



7368 Intelligent Services Access Manager ONT

7368 ISAM ONT G-240W-G Product Guide

3FE-47555-AAAA-TCZZA

Issue: 01

Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

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

© 2018 Nokia.

Contains proprietary/trade secret information which is the property of Nokia and must not be made available to, or copied or used by anyone outside Nokia without its written authorization. Not to be used or disclosed except in accordance with applicable agreements.

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 2, you must do what the step indicates.

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

- a** This is one option.
- b** This is another option.

2 You must perform this step.

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.

2 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

1	Preface	3
1.1	Scope	3
1.2	Audience.....	3
1.3	Required knowledge.....	3
1.4	Acronyms and initialisms	3
1.5	Assistance and ordering phone numbers	3
1.6	Nokia quality processes.....	4
1.7	Safety information.....	4
1.8	Documents	4
1.9	Special information	5
1.9.1	Procedures with options or substeps.....	6
1.10	Multiple PDF document search	7
2	ETSI ONT safety guidelines	17
2.1	Safety instructions	17
2.1.1	Safety instruction boxes	17
2.1.2	Safety-related labels.....	18
2.2	Safety standards compliance	19
2.2.1	EMC, EMI, and ESD compliance.....	19
2.2.2	Equipment safety standard compliance.....	19
2.2.3	Environmental standard compliance	20
2.2.4	CE RED RF Radiation Exposure Statement	20
2.2.5	Laser product standard compliance	20
2.2.6	Resistibility requirements compliance	20
2.2.7	Acoustic noise emission standard compliance	20
2.3	Electrical safety guidelines	21
2.3.1	Power supplies	21
2.3.2	Cabling	21
2.3.3	Protective earth	21
2.4	ESD safety guidelines	22
2.5	Laser safety guidelines.....	22
2.5.1	Laser classification	22
2.5.1.1	Laser warning labels.....	22
2.5.2	Laser classification	24
2.5.3	Transmit optical output	25
2.5.4	Normal laser operation	25
2.5.5	Location class.....	25
2.6	Environmental requirements.....	25
3	ETSI environmental and CRoHS guidelines.....	27
3.1	Environmental labels	27
3.1.1	Overview.....	27
3.1.2	Environmental related labels	27
3.1.2.1	Products below Maximum Concentration Value (MCV) label.....	27
3.1.2.2	Products containing hazardous substances above Maximum Concentration Value (MCV) label	28

3.2	Hazardous Substances Table (HST).....	29
3.3	Other environmental requirements	29
3.3.1	ONT environmental requirements	29
3.3.2	Storage	29
3.3.3	Transportation	30
3.3.4	Stationary use.....	30
3.3.5	Thermal limitations	30
3.3.6	Material content compliance.....	30
3.3.7	End-of-life collection and treatment.....	31
4	G-240W-G unit data sheet	33
4.1	G-240W-G part numbers and identification	33
4.2	G-240W-G general description.....	34
4.2.1	Configuring the G-240W-G to function as a single port ONT	36
4.2.2	Support for CFM over S-tunnel.....	36
4.2.3	TR-069 parameter support	37
4.2.3.1	Host object support.....	37
4.2.3.2	Port forwarding support	37
4.2.3.3	Optical parameters support	38
4.2.3.4	Object support for Wi-Fi parameters	38
4.2.3.5	Statistics and troubleshooting support.....	38
4.2.3.6	Diagnostic parameter support	38
4.2.3.7	Timing parameter support	39
4.2.4	Independent TR69 session with Saas.....	39
4.2.5	TR69 authentication using TLS and CA certificates	39
4.2.6	TR-104 parameter extension support for voice service.....	39
4.2.7	TR-104 voice-related alarms	40
4.2.8	TR-104 parameters for FX line testing	40
4.2.9	TR-111 support.....	40
4.2.10	TR-181 parameter support	40
4.2.11	Mobile offload support	42
4.2.12	Support for soft GRE tunnels.....	42
4.2.12.1	GRE.....	42
4.2.12.2	Soft GRE	43
4.3	G-240W-G software and installation feature support	44
4.4	G-240W-G interfaces and interface capacity.....	44
4.4.1	G-240W-G connections and components	44
4.5	G-240W-G LEDs	47
4.6	G-240W-G detailed specifications	49
4.7	G-240W-G GEM ports and T-CONTs.....	50
4.8	G-240W-G performance monitoring statistics	51
4.9	G-240W-G functional blocks.....	53
4.10	G-240W-G standards compliance	55
4.10.1	Energy-related products standby and off modes compliance.....	55
4.10.2	FCC statement	56
4.10.3	FCC Radiation Exposure Statement	56
4.11	G-240W-G special considerations.....	56
4.11.1	Wi-Fi service.....	57
4.11.1.1	Wi-Fi physical features	57
4.11.1.2	Wi-Fi standards and certifications	57

4.11.1.3	Wi-Fi GUI features	57
4.11.2	G-240W-G ONT considerations and limitations	57
5	Install a G-240W-G indoor ONT	59
5.1	Purpose	59
5.2	General.....	59
5.3	Prerequisites.....	59
5.4	Recommended tools.....	59
5.5	Safety information.....	60
5.6	Procedure	61
6	Replace a G-240W-G indoor ONT	65
6.1	Purpose	65
6.2	General.....	65
6.3	Prerequisites.....	65
6.4	Recommended tools.....	65
6.5	Safety information.....	66
6.6	Procedure	67
7	Configure a G-240W-G indoor ONT	71
7.1	General.....	71
7.2	HGU mode GUI configuration.....	71
7.2.1	Login.....	71
7.2.2	Device and connection status.....	72
7.2.3	Network configuration.....	89
7.2.4	Security configuration	115
7.2.5	Application configuration	127
7.2.6	Maintenance	137
7.2.7	RG troubleshooting counters.....	152
7.3	SFU mode configuration.....	154
7.3.1	Switch from default HGU mode to SFU mode.....	154
7.3.2	Login.....	156
7.3.3	Device and connection status.....	157
7.3.4	Maintenance	158
8	ONT configuration file over OMCI	163
8.1	Purpose	163
8.2	Supported configuration file types	163
8.2.1	Filename conventions.....	165
8.3	ONT configuration file over OMCI	165

List of figures

2	ETSI ONT safety guidelines	17
Figure 1	PSE certification	19
Figure 2	Laser product label	23
Figure 3	Laser classification label.....	23
Figure 4	Laser warning labels.....	24
Figure 5	Sample laser product safety label on the ONT equipment	25
3	ETSI environmental and CRoHS guidelines.....	27
Figure 6	Products below MCV value label.....	28
Figure 7	Products above MCV value label	28
Figure 8	Recycling/take back/disposal of product symbol	31
4	G-240W-G unit data sheet	33
Figure 9	Soft GRE-based architecture.....	43
Figure 10	G-240W-G indoor ONT physical connections	45
Figure 11	G-240W-G ONT without fiber cover	46
Figure 12	G-240W-G ONT with fiber cover	46
Figure 13	G-240W-G indoor ONT LEDs.....	48
Figure 14	Single-residence Wi-Fi ONT with Gigabit Ethernet and POTS and without RF video.....	53
Figure 15	G-240W-G ONT hardware block	54
5	Install a G-240W-G indoor ONT	59
Figure 16	G-240W-G ONT with connections and key mounting holes	62
6	Replace a G-240W-G indoor ONT	65
Figure 17	G-240W-G indoor ONT connections	67
7	Configure a G-240W-G indoor ONT	71
Figure 18	Web login window.....	72
Figure 19	Device Information window.....	73
Figure 20	LAN status window	75
Figure 21	WAN status window.....	77
Figure 22	WAN status IPv6 window	78
Figure 23	Home networking information window.....	80
Figure 24	Optics module status window	81
Figure 25	LAN ports Statistics window	83
Figure 26	WAN ports statistics window	84
Figure 27	WAN ports statistics message.....	85
Figure 28	WLAN ports statistics window	86
Figure 29	WLAN ports statistics message.....	87
Figure 30	Voice Information window.....	88
Figure 31	LAN network window	90
Figure 32	LAN IPv6 network window.....	92
Figure 33	WAN network window.....	94
Figure 34	WAN DHCP window	96
Figure 35	WiFi 2.4G network window	97
Figure 36	WiFi 5G network window	100

Figure 37	Wireless Schedule window.....	102
Figure 38	Routing network window.....	103
Figure 39	DNS network window	105
Figure 40	TR-069 network window.....	106
Figure 41	GRE Tunnel window.....	107
Figure 42	QoS Config window (L2).....	109
Figure 43	QoS Config window (L3).....	110
Figure 44	US Classifier Policy window	112
Figure 45	US Classifier window.....	113
Figure 46	US Classifier Rules window.....	114
Figure 47	Firewall window	116
Figure 48	MAC filter window.....	117
Figure 49	IP filter window	119
Figure 50	URL Filter window	120
Figure 51	Parental Control window.....	123
Figure 52	DMZ and ALG window.....	125
Figure 53	Access Control window	126
Figure 54	Port forwarding window	128
Figure 55	Port Triggering window.....	129
Figure 56	DDNS window	131
Figure 57	NTP window	132
Figure 58	USB window	134
Figure 59	UPnP and DLNA window.....	135
Figure 60	Voice setting window	136
Figure 61	Password window.....	139
Figure 62	Speed Test window	140
Figure 63	LOID Config window.....	141
Figure 64	SLID configuration window.....	142
Figure 65	Device management window.....	143
Figure 66	Backup and Restore window	144
Figure 67	Firmware upgrade window	145
Figure 68	Reboot window	146
Figure 69	Factory default window.....	147
Figure 70	Diagnose window	148
Figure 71	Log window.....	149
Figure 72	PPPoE Diagnostics window	151
Figure 73	PPPoE diagnostics results	152
Figure 74	RG Troubleshooting Counters window.....	153
Figure 75	Web login window.....	156
Figure 76	Device Information window.....	157
Figure 77	Password window.....	159
Figure 78	LOID configuration window.....	160
Figure 79	SLID configuration window.....	161

List of tables

2	ETSI ONT safety guidelines	17
Table 1	Safety labels	18
4	G-240W-G unit data sheet	33
Table 2	Identification of G-240W-G indoor ONTs.....	33
Table 3	G-240W-G power supply	34
Table 4	Support for TR-181 parameter categories.....	41
Table 5	G-240W-G indoor ONT interface connection capacity	44
Table 6	G-240W-G indoor ONT physical connections	47
Table 7	G-240W-G indoor ONT LED descriptions	48
Table 8	G-240W-G indoor ONT physical specifications	49
Table 9	G-240W-G indoor ONT power consumption specifications.....	50
Table 10	G-240W-G indoor ONT environmental specifications	50
Table 11	G-240W-G indoor ONT capacity for GEM ports and T-CONTs.....	50
Table 12	Package P ONTs ONTENET performance monitoring statistics.....	51
Table 13	Package P ONTs ONTL2UNI performance monitoring statistics	51
Table 14	Package P ONTs PONONTTC, PONONTMCTC, PONONTTCHSI, PONONTTCES, PONONTTCFLOW, PONONTTCVOIP performance monitoring statistics.....	52
Table 15	Package P ONTs PONONTTC aggregate performance monitoring statistics.....	52
Table 16	G-240W-G ONT considerations and limitations	57
7	Configure a G-240W-G indoor ONT	71
Table 17	Device Information parameters	73
Table 18	LAN status parameters.....	75
Table 19	WAN status parameters	77
Table 20	WAN status IPv6 parameters	79
Table 21	Home networking parameters	80
Table 22	Optics module status parameters.....	82
Table 23	Voice Information parameters	88
Table 24	LAN network parameters.....	90
Table 25	LAN IPv6 network parameters.....	92
Table 26	WAN network parameters	94
Table 27	WAN DHCP parameters.....	96
Table 28	WiFi 2.4G network parameters.....	97
Table 29	WiFi 5G network parameters.....	100
Table 30	Routing network parameters	104
Table 31	DNS network parameters	105
Table 32	TR-069 network parameters.....	106
Table 33	GRE Tunnel parameters.....	107
Table 34	QoS Config parameters.....	110
Table 35	US Classifier Policy parameters	112
Table 36	US Classifier parameters.....	113
Table 37	US Classifier Rules parameters	115
Table 38	Firewall parameters	116

Table 39	MAC filter parameters.....	118
Table 40	IP filter parameters	119
Table 41	URL Filter parameters	121
Table 42	Parental control parameters	124
Table 43	DMZ and ALG parameters	125
Table 44	Access control parameters	126
Table 45	Port forwarding parameters	128
Table 46	Port triggering parameters.....	129
Table 47	DDNS parameters	131
Table 48	NTP parameters	132
Table 49	USB parameters	134
Table 50	Voice setting parameters.....	136
Table 51	Password parameters.....	139
Table 52	LOID configuration parameters	141
Table 53	SLID configuration parameters.....	142
Table 54	Device management parameters	143
Table 55	PPPoE diagnostics results parameters	152
Table 56	RG Troubleshooting Counters parameters.....	153
Table 57	Device Information parameters	158
Table 58	Password parameters.....	159
Table 59	SLID configuration parameters.....	161
8	ONT configuration file over OMCI	163
Table 60	Supported configuration files	164

2 ETSI ONT safety guidelines

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

2.1 Safety instructions

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

2.1.1 Safety instruction boxes

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

The following is an example of the Danger box.



Danger — 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 ONTs. It does not provide safety-related instructions.

2.1.2 Safety-related labels

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

Table 1 provides sample safety labels on the ONT equipment.

Table 1 **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 1 shows the PSE certification.

Figure 1 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、混信が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、取扱説明書に従ってください。

19841

2.2 Safety standards compliance

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

2.2.1 EMC, EMI, and ESD compliance

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

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

2.2.2 Equipment safety standard compliance

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

2.2.3 Environmental standard compliance

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

2.2.4 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.

2.2.5 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.

2.2.6 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.

2.2.7 Acoustic noise emission standard compliance

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

2.3 Electrical safety guidelines

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



Note 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.

2.3.1 Power supplies

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

2.3.2 Cabling

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

- All cables must be approved by the relevant national electrical code.
- The cables for outdoor installation of ONTs must be suitable for outdoor use.
- POTS wiring run outside the subscriber premises must comply with the requirements of local electrical codes. In some markets, the maximum allowed length of the outside run is 140 feet (43 m). If the outside run is longer, NEC requires primary protection at both the exit and entry points for the wire.

2.3.3 Protective earth

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

2.4 ESD safety guidelines

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



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

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

2.5 Laser safety guidelines

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

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



Danger — 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.

2.5.1 Laser classification

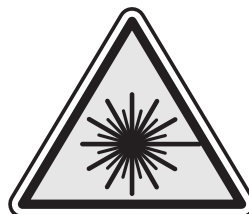
The ONT is classified as a Class 1 laser product based on its transmit optical output.

2.5.1.1 Laser warning labels

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

Figure 2 shows a laser product label.

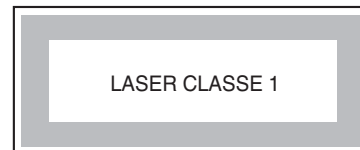
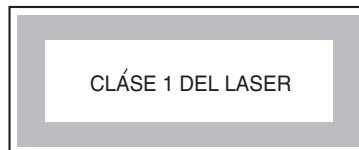
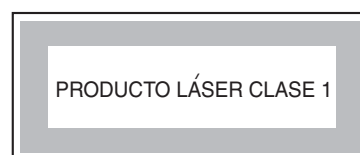
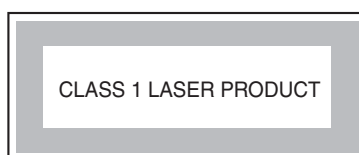
Figure 2 Laser product label



18455

Figure 3 shows a laser classification label. Laser classification labels may be provided in other languages.

Figure 3 Laser classification label



18992

Figure 4 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 4 Laser warning labels

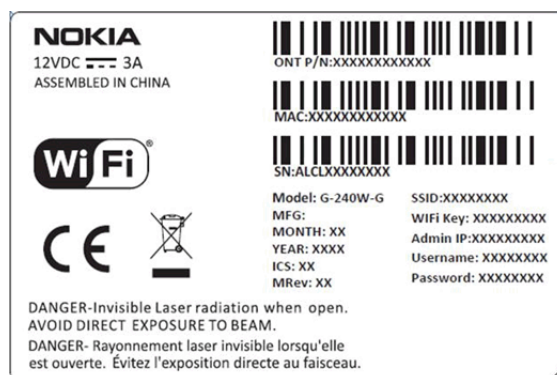
18993

2.5.2 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 5 shows a sample laser product safety label on the ONT equipment.

