

7368 Intelligent Services Access Manager CPE

A-020W-A WiFi

7368 ISAM CPE A-020W-A Product Guide

3FE-47511-AAAA-TCZZA

Issue: 01

Nokia — Proprietary and confidential Use pursuant to applicable agreements

Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

© 2018 Nokia.

Contains proprietary/trade secret information which is the property of Nokia and must not be made available to, or copied or used by anyone outside Nokia without its written authorization. Not to be used or disclosed except in accordance with applicable agreements.

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 (3FE-47157-AAAA-TCZZA).

1.5 Assistance and ordering phone numbers

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

For ordering information, contact your Nokia sales representative.

1.6 Nokia quality processes

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

1.7 Safety information

For safety information, see the appropriate safety guidelines chapter.

1.8 Documents

Documents are available using ALED or OLCS.

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

- 1 Navigate to <u>http://support.alcatel-lucent.com</u> 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 <u>http://support.alcatel-lucent.com</u> 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.



 $\ensuremath{\text{Note}}$ — 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

1	Preface	9
1.1	Scope	9
1.2	Audience	9
1.3	Required knowledge	9
1.4	Acronyms and initialisms	9
1.5	Assistance and ordering phone numbers	9
1.6	Nokia quality processes	10
1.7	Safety information	10
1.8	Documents	10
1.9	Special information	11
1.9.1	Procedures with options or substeps	12
1.10	Multiple PDF document search	13
2	ANSI safety guidelines	9
2.1	Safety instructions	9
2.1.1	Safety instruction boxes in customer documentation	9
2.1.2	Safety-related labels	10
2.2	Safety standards compliance	11
2.2.1	Responsible party	11
2.2.2	Energy-related products standby and off modes compliance	12
2.2.3	FCC statement	12
2.2.4	FCC Radiation Exposure Statement	13
2.2.5	Resistibility requirements compliance	13
2.3	Electrical safety guidelines	13
2.3.1	Power supplies	14
2.3.2	Cabling	14
3	ETSI safety guidelines	15
3.1	Safety instructions	15
3.1.1	Safety instruction boxes	15
3.1.2	Safety-related labels	16
3.2	Safety standards compliance	17
3.2.1	Responsible party	17
3.2.2	Energy-related products standby and off modes compliance	18
3.2.3	EMC and RED compliance	
3.2.4	Equipment safety standard compliance	
3.2.5	Environmental standard compliance	19
3.2.6	Resistibility requirements compliance	19
3.3	Electrical safety guidelines	
3.3.1	Power supplies	
3.3.2	Cabling	19
4	ETSI environmental guidelines	21
4.1		
4.1.1		
4.1.2	EU ROHS	
4.1.3	End-ot-lite collection and treatment	22

5	A-020W-A unit data sheet	23
5.1	A-020W-A part numbers and identification	23
5.2	A-020W-A general description	
5.2.1	TR-069 object support for WiFi parameters	
5.2.2	Independent TR69 session with SaaS	
5.2.3	TR69 authentication using TLS and CA certificates	
5.3	A-020W-A software and installation feature support	27
5.4	A-020W-A interfaces and interface capacity	27
5.4.1	A-020W-A connections and components	27
5.5	A-020W-A LEDs	
5.6	A-020W-A detailed specifications	
5.7	A-020W-A functional blocks	
5.8	A-020W-A standards compliance	31
5.9	A-020W-A special considerations	31
5.9.1	WiFi service	32
5.9.1.1	WiFi standards and certifications	
5.9.1.2	WiFi GUI features	32
5.9.2	A-020W-A considerations and limitations	
6	Install a A-020W-A	33
6.1	Purpose	
6.2	General	33
6.3	Prerequisites	33
6.4	Recommended tools	
6.5	Safety information	
6.6	Procedure	
7	Replace a A-020W-A	37
7.1	Purpose	
7.2	General	
7.3	Prerequisites	
7.4	Recommended tools	
7.5	Safety information	
7.6	Procedure	
8	Configure a A-020W-A	41
8.1	GUI configuration	41
8.1.1	Login	41
8.1.2	Device and connection status	
8.1.3	Network configuration	
8.1.4	Security configuration	71
8.1.5	Application configuration	
8.1.6	Maintenance	
8.1.7	RG troubleshooting counters	

List of figures

2 Figure 1	ANSI safety guidelines A-020W-A sample safety label	9 11
3	ETSI safety quidelines	15
Figure 2	A-020W-A sample safety label	17
4	ETSI environmental guidelines	21
Figure 3	Recycling/take back/disposal of product symbol	
5	A-020W-A unit data sheet	23
Figure 4	A-020W-A CPE	25
Figure 5	A-020W-A physical connections	
Figure 6	A-020W-A LEDs	29
Figure 7	Single-residence WiFi CPE with Gigabit Ethernet	31
6	Install a A-020W-A	33
Figure 8	A-020W-A connections	35
7	Replace a A-020W-A	37
Figure 9	A-020W-A connections	39
8	Configure a A-020W-A	41
Figure 10	Web login window	
Figure 11	Device Information window	
Figure 12	LAN status window	45
Figure 13	WAN Status window	47
Figure 14	WAN Status IPv6 window	49
Figure 15	Home Networking information window	51
Figure 16	Statistics window (LAN port statistics shown)	53
Figure 17	LAN settings window	54
Figure 18	LAN IPv6 network window	56
Figure 19	WAN window	58
Figure 20	WAN DHCP window	59
Figure 21	Wireless (2.4GHz) network window	61
Figure 22	Wireless (5GHz) network window	63
Figure 23	Wireless Schedule window	65
Figure 24	DNS network window	66
Figure 25	TR-069 network window	68
Figure 26	QoS Config window (L2)	69
Figure 27	QoS Config window (L3)	70
Figure 28	Firewall window	72
Figure 29	MAC filter window	74
Figure 30	IP filter window	76
Figure 31	URL Filter window	77
Figure 32	Parental Control window	78
Figure 33	DMZ and ALG window	80
Figure 34	Access Control window	81
Figure 35	Port forwarding window	83

Figure 36	Port Triggering window	84
Figure 37	DDNS window	86
Figure 38	NTP window	87
Figure 39	UPnP and DLNA window	88
Figure 40	Password window	90
Figure 41	Device Management window	91
Figure 42	Backup and Restore window	92
Figure 43	Firmware Upgrade window	93
Figure 44	Reboot Device window	94
Figure 45	Factory Default window	95
Figure 46	Diagnostics window	96
Figure 47	Log window	97
Figure 48	RG Troubleshooting Counters window	
-		

List of tables

2 Table 1	ANSI safety guidelines	9 10
Table 2	Responsible party contact information	11
3 Table 3	ETSI safety guidelines Safety labels	15 16
Table 4		
5	A-020W-A unit data sheet	23
Table 5	Identification of A-020W-A	23
Table 6	A-020W-A interface connection capacity	27
Table /	A-020W-A physical connections	
Table 8	A-020W-A LEDs	
Table 9	A-020W-A physical specifications	
Table 10	A-020W-A power consumption specifications	
Table 11	A-020W-A environmental specifications	
8	Configure a A-020W-A	41
Table 12	Device Information parameters	43
Table 13	LAN status parameters	46
Table 14	WAN Status parameters	47
Table 15	WAN status IPv6 parameters	49
Table 16	Home Networking parameters	51
Table 17	LAN parameters	54
Table 18	LAN IPv6 network parameters	56
Table 19	WAN parameters	58
Table 20	WAN DHCP parameters	60
Table 21	Wireless 2.4GHz network parameters	61
Table 22	Wireless 5GHz network parameters	64
Table 23	DNS network parameters	67
Table 24	TR-069 network parameters	68
Table 25	QoS Config parameters	71
Table 26	Firewall parameters	73
Table 27	MAC filter parameters	75
Table 28	IP filter parameters	76
Table 29	URL Filter parameters	78
Table 30	Parental control parameters	79
Table 31	DMZ and ALG parameters	80
Table 32	Access control parameters	82
Table 33	Port forwarding parameters	83
Table 34	Port triggering parameters	84
Table 35	DDNS parameters	86
Table 36	Password parameters	90
Table 37	Device Management parameters	91
Table 38	RG Troubleshooting Counters parameters	99

2 ANSI safety guidelines

This chapter provides information about the mandatory regulations that govern the installation and operation of A-020W-A CPE equipment in the North American or ANSI market.

2.1 Safety instructions

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

2.1.1 Safety instruction boxes in customer documentation

The safety instruction boxes are provided in the 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 A-020W-A CPE equipment. It does not provide safety-related instructions.

2.1.2 Safety-related labels

The A-020W-A CPE equipment is labeled with specific safety compliance information and instructions that are related to a variant of the A-020W-A. Observe the instructions on the safety labels.

Table 1 provides examples of the text in the various A-020W-A CPE safety labels.

Table 1Safety 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.

Figure 1 shows a sample safety label for the A-020W-A CPE, located on the base of the unit.

