

User Manual

----Apply to H12 Series Industrial 4G/3G Router

IOT SOLUTIONS



V3.0 http://www.homtecsm2m.com Jan., 2024



Copyright © Shenzhen Homtecs Technology Company Limited 2012 $\,\sim\,$ 2024

Without our written approval, anyone can't extract, copy whole or part of content of this file and can't spread out in any format.

Caution

Due to product updates or functional upgrading, we may renew the content of this file, and this file only for reference. All statement, information, suggestion etc. in this file does not compose any form of guarantee and we Homtecs reserves the right of final explanation.

Shenzhen Homtecs Technology Company Limited

Add: 2A, F5 Building, Zhongshanyuan Road, TCL International E-City, Xili, Nanshan District, China, 518000

Web: http://www.homtecsm2m.com

Email: info@homtecsm2m.com

Tel: 86-755-23903495



Contents

1 Hardware Installation	5
1.1 Panel	5
1.2 LED Status	6
1.3 How to Install	7
1.3.1 SIM/UIM card install	7
1.3.2 Ethernet Cable Connection	7
1.3.3 4G and Wi-Fi Antenna Plug	7
1.3.3 Power Supply	7
1.3.4 Review	7
2 Router Configuration	8
2.1 Local Configure	8
2.2 Status	9
2.3 Basic Network Settings	9
2.3.1 WAN Setting	10
2.3.2 Cellular Network Setting	10
2.3.3 LAN Setting	12
2.3.4 Dynamic DNS Setting	13
2.3.5 Routing Setting	14
2.4 WLAN Setting	15
2.4.1 Basic Setting	15
2.4.2 MultiSSID	16
2.4.3 Wireless Filter Setting	16
2.4.4 Advanced Wireless Setting	17
2.4.5 Wireless Survey	18
2.5 Advanced Network Setting	
2.5.1 Port Forwarding	
2.5.2 Port Redirecting	19
2.5.3 DMZ Setting	20
2.5.4 IP Passthrough Setting	20
2.5.5 Triggered Setting	21
2.5.6 Serial APP. Setting	22
2.5.7 UPnp/NAT-PMP Setting	23
2.5.8 Bandwidth Control Setting	23
2.5.9 VRRP Setting	24
2.5.10 Static DHCP Setting	24
2.6 Firewall	
2.6.1 IP/URL Filtering	25
2.6.2 Domain Filtering	26



2.7 VPN Tunnel	
2.7.1 GRE Setting	
2.7.2 OpenVPN Client Setting	27
2.7.3 VPN Client Setting	30
2.7.4 IPSec Setting	32
2.8 Administration	
2.8.1 Identification Setting	35
2.8.2 Time Setting	35
2.8.3 Admin Access Setting	36
2.8.4 Schedule Reboot Setting	
2.8.5 SNMP Setting	
2.8.6 M2M Access Setting (Apply to M2M Management Platform	37
2.8.8 System Log Setting	38
2.8.9 Firmware upgrade	39
2.9 System Reboot	
2.10 Debugging Setting	40
2.10.1 Logs Setting	40
2.10.2 Ping Setting	40
2.10.3 Trace Setting	41
2.11 "Reset" Button for Restore Factory Setting	41
2.12 Appendix (For advanced optional features only)	42
2.12.1 GPS Setting	42
2.12.2 Captive Portal Setting	44
2.12.3 VLAN	46
2.12.4 Schedule	49





This chapter is mainly for installation introduction, there would be some difference between the scheme and real object. But the difference won't have any influence to products performance.

1.1 Panel

Table 1-1	H12 Structure

Homtecs Tech.	H12 Series
Front panel	ALK UN LAN MET
Back panel	

Note:

There are some differences on Antenna interface and indicator light for the device with extended Wi-Fi, GPS features.

