



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

User Manual  
V1.3  
23<sup>rd</sup> November 2022

\*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](http://www.atoponline.com/request-support)

**Asia & Australia**

Jopson Li  
Tel: +886-918-694-073  
eMail: [jopsonli@atop.com.tw](mailto:jopsonli@atop.com.tw)

**China**

Sam Xia  
Tel: +86-21-649562-31  
eMail: [sales@atop.com.tw](mailto:sales@atop.com.tw)

**Europe**

Alessio Longhini  
Tel: +39-348-26-28-727  
eMail: [alessio@atop.com.tw](mailto:alessio@atop.com.tw)

**Germany**

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

**India & SAARC**

Prashant Mishra  
Tel: +91-80-492-06308  
eMail: [prasant.m@atop.com.tw](mailto:prasant.m@atop.com.tw)

**Indonesia**

Anisah Ambarwati  
Tel: +62-896-761-93026  
eMail: [anisah@atop.com.tw](mailto:anisah@atop.com.tw)

**Italy**

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

**Japan**

Keiichi Sagami  
Tel: +090-2284-9632  
eMail: [sakagami@atop.com.tw](mailto:sakagami@atop.com.tw)

**Latin America**

Jopson Li  
Tel: +886-918-694-073  
eMail: [jopsonli@atop.com.tw](mailto:jopsonli@atop.com.tw)

**Middle East & Africa**

Prashant Mishra  
Tel: +91-80-492-06308  
eMail: [prasant.m@atop.com.tw](mailto:prasant.m@atop.com.tw)

**Russia & CIS**

Timur Dautov  
Tel: +7-985-855-1056  
eMail: [timur@atop.com.tw](mailto:timur@atop.com.tw)

**Taiwan**

Tony Lin  
Tel: +886-968-386876  
eMail: [tonylin@atop.com.tw](mailto:tonylin@atop.com.tw)

**USA & Canada**

Prashant Mishra  
Tel: +91-80-492-06308  
eMail: [prasant.m@atop.com.tw](mailto: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](http://www.atoponline.com).

### Documentation Control

<b>Author:</b>	Saowanee Saewong
<b>Revision:</b>	1.3
<b>Revision History:</b>	Feature Update
<b>Creation Date:</b>	8 December 2021
<b>Last Revision Date:</b>	29 November 2022
<b>Document Status:</b>	Released

## Table of Contents

1	Introduction .....	13
1.1	Overview .....	13
1.2	Software Features .....	14
2	Getting Started .....	15
2.1	Default Factory Settings .....	15
2.1.1	Reset Button .....	15
2.2	Setting up a Connection .....	15
2.3	Login Process and Main Window Interface .....	18
3	Status Menu .....	22
3.1	Overview .....	22
3.2	System .....	23
3.3	Network .....	24
3.3.1	Mobile (CWR5805 Only) .....	24
3.3.2	WAN .....	26
3.3.3	LAN .....	28
3.3.4	Wireless (AWR5805/CWR5805 Only) .....	28
3.3.5	VRRP (AWR5805/CWR5805 Only) .....	30
3.3.6	Access .....	31
3.4	Routes .....	31
3.4.1	ARP .....	32
3.4.2	Active IPv4-Routes Section .....	32
3.5	Logs .....	33
3.5.1	System Log .....	33
3.5.2	Kernel Log .....	34
4	Network Menu .....	35
4.1	Mobile (CWR5805 only) .....	36
4.1.1	General Setup Tab .....	36
4.1.2	Advanced Settings Tab .....	37
4.1.3	SIM Switch .....	38
4.2	WAN .....	40
4.2.1	General Setup .....	41
4.2.2	Advanced Settings .....	44
4.3	LAN .....	48
4.3.1	Common Configuration .....	48
4.3.2	DHCP Server .....	49
4.3.3	Static Leases .....	51
4.4	Wireless .....	51
4.4.1	Wireless Overview .....	51
4.4.2	Associated Stations .....	58
4.4.3	Country .....	58
4.4.4	Tutorials .....	58
4.5	Mesh .....	61
4.6	IPv6 .....	63
4.7	VLAN .....	63
4.8	LB (Load Balancing) and Failover (CWR5805 only) .....	64
4.8.1	Overview .....	64
4.8.2	Configuration .....	65
4.9	Firewall .....	73
4.9.1	General Settings Tab .....	73
4.9.2	Port Forwards Tab .....	79

4.9.3	Traffic Rules Tab.....	80
4.9.4	Attack Prevention Tab .....	83
4.10	Static Routes.....	86
4.11	Dynamic Routes.....	87
4.11.1	RIP Protocol .....	87
4.11.2	OSPF Protocol.....	89
4.12	DNS .....	92
4.13	QoS.....	93
5	. Services Menu.....	95
5.1	Auto Reboot .....	95
5.1.1	Periodic Reboot – Configuration .....	95
5.2	NTP.....	96
5.2.1	General Section.....	96
5.2.2	Time Servers .....	97
5.3	VPN .....	98
5.3.1	OpenVPN .....	98
5.3.2	IPSec.....	103
5.3.3	L2TP.....	111
5.3.4	PPTP.....	114
5.3.5	GRE .....	116
5.4	VRRP .....	118
5.4.1	VRRP LAN configuration settings .....	118
5.4.2	Check Internet connection .....	119
5.5	GPS.....	120
5.6	Ping retry count .....	121
5.7	integer [1 to 9999]; default: none.....	121
5.8	How many times the router will retry sending ping requests before determining that the Internet connection has failed.....	121
5.9	MQTT .....	121
5.9.1	MQTT Broker .....	121
5.9.2	Broker Settings.....	122
6	. System.....	126
6.1	Administration .....	126
6.1.1	General .....	126
6.1.2	Access Control.....	127
6.1.3	Diagnostics.....	128
6.1.4	Logging.....	130
6.2	Firmware .....	131
6.3	Backup .....	133
6.3.1	Reboot .....	133
7	Logout.....	134
	.....	135
8	Specifications .....	135
8.1	Hardware Specification.....	135
8.2	CWR5805 Device Pin Assignments for WAN/LAN Port.....	136
9	Glossary.....	137

## List of Figures

Figure 1.1 . An Example of Wired and Wi-Fi Devices Connected to the Internet Via CWR5805 .....	13
Figure 2.1. Ethernet Properties Dialog Window.....	16
Figure 2.2. Internet Protocol Version 4 Properties Dialog Window .....	17
Figure 2.3. Status Dialog Window .....	18
Figure 2.4. Details on the Network Connection .....	18
Figure 2.5. Warning Dialog due to Invalid Certificate.....	19
Figure 2.6. Warning Dialog of Misconfiguration/Intercepting .....	19
Figure 2.7. Authorization Required Webpage .....	20
Figure 2.8. Invalid Username and/or Password .....	20
Figure 2.9. Prompt to Change Password .....	21
Figure 2.10. Authorization Required Webpage .....	21
Figure 3.1. Main Page .....	22
Figure 3.2. Status -> Overview .....	23
Figure 3.3. Status -> System.....	24
Figure 3.4. Status -> Network -> Mobile .....	25
Figure 3.5. Status -> Network -> WAN .....	27
Figure 3.6. Status -> Network -> LAN .....	28
Figure 3.7 Status -> Network -> Wireless .....	29
Figure 3.8. Status -> Network -> VRRP (Master) .....	30
Figure 3.9. Status -> Network -> VRRP (Backup).....	30
Figure 3.10. Status -> Network -> Access .....	31
Figure 3.11. Status -> Routes – ARP .....	32
Figure 3.12. Status -> Routes – Active IPv4 Routes.....	32
Figure 3.13 Status -> Log -> System Log .....	33
Figure 3.14. Status -> System -> Kernel Log .....	34
Figure 4.1. Network Overview.....	35
Figure 4.2. Webpage of the General Tab in Network->Mobile Submenu .....	36
Figure 4.3. Webpage of the Advanced Setting Tab in Network->Mobile Submenu .....	37
Figure 4.4. Webpage of the SIM Switch Tab in Network->Mobile Submenu .....	38
Figure 4.5. Data Connection Limit Configuration Subsection under Network->Mobile Submenu->SIM Switch Tab.....	39
Figure 4.6. SMS Warning Configuration Subsection under Network->Mobile Submenu->SIM Switch Tab.....	40
Figure 4.7. Clear Data Limit Subsection under Network->Mobile Submenu->SIM Switch Tab .....	40
Figure 4.8. General Setup Tab under the Network->WAN Submenu.....	41
Figure 4.9. Static Address Protocol in the General Setup Tab under the Network->WAN Submenu .....	42
Figure 4.10. DHCP Client Protocol in the General Setup Tab under the Network->WAN Submenu.....	43
Figure 4.11. PPPoE Protocol in the General Setup Tab under the Network->WAN Submenu.....	43
Figure 4.12. Static Address Protocol in the Advanced Setting Tab under the Network->WAN Submenu .....	45
Figure 4.13. DHCP Client Protocol in the Advanced Setting Tab under the Network->WAN Submenu.....	46
Figure 4.14. PPPoE Protocol in the Advanced Setting Tab under the Network->WAN Submenu .....	47
Figure 4.15. Common Configuration Section under the Network->LAN Submenu .....	48
Figure 4.16. General Setup Tab in the DHCP Section under the Network->LAN Submenu .....	50
Figure 4.17. Advanced Settings Tab in the DHCP Section under the Network->LAN Submenu .....	50
Figure 4.18. Static Leases Section under the Network->LAN Submenu.....	51
Figure 4.19. Wireless Overview Section under the Network->Wireless Submenu .....	52
Figure 4.20. After Clicking Scan Button in the Wireless Overview Section under the Network->Wireless Submenu .....	52
Figure 4.21. Device Configuration after Clicking Edit Button in the Wi-Fi 2.4GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section .....	53
Figure 4.22. Device Configuraiton after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section .....	54
Figure 4.23. Interface Configuration – General Setup Tab after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section .....	55
Figure 4.24. Interface Configuration – Wireless Security Tab after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section .....	55
Figure 4.25. Interface Configuration – MAC-Filter Tab after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section .....	56

Figure 4.26. Common Configuration after Clicking Edit Button in the Wi-Fi 2.4GHz Guest Subsection under the Network->Wireless Submenu->the Wireless Overview Section.....	56
Figure 4.27. DHCP Server – General Setup after Clicking Edit Button in the Wi-Fi 2.4GHz Guest Subsection under the Network->Wireless Submenu->the Wireless Overview Section .....	57
Figure 4.28. DHCP Server – Advanced Settings after Clicking Edit Button in the Wi-Fi 2.4GHz Guest Subsection under the Network->Wireless Submenu->the Wireless Overview Section .....	58
Figure 4.29. Associated Stations Section under the Network->Wireless Submenu .....	58
Figure 4.30. Country Section under the Network->Wireless Submenu .....	58
Figure 4.31. Details of the Wireless Network Connection .....	59
Figure 4.32. Wireless Overview Section under Network->Wireless Menu .....	59
Figure 4.33. Network & Internet Settings on the Android System .....	60
Figure 4.34. Select ATOP_WiFi_24G AP under Network & Internet Menu .....	60
Figure 4.35. Input Password (Network Key) for WiFi Connection .....	61
Figure 4.36. Wi-Fi Connected Information .....	61
Figure 4.37. Whole Home Mesh System under the Network->Mesh Submenu .....	62
Figure 4.38. Enable Mesh Function in Whole Home Mesh System under the Network->Mesh Submenu .....	62
Figure 4.39. IPv6 WAN Settings under the Network->IPv6 Submenu .....	63
Figure 4.40. 802.1Q VLAN under the Network->VLAN Submenu .....	64
Figure 4.41. Overview Tab under the Network->LB and Failover Submenu.....	65
Figure 4.42. General sub-tab within the Configuration tab under Network -> LB and Failover Submenu .....	65
Figure 4.43. Interfaces sub-tab within the Configuration tab under Network -> LB and Failover Submenu.....	66
Figure 4.44. After Clicking Edit Button in the Interfaces sub-tab within the Configuration tab under Network -> LB and Failover Submenu .....	67
Figure 4.45. Members Sub-tab within the Configuration tab under Network -> LB and Failover Submenu .....	68
Figure 4.46. After Clicking Edit/Add Button in the Members Sub-tab under Network -> LB and Failover Submenu -> the Configuration Tab .....	69
Figure 4.47. In the Policies Sub-tab under Network->LB and Failover Submenu->the Configuration Tab.....	70
Figure 4.48. After Clicking Edit/Add Button in the Policies Sub-tab under Network -> LB and Failover Submenu -> the Configuration Tab .....	70
Figure 4.49. In the Rules Sub-tab under Network->LB and Failover Submenu->the Configuration Tab .....	71
Figure 4.50. After Clicking Edit/Add Button in the Rules Sub-tab under Network -> LB and Failover Submenu -> the Configuration Tab .....	72
Figure 4.51. General Configuration Subsection in the General Settings Tab under Network -> Firewall Submenu. ....	73
Figure 4.52. Zone Configuration Subsection in the General Settings Tab under Network->Firewall Submenu .....	74
Figure 4.53. After Clicking Add/Edit in Zone Configuration Subsection – Zone “Lan” under Network->Firewall Submenu->General Settings Tab.....	75
Figure 4.54. After Clicking Add/Edit in Zone Configuration Subsection – Zone “Lan” under Network->Firewall Submenu->Advanced Settings Tab .....	76
Figure 4.55. Inter-Zone Forwarding in Zone Configuration Subsection – Zone “Lan” under Network->Firewall Submenu->General Settings Tab.....	76
Figure 4.56. After Clicking Add/Edit in Zone Configuration Subsection – Zone “wan” under Network->Firewall Submenu->General Settings Tab.....	77
Figure 4.57. After Clicking Add/Edit in Zone Configuration Subsection – Zone “wan” under Network->Firewall Submenu->Advanced Settings Tab .....	78
Figure 4.58. Inter-Zone Forwarding in Zone Configuration Subsection – Zone “wan” under Network->Firewall Submenu->General Settings Tab.....	78
Figure 4.59. Port forwarding Tab in the Network->Firewall Submenu .....	79
Figure 4.60. Traffic Rules Section under the Network->Firewall Submenu->Traffic Rules Tab .....	81
Figure 4.61. Open Ports on Router Section under the Network->Firewall Submenu->Traffic Rules Tab .....	82
Figure 4.62. New Forward Rules Section under the Network->Firewall Submenu->Traffic Rules Tab .....	82
Figure 4.63. Source NAT Section under the Network->Firewall Submenu->Traffic Rules Tab.....	83
Figure 4.64. SYN Flood Protection Section under the Network->Firewall Submenu->Attack Prevention Tab .....	83
Figure 4.65. SSH Attack Prevention Section under the Network->Firewall Submenu->Attack Prevention Tab .....	84
Figure 4.66. SSH Attack Prevention Section under the Network->Firewall Submenu->Attack Prevention Tab .....	85
Figure 4.67. Port Scan Section under the Network->Firewall Submenu->Attack Prevention Tab .....	86
Figure 4.68. Network -> Static Routes Submenu.....	86
Figure 4.69. General Settings Section under the Network -> Dynamic Routes Submenu-> RIP Tab.....	87
Figure 4.70. RIP Interfaces Section under the Network -> Dynamic Routes Submenu-> RIP Tab.....	88

Figure 4.71. Access List Filters Section under the Network -> Dynamic Routes Submenu-> RIP Tab .....	88
Figure 4.72. General Settings Section under the Network -> Dynamic Routes Submenu-> OSPF Tab .....	89
Figure 4.73. OSPF Interfaces Section under the Network -> Dynamic Routes Submenu-> OSPF Tab .....	90
Figure 4.74. After Clicking Edit Button in OSPF Interfaces Section under the Network -> Dynamic Routes Submenu-> OSPF Tab .....	90
Figure 4.75. OSPF Networks Section under the Network -> Dynamic Routes Submenu-> OSPF Tab .....	92
Figure 4.76. Network -> DNS Submenu.....	92
Figure 4.77. Network -> QoS Submenu .....	93
Figure 4.78. QoS-LAN/WiFi24/WiFi5 Setting Webpage after Clicking Edit Button in the Network -> QoS Submenu .....	94
Figure 5.1. Services .....	95
Figure 5.2. Service -> Auto Reboot .....	95
Figure 5.3. Service -> Auto Reboot -> Edit.....	96
Figure 5.4. Services -> NTP -> General.....	97
Figure 5.5. Services -> NTP -> Time Servers.....	97
Figure 5.6. Services -> VPN -> OpenVPN -> Overview .....	98
Figure 5.7. Services -> VPN -> OpenVPN -> sample_server -> Edit.....	100
Figure 5.8. Services -> VPN -> OpenVPN -> sample_client -> Edit.....	102
Figure 5.9 An Example of Host-to-Host Connection .....	104
Figure 5.10 Roadwarrior Application using Host-to-Subnet Connection .....	105
Figure 5.11 Gateway Application using Host-to-Subnet Connection .....	105
Figure 5.12 An example of network application using a subnet-to-subnet connection via the SE59XX and a peer device .....	105
Figure 5.13 An example of host-network application via the subnet-to-subnet connection .....	106
Figure 5.14 An example of host-host application via the subnet-to-subnet connection .....	106
Figure 5.15 Services -> VPN -> IPSec -> Settings (Part 1) .....	107
Figure 5.16 Services -> VPN -> IPSec -> Settings (Part 2) .....	108
Figure 5.17 Services -> VPN -> IPSec -> Settings (Part 3).....	108
Figure 5.18 Services -> VPN -> IPSec -> Status .....	111
Figure 5.19. Services -> VPN -> L2TP -> Overview .....	111
Figure 5.20. Services -> VPN -> L2TP -> Xl2tpsvr -> Edit.....	112
Figure 5.21. Services -> VPN -> L2TP -> Overview .....	113
Figure 5.22. Services -> VPN -> L2TP -> Xl2tpClient -> Edit.....	113
Figure 5.23. Services -> VPN -> PPTP Server -> General Settings .....	114
Figure 5.24. Services -> VPN -> PPTP Server -> Users Manager .....	115
Figure 5.25. Services -> VPN -> PPTP Server -> Online Users .....	116
Figure 5.26 Services -> VPN -> GRE -> GRE Instance: Tun1 .....	117
Figure 5.27. Services -> VRRP -> VRRP LAN Configuration Settings .....	119
Figure 5.28. Services -> VRRP -> Check Internet Connection .....	120
Figure 5.29. Services -> GPS.....	121
Figure 5.30. Services -> MQTT -> Broker.....	122
Figure 5.31. Services -> MQTT -> Security .....	123
Figure 5.32. Services -> MQTT -> Bridge.....	123
Figure 5.33. Services -> MQTT -> Miscellaneous .....	124
Figure 6.1. System.....	126
Figure 6.2. System -> Administration -> General Settings .....	126
Figure 6.3. System -> Administrator -> Access Control -> Telnet Access .....	127
Figure 6.4. System -> Administrator -> Access Control -> SSH Access.....	128
Figure 6.5. System -> Administrator -> Access Control -> Diagnostics .....	128
Figure 6.6. System -> Administrator -> Access Control -> Diagnostics -> Ping.....	129
Figure 6.7. System -> Administrator -> Access Control -> Diagnostics -> Traceroute .....	129
Figure 6.8. System -> Administrator -> Access Control -> Diagnostics -> Nslookup .....	130
Figure 6.9. System -> Administrator -> Access Control -> Logging.....	130
Figure 6.10. System -> Firmware.....	132
Figure 6.11. Confirm message of the Firmware Upgrade.....	132
Figure 6.12. System -> Backup .....	133
Figure 6.13. System -> Reboot.....	133
Figure 7.1. System -> Logout.....	134



---

Figure 8.1. WAN/LAN Port on RJ45 with Pin Numbering of CWR5805 Device .....	136
---	-----

## List of Tables

Table 2.1 Default Settings of the Network Interfaces .....	15
Table 2.2 Default Settings for Web Login .....	15
Table 3.1. Status -> Overview .....	23
Table 3.2. Status -> System .....	24
Table 3.3. Status -> Network -> Mobile .....	26
Table 3.4. Status -> Network -> WAN .....	27
Table 3.5. Status -> Network -> LAN .....	28
Table 3.6 Status -> Network -> Wireless .....	29
Table 3.7. Status -> Network -> VRRP .....	30
Table 3.8. Status -> Network -> Access .....	31
Table 3.9. Status -> Routes – ARP .....	32
Table 3.10. Status -> Routes – Active IPv4 Routes .....	33
Table 3.11 Status→ Log → System Log .....	33
Table 3.12. Status -> System -> Kernel Log .....	34
Table 4.1 Network Software Feature Supported List .....	35
Table 4.2. Detailed Setting Parameters of the General Tab in Network->Mobile Submenu .....	37
Table 4.3. Detailed Setting Parameters of the Advanced Settings Tab in Network->Mobile Submenu .....	37
Table 4.4. Detailed Setting Parameters of the SIM Switching Tab in Network->Mobile Submenu .....	38
Table 4.5. Parameters in Data Connection Limit Configuration Subsection under Network->Mobile Submenu->SIM Switch Tab .....	39
Table 4.6. Parameters Network->Mobile Submenu->SIM Switch Tab-> SMS Warning Configuration Subsection..	40
Table 4.7 Detailed Setting in Clear Data Limit Subsection under Network->Mobile Submenu->SIM Switch Tab ....	40
Table 4.8. Parameters of Static Address Protocol in the General Setup Tab under the Network->WAN Submenu	42
Table 4.9. Parameters of DHCP Client Protocol in the General Setup Tab under the Network->WAN Submenu ....	43
Table 4.10. Setting Parameters of PPPoE Protocol in the General Setup Tab under the Network->WAN Submenu .....	44
Table 4.11. Parameters of Static Address Protocol in the Network->WAN Submenu-> the Advanced Setting Tab	45
Table 4.12. Parameters of DHCP Client Protocol in the Advanced Setting Tab under the Network->WAN Submenu .....	46
Table 4.13. Parameters of PPPoE Protocol in the Advanced Setting Tab under the Network->WAN Submenu .....	47
Table 4.14. Parameters in the Common Configuration Section under the Network->LAN Submenu .....	49
Table 4.15. Parameters in the General Setup Tab under the Network->LAN Submenu-> DHCP Section .....	50
Table 4.16. Parameters in the Advanced Settings Tab under the Network->LAN Submenu-> DHCP Section .....	50
Table 4.17. Parameters in the Static Leases Section under the Network->LAN Submenu .....	51
Table 4.18. Parameters inside Wireless Overview Section under the Network->Wireless Submenu .....	52
Table 4.19. Parameters in the Scan Webpage under the Network->Wireless Submenu->Wireless Overview Section .....	52
Table 4.20. Setting Parameters of Device Configuration after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section .....	54
Table 4.21. Setting Parameters of Interface Configuration – General Setup Tab after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section .....	55
Table 4.22. Interface Configuration – Wireless Security Tab after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section .....	55
Table 4.23. Interface Configuration – MAC-Filter Tab after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section .....	56
Table 4.24. Parameters of Common Configuration after Clicking Edit Button in the Wi-Fi 2.4GHz GuestSubsection under the Network->Wireless Submenu->the Wireless Overview Section .....	56
Table 4.25. Parameters of DHCP Server Subsection – General Tab after Clicking Edit Button in the Wi-Fi 2.4GHz Guest Subsection under the Network->Wireless Submenu->the Wireless Overview Section .....	57
Table 4.26. Parameters of DHCP Server Subsection – General Tab after Clicking Edit Button in the Wi-Fi 2.4GHz Guest Subsection under the Network->Wireless Submenu->the Wireless Overview Section .....	58
Table 4.27. Parameters in the Associated Stations Section under the Network->Wireless Submenu .....	58
Table 4.28. Parameters in the Whole Home Mesh System under the Network->Mesh Submenu .....	62
Table 4.29. Parameters of IPv6 WAN Settings under the Network->IPv6 Submenu .....	63
Table 4.30. Setting Parameters of 802.1Q VLAN under the Network->VLAN Submenu .....	64
Table 4.31. Parameters in the Overview Tab under the Network->LB and Failover Submenu .....	65

Table 4.32. General sub-tab within the Configuration tab under Network -> LB and Failover Submenu .....	65
Table 4.33. Parameters in the Interfaces sub-tab within the Configuration tab under Network -> LB and Failover Submenu .....	66
Table 4.34. Setting Parameter of the Webpage Launched after Clicking Edit Button in the Interfaces sub-tab within the Configuration tab under Network -> LB and Failover Submenu .....	68
Table 4.35. Setting Parameters of the Members Sub-tab within the Configuration tab under Network -> LB and Failover Submenu .....	69
Table 4.36. Parameters in the Members Sub-tab under Network->LB and Failover Submenu->the Configuration Tab .....	69
Table 4.37. Parameters in the Policies Sub-tab under Network->LB and Failover Submenu->the Configuration Tab after Clicking Edit/Add Button .....	70
Table 4.38. Parameters in the Policies Sub-tab under Network->LB and Failover Submenu->the Configuration Tab after Clicking Edit/Add Button .....	70
Table 4.39. Parameters in the Rules Sub-tab under Network->LB and Failover Submenu->the Configuration Tab .....	71
Table 4.40. Parameters in the Rules Sub-tab under Network->LB and Failover Submenu->the Configuration Tab after Clicking Edit/Add Button .....	72
Table 4.41. Parameters in the General Settings Tab under Network -> Firewall Submenu .....	74
Table 4.42. Parameters under the General Settings Tab under Network->Firewall Submenu-> Zone Configuration Subsection .....	74
Table 4.43. Parameters in Zone Configuration Subsection – Zone “Lan” under Network->Firewall Submenu->General Settings Tab .....	75
Table 4.44. Parameters in Zone Configuration Subsection – Zone “Lan” under Network->Firewall Submenu->Advanced Settings Tab .....	76
Table 4.45. Parameters in Zone Configuration Subsection – Zone “wan” under Network->Firewall Submenu->General Settings Tab .....	77
Table 4.46. Parameters in Zone Configuration Subsection – Zone “wan” under Network->Firewall Submenu->Advanced Settings Tab .....	78
Table 4.47. Parameters in the Port Forwards Rules Section under the Network->Firewall Submenu->Port Forwarding Tab .....	79
Table 4.48. Parameters in the New Port Forwards Rules Section under the Network->Firewall Submenu->Port Forwarding Tab .....	80
Table 4.49. Parameters in Traffic Rules Section under the Network->Firewall Submenu->Traffic Rules Tab .....	81
Table 4.50. Parameters in Open Ports on Router Section under the Network->Firewall Submenu->Traffic Rules Tab .....	82
Table 4.51. Parameters in New Forward Rules Section under the Network->Firewall Submenu->Traffic Rules Tab .....	82
Table 4.52. Parameters in the Source NAT Section under the Network->Firewall Submenu->Traffic Rules Tab ....	83
Table 4.53. Parameters in SYN Flood Protection Section under the Network->Firewall Submenu->Attack Prevention Tab .....	84
Table 4.54. Parameters in SSH Attack Prevention Section under the Network->Firewall Submenu->Attack Prevention Tab .....	84
Table 4.55. Parameters in Http/Https Attack Prevention Section under the Network->Firewall Submenu->Attack Prevention Tab .....	85
Table 4.56. Parameters in Port Scan Section under the Network->Firewall Submenu->Attack Prevention Tab .....	86
Table 4.57. Parameters in Network -> Static Routes Submenu .....	86
Table 4.58. Parameters in the General Settings Section under the Network -> Dynamic Routes Submenu-> RIP Tab .....	87
Table 4.59. Parameters in the RIP Interface Section under the Network -> Dynamic Routes Submenu-> RIP Tab .....	88
Table 4.60. Parameters in the Access List Filters Section under the Network -> Dynamic Routes Submenu-> RIP Tab .....	88
Table 4.61. Parameters in the General Settings Section under the Network->Dynamic Routes Submenu->OSPF Tab .....	89
Table 4.62. Parameters in the OSPF Interfaces Section under the Network->Dynamic Routes Submenu->OSPF Tab .....	90
Table 4.63. Parameters of OSPF Protocol after Clicking Edit Button in the OSPF Interfaces Section under the Network->Dynamic Routes Submenu->OSPF Tab .....	91
Table 4.64. Parameters in the OSPF Networks Section under the Network->Dynamic Routes Submenu->OSPF Tab .....	92

Table 4.65. Parameters in the Network -> DNS Submenu .....	93
Table 4.66. Parameters in the QoS-LAN/WiFi24/WiFi5 Setting Page after Clicking Edit Button in the Network -> QoS Submenu .....	94
Table 5.1. Service -> Auto Reboot -> Edit .....	96
Table 5.2. Services -> NTP -> General .....	97
Table 5.3. Services -> NTP -> Time Servers .....	98
Table 5.4. Services -> VPN -> OpenVPN -> Overview .....	98
Table 5.5. Services -> VPN -> OpenVPN -> sample_server -> Edit .....	100
Table 5.6. Services -> VPN -> OpenVPN -> sample_client -> Edit .....	102
Table 5.7 Services -> VPN -> IPSec -> Settings .....	108
Table 5.8 Services -> VPN -> IPSec -> Status .....	111
Table 5.9. Services -> VPN -> L2TP -> Xl2tpsvr -> Edit .....	112
Table 5.10. Services -> VPN -> L2TP -> Xl2tpClient -> Edit .....	113
Table 5.11. Services -> VPN -> PPTP Server -> General Settings .....	114
Table 5.12. Services -> VPN -> PPTP Server -> Users Manager .....	115
Table 5.13. Services -> VPN -> PPTP Server -> Online Users .....	116
Table 5.14 Services -> VPN -> GRE -> GRE Instance: Tun1 .....	117
Table 5.15. Services -> VRRP -> VRRP LAN Configuration Settings .....	119
Table 5.16. Services -> VRRP -> Check Internet Connection .....	120
Table 5.17. Services -> GPS .....	121
Table 5.18. Services -> MQTT -> Broker .....	122
Table 5.19. Services -> MQTT -> Security .....	123
Table 5.20. Services -> MQTT -> Bridge .....	123
Table 5.21. Services -> MQTT -> Miscellaneous .....	124
Table 6.1. System -> Administration -> General Settings .....	127
Table 6.2. System -> Administrator -> Access Control -> Telnet Access .....	127
Table 6.3. System -> Administrator -> Access Control -> SSH Access .....	128
Table 6.4. System -> Administrator -> Access Control -> Logging .....	131
Table 8.1. Hardware Specification .....	135
Table 8.2. Assignment for RJ-45 Connector of CWR5805 Device .....	136

## 1 Introduction

### 1.1 Overview

Atop's AWR (**A**ccess Point **W**ireless **R**outer), CWR (**C**ellular **W**ireless **R**outer) and ER (**E**thernet **R**outer) 5805 series are the product lines of powerful industrial routers. The 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 and 5GHz), while users' Wi-Fi devices can conveniently connect to them via any chosen band.

CWR5805 supports both 5G NR (New Radio) and 4G LTE (Long Term Evolution) network. End devices can connect with it through a wireless connection. CWR5805 is also known as 5G CPE (Customer Premises Equipment) or 5G FWA (Fixed Wireless Access). It has a dual-SIM card backup to ensure a stable wireless connection. The Ethernet WAN and the 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 lets them share a high-speed cable or ADSL Internet connection.

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

By adding a compact 5G/LTE CWR5805 router in front of a wired-line WAN connection, the connectivity downtime can be resolved. As shown in Figure 1.1, once CWR5805 router senses that a wired WAN is lost or disrupted, it will automatically switch to 5G/LTE connection as a source of the Internet to provide a continuous Internet service to connected devices. Wired Internet Connection can then be shared among sensors within the IOT system via Ethernet, and to a 4K monitor via Wi-Fi.

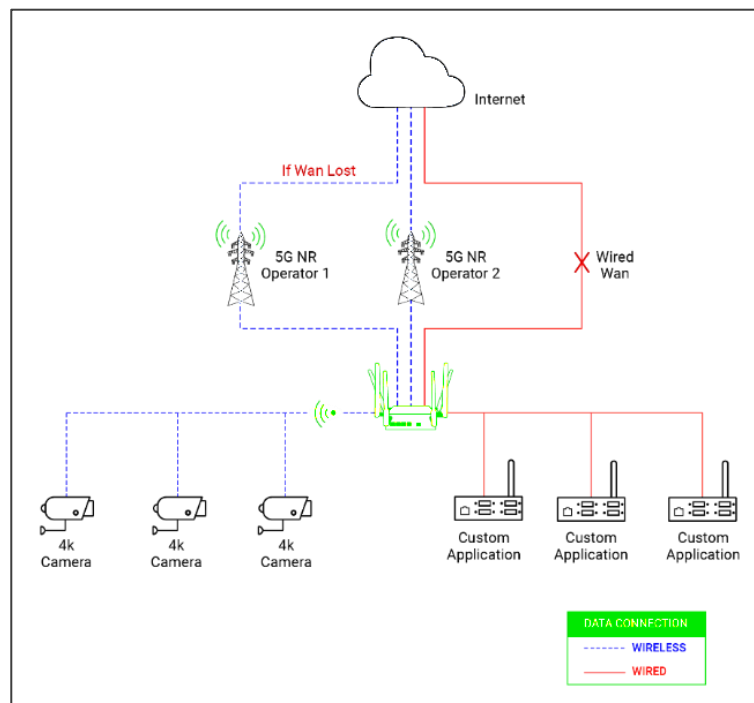


Figure 1.1 . An Example of Wired and Wi-Fi Devices Connected to the Internet Via CWR5805

*Note: Throughout 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 Base-T WAN
- 4 x RJ45 for 10/100/1000Mbps Base-T LAN
- Integrated DHCP server with dynamic and static IP address assignment
- Native firewall using NAT (Network Address Translation) technology
- Firewall and VPN (Virtual Private Network) for security connection
- Backup WAN interfaces for connection reliability
- 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 Features 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 Features 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
- GPS option for location service
- Time synchronization with GPS
- 1x micro-SD slot for flexible use

## 2 Getting Started

This chapter explains how to access the AWR5805/CWR5805/ER5805 routers for the first time. Herein after the device will be called xxR5805.

Users can access the managed switch easily using their web browser. We recommend Internet Explorer 8 or 11, Firefox 44, and Chrome 48 or later versions. Next, we will introduce the managed switch's functions through the web browser management.

### 2.1 Default Factory Settings

Below is the list of default factory settings. This information will be used during the login process. The computers accessing the xxR5805 router should have the same subnet's IP addresses and the same subnet mask. The xxR5805 default network parameters are listed in the table below.

Table 2.1 Default Settings of the Network Interfaces

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

The WebGUI's default username and password for login are listed in the table below. Please be careful when inputting them since both username and password are case sensitive.

Table 2.2 Default Settings for Web Login

Login Parameter	Default Values
Username	admin
Password	default

#### 2.1.1 Reset Button

If you forget the password or cannot access the device's web configuration, you can use the device's RESET button to restore the factory default configuration. However, this means you will lose all of your previous configurations. The password will also be reset to the factory default setting, and the LAN's IP address will be set as "192.168.1.1". Users are advised to view the device label for the default password. To reset the device, follow these steps:

1. Make sure that 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 can be used for testing network connection to xxR5805's LAN interfaces. A network cable such as unshielded twisted pair (UTP) with RJ45 connectors is also required for the Ethernet LAN interface. A 5G/LTE Nano-SIM card is used 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 (access point) interface of the device.

Follow the steps outlined below to set up a network connection 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 a xxR5805's LAN port socket and the other end to the PC's Ethernet port socket.

In the xxR5805 device, the IPv4 DHCP server is enabled by default for the LAN interfaces. It will dynamically assign an IP address to any device that enables IPv4 DHCP client in its Ethernet. The default IP address of CWR5805 is **192.168.1.1**, and the dynamic IP address of a LAN port ranges 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 DHCP protocol mode of the WAN interface on the xxR5805 is set to DHCP client. On the Cable/ADSL modem, make sure that an IPv4 DHCP server is enabled for its Ethernet port interface. It 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. Note that the SIM card slots of CWR5805 support Nano-SIM cards only. 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 correctly and firmly connected to the CWR5805 device. 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, launch the Network Connections window. Then, select an **Ethernet** icon before right clicking on **properties** to launch the **Ethernet Properties** dialog window, as shown in Figure 2.1. Next, click to highlight the **Internet Protocol Version 4 (TCP/IPv4)** item before clicking the **Properties** button to launch the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog window.

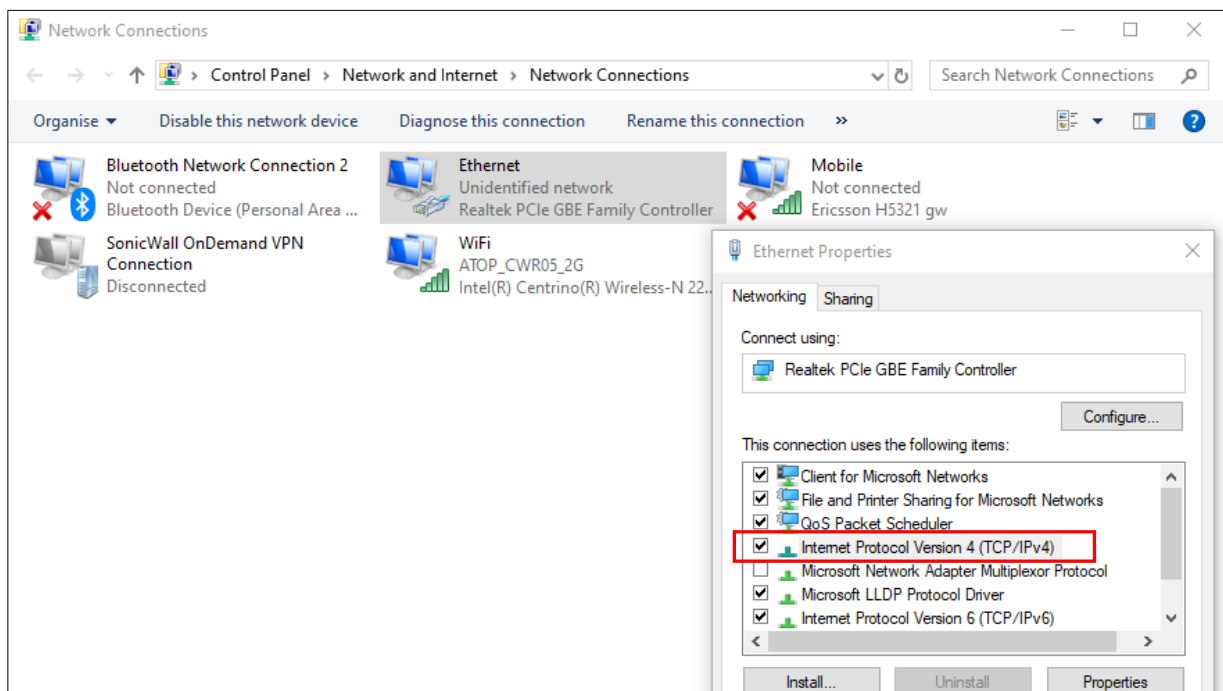


Figure 2.1. Ethernet Properties Dialog Window



Then, as shown in Figure 2.2, 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.