Figure 1	A-020W-A sample safety label		
	Nokia Wi-Fi B1	Image: Apple of the second	
	ASSEMBLED IN CHINA This unit complies with part 15 of the FCC Rules. Operation is subject to following two conditions. (1) This device may not cause harmful interference (2) This device must accept any interference received, including interference that may cause undesired operation.		

2.2 Safety standards compliance

This section describes the A-020W-A CPE compliance with North American safety standards. The A-020W-A is compliant with CE, FCC, CB and ETL requirements.



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 Responsible party

Table 2 lists the party in the US responsible for this device.

Table 2 Responsible party contact information

Legal Company name	Nokia USA Inc.
Address	2301 SUGAR BUSH RD. STE 300, RALEIGH, NC 27612
Phone, Fax	+1 866 582-3688

2.2.2 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the A-020W-A CPE 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 A-020W-A CPE devices qualify as high network availability (HiNA) equipment. Since the main purpose of A-020W-A 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 "A-020W-A interfaces and interface capacity" in chapter 5.

For information about power consumption, see "A-020W-A detailed specifications" in chapter 5.

2.2.3 FCC statement

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

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

2.2.4 FCC Radiation Exposure Statement

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

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

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



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

2.2.5 Resistibility requirements compliance

The A-020W-A CPE equipment complies with the requirements of ITU Recommendation K.21 for resistibility of telecommunication equipment installed in customer premises to overvoltage and overcurrents.

2.3 Electrical safety guidelines

This section provides the electrical safety guidelines for the A-020W-A CPE equipment.



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 A-020W-A CPE equipment:

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

3 ETSI safety guidelines

This chapter provides information about the mandatory regulations that govern the installation and operation of A-020W-A CPE equipment.

3.1 Safety instructions

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

3.1.1 Safety instruction boxes

The safety instruction boxes are provided in the 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.



service interruption.

Caution 1 — Possibility of service interruption.

Caution 2 — Service interruption.

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

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 A-020W-A CPE equipment. It does not provide safety-related instructions.

3.1.2 Safety-related labels

The A-020W-A CPE equipment is labeled with the specific safety instructions and compliance information that is related to a variant of the A-020W-A. Observe the instructions on the safety labels.

Table 3 provides sample safety labels on the A-020W-A CPE equipment.

Table 3Safety labels

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

Figure 2 shows a sample safety label for the A-020W-A CPE, located on the base of the unit.

Figure 2	A-020W-A sample safety label		
	Nokia Wi-Fi B1 Model: HA-020W-A Admin IP: Admin IP: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Image: Additional and the second s	
	This unit complies with part 15 of the FCC Rules. Operation is subject to following two conditions. (1) This device may not cause harmful interference (2) This device must accept any interference received, including interference that may cause undesired operation.		

Safety standards compliance 3.2

This section describes the device compliance with European 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.

3.2.1 **Responsible party**

Table 4 lists the party in the US responsible for this device.

Table 4 **Responsible party contact information**

Legal Company name	Nokia USA Inc.
Address	2301 SUGAR BUSH RD. STE 300, RALEIGH,NC 27612
Phone, Fax	+1 866 582-3688

3.2.2 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the A-020W-A CPE 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 A-020W-A CPE devices qualify as high network availability (HiNA) equipment. Since the main purpose of A-020W-A 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 "A-020W-A interfaces and interface capacity" in chapter 5.

For information about power consumption, see "A-020W-A detailed specifications" in chapter 5.

3.2.3 EMC and RED compliance

The A-020W-A CPE equipment complies with the following EMC, EMI, and ESD requirements:

- EN 300-386: Electromagnetic Compatibility and Radio Spectrum Matters (ERM): Telecommunications Network Equipment; Electromagnetic Compatibility (EMC) requirements; Electrostatic Discharge (ESD) requirements
- European Council Directive 2014/30/EU
- European Council Directive 2014/53/EU
- EN300328: Wide band transmission systems; data transmission equipment operating in the 2.4 GHz ISM band using wide band modulation techniques
- EN301893: 5 GHz RLAN
- EN50385: Compliance of base station equipment with a radio frequency of electromagnetic field exposure limits (110MHz-100GHz)

3.2.4 Equipment safety standard compliance

The A-020W-A CPE equipment complies with the requirements of EN 62368-1, Safety of Information Technology Equipment for use in a restricted location.

3.2.5 Environmental standard compliance

The A-020W-A CPE equipment complies with the following EN 300 019 European environmental standards:

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

3.2.6 Resistibility requirements compliance

The A-020W-A 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.

3.3 Electrical safety guidelines

This section provides the electrical safety guidelines for the A-020W-A CPE equipment.



Note — The devices comply with BS EN 61140.

3.3.1 Power supplies

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

3.3.2 Cabling

The following are the guidelines regarding cables used for the A-020W-A CPE equipment:

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

4 ETSI environmental guidelines

This chapter provides information about the ETSI environmental regulations that govern the installation and operation of A-020W-A CPE equipment. This chapter also includes environmental operation parameters of general interest.

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

4.1 Environmental requirements

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

4.1.1 Transportation

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

4.1.2 EU RoHS

European Union (EU) Directive 2011/65/EU, "Restriction of the use of certain Hazardous Substances" (RoHS), restricts the use of lead, mercury, cadmium, hexavalent chromium, and certain flame retardants in electrical and electronic equipment. Nokia products shipped to the EU comply with the EU RoHS Directive. Nokia has implemented a material/substance content management process. The process is described in: Nokia process for ensuring RoHS Compliance (1AA002660031ASZZA). This ensures compliance with the European Union Directive 2011/65/EU on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment.

4.1.3 End-of-life collection and treatment

Electronic products bearing or referencing the symbol shown in Figure 3, 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 3 Recycling/take back/disposal of product symbol



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

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

In compliance with legal requirements and contractual agreements, where applicable, Nokia will offer to provide for the collection and treatment of Nokia products bearing the logo shown in Figure 3 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 A-020W-A unit data sheet

- 5.1 A-020W-A part numbers and identification
- 5.2 A-020W-A general description
- 5.3 A-020W-A software and installation feature support
- 5.4 A-020W-A interfaces and interface capacity
- 5.5 A-020W-A LEDs
- 5.6 A-020W-A detailed specifications
- 5.7 A-020W-A functional blocks
- 5.8 A-020W-A standards compliance
- 5.9 A-020W-A special considerations

5.1 A-020W-A part numbers and identification

Table 5 provides part numbers and identification information for the A-020W-A CPE.

Table 5 Identification of A-020W-A

Ordering part number	Provisioning number	Description	CLEC	CPR	ECI/ Bar code
3FE 47471 AA	3FE 47511 AA	CPE with WiFi Wi-Fi Access Point and range extender, 2 Gigabit Ethernet UNI, dual bands 802.11ac 2x2 and 802.11n 2x2 WiFi; 12V/1A AC/DC US plug external power supply variant. The following accessories are included: • CA_RJ45: 1 1.5m Yellow • Power adapter: 1 1.5m Black • Packing list: 1 A6 Normal	_		_
3FE 47471 BA	3FE 47511 BA	 CPE with Wi-Fi Access Point and range extender, 2 Gigabit Ethernet UNI, dual bands 802.11ac 2x2 and 802.11n 2x2 WiFi; 12V/1A AC/DC EU plug, 2-pin external power supply variant. The following accessories are included: CA_RJ45: 1 1.5m Yellow Power adapter: 1 1.5m Black Packing list: 1 A6 Normal 	_		_

(1 of 2)

Ordering part number	Provisioning number	Description	CLEC	CPR	ECI/ Bar code
3FE 47471 CA	3FE 47511 BA	CPE with Wi-Fi Access Point and range extender, 2 Gigabit Ethernet UNI, dual bands 802.11ac 2x2 and 802.11n 2x2 WiFi; 12V/1A AC/DC UK plug, 3-pin external power supply variant. The following accessories are included: CA_RJ45: 1 1.5m Yellow Power adapter: 1 1.5m Black Packing list: 1 A6 Normal	_		
3FE 47471 DA	3FE 47511 DA	CPE with Wi-Fi Access Point and range extender, 2 Gigabit Ethernet UNI, dual bands 802.11ac 2x2 and 802.11n 2x2 WiFi; 12V/1A AC/DC AU plug external power supply variant. The following accessories are included: • CA_RJ45: 1 1.5m Yellow • Power adapter: 1 1.5m Black • Packing list: 1 A6 Normal	_	_	_

(2 of 2)

5.2 A-020W-A general description

WiFi is abundantly deployed in home networks. Users require a seamless experience at home to connect their devices. Traditional WiFi networks require unique SSIDs for each of the access points or WiFi extenders, which complicated the user experience. The Nokia WiFi network simplifies the user experience by providing a seamless network and automating network optimization.

The Nokia WiFi solution includes a Nokia WiFi gateway, one or more Nokia WiFi beacons, the WiFi Care Portal for the customer care team of the operator, and a mobile application for end-user self care.

The A-020W-A CPE is an Ethernet residential gateway and WiFi beacon in the Nokia WiFi solution. The residential gateway is the central controller of the network while the beacon can extend the WiFi coverage to every corner of the home, providing seamless roaming to the connected devices.

