NOKIA

7368 Intelligent Services Access Manager CPE

7368 ISAM CPE HA-030W-B Product Guide

3FE-47429-AAAA-TCZZA

Issue: 01

3FE-47429-AAAA-TCZZA

1 Preface

This preface provides general information about the documentation set for CPEs.

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 CPEs.

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. If this link does not work, copy and paste it directly into your web browser.

For ordering information, contact your Nokia sales representative.

1.6   Nokia quality processes

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

1.7   Safety information

For safety information, see the appropriate safety guidelines chapter.

1.8   Documents

Documents are available using ALED or OLCS.

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

1   Navigate to http://support.alcatel-lucent.com and enter your user name and password. If you are a new user and require access to this service, please contact your Nokia sales representative.

2   From the Technical Content for drop-down menu, choose the product.

3   Click on Downloads: Electronic Delivery.

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

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

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

Procedure 2   To access individual documents

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

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

1.9   Special information

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

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

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

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

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

1.9.1 Procedures with options or substeps

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

Procedure 3   Example of options in a procedure

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

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

    a   This is one option.

    b   This is another option.

2   You must perform this step.

Procedure 4   Example of required substeps in a procedure

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

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

    i   This is the first substep.

    ii   This is the second substep.

    iii   This is the third substep.

2   You must perform this step.

1.10   Multiple PDF document search

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

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

Procedure 5   To search multiple PDF files for a common term

1	Open Adobe Acrobat Reader.
2	Choose Edit→Search from the Acrobat Reader main menu. The Search PDF panel appears.
3	Enter the search criteria.
4	Click on the All PDF Documents In radio button.
5	Select the folder in which to search using the drop-down menu.
6	Click on the Search button. Acrobat Reader displays the search results. You can expand the entries for each document by clicking on the + symbol.

Table of contents

List of figures

List of tables

2 ANSI CPE safety guidelines

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

2.1 Safety instructions

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

2.1.1 Safety instruction boxes in customer documentation

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

The following is an example of the Danger box.

Danger — Possibility of personal injury.

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

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

The following is an example of the Warning box.

Warning 1 — Possibility of equipment damage.

Warning 2 — Possibility of data loss.

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

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

The following is an example of the Caution box.

Caution 1 — Possibility of service interruption.

Caution 2 — Service interruption.

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

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

The following is an example of the Note box.

Note — Information of special interest.

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

2.1.2   Safety-related labels

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

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

Table 1   **Safety labels**

Description	Label text
ETL compliance	Communication service equipment US listed. Type 3R enclosure - Rainproof.
TUV compliance	Type 3R enclosure - Rainproof.
ESD warning	Caution: This assembly contains electrostatic sensitive device.
FCC standards compliance	Tested to comply with FCC standards for home or office use.
CDRH compliance	Complies with 21 CFR 1040.10 and 1040.11.
Operation conditions	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.
CE marking	There are various CE symbols for CE compliance.

Figure 1 shows a sample safety label on the CPE equipment.

Figure 1   **Sample safety label on the CPE equipment**

Tested to Comply
with FCC Standards

FOR HOME OR OFFICE USE

COMMUNICATION SERVICE EQUIPMENT
LISTED
27FY

Type 3R Enclosure - Rainproof

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.

This Class A digital apparatus complies with Canadian ICES-003. Cet appareil
numerique de la class A est conforme a la norme NMB-003 du Canada

CAUTION
This Assembly Contains Electrostatic Sensitive Devices

18533

2.2   Safety standards compliance

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

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

2.2.1   EMC, EMI, and ESD standards compliance

The CPE equipment complies with the following requirements:
- Federal Communications Commission (FCC) CFR 47, Part 15, Subpart B, Class
  B requirements for OLT equipment
- GR-1089-CORE requirements, including:
  - Section 3 Electromagnetic Interference, Emissions Radiated and Conducted
  - Section 3 Immunity, Radiated and Conducted
  - Section 2 ESD Discharge Immunity: System Level Electrostatic Discharge and EFT
    Immunity: Electrically Fast Transients

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

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

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

2.2.2   Equipment safety standard compliance

The CPE equipment complies with the requirements of UL60950-1, Outdoor CPEs to "Communication Service Equipment" (CSE) and Indoor CPEs to Information Technology Equipment (ITE).

2.2.3   Environmental standards compliance

The CPE equipment complies with the following standards:

- GR-63-CORE (NEBS): requirements related to operating, storage, humidity, altitude, earthquake, office vibration, transportation and handling, fire resistance and spread, airborne contaminants, illumination, and acoustic noise
- GR-487-CORE: requirements related to rain, chemical, sand, and dust
- GR-487 R3-82: requirements related to condensation
- GR-3108: Requirements for Network Equipment in the Outside Plant (OSP)
- TP76200: Common Systems Equipment Interconnections Standards

2.2.4   Resistibility requirements compliance

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

2.3   Electrical safety guidelines

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

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

2.3.1   Power supplies

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

2.3.2   Cabling

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

- Use only cables approved by the relevant national electrical code.
- Use cables suitable for outdoor use for outdoor installation of CPEs.
- The CPEs have been evaluated for use with external POTS wiring without primary protection that may not exceed 140 ft (43 m) in reach. However, the power cable must not exceed 100 ft (31 m).

2.3.3   Protective earth

Earthing and bonding of the CPEs must comply with the requirements of NEC article 250 or local electrical codes.

2.4   ESD safety guidelines

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

Caution — This equipment is ESD sensitive. Proper ESD protections should be used when entering the TELCO Access portion of the CPE.

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

Nokia recommends that you prepare the site before you install the CPE equipment. In addition, you must control relative humidity, use static dissipating material for furniture or flooring, and restrict the use of air conditioning.

2.5   Environmental requirements

See the CPE technical specification documentation for temperature ranges for CPEs.

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

- The door of the CPE not be opened until temperature inside and outside the enclosure has stabilized.
- If the door of the CPE 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 CPE helps prevent condensation when the door is opened.

3 ETSI CPE safety guidelines

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

3.1 Safety instructions

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

3.1.1 Safety instruction boxes

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

The following is an example of the Danger box.

Danger — Possibility of personal injury.

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

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

The following is an example of the Warning box.

Warning 1 — Possibility of equipment damage.

Warning 2 — Possibility of data loss.

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

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

The following is an example of the Caution box.

Caution 1 — Possibility of service interruption.

Caution 2 — Service interruption.

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

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

The following is an example of the Note box.

Note — Information of special interest.

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

3.1.2   <Cond: Update> Safety-related labels

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

Table 2 provides sample safety labels on the CPE equipment.

Table 2   **Safety labels**

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

Figure 2 shows the PSE certification.

Figure 2 **PSE certification**

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

19841

3.2 <Cond: Update> Safety standards compliance

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

3.2.1 EMC, EMI, and ESD compliance

The CPE equipment complies with the following EMC, EMI, and ESD requirements:
- EN 300-386 V1.5.1: Electromagnetic Compatibility and Radio Spectrum Matters (ERM): Telecommunications Network Equipment; Electromagnetic Compatibility (EMC) requirements; Electrostatic Discharge (ESD) requirements
- EN 301489-1, -17
- EN 300328
- EN 301893
- EN 55022 (2006): Class B, Information Technology Equipment, Radio Disturbance Characteristics, limits and methods of measurement
- EN 55024 (2010): Information Technology Equipment, Immunity Characteristics, limits and methods of measurement
- European Council Directive 2004/108/EC
- EN 55022:2006 Class B (CPEs)

3.2.2 Equipment safety standard compliance

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

3.2.3   Environmental standard compliance

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

3.2.4   Resistibility requirements compliance

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

3.2.5   Acoustic noise emission standard compliance

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

3.3   <Cond: Update> Electrical safety guidelines

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

Note 1 — The CPEs 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 CPEs comply with BS EN 61140.

3.3.1   Power supplies

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

3.3.2   Cabling

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

- All cables must be approved by the relevant national electrical code.
- The cables for outdoor installation of CPEs 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.

3.3.3   Protective earth

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

3.4   <Cond: Update> ESD safety guidelines

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

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

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

3.5   <Cond: Update> Environmental requirements

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

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

- The door of the CPE not be opened until temperature inside and outside the enclosure has stabilized.
- If the door of the CPE 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 CPE helps prevent condensation when the door is opened.

4 ETSI environmental and CRoHS guidelines

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

4.1 Environmental labels

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

4.1.1 Overview

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

4.1.2 Environmental related labels

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

4.1.2.1 Products below Maximum Concentration Value (MCV) label

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

Figure 3   **Products below MCV value label**

18986

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

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

Figure 4   **Products above MCV value label**

18985

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

4.2   Hazardous Substances Table (HST)

This section describes the compliance of the OLT and CPE 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 CPE documentation.

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

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

3FE-47429-AAAA-TCZZA

4.3   Other environmental requirements

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

4.3.1   CPE environmental requirements

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

4.3.2   Transportation

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

4.3.3   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.

4.3.4   Material content compliance

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

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

4.3.5   End-of-life collection and treatment

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

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

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

At the end of their life, the OLT and CPE 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 5 at the end of their useful life, or products displaced by Nokia equipment offers. For information regarding take-back of equipment by Nokia, or for more information regarding the requirements for recycling/disposal of product, contact your Nokia account manager or Nokia take back support at sustainability.global@nokia.com.

5 HA-030W-B CPE unit data sheet

5.1   HA-030W-B CPE part numbers and identification

Table 3 provides part numbers and identification information for the HA-030W-B CPE.

Table 3   **Identification of HA-030W-B CPE**

Ordering part number	Provisioning number	Description	CLEC	CPR	ECI/ Bar code
3FE 47357 AA	3FE 47429 AA	WiFi Access Point and range extender, 1 Gigabit Ethernet UNI, 3x3 802.11n+4x4 802.11ac, 12V dc 1AC US plug variant.	—	—	—
3FE 47357 BA	3FE 4 7429 BA	WiFi Access Point and range extender, 1 Gigabit Ethernet UNI, 3x3 802.11n+4x4 802.11ac, 12V dc 1AC EU plug variant.	—	—	—
3FE 47357 CA	3FE 47429 CA	WiFi Access Point and range extender, 1 Gigabit Ethernet UNI, 3x3 802.11n+4x4 802.11ac, 12V dc 1AC UK plug variant.	—	—	—

5.2   HA-030W-B CPE general description

This is all from A-240Z-A. Please provide updated source.

HA-030W-B is the premium Ethernet gateway and AP/range extender as part of Nokia Whole Home WiFi solution.

The HA-030W-B CPE has built-in concurrent dual-band Wi-Fi® 802.11b/g/n and 802.11a/n/ac networking with triple play capability that simplifies the home equipment experience.

The HA-030W-B is a compact CPE that can easily fit on a desk or shelf. For dimensions, see section 5.6. Figure 6 shows the HA-030W-B in its stand.

Figure 6   **HA-030W-B CPE**
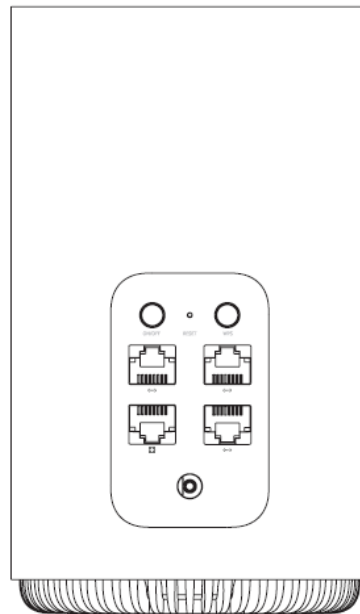
TI028232

The HA-030W-B CPE provides the following functions:

- GE Ethernet uplink

- Concurrent 802.11n 3x3 MIMO in 2.4GHz and 802.11a/n/ac 4x4 MIMO in 5GHz
- auto-negotiation for speed and duplex on a port by port basis
- routed mode per LAN port
- Advanced data features: VLAN tag manipulation, classification, and filtering
- Traffic classification and QoS capability
- MDI/MDIX auto-negotiation
- Line Rate L2 traffic
- Internal Switch
- UPnP IGD2.0 support
- Internal DHCP server, with configurable DHCP pool and gateway
- 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.
- WPS on/off button
- Ethernet-based Point-to-Point (PPPoE)
- Network Address Translation (NAT)
- Network Address Port Translation (NAPT)
- ALG and UPnP port forwarding
- DMZ
- IP/MAC filter
- Multi-level firewall
- DNS server
- DHCP client/server
- support for HT40 mode for increased channel bandwidth
- support for up to 32 simultaneous wireless connections
- remote software image download

5.2.1   <Cond: Update> TR-069 object support for WiFi parameters

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

- channel
- SSID

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

These are the same TR-069 object parameters that are supported in the GUI. For more information, see Tables 20 and 21 in the chapter "Configure an HA-030W-B CPE".

5.2.2   <Cond: Update> Independent TR69 session with Saas

The prime communication between the Nokia Motive cloud solution and the HA-030W-B CPE is TR-069.

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

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

5.2.3   <Cond: Update> TR69 authentication using TLS and CA certificates

HA-030W-B CPEs support TLS, as well as ACS authentication using SHA-256 pre-installed certificates.

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

5.3   HA-030W-B CPE software and installation feature support

For information on installing or replacing the HA-030W-B CPE, see:

- Install an HA-030W-B CPE
- Replace an HA-030W-B CPE

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

- General descriptions of features and functions
- Ethernet interface specifications
- Wi-Fi specifications
- SLID entry via Ethernet port

5.4   HA-030W-B CPE interfaces and interface capacity

Table 4 describes the supported interfaces and interface capacity for HA-030W-B CPEs.