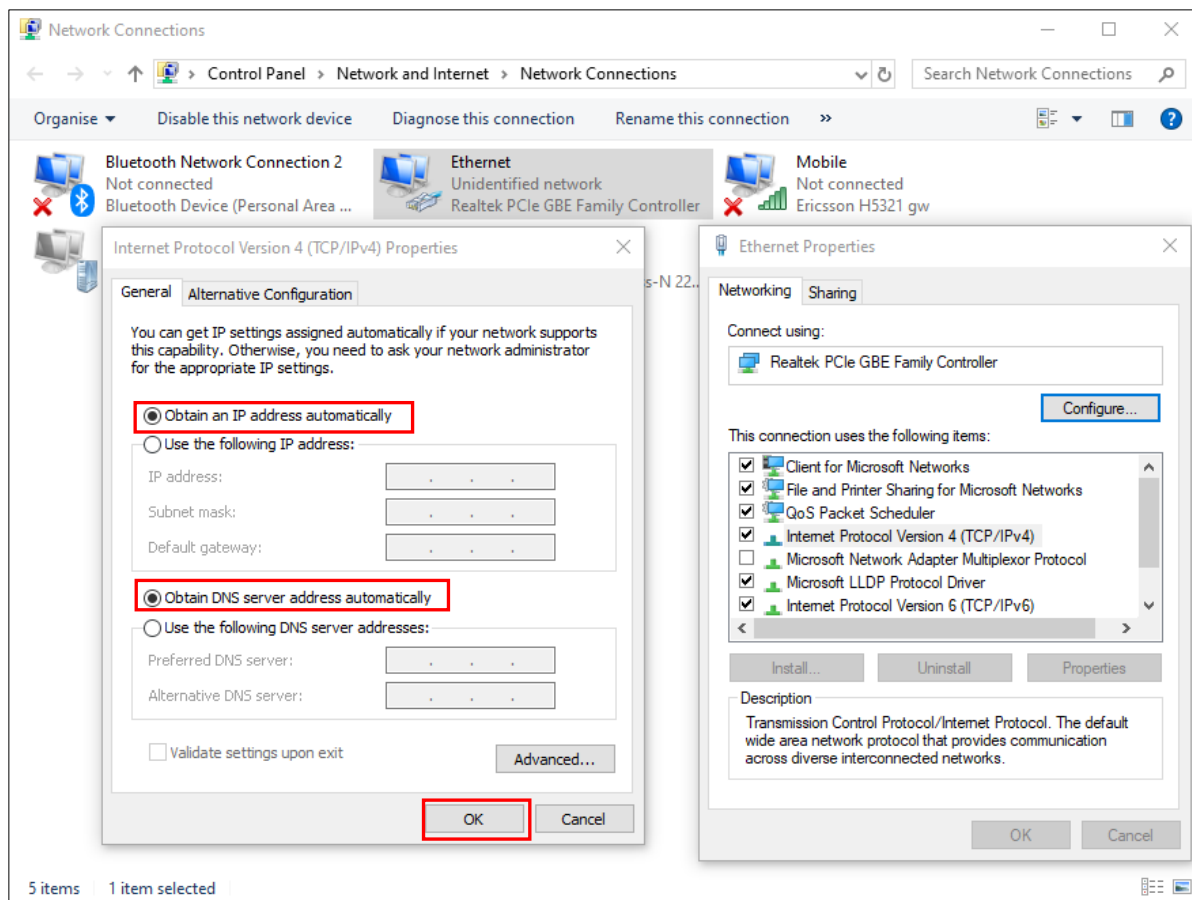


Figure 2.2. Internet Protocol Version 4 Properties Dialog Window

Next after connection is ready, select the **Ethernet** icon again and double-click mouse to enter the Ethernet Status dialog window, as shown in Figure 2.3.

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 Server 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 192.168.1.2 which is within the dynamic IP address range of 192.168.1.100 to 192.168.1.250.

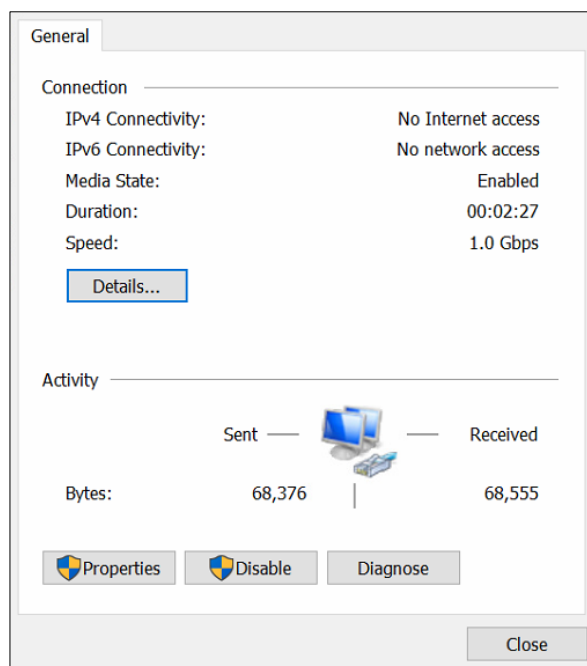


Figure 2.3. Status Dialog Window

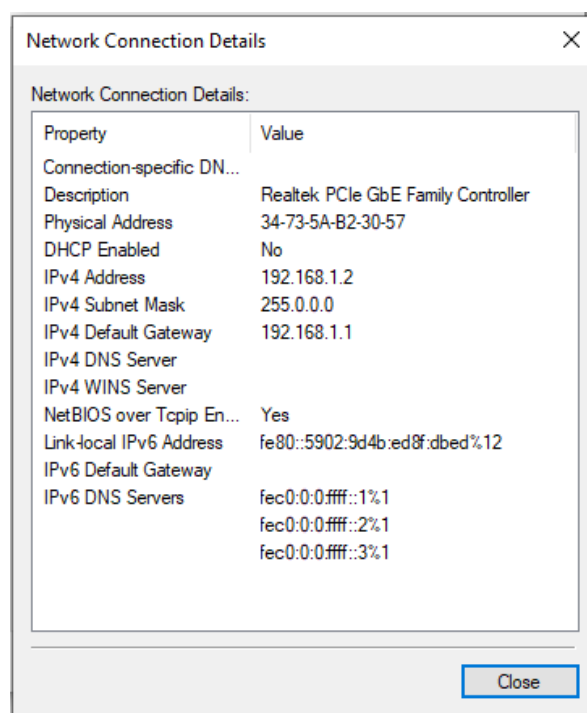


Figure 2.4. Details on the Network Connection

## 2.3 Login Process and Main Window Interface

To change the configuration of the device, you have to log in first. This can simply be done in the following steps.

A login authorization is required before you can access to the WebUI (Web Graphic User Interface) 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 **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 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 Figure 2.5.

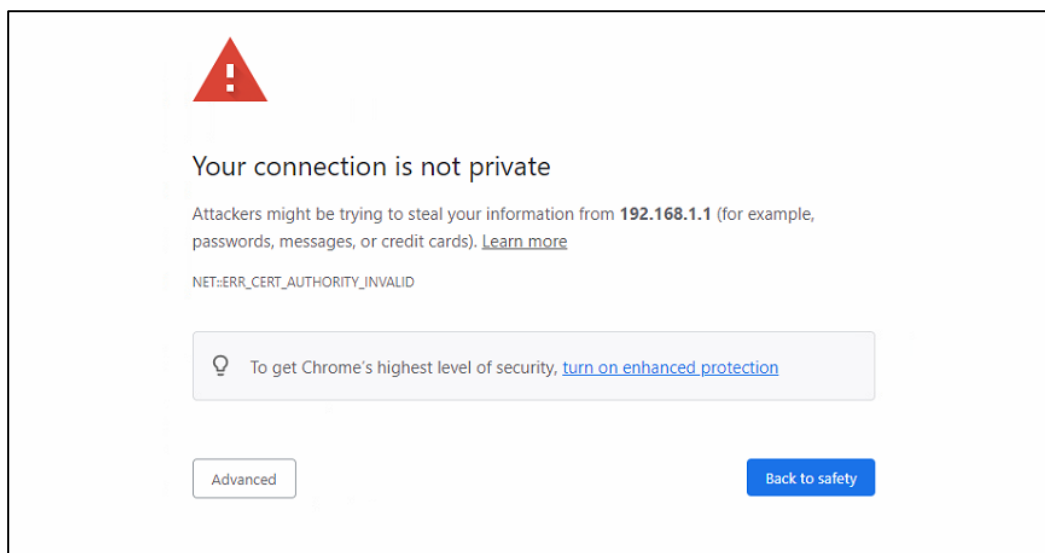


Figure 2.5. Warning Dialog due to Invalid Certificate

4. Once the **Advanced** button is clicked, an explanation will appear below the **Advanced** button, as shown in Figure 2.6. Here at the bottom of the web page, there is a hyperlink that the users can click to access the WebUI.

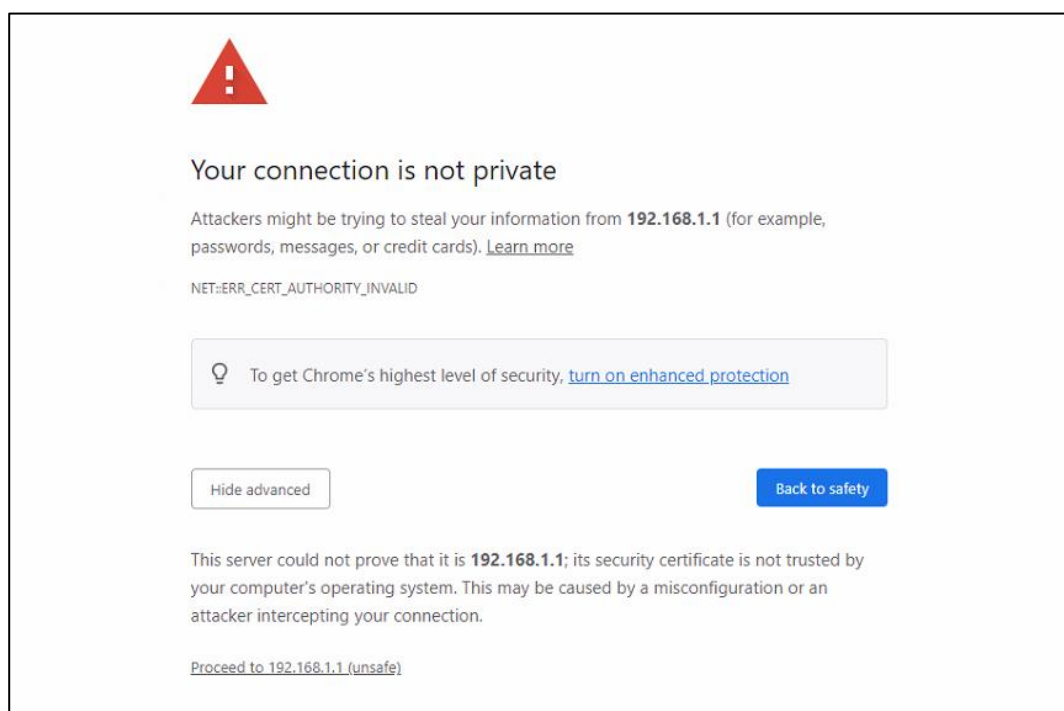


Figure 2.6. Warning Dialog of Misconfiguration/Intercepting

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, as shown in Figure 2.7. The user

can enter a **Username** and a **Password** to access the managed switch. Then, clicking on the **Login** button.

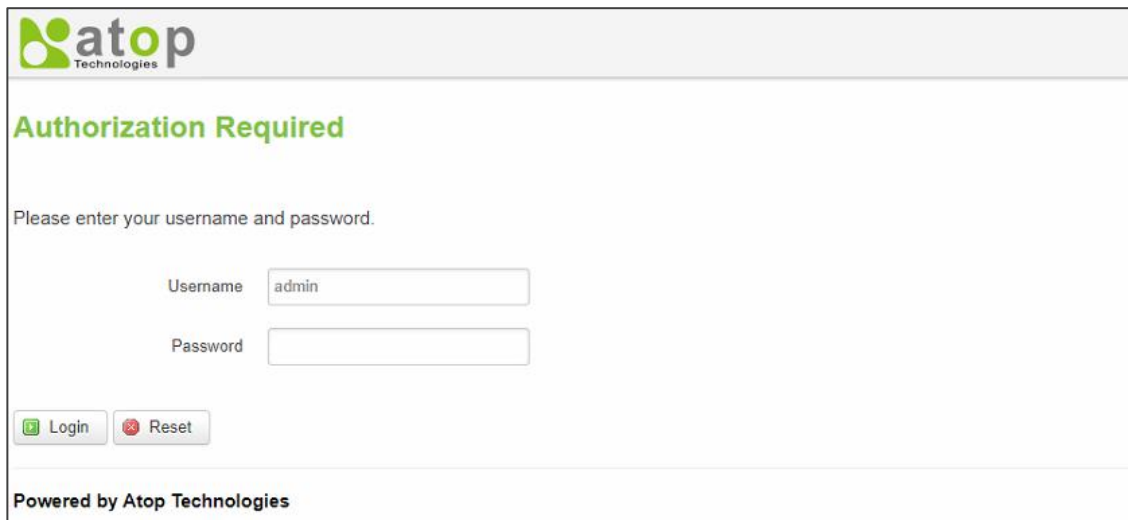


Figure 2.7. Authorization Required Webpage

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

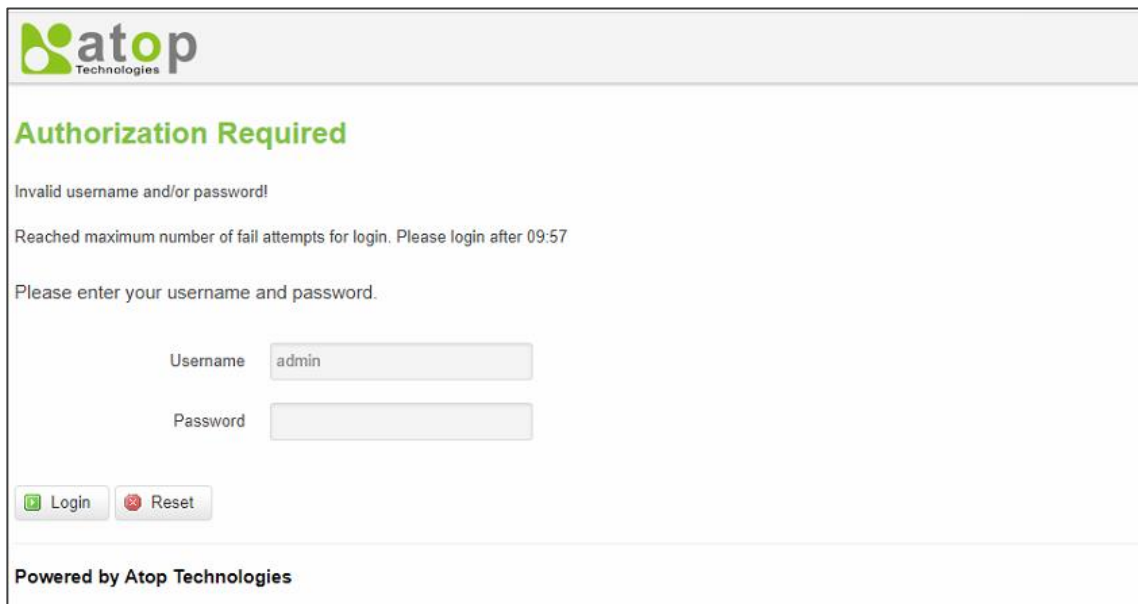
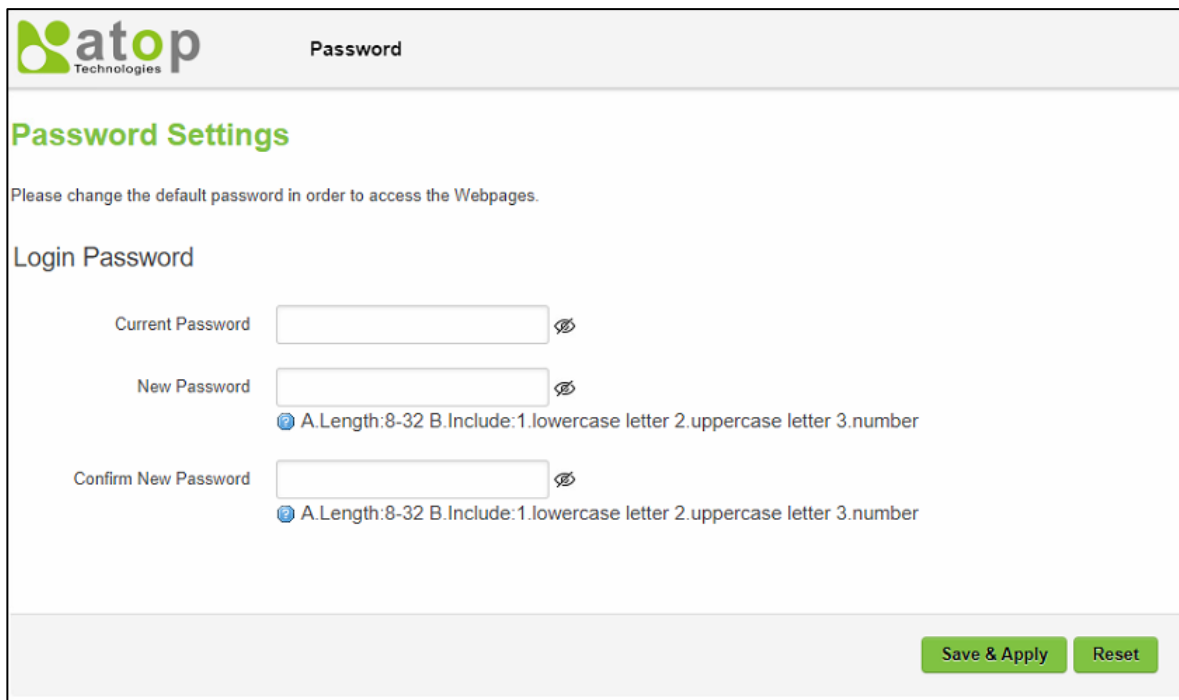


Figure 2.8. Invalid Username and/or Password

7. For security reason, you are immediately prompted to change the factory default password for the "admin" account as shown in Figure 2.9. After you entered the new password and confirmed the new password, click on the **Save & Apply** button. Otherwise, click on the **Reset** button to discard the change.

Note: The password is case-sensitive.



atop Technologies Password

### Password Settings

Please change the default password in order to access the Webpages.

Login Password

Current Password

New Password

A.Length:8-32 B.Include:1.lowercase letter 2.uppercase letter 3.number

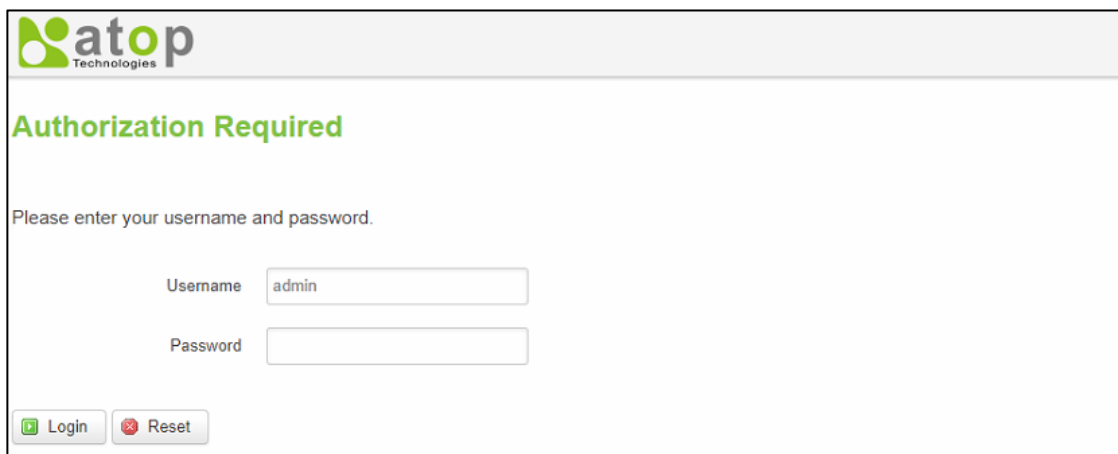
Confirm New Password

A.Length:8-32 B.Include:1.lowercase letter 2.uppercase letter 3.number

Save & Apply Reset

Figure 2.9. Prompt to Change Password

8. Input a new password.



atop Technologies

### Authorization Required

Please enter your username and password.

Username

Password

Login Reset

Figure 2.10. Authorization Required Webpage

**Note:**

1. Any unauthorized login to the xxR5805 router 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 device's information, current network information, as well as real-time traffic statistics of each network interface.

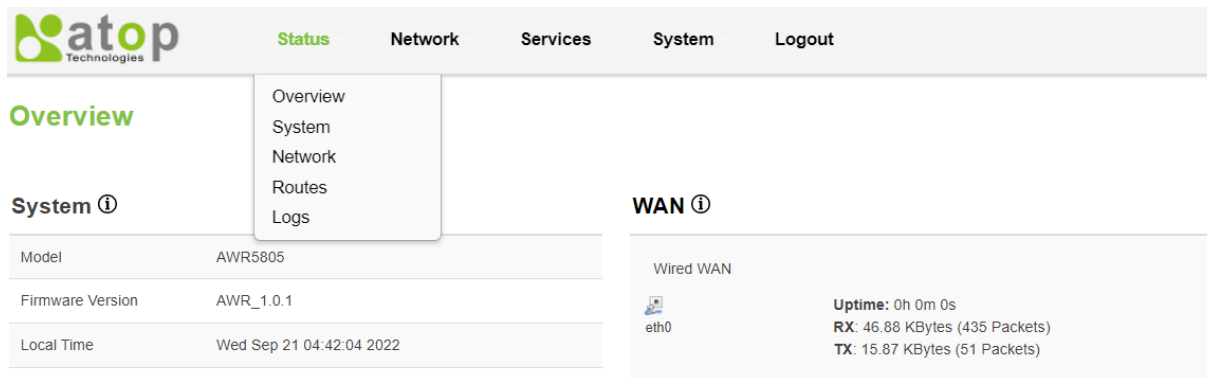


Figure 3.1. Main Page

#### 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. Due to different supporting features, CWR/AWR5805 have Mobile and Wireless sections while ER5805 does not.

This screen is the first webpage you see when you log into the CWR/AWR/ER5805. It also appears every time you click the **Status** icon in the navigation panel (the pull-down menus on the top of the webpage). The **Status** screen displays the CWR/AWR5805's connection information, wireless, mobile information, and traffic statistics.

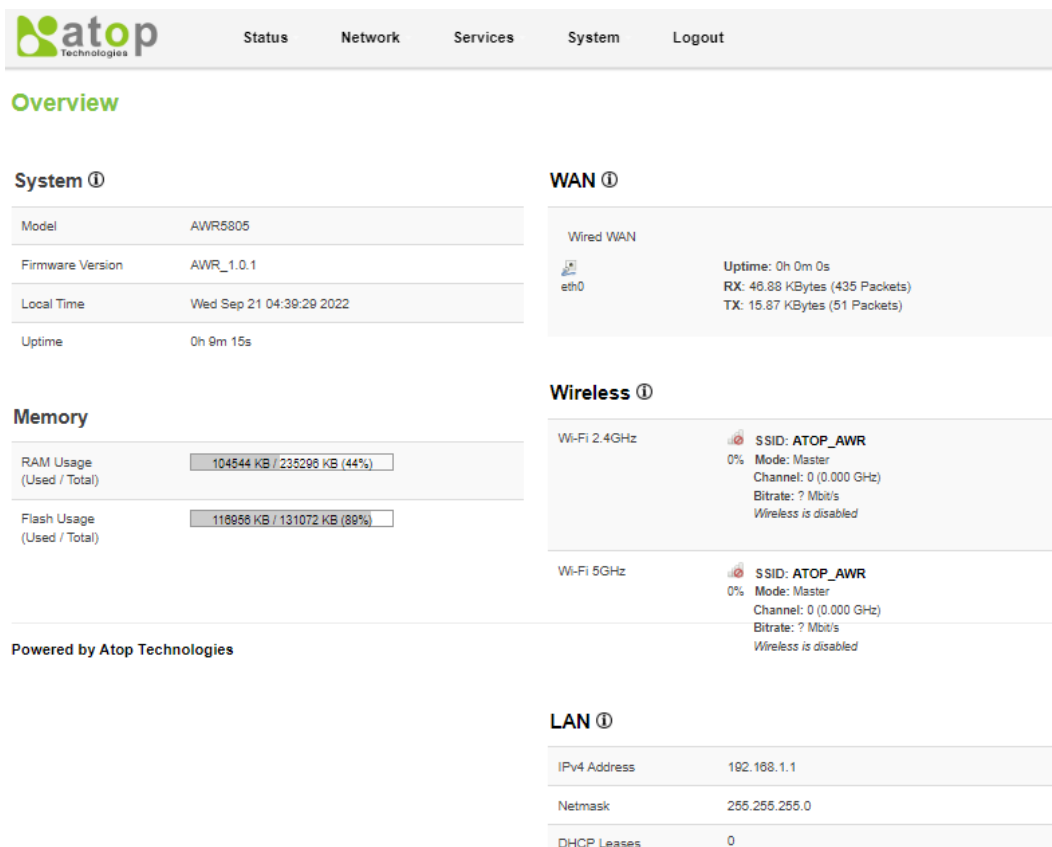



Figure 3.2. Status -&gt; Overview

Table 3.1. Status -&gt; Overview

Field	Description
System	
Model	The model name of the device.
Firmware Version	The current firmware version used on the device.
Local Time	Date and time information with time zone offset. The time zone offset can be selected on the Time zone field of the <b>System</b> webpage.
Uptime	Uptime measures the length of time that the device 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 3.3 shows the webpage of the **System** submenu under the **Status** menu. This webpage provides information about the device such as Hostname, Model, Firmware version, Kernel version, Local time, Uptime, and Load average (1min, 5min, 15min). Table 3.2 provides description of each field under the System Information webpage.



The screenshot displays the Atop Technologies router's status page. At the top, there is a navigation bar with the Atop Technologies logo and several menu items: Status, Network, Services, System, and Logout. Below this, the 'System Information' section is highlighted in green. Under 'System Information', there is a 'System' subsection. This subsection contains a table with the following data:

Hostname	AtopTechnologies
Model	AWR5805
Firmware version	AWR_1.0.1
Kernel version	4.4.60
Local time	Wed Sep 21 04:44:19 2022
Uptime	0h 14m 6s
Load average (1min, 5min, 15min)	0.00, 0.01, 0.02

At the bottom of the page, it says 'Powered by Atop Technologies'.

Figure 3.3. Status -&gt; System

Table 3.2. Status -&gt; 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 current firmware version used on the device
Kernel Version	The current kernel version used 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 the device 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 subsection is available only in CWR5805 model.

This subsection shows the status and information of the mobile interface on the CWR5905 router. 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 (International Mobile Equipment Identity), IMSI (International Mobile Subscriber Identity), and ICCID (Integrated Circuit Card ID). Figure 3.4 shows an example of **Mobile** tab under the **Status→Network** submenu. Table 3.3 provides description of each field under the **Mobile** tab.

Click **Connect** button to connect to a 5G/LTE network, and click **Stop** button to disconnect from a network. Click on the **Refresh** button to obtain the latest status and information related to the mobile interface of the device.









StatusNetworkServicesSystemLogout

MobileWANLANWirelessVRRPAccess

### 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.

Figure 3.4. Status -&gt; Network -&gt; Mobile

Table 3.3. Status -&gt; Network -&gt; 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 subnet 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 (Integrated Circuit Card ID) number of the current SIM.
SIM card state	SIM card's state, e.g. PIN required, Not inserted, etc.
Signal strength	The signal strength of the mobile signal. Signal's strength is measured in dBm.
Service provider	The name of ISP Network Provider.
LTE band	The band number 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 of LTE.
NSA band	The current 5G NR frequency bands.
NSA RSRP	The signal of 5G NR Reference Signal Received Power.
NSA RSRQ	The signal of current 5G NR Reference Signal Received Quality.
NSA SINR	The Signal to Interference plus Noise Ratio of 5G.
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 subsection shows the **WAN** (Wide Area Network) status information of the router. This webpage in Figure 3.5 provides the current configuration of the WAN interface. The WAN webpage is divided into three parts: **WAN**, **IPv6**, and **Load Balancing and Failover Status**. The WAN part lists the status of current WAN interface and its IPv4 configuration such as IPv4 address, Netmask, Gateway, and DNS. It also provides the duration of the current connection in the field called Connected. The IPv6 part lists the current IPv6's network information of the device. The last part of the webpage shows the current status of the WAN interface which can be WAN and Mobile. The WAN interface can be Ethernet or eth0 while the Mobile interface can be wwan0. The status of each interface can be Online, Offline, or Disabled. Table 3.4 summarizes the description of each field in the WAN's webpage. To obtain the latest status of the WAN information, click on the **Refresh** button.

**atop** Technologies

Status Network Services System Logout

WAN LAN Wireless VRRP Access

### WAN Information

WAN

Interface	Wired
Type	dhcp
IPv4 address	N/A
MAC address	00:60:E9:31:02:E8
Netmask	N/A
Gateway	N/A
DNS	N/A
Connected	0h 0m 0s

IPv6

Type	dhcpv6
IPv6 address	N/A
Prefix length	N/A
Gateway	N/A
DNS	N/A
Connected	0h 0m 0s

Load Balancing and Failover Status

wan (eth0) Disabled      mobile (wwan0) Disabled

Refresh

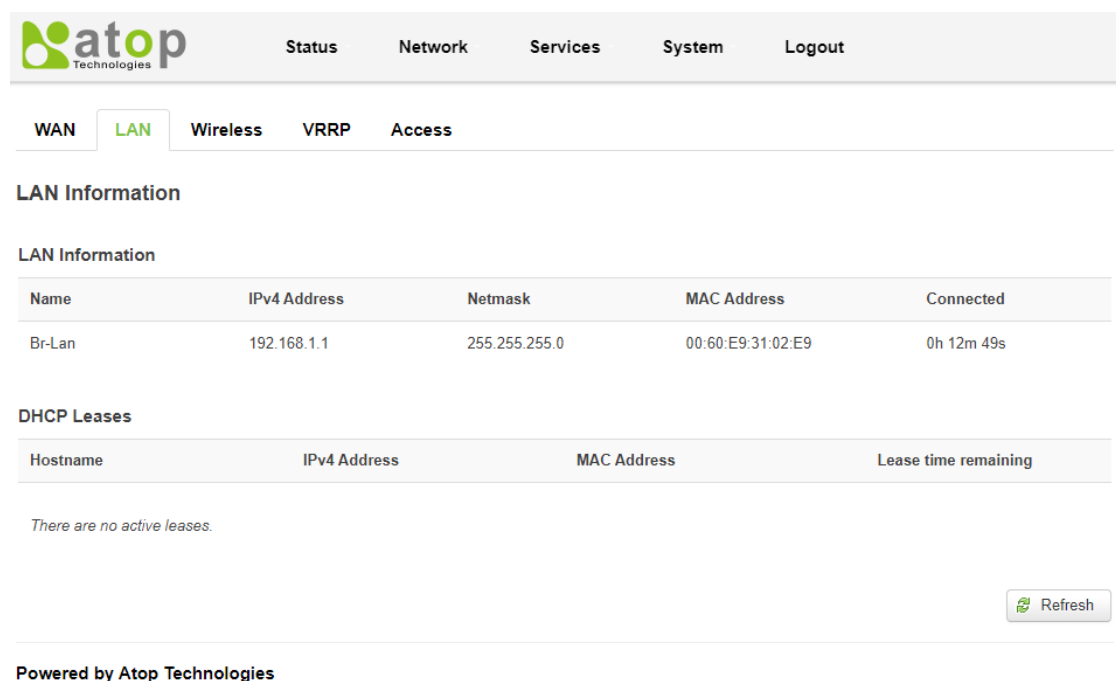
Figure 3.5. Status -&gt; Network -&gt; WAN

Table 3.4. Status -&gt; Network -&gt; 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 subsection shows the **LAN** status information of the router. Figure 3.6 depicts the LAN status webpage which is divided into two parts: LAN Information and DHCP Leases. The LAN information part lists all the current local area network interfaces. Each entry under the LAN information displays interface's Name, IPv4 Address, Netmask, MAC Address, and Connected. Under the DHCP Leases part, each entry provides the remaining lease time of a Hostname connected to the xxR5805 router with its corresponding IPv4 Address and MAC Address. To obtain the latest status of the LAN information, click on the **Refresh** button.



Powered by Atop Technologies

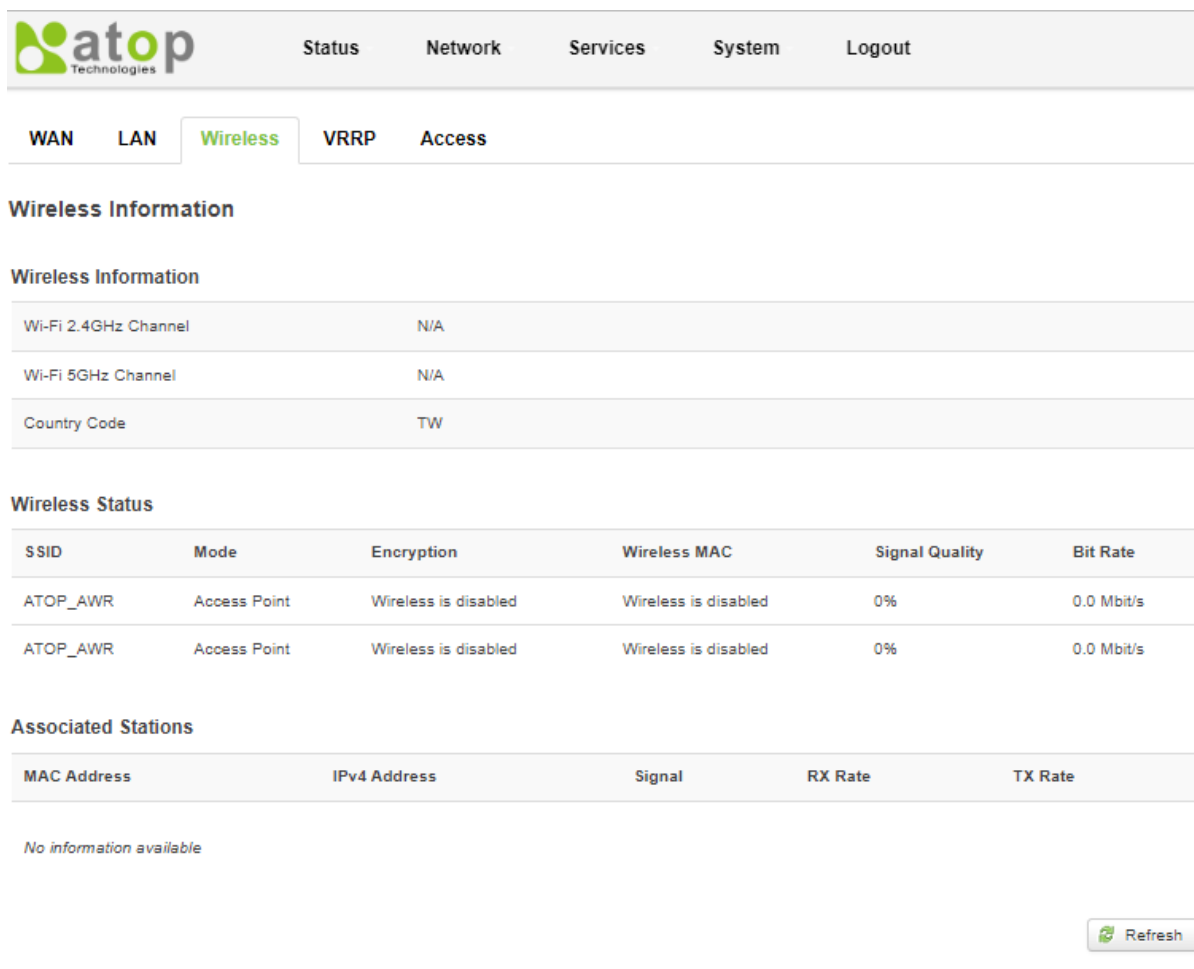
Figure 3.6. Status -> Network -> LAN

Table 3.5. 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 subsection is available in AWR5805 and CWR5805 model only. It shows the **Wireless** status information of the router. Figure 3.7 shows an example of Wireless Information webpage which is divided into three parts: **Wireless Information**, **Wireless Status**, **Associated Stations**. The first part called the Wireless Information lists the channel numbers for Wi-Fi 2.4GHz and 5GHz, and the device's Wi-Fi country code. The second part called Wireless Status lists information for each wireless local area network (WLAN) such as its SSID (Service Set ID), Mode, Encryption, Wireless MAC, Signal Quality, and Bit Rate. The last part of the webpage called Associated Stations is a table lists all the wireless clients currently connected or associated with the xxR5805 wireless router. The entry of each station contains its MAC Address, IPv4 Address, Signal (strength), RX (received data) rate, and TX (transmitted data) rate. Table 3.6 summarizes the description of each field in the Wireless Information webpage. To obtain the latest status of the Wireless information, click on the **Refresh** button.



The screenshot shows the Atop Technologies web interface. At the top, there is a navigation bar with the Atop logo and links for Status, Network, Services, System, and Logout. Below this, there is a sub-navigation bar with tabs for WAN, LAN, Wireless (selected), VRRP, and Access. The main content area is titled 'Wireless Information' and contains two sections: 'Wireless Information' and 'Wireless Status'.

**Wireless Information**

Wi-Fi 2.4GHz Channel	N/A
Wi-Fi 5GHz Channel	N/A
Country Code	TW

**Wireless Status**

SSID	Mode	Encryption	Wireless MAC	Signal Quality	Bit Rate
ATOP_AWR	Access Point	Wireless is disabled	Wireless is disabled	0%	0.0 Mbit/s
ATOP_AWR	Access Point	Wireless is disabled	Wireless is disabled	0%	0.0 Mbit/s

**Associated Stations**

MAC Address	IPv4 Address	Signal	RX Rate	TX Rate
No information available				

At the bottom right of the 'Associated Stations' section, there is a 'Refresh' button.