The A-020W-A CPE has built-in concurrent dual-band WiFi 802.11b/g/n and 802.11ac networking with triple-play capability. A-020W-A devices can be configured using the Nokia WiFi Mobile App, which can be downloaded on both iOS and Android devices.

Figure 4 shows the A-020W-A CPE in its stand.

Figure 4



28229

A-020W-A CPEs provide the following functions:

- GE Ethernet uplink
- Concurrent 802.11n 2x2 MIMO in 2.4GHz and 802.11ac 2x2 MIMO in 5GHz
- auto-negotiation for speed and duplex on a port by port basis
- MDI/MDIX Ethernet auto-negotiation or manual configuration
- routed mode per LAN port
- Advanced data features: VLAN tag manipulation, classification, and filtering
- Traffic classification and QoS capability
- · Internal Switch
- 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
- support for multiple SSIDs (private and public instances); contact your Nokia representative for further details.
- WPS on/off button
- Ethernet-based Point-to-Point (PPPoE) and IP over Ethernet (IPoE)
- Network Address Translation (NAT)
- Network Address Port Translation (NAPT)

- TR-069 management
- ALG and UPnP port forwarding
- DMZ
- IP/MAC filter
- Multi-level firewall
- DNS server
- DHCP client/server
- support for HT40 and VHT80 modes for increased channel bandwidth
- · support for up to 32 simultaneous wireless connections
- remote software image download

5.2.1 TR-069 object support for WiFi parameters

The A-020W-A CPE supports the status retrieval and configuration of the following WiFi parameters via TR-069:

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

These are the same TR-069 object parameters that are supported in the GUI. For more information, see Tables 21 and 22 in the chapter "Configure a A-020W-A".

5.2.2 Independent TR69 session with SaaS

The prime communication between the Nokia cloud management solution and the A-020W-A CPE is TR-069.

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

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

5.2.3 TR69 authentication using TLS and CA certificates

A-020W-A CPE devices support encrypted remote TR-069 management using TLS, as well as ACS authentication using SHA-256 pre-installed certificates.

If the ACS URL is set to the https://... format, by default, the connection will use TLS without authentication mode. The A-020W-A CPE can also authenticate the ACS using a pre-installed CA certificate.

5.3 A-020W-A software and installation feature support

For information on installing or replacing the A-020W-A CPE, see:

- Install a A-020W-A
- Replace a A-020W-A

5.4 A-020W-A interfaces and interface capacity

Table 6 describes the supported interfaces and interface capacity for A-020W-A CPE devices.

Table 6 A-020W-A interface connection capacity

Type and	Maximum capacity								
moder	POTS	10/ 100 BASE-T	10/ 100/1000 1000 BASE-T	RF video (CATV)	MoCA	VDSL2	E1/T1	Local craft	GE uplink
A-020W-A	—	—	2	_	—	_	_	—	1

5.4.1 A-020W-A connections and components

Figure 5 shows the physical connections for A-020W-A CPE devices.



Figure 5 A-020W-A physical connections

28230

Table 7 describes the physical connections for A-020W-A CPE devices.

Table 7A-020W-A physical connections

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

5.5 A-020W-A LEDs

Figure 6 shows the A-020W-A CPE LEDs.



28229

Table 8 provides LED descriptions for the A-020W-A CPE.

Table 8 A-020W-A LEDs

Indicator	LED color and behavior	LED behavior description			
Power	Green	Power on			
	Off	Power off			
	Red (default until software is running)	Failed on startup (for example corrupt flash), self test failed on startup, or self test failed during regular operation.			
WPS (2.4G	Green solid	WPS is successful (light turns off five minutes after successful WiFi setup)			
and 5G)	Green flashing	WPS is in progress (light turns off after two minutes if WPS is unsuccessful)			
	Off	WPS is not in progress			
	Solid Red	WPS error or overlapped (lights for 20 s and then turns off)			
INTERNET	Green solid	RG mode: Internet is up, IP address is assigned			
		Beacon mode: Connection to the access point is good, IP address is assigned			
	Green flashing	RG mode: Attempting to connect to the Internet			
		RG mode: Gateway has no Internet connection			
	Red	Beacon mode: No or poor connection to the access point			

Issue: 01

5.6 A-020W-A detailed specifications

Table 9 lists the physical specifications for the A-020W-A CPE.

Table 9A-020W-A physical specifications

Description	Specification
Width	42.2 mm (1.66 in.)
Height	123.22 mm (4.85 in.)
Depth	112.64 mm (4.43 in.)
Weight [within \pm 0.5 lb (0.23 kg)]	230g (0.5 lb)

Table 10 lists the power consumption specifications for the A-020W-A CPE.

Table 10A-020W-A power consumption specifications

Maximum power (Not to exceed)	Condition	Minimum power	Condition
8 W	2 10/100/1000 Base-T Ethernet, WiFi operational	2 W	interfaces/services not provisioned

Table 11 lists the environmental specifications for the A-020W-A CPE.

Table 11 A-020W-A environmental specifications

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

5.7 A-020W-A functional blocks

A-020W-A CPE devices are single-residence units that support Wireless (WiFi) service. WiFi service on these devices is compliant with the IEEE 802.11 standard. In addition to the WiFi service, these devices transmit Ethernet packets to two RJ-45 Ethernet ports.

Figure 7 shows the functional blocks for the A-020W-A CPE.


Figure 7 Single-residence WiFi CPE with Gigabit Ethernet

28228

5.8 A-020W-A standards compliance

A-020W-A CPE devices are compliant with the following standards:

- IEEE 802.1D (bridging), 802.1p (QoS), 802.1q (VLAN)
- IEEE 802.3 (2012) (Ethernet standard)
- IEEE 802.11n/ac 2x2 (WiFi 5G) and 802.11b/g/n 2x2 (WiFi 2.4G)

5.9 A-020W-A special considerations

This section describes the special considerations for A-020W-A CPE devices.

5.9.1 WiFi service

A-020W-A CPE devices feature WiFi service as well as data services. WiFi is a wireless networking technology that uses radio waves to provide wireless HSI and network connections. This device complies with the IEEE 802.11 standards, which the WiFi Alliance defines as the basis for WiFi technology.

5.9.1.1 WiFi standards and certifications

The WiFi service on A-020W-A CPE devices support the following IEEE standards and WiFi Alliance certifications:

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

5.9.1.2 WiFi GUI features

A-020W-A CPE devices have HTML-based WiFi configuration GUIs.

In addition to the traditional web-based GUI, the home user can download and use a mobile app for managing the A-020W-A CPE.

5.9.2 A-020W-A considerations and limitations

None.

6 Install a A-020W-A

- 6.1 Purpose
- 6.2 General
- 6.3 Prerequisites
- 6.4 Recommended tools
- 6.5 Safety information
- 6.6 Procedure

6.1 Purpose

This chapter provides the steps to install a A-020W-A CPE.

6.2 General

The steps listed in this chapter describe mounting and cabling for a A-020W-A CPE.

6.3 Prerequisites

You need the following items before beginning the installation:

all required cables

6.4 Recommended tools

You need the following tools for the installation:

- RJ-45 Ethernet cable
- paper clip

6.5 Safety information

Read the following safety information before installing the unit.



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

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

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



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



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

Note 2 — Observe the following:

- The device should be installed in accordance with the applicable requirements of the NEC or CEC. Local authorities and practices take precedent when there is conflict between the local standard and the NEC or CEC.
- The device must be installed by qualified service personnel.
- Indoor units must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the A-020W-A unit data sheet for the temperature ranges for these devices.

6.6 Procedure

Use this procedure to install a A-020W-A CPE.

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



Note — The A-020W-A CPE cannot be stacked with another A-020W-A or with other equipment. The installation requirements are:

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

2 Review the connection locations as shown in Figures 8.

Figure 8 A-020W-A connections



28230

- **3** Connect the Ethernet cables to the RJ-45 ports; see Figure 8 for the location of the RJ-45 ports.
- 4 Connect the WAN cable to the RJ-45 WAN port; see Figure 8 for the location of the RJ-45 WAN port.

5 Connect the power cable to the power connector.



- **Note** Observe the following:
- Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 12 V dc, 1 A. The polarity of the power adapter plug must match the A-020W-A CPE.
- 6 Power up the unit by using the On/Off power switch.
- 7 Verify the LEDs and voltage status.
- 8 Activate and test the services.
- 9 If necessary, reset the A-020W-A CPE.



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

- i Locate the Reset button as shown in Figure 8.
- ii Insert the end of a straightened paper clip or other narrow object into the hole in the Reset button to reset the device.
- **10** STOP. This procedure is complete.

7 Replace a A-020W-A

- 7.1 Purpose
- 7.2 General
- 7.3 Prerequisites
- 7.4 Recommended tools
- 7.5 Safety information
- 7.6 Procedure

7.1 Purpose

This chapter provides the steps to replace a A-020W-A CPE.

7.2 General

The steps listed in this chapter describe mounting and cabling for a A-020W-A CPE.