Table 4   **HA-030W-B CPE interface connection capacity**

CPE type and model	Maximum capacity								
	POTS	**10/ 100 BASE-T**	**10/ 100/1000 1000 BASE-T**	**RF video (CATV)**	**MoCA**	**VDSL2**	**E1/T1**	**Local craft**	**GE uplink**
HA-030W-B	—	—	3	—	—	—	—	—	1

5.4.1   HA-030W-B CPE connections and components

Figure 7 shows the physical connections for HA-030W-B CPEs.

Figure 7   **HA-030W-B CPE physical connections**
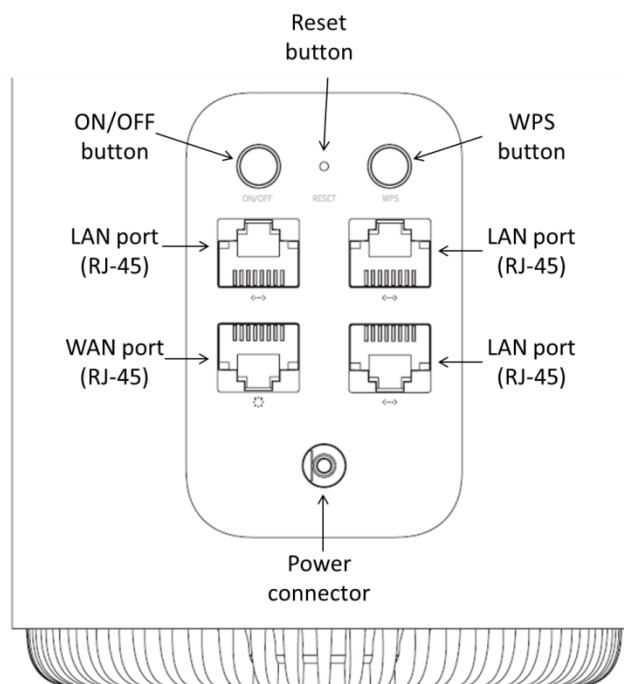
Table 5 describes the physical connections for HA-030W-B CPEs.

Table 5 **HA-030W-B CPE physical connections**

Connection [1]	Description
On/Off button	This button turns the unit on or off.
LAN 1/LAN 2/LAN 3	This connection is provided through Ethernet RJ-45 connectors. Up to three 10/100/1000 Base-T Ethernet interfaces are supported.The Ethernet ports can support both data and in-band video services on all three interfaces.
WAN port	This connection is provided through an RJ-45 Gigabit Ethernet interface.
WPS ON/Off button	This button is used to turn WPS on or off.
Reset button	Pressing the Reset button for less than 10 seconds reboots the device; pressing the Reset button for 10 seconds resets the device to the factory defaults, except for the LOID and SLID.
Power input	This connection is provided through the power connector. A power cable fitted with a barrel connector is used to make the connection.

Note

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

5.5 HA-030W-B CPE LEDs

The circular top of the HA-030W-B CPE functions as a multi-color LED indicator.
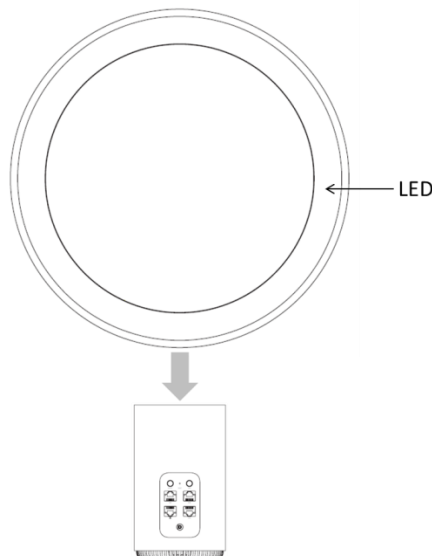
Table 6 provides LED descriptions for the HA-030W-B CPE.

Table 6 **HA-030W-B CPE LED indications**

LED color	LED behavior	LED behavior description

Off	Off	Power off
Red	Slow pulsing	No connection to Internet
	Solid	Bad backhaul connection, relocation needed
Yellow	Slow pulsing	Powered but nothing connected
	Solid	Connection is successful but not optimal. Relocation is recommended
Green	Slow pulsing	WPS mode enabled.
	3 quick pulses	WPS successful
	Solid	Good connection
White	Slow pulsing	Powering on
	Fast pulsing	Factory reset

5.6   HA-030W-B CPE detailed specifications

Table 7 lists the physical specifications for the HA-030W-B CPE.

Table 7   **HA-030W-B CPE physical specifications**

Description	Specification
Diameter	94 mm (3.7 in.)
Height	160 mm (6.3 in.)
Weight [within ± 0.5 lb (0.23 kg)]	650g (1.43 lb)

Table 8 lists the power consumption specifications for the HA-030W-B CPE.

Table 8   **HA-030W-B CPE power consumption specifications**

Maximum power (Not to exceed)	Condition	Minimum power	Condition
19.1 W	3 10/100/1000 Base-T Ethernet, Wi-Fi operational	2.9 W	interfaces/services not provisioned

Table 9 lists the environmental specifications for HA-030W-B CPE.

Table 9   **HA-030W-B CPE environmental specifications**

Mounting method	Temperature range and humidity	Altitude
On desk or shelf	Operating: -5°C to 45°C (23°F to 113°F) ambient temperature 5% to 93% relative humidity, non-condensing at 40°C Storage: -40°F to 158°F (-40°C to 70°C)	Contact your Nokia technical support representative for more information

5.7   HA-030W-B CPE functional blocks

HA-030W-B CPEs are single-residence units that support Wireless (Wi-Fi) service. Wi-Fi service on these devices is compliant with the IEEE 802.11 standard. In addition to the Wi-Fi service, these devices transmit Ethernet packets to three RJ-45 Ethernet ports.

Figure 8 shows the functional blocks for the HA-030W-B CPE.
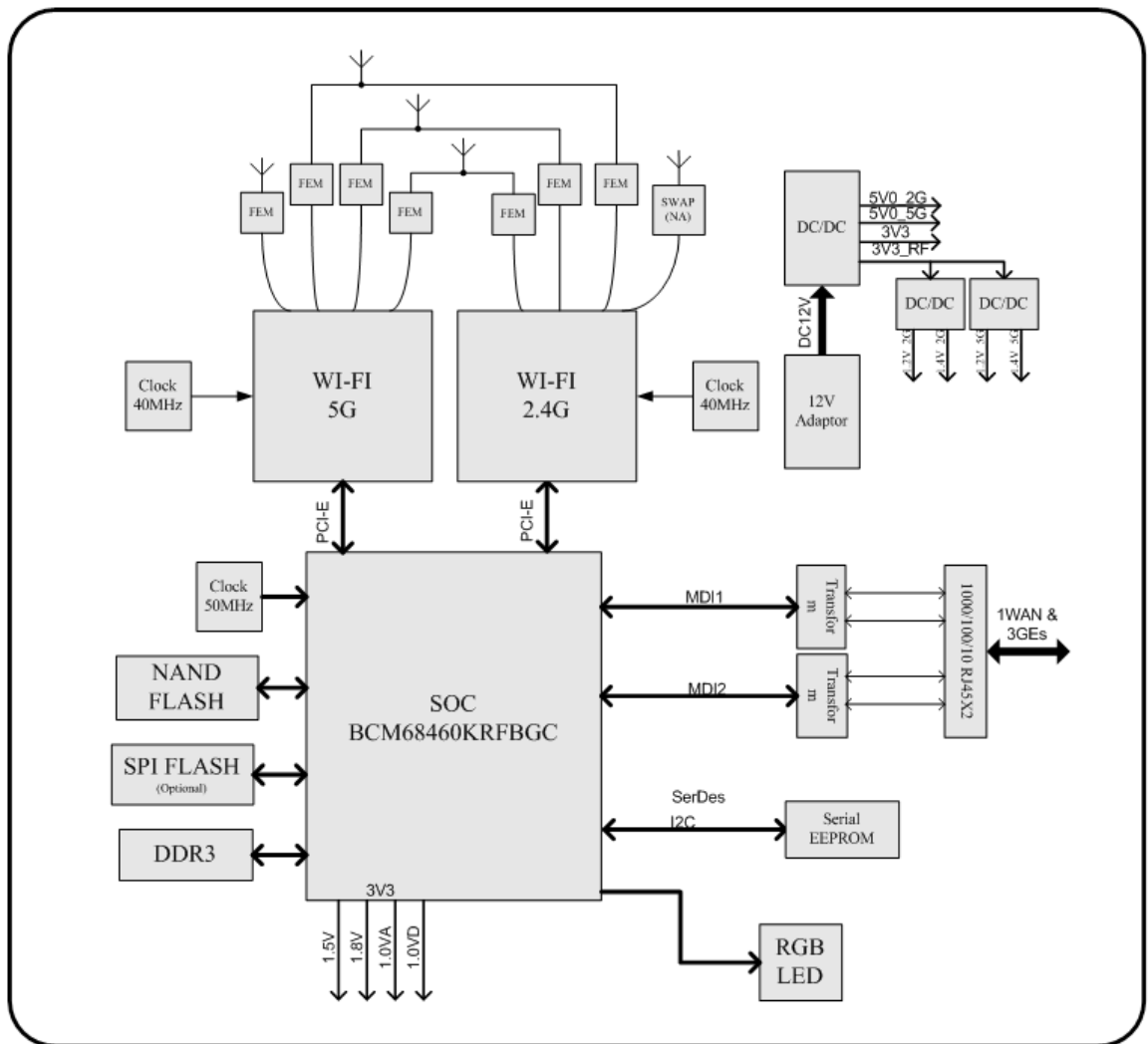
Figure 8   **Single-residence Wi-Fi CPE with Gigabit Ethernet**

```
TI028228 inserted here.
```

5.8   HA-030W-B CPE standards compliance

HA-030W-B CPEs are compliant with the following standards:

- IEEE 802.1D (QoS), 802.1p (bridging), 802.1q (VLAN)
- IEEE 802.3 (2012) (Ethernet standard)
- IEEE 802.11ac 4x4 (WiFi 5G) and 802.11b/g/n 3x3 (WiFi 2.4G)

Figure 9 shows the US safety label for the HA-030W-B CPE. (A-240Z-A labels shown)

Figure 9   **HA-030W-B CPE US safety label**

Figure 10 shows the European (EU) safety label for the HA-030W-B CPE.

Figure 10   **HA-030W-B CPE European (EU) safety label**

Figure 12 shows the location of the label.

Figure 12   **Label position on the HA-030W-B CPE**
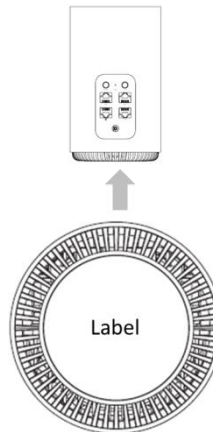
26030

5.8.1   Responsible party

Table 10 lists the party in the US responsible for this CPE.

Table 10   **Responsible party contact information**

Legal Company name	Nokia USA Inc.
Address	2301 SUGAR BUSH RD. STE 300, RALEIGH,NC 27612
Phone, Fax	+1 919 850 6000

5.8.2 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the HA-030W-B CPEs 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 HA-030W-B CPEs qualify as high network availability (HiNA) equipment. Since the main purpose of HA-030W-B devices is to provide network functionality with HiNA 7 days /24 hours, the modes Off/Standby, Power Management, and Networked Standby are inappropriate.

For information about the type and number of network ports, see "HA-030W-B CPE interfaces and interface capacity" in this chapter.

For information about power consumption, see "HA-030W-B CPE detailed specifications" in this chapter.

5.8.3 FCC statement

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

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

5.8.4 FCC Radiation Exposure Statement

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

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

1   this device may not cause harmful interference, and

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

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

5.8.5   Industry Canada license-exempt Radio Standards Specification (RSS) statement

This device complies with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions:

1   This device may not cause interference; and

2   This device must accept any interference, including interference that may cause undesired operation of the device.

- To satisfy IC RF exposure requirements, a separation distance of 20 cm or more should be maintained between the antenna of this device and persons during device operation. To ensure compliance, operations at closer than this distance is not recommended.
    - The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
    - For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
    - For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate.
    - Where applicable, antenna type(s), antenna models, and worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in section 6.2.2.3 shall be clearly indicated.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1   L'appareil ne doit pas produire de brouillage, et

2   L'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

• Les antennes installées doivent être situées de facon à ce que la population ne puisse y être exposée à une distance de moin de 20 cm. Installer les antennes de facon à ce que le personnel ne puisse approcher à 20 cm ou moins de la position centrale de l' antenne. La FCC des états-unis stipule que cet appareil doit être en tout temps éloigné d'au moins 20 cm des personnes pendant son functionnement.

  • Les dispositifs fonctionnant dans la bande de 5 150 à 5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

  • Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

  • Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas.

  • Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3), doivent être clairement indiqués.

5.9   HA-030W-B CPE special considerations

This section describes the special considerations for HA-030W-B CPEs.

5.9.1   Wi-Fi service

HA-030W-B CPEs feature Wi-Fi service as well as data services. Wi-Fi is a wireless networking technology that uses radio waves to provide wireless HSI and network connections. This device complies with the IEEE 802.11 standards, which the Wi-Fi Alliance defines as the basis for Wi-Fi technology.

5.9.1.1   Wi-Fi standards and certifications

The Wi-Fi service on HA-030W-B CPEs supports the following IEEE standards and Wi-Fi Alliance certifications:

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

5.9.1.2   Wi-Fi GUI features

HA-030W-B CPEs have HTML-based Wi-Fi configuration GUIs.

5.9.2   HA-030W-B CPE considerations and limitations

DFS channels are not supported in this release.

