NOKIA

7368 Intelligent Services Access Manager CPE

7368 ISAM CPE HA-140W-B Product Guide

3FE-48130-AAAA-TCZZA

Issue: 01

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.

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 devices in the North American or ANSI market.

2.1 Safety instructions

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

2.1.1 Safety instruction boxes in customer documentation

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

The following is an example of the Danger box.

Danger — Possibility of personal injury.

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

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

The following is an example of the Warning box.

Warning 1 — Possibility of equipment damage.

Warning 2 — Possibility of data loss.

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

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

The following is an example of the Caution box.

Caution 1 — Possibility of service interruption.

Caution 2 — Service interruption.

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

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

The following is an example of the Note box.

Note — Information of special interest.

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

2.1.2 Safety-related labels

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

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

Table 1 **Safety labels**

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

2.2 Safety standards compliance

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

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

2.2.1 EMC, EMI, and ESD standards compliance

The customer premises equipment complies with the following requirements:

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

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

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

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

2.2.2 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the HA-140W-B devices are in compliance with the essential requirements and other relevant provisions of Directive 2009/125/EC together with Commission Regulation (EC) No 1275/2008 and Commission Regulation (EC) No 801/2013.

The HA-140W-B devices qualify as high network availability (HiNA) equipment. Since the main purpose of HA-140W-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-140W-B interfaces and interface capacity” in chapter 5.

For information about power consumption, see “HA-140W-B detailed specifications” in chapter 5.

2.2.3 FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 23 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and consider removing the no-collocation statement.

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

1 this device may not cause harmful interference, and

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

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

2.2.4 Resistibility requirements compliance

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

2.3 Electrical safety guidelines

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

HA-140W-B devices are compliant with the following standards

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

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

2.3.1 Power supplies

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

2.3.2 Cabling

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

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

3 ETSI CPE safety guidelines

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

ℹ **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 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.

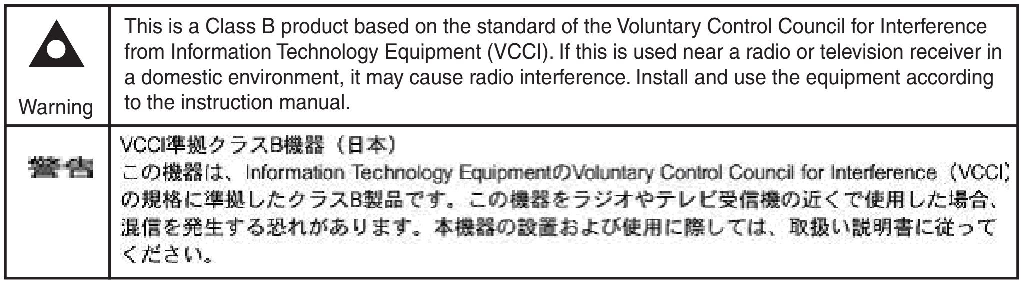
Table 2 provides sample safety labels on the CPE equipment.

Table 2 **Safety labels**

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

Figure 1 shows the PSE certification.

Figure 1 **PSE certification**



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

19841

3.2 Safety standards compliance

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

3.2.1 EMC, EMI, and ESD compliance

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

- EN 300-328 v2.1.1 wide band data transmission standards for 2.4GHz bands
- EN 301-893 v2.1.1 5 GHz wireless access systems (WAS) including RLAN equipment
- 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

3.2.2 Equipment safety standard compliance

The CPE equipment complies with the requirements of EN 62368, 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 CE RED RF Radiation Exposure Statement

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

3.2.5 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.

3.2.6 Acoustic noise emission standard compliance

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

3.3 Electrical safety guidelines

This section provides the electrical safety guidelines for the 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.
- 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, it may be advisable to provide 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 Environmental requirements

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

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 the 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.

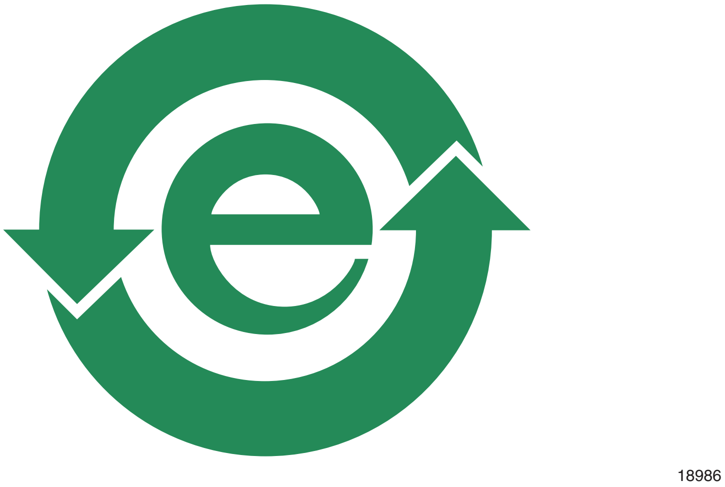
4.1.2 Environmental related labels

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

4.1.2.1 Products below Maximum Concentration Value (MCV) label

Figure 2 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.

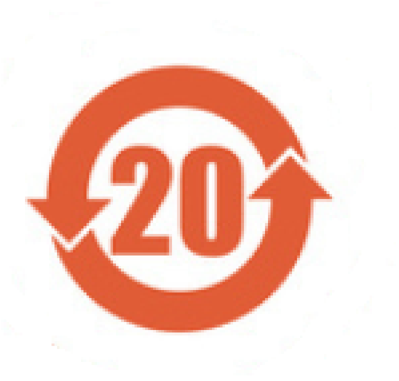
Figure 2 **Products below MCV value label**



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

Figure 3 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 3 **Products above MCV value label**



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

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.nokia-sbell.com/wwwroot/images/upload/private/1/media/ChinaRoHS.pdf

4.3 Other environmental requirements

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

4.3.1 CPE environmental requirements

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

4.3.2 Storage

According to ETS 300-019-1-1 - Class 1.2, storage of CPE equipment must be in Class 1.2, weather-protected, temperature-controlled locations.

4.3.3 Transportation

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

4.3.4 Stationary use

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

4.3.5 Material content compliance

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

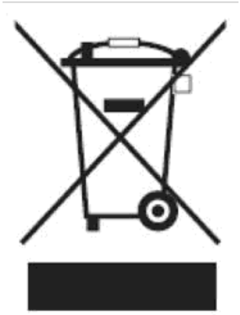
Nokia has implemented a material/substance content management process. The process is described in: Nokia process for ensuring RoHS Compliance (1AA002660031ASZZA). This ensures compliance with the European Union Directive 2011/65/EU on the Restriction of the Use of Certain Hazardous Substances in Electrical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

4.3.6 End-of-life collection and treatment

Electronic products bearing or referencing the symbol shown in Figure 4, 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 4 **Recycling/take back/disposal of product symbol**



At the end of their life, the 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 4 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-140W-B unit data sheet

5.1 HA-140W-B part numbers and identification

Table 3 provides part numbers and identification information for the HA-140W-B indoor CPE.

Table 3 **Identification of HA-140W-B indoor CPEs**

Ordering kit part number	Provisioning number	Description	CLEI	CPR	ECI/ Bar code
3FE 48111 AA	3FE 48130 AA	CPE with 1 WAN uplink (10/100/1000Mbps auto-negotiate), 1 FXS VoIP port, 4 10/100/1000 Base-T Ethernet interfaces, dual-band WiFi with 3x3 802.11b/g/n at 2.4 GHz and 4x4 802.11ac at 5 GHz. Includes a 2-pin wall-mounted US plug (12V, 2.5A, 6KV surge protection). This CPE also features 2 USB 2.0 ports.	—	—	—
3FE 48111 BA	3FE 48130 BA	CPE with 1 WAN uplink (10/100/1000Mbps auto-negotiate), 1 FXS VoIP port, 4 10/100/1000 Base-T Ethernet interfaces, dual-band WiFi with 3x3 802.11b/g/n at 2.4 GHz and 4x4 802.11ac at 5 GHz. Includes a 2-pin wall-mounted EU plug (12V, 2.5A, 6KV surge protection). This CPE also features 2 USB 2.0 ports.	—	—	—

(1 of 2)

Ordering kit part number	Provisioning number	Description	CLEI	CPR	ECI/ Bar code
3FE 48111 CA	3FE 48130 BA	CPE with 1 WAN uplink (10/100/1000Mbps auto-negotiate), 1 FXS VoIP port, 4 10/100/1000 Base-T Ethernet interfaces, dual-band WiFi with 3x3 802.11b/g/n at 2.4 GHz and 4x4 802.11ac at 5 GHz. Includes a 3-pin wall-mounted UK plug (12V, 2.5A, 6KV surge protection). This CPE also features 2 USB 2.0 ports.	—	—	—
3FE 48111 CB Customer-specific	3FE 48130 CA	CPE with 1 WAN uplink (10/100/1000Mbps auto-negotiate), 1 FXS VoIP port, 4 10/100/1000 Base-T Ethernet interfaces, dual-band WiFi with 3x3 802.11b/g/n at 2.4 GHz and 4x4 802.11ac at 5 GHz. Includes a 3-pin wall-mounted UK plug (12V, 2.5A, 6KV surge protection). This CPE also features 2 USB 2.0 ports.	—	—	—

(2 of 2)

Table 4 provides the power supply information for the HA-140W-B CPE. For more information on power supplies, see the *7368 ISAM ONT Power Supply and UPS Guide*.

Table 4 **HA-140W-B power supply**

Power supply company	Model	Country/Region	Power Watt
Fuhua	UES36WB-120250SPA	UK	30W
	UES36WU-120250SPA	US	30W
	UES36WV-120250SPA	EU	30W
Soy	Soy-1200300GB	UK	36W
	Soy-1200300EU	EU	36W
	Soy-1200300US	US	36W

5.2 HA-140W-B general description

HA-140W-B indoor CPEs provide the subscriber interface for the network by terminating the Ethernet uplink and converting it to user interfaces that directly connect to subscriber devices. The CPE is compatible with all existing subscriber equipment, including analog phones with both tone and rotary dial capabilities, cordless phones, modems, fax machines, and caller ID boxes (Type I, Type II, and Type III).

The indoor HA-140W-B can be placed in its pedestal on a flat surface, such as a desk or shelf, or wall mounted in a horizontal position, using the wall mounting holes.

HA-140W-B indoor CPE provides the following functions:

- One WAN Ethernet uplink (10/100/1000 auto-negotiate)
- Four LAN Ethernet ports (10/100/1000 auto-negotiate)
- WLAN on/off button
- Nokia WiFi mesh support
- Dual-band concurrent WiFi with 3x3 802.11b/g/n at 2.4 GHz and 4x4 802.11ac at 5 GHz
- WPS button (2.4 GHz and 5 GHz)
- Two USB 2.0 ports
- LEDs disable button
- One RJ-11 FXS VoIP port
- 5 REN per line
- Traffic classification and QoS capability
- Multiple voice Codec
- MDI/MDIX auto-negotiation
- Line Rate L2 traffic
- 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
- 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
- Compatible with Nokia access bridges (Fiber ONT and G.Fast/DSL/CPE)
- Compatible with Nokia management platforms (Nokia WiFi Mesh Controller, CDP)
- Compatible with Nokia WiFi Mobile app

5.2.1 TR-069 parameter support

The HA-140W-B CPE supports the following TR-069 features:

- Host object
- Port forwarding
- Object support for Wi-Fi parameters

- Statistics and troubleshooting
- Diagnostic parameter
- Timing parameter

5.2.1.1 Host object support

The CPE provides host object support for: InternetGatewayDeviceLANDevice.Hosts.Host.

5.2.1.2 Port forwarding support

The CPE supports the port forwarding of objects via TR-069:

- Application Name
- WAN Port
- LAN Port
- Internal Client
- Protocol
- Enable Mapping
- WAN Connection List

These are the same port forwarding parameters supported in the GUI. For more information, see Table 36 in the chapter “Configure an HA-140W-B indoor CPE”.

5.2.1.3 Object support for Wi-Fi parameters

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

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

These are the same TR-069 object parameters that are supported in the GUI. For more information, see Tables 23 and 24 in the chapter “Configure an HA-140W-B indoor CPE”.

5.2.1.4 Statistics and troubleshooting support

The CPE supports TR-069 statistics and troubleshooting for LAN, WAN, and WiFi.

For more information, see the Procedure “Statistics retrieval” in the chapter “Configure an HA-140W-B indoor CPE”.

5.2.1.5 Diagnostic parameter support

The CPE supports the following TR-069 diagnostic parameters:

- TR-143
- IP ping
- traceroute

These are the same diagnostic parameters supported in the GUI. For more information, see Procedure “Diagnose WAN connections” in the chapter “Configure an HA-140W-B indoor CPE”.

5.2.1.6 Timing parameter support

The CPE supports TR-069 timing parameters.

5.2.2 TR69 authentication using TLS and CA certificates

HA-140W-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 CPE can also authenticate the ACS using a pre-installed CA certificate.

5.2.3 TR-104 parameter extension support for voice service

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

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

The proprietary attribute is: X_ALU-COM_XML_File_Name_Path.

5.2.4 TR-104 voice-related alarms

The HA-140W-B CPE supports the following four TR-104 voice-related alarms on a per FXS port basis.

These alarms all represent SIP registration failures with an alarm level of MAJOR.

- SIPREGDNS: domain name could not be resolved
- SIPREGAUTH: authentication failed
- SIPREGTO: re-transmissions timed out
- SIPREGERFRSP: error response from the registration server

5.2.5 TR-104 parameters for FX line testing

New attributes have been added to the TR-104 Voice Service object structure to enable the ACS to perform line tests. The CPE supports the following electrical line tests:

- hazardous potential
- foreign electrical motive force
- resistive faults
- receiver off-hook test
- ringers test

5.2.6 TR-111 support

The HA-140W-B CPE supports TR-111, which extends the WAN Management Protocol defined in TR-069 to enhance the ability to remotely manage LAN devices.

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

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

5.2.7 TR-181 parameter support

TR-181 parameter support has been introduced or enhanced for the parameter categories and functions listed in Table 5.

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

Table 5 Support for TR-181 parameter categories

Parameter category	Functionality
Diagnostics	Bulk data: collection, reports, HTTP, and encoding
	DNS
	IP ping
	TR-143 uploading and downloading
	IPv6
	Periodic statistics
	Self test
	WiFi neighboring
End user functional features	Bridging port
	Captive portal
	Device information, including: processor, data model, and vendor log
	Device interface
	DHCPv4 and DCHPv6 client and server
	Ethernet interface
	Firewall
	Hosts
	Interface stack
	IP interface configuration
End user functional features	Management server
	NAT
	Neighbor discovery
	PPP interface
	QoS classification, QoS queue, and QoS shaper
	Routing and route information
	Timing
	Remote access
	User
	WiFi: AP configuration, radio configuration, and SSID configuration
Statistics and status monitoring	Bridging statistics
	Device information processes
	WiFi radio statistics

(1 of 2)

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

(2 of 2)

5.3 HA-140W-B software and installation feature support

For information on installing or replacing the HA-140W-B, see:

- Install an HA-140W-B indoor CPE
- Replace an HA-140W-B indoor CPE

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

- CPE and MDU general descriptions of features and functions
- Ethernet interface specifications
- POTS interface specifications
- Wi-Fi specifications

5.4 HA-140W-B interfaces and interface capacity

Table 6 describes the supported interfaces and interface capacity for HA-140W-B indoor CPEs.

Table 6 **HA-140W-B indoor CPE interface connection capacity**

CPE type and model	Maximum capacity								
	POTS	10/ 100 BASE-T	10/ 100/ 1000 BASE-T	RF video (CATV)	MoCA	VDSL2	E1/T1	Local craft	WAN uplink
HA-140W-B [1]	1	—	4	—	—	—	—	—	1

Note

[1] The HA-140W-B CPEs provide Wi-Fi service that is enabled and disabled using a Wi-Fi on/off switch.

5.4.1 HA-140W-B connections and components

Figure 5 shows the physical connections for HA-140W-B indoor CPEs.

Figure 5 **HA-140W-B indoor CPE physical connections**

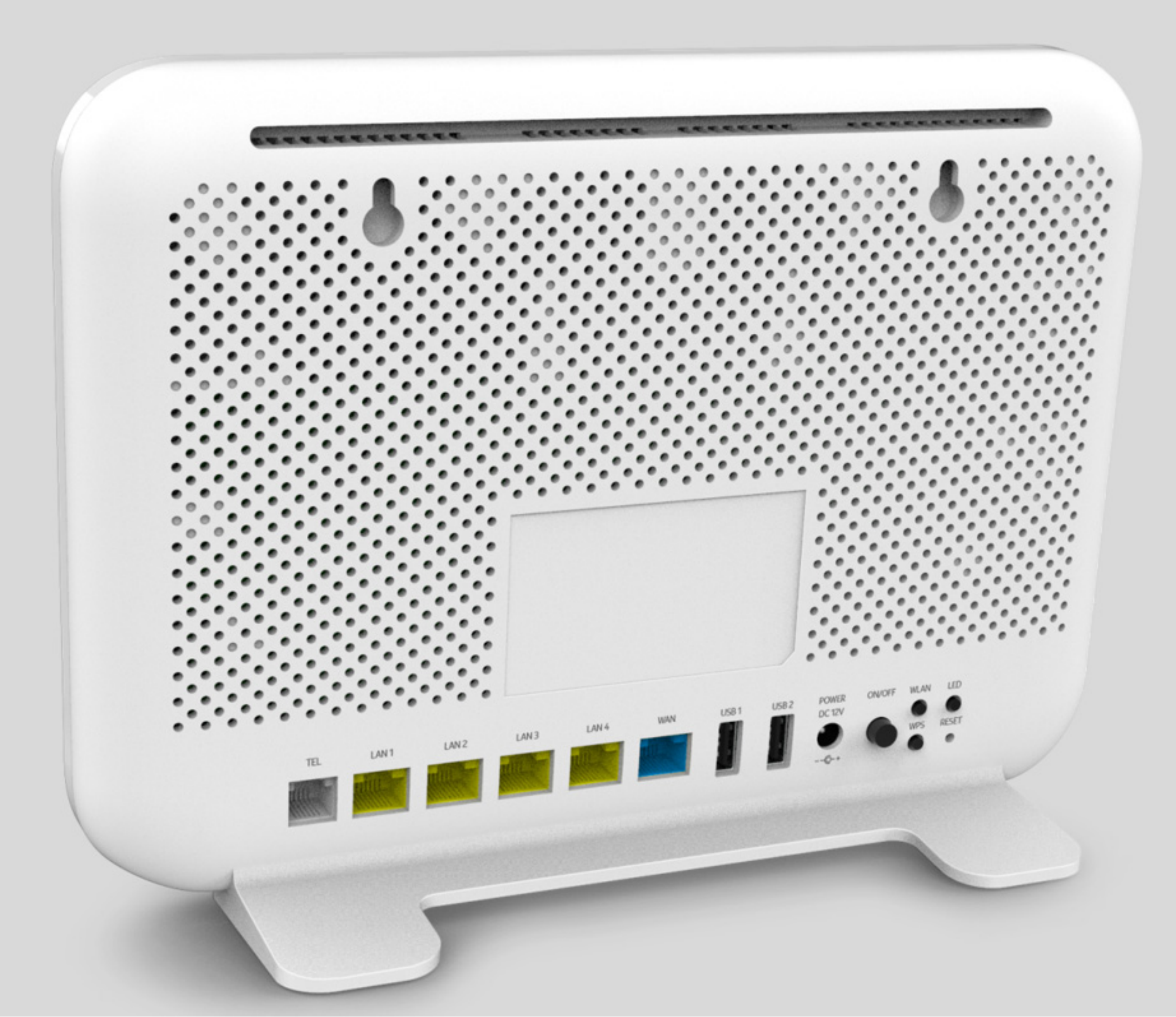


Table 7 describes the physical connections for HA-140W-B indoor CPEs.

Table 7 **HA-140W-B indoor CPE physical connections**

Connection	Description
TEL (POTS port)	This connection is provided through an RJ-11 port. One POTS connection is supported.The POTS port supports voice services.

(1 of 2)

Connection	Description
LAN 1-4 (Ethernet ports)	This connection is provided through an Ethernet RJ-45 connector. Up to four 10/100/1000 Base-T Ethernet interfaces are supported.The Ethernet ports can support both data and in-band video services on all four interfaces.
WAN port	This connection is provided through a broadband WAN interface. One 10/100/100 Gigabit Ethernet interface is supported.
USB ports	This connection is provided through a USB port. The CPE supports two external USB hard drives that can be made accessible to all LAN devices.
Power input DC 12V	This connection is provided through the power connector. A power cable fitted with a barrel connector is used to make the connection.
On/Off button	This button turns the CPE on or off.
WPS button	The Wi-Fi Protected Setup button is labeled as WPS. This button enables and disables WPS for 2.4 GHz and 5 GHz bands.
WLAN button	The WLAN button turns the Wi-Fi service on or off. Wi-Fi service is compliant with IEEE 802.11 standards and is enabled or disabled using the WLAN button.
LED	This turns the LEDs on or off.
Reset button	Pressing the Reset button for less than 10 seconds reboots the CPE. Pressing the Reset button for 10 seconds resets the CPE to its factory defaults.

(2 of 2)

5.5 HA-140W-B LEDs

Figure 6 shows the HA-140W-B indoor CPE LEDs.

