NOKIA

7368 Intelligent Services Access Manager ONT

7368 ISAM ONT E-240W-A Product Guide

3FE-46974-AAAA-TCZZA

Issue: 01

1 Preface

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

1.1 Scope

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

1.2 Audience

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

1.3 Required knowledge

The reader must be familiar with general telecommunications principles.

1.4 Acronyms and initialisms

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

1.5 Assistance and ordering phone numbers

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

For ordering information, contact your Nokia sales representative.

1.6 Nokia quality processes

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

1.7 Safety information

For safety information, see the appropriate safety guidelines chapter.

1.8 Documents

Documents are available using ALED or OLCS.

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

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

Procedure 2 To access individual documents

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

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

1.9 Special information

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

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

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

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

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

1.9.1 Procedures with options or substeps

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

Procedure 3 Example of options in a procedure

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

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

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

2 You must perform this step.

Procedure 4 Example of required substeps in a procedure

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

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

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

2 You must perform this step.

1.10 Multiple PDF document search

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

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

Procedure 5 To search multiple PDF files for a common term

1 Open Adobe Acrobat Reader.

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

3 Enter the search criteria.

4 Click on the All PDF Documents In radio button.

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

6 Click on the Search button.

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

Table of contents

List of figures

List of tables

2 ETSI ONT safety guidelines

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

2.1 Safety instructions

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

2.1.1 Safety instruction boxes

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

The following is an example of the Danger box.

Danger — Possibility of personal injury.

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

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

The following is an example of the Warning box.

Warning 1 — Possibility of equipment damage.

Warning 2 — Possibility of data loss.

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

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

The following is an example of the Caution box.

Caution 1 — Possibility of service interruption.

Caution 2 — Service interruption.

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

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

The following is an example of the Note box.

Note — Information of special interest.

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

2.1.2 Safety-related labels

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

Table 1 provides sample safety labels on the ONT equipment.

Table 1 **Safety labels**

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

Figure 1 shows the PSE certification.

Figure 1 **PSE certification**

Warning	This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.
警告	VCCI準拠クラスB機器（日本） この機器は、Information Technology EquipmentのVoluntary Control Council for Interference（VCCI）の規格に準拠したクラスB製品です。この機器をラジオやテレビ受信機の近くで使用した場合、混信を発生する恐れがあります。本機器の設置および使用に際しては、取扱い説明書に従ってください。

19841

2.2 Safety standards compliance

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

2.2.1 EMC, EMI, and ESD compliance

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

- ETSI EN 301 489-1 V2.1.1:2017 Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- ETSI EN 301 489-17 V3.1.1: 2017 Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for Broadband Data Transmission Systems
- EN 300-386 V1.5.1: Electromagnetic Compatibility and Radio Spectrum Matters (ERM): Telecommunications Network Equipment; Electromagnetic Compatibility (EMC) requirements
- EN 55032:2015 Class B, Information Technology Equipment, Radio Disturbance Characteristics, limits and methods of measurement
- EN 55024 (2010): Information Technology Equipment, Immunity Characteristics, limits and methods of measurement
- European Council Directive 2004/108/EC

2.2.2 Equipment safety standard compliance

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

2.2.3 Environmental standard compliance

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

2.2.4 Laser product standard compliance

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

2.2.5 Acoustic noise emission standard compliance

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

2.3 Electrical safety guidelines

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

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

Note 2 — The ONTs comply with BS EN 61140.

2.3.1 Power supplies

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

2.3.2 Cabling

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

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

2.3.3 Protective earth

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

2.4 ESD safety guidelines

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

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

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

2.5 Laser safety guidelines

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

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

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

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

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

2.5.1 Laser classification

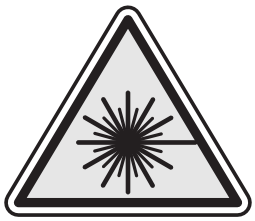
The ONT is classified as a Class 1 laser product based on its transmit optical output.

2.5.1.1 Laser warning labels

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

Figure 2 shows a laser product label.

Figure 2 **Laser product label**



18455

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

Figure 3 **Laser classification label**

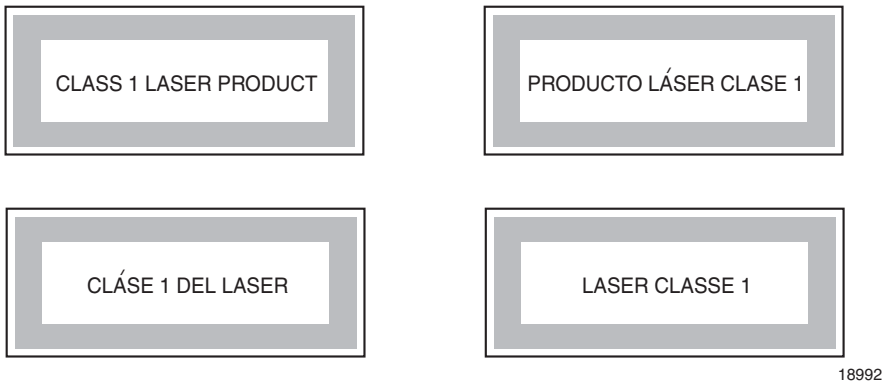
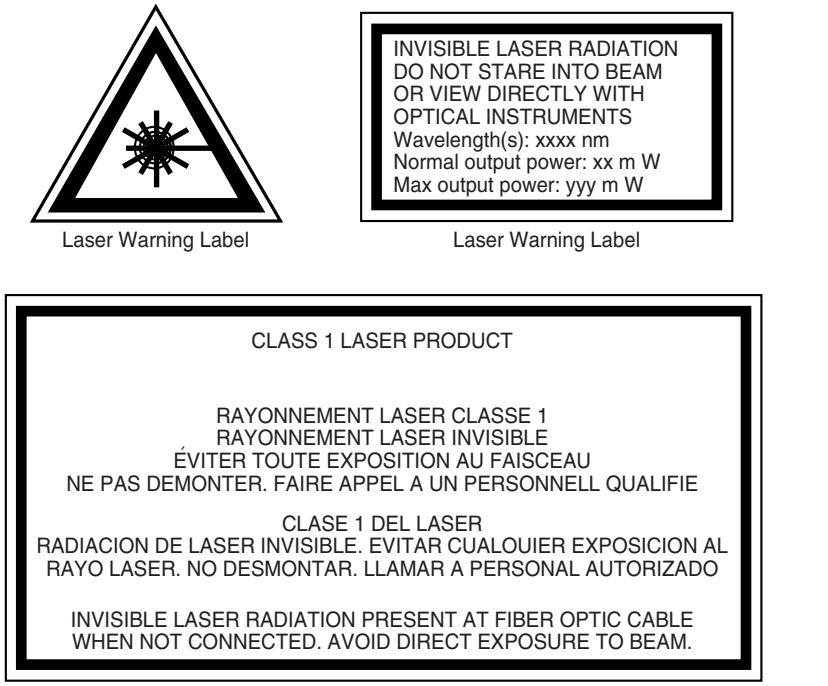


Figure 4 shows a laser warning label and an explanatory label for laser products. Labels and warning may be provided in other languages. The explanatory label provides the following information:

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

Figure 4 **Laser warning labels**



2.5.2 Transmit optical output

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

2.5.3 Normal laser operation

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

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

Danger — Risk of eye damage by laser radiation.

2.5.4 Location class

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

2.6 Environmental requirements

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

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

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

3 ETSI environmental and CRoHS guidelines

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

3.1 Environmental labels

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

3.1.1 Overview

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

3.1.2 Environmental related labels

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

3.1.2.1 Products below Maximum Concentration Value (MCV) label

Figure 5 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 5 **Products below MCV value label**

18986

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

Figure 6 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 6 **Products above MCV value label**

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

3.2 Hazardous Substances Table (HST)

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

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

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

3.3 Other environmental requirements

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

3.3.1 ONT environmental requirements

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

3.3.2 Storage

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

3.3.3 Transportation

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

3.3.4 Stationary use

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

3.3.5 Thermal limitations

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

- operating temperature: -5°C to 45°C (23°F to 113°F)
- short-term temperature: –5°C to 50°C (23°F to 122°F)
- operating relative humidity: 5% to 85%
- short-term relative humidity: 5% to 95%, but not to exceed 0.024 kg of water/kg

3.3.6 Material content compliance

European Union (EU) Directive 2002/95/EC, “Restriction of the use of certain Hazardous Substances” (RoHS), restricts the use of lead, mercury, cadmium, hexavalent chromium, and certain flame retardants in electrical and electronic equipment. This Directive applies to electrical and electronic products placed on the EU market after 1 July 2006, with various exemptions, including an exemption for lead solder in network infrastructure equipment. Nokia products shipped to the EU after 1 July 2006 comply with the EU RoHS Directive.

Nokia has implemented a material/substance content management process. The process is described in: Nokia process for ensuring RoHS Compliance (1AA002660031ASZZA). This ensures compliance with the European Union Directive 2011/65/EU on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS2). With the process equipment is assessed in accordance with the Harmonised Standard EN50581:2012 (CENELEC) on Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances.

3.3.7 End-of-life collection and treatment

Electronic products bearing or referencing the symbol shown in Figure 7, 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 7 **Recycling/take back/disposal of product symbol**

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

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

In compliance with legal requirements and contractual agreements, where applicable, Nokia will offer to provide for the collection and treatment of Nokia products bearing the logo shown in Figure 7 at the end of their useful life, or products displaced by Nokia equipment offers. For information regarding take-back of equipment by Nokia, or for more information regarding the requirements for recycling/disposal of product, contact your Nokia account manager or Nokia take back support at sustainability.global@nokia.com.

4 E-240W-A unit data sheet

4.1 E-240W-A part numbers and identification

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

Table 2 **Identification of E-240W-A indoor ONTs**

Ordering kit part number	Provisioning number	Description	CLEI	CPR	ECI/ Bar code
3FE 46964 CA	3FE 46974 AB	Turbo EPON RGW ONT with 2 POTS ports, 4 10/100/1000 Base-T Ethernet interfaces, 100mW, and 802.11ac 4x4 and 802.11b/g/n 2x2 Wi-Fi radio with on/off switch. This ONT also has 2 USB 2.0 ports. Includes a 12V/3A 3-pin wall-mounted UK power adapter.	—	—	—
3FE 46964 BA	3FE 46974 AB	Turbo EPON RGW ONT with 2 POTS ports, 4 10/100/1000 Base-T Ethernet interfaces, 100mW, and 802.11ac 4x4 and 802.11b/g/n 2x2 Wi-Fi radio with on/off switch. This ONT also has 2 USB 2.0 ports. Includes a 12V/3A 3-pin wall-mounted EU power adapter.	—	—	—

(1 of 2)

Ordering kit part number	Provisioning number	Description	CLEI	CPR	ECI/ Bar code
3FE 46964 DA (Customer-specific variant)	3FE 46974 AC	Turbo EPON RGW ONT with 2 POTS ports, 4 10/100/1000 Base-T Ethernet interfaces, 100mW, and 802.11ac 4x4 and 802.11b/g/n 2x2 Wi-Fi radio with on/off switch. 100 mW UPC Japan certified. This ONT also has 2 USB 2.0 ports. Includes a 12V/2.5A 2-pin wall-mounted Japan power adapter.	—	—	—

(2 of 2)

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

Table 3 **E-240W-A power supply**

ONT part numbers	Power model	Power information	Customer category or country compliance tested for	Notes
Kit: 3FE 46964 BA EMA: 3FE 46974 AB	Mass Power NBS40C120300VE	30 Watt AC/DC power adapter	Europe, CE certified	2-pin EU input plug
	SOY Technology SOY-1200300EU	30 Watt AC/DC power adapter	Europe, CE certified	2-pin EU input plug
Kit: 3FE 46964 CA EMA: 3FE 46974 AB	Mass Power NSB40C120300UK	30 Watt AC/DC power adapter	UK, CE certified	3-pin UK input plug
	SOY Technology SOY-1200300GB	30 Watt AC/DC power adapter	UK, CE certified	3pin UK input plug
Kit: 3FE 46964 DA EMA: 3FE 46974 AC	SOY Technology SOY-1200250-III	30 Watt AC/DC power adapter	JP certified	2-pin JP input plug

4.2 E-240W-A general description

E-240W-A indoor ONTs provide the subscriber interface for the network by terminating the PON interface and converting it to user interfaces that directly connect to subscriber devices. The ONT is compatible with all existing subscriber equipment, including analog phones with both tone and rotary dial capabilities, cordless phones, modems, fax machines, and caller ID boxes (Type I, Type II, and Type III).

E-240W-A indoor ONTs provide the following functions:

- Single fiber turbo EPON interface with 1G upstream and 2G downstream data rates
- network demarcation for all services
- DPoE multicast 2.0 message support

- 256 RAM and 256 Flash
- voice interworking function from the analog POTS lines to the VoIP/Ethernet layers
- interworking functions between LLIDs and Ethernet layers
- mux and demux functions to the PON
- optical to electrical conversion
- optics that support received signal strength indication (RSSI)
- Ethernet and POTS ports have Type 4 lightning protection
- Traffic classification and QoS capability
- Analog Telephone Adapter (ATA) function integrated based on SIP (RFC3261) with various CLASS services supported, including Caller ID, Call Waiting, Call Forwarding, and Call Transfer
- 5 REN per line
- Multiple voice Codec
- MDI/MDIX auto-negotiation
- Internal Switch
- UPnP IGD2.0 support
- Optics that support received signal strength indication (RSSI)
- Internal DHCP server, with configurable DHCP pool and gateway
- WPS on wireless authorization support
- 2.4GHz/5GHz dual band concurrency
- Enhanced ONT; SSH-Telnet-FTP and http server are disabled from the WAN side
- Concurrent 802.11n 2x2 MIMO in 2.4GHz and 802.11ac 4x4 MIMO in 5GHz
- 64/128 WEP encryption
- WPA, WPA-PSK/TKIP
- WPA2, WPA2-PSK/AES
- support for multiple SSIDs (private and public instances); contact your Nokia representative for further details.
- WLAN on/off push button
- WPS/PBC buttons (for 2.4G and 5G)
- Network Address Translation (NAT)
- Network Address Port Translation (NAPT)
- ALG and UPnP port forwarding
- DMZ
- IP/MAC filter
- Multi-level firewall
- DNS server
- DHCP client/server
- support for up to 32 simultaneous wireless connections
- External USB HD (Hard Drive) support, accessible to all LAN devices

4.2.1 TR-069 support

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

- laser bias current
- voltage
- temperature
- received signal levels
- lower thresholds

These are the same optical parameters supported in the GUI. For more information, see Table 16 in the chapter "Configure an E-240W-A indoor ONT".

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

- channel
- SSID
- password for WPA and WEP
- Tx power (transmission rate in percentage of maximum transmit power)

These are the same TR-069 object parameters that are supported in the GUI. For more information, see Tables 12, 22, and 23 in the chapter "Configure an E-240W-A indoor ONT".

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

4.2.2 TR-104 parameter extension support for voice service

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

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

The proprietary attribute is: X_ALU-COM_XML_File_Name_Path.

4.2.3 TR-111 support

The E-240W-A ONT supports TR-111, which extends the WAN Management Protocol defined in TR-069 to enhance the ability to remotely manage LAN devices.

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

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

4.2.4 TR-181 Wi-Fi objects adapted in TR-098

TR-181 is the device data model for TR-069 Wi-Fi objects.

The following TR-181 Wi-Fi objects (and sub-objects) adapted in TR-098 are supported in this release:

- Device.WiFi
- Device.WiFi.Radio.{i}.
- Device.WiFi.Radio.{i}.Stats.
- Device.WiFi.SSID.{i}.
- Device.WiFi.SSID.{i}.Stats.
- Device.WiFi.AccessPoint.{i}.
- Device.WiFi.AccessPoint.{i}.Security.
- Device.WiFi.AccessPoint.{i}.WPS.
- Device.WiFi.AccessPoint.{i}.AssociatedDevice{i}.
- Device.WiFi.Endpoint.{i}.
- Device.WiFi.Endpoint.{i}.Stats.
- Device.WiFi.Endpoint.{i}.Security.
- Device.WiFi.Endpoint.{i}.Profile{i}.
- Device.WiFi.Endpoint.{i}.Profile{i}.Security.
- Device.WiFi.Endpoint.{i}.WPS.
- Device.WiFi.NeighboringWiFiDiagnostics.
- Device.WiFi.NeighboringWiFiDiagnostics.Result.{i}.

4.2.5 Mobile offload support

As part of the E2E solution supported by the ISAM 7750 service router, the E-240W-A ONT offers Mobile Offload support using a combination of EAP-SIM and IEEE 802.3.

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

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

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

4.2.6 Support for soft GRE tunnels

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

4.2.6.1 GRE

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

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

4.2.6.2 Soft GRE

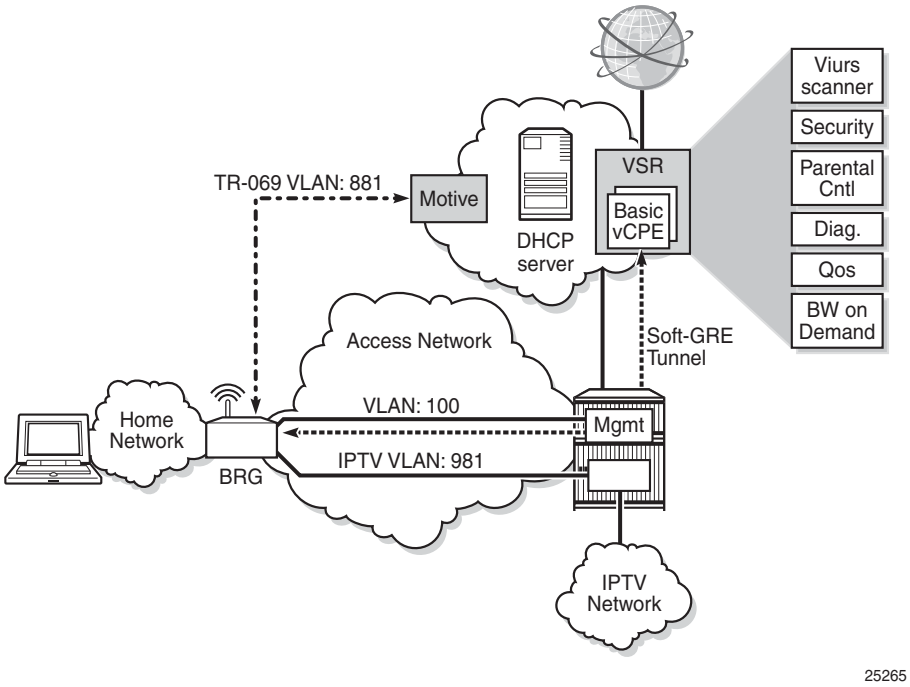
In soft GRE, only one side of the tunnel needs to be configured; the other end learns the remote IP addresses of all remote tunnel endpoints by examining the incoming GRE packets.

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

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

Figure 8 illustrates the soft GRE architecture.

Figure 8 **SoftGRE-based architecture**



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

4.3 E-240W-A software and installation feature support

For information on installing or replacing the E-240W-A see:

- Install an E-240W-A indoor ONT
- Replace an E-240W-A indoor ONT

For information on the following topics, see the *7368 ISAM ONT Product Overview Guide*:

- ONT and MDU general descriptions of features and functions
- Ethernet interface specifications
- POTS interface specifications
- RSSI specifications
- ONT optical budget
- ONT management using an ONT interface

4.4 E-240W-A interfaces and interface capacity

Table 4 describes the supported interfaces and interface capacity for E-240W-A indoor ONTs.

