



Nokia ONT

G-1427G-A Product Guide

3TN-01705-AAAA-TCZZA
Issue 1
December 2025

© 2025 Nokia. Nokia Confidential Information

Use subject to agreed restrictions on disclosure and use.

Legal notice

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

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia.

This document is intended for use by Nokia's customers ("You"/"Your") in connection with a product purchased or licensed from any company within Nokia Group of Companies. Use this document as agreed. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia's site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Copyright and trademark: Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners.

© 2025 Nokia.

Contents

About this document.....	15
1 What's new.....	21
1.1 Overview	21
1.2 What's new in BBD Release 25.04	21
2 G-1427G-A unit data sheet	23
2.1 Overview	23
2.2 G-1427G-A part numbers and identification.....	23
2.3 G-1427G-A general description	26
2.4 G-1427G-A software and installation feature support	32
2.5 G-1427G-A interfaces and interface capacity	32
2.6 G-1427G-A LEDs	34
2.7 G-1427G-A detailed specifications.....	36
2.8 G-1427G-A GEM ports and T-CONTs	38
2.9 G-1427G-A performance monitoring statistics	38
2.10 G-1427G-A functional blocks	40
2.11 G-1427G-A standards compliance	41
2.12 G-1427G-A special considerations	43
3 Install or replace a G-1427G-A ONT.....	47
3.1 Overview	47
3.2 Prerequisites	47
3.3 Recommended tools	47
3.4 Safety information	48
3.5 Desktop mounting of G-1427G-A.....	49
3.6 Wall mount an G-1427G-A indoor ONT	49
3.7 Replace a G-1427G-A ONT	55
3.8 Replace a G-1427G-A indoor ONT	59
4 Configure a G-1427G-A indoor ONT	63
4.1 Overview	63
GUI overview	66
4.2 General configuration.....	66
4.3 HGU mode GUI configuration	66
4.4 New password rules	66
4.5 WAN services overview	66

4.6	Logging in to the web-based GUI	70
4.7	Viewing overview information.....	72
4.8	G-1427G-A WebGUI Menu	74
WAN Configuration		76
4.9	Overview	76
4.10	Configuring WAN Services.....	76
4.11	Viewing WAN Statistics	86
4.12	Configuring TR-069.....	89
4.13	Configuring TR-369.....	90
4.14	Configuring GRE tunnel	92
4.15	Configuring Static routing.....	93
4.16	Viewing Optical Module Status	95
4.17	Configuring QoS	96
4.18	Configuring Upstream (US) Classifier	99
LAN Configuration		106
4.19	Overview	106
4.20	Configuring DHCP IPv4	106
4.21	Configuring DHCP IPv6	108
4.22	Configuring DNS	110
4.23	Viewing LAN Statistics	113
WiFi Configuration		115
4.24	Overview	115
4.25	Configuring WiFi Network	115
4.26	Configuring the WiFi Password.....	120
4.27	Configuring IoT Network	121
4.28	Configuring Guest Network.....	122
4.29	Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points ..	124
4.30	Optimizing WiFi Network.....	128
4.31	Configuring Wireless 2.4 GHz.....	128
4.32	Configuring Wireless 5 GHz.....	131
4.33	Configuring Wireless Schedules	133
4.34	Viewing WiFi Statistics	134
Devices.....		137
4.35	Overview	137
4.36	Viewing Device Information.....	137

Voice Configuration	140
4.37 Overview	140
4.38 Configuring Voice Settings	140
4.39 Viewing Voice Status	142
Security Configuration	144
4.40 Overview	144
4.41 Configuring the Firewall	144
4.42 Configuring the MAC Filter	145
4.43 Configuring the IP Filter	147
4.44 Configuring the URL Filter	149
4.45 Configuring Family Profiles	151
4.46 Configuring DMZ and ALG	157
4.47 Configuring Access Control	159
Advanced Settings	163
4.48 Overview	163
4.49 Configuring Port Forwarding	163
4.50 Configuring Port Triggering	164
4.51 Configuring DDNS	165
4.52 Configuring NTP	166
4.53 Configuring UPNP and DLNA	168
Maintenance	169
4.54 Overview	169
4.55 Configuring the Password	169
4.56 Backing Up the Configuration	171
4.57 Restoring the Configuration	172
4.58 Upgrading Firmware	173
4.59 Configuring LOID	175
4.60 Configuring SLID	176
4.61 Diagnosing WAN Connections	178
4.62 Viewing Log Files	180
4.63 Generating a delta configuration file	182
Troubleshooting	185
4.64 Troubleshooting counters	185
4.65 Speed Test	187

5	ONT configuration file over OMCI	191
5.1	Overview	191
5.2	Purpose.....	191
5.3	Supported configuration file types.....	191
5.4	ONT configuration file over OMCI.....	194
6	Environmental and Regulatory Compliance.....	199
6.1	Overview	199
6.2	For EU regulation market.....	199

List of tables

Table 2-1	Identification of G-1427G-A indoor ONTs.....	23
Table 2-2	G-1427G-A power supply ordering information.....	24
Table 2-3	Plug types	25
Table 2-4	Hardware parts required for G-1427G-A installations	25
Table 2-5	Support for TR-181 parameter categories	30
Table 2-6	G-1427G-A indoor ONT interface connection capacity	32
Table 2-7	G-1427G-A indoor ONT physical connections	34
Table 2-8	G-1427G-A indoor ONT LED descriptions	35
Table 2-9	G-1427G-A indoor ONT physical specifications	37
Table 2-10	G-1427G-A indoor ONT power consumption specifications.....	37
Table 2-11	G-1427G-A indoor ONT environmental specifications	37
Table 2-12	G-1427G-A indoor ONT Dimension data specifications.....	37
Table 2-13	G-1427G-A indoor ONT capacity for GEM ports and T-CONTs	38
Table 2-14	Package S ONTs ONTENET performance monitoring statistics.....	39
Table 2-15	Package S ONTs ONTL2UNI performance monitoring statistics	39
Table 2-16	Package S ONTs PONONTTC, PONONTMCTC, PONONTTCHSI, PONONTTCES, PONONTTCFLOW, PONONTTCVOIP performance monitoring statistics	39
Table 2-17	Package S ONTs PONONTTC aggregate performance monitoring statistics.....	40
Table 2-18	G-1427G-A ONT considerations and limitations	44
Table 4-1	Supported combinations of OMCI and ACS/WebGUI	68
Table 4-2	G-1427G-A WebGUI Menu	74
Table 4-3	<i>WAN services</i> parameters	82
Table 4-4	<i>WAN statistics</i> parameters.....	88
Table 4-5	<i>TR-069</i> parameters	89
Table 4-6	<i>TR-369</i> parameters	91
Table 4-7	GRE Tunnel parameters	92
Table 4-8	<i>IP routing</i> parameters.....	94
Table 4-9	<i>Optical module status</i> parameters	95
Table 4-10	<i>QoS config</i> parameters	98
Table 4-11	<i>US Classifier - Policy</i> parameters	100
Table 4-12	<i>US Classifier - Classifier</i> parameters	102
Table 4-13	<i>US Classifier - Classifier Rules</i> parameters.....	105

Table 4-14	<i>DHCP IPv4 parameters</i>	108
Table 4-15	<i>Static DHCP parameters</i>	108
Table 4-16	<i>DHCP IPv6 parameters</i>	109
Table 4-17	<i>DNS parameters</i>	112
Table 4-18	<i>LAN statistics parameters</i>	113
Table 4-19	<i>Add WiFi network parameters</i>	117
Table 4-20	<i>Guest network parameters</i>	123
Table 4-21	<i><Device> parameters</i>	127
Table 4-22	<i>Wireless 2.4 GHz parameters</i>	130
Table 4-23	<i>Wireless 5 GHz parameters</i>	132
Table 4-24	<i>WLAN statistics parameters</i>	135
Table 4-25	<i>Voice Setting parameters</i>	142
Table 4-26	<i>Voice status parameters</i>	143
Table 4-27	<i>Firewall parameters</i>	145
Table 4-28	<i>MAC filter - Ethernet Interface parameters</i>	146
Table 4-29	<i>MAC filter - WiFi SSID parameters</i>	147
Table 4-30	<i>IP filter parameters</i>	148
Table 4-31	<i>URL filter parameters</i>	150
Table 4-32	<i>ALG Configuration parameters</i>	158
Table 4-33	<i>DMZ Configuration parameters</i>	159
Table 4-34	<i>Access control parameters</i>	161
Table 4-35	<i>Trusted Network parameters</i>	161
Table 4-36	<i>Port forwarding parameters</i>	164
Table 4-37	<i>Port triggering parameters</i>	165
Table 4-38	<i>DDNS parameters</i>	166
Table 4-39	<i>NTP parameters</i>	167
Table 4-40	<i>Change password parameters</i>	171
Table 4-41	<i>LOID config parameters</i>	176
Table 4-42	<i>SLID configuration parameters</i>	177
Table 4-43	<i>Diagnostics parameters</i>	178
Table 4-44	<i>Log parameters</i>	182
Table 4-45	<i>Troubleshooting counters parameters</i>	187
Table 4-46	<i>Speed test parameters</i>	188

Table 5-1	Supported configuration files.....	192
Table 6-1	Frequency bands and transmit power.....	201
Table 6-2	Applicable country codes	202

List of figures

Figure 2-1	G-1427G-A ONT	26
Figure 2-2	G-1427G-A indoor ONT physical connections (back).....	33
Figure 2-3	G-1427G-A indoor ONT with fiber optic connector	33
Figure 2-4	G-1427G-A indoor ONT LEDs	35
Figure 2-5	G-1427G-A ONT functional block	41
Figure 2-6	Sample laser product safety label on the ONT equipment	44
Figure 3-1	G-1427G-A on a desk	49
Figure 3-2	G-1427G-A ONT in wall mounting bracket	50
Figure 3-3	G-1427G-A wall mount bracket	51
Figure 3-4	Wall mount bracket power cord placement.....	52
Figure 3-5	Power cord to ONT connection.....	52
Figure 3-6	ONT to wall mount connection.....	53
Figure 3-7	ONT in wall mount bracket—facing the room	54
Figure 3-8	G-1427G-A ONT connections.....	55
Figure 3-9	Connecting the cables to the ONT	57
Figure 3-10	G-1427G-A indoor ONT connections.....	59
Figure 4-1	Common forwarding model	68
Figure 4-2	Login page	71
Figure 4-3	Overview table in WAN services page.....	77
Figure 4-4	Create New Connection page	78
Figure 4-5	Create New Connection page - PPPoE Configuration	79
Figure 4-6	VLAN mode - VLAN Binding.....	80
Figure 4-7	Bridge mode - Transparent.....	81
Figure 4-8	Bridge mode - Tunnel	82
Figure 4-9	WAN Statistics page	86
Figure 4-10	WAN Statistics page info	87
Figure 4-11	TR-069 page	89
Figure 4-12	TR-369 page.....	91
Figure 4-13	GRE Tunnel page	92
Figure 4-14	IP routing page	94
Figure 4-15	Optical module status page	95

Figure 4-16	QoS config page (L2 Criteria)	96
Figure 4-17	QoS config page (L3 Criteria)	97
Figure 4-18	US Classifier - Policy page	100
Figure 4-19	US Classifier - Classifier page	102
Figure 4-20	US Classifier - Classifier Rules page	104
Figure 4-21	DHCP IPv4 page	107
Figure 4-22	DNS page (IPv4)	111
Figure 4-23	DNS page (IPv6)	112
Figure 4-24	LAN statistics page	113
Figure 4-25	WiFi network page	116
Figure 4-26	Add WiFi network page	117
Figure 4-27	WiFi network - example of SSID Configuration page	118
Figure 4-28	Edit Wi-Fi network page	121
Figure 4-29	IoT network page	122
Figure 4-30	Guest network page	123
Figure 4-31	Network map page	124
Figure 4-32	<Device> page	126
Figure 4-33	Change the name of your WiFi point page	127
Figure 4-34	Advanced settings - 2.4 GHz tab	129
Figure 4-35	Advanced settings - 5 GHz tab	131
Figure 4-36	Wireless schedule page	133
Figure 4-37	WiFi statistics page	135
Figure 4-38	Devices page	137
Figure 4-39	Device information page - L3 devices	138
Figure 4-40	Device Rename page	139
Figure 4-41	Voice Setting page	141
Figure 4-42	Voice status page	143
Figure 4-43	Firewall page	144
Figure 4-44	MAC filter page	146
Figure 4-45	IP filter page	148
Figure 4-46	URL filter page	150
Figure 4-47	Family profiles (Parental control) page	151
Figure 4-48	Add a profile page	152

Figure 4-49	Assign devices to family profile	152
Figure 4-50	Family profiles table.....	153
Figure 4-51	Family profile configuration page.....	153
Figure 4-52	<i>DMZ and ALG</i> page.....	158
Figure 4-53	<i>Access control</i> page	160
Figure 4-54	<i>Port forwarding</i> page	163
Figure 4-55	<i>Port triggering</i> page	164
Figure 4-56	<i>DDNS</i> page	166
Figure 4-57	<i>NTP</i> page	167
Figure 4-58	<i>UPNP and DLNA</i> page	168
Figure 4-59	<i>Change password</i> page.....	170
Figure 4-60	<i>Backup and restore</i> page	171
Figure 4-61	<i>Backup and restore</i> page	172
Figure 4-62	Backup and restore: Serial number	173
Figure 4-63	<i>Firmware upgrade</i> page	174
Figure 4-64	Example of upgrade status messages	175
Figure 4-65	<i>LOID config</i> page.....	176
Figure 4-66	<i>SLID configuration</i> page	177
Figure 4-67	<i>Diagnostics</i> page	178
Figure 4-68	Example of ping results	179
Figure 4-69	Example of traceroute results	180
Figure 4-70	<i>Log</i> page.....	181
Figure 4-71	<i>Delta CFG Tool</i> page	183
Figure 4-72	<i>Troubleshooting counters</i> page	186
Figure 4-73	<i>Speed test</i> page	188
Figure 6-1	Recycling/take back/disposal of product symbol	200

About this document

Purpose

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

Intended audience

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

The reader must be familiar with general telecommunications principles.

Safety information

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

Safety Information Examples



DANGER

Hazard

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



WARNING

Equipment Damage

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



CAUTION

Service Disruption

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

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

Acronyms and initialisms

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

Nokia quality processes

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

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

Documents

Documents are available using ALED or OLCS.

To download a ZIP file package of the customer documentation

- 1

Navigate to <http://customer.nokia.com/s/> and enter your user name and password. If you are a new user and require access to this service, please contact your Nokia sales representative.
- 2

Select **Products**.
- 3

Type your product name in the **Find and select a product** field and click the search icon.
Select a product.
- 4

Click **Downloads: ALED** to go to the Electronic Delivery: Downloads page.
- 5

Select **Documentation** from the list.
- 6

Select a release from the list.
- 7

Follow the on-screen directions to download the file.

END OF STEPS

To access individual documents

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

-
- 1

Navigate to <http://customer.nokia.com/s/> and enter your user name and password. If you are a new user and require access to this service, please contact your Nokia sales representative.
 - 2

Select **Products**.
 - 3

Type your product name in the **Find and select a product** field and click the search icon. Select a product.
 - 4

Click **Documentation: Doc Center** to go to the product page in the Doc Center.
 - 5

Select a release from the **Release** list and click **SEARCH**.
 - 6

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

END OF STEPS

Procedures with options or substeps

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

Example of options in a procedure

At [Step 1](#), you can choose option a or b. At [Step 2](#), you must do what the step indicates.

- 1

This step offers two options. You must choose one of the following:
 - a. This is one option.
 - b. This is another option.
- 2

You must perform this step.

END OF STEPS

Example of required substeps in a procedure

At [Step 1](#), you must perform a series of substeps within a step. At [Step 2](#), you must do what the step indicates.

1

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

- a. This is the first substep.
- b. This is the second substep.
- c. This is the third substep.

2

You must perform this step.

END OF STEPS

Multiple PDF document search

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

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

To search multiple PDF files for a common term

1

Open Adobe Acrobat Reader.

2

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

3

Enter the search criteria.

4

Select **All PDF Documents In**.

5

Select the folder in which to search using the list.

6

Click **Search**.

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

END OF STEPS

Technical support

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

For ordering information, contact your Nokia sales representative.

How to comment

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

1 What's new

1.1 Overview

1.1.1 Purpose

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

1.1.2 Contents

1.1 Overview	21
1.2 What's new in BBD Release 25.04	21

1.2 What's new in BBD Release 25.04

The Product guide is a new guide in BBD Release 25.04, issue 1. In future releases, this chapter will provide tables of the feature and document changes applicable to this guide.

2 G-1427G-A unit data sheet

2.1 Overview

2.1.1 Purpose

2.1.2 Contents

2.1 Overview	23
2.2 G-1427G-A part numbers and identification	23
2.3 G-1427G-A general description	26
2.4 G-1427G-A software and installation feature support	32
2.5 G-1427G-A interfaces and interface capacity	32
2.6 G-1427G-A LEDs	34
2.7 G-1427G-A detailed specifications	36
2.8 G-1427G-A GEM ports and T-CONTs	38
2.9 G-1427G-A performance monitoring statistics	38
2.10 G-1427G-A functional blocks	40
2.11 G-1427G-A standards compliance	41
2.12 G-1427G-A special considerations	43

2.2 G-1427G-A part numbers and identification

Table 2-1, “Identification of G-1427G-A indoor ONTs” (p. 23) provides part numbers and identification information for the G-1427G-A indoor ONT.

Table 2-1 Identification of G-1427G-A indoor ONTs

Ordering kit part number	Provisioning number	Description	CLEI Code	CPR	ECI/ Bar code
3TN01703AA	3TN01705AA	G-1427G-A, GPON ONT supports 1 POTS port, 1x2.5GE + 3xGE UNI, WiFi 7, 2+2, no USB, 512 MB, internal 5dBi antennas, with black enclosure. Includes a 12V 1.5A wall-mounted AC/DC power adapter with 2-pin US input plug.	—	—	—

Table 2-1 Identification of G-1427G-A indoor ONTs (continued)

Ordering kit part number	Provisioning number	Description	CLEI Code	CPR	ECI/ Bar code
3TN01703BA	3TN01705BA	G-1427G-A, GPON ONT supports 1 POTS port, 1x2.5GE + 3xGE UNI, WiFi 7, 2+2, no USB, 512 MB, internal 5dBi antennas, with white enclosure. Includes a 12V 1.5A wall-mounted AC/DC power adapter with 2-pin EU input plug.	—	—	—
3TN01703BB Customer-specific variant	3TN01705BB	G-1427G-A, EU Plug 4KV, GPON ONT supports 1 POTS port, 1x2.5GE + 3xGE UNI, WiFi 7, 2+2, no USB, 512 MB, internal 5dBi antennas, with white enclosure. Includes a 12V 1.5A wall-mounted AC/DC power adapter with 2-pin EU input plug.	—	—	—
3TN01703CA	3TN01705CA	G-1427G-A, GPON ONT supports 1 POTS port, 1x2.5GE + 3xGE UNI, WiFi 7, 2+2, no USB, 512 MB, internal 5dBi antennas, with white enclosure. Includes a 12V 1.5A wall-mounted AC/DC power adapter with 3-pin UK input plug.	—	—	—

Table 2-2, “G-1427G-A power supply ordering information” (p. 24) provides the power supply information for the G-1427G-A ONT. For more information on power supplies, see the **Nokia ONT Power Supply and UPS Guide**. The power consumption is less than 18 W.

Table 2-2 G-1427G-A power supply ordering information

Ordering part number	Manufacturer	Applicable power supply model	Power information	Compliance detail	Notes
Kit: 3TN01703AA EMA: 3TN01705AA	RUIDE	RD1201500-C55-198MG/BW120150-UC6C-HH01	12V 1.5A wall-mounted AC/DC power adapter with 2-pin US input plug	ANSI municipality US, UL/CB certified	—
	MOSO	MS-V1500R120-018L0-US/SC980-U3			
Kit: 3TN01703BA EMA: 3TN01705BA	MOSO	MS-V1500R120-018L0-DE/SC980-V3	12V, 1.5A wall-mounted AC/DC power adapter with 2-pin EU input plug	Europe, CE/CB certified	-
	RUIDE	RD1201500-C55-198OG/BW120150-EC6C-HH01			
Kit: 3TN01703BB EMA: 3TN01705BB Customer-specific variant	MOSO	MS-V1500R120-018L0-DE/SC980-V3	12V, 1.5A wall-mounted AC/DC power adapter with 2-pin EU input plug	Europe, CE/CB certified	-
	RUIDE	RD1201500-C55-198OG/BW120150-EC6C-HH01			
Kit: 3TN01703CA EMA: 3TN01705CA	MOSO	MS-V1500R120-018L0-GB/SC980-B2	12V, 1.5A wall-mounted AC/DC power adapter with 3-pin UK input plug	Europe, CE/CB certified	—
	RUIDE	RD1201500-C55-198YG/BW120150-YC6C-LL00			

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

Table 2-3 Plug types

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

Table 2-4, “Hardware parts required for G-1427G-A installations” (p. 25) lists the hardware parts required for mounting an G-1427G-A ONT.

Table 2-4 Hardware parts required for G-1427G-A installations

Part	Description
ONT unit	The G-1427G-A ONT
Wall mount bracket (Optional) (3FE49555AA)	The wall mount bracket is fastened to a wall. The G-1427G-A is seated in the wall mount bracket, with white color, 72 pieces per box.
Wall mount bracket (Optional) (3TN01607AA)	The wall mount bracket is fastened to a wall. The G-1427G-A is seated in the wall mount bracket, with black color, 72 pieces per box.
Mounting screws	Two screws are required to mount the wall mount bracket. The recommended screw is a M4 or #6.

2.3 G-1427G-A general description

G-1427G-A indoor ONTs provide the subscriber interface for the network by terminating the PON interface and converting it to user interfaces that directly connect to subscriber devices.

The G-1427G-A has built-in concurrent dual-band Wi-Fi® 802.11 b/g/n/ax/be and 802.11ac/ax/be networking with triple play capability and can provide triple play services with voice, video, and data. The G-1426G-A supports Wi-Fi 7 and Wi-Fi EasyMesh™. This coverage can be expanded by installing additional Wi-Fi EasyMesh-capable beacons.

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

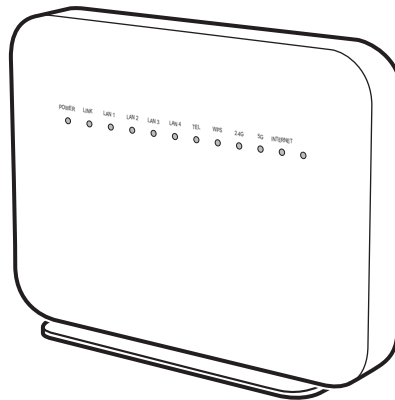
Note: The Nokia WiFi Care Portal can be accessed by the end user and the operator.

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

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

Figure 2-1, "G-1427G-A ONT " (p. 25) shows the G-1427G-A ONT.

Figure 2-1 G-1427G-A ONT



40575

G-1427G-A indoor ONTs provide the following functions:

- GPON uplink: G.984 and G.988 series standard compliant
- Wavelength: 1490 nm downstream; 1310 nm upstream
- Supports WBF filter. The GPON ONTs can co-exist with XGSPON ONTs in the same PON.
- Optics that support received signal strength indication (RSSI)
- G.984.3-compliant Advanced Encryption Standard (AES) in downstream
- Forward Error Correction (FEC)

-
- One 2.5 Gigabit standard RJ-45 2500/1000/100/10 Mbps, auto negotiating Ethernet ports and MDI/MDIX auto sensing
 - Three Gigabit standard RJ-45 1000/100/10 Mbps, auto negotiating Ethernet ports and MDI/MDIX auto sensing
 - One FXS port for VoIP service with RJ-11 connector
 - 512MB NAND Flash with bad block management, 512 MB DDR4 RAM, pin2pin compatible design for possible upgrade of RAM/Flash
 - Dual-band concurrent 2x2 IEEE 802.11 b/g/n/ax/be 2.4 GHz and 802.11ac/ax/be MIMO 5 GHz
 - Supports 802.11 b/g/n/ax/be 2x2 Wireless 2.4 GHz MIMO; Channel bandwidth 20, 40, 20/40 MHz
 - Supports 802.11ac/ax/be 2x2 Wireless 5 GHz Mu-MIMO; Channel bandwidth 20, 40, 80, 160 MHz PHY rate: 688.2 Mbps for 2.4 G and 2882.4 Mbps for 5 G
 - Internal antennas with 5dBi gain for each
 - WPA2, WPA2-PSK/AES
 - WPA3

Notes:

- When the channel bandwidth is configured to Auto in the ETSI domain, during boot up, operating channel of 80Mhz bandwidth will be selected. And during the maintenance time (3:00 am to 4:00 am) window, the ONT tries to expand the bandwidth to 160MHz after 10 minutes (depending on the channel selection by the initial channel selection algorithm) to complete Connection Admission Control (CAC) as required by the regulation. During this period, the 5GHz SSIDs of the ONT will not be operational and 2.4GHz SSIDs can be connected instead. After the 5GHz SSIDs come to operational, the WiFi client connection can be band-steered to 5GHz if appropriate.
- When the ONT is operational and needs to fall back from 160MHz to 80MHz channel bandwidth, it will only attempt to change to 160MHz during the maintenance time (3:00 am to 4:00 am) window. Hence, the potential 10-minute CAC will create minimal impact. You can change this behavior through the configuration file by either limiting to 80MHz channels only (will limit CAC to 1 minute) or by disabling the expansion from 80MHz to 160MHz during the maintenance time window.
- Support for multiple SSIDs (private and public instances); contact your Nokia representative for further details.
- Conductive power: 250 mW/24 dBm (2.4 GHz); 400 mW/26 dBm (5GHz)
- Maximum effective isotropic radiated power (EIRP): 5 dBi internal antenna: 800 mW/29 dBm (2.4GHz); 1260 mW/31 dBm (5GHz). Specific country variants of the ONT will further limit to comply with the regulatory limits.
- Bridged mode or routed mode per LAN port
- TR-069 support
- TR-181 support
- TR-157 LXC support
- Ethernet-based Point-to-Point (PPPoE)
- The dual stack WAN (IPv4 and IPv6) can work in different IP address mode for DHCP mode (static/dynamic mode).