6 Install an HA-030W-B CPE

6.1   Purpose

This chapter provides the steps to install an HA-030W-B CPE.

6.2   General

The steps listed in this chapter describe mounting and cabling for an HA-030W-B CPE.

6.3   Prerequisites

You need the following items before beginning the installation:

* all required cables

6.4   Recommended tools

You need the following tools for the installation:

* #2 Phillips screwdriver
* 1/4 in. (6 mm) flat blade screwdriver
* wire strippers
* RJ-45 cable plug crimp tool
* voltmeter or multimeter
* drill and drill bits
* paper clip

6.5   Safety information

Read the following safety information before installing the unit.

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

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

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

Caution — Keep indoor CPEs 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 device should be installed in accordance with the applicable requirements of the NEC or CEC. Local authorities and practices take precedent when there is conflict between the local standard and the NEC or CEC.
- The device must be installed by qualified service personnel.
- Indoor units must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the HA-030W-B CPE unit data sheet for the temperature ranges for these devices.

6.6 Procedure

Use this procedure to install an HA-030W-B CPE.

---

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


Note — The HA-030W-B CPE cannot be stacked with another CPE or with other equipment. The installation requirements are:

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

---

2 Review the connection locations as shown in Figures 13.

Figure 13   **HA-030W-B CPE connections**

---
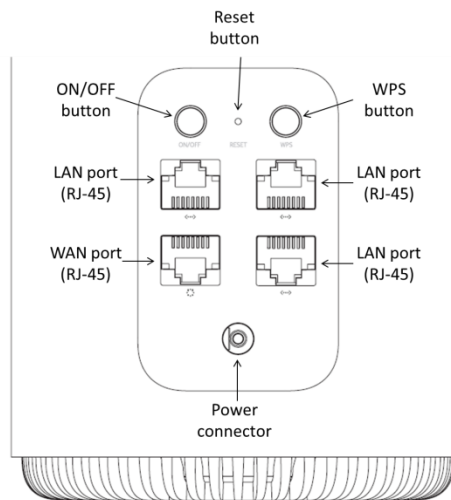
3 Connect the Ethernet cables to the RJ-45 ports; see Figure 13 for the location of the RJ-45 ports.

---

4 Connect the WAN cable to the RJ-45 WAN port; see Figure 13 for the location of the RJ-45 WAN port.

---

5 Connect the power cable to the power connector.

Note — Observe the following:

- Units must be powered by a Listed or CE approved and marked

limited power source power supply with a minimum output rate of
12 V dc, 2 A.

---

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

---

7   Verify the LEDs and voltage status; see the *7368 Hardware and Cabling Installation Guide*.

---

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

---

9   If necessary, reset the HA-030W-B CPE.

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

   i   Locate the Reset button as shown in Figure 13.

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

---

10   STOP. This procedure is complete.

7 Replace an HA-030W-B CPE

7.1 Purpose

This chapter provides the steps to replace an HA-030W-B CPE.

7.2 General

The steps listed in this chapter describe mounting and cabling for an HA-030W-B CPE.

7.3 Prerequisites

You need the following items before beginning the installation:

- all required cables

7.4 Recommended tools

You need the following tools for replacing the HA-030W-B CPE:

- #2 Phillips screwdriver
- 1/4 in. (6 mm) flat blade screwdriver
- wire strippers
- RJ-45 cable plug crimp tool
- voltmeter or multimeter
- drill and drill bits

7.5   Safety information

Read the following safety information before replacing the unit.

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

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

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

Caution — Keep indoor devices 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 device should be installed in accordance with the applicable requirements of the NEC or CEC. Local authorities and practices take precedent when there is conflict between the local standard and the NEC or CEC.
- The device must be installed by qualified service personnel.
- Indoor units must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the HA-030W-B CPE unit data sheet for the temperature ranges for these devices.

7.6   Procedure

Use this procedure to replace an HA-030W-B CPE.

---

1   Deactivate the services at the P-OLT.

    i   Use the RTRV-CPE command to verify the status and the associated services. Record the serial number of the HA-030W-B CPE displayed in the command output.

       Example:
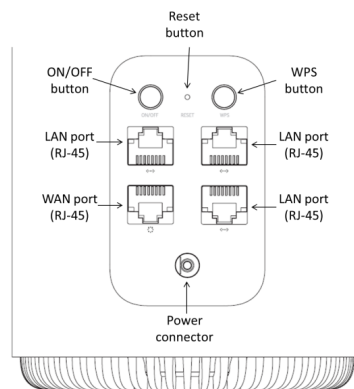
```
RTRV-CPE::CPE-1-1-1-1-1;
```

ii   If the unit is in service, place the HA-030W-B CPE in OOS state.

Example:

```
ED-CPE::CPE-1-1-1-1-1;
```

2   Power down the unit by using the on/off power switch. See Figure 14 for the connections on the HA-030W-B CPE.

Figure 14   **HA-030W-B CPE connections**

3   Disconnect the WAN, Ethernet, and power cables from the HA-030W-B CPE; see Figure 14 for the connector locations on the HA-030W-B CPE.

4   Replace the HA-030W-B CPE with the new CPE. The device can be placed on any flat surface, such as a desk or shelf.

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

6   Connect the WAN cable directly to the RJ-45 port; see Figure 14 for the location of the RJ-45 WAN port.

7   Connect the power cable to the power connector.

Note — Observe the following:

- Units must be powered by a Listed or CE approved and marked limited power source with a minimum output rate of 12 V dc, 2 A.

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

9   Verify the LEDs and voltage status; see the *7368 Hardware and Cabling Installation Guide*.

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

11   If necessary, reset the HA-030W-B CPE.

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

   i   Locate the Reset button on an HA-030W-B CPE 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 device.

12   STOP. This procedure is complete.

8　Configure an HA-030W-B CPE

8.1　General

Please refer to the configuration information provided with your OLT for the software configuration procedure for an HA-030W-B CPE.

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

8.2　GUI configuration

Use the procedures below to use the web-based GUI for the HA-030W-BCPE.

HA-030W-B is the premium Ethernet gateway and AP/range extender to connect devices in the home to the Internet. The GUI provides a variety of features for the home network including routing and firewall capability. By using the GUI, users can connect all smart equipment in their home, including personal computers, set-top boxes, mobile phones, and other consumer electronics devices, to the Internet.

8.2.1　Login

Use the procedure below to login to the web-based GUI for the HA-030W-BCPE.

Procedure 6　Login to web-based GUI

1　Open a web browser and enter the IP address of the HA-030W-B CPE in the address bar.

The login window appears.

The default gateway IP address is http://192.168.18.1. You can connect to this IP address using your web browser after connecting your PC to one of Ethernet ports of the HA-030W-B CPE. The static IP address of your PC must be in the same 192.168.18.x subnet as the HA-030W-B CPE.

2   Enter your username and password in the Log in window, as shown in Figure 15.

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

Figure 15   **Web login window**

Caution — 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.

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

3   Click Login. The Device Information screen appears.

Note — To help protect the security of your Internet connection, the application displays a pop-up reminder to change both the Wi-Fi password and the HA-030W-B CPE password.

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

4   STOP. This procedure is complete.

8.2.2 Device and connection status

The HA-030W-B CPE supports the retrieval of a variety of device and connection information, including:

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

Procedure 7   Device information retrieval

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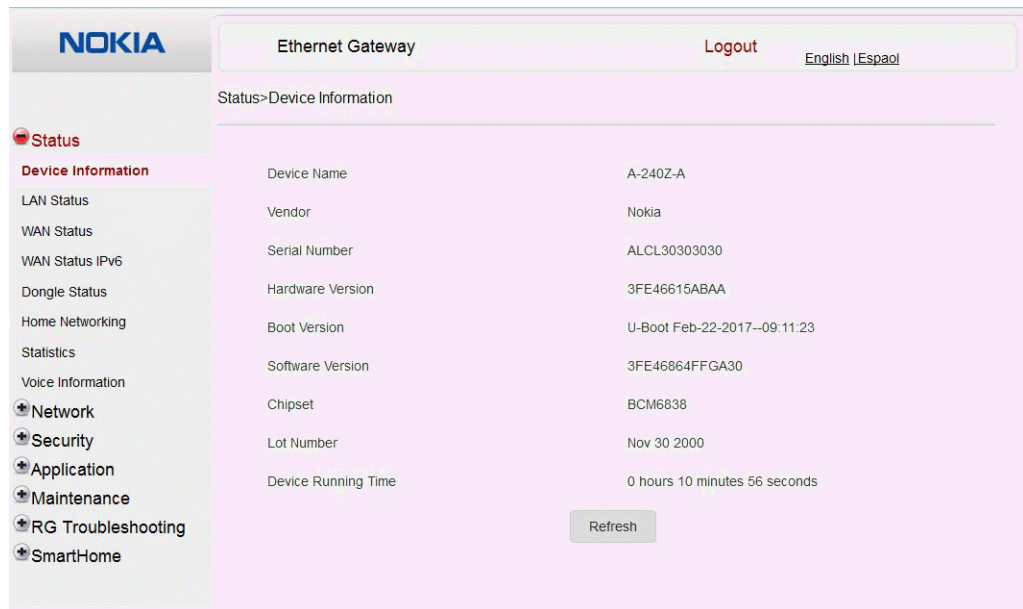
***Figure 16*   Device Information window**

Table 11 describes the fields in the Device Information window.

***Table 11*   Device Information parameters**

Field	Description
Device Name	Name on the HA-030W-B

(1 of 2)

Field	Description
Vendor	Name of the vendor
Serial Number	Serial number of the HA-030W-B
Hardware version	Hardware version of the HA-030W-B
Boot version	Boot version of the HA-030W-B
Software version	Software version of the HA-030W-B
Chipset	Chipset of the HA-030W-B
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 Ethernet Gateway window, as shown in Figure 17.

Figure 17   **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

(1 of 2)

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

(2 of 2)

---

2   Click Refresh to update the displayed information.

---

3   STOP. This procedure is complete.

Procedure 9   WAN status retrieval

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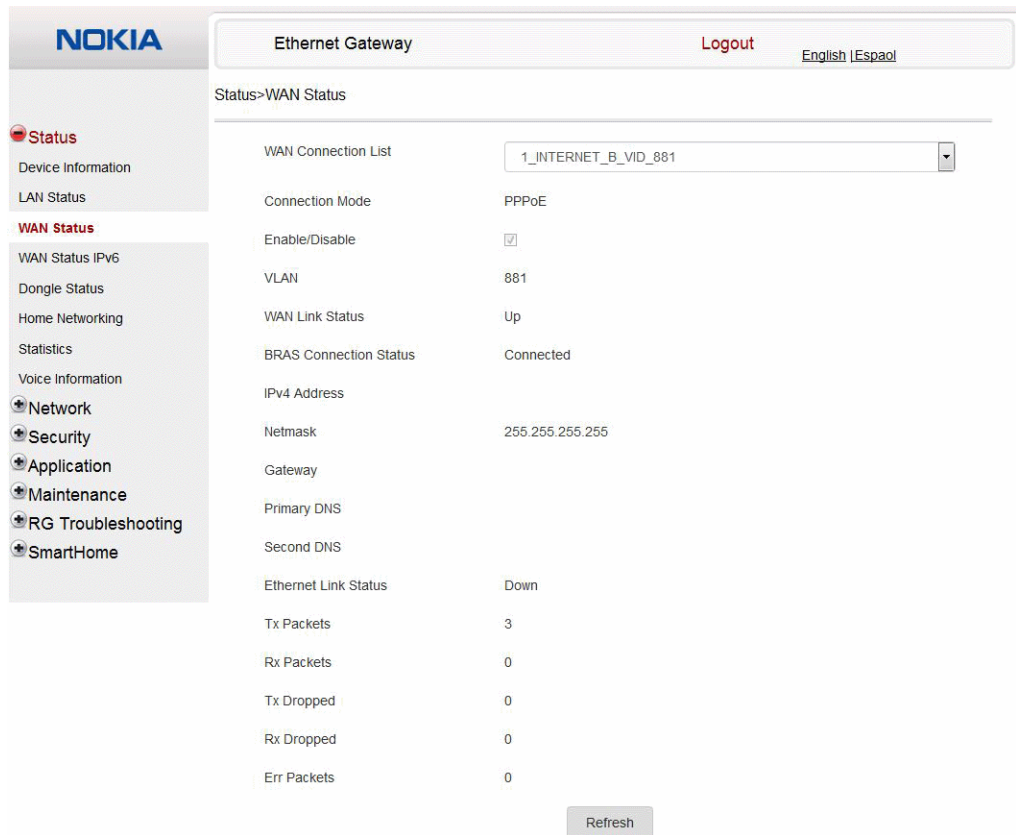
Figure 18   **WAN Status window**

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

(1 of 2)

Field	Description
WAN Link Status	Whether the WAN link is up or down
IPv4 Address	IPv4 address
Netmask	Netmask
Gateway	IPv4 gateway address
Primary DNS	Primary Domain Name Server
Second DNS	Secondary Domain Name Server
Ethernet Link Status	Whether the PON link is up or down
Tx Packets	Number of packets transmitted on the WAN connection
Rx Packets	Number of packets received on the WAN connection
Tx Dropped	Number of packets dropped on the transmit WAN connection
Rx Dropped	Number of packets dropped on the receive WAN connection
Err Packets	Number of errored packets on the WAN connection

(2 of 2)