Table 4 **E-240W-A indoor ONT interface connection capacity**

ONT type and model	Maximum capacity								
	POTS	10/ 100 BASE-T	10/ 100/ 1000 BASE-T	RF video (CATV)	MoCA	VDSL2	E1/T1	Local craft	Turbo EPON
E-240W-A (1)	2	—	4	—	—	—	—	—	1

Note

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

4.4.1 E-240W-A connections and components

Figure 9 shows the physical connections for E-240W-A indoor ONTs,

Figure 9 **E-240W-A indoor ONT physical connections**

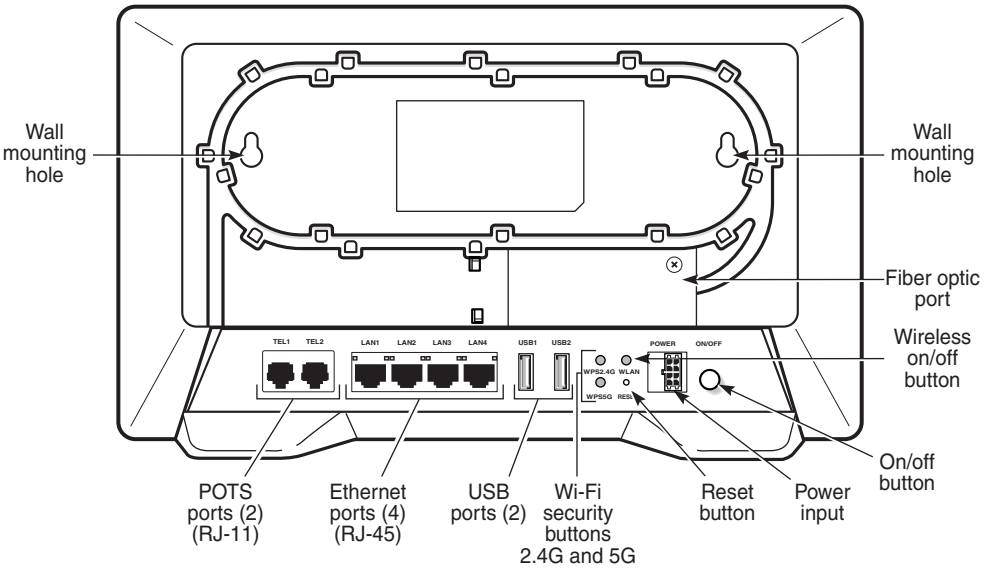


Figure 10 shows the E-240W-A ONT fiber optic connection

Figure 10 **E-240W-A ONT fiber optic connection**

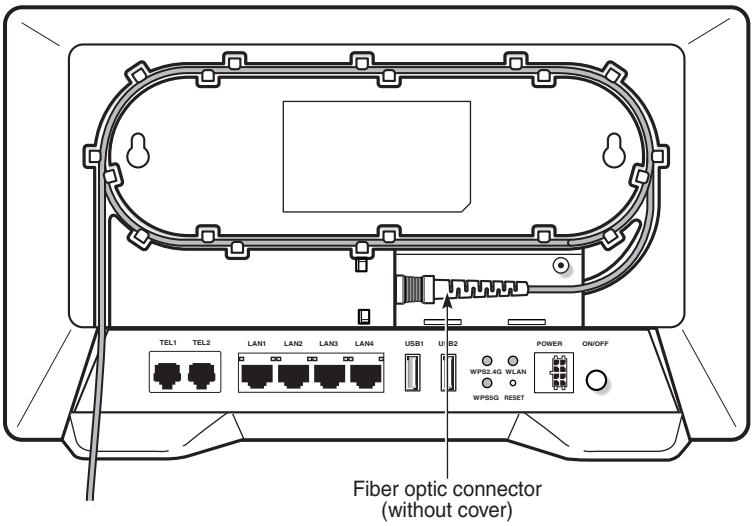


Figure 11 shows the E-240W-A ONT with the fiber cover

Figure 11 **E-240W-A ONT with fiber cover**

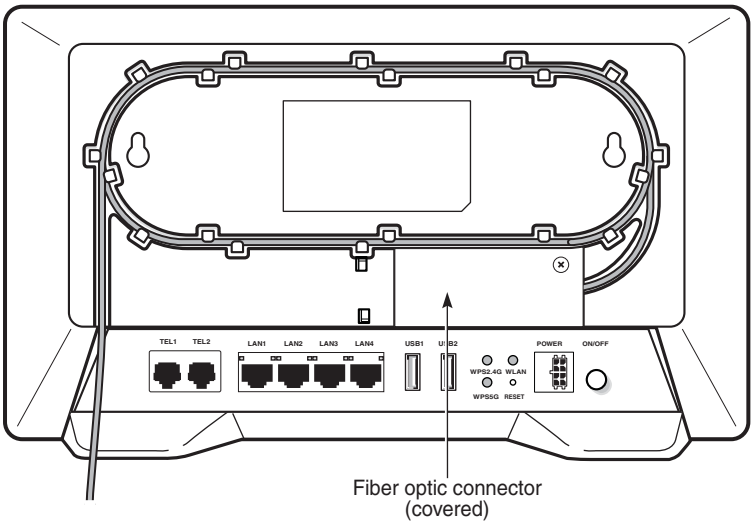


Table 5 describes the physical connections for E-240W-A indoor ONTs.

Table 5 **E-240W-A indoor ONT physical connections**

Connection [1]	Description
POTS ports	This connection is provided through RJ-11 ports. Up to two POTS connections are supported.The POTS ports support voice services.
Ethernet ports	This connection is provided through Ethernet RJ-45 connectors. Up to four 10/100/1000 Base-T Ethernet interfaces are supported.The Ethernet ports can support both data and in-band video services on all four interfaces.
USB ports	This connection is provided through 2 USB ports. The ONT supports external USB hard drives that can be made accessible to all LAN devices.
WPS buttons	The Wi-Fi Protected Setup buttons are labeled WPS2.4G and WPS5G. These buttons enable and disable WLAN data encryption.
WLAN button	Wi-Fi service is compliant with IEEE 802.11 standards and is enabled and disabled using the WLAN button.
Reset button	Pressing the Reset button for less than 10 seconds reboots the ONT; pressing the Reset button for 10 seconds resets the ONT to the factory defaults, except for the LOID and SLID.
Power input	This connection is provided through the power cable with a Molex connector.
On/Off button	This button turns the ONT on or off.
Fiber optic port	This port provides the connection for the fiber optic cable.

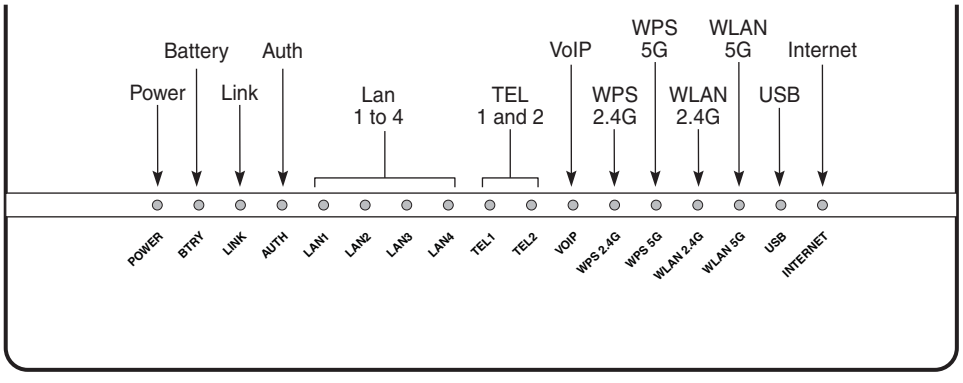
Note

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

4.5 E-240W-A LEDs

Figure 12 shows the E-240W-A indoor ONT LEDs.

Figure 12 **E-240W-A indoor ONT LEDs**



26028

Table 6 provides LED descriptions for E-240W-A indoor ONTs.

Table 6 E-240W-A indoor ONT LEDs

Indicator	LED color and behavior	LED behavior description
Power	Green solid Red solid Off	Power on Operating on battery power, or light failed on startup (for example corrupt flash), or self test failed on startup, or self test failed during regular operation or when executed over OMCI Power off
Battery	Green solid Flashing slow Flashing fast Off	Operating on battery power 1 second on, 1 second off: battery failure/non-rechargeable battery .5 second on, .5 second off: battery low Battery missing or not operating on battery power
Link	Green solid Off	EPON link between ONT and OLT is operating normally EPON link is down or no link connected
Auth	Off Green solid Green flashing	No fiber connected or no Rx power ONT has been configured on the OLT and is in service (UP) ONT is attempting to range with OLT ONT is ranged but not configured on OLT ONT is configured on OLT but admin is down and ONT is OOS ONT is in service and subsequently un-configured on the OLT ONT is in service while services are being configured ONT is in service but admin is down and ONT is OOS
LAN 1 to 4	Green solid Green flashing Off	Ethernet is linked LAN activity is present (in either direction) ONT power is off or Ethernet is not connected
TEL 1 to 2	Green solid Green flashing Off	Phone is off hook Phone is in ‘call in’ or ‘talking’ condition All phones are on hook
VOIP	Green solid Off	VOIP service is built up and can provide service VOIP service is not built up or out of service
WPS 2.4G and 5G	Green solid Green flashing Red solid Off	WiFi protected setup link is up (negotiation and auto-configuration successful) WiFi protected setup link activity (negotiation and auto-configuration ongoing) WiFi protected setup processing exception or multiple peers using WPS simultaneously WiFi protected setup link down or no link connected (negotiation has not started or has failed)
WLAN 2.4G and 5G	Off Green solid Green flashing	WLAN link is disabled WLAN link is enabled Traffic is passing via WLAN link
USB	Green solid Green flashing Off	At least one USB device is connected There is traffic activity on at least on USB device No USB device is connected

(1 of 2)

Indicator	LED color and behavior	LED behavior description
INTERNET	Green solid Green flashing Off	HSI WAN is connected: a) the device has an IP address assigned from IPCP, DHCP, or static, and no traffic has been detected; b) the session is dropped due to idle timeout but the PON link is still present. PPPoE or DHCP connection in progress HSI WAN is not connected: a) there is no physical interface connection; b) the device is in bridged mode without an assigned IP address; c) the session has been dropped for reasons other than idle timeout.

(2 of 2)

4.6 E-240W-A detailed specifications

Table 7 lists the physical specifications for E-240W-A indoor ONTs.

Table 7 **E-240W-A indoor ONT physical specifications**

Description	Specification
Length	11.0 in. (280 mm)
Width	6.7 in. (170 mm)
Height	2.7 in. (69 mm)
Weight [within ± 0.5 lb (0.23 kg)] (net weight of ONT)	1.42 lb (0.644 kg)

Table 8 lists the power consumption specifications for E-240W-A indoor ONT.

Table 8 **E-240W-A indoor ONT power consumption specifications**

Mnemonic	Maximum power (Not to exceed)	Condition	Minimum power	Condition
E-240W-A	23 W	2 POTS off-hook, 4 10/100/1000 Base-T Ethernet, Wi-Fi operational	5.74 W	2 POTS on-hook, other interfaces/services not provisioned

Table 9 lists the environmental specifications for E-240W-A indoor ONT.

Table 9 **E-240W-A indoor ONT environmental specifications**

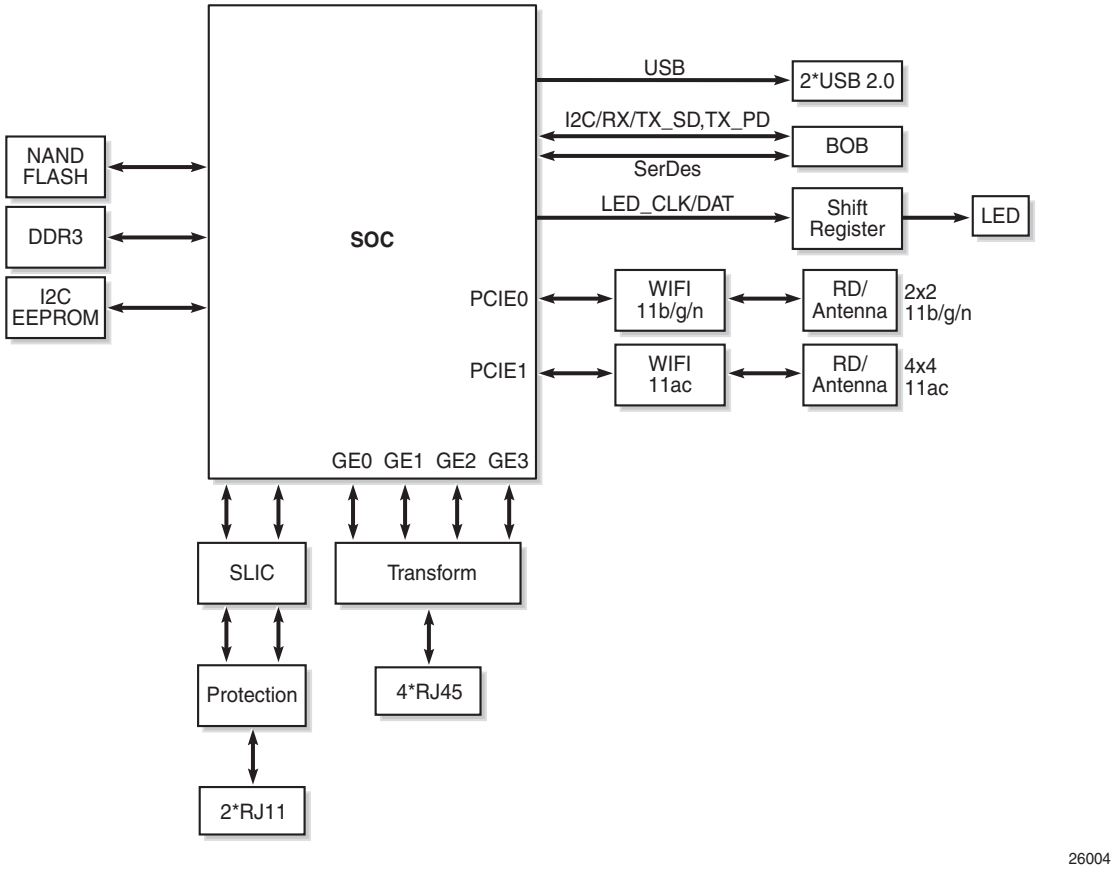
Mounting method	Temperature range and humidity	Altitude
On desk or wall mounted	Operating: 23°F to 113°F (-5°C to 45°C) ambient temperature 10% to 95% relative humidity, non-condensing	Contact your Nokia technical support representative for more information
	Storage: -4°F to 158°F (-20°C to 70C)	

4.7 E-240W-A functional blocks

E-240W-A indoor ONTs are single-residence ONTs that support Wireless (Wi-Fi) service. Wi-Fi service on these ONTs is compliant with the IEEE 802.11 standard and enabled or disabled using a WLAN button. In addition to the Wi-Fi service, these ONTs transmit Ethernet packets to four RJ-45 Ethernet ports and voice traffic to two RJ-11 POTS ports. These ONTs also feature fiber optic, USB, and power connectors.

Figure 13 shows the functional blocks for E-240W-A indoor ONT.

Figure 13 **Single-residence Wi-Fi ONT with Gigabit Ethernet and POTS and without RF video**



4.8 E-240W-A standards compliance

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

- EN 300-328 v1.9.1 wide band data transmission standards for 2.4GHz bands
- G.711 support for FAX and modem connection
- IEEE 802.3 CE
- IEEE 802.11ac/b/g/n for WiFi

4.8.1 Energy-related products standby and off modes compliance

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

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

For information about the type and number of network ports, see “E-240W-A interfaces and interface capacity” in this chapter.

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

4.8.2 FCC statement

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

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

4.8.3 FCC Radiation Exposure Statement

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

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

1 this device may not cause harmful interference, and

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

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

4.9 E-240W-A special considerations

This sections describes the WiFi details and special considerations for E-240W-A ONTs.

4.9.1 Wi-Fi service

E-240W-A indoor ONTs feature Wi-Fi service as well as voice and data services. Wi-Fi is a wireless networking technology that uses radio waves to provide wireless HSI and network connections. This ONT complies with the IEEE 802.11 standards, which the Wi-Fi Alliance defines as the basis for Wi-Fi technology.

4.9.1.1 Wi-Fi physical features

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

- WLAN button for enabling and disabling Wi-Fi service
- 6 internal antennae: 2 for 2.4G and 4 for 5G
- two Wi-Fi Protected Setup (WPS) push buttons (one each for 2.4G and 5G) for adding WPS-enabled wireless devices

4.9.1.2 Wi-Fi standards and certifications

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

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

4.9.1.3 Wi-Fi GUI features

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

4.9.2 E-240W-A ONT considerations and limitations

Table 10 lists the considerations and limitations for E-240W-A ONTs.

Table 10 **E-240W-A ONT considerations and limitations**

Considerations and limitations
Call History Data collection (ONTCALLHST) is supported, except for the following parameters: RTP packets (discarded), far-end RTCP and RTCP-XR participation, RTCP average and peak round trip delay, MOS, average jitter, number of jitter-buffer over-runs and under runs.
Some voice features are configurable on a per ONT basis, including Call Waiting, Call Hold, 3-Way Calling, and Call Transfer.
The following voice features / GSIP parameters are configurable on a per-Client/ per-ONT basis (not per-Subscriber): • Enable Caller ID and Enable Caller Name ID • Digitmap and the associated Interdigit and Critical timers and Enter key parameters • Warmline timer is enabled per subscriber, but the warmline timer value is configured per ONT and must have a lower value than the Permanent time • Miscellaneous timers: Permanent, Timed-release, Reanswer, Error-tone, and CW-alert timers • Features / functions: Message waiting mode, WMWI refresh interval, DTMF volume level • Service Codes for the following features: CCW, Call Hold and Warmline

5 Install an E-240W-A indoor ONT

5.1 Purpose

This chapter provides the steps to install an E-240W-A indoor ONT.

5.2 General

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

5.3 Prerequisites

You need the following items before beginning the installation:

- all required cables

5.4 Recommended tools

You need the following tools for the installation:

- #2 Phillips screwdriver
- 1/4 in. (6 mm) flat blade screwdriver
- wire strippers
- fiber optic splicing tools
- RJ-45 cable plug crimp tool
- voltmeter or multimeter
- optical power meter

- drill and drill bits
- paper clip

5.5 Safety information

Read the following safety information before installing the unit.

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

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

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

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

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

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

Note 2 — Observe the following:

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

5.6 Procedure

Use this procedure to install an E-240W-A indoor ONT.

1 Place the indoor ONT unit:

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

Note — The E-240W-A cannot be stacked with another ONT or with other equipment. The ONT mounting requirements are:

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

b On a wall, go to step 2.

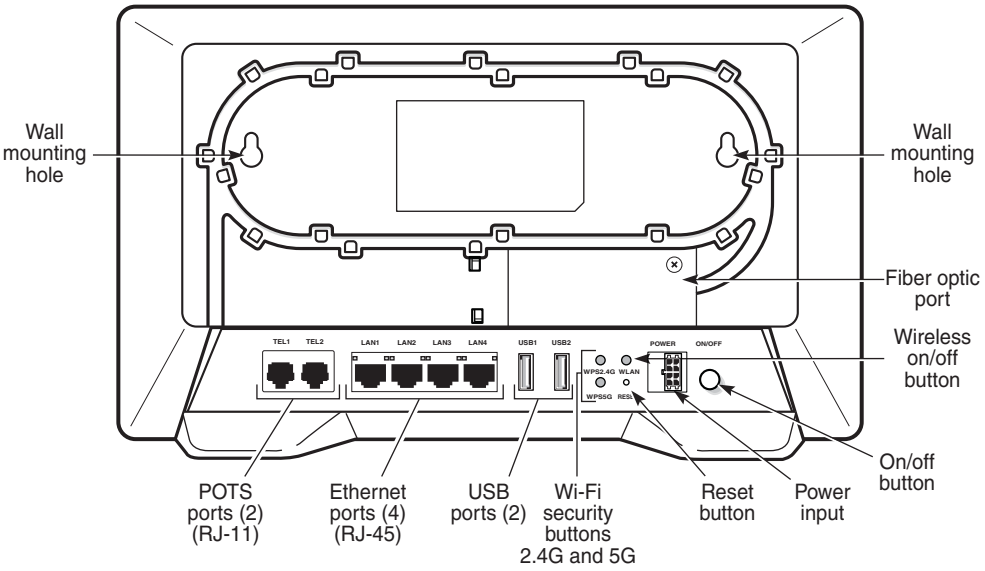
2 Mount the E-240W-A indoor ONT on a wall.

The E-240W-A indoor ONT must be mounted in a horizontal position, as indicated by the wall mounting key holes in Figure 14.

If possible, mount the ONT on a wall stud.

Figure 14 shows the ONT with the connections and the key mounting holes.

Figure 14 **E-240W-A ONT with connections and key mounting holes**



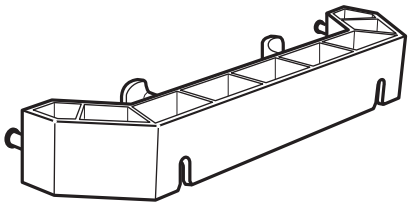
25272

i Attach the wall mount adapter bracket to the two wall mounting keyholes on the ONT.

Figure 15 shows the wall mounting bracket that is shipped with the ONT.

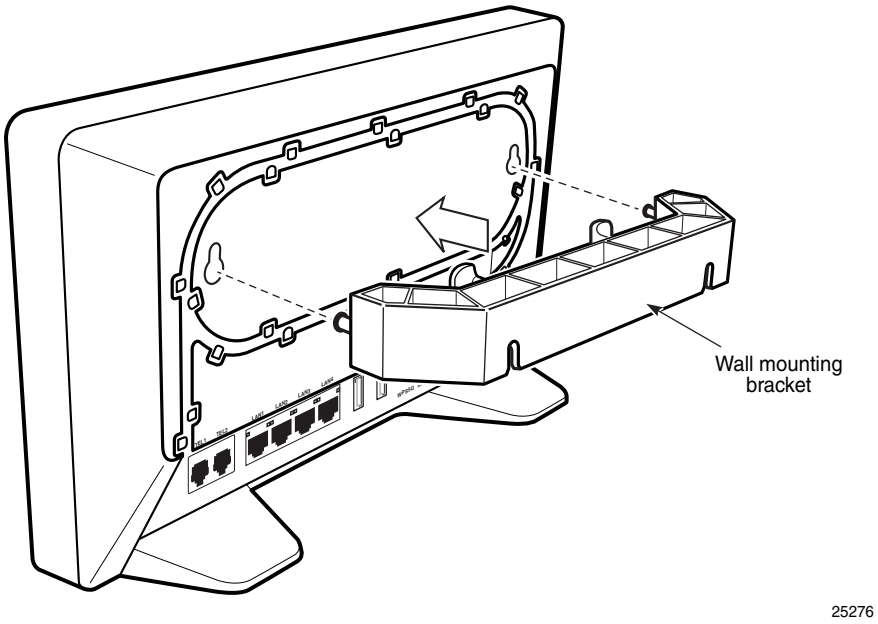
Figure 16 shows the ONT with the wall mounting bracket attached

Figure 15 **E-240W-A indoor ONT wall mounting bracket**



25275

Figure 16 **E-240W-A indoor ONT with wall mounting bracket attached**



ii Attach the ONT to the wall.