-
- DHCP client/server
 - DNS server/client
 - DDNS
 - Port forwarding
 - Network Address Translation (NAT)
 - Network Address Port Translation (NAPT)
 - UPnP IGD2.0 support
 - ALG
 - IGMP snooping and proxy (v2/v3)
 - Traffic classification and QoS capability
 - OMCI/TR-069 Web GUI configuration
 - Performance monitoring and alarm reporting
 - Remote software image downloading and activation
 - IP/MAC/URL filter
 - Multi-level firewall and ACL
 - SoftGRE supports IPv4 and IPv6 tunnel
 - Speed Test support
 - Supports ACS lock feature
 - WiFi on/off push button
 - WPS on/off push button
 - Reset button
 - USB 2.0 interface (Optional)
Note: Some variants of G-1427G-A do not support USB.
 - Triple-Play services, including voice, video and high speed Internet access
 - Support for fax services
 - Built-in layer 2 switch; Line Rate L2 traffic
 - IP video distribution
 - VLAN tagging/detagging and marking/remarking of IEEE 802.1p per Ethernet port
 - Dying gasp support
 - Voice Services via Session Initiation Protocol (SIP)
 - Multiple voice codecs
 - DTMF dialing
 - Echo cancellation (G.168)
 - Fax mode configuration (T.30/T.38)
 - Caller ID, call waiting, call hold, 3-way calling, call transfer, message waiting

2.3.1 TR-069 authentication using TLS and CA certificates

G-1427G-A ONTs support TLS, as well as ACS authentication using SHA-256 pre-installed certificates.

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

The G-1427G-A ONTs support TLSv1.3 for TR-069. The ONT supports download certification from ACS.

2.3.2 TR-104 parameter extension support for voice service

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

The -104 Voice Service Object is:

InternetGatewayDevice.Services.VoiceService.{i}.Capabilities.SIP.

The vendor specific attribute is: X_ALU-COM_XML_File_Name_Path.

2.3.3 TR-104 voice-related alarms

The G-1427G-A 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
- SIPREGERR: error response from the registration server

2.3.4 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

2.3.5 TR-111 support

The G-1427G-A ONT supports TR-111, which extends the WAN Management Protocol defined in TR-069 to enhance the ability to remotely manage LAN devices.

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

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

2.3.6 TR-157 support

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

The TR-157 objects are:

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

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

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

2.3.7 TR-181, TR-098, TR-104, TR-157 parameter support

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

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

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

Table 2-5 Support for TR-181 parameter categories

Parameter category	Functionality
Device info and statistics	Device information
	Optical statistics
	Ethernet statistics
	Wi-Fi statistics
	Bridge statistics
	PPP statistics
	IP statistics
	Periodic statistics
	Voice statistics

Table 2-5 Support for TR-181 parameter categories (continued)

Parameter category	Functionality
Diagnostics	Wi-Fi diagnostic
	Ping
	Trace route
	TR-143 Speed test
	Self test
	Voice diagnostics
	NSLookup diagnostics
Optical configuration	
Forwarding configuration	Ethernet
	Bridge
	PPP
	IP
	Routing
	QoS
	DSLite
	NAT
	Neighbor discovery
Hosts configuration	
Wi-Fi configuration	
Service configuration	Voice service
	DDNS
	DNS
	DHCP
	GRE
	IGMP
	NTP timing
Firewall	
WebGUI configuration	
Nokia Wi-Fi configuration	Nokia Wi-Fi cloud service



Note: Due to the internal chipset architecture, the application session time-out is not fully precise and ranges from session timer to session timer + 20 seconds. The applications with a session timer are ICMP connections, TCP sessions, and UDP sessions. The default session

time-out of an ICMP connection is 30 seconds. The background of this constraint is that the application session time-out is maintained and refreshed by both the software and hardware session timers maintained separately. The hardware session timer refreshes the software session timer, which results in the deviation of the software timer. The range of application session time is from session timer to session timer + 20 seconds.

2.4 G-1427G-A software and installation feature support

For information on installing or replacing the G-1427G-A see [Chapter 3, “Install or replace a G-1427G-A ONT”](#).

For information on the following topics, see the **Nokia 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

2.5 G-1427G-A interfaces and interface capacity

The following table describes the supported interfaces and interface capacity for G-1427G-A indoor ONTs.

Table 2-6 G-1427G-A indoor ONT interface connection capacity

ONT type and model	Maximum capacity			
	POTS	2500/1000/100/10 BASE-T	1000/100/10 BASE-T	GPON SC/APC
G-1427G-A ¹	1	1	3	1

Notes:

1. The G-1427G-A ONTs provide WiFi service that is enabled and disabled using a WiFi on/off switch.

2.5.1 G-1427G-A connections and components

[Figure 2-2, “G-1427G-A indoor ONT physical connections \(back\)” \(p. 33\)](#) shows the physical connections for G-1427G-A indoor ONTs.

Figure 2-2 G-1427G-A indoor ONT physical connections (back)

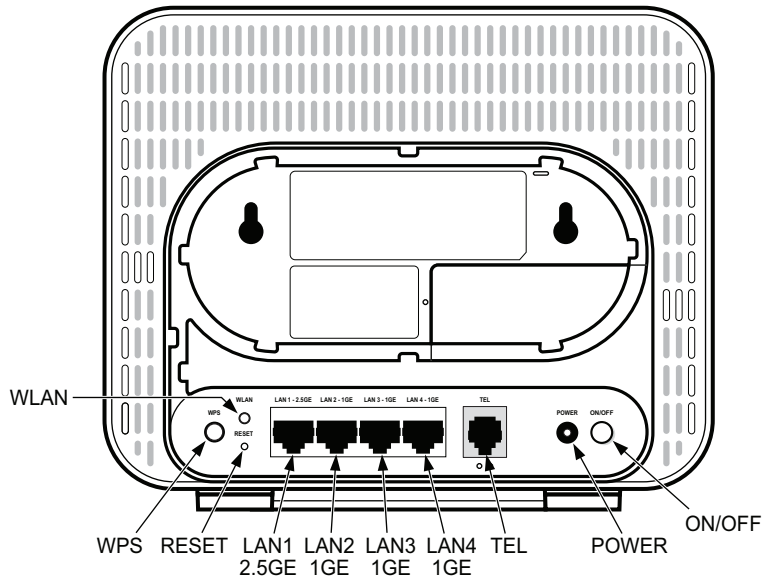


Figure 2-3, “G-1427G-A indoor ONT with fiber optic connector” (p. 33) shows the G-1427G-A indoor ONT with a fiber optic connector.

Figure 2-3 G-1427G-A indoor ONT with fiber optic connector

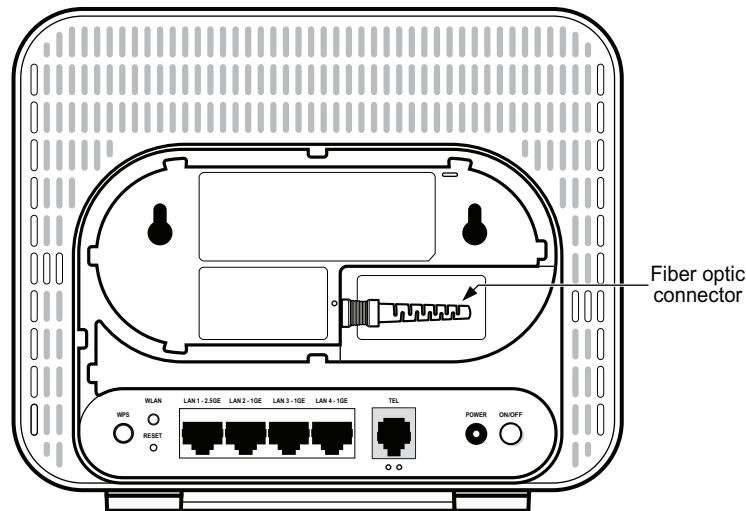


Table 2-7, “G-1427G-A indoor ONT physical connections” (p. 33) describes the physical connections for G-1427G-A indoor ONTs.

Table 2-7 G-1427G-A indoor ONT physical connections

Connection ¹	Print Letters	Description
WPS button	WPS	The WiFi Protected Setup (WPS) button enables and disables the WPS for 2.4GHz and 5GHz.
WLAN button	WLAN	Wi-Fi service is compliant with IEEE 802.11 standards and is enabled and disabled using the WLAN button.
Reset button	RESET	Pressing the Reset button for less than 10 seconds reboots the ONT; pressing the Reset button for 10 seconds resets the ONT to the factory defaults, except for the LOID and SLID. Accessible through a 2mm pin hole.
Ethernet ports	LAN1- 2.5GE	This connection is provided through Ethernet RJ-45 connectors. One 2500/1000/100/10 Base-T Ethernet interfaces are supported. The Ethernet ports can support both data and in-band video services on this interface.
	LAN2-1GE, LAN3-1GE, to LAN4-1GE	This connection is provided through Ethernet RJ-45 connectors. Up to three 1000/100/10 Base-T Ethernet interfaces are supported. The Ethernet ports can support both data and in-band video services on all three interfaces.
POTS port	TEL	This connection is provided through an RJ-11 port. One POTS connection is supported. The POTS port supports voice services.
Power input	POWER	This connection is provided through the power connector. A power cable fitted with a barrel connector is used to make the connection.
On/Off button	ON/OFF	This button turns the ONT on or off.
Fiber optic port	-	The SC/APC fiber optic port is located at the back of the ONT and provides the connection for the fiber optic cable.

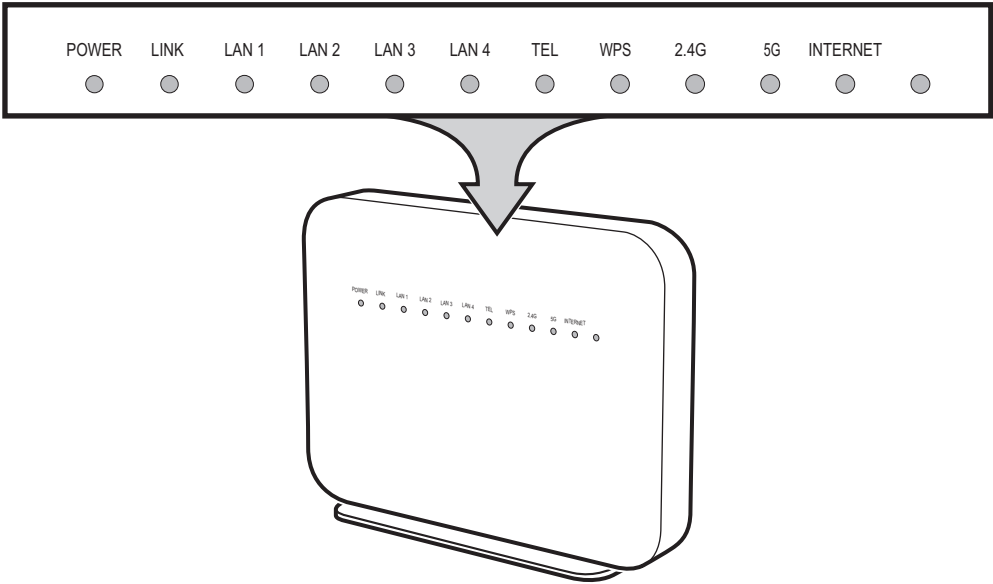
Notes:

1. The primary path for the earth ground for these ONTs is provided by the 12V return signal in the power connector.
2. USB connection is provided through one USB port on the ONT. The ONT supports external USB hard drives that can be made accessible to all LAN devices. This port is optional.

2.6 G-1427G-A LEDs

Figure 2-4, “G-1427G-A indoor ONT LEDs” (p. 35) shows the G-1427G-A indoor ONT LEDs.

Figure 2-4 G-1427G-A indoor ONT LEDs



40578

Table 2-8, “G-1427G-A indoor ONT LED descriptions” (p. 35) provides LED descriptions for G-1427G-A indoor ONTs.

Table 2-8 G-1427G-A indoor ONT LED descriptions

Indicator	LED color and behavior	LED behavior description
POWER	Green solid	Power on.
	Green flashing fast	Software update in progress.
	Green flashing slow	Failure at startup or loopback detected
	Off	Power off.
LINK	Green solid	ONT is configured on the OLT and is in service (UP). Device in O5 status and service configured, based on OMCI communication except MIB RESET.
	Green flashing fast	ONT is attempting to range with OLT. Device in O2/O3/O4 status, or O5 without Service Configured.
	Green flashing slow	ONT is disabled (Device in O7 status).
	Off	GPON link is down or no link is connected (Device in O1 status).
LAN 1 to 4	Green solid	ONT is connected to the associated LAN port (includes devices with wake-on-LAN capability where a slight voltage is supplied to an Ethernet connection).
	Green flashing	LAN activity is present (traffic in either direction).
	Off	ONT power is off or Ethernet is not connected.

Table 2-8 G-1427G-A indoor ONT LED descriptions (continued)

Indicator	LED color and behavior	LED behavior description
TEL	Green solid	Phone is off hook and VoIP service is build up.
	Green flashing fast	Phone is in "call in" or "talking" condition.
	Green flashing slow	VoIP service is out of service
	Off	All phones are on hook.
WPS	Green solid	Wi-Fi protected setup link is up (negotiation and auto-configuration successful).
	Green flashing slow	Wi-Fi protected setup link activity (negotiation and auto-configuration ongoing).
	Green flashing fast	WPS session overlap detected.
	Off	Wi-Fi protected setup link down or no link connected (negotiation has not started or has failed). Wi-Fi protected setup processing exception or multiple peers using WPS simultaneously.
2.4 GHz	Green solid	WLAN link is enabled in 2.4 GHz.
	Green flashing	Traffic is passing through the WLAN link.
	Off	WLAN link is disabled or no link is connected.
5 GHz	Green solid	WLAN link is enabled in 5 GHz.
	Green flashing	Traffic is passing through the WLAN link.
	Off	WLAN link is disabled or no link is connected.
INTERNET	Green solid	IP connected (the device has a WAN IP address from IPCP/DHCP/Static and Broadband link is up) and no traffic detected. If the IP or PPPoE session is dropped due to an idle timeout, the light will remain green if PON link is still present. If the session is dropped for any other reason, the light is turned off.
	Green flickering	PPPoE or DHCP connection is in progress.
	Off	Broadband physical connection power off, device in bridged mode with no IP address assigned to the device, or Broadband physical interface connection not present.
USB ¹	Green solid	A device is connected to the USB port.
	Green flashing	Traffic is passing through the USB connection.
	Off	No device is connected to the USB port.

Notes:

1. Some variants of G-1427G-A do not support USB.

2.7 G-1427G-A detailed specifications

Table 2-9, "G-1427G-A indoor ONT physical specifications" (p. 37) lists the physical specifications for G-1427G-A indoor ONTs.

Table 2-9 G-1427G-A indoor ONT physical specifications

Description	Specification
Depth of the bottom plate	46 mm (1.81 in.)
Length	193 mm (7.59 in.)
Width	32 mm (1.25 in.)
Height	159 mm (6.25 in.)
Weight [within ± 0.5 lb (0.23 kg)] (net weight of ONT)	0.370 Kg (0.81 lb)

Table 2-10, “G-1427G-A indoor ONT power consumption specifications” (p. 37) lists the power consumption specifications for G-1427G-A indoor ONT.

Table 2-10 G-1427G-A indoor ONT power consumption specifications

Mnemonic	Maximum power (Not to exceed)	Condition	Minimum power	Condition
G-1427G-A	18 W	1 POTS off-hook, all four Ethernet ports and 2.4G/5G WiFi DBDC are operational, USB port is linked.	6.4 W	2.4G/5G WiFi is operational, 1 POTS on-hook, other interfaces/services not provisioned

Table 2-11, “G-1427G-A indoor ONT environmental specifications” (p. 37) lists the environmental specifications for G-1427G-A indoor ONT.

Table 2-11 G-1427G-A indoor ONT environmental specifications

Mounting method	Temperature range and humidity	Altitude
On desk or shelf	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)	

Table 2-12, “G-1427G-A indoor ONT Dimension data specifications” (p. 37) lists the dimension data specifications for G-1427G-A indoor ONT.

Table 2-12 G-1427G-A indoor ONT Dimension data specifications

Dimensions	Specifications
Packet size supported	2000 bytes
Number of IP addresses supported (or ranges)	In LAN network, the supported range is: • IPv4: 192.168.1.1 ~192.168.1.253 • IPv6: No limitation
Number of supported WiFi clients (per radio, per device, per mesh)	64 per radio, 128 per device, 256 per mesh
Number of supported Beacons/APs in a mesh	6 (including the device)

Table 2-12 G-1427G-A indoor ONT Dimension data specifications (continued)

Dimensions	Specifications
Number of supported WAN interfaces	Supports 8 WAN connections
Number of supported VLANs	Supports 4094 VLANs
Number of priority queues, and overall buffer size	256 priority queues. Max 16MB for WAN and 4MB for LAN, 512KB SRAM buffer in PONMAC
Number of multicast groups (DAACL entries)	512

2.8 G-1427G-A GEM ports and T-CONTs

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

Table 2-13 G-1427G-A indoor ONT capacity for GEM ports and T-CONTs

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

2.9 G-1427G-A performance monitoring statistics

The following section identifies the supported performance monitoring statistics for G-1427G-A ONTs. A check mark indicates the statistic is supported on that ONT. An empty cell indicates the statistic is not supported. The following tables are categorized by supported alarm types:

- [Table 2-14, “Package S ONTs ONTENET performance monitoring statistics” \(p. 39\)](#) provides statistics for ONTENET type counters
- [Table 2-15, “Package S ONTs ONTL2UNI performance monitoring statistics” \(p. 39\)](#) provides statistics for ONTL2UNI type counters
- [Table 2-16, “Package S ONTs PONONTTC, PONONTMCTC, PONONTTCHSI, PONONTTCES, PONONTTCFLOW, PONONTTCVOIP performance monitoring statistics” \(p. 39\)](#) provides statistics for PONONTTC, PONONTMCTC, PONONTTCHSI, PONONTTCES, PONONTTCFLOW, and PONONTTCVOIP type counters
- [Table 2-17, “Package S ONTs PONONTTC aggregate performance monitoring statistics” \(p. 40\)](#) provides statistics for PONONTTC aggregate type counters

Note: If you have trouble accessing G-1427G-A ONTs performance monitoring statistics using TL1, please contact your Nokia support representative for more information about how to access and retrieve performance monitoring type counters.

The following table provides statistics for ONTENET type counters

Table 2-14 Package S ONTs ONTENET performance monitoring statistics

ONT	ONTENET statistics													
	FCSE	EC	LC	RBO	SCF	MCF	DT	IMTE	CSE	AE	IMRE	FTL	TBO	SQE
G-1427G-A ¹	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Notes:

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

Table 2-15 Package S ONTs ONTL2UNI performance monitoring statistics

ONT	ONTL2UNI statistics									
	FRAMES	BYTES	MCFRAMES	DSDRPFMRMS	USDRPFMRMS	USFRAMES	DSFRAMES	DSBYTES	USMCFRAMES	DSMCFRAMES
G-1427G-A ¹	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Notes:

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

Table 2-16 Package S 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-1427G-A ¹	✓	✓	✓	✓	✓	—

Notes:

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

Table 2-17 Package S ONTs PONONTTC aggregate performance monitoring statistics

ONT	PONONTTC (aggregate) statistics					
	TXBLOCKS	TXFRAGS	RXBLOCKS	RXFRAGS	LOSTFRAGS	BADGEMHDRS
G-1427G-A ¹	✓	✓	✓	✓	✓	—

Notes:

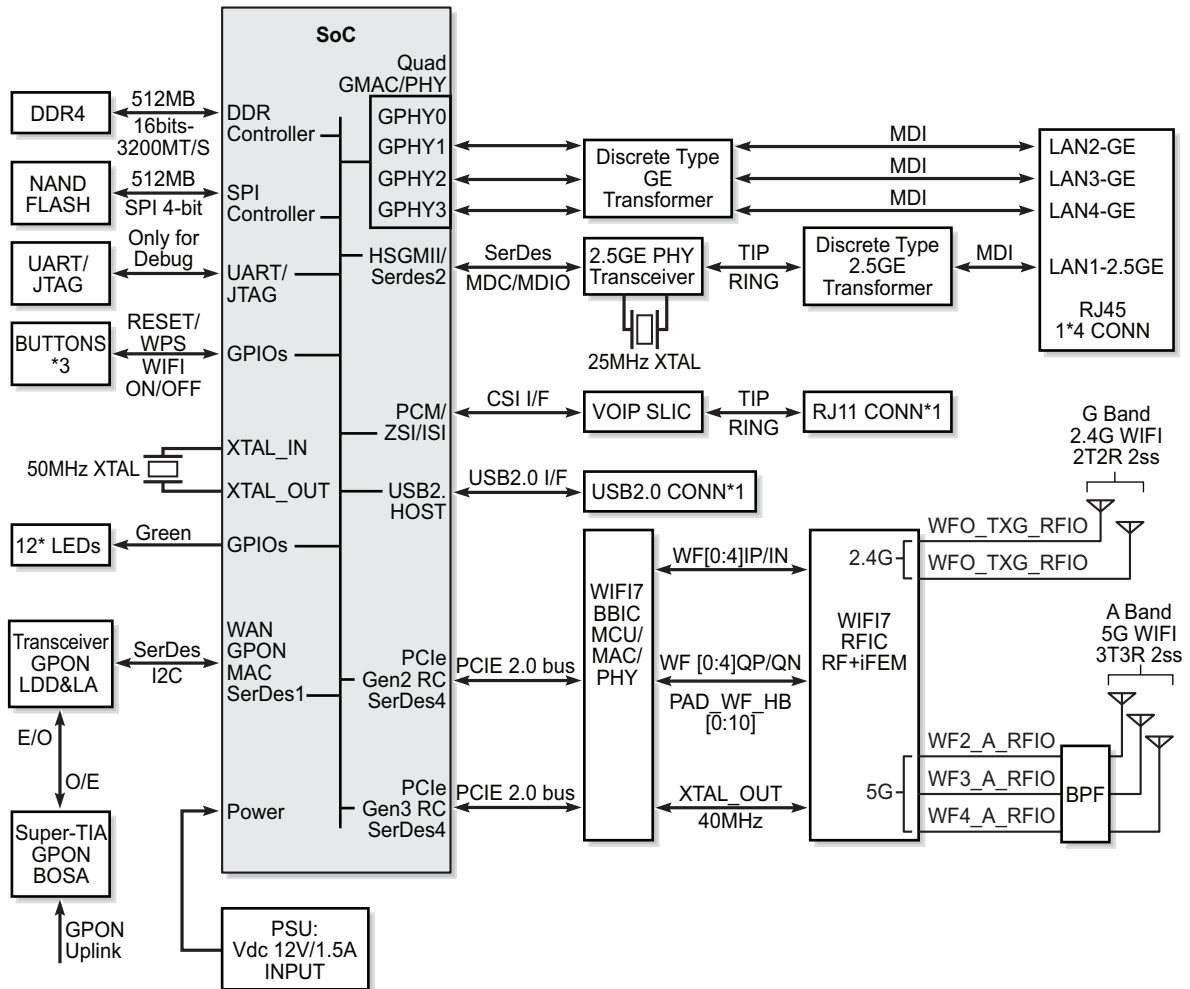
1. A 5 second polling window limitation exists on the ONT, therefore the margin of error for each 15-min window is 5 seconds.

2.10 G-1427G-A functional blocks

G-1427G-A indoor ONTs are single-residence ONTs that support Wireless (Wi-Fi) service. Wi-Fi service on these ONTs is compliant with the IEEE 802.11 standard and enabled or disabled using a WIFI button. In addition to the Wi-Fi service, these ONTs transmit Ethernet packets to four RJ-45 Ethernet ports and voice traffic to one RJ-11 POTS port. These ONTs also feature fiber optic, and power connectors.

The following figure shows the functional blocks for G-1427G-A indoor ONT.

Figure 2-5 G-1427G-A ONT functional block



40579

2.11 G-1427G-A standards compliance

G-1427G-A indoor ONTs are compliant with the following standards:

- CE marking for European standards for health, safety, and environmental protection
- ETSI EN 300 328 V2.2.2 wide band data transmission systems; Data transmission equipment operating in the 2.4 GHz band;
- ETSI EN 301 893 V2.2.1 5 GHz WAS/RLAN
- G.984 support GPON interface (framing)
- G.984.2 (Amd1, class B+) for GPON
- G.984.3 support for activation and password functions

- G.984.3 support for AES with operator enable/disable on per port-ID level
- G.984.3 support for dynamic bandwidth reporting
- G.984.3 support for FEC in both upstream and downstream directions
- G.984.3 support for multicast using a single GEM port-ID for all video traffic
- G.984.4 and G.983.2 support for ONT management and provisioning
- IEEE 802.1p for traffic prioritization
- IEEE 802.1q for VLANs
- IEEE 802.3 (2012)
- IEEE 802.11 ax/ac/b/g/n for Wi-Fi
- ITU-T G.711 A-law, G.711 μ -law, and G.729A and G.729B, G.723.1
- SIP RFC 3261

2.11.1 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the G-1427G-A ONTs are in compliance with the essential requirements and other relevant provisions of Directive 2009/125/EC together with Commission Regulation (EC) No 1275/2008 and Commission Regulation (EC) No 801/2013.

The G-1427G-A ONTS qualify as equipment with high network availability (HiNA) functionality. Since the main purpose of G-1427G-A ONTs is to provide network functionality with HiNA 7 days /24 hours, the modes Off/Standby, Power Management, and Networked Standby are inappropriate.

For information about the type and number of network ports, see [2.5 “G-1427G-A interfaces and interface capacity” \(p. 32\)](#) in this chapter.

For information about power consumption, see [2.7 “G-1427G-A detailed specifications” \(p. 36\)](#) in this chapter.

2.11.2 FCC statement

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

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

2.11.3 FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and consider removing the no-collocation statement.

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

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



CAUTION

Service Disruption

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

2.12 G-1427G-A special considerations

G-1427G-A is a package S ONT.

2.12.1 WiFi service

G-1427G-A indoor ONTs feature WiFi service as well as voice and data services. WiFi is a wireless networking technology that uses radio waves to provide wireless HSI and network connections. This ONT complies with the IEEE 802.11 standards, which the Wi-Fi Alliance defines as the basis for Wi-Fi technology.

Wi-Fi physical features

G-1427G-A indoor ONTs have the following physical features that assist in providing WiFi service:

- 1 WiFi button for enabling and disabling WiFi service
- 1 WiFi Protected Setup (WPS) push button for adding WPS-enabled wireless devices
- 5 internal antennas: 2 for 2.4G and 3 for 5G

WiFi standards and certifications

The WiFi service on G-1427G-A indoor ONTs supports the following IEEE standards and Wi-Fi Alliance certifications:

- Wi-Fi CERTIFIED 7™
- Wi-Fi CERTIFIED™ a, b, g, n, ac, ax, be
- WPA2™, WPA3™

- Wi-Fi Agile Multiband™
- WMM®, WMM®-Power Save
- Wi-Fi Protected Setup™
- EasyMesh R6

Figure 2-6, “Sample laser product safety label on the ONT equipment” (p. 43) shows a sample safety label located on the bottom of the G-1427G-A.

Figure 2-6 Sample laser product safety label on the ONT equipment



WiFi GUI features

G-1427G-A indoor ONTs have HTML-based WiFi configuration GUIs.

