Nokia WiFi Gateway 3

G-240W-E WiFi Gateway

Nokia WiFi Gateway 3 Product Guide

3FE-47464-AAAA-TCZZA

Issue: 01

1 Preface

This preface provides general information about the documentation set for Gateway 3 equipment.

1.1 Scope

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

1.2 Audience

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

1.3 Required knowledge

The reader must be familiar with general telecommunications principles.

1.4 Acronyms and initialisms

The expansions and optional descriptions of most acronyms and initialisms appear in the glossary (3FE-47157-AAAA-TCZZA).

1.5 Assistance and ordering phone numbers

Nokia provides global technical support through regional call centers. Phone numbers for the regional call centers are available at the following URL: http://support.alcatel-lucent.com. If this link does not work, copy and paste it directly into your web browser.

For ordering information, contact your Nokia sales representative.

1.6 Nokia quality processes

Nokia's quality practices are in compliance with TL 9000 requirements. These requirements are documented in the Fixed Networks Quality Manual 3FQ-30146-6000-QRZZA. The quality practices adequately ensure that technical requirements and customer end-point requirements are met. The customer or its representatives may be allowed to perform on-site quality surveillance audits, as agreed upon during contract negotiations

1.7 Safety information

For safety information, see the appropriate safety guidelines chapter.

1.8 Documents

Documents are available using ALED or OLCS.

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

1	Navigate to http://support.alcatel-lucent.com and enter your user name and password. If you are a new user and require access to this service, please contact your Nokia sales representative.
2	From the Technical Content for drop-down menu, choose the product.
3	Click on Downloads: Electronic Delivery.
4	Choose Documentation from the drop-down menu and click Next.
5	Select the image from the drop-down menu and click Next.
6	Follow the on-screen directions to download the file.

Procedure 2 To access individual documents

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

1. Navigate to http://support.alcatel-lucent.com and enter your user name and password. If you are a new user and require access to this service, please contact your Nokia sales representative.
2. From the Technical Content for drop-down menu, choose the product.
3. Click on Manuals and Guides to display a list of customer documents by title and part number. You can filter this list using the Release drop-down menu.
4. Click on the PDF to open or save the file.

1.9 Special information

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

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

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

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

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

1.9.1 Procedures with options or substeps

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

Procedure 3 Example of options in a procedure

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

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

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

2 You must perform this step.

Procedure 4 Example of required substeps in a procedure

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

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

- **i** This is the first substep.
- **ii** This is the second substep.
- **iii** This is the third substep.

2 You must perform this step.

1.10 Multiple PDF document search

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

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

Procedure 5 To search multiple PDF files for a common term

1 Open Adobe Acrobat Reader.

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

3 Enter the search criteria.

4 Click on the All PDF Documents In radio button.

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

6 Click on the Search button.

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

Table of contents

List of figures

List of tables

2 ANSI CPE safety guidelines

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

2.1 Safety instructions

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

2.1.1 Safety instruction boxes in customer documentation

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

The following is an example of the Danger box.

Danger — Possibility of personal injury.

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

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

The following is an example of the Warning box.

Warning 1 — Possibility of equipment damage.

Warning 2 — Possibility of data loss.

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

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

The following is an example of the Caution box.

Caution 1 — Possibility of service interruption.

Caution 2 — Service interruption.

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

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

The following is an example of the Note box.

Note — Information of special interest.

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

2.1.2 Safety-related labels

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

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

Table 1 **Safety labels**

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

Figure 1 shows a sample safety label located on the bottom of the Gateway 3 (G-240W-E).

Figure 1 **Sample safety label**

2.2 Safety standards compliance

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

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

2.2.1 EMC, EMI, and ESD standards compliance

The customer premises equipment complies with the following requirements:

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

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

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

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

2.2.2 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the Gateway 3 (G-240W-E) devices are in compliance with the essential requirements and other relevant provisions of Directive 2009/125/EC together with Commission Regulation (EC) No 1275/2008 and Commission Regulation (EC) No 801/2013.

The Gateway 3 (G-240W-E) devices qualify as high network availability (HiNA) equipment. Since the main purpose of Gateway 3 (G-240W-E) devices is to provide network functionality with HiNA 7 days/24 hours, the modes Off/Standby, Power Management, and Networked Standby are inappropriate.

For information about the type and number of network ports, see “Gateway 3 (G-240W-E) interfaces and interface capacity” in chapter 5.

For information about power consumption, see “Gateway 3 (G-240W-E) detailed specifications” in chapter 5.

2.2.3 FCC statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

2.2.4 FCC Radiation Exposure Statement

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

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

1 this device may not cause harmful interference, and

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

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

2.2.5 Resistibility requirements compliance

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

2.3 Electrical safety guidelines

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

Gateway 3 (G-240W-E) devices are compliant with the following standards

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

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

2.3.1 Power supplies

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

2.3.2 Cabling

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

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

3 ETSI CPE safety guidelines

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

3.1 Safety instructions

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

3.1.1 Safety instruction boxes

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

The following is an example of the Danger box.

Danger — Possibility of personal injury.

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

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

The following is an example of the Warning box.

Warning 1 — Possibility of equipment damage.

Warning 2 — Possibility of data loss.

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

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

The following is an example of the Caution box.

Caution 1 — Possibility of service interruption.

Caution 2 — Service interruption.

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

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

The following is an example of the Note box.

Note — Information of special interest.

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

3.1.2 Safety-related labels

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

Table 2 provides sample safety labels on the customer premises equipment.

Table 2 **Safety labels**

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

3.2 Safety standards compliance

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

3.2.1 EMC, EMI, and ESD compliance

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

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

3.2.2 Equipment safety standard compliance

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

Table 3 provides examples of the text in the various CPE safety labels.

Table 3 **Safety labels**

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

Figure 2 shows a sample safety label located on the bottom of the Gateway 3 (G-240W-E).

Figure 2 **Sample safety label**

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

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

3.2.3 Environmental standard compliance

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

3.2.4 Resistibility requirements compliance

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

3.2.5 Acoustic noise emission standard compliance

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

3.3 Electrical safety guidelines

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

Note 1 — The devices comply with the U.S. National Electrical Code. However, local electrical authorities have jurisdiction when there are differences between the local and U.S. standards.

Note 2 — The devices comply with BS EN 61140.

3.3.1 Power supplies

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

3.3.2 Cabling

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

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

4 ETSI environmental and CRoHS guidelines

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

4.1 Environmental labels

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

4.1.1 Overview

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

4.1.2 Environmental related labels

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

4.1.2.1 Products below Maximum Concentration Value (MCV) label

Figure 3 shows the label that indicates a product is below the maximum concentration value, as defined by standard SJ/T11363-2006 (Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products). Products with this label are recyclable. The label may be found in this documentation or on the product.

Figure 3 **Products below MCV value label**

18986

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

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

Figure 4 **Products above MCV value label**

18985

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

4.2 Hazardous Substances Table (HST)

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

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

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

4.3 Other environmental requirements

Observe the following environmental requirements when handling the P-OLT or CPE

4.3.1 CPE environmental requirements

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

4.3.2 Transportation

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

4.3.3 EU RoHS

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

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

4.3.4 End-of-life collection and treatment

Electronic products bearing or referencing the symbol shown in Figure 5, when put on the market within the European Union (EU), shall be collected and treated at the end of their useful life, in compliance with applicable EU and local legislation. They shall not be disposed of as part of unsorted municipal waste. Due to materials that may be contained in the product, such as heavy metals or batteries, the environment and human health may be negatively impacted as a result of inappropriate disposal.

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

Figure 5 **Recycling/take back/disposal of product symbol**

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

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

In compliance with legal requirements and contractual agreements, where applicable, Nokia will offer to provide for the collection and treatment of Nokia products bearing the logo shown in Figure 5 at the end of their useful life, or products displaced by Nokia equipment offers. For information regarding take-back of equipment by Nokia, or for more information regarding the requirements for recycling/disposal of product, contact your Nokia account manager or Nokia take back support at sustainability.global@nokia.com.

5 Gateway 3 (G-240W-E) unit data sheet

5.1 Gateway 3 (G-240W-E) part numbers and identification

Table 4 provides part numbers and identification information for the Gateway 3 (G-240W-E).

Table 4 **Identification of Gateway 3 (G-240W-E)**

Ordering part number	Provisioning number	Description	CLEC	CPR	ECI/ Bar code
3FE 47358 AA	3FE 47464 AA	Nokia WiFi Gateway 3 (G-240W-E), GPON residential gateway ONT with 2 POTS ports, 4 GE UNI, 5G Wi-Fi, and 3x3 2.4G Wi-Fi. Includes two USB 2.0 Type A ports and a 12V US 2-pin plug, wall-mounted power supply variant with a barrel-type DC connector.	BVMHX00ARA	N70GRC	472780
3FE 47358 BA	3FE 47464 BA	Nokia WiFi Gateway 3 (G-240W-E), GPON residential gateway ONT with 2 POTS ports, 4 GE UNI, 5G Wi-Fi, and 3x3 2.4G Wi-Fi. Includes two USB 2.0 Type A ports and a 12V EU 2-pin plug, wall-mounted power supply variant with a barrel-type DC connector.	—	—	—

(1 of 2)

Ordering part number	Provisioning number	Description	CLEC	CPR	ECI/ Bar code
3FE 47358 CA	3FE 47464 BA	Nokia WiFi Gateway 3 (G-240W-E), GPON residential gateway ONT with 2 POTS ports, 4 GE UNI, 5G Wi-Fi, and 3x3 2.4G Wi-Fi. Includes two USB 2.0 Type A ports and a 12V UK 3-pin plug, wall-mounted power supply variant with a barrel-type DC connector.	—	—	—

(2 of 2)

Table 5 provides power supply ordering information for the Gateway 3 (G-240W-E). The UPS connector is a reserved interface. The UPS adapter is specified by Nokia. The maximum overload rating should not exceed 8A, 100W.

Table 5 **Gateway 3 (G-240W-E) power supply ordering information**

Gateway 3 ordering part number	Manufacturer	Applicable power supply model	Power information	Compliance detail	Notes
3FE 47358 AA	Fu hua	UES36WA-120300SPAB	12V 3A 36W AC/DC power adapter	ANSI municipality US, FCC/ETL	2-pin US input plug
	Ruide	RD1203000-C55-20MG	12V 2A 36W AC/DC power adapter	ANSI municipality US, FCC/ETL	2-pin US input plug
3FE 47358 BA	Fu hua	UES36WA-120300SPAV	12V 3A 36W DC power adapter	Europe, CE certified	2-pin EU input plug
	Ruide	RD1203000-C55-20OG	12V 2A 36W DC power adapter	Europe, CE certified	2-pin EU input plug
3FE 47358 CA	Fu hua	UES36WA-120300SPAU	12V 3A 36W AC/DC power adapter	UK, CE certified	3-pin UK input plug
	Ruide	RD1203000-C55-20YG	12V 2A 36W AC/DC power adapter	UK, CE certified	3-pin UK input plug

5.2 Gateway 3 (G-240W-E) general description

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

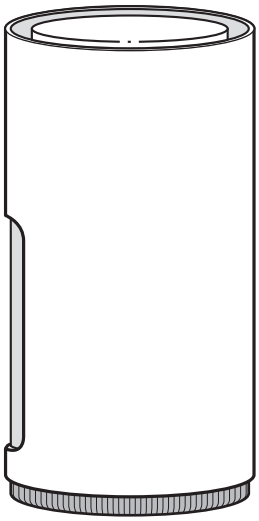
The overall Nokia WiFi solution is composed of one or more Nokia WiFi gateways, the WiFi Care Portal for the customer care team of the operator, and a mobile application for end-user self care.

The Gateway 3 (G-240W-E) can be deployed as either an Ethernet residential gateway or a WiFi gateway in the Nokia WiFi solution. The residential gateway is the central point of the mesh network providing access to the broadband network (Internet) while the gateway aids with extending the WiFi coverage to every corner of the home, providing seamless roaming to wireless connected devices.

The Gateway 3 (G-240W-E) has built-in concurrent dual-band WiFi 802.11b/g/n and 802.11ac networking with triple-play capability. Gateway 3 (G-240W-E) devices can be configured using the Nokia WiFi Mobile App, which can be downloaded on both iOS and Android devices.

Figure 6 shows the Gateway 3 (G-240W-E) gateway.

Figure 6 **Gateway 3 (G-240W-E)**



28280

The Gateway 3 (G-240W-E) provides the following functions and benefits:

- Automatically decide on wireless router mode and gateway mode in a mesh network
- Dual-band concurrent IEEE 802.11b/g/n 3x3 2.4 GHz and 802.11ac 4x4 5 GHz
- Four 10/100/1000Base-T interface with RJ-45 connectors
- Two POTS ports with R-J11 connectors
- Two USB 2.0 Type A ports
- Nokia intelligent mesh
- Embedded edge analytics optimize network performance in real time
- Real-time wireless spectrum analysis
- Supports DFS
- GPON uplink

Benefits:

- PHY rate up to 450 Mb/s for 2.4 GHz and 2170 Mb/s for 5 GHz (with 1024 QAM capable clients)
- Self-healing, self-optimizing network
- Mesh topology and intelligent mesh routing
- Seamless roaming (IEEE 802.11k, 802.11v, 802.11r/legacy)
- Band steering, channel optimization
- Embedded range boost technology helps to significantly extend absolute range
- Real-time wireless spectrum scan and analysis
- High quality of service (QoS) video over Wi-Fi
- Ease of setup and user intuitive information

Table 6 lists additional function details.

Table 6 **Gateway 3 (G-240W-E) function details**

Function	Detail
Installation	Desk mounted
WLAN interfaces	• Supports 3x3 802.11b/g/n 2.4 GHz wireless LAN (WLAN) interface • Supports 4x4 802.11ac 5 GHz WLAN interface with multi-user multiple input, multiple output (MU-MIMO) • Maximum effective isotropic radiated power (EIRP) on 2.4 GHz up to 500 mW and 5 GHz up to 1 W • 64-bit and 128-bit Wired Equivalent Privacy (WEP) support • Wi-Fi Protected Access (WPA) support including Pre-Shared Key (WPA-PSK) and WPA2 • Media access control (MAC) filters
Router mode	• IPv4 and IPv6 • Point-to-Point Protocol over Ethernet (PPPoE) and IP over Ethernet (IPoE) • Network Address Translation (NAT), demilitarized zone (DMZ) and firewall • Dynamic Host Configuration Protocol (DHCP) and domain name system (DNS) proxy • Internet Group Management Protocol (IGMP) v2/v3 proxy/Multicast Listener Discovery (MLD) proxy • Supports TR-069 • Supports virtual private network (VPN) pass- through for Point-to-Point Tunneling protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and IPSec • Port forwarding and DMZ/dynamic domain name system (DDNS) • Flexible video delivery options over Ethernet or wireless
Gateway mode	• Supports IPv4, IPv6 • Supports TR-069/TR-111 • Supports VPN pass-through for PPTP, L2TP and IPSec • IGMP v2/v3 snooping and MLD proxy • Flexible video delivery options over Ethernet or wireless
LED	• Top LED for simple and intuitive status indication • Safety and electromagnetic interference (EMI) • Protection of over voltage/current

(1 of 2)

Function	Detail
Regulatory compliance	• UL 62368-1 • FCC Part 15 • CE

(2 of 2)

5.2.1 TR-069 object support for WiFi parameters

The Gateway 3 supports the status retrieval and configuration of the following WiFi parameters via TR-069:

- channel
- SSID
- password for WPA and WEP
- Tx power (transmission rate in dBm)

These are the same TR-069 object parameters that are supported in the GUI. For more information, see Tables 24 and 25 in the chapter “Configure a Gateway 3 (G-240W-E)”.

5.2.2 Independent TR69 session with SaaS

The prime communication between the Nokia cloud management solution and the Gateway 3 (G-240W-E) is TR-069.

To keep the Nokia Home WiFi management independent from the ACS of the carrier, The device can establish an independent TR-069 session with the SaaS.

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

5.2.3 TR69 authentication using TLS and CA certificates

Gateway 3 (G-240W-E) devices support encrypted remote TR-069 management using TLS, as well as ACS authentication using SHA-256 pre-installed certificates.

If the ACS URL is set to the https://... format, by default, the connection will use TLS without authentication mode. The Gateway 3 can also authenticate the ACS using a pre-installed CA certificate.

5.3 Gateway 3 (G-240W-E) software and installation feature support

For information on installing or replacing the Gateway 3 (G-240W-E), see:

- Install a Gateway 3 (G-240W-E)
- Replace a Gateway 3 (G-240W-E)

5.4 Gateway 3 (G-240W-E) interfaces and interface capacity

Table 7 describes the supported interfaces and interface capacity for Gateway 3 (G-240W-E) devices.

Table 7 **Gateway 3 (G-240W-E) interface connection capacity**

Type and model	Maximum capacity								
	POTS	10/ 100 BASE-T	10/ 100/1000 1000 BASE-T	RF video (CATV)	MoCA	VDSL2	E1/T1	Local craft	GPON uplink
Gateway 3	2	—	4	—	—	—	—	—	1

5.4.1 Gateway 3 (G-240W-E) connections and components

Figure 7 shows the physical connections for Gateway 3 (G-240W-E) devices.

Figure 7 **Gateway 3 (G-240W-E) physical connections**

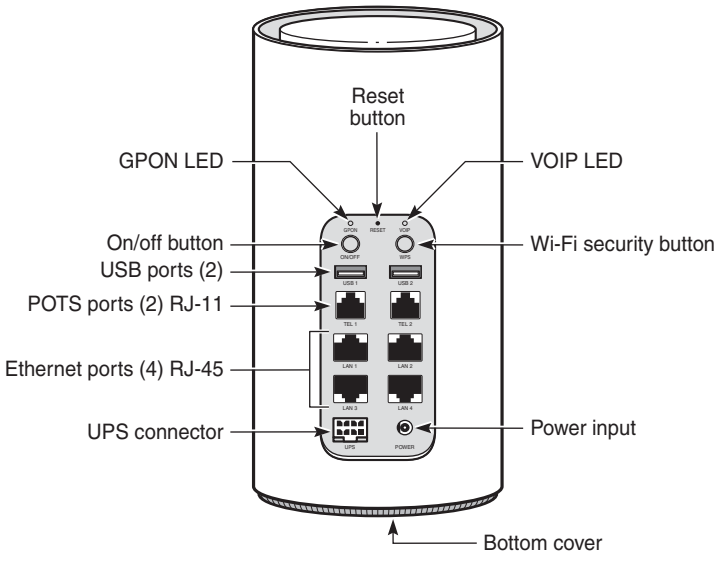


Table 8 describes the physical connections for Gateway 3 (G-240W-E) devices.

Table 8 **Gateway 3 (G-240W-E) physical connection**

Connection	Description
GPON LED	This LED is used to show the start of the GPON uplink.
VOIP LED	This LED is used to show the start of VOIP services.
On/Off button	This button powers the unit on or off.
WPS ON/Off button	This button is used to power the WiFi Protected Setup (WPS) of new WiFi devices on or off.
USB 1 and USB 2	This connection is provided through two USB 2.0 interfaces.
TEL1 and TEL2	This connection is provided through two RJ-11 POTS ports.
LAN 1 to LAN 4	This connection is provided through Ethernet RJ-45 connectors. Up to four 10/100/1000 Base-T Ethernet interfaces are supported. The Ethernet ports can support both data and in-band video services on all four interfaces.
UPS	This connection is a reserved interface provided through a UPS cable.
Reset button	Pressing the Reset button for less than 10 seconds reboots the device; pressing the Reset button for 10 seconds resets the device to the factory defaults.
Power input	This connection is provided through the power connector. A power cable fitted with a barrel connector is used to make the connection.

5.5 Gateway 3 (G-240W-E) LEDs

The circular top of the Gateway 3 (G-240W-E) functions as a multi-color LED indicator. The LED color and pulse rate acts as a signal to the home user, which indicates the state of the Gateway 3 and the quality of its backhaul link.

Table 9 provides LED descriptions for the Gateway 3 (G-240W-E).

