



ER5805/AWR5805/CWR5805
Industrial 5G-NR & Wi-Fi Mesh Router

User Manual

V1.4

27th July 2023

*The user interface on these products may be slightly different from the one shown on this user manual.

This PDF Document contains internal hyperlinks for ease of navigation.
For example, click on any item listed in the [Table of Contents](#) to go to that page.

Published by:

Atop Technologies, Inc.

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City,
Hsinchu County
Taiwan, R.O.C.

Tel: +886-3-550-8137
Fax: +886-3-550-8131
sales@atop.com.tw
www.atoponline.com

Technical Support Contact Information

www.atoponline.com/request-support

Asia & Australia

Jopson Li
Tel: +886-918-694-073
eMail: jopsonli@atop.com.tw

China

Sam Xia
Tel: +86-21-649562-31
eMail: sales@atop.com.tw

Europe

Alessio Longhini
Tel: +39-348-26-28-727
eMail: alessio@atop.com.tw

Germany

Mattel Tabarelli de Fatis
Tel: +886-919-209-290
eMail: matteo.tabarelli@atop.com.tw

India & SAARC

Prashant Mishra
Tel: +91-80-492-06308
eMail: prasant.m@atop.com.tw

Indonesia

Anisah Ambarwati
Tel: +62-896-761-93026
eMail: anisah@atop.com.tw

Italy

Mattel Tabarelli de Fatis
Tel: +886-919-209-290
eMail: matteo.tabarelli@atop.com.tw

Japan

Keiichi Sagami
Tel: +090-2284-9632
eMail: sakagami@atop.com.tw

Latin America

Jopson Li
Tel: +886-918-694-073
eMail: jopsonli@atop.com.tw

Middle East & Africa

Prashant Mishra
Tel: +91-80-492-06308
eMail: prasant.m@atop.com.tw

Russia & CIS

Timur Dautov
Tel: +7-985-855-1056
eMail: timur@atop.com.tw

Taiwan

Tony Lin
Tel: +886-968-386876
eMail: tonylin@atop.com.tw

USA & Canada

Prashant Mishra
Tel: +91-80-492-06308
eMail: prasant.m@atop.com.tw

Important Announcement

The information contained in this document is the property of Atop Technologies, Inc., and is supplied for the sole purpose of operation and maintenance of Atop Technologies, Inc., products.

No part of this publication is to be used for any other purposes, and it is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form, by any means, in whole or in part, without the prior explicit written consent of Atop Technologies, Inc.,

Offenders will be held liable for damages and prosecution.

All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Disclaimer

We have checked the contents of this manual for agreement with the hardware and the software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual is reviewed regularly and any necessary corrections will be included in subsequent editions.

Suggestions for improvement are welcome. All other product names referenced herein are registered trademarks of their respective companies.

Preface

This manual contains some advanced network management knowledge, instructions, examples, guidelines, and general theories. The contents are designed to help you manage the switch and use its software, a background in general theory is a must when reading it. Please refer to the Glossary for technical terms and abbreviations.

Who Should Use This User Manual

This manual is to be used by qualified network personnel or support technicians who are familiar with network operations and might be useful for system programmers or network planners as well. This manual also provides helpful and handy information for first-time. For any related problems, please contact your local distributor. If they are unable to assist you, please redirect your inquiries to www.atoponline.com.

Documentation Control

Author:	Non-switch Team
Revision:	1.4
Revision History:	Feature/Title Update
Creation Date:	8 December 2021
Last Revision Date:	27 July 2023
Document Status:	Released

Table of Contents

1	Introduction	11
1.1	Overview	11
1.2	Software Features	12
2	Getting Started	13
2.1	Default Factory Settings	13
2.1.1	The Reset Button	13
2.2	Setting up a connection	13
2.3	Login Process and Main Window Interface	16
3	Status Menu	20
3.1	Overview	20
3.2	System	21
3.3	Network	22
3.3.1	Mobile (CWR5805 Only)	22
3.3.2	WAN	24
3.3.3	LAN	25
3.3.4	Wireless (AWR5805/CWR5805 Only)	25
3.3.5	VRRP	26
3.3.6	Access	27
3.4	Routes	28
3.4.1	ARP	28
3.4.2	Active IPv4-Routes Section	29
3.5	Logs	30
3.5.1	System Log	30
3.5.2	Kernel Log	30
4	Network Menu	32
4.1	Mobile (CWR5805 only)	32
4.1.1	General Setup	32
4.1.2	Advanced Settings Sub-Tab	37
4.1.3	SIM Switch	38
4.2	WAN	39
4.2.1	General Setup	39
4.2.2	DHCP Client	41
4.2.3	Static address	42
4.2.4	PPPoE	44
4.3	LAN	46
4.3.1	General Setup	46
4.3.2	DHCP Server	47
4.4	Wireless	49
4.4.1	Wireless Overview	49
4.4.2	Associated Stations	50
4.4.3	Device Configuration	51
4.4.4	Tutorials	53
4.5	Mesh	56
4.6	IPv6	57
4.7	VLAN	58
4.7.1	Interface Based	58
4.8	LB (Load Balancing) and Failover (CWR5805 only)	58
4.8.1	Overview	59
4.8.2	Configuration	60

4.9	Firewall.....	66
4.9.1	General Settings.....	67
4.9.2	Port Forwards.....	71
4.9.3	Traffic Rules	72
4.9.4	Attack Prevention.....	75
4.10	Static Routes.....	78
4.11	DNS	79
4.12	QoS.....	80
5	Services Menu.....	81
5.1	Auto Reboot.....	81
5.1.1	Periodic Reboot - Configuration	82
5.2	Time	82
5.2.1	General Section.....	82
5.2.2	Time Servers	83
5.3	VPN	84
5.3.1	OpenVPN	84
5.3.2	IPSec.....	91
5.3.3	L2TP.....	96
5.3.4	PPTP Server	99
5.3.5	GRE	101
5.4	VRRP	104
5.4.1	VRRP LAN configuration settings	104
5.4.2	Check Internet connection	105
5.5	GPS.....	106
5.5.1	GPS Settings	106
5.5.2	GPS Information.....	106
5.6	MQTT	108
5.6.1	MQTT Broker.....	108
5.6.2	Broker Settings.....	109
6	System.....	113
6.1	Administration	113
6.1.1	Access Control.....	114
6.1.2	Diagnostics.....	115
6.1.3	Logging.....	117
6.1.4	WEB Management	118
6.1.5	Login Accounts	119
6.2	Firmware	120
6.3	Backup	122
6.3.1	Reboot	122
7	Logout.....	123
8	Specifications	124
8.1	Hardware Specification.....	124
8.2	CWR5805 Device Pin Assignments for WAN/LAN Port.....	125
9	Glossary.....	126

List of Figures

Figure 1. An Example of Wired and Wi-Fi Devices Connected to the Internet Via CWR5805.....	11
Figure 2. Ethernet Properties Dialog Window	15
Figure 3. Internet Protocol Version 4 Properties Dialog Window	15
Figure 4. Status Dalog Window	16
Figure 5. Network Connection Details on the Connection Details	16
Figure 6. Authorization Required Webpage	18
Figure 7. Main page.....	20
Figure 8. Status > Overview	21
Figure 9. Status > System	22
Figure 10. Status > Network > Mobile	23
Figure 11. Status > Network > WAN	24
Figure 12. Status > Network > LAN	25
Figure 13 Status > Network > Wireless	26
Figure 14. Status > Network > VRRP (Master).....	27
Figure 15. Status > Network > VRRP (Backup)	27
Figure 16. Status > Network > Access	28
Figure 17. Status > Routes - ARP.....	29
Figure 18. Status > Routes – Active IPv4 Routes	29
Figure 19. Status > System > System Log	30
Figure 20. Status > System > Kernel Log	31
Figure 21. Network	32
Figure 22. Network software feature supported list	32
Figure 23. Network > Mobile > General Setup	34
Figure 24. Network > Mobile > General Setup > Data Limit Configuration > Data Connection Limit Configuration	35
Figure 25. Network > Mobile > General Setup > Data Limit Configuration > SMS Warning Configuration	36
Figure 26. Network > Mobile > General Setup > Data Limit Configuration > Clear Data Limit.....	37
Figure 27. Network > Mobile > General Setup > Data Limit Configuration > Clear Data Limit.....	37
Figure 28. Network > Mobile > Advanced Settings	37
Figure 29. Network > Mobile > SIM Switch	38
Figure 30. Network > WAN > General Setup	40
Figure 31. Network > WAN > General Setup – DHCP Client	41
Figure 32. Network > WAN > Advanced Settings – DHCP Client	41
Figure 33. Network > WAN > General Setup – Static Address	42
Figure 34. Network > WAN > Advanced Settings – Static Address	43
Figure 35. Network > WAN > General Setup – PPPoE	44
Figure 36. Network > WAN > Advanced Setting – PPPoE	45
Figure 37. Network > LAN > Common Configuration – Static Address.....	46
Figure 38. Network > LAN > DHCP Server > General Setup	47
Figure 39. Network > LAN > DHCP Server > Static Leases	48
Figure 40. Network > LAN > DHCP Server > Advanced Settings	48
Figure 41. Network > Wireless > Wireless Overview	49
Figure 42. Network > Wireless > Wireless Scan	50
Figure 43. Network > Wireless > Associated Stations	50
Figure 44. Network > Wireless > Edit Wi-Fi AP 2.4GHz	51
Figure 45. Network > Wireless > Edit Wi-Fi AP 5GHz	51
Figure 46. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > General Setup.....	52
Figure 47. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > Wireless Security.....	53
Figure 48. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > MAC-Filter.....	53
Figure 49. Wireless Overview Webpage under Wifi Menu	54
Figure 50. Network & Internet Settings on the Android System	55
Figure 51. Select ATOP_WiFi_24G AP under Network & Internet Menu	55
Figure 52. Input Password (Network Key) for WiFi Connection	56
Figure 53. Wi-Fi Connected Information	56
Figure 54. Network > Mesh > Basic Settings	57
Figure 55. Network > IPv6.....	57

Figure 56. Network > VLAN > Interface Based	58
Figure 57. Network > LB and Failover > Overview	59
Figure 58. Network > LB and Failover > Configuration > General	60
Figure 59. Network > LB and Failover > Configuration > Interfaces	60
Figure 60. Network > LB and Failover > Configuration > Interfaces > Edit	61
Figure 61. Network > LB and Failover > Configuration > Members	62
Figure 62. Network > LB and Failover > Configuration > Members > Edit	63
Figure 63. Network > LB and Failover > Configuration > Policies	64
Figure 64. Network > LB and Failover > Configuration > Policies > Edit/Add	64
Figure 65. Network > LB and Failover > Configuration > Rules	65
Figure 66. Network > LB and Failover > Configuration > Rules > Edit/Add	66
Figure 67. Network > Firewall > General Settings	67
Figure 68. Network > Firewall > General Settings > Zone Configuration	68
Figure 69. Network > Firewall > General Settings > Zone Configuration > Zone "Lan"	69
Figure 70. Network > Firewall > General Settings > Zone Configuration > Zone "Lan" > Inter-Zone Forwarding	70
Figure 71. Network > Firewall > General Settings > Zone "wan"	70
Figure 72. Network > Firewall > Port Forwards > Port Forwards Rules	71
Figure 73. Network > Firewall > Traffic Rules > Traffic Rules	73
Figure 74. Network > Firewall > Traffic Rules > Open ports on router	74
Figure 75. Network > Firewall > Traffic Rules > New forward rule	74
Figure 76. Network > Firewall > Traffic Rules > Source NAT	75
Figure 77. Network > Firewall > Attack Prevention > SYN Flood Protection	75
Figure 78. Network > Firewall > Attack Prevention > SSH Attack Protection	76
Figure 79. Network > Firewall > Attack Prevention > Http/Https Attack Protection	77
Figure 80. Network > Firewall > Attack Prevention > Port Scan	78
Figure 81. Network > Static Routes	78
Figure 82. Network > DNS	79
Figure 83. Network > QoS	80
Figure 84. Network > QoS > QoS-LAN Settings	80
Figure 85. Service	81
Figure 86. Service > Auto Reboot	81
Figure 87. Service > Auto Reboot > Edit	82
Figure 88. Services > Time > General	83
Figure 89. Services > NTP > Time Servers	83
Figure 90. Services > VPN > OpenVPN > Overview	84
Figure 91. Services > VPN > OpenVPN > sample_server > Edit	85
Figure 92. Services > VPN > OpenVPN > sample_client > Edit	88
Figure 93. Services > VPN > IPsec > Settings	91
Figure 94. Services > VPN > IPsec > Status	96
Figure 95. Services > VPN > L2TP > Overview	96
Figure 96. Services > VPN > L2TP > Xl2tpsvr > Edit	97
Figure 97. Services > VPN > L2TP > Overview	98
Figure 98. Services > VPN > L2TP > Xl2tpClient > Edit	98
Figure 99. Services > VPN > PPTP Server > General Settings	99
Figure 100. Services > VPN > PPTP Server > Users Manager	100
Figure 101. Services > VPN > PPTP Server > Online Users	100
Figure 102. Services > VPN > GRE > Overview	101
Figure 103. Services > VPN > GRE > GRE Instance: Tun1/2	102
Figure 104. Services > VRRP > VRRP LAN Configuration Settings	104
Figure 105. Services > VRRP > Check Internet Connection	105
Figure 106. Services > GPS > Settings	106
Figure 107. Services > GPS > Information	106
Figure 108. Services > MQTT > Broker	108
Figure 109. Services > MQTT > Security	109
Figure 110. Services > MQTT > Bridge	110
Figure 111. Services > MQTT > Miscellaneous	111
Figure 112. System	113

Figure 113. System > Administration > General Settings	113
Figure 114. System > Administration > Access Control > Telnet Access.....	114
Figure 115. System > Administration > Access Control > SSH Access	115
Figure 116. System > Administration > Diagnostics	115
Figure 117. System > Administration > Diagnostics > Ping.....	116
Figure 118. System > Administration > Diagnostics > Traceroute	116
Figure 119. System > Administration > Diagnostics > Nslookup	117
Figure 120. System > Administration > Logging	117
Figure 121. System > Administration > WEB Management	118
Figure 122. System > Administration > Login Accounts.....	119
Figure 123. System > Firmware.....	121
Figure 124. Confirm message of the Firmware Upgrade.....	121
Figure 125. System > Backup	122
Figure 126. System > Reboot.....	122
Figure 127. System > Logout.....	123
Figure 128. WAN/LAN Port on RJ45 with Pin Numbering of CWR5805 Device	125

List of Tables

Table 1. Network Interfaces Default Settings.....	13
Table 2. Login Default Settings	13
Table 3. Status > Overview	21
Table 4. Status > System	22
Table 5. Status > Network > Mobile	24
Table 6. Status > Network > WAN	25
Table 7. Status > Network > LAN	25
Table 8 Status > Network > Wireless	26
Table 9. Status > Network > VRRP	27
Table 10. Status > Network > Access	28
Table 11. Status > Routes - ARP.....	29
Table 12. Status > Routes – Active IPv4 Routes	29
Table 13. Status > System > System Log	30
Table 14. Status > System > Kernel Log	31
Table 15. Network > Mobile > General Setup	35
Table 16. Network > Mobile > General Setup > Data Limit Configuration > Data Connection Limit Configuration .	36
Table 17. Network > Mobile > General Setup > Data Limit Configuration > SMS Warning Configuration	36
Table 18. Network > Mobile > Advanced Settings	37
Table 19. Network > Mobile > SIM Switch	38
Table 20. Network > WAN > General Setup – DHCP Client	41
Table 21. Network > WAN > Advanced Settings – DHCP Client	41
Table 22. Network > WAN > General Setup – Static Address	42
Table 23. Network > WAN > Advanced Settings – Static Address	43
Table 24. Network > WAN > General Setup – PPPoE	44
Table 25. Network > WAN > Advanced Setting – PPPoE.....	45
Table 26. Network > LAN > Common Configuration – Static Address.....	46
Table 27. Network > LAN > DHCP Server > General Setup	47
Table 28. Network > LAN > DHCP Server > Static Leases	48
Table 29. Network > LAN > DHCP Server > Advanced Settings	48
Table 30. Network > Wireless > Wireless Overview	49
Table 31. Network > Wireless > Wireless Scan	50
Table 32. Network > Wireless > Associated Stations	50
Table 33. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz	52
Table 34. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > General Setup	52
Table 35. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > General Setup	53
Table 36. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > MAC-Filter	53
Table 37. Network > Mesh > Basic Settings	57
Table 38. Network > IPv6.....	58
Table 39. Network > VLAN > Interface Based	58
Table 40. Network > LB and Failover > Overview	60
Table 41. Network > LB and Failover > Configuration > General.....	60
Table 42. Network > LB and Failover > Configuration > Interfaces	61
Table 43. Network > LB and Failover > Configuration > Interfaces > Edit.....	62
Table 44. Network > LB and Failover > Configuration > Members	62
Table 45. Network > LB and Failover > Configuration > Members > Edit	63
Table 46. Network > LB and Failover > Configuration > Policies.....	64
Table 47. Network > LB and Failover > Configuration > Policies > Edit/Add	64
Table 48. Network > LB and Failover > Configuration > Rules	65
Table 49. Network > LB and Failover > Configuration > Rules > Edit/Add	66
Table 50. Network > Firewall > General Settings.....	67
Table 51. Network > Firewall > General Settings > Zone Configuration	68
Table 52. Network > Firewall > General Settings > Zone Configuration > Zone “Lan”	69
Table 53. Network > Firewall > General Settings > Zone “wan” > Inter-Zone Forwarding.....	71
Table 54. Network > Firewall > Port Forwards > Port Forwards Rules.....	71
Table 55. Network > Firewall > Port Forwards > New Port Forwards Rules	72

Table 56. Network > Firewall > Traffic Rules > Traffic Rules	74
Table 57. Network > Firewall > Traffic Rules > Open ports on router	74
Table 58. Network > Firewall > Traffic Rules > New forward rule	74
Table 59. Network > Firewall > Traffic Rules > Source NAT	75
Table 60. Network > Firewall > Attack Prevention > SYN Flood Protection	76
Table 61. Network > Firewall > Attack Prevention > SSH Attack Protection	76
Table 62. Network > Firewall > Attack Prevention > Http/Https Attack Protection	77
Table 63. Network > Firewall > Attack Prevention > Port Scan	78
Table 64. Network > Static Routes	79
Table 65. Network > DNS	79
Table 66. Network > QoS > QoS-LAN Settings	80
Table 67. Service > Auto Reboot > Edit	82
Table 68. Services > NTP > General	83
Table 69. Services > NTP > Time Servers	84
Table 70. Services > VPN > OpenVPN > Overview	84
Table 71. Services > VPN > OpenVPN > sample_server > Edit	85
Table 72. Services > VPN > OpenVPN > sample_client > Edit	88
Table 73 Services > VPN > IPSec > Settings	93
Table 74 Services > VPN > IPSec > Status	96
Table 75. Services > VPN > L2TP > Xl2tpsvr > Edit	97
Table 76. Services > VPN > L2TP > Xl2tpClient > Edit	98
Table 77. Services > VPN > PPTP Server > General Settings	99
Table 78. Services > VPN > PPTP Server > Users Manager	100
Table 79. Services > VPN > PPTP Server > Online Users	100
Table 80. Services > VPN > GRE > Overview	101
Table 81 Services > VPN > GRE > GRE Instance: Tun1/2	102
Table 82. Services > VRRP > VRRP LAN Configuration Settings	104
Table 83. Services > VRRP > Check Internet Connection	105
Table 84. Services > GPS > Settings	106
Table 85. Services > GPS	106
Table 86. Services > MQTT > Broker	108
Table 87. Services > MQTT > Security	109
Table 88. Services > MQTT > Bridge	111
Table 89. Services > MQTT > Miscellaneous	112
Table 90. System > Administration > General Settings	114
Table 91. System > Administration > Access Control > Telnet Access	114
Table 92. System > Administration > Access Control > SSH Access	115
Table 93. System > Administration > Logging	118
Table 94. System > Administration > WEB Management	119
Table 95. System > Administration > General Settings	119
Table 96. Hardware Specification	124
Table 97. Assignment for RJ-45 Connector of CWR5805 Device	125

1 Introduction

1.1 Overview

Atop's AWR (Access Point **W**ireless **R**outer), CWR (**C**ellular **W**ireless **R**outer) and ER (**E**thernet **R**outer) 5805 series are the product line of powerful industrial router.

5805 series have built-in full-duplex 10/100/1000 Mbps ports (WAN, LANs) to connect with users' wired Ethernet devices for the speed up to 1 Gbps.

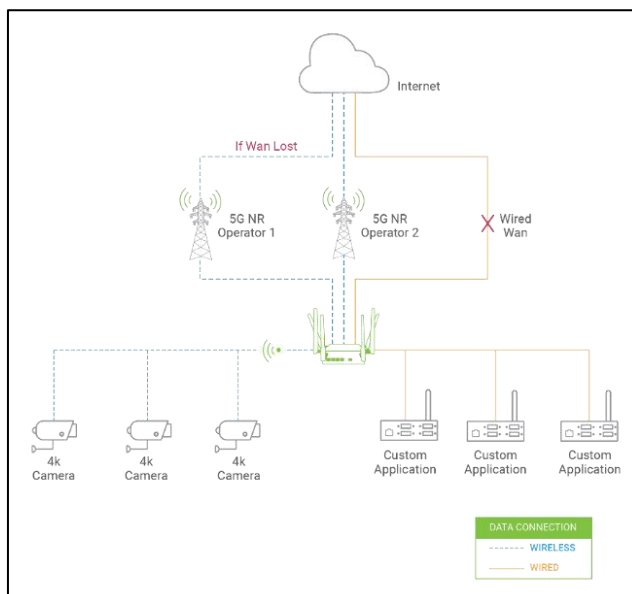
The AWR5805 and CWR5805 radiate signal in the dual-band (2.4GHz, 5GHz), while users' Wi-Fi devices can conveniently connect to them via any chosen band.

The CWR5805 support 5G NR and LTE network for the device through a wireless connection, it be a 5G CPE (Customer Premises Equipment), also known as 5G FWA . It has dual-SIM card backup to ensure a stable wireless network connection. The Ethernet WAN and mobile module on the CWR5805 device provide a load balancing/failover mechanism for Internet connection. The router function combines traffic for all connected devices and let them share a high-speed cable or ADSL Internet connection.

Nowadays, some IoT infrastructure are require multiple connection interface which can be connected via wired (Ethernet) or wireless interfaces (Wi-Fi and/or Cellular 5G/LTE). For instance, the sensor is an inseparable part of efficient IoT plant and monitor its environment status. Such SCADA (Supervisory Control and Data Acquisition) system need an active Internet connection via Wi-Fi/LAN to reach the IoT plant.

Connectivity downtime can be easily resolved by adding a cellular 5G/LTE router between existing wired WAN. This way, it is possible to use the wired Internet option and share the connection to the IoT system via Ethernet and to a 4K monitor via Wi-Fi using a single compact Cellular Router CWR5805. Once it senses that wired WAN is lost or disrupted, it automatically switches to 5G/LTE as a source of the Internet to provide continuous Internet service to connected devices.

Figure 1. An Example of Wired and Wi-Fi Devices Connected to the Internet Via CWR5805.



*Note: Through the manual, the symbol * indicates that more detailed information of the subject will be provided at the end of this book or as a footnote.*

1.2 Software Features

AWR5805, CWR5805, ER5805 Platform

- 1 x RJ45 for 10/100/1000Mbps BaseT WAN
- 4 x RJ45 for 10/100/1000Mbps BaseT LAN
- Integrated DHCP server with dynamic and static IP address assignment
- Natural firewall using NAT technology
- Firewall and VPN for security connection
- Industrial EMC protection, -40°C~75°C wide-range temperature operation
- Rugged metal case with a wall or DIN-Rail mount
- PoE PD support for flexible deployment
- Time sync with NTP server and Browser
- Power supply input supporting 12~48VDC

Additional Feature build in AWR5805 and CWR5805 Platform Only

- Wi-Fi 5
 - 802.11ac (5GHz)
 - 802.11a/b/g/n(2.4GHz/5GHz)
 - MU-MIMO 2x2
 - Wi-Fi Mesh

Additional Feature build in CWR5805 Platform Only

- Cellular
 - 5G-NR and 4G-LTE networks
 - Support 5G Non-standalone (NSA) and standalone mode (SA)
 - Data limitation control
- SIM Card
 - Dual nano-SIM card (4FF) with single standby
- Backup WAN interfaces for connection reliability
- GPS option for location service
- Time sync with GPS
- 1x micro-SD slot for flexible use

2 Getting Started

This chapter explains how to access the AWR5805/CWR5805/ER5805 for the first time. Hereinafter called xxR5805.

Users can access the managed switch easily using their web browsers (Internet Explorer 8 or 11, Firefox 44, Chrome 48 or later versions are recommended). We will proceed to use a web browser to introduce the managed switch's functions.

2.1 Default Factory Settings

Below is the list of default factory settings. This information will be used during the login process. Make sure that the computer accessing the xxR5805 has an IP address in the same subnet and the subnet mask is the same.

xxR5805 default network parameters are listed in the table below.

Table 1. Network Interfaces Default Settings

Interface	Device IP	Subnet Mask	Gateway IP	DNS
WAN	DHCP Client			
LAN/WiFi	192.168.1.1	255.255.255.0	None	None
5G NR/LTE	QMI Cellular			

Its WebGUI login default Username and password are listed in the table below. Please pay attention that username and password are case sensitive.

Table 2. Login Default Settings

Login Parameter	Default Values
Username	admin
Password	default

2.1.1 The Reset Button

If you forget the password or cannot access the Web Configurator of the device, you can use the RESET button to restore the factory default configuration file. This means you will lose all of your configurations after the resetting. The password will also be reset to the factory default setting (see the device label), and the LAN IP address will be "192.168.1.1". To reset the device, follow these steps:

1. Make sure the POWER LED is on (not blinking).
2. Press the "Reset" button on the panel from the same side of the terminal block for **5** seconds to restore the factory default settings. When the Wi-Fi and Ethernet LED begin to blink, the device is starting to restore its factory default setting.

2.2 Setting up a connection

There are essential communication devices and items which are needed to be prepared before setting up a testing environment. A personal computer (PC) or a laptop computer is used for testing network connection to LAN interfaces of xxR5805. A network cable such as unshield twisted pair (UTP) with RJ45 connectors is also required for the Ethernet LAN interface. A 5G/LTE Nano-SIM card is used to insert into the Nano-SIM card slot of the xxR5805 for testing the mobile interface connection.

A cable modem or an ADSL modem can be one of the external Internet connection sources for testing the WAN interface connection of xxR5805. A mobile phone or a tablet can be used for testing network connection to wireless AP interface of the device.

Follow the steps outlined below to setting up network connections for xxR5805 device.

LAN Connection

The first step is to configure a LAN connection between a PC and the xxR5805 device. Plug in one end of a network cable to one of the LAN port sockets of xxR5805 and the other end of the network cable to the PC's Ethernet port socket.

In the xxR5805 device, the IPv4 DHCP server is enabled by default for the LAN interfaces. Any device with IPv4 DHCP client enabled in its Ethernet interface will be assigned a dynamic IP address from xxR5805 device. The default IP address of CWR5805 is **192.168.1.1**, and the dynamic IP address range of LAN port is start from **192.168.1.100** to **192.168.1.250**.

WAN Connection

The second step is to configure a WAN connection between the xxR5805 device and a Cable/ADSL modem. The default mode of DHCP protocol of WAN interface on the xxR5805 is set to DHCP client. On the Cable/ADSL modem, make sure that there is an IPv4 DHCP server enabled for its Ethernet port interface which will be used to assign an IP address to the WAN interface of xxR5805 device. Plug in one end of a network cable to the WAN interface of xxR5805 device and the other end of the network cable to an Ethernet port interface of a Cable/ADSL modem.

Mobile Port Connection (CWR5805 only)

The third step is to setup the 5G/LTE network for the mobile Internet connection. The SIM slots of CWR5805 only support Nano-SIM cards. Insert a 5G/LTE Nano-SIM card into the primary Nano-SIM slot of the device.

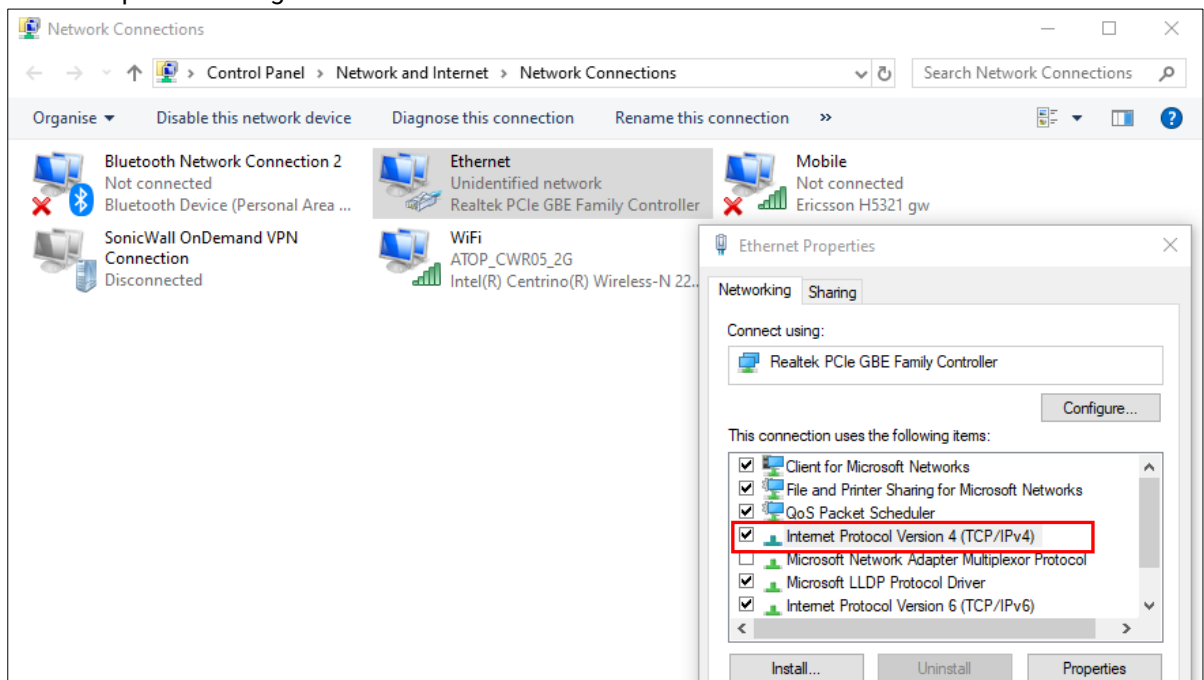
Power on xxR5805 Device

Before powering on the xxR5805 device, make sure that all of the 2.4GHz, 5GHz, and 5G/LTE SMA antennas are connected to the CWR5805 device firmly and correctly. Plug in the power line to CWR5805 device and turn on the power. The system takes approximately 50 seconds to boot into a stable state.