Figure 5 Sample laser product safety label on the ONT equipment

2.5.3 Transmit optical output

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

2.5.4 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.

2.5.5 Location class

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

2.6 Environmental requirements

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

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

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

3 ETSI environmental and CRoHS guidelines

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

3.1 Environmental labels

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

3.1.1 Overview

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

3.1.2 Environmental related labels

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

3.1.2.1 Products below Maximum Concentration Value (MCV) label

Figure 6 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 6 **Products below MCV value label**



18986

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

Figure 7 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 7 **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.

3.2 Hazardous Substances Table (HST)

This section describes the compliance of the OLT and ONT equipment to the CRoHS standard when the product and 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>

3.3 Other environmental requirements

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

3.3.1 ONT environmental requirements

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

3.3.2 Storage

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

3.3.3 Transportation

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

3.3.4 Stationary use

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

3.3.5 Thermal limitations

When the OLT is installed in the CO or CEV, install air filters on the P-OLT. The thermal limitations for OLT 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

3.3.6 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.

3.3.7 End-of-life collection and treatment

Electronic products bearing or referencing the symbol shown in Figure 8, 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 8 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 8 at the end of their useful life, or products displaced by Nokia equipment offers. For information regarding take-back of equipment by Nokia, or for more information regarding the requirements for recycling/disposal of product, contact your Nokia account manager or Nokia take back support at sustainability.global@nokia.com.

4 G-240W-G unit data sheet

4.1 G-240W-G part numbers and identification

4.2 G-240W-G general description

4.3 G-240W-G software and installation feature support

4.4 G-240W-G interfaces and interface capacity

4.5 G-240W-G LEDs

4.6 G-240W-G detailed specifications

4.7 G-240W-G GEM ports and T-CONTs

4.8 G-240W-G performance monitoring statistics

4.9 G-240W-G functional blocks

4.10 G-240W-G standards compliance

4.11 G-240W-G special considerations

4.1 G-240W-G part numbers and identification

Table 2 provides part numbers and identification information for the G-240W-G indoor ONT.

Table 2 Identification of G-240W-G indoor ONTs

Ordering kit part number	Provisioning number	Description	CLEI	CPR	ECI/Bar code
3FE 47536 AA (Customer-specific variant)	3FE 47555 AA	GPON indoor ONT, 2 POTS, 4 10/100/1000 Base-T Ethernet interfaces, WiFi 802.11n 2x2 and 802.11 ac 3x3, maximum power excluding antenna, customer-specific pre configuration file, SC/APC, AC/DC power adapter with LED, US plug, and customer logo.	—	—	—
3FE 47536 AB (Customer-specific variant)	3FE 47555 BA	GPON indoor ONT, 2 POTS, 4 10/100/1000 Base-T Ethernet interfaces, WiFi 802.11n 2x2 and 802.11 ac 3x3, maximum power excluding antenna, customer-specific pre configuration file, SC/APC, AC/DC power adapter with LED, US plug, and customer logo.	—	—	—

(1 of 2)

Ordering kit part number	Provisioning number	Description	CLEI	CPR	ECI/ Bar code
3FE 47536 AC (Customer-specific variant)	3FE 47555 CA	GPON indoor ONT, 2POTS, 4 10/100/1000 Base-T Ethernet interfaces, WiFi 802.11n 2x2 and 802.11 ac 3x3, maximum power excluding antenna, customer-specific pre configuration file, SC/APC, AC/DC power adapter with LED, US plug, and customer logo.	—	—	—

(2 of 2)

Table 3 provides the power supply information for the G-240W-G ONT. For more information on power supplies, see the *7368 ISAM ONT Power Supply and UPS Guide*.

Table 3 G-240W-G power supply

ONT part numbers	Power model	Power information	Customer category or country compliance tested for	Notes
Kit: 3FE 47536 AA EMA: 3FE 47555 AA	Mass Power RD1203000-C55-2 OMG	36 Watt AC/DC power adapter	ETSI, IEC 60950-1	2-pin US input plug with LED
	MSA-C3000CS12. 0-40W-US 1L43-US1230	36 Watt AC/DC power adapter		2-pin US input plug with LED
Kit: 3FE 47536 AB EMA: 3FE 47555 BA	Mass Power RD1203000-C55-2 OMG	36 Watt AC/DC power adapter		2-pin US input plug with LED
	MSA-C3000CS12. 0-40W-US 1L43-US1230	36 Watt AC/DC power adapter		2-pin US input plug with LED
Kit: 3FE 47536 AC EMA: 3FE 47555 CA	Mass Power RD1203000-C55-2 OMG	36 Watt AC/DC power adapter		2-pin US input plug with LED
	MSA-C3000CS12. 0-40W-US 1L43-US1230	36 Watt AC/DC power adapter		2-pin US input plug with LED

4.2 G-240W-G general description

G-240W-G 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-G 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
- 2.4GHz/5GHz dual band concurrency, both with configurable Wi-Fi tx power from 100mW to 500mW, in 100mW increments (as constrained by local regulations).
- antenna gain: 2.4G and 5G WiFi: 3dBi
- Enhanced ONT; SSH-Telnet-FTP and http server are disabled from the WAN side
- Concurrent 802.11n 2x2 MIMO in 2.4GHz and 802.11ac 3x3 MIMO in 5GHz
- 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 2.4G and 5G)
- 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
- support HT20/HT40 for 802.11b/g/n, and HT20/40/80 for 802.11AC
- support for up to 32 simultaneous wireless connections

- External USB HD (Hard Drive) support, accessible to all LAN devices
- support for AIS with DOWN MEP

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

In addition to functioning as a residential gateway, the G-240W-G 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-G as a single-port ONT. Contact your Nokia support engineer to arrange for a custom pre-configuration file.

4.2.2 Support for CFM over S-tunnel

The G-240W-G 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.

4.2.3 TR-069 parameter support

The G-240W-G 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

4.2.3.1 Host object support

The ONT provides host object support for:
InternetGatewayDevice.LANDevice.Hosts.Host.

4.2.3.2 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 45 in the chapter [“Configure a G-240W-G indoor ONT”](#).

4.2.3.3 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 22 in the chapter [“Configure a G-240W-G indoor ONT”](#).

4.2.3.4 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 28 and 29 in the chapter [“Configure a G-240W-G indoor ONT”](#).

4.2.3.5 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-G indoor ONT”](#).

4.2.3.6 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-G indoor ONT”](#).

4.2.3.7 Timing parameter support

The ONT supports TR-069 timing parameters.

4.2.4 Independent TR69 session with Saas

The prime communication between the Nokia Motive cloud solution and the G-240W-G ONT is TR-069.

To keep the Nokia solution independent from the ACS solution of the carrier, the ONT can establish an independent TR-069 session with the Saas.

The Saas WiFi Care URL and credentials can be programmed from the ACS solution of the carrier, or they can be incorporated in a pre-configuration file.

4.2.5 TR69 authentication using TLS and CA certificates

G-240W-G 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.

4.2.6 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`.

4.2.7 TR-104 voice-related alarms

The G-240W-G 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

4.2.8 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

4.2.9 TR-111 support

The G-240W-G 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.

4.2.10 TR-181 parameter support

TR-181 parameter support has been introduced or enhanced for the parameter categories and functions listed in Table 4.

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

Table 4 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 DHCPv6 client and server
	Ethernet interface
	Firewall
	Hosts
	Interface stack
	IP interface configuration
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

(1 of 2)

Parameter category	Functionality
WiFi	Access point configuration
	Access point associated device
	Radio configuration
	SSID configuration

(2 of 2)

4.2.11 Mobile offload support

As part of the E2E solution supported by the ISAM 7750 service router, the G-240W-G 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.

4.2.12 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.

4.2.12.1 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.

4.2.12.2 Soft GRE

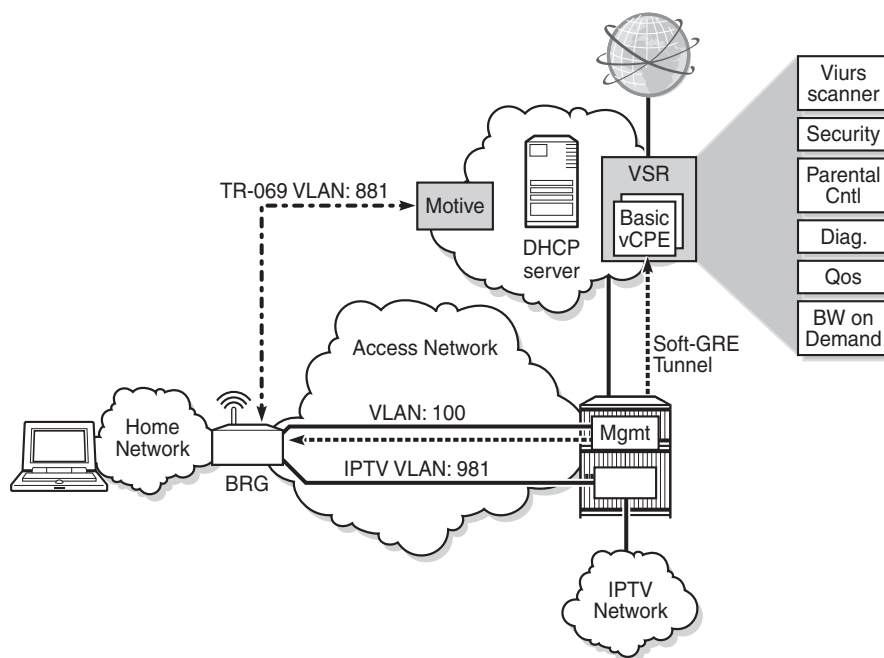
In soft GRE, only one side of the tunnel needs to be configured; the other end learns the remote IP addresses of all remote tunnel endpoints by examining the incoming GRE packets.

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 9 shows the soft GRE architecture.

Figure 9 Soft GRE-based architecture



25265

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

4.3 G-240W-G software and installation feature support

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

- [Install a G-240W-G indoor ONT](#)
- [Replace a G-240W-G 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

4.4 G-240W-G interfaces and interface capacity

Table 5 describes the supported interfaces and interface capacity for G-240W-G indoor ONTs.

Table 5 G-240W-G indoor ONT interface connection capacity

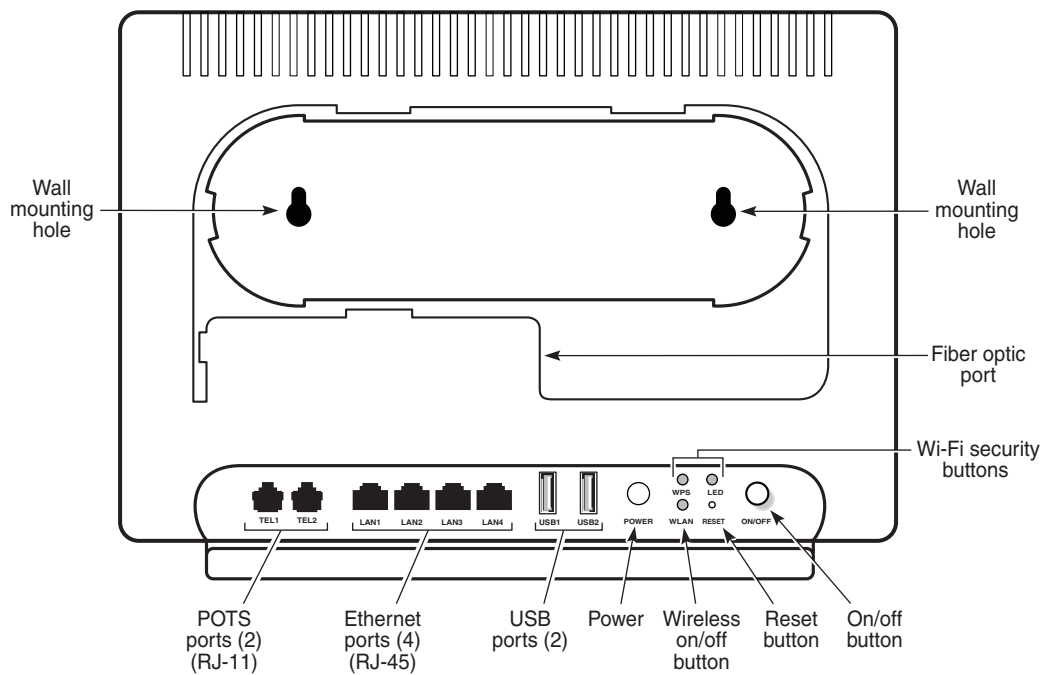
ONT type and model	Maximum capacity								
	POTS	10/ 100 BASE-T	10/ 100/ 1000 BASE-T	RF video (CATV)	MoCA	VDSL2	E1/T1	Local craft	GPON SC/APC
G-240W-G ⁽¹⁾	2	—	4	—	—	—	—	—	1

Note

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

4.4.1 G-240W-G connections and components

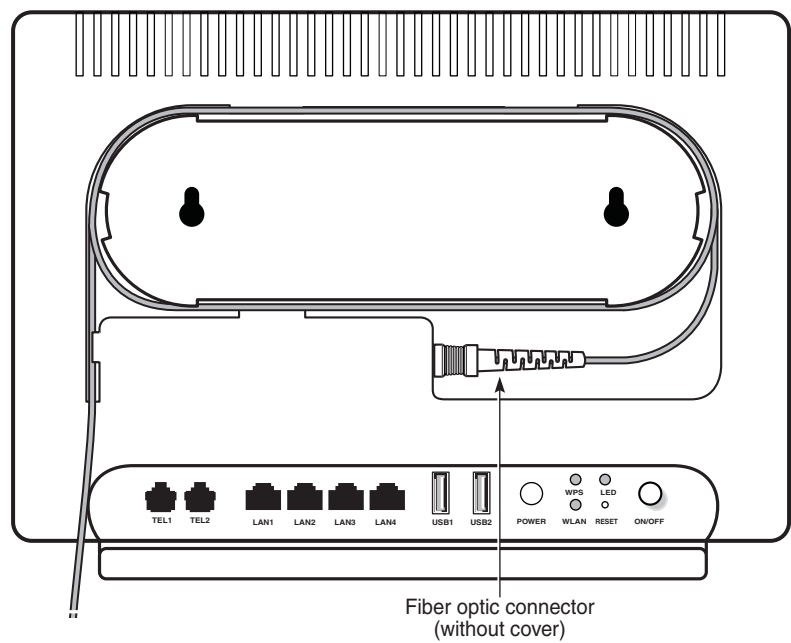
Figure 10 shows the physical connections for G-240W-G indoor ONTs,

Figure 10 G-240W-G indoor ONT physical connections

28302

Figure 11 shows the G-240W-G ONT without the fiber cover.

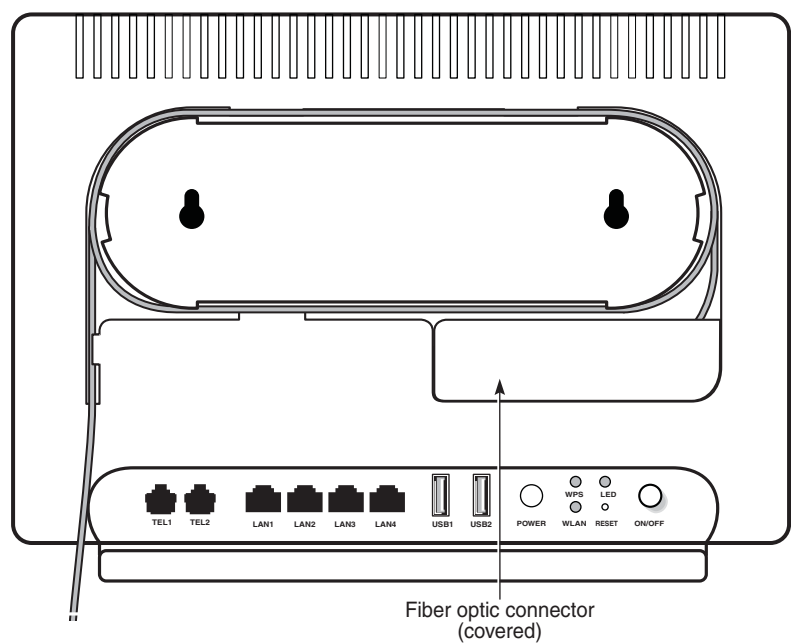
Figure 11 G-240W-G ONT without fiber cover



28303

Figure 12 shows the G-240W-G ONT with the fiber cover.

