

User Manual

COVER

WR315GR-2C-LTE6-GAX-EC

Industrial Secure Cellular Router, 2C (Dual Core), WLAN 6 + LTE 6-G, EC OS

EC OS Web interface and SSH commands
Aug.2026 V1.3g

Original version:

WR315GR-M2 Series

Industrial Secure Cellular Router, 2C (Dual Core) Series

WoMaster

WR315GR –M2 Series WR315GR-2C-LTE6-GAX-EC

Industrial Secured Cellular Router, 2C (Dual Core) Series

User Manual

Copyright Notice

© WoMaster. All rights reserved.

About This Manual

This user manual is intended to guide a professional installer to install and to configure the WoMaster Industrial Secured and Rugged LTE Serial Router. It includes procedures to assist you in avoiding unforeseen problems.

NOTE:

Only qualified and trained personnel should be involved with installation, inspection, and repairs of this router.

Disclaimer

WoMaster reserves the right to make changes to this Manual or to the product hardware at any time without notice. Information provided here is intended to be accurate and reliable. However, it might not cover all details and variations in the equipment and does not claim to provide for every possible contingency met in the process of installation, operation, or maintenance. Should further information be required or should particular problem arise which are not covered sufficiently for the user's purposes, the matter should be referred to WoMaster. Users must be aware that updates and amendments will be made from time to time to add new information and/or correct possible unintentional technical or typographical mistakes. It is the user's responsibility to determine whether there have been any such updates or amendments of the Manual. WoMaster assumes no responsibility for its use by the third parties.

WoMaster Online Technical Services

At WoMaster, you can use the online service forms to request the support. The submitted forms are stored in server for WoMaster team member to assign tasks and monitor the status of your service. Please feel free to write to help@womaster.eu if you encounter any problems.

TABLE OF CONTENTS

COVER	1
TABLE OF CONTENTS	3
DECLARATION OF CONFORMITY	5
SAFETY PRECAUTION	11
PROFESSIONAL INSTALLATION PRECAUTION	13
1. INTRODUCTION	14
1.1 OVERVIEW	14
1.2 MAJOR FEATURES	15
2. HARDWARE INSTALLATION	16
2.1 HARDWARE DIMENSION	16
2.2 INSTALLATION	19
2.3 WIRING THE POWER INPUTS	19
2.4 WIRING THE ALARM RELAY OUTPUT (DO)	20
2.5 CONNECTING THE GROUNDING SCREW	20
2.6 DIN RAIL MOUNTING	21
2.7 OPTIONAL ANTENNA	22
2.9 HARDWARE WATCHDOG	26
2.10 LED INDICATION	27
3. WR315G-2C-LTE6-GAX-EC EC OS INTRODUCTION	28
3.1 EC OS SOFTWARE SPECIFICATION:	28
3.2 WR315G-2C-LTE6-GAX-EC QIG	29
3.3 PREPARATION FOR MANAGEMENT	35
3.4 LUCI WEB MANAGEMENT	39
3.4.1 STATUS	39
3.4.2 SYSTEM	45
3.4.2.1 System → System	45
3.4.2.2 System → Administration	46
3.4.2.3 System → Flash Operation	47
3.4.2.4 System → Reboot	51
3.4.2.5 Advanced Settings:	52
3.4.3 Network	53
3.4.3.1 Interfaces	53
3.4.3.2 Wireless(Wi-Fi)	59

3.4.4.3 Routing	63
3.4.4.4 DHCP and DNS	64
3.4.4.5 Diagnostics	66
3.4.4.5 Firewall	67
3.4.4 Services/Watchcat	71
3.4.5 VPN.....	72
4. SSH Management	73
4.1 LOGIN THE ROUTER THROUGH SSH	73
4.2 MAJOR OPENWRT CLI	76
4.2.1 CLI - Cellular	76
4.2.2 CLI- lan	80
4.2.3 CLI – WIFI(Wireless)	81
4.3 CUSTOMIZED CLI & SCRIPT.....	84
4.3.1 Get Information Script: <i>wr-info-get.sh</i>	84
4.3.2 Wireless Operation Mode Script: <i>wr-wireless-mode.sh</i>	88
4.3.3.1 Network Ping Alarm.....	89
4.3.3.2 Hardware Condition Alarm	91
4.3.3.3 Reading Alarm Status	94
4.4 FIRMWARE UPGRADE	95
4.5 CONFIGURATION BACKUP/RESTORE	99
4.6 RESET TO DEFAULT	100
5. REVISION HISTORY	101

Declaration of Conformity

CE RED (Radio Device Directive)

While you see the CE Marking print in our product, it indicates the product conform to the requirement of the CE RED.

We provide the CE RED Declaration of Conformity (DoC) for our Wireless Router products in our web site. The DoC includes the Brand Name, Product Name, Model Name, Description, compliant standards and Manufacture information. Different product may conform to different standards of Safety, Health, EMC, Radio and other specific standard. You can download the formal document of the product in our Web site or apply from our Sales/Technical people.

The DoC in this product manual applied to below models:

Brand Name: **WoMaster**

Product Name: **Industrial Grade Dual-Core Secure 5GNR/LTE Router**

Model Name: **WR315GR-2C-M2**

Serial Model Name: **WR315GR-2C-5GM2-EU, WR315GR-2C-5GM2-GL,
WR315GR-2C-LTE6-GAX-EC, WR315GR-2C-LTE6, WR315GR-2C-LTE**

Compliant Standard:

Safety: EN IEC 62368-1

EMC: EN301489-1/17/52, EN50121-4

MPE: EN IEC 62311

RF(By Module): EN301908-1/2/13, EN300328, EN301893

The declaration of CE RED is authorized at the following company and address.

WoM ASIA CO., LTD

(Manufacturer Name)

13F, No.190, Sec.2, Zhongxing Rd., Xindian Dist., New Taipei 231, Taiwan

(Manufacturer Address)

I. U.S. Federal Communications Commission (FCC)

Model Name: WR315GR-2C-LTE6-GAX-EC

FCC ID: 2AXAMWR315GM2

Contains Transmitter Module FCC ID: 2AXAM8XM0004

FCC Part 15 Compliance

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

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Class A Digital Device Notice

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC RF Exposure Compliance

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirement, please follow operation instruction as documented in this manual.

Radiation Exposure Statement:

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

II. Innovation, Science and Economic Development Canada (ISED)

ISED (IC Certification Information)

English	Français (French)
Model: WR315GR-2C-LTE6-GAX-EC	Modèle: WR315GR-2C-LTE6-GAX-EC

Contains Transmitter Module IC ID: 34378-WR315GRLTE6, 34378-WR315GRGAX

Industry Canada ICES-003 Compliance:

This Class A digital apparatus complies with Canadian ICES-003. **CAN ICES-003 (A)/NMB-003 (A)**

Avis de conformité à la réglementation d'Industrie Canada : Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

ISED Compliance Statement

English (ISED Standard Statement)	Français (Déclaration ISED Standard)
This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.	L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage; (2) l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

ISED RF Exposure Compliance (RSS-102)

English	Français
This equipment complies with ISED RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.	Cet équipement est conforme aux limites d'exposition aux radiations ISED CNR-102 établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps.

Transmitter Antenna Information (RSS-Gen Section 6.8)

This radio transmitter **IC:** 34378-WR315GRLTE6, 34378-WR315GRGAX has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated for each antenna type. Antenna types not included in this list, having a gain greater than the maximum gain

indicated for any type listed, are strictly prohibited for use with this device.

Français

Le présent émetteur radio **IC**: 34378-WR315GRLTE6, 34378-WR315GRGAX a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste sont strictement interdits pour l'exploitation de cet appareil.

Note: Although the antenna datasheet specifies a frequency range of 5150–7125 MHz, the device's transmitter is firmware-locked to operate strictly within the 5150–5850 MHz band. **Remarque :** Bien que la fiche technique de l'antenne indique une plage de fréquences de 5150 à 7125 MHz, l'émetteur de l'appareil est verrouillé par micrologiciel pour fonctionner uniquement dans la bande 5150 à 5850 MHz.

III. Operation and Installation Restrictions

5 GHz Operation Restriction (FCC §15.407(e) / RSS-247 Clause 7.3.7(c))

English (Mandatory Restriction)	Français (Restriction Obligatoire)
Indoor Use Requirement: Any device capable of operating in the band 5150–5250 MHz shall only be used indoors to reduce the potential for harmful interference to co-channel mobile satellite systems (this requirement does not apply to OEM devices installed in vehicles by vehicle manufacturers).	Exigence d'utilisation à l'intérieur : Les dispositifs fonctionnant dans la bande 5150–5250 MHz sont réservés uniquement à une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux (cette exigence ne s'applique pas aux dispositifs OEM installés dans des véhicules par les constructeurs automobiles).
Antenna Gain (5250–5350 MHz and 5470–5725 MHz): For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250–5350 MHz and 5470–5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.	Gain d'antenne (5250–5350 MHz et 5470–5725 MHz) : Pour les dispositifs munis d'antennes détachables, le gain d'antenne maximal autorisé pour les dispositifs dans les bandes 5250–5350 MHz et 5470–5725 MHz doit être conforme à la limite de p.i.r.e.
Antenna Gain (5725–5850 MHz): For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725–5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate.	Gain d'antenne (5725–5850 MHz) : Pour les dispositifs munis d'antennes détachables, le gain d'antenne maximal autorisé pour les dispositifs dans la bande 5725–5850 MHz doit être conforme aux limites de p.i.r.e. applicables.
Elevation Mask Compliance: Where	Conformité au masque d'élévation : Le cas

applicable, antenna type(s), antenna model(s), and worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in section 7.3.2.4 or 7.3.5.3 shall be clearly indicated.	échéant, les types d'antennes, les modèles d'antennes et les angles d'inclinaison dans le pire des cas nécessaires pour rester conforme à l'exigence de la p.i.r.e. relative au masque d'élévation énoncée à la section 7.3.2.4 ou 7.3.5.3 doivent être clairement indiqués.
--	--

Installer Compliance Responsibility (KDB 353028 D01 Compliant)

Model WR315GR-2C-LTE6-GAX-EC is restricted to professional installation only.

Professional Installation Requirement: This device is restricted to **Professional Installation** only.

1. Distribution Channel: The equipment is intended for industrial and commercial applications and is marketed and sold only through authorized distributors and system-integrator partners; it is not sold through general retail channels or directly to the general public.
2. Installation Expertise: Installation and configuration must be performed by trained professional installers who are familiar with RF planning and local regulatory requirements.
3. Antenna Restriction:
 - Any antenna substitution or replacement must be performed by a professional installer.
 - The professional installer is responsible for ensuring that the chosen antenna type and gain, when combined with the device's output power settings, results in an Equivalent Isotropically Radiated Power (EIRP) that remains compliant with local FCC and ISSED regulatory limits.
 - End-users are prohibited from replacing the antenna or adjusting antenna-related configuration parameters.
4. Installer Responsibility: The professional installer is responsible for ensuring that the device is operated in accordance with local country regulatory requirements, including antenna selection, output power settings, and permitted operating frequency bands.
5. End-User Control Restriction: End-users do not have access to controls that could change the operational parameters of the device (such as antenna gain or output power) that would violate FCC and ISSED regulatory compliance.

Le modèle WR315GR-2C-LTE6-GAX-EC est réservé à une installation professionnelle.

Exigence d'installation professionnelle : Cet appareil est limité à une installation professionnelle uniquement.

1. Canal de distribution (Distribution Channel) : L'équipement est destiné aux applications industrielles et commerciales et est commercialisé et vendu uniquement par l'intermédiaire de distributeurs agréés et de partenaires intégrateurs de systèmes ; il n'est pas vendu par les canaux de vente au détail généraux ni directement au grand public.
2. Expertise en installation (Installation Expertise) : L'installation et la configuration doivent être effectuées par des installateurs professionnels formés qui connaissent la planification des radiofréquences (RF) et les exigences réglementaires locales.
3. Restriction relative à l'antenne (Antenna Restriction) :
 - Toute substitution ou remplacement d'antenne doit être effectué par un installateur professionnel.

- L'installateur professionnel est responsable de s'assurer que le type d'antenne et le gain choisis, lorsqu'ils sont combinés aux réglages de puissance de sortie de l'appareil, entraînent une puissance isotrope rayonnée équivalente (PIRE) qui reste conforme aux limites réglementaires locales de la FCC et de l'ISDE.
 - Il est interdit aux utilisateurs finaux de remplacer l'antenne ou de modifier les paramètres de configuration liés à l'antenne.
4. Responsabilité de l'installateur (Installer Responsibility) : L'installateur professionnel est responsable de s'assurer que l'appareil est utilisé conformément aux exigences réglementaires du pays local, y compris la sélection de l'antenne, les réglages de puissance de sortie et les bandes de fréquences de fonctionnement autorisées.
 5. Restriction du contrôle par l'utilisateur final (End-User Control Restriction) : Les utilisateurs finaux n'ont pas accès aux commandes qui pourraient modifier les paramètres opérationnels de l'appareil (tels que le gain de l'antenne ou la puissance de sortie) qui violeraient la conformité réglementaire de la FCC et de l'ISDE.

SAFETY PRECAUTION

- **Statement regarding restricted access:**  The equipment is intended to be used in a restricted access location. Access should only be given to skilled person or instructed person who has been trained in the operation of the equipment and informed of the potential hazards.
- **Power Specification:** Follow the power installing instruction of the user manual, it indicates the available input voltage range, V+/V- pin assignment, power consumption and other notice. Only operate the device within the specified input voltage range as indicated in the user manual and the device label.



Connecting power with reverse polarity or using the wrong type of power supply may damage the equipment. Make sure that the power supply is connected correctly and of the recommended type.

- **Disconnect Device:** A readily accessible disconnect device (such as a circuit breaker or switch) shall be incorporated in the building installation wiring for permanently connected equipment.
- **Overcurrent Protection:** To ensure protection against short circuits and fire hazards in the supply circuit, it is recommended to install an external fuse or circuit breaker rated at 2A (for 24V) or 3A (for 12V) on the power input line.
- **Switch ON Notice:** Only switch on the supply voltage after verifying that the housing is closed, the input voltage is correct, and the terminal blocks are wired correctly.
- **Grounding:** To avoid system damage, the equipment should be connected to ground. Reliable grounding is essential for EMC compliance and safety. Ensure the equipment is properly connected to the protective earth (PE) ground before connecting the power supply. Use a grounding wire with a minimum cross-sectional area of 18 AWG. For better EMC performance (noise immunity), a thicker and shorter grounding wire is recommended.
- **Wiring:** Use connection cables that are rated for the specified voltage, current, wire diameter, and temperature range. For reliable data transmission in harsh environments, use high-quality industrial-grade RJ45 connectors to prevent signal loss or intermittent connection.

Note for PoE application (if used): If the equipment is installed in a PoE (Power over Ethernet) environment (e.g., using a PoE splitter), use high-quality industrial-grade RJ45 connectors. In harsh environments, inferior quality plugs may cause arcing, short circuits, or damage to the PD (Powered Device).



- **Hot Surface Warning: Caution:** The metal housing may become very hot during operation (especially when PoE power is supplied), avoid touching the surface directly. Allow the equipment to cool down before handling or maintenance.

- **Mounting:**  The equipment is only suitable for mounting at height $\leq 2\text{m}$.
- **Environment:** Only operate the device at the specified ambient temperature and humidity. Do not expose the device to rain or moisture unless it is rated for such environments.
- **SIM Card:**  **Caution:** Disconnect the power supply before removing the SIM cover or inserting/removing the SIM card.
- **SIM Card:**  Ensure that the SIM card is installed correctly to avoid damage to the SIM card or the router.
The SIM cover must be mounted again before power is reapplied.
- **NOT allow to open the housing:** There are no user-serviceable parts inside. Only technicians authorized by the manufacturer are permitted to service the equipment.

Professional Installation PRECAUTION

Notice on Professional Installation:

WOM ASIA CO., LTD. hereby states that the products bearing FCC ID **2AXAMWR315GM2** (Model: WR315GR-2C-LTE6-GAX-EC) are limited to **professional installation only**. These devices are designed for complex industrial network environments and are not intended for sale to the general public or for installation by untrained individuals.

Proper configuration, optimization, and safe operation require specialized technical knowledge. Improper installation by a non-professional could result in non-compliance with technical standards and regulatory requirements, including potential harmful interference to radio communications.

WOM ASIA CO., LTD will ensure the professional installation of this device through the following measures:

1. **Restricted Sales Channels:** The product is sold exclusively through authorized professional integrators, value-added resellers, and distribution channels that serve the industrial and enterprise markets. Sales to retail outlets or directly to the general public will not be permitted.
2. **Clear Product Labeling:** The products and their packaging will be clearly marked with a product label stating the correct power input range, and the **Quick Installation Guide** will include a more detailed Professional Installation Attestation.
3. **User Manual:** The device's user manual will explicitly state that installation must be performed by a qualified professional. The guide will include specific instructions and warnings to this effect.
4. **Specialized Features:** The device's advanced configuration and optional expansion antenna are not intuitive for end-users and require technical expertise to set up correctly.

1. INTRODUCTION

1.1 OVERVIEW

New industrial high-performance router WR315GR-M2 Series with dual-core 880MHz CPU has a M2 expansion socket for 5G NR Cellular as well as 4G LTE, 3G/2G networks. One Gigabit WAN port and four Gigabit LAN ports provide switch functions as well as WAN redundancy upon cellular networks.

The **WR315GR-2C-LTE6-GAX-EC** series supports LTE Cat.6 and Wi-Fi 6 Client mode for cellular and Wireless LAN connectivity and latest OpenWRT operating system.

Model Name	Description
WR315GR-M2	Industrial Secure Router, Dual Core , 5GbE, 1 Relay, 2SIM, 1x Expansion M2 socket
WR315GR-2C-LTE6-G-EC	Industrial Secure Router, Dual Core, 5GbE, 1 Relay, EC OS, LTE6-G
WR315GR-2C-LTE6-GAX-EC	Industrial Secure Router, Dual Core, 5GbE, 1 Relay, EC OS, 802.11ax WLAN6 client, LTE6-G
	EC OS: Embedded Computing based on OpenWRT OS. Note: The web GUI/SSH command is different than standard WOM OS version, it supports one SIM only. 5G NR/LTE Frequency/Bands: *choose one by region: For other frequency bands not listed, please inquire with our sales. List the available 4G LTE module/region in below *1/2 Serial Port support by request, please inquire with our sales.
© WoMaster Inc. All rights reserved. Specifications are subject to change without notice. Please ask our sales for the most up-to-date product information.	

1.2 MAJOR FEATURES

Below are the major features of WR315GR-2C-LTE6-GAX-EC:

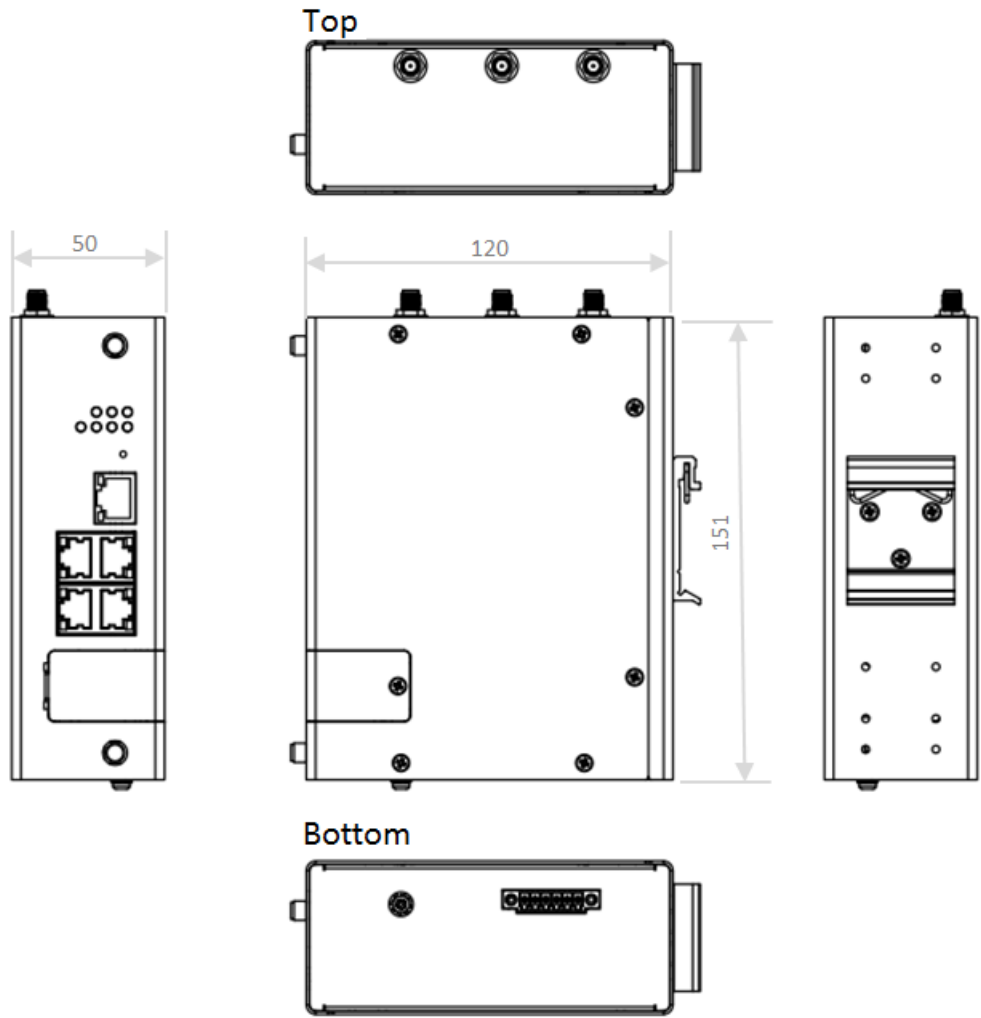
- Dual Core High Speed Processor
- 5 x 100/1000MBase-T RJ45, Auto Negotiation, supports routing mode with 1xWAN and 4xLAN ports
- Extended M2 socket for 4G LTE Cat.6, up to 300Mbps DL speed, backward compatible with 3G
- Supports Wi-Fi 6 Client WAN connectivity, 2.4G/5GHz Wi-Fi 6 station with up to 1800Mbps peak rate
- Support Nano SIM for 4G LTE connectivity
- The **EC OS** version software supports **LTE Cat.6 Global band + Wi-Fi 6 Client mode (Mode with LTE6-GAX-EC)**
 - Features: OpenWRT 23.05, Router mode of 1xWAN+4xLAN, SSH terminal, LuCI web GUI includes System Setting, NTP Setting, Router Password setting with strength check, SSH Access and Key upload, HTTPS, init script startup setting, configuration backup/restore, firmware upgrade, system reboot, watchcat(watchdog), ser2net, Interface configuration, Wi-Fi interface setting, DHCP server/client, DHCP Relay, DNS, firewall setting, static router, Diagnostic Ping, traceroute, Nslookup, Device Status and Mobile Information.
 - WLAN Configuration: Support Wi-Fi Client mode.
WLAN Basic Settings: Radio on/off, mode selection, 2.4G/5G 11ax Band and Frequency selection, SSID, Hide SSID, Wireless Security encryption includes WPA3-SAE and WPA2-PSK/WPA-PSK/Open, advanced WLAN settings, WLAN MAC Filter, 802.11r fast transition
 - Cellular Configuration: Support Modem manager tool for Radio on/off, 4G LTE/3G HSPA Configuration, APN, SIM Security, Connection Status and Cellular diagnostic
- Steel Metal Housing and aluminum heat sinks inside for heat dissipation
- Wide range operating temperature -40~70°C
- Typical 24V (9-48V) power input
- IP30 ingress protection

2. HARDWARE INSTALLATION

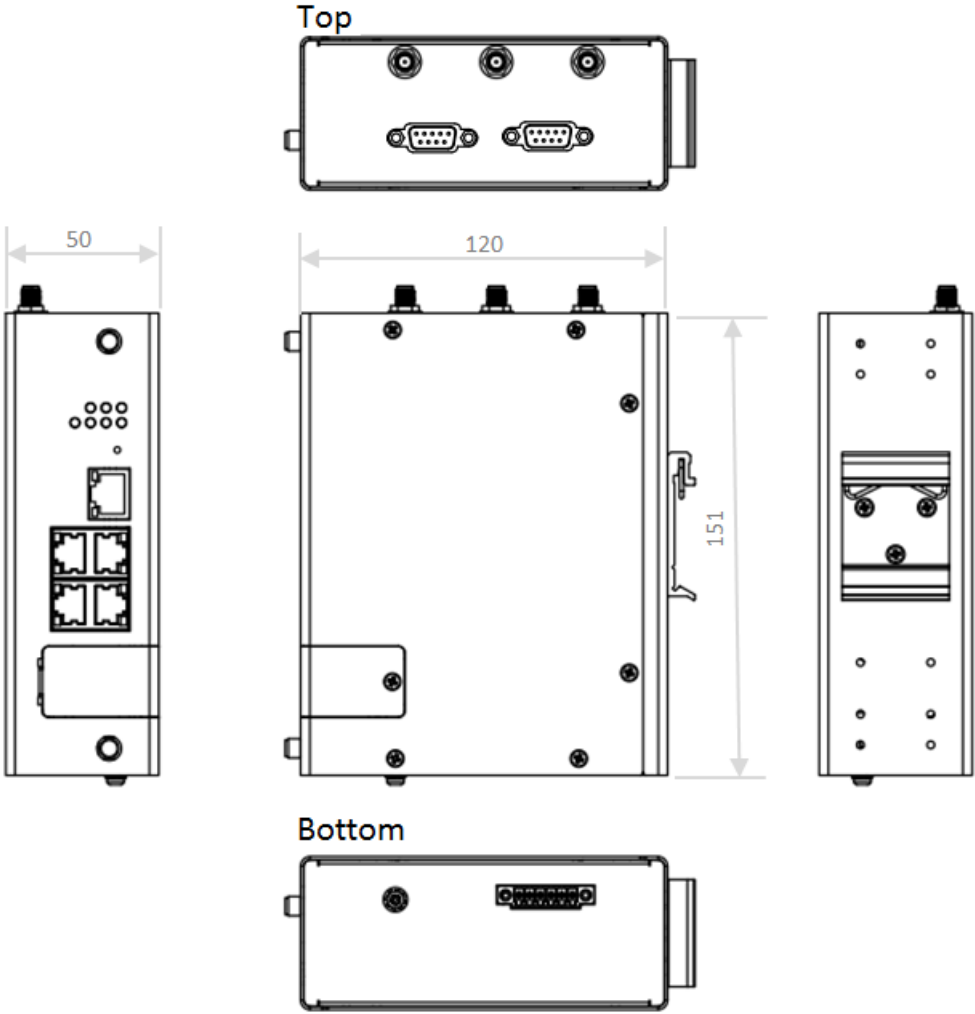
This chapter introduces hardware and contains information on installation and configuration procedures.