2   Click Refresh to update the displayed information.

3   STOP. This procedure is complete.

Procedure 10 WAN status IPv6 retrieval

1 Select Status > WAN Status IPv6 from the top-level menu in the Ethernet Gateway window, as shown in Figure 19.
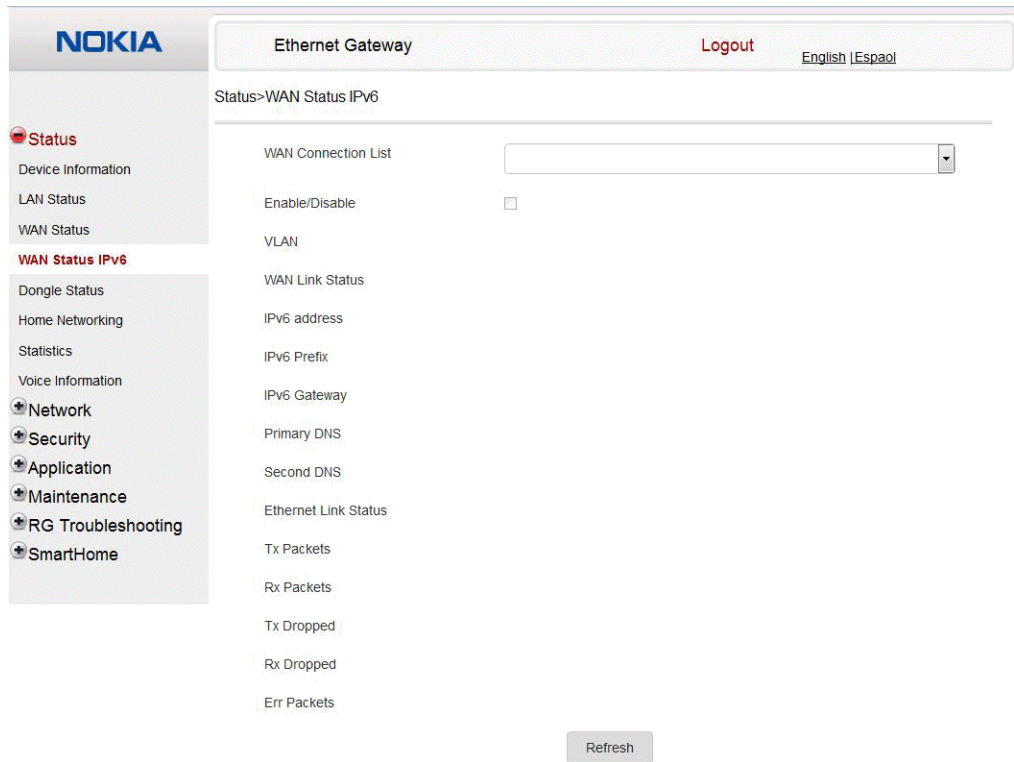
Figure 19 **WAN Status IPv6 window**

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 selected is the connection for which WAN status will be shown.
Enable/Disable	Select this check box to enable the WAN connection
VLAN	VLAN ID
WAN Link Status	Whether the WAN link is up or down
IPv6 Address	IPv6 address that identifies the device and its location
IPv6 Prefix	IPv6 prefix
IPv6 Gateway	IPv6 gateway address

(1 of 2)

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

(2 of 2)

2   Click Refresh to update the displayed information.

3   STOP. This procedure is complete.

Procedure 11   Home networking information retrieval

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

Figure 20   **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	
Network Name	Name of the wireless network access point

(1 of 2)

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

(2 of 2)

---

2   Click Delete to delete a particular local device connection.

---

3   Click Refresh to update the displayed information.

---

4   STOP. This procedure is complete.

Procedure 12   Statistics retrieval

---

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

Statistics are available for LAN ports and WAN ports.

Figure 21 shows the statistics for the LAN ports.

***Figure 21*   LAN ports statistics window**

2   Click Refresh to update the displayed information.

3   STOP. This procedure is complete.

8.2.3   Network configuration

HA-030W-B CPE also supports network configuration, including:

- LAN
- LAN IPv6
- WAN
- WAN DHCP
- Wireless 2.4G
- Wireless 5G
- wireless schedule
- routing
- DNS
- TR-069
- QoS Configuration

Procedure 13   LAN configuration

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

Figure 22   **LAN settings window**

Table 16 describes the fields in the LAN window.

Table 16   **LAN parameters**

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

(1 of 2)

Field	Description
Primary DNS	Primary domain name server address
Secondary DNS	Secondary domain name server address
Static DHCP MAC Address	Hexadecimal MAC address to associate to the LAN
Static DHCP IP Address	IP address to associate to the bound MAC address

(2 of 2)

2   Configure the LAN.

3   Click Save.

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

5   STOP. This procedure is complete.

Procedure 14   LAN IPv6 networking configuration

1   Select Network > LAN_IPv6 from the top-level menu in the Ethernet Gateway window, as shown in Figure 23.

Figure 23   **LAN IPv6 network window**

Table 17 describes the fields in the LAN IPv6 network window.

Table 17   **LAN IPv6 network parameters**

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

(1 of 2)

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

(2 of 2)

---

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

---

3   Enter the DHCP configuration information.

---

4   Enter the maximum and minimum intervals for RA messages.

---

5   Click Save/Apply.

---

6   STOP. This procedure is complete.

Procedure 15   WAN networking configuration

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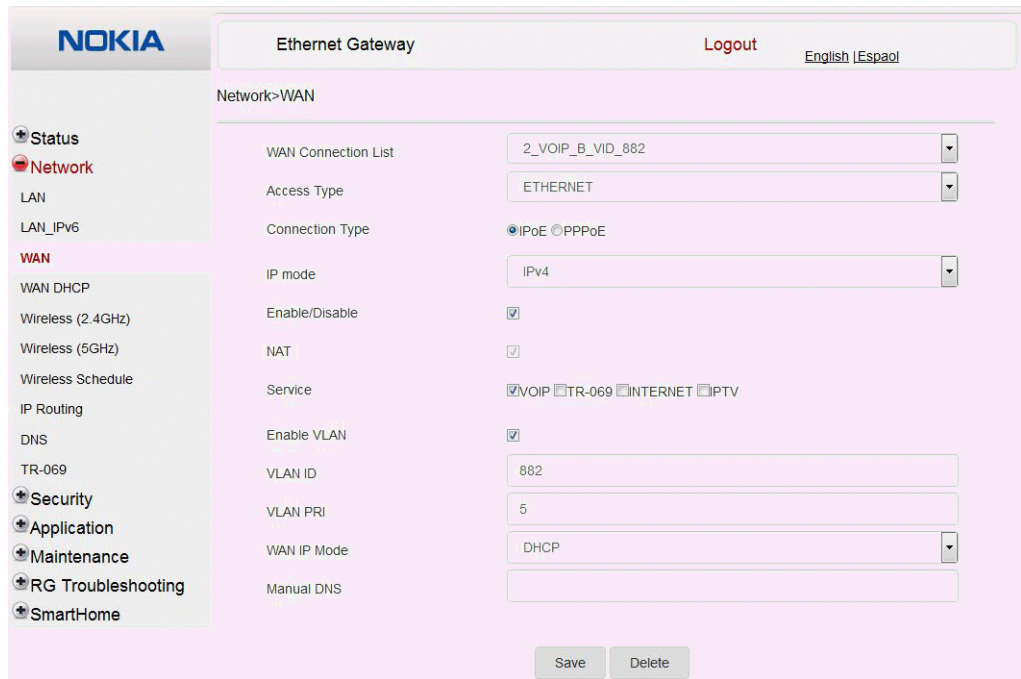
Figure 24   **WAN window**

Table 18 describes the fields in the WAN window.

Table 18   **WAN parameters**

Field	Description
WAN Connection List	Choose a WAN connection from the drop-down menu to set the connection parameters
Connection Type	Select a connection type: IPoE or PPPoE
IP Mode	Choose an IP mode from the drop-down menu: IPv4 or IPv6
Enable/Disable	Select this checkbox to enable the WAN connection
NAT	Select this checkbox to enable NAT
Service	Select the checkboxes to enable service types for this connection
Enable VLAN	Select this checkbox to enable VLAN
VLAN ID	Enter the VLAN ID
VLAN PRI	Enter the VLAN PRI

(1 of 2)

Field	Description
WAN IP Mode	Choose an IP mode from the drop-down menu
Manual DNS	Enter a DNS

(2 of 2)

2   Configure a specific WAN connection.

3   Click Save.

4   STOP. This procedure is complete.

Procedure 16   WAN DHCP configuration

1   Select Network > WAN DHCP from the top-level menu in the Ethernet Gateway window, as shown in Figure 25.
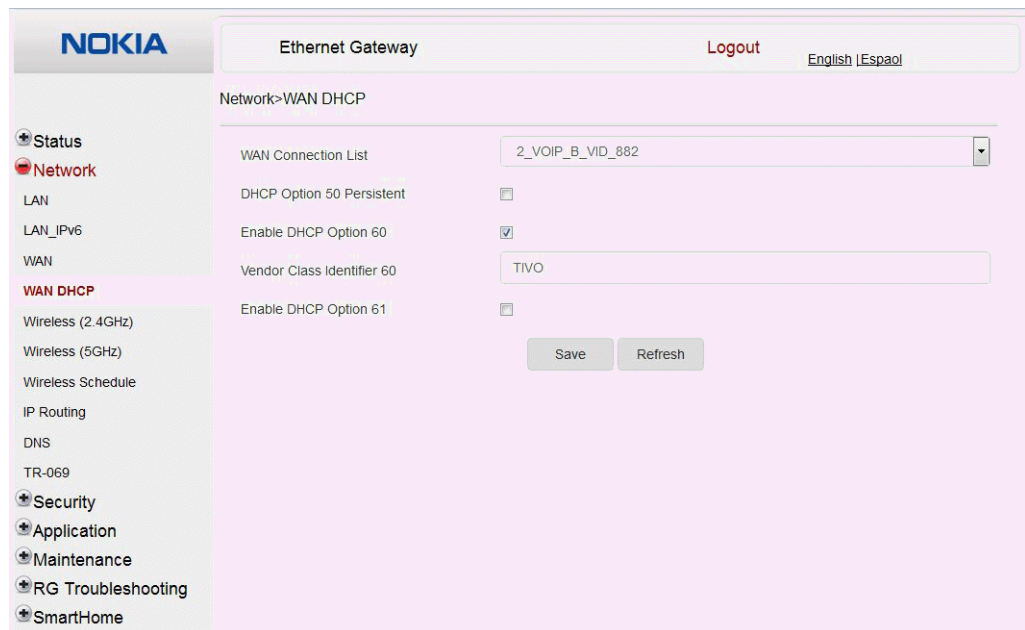
Figure 25   **WAN DHCP window**

Table 19 describes the fields in the WAN DHCP window.

Table 19   **WAN DHCP parameters**

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

2   Configure a WAN DHCP option.

3   Click Save.

4   STOP. This procedure is complete.

Procedure 17   Wireless 2.4G networking configuration

1   Select Network > Wireless 2.4GHz from the top-level menu in the Ethernet Gateway window, as shown in Figure 26.
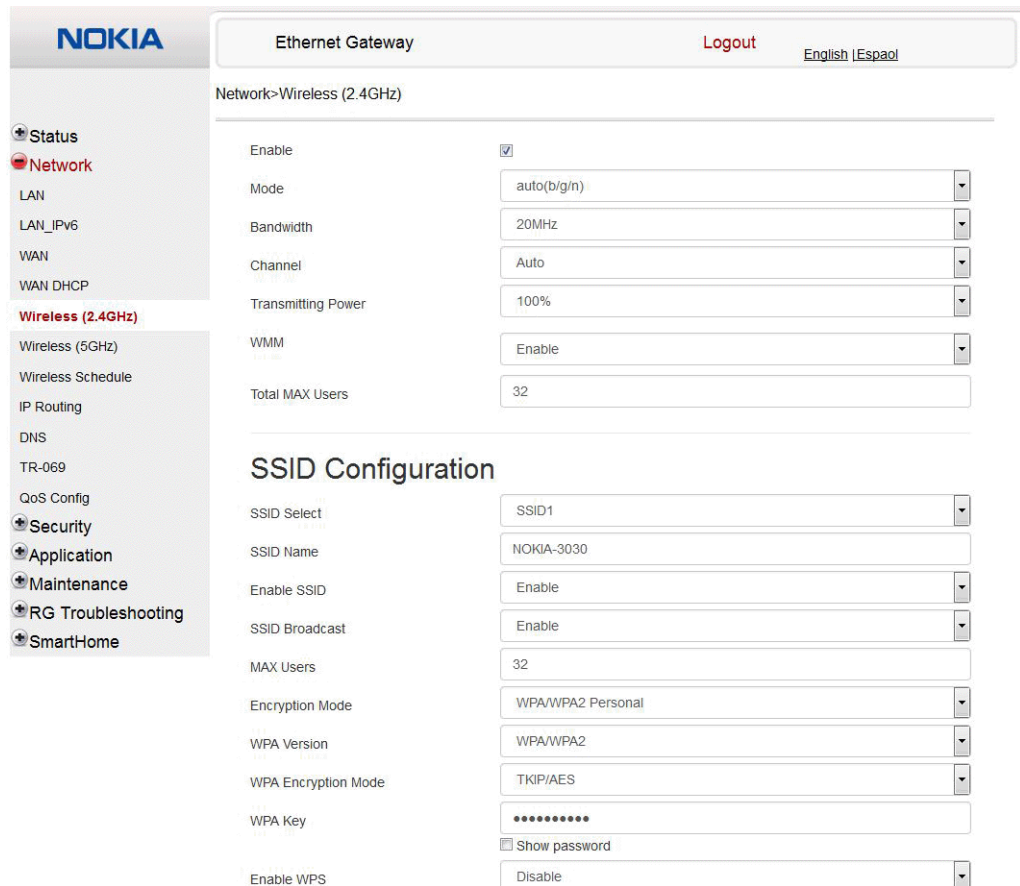
Figure 26   **Wireless 2.4GHz network window**

Table 20 describes the fields in the Wireless 2.4GHz network window.