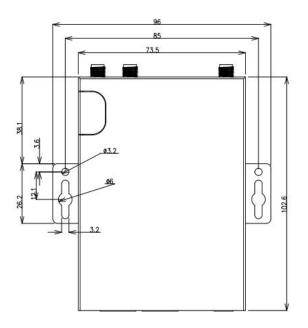
Table 1-2	H12 Interface
-----------	---------------

Port	Instruction	Remark
USIM	Plug type SIM Slot, support 1.8/3V/5V automatic detection.	
Main	LTE antenna, SMA connector, 50 Ω .	
Aux	LTE MIMO antenna	
GPS	GPS antenna, SMA connector, 50 Ω .	Optional
Wi-Fi	Wi-Fi dual-band antenna, SMA connector	Optional
LAN	10/100/1000Base-TX, MDI/MDIX self-adaption.	1
Reset	Reset button, (press on button at least 15 seconds)	



PWR	Power connector	7.5 ~ 32V DC
Serial port	RS-232/RS485.	

H12 Dimension



Note:

The equipment supports a variety of installation methods, such as embedded integration, desktop placement, wall installation and din-rail installation and other ways.

1.2 LED Status

Silk	Color	Status	Indication		
	Green	Solid light	4G online, CSQ: (15-31)		
	Yellow	Solid light	4G online, CSQ: (11-14)		
	Red	Solid light	4G online, CSQ: \leq 10		
	Green	1S light, 1S off, blinking	3G online, CSQ: (15-31)		
NET	Green	1S light, 1S off, blinking	3G online, CSQ: (11-14)		
	Red 1S light, 1S off, blinking		3G online, CSQ: ≤10		
	Green	0.25S light, 0.25S off, blinking	Sign up for the network		
	Red	0.5S light, 0.5S off, blinking	Read module and SIM status		
	Dark	30s off	Dial-up failed and reset the module		
WLAN	Green	Solid light	WLAN enabled, but no data communication.		
VVLAN	Green	Blinking quickly	Data is in transmitting		



	Green Off		WLAN disabled (firmware is without WLAN driver)
	Green	Solid light	Connected, but no data communication
LAN	Green	Blinking quickly	Data is in transmitting
	Green	Off	Disconnected
	Green	Solid light	Connected, but no data communication
WAN	Green	Blinking quickly	Data is in transmitting
	Green	Off	Disconnected

Table 1-4 H12 LED indicator Status

Note:

There are some differences in the LED indicator of the router with expanded Wi-Fi, GPS function and single module dual SIM.

1.3 How to Install

1.3.1 SIM/UIM card install

Please insert the SIM cards before configure the router.

Note:

Before connecting, please disconnect any power resource of router

1.3.2 Ethernet Cable Connection

Connect the router with a computer by an Ethernet cable for GUI configuration, or transit by a switch.

1.3.3 4G and Wi-Fi Antenna Plug

Connect the two magnetic 4G antennas to Main and Aux interfaces, and the one paddle shape Wi-Fi antenna interface.

Note:

Wi-Fi antenna only supports 2.4G.

1.3.3 Power Supply

Plug in power adaptor. Input range of voltage: +7.5~32VDC. (Extended models: 7.5~ 48VDC)

1.3.4 Review

After insert the SIM/UIM card and connect Ethernet cable and antenna, connect power supply adaptor or power cable.

CAUTION:

Please connect the antenna before power on, otherwise the signal maybe poor because of impedance mismatching.



Note:

Step 1 Check the antenna connection.Step 2 Check SIM/UIM card, confirm SIM/UIM card is available.Step 3 Power on the industrial Router

----END



H Series routers support GUI and CLI configuration. This chapter introduce GUI configuration via Ethernet port, if need CLI configuration guide, please contact our technical support department by email: info@homtecsm2m.com

2.1 Local Configure

The router supports to be configured by local Ethernet port, you could specify a static IP or set as DHCP. The default IP address is 192.168.1.1, subnet mask is 255.255.255.0, please refer to followings:

Step 1 Click "start > control panel", find "Network Connections" icon and double click it to enter, select "Local Area Connection" corresponding to the network card on this page. Refer to the figure below.



