

WS-431E 4G Router User Manual



Figure 1 WS-431E 4G Router

WS-431E 4G Router

1. OVERVIEW

- Support 4G/3G/2G Internet access in various modes, which can be used in the fields of Internet of Networked Medical Treatment, Intelligent Agriculture, Smart City, Smart Robots, Security Monitoring Networking, Intelligent Bus Wifi etc.
- 1x WAN RJ45 port (configurable for LAN), 10/100 Mbps, supports automatic MDI/MDIX, 1.5KV electromagnetic isolation protection.
- 2 x LAN RJ45 port, 10/100 Mbps, supports automatic MDI/MDIX,1.5KV electromagnetic isolation protection.
- Support 1 WLAN(802.11b/g/n)
- Support Web Server
- Support LED to show work status
- Support Reload button to restore default settings by hardware way
- Support VPN client(PPTP/L2TP)
- Support one SIM card socket
- Support DDNS and port forwarding
- Support QoS and firewall

CONTENTS

	1. OVERVIEW		2
	CONTENTS		
	2. PRODUCT OVERVIEW		5
	2.1. INTRODUCTION		5
	2.2. SPECIFICATIONS		5
	2.3. INTERFACE DESCRIPTION	DN	6
	2.4. HARDWARE SIZE		7
	3. QUICK START		7
	3.1.1. HARDWARE EN	VIRONMENT	
	3.1.2. NETWORK CON	NECTION	
	4. PRODUCT FUNCTIONS		
	4.1. INSTALL PROCEDURE		
	4.2. APN		
	4.2.1. APN CONFIGUR	ATION BY WEB SERVER	
	4.2.2. CREATE A VPN	CLIENT	
	4.3. NETWORKING MODE.		
	4.3.1. WAN+LAN+4G.		
	4.3.2. LAN+LAN+4G		
	4.4. COMMON FUNCTIONS		
	4.4.1. 4G INTERFACE.		15
	4.4.2. LAN INTERFACE		
	4.4.3. WAN INTERFAC	Έ	
	4.4.4. WLAN INTERFA	CE	
	4.4.5. NETWORK DIAC	GNOSIS	
	4.4.6. MODULE NAME	E AND TIME ZONE	23
	4.4.7. STATIC ROUTE.		
	4.5. BASIC FUNCTIONS		
	4.5.1. WEB SERVER PA	ASSWORD	25
	4.5.2. RESTORE		
	4.5.3. UPGRADE FIRM	IWARE VERSION	27
	4.5.4. RESET		
	4.6. FIREWALL FUNCTION.		
	4.6.1. BASIC SETTING	S	
	4.6.2. NAT FUNCTION		
ww	w.waveshare.com	3 / 68	www.waveshare.com/wiki

WAVESHARE

	4.6.3. COMMUNICATION RULES	38
	4.6.4. ACCESS RESTRICTION	56
4.7	· VPN FUNCTION	58
	4.7.1. PPTP CLIENT	.59
	4.7.2. L2TP CLIENT	61
	4.7.3. IPSEC	63
	4.7.4. OPENVPN	65
	4.7.5. GRE	67

2. PRODUCT OVERVIEW

2.1. INTRODUCTION

The WS-431E 4G Router is a new Qualcomm solution Wi-Fi enhanced industrial router with excellent anti-interference capability and stable connection performance, supports WIFI hotspot, WIFI client, and WIFI relay modes, and is integrated with 4G LTE, Wi-Fi, Ethernet ports (2LAN and 1WAN/LAN) and VPN technologies.

The WS-431E can provide advanced Internet connectivity and high-speed data access for the devices, allowing users to quickly build their own application network, and also helping enterprise customers achieve efficient large-scale network deployment and management. It is suitable for various IoT and M2M solutions such as service robots, inspection robots, unmanned vehicle networking, massage chair networking, AGV car, and other industrial application scenarios.

2.2. SPECIFICATIONS

CELLULAR NETWORK PARAMETERS					
Frequency band	TDD-LTE: B38/40/41				
	FDD-LTE: B1/3/7/8/20/28A				
	WCDMA: B1/8				
	GSM/EDGE:B3/8				
WIFI					
Standard	IEEE 802.11b/g/n, 2.4GHz				
Data speed	300Mbps				
MIMO	2×2				
Transmission	500 meters with an open field, the actual transmission distance				
distance depends on the environment of the site					
	INTERFACES				
WAN/LAN	1× WAN RJ45 port (can be configured as LAN), 10/100 Mbps,				
	supports auto MDI/MDIX, 1.5KV electromagnetic isolation				
	supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection				
LAN	supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection 2× LAN RJ45 port, 10/100 Mbps, supports auto MDI/MDIX, 1.5KV				
LAN	supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection 2× LAN RJ45 port, 10/100 Mbps, supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection				
LAN SIM card slot	supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection 2× LAN RJ45 port, 10/100 Mbps, supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection Supports standard Nano (3 V/1.8 V)				
LAN SIM card slot Antenna	supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection 2× LAN RJ45 port, 10/100 Mbps, supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection Supports standard Nano (3 V/1.8 V) SMA-K standard antenna connector, comes with 1x 4G antennas,				
LAN SIM card slot Antenna	supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection 2× LAN RJ45 port, 10/100 Mbps, supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection Supports standard Nano (3 V/1.8 V) SMA-K standard antenna connector, comes with 1x 4G antennas, 2x WiFi antennas by default				
LAN SIM card slot Antenna TBD	supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection 2× LAN RJ45 port, 10/100 Mbps, supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection Supports standard Nano (3 V/1.8 V) SMA-K standard antenna connector, comes with 1x 4G antennas, 2x WiFi antennas by default Debug interface				
LAN SIM card slot Antenna TBD Reload button	supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection 2× LAN RJ45 port, 10/100 Mbps, supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection Supports standard Nano (3 V/1.8 V) SMA-K standard antenna connector, comes with 1x 4G antennas, 2x WiFi antennas by default Debug interface Supports factory restore				
LAN SIM card slot Antenna TBD Reload button Grounding	supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection 2× LAN RJ45 port, 10/100 Mbps, supports auto MDI/MDIX, 1.5KV electromagnetic isolation protection Supports standard Nano (3 V/1.8 V) SMA-K standard antenna connector, comes with 1x 4G antennas, 2x WiFi antennas by default Debug interface Supports factory restore Grounding protection				

	INDICATORS			
PWR	Power indicator, lights up after powered on			
WIFI	Lights up when WiFi is enabled			
2/3/4G network	2G led lights up after being connected to 2G network			
indicator	3G led lights up after being connected to 3G network			
	Both leds light up after being connected to 4G network			
SIG	2× signal strength indicator: lights up one indicates that the signal			
	is average; lights up two indicates that the signal is strong			
	POWER SUPPLY			
Power adapter	DC 12V/1A			
Input voltage	DC 9-36V			
Power Average 260mA/12V				
consumption				
	PHYSICAL CHARACTERISTICS			
Operating	-20℃~+70℃			
temperature				
Storage	-40 $^\circ \text{C} \sim$ +125 $^\circ \text{C}$ (non-condensing)			
temperature				
Relative	5%~95% (non-condensing)			
humidity				
Case material	Metal case, IP30 protection level			
Dimensions	104.0×102.0×28.0mm			
$(L \times W \times H)$				
Installation	DIN rail mounting, wall mounting, tabletop			
EMC	level 3			

2.3. INTERFACE DESCRIPTION

The interface description as follows:



Figure 2 Interface description

The SIM card does not support hot swap. Therefore, install or replace the SIM card with the power off.

2.4. HARDWARE SIZE

The hardware dimensions as follows:



Figure 3 Interface description

- Sheet metal shell, fixed holes on both sides, compatible with rail mounting parts
- Length, width and height are 102*104*28mm (excluding power terminal, antenna and antenna base)
- Installation method: 35mm guide rail installation, hanging ear installation.

3. QUICK START

4G router provides a wireless remote fast networking solution for user devices, and parameters are set through the built-in web page to meet the application scenario. This chapter is a quick introduction to WS-431E router products. It is recommended that users read this chapter and follow the instructions to have a basic understanding of 4G router products. Refer to subsequent sections for specific functional details and descriptions.

3.1.1. HARDWARE ENVIRONMENT

Product test data flow topology:





- Hardware: 1 PC, 1 set of router (including antenna, power adapter), 1 network cable (self-provided), 4G SIM card (self-provided)
- Wiring: The computer is connected to the LAN port of the WS-431E through the network cable, and the WiFi antenna and the full-frequency antenna are connected to the corresponding antenna interface in turn
- Networking: Insert the SIM card in the power off state (the front of the card slot corresponds to the positive direction of the "sim "screen printing)
- Power supply: The working voltage of the WS-431E is DC5-36V. You are advised to use the DC 12V/1A power adapter provided by the factory
- After power-on, observe the indicators: the PWR is on, the LAN is blinking, the 4G indicator (3G+2G) is on, and the indicator is all on, indicating that the signal is good



Figure 5 4G indicator (3G+2G)

3.1.2. NETWORK CONNECTION

Internet test: Power on the WS-431E, wait for about 2 minutes, the 2/3G indicator starts to light, indicating that the 4G network of the router is successful, then you can directly surf the Internet. Let's go to the Settings to check the network status through the default parameters of WS-431E.

Default parameters of WS-431E as follows:

SSID	WS-431E-XXXX
IP Address	192.168.1.1
User name	admin
Password	admin
WLAN Password	www.waveshare.com

Take default parameters as example: User can connect PC to SSID WS-431E-XXXX. Then open browser and enter 192.168.1.1, log in with User name and Password(both are admin), user can enter WebServer.

WS-431E		
waveshare -share awesome hardware-		
	Authorization Required Please enter your username and password.	
	Username: admin Password: admin	
	Login Reset	
		WAVESHARE

Figure 6 Web Server login web

Enter admin for the user name and password. On the left menu bar, select Network => Network Diagnosis => ping. If the domain name can be pinged, the network connection is normal. You can also directly open the browser and enter the URL of the website you want to land.

www.share awesome hard	R E ware-		-228
WS-431E	Diagnostics		
> Status	Network Utilities		
 Services Network 	8.8.8.8	8.8.8.8 Traceroute	www.google.com
WAN LAN Cellular Nework Network/ailover WLAN AP WLAV STA	PING 8.8.8.8 (8.8.8.8): 56 d 64 bytes from 8.8.8.8: seq= 64 bytes from 8.8.8: seq= 64 bytes from 8.8.8: seq= 64 bytes from 8.8.8: seq= 64 bytes from 8.8.8: seq= 8.8.8.9 ping statistics 5 packets transmitted, 5 pac round-trip min/avg/max = 3	Jata bytes =0 ttl=114 time=33.138 ms =1 ttl=114 time=43.0349 ms =2 ttl=114 time=42.077 ms =3 ttl=114 time=34.441 ms =4 ttl=114 time=34.634 ms =4 ttl=114 time=34.634 ms =4 ttl=114 time=34.634 ms =3.138/37.127/42.077 ms	
DHCP Static Routes Diagnostics > VPN Eirawall			
> System			
> Logout			WAVESHARE

Figure 7 Network diagnosis page

This chapter introduces the functions of WS-431E, as the following diagram shown, you can get an overall knowledge of it.