Table 9 **Gateway 3 (G-240W-E) LED indications**

LED color	LED behavior	Router mode	Bridge mode	LED behavior description
Off	Off	✓	✓	Power off.
Blue-Green	Solid	✓		Good backhaul connection to the Internet.
	Solid		✓	Good backhaul connection. A link to the next node is available.
Yellow	Solid		✓	Backhaul connection is successful but not optimal. A link to the next node is below standard.
	Slow pulsing	✓	✓	Configuration mode. The unit is waiting to be configured.
Red	Solid	✓		No connection to the Internet.
	Solid		✓	Backhaul connection is not successful. A link to the next node is not operational.
	Fast pulsing	✓	✓	Factory reset
White	Slow pulsing	✓	✓	WPS enabled
	3 quick pulses	✓	✓	WPS successful
	Solid	✓	✓	Powering on

5.6 Gateway 3 (G-240W-E) detailed specifications

Table 10 lists the physical specifications for the Gateway 3 (G-240W-E).

Table 10 **Gateway 3 (G-240W-E) physical specifications**

Description	Specification
Diameter	94 mm (3.7 in.)
Height	200 mm (78.7 in.)
Weight [within ± 0.5 lb (0.23 kg)]	857g (1.89 lb)

Table 11 lists the power consumption specifications for the Gateway 3 (G-240W-E).

Table 11 **Gateway 3 (G-240W-E) power consumption specifications**

Maximum power (Not to exceed)	Condition	Minimum power	Condition
32 W	4 10/100/1000 Base-T Ethernet, WiFi operational	8 W	interfaces/services not provisioned

Table 12 lists the environmental specifications for Gateway 3 (G-240W-E).

Table 12 **Gateway 3 (G-240W-E) environmental specifications**

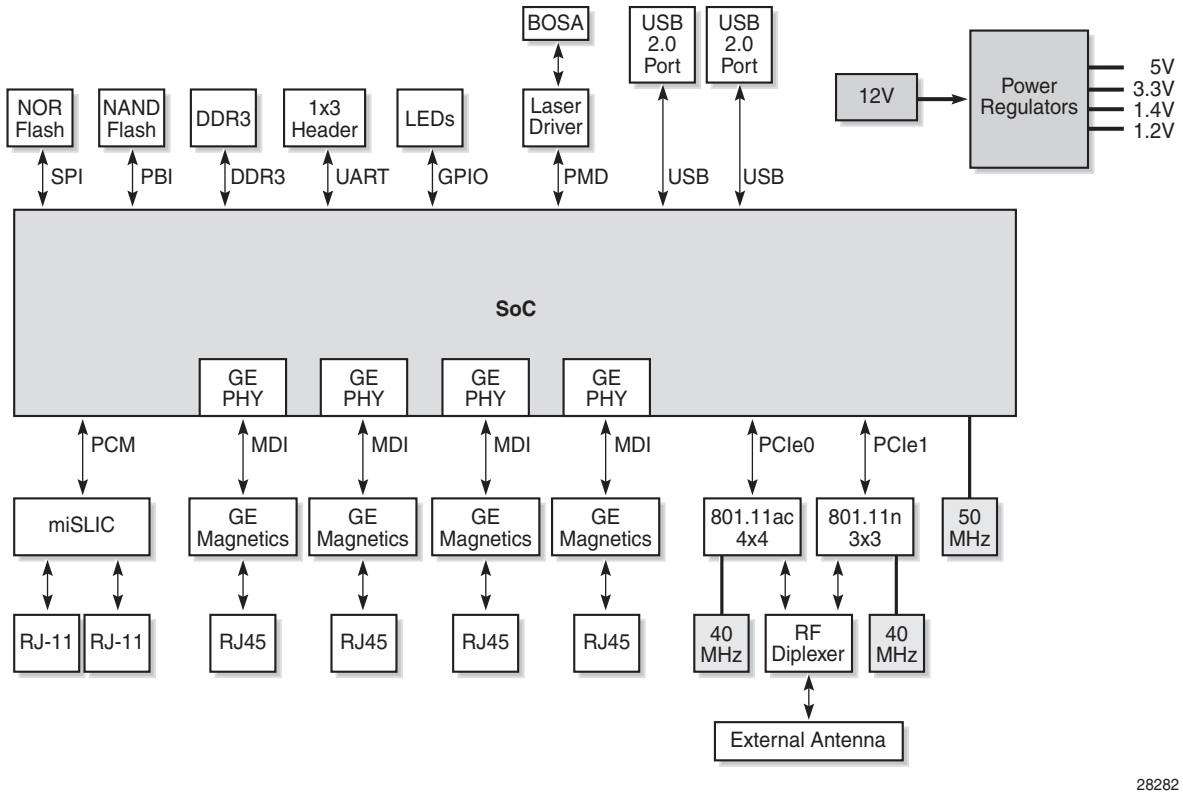
Mounting method	Temperature range and humidity	Altitude
On desk or shelf	Operating: -5°C to 45°C (23°F to 113°F) ambient temperature 5% to 95% relative humidity, non-condensing	Contact your Nokia technical support representative for more information
	Storage: -20°C to 85°C (-4°F to 185°F)	

5.7 Gateway 3 (G-240W-E) functional blocks

Gateway 3 (G-240W-E) devices are single-residence units that support Wireless (WiFi) service. WiFi service on these devices is compliant with the IEEE 802.11 standard. In addition to the WiFi service, these devices transmit Ethernet packets to two RJ-45 Ethernet ports.

Figure 8 shows the functional blocks for the Gateway 3 (G-240W-E).

Figure 8 **Single-residence WiFi CPE with Gigabit Ethernet**



5.8 Gateway 3 (G-240W-E) responsible party

Table 13 lists the party in the US responsible for the Gateway 3.

Table 13 **Responsible party contact information**

Legal Company name	Nokia USA Inc.
Address	2301 SUGAR BUSH RD. STE 300, RALEIGH,NC 27612
Phone, Fax	+(866) 582-3688

5.9 Gateway 3 (G-240W-E) special considerations

This section describes the special considerations for Gateway 3 (G-240W-E) devices.

5.9.1 WiFi service

Gateway 3 (G-240W-E) devices feature WiFi service as well as data services. WiFi is a wireless networking technology that uses radio waves to provide wireless HSI and network connections. This device complies with the IEEE 802.11 standards, which the WiFi Alliance defines as the basis for WiFi technology.

5.9.1.1 WiFi standards and certifications

The WiFi service on Gateway 3 (G-240W-E) devices supports the following IEEE standards and WiFi Alliance certifications:

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

5.9.1.2 WiFi GUI features

Gateway 3 (G-240W-E) devices have HTML-based WiFi configuration GUIs.

In addition to the traditional web-based GUI, the home user can download and use a mobile app for managing the Gateway 3.

5.9.2 Gateway 3 (G-240W-E) considerations and limitations

Table 14 lists the considerations and limitations for Gateway 3 (G-240W-E) devices.

Table 14 **Gateway 3 (G-240W-E) considerations and limitations**

Considerations and limitations
There are no special considerations or limitations at this time.

6 Install a Gateway 3 (G-240W-E)

6.1 Purpose

This chapter provides the steps to install a Gateway 3 (G-240W-E).

6.2 General

The steps listed in this chapter describe mounting and cabling for a Gateway 3 (G-240W-E).

6.3 Prerequisites

You need the following items before beginning the installation:

- all required cables

6.4 Recommended tools

You need the following tools for the installation:

- RJ-45 Ethernet cable
- paper clip

6.5 Safety information

Read the following safety information before installing the unit.

Danger 1 — Hazardous electrical voltages and currents can cause serious physical harm or death. Always use insulated tools and follow proper safety precautions when connecting or disconnecting power circuits.

Danger 2 — Make sure all sources of power are turned off and have no live voltages present on feed lines or terminals. Use a voltmeter to measure for voltage before proceeding.

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

Caution 1 — Keep indoor devices out of direct sunlight. Prolonged exposure to direct sunlight can damage the unit.

Caution 2 — Keep 20 cm away from the Gateway 3 (G-240W-E) when configuring functions on the local web or app.

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

Note 2 — Observe the following:

- The device should be installed in accordance with the applicable requirements of the NEC or CEC. Local authorities and practices take precedent when there is conflict between the local standard and the NEC or CEC.
- The device must be installed by qualified service personnel.
- Indoor units must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the Gateway 3 (G-240W-E) unit data sheet for the temperature ranges for these devices.

6.6 Procedure

Use this procedure to install a Gateway 3 (G-240W-E).

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

Note — The Gateway 3 (G-240W-E) cannot be stacked with another or with other equipment. The installation requirements are:

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

2 Connect the fiber optic cable with the SC/APC adapter into the SC/APC connector.

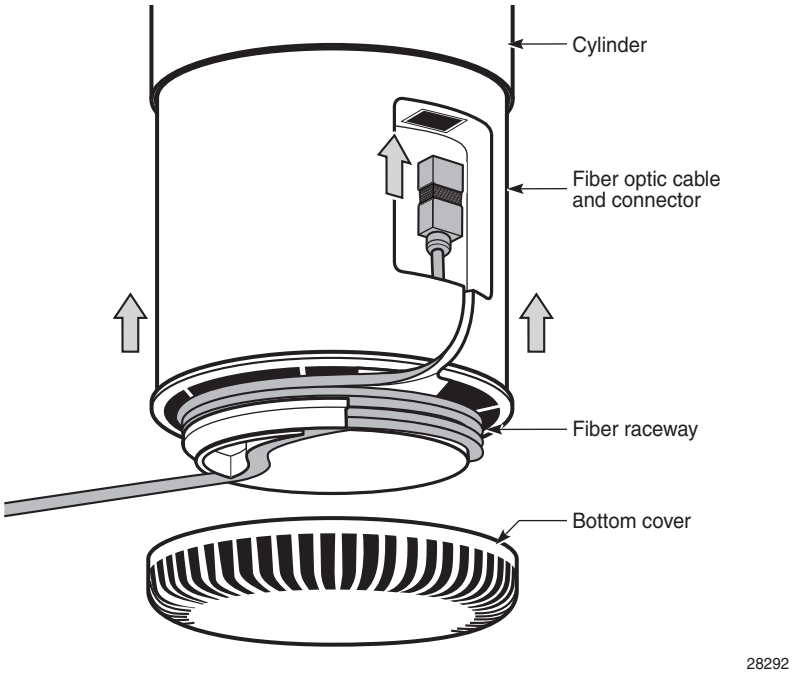
Danger — Fiber cables transmit invisible laser light. To avoid eye damage or blindness, never look directly into fibers, connectors, or adapters.

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

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

i Remove the fiber optic connection cover (white cylinder), as shown in Figure 9.

Figure 9 **Gateway 3 (G-240W-E) cylinder removal**



ii Detach the bottom cover.

iii Plug the fiber optic cable with the SC/APC adapter into the fiber optic connector, as shown in Figure 9.

iv Wind the fiber optic cable through the fiber track at the base of the cylinder until the desired length of the cable is reached.

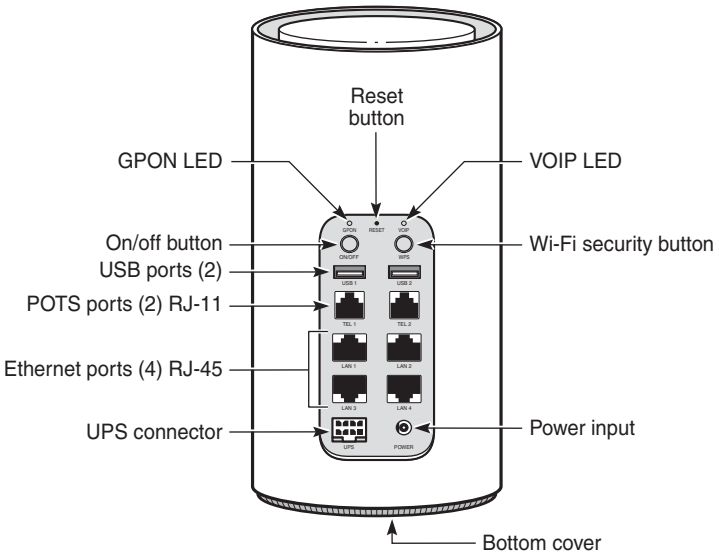
v Press the fiber optic cable into the slot.

vi Replace the bottom cover.

vii Replace the fiber optic connection cover (white cylinder).

3 Review the connection locations, as shown in Figure 10.

Figure 10 **Gateway 3 (G-240W-E) connections**



4 Connect the Ethernet cables to the RJ-45 ports; see Figure 10 for the location of the RJ-45 ports.

5 Connect the power cable to the power connector.

Note — Observe the following:

- Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 12 V dc, 3 A. The polarity of the power adapter plug must match the Gateway 3.

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

7 Verify the LEDs and voltage status.

8 Activate and test the services.

9 If necessary, reset the Gateway 3 (G-240W-E).

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

i Locate the Reset button as shown in Figure 10.

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

10 STOP. This procedure is complete.

7 Replace a Gateway 3 (G-240W-E)

7.1 Purpose

This chapter provides the steps to replace a Gateway 3 (G-240W-E).

7.2 General

The steps listed in this chapter describe mounting and cabling for a Gateway 3 (G-240W-E).

7.3 Prerequisites

You need the following items before beginning the installation:

- all required cables

7.4 Recommended tools

You need the following tools for replacing the Gateway 3 (G-240W-E):

- RJ-45 cable
- paper clip

7.5 Safety information

Read the following safety information before replacing the unit.

Danger 1 — Hazardous electrical voltages and currents can cause serious physical harm or death. Always use insulated tools and follow proper safety precautions when connecting or disconnecting power circuits.

Danger 2 — Make sure all sources of power are turned off and have no live voltages present on feed lines or terminals. Use a voltmeter to measure for voltage before proceeding.

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

Caution 1 — Keep indoor devices out of direct sunlight. Prolonged exposure to direct sunlight can damage the unit.

Caution 2 — Keep 20 cm away from the Gateway 3 (G-240W-E) when configuring functions on the local web or app.

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

Note 2 — Observe the following:

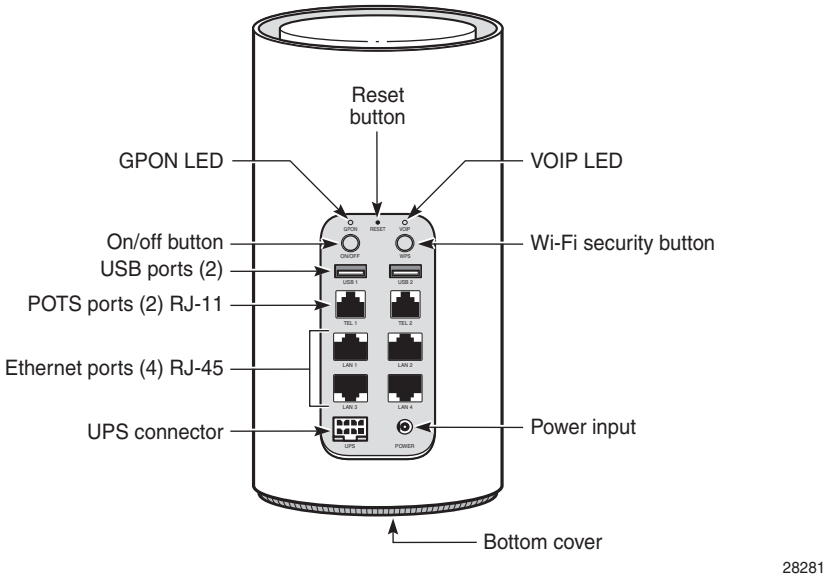
- The device should be installed in accordance with the applicable requirements of the NEC or CEC. Local authorities and practices take precedent when there is conflict between the local standard and the NEC or CEC.
- The device must be installed by qualified service personnel.
- Indoor units must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the Gateway 3 (G-240W-E) unit data sheet for the temperature ranges for these devices.

7.6 Procedure

Use this procedure to replace a Gateway 3 (G-240W-E).

1 Power down the unit by using the on/off power switch. See Figure 11 for the connections on the Gateway 3 (G-240W-E).

Figure 11 **Gateway 3 (G-240W-E) connections**



2 Disconnect the WAN, Ethernet, and power cables from the Gateway 3 (G-240W-E); see Figure 11 for the connector locations on the Gateway 3 (G-240W-E).

3 If necessary, disconnect the fiber optic cable. Go to step 5.

4 Replace the Gateway 3 (G-240W-E) with the new device. The device can be placed on any flat surface, such as a desk or shelf.

5 Connect the fiber optic cable with the SC/APC adapter into the SC/APC connector.

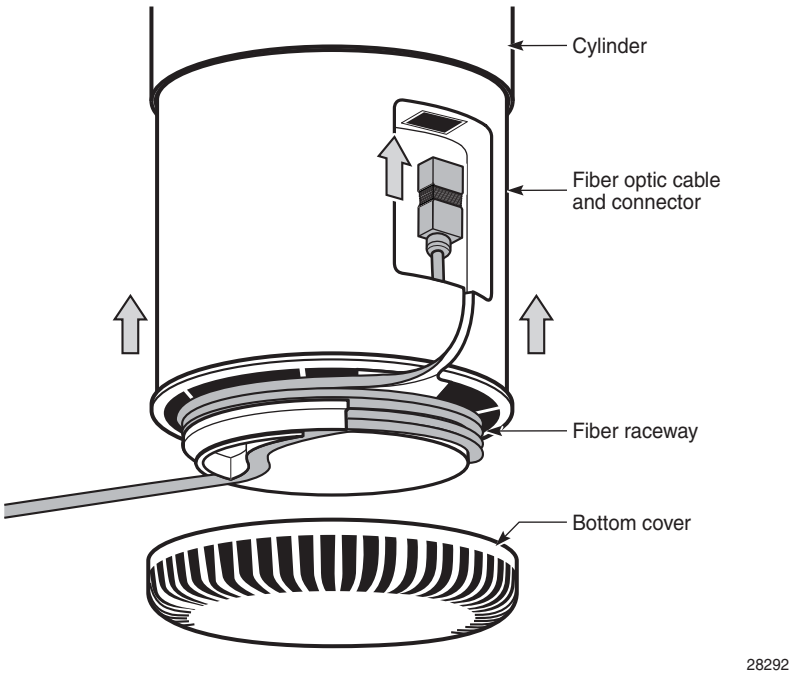
Danger — Fiber cables transmit invisible laser light. To avoid eye damage or blindness, never look directly into fibers, connectors, or adapters.

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

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

i Remove the fiber optic connection cover (white cylinder), as shown in Figure 12.

Figure 12 **Gateway 3 (G-240W-E) cylinder removal**



ii Detach the bottom cover.

iii Plug the fiber optic cable with the SC/APC adapter into the fiber optic connector, as shown in Figure 12.

iv Wind the fiber optic cable through the fiber track at the base of the cylinder until the desired length of the cable is reached.

v Press the fiber optic cable into the slot.

vi Replace the bottom cover.

vii Replace the fiber optic connection cover (white cylinder).

6 Connect the Ethernet cables directly to the RJ-45 ports; see Figure 11 for the location of the RJ-45 ports.

7 Connect the power cable to the power connector.

Note — Observe the following:

- Units must be powered by a Listed or CE approved and marked limited power source with a minimum output rate of 12 V dc, 3 A. The polarity of the power adapter plug must match the Gateway 3.

8 Power up the unit by using the On/Off power button.

9 Verify the LEDs and voltage status.

10 Activate and test the services.

11 If necessary, reset the Gateway 3 (G-240W-E).

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

i Locate the Reset button on a Gateway 3 (G-240W-E) as shown in Figure 11.

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

12 STOP. This procedure is complete.

8 Configure a Gateway 3 (G-240W-E)

8.1 GUI configuration

Use the procedures below to use the web-based GUI for the Gateway 3 (G-240W-E).

The Gateway 3 (G-240W-E) is used as an Ethernet gateway to connect devices in the home to the Internet. The GUI provides a variety of features for the home network including routing and firewall capability. By using the GUI, users can configure the right network connectivity for all equipment in their home, including personal computers, set-top boxes, mobile phones, and other consumer electronics devices, to the Internet.

Caution — Keep 20 cm away from the Gateway 3 (G-240W-E) when configuring functions on the local web or app.