Figure 2-3 Network Connection

Step 2 Obtain a IP address automatically(DHCP) or set up IP address 192.168.1.xxx (XXX can be any number between $2\sim$ 254)

Step 3 Run an Internet Explorer and visit "http://192.168.1.1/", to enter identify page.

User should use the default user name and password(admin/admin) when log in for the first time



Connect to 19	2.168.8.1 ? 2
User name: Password:	🖸 admin 💌
	Remember my password

Figure 2-4 User Identify Interface

----END

2.2 Status

Check routers status after login router.

Status Overview	*		You h	aven't changed t	he default pas	sword for	this router. To change rout	er password <u>click here.</u>		
Traffic Stats.		System				~	WAN		٥	~
Device List		Router Name	Router				Connection Type	Cellular Network		
Basic Network	>	Hardware Version	C11-D20				Modem IMEI	868704042207165		
WLAN	>	Firmware Version	G5.0.1.5				Modem Status	Ready		
Advanced Network	>	Router Sn	1120G51	2004170001			Cellular ISP	"CHINA MOBILE"		
R Auvanced NetWork		Chipset	ARMv7 P	rocessor rev 5 (v7l)			Cellular Network	2G		
Firewall	>						USIM Status	Ready		
VPN Tunnel	>	Router Time	Tue, 19 N	1ay 2020 16:33:42 +08	00 Clock Sync.		CSQ	21		
		Uptime	00:01:43				IP Address	10.203.168.227		
R Administration	>	Memory Usage		/ 122.20 MB (31.61%)			Subnet Mask	255.255.255.248		
		NVRAM Usage		/ 64.00 KB (53.03%)			Gateway	10.203.168.228		
		iterioan osuge	0000110				DNS	211.136.17.107:53, 211.136.20.203:53		
							Connection Status	Connected		
							Connection Uptime	00:00:26		
		Ethernet Ports Statu	IS			~	Remaining Lease Time	01:59:19		
		WAN/LAN1	LAN2	LAN3	LAN4					
		1	1	1	-		Wireless (5 GHz)		\$	~
		Unplugged	Unplugged	Unplugged	100M Full		MAC Address	34:0A:A4:17:51:04		
							Wireless Mode	Access Point		
(i) More Info							Wireless Network Mode	Auto		

Note:

After login, router status will be show as below, then you should change the password according to the prompts.

You haven't changed the default password for this router. To change router password click here.

The UI will display" already changed login password successfully" after router reboot.

Already changed login password successfully.

2.3 Basic Network Settings



2.3.1 WAN Setting

Step 1 Basic Network>WAN to enter below interface

	Status	>	Already changed login password successfully.
	Basic Network	×	WAN / Internet
	Cellular LAN		Туре Онср •
	VLAN Schedule		MTU Default * 1500
	DDNS		
	Routing	>	Save-X Cancel X
-	Advanced Network	>	
1	Firewall	>	
0	VPN Tunnel	>	
黒	Administration	>	

Table 3-1 WAN Setting Instruction

Parameter	Instruction	Remark
Туре	Disable, DHCP, PPPoE, Static IP	
MTU	Default is 1500	

Step 2 After setting, please click "save" to finish, the device will reboot.

----End

2.3.2 Cellular Network Setting

Step 1 Basic Network-> Cellular, you can modify relevant parameter according to the application.