Table 20   **Wireless 2.4GHz network parameters**

Field	Description
Enable	Select this check box to enable WiFi

(1 of 2)

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

(2 of 2)

---

2   Configure the WiFi connection.

---

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

4   Click Save.

5   STOP. This procedure is complete.

Procedure 18   Wireless 5G networking configuration

1   Select Network > Wireless 5GHz from the top-level menu in the Ethernet Gateway window, as shown in Figure 27.

Figure 27   **Wireless 5GHz network window**

Table 21 describes the fields in the Wireless 5GHz network window.

Table 21   **Wireless 5GHz network parameters**

Field	Description
Enable	Select this check box to enable WiFi
Bandwidth	Choose from: • 20 MHz • 40 MHz • 80 MHz
Channel	Choose a channel from the drop-down menu or choose Auto to have the channel automatically assigned
Transmitting Power	Choose a percentage for the transmitting power from the drop-down menu: • Low (20%) • Medium (40%) • High (60%) • Maximum (100%)
WMM	Select this check box to enable or disable wireless multi media
Enable MU-MIMO	Choose Enable or disable MU-MIMO from this drop-down menu The default is Enable, which enables users and wireless terminals to communicate with each other. MU-MIMO may decrease 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	Select this check box to enable or disable DFS re-entry
SSID Select	Choose the SSID from the drop-down menu
SSID Name	Change the name of the selected SSID
Enable SSID	Choose Enable or disable SSID from this drop-down menu
SSID Broadcast	Choose Enable or disable SSID broadcast from this drop-down menu
MAX Users	Enter the number of MAX users
Encryption Mode	Choose an encryption mode from the drop-down menu: • OPEN • WEP • WPA/WPA2 Personal • WPA/WPA2 Enterprise [1][2]
WPA Key	Enter the WPA key
Enable WPS	Choose Enable or disable WPS from this drop-down menu

Notes

[1] When Encryption Mode is set to "WPA/WPA2 Enterprise", the following options are no longer available: WPA version, WPA encryption mode, WPA key, Enable WPS, WPS mode.

[2] When Encryption Mode is set to "WPA/WPA2 Enterprise", the following options become available: Primary RADIUS server, port and password; Secondary RADIUS server, port, and password; RADIUS accounting port.
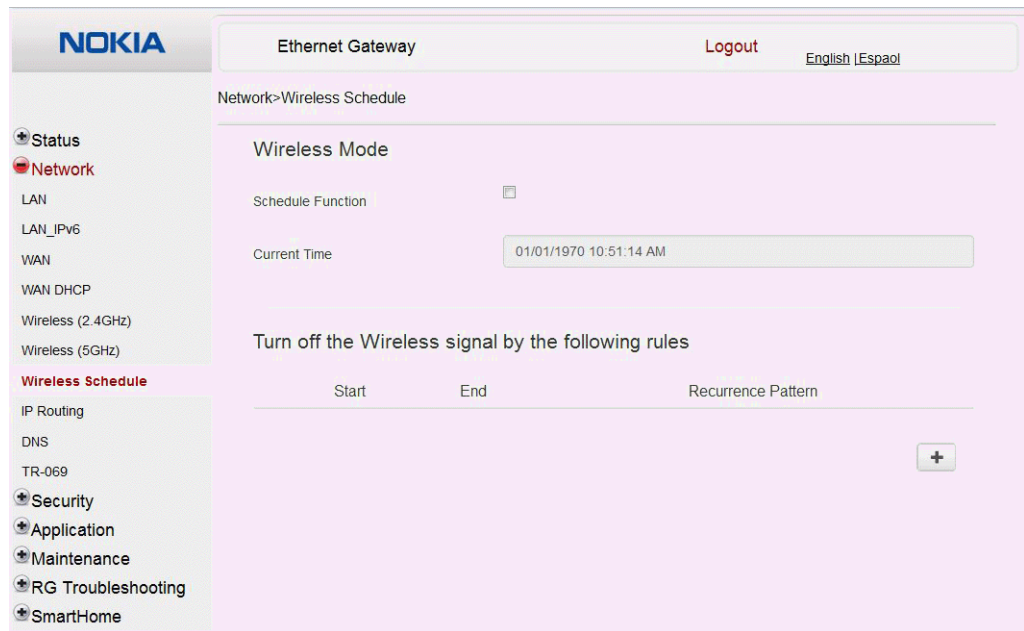
2   Configure the Wireless connection.

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

4 Click Save.

5 STOP. This procedure is complete.

Procedure 19   Wireless scheduling

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

Figure 28   **Wireless Schedule window**

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

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

A separate panel appears for configuring wireless schedule rules.

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

5	Choose Everyday or Individual Days from the drop-down menu.
6	If you chose Individual Days, select the check boxes for the desired days. The Recurrence Pattern shows the rules created to date.
7	If desired, click the plus sign (+) to add more rules.
8	Click Save Changes.
9	STOP. This procedure is complete.

Procedure 20   DNS configuration

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

Figure 29   **DNS network window**

Table 22 describes the fields in the DNS network window.

Table 22   **DNS network parameters**

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

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

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

4   STOP. This procedure is complete.

Procedure 21   TR-069 configuration

1   Select Network > TR-069 from the top-level menu in the Ethernet Gateway window, as shown in Figure 30.

Figure 30   **TR-069 network window**

Table 23 describes the fields in the TR-069 network window.

Table 23   **TR-069 network parameters**

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

2   Configure TR-069 by entering the required information.

3   Click Save.

4   STOP. This procedure is complete.

Procedure 22   QoS configuration

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

Figure 31 shows the window for configuring QoS L2 (Layer 2 packet sizes).

Figure 31   **QoS Config window (L2)**

Figure 32 shows the window for configuring QoS L3 (Layer 3 packet sizes).

Figure 32   **QoS Config window (L3)**

Table 24 describes the fields in the QoS Config window.

Table 24   **QoS Config parameters**

Field	Description
Type	Choose a QoS service layer type from the drop-down menu, either L2 or L3.
Source MAC	Enter the source MAC. Select the Exclude check box to exclude the source MAC
Interface	Choose an interface from the drop-down menu
DSCP Remark	Enter the value for the DSCP mark (range: 0-63); valid only for L3 Criteria
802.1p Mark	Enter the value for the 802.1p (range: 0-7)
Forwarding Policy	Enter the number for the forwarding policy (range: 1-7)
Additional fields for L3	
Protocol	Choose a protocol from the drop-down menu, or select the Exclude check box
Application	Choose an application from the drop-down menu
Source IP and Source IP Mask	Enter the values for the source IP and IP mask, or select the Exclude check box
Destination IP and Destination IP Mask	Enter the values for the destination IP and IP mask, or select the Exclude check box
Source Port and Source Port Max	Enter the values for the source port and port max (highest port number) or select the Exclude check box
Destination Port and Destination Port Max	Enter the values for the destination port and port max (highest port number), or select the Exclude check box

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

3   Configure a QoS policy.

4   Click Add to add a QoS policy.

5   STOP. This procedure is complete.

8.2.4   Security configuration

HA-030W-B CPE also supports security configuration, including:

- firewall
- MAC filter

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

Procedure 23   Firewall configuration

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

Figure 33   **Firewall window**
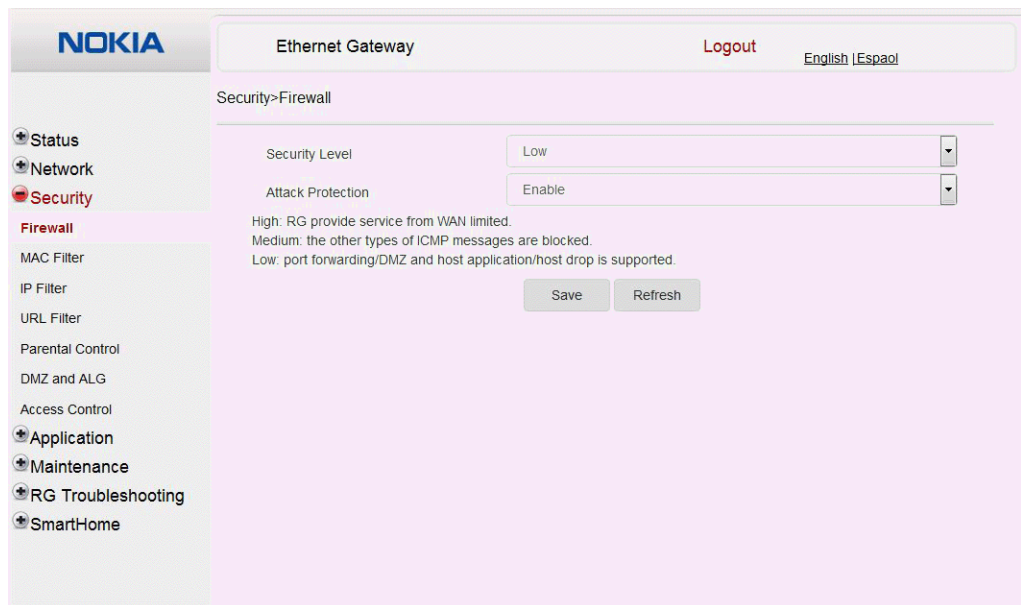
Firewall security applies only to services provided by the HA-030W-B CPE. Internet access from the LAN side is not affected by this firewall.

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

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

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

At the High level, pre-routing and application services are not supported. UDP Port 8000 can be used to access the services, for example FTP can use 8021 and Telnet can use 8023. Regular UDP cannot be used. RG access is permitted via the LAN side but not via the WAN side.

Table 25 describes the fields in the firewall window.

Table 25   **Firewall parameters**

Field	Description
Security level	Choose the security level from the drop-down menu: Off, Low, or High
Attack Protect (Protection against DoS or DDoS attacks)	Choose enable or disable attack protect from the drop-down menu The default is disable

2   Configure the firewall.

3   Click Save.

4   STOP. This procedure is complete.

Procedure 24   MAC filter configuration

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

Figure 34   **MAC filter window**
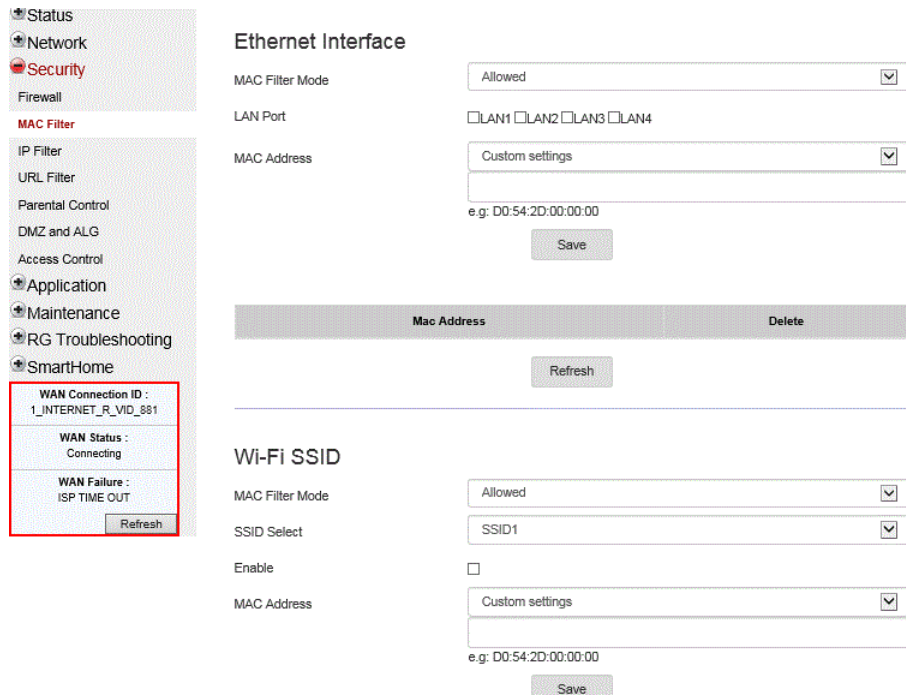
Table 26 describes the fields in the MAC filter window.

Table 26   **MAC filter parameters**

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

2	Configure a MAC filter for the Ethernet interface.
3	Click Save.
4	If desired, select a MAC address and click the Delete column to delete a MAC address.
5	Click Refresh to update the information.
6	Configure a MAC filter for WiFi SSID (WLAN MAC filter).
7	Click Save.
8	STOP. This procedure is complete.

Procedure 25   IP filter configuration

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

*Figure 35*   **IP filter window**

Table 27 describes the fields in the IP filter window.