2.12.2 G-1427G-A ONT considerations and limitations

The following table lists the considerations and limitations for Package S G-1427G-A ONTs.

Table 2-18 G-1427G-A ONT considerations and limitations

Considerations and limitations
Call History Data collection (ONTCALLHST) is supported, except for the following parameters: RTP packets (discarded), far-end RTCP and RTCP-XR participation, RTCP average and peak round trip delay, MOS, average jitter, number of jitter-buffer over-runs and under runs.
Some voice features are configurable on a per ONT basis, including Call Waiting, Call Hold, 3-Way Calling, and Call Transfer.
The maximum value of the ringing AC voltage is 60Vrms, and the ring DC offset voltage is suggested to be 0V.

Table 2-18 G-1427G-A ONT considerations and limitations (continued)

Considerations and limitations
The following voice features/GSIP parameters are configurable on a per-Client/per-ONT basis (not per-Subscriber): • Enable Caller ID and Enable Caller Name ID • Digitmap and the associated Interdigit and Critical timers and Enter key parameters • Warmline timer is enabled per subscriber, but the warmline timer value is configured per ONT and must have a lower value than the permanent time • Miscellaneous timers: Permanent, Timed-release, Reanswer, Error-tone, and CW-alert timers • Features/ functions: Message waiting mode, WMWI refresh interval, DTMF volume level • Service Codes for the following features: CW, Call Hold and Warmline

3 Install or replace a G-1427G-A ONT

3.1 Overview

3.1.1 Purpose

This chapter provides the steps to:

- Install a G-1427G-A ONT
- Replace a G-1427G-A ONT

3.1.2 Contents

3.1 Overview	47
3.2 Prerequisites	47
3.3 Recommended tools	47
3.4 Safety information	48
3.5 Desktop mounting of G-1427G-A	49
3.6 Wall mount an G-1427G-A indoor ONT	49
3.7 Replace a G-1427G-A ONT	55
3.8 Replace a G-1427G-A indoor ONT	59

3.2 Prerequisites

Ensure to check following pre-requisites:

- Make sure to use the qualified PSU for this ONT G-1427G-A.

3.3 Recommended tools

You need the following tools:

- #2 Phillips screwdriver
- 1/4 in. (6 mm) flat blade screwdriver
- Wire strippers
- Fiber optic splicing tools
- RJ-45 cable plug crimp tool
- Voltmeter or multimeter
- Optical power meter
- Drill and drill bits
- Mounting brackets provided with the ONT ordering kit, if installing on a rack

3.4 Safety information

Read the following safety information before installing the unit.



DANGER

Hazard

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

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

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



WARNING

Equipment Damage

This equipment is ESD sensitive. Proper ESD protections should be used when connecting or removing the fiber optic cable to or from the ONT.



CAUTION

Service Disruption

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



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

The 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 ONT must be installed by qualified service personnel.

Indoor ONTs must be installed with cables that are suitably rated and listed for indoor use.

In order to assure personnel safety, EMC and protection of installations against damage, this product must be reliably grounded during use.

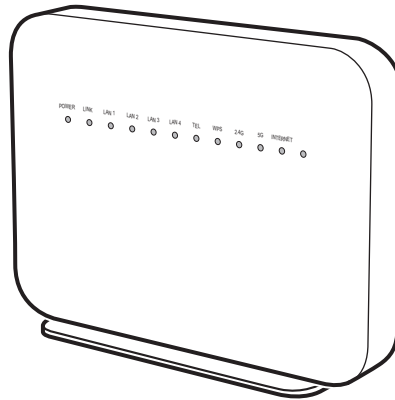
All devices in the network box are connected to the ground bar through the ground cable (the diameter of the cable should be no less than 6 mm²)

The ground bar is equipotential connected with the network box through the metal structure. When the PE cable of the AC power cable is not grounded, the network box must pass through External ground cables (PGND cables) which are grounded. The external grounding cable (PGND cable) of the network box must be connected to the external grounding device, this wire diameter should not be less than 16 mm².

3.5 Desktop mounting of G-1427G-A

Place the ONT on the flat surface, such as a desktop as shown in [Figure 3-1, “G-1427G-A on a desk”](#) (p. 48).

Figure 3-1 G-1427G-A on a desk



40575

i **Note:** The G-1427G-A cannot be stacked with another ONT or with other equipment.

The ONT mounting requirements are:

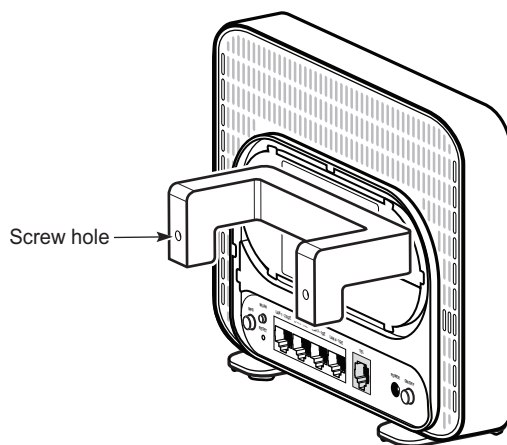
- Allow a minimum 100 mm clearance above the top cover.
- Allow a minimum 50 mm clearance from the side.
- Do not place any heat source directly above the top cover or below the bottom cover.

3.6 Wall mount an G-1427G-A indoor ONT

This chapter provides the steps to mount an G-1427G-A indoor ONT on a wall using a wall mount bracket (3FE49555AA or 3TN01607AA). The G-1427G-A indoor ONT is shipped without the wall mount bracket. The wall mount bracket (3FE49555AA or 3TN01607AA) must be ordered separately.

i **Note:** The recommended bracket installation height must not be higher than 2m.

Figure 3-2 G-1427G-A ONT in wall mounting bracket



40580

3.6.1 Recommended tools

See section 3.3 “Recommended tools” (p. 47) for the recommended tools.

3.6.2 Procedure

Use this procedure to mount an G-1427G-A ONT on a wall. Two installation options are available:

- Option 1—facing the room for the LEDs to be visible
- Option 2—facing the wall for the connectors and buttons to be visible

1

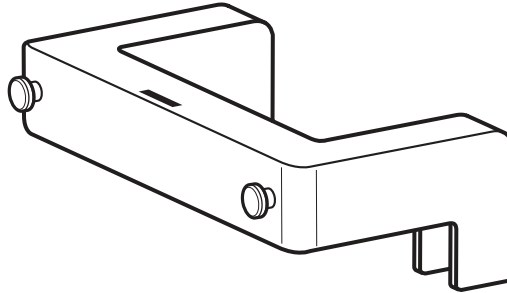
Place the indoor ONT unit:

- a. Facing the room, go to [Step 2](#). See [Figure 3-7, “ONT in wall mount bracket—facing the room” \(p. 54\)](#).
- b. Facing the wall, go to [Step 3](#). See [Figure 3-6, “ONT to wall mount connection” \(p. 53\)](#).

2

Mount the ONT on a wall facing the room using the wall mount bracket (3FE49555AA or 3TN01607AA), as shown in [Figure 3-3, “G-1427G-A wall mount bracket” \(p. 51\)](#).

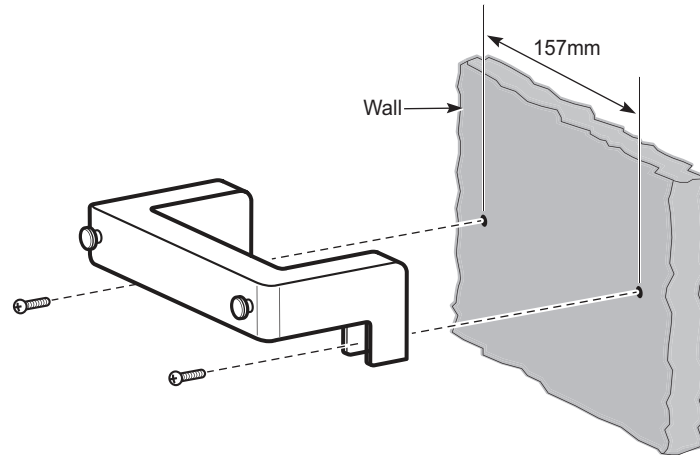
Figure 3-3 G-1427G-A wall mount bracket



40581

- a. Determine the location of the two anchor holes for the wall mount bracket. The bracket can be used as a template for marking and drilling the holes.
It is recommended to use a level to ensure that the ONT unit is installed properly.
- b. Drill two holes 35 mm (1.37 in.) depth into the wall and with the centers spaced 100 mm (3.9 in.).
- c. Insert the two mounting screws and optional anchors into the holes, leaving a 2 mm (0.078 in.) gap between the screw head and the wall.
- d. At this point, perform a test to ensure that the wall mount bracket fits securely over the screw heads. Mount the bracket flush to the wall so that it does not warp or twist.
- e. Remove the wall mount bracket from the wall.
- f. Route the power cord through the slot in the wall mount bracket. The ferrite bead on the power cord should remain on the underside of the wall mount bracket. See [Figure 3-4, "Wall mount bracket power cord placement"](#) (p. 52).

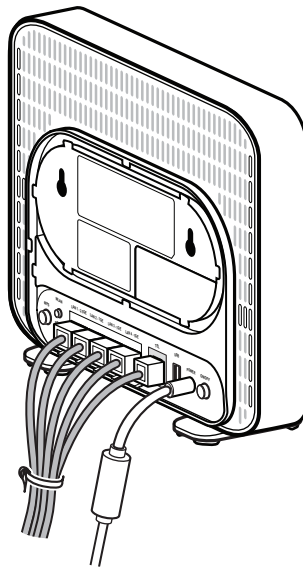
Figure 3-4 Wall mount bracket power cord placement



40582

Connect the power cord to the G-1427G-A ONT. See [Figure 3-5, “Power cord to ONT connection” \(p. 52\)](#).

Figure 3-5 Power cord to ONT connection

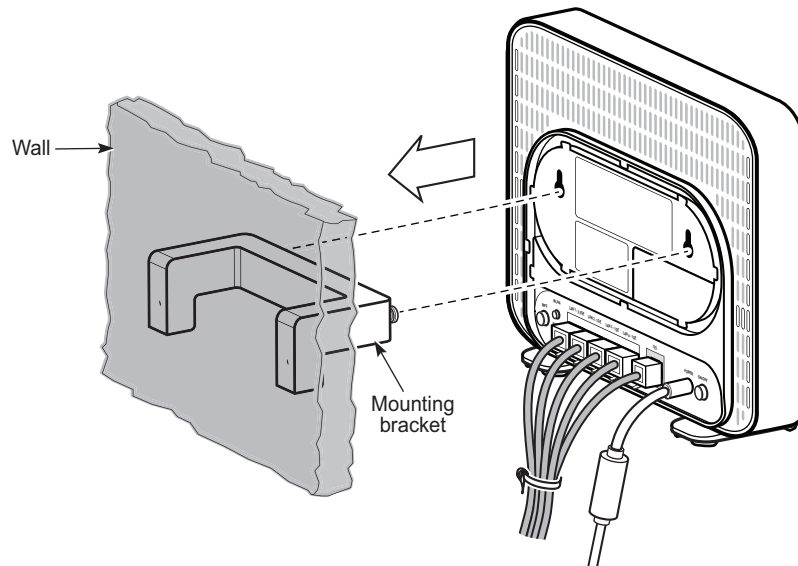


40583

g. Install the ONT into the wall mount bracket by lifting the unit above the bracket and sliding it

downward onto the bottom ledge of the bracket. See [Figure 3-6, “ONT to wall mount connection”](#) (p. 52).

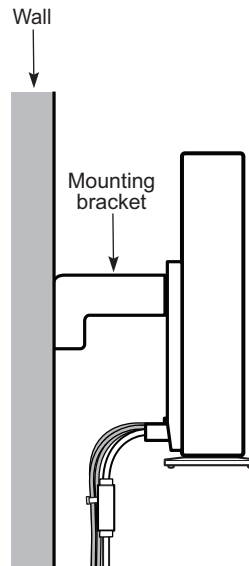
Figure 3-6 ONT to wall mount connection



40584

- h. Seat the ONT into the wall mount bracket by engaging the hooks on the base of the unit with those on the bracket; see [Figure 3-7, “ONT in wall mount bracket—facing the room”](#) (p. 54). Engaging the hooks ensures that the ONT stays in place while the unit is mounted onto the wall.
- i. Connect the cables.
- j. Hang the unit onto the wall. [Figure 3-7, “ONT in wall mount bracket—facing the room”](#) (p. 54) shows the cables routed through the wall mount bracket and the ONT facing the room.

Figure 3-7 ONT in wall mount bracket—facing the room



40485

3

Mount the ONT facing the wall using the wall mount bracket

- a. Determine the location of the two anchor holes for the wall mount bracket. The bracket can be used as a template for marking and drilling the holes.
It is recommended to use a level to ensure that the ONT unit is installed properly.
- b. Drill two holes 35 mm (1.37 in.) depth into the wall and with the centers spaced 157 mm (6.2 in.).
- c. Insert the two mounting screws and optional anchors into the holes, leaving a 2 mm (0.078 in.) gap between the screw head and the wall.
- d. At this point, perform a test to ensure that the wall mount bracket fits securely over the screw heads. Mount the bracket flush to the wall so that it does not warp or twist.
- e. Remove the wall mount bracket from the wall.
- f. On a flat surface such as a desk, install the ONT into the wall mount bracket by lifting the unit above the bracket and sliding it downward onto the bottom ledge of the bracket.
- g. Seat the ONT into the wall mount bracket by engaging the hooks on the base of the unit with those on the bracket. Engaging the hooks ensures that the ONT stays in place while the unit is mounted onto the wall.
- h. Mount the unit onto the wall.
- i. Connect the cables. See [Chapter 3, "Install or replace a G-1427G-A ONT"](#).

Figure 3-5, “Power cord to ONT connection” (p. 52) shows the mounted unit facing the wall with the cables (including the fiber) installed.

END OF STEPS

3.7 Replace a G-1427G-A ONT

1

Deactivate the ONT services at the OLT prior to deactivating the ONT.

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

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

Example:

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

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

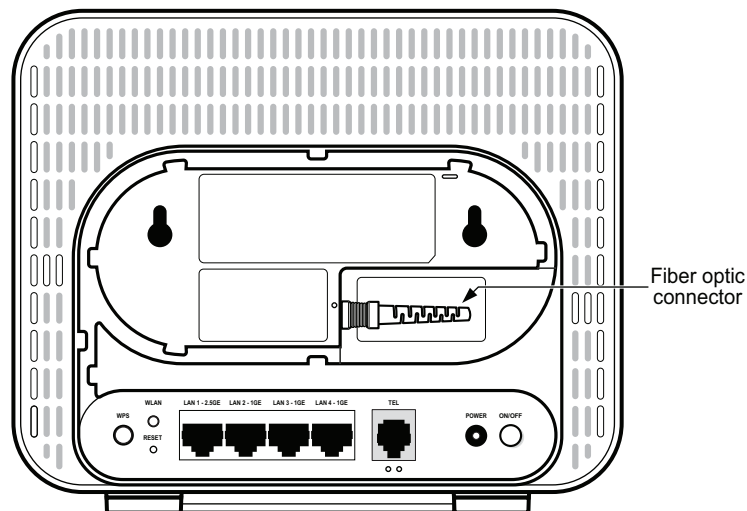
Example:

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

2

Disconnect the Ethernet, power, ground, RS485/RS232 and DI/DO cables from the ONT; see the following figure for the location of the connectors.

Figure 3-8 G-1427G-A ONT connections



40577

3



DANGER

Hazard

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



WARNING

Equipment Damage

Be careful to maintain a bend radius of no less than 1.5 inches (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.

Disconnect the SC/APC fiber optic cable to the SC/APC connector.

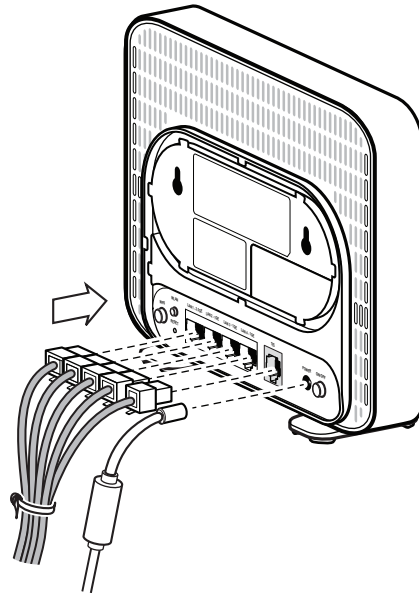
4

Replace the ONT with a new unit. You can install the new ONT on a flat surface, in a rack, or on a DIN rail.

5

Connect the Ethernet cables to the ONT; see [Figure 3-8, “G-1427G-A ONT connections” \(p. 55\)](#) for the location of the Ethernet ports.

Figure 3-9 Connecting the cables to the ONT



40586

6



DANGER

Hazard

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

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

7



DANGER

Hazard

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



WARNING

Equipment Damage

Be careful to maintain a bend radius of no less than 1.5 inches (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.

Connect the SC/APC fiber optic cable to the SC/APC connector.



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.

8



CAUTION

Service Disruption

Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 100 V to 240 V ac.

Install the power supply according to manufacturer specifications and connect the power cable to the ONT. The G-1427G-A supports DC power connections.

9

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

Alphanumeric mode (Length(1..10)): limit to character and number in He mode(Length(1..20)).



Note: For Hex mode, the prefix value is 0x.



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 OLT using TL1 or a network manager. If the old SLID is used, no changes need to be made at the OLT; see the operations and maintenance documentation for the OLT for more details.

10

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

Activate and test the services; see the **Nokia ONT Hardware and Cabling Installation Guide**.

11

If necessary, reset the ONT.

- a. Locate the Reset button on the ONT as shown in [Figure 3-8, "G-1427G-A ONT connections" \(p. 55\)](#).

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

END OF STEPS

3.8 Replace a G-1427G-A indoor ONT

1

Deactivate the ONT services at the P-OLT.