Setting up a DHCP IP address on a Windows 10 PC

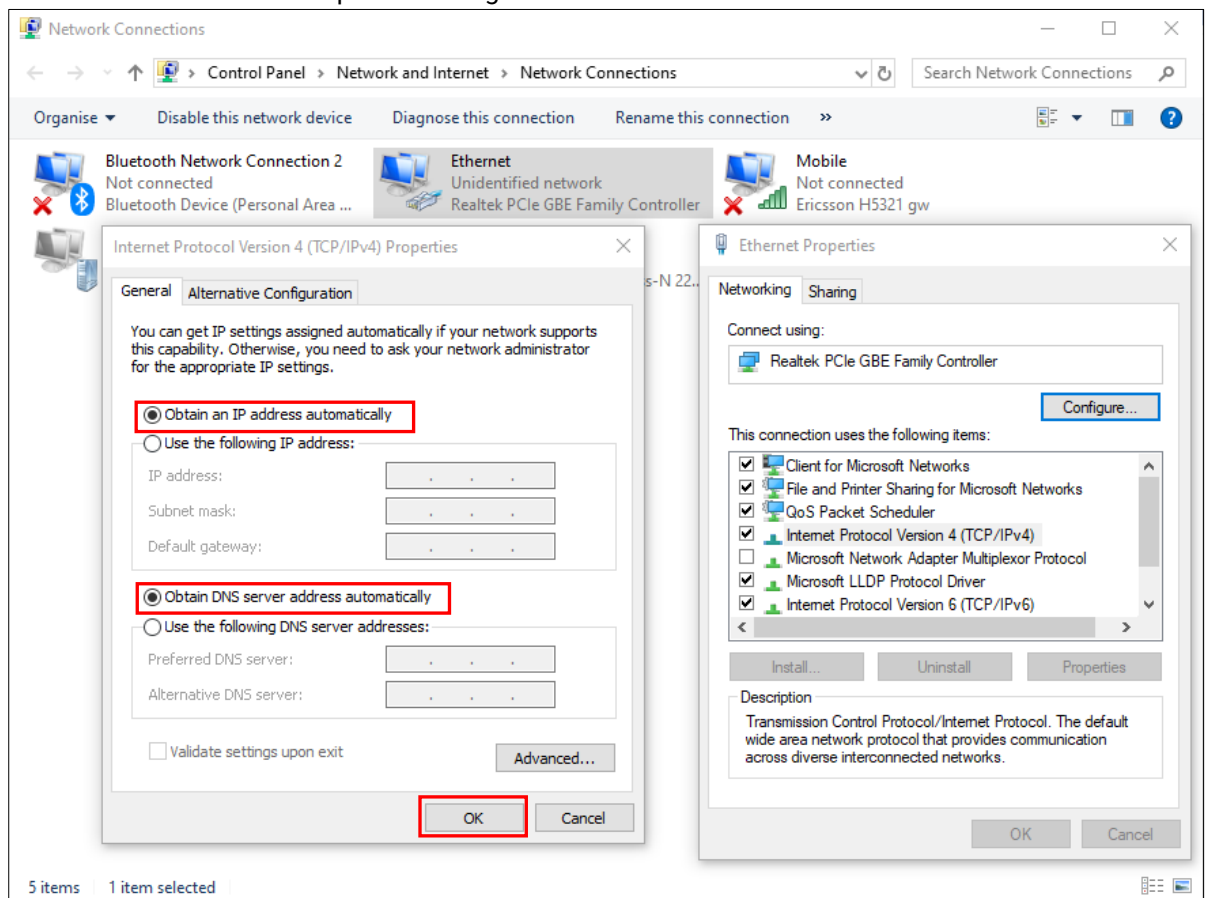
On the PC, open the Network Connections window. Then, select the physical network interface icon and right click to open properties and enter the Ethernet Properties dialog window. As shown in the Figure below, check the **Internet Protocol Version 4 (TCP/IPv4)** item and push the properties button to enter the Internet Protocol Version 4 Properties dialog window.

Figure 2. Ethernet Properties Dialog Window



Then, as shown in the Figure below, select the **Obtain an IP address automatically** item and the **Obtain DNS server address automatically** item on General tab of the Internet Protocol Version 4 (TCP/IPv4) Properties dialog window. Click the OK button to obtain a dynamic IP address from xxR5805 device.

Figure 3. Internet Protocol Version 4 Properties Dialog Window



Next, select the physical network interface icon again, then double-click mouse to enter the Ethernet Status dialog window as shown in the Figure below.

Push the **Details** button to view the assigned IPv4 address and others info. In Network Connection Details dialog window, the IPv4 address of IPv4 Default Gateway, IPv4 DHCP Server, and IPv4 DNS Sever are the same **192.168.1.1** address which is an IPv4 address of the LAN port interface on xxR5805 device.

In this example, the assigned IPv4 address of the PC is 192.168.1.227 which is within the dynamic IP address range of 192.168.1.100 to 192.168.1.250.

Figure 4. Status Dialog Window

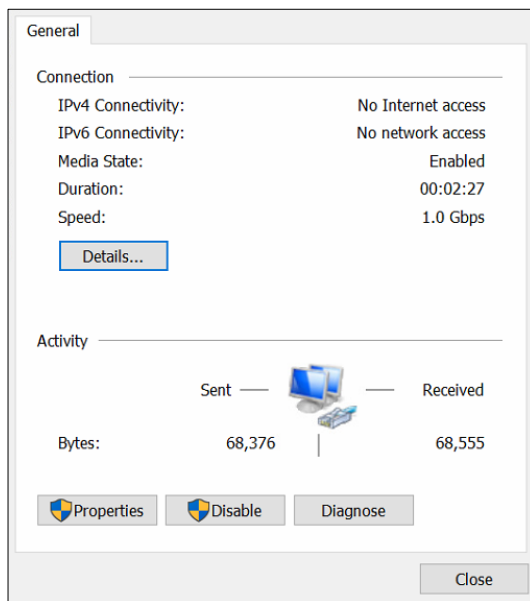


Figure 5. Network Connection Details on the Connection Details

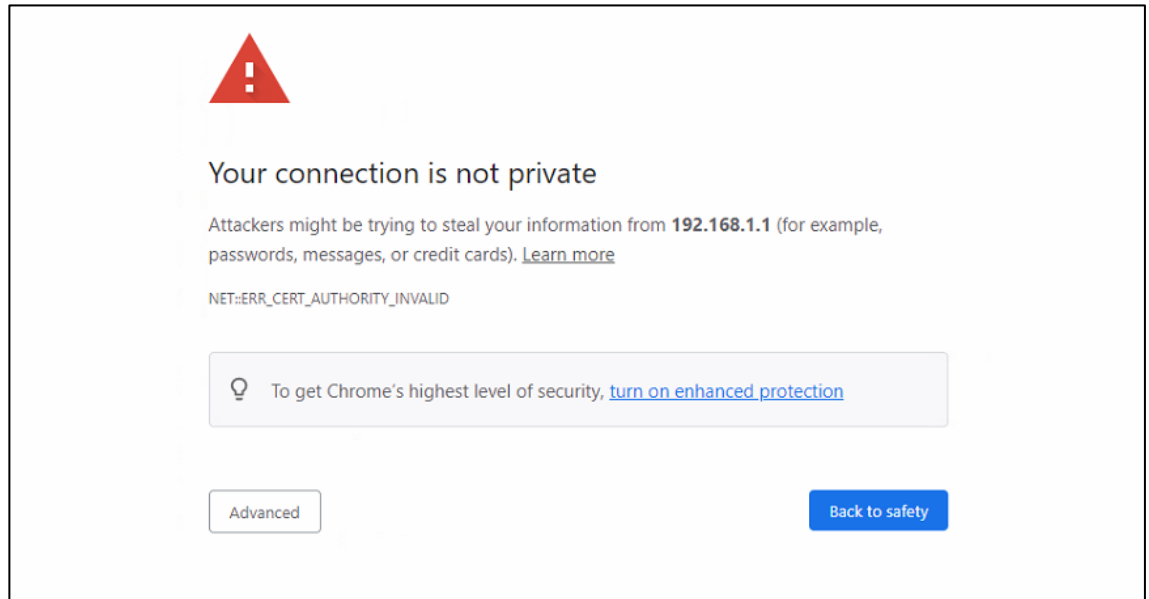
2.3 Login Process and Main Window Interface

Before scan access the configuration, you have to log in. This can simply be done in the following steps.

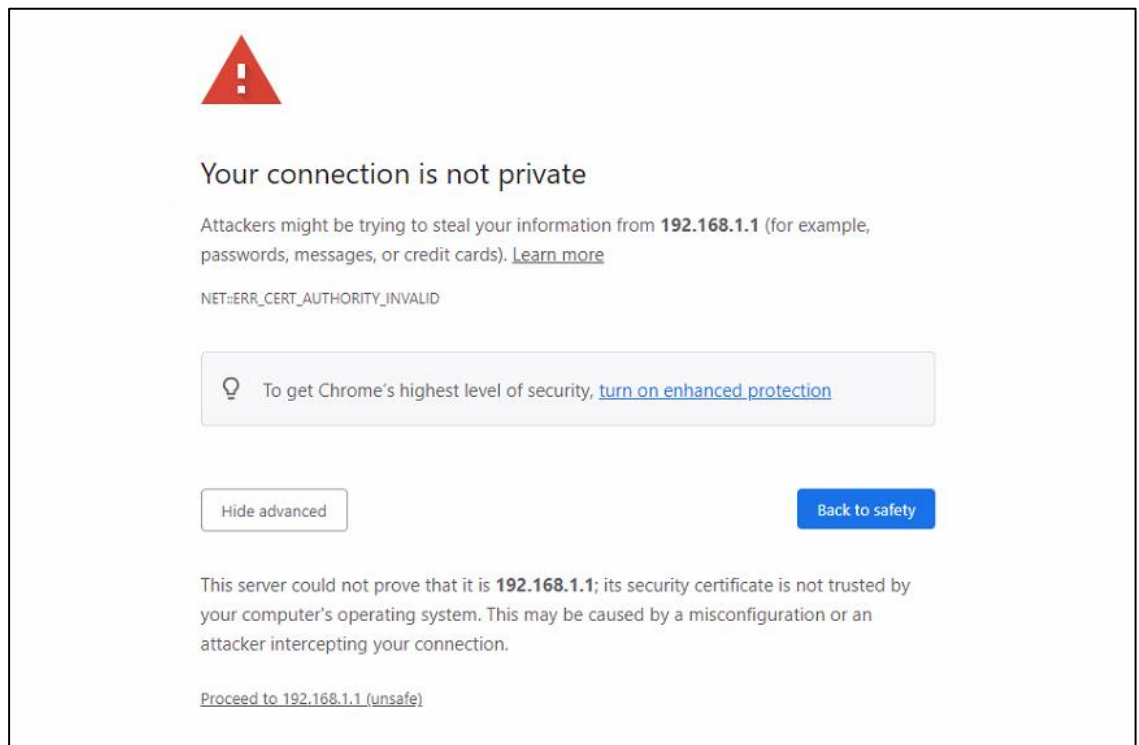
A login authorization is required before a you can access to WebUI of the xxR5805 device. The default URL to access the device's WebUI is <https://192.168.1.1>. It will be redirected to the login authorization webpage after pressing the enter key.

As shown in the Figure below, you need to enter the correct Username and Password to access the device's WebUI. The default value for the Username is **admin** and for the Password is the **default**.

1. Launch a web browser.
2. Type in the xxR5805 IP address, e.g. <https://192.168.1.1>.
3. If it is the first time that the users access the managed switch, the web the browser such as Google Chrome may detect that the switch does not have a valid certificate authority. The users can proceed by clicking on the Advanced button as shown in below figure.

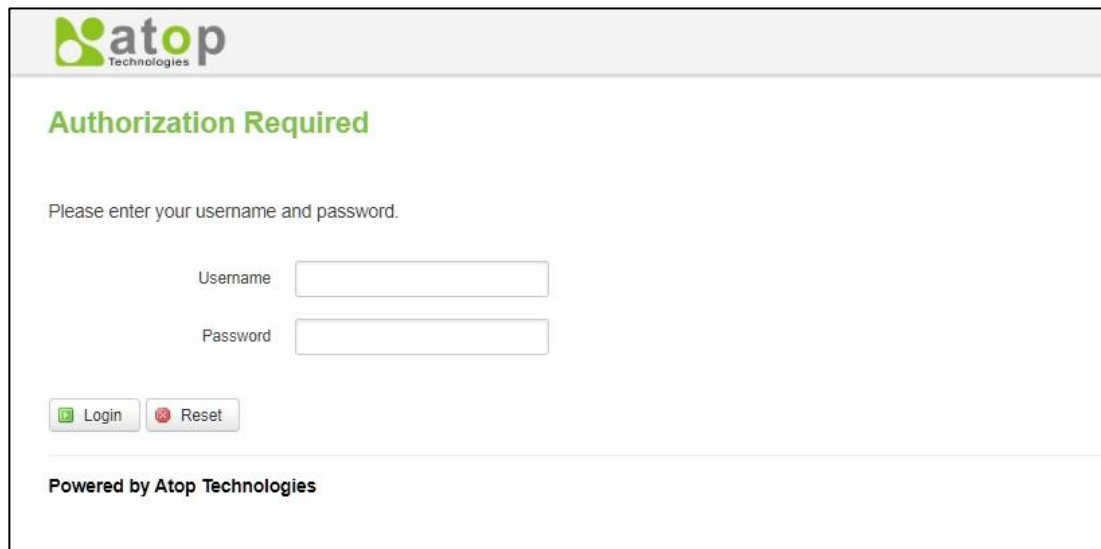


4. Once the Advanced button is clicked, an explanation text will appear below the button as shown in below Figure. Here at the bottom of the web page, there is a hyperlink that the users can click to access the web GUI.



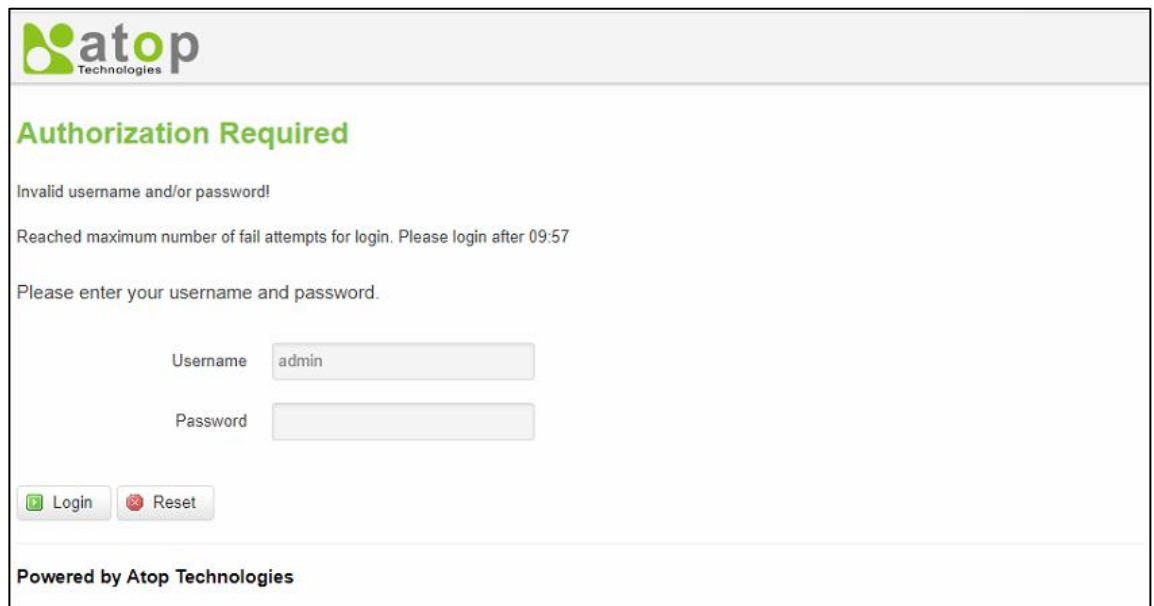
5. After proceeding through the invalid certificate warning and clicking on the **Proceed to 192.168.1.1 (unsafe)** hyperlink, a login page will be presented shown in below Figure. The user can enter a **Username** and a **Password** to access the managed switch. Then, clicking on the **Login** button.

Figure 6. Authorization Required Webpage



The screenshot shows the Atop Technologies logo at the top left. Below it, the heading "Authorization Required" is displayed in green. A message "Please enter your username and password." is followed by two input fields: "Username" and "Password". Below the input fields are two buttons: "Login" (with a green checkmark icon) and "Reset" (with a red X icon). At the bottom, it says "Powered by Atop Technologies".

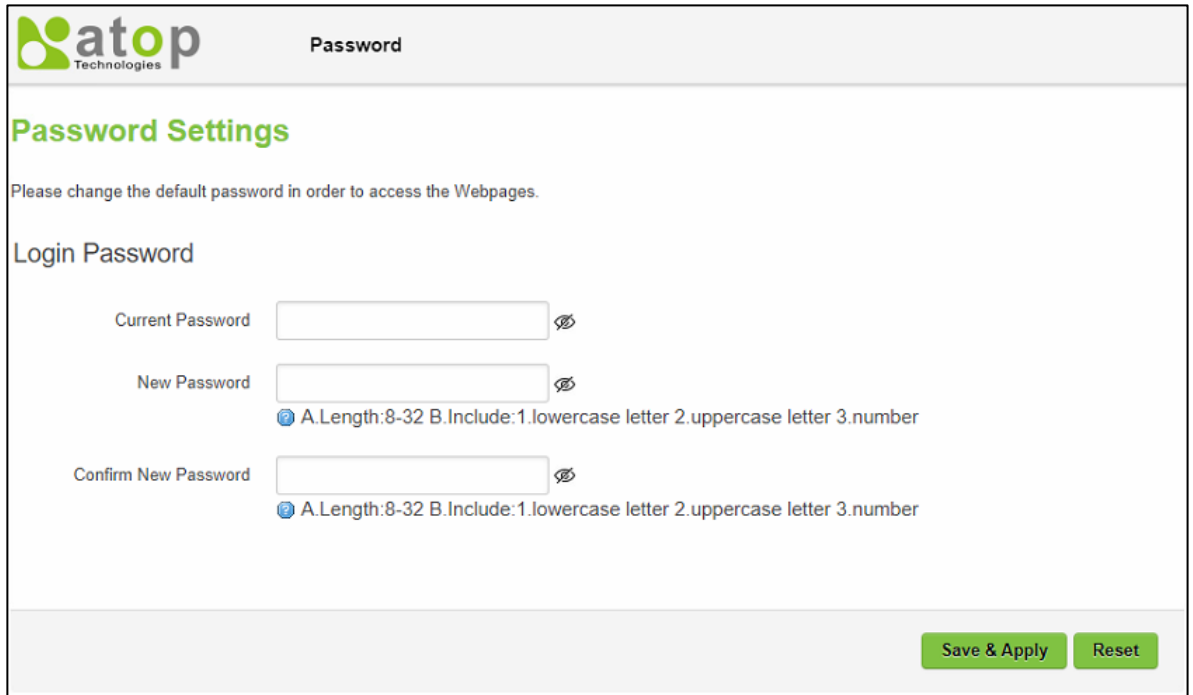
6. If the user entered wrong passwords more than three times within 3 times, the account will be temporary blocked for 10 minutes. An error pop-up notification will be shown as in below Figure. The user can click **Try again** button to access the login page again after the duration of 15 minutes.



The screenshot shows the Atop Technologies logo at the top left. Below it, the heading "Authorization Required" is displayed in green. An error message "Invalid username and/or password!" is shown, followed by "Reached maximum number of fail attempts for login. Please login after 09:57". Below this, the message "Please enter your username and password." is followed by two input fields: "Username" (containing "admin") and "Password". Below the input fields are two buttons: "Login" (with a green checkmark icon) and "Reset" (with a red X icon). At the bottom, it says "Powered by Atop Technologies".

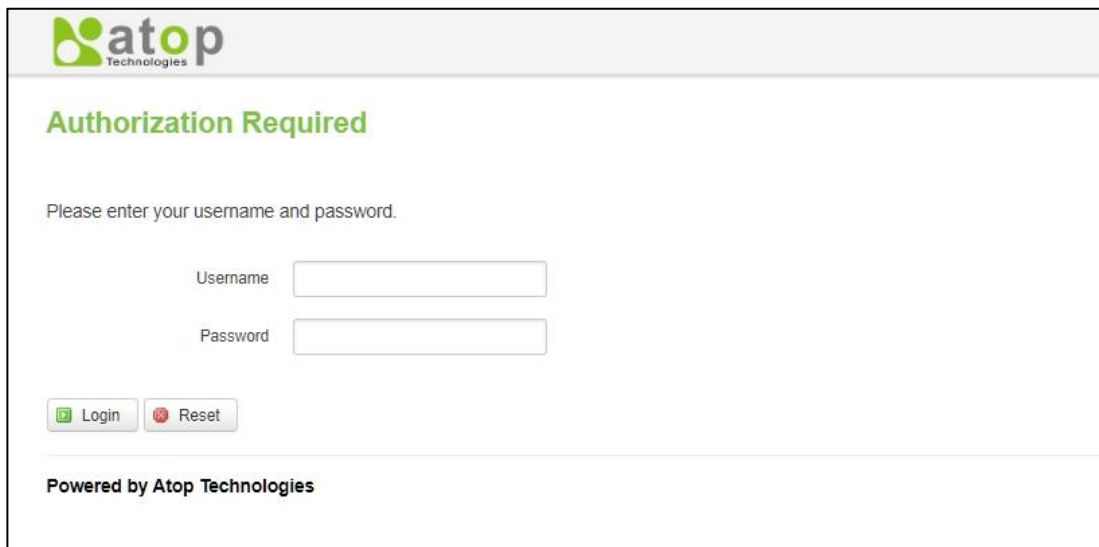
7. For security, you are immediately prompted to change the factory default password for the "admin" account.

Note: The password is case-sensitive.



The screenshot shows the 'Password Settings' page of the Atop Technologies interface. The page has a header with the Atop Technologies logo and the title 'Password'. Below the header, the section is titled 'Password Settings' in green. A message states: 'Please change the default password in order to access the Webpages.' The main content area is titled 'Login Password' and contains three password input fields: 'Current Password', 'New Password', and 'Confirm New Password'. Each field has a toggle icon to its right. Below the 'New Password' and 'Confirm New Password' fields, there is a password strength indicator: 'A.Length:8-32 B.Include:1.lowercase letter 2.uppercase letter 3.number'. At the bottom right of the form, there are two green buttons: 'Save & Apply' and 'Reset'.

8. Input Username: admin with new password.



The screenshot shows the 'Authorization Required' page of the Atop Technologies interface. The page has a header with the Atop Technologies logo. Below the header, the section is titled 'Authorization Required' in green. A message states: 'Please enter your username and password.' The main content area contains two input fields: 'Username' and 'Password'. Below these fields, there are two buttons: 'Login' (with a green icon) and 'Reset' (with a red icon). At the bottom of the page, it says 'Powered by Atop Technologies'.

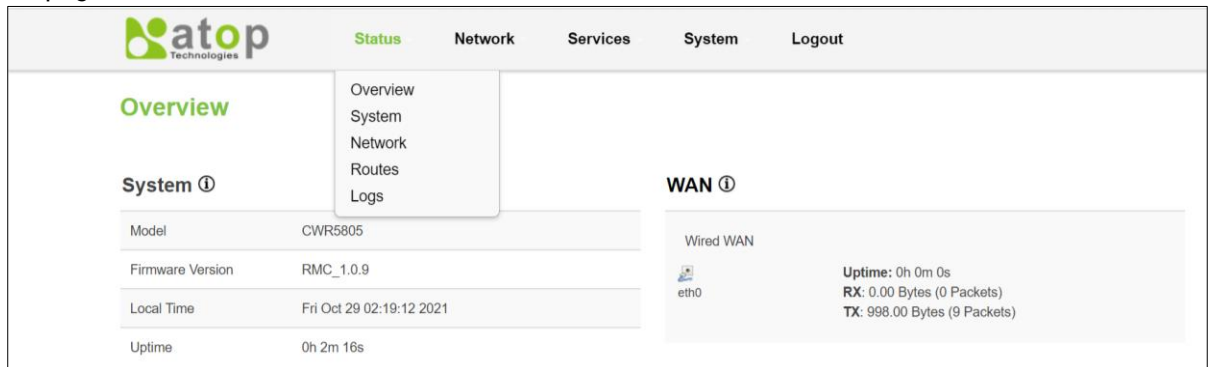
Note:

1. Any unauthorized login to the 5805 will be recorded to device's syslog.
2. After the user logs in to the main interface if the user is idle or inactive for more than 5 minutes, the user will be logged out automatically.

3 Status Menu

As shown in the Figure below, the Status menu contains the following sub-menus: Overview, System, Network, Routes and Logs. These sub-menus display the current network information, as well as real-time traffic statistics of each network interface.

Figure 7. Main page



3.1 Overview

The **Overview** sub-menu under the Status menu contains a summary of the device's information, i.e., System, Memory, Mobile, WAN, Wireless, and LAN interface live status.

This screen is the first thing you see when you log into the CWR5805. It also appears every time you click the **Status** icon in the navigation panel. The **Status** screen displays the CWR5805's connection information, wireless, mobile information, and traffic statistics.

Figure 8. Status > Overview

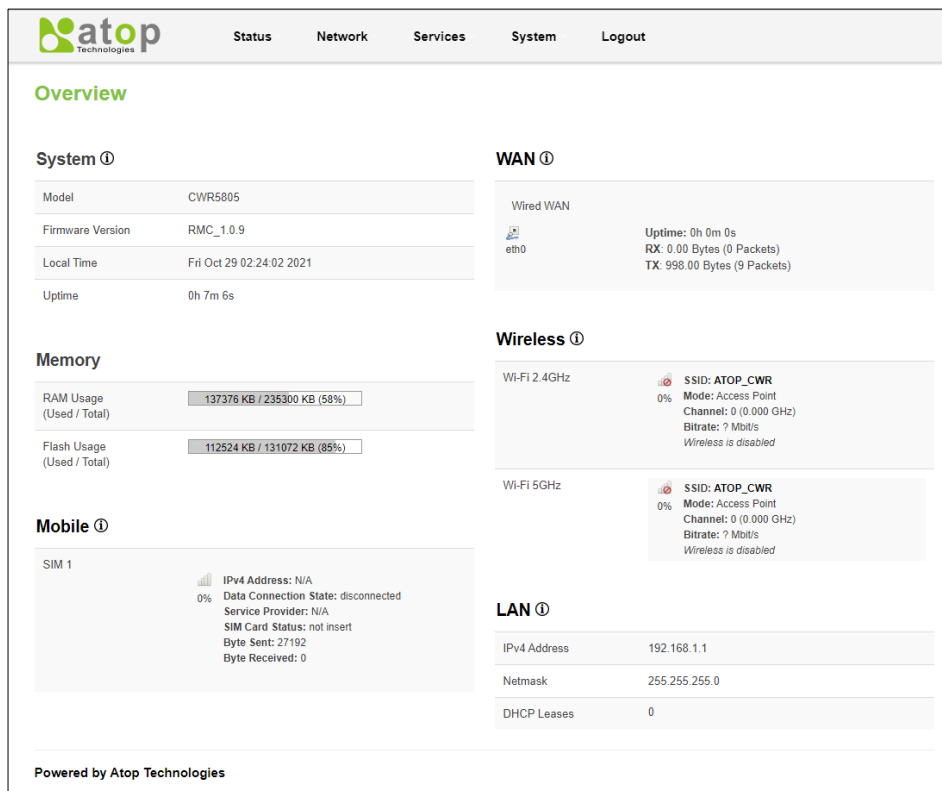


Table 3. Status > Overview

Field	Description
System	
Model	The model name of the device.
Firmware Version	The currently used firmware version on the device.
Local Time	Date and time information with timezone offset. The timezone offset can be selected on the Timezone field of the System webpage.
Uptime	Uptime measures the length of time a system has been running since it was booted.
Memory	
RAM Usage	Amount of random-access memory (RAM) that is currently in use by the device.
Flash Usage	Amount of Flash (storage) memory that is currently in use by the device.
Mobile	
SIM 1/2	The current Primary SIM card state.
WAN	
Wired WAN	The current WAN state.
Wireless	
Wi-Fi 2.4GHz	The current Wi-Fi 2.4GHz state.
Wi-Fi 5GHz	The current Wi-Fi 5GHz state.
LAN	
IPv4 Address	IPv4 address of the LAN interface.
Netmask	Netmask of the LAN interface.
DHCP Lease	The number of DHCP Clients connected.