Table 27   **IP filter parameters**

Field	Description
Enable IP Filter	Select this check box to enable an IP filter
Mode	Choose an IP filter mode from the drop-down menu: • Drop for upstream • Drop for downstream
Internal Client	Choose an internal client from the drop-down menu: • Customer setting - uses the IP address input below • IP - uses the connecting devices' IP to the CPE
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 26   URL filter configuration

1   Select Security > URL Filter from the top-level menu in the Ethernet Gateway window, as shown in Figure 36.
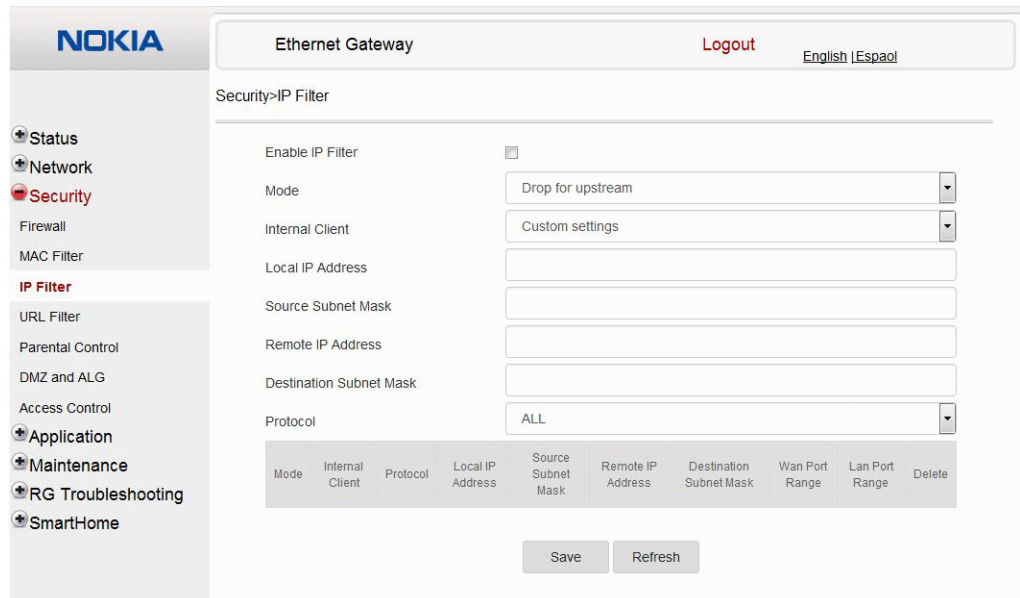
Figure 36   **URL Filter window**
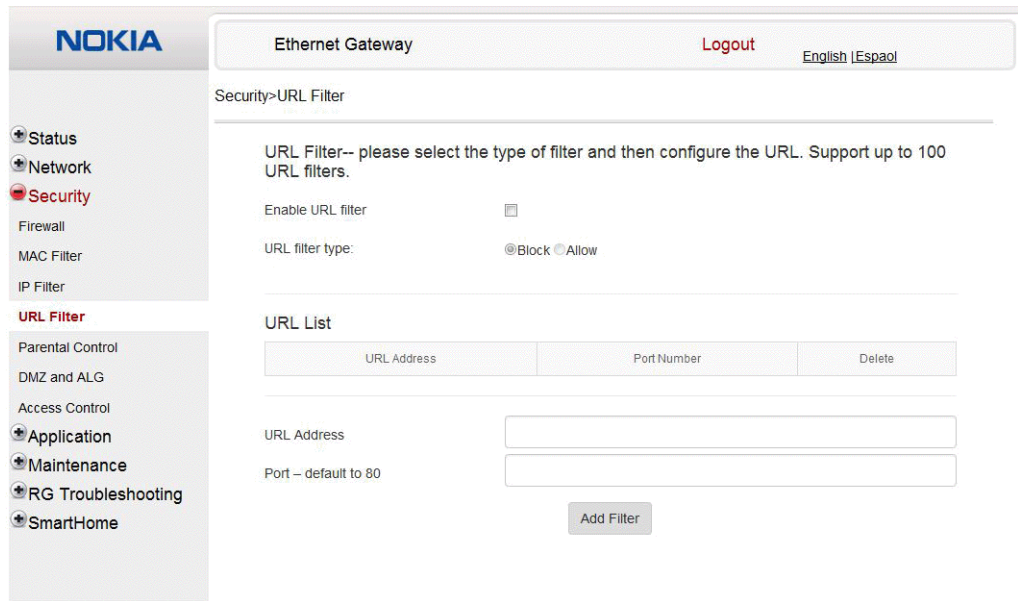
Table 28 describes the fields in the URL Filter window.

Table 28   **URL Filter parameters**

Field	Description
Enable URL filter	Select the check box to enable the URL filter
URL filter type	Select the radio button for Exclude URL or Include URL
URL Address	Enter the URL address
Port	Enter the port number; the default is 80

2   Configure the URL Filter.

3   Click Add Filter.

4   STOP. This procedure is complete.

Procedure 27   Parental control

1   Select Security > Parent Control from the top-level menu in the Ethernet Gateway window, as shown in Figure 37.
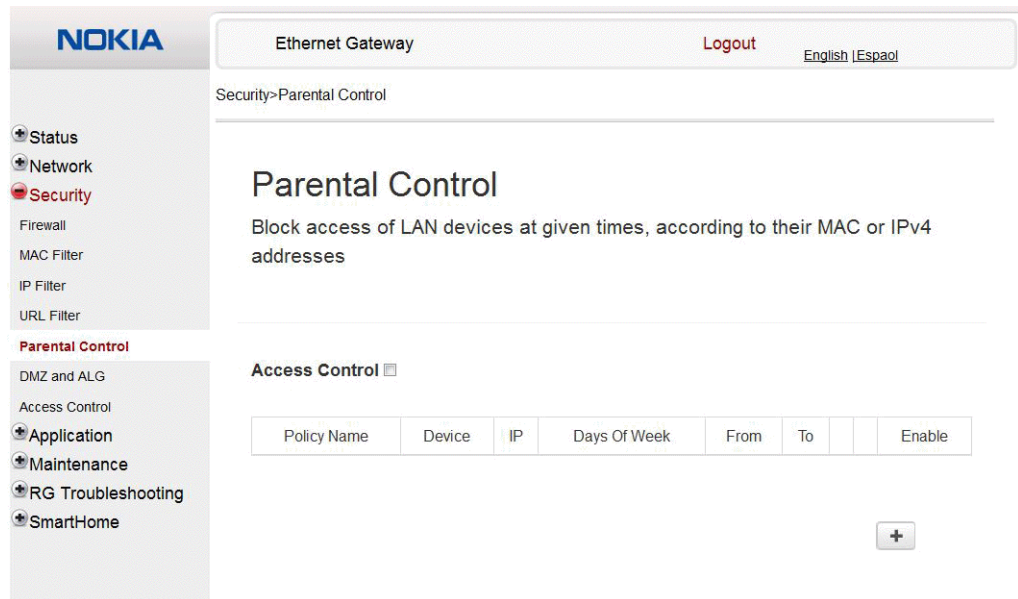
Figure 37   **Parental Control window**

Table 29 describes the fields in the Parental Control window.

Table 29   **Parental control parameters**

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

2   Select the Access Control check box.

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

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

---

4   Configure the parental control policy.

---

5   Click Enable to activate the policy.

---

6   STOP. This procedure is complete.

Procedure 28   DMZ and ALG configuration

---

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

Figure 38   **DMZ and ALG window**
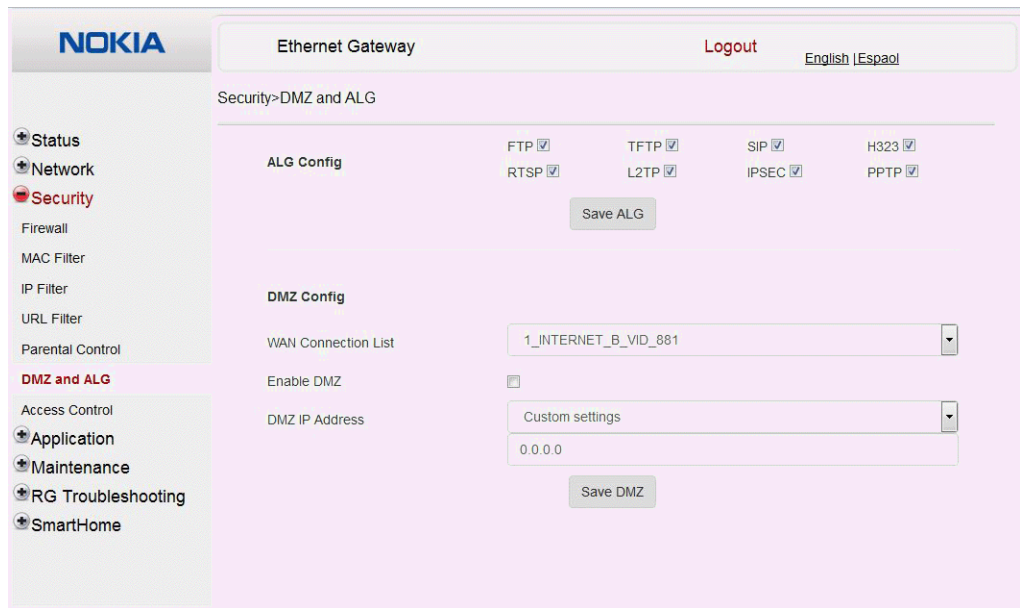
Table 30 describes the fields in the DMZ and ALG window.

Table 30   **DMZ and ALG parameters**

Field	Description
ALG Config	Select the check boxes to enable the protocols to be supported by the ALG: FTP, TFTP, SIP, H323, RTSP, L2TP, IPSEC, PPTP
DMZ Config	

(1 of 2)

Field	Description
WAN Connection List	Choose a WAN connection from the drop-down menu
Enable DMZ	Select this check box to enable DMZ on the chosen WAN connection
DMZ IP Address	Choose Customer Setting and enter the DMZ IP address or choose the IP address of a connected device from the drop-down menu

(2 of 2)

---

2   Configure ALG.

---

3   Click Save ALG.

---

4   Configure DMZ.

---

5   Click Save DMZ.

---

6   STOP. This procedure is complete.

Procedure 29   Access control configuration

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

Note 1 — ACL takes precedence over the firewall policy.

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

1   Select Security > Access Control from the top-level menu in the Ethernet Gateway window, as shown in Figure 39.

Figure 39   **Access Control window**

Table 31 describes the fields in the Access Control window.

Table 31   **Access control parameters**

Field	Description
WAN	Choose a connection from the drop-down menu
Trusted Network Enable	Click to enable or disable

(1 of 2)

Field	Description
ICMP, Telnet, SSH, HTTP, TR-069, HTTPS	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 of 2)

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

3   Click to enable or disable Trusted Network.

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

5   Click Save.

6   Optionally, add one or more subnet trusted networks.

The maximum number of entries is 32.

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

7   STOP. This procedure is complete.

8.2.5   Application configuration

The HA-030W-B CPE also supports application configuration, including:

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

Procedure 30   Port forwarding configuration

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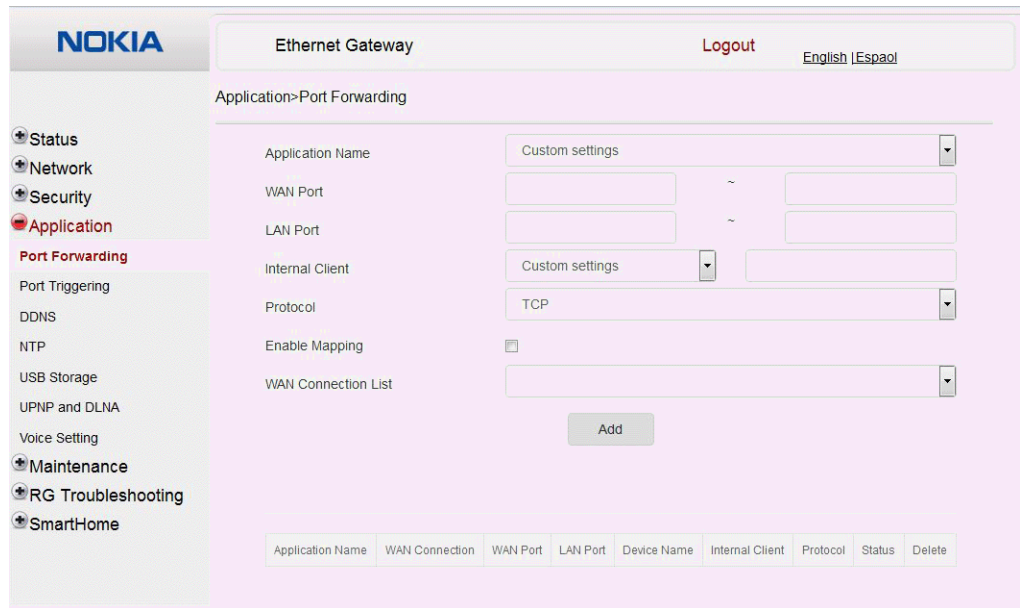
Figure 40   **Port forwarding window**

Table 32 describes the fields in the port forwarding window.

Table 32   **Port forwarding parameters**

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

2   Configure port forwarding.

3   Click Add.

4   STOP. This procedure is complete.

Procedure 31   Port triggering

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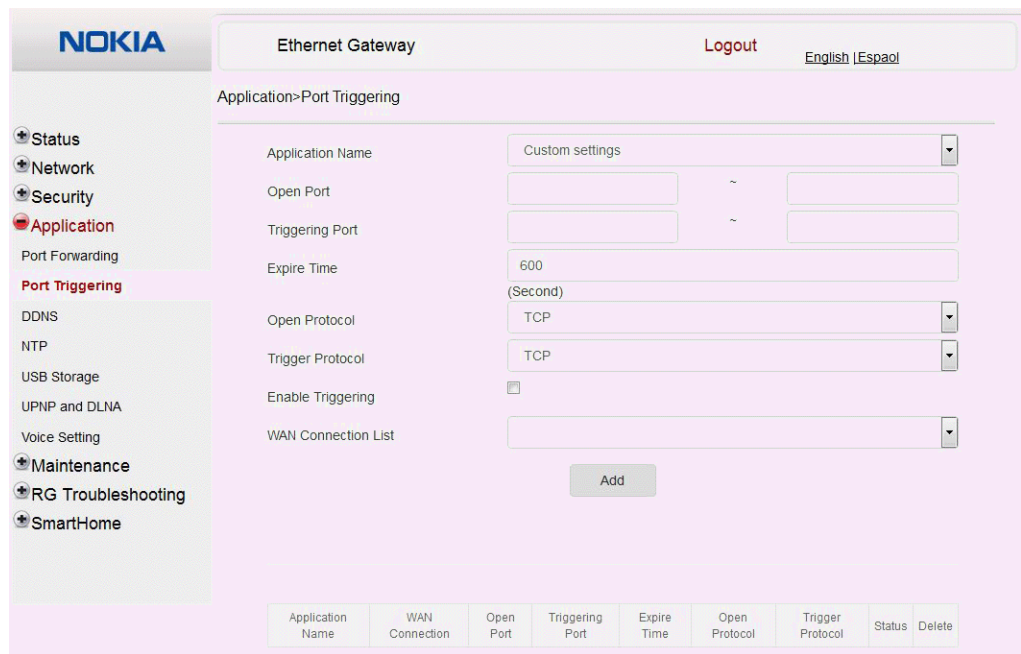
Figure 41   **Port Triggering window**

Table 32 describes the fields in the Port Triggering window.