O Status	>		Already changed login password successfully.
 Basic Network WAN Cellular LAN 	*	Cellular Settings Enable Modem	•
VLAN Schedule DDNS Routing		Basic Settings SIM 1 Use PPP	
🗇 WLAN	>	ICMP Check	
Advanced Network	>	Cellular Traffic Check	
VPN Tunnel	>	CIMI Send to	
Administration	>	SMS Code	
		Operator Lock Save-/ Cancel ×	ec46001



Status	>		Already changed login password successfully.
Basic Network WAN Cellular LAN	×	Cellular Settings Enable Modem	
VLAN Schedule DDNS Routing		Basic Settings SIM 1 Mode	Auto •
🛜 WLAN	>	PIN Code	
Advanced Network	>	APN	3GNET
VPN Tunnel	>	User	CARD
R Administration	>	Password	
		Dial Number	199#
		Auth Type	Auto •
		Local IP Address	

Figure 3-2 Cellular Setting GUI

Parameter	Instruction
Use PPP	ECM dial-up as default. PPP optional.
ICMP Check	If enable ICMP check and setup a reachable IP address as
	destination IP, the router will reconnect/reboot once ICMP
	check failed.
Cellular Traffic Check	The router will reconnect/reboot once there's no Rx/Tx data.
CIMI Send to	Send CIMI to a defined IP and port by TCP protocol.
SMS Code	Remote control the router by SMS. Only the configured SMS
	code will work.
Operator Lock	Lock a specified operator for the router by MCC/MNC code.
SIM1 Mode	[Auto] The router will automatically connect to 3G/4G networks
	and give priority to 4G.
	【LTE】 Router will connect to 4G only.
	【 3G 】 Router will connect to 3G only.
Pin Code	Some SIM cards are locked with a Personal Identification Number
	(PIN) code in case they are lost or stolen.
APN	APN is provided by local ISP, usually in CDMA/EVDO networks
	APN does not need to be set.
User	SIM card user name is provided by ISP
Password	SIM card password is provided by ISP
Auth. Type	Auto/PAP/Chap/MS-Chap/MS-Chapv2 authentication optional.



SIM Local IPFix SIM IP. The feature is available if carrier can provide this service.Address

Note:

ICMC Check and Cellular Traffic Check are alternative.

【ICMP Check】

Enable ICMP, Router will automatically check whether the defined IP address is reachable per 60s. If the IP address is unreachable and ICMP check is timeout at the first time, it will check 2 times every 3 seconds. If the third time is still failed, the router will redial.

The ICMP Check IP is a public IP or company server IP address.

ICMP Check	
Check IP	8.8.8
Check IP (Optional)	4.4.4.4
Interval	60 (seconds)
Retries	3 (Times)
Fail Action	Reboot System 🔹

Cellular Traffic Check

[Check Mode] there are Rx(Receive), Tx(Transmission) and Rx/Tx check modes.

[Rx] Router will check the 3G/LTE cellular receiver traffic. If no receiver traffic within the defined check interval, the router will implement the specified action reconnect or reboot.

Cellular Traffic Check	~	
Check Mode	Rx	7
Check Interval	10	(minutes)Range: 1 ~ 1440
Fail Action	Cellular Re	connect 🔻

Step 2 After Setting, please click "save" icon.

----End

2.3.3 LAN Setting

Step 1 Basic Network>LAN to enter below interface



	Status	>		Already changed login password successfully.				
	Basic Network	×	LAN					~
	Cellular LAN		Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
-	VLAN		br0	192.168.2.1	255.255.255.0	~	192.168.2.2 - 51	1440
-	Schedule DDNS Routing		1	•				
(()-	WLAN	>	Add+					
R	Advanced Network	>						
1	Firewall	>	DNS					~
Ø	VPN Tunnel	>	Use Custom DNS					
黒	Administration	>						
			Save ✓ Cancel ×					

Figure 3-3 LAN Setting GUI

Table 3-2 LAN Setting Instruction

Table 5-2 LAN Settin	
Parameter	Instruction
IP Address	Router IP address, default IP is 192.168.1.1
Subnet Mask	Router subnet mask, default mask is 255.255.255.0
DHCP Server	Dynamic allocation IP service, after enable, it will show the
	IP address range and options of lease
IP Address Range	IP address range within LAN
Lease	The valid time
Use Internal DNS	If click this option, router will use 3G/4G network DNS which is
	assigned by 3G/4G network. If not click this option, router will
	use custom DNS
Primary DNS	Available as customer configured
Secondary DNS	Available as customer configured

Step 2 After setting, please click "save" to finish, the device will reboot.