8.1.1 Login

Use the procedure below to login to the web-based GUI for the Gateway 3 (G-240W-E).

Procedure 6 Login to web-based GUI

1 Open a web browser and enter the IP address of the Gateway 3 (G-240W-E) in the address bar.

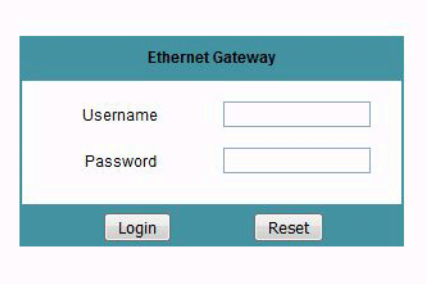
The login window appears.

The default gateway IP address is http://192.168.18.1. You can connect to this IP address using your web browser after connecting your PC to one of Ethernet ports of the Gateway 3 (G-240W-E). The static IP address of your PC must be in the same 192.168.18.x subnet as the Gateway 3 (G-240W-E).

2 Enter your username and password in the Log in window, as shown in Figure 13.

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

Figure 13 **Web login window**



Caution — If you forget the current username and password, press the reset button for 10s and the default values for the username and password will be recovered at startup.

Pressing the Reset button for less than 10 seconds reboots the device; pressing the Reset button for 10 seconds resets the device to the factory defaults.

3 Click Login. The Device Information screen appears.

Note — To help protect the security of your Internet connection, the application displays a pop-up reminder to change both the WiFi password and the Gateway 3 (G-240W-E) password.

To increase password security, use a minimum of 10 characters, consisting of a mix of numbers and upper and lowercase letters.

4 STOP. This procedure is complete.

8.1.2 Device and connection status

The Gateway 3 (G-240W-E) supports the retrieval of a variety of device and connection information, including:

- device information
- LAN status
- WAN status
- WAN status IPv6
- home networking information
- statistics

Procedure 7 Device information retrieval

1 Select Status > Device Information from the top-level menu in the Ethernet Gateway window, as shown in Figure 14.

Figure 14 **Device Information window**

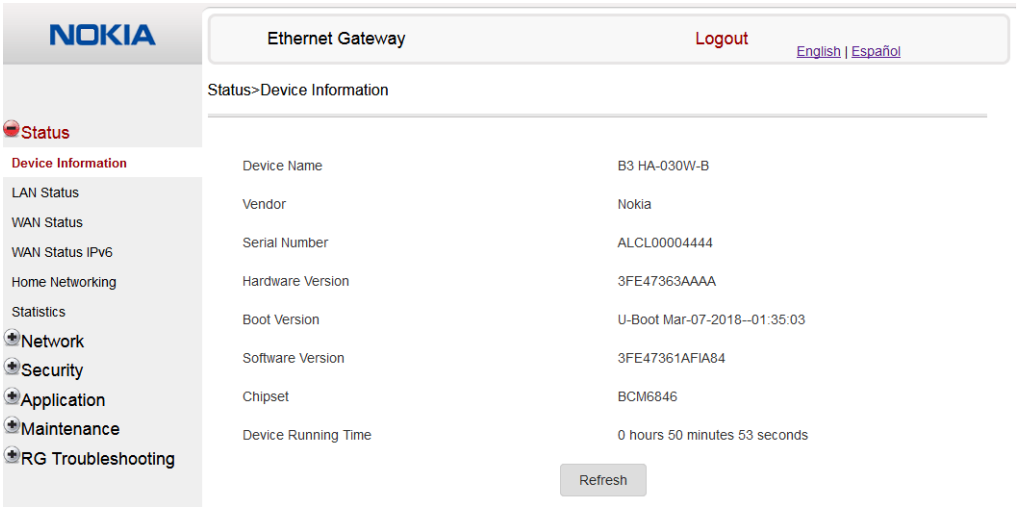


Table 15 describes the fields in the Device Information window.

Table 15 **Device Information parameters**

Field	Description
Device Name	Name on the Gateway 3 (G-240W-E)
Vendor	Name of the vendor
Serial Number	Serial number of the Gateway 3 (G-240W-E)
Hardware version	Hardware version of the Gateway 3 (G-240W-E)
Boot version	Boot version of the Gateway 3 (G-240W-E)
Software version	Software version of the Gateway 3 (G-240W-E)
Chipset	Chipset of the Gateway 3 (G-240W-E)
Device Running Time	Amount of time the device has run since last reset in hours, minutes, and seconds

2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

Procedure 8 LAN status retrieval

1 Select Status > LAN Status from the top-level menu in the Ethernet Gateway window, as shown in Figure 15.

Figure 15 **LAN status window**

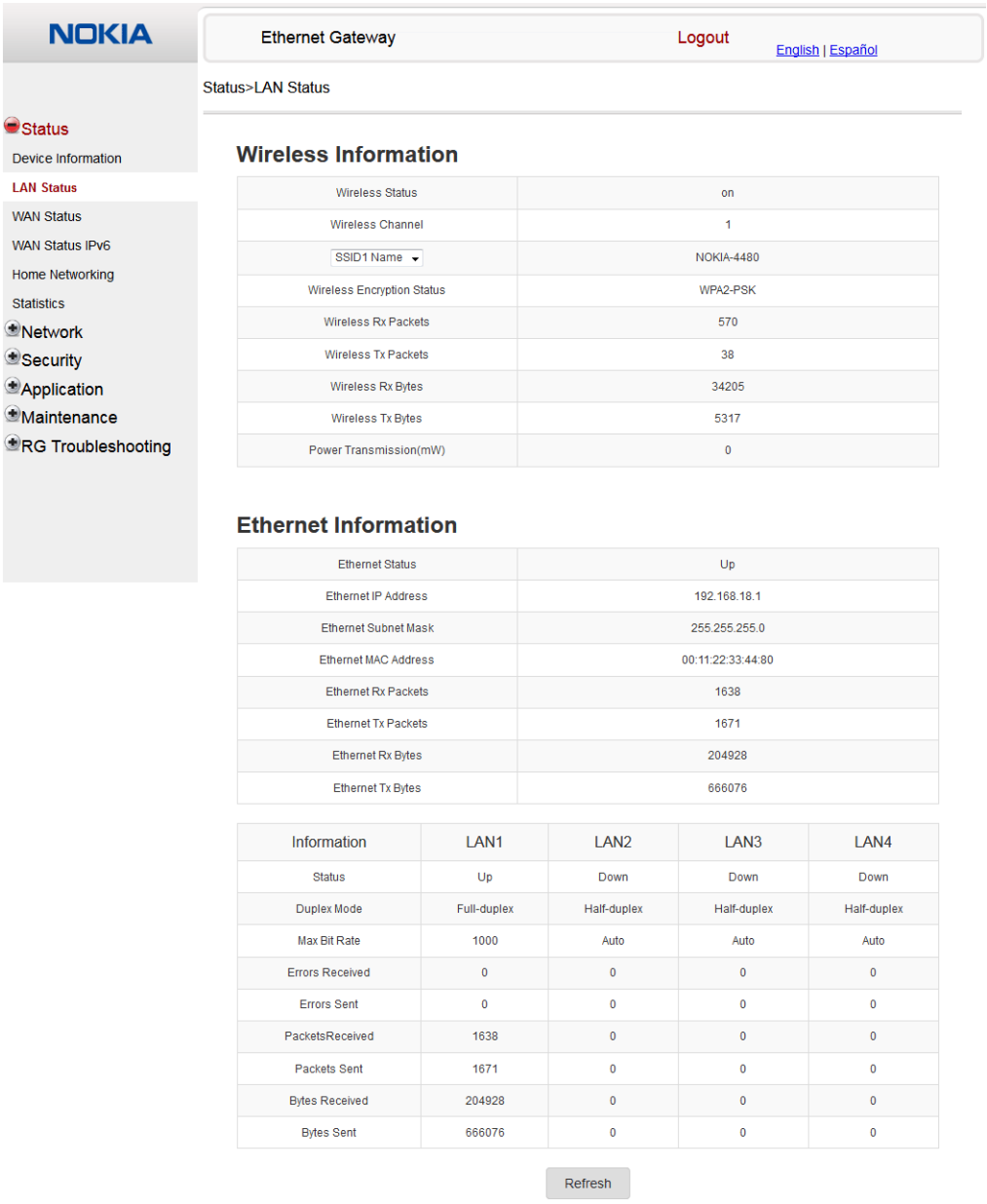


Table 16 describes the fields in the LAN status window.

Table 16 **LAN status parameters**

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

2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

Procedure 9 WAN status retrieval

1 Select Status > WAN Status from the top-level menu in the Ethernet Gateway window, as shown in Figure 16.

Figure 16 **WAN Status window**

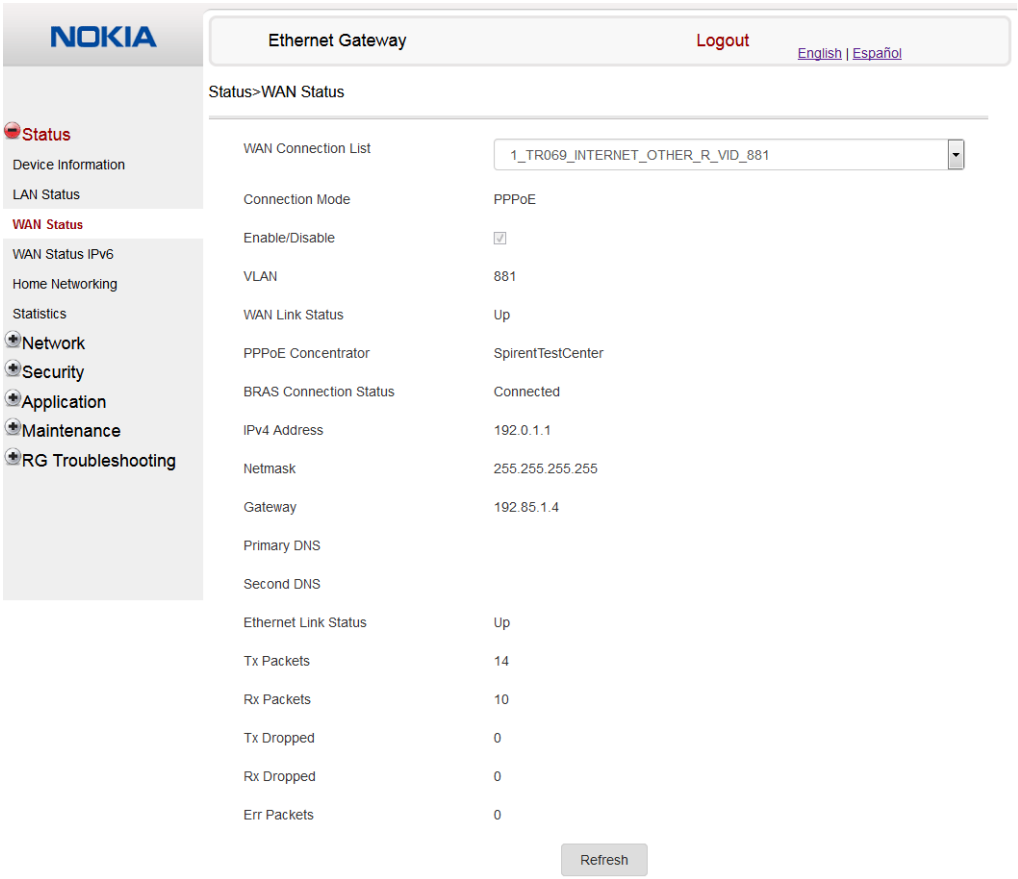


Table 17 describes the fields in the WAN Status window.

Table 17 **WAN Status parameters**

Field	Description
WAN connection list	Drop-down menu listing all WAN connections. The connection shown is the connection for which WAN status will be shown.
Connection Mode	Connection mode of the WAN connection
Enable/Disable	Select this checkbox to enable the WAN connection
VLAN	VLAN ID

(1 of 2)

Field	Description
WAN Link Status	Whether the WAN link is up or down
PPPoE Concentrator	Read-only field identifying the PPPoE Concentrator
BRAS Connection Status	Read-only field indicating the status of the broadband remote access server
IPv4 Address	IPv4 address
Netmask	Netmask
Gateway	IPv4 gateway address
Primary DNS	Primary Domain Name Server
Second DNS	Secondary Domain Name Server
Ethernet Link Status	Whether the PON link is up or down
Tx Packets	Number of packets transmitted on the WAN connection
Rx Packets	Number of packets received on the WAN connection
Tx Dropped	Number of packets dropped on the transmit WAN connection
Rx Dropped	Number of packets dropped on the receive WAN connection
Err Packets	Number of errored packets on the WAN connection

(2 of 2)

2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

Procedure 10 WAN status IPv6 retrieval

1 Select Status > WAN Status IPv6 from the top-level menu in the Ethernet Gateway window, as shown in Figure 17.

Figure 17 **WAN Status IPv6 window**

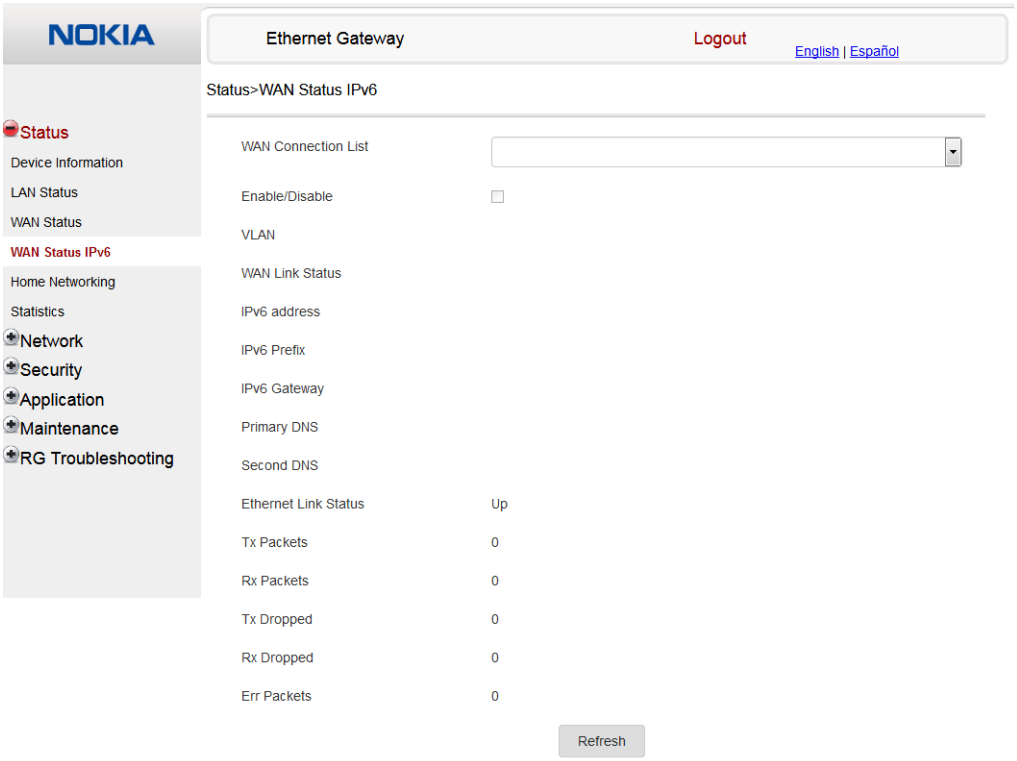


Table 18 describes the fields in the WAN status IPv6 window.

Table 18 **WAN status IPv6 parameters**

Field	Description
WAN connection list	Drop-down menu listing all WAN connections. The connection selected is the connection for which WAN status will be shown.
Enable/Disable	Select this check box to enable the WAN connection
VLAN	VLAN ID
WAN Link Status	Whether the WAN link is up or down
IPv6 Address	IPv6 address that identifies the device and its location
IPv6 Prefix	IPv6 prefix

(1 of 2)

Field	Description
IPv6 Gateway	IPv6 gateway address
Primary DNS	Primary Domain Name Server address
Second DNS	Secondary Domain Name Server address
Ethernet Link Status	Whether the link is up or down
Tx Packets	Number of packets transmitted on the WAN connection
Rx Packets	Number of packets received on the WAN connection
Tx Dropped	Number of packets dropped on the transmit WAN connection
Rx Dropped	Number of packets dropped on the receive WAN connection
Err Packets	Number of errored packets on the WAN connection

(2 of 2)

2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

Procedure 11 Home networking information retrieval

1 Select Status > Home Networking from the top-level menu in the Ethernet Gateway window, as shown in Figure 18.

Figure 18 **Home Networking information window**

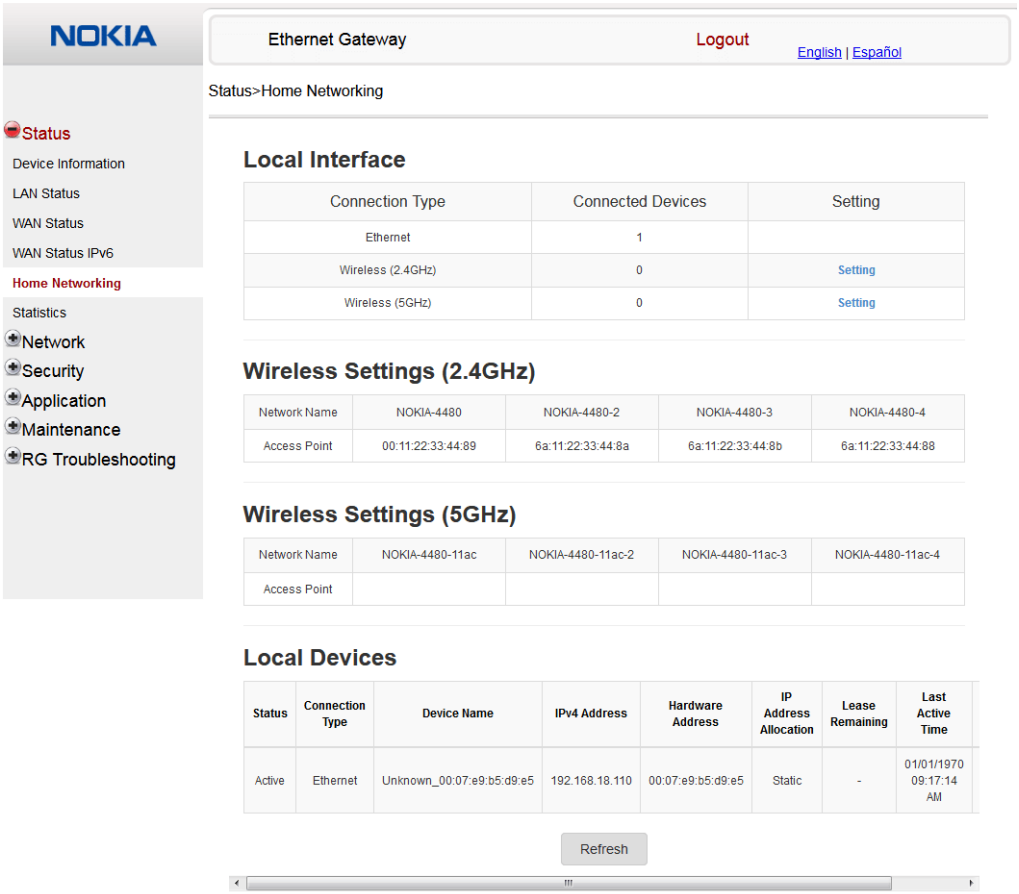


Table 19 describes the fields in the Home Networking window.

Table 19 **Home Networking parameters**

Field	Description
Local Interface	
Ethernet	Table displays the number of Ethernet connections and their settings
Wireless	Table displays the number of wireless connections and their settings
Wireless Settings	

(1 of 2)

Field	Description
Network Name	Name of the wireless network access point
Access Point	Hexadecimal address of the wireless access point
Local Devices	
Table entry	Each entry indicates the status (active or inactive), connection type, device name, IP address, hardware address, and IP address allocation, lease remaining, and last active time of each connected local device.