Figure 12 G-240W-G ONT with fiber cover



28304

Table 6 describes the physical connections for G-240W-G indoor ONTs.

Table 6 G-240W-G indoor ONT physical connections

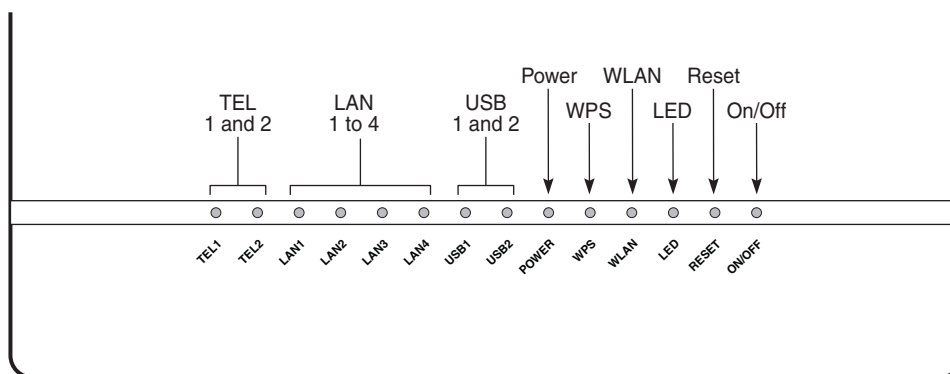
Connection ⁽¹⁾	Description
POTS ports	This connection is provided through RJ-11 ports. Up to two POTS connections are supported. The POTS ports support voice services.
Ethernet ports	This connection is provided through Ethernet RJ-45 connectors. Up to four 10/100/1000 Base-T Ethernet interfaces are supported. 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 WLAN data encryption.
WLAN button	Wi-Fi service is compliant with IEEE 802.11 standards and is enabled and disabled using the WLAN button.
LED On/Off button	This button, located on the side of the ONT, turns all LED indicators on or off.
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 the 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.

4.5 G-240W-G LEDs

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

Figure 13 G-240W-G indoor ONT LEDs

28310

Table 7 provides LED descriptions for G-240W-G indoor ONTs.

Table 7 G-240W-G 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 connected
Auth	Off Green solid Green flashing	No fiber connected or no Rx power ONT has been configured on the OLT and is in service (UP) ONT is attempting to range with OLT ONT is ranged but not configured on OLT ONT is configured on OLT but admin is down and ONT is OOS ONT is in service and subsequently un-configured on the OLT ONT is in service while services are being configured ONT is in service but admin is down and ONT is OOS
LAN 1 to 4	Green solid Green flashing Off	Ethernet is linked LAN activity is present (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

(1 of 2)

Indicator	LED color and behavior	LED behavior description
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	Off Green solid Green flashing	WLAN link is disabled WLAN link is enabled Traffic is passing via WLAN link
USB	Green solid Green flashing Off	At least one USB device is connected There is traffic activity on at least on USB device No USB device is connected
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 in progress 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)

4.6 G-240W-G detailed specifications

Table 8 lists the physical specifications for G-240W-G indoor ONTs.

Table 8 G-240W-G indoor ONT physical specifications

Description	Specification
Length	9.6 in. (244 mm)
Width	1.4 in. (35.5 mm)
Height	7.6 in. (192 mm)
Weight [within ± 0.5 lb (0.23 kg)] (net weight of ONT)	1.23 lb (0.558 kg)

Table 9 lists the power consumption specifications for G-240W-G indoor ONT.

Table 9 G-240W-G indoor ONT power consumption specifications

Mnemonic	Maximum power (Not to exceed)	Condition	Minimum power	Condition
G-240W-G	19.35 W	2 POTS off-hook, 4 10/100/1000 Base-T Ethernet, Wi-Fi operational	2.33 W	2 POTS on-hook, other interfaces/services not provisioned

Table 10 lists the environmental specifications for G-240W-G indoor ONT.

Table 10 G-240W-G 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 10% to 90% relative humidity, non-condensing	Contact your Nokia technical support representative for more information
	Storage: -4°F to 158°F (-20°C to 70°C)	

4.7 G-240W-G GEM ports and T-CONTs

Table 11 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 11 G-240W-G indoor ONT capacity for GEM ports and T-CONTs

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

4.8 G-240W-G performance monitoring statistics

The following section identifies the supported performance monitoring statistics for G-240W-G 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 12 provides statistics for ONTENET type counters
- Table 13 provides statistics for ONTL2UNI type counters
- Table 14 provides statistics for PONONTTC, PONONTMCTC, PONONTTCHSI, PONONTTCES, PONONTTCFLOW, and PONONTTCVOIP type counters
- Table 15 provides statistics for PONONTTC aggregate type counters



Note — If you have trouble accessing G-240W-G 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 12 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-G ⁽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 13 Package P ONTs ONTL2UNI performance monitoring statistics

ONT	ONTL2UNI statistics										
	FRAMES	BYTES	MCFRAMES	DSDRPFDRMS	USDRPFDRMS	USFRAMES	DSFRAMES	USBYTES	DSBYTES	USMCFRAMES	DSMCFRAMES
G-240W-G ⁽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 PONONTTC, PONONTMCTC, PONONTTCHSI, PONONTTCES, PONONTTCFLOW, PONONTTCVOIP performance monitoring statistics

ONT	PONONTTC, PONONTMCTC, PONONTTCHSI, PONONTTCES, PONONTTCFLOW, PONONTTCVOIP statistics					
	TXBLOCKS	TXFRAGS	RXBLOCKS	RXFRAGS	LOSTFRAGS	BADGEMHDRS
G-240W-G ⁽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 aggregate performance monitoring statistics

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

Note

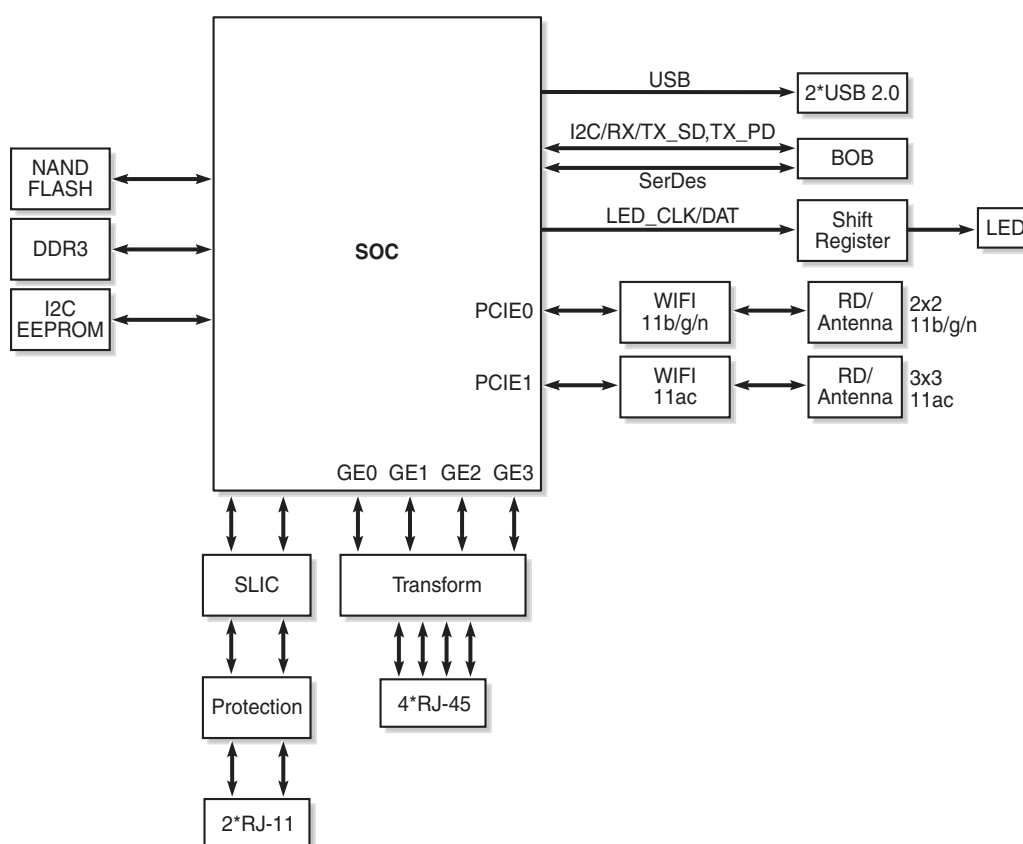
- (1) A 5 second polling window limitation exists on the ONT, therefore the margin of error for each 15-min window is 5 seconds

4.9 G-240W-G functional blocks

G-240W-G 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, USB, and power connectors.

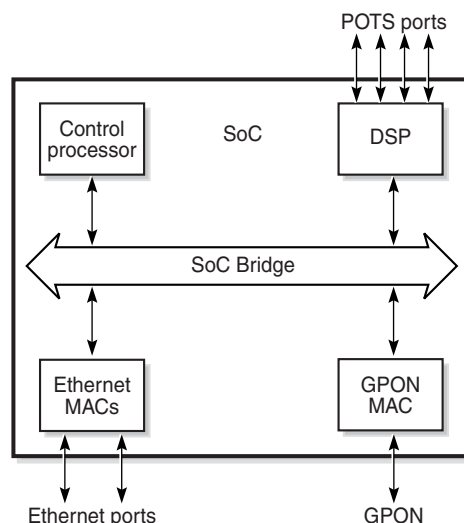
Figure 14 shows the functional blocks for G-240W-G indoor ONT.

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



28301

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

Figure 15 G-240W-G ONT hardware block

19421

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.

4.10 G-240W-G standards compliance

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

- 802.1p marking and VLAN based pbit is supported
- EN 300-328 v1.9.1 wide band data transmission standards for 2.4GHz bands
- 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
- G.984.4 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

4.10.1 Energy-related products standby and off modes compliance

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

For information about power consumption, see [“G-240W-G detailed specifications”](#) in this chapter.

4.10.2 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.

4.10.3 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 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and consider removing the no-collocation statement.

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

- 1 this device may not cause harmful interference, 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.

4.11 G-240W-G special considerations

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

4.11.1 Wi-Fi service

G-240W-G 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.

4.11.1.1 Wi-Fi physical features

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

- WLAN button for enabling and disabling Wi-Fi service
- 5 internal antennas: 2 for 2.4G and 3 for 5G
- one Wi-Fi Protected Setup (WPS) push button for both 2.4G and 5G controlling

4.11.1.2 Wi-Fi standards and certifications

The Wi-Fi service on G-240W-G 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

4.11.1.3 Wi-Fi GUI features

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

4.11.2 G-240W-G ONT considerations and limitations

Table 16 lists the considerations and limitations for Package P G-240W-G ONTs.

Table 16 G-240W-G 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)

5 Install a G-240W-G indoor ONT

5.1 Purpose

5.2 General

5.3 Prerequisites

5.4 Recommended tools

5.5 Safety information

5.6 Procedure

5.1 Purpose

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

5.2 General

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

5.3 Prerequisites

You need the following items before beginning the installation:

- all required cables

5.4 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

5.5 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-G unit data sheet](#) for the temperature ranges for these ONTs.

5.6 Procedure

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

1 Place the indoor ONT unit:

- a** On the flat surface, such as a desk; go to step [3](#).



Note — The G-240W-G 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

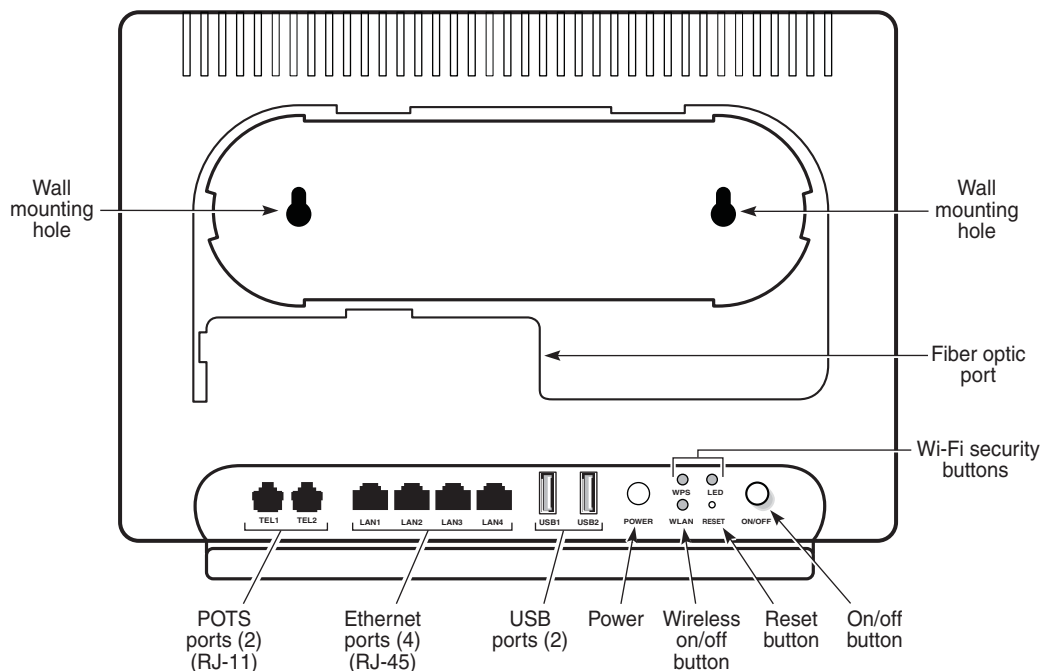
- b** On a wall, go to step [2](#).

2 Mount the G-240W-G indoor ONT on a wall.

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

If possible, mount the ONT on a wall stud.

Figure [16](#) shows the ONT with the connections and the key mounting holes.

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

28302

- i Attach the wall mounting keyholes on the ONT.
- ii Attach the ONT to the wall.

- 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 1.5 in. (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 12VDC, 3A.

-
- 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 on the ONT; see Figure 16 for location of the WLAN button.
- ii Press the WLAN button to change the status of the Wi-Fi service.

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

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

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

14 If necessary, reset the ONT.

- i** Locate the Reset button on a G-240W-G indoor ONT as shown in Figure [16](#).
- ii** Insert the end of a straightened paper clip or other narrow object into the hole in the Reset button to reset the ONT.

15 STOP. This procedure is complete.

6 Replace a G-240W-G indoor ONT

6.1 Purpose

6.2 General

6.3 Prerequisites

6.4 Recommended tools

6.5 Safety information

6.6 Procedure

6.1 Purpose

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

6.2 General

The steps listed in this chapter describe mounting and cabling for G-240W-G 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 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

6.5 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-G unit data sheet](#) for the ONT temperature ranges for these ONTs.