Figure 8 Product functions

4.1. INSTALL PROCEDURE

- (1) Connect the 4G antenna and Wi-Fi antenna to the router. (Shorter one is 3G/4G antenna and Longer one is Wi-Fi antenna.)
- (2) Plug the SIM card in socket.
- (3) Power on the module by power adaptor and check the LED status.
- (4) Connect PC or mobile to the WS-431E router via LAN interface or Wi-Fi interface. Wi-Fi password is "www.waveshare.com".
- (5) Log in Web Server of router. (Default IP address of router is 192.168.1.1, either the username and password is "admin" .)
- (6) Configure APN parameters according to SIM card. Some SIM card APN can be recognized automatically.
- (7) Configure other parameters according to user applications.

4.2. APN

4.2.1. APN CONFIGURATION BY WEB SERVER

WAVESHARE

WS-431E			
	Cellular Network Con	figuration	
> Status	Configure the APN paramet	ers, network priority, SIM card PIN code, network detection and othe	r functions of the mobile network.
Services	Configure network search p	nonty to reduce network search time.	
✓ Network	Config		
WAN	WAN 4G Settings Pine	Detection Settings Mobile Information	
LAN			
Cellular Network	APN	Automatic Input your APN Name. 0-62 characters	
Network Failover			
WLAN AP	Username	User name for apn, 0-62 characters	
WLAN STA	Password		
DHCP		User password for apn, 0-62 characters	
Static Routes	Auth Method	PAP 🗸	
Diagnostics		 Authentication type for apn 	
> VPN	Network Type	AUTO 🗸	
> Firewall	Priority Of Network Search	AUTO 🗸	
> System		The priority of network search	
> Logout	PIN Enable	If SIM card enable PIN, enable this function to enter the PIN co	de
	EHRPD Enable	Disable	
			WAVESNAKE

Figure 9 APN configuration

4.2.2. CREATE A VPN CLIENT

User can set VPN client configuration by Web Server as follow:

Enhanced OpenVPN d	esign allows 3 OpenVP	N Clients and 1 OpenVPN	Server			
OpenVPN Configu	iration					
Name	Туре	Description	Enal	ple	Status	
CLIENT_1	CLIENT		OFF	~	Disconnected	🗾 Edit
CLIENT_2	CLIENT		OFF	~	Disconnected	Z Edit
CLIENT_3	CLIENT		OFF	~	Disconnected	🗷 Edit
SERVER_1	SERVER		OFF	~	Disconnected	🗹 Edit
	OpenVPN Configu Name CLIENT_1 CLIENT_2 CLIENT_3 SERVER_1	Open/VPN Configuration Name Type CLIENT_1 CLIENT CLIENT_2 CLIENT CLIENT_3 CLIENT SERVER_1 SERVER	OpenVPN Configuration Name Type Description CLIENT_1 CLIENT CLIENT CLIENT_2 CLIENT CLIENT CLIENT_3 CLIENT SERVER	OpenVPN Configuration Name Type Description Enablight CLIENT_1 CLIENT OFF CLIENT_2 CLIENT OFF CLIENT_2 CLIENT OFF <	OpenVPN Configuration Enable CUENT_1 CUENT OFF CUENT_2 CUENT OFF CUENT_3 CUENT OFF SERVER_1 SERVER OFF	OpenVPN Configuration Enable Status CLIENT_1 CLIENT OFF Disconnected CLIENT_2 CLIENT OFF Disconnected CLIENT_3 CLIENT OFF Disconnected SERVER_1 SERVER OFF Disconnected

Figure 10 VPN Client

4.3. NETWORKING MODE

4.3.1. WAN+LAN+4G

www.waveshare.com

In this networking mode, user can access internet through WAN interface and 4G interface. WAN interface has higher priority than 4G interface to ensure communication and save 4G flows. When WAN interface occurs problems, router can change to 4G interface to connect internet. In this mode, user can also connect to router through WIFI.

To achieve this mode, user don't need to change the router's parameters. Just connect the cable to router and insert SIM card, then power the router.



Application diagram as follow:

Figure 11 WAN+LAN+4G networking

4.3.2. LAN+LAN+4G

In this networking mode, three devices can connect to router through LAN and access the Internet by 4G network. User can achieve this by Web Server as follow:

WS-431E 4G Router

WAVESHARE

-share awesome hardware-		
WS-431E		
	LAN	
Status	LAN Overview	
Services	Network Status	Actions
Network	LAN Uptime: 0h 5m 27s MAC-Address: D4:AD:20:68:66:14	
WAN	B RX: 225.49 KB (1901 Pkts.) br-lan TX: 912.44 KB (1915 Pkts.)	Sconnect dit
	IPv4: 10.10.100.254/24	
lellular Network	Vlan Management	
VI AN AP	Enable Vlan	
VLAN STA		
HCP	Apply	Save
tatic Routes		
liagnostics		
PN		
irewall		
vstem		
ogout WAVESHARE -share awesome hardware-		WAVESHAR Auto refresh on
WAVESHARE share awesome hardware- WS-431E		WAVESHAR auto refresh on
vgout WAVESHARE share avesome hardware- NS-431E	LAN	WAVESHAR auto refressi on
igout WAVESHARE share awesome hardware- WS-431E atus	LAN LAN Overview	WAVESHAR Auto refresh on
gout WAVESHARE share avesome hardware- VS-431E atus rvices	LAN LAN Overview Network Status	MAVESHAR Auto refresh on Actions
gout VAVESHARE hare avesome hardware- VS-431E atus truces stwork	LAN LAN Overview Network Status Uptime: 0h 6m 375 MAC.Addrese: D4AD:2058566:14	MAVESHAR Auto refresh on Actions
gout VAVESHARE share avesome hardware- VS-431E stus rvices twork AN N	LAN LAN Overview Network Status Uptime: 0h 6m 37s. MAC: Address: 04AD:2058656:14 RX: 2661.848 (2215 Pkts.) TX: 943.71 K8 (2153 Pkts.) TX: 943.71 K8 (2153 Pkts.)	Actions
VAVESHARE ihare avesome hardware- VS-431E itus rvices ttwork AN N Ilular Network	LAN LAN Overview Network Status Uptime: 0h 6m 37s MAC-Address: 04ADi2058656114 BP (2019) Dr-Ban Uptime: 0h 2015 Dr. Ban	Actions
yout VAVESHARE hare awesome hardware- VS-431E tus twork twork N N Itular Network twork failover	LAN LAN Overview Network LAN LAN Status Macradeness: 04A02206866;14 PX: 266.18 KB (2215 Pkts.) TX: 943.71 KB (2153 Pkts.)	Actions
gout WAVESHARE share awesome hardware- VS-431E atus rvices stwork AN N Iluliar Network etwork Failover LAN AP	LAN LAN Overview Network LAN Uptime: 0h 6m 37s MAC.Address: 04AD:2068666:14 RX: 266.18 KB (2215 Pkts.) TX: 943.71 KB (2153 Pkts.) TX: 943.71 KB (2153 Pkts.) IPV4: 10.10.100.254/24 Vlan Management Enable Vlan	Actions Connect Content and Edit
gout NAVESHARE chare avesome hardware- NS-431E atus etwork atus etwork AN N Hular Network etwork Failover LAN AP LAN STA	LAN LAN Overview LAN B ^g (2000) br-lan Uptime: 0h 6m 37s MAC-Address: D4AD:20c68:66:14 RX 266.18 KB (2215 Pkts.) TXX 266.18 KB (2215 Pkts.) IPv4: 10.10.100.254/24 Vlan Management Enable Vlan	Actions
gout VAVESHARE hare avesome hardware- VS-431E atus rvices stwork AN N Ilular Network etwork Failover LAN AP LAN STA ICP	LAN LAN Overview Network LAN B ¹² B ¹² B ¹² Uptime: 0h 6m 37s MAC-Address: 04AD:2068.66:14 RX: 266.18 KB (2215 Pkts.) TX: 266.18 KB (2215 Pkts.) IV: 10.10.100.254/24 Vian Management Enable Vian	Actions @ Connect @ Edit PORTS
gout NAVESHARE chare awesome hardware- vS-431E atus rvices etwork AN N N Ilular Network etwork Failover LAN AP LAN STA HCP atic Routes	LAN LAN Overview Network Status Uptime: 0h 6m 37s. MAC: Address: D4AD:2068:66:14 W2: 266:18 KB (2215 Pkts.) TX: 943:71 KB (2155 Pkts.) TX: 943:71 KB (2155 Pkts.) IV:41:101:10:02:54/24 Vian Management Enable Vian	Actions © Connect @ Edit PORTS LAN2
yout VAVESHARE hare avesome hardware- VS-431E tus vvices twork twork N N N N N N N N N N N N N N N N N N N	LAN LAN Overview Network Status Uptime: 0h 6m 37s. MAC: Address: 04AD:2068666:14 RXC: Address: 04AD:2058666:14 RXC: Address: 04AD:2058666:14 RXC: Address: 04AD:2058666:14 RXC: 34371 KB (2153 Picks) IPV4: 10.100.254/24 Vian Management Enable Vian C Vian List Network Interface Lan(br-lan)	Actions Actions Actions Actions MUD REFRESHON MULAN2 MUL
gout WAVESHARE share awesome hardware- wS-431E atus ervices etwork AN VU etwork Failover LAN AP LAN STA HCP atic Routes agnostics *N	LAN LAN Overview Network Status Uptime: 0h 6m 37s Uptime: 0h 6m 37	Actions Actions LANI PORTS LANI LAN2
gout VAVESHARE share awesome hardware- VS-431E atus rvices etwork AN IN IIular Network twork Failover LAN AP LAN STA ICP atic Routes agnostics IN ewall	LAN LAN Vetwork Status Uptime: 0h 6m 37s MAC-Address: 04AD:206866:14 PR Pr-lan Dr-lan Vian Management Enable Vian Vlan List Network interface Ian(br-lan) Ian3(br-lan3)	Actions Actions LANN PORTS UNIVERSIDATION

Figure 12 Switch WAN/LAN interface

Application diagram as follow:



Figure 13 LAN+LAN+4G networking

4.4. COMMON FUNCTIONS

4.4.1. 4G INTERFACE

WS-431E 4G Router supports one 4G interface to access internet. Functional diagram as follow:



Figure 14 4G interface

User can configure 4G interface by Web Server as follow:

WAVESHARE

-share awesome hardware-			
WS-431E	WAN		
> Status	WAN Overview		
Services	Network	Status	Actions
V Network	WAN_4G	MAC-Address: 00:00:00:00:00:00:00 RX: 0.00 B (0 Plets.) TX: 0.00 B (0 Plets.)	Se Connect
LAN Cellular Network Network Failover	WAN_WIRED	Uptime: oh om os MAC-Address: D4:AD:20:68:66:12 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	🖉 Connect. 📝 Edit
WLAN AP WLAN STA			
DHCP			
Static Routes			
VPN			
Firewall			
System			
> Logout			WAVESHARE

4.4.2. LAN INTERFACE

WS-431E supports two LAN interface (one is WAN/LAN interface).

Default settings: One LAN interface (WAN/LAN used as WAN interface; IP address: 192.168.1.1; Subnet mask: 255.255.255.0; Open DHCP function).