2.1 HARDWARE DIMENSION

Dimensions of WR315GR-M2: 50 x 151 x 120 (W x H x D) / without DIN Rail Clip

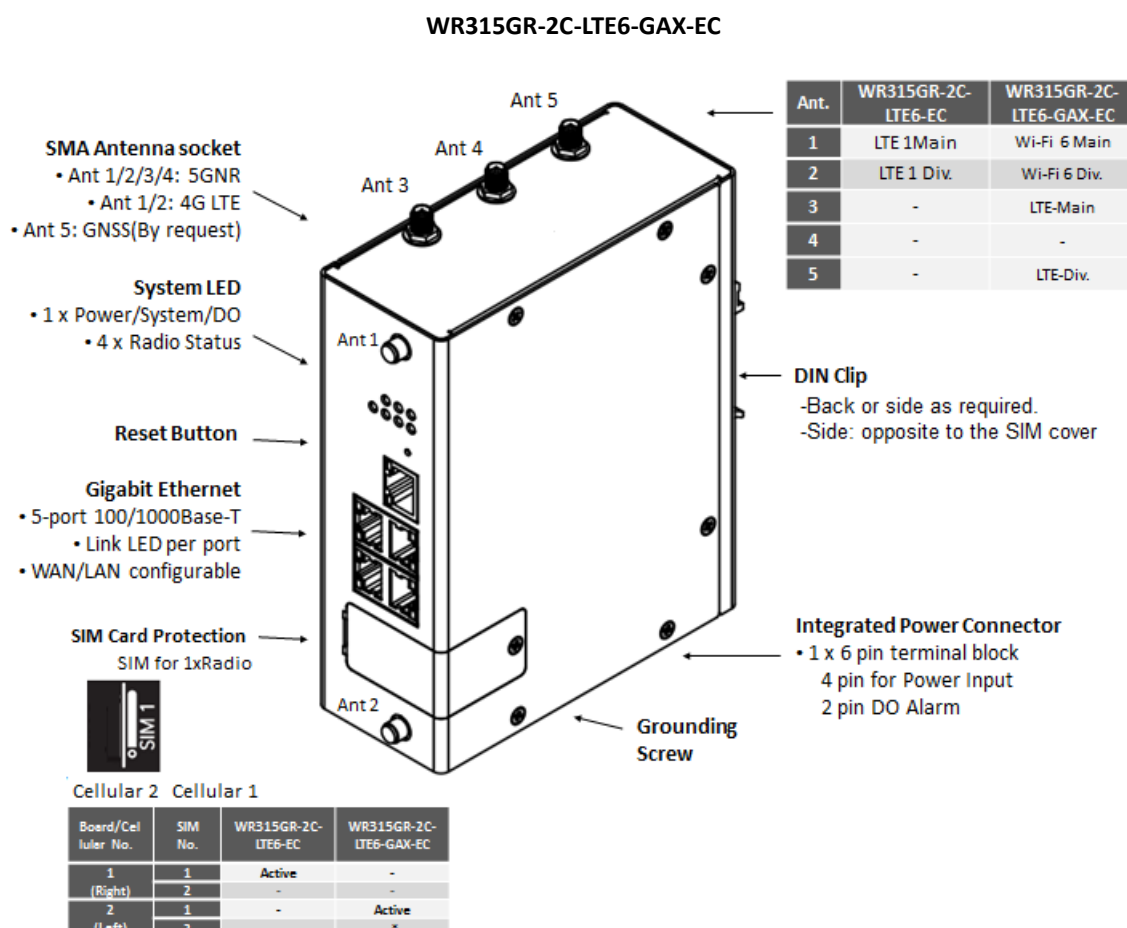


Dimensions of WR315GR-M2+2COM: 50 x 151 x 120 (W x H x D) / without DIN Rail Clip
(Model with 1 or 2 Serial ports)



Front Panel Layout

The front panel from WR315GR routers include 5 ports Giga Ethernet (100/1000 Base-T, RJ45), System + Ethernet + Radio LEDs, Reset button, 1 x 6-pin terminal block connector (4 pin for power inputs and 2 pin for Relay Output) and 1 chassis grounding screw on bottom side. There are 5 SMA antenna sockets, 5G NR connection usually requires 4 antennas, 4G LTE connection usually requires 2 antennas and one is reserved for GPS/GNSS. On the rear side of the device, there is DIN rail clip attached.



Ethernet Port Map:

Port Map	Port Number	Bridge Mode	Router Mode(1xWAN)
	Port 1	LAN	WAN 1 (Default)
	Port 2		LAN
	Port 3		
	Port 4		
	Port 5		

Default port configuration is **Router** Mode in WR315GR-2C-LTE6-GAX-EC, the default IP of the interface LAN ports: 192.168.10.1. Default IP of the interface WAN is DHCP Client

Antenna Map:

	WR315GR-2C-LTE/LTE6-EC	WR315GR-2C-LTE6-GAX-EC
Ant 1	LTE/LTE6 Main	Wi-Fi Main
Ant 2	LTE/LTE6 Div.	Wi-Fi Div.
Ant 3	-	LTE6 Main
Ant 4	-	-
Ant 5	-	LTE6 Div.

Note: *GNSS software by request

Note: Due to the different number of antennas used by 5G NR/4G LTE/3G/2G model, the feature of the antenna number may be different, the unused antenna positions will be covered by caps (even it has no functionality).

Note: If you only connect one antenna, please always connect the Main Ant. With one antenna attached, the connection speed, signal quality, and performance will be affected and cannot be guaranteed.

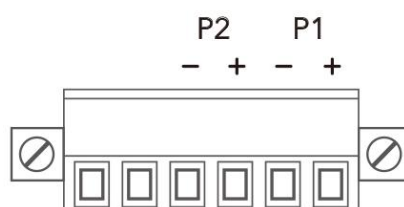
2.2 INSTALLATION

After unpack the box, follow the steps below in order to properly connect the device. For better signal/performance, put the device in a clearly visible spot, as obstacles such as walls and doors hinder the signal.

1. First, assemble router by attaching the necessary antennas and inserting the SIM card.
2. To power up router, please use the qualified power supply, connect the power input and reserved 24V@3A for the router.

2.3 WIRING THE POWER INPUTS

Power Input port in the router provides 2 sets of power input connections (P1 and P2) on the terminal block. On the picture below is the power connector.



Wiring the Power Input

1. Insert the positive and negative wires into the V+ and V- contact on the terminal block connector.
2. Tighten the wire-clamp screws to prevent the power wires from being loosened.
3. Connect the power wires to suitable DC Switching type power supply. The typical input DC voltage is 24V,

range of 9VDC to 48VDC.

WARNING: Turn off DC power input source before connecting the Power to the terminal block connectors, for safety purpose. Don not turn-on the source of DC power before all of the connections were well established.

2.4 WIRING THE ALARM RELAY OUTPUT (DO)

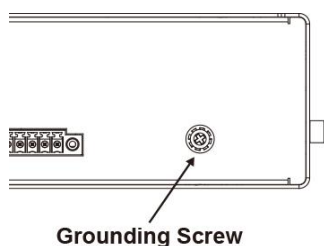
The relay output contacts are located on the front panel of the router. The relay output consists of the 2-pin terminal block connector that used to detect user-configured events. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured event does not occur, the fault circuit remains open. The fault conditions such as Ethernet port link down or other pre-defined events (by customized) which can be configured in the device. Screw the DO wire tightly after digital output wire is connected.



NOTE: The relay contact only supports 1 A current, DC 24V. Do not apply voltage and current higher than the specifications.

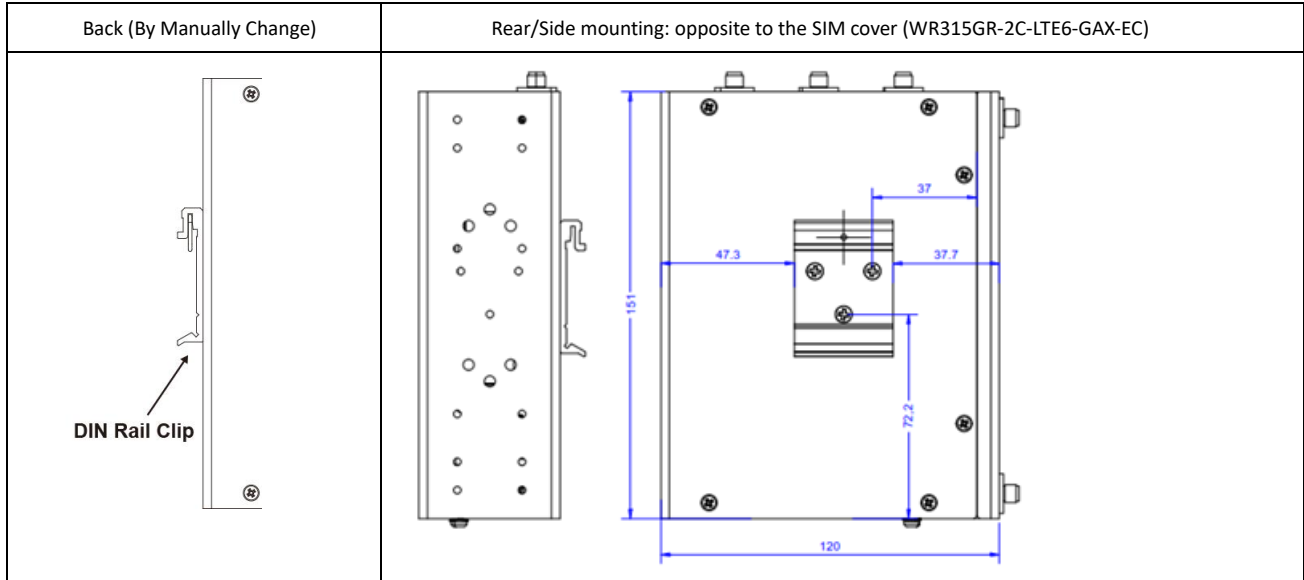
2.5 CONNECTING THE GROUNDING SCREW

Grounding screw is located on the bottom side of the router. Grounding Screw helps limit the effects of noise due to electromagnetic interference (EMI) such as lightning or surge protection. Run the ground connection from the ground screw to the grounding surface prior to connecting devices. And tighten and wire to chassis grounding for better durability.



2.6 DIN RAIL MOUNTING

The EN50022 DIN-Rail plate should be already attached to the Side/back panel of the device screwed tightly. If user needs to reattach the DIN-Rail attachment plate to the device, make sure the plate is situated towards the top, as shown by the following figures.



To mount the router on DIN Rail track, do the following instruction:

1. Insert the top side of DIN Rail track into the slot of DIN Rail clip.
2. Lightly clip the bottom of DIN-Rail to the track and make sure it attached well.
3. To remove the device from the track, reverse the steps.

Note: In WR315GR-2C-LTE6-GAX-EC, the DIN Clip is pre-installed at the factory for Side mounting. The DIN clip is located opposite to the SIM card cover. If you need to change to rear mounting, move the DIN to the rear screw hole.

2.7 Optional ANTENNA

WR315GR-2C-LTE6-GAX-EC supports 4 antenna sockets, where 2G/3G/4G LTE and Wi-Fi antennas are supported.

In the charging station project, the **RFA-J21-T565-13701** antenna connectors will be connected together with the router, and the antenna will be roof-mounted on the top of the chassis box. **Note: This antenna was custom-made for this project and is for professional installation only.** For information on the context of choosing this antenna, or if you have similar application needs, please contact our sales team for details.

RFA-J21-T565-13701 Major Spec.:

Multi-band Roof Mount
2x (LTE + Wi-Fi) Antenna
RFA-J21-T565-13701
(WR315G-2C-LTE6+GAX-EC)



Frequency of Wi-Fi: 2400~2500/5150~7120MHz

Peak Gain & Ave. Efficiency of Wi-Fi: (Frequency: Connector Number;; Peak Gain(Efficiency))

2400~2500MHz: P1:4.4dbi(47%); P4:4.0dbi(49%); P2:3.9dbi(44%); P3:3.8dbi(44%)

5150-7125MHz: P1:4.9dBi(27%); P4:5.0dBi(29%); P2:4.2dBi(24%); P3:4.6dBi(28%)

Connector of Wi-Fi: 2x2 RP SMA PLUG (Professional Engineer for Installation Required)

Frequency of LTE: 617-960MHz / 1710~2700MHz

Peak Gain & Ave. Efficiency of LTE: (Frequency: Connector Number;; Peak Gain(Efficiency))

617-960MHz: P1:2.8dBi(34%); P4:4.1dBi(42%); P2:4.1dBi(44%); P3:3.6dBi(44%)

1710-1755MHz: P1:4.3dBi(52%); P4:4.8dBi(47%); P2:4.1dBi(41%); P3:3.2dBi(48%)

1785-2170MHz: P1:6.9dBi(51%); P4:5.1dBi(49%); P2:6.4dBi(51%); P3:6.5dBi(51%)

2300-2400MHz: P1:3.2dBi(42%); P4:2.5dBi(40%); P2:3.9dBi(39%); P3:2.7dBi(45%)

2400-2500MHz: P1:4.7dBi(37%); P4:3.4dBi(38%); P2:2.4dBi(38%); P3:2.8dBi(38%)

Connector of LTE: 2x2 SMA PLUG

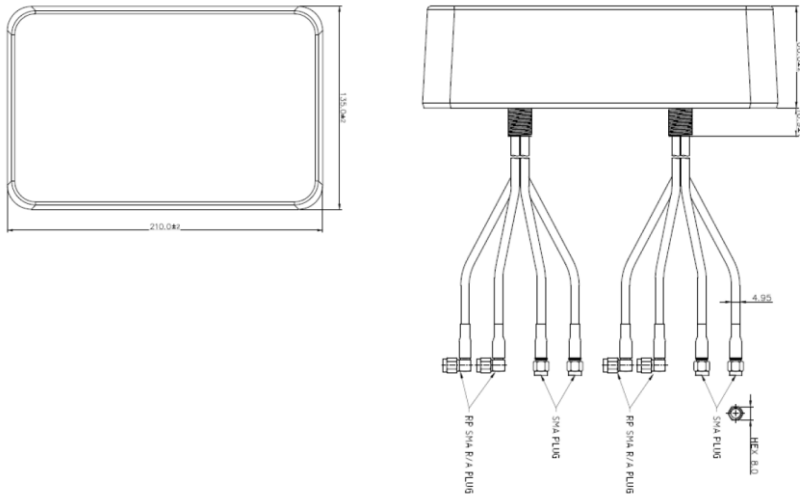
Dimension: 210(L) x 135(W) x 60(H)mm; 76.9(H)mm include through-hole mounting ring

Mounting: Roof-mount/Through-hole mount

Cable Length: 2x4 RG58 / Length=2M

Environment: Temperature: -40~70℃, Humidity: 95%@25℃

Dimension:



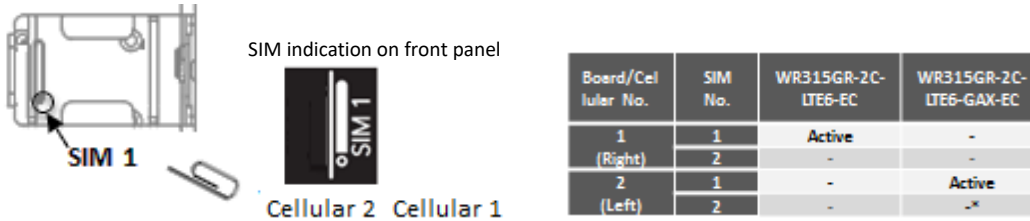
Note: For other optional antennas for non-EU regions, WR315GR-5GM2-2C does not come with default antennas while shipment, please contact our sales to order them separately.

2.8 SIM CARD INSTALLATION

SIM Card Slot

The SIM Card Slot is used to insert the cellular card. The WR315GR-2C-LTE6-GAX-EC supports one SIM. It is SIM 1 location of the CELL 2 PCBA board.

(**Note:** EC OS version software supports one SIM only due to the restriction of current OpenWRT OS.)



To install/uninstall SIM card:

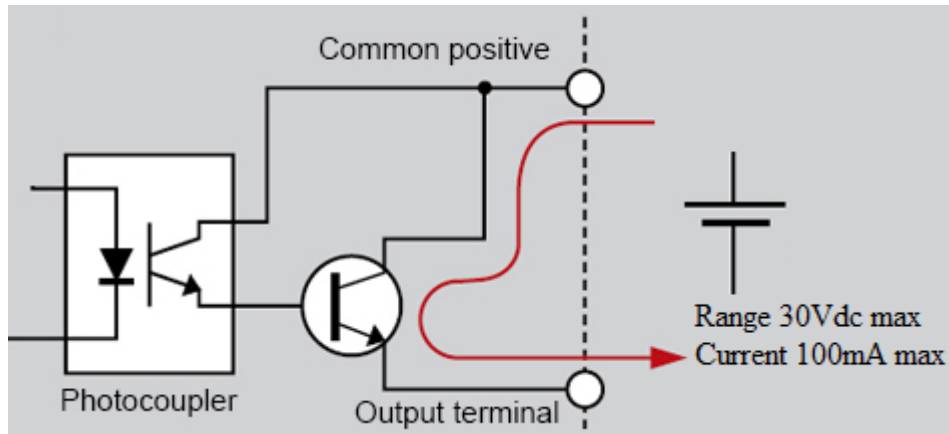
1. Use screwdriver to loosen screws and remove SIM cover.
2. Insert a paper clip or a SIM-eject tool into the hole beside the SIM socket. Push in towards the device, but don't force it. The SIM 1 is the primary SIM in the default configuration.
3. (When install) Draw out SIM tray and install SIM card on top side of tray
(When uninstall) Draw out SIM tray and uninstall SIM card

WARNING: Be careful when install the SIM Card, wrong installation procedure will cause damage.
Please follow the mechanical print out to install the SIM Card.

4. Insert tray back to SIM socket and reattach SIM cover.

2.9 WIRING THE DIGITAL OUTPUT (Reserved)

The digital output of the terminal block is used to detect user-configured events. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured event does not occur, the fault circuit remains opened.



Wiring the Digital Output

1. Insert the positive and negative wires into the DO+ and DO- contact on the terminal block connector.
2. Tighten the wire-clamp screws to prevent the wires from being loosened.

WARNING: Please confirm the wire installation according to the above steps, otherwise it would not work properly. It only supports 0.1 A current, DC 30V. Do not apply voltage and current higher than the specifications.

Note: WR315-M2 supports Relay Output. Not every model of WR315 series supports Digital Input and Digital Output. The feature is reserved for the WR315GR-M2 with Digital Output model only.

2.9 HARDWARE WATCHDOG

The device provides a hardware watchdog mechanism for critical event, such as system reboot is to cut the power of the whole device to get a clean restart of all components.

The device also provides a “dying gasp” alert. The router can generate syslog event or SNMP trap to target server when the router loses power. (Note: The dying gasp alarm software feature is not supported in current EC OS.)

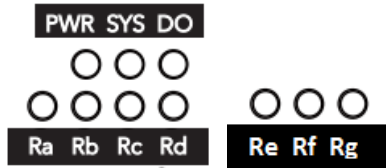
Some of the features are also available as watchdog. Refer to:

Ping Watchdog

Periodic Reboot/Restart Interface

2.10 LED INDICATION

WR315GE-2C-LTE6-GAX-EC (Model with LTE Cat.6 + Wi-Fi 6 client modules)



LED		Status	Description
WR315GR-2C-LTE6 -GAX-EC	Ra	Green On	11ax 5GHz Client mode
		Green Blinking	11ax 5GHz Transmitting
		Off	Disabled
	Rb	Green On	11ax 2.4G Client mode
		Green Blinking	11ax 2.4G Transmitting
		Off	Disabled
	Rc	OFF	N/A
	Rd	(Reserved)	(Controlled by module)
	Re	Green On	SIM detected
		Off	SIM not insert
	Rf	Green On	4G/3G/2G Signal Strength Good ($-90 \leq \text{rsrp}$)
		Green Blinking	4G/3G/2G Signal Strength Medium($-100 \leq \text{rsrp} \leq -90$)
		Off	4G/3G/2G Signal Strength Low($\text{rsrp} \leq -100$)
	Rg	(Reserved)	(Controlled by LTE module)

Rc LED is not used in this model.

Rd/Rg LED is applied to Radio module's LED, its behavior is depends on radio module.

3. WR315G-2C-LTE6-GAX-EC EC OS Introduction

3.1 EC OS Software Specification:

Software (EC OS Version, OpenWRT, WR315GR-2C-LTE6-GAX-EC series)	
Applied Model	WR315GR-2C-LTE6-G-EC, WR315GR-2C-LTE6-GAX-EC, WR315GR-2C-M2-EC, WR315GR-2C-LTE-G-EC, WR315GR-2C-LTE-GAX-EC
OS	OpenWRT 23.05
Web Server	LuCI Web Interface
Terminal Server (SSH)	Secure encrypted communications between two untrusted hosts over an insecure network
Kernel	GNU/Linux kernel v5.15
Internet Protocol Suite	TCP, UDP, IPv4, IPv6, ICMP, ARP, HTTP, DHCP, NTP, SSH, PPP, SFTP, SSL, SCP
Internet Security Suite	OpenVPN, IPSec, Netfilter/iptables
Network Control Protocol	Router mode (1xWAN+4xLAN), NAT/PAT, VLAN, QoS, NTP client/server, IGMP, PPP, PPPoE, SSL, port forwarding
Network Security	HTTPS, SSH, VPN tunnels, SFTP, DMZ, firewall (IP filtering, MAC address filtering, inbound/outbound port filtering)
Cryptographic	AES, SHA, OpenSSL, random generator
Cellular Networking	Features: Cellular Configuration Radio on/off, 2G/3G and 4G modes configurable, Enter PIN code for SIM Security, Connection status, display module info, GPS positioning(by model*) Modem manager: uQMI(user QMI) for talking to WWAN modems and devices that speak the Qualcomm MSM Interface (QMI) protocol. *EC version doesn't support dual SIM due to uQMI restriction.
Time Management	NTP, Cellular Time(by module)
Watchdog	Periodic Reboot, Ping watchdog for keep-Alive connection monitoring, Restart interface for mobile modem, run script
Web GUI Management	Based on LuCI WebGUI System Setting, NTP Setting, Router Password setting with strength check, SSH Access and Key upload, HTTPS, init script startup setting, configuration backup/restore, firmware upgrade, system reboot, watchcat/watchdog, ser2net, Interface configuration, Wi-Fi interface setting, DHCP server/client, DHCP Relay, DNS, firewall setting, static router, Diagnostic Ping, traceroute, Nslookup, Device Status and Mobile Information
WLAN Configuration (Model with WLAN module)	Support Wi-Fi Client mode. WLAN Basic Settings: Radio on/off, mode selection, 2.4G/5G 11ax Band and Frequency selection, SSID configuration, Wireless Security encryption includes WPA3-SAE and WPA2-PSK/WPA-PSK/Open, advanced WLAN settings, WLAN MAC Filter, 802.11r fast transition

3.2 WR315G-2C-LTE6-GAX-EC QIG

This chapter introduces the Quick Installation Guide of the WR315G-2C-LTE6-GAX-EC.