(2 of 2)

2 Click Delete to delete a particular local device connection.

3 Click Refresh to update the displayed information.

4 STOP. This procedure is complete.

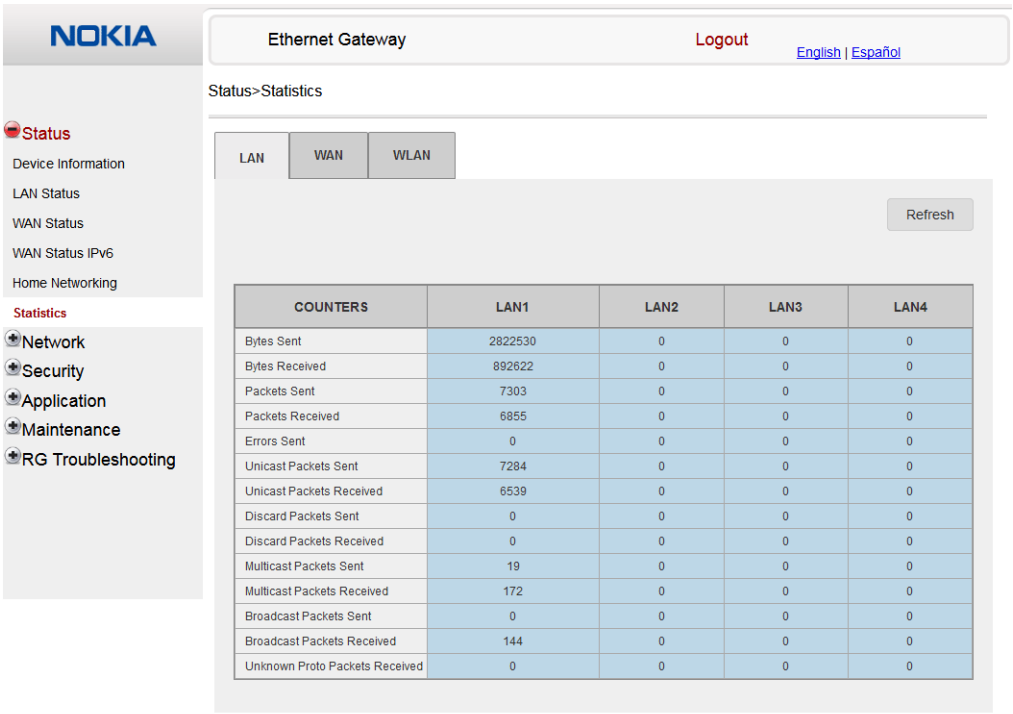
Procedure 12 Statistics retrieval

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

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

Figure 19 shows the statistics for the LAN ports.

Figure 19 **LAN ports statistics window**



2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

8.1.3 Network configuration

The Gateway 3 (G-240W-E) also supports network configuration, including:

- LAN
- LAN IPv6
- WAN
- WAN DHCP
- Wireless 2.4GHz
- Wireless 5GHz
- Wireless Schedule
- IP routing
- DNS

- TR-069
- QoS Configuration

Procedure 13 LAN configuration

1 Select Network > LAN from the top-level menu in the Ethernet Gateway window, as shown in Figure 20.

Figure 20 **LAN settings window**

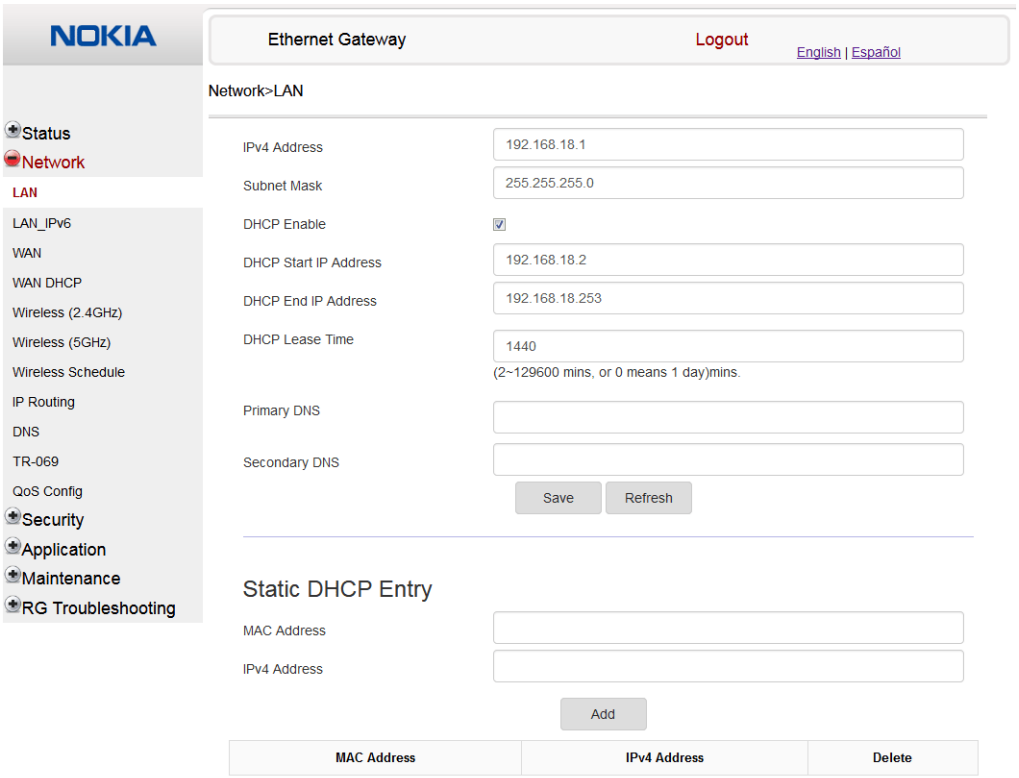


Table 20 describes the fields in the LAN window.

Table 20 **LAN parameters**

Field	Description
IPv4 Address	IP Address of the
Subnet Mask	Subnet mask of the
DHCP enable	Select this check box to enable DHCP

(1 of 2)

Field	Description
DHCP Start IP Address	Starting DHCP IP address
DHCP End IP Address	Ending DHCP IP address
DHCP Lease Time	DHCP lease time (in min)
Primary DNS	Primary domain name server address
Secondary DNS	Secondary domain name server address
Static DHCP MAC Address	Hexadecimal MAC address to associate to the LAN
Static DHCP IP Address	IP address to associate to the bound MAC address

(2 of 2)

2 Configure the LAN.

3 Click Save.

4 Bind a MAC address to the LAN by entering the MAC and IP addresses in the Static DHCP Entry fields and then clicking Add. Repeat for all MAC addresses to be bound.

5 STOP. This procedure is complete.

Procedure 14 LAN IPv6 networking configuration

1 Select Network > LAN_IPv6 from the top-level menu in the Ethernet Gateway window, as shown in Figure 21.

Figure 21 **LAN IPv6 network window**

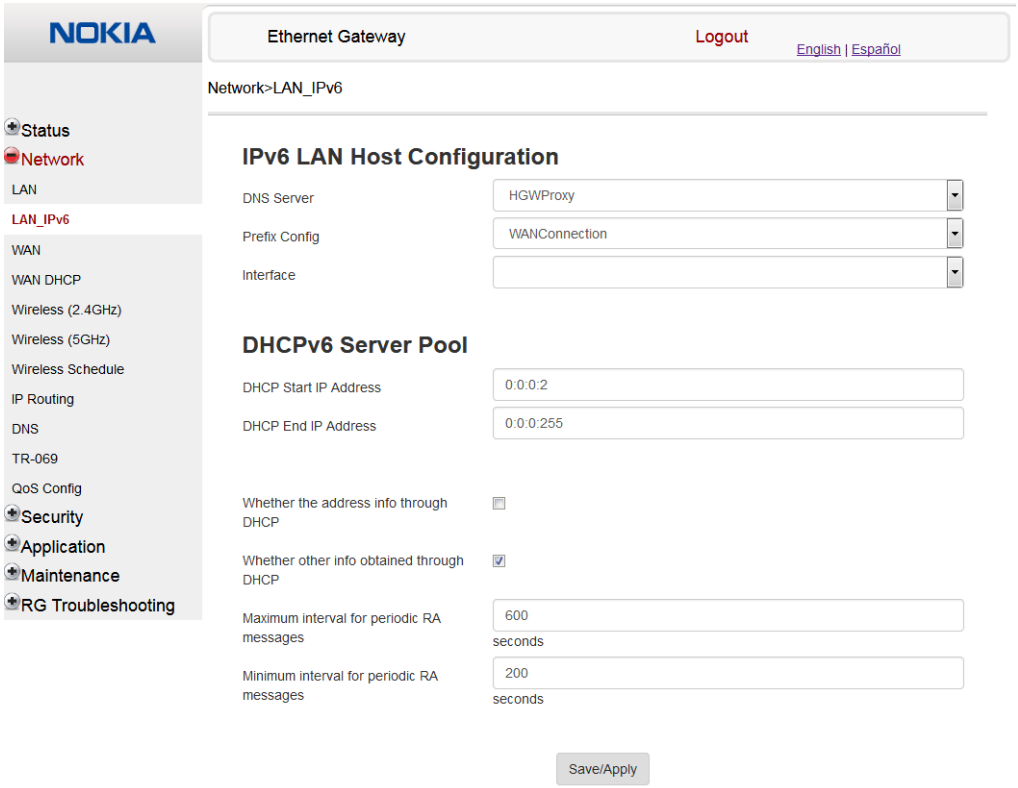


Table 21 describes the fields in the LAN IPv6 network window.

Table 21 **LAN IPv6 network parameters**

Field	Description
DNS Server	Choose a DNS server from the drop-down menu.
Prefix Config	Choose a prefix config option from the drop-down menu, either WANConnection (prefix will be obtained from the WAN) or Static (enables you to enter the prefix).
Prefix	This field appears if you selected the “Static” option for the “prefix config” field. Type a connection.
Interface	This field appears if you selected the Wan Connection option for the “prefix config” field. Choose a WAN connection interface from the drop-down menu.
DHCP Start IP Address	Enter the starting DHCP IP address.

(1 of 2)

Field	Description
DHCP End IP Address	Enter the ending DHCP IP address.
Whether the address info through DCHP	Select this check box to enable address information retrieval through DHCP.
Whether other info obtained through DHCP	Select this check box to enable retrieval of other information through DHCP.
Maximum interval for periodic RA messages	Enter the maximum interval (in seconds) for periodic Router Advertisement messages. The interval range is from 4 to 1800.
Minimum interval for periodic RA messages	Enter the minimum interval (in seconds) for periodic Router Advertisement messages. The interval range is from 4 to 1800.

(2 of 2)

2 Choose a DNS server, Prefix Config, and Interface.

3 Enter the DHCP configuration information.

4 Enter the maximum and minimum intervals for RA messages.

5 Click Save/Apply.

6 STOP. This procedure is complete.

Procedure 15 WAN networking configuration

1 Select Network > WAN from the top-level menu in the Ethernet Gateway window, as shown in Figure 22.

Figure 22 **WAN window**

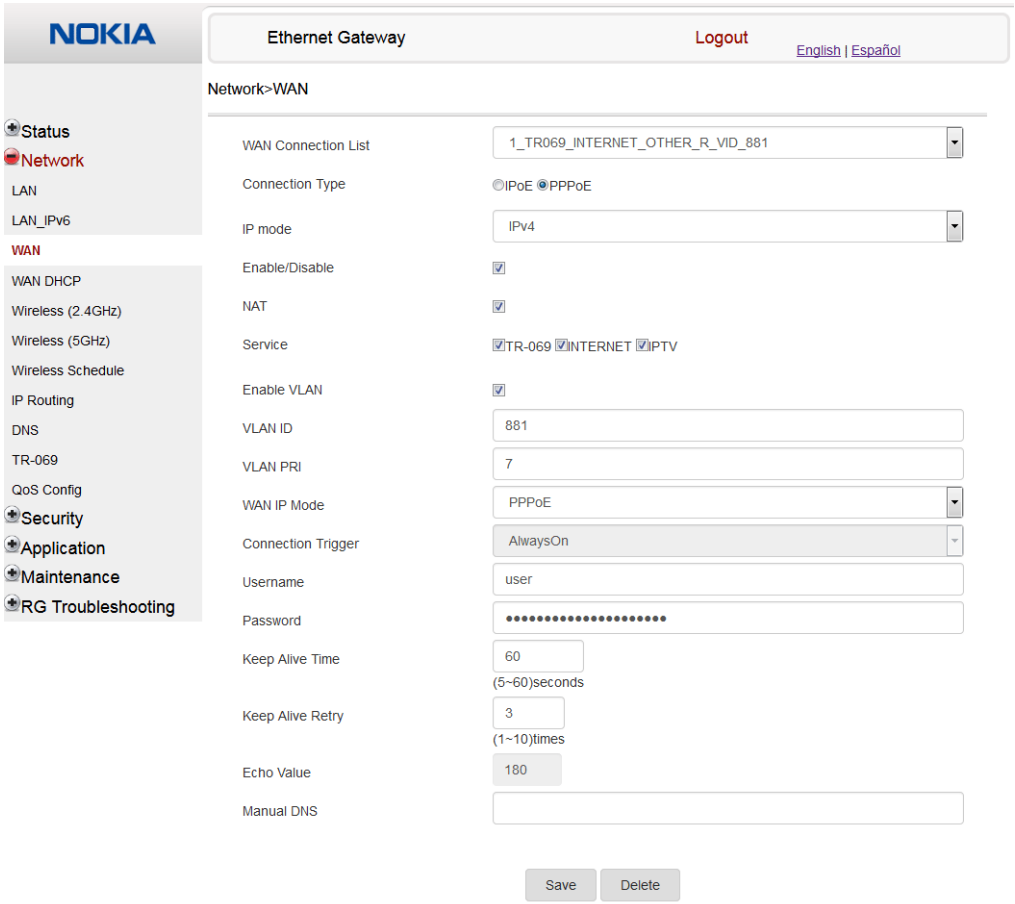


Table 22 describes the fields in the WAN window.

Table 22 **WAN parameters**

Field	Description
WAN Connection List	Choose a WAN connection from the drop-down menu to set the connection parameters
Connection Type	Select a connection type: IPoE or PPPoE
IP Mode	Choose an IP mode from the drop-down menu: IPv4 or IPv6

(1 of 2)

Field	Description
Enable/Disable	Select this checkbox to enable the WAN connection
NAT	Select this checkbox to enable NAT
Service	Select the checkboxes to enable service types for this connection
Enable VLAN	Select this checkbox to enable VLAN
VLAN ID	Enter the VLAN ID
VLAN PRI	Enter the VLAN PRI
WAN IP Mode	Choose an IP mode from the drop-down menu
Connection Trigger	Choose the trigger type from the drop-down menu
Username	Enter the Username provided by your ISP
Password	Enter the Password provided by your ISP
Keep Alive Time	Enter the keep alive time (5 to 60 seconds)
Keep Alive Retry	Enter the number of keep alive time retries (1 to 10 times)
Echo Value	The echo value: the keep alive time value multiplied by the number of retries
Manual DNS	Enter a DNS

(2 of 2)

2 Configure a specific WAN connection.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 16 WAN DHCP configuration

1 Select Network > WAN DHCP from the top-level menu in the Ethernet Gateway window, as shown in Figure 23.

Figure 23 **WAN DHCP window**

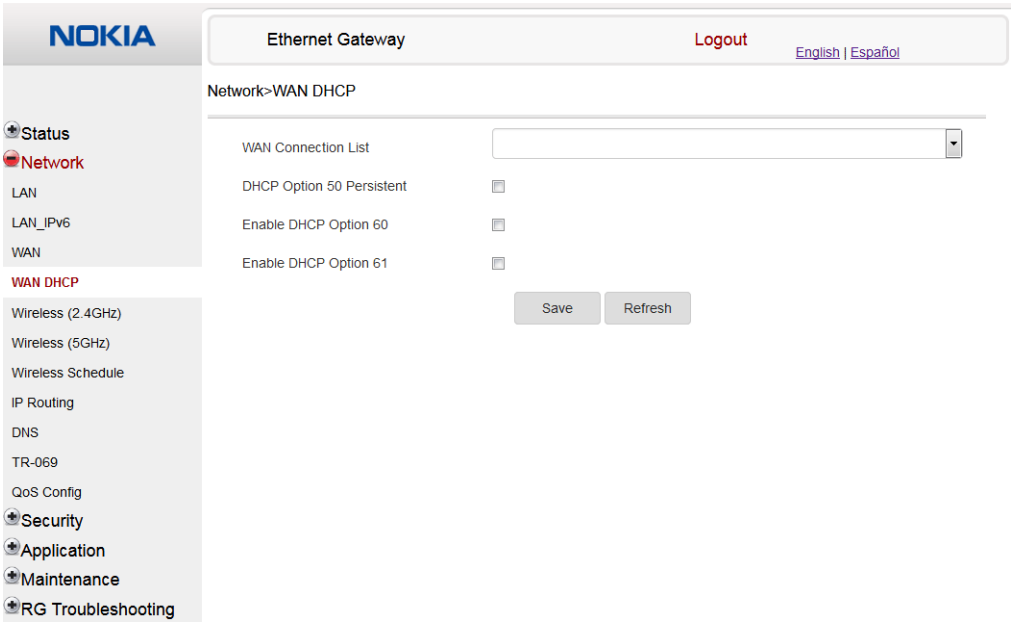


Table 23 describes the fields in the WAN DHCP window.

Table 23 **WAN DHCP parameters**

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

2 Configure a WAN DHCP option.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 17 Wireless 2.4G networking configuration

1 Select Network > Wireless 2.4GHz from the top-level menu in the Ethernet Gateway window, as shown in Figure 24.

Figure 24 **Wireless 2.4GHz network window**

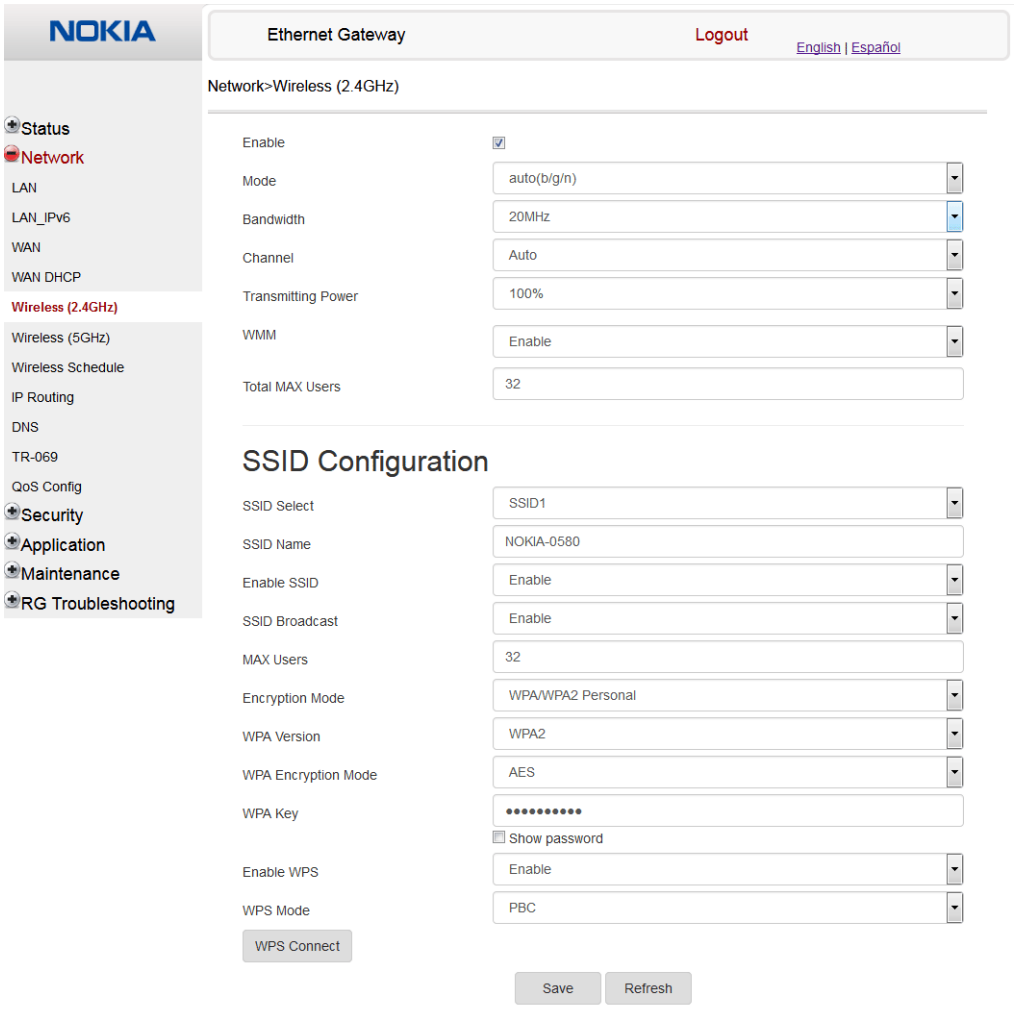


Table 24 describes the fields in the Wireless 2.4GHz network window.