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

- a. Use the RTRV-ONT command to verify the ONT status and 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;
```

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

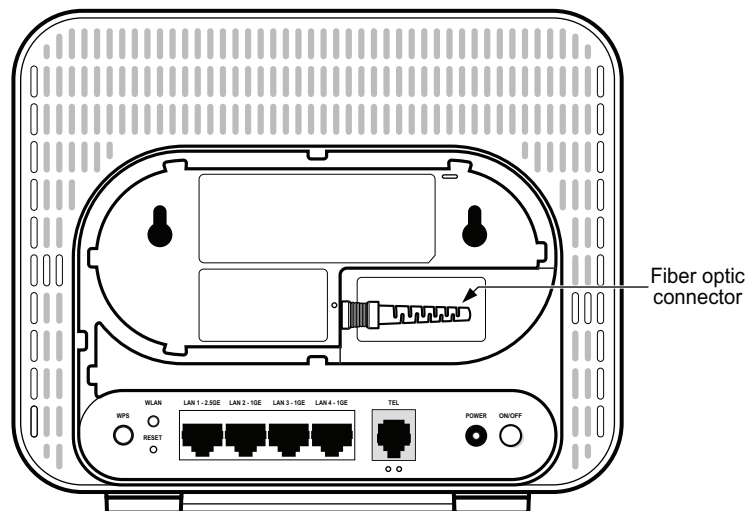
Example:

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

2

If used, disable the Wi-Fi service by pressing the WLAN button. The following figure shows the location of the WLAN button.

Figure 3-10 G-1427G-A indoor ONT connections



40577

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 3-10, "G-1427G-A indoor ONT connections" \(p. 59\)](#) for the connector locations on the G-1427G-A indoor ONT.

5



DANGER

Hazard

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

Disconnect the fiber optic cables.

- a. Unplug the fiber optic cable with SC/APC connector from the bottom of the ONT.
- b. Attach a fiber dust cover to the end of the SC/APC connector.

6

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

7

Connect the Ethernet cables directly to the RJ-45 ports; see [Figure 3-10, "G-1427G-A indoor ONT connections" \(p. 59\)](#) for the location of the RJ-45 ports.

8

Connect the POTS cable directly to the RJ-11 port as per local practices; see [Figure 3-10, "G-1427G-A indoor ONT connections" \(p. 59\)](#) for the location of the RJ-11 ports.

9



DANGER

Hazard

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

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

10



DANGER

Hazard

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



WARNING

Equipment Damage

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

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



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

11

Connect the power cable to the power connector.

12

Power up the unit by using the power switch.

13

If used, enable the Wi-Fi service by pressing the WLAN button; see [Figure 3-10, “G-1427G-A indoor ONT connections” \(p. 59\)](#) for the location of the WLAN button.

14

If used, configure the SLID; see the **Nokia 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.

15

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

16

Activate and test the services; see the **Nokia ONT Hardware and Cabling Installation Guide**.

17

If necessary, reset the ONT.

- a. Locate the Reset button on a G-1427G-A indoor ONT as shown in [Figure 3-10, “G-1427G-A indoor ONT connections” \(p. 59\)](#).
- b. Insert the end of a straightened paper clip or other narrow object into the hole in the Reset button to reset the ONT.

END OF STEPS

4 Configure a G-1427G-A indoor ONT

4.1 Overview

4.1.1 Purpose

This chapter describes the WebGUI configuration procedures.

4.1.2 Contents

4.1 Overview	63
GUI overview	66
4.2 General configuration	66
4.3 HGU mode GUI configuration	66
4.4 New password rules	66
4.5 WAN services overview	66
4.6 Logging in to the web-based GUI	70
4.7 Viewing overview information	72
4.8 G-1427G-A WebGUI Menu	74
WAN Configuration	76
4.9 Overview	76
4.10 Configuring WAN Services	76
4.11 Viewing WAN Statistics	86
4.12 Configuring TR-069	89
4.13 Configuring TR-369	90
4.14 Configuring GRE tunnel	92
4.15 Configuring Static routing	93
4.16 Viewing Optical Module Status	95
4.17 Configuring QoS	96
4.18 Configuring Upstream (US) Classifier	99
LAN Configuration	106
4.19 Overview	106
4.20 Configuring DHCP IPv4	106

4.21 Configuring DHCP IPv6	108
4.22 Configuring DNS	110
4.23 Viewing LAN Statistics	113
WiFi Configuration	115
4.24 Overview	115
4.25 Configuring WiFi Network	115
4.26 Configuring the WiFi Password	120
4.27 Configuring IoT Network	121
4.28 Configuring Guest Network	122
4.29 Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points	124
4.30 Optimizing WiFi Network	128
4.31 Configuring Wireless 2.4 GHz	128
4.32 Configuring Wireless 5 GHz	131
4.33 Configuring Wireless Schedules	133
4.34 Viewing WiFi Statistics	134
Devices	137
4.35 Overview	137
4.36 Viewing Device Information	137
Voice Configuration	140
4.37 Overview	140
4.38 Configuring Voice Settings	140
4.39 Viewing Voice Status	142
Security Configuration	144
4.40 Overview	144
4.41 Configuring the Firewall	144
4.42 Configuring the MAC Filter	145
4.43 Configuring the IP Filter	147
4.44 Configuring the URL Filter	149
4.45 Configuring Family Profiles	151
4.46 Configuring DMZ and ALG	157

4.47 Configuring Access Control	159
Advanced Settings	163
4.48 Overview	163
4.49 Configuring Port Forwarding	163
4.50 Configuring Port Triggering	164
4.51 Configuring DDNS	165
4.52 Configuring NTP	166
4.53 Configuring UPNP and DLNA	168
Maintenance	169
4.54 Overview	169
4.55 Configuring the Password	169
4.56 Backing Up the Configuration	171
4.57 Restoring the Configuration	172
4.58 Upgrading Firmware	173
4.59 Configuring LOID	175
4.60 Configuring SLID	176
4.61 Diagnosing WAN Connections	178
4.62 Viewing Log Files	180
4.63 Generating a delta configuration file	182
Troubleshooting	185
4.64 Troubleshooting counters	185
4.65 Speed Test	187

GUI overview

This section provides an overview of the G-1427G-A WebGUI.

4.2 General configuration

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

4.3 HGU mode GUI configuration

Use the procedures below to use the web-based GUI for the G-1427G-A in HGU mode. This mode is preset at delivery.

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

4.4 New password rules

For security reasons, operators can mandate a change of password for the WiFi network and user accounts at the first login. Operators can also allow users to change passwords with or without password rules.

A pop-up message is displayed for users to change password for the WiFi network and user accounts at the first login.

4.5 WAN services overview

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

The following WAN services can be configured.

4.5.1 Forwarding model

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

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

4.5.2 VLAN binding service

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

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

4.5.3 Tunnel service

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

4.5.4 Transparent service (Special case of Tunnel mode)

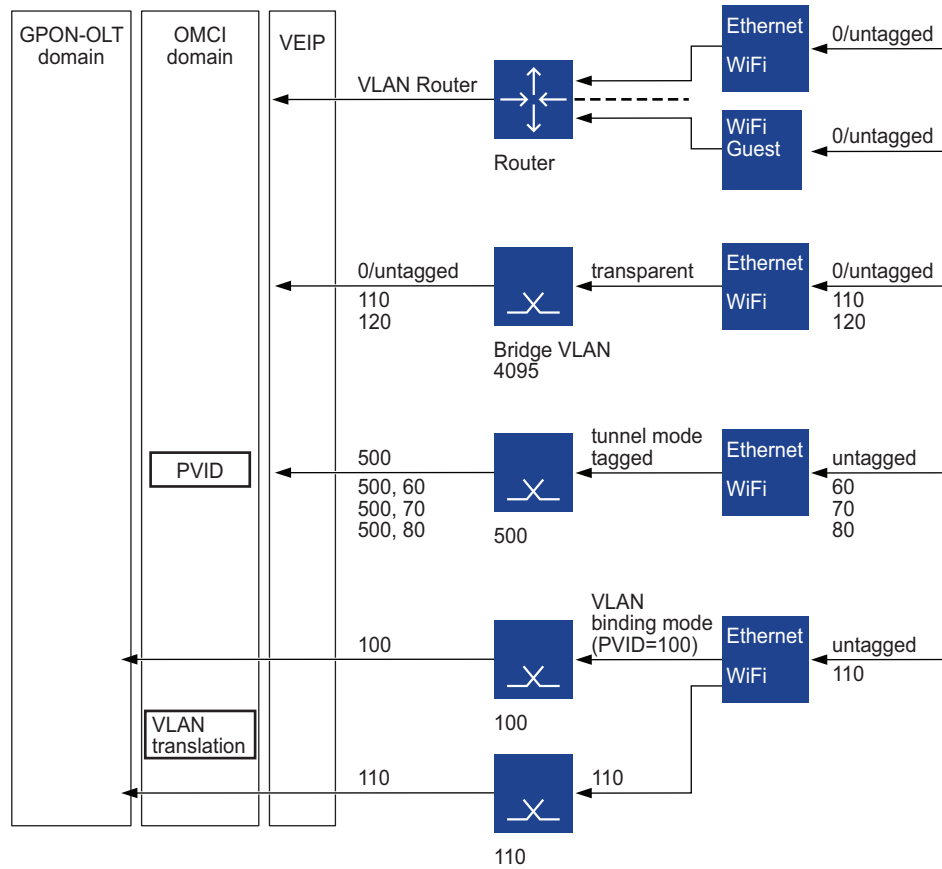
This service is an extension of the bridge tunnel service, where the service VLAN is considered as NULL or empty. This model is applicable only for xPON RGs. The traffic from the LAN side is transmitted on the associated WAN side without adding/stripping a service VLAN. In this service, a PVID is configured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

4.5.5 Routing service

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

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

Figure 4-1 Common forwarding model



38446

4.5.6 Supported combinations

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

Table 4-1 Supported combinations of OMCI and ACS/WebGUI

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

Table 4-1 Supported combinations of OMCI and ACS/WebGUI (continued)

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

Table 4-1 Supported combinations of OMCI and ACS/WebGUI (continued)

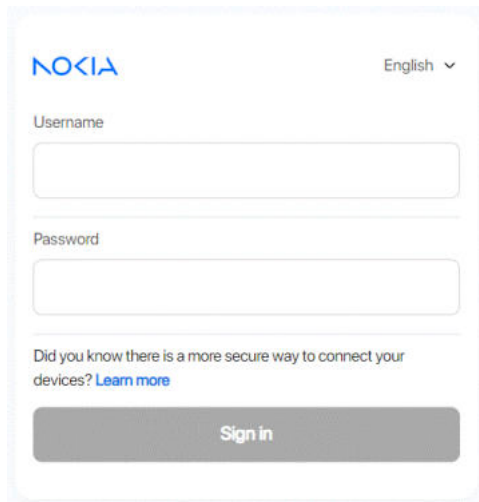
Service Type	Operation	Untagged traffic at LAN	Tagged traffic at LAN
Bridge (VLAN binding, Tunnel)	Set WAN P-bit	ACS/WebGUI	ACS/WebGUI (take recent P-bit)
	Set WAN-VID	ACS/WebGUI	ACS/WebGUI
	Remark P-bit per VLAN (single P-bit)	Not supported (OMCI) (no PVID configured)	Not supported (OMCI)
	Remap P-bit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

4.6 Logging in to the web-based GUI

1

Open a web browser and enter the IP address of the ONT in the address bar.
The *Login* page displays.

Figure 4-2 Login page



The default gateway IP address must be same as the one printed on the device label. You can connect to this IP address using your web browser after connecting your PC to one of Ethernet ports of the ONT or via WiFi connection. The static IP address of your PC must be in the same default gateway subnet as the ONT. You can also access the login page via "https://www.webgui.nokiawifi.com/" and "http://www.webgui.nokiawifi.com/".

2



CAUTION

Service Disruption

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

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

Enter your username and password in the *Login* page, as shown in [Figure 4-2, “Login page” \(p. 71\)](#).

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

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

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

3

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



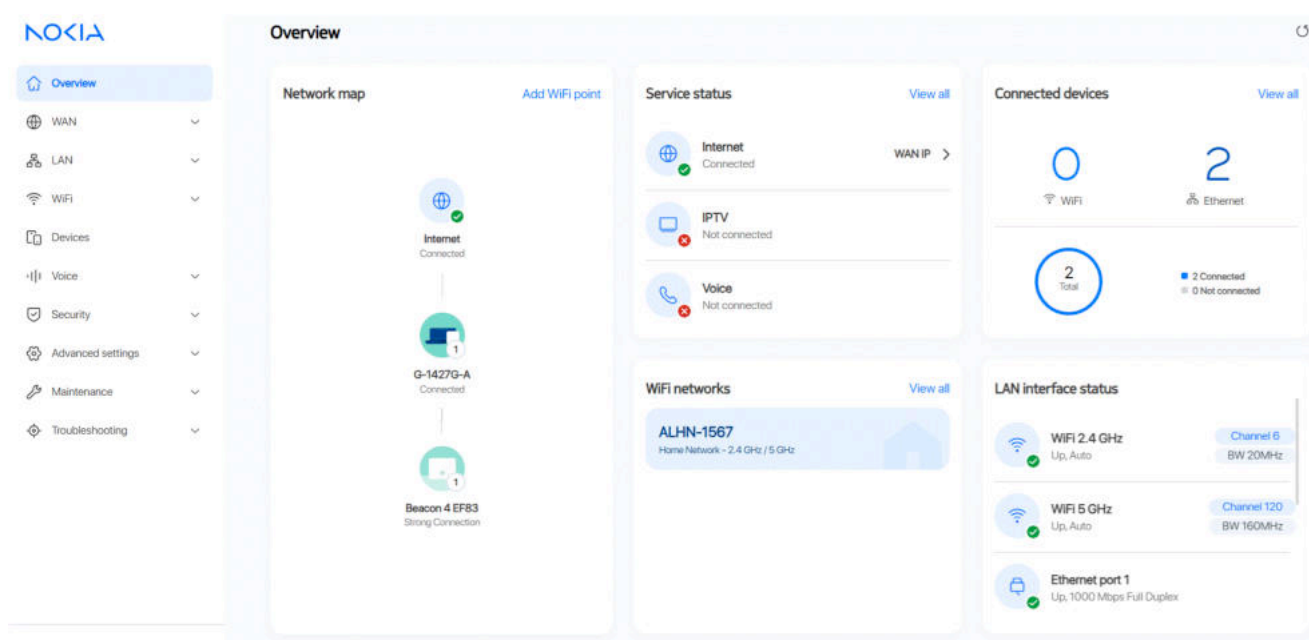
Note: To help protect the security of your Internet connection, the application displays a pop-up reminder to change both the WiFi password and the ONT password. To increase password security, use a minimum of 10 characters, consisting of a mix of numbers and upper and lower case letters.

END OF STEPS

4.7 Viewing overview information

1

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



END OF STEPS

4.7.1 Network Map

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

Root device

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

Extender device

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

4.7.2 Service Status

Displays the active status of the triple-play services.

Internet service

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

IPTV service

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

4.7.3 WiFi Networks

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

4.7.4 Connected Clients

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

4.7.5 LAN Interface Status

Displays information about all the LAN ports of the device.

WiFi 2.4GHz

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

WiFi 5GHz

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

Ethernet Port

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

4.8 G-1427G-A WebGUI Menu

The following table lists the main menu and sub-menu options in the G-1427G-A WebGUI:

Table 4-2 G-1427G-A WebGUI Menu

Main Menu	Sub-menu	Procedure Reference
Overview	-	4.7 "Viewing overview information" (p. 72)
WAN	WAN services	4.10 "Configuring WAN Services" (p. 76)
WAN	WAN statistics	4.11 "Viewing WAN Statistics" (p. 86)
WAN	TR-069	4.12 "Configuring TR-069" (p. 89)
WAN	TR-369	4.13 "Configuring TR-369" (p. 90)
WAN	IP routing	4.15 "Configuring Static routing" (p. 93)
WAN	Qos config	4.17 "Configuring QoS" (p. 96)
WAN	Upstream (US) Classifier	4.18 "Configuring Upstream (US) Classifier " (p. 99)
WAN	GRE tunnel	4.14 "Configuring GRE tunnel" (p. 92)
LAN	DHCP IPv4	4.20 " Configuring DHCP IPv4" (p. 106)
LAN	DHCP IPv6	4.21 " Configuring DHCP IPv6" (p. 108)
LAN	DNS	4.22 "Configuring DNS" (p. 110)
LAN	LAN statistics	4.23 "Viewing LAN Statistics" (p. 113)
WiFi	WiFi networks	4.25 "Configuring WiFi Network" (p. 115)
WiFi	IoT network	4.27 "Configuring IoT Network" (p. 121)
WiFi	Guest network	4.28 "Configuring Guest Network" (p. 122)
WiFi	Network map	4.29 "Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points" (p. 124)
WiFi	Optimizing Network	4.30 "Optimizing WiFi Network" (p. 128)
WiFi	Advanced settings	4.31 "Configuring Wireless 2.4 GHz" (p. 128) 4.32 "Configuring Wireless 5 GHz" (p. 131)
WiFi	Wireless schedule	4.33 "Configuring Wireless Schedules" (p. 133)
WiFi	WiFi statistics	4.34 "Viewing WiFi Statistics" (p. 134)
Devices	-	4.36 "Viewing Device Information" (p. 137)
Voice	Voice setting	4.38 "Configuring Voice Settings" (p. 140)
Voice	Voice status	4.39 "Viewing Voice Status" (p. 142)
Security	Firewall	4.41 "Configuring the Firewall" (p. 144)

Table 4-2 G-1427G-A WebGUI Menu (continued)

Main Menu	Sub-menu	Procedure Reference
Security	MAC filter	4.42 "Configuring the MAC Filter" (p. 145)
Security	IP filter	4.43 "Configuring the IP Filter" (p. 147)
Security	Family profiles	4.45 "Configuring Family Profiles" (p. 151)
Security	DMZ and ALG	4.46 "Configuring DMZ and ALG" (p. 157)
Security	Access control	4.47 "Configuring Access Control" (p. 159)
Advanced settings	Port forwarding	4.49 "Configuring Port Forwarding" (p. 163)
Advanced settings	Port triggering	4.50 "Configuring Port Triggering" (p. 164)
Advanced settings	DDNS	4.51 "Configuring DDNS" (p. 165)
Advanced settings	NTP	4.52 "Configuring NTP" (p. 166)
Advanced settings	UPNP and DLNA	4.53 "Configuring UPNP and DLNA" (p. 168)
Maintenance	Change password	4.55 "Configuring the Password" (p. 169)
Maintenance	Backup and restore	4.56 "Backing Up the Configuration" (p. 171) 4.57 "Restoring the Configuration" (p. 172)
Maintenance	Firmware upgrade	4.58 "Upgrading Firmware" (p. 173)
Maintenance	Diagnostics	4.61 "Diagnosing WAN Connections" (p. 178)
Maintenance	Log	4.62 "Viewing Log Files" (p. 180)
Maintenance	Delta CFG tool	4.63 "Generating a delta configuration file" (p. 182)
Troubleshooting	Troubleshooting counters	4.64 "Troubleshooting counters" (p. 185)
Troubleshooting	Speed test	4.65 "Speed Test" (p. 187)

WAN Configuration

4.9 Overview

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

Sub-menu	Procedure
WAN services	4.10 "Configuring WAN Services" (p. 76)
WAN statistics	4.11 "Viewing WAN Statistics" (p. 86)
TR-069	4.12 "Configuring TR-069" (p. 89)
TR-369	4.13 "Configuring TR-369" (p. 90)
IP routing	4.15 "Configuring Static routing" (p. 93)
Optical module status	4.16 "Viewing Optical Module Status" (p. 95)
Qos config	4.17 "Configuring QoS" (p. 96)
GRE tunnel	4.14 "Configuring GRE tunnel" (p. 92)
US classifier	4.18 "Configuring Upstream (US) Classifier" (p. 99)

4.10 Configuring WAN Services

1

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

The device supports dual-stack functionality on the WAN side, enabling it to use both IPv4 and IPv6 simultaneously. Typically, both addresses are assigned automatically through DHCP. However, the IPv4 address can also be configured manually (static), while IPv6 continues to be assigned automatically.



Note:

If the ACS lock is enabled, impacts for all the users are as follows:

- Creation of new WAN services are blocked.
- Deletion of existing WAN services are blocked.
- No parameters can be edited.

Figure 4-3 Overview table in WAN services page

WAN / WAN services ↻ Add +

Overview				
Service Name	Connection mode	Enable/Disable status	Service	IP address
1_VOIP_TR069_INTERNET_R_VID_981	Route	Enable	VOIP, TR-069, Internet	192.168.124.22
2_INTERNET_R_VID_1001	Route	Enable	Internet	192.168.91.109
3_OTHER_R_VID_1002	Route	Enable	IPTV	192.168.92.101
4_INTERNET_R_VID_3000	Route	Enable	Internet	1.1.1.149 / 2003:1:1:1:18

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

Figure 4-4 Create New Connection page

← WAN / WAN services / **Create New Connection**

↺ Delete

Save

WAN connection list

Create New Connection

Enabled

Connection type

IPv4E

Connection mode

Route Mode

IP mode

IPv4

NAT

TR-069

VQIP

Internet

IPTV

Enable VLAN

VLAN ID

VLAN PRI

WAN IP mode

DHCP

Manual DNS

Pri DNS

Sec DNS

Figure 4-5 Create New Connection page - PPPoE Configuration

← WAN / WAN services / **Create New Connection**
↻
Delete
Save

WAN connection list

Create New Connection

Enabled
☐

Connection type

PPPoE

Connection mode

Route Mode

IP mode

IPv4

NAT
☒

TR-069
☐

VOIP
☐

Internet
☐

IPTV
☐

Enable VLAN
☒

VLAN ID

VLAN PRI

WAN IP mode

PPPoE

Connection trigger

AlwaysOn

Username

Password

Keep alive time

(5-60 seconds)

Keep alive retry

(1-10 times)

Echo value

Manual DNS
☐

DSL PPAUC

Figure 4-6 VLAN mode - VLAN Binding

← WAN / WAN services / **Create New Connection**
↺ Delete Save

WAN connection list

Create New Connection

Enabled

Connection mode

Bridge Mode

IPTV

VLAN mode

VLAN binding

VLAN ID

VLAN PRI

LAN port binding

LAN 1

PVID

LAN 2

PVID

LAN 3

PVID

LAN 4

PVID

SSID port binding

SSID 1

PVID

SSID 2

PVID

SSID 3

PVID

SSID 4

PVID

SSID 5

PVID

SSID 6

PVID

SSID 7

PVID

Figure 4-7 Bridge mode - Transparent

The screenshot shows the 'Create New Connection' page in the WAN configuration interface. The page is titled 'WAN / WAN services / Create New Connection' and includes a 'Delete' button and a 'Save' button. The configuration is set to 'Bridge Mode' and 'Transparent' VLAN mode. The 'WAN connection list' shows 'Enabled'. The 'Connection mode' is set to 'Bridge Mode'. The 'IPTV' toggle is off. The 'VLAN mode' is set to 'Transparent'. The 'LAN port binding' section shows four LAN ports (LAN 1, LAN 2, LAN 3, LAN 4) with toggle switches. The 'SSID port binding' section shows eight SSID ports (SSID 1 through SSID 8) with toggle switches.

← WAN / WAN services / **Create New Connection** ↺ Delete Save

WAN connection list Create New Connection

Enabled

Connection mode Bridge Mode

IPTV

VLAN mode Transparent

LAN port binding

LAN 1

LAN 2

LAN 3

LAN 4

SSID port binding

SSID 1

SSID 2

SSID 3

SSID 4

SSID 5

SSID 6

SSID 7

SSID 8

Figure 4-8 Bridge mode - Tunnel

← WAN / WAN services / Create New Connection

↺ Delete

Save

WAN connection list

Create New Connection

Enabled

Connection mode

Bridge Mode

IPTV

VLAN mode

Tunnel

VLAN ID

VLAN PRI

LAN port binding

LAN 1

LAN 2

LAN 3

LAN 4

SSID port binding

SSID 1

SSID 2

SSID 3

SSID 4

SSID 5

SSID 6

SSID 7

SSID 8

3

Configure the following parameters:

Table 4-3 WAN services parameters

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

Table 4-3 WAN services parameters (continued)

Field	Description
Enabled	Select the toggle button to enable the WAN connection.
Connection type	Select a connection type from the list: • IPoE • PPPoE
Connection mode	Select the connection mode of the WAN connection from the list: • Route Mode • Bridge Mode
IP mode	This field is applicable only if the connection mode is Route Mode . Select an IP mode from the list: • IPv4 • IPv4 & IPv6 • IPv6 When the IP mode IPv4 & IPv6 or IPv6 is selected, you need to configure Address method , Enabled prefix delegation and Prefix type .
NAT	Select the toggle button to enable NAT. This option is applicable only if the connection mode is Route Mode .
TR-069	Select the toggle button to enable TR-069. This option is applicable only if the connection mode is Route Mode .
VOIP	Select the toggle button to enable voice services. This option is applicable only if the connection mode is Route Mode .
Internet	Select the toggle button to enable Internet. This option is applicable only if the connection mode is Route Mode .
IPTV	Select the toggle button to enable IPTV.
Enable VLAN	Select the toggle button to enable VLAN. This option is applicable only if the connection mode is Route Mode .
VLAN mode	Select a VLAN mode from the list: • VLAN binding • Tunnel • Transparent This option is applicable only if the connection mode is Bridge Mode .
VLAN ID	Enter the VLAN ID. Allowed values: 2 to 4094 In the bridge mode, this option is applicable only if the VLAN mode is VLAN binding and Tunnel .
VLAN PRI	Enter the VLAN PRI. VLAN priority allows to assign a priority to outbound packets containing the specified VLAN ID. Allowed values: 0 to 7 In the bridge mode, this option is applicable only if the VLAN mode is VLAN binding or Tunnel .

Table 4-3 WAN services parameters (continued)

Field	Description
LAN port binding	Select the toggle button next to the LAN to enable it. Select the toggle button next to the PVID to enable it. This option is applicable in all VLAN modes.
SSID port binding	Select the toggle button next to the SSID to enable it. Select the toggle button next to the PVID to enable it. This option is applicable in all VLAN modes.
WAN IP mode	Select an IP mode from the list: • DHCP • PPPoE This option is visible only if you select PPPoE as the connection type. • Static
Manual DNS	If the selected IP mode is IPv4 and the WAN IP mode is DHCP , enter the Domain Name Server (DNS) to be configured manually. You can also enter the Domain Name Server (DNS) to be configured manually if the selected IP mode is IPv4 and the connection type is PPPoE .
IPv4 Address	If the selected IP mode is IPv4 or IPv4&IPv6 and the WAN IP mode is Static , enter the static IPv4 address.
Netmask	If the selected IP mode is IPv4 or IPv4&IPv6 and the WAN IP mode is Static , enter the netmask.
Gateway	If the selected IP mode is IPv4 or IPv4&IPv6 and the WAN IP mode is Static , enter the gateway IP address.
Pri DNS	If the selected IP mode is IPv4 or IPv4&IPv6 and the WAN IP mode is Static , enter the primary Domain Name Server (DNS). Also, if the selected IP mode is IPv4 and the Connection type is PPPoE , enter the primary Domain Name Server (DNS).
Sec DNS	If the selected IP mode is IPv4 or IPv4&IPv6 and the WAN IP mode is Static , enter the secondary Domain Name Server (DNS). Also, if the selected IP mode is IPv4 and the Connection type is PPPoE , enter the secondary Domain Name Server (DNS).
Ter DNS	If the selected IP mode is IPv4 or IPv4&IPv6 and the WAN IP mode is Static , enter the tertiary Domain Name Server (DNS).
Connection trigger	Select the connection trigger type from the list. The default option is Always On . This option is applicable only if the WAN IP mode is PPPoE .
Username	Enter the username to log in to the configuration server. This option is applicable only if the WAN IP mode is PPPoE .
Password	Enter the password to log in to the configuration server. Allowed values are limited to numbers, letters and special characters ! # + , - . / : = @ _ . This option is applicable only if the WAN IP mode is PPPoE .

Table 4-3 WAN services parameters (continued)

Field	Description
Keep alive time	The PPPoE connection type triggers one heartbeat each, at the configured time interval to keep the session online. Allowed values: 5 to 60 seconds. This option is applicable only if the WAN IP mode is PPPoE .
Keep alive retry	Configure the number of retries to check the Keep Alive status of the PPPoE session after time-out. Allowed values: 1 to 10. This option is applicable only if the WAN IP mode is PPPoE .
Echo value	Indicates the number of times the device sends messages to the server to check if the IP address is available or not. This option is applicable only if the WAN IP mode is PPPoE .
Address method	If the selected IP mode is IPv6 or IPv4&IPv6 , select the address method from the list: • AutoConfigured • DHCPv6 • DHCPv6_PD • DHCPv6_NA • Static
Enable prefix delegation	If the selected address method is AutoConfigured , select the toggle button to enable inclusion of the Identity Association (IA) for Prefix Delegation option in Solicit messages.
Prefix type	Displays mechanism through which the prefix was assigned or most recently updated.
IP Address (v6)	If the selected address method is Static , enter the IPv6 address.
Gateway (v6)	If the selected address method is Static , enter the gateway IPv6 address.
IPv6 address prefix	If the selected address method is Static , enter the IPv6 address prefix.
Pri DNS (v6)	If the selected address method is Static , enter the primary DNS IP address.
Sec DNS (v6)	If the selected address method is Static , enter the secondary DNS IP address.
DHCP option 50 persistent	Select the toggle button to enable DHCP Option 50 persistent.
Enable DHCP option 60	Select the toggle button to enable DHCP Option 60 (vendor class identifier).
Enable DHCP option 61	Select the toggle button to enable DHCP Option 61 (client identifier).
Enable DHCP option 77	Select the toggle button to enable DHCP Option 77 (user class information).
Enable DHCP option 90	Select the toggle button to enable DHCP Option 90 (authentication information).

4

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

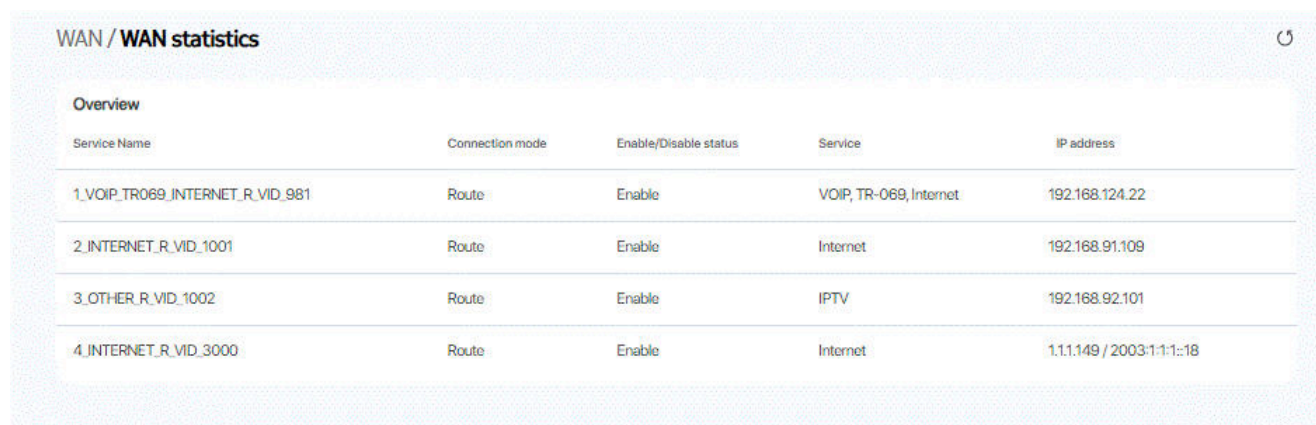
END OF STEPS

4.11 Viewing WAN Statistics

1

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

Figure 4-9 WAN Statistics page



WAN / WAN statistics				
Overview				
Service Name	Connection mode	Enable/Disable status	Service	IP address
1_VOIP_TR069_INTERNET_R_VID_981	Route	Enable	VOIP, TR-069, Internet	192.168.124.22
2_INTERNET_R_VID_1001	Route	Enable	Internet	192.168.91.109
3_OTHER_R_VID_1002	Route	Enable	IPTV	192.168.92.101
4_INTERNET_R_VID_3000	Route	Enable	Internet	1.1.1.149 / 2003:1:1:1::18

2

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

Figure 4-10 WAN Statistics page info

← WAN / WAN statistics / 1_VOIP_TR069_INTERNET_R_VID_981

PON port status

PON link status

Up

Service

WAN connection list

1_VOIP_TR069_INTERNET_R_VID_981

Enabled

Service details

Access type	access_dsl1
Connection mode	Dynamic DHCP
VLAN	981
WAN link status	Up
MAC address	50:21:54:6a:52:dc
IPv4 address	192.168.124.22
Netmask	255.255.255.0
Gateway	192.168.124.1
Primary DNS	8.8.8.8
Secondary DNS	192.168.23.30
DHCP Keep Alive	Disabled

Service statistics

Counters	1_VOIP_TR069_INTERNET_R_VID_981
Bytes sent	503292
Bytes received	2899307
Packets sent	4365
Packets received	17637
Unicast packets sent	4365
Unicast packets received	17637
Unknown proto packets received	0

Table 4-4 WAN statistics parameters

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

END OF STEPS

4.12 Configuring TR-069

1

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



Note: If the ACS Lock is enabled, TR-069 option is not displayed in the left pane and the TR-069 WebGUI screen is not accessible to all the users until the lock is disabled.

Figure 4-11 TR-069 page

2

Configure the following parameters:

Table 4-5 TR-069 parameters

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

Table 4-5 TR-069 parameters (continued)

Field	Description
Username	Enter the Username used to authenticate the CPE when making a connection to the ACS.
Password	Enter the Password used to authenticate the CPE when making a connection to the ACS.
Connect request username	Enter the Username used to authenticate an ACS making a Connection Request to the CPE.
Connect request password	Enter the Password used to authenticate an ACS making a Connection Request to the CPE.