7.3 Prerequisites

You need the following items before beginning the installation:

all required cables

7.4 Recommended tools

You need the following tools for replacing the A-020W-A CPE:

- RJ-45 Ethernet cable
- paper clip

7.5 Safety information

Read the following safety information before replacing the unit.



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

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

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



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



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

Note 2 — Observe the following:

- The device should be installed in accordance with the applicable requirements of the NEC or CEC. Local authorities and practices take precedent when there is conflict between the local standard and the NEC or CEC.
- The device must be installed by qualified service personnel.
- Indoor units must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the A-020W-A unit data sheet for the temperature ranges for these devices.

7.6 Procedure

Use this procedure to replace a A-020W-A CPE.

1 Power down the unit by using the on/off power switch. See Figure 9 for the connections on the A-020W-A CPE.

Figure 9 A-020W-A connections



28230

- 2 Disconnect the WAN, Ethernet, and power cables from the A-020W-A CPE; see Figure 9 for the connector locations on the A-020W-A.
- **3** Replace the A-020W-A CPE with the new A-020W-A. The device can be placed on any flat surface, such as a desk or shelf.
- 4 Connect the Ethernet cables directly to the RJ-45 ports; see Figure 9 for the location of the RJ-45 ports.
- 5 Connect the WAN cable directly to the RJ-45 port; see Figure 9 for the location of the RJ-45 WAN port.

6 Connect the power cable to the power connector.



- **Note** Observe the following:
- Units must be powered by a Listed or CE approved and marked limited power source with a minimum output rate of 12 V dc, 1 A. The polarity of the power adapter plug must match the A-020W-A CPE.
- 7 Power up the unit by using the On/Off power button.
- 8 Verify the LEDs and voltage status.
- **9** Activate and test the services.
- 10 If necessary, reset the A-020W-A CPE.



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

- i Locate the Reset button on a A-020W-A CPE, as shown in 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 device.
- **11** STOP. This procedure is complete.

8 Configure a A-020W-A

8.1 GUI configuration

8.1 GUI configuration

Use the procedures below to use the web-based GUI for the A-020W-A CPE.

The A-020W-A CPE is used as an Ethernet gateway to connect devices in the home to the Internet. The GUI provides a variety of features for the home network including routing and firewall capability. By using the GUI, users can configure the right network connectivity fort all equipment in their home, including personal computers, set-top boxes, mobile phones, and other consumer electronics devices, to the Internet.

8.1.1 Login

Use the procedure below to login to the web-based GUI for the A-020W-A CPE.

Procedure 6 Login to web-based GUI

1 Open a web browser and enter the IP address of the A-020W-A CPE in the address bar.

The login window appears.

The default gateway IP address is http://192.168.18.1. You can connect to this IP address using your web browser after connecting your PC to one of Ethernet ports of the A-020W-A CPE. The static IP address of your PC must be in the same 192.168.18.x subnet as the A-020W-A.

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

The default user name is admin. The default password is a random number, which is included in the A-020W-A CPE kit.

Ethernet Gateway			
Username Password			
Login	Reset		

Figure 10 Web login window



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

Pressing the Reset button for less than 10 seconds reboots the A-020W-A CPE; pressing the Reset button for 10 seconds resets the A-020W-A to the factory defaults.

3 Click Login. The Device Information screen appears.



Note — To help protect the security of your Internet connection, the application displays a pop-up reminder to change both the WiFi password and the A-020W-A CPE password.

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

4 STOP. This procedure is complete.

8.1.2 Device and connection status

The A-020W-A CPE supports the retrieval of a variety of device and connection information, including:

- device information
- LAN status
- WAN status
- WAN status IPv6

- home networking information
- statistics

Procedure 7 Device information retrieval

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

Figure 11 Device Information window

NOKIA	Ethernet Gateway	Logout English Español
	Status>Device Information	
●Status		
Device Information	Device Name	HA-020W-A
LAN Status	Vendor	Nokia
WAN Status	Vendor	- TONIA
WAN Status IPv6	Serial Number	ALCL00861234
Home Networking	Hardware Version	3FE47239AAAA
Statistics	Root Version	LI Root Doc 24 2016 12:00:00
Network	BOUT VEISION	0-0001 Dec-31-201012.00.00
Security	Software Version	3FE473360.00
Application	Chipset	MTK7621F
Maintenance	Douise Dupping Time	0 hours 6 minutes 0 seconds
RG Troubleshooting	Device Running Time	o nours o minutes a seconds
		Refresh

Table 12 describes the fields in the Device Information window.

Table 12Device Information parameters

Field	Description	
Device Name	Mnemonic of the A-020W-A CPE	
Vendor	Name of the vendor	
Serial Number	Serial number of the A-020W-A CPE	
Hardware version	Hardware version of the A-020W-A CPE	
Boot version	Boot version of the A-020W-A CPE	
Software version	Software version of the A-020W-A CPE	
Chipset	Chipset of the A-020W-A CPE	

Field	Description		
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

NOKIA	Ethernet Gateway	Logout English Espeñol
	Status>LAN Status	
Status Device Information	Wireless Information	
LAN Status	Wireless Status	on
WAN Status	Wreiess Channel	4
Home Networking	SSID1 Name 🗸	NCKIA-1910
Statistics	Wireless Encryption Status	WPA2-PSK
 Network Security Application Maintenance RG Troubleshooting 	Wheless Rx Packets	0
	Wreiezs Tz Packets	0
	Wreless R: Sytes	٥
	Wireless Tx Sytes	٥
	Power Transmission(mW)	200
	Ethernet Information	

Ethernet Status	Up
Ethernet IP Address	192.165.15.1
Ethernet Subnet Mask	255.255.255.0
Ethernet MAC Address	00:20:15:11:19:10
Ethernet Rx Packets	0
Ethernet To Packets	0
Ethernet Rx Sytes	4259459752
Ethernet Tx Bytes	4259459780

Up	Down	
Full-duplex	Half-duplex	
1000	Auto	
٥	٥	
0	0	
٥	٥	
0	٥	
2144729576	2144729576	
2144729550	2144729580	
	LUp Full-tugies: 1000 0 0 0 0 2144728576 2144728550	

Refresh

Table 13 describes the fields in the LAN status window.

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

Table 13LAN status parameters

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

NOKIA	Ethernet Gateway			Logout	English Español	
	Status>WAN Status					
Status Device Information	WAN Connection List					~
LAN Status	Connection Mode					
WAN Status WAN Status IPv6	Enable/Disable					
Home Networking	VLAN					
Statistics	WAN Link Status					
Security ■ Security	IPv4 Address					
Application	Netmask					
Maintenance	Gateway					
RG Troubleshooting	Primary DNS					
	Second DNS					
	Manual DNS					
	Ethernet Link Status	Down				
	Tx Packets	0				
	Rx Packets	0				
	Tx Dropped	0				
	Rx Dropped	0				
	Err Packets	0				
		[Refresh			

Table 14 describes the fields in the WAN Status window.

Table 14WAN 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

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

(2 of 2)

2 Click Refresh to update the displayed information.

3 STOP. This procedure is complete.

Procedure 10 WAN status IPv6 retrieval

1 Select Status > WAN Status IPv6 from the top-level menu in the Ethernet Gateway window, as shown in Figure 14.

Figure 14 WAN Status IPv6 window

NOKIA	Ethernet Gateway		Logout	Englisb Español
	Status>WAN Status IPv6			
Status Device Information	WAN Connection List			
LAN Status WAN Status	Enable/Disable			
WAN Status IPv6	VLAN			
Home Networking	WAN Link Status			
Statistics	IPv6 address			
Security	IPv6 Prefix			
Application	IPv6 Gateway			
Maintenance	Primary DNS			
RG Troubleshooting	Second DNS			
	Ethernet Link Status	Down		
	Tx Packets	0		
	Rx Packets	0		
	Tx Dropped	0		
	Rx Dropped	0		
	Err Packets	0		
		F	Refresh	

Table 15 describes the fields in the WAN status IPv6 window.

Table 15WAN status IPv6 parameters

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

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

(2 of 2)

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

Procedure 11 Home networking information retrieval

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

Figure 15 Home Networking information window

NOKIA	Ethernet Gateway			Logout English Español						
	Status>Home N	Vetworking	9							
Status Device Information	Local	Interfa	ice							
LAN Status		Conne	tion Type		Connected Devices			Setting		
VAN Status		Et	hernet			1				
fome Networking		Wireles	6 (2.4GHz)			o			Setting	
Statistics		Wirele	ss (5GHz)		0			Setting		
Maintenance RG Troubleshooting	Network Na Access Po	ame bint (NOKIA-1910 0:20:18:11:19:19		NOKU 02:20:1	A-1910-2 8:11:19:19	NOKIA-1: 02:20:18:2	910-3 1:19:19	NOKIA- 02:20:18:	1910-4 31:19:19
	Wirele	ss Set	tings (50	GHz)						
	Network Na	ame N	IOKIA-1910-11ac	N	OKIA-1	910-11ac-2	NOKIA-1910	D-11ac-3	NOKIA-191	10-11ac-4
	Access Po	oint C	0:20:18:11:19:1d		02:20:1	8:10:19:1d	02:20:18:1	1:19:1d	02:20:18:	12:19:1d
	Local	Device	es							
	Statue C	onnection Type	Device Name	IPv4 Add	rees	Hardware Address	IP Address Allocation	Lease Remaining	Last Active	Delete

Refresh	

Static

01/01/1970

08:01:07 AM

Delete

Table 16 describes the fields in the Home Networking window.