3 Review the connection locations as shown in Figure 14.

4 Connect the Ethernet cables to the RJ-45 ports; see Figure 14 for the location of the RJ-45 ports.

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

The POTS port to the left is labeled 1 for Line 1 while the port on the right is labeled 2 for Line 2, as shown in Figure 14.

6 Connect the fiber optic cable with SC/APC adapter into the SC/APC connector (or SC/UPC for the 3FE46964DA variant); see Figure 14 for the location of the 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 or SC/UPC fiber optic pigtail cable.

7 Install the power supply according to manufacturer specifications.

Note — Observe the following:

- Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 12VDC, 2.5 A.

8 Connect the power cable to the power connector.

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

10 If used, enable the Wi-Fi service.

i Locate the WLAN button on the ONT; see Figure 14 for location of the WLAN button.

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

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

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

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

14 If necessary, reset the ONT.

i Locate the Reset button on an E-240W-A indoor ONT as shown in Figure 14.

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

15 STOP. This procedure is complete.

6 Replace an E-240W-A indoor ONT

6.1 Purpose

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

6.2 General

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

6.3 Prerequisites

You need the following items before beginning the installation:

- all required cables

6.4 Recommended tools

You need the following tools for replacing the ONT:

- #2 Phillips screwdriver
- 1/4 in. (6 mm) flat blade screwdriver
- wire strippers
- fiber optic splicing tools
- RJ-45 cable plug crimp tool
- voltmeter or multimeter

- optical power meter
- drill and drill bits

6.5 Safety information

Read the following safety information before replacing the unit.

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

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

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

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

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

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

Note 2 — Observe the following:

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

6.6 Procedure

Use this procedure to replace an E-240W-A indoor ONT.

1 Deactivate the ONT services at the P-OLT.

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

Example:

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

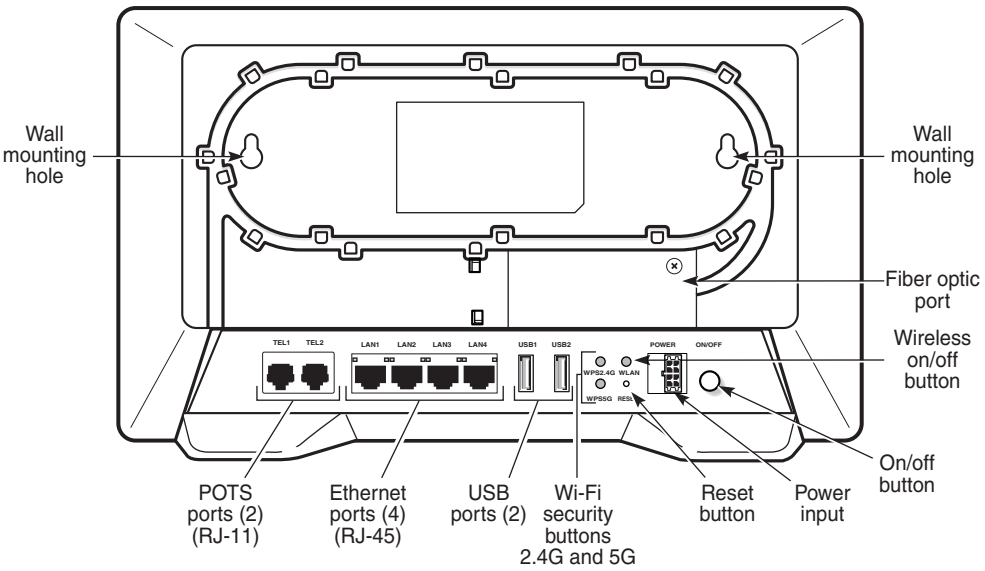
ii If the ONT is in service, place the ONT in OOS state.

Example:

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

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

Figure 17 **E-240W-A indoor ONT connections**



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

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

5 Disconnect the fiber optic cables.

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

i Unplug the fiber optic cable with SC/APC connector (or SC/UPC for the 3FE46964DA variant) from the ONT; see Figure 17 for the location of the fiber optic port.

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

6 Replace the ONT with a new unit:

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

b On a wall.

i Remove the old ONT from the wall.

ii Attach the wall mount adapter bracket (shipped with the ONT) to the two wall mounting key holes on the new ONT.

iii Attach the new ONT to the wall.

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

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

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

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

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

10 Connect the fiber optic cable with SC/APC adapter into the SC/APC connector (or SC/UPC to the SC/UPC connector for the 3FE46964DA variant). Figure 17 shows the location of the 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 or SC/UPC fiber optic pigtail cable.

11 Install the power supply according to manufacturer specifications.

Note — Observe the following:

- Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 12 VDC, 2.5 A.

12 Connect the power cable to the power connector.

13 Power up the unit by using the power switch.

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

15 If used, configure the SLID; see the *7368 ISAM ONT Configuration, Management, and Troubleshooting Guide* for more information.

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

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

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

18 If necessary, reset the ONT.

i Locate the Reset button on an E-240W-A indoor ONT as shown in Figure 17.

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

19 STOP. This procedure is complete.

7 Configure an E-240W-A indoor ONT

7.1 General

Please refer to the configuration information provided with your OLT for the software configuration procedure for an E-240W-A ONT.

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

7.2 HGU mode GUI configuration

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

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

7.2.1 Login

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

Procedure 6 Login to web-based GUI

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

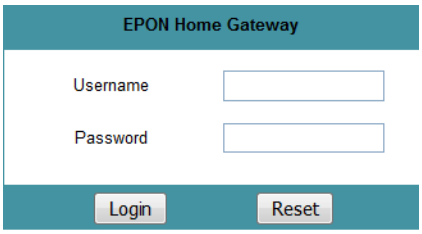
The login window appears.

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

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

The default user name is admin (or superadmin for administrators). The default password is a random number, which is included in the ONT kit.

Figure 18 **Web login window**



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

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

3 Click Login. The Device Information screen appears.

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

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

4 STOP. This procedure is complete.

7.2.2 Device and connection status

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

- device information
- LAN status

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

Procedure 7 Device information retrieval

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

Figure 19 **Device Information window**

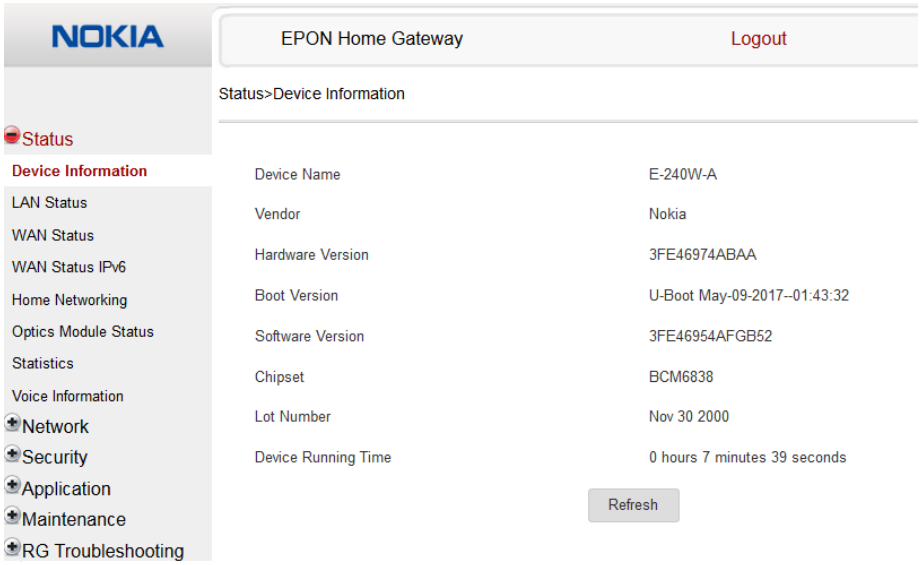


Table 11 describes the fields in the Device Information window.

Table 11 **Device Information parameters**

Field	Description
Device Name	Name on the ONT
Vendor	Name of the vendor
Hardware version	Hardware version of the ONT
Boot version	Boot version of the ONT
Software version	Software version of the ONT

(1 of 2)

Field	Description
Chipset	Chipset of the ONT
Lot Number	Production date of the ONT
Device Running Time	Amount of time the device has run since last reset in hours, minutes, and seconds

(2 of 2)

2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

Procedure 8 LAN status retrieval

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

Figure 20 **LAN status window**

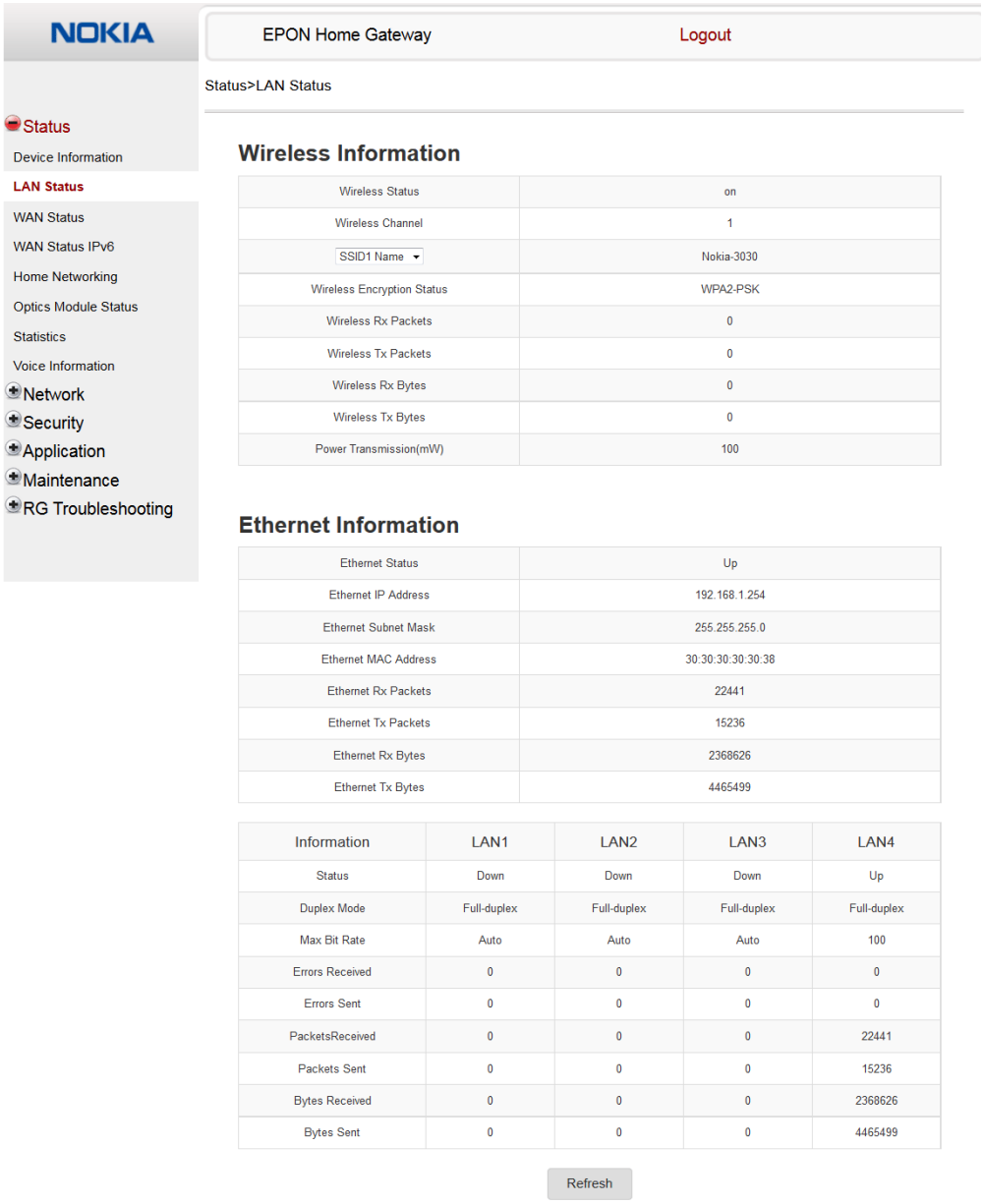


Table 12 describes the fields in the LAN status window.

Table 12 **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
Information (for each LAN line)	
Status	Status of the LAN line: up or down
Duplex Mode	Duplex mode: full duplex or half duplex
Max Bit Rate	Max bit rate: auto or number
Errors Received	Number of errors received
Errors Sent	Number of errors sent
Packets Received	Number of packets received
Packets Sent	Number of packets sent
Bytes Received	Number of bytes received
Bytes Sent	Number of bytes sent

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 EPON Home Gateway window, as shown in Figure 21.

Figure 21 **WAN status window**

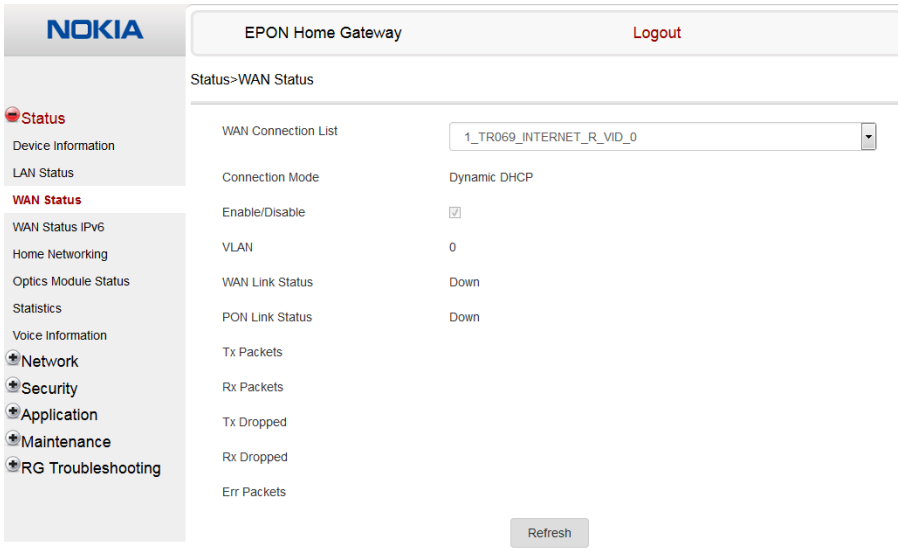


Table 13 describes the fields in the WAN status window.

Table 13 **WAN status parameters**

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

(1 of 2)

Field	Description
PON Link Status	Whether the PON link is up or down
Tx Packets	Number of packets transmitted on the WAN connection
Rx Packets	Number of packets received on the WAN connection
Tx Dropped	Number of packets dropped on the transmit WAN connection
Rx Dropped	Number of packets dropped on the receive WAN connection
Err Packets	Number of errored packets on the WAN connection

(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 EPON Home Gateway window, as shown in Figure 22.

Figure 22 **WAN status IPv6 window**

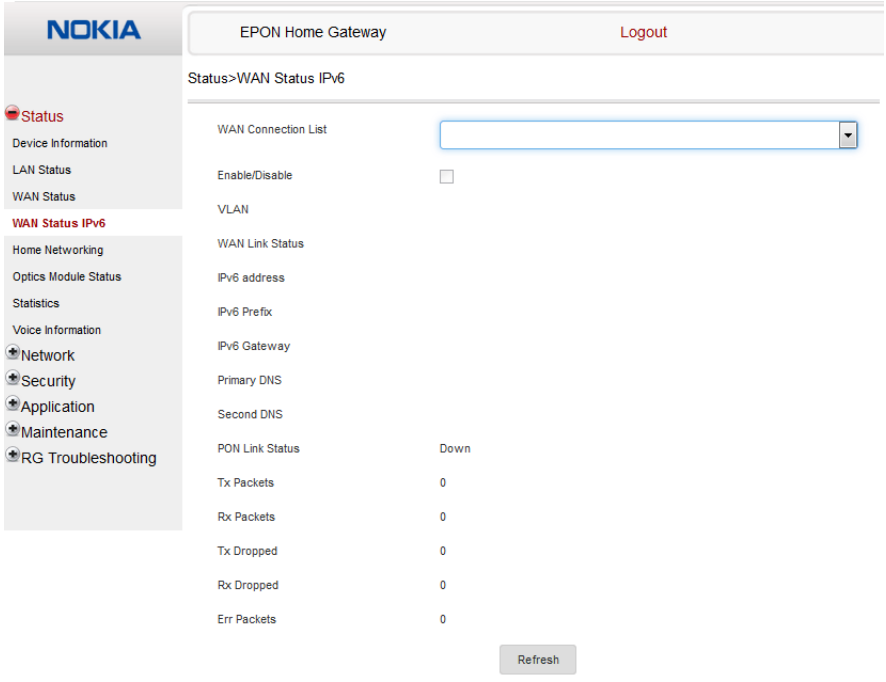


Table 14 describes the fields in the WAN status IPv6 window.

Table 14 **WAN status IPv6 parameters**

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

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 EPON Home Gateway window, as shown in Figure 23.

Figure 23 **Home networking information window**

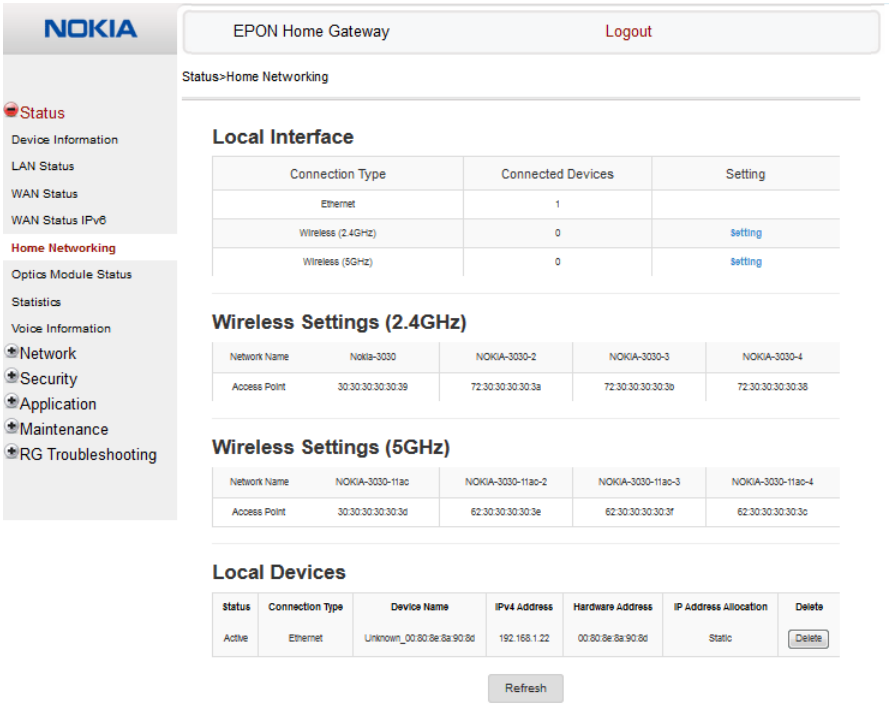


Table 15 describes the fields in the Home networking window.

Table 15 **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 (2.4GHz and 5GHz)	
Network Name	Name of the wireless network
Access Point	Hexadecimal address of the wireless access point
Local Devices	

(1 of 2)

Field	Description
Table entry	Each entry indicates the status (active or inactive), connection type, device name, IP address, hardware address, and IP address allocation of each connected local device.

(2 of 2)

2 Click Delete to delete a particular local device connection.

3 Click Refresh to update the displayed information.

4 STOP. This procedure is complete.

Procedure 12 Optics module status retrieval

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

Figure 24 **Optics module status window**

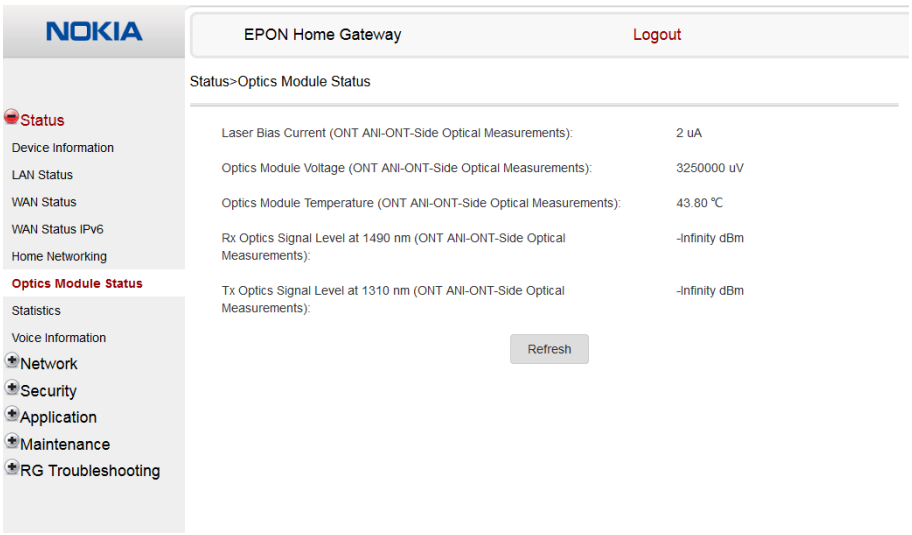


Table 16 describes the fields in the Optics module status window.