User can configure LAN interface by Web Server as follow:

WAVESHARE -share awesome hardware-			ALTO RETRESH ON
WS-431E	LAN		
> Status	LAN Overview		
> Services	Network	Status	Actions
Vetwork WAN	LAN 8 ³ (*****) br-lan	Uptime: 7h 28m 23s MAC-Address: D4AD:20:68:66:14 RX: 5.36 MB (47472 Pkts.) TX: 37.70 MB (61831 Pkts.) IPv4: 10.10.100.254/24	Connect dit
Cellular Network Network Failover WLAN AP WLAN STA DHCP	Vian Manageme Enab	ent 🔹	pply Save
Static Routes Diagnostics			
> VPN > Firewall			
> System > Logout			WAVESHARE

Figure 16 LAN interface

DHCP default range of distribution is from 192.168.1.100 to 192.168.1.250 and default address lease time is 12 hours. Address range and lease time can be changed.

www.waveshare.com

you can find 'DHCP Server'as follow:

				AUTO REFRESH ON	
-snare awesome nardware-					
WS-431E	DHCP and Static				
StatusServices	DHCP list information and Stat Static leases are used to assign configurations where only hos	tic Lease n fixed IP addresses and symbolic ho ts with a corresponding lease are se	ostnames to DHCP clients. They as rved.	re also required for non-dynamic interface	
 Network 	Active DHCP Leases				
WAN	Hostname	IPv4-Address	MAC-Address	Leasetime remaining	
LAN	?	10.10.100.137	12:ae:92:1d:47:a9	6h 7m 33s	
Cellular Network	DESKTOP-NAEG2FU	10.10.100.215	f0:d4:15:4c:96:7c	8h 54m 38s	
Network Failover					
WLAN AP	T Static Leases				
WLAN STA	Hostname	MA	-Address	IPv4-Address	
Chatic Boutes					
Diagnostics		This s	ection contains no values yet		
> VPN					
Firewall	New rule:				
System	Hostname	MAC-Address		IPv4-Address	
> Logout	New rule		~	× 🛅 .	Add
				WWWEGUNG	12
			Analy Cours	ULANESHAL	23
			Apply Save		

Figure 17 DHCP function

4.4.3. WAN INTERFACE

WS-431E supports one WAN interface and WAN interface can switch between WAN/LAN interface. WAN interface supports DHCP and Static IP, and default setting is DHCP. User can configure WAN interface by Web Server as follow:

wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww			AUTO REFRESH ON
WS-431E	WAN		
> Status	WAN Overview		
> Services	Network	Status	Actions
V Network	WAN_4G	MAC-Address: 00:00:00:00:00:00 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	🦉 Connect 🗹 Edit
LAN Cellular Network Network Failover	WAN_WIRED	Uptime: 0h 0m 0s MAC-Address: D4:AD:20:68:66:12 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Edit
WLAN AP WLAN STA			
DHCP Static Routes Diagnostics			
> VPN			
> Firewall			
> System			WAVERUARE
> Logout			WAVESHARE

Figure 18 WAN interface

4.4.4. WLAN INTERFACE

Default parameters as follows:

SSID	WS-431E-XXXX(XXXX 是 MAC)
Password	www.waveshare.com
Channel	auto
HT Mode	auto
Encryption	mixed-psd

Figure 19 WLAN default parameters

V	waveshare awesome h	ARE hardware-		AUTO REFRESH ON	<u> </u>
	WS-431E	WLAN AP Settings			Î
> >	Status Services	2.4G Settings Client Inf	formation		7
~	Network WAN LAN Cellular Network	Status	Mode: Master SSID: WS-431E-6612 BSSID: D4:AD:20:68:66:15 Channel: 6 (2.437 GHz) Tx-Power: 26 dBm		
	Network Failover WLAN AP WLAN STA DHCP Static Pourtes	Enable Hide SSID SSID Encryption	☑ □ WS-431E-6612 mixed-psk ✓		
	Diagnostics	Кеу	•••••	8	
	VPN Firewall System	HW Mode Channel	11ng auto If STA is enabled, the configura	tion is affected by STA.	
	Logout	HT Mode	auto V	tion is affected by STA.	
		Regions	00 - World ~	Apply Save	

Figure 20 WLAN interface

Entering WLAN interface configuration web, user can change follow parameters. User can configure SSID on Web Server as follow:

WAVES -share aweso	HARE me hardware-	AUTO REFRESH ON
WS-431E	WLAN AP Settings WLAN AP Settings	Â
> Status > Services	2.4G Settings Client In	formation
 Vetwork WAN LAN Cellular Network 	Status	Mode: Master SSID: WS-431E-6612 BSSID: D4:AD:20:68:66:15 Channel: 6 (2.437 GHz) Tx-Power: 26 dBm
Network Failover WLAN AP WLAN STA	Enable Hide SSID	
DHCP Static Routes	SSID	WS-431E-6612 mixed-psk
Diagnostics	Key	·····
> VPN > Firewall > System	HW Mode Channel	11ng • auto • If STA is enabled the configuration is affected by STA
> Logout	HT Mode	auto If STA is enabled, the configuration is affected by STA. If STA is enabled, the configuration is affected by STA.
	Regions	00 - World WAVESHARE Apply Save

Figure 21 WLAN interfaceConfigure SSID

User can configure password on Web Server as follow:

WAVESHARE

V	waveshare awesome	ARE hardware-	AUTO REFRESH ON
	WS-431E	WLAN AP Settings WLAN AP Settings	
	Status Services	2.4G Settings Client In	formation
~	Network WAN LAN Cellular Network	Status	Mode: Master SSID: WS-431E-6612 BSSID: D4:AD:20:68:66:15 Channel: 6 (2.437 GHz) Tx-Power: 26 dBm
[Network Failover WLAN AP WLAN STA	Enable Hide SSID	
	DHCP Static Routes	SSID	WS-431E-6612 mixed-psk
	Diagnostics	Кеу	•••••
	VPN Firewall System	HW Mode Channel	11ng auto If STA is enabled, the configuration is affected by STA.
	Logout	HT Mode	auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto auto au
		Regions	00 - World V ISHARE Apply Save

Figure 22 Configure password

Other settings on Web Server as follow:

WAVESHARE

V	wavesh -share awesome	ARE hardware-		AUTO REFRESH ON	
	WS-431E	WLAN AP Settings WLAN AP Settings			Î
	Status Services	2.4G Settings Client In	formation		
~	Network WAN LAN Cellular Network	Status	Mode: Master SSID: WS-431E-6612 BSSID: D4:AD:20:68:66:15 Channel: 6 (2.437 GHz) Tx-Power: 26 dBm		
C	Network Failover WLAN AP WLAN STA	Enable Hide SSID			
	DHCP Static Routes Diagnostics	SSID Encryption Key	WS-431E-6612 mixed-psk ~	8	
	VPN Firewall	HW Mode	11ng ~		
	System	Channel	auto	tion is affected by STA.	
	Logout	HT Mode	auto 🗸	tion is affected by STA.	
		Regions	VESHARE	Apply Save	

Figure 23 Other settings

You can view the list of wifi clients on the wireless screen:

WS-431E 4G Router

WAVESHARE

Wŷ	WAVESHARE						A	JTO REFRESH ON	**
	WS-431E	WLAN AP Setting	IS						
>	Status	WLAN AP Settings							
	Services								
	Network	2.4G Settings	ent Information						-
	WAN	SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate	
	LAN	WS-431E-6612	F0:D4:15:4C:96:7C	10.10.100.215	-47 dBm	-95 dBm	130.9 Mbit/s	144.4 Mbit/s	
	Cellular Network								
	Network Failover								
	WLAN AP			Apply	Save				
	WLAN STA								
	DHCP								
	Static Routes								
	Diagnostics								
	VPN								
	Firewall								
	System						000000	Renve	2
	Logout						UUAUU	elviance	5
	Figure 24 WiFi client list page								

4.4.5. NETWORK DIAGNOSIS

User can use network diagnosis function by Web Server as follow:

waveshare -share awesome hardware-			
WS-431E	Diagnostics		
> Status > Services	Network Utilities 8.8.8.8	8.8.8.8	www.google.com
Vetwork WAN LAN			aa residokop
Cellular Network Network Failover WLAN AP			
WLAN STA DHCP			
Diagnostics			
 Firewall System 			
> Logout			WAVESHAR

Figure 25 Network diagnosis

- Ping: User can do PING test to a specific address in WS-431E.
- Traceroute: Can acquire routing path to visit a specific address.

• Nslookup: Can analyse DNS into IP address

4.4.6. MODULE NAME AND TIME ZONE

WS-431E default module name is WS-431E and default Time Zone is New York time zone.

User can configure module name and Time Zone by Web Server as follow:

wavesi -share awesom	HARE 1e hardware-	
WS-431E	System	
> Status > Services	Here you can configure the basic aspects of your device like its System Properties	hostname or the timezone.
> Network > VPN	General Settings Design	
Firewall System	HOSUIAIIIE W3-431L	
Administration Reboot Timer		Apply Save
NTP Http Port		
Syslog Backup/Upgrade		
> Logout		WAVESHARE
WAVESHARE share awesome hardware-		АЛО ИСИКСИ ОН 📑 🛀
WS-431E Status Services	NTP The Time Synchronization section is used to configure general router time settings, like selecting the local Time Parameter	time zone, synchronizing the time and NTP.
> Network > VPN > Firewall > System	Current System Time 2023-05-30 12-09:52 Tue Sync with browser Time Zone America/New York:	
System Administration Reboot Timer Http Port Syslog Backup/Upgrade	Time Synchronization Enable NTP Client NTP Server Alternate NTP Server pool.ntp.org au pool.ntp.org au pool.ntp.org	
Reboot Logout 	us.pool.ingl.org 📖	WAVESHARE

Figure 26 Module name and Time Zone

4.4.7. STATIC ROUTE

www.waveshare.com

The static route has the following parameters. By default, a maximum of 20 static routes can be added.

Name	Description	Default parameter	
port	Lan, wan_4G, wan_wired, vpn interfaces	Lan	
Object (destination	The address or address range of the	empty	
address)	object to be accessed		
Subnot mark	The subnet mask of the object network	empty	
Subilet mask	to be accessed		
Gateway (Next hop)	The address to forward to	empty	
Metric	Number of packet hops	empty	

Figure 27 Static route parameter table

Static route describes the routing rules of Ethernet packets.Test example: Test environment, two flat routers A and B, as shown below.



Figure 28 Static routing table example diagram

The WAN ports of routers A and B are connected to the network at 192.168.0.0. The LAN port of router A is on the 192.168.2.0 subnet, and the LAN of router B is on the 192.168.1.0 subnet.Now, if we want to make A route on router A so that when we access the 192.168.1.x address, it is automatically forwarded to the router

WAVESHARE

waveshare -share awesome hardware-					
WS-431E	Static Routing				
) Status	To find information	n on static routing configur	ation, refer to the figure and table b	elow	
> Services	Static Routing	Routing Table			
✓ Network	Static IDud Dour	too			
WAN	Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric
LAN		2			
Cellular Network	This section contains	no values vet			
Network Failover					
WLAN AP	New Rule:				
WLAN STA	Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric
DHCP		Host-IP or Network	If target is a network		
Static Routes		Host a of Healone	in target is a network		
Diagnostics	lan 🗸	192.168.1.0	255.255.255.0	192.168.0.202	0 Add
> VPN	25				
> Firewall			Apply	Save	
> System					MANESUADE
> Logout					UNUSONNE

Figure 29 Add routing table page

4.5. BASIC FUNCTIONS

4.5.1. WEB SERVER PASSWORD

Default password is root, this password is used to enter Web Server.