Overview

The **WR315GR-2C-LTE6-GAX-EC** is a high-performance industrial router featuring **4G LTE and Wi-Fi 6** connectivity. Powered by a **dual-core 880 MHz CPU**, it includes two expansion sockets—one for an **LTE Cat.6 cellular module** and one for a **Wi-Fi 6 client module**. The router provides **five Gigabit Ethernet ports**, including **one WAN port** and **four LAN ports**, supporting routing between Ethernet LAN and WAN networks. Either the **4G cellular module** or the **Wi-Fi 6 client module** can function as a **Wireless WAN interface**, enabling wireless Internet connectivity. The router runs on the **OpenWrt-based embedded operating system**, referred to as **EC OS**, which offers both the **UCLI web interface** and **SSH access** for management, along with a rich set of software features.

Model	Description
WR315GR-2C-LTE6-G-EC	Industrial Secure Router, Dual Core, 5GbE, 1 Relay, EC OS, LTE6-G
WR315GR-2C-LTE6-GAX-EC	Industrial Secure Router, Dual Core, 5GbE, 1 Relay, EC OS, 802.11ax WLAN6 client, LTE6-G

Power Input: 24VDC (9V~48VDC)

LTE6-G: (FCC ID: 2AJYU-8XM0004)

LTE-FDD: B1/B2/B3/B4/B5/B7/B8/B12/B13/B14/B17/B18/B19/B20/B25/B26/B28/B29/B30/B32/B66

LTE-TDD: B38/B40/B41/B42/B43/B46/B48

WLAN 6: 2.4GHz/5GHz 802.11ax/ac/n/g/a/b, MU-MIMO 2T2R (FCC ID RAS-MY7922A22M)

Installation

• SIM Card Slot

To install/uninstall SIM card:

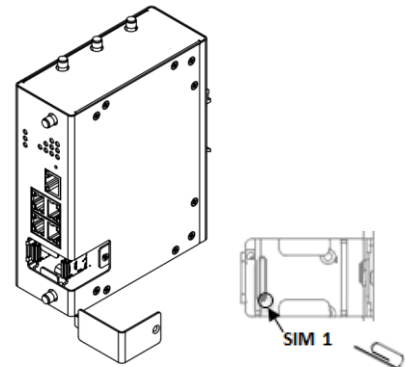
1. Use screwdriver to loosen screws and remove SIM cover.
2. Insert a paper clip or a SIM-eject tool into the hole beside the SIM socket.

Gently push inward, do not use excessive force. SIM 1 is the primary SIM in the default configuration.

3. To Install: Draw out SIM tray and place the SIM card on top side of tray

To uninstall: Draw out SIM tray and remove SIM card

4. WR315G-2C-LTE6-GAX-EC supports only one SIM card due to limitation of OpenWrt system.

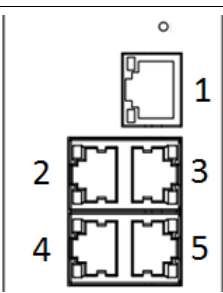


Warning: Be careful when install the SIM Card, wrong installation procedure will cause damage. Make sure the SIM Card is facing the correct position.

• Interface - Ethernet

WR315G-2C-LTE6-GAX Ethernet Port Map:

Default Ethernet port configuration in WR315G-2C-LTE6-GAX is Router Mode, LAN to WAN routing enabled.

Port Map	Port Number	Router Mode(Default)
	Port 1	WAN (Default: DHCP Client)
	Port 2	LAN (Default IP: 192.168.10.1) (Web GUI: Lan 2/3/4/5)
	Port 3	
	Port 4	
	Port 5	

Interface Name:

 lan br-lan	Protocol: Static address Uptime: 0h 20m 19s MAC: 4E:A0:B1:85:7C:E1 RX: 2.33 MB (29916 Pkts.) TX: 8.96 MB (9782 Pkts.) IPv4: 192.168.10.1/24	Restart Stop Edit Delete
 wan wan	Protocol: DHCP client MAC: 4E:A0:B1:85:7C:E1 RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	Restart Stop Edit Delete

The default IP of the interface LAN ports: 192.168.10.1

The default IP of the interface WAN port: DHCP Client

Note: “wan6” is the IPv6 configuration of WAN interface. It is usually not used.

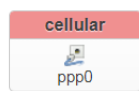
Port Status in Web GUI- Status:

Port status

lan2  no link ▲ 0 B ▼ 0 B	lan3  1 GbE ▲ 8.0 MiB ▼ 2.1 MiB	lan4  no link ▲ 0 B ▼ 0 B	lan5  no link ▲ 0 B ▼ 0 B	wan  no link ▲ 0 B ▼ 0 B
---	---	---	---	--

• Interface - Cellular

The router support 4G LTE Cat.6 cellular interface.



Protocol: ModemManager
Uptime: 0h 19m 44s
RX: 1.87 MB (3772 Pkts.)
TX: 503.40 KB (4201 Pkts.)
IPv4: 10.158.20.29/32

[Restart](#)[Stop](#)[Edit](#)[Delete](#)

Cellular Interface: Default is Enabled.

Logical name: cellular (ppp), works as WAN interface.

Apn: internet

Auth: none

Iptype: ipv4v6

Signal Refresh Rate: 5 second

Interfaces » cellular

[General Settings](#) [Advanced Settings](#) [Firewall Settings](#) [DHCP Server](#)

Status

 Device: ppp0
Uptime: 0h 1m 10s
RX: 84.05 KB (286 Pkts.)
TX: 37.55 KB (336 Pkts.)
IPv4: 10.232.164.21/32

Protocol

ModemManager ▼

Disable this interface

☐

Bring up on boot

☒

Modem device

SIMCOM INCORPORATED - S ▼

APN

internet

PIN

Authentication Type

None ▼

Allowed network technology

any ▼

 Setting the allowed network technology.

IP Type

IPv4/IPv6 (both - defaults to IPv4 ▼)

Signal Refresh Rate

5

 In seconds

• Interface – Wi-Fi

The router supports Wi-Fi 6 (client) interface.

wwan

radio0.network1

Protocol: DHCP client
 RX: 0 B (0 Pkts.)
 TX: 0 B (0 Pkts.)
 Error: Network device is not present

Restart Stop Edit Delete

Wireless LAN:

Default is Disabled.

Default value after enabled:

Wireless Mode: Client Mode

Radio Setting: IEEE802.11ax, 5G, Auto channel, Bandwidth 20Mhz

SSID: Wireless

Encryption: None

Network Interface: wwan

Default IP: DHCP Client

Web GUI:

Wireless Network: Client "Wireless" (radio0.network1)

Device Configuration

[General Setup](#)
[Advanced Settings](#)

Status

Mode: Client | SSID: Wireless
 ---dBm Wireless is not associated

Wireless network is disabled
 [Enable](#)

Operating frequency

Mode	Band	Channel	Width
AX	5 GHz	auto	20 MHz

Maximum transmit power

driver default
 - Current power: unknown

ⓘ Specifies the maximum transmit power the wireless radio may use. wireless usage, the actual transmit power may be reduced by the c

Interface Configuration

[General Setup](#)
[Wireless Security](#)
[Advanced Settings](#)

Mode

Client

ESSID

Wireless

BSSID

Network

wwan:

ⓘ Choose the network(s) you want to attach to this wireless interface network.

• Antenna

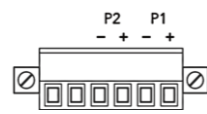
WR315G-2C series supports max. 4 SMA socket, which are for 4G LTE or Wi-Fi antennas. User must install the antennas to correct socket while use. WR315G-2C-LTE6-GAX-EC uses the Antenna 1/2/3/5 sockets as shown in the table on the left.

Note: Due to the different number of antennas used by LTE/WLAN models, the unused antenna positions will be covered by caps.

	WR315GR-2C-LTE6-GAX-EC
Ant 1	Wi-Fi Main
Ant 2	Wi-Fi Div.
Ant 3	LTE6 Main
Ant 4	-
Ant 5	LTE6 Div.

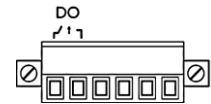
• Wiring the Power Input

- 1) Insert positive and negative wires into V+ and V- contact on the terminal block connector.
- 2) Tighten the wire-clamp screws to prevent the power wires from being loosened.
- 3) Connect the power wires to suitable DC Switching type power supply. The typical input DC voltage is 24V.



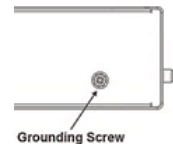
• Wiring the Relay Output/DO Alarm

The relay output of the 6-pin terminal block connector is used to detect user-configured events, for example the Ethernet port link down. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured event does not occur, the fault circuit remains opened.



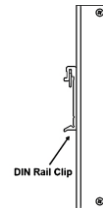
• Grounding Screw

The grounding screw is located on the bottom side of the router. For avoiding system damage by noise or electric shock, establish a direct connection between the ground screw and the grounding surface prior to connecting devices.



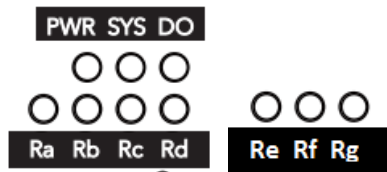
• DIN Rail mount

To mount the router on the DIN Rail track, insert the upper end of the DIN-Rail clip into the back of the DIN-Rail track from its upper side and lightly push the bottom of the DIN-Rail clip into the track. The DIN Rail should comply with DIN EN50022 standard. Using wrong DIN rail may cause unsafe installation.



• LED:

WR315GE-2C-LTE6-GAX-EC (Model with LTE Cat.6 + Wi-Fi 6 client modules)



LED		Status	Description
WR315GR-2C-LTE6 -GAX-EC	Ra	Green On	11ax 5GHz Client mode
		Green Blinking	11ax 5GHz Transmitting
		Off	Disabled
	Rb	Green On	11ax 2.4G Client mode
		Green Blinking	11ax 2.4G Transmitting
		Off	Disabled
	Rc	OFF	N/A
	Rd	(Reserved)	(Controlled by module)
	Re	Green On	SIM detected
		Off	SIM not insert
	Rf	Green On	4G/3G/2G Signal Strength Good ($-90 \leq \text{rsrp}$)
		Green Blinking	4G/3G/2G Signal Strength Medium($-100 \leq \text{rsrp} \leq -90$)
		Off	4G/3G/2G Signal Strength Low($\text{rsrp} \leq -100$)
	Rg	(Reserved)	(Controlled by LTE module)

Rc LED is not used in this model.

Rd/Rg LED is applied to Radio module's LED, its behavior is depends on radio module.

3.3 PREPARATION for Management

To access the management interface of the **EC OS based on the OpenWrt** operating system, WoMaster routers provide two primary access methods over the network: web-based management and SSH/Telnet command-line management.

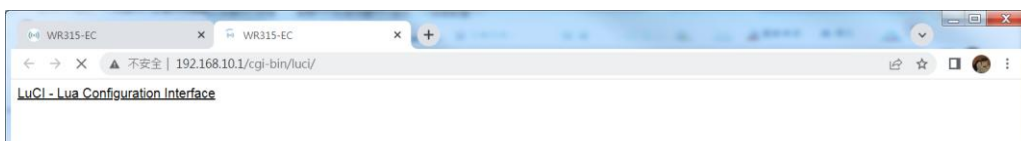
Web management is the most commonly used and user-friendly method. It allows users to monitor device status and perform basic configuration tasks through a standard web browser via the built-in **LuCI web interface**. This interface provides access to system information, network settings, and essential router controls.

If the web interface is unavailable due to network issues or misconfiguration, users can alternatively access the router via **SSH** or Telnet. This method provides full access to the router's command-line interface (CLI), allowing advanced configuration and troubleshooting.

PREPARATION FOR WEB MANAGEMENT

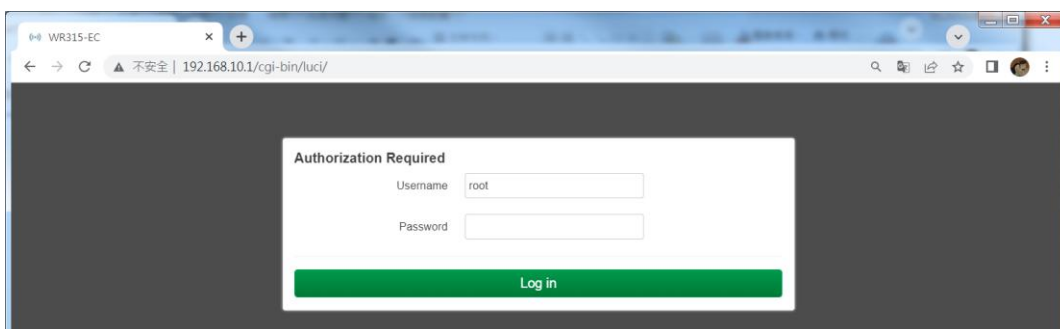
WoMaster router running OpenWrt-based EC OS provides a LuCI Web-based management interface accessible through standard web-browser such as Microsoft Internet Explorer, or Mozilla, or Google Chrome, to access and configure the router management on the network.

1. Plug the DC power to the router and connect router to computer via Ethernet.
2. The router's default IP address is **192.168.10.1**.
3. Check that PC has an IP address on the same subnet as the router. For example, assign your PC and IP address like **192.168.10.2**, with a subnet mask of **255.255.255.0** and a default gateway of **192.168.10.1**
4. Alternatively, if the router's DHCP Server is enabled, set your PC to DHCP Client mode to obtain an IP address automatically.
5. Open a command prompt and ping **192.168.10.1** to verify that the router is reachable.
6. Launch the web browser (Internet Explorer or Mozilla Firefox or Google Chrome) on the PC.
7. Type <http://192.168.10.1> (or the IP address of the router) in the address bard. Press **Enter** and the login page will appear.

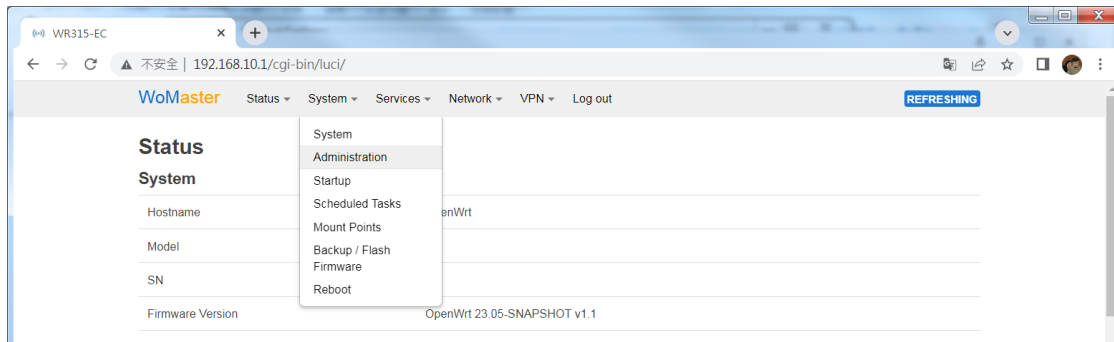


8. Type user name and the password.

The default user name: **root** and password: **root**. Then click **Login**.



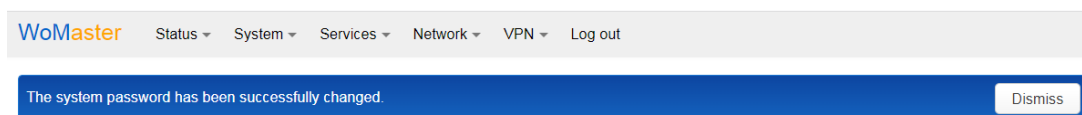
9. **For security concern, it is commend to change the default password with a new password in first Login.** Go to “System” → “Administrator” page, you can enter new password and Save to apply the change. Please follow the prompt to enter new password.



Then enter with the new password and click “Save” to apply the change.

A screenshot of the 'Router Password' page in the WoMaster interface. The page title is 'Router Password' with a subtitle 'Changes the administrator password for accessing the device'. There are two password input fields: 'Password' and 'Confirmation', both masked with dots. Below the 'Confirmation' field, a message indicates 'Password strength: Strong' with a green checkmark. At the bottom right, there is a green 'Save' button.

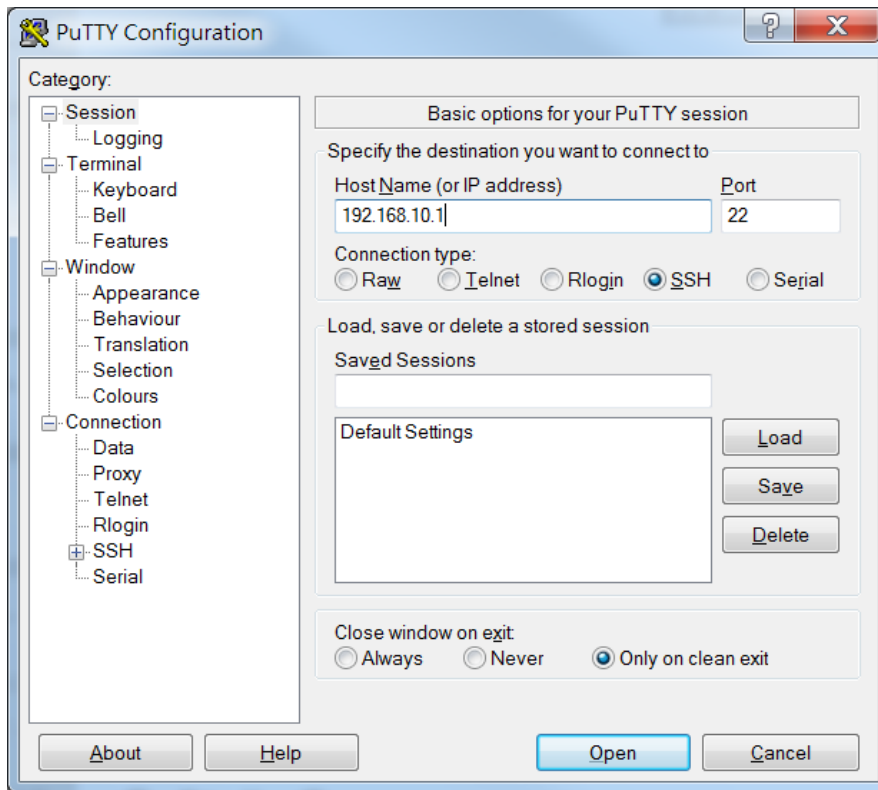
After clicking “Save”, a prompt message will appear saying “The system password has been successfully changed.” Click “Log out”, you will be required to use the new password in the next time you login.



Using SSH to Configure OpenWrt

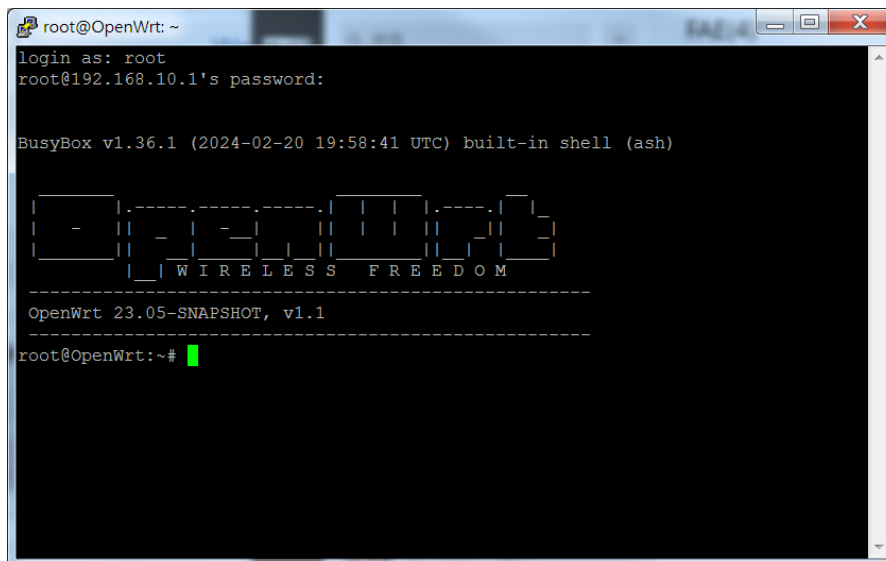
OpenWrt supports remote command-line access via SSH, allowing users to perform advanced configurations and troubleshooting.

1. Ensure network connectivity between your PC and the OpenWrt router (e.g., same subnet or reachable IP).
2. On your PC, open a terminal or SSH client (such as PuTTY, download OpenSSH for Windows or a Linux terminal).
3. Using Putty:
Type the IP address of the router and use the access Port 22.



The SSH console will appear:

The default user name: **root** and password: **root**.



4. In Window OS 10 1809+, the SSH(OpenSSH) console is built-in. For earlier OS version, please download the OpenSSH through internet for your windows.

Through the Window Command prompt, you can enter the following command to connect.

ssh 192.168.10.1 -l root

(Replace 192.168.10.1 with your router's actual IP address.) [-l login_name]

When prompted, enter the root password. (default password: root)

3.4 LuCI Web Management

The following content mainly introduces the major Web GUI settings. Since openwrt is a public system, if it is not listed here, you can also find its web gui settings through the Internet or the openwrt website.

3.4.1 STATUS

In the **OpenWrt LuCI web interface**, the **Status** section provides a comprehensive overview of the system's current state and runtime information. It is commonly used for diagnostics, monitoring, and quick verification of network and system status.

Key Features Available Under the Status Menu:

Overview

General system information: Hostname, Model, SN, Firmware version, Kernel Version, Local Time, Uptime, Load average, memory usage, Storage space...etc.

WoMaster Status ▾ System ▾ Services ▾ Network ▾ VPN ▾ Log out

Status

System

Hostname	OpenWrt
Model	WR315-EC
SN	1234567890
Firmware Version	OpenWrt 23.05-SNAPSHOT v1.0
Kernel Version	5.15.148
Local Time	2025-04-24 12:21:42
Uptime	0h 3m 3s
Load Average	2.05, 1.13, 0.45

Port Status: It indicates the link status of the LAN port 2/3/4/5 and WAN port (port 1).

Port status

lan2 no link ▲ 0 B ▼ 0 B	lan3 1 GbE ▲ 18.5 MiB ▼ 4.9 MiB	lan4 no link ▲ 0 B ▼ 0 B	lan5 no link ▲ 0 B ▼ 0 B	wan no link ▲ 0 B ▼ 0 B
--	---	--	--	---

Network: It provides the information of the upstream interface, includes the IP addresses, connected time, active interface, DHCP status.

Network

IPv4 Upstream
Protocol: ModemManager
Address: 10.158.20.29/32
Gateway: 10.64.64.64
DNS 1: 61.31.1.1
DNS 2: 61.31.233.1
Connected: 0h 49m 35s
Device: Ethernet Adapter: "ppp0"

Active DHCP Leases

Hostname	IPv4 address	MAC address	Lease time remaining	Static Lease
Porsche-P5430UA (Porsche-P5430UA.lan)	192.168.10.142	38:D5:47:94:13:35	11h 8m 57s	<button>Set Static</button>

Wireless: It shows the Wi-Fi Client status (default is disabled) and associated Stations. It shows the real-time view of wireless interfaces and modes and associated stations.

Wireless

radio0
Type: MAC80211 802.11ac/ax/b/g/n Channel: 0 (0.000 GHz) Bitrate: - SSID: Wireless Mode: Client Wireless is disabled

Associated Stations

Network	MAC address	Host	Signal / Noise	RX Rate / TX Rate
No information available				

Routes

Lists active IPv4 and IPv6 routing tables.

Active IPv4 Routes can check the IP address of the activated interfaces.

Routing

The following rules are currently active on this system.

[IPv4 Routing](#) [IPv6 Routing](#)

IPv4 Neighbours

IP address	MAC address	Interface
192.168.10.142	38:D5:47:94:13:35	lan

Active IPv4 Routes

Device	Target	Gateway	Metric	Table	Protocol
cellular	0.0.0.0/0	10.64.64.64	0	main	static
cellular	10.64.64.64	-	0	main	kernel
lan	192.168.10.0/24	-	0	main	kernel

Note: The entry of “Target 0.0.0.0/0” is very important!