3.2 System

This section shows the system status information of your router.

Figure 9. Status > System

atopTechnologies

Status

Network

Services

System

Logout

System Information

System

Hostname	AtopTechnologies
Model	CWR5805
Firmware version	RMC_1.0.9
Kernel version	4.4.60
Local time	Fri Oct 29 06:33:46 2021
Uptime	4h 16m 50s
Load average (1min, 5min, 15min)	0.30, 0.41, 0.42

Powered by Atop Technologies

Table 4. Status > System

Field	Description
Hostname	This value can be modified on the Hostname field of the System webpage.
Model	The model name of the device.
Firmware Version	The currently used firmware version on the device
Kernel Version	The currently used kernel version of the device
Local Time	Date and time information with timezone offset. The timezone offset can be selected on the Timezone field of the System webpage.
Uptime	Uptime measures the length of time a system has been running since it was booted.
Load Average	It is the average system load calculated over a given period time of 1, 5 and 15 minutes.

3.3 Network


3.3.1 Mobile (CWR5805 Only)

This chapter is available in CWR5805 model.

This section shows the Internet status information of the router. The status of the mobile interface. It contains information on the primary SIM card number, the data connection state, the service provider, the network type, the signal strength, the number of bytes sent, the number of bytes received, IMEI, IMSI, and ICCID.


Click **Connect** to connect to a 5G/LTE network, and click **Stop** to disconnect from a network.

Figure 10. Status > Network > Mobile


Status
Network
Services
System
Logout

Mobile
WAN
LAN
Wireless
VRRP
Access

Mobile Information

Mobile 

Data connection state	connected
IPv4 address	10.183.222.157
Netmask	255.255.255.252
MAC address	96:60:8D:88:3F:35
IMEI	359047100139367
IMSI	466924133586118
ICCID	89886920041335861180
SIM card state	inserted
Signal strength	-51
Service provider	Chunghwa Telecom
LTE band	8
LTE RSRP	-53
LTE RSRQ	-4
LTE SINR	17
NSA band	N/A
NSA RSRP	N/A
NSA RSRQ	N/A
NSA SINR	N/A
Bytes received *	39294
Bytes sent *	273336

Connect
Stop
Refresh

*Your carrier's data usage accounting may differ. Atop is not liable should any accounting discrepancies occur.

Table 5. Status > Network > Mobile

Field	Description
Data connection state	The Mobile data connection status.
IPv4 address	The IP address that the router uses to connect to the internet.
Netmask	Specifies a mask used to define how large the WAN network is.
Mac address	MAC (Media Access Control) address of the mobile module.
IMEI	IMEI (International Mobile Equipment Identity) number of the mobile module.
IMSI	IMSI (International Mobile Subscriber Identity) number of the current SIM.
ICCID	ICCID number of the current SIM.
SIM card state	SIM card's state, e.g. PIN required, Not inserted, etc.
Signal strength	The signal strength. Signal's strength measured in dBm.
Service provider	The name of ISP Network Provider.
LTE band	The band of the current network.
LTE RSRP	The signal of LTE Reference Signal Received Power.
LTE RSRQ	The signal of current LTE Reference Signal Received Quality.
LTE SINR	The Signal to Interference plus Noise Ratio.
NSA band	The current NSA frequency bands.
NSA RSRP	The signal of 5G NR Reference Signal Received Power.
NSA RSRQ	The signal of current LTE Reference Signal Received Quality.
NSA SINR	The Signal to Interference plus Noise Ratio.
Bytes received	The number of bytes were received via the mobile data connection.
Bytes sent	The number of bytes were sent via the mobile data connection.

3.3.2 WAN

This section shows the WAN status information of the router.

Figure 11. Status > Network > WAN

The screenshot displays the ATop Technologies web interface. At the top, there is a navigation bar with the logo and tabs for Status, Network, Services, System, and Logout. Below this, a sub-navigation bar shows tabs for Mobile, WAN (which is highlighted), LAN, Wireless, VRRP, and Access. The main content area is titled 'WAN Information' and contains a section for 'WAN' with a table of configuration details:

Interface	Wired
Type	dhcp
IPv4 address	N/A
MAC address	7A:99:E2:7F:F0:18
Netmask	N/A
Gateway	N/A
DNS	N/A
Connected	3h 54m 35s

Below the table, there is a section for 'WAN Load Balancing Status' showing two buttons: 'wan (eth0) Disabled' and 'mobile (wwan0_1) Disabled'. A 'Refresh' button is located at the bottom right of the interface.

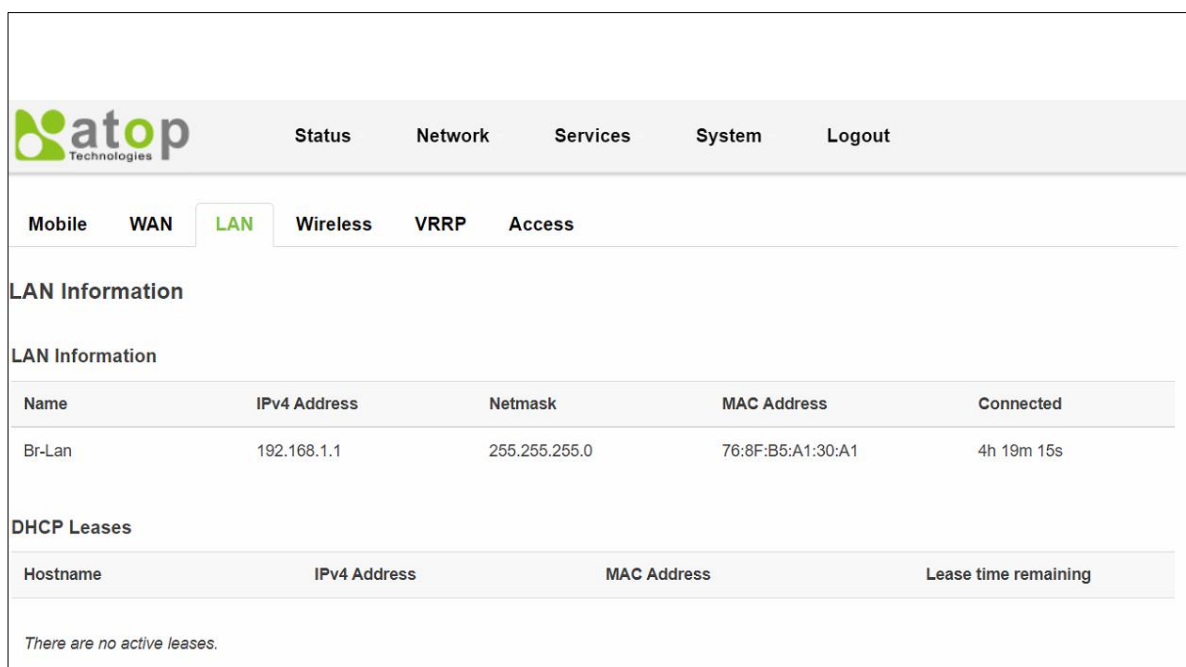
Table 6. Status > Network > WAN

Field	Description
Interface	Interface used for WAN connection.
Type	The current connection type status (DHCP/Static /PPPoE).
IPv4 address	The WAN IP address of the router.
MAC address	The WAN MAC address of the router.
Netmask	The WAN Netmask of the router.
Gateway	The WAN Gateway of the router.
DNS	The WAN DNS of the router.
Connected	The current amount of time which router has been connected.
wan (eth0)	The current wan status (Online/Offline/Disabled) of the WAN port interface.
mobile (wwan0_1)	The current wan status (Online/Offline/Disabled) of the mobile interface.

3.3.3 LAN

This section shows the LAN status information of the router.

Figure 12. Status > Network > LAN



The screenshot displays the router's web interface. At the top, there is a navigation bar with the 'atop Technologies' logo and tabs for Status, Network, Services, System, and Logout. Below this, a sub-navigation bar shows tabs for Mobile, WAN, LAN (which is highlighted in green), Wireless, VRRP, and Access. The main content area is titled 'LAN Information' and contains a table with the following data:

Name	IPv4 Address	Netmask	MAC Address	Connected
Br-Lan	192.168.1.1	255.255.255.0	76:8F:B5:A1:30:A1	4h 19m 15s

Below the table, there is a section for 'DHCP Leases' with a table that has columns for Hostname, IPv4 Address, MAC Address, and Lease time remaining. A message at the bottom states: 'There are no active leases.'


Table 7. Status > Network > LAN

Field	Description
Hostname	DHCP client's hostname.
IPv4-Address	DHCP client's IP address.
MAC-Address	DHCP client's MAC address.
Lease time remaining	The remaining lease time for a DHCP client. DHCP lease settings can be changed in the Network>Interface>LAN>DHCP Server section.

3.3.4 Wireless (AWR5805/CWR5805 Only)

This section is available in AWR5805 and CWR5805 model only. It shows the Wireless status information of the router.

Figure 13 Status > Network > Wireless



Status

Network

Services

System

Logout

Mobile

WAN

LAN

Wireless

VRRP

Access

Wireless Information

Wireless Information

Wi-Fi 2.4GHz Channel	1 (2.412 GHz)
Wi-Fi 5GHz Channel	48 (5.240 GHz)
Country Code	US

Wireless Status

SSID	Mode	Encryption	Wireless MAC	Signal Quality	Bit Rate
ATOP_CWR	Access Point	None	76:8F:B5:A1:30:A2	100%	300.0 Mbit/s
ATOP_CWR	Access Point	None	76:8F:B5:A1:30:A3	100%	866.0 Mbit/s

Associated Stations

MAC Address	IPv4 Address	Signal	RX Rate	TX Rate
76:63:73:FE:A4:C5	192.168.1.11	-70 dBm	78.0 Mbit/s	57.0 Mbit/s

Refresh

Table 8 Status > Network > Wireless

Field	Description
Wi-Fi 2.4GHz Channel	The display name of the Wi-Fi 2.4GHz interface on the CWR5805 device.
Wi-Fi 5GHz Channel	The display name of the Wi-Fi 5GHz interface on the CWR5805 device.
SSID	The broadcasted SSID of the wireless network that the client devices are connected to.
Mode	Access Point Mode.
Encryption	Type of Wi-Fi encryption that will be used.
Wireless MAC	Identify the basic service sets that are 48-bit labels and conform to the MAC-48 convention.
Signal Quality	The strength of the signal.
Bit Rate	The physical maximum possible throughput that the routers radio can handle. This value is cumulative. The bit rate will be shared between the router and other possible devices that connect to the local AP.
MAC Address	The MAC address of the associated station.
IPv4 Address	The IP address of the associated station.
Signal	The strength of the wireless between the CWR5805 and the associated station.
Rx Rate	The rate of the received packets from the associated station.
Tx Rate	The rate of the sent packets to the associated station.

3.3.5 VRRP

This section is available in AWR5805 and CWR5805 model only. The **Virtual Router Redundancy Protocol (VRRP)** is a computer networking protocol used for automatic default gateway selection for

clients on a **LAN network** in case the main router (Master) becomes unavailable. Another VRRP router (Backup) then assumes the role of Master; thus backing up the connection.

Figure 14. Status > Network > VRRP (Master)

VRRP LAN Status	
Status	Enabled
Virtual ip	192.168.1.253
Priority	100
Router	Master

Refresh

Figure 15. Status > Network > VRRP (Backup)

VRRP LAN Status	
Status	Enabled
Virtual ip	192.168.1.253
Priority	100
Router	Backup
Master ip	192.168.1.1

Table 9. Status > Network > VRRP

Field	Value	Description
Status	default: disable	VRRP status.
Virtual IP	default: 192.168.1.253	Virtual IP address(-es) for LAN's VRRP (Virtual Router Redundancy Protocol) cluster.
Priority	integer [1 - 255]; default: 100	The router with the highest priority value on the same VRRP cluster will act as a master.
Router	Master/Backup	Connection mode.
Master ip	ip	Master IP.

3.3.6 Access

Display information about local and remote active connections status.

Figure 16. Status > Network > Access

atop Technologies				
Status Network Services System Logout				
Mobile WAN LAN Wireless VRRP Access				
Access Status				
Access Information				
Local Access				
Type	Status	Port	Active connections	
SSH	Enabled	22	0 (0.00 B)	
TELNET	Enabled	23	0 (0.00 B)	
HTTP	Disabled	80	0 (0.00 B)	
HTTPS	Enabled	443	0 (0.00 B)	
Remote Access				
Type	Status	Port	Active connections	
SSH	Enabled	22	0 (0.00 B)	
TELNET	Enabled	23	0 (0.00 B)	
HTTP	Disabled	80	0 (0.00 B)	
HTTPS	Enabled	443	3 (9.50 KB)	
Refresh				

Table 10. Status > Network > Access

Field	Value	Description
Type	SSH/TELNET/HTTP/HTTPS	Type of connection protocol.
Status	disabled/enabled	Connection status.
Port	22/23/80/443	Connection port used.
Active connections	integer/data usage	Count of active connections and the amount of data transmitted.

3.4 Routes

The **Routes** sub-menu under the Status menu provides information such as an ARP table and a table of active IPv4 routes of the CWR5805 device.

3.4.1 ARP

The ARP section shows the router's active ARP table. An ARP table contains recently cached MAC addresses of every immediate device that was communicating with the router. This section also shows the router's routing table.

The description of each field in the ARP section is shown in the table below.

Figure 17. Status > Routes - ARP


 Status Network Services System Logout		
Routes		
ARP		
IPv4 Address	MAC Address	Interface
10.0.50.130	00:60:E9:09:61:4B	eth0
10.0.50.60	D0:37:45:3B:CD:37	eth0
192.168.1.2	D0:37:45:3B:C0:63	br-lan
192.168.1.7	00:60:E9:2D:A3:8B	br-lan

Table 11. Status > Routes - ARP

Field	Description
IPv4 Address	Recently cached IP addresses of every immediate device that was communicating with the router.
MAC-Address	Recently cached MAC addresses of every immediate device that was communicating with the router.
Interface	Interface used for the connection.

3.4.2 Active IPv4-Routes Section

The Active IPv4 Routes section indicates where a TCP/IP packet, with a specific IP address, should be directed to.

The description of each field is shown in the table below.

Figure 18. Status > Routes – Active IPv4 Routes

Active IPv4 Routes			
Network	Target	IPv4 Gateway	Metric
mobile	0.0.0.0/0	10.177.8.69	99
wan	10.0.50.0/24		0
mobile	10.177.8.64/29		0
mobile	10.177.8.69		0
lan	192.168.1.0/24		0

Table 12. Status > Routes – Active IPv4 Routes

Field	Description
Network	Interface to be used to transmit TCP/IP packets through.
Target	IP address and mask of the destination network. It is used to determine the actual IP addresses which the routing rule is applied. This field is represented by Classless Inter Domain Routing (CIDR) notation.
IPv4-Gateway	An IP address where the CWR5805 device should send all the traffic to.
Metric	A metric number indicating interface priority of usage. This value is used as a sorting method. If a routing packet falls into the category of two rules, the one with the lower metric is applied.

3.5 Logs

3.5.1 System Log

The **System Log** sub-menu under the Status menu follows a Message Logging standard. System Log collects data from most applications on the xxR5805 device, such as status, events, and diagnostics. The system Log message is categorized into 3 levels: Debug, Normal, and Warning.

This webpage substitute troubleshooting file that can be published to the external system log server.

Figure 19. Status > System > System Log

No. ⬆	Date-Time ⬆	Log type ⬆	Message ⬆
01205	2021-11-05 05:52:38	user.notice	vrrpd is running
01204	2021-11-05 05:52:38	user.notice	Ping to 8.8.8.8 successful
01203	2021-11-05 05:52:28	user.notice	vrrpd is running
01202	2021-11-05 05:52:28	user.notice	Ping to 8.8.8.8 successful
01201	2021-11-05 05:52:18	user.notice	vrrpd is running
01200	2021-11-05 05:52:18	user.notice	Ping to 8.8.8.8 successful
01199	2021-11-05 05:52:08	user.notice	PING failed. Retry 1 of
01198	2021-11-05 05:51:56	user.notice	vrrpd is running
01197	2021-11-05 05:51:56	user.notice	Ping to 8.8.8.8 successful
01196	2021-11-05 05:51:46	user.notice	vrrpd is running

Showing 1 to 10 of 1206 entries

<< Prev Next >>

Table 13. Status > System > System Log

Field	Description
Date-Time	The time format: YYYY-MM-DD HH-MM-SS.
Log Type	Log type.
Message	The description of the System log.

3.5.2 Kernel Log

The Kernel Log Provides on-screen Kernel logging information.

Figure 20. Status > System > Kernel Log

atop Technologies

Status Network Services System Logout

System Log Kernel Log

Kernel Log

Logs per page 10 Search

No. ↕	Timestamp ↕	Message ↕
01100	59.519343	__mc_netlink_receive: Enable bridge snooping!
01099	50.556145	[wifi1] FWLOG: [59426] VDEV_MGR_AP_TBTT_CONFIG (0x0, 0x1671, 0x0, 0x0)
01098	50.549535	[wifi1] FWLOG: [59426] RESMGR_OCS_GEN_PERIODIC_NOA (0x0)
01097	50.542937	[wifi1] FWLOG: [59426] RESMGR_OCS_GEN_PERIODIC_NOA (0x1)
01096	50.535385	[wifi1] FWLOG: [59426] VDEV_MGR_HP_START_TIME (0x0, 0x1671, 0xfb9001)
01095	50.529136	[wifi1] FWLOG: [59411] VDEV_MGR_VDEV_START_RESP (0x0)
01094	50.516553	[wifi1] FWLOG: [59220] WAL_DBGID_RST_STATS (0x2, 0x80, 0x1671, 0x1)
01093	50.512904	[wifi1] FWLOG: [59220] WAL channel change freq=5745, mode=10 flags=0 rx_ok=1 tx_ok=1
01092	50.505006	[wifi1] FWLOG: [59220] vap-0 VDEV_MGR_VDEV_START (0x1671, 0x2, 0x0, 0x0)
01091	50.498606	[wifi1] FWLOG: [59214] RESMGR_OCS_GEN_PERIODIC_NOA (0x0)

Showing 1 to 10 of 1100 entries << Prev Next >>

Table 14. Status > System > Kernel Log

Field	Description
Timestamp	The kernel log timestamp.
Message	The description of the Kernel log.

4 Network Menu

The Network menu contains 12 sub-menu items which provide some useful network applications on the xxR5805 device. The sub-menus are as follows: Mobile(CWR5805 only), WAN, LAN, Wireless(AWR5805 and CWR5805 only), Mesh(AWR5805 and CWR5805 only), IPv6, VLAN, LB and Failover(CWR5805 only), Firewall, Static Routes, DNS, and QoS.

Figure 21. Network

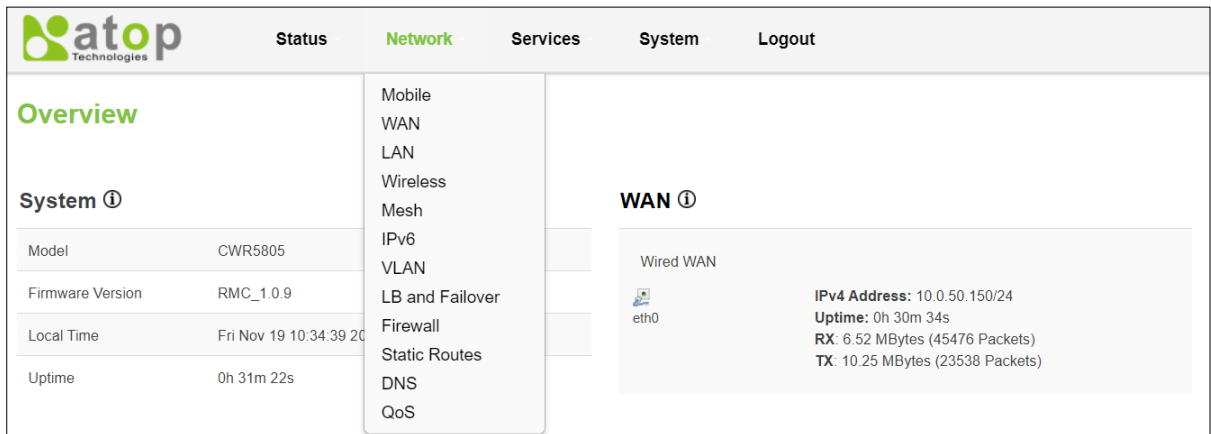


Figure 22. Network software feature supported list

	ER5805 series	AWR5805 series	CWR5805 series
Mobile	-	-	Supported
WAN	Supported	Supported	Supported
LAN	Supported	Supported	Supported
Wireless	-	Supported	Supported
Mesh	-	Supported	Supported
IPv6	Supported	Supported	Supported
VLAN	Supported	Supported	Supported
LB and Failover	-	-	Supported
Firewall	Supported	Supported	Supported
Static Routes	Supported	Supported	Supported
DNS	Supported	Supported	Supported
QoS	Supported	Supported	Supported

4.1 Mobile (CWR5805 only)

CWR5805 is also equipped with a 5G/LTE module. In the MOBILE tab of the Interfaces sub-menu of the Network menu, you can configure parameters related to the mobile data connection. The MOBILE tab consists of General Setup, Advanced Settings, and SIM Switch sub-tabs.


4.1.1 General Setup

In the **General Setup** sub-tab of Network-Interfaces-MOBILE tab, the **Status field** displays the current Mobile interface information of Uptime, MAC Address, RX, TX, and IPv4. You can configure QMI protocol parameters for the mobile interface, as shown in the Figure below.

You can modify these values in the General Setup tab except IP, which depends on their ISP SIM card information. For example, if the ISP SIM card supports public IP dial-up for Internet connection, then the value of the APN field can be set to public.

In the Mobile webpage, the default protocol is set as QMI (Qualcomm MSM Interface) Cellular, which is used for 5G/LTE dial-up to Internet connection. The default value of APN field is set to the Internet, and the default value of the PIN field is set to 0000. These default settings under the General Setup tab of the Interface-Mobile webpage apply to most ISP SIM card dial-up settings.

Figure 23. Network > Mobile > General Setup



StatusNetworkServicesSystemLogout

Mobile


Common Configuration

General Setup

Advanced Settings

SIM Switch

Status


wwan0_1

Uptime: 22h 27m 23s
MAC Address: EE:AE:CB:50:0F:B5
RX: 631.00 KBytes (7455 Packets)
TX: 861.68 KBytes (8722 Packets)
IPv4: 10.177.8.68/29

SIM1 Configuration

Protocol

QMI Cellular

Modem device

/dev/cdc-wdm0

APN

internet

PIN

0000

PAP/CHAP username

PAP/CHAP password

Authentication Type

NONE

Data roaming

☐

SIM2 Configuration

Protocol

QMI Cellular

Modem device

/dev/cdc-wdm0

APN

internet

PIN

0000

PAP/CHAP username

PAP/CHAP password

Authentication Type

NONE

Data roaming

☐

Table 15. Network > Mobile > General Setup

Field	Value	Description
Protocol	default: QMI Cellular	The protocol is used by the MOBILE interface.
Modem Device	default: /dev/cdc-wdm0	QMI device node.
APN	default: internet	An Access Point Name (APN) is the name of a gateway between a 5G/LTE mobile network. A mobile device making a data connection must be configured with an APN to present to the carrier. The carrier will then assign some connection parameters (e.g., security and priority level) based on the suitable type of network connection for that mobile device, depending on the contract with the operator.
PIN	default: 0000	A password is used for authenticating the modem to the SIM card.
PAP/CHAP Username	default: none	Username for PAP/CHAP authentication.
PAP/CHAP Password	default: none	Password for PAP/CHAP authentication.
Authentication Type	PAP/CHAP(both)/ PAP/CHAP/None/Custom default: none	Authentication method that the 5G/LTE carrier uses to authenticate new connections on its network. If PAP or CHAP is selected, you will also be required to enter a Username and password.
Data Roaming	default: disable	By default, this option is unchecked to prevent the CWR5805 device from establishing a mobile data connection while not in the device's home network.

4.1.1.1 Data Limit Configuration

In the **Data Limit Configuration** section within all sub-tabs of the MOBILE tab, you can configure the data usage limit to avoid unwanted data charges. The limit on the data connections can be pre-selected for each SIM card. When the limit is later reached, the data usage warnings will be sent to notify you via SMS messages.

4.1.1.2 Data Connection Limit Configuration

The **Data Connection Limit Configuration** section is used to configure custom mobile data limits for your SIM card. When the mobile data limit set for the SIM card is reached, the CWR5805 device will no longer use the mobile connection to establish a data connection until the limitation period is over or the limit is reset by you.

Figure 24. Network > Mobile > General Setup > Data Limit Configuration > Data Connection Limit Configuration

SIM1 Setup **SIM2 Setup**

Data Connection Limit Configuration

Enable data connection limit ☒ Disables mobile data when a limit for current period is reached

Data limit* (MB) Disable mobile data after limit value in MB is reached

Period Period for which mobile data limiting should apply

Start hour A starting hour in a day for mobile data limiting period

Table 16. Network > Mobile > General Setup > Data Limit Configuration > Data Connection Limit Configuration

Field	Values	Description
Enable Data Connection Limit	default: disable	Turns mobile data limitations on/off.
Data Limit (MB)	default: none	The amount of data that can be downloaded/uploaded over the specified period. When the limit is reached, the CWR5805 device will no longer be able to establish any data connection until the period is over or the data limit is reset.
Period	Day/Week/Month; default: Month	Length of time to monitor the data usage.
Start Hour	integer [1 – 24]; default: 1	Specify the hour that the monitoring period begins. After the period is over, the data usage is reset before the monitoring process restarts.

4.1.1.3 SMS Warning Configuration

In the **SMS Warning Configuration** section, you can configure a rule to send SMS messages after the data connection sent/received through the CWR5805 device's SIM card is reached the specified limit.

Figure 25. Network > Mobile > General Setup > Data Limit Configuration > SMS Warning Configuration

SMS Warning Configuration

Enable SMS warning ☒ ⓘ Enables sending of warning SMS message when mobile data limit for current period is reached

Data limit* (MB) ⓘ Send warning SMS message after limit value in MB is reached

Period ⓘ Period for which SMS warning for mobile data limit should apply

Start hour ⓘ A starting hour in a day for mobile data limit SMS warning

Phone number ⓘ A phone number to send warning SMS message to, e.g. +37012345678

Table 17. Network > Mobile > General Setup > Data Limit Configuration > SMS Warning Configuration

Field	Description
Enable SMS Warning	Turns SMS warning on/off.
Data Limit (MB)	The amount of the limit data usage in Mbytes before the CWR5805 device will send SMS warnings to the specified phone number.
Period	Length of time to monitor the data usage. Currently, the field supports the monitoring period monthly, weekly, and daily.
Start Day/ Start Hour	Specify the day that the monitoring period begins. After the period is over, the data usage is reset before the monitoring process restarts.
Phone Number	The recipient's phone number that the SMS messages will be sent.

4.1.1.4 Clear Data Limit

The **Clear Data Limit** section contains only one button - 'Clear data limit'. When clicked, the button resets the data limit counter for the selected SIM card. Thus, the count is started over again regardless of the specified period.

Figure 26. Network > Mobile > General Setup > Data Limit Configuration > Clear Data Limit

Clear Data Limit

Clear data limit

Clear

* Important: data limit database is not reset when the functionality is disabled and then re-enabled. Automatically the database is reset at a given Period (month, week, day). If you wish to reset it manually you can hit the "Clear" button.

Figure 27. Network > Mobile > General Setup > Data Limit Configuration > Clear Data Limit

Field	Description
Clear Data Limit	When clicked, the data limit counter for the selected SIM card is reset. The count is started at 0 regardless of when it occurred in the specified period.

4.1.2 Advanced Settings Sub-Tab

In the **Advanced Setting** sub-tab of the Network-Interfaces-MOBILE tab, you can configure network functionalities in more detail based on your requirement for the mobile interface.

Figure 28. Network > Mobile > Advanced Settings

Mobile

Common Configuration

General Setup

Advanced Settings

SIM Switch

Bring up on boot

☒

cellular_mode

LTE+5G NR

▼

Use gateway metric

99

MTU mode

Auto

▼

Use regular ping

☐

Table 18. Network > Mobile > Advanced Settings

Field	Value	Description
Bring Up on Boot	default: enable	Specify whether or not to bring up the WAN interface on the boot.
cellular_mode	default: LTE+5G NR	Specify the Mobile mode: LTE+5G NR. LTE only, 5G only.
Use Gateway Metric	default: 99	The priority of the gateway on the WAN interface. By default, a routing table entry is generated. You can alter the metric of that entry in this field.
MTU mode	default: Auto	MTU size is based on ISP.
MTU value	576~1500	Specify the value of MTU when select MTU mode with "Custom".
Use regular ping	default: disable	Use regular ping to check the stability of mobile Network.
Interval (seconds)	default: 30	Define the interval time during every regular ping round.
Ping IP	default: 8.8.8.8	Specify the Host IP that CAN be ping.
Ping retry	default: 2	Define the Ping retry numbers for one regular ping round.
Ping timeout (seconds)	default: 2	Define the timeout of one Ping if DUT doesn't receive ping response..
Redial after failed rounds	default: 2	Define meet the numbers of failed regular ping rounds and then let mobile redial. (If Enable "No Network" in SIM Switch, do SIM Switch action.)

4.1.3 SIM Switch

In the **SIM Switch** sub-tab of the Network-Interfaces-MOBILE tab, you can configure switching the current SIM card to the other SIM card when the 5G/LTE network conditions are proper.