Figure 6 **HA-140W-B indoor CPE LEDs**

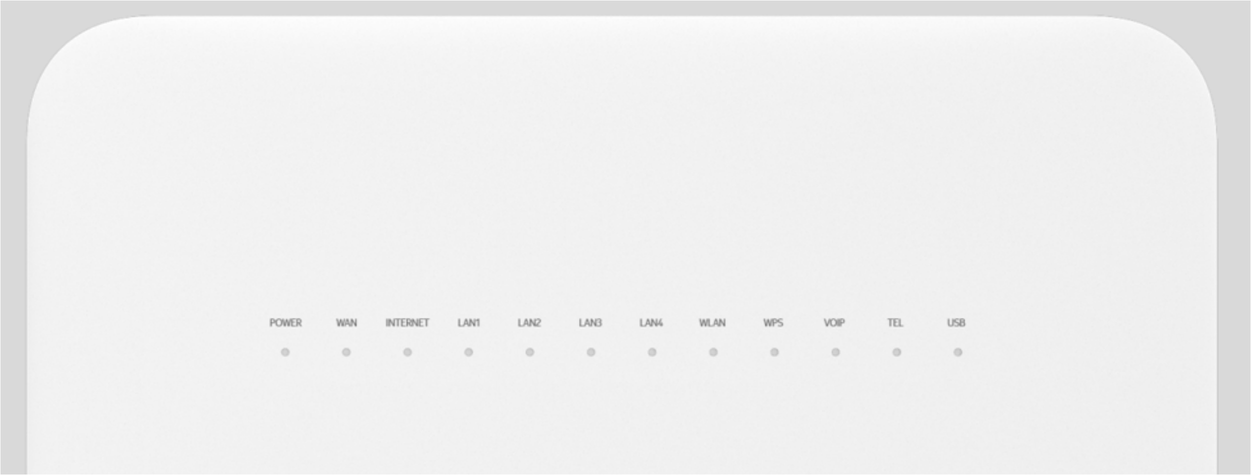


Table 8 provides LED descriptions for HA-140W-B indoor CPEs.

Table 8 HA-140W-B indoor CPE LED descriptions

Indicator	LED color and behavior	LED behavior description
POWER	Off Green solid Green flashing Red solid Red flashing Orange flashing	Power off. Power on (self test succeeded). Device is posting and booting. Normal for 5 seconds after powering up; after that: device is unable to load software. Power on self test fails on startup (for example, flash is corrupt). Firmware upgrade in progress.
WAN	Off Green solid Orange solid Orange/green flashing	Ethernet link is down or no link is connected. Ethernet link is up; WAN connection at Gigabit speed. Ethernet link is up; WAN connection at 100 or 1000Mbps speed. Ethernet traffic in either direction; (LED color indicates the sync speed of the port).
INTERNET	Off Green solid [1] Green flashing Red solid	a) Broadband physical connection is not present or power is off; or b) Device is in bridged mode without an assigned IP address. Device has a WAN IP address from IPCP or DHCP, or Static, and the broadband link is up. The device is acquiring an IP address using PPPoE or DHCP. The IP connection could not be set up.
LAN 1 to 4	Off Green solid [2] Orange solid Orange/green flashing	Ethernet link is down or no link is connected. Ethernet link is up; device is connected to LAN at Gigabit speed. Ethernet link is up; device is connected to LAN at 10 or 100Mbps speed. Ethernet traffic in either direction; (LED color indicates the sync speed of the port).
WLAN	Off Green solid	WLAN link (2.4GHz and 5GHz) is disabled or no link is connected. WLAN link is enabled (2.4GHz or 5GHz link is up).
WPS	Off Green solid Green flashing Red solid	WiFi protected setup link down or no link connected (negotiation has not started or has failed). WiFi protected setup link is up (negotiation and auto-configuration successful). WiFi protected setup link activity (negotiation and auto-configuration ongoing). WiFi protected setup processing exception or multiple peers using WPS simultaneously.
VOIP	Off Green solid	VoIP service is not built up or out of service. VoIP service is built up and can provide service.
TEL	Off Green solid Green flashing	Phone is on hook (no incoming call). Phone is off hook (with or without call in progress). Phone is ringing (incoming call).
USB	Off Green solid Green flashing	No device is connected to any USB port. At least one device is connected to a USB port. There is traffic activity on at least one device connected to a USB port.

Notes

[1] If he PPPoE session is dropped due to an idle timeout but the Ethernet WAN link is still present, the light remains green. If the session is dropped for any other reason, the light is turned off.

[2] Includes devices with wake-on-LAN capability where a slight voltage is supplied to an Ethernet connection.

5.6 HA-140W-B detailed specifications

Table 9 lists the physical specifications for HA-140W-B indoor CPEs.

Table 9 **HA-140W-B indoor CPE physical specifications**

Description	Specification
Length	9.62 in. (244.3 mm)
Height	7.08 in. (179.8 mm)
Height with pedestal	7.12 in. (180.8 mm)
Width	1.12 in. (28.55 mm)
Width with pedestal	2.58 in. (68.55 mm)
Weight [within ± 0.5 lb (0.23 kg)] (net weight of CPE)	1.05 lb (0.48 kg)

Table 10 lists the power consumption specifications for HA-140W-B indoor CPE.

Table 10 **HA-140W-B indoor CPE power consumption specifications**

Mnemonic	Maximum power (Not to exceed)	Condition	Minimum power	Condition
HA-140W-B	26.4 W	1 POTS off-hook, 4 10/100/1000 Base-T Ethernet, Wi-Fi operational	3.96W	1 POTS on-hook, other interfaces/services not provisioned

Table 11 lists the environmental specifications for HA-140W-B indoor CPE.

Table 11 **HA-140W-B indoor CPE environmental specifications**

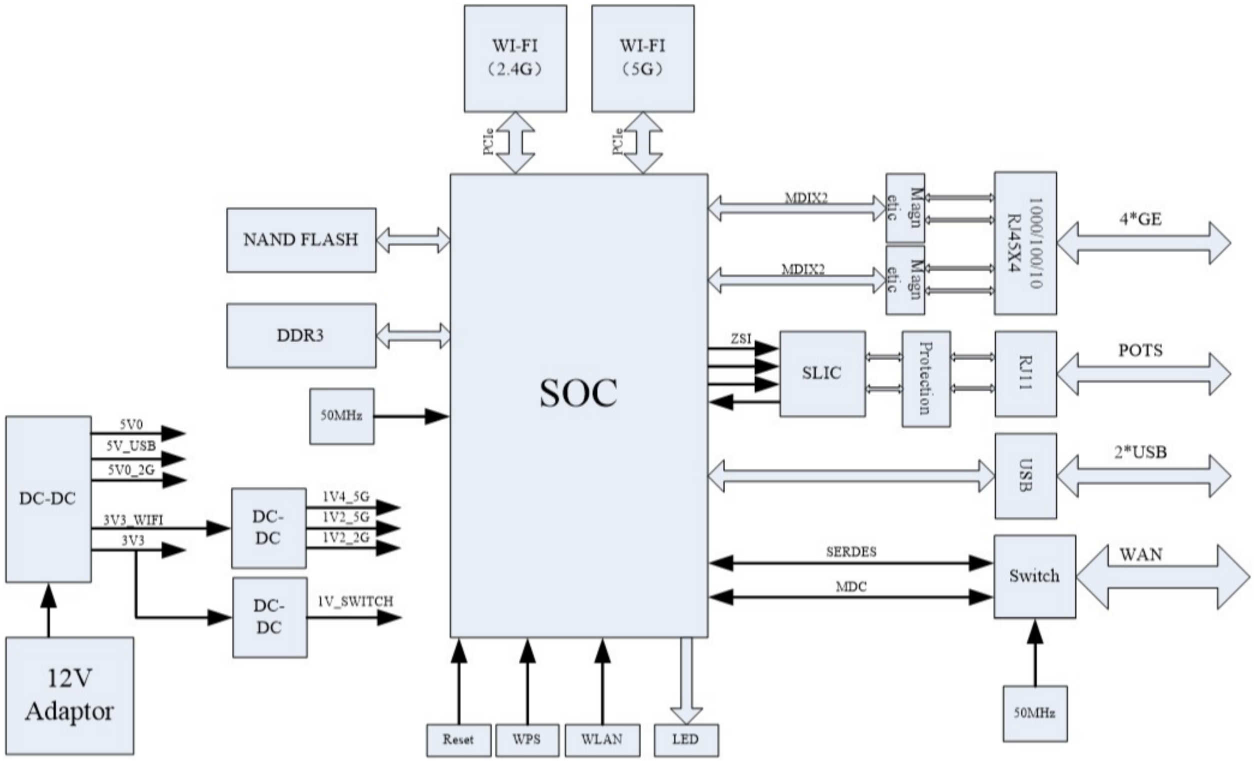
Mounting method	Temperature range and humidity	Altitude
On desk or wall mounted	Operating: 23°F to 113°F (-5°C to 45°C) ambient temperature 5% to 95% relative humidity, non-condensing	Contact your Nokia technical support representative for more information
	Storage: -4°F to 158°F (-20°C to 70°C) Storage humidity: 5% to 100%	

5.7 HA-140W-B functional blocks

HA-140W-B indoor CPEs are single-residence CPEs that support Wireless (Wi-Fi) service. Wi-Fi service on these CPEs is compliant with the IEEE 802.11 standard and enabled or disabled using a WLAN button. In addition to the Wi-Fi service, these CPEs transmit Ethernet packets to four RJ-45 Ethernet ports and voice traffic to one RJ-11 POTS port. These CPEs also feature two USB ports, and power connectors.

Figure 7 shows the functional blocks for HA-140W-B indoor CPE.

Figure 7 **Single-residence Wi-Fi CPE with Gigabit Ethernet and POTS and without RF video**



5.8 HA-140W-B standards compliance

HA-140W-B indoor CPEs are compliant with the following standards:

- 802.1p marking and VLAN based pbit is supported
- 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)
- EN 300 328 v2.1.1 wide band data transmission standards for 2.4 GHz bands

- EN 301 893 v2.1.1 5 GHz RLAN: Harmonized Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU
- G.711, G.722, G.723, G.726, G.729 A, B (voice)
- ITU-T 1.552 for POTS ports
- CE marking for European standards for health, safety, and environmental protection
- FCC marking for US standards for health, safety, and environmental protection

5.8.1 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the HA-140W-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-140W-B CPES qualify as equipment with high network availability (HiNA) functionality. Since the main purpose of HA-140W-B CPEs 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-140W-B interfaces and interface capacity” in this chapter.

For information about power consumption, see “HA-140W-B detailed specifications” in this chapter.

5.8.2 FCC statement

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

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

5.8.3 FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 23 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.

5.9 HA-140W-B Wi-Fi features

5.9.1 Wi-Fi service

HA-140W-B indoor CPEs feature Wi-Fi service as well as voice and data services. Wi-Fi is a wireless networking technology that uses radio waves to provide wireless HSI and network connections. This CPE 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 physical features

HA-140W-B indoor CPEs have the following physical features that assist in providing Wi-Fi service:

- WLAN button for enabling and disabling Wi-Fi service
- 7 internal antennas: 3 for 2.4GHz and 4 for 5GHz
- one Wi-Fi Protected Setup (WPS) push button for both 2.4GHz and 5GHz controlling

5.9.1.2 Wi-Fi standards and certifications

The Wi-Fi service on HA-140W-B indoor CPEs supports the following IEEE standards and Wi-Fi Alliance certifications:

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

5.9.1.3 Wi-Fi GUI features

HA-140W-B indoor CPEs have HTML-based Wi-Fi configuration GUIs.

5.10 HA-140W-B CPE considerations and limitations

Table 12 lists the considerations and limitations for Package P HA-140W-B CPEs.

Table 12 **HA-140W-B CPE considerations and limitations**

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

6 Install an HA-140W-B indoor CPE

6.1 Purpose

This chapter provides the steps to install a HA-140W-B indoor CPE.

6.2 General

The steps listed in this chapter describe mounting and cabling for HA-140W-B indoor CPEs.

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:

- for wall mounting:
  - screws and screwdriver
  - 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 indoor CPE 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.
- Indoor CPEs must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the HA-140W-B unit data sheet for the temperature ranges for these CPEs.

6.6 Procedure

Use this procedure to install a HA-140W-B indoor CPE.

1 Place the indoor CPE unit:

a In its pedestal on a flat surface, such as a desk or shelf; go to step 3.

Note — The HA-140W-B cannot be stacked with another CPE or with other equipment. The CPE mounting requirements are:

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

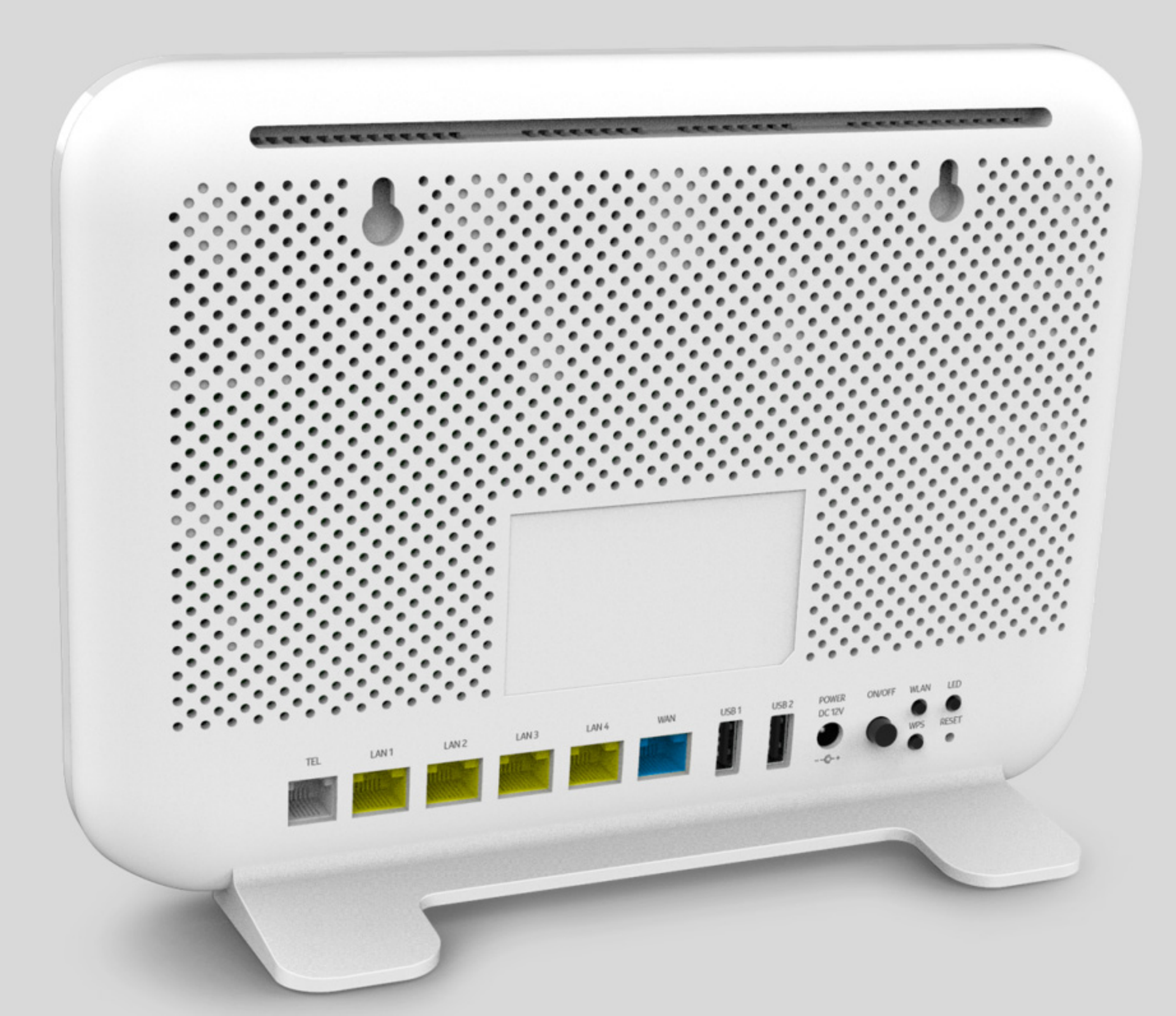
b On a wall; go to step 2.

2 Mount the HA-140W-B indoor CPE to a wall.

The HA-140W-B indoor CPE must be mounted in a horizontal position, as indicated by the wall mounting key holes in Figure 8.

Figure 8 shows the CPE with the connections and the key mounting holes.

Figure 8 **HA-140W-B CPE with connections and key mounting holes**



i Drill two holes into the wall where the CPE will be mounted. If possible, mount the CPE on a wall stud.

Do not drive the screw into the wall completely. Leave approximately 1/8 in. (6 mm) between the screw head and the wall surface.

ii Drive the mounting screws into the holes.

The recommended length of the mounting screw is 1.15 in. (3.8 cm).

iii Slide the wall mount keyholes on the CPE enclosure down over the mounting screws until the CPE is securely seated.

3 Review the connection locations, as shown in Figure 8.

4 Route the POTS cable directly to the RJ-11 TEL port as per local practices; see Figure 8.

5 Connect the Ethernet WAN and LAN cables to the RJ-45 ports; see Figure 8 for the location of the RJ-45 ports.

6 Connect the power cable to the power connector.

7 Plug the power supply in a power socket.

Note — Observe the following:

- Nokia recommends that you use only the power adapter supplied with the CPE.

  In case an alternative adapter is used, make sure that it is approved by local regulation and matches polarity, voltage, and minimum power, as indicated on the CPE.

8 Power up the CPE unit by using the power switch.

9 If used, enable the Wi-Fi service.

i Locate the WLAN button; see Figure 8 for the location of the WLAN button.

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

10 If used, enable the WPS.

i Locate the WPS button; see Figure 8 for the location of the WPS button.

ii Press the WPS button to change the status of the WPS.

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

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

13 If necessary, reset the CPE.

i Locate the Reset button; see Figure 8.

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

14 STOP. This procedure is complete.

7 Replace an HA-140W-B indoor CPE

7.1 Purpose

This chapter provides the steps to replace HA-140W-B indoor CPEs.

7.2 General

The steps listed in this chapter describe mounting and cabling for HA-140W-B indoor CPEs.

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 CPE:

- for wall mounting:
  - screws and screwdriver
  - drill and drill bits
- paper clip

7.5 Safety information

Read the following safety information before replacing the unit.

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

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

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

Caution — 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:

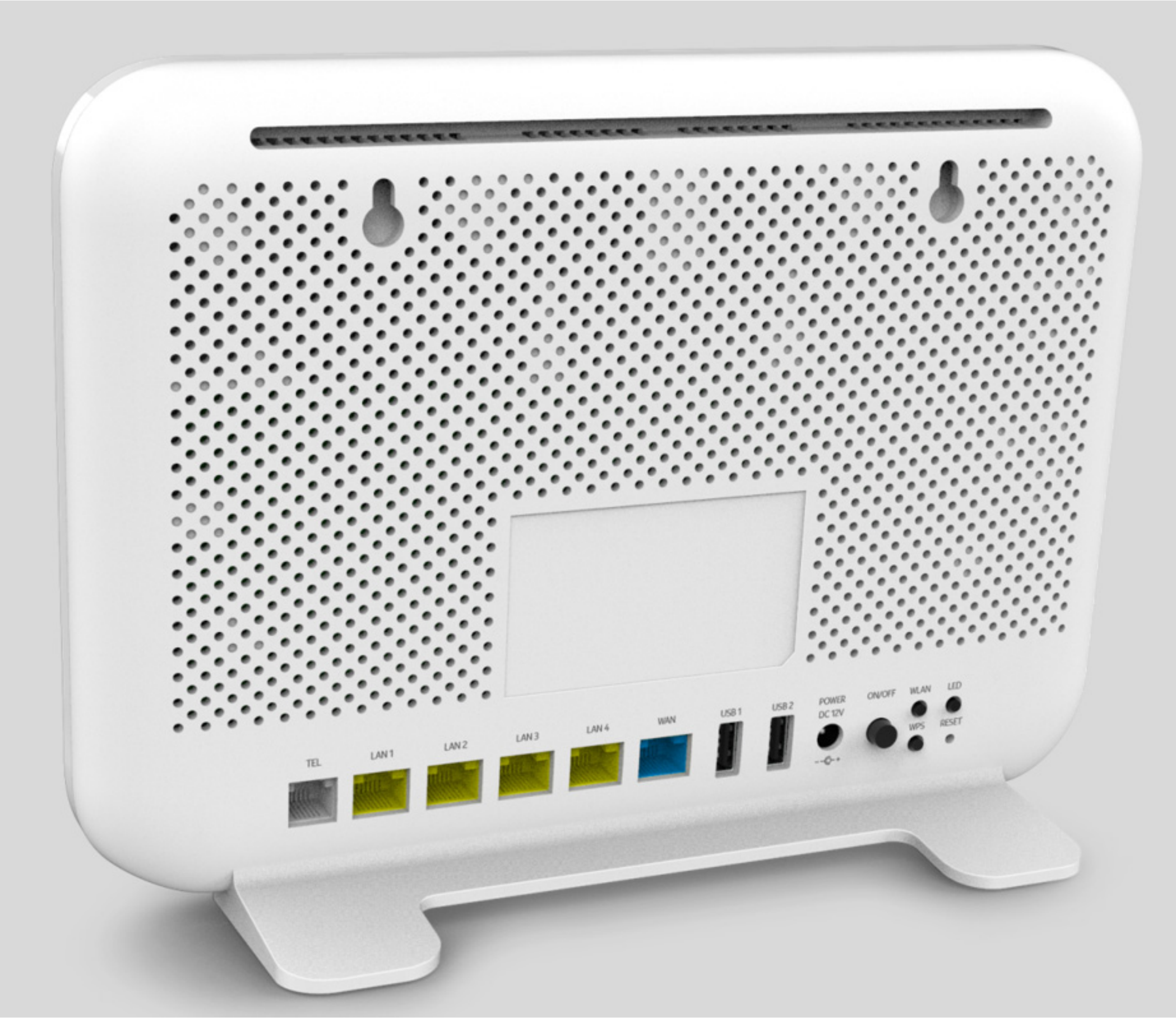
- The indoor CPE should be installed in accordance with the applicable requirements of the NEC or CEC. Local authorities and practices take precedent when there is conflict between the local standard and the NEC or CEC.
- Indoor CPEs must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the HA-140W-B unit data sheet for the CPE temperature ranges for these CPEs.