Once you have more than one default gateway, for example both the 4G cellular and Wifi client enabled to internet, the device's routing table will be constantly changing, and if it's missing entries, that means you can access the router, but can't access the Internet.

~~cellular 0.0.0.0/0 10.64.64.64 0 main static~~

For example: If you are missing the cellular interface's 0.0.0.0/0 entry, it means the 4G network is not available, you will need to restart the cellular interface and remove the unused wan/wwan (wireless client) interfaces in case it happen again.

Mobile Service

In Mobile Service, it shows the information of the Modem, Network Registration, Cell Location and SIM card.

Mobile Service

`/sys/devices/platform/1e1c0000.xhci/usb1/1-2/1-2.2`

Modem Info

Manufacturer	SIMCOM INCORPORATED
Model	SIMCOM_SIM7906G-M2
Revision	2110B03X12M22A-M2
IMEI	869951070078591
Device Identifier	0c7ed2200358499533e0c6463a431c265c88e230
Power State	on
State	connected

Network Registration

Own Numbers	
Access Technologies	lte
Operator	TW Mobile
Operator Code	46697
Registration State	home
Packet Service State	attached
Signal Quality	77 %

Cell Location

CID	038735E8
LAC	0000
MCC	466
MNC	97
TAC	002CC4

SIMs

SIM 1

Active	yes
ICCID	89886972401703558791
IMSI	466977005873795

Firewall

Displays current firewall zones and rules.

Shows active connections and NAT rules.

System Log

Shows the system's kernel and service logs.

Helpful for debugging service behavior and startup issues.

System Log Kernel Log

System Log

Scroll to tail

Mon May	5	02:44:50	2025	daemon.debug	[22006]	<debug>	[1746413090.494620]	[ttyUSB3/at]	<-->	<CR><LF><CESQ: 99,99,255,255,10,44<CR><LF><CR><LF>
Mon May	5	02:44:50	2025	daemon.debug	[22006]	<debug>	[1746413090.496447]	[modem0]	lte	extended signal information updated
Mon May	5	02:44:50	2025	daemon.debug	[22006]	<debug>	[1746413090.498087]	[ttyUSB3/at]	device	open count is 1 (close)
Mon May	5	02:44:55	2025	daemon.debug	[22006]	<debug>	[1746413095.486811]	[ttyUSB3/at]	device	open count is 2 (open)
Mon May	5	02:44:55	2025	daemon.debug	[22006]	<debug>	[1746413095.487304]	[ttyUSB3/at]	-->	'AT+CESQ<CR>'
Mon May	5	02:44:55	2025	daemon.debug	[22006]	<debug>	[1746413095.498636]	[ttyUSB3/at]	<-->	<CR><LF><CESQ: 99,99,255,255,7,44<CR><LF><R><CR><LF>
Mon May	5	02:44:55	2025	daemon.debug	[22006]	<debug>	[1746413095.500643]	[modem0]	lte	extended signal information updated
Mon May	5	02:44:55	2025	daemon.debug	[22006]	<debug>	[1746413095.502907]	[ttyUSB3/at]	device	open count is 1 (close)
Mon May	5	02:45:00	2025	daemon.debug	[22006]	<debug>	[1746413100.486250]	[ttyUSB3/at]	device	open count is 2 (open)
Mon May	5	02:45:00	2025	daemon.debug	[22006]	<debug>	[1746413100.486756]	[ttyUSB3/at]	-->	'AT+CESQ<CR>'
Mon May	5	02:45:00	2025	daemon.debug	[22006]	<debug>	[1746413100.498405]	[ttyUSB3/at]	<-->	<CR><LF><CESQ: 99,99,255,255,11,44<CR><LF><CR><LF>
Mon May	5	02:45:00	2025	daemon.debug	[22006]	<debug>	[1746413100.500216]	[modem0]	lte	extended signal information updated
Mon May	5	02:45:00	2025	daemon.debug	[22006]	<debug>	[1746413100.501828]	[ttyUSB3/at]	device	open count is 1 (close)
Mon May	5	02:45:05	2025	daemon.debug	[22006]	<debug>	[1746413105.486061]	[ttyUSB3/at]	device	open count is 2 (open)
Mon May	5	02:45:05	2025	daemon.debug	[22006]	<debug>	[1746413105.486567]	[ttyUSB3/at]	device	open count is 3 (open)
Mon May	5	02:45:05	2025	daemon.debug	[22006]	<debug>	[1746413105.488224]	[ttyUSB3/at]	-->	'AT+CGACT?<CR>'
Mon May	5	02:45:05	2025	daemon.debug	[22006]	<debug>	[1746413105.502963]	[ttyUSB3/at]	<-->	<CR><LF><CGACT: 1,0<CR><LF><CGACT: 1,0<CR><LF><CR><LF>

Processes

Shows currently running processes with PID, memory usage, and CPU usage...

This list gives an overview over currently running system processes and their status.

Processes

This list gives an overview over currently running system processes and their status

PID	Owner	Command	CPU usage (%)	Memory usage (%)			
1	root	/sbin/procd	0%	1%	<button>Hang Up</button>	<button>Terminate</button>	<button>Kill</button>
2	root	[kthreadd]	0%	0%	<button>Hang Up</button>	<button>Terminate</button>	<button>Kill</button>
3	root	[rcu_gp]	0%	0%	<button>Hang Up</button>	<button>Terminate</button>	<button>Kill</button>
4	root	[rcu_par_gp]	0%	0%	<button>Hang Up</button>	<button>Terminate</button>	<button>Kill</button>
5	root	[slub_flushwq]	0%	0%	<button>Hang Up</button>	<button>Terminate</button>	<button>Kill</button>

Channel Analysis

Shows the current channel detected by the Wi-Fi radios.

It helps to understand the radio network status while you need to optimize the WLAN performance.

Channel Analysis

Refresh Channels

radio0 (2.4GHz) radio0 (5GHz)



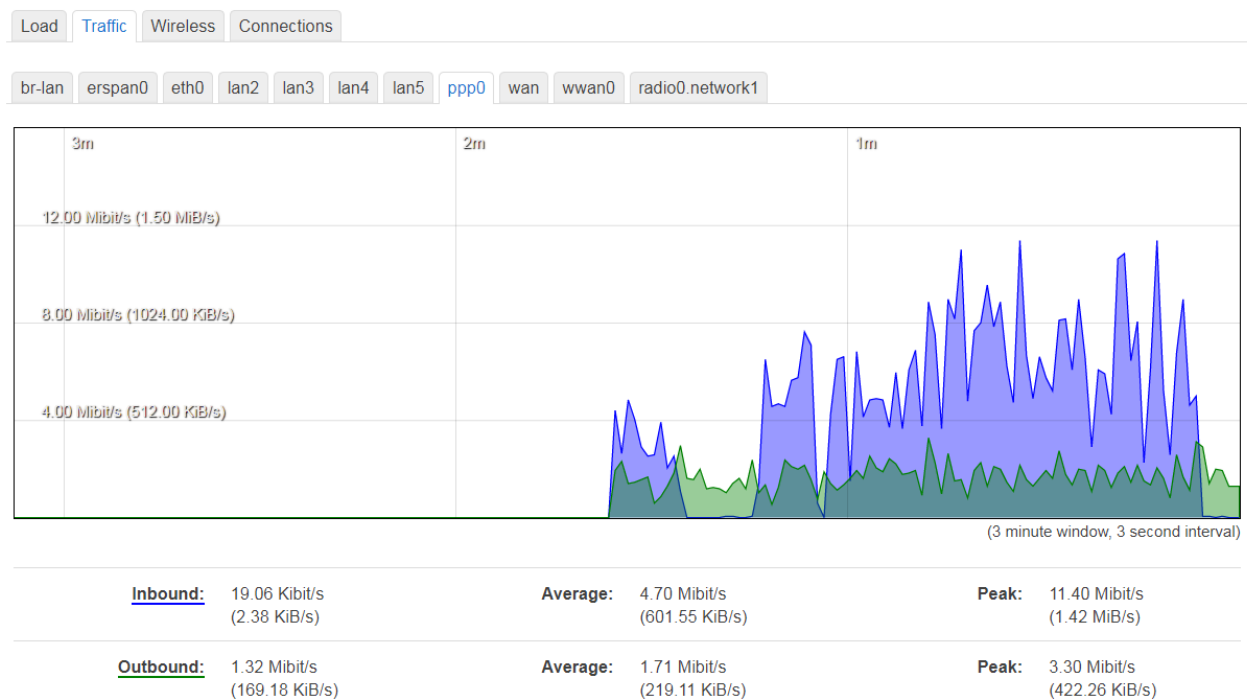
Signal	SSID	Channel	Channel Width	Mode	BSSID
-93 dBm	☐ SURGITECH	36	80 MHz	Master	5C:6A:80:ED:4D:04
-92 dBm	☐ Sean-5G	36	80 MHz	Master	60:6C:63:1F:B4:9F

Realtime Graphs

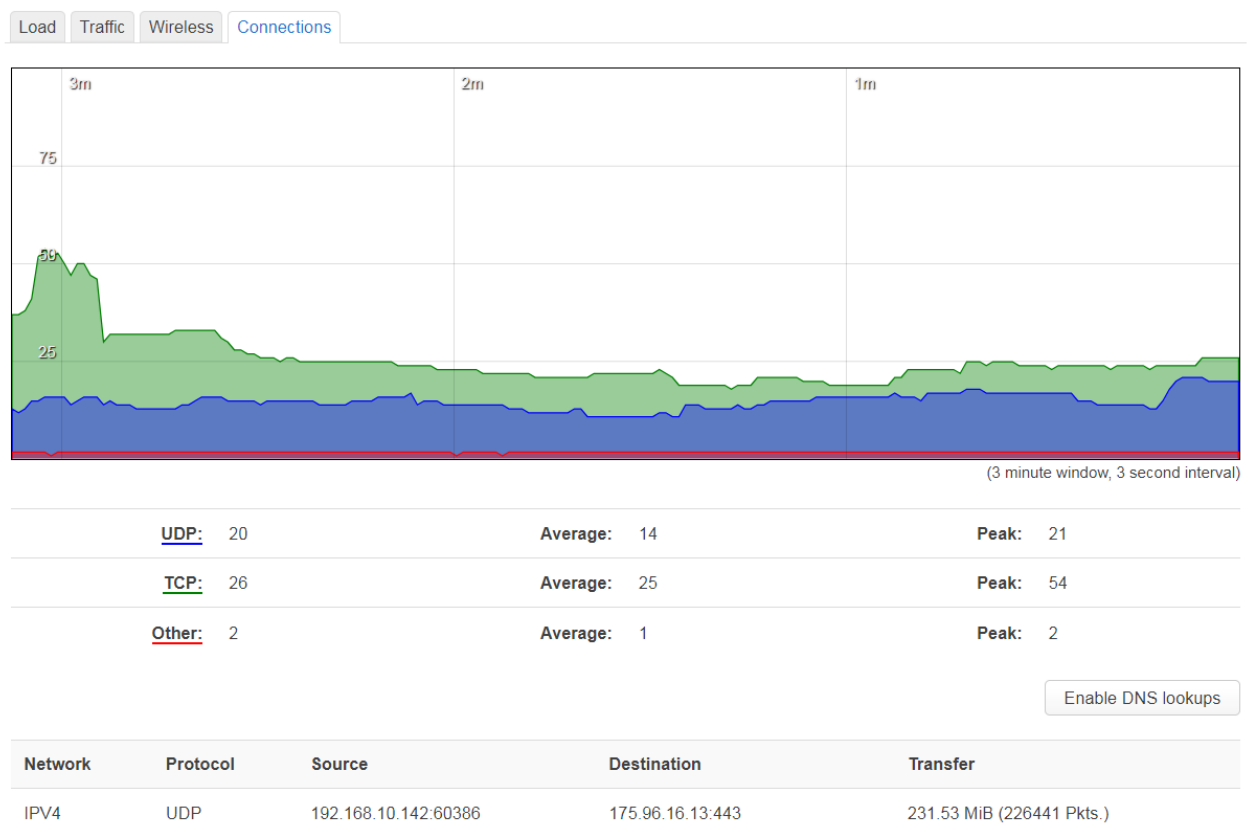
Show the system **Load**, network **Traffic** usage, **Wireless** and **Connection** load graphs in real-time.

Helps visually monitor resource load and interface throughput.

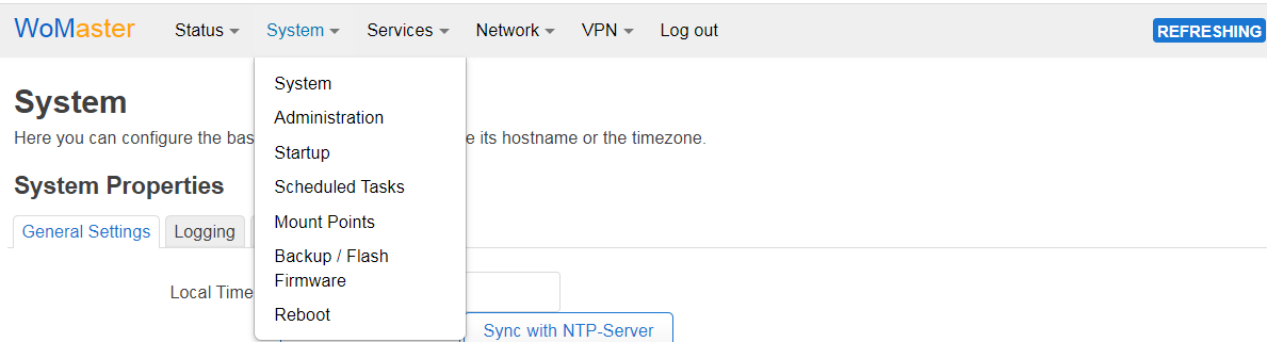
Example of the 4G LTE network Traffic usage:



Example of the Connection usage and source device:



3.4.2 SYSTEM



3.4.2.1 System → System

System Properties allows you to configure Device Settings, Log setting and NTP Server settings.

- **General Settings:** It shows the **Local Time** and allow you to select “Sync with browser” or “Sync with NTP Server”. Set **hostname**, **Description** and “**Notes**” about this device. And configure the **Timezone**.
- Configure **Logging** settings
- Configure the **NTP Server Setting**. Default is NTP Client. You can add your prefer NTP server here. Ex: time.google.com (Google NTP Server)

System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

[General Settings](#) [Logging](#) [Time Synchronization](#)

Local Time

2025-05-05 03:05:13

[Sync with browser](#) [Sync with NTP-Server](#)

Hostname

OpenWrt

Description

[?](#) An optional, short description for this device

Notes

[?](#) Optional, free-form notes about this device

Timezone

UTC

▼

[Save & Apply](#) [Save](#) [Reset](#)

System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

General Settings Logging Time Synchronization

Enable NTP client ☒

Provide NTP server ☐

Use DHCP advertised servers ☒

NTP server candidates

0.openwrt.pool.ntp.org	✖
time.google.com	✖
	+

Save & Apply

Save

Reset

3.4.2.2 System → Administration

- **Router Password:** Change **web GUI and SSH password**. Password Strength indicates whether the password you enter is strong enough or not.
- **SSH Access:** Set **SSH access settings**. You can assign the given interfaces. Select “unspecified” means all interfaces.
- **SSH-Keys:** Upload and manage SSH public keys
- **HTTP(S) Access:** Enable automatic redirection of HTTP requests to HTTPS port.

Router Password SSH Access SSH-Keys HTTP(S) Access

Router Password

Changes the administrator password for accessing the device

Password

Confirmation

 Password strength: **Strong**

Save

3.4.2.3 System → Flash Operation

The Flash operations allow you to backup/restore the configuration file and firmware upgrade.

Flash operations

Actions

Configuration

Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup

Generate archive

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Reset to defaults

Perform reset

Restore backup

Upload archive...

 Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware.

Image

Flash image...

- **Backup:** Download or upload configuration backups
- **Restore:** Restore settings from a backup file. Perform Reset to default.
- **Flash new firmware image:** (with or without keeping settings)

■ Flash Operation: Backup/Restore

To **Backup** the configuration file. Execute the **“Generate archive”** command and you will see a configuration file automatically generated at the bottom of the web GUI screen. This file is usually saved in your default Download folder.

Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup

Generate archive

Example: A back file name: “backup-OpenWrt-2025-05-05.tar.gz” is generated.

 backup-Open....tar.gz ^

To **Restore** the configuration file from one device to the device. Execute the **“Upload archive”** command and you will see a pop-up window for uploading file.

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Reset to defaults

Perform reset

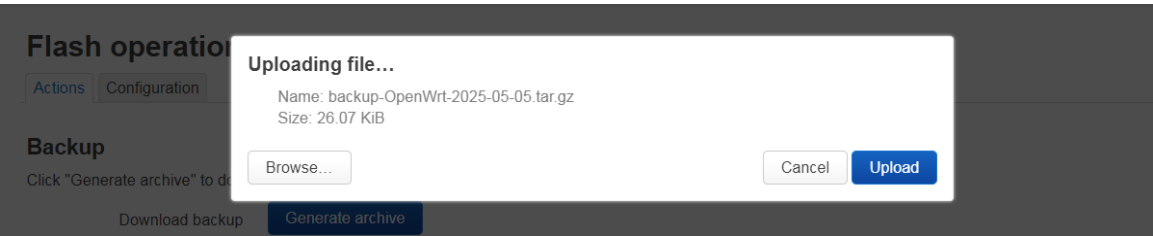
Restore backup

Upload archive...

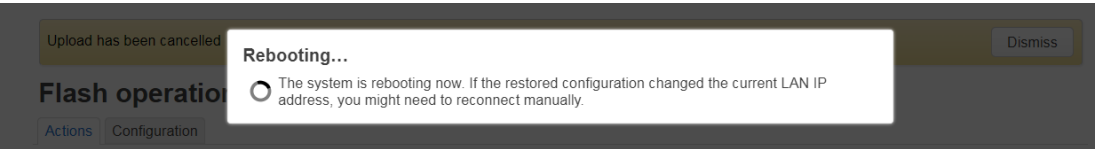
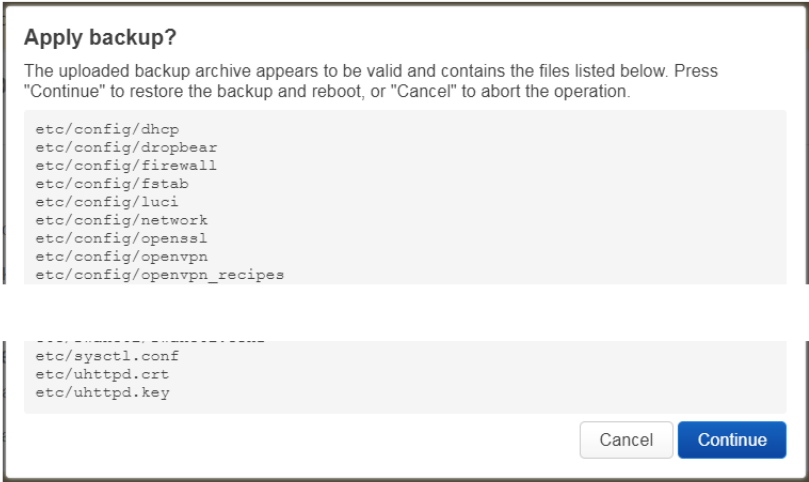
?

Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

Browse the folder of the configuration file, ex: **“backup-OpenWrt-2025-05-05.tar.gz”**. You can see the file name on the pop-up window. Click **“Upload”** to restore the configuration file to the router.

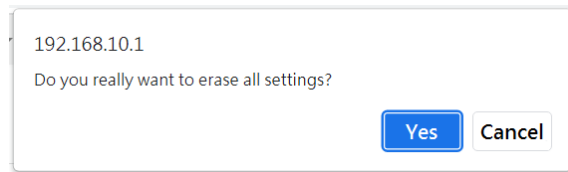


A pop-up window will ask confirm **“Apply backup?”** Press **“Continue”** to restore the configuration file and the router will reboot automatically.

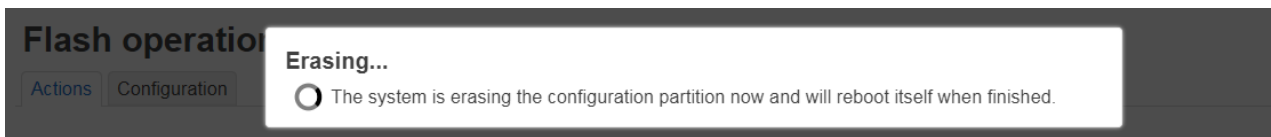


■ Flash Operation: Reset to Default

Click **“Perform reset”**. A pop-up window will ask you **“Do you really want to erase all settings?”**



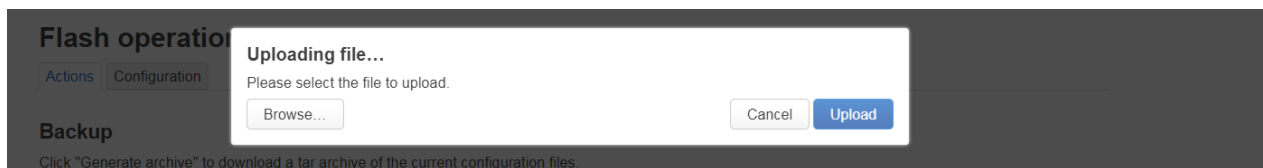
Click **“Yes”**. The router will erase the configuration and will reboot itself with the default configuration.



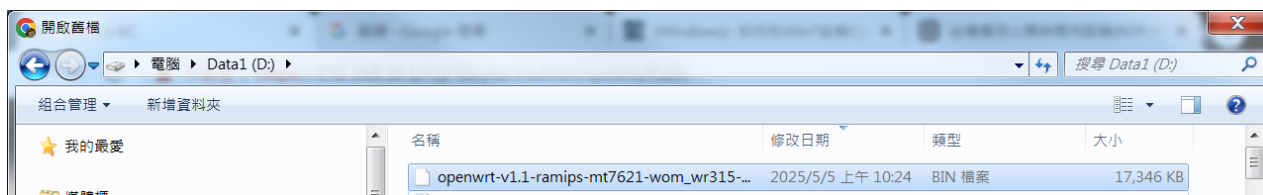
If the system cannot automatically reconnect to the web GUI due to the removal of the IP and settings, please reconnect to the web GUI with the default IP Address.

Flash Operation: Firmware Upgrade

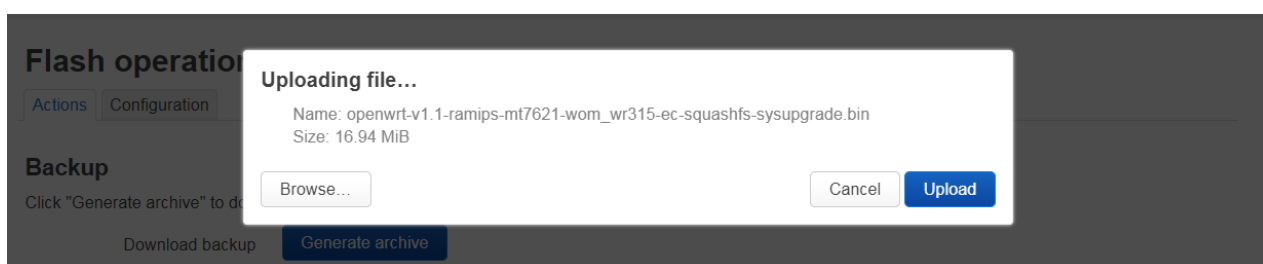
Click “Flash image...”, you can see the below popup window.



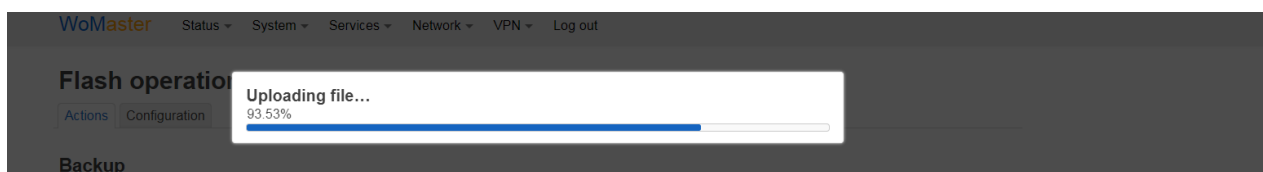
Then click “Browse...”, browse the folder of the firmware file and select the correct new firmware image file.