Powered by Atop Technologies

Figure 3.7 Status -> Network -> Wireless

Table 3.6 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.
Country Code	Country code.
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 (AWR5805/CWR5805 Only)

This subsection 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**. It can be used in case that the main router (Master) becomes unavailable. Another VRRP router (Backup) then assumes the role of Master; thus, backing up the connection. Figure 3.8 shows an example of VRRP status webpage when the router is acting as the Master, while Figure 3.9 shows an example of VRRP status webpage when the router is acting as the Backup. The VRRP Information on this page provides the **Status**, **Virtual IP**, **Priority**, and the role of the **Router**. Note that when the route is a Backup, the VRRP Information also shows the IP address of the Master behind the Master ip field. Table 3.7 summarizes the description of each field under the VRRP Information webpage. To obtain the latest status of the VRRP information, click on the **Refresh** button.

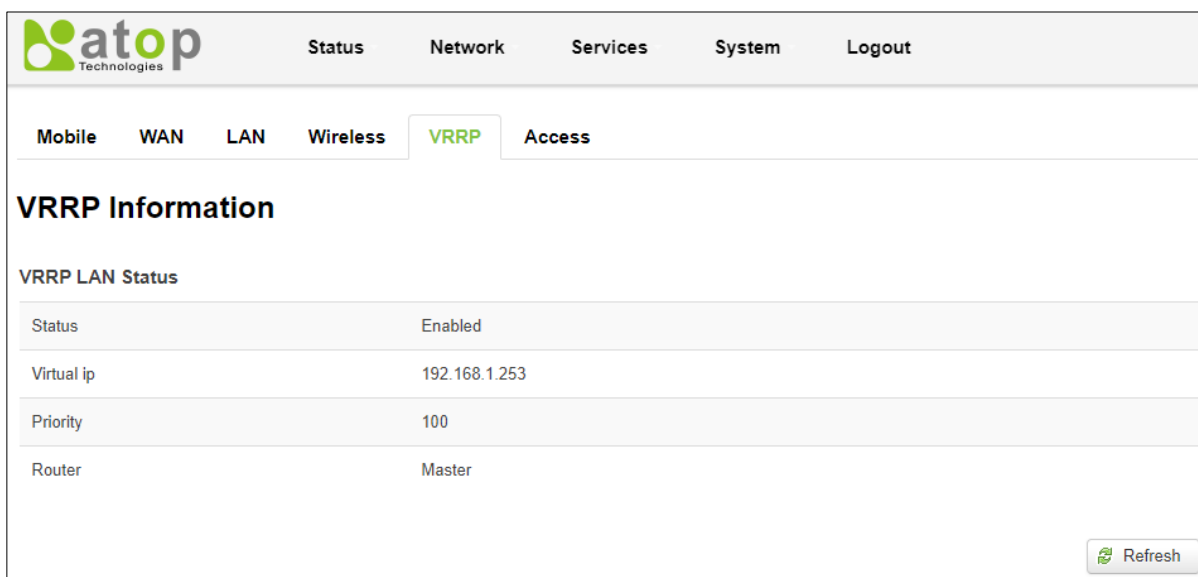


Figure 3.8. Status -> Network -> VRRP (Master)

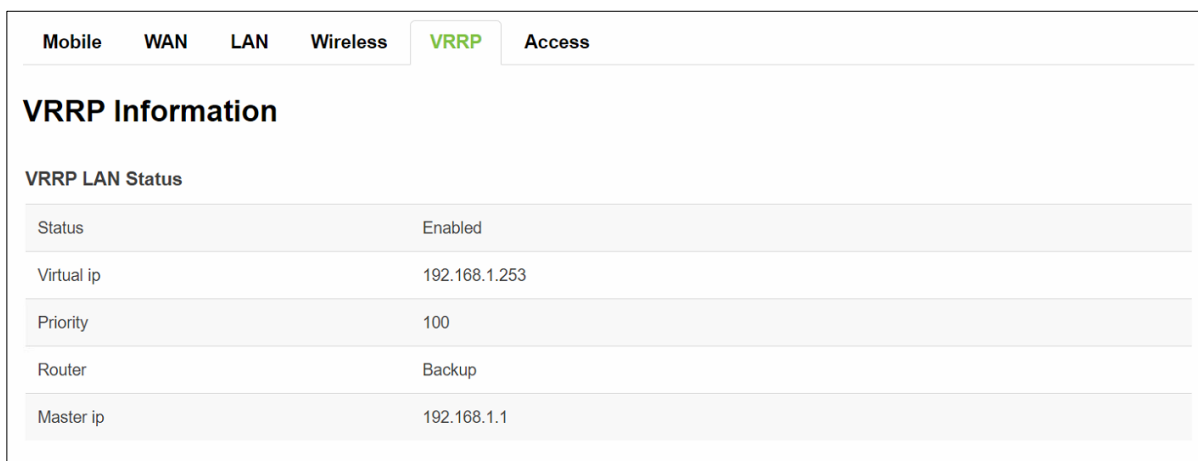


Figure 3.9. Status -> Network -> VRRP (Backup)

Table 3.7. Status -> Network -> VRRP

Field	Value	Description
Status	default: <b>disable</b>	VRRP status.
Virtual IP	default: <b>192.168.1.253</b>	Virtual IP address(-es) for LAN's VRRP (Virtual Router Redundancy Protocol) cluster.
Priority	integer [1 – 255]; default: <b>100</b>	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 address format	Master IP.

### 3.3.6 Access

This subsection displays information about local and remote active connections status. Figure 3.10 shows an example of **Access Status** webpage. It is divided into two parts: **Local Access** and **Remote Access**. Each part lists the Type of protocol, Status, Port number and number of Active Connections of application protocols such as SSH, TELNET, HTTP, and HTTPS. Table 3.8 summarizes the description of each field under the Access Status webpage. To obtain the latest status of the Access information, click on the **Refresh** button.

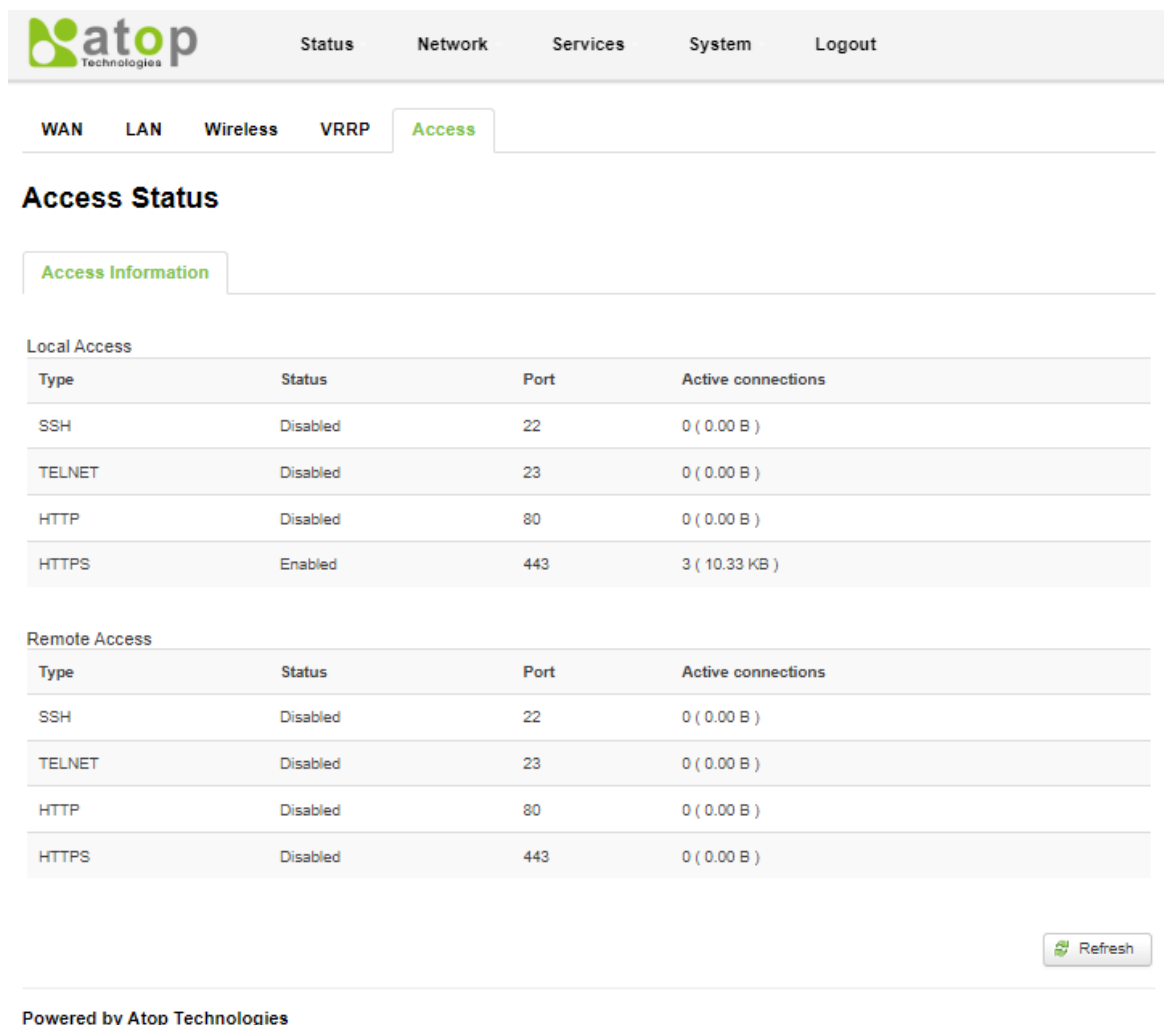


Figure 3.10. Status -> Network -> Access

Table 3.8. Status -> Network -> Access

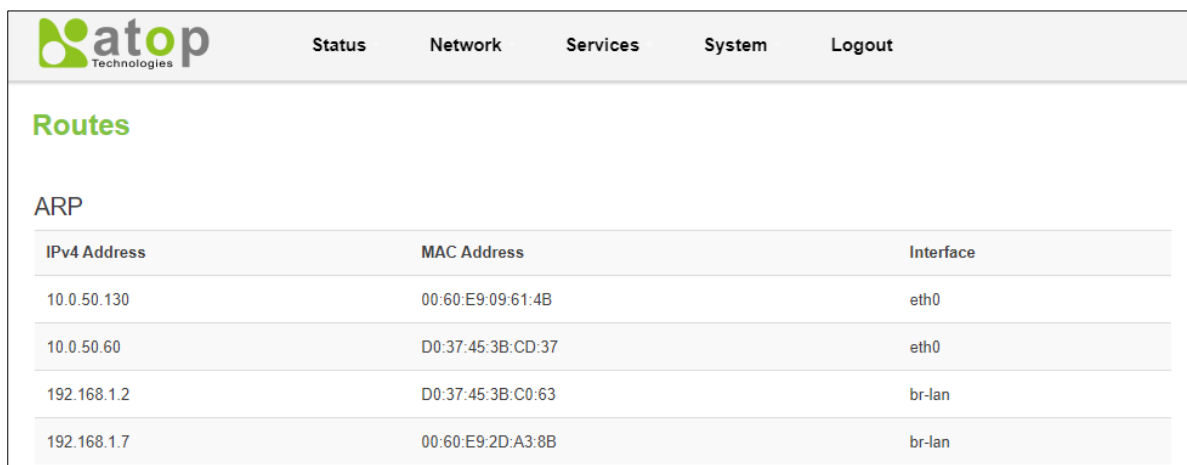
Field	Value	Description
Type	SSH/TELNET/HTTP/HTTPS	Type of connection protocol.
Status	disabled/enabled	Connection status.
Port	22/80/443	Port number used by the connection.
Active connections	integer/data usage	Count of active connections and the amount of data transmitted.

## 3.4 Routes

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

### 3.4.1 ARP

The ARP subsection 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 subsection also shows the router's routing table. Each entry in the table contains the IPv4 Address, MAC Address, and the Interface name used for the connection of the device. Figure 3.11 shows an example of ARP table. The description of each field in the ARP section is shown in the table below.



The screenshot shows the atop Technologies web interface. At the top, there are navigation tabs: Status, Network, Services, System, and Logout. Below the tabs, the 'Routes' section is active, displaying the 'ARP' table. The table has three columns: IPv4 Address, MAC Address, and Interface. It contains four entries:

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

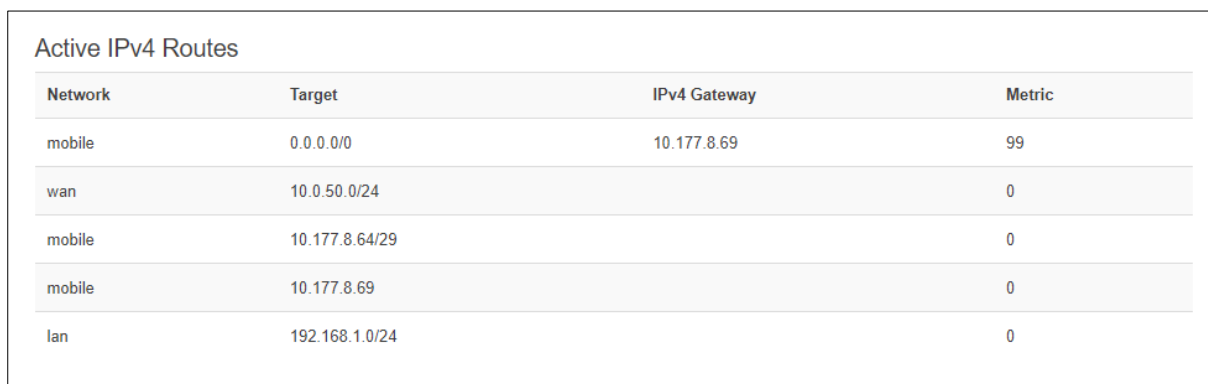
Figure 3.11. Status -> Routes – ARP

Table 3.9. 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. Examples of the routes are shown in Figure 3.12. The description of each field is shown in the table below.



The screenshot shows the 'Active IPv4 Routes' section of the atop Technologies web interface. It displays a table with four columns: Network, Target, IPv4 Gateway, and Metric. The table contains six entries:

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

Figure 3.12. Status -> Routes – Active IPv4 Routes



Table 3.10. Status -&gt; 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. The webpage substitutes troubleshooting file that can be published to the external system log server.

The screenshot displays the 'System Log' interface. At the top, there's a navigation bar with 'Status', 'Network', 'Services', 'System', and 'Logout'. Below this, there are two tabs: 'System Log' (selected) and 'Kernel Log'. The main content area shows a table of log entries. The table has four columns: 'No.', 'Date-Time', 'Log type', and 'Message'. The log entries include various system events, such as user logins, device errors, and daemon information. At the bottom of the table, it says 'Showing 1 to 10 of 3294 entries'. Below the table, there's a footer that says 'Powered by Atop Technologies'.

Figure 3.13 Status -&gt; Log -&gt; System Log

Table 3.11 Status→ Log → 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 sub-menu provides on-screen Kernel logging information. Figure 3.14 shows an example of Kernel Log webpage. The description of each field is listed in Table 3.12.

The screenshot shows the Atop Technologies web interface. The top navigation bar includes 'Status', 'Network', 'Services', 'System', and 'Logout'. Below this, there are tabs for 'System Log' and 'Kernel Log'. The 'Kernel Log' tab is selected, displaying a table of log entries. The table has three columns: 'No.', 'Timestamp', and 'Message'. The log entries show various network-related events, including bridge snooping, netlink parsing, and interface state changes. At the bottom of the page, it says 'Powered by Atop Technologies'.

No.	Timestamp	Message
00868	45.571167	__mo_netlink_receive: Enable bridge snooping!
00867	44.558851	netlink: 12 bytes leftover after parsing attributes in process 'ip'.
00866	44.559797	netlink: 12 bytes leftover after parsing attributes in process 'ip'.
00865	44.106723	br-lan: port 1(eth1) entered forwarding state
00864	43.483392	__mo_netlink_receive: Disable bridge snooping!
00863	42.111589	IPv6: ADDRCONF(NETDEV_CHANGE): br-lan: link becomes ready
00862	42.107099	br-lan: port 1(eth1) entered forwarding state
00861	42.106956	br-lan: port 1(eth1) entered forwarding state
00860	41.122377	IPv6: ADDRCONF(NETDEV_UP): br-lan: link is not ready
00859	41.118918	device eth1 entered promiscuous mode

Showing 1 to 10 of 868 entries

<< Prev Next >>

Powered by Atop Technologies

Figure 3.14. Status -> System -> Kernel Log

Table 3.12. Status -> System -> Kernel Log

Field	Description
Timestamp	The kernel log's 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.

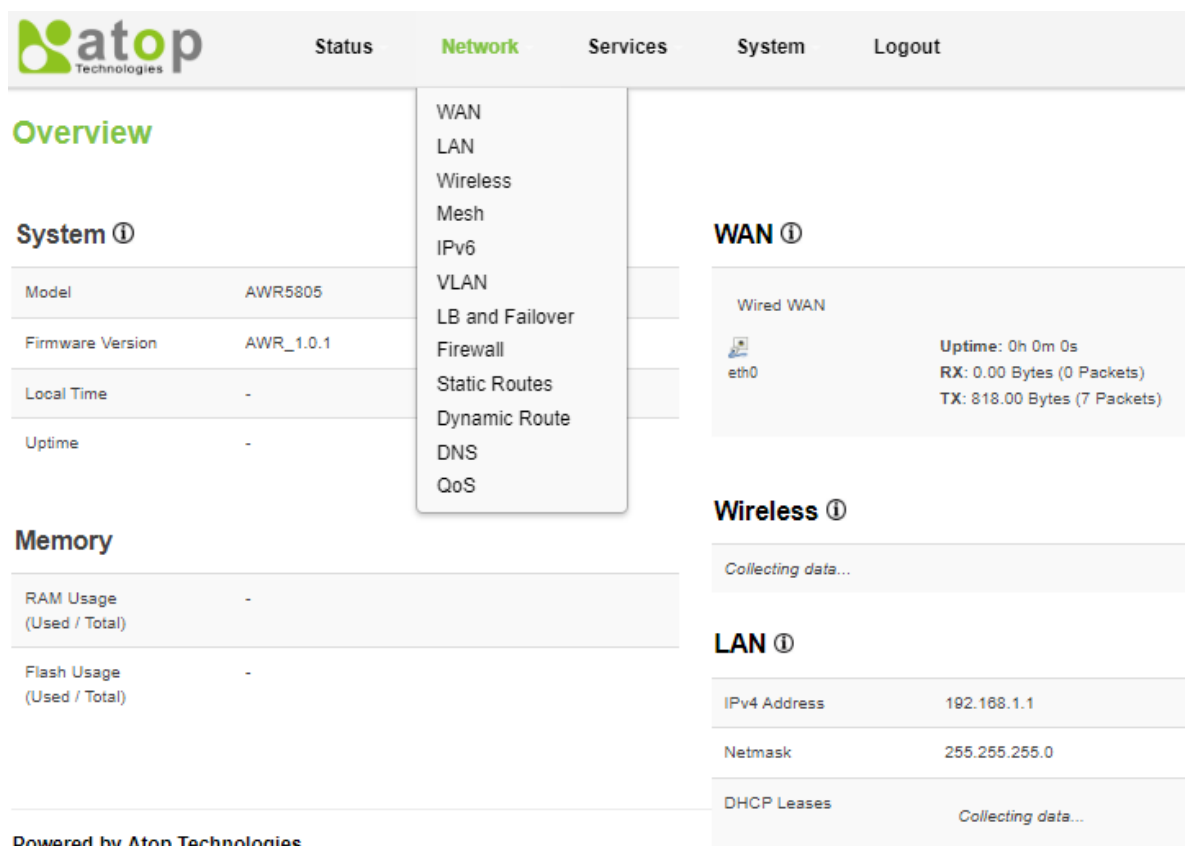


Figure 4.1. Network Overview

Table 4.1 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 Network->Mobile submenu, users can configure parameters related to the mobile data connection in three tabs: General Setup, Advanced Settings, and SIM Switch tabs.

### 4.1.1 General Setup Tab

The **Status** field in the **General Setup** tab displays the current information of the mobile interface such as uptime, MAC Address, RX, TX, and IPv4 address. Under the SIM configuration in the **General Setup** tab, user can also configure QMI (Qualcomm MSM Interface) protocol parameters for the mobile interface, as shown in the Figure 4.2. Only the APN (Access Point Name) that cannot be configured, because its value depends on the information in the ISP (Internet Service Provider) SIM card. 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. However, due to settings in most ISP SIM card dial-up, the default values of Protocol, APN, and PIN (Personal Identification Number) fields are set to: QMI Cellular, Internet, and 0000, respectively. QMI Cellular is used for 5G/LTE dial-up to Internet connection. Table 4.2 shows the detailed setting parameters of the General Tab in Network->Mobile submenu

The screenshot displays the 'Mobile' configuration page for the AWR5805/CWR5805/ER5805 device. The page is divided into three main sections: 'Common Configuration', 'SIM1 Configuration', and 'SIM2 Configuration'. The 'Common Configuration' section includes a 'Status' tab showing the following information:

- Uptime: 22h 27m 23s
- MAC Address: EE:AE:C8:50:0F:B5
- RX: 631.00 KBytes (7455 Packets)
- TX: 881.68 KBytes (8722 Packets)
- IPv4: 10.177.8.69/29

The 'SIM1 Configuration' and 'SIM2 Configuration' sections each contain the following fields:

- Protocol: QMI Cellular (dropdown menu)
- Modem device: /dev/cdc-wdm0 (dropdown menu)
- APN: internet (text input)
- PIN: 0000 (text input)
- PAP/CHAP username: (text input)
- PAP/CHAP password: (text input with toggle icon)
- Authentication Type: NONE (dropdown menu)
- Data roaming: (checkbox, unchecked)

Figure 4.2. Webpage of the General Tab in Network->Mobile Submenu

Table 4.2. Detailed Setting Parameters of the General Tab in Network-&gt;Mobile Submenu

Field	Value	Description
Protocol	default: <b>QMI Cellular</b>	The protocol which is used by the mobile interface.
Modem Device	default: <b>/dev/cdc-wdm0</b>	QMI device node.
APN	default: <b>internet</b>	An Access Point Name (APN) is the name of a gateway between a 5G/LTE mobile network and a local network. Its value is set based on the contract between the operator and the subscriber. When a mobile device is making a data connection, it must relay its configured APN to the carrier. After received it, carrier will assign some connection parameters (e.g., security and priority level) that are suitable to the pre-agreed contract.
PIN	default: <b>0000</b>	A password that is used for authenticating the modem to the SIM card.
PAP/CHAP Username	default: <b>none</b>	Username for PAP/CHAP authentication.
PAP/CHAP Password	default: <b>none</b>	Password for PAP/CHAP authentication.
Authentication Type	PAP/CHAP (both)/ PAP/CHAP/None/Custom default: <b>none</b>	Authentication method that the 5G/LTE carrier uses to authenticate new connections on its network. If PAP or CHAP is selected, users will also be required to enter a Username and password.
Data Roaming	default: <b>disable</b>	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.

#### 4.1.2 Advanced Settings Tab

In the **Advanced Setting** tab under the Network->Mobile submenu, you can configure network functionalities in more detail based on your requirement for the mobile interface. Figure 4.3 shows the webpage of the advanced setting tab in Network->Mobile submenu. Table 4.3 shows the detailed setting parameters of the advanced settings tab in Network->Mobile submenu.

Figure 4.3. Webpage of the Advanced Setting Tab in Network-&gt;Mobile Submenu

Table 4.3. Detailed Setting Parameters of the Advanced Settings Tab in Network-&gt;Mobile Submenu

Field	Value	Description
Bring Up on Boot	default: <b>enable</b>	Specify whether or not to bring up the WAN interface on the boot.
Use Gateway Metric	default: <b>99</b>	The priority of the gateway on the WAN interface. A routing table entry is generated based on this field. User can alter the metric of that entry by changing this field.

### 4.1.3 SIM Switch

In the **SIM Switch** tab under the Network->Mobile submenu, users can configure switching the current SIM card to the other SIM card when the 5G/LTE network conditions are proper. Figure 4.4 shows the webpage of the SIM Switch tab in Network->Mobile submenu. Table 4.4 shows the detailed setting parameters of the SIM Switching tab in Network->Mobile submenu.

Figure 4.4. Webpage of the SIM Switch Tab in Network->Mobile Submenu

Table 4.4. Detailed Setting Parameters of the SIM Switching Tab in Network->Mobile Submenu

Field	Values	Description
Primary SIM Card	SIM1/SIM2; default: <b>SIM1</b>	Specify the SIM card slot that is used for 5G/LTE dial-up as the primary SIM card.
Automatic Switching	Enable/Disable; default: <b>disable</b>	If this function is checked or enabled, the 5G/LTE network status will be monitored regularly. In case that one of the conditions which are On Weak Signal/On Data Limit/No Network is matched, then the device will switch to another SIM, and use it as the primary SIM Slot.
Check Interval	5/15/30/60/120 Sec; default: <b>5</b>	The device will check whether the 5G/LTE network status is matched with what user specified in Automatic Switching or not every Check Interval.
On Weak Signal	Disable, 10%, 20%, 30%, 40%, 50%; Default: <b>disable</b>	If checked, the device detects whether the current 5G/LTE signal status is weaker than the pre-set threshold or not.
On Data Limit	Enable/Disable; default: <b>disable</b>	If checked or enabled, the device detects whether the current 5G/LTE data traffic reaches size limit or not.
No Network	Enable/Disable; default: <b>disable</b>	If checked or enabled, the device detects whether the current 5G/LTE network is unavailable or not.
Current SIM Slot	1/2; default: <b>1</b>	Display the current primary SIM card slot which is used for 5G/LTE dial-up.

#### 4.1.3.1 Data Limit Configuration

In the **Data Limit Configuration** section within the **SIM Switch** tab under the Network->Mobile submenu, you can configure the data usage limit to avoid unwanted data charges. The usage limit on the data connections can be pre-selected for each SIM card. When the usage limit is reached, the data usage warnings will be sent to notify you via SMS messages.

##### 4.1.3.1.1 Data Connection Limit Configuration

In the **Data Connection Limit Configuration** subsection, as shown in Figure 4.5, the mobile data limits of your SIM card can be customized here. 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 user. Table 4.5 shows the detailed Setting parameters in Data Connection Limit Configuration subsection under Network->Mobile Submenu->SIM Switch tab.

Figure 4.5. Data Connection Limit Configuration Subsection under Network->Mobile Submenu->SIM Switch Tab

Table 4.5. Parameters in Data Connection Limit Configuration Subsection under Network->Mobile Submenu->SIM Switch Tab

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

##### 4.1.3.1.2 SMS Warning Configuration

In the **SMS Warning Configuration** subsection, as shown in Figure 4.6, you can configure a rule for sending SMS messages, e.g., sending SMS warnings when the data usage of the CWR5805 device's SIM card is reached the specified limit. Table 4.6 shows the detailed Setting parameters in SMS Warning Configuration subsection under Network->Mobile Submenu->SIM Switch tab.

**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

Figure 4.6. SMS Warning Configuration Subsection under Network-&gt;Mobile Submenu-&gt;SIM Switch Tab

Table 4.6. Parameters Network-&gt;Mobile Submenu-&gt;SIM Switch Tab-&gt; SMS Warning Configuration Subsection

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.

#### 4.1.3.1.3 Clear Data Limit

In the **Clear Data Limit** subsection, only a **Clear** button located after the **Clear data limit** field is presented here, as shown in Figure 4.7. When users clicked this button, the counter of the data usage limit for the selected SIM card will be reset. The data usage is restarted to count again, regardless of the specified period.

**Clear Data Limit**

Clear data limit

\* 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 4.7. Clear Data Limit Subsection under Network-&gt;Mobile Submenu-&gt;SIM Switch Tab

Table 4.7 Detailed Setting in Clear Data Limit Subsection under Network-&gt;Mobile Submenu-&gt;SIM Switch Tab

Field	Description
Clear Data Limit	When user clicked the Clear button, the counter of the data usage limit for the selected SIM card is reset. The count is restarted to 0 regardless of when the clicking event is occurred in the specified period.

## 4.2 WAN

A **Wide Area Network** (WAN) is a telecommunication network or computer network that extends over a large geographical distance. For example, the Internet is a wide area network. Here, there are three protocols supported for WAN communications: Static Address, DHCP Client, and PPPoE. Under the Network->WAN submenu, there are two tabs here: General Setup, and Advanced Settings. When user select supported protocol in the General Setup tab, the setting parameters in Advanced Settings tab are also changed accordingly. Here, the setting parameters under the General Setup are discussed first in Section 4.2.1. Then, the setting parameters under the Advanced Settings will be followed in Section 4.2.2.



### 4.2.1 General Setup

In the General Setup tab under the Network->WAN submenu, different protocols i.e., Static Address, DHCP Client, PPPOE for the WAN interface can be configured. Figure 4.9 shows the webpage after selecting Network->WAN submenu. User can switch between Static, DHCP, or PPPoE protocol by selecting the protocol that user wants to use and then pressing Switch Protocol. The default protocol is set to DHCP client where the WAN interface can get a dynamic IPv4 address from its connected Ethernet port of a Cable/ADSL modem. Static address is the simplest form of configuration but it is a fixed and inflexible setting. PPPoE allows connection of multiple hosts on a single Ethernet local area network to a remote site via a common device such as a cable, a DSL modem, and a wireless connection to the internet. PPPoE encapsulates Point-to-Point Protocol (PPP) frames inside Ethernet frames while providing connectivity across Ethernet networks. PPoE supports managing multiple client systems, authenticating their access to its services and tracking customer data usage. Also, it supports services such as data encryption and compression.

atop Technologies

Status Network Services System Logout

## WAN

### Common Configuration

**General Setup** Advanced Settings

Status eth0 Uptime: 0h 0m 0s  
MAC Address: 00:60:E9:31:02:E8  
RX: 0.00 Bytes (0 Packets)  
TX: 818.00 Bytes (7 Packets)

Protocol DHCP client after selecting one of the protocols to switch to Static address

Static address  
DHCP client  
PPPoE

Really switch protocol? ☐ Switch protocol

Save & Apply Reset

Powered by Atop Technologies

Figure 4.8. General Setup Tab under the Network->WAN Submenu

#### 4.2.1.1 Static Address Protocol

After selecting **Static Address protocol** and clicking **Switch Protocol button**, user will be allowed to configure IPv4 address, IPv4 netmask, IPv4 address gateway, and add some custom DNS servers. User can click icon at the rightmost of the input textbox to add more DNS server, or click icon to delete any of no longer wanted DNS server. Figure 4.9 shows the webpage when the Static Address protocol in the General Setup Tab under the Network->WAN Submenu is selected.

atop Technologies

Status Network Services System Logout

## WAN

### Common Configuration

**General Setup** Advanced Settings

Status

eth0 Uptime: 0h 0m 0s  
MAC Address: 00:80:E9:31:02:E8  
RX: 0.00 Bytes (0 Packets)  
TX: 818.00 Bytes (7 Packets)

Protocol Static address

IPv4 address

IPv4 netmask 255.255.255.255

IPv4 gateway

Use custom DNS servers

Save & Apply Reset

Powered by Atop Technologies

Figure 4.9. Static Address Protocol in the General Setup Tab under the Network-&gt;WAN Submenu

Table 4.8. Parameters of Static Address Protocol in the General Setup Tab under the Network-&gt;WAN Submenu

Field	Value	Description
Protocol	Static/DHCP/PPPoE; default: <b>DHCP</b>	The protocol that is used by the WAN interface. This field currently supports static address, DHCP clients, and PPPoE.
IPv4 address	ip4; default: <b>none</b>	IPv4 address of the router on the WAN network.
IPv4 netmask	netmask; default: <b>none</b>	IPv4 netmask of the router, where IPv4 netmask defines size of network.
IPv4 gateway	ip4; default: <b>none</b>	The IPv4 address of the gateway of this interface. An interface's gateway is the default next-hop address to access other networks.
IPv4 broadcast	ip4; default: <b>none</b>	IPv4 broadcast are used by BOOTP and DHCP clients to find and send requests to their respective servers.
Use custom DNS servers	ip4; default: <b>none</b>	Hostname will be resolved from the input custom DNS servers. User can enter multiple DNS servers to provide redundancy in case one of the servers fails.

#### 4.2.1.2 DHCP Client Protocol

After selecting **DHCP Client protocol** and clicking **Switch Protocol button**, user will be allowed to enter a hostname; e.g., AtopTechnologies in the **Hostname to send when requesting DHCP** field. Figure 4.10 shows the webpage when the DHCP Client protocol in the General Setup Tab under the Network->WAN Submenu is selected. Table 4.9 describes the setting parameters for DHCP client.

The screenshot shows the Atop Technologies web interface. The top navigation bar includes links for Status, Network, Services, System, and Logout. The 'WAN' section is highlighted in green. Under 'Common Configuration', the 'General Setup' tab is active. The 'Advanced Settings' tab is also visible. The 'Status' section shows the interface 'eth0' with 'Uptime: 0h 0m 0s', 'MAC Address: 00:60:E9:31:02:E8', 'RX: 0.00 Bytes (0 Packets)', and 'TX: 818.00 Bytes (7 Packets)'. The 'Protocol' is set to 'DHCP client'. The 'Hostname to send when requesting DHCP' is set to 'AtopTechnologies'. At the bottom right, there are 'Save & Apply' and 'Reset' buttons.

Figure 4.10. DHCP Client Protocol in the General Setup Tab under the Network-&gt;WAN Submenu

Table 4.9. Parameters of DHCP Client Protocol in the General Setup Tab under the Network-&gt;WAN Submenu

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

#### 4.2.1.3 PPPoE Protocol

The screenshot shows the Atop Technologies web interface. The top navigation bar includes links for Status, Network, Services, System, and Logout. The 'WAN' section is highlighted in green. Under 'Common Configuration', the 'General Setup' tab is active. The 'Advanced Settings' tab is also visible. The 'Status' section shows the interface 'pppoe-wan' with 'RX: 0.00 Bytes (0 Packets)' and 'TX: 0.00 Bytes (0 Packets)'. The 'Protocol' is set to 'PPPoE'. The 'PAP/CHAP username' and 'PAP/CHAP password' fields are empty. The 'Access Concentrator' is set to 'auto' with a note 'Leave empty to autodetect'. The 'Service Name' is set to 'auto' with a note 'Leave empty to autodetect'. At the bottom right, there are 'Save & Apply' and 'Reset' buttons.

Figure 4.11. PPPoE Protocol in the General Setup Tab under the Network-&gt;WAN Submenu

After selecting **PPPoE protocol** and clicking **Switch Protocol button**, user will be allowed to input values in PAP/CHAP username and password, Access Concentrator, and Service Name fields. Figure 4.11 shows the webpage when the PPPoE protocol in the General Setup Tab under the Network->WAN Submenu is selected. 錯誤! 找不到參照來源。 describes the setting parameters for PPPoE protocol. PPPoE protocol is mainly used by DSL providers.

Table 4.10. Setting Parameters of PPPoE Protocol in the General Setup Tab under the Network->WAN Submenu

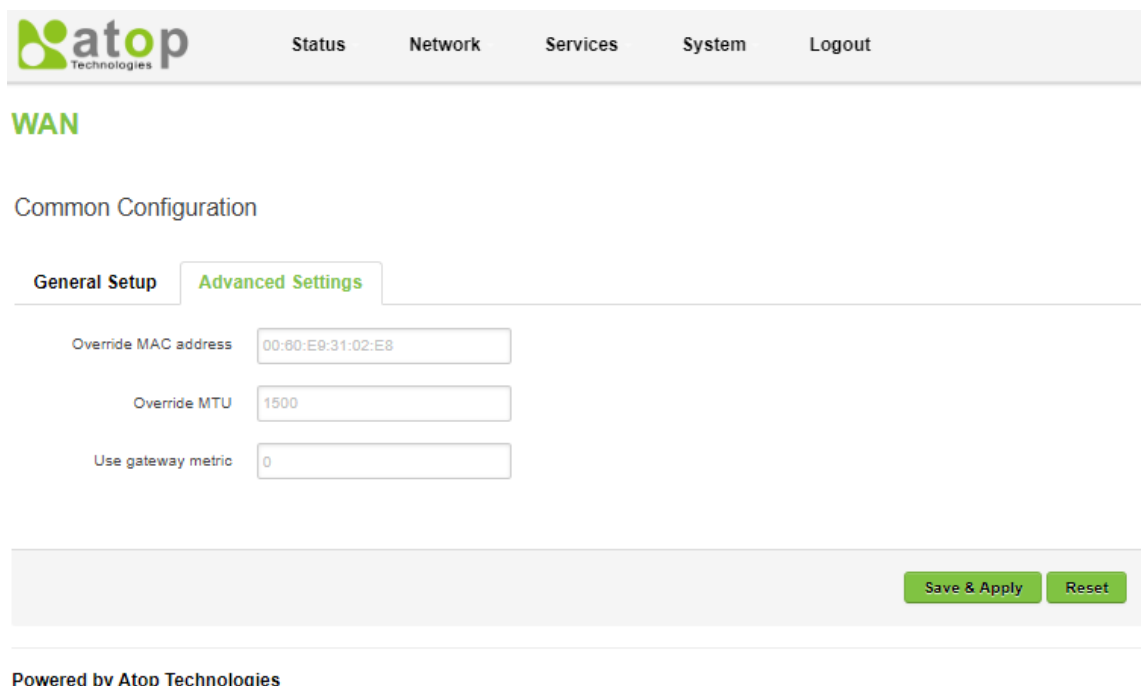
Field	Value	Description
Protocol	Static /DHCP /PPPoE default: DHCP	The protocol is used by the WAN interface. This field currently supports static address, DHCP client, and PPPoE.
PAP/CHAP Username	default: <b>none</b>	The username used in PAP/CHAP authentication.
PAP/CHAP password	default: <b>none</b>	The password used in PAP/CHAP authentication.
Access Concentrator	default: <b>auto</b>	Access Concentrators is used for routing their PPPoE connections to ISP. Usually, the settings are received automatically; however, in some cases, it is required to specify the name for an Access Concentrator. User can leave this field empty to detect Access Concentrators automatically.
Service Name	default: <b>auto</b>	A service name defines the set of services that the router can provide to a PPPoE client. Leave this field empty to detect the Service name automatically.

## 4.2.2 Advanced Settings

In the Advanced Setting tab under the Network->WAN submenu, user can configure the WAN interface in more detail. Setting parameters shown in the Advanced Setting tab will correspond to the protocol that user selected in the General Setup tab. It is highly recommended to leave this tab to a trained professional, especially if user really feel uncertain of how to alter these attributes.