User can change password by Web Server as follow:

V	share awesome	IARE hardware-		
	WS-431E	Route	r Password	
	Status	Change	s the administrator p	assword for accessing the device
	Services	Config	uration	
	Network		Dacsword	đ
	VPN		Passworu	Password support: numbers, letters and symbols.no more than 16
>	Firewall	-	Confirmation	2) 2)
~	System			
	System			
	Administration			Apply
	Reboot Timer			
	NTP			
	Http Port			
	Syslog			
	Backup/Upgrade			
	Reboot			WAWBSLADE
>	Logout			UNUCOUNKE

Figure 30 Web Server password

4.5.2. RESTORE

Hardware restore: Press Reload button over 5 seconds and release, WS-431E will restore default settings and reset.

User can restore default settings by Web Server as follow:

WS-431E 4G Router

WAVESHARE

waveshare	-
WS-431E	Backup / Flash Firmware
> Status	Backup / Restore
> Services	Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" .
> Network	Download backup: Generate archive
> VPN	Reset to defaults:
> Firewall	
∽ System	To restore a miguration files, you can upload a previously generated backup archive here.
System	Restore backup: Please select file 🛛 Browse 🕼 Upload archive
Administration	
Reboot Timer	
NTP	Flash new firmware image
Http Port	Upload a proper image here to replace the running firmware. Check "Keep settings" to retain the current configuration.
Syslog	Keep settings:
Backup/Upgrade	Image: Please select file Browse Image
Reboot	
> Logout	WAVESHARE

Figure 31 Restore default settings

4.5.3. UPGRADE FIRMWARE VERSION

Upgrade by Web Server as follow:

www waveshare	E E
WS-431E	Backup / Flash Firmware
> Status	Backup / Restore
> Network	Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform Download backup:
> VPN > Firewall	Reset to defaults:
∽ System	To restore configuration files, you can upload a previously generated backup archive here.
System	Restore backup: Please select file Browse Dyload archive
Administration	Choose firmware name Upgrade
Reboot Timer	
NTP	Flash new firmware image
Http Port	Upload a proper image here to replace the running firmware Check "Keep settings" to retain the current configuration.
Syslog	Keep settings:
Backup/Upgrade	Image: Please select file Browse I Flash image
Reboot	
> Logout	

Figure 32 Upgrade firmware version

The whole upgrade process will last about 1 minute, user can enter Web Server after about 1 minute. User can choose saving settings. User should keep powering up and LAN/WIFI connection during the whole upgrade process.

4.5.4. RESET

Reset time is about 40~60 seconds.Reset by Web Server as follow:

WAVE -share awes	SHARE E
WS-431E	System
> Status	Reboots the operating system of your device
> Services	Reboot
> Network	
> VPN	2 Perform reboot
> Firewall	
∽ System	
System	
Administration	
Reboot Timer	
NTP	
Http Port	
Syslog	
Backup/Upgrac	le
Reboot	
> Logout	WAVESHARE

Figure 33 Reset module

4.6. FIREWALL FUNCTION

4.6.1. BASIC SETTINGS

The default value is two firewall rules.

WA -share	VESHARE awesome hardware-							
WS- > Status > Servic > Netw > VPN • Firew. Gener	431E es vrk NI al Settings	Firewall - Zone Setting The firewall creates zones ov General Settings Enable SYN-flood protection Drop invalid packets Input	rer your network interfaces to co	ntrol network traffi	: flow.	2020		
Port F Traffic Acces > Syster > Logou	orwards Rules s Restrictions n ıt	Output Forward Zones=>Forward	accept accept			W/A	Vesh	ANKE
		Source Zone	e=>Destination zones : :::::::::::::::::::::::::::::::::::	Apply	Output accept accept	Forward	Masquerading	MSS clamping

Figure 34 Firewall setting interface

<Introduction>

- Input: a packet accessing the router IP.
- Output: the packet to be sent by the router IP;
- Forwarding: data forwarding between interfaces, without going through the route itself;
- Masquerading: it is only meaningful for WAN port and 4G port, and the camouflage of IP address when accessing external network;
- MSS clamping: limits the size of message MSS, which is generally 1460.

<A, Rule 1>

- Input and forwarding from LAN port to wired WAN port are accepted;
- If there is a data packet from the LAN port and needs to access the WAN port, allowing the data packet to be forwarded from the LAN port to the WAN port is considered forwarding.
- You can also open the router's webpage on the LAN port, which is considered "input".
- The router itself connects to the external network, such as synchronizing time, which is considered "output".

<B, Rule 2>

- Wired WAN port and 4G port accept "inbound", "outbound" and "forwarding";
- If there is an "input" packet, logging in to the router's webpage from the WAN port is allowed;
- If there is an "output" packet, the router accessing the external network through WAN port or 4G port is allowed;
- If there is a "forward" packet, a packet from WAN port being forwarded to 4G port is allowed.

For example: In a certain application scenario, the LAN port needs to access the router's settings, and the router is also capable of connecting to the internet. However, devices connected to the LAN port are not allowed to access the internet. In this case, the LAN to WAN forwarding rule can be set to "deny" or "discard" (discard meaning no feedback information) to achieve this requirement. In a certain application scenario, the LAN port needs to access the router's settings, and the router is also capable of connecting to the internet. However, devices connected to the LAN port are not allowed to access the internet. In this case, the LAN to WAN forwarding rule can be set to "deny" or "discard" (discard meaning no feedback information) to achieve the LAN port are not allowed to access the internet. In this case, the LAN to WAN forwarding rule can be set to "deny" or "discard" (discard meaning no feedback information) to achieve this requirement.

waveshare -share awesome hardware-						
WS-431E	Firewall - Zone Settings The firewall creates zones over yo	our network interfaces to contro	network traffic flow.	2		
Status Services Network	General Settings					
> VPN	Enable SYN-flood protection Drop invalid packets					
General Settings Port Forwards	Input act	cept ~			WAVES	SHARE
Access Restrictions	Forward ac	cept 🗸				
> Logout	Zones=>Forward					
	Source Zone=>I	estination zones	accept 🗸	accept v reject v	Masquerading	
	wan: wan_wired: 🔊 w	wan_4g:) ⇒ ACCEPT	accept 🗸	accept 🗸 accept 🗸	2	
			Apply Save	2		

Figure 35 Firewall Settings page 2

4.6.2. NAT FUNCTION

1. IP address masquerading

IP address masquerading refers to the practice of modifying the source IP address of outgoing data packets to a specific interface's IP address on the router. When the "Masquerading" option is selected, the system will change the source IP address of outgoing data packets to the IP address of the WAN port on the router.

Note: IP dynamic masquerading and MSS clamping must be turned on on WAN port, and IP dynamic masquerading and MSS clamping are prohibited on LAN port.

IP address masquerading settings are located in the "Firewall-Zone Settings" interface.

WAVESHARE -share awesome hardware-							-
WS-431E	Firewall - Zone Setting The firewall creates zones on	gs ver your network interfaces t	to control network tra	ific flow.			
> Status > Services	General Settings						
> Network > VPN	Enable SYN-flood protection						
Firewall General Settings	Drop invalid packets	arcent	v				
Port Forwards Traffic Rules	Output	accept	~		D	NAVES	SHARE
Access Restrictions	Forward	accept	~				
> System	Zones=>Forward						_
	Source Zon	e=>Destination zones	Inp	ut Ocryput	Forward	Masquerading	MSS clamping
	lan: lar	:: ﷺ ⇒ wan	accept	✓ accept	✓ accept ✓		
	wan: wan_wired:	wan_4g: ⊉ ⇒ ACCI	accept	✓ accept	✓ accept ✓		
			Apply	Save			

Figure 36 IP address camouflage Settings

2.SNAT

Source NAT is a special form of packet masquerading, which changes the source address of packets leaving the router and fixes the source IP address of packets leaving the router as a specific IP to send out. When using it, you should disable the IP dynamic masquerading of the WAN port.

WĄ	WAVESHARE -share awesome hardware-								
,	WS-431E Status	Firewall - Zone Setting The firewall creates zones on	75 ver your network interface	es to control net	work traffic fl	ow.			
>	Services Network VPN	General Settings Enable SYN-flood protection							
	Firewall General Settings Port Forwards Traffic Rules Access Restrictions	Drop invalid packets Input Output Forward	accept accept accept	*				WAVES	HARE
>	System Logout	Zones=>Forward Source Zon	e=>Destination zones		Input	Onqut	Forward	Masquerading	MSS clamping
		lan: lan wan: wan_wired:	r: ∰ 兼 ⇒ wan ⊉ wan_4g: ⊉ ⇒ Ac	CEPT	accept	 accept ✓ accept ✓ 	accept 🗸		
					Apply S	ave			

Figure 37 SNAT setting 1

Then set the Source NAT, and change the source IP address of the packet leaving the router to a fixed IP, which is located under "firewall-Traffic rules". Fix the source IP address to 192.168.9.1, and its setting interface is as follows.

WS-431E 4G Router

WAVESHARE

waveshare					
WS-431E	Firewall - Traffic	Rules			
> Status	Traffic rules define po router.	licies for packets traveling between different zones, for exar	mple to reject traffic betwee	n certain hosts or to	open WAN ports on the
Services Network V/PN	Traffic Rules	Protocol	Action	Enable Sort	
Firewall General Settings Port Forwards	Allow- Ping	IPv4-ICMP with type echo-request From any host in wan To any router IP on this device	Accept input	2 • •	Edit Edit
Traffic Rules Access Restrictions	Open ports on router: Name	Protocol External port			
> System > Logout	New input rule	TCP+UDP 🗸	ld	WAW	eshar
	New forward rule	Source zone Destination zone			
	Source NAT	Protocol		Action	Enable S
		This section contain:	s no values yet		
	New source NAT:	Source zone Destination zone To s	ource IP To source port	t	
	test	lan v wan v 192	2.168.9.1 V Do not rewrit	te 🔳	Add and edit
		Apply	Save		

Figure 38 SNAT setting 2

Click "Add" and "Edit".

WC 1245		
WS-43TE	irewall - Traffic Rules	- SNAT test
Status	his page allows you to cha	nge advanced properties of the traffic rule entry, such as matched source and destination hosts.
Services	Enable	Oisable
Network		
> VPN	Name	test
✓ Firewall	Protocol	TCP+UDP 🗸
General Settings	Source zone	
Port Forwards		
Traffic Rules		O wan: wan_wired: 🔬 wan_4g: 🔬
Access Restrictions	Source IP address	any 🗸
System		Only match incoming traffic from this IP or range.
	Source port	any
Luguar		Match incoming traffic originating from the given source port or port range on the client host.
	Destination zone	O lan: lan: 🐲 👳
		wan: wan_wired: J wan_4g: J
	Destination IP address	Destination in or in ranne
		Bestination (p on p range.
	Destination port	any O Destination port or port range.
	CNAT ID address	100 100 0 1
	SINAT IP address	Rewrite matched traffic to the given address.
	SNAT port	Do not rewrite
	Silki porc	Rewrite matched traffic to the given source port. May be left empty to only rewrite the IP address.

Figure 39 SNAT setting 3

If the source IP, source port and destination IP and destination port are not filled in, all IP and ports will be defaulted. Save after setting.