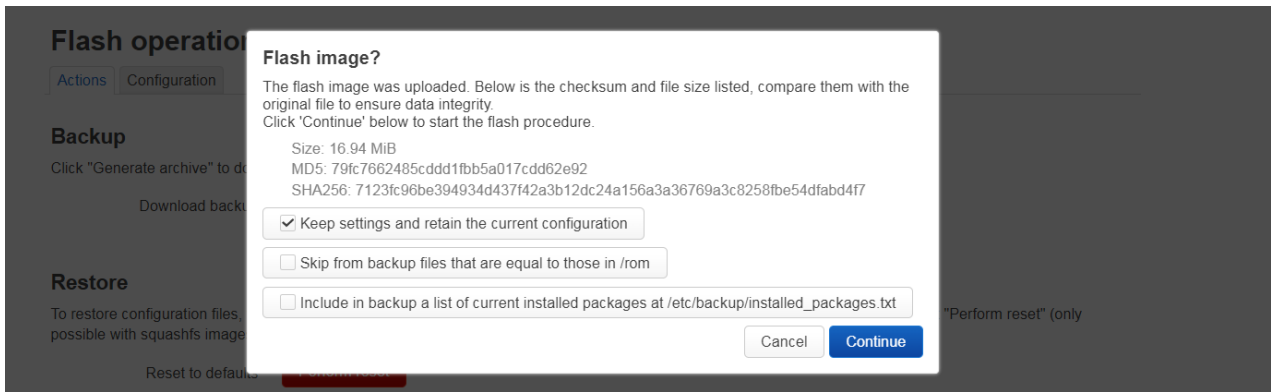
After selected the file, you will be the file name at the popup window.



Click “Upload”, the file will be uploading...

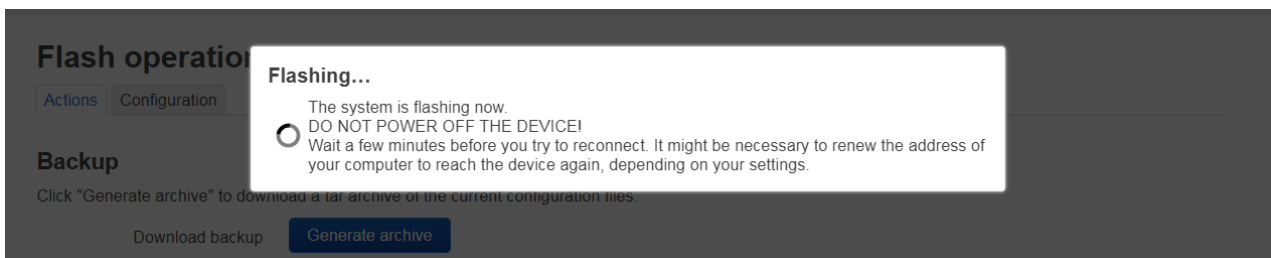


After uploaded, you can keep current configuration by selecting the “Keep Settings and retain the current configuration”.



After “Continue”, you will see the Flashing... The system is flashing the image...

Warning!! DO NOT POWER OFF THE DEVICE while Flashing...!!



The router will automatically reboot after finished the progress.

Note: Since OpenWrt is based on an open system architecture, system settings may be altered after a firmware update. If an external device (such as a 4G or Wi-Fi module) fails to activate properly, try restarting the device or modifying its settings, then apply and save the changes to reactivate it.

3.4.2.4 System → Reboot

Reboot the device manually.

Reboot

Reboots the operating system of your device

Perform reboot

3.4.2.5 Advanced Settings:

The OpenWrt system provides some advanced settings to change the router’s initial state. However, these functions are only suitable for engineers who are familiar with the OpenWrt system.

■ System → Startup

You can enable or disable installed init scripts here. Changes will applied after a device reboot.

Startup

Initscripts Local Startup

You can enable or disable installed init scripts here. Changes will applied after a device reboot.
Warning: If you disable essential init scripts like "network", your device might become inaccessible!

Start priority	Initscript				
00	sysfixtime	Enabled	Start	Restart	Stop
00	umount	Enabled	Start	Restart	Stop
00	urngd	Enabled	Start	Restart	Stop
00	wifi	Enabled	Start	Restart	Stop

- View and manage **init.d scripts** (boot-time services). Enable/disable services...
- Control startup order and status.

Warning: If you disable essential init scripts like "network", your device might become inaccessible!

■ System → Scheduled Tasks (crontab)

- Add scheduled jobs using **cron syntax**
- Useful for automating tasks like reboots, interface resets, or logging

■ System → Mount Points

- Configure **external storage (USB drives, SD cards)**
- Set up automatic mounting of storage volumes

3.4.3 Network

3.4.3.1 Interfaces

The router has created the existed interfaces of the WR315G-2C-LTE6-GAX-EC, such as Cellular(4G LTE), lan (Ethernet-LAN, physical port 2/3/4/5), wan(Ethernet-Wan, physical Port 1), and wwan (Wi-Fi 6 client mode) as below.

WoMaster

Status ▾System ▾Services ▾Network ▾VPN ▾Log out

REFRESHINGUN SAVED CHANGES: 7

InterfacesDevicesGlobal network options

Interfaces

cellular

ppp0

Protocol: ModemManager

Uptime: 0h 19m 44s

RX: 1.87 MB (3772 Pkts.)

TX: 503.40 KB (4201 Pkts.)

IPv4: 10.158.20.29/32

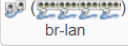
Restart

Stop

Edit

Delete

lan

br-lan

Protocol: Static address

Uptime: 0h 20m 19s

MAC: 4E:A0:B1:85:7C:E1

RX: 2.33 MB (29916 Pkts.)

TX: 8.96 MB (9782 Pkts.)

IPv4: 192.168.10.1/24

Restart

Stop

Edit

Delete

wan

wan

Protocol: DHCP client

MAC: 4E:A0:B1:85:7C:E1

RX: 0 B (0 Pkts.)

TX: 0 B (0 Pkts.)

Restart

Stop

Edit

Delete

wwan

radio0.network1

Protocol: DHCP client

RX: 0 B (0 Pkts.)

TX: 0 B (0 Pkts.)

Error: Network device is not present

Restart

Stop

Edit

Delete

Add new interface...

Save & Apply ▾

Save

Reset

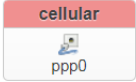
Note: “wan6” is the IPv6 configuration of WAN interface. It is usually not used.

The “**Add new interface**” allows you to add additional interfaces, or recreate an interface after you have deleted it. Click “**Save & Apply**” after you changed the settings.

Note: The Router has already created the current user interface for you. If you want to delete or add other interfaces, please be careful and be familiar with the working principle of OpenWrt operating system. If you delete it by mistake and don't know how to restore it, you can use reset to default to restore the factory settings.

The following page explains the meanings of each interfaces.

■ Interface: Cellular

	Protocol: ModemManager Uptime: 0h 19m 44s RX: 1.87 MB (3772 Pkts.) TX: 503.40 KB (4201 Pkts.) IPv4: 10.158.20.29/32	<button>Restart</button> <button>Stop</button> <button>Edit</button> <button>Delete</button>
---	--	--

The Cellular interface displays the status of the mobile broadband (4G/5G) connection used by the device to access the internet. It is typically used as a primary or backup WAN interface, especially in remote or mobile environments. This status panel provides real-time information about the cellular connection:

- **Interface Name:** Shown as ppp0, this is the system-assigned name for the point-to-point (PPP) cellular connection.
- **Protocol:** Indicates the connection manager used, such as ModemManager, which controls and communicates with the cellular modem.
- **Uptime:** Shows how long the current cellular session has been active.
- **RX / TX:** Displays the amount of data received (RX) and sent (TX) over the cellular network, along with the number of packets transferred.
- **IPv4 Address:** Shows the assigned IP address and subnet, typically used for routing cellular traffic.

Control buttons on the right allow the user to:

- **Restart** the interface (reconnect),
- **Stop** the interface (disconnect),
- **Edit** configuration settings, or
- **Delete** the interface (use cautiously).

Warning: Do **NOT** delete this interface unless you use other non-default 4G/5G cellular modules and you are quite familiar with how OpenWrt works. Generally, we do not recommend or authorize users to replace the 4G module by themselves. Any self-replacement of the hardware module is not covered under the product warranty or support services. The manufacturer shall not be held liable for any damage or malfunction resulting from unauthorized hardware modifications.

Edit interface

After clicking "**Edit**" on a Cellular interface (usually named wwan, 4G, ppp0, or similar), you'll be taken to a configuration page that allows you to modify various connection and network parameters.

The page is mainly used to modify the APN, Disable the interface if you do not use 4G/Cellular...etc.

The default APN name is internet which is popular used in worldwide.

You can type SIM PIN number (password) if it is configured, but, do not allow you to modify the PIN number.

The cellular interface is enabled in default setting, while it will start the connection automatically on boot.

Interfaces » cellular

[General Settings](#) [Advanced Settings](#) [Firewall Settings](#) [DHCP Server](#)

Status

Device: ppp0
Uptime: 0h 1m 10s
RX: 84.05 KB (286 Pkts.)
TX: 37.55 KB (336 Pkts.)
IPv4: 10.232.164.21/32

Protocol

ModemManager

Disable this interface

☐

Bring up on boot

☒

Modem device

SIMCOM INCORPORATED - S

APN

internet

PIN

Authentication Type

None

Allowed network technology

any

Setting the allowed network technology.

IP Type

IPv4/IPv6 (both - defaults to IPv

Signal Refresh Rate

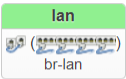
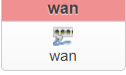
5

In seconds

This is where you set the **main connection parameters**:

- **Protocol:** ModemManager
- **Modem device:** Automatically detected (e.g., SIMCOM... module)
- **APN(Access Point Name):** The APN provided by your mobile operator, default: internet
- **PIN:** SIM card PIN (if enabled) (Modify the SIM Card PIN is not supported)
- **Authentication:**
 - Options: None, PAP, CHAP
 - Some networks require this for authentication.
- **Allowed Network Topology:** any
- **IP Type:**
 - IPv4, IPv6, or IPv4v6
 - Select based on what your mobile operator supports.
- **Signal Refresh Rate:** 5 (in seconds)

■ 3.4.3.2 Interface: lan/wan

	lan br-lan	Protocol: Static address Uptime: 0h 20m 19s MAC: 4E:A0:B1:85:7C:E1 RX: 2.33 MB (29916 Pkts.) TX: 8.96 MB (9782 Pkts.) IPv4: 192.168.10.1/24	<button>Restart</button> <button>Stop</button> <button>Edit</button> <button>Delete</button>
	wan wan	Protocol: DHCP client MAC: 4E:A0:B1:85:7C:E1 RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	<button>Restart</button> <button>Stop</button> <button>Edit</button> <button>Delete</button>

This section shows the status of the **LAN (Local Area Network)**, which connects local devices (like PCs or IoT nodes) to the router. And the **WAN (Wide Area Network)** interface, used for internet access via a wired uplink (e.g., fiber, DSL, cable modem).

Displayed information of the **LAN interface** includes:

- **Interface name** (e.g., br-lan) – This indicates a **bridge** interface that combines multiple physical ports (e.g., LAN port 2, port 3, port 4 and port 5) into one logical network.
- **Protocol** – The IP assignment method. Ex: Static address indicates the Lan interface has a fixed IP.
- **Uptime** – How long the interface has been active.
- **MAC address** – Unique hardware identifier for the interface.
- **RX/TX** – Received and transmitted data, showing current traffic flow.
- **IPv4 address** – The IP address assigned to the interface (default: 192.168.10.1). The IP is usually acts as the default gateway of the connected devices.

The **WAN interface** connects the router to the internet or an upstream network. It commonly uses **DHCP client mode** to obtain an IP address automatically from the internet provider.

Displayed information of the **WAN interface** includes:

- **Interface Name:** wan
- **Protocol:** DHCP client. It tries to get an IP address from your internet provider (or upstream router).
- **MAC:** The hardware address of the WAN interface.
- **RX/TX:** Received and transmitted data. 0B(0 pke/s) means No data has been received or sent yet. This may mean the WAN cable is unplugged or the upstream device is down.
- **IPv4:** The IP address of this interface. Not shown — likely because no IP address has been obtained yet.

Each interface includes control buttons:

- **Restart** – Re-establish the connection.
- **Stop** – Temporarily disable the interface.
- **Edit** – Change settings like IP, DNS, or protocol type.
- **Delete** – Remove the interface configuration (for advanced users only).

Note: The router has one wan interface port 1 and lan interface port 2/3/4/5 by default configuration.

Note: “wan6” is the IPv6 configuration of WAN interface. It is usually not used.

■ 3.4.3.3 Interface: wwan

wwan
phy0-sta0

Protocol: DHCP client
Uptime: 0h 1m 57s
MAC: 44:FA:66:9C:FF:E3
RX: 116.50 KB (662 Pkts.)
TX: 43.06 KB (329 Pkts.)
IPv4: 192.168.1.146/24

Restart Stop Edit Delete

The **WWAN (Wireless Wide Area Network)** interface allows the device to connect to an external Wi-Fi network as a **client**, functioning similarly to how a laptop or smartphone connects to a hotspot or access point. This interface is typically used when a wired WAN or cellular connection is unavailable.

By default, this interface is **disabled** to prevent unintentional conflicts with other network interfaces.

wwan
radio0.network1

Protocol: DHCP client
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
Error: Network device is not present

Restart Stop Edit Delete

N

ote: It is strongly recommended to use **only one wireless interface** for external network access at a time. Using both the **WWAN interface (Wi-Fi client)** and **4G cellular** as uplinks simultaneously can cause routing conflicts. This may lead to unpredictable network behavior, as the system may be unable to clearly determine which interface to use for outgoing traffic.

Key Details Shown in the Status Panel:

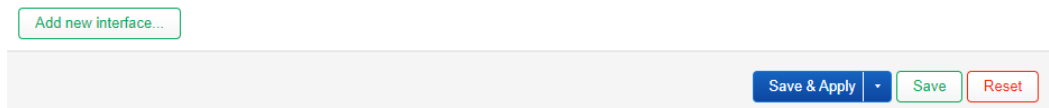
- **Interface Name:** Represents the logical name of the Wi-Fi WAN connection (e.g., wwan).
- **Associated Device:** Indicates the internal wireless radio (e.g., radio0) used for the connection.
- **Protocol:** Usually set to **DHCP client**, meaning the device will automatically request an IP address from the upstream Wi-Fi network.
- **MAC Address:** The MAC address of the radio module.
- **RX/TX:** Shows the amount of data received and transmitted over the wireless link. If values are zero, the connection may not be established.
- **Error Message:** If the message “Network device is not present” appears, it means the wireless hardware is either disabled, unconfigured, or failed to connect. (Not Enable State)
- **IPv4:** The IP address of the interface. Obtain the IP address from the AP in DHCP client mode.

Control Options:

- **Restart** – Attempts to reconnect to the Wi-Fi network.
- **Stop** – Disables the wireless client connection.
- **Edit** – Opens configuration settings to set SSID, password, or network mode.
- **Delete** – Removes the WWAN interface configuration (for advanced users only).

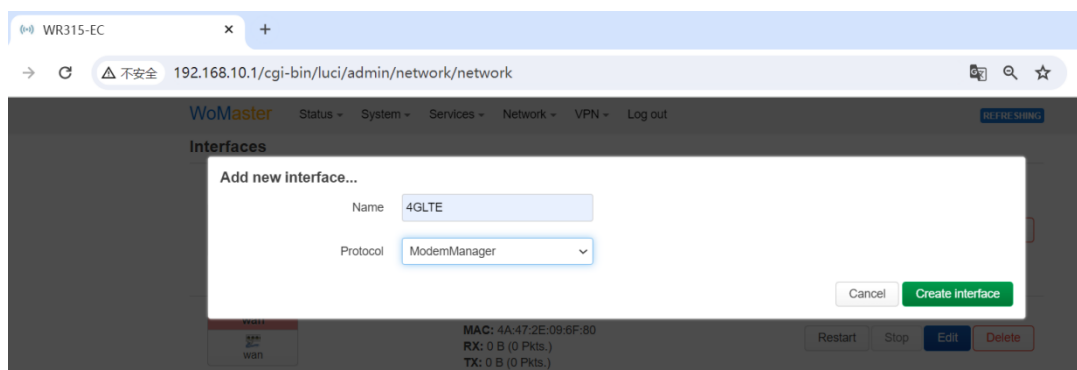
■ 3.4.4.4 Add new Interface

The following example demonstrates how to restore a 4G network interface in case it is accidentally deleted. This procedure is provided solely for recovery purposes and should not be used for general configuration or hardware modifications.



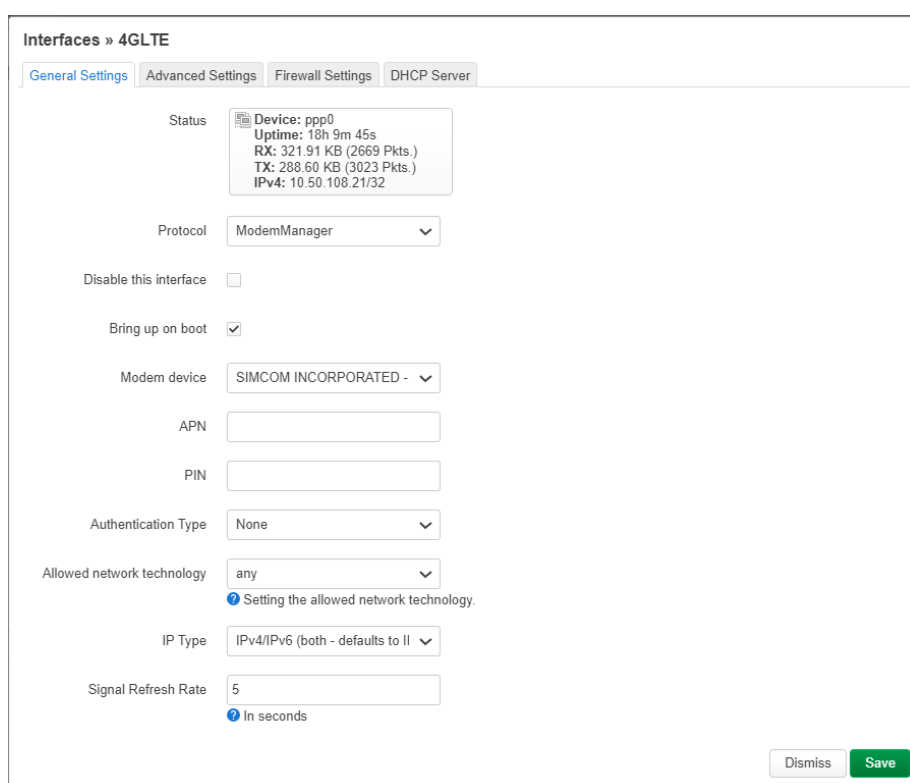
Click on “Add new interface”.

Set parameters in the pop-up window. Enter the name and select “ModemManager” from the dropdown menu.



Click on “Create interface”. The following window will pop up.

Then type the APN...settings.



After configured, then click on “Save”, it will return to the Interfaces page.

WoMaster
Status
System
Services
Network
VPN
Log out
REFRESHING
UNSAVED CHANGES: 7

Interfaces
Devices
Global network options

Interfaces

4GLTE modemmanager-4GLTE	Protocol: ModemManager Interface has 7 pending changes	Restart Stop Edit Delete
lan br-lan	Protocol: Static address Uptime: 18h 13m 35s MAC: 4A:01:DD:26:20:82 RX: 1.65 MB (12660 Pkts.) TX: 7.28 MB (10715 Pkts.) IPv4: 192.168.10.1/24 IPv6: fd::1/60	Restart Stop Edit Delete
wan br-wan	Protocol: DHCP client RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	Restart Stop Edit Delete
wan6 br-wan6	Protocol: DHCPv6 client RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	Restart Stop Edit Delete
wwan phy0-ap0	Protocol: DHCP client MAC: F8:54:F6:89:48:94 RX: 76.05 KB (691 Pkts.) TX: 8.05 MB (24714 Pkts.)	Restart Stop Edit Delete

Add new interface...

Save & Apply
Save
Reset

3.4.3.2 Wireless(Wi-Fi)

Here is the web interface for you to configure Wi-Fi settings.

In initial state, the Wi-Fi interface is disabled. And there is no associated station.

Wireless Overview

radio0	Generic MAC80211 802.11ac/ax/b/g/n <i>Device is not active</i>	Restart Scan Add
disabled	SSID: Wireless Mode: Client <i>Wireless is disabled</i>	Enable Edit Remove

Associated Stations

Network	MAC address	Host	Signal / Noise	RX Rate / TX Rate
No information available				

Save & Apply
Save

Click “Scan” to scan the Wi-Fi network over the air. Below screen shows part of the wireless network the router has discovered...

Join Network: Wireless Scan						
Signal	SSID	Channel	Mode	BSSID	Encryption	
 -52 dBm	WOMTEK_Guest	1	Master	B0:6E:BF:3B:A7:F9	WPA2 PSK (CCMP)	Join Network
 -52 dBm	WOMTEKex(Mobile)	1	Master	B0:6E:BF:3B:A7:F8	WPA2 PSK (CCMP)	Join Network
 -56 dBm	WOMTEKex(Mobile)_5G	149	Master	B0:6E:BF:3B:A7:FC	WPA2 PSK (CCMP)	Join Network
 -60 dBm	WOMTEKex(Mobile)	1	Master	00:0A:52:0B:2E:54	WPA2 PSK (CCMP)	Join Network

Select the target AP you want to connect and click **“Join Network”**.

Joining Network: "WOMTEKex(Mobile)"

Replace wireless configuration ☐

☒ Check this option to delete the existing networks from this radio.

Name of the new network

☒ Name for OpenWrt network configuration. (No relation to wireless network name/SSID)
The allowed characters are: `A-Z`, `a-z`, `0-9` and `_`

WPA passphrase

☒ Specify the secret encryption key here.

Lock to BSSID ☐

☒ Instead of joining any network with a matching SSID, only connect to the BSSID `B0:6E:BF:3B:A7:F8`.

Create / Assign firewall-zone wan wan6 wwan cellular

☒ Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *custom* field to define a new zone and attach the interface to it.

Type the WPA password, and click **“Submit”**. Then the Device Configuration pop-up window appears and you can configure the Wi-Fi parameters here.

Wireless Network: Client "WOMTEKex(Mobile)" (radio0.network2)

Device Configuration

Status **Mode:** Client | **SSID:** WOMTEKex(Mobile)
--- dBm Wireless is not associated

Wireless network is enabled

Operating frequency

Mode	Band	Channel	Width
AX	5 GHz	auto	20 MHz

Maximum transmit power driver default - Current power: *unknown*

☒ Specifies the maximum transmit power the wireless radio may use. Depending on regulatory requirements and wireless usage, the actual transmit power may be reduced by the driver.

Interface Configuration

Mode Client

ESSID WOMTEKex(Mobile)

BSSID

Network wwan

☒ Choose the network(s) you want to attach to this wireless interface or fill out the *custom* field to define a new network.

Wireless Security setting:

Interface Configuration

Encryption WPA2-PSK (strong security)

Cipher auto

Key

802.11w Management Frame Protection Disabled

☒ Note: Some wireless drivers do not fully support 802.11w. E.g. mwlwifi may have problems

After configured, click **“Save”** to apply the settings.

○ Applying configuration changes... 86s

After applied the settings, you can see the SSID you connect in the Wireless Overview.

Wireless Overview

	Generic MAC80211 802.11ac/ax/b/g/n <i>Device is not active</i>	<button>Restart</button> <button>Scan</button> <button>Add</button>
	SSID: Wireless Mode: Client <i>Wireless is disabled</i>	<button>Enable</button> <button>Edit</button> <button>Remove</button>
	SSID: WOMTEKex(Mobile) Mode: Client <i>Wireless is disabled</i>	<button>Enable</button> <button>Edit</button> <button>Remove</button>

Click “**Enable**” of the interface with SSID you select. While you see the link quality, BSSID and Encryption info, it means you already connect to the target AP. You can also see the Associated Station table on the same page.

Wireless Overview

	Generic MAC80211 802.11ac/ax/b/g/n Channel: 1 (2.412 GHz) Bitrate: 52 Mbit/s	<button>Restart</button> <button>Scan</button> <button>Add</button>
	SSID: Wireless Mode: Client <i>Wireless is disabled</i>	<button>Enable</button> <button>Edit</button> <button>Remove</button>
	SSID: WOMTEKex(Mobile) Mode: Client BSSID: 44:FA:66:9C:FF:E3 Encryption: WPA2 PSK (CCMP)	<button>Disable</button> <button>Edit</button> <button>Remove</button>

Associated Stations

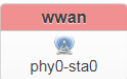
Network	MAC address	Host	Signal / Noise	RX Rate / TX Rate
 Client "WOMTEKex(Mobile)" (phy0-sta0)	B0:6E:BF:3B:A7:F8	?	 -51 dBm	130.0 Mbit/s, 20 MHz, MCS 15 52.0 Mbit/s, 20 MHz, MCS 11

Save & Apply Save

In Associated Stations list, you can see the wireless network you join, signal quality, RX/TX rate and bandwidth information. Click “**Save&Apply**” to permanently activate.