### 4.2.2.1 Static Address

Figure 4.12 shows advanced setting parameters of Static Address protocol. Here, user can **override MAC address** of LAN interface, **override the Maximum Transfer Size (MTU)** of a data packet, and alter the routing table entry by setting value in the **Use gateway metric** field.



atop Technologies

Status Network Services System Logout

WAN

Common Configuration

General Setup **Advanced Settings**

Override MAC address 00:80:E9:31:02:E8

Override MTU 1500

Use gateway metric 0

Save & Apply Reset

Powered by Atop Technologies

Figure 4.12. Static Address Protocol in the Advanced Setting Tab under the Network-&gt;WAN Submenu

Table 4.11. Parameters of Static Address Protocol in the Network-&gt;WAN Submenu-&gt; the Advanced Setting Tab

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

#### 4.2.2.2 DHCP Client Protocol

This section describes about advanced setting parameters of DHCP Client protocol. Here, user can use **broadcast flag**, use enabled/disabled **default gateway**, and enabled/disabled **DNS server advertised by peer**. Also, when requesting DHCP, user can specify the **Client ID**, and the **Vendor Class** that the user needs. Lastly, user can **override MAC address** of LAN interface, **override the Maximum Transfer Size (MTU)** of a data packet, and alter the routing table entry by setting value in the **Use gateway metric** field. Figure 4.13 shows webpage of the setting parameters of the DHCP Client Protocol in the Advanced Setting Tab under the Network->WAN Submenu. Table 4.12 show the details of setting parameters that are shown in Figure 4.13.

The screenshot shows the 'atop Technologies' logo and navigation tabs: Status, Network, Services, System, and Logout. The 'WAN' section is active, showing 'Common Configuration'. Under 'Advanced Settings', the following options are visible:

- Use broadcast flag:** ☐ Required for certain ISPs, e.g. Charter with DOCSIS 3
- Use default gateway:** ☒ If unchecked, no default route is configured
- Use DNS servers advertised by peer:** ☒ If unchecked, the advertised DNS server addresses are ignored
- Use gateway metric:**
- Client ID to send when requesting DHCP:**  The length of client ID needs less than 256
- Vendor Class to send when requesting DHCP:**
- Override MAC address:**
- Override MTU:**

At the bottom right, there are 'Save & Apply' and 'Reset' buttons.

Powered by Atop Technologies

Figure 4.13. DHCP Client Protocol in the Advanced Setting Tab under the Network->WAN Submenu

Table 4.12. Parameters of DHCP Client Protocol in the Advanced Setting Tab under the Network->WAN Submenu

Field	Value	Description
Use broadcast flag	default: <b>Unchecked</b>	If checked, it will specify how to transmit DHCP Offer reply packets and DHCP ACK and NAK reply packets back to DHCP clients during the discovery process. This field is required for certain ISPs, e.g., Charter with DOCSIS 3.
Use default gateway	default: <b>Checked</b>	If unchecked, no default route is configured.
Use DNS servers advertised by peer	default: <b>Checked</b>	If unchecked, the advertised DNS server addresses are ignored.
Use gateway metric	default: <b>0</b>	The WAN configuration by default generates a routing table entry. With this field, you can alter the metric of that entry.
Client ID to send when requesting DHCP	default: <b>Empty</b>	If there is an input value, it will permit using Client ID to specify a device on the network instead of its MAC address. If empty, the device will be identified by its MAC address only. Length of this Client ID must be less than 256.
Vendor Class to send when requesting DHCP	default: <b>Empty</b>	If there is an input value, DHCP administrators are allowed to assign vendor-specific DHCP options to devices without running the risk of duplicating options within the DHCP scope. For example, it allows an

		organization to supply separate DHCP option 43 values to different vendor devices.
Override MAC address	default: <b>Device's MAC</b>	Override the MAC address of the LAN interface.
Override MTU	default: <b>1500</b>	Specify the maximum transferred size of a data packet.

#### 4.2.2.3 PPPoE Protocol

Figure 4.14 shows advanced setting parameters of PPPoE protocol. Here, user can enable IPv6 negotiation on the PPP link, enabled/disabled **use default gateway**, and enabled/disabled **DNS server advertised by peer**. Also, when using PPPoE protocol, user can set **LCP (Link Control Protocol) echo failure threshold** and **LCP echo interval**. Lastly, user can **override the Maximum Transfer Size (MTU)** of a data packet, and alter the routing table entry by setting value in the **Use gateway metric** field. Figure 4.14 shows webpage of the setting parameters of the PPPoE Protocol in the Advanced Setting Tab under the Network->WAN Submenu. Table 4.13 show the details of setting parameters that are shown in Figure 4.14.

The screenshot displays the 'WAN' configuration page for PPPoE. The 'Advanced Settings' tab is active. The configuration options are as follows:

- 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:**

Buttons: **Save & Apply**, **Reset**

Powered by Atop Technologies

Figure 4.14. PPPoE Protocol in the Advanced Setting Tab under the Network->WAN Submenu

Table 4.13. Parameters of PPPoE Protocol in the Advanced Setting Tab under the Network->WAN Submenu

Field	Value	Description
Bring up on boot	default: <b>enable</b>	Specify whether to bring up the WAN interface on boot or not.
Enable IPv6 negotiation on the PPP link	default: <b>disable</b>	If enabled, IPv6 negotiation on the Point-to-point link protocol.
Use default gateway	default: <b>enable</b>	If unchecked, no default route is configured.
Use gateway metric	default: <b>0</b>	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: <b>enable</b>	If unchecked or disabled, the advertised DNS server addresses are ignored.
LCP echo failure threshold	default: <b>0</b>	Presume that peer will be dead after received the given amount of LCP echo failures. Ignore failures if the threshold is set to 0.
LCP echo interval	default: <b>6</b>	Send LCP echo requests every given interval (in seconds). The method to detect active or inactive peer will only be effective in conjunction with the setting of failure threshold.
Inactivity timeout	default: <b>0</b>	Close inactive connection after the given number of seconds. User can input 0 in the field to open the connection even it is inactive.
Override MTU	default: <b>1500</b>	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.

There are total of three sections under that **Network->LAN** submenu: Common Configuration, DHCP Server, and Static Leases. In the **Common Configuration** section, only **Static address** protocol is supported. In the **DHCP Server** section, user can basically and advanced set DHCP function in the **General Setup** tab and in **Advanced Settings** tab, respectively. In the **Static Leases** section, Static IP addresses are configured manually, directly on the client. Reserved IP addresses are leased from the DHCP server, but the given client will always receive the same IP address. The DHCP service identifies the client by MAC address.

#### 4.3.1 Common Configuration

In the General Setup tab under the Network->WAN submenu->Common Configuration section, user can configure the CWR5805 device's network settings; e.g., IP address, IP netmask, IP gateway, and DNS server. The default protocol is set to a **Static address** with a default IPv4 address of 192.168.1.1. As shown in the Figure below, the Status field currently displays LAN port interface (br-lan) information of Uptime, MAC Address, RX, TX, and IP.

### LAN

#### Common Configuration

The screenshot shows the 'General Setup' tab for LAN configuration. Under the 'Status' section, the interface 'br-lan' is shown with the following details: Uptime: 1h 3m 23s, MAC Address: 00:60:E9:31:02:E9, RX: 1.92 MBytes (19922 Packets), TX: 5.20 MBytes (10338 Packets), IPv4: 192.168.1.1/24, and IPv6: fd4f:d261:5d3b::1/60. In the configuration section, the 'Protocol' is set to 'Static address'. The 'IPv4 address' is '192.168.1.1' and the 'IPv4 netmask' is '255.255.255.0'. There is a field for 'Use custom DNS servers' which is currently empty.

Figure 4.15. Common Configuration Section under the Network->LAN Submenu



Table 4.14. Parameters in the Common Configuration Section under the Network-&gt;LAN Submenu

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

#### 4.3.2 DHCP Server

A **DHCP** (Dynamic Host Configuration Protocol) **server** is a service that can automatically configure the TCP/IP settings of any device that requests such a service. With a dynamic IP configuration, a client device leases an IP configuration from a DHCP server. This server is configured with a pool of available IPs and other settings beforehand. Clients contact the server and temporarily borrow an IP address configuration. After received IP address, the LAN client device can communicate with other devices 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. That means, for any IPv4 DHCP client devices that are connected to a LAN port interface, wireless 2.4GHz/5GHz AP can assign them dynamic IPv4 addresses that are 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

User can perform DHCP server's basic setting in the **General Setup Tab** under the Network->LAN Submenu->DHCP Section.

On the LAN interface, the IPv4 DHCP server is enabled by default. Therefore, XWR5805 will dynamically assign an IPv4 address to any device with enabled IPv4 DHCP client function. The default IP address of the IPv4 DHCP server is 192.168.1.1, and the dynamic IP address range is from 192.168.1.100 to 192.168.1.250.

## 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

Figure 4.16. General Setup Tab in the DHCP Section under the Network-&gt;LAN Submenu

Table 4.15. Parameters in the General Setup Tab under the Network-&gt;LAN Submenu-&gt; DHCP Section

Field	Value	Description
Disable DHCP	default: <b>disable</b>	To enable/disable DHCP server for LAN interface.
Start	default: <b>100</b>	The starting IPv4 address value.
Limit	default: <b>150</b>	Maximum numbers of IPv4 addresses that the DHCP server can lease out.
Leasetime	default: <b>12h</b>	The duration that an IPv4 address can be leased out. Leased out addresses will be expired after the amount of time specified in this field run out. Then, the device have to request a new IPv4 address.

## 4.3.2.2 Advanced Settings

User can perform DHCP server's more advanced setting in the **Advanced Settings Tab** under the Network->LAN Submenu->DHCP Section.

## 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.

Figure 4.17. Advanced Settings Tab in the DHCP Section under the Network-&gt;LAN Submenu

Table 4.16. Parameters in the Advanced Settings Tab under the Network-&gt;LAN Submenu-&gt; DHCP Section

Field	Description
Dynamic DHCP	If checked or enabled, XWR5805 will dynamically allocate DHCP addresses for clients. If not checked or disabled, it only provides service to static IP address clients.

DHCP-Options	Define an additional DHCP option which is advertising different DNS servers to clients. User can click  icon to add a new list of DNS server. For example, "192.168.2.1,192.168.2.2" is the result of adding two new lists of DNS servers.
--------------	---

### 4.3.3 Static Leases

The **Static Leases** section is used to reserve specific IP addresses for specific client devices by binding them to their MAC address. It is useful when user have a stationary device that needs to be reached frequently in the network; e.g., printer and IP phone.

#### Static Leases

Hostname	MAC Address	IPv4 Address
This section contains no values yet		
<div>Add</div>		
		<div>Save &amp; Apply</div> <div>Reset</div>

Figure 4.18. Static Leases Section under the Network->LAN Submenu

Table 4.17. Parameters in the Static Leases Section under the Network->LAN Submenu

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

## 4.4 Wireless

User can configure wireless access points, monitor connected wireless stations, choose the method to scan wireless station, and set the compatibility of number of channels to different countries in the webpage under the **Network->Wireless** Submenu. There are three main sections within this webpage: **Wireless Overview** Section, **Associated Stations** Section, and **Country** Section. The AWR5805 and CWR5805 device supports **IEEE802.11 a/b/g/n/ac** wireless technologies. The tutorial of how to set up a CWR; e.g., configuring its wireless access point functions and testing its connectivity, is shown in Section 4.4.4.

### 4.4.1 Wireless Overview

User can configure wireless access points and choose the method to scan wireless station in the **Wireless Overview** Section under the **Network->Wireless** Submenu by clicking **Edit** button and **Scan** button, respectively. User can enable/disable WI-FI interfaces by clicking on **Enable** or **Disable** button. A new SSID can be added by clicking on **Add Guest** button. After clicking **Add Guest** button, user will be directed to a Wi-Fi configuration page. Here, a default name for new SSID is given: ATOP\_Guest24; however, it can be changed later by user. Only two SSIDs can be allocate for each frequency. Two frequencies are now supported for XXR5805: 2.4GHz and 5GHz. Therefore, the total of maximum four tabs are supported in this Wi-Fi configuration page. User can also be directed to this Wi-Fi configuration page when clicking on an Edit button of any WI-Fi Interface's SSID in the Wireless Overview Section. User has a choice to delete this newly added SSID later by using the corresponding **Delete** button. The AWR5805 and CWR5805 device supports **IEEE802.11 a/b/g/n/ac** wireless technologies.

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. Whereas, 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.

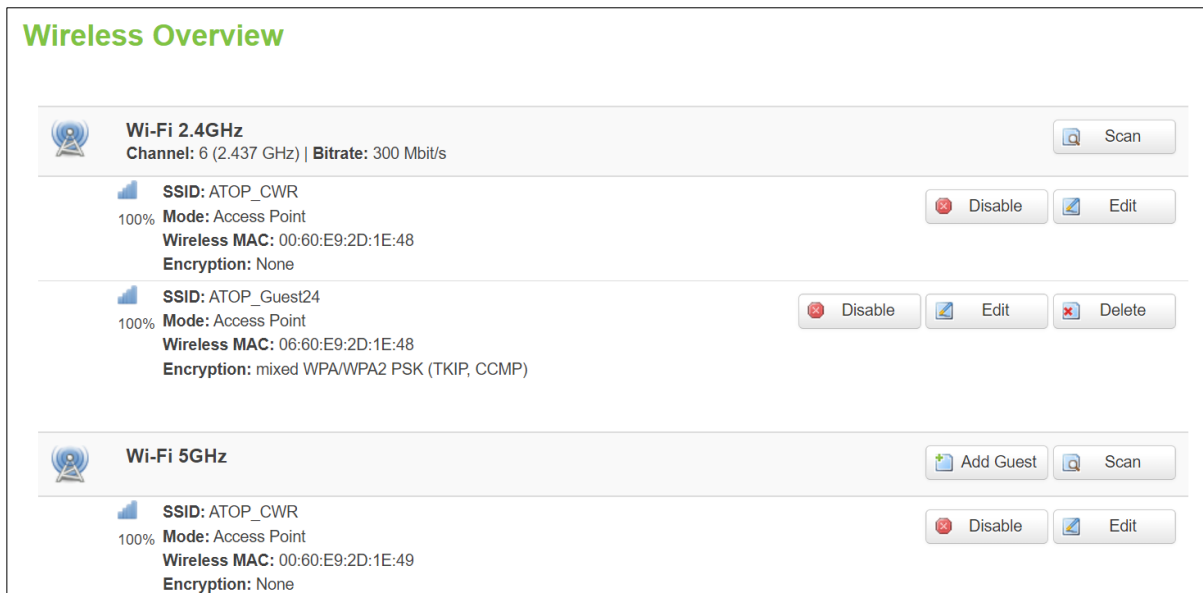


Figure 4.19. Wireless Overview Section under the Network-&gt;Wireless Submenu

Table 4.18. Parameters inside Wireless Overview Section under the Network-&gt;Wireless Submenu

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.

#### 4.4.1.1 Wireless Scan

Click the **Scan** button to scan the currently available Wi-Fi Access Points in the surrounding area which will be displayed, as shown in the Figure 4.20. This webpage will be launched when user clicks the **Scan** button in the **Wireless Overview** section.

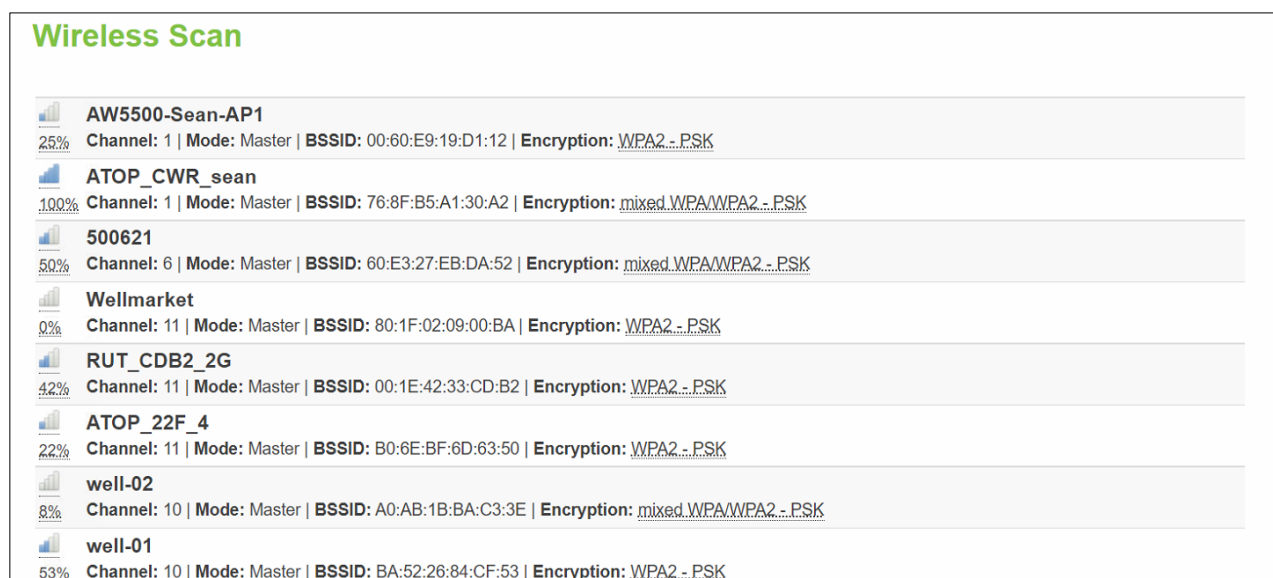


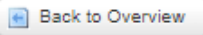
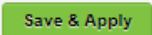

Figure 4.20. After Clicking Scan Button in the Wireless Overview Section under the Network-&gt;Wireless Submenu

Table 4.19. Parameters in the Scan Webpage under the Network-&gt;Wireless Submenu-&gt;Wireless Overview Section

Field	Description
Signal Level	Received Signal Strength Indicator (RSSI) level measured in the percentage.
SSID	Broadcasted SSID of the wireless network that clients will be connected to.
Channel	Wi-Fi channel that is currently used by the access point.
Mode	Currently only support Master (access point) mode.

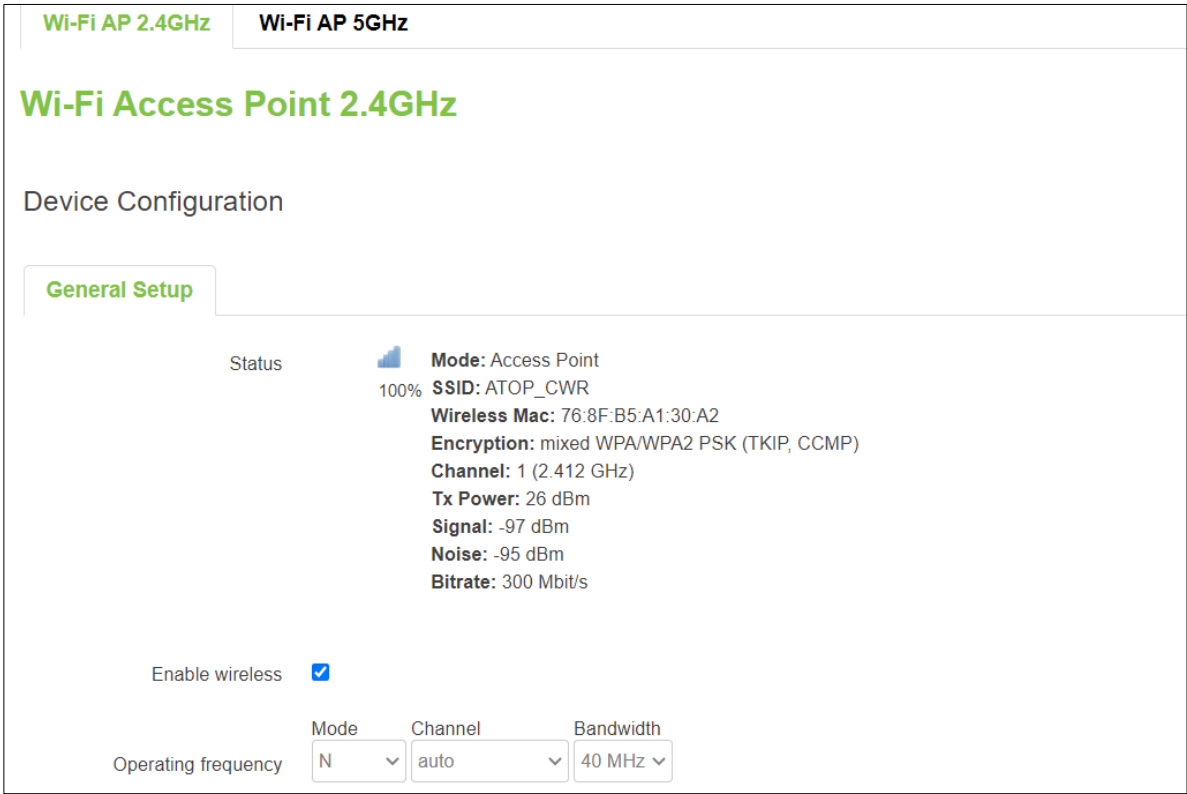
BSSID	This value identifies the basic service set that are 48-bit labels conforming to the MAC-48 convention. This value is the same as MAC address.
Encryption	Encryption type that the Wi-Fi access point uses.

#### 4.4.1.2 Wi-Fi AP 2.4/5GHz

In the **Wireless Overview** Section under the **Network->Wireless** Submenu, user can click the **Edit** button of the wireless AP's corresponding frequency to configure the setting parameters. The **Wi-Fi 2.4/5GHz** webpage will be launched afterwards. Within this page, there is the **Device Configuration** subsection and the **Interface Configuration** subsection. For **Wi-Fi 2.4 GHz Guest** webpage, there are two more subsections followed the Interface Configuration subsection, which are the **Common Configuration** and the **DHCP Server**. At the end of the webpage, user can click  to go back to the Wireless Overview Section,  to save and apply the new setting, or  to reset back to the previously saved setting.

##### 4.4.1.2.1 Device Configuration

Figure 4.21 and Figure 4.22 illustrate a device configuration subsection where general information of Wi-Fi access point is displayed.



The screenshot displays the 'Wi-Fi Access Point 2.4GHz' configuration page. At the top, there are tabs for 'Wi-Fi AP 2.4GHz' (selected) and 'Wi-Fi AP 5GHz'. Below the tabs, the title 'Wi-Fi Access Point 2.4GHz' is shown in green. Underneath, the 'Device Configuration' section is visible, with the 'General Setup' tab selected. The 'General Setup' tab contains a 'Status' section with a signal strength indicator at 100% and a list of configuration parameters: Mode: Access Point, 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, and Bitrate: 300 Mbit/s. Below the status section, there is a checkbox for 'Enable wireless' which is checked. At the bottom, there is an 'Operating frequency' section with three dropdown menus: 'Mode' set to 'N', 'Channel' set to 'auto', and 'Bandwidth' set to '40 MHz'.

Figure 4.21. Device Configuration after Clicking Edit Button in the Wi-Fi 2.4GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section

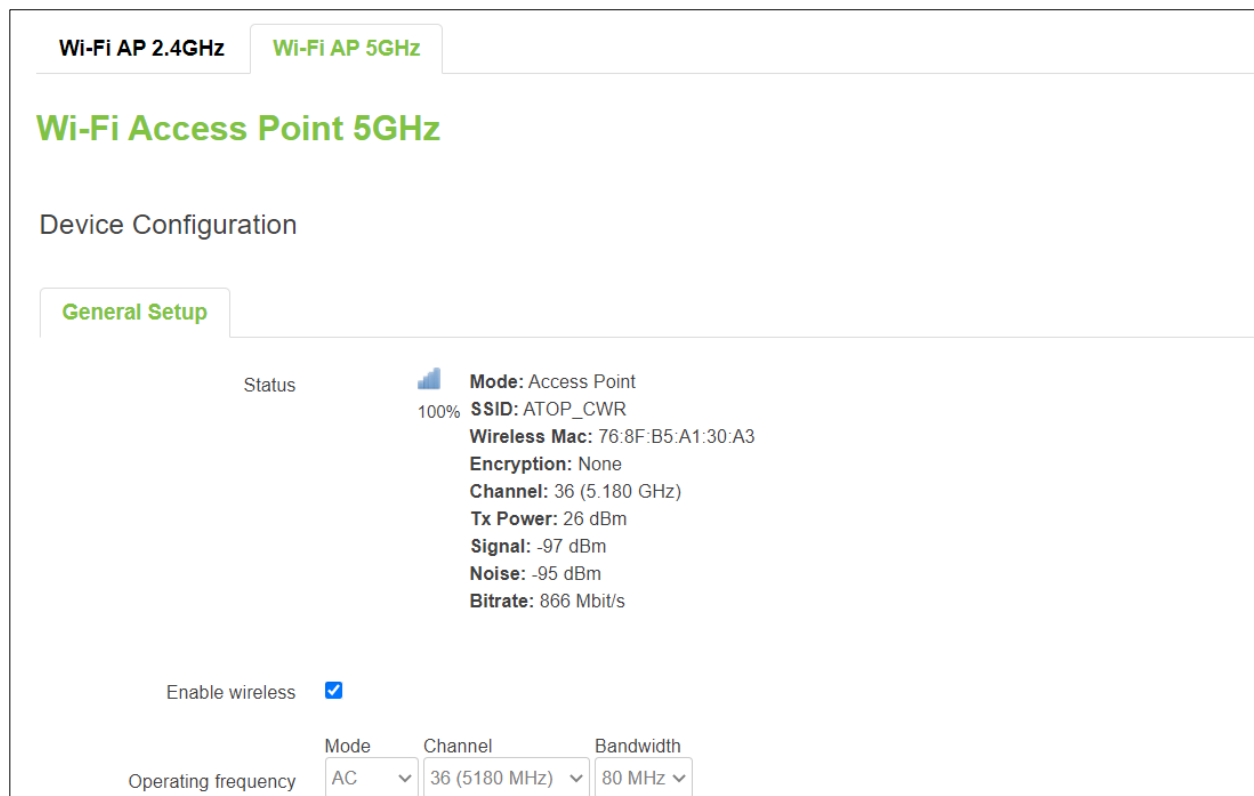


Figure 4.22. Device Configuraiton after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section

Table 4.20. Setting Parameters of Device Configuration after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section

Field		Value	Description
Status		No default value	The status of Wi-Fi 2.4GHz/5GHz access point, which contains signal level, mode, SSID, Wireless Mac (or BSSID), encryption, channel, tx-power, SNR, and bitrate information.
Enable Wireless		disable/enable; default: <b>disable</b>	To enable/disable Wi-Fi 2.4GHz/5GHz access point.
Operating Frequency -Mode	<b>2.4GHz</b>	legacy (b/g) mode and N mode	The wireless protocol which is currently used by the access point.
	<b>5GHz</b>	legacy (a) mode, N mode, and AC mode	
Operating Frequency -Channel	<b>2.4GHz</b>	Auto/1/2/3/4/5/6/7/8/9/10/11; default: Auto	
	<b>5GHz</b>	Auto/36/40/44/48/149/153/157/161/165; default: Auto	
Operating Frequency -Width	<b>2.4GHz</b>	20/40MHz in N mode	
	<b>5GHz</b>	20/40 MHz in N mode, and 20/40/80/160 MHz in AC mode	

#### 4.4.1.2.2 Interface Configuration

Under the WiFi-AP 2.4/5GHz configuration webpage, there is an **interface configuration** subsection after **the device configuration** subsection. Within this interface configuration subsection, there are three tabs: **General Setup**, **Wireless Security**, and **MAC-Filter**.

##### 4.4.1.2.2.1 General Setup

In the **General Setup** tab within the Interface Configuration subsection, user can configure the SSID of Wi-Fi 2.4GHz/5GHz Access Points, as shown in Figure 4.23. Table 4.21 shows detailed parameters within the webpage in Figure 4.23.

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

Figure 4.23. Interface Configuration – General Setup Tab after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section

Table 4.21. Setting Parameters of Interface Configuration – General Setup Tab after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section

Field	Value	Description
SSID	default: <b>ATOP_CWR</b>	The broadcast SSID of the wireless network that clients will be connected to.
Mode	default: <b>Access Point</b>	Currently support only Access Point mode.
Hide SSID	default: <b>disable</b>	Hide access point's SSID from scanning of other devices in the area.

#### 4.4.1.2.2.2 Wireless Security

In the **Wireless Security** tab within the Interface Configuration subsection, user can configure the encryption type that will be used in Wi-Fi Access Point 2.4GHz/5GHz, as shown in Figure 4.24. Table 4.22 shows detailed parameters within the webpage in Figure 4.24.

Interface Configuration

General Setup | **Wireless Security** | MAC-Filter

Encryption:

Cipher:

Key:

Figure 4.24. Interface Configuration – Wireless Security Tab after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section

Table 4.22. Interface Configuration – Wireless Security Tab after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section

Field	Value	Description
Encryption	No Encryption/OWE/WPA2-PSK/WPA-PSK &WPA2-PSK Mixed Mode/WPA3-Personal (SAE) default: <b>No Encryption</b>	Type of used Wi-Fi encryption
Cipher*	Auto/Force CCMP (AES)/Force TKIP and CCMP (AES) default: <b>auto</b>	An algorithm for performing encryption or decryption.

Key	default: <b>none</b>	A custom passphrase which is used for authentication (at least 8 characters long).
-----	----------------------	--

\*: WPA&WPA2 only

#### 4.4.1.2.2.3 MAC-Filter

In the **MAC-Filter** tab within the Interface Configuration subsection, user can define a to-do rule for the pre-defined MAC list. User have a choice to either **Allow listed only** or **Allow all except listed**. In **Allow listed only**, user has to keep a list of MACs that their traffic is allowed to forward. In **Allow all except listed**, user has to keep a list of MACs that their traffic is forbidden to forward. Figure 4.26 shows a **MAC-Filter** tab webpage under the **Interface Configuration** Subsection. Table 4.24 shows detailed parameters with in the webpage in Figure 4.26.

Figure 4.25. Interface Configuration – MAC-Filter Tab after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section

Table 4.23. Interface Configuration – MAC-Filter Tab after Clicking Edit Button in the Wi-Fi 5GHz Subsection under the Network->Wireless Submenu->the Wireless Overview Section

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

#### 4.4.1.2.3 Common Configuration

Under the Wi-Fi Access Point 2.4GHz Guest webpage, there is a **Common configuration** subsection after the **Interface Configuration** subsection. Within this Common Configuration subsection, there is a tab named **General Setup**.

Figure 4.26. Common Configuration after Clicking Edit Button in the Wi-Fi 2.4GHz Guest Subsection under the Network->Wireless Submenu->the Wireless Overview Section

Table 4.24. Parameters of Common Configuration after Clicking Edit Button in the Wi-Fi 2.4GHz Guest Subsection under the Network->Wireless Submenu->the Wireless Overview Section

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



Status	No default value	The status of Wi-Fi 2.4GHz Guest access point, which contains Uptime Wireless Mac, Rx, Tx, and IPv4 information.
IPv4 Address	IPv4 Default: 192.168.100.1	The IP address of the destination network or host.
IPv4 Netmask	Default: 255.255.255.0	A subnet mask that is applied to the target field to determine to what actual IP addresses the routing rule applies.
Use Custom DNS Servers	Default: 8.8.8.8	Router will resolve hostname using these input DNS servers. User can enter multiple DNS servers to provide redundancy in case that one of the servers fails.

#### 4.4.1.2.4 DHCP Server

Under the Wi-Fi Access Point 2.4GHz Guest webpage, there is a **DHCP Server** subsection after the **Common Configuration** subsection. Within this **DHCP Server** subsection, there are a tab named **General Setup** and **Advanced Settings**.

##### DHCP Server

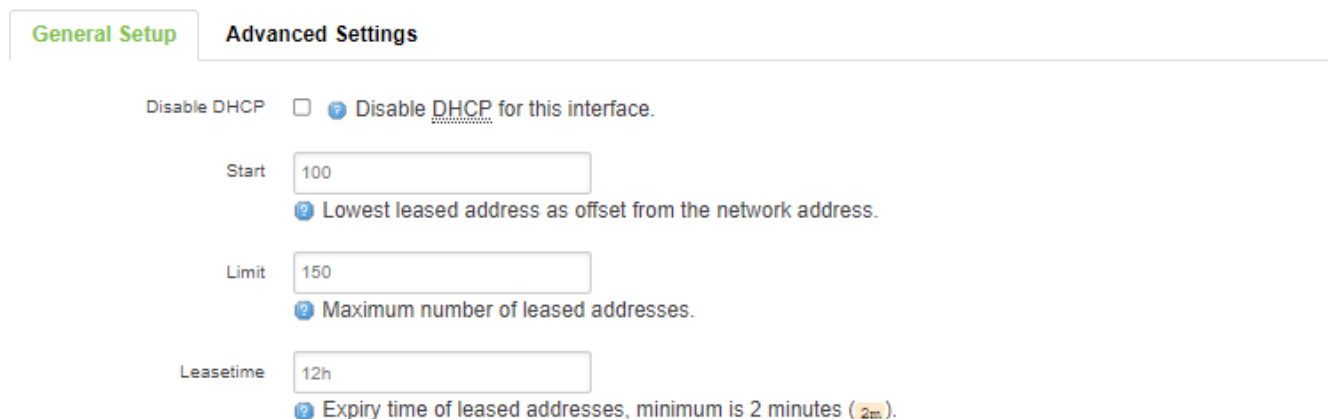


Figure 4.27. DHCP Server – General Setup after Clicking Edit Button in the Wi-Fi 2.4GHz Guest Subsection under the Network->Wireless Submenu->the Wireless Overview Section

Table 4.25. Parameters of DHCP Server Subsection – General Tab after Clicking Edit Button in the Wi-Fi 2.4GHz Guest Subsection under the Network->Wireless Submenu->the Wireless Overview Section

Field	Value	Description
Disable DHCP	Action <b>Default: Unchecked</b>	Check to disable DHCP function of this interface
Start	integer <b>Default: 100</b>	Lowest leased address as offset from the network address
Limit	Integer <b>Default: 150</b>	Maximum number of leased addresses
Leasetime	Integer in hours <b>Default: 12h</b>	Expiry time of leased addresses. The minimum value is set to 2 minutes.

##### DHCP Server

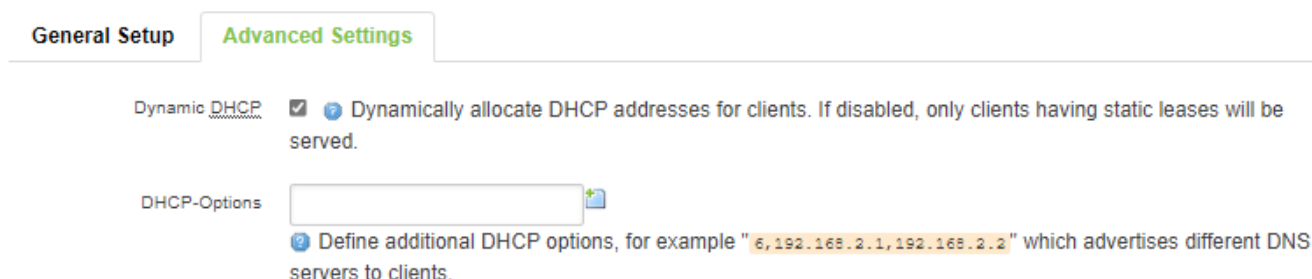



Figure 4.28. DHCP Server – Advanced Settings after Clicking Edit Button in the Wi-Fi 2.4GHz Guest Subsection under the Network->Wireless Submenu->the Wireless Overview Section

Table 4.26. Parameters of DHCP Server Subsection – General Tab after Clicking Edit Button in the Wi-Fi 2.4GHz Guest Subsection under the Network->Wireless Submenu->the Wireless Overview Section

Field	Value	Description
Dynamic DHCP	<b>Default: Checked</b>	Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
DHCP-Options	<b>Default: Empty</b>	Define additional DHCP options. For example, "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients. Click  to add more option.

#### 4.4.2 Associated Stations

In the **Associated Stations** Section, user can view a list of all Wi-Fi Stations that are currently maintaining connections with XXR5805 in term of: SSID, MAC Address, IPv4 Address, Signal, RX Rate, and TX Rate.



The screenshot shows the 'Associated Stations' section with a title in green. Below the title is a table with the following data:


SSID	MAC Address	IPv4 Address	Signal	RX Rate	TX Rate
 ATOP_CWR	76:63:73:FE:A4:C5	192.168.1.12	-71 dBm	78.0 Mbit/s	520.0 Mbit/s

Figure 4.29. Associated Stations Section under the Network->Wireless Submenu

Table 4.27. Parameters in the Associated Stations Section under the Network->Wireless Submenu

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

#### 4.4.3 Country

User can set the country that the Wi-Fi Access Point is located to ensure the compatibility of number of channels to other local Wi-Fi Access Points, as shown in Figure 4.30.

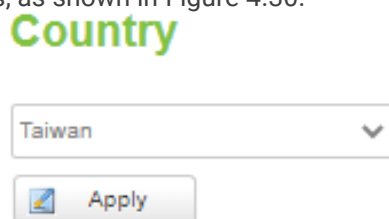


Figure 4.30. Country Section under the Network->Wireless Submenu

#### 4.4.4 Tutorials

This tutorial shows how to set up a CWR by configuring its wireless access point functions and testing its connectivity. Figure 4.31 shows details of the success network connection.

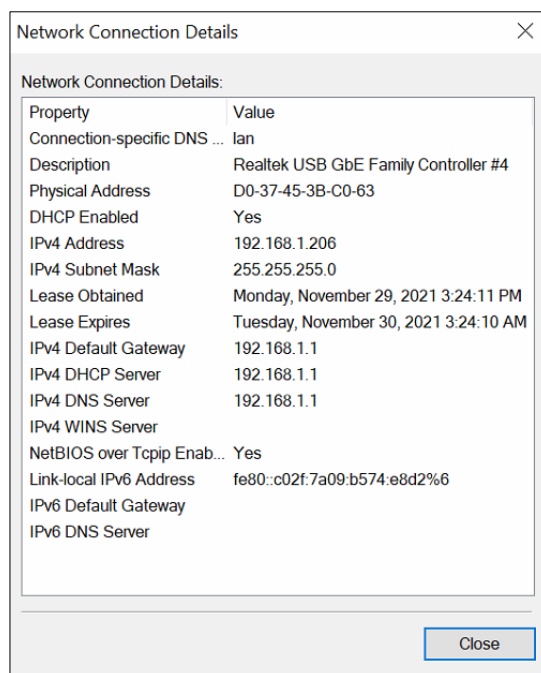


Figure 4.31. Details of the Wireless Network Connection

In **Wireless Overview** Section under the Network->Wireless menu, there are two wireless AP services available. By default, the Wi-Fi 2.4GHz interface is operated with 802.11N mode, and the Wi-Fi 5GHz interface is operated with 802.11AC mode. The **Associated Stations** Section lists connected client devices under these two wireless AP networks (SSID). User can connect any wireless devices; e.g., mobile phone, tablet, and laptop to the wireless APs.