Table 16 **Optics module status parameters**

Field	Description
Laser Bias Current (ONT ANI-ONT-Side Optical Measurements)	Laser bias current, measured in uA
Optics Module Voltage (ONT ANI-ONT-Side Optical Measurements)	Optics module voltage, measured in V
Optics Module Temperature (ONT ANI-ONT-Side Optical Measurements)	Optics module temperature, measured in C
Rx Optics Signal Level at 1490 nm (ONT ANI-ONT-Side Optical Measurements)	Received optics signal level at 1490 nm, measured in dBm
Tx Optics Signal Level at 1310 nm (ONT ANI-ONT-Side Optical Measurements)	Transmitted optics signal level at 1310 nm, measured in dBm

2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

Procedure 13 Statistics retrieval

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

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

Figure 25 shows the statistics for the LAN ports.

Figure 25 **LAN ports Statistics window**

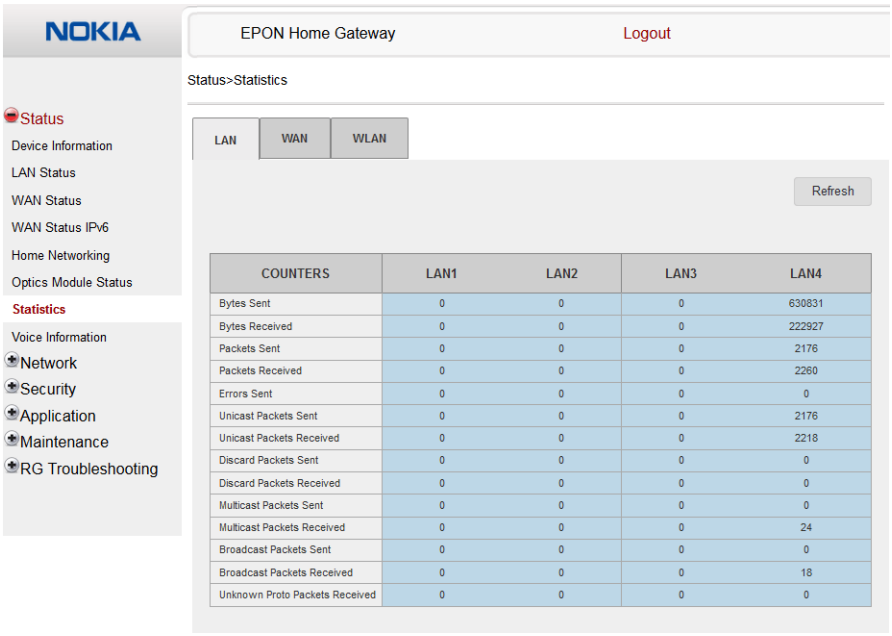
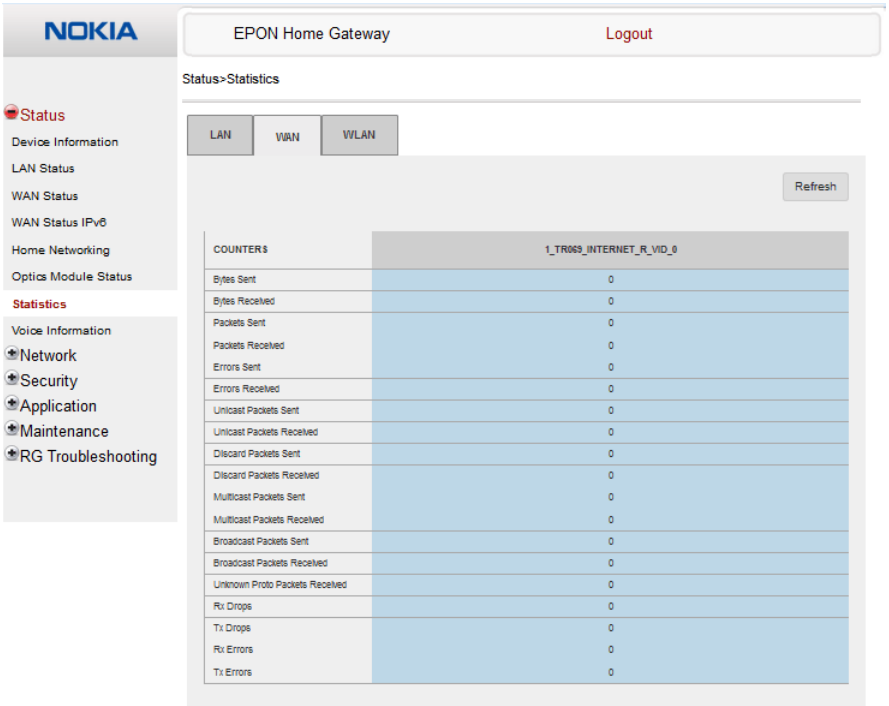


Figure 26 shows the statistics for the WAN ports.

Figure 26 **WAN ports statistics window**



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

Figure 27 **WAN ports statistics message**

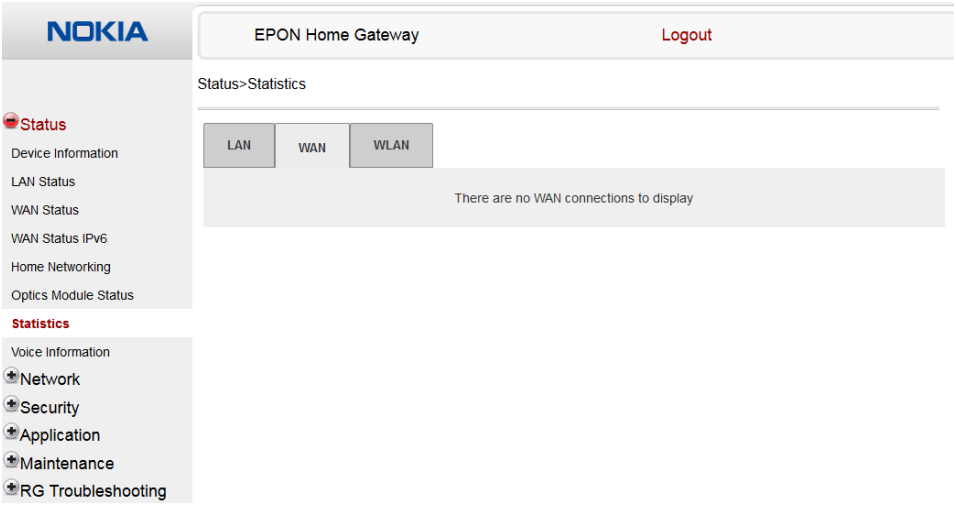
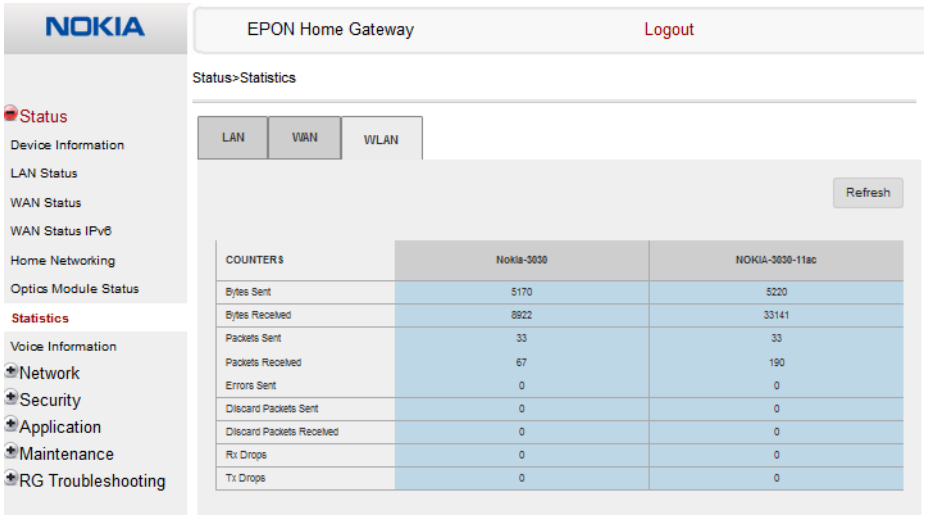


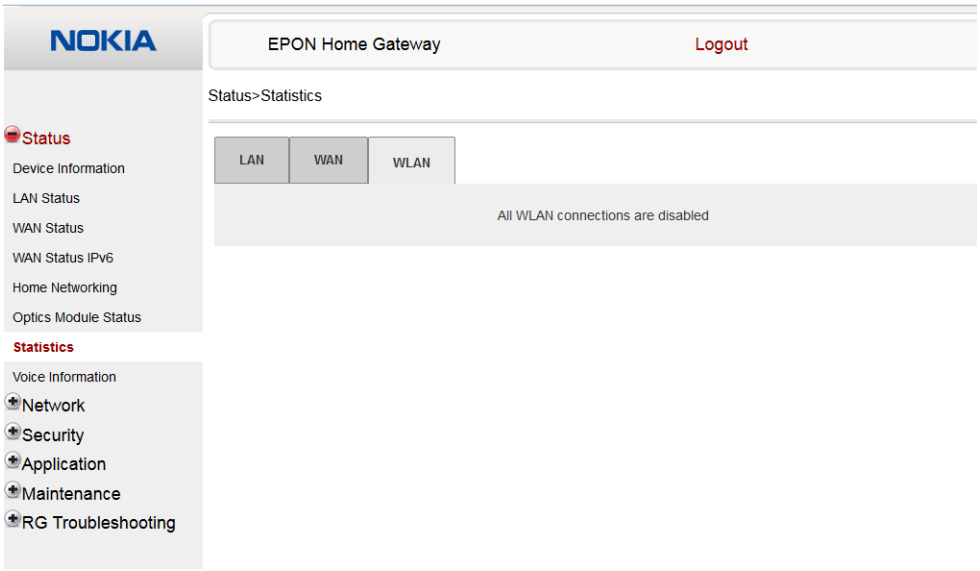
Figure 28 shows the statistics for the WLAN ports.

Figure 28 **WLAN ports statistics window**



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

Figure 29 **WLAN ports statistics message**



2 STOP. This procedure is complete.

Procedure 14 Voice information retrieval

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

Figure 30 **Voice Information window**

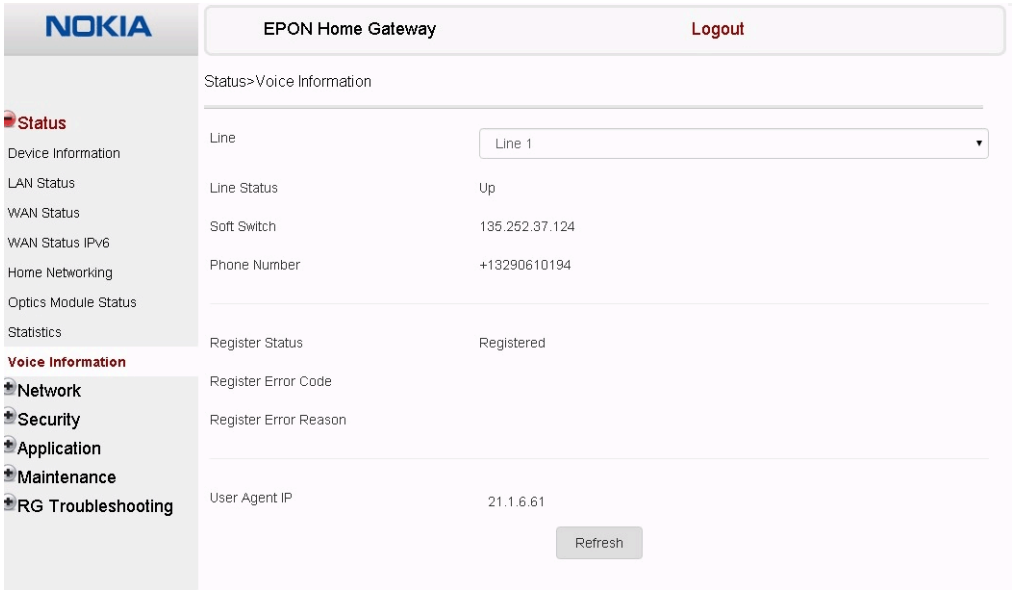


Table 17 describes the fields in the Voice Information window.

Table 17 **Voice Information parameters**

Field	Description
Line	Select the POTS line: 1 or 2
Line Status	Status of the selected POTS line: IDLE, Off Hook, or On Hook
Softswitch(1)	Proxy IP address; blank if the line is not registered
Phone number(1)	Phone number configured for the selected telephone line
Register Status	Registration status of the selected POTS port: registered or unregistered
Register Error Code	Error code for the unregistered POTS port
Register Error Reason	Error reason for the unregistered POTS port
User Agent IP	IP address of the user agent

Note

(1) This field is only visible at the adminEPON level; it is not visible at the userAdmin level.

2	Click Refresh to update the displayed information.
3	STOP. This procedure is complete.

7.2.3 Network configuration

E-240W-A ONTs also support network configuration, including:

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

Procedure 15 LAN networking configuration

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

Figure 31 **LAN network window**

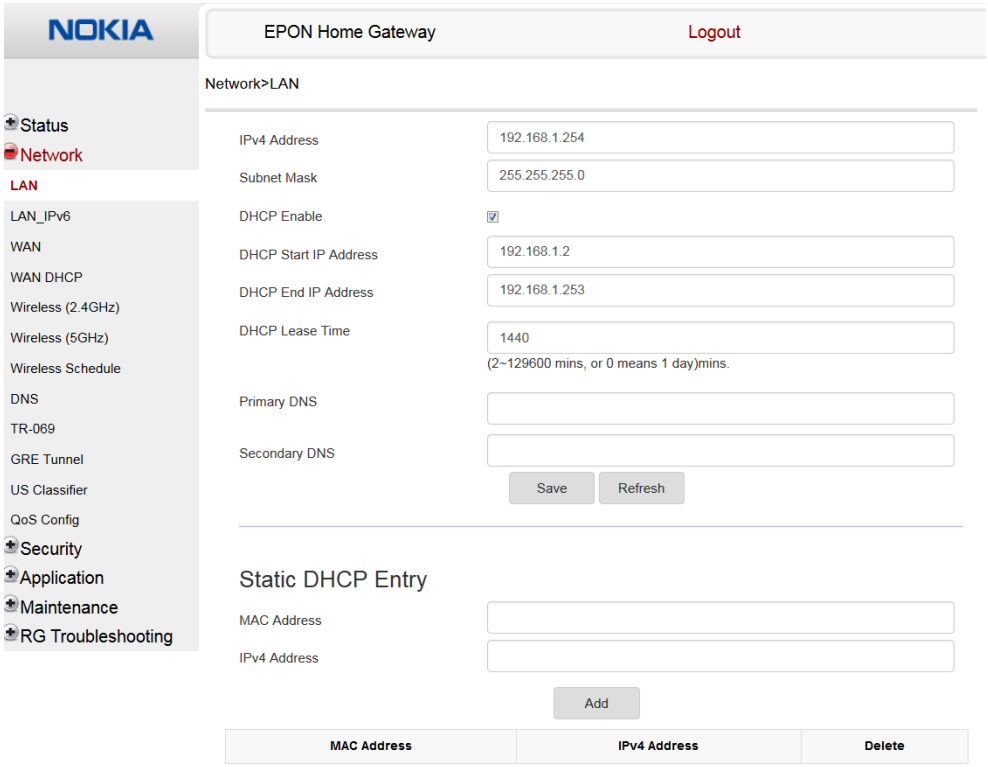


Table 18 describes the fields in the LAN network window.

Table 18 **LAN network parameters**

Field	Description
IPv4 Address	IP Address of the ONT
Subnet Mask	Subnet mask of the ONT
DHCP enable	Select this checkbox to enable DHCP
DHCP Start IP Address	Starting DHCP IP address
DHCP End IP Address	Ending DHCP IP address
DHCP Lease Time	DHCP lease time (in min)
Primary DNS	Primary DNS identifier

(1 of 2)

Field	Description
Secondary DNS	Secondary DNS identifier
Static DHCP Entry MAC Address	MAC address for the static DHCP
Static DHCP Entry IPv4 Address	IPv4 address for the static DHCP

(2 of 2)

2 Select the mode for each port.

3 Click Save.

4 Enter the DHCP configuration information.

5 Click Save.

6 Enter the Static DHCP information.

7 Click Add.

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

8 STOP. This procedure is complete.

Procedure 16 LAN IPv6 networking configuration

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

Figure 32 **LAN IPv6 network window**

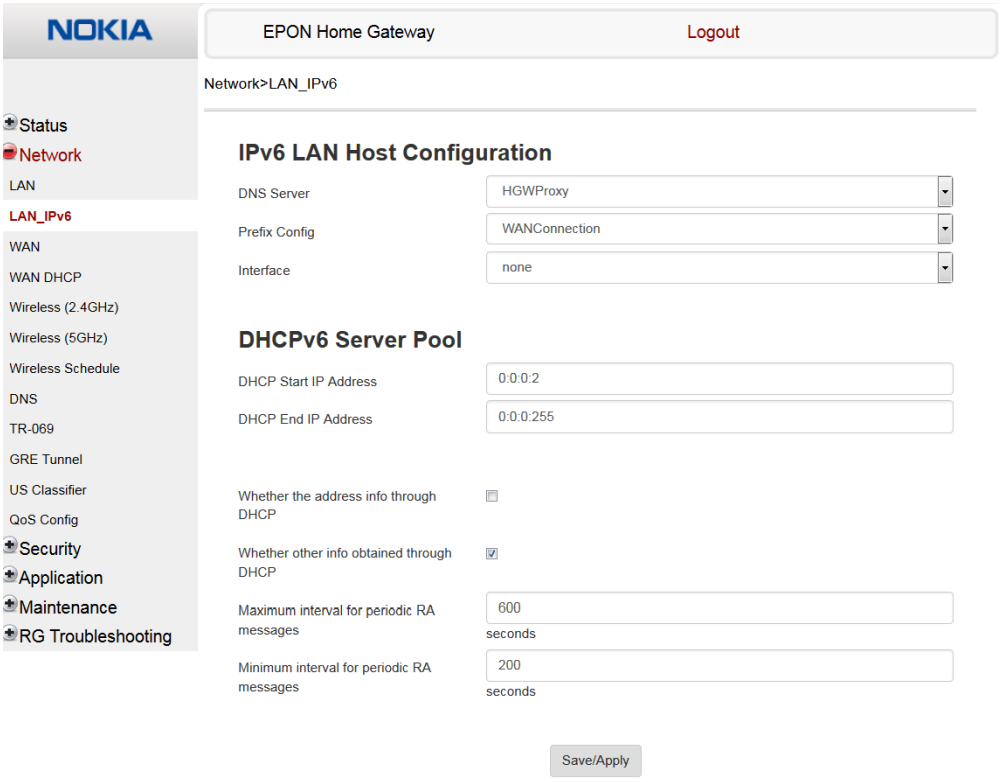


Table 19 describes the fields in the LAN IPv6 network window.

Table 19 **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 checkbox to enable address information retrieval through DHCP.
Whether other info obtained through DHCP	Select this checkbox to enable retrieval of other information through DHCP.
Maximum interval for periodic RA messages	Enter the maximum interval (in seconds) for periodic Router Advertisement messages. The interval range is from 4 to 1800.
Minimum interval for periodic RA messages	Enter the minimum interval (in seconds) for periodic Router Advertisement messages. The interval range is from 4 to 1800.

(2 of 2)

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

3 Select or enter the DHCP configuration information.

4 Enter the maximum and minimum intervals for RA messages.

5 Click Save/Apply.

6 STOP. This procedure is complete.

Procedure 17 WAN networking configuration

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

Figure 33 **WAN network window**

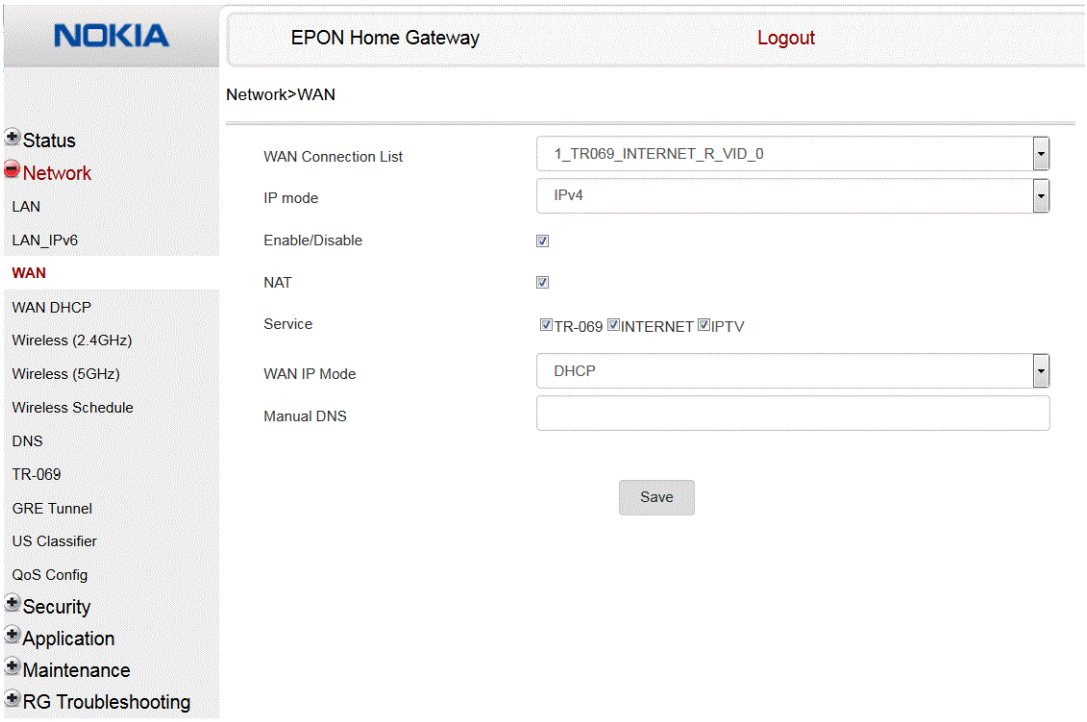


Table 20 describes the fields in the WAN network window.