Figure 29. Network > Mobile > SIM Switch

Mobile

Common Configuration

General Setup

Advanced Settings

SIM Switch

Primary SIM Card

SIM1

Automatic Switching

☒

Check Interval

5 Sec

On Weak Signal

☐

On Data Limit

☐

No Network

☐

Current SIM Slot

1

Table 19. Network > Mobile > SIM Switch

[illegible]

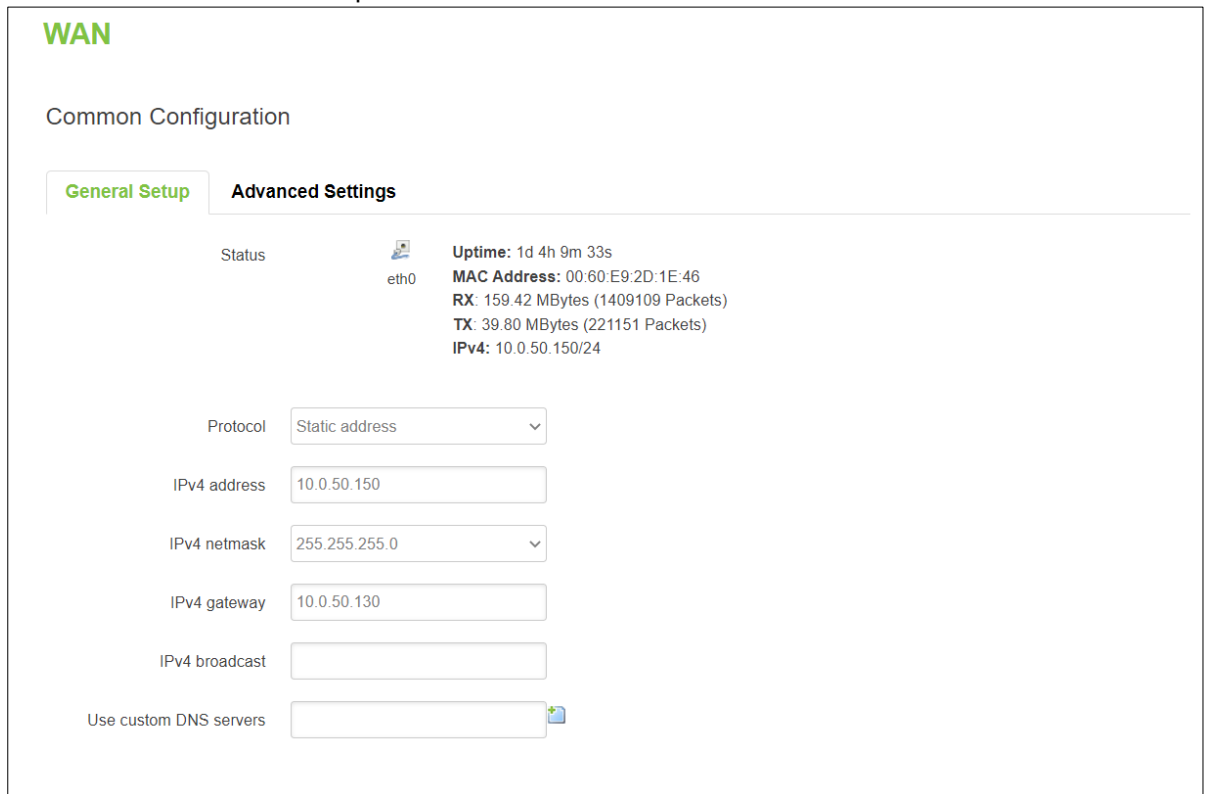
4.2 WAN

A **Wide Area Network** (WAN) is a telecommunications network or computer network that extends over a large geographical distance. For example, the Internet is a wide area network.

4.2.1 General Setup

In the General Setup sub-tab of the Network-Interfaces-WAN tab, different protocols for the WAN interface can be configured.


Figure 30. Network > WAN > General Setup



WAN

Common Configuration

General Setup Advanced Settings

Status  **Uptime:** 1d 4h 9m 33s
MAC Address: 00:60:E9:2D:1E:46
RX: 159.42 MBytes (1409109 Packets)
TX: 39.80 MBytes (221151 Packets)
IPv4: 10.0.50.150/24


Protocol Static address ▼

IPv4 address 10.0.50.150

IPv4 netmask 255.255.255.0 ▼

IPv4 gateway 10.0.50.130

IPv4 broadcast

Use custom DNS servers 

You can switch between Static, DHCP, or PPPoE protocol by selecting the protocol that you want to use and then pressing **Switch Protocol**.

In the **WAN** webpage, the default protocol is set to **DHCP client**. It means that the WAN interface can get a dynamic IPv4 address from its connected Ethernet port of a Cable/ADSL modem.

As shown in the Figure above, the **Status** field currently displays the WAN interface (eth0) information of Uptime, MAC Address, RX, TX, and IPv4. If the connected Cable/ADSL modem can provide an Internet service, CWR5805 also has an Internet service available via its WAN interface.

In addition, there are two other protocols supported by the WAN interface which are **Static address** and **PPPoE**. The setting of the protocol option for the WAN interface depends on the protocol requirement of the connected frontend Cable/ADSL modem.

4.2.2 DHCP Client


4.2.2.1 General Setup

Figure 31. Network > WAN > General Setup – DHCP Client

WAN

Common Configuration

General Setup Advanced Settings

Status  **Uptime:** 0h 8m 26s
MAC Address: B6:00:71:A9:B0:7D
RX: 1.57 MBytes (13358 Packets)
TX: 953.99 KBytes (2173 Packets)
IPv4: 10.0.50.150/16

Protocol

Hostname to send when requesting DHCP

Table 20. Network > WAN > General Setup – DHCP Client

Field	Value	Description
Protocol	Static, DHCP and PPPoE; default: DHCP	The protocol is used by the WAN interface.
Hostname to send when requesting DHCP	ip/hostname; default: none	Hostname to which the DHCP request will be sent.

4.2.2.2 Advanced Settings

In the General Setup sub-tab of the Network-Interfaces-WAN tab, you can configure the WAN interface in more detail.

Figure 32. Network > WAN > Advanced Settings – DHCP Client

WAN

Common Configuration

General Setup **Advanced Settings**

Override MAC address

Override MTU

Use gateway metric

Table 21. Network > WAN > Advanced Settings – DHCP Client

Field	Value	Description
-------	-------	-------------

Override MAC address	default: CWR's MAC	To override the MAC address of the WAN interface. For example, your ISP (Internet Service Provider) gives you a static IP address and it might also bind it to your computers' MAC address. In this field, you can enter the computer's MAC address and fool the gateway into thinking that it is communicating with your computer.
Override MTU	integer [1 – 1500]; default: 1500	Specify the maximum transferred size of a data packet.
Use Gateway Metric	default: 0	By default, the WAN configuration generates a routing table entry. You can change the metric of that entry here.

4.2.3 Static address

4.2.3.1 General Setup

Figure 33. Network > WAN > General Setup – Static Address

The screenshot shows the 'WAN' configuration page with the 'General Setup' tab selected. Under 'Common Configuration', the 'eth0' interface status is displayed with uptime, MAC address, RX/TX statistics, and IPv4 address. Below this, the 'Protocol' is set to 'Static address'. The 'IPv4 address' is 10.0.50.150, 'IPv4 netmask' is 255.255.255.0, 'IPv4 gateway' is 10.0.50.254, and 'IPv4 broadcast' is 10.0.50.255. The 'Use custom DNS servers' checkbox is checked with the value 8.8.8.8.

Table 22. Network > WAN > General Setup – Static Address

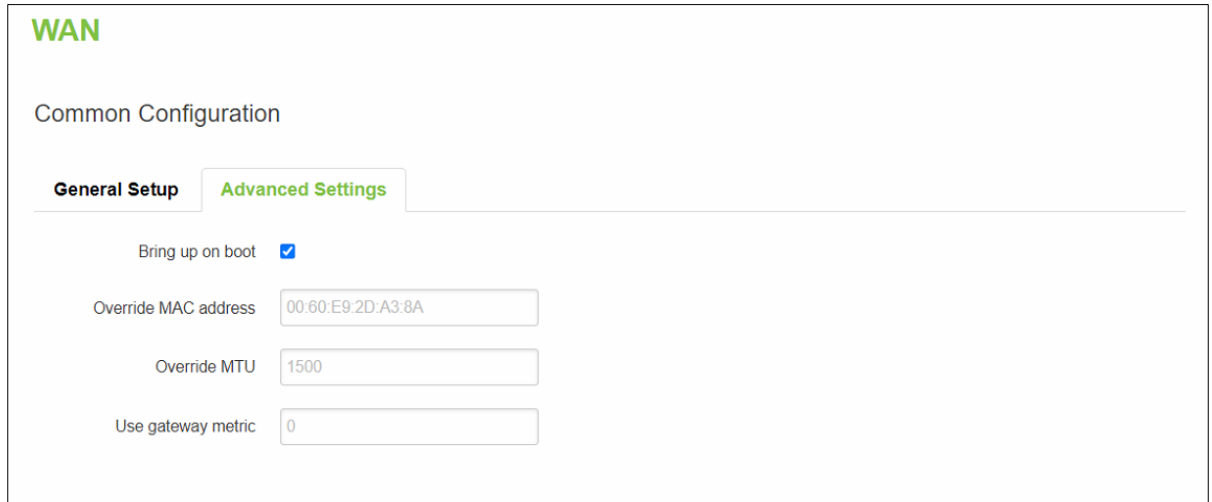
Field	Value	Description
Protocol	Static/DHCP/PPPoE; default: DHCP	The protocol is used by the WAN interface. This field currently supports DHCP clients, static address, and PPPoE.
IPv4 address	ip4; default: none	Your router's address on the WAN network.
IPv4 netmask	netmask; default: none	Netmask defines how "large" a network is.
IPv4 gateway	ip4; default: none	The IPv4 address gateway of this interface. An interface's gateway is the default next-hop address to access other networks.
IPv4 broadcast	ip4; default: none	IP broadcasts are used by BOOTP and DHCP clients to find and send requests to their respective servers.

Use custom DNS servers	ip4; default: none	By entering custom DNS servers, the router will take care of the hostname resolution. You can enter multiple DNS servers to provide redundancy in case one of the servers fails.
------------------------	---------------------------	--

4.2.3.2 Advanced Settings

These are the advanced settings for each of the protocols. If you are unsure of how to alter these attributes, it is highly recommended to leave them to a trained professional:

Figure 34. Network > WAN > Advanced Settings – Static Address



WAN

Common Configuration

General Setup **Advanced Settings**

Bring up on boot ☒

Override MAC address

Override MTU

Use gateway metric

Table 23. Network > WAN > Advanced Settings – Static Address

Field	Value	Description
Bring up on boot	default: enable	Specify whether to bring up the LAN interface on boot or not.
Override MAC address	default: Device's MAC	Override the MAC address of the LAN interface.
Override MTU	default: 1500	Specify the maximum transferred size of a data packet.
Use gateway metric	default: 0	The WAN configuration by default generates a routing table entry. With this field, you can alter the metric of that entry.

4.2.4 PPPoE

4.2.4.1 General Setup


This protocol is mainly used by DSL providers.

Figure 35. Network > WAN > General Setup – PPPoE

WAN

Common Configuration


General Setup | Advanced Settings

Status  pppoe-wan RX: 0.00 Bytes (0 Packets) TX: 0.00 Bytes (0 Packets)

Protocol:

PAP/CHAP username:

PAP/CHAP password:

Access Concentrator:
 Leave empty to autodetect


Service Name:
 Leave empty to autodetect

Table 24. Network > WAN > General Setup – PPPoE

Field	Value	Description
Protocol	Static /DHCP /PPPoE default: DHCP	The protocol is used by the WAN interface. This field currently supports DHCP client, static address, and PPPoE.
PAP/CHAP Username	default: non	The username used in PAP/CHAP authentication.
PAP/CHAP password	default: none	The password used in PAP/CHAP authentication.
Access Concentrator	default: auto	The Access Concentrator to connect to ISPs used Access Concentrators to route their PPPoE connections. Usually, the settings are received automatically, however, in some cases, it is required to specify the name for an Access Concentrator. Leave this field empty to detect Access Concentrators automatically.
Service Name	default: auto	The Service Name to connect to. Leave this field empty to detect the Service name automatically.

4.2.4.2 Advanced Settings

Figure 36. Network > WAN > Advanced Setting – PPPoE

WAN

Common Configuration

General Setup

Advanced Settings

Bring up on boot ☒

Enable IPv6 negotiation on the PPP link ☐

Use default gateway ☒ ⓘ If unchecked, no default route is configured

Use gateway metric

Use DNS servers advertised by peer ☒ ⓘ If unchecked, the advertised DNS server addresses are ignored

LCP echo failure threshold ⓘ Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures

LCP echo interval ⓘ Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold

Inactivity timeout ⓘ Close inactive connection after the given amount of seconds, use 0 to persist connection

Override MTU

Table 25. Network > WAN > Advanced Setting – PPPoE

Field	Value	Description
Bring up on boot	default: enable	Specify whether to bring up the WAN interface on boot or not.
Enable IPv6 negotiation on the PPP link	default: disable	Point-to-point protocol.
Use default gateway	default: enable	If unchecked, no default route is configured.
Use gateway metric	default: 0	The WAN configuration by default generates a routing table entry. With this field, you can alter the metric of that entry.
Use DNS servers advertised by peer	default: enable	If unchecked, the advertised DNS server addresses are ignored.
LCP echo failure threshold	default: 0	Presume peer to be dead after the given amount of LCP echo failures, use 0 to ignore failures.
LCP echo interval	default: 6	Send LCP echo requests at the given interval in seconds, only effective in conjunction with the failure threshold.
Inactivity timeout	default: 0	Close inactive connection after the given number of seconds, use 0 to persist connection.
Override MTU	default: 1500	Specify the maximum transferred size of a data packet.

4.3 LAN

A **local area network** (LAN) is a computer network that interconnects computers within a limited area such as a residence, a school, a laboratory, a university campus, or an office building.

In the **Interface-LAN** webpage, the default protocol is set to a **Static address** with a default IPv4 address of 192.168.1.1.

The IPv4 DHCP server is also enabled by default on this interface. It means that any device with IPv4 DHCP client enabled in its Ethernet interface will be assigned a dynamic IP address from the LAN port interface of CWR5805. The default IP address of the IPv4 DHCP server is 192.168.1.1, and the dynamic IP address range starts from 192.168.1.100 to 192.168.1.250.

4.3.1 General Setup

In the **General Setup** sub-tab of the Network-Interfaces-LAN tab, you can configure the CWR5805 device’s network settings e.g., IP address, IP netmask, IP gateway, and DNS server.

As shown in the Figure below, the Status field currently displays LAN port interface (br-lan) information of Uptime, MAC Address, RX, TX, and IPv4. For a DHCP client, a device connected to a LAN port interface will be assigned an IPv4 address.

Figure 37. Network > LAN > Common Configuration – Static Address

LAN

Common Configuration

General Setup

Status

br-lan

Uptime: 1h 29m 32s

MAC Address: E2:45:C0:8C:44:41

RX: 611.93 KBytes (4442 Packets)

TX: 1.12 MBytes (5387 Packets)

IPv4: 192.168.1.1/24

Protocol

Static address

IPv4 address

192.168.1.1

IPv4 netmask

255.255.255.0

IPv4 broadcast

Use custom DNS servers

Table 26. Network > LAN > Common Configuration – Static Address

Field	Value	Description
Protocol	Static address	The protocol is used by the LAN interface. This field currently supports DHCP client and Static address.
IPv4 Address	default: 192.168.1.1	IPv4 that the router uses on the LAN network.
IPv4 Netmask	default: 255.255.255.0	IPv4 netmask is used to define how "large" the LAN network is.
IPv4 Gateway	default: none	Default IPv4 gateway for LAN network.
IPv4 Broadcast	default: none	IP broadcast is used by BOOTP and DHCP clients to find and send requests to their respective servers.
Use Custom DNS servers	ip; default: none	Specify DNS server for LAN network.

4.3.2 DHCP Server

A **DHCP server** is a service that can automatically configure the TCP/IP settings of any device that requests such a service (i.e., connects to the device with the operational DHCP server). If you connect a device that has been configured to obtain an IP address automatically, the DHCP server will lease out an IP address from the available IP pool and the device will be able to communicate within the private network.

The physical network interfaces of Ethernet Adapter (eth1), Wi-Fi 2.4GHz (ATOP_CWR), and Wi-Fi 5GHz (ATOP_CWR) are bridged together. In another word, any IPv4 DHCP client devices connected to a LAN port interface, wireless 2.4GHz/5GHz AP can be assigned a dynamic IPv4 address in the same network domain of 192.168.1.x. This means that these IPv4 DHCP client devices can communicate with each other via the bridged interface (br-lan).

4.3.2.1 General Setup

In the **General Setup** inner sub-tab of the DHCP Server section within the Network-Interface-LAN tab. Sub-tabs in the basic setting of the DHCP server service is available.

Figure 38. Network > LAN > DHCP Server > General Setup

DHCP Server

General Setup Advanced Settings

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

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

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

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

Start IP address 192.168.1.100

End IP address 192.168.1.249

Table 27. Network > LAN > DHCP Server > General Setup

Field	Value	Description
Disable DHCP	default: disable	To enable/disable DHCP server for LAN interface.
Start	default: 100	The starting IP address value.

Limit	default: 150	Maximum numbers of IP addresses the DHCP server can lease out.
Leasetime	default: 12h	The duration of an IP address lease. Leased out addresses will expire after the amount of time specified in this field and the device that was using the lease will have to request a new DHCP lease.

4.3.2.2 Static Leases

The **Static Leases** section is used to reserve specific IP addresses for specific client devices by binding them to their MAC address. This is useful when you have a stationary device connected to a network that needs to be reached frequently, e.g., printer, IP phone, etc.

Figure 39. Network > LAN > DHCP Server > Static Leases

Static Leases

Hostname	MAC Address	IPv4 Address
<input type="text"/>	<input type="text"/>	<input type="text"/>

Table 28. Network > LAN > DHCP Server > Static Leases

Field	Description
Hostname	A custom name that will be linked with the device.
MAC-Address	Device's MAC address.
IPv4-Address	The desirable IP address will be reserved for the specified device.
Add	To add a new static IP leased entry.

4.3.2.3 Advanced Settings

In the **Advanced Settings** inner sub-tab of the DHCP Server section within Network-Interface-LAN tap-All sub taps, you can configure more complicated settings of the DHCP server service.

Figure 40. Network > LAN > DHCP Server > Advanced Settings

DHCP Server

General Setup **Advanced Settings**

Dynamic DHCP ☒ Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

DHCP-Options

Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.

Table 29. Network > LAN > DHCP Server > Advanced Settings

Field	Description
Dynamic DHCP	If checked, dynamically allocate DHCP addresses for clients. If not checked, only provides service to static IP address clients.

DHCP-Options	Define additional DHCP options, for example, "192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.
--------------	---

4.4 Wireless

In the Wireless Overview section within the Network-Wifi sub-menu, you can configure wireless access points and choose the method to scan wireless stations. Here, you can disable or enable WiFi interfaces, or configure each WiFi interface in detail by pressing the Edit button. The configuration webpage of the selected WiFi interface will be initialized.

In the **Wifi** sub-menu within the Network menu, you can manage and configure Wi-Fi Access Points (AP) and Wi-Fi Stations (STA). The AWR5805 and CWR5805 device supports **IEEE802.11 a/b/g/n/ac** wireless technologies.

4.4.1 Wireless Overview

The Wi-Fi 2.4GHz field indicates the status of the Wi-Fi 2.4GHz port interface (wifi0). It contains information about SNR, SSID, mode, bit rate, BSSID, and encryption.

The Wi-Fi 5GHz field indicates the status of the Wi-Fi 5GHz port interface (wifi1). It contains information about SNR, SSID, mode, bit rate, BSSID, and encryption.

Figure 41. Network > Wireless > Wireless Overview

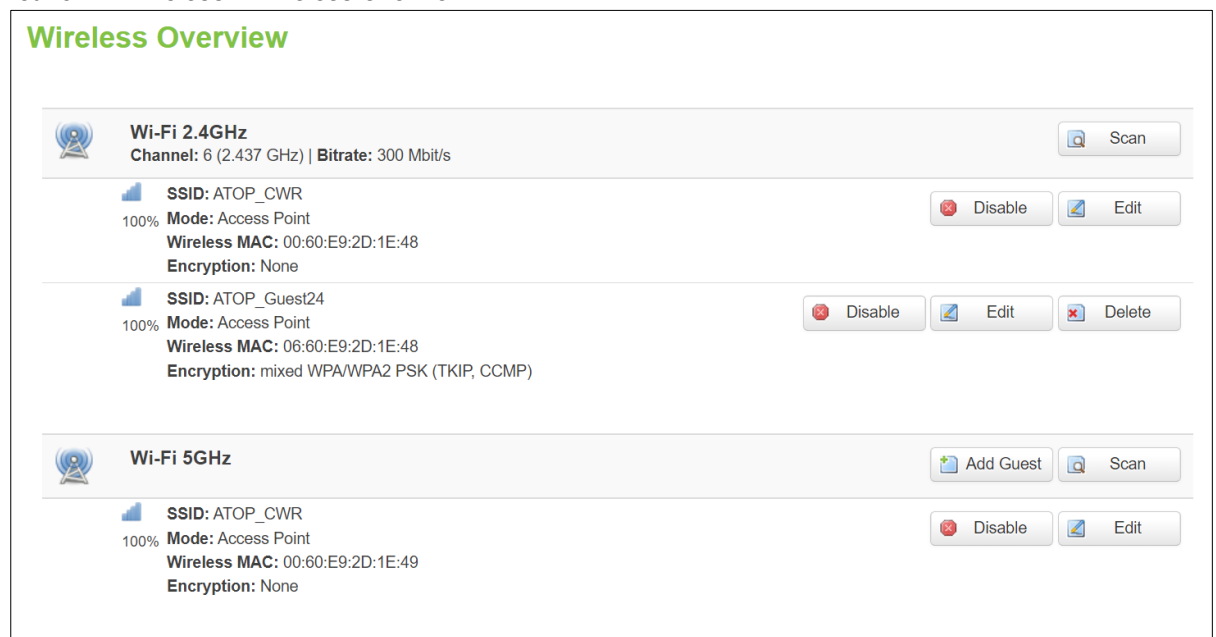


Table 30. Network > Wireless > Wireless Overview

Field	Description
Scan	To scan for available wireless stations within the surrounding area.
Enable/Disable	To enable/disable Wi-Fi 2.4GHz/5GHz access point.
Edit	To configure Wi-Fi 2.4GHz/5GHz access point in detail.

Click the **Scan** button to scan the currently available Wi-Fi Access Points in the surrounding area is displayed, as shown in the Figure below. This section will be initialized with you click the "Scan" button in the Wireless Overview section.

Figure 42. Network > Wireless > Wireless Scan

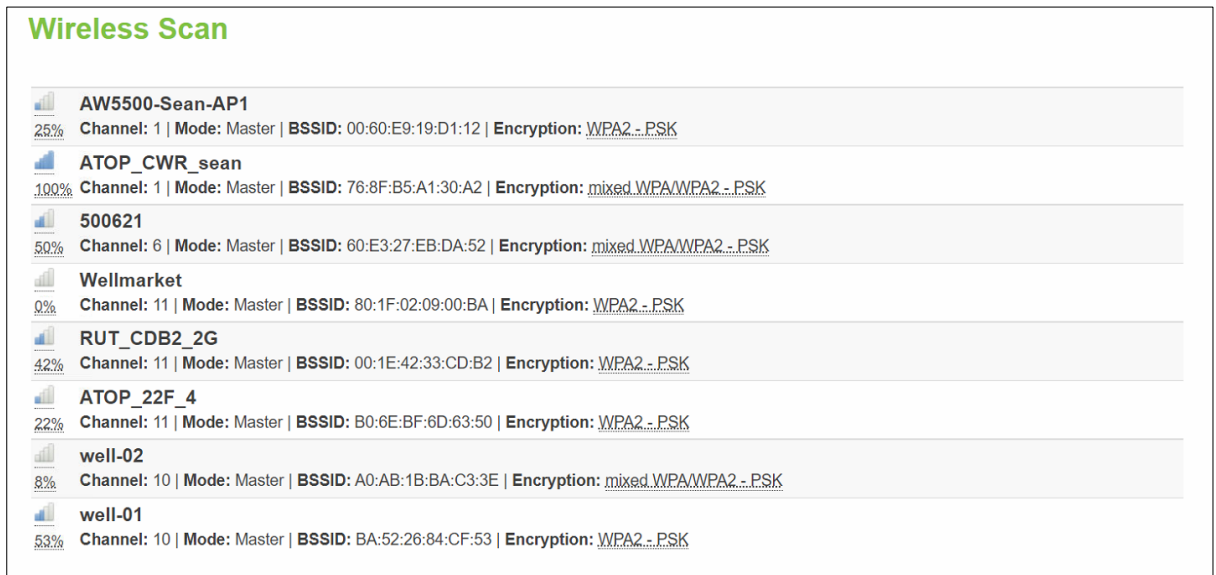


Table 31. Network > Wireless > Wireless Scan

Field	Description
Signal Level	Received Signal Strength Indicator (RSSI) level measured in percentage.
SSID	The broadcasted SSID of the wireless network that clients will be connected to.
Channel	Currently used Wi-Fi channel by the access point.
Mode	Current only support Master (access point) mode.
BSSID	MAC address. Identify the basic service sets that are 48-bit labels. It conforms to the MAC-48 convention.
Encryption	Encryption type that Wi-Fi access point use.

4.4.2 Associated Stations

The section displays a list of all devices and their MAC address that are maintaining connections with your router right now.

Figure 43. Network > Wireless > Associated Stations



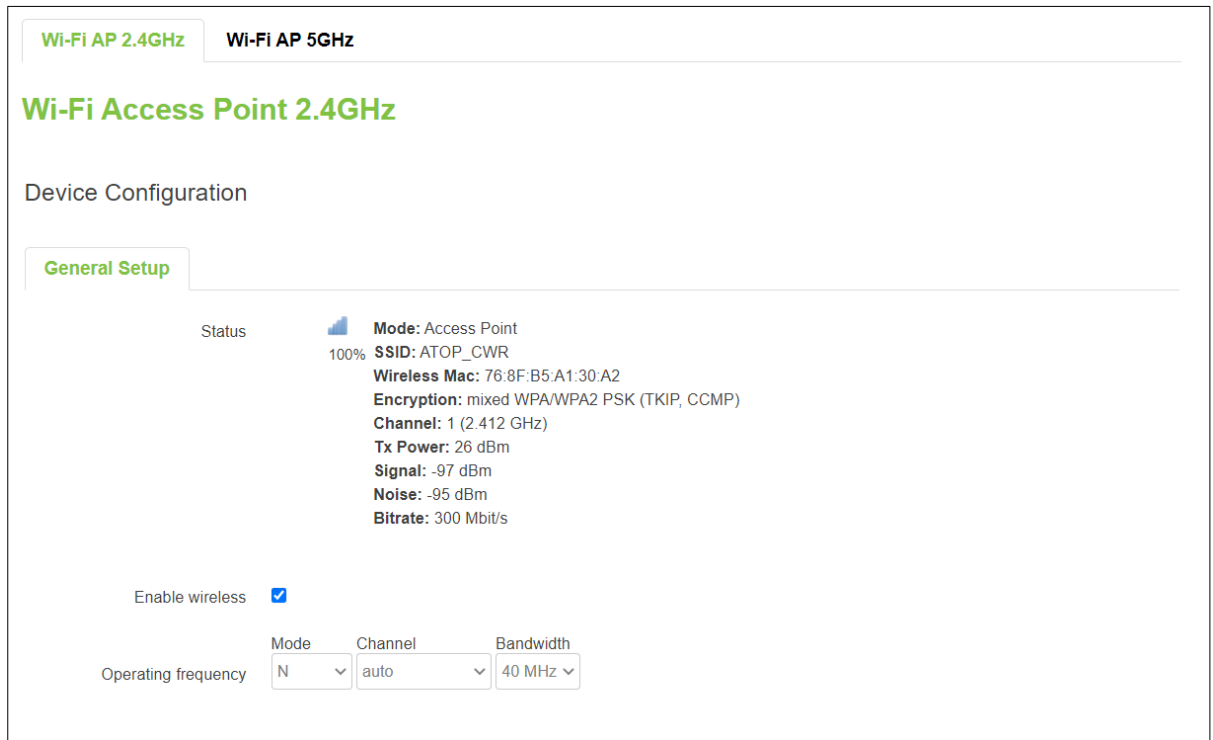
Table 32. Network > Wireless > Associated Stations

Field	Description
MAC Address	The MAC address of the associated station.
IPv4 Address	The IP address of the associated station.
Signal	The strength of the wireless between the the CWR5805 and associated station.
Rx Rate	The rate of the received packets from the associated station.
Tx Rate	The rate of the sent packets to the associated station.

4.4.3 Device Configuration

In the **Device Configuration** webpage of the Wireless Overview section within the Network-Wifi sub-menu, you can configure the parameters of the Wi-Fi 2.4GHz/5GHz access point, as shown in the Figure below. This section will be initialized when you click on the “Edit” button in the Wireless Overview section.