6.6 Procedure

Use this procedure to replace a G-240W-G 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 the 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;
```

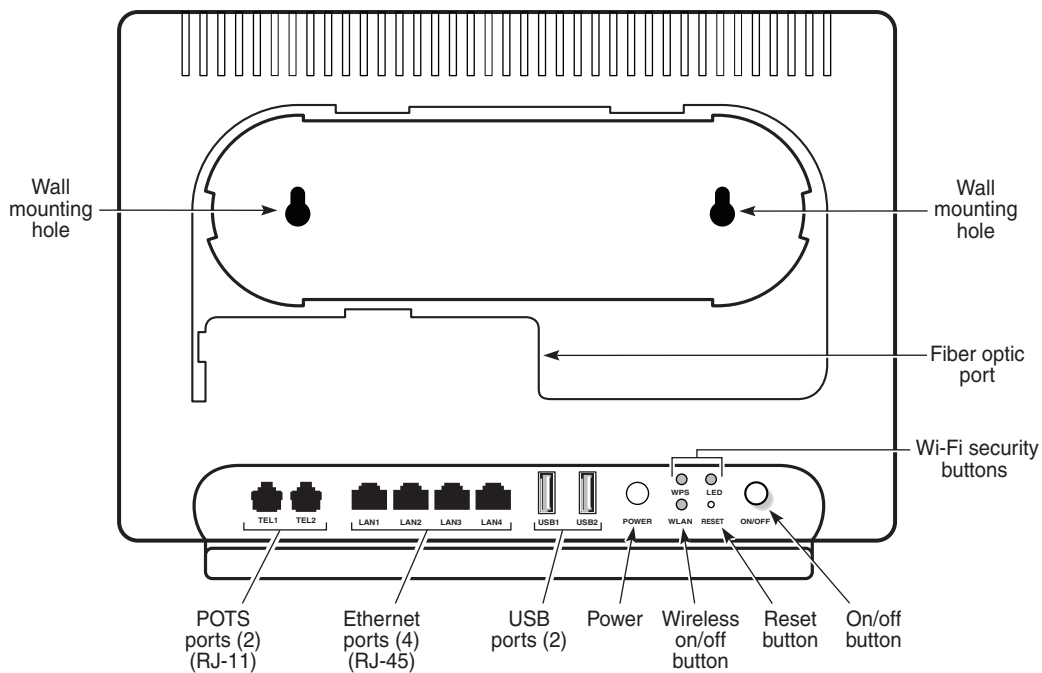
- ii If the ONT is in service, place the ONT in OOS state.

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-G indoor ONT connections



28302

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

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

5 Disconnect the fiber optic cables.



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 on a flat surface, horizontally resting on its four feet.
- b On a wall.
 - i Remove the old ONT from the wall.
 - ii Attach the wall mount adapter bracket (shipped with the ONT) to the two wall mounting key holes on the new ONT.
 - iii Attach the new ONT to the wall.

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 1.5 in. (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, 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.

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

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

18 If necessary, reset the ONT.

- i** Locate the Reset button on a G-240W-G indoor ONT as shown in 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.

19 STOP. This procedure is complete.

7 Configure a G-240W-G indoor ONT

7.1 General

7.2 HGU mode GUI configuration

7.3 SFU mode configuration

7.1 General

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

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

7.2 HGU mode GUI configuration

Use the procedures below to use the web-based GUI for the G-240W-G in HGU mode. This mode is preset at delivery.

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

7.2.1 Login

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

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

The image shows a web login window titled "GPON Home Gateway". It has a teal header bar. Below the header, there are two input fields: "Username" and "Password". At the bottom of the window, there are two buttons: "Login" and "Reset".

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.
-

7.2.2 Device and connection status

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

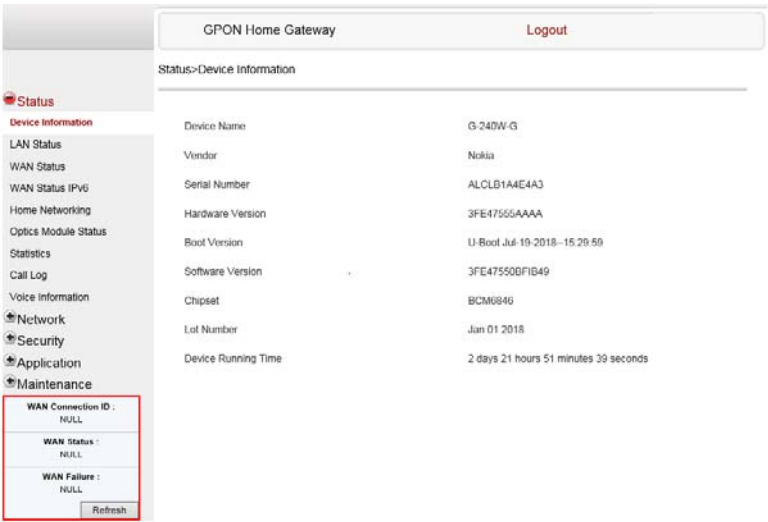
- device information
- LAN status
- WAN status

- 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



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 17 describes the fields in the Device Information window.

Table 17 Device Information parameters

Field	Description
Device Name	Name on the ONT
Vendor	Name of the vendor

(1 of 2)

Field	Description
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 of 2)

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

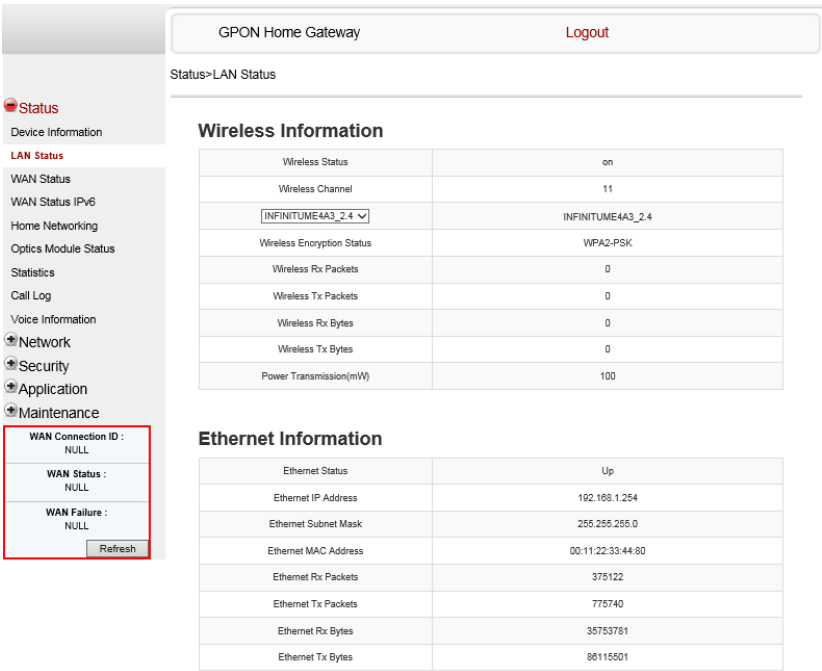


Table 18 describes the fields in the LAN status window.

Table 18 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
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

(1 of 2)

Field	Description
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

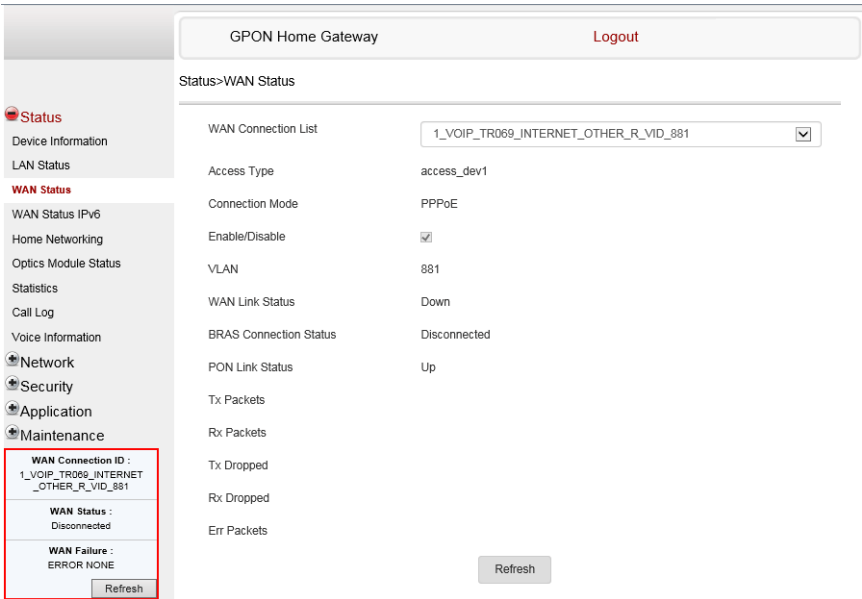


Table 19 describes the fields in the WAN status window.

Table 19 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.
Access Type	
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)

Field	Description
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

The screenshot shows the GPON Home Gateway web interface. The sidebar menu on the left has 'Status' selected, and 'WAN Status IPv6' is highlighted under the 'WAN Status' section. The main content area displays the 'WAN Status IPv6' window. At the top, there is a 'WAN Connection List' with a dropdown menu showing '1_VOIP_TR069_INTERNET_OTHER_R_VID_881'. Below this, there is a table of WAN connection statistics:

Field	Value
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

Below the table, there is an 'Auto Configure' section with fields for IPv6 address, IPv6 Prefix, IPv6 Gateway, Primary DNS, and Second DNS. A 'Refresh' button is located at the bottom right of the main content area. A red box highlights the 'WAN Connection ID' field and the 'Refresh' button.

Table 20 describes the fields in the WAN status IPv6 window.

Table 20 **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

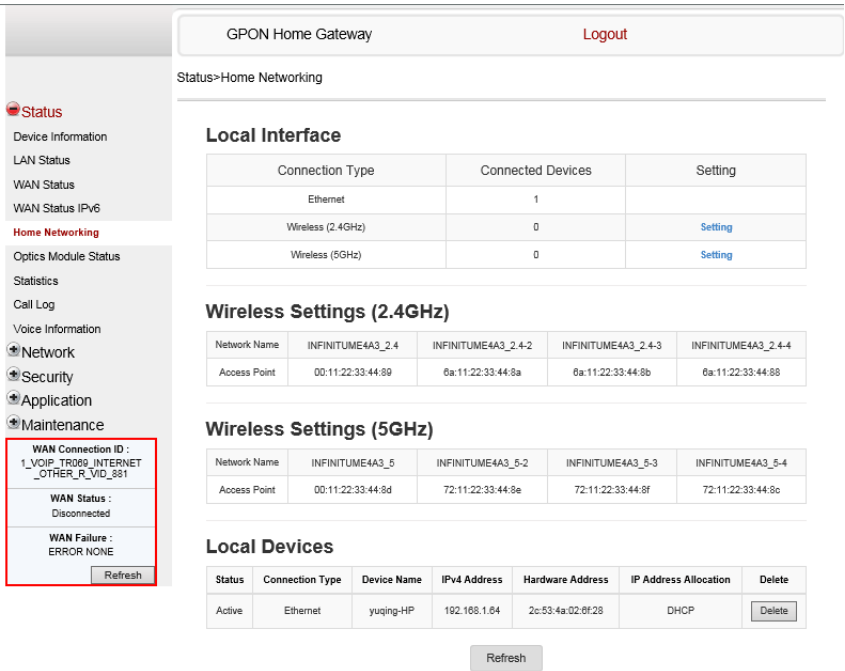


Table 21 describes the fields in the Home networking window.

Table 21 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)

Field	Description
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

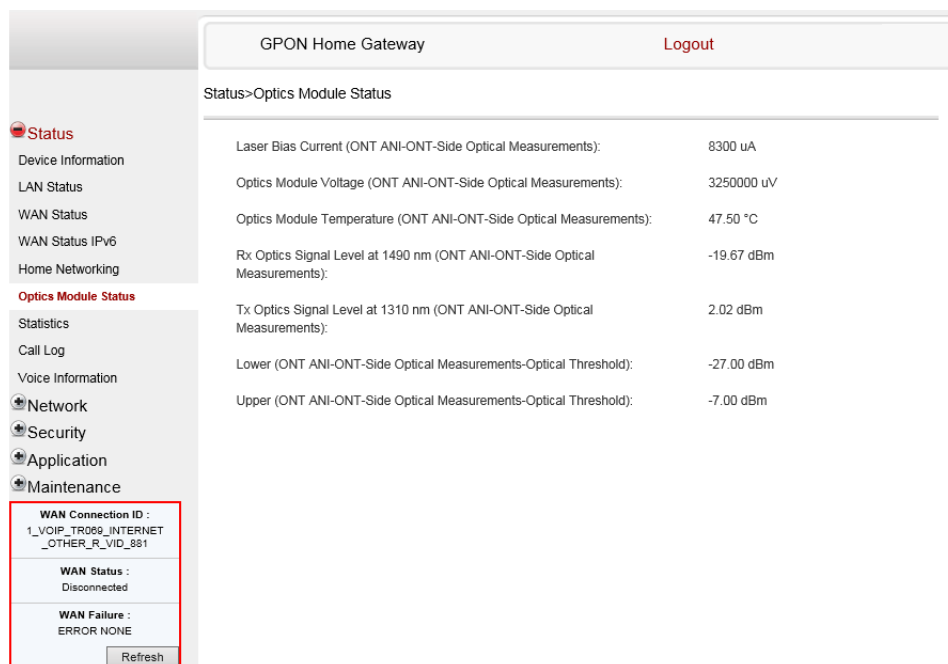


Table 22 describes the fields in the Optics module status window.

Table 22 **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.

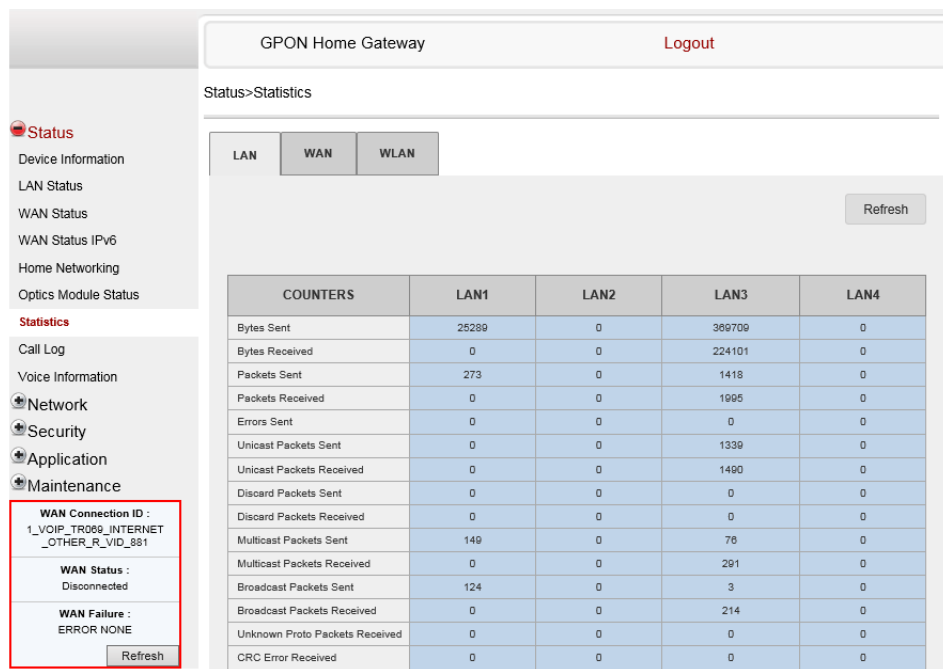
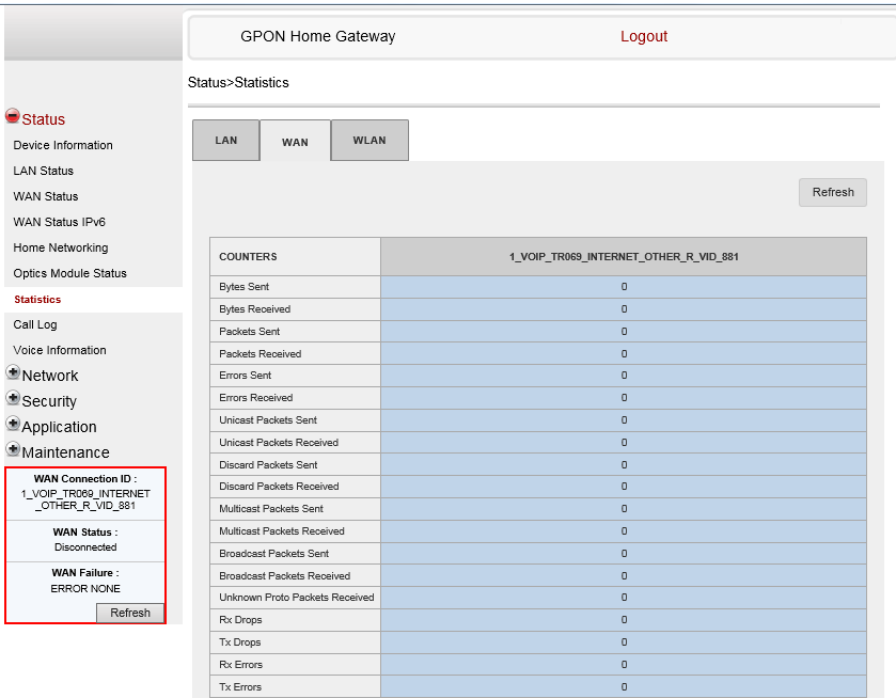
Figure 25 LAN ports Statistics window

Figure 26 shows the statistics for the WAN ports.

Figure 26 WAN ports statistics window



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

Figure 27 WAN ports statistics message

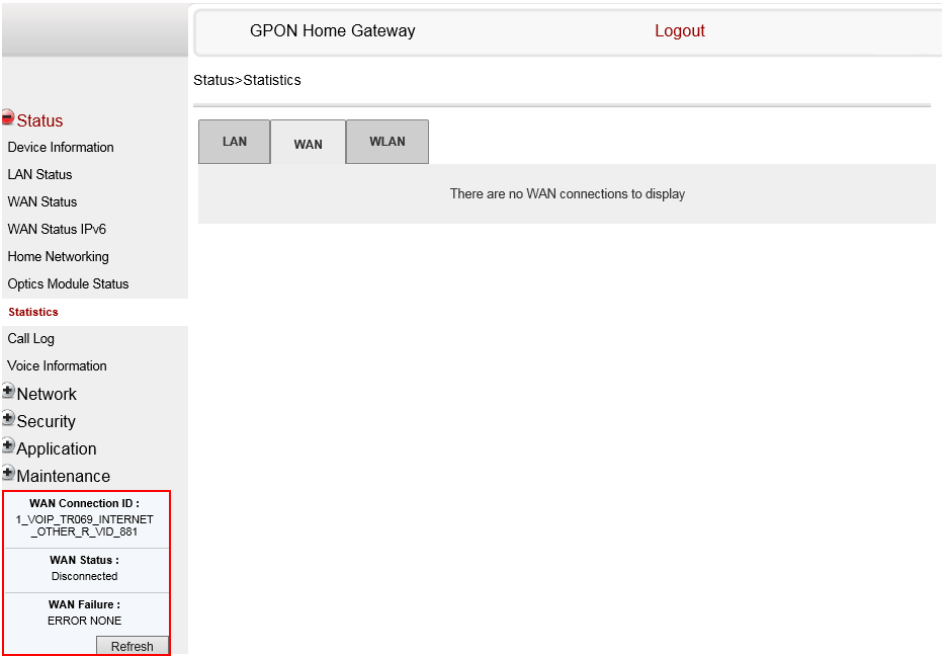
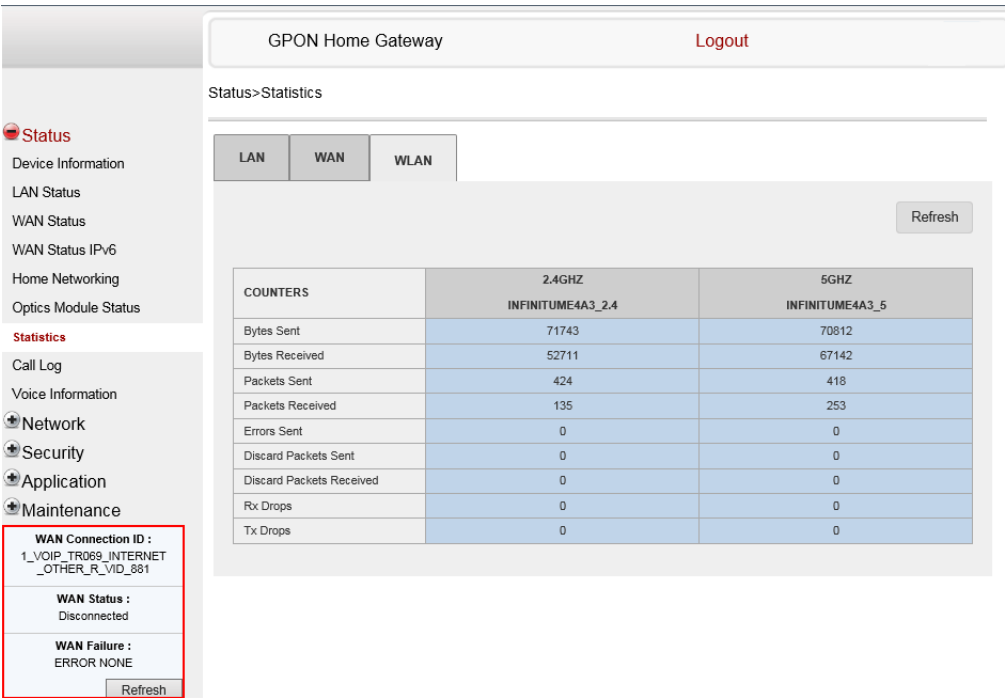
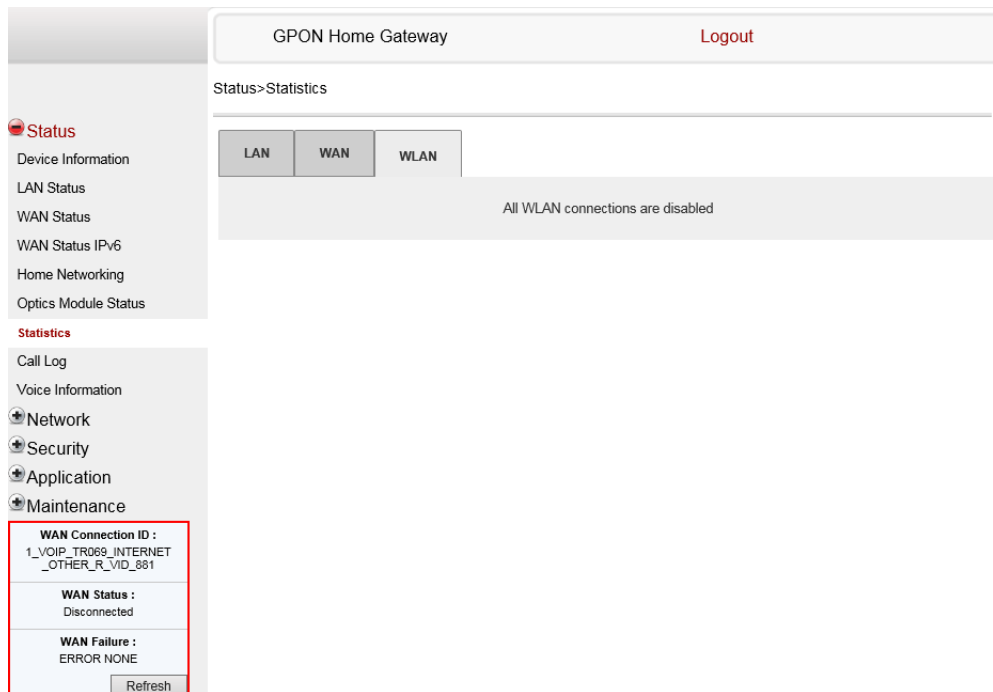


Figure 28 shows the statistics for the WLAN ports.

Figure 28 WLAN ports statistics window



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

Figure 29 WLAN ports statistics message

2 STOP. This procedure is complete.

Procedure 14 Voice information retrieval

- 1
- 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

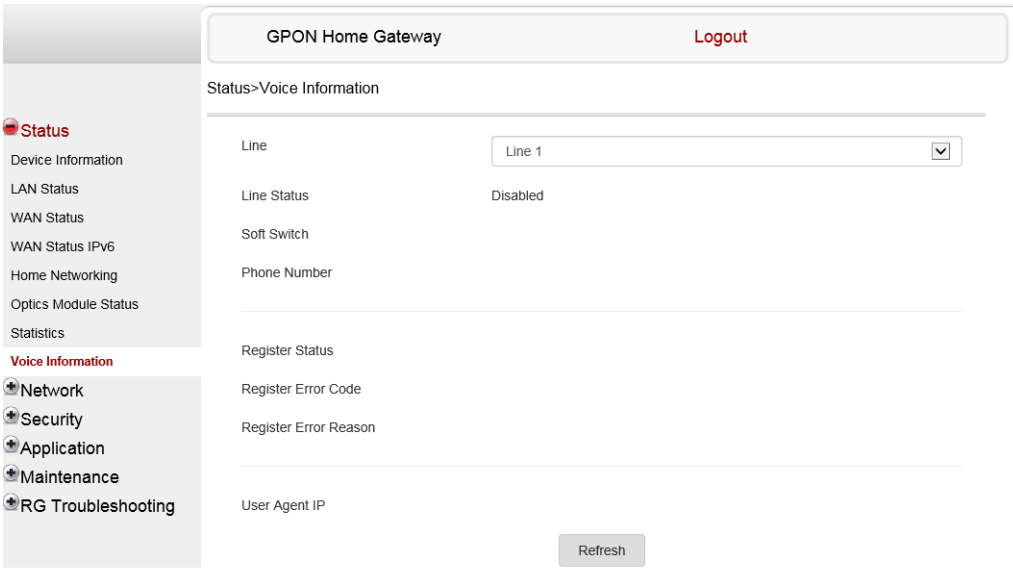


Table 23 describes the fields in the Voice Information window.

Table 23 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 WANPPPPConnection

(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.

7.2.3 Network configuration

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

- LAN
- LAN IPv6
- WAN
- WAN DHCP
- WiFi 2.4G
- WiFi 5G
- Wireless schedule
- Routing
- DNS
- TR-069
- GRE tunnel
- QoS
- US (upstream) classification

Procedure 15 LAN networking configuration

- 1
- Select Network > LAN from the top-level menu in the GPON Home Gateway window, as shown in Figure 31.

Figure 31 LAN network window

GPON Home Gateway

Logout

Network>LAN

Status

Network

LAN

LAN IPv6

WAN

WAN DHCP

Wireless (2.4GHz)

Wireless (5GHz)

Wireless Schedule

IP Routing

DNS

GRE Tunnel

US Classifier

Security

Application

Maintenance

WAN Connection ID : 1_VOIP_TROUS_INTERNET_OTHER_R_VID_881

WAN Status : Disconnected

WAN Failure : ERROR NONE

Refresh

Port Mode

All Ports to Bridge Mode ☐

Port1

Route Mode

Port2

Route Mode

Port3

Route Mode

Port4

Route Mode

Save

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

Save

Static DHCP Entry

MAC Address

IPv4 Address

Add

MAC Address

IPv4 Address

Delete

Table 24 describes the fields in the LAN network window.

Table 24 LAN network parameters

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

(1 of 2)

Field	Description
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

(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.

Procedure 16 LAN IPv6 networking configuration

- 1 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

Status

Network

LAN

LAN IPv6

WAN

WAN DHCP

Wireless (2.4GHz)

Wireless (5GHz)

Wireless Schedule

IP Routing

DNS

QoS Tunnel

USB Classifier

Security

Application

Maintenance

GPON Home Gateway

Logout

Network-LAN_IPv6

IPv6 LAN Host Configuration

DNS Server

WANConnection

Interface

1_VOIP_TR069_INTERNET_OTHER_RL_VID_881

LAN Prefix

1_LAN_Prefix

Enable

☒

Prefix Config

WANConnection

WAN Interface

1_VOIP_TR069_INTERNET_OTHER_RL_VID_881

WAN Prefix

none

Save/Apply

Delete

DHCPv6 Server

Enable

☒

DHCPv6 Server Pool

LAN Prefix

1_LAN_Prefix

Save/Apply

