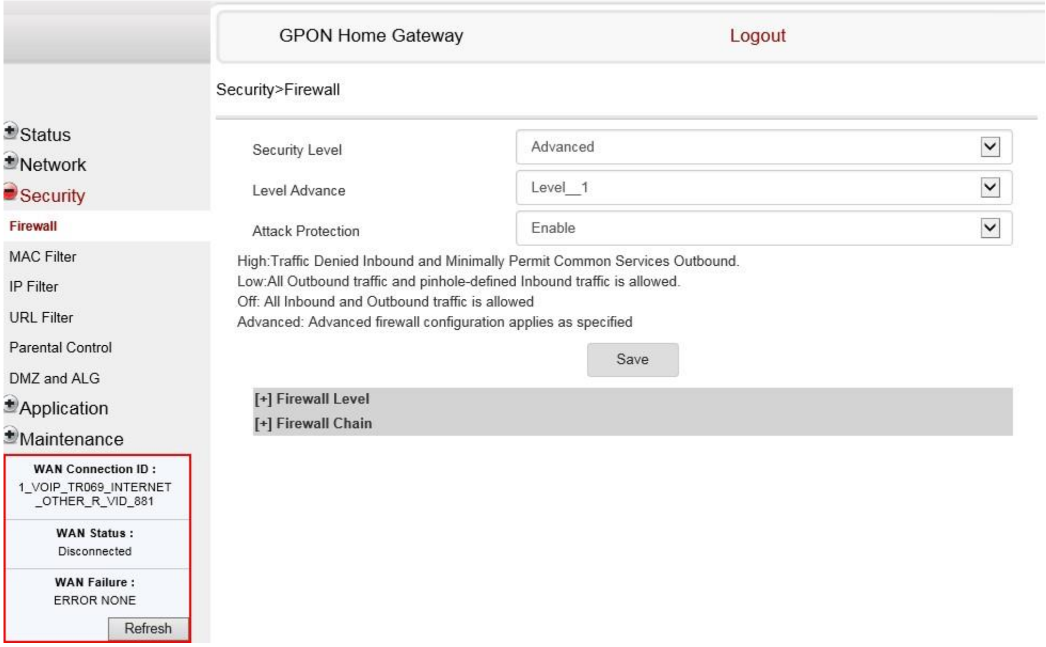
G-240W-J ONTs support security configuration, including:

- firewall
- MAC filter
- IP filter
- URL filter
- parental control
- DMZ and ALG
- access control

Procedure 28 Firewall configuration

1 Select Security > Firewall from the top-level menu in the GPON Home Gateway window, as shown in Figure 47.

Figure 47 Firewall window



Security>Firewall

Security Level: Advanced

Level Advance: Level__1

Attack Protection: Enable

High:Traffic Denied Inbound and Minimally Permit Common Services Outbound.
Low:All Outbound traffic and pinhole-defined Inbound traffic is allowed.
Off: All Inbound and Outbound traffic is allowed
Advanced: Advanced firewall configuration applies as specified

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Four security options are available: High, Low, Off, and Advanced.

High—Traffic denied inbound and minimally permit common services outbound

Low—All outbound traffic and pinhole-defined inbound traffic is allowed

Off—All inbound and outbound traffic is allowed

Advanced—Advanced firewall configuration applies as specified

Table 39 describes the fields in the firewall window.

Table 39 Firewall parameters

Field	Description
Security Level	Choose the security level from the drop-down menu: High, Low, Off, or Advanced
Level Advance	Choose Advanced to configure the DMZ and IP filter
Attack Protection (Protection against DoS or DDoS attacks)	Choose Enable or Disable attack protection from the drop-down menu. The default is Enable.

(1 of 2) **(2 of 2)**

2 Configure the firewall.

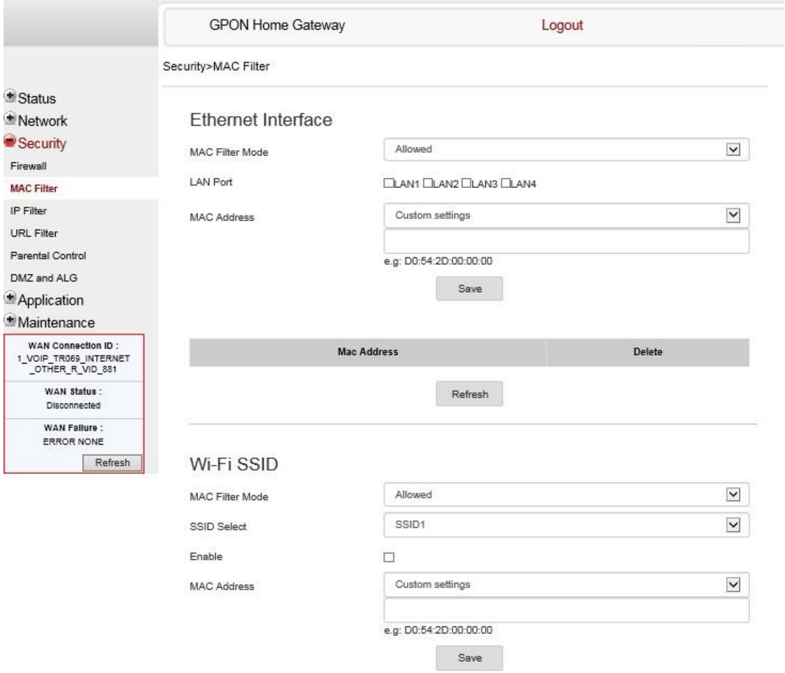
3 Click Save.

4 STOP. This procedure is complete.

Procedure 29 MAC filter configuration

1 Select Security > Mac Filter from the top-level menu in the GPON Home Gateway window, as shown in Figure 48.

Figure 48 **MAC filter window**



WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Ethernet Interface

MAC Filter Mode: Allowed

LAN Port: □LAN1 □LAN2 □LAN3 □LAN4

MAC Address: Custom settings

e.g: D0:54:2D:00:00:00

Wi-Fi SSID

MAC Filter Mode: Allowed

SSID Select: SSID1

Enable: □

MAC Address: Custom settings

e.g: D0:54:2D:00:00:00

Table 40 describes the fields in the MAC filter window.

Table 40 **MAC filter parameters**

Field	Description
Ethernet Interface	

MAC Filter Mode	Choose the MAC filter mode from the drop-down menu: Blocked or Allowed
LAN Port	LAN port range
MAC Address	Choose a MAC address from the drop-down menu or enter the address in the text field
Wi-Fi SSID	
MAC Filter Mode	Choose the MAC filter mode from the drop-down menu: Blocked or Allowed
SSID Select	Choose the SSID from the drop-down menu
Enable	Select this checkbox to enable the MAC filter
MAC Address	Choose a MAC address from the drop-down menu or enter the address in the text field

2 Click Refresh to update the information.

3 Configure a MAC filter.

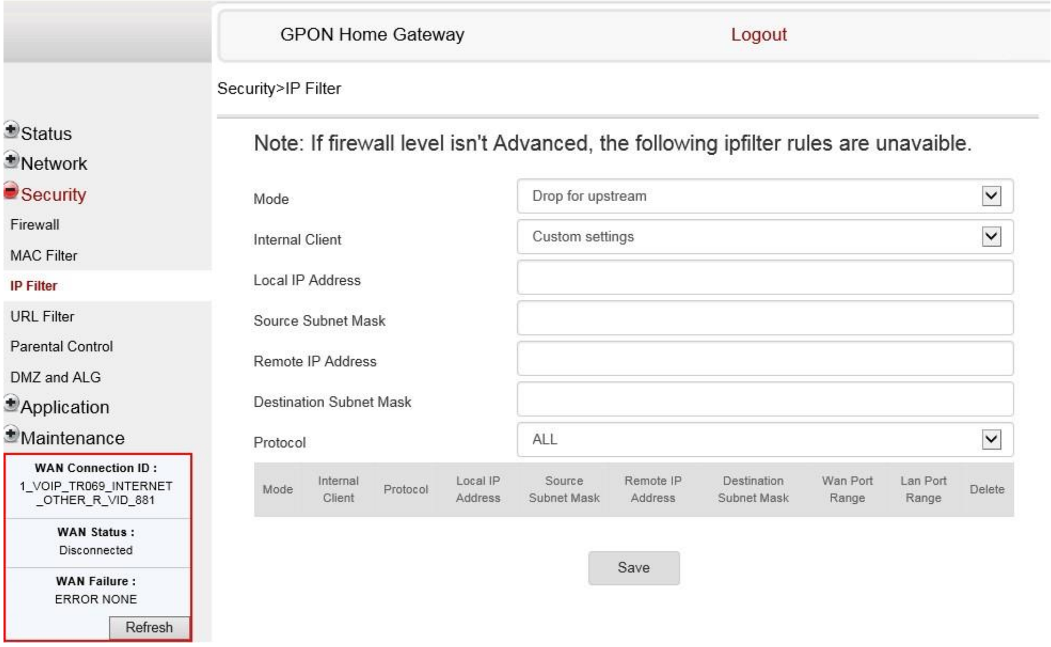
4 Click Add.

5 STOP. This procedure is complete.

Procedure 30 IP filter configuration

1 Select Security > IP filter from the top-level menu in the GPON Home Gateway window, as shown in Figure 49.

Figure 49 **IP filter window**



Security>IP Filter

Note: If firewall level isn't Advanced, the following ipfilter rules are unavaible.

Mode	Drop for upstream
Internal Client	Custom settings
Local IP Address	
Source Subnet Mask	
Remote IP Address	
Destination Subnet Mask	
Protocol	ALL

Mode	Internal Client	Protocol	Local IP Address	Source Subnet Mask	Remote IP Address	Destination Subnet Mask	Wan Port Range	Lan Port Range	Delete

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 41 describes the fields in the IP filter window. If the firewall level is not set to advanced, the IP filter rules are not available.

Table 41 **IP filter parameters**

Field	Description
Mode	Choose an IP filter mode from the drop-down menu: • Drop for upstream • Drop for downstream
Internal Client	Choose an internal client from the drop-down menu: • Customer setting - uses the IP address input below • IP - uses the connecting devices' IP to the ONT
Local IP Address	Local IP address
Source Subnet Mask	Source subnet mask
Remote IP Address	Remote IP address
Destination Subnet Mask	Destination subnet mask
Protocol	Choose an application protocol or all from the drop-down menu

2 Configure the IP filter.

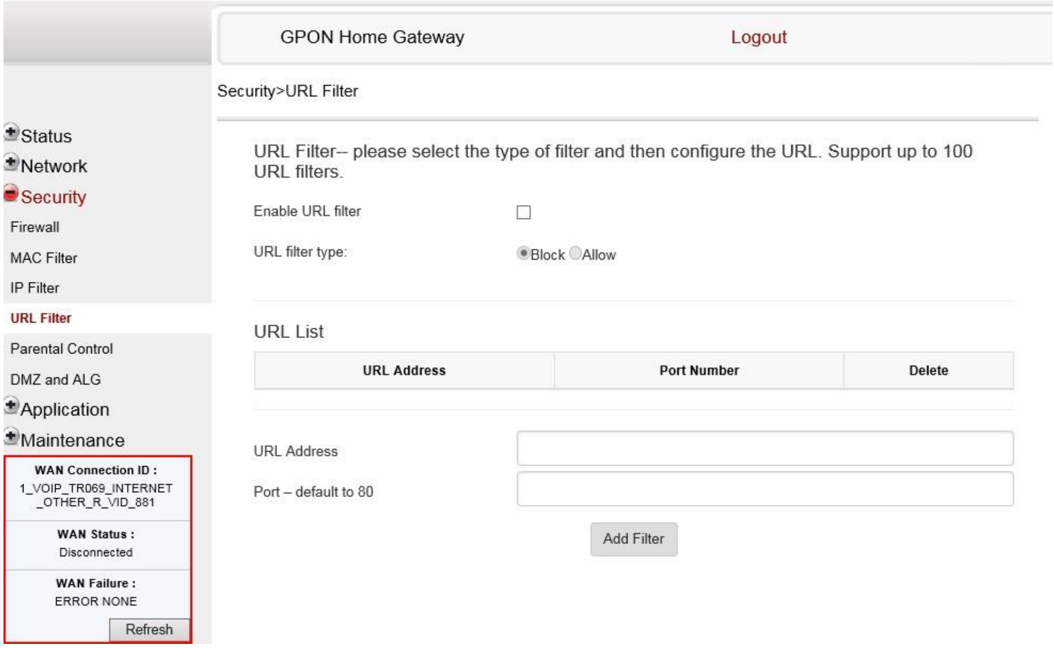
3 Click Add.