Figure 44. Network > Wireless > Edit Wi-Fi AP 2.4GHz




Wi-Fi AP 2.4GHz **Wi-Fi AP 5GHz**

Wi-Fi Access Point 2.4GHz

Device Configuration

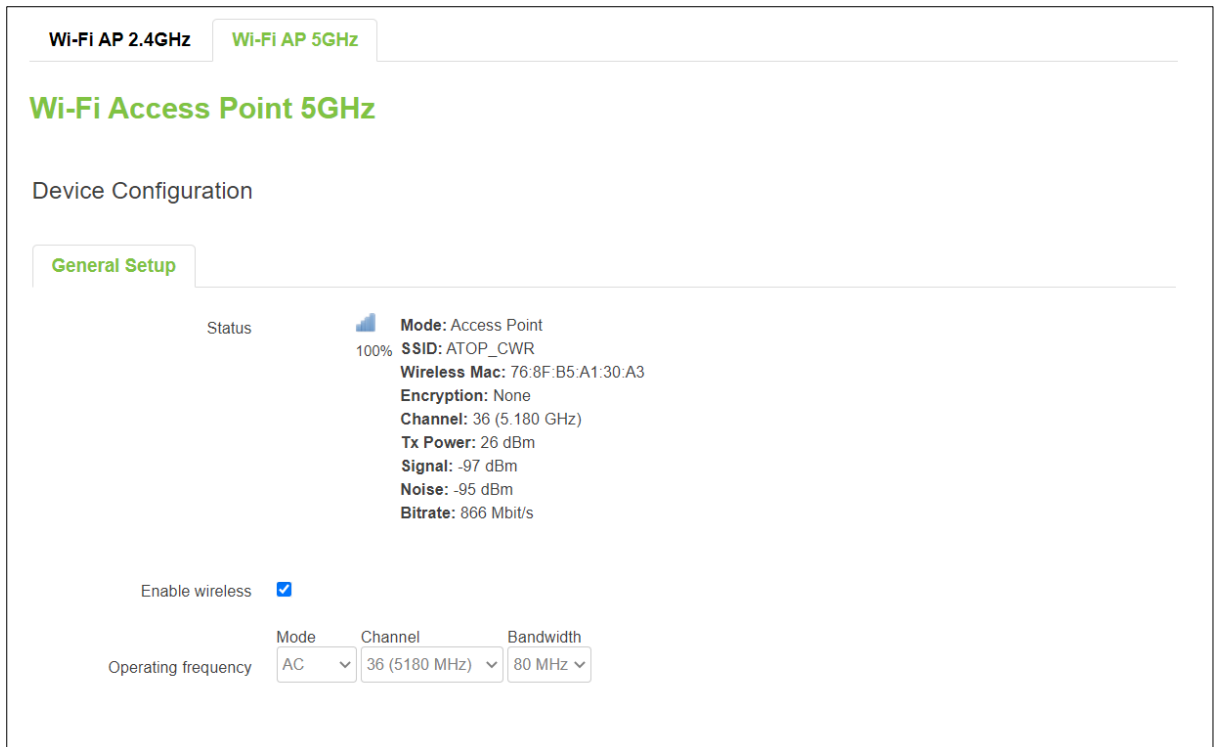
General Setup

Status  **Mode:** Access Point
100% **SSID:** ATOP_CWR
Wireless Mac: 76:8F:B5:A1:30:A2
Encryption: mixed WPA/WPA2 PSK (TKIP, CCMP)
Channel: 1 (2.412 GHz)
Tx Power: 26 dBm
Signal: -97 dBm
Noise: -95 dBm
Bitrate: 300 Mbit/s

Enable wireless ☒

Operating frequency **Mode** **Channel** **Bandwidth**
N auto 40 MHz

Figure 45. Network > Wireless > Edit Wi-Fi AP 5GHz




Wi-Fi AP 2.4GHz **Wi-Fi AP 5GHz**

Wi-Fi Access Point 5GHz

Device Configuration

General Setup

Status  **Mode:** Access Point
100% **SSID:** ATOP_CWR
Wireless Mac: 76:8F:B5:A1:30:A3
Encryption: None
Channel: 36 (5.180 GHz)
Tx Power: 26 dBm
Signal: -97 dBm
Noise: -95 dBm
Bitrate: 866 Mbit/s

Enable wireless ☒

Operating frequency **Mode** **Channel** **Bandwidth**
AC 36 (5180 MHz) 80 MHz

Table 33. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz

Field	Value		Description
Status	-		The status of Wi-Fi 2.4GHz/5GHz access point, which contains signal level, mode, BSSID, encryption, channel, tx-power, SNR, and bitrate info.
Enable Wireless	disable/enable; default: disable		To enable/disable Wi-Fi 2.4GHz/5GHz access point.
Operating Frequency -Mode	2.4GHz	legacy (b/g) mode and N mode	The wireless protocol is used by the access point.
	5GHz	legacy (a) mode, N mode, and AC mode	
Operating Frequency -Channel	2.4GHz	Auto/1/2/3/4/5/6/7/8/9/10/11; default: Auto	
	5GHz	Auto/36/40/44/48/149/153/157/161/165; default: Auto	
Operating Frequency -Width	2.4GHz	20/40MHz in N mode	
	5GHz	20/40 MHz in N mode, and 20/40/80 MHz in AC mode	

4.4.3.1 Interface Configuration

In the **Interface Configuration** webpage of the Wireless Overview section within the Network-Wifi sub-menu, you can configure the software parameters of the Wi-Fi 2.4GHz/5GHz access point. This section will be initialized with you click the “Edit” button in the Wireless Overview section.

4.4.3.1.1 General Setup

In the **General Setup** sub-tab within the Interface Configuration webpage, you can configure the SSID of Wi-Fi 2.4GHz/5GHz Access Points, as shown in the Figure below.

Figure 46. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > General Setup

Interface Configuration

General Setup Wireless Security MAC-Filter

SSID:

Mode:

Hide SSID ☐ Will render your SSID hidden from other devices that try to scan the area

Table 34. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > General Setup

Field	Value	Description
SSID	default: ATOP_CWR	The broadcast SSID of the wireless network that clients will be connected to.
Mode	default: Access Point	Access Point mode only.
Hide SSID	default: disable	Will render your SSID hidden from other devices that try to scan the area.

4.4.3.1.2 Wireless Security

In the **Wireless Security** sub-tab within the Interface Configuration webpage, you can configure the encryption type that will be used in Wi-Fi Access Point 2.4GHz/5GHz, as shown in the Figure below.

Figure 47. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > Wireless Security

Interface Configuration

General Setup **Wireless Security** MAC-Filter

Encryption WPA-PSK/WPA2-PSK Mixed Mode

Cipher auto

Key *****

Table 35. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > General Setup

Field	Value	Description
Encryption	No Encryption OWE WPA2-PSK WPA - PSK/WPA2-PSK Mixed Mode WPA3-Personal (SAE) default: No Encryption	Type of Wi-Fi encryption used.
Cipher*	auto/Force CCMP (AES)/Force TKIP and CCMP (AES) default: auto	An algorithm for performing encryption or decryption.
Key	default: none	A custom passphrase is used for authentication (8-63 characters long).

*: WPA&WPA2 used

4.4.3.1.3 MAC-Filter

You can define a rule for what to do with the MAC list you have defined. You can either allow only the listed MACs or allow "ALL" but forbid the listed ones.

Figure 48. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > MAC-Filter

Interface Configuration

General Setup Wireless Security **MAC-Filter**

MAC-Address Filter Allow listed only

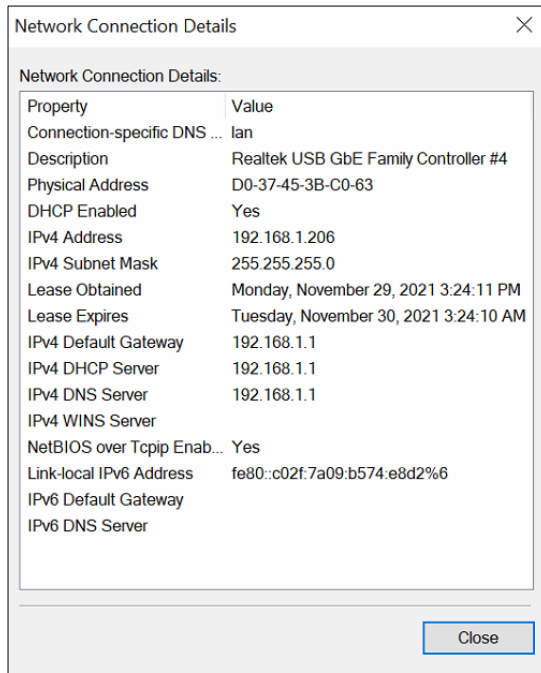
MAC-List

Table 36. Network > Wireless > Edit Wi-Fi AP 2.4/5GHz > MAC-Filter

Field	Value	Description
MAC-Address Filter	disable/Allow listed only/Allow all except listed; default: disable	Select MAC address Filter mode.
MAC-List	MAC; default: none	Input MAC list.

4.4.4 Tutorials

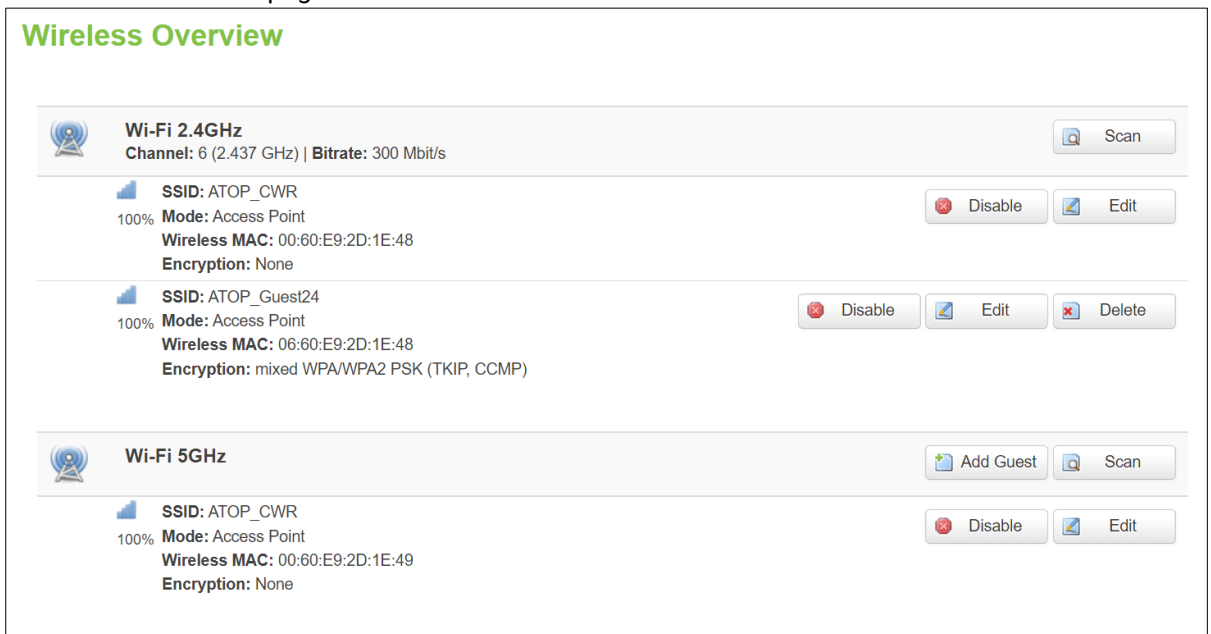
This tutorial shows how to set up a CWR by configuring its wireless access point functions and testing its connectivities.



4.4.4.1 Configuring Wireless Access Point

In Wireless Overview webpage, there are two wireless AP services available. By default, the Wi-Fi 2.4Ghz interface operated with 802.11N mode, and the Wi-Fi 5GHz interface operated with 802.11AC mode. The Associated Stations table lists connected client devices under the two wireless AP networks (SSID).

Figure 49. Wireless Overview Webpage under Wifi Menu



You can use any wireless devices such as mobile phone, tablet, and laptop to connect to wireless APs.

For the 2.4 GHz band wireless AP

1. ESSID is set to **ATOP_WiFi_24G** in General Setup tab.
2. Encryption is set to mixed **WPA-PSK/WPA2-PSK Mixed Mode** in Wireless Security tab.

3. Key is set **atopatop** in Wireless Security tab.

For the 5 GHz band wireless AP

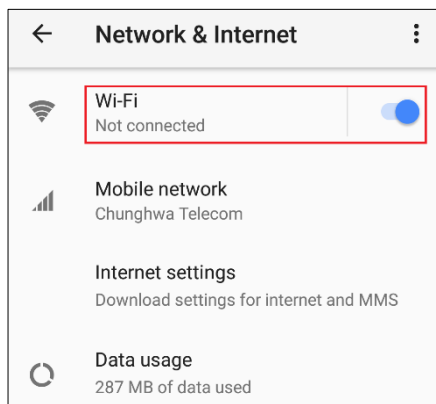
1. ESSID is set to ATOP_WiFi_5G in General Setup tab.
2. Encryption is set to mixed WPA-PSK/WPA2-PSK Mixed Mode in Wireless Security tab.
3. Key is set atopatop in Wireless Security tab.

The following steps show the method to connect an Android smartphone to the 2.4GHz band wireless AP on CWR5805 device.

Step1: Turning on Wi-Fi on Andriod Smartphone

Select the **Settings** icon to enter Settings and then select **Network & Internet** to enter the Network & Internet screen. As shown in the Figure below, select the Wi-Fi item and turn Wi-Fi on.

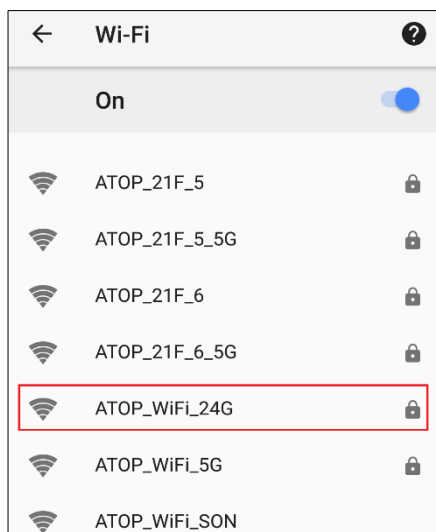
Figure 50. Network & Internet Settings on the Android System



Step 2: Selecting the 2.4 GHz band wireless AP

Tap on the **Wi-Fi** icon to enter the Wi-Fi scanning screen, select SSID named **ATOP_WiFi_24G** for connection.

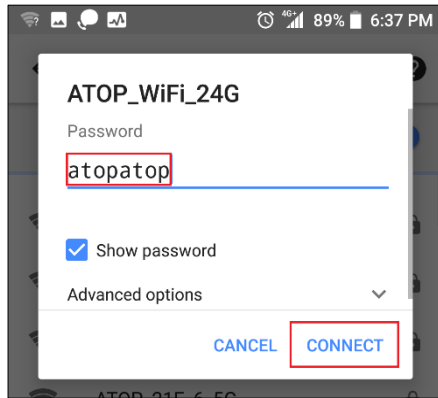
Figure 51. Select ATOP_WiFi_24G AP under Network & Internet Menu



Step 3: Input password (network key) for Wi-Fi connection

As shown in the Figure below, input the password (network key) which is “atopatop” in the Password field, then push the CONNECT button thus starting a Wi-Fi connection.

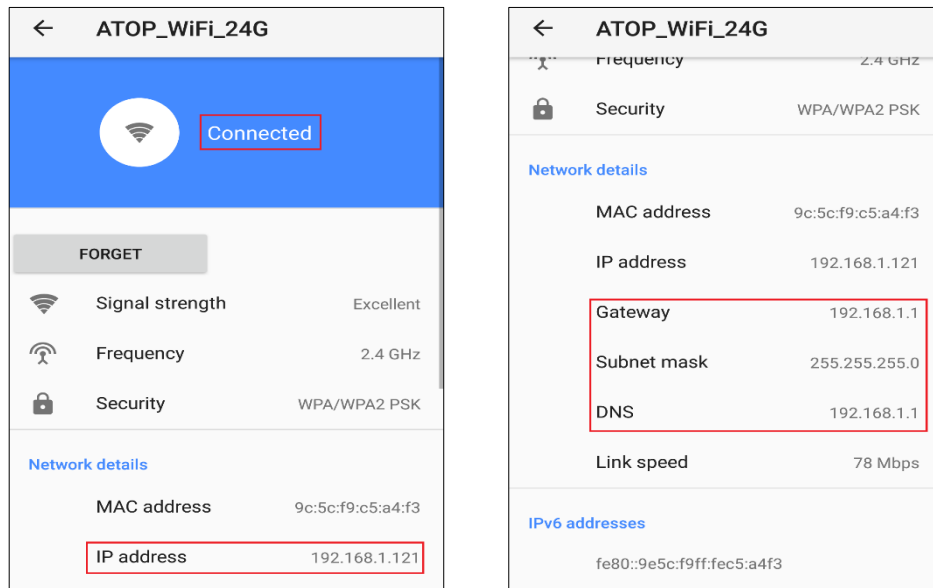
Figure 52. Input Password (Network Key) for WiFi Connection



Step 4: Wi-Fi Connected Information

After Wi-Fi connection is established successfully, push the **SSID** named **ATOP_WiFi_24G** again to enter the connection details screen. As shown in the Figure below, the assigned IPv4 address, subnet mask, gateway, and DNS come from bridged interface (br-lan) of CWR5805 device.

Figure 53. Wi-Fi Connected Information



For the 5 GHz wireless access point connection of an Android mobile phone, repeat Step 1 to Step 4 to establish the Wi-Fi connection but selecting the SSID name of **ATOP_WiFi_5G** for connection.

4.5 Mesh

On the **Whole Home Mesh System** webpage, you can build the mesh network with another CWR5805 device. The mesh network must have at least one Central Access Point (CAP) mode CWR5805 device and one Access Point mode CWR5805 device connecting. These settings can be configured on this webpage for CAP mode and AP mode, respectively.

Figure 54. Network > Mesh > Basic Settings

Mesh Settings

Whole Home Mesh System

Configuration of Whole Home Mesh Features

Basic Settings

Mesh Enable

☒

Mode

Router

SSID

ATOP_CWR

WPA2-PSK Key

Table 37. Network > Mesh > Basic Settings

Field	Value	Description
Mesh Enable	Disable/Enable; default: disable	To enable/disable the mesh feature.
Mode	Router/Satellite; default: Router	Select mesh mode of Central Access Point or Access Point.
SSID	default: ATOP_CWR	The broadcasted SSID of the mesh network. Both CAP mode and AP mode CWR5805 devices must be set to the same ESSID.
WPA2-PSK Key	default: ATOP_CWR	Specifies the encryption key of WPA2-PSK. Both CAP mode and AP mode CWR5805 devices must use the same WPA2-PSK key.

4.6 IPv6

In the **IPv6** webpage, you can manage the IPv6 IP settings. The IPv6 server device’s web GUI and SNMP only.

Figure 55. Network > IPv6

IPv6 WAN settings

Disable

☐

Protocol

Static

IPv6 address

Gateway

Prefix length

DNS server

Table 38. Network > IPv6

Field	Value	Description
Disable	Disable/Enable; default: Enable	Check Disable box to disable IPv6.
Protocol	DHCPv6/Static; default: DHCPv6	The protocol is used by the WAN interface.
IPv6 address	ip6; default: none	Your router's address on the WAN network.
Gateway	ip6; default: none	The IPv6 address gateway of this interface. An interface's gateway is the default next-hop address to access other networks.
Prefix length	integer [1 - 64]; default: none	Like an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address.
DNS server	ip6; default: none	By entering custom DNS servers the router will take care of the hostname resolution. You can enter multiple DNS servers to provide redundancy in case one of the servers fails.

4.7 VLAN

On this page, you can configure your Virtual LAN settings.

4.7.1 Interface Based

Figure 56. Network > VLAN > Interface Based

Table 39. Network > VLAN > Interface Based

Field	Value	Description
VLAN ID	integer [1 - 4094]; default: none	VLAN identification number.
Interface	wan/lan default: wan	Select to which interface will be applied.

4.8 LB (Load Balancing) and Failover (CWR5805 only)

Load balancing (LB) lets user create rules that divide the traffic between different interfaces. In this case, there are the WAN and the Mobile interfaces. The LB mechanism provides the data traffic balancing control between WAN and 5G/LTE connections.

The **Failover** mechanism provides the data traffic redirection to the Mobile port interface while the WAN interface is disconnected, and versa.

4.8.1 Overview

The **Overview** tab contains the Interface Status and Detailed Status sub-tabs which shows the current status info of each configured Multi-WAN interfaces.

Figure 57. Network > LB and Failover > Overview



Table 40. Network > LB and Failover > Overview

Field	Description
wan (eth0)	Current multi-wan status (Online/Offline/Disabled) of the WAN port interface.
mobile (wwan0)	Current multi-wan status (Online/Offline/Disabled) of the mobile interface.

The WAN Interface Syslog (System log) section shows recent Multi-WAN interface log messages.

In the Detailed Status sub-tab, the Multi-WAN interfaces status, configured policies, activated rules, and local connected networks information are displayed.

4.8.2 Configuration

The **Configuration** tab consists of five sub-tabs, which are General, Interfaces, Members, Policies, and rules.

4.8.2.1 General

In **General** sub-tab, the load balancing feature is disabled by default. You can check the Enable field to start the load balancing service.

Figure 58. Network > LB and Failover > Configuration > General



Table 41. Network > LB and Failover > Configuration > General

Field	Value	Description
Enabled	default: disable	Enable/Disable load balancing service.

4.8.2.2 Interfaces

In **Interfaces** sub-tab, you can configure each WAN/Mobile interface under Interfaces section and defines how each WAN/Mobile interface is tested for up/down status. Each interface section must have a name that corresponds with the interface name in you's network configuration.

Figure 59. Network > LB and Failover > Configuration > Interfaces

Interfaces Configuration											
Interfaces											
Interface	Enabled	Tracking IP	Tracking reliability	Ping count	Ping timeout	Ping interval	Interface down	Interface up	Metric	Errors	Sort
wan	Yes	8.8.4.4 8.8.8.8 208.67.222.222 208.67.220.220	2	1	2s	5s	3	8	0		<div> <div></div> <div></div> </div> <div>Edit</div>
mobile	Yes	8.8.8.8 208.67.220.220	1	1	2s	5s	3	8	99		<div> <div></div> <div></div> </div> <div>Edit</div>

Table 42. Network > LB and Failover > Configuration > Interfaces

Field	Description
Interface	The interface name as shown in Network -> Interfaces list (if using a PPPoE interface, the interface name specified here should be the underlying interface name, not the "pppoe-..." interface name).
Enabled	Enable/Disable load balancing service on this interface.
Tracking IP	The hosts to test if the interface is still alive. If this value is missing the interface is always considered up.
Tracking Reliability	A number of tracking IP hosts that must reply for the test to be considered as successful. Ensure that there are at least these many tracking IP hosts defined, or the interface will always be considered down.
Ping Count	The number of checks to send to each host with each test.
Ping Timeout	The number of seconds to wait for an echo-reply after an echo-request.
Ping Interval	The number of seconds between each test.
Interface down	The number of failed tests to considered link as dead.
Interface Up	The number of successful tests to considered link as alive.
Metric	The metric value of this interface.
Sort	To sort the port forward rules. The top classification rule means highest priority.

Figure 60. Network > LB and Failover > Configuration > Interfaces > Edit

Overview **Configuration**

General **Interfaces** Members Policies Rules

Interfaces Configuration - wan

Enabled

Tracking IP

This IP address will be pinged to determine if the link is up or down. Leave blank to assume interface is always online

Tracking reliability

Acceptable values: 1-100. This many Tracking IP addresses must respond for the link to be deemed up

Ping count

Ping timeout

Ping interval

Interface down

Interface will be deemed down after this many failed ping tests

Interface up

Downed interface will be deemed up after this many successful ping tests

Metric

This displays the metric assigned to this interface in /etc/config/network

Table 43. Network > LB and Failover > Configuration > Interfaces > Edit

Field	Value	Description
Enabled*	no/yes; default: no	Enable/Disable load balancing service on this interface.
Tracking IP	ip; default: 8.8.8.8/8.8.4.4	The hosts to test if the interface is still alive. If this value is missing the interface is always considered up.
Tracking Reliability	integer [1 – 100]; default: 1	The number of tracking IP hosts that must reply for the test to be considered as successful. Ensure that there are at least these many tracking IP hosts defined, or the interface will always be considered down.
Ping Count	integer [1 – 5]; default: 1	The number of checks to send to each host with each test.
Ping Timeout	integer [1 – 10]; default: 1	The number of seconds to wait for an echo-reply after an echo-request.
Ping Interval	1/3/5/10/20/30 seconds 1/5/10/15/30 minutes 1 hour default: 2 seconds	The number of seconds between each test.
Interface down	integer [1 – 10]; default: 3	The number of failed tests to considered link as dead.
Interface Up	integer [1 – 10]; default: 8	The number of successful tests to considered link as alive.
Metric	Same as configured	The metric value of this interface.

4.8.2.3 Members

Each member represents an interface with a metric and a weight value. Members are referenced in policies to define a pool of interfaces with corresponding metric and load-balancing weight. Members can not be used for rules directly.

Figure 61. Network > LB and Failover > Configuration > Members

Overview Configuration					
General Interfaces Members Policies Rules					
Members Configuration					
Members					
Member	Interface	Metric	Weight	Sort	
wan_m1_w3	wan	1	3	↑ ↓	Edit Delete
wan_m2_w3	wan	2	3	↑ ↓	Edit Delete
mobile_m1_w2	mobile	1	2	↑ ↓	Edit Delete
mobile_m2_w2	mobile	2	2	↑ ↓	Edit Delete
					Add

Table 44. Network > LB and Failover > Configuration > Members

Field	Description
Member	A name to define this member profile.
Interface	Member applies to this interface (use the same interface name as used in the Interface Configuration section, above).
Metric	Members within one policy with a lower metric have precedence over higher metric members.
Weight	Members with same metric will distribute the load based on this weight value.

Figure 62. Network > LB and Failover > Configuration > Members > Edit

Members Configuration - wan_m1_w4

Interface:

Metric:
 ⓘ Acceptable values: 1-1000. Defaults to 1 if not set

Weight:
 ⓘ Acceptable values: 1-1000. Defaults to 1 if not set

Table 45. Network > LB and Failover > Configuration > Members > Edit

Field	Value	Description
Interface	wan/mobile; default: wan	The VRRP interface.
Metric	integer [1 – 1000]; default: 1	The metric value of this interface. A larger number means higher priority. Used as a sorting measure. If a packet is routed with two rules, the higher metric will be chosen first.
Weight	integer [1 – 1000]; default: 4	A smaller number means lower weight.

4.8.2.4 Policies

Policies define how traffic is routed through different WAN interfaces. Every policy has at least one or more members assigned to it, which defines the policy's traffic behavior. If a policy has a single member, traffic will only go out through that member. If a policy has more than one member, it will either load-balance among members or uses one member as a primary but fail-over to another, depending on how the members are configured.

If there is more than one member assigned to a policy, members within the policy with a lower metric have precedence over higher metric members. Members with the same metric will load-balance. Load-balancing members (with the same metric) will distribute the load based on assigned weight values.

Figure 63. Network > LB and Failover > Configuration > Policies

Overview

Configuration

General

Interfaces

Members

Policies

Rules

Policies Configuration

Policies

Policy	Members assigned	Last resort	Errors	Sort
wan_only	wan_m1_w3	unreachable (reject)	<div><div></div><div></div></div>	<div><div>Edit</div><div>Delete</div></div>
mobile_only	mobile_m1_w2	unreachable (reject)	<div><div></div><div></div></div>	<div><div>Edit</div><div>Delete</div></div>
balanced	wan_m1_w3 mobile_m1_w2	unreachable (reject)	<div><div></div><div></div></div>	<div><div>Edit</div><div>Delete</div></div>
wan_mobile	wan_m1_w3 mobile_m2_w2	unreachable (reject)	<div><div></div><div></div></div>	<div><div>Edit</div><div>Delete</div></div>
mobile_wan	wan_m2_w3 mobile_m1_w2	unreachable (reject)	<div><div></div><div></div></div>	<div><div>Edit</div><div>Delete</div></div>

Add

Table 46. Network > LB and Failover > Configuration > Policies

Field	Description
Policy	A name to define this policy profile.
Member Assigned	Member's name is assigned to this policy.
Last Resort	If a traffic rule matches a policy, but all the members (interfaces) for that policy are down, the exit strategy for that policy will default to "unreachable". Valid values are blackhole, unreachable, or default.

Figure 64. Network > LB and Failover > Configuration > Policies > Edit/Add

Overview	Configuration
General	Interfaces
Members	Policies
Rules	
Policies Configuration - wan_only	
Member used	wan_m1_w4
Last resort	unreachable (reject)
<div> <div>?</div> When all policy members are offline use this behavior for matched traffic </div>	

Table 47. Network > LB and Failover > Configuration > Policies > Edit/Add

Field	Description
Member used	The member assigned to this policy.
Last resort	Determine the fallback routing behavior if all WAN members in the policy are down.

4.8.2.5 Rules

A **rule** describes what traffic to match and what policy to assign for that traffic.

Figure 65. Network > LB and Failover > Configuration > Rules

Rule	Source address	Source port	Destination address	Destination port	Protocol	Sticky	Sticky timeout	IPset	Policy assigned	Errors	Sort
youtube	—	—	—	80,443	tcp	Yes	600s	youtube	balanced		
https	—	—	—	443	tcp	Yes	600s	—	balanced		
default_rule	—	—	0.0.0.0/0	—	all	No	—	—	balanced		

Table 48. Network > LB and Failover > Configuration > Rules

Field	Description
Rule	A name to define this rule profile.
Source Address	Match traffic from the specified source IP address.
Source Port	Match traffic from the specified source port or port range, if the relevant protocol is specified.
Source Address	Match traffic from the specified source IP address.
Source Port	Match traffic from the specified source port or port range, if the relevant protocol is specified.
Dest. Address	Match traffic directed to the specified destination IP address.
Dest. Port	Match traffic directed to the given destination port or port range, if the relevant protocol is specified.
Protocol	Match traffic using the given protocol. Can be one of TCP, UDP, ICMP, or all or it can be a numeric value, representing one of these protocols or a different one.
Sticky	Allow traffic from the same source IP address within the timeout limit to use the same WAN interface as a prior session.
Sticky Timeout	Stickiness timeout value in seconds.