Table 16Home Networking parameters

Active

Ethernet

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

CV0042077N0 192.168.18.100 fc:3f:db:fb:7b:85

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

(2 of 2)

- 2 Click Delete to delete a particular local device connection.
- **3** Click Refresh to update the displayed information.
- 4 STOP. This procedure is complete.

Procedure 12 Statistics retrieval

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

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

Figure 16 shows the statistics for the LAN ports.

NOKIA	Ethernet Gateway		Logout English Español
	Status>Statistics		
Status			
Device Information	LAN WAN WLAI	N	
LAN Status			
WAN Status			Refresh
WAN Status IPv6			
Home Networking			
Statistics	COUNTERS	LAN1	LAN2
Network	Bytes Sent	2144729880	2144729880
Security	Bytes Received	2144729876	2144729876
Application	Packets Sent	D	0
Maintenance	Packets Received	D	0
RG Troubleshooting	Errors Sent	D	0
	Unicast Packets Sent	2144729868	2144729868
	Unicast Packets Received	2144729868	2144729868
	Discard Packets Sent	4004011016	4004011016
	Discard Packets Received	1129136668	1129136668
	Multicast Packets Sent	2144729868	2144729868
	Multicast Packets Received	2144729868	2144729868
	Broadcast Packets Sent	2144729868	2144729868
	Broadcast Packets Received	2144729868	2144729868
	Unknown Proto Packets Received	D	0

Figure 16 Statistics window (LAN port statistics shown)

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

8.1.3 Network configuration

The A-020W-A CPE also supports network configuration, including:

- LAN
- LAN IPv6
- WAN
- WAN DHCP
- Wireless 2.4G
- Wireless 5G
- wireless schedule
- DNS

- TR-069
- QoS Configuration

Procedure 13 LAN configuration

1 Select Network > LAN from the top-level menu in the Ethernet Gateway window, as shown in Figure 17.

NOKIA	Ethernet Gateway	Logout English Español		
	Network>LAN			
Status Network	IPv4 Address	192.168.18.1		
LAN	Subnet Mask	255.255.255.0		
LAN_IPv6	DHCP Enable	V		
WAN WAN DHCP	DHCP Start IP Address	192.168.18.2		
Wireless (2.4GHz)	DHCP End IP Address	192.168.18.253		
Wireless (5GHz)	DHCP Lease Time	1440		
DNS		(2~129600 mins, or 0 means 1 day)mins.		
TR-069	Primary DNS			
QoS Config Security	Secondary DNS			
Application		Save Refresh		
Maintenance				
RG Troubleshooting	Static DHCP Entry			
	MAC Address			
	IPv4 Address			
		Add		
	MAC Address	IPv4 Address Delete		

Figure 17 LAN settings window

Table 17 describes the fields in the LAN window.

Table 17 LAN parameters

Field	Description
IPv4 Address	IP Address of the A-020W-A CPE
Subnet Mask	Subnet mask of the A-020W-A CPE
DHCP enable	Select this check box to enable DHCP
DHCP Start IP Address	Starting DHCP IP address

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

(2 of 2)

- 2 Configure the LAN.
- 3 Click Save.
- 4 Bind a MAC address to the LAN by entering the MAC and IP addresses in the Static DHCP Entry fields and then clicking Add. Repeat for all MAC addresses to be bound.
- **5** STOP. This procedure is complete.

Procedure 14 LAN IPv6 networking configuration

1 Select Network > LAN_IPv6 from the top-level menu in the Ethernet Gateway window, as shown in Figure 18.

Figure 18 LAN IPv6 network window

NOKIA	Ethernet Gateway	Logout	English Español	
	Network>LAN_IPv6			
●Status				
Network	IPv6 LAN Host Config	guration		
LAN	DNS Server	HGWProxy		
LAN_IPv6				
WAN	Prefix Config	WAINConnection		
WAN DHCP	Interface			\checkmark
Wireless (2.4GHz)				
Wireless (5GHz)	DHCBy6 Server Bool			
Wireless Schedule	DHCFV0 Server F001			
DNS	DHCP Start IP Address	0:0:0:2		
TR-069	DHCP End IP Address	0:0:0:255		
QoS Config				
Security				
Application Maintenance	Whether the address info through DHCP			
RG Troubleshooting	Whether other info obtained through DHCP	V		
	Maximum interval for periodic RA	600		
	messages	seconds		
	Minimum interval for periodic RA	200		
	messages	seconds		
		Save/Apply		

Table 18 describes the fields in the LAN IPv6 network window.

Table 18LAN IPv6 network parameters

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

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

(2 of 2)

- 2 Choose a DNS server, Prefix Config, and Interface.
- **3** Enter the DHCP configuration information.
- 4 Enter the maximum and minimum intervals for RA messages.
- 5 Click Save/Apply.
- **6** STOP. This procedure is complete.

Procedure 15 WAN networking configuration

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

Figure 19 WAN window

NOKIA	Ethernet Gateway	Logout English Español
	Network>WAN	
● Status ● Network	WAN Connection List	Create One New Connection
LAN	Connection Type	®IPoE ○PPPoE
LAN_IPv6	IP mode	IPv4
WAN DHCP	Enable/Disable	
Wireless (2.4GHz)	NAT	¥.
Wireless (5GHz) Wireless Schedule	Service	
DNS	Enable VLAN	Z
TR-069 QoS Config	VLAN ID	
Security	VLAN PRI	
Application	WAN IP Mode	DHCP
 Maintenance RG Troubleshooting 	Manual DNS	
		Save Delete

Table 19 describes the fields in the WAN window.

Table 19WAN parameters

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

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

(2 of 2)

- 2 Configure a specific WAN connection.
- 3 Click Save.
- 4 STOP. This procedure is complete.

Procedure 16 WAN DHCP configuration

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

NOKIA	Ethernet Gateway			Logout	English Español	
	Network>WAN DHCP					
●Status ●Network	WAN Connection List					V
LAN	DHCP Option 50 Persistent					
LAN_IPv6	Enable DHCP Option 60					
WAN DHCP	Enable DHCP Option 61					
Wireless (2.4GHz)		Save	Refresh			
Wireless (5GHz)						
Wireless Schedule						
DNS						
TR-069						
QoS Config						
Security						
Application						
Maintenance						
RG Troubleshooting						

Table 20 describes the fields in the WAN DHCP window.

Table 20WAN DHCP parameters

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

- 2 Configure a WAN DHCP option.
- 3 Click Save.
- 4 STOP. This procedure is complete.

Procedure 17 Wireless (2.4GHz) networking configuration

1 Select Network > Wireless (2.4GHz) from the top-level menu in the Ethernet Gateway window, as shown in Figure 21.

Figure 21 Wireless (2.4GHz) network window

NOKIA	Ethernet Gateway	Logout	English Español
	Network>Wireless (2.4GHz)		
Status ■Network	Enable	Ø	
LAN	Mode	auto(b/g/n)	\checkmark
LAN_IPv6	Bandwidth	20MHz	\checkmark
WAN WAN DHCP	Channel	Auto	V
Wireless (2.4GHz)	Transmitting Power	100%	✓
Wireless (5GHz) Wireless Schedule	WMM	Enable	\checkmark
DNS	Total MAX Users	32	
QoS Config Security	SSID Configurat	ion	
Application	SSID Select	SSID1	\checkmark
Maintenance	SSID Name	NOKIA-1910	
RG Troubleshooting	Enable SSID	Enable	\checkmark
	SSID Broadcast	Enable	¥
	MAX Users	32	
	Encryption Mode	WPA/WPA2 Personal	⊻
	WPA Version	WPA2	\checkmark
	WPA Encryption Mode	AES	\checkmark
	WPA Key		
	Enable WPS	Enable	
	WPS Mode	PBC	
	WPS Connect		
		Save Refresh	

Table 21 describes the fields in the Wireless 2.4GHz network window.

Table 21 Wireless 2.4GHz network parameters

Field	Description
Enable	Select this check box to enable WiFi

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

(2 of 2)

2 Configure the WiFi connection.

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

4 Click Save.

5 STOP. This procedure is complete.

Procedure 18 Wireless (5GHz) networking configuration

1 Select Network > Wireless (5GHz) from the top-level menu in the Ethernet Gateway window, as shown in Figure 22.

NOKIA	Ethernet Gateway	Logout	English Español
	Network>Wireless (2.4GHz)		
≝Status ■Network	Enable		
LAN	Mode	auto(b/g/n)	\checkmark
LAN_IPv6	Bandwidth	20MHz	\checkmark
WAN WAN DHCP	Channel	Auto	\checkmark
Wireless (2.4GHz)	Transmitting Power	100%	\checkmark
Wireless (5GHz) Wireless Schedule	WMM	Enable	
DNS TR-069	Total MAX Users	32	
QoS Config Security	SSID Configurat	ion	
Application	SSID Select	SSID1	\checkmark
Maintenance	SSID Name	NOKIA-1910	
■RG Troubleshooting	Enable SSID	Enable	\checkmark
	SSID Broadcast	Enable	~
	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	\checkmark
	WPS Connect		
		Save Refresh	

Figure 22 Wireless (5GHz) network window

Table 22 describes the fields in the Wireless 5GHz network window.