4 STOP. This procedure is complete.

Procedure 31 URL filter configuration

1 Select Security > URL Filter from the top-level menu in the GPON Home Gateway window, as shown in Figure 50.

Figure 50 **URL Filter window**



URL Filter-- please select the type of filter and then configure the URL. Support up to 100 URL filters.

Enable URL filter ☐

URL filter type: ● Block ○ Allow

URL List

URL Address	Port Number	Delete

URL Address

Port – default to 80

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

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

Table 42 describes the fields in the URL Filter window.

Table 42 **URL Filter parameters**

Field	Description
Enable URL filter	Select the checkbox to enable the URL filter
URL filter type	Select the radio button to block the URL or allow the URL

URL List	
URL Address	Type the URL address
Port - default to 80	Type the port number; the default is 80

2 Configure the URL Filter.

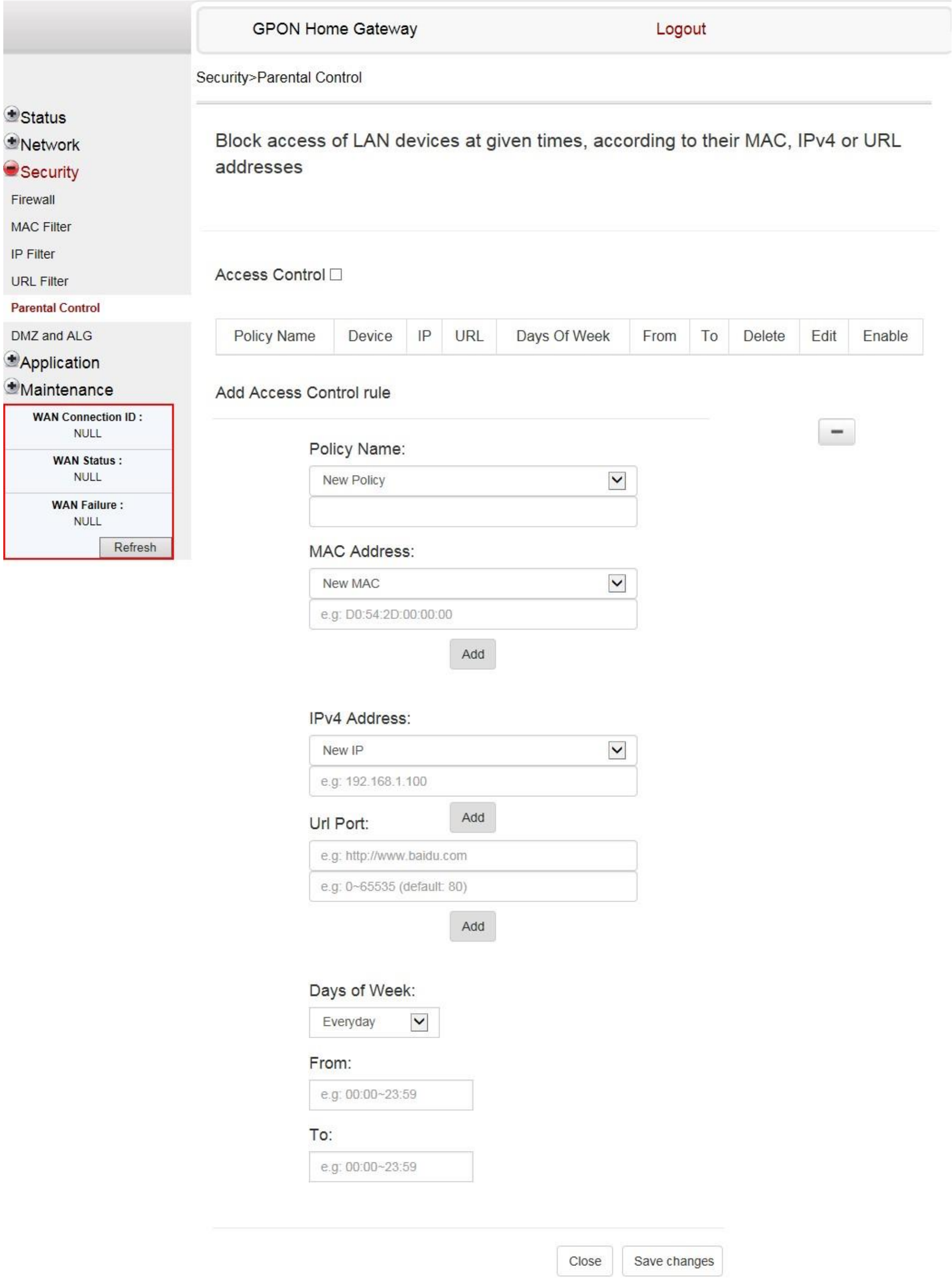
3 Click Add Filter.

4 STOP. This procedure is complete.

Procedure 32 Parental control

1 Select Security > Parent Control from the top-level menu in the GPON Gateway window, as shown in Figure 51.

Figure 51 **Parental Control window**



WAN Connection ID : NULL

WAN Status : NULL

WAN Failure : NULL

Block access of LAN devices at given times, according to their MAC, IPv4 or URL addresses

Access Control □

Policy Name	Device	IP	URL	Days Of Week	From	To	Delete	Edit	Enable

Add Access Control rule

Policy Name: New Policy

MAC Address: New MAC
e.g: D0:54:2D:00:00:00

IPv4 Address: New IP
e.g: 192.168.1.100

Url Port:
e.g: http://www.baidu.com
e.g: 0~65535 (default: 80)

Days of Week: Everyday

From: e.g: 00:00~23:59

To: e.g: 00:00~23:59

Table 43 describes the fields in the Parental Control window.

Table 43 **Parental control parameters**

Field	Description

Access Control	Select this checkbox to enable access control
Add Access Control rule	
Policy Name	Enter a name for the parental control policy or choose a policy from the list
MAC Address	Enter the MAC address or choose a MAC address from the list
IPv4 Address	Enter the IPv4 address for the device or choose an IPv4 address from the list
Url Port	Enter the URL port for the device
Days of week	Choose Every Day, or Individual Days and select the checkboxes for the days of the week for which the policy applies
From	Enter the times for the policy to be in effect
To	

2 Select the Access Control checkbox.

3 Click on the plus sign (+) to add a policy.

A separate panel displays for configuring the policy name, IP address of the device, and dates and times for the policy.

4 Configure the parental control policy.

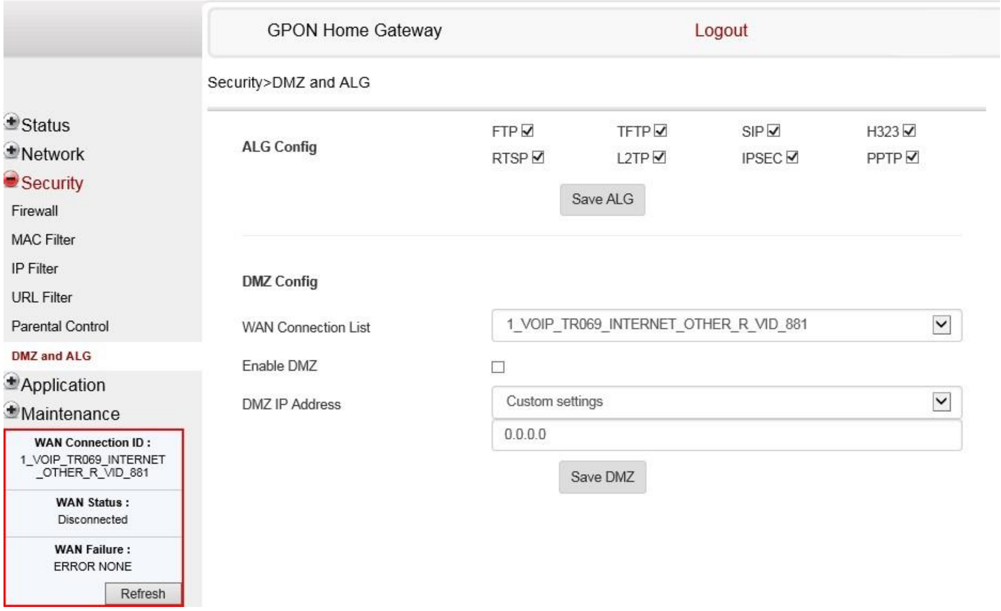
5 Click Enable to activate the policy.

6 STOP. This procedure is complete.

Procedure 33 DMZ and ALG configuration

1 Select Security > DMZ and ALG from the top-level menu in the GPON Home Gateway window, as shown in Figure 52.

Figure 52 DMZ and ALG window



ALG Config: FTP ☑ TFTP ☑ SIP ☑ H323 ☑ RTSP ☑ L2TP ☑ IPSEC ☑ PPTP ☑

DMZ Config

WAN Connection List: 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

Enable DMZ: □

DMZ IP Address: Custom settings, 0.0.0.0

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 44 describes the fields in the DMZ and ALG window.

Table 44 DMZ and ALG parameters

Field	Description
ALG Config	Select the checkboxes to enable the protocols to be supported by the ALG: FTP, TFTP, SIP, H323, RTSP, L2TP, IPSEC, PPTP
DMZ Config	
WAN Connection List	Choose a WAN connection from the drop-down menu
Enable DMZ	Select this checkbox to enable DMZ on the chosen WAN connection
DMZ IP Address	Choose Customer Setting and enter the DMZ IP address or choose the IP address of a connected device from the drop-down menu

2 Configure ALG.

3 Click Save ALG.

4 Configure DMZ.

5 Click Save DMZ.

6 STOP. This procedure is complete.

Procedure 34 Access control configuration

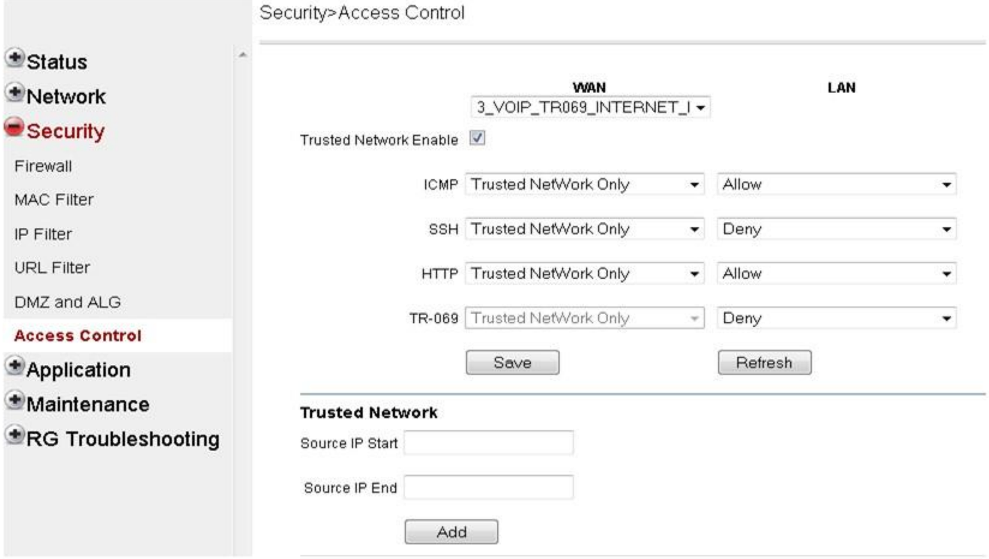
This procedure describes how to configure the access control level (ACL).