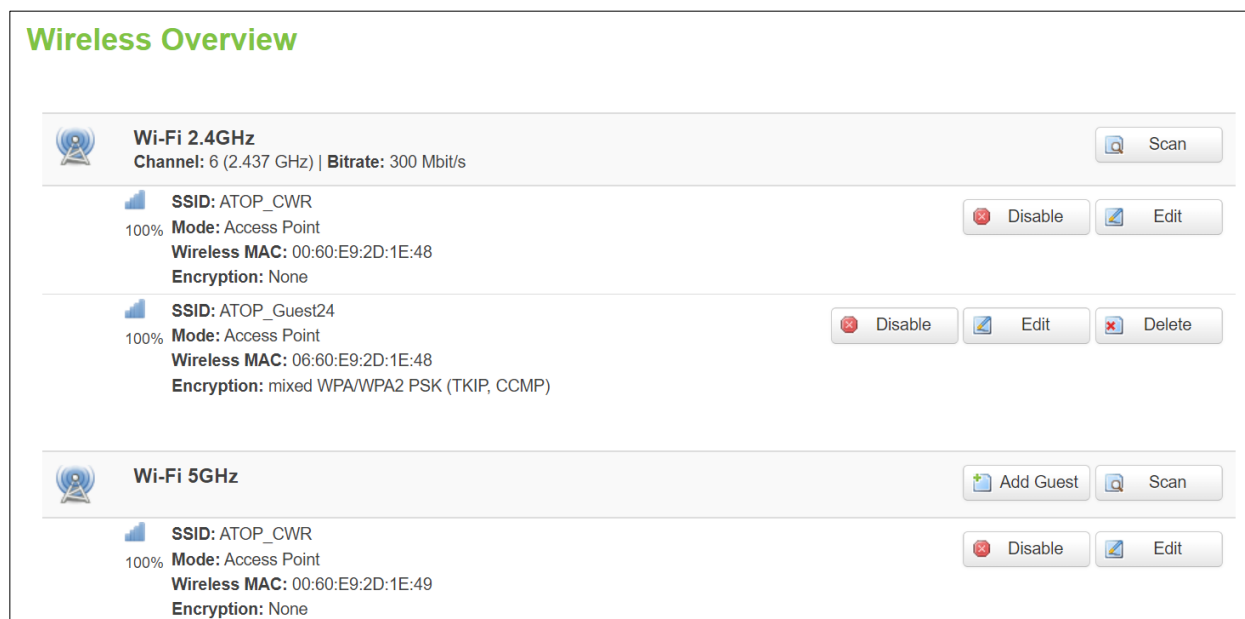


Figure 4.32. Wireless Overview Section under Network-&gt;Wireless Menu

For the 2.4 GHz band wireless AP

1. ESSID is set to **ATOP\_CWR** in the General Setup tab.
2. Encryption is set to **none** in the Wireless Security tab.

For the 2.4 GHz band wireless AP Guest

1. ESSID is set to **ATOP\_Guest24** in the General Setup tab.
2. Encryption is set to the **WPA-PSK/WPA2-PSK Mixed Mode** in the Wireless Security tab.
3. Key is set **atopatop** in the Wireless Security tab.

For the 5 GHz band wireless AP

1. ESSID is set to **ATOP\_CWR** in the General Setup tab.

2. Encryption is set to **none** in the Wireless Security tab.

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

**Step 1:** *Turning on Wi-Fi on Android 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.

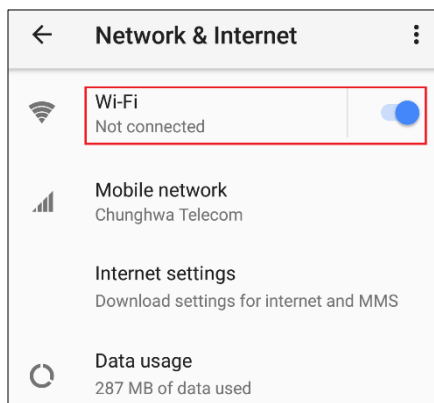


Figure 4.33. Network & Internet Settings on the Android System

**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.

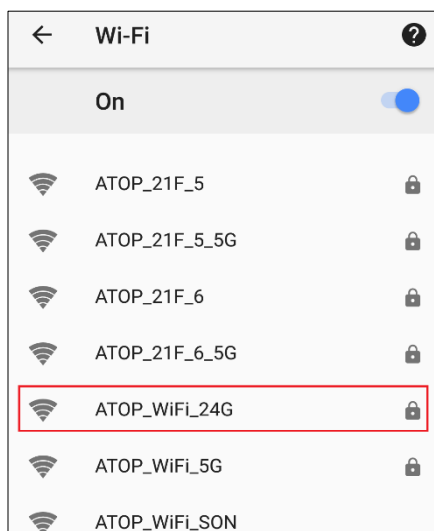


Figure 4.34. Select ATOP\_WiFi\_24G AP under Network & Internet Menu

**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.

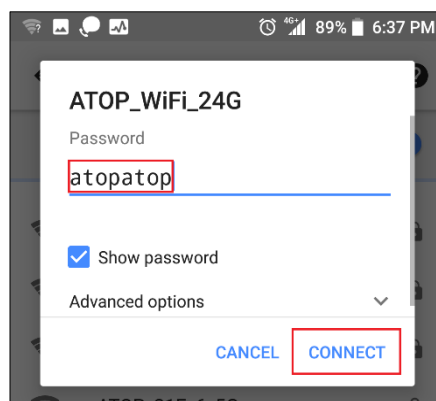


Figure 4.35. Input Password (Network Key) for WiFi Connection

**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.

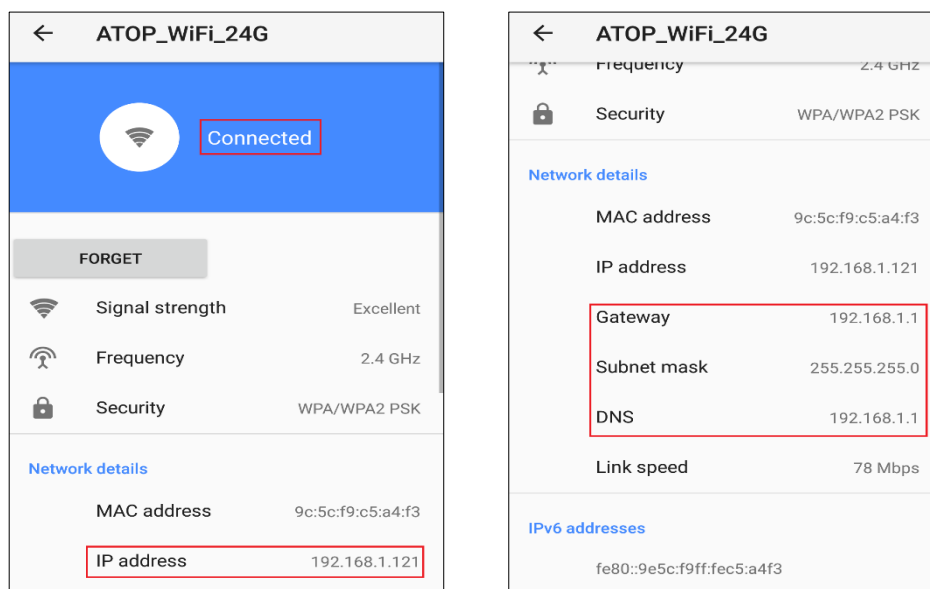


Figure 4.36. Wi-Fi Connected Information

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

Under Network->Mesh menu, the **Whole Home Mesh System** webpage in the mesh Settings tab is launched, as shown in Figure 4.37. Here, the setting only supports basic one.

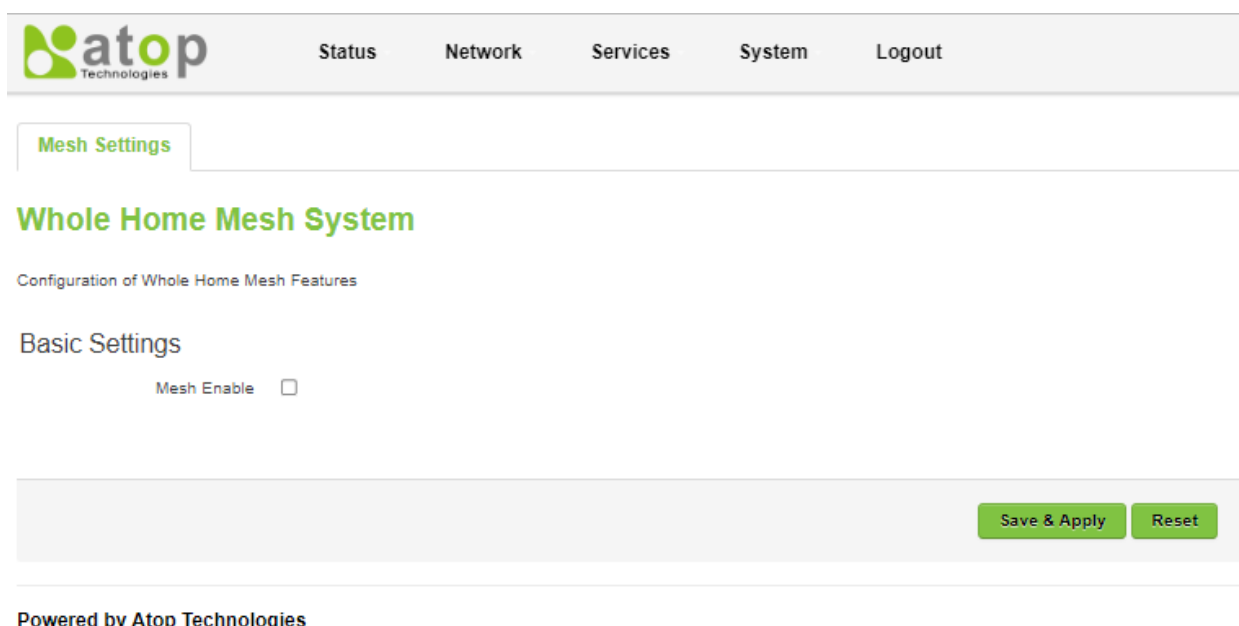


Figure 4.37. Whole Home Mesh System under the Network-&gt;Mesh Submenu

User can click checkbox to enable a Mesh function. The setting parameters of mesh which include mode (i.e., Router or Satellite), SSID, and WPA2-PSK Key will be appeared, as shown in Figure 4.38. User can build a mesh network if there is at least one CWR5805 with a central AP mode connected to another CWR5805 with an AP mode.

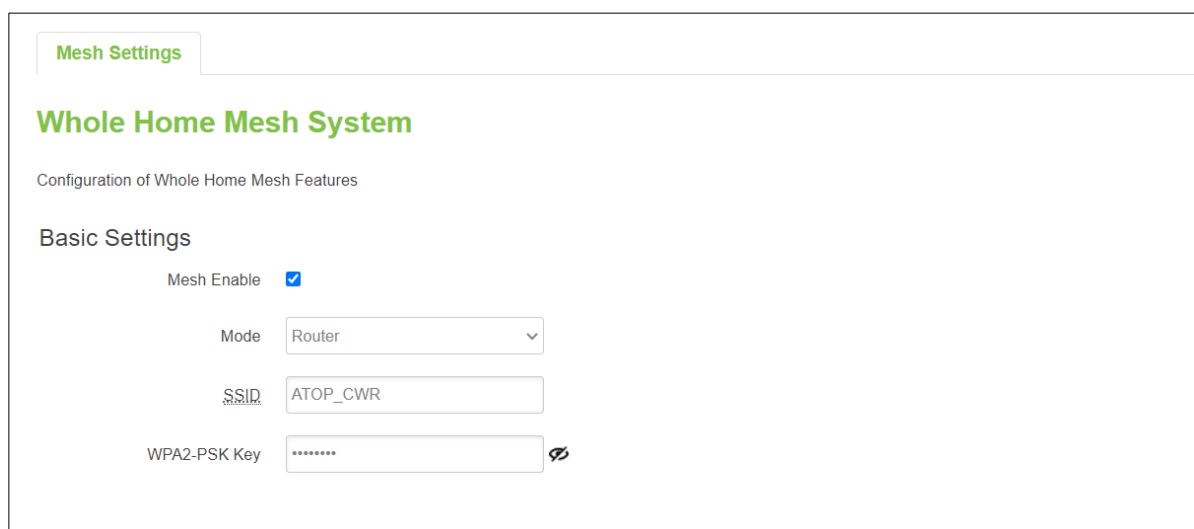


Figure 4.38. Enable Mesh Function in Whole Home Mesh System under the Network-&gt;Mesh Submenu

Table 4.28. Parameters in the Whole Home Mesh System under the Network-&gt;Mesh Submenu

Field	Value	Description
Mesh Enable	Disable/Enable; default: <b>disable</b>	To enable/disable the mesh feature.
Mode	Router/Satellite; default: Router	Select mesh mode of an access point: normal (AP) or central mode (CAP).
SSID	default: <b>ATOP_CWR</b>	The broadcast SSID of the mesh network. Both CAP mode and AP mode CWR5805 devices must be set to the same SSID.
WPA2-PSK Key	default: <b>ATOP_CWR</b>	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

User can configure the IPv6 settings under Network->IPv6 submenu, as shown in Figure 4.39. Here, user can click checkbox to disable IPv6 WAN setting, set the protocol, IPv6 address, Gateway, Prefix length, and the DNS server. Details of setting parameters are illustrated in Table 4.29.

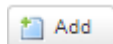
Figure 4.39. IPv6 WAN Settings under the Network->IPv6 Submenu

Table 4.29. Parameters of IPv6 WAN Settings under the Network->IPv6 Submenu

Field	Value	Description
Disable	Disable/Enable; default: <b>Enable</b>	Click the Disable checkbox to disable IPv6 function.
Protocol	DHCPv6/Static; default: DHCPv6	The protocol that is used by the WAN interface. It is either IPv6 static or dynamically assignment.
IPv6 address	ip6; default: <b>none</b>	IPv6 address of the router on the WAN network.
Gateway	ip6; default: <b>none</b>	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: <b>none</b>	Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address.
DNS server	ip6; default: <b>none</b>	Router will resolve hostname using these input DNS servers. User can enter multiple DNS servers to provide a redundancy in case one of the servers fails.

## 4.7 VLAN

User can configure the virtual LAN settings under Network->VLAN menu, as shown in Figure 4.40. User can click



icon to input information of a new VLAN ID and the interface that it would be used on. The



icon allows delete the entry if it is no longer needed.

Figure 4.40. 802.1Q VLAN under the Network-&gt;VLAN Submenu

Table 4.30. Setting Parameters of 802.1Q VLAN under the Network-&gt;VLAN Submenu

Field	Value	Description
VLAN ID	integer [1 - 4094]; default: <b>none</b>	VLAN identification number
Interface	wan/lan default: <b>wan</b>	Select which interface that the VLAN ID will be used on, LAN or WAN.

## 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.

There are two tabs under this Network->LB and Failover menu: **Overview** and **Configuration**. In the **Overview** tab, user can view the status of load balancing and failover whether it is disabled or enabled. Also, user can view load balancing and failover log here. In the **Configuration** tab, user can configure load balancing and failover in more details. Within this tab, there are total of five sub-tabs: **General**, **Interfaces**, **Members**, **Policies**, and **Rules**.

### 4.8.1 Overview

The **Overview** tab under Network->LB and Failover submenu contains status as well as a load balancing log of each interface, as shown in Figure 4.41 where the parameters are described in Table 4.31. The system log shows up and down timing of each interface.





Figure 4.41. Overview Tab under the Network-&gt;LB and Failover Submenu

Table 4.31. Parameters in the Overview Tab under the Network-&gt;LB and Failover Submenu

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

## 4.8.2 Configuration

The **Configuration** tab within Network->LB and Failover submenu consists of five sub-tabs, which are **General**, **Interfaces**, **Members**, **Policies**, and **rules**.

### 4.8.2.1 General

In the **General** sub-tab within the Configuration tab under Network -> LB and Failover Submenu, the load balancing feature is disabled by default. User can click **Enable** box to start load balancing service.

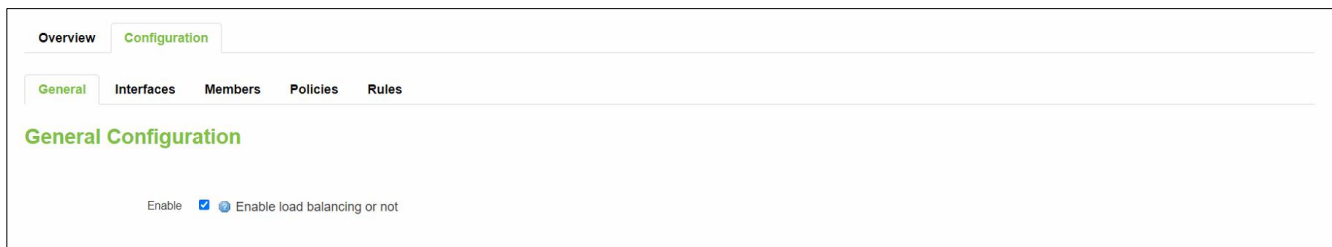


Figure 4.42. General sub-tab within the Configuration tab under Network -&gt; LB and Failover Submenu

Table 4.32. General sub-tab within the Configuration tab under Network -&gt; LB and Failover Submenu

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

### 4.8.2.2 Interfaces

In **Interfaces** sub-tab within the Configuration tab under Network -> LB and Failover Submenu, user can configure each WAN/Mobile interface 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 the network configuration. The method used for testing include tracking IP, ping, the number of testing before considering conclusive result of up and down interface, and sorting rule to forward priority traffic. Figure 4.43 illustrates the webpage of Interfaces sub-tab within the Configuration tab under Network -> LB and Failover Submenu, where user can view information of the test. The details of setting parameters in Figure 4.43 is described in Table 4.33.









Overview <b>Configuration</b>											
General <b>Interfaces</b> Members Policies Rules											
<b>Interfaces Configuration</b>											
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		   Edit
mobile	Yes	8.8.8.8 208.67.220.220	1	1	2s	5s	3	8	99		   Edit

Figure 4.43. Interfaces sub-tab within the Configuration tab under Network -&gt; LB and Failover Submenu

Table 4.33. Parameters in the Interfaces sub-tab within the Configuration tab under Network -&gt; LB and Failover Submenu

Field	Description
Interface	Display the interface's names. Note that if using a PPPoE interface, the interface name specified here should be the underlying interface name, not the "PPPoE-..." interface name.
Enabled	Display whether load balancing service is enabled/disabled on this interface.
Tracking IP	Hosts that are used for testing whether the interface is still alive or not. If this value is missing, the interface is considered up.
Tracking Reliability	Define a number of tracking IP hosts that must reply, so that the test is considered successful. User must ensure that enough tracking IP hosts are defined, or else the interface will always be considered down.
Ping Count	The number of pings that must be sent to each host in each test.
Ping Timeout	The waiting time (in seconds) for an echo-reply after an echo-request is sent.
Ping Interval	The interval time (in seconds) between each ping test.
Interface down	The number of failed tests before considering that the link is dead.
Interface Up	The number of successful tests before considering that the link is alive.
Metric	The metric value of this interface.
Sort	To sort the port forwarding rules. User can click   to move the priority of the interface. The interface that stays on top has the highest priority.

User can change the testing parameters of each interface by clicking the corresponding **Edit** button at the end of each row, as shown in Figure 4.43. Figure 4.44 shows the webpage that will be launched after clicking the edit button. The details of setting parameters in Figure 4.44 is described in Table 4.34.

The screenshot displays the 'Interfaces Configuration - wan' page. At the top, there are tabs for 'Overview' and 'Configuration', with 'Configuration' being the active tab. Below this, there are sub-tabs: 'General', 'Interfaces' (which is selected), 'Members', 'Policies', and 'Rules'. The main heading is 'Interfaces Configuration - wan'. The settings are as follows:

- Enabled:** A dropdown menu set to 'Yes'.
- Tracking IP:** A list of four IP addresses: 8.8.4.4, 8.8.8.8, 208.67.222.222, and 208.67.220.220. Each IP has a red 'X' icon to its right, except for the last one which has a green checkmark icon.
- Tracking reliability:** A text input field containing the value '2'. Below it, a note states: 'Acceptable values: 1-100. This many Tracking IP addresses must respond for the link to be deemed up'.
- Ping count:** A dropdown menu set to '1'.
- Ping timeout:** A dropdown menu set to '2 seconds'.
- Ping interval:** A dropdown menu set to '5 seconds'.
- Interface down:** A dropdown menu set to '3'. Below it, a note states: 'Interface will be deemed down after this many failed ping tests'.
- Interface up:** A dropdown menu set to '8'. Below it, a note states: 'Downed interface will be deemed up after this many successful ping tests'.
- Metric:** A text input field containing the value '0'. Below it, a note states: 'This displays the metric assigned to this interface in /etc/config/network'.

Figure 4.44. After Clicking Edit Button in the Interfaces sub-tab within the Configuration tab under Network -> LB and Failover Submenu

Table 4.34. Setting Parameter of the Webpage Launched after Clicking Edit Button in the Interfaces sub-tab within the Configuration tab under Network -> LB and Failover Submenu

Field	Value	Description
Enabled*	no/yes; default: <b>no</b>	Display whether load balancing service is enabled/disabled on this interface.
Tracking IP	ip; default: <b>8.8.8.8/8.8.4.4</b>	Hosts that are used for testing whether the interface is still alive or not. If this value is missing, the interface is considered up.
Tracking Reliability	integer [1 – 100]; default: <b>1</b>	Define a number of tracking IP hosts that must reply, so that the test is considered successful. User must ensure that enough tracking IP hosts are defined, or else the interface will always be considered down.
Ping Count	integer [1 – 5]; default: <b>1</b>	The number of pings that must be sent to each host in each test.
Ping Timeout	integer [1 – 10]; default: <b>1</b>	The waiting time (in seconds) for an echo-reply after an echo-request is sent.
Ping Interval	1/3/5/10/20/30 seconds 1/5/10/15/30 minutes 1 hour default: <b>2 seconds</b>	The interval time (in seconds) between each ping test.
Interface down	integer [1 – 10]; default: <b>3</b>	The number of failed tests before considering that the link is dead.
Interface Up	integer [1 – 10]; default: <b>8</b>	The number of successful tests before considering that the link is alive.
Metric	Same as configured	The metric value of this interface.

#### 4.8.2.3 Members

In **Members** sub-tab within the Configuration tab under Network -> LB and Failover Submenu, user can add/view/edit members of each interface. Each member represents an interface with a metric and a weight value. The same name used in the **Member** column under the **Members** sub-tab is also used in the **Members assigned** column under the **Policies** sub-tab. Members must be referenced in the **Policies** sub-tab to define a pool of interfaces with the corresponding metric and load-balancing weight. Members cannot be used for rules directly. Figure 4.45 shows the webpage in the **Members** sub-tab within the Configuration tab under Network -> LB and Failover Submenu. Table 4.35 describes the setting parameters of Figure 4.45.

Member	Interface	Metric	Weight	Sort	
wan_m1_w3	wan	1	3	▼ ▲	<a href="#">Edit</a> <a href="#">Delete</a>
wan_m2_w3	wan	2	3	▼ ▲	<a href="#">Edit</a> <a href="#">Delete</a>
mobile_m1_w2	mobile	1	2	▼ ▲	<a href="#">Edit</a> <a href="#">Delete</a>
mobile_m2_w2	mobile	2	2	▼ ▲	<a href="#">Edit</a> <a href="#">Delete</a>

[Add](#)

Figure 4.45. Members Sub-tab within the Configuration tab under Network -> LB and Failover Submenu

Table 4.35. Setting Parameters of the Members Sub-tab within the Configuration tab under Network -&gt; LB and Failover Submenu

Field	Description
Member	A name to define this member profile.
Interface	The interface that the member is applied to. Must use the same interface name as what is used in the Interfaces sub-tab.
Metric	Within the same policy, the members with a lower metric have precedence over the higher metric members.
Weight	Members that have the same metric will share the load based on this weight value.


To add a member, user must enter the name and click . The router will redirect to webpage as shown in Figure 4.46 where its description is shown in Table 4.36.



Figure 4.46. After Clicking Edit/Add Button in the Members Sub-tab under Network -&gt; LB and Failover Submenu -&gt; the Configuration Tab

Table 4.36. Parameters in the Members Sub-tab under Network-&gt;LB and Failover Submenu-&gt;the Configuration Tab

Field	Value	Description
Interface	wan/mobile; default: <b>wan</b>	Virtual Router Redundancy Protocol (VRRP) interface.
Metric	integer [1 – 1000]; default: <b>1</b>	The metric value of this interface, where the larger number means the higher priority. This value is 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: <b>4</b>	The smaller number means the lower weight.

#### 4.8.2.4 Policies

User can configure the policy for traffic behavior in the **Policies** sub-tab within the Configuration tab under Network -> LB and Failover Submenu. **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 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 4.47 shows the current policy of traffic behaviour used in the Policies Sub-tab under Network->LB and Failover Submenu->the Configuration Tab, where the parameters are described in Table 4.37.

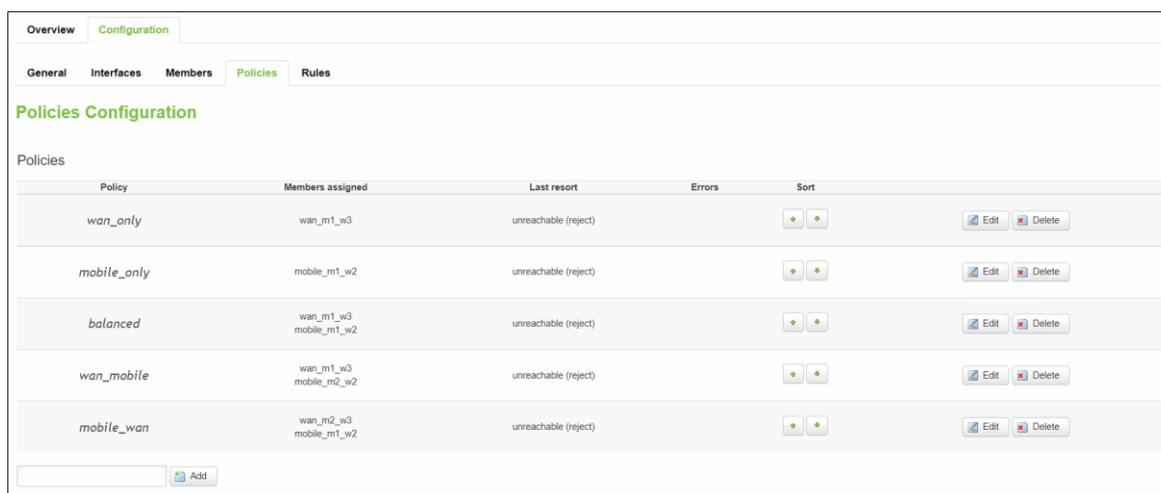



Figure 4.47. In the Policies Sub-tab under Network->LB and Failover Submenu->the Configuration Tab

Table 4.37. Parameters in the Policies Sub-tab under Network->LB and Failover Submenu->the Configuration Tab after Clicking Edit/Add Button

Field	Description
Policy	A name to define this policy profile.
Member Assigned	Member's name that 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". The valid values are blackhole, unreachable, or default.

To add a policy, user must enter the name and click . The router will redirect to webpage as shown in Figure 4.48 where its description is shown in Table 4.38.

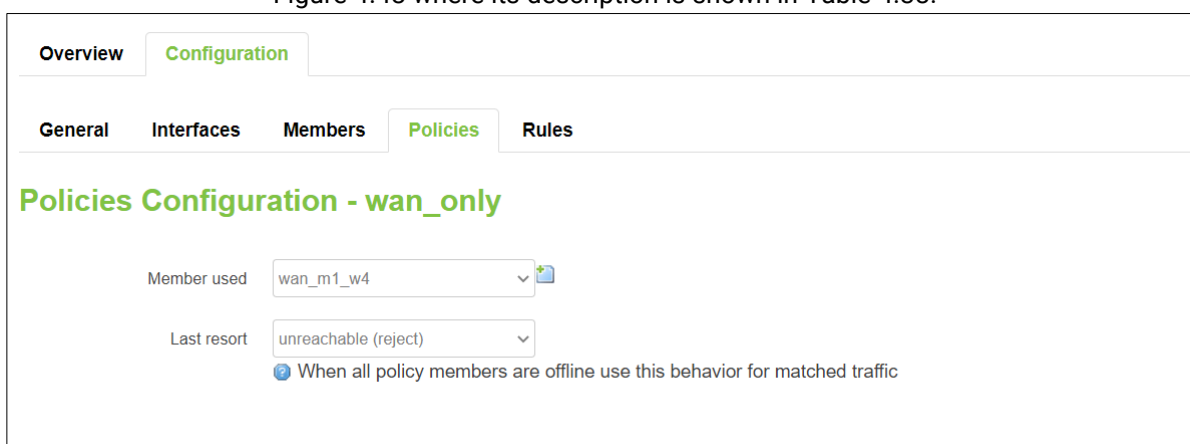


Figure 4.48. After Clicking Edit/Add Button in the Policies Sub-tab under Network -> LB and Failover Submenu -> the Configuration Tab

Table 4.38. Parameters in the Policies Sub-tab under Network->LB and Failover Submenu->the Configuration Tab after Clicking Edit/Add Button

Field	Description
Member used	The member that is assigned to this policy.
Last resort	Determine the fall back routing behaviour if all WAN members in the policy are down.

#### 4.8.2.5 Rules

User can configure the rule for traffic behavior in the **Rules** sub-tab within the Configuration tab under Network -> LB and Failover Submenu. A **rule** describes what traffic to match and what policy to assign for that traffic. Figure


4.49 shows the Rules Sub-tab under Network->LB and Failover Submenu->the Configuration Tab where Table 4.51 describes the parameters within Figure 4.49.

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		

Figure 4.49. In the Rules Sub-tab under Network->LB and Failover Submenu->the Configuration Tab

Table 4.39. Parameters in the Rules Sub-tab under Network->LB and Failover Submenu->the Configuration Tab

Field	Description
Rule	A name that is used to define this rule profile.
Source Address	Match traffic from the specified source IP address.
Source Port	If the relevant protocol is specified, match traffic from the specified source port or port range.
Dest. Address	Match traffic that is directed to the specified destination's IP address.
Dest. Port	Match traffic that is directed to the given destination port or port range, if the relevant protocol is specified.
Protocol	Match traffic using the given protocol which can be in term of the protocol name (e.g., TCP, UDP, ICMP, or all), or a numeric value which represents any of these protocols.
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 which has a value in seconds.

To add a rule, user must enter the name and click . The router will redirect to webpage as shown in Figure 4.50 where its description is shown in Table 4.40.

**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

Figure 4.50. After Clicking Edit/Add Button in the Rules Sub-tab under Network -> LB and Failover Submenu -> the Configuration Tab

Table 4.40. Parameters in the Rules Sub-tab under Network->LB and Failover Submenu->the Configuration Tab after Clicking Edit/Add Button

Field	Value	Description
Source Address	IP/submask; default: <b>none</b>	Match traffic from the specified source IP address.
Source Port	port; default: <b>none</b>	If the relevant protocol is specified, match traffic from the specified source port or port range.
Destination Address	IP/submask; default: <b>none</b>	Match traffic that is directed to the specified destination's IP address.
Destination Port	port; default: <b>none</b>	Match traffic that is directed to the given destination port or port range, if the relevant protocol is specified.
Protocol	TCP/UDP/ICMP; default: <b>TCP</b>	Match traffic using the given protocol which can be in term of the protocol name (e.g., TCP, UDP, ICMP, or all), or a numeric value which represents any of these protocols.
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: <b>600</b>	Stickiness timeout which has a value in seconds.
IPset	string; default: <b>none</b>	Match traffic that is directed at the given destination domain name address to an IP set.
Policy assigned	default: <b>balanced</b>	Type of the assigned policy.



## 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.

User can configure the router's firewall function in the Network->Firewall submenu. There are four tabs under this Network-> Firewall submenu: **General Settings**, **Port Forwards**, **Traffic Rules**, and **Attack Prevention**. In the **General Settings** tab, user can view the general configuration and zone configuration, and enable/disable forward blocking of LAN and Wi-Fi. In the **Port Forwards** tab, user can add a new rule of port forward. In the **Traffic Rules** tab, user can open ports on the router, add a new forward rule, and add a new source NAT. In the **Attack Prevention** tab, user can set an attack prevention on SYN Flood, SSH Attack, Http/Https Attack, and Port scan.

### 4.9.1 General Settings Tab

#### 4.9.1.1 General Configuration

The **General Settings** tab in the Network->Firewall submenu 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. Figure 4.51 show the general configuration webpage under Network -> Firewall Submenu where the parameters within the webpage is described in Table 4.41. Here user can click/unclick to enable/disable SYN-flood protection and drop invalid packets according to the value set in the Input, Output, and Forward fields.

Figure 4.51. General Configuration Subsection in the General Settings Tab under Network -> Firewall Submenu

The explanation of the value within the Input, Output, and Forward fields is as follows:




- Accept: Packet is allowed to continue down to the next chain.
- Drop: Packet is stopped and deleted.
- Reject: Packet is stopped and deleted with a returning ICMP packet.

The *Reject* rule immediately rejected the ICMP echo requests with a *Destination Port Unreachable* error. On the other hand, for *Drop*, the ICMP echo request timed out after a while. That is, *Reject* will be used to disallow trusted hosts by gracefully informing them that the traffic is not allowed to pass, and *Drop* will be used in an attempt to cause delays and disruption to a no so persistent attacker by sending their packets into a black hole without any response for them to analyse.

Table 4.41. Parameters in the General Settings Tab under Network -&gt; Firewall Submenu

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

#### 4.9.1.2 Zones Configuration

A **zone** is a group of network interfaces. By default, all interfaces within a zone are allowed to initialize network communication with each other, but any network traffic initialized outside of a zone to the interfaces within the zone is denied. Forwardings are used to allow traffic to traverse zones. Policy actions are used to define how traffic passing through a zone forwarding is filtered. Zones can be added, edited, or deleted by clicking  icon,  icon, and  icon, respectively.

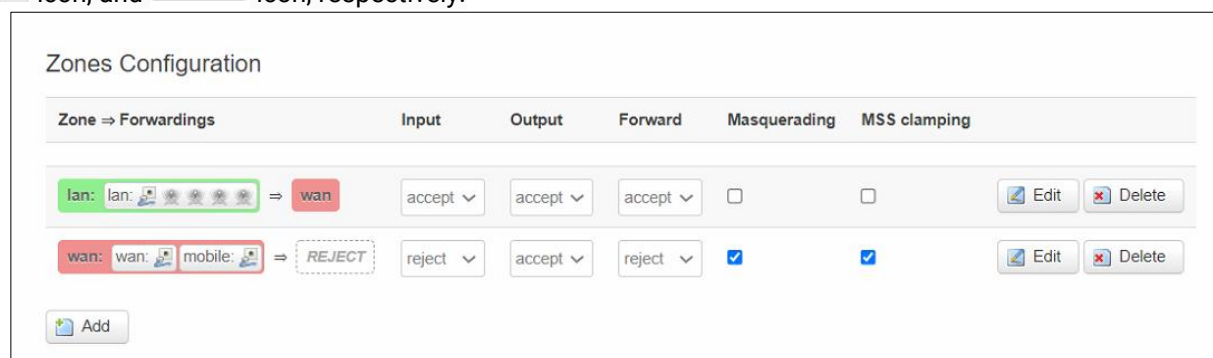


Figure 4.52. Zone Configuration Subsection in the General Settings Tab under Network-&gt;Firewall Submenu



Table 4.42. Parameters under the General Settings Tab under Network-&gt;Firewall Submenu-&gt; Zone Configuration Subsection

Field	Description
Zone=>Forwardings	The zone=>Forwardings column contains the source zone which data packets will be redirected from, and the destination zone which data packets will be redirected to.
Input	Action to be performed for packets that pass through the Input chain.
Output	Action to be performed for packets that pass through the Output chain.
Forward	Action 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 the outgoing zone traffic.

##### 4.9.1.2.1 Zones Configuration - Zone "lan"

There are two sub-tabs within Zone Configuration – Zone "lan": General Settings and Advanced Settings.

##### 4.9.1.2.1.1 General Settings

User can add a new firewall zone to LAN interface by first clicking  icon. Then, user can name the firewall zone "lan" and select lan interface for the Covered Networks. For the already defined zone, user can click  icon to reconfigure the zone. If user would like to remove that zone from all interfaces, user can unclick all interfaces in the covered networks field. Figure 4.53 shows Zone "lan" webpage after clicking Add/Edit button in Zone Configuration Subsection under Network->Firewall Submenu->General Settings Tab, where its description is in Table 4.43.

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: lan
Input: accept
Output: accept
Forward: accept
Masquerading: ☐
MSS clamping: ☐
Covered networks:
☒ lan:
☐ mobile:
☐ wan:
☐ xl2tpd:

Figure 4.53. After Clicking Add/Edit in Zone Configuration Subsection – Zone "Lan" under Network->Firewall Submenu->General Settings Tab

Table 4.43. Parameters in Zone Configuration Subsection – Zone "Lan" under Network->Firewall Submenu->General Settings Tab

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.
Covered Networks	Click the corresponding interface to apply this firewall zone to. There are four supported interfaces for this router: lan, mobile, wan, and xl2tpd.





#### 4.9.1.2.1.2 Advanced Settings

The screenshot shows the 'Advanced Settings' tab for the 'Lan' zone. It contains the following settings:

- Restrict to address family:** A dropdown menu set to 'IPv4 and IPv6'.
- Restrict Masquerading to given source subnets:** A text input field containing '0.0.0.0/0' with an 'Add' icon to its right.
- Restrict Masquerading to given destination subnets:** A text input field containing '0.0.0.0/0' with an 'Add' icon to its right.
- Force connection tracking:** An unchecked checkbox.
- Enable logging on this zone:** An unchecked checkbox.

Figure 4.54. After Clicking Add/Edit in Zone Configuration Subsection – Zone “Lan” under Network->Firewall Submenu->Advanced Settings Tab

Table 4.44. Parameters in Zone Configuration Subsection – Zone “Lan” under Network->Firewall Submenu->Advanced Settings Tab

Field	Description
Restrict to address family	Two choices are available here: IPv4 only, IPv4 and IPv6.
Restrict Masquerading to given source subnets	Click  icon to add masquerading IP address and netmask for the given source subnets. Click  icon to delete masquerading IP address and netmask that is no longer needed.
Restrict Masquerading to given destination subnets	Click  icon to add masquerading IP address and netmask for the given destination subnets. Click  icon to delete masquerading IP address and netmask that is no longer needed.
Force connection tracking	Enable/Disable connection tracking.
Enable logging on this zone	Enable/Disable logging on this zone.