Table 20 **WAN network parameters**

Field	Description
WAN Connection List	Choose a WAN connection from the drop-down menu to set the connection parameters
IP Mode	Choose an IP mode from the drop-down menu: IPv4 or IPv6
Enable/Disable	Select this checkbox to enable the WAN connection
NAT	Select this checkbox to enable NAT
Service	Select the checkboxes to enable the following service types for this connection: • TR-069 • INTERNET • IPTV
WAN IP Mode	Choose an IP mode from the drop-down menu

(1 of 2)

Field	Description
Manual DNS	Enter a manual DNS

(2 of 2)

2 Configure a specific WAN connection.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 18 WAN DHCP configuration

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

Figure 34 **WAN DHCP window**

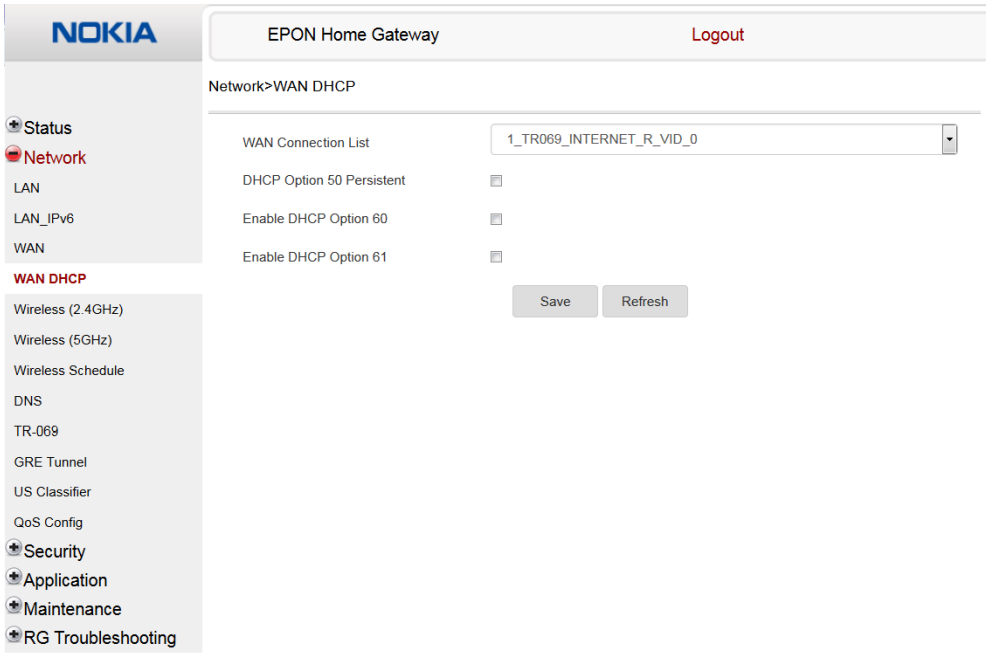


Table 21 describes the fields in the WAN DHCP window.

Table 21 **WAN DHCP parameters**

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

2 Configure a WAN DHCP option.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 19 WiFi 2.4G networking configuration

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

Figure 35 **WiFi 2.4G network window**

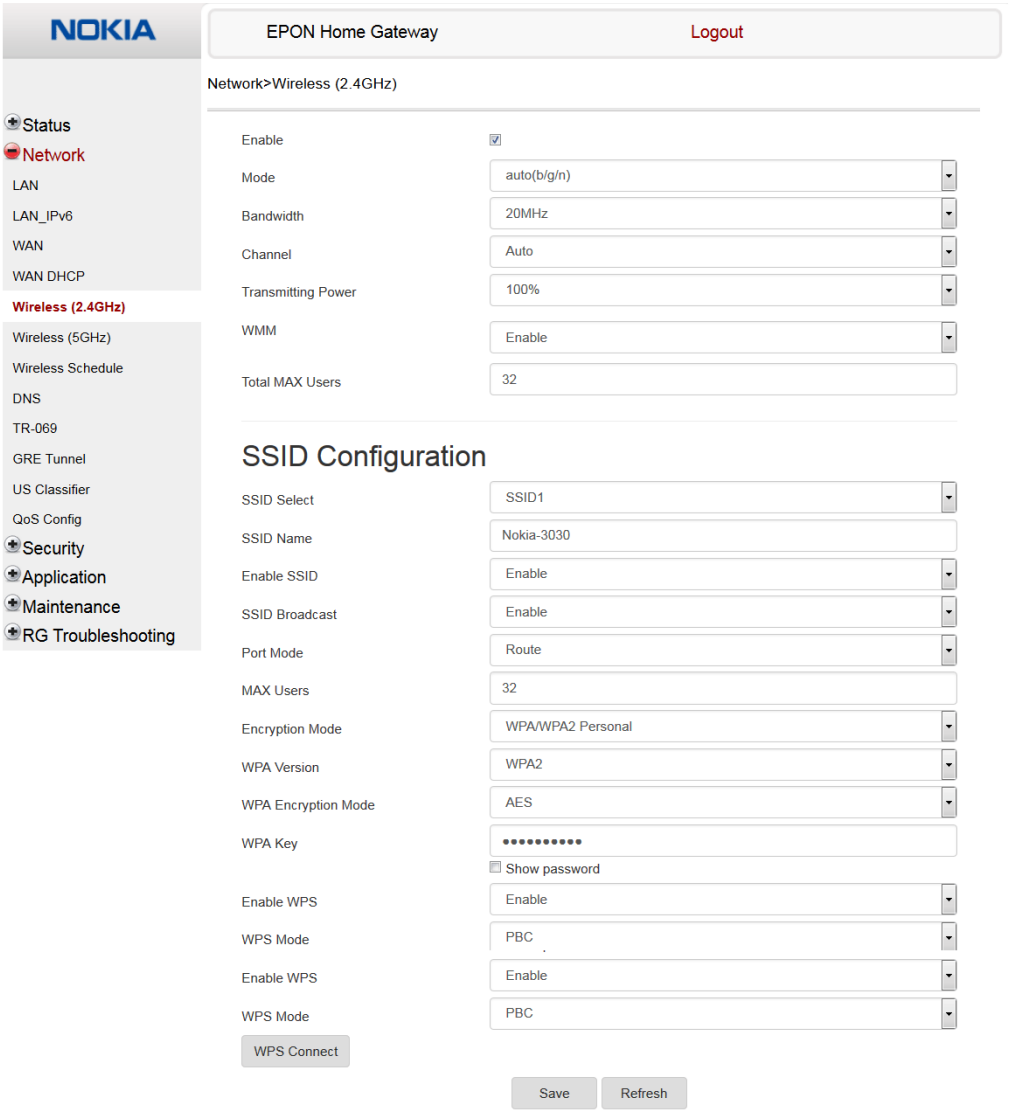


Table 22 describes the fields in the WiFi 2.4G network window.

Table 22 WiFi 2.4G network parameters

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

(1 of 2)

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

(2 of 2)

Notes

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

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

2 Configure the WiFi connection.

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

4 Click Save.

5 STOP. This procedure is complete.

Procedure 20 WiFi 5G networking configuration

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

Figure 36 **WiFi 5G network window**

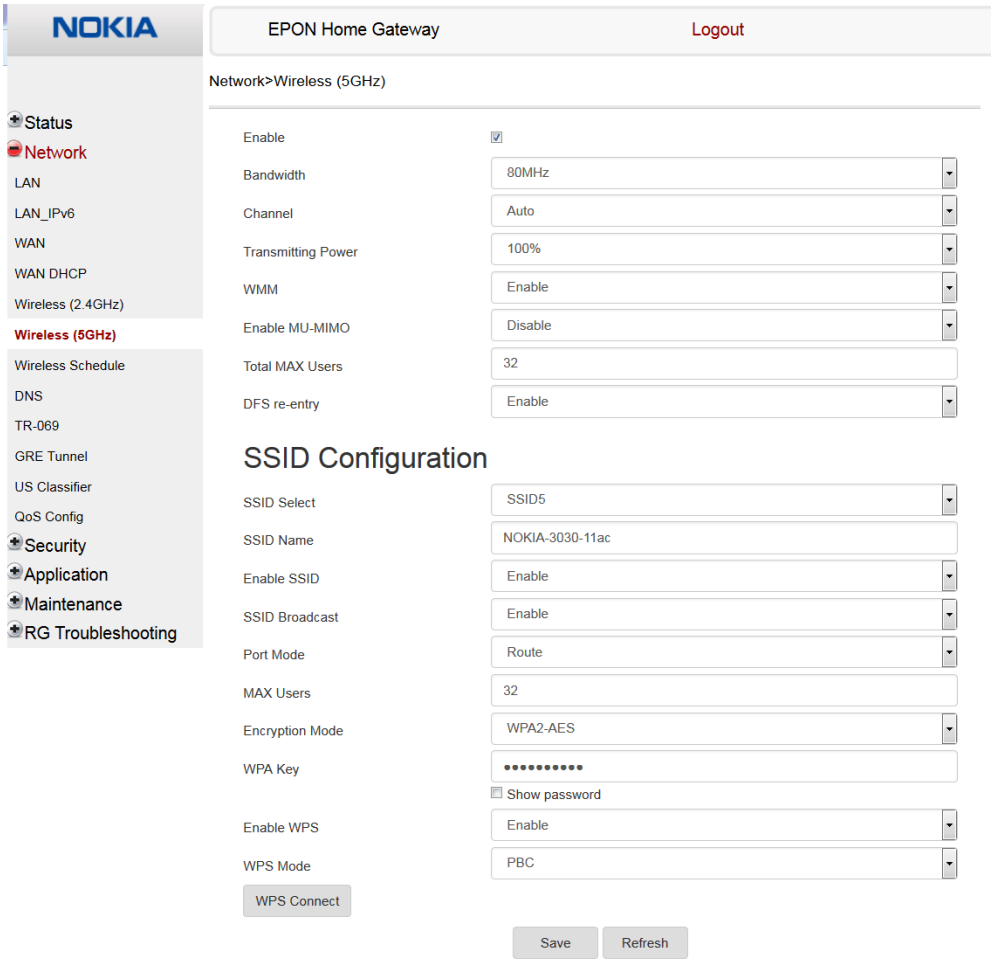


Table 23 describes the fields in the WiFi 5G network window.

Table 23 **WiFi 5G network parameters**

Field	Description
Enable	Select this checkbox to enable WiFi

(1 of 2)

Field	Description
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	Choose Enable or Disable from the drop-down menu to enable or disable WiFi multi-media
Enable MU-MIMO	Choose Enable or disable MU-MIMO from this drop-down menu The default is Enable, which enables users and wireless terminals to communicate with each other. MU-MIMO may decrease Wi-Fi performance for clients who do not support it, in which case Nokia recommends that you choose Disable.
Total MAX Users	Enter the total number of MAX users
DFS re-entry	Choose Enable or Disable from the drop-down menu to enable or disable DFS re-entry
SSID 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
Port Mode	Choose a port mode from the drop-down menu: route or bridge
MAX Users	Enter the number of MAX users
Encryption Mode	Choose an encryption mode from the drop-down menu: • OPEN • WEP • WPA/WPA2 Personal • WPA/WPA2 Enterprise (1)(2)
WPA Key	Enter the WPA key
Enable WPS	Choose Enable or disable WPS from this drop-down menu
WPS Mode	Choose a WPS mode from the drop-down menu: PBC (Push Button Connect) or PIN (Personal Identification Number)

(2 of 2)

Notes

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

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

2 Configure the WiFi connection.

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

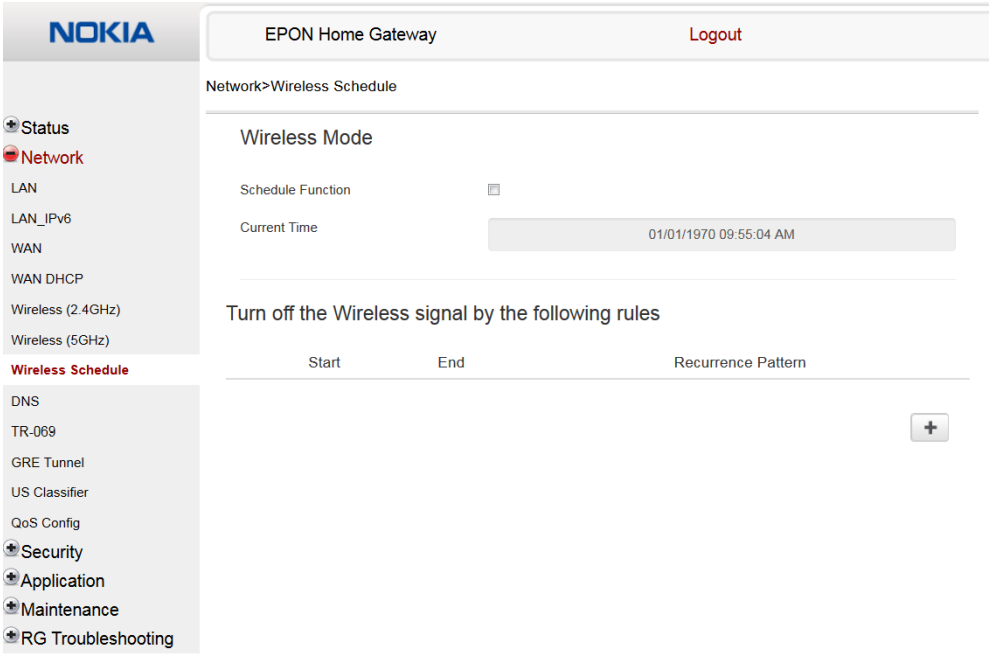
4 Click Save.

5 STOP. This procedure is complete.

Procedure 21 Wireless scheduling

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

Figure 37 **Wireless Schedule window**



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

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

A separate panel displays for configuring wireless schedule rules.

4	Enter a start time and end time for the period in which you want the wireless signal off.
5	Choose Everyday or Individual Days from the drop-down menu.
6	If you chose Individual Days, select the checkboxes for the desired days. The Recurrence Pattern shows the rules created to date.
7	If desired, click the plus sign (+) to add more rules.
8	Click Save Changes.
9	STOP. This procedure is complete.

Procedure 22 DNS configuration

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

Figure 38 **DNS network window**

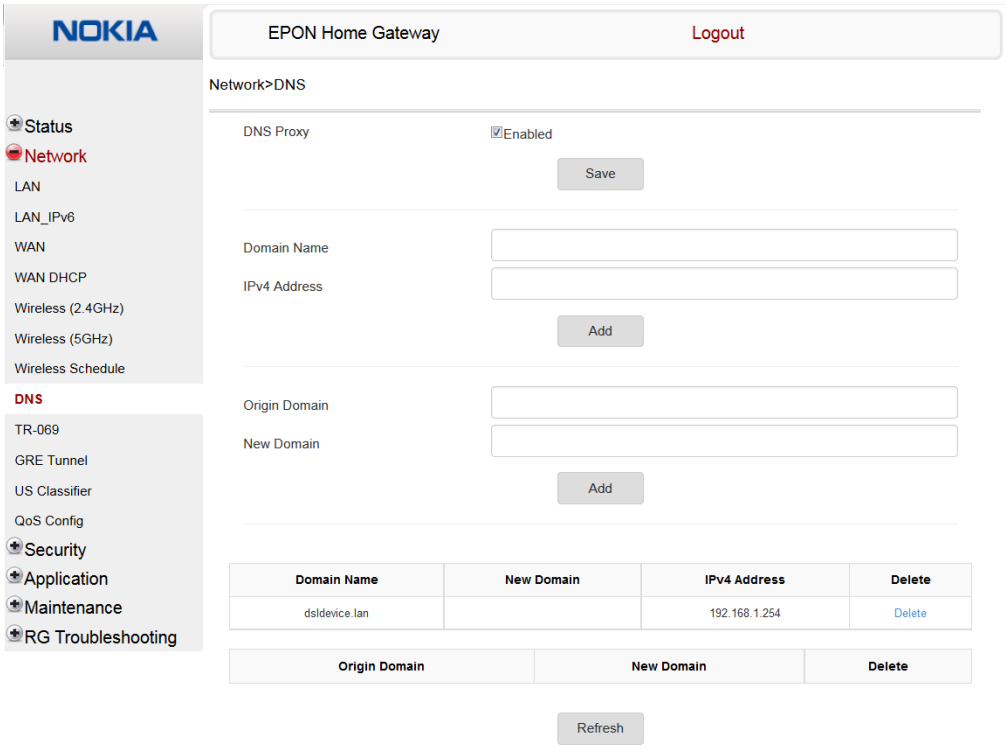


Table 24 describes the fields in the DNS network window.

Table 24 **DNS network parameters**

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

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

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

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

5 STOP. This procedure is complete.

Procedure 23 TR-069 configuration

1 Select Network > TR-069 from the top-level menu in the EPON Home Gateway window, as shown in Figure 39.

Figure 39 **TR-069 network window**

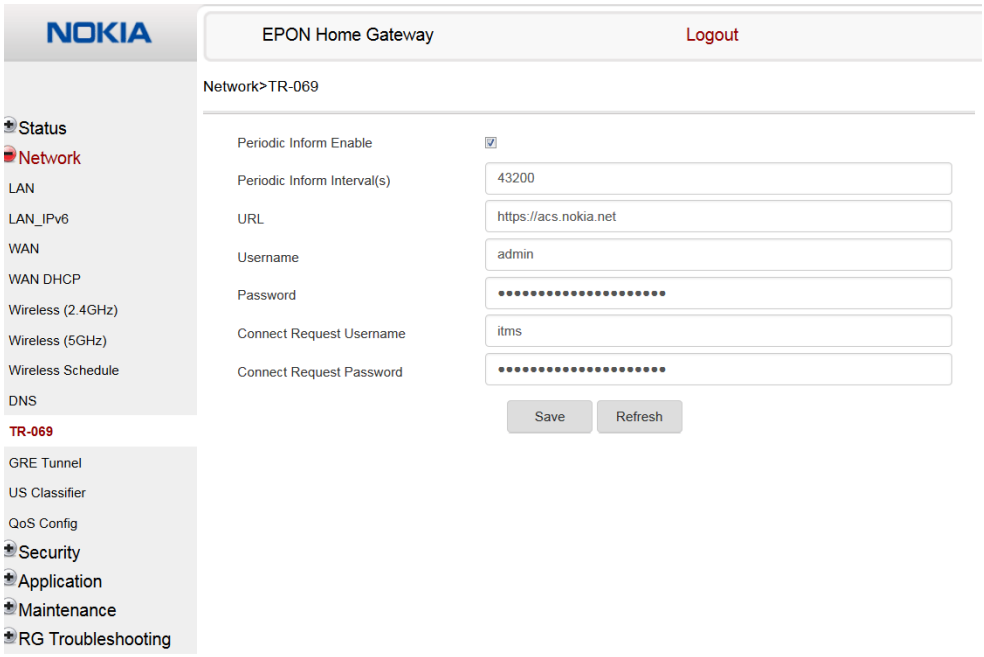


Table 25 describes the fields in the TR-069 network window.

Table 25 **TR-069 network parameters**

Field	Description
Periodic Inform Enable	Select this checkbox to enable periodic inform updates

(1 of 2)

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

(2 of 2)

2 Configure TR-069 by entering the required information.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 24 GRE Tunnel configuration

1 Select Network > GRE Tunnel from the top-level menu in the EPON Home Gateway window, as shown in Figure 40.

Figure 40 **GRE Tunnel window**

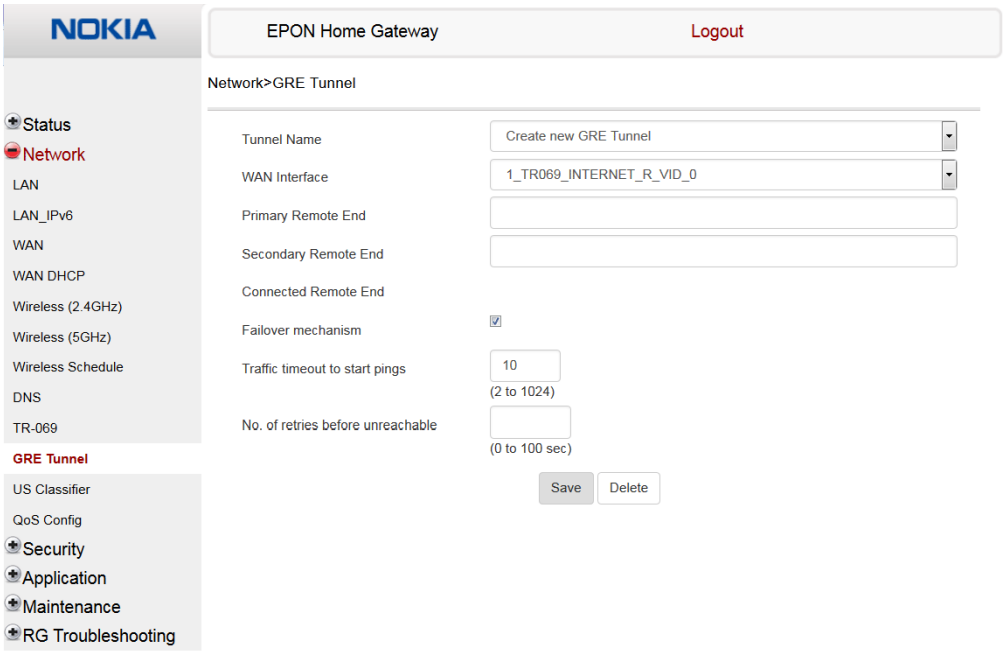


Table 26 describes the fields in the GRE Tunnel window.