Name	Description	Default parameter
Name	The name of this firewall rule	-
Protocol	Configurable: TCP+UDP/TCP/UDP/ICMP	TCP+UDP
	Need to match the source IP of input	
Source IP address	traffic.	empty
	Empty means matching all source IPS.	
	Need to match the source port of input	
Source port	traffic.	omntv
	Empty means all source ports are	empty
	matched.	
	Need to match the destination IP of	
Doctoption IP	input traffic.	omente
Desteation in	Empty means that all target IPS are	empty
	matched.	
Target port	Destination port that needs to match	empty

www.waveshare.com

	input traffic, empty means matching	
	the destination port.	
	Customized IP when	
SINAT IP duuless	traffic to this address.	adding
	Modify the source port of matching	
SNAT port	traffic to this port, empty means	empty
	using the source port.	

WAVESH -share awesome	ARE hardware-			
WS-431E	Firewall - Traffic I	Rules		
StatusServices	Traffic rules define po router.	licies for packets traveling between different zones, for ex	ample to reject traffic between	n certain hosts or to open WAN ports on the
> Network > VPN	Traffic Rules Name	Protocol	Action	Enable Sort
General Setting Port Forwards	Allow- Ping	IPv4-ICMP with type echo-request From any host in wan To any router IP on this device	Accept input	🔹 🔹 🗹 Edit 💌 Delete
Traffic Rules	Open ports on router:			
Access Restrict System Logout	Name New input rule New forward rule:	Protocol External port	.dd	WAVESHARE
	Name	Source zone Destination zone	+	
	Source NAT	Protocol	Action	Fnable Sort
	test	Any TCP, UDP From any host in Ian To any host in wan	Rewrite to source IP 192.168.9.1	Z • • Z Edit Z Delete
	New source NAT:			
	Name New SNAT rule	Source zone Destination zone To	source IP To source port Please choc	te Add and edit
		Apply	Save	

Figure 40 SNAT setting 4

3. Port forwarding

Port forwarding allows computers or services from the Internet to access computers or services within a private local area network (LAN). It involves mapping a specified port of the wide area network (WAN) address to a host within the internal network (LAN).

WS-431E 4G Router

WAVESHARE

WĄ	WAVESHARE -share awesome hardware-					
	WS-431E	Firewall - Port Forv	vards			
	Status	Port forwarding allows r	emote computers on t	he Internet to connect to a specifi	c computer or service within the private LAN.	
	Services	Port Forwards				
	Network	Name	Match Ru	les	Forwarding To	Enable Sort
	VPN					
~	Firewall			This section contain	is no values yet	
-	General Settings					
	Port Forwards	New Port Forwarding Rul	es:			
	Traffic Rules Access Restrictions	Name	Protocol	External External port zone	Internal Internal IP Internal port zone address	
	System	test	TCP+UDP	✔ wan ✔ 81	lan 💙 192.168.1.1 (🎔 81	🔛 Add
>	Logout			Appiy	Save	

Figure 41 Port setting interface 1

After setting the forwarding rule, you need to click the "Add" button on the right, and then this rule will be displayed in the rule column.

www.eshare wesome hardware-						
WS-431E	Firewall - Port For	rwards	he Internet to connect to a sne	cific computer or service within th	e private I AN	
> Status						
> Services	Port Forwards					
> Network	Name	Match Rules		Forwarding To	Enable	Sort
> VPN						
✓ Firewall General Settings ✓	test	IPv4-TCP, UDP From <i>any host</i> in <i>wa</i> Via <i>any router IP</i> at por	n t 81	IP 192.168.1.1, port 81 in lan	8	• • EDelete
Port Forwards Traffic Rules	New Port Forwarding R	ules:				
Access Restrictions	Name	Protocol	External External port zone	Internal Internal IP zone address	Internal port	
> System > Logout	New port forward	TCP+UDP	♥ wan ♥	lan 🗸	~	Add 🔛
			Apply	Save		

Figure 42 Port setting interface II

Then click the "Save & Apply" button in the lower right corner to make the settings take effect.

The above setting, 192.168.1.1:80 is the router's own web server. If we want to access a device within the local area network (LAN) from the Internet, we need to set up an external network to internal network mapping, also known as port forwarding. For example, we can set up the external network port as 81 and map it to the internal network IP address 192.168.1.1 with an internal network port of 80.

When we access port 81 from WAN, the access request will be transferred to

192.168.1.1:80.

< description >

You can add 20 rules to the upper limit of port forwarding rules.

Name	Description	Default parameter	
name	Name and character type of this port	ometu	
name	forwarding rule	empty	
Drotocol	Protocol type, which can be set as		
Protocol	TCP+UDP/TCP/UDP.	TCP+UDP	
External area	Include wired wan, 4G, VPN.	wan	
	You can set a single port or port range,		
Extornal nort	such as 8000-9000. Description: It is a	ometu	
	DMZ function when the external port	empty	
	and the internal port are empty.		
Internal region	Router subnet area	lan	
Internal IP	Router LAN area IP address	empty	
	You can set a single port or port range,		
Internal port	such as 8000-9000. Description: It is a	omntu	
	DMZ function when the external port	empty	
	and the internal port are empty.		

4. NAT DMZ

Port mapping is to map a designated port of the WAN port address to a host in the internal network. The function of DMZ is to map all ports of the WAN port address to a host, and the setting interface and port forwarding are in the same interface. When setting, the external port is left blank.

WAVESHARE

WĄ	WAVESHARE -share awesome hardware-				
	WS-431E	Firewall - Port Forward	ds		
	Status	Port forwarding allows remo	te computers on the Internet to connect to a specific	computer or service within the private LAN.	
	Services	Port Forwards			
	Network	Name	Match Rules	Forwarding To	Enable Sort
	VPN				
~	Firewall		This section contains	no values yet	
	General Settings				
Г	Port Forwards	New Port Forwarding Rules:			
	Traffic Rules	Name	Protocol External External port	Internal Internal IP Internal por	
	Access Restrictions		zone	zone address	
	System	test	TCP+UDP ♥ wan ♥	lan ♥ 192.168.1.1 (♥	🗋 Add
	Logout				
			Apply	Save	

Figure 43 DMZ setting one

Click Add and save.

W	WAVESHARE -share awesome hardware-						
	WS-431E	Firewall - Port Forwa	ırds				
;	Status Services	Port forwarding allows rer Port Forwards	note computers on the	Internet to connect to a spec	ific computer or service within t	he private LAN.	
	Network VPN	Name	Match Rules		Forwarding To	Enable	Sort
· ·	Firewall General Settings	test	IPv4-TCP, UDP From any host in wan Via any router IP		IP <i>192.168.1.1</i> in <i>lan</i>	2	• • E Delete
L	Traffic Rules	New Port Forwarding Rule	E				
	Access Restrictions	Name	Protocol	External External port zone	Internal Internal IP zone address	Internal port	
	System Logout	New port forward	TCP+UDP	v wan v Apply	Ian V	*	t Add

Figure 44 DMZ setting two

< Note >

Port mapping and DMZ functions cannot be used at the same time.

4.6.3. COMMUNICATION RULES

Communication rules can selectively filter specific Internet data types and prevent Internet access requests, and enhance network security through these communication rules. Firewall has a wide range of applications. Here are some common applications.

Name	Description	Default parameter
name	Name and character type of this rule	-
Restricted address	Restrict IPv4 address	IPv4 address only
Protocol	The protocol type of the restriction rule can be selected from: TCP+UDP/TCP/UDP/ICMP	TCP+UDP
Matching ICMP type	Matching ICMP rules, just select any.	Any
Source region	Data stream source area, optional: any area, WAN, LAN. LAN: indicate that rules for subnet access to external network. WAN: indicates the rules for external network to access internal network.	LAN
Source MAC address	The source MAC that needs to match the rule can be multiple Macs. When there are multiple Macs, the Macs are separated by spaces. Empty: indicates that all Macs are matched. Note: When matching the source MAC address, the source IP address should be set to empty.	empty
Source IP address	The source IP that needs to match the rule can be an IP range. Example of IP range: 192.168.1.100-192.168.1.200 Empty: indicates that all IPS are matched. Note: When matching the source IP address, the source MAC address should be set to empty.	empty
Source port	The source port that needs to match the rule can be a port range. Example of port range: 8000-9000 Empty: means to match all ports.	empty
Target area	Target area of data flow, optional: any area, WAN, LAN. LAN: indicate that rules for subnet access to external network.	WAN

www.waveshare.com

www.waveshare.com/wiki

	WAN: indicates the rules for external	
	network to access internal network.	
	The destination IP address of the	
Destination address	access.	empty
	Empty: Represents all addresses.	
	The destination port number of the	
Destination port	access.	empty
	Empty: stands for all.	
	You can choose to discard, accept,	
	reject and do nothing when you receive	
	such a packet.	
	Discard: packets that receive this rule	
	will be discarded.	
action	Accept: packets that receive this rule	Accept
	will be accepted.	
	Reject: packets receiving this rule will	
	be rejected.	
	No action: no action will be taken when	
	receiving this rule packet.	

1. IP Addresses Blacklist

First, enter the name of the new forwarding rule, and then click the "Add and Edit" button.

WAVESHARE -share awesome hardware						
WS-431E	Firewall - Traffic	Rules				
> Status	Traffic rules define po router.	licies for packets traveling between different zones, for example	to reject traffic betwee	n certain h	osts or to open '	WAN ports on th
> Services						
> Network	Iraffic Rules	Protocol	Action	Enable	Sort	
> VPN	Name	PIOLOGI	Action	Lilable	3011	
 Firewall General Settings Port Forwards 	Allow- Ping	IPv4-ICMP with type echo-request From any host in wan To any router IP on this device	Accept input		• •	Edit 🛛 Dele
Traffic Rules	Open ports on router:					
Access Restrictions	Name	Protocol External port				
> System	New intro gule					
> Logout	Her hipe and					
	New forward rule:					
	Name	Source zone Destination zone				
	New forward rule	lan 🗸 wan 🗸 🖻 Add and edit				
	Source NAT					
	Name	Protocol			Action	Enable S
		This section contains no v	values yet			
	New source NAT:					
	Name	Source zone Destination zone To source	IP To source por	t		
	New SNAT rule	lan 🗸 wan 🗸 Pleas	e chot¥ Do not rewr	te	🔳 Add ar	nd edit
		Apply				

Figure 45 Firewall IP blacklist 1

In the jumped page, select "lan" as the source zone, and select "any" as the source MAC addresses and source IP address options (if only the specific IP in the local area network is restricted from accessing the specific IP of the external network, you need to fill in the IP address or MAC address here, one of which is "any" or the IP address corresponds to the MAC address, otherwise it will not take effect), as shown in the following figure.

WAVESHARE -share awesome hardware-		
WS-431E	Firewall - Traffic Rules	- test
> Status	This page allows you to chan	ge advanced properties of the traffic rule entry, such as matched source and destination hosts.
 Services Network VPN Firewall General Settings Port Forwards Traffic Rules Access Restrictions System Logout 	Enable Name Restrict to address family Protocol Match ICMP type Source zone	Disable test IPv4 only TCP+UDP any Any zone Ian: Ian: ::::::::::::::::::::::::::::::
	Source MAC address Source IP address	any Only match incoming traffic from these MACs. any Only match incoming traffic from this IP or range.
	Source port	any Only match incoming traffic originating from the given source port or port range on the client host
	Destination zone	 Device (input) Any zone (forward) Ian: Ian: *** * wan: wan_wired: * wan_4g: *
	Destination address	any Redirect matched incoming traffic to the specified internal host
	Destination port	any Redirect matched incoming traffic to the given port on the internal host
	Action	accept 👻
	Back to Overview	Apply Save

Figure 46 Firewall IP blacklist 2

Select WAN in the destination zone, fill in the destination address that is forbidden to access, and click "Save" and "Apply" after the setting of "Reject" is selected. As shown below.