Table 24 **Wireless 2.4GHz network parameters**

Field	Description
Enable	Select this check box to enable WiFi
Mode	Choose a WiFi mode from the drop-down menu: • auto (b/g/n) • b • g • n • b/g
Bandwidth	Choose 20 MHz or 40 MHz from the drop-down menu.
Channel	Choose a channel from the drop-down menu or choose Auto to have the channel automatically assigned
Transmitting Power	Choose the percentage transmitting power from the drop-down menu
WMM	Select this check box to enable or disable wireless multi media
Total MAX Users	Enter the total number of MAX users
SSID Select	Choose the SSID from the drop-down menu
SSID Name	Enter the SSID name
Enable SSID	Enable or disable SSID from this drop-down menu
SSID Broadcast	Enable or disable SSID broadcast from this drop-down menu
MAX Users	Enter the number of MAX users
Encryption Mode	Choose an encryption mode from the drop-down menu: • OPEN • WEP • WPA/WPA2 Personal • WPA/WPA2 Enterprise
WPA Version	Choose a WPA version from the drop-down menu: • WPA1 • WPA2 • WPA1/WPA2
WPA Encryption Mode	Choose a WPA encryption mode from the drop-down menu: • TKIP • AES • TKIP/AES
WPA Key	Enter the WPA key
Enable WPS	Enable or disable WPS from this drop-down menu
WPS Mode	Select a WPS mode from the drop-down menu: PBC (Push Button Connect) or PIN (Personal Identification Number)

2 Configure the WiFi connection.

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

4 Click Save.

5 STOP. This procedure is complete.

Procedure 18 Wireless 5G networking configuration

1 Select Network > Wireless 5GHz from the top-level menu in the Ethernet Gateway window, as shown in Figure 25.

Figure 25 **Wireless 5GHz network window**

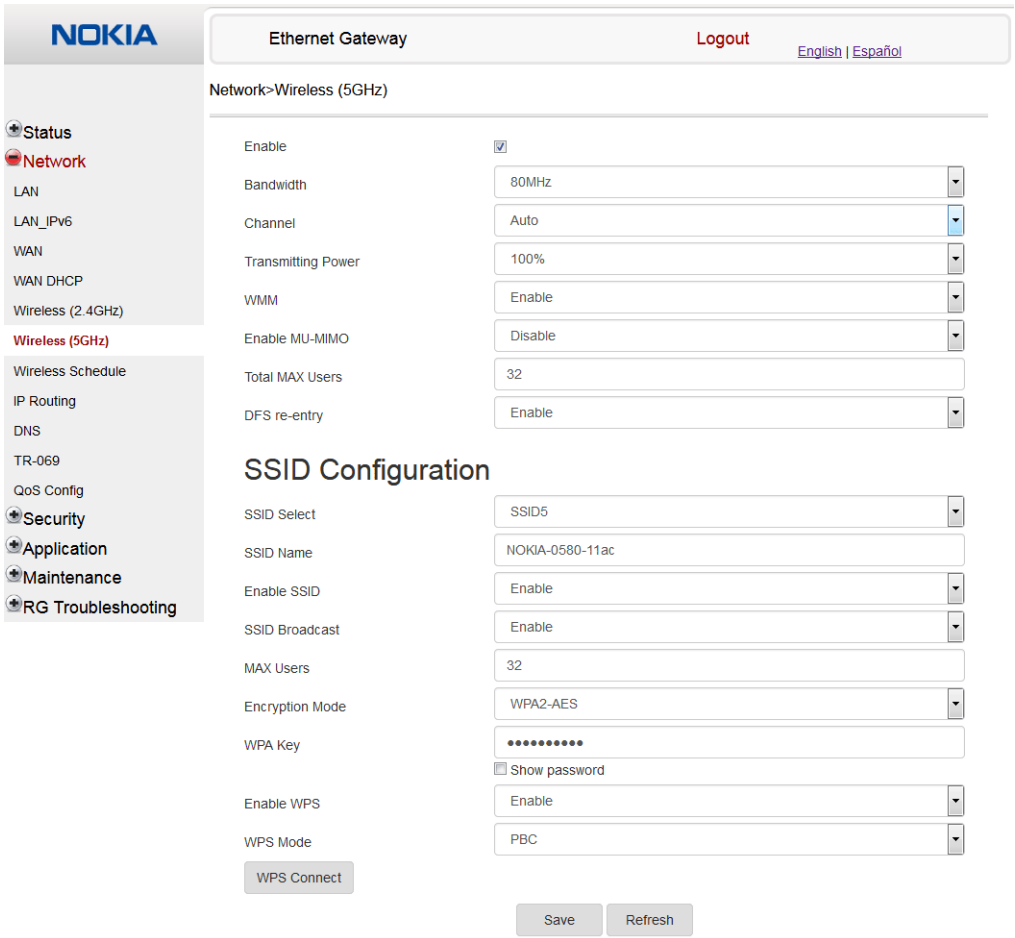


Table 25 describes the fields in the Wireless 5GHz network window.

Table 25 Wireless 5GHz network parameters

Field	Description
Enable	Select this check box to enable WiFi
Bandwidth	Choose from: • 20 MHz • 40 MHz • 80 MHz
Channel	Choose a channel from the drop-down menu or choose Auto to have the channel automatically assigned
Transmitting Power	Choose a percentage for the transmitting power from the drop-down menu: • Low (20%) • Medium (40%) • High (60%) • Maximum (100%)
WMM	Select this check box to enable or disable wireless multi media
Enable MU-MIMO	Choose Enable or disable MU-MIMO from this drop-down menu The default is Enable, which enables users and wireless terminals to communicate with each other. MU-MIMO may decrease WiFi performance for clients who do not support it, in which case Nokia recommends that you choose Disable.
Total MAX Users	Enter the total number of MAX users
DFS re-entry	Select this check box to enable or disable DFS re-entry
SSID Select	Choose the SSID from the drop-down menu
SSID Name	Change the name of the selected SSID
Enable SSID	Choose Enable or disable SSID from this drop-down menu
SSID Broadcast	Choose Enable or disable SSID broadcast from this drop-down menu
MAX Users	Enter the number of MAX users
Encryption Mode	Choose an encryption mode from the drop-down menu: • OPEN • WEP • WPA/WPA2 Personal • WPA/WPA2 Enterprise (1)(2)
WPA Key	Enter the WPA key
Enable WPS	Choose Enable or disable WPS from this drop-down menu

Notes

(1) When Encryption Mode is set to “WPA/WPA2 Enterprise”, the following options are no longer available: WPA version, WPA encryption mode, WPA key, Enable WPS, WPS mode.

(2) When Encryption Mode is set to “WPA/WPA2 Enterprise”, the following options become available: Primary RADIUS server, port and password; Secondary RADIUS server, port, and password; RADIUS accounting port.

2 Configure the Wireless connection.

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

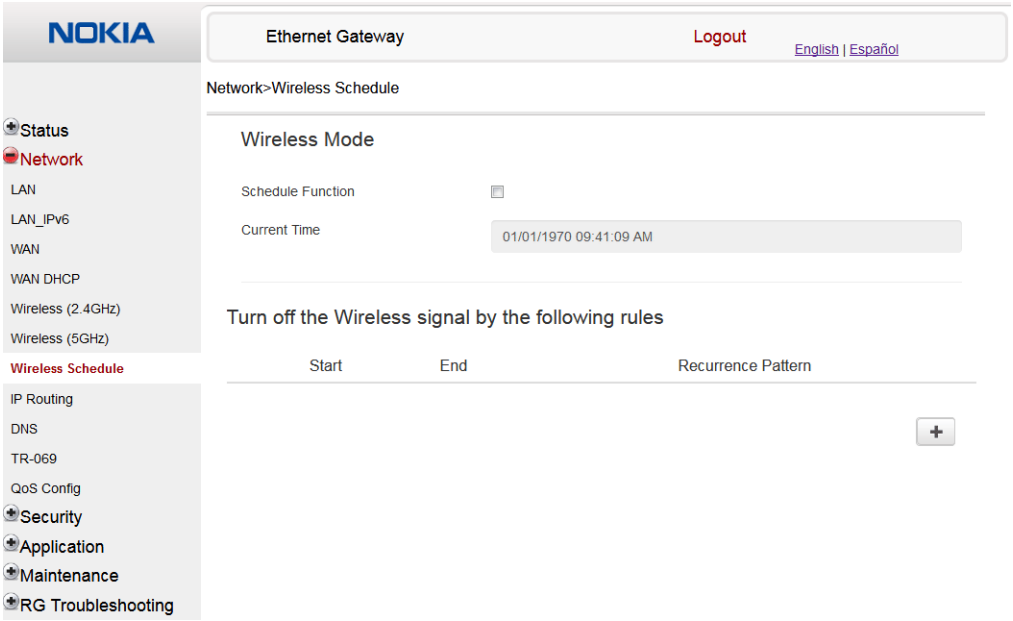
4 Click Save.

5 STOP. This procedure is complete.

Procedure 19 Wireless scheduling

1 Select Network > Wireless Schedule from the top-level menu in the Ethernet Gateway window, as shown in Figure 26.

Figure 26 **Wireless Schedule window**



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

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

A separate panel appears for configuring wireless schedule rules.

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

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

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

The Recurrence Pattern shows the rules created to date.

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

8 Click Save Changes.

9 STOP. This procedure is complete.

Procedure 20 IP Routing

1 Select Network > IP Routing from the top-level menu in the Ethernet Gateway window, as shown in Figure 27.

Figure 27 **IP Routing window**

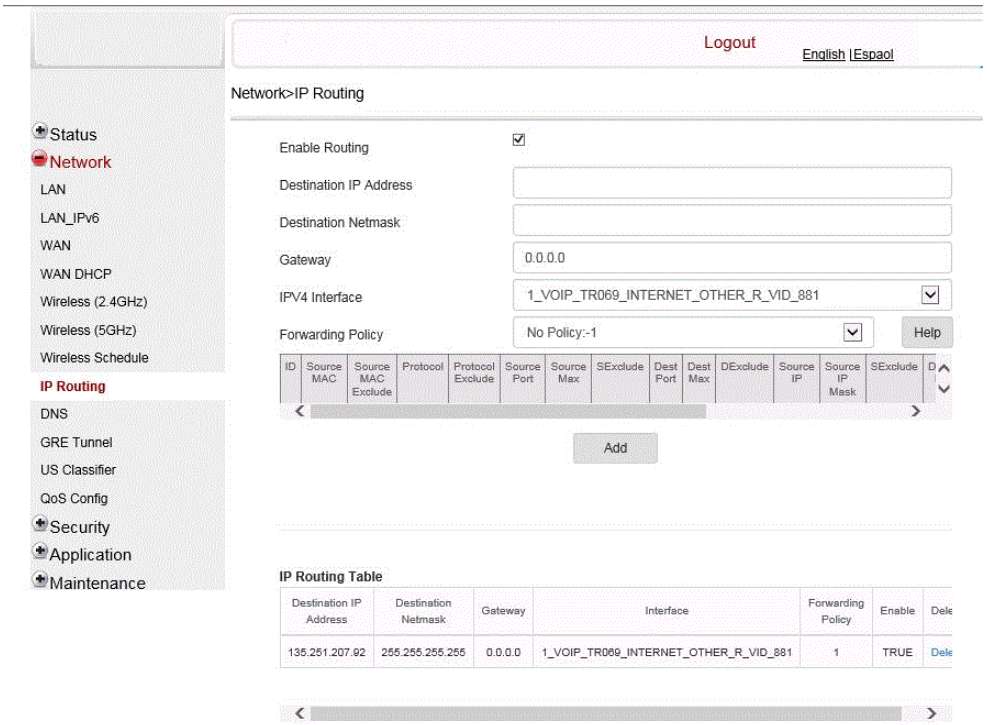


Table 27 describes the fields in the IP Routing window.

Table 26 **IP Routing parameters**

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

2 Enter the routing information.

3 Click Add.

4 STOP. This procedure is complete.

Procedure 21 DNS configuration

1 Select Network > DNS from the top-level menu in the Ethernet Gateway window, as shown in Figure 28.

Figure 28 **DNS network window**

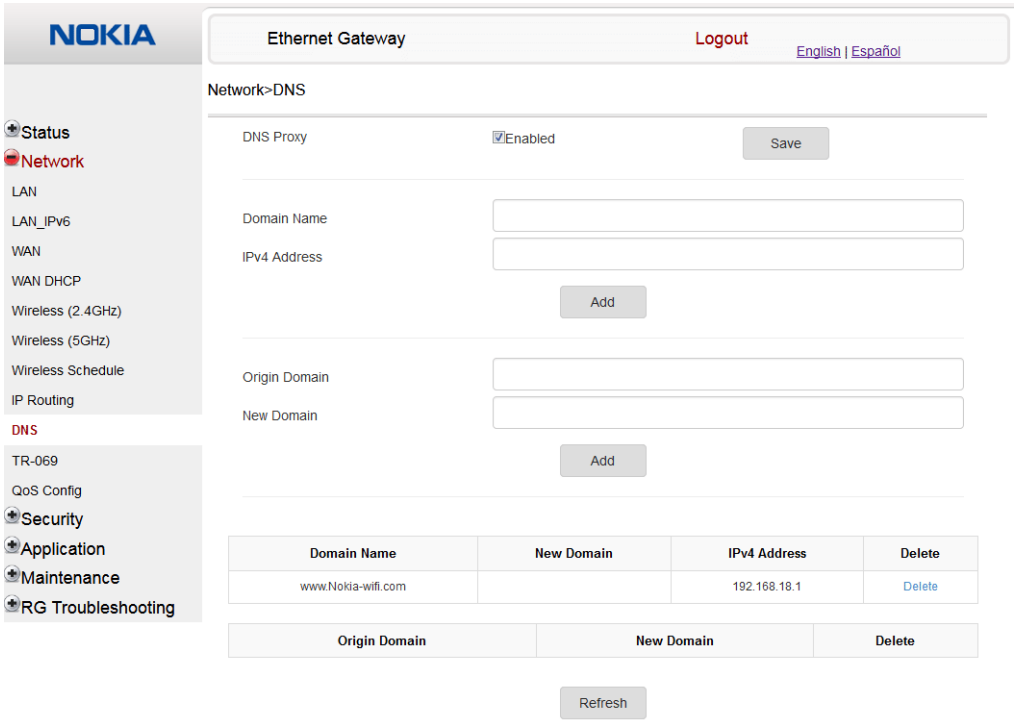


Table 27 describes the fields in the DNS network window.

Table 27 **DNS network parameters**

Field	Description
DNS Proxy	Select this check box to enable DNS proxy
Domain Name	Domain name
IPv4 Address	Domain IP address
Origin Domain	Origin domain name
New Domain	New domain name

2 Enter the domain name and IP address and click Add.

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

4 STOP. This procedure is complete.

Procedure 22 TR-069 configuration

1 Select Network > TR-069 from the top-level menu in the Ethernet Gateway window, as shown in Figure 29.

Figure 29 **TR-069 network window**

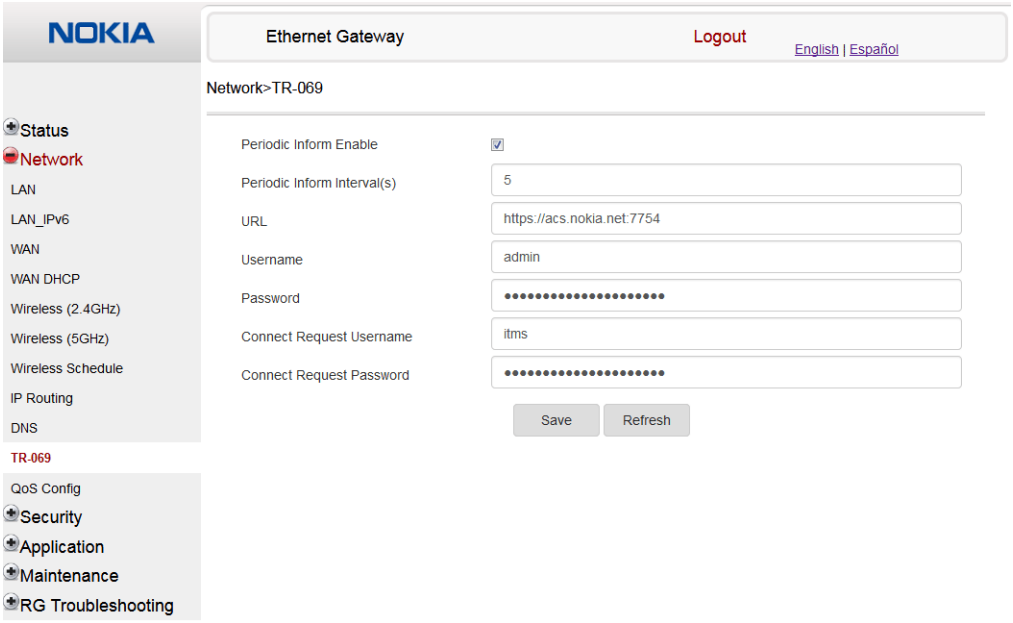


Table 28 describes the fields in the TR-069 network window.

Table 28 **TR-069 network parameters**

Field	Description
Periodic Inform Enable	Select this check box to enable periodic inform updates
Periodic Inform Interval(s)	Time between periodic inform updates, in seconds
URL	URL of the auto-configuration server
Username	Username used to log in to the Gateway 3 (G-240W-E)

(1 of 2)

Field	Description
Password	Password used to log in to the Gateway 3 (G-240W-E)
Connect Request Username	Username used to log in to the auto-configuration server
Connect Request Password	Password used to log in to the auto-configuration server

(2 of 2)

2 Configure TR-069 by entering the required information.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 23 QoS configuration

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

Figure 30 shows the window for configuring QoS L2 (Layer 2 packet sizes).

Figure 30 **QoS Config window (L2)**

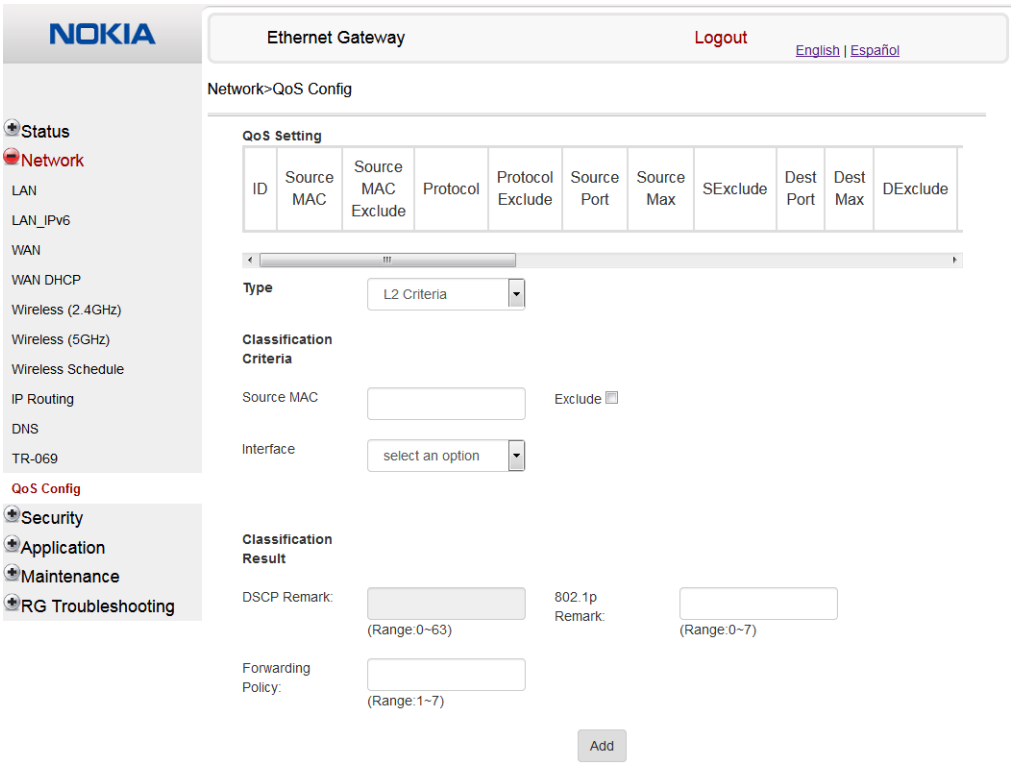


Figure 31 shows the window for configuring QoS L3 (Layer 3 packet sizes).