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

Save/Apply

Table 25 describes the fields in the LAN IPv6 network window.

Table 25 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 DHCP	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.

Procedure 17 WAN networking configuration

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

Figure 33 WAN network window

GPON Home Gateway

Logout

Status

Network

LAN

LAN_IPV6

WAN

WAN_DHCP

Wireless (2.4GHz)

Wireless (5GHz)

Wireless Schedule

IP Routing

DNS

GRE Tunnel

US Classifier

Security

Application

Maintenance

WAN Connection ID:
1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status:
Disconnected

WAN Failure:
ERROR NONE

Refresh

Network>WAN

WAN Connection List
1_VOIP_TR069_INTERNET_OTHER_R_VID_881

Connection Type
IPoE @PPPoE

IP mode
IPv4&IPv6

Enable/Disable
☒

NAT
☒

Service
☒VOIP ☒TR-069 ☒INTERNET ☒IPTV

Enable VLAN
☒

VLAN ID
881

VLAN PRI
0

WAN IP Mode
PPPoE

Username
ED3005LALCLB1A4E4A3@prodgyweb.com.mx

Password

Keep Alive Time
50
(5-60)seconds

Keep Alive Retry
3
(1-10)times

Echo Value
150

DHCPv6 Enable
☐

Request Address
☐

Request Prefix
☐

Request Option

AutoConfigured Enable
☒

Save Delete

Table 26 describes the fields in the WAN network window.

Table 26 WAN network parameters

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

(1 of 2)

Field	Description
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 Type	Choose a connection type from the drop-down menu
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 retries (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
DHCPv6 Enable	
Request Address	
Request Prefix	
Request Option	
Auto Configured Enable	

(2 of 2)

2 Configure a specific WAN connection.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 18 WAN DHCP configuration

- 1 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

Table 27 describes the fields in the WAN DHCP window.

Table 27 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

- 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

GPON Home Gateway

Logout

Status

Network

LAN

LAN IPv6

WAN

WAN DHCP

Wireless (2.4GHz)

Wireless (5GHz)

Wireless Schedule

IP Routing

DNS

GRE Tunnel

US Classifier

Security

Application

Maintenance

WAN Connection ID :
1_VOIP_TRGS_INTERNET
_OTHER_V_ID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Refresh

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

INFINITIME4A3_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

WPS Connect

Save

Table 28 describes the fields in the WiFi 2.4G network window.

Table 28 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

GPON Home Gateway

Logout

Network>Wireless (5GHz)

Status

Network

LAN

LAN_IPv6

WAN

WAN_DHCP

Wireless (2.4GHz)

Wireless (5GHz)

Wireless Schedule

IP Routing

DNS

GRE Tunnel

US Classifier

Security

Application

Maintenance

WAN Connection ID :
1_VOIP_TR069_INTERNET
_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Refresh

Enable

☒

Bandwidth

80MHz

Channel

Auto

Transmitting Power

Medium

WMM

Enable

Enable MU-MIMO

Disable

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

WPS Connect

Save

Table 29 describes the fields in the WiFi 5G network window.

Table 29 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
Enable MU-MIMO	Choose Enable or disable MU-MIMO from this drop-down menu The default is Enable, which enables users and wireless terminals to communicate with each other. MU-MIMO may decrease Wi-Fi performance for clients who do not support it, in which case Nokia recommends that you choose Disable.
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.

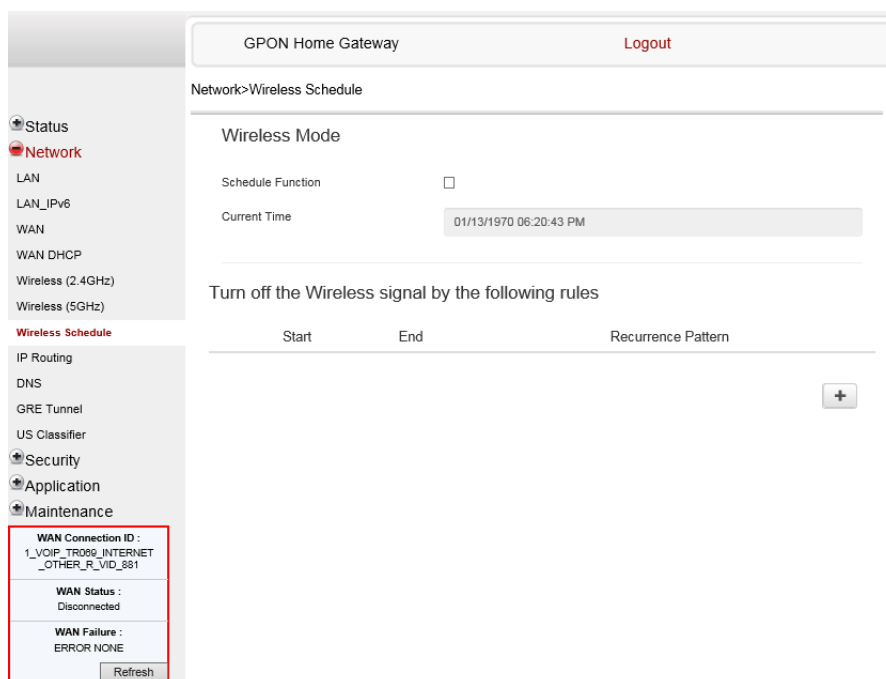
2 Configure the WiFi connection.**3** If you have enabled and configured WPS, click WPS connect.

- 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



- 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

GPON Home Gateway

Logout

Network>IP Routing

Status

Network

LAN

LAN_IPv6

WAN

WAN_DHCP

Wireless (2.4GHz)

Wireless (5GHz)

Wireless Schedule

IP Routing

DNS

GRE Tunnel

US Classifier

Security

Application

Maintenance

WAN Connection ID :
1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Refresh

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

Help

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

Add

IP Routing Table

Destination IP Address	Destination Netmask	Gateway	Interface	Forwarding Policy	Enable	Delete

Table 30 describes the fields in the Routing network window.

Table 30 **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

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

GPON Home Gateway

Logout

Network>DNS

Status

Network

LAN

LAN_IPv6

WAN

WAN_DHCP

Wireless (2.4GHz)

Wireless (5GHz)

Wireless Schedule

IP Routing

DNS

GRE Tunnel

US Classifier

Security

Application

Maintenance

WAN Connection ID :
1_VOIP_TROOP_INTERNET
_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Refresh

DNS Proxy

☒Enabled

Save

Domain Name

IPv4 Address

Add

Origin Domain

New Domain

Add

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

Origin Domain	New Domain	Delete
---------------	------------	--------

Table 31 describes the fields in the DNS network window.

Table 31 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

- 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

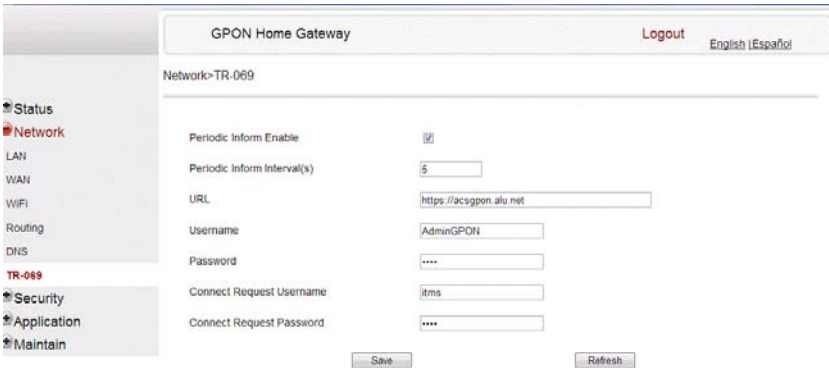


Table 32 describes the fields in the TR-069 network window.

Table 32 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

GPON Home GatewayLogout

Network>GRE Tunnel

Status

Network

LAN

LAN_IPv6

WAN

WAN_DHCP

Wireless_(2.4GHz)

Wireless_(5GHz)

Wireless_Schedule

IP_Routing

DNS

GRE Tunnel

US_Classifier

Security

Application

Maintenance

WAN_Connection_ID :
1_VOIP_TR069_INTERNET
_OTHER_R_VID_881

WAN_Status :
Disconnected

WAN_Failure :
ERROR_NONE

Refresh

Tunnel_Name

Create_new_GRE_Tunnel

WAN_Interface

Primary_Remote_End

Secondary_Remote_End

Connected_Remote_End

Failover_mechanism

Traffic_timeout_to_start_pings

No._of_retries_before_unreachable

10

(2 ~ 1024)seconds

3

(0 ~ 100)times

SaveDelete

Table 33 describes the fields in the GRE Tunnel window.

Table 33 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)

NOKIA

GPON Home Gateway

Logout

English |Español

Status

Network

LAN

LAN_IPv6

WAN

WAN_DHCP

Wireless_2.4GHz

Wireless_5GHz

Wireless_Schedule

IP_Routing

DNS

TR-069

GRE_Tunnel

US_Classifier

QoS_Config

Security

Application

Maintenance

Network>QoS Config

QoS Setting

ID	Source MAC	Source MAC Exclude	Protocol	Protocol Exclude	Source Port	Source Max	SExclude	Dest Port	Dest Max	DEExclude	Si
----	------------	--------------------	----------	------------------	-------------	------------	----------	-----------	----------	-----------	----

Type

L2 Criteria

Classification Criteria

Source MACExclude ☐

Interface

select an option

Classification Result

DSCP Remark:(Range:0~63)

802.1p Remark:(Range:0~7)

Forwarding Policy:(Range:1~7)

Add

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

Figure 43 QoS Config window (L3)

NOKIA

GPON Home Gateway

Logout

English | Español

Status

Network

LAN

LAN_Pv6

WAN

WAN DHCP

Wireless (2.4GHz)

Wireless (5GHz)

Wireless Schedule

IP Routing

DNS

TR-069

GRE Tunnel

US Classifier

QoS Config

Security

Application

Maintenance

RG Troubleshooting

SmartHome

Network>QoS Config

QoS Setting

ID	Source MAC	Source MAC Exclude	Protocol	Protocol Exclude	Source Port	Source Max	SExclude	Dest Port	Dest Max	DExclude	St
----	------------	--------------------	----------	------------------	-------------	------------	----------	-----------	----------	----------	----

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

802.1p