WAVESHARE	
WS-431E	s , test
This page allows you to ch	ange advanced properties of the traffic rule entry, such as matched source and destination hosts.
Status	
Services Enable	Ø Disable
Network Name	test
VPN Restrict to address family	IPv4 only
Firewall	
General Settings Protocol	
Port Forwards Match ICMP type	any
Traffic Rules Source zone	O Any zone
Access Restrictions	lan: lan: *** *
System	
Logout	○ wan: wan_wired: ﷺ wan_4g: ﷺ
Source MAC address	any
	Only match incoming traffic from these MACs.
Source IP address	any v
	only match incoming dame from this iP or lange.
Source port	any ② Only match incoming traffic originating from the given source port or port range on the client host
Destination zone	
Destination zone	O Device (input)
	O Any zone (forward)
	O lan: lan: 🕎 🗶
N 1997	• wan: wan_wired: 🛃 wan_4g: 🛃
Destination address	any @ Redirect matched incoming traffic to the specified internal host
Destination and	
Destination por	 Redirect matched incoming traffic to the given port on the internal host
Action	reject 🗸

Figure 47 Firewall IP blacklist 3

WĄ	WAVESHARE -share awesome hardware-					-20
,	WS-431E	Firewall - Traffic R	ules			
> \$	Status Services	Iraffic rules define poli router.	cies for packets traveling between different zones, for example	e to reject traffic betweer	n certain h	osts or to open WAN ports on the
1 < / <	Network VPN	Traffic Rules Name	Protocol	Action	Enable	Sort
~ F	Firewall General Settings	Allow- Ping	IPv4-ICMP with type echo-request From any host in wan To any router IP on this device	Accept input		🔹 🔹 🧭 Edit 💌 Delete
F 1	Port Forwards Traffic Rules Access Restrictions	test	IPv4-TCPJUDP From any host in Ian To any host in wan	Refuse forward		* * Edit Edit Delete
> s > t	System Logout	Open ports on router:	Protocol External port			
		New input rule	TCP+UDP 🗸 🛅 Add			
		New forward rule:	funner Durticities and			
		New forward rule	Ian v wan v Add and edit			
		Source NAT				
		Name	Protocol			Action Enable Sort
			This section contains no	values yet		
		New source NAT:	Source zone Destination zone To source	ce IP To source port		
		New SNAT rule	lan 🗸 wan 🗸 Plea	ise choc∽ Do not rewrit	:e	Add and edit
			Apply Sav	/e		

Figure 48 Firewall IP blacklist 4

Once this configuration is set up, the blacklist function will be implemented.

2. IP address Whitelist

First, add the communication rule of IP or MAC address to be whitelisted, enter the name of the rule in the new forwarding rule, and then click Add and Edit.

WS-431E 4G Router

WAVESHARE

WS-431E	Firewall - Traffic	: Rules						
	Traffic rules define p	olicies for packets trave	eling between different zo	nes, for example to reje	ect traffic betweer	n certain h	osts or to open V	/AN ports on t
Status	router.							
Services	Traffic Rules							
VPN	Name	Pi	otocol		Action	Enable	Sort	
 Firewall 								
General Settings	Allow-	IPv4-ICMP wit From ar	n type echo-request ay host in wan		Accept input			Edit 🛛 💌 De
Port Forwards	Ping	To any route	r IP on this device					
Traffic Rules	Open ports on router	:						
Access Restrictions	Name	Protocol	External port					
System		TC0. UDD	1					
Logout	New in uc Tule	TCFTODF		Add				
	New forward rule:	C	Destination and					
	IName	Source zone	Destination zone					
	test	lan	wan 🗸 🖻 A	Id and edit				
	Source NAT							
	Name		Protocol				Action	Enable
			This sec	tion contains no values	yet			
	New source NAT:							
	Name	S	ource zone Destination	on zone To source IP	To source port			
	New SNAT rule	1	an 💙 wan	 Please chool 	 Do not rewrit 	e	Add and	l edit

Figure 49 Firewall IP white list 1

In the jumped page, select "lan" as the source zone, and select "any" as the source MAC address and source address (if it is a specific IP that allows a specific IP in the LAN to access the external network, you need to fill in the IP address or MAC address here, one of which is "any" or the IP address corresponds to the MAC address, otherwise it will not take effect), as shown in the following figure.

WAVESHARE -share awesome hardware-		ì	
WS-431E			
	Firewall - Traffic Rules	- test	
> Status	This page allows you to chan	ge advanced properties of the traffic rule entry, such as matched source and destination hosts.	
> Services	Enable	S Disable	
> Network	N	hast	
> VPN	Name		
✓ Firewall	Restrict to address family	IPv4 only	
General Settings	Protocol	TCP+UDP 🗸	
Port Forwards	Match ICMP type	any	
Traffic Rules	Source zone		
Access Restrictions	Dourte Lone	O Any zone	
> System) Ian: Ian: 🕎 👷	
> Logout		O wan: wan_wired: 🔬 wan_4g: 🔬	
	Source MAC address Source IP address	any Only match incoming traffic from these MACs. any Only match incoming traffic from this IP or range.	
	Source port	any Only match incoming traffic originating from the given source port or port range on the client host	
	Destination zone	Device (input) Any zone (forward)	
		 Jan: Ian: 25 ★ wan: wan_wired: 2 wan_4g: 2 	
	Destination address	any Redirect matched incoming traffic to the specified internal host	
	Destination port	any Redirect matched incoming traffic to the given port on the internal host	
	Action	accept 🗸	
	Back to Overview	Apply Save	

Figure 49 Firewall IP white list 2

Select WAN in the target zone, fill in the IP allowed to access in the target address, and click "Save" and "Apply" after the setting "Accept" is selected. As shown below.

WAVESHARE

Waveshare	
WS-431E	iles - test
This page allows you to	change advanced properties of the traffic rule entry, such as matched source and destination hosts.
> Status	
> Services Enal	le SDisable
Network Nat	ne test
VPN Restrict to address fam	ily IPv4 only
General Settings Proto	TCP+UDP V
Port Forwards Match ICMP by	
Traffic Rules	
Access Restrictions	ne O Any zone
> System	● lan: lan: 評 魚
> Logout	O wan: wan_wired: 🔊 wan_49: 🔊
Source MAC addre	ss any
	Only match incoming traffic from these MACs.
Source IP addre	ss any 🗸
	Only match incoming traffic from this IP or range.
Source p	any Only match incoming traffic originating from the given square part or part range on the client host
	ong maten moning dunic orginating nom ale grein source por en por range en ale enem nov
estination zo	Device (input)
	O Any zone (forward)
	O lan: lan: ﷺ ⊛
	wan: wan_wired: a wan_4g: a
Destination addr	
	Redirect matched incoming traffic to the specified internal host
Destination p	any
	Redirect matched incoming traffic to the given port on the internal host
Acti	on accept v
Back to Overview	Apply Save

Figure 50 Firewall IP white list 3

Next, set a rule that all communications are rejected. The source address is set to "any", the destination address is set to "any", and the action is selected to Reject. Pay attention to the order of the two rules. The allowed rules must come first and the rejected rules must come last. After the overall setting is completed, the following figure is shown:

Share awesome hard	E ware-					
WS-431E	Firewall - Traffic	Rules				
1. 1896 - 17. 1	Traffic rules define po	licies for packets traveling between different zones, for example	e to reject traffic between	certain ho	osts or to open WA	N ports on the
Status	router.					
Network	Traffic Rules					
VDN	Name	Protocol	Action	Enable	Sort	
 Firewall 	_					
General Settings	Allow- Ping	IPv4-ICMP with type <i>echo-request</i> From <i>any host</i> in <i>wan</i> To <i>any router IP</i> on <i>this device</i>	Accept input		• • Z Ec	dit 🛛 🗷 Delet
Port Forwards Traffic Rules	test	IPv4-TCPUDP From any host in lan	Accept forward		* * 🛛 🖾 Ec	dit 🛛 💌 Delet
Access Restrictions		io any nost in wan				
System	Open ports on router:					
Logout	Name	Protocol External port				
	New input rule	TCP+UDP 🗸 🖆 Add				
	New forward rule:					
	Name	Source zone Destination zone				
	New forward rule	Ian 🗸 wan 🗸 🖻 Add and edit				
	Source NAT					
	Name	Protocol			Action	Enable So
		This section contains no	values yet			
	New source NAT:					
	Name	Source zone Destination zone To source	ce IP To source port			
	New SNAT rule	Ian 🗸 wan 🗸 Pleas	se choc❤ Do not rewrite	3	Add and e	edit
		Security Security				

Figure 51 Firewall IP white list 4

3. Denies a subnet device access to a specified IP.

First add a forwarding rule.

-share awesome hardware	-					15
WS-431E	Firewall - Traffic	Rules				
> Status	Traffic rules define p router.	olicies for packets traveling between different zones, for example to	o reject traffic betwee	n certain h	osts or to open V	VAN ports on th
> Services						
> Network	Traffic Rules					
> VPN	Name	Protocol	Action	Enable	Sort	
 Firewall General Settings Port Forwards 	Allow- Ping	IPv4-ICMP with type echo-request From any host in wan To any router IP on this device	Accept input	0	••	Edit 🛛 💌 De
Traffic Rules	Open ports on router					
Access Restrictions	Name	Protocol External port				
> System						
	New forward rule: Name	Source zone Destination zone				
	Source NAT	Jah V Wali V Auu anu eur			Action	Fachia
	Name	Protocol	lucar unt		Action	Enable
		This section contains to ve	inter for			
	New source NAT:					
	Name	Source zone Destination zone To source	IP To source por	в		
	New SNAT rule	lan 💙 wan 💙 Please	choc~ Do not rewri	te	Add an	d edit
	New ShiAi rule	ian • wan • Please	unor Do not rewri		Aud all	a cultur

Figure 52 Firewall setting 1

- If TCP+UDP is selected as the protocol, the specified destination IP can be ping for the specified source IP, and the TCP/UDP connection cannot be established;
- If ICMP is selected as the protocol, the specified source IP cannot ping the specified target IP, and TCP/UDP connection can be established;
- If All protocols is selected, the specified destination IP cannot be ping for the specified source IP, and the TCP/UDP connection cannot be established.

< Note >

If you want to disable a port of a subnet device from accessing the specified target IP (or a port of the specified target IP), the protocol cannot choose All protocols or ICMP.

This example chooses TCP protocol.

WS-431E 4G Router

WAVESHARE



Figure 53 Firewall setting 2

Please keep the source area and destination area as the default, and select one of the source MAC and source IP. If both are filled in, please keep the MAC and IP corresponding, otherwise it will not take effect. The following example is to prohibit the 8899 port of a device with a source MAC of 48:95:07:AB:58:7B (if the port is left blank, it will be all ports by default) and to prohibit the establishment of a TCP connection with a destination address of 192.168.0.166 and a port of 9999 (if the port is left blank, it will be all ports by default). If both the source port and the destination port are left blank, it is forbidden to establish a TCP connection between a device with a source MAC of 48:95:07:AB:58:7B and a destination address of 192.168.0.166.