To see the Wi-Fi information, you can also find the changed in the **Network Interface** and **STATUS overview**.

Network Interface: wwan

	Protocol: DHCP client Uptime: 0h 1m 57s MAC: 44:FA:66:9C:FF:E3 RX: 116.50 KB (662 Pkts.) TX: 43.06 KB (329 Pkts.) IPv4: 192.168.1.146/24	<button>Restart</button> <button>Stop</button> <button>Edit</button> <button>Delete</button>
---	---	--

3.4.4.3 Routing

Our device has preset **LAN to wwan(Wi-Fi) /cellular(4G LTE)** routing rules. You can find it on the STATUS-Routing page. If it is not enough for your use, you can add new rules here.

STATUS-Routing:

Routing

The following rules are currently active on this system.

IPv4 Routing IPv6 Routing

IPv4 Neighbours

IP address	MAC address	Interface
192.168.10.142	38:D5:47:94:13:35	lan
192.168.1.1	B0:6E:BF:3B:A7:F8	wwan

Active IPv4 Routes

Device	Target	Gateway	Metric	Table	Protocol
wwan	0.0.0.0/0	192.168.1.1	0	main	static
cellular	10.64.64.64	-	0	main	kernel
wwan	192.168.1.0/24	-	0	main	kernel
lan	192.168.10.0/24	-	0	main	kernel

Click **“Add”**, you can add new rules, but be careful not to conflict with each other.

Routing

Routing defines over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes Static IPv6 Routes IPv4 Rules IPv6 Rules

Static IPv4 Routes

Interface	Target	Gateway	Metric	Table	Disable
-----------	--------	---------	--------	-------	---------

This section contains no values yet

Add

Save & Apply Save Reset

3.4.4.4 DHCP and DNS

The DHCP Server feature is enabled by default configuration. You can find this in DHCP Server feature set of the Interface-Lan, as shown in below screen. The default IP of the lan interface is 192.168.10.1. It means the IP pool is started from 192.168.10.100 to 192.168.10.150. The default DHCP lease time is 12h.

Interface – lan – edit – DHCP Server

Interfaces » lan

General Settings Advanced Settings Firewall Settings **DHCP Server**

General Setup Advanced Settings IPv6 Settings IPv6 RA Settings

Ignore interface ☐

[?](#) Disable DHCP for this interface.

Start

[?](#) Lowest leased address as offset from the network address.

Limit

[?](#) Maximum number of leased addresses.

Lease time

[?](#) Expiry time of leased addresses, minimum is 2 minutes ().

Dismiss Save

In **Status Overview**, you can find the connected clients and the IP address they obtained.

Active DHCP Leases

Hostname	IPv4 address	MAC address	Lease time remaining	Static Lease
Porsche-P5430UA (Porsche-P5430UA.lan)	192.168.10.142	38:D5:47:94:13:35	10h 21m 22s	Set Static

This is the **DHCP and DNS configuration page** in OpenWrt’s LuCI web interface, where the system is using **Dnsmasq** as a lightweight **DHCP server** and **DNS forwarder**. Here’s a breakdown of what each setting means:

DHCP and DNS

Dnsmasq is a lightweight DHCP server and DNS forwarder.

Delete

CFG01411C

General

Devices & Ports

Filter

Forwards

Limits

Log

Resolv & Hosts Files

Static Leases

Relay

Authoritative

☒

?

This is the only DHCP server in the local network.

Resolve these locally

/lan/

?

Never forward these matching domains or subdomains; resolve from DHCP or hosts files only.

Local domain

lan

?

Local domain suffix appended to DHCP names and hosts file entries.

Expand hosts

☐

?

Add local domain suffix to names served from hosts files.

Addresses

/router.local/router.lan/192.168.0.1

+

?

Resolve specified FQDNs to an IP.
Syntax: `/fqdn[/fqdn...]/[ipaddr]`.
`/example.com/` returns `NXDOMAIN`.
`/#/` matches any domain (and returns `NXDOMAIN`).
`/example.com/#` returns `NULL` addresses (`0.0.0.0`, `::`) for `example.com` and its subdomains.

In **General** setting, the **Authoritative** is Checked. This tells Dnsmasq to **act as the only DHCP server** on the local network. If a device requests an IP and isn't known, Dnsmasq will respond definitively (rather than ignoring the request). The **Resolve these locally** and **Local domain** are applied to **lan**.

In **Static Lease**, you can assign specific MAC to specific host. You can also configure DHCP Relay in **Relay** setting.

CFG01411C

General

Devices & Ports

Filter

Forwards

Limits

Log

Resolv & Hosts Files

Static Leases

Relay

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

Use the *Add* Button to add a new lease entry. The *MAC address* identifies the host, the *IPv4 address* specifies the fixed address to use, and the *Hostname* is assigned as a symbolic name to the requesting host. The optional *Lease time* can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.

The tag construct filters which host directives are used; more than one tag can be provided, in this case the request must match all of them. Tagged directives are used in preference to untagged ones. Note that one of mac, duid or hostname still needs to be specified (can be a wildcard).

Hostname	MAC address(es)	IPv4 address	Lease time	DUID	IPv6-Suffix (hex)	Tag	Match Tag
This section contains no values yet							

Add

Active DHCP Leases

Hostname	IPv4 address	MAC address	Lease time remaining
Porsche-P5430UA (Porsche-P5430UA.lan)	192.168.10.142	38:D5:47:94:13:35	10h 14m 0s

3.4.4.5 Diagnostics

This section is used to test network connectivity and DNS resolution from the router itself. It provides simple but essential tools to troubleshoot network issues. Type the target IP address and the tool to diagnostic.

Diagnostics

Execution of various network commands to check the connection and name resolution to other systems.

The screenshot shows the OpenWrt Diagnostics interface with three tool configurations:

- IPv4 Ping:** Target is 'openwrt.org'. Below the input field is a dropdown menu showing 'IPv4 Ping'.
- IPv4 Traceroute:** Target is 'openwrt.org'. Below the input field is a dropdown menu showing 'IPv4 Traceroute'.
- Nslookup:** Target is 'openwrt.org'. Below the input field is a button labeled 'Nslookup'.

The output of the IPv4 Ping command is displayed in a text area:

```
PING openwrt.org (64.226.122.113): 56 data bytes
64 bytes from 64.226.122.113: seq=0 ttl=50 time=228.133 ms
64 bytes from 64.226.122.113: seq=1 ttl=50 time=227.504 ms
64 bytes from 64.226.122.113: seq=2 ttl=50 time=229.257 ms
64 bytes from 64.226.122.113: seq=3 ttl=50 time=230.009 ms
64 bytes from 64.226.122.113: seq=4 ttl=50 time=230.030 ms

--- openwrt.org ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 227.504/228.986/230.030 ms
```

■ IPv4 Ping

Send Ping (ICMP echo requests) to the specified host. It is useful for checking **connectivity** and **response time**. In the screenshot, “openwrt.org” is the target host, you can type target host’s IP address here. The responded successfully with **0% packet loss** and round-trip times between ~227–230ms.

■ IPv4 Traceroute

Trace the path (hops) from the router to the target host. It helps diagnose **routing issues** or determine where a connection might be failing.

■ Nslookup

Perform a DNS lookup to check if the router can **resolve a domain name to an IP address**. It’s useful for checking if DNS is working properly.

3.4.4.5 Firewall

The firewall feature manages traffic between network zones (e.g., LAN/WAN) using policies, NAT, and packet filtering. This default firewall setting is very safe and is usually used in WAN interface (4G module, wireless wan, Ethernet-wan to ISP). Prevent external access to the router or internal network. At the same time, allow intranet devices to access the Internet normally through NAT.

[General Settings](#) [Port Forwards](#) [Traffic Rules](#) [NAT Rules](#) [IP Sets](#)

Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection ☒

Drop invalid packets ☐

Input

Output

Forward

Routing/NAT Offloading

Experimental feature. Not fully compatible with QoS/SQM.

Software flow offloading ☐

[?](#) Software based offloading for routing/NAT

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	
lan ⇒ wan	accept	accept	accept	☐	Edit Delete
wan ⇒ REJECT	reject	accept	reject	☒	Edit Delete

[Add](#)

[Save & Apply](#) [Save](#) [Reset](#)

Key sections include:

■ General Settings

SYN-flood Protection: Checked.

Purpose: To prevent SYN flood attacks, which is a common DDoS (Distributed Denial of Service) attack method.

Attack method: Send a large number of TCP SYN packets in a short period of time, so that system resources are exhausted and the connection cannot be established.

Once enabled, the router will limit or discard connection requests with abnormal frequencies to reduce the risk of service interruption.

Drop Invalid Packets: Discards malformed or suspicious packets (e.g., invalid TCP flags).

Input: REJECT (blocks incoming traffic from the internet, ex: SSH, HTTP from internet).

Output: ACCEPT (allows outgoing traffic from the router).

Forward: REJECT (blocks traffic routed through the router between interfaces).

■ Zones

Zones define security boundaries for interfaces (e.g., LAN, WAN). Each zone has policies for traffic flow:

Example Zones:

lan Zone:

Forwardings: wan (routes traffic to the WAN zone).

Policies:

Input/Output/Forward: ACCEPT (allows all internal LAN traffic).

Masquerading: Enabled (NAT: hides LAN IPs behind the WAN IP).

wan Zone (External Network):

Policies:

Input: **REJECT** (blocks incoming traffic from the internet, ex: SSH, HTTP from internet is blocked).

Output: ACCEPT (allows the router to send traffic to the internet).

Forward: **REJECT** (blocks traffic from WAN to other zones).

This design is very safe and is usually used in WAN interface (4G module, wireless wan, Ethernet-wan to ISP).

Prevent external access to the router or internal network. At the same time, allow intranet devices to access the Internet normally through NAT.

Actions

Add: Create new zones (e.g., VPN, guest network).

Edit/Delete: Modify or remove zone rules.

■ Routing/NAT Offloading

Software Flow Offloading: Optimizes routing/NAT performance by offloading tasks to the CPU.

Note: Marked as *experimental*; may conflict with QoS/SQM (traffic shaping).

Buttons

Save & Apply: Commit changes and reload the firewall.

Save: Store changes without applying.

Reset: Discard unsaved changes.

■ Additional Tabs

Port Forwards: Redirect external traffic to internal services (e.g., hosting a server). You can specify the protocol from the source zone (wan), external port to destination zone (lan), internal IP address and port.

Firewall - Port Forwards - Unnamed forward

General Settings Advanced Settings

Name Unnamed forward

Restrict to address family automatic

Protocol TCP UDP

Source zone wan wan: wan6: cellular: wwan:

External port

Match incoming traffic directed at the given destination port or port range on this host

Destination zone lan lan:

Internal IP address any

Redirect matched incoming traffic to the specified internal host

Internal port any

Redirect matched incoming traffic to the given port on the internal host

Dismiss Save

Traffic Rules: Define custom rules. Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

NAT Rules: Configure advanced Network Address Translation.

Firewall - NAT Rules - Unnamed NAT

General Settings Advanced Settings Time Restrictions

Name Unnamed NAT

Restrict to address family automatic

Protocol Any

Outbound zone lan lan:

Source address any

Match forwarded traffic from this IP or range.

Destination address any

Match forwarded traffic directed at the given IP address.

Action SNAT - Rewrite to specific source

Rewrite IP address unspecified

Rewrite matched traffic to the specified source IP address.

Dismiss Save

IP Sets: Manage groups of IPs/networks for simplified rule creation.

When configuring NAT features in OpenWrt, it is important to understand how source and destination zones are

defined. The following table summarizes common NAT use cases and their typical zone settings:

NAT Function	Source Zone (Outbound)	Destination Zone (Inbound)	Description
Masquerading (Source NAT)	LAN	WAN	Allows internal devices to access the internet by translating their IP to the router's public IP address.
Port Forwarding	WAN	LAN	Redirects incoming traffic from the internet to specific internal devices or services.
SNAT/DNAT Rules	Usually LAN	WAN or LAN	Enables custom translation of source or destination IP addresses for advanced routing needs.

Notes:

Masquerading is used for outbound traffic from LAN to WAN.

Port Forwarding handles inbound connections to internal services from the WAN.

Incorrect zone assignments may cause NAT to fail or create security vulnerabilities.

3.4.4 Services/Watchcat

Here's an overview of **Watchcat** features in OpenWrt's web UI (LuCI):

Watchcat

Here you can set up several checks and actions to take in the event that a host becomes unreachable. Click the **Add** button at the bottom to set up more than one action.

Watchcat

These rules will govern how this device reacts to network events.

Delete

General Settings

Mode

Ping Reboot

Ping Reboot

Periodic Reboot

Restart Interface

Run Script

Run Script: Run a script on a ping to a specified host fails for a specified duration of time.

Periodic Reboot: Reboot the router after a specified interval of time.

Restart Interface: Restart the network interface if a ping to a specified host fails for a specified duration of time.

Run Script: Run a script on a ping to a specified host fails for a specified duration of time.

Period

6h

?

In Periodic Reboot mode, it defines how often to reboot.

In Ping Reboot mode, it defines the longest period of time without a reply from the Host To Check before a reboot is engaged.

In Network Restart or Run Script mode, it defines the longest period of time without a reply from the Host to Check before the interface is restarted or the script is run.

The default unit is seconds, without a suffix, but you can use the suffix **m** for minutes, **h** for hours or **d** for days.

Examples:

10 seconds would be: 10 or 10s

5 minutes would be: 5m

1 hour would be: 1h

1 week would be: 7d

Host To Check

8.8.8.8

■ Ping Reboot for connectivity monitoring

Ping-Based Monitoring: Continuously checks internet connectivity by pinging a reliable server (e.g., 8.8.8.8 or a custom IP/domain).

Period: In Periodic Reboot mode, it defines how often to reboot.

Host To Check: Target IP address or hostname to ping. Ex: 8.8.8.8 (google)

Check (Ping) Interval: Adjust the frequency of connectivity checks (e.g., every 10 seconds). Examples: 10 seconds would be: 10 or 10s, 5 minutes would be: 5m, 1 hour would be: 1h, 1 week would be: 7d

Force Reboot Delay: Applies to Ping Reboot and Periodic Reboot modes. When rebooting the router, the service will trigger a soft reboot. Entering a non-zero value here will trigger a delayed hard reboot if the soft reboot were to fail. Enter the number of seconds to wait for the soft reboot to fail or use 0 to disable the forced reboot delay

■ Scheduled Periodic Reboots

Periodic Reboot: Forces the router to reboot at defined intervals (e.g., daily/weekly) to prevent memory leaks or software instability.

Period: Configure specific reboot times (e.g., every 24 hours) or use cron-like syntax for precise scheduling.

Examples: 10 seconds would be: 10 or 10s, 5 minutes would be: 5m, 1 hour would be: 1h, 1 week would be: 7d

71

3.4.5 VPN

In UCLI web interface, it provides the OpenVPN.
For IPSec or others, please use SSH to configure.

OpenVPN

OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

Name	Enabled	Started	Start/Stop	Port	Protocol		
custom_config	☐	no	<button>start</button>	-	-	<button>Edit</button>	<button>Delete</button>
sample_server	☐	no	<button>start</button>	1194	udp	<button>Edit</button>	<button>Delete</button>
sample_client	☐	no	<button>start</button>	-	udp	<button>Edit</button>	<button>Delete</button>

Template based configuration

Add

OVPN configuration file upload

選擇檔案

未選擇任何檔案

Upload

Save & Apply

Save

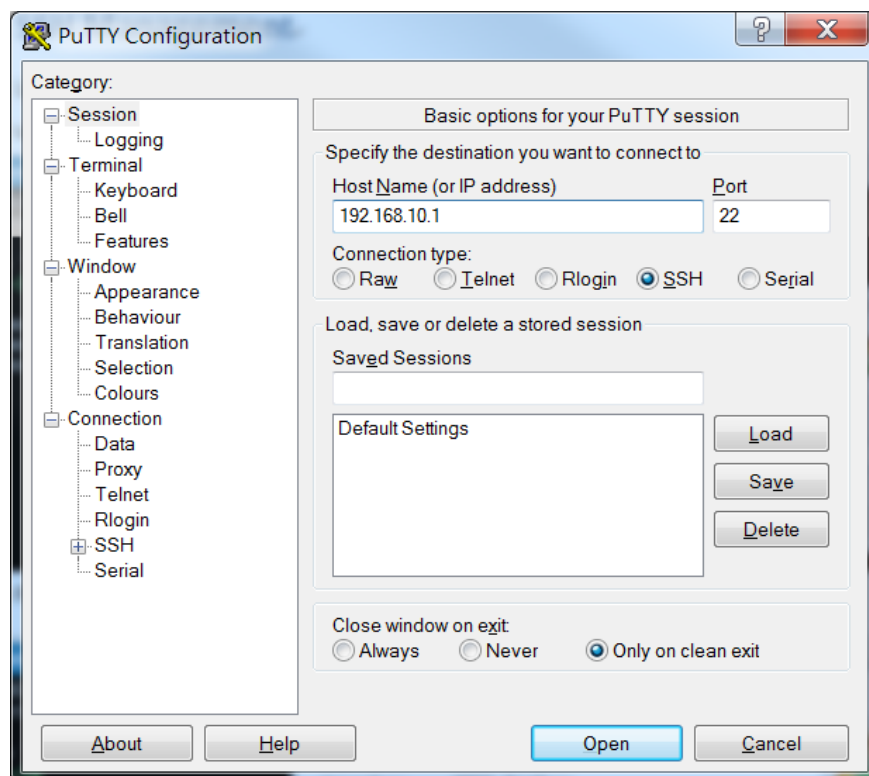
Reset

4. SSH Management

4.1 Login the router through SSH

There are both paid and free SSH terminal software available online, for example Putty, OpenSSH, XShell, MobaXterm...etc. Below is an example by using PuTTY.

Open SSH Terminal Tool, type the IP address and SSH port of the router. Ex: 192.168.10.1, port 22

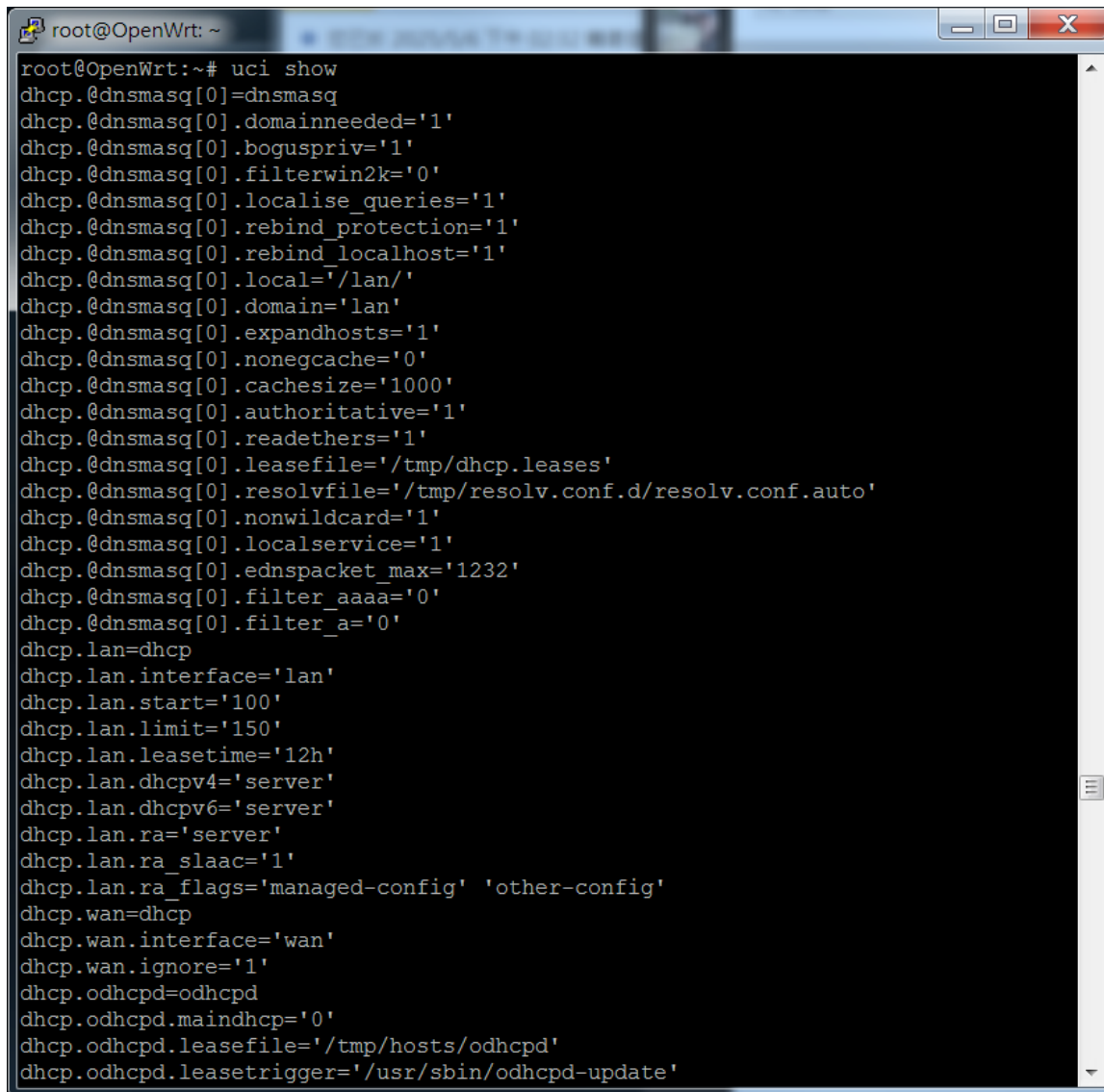


Enter username : root

Enter Password : root (default)

Read Configuration File:

root@OpenWrt:~# uci show

A screenshot of a terminal window titled 'root@OpenWrt: ~'. The terminal displays the output of the 'uci show' command, which lists various configuration settings for the DHCP service. The settings are organized into sections: @dnsmasq[0], lan, wan, and odhcpd. The @dnsmasq[0] section includes settings like domainneeded, boguspriv, filterwin2k, localise_queries, rebind_protection, rebind_localhost, local, domain, expandhosts, nonegcache, cachesize, authoritative, readethers, leasefile, resolvfile, nonwildcard, localservice, ednspacket_max, filter_aaaa, and filter_a. The lan section includes interface, start, limit, leasetime, dhcpv4, dhcpv6, ra, ra_slaac, and ra_flags. The wan section includes interface, ignore, and odhcpd. The odhcpd section includes maindhcp, leasefile, and leasetrigger. The terminal window has a standard Linux-style title bar with minimize, maximize, and close buttons.

```
root@OpenWrt:~# uci show
dhcp.@dnsmasq[0]=dnsmasq
dhcp.@dnsmasq[0].domainneeded='1'
dhcp.@dnsmasq[0].boguspriv='1'
dhcp.@dnsmasq[0].filterwin2k='0'
dhcp.@dnsmasq[0].localise_queries='1'
dhcp.@dnsmasq[0].rebind_protection='1'
dhcp.@dnsmasq[0].rebind_localhost='1'
dhcp.@dnsmasq[0].local='/lan/'
dhcp.@dnsmasq[0].domain='lan'
dhcp.@dnsmasq[0].expandhosts='1'
dhcp.@dnsmasq[0].nonegcache='0'
dhcp.@dnsmasq[0].cachesize='1000'
dhcp.@dnsmasq[0].authoritative='1'
dhcp.@dnsmasq[0].readethers='1'
dhcp.@dnsmasq[0].leasefile='/tmp/dhcp.leases'
dhcp.@dnsmasq[0].resolvfile='/tmp/resolv.conf.d/resolv.conf.auto'
dhcp.@dnsmasq[0].nonwildcard='1'
dhcp.@dnsmasq[0].localservice='1'
dhcp.@dnsmasq[0].ednspacket_max='1232'
dhcp.@dnsmasq[0].filter_aaaa='0'
dhcp.@dnsmasq[0].filter_a='0'
dhcp.lan=dhcp
dhcp.lan.interface='lan'
dhcp.lan.start='100'
dhcp.lan.limit='150'
dhcp.lan.leasetime='12h'
dhcp.lan.dhcpv4='server'
dhcp.lan.dhcpv6='server'
dhcp.lan.ra='server'
dhcp.lan.ra_slaac='1'
dhcp.lan.ra_flags='managed-config' 'other-config'
dhcp.wan=dhcp
dhcp.wan.interface='wan'
dhcp.wan.ignore='1'
dhcp.odhcpd=odhcpd
dhcp.odhcpd.maindhcp='0'
dhcp.odhcpd.leasefile='/tmp/hosts/odhcpd'
dhcp.odhcpd.leasetrigger='/usr/sbin/odhcpd-update'
```

Scroll up/down to view all the configurations for the device.