----End

2.3.4 Dynamic DNS Setting

Step 1 Basic Network->DDNS to enter the DDNS setting page.



Basic Network Dynamic DNS	~
Cellular IP Address Use WAN IP Address 10.65.68.116 (recommended) LAN VLAN Auto refresh every 28 minutes (0 = Disabled)	
BONS Dynamic DNS1 WILAN Service Advanced Network Service	~
Dynamic DNS2	~

Figure 3-4 DDNS Setting GUI

Table 3-3 DDNS Setting Instruction

Parameter	Instruction
IP address	Default is standard DDNS protocol, for customized protocol, please contact Homtecs engineer. Usually, use default IP 0.0.0.0
Auto refresh every	Set the interval of the DDNS client obtains new IP, suggest 240s or above
Dynamic DNS1 Dynamic DNS2	Select the DDNS service provider that listed.

Step 2 Please Click "Save" to finish.

----End

2.3.5 Routing Setting

Step 1 Basic Network->Routing to enter the DDNS setting GUI.

Status	>			Already changed log	in password successfully.			
Basic Network WAN	*	Current Routing Table						~
Cellular		Destination	Gateway / Next Hop		Subnet Mask	Metric	Interface	
LAN VLAN		10.65.68.117			255.255.255.255	0	WAN	
Schedule		10.65.68.112			255.255.255.248	0	WAN	
DDNS Routing		192.168.2.0			255.255.255.0	0	LAN	
🗟 WLAN	>	127.0.0.0			255.0.0.0	0	lo	
Advanced Network	>	default	10.65.68.117		0.0.0.0	0	WAN	
G Firewall	>							
O VPN Tunnel	>	Static Routing Table						~
R Administration	>	Destination	Gateway	Subnet Mask	Metric	Interface	Description	
			0.0.0.0		0	LAN *		
		Add +						

Figure 3-5 Routing Setting

Table 3-4 Routing Setting Instruction



Parameter	Instruction
Destination	Router can reach the destination IP address.
Gateway	Next hop IP address which the router will reach
Subnet Mask	Subnet mask for destination IP address
Metric	Metrics are used to determine whether one particular route should be chosen over another.
Interface	Interface from router to gateway.
Description	Describe this routing name.

Step 2 Please Click "Save" to finish.

----End

2.4 WLAN Setting

It's mainly for router which support Wi-Fi, you can modify and configure WLAN parameter through Web GUI, below is the common setting

2.4.1 Basic Setting

Step 1 WLAN->Basic Setting to configure relative parameter

Status	>	Radio Mode	2.4G + 5G *
Basic Network	>		
🛜 WLAN	>	Wireless(2.4 GHz) Wireless(5 GHz)	
Basic Settings		Enable WLAN	
MultiSSID Wireless Survey		MAC Address	34:0A:A4:17:51:03
Advanced Network		Wireless Mode	Access Point 🔻
🐼 Firewall		Wireless Network Mode	Auto 🔻
VPN Tunnel Administration		SSID	router-wifi_175103
		Broadcast SSID	2
		Channel	7 - 2.442 GHz 🔻 Scan Q
		Channel Width	40 MHz •
		Control Sideband	Lower 🔻
		Maximum Clients	128 (range: 1 - 255)
(i) More Info		Security option	Disabled •

Figure 3-6 WLAN Basic Settings GUI



Table 3-5 Basic Setting Instruction

Parameter	Instruction
Enable wireless	Enable or Disable the Wireless
Wireless mode	Support AP, AP+WDS, Bridge, Client, WDS
Wireless Network protocol	Support Auto, IEEE 11b/g/n optional
SSID	The default is router, can be modified as per application.
Channel	The channel of wireless network, suggest keep the default
Channel Width	20MHZ and 40MHZ alternative
Security	Support various encryption method

Step 2 Please click "Save" to finish.