Note 1 — ACL takes precedence over the firewall policy.

Note 2 — The trusted network object will be shared for all WAN connections; it is not applied individually to a WAN connection.

1 Select Security > Access Control from the top-level menu in the GPON Home Gateway window, as shown in Figure 53.

Figure 53 Access Control window



WAN: 3_VOIP_TR069_INTERNET_I

Trusted Network Enable ☑

	WAN	LAN
ICMP	Trusted NetWork Only	Allow
SSH	Trusted NetWork Only	Deny
HTTP	Trusted NetWork Only	Allow
TR-069	Trusted NetWork Only	Deny

Source IP Start

Source IP End

Table 45 describes the fields in the Access Control window.

Table 45 Access control parameters

Field	Description
WAN	Choose a connection from the drop-down menu
Trusted Network Enable	Click the checkbox to enable or disable
ICMP, SSH, HTTP, TR-069	Select an access control level for each protocol: WAN side: Allow, Deny, or Trusted Network Only LAN side: Allow or Deny

Trusted Network	
Source IP Start	Enter a start IP address for the new subnet trusted network
Source IP End	Enter an end IP address for the new subnet trusted network

(2 of 2)

2 Select a WAN connection from the drop-down menu.

3 Click to enable or disable Trusted Network.

4 Select an access control level for each of the four protocols: ICMP, SSH, HTTP, and TR-069 for both the WAN and the LAN side.

5 Click Save.

6 Optionally, add one or more subnet trusted networks.

The maximum number of entries is 32.

You can also use the Source IP fields to delete a previously created entry for a subnet trusted network.

7 STOP. This procedure is complete.

8.2.5 Application configuration

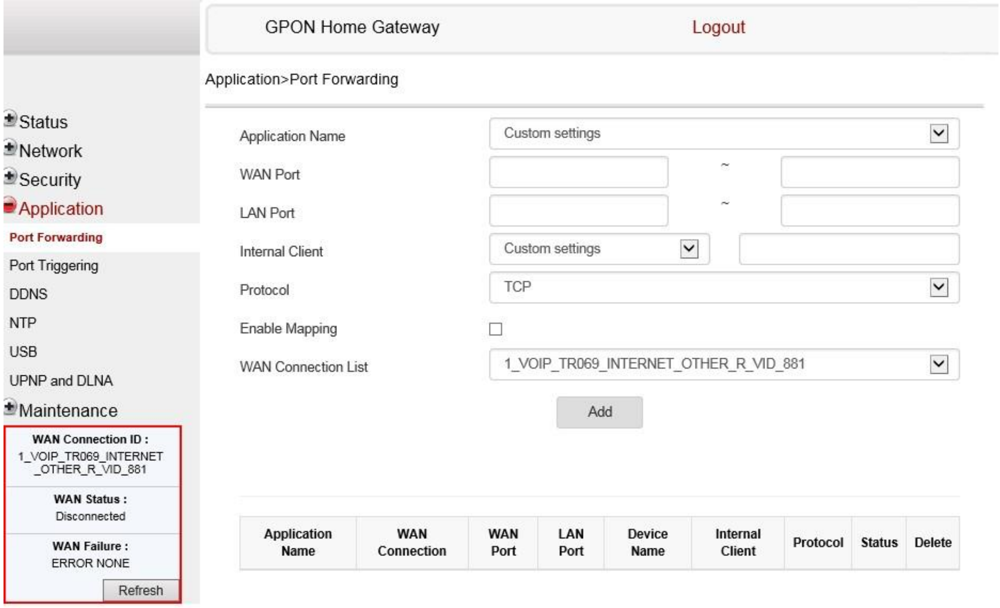
G-240W-J ONTs support application configuration, including:

- port forwarding
- port triggering
- DDNS
- NTP
- USB
- UPnP and DLNA
- voice setting

Procedure 35 Port forwarding configuration

1 Select Application > Port forwarding from the top-level menu in the GPON Home Gateway window, as shown in Figure 54.

Figure 54 **Port forwarding window**



Application Name: Custom settings

WAN Port: ~

LAN Port: ~

Internal Client: Custom settings

Protocol: TCP

Enable Mapping □

WAN Connection List: 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

Application Name	WAN Connection	WAN Port	LAN Port	Device Name	Internal Client	Protocol	Status	Delete

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 46 describes the fields in the port forwarding window.

Table 46 **Port forwarding parameters**

Field	Description
Application Name	Choose an application name from the drop-down menu
WAN Port	WAN port range
LAN Port	LAN port range
Internal Client	Choose a connected device from the drop-down menu and enter the associated IP address
Protocol	Choose the port forwarding protocol from the drop-down menu: • TCP • UDP • TCP/UDP
Enable Mapping	Select this checkbox to enable mapping
WAN Connection List	Choose a WAN connection from the drop-down menu Note: only active devices are shown on this menu

2 Configure port forwarding.

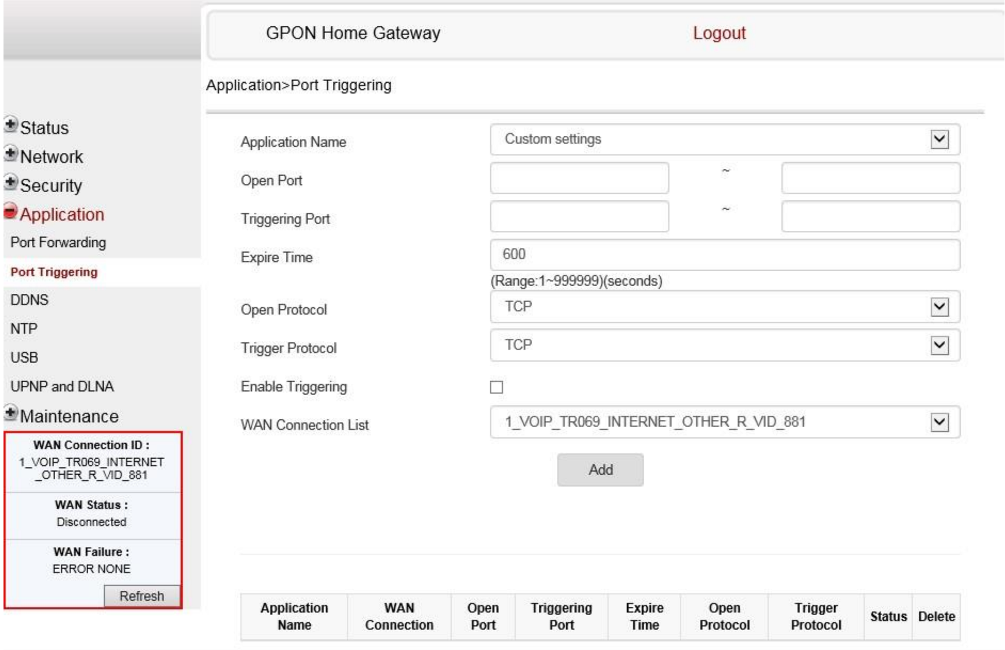
3 Click Add.

4 STOP. This procedure is complete.

Procedure 36 Port triggering

1 Select Application > Port Triggering from the top-level menu in the GPON Gateway window, as shown in Figure 55.

Figure 55 Port Triggering window



Application>Port Triggering

Application Name	Custom settings
Open Port	~
Triggering Port	~
Expire Time	600 (Range:1~999999)(seconds)
Open Protocol	TCP
Trigger Protocol	TCP
Enable Triggering	□
WAN Connection List	1_VOIP_TR069_INTERNET_OTHER_R_VID_881

Application Name	WAN Connection	Open Port	Triggering Port	Expire Time	Open Protocol	Trigger Protocol	Status	Delete

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 47 describes the fields in the Port Triggering window.

Table 47 Port triggering parameters

Field	Description
Application Name	Choose an application name from the drop-down menu
Open Port	Enter the open port range
Triggering Port	Enter the triggering port range
Expire Time	Enter the expiration time in seconds

(1 of 2)

Field	Description
Open Protocol	Choose the open port protocol from the drop-down menu: • TCP • UDP • TCP/UDP
Trigger Protocol	Choose the triggering port protocol from the drop-down menu: • TCP • UDP • TCP/UDP
Enable Triggering	Select this checkbox to enable port triggering
WAN Connection List	Choose a WAN connection from the drop-down menu Note: only active devices are shown on this menu

(2 of 2)

2 Configure port triggering.

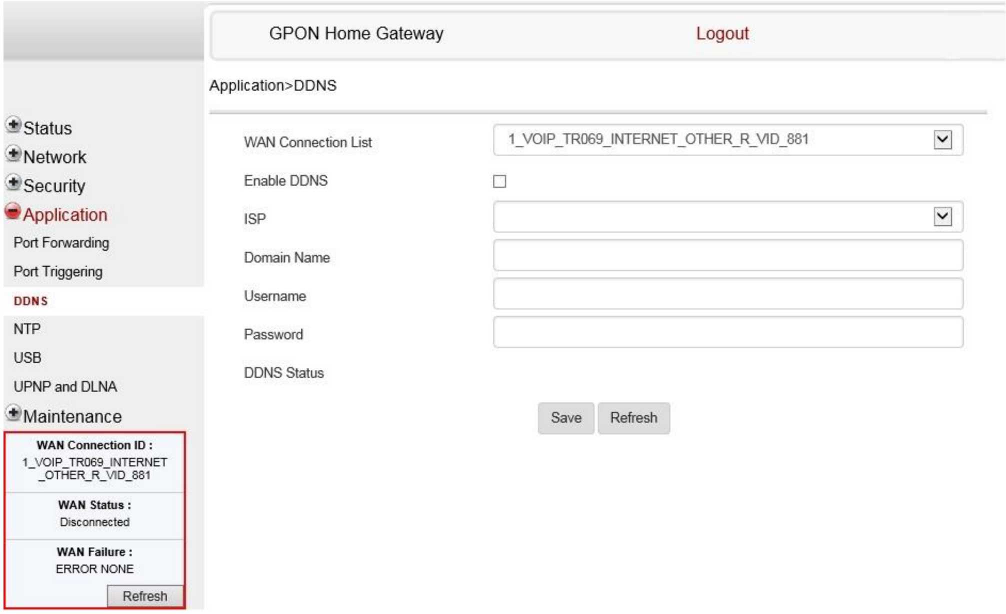
3 Click Add.