Find the interface/configuration you want to manage, then you can use “uci set” command to modify the settings.

And you may need to restart that interface/service to activate.

Since there are lots of CLI commands, the manual can only list some of them. If the command is not listed in this manual, you can contact our technical support, find the command through internet, such as the openwrt web site, Chatgpt...etc.

4.2 Major OpenWRT CLI

This chapter introduces a selected subset of commonly used OpenWrt CLI commands for basic configuration and troubleshooting. Some commands have been customized for this product and may differ from the standard OpenWrt implementation, syntax, or default behavior. It does not cover every available Linux/OpenWrt command.

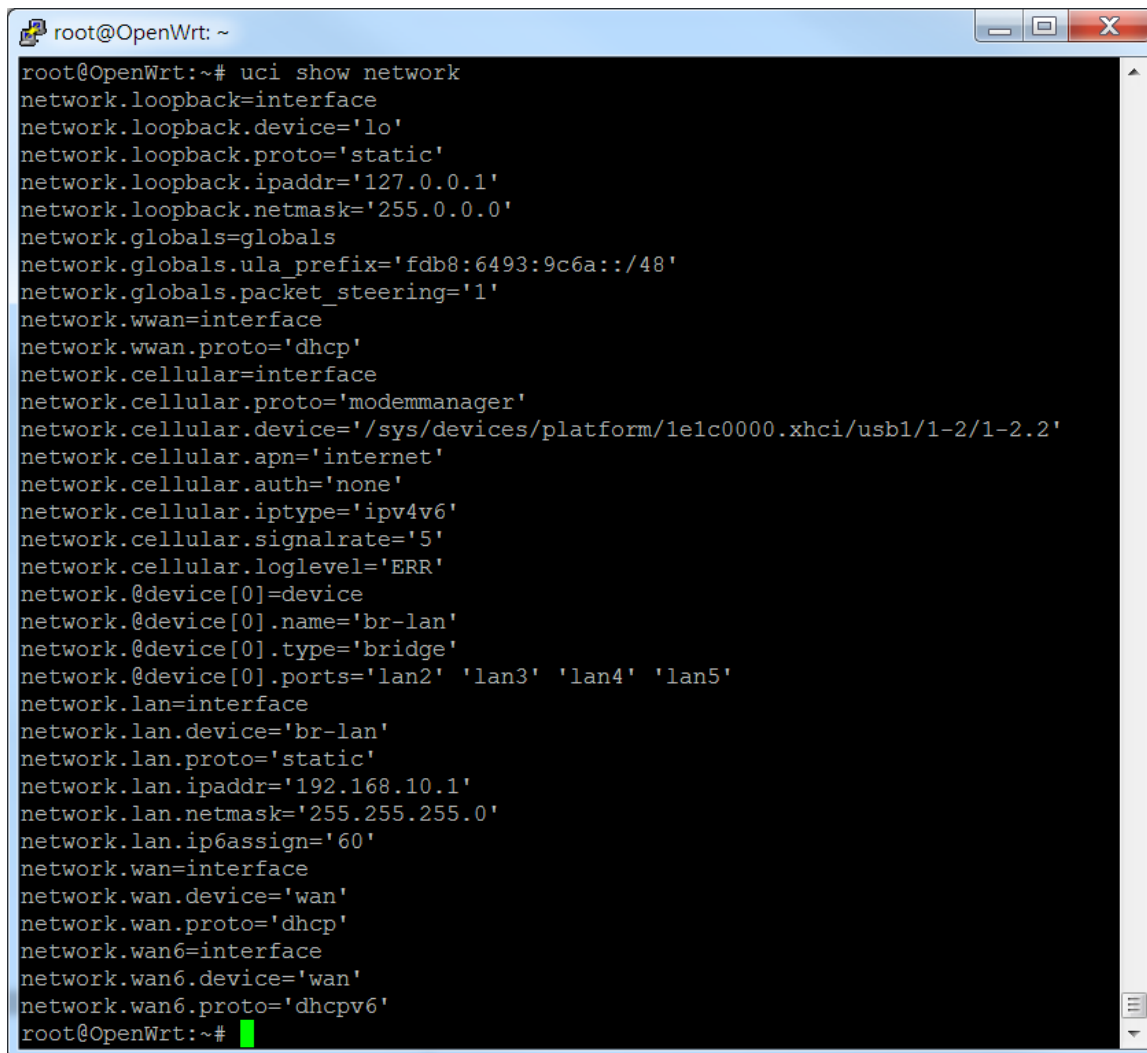
For further details on generic OpenWrt commands, please consult the official OpenWrt website (<https://openwrt.org>) or other reputable technical resources on the Internet. In case of any differences, please follow the behavior and examples described in this manual for this device.

A set of product-specific customized CLI commands is described in the next chapter, 4.3 Customized CLI. Where customized commands are provided for a given function, please follow the customized commands in preference to the generic OpenWrt commands shown in this chapter.

4.2.1 CLI - Cellular

The default configuration of the Cellular interface is enabled.

Use “**uci show network**”, you can find the default network related settings.



```
root@OpenWrt: ~  
root@OpenWrt:~# uci show network  
network.loopback=interface  
network.loopback.device='lo'  
network.loopback.proto='static'  
network.loopback.ipaddr='127.0.0.1'  
network.loopback.netmask='255.0.0.0'  
network.globals=globals  
network.globals.ula_prefix='fdb8:6493:9c6a::/48'  
network.globals.packet_steering='1'  
network.wwan=interface  
network.wwan.proto='dhcp'  
network.cellular=interface  
network.cellular.proto='modemmanager'  
network.cellular.device='/sys/devices/platform/1e1c0000.xhci/usb1/1-2/1-2.2'  
network.cellular.apn='internet'  
network.cellular.auth='none'  
network.cellular.ipvtype='ipv4v6'  
network.cellular.signalrate='5'  
network.cellular.loglevel='ERR'  
network.@device[0]=device  
network.@device[0].name='br-lan'  
network.@device[0].type='bridge'  
network.@device[0].ports='lan2' 'lan3' 'lan4' 'lan5'  
network.lan=interface  
network.lan.device='br-lan'  
network.lan.proto='static'  
network.lan.ipaddr='192.168.10.1'  
network.lan.netmask='255.255.255.0'  
network.lan.ip6assign='60'  
network.wan=interface  
network.wan.device='wan'  
network.wan.proto='dhcp'  
network.wan6=interface  
network.wan6.device='wan'  
network.wan6.proto='dhcpv6'  
root@OpenWrt:~#
```

■ Parameter change:

Below is an example of changing cellular's APN name and signal refresh rate. Use **"uci commit network"** to activate the setting.

```
root@OpenWrt:~# uci set network.cellular.apn='chtapn'
root@OpenWrt:~# uci set network.cellular.signalrate='10'
root@OpenWrt:~# uci commit network

root@OpenWrt:~# uci show network.cellular
network.cellular=interface
network.cellular.proto='modemmanager'
network.cellular.device='/sys/devices/platform/1e1c0000.xhci/usb1/1-2/1-2.2'
network.cellular.apn='chtapn'
network.cellular.auth='none'
network.cellular.ipctype='ipv4v6'
network.cellular.signalrate='10'
network.cellular.loglevel='ERR'
```

After modified the configuration, use below command to reload/restart the network interfaces:

```
root@OpenWrt:~# /etc/init.d/network reload    (reload the modified network interface)
root@OpenWrt:~# /etc/init.d/network restart    (restart all network interfaces)
```

Below is another command to watch the status of the cellular module.

■ **show cellular status**

```
root@OpenWrt:~# mmcli -m 0                    (index 0, you can use Any if it is not 0)
```

```

root@OpenWrt:~# mmcli -m 0
-----
General | path: /org/freedesktop/ModemManager1/Modem/0
        | device id: 981d3c47f8d7ff641b7b8faf200a20d4973309d0
-----
Hardware | manufacturer: SIMCOM INCORPORATED
        | model: SIMCOM_SIM7906G-M2
        | firmware revision: 2110B03X12M22A-M2
        | supported: gsm-umts, lte
        | current: gsm-umts, lte
        | equipment id: 869951070080837
-----
System | device: /sys/devices/platform/1e1c0000.xhci/usb1/1-2/1-2.2
        | drivers: option1
        | plugin: simtech
        | primary port: ttyUSB2
        | ports: ttyUSB0 (ignored), ttyUSB1 (gps), ttyUSB2 (at),
        |         ttyUSB3 (at), ttyUSB4 (audio)
-----
Status | unlock retries: sim-pin (3), sim-puk (10), sim-pin2 (3), sim-puk2 (10)
        | state: connected
        | power state: on
        | signal quality: 93% (cached)
-----
Modes | supported: allowed: 2g; preferred: none
        |         allowed: 3g; preferred: none
        |         allowed: 2g, 3g; preferred: none
        |         allowed: 2g, 3g; preferred: 2g
        |         allowed: 2g, 3g; preferred: 3g
        | current: allowed: any; preferred: none
-----
IP | supported: ipv4, ipv6, ipv4v6
-----
3GPP | imei: 869951070080837
        | operator id: 46011
        | operator name: CHN-CT
        | registration: home
        | packet service state: attached
-----
3GPP EPS | ue mode of operation: csps-2
-----
SIM | primary sim path: /org/freedesktop/ModemManager1/SIM/0
-----
Bearer | paths: /org/freedesktop/ModemManager1/Bearer/1
root@OpenWrt:~#

```

■ query the signal

root@OpenWrt:~# mmcli -m 0 --signal-get

```
root@OpenWrt:~# mmcli -m 0 --signal-get
-----
Signal | refresh rate: 5 seconds
      | rssi threshold: 0 dBm
      | error rate threshold: no
-----
LTE    | rsrq: -9.50 dB
      | rsrp: -85.00 dBm
root@OpenWrt:~#
```

■ 3) query the cellular time

root@OpenWrt:~# mmcli -m 0 --time

```
root@OpenWrt:~# mmcli -m 0 --time
-----
Time    | current: 2025-04-29T16:18:30+08
-----
Timezone | current: 480
root@OpenWrt:~#
```

root@OpenWrt:~# mmcli -m 0 --sim=0

```
root@OpenWrt:~# mmcli -m 0 --sim=0
-----
General | path: /org/freedesktop/ModemManager1/SIM/0
-----
Properties | active: yes
          | imsi: 460115134842244
          | iccid: 89860321745151703140
          | operator id: 46011
          | operator name: CT
root@OpenWrt:~#
```

4.2.2 CLI– lan

Use “**uci show network.lan**”, you can find the default network lan settings.

```
root@OpenWrt:~# uci show network.lan
network.lan=interface
network.lan.device='br-lan'
network.lan.proto='static'
network.lan.ipaddr='192.168.10.1'
network.lan.netmask='255.255.255.0'
network.lan.ip6assign='60'
```

■ Remove specific port/ports from the bri-lan interface.

Below is an example of removing the LAN port 4 and port 5 from the bridge-lan interface. This means that the port 4 and 5 are no longer used on the network.

```
root@OpenWrt:~# uci set network.@device[0].ports='lan2 lan3'
root@OpenWrt:~# uci commit network
root@OpenWrt:~# /etc/init.d/network reload
```

After changed the settings, use “**uci commit network**” and “**/etc/init.d/network reload**” to activate the new setting.

■ Change Router’s IP address:

```
root@OpenWrt:/# uci set network.lan.ipaddr='192.168.10.2'
root@OpenWrt:/# uci commit network
root@OpenWrt:/# /etc/init.d/network restart
```

■ Interface Shutdown

Interface shutdown command. But, this command can’t be saved in the configuration file, for temporary use.

```
root@OpenWrt:~# ifconfig lan3 down
```

■ Default Route

Use “**ip route**”, you can find the default route of the lan interface.

```
root@OpenWrt:~# ip route
default via 10.64.64.64 dev ppp0 proto static           (WAN: cellular ppp0 interface)
10.64.64.64 dev ppp0 proto kernel scope link src 10.128.173.51
192.168.10.0/24 dev br-lan proto kernel scope link src 192.168.10.1
```

NOTE: Currently, multiple default gateways are not supported. Therefore, if you enable multiple network segments simultaneously and disable the original default gateway, it may cause the default route to be lost. Please restart the default gateway interface or restart all network interfaces.

SSH command: **/etc/init.d/network restart**

4.2.3 CLI – WIFI(Wireless)

The default configuration of the Wi-Fi interface is **Enabled**.

The standard SSH commands described in this chapter are intended to be used in **station (client) mode only**.

Use “**uci show**”/“**uci show wireless**”, you can find the default settings of the wireless interface. For example:

====Default: Wi-Fi radio is Disabled====

```
wireless.radio0=wifi-device
wireless.radio0.type='mac80211'
wireless.radio0.path='1e140000.pcie/pci0000:00/0000:00:00.0/0000:01:00.0'
wireless.radio0.channel='auto'
wireless.radio0.band='5g'
wireless.radio0.htmode='HE20'
wireless.radio0.disabled='1'
wireless.default_radio0=wifi-iface
wireless.default_radio0.device='radio0'
wireless.default_radio0.network='wwan'
wireless.default_radio0.mode='sta'
wireless.default_radio0.ssid='Wireless'
wireless.default_radio0.encryption='none'
```

=====

Enable/Disable Wi-Fi Interface

Setting	Level	Function	Example
<code>wireless.radio0.disabled</code>	Physical layer (radio / PHY)	Controls whether the entire wireless radio (e.g., 2.4GHz or 5GHz module) is enabled. If set to 1 , the radio is completely disabled and the driver will not load.	Turns off the whole 2.4GHz or 5GHz hardware
<code>wireless.default_radio0.disable</code>	Logical layer (interface)	Controls whether a specific wireless interface (like an SSID in AP mode) is enabled under an active radio. The radio can be on, but individual SSIDs can be selectively turned off.	Keeps the radio on, but hides a specific SSID from broadcasting

Enable/Disable Physical Radio0:

```
root@OpenWrt:~# uci set wireless.radio0.disabled='0'      --Enable Wireless Radio0 interface
root@OpenWrt:~# uci set wireless.radio0.disabled='1'      --Disable Wireless Radio0 interface
```

Enable/Disable logical layer (SSID)

```
root@OpenWrt:~# uci set wireless.default_radio0.disable='0'  --Enable default wireless radio
root@OpenWrt:~# uci set wireless.default_radio0.disable='1'  --Disable default wireless radio
```

- `wireless.radio0.disabled='1'` → The radio is off, so no wireless signal is broadcast.
- `wireless.radio0.disabled='0'` and `wireless.default_radio0.disable='1'` → The radio is on, but SSID is disabled — interface won't broadcast.
- `wireless.radio0.disabled='0'` and `wireless.default_radio0.disable='0'` → Both the radio and SSID are active, so the Wi-Fi network is visible and working.

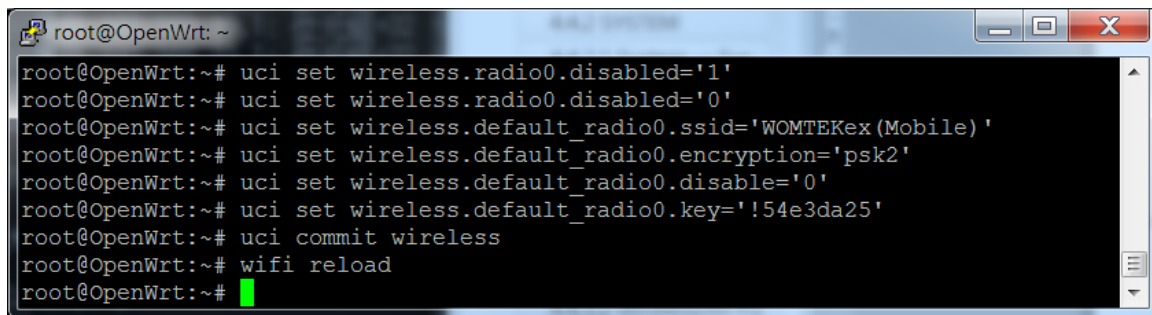
After changed the settings, use “**uci commit wireless**” and “**wifi reload**” to activate the new settings.

Change SSID Settings:

The router supports one physical radio interface and the default mode setting is client mode, you don't need to change the setting. You just need enter correct SSID, Encryption, Key and apply the settings.

Below is the example to use “**uci set**” to configure the wireless settings.

```
root@OpenWrt:~# uci set wireless.radio0.disabled='0'
root@OpenWrt:~# uci set wireless.default_radio0.ssid='WOMTEKex(Mobile)'
root@OpenWrt:~# uci set wireless.default_radio0.encryption='psk2'
root@OpenWrt:~# uci set wireless.default_radio0.disable='0'
root@OpenWrt:~# uci set wireless.default_radio0.key='!54e3da25'
root@OpenWrt:~# uci commit wireless
root@OpenWrt:~# wifi reload
```

A screenshot of a terminal window with a black background and white text. The window title is 'root@OpenWrt: ~'. The terminal shows the following commands and their outputs: 'uci set wireless.radio0.disabled='1'', 'uci set wireless.radio0.disabled='0'', 'uci set wireless.default_radio0.ssid='WOMTEKex(Mobile)'' (with a space before the quote), 'uci set wireless.default_radio0.encryption='psk2'', 'uci set wireless.default_radio0.disable='0'', 'uci set wireless.default_radio0.key='!54e3da25'', 'uci commit wireless', 'wifi reload', and finally a green cursor at the prompt 'root@OpenWrt:~#'.

```
root@OpenWrt:~# uci set wireless.radio0.disabled='1'
root@OpenWrt:~# uci set wireless.radio0.disabled='0'
root@OpenWrt:~# uci set wireless.default_radio0.ssid='WOMTEKex(Mobile) '
root@OpenWrt:~# uci set wireless.default_radio0.encryption='psk2'
root@OpenWrt:~# uci set wireless.default_radio0.disable='0'
root@OpenWrt:~# uci set wireless.default_radio0.key='!54e3da25'
root@OpenWrt:~# uci commit wireless
root@OpenWrt:~# wifi reload
root@OpenWrt:~#
```

After changed the settings, use “**uci commit wireless**” and “**wifi reload**” to activate the new settings.

Use “**uci show wireless**” to check the new settings:

====Enabled Wi-Fi radio0 interface and add new SSID/encryption/Key=====

```
wireless.radio0=wifi-device
wireless.radio0.type='mac80211'
wireless.radio0.path='1e140000.pcie/pci0000:00/0000:00:00.0/0000:01:00.0'
wireless.radio0.channel='auto'
wireless.radio0.band='5g'
wireless.radio0.htmode='HE20'
wireless.radio0.disabled='0'
wireless.default_radio0=wifi-iface
wireless.default_radio0.device='radio0'
wireless.default_radio0.network='wwan'
wireless.default_radio0.mode='sta'
wireless.default_radio0.ssid='WOMTEKex(Mobile)'
wireless.default_radio0.encryption='psk2'
wireless.default_radio0.disable='0'
wireless.default_radio0.key='!54e3da25'
```

=====

Note: When Cellular and WiFi are enabled at the same time, the default route may be changed to the wwan (wifi) interface. At this time, if you turn off the WiFi radio, the default route may be deleted. Please restart your cellular interface or reload/restart the network interface to restore it.

SSH command: /etc/init.d/network restart

```
root@OpenWrt:~# /etc/init.d/network restart
```

Wi-Fi Status: iwinfo

Station mode:

```
root@OpenWrt:/# iwinfo
```

```
phy0-sta0 ESSID: "Wireless_5G_1E8D10"  
    Access Point: DE:56:7B:D6:9B:A9  
    Mode: Client   Channel: 36 (5.180 GHz)   HT Mode: HE80  
    Center Channel 1: 42 2: unknown  
    Tx-Power: 3 dBm   Link Quality: 63/70  
    Signal: -47 dBm   Noise: unknown  
    Bit Rate: 1200.9 MBit/s  
    Encryption: WPA2 PSK (CCMP)  
    Type: nl80211   HW Mode(s): 802.11ac/ax/b/g/n  
    Hardware: 14C3:7922 105B:E132 [Generic MAC80211]  
    TX power offset: unknown  
    Frequency offset: unknown  
    Supports VAPs: no   PHY name: phy0
```

```
root@OpenWrt:~# iw dev phy0-sta0 info
```

```
Interface phy0-sta0
```

```
    ifindex 159
```

```
    wdev 0x2b
```

```
    addr de:56:7b:d6:9b:a9
```

```
    ssid Wireless_5G_1E8D10
```

```
    type managed
```

```
    wiphy 0
```

```
    channel 36 (5180 MHz), width: 80 MHz, center1: 5210 MHz
```

```
    txpower 3.00 dBm
```

```
    multicast TXQ:
```

qsz-byt	qsz-pkt	flowsdrops	marks	overlmt	hashcol	tx-bytes	tx-packets
0	0	0	0	0			

4.3 Customized CLI & Script

This chapter describes product-specific scripts and customized CLI commands. These commands are mainly provided for collecting device information, alarm control configuration, configuring Wi-Fi operating modes, and handling related precautions. In particular, Wi-Fi configuration on this product follows a specific design and command sequence; please configure Wi-Fi strictly according to the recommended procedures and examples in this chapter to ensure correct operation and regulatory compliance.

4.3.1 Get Information Script: `wr-info-get.sh`

Cellular Information Retrieval Script (`wr-info-get.sh`)

This script is a customized script after firmware V1.8 released. The script can help you to get the information of the router quickly.

This guide outlines how to use the command-line utility `wr-info-get.sh` to retrieve detailed information about your device's cellular modem, connection, and signal quality. The output for all commands is provided in JSON format.

Execution Command

To use the script, execute it with the desired information keyword as the argument:

Script name: `wr-info-get.sh`

Usage syntax:

`wr-info-get.sh [OPTIONS...] [-J]`

- Multiple options can be passed in one call; the script will output all requested fields in a single JSON object.
- JSON output is enabled by default. The `-J` flag is currently accepted but does not change the output format.

Available Information Keywords (Grouped)

1. System and Hardware information ⓘ

Keyword	Description	Information Retrieved
<code>sys_all</code>	Comprehensive system summary (various data points).	A single query to fetch all system-related parameters.
<code>version</code>	Firmware/Software Version	The current operating system or firmware version.
<code>model</code>	Device Model Name	The hardware model of the device.
<code>imei</code>	International Mobile Equipment Identity	Unique identifier for the modem hardware.
<code>meid</code>	Mobile Equipment Identifier	Used primarily for CDMA networks.
<code>provider</code>	Modem Vendor/Supplier	The manufacturer of the cellular modem.

2. Modem and SIM Status 📶

Keyword	Description	Information Retrieved
<code>modem_state</code>	Modem Operating Status	The current state of the modem (e.g., powered on, ready,

		error).
sim_info	SIM Card Summary	Comprehensive information about the SIM card status.
imsi	International Mobile Subscriber Identity	Unique identifier for the subscriber (your account).
iccid	SIM Card Serial Number	The unique serial number of the inserted SIM card.
pin	SIM Card PIN Status	Indicates if the PIN is required, verified, or disabled.

3. Network Registration and APN Settings 📶

Keyword	Description	Information Retrieved
connection_info	Connection Status Summary	A combined view of network registration and data service status.
operator_name	Mobile Network Operator Name	The name of the currently connected carrier (e.g., AT&T, O2).
operator_state	Network Registration Status	Indicates if the device is registered to the network (e.g., registered, searching). 0: not registered 1: registered, home network 2: not registered, but MT is trying to attach or searching an operator to register to 3: registration denied 4: unknown (ex: out of E-UTRAN coverage) 5: registered, roaming (not list, please check with our support engineer.)
data_service_state	Data Service Status	Indicates if the data connection is active (e.g., connected, disconnected).
operator_id	Operator ID	The numerical identifier for the network (e.g., MCC + MNC).
mcc / mnc	Mobile Country/Network Code	Codes identifying the country and the specific operator.
apn	Access Point Name	The name of the configured data access point.
auth	APN Authentication Type	The authentication protocol used for the APN (e.g., PAP, CHAP).
cell_user / cell_password	APN Credentials	Username and password for APN authentication (if required).
interface_addr / interface_addr_ipv6	Interface IP Address	The device's assigned IPv4 and IPv6 addresses on the cellular interface.
conn_date	Connection Timestamp	The time and date when the current connection was established.

4. Signal Strength and Quality Metrics 📶

These metrics are crucial for evaluating cellular performance.