7.6 Procedure

Use this procedure to replace a HA-140W-B indoor CPE.

1 If used, disable the Wi-Fi service by pressing the WLAN button; see Figure 9 for the location of the WLAN button.

Figure 9 **HA-140W-B indoor CPE connections**



2 Power down the unit by using the on/off power switch; see Figure 9 for the location of the power switch.

3 Disconnect the POTS, Ethernet, and power cables from the CPE; see Figure 9 for the connector locations on the HA-140W-B indoor CPE.

4 Replace the CPE with a new unit:

a On a flat surface, such as a desk, substitute the new CPE for the old CPE, horizontally resting in its pedestal.

b On a wall.

i Slide the old CPE off of the mounting screws until the CPE is free of the wall.

ii Slide the wall mount holes onto the CPE enclosure over the mounting screws until it is securely seated.

5 Connect the POTS cable directly to the RJ-11 port as per local practices; see Figure 9 for the location of the RJ-11 port.

6 Connect the Ethernet WAN and LAN cables directly to the RJ-45 ports; see Figure 9 for the location of the RJ-45 ports.

7 Connect the power cable to the power connector.

8 Plug the power supply in a power socket.

Note — Observe the following:

- Nokia recommends that you use only the power adapter supplied with the CPE.

  In case an alternative adapter is used, make sure that it is approved by local regulation and matches polarity, voltage, and minimum power, as indicated on the CPE.

9 Power up the unit by using the power switch.

10 If used, enable the Wi-Fi service by pressing the WLAN button; see Figure 9 for the location of the WLAN button.

11 If used, enable the WPS by pressing the WPS button; see Figure 9 for the location of the WPS button.

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

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

14 If necessary, reset the CPE.

i Locate the Reset button; see Figure 9.

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

15 STOP. This procedure is complete.

8 Configure an HA-140W-B indoor CPE

8.1 General

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

8.2 HGU mode GUI configuration

Use the procedures below to use the web-based GUI for the HA-140W-B in HGU mode. This mode is preset at delivery.

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

8.2.1 Login

Use the procedure below to login to the web-based GUI for the HA-140W-B.

Procedure 6 Login to web-based GUI

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

The login window appears.

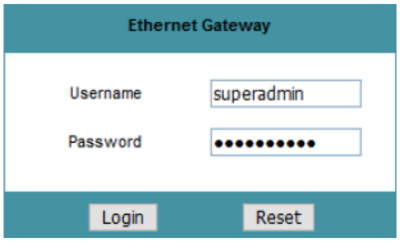
The default gateway IP address is http://192.168.1.1. You can connect to this IP address using your web browser after connecting your PC to one of Ethernet ports of the CPE. The static IP address of your PC must be in the same 192.168.1.x subnet as the CPE.

Depending on the operator settings, the HGU may also provide an IP address to the connected device without requiring a static IP address.

2 Enter your username and password in the Log in window, as shown in Figure 10.

The default user name is admin or superadmin. The default password is shown on the device label.

Figure 10 **Web login window**



Ethernet Gateway

Username: superadmin

Password: ●●●●●●●●●●

Caution — 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, except for the LOID and SLID.

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

3 Click Login. The Device Information screen appears.

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

HA-140W-B CPEs support the retrieval of a variety of device and connection information, including:

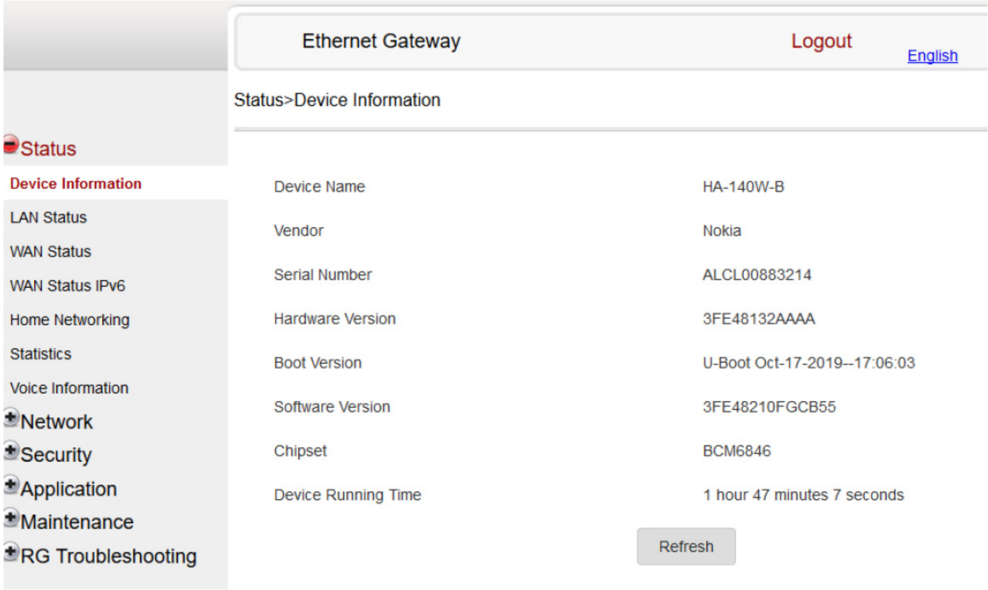
- device information
- LAN status

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

Procedure 7 Device information retrieval

1 Select Status > Device Information from the top-level menu in the Ethernet Gateway window, as shown in Figure 11.

Figure 11 **Device Information window**



Status>Device Information

Device Name	HA-140W-B
Vendor	Nokia
Serial Number	ALCL00883214
Hardware Version	3FE48132AAAA
Boot Version	U-Boot Oct-17-2019--17:06:03
Software Version	3FE48210FGCB55
Chipset	BCM6846
Device Running Time	1 hour 47 minutes 7 seconds

Table 13 describes the fields in the Device Information window.

Table 13 **Device Information parameters**

Field	Description
Device Name	Name on the CPE
Vendor	Name of the vendor
Serial Number	Serial number of the CPE
Hardware version	Hardware version of the CPE
Boot version	Boot version of the CPE

(1 of 2)

Field	Description
Software version	Software version of the CPE
Chipset	Chipset of the CPE
Device Running Time	Amount of time the device has run since last reset in hours, minutes, and seconds

(2 of 2)

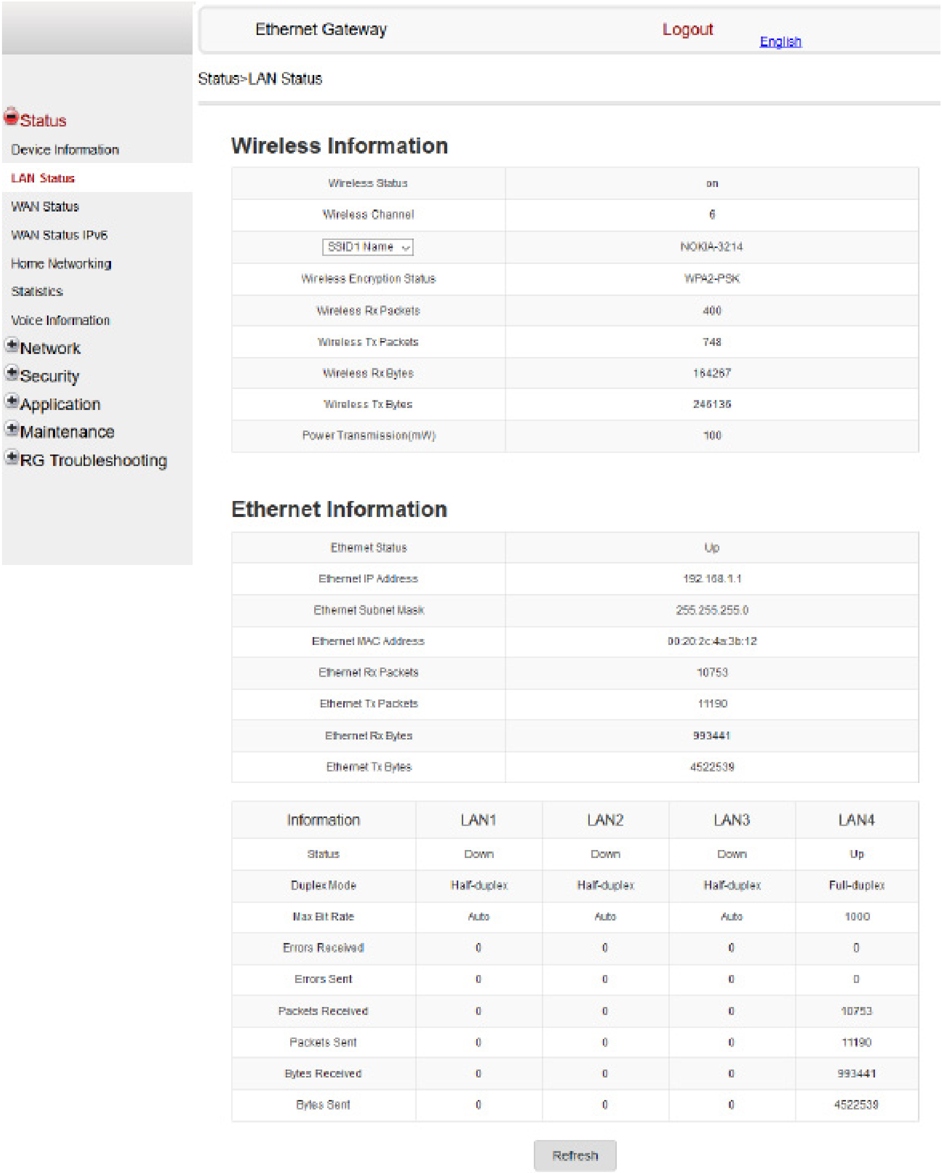
2 Click Refresh to update the displayed information.

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 12.

Figure 12 LAN status window



Wireless Information

Wireless Status	on
Wireless Channel	6
SSID1 Name	NOKIA-3214
Wireless Encryption Status	WPA2-PSK
Wireless Rx Packets	400
Wireless Tx Packets	748
Wireless Rx Bytes	184267
Wireless Tx Bytes	246136
Power Transmission(mW)	100

Ethernet Information

Ethernet Status	Up
Ethernet IP Address	192.168.1.1
Ethernet Subnet Mask	255.255.255.0
Ethernet MAC Address	00:20:2c:4a:3b:12
Ethernet Rx Packets	10753
Ethernet Tx Packets	11190
Ethernet Rx Bytes	993441
Ethernet Tx Bytes	4522539

Information	LAN1	LAN2	LAN3	LAN4
Status	Down	Down	Down	Up
Duplex Mode	Half-duplex	Half-duplex	Half-duplex	Full-duplex
Max Bit Rate	Auto	Auto	Auto	1000
Errors Received	0	0	0	0
Errors Sent	0	0	0	0
Packets Received	0	0	0	10753
Packets Sent	0	0	0	11190
Bytes Received	0	0	0	993441
Bytes Sent	0	0	0	4522539

Table 14 describes the fields in the LAN status window.

Table 14 **LAN status parameters**

Field	Description
Wireless Information	
Wireless Status	Indicates whether the wireless is on or off
Wireless Channel	Wireless channel number
SSID Name	Name of each SSID
Wireless Encryption Status	Encryption type used on the wireless connection
Wireless Rx Packets	Number of packets received on the wireless connection
Wireless Tx Packets	Number of packets transmitted on the wireless connection
Wireless Rx Bytes	Number of bytes received on the wireless connection
Wireless Tx Bytes	Number of bytes transmitted on the wireless connection
Power Transmission (mW)	Power of the wireless transmission, in mW
Ethernet Information	
Ethernet Status	Indicates whether the Ethernet connection is on or off
Ethernet IP Address	IP address of the Ethernet connection
Ethernet Subnet Mask	Subnet Mask of the Ethernet connection
Ethernet MAC Address	MAC address of the Ethernet connection
Ethernet Rx Packets	Number of packets received on the Ethernet connection
Ethernet Tx Packets	Number of packets transmitted on the Ethernet connection
Ethernet Rx Bytes	Number of bytes received on the Ethernet connection
Ethernet Tx Bytes	Number of bytes transmitted on the Ethernet connection
Information LAN 1-4	Status and other details for the LANs

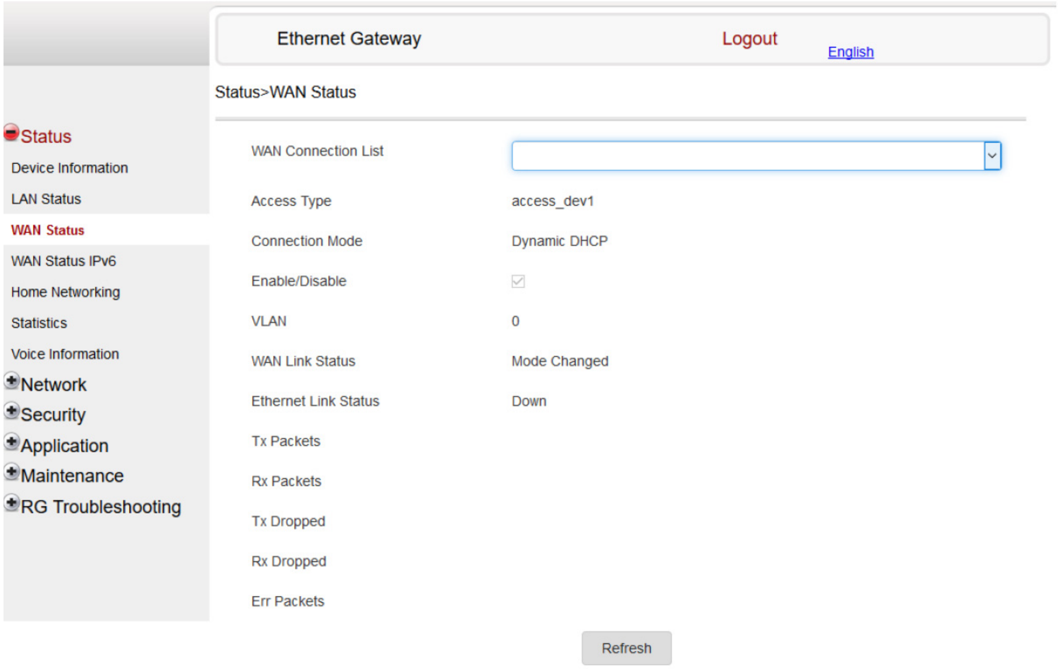
2 Click Refresh to update the displayed information.

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 13.

Figure 13 WAN status window



WAN Connection List

Access Type access_dev1

Connection Mode Dynamic DHCP

Enable/Disable ☑

VLAN 0

WAN Link Status Mode Changed

Ethernet Link Status Down

Tx Packets

Rx Packets

Tx Dropped

Rx Dropped

Err Packets

Table 15 describes the fields in the WAN status window.

Table 15 WAN status parameters

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

(1 of 2)

Field	Description
Rx Dropped	Number of packets dropped on the receive WAN connection
Err Packets	Number of errored packets on the WAN connection

(2 of 2)

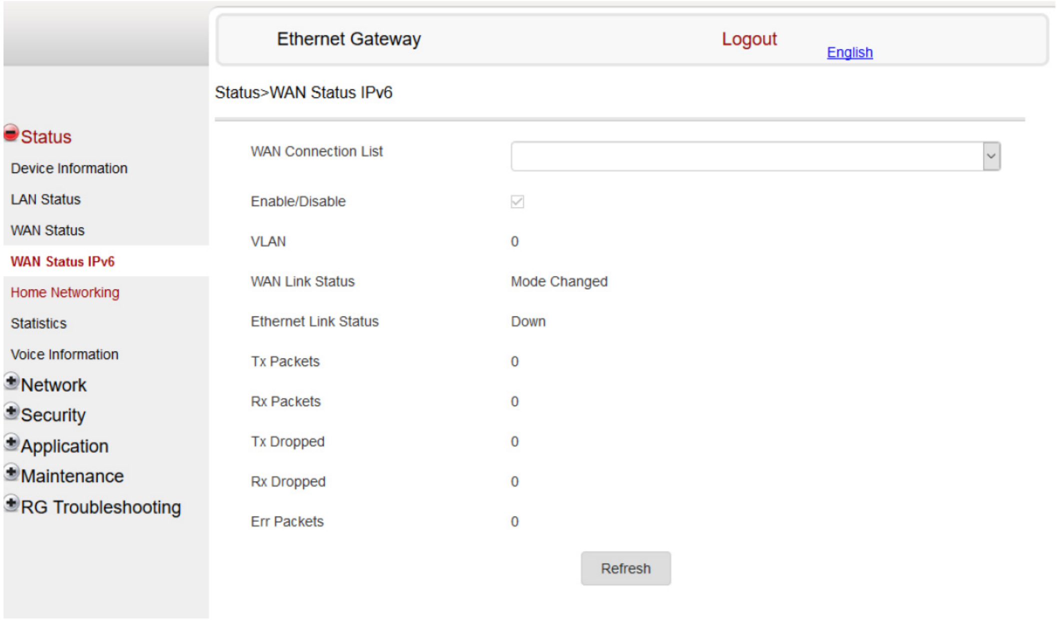
2 Click Refresh to update the displayed information.

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 14.

Figure 14 **WAN status IPv6 window**



Status>WAN Status IPv6

WAN Connection List	
Enable/Disable	☑
VLAN	0
WAN Link Status	Mode Changed
Ethernet Link Status	Down
Tx Packets	0
Rx Packets	0
Tx Dropped	0
Rx Dropped	0
Err Packets	0

Table 16 describes the fields in the WAN status IPv6 window.

Table 16 WAN status IPv6 parameters

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

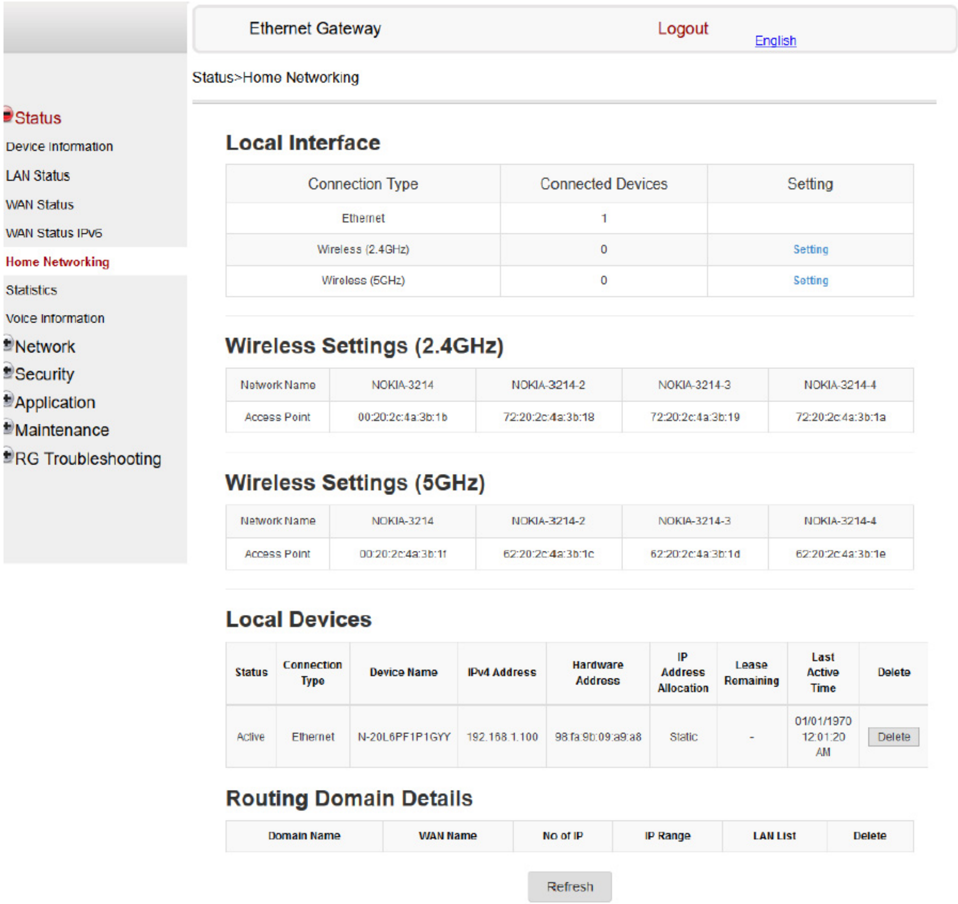
2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

Procedure 11 Home networking information retrieval

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

Figure 15 Home networking information window



Local Interface

Connection Type	Connected Devices	Setting
Ethernet	1	
Wireless (2.4GHz)	0	Setting
Wireless (5GHz)	0	Setting

Wireless Settings (2.4GHz)

Network Name	NOKIA-3214	NOKIA-3214-2	NOKIA-3214-3	NOKIA-3214-4
Access Point	00:20:2c:4a:3b:1b	72:20:2c:4a:3b:18	72:20:2c:4a:3b:19	72:20:2c:4a:3b:1a

Wireless Settings (5GHz)

Network Name	NOKIA-3214	NOKIA-3214-2	NOKIA-3214-3	NOKIA-3214-4
Access Point	00:20:2c:4a:3b:1f	62:20:2c:4a:3b:1c	62:20:2c:4a:3b:1d	62:20:2c:4a:3b:1e

Local Devices

Status	Connection Type	Device Name	IPv4 Address	Hardware Address	IP Address Allocation	Lease Remaining	Last Active Time	Delete
Active	Ethernet	N-20L6PF1P1GYY	192.168.1.100	98:fa:9b:09:a9:a8	Static	-	01/01/1970 12:01:20 AM	Delete

Routing Domain Details

Domain Name	WAN Name	No of IP	IP Range	LAN List	Delete

Table 17 describes the fields in the Home networking window.