Table 22Wireless 5GHz network parameters

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

Notes

- ⁽¹⁾ When Encryption Mode is set to "WPA/WPA2 Enterprise", the following options are no longer available: WPA version, WPA encryption mode, WPA key, Enable WPS, WPS mode.
- ⁽²⁾ When Encryption Mode is set to "WPA/WPA2 Enterprise", the following options become available: Primary RADIUS server, port and password; Secondary RADIUS server, port, and password; RADIUS accounting port.

- 2 Configure the Wireless connection.
- 3 If you have enabled and configured WPS, click WPS connect.
- 4 Click Save.
- **5** STOP. This procedure is complete.

Procedure 19 Wireless scheduling

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

Figure 23 Wireless Schedule window

NOKIA	Ethernet Gateway		Logout English Español
	Network>Wireless Schedule		
●Status ●Network	Wireless Mode		
LAN	Schedule Function		
LAN_IPv6	Current Time		
WAN	our ent mile	01/01/1970	0 08:22:06 AM
WAN DHCP			
Wireless (2.4GHz)	Turn off the Wireless	s signal by the follo	
Wireless (5GHz)	run on the wheles.	s signal by the lone	
Wireless Schedule	Start	End	Recurrence Pattern
DNS			
TR-069			+
QoS Config			
●Security			
Application			
Maintenance			
RG Troubleshooting			

- 2 Select the Schedule Function check box to turn the wireless signal off for the configured period.
- **3** Click the plus sign (+) to add a scheduling rule.

A separate panel appears for configuring wireless schedule rules.

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

- **5** Choose Everyday or Individual Days from the drop-down menu.
- 6 If you chose Individual Days, select the check boxes for the desired days.

The Recurrence Pattern shows the rules created to date.

- 7 If desired, click the plus sign (+) to add more rules.
- 8 Click Save Changes.
- **9** STOP. This procedure is complete.

Procedure 20 DNS configuration

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

NOKIA	Ethernet Gateway	Logout English Español		
	Network>DNS			
[●] Status ●Network	DNS Proxy	related	Save	
LAN LAN_IPv6 WAN	Domain Name			
WAN DHCP Wireless (2.4GHz)	IPv4 Address	Add		
Wireless (5GHz) Wireless Schedule DNS	Origin Domain			
TR-069 QoS Config	New Domain	Add		
Security Application				
■ RG Troubleshooting	Domain Name	New Domain	IPv4 Address	Delete
	Origin Domain	New	v Domain	Delete

Figure 24 DNS network window
Table 23 describes the fields in the DNS network window.

Table 23	DNS network	parameters

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

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

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

4 STOP. This procedure is complete.

Procedure 21 TR-069 configuration

1 Select Network > TR-069 from the top-level menu in the Ethernet Gateway window, as shown in Figure 25.

Figure 25 TR-069 network window

NOKIA	Ethernet Gateway	Logout English Español
	Network>TR-069	
●Status ●Network	Periodic Inform Enable	
LAN	Periodic Inform Interval(s)	5
LAN_IPv6	URL	https://acs.nokia.net:7754
WAN WAN DHCP	Username	admin
Wireless (2.4GHz)	Password	**********
Wireless (5GHz)	Connect Request Username	itms
Wireless Schedule DNS	Connect Request Password	•••••
TR-069		Save Refresh
QoS Config Security Application Maintenance RG Troubleshooting		

Table 24 describes the fields in the TR-069 network window.

Table 24TR-069 network parameters

Field	Description
Periodic Inform Enable	Select this check box to enable periodic inform updates
Periodic Inform Interval(s)	Time between periodic inform updates, in seconds
URL	URL of the auto-configuration server
Username	Username used to log in to the A-020W-A CPE
Password	Password used to log in to the A-020W-A CPE
Connect Request Username	Username used to log in to the auto-configuration server
Connect Request Password	Password used to log in to the auto-configuration server

2 Configure TR-069 by entering the required information.

3 Click Save.

4 STOP. This procedure is complete.

Procedure 22 QoS configuration

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

Figure 26 shows the window for configuring QoS L2 (Layer 2 packet sizes).

Figure 26 QoS Config window (L2)

NOKIA	Ethernet Gateway	Logout <u>English</u> <u>Español</u>
	Network>QoS Config	
	QoS Setting	
Network	Source	
LAN	ID Source MAC Protocol Source Exclude Port	Source SExclude Dest Dest DExclude
LAN_IPv6	Exclude	
WAN		
WAN DHCP	Ture	7
Wireless (2.4GHz)	L2 Criteria	
Wireless (5GHz)	Classification	
Wireless Schedule	Criteria	
DNS	Source MAC Exclude	
TR-069		
QoS Config	Interface select an option	
Security		
Application		
Maintenance	Classification	
RG Troubleshooting	Result	
	DSCP Remark: 802.1p Rema	rk:
	(Range:0~63)	(Range:0~7)
	Forwarding Policy: (Range:1~7)	
	Add	

Figure 27 shows the window for configuring QoS L3 (Layer 3 packet sizes).

		Source									
ID	Source MAC	MAC	Protocol	Protoco Exclud	e Port	Source Max	SExclude	Dest Port	Dest Max	DExclud	
4											
Туре		L3 CI	riteria	T							
Class Criter	sification ria										
Proto	col	None	•	T	Exclude 🗆						
Applic	ation			¥							
Sourc	e Ip				Source Ip M	ask			E	xclude 🗆	
Dest I	lp				Dest Ip Mas	k			E	xclude 🗆	
Sourc	e Port				Source Port Max				E	Exclude	
Dest I	Port				Dest Port M	ax			Exclude		
Sourc	ce Ip				Source Ip M	ask	ask			Exclude	
Dest	lp				Dest Ip Mas	Dest Ip Mask				Exclude	
Sourc	ce Port				Source Port Max				E	xclude 🗆	
Dest	Port				Dest Port M	ax			E	xclude 🗆	
802.1	р										
		(Range	:0~7)								
Interf	ace	selec	t an option	•							
Class Resu	sification It										
802.1 Rema	p ark:	(Range	:0~7)		DSCP Rema	ark: (F	Range:0~63)				
Forwa Policy	arding /:										
		(Range	:1~7)		Add						

Figure 27 QoS Config window (L3)

Table 25 describes the fields in the QoS Config window.

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

Table 25QoS Config parameters

- 2 Choose a QoS type from the drop-down menu: L2 or L3.
- 3 Configure a QoS policy.
- 4 Click Add to add a QoS policy.
- **5** STOP. This procedure is complete.

8.1.4 Security configuration

The A-020W-A CPE also supports security configuration, including:

- firewall
- MAC filter
- IP filter
- URL filter

- parental control
- DMZ and ALG
- access control

Procedure 23 Firewall configuration

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



Figure 28 **Firewall window**

> Firewall security applies only to services provided by the A-020W-A CPE. Internet access from the LAN side is not affected by this firewall.

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

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

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

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

Table 26 describes the fields in the firewall window.

Table 26Firewall parameters

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

- 2 Configure the firewall.
- 3 Click Save.
- **4** STOP. This procedure is complete.

Procedure 24 MAC filter configuration

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

Figure 29 MAC filter window

NOKIA	Ethernet Gateway		Logout	English Español
	Security>MAC Filter			
[≇] Status [≇] Network	Ethernet Interface			
Firewall	MAC Filter Mode	Allowed		Y
MAC Filter	LAN Port	LAN1 LAN2		
IP Filter URL Filter	MAC Address	Custom settings		Y
Parental Control		e.g: D0:54:2D:00:00:00		
DMZ and ALG Access Control		Save		
Application				
Maintenance	M	ac Address		Delete
_		Refresh		
	Wi-Fi SSID			
	MAC Filter Mode	Allowed		⊻
	SSID Select	SSID1		\checkmark
	Enable			
	MAC Address	Custom settings		
		e.g: D0:54:2D:00:00:00		
		Save		
	M	ac Address		Delete
		Refresh		

Table 27 describes the fields in the MAC filter window.

Table 27MAC filter parameters

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

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

Procedure 25 IP filter configuration

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

Figure 30 IP filter window

NOKIA	Ethernet Gateway					Logout	English	<u>Español</u>		
	Security>IP	Filter								
●Status ●Network	Enable	IP Filter								
Security	Mode				Drop for ups	tream				~
Firewall	Internal	Client			Custom sett	ings				~
MAC Filter	Local IP Address									
URL Filter	Source	Source Subnet Mask								
Parental Control	Remote	IP Addres	s							
DMZ and ALG Access Control	Destinat	Destination Subnet Mask								
Application	Protoco	Protocol			ALL					~
Maintenance	Mode	Internal Client	Protocol	Local IP Address	Source Subnet Mask	Remote IP Address	Destination Subnet Mask	Wan Port Range	Lan Port Range	Delete
·					Save	Refres	h			

Table 28 describes the fields in the IP filter window.