4 STOP. This procedure is complete.

Procedure 37 DDNS configuration

1 Select Application > DDNS from the top-level menu in the GPON Home Gateway window, as shown in Figure 56.

Figure 56 **DDNS window**



WAN Connection List: 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

Enable DDNS: □

ISP:

Domain Name:

Username:

Password:

DDNS Status:

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 48 describes the fields in the DDNS window.

Table 48 **DDNS parameters**

Field	Description
WAN Connection List	Choose a WAN connection from the drop-down menu
Enable DDNS	Select this checkbox to enable DDNS on the chosen WAN connection
ISP	Choose an ISP from the drop-down menu.
Domain Name	Domain name
Username	Username
Password	Password
DDNS Status	Displays the status of the DDNS: Synchronized, Synchronization failed, or blank if no update message has been received from the ISP.

2 Configure DDNS.

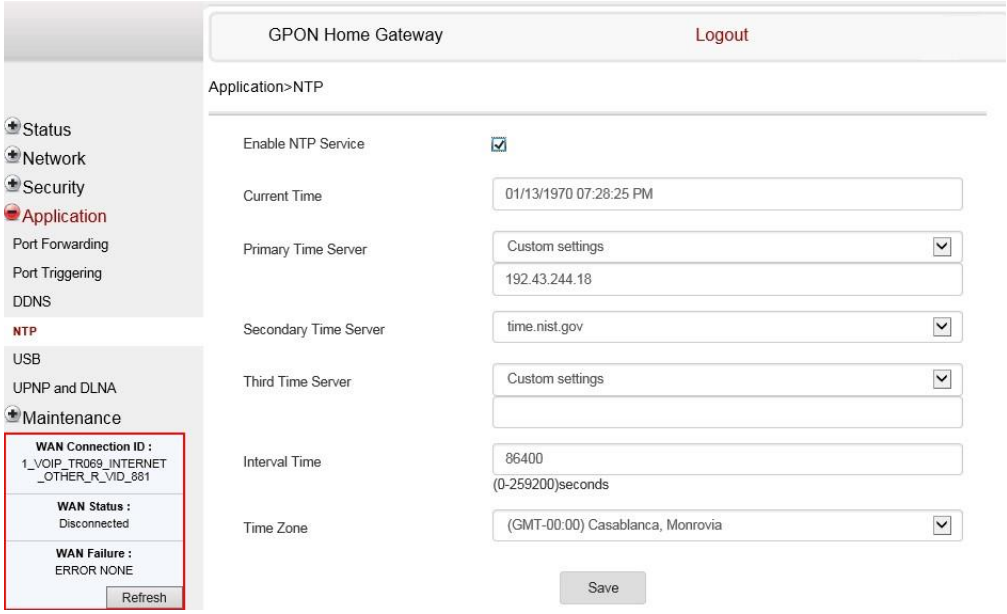
3 Click Save.

4 STOP. This procedure is complete.

Procedure 38 NTP configuration

1 Select Application > NTP from the top-level menu in the GPON Home Gateway window, as shown in Figure 57.

Figure 57 **NTP window**



Application>NTP

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Enable NTP Service	☑
Current Time	01/13/1970 07:28:25 PM
Primary Time Server	Custom settings 192.43.244.18
Secondary Time Server	time.nist.gov
Third Time Server	Custom settings
Interval Time	86400 (0-259200)seconds
Time Zone	(GMT-00:00) Casablanca, Monrovia

Table 49 describes the fields in the NTP window.

Table 49 **NTP parameters**

Field	Description
Enable NTP Service	Select this checkbox to enable NTP service
Current Time	Enter the current local date and time
Primary Time Server	Choose a time server from the drop-down menu or choose Customer setting and enter the address of the time server.
Secondary Time Server	Choose a time server from the drop-down menu or choose Customer setting and enter the address of the time server.

(1 of 2)

Field	Description
Third Time Server	Choose a time server from the drop-down menu or choose Customer setting and enter the address of the time server.
Interval Time	Interval at which to get the time from the time server, in seconds
Time Zone	Choose the local time zone from the drop-down menu

(2 of 2)

2 Configure NTP.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 39 USB configuration

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

Note — Due to image size limitations, some OLTs may not be able to support the Samba server feature.

For this reason, two types of ONT software images are available: the Premium Image supports the FTP, SFTP, and Samba features; the Advanced Image supports the FTP and SFTP features but does not support the Samba server feature.

For more information, contact your Nokia representative.

You can also use the USB menu to enable and disable USB printer sharing across clients on the LAN.

The USB connected devices are shown in overview table on the bottom of the USB window.

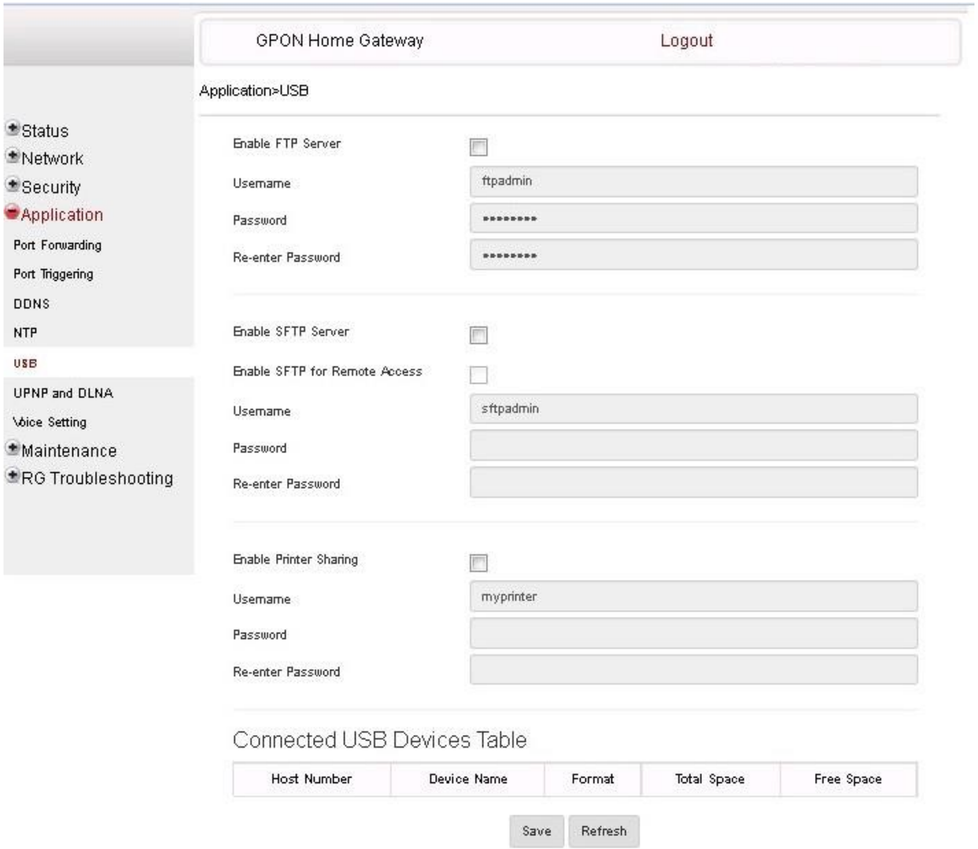
The device incorporates a CUPS server to enable USB printer sharing across the LAN by using the RAW print-through protocol. When a USB printer is connected to the device, it can be configured on LAN clients by referring to

```
http://<hostname>:631/printers/<printer_name>
```

as a shared printer, where <hostname> refers to the DNS name or the IP address of the device and the <printer_name> is displayed in the connected USB device table of the USB page. The USB printer driver must be installed on the LAN client to execute print jobs. When an error prevents the print job from being completed, a generic error message is returned to the LAN client. Up to four print jobs at a time are supported.

1 Select Application > USB from the top-level menu, as shown in Figure 58.

Figure 58 **USB window**



Application>USB

Enable FTP Server ☐
Username ftpadmin
Password ********
Re-enter Password ********

Enable SFTP Server ☐
Enable SFTP for Remote Access ☐
Username sftpadmin
Password
Re-enter Password

Enable Printer Sharing ☐
Username myprinter
Password
Re-enter Password

Connected USB Devices Table

Host Number	Device Name	Format	Total Space	Free Space

Table 50 describes the fields in the USB window.

Table 50 **USB parameters**

Field	Description
Enable FTP server	Select this checkbox to enable using an FTP server
Username	Username for the FTP server
Password	Password for the FTP server

(1 of 2)

Field	Description

Re-enter Password	Password for the FTP server
Enable SFTP Server	Select this checkbox to enable using an SFTP server
Enable SFTP for Remote Access	Select this checkbox to enable SFTP for remote access
Username	Username for the SFTP server
Password	Password for the SFTP server
Re-enter Password	Password for the SFTP server
Enable Printer Sharing	Select this checkbox to enable printer sharing Printer sharing is disabled by default
Username	Username for printer sharing
Password	Password for printer sharing
Re-enter Password	Password for printer sharing
Connected USB Devices Table	For each printer that is connected to the ONT, the following fields are displayed: • Host Number—for example: Printer1, Printer2 • Device Name—name or identification for the USB device • Format—for a USB printer, the printing protocol is RAW; for a USB storage device, this field displays the storage format • Total space—applies only to a USB storage device • Free space—applies only to a USB storage device

(2 of 2)

2 Configure the USB.

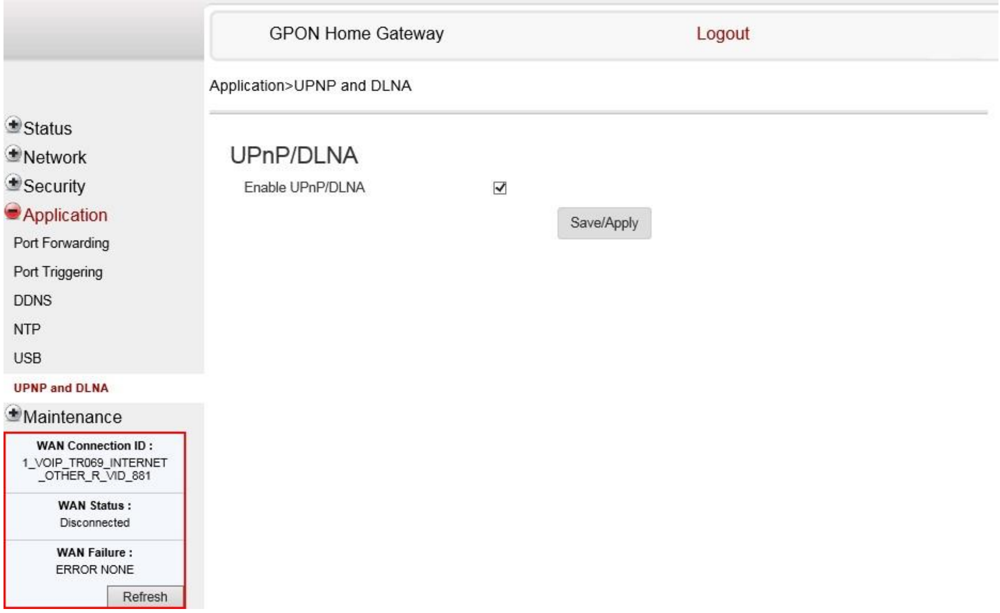
3 Click Save.