----End

2.4.2 MultiSSID

Step 1 WLAN > MultiSSID

nterface		Enabled	SSID		Mode	Bridge
th1 (wl0)		Yes	router-wifi_17510	3	Access Point	LAN (br0)
th2 (wl1)		Yes	router-wifi_175103	5G	Access Point	LAN (br0)
wl0.1	Ψ.	_		Access Point	v	LAN (br0)
Add+						

2.4.3 Wireless Filter Setting

Step 1 WLAN > Wireless Filter



Wireless Client Filter							
O Disable filter Permit only the following clients Block the following clients							
MAC Address	Description						
00:00:00:00:00:00							
Add+							
Save- Cancel ×							
Figure	3-7 Wireless Client Filter Setting GUI						

5

The Wireless Filter enable to set the permitted client or prohibit the specific client to connect the WiFi, However, this feature is invalid for wired connection application.

Parameter	Instruction
Disable Filter	Choose to disable
Permit on the	Only allow the listed MAC address to connect to router by wireless
following client	
Block the follow	Prevent the listed MAC address to connect to router by wireless
Client	

Table 3-6 "Wireless Client Filter" Setting Instruction

Step 2 Please click "Save" to finish

----End

2.4.4 Advanced Wireless Setting

Step 1 WLAN> Advanced Wireless to check or modify the relevant parameter

Wireless Advanced Settings(2.4 GHz)	
Afterburner	Auto •
AP Isolation	Disabled * •
Authentication Type	Auto *
Basic Rate	Default *
Beacon Interval	100 (range: 1 - 65535; Default: 100)
CTS Protection Mode	Auto 💌
Regulatory Mode	Disabled *
Country / Region	UNITED STATES •
Bluetooth Coexistence	Disabled * •
Distance / ACK Timing	0 meters (range: 0 - 999999; Default: 0)
DTIM Interval	3 (range: 1 - 255; Default: 1)
Fragmentation Threshold	2346 (range: 256 - 2346; Default: 2346)

Figure 3-8 Advanced Wireless Setting GUI



Step 2 Please click "Save" to finish.

----End

2.4.5 Wireless Survey

Step 1 WLAN> Wireless Survey to check survey.

Wireless Site Survey Last Seen ^ SSID BSSID RSSI Capabilities Noise Ouality Ch Rates infra wep 1.2.5.5.11 Thu 14:44:20 shortslot 32 Homtecs-WiFi 2.4G 00:90:4C:1E:20:2F -60 dBm -92 dBm 802.11n sgi20 sgi40 6,9,12,18,24,36,48,54 NEW (0m) 40 MHz infra wep 802.11n sgi20 Thu 14:44:20 NEW (0m) 155 6,12,24 Homtecs-WiFi_5G 00:90:4C:1E:20:30 -45 dBm -90 dBm 45 10 MHz 9,18,36,48,54 sgi40 infra wep shortslot Thu 14:44:20 NEW (0m) 1,2,5.5,11 Detran_Ltd_VD 00:9A:CD:99:E4:2C -88 dBm -92 dBm 4 6,9,12,18,24,36,48,54 40 MHz 802.11n sgi20 sgi40 infra wep Thu 14:44:20 1,2,5.5,11 6,9,12,18,24,36,48,54 . 4 shortslot 802.11n 00:94:CD:99:E4:2D -88 dBm -92 dBm NEW (0m) 40 MHz infra wep Thu 14:44:20 155 6.12.24 Detran_Ltd_VD_5G 00:9A:CD:99:E4:30 -76 dBm -90 dBm _____14 802.11n sgi20 NEW (0m) 10 MHz 9,18,36,48,54 sgi40 infra wep Thu 14:44:20 NEW (0m) 155 10 MHz RTL8186-default 00:9A:CD:F9:E4:30 -75 dBm -90 dBm _____15 6,9,12,18,24,36,48,54 shortslot 802.11n

Figure 3-9 Wireless Survey Setting GUI

----End

2.5 Advanced Network Setting

2.5.1 Port Forwarding

Step 1 Advanced Network > Port Forwarding to enter the GUI, you may modify the router name, Host name and Domain name according to the application requirement.