Table 28IP filter parameters

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

- 2 Configure the IP filter.
- 3 Click Add.
- 4 STOP. This procedure is complete.

Procedure 26 URL filter configuration

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

Figure 31 URL Filter window

NOKIA	Ethernet Gateway		Logout	English Español
	Security>URL Filter			
Status Network Security	URL Filter please select URL filters. Enable URL filter	t the type of fi	Iter and then configure the URL.	Support up to 100
MAC Filter	ORL miler type.	BIOCK	CAllow	
URL Filter	URL List			
Parental Control DMZ and ALG Access Control	URL Address		Port Number	Delete
 Application Maintenance RG Troubleshooting 	URL Address Port – default to 80		Add Filter	



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

Table 29 describes the fields in the URL Filter window.

Table 29	URL Filter parameters
----------	-----------------------

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

- 2 Configure the URL Filter.
- 3 Click Add Filter.
- 4 STOP. This procedure is complete.

Procedure 27 Parental control

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

Figure 32 Parental Control window

NOKIA	Ethernet Ga	teway			Lo	ogout	Englis	<u>h Españ</u>	<u>ol</u>
	Security>Parental Con	itrol							
Status Network Security Firewall MAC Filter	Block access o addresses	of LAN de	vices	at given times, a	according	g to th	neir MAC	or IPv	/4
IP Filter URL Filter Parental Control	Access Control]							
DMZ and ALG	Policy Name	Device	IP	Days Of Week	From	То	Delete	Edit	Enable
Access Control Application Maintenance RG Troubleshooting									+

Table 30 describes the fields in the Parental Control window.

Table 30Parental control parameters

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

- 2 Select the Access Control check box.
- **3** Click the plus sign (+) to add a policy.

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

- 4 Configure the parental control policy.
- **5** Click Enable to activate the policy.
- 6 STOP. This procedure is complete.

Procedure 28 DMZ and ALG configuration

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

Figure 33 DMZ and ALG window

FTP 전 TFTP 전 SIP 전 H323 전 RTSP 전 L2TP 전 IPSEC 전 PPTP 전 Save ALG	1
FTP I TFTP I SIP I H323 I RTSP I L2TP I IPSEC I PPTP I Save ALG	1
Save ALG	
	~
Custom settings	~
Save DMZ	
	Custom settings

Table 31 describes the fields in the DMZ and ALG window.

Table 31DMZ and ALG parameters

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

- 2 Configure ALG.
- 3 Click Save ALG.
- 4 Configure DMZ.

- 5 Click Save DMZ.
- **6** STOP. This procedure is complete.

Procedure 29 Access control configuration

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



Note 1 — ACL takes precedence over the firewall policy.

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

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

Figure 34 Access Control window

NOKIA	Ethernet Gateway			Log	gout	English Español
	Security>Access Control					
Status			WAN	LAN	I	
Network			\checkmark			
Security	Trusted Network Enable					
ïrewall	ICMP	Allow		Allow		
AC Filter	IGMP	Allow		Allow	•	
P Filter	Telnet	Allow	\checkmark	Deny	~	
JRL Filter	SSH	Allow		Deny	~	
Parental Control	UTTO	All		Allaur		
DMZ and ALG	nur	Allow		Allow	•	
Access Control	TR-069	Allow	\checkmark	Deny	\checkmark	
Application	HTTPS	Allow		Allow	~	
Maintenance	0570	A.B		Denu		
RG Troubleshooting	SELE	Allow	SETR appear can be se	Deny	20	
		Sava	SFIF access call be se	Refreeb		
		Save		Rendan		
	Trusted Network					
	Source IP Start					
	Source IP End					
			Ad	d		
	Source IP Start		Source I	P End		Delete

Table 32 describes the fields in the Access Control window.

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

Table 32Access control parameters

- 2 Select a WAN connection from the drop-down menu.
- 3 Click to enable or disable Trusted Network.
- 4 Select an access control level for each of the six protocols: ICMP, Telnet, SSH, HTTP, TR-069, and HTTPS for both the WAN and the LAN side.
- 5 Click Save.
- 6 Optionally, add one or more subnet trusted networks.

The maximum number of entries is 32.

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

7 STOP. This procedure is complete.

8.1.5 Application configuration

The A-020W-A CPE also supports application configuration, including:

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

Procedure 30 Port forwarding configuration

1 Select Application > Port forwarding from the top-level menu in the Ethernet Gateway window, as shown in Figure 35.

Figure 35 Port forwarding window

NOKIA	Ethernet Gateway					Logout English Español				
	Application>Port Forwa	arding								
Status			Custo	m settings						
Network	Application Name	WAN Port								
Security	WAN Port				~					
Application	LAN Port					~				
Port Forwarding	lateral Olivert		Custo	m sottings						
Port Triggering	Protocol		Cusic	in settings						
DDNS			TCP						~	
NTP	Enable Mapping									
UPNP and DLNA	WAN Organities Li								V	
Maintenance	WAN Connection Li	st							•	
RG Troubleshooting				Ad	d					
	Application	WAN	WAN	LAN	Device	Internal		_		
	Name	Connection	Port	Port	Name	Client	Protocol	Status	Delete	

Table 33 describes the fields in the port forwarding window.

Table 33Port forwarding parameters

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

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

Procedure 31 Port triggering

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

Figure 36 Port Triggering window

NOKIA	Ethernet G	Ethernet Gateway					English E		
	Application>Port Trig	gering							
Status Network	Application Name		C	ustom settings					~
Security	Open Port					~			
Application	Triggering Port					~			
Port Forwarding Port Triggering	Expire Time		6	00	(
DDNS	Open Protocol		(Ra T	nge:1~999999) CP	(seconds)				~
NTP UPNP and DLNA	Trigger Protocol		Т	CP					~
Maintenance	Enable Triggering								
RG Troubleshooting	WAN Connection	List							~
				Ad	d				
	Application Name	WAN Connection	Open Port	Triggering Port	Expire Time	Open Protocol	Trigger Protocol	Status	Delete

Table 33 describes the fields in the Port Triggering window.

Table 34Port triggering parameters

Field	Description
Application Name	Choose an application name from the drop-down menu

(1 of 2)

Field	Description	
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 check box to enable port triggering	
WAN Connection List	Choose a WAN connection from the drop-down menu Note: only active devices are shown on this menu	

(2 of 2)

- 2 Configure port triggering.
- 3 Click Add.
- **4** STOP. This procedure is complete.

Procedure 32 DDNS configuration

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

Figure 37 DDNS window

	Ethernet Gateway	Logout Englis	sh Español
A	Application>DDNS		
Status Network	WAN Connection List		V
Security	Enable DDNS		
Application	ISP	DynDNS.org	~
Port Forwarding Port Triggering	Domain Name		
DDNS	Username		
NTP UPNP and DLNA	Password		
Maintenance		Save Refresh	
RG Troubleshooting			

Table 35 describes the fields in the DDNS window.

Table 35DDNS parameters

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

2 Configure DDNS.

- 3 Click Save.
- 4 STOP. This procedure is complete.

Procedure 33 NTP configuration

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

NOKIA	Ethernet Gateway			Logout	English Español
	Application>NTP				
tatus etwork	Enable NTP Service				
ecurity pplication		Save	Refresh		
t Forwarding					
t Triggering NS					
)					
NP and DLNA aintenance G Troubleshooting					

- 2 Select the Enable NTP Service check box.
- 3 Click Save.
- 4 STOP. This procedure is complete.

Procedure 34 UPnP and DLNA configuration

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

Figure 39 UPnP and DLNA window

NOKIA	Ethernet Gateway		Logout	English Español
	Application>UPNP and DLNA			
●Status				
Network	UPnP/DLNA			
Security	Enable UPnP/DLNA			
Application		Save/Apply		
Port Forwarding		,		
Port Triggering				
DDNS				
NTP				
UPNP and DLNA				
Maintenance				
RG Troubleshooting				

- 2 Select the Enable UPnP check box to enable UPnP.
- 3 Click Save/Apply.
- 4 STOP. This procedure is complete.

8.1.6 Maintenance

The A-020W-A CPE supports maintenance tasks, including:

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

- restore factory defaults
- diagnostics
- log

Procedure 35 Password configuration

A password must adhere to the following password rules:

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

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

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

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

- the first character cannot be a special character
- there are not enough character classes
- 1 Select Maintenance > Password from the top-level menu in the GPON Home Gateway window, as shown in Figure 40.