Figure 66. Network > LB and Failover > Configuration > Rules > Edit/Add

Rules Configuration - https

Source address
 ⓘ Supports CIDR notation (eg "192.168.100.0/24") without quotes

Source port
 ⓘ May be entered as a single or multiple port(s) (eg "22" or "80,443") or as a portrange (eg "1024:2048") without quotes

Destination address
 ⓘ Supports CIDR notation (eg "192.168.100.0/24") without quotes

Destination port
 ⓘ May be entered as a single or multiple port(s) (eg "22" or "80,443") or as a portrange (eg "1024:2048") without quotes

Protocol
 ⓘ View the contents of /etc/protocols for protocol descriptions

Sticky
 ⓘ Traffic from the same source IP address that previously matched this rule within the sticky timeout period will use the same WAN interface

Sticky timeout
 ⓘ Seconds. Acceptable values: 1-1000000. Defaults to 600 if not set

IPset
 ⓘ Name of IPset rule. Requires IPset rule in /etc/dnsmasq.conf (eg "ipset=/youtube.com/youtube")

Policy assigned

Table 49. Network > LB and Failover > Configuration > Rules > Edit/Add

Field	Value	Description
Source Address	IP/submask; default: none	Match traffic from the specified source IP address.
Source Port	port; default: none	Match traffic from the specified source port or port range, if the relevant protocol is specified.
Destination Address	IP/submask; default: none	Match traffic directed to the specified destination IP address.
Destination Port	port; default: none	Match traffic directed to the given destination port or port range, if the relevant protocol is specified.
Protocol	TCP/UDP/ICMP; default: TCP	Match traffic using the given protocol. Can be one of TCP, UDP, ICMP, or all or it can be a numeric value, representing one of these protocols or a different one.
Sticky	default: yes	Allow traffic from the same source IP address within the timeout limit to use the same WAN interface as a prior session.
Sticky Timeout	integer [1 - 1000000]; default: 600	Stickiness timeout value in seconds.
IPset	string; default: none	Match traffic directed at the given destination domain name address to an ipset.
Policy assigned	default: balanced	Type of the policy assigned.

4.9 Firewall

The xxR5805 device uses a standard Linux **iptables** package as its firewall, which uses routing chains and policies to facilitate control over inbound and outbound traffic.

4.9.1 General Settings

4.9.1.1 General Configuration

The **General Settings** tab is used to configure the main policies of the xxR5805 device's firewall. The firewall creates zones over network interfaces to control network traffic flow.

The value's explanation of Input, Output, and Forward fields is as below:

- Accept - packet gets to continue down to the next chain.
- Drop - packet is stopped and deleted.
- Reject - packet is stopped, deleted and, and differently from Drop, an ICMP packet containing a message.

Figure 67. Network > Firewall > General Settings

The screenshot shows the 'General Settings' configuration page. At the top, there are four tabs: 'General Settings' (active), 'Port Forwards', 'Traffic Rules', and 'Attack Prevention'. Below the tabs, the title 'General Settings' is displayed in green. Under the 'General Configuration' section, there are two checkboxes: 'Enable SYN-flood protection' which is checked, and 'Drop invalid packets' which is unchecked. Below these are three dropdown menus labeled 'Input', 'Output', and 'Forward'. The 'Input' dropdown is set to 'accept', the 'Output' dropdown is set to 'accept', and the 'Forward' dropdown is set to 'reject'.

Table 50. Network > Firewall > General Settings

Field	Value	Description
Enable SYN-flood Protection	default: enable	To enable/disable SYN-flood protection.
Drop Invalid Packets	default: disable	A "Drop" action is performed on a packet that is determined to be invalid.
Input	default: accept	Action that is to be performed for packets that pass through the Input chain.
Output	default: accept	Action that is to be performed for packets that pass through the Output chain.
Forward	default: reject	Action that is to be performed for packets that pass through the Forward chain.

4.9.1.2 Zones Configuration

Figure 68. Network > Firewall > General Settings > Zone Configuration

Zones Configuration

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: [icon] = wan	accept ▼	accept ▼	accept ▼	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
wan: wan: [icon] mobile: [icon] = REJECT	reject ▼	accept ▼	reject ▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Delete

Add

Table 51. Network > Firewall > General Settings > Zone Configuration

Field	Description
Zone⇒Forwardings	The zone forwarding contains the source zone from which data packets will redirect and the destination zone to which data packets will be redirected.
Input	Action that is to be performed for packets that pass through the Input chain.
Output	Action that is to be performed for packets that pass through the Output chain.
Forward	Action that is to be performed for packets that pass through the Forward chain.
Masquerading	Specifies whether outgoing zone traffic should be masqueraded. This is typically enabled on the WAN zone.
MSS Clamping	To enable/disable MSS clamping for outgoing zone traffic.

4.9.1.2.1 Zones Configuration - Zone "lan"

Choose the firewall zone that you want to assign to the LAN interface or select "unspecified" to remove the LAN interface from the associated zone, or fill out the create field to define a new zone and attach it to the LAN interface.

Figure 69. Network > Firewall > General Settings > Zone Configuration > Zone "Lan"

General Settings Port Forwards Traffic Rules Attack Prevention

Zone Configuration - Zone "lan"

Zone "lan"

This section defines common properties of "lan". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.

General Settings Advanced Settings

Name:

Input:

Output:

Forward:

Masquerading: ☐

MSS clamping: ☐

Covered networks: ☒ lan ☐ mobile ☐ wan ☐ xl2tpd

Table 52. Network > Firewall > General Settings > Zone Configuration > Zone "Lan"

Field	Description
Zone→Forwardings	The zone forwarding contains the source zone from which data packets will redirect and the destination zone to which data packets will be redirected.
Input	Action that is to be performed for packets that pass through the Input chain.
Output	Action that is to be performed for packets that pass through the Output chain.
Forward	Action that is to be performed for packets that pass through the Forward chain.
Masquerading	Specifies whether outgoing zone traffic should be masqueraded. This is typically enabled on the WAN zone.
MSS Clamping	To enable/disable MSS clamping for outgoing zone traffic.

Figure 70. Network > Firewall > General Settings > Zone Configuration > Zone "Lan" > Inter-Zone Forwarding

Inter-Zone Forwarding

The options below control the forwarding policies between this zone (lan) and other zones. *Destination zones* cover forwarded traffic originating from "lan". *Source zones* match forwarded traffic from other zones **targeted at "lan"**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination* zones:

☒

wan: wan: mobile:

Allow forward from *source* zones:

☐

wan: wan: mobile:

4.9.1.2.2 Zone Configuration-WAN

In the Firewall Setting sub-tab of the Network-Interfaces-WAN tab, you can assign a firewall zone to the WAN interface.

Figure 71. Network > Firewall > General Settings > Zone "wan"

General Settings Port Forwards Traffic Rules Attack Prevention

Zone Configuration - Zone "wan"

Zone "wan"

This section defines common properties of "wan". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.

General Settings Advanced Settings

Name

wan

Input

reject

Output

accept

Forward

reject

Masquerading

☒

MSS clamping

☒

Covered networks

☐ lan:

☒ mobile:

☒ wan:

☐ xl2tpd:




Table 53. Network > Firewall > General Settings > Zone “wan” > Inter-Zone Forwarding

Inter-Zone Forwarding

The options below control the forwarding policies between this zone (wan) and other zones. *Destination zones* cover forwarded traffic originating from “wan”. *Source zones* match forwarded traffic from other zones targeted at “wan”. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.




Allow forward to destination zones:

☐

lan: lan:    

Allow forward from source zones:

☒

lan: lan:    

4.9.2 Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN. It is a way of redirecting an incoming connection to another IP address, port, or a combination of both.

Figure 72. Network > Firewall > Port Forwards > Port Forwards Rules

General Settings

Port Forwards

Traffic Rules

Attack Prevention

Port Forwards

Port Forwards Rules

Name	Match	Forward to	Enable	Sort
This section contains no values yet				

New Port Forward Rule

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
New port forward	TCP+UDP	wan		lan		

Add

Table 54. Network > Firewall > Port Forwards > Port Forwards Rules

Field	Description
Name	Name of the port forward rule, used only for easier management purposes.
Match	Display matched conditions of the port forwarding rule.
Forward to	Display the port forward destination info when matched with the conditions.

Table 55. Network > Firewall > Port Forwards > New Port Forwards Rules

Field	Value	Description
Name	-	Name of the port forward rule, used only for easier management purposes.
Protocol	default: TCP+UDP	Type of protocol of the incoming packet.
External Zone	default: wan	The WAN network that data traffic will be redirected from.
External Port	integer [0-65535] range of integers [0-65534] - [1-65535]; default: none	Traffic will be forwarded from this port on the WAN network. The rule will match the source port used by the connecting host with the port number(s) specified in this field. Leave empty to make the rule skip source port matching.
Internal Zone	default: lan	The LAN network that data traffic will be redirected to.
Internal IP Address	-	The IP address of the internal machine that hosts some services that you want to access from the outside.
Internal Port	integer [0-65535] range of integers [0-65534] - [1-65535]; default: none	The rule will redirect the data traffic to this port on the internal machine.

4.9.3 Traffic Rules

The **Traffic Rules** tab contains a more generalized rule definition. You can block or open ports, alter how traffic is forwarded between LAN and WAN, and many other things. Traffic Rules

Figure 73. Network > Firewall > Traffic Rules > Traffic Rules

General Settings **Port Forwards** **Traffic Rules** **Attack Prevention**

Traffic Rules

Traffic Rules

Name	Match	Action	Enable	Sort	
Allow-DHCP-Renew	IPv4-UDP From <i>any host</i> in <i>wan</i> To <i>any router IP</i> at port 68 on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>	<div>↑</div> <div>↓</div>	<div>Edit</div> <div>Delete</div>
Allow-Ping	IPv4-ICMP with type <i>echo-request</i> From <i>any host</i> in <i>wan</i> To <i>any router IP</i> on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>	<div>↑</div> <div>↓</div>	<div>Edit</div> <div>Delete</div>
Allow-IGMP	IPv4-IGMP From <i>any host</i> in <i>wan</i> To <i>any router IP</i> on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>	<div>↑</div> <div>↓</div>	<div>Edit</div> <div>Delete</div>
-	Any IPSEC-ESP From <i>any host</i> in <i>wan</i> To <i>any host</i> in <i>lan</i>	Accept forward	<input checked="" type="checkbox"/>	<div>↑</div> <div>↓</div>	<div>Edit</div> <div>Delete</div>
-	Any UDP From <i>any host</i> in <i>wan</i> To <i>any host</i> , port 500 in <i>lan</i>	Accept forward	<input checked="" type="checkbox"/>	<div>↑</div> <div>↓</div>	<div>Edit</div> <div>Delete</div>
pptp	Any TCP From <i>any host</i> in <i>wan</i> To <i>any router IP</i> at port 1723 on <i>this device</i>	Accept input	<input type="checkbox"/>	<div>↑</div> <div>↓</div>	<div>Edit</div> <div>Delete</div>
gre	Any GRE From <i>any host</i> in <i>wan</i> To <i>any router IP</i> on <i>this device</i>	Accept input	<input type="checkbox"/>	<div>↑</div> <div>↓</div>	<div>Edit</div> <div>Delete</div>
l2tp	Any UDP From <i>any host</i> in <i>wan</i> To <i>any router IP</i> at port 1701 on <i>this device</i>	Accept input	<input type="checkbox"/>	<div>↑</div> <div>↓</div>	<div>Edit</div> <div>Delete</div>

Table 56. Network > Firewall > Traffic Rules > Traffic Rules

Field	Description
Name	Name of the traffic rule, used only for simplified management purposes.
Match	Display matched conditions of the traffic rule.
Action	Action to be performed with the packet if it matches the rule.
Enable	To enable/disable this traffic rule.
Sort	To sort the traffic rules. The top classification rule means the highest priority.
Edit	To configure selected traffic rule.
Delete	To remove selected traffic rule.

4.9.3.1.1 Open Ports on Router

Open Ports on Router rules can open certain ports and redirect hosts connecting to the router from specified zones to specified ports.

Figure 74. Network > Firewall > Traffic Rules > Open ports on router

Table 57. Network > Firewall > Traffic Rules > Open ports on router

Field	Description
Name	Name of the traffic rule, used only for easier management purposes.
Protocol	Specifies to which protocols the rule should apply.
External Port	Specifies which port should be opened.
Add	Add a new open port on the router rule.

4.9.3.1.2 New Forward Rule

New Forward Rules enable you to create custom zone forwarding rules. This is used to create firewall rules that control traffic on the FORWARD chain.

Figure 75. Network > Firewall > Traffic Rules > New forward rule

Table 58. Network > Firewall > Traffic Rules > New forward rule

Field	Description
Name	Name of the traffic rule, used only for easier management purposes.
Source Zone	Match incoming traffic from selected address family only.
Destination Zone	Forward incoming traffic to selected address family only.

4.9.3.1.3 Source NAT

SNAT is a form of masquerading used to change a packet's source address and/or port number to a static, user-defined value. It is performed in the POST ROUTING chain, just before a packet leaves the device. For example, it enables the mapping of multiple WAN addresses to internal subnets.

Figure 76. Network > Firewall > Traffic Rules > Source NAT

Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort
This section contains no values yet				

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port
<input type="text" value="New SNAT rule"/>	<input type="text" value="lan"/>	<input type="text" value="wan"/>	<input type="text" value="-- Please choose --"/>	<input type="text" value="Do not rewrite"/>

Table 59. Network > Firewall > Traffic Rules > Source NAT

Field	Description
Name	Name of the traffic rule, used only for easier management purposes.
Source Zone	Match incoming traffic from selected address family only.
Destination Zone	Forward incoming traffic to selected address family only.
To Source IP	Match incoming traffic from the specified source IP address.
To Source Port	Match incoming traffic originating from the given source port or port range on the client host.

4.9.4 Attack Prevention

4.9.4.1 SYN Flood Protection

SYN Flood Protection allows you to protect your router from attacks that exploit part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive. Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation.

Figure 77. Network > Firewall > Attack Prevention > SYN Flood Protection

General Settings **Port Forwards** **Traffic Rules** **Attack Prevention**

Attack Prevention

SYN Flood Protection

Enable ☒

SYN flood rate
 Range of the value must be from 1 to 10000

SYN flood burst
 Range of the value must be from 1 to 10000

TCP SYN cookies ☒

Table 60. Network > Firewall > Attack Prevention > SYN Flood Protection

Field	Value	Description
Enable	default: enable	Makes the router more resistant to SYN flood attacks.
SYN flood rate	integer [1 to 10000]; default: 25	Set rate limit (packets/second) for SYN packets above which the traffic is considered flooding.
SYN flood burst	integer [1 to 10000]; default: 50	Set burst limit for SYN packets above which the traffic is considered flooded if it exceeds the allowed rate.
TCP SYN cookies	default: enable	Enable the use of SYN cookies (particular choices of initial TCP sequence numbers by TCP servers).

4.9.4.2 SSH Attack Prevention

SSH Attack Prevention allows you to run commands on a machine's command prompt without them being physically present near the machine and attacks by limiting connections in a defined period.

Figure 78. Network > Firewall > Attack Prevention > SSH Attack Protection

SSH Attack Prevention

Enable ☒

Limit period

Second

Limit period

5

Range of the value must be from 1 to 10000

Limit burst

10

Range of the value must be from 1 to 10000

Table 61. Network > Firewall > Attack Prevention > SSH Attack Protection

Field	Value	Description
Enable	default: enable	Enable SSH connections to limit in the selected period.
Limit period	Second/Minute/Hour/Day; default: Second	Select in what period limit SSH connections.
Limit	integer [1 to 10000]; default: 5	Maximum SSH connections during the period.
Limit burst	integer [1 to 10000]; default: 10	Indicating the maximum burst before the above limit kicks in.

4.9.4.3 Http/Https Attack Prevention

HTTP attacks send a complete, legitimate HTTP header, which includes a 'Content-Length' field to specify the size of the message body to follow. However, the attacker then proceeds to send the actual message body at an extremely slow rate (i.e. 1 byte/110 seconds). Due to the entire message being correct and complete, the target server will attempt to obey the 'Content-Length' field in the header, and wait for the entire body of the message to be transmitted, hence slowing it down.

Figure 79. Network > Firewall > Attack Prevention > Http/Https Attack Protection

Http/Https Attack Prevention

Enable ☒

Limit period

Limit period
 Range of the value must be from 1 to 10000

Limit burst
 Range of the value must be from 1 to 10000

Table 62. Network > Firewall > Attack Prevention > Http/Https Attack Protection

Field	Value	Description
Enable	default: enable	Enable HTTP connections to limit in the selected period.
Limit period	Second/Minute/Hour/Day; default: Second	Select in what period limit HTTP connections.
Limit	integer [1 to 10000]; default: 5	Maximum HTTP connections during the period.
Limit burst	integer [1 to 10000]; default: 10	Indicating the maximum burst before the above limit kicks in.

4.9.4.4 Port Scan

Port Scan attacks scan which of the targeted host's ports are open. Network ports are the entry points to a machine that is connected to the Internet. A service that listens on a port can receive data from a client application, process it and send a response back. Malicious clients can sometimes exploit vulnerabilities in the server code so they gain access to sensitive data or execute malicious code on the machine remotely.

Port scanning is usually done in the initial phase of a penetration test in order to discover all network entry points into the target system. The Port Scan section provides you with the possibility to enable protection against port scanning software. The Defending Type section provides the possibility for the user to enable protections from certain types of online attacks. These include **SYN-FIN**, **SYN-RST**, **X-Mas**, **FIN scan** and **NULLflags** attacks.

Figure 80. Network > Firewall > Attack Prevention > Port Scan

Port Scan

Enable ☒

Scan count
 ⓘ Range of the value must be from 5 to 10000

Interval
 ⓘ Range of the value must be from 10 to 1000

SYN-FIN attack ☒

SYN-RST attack ☒

X-Mas attack ☒

FIN scan ☒

NULL flags attack ☒

Table 63. Network > Firewall > Attack Prevention > Port Scan

Field	Value	Description
Enable	default: enable	Enable port scan prevention.
Scan count	integer [5 to 10000]; Default: none	The numbers port of scanned before blocked.
Interval	integer [10 to 1000]; default: 10	Time interval in seconds counting the length of the scan (10 – 60 sec).
SYN-FIN attack	default: enable	Protect from SYN-FIN attack.
SYN-RST attack	default: enable	Protect from SYN-RST attack.
X-Mas attack	default: enable	Protect from X-Mas attack.
FIN scan	default: enable	Protect from FIN scan.
NULL flags attack	default: enable	Protect from NULLflags attack.

4.10 Static Routes

Static routes specify over which interface and gateway a certain host or network can be reached. You can configure the custom routes in this webpage.

Figure 81. Network > Static Routes

Static Routes

Static IPv4 Routes

Interface	Target	IPv4 Netmask	IPv4 Gateway	Metric	MTU	
Host IP or Network		if target is a network				
lan	192.168.1.2	255.255.255.0	10.0.50.254	10	1500	Delete
Add						

Table 64. Network > Static Routes

Field	Description
Interface	Interface which will be used for the route in IPv4 routing table.
Target	The IP address of the destination network or host.
IPv4 Netmask	A subnet mask that is applied to the Target field to determine to what actual IP addresses the routing rule applies.
IPv4 Gateway	Defines where the xxR5805 device should send all the traffic that applies to the rule.
Metric	The Metric value is used as a sorting measure. If a packet about to be routed fits two rules, the one with the lower metric is applied.
MTU	Specifies the largest possible size of a data packet.
Delete	To remove selected static IPv4 route entry.
Add	To add a new static IPv4 route entry.

4.11 DNS

The DNS page is used to set up the how the device utilized its own and other DNS servers.

Figure 82. Network > DNS

Table 65. Network > DNS

Field	Value	Description
Log queries	enable/disable; default: disable	When enabled, write received DNS requests to syslog.
DNS server	default: none	List of DNS servers to forward requests to.
Rebind protection	enable/disable; default: enable	Discard upstream RFC1918 responses. When enabled, the device will not resolve domain names for internal hosts.
Local Service Only	enable/disable; default: enable	Limit DNS service to subnets and interfaces on which this device is serving as a DNS server.
Listen Interfaces	LAN/WAN; default: none	Limits listening for DNS queries to interfaces specified in the field and loopback. Leave empty to listen on all interfaces.
Filter private	enable/disable; default: enable	Do not forward reverse lookups for local networks.
Localise queries	enable/disable; default: enable	Localise hostname depending on the requesting subnet if multiple IPs are available.

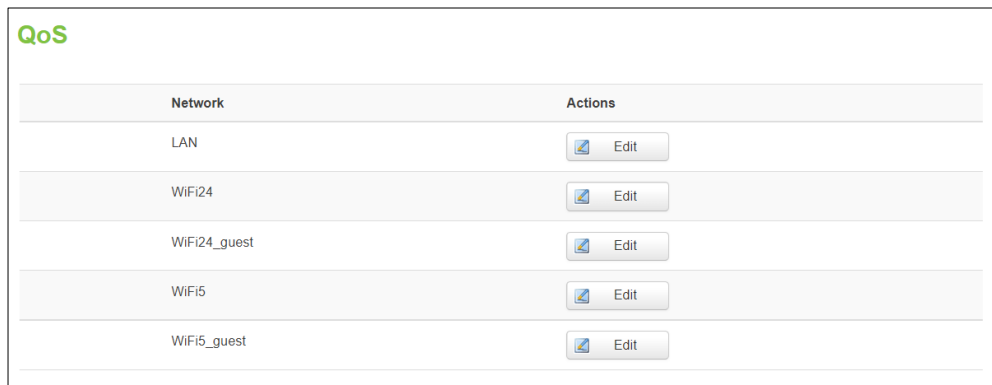
Size of DNS query cache	Integer [0 to 10000]; default: none	Number of cached DNS entries. Set to 0 for no caching.
-------------------------	--	--

4.12 QoS

The **QoS (Quality of Service)** page is used to set up Smart Queue Management (SQM) instances which can limit the download and upload speeds of selected network interfaces.

This manual page provides an overview of the QoS windows.

Figure 83. Network > QoS



Network	Actions
LAN	Edit
WiFi24	Edit
WiFi24_guest	Edit
WiFi5	Edit
WiFi5_guest	Edit

Figure 84. Network > QoS > QoS-LAN Settings



QoS-LAN

QoS-LAN Settings

Enable Total Bandwidth ☐

Download (kbps/s)

Upload (kbps/s)

Enable User Bandwidth ☐

Download (kbps/s)

Upload (kbps/s)

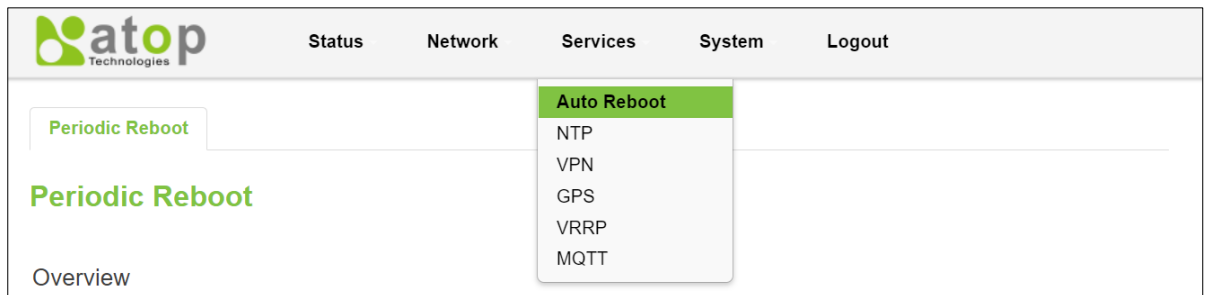
Table 66. Network > QoS > QoS-LAN Settings

Field	Value	Description
Enable Total Bandwidth	disable/enable; Default: disable	Overall Speed limits for all LANs.
Download (kbps/s)	integer [0 - 1000000]; default: 30000	Limits the download speed (ingress) of the selected interface to the value specified in this field.
Upload (kbps/s)	integer [0 - 1000000]; default: 30000	Limits the upload speed (egress) of the selected interface to the value specified in this field.
Enable User Bandwidth	disable/enable; Default: disable	Speed limits for each user.
Download (kbps/s)	integer [0 - 1000000]; default: 30000	Limits the download speed (ingress) of the selected interface to the value specified in this field.
Upload (kbps/s)	integer [0 - 1000000]; default: 30000	Limits the upload speed (egress) of the selected interface to the value specified in this field.

5 Services Menu

The **Services** menu as shown in the Figure below consists of the following sub-menus: Auto Reboot, NTP, VPN, GPS, VRRP and MQTT.

Figure 85. Service

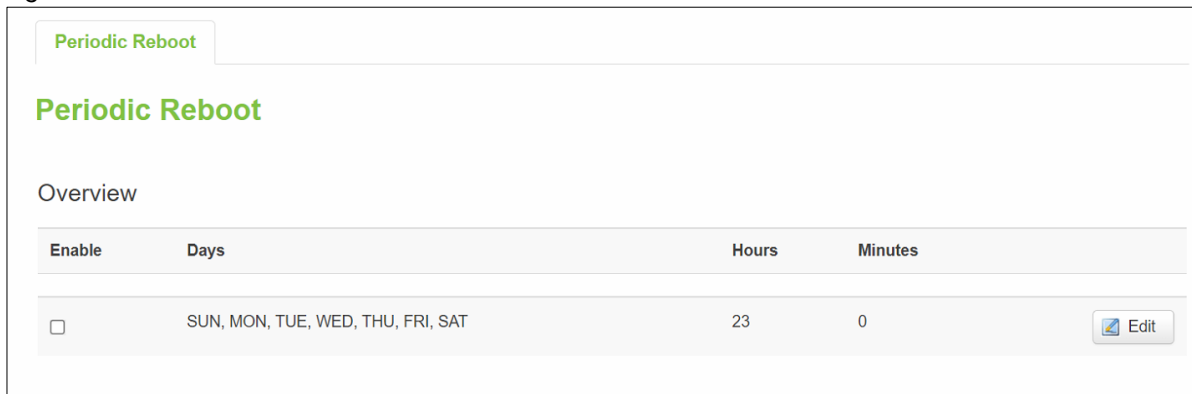


5.1 Auto Reboot

Various automatic device reboot scenarios can be configured in the **Auto Reboot** section. Automatic reboots can be used as a prophylactic or precautionary measure that ensures the device will self-correct some unexpected issues, especially related to connection downtime.

The **Periodic Reboot** is a function that reboots the device at a specified time interval regardless of other circumstances. It can be used as a prophylactic measure, for example, to reboot the device once at the end of every Monday.

Figure 86. Service > Auto Reboot



5.1.1 Periodic Reboot - Configuration

Figure 87. Service > Auto Reboot > Edit

Periodic Reboot

Enable ☐ [Enable periodic reboot feature](#)

Days ☒ Sunday
☒ Monday
☒ Tuesday
☒ Wednesday
☒ Thursday
☒ Friday
☒ Saturday

[Periodic reboot will be performed on selected days](#)

Hours
[Periodic reboot will be performed at this hour. Range \[0 - 23\]](#)

Minutes
[Periodic reboot will be performed at this minute. Range \[0 - 59\]](#)

Table 67. Service > Auto Reboot > Edit

Field	Value	Description
Enable	default: disable	This check box will enable or disable Periodic reboot feature.
Days	SUN/MON/TUE/WED/THU/FRI/SAT; default: SUN/MON/TUE/WED/THU/FRI/SAT	Uploading will be done on that specific time of the day.
Hours	integer [0 – 23] hours; default: 23	Uploading will be done on that specific time of the hours.
Minutes	integer [0 – 59] minutes; default: 0	Uploading will be done on that specific time of the minutes.

5.2 Time

5.2.1 General Section

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

You synchronize the time values of xxR5805 device in the **General** section within NTP sub-menu. These time settings include an update interval (in seconds) and count of time measurements.

Figure 88. Services > Time > General

Time

General

Current system time

2023-07-06 10:12:10

Timezone

UTC

Synchronization

NTP

Update interval (in seconds)

600

Count of time measurements

empty = infinite

Table 68. Services > NTP > General

Field	Value	Description
Time zone	default: UTC	Time zone of your country.
Synchronization	NTP/GPS default: NTP	System time synchronization with time server using NTP (Network Time Protocol) or GPS.
Update Interval (in seconds)	default: 600	Frequency that the NTP client service on xxR5805 device will update the time.
Count of Time Measurements	default: empty	The amount of times that NTP client service on xxR5805 device will perform time synchronizations. Leave it empty if set to infinite.

5.2.2 Time Servers

The NTP servers used by the xxR5805 device is displayed in the **Time Servers** section within **Time Synchronisation** sub-menu.

Figure 89. Services > NTP > Time Servers

Time Servers

Hostname

Port

time.nist.gov

123

Delete

Add

Table 69. Services > NTP > Time Servers

Field	Value	Description
Hostname	string [1 - 253] default: time.nist.gov	Hostname of NTP server
Port	integer [1 - 65535] default: 123	Port number that the NTP server is listening on

5.3 VPN

Virtual Private Network (VPN) is a method to connect multiple private networks across the Internet. VPNs can be used to achieve many different goals, but its main purpose are for: device accessibility among the remote private networks, data encryption and anonymity when browsing the Internet.

5.3.1 OpenVPN

OpenVPN that implements VPN techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It is often regarded as being the most universal VPN protocol because of its flexibility, support of SSL/TLS security, multiple encryption methods, many networking features.

5.3.1.1 Overview

In the **OpenVPN** sub-menu within the **Service** menu, two OpenVPN instances are already created by default, as shown in the figure below. It is referred to as "sample_server" and "sample_client", respectively. These two instances are editable as it is not yet operational by default.