Table 26 **GRE Tunnel parameters**

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

(1 of 2)

Field	Description
Connected Remote End	This field displays the current data traffic path for the GRE tunnel.
Failover mechanism	This feature is automatically selected by the system.
Traffic timeout to start pings	Enter the traffic timeout in seconds (0 to 100).
No. of retries before unreachable	Enter the number of retries before the tunnel is declared down (2 to 1024).

(2 of 2)

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

3 Click Save.

4 STOP. This procedure is complete.

Procedure 25 Upstream (US) Classifier configuration

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

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

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

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

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

1 Select Network > US Classifier from the top-level menu in the EPON Home Gateway window, as shown in Figure 41.

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

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

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

Figure 41 **US Classifier window**

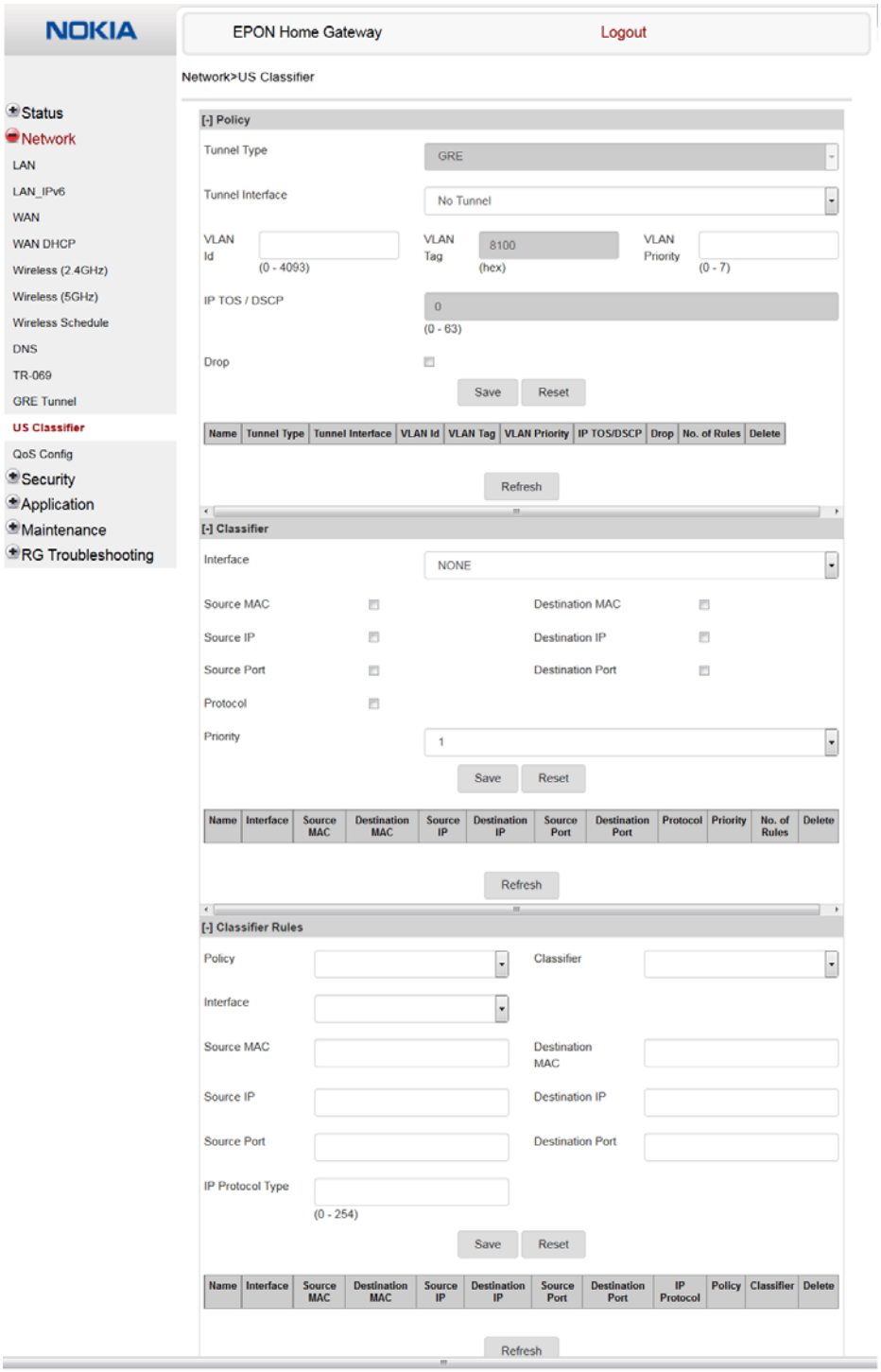


Table 27 describes the fields in the US Classifier window.

Table 27 US Classifier parameters

Field	Description
Policy parameters	
Tunnel Type	The tunnel type is set to GRE and cannot be modified.
Tunnel Interface	Choose a tunnel interface from the drop-down menu: No Tunnel, GRE Tunnel, or LAN traffic.
VLAN ID	Enter a VLAN ID (0-4094).
VLAN Tag	This field is not configurable. The VLAN tag is set to 8100.
VLAN Priority	Enter a VLAN priority level (0 to 7). A lower number indicates a higher priority.
IP TOS/DSCP	This field is not configurable. All tunnel packets are generated with a default DSCP value (usually 0).
Classifier parameters	
Interface	Choose an interface from the drop-down menu, for example: None, LAN, 2.4G SSID, 5G SSID.
Source MAC	Click to enter a source MAC.
Destination MAC	Click to enter a destination MAC.
Source IP	Click to enter a source IP.
Destination IP	Click to enter a destination IP.
Source Port	Click to enter a source port.
Destination Port	Click to enter a destination port.
Protocol	Click to enter a protocol.
Priority	Choose a priority level from 1 to 8. The lower the number, the higher the priority. No more than 1 classifier can be created with the same priority.
Classifier Rules parameters	
Policy	Choose a policy from the drop-down menu.
Classifier	Choose a classifier from the drop-down menu.
Interface	Choose an interface from the drop-down menu, for example: None, LAN, 2.4G SSID, 5G SSID.
Source MAC	Enter a source MAC.
Destination MAC	Enter a destination MAC.
Source IP	Enter a source IP.
Destination IP	Enter a destination IP.
Source Port	Enter a source port.
Destination Port	Enter a destination port.
IP Protocol type	Enter a value between 0 and 254.

2 Select a tunnel interface.

3 Enter a VLAN ID and priority level.

4 Click Save.

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

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

6 Configure the US classifier.

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

7 Click Save.

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

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

9 Configure the classifier rule.

10 Click Save.

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

12 STOP. This procedure is complete.

Procedure 26 QoS configuration

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

Figure 42 shows the window for configuring QoS L3 (Layer 3 packet sizes).

Figure 42 **QoS Config window (L3)**

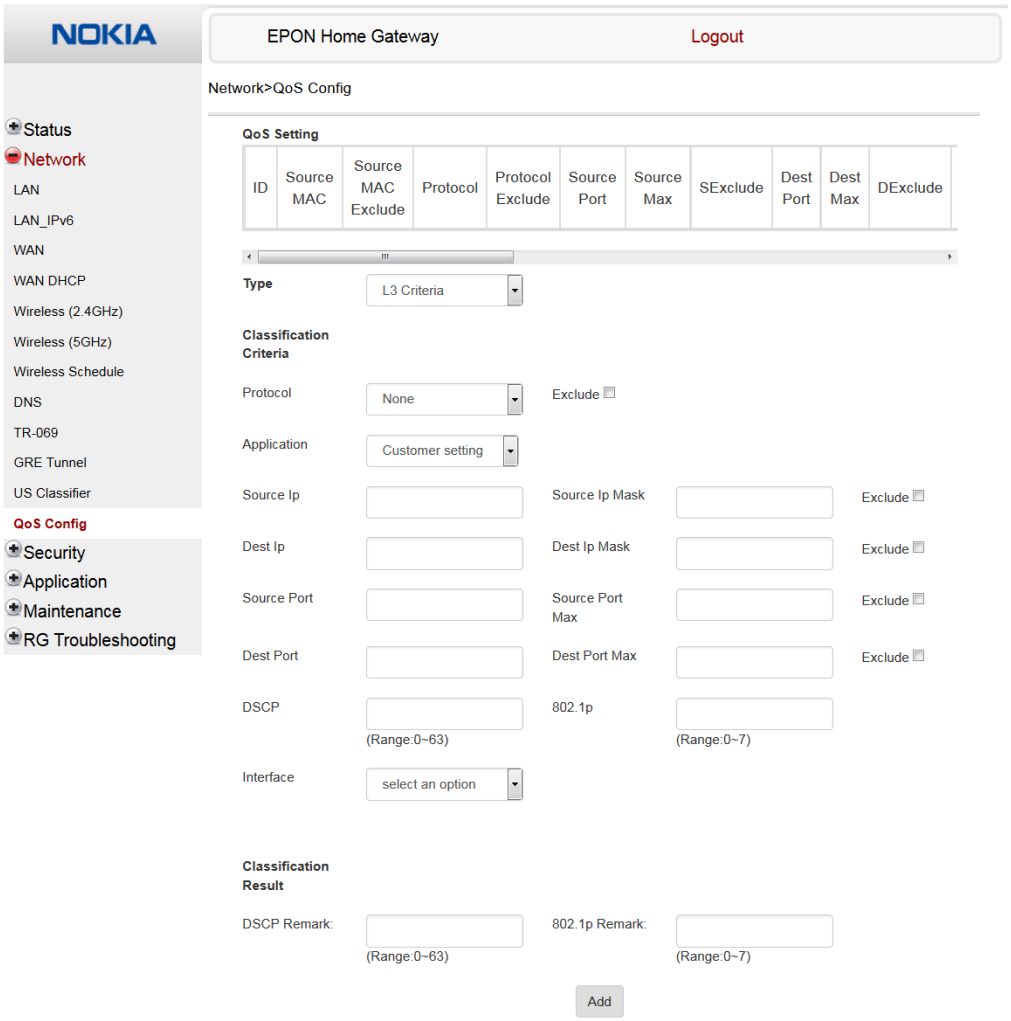


Table 28 describes the fields in the QoS Config window.

Table 28 **QoS Config parameters**

Field	Description
Type	Choose a QoS service layer type from the drop-down menu L2 or L3.
Source MAC	Enter the source MAC. Select the Exclude checkbox to exclude the source MAC
Interface	Choose an interface from the drop-down menu

(1 of 2)

Field	Description
802.1p Remark	Enter the value for the 802.1p (range: 0-7)
DSCP Remark	Enter the value for the DSCP mark (range: 0-63)
Additional fields for L3	
Protocol	Choose a protocol from the drop-down menu, or select the Exclude checkbox
Application	Choose an application from the drop-down menu
Source IP and Source IP Mask	Enter the values for the source IP and IP mask, or select the Exclude checkbox
Destination IP and Destination IP Mask	Enter the values for the destination IP and IP mask, or select the Exclude checkbox
Source Port and Source Port Max	Enter the values for the source port and port max (highest port number) or select the Exclude checkbox
Destination Port and Destination Port Max	Enter the values for the destination port and port max (highest port number), or select the Exclude checkbox

(2 of 2)

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

3 Configure a QoS policy.

4 Click Add to add a QoS policy.

5 STOP. This procedure is complete.

7.2.4 Security configuration

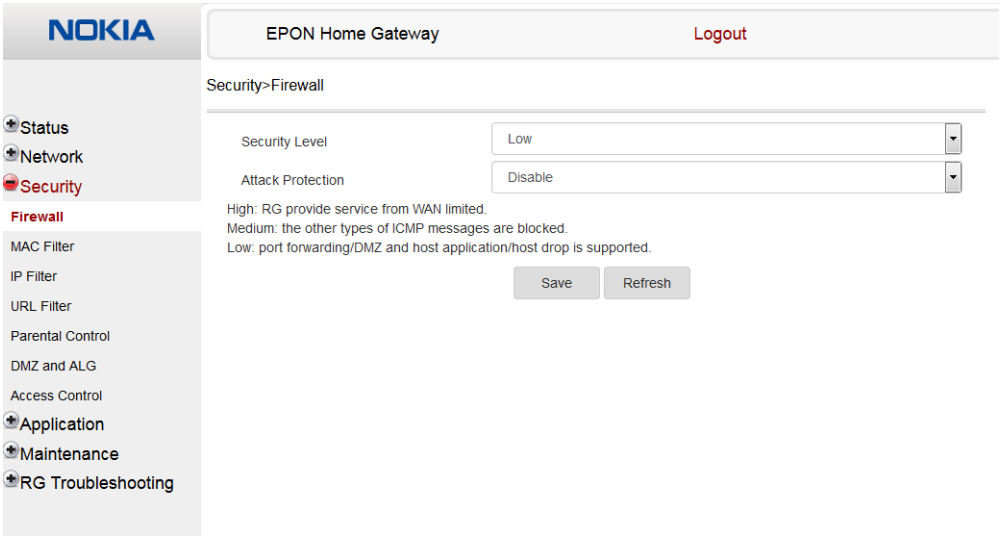
E-240W-A ONT also supports security configuration, including:

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

Procedure 27 Firewall configuration

1 Select Security > Firewall from the top-level menu in the EPON Home Gateway window, as shown in Figure 43.

Figure 43 **Firewall window**



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

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.

At the Medium 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, 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 29 describes the fields in the firewall window.

Table 29 **Firewall parameters**

Field	Description
Security level	Choose the security level from the drop-down menu: low, medium, or high

(1 of 2)

Field	Description
Attack Protect (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 28 MAC filter configuration

1 Select Security > Mac Filter from the top-level menu in the EPON Home Gateway window, as shown in Figure 44.

Figure 44 **MAC filter window**

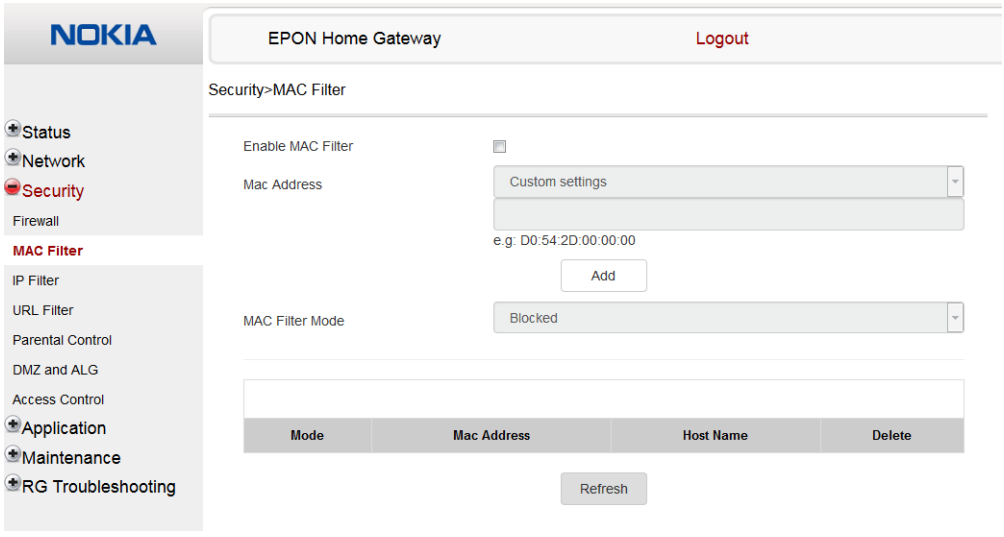


Table 30 describes the fields in the MAC filter window.

Table 30 **MAC filter parameters**

Field	Description
Enable MAC filter	Select this checkbox to enable the MAC filter
Mac Address	Choose a MAC address from the drop-down menu or enter the address in the text field
Mac Filter Mode	Choose the MAC filter mode from this drop-down menu: Blocked or Allowed

2 Click Refresh to update the information.

3 Configure a MAC filter.

4 Click Add.

5 STOP. This procedure is complete.

Procedure 29 IP filter configuration

1 Select Security > IP filter from the top-level menu in the EPON Home Gateway window, as shown in Figure 45.

Figure 45 **IP filter window**

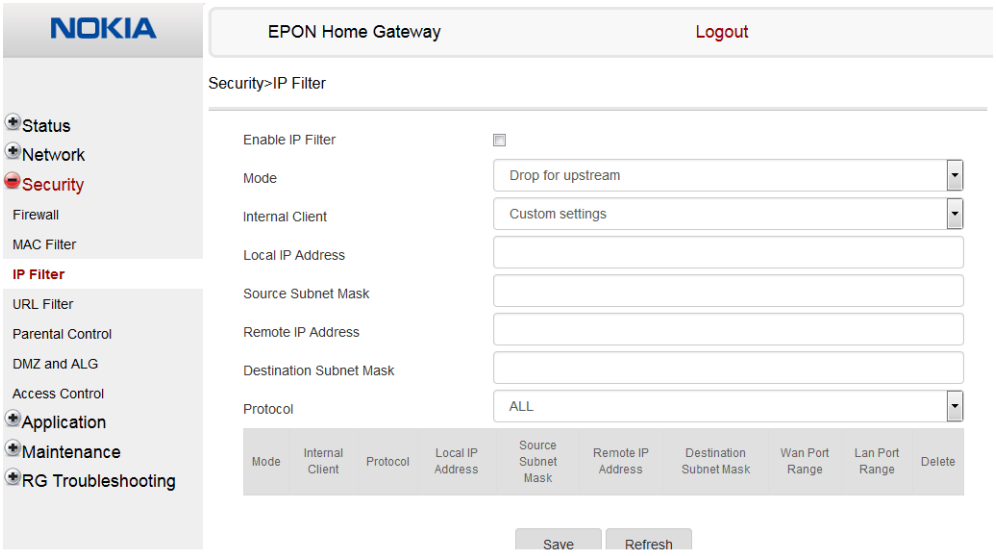


Table 31 describes the fields in the IP filter window.

Table 31 **IP filter parameters**

Field	Description
Enable IP Filter	Select this checkbox 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 ONT
Local IP Address	Local IP address
Source Subnet Mask	Source subnet mask
Remote IP Address	Remote IP address
Destination Subnet Mask	Destination subnet mask
Protocol	Choose an application protocol or all from the drop-down menu

2 Configure the IP filter.

3 Click Add.

4 STOP. This procedure is complete.

Procedure 30 URL filter configuration

1 Select Security > URL Filter from the top-level menu in the EPON Home Gateway window, as shown in Figure 46.

Figure 46 **URL Filter window**

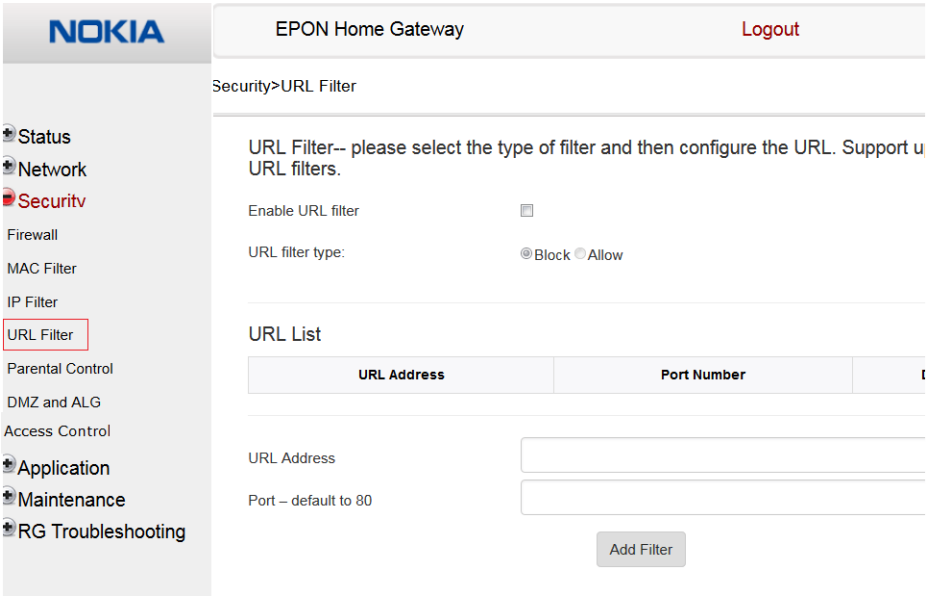


Table 32 describes the fields in the URL Filter window.