3

Click **Save**.

END OF STEPS

4.13 Configuring TR-369



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

1

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



Note: If the ACS Lock is enabled, TR-369 option is not displayed in the left pane and the TR-369 WebGUI screen is not accessible to all the users until the lock is disabled.

Figure 4-12 TR-369 page

2

Configure the following parameters:

Table 4-6 TR-369 parameters

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

3

Click **Save**.

END OF STEPS

4.14 Configuring GRE tunnel

1

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

Figure 4-13 GRE Tunnel page

WAN / GRE tunnel

Tunnel name

Create new GRE tunnel

IP mode

IPv4

WAN interface

1_TR069_INTERNET_VOIP_R_VID_881

Primary remote end

Secondary remote end

Connected remote end

-

Connectivity check

Traffic timeout to start pings

10

No. of retries before unreachable

3

2

Configure the following parameters:

Table 4-7 GRE Tunnel parameters

Field	Description
Tunnel Name	Select Create new GRE Tunnel or select an existing tunnel from the list. The tunnel name is automatically assigned by the system. Up to 3 GRE tunnels are supported.

Table 4-7 GRE Tunnel parameters (continued)

Field	Description
IP mode	Select an IP mode from the drop-down list.
WAN Interface	Select a WAN interface from the list. GRE tunnels can only be created on HSI-enabled WAN interfaces.
Primary Remote End Secondary Remote End (optional)	Enter an IP address or FQDN that is unique in the system. If the primary remote endpoint is down or unreachable, the secondary remote endpoint becomes active, if configured. The secondary remote endpoint remains active until it becomes unreachable, in which case the primary remote endpoint becomes active again. Revertive mode is not supported. If both endpoints are unreachable, the GRE tunnel is declared down.
Connected Remote End	This field displays the current data traffic path for the GRE tunnel.
Connectivity check	This feature is automatically selected by the system.
Traffic timeout to start pings	Enter the traffic timeout in seconds (2 to 1024).
No. of retries before unreachable	Enter the number of retries before the tunnel is declared down (0 to 100).

3

Click **Save**.



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

END OF STEPS

4.15 Configuring Static routing

1

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

Figure 4-14 IP routing page

WAN / Static routing

IP routing

Enable IP routing

Destination IP address

Destination netmask

Gateway

IPv4 interface

Forwarding policy ⓘ

Add

☒

0.0.0.0

1_INTERNET_R_VID_81

No Policy:-1

2

Configure the following parameters:

Table 4-8 IP routing parameters

Field	Description
Enable IP routing	Select the toggle button to enable IP routing.
Destination IP address	Enter the destination IP address.
Destination netmask	Enter the destination netmask.
Gateway	Enter the gateway IP address.
IPv4 interface	Select an IPv4 interface from the list.
Forwarding policy	Select a forwarding policy from the list.

3

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

END OF STEPS

4.16 Viewing Optical Module Status

- 1
- Click **WAN**→**Optical module status** in the left pane. The *Optical module status* page displays the following information.

Figure 4-15 Optical module status page

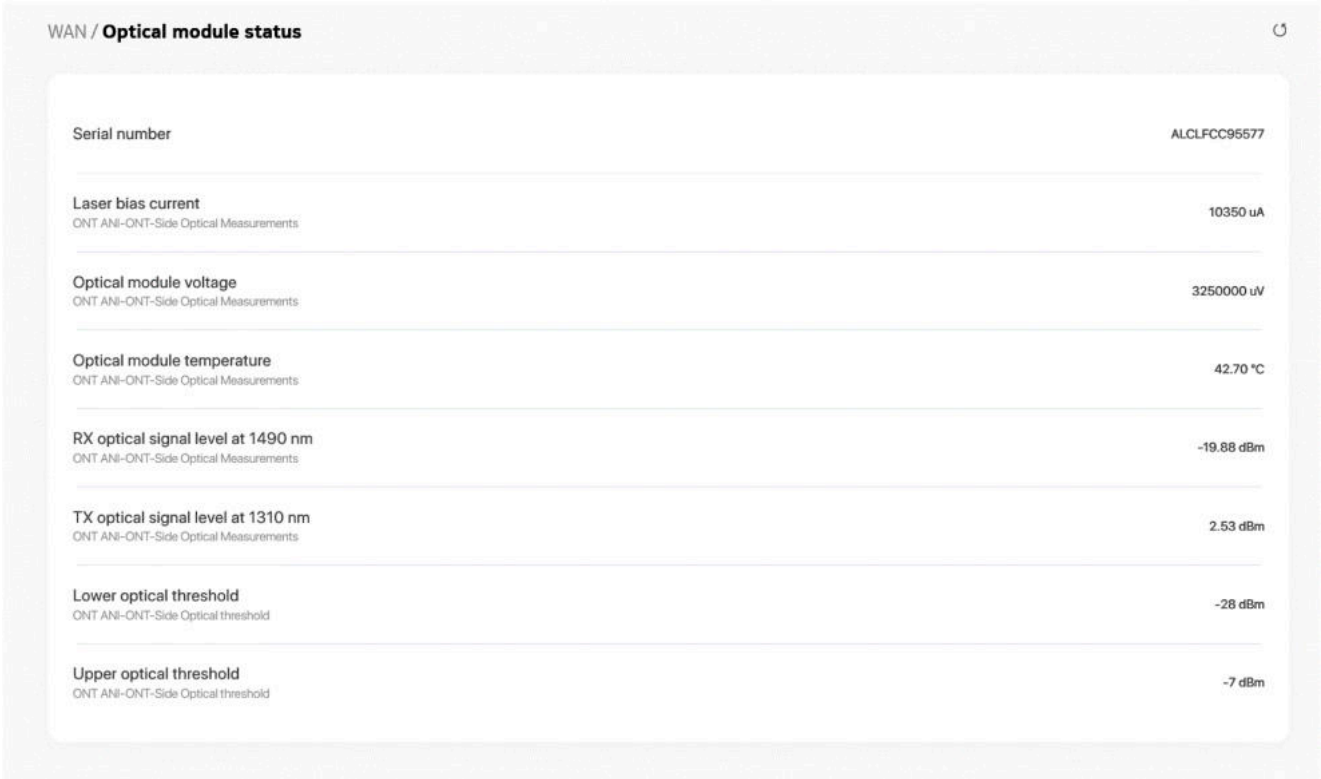


Table 4-9 Optical module status parameters

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

Table 4-9 Optical module status parameters (continued)

Field	Description
Rx optical signal level at 1310 nm (ONT ANI-ONT-Side Optical Measurements)	Transmitted opticals signal level at 1310 nm, measured in dBm.
Lower (ONT ANI-ONT-Side Optical Threshold)	Lower optical threshold, measured in dBm.
Upper (ONT ANI-ONT-Side Optical Threshold)	Upper optical threshold, measured in dBm.

END OF STEPS

4.17 Configuring QoS

1

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

Figure 4-16 QoS config page (L2 Criteria)

WAN / QoS config

Type

L2 Criteria

Classification criteria

Source Mac

Ex: AA:BB:CC:DD:EE:FF

Enable source MAC mask

Interface

Select option

Classification row

DSCP remark

Range 0-63

802.1p Remark

Range 0-7

Forwarding policy

Range 1-7

Figure 4-17 QoS config page (L3 Criteria)

WAN / QoS config

↻

Add

Type

L3 Criteria

Classification criteria

Protocol

None

Application

Customer Setting

Source IP

Source IP Mask

Dest IP

Dest IP mask

Source Port

Source Port Max

Destination Port

Dest Port Max

802.1p

Interface

Select option

Classification row

DSCP remark

Range 0-63

802.1p Remark

Range 0-7

Forwarding policy

Range 1-7

2

Configure the following parameters:

Table 4-10 QoS config parameters

Field	Description
Type	Select a QoS service layer type from the list: • L2 Criteria • L3 Criteria
Classification criteria (L2)	
Source MAC	Enter the source MAC address.
Enable source MAC mask	Select the toggle button to enable the source MAC mask. This button is disabled by default.
Source MAC mask	Enter the source MAC mask address. The syntax is for example: FF:FF:FF:00:00:00 which must be a continuous bit mask pattern on this device. This field is visible only if the Enable source MAC mask button is enabled.
Interface	Select an interface from the list.
Classification criteria (L3)	
Protocol	Select a protocol from the list.
Application	Select an application from the list or select Custom Settings and enter an application name.
Source IP	Enter the source IP address.
Source IP mask	Enter the source IP address netmask.
Destination IP	Enter the destination IP address.
Destination IP mask	Enter the destination IP address netmask.
Source port	Enter the source port number.
Source port max	Enter the values for the source port max (highest port number).
Destination port	Enter the destination port number.
Destination port max	Enter the values for the destination port max (highest port number).
802.1p	Indicates whether 802.1p is enabled.
Interface	Select an interface from the list.
Classification row	
DSCP remark	Enter the value for the DSCP remark (applicable only for L3 criteria). Allowed values: 0 to 63
802.1p Remark	Enter the value for the 802.1p remark. Allowed values: 0 to 7
Forwarding policy	Enter the number for the forwarding policy. Allowed values: 1 to 7

3

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

END OF STEPS

4.18 Configuring Upstream (US) Classifier

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

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

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

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

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

1

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

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

Figure 4-18 US Classifier - Policy page

WAN / US classifier

Policy
Classifier
Classifier Rules

Tunnel Type
Select option

Tunnel Interface
Select option

VLAN id
0-4093

VLAN Tag
hex

VLAN Priority
0-7

IP TOS/DSCP
0

Drop

Save
Reset

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

2

Configure the following parameters:

Table 4-11 US Classifier - Policy parameters

Field	Description
Tunnel Type	The tunnel type is set to GRE and cannot be modified.
Tunnel Interface	Select a tunnel interface from the list: No Tunnel

Table 4-11 US Classifier - Policy parameters (continued)

Field	Description
VLAN ID	Enter a VLAN ID. Allowed values: 0 to 4093
VLAN Tag	This field is not configurable. The VLAN tag is set to 8100 (hexadecimal). Determines the VLAN tag used inside the GRE tunnel.
VLAN Priority	Enter a VLAN priority level. A lower number indicates a higher priority. Allowed values: 0 to 7
IP TOS/DSCP	This field is not configurable. All tunnel packets are generated with a default DSCP value (usually 0). Allowed values: 0 to 63
Drop	Select the toggle button to enable dropping of the packets.

3

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

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

4

Select the **Classifier** tab.

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

Figure 4-19 US Classifier - Classifier page

WAN / **US classifier**

Policy
Classifier
Classifier Rules

Interface
Select option

Source MAC

Source IP

Source Port

Protocol

Destination MAC

Destination IP

Destination Port

Priority
Select option

Save
Reset

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

5

Configure the following parameters:

Table 4-12 US Classifier - Classifier parameters

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

Table 4-12 US Classifier - Classifier parameters (continued)

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

6

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

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

7

Select the **Classifier Rules** tab.

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

Figure 4-20 US Classifier - Classifier Rules page

WAN / 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

Select option

Select option

Select option

Save

Reset

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

8

Configure the following parameters:

Table 4-13 US Classifier - Classifier Rules parameters

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

9

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

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

END OF STEPS

LAN Configuration

4.19 Overview

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

Sub-menu	Procedure
DHCP IPv4	4.20 "Configuring DHCP IPv4" (p. 106)
DHCP IPv6	4.21 "Configuring DHCP IPv6" (p. 108)
DNS	4.22 "Configuring DNS" (p. 110)
LAN statistics	4.23 "Viewing LAN Statistics" (p. 113)

4.20 Configuring DHCP IPv4

- 1
- Click **LAN**→**DHCP IPv4** in the left pane. The *DHCP IPv4* page displays.

Figure 4-21 DHCP IPv4 page

LAN / DHCP IPv4

Port Mode

All ports to bridge mode

Port 1

Port 2

Port 3

Port 4

Save

Route Mode

Route Mode

Route Mode

Route Mode

IPv4 address

Subnet mask

DHCP enable

DHCP start IP address

DHCP end IP address

DHCP lease time

Primary DNS

Secondary DNS

Save

Static IPv4 address reservations

MAC address

IPv4 address

Add

2

Configure the following LAN parameters:

Table 4-14 DHCP IPv4 parameters

Field	Description
IPv4 address	Enter the IPv4 address of the ONT.
Subnet mask	Enter the subnet mask of the ONT.
DHCP enable	Select the toggle button to enable DHCP. If this toggle button is not enabled, the DHCP functionality cannot be used. you need not configure DHCP start IP address, DHCP end IP address and DHCP lease time if this toggle button is not enabled.
DHCP start IP address	Enter the starting range of the DHCP IP address.
DHCP end IP address	Enter the ending range of the DHCP IP address.
DHCP lease time	Enter the DHCP lease time (in minutes). Allowed values: 5 to 129600 minutes or 0 for 1 day
Primary DNS	Enter the primary DNS IP address.
Secondary DNS	Enter the secondary DNS IP address.

3

Click **Save**.

4

Configure the Static DHCP parameters.

Table 4-15 Static DHCP parameters

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

5

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

END OF STEPS

4.21 Configuring DHCP IPv6

1

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

LAN / DHCP IPv6

Save

LAN prefix configuration

Prefix Config

Select option

Interface

4_INTERNET_R_VID_3000

Received IPv6 prefix

2003:10:10:1b3c::/64

LAN prefix configuration for gateways

Enable prefix delegation

IPv6 address method

Address method

Stateless Address Autoconfig (SLAAC)

Receive additional options via DHCPv6

Advanced router advertisement configuration

Maximum interval for periodic RA messages

600

seconds

Minimum interval for periodic RA messages

200

seconds

2

Configure the following parameters:

Table 4-16 DHCP IPv6 parameters

Field	Description
LAN prefix configuration	

Table 4-16 DHCP IPv6 parameters (continued)

Field	Description
Prefix Config	Select a prefix configuration option from the list: • Use WAN provided prefix (prefix is obtained from the WAN) • Static (enables you to enter the prefix)
Interface	This field displays if you select the Use WAN provided prefix option from the Prefix Config list. Select a WAN connection interface from the list.
Received IPv6 prefix	This field displays the received IPv6 prefix. This field is displayed only when Prefix Config is set to Use WAN provided prefix .
Static IPv6 prefix	This field displays the static IPv6 prefix. This field is displayed only when Prefix Config is set to Static .
IPv6 address method	
Address method	Select a address method option from the list: • Stateless Address Autoconfig (SLAAC) • Stateful DHCPv6
Received additional options via DHCPv6	Select the toggle button to enable additional options via DHCPv6. This field is displayed only when Address method is set to Stateless Address Autoconfig (SLAAC) .
Advanced router advertisement configuration	
Maximum interval for periodic RA messages	Enter the maximum interval (in seconds) for periodic Router Advertisement messages. Allowed values: 4 to 1800 seconds.
Minimum interval for periodic RA messages	Enter the minimum interval (in seconds) for periodic Router Advertisement messages. Allowed values: 4 to 1800 seconds

3

Click **Save**.

END OF STEPS

4.22 Configuring DNS

4.22.1 IPv4 DNS configuration

1

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

Figure 4-22 DNS page (IPv4)

LAN / DNS

IPv4 IPv6

DNS Proxy ☒

Save

Domain Name

IPv4 address

Add

Origin Domain

New Domain

Add

Static DNS entries

Domain Name	IPv4 address	Delete
dsdevice.lan	192.168.1.254	Delete

2

Configure the following parameters:

- Select the **DNS proxy** toggle button to enable the DNS proxy and click **Save**.
- Configure the following:
 - Enter the domain name in the Domain Name field.
 - Enter the domain IP address in the IPv4 Address field.
 - Click **Add**.
- Configure the following:
 - Enter the origin domain name in the Origin Domain field.
 - Enter the new domain name in the New Domain field.
 - Click **Add** to associate an origin domain with a new domain.

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

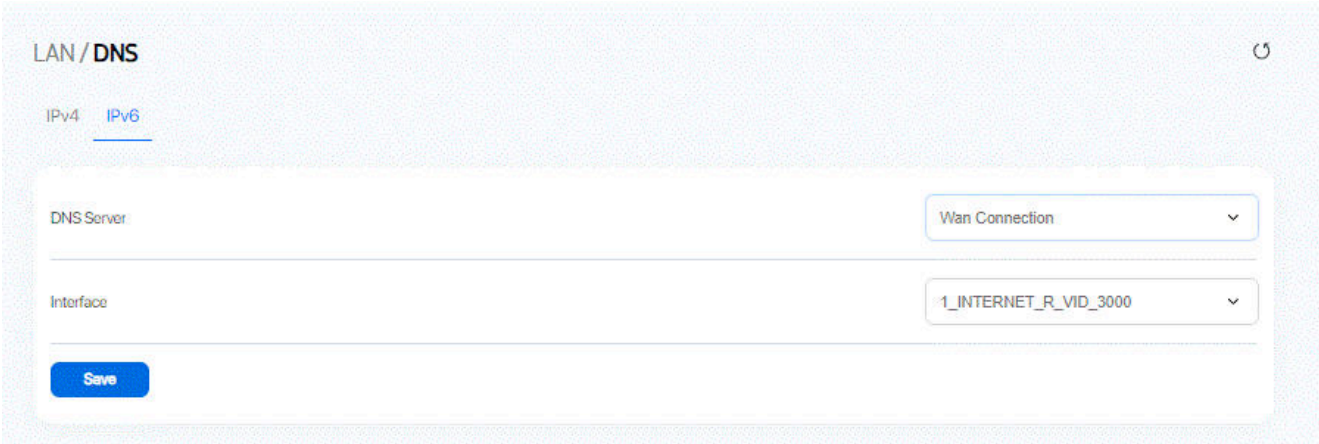
END OF STEPS

4.22.2 IPv6 DNS configuration

1

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

Figure 4-23 DNS page (IPv6)



2

Configure the following parameters

Table 4-17 DNS parameters

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

3

Click **Save**.

END OF STEPS

4.23 Viewing LAN Statistics

1

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

Figure 4-24 LAN statistics page

Item	LAN 1	LAN 2	LAN 3	LAN 4
Status	Up	Down	Down	Down
Duplex mode	Full Duplex	Half Duplex	Half Duplex	Half Duplex
Speed (kbps)	1000	Auto	Auto	Auto
Bytes sent	18171543	0	0	0
Bytes received	15468599	0	0	0
Packets sent	87280	0	0	0
Packets received	130448	0	0	0
Errors sent	0	0	0	0
Unicast packets sent	76103	0	0	0
Unicast packets received	108893	0	0	0
Broadcast packets sent	0	0	0	0
Broadcast packets received	0	0	0	0
Multicast packets sent	11102	0	0	0
Multicast packets received	77755	0	0	0
Broadcast packets sent	4	0	0	0
Broadcast packets received	1908	0	0	0
Unicast packets received	0	0	0	0
CRC errors received	0	0	0	0

Table 4-18 LAN statistics parameters

Field	Description
SSID name	Select an SSID from the list.
LAN Wireless info	Displays the wireless status, wireless channel, encryption status, received and transmitted bytes and packets and power transmission in mW.

Table 4-18 LAN statistics parameters (continued)

Field	Description
LAN Ethernet info	Displays the Ethernet status IP address, subnet mask, MAC address, received and transmitted bytes and packets.
Info	Displays the information of each such as status, duplex mode, maximum bit rate, packets received and sent, CRC errors, and so on.

END OF STEPS

WiFi Configuration

4.24 Overview

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

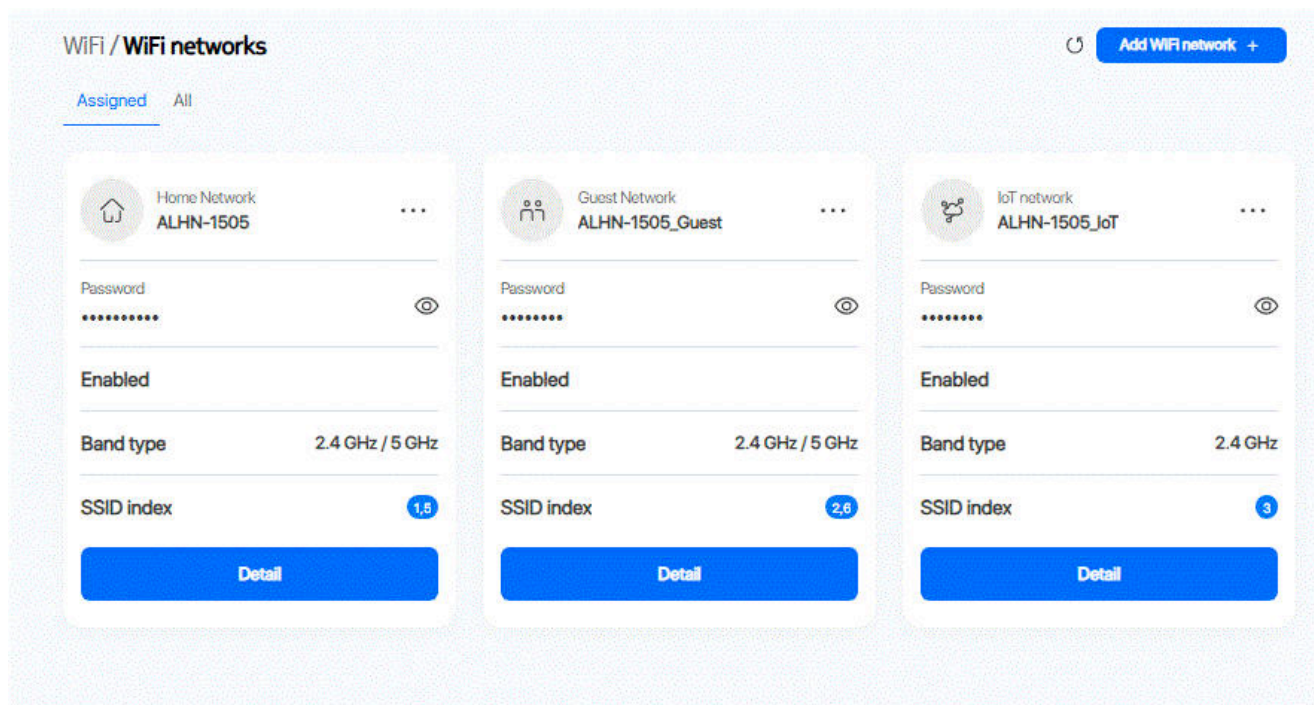
Sub-menu	Procedure
WiFi networks	4.25 "Configuring WiFi Network" (p. 115)
IoT network	4.27 "Configuring IoT Network" (p. 121)
Guest network	4.28 "Configuring Guest Network" (p. 122)
Network map	4.29 "Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points" (p. 124)
Advanced settings	4.31 "Configuring Wireless 2.4 GHz" (p. 128) 4.32 "Configuring Wireless 5 GHz" (p. 131)
Wireless schedule	4.33 "Configuring Wireless Schedules" (p. 133)
WiFi statistics	4.34 "Viewing WiFi Statistics" (p. 134)

4.25 Configuring WiFi Network

1

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

Figure 4-25 WiFi network page



2

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



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

Figure 4-26 Add WiFi network page

Add WiFi network

Please select a preferred network type from the options below.

Multi Band

Recommended — Band steering will intelligently move your devices from the 2.4GHz and 5GHz network based on usage, speed, coverage and distance.

☒

2.4 GHz

☐

5 GHz

☐

Next

3

Configure the following parameters:

Table 4-19 Add WiFi network parameters

Field	Description
Multiband	Select this option to configure a multiband wireless network on all supported bands. This option is recommended. Your devices will roam to a different wireless band based on usage, speed, coverage and distance. The wireless encryption of this network is WPA3-Personal Transition.
2.4 GHz	Select this option to configure a 2.4 GHz wireless network. This might be needed if some older devices have issues connecting to a band-steering network. The wireless encryption of this new network is WPA2-Personal.
5 GHz	Select this option to configure a 5 GHz wireless network. This might be needed if some older devices have issues connecting to a band-steering network. The wireless encryption of this new network is WPA2-Personal.

4

Click **Next**.

5

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

- 6
- Enter the password for the network in the Password field and click **Save**.
The WiFi network is created and is displayed as a card in the **Enabled** tab of the *WiFi networks* page.



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

- 7
- Click **Detail** to view and edit the SSID configuration for your network.

Figure 4-27 WiFi network - example of SSID Configuration page

← Network / WiFi networks / ALHN-EC1B1111

SSID configuration

SSID name

ALHN-EC1B1111

Enable WiFi network

☒

Band type

2.4 GHz / 5 GHz

SSID index

1,5

Broadcast the WiFi network

☒

Guest mode

Disabled

Isolation

☐

Total max users ⓘ

128

Encryption mode

WPA3-Personal-Transition

Password

•••••••• ⓘ

Enable WPS

☐

Save

- 8
- Configure the following parameters:
- | Field | Description |
|----------------------------|--|
| SSID name | Displays the SSID name. |
| Enable WiFi network | Select the toggle button to enable WiFi network. |
| Band type | Displays the band type. |
| SSID index | Displays the SSID index. |
| Broadcast the WiFi network | Select the toggle button to enable broadcasting of the WiFi network. |

Field	Description
Guest Mode	Indicates whether guest mode is enabled or disabled. When a particular SSID is enabled with Guest Mode, LAN devices connected to the SSID can only connect to the Internet. Such devices cannot see or communicate with other LAN devices.
Port Mode	Select the required port from the list.
Isolation	Select the toggle button to enable isolation.
Total MAX users	Enter the maximum number of users.
Encryption Mode	Select an encryption mode from the list: • None • WPA2-Personal • WPA3-Personal • WPA3-Personal-Transition • WPA3-Enterprise
Enable WPS	Select the toggle button to enable WPS. Note: When you select Enable, a security warning is displayed. Click OK to continue.
WPS Mode	Select the required WPS mode from the list: • PBC • STA PIN • AP PIN Select a WPS mode from the list: PBC (Push Button Connect) or STA PIN (Personal Identification Number) or AP PIN (Access Point Personal Identification Number). If the WPS mode is AP PIN, Click Get PIN Number. A PIN Code Number is generated. Then, the end user must click WPS Connect and enter the generated PIN Code Number into the station, so that the station can connect to the selected SSID. If the WPS mode is STA PIN, the PIN Code Number will be generated by the station. Then, the end user must enter this PIN Code Number into the PIN Code Number field and click WPS Connect, so that the station can connect to the selected SSID.
Domain Grouping	Select the toggle button to enable domain grouping.

Notes:

1. The EasyMesh standard does not support synchronizing WPA3-only mode to the other nodes that participate in the mesh. For this reason, the WPA3 (only) mode should not be used on devices that participate in an EasyMesh mesh. Instead, WPA2/WPA3 mode should be used, as is also mentioned in the EasyMesh standard.

9

Click **Save**.

END OF STEPS

4.26 Configuring the WiFi Password

A password must adhere to the following password rules:

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

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

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

- First character cannot be special one
- Password can only contain numbers, letters and special character !#+, -./:=@
- The password should use at least one uppercase letter, one lowercase letter, one number, and one special character
- Password should be atleast 8 characters
- Password should be atmost 24 characters
- The same character cannot appear consecutively 8 times

1

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

Figure 4-28 Edit Wi-Fi network page

Edit WiFi network ×

Name

ALHN-1505

Password

.....

Password requirements:

- 8-63 characters long
- Password can only contain numbers, letters and special character !#+, -./:=@_
- The password should use at least one uppercase letter, one lowercase letter, one number, and one special character
- The same character can not appear consecutively 8 times

Save

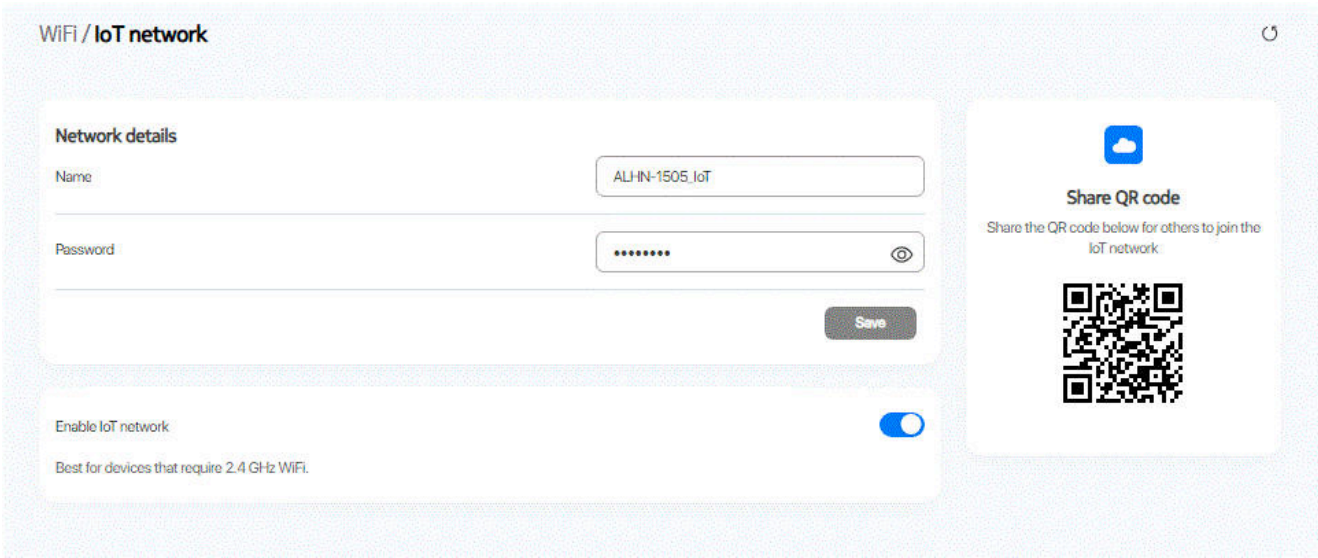
- 2 _____
Enter the new password.
- 3 _____
Click **Save**.

END OF STEPS _____

4.27 Configuring IoT Network

- 1 _____
Click **WiFi→IoT network** in the left pane. The *IoT network* page displays the IoT network details.

Figure 4-29 IoT network page



2 _____

Configure the following parameters:

Field	Description
Name	Enter the name for the IoT network.
Password	Enter the password for the IoT network.
Enable IoT network	Select the toggle button to enable the IoT network.

3 _____

Click **Save**.

4 _____

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

END OF STEPS _____

4.28 Configuring Guest Network

1 _____

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

Figure 4-30 Guest network page

WiFi / Guest network

Network details

Name

NOKIA-5C91_Guest

Password

.....

Use 8 or more characters.

Save

Enable guest network

Allow guests to access the Internet. Devices connected to this network will not be able to access other devices in your home network.

Share QR code

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

2

Configure the following parameters:

Table 4-20 Guest network parameters

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

3

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

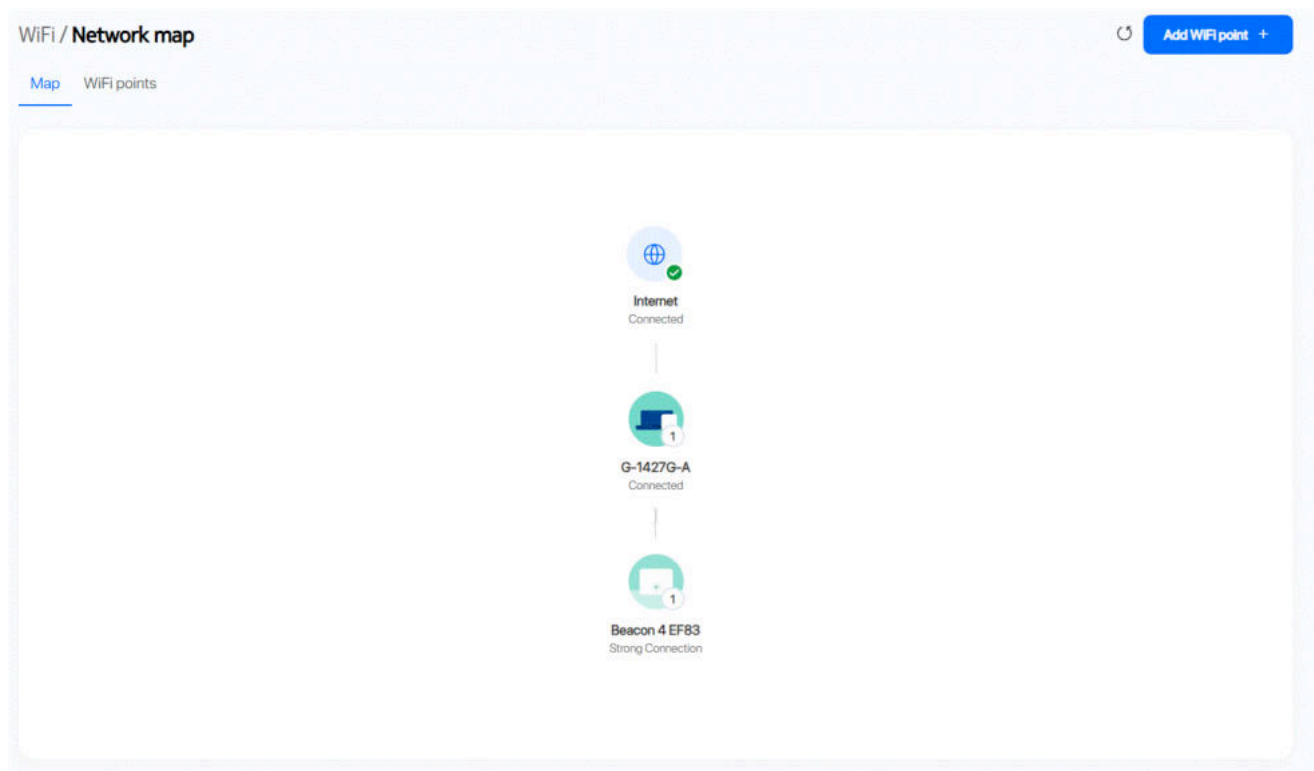
END OF STEPS

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

1

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

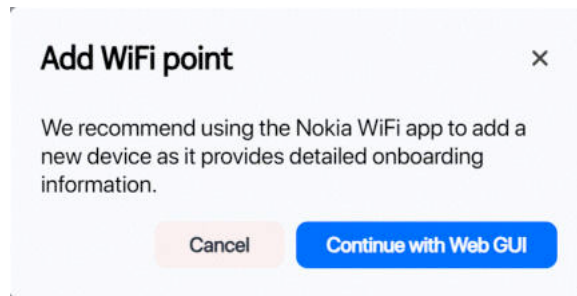
Figure 4-31 Network map page



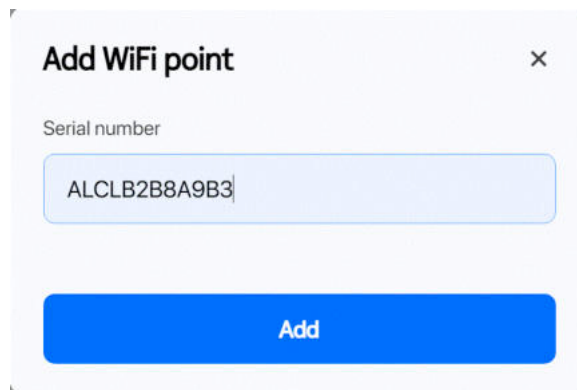
2

Perform the following steps to add a WiFi point:

- Click **Add WiFi point** at the top right corner of the *Device Info* page. A message displays that it is recommended to use the Nokia WiFi mobile app to add a WiFi point.
- To add a WiFi point using the WebGUI, click **Continue with WebGUI**.



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

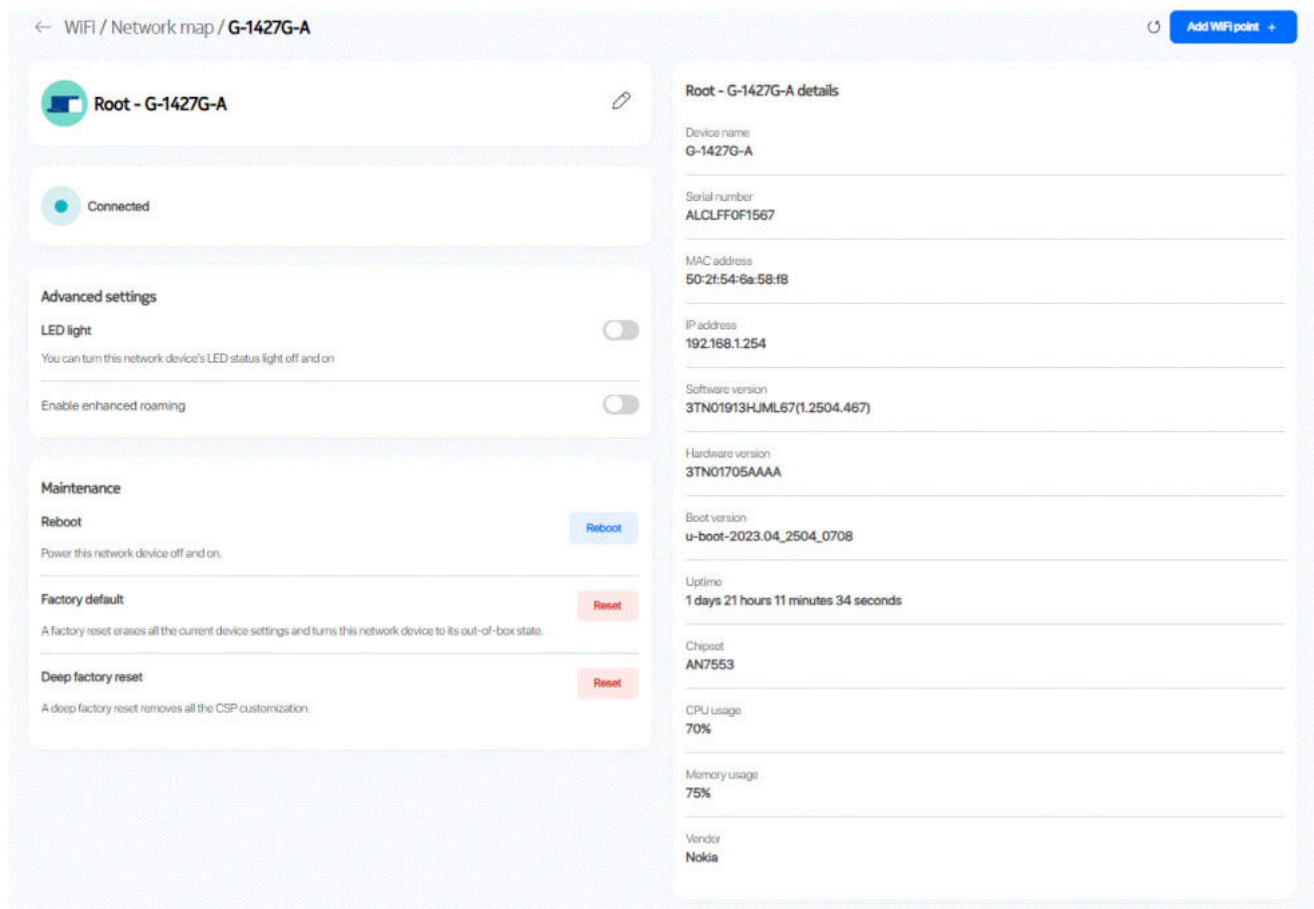


The WiFi point is displayed in the *Detected* or *Not detected* list of the *Onboarding Status* panel in the *Device Info* page.

3

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

Figure 4-32 <Device> page



4

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

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

- To edit the name of the WiFi point, click the Edit icon . The **Change the name of your WiFi point** page displays.
- On the page **Change the name of your WiFi point**, click the drop-down menu to select a name for the WiFi point, or enter a **Custom name** to create your own customized name.
- Click **Save**.

Figure 4-33 Change the name of your WiFi point page

Table 4-21 <Device> parameters

Field	Description
Device name	Name on the device
Serial number	Serial number of the device
Software version	Software version of the device (displays only for a root device)
Hardware version	Hardware version of the device (displays only for a root device)
Boot version	Boot version of the device (displays only for a root device)
Uptime	Amount of time the device has run since last reset in hours, minutes, and seconds (displays only for a root device)
Chipset	Chipset of the device (displays only for a root device)
Vendor	Name of the vendor (displays only for a root device)
Onboarding status	Onboarding status of the device in the WiFi network (displays only for an extender device)
Backhaul status	Backhaul status of the device (displays only for an extender device)
Location nickname	Name of the location of the device (displays only for an extender device)

5

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

6

Perform any of the following, as applicable:

- **Reboot the device:**

1. Click **Reboot**. A message displays asking if you want reboot the device.

2. Click **OK** to reboot the ONT. The device reboots and displays the login page.