(Range: 0~63)

(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)

Add

Table 34 describes the fields in the QoS Config window.

Table 34 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

GPON Home Gateway

Logout

Network>US Classifier

Status

Network

LAN

LAN_IPv6

WAN

WAN_DHCP

Wireless (2.4GHz)

Wireless (5GHz)

Wireless Schedule

IP Routing

DNS

GRE Tunnel

US Classifier

Security

Application

Maintenance

WAN Connection ID :
1_VOIP_TR069_INTERNET
_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Refresh

[-] Policy

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

☐

SaveReset

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

Refresh

[+] Classifier

[+] Classifier Rules

Table 35 describes the fields in the US Classifier Policy window.

Table 35 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

Table 36 describes the fields in the US Classifier window.

Table 36 US Classifier parameters

Field	Description
Interface	Choose an interface from the drop-down menu; for example, None, LAN, 2.4G SSID, or 5G SSID.
Source MAC	Click to enter a source MAC
Destination MAC	Click to enter a destination MAC
Source IP	Click to enter a source IP

(1 of 2)

Field	Description
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.

(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

GPON Home Gateway Logout

Network>US Classifier

[+] Policy
[+] Classifier
[-] Classifier Rules

Policy ☐ Classifier ☐

Interface ☐

Source MAC Destination MAC

Source IP Destination IP

Source Port Destination Port

IP Protocol Type
(0 - 254)

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

Status
 Network
 LAN
 LAN IPv6
 WAN
 WAN DHCP
 Wireless (2.4GHz)
 Wireless (5GHz)
 Wireless Schedule
 IP Routing
 DNS
 GRE Tunnel
 US Classifier
 Security
 Application
 Maintenance

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 Rules window.

Table 37 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.

7.2.4 Security configuration

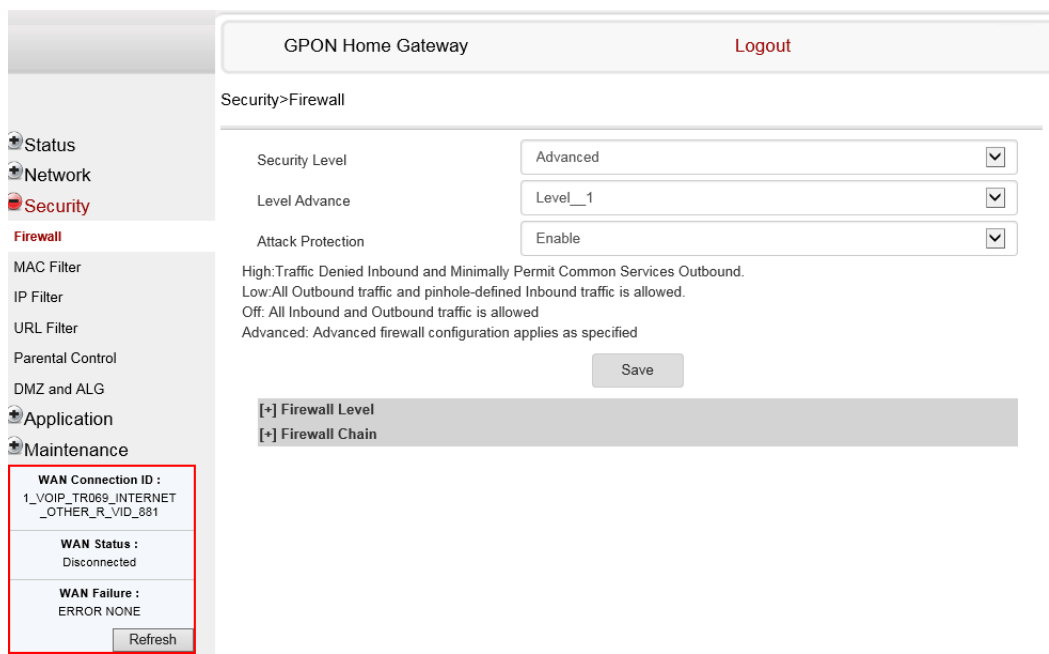
G-240W-G ONTs also supports security configuration, including:

- 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



Firewall security applies only to services provided by the ONT. Internet access from the LAN side is not affected by this firewall.

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 38 describes the fields in the firewall window.

Table 38 Firewall parameters

Field	Description
Security Level	Choose the security level from the drop-down menu: High, Low, Off, or Advanced

(1 of 2)

Field	Description
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.

(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

The screenshot shows the 'GPON Home Gateway' configuration interface. The left sidebar contains a menu with 'Security' selected, and 'MAC Filter' highlighted under the 'Security' section. The main content area is titled 'Security > MAC Filter' and contains two sections: 'Ethernet Interface' and 'Wi-Fi SSID'.

Ethernet Interface:

- MAC Filter Mode:
- LAN Port: ☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4
- MAC Address: (e.g. D0:54:2D:00:00:00)
- Save button

Mac Address Table:

Mac Address	Delete
Refresh	

Wi-Fi SSID:

- MAC Filter Mode:
- SSID Select:
- Enable: ☐
- MAC Address: (e.g. D0:54:2D:00:00:00)
- Save button

Table 39 describes the fields in the MAC filter window.

Table 39 **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

GPON Home Gateway

Logout

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
------	-----------------	----------	------------------	--------------------	-------------------	-------------------------	----------------	----------------	--------

Save

Status

Network

Security

Firewall

MAC Filter

IP Filter

URL Filter

Parental Control

DMZ and ALG

Application

Maintenance

WAN Connection ID :
1_VOIP_TR069_INTERNET
_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Refresh

Table 40 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 40 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

GPON Home Gateway

Logout

Security>URL Filter

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		

Add Filter

i

Note

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

Table 41 describes the fields in the URL Filter window.

Table 41 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

GPON Home GatewayLogout

Security-Parental Control

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

Add

IPv4 Address:

New IP

e.g. 192.168.1.100

Add

Url Port:

e.g. http://www.baidu.com

e.g. 0~65535 (default: 80)

Add

Days of Week:

Everyday

From:

e.g. 00:00~23:59

To:

e.g. 00:00~23:59

Close

Save changes

Status

Network

Security

Firewall

MAC Filter

IP Filter

URL Filter

Parental Control

DMZ and ALG

Application

Maintenance

WAN Connection ID : NULL

WAN Status : NULL

WAN Failure : NULL

Refresh

Table 42 describes the fields in the Parental Control window.

Issue: 01

3FE-47555-AAAA-TCZZA

123

Table 42 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

GPON Home Gateway

Logout

Security>DMZ and ALG

Status

Network

Security

Firewall

MAC Filter

IP Filter

URL Filter

Parental Control

DMZ and ALG

Application

Maintenance

WAN Connection ID :
1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Refresh

ALG Config

FTP ☒ TFTP ☒ SIP ☒ H323 ☒
RTSP ☒ L2TP ☒ IPSEC ☒ PPTP ☒

Save ALG

DMZ Config

WAN Connection List

1_VOIP_TR069_INTERNET_OTHER_R_VID_881

Enable DMZ☐

DMZ IP Address

Custom settings

0.0.0.0

Save DMZ

Table 43 describes the fields in the DMZ and ALG window.

Table 43 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

Status

Network

Security

Firewall

MAC Filter

IP Filter

URL Filter

DMZ and ALG

Access Control

Application

Maintenance

RG Troubleshooting

Security>Access Control

WAN

LAN

3_VOIP_TR069_INTERNET_J

Trusted Network Enable ☒

ICMP

Trusted NetWork Only

Allow

SSH

Trusted NetWork Only

Deny

HTTP

Trusted NetWork Only

Allow

TR-069

Trusted NetWork Only

Deny

Save

Refresh

Trusted Network

Source IP Start

Source IP End

Add

Table 44 describes the fields in the Access Control window.

Table 44 Access control parameters

Field	Description
WAN	Choose a connection from the drop-down menu

(1 of 2)

Field	Description
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.

7.2.5 Application configuration

G-240W-G ONTs also supports 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

GPON Home GatewayLogout

Application>Port Forwarding

Status

Network

Security

Application

Port Forwarding

Port Triggering

DDNS

NTP

USB

UPNP and DLNA

Maintenance

WAN Connection ID :
1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Refresh

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

Add

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

Table 45 describes the fields in the port forwarding window.

Table 45 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

GPON Home Gateway

Logout

Application>Port Triggering

Status

Network

Security

Application

Port Forwarding

Port Triggering

DDNS

NTP

USB

UPNP and DLNA

Maintenance

WAN Connection ID :
1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Refresh

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

Add

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

Table 46 describes the fields in the Port Triggering window.

Table 46 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

GPON Home Gateway

Logout

Application>DDNS

Status

Network

Security

Application

Port Forwarding

Port Triggering

DDNS

NTP

USB

UPNP and DLNA

Maintenance

WAN Connection ID :
1_VOIP_TR069_INTERNET_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Refresh

WAN Connection List

1_VOIP_TR069_INTERNET_OTHER_R_VID_881