Table 32 **URL Filter parameters**

Field	Description
Enable URL filter	Select the checkbox to enable the URL filter
URL filter type	Select the checkbox for Exclude URL or Include URL
URL Address	Type the URL address
Port Number	Type the port number; the default is 80

2 Configure the URL Filter.

3 Click Add Filter.

4 STOP. This procedure is complete.

Procedure 31 Parental control

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

Figure 47 **Parental Control window**

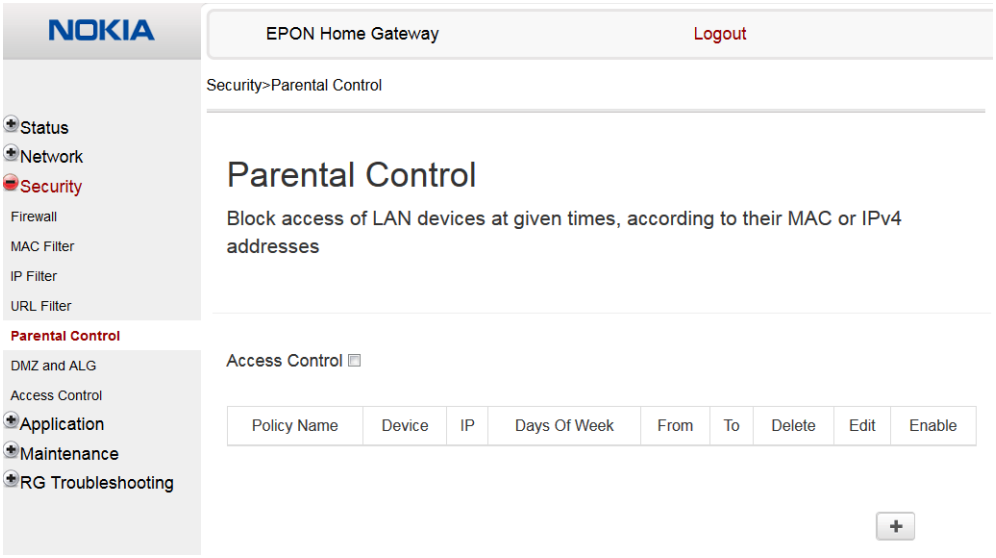


Table 33 describes the fields in the Parental Control window.

Table 33 **Parental control parameters**

Field	Description
Policy Name	Enter a name for the parental control policy or choose a policy from the list
Device	Enter the MAC address or choose a MAC address from the list
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 checkboxes for the days of the week for which the policy applies
From/To	Enter the times for the policy to be in effect

2 Select the Access Control checkbox.

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

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

4 Configure the parental control policy.

5 Click Enable to activate the policy.

6 STOP. This procedure is complete.

Procedure 32 DMZ and ALG configuration

1 Select Security > DMZ and ALG from the top-level menu in the EPON Home Gateway window, as shown in Figure 48.

Figure 48 **DMZ and ALG window**

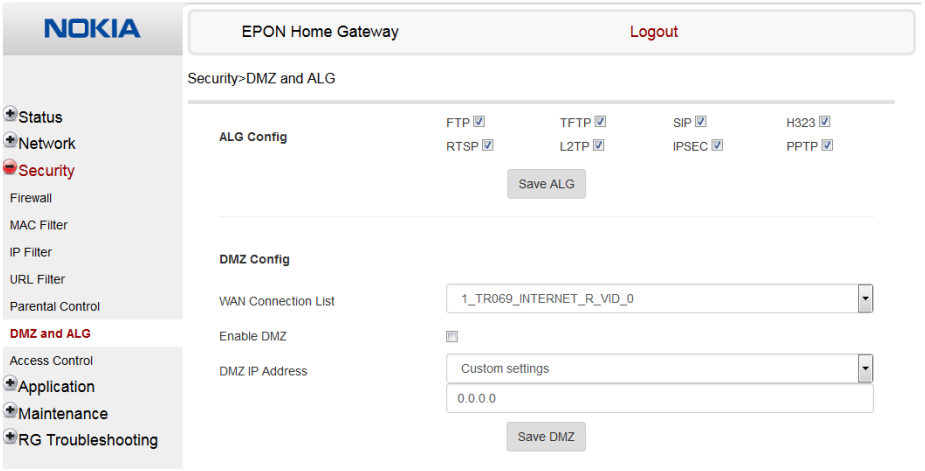


Table 34 describes the fields in the DMZ and ALG window.

Table 34 **DMZ and ALG parameters**

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

2	Configure ALG.
3	Click Save ALG.
4	Configure DMZ.
5	Click Save DMZ.
6	STOP. This procedure is complete.

Procedure 33 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 EPON Home Gateway window, as shown in Figure 49.

Figure 49 **Access Control window**

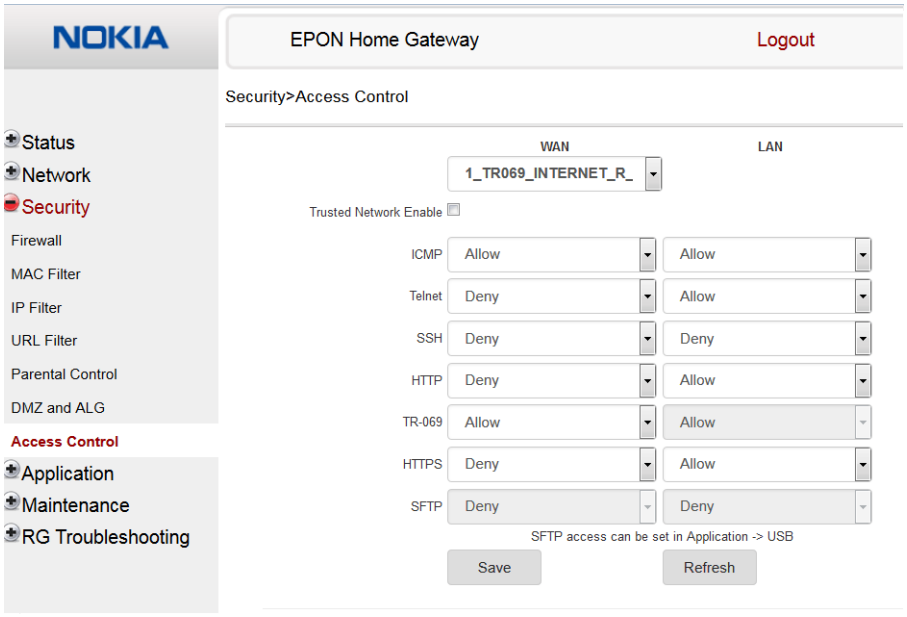


Table 35 describes the fields in the Access Control window.

Table 35 **Access control parameters**

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

5 Click Save.

6 Optionally, add one or more subnet trusted networks.

The maximum number of entries is 32.

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

7 STOP. This procedure is complete.

7.2.5 Application configuration

E-240W-A ONT also supports application configuration, including:

- port forwarding
- port triggering
- DDNS
- NTP
- USB storage

- UPnP and DLNA
- voice setting

Procedure 34 Port forwarding configuration

1 Select Application > Port forwarding from the top-level menu in the EPON Home Gateway window, as shown in Figure 50.

Figure 50 **Port forwarding window**

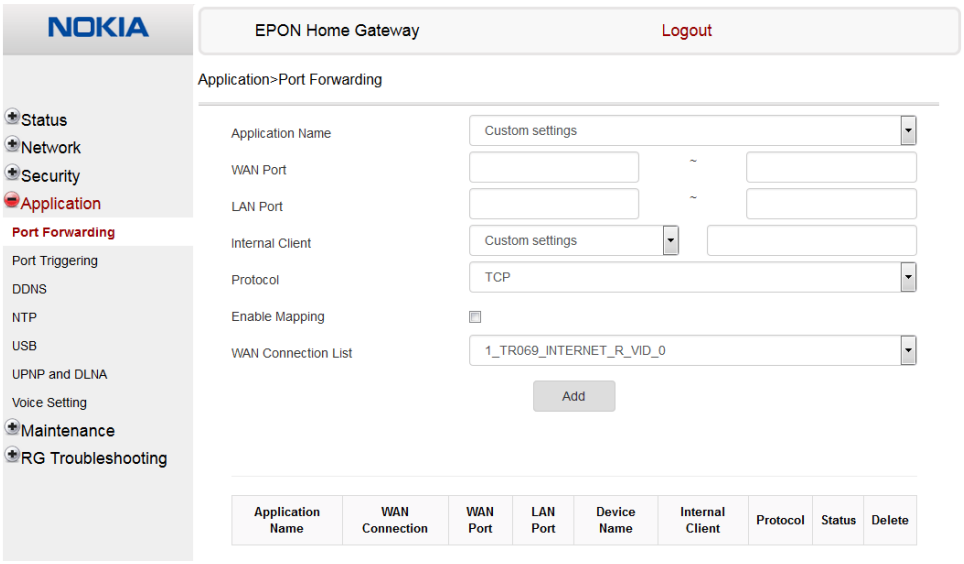


Table 36 describes the fields in the port forwarding window.

Table 36 **Port forwarding parameters**

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

(1 of 2)

Field	Description
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 forwarding.

3 Click Add.

4 STOP. This procedure is complete.

Procedure 35 Port triggering

1 Select Application > Port Triggering from the top-level menu in the EPON Home Gateway window, as shown in Figure 51.

Figure 51 **Port Triggering window**

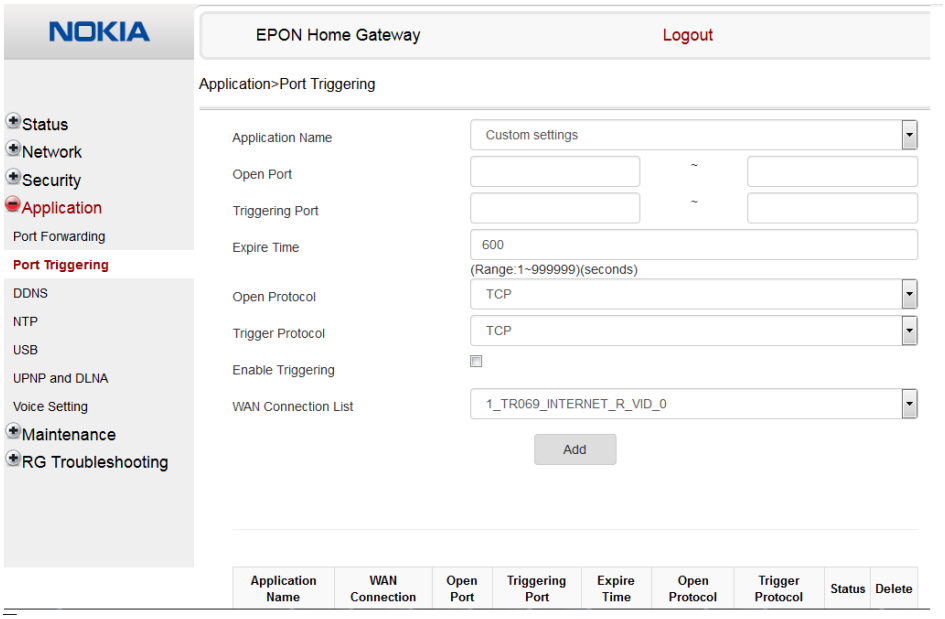


Table 37 describes the fields in the Port Triggering window.

Table 37 **Port triggering parameters**

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

2 Configure port triggering.

3 Click Add.

4 STOP. This procedure is complete.

Procedure 36 DDNS configuration

1 Select Application > DDNS from the top-level menu in the EPON Home Gateway window, as shown in Figure 52.

Figure 52 **DDNS window**

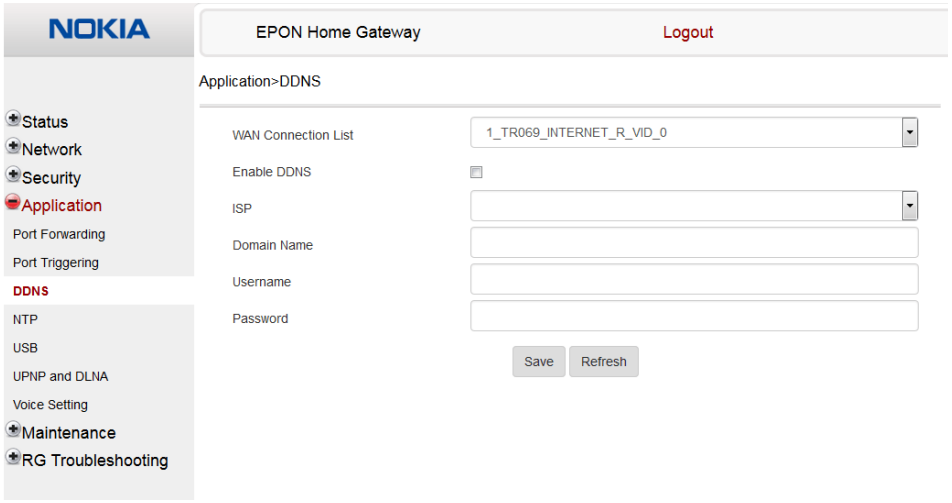


Table 38 describes the fields in the DDNS window.

Table 38 **DDNS parameters**

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

2 Configure DDNS.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 37 NTP configuration

1 Select Application > NTP from the top-level menu in the EPON Home Gateway window, as shown in Figure 53.

Figure 53 **NTP window**

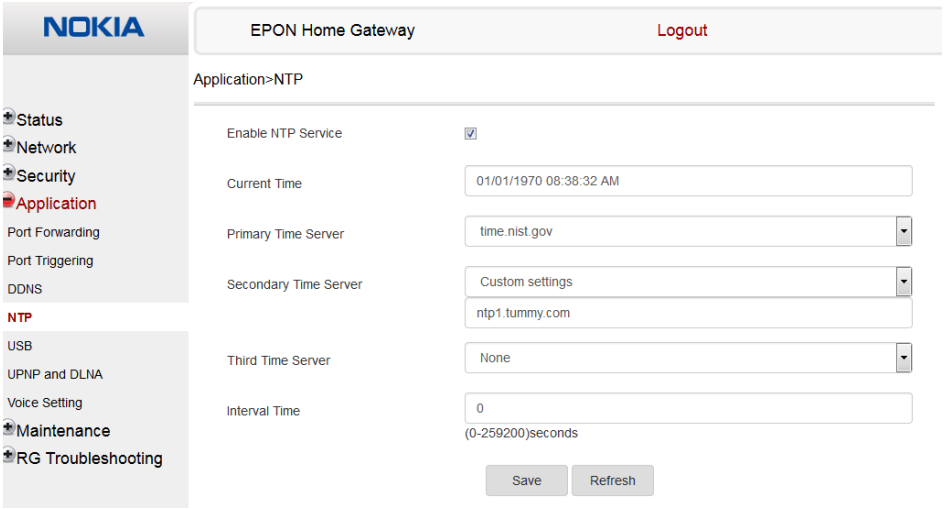


Table 39 describes the fields in the NTP window.

Table 39 **NTP parameters**

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

(1 of 2)

Field	Description
Interval Time	Interval at which to get the time from the time server, in seconds

(2 of 2)

2 Configure NTP.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 38 USB configuration

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

Figure 54 **USB window**

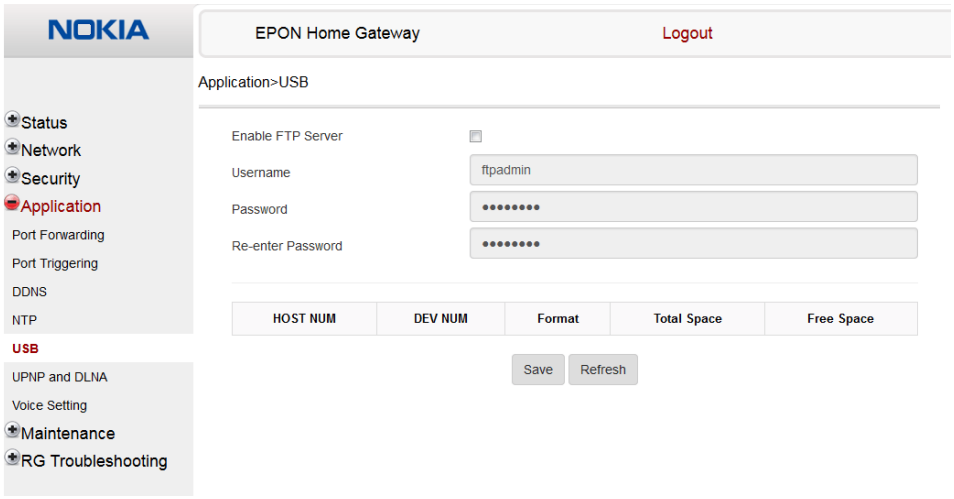


Table 40 describes the fields in the USB window.

Table 40 **USB parameters**

Field	Description
Enable FTP server	Select this checkbox to enable using an FTP server for data storage
Username	Username for FTP server

(1 of 2)

Field	Description
Password	Password for FTP server
Re-enter Password	Password for FTP server

(2 of 2)

2 Configure USB.

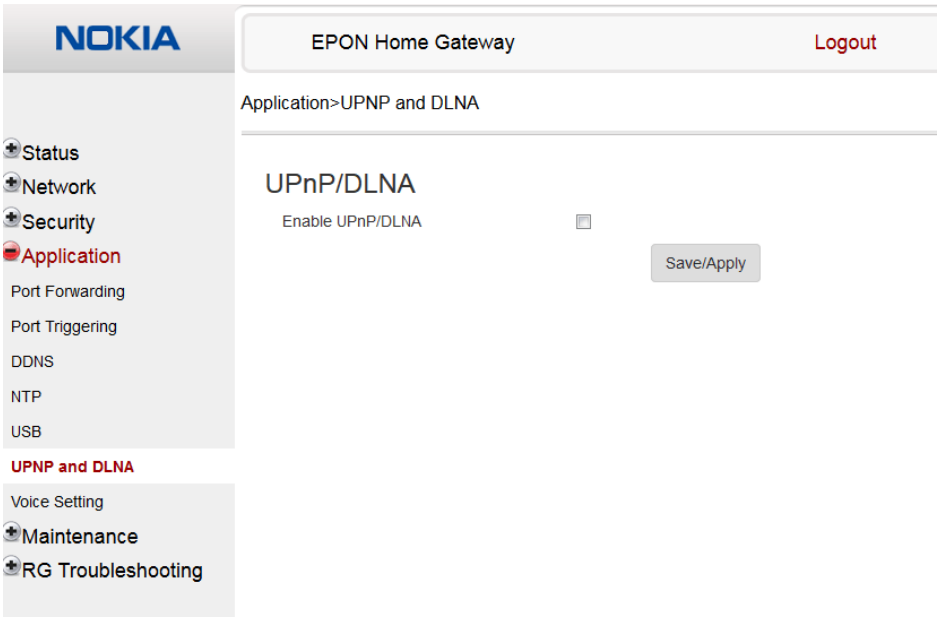
3 Click Save.

4 STOP. This procedure is complete.

Procedure 39 UPnP and DLNA configuration

1 Select Application > UPnP and DLNA from the top-level menu in the EPON Home Gateway window, as shown in Figure 55.

Figure 55 **UPnP and DLNA window**



2 Select the Enable UPnP checkbox to enable UPnP.

3	Click Save/Apply.
4	STOP. This procedure is complete.

Procedure 40 Voice setting

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

Figure 56 **Voice setting window**

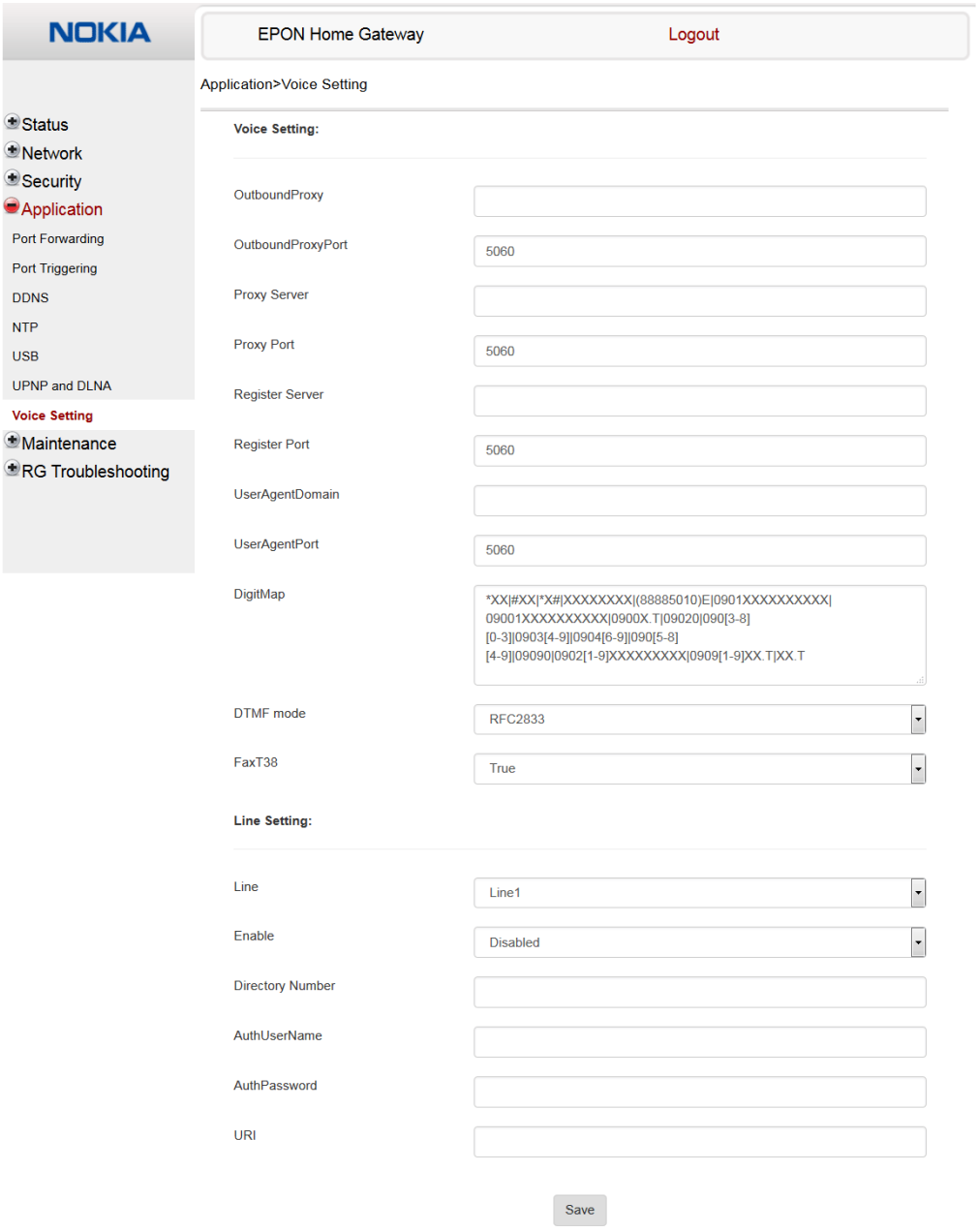


Table 41 describes the fields in the Voice Setting window.