- **Reset the device to factory default settings:**

1. Click **Factory default**. A message displays asking if you want to reset the system configuration to the factory default settings.
2. Click **OK** to reset the ONT to the factory default settings.

- **Reset the device to deep factory default settings:**

1. Click **Deep factory reset**. A message displays asking if you want to reset the system configuration to the factory default settings.
2. Click **OK** to reset the ONT so that all the downloaded configuration files such as Web customization, delta-config, certification file and so on will be removed.

END OF STEPS

4.30 Optimizing WiFi Network

In the **WiFi→Advanced settings**, the **Run channel optimization** button can be clicked by the user to initiate an immediate network assessment. If a more suitable channel is available, the system initiates a channel switch.

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

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

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

4.31 Configuring Wireless 2.4 GHz

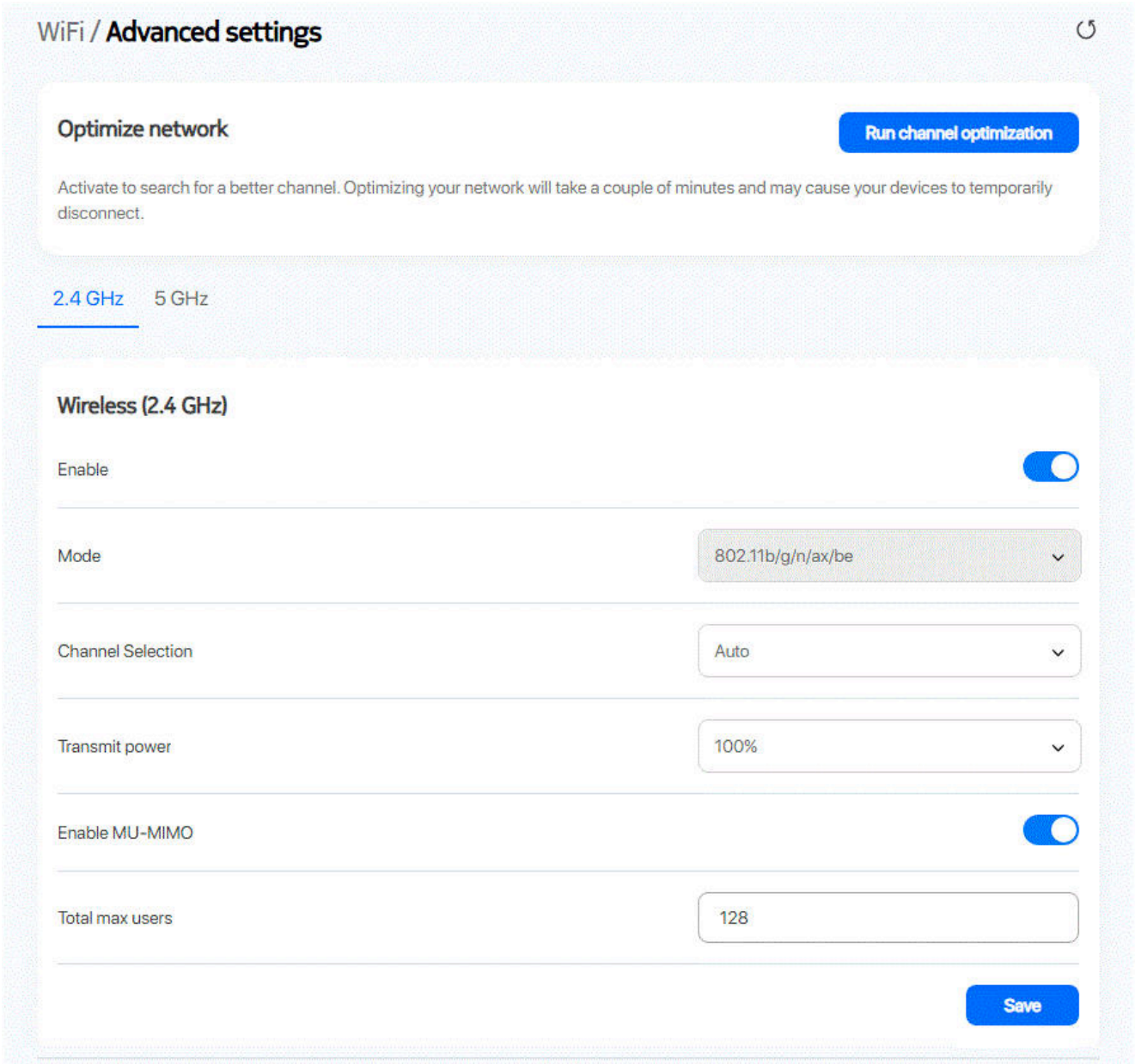
1

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

2

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

Figure 4-34 Advanced settings - 2.4 GHz tab



3

Configure the following parameters:

Table 4-22 Wireless 2.4 GHz parameters

Field	Description
Enable	Select the toggle button to enable Wireless (2.4 GHz).
Mode	Select a wireless mode from the list: • 802.11b/g/n/ax • 802.11b/g/n • 802.11b • 802.11g • 802.11n • 802.11b/g • 802.11g/n • 802.11n/ax
Channel Selection	Select a channel from the list: • Auto • Manual Note: When changing from automatic to manual channel management, depending on the channel, channel bandwidth, and region, it can take several minutes for the changes to take into effect and for the wireless network to be functional again. Also, after a reboot, this same delay is observed. It is recommended to set this value to "Auto".
Channel bandwidth	Select the bandwidth range from the list: • 20 MHz • 40 MHz This parameter is visible only if the Channel Selection is Manual.
Channel	Select a channel from the list . This parameter is visible only if the Channel Selection is Manual .
Transmit power	Select a percentage for the transmitting power from the list: • 25% • 50% • 75% • 100%
Enable MU-MIMO	Select the toggle button to enable or disable MU-MIMO.
Total max users	Enter the maximum number of users.

4

Click **Save**.

END OF STEPS

For optimizing WiFi network, see [4.30 "Optimizing WiFi Network" \(p. 128\)](#).

4.32 Configuring Wireless 5 GHz

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

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

Figure 4-35 Advanced settings - 5 GHz tab

Optimize network Run channel optimization

Activate to search for a better channel. Optimizing your network will take a couple of minutes and may cause your devices to temporarily disconnect.

2.4 GHz 5 GHz

Wireless (5 GHz)

Enable ☒

Mode 802.11a/n/ac/ax/be

Channel Selection Auto
☐ Exclude 160 MHz bandwidth ?

Transmit power 100%

Enable MU-MIMO ☒

Total max users 128

Save

3

Configure the following parameters:

Table 4-23 Wireless 5 GHz parameters

Field	Description
Enable	Select this toggle button to enable WiFi.
Mode	Select the mode from the list: • 802.11a/n/ac • 802.11a/n/ac/ax • 802.11n/ac/ax
Channel Selection	Select a channel from the list: • Auto • Manual Note: When changing from automatic to manual channel management, depending on the channel, channel bandwidth, and region, it can take several minutes for the changes to take into effect and for the wireless network to be functional again. Also, after a reboot, this same delay is observed. It is recommended to set this value to "Auto". To set the operating channel bandwidth to 80 MHz, select the Exclude 160 MHz bandwidth checkbox.
Channel bandwidth	Select the bandwidth range from the list: • 20 MHz • 40 MHz • 80 MHz • 160 MHz • Auto This parameter is visible only if the Channel Selection is Manual.
Channel	Select a channel from the list . This parameter is visible only if the Channel Selection is Manual .
Transmit power	Select a percentage for the transmitting power from the list: • 25% • 50% • 75% • 100%
Enable MU-MIMO	Select the toggle button to enable MU-MIMO. This can be enabled when multiple users are trying to access the wireless network. When this parameter is enabled, multiple users can access router functions without the congestion.
Total max users	Enter the total number of MAX users. The maximum users allowed is 64.

4

Click **Save**.

END OF STEPS

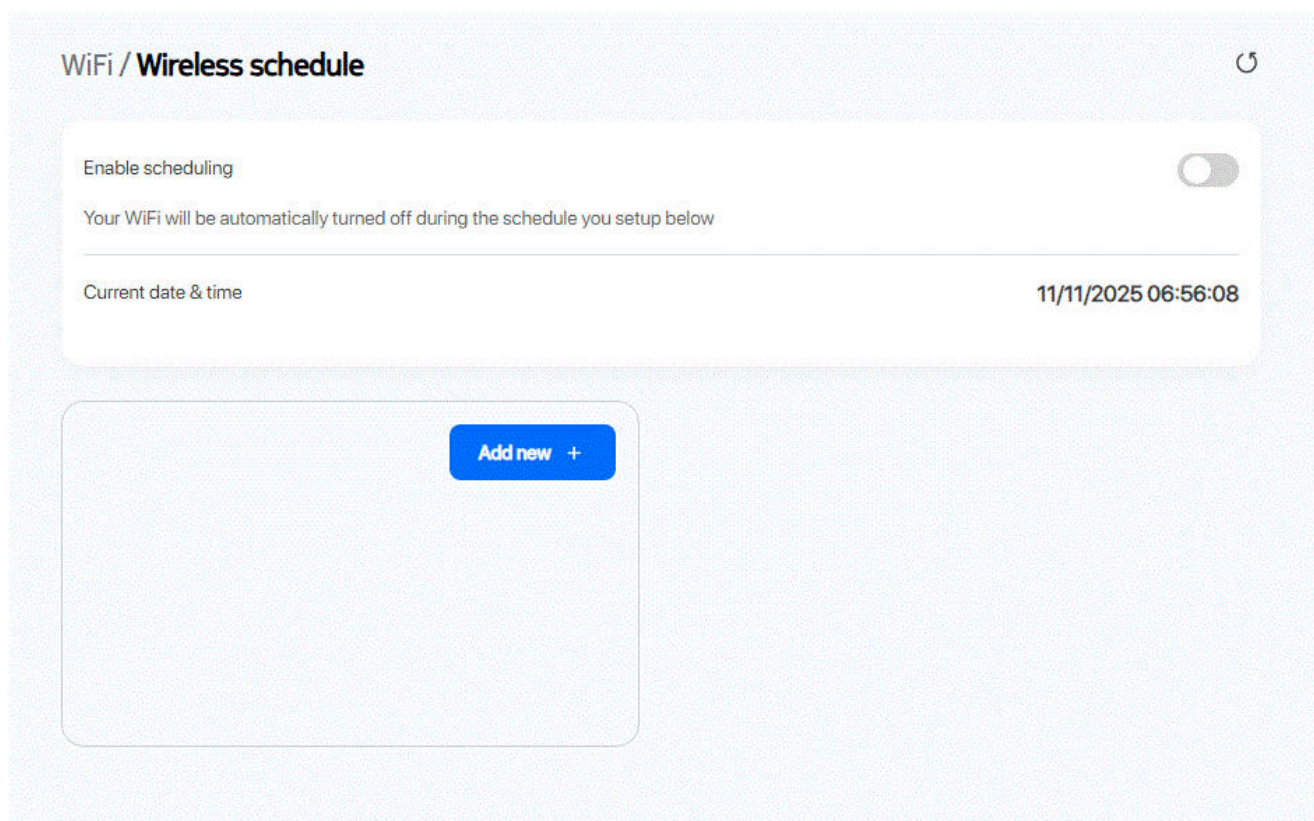
For optimizing the WiFi network, see [4.30 “Optimizing WiFi Network” \(p. 128\)](#).

4.33 Configuring Wireless Schedules

1

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

Figure 4-36 Wireless schedule page



2

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



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

3

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

4

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

5

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

6

If you select **Individual Days**, select the checkboxes for the desired days.
The Recurrence Pattern shows the rules created to date.

7

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

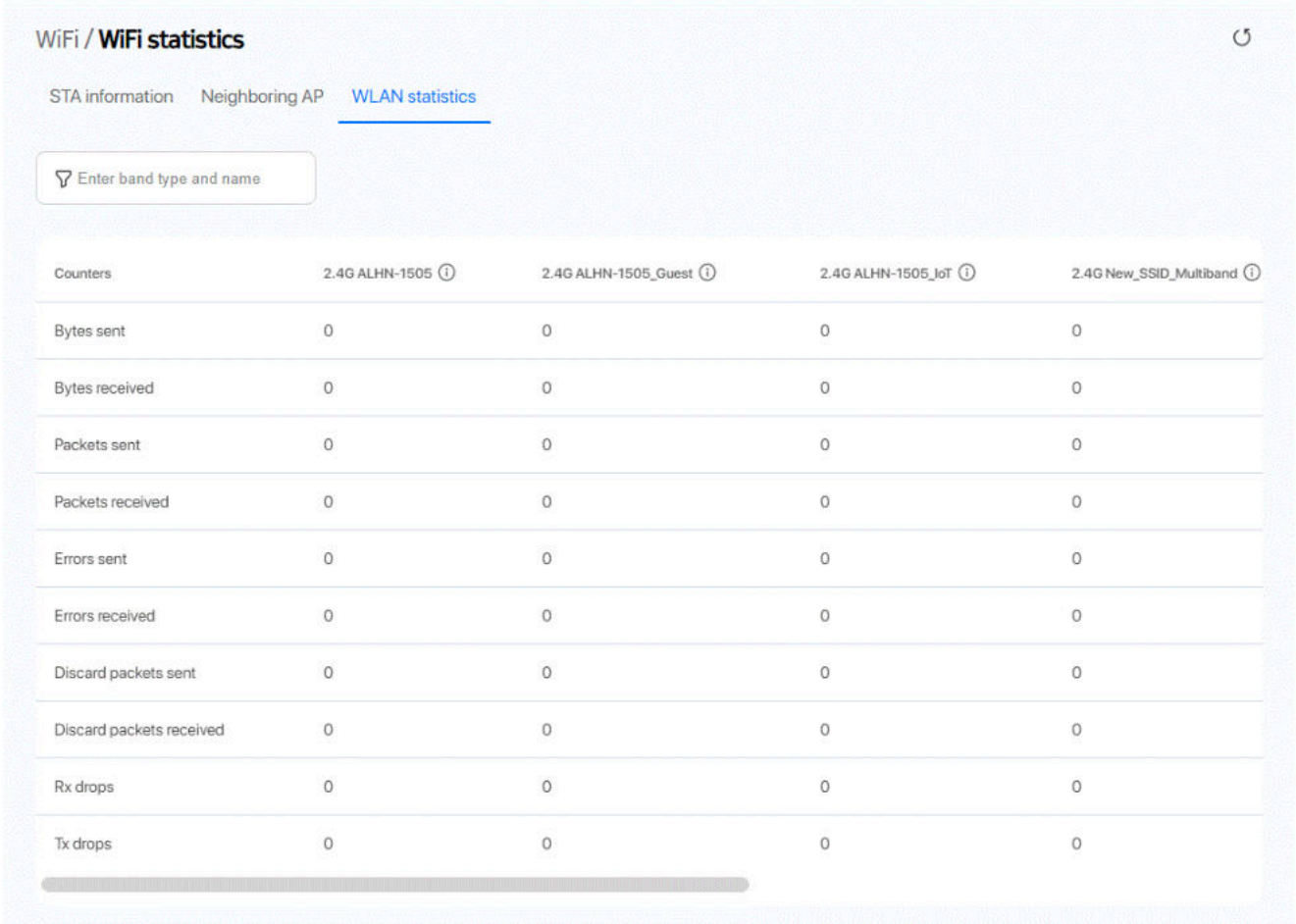
END OF STEPS

4.34 Viewing WiFi Statistics

1

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

Figure 4-37 WiFi statistics page



2 _____

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

Table 4-24 WLAN statistics parameters

Field	Description
Bytes sent	Displays the bytes sent.
Bytes received	Displays the bytes received.
Packets sent	Displays the packets sent.
Packets received	Displays the packets received.
Errors sent	Displays the errors sent.

Table 4-24 WLAN statistics parameters (continued)

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

END OF STEPS

Devices

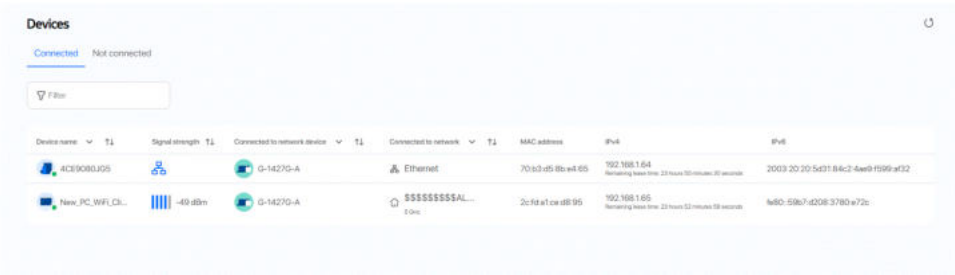
4.35 Overview

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

4.36 Viewing Device Information

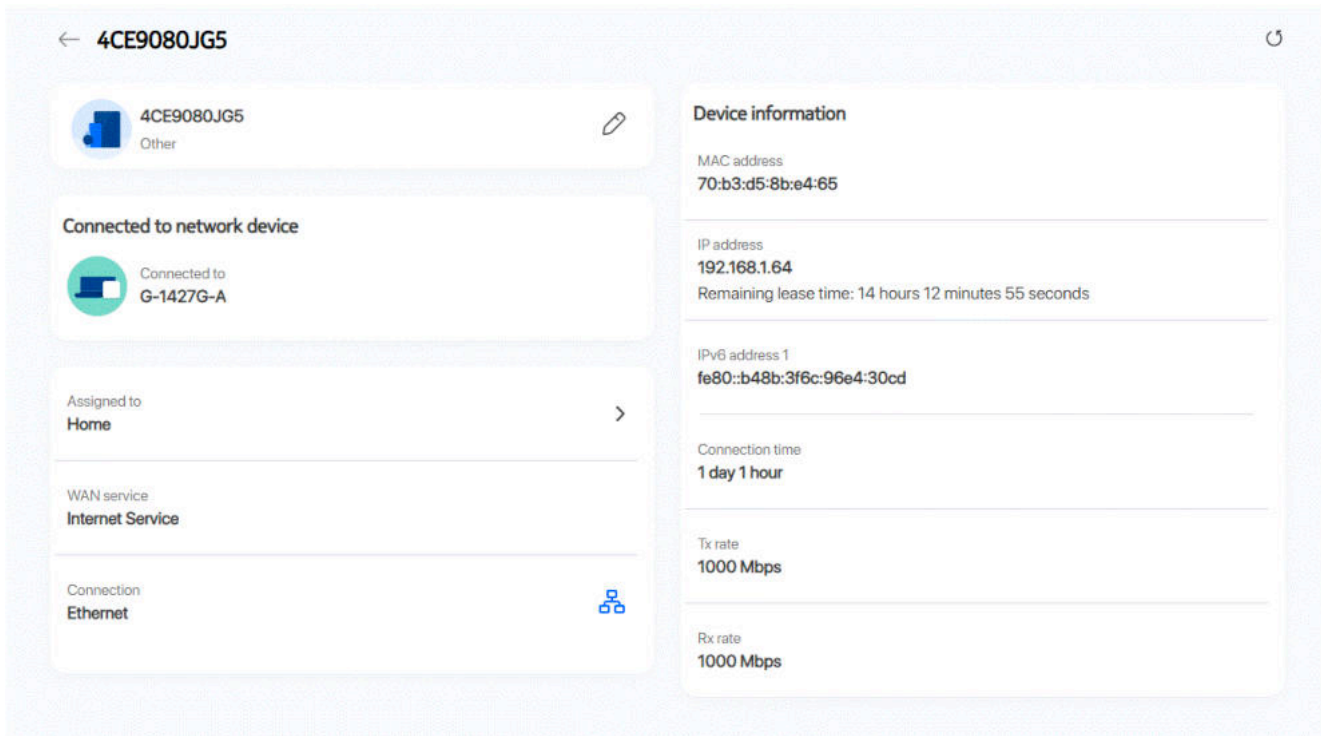
- 1
- Click **Devices** in the left pane. The *Devices* page displays the devices.

Figure 4-38 *Devices* page



- 2
- The *Devices* page lists the devices. Click on a Device to view the respective device Info page. The *Device Info* page displays the details of the selected device in a network.

Figure 4-39 Device information page - L3 devices



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

Perform the following steps to rename the client device:

- To rename the client device, click the Edit icon . The **Edit** page displays.
- On the **Edit** page, enter the name to create your own customized name or select a category listed in the drop-down menu.
- Click **Save**.

Figure 4-40 Device Rename page

Edit ×

Name

New_PC_Connection

Category

Desktop

Appliance

Audio

Camera

Save

END OF STEPS

Voice Configuration

4.37 Overview

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

Sub-menu	Procedure
Voice setting	4.38 "Configuring Voice Settings" (p. 140)
Voice status	4.39 "Viewing Voice Status" (p. 142)

4.38 Configuring Voice Settings

- 1
- Click **Voice**→**Voice Setting** in the left pane. The *Voice Setting* page displays.

Figure 4-41 Voice Setting page

Voice / Voice Setting

Outbound Proxy

Outbound Proxy Port

5060

Proxy Server

Proxy Server Port

5060

Registrar Server

Registrar Server Port

5060

User Agent Domain

User Agent Port

5060

Digit Map

*XX[#XX]*X#XXXXXXXXX(B8885010)E|0901XXXXXXXXXX|09001XXXXXXXXXX|0900X.T|09020|090[3-8][0-3]|0903[4-9]|0904[6-9]|090[5-8][4-9]|09090|0902[1-9]XXXXXXXXXX|0909[1-9]XX.T|XX.T

DTMF Mode

RFC2833

FAXT38

True

POTS line

Line1

Enable

Directory Number

Auth User Name

Auth Password

URI

Save

2

Configure the following parameters:

Table 4-25 Voice Setting parameters

Field	Description
Outbound Proxy	Enter the outbound proxy details.
Outbound Proxy Port	Enter the outbound proxy port.
Proxy Server	Enter the proxy server details.
Proxy Server Port	Enter the proxy server port.
Registrar Server	Enter the registrar server details.
Registrar Server Port	Enter the registrar server port.
User Agent Domain	Enter the user agent domain details.
User Agent Port	Enter the user agent port.
Digit Map	Enter the digit map value.
DTMF Mode	Select a DTMF mode from the list.
FAXT38	Select True or False from the list.
POTS Line	Select a POTS line from the list.
Enable	Select the toggle button to enable.
Directory Number	Enter the directory number.
Auth User Name	Enter the authentication username.
Auth Password	Enter the authentication password.
URI	Enter the URI.

3

Click **Save**.

END OF STEPS

4.39 Viewing Voice Status

1

Click **Voice**→**Voice status** in the left pane. The *Voice status* page displays the following information:

Figure 4-42 Voice status page

Voice / Voice status

POTS 1 registration status

POTS 1 line state

Disabled

Softswitch line 1

Telephone line 1 phone number

Line 1 registration error code

Line 1 registration error reason

User agent IP

Table 4-26 Voice status parameters

Field	Description
POTS 1 registration status	Indicates if POTS 1 is registered or not. If POTS 1 is registered, the status displays as Registered. The status is empty if no voice service is provisioned.
POTS 1 line state	Indicates the line in POTS 1. The default is Disabled.
Softswitch line 1	Proxy IP address; blank if the line is not registered.
Telephone line 1 phone number	Phone number configured for a telephone line 1.
Line 1 registration error code	SIP standard error code for the registration status; for example, 401, 403, 503. This field is blank if the registration is OK.
Line 1 registration error reason	SIP standard error reason for the register status. This field is blank if the registration is OK.
User agent IP	IP address of the user agent.

END OF STEPS

Security Configuration

4.40 Overview

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

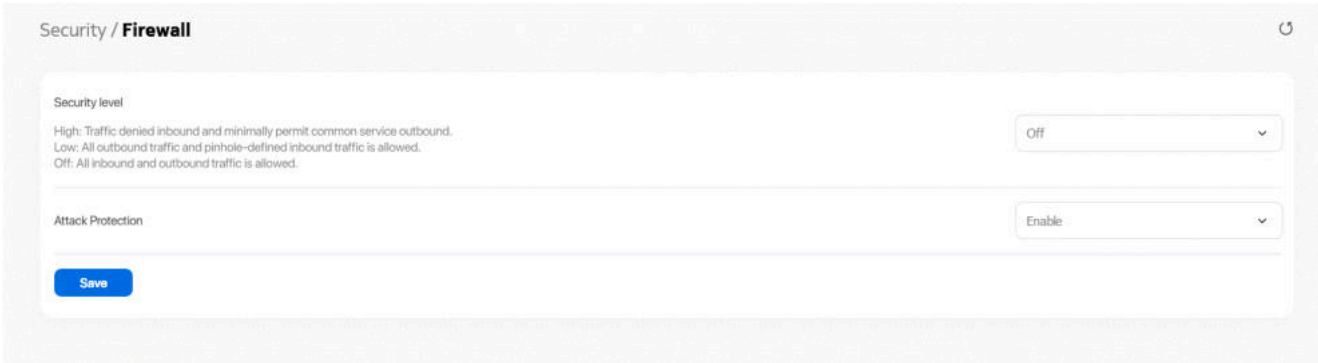
Sub-menu	Procedure
Firewall	4.41 "Configuring the Firewall" (p. 144)
MAC filter	4.42 "Configuring the MAC Filter" (p. 145)
IP filter	4.43 "Configuring the IP Filter" (p. 147)
URL filter	4.44 "Configuring the URL Filter" (p. 149)
Family profiles	4.45 "Configuring Family Profiles" (p. 151)
DMZ and ALG	4.46 "Configuring DMZ and ALG" (p. 157)
Access control	4.47 "Configuring Access Control" (p. 159)

4.41 Configuring the Firewall

1 _____

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

Figure 4-43 Firewall page



2 _____

Configure the following parameters.

Table 4-27 Firewall parameters

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

3

Click **Save**.

END OF STEPS

4.42 Configuring the MAC Filter

1

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

Figure 4-44 MAC filter page

Security / MAC filter

Ethernet

WiFi

SSID

SSID 1

Filter mode

Allowed

Enabled

Save

SSID

SSID 1

MAC address

Custom Settings

eg: D0:54:2D:00:00:00

Add

2

Configure the following parameters:

Table 4-28 MAC filter - Ethernet Interface parameters

Field	Description
Ethernet Interface	
MAC Filter mode	Select the MAC filter mode from the list: - Blocked - Allowed
LAN port	Select the toggle button to enable any of the LAN ports.
MAC address	Select a MAC address from the list or enter the MAC address in the text field.

3

Click **Save**.

4

Configure the following parameters:

Table 4-29 MAC filter - WiFi SSID parameters

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

5

Click **Save**.

END OF STEPS

4.43 Configuring the IP Filter

1

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

2

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

Figure 4-45 IP filter page

3

Configure the following parameters:

Table 4-30 IP filter parameters

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

Table 4-30 IP filter parameters (continued)

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

4

Click **Save**.

END OF STEPS

4.44 Configuring the URL Filter



Note: You can add up to 100 URL filters.

1

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

Figure 4-46 URL filter page

Security / URL filter

URL filter

Please select the type of filter and then configure the URL. Support upto 100 URL filters.

Enable URL filter

URL filter type

Block

URL address

Port number

The default port number is 80

Add filter +

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

2

Configure the following parameters:

Table 4-31 URL filter parameters

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

3

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

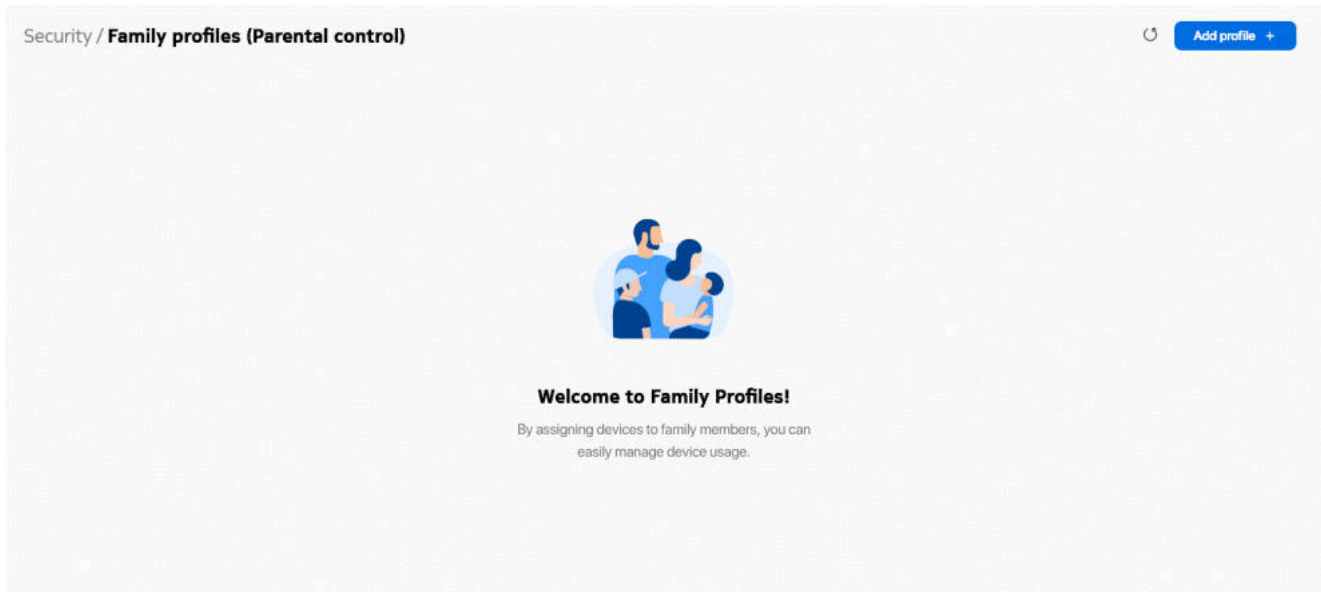
END OF STEPS

4.45 Configuring Family Profiles

1

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

Figure 4-47 Family profiles (Parental control) page



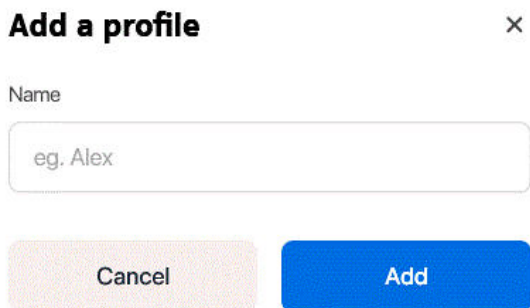
2

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

3

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

Figure 4-48 Add a profile page



The dialog box titled "Add a profile" has a close button (X) in the top right corner. It contains a text input field labeled "Name" with the placeholder text "eg. Alex". Below the input field are two buttons: "Cancel" and "Add".

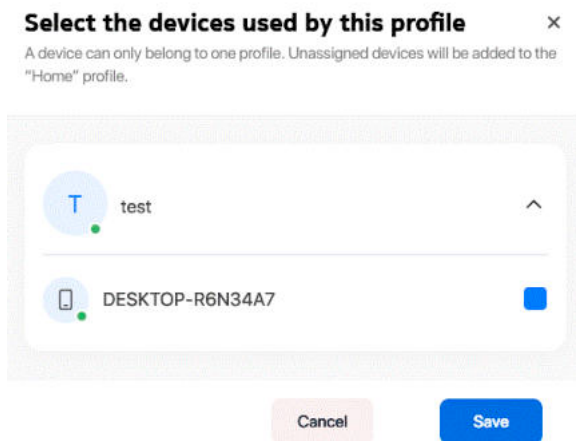
4

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



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

Figure 4-49 Assign devices to family profile



The dialog box titled "Select the devices used by this profile" has a close button (X) in the top right corner. Below the title is a note: "A device can only belong to one profile. Unassigned devices will be added to the 'Home' profile." The main area contains a list of devices. The first device is "test" with a blue circle icon containing a 'T' and a green status dot. The second device is "DESKTOP-R6N34A7" with a blue square icon and a checked checkbox. Below the list are "Cancel" and "Save" buttons.

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

Figure 4-50 Family profiles table

Security / Family profiles (Parental control)						⌂ Add profile +
Profile name	Device	Schedules	Bedtime	Blocked websites	Visit attempts (blocked sites)	
 Home Enabled	0	0	0	0	0	
 Client_1 Enabled	1	2	3	4	0	Delete
 Client_2 Enabled	1	1	2	1	0	Delete
 profile_3 Enabled	0	0	0	1	0	Delete

- 5
- Click a profile to configure parental control for the profile. A page displays the profile parameters.

Figure 4-51 Family profile configuration page

Security / Family profiles (Parental control)



test
Enabled

Assigned Devices
1 Device

Internet Access
Enabled for this profile

Schedules
None

Bedtime
None

Website blocking
Disabled

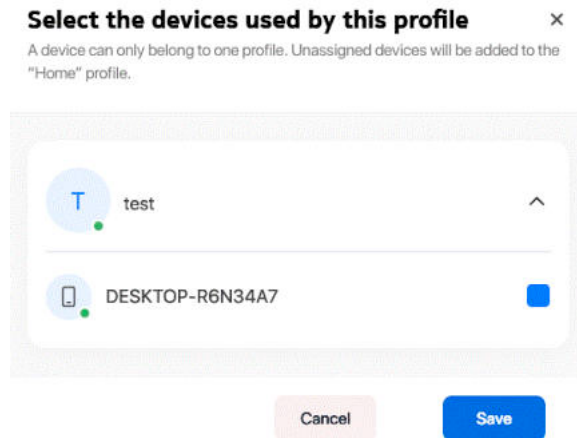
- 6
- Select the **Internet Access** toggle button to enable internet access.

Assign more devices

7

Assign more devices to the profile, if required:

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



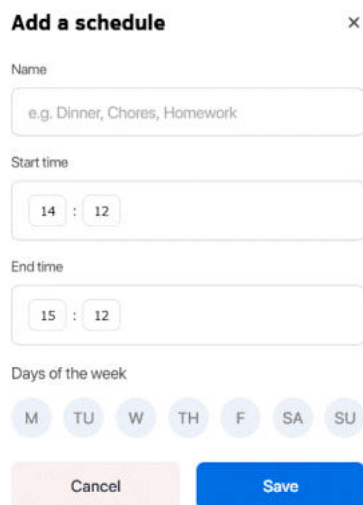
- b. Select the check box next to the device to assign to the profile.
- c. Click **Save**.

Configure and enable schedules

8

Configure schedules for the profile:

- a. In the profile page, click the edit icon  next to **Schedules** to create one or more schedules for the profile to set specific days and time slots when the Internet should be turned off.
- b. Click **Create Schedule**.
- c. In the *Add a schedule* page, configure the following:



Add a schedule ×

Name
e.g. Dinner, Chores, Homework

Start time
14 : 12

End time
15 : 12

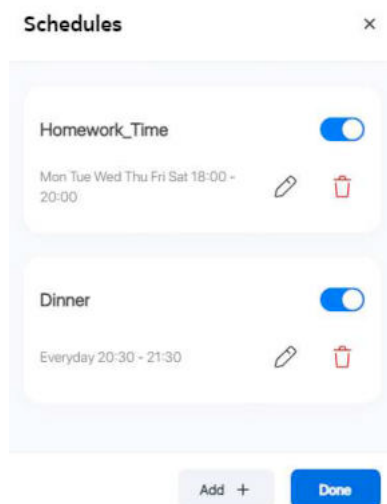
Days of the week
M TU W TH F SA SU

Cancel Save

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

9

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



Schedules ×

Homework_Time ☒

Mon Tue Wed Thu Fri Sat 18:00 - 20:00  

Dinner ☒

Everyday 20:30 - 21:30  

Add + Done

Configure and enable bedtime

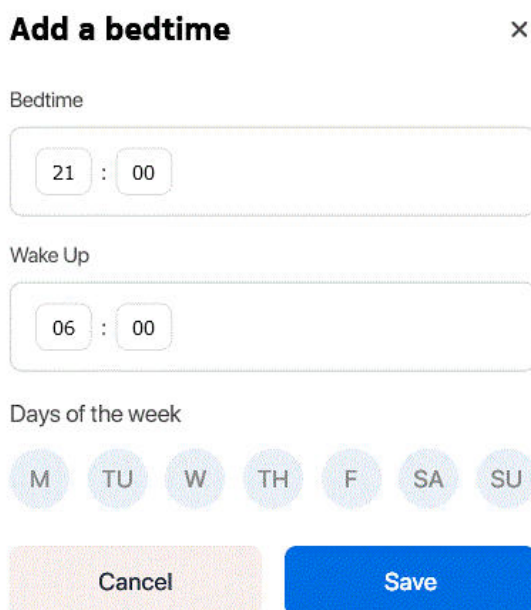
10

Configure bedtime for the profile:

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

Only one bedtime can be assigned per day.

- Click **Create Bedtime**.
- In the *Add a bedtime* page, configure the following:



- Select the Bedtime, Wake Up time, and select the days of the week on which the bedtime will be in effect.
 - Click **Save**. The bedtime is created and listed in the *Bedtime* page.
- In the *Bedtime* page, select the toggle button to enable the bedtime and click **Done**.

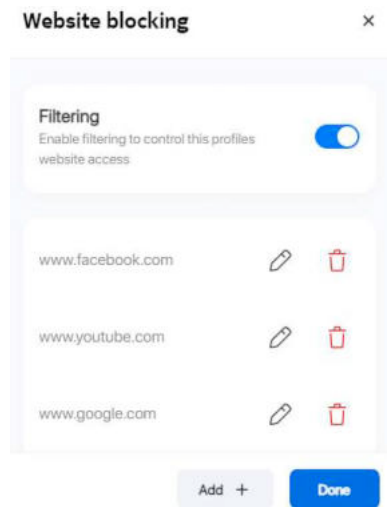
Configure website blocking

11

Configure website blocking for the profile:

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

- b. Click **Continue**.
- c. In the *Website blocking* page, perform the following:



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

END OF STEPS

4.46 Configuring DMZ and ALG

1

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

Figure 4-52 DMZ and ALG page

Security / DMZ and ALG

ALG Configuration

FTP

TFTP

SIP

H323

RTSP

L2TP

IPSEC

PPTP

Save

DMZ Configuration

WAN connection list

1_TR069_INTERNET_VOIP_R_VID_881

Enable DMZ

DMZ IP address

Custom Settings

0.0.0.0

Save

2

Configure the following parameters:

Table 4-32 ALG Configuration parameters

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

3

Click **Save**.

4

Configure the following parameters:

Table 4-33 DMZ Configuration parameters

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

5

Click **Save**.

END OF STEPS

4.47 Configuring Access Control

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



Note: ACL takes precedence over the firewall policy.

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

1

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

Figure 4-53 Access control page

Security / Access control

WAN LAN

WAN connection list: 1_TR069_INTERNET_R_VID_981

Enable trusted network: ☐

Protocol	Action
ICMP	Allow
Telnet	Deny
SSH	Deny
HTTP	Deny
TR-069	Allow
HTTPS	Deny

Save

Trusted network

Source IP start:

Source IP end:

Add +

2

Configure the following parameters:

Table 4-34 Access control parameters

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

3

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

4

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

Table 4-35 Trusted Network parameters

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

5

Click **Add +**.

END OF STEPS

Advanced Settings

4.48 Overview

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

Sub-menu	Procedure
Port forwarding	4.49 "Configuring Port Forwarding" (p. 163)
Port triggering	4.50 "Configuring Port Triggering" (p. 164)
DDNS	4.51 "Configuring DDNS" (p. 165)
NTP	4.52 "Configuring NTP" (p. 166)
UPNP and DLNA	4.53 "Configuring UPNP and DLNA" (p. 168)

4.49 Configuring Port Forwarding

1

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

Figure 4-54 Port forwarding page

Advanced settings / Port forwarding

WAN port

-

LAN port

-

Internal client

Custom Settings

Protocol

TCP

WAN connection list

2_INTERNET_R_VID_2101

Save

2

Configure the following parameters:

Table 4-36 Port forwarding parameters

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

3

Click **Save**.

END OF STEPS

4.50 Configuring Port Triggering

1

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

Figure 4-55 Port triggering page

Advanced settings / **Port triggering** Save

Open port -

Triggering port -

Expiration time
Range: 1-999999 secs

Open protocol

Trigger protocol

WAN connection list

2

Configure the following parameters:

Table 4-37 Port triggering parameters

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

3

Click **Save**.

END OF STEPS

4.51 Configuring DDNS

1

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

Figure 4-56 DDNS page

Advanced settings / DDNS

WAN connection list

1_TR069_INTERNET_VOIP_R_VID_681

Enable DDNS

ISP

DynDNS.org

Domain Name

Username

Password

Save

2

Configure the following parameters:

Table 4-38 DDNS parameters

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

3

Click **Save**.

END OF STEPS

4.52 Configuring NTP

1

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

Figure 4-57 NTP page

Advanced settings / NTP

Enable NTP service

Current date & time

01/14/1970 03:08:55 AM

Primary Time Server

Custom Settings

Secondary Time Server

None

Third time server

None

Interval time

0

0,15-259200 secs

Time zone

(GMT-00:00) Casablanca, Monrovia

Save

2

Configure the following parameters:

Table 4-39 NTP parameters

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

3

Click **Save**.

END OF STEPS

4.53 Configuring UPNP and DLNA

1

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

Figure 4-58 UPNP and DLNA page



2

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

3

Select the **IGD version** from the drop down list, consisting of the options : v1 and v2.

4

Click **Save**.

END OF STEPS

Maintenance

4.54 Overview

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

Sub-menu	Procedure
Change password	4.55 "Configuring the Password" (p. 169)
Backup and restore	4.56 "Backing Up the Configuration" (p. 171) 4.57 "Restoring the Configuration" (p. 172)
Firmware upgrade	4.58 "Upgrading Firmware" (p. 173)
LOID config	4.59 "Configuring LOID" (p. 175)
SLID configuration	4.60 "Configuring SLID" (p. 176)
Diagnostics	4.61 "Diagnosing WAN Connections" (p. 178)
Log	4.62 "Viewing Log Files" (p. 180)
Delta CFG tool	4.63 "Generating a delta configuration file" (p. 182)

4.55 Configuring the Password

Operators can allow users to set passwords with or without password rules.

The password rules are different based on each operator's configuration.

Password rule configuration can be any or all of these as well as additional added rules. The following password rules can be applied:

- First character cannot be special one.
- Password can only contain numbers, letters and special character !#+, -./:=@_
- Password should be at most 63 characters.
- At least two character classes are required.
- Password should be at least 8 characters.
- The same character can not appear consecutively 8 times.

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:

- First character cannot be special one
- Password can only contain numbers, letters and special character !#+, -./:=@
- The password should use at least one uppercase letter, one lowercase letter, one number, and one special character
- Password should be at least 8 characters

- Password should be at most 24 characters
- The same character cannot appear consecutively 8 times

1

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

Figure 4-59 Change password page

Maintenance / **Change password** 

Original password

New password

☐ At least 1 number

☐ At least 1 lower case letter

☐ At least 1 upper case letter

☐ At least 8 characters

☐ At least 1 special character (only !#+, -./:=@_)

☐ No consecutive 8 identical characters

☐ The first character must not be special

☐ No more than 24 characters

Repeat new password

Password hint

For better security, avoid using your password or any part of it in the password hint.

Save

2

Configure the following parameters:

Table 4-40 Change password parameters

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

3

Click **Save**.

END OF STEPS

4.56 Backing Up the Configuration

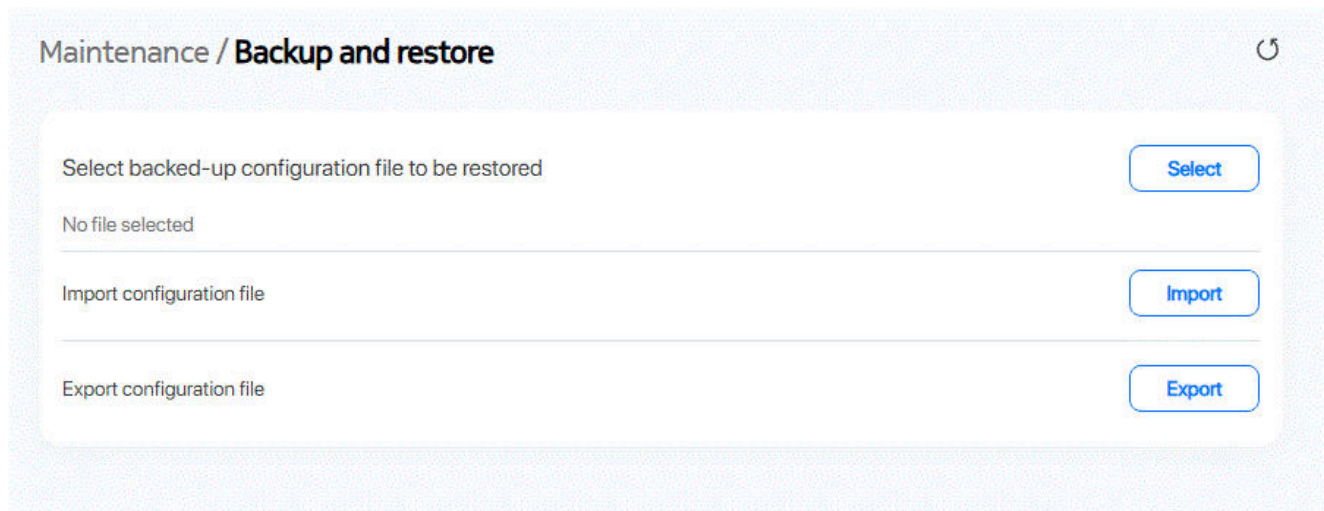
1

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



Note: If the ACS Lock is enabled, Backup and Restore option is not displayed in the left pane and the Backup and Restore WebGUI screen is not accessible to all the users until the lock is disabled.

Figure 4-60 Backup and restore page



2

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

END OF STEPS

4.57 Restoring the Configuration

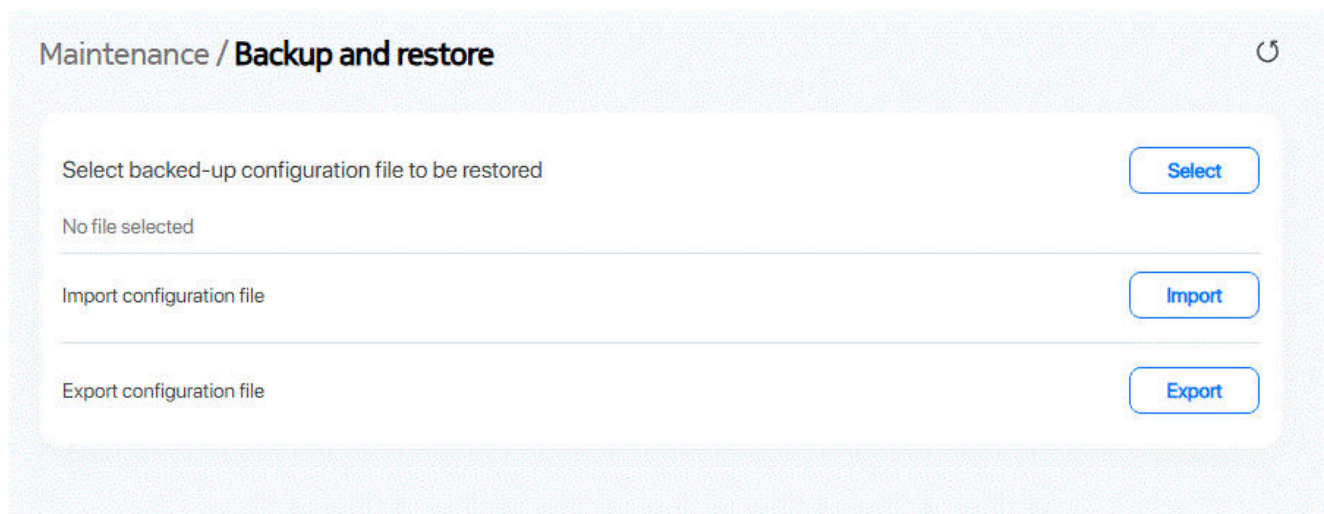
i **Note:** Ensure that you have a previously backed-up configuration file.

1

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

i **Note:** If the ACS Lock is enabled, Backup and Restore option is not displayed in the left pane and the Backup and Restore WebGUI screen is not accessible to all the users until the lock is disabled.

Figure 4-61 Backup and restore page



2

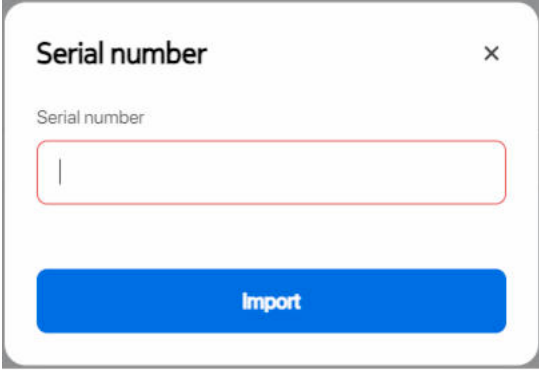
Click **Select** and select the previously backed-up configuration file.

3

Click **Import** to import the configuration file created in [4.56 “Backing Up the Configuration”](#) (p. 171) and restore the ONT to the backed-up configuration.

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

Figure 4-62 Backup and restore: Serial number



- b. If you enter an invalid serial number, the back up fails and an error message is displayed.
- c. The backup cannot be restored for the configuration files from a different ONT variant, OPID, or different release prior to Release 2402.

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

END OF STEPS

4.58 Upgrading Firmware

1

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



Note: If the ACS Lock is enabled, Firmware Upgrade option is not displayed in the left pane and the Firmware Upgrade WebGUI screen is not accessible to all the users until the lock is disabled.

Figure 4-63 Firmware upgrade page

The screenshot shows the 'Maintenance / Firmware upgrade' page. At the top right is a refresh icon. The main area contains a file selection section with a 'Select file' label, a 'No file selected' status, and a blue 'Select' button. Below this is a blue 'Upgrade' button. At the bottom is an 'Upgrade status' section with a horizontal line for status updates.

- 2 _____
Click **Select** and select the file for firmware upgrade.
- 3 _____
Click **Upgrade** to upgrade the firmware. The status displays in the *Upgrade status* panel. The device reboots after firmware upgrade and displays the login page.

Figure 4-64 Example of upgrade status messages