Keyword	Description	Typical Use
rsqi / scc_rsqi	Received Signal Strength Indicator (Primary/Secondary Carrier)	General measurement of signal power. Higher (closer to 0) is better.
rsrp / scc_rsrp	Reference Signal Received Power (Primary/Secondary Carrier)	A more accurate measure of the power from the serving cell tower. Higher (closer to 0) is better.
rsrq / scc_rsrq	Reference Signal Received Quality (Primary/Secondary Carrier)	Measures the quality of the signal, considering noise and interference. Higher (closer to 0) is better.
sinr	Signal-to-Interference-plus-Noise Ratio	Measures the useful signal power relative to interference. Positive values are good.
rscp	Received Signal Code Power	Used for 3G (WCDMA) networks.
band_info	Detailed Cell/Band Information	Includes Cell ID, Band, EARFCN, DL/UL Bandwidth, and Carrier Aggregation (SCC) details.

5. Connection Details and Data Usage 📶

Keyword	Description	Information Retrieved
band_info	Detailed Cell/Band Information	Detailed metrics including Cell ID, Band, EARFCN (Frequency Channel), DL/UL Bandwidth, and Carrier Aggregation (SCC) details.
data_transmission_info	Data Transmission Summary	Combined summary of band, bandwidth, signal metrics, and data usage.
interface_addr / interface_addr_ipv6	Interface IP Address	The device's assigned IPv4 and IPv6 addresses on the cellular interface.
conn_date	Connection Timestamp	The time and date when the current connection was established.
cell_rx_bytes / cell_tx_bytes	Data Traffic (Received/Transmitted)	The total number of bytes downloaded (rx) and uploaded (tx) since the last modem restart or reset.
cell_rx_tx_bytes	Total Data Traffic	A combined output of both received and transmitted bytes.

6. Wi-Fi Client Connection Information (STA)

These commands are used when the device operates as a client (Station) connecting to an upstream Wi-Fi network.

Keyword	Description	Information Retrieved (Equivalent to)
---------	-------------	---------------------------------------

sta_info	Summary STA Connection Status	sta_state (Connection Status), ESSID, and Channel. Aggregates STA state, association, signal and data rates into a single JSON object.
sta_state	Detailed STA Connection Info	Returns the STA mode state, enabled or disabled.
sta_assoc		Returns association status and BSSID/SSID info.
sta_signal		Returns the Wi-Fi RSSI/Signal level for the STA link.
sta_rx_rate		Returns the current RX data rate of the STA link.
sta_tx_rate		Returns the current TX data rate of the STA link.
sta_addr		Returns the MAC address of the STA interface.

> Note: `sta\_tx\_power` is implemented internally but its CLI option is commented out in this version.

7. Multi-WAN path selection

- `network\_used` – Returns which uplink path is currently used by the system (e.g. wired WAN vs. cellular vs. Wi-Fi), based on routing and interface checks.

8. Alarm State and Status

These commands are used to monitor the alarm state and status.

Keyword	Description	Information Retrieved (Equivalent to)
alarm_state	Alarm state enabled or not enabled	Return: "alarm_state":0
alarm_status	Monitor the status of Ping alarm, high temperature alarm, Cellular and Wi-Fi module's hardware ready or not	You can see the specific alarm is activated or not. There are five different return types: "alarm_state":0, =>alarm state "alarm_ping":0, =>Ping alarm/watchdog "alarm_temperature":0, =>High Temperature alarm "alarm_hw_cellular":0, =>Cellular module hardware status "alarm_hw_wireless":0 =>Wi-Fi module hardware status

9. Formatting / flags

* `-j` – Reserved flag for JSON output. In this version it is accepted but does not modify behavior (JSON output is always enabled).

4.3.2 Wireless Operation Mode Script: wr-wireless-mode.sh

Wireless Operating Modes User Manual

Your device's Wi-Fi module is primarily designed to function as a client (Station), allowing it to connect to an external network. You can control the mode using the dedicated command line utility: wr-wireless-mode.sh.

Station (STA) Mode (Primary Client Mode)

Purpose: The default and most stable mode for accessing an external network.

Feature	Description
Role	Your device acts as a standard Wi-Fi client.
Connectivity	Connects to an external Wi-Fi router or access point (the upstream network).
Status	Active only when authenticated and connected.

Command: wr-wireless-mode.sh sta

Expected Output: return: success

Dynamic Frequency Selection (DFS)

What are DFS Bands?

DFS (Dynamic Frequency Selection) bands are a set of 5 GHz channels shared with high-priority radar systems. Wi-Fi equipment operating on these channels must constantly listen for radar and, if detected, **immediately cease transmission** and switch channels.

DFS Regulatory Declaration:

"DFS (Dynamic Frequency Selection) channel capability is enabled by default in STA (Client) mode, requiring no additional user configuration or commands. When operating as a client, the device automatically complies with the upstream AP's channel decisions and follows its operation within the DFS band. **All hardware and firmware restrictions regarding DFS parameters are strictly defined in accordance with regulatory requirements and are completely locked from user modification.**"

4.3.3 Alarm-Ctl Function

The **alarm-ctl** function monitors various hardware and network conditions and drives a GPIO output when an alarm is triggered. Each alarm type is configured as a separate **alarm-ctl** section in UCI and uses a common GPIO pin (default: gpio491) as the alarm output.

This chapter describes the following alarm types:

- Network Condition: Ping alarm (network reachability)
- Hardware Condition: Temperature alarm (LTE module temperature), Wireless module alarm (Wi-Fi hardware errors), LTE module alarm (cellular module presence)

Uci show to list all the alarm-ctl setting as below:

```
root@OpenWrt:/# uci show alarm-ctl
alarm-ctl.@alarm-ctl[0]=alarm-ctl
alarm-ctl.@alarm-ctl[0].gpio='gpio491'
alarm-ctl.@alarm-ctl[0].mode='none'
alarm-ctl.@alarm-ctl[0].target_ip='8.8.8.8'
alarm-ctl.@alarm-ctl[0].count='1'
alarm-ctl.@alarm-ctl[0].timeout='1'
alarm-ctl.@alarm-ctl[0].defer_time='15'
alarm-ctl.@alarm-ctl[0].interval='10'
alarm-ctl.@alarm-ctl[0].fail_limit='3'
alarm-ctl.@alarm-ctl[1]=alarm-ctl
alarm-ctl.@alarm-ctl[1].gpio='gpio491'
alarm-ctl.@alarm-ctl[1].mode='temperature'
alarm-ctl.@alarm-ctl[1].high='80'
alarm-ctl.@alarm-ctl[1].low='-30'
alarm-ctl.@alarm-ctl[1].interval='15'
alarm-ctl.@alarm-ctl[2]=alarm-ctl
alarm-ctl.@alarm-ctl[2].gpio='gpio491'
alarm-ctl.@alarm-ctl[2].mode='hw-wireless'
alarm-ctl.@alarm-ctl[2].interval='10'
alarm-ctl.@alarm-ctl[3]=alarm-ctl
alarm-ctl.@alarm-ctl[3].gpio='gpio491'
alarm-ctl.@alarm-ctl[3].mode='hw-cellular'
alarm-ctl.@alarm-ctl[3].interval='10'
```

4.3.3.1 Network Ping Alarm

The **Ping Alarm** function periodically sends ICMP echo requests (ping) to a target IP address. When consecutive ping failures reach the configured limit, the alarm state is triggered and the corresponding GPIO output can be used as an alarm signal.

```
root@OpenWrt:/# cat /etc/config/alarm-ctl
config alarm-ctl
    option gpio 'gpio491'
    option mode 'none'
    option target_ip '8.8.8.8'
    option count '1'
    option timeout '1'
    option defer_time '15'
    option interval '10'
    option fail_limit '3'
```

- i. **gpio**: Specifies the GPIO pin used for the alarm output. Default: gpio491 (No need to change this!!)

ii. **mode**: Controls whether the ping alarm function is enabled.

"ping" – enable ping alarm function

"none" – disable ping alarm function

iii. **target_ip**: Specifies the target IP address to be pinged (e.g. gateway, server, or DNS).

iv. **count**: Number of ping packets sent in each check cycle.

v. **timeout**: Ping timeout for each packet, in seconds.

vi. **defer_time**: Initial delay before the first ping check is started, in seconds.

vii. **interval**: Interval between ping check cycles, in seconds.

viii. **fail_limit**: Number of **consecutive** failed ping check cycles required to trigger the alarm.

Configuration Examples

(1) Enable Ping Alarm

The following example enables the ping alarm and pings 8.8.8.8 periodically:

```
uci set alarm-ctl.@alarm-ctl[0].mode='ping'
uci set alarm-ctl.@alarm-ctl[0].target_ip='8.8.8.8'
uci set alarm-ctl.@alarm-ctl[0].count='1'
uci set alarm-ctl.@alarm-ctl[0].timeout='1'
uci set alarm-ctl.@alarm-ctl[0].defer_time='15'
uci set alarm-ctl.@alarm-ctl[0].interval='10'
uci set alarm-ctl.@alarm-ctl[0].fail_limit='3'
uci commit alarm-ctl
/etc/init.d/alarm-ctl restart
```

In this example:

The first ping check starts after **15 seconds** (`defer_time='15'`). Then the device sends **1 ping** every **10 seconds** (`count='1'`, `interval='10'`). If **3 consecutive cycles** fail (`fail_limit='3'`), the alarm is triggered.

(2) Disable Ping Alarm

```
uci set alarm-ctl.@alarm-ctl[0].mode='none'
uci commit alarm-ctl
/etc/init.d/alarm-ctl restart
```

4.3.3.2 Hardware Condition Alarm

There are three different types Hardware Condition alarms: **Temperature alarm** (LTE module temperature), **Wireless module alarm** (Wi-Fi hardware errors), **LTE module alarm** (cellular module presence)

1. Temperature Alarm (LTE Module Temperature)

The **temperature alarm** monitors the temperature reported by the LTE module. If the measured temperature is higher than the configured **high** limit or lower than the configured **low** limit, the alarm is triggered and the GPIO output will indicate an alarm condition.

1)Parameters

gpio: Specifies the GPIO pin used for the alarm output. Default: gpio491

mode

Controls whether the temperature alarm is enabled.

"temperature" – enable temperature alarm

"none" – disable this alarm

High: High temperature threshold in degrees Celsius (integer).

Low: Low temperature threshold in degrees Celsius (integer).

Interval: Measurement interval in seconds.

2) Default configuration

Status: **Enabled**

gpio: gpio491

high: 80 °C

low: -30 °C

interval: 15 seconds

3) Configuration examples

Enable temperature alarm

```
uci set alarm-ctl.@alarm-ctl[1].mode='temperature'
uci set alarm-ctl.@alarm-ctl[1].high='10'
uci set alarm-ctl.@alarm-ctl[1].low='-10'
uci set alarm-ctl.@alarm-ctl[1].interval='15'
uci commit alarm-ctl
/etc/init.d/alarm-ctl restart
```

Disable temperature alarm

```
uci set alarm-ctl.@alarm-ctl[1].mode='none'
uci commit alarm-ctl
/etc/init.d/alarm-ctl restart
```

2. Wireless Module Alarm (Wi-Fi Hardware Errors)

The **wireless module alarm** checks for hardware-related errors during system boot and periodically scans the kernel log (dmesg) for Wi-Fi error messages.

1) Parameters

gpio: Specifies the GPIO pin used for the alarm output. Default: gpio491

mode: Controls whether the wireless-module alarm is enabled.

"hw-wireless" – enable wireless hardware alarm

"none" – disable this alarm

Interval: Polling interval in seconds for checking the kernel log.

2) Default configuration

Status: **Enabled**

gpio: gpio491

interval: 10 seconds

3) Configuration examples

Enable wireless module alarm

```
uci set alarm-ctl.@alarm-ctl[2].mode='hw-wireless'  
uci set alarm-ctl.@alarm-ctl[2].interval='15'  
uci commit alarm-ctl  
/etc/init.d/alarm-ctl restart
```

Disable wireless module alarm

```
uci set alarm-ctl.@alarm-ctl[2].mode='none'  
uci commit alarm-ctl  
/etc/init.d/alarm-ctl restart
```

3. LTE Module Alarm (Cellular Presence/Health)

The **LTE module alarm** periodically checks the LTE/cellular module hardware health.

1) Parameters

Gpio: Specifies the GPIO pin used for the alarm output. Default: gpio491

Mode: Controls whether the LTE-module alarm is enabled.

"hw-cellular" – enable LTE hardware alarm

"none" – disable this alarm

Interval: Polling interval in seconds for checking the LTE module status.

2) Default configuration

Status: **Enabled**

gpio: gpio491

interval: 10 seconds

3) Configuration examples

Enable LTE module alarm

```
uci set alarm-ctl.@alarm-ctl[3].mode='hw-cellular'  
uci set alarm-ctl.@alarm-ctl[3].interval='15'  
uci commit alarm-ctl  
/etc/init.d/alarm-ctl restart
```

Disable LTE module alarm

```
uci set alarm-ctl.@alarm-ctl[3].mode='none'  
uci commit alarm-ctl  
/etc/init.d/alarm-ctl restart
```

4.3.3.3 Reading Alarm Status

Get Alarm State

You can query the current alarm state using the following command:

Command: wr-info-get.sh alarm_state

Return values:

0 – alarm is not triggered

```
root@OpenWrt:/# wr-info-get.sh alarm_state
{
  "alarm_state":0
}
```

1 – alarm is triggered

```
root@OpenWrt:~# time wr-info-get.sh alarm_state
{
  "alarm_state":1
}
real    0m 0.04s
user    0m 0.02s
sys     0m 0.01s
root@OpenWrt:~#
```

Get Alarm Status

Command: wr-info-get.sh alarm_status

```
root@OpenWrt:/# wr-info-get.sh alarm_status
{
  "alarm_state":1,
  "alarm_ping":0,
  "alarm_temperature":0,
  "alarm_hw_cellular":0,
  "alarm_hw_wireless":1
}
```

Ex:

It shows the Wireless Module Alarm is triggered.

4.4 Firmware upgrade

- User can use **SCP** to upload firmware file to directory **/tmp**
`cd /tmp`
`wget http://your-server.com/firmware/openwrt-v1.9-ramips-mt7621-wom_wr315-ec-squashfs-sysupgrade.bin`
or
`scp /folder/openwrt-v1.9-ramips-mt7621-wom_wr315-ec-squashfs-sysupgrade.bin root@192.168.10.1:/tmp/`
(root@192.168.10.1 = Login username is root, Router IP is 192.168.10.1)

- **Firmware upgrade and keep configuration**

command: `sysupgrade -c firmware_name`

example: `upgrade /tmp/openwrt-v1.2-ramips-mt7621-wom_wr315-ec-squashfs-sysupgrade.bin` and keep configuration

```
root@OpenWrt:/# sysupgrade -c /tmp/openwrt-v1.2-ramips-mt7621-wom_wr315-ec-squashfs-sysupgrade.bin
Tue Jun  3 05:36:21 UTC 2025 upgrade: Saving config files...
rmmod mt7915e
```

- **Firmware upgrade and reload default**

command: `sysupgrade -n firmware_name`

example: `upgrade /tmp/openwrt-v1.2-ramips-mt7621-wom_wr315-ec-squashfs-sysupgrade.bin` and reload default

```
root@OpenWrt:/# sysupgrade -n /tmp/openwrt-v1.2-ramips-mt7621-wom_wr315-ec-squashfs-sysupgrade.bin
rmmod mt7915e
rmmod mt7921e
Tue Jun  3 05:44:11 UTC 2025 upgrade: Commencing upgrade. Closing all shell sessions.
```

- Firmware Upgrade Options Explained (LuCI vs. CLI sysupgrade)

Below is the screenshot of the firmware upgrading when using LuCI Web GUI. The LuCI options correspond directly to the parameters used in the CLI command `'sysupgrade'`.

Flash image?

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
Click 'Continue' below to start the flash procedure.

Size: 17.13 MiB
MD5: 09a7edf469ec88bc27360bfa18c5e696
SHA256: 8956a2a1d937fe2ae5cf526ae821f8ee70169d53dc473472b9dddadda9a3238f

☒ Keep settings and retain the current configuration

☐ Skip from backup files that are equal to those in /rom

☐ Include in backup a list of current installed packages at /etc/backup/installed_packages.txt

Cancel Continue

Firmware Upgrade While Keeping Configuration

(This corresponds to the ****checked**** “Keep settings and retain the current configuration” option shown in the screenshot.)

CLI Equivalent

1. ``sysupgrade -c``

The ``-c`` parameter keeps the current configuration and skips all files that are identical to those in ``/rom``.

This mode provides the most complete preservation of user settings while avoiding unnecessary backup files.

This is equivalent to:

- ✓ Keep settings and retain the current configuration
- ✓ Skip from backup files that are equal to those in /rom

2. ``sysupgrade`` (no parameters)

Without ``-c``, sysupgrade uses the default backup behavior. (The system backs up: ``/etc/`` and files listed in ``/lib/upgrade/keep.d/``)

This is equivalent to:

- ✓ Keep settings and retain the current configuration
- ✗ Skip from backup files that are equal to those in /rom (not selected)

Firmware Upgrade and Reset to Factory Defaults

(This corresponds to **NOT checking** “Keep settings and retain the current configuration”).

CLI Equivalent

``sysupgrade -n``

The ``-n`` parameter discards all current settings.

No configuration is backed up or restored after flashing.

The device boots with factory-default configuration.

This equals leaving all options unchecked:

- ✗ Keep settings and retain the current configuration
- ✗ Skip from backup files equal to /rom
- ✗ Include list of current installed packages

Summary Table:

Mode	LuCI Option	CLI Equivalent	Behavior
Upgrade + Keep Config (Full)	✓ Keep settings, ✓ Keep identical	Sysupgrade -c	Keep config; skip files identical to /rom
Upgrade + Keep Config (Default)	✓ Keep settings, ✗ Skip identical	Sysupgrade	Keep config using default backup rules
Upgrade + Reset to Default	✗ Keep settings	Sysupgrade -n	Do not keep any configuration

- Below is the example of upgrading firmware V1.9 to the router through the WinXP computer.

C:\Users\user>pscp -scp c:\deltascip\openwrt-v1.9-ramips-mt7621-wom_wr315-ec-squashfs-sysupgrade.bin root@192.168.10.2:/tmp

'=>upload file to router 192.168.10.2, username is root; (enter the password during the pop-up prompt window)

```
C:\Users\user>pscp -scp c:\deltascip\openwrt-v1.9-ramips-mt7621-wom_wr315-ec-squashfs-sysupgrade.bin root@192.168.10.2:/tmp
root@192.168.10.2's password:
openwrt-v1.9-ramips-mt7621 | 17665 kB | 2523.6 kB/s | ETA: 00:00:00 | 100%
C:\Users\user>
```

root@192.168.10.1's password: '=>type the login password
openwrt-v1.9-ramips-mt7621 | 17665 kB | 2208.1 kB/s | ETA: 00:00:00 | 100% '=>wait until 100% done

root@OpenWrt:~# ls /tmp

'=>Check whether the file is uploaded or not. Not must.

```
root@OpenWrt:~# ls /tmp
TZ
alarm-hw-cellular.state
alarm-hw-wireless.state
alarm-temperature.state
at_clteinfo.log
at_cpsi.log
at_csq.log
board.json
dhcp.leases
dnsmasq.d
etc
extroot
hosts
ipsec
lib
lock
log
modem_info.log
openwrt-v1.9-ramips-mt7621-wom_wr315-ec-squashfs-sysupgrade.bin
overlay
resolv.conf
resolv.conf.d
run
ser2net.conf
shw
state
swanctl
sysinfo
tmp
trm_runtime.json
wr-info-poll.lock
wr-wireless-mode.log
root@OpenWrt:~#
```

root@OpenWrt:~# sysupgrade /tmp/openwrt-v1.9-ramips-mt7621-wom_wr315-ec-squashfs-sysupgrade.bin

and keep configuration

'=>System upgrade and keep the configuration.

```
root@OpenWrt:~# sysupgrade /tmp/openwrt-v1.9-ramips-mt7621-wom_wr315-ec-squashfs-sysupgrade.bin and keep configuration
Wed Nov 26 09:12:01 UTC 2025 upgrade: Saving config files...
rmmod mt7915e
rmmod mt7921e
Wed Nov 26 09:12:03 UTC 2025 upgrade: Commencing upgrade. Closing all shell sessions.
Command failed: Connection failed
root@OpenWrt:~#
Connection closed by foreign host.

Disconnected from remote host(192.168.10.2:22) at 17:12:03.

Type 'help' to learn how to use Xshell prompt.
[c:\~]$
```

[c:\~]\$ ssh 192.168.10.2

'=>Reconnect the router's SSH interface

```
[c:\~]$ ssh 192.168.10.2

Connecting to 192.168.10.2:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+J'.

BusyBox v1.36.1 (2024-02-20 19:58:41 UTC) built-in shell (ash)

 _ _ _ _ _
|_| _ _ _ _ _
|_| W I R E L E S S   F R E E D O M
|_| _ _ _ _ _
-----
OpenWrt 23.05-SNAPSHOT, v1.9
-----
```

OpenWrt 23.05-SNAPSHOT, v1.9

'=>You can see the firmware version is updated.

root@OpenWrt:~# cat /etc/openwrt_release

'=>Check Firmware version

```
root@OpenWrt:~# cat /etc/openwrt_release
DISTRIB_ID='OpenWrt'
DISTRIB_RELEASE='23.05-SNAPSHOT'
DISTRIB_REVISION='r23754-60768064ce'
DISTRIB_TARGET='ramips/mt7621'
DISTRIB_ARCH='mipsel_24kc'
DISTRIB_DESCRIPTION='OpenWrt 23.05-SNAPSHOT v1.9'
DISTRIB_TAINTS='no-all busybox'
root@OpenWrt:~#
```

root@OpenWrt:~# wr-info-get.sh sys_all

'=>Check System info by WOM script

```
root@OpenWrt:~# wr-info-get.sh sys_all
{
  "version": "OpenWrt 23.05-SNAPSHOT v1.9",
  "model": "WR315GR-2C-LTE6-GAX-EC"
}
```

4.5 Configuration backup/restore

- Uer can use SCP to upload/download configuration file to/from directory /tmp

- **Backup**

command: sysupgrade -b file_name

example: backup configuration to /tmp/backup.tar.gz

```
root@OpenWrt:/# sysupgrade -b /tmp/backup.tar.gz
Tue Jun  3 05:15:01 UTC 2025 upgrade: Saving config files...
root@OpenWrt:/#
```

- **Restore**

command: sysupgrade -r file_name

Note: You need to reboot the router to activate the settings of the uploaded config file!

example: restore /tmp/backup.tar.gz and reboot

```
root@OpenWrt:/# sysupgrade -r /tmp/backup.tar.gz
Tue Jun  3 05:20:32 UTC 2025 upgrade: Restoring config files...
root@OpenWrt:/# reboot
```

4.6 Reset to Default

User can use '**jffs2reset**' to progress the reset default, this command is the same as you user "Reset" button to active reload default.

```
root@OpenWrt:~# jffs2reset
```

This will erase all settings and remove any installed packages. Are you sure? [N/y]

y

/dev/mtdblock6 is mounted as /overlay, only erasing files

```
root@OpenWrt:~# reboot
```

Compare to the Web GUI:

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Reset to defaults

Perform reset

5. REVISION HISTORY

Version	Description	Date	Editor
Draft 1	1 st draft version, modify from WR3x2GR UM, update the Hardware description of the WR315GR-2C.	2022/11/22	Orwell
Draft 2	2 nd draft version, update SW functions and web GUI.	2022/11/23	Orwell
Draft 3	Modify Antenna to Optional Antenna, update SMA mapping Remove SD features & description	2022/12/14	Orwell
Draft 4	Update web configuration function based on firmware v1.3	2022/12/16	Jerry.Lian
V1.0	Change draft 5 to V1.0 Add WR315G-LTE _x 2	2023/09/06	Jerry.Lian /Orwell
V1.1	Update LED Indication of WR315GR-LTE _x 2 Add more description of the Dual SIM dual Active mode	2024/09/07	Orwell
V1.2	Add WR315G-2C-LTE6-GAX model Add EC OS in the manual	2024/4/30	Orwell
V1.2a	Add SSH command of the OpenWrt EC OS	2024/5/5	Orwell
V1.3	For WR315G-2C-LTE6-GAX-EC model only. Add customized script to get info, wireless operation configuration and alarm configuration. Add Firmware upgrade, confirmation backup, reset to default CLI.	2025/12/01	Orwell
V1.3 draft 6	Add Declaration of conformity, Safety Precaution	2026/1/8	Orwell
V1.3b/c/d/e	Correct wording Update optional antenna's gain table	2026/7/30	Orwell
V1.3f	Add Professional Installation Precaution in page 12, next to FCC statement	2026/8/5	Orwell
V1.3g	Remove optional dipole antenna for non-EU countries, due to the antenna is not standard/default antenna in WR315GR-2C-LTE6-GAX-EC	2026/8/10	Orwell