Table 41 **Voice setting parameters**

Field	Description
Outbound Proxy	Enter the SIP outbound proxy
Outbound Proxy Port	Enter the outbound proxy port
Proxy Server	Enter the proxy server
Proxy Port	Enter the proxy port
Register Server	Enter the register server
Register Port	Enter the register port
User Agent Domain	Enter the user agent domain
User Agent Port	Enter the user agent port
DTMF Mode	Choose InBand, rfc2822, Info, or Auto from the drop-down menu
FaxT38	Choose False or True from the drop-down menu
Line	Choose a line from the drop-down menu
Enable	Choose Enabled or Disabled from the drop-down menu
Directory Number	Enter a directory number
AuthUserName	Enter an authorized user name
AuthPassword	Enter a password for the user
URL	Enter the URL

2 Configure voice setting.

3 Click Save.

4 STOP. This procedure is complete.

7.2.6 Maintenance

E-240W-A ONT also supports maintenance tasks, including:

- change password
- manage device
- backup and restore
- upgrade firmware
- reboot device

- restore factory defaults
- diagnose WAN connections
- view log

Procedure 41 Password configuration

1 Select Maintenance > Password from the top-level menu in the EPON Home Gateway window, as shown in Figure 57.

Figure 57 **Password window**

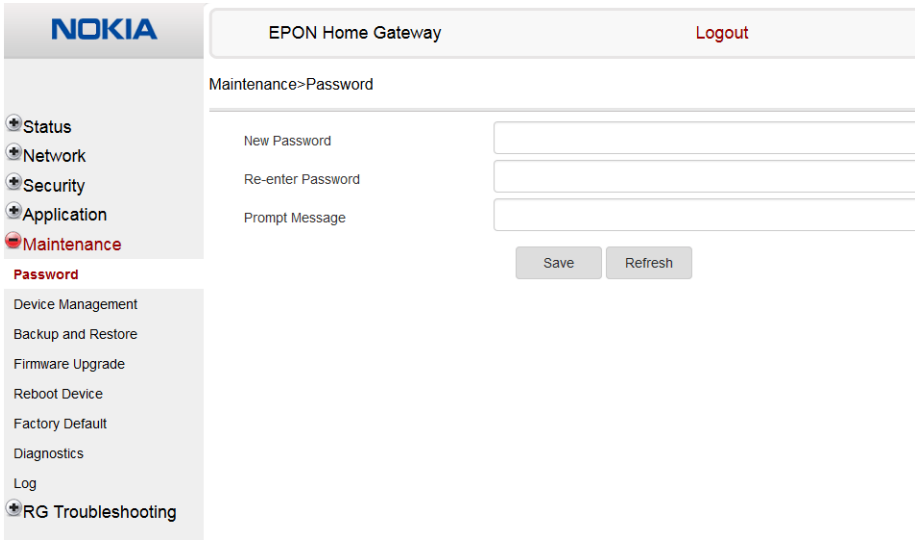


Table 42 describes the fields in the password window.

Table 42 **Password parameters**

Field	Description
New Password	New password
Re-enter password	Password must match password entered above
Prompt message	Password prompt message

2 Configure the new password.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 42 Device management

1 Select Maintenance > Device Management from the top-level menu in the EPON Home Gateway window, as shown in Figure 58.

Figure 58 **Device management window**

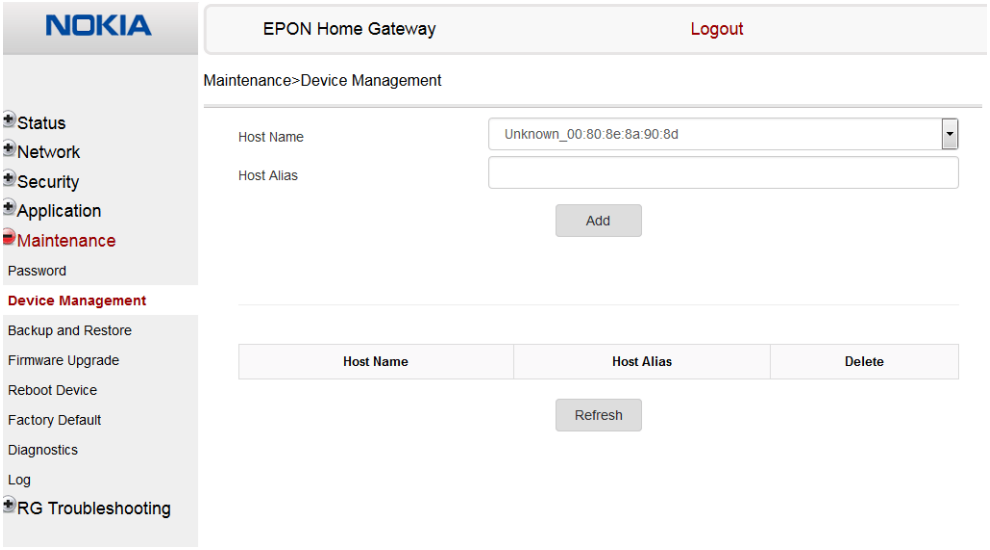


Table 43 describes the fields in the Device management window.

Table 43 **Device management parameters**

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

2 Configure an alias for a specific host.

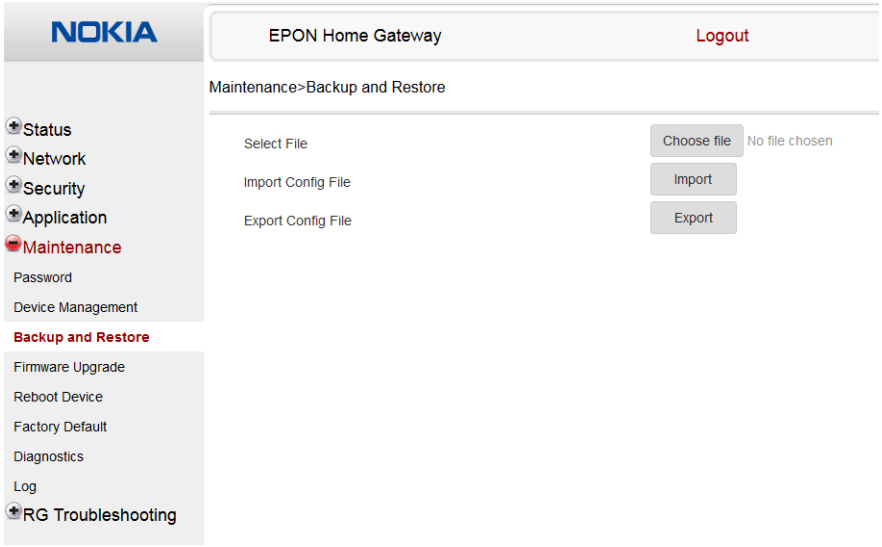
3 Click Add.

4 STOP. This procedure is complete.

Procedure 43 Backup and restore

1 Select Maintenance > Backup and Restore from the top-level menu in the EPON Home Gateway window, as shown in Figure 59.

Figure 59 **Backup and Restore window**



2 Click Select File and choose the backup file.

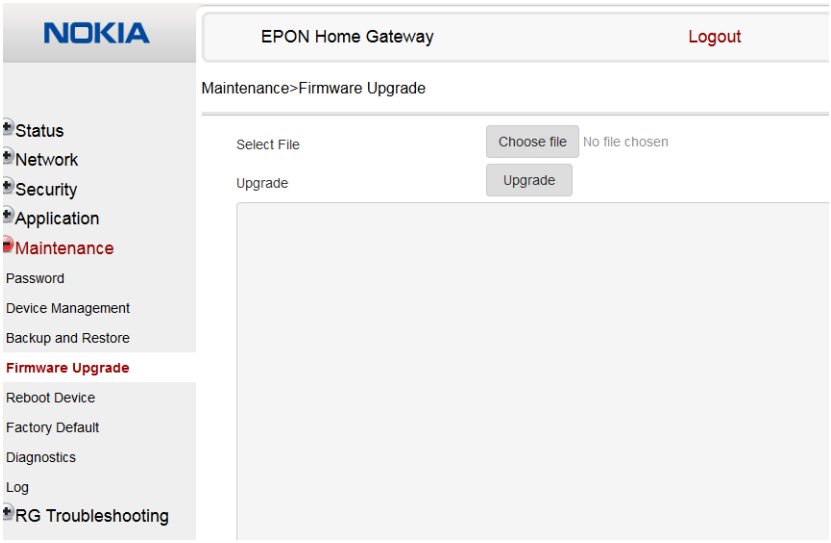
3 Click Import Config File to restore the ONT to the saved backup or click Export Config File to export the current ONT configuration to the backup file.

4 STOP. This procedure is complete.

Procedure 44 Upgrade firmware

1 Select Maintenance > Firmware Upgrade from the top-level menu in the EPON Home Gateway window, as shown in Figure 60.

Figure 60 **Firmware upgrade window**



2 Click Select File and choose the firmware file.

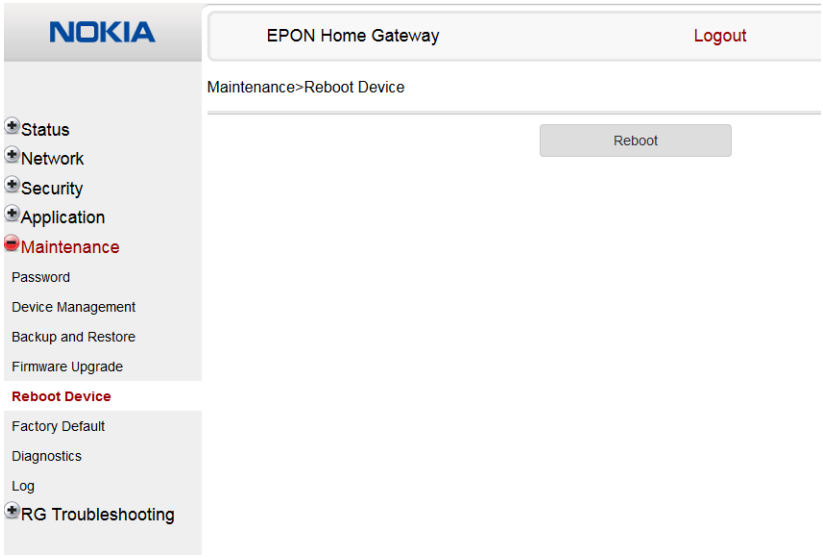
3 Click Upgrade to upgrade the firmware.

4 STOP. This procedure is complete.

Procedure 45 Reboot ONT

1 Select Maintenance > Reboot Device from the top-level menu in the EPON Home Gateway window, as shown in Figure 61.

Figure 61 **Reboot Device window**



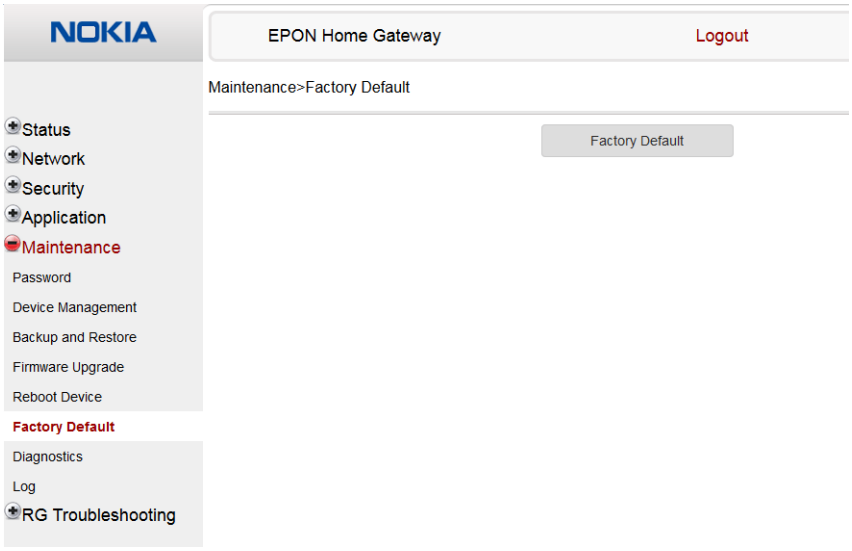
2 Click Reboot to reboot the ONT.

3 STOP. This procedure is complete.

Procedure 46 Restore factory defaults

1 Select Maintenance > Factory Default from the top-level menu in the EPON Home Gateway window, as shown in Figure 62.

Figure 62 **Factory default window**



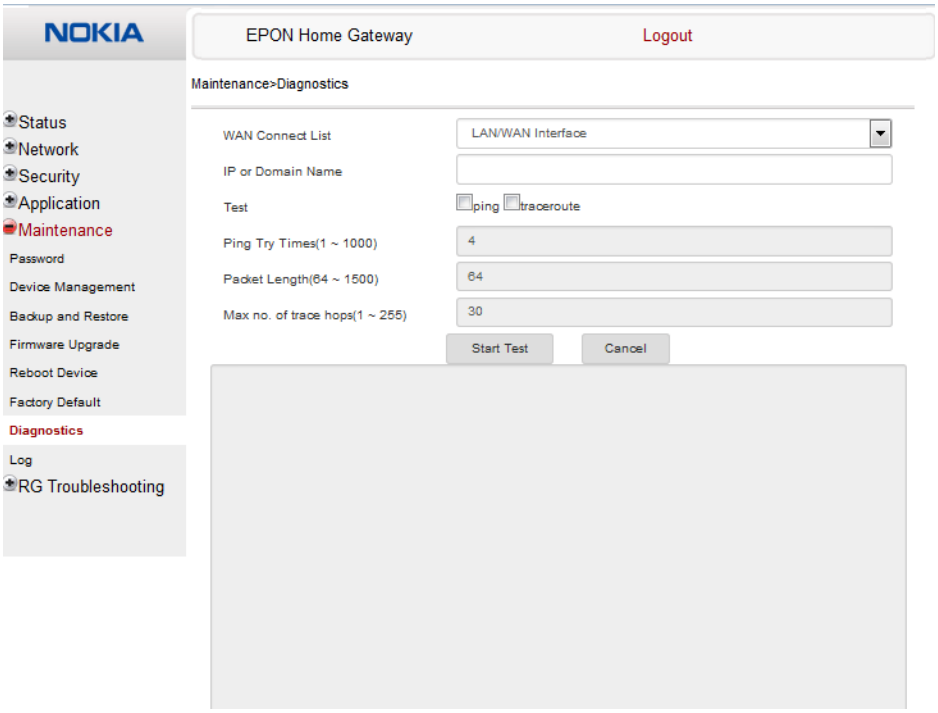
2 Click Factory Default to reset the ONT to its factory default settings.

3 STOP. This procedure is complete.

Procedure 47 Diagnose WAN connections

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

Figure 63 **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 - 1000); the default is 4.

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

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

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

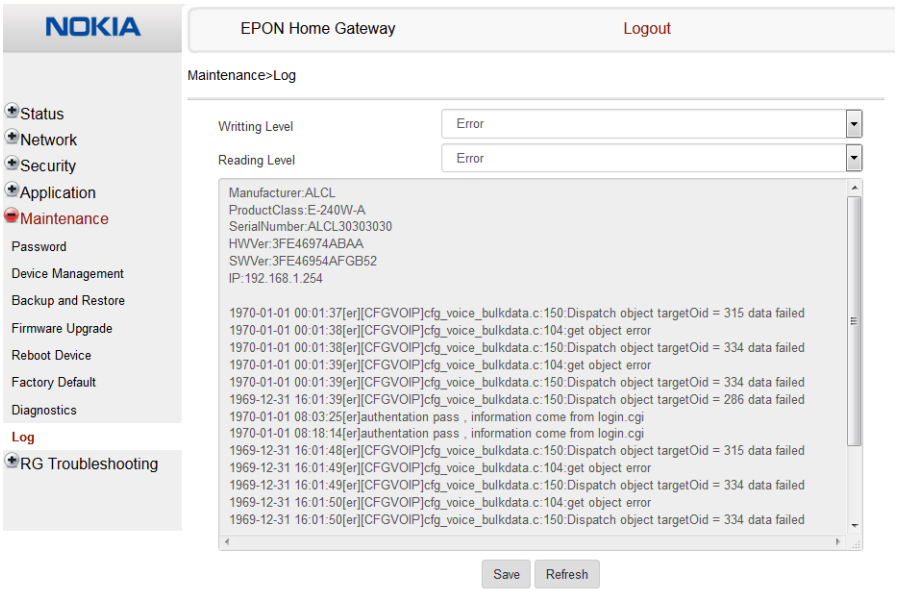
9 Click Cancel to cancel the test.

10 STOP. This procedure is complete.

Procedure 48 View log files

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

Figure 64 **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.

7.2.7 RG troubleshooting counters

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

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

Procedure 49 Retrieve Residential Gateway (RG) troubleshoot counters

1 Select RG Troubleshoot Counters from the left menu in the EPON Home Gateway window.

The RG Troubleshoot Counters window appears; see Figure 65.

Figure 65 **RG Troubleshoot Counters window**

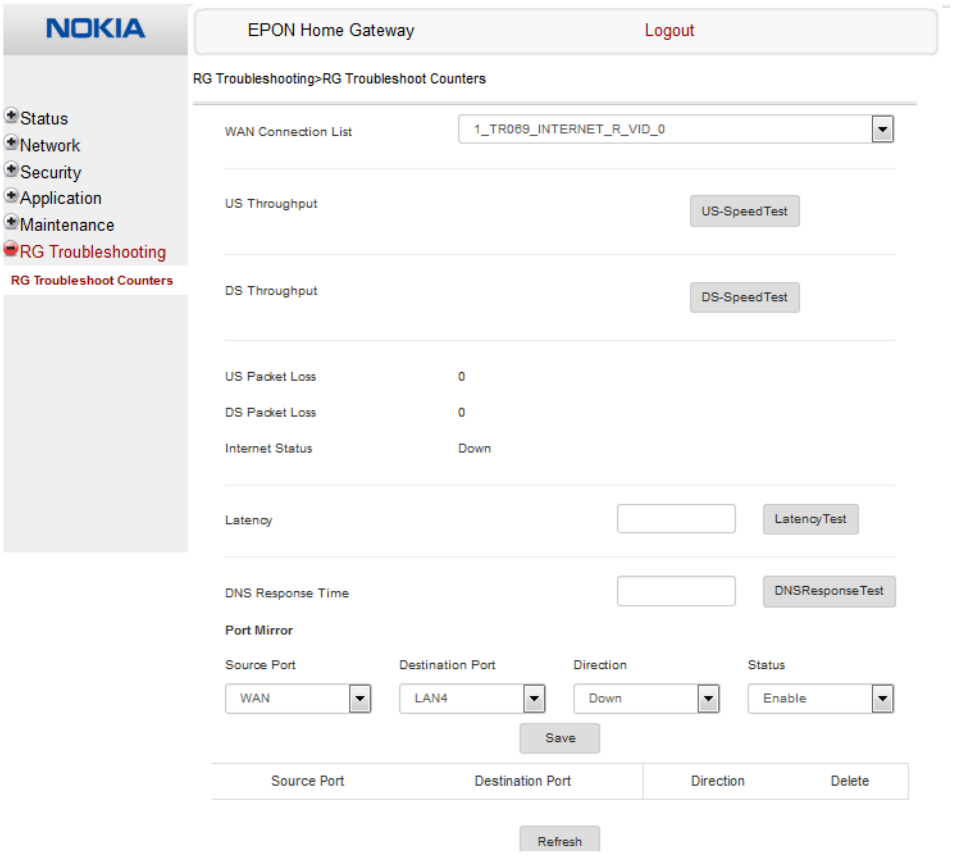


Table 44 describes the fields in the RG Troubleshoot Counters window.

Table 44 **RG Troubleshoot Counters parameters**

Field	Description
WAN Connection List	Choose a WAN connection from the drop-down menu
US Throughput	This test is used to determine the upstream throughput/speed Click US Speed Test to specify the time for the upstream test The default is weekly, performed at idle to a public server
DS Throughput	This test is used to determine the downstream throughput/speed Click DS Speed Test to specify the time for the downstream test The default is weekly, performed at idle to a public server
US Packet Loss	The number of upstream packages lost
DS Packet Loss	The number of downstream packages lost
Internet Status	Whether the broadband connections is active (UP) or not (DOWN)

(1 of 2)

Field	Description
Latency	This test is used to determine the lowest round-trip time in milliseconds by pinging the target server multiple times Click Latency Test to specify the time for the test The default is weekly, performed at idle to a public server
DNS Response Time	This test is used to determine the lowest round-trip time in milliseconds by sending a request to the target DNS server Click DNS Response Test to specify the time for the test The default is weekly, performed at idle to a public server
Port Mirror	Choose the source and destination ports, the direction (up or down), and the status (enable or disable) from the drop-down menu, and click Save

(2 of 2)

2 Configure the tests.

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-46974-AAAA-TCZZA