Table 33   **Port triggering parameters**

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

(1 of 2)

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

(2 of 2)

---

2 Configure port triggering.

---

3 Click Add.

---

4 STOP. This procedure is complete.

Procedure 32   DDNS configuration

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

Figure 42   **DDNS window**

Table 34 describes the fields in the DDNS window.

Table 34   **DDNS parameters**

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

2   Configure DDNS.

3　　Click Save.

4　　STOP. This procedure is complete.

Procedure 33　　NTP configuration

1　　Select Application > NTP from the top-level menu in the Ethernet Gateway window, as shown in Figure 43.
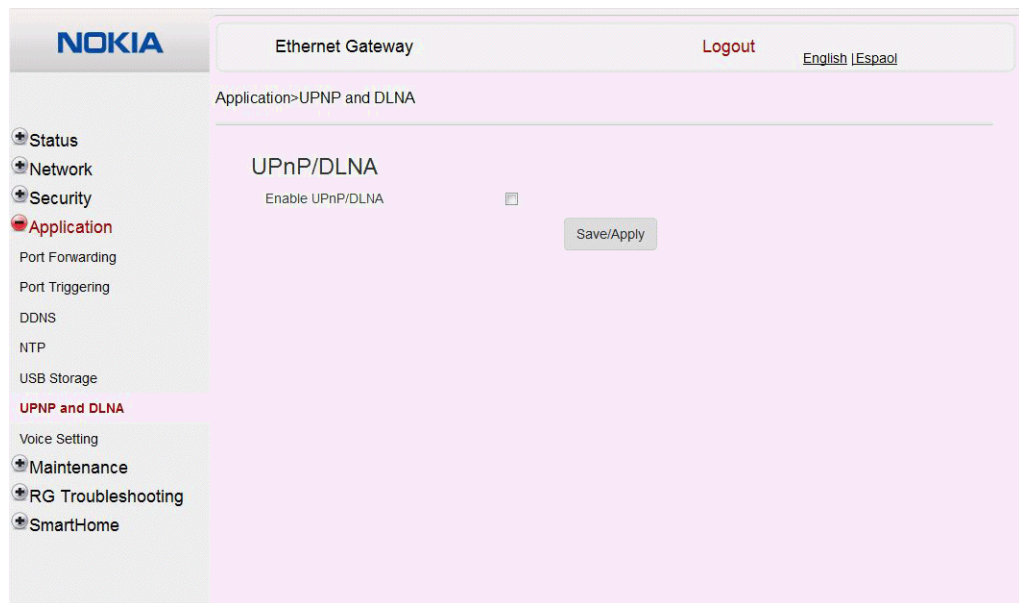
Figure 43　　**NTP window**
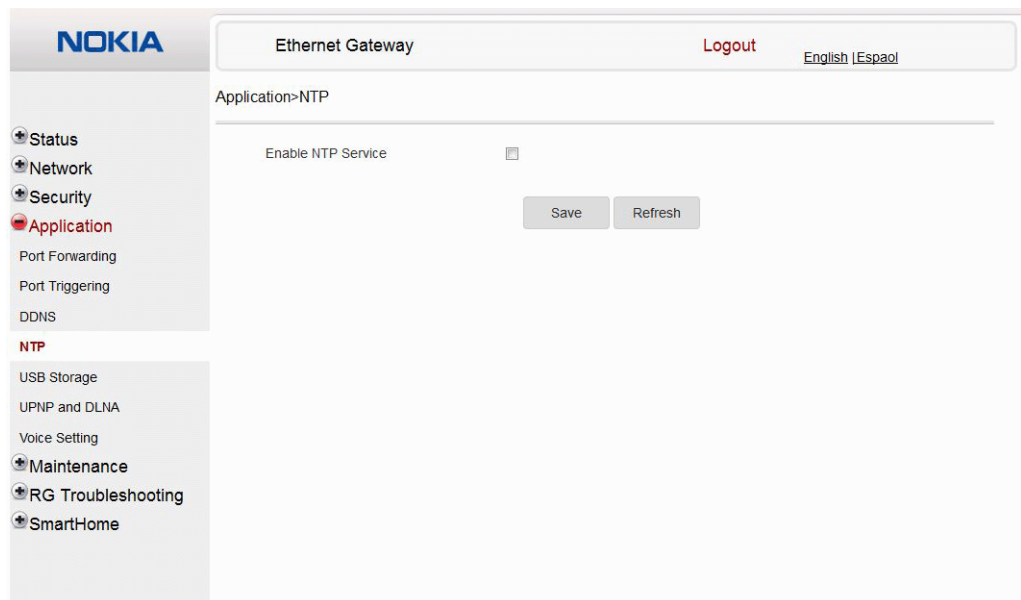
2　　Select the Enable NTP Service check box.

3　　Click Save.

4　　STOP. This procedure is complete.

Procedure 34   UPnP and DLNA configuration

1   Select Application > UPnP and DLNA from the top-level menu in the Ethernet Gateway window, as shown in Figure 44.

Figure 44   **UPnP and DLNA window**

2   Select the Enable UPnP check box to enable UPnP.

3   Click Save/Apply.

4   STOP. This procedure is complete.

8.2.6   Maintenance

The HA-030W-B CPE supports maintenance tasks, including:

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

- restore factory defaults
- diagnostics
- log

Procedure 35   Password configuration

A password must adhere to the following password rules:

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

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

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

- the password is too short
- the password is too long

- the first character cannot be a special character
- there are not enough character classes

---

1   Select Maintenance > Password from the top-level menu in the GPON Home Gateway
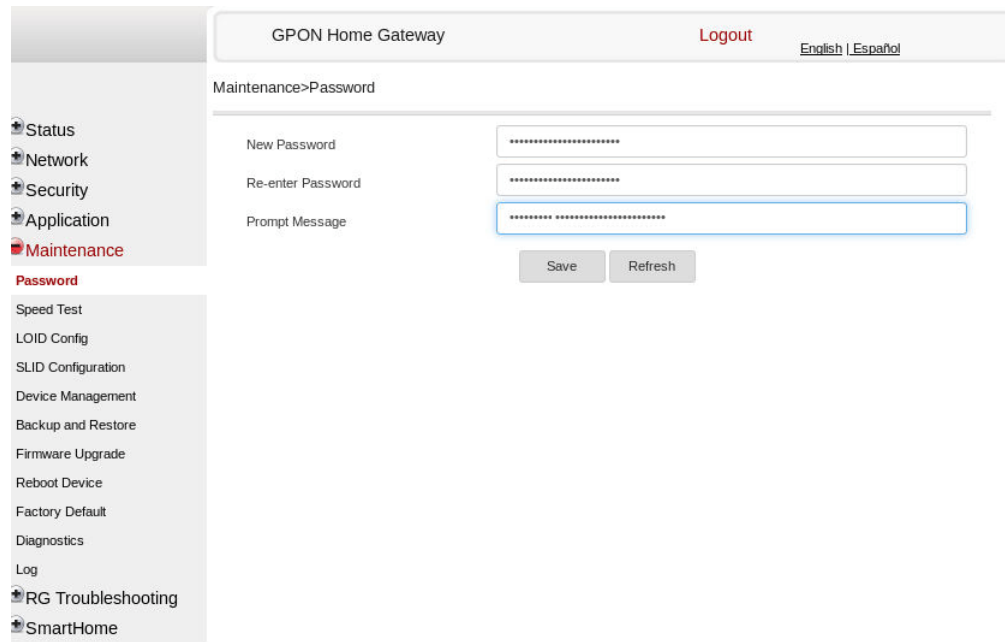window, as shown in Figure 45.

Figure 45   **Password window**

Table 35 describes the fields in the password window.

Table 35   **Password parameters**

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

---

2   Configure the new password.

3   Click Save.

4   STOP. This procedure is complete.

Procedure 36   Device management

1   Select Maintenance > Device Management from the top-level menu in the Ethernet Gateway window, as shown in Figure 46.
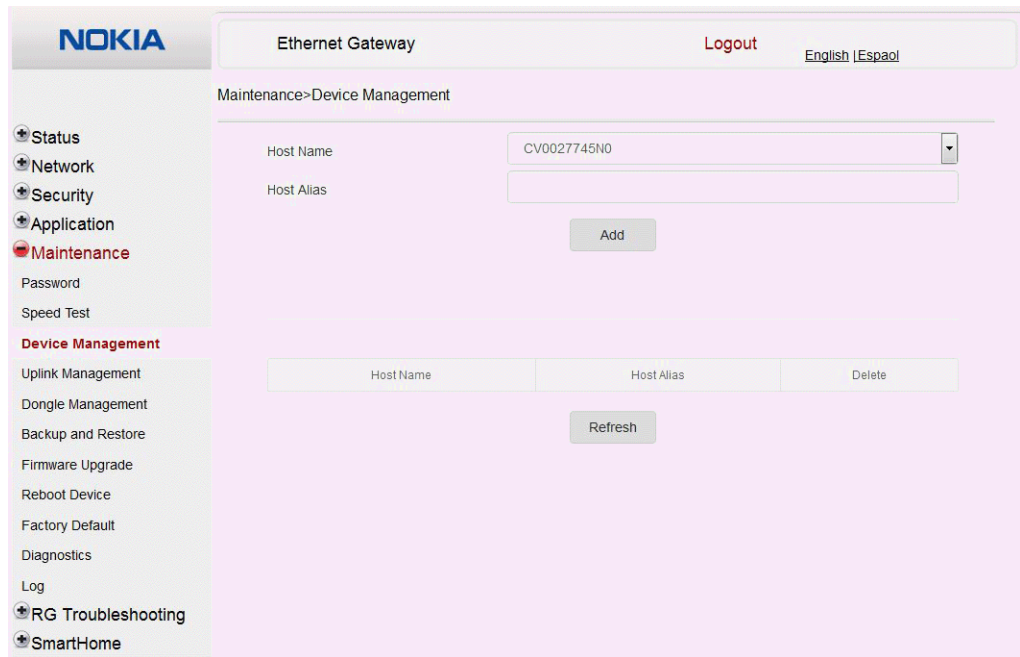
Figure 46   **Device Management window**

Table 36 describes the fields in the Device Management window.

Table 36   **Device Management parameters**

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

2   Configure an alias for a specific host.

3   Click Add.

4   STOP. This procedure is complete.

Procedure 37   Backup and Restore

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

Figure 47   **Backup and Restore window**
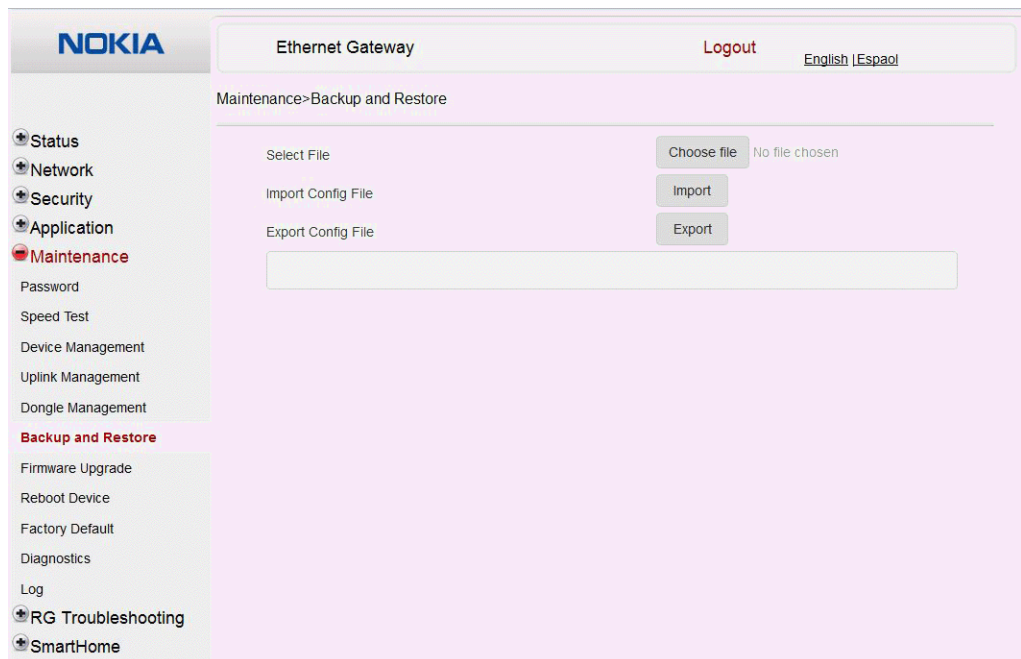
2   Click Select File and choose the backup file.

3   Click Import Config File to restore the HA-030W-B CPE to the saved backup or click Export Config File to export the current configuration to the backup file.