WĄ	WAVESHARE			
	WS-431E	Firewall - Traffic Rules	- test	
	Status	This page allows you to chan	ge advanced properties of the traffic rule entry, such as matched source and destination hosts.	
	Services	Enable	O Dicable	
	Network	Lindie		
	VPN	Name	test	
~	Firewall	Restrict to address family	IPv4 only 🗸	
	General Settings	Protocol	TCP 🗸	
	Port Forwards	Match ICMP type	any	
	Traffic Rules			
	Access Restrictions	Source zone	O Any zone	
	System		Ian: Ian: 📰 👷	
	Logout		O wan: wan_wired: 🔬 wan_4g: 🛃	
		Source MAC address Source IP address	08:BF:B8:00:7B:AC (DESK Only match incoming traffic from these MACs. any Only match incoming traffic from this IP or range.	
		Source port	8899 Only match incoming traffic originating from the given source port or port range on the client host	
		Destination zone	 Device (input) Any zone (forward) Ian: Ian: *** * Wvan: wan_wired: * wan_4g: * 	
		Destination address	192.168.0.166	
		Destination port	9999 Redirect matched incoming traffic to the given port on the internal host	
		Action	reject 🗸	
		Back to Overview	Apply Save	

Figure 54 Firewall setting 3

4. Disable Ping function

First, add a forwarding rule.

www.eshare awesome hardware-		
WS-431E	Firewall - Traffic Rules	
> Status > Services	Traffic rules define policies for packets traveling between different zones, for example to reject traffic between c router.	ertain hosts or to open WAN ports on the
> Network > VPN	Iraffic Kules Name Protocol Action I	Enable Sort
Firewall General Settings Doct Forewards	Allow- IPv4-ICMP with type ecto-request From any host in wan Accept input Ping To any router IP on this device	C * * Z Edit X Delete
Traffic Rules Access Restrictions	IPV4-TCP test From any host in Ian with source port 8899 and MAC 08:8F.88:00:76:AC Refuse forward To IP 192.168.0.166, port 9999 in wan	🛛 🔹 🏹 Edit 💌 Delete
> System	open ports on router:	
> Logout	Name Protocol External port	
	New input Ne TCP+UDP V 🗃 Add	
	New forward rule:	
	Name Source zone Destination zone	
	test Ian v wan v Add and edit	
	Source NAT	Antine Parkle Cost
	Name Protocol	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 Ian v wan v Please chorv Do not rewrite	🖻 Add and edit
	Apply Save	

Figure 55 Firewall setting 1

Protocol selects ICMP

WAVESHARE

W	WAVESHARE -share awesome hardware-			
	WS-431E	Firewall - Traffic Rules	- test	
>	Status	This page allows you to char	nge advanced properties of the traffic rule entry, such as matched source and destination hosts.	
>	Services	Enable	Ø Disable	
>	Network	Name	test	
2	VPN	Restrict to address family	IPv4 only	
~	Firewall	Protocol	TCMP	
	Port Forwards	Match ICMD hum		
[Traffic Rules Access Restrictions	Source zone	Any zone	
>	System		Ian: lan: # 10	
>	Logout		O wan: wan_wired: 🐊 wan_4g: 🐊	
		Source MAC address	any Only match incoming traffic from these MACs.	
		Source IP address	any Only match incoming traffic from this IP or range.	
		Source port	any Only match incoming traffic originating from the given source port or port range on the client host	

Figure 56 Firewall setting 2

The source zone and target zone can be defaulted.

Select all the source MAC and IP (according to whether all subnet devices are forbidden to ping according to the demand), and the source port number is not required to be filled in.

Select all the destination IP, and you can fill in whether ping to a certain IP is prohibited or ping detection to all IP is prohibited as required. The destination port should not be filled in.

<For example>

WS-431E 4G Router

In this example, it is forbidden to ping devices with subnet IP of 192.168.1.133 to destination address of 192.168.0.100.

www.eshare -share avesome hardware-	
WS-431E Firewall - Traffic	Rules - test
Status Services Services Network VPN Firewall General Settings Port Forwards Access Restrictions System Logout	o change advanced properties of the traffic rule entry, such as matched source and destination hosts. able Disable Test Test Test
Source MAC add	ress any • Image: Only match incoming traffic from these MACs. ress 192.168.1.133 Image: Only match incoming traffic from this IP or range.
Source Destination	port any ② Only match incoming traffic originating from the given source port or port range on the client host cone Device (input) ○ Any zone (forward) ○ lan: lan: ﷺ ○ wan: wan_wired: ﷺ wan_4g: ﷺ
Destination add Destination A Back to Overview	ress 192.168.0.100

Figure 57 Firewall setting 3

Click Apply to take effect immediately after the setting is completed. To temporarily disable the "Ping" function or other firewall policy settings, uncheck the box on the right and click Apply. To enable it again, check the box and click Apply.

WAVESHARE -share awesome hardware-					
WS-431E	Firewall - Traffic I	Rules			
> Status > Services	Traffic rules define pol router.	licies for packets traveling between different zones, for example to re	eject traffic between	certain hosts or to open WA	N ports on the
> Network > VPN	Iraffic Rules	Protocol	Action	Enable Sort	
 Firewall General Settings Post Forwards 	Allow- Ping	IPv4-ICMP with type echo-request From any host in wan To any router IP on this device	Accept input	• • • Z Ec	lit 🗴 Delete
Traffic Rules Access Restrictions	test	IPv4-ICMP From IP <i>192.168.1.133 in lan</i> To IP <i>192.168.0.100 on this device</i>	Refuse input	🛛 🔹 🔹 🖾 Ec	dit 💌 Delete
> System	Open ports on router:				
> Logout	Name	Protocol External port			
	New input rule	TCP+UDP 🗸 🛅 Add			
	New forward rule:				
	Name	Source zone Destination zone			
	New forward rule	Ian 🗸 wan 🗸 🖻 Add and edit			
	Source NAT				
	Name	Protocol		Action	Enable Sort
		This section contains no value	es yet		
	New source NAT:				
	Name	Source zone Destination zone To source IP	To source port		
	New SNAT rule	lan v wan v Please ch	Do not rewrite	Add and e	edit
		Apply Save			

Figure 58 Firewall setting 4

No ping function takes effect.

56(84) bytes of data. From 192.168.1.1: icmp_seq=1 Destination Port Unreachable From 192.168.1.1: icmp_seq=2 Destination Port Unreachable From 192.168.1.1: icmp_seq=3 Destination Port Unreachable From 192.168.1.1: icmp_seq=4 Destination Port Unreachable From 192.168.1.1: icmp_seq=5 Destination Port Unreachable

--- 192.168.0.100 ping statistics ---5 packets transmitted, 0 received, +5 errors, 100% packet Loss, time 4019ms

Figure 59 Firewall setting 5

VAVESHARE

4.6.4. ACCESS RESTRICTION

Access restriction implements access restriction on specified domain names, and supports setting of blacklist and whitelist of domain names. When the blacklist is selected, devices connected to routers cannot access blacklisted domain names, but other domain names can be accessed normally. When whitelist is selected, devices connected to routers cannot access other domain names except those set in whitelist, and multiple blacklists and whitelists can be set. This function is turned off by default.

1. Domain name blacklist

First, select the blacklist in the mode option, click Add to enter the name and correct domain name of the rule, and then click Save. The rule will take effect immediately, and devices connected to the router will not be able to access the domain name. If blacklist is selected without adding rules, the default blacklist is empty, that is, all domain names can be accessed. As shown in the figure, except Google, other domain names can be accessed normally.

WS-431E 4G Router

WAVESHARE

WĄ	WAVESHARE				
	WS-431E	Access Restrictions			
>	Status Services	Enter the domain name keys access fails, please revisit.	vord.Note: When setting the whiteli	ist, the PC may fail to visit the whitelist si	te for the first time due to browser reasons. If the
	Network	Configurations			
~	VPN Firewall	Method	Black List 🗸		
	General Settings Port Forwards	Name	Domain Name	e Enable	
	Access Restrictions	test	google.com		🗷 Delete
	System Logout	New Firewall Rule:			
			Name	Domain Name	🖀 Add
				Apply Save	

Figure 60 Domain name blacklist

2. Domain name whitelist

First, select the white list in the mode option, click Add to enter the name and correct domain name of the rule, and then click Save. The rule will take effect immediately, and the devices connected to the router will not be able to access other domain names except the domain name in the rule. If white list is selected without adding rules, the default white list is empty, that is, all domain names cannot be accessed. As shown in the figure, devices can access Google.

WS-431E 4G Router

WUAVESHARE

W	WAVESHARE -share awesome hardware-				
	WS-431E	Access Restrictions			
>	Status	Enter the domain name keyw access fails, please revisit.	rord.Note: When setting the whitelist, th	e PC may fail to visit the whitelist site for th	e first time due to browser reasons. If the
	Network	Configurations			
>	VPN	Method	White List 🗸		
~	Firewall General Settings				
	Port Forwards	Name	Domain Name	Enable	
Г	Traffic Rules	test	google.com	5	🗷 Delete
>	System				
	Logout	New Firewall Rule:			
		N	Name	Domain Name	Add
				Apply Save	

Figure 61 Domain name whitelist

4.7. VPN FUNCTION

VPN (Virtual Private Network) is divided into PPTP, L2TP, IPSec, OpenVPN, GRE, etc. Next, the principles of creating VPN by these protocols are introduced respectively.

PPTP: a point-to-point tunneling protocol, which uses a TCP (port 1723) connection to maintain the tunnel, uses the general routing encapsulation (GRE) technology to encapsulate the data into PPP data frames and transmit them through the tunnel, and encrypts or compresses the load data in the encapsulated PPP frames. The MPPE will encrypt the PPP frame through the encryption key generated by the MS-CHAP V2 authentication process.

L2TP: It is a Layer 2 tunneling protocol, similar to PPTP. At present, G806 supports tunnel password authentication, CHAP and other authentication methods, and the encryption method supports MPPE encryption and L2TP OVER IPSec pre-shared key encryption.

IPSec: Protocol is not a single protocol, it gives a set of architecture for application and network data security on IP layer, including network authentication protocols ESP, IKE and some algorithms for network authentication and encryption. Among them, ESP protocol is used to provide security services and IKE protocol is used for key exchange.

OpenVPN: Support certificate-based two-way authentication, that is, the client needs to authenticate the server, and the server needs to authenticate the client.

GRE: GRE (General Routing Encapsulation) protocol encapsulates data packets of some network layer protocols (such as IP and IPX) so that these encapsulated data packets can be

transmitted in another network layer protocol (such as IP). GRE adopts the technology of Tunnel, which is the third layer tunnel protocol of VPN.

Note: These protocols can build VPN, and you can choose a more suitable protocol according to your own needs.