Inter-Zone Forwarding option controls the forwarding policies between this zone (lan) and the other zones. As shown in Figure 4.55, user can control firewall zone by clicking **Allow forward to destination** or **Allow forward from source 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.

The screenshot shows the 'Inter-Zone Forwarding' section. It includes a descriptive paragraph and two configuration options:

**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:** This option is checked with a blue checkbox. Below it, a red button contains the text 'wan: wan: mobile:' with small icons next to each zone name.
- Allow forward from source zones:** This option is unchecked with a grey checkbox. Below it, a red button contains the text 'wan: wan: mobile:' with small icons next to each zone name.

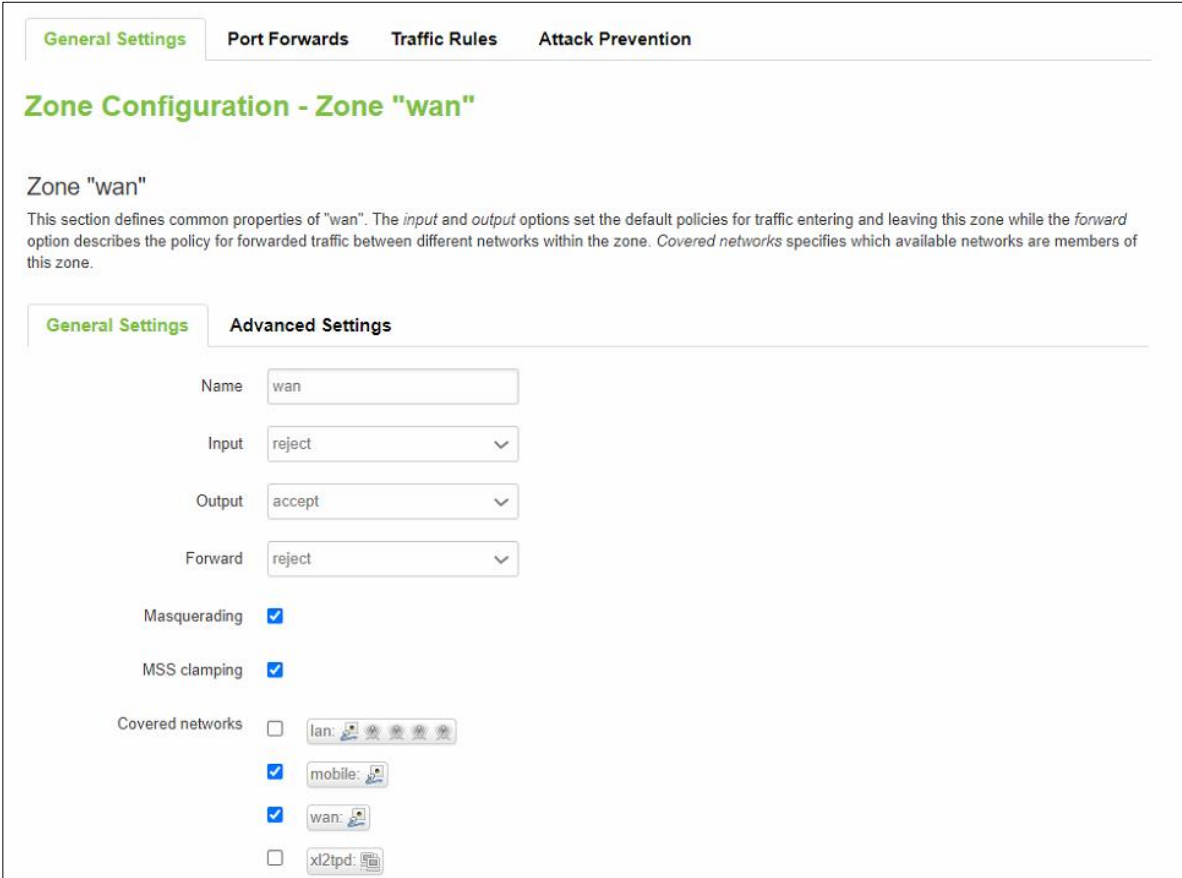
Figure 4.55. Inter-Zone Forwarding in Zone Configuration Subsection – Zone “Lan” under Network->Firewall Submenu->General Settings Tab

#### 4.9.1.2.2 Zone Configuration-WAN

There are two sub-tabs within Zone Configuration – Zone “wan”: General Settings and Advanced Settings.

##### 4.9.1.2.2.1 General Settings

User can add a new firewall zone to WAN interface by first clicking  icon. Then, user can name the firewall zone “wan” and select wan interface for the Covered Networks. For the already defined zone, user can click  icon to reconfigure the zone. If user would like to remove that zone from all interfaces, user can unclick all interfaces in the covered networks field. Figure 4.56 shows Zone “wan” webpage after clicking Add/Edit button in Zone Configuration Subsection under Network->Firewall Submenu->General Settings Tab, where its description is in Table 4.47.



**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:

Input:

Output:

Forward:

Masquerading: ☒

MSS clamping: ☒

Covered networks:





- ☐ lan: 
- ☒ mobile: 
- ☒ wan: 
- ☐ xl2tpd: 

Figure 4.56. After Clicking Add/Edit in Zone Configuration Subsection – Zone “wan” under Network->Firewall Submenu->General Settings Tab

Table 4.45. Parameters in Zone Configuration Subsection – Zone “wan” under Network->Firewall Submenu->General Settings Tab

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.
Covered Networks	Click the corresponding interface to apply this firewall zone to. There are four supported interfaces for this router: lan, mobile, wan, and xl2tpd.

## 4.9.1.2.2.2 Advanced Settings

General Settings **Advanced Settings**

Restrict to address family: IPv4 and IPv6

Restrict Masquerading to given source subnets: 0.0.0.0/0

Restrict Masquerading to given destination subnets: 0.0.0.0/0

Force connection tracking: ☐

Enable logging on this zone: ☐

Figure 4.57. After Clicking Add/Edit in Zone Configuration Subsection – Zone “wan” under Network->Firewall Submenu->Advanced Settings Tab

Table 4.46. Parameters in Zone Configuration Subsection – Zone “wan” under Network->Firewall Submenu->Advanced Settings Tab

Field	Description
Restrict to address family	Two choices are available here: IPv4 only, IPv4 and IPv6.
Restrict Masquerading to given source subnets	Click  icon to add masquerading IP address and netmask for the given source subnets. Click  icon to delete masquerading IP address and netmask that is no longer needed.
Restrict Masquerading to given destination subnets	Click  icon to add masquerading IP address and netmask for the given destination subnets. Click  icon to delete masquerading IP address and netmask that is no longer needed.
Force connection tracking	Enable/Disable connection tracking.
Enable logging on this zone	Enable/Disable logging on this zone.

Inter-Zone Forwarding is the option to 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 role is unidirectional, e.g., a forward from lan to wan does not imply a permission to forward from wan to lan as well.

**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:

Figure 4.58. Inter-Zone Forwarding in Zone Configuration Subsection – Zone “wan” under Network->Firewall Submenu->General Settings Tab

#### 4.9.2 Port Forwards Tab

The **Port forwarding** tab in the Network->Firewall submenu is used to configure port forwards rules of the xxR5805 device's firewall. **Port forwarding** allows remote computers on the Internet to connect to a specific computer or a 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 4.59 show the Port Forward's configuration webpage under Network -> Firewall Submenu where the parameters within the webpage is described in Table 4.47. There are two sections within this **Port forwarding** tab: **Port Forwards Rules** and **New Port Forward Rule**. In the **Port Forwards Rules** section, a list of rules for forwarding traffic through port is displayed. In the **New Port Forward Rule** section, user can add a new port forwarding rule. Here, user can enter a new name of port forwarding rule, select protocol, select internal and external zones as well as ports that are used, and enter an internal IP address and port before clicking  icon.

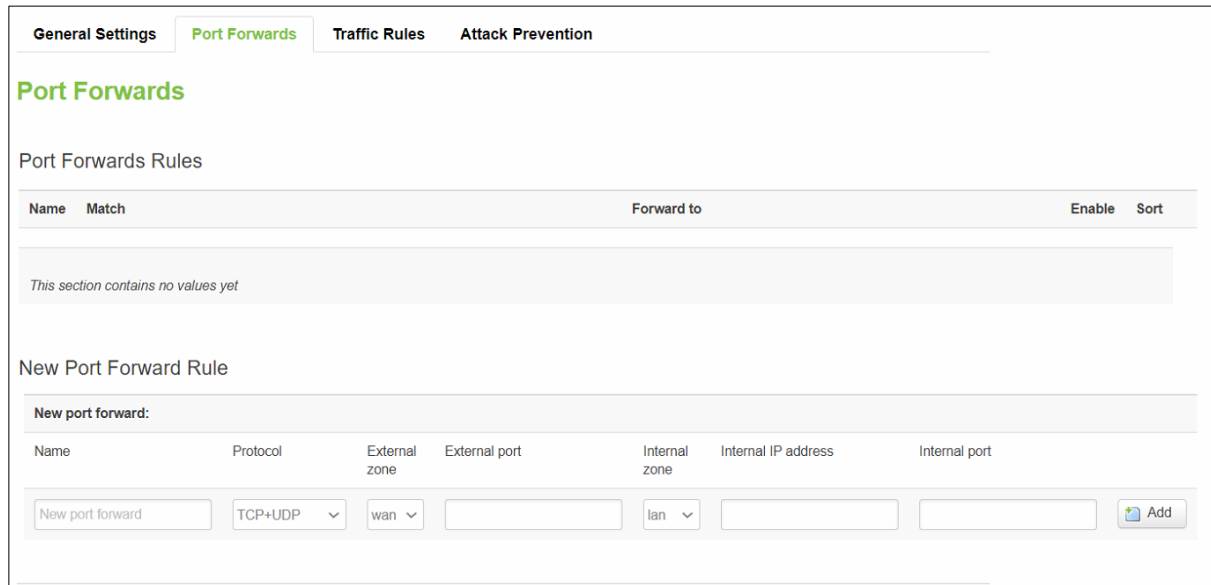


Figure 4.59. Port forwarding Tab in the Network->Firewall Submenu

Table 4.47. Parameters in the Port Forwards Rules Section under the Network->Firewall Submenu->Port Forwarding Tab

Field	Description
Name	To simplify the management, name of the port forward rule is set here.
Match	Display matched conditions of the port forwarding rule.
Forward to	Display the port information of the forward destination when the rule is matched with the conditions.

Table 4.48. Parameters in the New Port Forwards Rules Section under the Network-&gt;Firewall Submenu-&gt;Port Forwarding Tab

Field	Value	Description
Name	default: <b>Empty</b>	To simplify the management, name of the port forward rule is set here.
Protocol	default: <b>TCP+UDP</b>	Specify type of protocol of the incoming packet.
External Zone	default: <b>wan</b>	Specify the WAN network that data traffic will be redirected from.
External Port	integer [0-65535]   range of integers [0-65534] - [1-65535]; default: <b>none</b>	Traffic will be forwarded from this port on the WAN network. The rule will try to match port number of the source port used by the connecting host with the port number(s) specified in this field. Leave this field empty to skip matching.
Internal Zone	integer [0-65535]   range of integers [0-65534] - [1-65535]; default: <b>none</b>	Specify the LAN network that data traffic will be redirected to.
Internal IP Address	default: <b>Empty</b>	The IP address of the internal machine that hosts services that user wants to access from the outside.
Internal Port	default: <b>lan</b>	The rule will redirect the data traffic to this port on the internal machine.

#### 4.9.3 Traffic Rules Tab

The **Traffic Rules** tab in the Network->Firewall submenu is used to display and configure traffic rules of the xxR5805 device's firewall. **Traffic Rules** contains a more generalized rule definition. User can block or open ports, alter how traffic is forwarded between LAN and WAN, and many other things. Figure 4.60 show the Traffic Rules' configuration webpage under Network -> Firewall Submenu where the parameters within the webpage is described in Table 4.49. There are four sections within this **Traffic Rules** tabs: **Traffic Rules**, **Open Ports on Router**, **New Forward Rule**, and **Source NAT**. In the **Traffic Rules** section, rules to match traffic are displayed as well as their explanation. Here, actions that would be taken for matching rules are also displayed as well as the priorities of traffic rules. In the **Open Ports on Router** section, user can configure ports to which traffic will be redirected from the specified zones. In the **New Forward Rule** section, user can create a custom zone for forwarding rules. Lastly, in the **Source NAT** section, a packet's source address and/or port number can be disguised into a static and user-defined value.



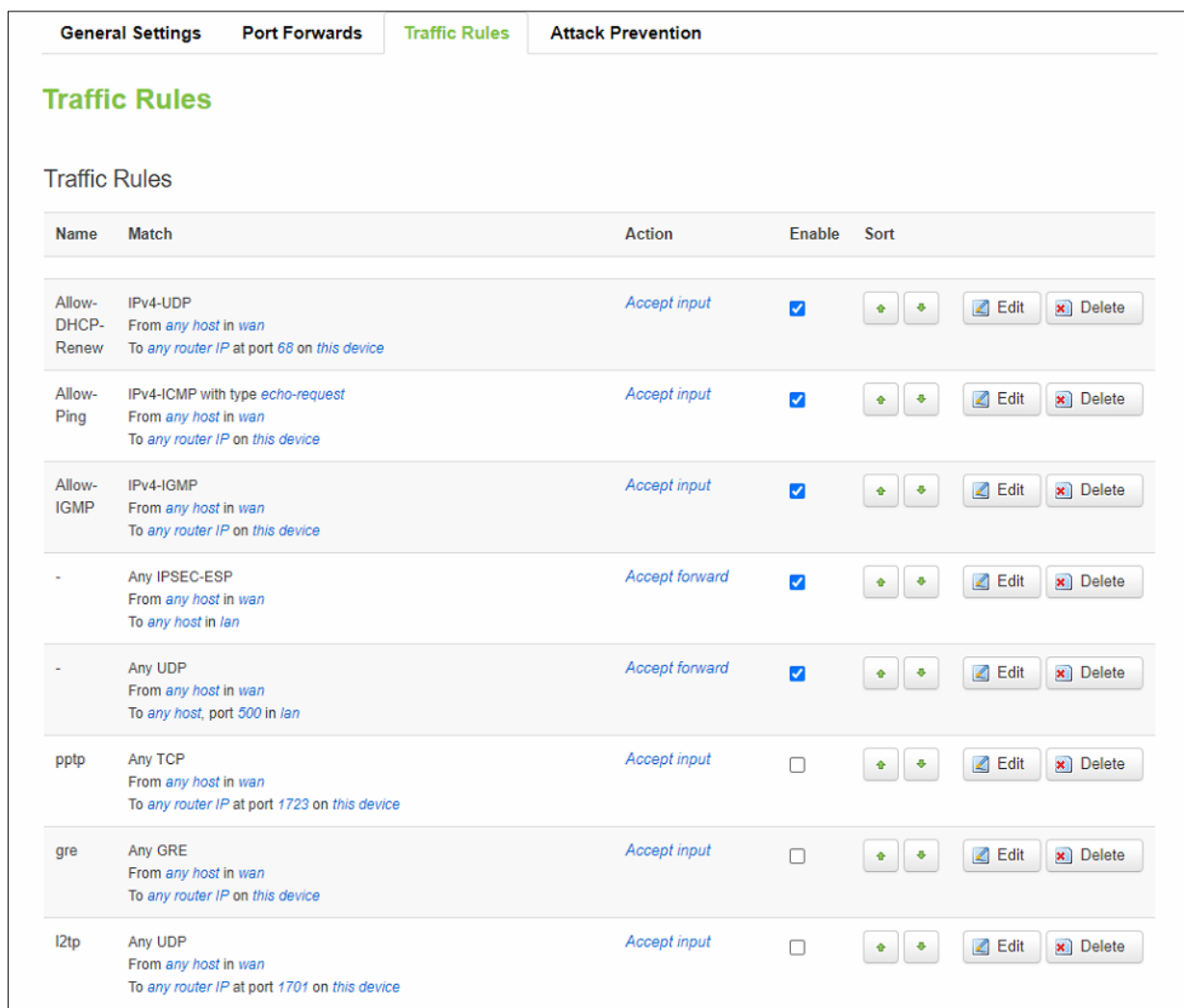


Figure 4.60. Traffic Rules Section under the Network-&gt;Firewall Submenu-&gt;Traffic Rules Tab

Table 4.49. Parameters in Traffic Rules Section under the Network-&gt;Firewall Submenu-&gt;Traffic Rules Tab

Field	Description
Name	To simplify the management, name of the traffic rule is set here.
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

In the **Open Ports on Router** section within the **Traffic Rules** tab in the Network->Firewall submenu, user can open certain ports and forwarding traffic from the specified zones to these ports by entering a new rule name, selecting a transport protocol, and specifying a port number before clicking **Add** icon.

Figure 4.61. Open Ports on Router Section under the Network-&gt;Firewall Submenu-&gt;Traffic Rules Tab

Table 4.50. Parameters in Open Ports on Router Section under the Network-&gt;Firewall Submenu-&gt;Traffic Rules Tab

Field	Description
Name	To simplify the management, name of the traffic rule is set here.
Protocol	Specify which protocols that the rule should be applied to.
External Port	Specify which port should be opened.
Add	Add a new open port on the router rule.

#### 4.9.3.1.2 New Forward Rule

In the **New Forward Rules** section within the **Traffic Rules** tab in the Network->Firewall submenu, user can customarily create zone for forwarding rules which are firewall rules that control traffic on the FORWARD chain, by entering a new forwarding rule, a source zone, and a destination zone before clicking **Add and edit** button. Figure 4.62 shows the New Forward Rules section under the Network->Firewall Submenu->Traffic Rules Tab, where the description is shown in Table 4.51.

Figure 4.62. New Forward Rules Section under the Network-&gt;Firewall Submenu-&gt;Traffic Rules Tab

Table 4.51. Parameters in New Forward Rules Section under the Network-&gt;Firewall Submenu-&gt;Traffic Rules Tab

Field	Description
Name	To simplify the management, name of the traffic rule is set here.
Source Zone	Match incoming traffic from the selected address family only.
Destination Zone	Forward incoming traffic to the selected address family only.

#### 4.9.3.1.3 Source NAT

In the **Source NAT** section within the **Traffic Rules** tab in the Network->Firewall submenu, user can disguise a packet's source address and port number by using static predefined values instead. Source NAT is performed in the POST ROUTING chain, just before a packet leaves the router/device. It allows the mapping of multiple WAN addresses to internal subnets.

To configure a new source NAT, user can enter a new SNAT rule, a source and destination zones, and a source IP address and port, before clicking **Add and edit** button, as shown in Figure 4.63Figure 4.62. The description of Source NAT's parameters is described in Table 4.52.

**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
New SNAT rule	lan	wan	-- Please choose	Do not rewrite

[Add and edit...](#)

Figure 4.63. Source NAT Section under the Network-&gt;Firewall Submenu-&gt;Traffic Rules Tab

Table 4.52. Parameters in the Source NAT Section under the Network-&gt;Firewall Submenu-&gt;Traffic Rules Tab

Field	Description
Name	To simplify the management, name of the traffic rule is set here.
Source Zone	Select interface that source zone is applied to; i.e., GuestWiFi, lan, and wan.
Destination Zone	Select interface that destination zone is applied to; i.e., GuestWiFi, lan, and wan.
To Source IP	Disguise or NAT only the incoming traffic from the specified source IP address.
To Source Port	Disguise or NAT only the incoming traffic from the specified source port.

#### 4.9.4 Attack Prevention Tab

In the **Attack Prevention** tab under the Network->Firewall submenu, user can configure security on the attack prevention. There are the total of four preventions/sections within this tab: **SYN Flood Protection**, **SSH Attack Prevention**, **Http/Https Attack Prevention**, and **Port Scan**.

##### 4.9.4.1 SYN Flood Protection

**SYN flood attacks** work by exploiting the handshake process of a TCP connection. Under normal conditions, the client sends a SYN packet to the server in order to initiate the connection. The server then responds to that initial packet with a SYN/ACK packet, in order to acknowledge the communication. Finally, the client returns an ACK packet to acknowledge the receipt of the packet from the server. After completing this sequence of packet sending and receiving, the TCP connection is open and able to send and receive data. In networking, when a server is leaving a connection open but the machine on the other side of the connection is not, the connection is considered half-open. In this type of DDoS attack, the targeted server is continuously leaving open connections and waiting for each connection to timeout before the ports become available again.

**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 ☒

Figure 4.64. SYN Flood Protection Section under the Network-&gt;Firewall Submenu-&gt;Attack Prevention Tab

User can configure SYNC flood protection in the **SYN Flood Protection** section under the Network->Firewall submenu->Attack Prevention tab. In this webpage, user can enable the SYN Flood Protection, set the SYN Flood rate and burst, and click to allow TCP SYN cookies, as shown in Figure 4.64Figure 4.62. The description of SYN Flood Protection's parameters is described in Table 4.53. A SYNC flood attack exploits the normal TCP three-way handshake, so that resources on the target is consumed and rendered unresponsively. Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than what the targeted machine can process, causing network saturation.

Table 4.53. Parameters in SYN Flood Protection Section under the Network->Firewall Submenu->Attack Prevention Tab

Field	Value	Description
Enable	default: <b>enable</b>	Enable/Disable the router to be more resistant to SYN flood attacks.
SYN flood rate	integer [1 to 10000]; default: <b>25</b>	When SYN packet is considered flooding, set rate limit (in packets/second) for the received traffic
SYN flood burst	integer [1 to 10000]; default: <b>50</b>	When SYN packets is considered flooded, set burst limit for the received traffic, so it will not exceed the allowed rate.
TCP SYN cookies	default: <b>enable</b>	Enable the use of SYN cookies (particular choices of initial TCP sequence numbers by TCP servers).

#### 4.9.4.2 SSH Attack Prevention

An **SSH Brute Force attack** is a form of cybersecurity attack in which an attacker uses trial and error to guess credentials to access a server. Cybercriminals rely on weak or guessable credentials. It is fairly simple and have a high success rate, with several tools and programs available for attackers to use. Once an attacker correctly guesses valid credentials, they may be able to view, copy, or delete important files or execute malicious code.

SSH Attack Prevention

Enable ☒

Limit period Second

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

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

Figure 4.65. SSH Attack Prevention Section under the Network->Firewall Submenu->Attack Prevention Tab

User can configure SSH attack prevention in the **SSH Attack Prevention** section under the Network->Firewall submenu->Attack Prevention tab. In this webpage, user can enable the SSH Attack Prevention, as well as set the limit period and limit burst, as shown in Figure 4.65Figure 4.62. The description of SSH Attack Prevention's parameters is described in Table 4.54. SSH attack prevention allows user to remotely run commands on a machine's command prompt and prevents attacks by limiting connections in a defined period.

Table 4.54. Parameters in SSH Attack Prevention Section under the Network->Firewall Submenu->Attack Prevention Tab

Field	Value	Description
Enable	default: <b>enable</b>	Enable/Disable SSH attack prevention using the connection limit within the selected period.
Limit period	Second/Minute/Hour/Day; default: <b>Second</b>	Set the period that SSH connections are limited in term of second/minute/hour/day.
Limit period	integer [1 to 10000]; default: <b>5</b>	Set the maximum number of SSH connections that are allowed during the period.
Limit burst	integer [1 to 10000]; default: <b>10</b>	Indicate the maximum allowed burst of SSH connections before the limitation in period and in connections begins.

#### 4.9.4.3 Http/Https Attack Prevention

In a Slow Post DDoS attack, the attacker sends legitimate HTTP POST headers to a Web server, which includes a 'Content-Length' field to specify the size of the message body that will follow. However, the attacker then proceeds to send the actual message body at an extremely slow rate, e.g., 1 byte/110 seconds but not slowly enough for the server to time out. 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. When attackers launch hundreds or even thousands Slow POST attacks at the same time, server resources are rapidly consumed, making legitimate connections unachievable.

User can configure Http/Https attack prevention in the **Http/Https Attack Prevention** section under the Network->Firewall submenu->Attack Prevention tab. In this webpage, user can enable the Http/Https Attack Prevention, as well as set the limit period and limit burst, as shown in Figure 4.66. The description of Http/Https Attack Prevention's parameters is described in Table 4.55

Figure 4.66. SSH Attack Prevention Section under the Network->Firewall Submenu->Attack Prevention Tab  
Table 4.55. Parameters in Http/Https Attack Prevention Section under the Network->Firewall Submenu->Attack Prevention Tab

Field	Value	Description
Enable	default: <b>enable</b>	Enable/Disable Http/Https attack prevention using the connection limit within the selected period.
Limit period	Second/Minute/Hour/Day; default: <b>Second</b>	Set the period that Http/Https connections are limited in term of second/minute/hour/day.
Limit period	integer [1 to 10000]; default: <b>5</b>	Set the maximum number of Http/Https connections that are allowed during the period.
Limit burst	integer [1 to 10000]; default: <b>10</b>	Indicate the maximum allowed burst of Http/Https connections before the limitation in period and in connections begins.

#### 4.9.4.4 Port Scan

**Port Scan** attacks scan to discover which 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 that they can gain an access to the sensitive data or they can execute a 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 under the Network->Firewall submenu->Attack Prevention tab provides user with the possibility to enable protection against port scanning software. User can defend his/her machines by enabling protections from the following types of online attacks, which include **SYN-FIN**, **SYN-RST**, **X-Mas**, **FIN scan**, and **NULLflags** attacks. As shown in Figure 4.67. The description of Port Scan's parameters is described in Table 4.56.

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 ☒


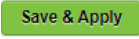
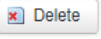
NULL flags attack ☒

Figure 4.67. Port Scan Section under the Network-&gt;Firewall Submenu-&gt;Attack Prevention Tab

Table 4.56. Parameters in Port Scan Section under the Network-&gt;Firewall Submenu-&gt;Attack Prevention Tab

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

#### 4.10 Static Routes

In Network->Static Routes Submenu, user can configure custom static routes by specifying the interface and gateway that a certain host or network can be reached. As shown in Figure 4.68, user can click  icon to insert a new static route. Some parameters must be entered before clicking  icon. User can click  icon to delete a static route that is no longer needed. The description of static routes' parameters is described in Table 4.57.

Static Routes

Static IPv4 Routes

Interface	Target	IPv4 Netmask	IPv4 Gateway	Metric	MTU
lan	192.168.1.2	255.255.255.0	10.0.50.254	10	1500

 Add 

Figure 4.68. Network -&gt; Static Routes Submenu

Table 4.57. Parameters in Network -&gt; Static Routes Submenu

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 used to determine to the actual IP addresses that 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 Dynamic Routes

**Dynamic routes** specify the interface and gateway that a certain host or network can be reached. User can configure the custom dynamic routes in this webpage. There are two tabs within this Network->Dynamic Rules submenu: RIP and OSPF.

### 4.11.1 RIP Protocol

Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an Administrative Distance (AD) of 120 and works on the Network layer of the OSI model. RIP uses port number 520. There are two versions of RIP: RIPv1 and RIPv2.

RIPv1 uses classful routing. The periodic routing updates do not carry subnet information, lacking support for variable length subnet masks (VLSM). This limitation makes it impossible to have different-sized subnets inside of the same network class. In other words, all subnets in a network class must have the same size. There is also no support for router authentication, making RIP vulnerable to various attacks.

RIPv2 is a classless, distance vector routing protocol as defined in RFC 1723. Being a classless routing protocol, means, it includes the subnet mask with the network addresses in its routing updates.

User can configure RIP In the **RIP** tab under the Network->Dynamic Routes submenu. There are three sections within this tab: General Settings, RIP Interfaces, and Access List Filters.

#### 4.11.1.1 General Settings

Figure 4.69.shows the webpage of General Settings Section under the Network -> Dynamic Routes Submenu-> RIP Tab. In this page, user can configure the followings. User can click to enable dynamic routing RIP and Virtual teletype (vty). VTY is a virtual port and used to get Telnet or SSH access to the device. VTY is solely used for inbound connections to the device. User can select version of RIP. Currently two version RIPv1 and RIPv2 are supported. Lastly, user can configure neighbour.

Figure 4.69. General Settings Section under the Network -> Dynamic Routes Submenu-> RIP Tab

Table 4.58. Parameters in the General Settings Section under the Network -> Dynamic Routes Submenu-> RIP Tab

Field	Description
Enable	Enable/Disable dynamic RIP routing protocol.
Enable vty	Enable/Disable vty and allow inbound connection to the device.
Version	Currently RIP supports v1 and v2.
Neighbor	Typically RIP messages are sent in broadcast or multicast. To enable RIP on a link that does not support broadcast or multicast, user must manually specify RIP neighbors.

#### 4.11.1.2 RIP Interfaces

Figure 4.70 shows the webpage of RIP Interfaces Section under the Network -> Dynamic Routes Submenu-> RIP Tab. User can configure RIP Interface' name, RIP interface, and enable Passive Interface. RIP interfaces are the interfaces that RIP updates will be sent on. Sometimes, it is pointless to send RIP updates on the interface that there are no other RIP routers on. Passive interface will ensure that the network is advertised in RIP but it will not send RIP updates on the interface. Table 4.59 describes the parameters shown in Figure 4.70.

##### RIP Interfaces

Name	Interface	Passive Interface	Enable
<input type="text"/>	<div> <div>wan</div> <div>wan</div> <div>lan</div> </div>	<input type="checkbox"/>	<input type="checkbox"/>





 Add  Delete

Figure 4.70. RIP Interfaces Section under the Network -> Dynamic Routes Submenu-> RIP Tab

Table 4.59. Parameters in the RIP Interface Section under the Network -> Dynamic Routes Submenu-> RIP Tab



Field	Description
Name	Name of the routing interface. This is only for the simplification of the management.
Interface	The interface that RIP updates will be sent on, e.g., wan or lan.
Passive Interface	Enable/Disable passive interface where the network is advertised in RIP but it will not send RIP updates on the interface.
Enable	Enable/Disable RIP interface.

#### 4.11.1.3 Access List Filters

User can restrict what routing information is exchanged within RIP by filtering inbound RIP routes on a per interface basis with access list filters. User can click  Add icon to add dynamic RIP routes and click  Delete icon to delete existed RIP routes. As shown in Figure 4.71, user can configure access list filters (ALF) by entering ALF's name, and selecting RIP interface that ALF will be applied to. Also, user must input what action must be taken (e.g., Permit and Deny) when the condition is matched, network to route to (i.e., IP address and netmask), and the direction that routing is applied (i.e., inbound or outbound). Table 4.60 shows the description of the parameters in Figure 4.71

##### Access List Filters

Name	RIP Interface	Action	Network	Direction	Enable
<input type="text"/>	wan-m1	Permit	ip/mask ex: 10.10.10.0/24	<div>Inbound</div> <div>Inbound</div> <div>Outbound</div>	<input type="checkbox"/>

 Add  Delete

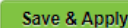

 Save & Apply  Reset

Figure 4.71. Access List Filters Section under the Network -> Dynamic Routes Submenu-> RIP Tab

Table 4.60. Parameters in the Access List Filters Section under the Network -> Dynamic Routes Submenu-> RIP Tab



Field	Description
Name	Name of the access list filter (ALF)
RIP Interface	Same as names created in the RIP Interfaces section
Action	Action taken when conditions in ALF is matched (e.g., permit or deny)
Network	IP Address/ Mask e.g., 10.10.10.0/24
Direction	Direction that routing is applied to (i.e., inbound or outbound)
Enable	Enable/Disable ALF function on RIP protocol

#### 4.11.2 OSPF Protocol

OSPF is an interior gateway protocol (IGP) that routes packets within a single autonomous system (AS). OSPF uses link-state information to make routing decisions, making route calculations using the shortest-path-first (SPF) algorithm (also referred to as the Dijkstra algorithm). Each router running OSPF floods link-state advertisements throughout the AS or area that contain information about that router's attached interfaces and routing metrics. Each router uses the information in these link-state advertisements to calculate the least cost path to each network and create a routing table for the protocol.

User can configure OSPF in the **OSPF** tab under the Network->Dynamic Routes submenu. There are three sections within this tab: General Settings, OSPF Interfaces, and OSPF Networks.

##### 4.11.2.1 General Settings

Figure 4.72 shows the webpage of General Settings Section under the Network -> Dynamic Routes Submenu-> OSPF Tab. In this page, user can configure the followings. User can click to enable dynamic routing OSPF and Virtual teletype (vty). VTY is a virtual port and used to get Telnet or SSH access to the device. VTY is solely used for inbound connections to the device. User can select Router ID in term of IP address. Lastly, user can select Passive Interfaces which include none, lan, or wan.

#### OSPF Protocol

##### General Settings

Enable service ☐

Enable vty ☐

Router ID

Passive interfaces 

none

none  
lan  
wan

Figure 4.72. General Settings Section under the Network -> Dynamic Routes Submenu-> OSPF Tab  
Table 4.61. Parameters in the General Settings Section under the Network->Dynamic Routes Submenu->OSPF Tab

Field	Description
Enable service	Enable/Disable dynamic OSPF routing
Enable vty	Enable/Disable vty and allow inbound connection to the device.
Router ID	Specify router ID in x.x.x.x
Passive interfaces	Enable/Disable passive interface where the network is advertised in OSPF but it will not send OSPF updates on the interface. Supported options here are none, lan, or wan interface.

##### 4.11.2.2 OSPF Interfaces

Figure 4.73 shows the webpage of OSPF Interfaces Section under the Network -> Dynamic Routes Submenu-> OSPF Tab. User can configure OSPF Interface and enable this dynamic routing interface. Table 4.62 describes the parameters shown in Figure 4.73. Note that user needs to add a Router ID in the General Settings section under the OSPF protocol tab first in order to add interface in the OSPF Interface section.

## OSPF Interface

Interface	Enable	
wan	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>
wan		
lan		

Figure 4.73. OSPF Interfaces Section under the Network -&gt; Dynamic Routes Submenu-&gt; OSPF Tab

Table 4.62. Parameters in the OSPF Interfaces Section under the Network-&gt;Dynamic Routes Submenu-&gt;OSPF Tab

Field	Description
Interface	Define OSPF interface that OSPF updates will be sent on, e.g., wan or lan.
Enable	Enable/Disable OSPF Interface

After clicking Edit button in OSPF Interfaces section under the Network -> Dynamic Routes submenu-> OSPF tab, Figure 4.74 is launched. Here, user can configure OSPF protocol in more details. For example, user can set interface, cost, hello interval time, router dead interval time, number of retransmissions, priority, type (i.e., Broadcast, non-Broadcast, point to point, and point to multipoint), and authentication type (i.e., none, password, MD5-HMAC). Table 4.63 describes the parameters shown in Figure 4.74

## OSPF Protocol

Enable ☐

Interface

Cost

Hello interval

Router Dead interval

Retransmit

Priority

Type

Authentication

Figure 4.74. After Clicking Edit Button in OSPF Interfaces Section under the Network -&gt; Dynamic Routes Submenu-&gt; OSPF Tab

Table 4.63. Parameters of OSPF Protocol after Clicking Edit Button in the OSPF Interfaces Section under the Network->Dynamic Routes Submenu->OSPF Tab

Field	Description
Enable	Enable/Disable OSPF dynamic routing protocol.
Interface	Define OSPF interface that OSPF updates will be sent on, e.g., wan or lan.
Cost	The value of metric and uses a Reference Bandwidth of 100 Mbps for cost calculation. The formula to calculate the cost is Reference Bandwidth divided by interface bandwidth. For example, in the case of 10 Mbps Ethernet , OSPF Metric Cost value is 100 Mbps / 10 Mbps = 10
Hello Interval	Specifies the length of time, in seconds, before the routing device sends a hello packet out of an interface.
Router Dead Interval	The number of seconds that a neighbor router waits for a hello packet from the device before declaring the router down.
Retransmit	A limit to the number of retransmissions of database exchange and update packets for both demand and non-demand circuits.
Priority	Priority in OSPF is mainly used to influence/determine a designated router/backup designated router for a network. By default, the priority is 1 on all routers. The larger the numeric value of the priority, the higher the chances for it to become the designated router. Setting a priority of 0 makes the router ineligible to become a designated router or back up designated router.
Type	There are total of four network type supported (i.e., Broadcast, non-Broadcast, point to point, and point to multipoint). The <b>Broadcast</b> network type is the default for an OSPF enabled Ethernet interface. The Broadcast network type requires that a link support Layer 2 Broadcast capabilities. The Broadcast network type has a 10 second hello and 40 second dead timer. <b>Non-broadcast</b> multiple access (NBMA) is one of four network types in the Open Shortest Path First (OSPF) communications protocol. In an NBMA network all hosts are connected on a single network, but data is sent from one host directly to the next host and is not broadcast across to all hosts. A <b>Point-to-Point</b> network type is, as its name implies, a connection between two specific points (or OSPF routers). On a point-to-point link, a packet delivered from one of the routers will always have precisely one recipient. The <b>Point-to-Multipoint</b> (PtMP) network type in OSPF is ideal for network segments that do not provide full mutual connectivity between the attached routers. The main characteristics of this network type are: Multicasts are still used to allow the neighbors to detect each other dynamically. There is no DR or BDR elected.
Authentication	Three types of OSPF can be configured: None: No authentication. Default value is none. Password: Clear text authentication where passwords are exchanged in clear text on the network, MD5 HMAC:: A cryptographic method using the open stand Message Digest type 5 (MD5) encryption.

#### 4.11.2.3 OSPF Networks

Figure 4.75 shows the webpage of OSPF Networks Section under the Network -> Dynamic Routes Submenu-> OSPF Tab. User can configure OSPF Network's name, Network (IP address and netmask), Area (IP address or area value) and enable OSPF Networks. Table 4.64 describes the parameters shown in Figure 4.75.

## OSPF Networks

Name	Network	Area	Enable	
<input type="text"/>	<input type="text" value="ip/mask ex: 10.10.10.0/24"/>	<input type="text" value="ip address or area value"/>	<input type="checkbox"/>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>				
<input type="button" value="Save &amp; Apply"/> <input type="button" value="Reset"/>				

Figure 4.75. OSPF Networks Section under the Network -&gt; Dynamic Routes Submenu-&gt; OSPF Tab

Table 4.64. Parameters in the OSPF Networks Section under the Network-&gt;Dynamic Routes Submenu-&gt;OSPF Tab

Field	Description
Name	Name of the OSPF Network. This is only for the simplification of the management.
Network	IP Address/ Mask e.g., 10.10.10.0/24
Area	OSPF area is a collection of networks, not a collection of routers. A backbone network segment is an IP subnet that belongs to the area identified by 0.0. 0.0. Areas that are not physically connected to the backbone are logically connected by a backbone ABR using an OSPF virtual link.
Enable	Enable/Disable OSPF Network Area.