Table 17 Home networking parameters

Field	Description
Local Interface	
Ethernet	Table displays the number of Ethernet connections and their settings
Wireless (2.4GHz)	Table displays the number of wireless connections and their settings
Wireless (5GHz)	

(1 of 2)

Field	Description
Wireless Settings (2.4GHz)	
Network Name	Name of the wireless network
Access Point	Hexadecimal address of the wireless access point
Wireless Settings (5GHz)	
Network Name	Name of the wireless network
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.
Routing Domain Details	
Table entry	Shows the domain name, WAN name, number of IPs, IP range, and LAN list.

(2 of 2)

2 Click Delete to delete a particular local device connection.

3 Click Refresh to update the displayed information.

4 STOP. This procedure is complete.

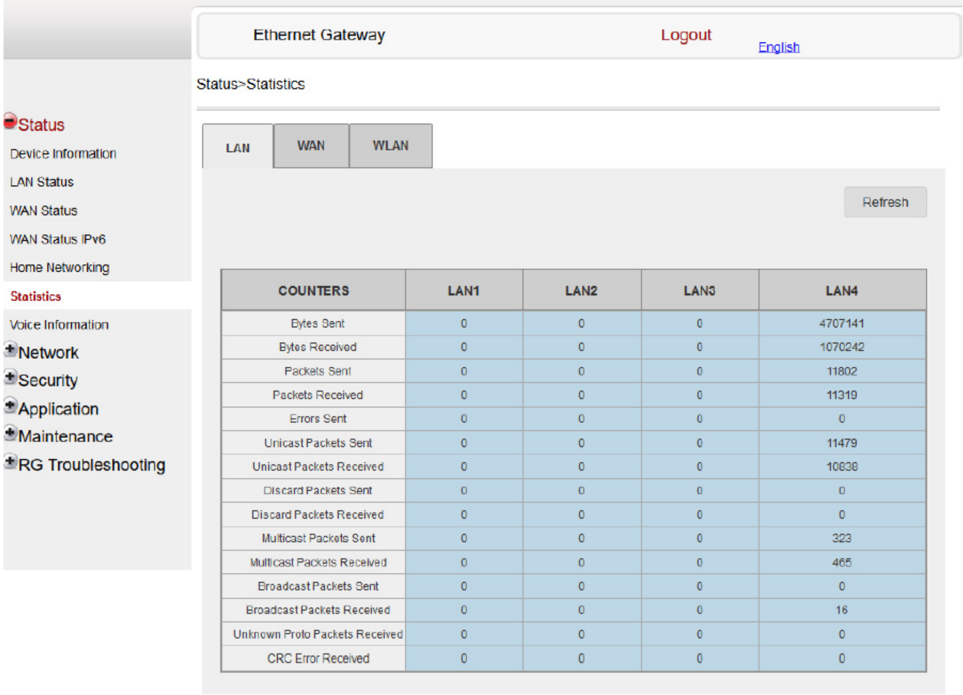
Procedure 12 Statistics retrieval

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

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

Figure 16 shows the statistics for the LAN ports.

Figure 16 **LAN ports Statistics window**



COUNTERS	LAN1	LAN2	LAN3	LAN4
Bytes Sent	0	0	0	4707141
Bytes Received	0	0	0	1070242
Packets Sent	0	0	0	11802
Packets Received	0	0	0	11319
Errors Sent	0	0	0	0
Unicast Packets Sent	0	0	0	11479
Unicast Packets Received	0	0	0	10838
Discard Packets Sent	0	0	0	0
Discard Packets Received	0	0	0	0
Multicast Packets Sent	0	0	0	323
Multicast Packets Received	0	0	0	465
Broadcast Packets Sent	0	0	0	0
Broadcast Packets Received	0	0	0	16
Unknown Proto Packets Received	0	0	0	0
CRC Error Received	0	0	0	0

If there are no WAN connections to display, the system displays a message.

If there are no WLAN connections to display, the system displays a message.

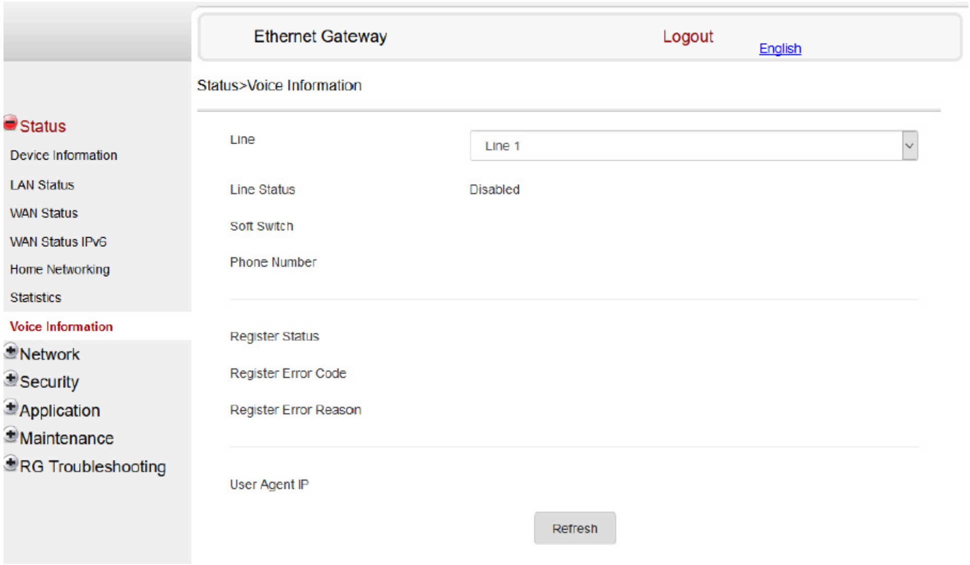
---

2 STOP. This procedure is complete.

Procedure 13 Voice information retrieval

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

Figure 17 Voice Information window



Status>Voice Information

Line: Line 1

Line Status: Disabled

Soft Switch

Phone Number

Register Status

Register Error Code

Register Error Reason

User Agent IP

Table 18 describes the fields in the Voice Information window.

Table 18 Voice Information parameters

Field	Description
Line	Choose a line from the drop-down menu. The default is Line 1.
Line Status	Depending on the line chosen, the line options are: • Up • Initializing • Registering • Unregistering • Error • Testing • Quiescent • Disabled The default is Disabled
Soft Switch(1)	Proxy IP address; blank if the line is not registered
Phone Number(1)	Phone number configured for a telephone line 1; +13290611266

(1 of 2)

Field	Description
Register Status	The default is Registered Blank if no voice service is provisioned
Register Error Code	SIP standard error code for the register status; for example, 401, 403, 503 This field is blank if the register is set to OK
Register Error Reason	SIP standard error reason for the register status This field is blank if the register is set to OK
User Agent IP	IP address of the user agent ExternalIPAddress in WANIPConnection or WANPPPConnection

(2 of 2)

Note

[1] This field is only visible at the Super User level; it is not visible at the normal user level.

2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

8.2.3 Network configuration

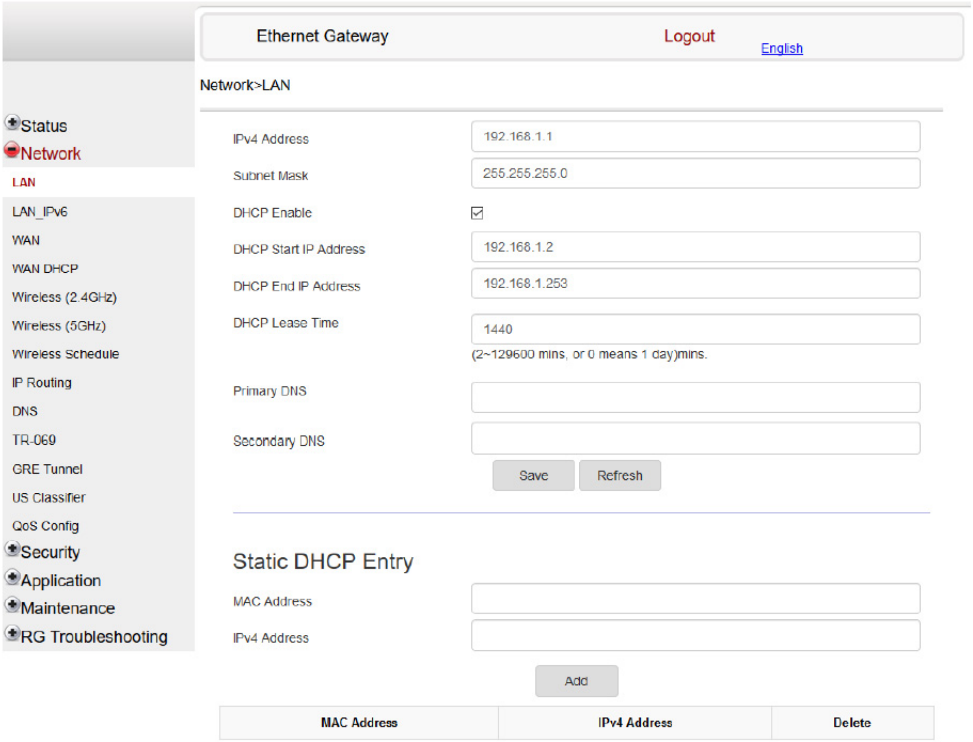
HA-140W-B CPEs support network configuration, including:

- LAN
- LAN IPv6
- WAN
- WAN DHCP
- WiFi 2.4G
- WiFi 5G
- Wireless schedule
- Routing
- DNS
- TR-069
- QoS

Procedure 14 LAN networking configuration

1 Select Network > LAN from the top-level menu in the Ethernet Gateway window, as shown in Figure 18.

Figure 18 LAN network window



IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

DHCP Enable ☑

DHCP Start IP Address 192.168.1.2

DHCP End IP Address 192.168.1.253

DHCP Lease Time 1440
(2~129600 mins, or 0 means 1 day)mins.

Primary DNS

Secondary DNS

Static DHCP Entry

MAC Address

IPv4 Address

MAC Address	IPv4 Address	Delete

Table 19 describes the fields in the LAN network window.

Table 19 LAN network parameters

Field	Description
Port Mode	
IPv4 Address	IP Address of the CPE
Subnet Mask	Subnet mask of the CPE
DHCP Enable	Select this checkbox to enable DHCP
DHCP Start IP Address	Starting DHCP IP address
DHCP End IP Address	Ending DHCP IP address
DHCP Lease Time	DHCP lease time (in min)

(1 of 2)

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

(2 of 2)

2 Select the mode for each port.

3 Click Save.

4 Enter the DHCP configuration information.

5 Click Save.

6 Enter the Static DHCP information.

7 Click Add.

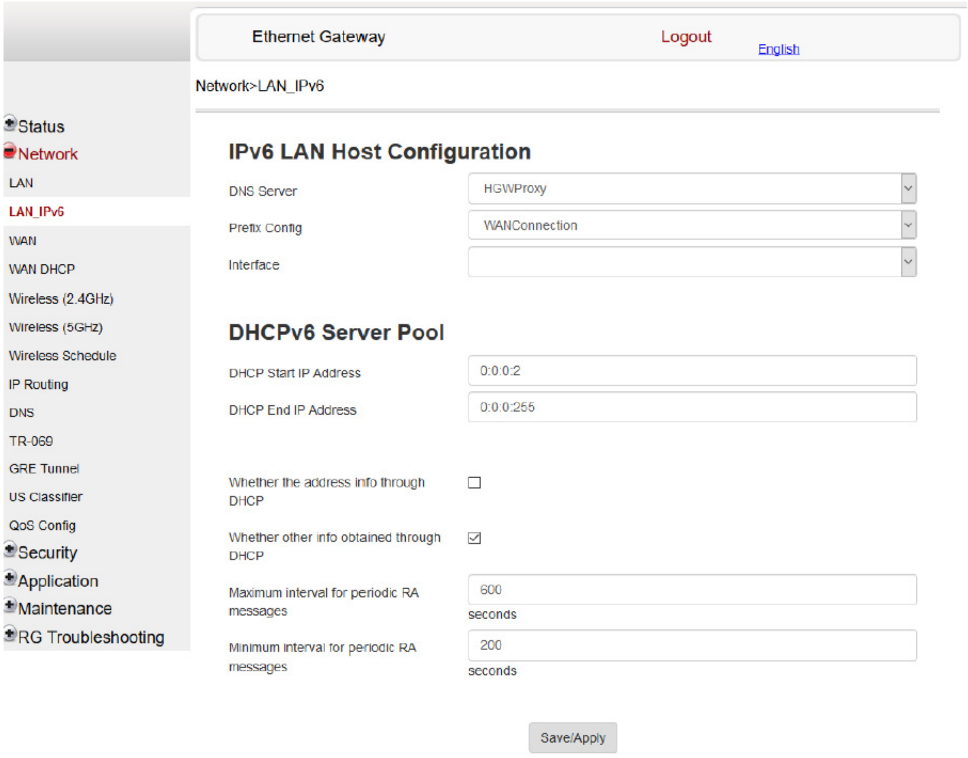
You can also use this panel to delete a Static DHCP MAC address or IPv4 address.

8 STOP. This procedure is complete.

Procedure 15 LAN IPv6 networking configuration

1 Select Network > LAN_IPv6 from the top-level menu in the Ethernet Gateway window, as shown in Figure 19.

Figure 19 LAN IPv6 network window



Network>LAN_IPv6

IPv6 LAN Host Configuration

DNS Server: HGWProxy

Prefix Config: WANConnection

Interface:

DHCPv6 Server Pool

DHCP Start IP Address: 0:0:0:2

DHCP End IP Address: 0:0:0:255

Whether the address info through DHCP ☐

Whether other info obtained through DHCP ☑

Maximum interval for periodic RA messages: 600 seconds

Minimum interval for periodic RA messages: 200 seconds

Table 20 describes the fields in the LAN IPv6 network window.

Table 20 LAN IPv6 network parameters

Field	Description
IPv6 LAN Host Configuration	
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).
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.
DHCPv6 Server Pool	
DHCP Start IP Address	Start IP address.
DHCP End IP Address	End IP address.
Whether the address info through DCHP	Select this checkbox to enable address information retrieval through DHCP.
Whether other info obtained through DHCP	Select this checkbox to enable retrieval of other information through DHCP.
Maximum interval for periodic RA messages	Enter the maximum interval (in seconds) for periodic Router Advertisement messages. The interval range is from 4 to 1800.
Minimum interval for periodic RA messages	Enter the minimum interval (in seconds) for periodic Router Advertisement messages. The interval range is from 4 to 1800.

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

3 Select or enter the DHCP configuration information.

4 Enter the maximum and minimum intervals for RA messages.

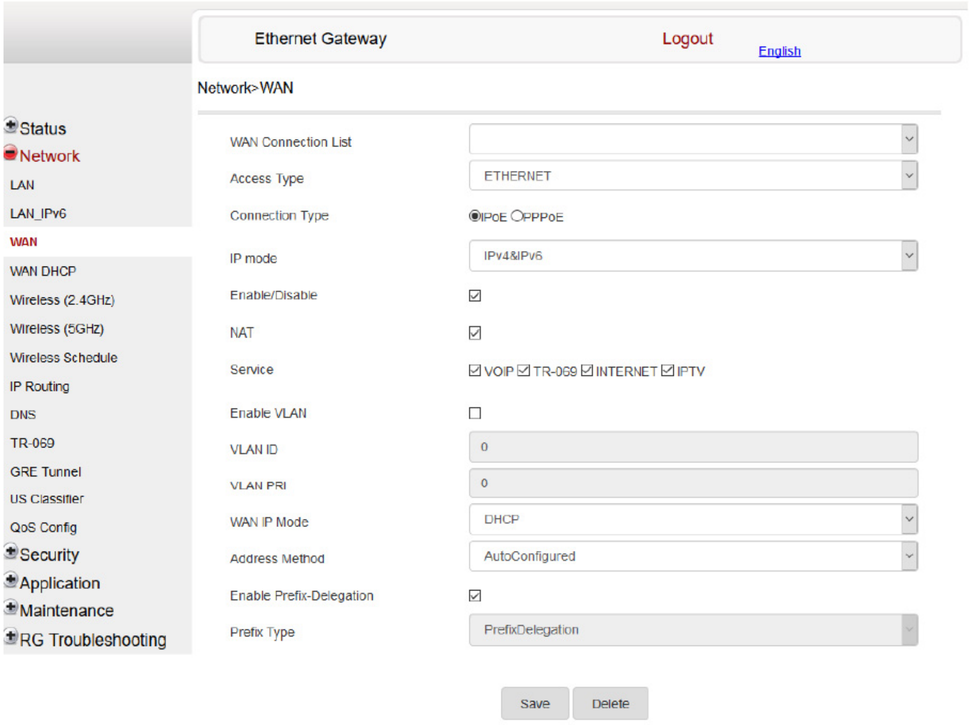
5 Click Save/Apply.

6 STOP. This procedure is complete.

Procedure 16 WAN networking configuration

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

Figure 20 WAN network window



Network>WAN

WAN Connection List	
Access Type	ETHERNET
Connection Type	● IPoE ○ PPPoE
IP mode	IPv4&IPv6
Enable/Disable	☑
NAT	☑
Service	☑ VOIP ☑ TR-069 ☑ INTERNET ☑ IPTV
Enable VLAN	□
VLAN ID	0
VLAN PRI	0
WAN IP Mode	DHCP
Address Method	AutoConfigured
Enable Prefix-Delegation	☑
Prefix Type	PrefixDelegation

Table 21 describes the fields in the WAN network window.

Table 21 WAN network parameters

Field	Description
WAN Connection List	Choose a WAN connection from the drop-down menu to set the connection parameters
Access Type	Choose an access type, for example Ethernet
Connection Type	Choose a connection type: IPoE or PPPoE
IP mode	Choose an IP mode from the drop-down menu: IPv4 or IPv6
Enable/Disable	Select this checkbox to enable the WAN connection
NAT	Select this checkbox to enable NAT
Service	Select the checkboxes to enable service types for this connection: VoIP, TR-069, Internet, IPTV

(1 of 2)

Field	Description
Enable VLAN	Select this checkbox to enable VLAN
VLAN ID	Enter the VLAN ID
VLAN PRI	Enter the VLAN PRI
WAN IP Mode	Choose an IP mode from the drop-down menu
Address Method	Choose an address method from the drop-down menu; for example, AutoConfigured
Enable Prefix Delegation	Select this checkbox to enable prefix delegation
Prefix Type	Displays the prefix type

(2 of 2)

2 Configure a specific WAN connection.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 17 WAN DHCP configuration

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

Figure 21 WAN DHCP window

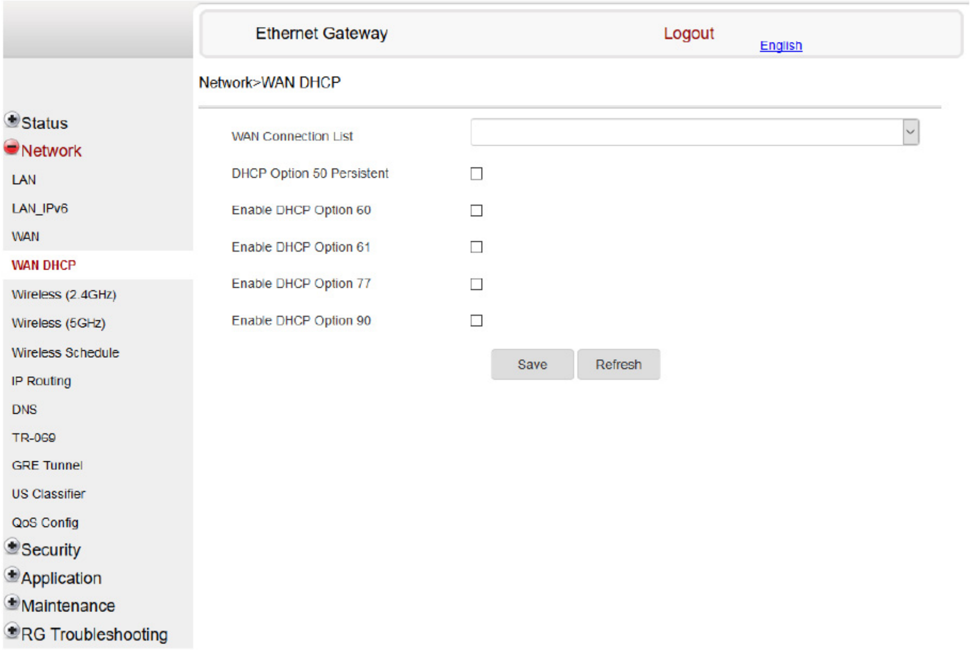


Table 22 describes the fields in the WAN DHCP window.