4.7.1. PPTP CLIENT

Before application, you need to get the address, account, password and encryption method of VPN server, then enable PPTP client, and write other parameters in turn.

www.www.www.www.www.www.www.www.www.ww			
WS-431E	PPTP Setting		
> Status	PPTP Parameters		
> Services	PPTP Client	Enable O Dis	sable
> Network	Server Address	192.168.1.147	
VPN	Interface	auto	~
РРТР		Auto refers used defau	It route interface to connect
L2TP	User Name		
IPSec	Deserved		4
OpenV/PM	Password		19
Openvrn	Remote Subnet	192.168.1.10	
Certificate Management		eg. 152.100.10.0	
GRE	Remote Subnet Mask	255.255.255.0	
VPN Status		G (G (D))(D))(D))	
> Firewall	NAT		
> System	Enable MPPE Encryption		
> Logout	MTU	1450	
	0004-05-36	600~1450	
	Extra option		
		Append pppd options,	Non - professional,careful modification
	Enable Static Tunnel IP Address		
	Default Gateway	All traffic goes t	to VPN, except WAN protocol is PPPOE
	Enable Ping	Reconnect Whe	n Fails to Ping
WAVESHARE	L		Apply Save

Figure 62 Router adds VPN operation 1

< Description >

• Server address: fill in the IP or domain name of the VPN server to be connected;

- Interface: wan_4G, wan_wired and automatic can be selected according to different networking modes;
- User name/password: obtained from VPN server;
- Encryption method: MPPE encryption, no encryption, obtained from VPN server, and checked or unchecked according to the actual situation;
- MTU: set the MTU value of the channel, which is 1450 by default. This setting should correspond to the VPN server;
- NAT: This function is turned on by default. When the content needs to communicate with the outside, replace the internal address with the public address. If this item is disabled, the network address translation function cannot be realized;
- Peer subnet & mask: after filling in correctly, the subnet interworking function under VPN can be directly realized when NAT function is turned on;
- Enable static tunnel IP address: it is not enabled by default, and the server automatically allocates IP. You can fill in the static tunnel IP here;
- Extra opption: append the PPPD parameters, magic words, etc. No operation is required by default;
- Enable ping: a real-time VPN online detection and reconnection mechanism. Ping custom IP to ensure stable connection. Disabled by default.





4.7.2. L2TP CLIENT

L2TP is a Layer 2 tunneling protocol, similar to PPTP. At present, WS-431E supports tunnel password authentication, MPPE encryption and L2TP OVER IPSec pre-shared key encryption. Enter the VPN--L2TP interface, select Enable L2TP client, and fill in the parameters in turn.

	1 2TP Setting		
WS-431E	L2TP Setting		
	L2TP Parameters		
> Status	L2TP Client	Enable O Disable	
> Services	Server Address	192.168.1.148	
> Network	Interface	auto	•
✓ VPN	interface	 Auto refers used default route 	interface to connect
PPTP	User Name	admin	
L2TP			
IPSec	Password	*****	a.
OpenVPN	Tunnel Name		
Certificate Management	Tunnel Password		2
CDE		Oharacter(0-50)	
GRE	Enable IPsec		
VPN Status			
> Firewall	Remote Subnet	192.168.55.0 (a) eg: 192.168.10.0	
> System		255 255 255 0	
> Logout	Remote Subnet Mask	(2) eg: 255.255.255.0	
	NAT		
	MTU	1450	
		600~1450	
	Extra option		
		Append pppd options,Non - p	rofessional,careful modificati
	Enable Static Tunnel IP Address		
	Default Gateway	All traffic goes to VPN,	except WAN protocol is PPPC

Figure 64 L2TP Client Enable Settings Interface

< Description >

- L2TP supports tunnel password authentication, MPPE encryption and L2TP OVER IPSec encryption;
- Server address: fill in the IP or domain name of the VPN server to be connected;
- Interface: wan_4G, wan_wired and automatic can be selected according to different networking modes;
- User name/password: obtained from VPN server;
- Encryption/authentication: tunnel password authentication, MPPE encryption and IPSec encryption, which are obtained from VPN server and filled in correctly;

```
www.waveshare.com
```

- Enable static tunnel IP Address: it is not enabled by default, and the server automatically allocates IP. You can fill in the static tunnel IP here;
- Extra option: append the PPPD option, magic words, etc. No operation is required by default;
- NAT: This function is enabled by default. When the content needs to communicate with the
 outside, replace the internal address with the public address. If this item is disabled, the
 network address translation function cannot be realized;
- Peer subnet & mask: after filling in correctly, the subnet interworking function under VPN can be directly realized when NAT function is turned on;
- Enable ping: Real-time VPN online detection and reconnection mechanism. Not enabled by default. Checking this option indicates that the VPN will be reconnected if the ping fails.
- L2TP connection succeeded: after filling in the relevant parameters, save & apply, and enter VPN--VPN status to check the connection status.

4.7.3. IPSEC

WAVESHARE			
WS-431E	IPSec Connection Con	figuration	
	IPSec Parameters		
Status	IPSec	Enable O Dis	sable
Services	Interface	auto	~
> Network		Auto refers used defau	It route interface to connect
VPN	Peer Address	192.168.0.2	
РРТР		IP address or domain of the second	or %any,eg:10.10.1.88, eg:%any
12TP	Negotiation Method	Main	~
IDCas			
IPSec	Tunnel Type	Site To Site	~
OpenVPN	Local Subnet	192.168.1.0/24	
Certificate Management		() eg: 192.168.10.0/24	
GRE	Peer Subnat	192 168 55 0/24	
VPN Status	reel Subliet	@ eg: 192.168.20.0/24	
Firewall	IVE Encryption Algorithm	2055	u l
C	TRE Encryption Algorithm	SDES	
System	IKE Integrity Algorithm	MD5	~
> Logout	Diffie-Hellman Group	Group2(1024bits)	~
	IKE Life Time	28800	
		🥶 400-86400 seconas	
	Authentication Type	Pre-shared Key	~
	Pre-shared Key		2
		Character(1-50)	
	Local Identifier	@client	
		IP address or @domain	n,Character(0-29).eg:10.10.1.88, eg:@root
	Peer Identifier	@server	
	ree toentiner	IP address or @domain	n,Character(0-29).eg:10.10.1.88, eg:@root
WAVERUADE	ESP Encryption Algorithm	AES-128	v
WAVESHARE		linese e su	
	ESP Integrity Algorithm	SHA-1	v

Figure 65 Basic settings after enabling IPSec

< Description >

- Interface: wan_4G, wan_wired and automatic can be selected according to different networking modes;
- Peer address: it can be divided into VPN client and VPN server. Please fill in the IP/ domain name of the peer;
- Negotiation mode: main mode, aggressive mode (aggressive negotiation mode), with main mode as the default;
- Tunnel types: subnet to subnet, subnet to host, host to subnet, host to host. Select one according to the actual application mode;
- Local subnet: IPSec local subnet and subnet mask;
- Local identifier: the local identifier of the channel, which can be IP or FQDN. Pay attention to adding @ when defining the domain name; IKE Encryption Algorithm: The first stage

includes encryption mode, integrity scheme and DH exchange algorithm in IKE stage; IKE life time: set the life cycle of IKE, in seconds, the default is 28800;

- Authentication type: currently, the authentication mode of pre-shared key is supported;
- ESP encryption algorithm: the second stage includes the encryption mode and integrity scheme;
- ESP life time: set the ESP life cycle in seconds, and the default value is 3600;
- Perfect Forward Secrecy (PFS) for Session Key Encryption: There are four options: disabled, DH1, DH2 and DH5. This setting should be consistent between this end and the peer.
- Enable DPD Detection: What action should be taken when the DPD declares the peer as dead.
- DPD detection period: Set the time interval of connection detection (DPD);
- DPD timeout: Set the connection detection (DPD) timeout;
- DPD operation: Set the operation of connection detection. Including restart, dismantle, keep, none, restart by default;
- IPSec Connection Successful: After successfully establishing an IPSec connection with the remote endpoint, navigate to the VPN-to-VPN Status section to check the connection status.

4.7.4. OPENVPN

Enable OpenVPN to build VPN, and you can choose TUN (routing mode) or TAP (bridge mode) internally:

waveshare -share awesome hardware-							
WS-431E	OpenVPN Config	uration					
> Status	Enhanced OpenVPN d	esign allows 3 OpenVPI	N Clients and 1 OpenVPN	Server			
> Services	OpenVPN Configu	ration					
> Network	Name	Туре	Description	Enab	ble	Status	
VPN PPTP	CLIENT_1	CLIENT		OFF	*	Disconnected	Edit
L2TP	CLIENT_2	CLIENT		OFF	~	Disconnected	Z Edit
IPSec OpenVPN	CLIENT_3	CLIENT		OFF	~	Disconnected	Edit
Certificate Management	SERVER_1	SERVER		OFF	*	Disconnected	Z Edit
GRE VPN Status				Apply			
> Firewall				крриу			
> System						WA	Veshare
> Logout							

Figure 66 OpenVPN Enable Settings Interface

< Description >

- Device: TUN (routing mode) or TAP (bridge mode) can be selected;
- Channel protocol: UDP or TCP;
- Port: the listening port of OpenVPN client;
- VPN server address: IP/ domain name of OpenVPN server;
- Interface: wan_4G, wan_wired and automatic can be selected according to different networking modes;
- CA certificate: CA certificate common to both server and client;
- CRT public certificate: client certificate;
- Client private key: the key of the client;
- TLS authentication key: the authentication key of the secure transport layer;
- Encryption algorithms: None, Blowfish-128, DES-128, 3DES-192, AES-128, AES-192, AES-256.
 Hash algorithm: none, SHA1, SHA256, SHA512, MD5. Encryption and hash algorithms must be consistent with the VPN server.
- Use LZO Compression: Enable or disable the use of LZO compression for transmitting data.
- NAT Settings: This function is turned on by default. When the content needs to communicate with the outside, replace the internal address with the public address. If this item is turned off, the network address translation function cannot be realized;
- Enable Keepalive: enabled by default and configured as keepalive 10 120 by default. This setting should correspond to the VPN server;
- MTU setting: set the MTU value of the channel, which is 1500 by default. This setting should correspond to the VPN server; Enable Ping function: after setting the address of ping detection, vpn can be reconnected under abnormal disconnection;
- OpenVPN connection is successful: after successfully connecting with the VPN server, enter the VPN--VPN state to check the connection status.
- Note:
- Before the client connects with the server, CA certificate, client certificate, client key and TLS authentication key need to be provided by the server.

• After obtaining the certificate file, add different certificate contents to the configuration interface respectively.

-share awesome hardware-		
WS-431E	GRE Setting	
> Status	GRE Parameters	
> Services	GRE	● Enable ○ Disable
Notwork	Interface Name	gre1
Network		Inused,eg: gre1
VPN	Local WAN IP	192.168.0.151
PPTP		
L2TP	Peer WAN IP	192.168.0.10
IPSec	Peer Tunnel IP	10.10.10.1
OpenVPN	Deer Cubret	192 168 55 0/24
Certificate Management	Feel Subliet	@ eg:192.168.1.0/24
	I seel Tread ID	10 10 10 2
GRE	Local Tunnel IP	10.10.10.2
VPN Status	NAT	
> Firewall	TTI	255
> System	105	② 1~255
> Logout	Logout	1500
	ino	(a) 600~1500
	Enable Ping	Reconnect When Fails to Ping

Figure 67 GRE basic configuration

< Description >

- Peer WAN IP: The WAN IP address of the remote GRE peer.
- Local WAN IP: the addresses of local wan_wired and wan_4G, which are input differently according to the networking mode;
- Remote Tunnel IP: The GRE tunnel IP address of the remote endpoint.
- Peer Subnet: setting subnet mask can be expressed as follows: 255.255.255.0 can be written as IP/24, 255.255.255 can be written as IP/32.

For example: 172.16.10.1/24, corresponding to IP of 172.16.10.1 and subnet mask of 255.255.255.0;

- Local tunnel IP: IP address of local GRE tunnel;
- TTL: set the TTL of GRE channel, which is 255 by default;
- Set MTU: set the MTU of GRE channel, and the default is 1450.