## 4.12 DNS

User can configure how the device utilizes its own and other DNS servers through the webpage under the Network->DNS submenu, as shown in Figure 4.76. Table 4.65 describes the parameters shown in Figure 4.76.

**DNS**

**DNS Settings**

Log queries ☐ Log the results of DNS queries

DNS server

Rebind protection ☒ Discard upstream RFC1918 responses

Local Service Only ☒

Listen Interfaces ☐ LAN  
☐ WAN

Filter private ☒ Do not forward reverse lookups to local networks

Localise queries ☒

Size of DNS query cache   
 0 is no caching, max is 10000

Figure 4.76. Network -&gt; DNS Submenu

Table 4.65. Parameters in the Network -&gt; DNS Submenu

Field	Value	Description
Log queries	enable/disable; default: <b>disable</b>	When enabled, write the received DNS requests to syslog.
DNS server	default: none	List of DNS servers to forward requests to.
Rebind protection	enable/disable; default: <b>enable</b>	Discard upstream RFC1918 responses. When enabled, the device will not resolve domain names for the internal hosts.
Local Service Only	enable/disable; default: <b>enable</b>	Limit DNS service to subnets and interfaces on which this device is serving as a DNS server.
Listen Interfaces	LAN/WAN; default: <b>none</b>	Limits listening for DNS queries to interfaces specified in the field and loopback. Leave this field empty to listen on all interfaces.
Filter private	enable/disable; default: <b>enable</b>	Do not forward reverse lookups for local networks.
Localise queries	enable/disable; default: <b>enable</b>	Localise hostname depending on the requesting subnet if multiple IP addresses are available.
Size of DNS query cache	Integer [0 to 10000]; default: <b>none</b>	Number of cached DNS entries. Set to 0 for no caching.

### 4.13 QoS

The **QoS (Quality of Service)** webpage under the Network->QoS submenu is used to set up Smart Queue Management (SQM) instances which can limit the download and upload speeds of selected network interfaces, as shown in Figure 4.77 - Figure 4.78. Table 4.66 describes the parameters shown in both figures.

This manual page provides an overview of the QoS windows.





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

Figure 4.77. Network -&gt; QoS Submenu

## QoS-LAN

### QoS-LAN Settings

Enable Total Bandwidth ☐

Download (kbps/s)

Upload (kbps/s)

Enable User Bandwidth ☐

Download (kbps/s)

Upload (kbps/s)

Figure 4.78. QoS-LAN/WiFi24/WiFi5 Setting Webpage after Clicking Edit Button in the Network -&gt; QoS Submenu

Table 4.66. Parameters in the QoS-LAN/WiFi24/WiFi5 Setting Page after Clicking Edit Button in the Network -&gt; QoS Submenu

Field	Value	Description
Enable Total Bandwidth	disable/enable; Default: <b>disable</b>	Overall Speed limits for all LANs.
Download (kbps/s)	integer [0 - 1000000]; default: <b>30000</b>	Limits the download speed (ingress) of the selected interface to the value specified in this field.
Upload (kbps/s)	integer [0 - 1000000]; default: <b>30000</b>	Limits the upload speed (egress) of the selected interface to the value specified in this field.
Enable User Bandwidth	disable/enable; Default: <b>disable</b>	Speed limits for each user.
Download (kbps/s)	integer [0 - 1000000]; default: <b>30000</b>	Limits the download speed (ingress) of the selected interface to the value specified in this field.
Upload (kbps/s)	integer [0 - 1000000]; default: <b>30000</b>	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** (Network Time Protocol), **VPN** (Virtual Private Network), **GPS** (Global Positioning System), **VRRP** (Virtual Router Redundancy Protocol) and **MQTT** (Message Queueing Telemetry Transport). These are the services running inside the xxR5805 router.

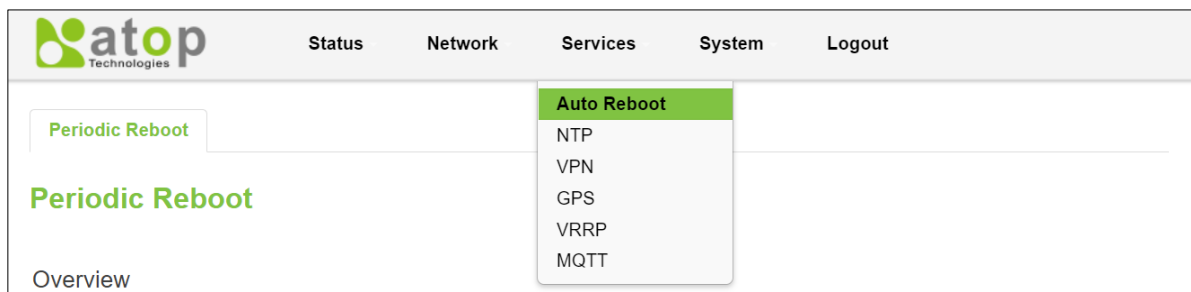


Figure 5.1. Services

### 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 5.2 shows an example of **Overview** webpage of **Periodic Reboot**. It shows whether the reboot is enabled on which day(s) of the week and when (at what time) it will be rebooted. To configure the Periodic Reboot, click on the **Edit** button at the end of the row. See the next subsection on how to configure the periodic reboot feature.

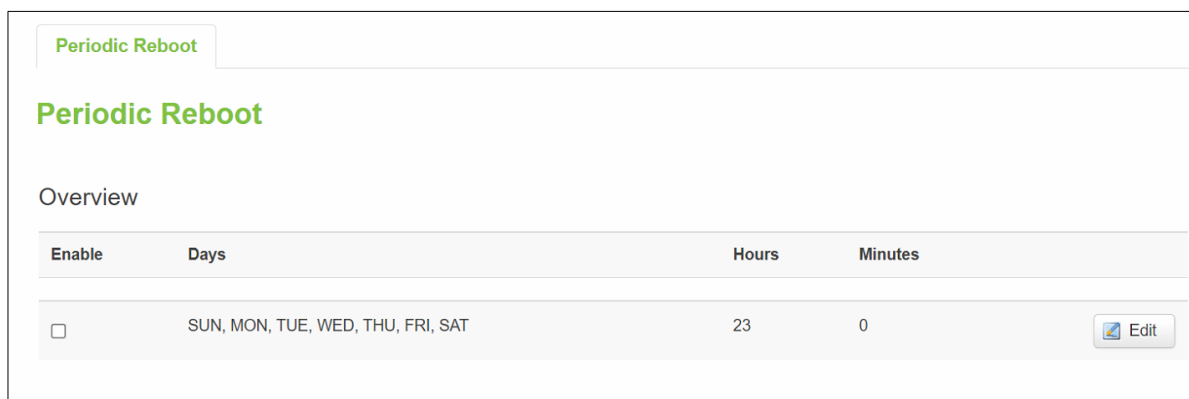


Figure 5.2. Service -> Auto Reboot

#### 5.1.1 Periodic Reboot – Configuration

Once the user click on the **Edit** button, the webpage is updated as shown in Figure 3.5. The first option is the Enable's check box. To enable the periodic reboot, check the box behind the **Enable** field. Then, select the desired day(s) of the week on the check box(es) behind the **Days** field. Then, enter the **Hours** between 0 and 23 and the **Minutes** between 0 and 59. Table 5.1 summarizes the description of each option for editing the periodic reboot.

Periodic Reboot

## 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]

Figure 5.3. Service -&gt; Auto Reboot -&gt; Edit

Table 5.1. Service -&gt; Auto Reboot -&gt; Edit

Field	Value	Description
Enable	default: <b>disable</b>	This check box will enable or disable Periodic reboot feature.
Days	SUN/MON/TUE/WED/THU/FRI/SAT; default: <b>SUN/MON/TUE/WED/THU/FRI/SAT</b>	Rebooting will be done on that specific day(s).
Hours	integer [0 – 23] hours; default: <b>23</b>	Rebooting will be done on that specific hour.
Minutes	integer [0 – 59] minutes; default: <b>0</b>	Rebooting will be done on that specific minute.

## 5.2 NTP

### 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. This enables you to synchronize the time of the router to a reference system called time server. The user can synchronize the time values of xxR5805 device in the **General** section within NTP sub-menu. Figure 5.4 shows the General webpage under the NTP sub-menu. It displays the current system time at the top of the page. There are two buttons next to the current system time: **Sync with browser** and **Sync with GPS**. The next option is the drop-down list of **Timezone** that can be selected. The user can enable or disable the NTP by checking or unchecking the **Enable NTP** checkbox. Additional time settings includes the **Update Interval (in seconds)** and the **Count of time measurements**. The user can enter the update interval for NTP in seconds and/or value for the count of time measurement that the NTP client on the router will perform the time synchronization with NTP server. Note that the empty value for count of time value represents infinite count of time synchronization. Finally, the last option called **GPS synchronization** if checked will enable the router to use GPS module for periodic synchronization of the system time. Table 5.2 summarizes the descriptions of the options under the General NTP setting.



**NTP**

General

Current system time 2021-11-10 14:46:28

Timezone Asia/Taipei

Enable NTP ☒

Update interval (in seconds) 600

Count of time measurements   
empty = infinite

GPS synchronization ☐ Enable to use GPS module for periodic time synchronization of the system time (no require internet connection)

Figure 5.4. Services -&gt; NTP -&gt; General

Table 5.2. Services -&gt; NTP -&gt; General

Field	Value	Description
Sync with browser	(none)	Sync with browser.
Sync with GPS	(none)	Sync with GPS.
Time zone	default: <b>UTC</b>	Time zone of your country.
Enable NTP	default: <b>enable</b>	Enable system's time synchronization with time server using NTP (Network Time Protocol).
Update Interval (in seconds)	default: <b>600</b>	Frequency that the NTP client service on xxR5805 device will update the time.
Count of Time Measurements	default: <b>none</b>	The amount of times that NTP client service on xxR5805 device will perform time synchronizations. Leave it empty if set to infinite.
GPS synchronization	default: <b>disable</b>	Enable to use GPS module for periodic time synchronization of the system time.

### 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 5.5 shows a list of Time Servers where each entry in the list contains the **Hostname** and the corresponding **Port** number. To remove an entry from the list, click the **Delete** button. To add a new NTP server, click on the **Add** button. Table 5.3 summarizes the descriptions of fields for Time Servers.

Time Servers

Hostname	Port
time.nist.gov	123

Figure 5.5. Services -&gt; NTP -&gt; Time Servers

Table 5.3. Services -&gt; NTP -&gt; Time Servers

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

### 5.3 VPN

A **virtual private network** (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private networks, while benefiting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. 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→VPN** 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 or enabled by default. To configure the **sample\_server** and **sample\_client**, click on the corresponding **Edit** buttons as shown in Figure 5.6 and follow the steps provided in the next two subsections. Once the setup is ready, you can click on the **Start** button to start the OpenVPN service or **Stop** button to end the service. Clicking on the **Refresh** button to obtain the latest status. Table 5.4 provides the descriptions of fields under the OpenVPN Overview webpage.

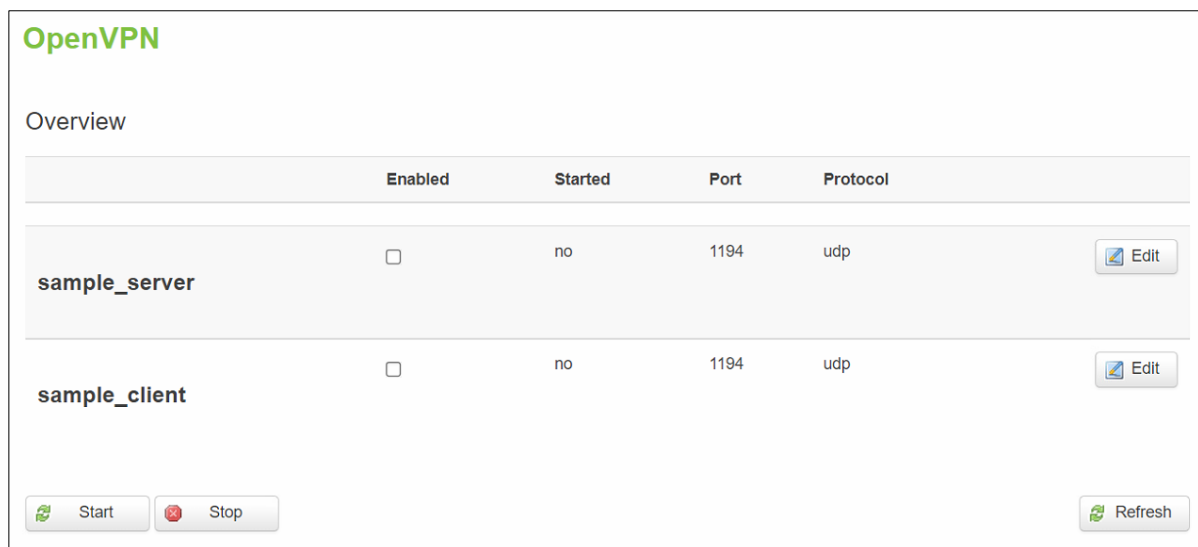


Figure 5.6. Services -&gt; VPN -&gt; OpenVPN -&gt; Overview

Table 5.4. Services -&gt; VPN -&gt; OpenVPN -&gt; Overview

Field	Description
Enabled	To enable/disable selected OpenVPN service instance.
Started	Display whether the current OpenVPN service is started or not.
Port	Display the port number that the specified OpenVPN service is listening on.

Field	Description
Protocol	Display TCP/UDP protocol that the OpenVPN service used.
Edit	Click this button to configure selected OpenVPN service instance.
Start/Stop	Click these buttons to start or stop selected OpenVPN service.

### 5.3.1.2 OpenVPN Server

To configure OpenVPN server service, click **Edit** button at the end of the "sample\_server" entry to edit OpenVPN server instance. The editing webpage which contains the default OpenVPN server instance's configuration is initialized as shown in Figure 5.7. Note that the edit webpage here is for basic setting.

**Overview » Instance "sample\_server"**

Enable ☐

TUN/TAP

Protocol

Port

LZO

Authentication

Encryption

Route traffic between clients ☐

Push option

Keepalive interval

Keepalive timeout

HMAC algorithm

Certificate authority  No file chosen

Server certificate  No file chosen

Server key  No file chosen

Diffie Hellman parameters  No file chosen

CRL file (optional)  No file chosen

**Clients Setting**

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

Figure 5.7. Services -&gt; VPN -&gt; OpenVPN -&gt; sample\_server -&gt; Edit

Table 5.5 summarizes the description of each field or option of the OpenVPN's sample server.

Table 5.5. Services -&gt; VPN -&gt; OpenVPN -&gt; sample\_server -&gt; Edit

Field	Value	Description
Enable	Enable/Disable; default: <b>Disable</b>	Switches configuration to enable or disable. This option must be selected or enabled to make configuration active.
TUN/TAP	TUN (Tunnel)   TAP (Bridged); default: <b>TUN (Tunnel)</b>	Virtual network device type: <ul style="list-style-type: none"> <li><b>TUN</b> - a virtual point-to-point IP link which operates at the network layer (OSI layer 3), used when routing is required.</li> <li><b>TAP</b> - a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.</li> </ul>
Protocol	UDP/TCP; default: <b>UDP</b>	Transfer protocol used by the OpenVPN connection. <ul style="list-style-type: none"> <li><b>User Datagram Protocol (UDP)</b> - 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).</li> <li><b>Transmission Control Protocol (TCP)</b> - 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).</li> </ul>
Port	integer [1-65535] default: <b>1194</b>	TCP/UDP port number used for the connection. Make sure it matches the port number specified on the server side. <b>NOTE:</b> traffic on the selected port will be automatically allowed in the device firewall rules.
LZO	Adaptive/Yes/No; default: <b>Adaptive</b>	LZO data compression mode.
Authentication	TLS/Static Key; default: <b>TLS</b>	Authentication mode, used to secure data sessions. <ul style="list-style-type: none"> <li><b>TLS</b> authentication mode uses X.509 type certificates: <ul style="list-style-type: none"> <li>Certificate Authority (CA)</li> <li>Server certificate</li> <li>Server key</li> <li>Diffie Hellman parameters</li> <li>CRL file (optional)</li> </ul> </li> </ul> <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"> <li><b>Static key</b> is a secret key used for server-client authentication.</li> </ul>
Encryption	BF-CBC/AES-128-CBC/AES-192-CBC/AES-256-CBC/AES-128-GCM/AES-192-GCM/AES-256-GCM/none; default: <b>BF-CBC</b>	Algorithm used for packet encryption. BF-CBC= Blowfish-Cipher Block Chaining AES = Advanced Encryption Standard GCM = Galois/Counter Mode
Route traffic between clients	enable/disable; default: <b>disable</b>	Allows OpenVPN clients to communicate with each other on the VPN network.
Push option	default: <b>none</b>	Push options are a way to "push" routes and other additional OpenVPN options to connecting clients.

Field	Value	Description
Keepalive interval	integer [1 to 60]; default: <b>10</b>	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: <b>60</b>	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: <b>none</b>	This field specifies the tunnel's virtual IP and netmask.
HMAC algorithm	SHA1   SHA512   SHA384   SHA256   SHA224   MD5   None; default: <b>SHA1</b>	HMAC authentication algorithm type. SHA = Secure Hash Algorithm MD = Message Digest
Certificate authority	.ca file; default: <b>none</b>	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: <b>none</b>	A type of digital certificate that is used to identify the OpenVPN server.
Serve key	.key file; default: <b>none</b>	Authenticates clients to the server.
Diffie Helman parameters	.pem file; default: <b>none</b>	DH parameters define how OpenSSL performs the Diffie-Hellman (DH) key-exchange.
CRL file (optional)	.pem file   .crl file; default: <b>none</b>	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: <b>none</b>	Client's Common Name (CN) found in the client certificate file.
LAN Network	ip; default: <b>none</b>	Client's private network (LAN) IP address.
Netmask	netmask; default: <b>none</b>	Client's private network (LAN) IP netmask.
To Server LAN Side	default: <b>disable</b>	Enable LAN to LAN function

### 5.3.1.3 OpenVPN Client

To configure OpenVPN client service, click **Edit** button at the end of the "sample\_client" entry to edit OpenVPN client instance. The editing webpage which contains the default OpenVPN client instance's configuration is initialized as shown in Figure 5.8. Note that the edit webpage here is for basic setting. Table 5.6 summarizes the description of each field or option of the OpenVPN's sample client.

**Overview »** Instance "sample\_client"

Enable ☐

TUN/TAP

Protocol

Port

LZO

Authentication

Encryption

Remote host/IP address

Keepalive interval

Keepalive timeout

HMAC algorithm

Certificate authority  No file chosen

Client certificate  No file chosen

Client key  No file chosen

Figure 5.8. Services -&gt; VPN -&gt; OpenVPN -&gt; sample\_client -&gt; Edit

Table 5.6. Services -&gt; VPN -&gt; OpenVPN -&gt; sample\_client -&gt; Edit

Field	Value	Description
Enable	enable/disable; default: <b>disable</b>	Switches configuration enable or disable. This must be selected to make configuration active.
TUN/TAP	TUN (Tunnel)   TAP (Bridged); default: <b>TUN (Tunnel)</b>	Virtual network device type. <ul style="list-style-type: none"> <li><b>TUN</b> - a virtual point-to-point IP link which operates at the network layer (OSI layer 3), used when routing is required.</li> <li><b>TAP</b> - a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.</li> </ul>
Protocol	UDP/TCP; default: <b>UDP</b>	Transfer protocol used by the OpenVPN connection. <ul style="list-style-type: none"> <li><b>User Datagram Protocol (UDP)</b> - 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).</li> <li><b>Transmission Control Protocol (TCP)</b> - 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.</li> </ul>

Field	Value	Description
		It should be used when reliability is crucial (for example, in file transfer).
Port	integer [1-65535] default: <b>1194</b>	TCP/UDP port that the local OpenVPN server listening on. TCP/UDP port number is used for the connection. Make sure it matches the port number specified on the server side. <b>NOTE:</b> traffic on the selected port will be automatically allowed in the device firewall rules.
LZO	Adaptive/Yes/No; default: <b>Adaptive</b>	LZO data compression mode.
Authentication	TLS/Static Key; default: <b>TLS</b>	Authentication mode, used to secure data sessions. <ul style="list-style-type: none"> <li><b>TLS</b> authentication mode uses X.509 type certificates: <ul style="list-style-type: none"> <li>Certificate Authority (CA)</li> <li>Client certificate</li> <li>Client key: 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.</li> </ul> </li> <li><b>Static key</b> is a secret key used for server–client authentication.</li> </ul>
Encryption	BF-CBC/AES-128-CBC/AES-192-CBC/AES-256-CBC/ AES-128-GCM/AES-192- GCM /AES-256- GCM /none; default: <b>BF-CBC</b>	Algorithm used for packet encryption. BF-CBC= Blowfish-Cipher Block Chaining AES = Advanced Encryption Standard GCM = Galois/Counter Mode
Remote host/IP address	IP, netmask; default: <b>my_server_1 1194</b>	LAN IP address and LAN IP subnet of the remote network (server).
Keepalive interval	integer [1 to 60]; default: <b>10</b>	Frequency (in seconds) at which "keep alive" packets are sent to the remote instance.
Keepalive timeout	integer [10 to 180]; default: <b>60</b>	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/SHA512SHA384/SHA256/SHA224/MD5/None; default: <b>SHA1</b>	The authentication algorithm must match with another incoming connection (with server). SHA = Secure Hash Algorithm MD = Message Digest
Certificate authority	.ca file; default: <b>none</b>	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: <b>none</b>	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: <b>none</b>	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. The IPsec submenu consists of two tabs: **Settings** and **Status**.

IPsec (or Internet Protocol Security) which is a network protocol suit that can establish secure and reliable communications for different application scenarios. IPsec enables data confidentiality, data integrity, data origin authentication, and antireplay. For example, a corporate headquarter and its branch offices in the fields do not need to apply for dedicated communication lines for sharing their network resources securely. To securely communicate and shared company's resources over the Internet, IPsec connections can be employed to secure all applications at the IP layer. In another case, when employees are on a business trip, they can establish IPsec connections with their company over their mobile devices or the public network to access the internal network resources in their company.

The xxR5805 router has an IPsec connection function to establish a secure communication link between **host-to-host**, **host-to-subnet** (or host-to-network), and **subnet-to-subnet** (or network-to-network). Note that at the other endpoint of the Internet, a router or gateway with full IPsec capability is required to successfully establish the secure communication. There are two types of IPsec connection modes or types supported by xxR5805 router which are **Tunnel mode** and **Transport mode**.

- In **Tunnel mode**, the entire IP packet is encrypted and authenticated. The IP packet is then encapsulated into a new IP packet with a new IP header. The **Tunnel mode** which is used to create Virtual Private Network (VPN) can be applied to the **host-to-host**, the **host-to-subnet**, and the **subnet-to-subnet** communications. The packet (datagram) format for **Tunnel mode** is as follow:

New IP Header	IPsec Header	Original IP Packet	Optional IPsec Trailer
---------------	--------------	--------------------	------------------------

- In **Transport mode**, only the payload of the IP packet is usually encrypted or authenticated. The routing is intact because the IP header is not modified and not encrypted. However, when the authentication header is used, the IP addresses cannot be modified by Network Address Translation (NAT). The **Transport mode** can only be applied in the **host-to-host** communication. The packet (datagram) format for **Transport mode** is as follow:

Original IP Header	IPsec Header	Original IP Packet	Optional IPsec Trailer
--------------------	--------------	--------------------	------------------------

A **host-to-host** connection is typically used in a simple point-to-point communication. It is useful for a direct communication with a server or between the device (xxR5805 router) and a peer device (such as another xxR5805 router). Note that this type of connection cannot be use for accessing entire sub-network resources. Figure 5.9 illustrates an example of host-to-host connection. This configuration can be set in both **Tunnel mode** and **Transport mode**.

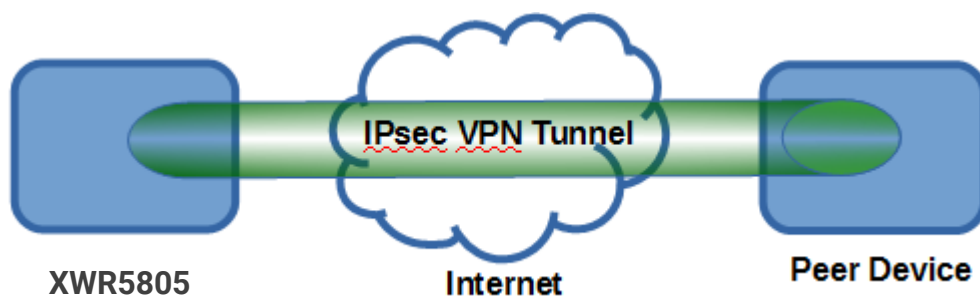


Figure 5.9 An Example of Host-to-Host Connection

A **host-to-subnet** (or host-to-network) connection is mainly applied when one endpoint needs to access the other side's sub-networks. Typical applications are employees who are travelling on business and would like to connect back to their corporate headquarters via mobile devices. They can establish IPsec connections to access the internal corporate network resources. Figure 5.10 illustrates a road-warrior application in which xxR5805 router can access a remote sub-network resource via a peer gateway. Figure 5.11 illustrates a gateway application in which



xxR5805 router can passively accept connection requests from remote sides and provide access to the xxR5805 sub-network resources. Note that both of these configurations must set the connection type to **Tunnel mode** only.

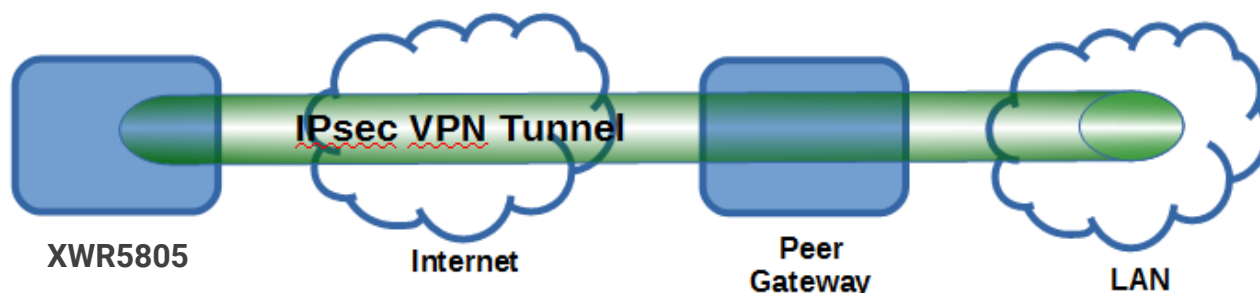


Figure 5.10 Roadwarrior Application using Host-to-Subnet Connection

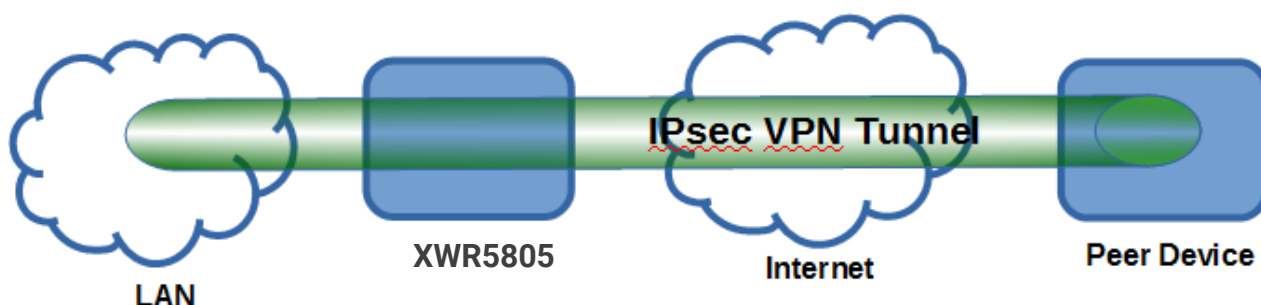


Figure 5.11 Gateway Application using Host-to-Subnet Connection

A **subnet-to-subnet** connection is mainly used to connect two subnets from different sides together. Typically, applications are corporate headquarters and branch offices that share internal network resources. A specific application can also be set up as one side's subnet to establish IPsec VPN tunnels for accessing a device in the other side's subnet or as a device in one's side subnet to establish IPsec VPN tunnels for accessing another device in the other side's subnet. Figure 5.12 illustrates an example of the subnet-to-subnet connection with a network application. A host inside the remote subnet can also connect to a local subnet (host-network application) based on this subnet-to-subnet connection as shown in Figure 5.13. On the other hand, two different devices on two different subnets (host-host application) can be connected via an IPsec VPN tunnel based on this subnet-to-subnet connection as shown in Figure 5.14. Note that all subnet-to-subnet configurations must set the connection type to **Tunnel mode** only.

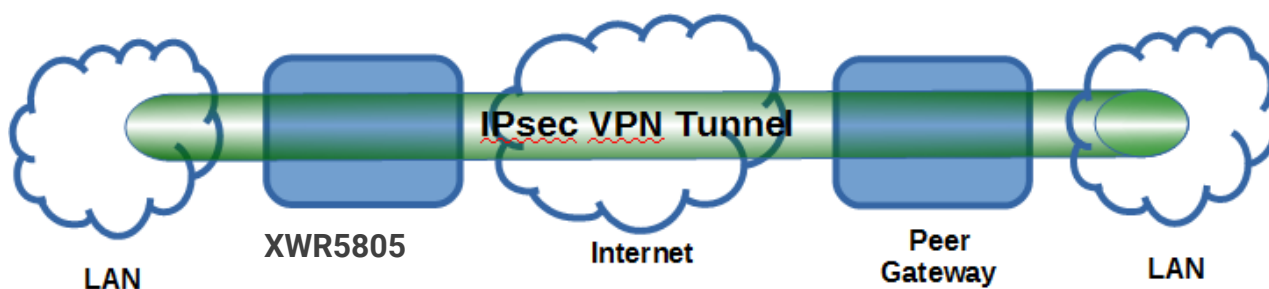


Figure 5.12 An example of network application using a subnet-to-subnet connection via the SE59XX and a peer device

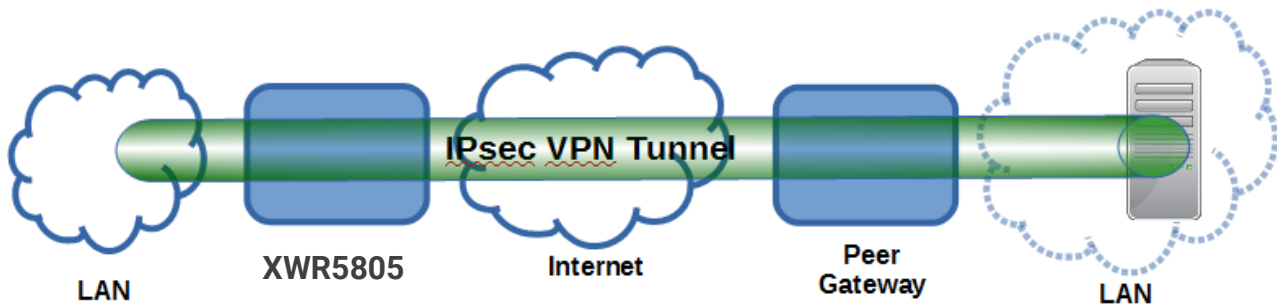


Figure 5.13 An example of host-network application via the subnet-to-subnet connection

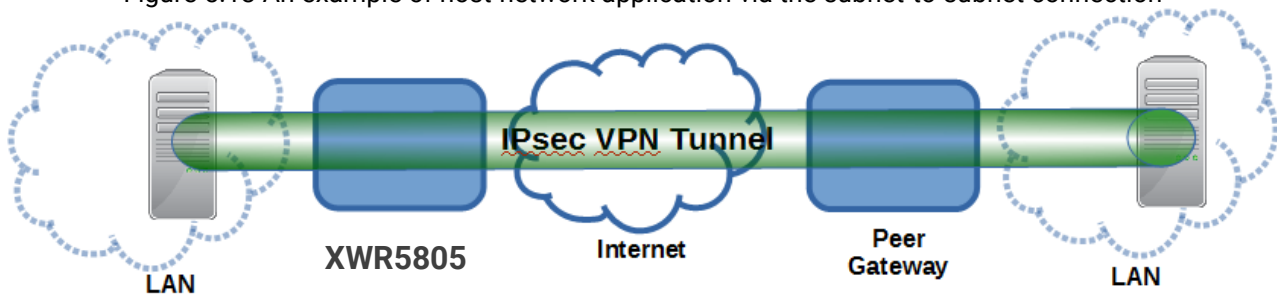


Figure 5.14 An example of host-host application via the subnet-to-subnet connection

In some network configuration, there is an implementation of network address translation (NAT) on its gateway/routers. NAT is typically used to allow private IP addresses on private networks behind gateways/routers with a single public IP address connecting to the public Internet. The internal network devices can communication with hosts on the external network by changing the source address of outgoing requests to that of the NAT device (gateway/router) and relaying replies back to the originating device. IPsec virtual private network (VPN) clients use network address translation (NAT) traversal in order to have Encapsulating Security Payload (ESP) packets traverse NAT. IPsec uses several protocols in its operation, which must be enabled to traverse firewalls and network address translators (NATs), such as

- Internet Key Exchange (IKE) protocol uses User Datagram Protocol (UDP) port number 500.
- Encapsulating Security Payload (ESP) uses IP protocol number 50.
- Authentication Header (AH) uses IP protocol number 51.
- IPsec NAT traversal uses UDP port number 4500 when NAT traversal is in use.

xxR5805 router also has a feature called NAT traversal (NAT-T) that allows the IPsec tunnel to pass through the NAT in its network. xxR5805 router will activate this option automatically and encapsulate the IPsec packets inside UDP port 4500 to be able to pass through a NAT router.

To provide security service for all types of tunnel connections and applications described above, xxR5805 router utilizes the Internet Key Exchange (IKE) protocol to set up a security association (SA) in the IPsec protocol suite. Note that IKE builds upon the Oakley protocol and ISAKMP (Internet Security Association and Key Management Protocol). IKE uses X.509 certificates for authentication either pre-shared or distributed using DNS (preferably with DNSSEC). IKE also uses a Diffie-Hellman key (DH) key exchange to set up a shared session secret from which cryptographic keys are derived. The IPsec security association (SA) is divided into two phases. In phase one, IKE creates an authenticated secure channel between xxR5805 router and its peer device, which is called the IKE Security Association. The Diffie-Hellman (DH) key agreement is always performed in this phase to create a shared secret key or DH key. In phase two, IKE negotiates the IPsec security associations and generates the required key material for IPsec. This IPsec key which is a symmetrical key will be used for bulk data transfer inside the IPsec tunnel. A new Diffie-Hellman agreement can be done in phase two, or the keys can be derived from the phase one shared secret.

### 5.3.2.1 IPSec – Settings

To configure IPSec, the user can select **Settings** tab as shown in Figure 5.15, Figure 5.16, and Figure 5.17. The first part of the IPSec **Settings** tab is called **General**. The user can enable IPSec in this part by checking the

**Enable** box. Then, the user must enter the **Remote host's** IP address, select the **Connection type**, and fill in **Local subnet/mask** and **Remote subnet/mask**. Optionally, the **Local protocol port** and **Remote protocol port** can be specified. The second part is called **Authentication**. The user can choose the authentication **Method** such as **Pre-shared key** or **X.509** from the drop-down list and fill in the pre-shared key in the next textbox. Optionally, the Local identifier and the Remote identifier can be entered in the corresponding textboxes.

The screenshot shows the IPsec Settings configuration interface. It is divided into two main sections: **General** and **Authentication**.

**General Section:**

- Enable:** A checkbox that is currently unchecked.
- Remote host:** A text input field.
- Connection type:** A dropdown menu with 'Tunnel' selected.
- Local subnet/mask:** A text input field containing '192.168.1.0/24'. A hint below says 'e.g. 192.168.1.0/24'.
- Remote subnet/mask:** A text input field containing '192.168.2.0/24'. A hint below says 'e.g. 192.168.2.0/24'.
- Local protocol port(Optional):** A text input field containing 'tcp/1500'. A hint below says 'e.g. tcp, tcp/1500, gre'.
- Remote protocol port(Optional):** A text input field containing 'tcp/1500'. A hint below says 'e.g. tcp, tcp/1500, gre'.

**Authentication Section:**

- Method:** A dropdown menu with 'Pre-shared key' selected.
- Pre-shared key:** A text input field with masked characters (dots). A hint below says 'Key should be in 8-63 characters'.
- Local identifier(Optional):** A text input field. A hint below says 'Under x509: if string clude '=' or '' , please add ""'. e.g. "CN=CWR\_Server"'.
- Remote identifier(Optional):** A text input field. A hint below says 'Under x509: if string clude '=' or '' , please add ""'. e.g. "CN=CWR\_Server"'.

Figure 5.15 Services -> VPN -> IPsec -> Settings (Part 1)

The third, the fourth, and the fifth parts under the IPsec's Settings tab are shown in Figure 5.16. These parts are actually Internet Key Exchange (IKE) settings. The third part is called Phase 1 proposal or Phase 1 SA (ISAKMP). There are five security options (Mode, Key exchange protocol, Encryption algorithm, Hash algorithm, and DH group) to be configured as shown in Figure 5.16. In phase 1, two VPN gateways exchange information about the encryption algorithms that they support and then establish a temporary secure connection to exchange authentication information. The fourth part is called Phase 2 proposal or Phase 2 SA. Within the Phase 2 SA, there are four security options to be configured. Similar to Phase 1 SA, the xxR5805 router and its peer device will negotiate or exchange proposals to determine which security parameters will be used in this Phase 2 SA. The fifth part has one more option for the Internet Key Exchange which is Phase 1 IKE lifetime. Finally, the sixth and the seventh parts of the IPsec's Settings tab are shown in Figure 5.17 which are used for setting the Dead Peer Detection's options and enabling the IPsec Enhancement option. Descriptions of these options are summarized in Table 5.7.