Table 22 WAN DHCP parameters

Field	Description
WAN Connection List	Choose a WAN connection from the drop-down menu
DHCP Option 50 Persistent	Select this checkbox to enable DHCP Option 50 persistent
Enable DHCP Option 60	Select this checkbox to enable DHCP Option 60 (vendor class identifier)
Enable DHCP Option 61	Select this checkbox to enable DHCP Option 61 (client identifier)
Enable DHCP Option 77	Select this checkbox to enable DHCP Option 77
Enable DHCP Option 90	Select this checkbox to enable DHCP Option 90

2 Configure a WAN DHCP option.

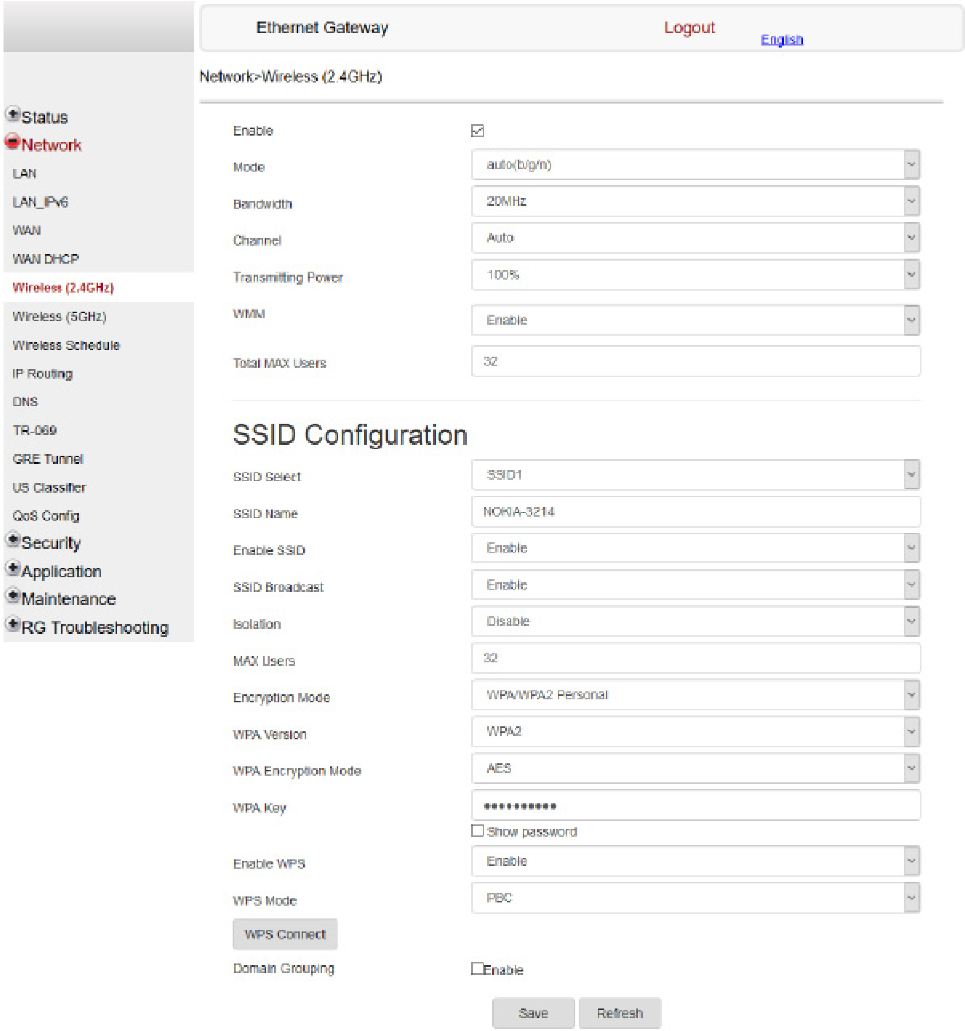
3 Click Save.

4 STOP. This procedure is complete.

Procedure 18 WiFi 2.4G networking configuration

1 Select Network > WiFi 2.4G from the top-level menu in the Ethernet Gateway window, as shown in Figure 22.

Figure 22 WiFi 2.4G network window



Network>Wireless (2.4GHz)

Enable	☑
Mode	auto(b/g/n)
Bandwidth	20MHz
Channel	Auto
Transmitting Power	100%
WMM	Enable
Total MAX Users	32

SSID Configuration

SSID Select	SSID1
SSID Name	NOKIA-3214
Enable SSID	Enable
SSID Broadcast	Enable
Isolation	Disable
MAX Users	32
Encryption Mode	WPA/WPA2 Personal
WPA Version	WPA2
WPA Encryption Mode	AES
WPA Key	•••••••••• ☐ Show password
Enable WPS	Enable
WPS Mode	PBC
Domain Grouping	☐ Enable

Table 23 describes the fields in the WiFi 2.4G network window.

Table 23 **WiFi 2.4G network parameters**

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

(1 of 2)

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

(2 of 2)

Notes

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

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

2 Configure the WiFi connection.

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

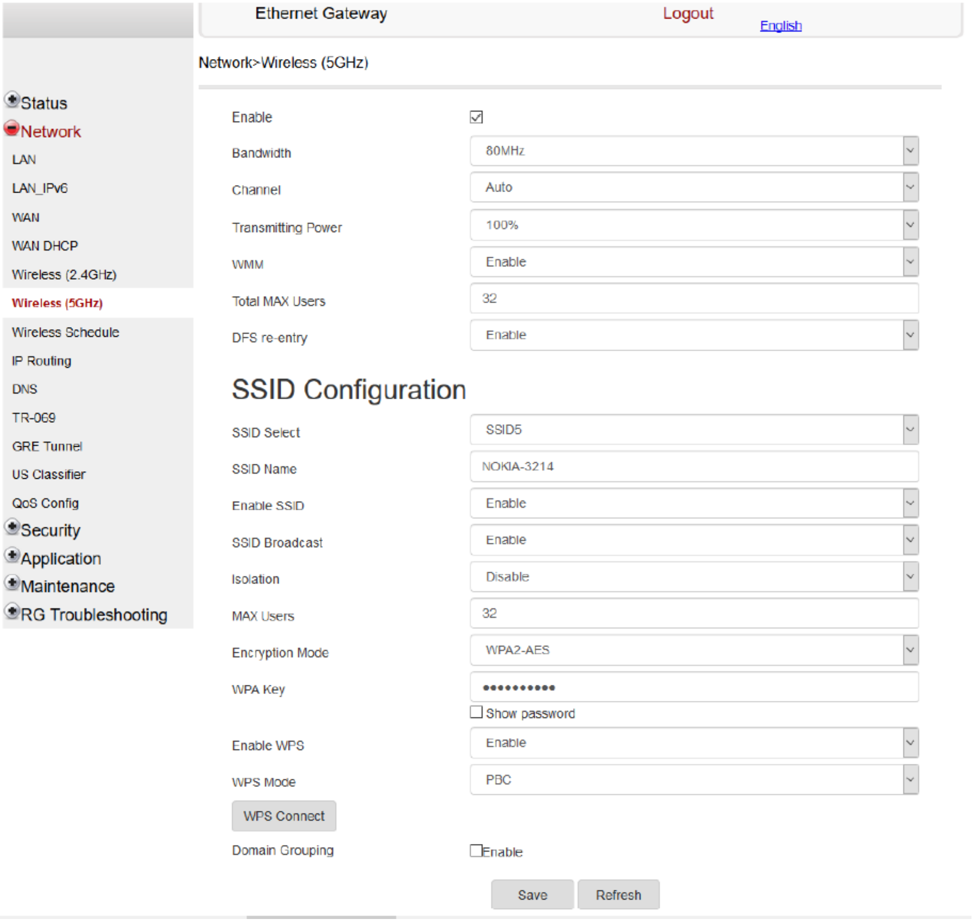
4 Click Save.

5 STOP. This procedure is complete.

Procedure 19 WiFi 5G networking configuration

1 Select Network > WiFi 5G from the top-level menu in the Ethernet Gateway window, as shown in Figure 23.

Figure 23 WiFi 5G network window



Network>Wireless (5GHz)

Enable ☑

Bandwidth 80MHz

Channel Auto

Transmitting Power 100%

WMM Enable

Total MAX Users 32

DFS re-entry Enable

SSID Configuration

SSID Select SSID5

SSID Name NOKIA-3214

Enable SSID Enable

SSID Broadcast Enable

Isolation Disable

MAX Users 32

Encryption Mode WPA2-AES

WPA Key ••••••••••

□ Show password

Enable WPS Enable

WPS Mode PBC

Domain Grouping □Enable

Table 24 describes the fields in the WiFi 5G network window.

Table 24 WiFi 5G network parameters

Field	Description
Enable	Select this checkbox to enable WiFi

(1 of 2)

Field	Description
Bandwidth	Choose from: • 20 MHz • 40 MHz • 80 MHz
Channel	Choose a channel from the drop-down menu or choose Auto to have the channel automatically assigned
Transmitting Power	Choose a percentage for the transmitting power from the drop-down menu: • Low (20%) • Medium (40%) • High (60%) • Maximum (100%)
WMM	Choose Enable or Disable from the drop-down menu to enable or disable WiFi multi-media
Total MAX Users	Enter the total number of MAX users
DFS re-entry	Choose Enable or Disable from the drop-down menu to enable or disable DFS re-entry
SSID Configuration	
SSID Select	Choose the SSID from the drop-down menu
SSID Name	Change the name of the selected SSID
Enable SSID	Choose Enable or disable SSID from this drop-down menu
SSID Broadcast	Choose Enable or disable SSID broadcast from this drop-down menu
Isolation	Choose Enable or disable isolation from this drop-down menu
MAX Users	Enter the number of MAX users
Encryption Mode	Choose an encryption mode from the drop-down menu: • OPEN • WEP • WPA/WPA2 Personal • WPA/WPA2 Enterprise (1) (2)
WPA Key	Enter the WPA key
Enable WPS	Choose Enable or disable WPS from this drop-down menu
WPS Mode	Choose a WPS mode from the drop-down menu: PBC (Push Button Connect) or PIN (Personal Identification Number)
Domain Grouping	Choose Enable or disable domain grouping from this drop-down menu

(2 of 2)

Notes

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

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

2 Configure the WiFi connection.

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

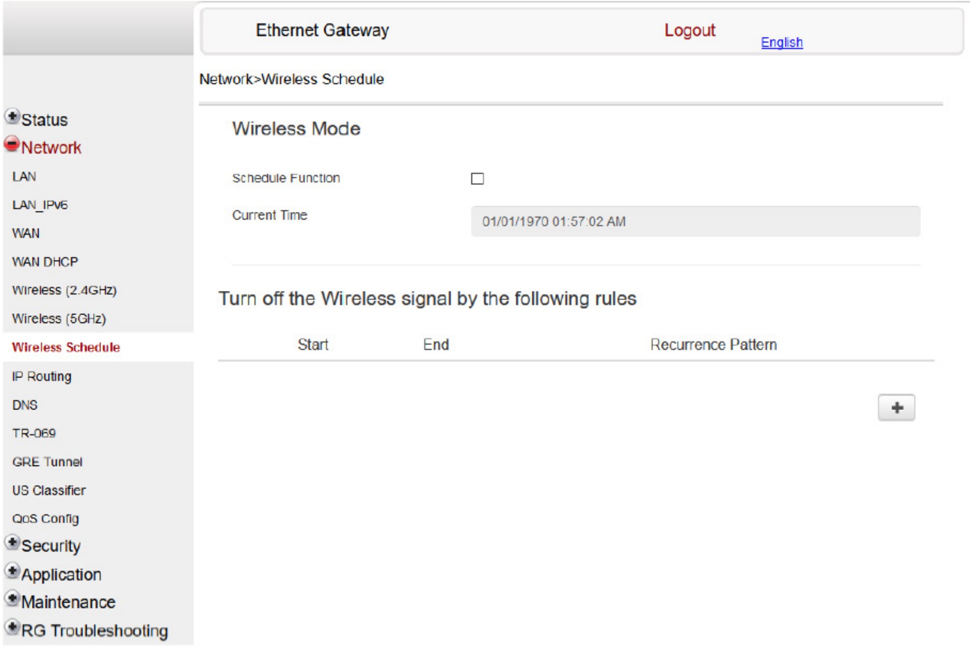
4 Click Save.

5 STOP. This procedure is complete.

Procedure 20 Wireless scheduling

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

Figure 24 **Wireless Schedule window**



Wireless Mode

Schedule Function □

Current Time 01/01/1970 01:57:02 AM

Turn off the Wireless signal by the following rules

Start	End	Recurrence Pattern

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

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

A separate panel displays for configuring wireless schedule rules.

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

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

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

The Recurrence Pattern shows the rules created to date.

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

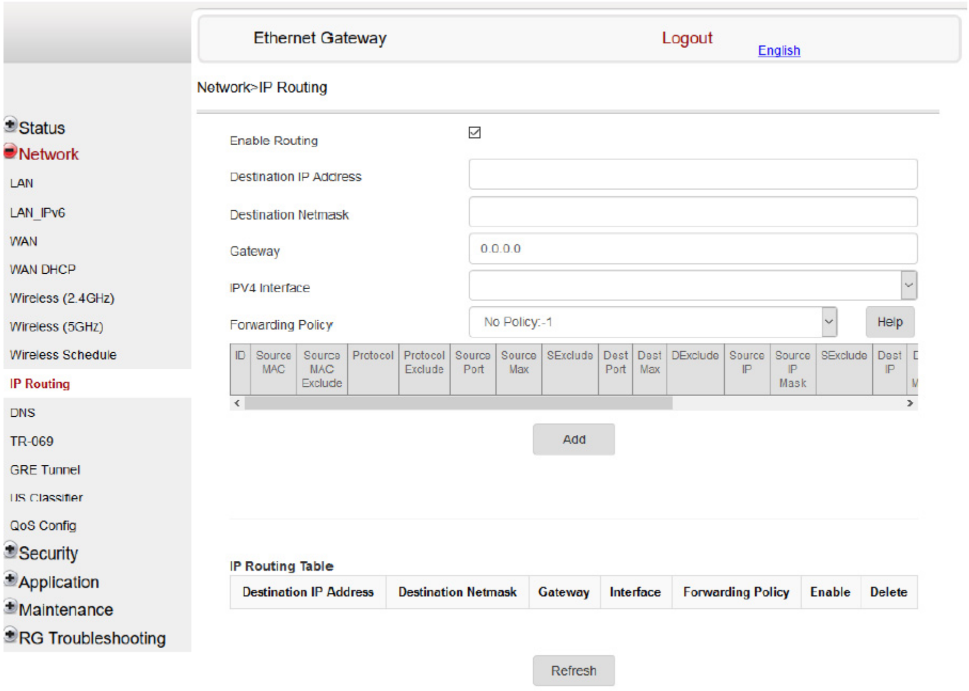
8 Click Save Changes.

9 STOP. This procedure is complete.

Procedure 21 Routing configuration

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

Figure 25 Routing network window



Network>IP Routing

Enable Routing ☑

Destination IP Address

Destination Netmask

Gateway 0.0.0.0

IPV4 Interface

Forwarding Policy No Policy:-1

ID	Source MAC	Source MAC Exclude	Protocol	Protocol Exclude	Source Port	Source Max	SExclude	Dest Port	Dest Max	DExclude	Source IP	Source IP Mask	SExclude	Dest IP	D M

IP Routing Table

Destination IP Address	Destination Netmask	Gateway	Interface	Forwarding Policy	Enable	Delete

Table 25 describes the fields in the Routing network window.

Table 25 Routing network parameters

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

2 Enter the routing information.

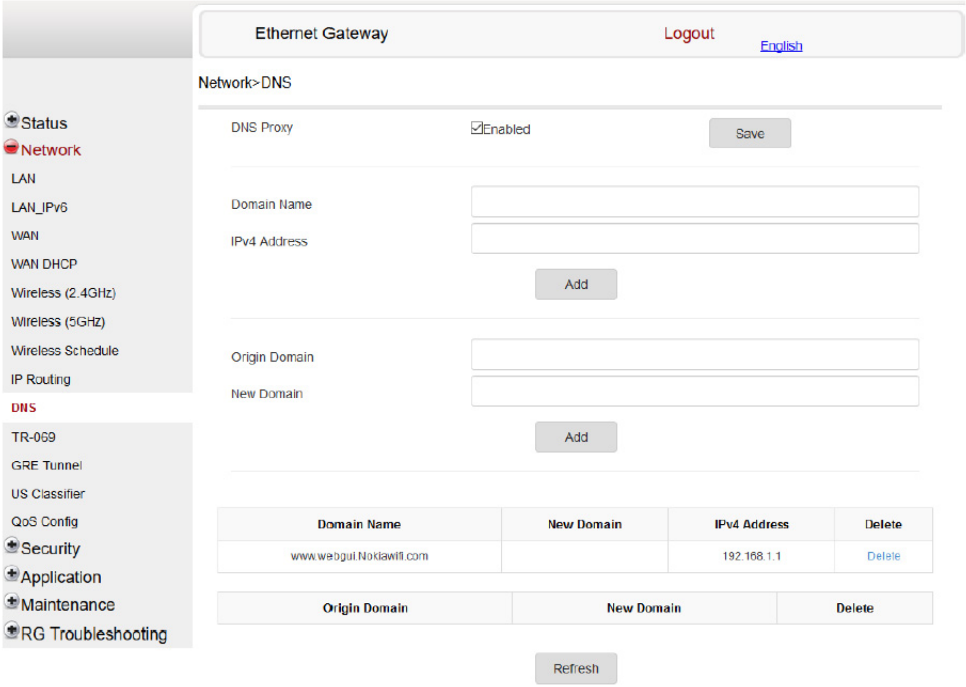
3 Click Add.

4 STOP. This procedure is complete.

Procedure 22 DNS configuration

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

Figure 26 DNS network window



DNS Proxy ☑Enabled

Domain Name

IPv4 Address

Origin Domain

New Domain

Domain Name	New Domain	IPv4 Address	Delete
www.webgui.Nokiawifi.com		192.168.1.1	Delete

Origin Domain	New Domain	Delete

Table 26 describes the fields in the DNS network window.

Table 26 DNS network parameters

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

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

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

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

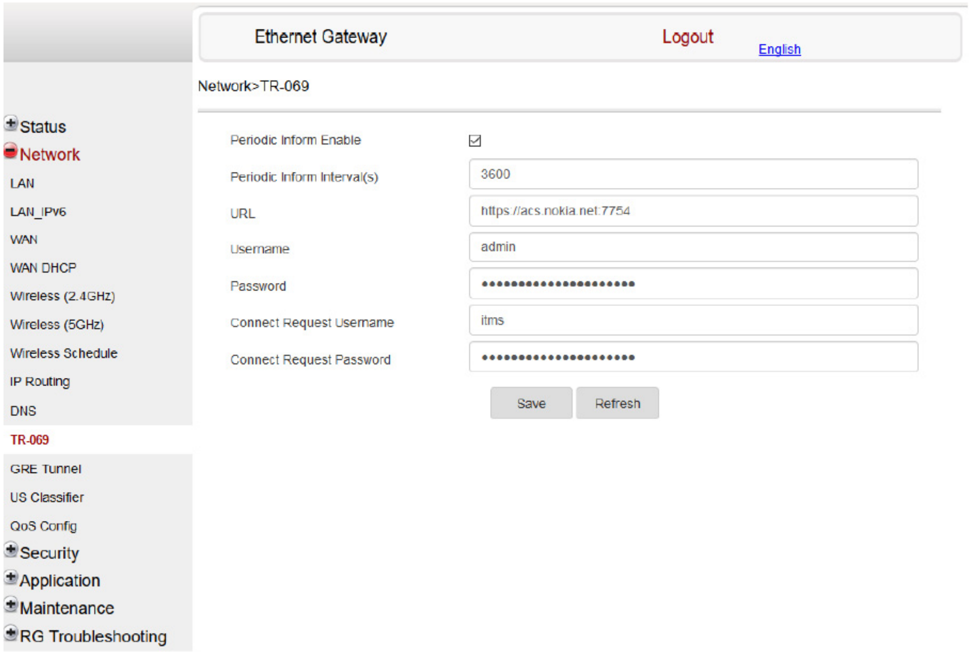
5 STOP. This procedure is complete.

Procedure 23 TR-069 configuration

Note — You need to have administrator (SuperAdmin) account privileges for TR-069 configuration; a user account (userAdmin) does not provide access to this procedure.

1 Select Network > TR-069 from the top-level menu in the Ethernet Gateway window, as shown in Figure 27.

Figure 27 **TR-069 network window**



Network>TR-069

Periodic Inform Enable ☑

Periodic Inform Interval(s) 3600

URL https://acs.nokia.net:7754

Username admin

Password •••••••••••••••••••••

Connect Request Username itms

Connect Request Password •••••••••••••••••••••

Table 27 describes the fields in the TR-069 network window.

Table 27 **TR-069 network parameters**

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

2 Configure TR-069 by entering the required information.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 24 QoS configuration

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

Figure 28 shows the window for configuring QoS L2 (Layer 2 packet sizes).