4 STOP. This procedure is complete.

Procedure 40 UPnP and DLNA configuration

1 Select Application > UPnP and DLNA from the top-level menu in the GPON Home Gateway window, as shown in Figure 59.

Figure 59 **UPnP and DLNA window**



UPnP/DLNA

Enable UPnP/DLNA ☑

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

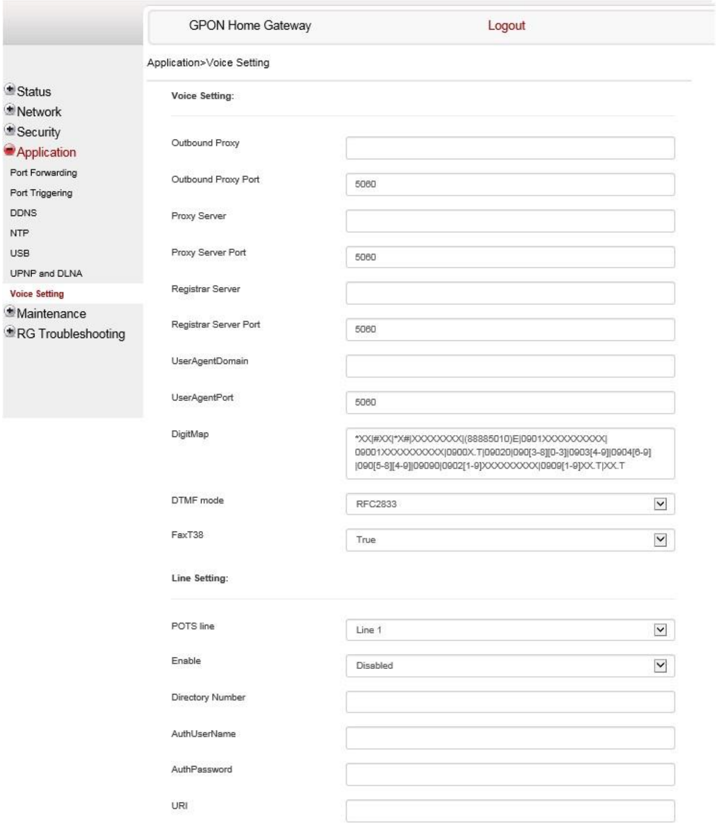
2 Select the Enable UPnP/DLNA checkbox to enable UPnP/DLNA.

3 Click Save/Apply.

4 STOP. This procedure is complete.

Procedure 41 Voice setting

1 Select Application > Voice Setting from the top-level menu in the GPON Home Gateway window, as shown in Figure 60.



Application>Voice Setting

Voice Setting:

Outbound Proxy

Outbound Proxy Port 5060

Proxy Server

Proxy Server Port 5060

Registrar Server

Registrar Server Port 5060

UserAgentDomain

UserAgentPort 5060

DigitMap *XX|#XX|*X#|XXXXXXXX|(88885010)E|0901XXXXXXXXXX|09001XXXXXXXXXX|0900X.T|09020|090[3-8][0-3]|0903[4-9]|0904[6-9]|090[5-8][4-9]|09090|0902[1-9]XXXXXXXXX|0909[1-9]XX.T|XX.T

DTMF mode RFC2833

FaxT38 True

Line Setting:

POTS line Line 1

Enable Disabled

Directory Number

AuthUserName

AuthPassword

URI

Figure 60 Voice setting window

Table 51 describes the fields in the Voice Setting window.

Table 51 Voice setting parameters

Field	Description
Voice Setting	
Outbound Proxy	Enter the SIP outbound proxy
Outbound Proxy Port	Enter the outbound proxy port
Proxy Server	Enter the proxy server
Proxy Server Port	Enter the proxy server port
Registrar Server	Enter the registrar server

(1 of 2)

Registrar Server Port	Enter the registrar server port
UserAgentDomain	Enter the user agent domain
UserAgentPort	Enter the user agent port
DigitMap	A string of characters with a length limit of 1024 bytes. A dial plan can consist of several dial plan tokens. Each token is a component of the overall dial plan.
DTMF Mode	Choose InBand, RFC2833 or Auto from the drop-down menu
FaxT38	Choose False or True from the drop-down menu
Line Setting	
POTS line	Choose a POTS line from the drop-down menu
Enable	Choose Enabled or Disabled from the drop-down menu
Directory Number	Enter a directory number
AuthUserName	Enter an authorized user name
AuthPassword	Enter a password for the user
URI	The Uniform Resource Identifier of the SIP URL

(2 of 2)

2 Configure voice setting.

3 Click Save.

4 STOP. This procedure is complete.

8.2.6 Maintenance

G-240W-J ONTs support maintenance tasks, including:

- change password
- test WAN speed
- configure LOID
- configure SLID
- manage device
- backup and restore
- upgrade firmware

- reboot device
- restore factory defaults
- diagnose WAN connections
- view log
- diagnose PPPoE connection

Procedure 42 Password configuration

A password must adhere to the password rules, which are as follows:

- 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

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

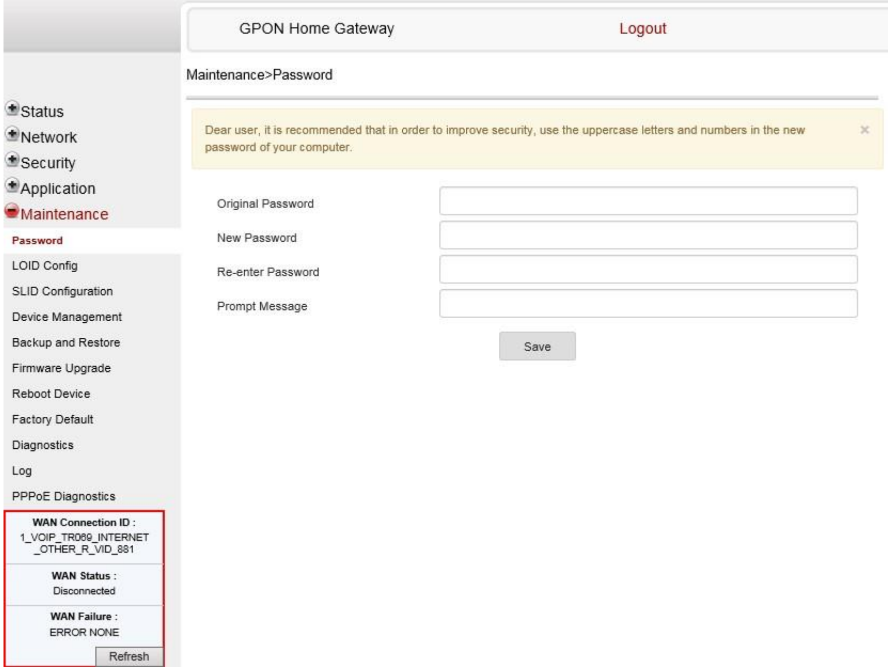
When the password does not meet the password rules, the application displays a message to indicate which password rule has not been followed, for example:

- 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 Select Maintenance > Password from the top-level menu in the GPON Home Gateway window, as shown in Figure 61.

Figure 61 **Password window**



Dear user, it is recommended that in order to improve security, use the uppercase letters and numbers in the new password of your computer.

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 52 describes the fields in the password window.

Table 52 **Password parameters**

Field	Description
Original Password	Current password
New Password	New password (must adhere to the password rules described above)
Re-enter password	Must match the new password entered above exactly
Prompt message	Password prompt message

2 Configure the new password.

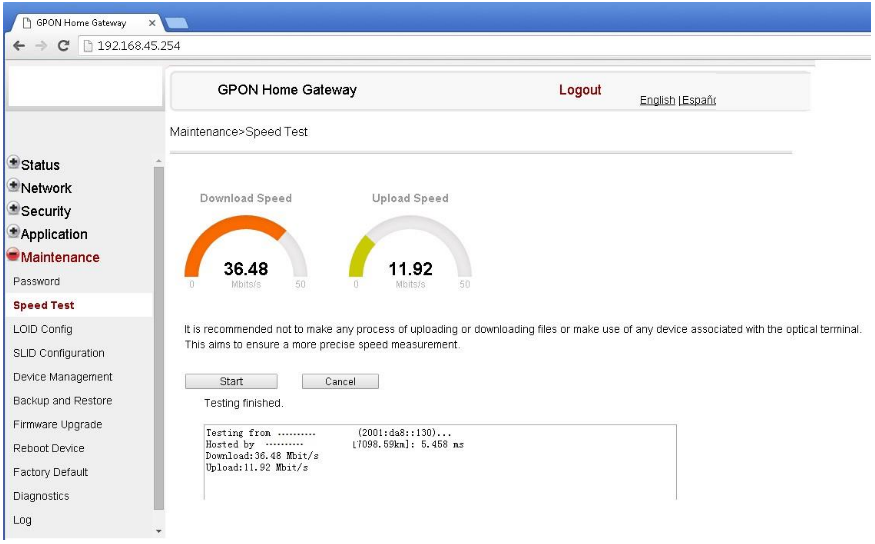
3 Click Save.

4 STOP. This procedure is complete.

Procedure 43 WAN speed test

1 Select Maintenance > Speed Test from the top-level menu in the GPON Home Gateway window, as shown in Figure 62.

Figure 62 **Speed Test window**



It is recommended not to make any process of uploading or downloading files or make use of any device associated with the optical terminal. This aims to ensure a more precise speed measurement.

Testing finished.

```
Testing from ..........        (2001:da8::130)...
Hosted by  ..........         [7098.59km]: 5.458 ms
Download:36.48 Mbit/s
Upload:11.92 Mbit/s
```

2 Click Start to start the speed test.

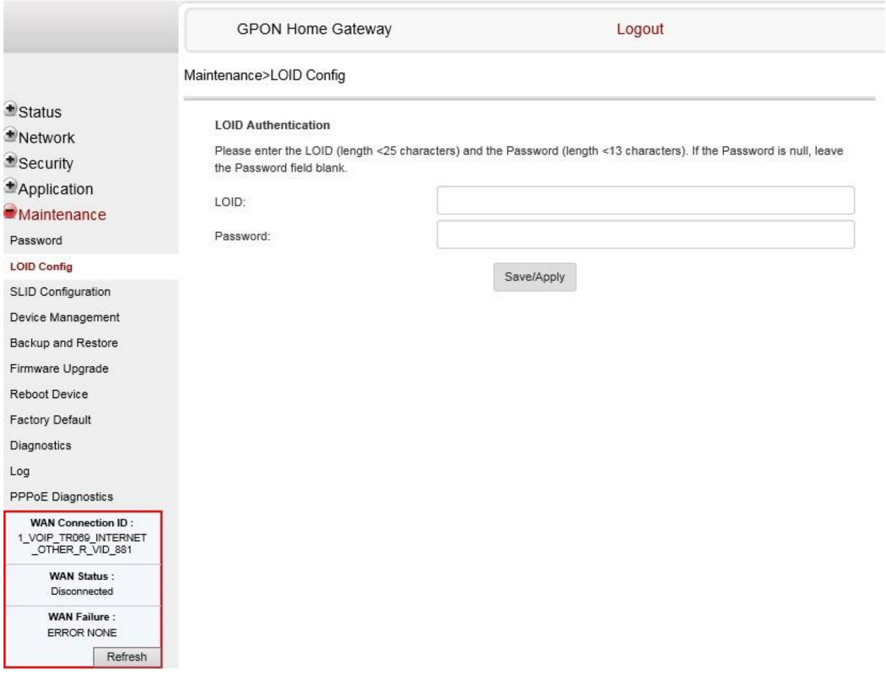
Enter the URL for the test server in the pop-up window.