Figure 31 **QoS Config window (L3)**

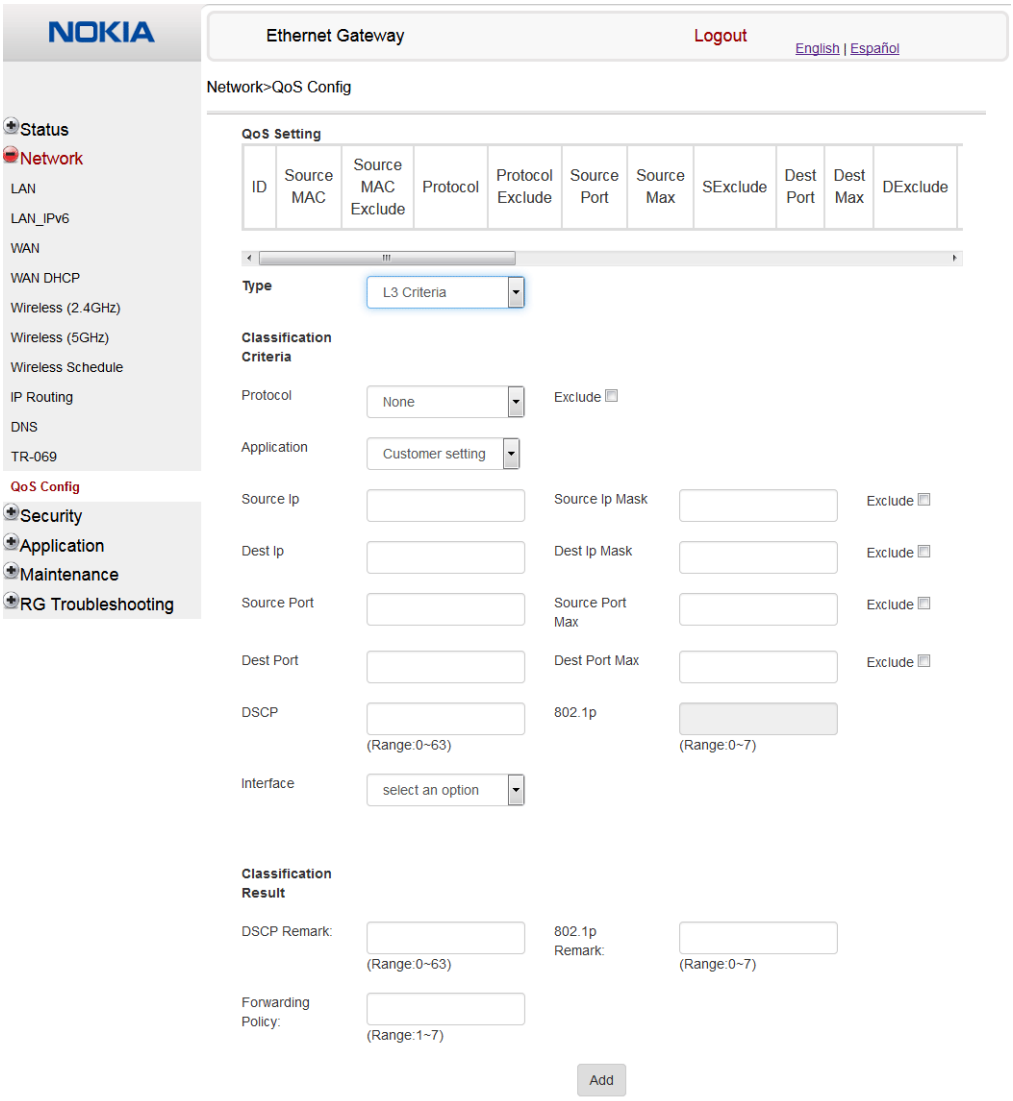


Table 29 describes the fields in the QoS Config window.

Table 29 **QoS Config parameters**

Field	Description
Type	Choose a QoS service layer type from the drop-down menu, either L2 or L3.
Source MAC	Enter the source MAC. Select the Exclude check box to exclude the source MAC

(1 of 2)

Field	Description
Interface	Choose an interface from the drop-down menu
DSCP Remark	Enter the value for the DSCP mark (range: 0-63); valid only for L3 Criteria
802.1p Mark	Enter the value for the 802.1p (range: 0-7)
Forwarding Policy	Enter the number for the forwarding policy (range: 1-7)
Additional fields for L3	
Protocol	Choose a protocol from the drop-down menu, or select the Exclude check box
Application	Choose an application from the drop-down menu
Source IP and Source IP Mask	Enter the values for the source IP and IP mask, or select the Exclude check box
Destination IP and Destination IP Mask	Enter the values for the destination IP and IP mask, or select the Exclude check box
Source Port and Source Port Max	Enter the values for the source port and port max (highest port number) or select the Exclude check box
Destination Port and Destination Port Max	Enter the values for the destination port and port max (highest port number), or select the Exclude check box

(2 of 2)

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

3 Configure a QoS policy.

4 Click Add to add a QoS policy.

5 STOP. This procedure is complete.

8.1.4 Security configuration

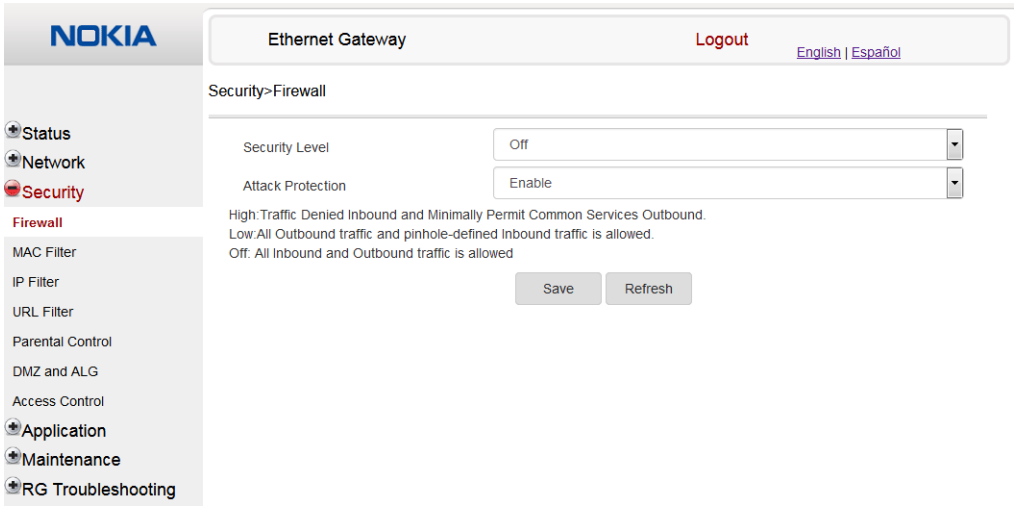
The Gateway 3 (G-240W-E) also supports security configuration, including:

- Firewall
- MAC Filter
- IP Filter
- URL Filter
- Parental Control
- DMZ and ALG
- Access Control

Procedure 24 Firewall configuration

1 Select Security > Firewall from the top-level menu in the Ethernet Gateway window, as shown in Figure 32.

Figure 32 **Firewall window**



Firewall security applies only to services provided by the Gateway 3 (G-240W-E). Internet access from the LAN side is not affected by this firewall.

Three security levels are available: Off, Low, and High.

At the Off level, no firewall security is in effect,

At the Low level, pre-routing is supported: port forwarding, DMZ, host application, and host drop. Also supported are application services: DDNS, DHCP, DNS, H248, IGMP, NTP client, SSH, Telnet, TFTP, TR-069, and VoIP. The following types of ICMP messages are permitted: echo request and reply, destination unreachable, and TTL exceeded. Other types of ICMP messages are blocked. DNS proxy is supported from LAN to WAN but not from WAN to LAN.

At the High level, 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.

Table 30 describes the fields in the firewall window.

Table 30 **Firewall parameters**

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

(1 of 2)

Field	Description
Attack Protection (Protection against DoS or DDoS attacks)	Choose enable or disable attack protect from the drop-down menu The default is disable

(2 of 2)

2 Configure the firewall.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 25 MAC filter configuration

1 Select Security > MAC Filter from the top-level menu in the Ethernet Gateway window, as shown in Figure 33.

Figure 33 **MAC filter window**

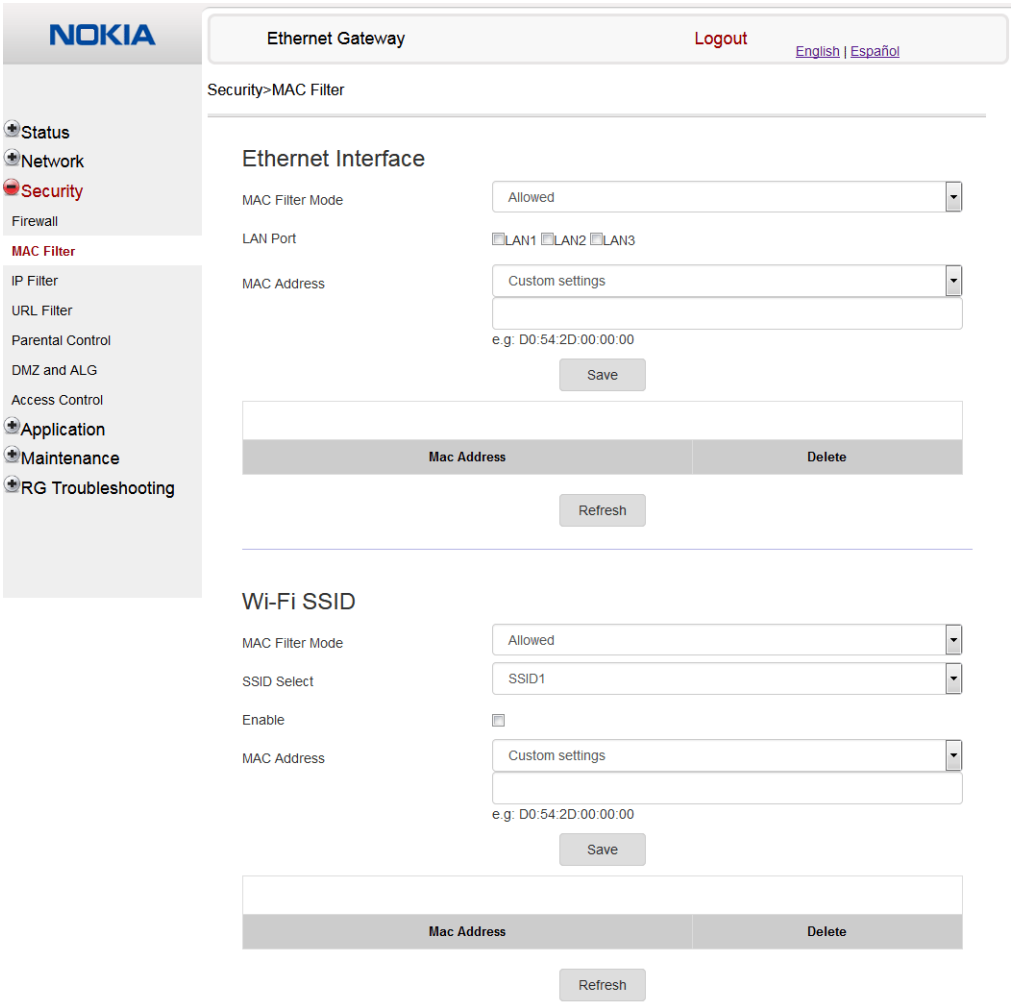


Table 31 describes the fields in the MAC filter window.

Table 31 **MAC filter parameters**

Field	Description
Ethernet Interface	

(1 of 2)

Field	Description
MAC Filter Mode	Choose the MAC filter mode from this drop-down menu: Blocked or Allowed
LAN Port	Select the check boxes for the LAN ports
MAC Address	Choose a MAC address from the drop-down menu or enter the address in the text field
WiFi SSID	
MAC Filter Mode	Choose the MAC filter mode from this drop-down menu: Blocked or Allowed
SSID Select	Choose an SSID option from the drop-down menu
Enable	Select this check box to enable MAC filtering for WiFi SSID
MAC Address	Choose a MAC address from the drop-down menu or enter the address in the text field

(2 of 2)

2 Configure a MAC filter for the Ethernet interface.

3 Click Save.

4 If desired, select a MAC address and click the Delete column to delete a MAC address.

5 Click Refresh to update the information.

6 Configure a MAC filter for WiFi SSID (WLAN MAC filter).

7 Click Save.

8 STOP. This procedure is complete.

Procedure 26 IP filter configuration

1 Select Security > IP filter from the top-level menu in the Ethernet Gateway window, as shown in Figure 34.

Figure 34 **IP filter window**

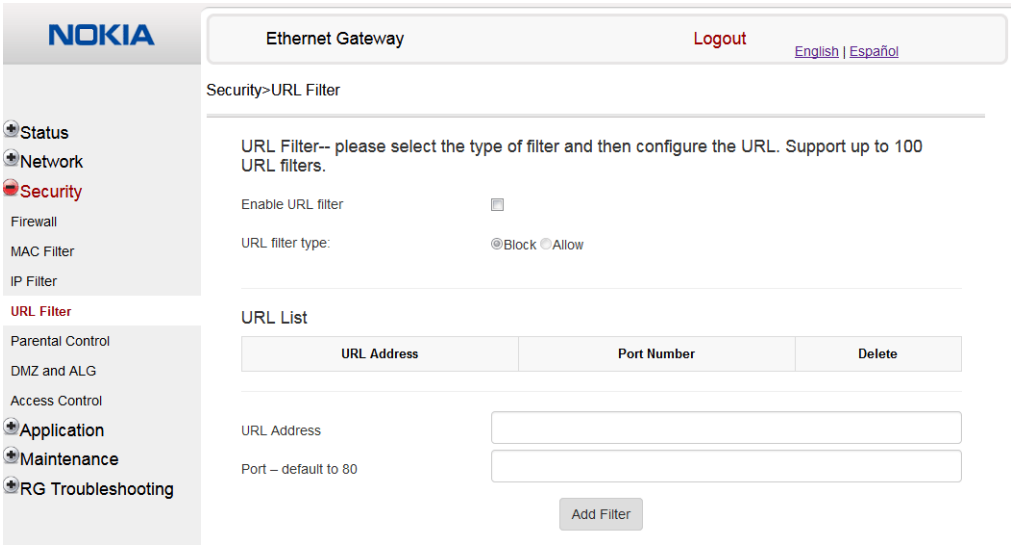


Table 32 describes the fields in the IP filter window.

Table 32 **IP filter parameters**

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

2 Configure the IP filter.

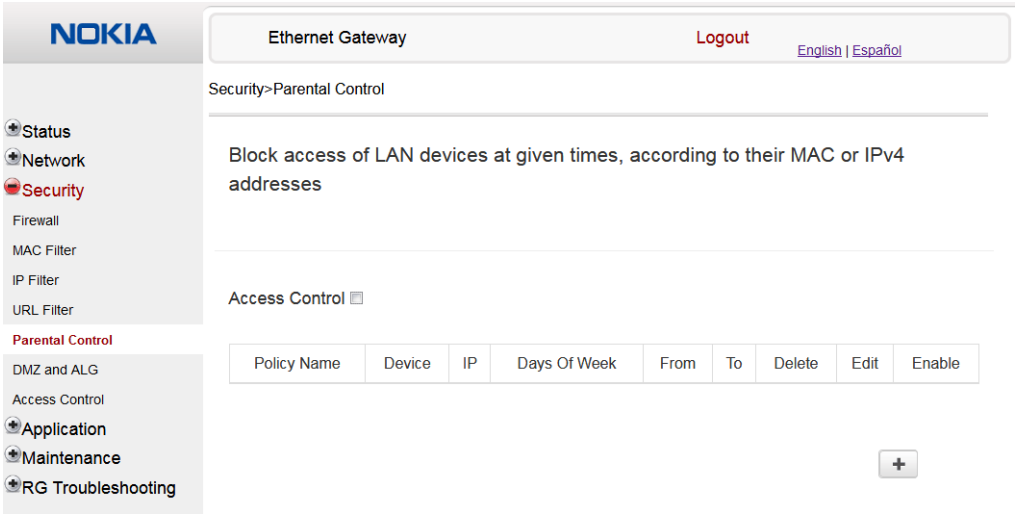
3 Click Add.

4 STOP. This procedure is complete.

Procedure 27 URL filter configuration

1 Select Security > URL Filter from the top-level menu in the Ethernet Gateway window, as shown in Figure 35.

Figure 35 **URL Filter window**



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

Table 33 describes the fields in the URL Filter window.

Table 33 **URL Filter parameters**

Field	Description
Enable URL filter	Select the check box to enable the URL filter
URL filter type	Select the radio button for Block or Allow the URL
URL Address	Enter the URL address

(1 of 2)

Field	Description
Port	Enter the port number; the default is 80

(2 of 2)

2 Configure the URL Filter.

3 Click Add Filter.

4 STOP. This procedure is complete.

Procedure 28 Parental control

1 Select Security > Parent Control from the top-level menu in the Ethernet Gateway window, as shown in Figure 36.

Figure 36 **Parental Control window**

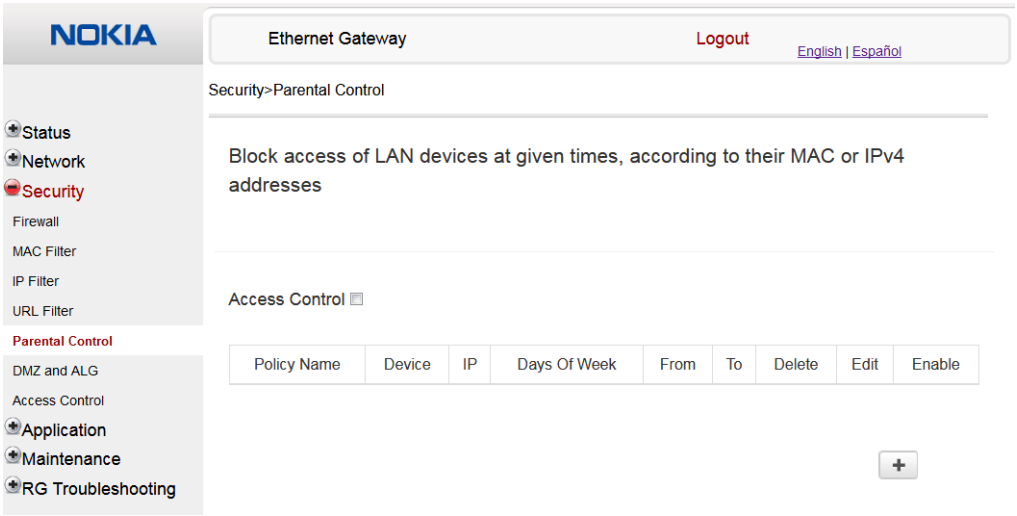


Table 34 describes the fields in the Parental Control window.