Figure 28 QoS Config window (L2)

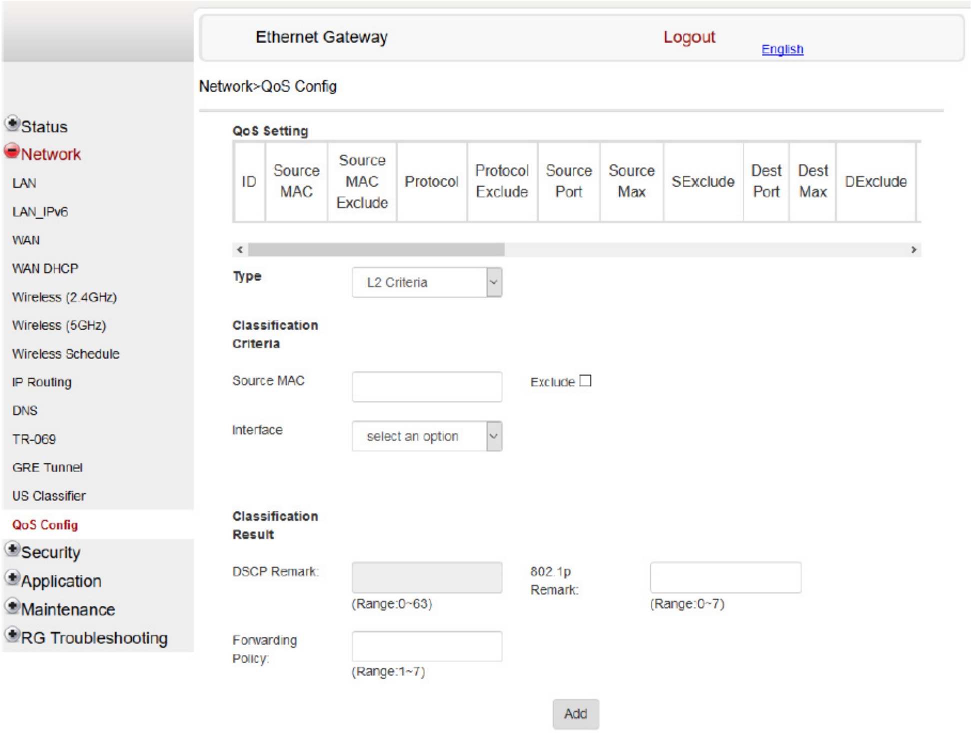


Table 28 describes the fields in the QoS Config window.

Table 28 QoS Config parameters

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

(1 of 2)

Field	Description
Destination IP and Destination IP Mask	Enter the values for the destination IP and IP mask, or select the Exclude checkbox
Source Port and Source Port Max	Enter the values for the source port and port max (highest port number) or select the Exclude checkbox
Destination Port and Destination Port Max	Enter the values for the destination port and port max (highest port number), or select the Exclude checkbox

(2 of 2)

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

3 Configure a QoS policy.

4 Click Add to add a QoS policy.

5 STOP. This procedure is complete.

8.2.4 Security configuration

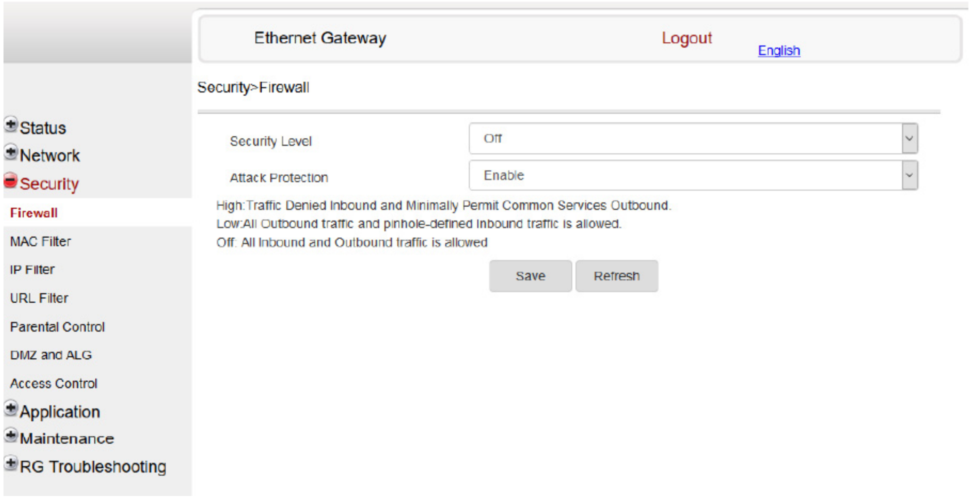
HA-140W-B CPEs support security configuration, including:

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

Procedure 25 Firewall configuration

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

Figure 29 **Firewall window**



Security Level: Off

Attack Protection: Enable

High:Traffic Denied Inbound and Minimally Permit Common Services Outbound.
Low:All Outbound traffic and pinhole-defined inbound traffic is allowed.
Off: All Inbound and Outbound traffic is allowed

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

High—Traffic denied inbound and minimally permit common services outbound

Low—All outbound traffic and pinhole-defined inbound traffic is allowed

Off—All inbound and outbound traffic is allowed

Table 29 describes the fields in the firewall window.

Table 29 **Firewall parameters**

Field	Description
Security Level	Choose the security level from the drop-down menu: High, Low, Off, or Advanced
Attack Protection (Protection against DoS or DDoS attacks)	Choose Enable or Disable attack protection from the drop-down menu. The default is Enable.

2 Configure the firewall.

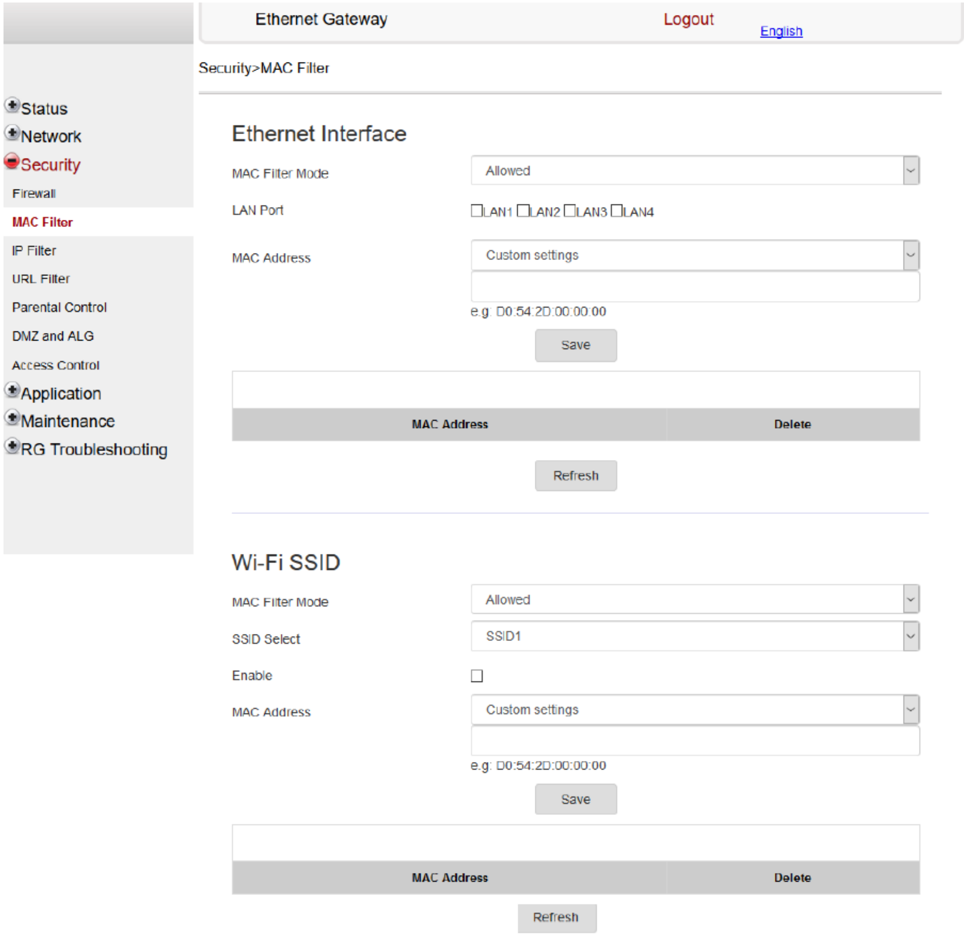
3 Click Save.

4 STOP. This procedure is complete.

Procedure 26 MAC filter configuration

1 Select Security > Mac Filter from the top-level menu in the Ethernet Gateway window, as shown in Figure 30.

Figure 30 **MAC filter window**



Ethernet Interface

MAC Filter Mode: Allowed

LAN Port: □LAN1 □LAN2 □LAN3 □LAN4

MAC Address: Custom settings

e.g. D0:54:2D:00:00:00

Wi-Fi SSID

MAC Filter Mode: Allowed

SSID Select: SSID1

Enable: □

MAC Address: Custom settings

e.g. D0:54:2D:00:00:00

Table 30 describes the fields in the MAC filter window.

Table 30 **MAC filter parameters**

Field	Description
Ethernet Interface	
MAC Filter Mode	Choose the MAC filter mode from the drop-down menu: Blocked or Allowed
LAN Port	LAN port range
MAC Address	Choose a MAC address from the drop-down menu or enter the address in the text field
Wi-Fi SSID	
MAC Filter Mode	Choose the MAC filter mode from the drop-down menu: Blocked or Allowed
SSID Select	Choose the SSID from the drop-down menu
Enable	Select this checkbox to enable the MAC filter
MAC Address	Choose a MAC address from the drop-down menu or enter the address in the text field

2 Click Refresh to update the information.

3 Configure a MAC filter.

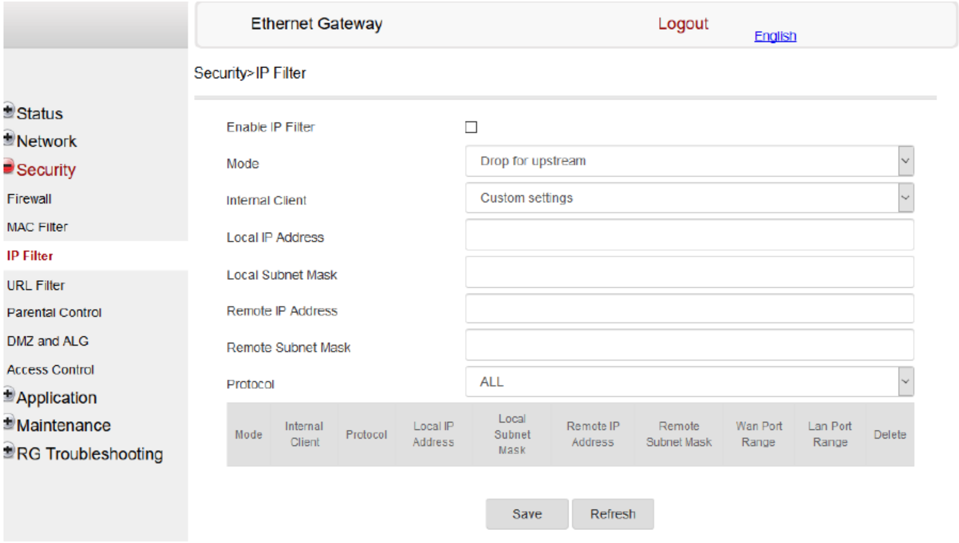
4 Click Add.

5 STOP. This procedure is complete.

Procedure 27 IP filter configuration

1 Select Security > IP filter from the top-level menu in the Ethernet Gateway window, as shown in Figure 31.

Figure 31 IP filter window



Security>IP Filter

Enable IP Filter ☐

Mode: Drop for upstream

Internal Client: Custom settings

Local IP Address

Local Subnet Mask

Remote IP Address

Remote Subnet Mask

Protocol: ALL

Table 31 describes the fields in the IP filter window. If the firewall level is not set to advanced, the IP filter rules are not available.

Table 31 IP filter parameters

Field	Description
Enable IP Filter	Select this checkbox to enable 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.

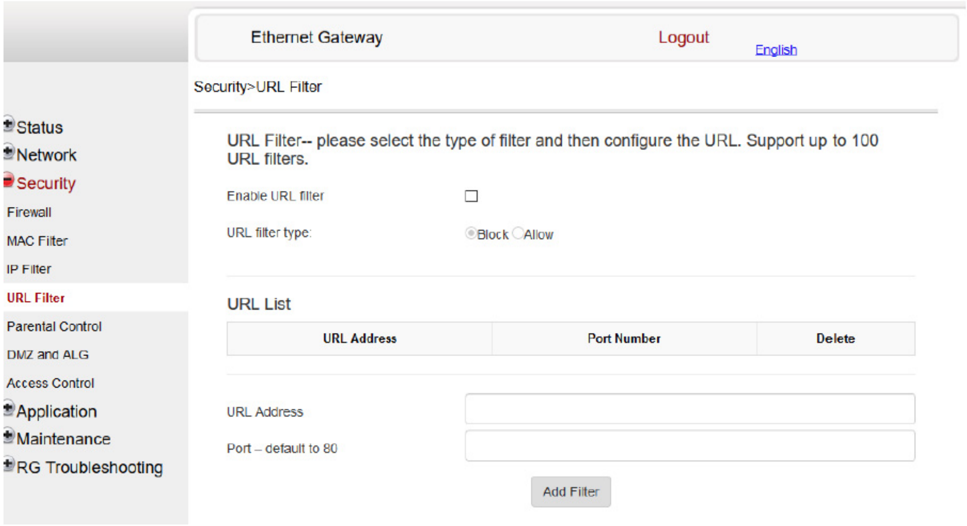
3 Click Add.

4 STOP. This procedure is complete.

Procedure 28 URL filter configuration

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

Figure 32 **URL Filter window**



Security>URL Filter

URL Filter-- please select the type of filter and then configure the URL. Support up to 100 URL filters.

Enable URL filter □

URL filter type: ● Block ○ Allow

URL List

URL Address	Port Number	Delete

URL Address

Port – default to 80

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

Table 32 describes the fields in the URL Filter window.

Table 32 **URL Filter parameters**

Field	Description
Enable URL filter	Select the checkbox to enable the URL filter

(1 of 2)

Field	Description
URL filter type	Select the radio button to block the URL or allow the URL
URL List	
URL Address	Type the URL address
Port - default to 80	Type the port number; the default is 80

(2 of 2)

2 Configure the URL Filter.

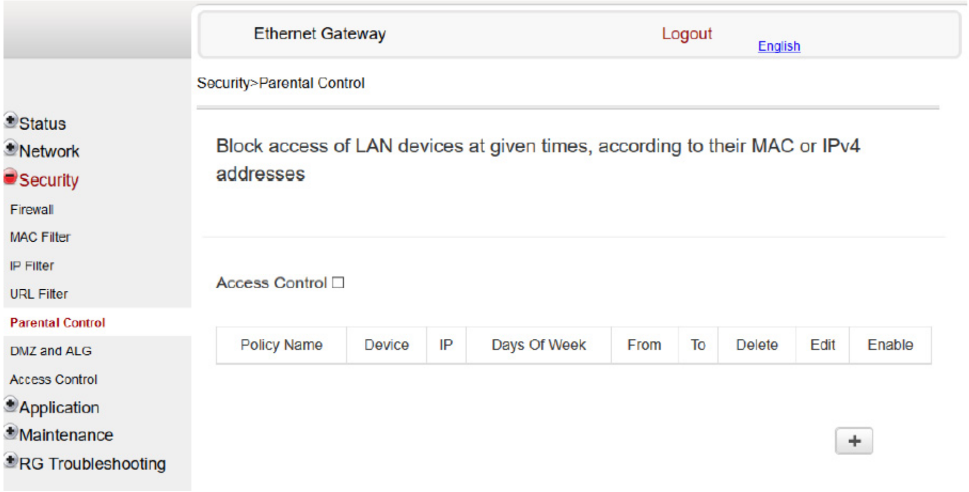
3 Click Add Filter.

4 STOP. This procedure is complete.

Procedure 29 Parental control

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

Figure 33 **Parental Control window**



Block access of LAN devices at given times, according to their MAC or IPv4 addresses

Access Control □

Policy Name	Device	IP	Days Of Week	From	To	Delete	Edit	Enable

Table 33 describes the fields in the Parental Control window.

Table 33 **Parental control parameters**

Field	Description
Access Control	Select this checkbox to enable access control
Add Access Control rule	
Policy Name	Enter a name for the parental control policy or choose a policy from the list
Device	Enter the device or choose one from the list
IP	Enter the IPv4 address for the device or choose an IPv4 address from the list
Days of week	Choose Every Day, or Individual Days and select the checkboxes for the days of the week for which the policy applies
From	Enter the times for the policy to be in effect
To	

2 Select the Access Control checkbox.

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

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

4 Configure the parental control policy.

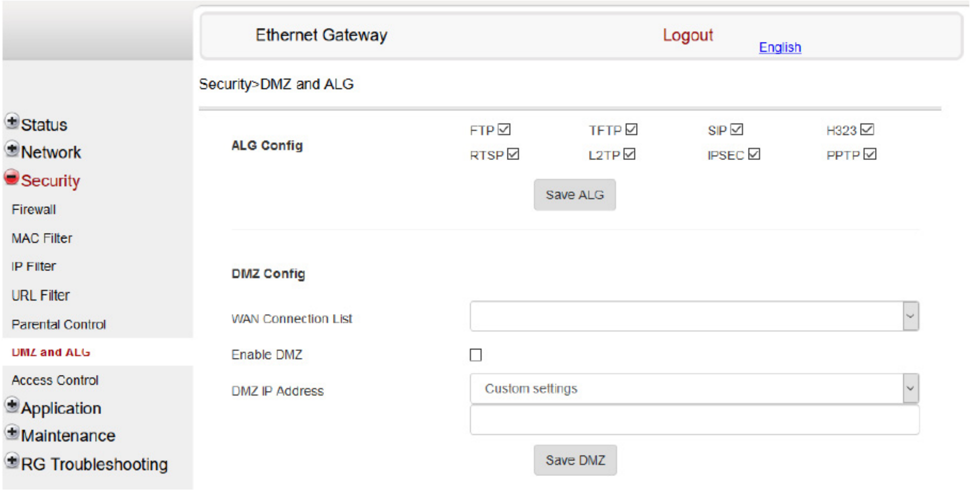
5 Click Enable to activate the policy.

6 STOP. This procedure is complete.

Procedure 30 DMZ and ALG configuration

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

Figure 34 DMZ and ALG window



ALG Config
FTP ☑ TFTP ☑ SIP ☑ H323 ☑
RTSP ☑ L2TP ☑ IPSEC ☑ PPTP ☑

DMZ Config
WAN Connection List
Enable DMZ ☐
DMZ IP Address Custom settings

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

Table 34 DMZ and ALG parameters

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

2 Configure ALG.

3 Click Save ALG.

4 Configure DMZ.

5 Click Save DMZ.

6 STOP. This procedure is complete.

Procedure 31 Access control configuration

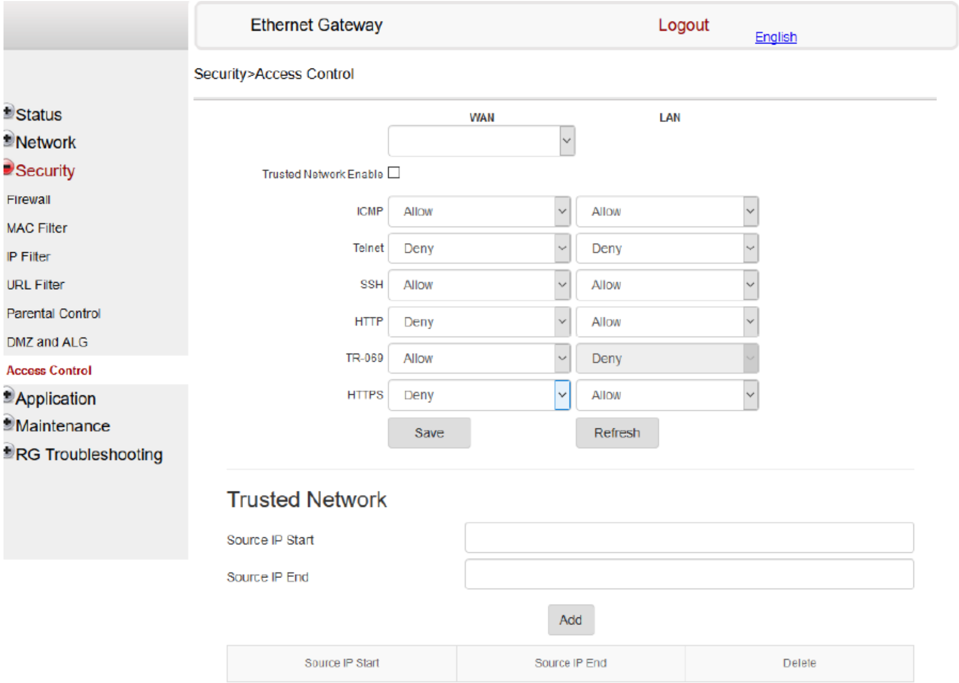
This procedure describes how to configure the access control level (ACL).

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 35.

Figure 35 **Access Control window**



Security>Access Control

Trusted Network Enable ☐

	WAN	LAN
ICMP	Allow	Allow
Telnet	Deny	Deny
SSH	Allow	Allow
HTTP	Deny	Allow
TR-069	Allow	Deny
HTTPS	Deny	Allow

Trusted Network

Source IP Start

Source IP End

Source IP Start	Source IP End	Delete

Table 35 describes the fields in the Access Control window.

Table 35 **Access control parameters**

Field	**Description**
WAN	Choose a connection from the drop-down menu
Trusted Network Enable	Click the checkbox to enable or disable
ICMP, 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
Trusted Network	
Source IP Start	Enter a start IP address for the new subnet trusted network
Source IP End	Enter an end IP address for the new subnet trusted network

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

3 Click to enable or disable Trusted Network.

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

5 Click Save.

6 Optionally, add one or more subnet trusted networks.

The maximum number of entries is 32.