3 STOP. This procedure is complete.

Procedure 44 LOID configuration

1 Select Maintenance > LOID Config from the top-level menu in the GPON Home Gateway window, as shown in Figure 63.

Figure 63 LOID Config window



Maintenance>LOID Config

LOID Authentication

Please enter the LOID (length <25 characters) and the Password (length <13 characters). If the Password is null, leave the Password field blank.

LOID:

Password:

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 53 describes the fields in the LOID configuration window.

Table 53 LOID configuration parameters

Field	Description
LOID	Type the LOID; the maximum number of characters is 24 If the password is null, this field may be left blank
Password	Type the password; the maximum number of characters is 12

2 Configure the LOID.

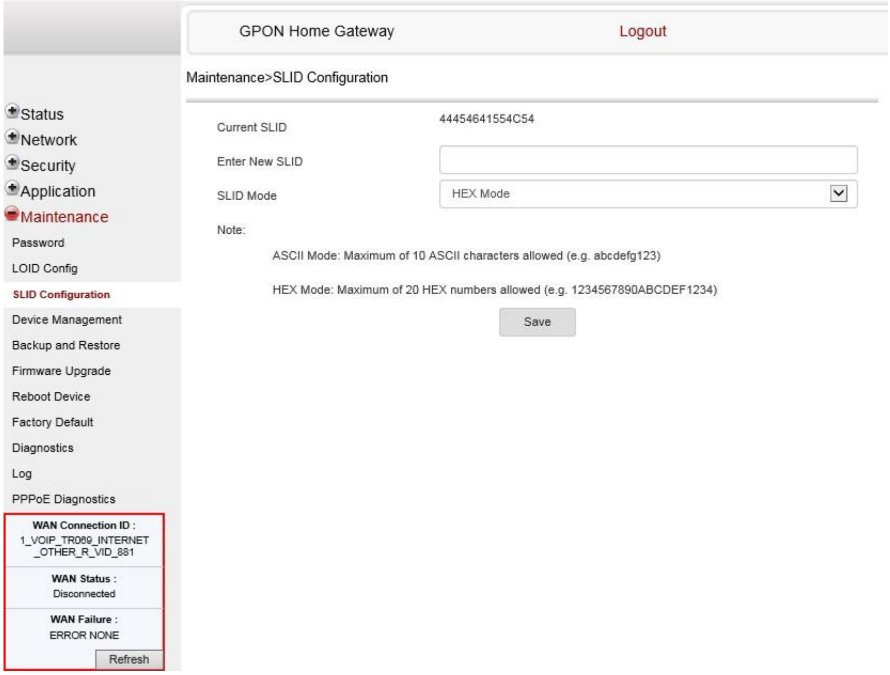
3 Click Save/Apply.

4 STOP. This procedure is complete.

Procedure 45 SLID configuration

1 Select Maintenance > SLID Configuration from the top-level menu in the GPON Home Gateway window, as shown in Figure 64.

Figure 64 **SLID configuration window**



Maintenance>SLID Configuration

Current SLID 44454641554C54

Enter New SLID

SLID Mode HEX Mode

Note:

ASCII Mode: Maximum of 10 ASCII characters allowed (e.g. abcdefg123)

HEX Mode: Maximum of 20 HEX numbers allowed (e.g. 1234567890ABCDEF1234)

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 54 describes the fields in the SLID configuration window.

Table 54 **SLID configuration parameters**

Field	Description
Current SLID	Displays current SLID
Enter new SLID	Input new SLID
SLID Mode	Choose a SLID mode from the drop-down menu

2 Configure the new SLID.

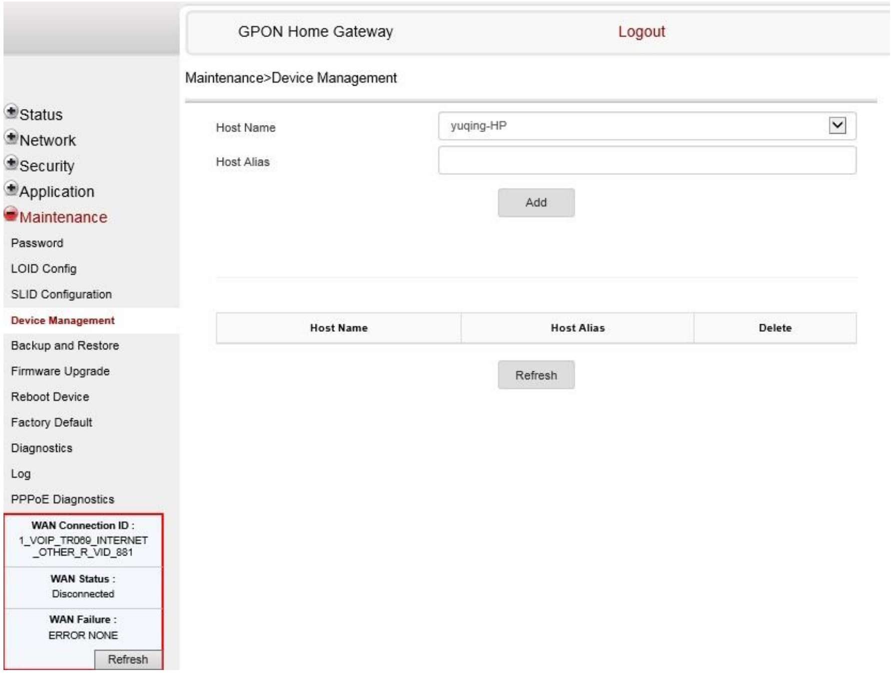
3 Click Save.

4 STOP. This procedure is complete.

Procedure 46 Device management

1 Select Maintenance > Device Management from the top-level menu in the GPON Home Gateway window, as shown in Figure 65.

Figure 65 **Device management window**



Maintenance>Device Management

Host Name: yuqing-HP

Host Alias:

Host Name	Host Alias	Delete

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 55 describes the fields in the Device management window.

Table 55 **Device management parameters**

Field	Description
Host Name	Choose a host from the drop-down menu
Host Alias	Enter an alias for the chosen host

Procedure 47

2 Configure an alias for a specific host.

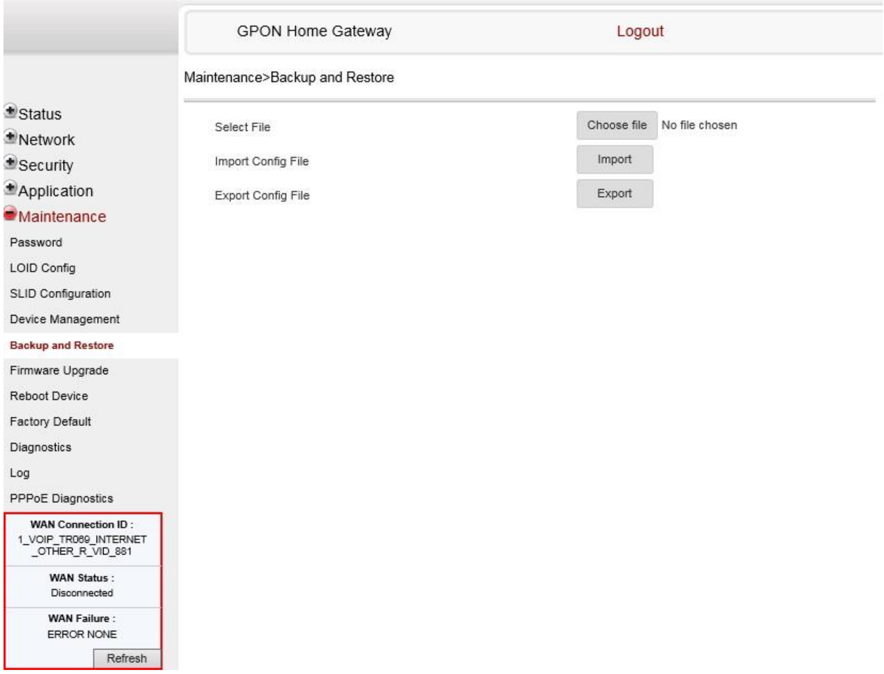
3 Click Add.

4 STOP. This procedure is complete.

Backup and restore

1 Select Maintenance > Backup and Restore from the top-level menu in the GPON Home Gateway window, as shown in Figure 66.

Figure 66 **Backup and Restore window**



No file chosen

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

2 Click Choose file and select a backup file.

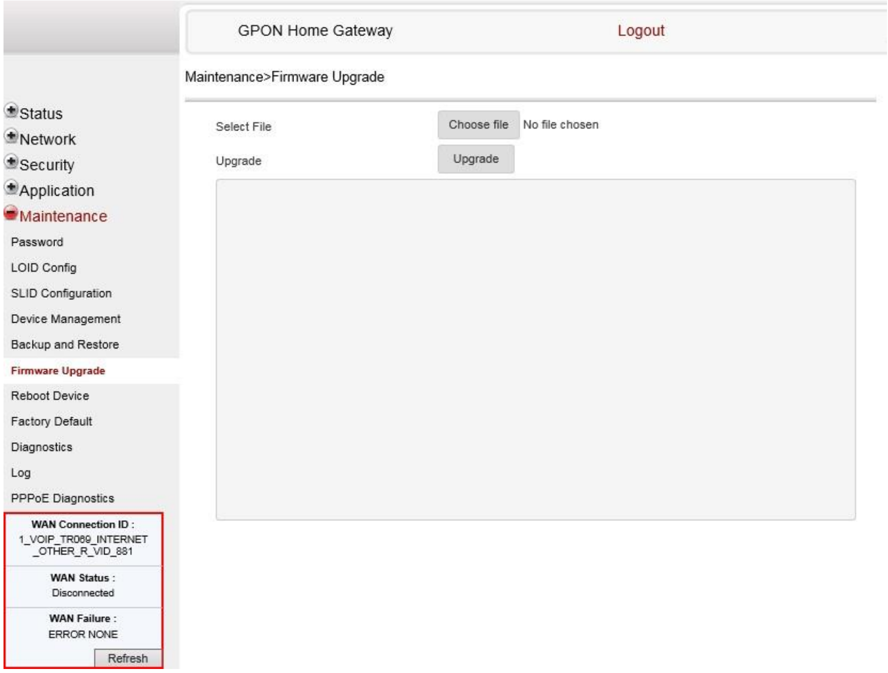
3 Click Import Config File to restore the ONT to the saved backup or click Export Config File to export the current ONT configuration to the backup file.