Figure 90. Services > VPN > OpenVPN > Overview

OpenVPN				
Overview				
	Enabled	Started	Port	Protocol
sample_server	<input type="checkbox"/>	no	1194	udp
sample_client	<input type="checkbox"/>	no	1194	udp

Table 70. Services > VPN > OpenVPN > Overview

Field	Description
Enabled	To enable/disable selected OpenVPN service instance.
Started	Display current OpenVPN service is started or not.
Port	Display port number the OpenVPN service listening on.
Protocol	Display TCP/UDP protocol the OpenVPN service used.
Edit	To configure selected OpenVPN service instance.
Start/Stop	To start/stop selected OpenVPN service.

5.3.1.2 OpenVPN Server

If you click “**Edit**” button to edit OpenVPN instance, the editing webpage which contains the OpenVPN instance’s configuration is initialized. The Figure below shows the edit webpage of the default OpenVPN server instance called “sample_server”. Note that the edit webpage here is for basic setting.

Figure 91. Services > VPN > OpenVPN > sample_server > Edit

Overview » Instance "sample_server"

Enable
☐

TUN/TAP

TUN (Tunnel) ▼

Protocol

UDP ▼

Port

1194

LZO

Adaptive ▼

Authentication

TLS ▼

Encryption

BF-CBC ▼

Route traffic between clients
☐

Push option

Keepalive interval

10

Keepalive timeout

60

HMAC algorithm

SHA1 ▼

Certificate authority

Choose File

 No file chosen

Server certificate

Choose File

 No file chosen

Server key

Choose File

 No file chosen

Diffie Hellman parameters

Choose File

 No file chosen

CRL file (optional)

Choose File

 No file chosen

Clients Setting

Common Name	LAN Network	Netmask	To Server LAN Side
This section contains no values yet			

Add

Table 71. Services > VPN > OpenVPN > sample_server > Edit

Field	Value	Description
Instance "sample_server"		
Enable	Enable/Disable; default: Disable	Switches configuration enable or disable. This must be selected to make configuration active.
TUN/TAP	TUN (Tunnel) TAP (Bridged); default: TUN (Tunnel)	Virtual network device type. <ul style="list-style-type: none"> TUN - a virtual point-to-point IP link which operates at the network layer (OSI layer 3), used when routing is required. TAP - a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.
Protocol	UDP/TCP; default: UDP	Transfer protocol used by the OpenVPN connection. <ul style="list-style-type: none"> User Datagram Protocol (UDP) - packets are sent to the recipient without error-checking or back-and-forth quality control, meaning that when packets are lost, they are gone forever. This makes it less reliable but faster than TCP; therefore, it should be used when transfer speed is crucial (for example, in video streaming, live calls). Transmission Control Protocol (TCP) - most commonly used protocol in the Internet Protocol (IP) suite. It ensures the recipient will receive packets in the order they were sent by numbering, analysing response messages, checking for errors and resending them if an issue occurs. It should be used when reliability is crucial (for example, in file transfer).
Port	integer [1-65535] default: 1194	TCP/UDP port number used for the connection. Make sure it matches the port number specified on the server side. NOTE: traffic on the selected port will be automatically allowed in the device firewall rules.
LZO	Adaptive/Yes/No; default: Adaptive	LZO data compression mode.
Authentication	TLS/Static Key; default: TLS	Authentication mode, used to secure data sessions. <ul style="list-style-type: none"> TLS authentication mode uses X.509 type certificates: <ul style="list-style-type: none"> Certificate Authority (CA) Server certificate Server key Diffie Hellman parameters CRL file (optional) <p>All mentioned certificates can be generated using OpenVPN or Open SSL utilities on any type of host machine. One of the most popular utilities used for this purpose is called Easy-RSA.</p> <ul style="list-style-type: none"> Static key is a secret key used for server-client authentication.

Encryption	BF-CBC/AES-128-CBC/AES-192-CBC/AES-256-CBC/AES-128-GCM/AES-192-GCM /AES-256-GCM /none; default: BF-CBC	Algorithm used for packet encryption.
Route traffic between clients	enable/disable; default: disable	Allows OpenVPN clients to communicate with each other on the VPN network.
Push option	default: none	Push options are a way to "push" routes and other additional OpenVPN options to connecting clients.
Keepalive interval	integer [1 to 60]; default: 10	Frequency (in seconds) at which "keep alive" packets are sent to the remote instance. If no response is received, the device will attempt to re-establish the tunnel.
Keepalive timeout	integer [10 to 180]; default: 60	Time in seconds. If no packets pass through the tunnel between this server and a client, the server will terminate the connection to that client after the amount of time specified in this field passes.
Virtual Network and Netmask	default: none	This field specifies the tunnel's virtual IP and netmask.
HMAC algorithm	SHA1 SHA512 SHA384 SHA256 SHA224 MD5 None; default: SHA256	HMAC authentication algorithm type.
Certificate authority	.ca file; default: none	Certificate authority is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
Server certificate	.crt file; default: none	A type of digital certificate that is used to identify the OpenVPN server.
Serve key	.key file; default: none	Authenticates clients to the server.
Diffie Helman parameters	.pem file; default: none	DH parameters define how OpenSSL performs the Diffie-Hellman (DH) key-exchange.
CRL file (optional)	.pem file .crl file; default: none	A certificate revocation list (CRL) file is a list of certificates that have been revoked by the certificate authority (CA). It indicates which certificates are no longer accepted by the CA and therefore cannot be authenticated to the server.
Clients Setting		
Common Name	string; default: none	Client's Common Name (CN) found in the client certificate file.
LAN Network	ip; default: none	Client's private network (LAN) IP address.
Netmask	netmask; default: none	Client's private network (LAN) IP netmask.
To Server LAN Side	default: disable	Enable LAN to LAN function

5.3.1.3 OpenVPN Client

Figure 92. Services > VPN > OpenVPN > sample_client > Edit

Overview » Instance "sample_client"

Enable

☐

TUN/TAP

TUN (Tunnel) ▾

Protocol

UDP ▾

Port

1194

LZO

Adaptive ▾

Authentication

TLS ▾

Encryption

BF-CBC ▾

Remote host/IP address

my_server_1 1194

Keepalive interval

10

Keepalive timeout

60

HMAC algorithm

SHA1 ▾

Certificate authority

Choose File

No file chosen

Client certificate

Choose File

No file chosen

Client key

Choose File

No file chosen

Table 72. Services > VPN > OpenVPN > sample_client > Edit

Field	Value	Description
Enable	enable/disable; default: disable	Switches configuration enable or disable. This must be selected to make configuration active.
TUN/TAP	TUN (Tunnel) TAP (Bridged); default: TUN (Tunnel)	Virtual network device type. <ul style="list-style-type: none"> • TUN - a virtual point-to-point IP link which operates at the network layer (OSI layer 3), used when routing is required. • TAP - a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.
Protocol	UDP/TCP; default: UDP	Transfer protocol used by the OpenVPN connection. <ul style="list-style-type: none"> • User Datagram Protocol (UDP) - packets are sent to the recipient without error-checking or back-and-forth quality control, meaning that when packets are lost, they are gone forever. This makes it less reliable but faster than TCP; therefore, it should be used when transfer speed is crucial (for example, in video streaming, live calls). • Transmission Control Protocol (TCP) - most commonly used protocol in the Internet Protocol (IP) suite. It ensures the recipient will receive packets in the order they were sent by numbering, analysing response messages, checking for errors and resending them if an issue occurs. It should be used when reliability is crucial (for example, in file transfer).
Port	integer [1-65535] default: 1194	TCP/UDP port the local OpenVPN server listening on. TCP/UDP port number used for the connection. Make sure it matches the port number specified on the server side. NOTE: traffic on the selected port will be automatically allowed in the device firewall rules.
LZO	Adaptive/Yes/No; default: Adaptive	LZO data compression mode.
Authentication	TLS/Static Key; default: TLS	Authentication mode, used to secure data sessions. <ul style="list-style-type: none"> • TLS authentication mode uses X.509 type certificates: <ul style="list-style-type: none"> • Certificate Authority (CA) • Client certificate • Client key <p>All mentioned certificates can be generated using OpenVPN or Open SSL utilities on any type of host machine. One of the most popular utilities used for this purpose is called Easy-RSA.</p> • Static key is a secret key used for server–client authentication.

Encryption	BF-CBC/AES-128-CBC/AES-192-CBC/AES-256-CBC/ AES-128-GCM/AES-192-GCM /AES-256-GCM /none; default: BF-CBC	Algorithm used for packet encryption.
Rremote host/IP address	ip, netmask; default: my_server_1 1194	LAN IP address and LAN IP subnet of the remote network (server).
Keepalive interval	integer [1 to 60]; default: 10	Frequency (in seconds) at which "keep alive" packets are sent to the remote instance.
Keepalive timeout	integer [10 to 180]; default: 60	Time in seconds. If no packets pass through the tunnel between this server and a client, the server will terminate the connection to that client after the amount of time specified in this field passes.
Authentication algorithm	SHA1/SHA512SH A384/SHA256/SH A224/MD5/None; default: SHA256	The authentication algorithm must match with another incoming connection.
Certificate authority	.ca file; default: none	Certificate authority is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
Client certificate	.crt file; default: none	Client certificate is a type of digital certificate that is used by client systems to make authenticated requests to a remote server. Client certificates play a key role in many mutual authentication designs, providing strong assurances of a requester's identity.
Client key	.key file; default: none	Authenticates the client to the server and establishes precisely who they are.

5.3.2 IPSec

Internet Protocol Security (IPsec) is a secure network protocol suite of IPv4 that authenticates and encrypts the packets of data sent over an IP Protocol network. It is used in virtual private networks (VPNs). IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks.

5.3.2.1 IPSec – Settings

Figure 93 Services > VPN > IPSec > Settings

Settings


Status


General

Enable ☐

Remote host

Connection type Tunnel ▼

Local subnet/mask 
e.g. 192.168.1.0/24


Remote subnet/mask 
e.g. 192.168.2.0/24

Local protocol port(Optional)
e.g. tcp, tcp/1500, gre

Remote protocol port(Optional)
e.g. tcp, tcp/1500, gre

Authentication

Method Pre-shared key ▼

Pre-shared key 
Key should be in 8-63 characters

Local identifier(Optional)
Under x509: if string clude '=' or ' ', please add '"'. e.g. "CN=CWR_Server"

Remote identifier(Optional)
Under x509: if string clude '=' or ' ', please add '"'. e.g. "CN=CWR_Server"

Phase 1 proposal


Mode	<input type="text" value="Main"/>
Key exchange protocol	<input type="text" value="IKEv1"/>
Encryption algorithm	<input type="text" value="AES 128"/>
Hash algorithm	<input type="text" value="SHA 1"/>
DH group	<input type="text" value="MODP 1024"/>

Phase 2 proposal



Security protocol	<input type="text" value="ESP"/>
Encryption method	<input type="text" value="AES 128"/>
Hash algorithm	<input type="text" value="SHA 1"/>
PFS DH group	<input type="text" value="MODP 1024"/>

Life time

Phase 1 IKE lifetime	<input type="text" value="10800"/>
----------------------	------------------------------------

 180-86400 seconds

Dead Peer Detection

Action	<input type="text" value="None"/>
Interval	<input type="text" value="30"/>
	 30-3600 second
Timeout	<input type="text" value="60"/>
	 Multiples of 10 seconds. eg:60

IPSEC enhancement

Enable ☒

Table 73 Services > VPN > IPSec > Settings

Field	Value	Description
General		
Enable	default: disable	Check the box to enable the IPSec function.
Remote host	default: none	WAN IP address of the Server blank
Connection type	Tunnel Transport; Default: Tunnel	Two distinct modes of IPsec operation
Local subnet/mask	default: 192.168.1.0/24	(only for tunnel mode) LAN IP address/Subnet mask of the router on which the IPSec instance is configured
Remote subnet/mask (only for tunnel mode)	default: 192.168.2.0/24	(only for tunnel mode) LAN IP address/Subnet mask of the opposite router
Protocol over IPSEC	None GRE L2TP; default: None	(only for transport mode) Only the selected protocol can be encrypted in IPSec tunnel.
Local protocol port(Optional)	default: tcp/1500	Only the selected protocol or port can be encrypted it.
Remote protocol port(Optional)	default: tcp/1500	Only the selected protocol or port can be encrypted it.
Authentication		
Method	Pre-shared key X.509; default: Pre-shared key	Specify authentication method. Choose between Pre-shared key and X.509 certificates. <ul style="list-style-type: none"> Pre-shared key - A shared password used for authentication between the peers. The value of this field must match on both instances X.509 - An X.509 certificate binds an identity to a public key using a digital signature. When a certificate is signed by a trusted certificate authority, or validated by other means, the other device holding that certificate can use the public key it contains to establish secure communications.
Pre-shared key	default: a2\$&9eX^	Key should be in 8-63 characters
Local identifier (Optional)	default: none	Defines which protocol and port can be encrypted in IPSec on local side.
Remote identifier (Optional)	default: none	Defines which protocol and port can be encrypted in IPSec on remote side.

Field	Value	Description
Phase 1 proposal		
Mode	Main Aggressive; default: Main	Choose the mode for outgoing connections. <ul style="list-style-type: none"> • Main mode - (a total of 6 messages) by storing most data into the first exchange. • Aggressive mode - performs fewer exchanges (a total of 4 messages) than
Key exchange protocol	IKEv1 IKEv2; default: IKEv1	Internet Key Exchange (IKE) version used for key exchange. <ul style="list-style-type: none"> • IKEv1 - more commonly used but contains known issues, for example, dealing with NAT. • IKEv2 - updated version with increased and improved capabilities, such as integrated NAT support, supported multihosting, deprecated exchange modes (does not use main or aggressive mode; only 4 messages required to establish a connection).
Encryption algorithm	3DES AES 128 AES 192 AES 256 AES128 GCM8 AES192 GCM8 AES256 GCM8 AES128 GCM12 AES192 GCM12 AES256 GCM12 AES128 GCM16 AES192 GCM16 AES256 GCM16; default: AES 128	Algorithm used for data encryption.
Hash algorithm	D5 SHA1 SHA256 SHA384 SHA512; default: SHA256	Algorithm used for exchanging authentication and hash information.
DH group	MODP768 MODP1024 MODP1536 MODP2048 MODP3072 MODP4096 MODP6144 MODP8192 ECP192 ECP224 ECP256 ECP384 ECP521 No PFS; default: MODP1536	Diffie-Hellman (DH) group used in the key exchange process. Higher group numbers provide more security, but take longer and use more resources to compute the key. Must match with another incoming connection to establish IPsec.

Field	Value	Description
Phase 2 proposal		
Security protocol	ESP AH; default: ESP	<ul style="list-style-type: none"> • ESP protocol - provides data confidentiality (encryption) and authentication (data integrity, data origin authentication, and replay protection). • AH - provides a mechanism for authentication only.
Encryption method	3DES AES 128 AES 192 AES 256 AES128 GCM8 AES192 GCM8 AES256 GCM8 AES128 GCM12 AES192 GCM12 AES256 GCM12 AES128 GCM16 AES192 GCM16 AES256 GCM16; default: AES 128	Algorithm used for data encryption.
Hash algorithm	MD5 SHA1 SHA256 SHA384 SHA512; default: SHA256	Algorithm used for exchanging authentication and hash information.
PFS DH group	None MODP768 MODP1024 MODP1536 MODP2048 MODP3072 MODP4096 MODP6144 MODP8192 ECP192 ECP224 ECP256 ECP384 ECP521; default: MODP1536	The PFS (Perfect Forward Secrecy). Must match with another incoming connection to establish IPsec.
Life time		
Phase 1 IKE lifetime	180-86400 seconds; default: 10800	How long the keying channel of a connection (ISAKMP or IKE SA) should last before being renegotiated. The time is specified in seconds.
Phase 2 SA lifetime	180-86400 seconds; default: 3600	How long the keying channel of a connection (ISAKMP or IKE SA) should last before being renegotiated. The time is specified in seconds.
Dead Peer Detection		
Action	None Clear Hold Restart ; default: None	Controls the use of the Dead Peer Detection protocol where notification messages are periodically sent in order to check the liveness of the IPsec peer.
Interval	30-3600 seconds; default: 30	The frequency of sending messages or INFORMATIONAL exchanges to peer.
Timeout	default: 60	Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity.
IPSEC enhancement		
Enable	default: Enable	Check the box to enhance the IPsec function.

5.3.2.2 IPsec – Status

Figure 94 Services > VPN > IPsec > Status

The screenshot shows the 'Status' tab of the IPsec configuration page. It features a table with columns for 'Peer Address', 'VPN Tunnel', and 'Status'. The table is currently empty, displaying 'No information available'. Below the table, there are three buttons: 'Restart' (with a green refresh icon), 'Stop' (with a red stop icon), and 'Refresh' (with a green refresh icon).

Table 74 Services > VPN > IPsec > Status

Field	Description
Peer address	The IP address of the device from which the VPN terminate.
VPN Tunnel	The local subnet/mask and the remote subnet/mask.
Status	Established time.
Restart	Restart the tunnel.
Stop	Stop the tunnel.
Refresh	Refresh the status.

5.3.3 L2TP

Layer 2 Tunneling Protocol (L2TP) is a tunnelling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

5.3.3.1 L2TP Overview

Figure 95. Services > VPN > L2TP > Overview

The screenshot shows the 'L2TP Overview' page. It contains a table with the following data:

Name	Type	Enable
Xl2tpsvr	Server	<input type="checkbox"/>

Below the table, there are controls for adding new configurations: a 'Role' dropdown menu currently set to 'Client', a text input field for 'New configuration name:', and an 'Add New' button.

5.3.3.2 L2TP Server

Allows setting up a L2TP server or client. Below is L2TP server configuration example.

As mentioned in the prerequisites section, the router that acts as the **server** must have a Public Static or Public Dynamic IP address.

Figure 96. Services > VPN > L2TP > Xl2tpsvr > Edit

L2TP Server Instance: Xl2tpsvr

Main Settings

Enable ☐ ☒ Enable current configuration

Local IP
 ⓘ Server IP address, e.g. 192.168.0.1

Remote IP range begin
 ⓘ IP address leases begin, e.g. 192.168.0.20

Remote IP range end
 ⓘ IP address leases end, e.g. 192.168.0.30, but < 256

User name	Password	L2TP Client's IP
The user name for authorization with the server	The password for authorization with the server. Allowed characters (a-zA-Z0-9!@#%&*+./=:?^_`{ }~.)	This virtual IP will be given to L2TP client. For auto assignment leave empty
<input type="text" value="youruser"/>	<input type="password" value="*****"/> ⓘ	<input type="text"/>
		<input type="button" value="Delete"/>
<input type="button" value="Add"/>		

The description of each field is shown in the table below.

Table 75. Services > VPN > L2TP > Xl2tpsvr > Edit

Field	Value	Description
Enable	default: disable	Check the box to enable the L2TP Tunnel function.
Local IP	default: 192.168.0.1	IP Address of this device.
Remote IP range begin	default: 192.168.0.20	IP address leases beginning.
Remote IP range end	default: 192.168.0.30	IP address leases end.
Username	default: youruser	Username to connect to L2TP (this) server.
Password	default: yourpass	Password to connect to L2TP server.
L2TP Client's IP	default: none	This virtual IP will be given to L2TP client. For auto assignment leave empty.

5.3.3.3 L2TP Client

The description of each field is shown in the table below.

Figure 97. Services > VPN > L2TP > Overview

L2TP

Overview

Name	Type	Enable	
Xl2tpsvr	Server	<input type="checkbox"/>	Edit Delete
Xl2tpClient	Client	<input type="checkbox"/>	Edit Delete

Role: Client ▼ New configuration name: Add New

Figure 98. Services > VPN > L2TP > Xl2tpClient > Edit

L2TP Client Instance: Xl2tpClient

Main Settings

Enable ☐ Check the box to enable the L2TP client

Server Specifies the server IP address or a hostname

Username Specifies authorization username

Password Specifies authorization password. Allowed characters (a-zA-Z0-9!@#\$%&*+./=:?^_`{|}~.-)

Authentication L2TP tunnel authentication password.

Keep alive Send LCP echo requests to server. Interval in seconds

Default route ☐ Check the box to set the L2PT tunnel as default route

Use this option when multiwan is off

Table 76. Services > VPN > L2TP > Xl2tpClient > Edit

Field	Value	Description
Enable	default: disable	Check the box to enable the L2TP Tunnel function.
Server	IP/hostname; default: none	Specifies the server IP address or a hostname.
Username	Username; default: none	Username to connect to L2TP server.
Password	default: none	Password to connect to L2TP server.
Authentication	default: none	L2TP tunnel authentication password.
Keep alive	default: none	Send LCP echo requests to server in seconds.
Default route	default: none	Check the box to set the L2PT tunnel as default route.

5.3.4 PPTP Server

Point-to-Point Tunneling Protocol (PPTP) is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. A company no longer needs to lease its own lines for wide-area communication but can securely use the public networks. This kind of interconnection is known as a virtual private network (VPN).

5.3.4.1 PPTP Server – General Settings

A **PPTP server** is an entity that waits for incoming connections from PPTP clients.

Figure 99. Services > VPN > PPTP Server > General Settings

Table 77. Services > VPN > PPTP Server > General Settings

Field	Value	Description
Enable VPN Server	default: disable	Check the box to enable the PPTP function.
Server IP	default: 10.0.0.1	IP address of this xxR5805 PPTP network interface.
Client IP	default: 10.0.0.2-254	PPTP IP address leases will begin to end from the address specified in this field.
DNS IP address	default: 114.114.114.114	IP address of the DNS server which will be sent to the client.
Enable MPPE Encrption	default: enable	Allows 128-bit encrypted connection.
Enable NAT Forward	default: enable	Allows forwarding traffic.
Enable remote service	default: enable	Allows remote computers on the internet to connect to VPN server.

5.3.4.2 PPTP Server – Users Manager

Figure 100. Services > VPN > PPTP Server > Users Manager

Table 78. Services > VPN > PPTP Server > Users Manager

Field	Value	Description
Enabled	default: enable	Check the box to enable the PPTP function.
You name	default: username	Username to connect to PPTP (xxR5805) server.
Password	default: password	Password to connect to PPTP (xxR5805) server.
IP address	default: Automatically	Accepted PPTP Client source IP.

5.3.4.3 PPTP Server – Online Users

The **Online User** section is used to user authentication settings required to successfully connect to this server. The list is empty by default.

Figure 101. Services > VPN > PPTP Server > Online Users

Table 79. Services > VPN > PPTP Server > Online Users

Field	Description
Server IP	The PPTP IP of the device.
Client IP	PPTP Client's PPTP IP.
IP address	PPTP Client's real IP.
Blacklist	Block PPTP Client on the list and allow everything else. Button type: Add to Blacklist/Remove from Blacklist.
Forced offline	Disconnect PPTP Client.

5.3.5 GRE

GRE (Generic Routing Encapsulation RFC2784) is a solution for tunnelling RFC1812 private address-space traffic over an intermediate TCP/IP network such as the Internet. GRE tunnelling does not use encryption it simply encapsulates data and sends it over the WAN.

5.3.5.1 GRE Overview

Support two GRE Tunnels and the **Overview** tab contains the Name, Local, Remote endpoint, and Tunnel Network of GRE Information.

Figure 102. Services > VPN > GRE > Overview

Enable	Name	Local	Remote endpoint	Tunnel Network
<input type="checkbox"/>	Tun1			Edit
<input type="checkbox"/>	Tun2			Edit

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

Table 80. Services > VPN > GRE > Overview

Field	Description
Enable	Enable/disable GRE tunnels by checkbox.
Name	The Name of GRE tunnel.
Local	IP Address of this device.
Remote endpoint	The Public IP address of the opposite device.
Tunnel Network	IP address and subnet mask of the local GRE Tunnel network interface.

5.3.5.2 GRE Instance

Figure 103. Services > VPN > GRE > GRE Instance: Tun1/2

GRE Instance: Tun1

Main Settings

Enabled ☐

Remote endpoint IP address

Bind Interface Unspecified ▼

Local IP address

Firewall zone Unspecified ▼

MTU
Range of the value must be from 68 to 1476

Outbound key
Range of the value must be from 1 to 4294967295

Inbound key
Range of the value must be from 1 to 4294967295

Outbound checksum ☐

Inbound checksum ☐

Outbound serialization ☐

Inbound serialization ☐

Path MTU Discovery ☒

TTL
Range of the value must be from 1 to 255

Tunnel Settings

Local GRE interface IP address

Local GRE interface netmask

Table 81 Services > VPN > GRE > GRE Instance: Tun1/2

Field	Value	Description
Main Settings		
Enabled	default: disable	Check the box to enable the GRE function.
Remote endpoint IP address	default: none	The Public IP address of the opposite device.
Bind Interface	Unspecified lan wan; default: Unspecified	Network interface used to establish the GRE Tunnel.
Local IP address	default: none	IP Address of this device.
Firewall zone	Unspecified lan wan; default: Unspecified	Specify GRE work on which interface.

MTU	Value from 68 to 1476; default: 1280	Sets the maximum transmission unit (MTU) size. It is the largest size of a protocol data unit (PDU) that can be transmitted in a single network layer transaction.
Outbound key	Value from 1 to 4294967295; default: none	A key used to identify outgoing packets. This value should match the "Inbound key" value set on the opposite GRE instance or both key values should be omitted on both sides.
Inbound key	Value from 1 to 4294967295; default: none	A key used to identify incoming packets. This value should match the "Outbound key" value set on the opposite GRE instance or both key values should be omitted on both sides.
Outbound checksum	default: disable	Check to verify outbound checksum for the GRE header and payload.
Inbound checksum	default: disable	Check to verify inbound checksum for the GRE header and payload.
Outbound serialization	default: disable	Check to verify outbound serialization for the GRE header and payload.
Inbound serialization	default: disable	Check to verify inbound serialization for the GRE header and payload.
Path MTU Discovery	Value from 1 to 255; default: check TTL: 64	Sets a custom TTL (Time to Live) value for encapsulated packets. TTL is a field in the IP packet header which is initially set by the sender and decreased by 1 on each hop. When it reaches 0 it is dropped and the last host to receive the packet sends an ICMP "Time Exceeded" message back to the source.
Tunnel Settings		
Local GRE interface IP address	default: none	IP address of the local GRE Tunnel network interface.
Local GRE interface netmask	default: none	Subnet mask of the local GRE Tunnel network interface.

5.4 VRRP

The **Virtual Router Redundancy Protocol (VRRP)** is a computer networking protocol used for automatic default gateway selection for clients on a LAN network when the main router (Master) becomes unavailable. Another VRRP router (Backup) then assumes the role of Master and thus backing up the connection.

5.4.1 VRRP LAN configuration settings

The **VRRP LAN configuration settings** section is used to set the main settings of VRRP. Refer to the figure and table below for information on the fields contained in that section.

Figure 104. Services > VRRP > VRRP LAN Configuration Settings

VRRP Configuration

VRRP LAN Configuration Settings

Enable ☒ Enable VRRP (Virtual Router Redundancy Protocol) for LAN

IP address Virtual IP address(es) for LAN's VRRP (Virtual Router Redundancy Protocol) cluster

Virtual ID Routers with same IDs will be grouped in the same VRRP (Virtual Router Redundancy Protocol) cluster, range [1 - 255]

Priority Router with highest priority value on the same VRRP (Virtual Router Redundancy Protocol) cluster will act as a master, range [1 - 255]

Advertisement Interval Time interval in seconds between advertisements, range [1 - 255]

Table 82. Services > VRRP > VRRP LAN Configuration Settings

Field	Value	Description
Enable	default: disable	Turns VRRP on or off.
IP address	default: 192.168.1.253	Virtual IP address for the router's LAN VRRP cluster.
Virtual ID	integer [1 - 255]; default: 1	The Virtual Router Identifier (VRID) is a field in the VRRP packet IP header used to identify the virtual router in the VRRP cluster. Routers with identical IDs will be grouped in the same VRRP cluster.
Priority	integer [1 - 255]; default: 100	VRRP priority of the virtual router. Smaller values equal higher priority. The router with the highest priority is considered to be the <i>Master router</i> while other routers are <i>Backup routers</i> . <ul style="list-style-type: none"> • Master router - the first hop router in the VRRP cluster (i.e., the router that provides connectivity to LAN devices by default). • Backup router - assumes the role of Master router in case it becomes unavailable. If there are multiple Backup routers in the VRRP cluster, the one with the highest priority will assume the role of Master.

Advertisement Interval	integer [1 - 255]; default: 1	Time interval in seconds between advertisements.
------------------------	----------------------------------	--

5.4.2 Check Internet connection

The **Check Internet connection** section is used to set the parameters that define how the router will determine whether the Internet connection is still available or not. This is done by periodically sending ICMP packets to a defined host and awaiting responses. If no response is received after a defined period of time, the connection is determined to be down, and thus the role of Master is assumed by another router in the network.

Refer to the figure and table below for information on the fields contained in the Check Internet connection section.

Figure 105. Services > VRRP > Check Internet Connection

Table 83. Services > VRRP > Check Internet Connection

Field	Value	Description
Enable	default: none	Turns Internet connection checking on or off.
Ping IP address	default: none	IP address or hostname to which the router will send ICMP packets. This is used to determine whether the Internet connection is still available or not. Therefore, it is recommended that you enter the address of remote host that is usually available (for example, 8.8.8.8).
Ping interval	default: 10	Time interval (in seconds) between two Pings.
Ping timeout (sec)	integer [1 to 9999]; default: 1	The maximum amount of time the router will wait for a response to a ping request. If it does not receive a response for the amount of time defined in this field, the ping request will be considered to have failed.
Ping packet size	integer [1 to 1000]; default: none	The size (in bytes) of sent ICMP packets.
Ping retry count	integer [1 to 9999]; default: none	How many times the router will retry sending ping requests before determining that the Internet connection has failed.

5.5 GPS

The **Global Positioning System (GPS)** is a space-based radio navigation system.