Status	>				Already change	l login password succ	cessfully.	
Basic Network	>	PortFor	warding					
WLAN		On	Proto	Src Address	Ext Ports	Int Port	Int Address	Description 🔨
Port Forwarding		×	UDP		1000,2000		192.168.1.2	ex: 1000 and 2000
Port Redirecting		×	Both		1000-2000,3000		192.168.1.2	ex: 1000 to 2000, and 3000
- DMZ IP Passthrough		×	Both	1.1.1.0/24	1000-2000		192.168.1.2	ex: 1000 to 2000, restricted
Triggered		×	TCP		1000	2000	192.168.1.2	ex: different internal port
Captive Portal			TCP	Ŧ				
UPnP/NAT-PMP		Add +						
Bandwidth Limiter								
VRRP Static DHCP		• Ext	Ports - The ports to	Forward only if from this address. e be forwarded, as seen from the WA	N. ex: "2345", "200,300", "200-3	00,400".		
Firewall	>			ation address inside the LAN. If i	plank, the destination port is th	e same as <i>Ext Ports</i> . Only one	e port per entry is supported when	n forwarding to a different internal port
VPN Tunnel	>							
Administration	>	Save✓	Cancel ×					

Figure 3-10 Port Forwarding GUI



Table 3-7 "Port Forwarding" Instruction

Parameter	Instruction			
Protocol	Support UDP, TCP, both UDP and TCP			
Src. Address	Source IP address. Forward only if from this address.			
Ext. Ports	External ports. The ports to be forwarded, as seen from the WAN.			
Int. Port	Internal port. The destination port inside the LAN. If blank, the destination port is the same as Ext Ports. Only one port per entry is supported when forwarding to a different internal port.			
Int. Address	Internal Address. The destination address inside the LAN.			
Description	Remark the rule			

Step 2 Please click "Save" to finish.

----End

2.5.2 Port Redirecting

Step 1 Advanced Network > Port Redirecting to enter the GUI, you may modify the router name, Host name and Domain name according to the application requirement.

0	Status	>		Already changed login password successfully.				
Q	Basic Network	>	PortRed	PortRedirecting				
((*	WLAN	>		Proto	1.4.04	Dst Address	Col David	Developing
	Advanced Network	*	On	Proto	Int Port	Dst Address	Ext Port	Description
	Port Forwarding		<u>~</u>	TCP	Ψ.			
	Port Redirecting DMZ		Add+					
	IP Passthrough		_	-				
10	Triggered							
	Captive Portal		Save✓	Cancel×				
	Serial App.		Savev	Cancerx				

Figure 3-11 Port Forwarding GUI

Parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Int Port	Internal port.
Dst. Address	The redirecting IP address.

Table 3-8 "Port Redirecting" Instruction



Ext. Ports	External port for redirection.
Description	Remark the rule

Step 2 Please click "Save" to finish.

----End

2.5.3 DMZ Setting

Step 1 Advanced Network> DMZ to check or modify the relevant parameter

0	Status	>		Already changed login password successfully.				
Ø	Basic Network	>						
(0	WLAN	>	DMZ					
	Advanced Network	~	Enable DMZ					
ŀ	Port Forwarding		Internel Address	192.168.2.0				
-	Port Redirecting							
	DMZ		Source Address	(optional; ec: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" or "me.example.com")				
	IP Passthrough		Restriction					
1	Triggered							
-	Captive Portal		Leave CLI Remote Access	 (Redirect remote access ports for CLI to router) 				
1	Serial App.							
-	UPnP/NAT-PMP		Leave WEB Remote Access	(Redirect remote access ports for HTTP(s) to router)				
t	Bandwidth Limiter							
+	VRRP							
1	Static DHCP		Save ✓ Cancel ×					

Figure 3-12 DMZ GUI

Table 3-9 "DMZ" Instruction

Parameter	Instruction
Destination	The destination address inside the LAN.
Address	
Source	If no IP address inside, it will allow all IP address to access.
Address	If define IP address, it will just allow the defined IP address
Restriction	to access.
Leave Remote	
Access	

Step 2 Please click "Save" to finish.