4 STOP. This procedure is complete.

Procedure 48 Upgrade firmware

1 Select Maintenance > Firmware Upgrade from the top-level menu in the GPON Home Gateway window, as shown in Figure 67.

Figure 67 **Firmware upgrade window**



No file chosen

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

2 Click Choose file and select the firmware file.

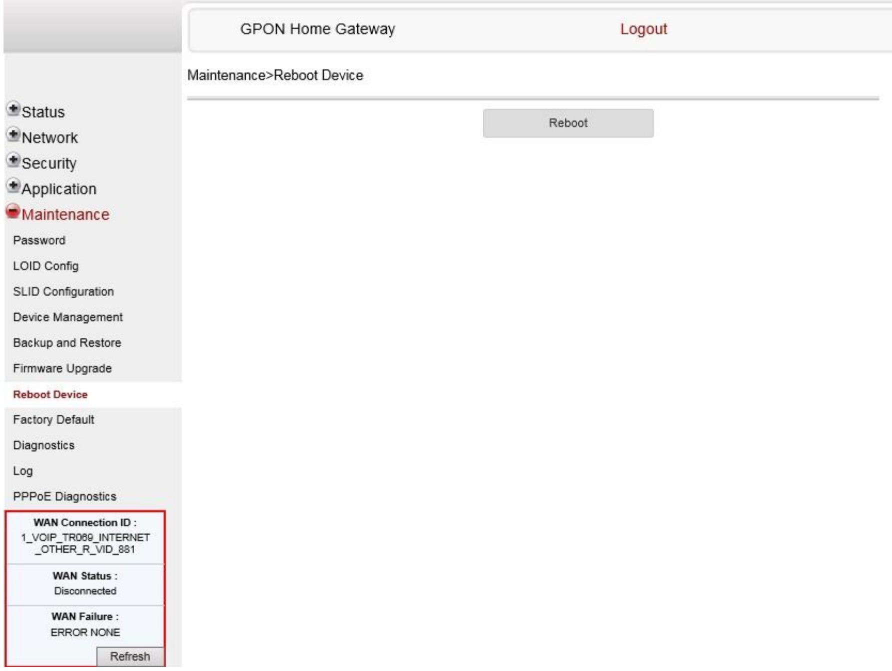
3 Click Upgrade to upgrade the firmware.

4 STOP. This procedure is complete.

Procedure 49 Reboot ONT

1 Select Maintenance > Reboot Device from the top-level menu in the GPON Home Gateway window, as shown in Figure 68.

Figure 68 **Reboot window**



WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

2 Click Reboot to reboot the ONT.

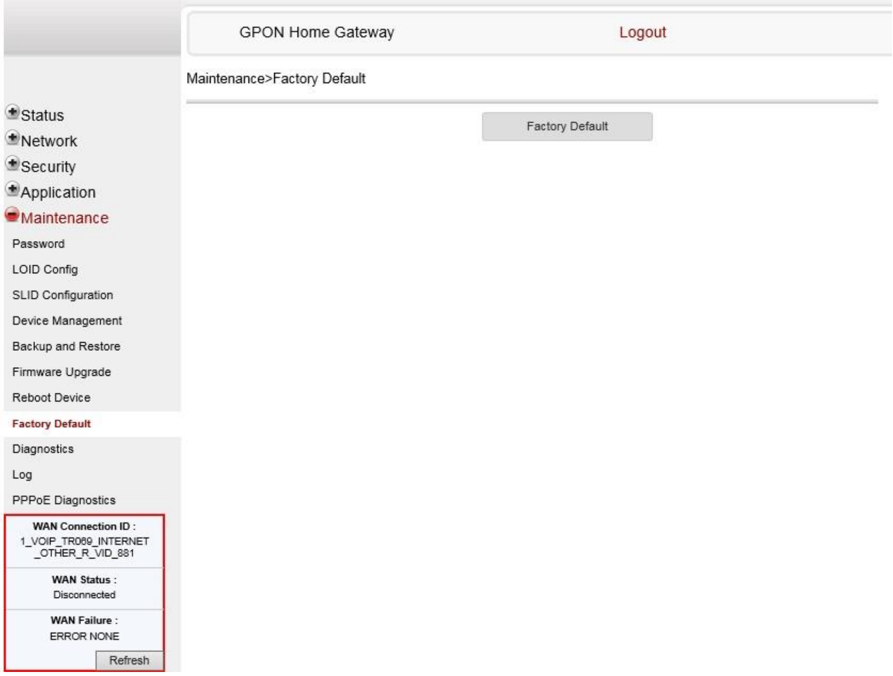
3 STOP. This procedure is complete.

Procedure 50 Restore factory defaults

Select Maintenance > Factory Default from the top-level menu in the GPON Home Gateway window, as shown in Figure 69.

1

Figure 69 **Factory default window**



WAN Connection ID :
1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

2 Click Factory Default to reset the ONT to its factory default settings.

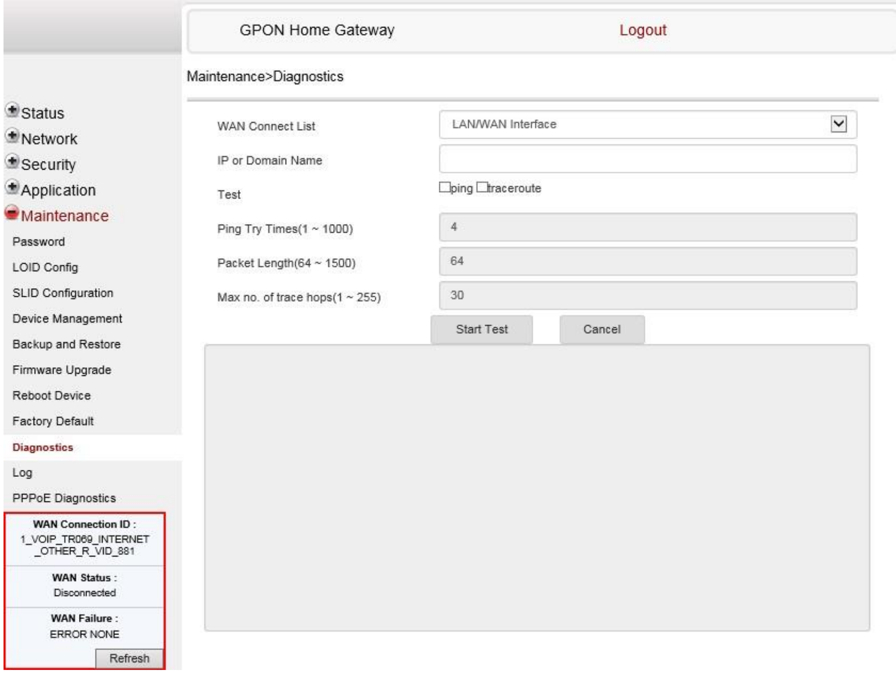
3 STOP. This procedure is complete.

Procedure 51 Diagnose WAN connections

Select Maintenance > Diagnose from the top-level menu in the GPON Home Gateway window, as shown in Figure 70.

1

Figure 70 **Diagnose window**



WAN Connect List: LAN/WAN Interface

IP or Domain Name:

Test: □ping □traceroute

Ping Try Times(1 ~ 1000): 4

Packet Length(64 ~ 1500): 64

Max no. of trace hops(1 ~ 255): 30

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

2 Choose a WAN connection to diagnose from the drop-down menu.

3 Enter the IP address or domain name.

4 Select the test type: ping, traceroute, or both.

5 Enter the number of ping attempts to perform (1 - 1000); the default is 4.

6 Enter a ping packet length (64-1024); the default is 64.

7 Enter the maximum number of trace hops (1-255); the default is 30.

8 Click Start Test. Results will be displayed at the bottom of the window.

Procedure 52

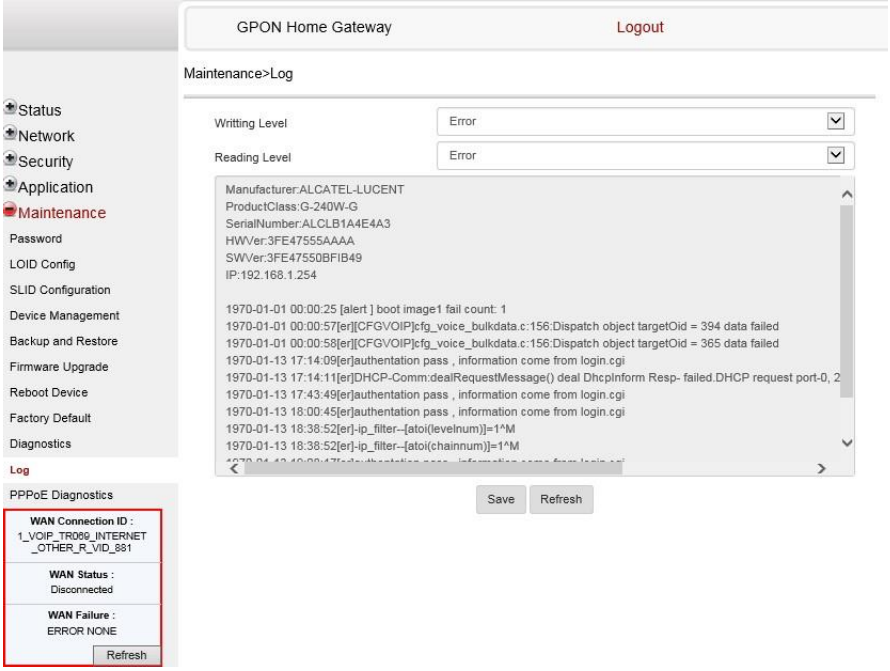
9 Click Cancel to cancel the test.

10 STOP. This procedure is complete.

View log files

1 Select Maintenance > Log from the top-level menu in the GPON Home Gateway window, as shown in Figure 71.

Figure 71 **Log window**



Writting Level: Error

Reading Level: Error

```
Manufacturer:ALCATEL-LUCENT
ProductClass:G-240W-G
SerialNumber:ALCLB1A4E4A3
HWVer:3FE47555AAAA
SWVer:3FE47550BFIB49
IP:192.168.1.254

1970-01-01 00:00:25 [alert ] boot image1 fail count: 1
1970-01-01 00:00:57[er][CFGVOIP]cfg_voice_bulkdata.c:156:Dispatch object targetOid = 394 data failed
1970-01-01 00:00:58[er][CFGVOIP]cfg_voice_bulkdata.c:156:Dispatch object targetOid = 365 data failed
1970-01-13 17:14:09[er]authentation pass , information come from login.cgi
1970-01-13 17:14:11[er]DHCP-Comm:dealRequestMessage() deal DhcpInform Resp- failed.DHCP request port-0, 2
1970-01-13 17:43:49[er]authentation pass , information come from login.cgi
1970-01-13 18:00:45[er]authentation pass , information come from login.cgi
1970-01-13 18:38:52[er]-ip_filter--[atoi(levelnum)]=1^M
1970-01-13 18:38:52[er]-ip_filter--[atoi(chainnum)]=1^M
```

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

2 Choose a write level from the drop-down menu to determine which types of events are recorded in the log file:

- Emergency
- Alert
- Critical
- Error

- Warning
- Notice
- Informational
- Debug

3 Choose a reading level from the drop-down menu to determine which types of events to display from the log file:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug

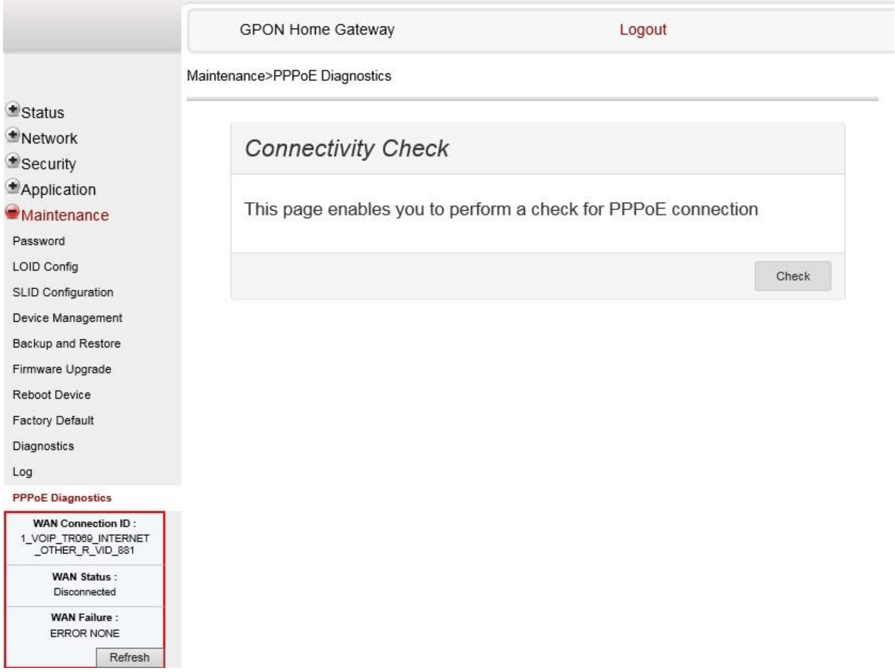
4 The log file is displayed at the bottom of the window.