4   STOP. This procedure is complete.

Procedure 38   Upgrade firmware

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

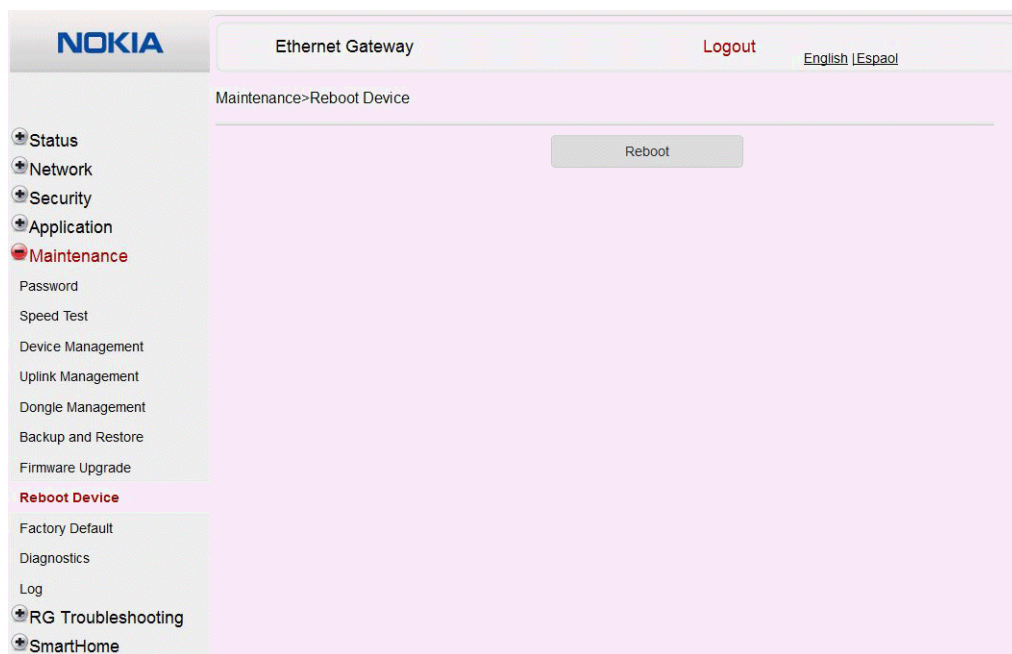*Figure 48*   **Firmware Upgrade window**
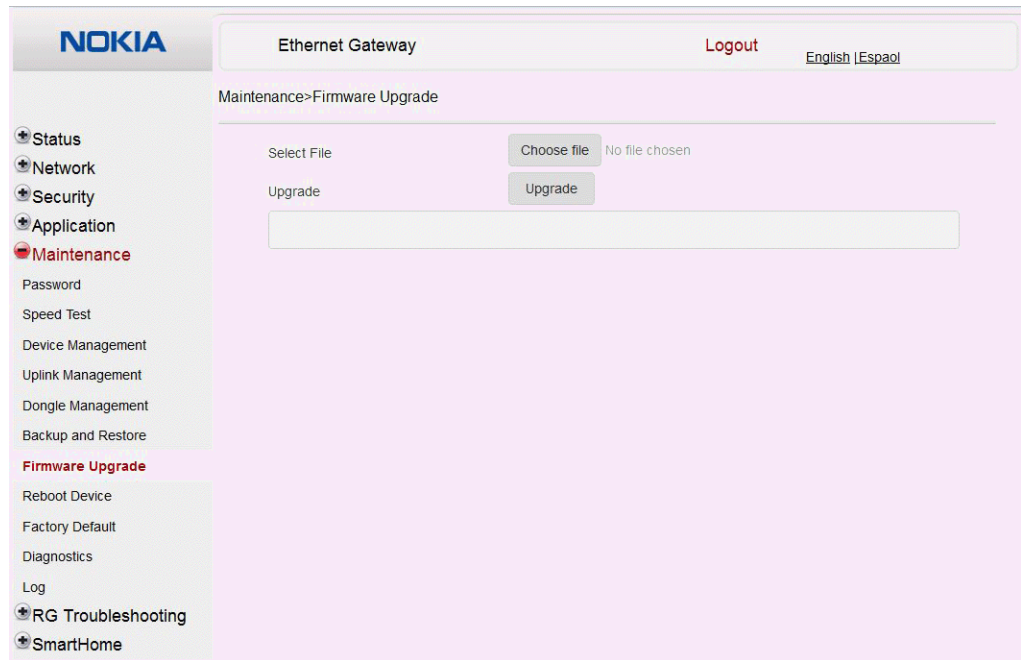
2   Click Select File and choose the new firmware file.

3   Click Upgrade to upgrade the firmware.

4   STOP. This procedure is complete.

Procedure 39   Reboot

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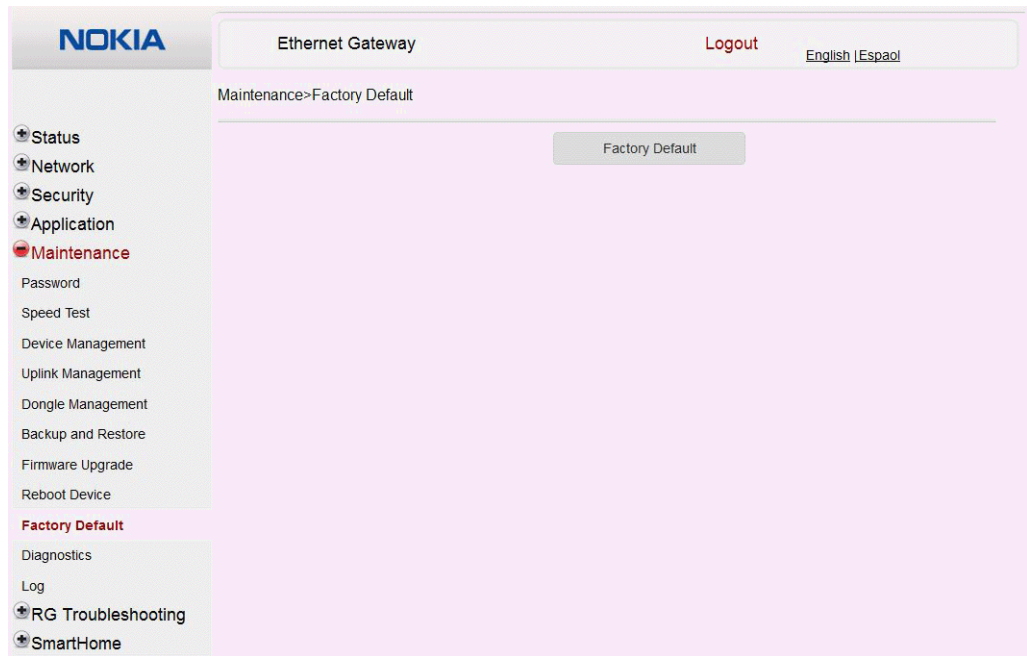
Figure 49   **Reboot Device window**

2   Click Reboot to reboot the HA-030W-B CPE.

3   STOP. This procedure is complete.

Procedure 40   Restore factory defaults

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

Figure 50   **Factory Default window**

Note — A factory reset also removes the IoT software image that was installed separately; see "IOT application software package download".

2   Click Factory Default to reset the HA-030W-B CPE to its factory default settings.

3   STOP. This procedure is complete.

Procedure 41   Diagnose connections

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

Figure 51   **Diagnostics window**

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

3   Enter the IP address or domain name.

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

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

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

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

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

9   Click Cancel to cancel the test.

10   STOP. This procedure is complete.

Procedure 42   View log files

1   Select Maintenance > Log from the top-level menu in the Ethernet Gateway window, as shown in Figure 52.

Figure 52   **Log window**
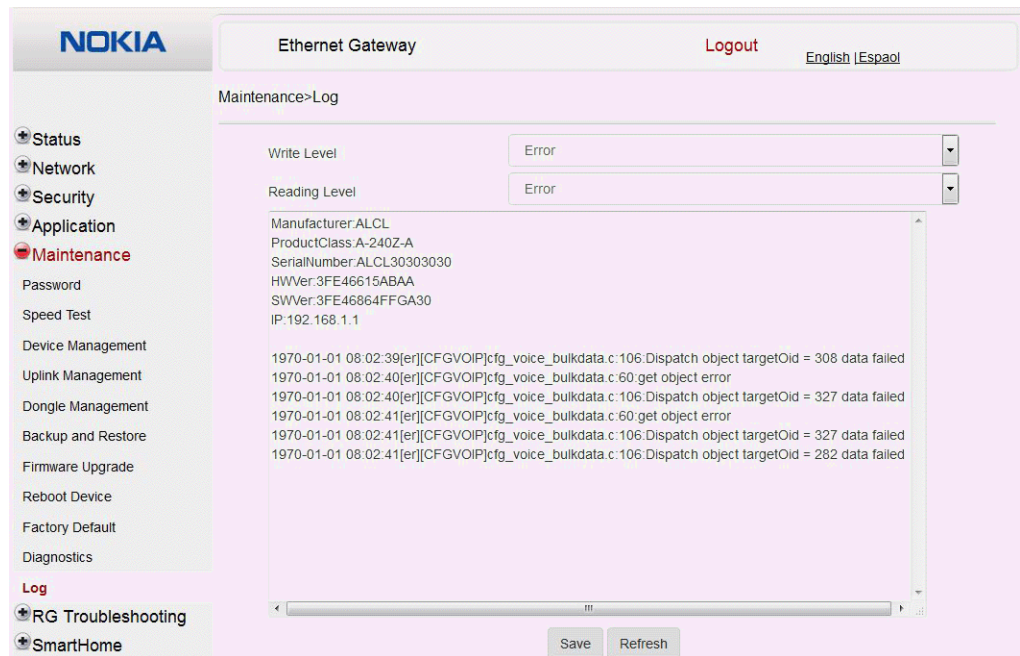
2   Choose a write level from the drop-down menu to determine which types of events are
recorded in the log file:

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

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

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

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

5   STOP. This procedure is complete.

8.2.7   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 43   Retrieve Residential Gateway (RG) troubleshooting counters

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

The RG Troubleshooting Counters window appears; see Figure 53.
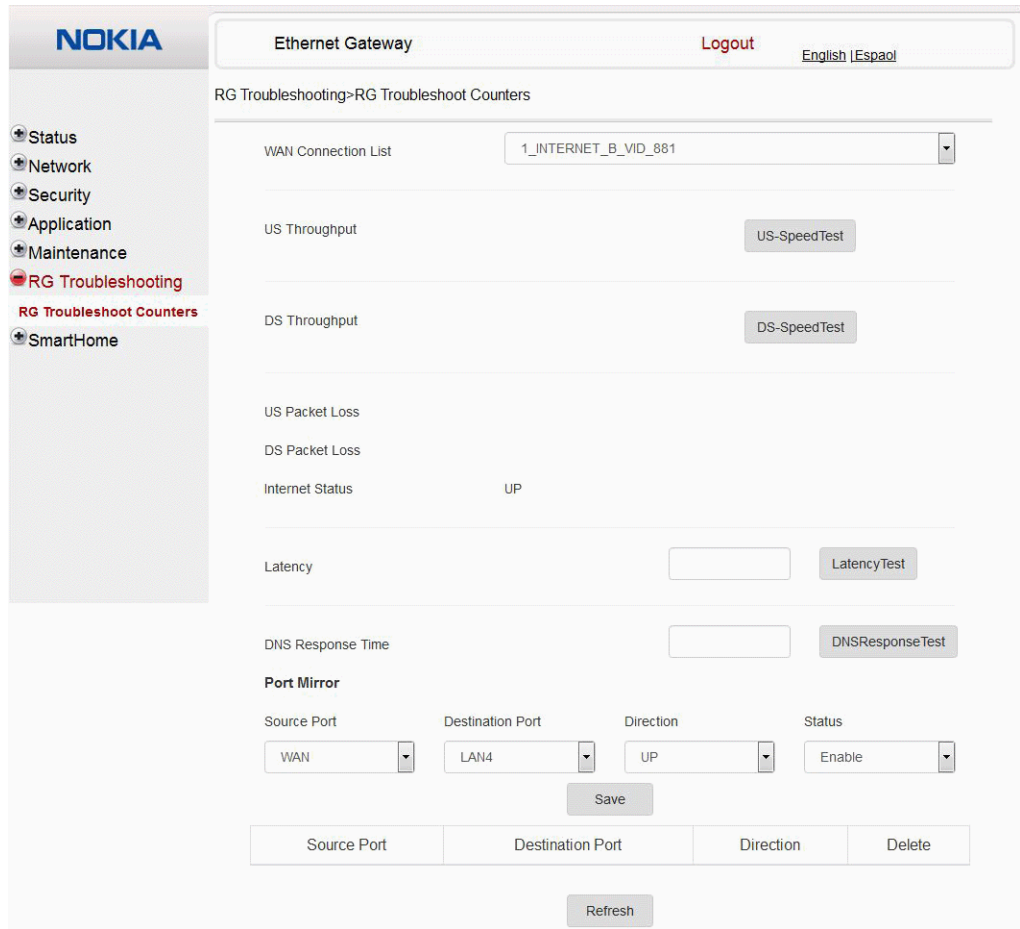
Figure 53   **RG Troubleshooting Counters window**

Table 37 describes the fields in the RG Troubleshooting Counters window.

Table 37   **RG Troubleshooting Counters parameters**

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

(1 of 2)

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

(2 of 2)

2   Configure the test times if desired.

3   Click Refresh to update the data.

**4**   STOP. This procedure is complete.

FCC Regulations:

● 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.

● 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.

● Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

● This device is restricted to indoor use.

FCC RF Radiation Exposure Statement

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

Customer document and product support
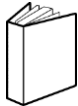
Customer documentation

Customer Documentation Welcome Page

Technical Support

Customer Documentation Technical Support

Documentation feedback

Customer Documentation Feedback