Phase 1 proposal

Mode

Key exchange protocol

Encryption algorithm

Hash algorithm

DH group

Phase 2 proposal

Security protocol

Encryption method

Hash algorithm

PFS DH group

Life time

Phase 1 IKE lifetime



 180-86400 seconds

Figure 5.16 Services -&gt; VPN -&gt; IPsec -&gt; Settings (Part 2)


Dead Peer Detection

Action

Interval

 30-3600 second

Timeout

 Multiples of 10 seconds. eg:60

IPSEC enhancement

Enable ☒

Figure 5.17 Services -&gt; VPN -&gt; IPsec -&gt; Settings (Part 3)

Table 5.7 Services -&gt; VPN -&gt; IPsec -&gt; Settings

Field	Value	Description
<b>General</b>		
Enable	default: <b>disable</b>	Check the box to enable the IPsec function.
Remote host	default: <b>none</b>	WAN IP address of the Server   blank
Connection type	Tunnel   Transport; Default: <b>Tunnel</b>	Two distinct modes of IPsec operation: Tunnel mode or Transport mode.
Local subnet/mask	default: <b>192.168.1.0/24</b>	(Only for tunnel mode) LAN IP address/Subnet mask of the router on which the IPsec instance is configured

Field	Value	Description
Remote subnet/mask (only for tunnel mode)	default: <b>192.168.2.0/24</b>	(Only for tunnel mode) LAN IP address/Subnet mask of the opposite router
Protocol over IPSEC	None   GRE   L2TP; default: <b>None</b>	(Only for transport mode) Only the selected protocol can be encrypted in IPsec tunnel.
Local protocol port (Optional)	default: <b>tcp/1500</b>	Only the selected protocol or port can be encrypted it.
Remote protocol port (Optional)	default: <b>tcp/1500</b>	Only the selected protocol or port can be encrypted it.
<b>Authentication</b>		
Method	Pre-shared key   X.509; default: <b>Pre-shared key</b>	Specify authentication method. Choose between Pre-shared key and X.509 certificates. <ul style="list-style-type: none"> <li>• <b>Pre-shared key</b> - A shared password used for authentication between the peers. The value of this field must match on both instances</li> <li>• <b>X.509</b> - 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.</li> </ul>
Local identifier (Optional)	default: <b>none</b>	Defines which protocol and port can be encrypted in IPsec on local side.
Remote identifier (Optional)	default: <b>none</b>	Defines which protocol and port can be encrypted in IPsec on remote side.
<b>Phase 1 proposal</b>		
Mode	Main   Aggressive; default: <b>Main</b>	Choose the mode for outgoing connections: <ul style="list-style-type: none"> <li>• <b>Main mode</b> - (a total of 6 messages) by storing most data into the first exchange.</li> <li>• <b>Aggressive mode</b> - performs fewer exchanges (a total of 4 messages) than the Main mode</li> </ul>
Key exchange protocol	IKEv1   IKEv2; default: <b>IKEv1</b>	Internet Key Exchange (IKE) version used for key exchange. <ul style="list-style-type: none"> <li>• <b>IKEv1</b> - more commonly used but contains known issues, for example, dealing with NAT.</li> <li>• <b>IKEv2</b> - updated version with increased and improved capabilities, such as integrated NAT support, supported multi-hosting, deprecated exchange modes (does not use main or aggressive mode; only 4 messages required to establish a connection).</li> </ul>
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: <b>AES 128</b>	Algorithm used for data encryption.
Hash algorithm	D5   SHA1   SHA256   SHA384   SHA512; default: <b>SHA1</b>	Algorithm used for exchanging authentication and hash information.
DH group	MODP768   MODP1024   MODP1536   MODP2048   MODP3072   MODP4096   MODP6144   MODP8192   ECP192   ECP224   ECP256	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
	ECP384   ECP521   No PFS; default: <b>MODP1024</b>	
<b>Phase 2 proposal</b>		
Security protocol	ESP   AH; default: <b>ESP</b>	<ul style="list-style-type: none"> <li>• <b>ESP protocol</b> - provides data confidentiality (encryption) and authentication (data integrity, data origin authentication, and replay protection).</li> <li>• <b>AH</b> - provides a mechanism for authentication only.</li> </ul>
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: <b>AES 128</b>	<ul style="list-style-type: none"> <li>• Algorithm used for data encryption.</li> </ul>
Hash algorithm	MD5   SHA1   SHA256   SHA384   SHA512; default: <b>SHA1</b>	<ul style="list-style-type: none"> <li>• Algorithm used for exchanging authentication and hash information.</li> </ul>
PFS DH group	None   MODP768   MODP1024   MODP1536   MODP2048   MODP3072   MODP4096   MODP6144   MODP8192   ECP192   ECP224   ECP256   ECP384   ECP521; default: <b>MODP1024</b>	<ul style="list-style-type: none"> <li>• The PFS (Perfect Forward Secrecy). Must match with another incoming connection to establish IPsec.</li> </ul>
<b>Life time</b>		
Phase 1 IKE lifetime	180-86400 seconds; default: <b>10800</b>	<ul style="list-style-type: none"> <li>• How long the keying channel of a connection (ISAKMP or IKE SA) should last before being renegotiated. The time is specified in seconds.</li> </ul>
Phase 2 SA lifetime	180-86400 seconds; default: <b>3600</b>	<ul style="list-style-type: none"> <li>• How long the keying channel of a connection (ISAKMP or IKE SA) should last before being renegotiated. The time is specified in seconds.</li> </ul>
<b>Dead Peer Detection</b>		
Action	None   Clear   Hold   Restart  ; default: <b>None</b>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
Interval	30-3600 seconds; default: <b>30</b>	<ul style="list-style-type: none"> <li>• The frequency of sending messages or INFORMATIONAL exchanges to peer.</li> </ul>
Timeout	default: <b>60</b>	<ul style="list-style-type: none"> <li>• Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity.</li> </ul>
<b>IPSEC enhancement</b>		
Enable	default: <b>disable</b>	<ul style="list-style-type: none"> <li>• Check the box to enhance the IPsec function.</li> </ul>

### 5.3.2.2 IPsec – Status

This **IPsec's Status** tab enable the user to check the status of IPsec connection between xxR5805 router and its peer device in different connection types and modes. Figure 5.18 show the IPsec's Status webpage. The first information is the **Peer Address** which is the IP address of the other device that is connected to xxR5805 router. The second information is the **VPN Tunnel's** status. The third information is the **Status** of the IPsec connection which can be Disabled, Listening, or Connected. There are three buttons at the end of the webpage which are **Restart**, **Stop**, and **Refresh**. The **Restart** and **Stop** buttons allow you to establish or tear down the IPsec connection.

The **Refresh** button enable you to check the latest status of the connection. Table 5.8 summarizes the description of each field in **IPSec's Status** webpage.

Figure 5.18 Services -> VPN -> IPSec -> Status

Table 5.8 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) 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. The following subsections will describe the WebUI for L2TP and how to configure the L2TP instance.

#### 5.3.3.1 L2TP Overview

Figure 5.19 shows an example of **L2TP Overview** page. Under this page, there can be one or more entries of the L2TP instance. To configure the existing L2TP instance in the list, the user can click on the **Edit** button. The explanation of how to configure the L2TP instance will be presented in the next two subsections. To remove an instance, the user can click on the **Delete** button. To add new instance, the user can first select the **Role** from the drop-down list, then fill in the **New configuration name** in the textbox, and click on the **Add New** button.

Figure 5.19. Services -> VPN -> L2TP -> Overview

#### 5.3.3.2 L2TP Server

After the user clicking on the **Edit** button of a L2TP server entry, the webpage will be updated to a setting webpage as shown in Figure 5.20. Note that the router that acts as the L2TP server must have a public static or public



dynamic IP address. The upper part of the Main Settings consists of four fields: Enable, Local IP, Remote IP range begin and Remote IP range end. The lower part of the Main Settings has a list of L2TP accounts which can be added using the **Add** button or removed using the **Delete** button. There are descriptions and guideline on how to create the L2TP accounts which consists of Username, Password, and L2TP client's IP. Table 5.9 provides the description of each field for setting up the L2TP Server Instance.

### 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"/>		

Figure 5.20. Services -&gt; VPN -&gt; L2TP -&gt; Xl2tpsvr -&gt; Edit

Table 5.9. Services -&gt; VPN -&gt; L2TP -&gt; Xl2tpsvr -&gt; Edit

Field	Value	Description
Enable	default: <b>disable</b>	Check the box to enable the L2TP Tunnel function.
Local IP	default: <b>192.168.0.1</b>	IP Address of this device.
Remote IP range begin	default: <b>192.168.0.20</b>	The beginning IP address to be leased for L2TP client
Remote IP range end	default: <b>192.168.0.30</b>	The ending IP address to be leased for L2TP client
Username	default: <b>your user</b>	Username to connect to L2TP (this) server.
Password	default: <b>your password</b>	Password to connect to L2TP server.
L2TP Client's IP	default: <b>none</b>	This virtual IP will be given to L2TP client. For auto assignment leave empty.



### 5.3.3.3 L2TP Client

To configure L2TP client, the user can either edit an existing L2TP client on the list of **Overview** page or add a new L2TP client. To edit an L2TP client, the user can click on the **Edit** button at the end of the Client type entry as shown in the second line of Figure 5.21. To add a new L2TP client, select the **Client** role from the **Role** drop-down list and fill in the name for **New configuration name** text field and click the **Add New** button. Figure 5.22 shows an example of **Main Settings** webpage for L2TP Client Instance. The user can configure: Enable, Server, Username, Password, Authentication, Keep alive, and Default route. The description of each field is shown in the Table 5.10 below.

**L2TP**

Overview

Name	Type	Enable	
Xi2tpsvr	Server	<input type="checkbox"/>	Edit  Delete
Xi2tpClient	Client	<input type="checkbox"/>	Edit  Delete

Role: Client ▼ New configuration name:  Add New

Figure 5.21. Services -> VPN -> L2TP -> Overview

**L2TP Client Instance: Xi2tpClient**

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

Figure 5.22. Services -> VPN -> L2TP -> Xi2tpClient -> Edit

Table 5.10. Services -> VPN -> L2TP -> Xi2tpClient -> Edit

Field	Value	Description
Enable	default: <b>disable</b>	Check the box to enable the L2TP Tunnel function.
Server	IP/hostname; default: <b>none</b>	Specifies the server IP address or a hostname.
Username	Username; default: <b>none</b>	Username to connect to L2TP server.
Password	default: <b>none</b>	Password to connect to L2TP server.
Authentication	default: <b>none</b>	L2TP tunnel authentication password.

Field	Value	Description
Keep alive	default: <b>none</b>	Send LCP echo requests to server in seconds.
Default route	default: <b>none</b>	Check the box to set the L2PT tunnel as default route.

### 5.3.4 PPTP

**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). PPTP (Point-to-Point Tunneling Protocol) is a method for implementing virtual private networks. Select the PPTP sub-menu in the VPN menu to configure a PPTP tunnel.

#### 5.3.4.1 PPTP Server – General Settings

The xR5805 router can be configured as a VPN server or PPTP server. A **PPTP server** is an entity that waits for incoming connections from PPTP clients. Under the PPTP Server sub-menu, there are three settings tabs which are **General Settings**, **Users Manager**, and **Online Users**. This subsection will discuss on the General Settings tab first. The other two tabs will be described in the following subsections.

To enable the PPTP Server, check the box behind the **Enable VPN Server** as shown in Figure 5.23. The first field is the Server IP which is the IP address of the xR5805 router's PPTP network interface. The second field is the Client IP address range which defines the starting and ending IP address for PPTP clients that will be connecting to the PPTP server (xR5805 router). The third field is the IP address of DNS (Domain Name Service) server which will be relayed to the clients. The other three options are Enable MPPE (Microsoft Point-to-Point Encryption) Encryption, Enable NAT (Network Address Translation) Forward, and Enable remote service. The user can select any of these options by checking the corresponding box(es). Table 5.11 summarizes the description of each fields and options for General Settings tab of PPTP Server.

General Settings   Users Manager   Online Users

General settings

Enable VPN Server ☐

Server IP   
VPN Server IP address, it not required.

Client IP   
VPN Client IP address, it not required.

DNS IP address   
This will be sent to the client, it not required.

Enable MPPE Encryption ☒ Allows 128-bit encrypted connection.

Enable NAT Forward ☒ Allows forwarding traffic.

Enable remote service ☒ Allows remote computers on the Internet to connect to VPN Server.

Figure 5.23. Services -> VPN -> PPTP Server -> General Settings

Table 5.11. Services -> VPN -> PPTP Server -> General Settings

Field	Value	Description
Enable VPN Server	default: <b>disable</b>	Check the box to enable the PPTP function.
Server IP	default: <b>10.0.0.1</b>	IP address of this xxR5805 PPTP network interface.

Field	Value	Description
Client IP	default: <b>10.0.0.2-254</b>	PPTP IP address leases will begin to end from the address specified in this field.
DNS IP address	default: <b>114.114.114.114</b>	IP address of the DNS server which will be sent to the client.
Enable MPPE Encryption	default: <b>enable</b>	Allows 128-bit encrypted connection.
Enable NAT Forward	default: <b>enable</b>	Allows forwarding traffic.
Enable remote service	default: <b>enable</b>	Allows remote computers on the internet to connect to VPN server.

#### 5.3.4.2 PPTP Server – Users Manager

The second tab under the PPTP Server is the Users Manager. This tab as shown in Figure 5.24 allows the user of xxR5805 router to manage the accounts of the PPTP clients. To add a new account, clicking on the **Add** button then fill in the User name and Password. Optionally, the IP address of a client can be specified or leave it as automatically assignment. To remove an account, click on the **Delete** button of that account. An account can be enabled by checking on the **Enabled** box in front of that account. Table 5.12 summarizes the description of each field on the Users Manager tab.

Figure 5.24. Services -> VPN -> PPTP Server -> Users Manager

Table 5.12. Services -> VPN -> PPTP Server -> Users Manager

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

#### 5.3.4.3 PPTP Server – Online Users

The **Online Users** tab as shown in Figure 5.25 can be used to check currently online VPN or PPTP clients. It can be used to verify that a user can successfully connect to this server. Note that the list is empty by default. For each online user or PPTP client, there are **Add to Blacklist** button and **Forced offline** button which can be used to block and disconnect that account, respectively. Table 5.13 describes fields on the **Online Users** tab.

Server IP	Client IP	IP address	Blacklist	Forced offline
10.0.0.1	10.0.0.2	10.0.50.2	Add to Blacklist	Forced offline

Figure 5.25. Services -&gt; VPN -&gt; PPTP Server -&gt; Online Users

Table 5.13. Services -&gt; VPN -&gt; PPTP Server -&gt; 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

The xxR5805 router can set up GRE tunnel using this GRE sub-menu as shown in Figure 5.26. For each GRE instance, there are two sections: **Main Settings** and **Tunnel Settings**. Under the **Main Settings** section, the user can enable the current GRE instance by checking the **Enabled** box. Table 5.14 provides the description of each field on the GRE instance webpage.

### GRE Instance: Tun1

#### Main Settings

Enabled ☐

Remote endpoint IP address

Bind Interface

Local IP address

Firewall zone

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

Figure 5.26 Services -&gt; VPN -&gt; GRE -&gt; GRE Instance: Tun1

Table 5.14 Services -&gt; VPN -&gt; GRE -&gt; GRE Instance: Tun1

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

Field	Value	Description
Firewall zone	Unspecified   lan   wan; default: <b>Unspecified</b>	Specify GRE work on which interface.
MTU	Value from 68 to 1476; default: <b>1280</b>	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: <b>none</b>	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: <b>none</b>	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: <b>disable</b>	Check to verify outbound checksum for the GRE header and payload.
Inbound checksum	default: <b>disable</b>	Check to verify inbound checksum for the GRE header and payload.
Outbound serialization	default: <b>disable</b>	Check to verify outbound serialization for the GRE header and payload.
Inbound serialization	default: <b>disable</b>	Check to verify inbound serialization for the GRE header and payload.
Path MTU Discovery	Value from 1 to 255; default: <b>check</b>   TTL: <b>64</b>	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.
<b>Tunnel Settings</b>		
Local GRE interface IP address	default: <b>none</b>	IP address of the local GRE Tunnel network interface.
Local GRE interface netmask	default: <b>none</b>	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. The xxR5805 router can be configured with VRRP under this submenu.


### 5.4.1 VRRP LAN configuration settings


The **VRRP LAN configuration settings** section is used to set the main settings of VRRP. Figure 5.27 shows the VRRP LAN Configuration Settings section. The first option allows the user to enable the VRRP. The second field is the virtual IP address for the VRRP cluster. The third field is the Virtual ID for the group of routers on the same VRRP cluster. The fourth field is the Priority value of the current router which is used to decide whether the current route will be the Master or the main router. Note that the router with the largest Priority value in a cluster will be the cluster's Master. The last field is the Advertisement interval which is the time in seconds between advertisement messages. Table 5.15 provides descriptions of all fields in this section.

### 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]

Figure 5.27. Services -&gt; VRRP -&gt; VRRP LAN Configuration Settings


Table 5.15. Services -&gt; VRRP -&gt; VRRP LAN Configuration Settings


Field	Value	Description
Enable	default: <b>disable</b>	Turns VRRP on or off.
IP address	default: <b>192.168.1.253</b>	Virtual IP address for the router's LAN VRRP cluster.
Virtual ID	integer [1 - 255]; default: <b>1</b>	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: <b>100</b>	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> . <b>Master router</b> - the first hop router in the VRRP cluster (i.e., the router that provides connectivity to LAN devices by default). <b>Backup router</b> - 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: <b>1</b>	Time interval in seconds between advertisements.


#### 5.4.2 Check Internet connection


The **Check Internet connection** section as shown in Figure 5.28 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. Table 5.16 provides information on the fields contained in the **Check Internet connection** section.


Check Internet Connection

Enable ☒  Check to enable internet connection checking

Ping IP address 
  
 e.g. 192.168.1.1 (or www.host.com if DNS server configured correctly)

Ping interval  10
  
 Time interval in seconds between two pings

Ping timeout (sec)  1
  
 Specify time to receive ping, range [1-9999]

Ping packet size 
  
 Ping packet size, range [0-1000]


Ping retry count 
  
 Number of time trying to send ping to a server after time interval if echo receive was unsuccessful, range [1-9999]

Figure 5.28. Services -&gt; VRRP -&gt; Check Internet Connection

Table 5.16. Services -&gt; VRRP -&gt; Check Internet Connection

Field	Value	Description
Enable	default: <b>none</b>	Turns Internet connection checking on or off.
Ping IP address	default: <b>none</b>	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: <b>10</b>	Time interval (in seconds) between two Pings.
Ping timeout (sec)	integer [1 to 9999]; default: <b>1</b>	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: <b>none</b>	The size (in bytes) of sent ICMP packets.
Ping retry count	integer [1 to 9999]; default: <b>none</b>	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. The GPS signal can provide a precision clock or time reference to the xxR5805 router. The user can enable this GPS feature on this sub-menu. However, the router will require a GPS antenna and clear reception (no obstruction) of the GPS signal from the sky. If the router cannot received GPS signal, a pop-up window may appear with a message "Unable to update GPS information! Please make sure GPS service is enabled and device is receiving GPS data". Figure 5.29 shows the **GPS Configuration** webpage and Table 5.17 provides the description of each field on the page.



## GPS Configuration

Overview

Enable GPS service ☒

Fix time	2021-11-11 07:07:16
Latitude	24.184508
Longitude	120.618874

Figure 5.29. Services -&gt; GPS

Table 5.17. Services -&gt; GPS

Field	Value	Description
Fix time	YYYY-MM-DD HH:MM:SS; default: <b>none</b>	The last GNSS fix time.
Latitude	xxx.xxxxxx; default: <b>none</b>	It shows the angle between the straight line in the certain point and the equatorial plane.
Longitude	xxx.xxxxxx; default: <b>none</b>	It is defined as an angle pointing west or east from the Greenwich Meridian, which is taken as the Prime Meridian.

## 5.6 Ping retry count

## 5.7 integer [1 to 9999]; default: none

## 5.8 How many times the router will retry sending ping requests before determining that the Internet connection has failed.

## 5.9 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. This protocol is often deployed for the Internet of Things (IoT).

### 5.9.1 MQTT Broker

xxR5805 devices support this functionality via an open source Mosquito broker which is an implementation of MQTT broker. The messages are sent in the following brief description. A client (called subscriber) subscribes to a topic(s) on the MQTT broker. A publisher (such as an IoT device) 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 (xxR5805 router) as an MQTT Broker, enable it on this webpage by checking the **Enable** box as shown in Figure 5.30. To specify which port number on the device that the MQTT will be listened

to, please specify the port number in the Local Port field. In order to make the device accept MQTT connections from WAN (remote networks), you also need to check the **Enable Remote Access** box. Table 5.18 provides descriptions of fields for configuring 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

Figure 5.30. Services -&gt; MQTT -&gt; Broker

Table 5.18. Services -&gt; MQTT -&gt; Broker

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

## 5.9.2 Broker Settings

Under the **Broker Settings** sub-menu, there are three tabs: **Security**, **Bridge**, and **Miscellaneous**. These allows the user to configure the MQTT broker in more details. The following subsections describe each tab.

### 5.9.2.1 Broker – Security

To provide security on the message exchanged by the MQTT broker, the user can configure the security mechanism for MQTT in this tab as shown in Figure 5.31. Basically, the **TLS/SSL** can be enabled for the MQTT's connection. The user can add credentials and public key such as **CA Cert file**, **Server Cert file**, and **Server Key file**. The user can also select the support **TLS version** in the last option on the webpage. Table 5.19 summarizes the description of each field on the webpage.

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

Figure 5.31. Services -&gt; MQTT -&gt; Security

Table 5.19. Services -&gt; MQTT -&gt; Security

Field	Value	Description
Use TLS/SSL	default: <b>disable</b>	Turns the use of TLS/SSL for this MQTT connection on or off.
CA Cert File	File type: .ca file default: <b>none</b>	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: <b>none</b>	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: <b>none</b>	Uploads a server (broker) key file.
TLS version	tlsv1.1/tlsv1.2/Support all; default: Support all	Specifies which TLS version(s) is will be supported by this broker.

### 5.9.2.2 Broker - Bridge

This MQTT broker's **Bridge** tab as shown in Figure 5.31 allows the configuration of connection to a remote bridge. The first option is used to enable this feature. Then, the user can specify the **Connection Name**, **Remote Address**, and **Remote Port** number. Then, four more options can be enabled which are **Use Remote TLS/SSL**, **Use Remote Bridge Login**, **Try Private**, and **Clean Session**. The bottom part of the webpage lists current **Topic**, **Direction**, and **QoS Level** that the broker subscribes to. Additional topics to be subscribed can be added by clicking on the **Add** button. Table 5.20 summarizes the description of each field on this **Bridge** tab.

Broker settings

Security **Bridge** Miscellaneous

Enable ☒ Enable connection to remote bridge

Connection Name

Remote Address   
[Select remote bridge address](#)

Remote Port   
[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](#)

Figure 5.32. Services -&gt; MQTT -&gt; Bridge

Table 5.20. Services -&gt; MQTT -&gt; Bridge

Field	Value	Description
Enable	default: <b>disable</b>	Enable/Disable MQTT Bridge.

Connection Name	default: <b>none</b>	Name of the Bridge connection. This is used for easier management purposes.
Remote Address	default: <b>none</b>	Remote Broker's address.
Remote Port	integer [0-65535]; default: <b>1883</b>	Specifies which port the remote broker uses to listen for connections.
Use Remote TLS/SSL	default: <b>disable</b>	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: <b>disable</b>	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: <b>disable</b>	Check if the remote Broker is another instance of a daemon.
Clean Session	default: <b>disable</b>	When turned on, discards session state after connecting or disconnecting.
Topic Name	default: <b>none</b>	The name of the topics that the broker will subscribe to.
Direction	Out/In/Both; default: <b>none</b>	The direction that the messages will be shared.
QoS Level	At most once (0)   At least once (1)   Exactly once (2) default: <b>none</b>	Sets the publish/subscribe QoS level used for this topic

### 5.9.2.3 Broker – Miscellaneous

The **Miscellaneous** section is used to configure MQTT broker parameters that are related to neither Security nor Bridge features. Figure 5.33 shows the Miscellaneous tab for MQTT broker. Table 5.21 provides descriptions of fields on this Miscellaneous tab.

Broker settings

Security Bridge **Miscellaneous**

ACL File  No file chosen

Password File  No file chosen

Persistence ☐

Allow Anonymous ☐

Figure 5.33. Services -> MQTT -> Miscellaneous

Table 5.21. Services -> MQTT -> Miscellaneous

Field	Value	Description
ACL File	ACL file default: <b>none</b>	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: <b>none</b>	Uploads a password. A password file stores Usernames and corresponding passwords, used for authentication.

Field	Value	Description
Persistence	default: <b>disable</b>	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: <b>disable</b>	Turns anonymous access to this broker on or off.

## 6. System

As shown in Figure 6.1, 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. The following subsections will describe each sub-menu.

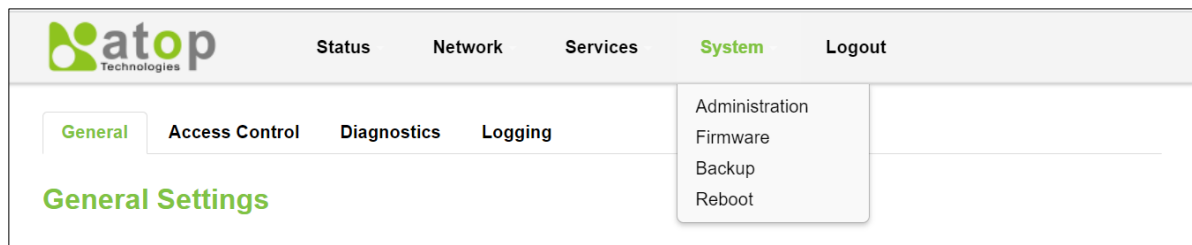


Figure 6.1. System

### 6.1 Administration

The **Administration** sub-menu is further divided into four tabs: **General**, **Access Control**, **Diagnostics**, and **Logging**.

#### 6.1.1 General

Under the General tab, there is the **General Settings** webpage as shown in Figure 6.2. This webpage consists of three parts: **System Properties**, **Login Password**, and **Restore Default Settings**. Under the **System Properties** part, the user can configure the **Hostname**. This field 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** part, the user 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. Finally, in the **Restore Default Settings** part, the user can click the “**Restore**” button to reset the configuration files to factory default settings of the xxR5805 device. Table 6.1 summarizes the description of each field on this General Settings webpage.

The screenshot shows the 'General Settings' webpage. At the top, there is a navigation bar with tabs: General (highlighted in green), Access Control, Diagnostics, and Logging. Below the navigation bar, the title 'General Settings' is displayed in green. The page is divided into three sections: 1. System Properties: Contains a 'Hostname' field with the value 'AtopTechnologies'. 2. Login Password: Contains three password fields: 'Current Password', 'New Password', and 'Confirm New Password'. Each field has a toggle icon to the right. 3. Restore Default Settings: Contains a 'Restore to default' label and a 'Restore' button.

Figure 6.2. System -> Administration -> General Settings

Table 6.1. System -&gt; Administration -&gt; 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.
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.

### 6.1.2 Access Control

The **Access Control** tab is used to manage remote and local access to device. This tab can configure Telnet access and SSH access which will be described in the following subsections.

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

#### 6.1.2.1.1 Telnet Access

The first part of Access Control tab is the Telnet Access part as shown in Figure 6.3. The user can enable Telnet access to the device and change the port number for the telnet protocol. Table 6.2 describes the fields in this part.

Figure 6.3. System -&gt; Administrator -&gt; Access Control -&gt; Telnet Access

Table 6.2. System -&gt; Administrator -&gt; Access Control -&gt; Telnet Access

Field	Value	Description
Enable	default: <b>enable</b>	Check box to enable Telnet access.
Port	default: <b>23</b>	Port to be used for Telnet connection.

#### 6.1.2.2 SSH Access

In the **SSH Access** part of the Access Control within the **Administration** sub-menu, you can enable the SSH service. This service will allow the remote SSH hosts to access xxR5805 device from the specified network interface. The user can configure which interface on the device will be allowed to have remote SSH access from the list of interface as shown in Figure 6.4. The port number can also be changed for SSH access on this page. Table 6.3 describes each field in this part.

Figure 6.4. System -&gt; Administrator -&gt; Access Control -&gt; SSH Access

Table 6.3. System -&gt; Administrator -&gt; Access Control -&gt; SSH Access

Field	Value	Description
Enable	default: <b>enable</b>	Turn SSH service on/off.
Interface	default: <b>unspecified</b>	Network interface that the SSH service will be listening to.
Port	default: <b>22</b>	Port number that the SSH service will be listening to.

### 6.1.3 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 6.5. System -&gt; Administrator -&gt; Access Control -&gt; Diagnostics

#### 6.1.3.1 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.



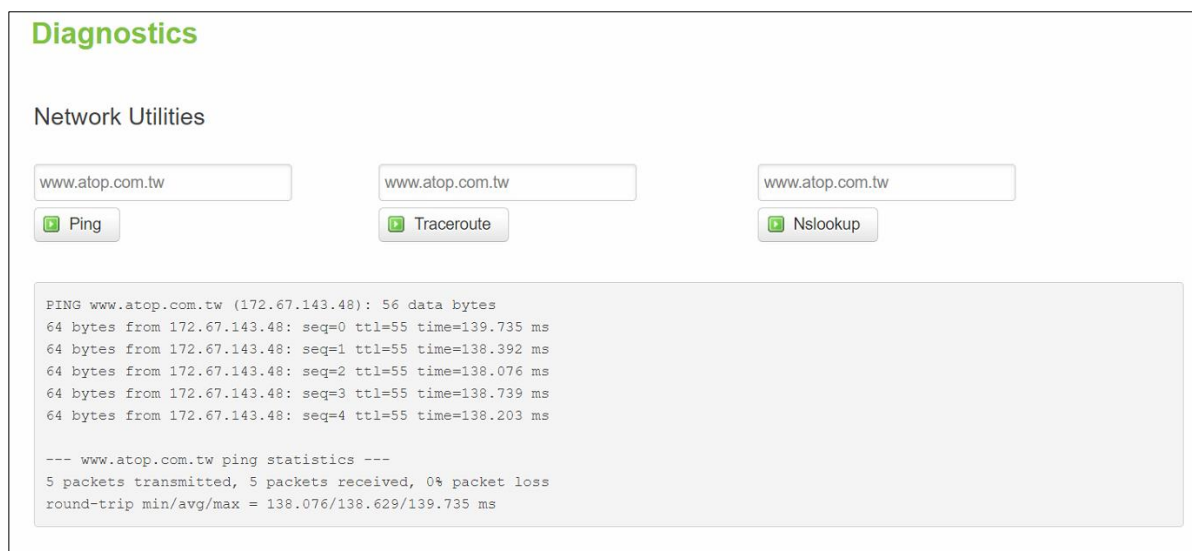


Figure 6.6. System -&gt; Administrator -&gt; Access Control -&gt; Diagnostics -&gt; Ping

### 6.1.3.2 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>.

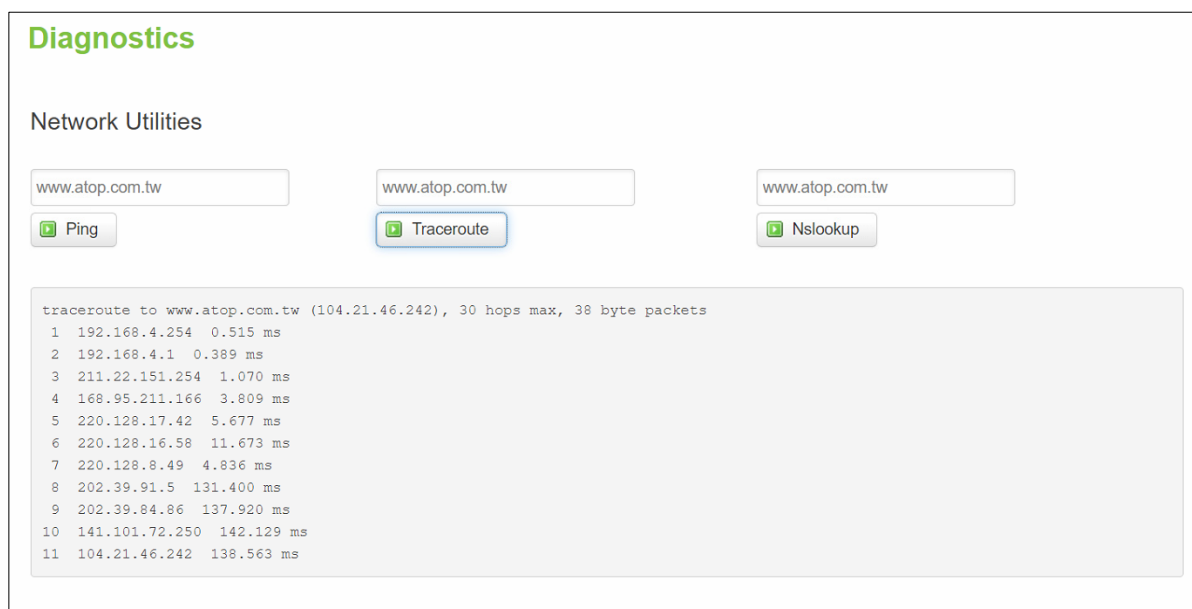


Figure 6.7. System -&gt; Administrator -&gt; Access Control -&gt; Diagnostics -&gt; Traceroute

### 6.1.3.3 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>.

The screenshot shows the 'Diagnostics' section of a web interface. Under 'Network Utilities', there are three input fields, each containing 'www.atop.com.tw'. Below each field is a button: 'Ping', 'Traceroute', and 'Nslookup'. The 'Nslookup' button is highlighted with a blue border. Below the 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
```

Figure 6.8. System -> Administrator -> Access Control -> Diagnostics -> Nslookup

#### 6.1.4 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.

The screenshot shows the 'Logging' section of a web interface. Under 'System Log Settings', there are several configuration options:

- 'System log buffer size' is set to '64' with a unit selector set to 'KB'.
- 'Enable external system log server' is an unchecked checkbox.
- 'External system log server' is set to '0.0.0.0'.
- 'External system log server port' is set to '514'.
- 'System Log Level' is set to 'Normal' with a dropdown arrow.

Figure 6.9. System -> Administrator -> Access Control -> Logging

Table 6.4. System -&gt; Administrator -&gt; Access Control -&gt; Logging

Field	Value	Description
System Log Buffer Size	default: <b>64</b>	Size of the system log message buffer.
External System Log Server	default: <b>disable</b>	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: <b>none</b>	Port number of the remote syslog server
Log Output Level	default: <b>none</b>	The maximum log level for system messages to be logged to the console. Only messages with a level lower than this will be printed to the console. Messages with higher system level will have lower number of log level. For example, the highest system level message will be saved in log level 0. If you want more messages in console, put "log output level" to Debug. But if you want less messages in the console, put "log output level" to Error.
Cron Output Level	Debug/Normal/Warning; default: <b>Normal</b>	The minimum level for cron messages to be logged to syslog

## 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.

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

## 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

Figure 6.10. System -&gt; Firmware

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

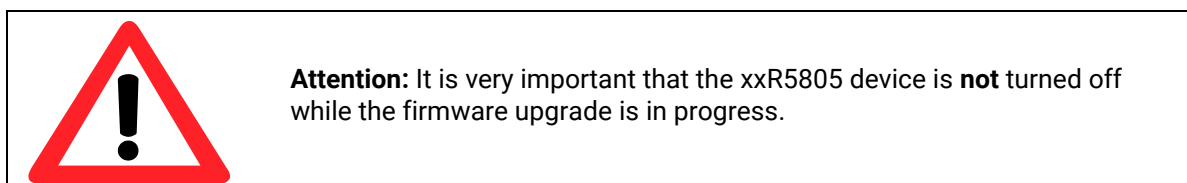
## Firmware Upgrade - Verify

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.

Figure 6.11. Confirm message of the Firmware Upgrade

- 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).
- The xxR5805 device will be restarted and the web browser on the local computer will be redirected to Login webpage.



## 6.3 Backup

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

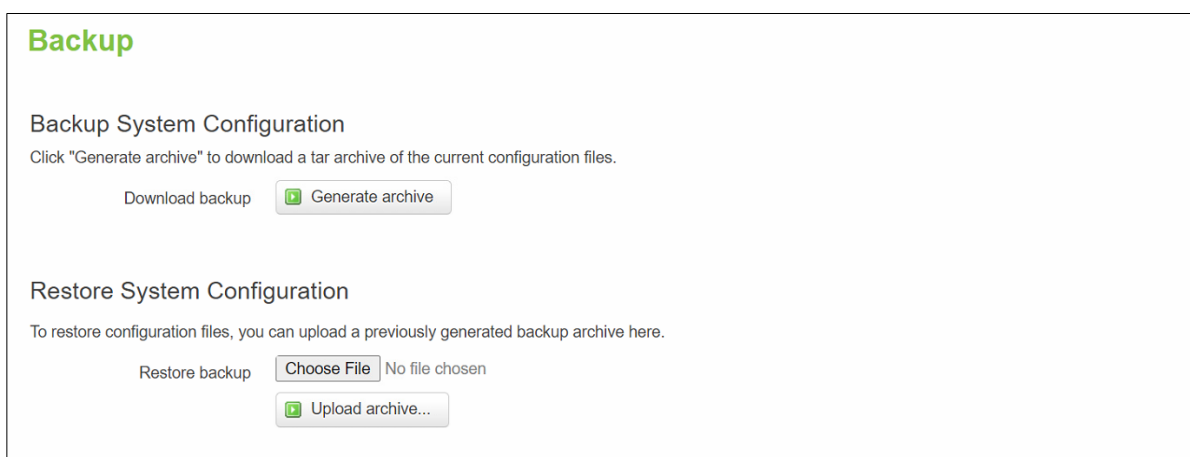
### Backup System Configuration

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.



The screenshot shows a web interface titled "Backup" in green. It contains two main sections: "Backup System Configuration" and "Restore System Configuration". The first section has a "Download backup" link and a "Generate archive" button. The second section has a "Restore backup" link, a "Choose File" button (which shows "No file chosen"), and an "Upload archive..." button.

Figure 6.12. System -> Backup

### 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.



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 is a "Perform Reboot" button.

Figure 6.13. System -> Reboot

## 7 Logout

Click the **Logout** menu to log the current user out safely. After logging out, the web browser will redirect the user to the login page.

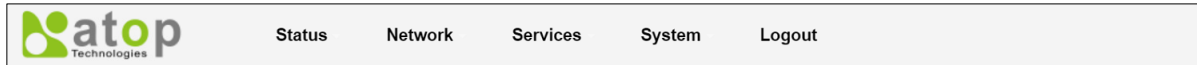


Figure 7.1. System -> Logout

## 8. Specifications

### 8.1 Hardware Specification

Table 8.1. 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

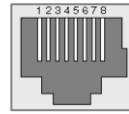


Figure 8.1. WAN/LAN Port on RJ45 with Pin Numbering of CWR5805 Device

Table 8.2. 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](http://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](mailto:sales@atop.com.tw)

**ATOP CHINA BRANCH:**

3F, 75<sup>th</sup>, No. 1066 Building,  
Qingzhou North Road,  
Shanghai, China  
Tel: +86-21-64956231