5 STOP. This procedure is complete.

Procedure 53 Diagnose PPPoE connections

1 Select Maintenance > PPPoE Diagnostics from the top-level menu in the GPON Home Gateway window, as shown in Figure 72.

Figure 72 **PPPoE Diagnostics window**



Connectivity Check

This page enables you to perform a check for PPPoE connection

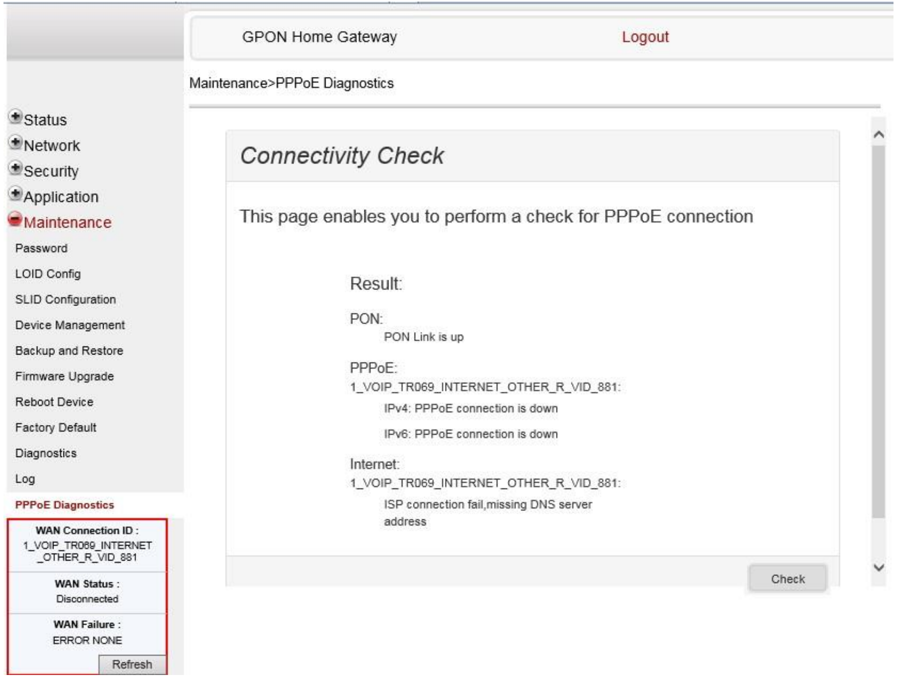
WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

2 Click Check to view the results for the PPPoE diagnostics, as shown in Figure 73.

Figure 73 **PPPoE diagnostics results**



Connectivity Check

This page enables you to perform a check for PPPoE connection

```
Result:
PON:
        PON Link is up
PPPoE:
1_VOIP_TR069_INTERNET_OTHER_R_VID_881:
        IPv4: PPPoE connection is down
        IPv6: PPPoE connection is down
Internet:
1_VOIP_TR069_INTERNET_OTHER_R_VID_881:
        ISP connection fail,missing DNS server
        address
```

WAN Connection ID : 1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Table 56 describes the fields on the PPPoE diagnostics results window.

Table 56 **PPPoE diagnostics results parameters**

Field	Description
PON	Reports whether the PON link is up or down
PPPoE	Reports whether the PPPoE IPv4 or IPv6 connection is up, connecting, down, not configured, or not found
Internet	For each Internet connection, reports whether the connection succeeded, failed (missing DNS address), or was not found; also reports failures due to packet loss higher than the threshold of 30

3 STOP. This procedure is complete.

8.2.7 RG troubleshooting counters

The Troubleshooting Counters feature enables service providers and end users to monitor the performance of their broadband connection.

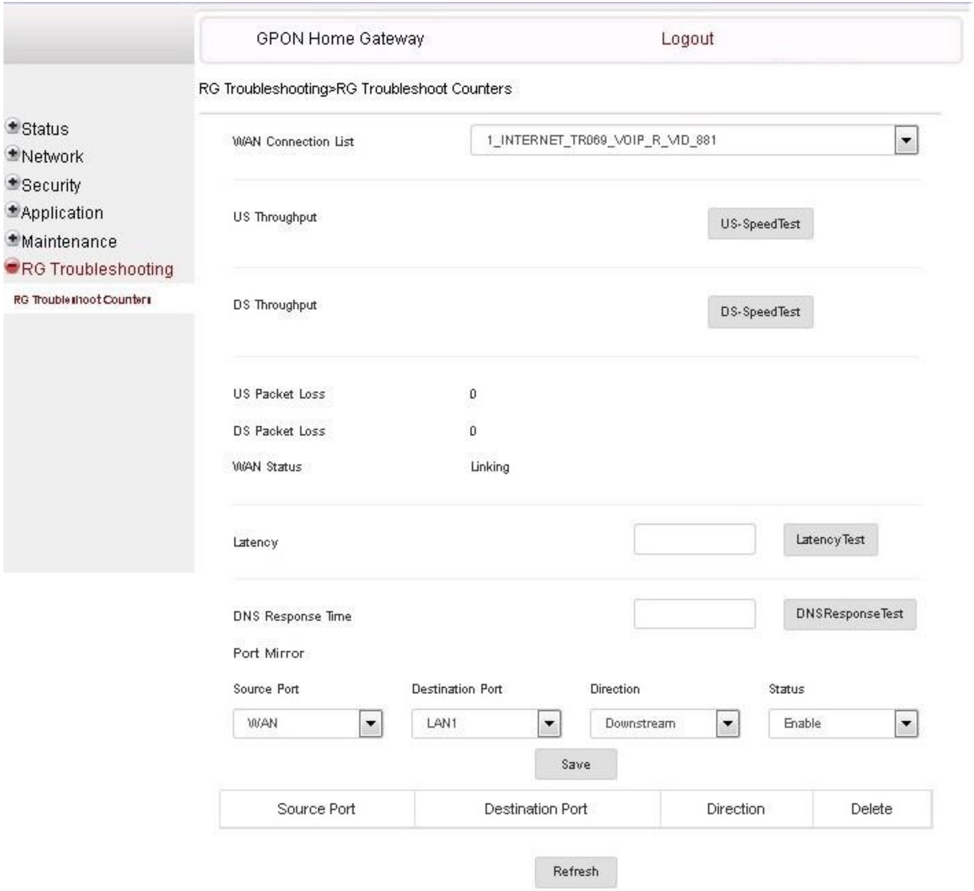
Tests are run to retrieve upstream and downstream throughput, latency, and DNS response time. The Troubleshooting Counters window also displays upstream and downstream packet loss and Internet status.

Procedure 54 Retrieve Residential Gateway (RG) troubleshooting counters

1 Select RG Troubleshooting Counters from the left menu in the GPON Home Gateway window.

The RG Troubleshooting Counters window appears; see Figure 74.

Figure 74 RG Troubleshooting Counters window



RG Troubleshooting>RG Troubleshoot Counters

WAN Connection List: 1_INTERNET_TR069_VOIP_R_VID_881

US Throughput

DS Throughput

US Packet Loss: 0

DS Packet Loss: 0

WAN Status: Linking

Latency

DNS Response Time

Port Mirror

Source Port	Destination Port	Direction	Status
WAN	LAN1	Downstream	Enable

Source Port	Destination Port	Direction	Delete

Table 57 describes the fields in the RG Troubleshooting Counters window.

Table 57 RG Troubleshooting Counters parameters

Field	Description
WAN Connection List	Choose a WAN connection from the list
US Throughput	This test is used to determine the upstream throughput/speed Click US Speed Test to specify the time for the upstream test The default is weekly, performed at idle to a public server
DS Throughput	This test is used to determine the downstream throughput/speed Click DS Speed Test to specify the time for the downstream test The default is weekly, performed at idle to a public server
US Packet Loss	The number of upstream packages lost
DS Packet Loss	The number of downstream packages lost

WAN Status	Whether the WAN linking is (UP) or not (DOWN)
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 The default is weekly, performed at idle to a public server
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 The default is weekly, performed at idle to a public server
Port Mirror	Choose the source and destination ports, the direction (Downstream or Upstream), and the status (Enable or Disable) from the drop-down menus, and click Save

2 Configure the test times if desired.

3 Click Refresh to update the data.

4 STOP. This procedure is complete.

9 ONT configuration file over OMCI

9.1 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.

9.2 Supported configuration file types

Table 58 describes the configuration file types that are supported from 7368 ISAM ONT R05.02.00 and later.

Table 58 **Supported configuration files**

File Index	Description	Details	Supported ONTs/DPU

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"	HGU ONTs: G-240G-C,G-240W-A, G-240W-B, G-240W-C, G-240W-G, G-240W-J, I-240W-A
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"	
XML	Voice XML file	The Voice XML file provides an alternate method for securely downloading voice parameters from the OLT, rather than using FTP (OMCIv1/OMCIv2) or HTTPS (TR-069). Downloading this file makes the applicable changes in the voice parameters. This file enables operators to change the voice behavior by downloading the updated voice XML file. Nokia recommends using this procedure, rather than embedded voice XML files. The Nokia defined index for the Voice XML file is: "XML"	

(1 of 2)

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"	HGU ONTs: G-240G-C,G-240W-A, G-240W-B, G-240W-C, G-240W-G, G-240W-J, I-240W-A

(2 of 2)

9.2.1 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.

9.3 ONT configuration file over OMCI

⚠ **Warning —** Executing the following procedure will trigger the ONT to reboot, which will impact ongoing services.

Use this procedure to configure ONTs using configuration files via OMCI.

Procedure 55

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:

i On a Linux platform, rename the raw configuration file to adhere to the naming convention, as described in section 9.2.

ii 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.

iii Rename *ABCXXXXVER* to *ABCXXXXVER*.org

2 **iv** Remove the “.tar” extension from *ABCXXXXVER*.tar file.

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: X can be 1 or 2 unless specified:

i If `pland-cfgfileX= Disabled` and `dnload-cfgfileX= Disabled` ,

no file will be downloaded to the ONT.

ii If `pland-cfgfileX=FILENAME1` and `dnload-cfgfileX= Disabled` , FILENAME1 will be downloaded and FILENAME1 will be made active. An ONT reboot is required.

iii If `pland-cfgfileX=Disabled` and `dnload-cfgfileX= FILENAME2`

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

iv If `pland-cfgfileX=FILENAME3` and `dnload-cfgfileX= FILENAME 4`, the OLT reports an error because the filenames are not the same.

v 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. **vi** If `pland-cfgfileX=Auto` and `dnload-cfgfileX= Auto`

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

4 STOP. This procedure is complete.

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.

Customer document and product support

Customer documentation

Customer Documentation Welcome Page

Technical Support

Customer Documentation Technical Support

Documentation feedback

Customer Documentation Feedback

3FE-48009-AAAA-TCZZA