Table 34 **Parental control parameters**

Field	Description
Policy Name	Enter a name for the parental control policy or choose a policy from the list

(1 of 2)

Field	Description
Device	The device for which the rule will apply
IP	Enter the IPv4 address for the device or choose an IPv4 address from the list
Days of the week	Choose Every Day, or Individual Days and select the check boxes for the days of the week for which the policy applies
From/To	Enter the times for the policy to be in effect

(2 of 2)

2 Select the Access Control check box.

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

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

4 Configure the parental control policy.

5 Click Enable to activate the policy.

6 STOP. This procedure is complete.

Procedure 29 DMZ and ALG configuration

1 Select Security > DMZ and ALG from the top-level menu in the Ethernet Gateway window, as shown in Figure 37.

Figure 37 **DMZ and ALG window**

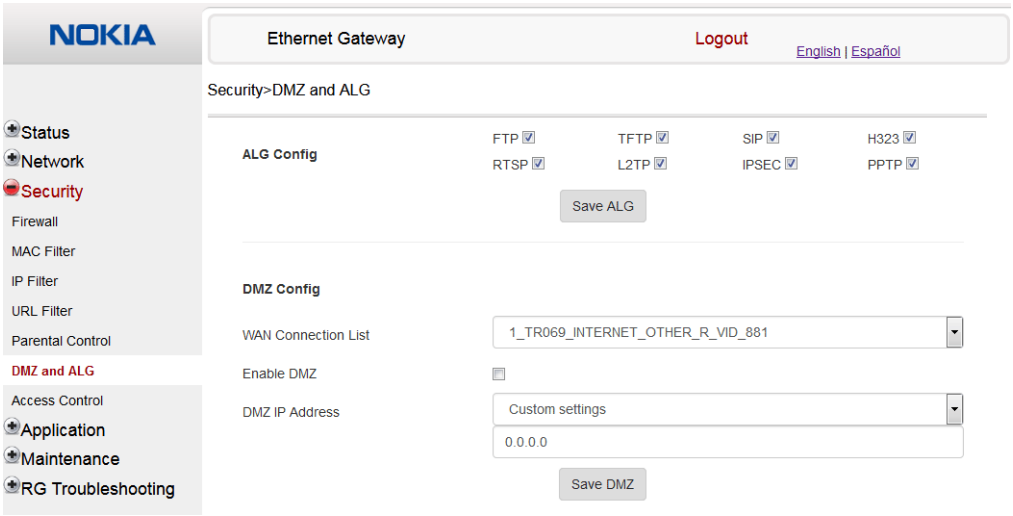


Table 35 describes the fields in the DMZ and ALG window.

Table 35 **DMZ and ALG parameters**

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

2 Configure ALG.

3 Click Save ALG.

4 Configure DMZ.

5 Click Save DMZ.

6 STOP. This procedure is complete.

Procedure 30 Access control configuration

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

Note 1 — ACL takes precedence over the firewall policy.

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

1 Select Security > Access Control from the top-level menu in the Ethernet Gateway window, as shown in Figure 38.

Figure 38 **Access Control window**

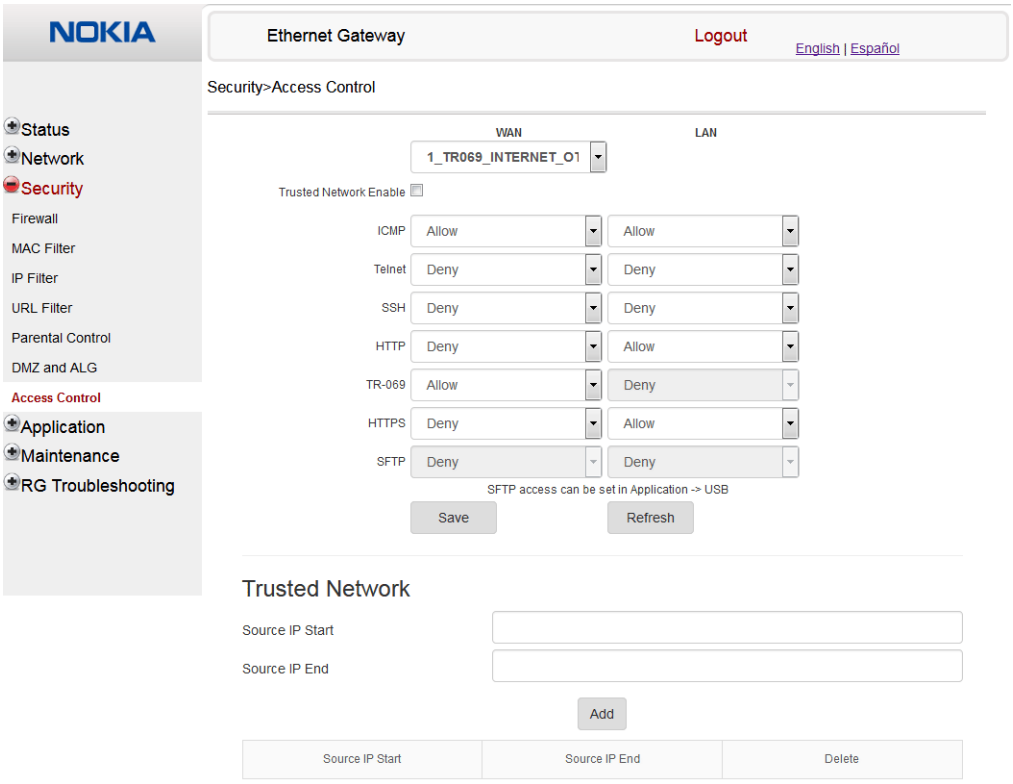


Table 36 describes the fields in the Access Control window.

Table 36 **Access control parameters**

Field	Description
WAN	Choose a connection from the drop-down menu
Trusted Network Enable	Click to enable or disable
ICMP, Telnet, SSH, HTTP, TR-069, HTTPS, SFTP	Select an access control level for each protocol: WAN side: Allow, Deny, or Trusted Network Only LAN side: Allow or Deny
Source IP Start	Enter a start IP address for the new subnet trusted network
Source IP End	Enter an end IP address for the new subnet trusted network

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

3 Click to enable or disable Trusted Network.

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

5 Click Save.

6 Optionally, add one or more subnet trusted networks.

The maximum number of entries is 32.

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

7 STOP. This procedure is complete.

8.1.5 Application configuration

The Gateway 3 (G-240W-E) also supports application configuration, including:

- port forwarding
- port triggering
- DDNS
- NTP
- UPnP and DLNA

Procedure 31 Port forwarding configuration

1 Select Application > Port forwarding from the top-level menu in the Ethernet Gateway window, as shown in Figure 39.

Figure 39 **Port forwarding window**

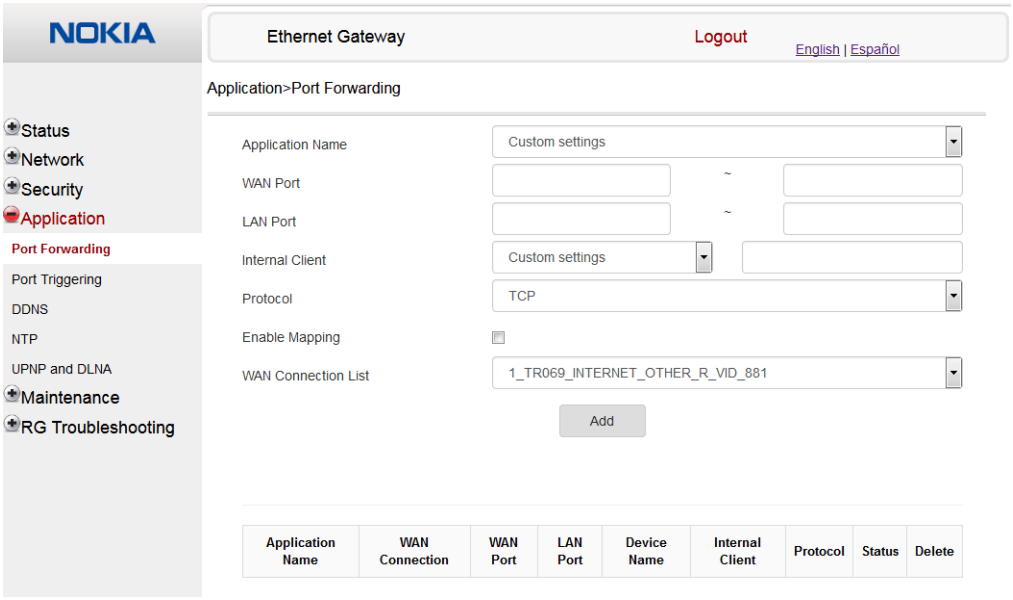


Table 37 describes the fields in the port forwarding window.

Table 37 **Port forwarding parameters**

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

2	Configure port forwarding.
3	Click Add.
4	STOP. This procedure is complete.

Procedure 32 Port triggering

1	Select Application > Port Triggering from the top-level menu in the Ethernet Gateway window, as shown in Figure 40.

Figure 40 **Port Triggering window**

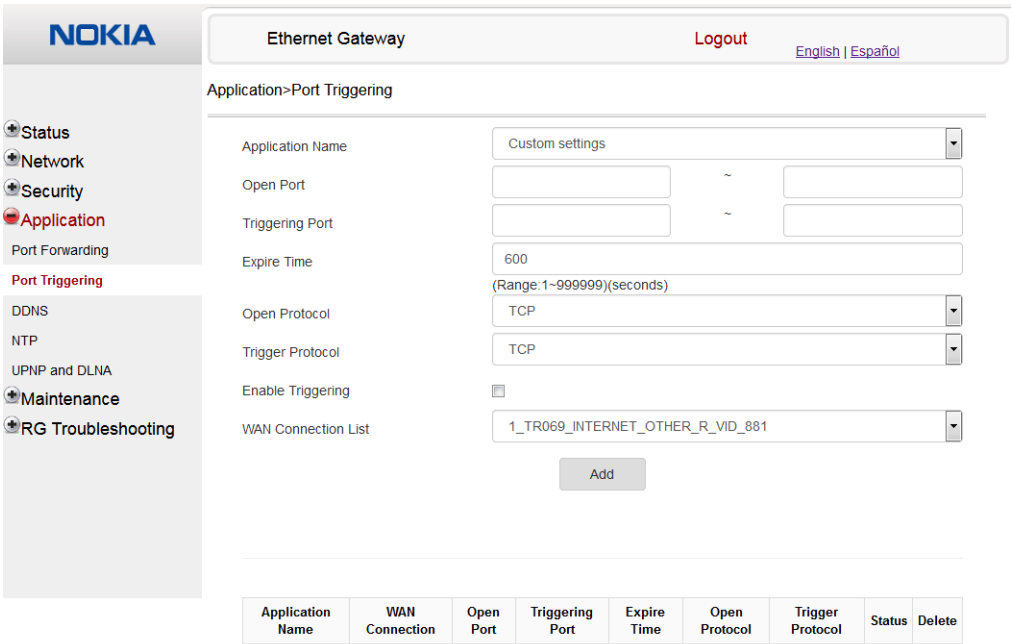


Table 37 describes the fields in the Port Triggering window.

Table 38 **Port triggering parameters**

Field	Description
Application Name	Choose an application name from the drop-down menu
Open Port	Enter the open port range

(1 of 2)

Field	Description
Triggering Port	Enter the triggering port range
Expire Time	Enter the expiration time in seconds
Open Protocol	Choose the open port protocol from the drop-down menu: • TCP • UDP • TCP/UDP
Trigger Protocol	Choose the triggering port protocol from the drop-down menu: • TCP • UDP • TCP/UDP
Enable Triggering	Select this check box to enable port triggering
WAN Connection List	Choose a WAN connection from the drop-down menu Note: only active devices are shown on this menu

(2 of 2)

2 Configure port triggering.

3 Click Add.

4 STOP. This procedure is complete.

Procedure 33 DDNS configuration

1 Select Application > DDNS from the top-level menu in the Ethernet Gateway window, as shown in Figure 41.

Figure 41 **DDNS window**

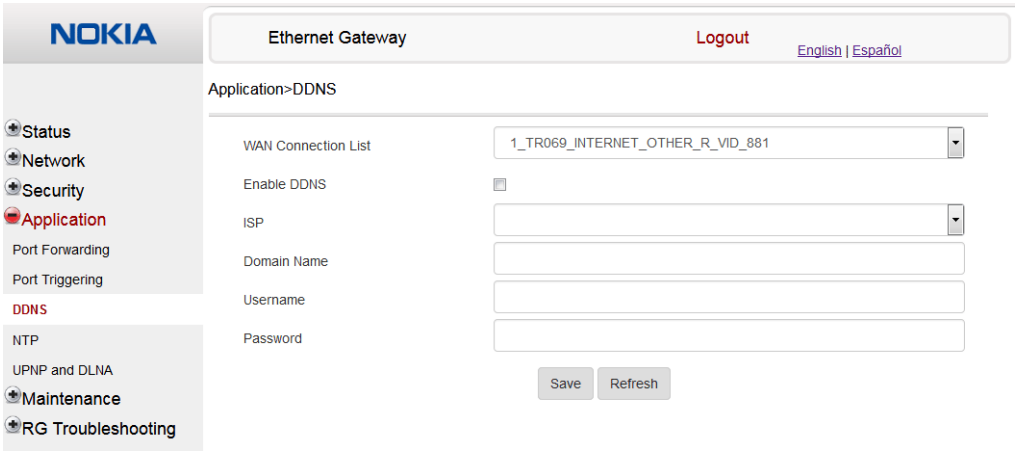


Table 39 describes the fields in the DDNS window.

Table 39 **DDNS parameters**

Field	Description
WAN Connection List	Choose a WAN connection from the drop-down menu
Enable DDNS	Select this check box to enable DDNS on the chosen WAN connection
ISP	Choose an ISP from the drop-down menu.
Domain Name	Enter the domain name for the DDNS server
Username	Enter the DDNS username
Password	Enter the DDNS password

2 Configure DDNS.

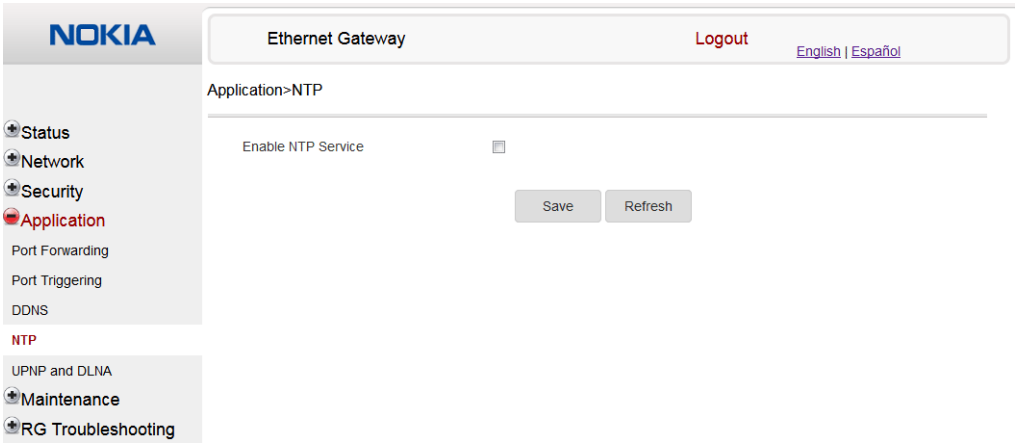
3 Click Save.

4 STOP. This procedure is complete.

Procedure 34 NTP configuration

1 Select Application > NTP from the top-level menu in the Ethernet Gateway window, as shown in Figure 42.

Figure 42 **NTP window**



2 Select the Enable NTP Service check box.

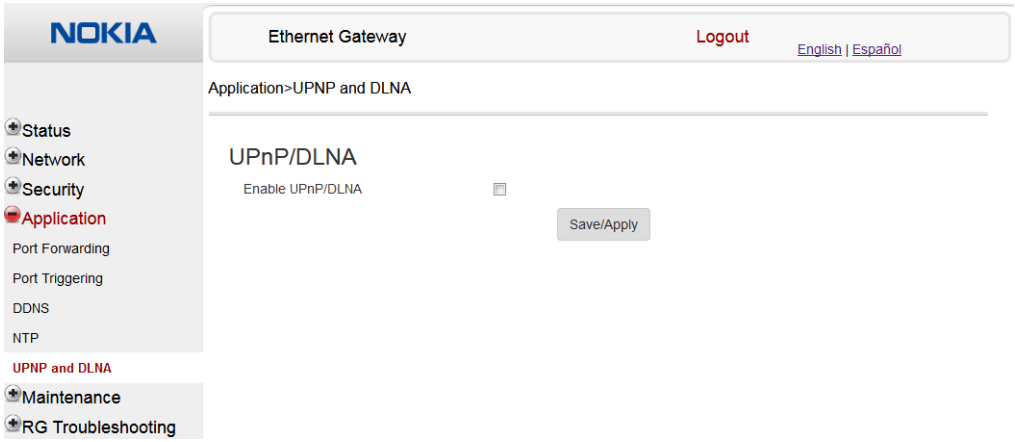
3 Click Save.

4 STOP. This procedure is complete.

Procedure 35 UPnP and DLNA configuration

1 Select Application > UPnP and DLNA from the top-level menu in the Ethernet Gateway window, as shown in Figure 43.

Figure 43 **UPnP and DLNA window**



2 Select the Enable UPnP check box to enable UPnP.

3 Click Save/Apply.

4 STOP. This procedure is complete.

8.1.6 Maintenance

The Gateway 3 (G-240W-E) supports maintenance tasks, including:

- Password change
- Device Management
- Backup and Restore
- Firmware Upgrade
- Device Reboot
- Restore Factory Defaults
- Diagnostics
- View Logs

Procedure 36 Password configuration

A password must adhere to the following password rules:

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

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

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

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

1 Select Maintenance > Password from the top-level menu in the GPON Home Gateway window, as shown in Figure 44.

Figure 44 **Password window**

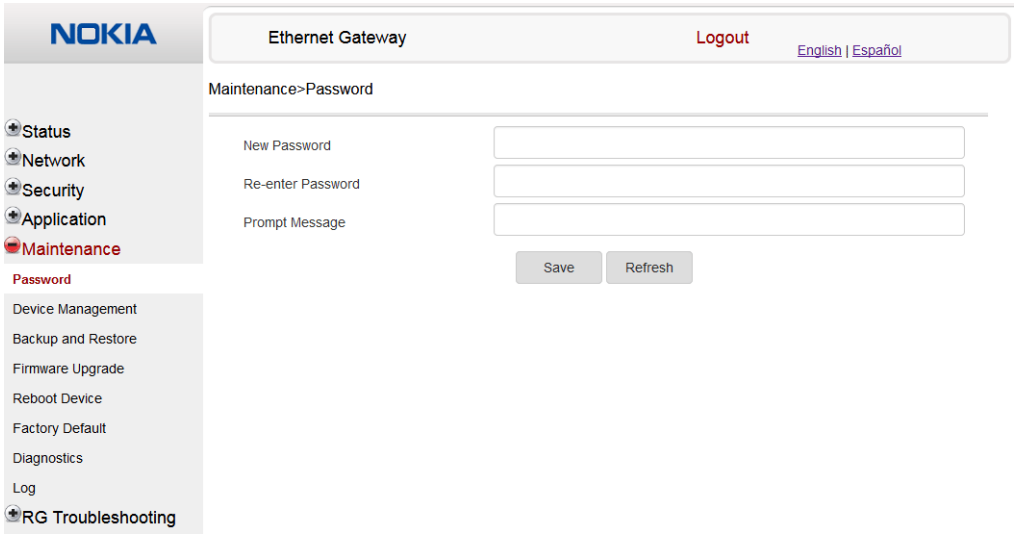


Table 40 describes the fields in the password window.