Enable DDNS

☐

ISP

Domain Name

Username

Password

DDNS Status

Save

Refresh

Table 47 describes the fields in the DDNS window.

Table 47 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

GPON Home Gateway

Logout

Application>NTP

Status

Network

Security

Application

Port Forwarding

Port Triggering

DDNS

NTP

USB

UPNP and DLNA

Maintenance

WAN Connection ID :
1_VOIP_TR069_INTERNET
_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Refresh

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

Save

Table 48 describes the fields in the NTP window.

Table 48 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

Status

Network

Security

Application

Port Forwarding

Port Triggering

DDNS

NTP

USB

UPNP and DLNA

Maintenance

GPON Home Gateway

Logout

Application>USB

Enable FTP Server

☒

Username

ftpadmin

Password

Re-enter Password

Connected USB Devices Table

Host Number	Device Name	Format	Total Space	Free Space
-------------	-------------	--------	-------------	------------

Save

Refresh

WAN Connection ID :

1_VOIP_TR069_INTERNET

_OTHER_R_VID_881

WAN Status :

Disconnected

WAN Failure :

ERROR NONE

Refresh

Table 49 describes the fields in the USB window.

Table 49 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
Re-enter Password	Password for the FTP server

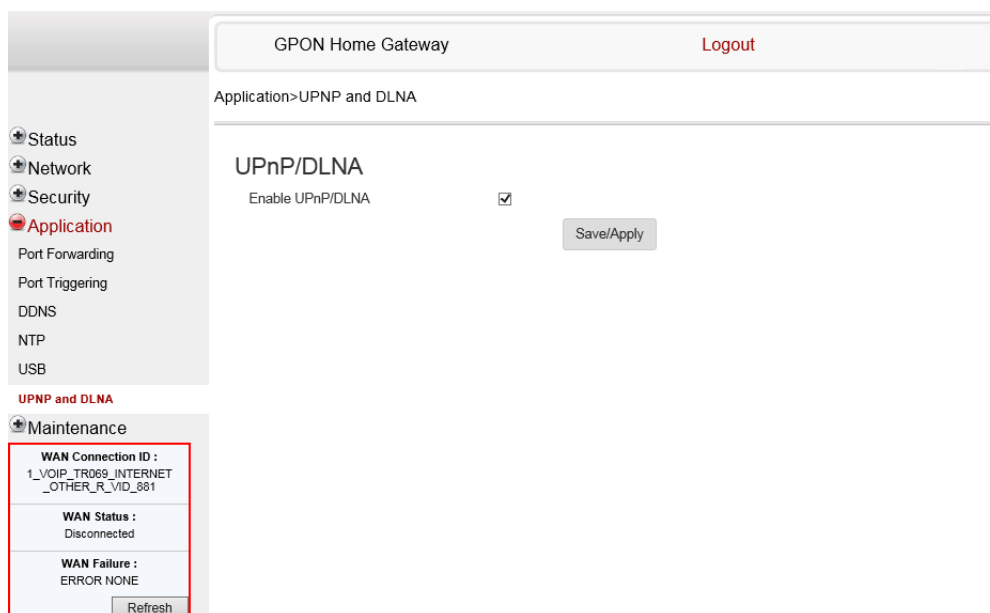
- 2
- Configure USB.

- 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



- 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.

Figure 60 Voice setting window

GPON Home Gateway

Logout

Application>Voice Setting

Status

Network

Security

Application

Port Forwarding

Port Triggering

DDNS

NTP

USB

UPNP and DLNA

Voice Setting

Maintenance

RG Troubleshooting

Voice Setting:

Outbound Proxy

Outbound Proxy Port

Proxy Server

Proxy Server Port

Registrar Server

Registrar Server Port

UserAgentDomain

UserAgentPort

DigitMap

DTMF mode

FaxT38

Line Setting:

POTS line

Enable

Directory Number

AuthUserName

AuthPassword

URI

Table 50 describes the fields in the Voice Setting window.

Table 50 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

(1 of 2)

Field	Description
Registrar Server	Enter the registrar server
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, Info, 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.

7.2.6 Maintenance

G-240W-G ONTs also supports 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

GPON Home Gateway Logout

Maintenance>Password

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

Original Password

New Password

Re-enter Password

Prompt Message

Save

WAN Connection ID :
1_VOIP_TR089_INTERNET
_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Refresh

Table 51 describes the fields in the password window.

Table 51 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

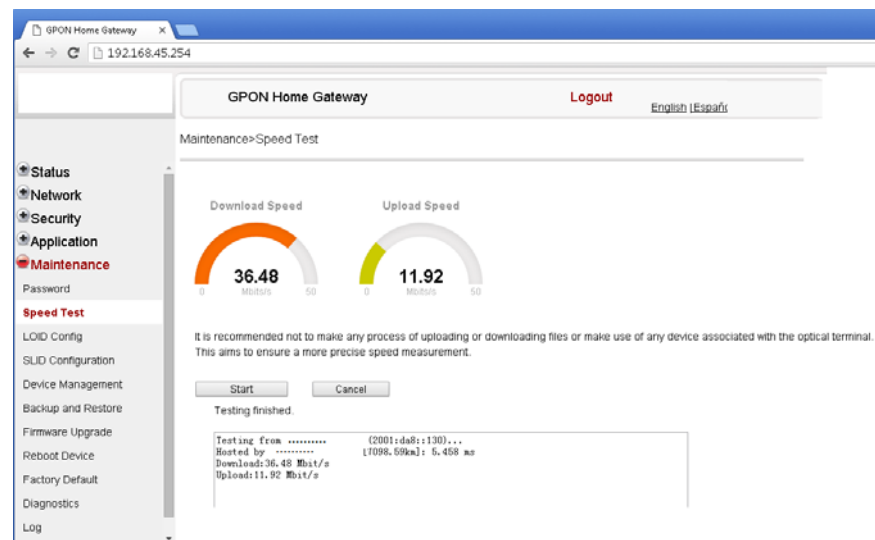
2 Configure the new password.

- 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



- 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

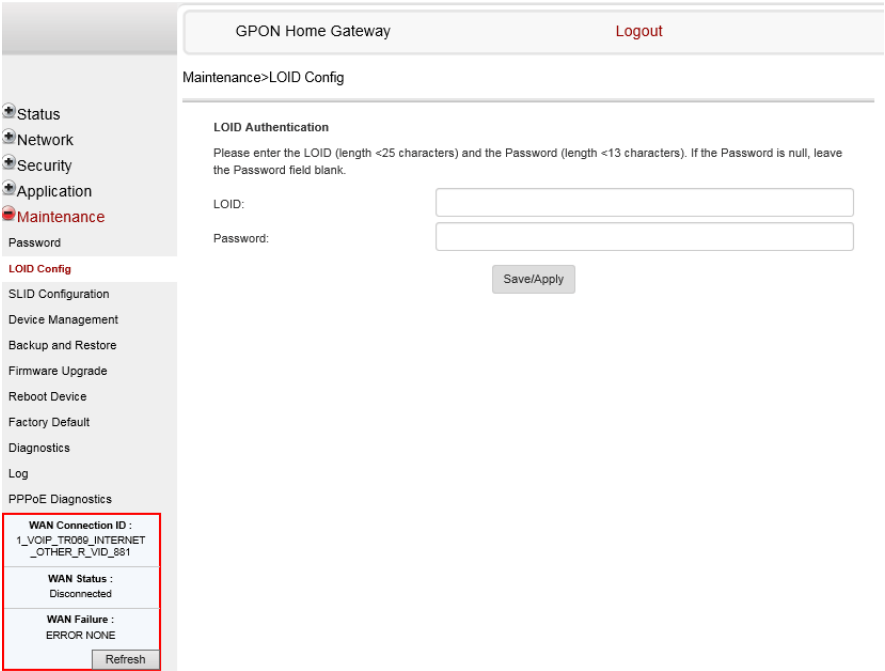


Table 52 describes the fields in the LOID configuration window.

Table 52 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

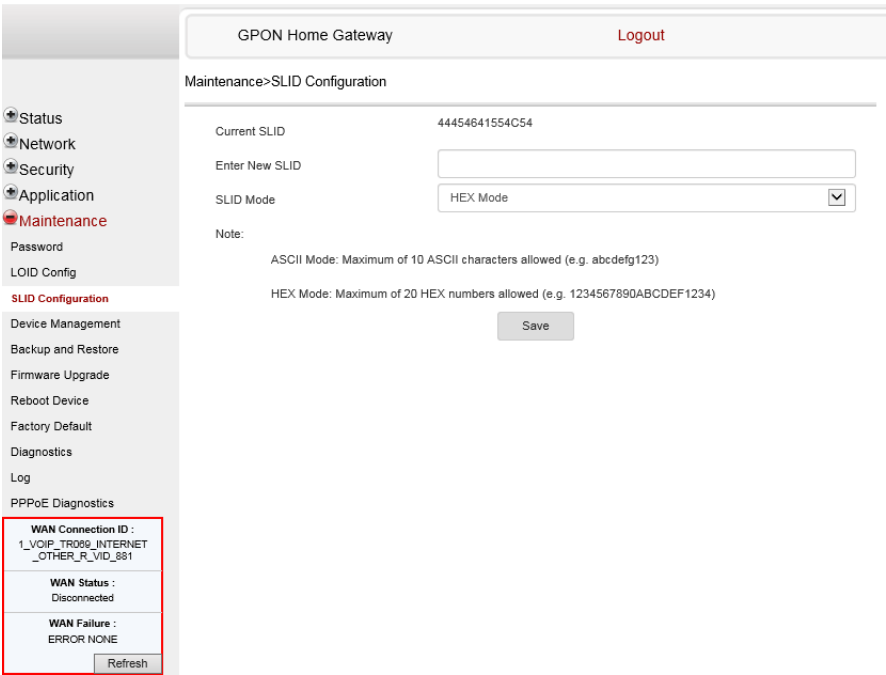


Table 53 describes the fields in the SLID configuration window.

Table 53 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

GPON Home Gateway

Logout

Maintenance>Device Management

Status

Network

Security

Application

Maintenance

Password

LOID Config

SLID Configuration

Device Management

Backup and Restore

Firmware Upgrade

Reboot Device

Factory Default

Diagnostics

Log

PPPoE Diagnostics

WAN Connection ID :
1_VOIP_TR006_INTERNET
_OTHER_R_VID_881

WAN Status :
Disconnected

WAN Failure :
ERROR NONE

Refresh

Host Name

yuqing-HP

Host Alias

Add

Host Name	Host Alias	Delete
-----------	------------	--------

Refresh

Table 54 describes the fields in the Device management window.

Table 54 Device management parameters

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

2 Configure an alias for a specific host.

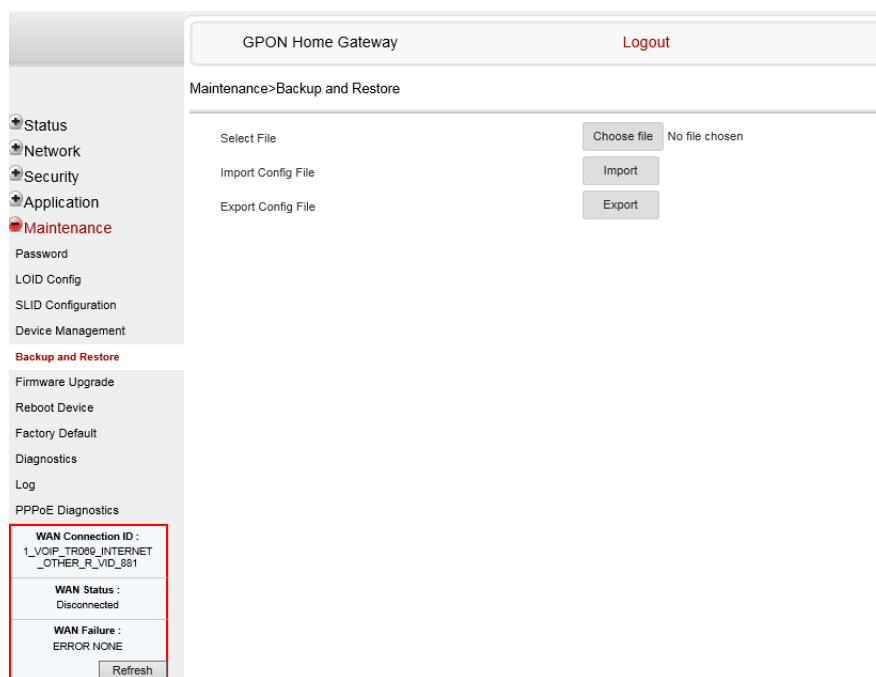
3 Click Add.

4 STOP. This procedure is complete.

Procedure 47 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



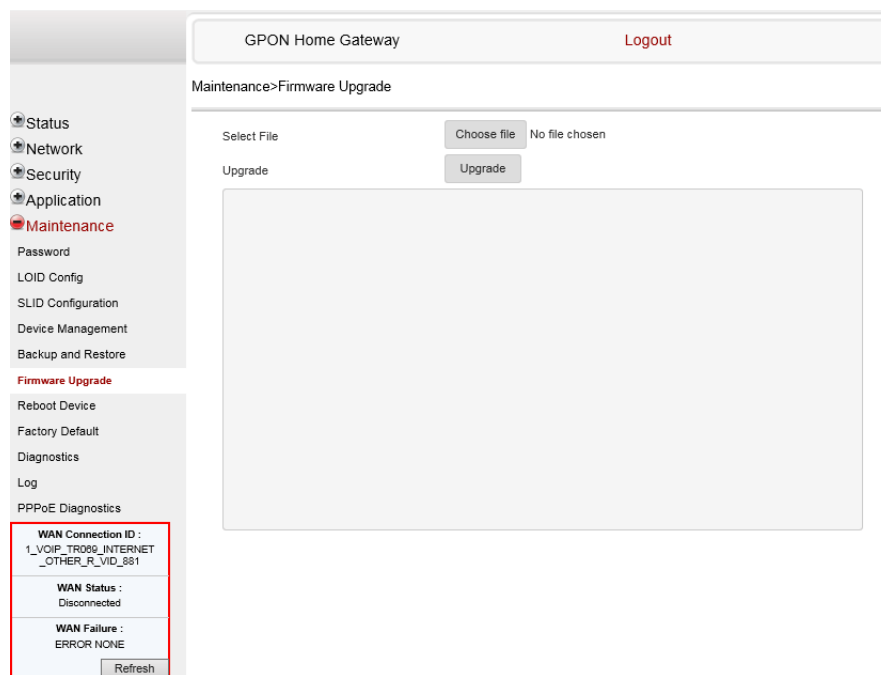
2 Click Choose file and select a backup file.

- 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

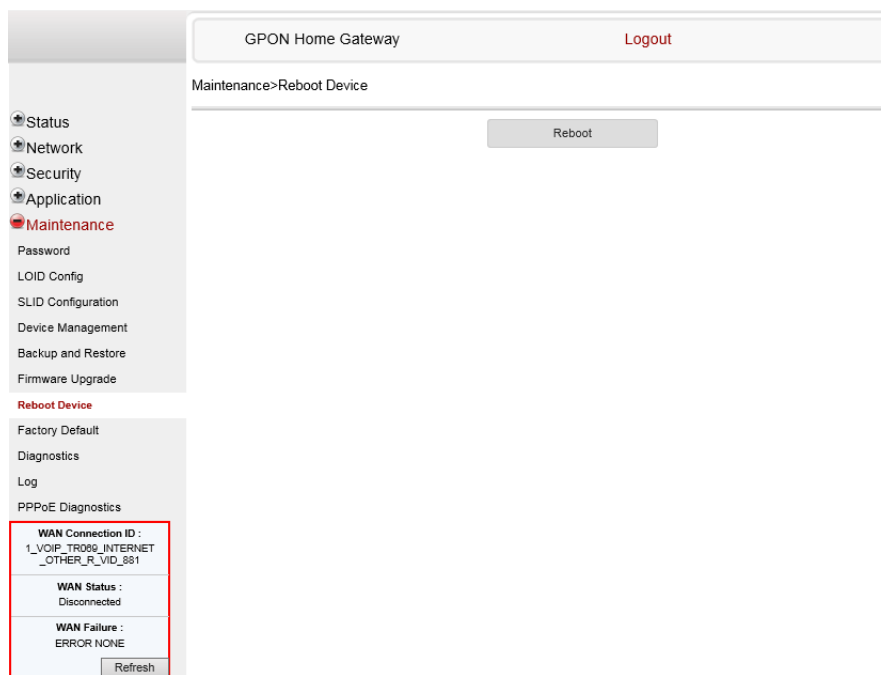


- 2 Click Choose file and select the firmware file.
- 3 Click Upgrade to upgrade the firmware.
- 4 STOP. This procedure is complete.

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

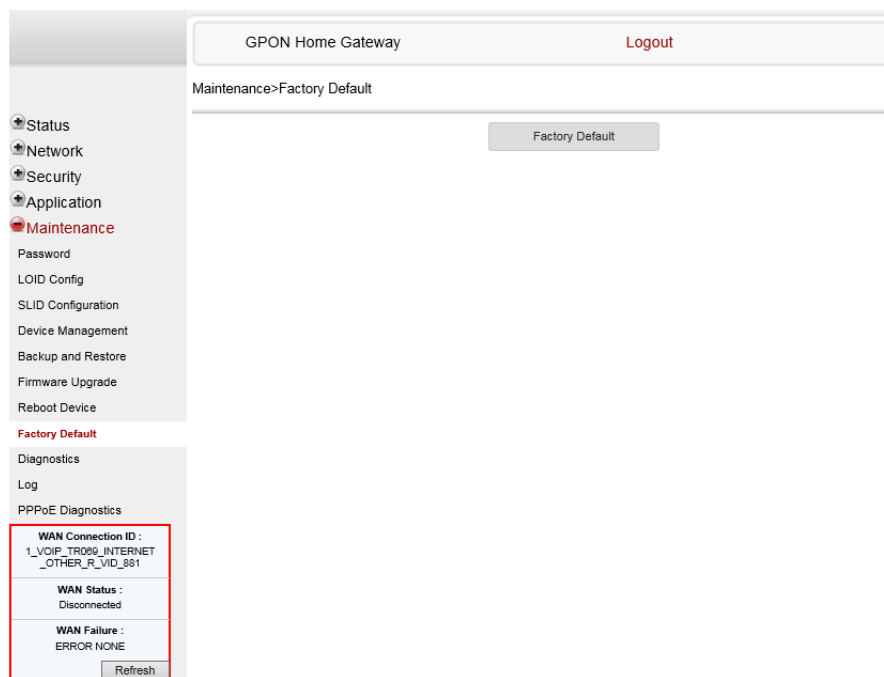


- 2 Click Reboot to reboot the ONT.
 - 3 STOP. This procedure is complete.
-

Procedure 50 Restore factory defaults

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

Figure 69 Factory default window

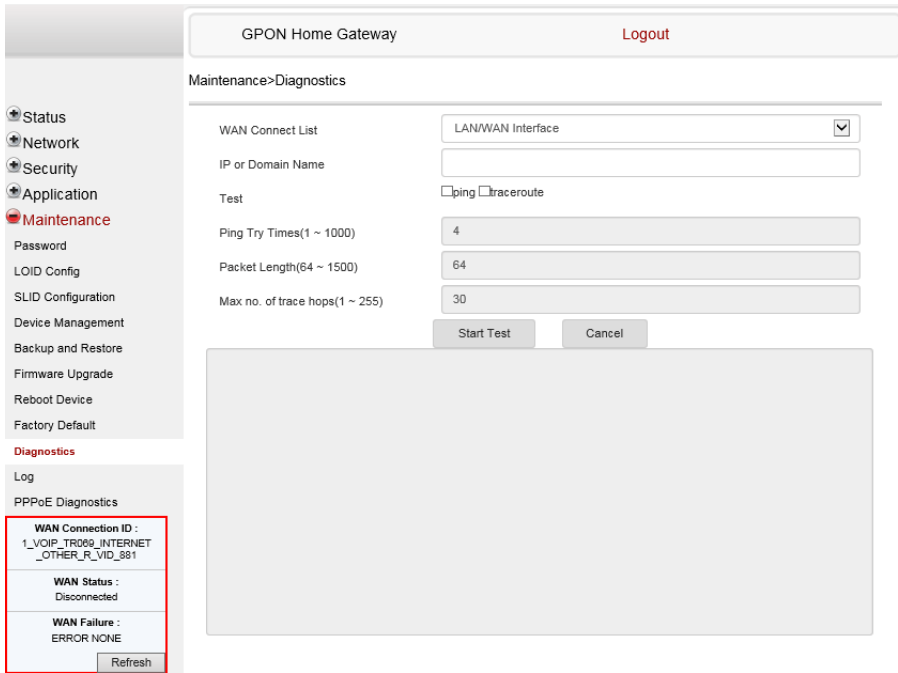


- 2 Click Factory Default to reset the ONT to its factory default settings.
- 3 STOP. This procedure is complete.

Procedure 51 Diagnose WAN connections

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

Figure 70 Diagnose window



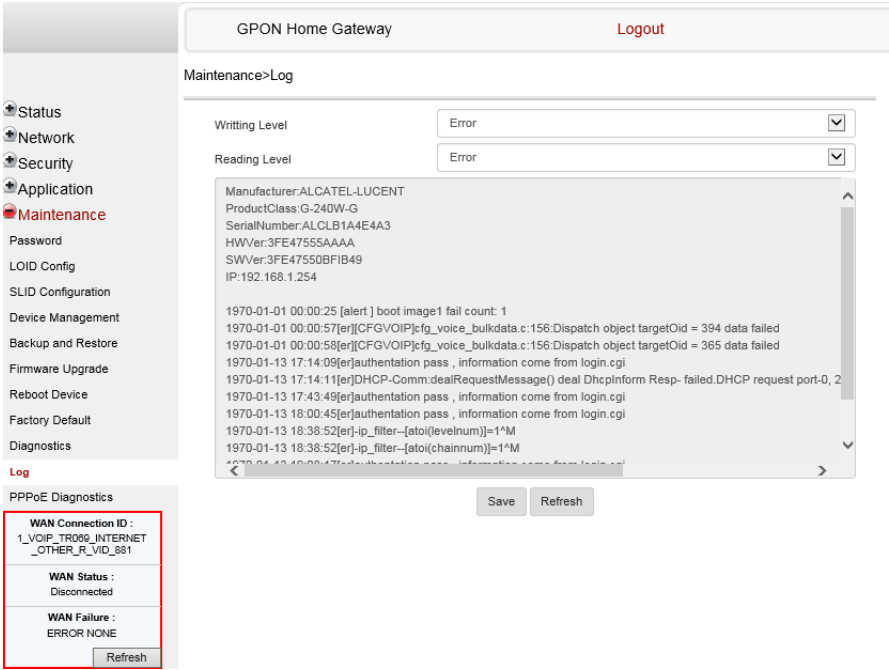
- 2 Choose a WAN connection to diagnose from the drop-down menu.
- 3 Enter the IP address or domain name.
- 4 Select the test type: ping, traceroute, or both.
- 5 Enter the number of ping attempts to perform (1 - 1000); the default is 4.
- 6 Enter a ping packet length (64-1024); the default is 64.
- 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.

- 9 Click Cancel to cancel the test.
- 10 STOP. This procedure is complete.

Procedure 52 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

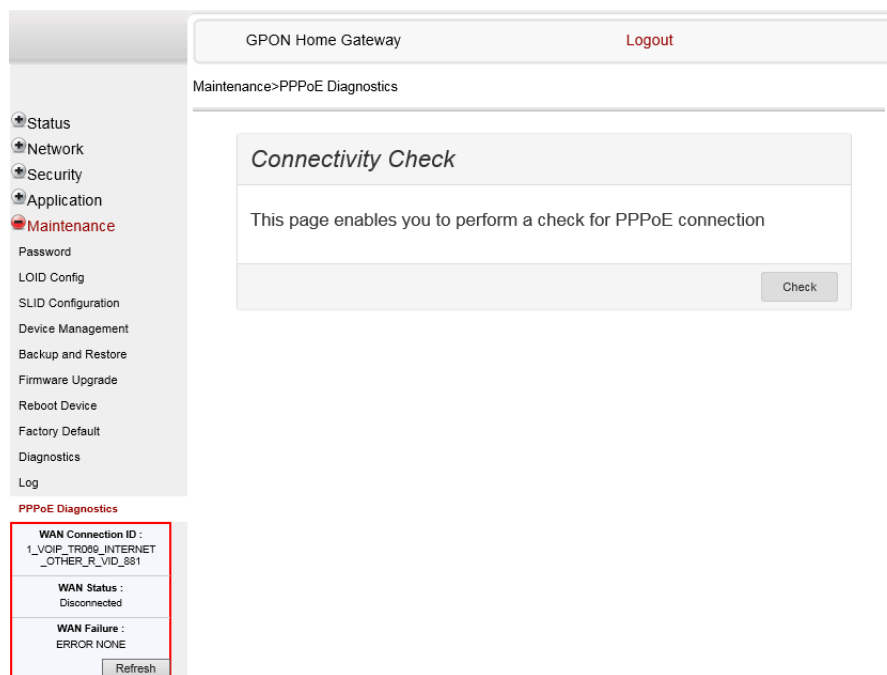


-
- 2 Choose a write level from the drop-down menu to determine which types of events are recorded in the log file:
 - Emergency
 - Alert
 - Critical
 - Error
 - Warning
 - Notice
 - Informational
 - Debug
-
- 3 Choose a reading level from the drop-down menu to determine which types of events to display 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



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

Figure 73 PPPoE diagnostics results

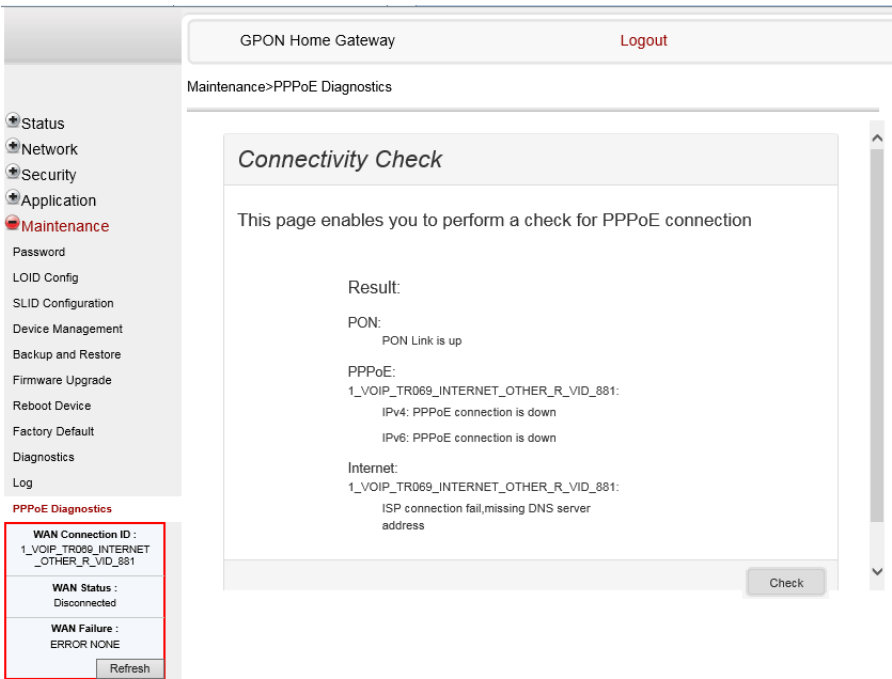


Table 55 describes the fields on the PPPoE diagnostics results window.

Table 55 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.

7.2.7 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

Table 56 describes the fields in the RG Troubleshooting Counters window.

Table 56 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
Internet Status	Whether the broadband connections is active (UP) or not (DOWN)

(1 of 2)

Field	Description
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

(2 of 2)

-
- 2 Configure the test times if desired.
 - 3 Click Refresh to update the data.
 - 4 STOP. This procedure is complete.
-

7.3 SFU mode configuration

HGU is the default mode for the G-240W-G ONT, but you can use SFU mode to view device status information, change the password, authenticate the LOID, and change the SLID.

7.3.1 Switch from default HGU mode to SFU mode

To switch from the default HGU mode to using SFU mode, use the procedure below.

Procedure 55 Switching to SFU mode

-
- 1 Power up the G-240W-G ONT.
 - 2 Change the Operator ID (OPID) to XXXX to enable the ONT to switch to SFU mode, as described in [“Modifying the operator ID”](#).
 - 3 Reboot the ONT.
 - 4 STOP. This procedure is complete.
-

Procedure 56 Modifying the operator ID

1 Register the ONT with the OLT.

2 Check the original OPID.

Use the T&D command on the ONT console (ri tool dump) to check the current OPID.

3 Using an XML editor, create a file called OntConfig.xml with the following content:

```
<OperatorObject version="1.0">
  <OperatorID="abcd">
</OperatorObject>
```

where: *abcd* is the correct operator ID, for example ALCL for HGU mode with TR-069 or TR-104 voice management, ALCO for HGU mode with OMCI V1 or V2 voice management, or XXXX for generic SFU mode.

4 Use a TFTP client tool to transfer the OntConfig.xml file to the OLT's ONT directory and change the filename to the software version number, for example, 3FE123456789.xml.

See the OLT documentation for the location of the ONT directory.

5 Use a TL1 command to configure ONUSWCRTL:

```
ENT-ONTSWCTRL::1:::HWVER=hwver,VARNT=,PLNSWVER=UNPLANNED,
PLNSWVERCONF=UNPLANNED,DLDSWVER=swver;
```

where:

hwver is the EQPTVERNUM, for example EQPTVERNUM=3FE12345AAAA.

swver is the software version number used as the filename in step 2, for example 3FE123456789.xml.

See the *TL1 Commands and Messages Guide* for the 7342 or 7360 for more information about the ENT-ONTSWCTRL command.

6 Download the xml file to update the operator ID:

```
ED-ONT::ONT-1/1/3/1/19:::DLSW=AUTO;
```

7 Restart the ONT, then connect to the LAN and use the T&D command on the ONT console (ri tool dump) to check the OPID.

8 Use a TL1 command to disable further downloads:

```
ED-ONT::ONT-1/1/3/1/19:::DLSW=DISABLED;
```

To enable auto download again, use the DEL-ONTSWCTRL command. See the *TL1 Commands and Messages Guide* for the 7342 or 7360 for more information about the DEL-ONTSWCTRL command.

-
- 9 STOP. This procedure is complete.
-

7.3.2 Login

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

Procedure 57 Login to web-based GUI

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

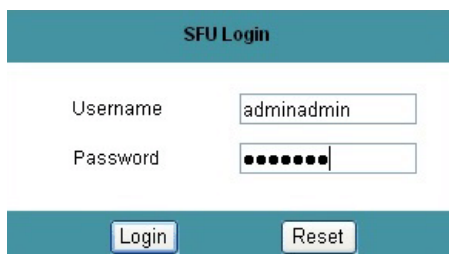
The login window appears.

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 subnet as the ONT.

-
- 2 Enter your username and password in the Log in window, as shown in Figure 75.

The default username is adminadmin. The default password is ALC#FGU.

Figure 75 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.
- 4 STOP. This procedure is complete.

7.3.3 Device and connection status

G-240W-G ONTs support the retrieval of a variety of device information.

Procedure 58 Device information retrieval

- 1 Select Status > Device Information from the top-level menu in the GPON Home Gateway window, as shown in Figure 76.

Figure 76 Device Information window

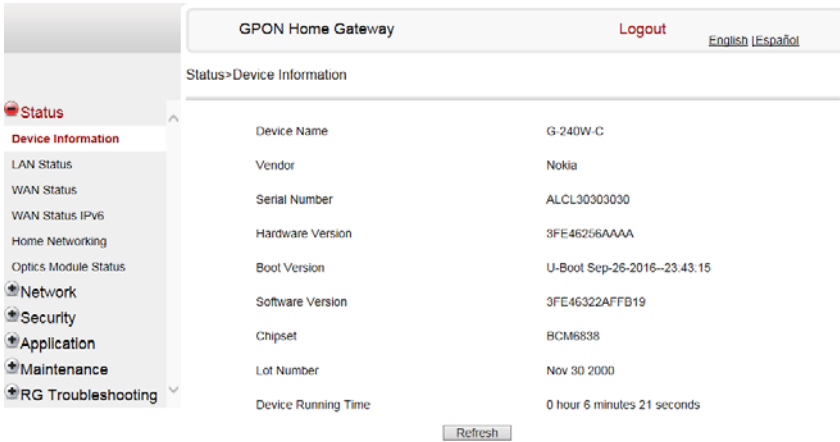


Table 57 describes the fields in the Device Information window.

Table 57 **Device Information parameters**

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
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.

7.3.4 Maintenance

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

- password change
- LOID configuration
- SLID configuration

Procedure 59 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 77.

Figure 77 Password window

Table 58 describes the fields in the password window.

Table 58 Password parameters

Field	Description
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 60 LOID configuration

-
- 1 Select Maintenance > LOID Config from the top-level menu in the GPON Home Gateway window, as shown in Figure 78.

Figure 78 LOID configuration window

The screenshot shows the 'GPON Home Gateway' web interface. At the top, there is a header bar with 'GPON Home Gateway' on the left, 'Logout' in red on the right, and language links 'English', 'Español', and '中文'. Below the header, a sidebar menu on the left contains 'Status', 'Maintain' (highlighted in red), 'Password', 'LOID Config' (highlighted in red), and 'SLID Configuration'. The main content area is titled 'Maintain>LOID Config'. Under the heading 'LOID Authenticate', there is a text instruction: 'Please input Loid(the length<25) and the password(the length<13).You need not to input anything when the password is null.' Below this, there are two input fields: 'LOID:' and 'Password:'. The 'LOID' field is empty, and the 'Password' field contains a series of dots. At the bottom of the form is a 'Save/Apply' button.

-
- 2 Enter the LOID.
 - 3 Enter the password, if applicable.
 - 4 Click Save/Apply.
 - 5 STOP. This procedure is complete.
-

Procedure 61 SLID configuration

- 1
- Select Maintenance > SLID Configuration from the top-level menu in the GPON Home Gateway window, as shown in Figure 79.

Figure 79 SLID configuration window



Table 59 describes the fields in the SLID configuration window.

Table 59 SLID configuration parameters

Field	Description
Current SLID	Displays current SLID
Input New SLID	Enter 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.

8 ONT configuration file over OMCI

8.1 Purpose

8.2 Supported configuration file types

8.3 ONT configuration file over OMCI

8.1 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.

8.2 Supported configuration file types

Table [60](#) describes the configuration file types that are supported from 7368 ISAM ONT R05.02.00 and later.

Table 60 **Supported configuration files**

File Index	Description	Details	Supported ONTs/DPU
PRE	ONT pre-configuration file	The XML-based PRECONFIG file controls the working mechanics of the ONT for various services. The default behavior of different ONTs may vary based on the factory settings. The pre-configuration file includes the factory default value for the residential gateway. Note: the pre-configuration file does not work with SFU ONTs; therefore, this feature applies only to Residential Gateway ONTs. The pre-configuration file can be used as is, but Nokia provides its customers with the flexibility to customize the pre-configuration file. This pre-configuration file enables operators to change the default behavior by downloading a customized pre-configuration based on customer inputs. This PRE XML file includes a custom OPERID. The Nokia defined index for the PRECONFIG file is: "PRE"	HGU ONTs: G-240G-C, G-240W-A, G-240W-B, G-240W-C, G-240W-G, 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)

File Index	Description	Details	Supported ONTs/DPU
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, I-240W-A

(2 of 2)

8.2.1 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.

8.3 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 62 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 8.2.

- 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*

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

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

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

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

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

Please note:

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

Examples

Note: 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](#)