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

7 STOP. This procedure is complete.

8.2.5 Application configuration

HA-140W-B CPEs support application configuration, including:

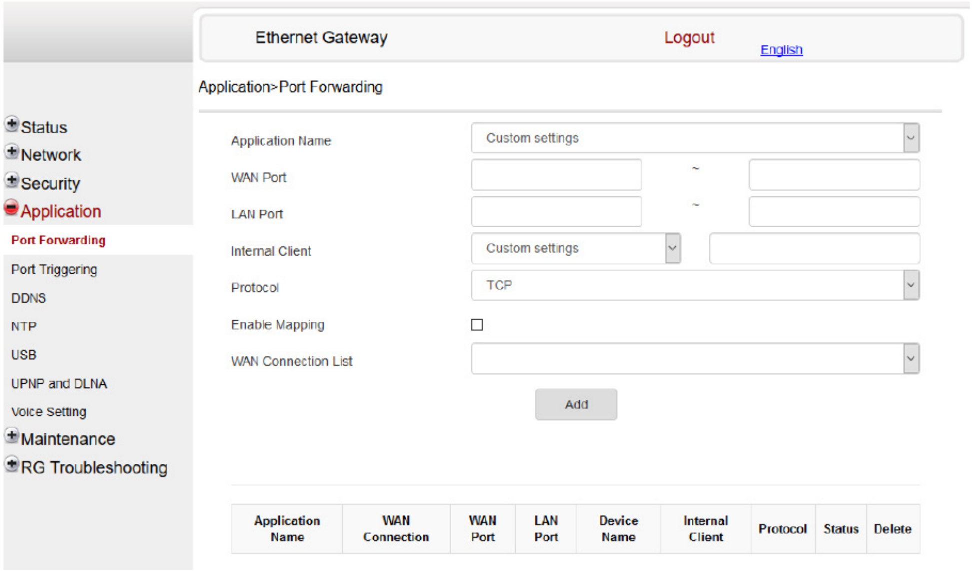
- port forwarding
- port triggering
- DDNS
- NTP
- USB

- UPnP and DLNA
- voice setting

Procedure 32 Port forwarding configuration

1 Select Application > Port forwarding from the top-level menu in the Ethernet Gateway window, as shown in Figure 36.

Figure 36 Port forwarding window



Application>Port Forwarding

Application Name: Custom settings

WAN Port: ~

LAN Port: ~

Internal Client: Custom settings

Protocol: TCP

Enable Mapping: □

WAN Connection List:

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

Table 36 describes the fields in the port forwarding window.

Table 36 Port forwarding parameters

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

(1 of 2)

Field	Description
WAN Connection List	Choose a WAN connection from the drop-down menu Note: only active devices are shown on this menu

(2 of 2)

2 Configure port forwarding.

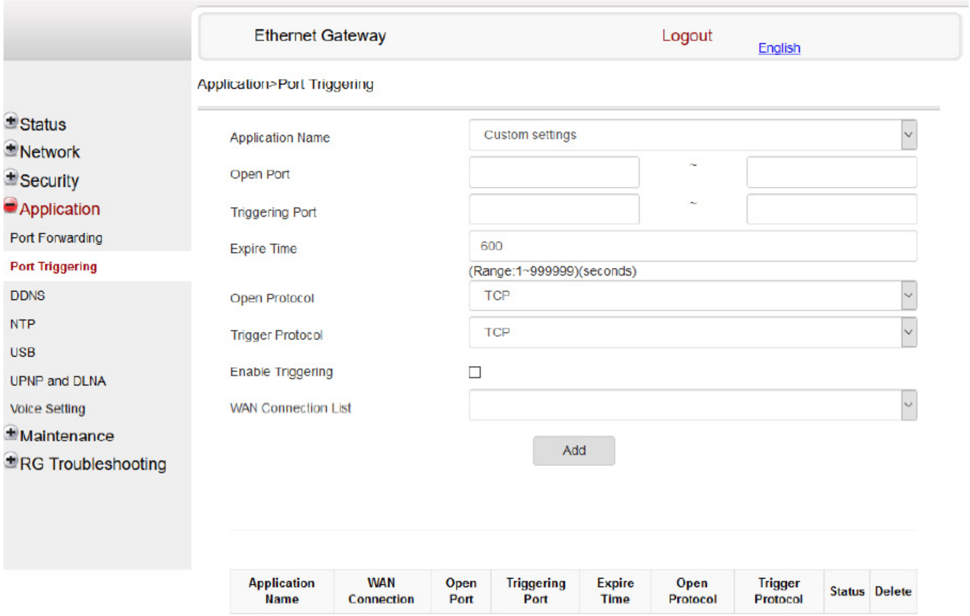
3 Click Add.

4 STOP. This procedure is complete.

Procedure 33 Port triggering

1 Select Application > Port Triggering from the top-level menu in the Ethernet Gateway window, as shown in Figure 37.

Figure 37 Port Triggering window



Application>Port Triggering

Application Name	Custom settings		
Open Port		~	
Triggering Port		~	
Expire Time	600 (Range:1~999999)(seconds)		
Open Protocol	TCP		
Trigger Protocol	TCP		
Enable Triggering	□		
WAN Connection List			

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

Table 37 describes the fields in the Port Triggering window.

Table 37 **Port triggering parameters**

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

2 Configure port triggering.

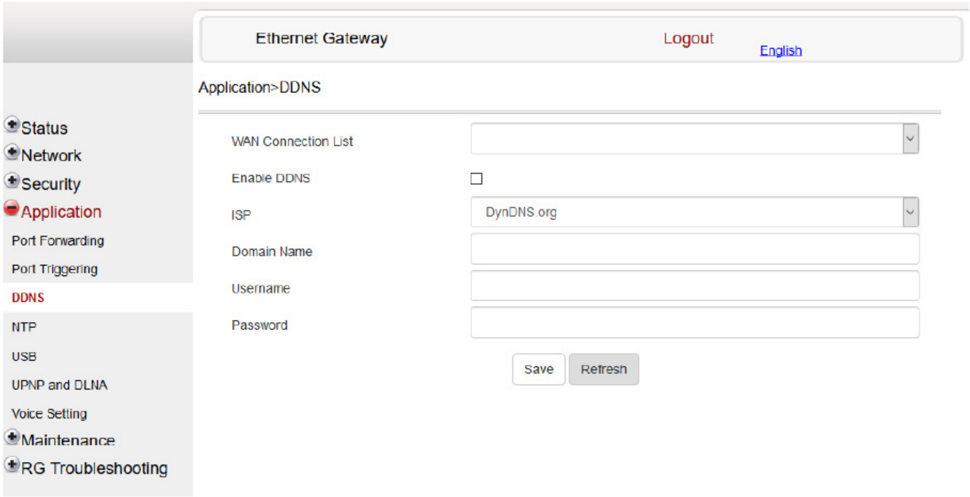
3 Click Add.

4 STOP. This procedure is complete.

Procedure 34 DDNS configuration

1 Select Application > DDNS from the top-level menu in the Ethernet Gateway window, as shown in Figure 38.

Figure 38 DDNS window



WAN Connection List

Enable DDNS □

ISP DynDNS.org

Domain Name

Username

Password

Table 38 describes the fields in the DDNS window.

Table 38 DDNS parameters

Field	Description
WAN Connection List	Choose a WAN connection from the drop-down menu
Enable DDNS	Select this checkbox to enable DDNS on the chosen WAN connection
ISP	Choose an ISP from the drop-down menu.
Domain Name	Domain name
Username	Username
Password	Password

2 Configure DDNS.

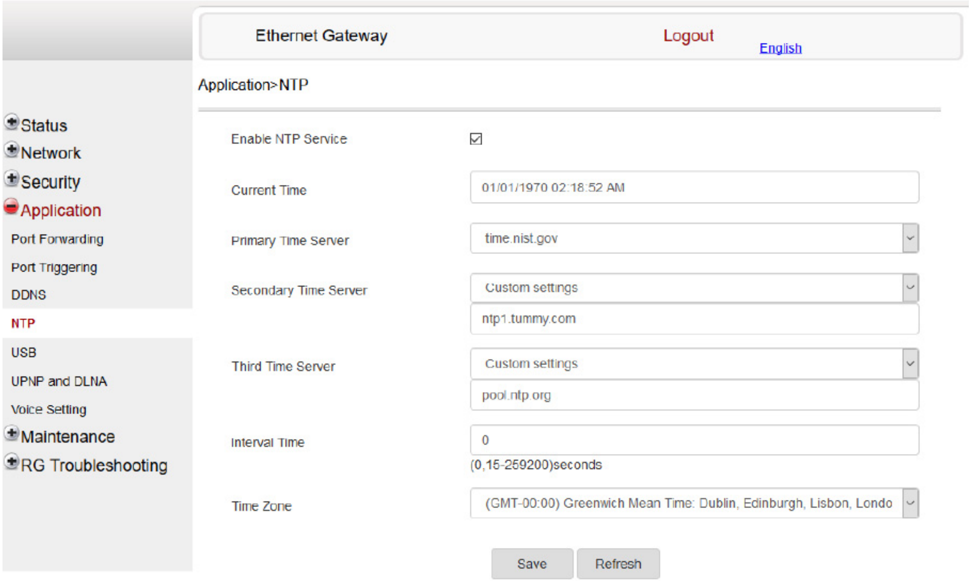
3 Click Save.

4 STOP. This procedure is complete.

Procedure 35 NTP configuration

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

Figure 39 NTP window



Enable NTP Service ☑

Current Time 01/01/1970 02:18:52 AM

Primary Time Server time.nist.gov

Secondary Time Server Custom settings ntp1.tummy.com

Third Time Server Custom settings pool.ntp.org

Interval Time 0 (0,15-259200)seconds

Time Zone (GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, Londo

Table 39 describes the fields in the NTP window.

Table 39 NTP parameters

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

2 Configure NTP.

3 Click Save.

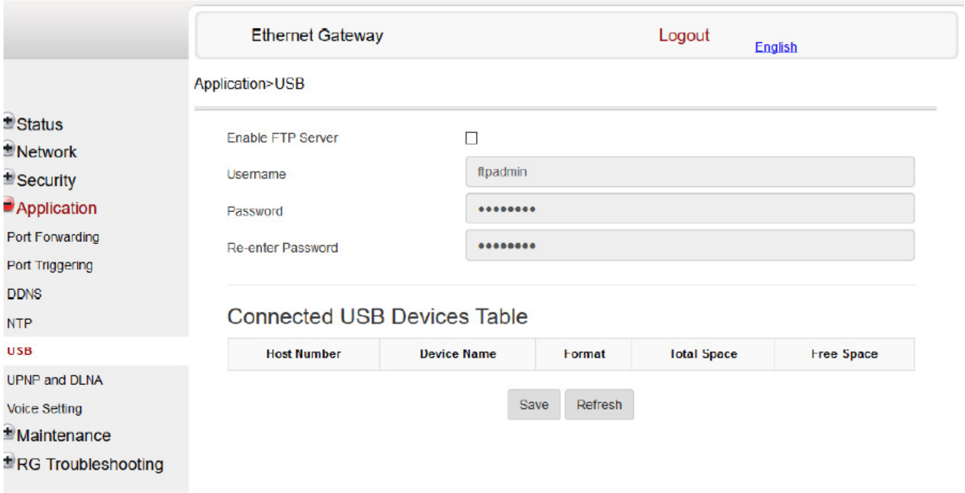
4 STOP. This procedure is complete.

Procedure 36 USB configuration

You can connect USB storage devices and USB printers to the USB ports of the device.

1 Select Application > USB from the top-level menu, as shown in Figure 40.

Figure 40 USB window



Enable FTP Server □

Username ftpadmin

Password ••••••••

Re-enter Password ••••••••

Connected USB Devices Table

Host Number	Device Name	Format	Total Space	Free Space

Table 40 describes the fields in the USB window.

Table 40 USB parameters

Field	Description
Enable FTP server	Select this checkbox to enable using an FTP server
Username	Username for the FTP server
Password	Password for the FTP server
Re-enter Password	Password for the FTP server

(1 of 2)

Field	Description
Connected USB Devices Table	For each printer that is connected to the CPE, the following fields are displayed: • Host Number—for example: Printer1, Printer2 • Device Name—name or identification for the USB device • Format—for a USB printer, the printing protocol is RAW; for a USB storage device, this field displays the storage format • Total space—applies only to a USB storage device • Free space—applies only to a USB storage device

(2 of 2)

2 Configure the USB.

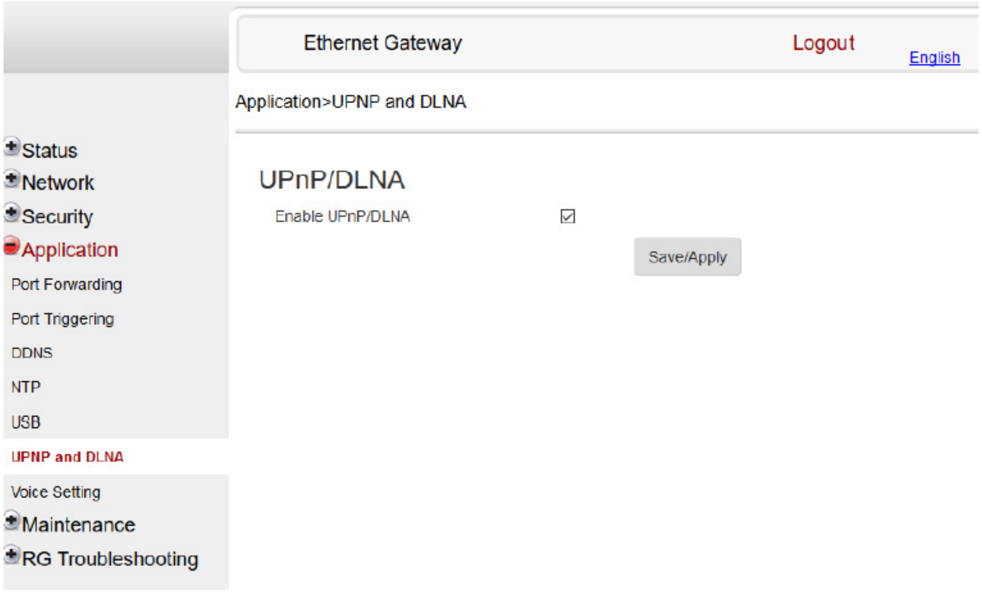
3 Click Save.

4 STOP. This procedure is complete.

Procedure 37 UPnP and DLNA configuration

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

Figure 41 UPnP and DLNA window



Enable UPnP/DLNA ☑

2 Select the Enable UPnP/DLNA checkbox to enable UPnP/DLNA.

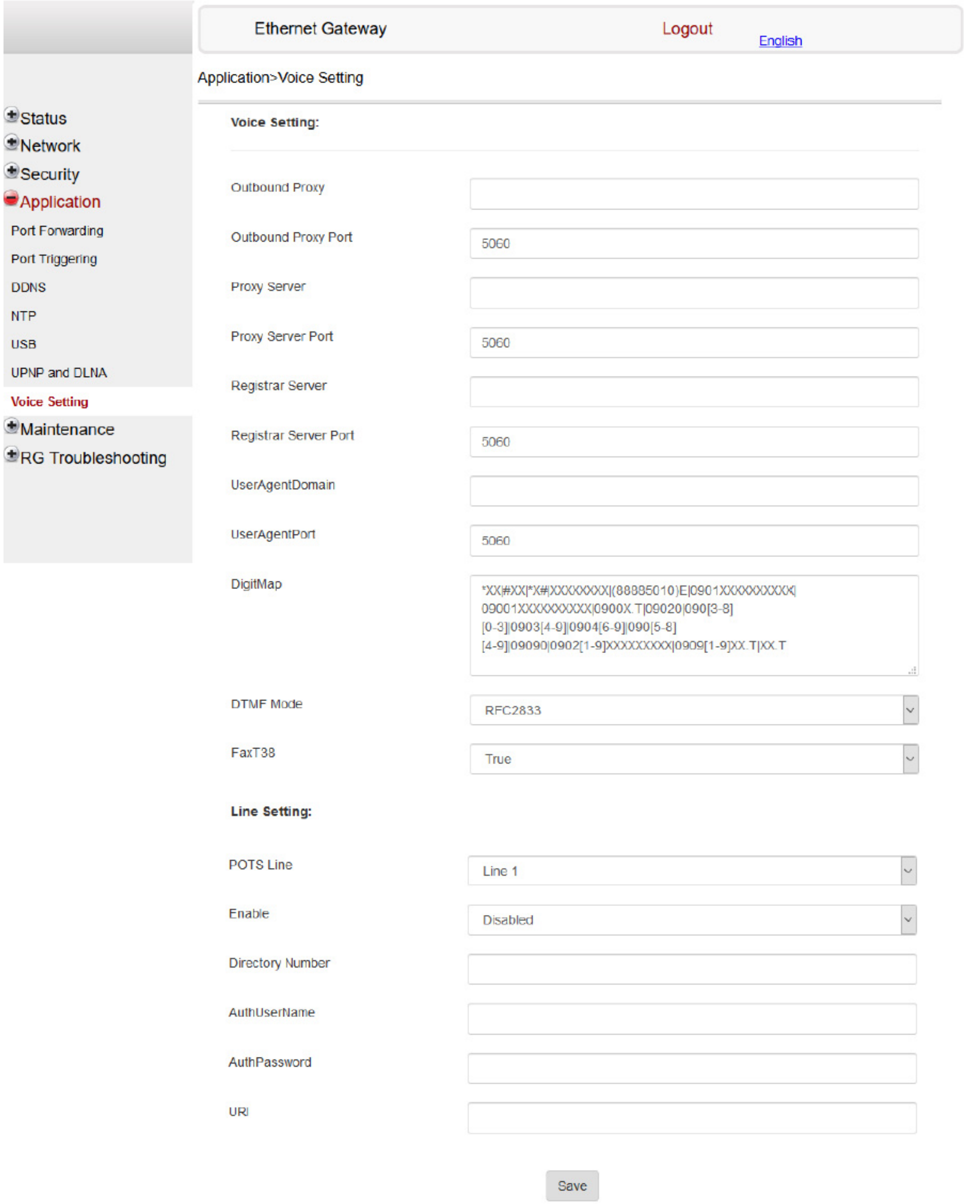
3 Click Save/Apply.

4 STOP. This procedure is complete.

Procedure 38 Voice setting

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

Figure 42 Voice setting window



Application>Voice Setting

Voice Setting:

Outbound Proxy	
Outbound Proxy Port	5060
Proxy Server	
Proxy Server Port	5060
Registrar Server	
Registrar Server Port	5060
UserAgentDomain	
UserAgentPort	5060
DigitMap	*XX|#XX|*X#|XXXXXXXX|(88885010)E|0901XXXXXXXXXX| 09001XXXXXXXXXX|0900X.T|09020|090[3-8] [0-3]|0903[4-9]|0904[6-9]|090[5-8] [4-9]|09090|0902[1-9]XXXXXXXXX|0909[1-9]XX.T|XX.T
DTMF Mode	RFC2833
FaxT38	True

Line Setting:

POTS Line	Line 1
Enable	Disabled
Directory Number	
AuthUserName	
AuthPassword	
URI	

Table 41 describes the fields in the Voice Setting window.

Table 41 **Voice setting parameters**

Field	Description
Voice Setting	
Outbound Proxy	Enter the SIP outbound proxy
Outbound Proxy Port	Enter the outbound proxy port
Proxy Server	Enter the proxy server
Proxy Server Port	Enter the proxy server port
Registrar Server	Enter the registrar server
Registrar Server Port	Enter the registrar server port
UserAgentDomain	Enter the user agent domain
UserAgentPort	Enter the user agent port
DigitMap	A string of characters with a length limit of 1024 bytes. A dial plan can consist of several dial plan tokens. Each token is a component of the overall dial plan.
DTMF Mode	Choose InBand, RFC2833 or Auto from the drop-down menu
FaxT38	Choose False or True from the drop-down menu
Line Setting	
POTS line	Choose a POTS line from the drop-down menu
Enable	Choose Enabled or Disabled from the drop-down menu
Directory Number	Enter a directory number
AuthUserName	Enter an authorized user name
AuthPassword	Enter a password for the user
URI	The Uniform Resource Identifier of the SIP URL

2 Configure voice setting.

3 Click Save.

4 STOP. This procedure is complete.

8.2.6 Maintenance

HA-140W-B CPEs support maintenance tasks, including:

- change password
- manage device

- backup and restore
- upgrade firmware
- reboot device
- restore factory defaults
- diagnose WAN connections
- view log

Procedure 39 Password configuration

A password must adhere to the password rules, which are as follows:

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

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

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

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

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

1 Select Maintenance > Password from the top-level menu in the Ethernet Gateway window, as shown in Figure 43.

Figure 43 Password window

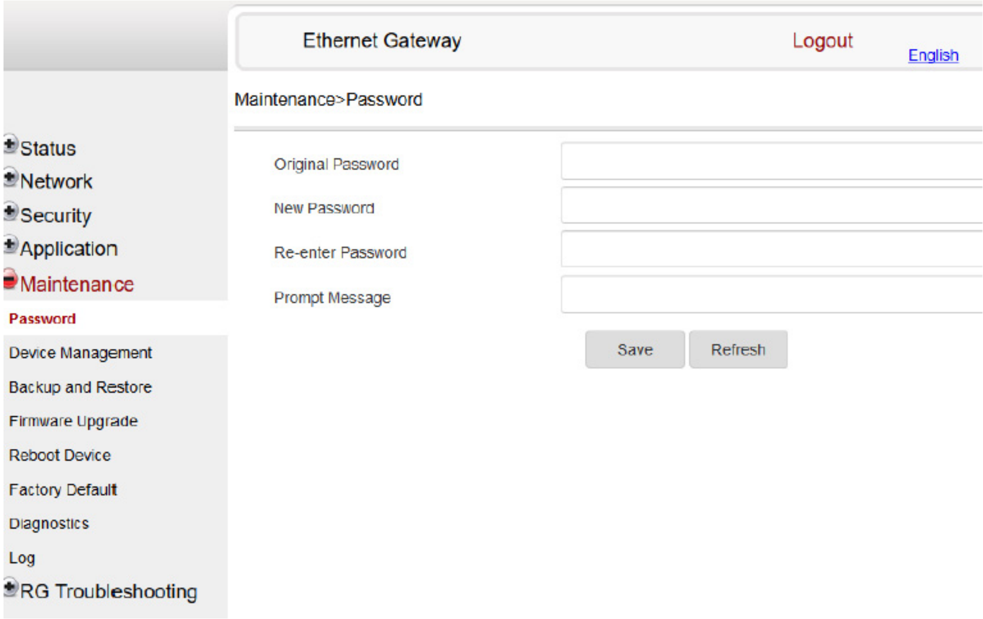


Table 42 describes the fields in the password window.