Table 40 **Password parameters**

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

2 Configure the new password.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 37 Device management

1 Select Maintenance > Device Management from the top-level menu in the Ethernet Gateway window, as shown in Figure 45.

Figure 45 **Device Management window**

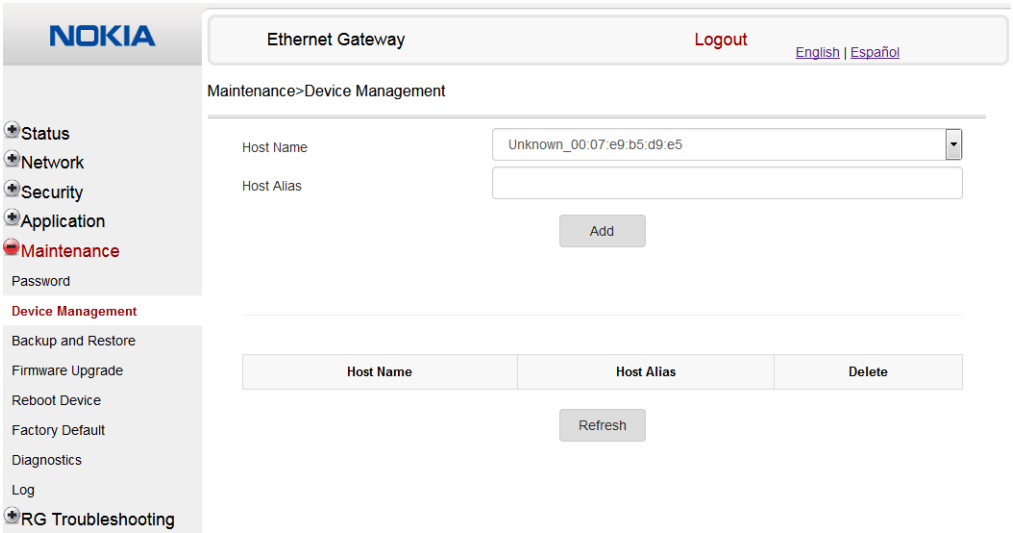


Table 41 describes the fields in the Device Management window.

Table 41 **Device Management parameters**

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

2 Configure an alias for a specific host.

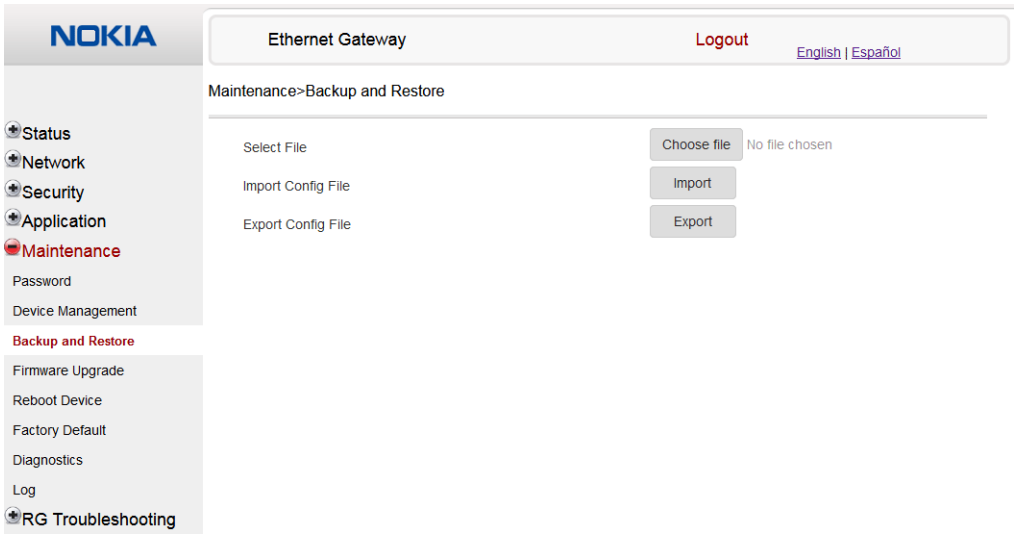
3 Click Add.

4 STOP. This procedure is complete.

Procedure 38 Backup and Restore

1 Select Maintenance > Backup and Restore from the top-level menu in the Ethernet Gateway window, as shown in Figure 46.

Figure 46 **Backup and Restore window**



2 Click Select File and choose the backup file.

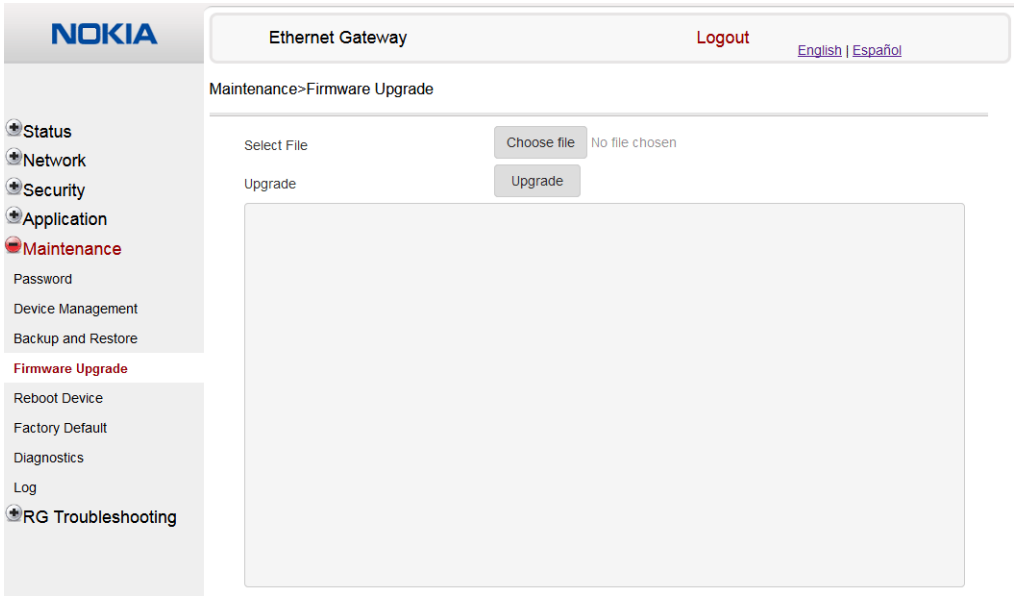
3 Click Import Config File to restore the Gateway 3 (G-240W-E) to the saved backup or click Export Config File to export the current configuration to the backup file.

4 STOP. This procedure is complete.

Procedure 39 Upgrade firmware

1 Select Maintenance > Firmware Upgrade from the top-level menu in the Ethernet Gateway window, as shown in Figure 47.

Figure 47 **Firmware Upgrade window**



2 Click Select File and choose the new firmware file.

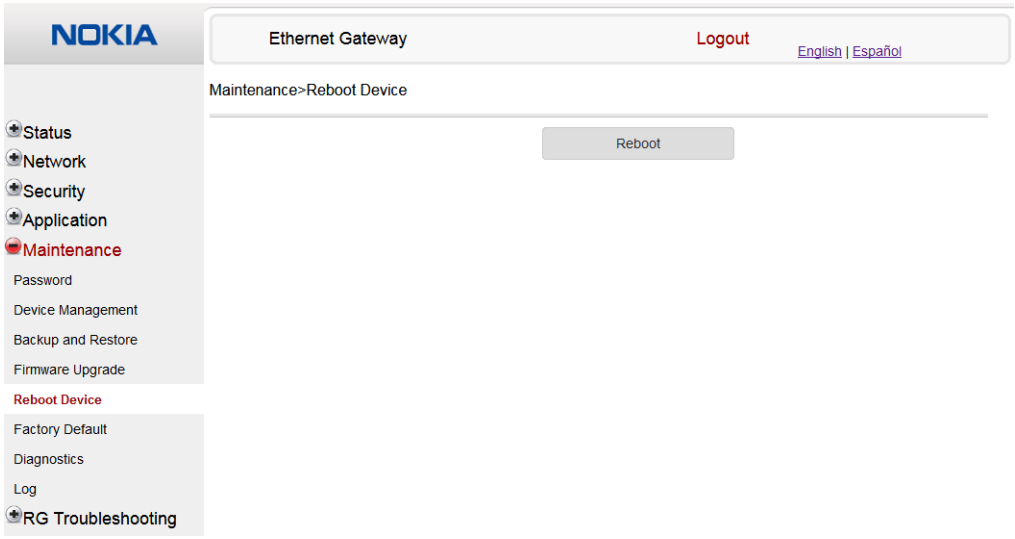
3 Click Upgrade to upgrade the firmware.

4 STOP. This procedure is complete.

Procedure 40 Reboot

1 Select Maintenance > Reboot Device from the top-level menu in the Ethernet Gateway window, as shown in Figure 48.

Figure 48 **Reboot Device window**



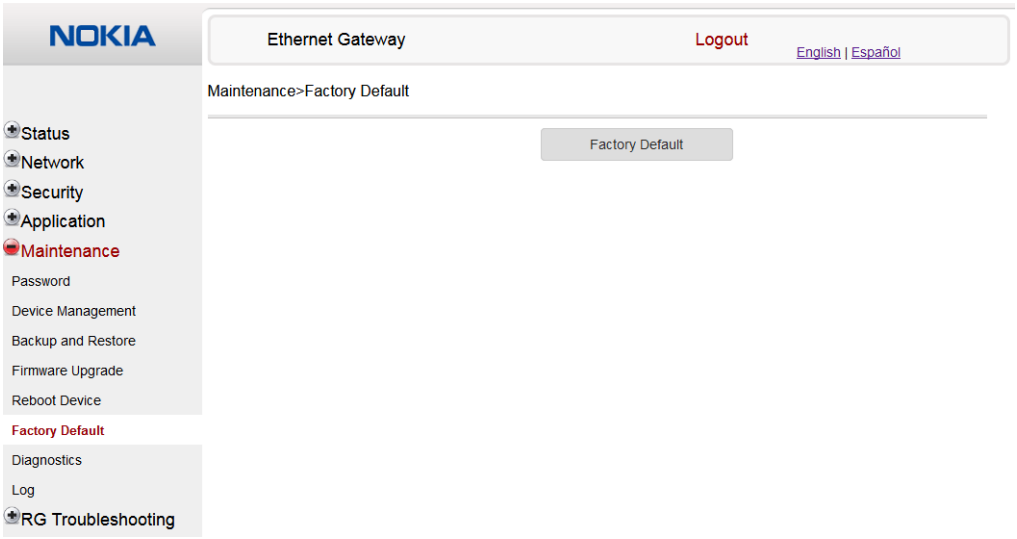
2 Click Reboot to reboot the Gateway 3 (G-240W-E).

3 STOP. This procedure is complete.

Procedure 41 Restore factory defaults

1 Select Maintenance > Factory Default from the top-level menu in the Ethernet Gateway window, as shown in Figure 49.

Figure 49 **Factory Default window**



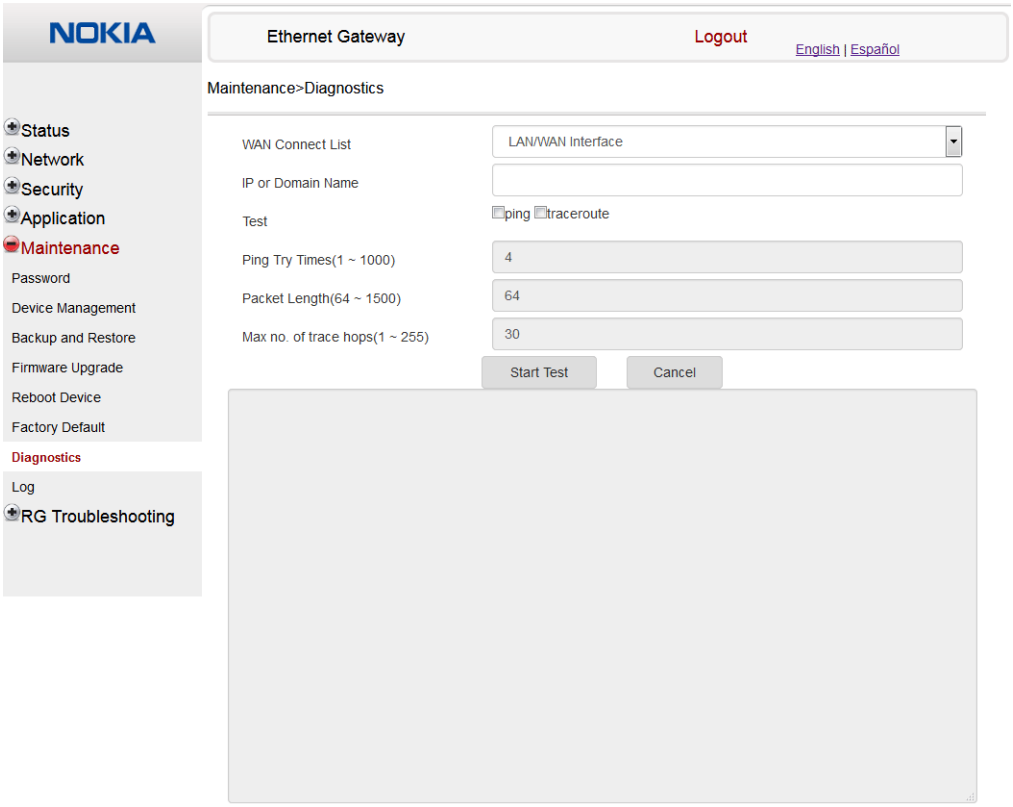
2 Click Factory Default to reset the Gateway 3 (G-240W-E) to its factory default settings.

3 STOP. This procedure is complete.

Procedure 42 Diagnose connections

1 Select Maintenance > Diagnostics from the top-level menu in the Ethernet Gateway window, as shown in Figure 50.

Figure 50 **Diagnostics window**



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

3 Enter the IP address or domain name.

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

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

6 Enter a ping packet length (64 to 1500); the default is 64.

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

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

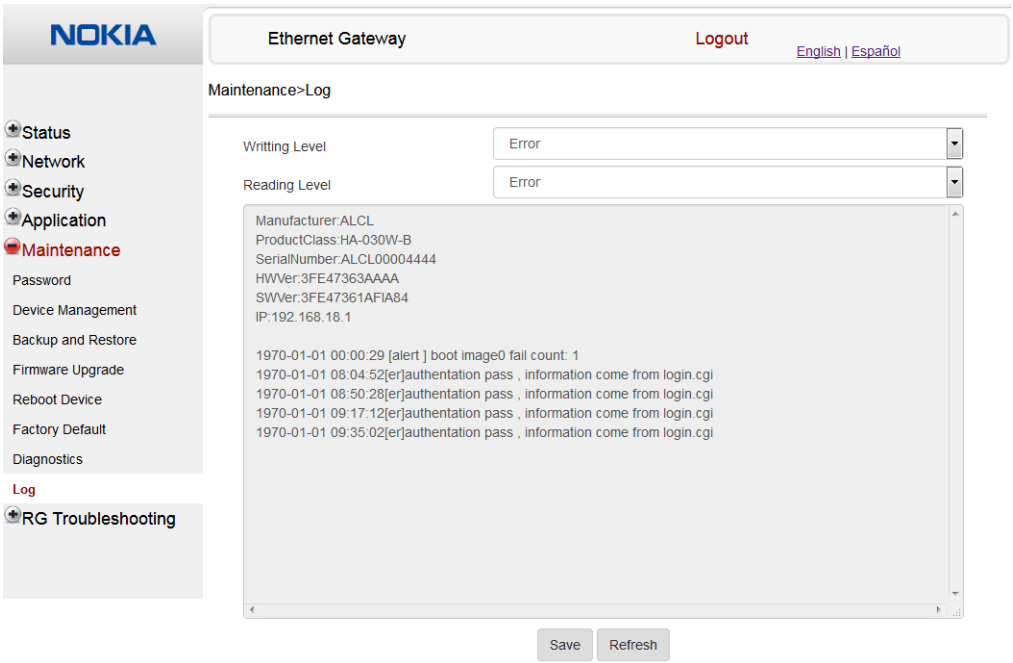
9 Click Cancel to cancel the test.

10 STOP. This procedure is complete.

Procedure 43 View log files

1 Select Maintenance > Log from the top-level menu in the Ethernet Gateway window, as shown in Figure 51.

Figure 51 **Log window**



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

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

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

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

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

5 STOP. This procedure is complete.

8.1.7 RG troubleshooting counters

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

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

Procedure 44 Retrieve Residential Gateway (RG) troubleshooting counters

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

The RG Troubleshooting Counters window appears; see Figure 52.

Figure 52 **RG Troubleshooting Counters window**

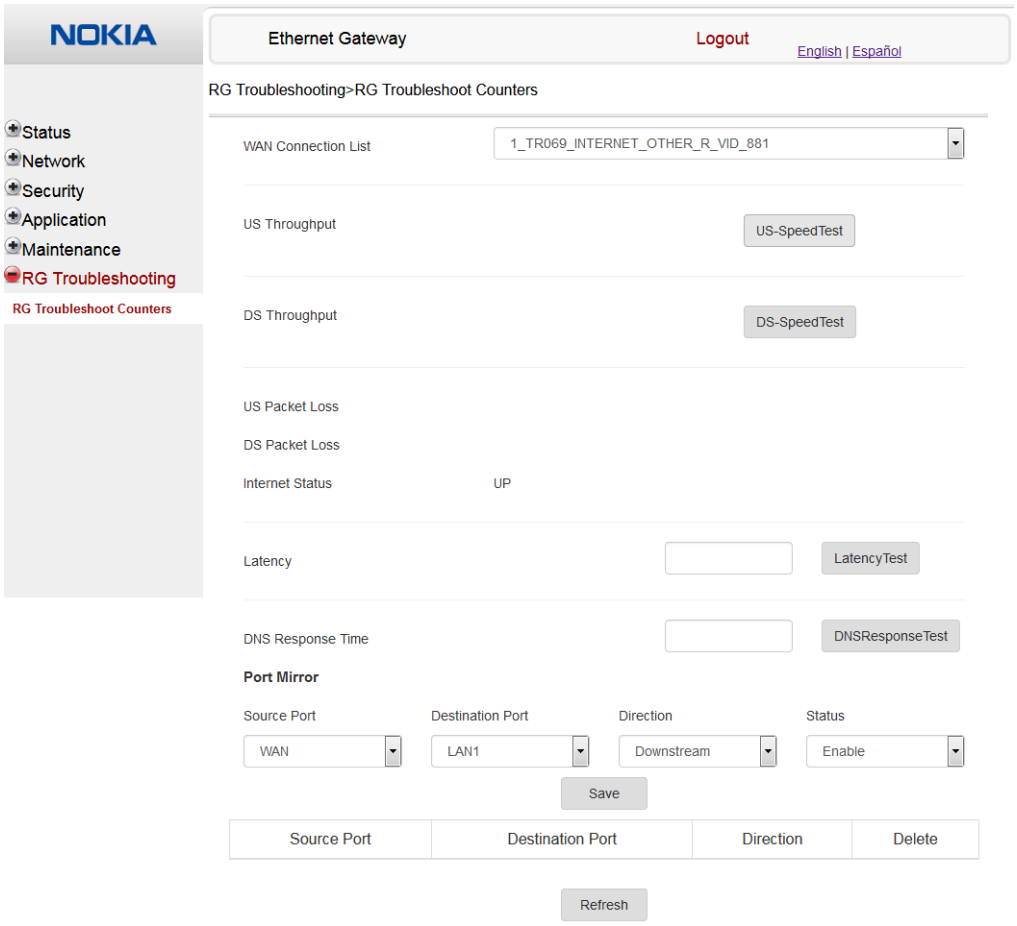


Table 42 describes the fields in the RG Troubleshooting Counters window.

Table 42 **RG Troubleshooting Counters parameters**

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

(1 of 2)

Field	Description
DS Packet Loss	The number of downstream packages lost
Internet Status	Whether the broadband connections is active (UP) or not (DOWN)
Latency	This test is used to determine the lowest round-trip time in milliseconds by pinging the target server multiple times Click Latency Test to specify the time for the test The default is weekly, performed at idle to a public server
DNS Response Time	This test is used to determine the lowest round-trip time in milliseconds by sending a request to the target DNS server Click DNS Response Test to specify the time for the test The default is weekly, performed at idle to a public server
Port Mirror	Select Source Port, Destination Port, Direction (Up or Down) and Status (Enable or Disable)

(2 of 2)

2 Configure the test times if desired.

3 Click Refresh to update the data.

4 STOP. This procedure is complete.

Customer document and product support

Customer documentation

Customer Documentation Welcome Page

Technical Support

Customer Documentation Technical Support

Documentation feedback

Customer Documentation Feedback

3FE-47464-AAAA-TCZZA