Figure 40 Password window

Maintenance>Password Status Network Security Application Maintenance Password Prompt Message Save Refresh Save Refresh Save Refresh	NOKIA	Ethernet Gateway	Logout English Español
Status Network Security Re-enter Password Application Prompt Message Maintenance Password Save Refresh Save Refresh		Maintenance>Password	
Password Save Refresh Device Management Backup and Restore Firmware Upgrade Reboot Device Factory Default Diagnostics Log	Status Network Security Application Maintenance	New Password Re-enter Password Prompt Message	
Device Management Backup and Restore Firmware Upgrade Firmware Upgrade Factory Default Diagnostics Log RG Troubleshooting	Password		Save Refresh
	Device Management Backup and Restore Firmware Upgrade Reboot Device Factory Default Diagnostics Log RG Troubleshooting		

Table 36 describes the fields in the password window.

Table 36Password parameters

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

- 2 Configure the new password.
- 3 Click Save.
- 4 STOP. This procedure is complete.

Procedure 36 Device management

1 Select Maintenance > Device Management from the top-level menu in the Ethernet Gateway window, as shown in Figure 41.

Figure 41 Device Management window

NOKIA	Ethernet Gateway	Logout	English Español
	Maintenance>Device Management		
●Status		01/00/2077N0	
Network	Host Name	CV0042077N0	
●Security	Host Alias		
Application		Add	
Maintenance		Adu	
Password			
Device Management			
Backup and Restore			
Firmware Upgrade	Host Name	Host Alias	Delete
Reboot Device			
Factory Default		Refresh	
Diagnostics			
Log			
RG Troubleshooting			

Table 37 describes the fields in the Device Management window.

Table 37Device Management parameters

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

- 2 Configure an alias for a specific host.
- 3 Click Add.
- 4 STOP. This procedure is complete.

Procedure 37 Backup and Restore

1 Select Maintenance > Backup and Restore from the top-level menu in the Ethernet Gateway window, as shown in Figure 42.

Figure 42 Backup and Restore window

NOKIA	Ethernet Gateway	Logout English Español
	Maintenance>Backup and Restore	
●Status	Select File	Choose file No file chosen
*Network	Import Config File	Import
	Furgert Config File	Export
Maintenance	Export Config File	Export
Password		
Device Management		
Backup and Restore		
Reboot Device		
Factory Default		
Diagnostics		
Log		
and mobileshooting		

- 2 Click Select File and choose the backup file.
- 3 Click Import Config File to restore the A-020W-A CPE to the saved backup or click Export Config File to export the current configuration to the backup file.
- 4 STOP. This procedure is complete.

Procedure 38 Upgrade firmware

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

Figure 43 Firmware Upgrade window

NOKIA	Ethernet Gateway	Logout English Español
	Maintenance>Firmware Upgrad	e
●Status	Select File	Choose file No file chosen
≝Network ≇Security	Upgrade	Upgrade
Application		
Password		
Device Management		
Backup and Restore Firmware Upgrade		
Reboot Device		
Factory Default		
Diagnostics Log		
RG Troubleshooting		

- 2 Click Select File and choose the new firmware file.
- **3** Click Upgrade to upgrade the firmware.
- 4 STOP. This procedure is complete.

Procedure 39 Reboot

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

Figure 44 Reboot Device window

NOKIA	Ethernet Gateway		Logout	English Español
	Maintenance>Reboot Device			
●Status		Debo	vot	
Network		Rebu		
Security				
Application				
Maintenance				
Password				
Device Management				
Backup and Restore				
Firmware Upgrade				
Reboot Device				
Factory Default				
Diagnostics				
Log				
■RG Troubleshooting				

- 2 Click Reboot to reboot the A-020W-A CPE.
- **3** STOP. This procedure is complete.

Procedure 40 Restore factory defaults

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

Figure 45 Factory Default window

NOKIA	Ethernet Gateway	Logout Eng	<u>ilish Español</u>
	Maintenance>Factory Default		
●Status		Factor: Default	
Network		Factory Delault	
●Security			
Application			
Maintenance			
Password			
Device Management			
Backup and Restore			
Firmware Upgrade			
Reboot Device			
Factory Default			
Diagnostics			
Log			
RG Troubleshooting			

- 2 Click Factory Default to reset the A-020W-A CPE to its factory default settings.
- **3** STOP. This procedure is complete.

Procedure 41 Diagnose connections

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

Figure 46 Diagnostics window

NOKIA	Ethernet Gateway		Logout	English Español
	Maintenance>Diagnostics			
Status Network Security Application Maintenance Password Device Management	WAN Connect List IP or Domain Name Test Ping Try Times(1 ~ 1000) Packet Length(64 ~ 1500)	LAN/WAN Interface	9	
3ackup and Restore Firmware Upgrade Reboot Device Factory Default	Max no. of trace hops(1 ~ 255)	30 Start Test	Cancel	
Diagnostics Log ≹RG Troubleshooting				

- 2 Choose a WAN connection to diagnose from the drop-down menu.
- 3 Enter the IP address or domain name.
- 4 Select the test type: ping, traceroute, or both.
- **5** Enter the number of ping attempts to perform (1 to 1000); the default is 4.
- 6 Enter a ping packet length (64 to 1500); the default is 64.
- 7 Enter the maximum number of trace hops (1 to 255); the default is 30.
- 8 Click Start Test. Results will be displayed at the bottom of the window.

- 9 Click Cancel to cancel the test.
- **10** STOP. This procedure is complete.

Log window

Procedure 42 View log files

Figure 47

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

NOKIA	Ethernet Gateway	Logout English Espa	añol	
1	Maintenance>Log			
Status		Error		
Network	whiting Level	LIG	×	
Security	Reading Level	Error	\checkmark	
Application	Manufacturer:ALCL		_	
Maintenance	ProductClass:HA-020W-A			
ssword	HWVer:3FE47239AAAA			
evice Management	SWVer:3FE473360.00			
ackup and Restore	IP:192.168.18.1			
mware Upgrade	1970-01-01 00:00:18[al]BMT start at bl	lock 1885		
boot Device	1970-01-01 00:00:18[al]show last inde: 1970-01-01 00:00:18[al]assigned size	x 0xe000000 chip size eba0000		
ctory Default	1970-01-01 00:00:18[al]PROC INIT OF	</td <td></td>		
agnostics	1970-01-01 00:00:18[al]button_task_init: btn_get_cfgtbl success 1970-01-01 00:00:18[al]btn_event_task_init: success			
9	1970-01-01 00:00:18[em]igmpmap Igm	npMapFilterConfig IPTV Filter mode changed from 1 to 5 ^M		
RG Troubleshooting	1970-01-01 00:00:29[em]dhcp_cond_ft 1970-01-01 00:01:16[em]iampbl hal ke	lag: 0, dhcp_pool_iptv_count: 0 ernel_create_vlan_entrv_id:787LogicPort:class(0=Eth)id(2)create	e entrvld(42 💙	
•			and a state of the	

- 2 Choose a write level from the drop-down menu to determine which types of events are recorded in the log file:
 - Emergency
 - Alert
 - Critical
 - Error
 - Warning
 - Notice
 - Informational
 - Debug

- 3 Choose a reading level from the drop-down menu to determine which types of events to display from the log file:
 - Emergency
 - Alert
 - Critical
 - Error
 - Warning
 - Notice
 - Informational
 - Debug
- 4 The log file is displayed at the bottom of the window.
- 5 STOP. This procedure is complete.

8.1.7 RG troubleshooting counters

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

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

Procedure 43 Retrieve Residential Gateway (RG) troubleshooting counters

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

The RG Troubleshooting Counters window appears; see Figure 48.

ubleshooting>RG Trout IN Connection List Throughput Throughput Packet Loss Packet Loss ernet Status	bleshoot Counter	5		US-Spe DS-Spe	eedTest
IN Connection List Throughput Throughput Packet Loss Packet Loss ernet Status				US-Spe DS-Spe	eedTest
Throughput Throughput Packet Loss Packet Loss ernet Status				US-Spe DS-Spe	edTest
Throughput Packet Loss Packet Loss ernet Status				DS-Spe	redTest
Packet Loss Packet Loss armet Status					
ernet Status					
ency					LatencyTest
S Response Time rt Mirror					DNSResponseTest
urce Port	Destination Port		Direction		Status
WAN 💌	LAN1		Downstream	n 🔽	Enable 💌
		Sav	/e		
Source Port	Des	tination Por	rt	Direction	n Delete
	rt Mirror urce Port VAN 💌 Source Port	rt Mirror Urce Port Destination Port VAN Source Port Des	rt Mirror Urce Port Destination Port VAN V LAN1 V Sau Source Port Destination Po	rt Mirror urce Port Destination Port Direction VAN LAN1 Downstream Save Source Port Destination Port	rt Mirror urce Port Destination Port Direction VAN V LAN1 V Downstream V Save Source Port Destination Port Direction

Figure 48 RG Troubleshooting Counters window

Table 38 describes the fields in the RG Troubleshooting Counters window.

Table 38 RG Troubleshooting Counters parameters

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

(1 of 2)

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

(2 of 2)

- **2** Configure the test times if desired.
- **3** Click Refresh to update the data.
- **4** STOP. This procedure is complete.

Customer document and product support

Customer documentation

Customer Documentation Welcome Page



Technical Support

Customer Documentation Technical Support



Documentation feedback

Customer Documentation Feedback

Copyright 2018 Nokia. 3FE-47511-AAAA-TCZZA