Table 42 Password parameters

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

2 Configure the new password.

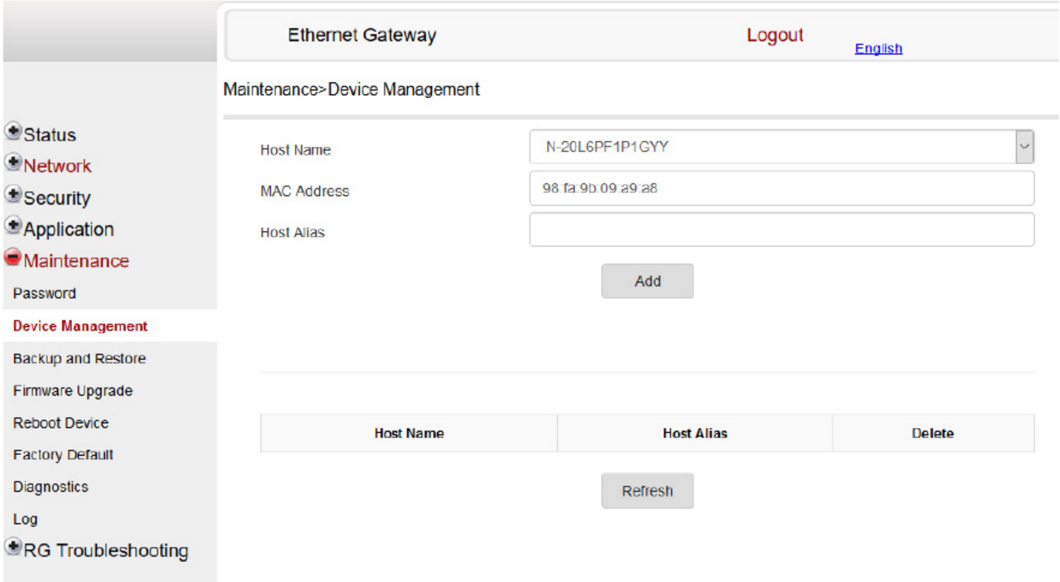
3 Click Save.

4 STOP. This procedure is complete.

Procedure 40 Device management

1 Select Maintenance > Device Management from the top-level menu in the Ethernet Gateway window, as shown in Figure 44.

Figure 44 Device management window



Maintenance>Device Management

Host Name N-20L6PF1P1GYY

MAC Address 98:fa:9b:09:a9:a8

Host Alias

Host Name	Host Alias	Delete

Table 43 describes the fields in the Device management window.

Table 43 Device management parameters

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

2 Configure an alias for a specific host.

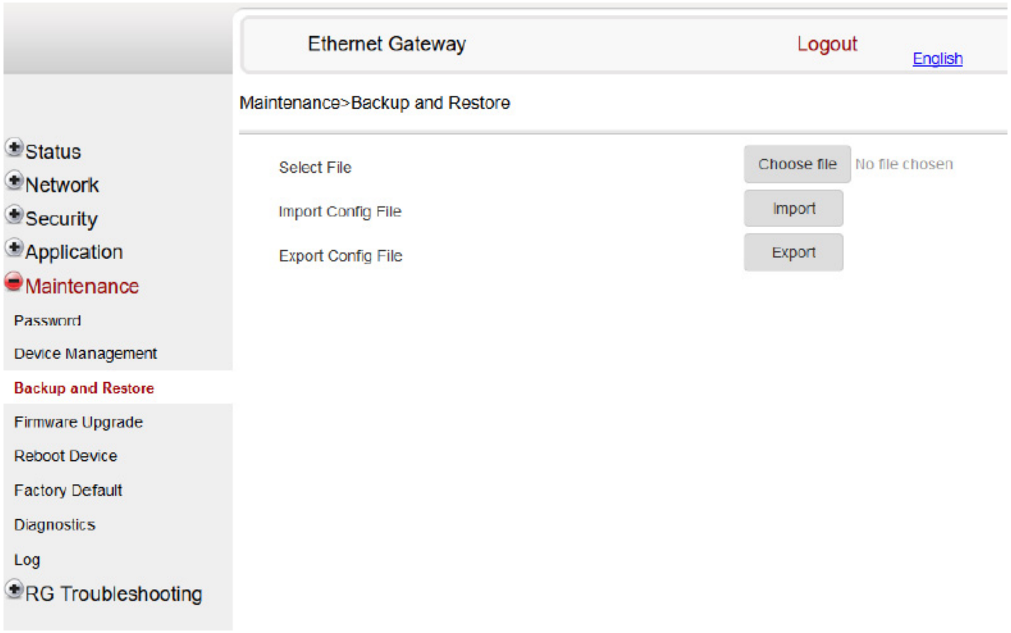
3 Click Add.

4 STOP. This procedure is complete.

Procedure 41 Backup and restore

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

Figure 45 Backup and Restore window



2 Click Choose file and select a backup file.

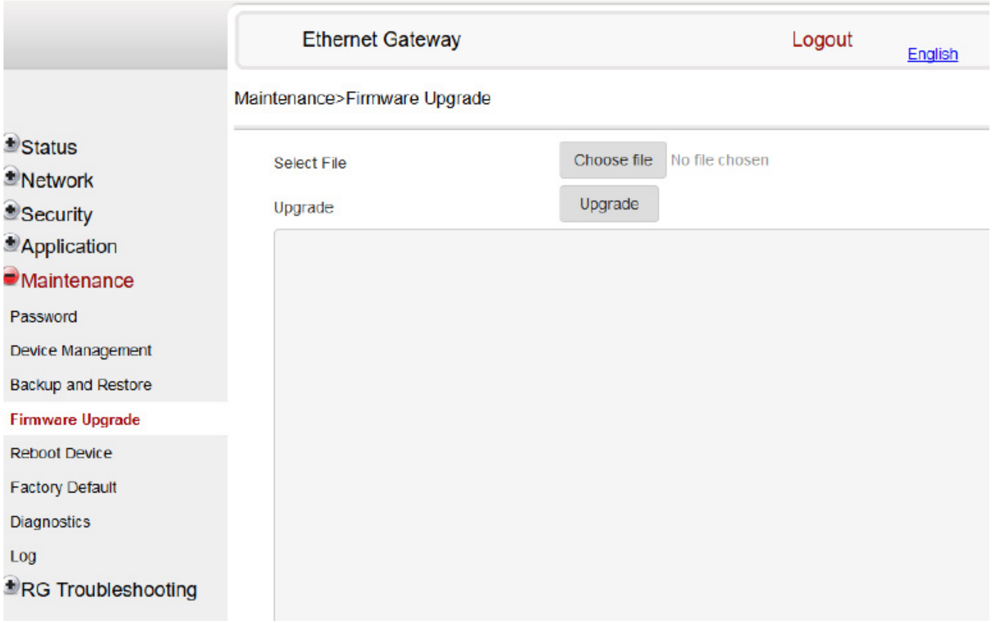
3 Click Import Config File to restore the CPE to the saved backup or click Export Config File to export the current CPE configuration to the backup file.

4 STOP. This procedure is complete.

Procedure 42 Upgrade firmware

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

Figure 46 Firmware upgrade window



2 Click Choose file and select the firmware file.

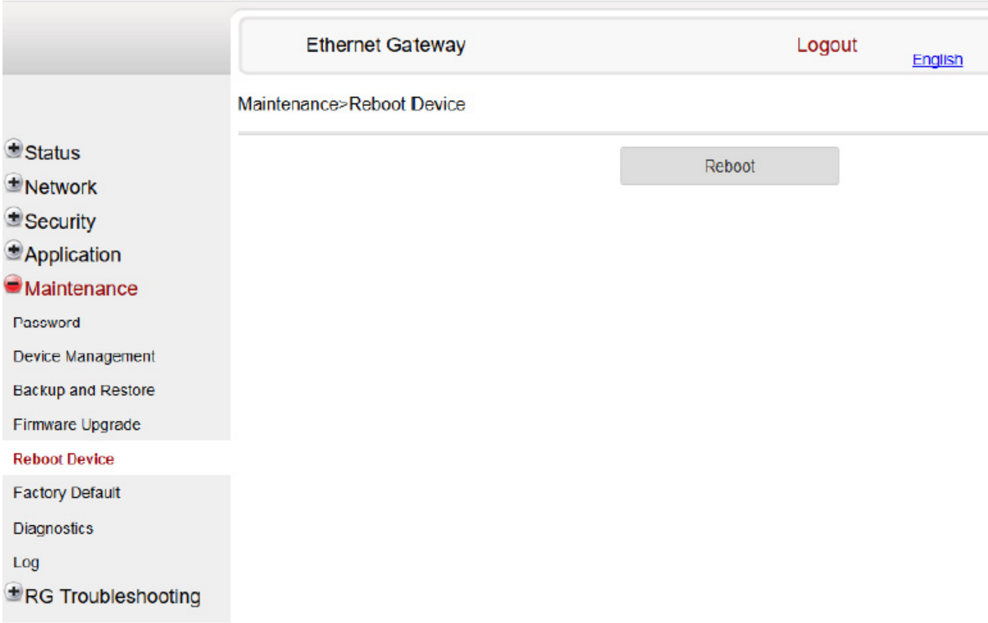
3 Click Upgrade to upgrade the firmware.

4 STOP. This procedure is complete.

Procedure 43 Reboot device

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

Figure 47 **Reboot window**



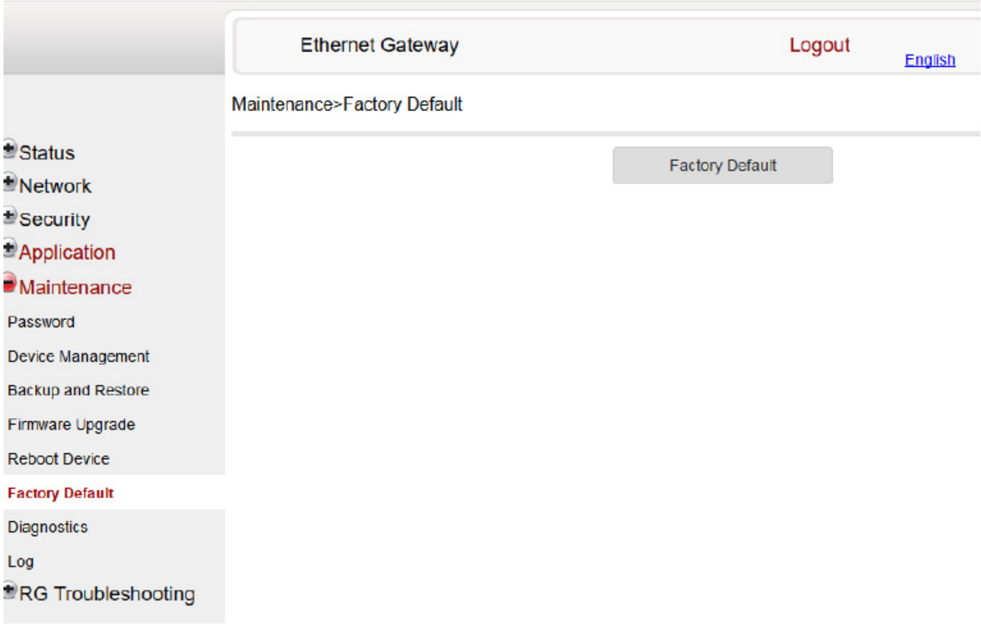
2 Click Reboot to reboot the CPE.

3 STOP. This procedure is complete.

Procedure 44 Restore factory defaults

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

Figure 48 **Factory default window**



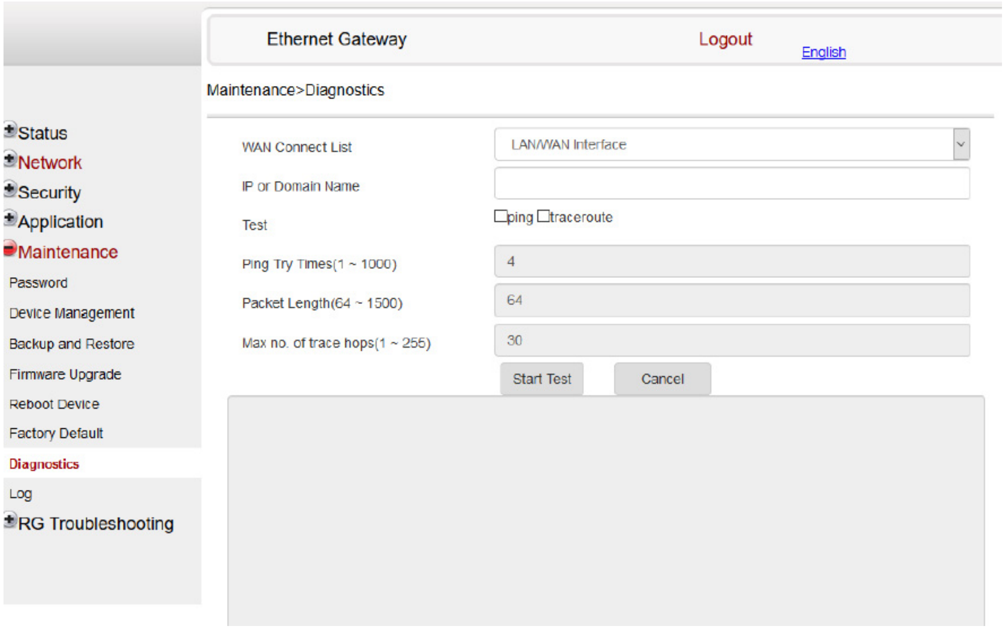
2 Click Factory Default to reset the CPE to its factory default settings.

3 STOP. This procedure is complete.

Procedure 45 Diagnose WAN connections

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

Figure 49 Diagnose window



WAN Connect List	LAN/WAN Interface
IP or Domain Name	
Test	□ping □traceroute
Ping Try Times(1 ~ 1000)	4
Packet Length(64 ~ 1500)	64
Max no. of trace hops(1 ~ 255)	30

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

3 Enter the IP address or domain name.

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

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

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

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

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

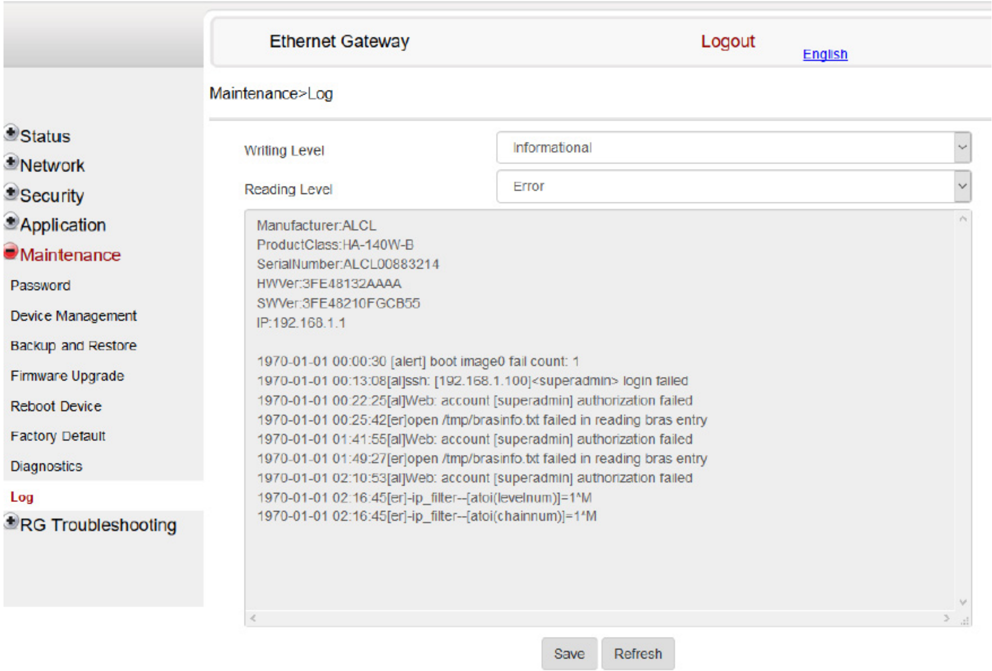
9 Click Cancel to cancel the test.

10 STOP. This procedure is complete.

Procedure 46 View log files

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

Figure 50 **Log window**



Writing Level: Informational

Reading Level: Error

```
Manufacturer:ALCL
ProductClass:HA-140W-B
SerialNumber:ALCL00883214
HWVer:3FE48132AAAA
SWVer:3FE48210FGCB55
IP:192.168.1.1

1970-01-01 00:00:30 [alert] boot image0 fail count: 1
1970-01-01 00:13:08[al]ssh: [192.168.1.100]<superadmin> login failed
1970-01-01 00:22:25[al]Web: account [superadmin] authorization failed
1970-01-01 00:25:42[er]open /tmp/brasinfo.txt failed in reading bras entry
1970-01-01 01:41:55[al]Web: account [superadmin] authorization failed
1970-01-01 01:49:27[er]open /tmp/brasinfo.txt failed in reading bras entry
1970-01-01 02:10:53[al]Web: account [superadmin] authorization failed
1970-01-01 02:16:45[er]-ip_filter--[atoi(levelnum)]=1^M
1970-01-01 02:16:45[er]-ip_filter--[atoi(chainnum)]=1^M
```

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.

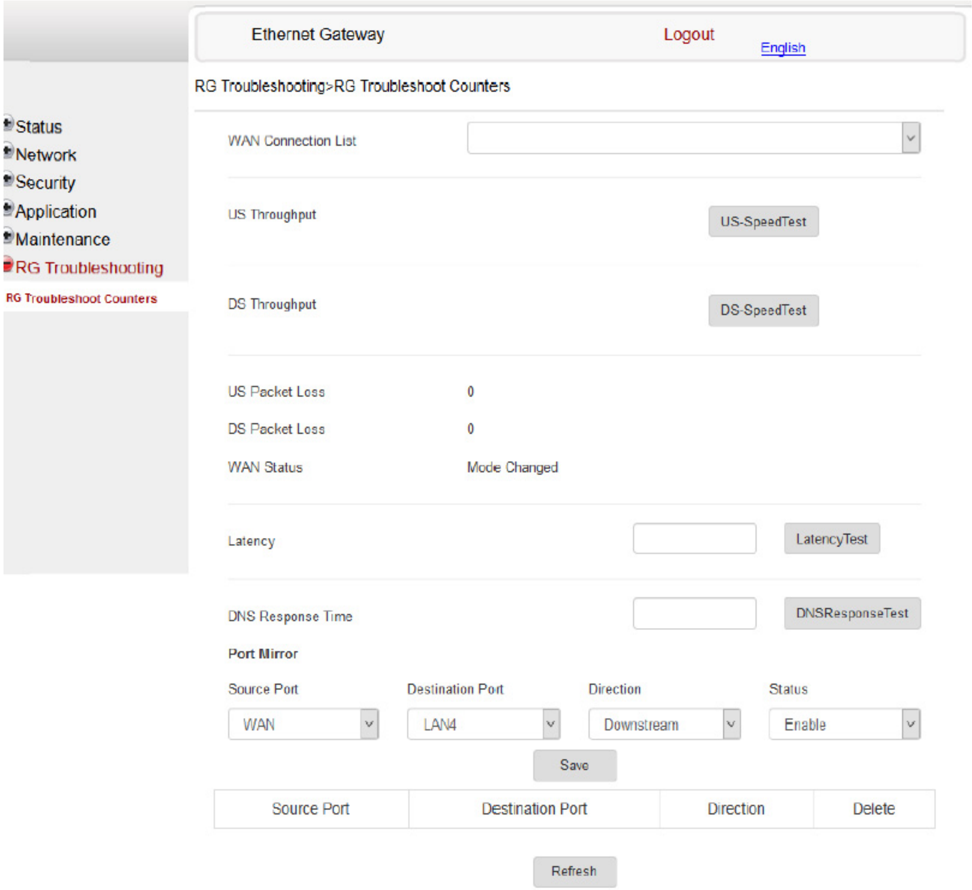
Tests are run to retrieve upstream and downstream throughput, latency, and DNS response time. The Troubleshooting Counters window also displays upstream and downstream packet loss and Internet status.

Procedure 47 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 51.

Figure 51 RG Troubleshooting Counters window



RG Troubleshooting>RG Troubleshoot Counters

WAN Connection List	
US Throughput	
DS Throughput	
US Packet Loss	0
DS Packet Loss	0
WAN Status	Mode Changed
Latency	
DNS Response Time	

Port Mirror

Source Port	Destination Port	Direction	Status
WAN	LAN4	Downstream	Enable

Source Port	Destination Port	Direction	Delete

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

Table 44 RG Troubleshooting Counters parameters

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

(1 of 2)

Field	Description
WAN Status	Whether the WAN linking is (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	Choose the source and destination ports, the direction (Downstream or Upstream), and the status (Enable or Disable) from the drop-down menus, and click Save

(2 of 2)

2 Configure the test times if desired.

3 Click Refresh to update the data.

4 STOP. This procedure is complete.

Customer Document and Product Support

Customer Documentation

Customer Documentation Welcome Page

Technical Support

Product Support Portal

Documentation Feedback

Customer Documentation Feedback