5.5.1 GPS Settings

Device CAN Update GPS information without plugging SIM Card! Please make sure GPS service is enabled and device is receiving GPS data.

Figure 106. Services > GPS > Settings



Table 84. Services > GPS > Settings

Field	Value	Description
Enable	default: disable	Turn on/off the GPS Service.
Get GPS information	default: auto	Specify the GPS work mode. Now is only auto.

5.5.2 GPS Information

Display the GPS Synchronization status, Time(UTC), Latitude, and Longitude.

Figure 107. Services > GPS > Information

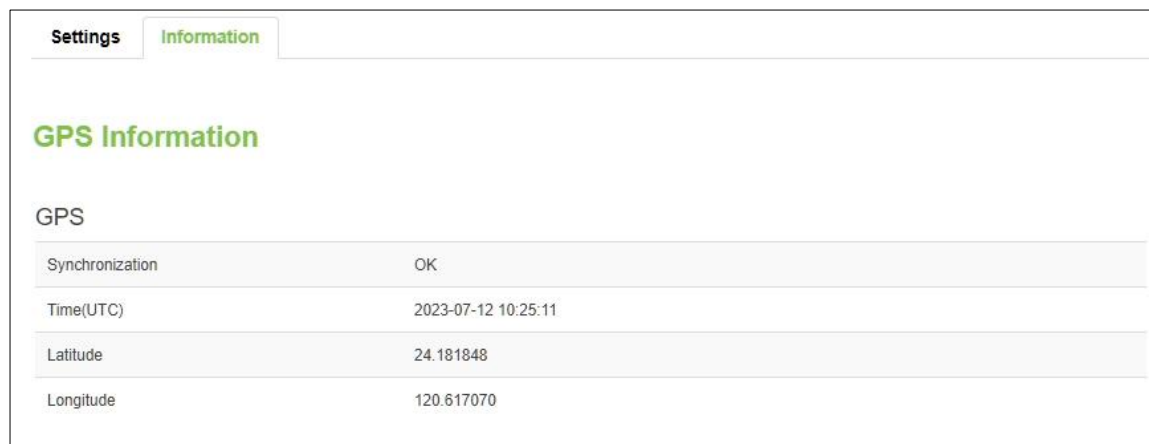


Table 85. Services > GPS

Field	Value	Description
Synchronization	default: none	The GPS Synchronization status. none: Not synchronize or doesn't receiving GPS data. OK: Synchronized and receiving GPS data.

Time(UTC)	YYYY-MM-DD HH:MM:SS	The last GNSS with UTC timezone. (Update every 6 seconds.)
Latitude	xx.xxxxxx;	It it shows the angle between the straight line in the certain point and the equatorial plane.
Longitude	xxx.xxxxxx;	It is defined as an angle pointing west or east from the Greenwich Meridian, which is taken as the Prime Meridian.

5.6 MQTT

MQTT (MQ Telemetry Transport or Message Queue Telemetry Transport) is an ISO standard (ISO/IEC PRF 20922) publish-subscribe-based "lightweight" messaging protocol for use on top of the TCP/IP protocol. It is designed to send short messages from one client (*publisher*) to another (*subscriber*) through *brokers*, which are responsible for message delivery to the end point.

5.6.1 MQTT Broker

xxR5805 devices support this functionality via an open source Mosquitto broker. The messages are sent this way: a client (subscriber) subscribes to a topic(s); a publisher posts a message to that specific topic(s). The broker then checks who is subscribed to that topic(s) and transmits data from the publisher to the subscriber.

The **MQTT Broker** is an entity that listens for connections on the specified port and relays received messages to MQTT client. To begin using this device as an MQTT Broker, enable it in this page. In order to make the device accept MQTT connections from WAN (remote networks), you also need to check the 'Enable Remote Access' button on.

Figure 108. Services > MQTT > Broker

Broker

MQTT Broker

Enable ☐ ⓘ Select to enable MQTT

Local Port ⓘ Specify local port which the MQTT will be listen to

Enable Remote Access ☐ ⓘ Select to enable remote access

Table 86. Services > MQTT > Broker

Field	Value	Description
Enable	default: disable	Enable/Disable MQTT Broker.
Local Port	Integer [0 - 65535]; default: 1883	The TCP port on which the MQTT broker will listen for connections.
Enable Remote Access	default: disable	Enable/Disable remote access to this MQTT broker function.

5.6.2 Broker Settings

5.6.2.1 Broker - Security

Figure 109. Services > MQTT > Security

Broker settings

Security Bridge Miscellaneous

Use TLS/SSL ☒ Mark to use TLS/SSL for connection

CA Cert File No file chosen
 Upload CA cert file

Server Cert File No file chosen
 Upload server cert file

Server Key File No file chosen
 Upload server key file

TLS version Used TLS version

Table 87. Services > MQTT > Security

Field	Value	Description
Use TLS/SSL	default: disable	Turns the use of TLS/SSL for this MQTT connection on or off.
CA Cert File	File type: .ca file default: none	Uploads a Certificate Authority (CA) file. A Certificate Authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
Server Cert File	File type: .crt file default: none	Uploads a server (broker) certificate file. A certificate file is a type of digital certificate that is used by client systems to make authenticated requests to a remote server.
Server Key File	File type: .key file default: none	Uploads a server (broker) key file.
TLS version	tls1.1/tls1.2/Support all; default: Support all	Specifies which TLS version(s) is will be supported by this broker.

5.6.2.2 Broker - Bridge

Figure 110. Services > MQTT > Bridge

Broker settings

Security

Bridge

Miscellaneous

Enable

☒

Enable connection to remote bridge

Connection Name

Remote Address

Select remote bridge address

Remote Port

1883

Select remote port

Use Remote TLS/SSL

☐

Select to use TLS/SSL for remote connection

Use Remote Bridge Login

☐

Select to use login for bridge

Try Private

☐

Check if remote broker is another instance of a daemon

Clean Session

☐

Discard session state when connecting or disconnecting

Topic	Direction	QoS level
There are no topics created yet.		

Add

Table 88. Services > MQTT > Bridge

Field	Value	Description
Enable	default: disable	Enable/Disable MQTT Bridge.
Connection Name	default: none	Name of the Bridge connection. This is used for easier management purposes.
Remote Address	default: none	Remote Broker's address.
Remote Port	integer [0-65535]; default: 1883	Specifies which port the remote broker uses to listen for connections.
Use Remote TLS/SSL	default: disable	Enables the use of TLS/SSL certificates of the remote broker. If this is checked, you will be prompted to upload TLS/SSL certificates. More information can be found in the Security section of this chapter.
Use Remote Bridge Login	default: disable	Indicates whether the remote side of the connection requires login information. If this is turned on, you will be required to enter a remote client ID, Username and password.
Try Private	default: disable	Check if the remote Broker is another instance of a daemon.
Clean Session	default: disable	When turned on, discards session state after connecting or disconnecting.
Topic Name	default: none	The name of the topics that the broker will subscribe to.
Direction	Out/In/Both; default: none	The direction that the messages will be shared.
QoS Level	At most once (0) At least once (1) Exactly once (2) default: none	Sets the publish/subscribe QoS level used for this topic

5.6.2.3 Broker – Miscellaneous

The **Miscellaneous** section is used to configure MQTT broker parameters that are related to neither Security nor Bridge.

Figure 111. Services > MQTT > Miscellaneous

Broker settings

Security

Bridge

Miscellaneous

ACL File

Choose File No file chosen

Select ACL file

Password File

Choose File No file chosen

Uploads passwords/users file

Persistence

☐ If true, connection, subscription and message data will be written to the disk

Allow Anonymous

☐ Allows anonymous access

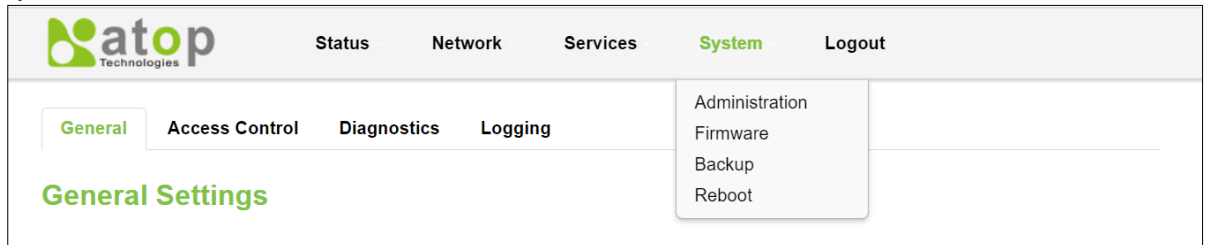
Table 89. Services > MQTT > Miscellaneous

Field	Value	Description
ACL File	ACL file default: none	Uploads an ACL file. The contents of this file are used to control client access to topics of the broker.
Password File	Password file default: none	Uploads a password. A password file stores Usernames and corresponding passwords, used for authentication.
Persistence	default: disable	When turned on, connection, subscription and message data will be written to the disk. Otherwise, the data is stored in the device memory only.
Allow Anonymous	default: disable	Turns anonymous access to this broker on or off.

6 System

As shown in the Figure below, the system menu consists of the following sub-menus: Administration, Firmware, Backup and Reboot which are related to system-level setup on the xxR5805 device.

Figure 112. System



6.1 Administration

In **Hostnames** section, it provides a static mapping of an IP address to a hostname, which will be served by the DNS on the xxR5805 device. The hostname will also display on the Hostname field of DHCP Release section of the Overview menu when a DHCP client device is assigned a mapped IP address.

In the **Login Password** section, you can improve the system security by changing the password from the default value to ensure that only the authorized access to the router is allowed.

Click the **"Restore"** button to reset the configuration files to factory default settings of the xxR5805 device.

Figure 113. System > Administration > General Settings

The screenshot shows the 'General Settings' page in the Atop Technologies web interface. The navigation bar at the top includes General (highlighted in green), Access Control, Diagnostics, Logging, WEB Management, and Login Accounts. The main content area is titled 'General Settings' in green. Under 'System Properties', there is a 'Hostname' field with the value 'AtopTechnologies'. Under 'Login Password', there are three password fields: 'Current Password', 'New Password', and 'Confirm New Password'. Each field has a toggle icon to the right. Below the 'New Password' and 'Confirm New Password' fields, there is a password strength indicator: 'A.Length:8-32 B.Include:1.lowercase letter 2.uppercase letter 3.number'. At the bottom, there is a 'Restore Default Settings' section with a 'Restore to default' button and a 'Restore' button.

Table 90. System > Administration > General Settings

Field	Description
Hostname	Hostname which is mapped to a specified IP address.
Current Password	Input current password for admin account.
New Password	Input new password for admin account. Need follow the rules as below: A.Length:8-32 B.Include:1.lowercase letter 2.uppercase letter 3.number
Confirm New Password	Re-enter the new password for admin account. Both values on Password field and Confirmation field must be the same, so that the new password can be saved and takes effect.

6.1.1 Access Control

The **Access Control** page is only used for **LAN Interface** to access device.

Important: turning on remote access leaves your device vulnerable to external attackers. Make sure you use a strong password.

6.1.1.1 Telnet Access

In the **Telnet Access** Section within the **Administration** sub-menu, you can enable the Telnet service. The service will allow the remote Telnet hosts to access xxR5805 device only for **LAN** interface.

Figure 114. System > Administration > Access Control > Telnet Access

Table 91. System > Administration > Access Control > Telnet Access

Field	Value	Description
Enable	default: Disable	Check box to enable Telnet access.
Port	default: 23	Port to be used for Telnet connection.

6.1.1.2 SSH Access

In the **SSH Access** Section within the **Administration** sub-menu, you can enable the SSH service (dropbear, putty). The service will allow the remote SSH hosts to access xxR5805 device only for **LAN** interface.

Figure 115. System > Administration > Access Control > SSH Access

SSH Access

Enabling SSH access makes your device reachable from specified interface

Enable ☐ Turn SSH on/off

Port Specifies the listening port

Table 92. System > Administration > Access Control > SSH Access

Field	Value	Description
Enable	default: disable	Turn SSH service on/off.
Port	default: 22	Port number that the SSH service will be listening to.

6.1.2 Diagnostics

There are three network diagnostic utilities available in **Diagnostics** webpage under Network menu. As shown in the Figure below, these utilities are called **ping**, **traceroute**, and **nslookup**. Each utility can be used to test network functionality, and to diagnose network quality and network connection state.

Figure 116. System > Administration > Diagnostics

General **Access Control** **Diagnostics** **Logging**

Diagnostics

Network Utilities

6.1.2.1 Ping

The ping network diagnostic utility is used to test network reachability. You can use the **Ping** function to determine whether xxR5805 device can reach the gateway or other devices in the network.

To use the Ping, enter a destination IP address or FQDN (Fully Qualified Domain Name) in the text box above the **Ping** button and click Ping button to start a ping process as shown in the Figure below. This process takes a few second, also represents successful ping process without packet loss from xxR5805 device to <http://www.atop.com.tw> and back.

Figure 117. System > Administration > Diagnostics > Ping

Diagnostics

Network Utilities

www.atop.com.tw www.atop.com.tw www.atop.com.tw


```

PING www.atop.com.tw (172.67.143.48): 56 data bytes
64 bytes from 172.67.143.48: seq=0 ttl=55 time=139.735 ms
64 bytes from 172.67.143.48: seq=1 ttl=55 time=138.392 ms
64 bytes from 172.67.143.48: seq=2 ttl=55 time=138.076 ms
64 bytes from 172.67.143.48: seq=3 ttl=55 time=138.739 ms
64 bytes from 172.67.143.48: seq=4 ttl=55 time=138.203 ms

--- www.atop.com.tw ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 138.076/138.629/139.735 ms
  
```

6.1.2.2 Traceroute

The traceroute network diagnostic utility is used to trace routing path of packets.

You can use the **Traceroute** function to trace the routes of packets to destination IP address or FQDN from xxR5805 device in the network. To use Traceroute function, enter a destination IP address or FQDN in the text box above the **Traceroute** button and click the button to start a traceroute process as shown in the Figure below.

This process usually takes a few seconds, also represents a successful traceroute process from xxR5805 device to Atop's website <http://www.atop.com.tw>.

Figure 118. System > Administration > Diagnostics > Traceroute

Diagnostics

Network Utilities

www.atop.com.tw www.atop.com.tw www.atop.com.tw


```

traceroute to www.atop.com.tw (104.21.46.242), 30 hops max, 38 byte packets
 1  192.168.4.254  0.515 ms
 2  192.168.4.1  0.389 ms
 3  211.22.151.254  1.070 ms
 4  168.95.211.166  3.809 ms
 5  220.128.17.42  5.677 ms
 6  220.128.16.58  11.673 ms
 7  220.128.8.49  4.836 ms
 8  202.39.91.5  131.400 ms
 9  202.39.84.86  137.920 ms
10  141.101.72.250  142.129 ms
11  104.21.46.242  138.563 ms
  
```

6.1.2.3 Nslookup

The nslookup network diagnostic utility is used to send a query to the DNS (Domain Name System) to obtain domain or IP address mapping, or other DNS records.

You can use the **Nslookup** function to query an IP address mapping of destination FQDN from xxR5805 device in the network. To use the Nslookup function, enter a FQDN in the text box above the **Nslookup** button and click it to start a nslookup process as shown in the Figure below.

This process usually takes a few seconds, also represents a successful nslookup process from xxR5805 device to the Atop's website <http://www.atop.com.tw>.

Figure 119. System > Administration > Diagnostics > Nslookup

The screenshot shows the 'Diagnostics' section with a sub-tab 'Network Utilities'. It contains three input fields, each with 'www.atop.com.tw' entered. Below each field are buttons for 'Ping', 'Traceroute', and 'Nslookup'. The 'Nslookup' button is highlighted with a blue border. Below these buttons is a text area displaying the results of the nslookup command:

```
Server: 127.0.0.1
Address 1: 127.0.0.1 localhost

Name: www.atop.com.tw
Address 1: 2606:4700:3034::6815:2ef2
Address 2: 2606:4700:3037::ac43:8f30
Address 3: 172.67.143.48
Address 4: 104.21.46.242
```

6.1.3 Logging

Shows the **Logging** tab within the **System** sub-menu. You can monitor the system log for debugging purpose on the xxR5805 device. The configuration is also allowed you to send message log to the external server. Press Download log button CAN download system log file (system_log.tar.gz) in Local PC. Press Delete log button CAN delete all System Log and Kernel Log in Status > Logs.

Figure 120. System > Administration > Logging

The screenshot shows the 'Logging' section with a sub-tab 'System Log'. It contains the following configuration options:

- Enable:** A checkbox that is checked.
- Buffer size:** A text input field containing '1024'.
- Unit:** A dropdown menu showing 'KB'.
- Level:** A dropdown menu showing 'Normal'.
- Download log:** A button with a green download icon and the text 'Download'.
- Delete log:** A button with a red delete icon and the text 'Delete'.

Below these options is the 'External system log server' section:

- Enable:** A checkbox that is unchecked.
- IP:** A text input field containing '0.0.0.0'.
- Port:** A text input field containing '514'.

Table 93. System > Administration > Logging

Field	Value	Description
Buffer size	default: 1024	Size of the system log message buffer.
Buffer size	default: 1024	Size of the system log message buffer.
Level	Debug/Normal/Warning; default: Normal	Define the level of system log that displayed above severity in Status > Logs. Severity Level: Warning > Normal > Debug
External System Log Server	default: disable	IP address of a syslog server to which the system log messages should be sent in addition to the local destination.
External System Log Server Port	default: 514	Port number of the remote syslog server

6.1.4 WEB Management

Administrator CAN modify the Web HTTP/HTTPS server port in **WEB server**. Administrator CAN defined the time of idle timeout/ Login attempts numbers/ Failed & the time of Lock time in WEB Management. The purpose is that protect device under login retry attack.

Figure 121. System > Administration > WEB Management

The screenshot shows the 'WEB Management' tab selected in the 'System > Administration' menu. The page is divided into two main sections: 'Web server' and 'WEB Management'.

Web server

Port

HTTP: 80

HTTPS: 443

WEB Management

Idle Timeout Settings

Time: 5

Please enter in minutes. Default is 5.

User Login Settings

Attempts: 3

Number of failed attempts to prevent User to login. Default is 3.

Lock Time: 10

Time to login after failed login attempts. Please enter in minutes. Default is 10.

Table 94. System > Administration > WEB Management

Field	Value	Description
HTTP	default: 80	Specify the port of HTTP protocol. (If use HTTP with specified port correctly, Web will transmit to HTTPS.)
HTTPS	default: 443	Specify the port of HTTPS protocol.
Idle Timeout Settings/Time	integer [1 - 5000]; default: 5	Defined the time that login user is inactive and then logout automatically.
User Login Settings/Attempts	integer [2 - 10]; default: 3	Number of failed attempts to prevent User to login.
User Login Settings/Lock Time	integer [1 - 5000]; default: 10	Defined the Lock Time after failed login attempts.

6.1.5 Login Accounts

Administrator CAN add Admin User and Guest User accounts. The permission of Admin User is the same with Administrator. The permission of Admin User is only checking Status Menu.

Figure 122. System > Administration > Login Accounts

Table 95. System > Administration > General Settings

Field	Description
Username	Hostname which is mapped to a specified IP address.
Password	Input password for Admin/Guest User account. Need follow the rules as below: A.Length:8-32 B.Include:1.lowercase letter 2.uppercase letter 3.number

6.2 Firmware

The mechanism to upgrade firmware of the xxR5805 device to optimize performance or fix bugs is provided in the **Flash new firmware image** Section within the **Backup/Flash Firmware** sub-menu. It is imperative that xxR5805 device must **NOT be turned off or powered off during the firmware upgrade**.

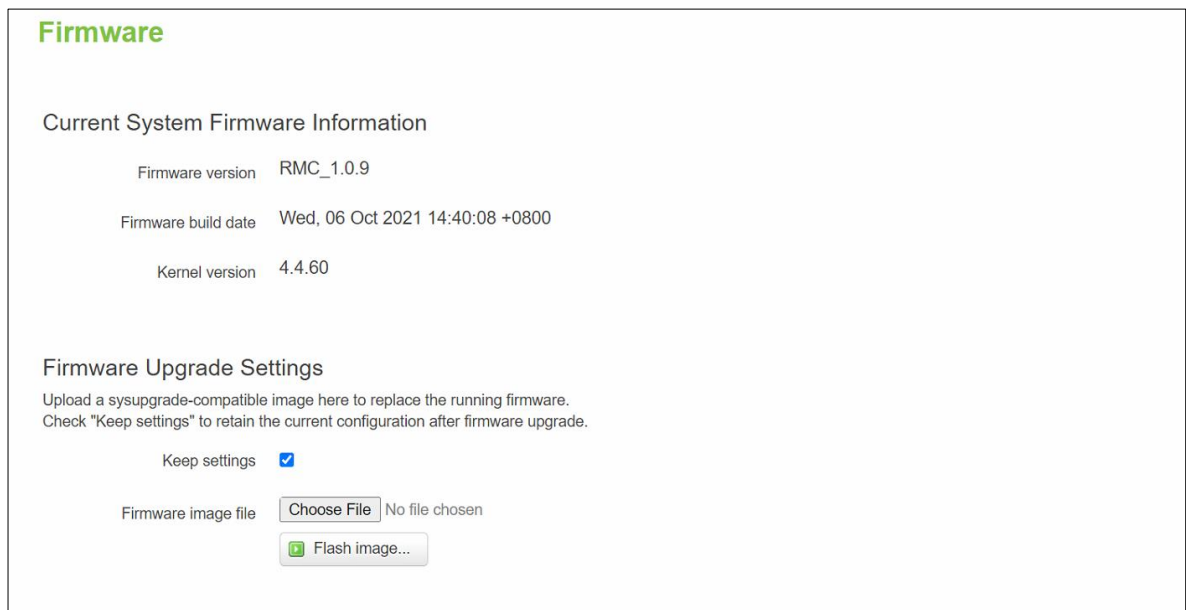
Here are the steps to follow for the firmware upgradation:

1. Before upgrading the firmware, please make sure that the device has a reliable power source and will not power off or restart during the firmware upgrading process.
2. Download the latest firmware for the correct model of the xxR5805 device from the Download page under the Support link on Atop's main webpage.
3. Copy the newly downloaded firmware file on to your local computer. Note that the firmware file is a binary file with ".img" extension.
4. Open the Web UI and select Backup/Flash Firmware sub-menu under the System > Firmware menu.
5. For a more advanced feature, you can click on "Generate archive" checkbox on the System > Backup to perform backup configuration files of the xxR5805 device before upgrading its firmware. This will allow you to restore the xxR5805 device's configuration after firmware upgrade has been done.
6. Click "Chose File" button to find and choose the new firmware file.

Note: You may need to re-configure your xxR5805 device if you had unchecked the "Keep settings" field in Flash new firmware image section after the firmware upgrade.

7. Then, click "Flash image" button to start the firmware upgrade process.

Figure 123. System > Firmware



Firmware

Current System Firmware Information

Firmware version	RMC_1.0.9
Firmware build date	Wed, 06 Oct 2021 14:40:08 +0800
Kernel version	4.4.60

Firmware Upgrade Settings


Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration after firmware upgrade.

Keep settings ☒

Firmware image file No file chosen

8. In the Figure below, the “Flash Upgrade – Verify” webpage will be displayed after the firmware file has been successfully verified by system successfully.

Figure 124. Confirm message of the Firmware Upgrade



Firmware Upgrade - Verify

The firmware image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Upgrade" below to start the firmware upgrade procedure.

- Checksum: 02ad376f3c19326f73a4fa250b1ef4e1
- Size: 27.37 MB
- Note: System Configuration files will be kept.

9. Click the “Upgrade” button. Then, program will show “Waiting for changes to applied...” on the System – Flashing... webpage. Please wait until the uploading process is finished (the amount of time varies depending on the equipment used).
10. ThexxR5805 device will be restarted and the web browser on the local computer will be redirected to Login webpage.



Attention: It is very important that the xxR5805 device is **not** turned off while the firmware upgrade is in progress.

6.3 Backup

In the **Backup** sub-menu within the **System** menu, you can perform system backup and restore xxR5805 device's configuration files.

Backup System Configuration

Click the **Generate archive** button to backup configuration files from xxR5805 device to your local host device. These backup configuration files are archived to a **backup-Hostname-yyyy-mm-dd.tar.gz** file.

Restore System Configuration

To restore previously saved configuration files from a local host device to the xxR5805 device, please perform the following steps:

1. Click **Choose File** button to select the archive file (backup-Hostname-yyyy-mm-dd.tar.gz).
2. Click **Upload archive** button to start restoring the archive file to the xxR5805 device.

Figure 125. System > Backup

The screenshot shows a web interface titled "Backup" in green. It contains two main sections: "Backup System Configuration" and "Restore System Configuration".

Backup System Configuration: This section includes the instruction "Click 'Generate archive' to download a tar archive of the current configuration files." Below this, there are two buttons: "Download backup" and "Generate archive" (which has a green download icon).

Restore System Configuration: This section includes the instruction "To restore configuration files, you can upload a previously generated backup archive here." Below this, there are two buttons: "Restore backup" and "Choose File" (which is disabled and shows "No file chosen"). Below these is an "Upload archive..." button with a green upload icon.

6.3.1 Reboot

In the **Reboot** sub-menu within the **System** menu, you can reboot the CWR5805 device by clicking the **Perform Reboot** button. The webpage will then display "**Please wait: Device rebooting...**" and initiate a system restart. When the system rebooting process is finished, the web browser will be redirected to the **Login** webpage. Please enter the correct login password in the **Password** field for logging in.

Figure 126. System > Reboot

The screenshot shows a web interface titled "Reboot" in green. It contains a warning message: "Warning! Device will temporarily lose the connection during reboot." Below the warning, there is a single button labeled "Perform Reboot" with a green reboot icon.

7 Logout

Click to log the current you out safely, after logging out, it will switch to login page.

Figure 127. System > Logout



8 Specifications

8.1 Hardware Specification

Table 96. Hardware Specification

System		
CPU	Qualcomm IPQ4029	
Flash Memory	128MB	
RAM	DDR3L 256MB	
Network		
Ethernet Interface	1x10/100/1000 WAN 4x10/100/1000 LAN Connector: RJ45	
Wireless Interface	802.11ac, 802.11a, 802.11n, 802.11 b/g MU-MIMO access point	
5G/LTE Interface	Up to 2x Nano-SIM card slots	
	5G model	5G-NR SA and NSA
	LTE Model	LTE Cat.6
Wi-Fi Security	AES-CCMP, TKIP, WPA3-PSK, WPA2-PSK, WPA-PSK	
LED Indicator		
LED indication	Power x1 Wi-Fi 2.4G x 1 Wi-Fi 5G x 1 WAN x 1 LAN x 4 Mobile SIM1 signal x 3 Mobile SIM2 signal x 3	
Power Requirement		
Input	Single 12~48 VDC 3-pin terminal block connector	
Mechanical		
Dimensions (W x H x D)	145 x 120 x 46 mm	
Enclosure	IP30 protection, metal housing	
Environmental		
Temperature	Operations	-40°C ~ 75°C
	Storage	-40°C ~ 85°C
Relative Humidity	5% ~ 95%, 55°C Non-condensing	

8.2 CWR5805 Device Pin Assignments for WAN/LAN Port

RJ45 connectors for 10/100/1000Base-T(X) Ethernet

Figure 128. WAN/LAN Port on RJ45 with Pin Numbering of CWR5805 Device

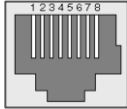


Table 97. Assignment for RJ-45 Connector of CWR5805 Device

10/100/1000Base-T(x)								
Pin#	1	2	3	4	5	6	7	8
Signal	Tx+	Tx-	Rx+	-	-	Rx-	-	-
1000Base-T								
Pin#	1	2	3	4	5	6	7	8
Signal	BI_DA+	BI_DA-	BI_DB+	BI_DC+	BI_DC+	BI_DB-	BI_DD+	BI_DD-

It is strongly recommended for you to set the Network Parameters through **Device Management Utility**© first. Other device-specific configurations can later be carried out via Atop's user-friendly Web-Interface.

9 Glossary

- AP – Access Point
- APN – Access Point Name
- AS – Autonomous System
- BIRD – Bird Internet Routing Daemon
- BSSID – Basic Service Set Identifiers
- CAP – Central Access Point
- CIDR – Classless Inter-Domain Routing
- DHCP – Dynamic Host Configuration Protocol
- DDNS – Dynamic Domain Name Service
- DNS – Domain Name Service
- FQDN – Fully Qualified Domain Name
- IP – Internet Protocol
- IP Address – Internet Protocol Address
- IGP – Interior Gateway Protocol
- ISP – Internet Service Provider
- LAN – Local Area Network
- LSR – Link State Routing
- LTE – Long Term Evolution
- MTU - Maximum Transmission Unit
- MU-MIMO – Multi-User Multiple-Input Multiple-Output
- NAT – Network Address Translation
- NTP – Network Time Protocol
- OSPF – Open Shortest Path First
- PPPoE – Point-to-Point Protocol over Ethernet
- QMI – Qualcomm MSM Interface
- RSSI - Received Signal Strength Indicator
- SIM – Subscriber Identity Module
- SMS – Short Message Service
- SNR – Signal to Noise Ratio
- SSID – Service Set Identifier
- SSL – Secure Sockets Layer
- STP – Spanning Tree Protocol
- TLS – Transport Layer Security
- VPN – Virtual Private Network
- WAN – Wide Area Network



Atop Technologies, Inc.

www.atoponline.com

**TAIWAN HEADQUARTER and
INTERNATIONAL SALES:**

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.

Tel: +886-3-550-8137

Fax: +886-3-550-8131

sales@atop.com.tw

ATOP CHINA BRANCH:

3F, 75th, No. 1066 Building,
Qingzhou North Road,
Shanghai, China

Tel: +86-21-64956231