```
Upgrade status
Upgrade Done!
-----
get_cert_type_from_buildinfo NCG
Image check pass, everything is OK
Saving config files...
Performing system upgrade...
Upgrade completed
4
mkdir: can't create directory '/configs/swdl': File exists
sh: using fallback suid method
sync: using fallback suid method
date: using fallback suid method
Upgrade ok, Rebooting...
```

END OF STEPS

4.59 Configuring LOID

1

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

Figure 4-65 LOID config page

Maintenance / LOID config

LOID authentication

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

LOID

Password

Save

- 2
- Configure the following parameters:

Table 4-41 LOID config parameters

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

- 3
- Click **Save**.

END OF STEPS

4.60 Configuring SLID

- 1
- Click **Maintenance**→**SLID configuration** in the left pane. The *SLID configuration* page displays.

Figure 4-66 SLID configuration page

Maintenance / SLID configuration

Current SLID44454641554C54

Enter new SLID

SLID mode

Maximum of 20 Hex numbers allowed.

HEX Mode

Save

2

Configure the following parameters:

Table 4-42 SLID configuration parameters

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

3

Click **Save**.

END OF STEPS

4.61 Diagnosing WAN Connections

- 1
- Click **Maintenance**→**Diagnostics** in the left pane. The *Diagnostics* page displays.

Figure 4-67 Diagnostics page

Maintenance / **Diagnostics**

WAN

Protocol

IPv4

WAN connect list

LAN/WAN Interface

IP or domain name

Ping

Traceroute

Ping try times

4

1-1000

Packet length

64

64-1500

Max number of trace hops

30

1-255

Start test

Cancel

- 2
- Configure the following parameters.

Table 4-43 Diagnostics parameters

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

Table 4-43 Diagnostics parameters (continued)

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

3

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

Figure 4-68 Example of ping results

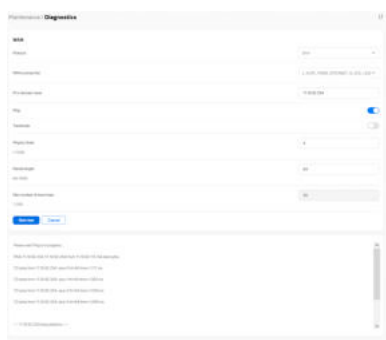
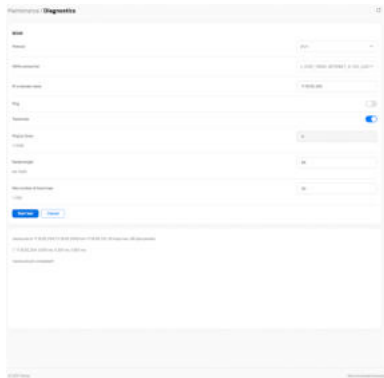


Figure 4-69 Example of traceroute results



END OF STEPS

4.62 Viewing Log Files

1

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

Figure 4-70 Log page

Maintenance / Log

Save

Export log

Writing level

Notice

Reading level

Error

Manufacturer:ALCL

ProductClass:G-1427G-A

SerialNumber:ALCLFF0F1505

HWVer:3TN01705AAAA

SWVer:3TN01913HJML76

IP:192.168.1.254

[crit] <130>1 2025-11-10T10:15:06.043188+00:00 OpenWrt syslog - - - restarting ndk_udhcpd due to config changes, flag=1

[crit] <130>1 2025-11-10T10:15:10.159679+00:00 OpenWrt syslog - - - restarting ndk_udhcpd due to config changes, flag=0

[crit] <130>1 2025-11-10T10:16:14.518366+00:00 AONT syslog - - - restarting ndk_udhcpd due to config changes, flag=1

[crit] <130>1 2025-11-10T10:16:18.420516+00:00 AONT syslog - - - restarting ndk_udhcpd due to config changes, flag=0

[err] <131>1 2025-11-10T15:39:21.987808+00:00 AONT syslog - - -

InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.Line.1.VoiceProcessing. RTS failed, ret=-1

[err] <131>1 2025-11-10T15:39:57.726047+00:00 AONT web_customization_web_app.cgi - - - [capability-webapp]: Selcting the object ONT

Finally from [get_object_to_be_selected_for_hw]

2

Configure the following parameters:

Table 4-44 Log parameters

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

3

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

4

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

END OF STEPS

4.63 Generating a delta configuration file

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

1

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

- To generate a delta CFG file without merging with a previous CFG file, go to [Step 2](#).
- To merge delta CFG file, go to [Step 3](#).

Figure 4-71 Delta CFG Tool page

Maintenance / **Delta CFG tool**

Please double confirm if you are trying to modify the parameters in Delta CFG below, such as the WiFi SSID name or password. These are usually controlled by the end user, so changing these parameters may impact their usage.

Merge Delta CFG file

No file selected **Select file** **Start recording**

This will include the content of the Delta CFG file you select to the new one.
Pay attention to the dynamic objects when using this option.

Export Delta CFG file **Export**

2

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

- Click **Start recording**.
- Perform the required configuration such as adding/deleting WAN connection, changing WAN connection VLAN ID, changing ACS URL and so on. If reboot is needed after modifying a parameter, for example, disabling the DNS Proxy in the DNS page, wait until the ONT is rebooted and continue with the configuration.
- Click **Stop recording** to stop recording.
- Click **Export** to download the delta CFG file to the local computer. The delta CFG file is in plain text format with the filename *delta_config_result file*. If required, rename the file and convert the file to .tar format before downloading it to the ONT .



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

3

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

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

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



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

- b. Click **Start recording**.
- c. Perform the required configuration such as adding/deleting WAN connection, changing WAN connection VLAN ID, changing ACS URL and so on. If reboot is needed after modifying a parameter, for example, disabling the DNS Proxy in the DNS page, wait until the ONT is rebooted and continue with the configuration.
- d. Click **Stop recording** to stop recording.
- e. Click **Export** to download the delta CFG file to the local computer. The delta CFG file is in plain text format with the filename *delta_config_result file*. If required, rename the file and convert the file to .tar format before downloading it to the ONT .



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

END OF STEPS

Troubleshooting

4.64 Troubleshooting counters

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

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

1

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

Figure 4-72 Troubleshooting counters page

Troubleshooting / Troubleshooting counters

WAN connection list

1_TROES_INTERNET_R_VID_981

WAN status

Up

Troubleshoot counters

UIS throughput snapshot

Take snapshot

DS throughput snapshot

Take snapshot

UIS packet loss

0

DS packet loss

0

Latency

Latency test

DNS response time

DNS response test

Port mirrors

Source Port

WAN

Destination Port

LAN1

Direction

Bi-directional

Status

Enable

Save

2

Configure the following parameters:

Table 4-45 Troubleshooting counters parameters

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

3

Click **Save**.

END OF STEPS

4.65 Speed Test

1

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

Figure 4-73 Speed test page

Troubleshooting / Speed test

Save

TR-143 server settings

Upload test server URL

URL Ex.http://upload.server.com/test

Number of upload connections

4

Download test server URL

URL Ex.http://download.server.com/download.fil

Number of download connections

4

Host

IP address Ex.192.168.50.32

Test mode

File based

Upload file size

File size in MB Ex.1000

Results

Upload speed

-

Download speed

-

Latency

0

Start test

Table 4-46 Speed test parameters

Field	Description
TR-143 server settings	
Upload test server URL	Enter the Upload test server URL.

Table 4-46 Speed test parameters (continued)

Field	Description
Number of upload connections	Enter the Number of upload connections.
Download test server URL	Enter the Download test server URL.
Number of download connections	Enter the Number of download connections.
Host	Enter Host.
Test mode	Select a Test mode: • Time based • File based
Upload file size	Displays the file size in MB. This parameter is visible only if the Test mode is File Based .
Duration	Displays the time duration in sec. This parameter is visible only if the Test mode is Time Based .
Results	
Upload speed	Displays the upload speed.
Download speed	Displays the download speed.
Latency	Displays the latency.

2

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

3

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

END OF STEPS

5 ONT configuration file over OMCI

5.1 Overview

5.1.1 Purpose

5.1.2 Contents

5.1 Overview	191
5.2 Purpose	191
5.3 Supported configuration file types	191
5.4 ONT configuration file over OMCI	194

5.2 Purpose

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

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



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

5.3 Supported configuration file types

[Table 5-1, “Supported configuration files” \(p. 192\)](#) describes the configuration file types that are supported from Nokia ONT R05.02.00 and later.

Table 5-1 Supported configuration files

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

Table 5-1 Supported configuration files (continued)

File Index	Description	Details	Supported ONTs/DPU
WebGUI (unified)	WEB, example: WEBXXXXVER	AdminUser.json – WebGUI privilege customization file for the admin user account NormalUser.json – WebGUI privilege customization file for the end user account logo.svg – The operator logo that will be shown in the WebGUI in the login page and side menu CSS file – The operator brand color palette file to customize the WebGUI color theme Font file – The operator brand font file to customize the WebGUI font style	All Nokia GPON and 10 GPON ONT.

5.3.1 Filename conventions

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

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

ABCXXXXVER

where

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

XXXX is the operator ID

For PRE and CFG, a valid operator ID is required

For XML and GFT, any characters may be used

VER is the file version (from 001 to 999)

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

5.3.2 Download configuration file

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

ONT type	Legacy method download		Zero management download	
	PRE file	CFG file	PRE file	CFG file
MTK (example: G240WF)	=	✓	✓	✓

5.4 ONT configuration file over OMCI



WARNING

Equipment Damage

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

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

5.4.1 Configuring an ONT using a configuration file via legacy method

1

Upload the ABCXXXXVER TAR file to the /ONT/ directory in the OLT.
A maximum of 250 files can be kept in the OLT file system.

2

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

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

Please note:

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

Examples



Note: X can be 1 or 2 unless specified:

- If **pland-cfgfileX= Disabled** and **dnload-cfgfileX= Disabled**,
no file is downloaded to the ONT.
- If **pland-cfgfileX=FILENAME1** and **dnload-cfgfileX= Disabled**,
FILENAME1 is downloaded and FILENAME1 is made active. An ONT reboot is required.
- If **pland-cfgfileX=Disabled** and **dnload-cfgfileX= FILENAME2**,
FILENAME2 is downloaded and FILENAME2 is made passive. An ONT reboot is not required.
- If **pland-cfgfileX=FILENAME3** and **dnload-cfgfileX= FILENAME4**, the OLT reports an error because the filenames are not the same.
- Configure equipment interface **pland-cfgfile1=XMLXXXXXX1** and **dnload-cfgfile1 XMLXXXXXX1**
Configure equipment interface **pland-cfgfile2=XMLXXXXXX2** and **dnload-cfgfile2 XMLXXXXXX2**

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

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

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

END OF STEPS

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

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

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

5.4.2 Configuring an ONT using a configuration file via OMCI

1

Generate the TAR file to be uploaded to the OLT.

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

- a. On a Linux platform, rename the raw configuration file to adhere to the naming convention, as described in section [5.3 "Supported configuration file types" \(p. 191\)](#).
- b. Tar the **ABCXXXXXVER** raw configuration file:

```
tar -cf ABCXXXXXVER.tar ABCXXXXXVER
```

Where

ABCXXXXXVER

Is the name of the file created in step i.

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

- c. Rename **ABCXXXXXVER** to **ABCXXXXXVER.org**
- d. Remove the ".tar" extension from **ABCXXXXXVER.tar** file.

2

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

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

3

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

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

Please note:

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

Examples



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

- a. If **pland-cfgfileX= Disabled** and **dnload-cfgfileX= Disabled**
no file is downloaded to the ONT.
- b. If **pland-cfgfileX=FILENAME1** and **dnload-cfgfileX= Disabled**
FILENAME1 is downloaded and FILENAME1 is made active. An ONT reboot is required.
- c. If **pland-cfgfileX=Disabled** and **dnload-cfgfileX= FILENAME2**
FILENAME2 is downloaded and FILENAME2 is made passive. An ONT reboot is not required.
- d. If **pland-cfgfileX=FILENAME3** and **dnload-cfgfileX= FILENAME4**, the OLT reports an error because the filenames are not the same.
- e. Configure equipment interface **pland-cfgfile1=XMLXXXXXX1** and **dnload-cfgfile1 XMLXXXXXX1**
Configure equipment interface **pland-cfgfile2=XMLXXXXXX2** and **dnload-cfgfile2 XMLXXXXXX2**
Although the OLT permits the above two steps without reporting an error, Nokia does not recommend executing them, because the ONT may exhibit unexpected behavior.
- f. If **pland-cfgfileX=Auto** and **dnload-cfgfileX= Auto**
The OLT will download the XML file from "sw-ctr-list" (**configure equipment ont sw-ctrl**)

END OF STEPS

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

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

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

5.4.3 Configuring ONT using a Combined Customized Software Package

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



Note:

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

1

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

2

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

3

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

END OF STEPS

5.4.4 ONT configuration file over ACS or USP server

1

Refer to the section 7 Configure file update in document *3HH-10684-9012-TCZZA-16 TR069 Service Configurations User Guide TR098*.

2

Refer to USP Service Configurations User Guide *3HH-10684-9012-TCZZA-16 TR069 Service Configurations User Guide TR098*.

END OF STEPS

6 Environmental and Regulatory Compliance

6.1 Overview

6.1.1 Purpose

This chapter provides information about the environmental and regulatory compliance.

6.1.2 Contents

6.1 Overview	199
6.2 For EU regulation market	199

6.2 For EU regulation market

The Products are manufactured by Nokia Solutions and Networks Oy and imported by Nokia Solutions and Networks Oy, Karakaari 7,02610 Espoo, Finland.

Nokia is a registered trademark of Nokia Corporation.

Nokia Solutions and Networks Oy declares that the device is in compliance with Radio Equipment Directive 2014/53/EU(for device with WiFi); Low Voltage Directive 2014/35/EU(for device without WiFi); EMC Directive 2014/30/EU(for device without WiFi); RoHS Directive 2011/65/EU; Eco-design Directive 2009/125/EC and EAA - Directive 2019/882/EU.

6.2.1 RoHS (Restriction of Hazardous Substances Directive)

Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (European Union (EU) Directive 2011/65/EU and as amended).

Nokia Solutions and Networks Oy declares that the device is in compliance with the EU RoHS Directive.

6.2.2 WEEE (End of Life Collection and Treatment)

In the European Union, the below label indicates that this device should not be disposed of with household waste. It should be deposited in an appropriate facility to enable recovery and recycling.

Figure 6-1 Recycling/take back/disposal of product symbol



The device is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. Electronic products bearing or referencing the WEEE mark shown above, 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.

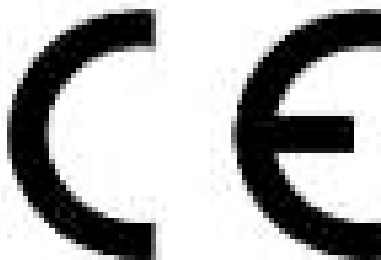
Due to materials that may be contained in the Product, such as heavy metals or batteries, the environment and human health may be negatively impacted as a result of inappropriate disposal.

At the end of their life, the Products are subject to the applicable local legislations that implement the European Directive 2012/19/EU on 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 Products bearing the logo above at the end of their useful life, or Products displaced by Nokia equipment offers. The equipment can be disposed at electronic waste collection points or to stores that sell electronics.

For more information regarding the requirements for recycling/disposal of the Product you may contact Nokia or your service provider.

6.2.3 Simplified EU Declaration of Conformity



Hereby, Nokia Solutions and Networks Oy declares that the device is in compliance with:

- Radio Equipment Directive 2014/53/EU; (for device with WiFi)
- Low Voltage Directive 2014/35/EU; (for device without WiFi)
- EMC Directive 2014/30/EU; (for device without WiFi)
- RoHS Directive 2011/65/EU
- Eco-design Directive 2009/125/EC
- Directive European Accessibility Act - 2019/882/EU

In accordance with Article 10.8(a) and 10.8(b) of the RED, the below table provides information on the frequency bands used and the maximum radio frequency transmit power of the Products with WiFi.

Table 6-1 Frequency bands and transmit power

Radio Frequency Maximum	Transmit Power
2400 – 2483.5 MHz	100mW EIRP
5150 – 5350 MHz	200mW EIRP
5470 – 5725 MHz	1000mW EIRP
5925 – 6425 MHz	200mW EIRP

The full text of the EU declaration of conformity is available at Declaration of conformity | Nokia.com.

6.2.4 Specific precautions for EMC Warning

The device is compliant with Class B of EN 55032. In a residential environment this equipment may cause radio interference. The Products are tested to the requirements of EN 55032 (Emissions) and EN 55035 (immunity).

There are no specific precautions which must be taken in order to comply with the requirements of Directive 2014/30/EU Essential Requirements in Section 1 of Annex I. In addition, the Products are further tested to ensure spurious emissions are within the specified limits, as well as meeting the requirements for adaptivity, which mitigates against problems caused by co-location with other

wireless products. The Products are not subject to the requirements in Section 2 of Annex I of Directive 2014/30/EU for fixed installations.

6.2.5 Restriction used in European for devices with WiFi

The device with WiFi could be used with a separation distance of 20 cm to the human body.

The device with WiFi is restricted to indoor use only when operating in the 5150 to 5350 MHz, 5945 to 6425 MHz (LPI) frequency range, see [Table 6-2, "Applicable country codes" \(p. 201\)](#) regarding indoor use in the 5150 to 5350 MHz, 5945 to 6425 MHz (LPI) frequency range for applicable country codes.

Table 6-2 Applicable country codes

AT	BE	BG	HR	NO
CY	CZ	DK	EE	IS
FI	FR	DE	EL	LI
HU	IE	IT	LV	CH
LT	LU	MT	NL	TR
PL	PT	RO	SK	
SI	ES	SE	UK (NI)	