----End

2.5.4 IP Passthrough Setting

Step 1 Advanced Network> IP Passthrough to check or modify the relevant parameter



0	Status	>		Already changed login password successfully.
Ø	Basic Network	>		
((1+	WLAN	>	IP Passthrough	
	Advanced Network		Enabled	
	Port Forwarding		MAC Address	
	Port Redirecting DMZ		Gateway	
	IP Passthrough			
	Triggered			
	Captive Portal	1	Save ✓ Cancel ×	
	Serial App.	1		

Figure 3-13 IP Passthrough GUI

Parameter	Instruction		
Enable	Enable IP Passthrough		
MAC Address	Enable DHCP of device. Configure device Mac.		
	Device will be assigned SIM IP.		
Gateway	If router connect to multiple devices, input other devices		
	gateway. The device might access to router GUI.		

Table 3-10 "IP Passthrough" Instruction

Step 2 Please click "Save" to finish.

----End

2.5.5 Triggered Setting

Step 1 Advanced Network> Triggered to check or modify the relevant parameter.

Status	>	Already changed login password successfully.					
Basic Network	>						
🗇 WLAN	>	Triggered Port Forwarding					
Advanced Network	~	On Protocol Trigger Ports Forwarded Ports Description	1 ^				
Port Forwarding		× TCP 3000-4000 5000-6000 ex: open 50	100-6000 if 3000-4000				
Port Redirecting		тср т					
DMZ							
IP Passthrough		Add+					
Captive Portal		- (200.200)					
Serial App.		(200-300). These ports are automatically closed after a few minutes of inactivity.					
UPnP/NAT-PMP Bandwidth Limiter							
···· VRRP		Save- Cancel ×					

Figure 3-14 Triggered GUI

Table 3-11 "Tri	ggered" Instruction
-----------------	---------------------

Parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Triggered Ports	Trigger Ports are the initial LAN to WAN "trigger".



Transferred	Forwarded Ports are the WAN to LAN ports that are			
Ports	opened if the "trigger" is activated.			
Note	Port triggering opens an incoming port when your			
	computer is using a specified outgoing port for specific			
	traffic.			

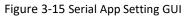
Step 2 Please click "Save" to finish.

----End

2.5.6 Serial APP. Setting

Step 1 Advanced Network> Serial APP to check or modify the relevant parameter.

♥ Status	Serial to TCP/IP	
Basic Network	IPoC Mode	Serial *
🗇 WLAN		
😭 Advanced Network 🛛 👻	Serial to TCP/IPMode	Client
Port Forwarding	Server IP/Port	8.8.8.8 : 40002
Port Redirecting		
··· IP Passthrough	Socket Type	TCP *
Triggered	Socket Timeout	500 (milliseconds)
Captive Portal Serial App.	Serial Timeout	500 (milliseconds)
GPS	Sendi Hineoda	
UPnP/NAT-PMP	Packet Payload	1024 (bytes)
Bandwidth Limiter VRRP		
Static DHCP	Heart-Beat Content	Homtecs2012
🗑 Firewall >	Heart-Beat Interval	2. (seconds)
VPN Tunnel	Port Type	R5485/R5232 •
界 Administration >		
	Cache Enable	
(i) More Info		



Parameter	Instruction
Serial to TC/IP mode	Support Disable, Server and Client mode. Such as Client.
Server IP/Port	IP address and domain name are acceptable for Server IP
Socket Type	Support TCP/UDP protocol
Socket Timeout	Router will wait the setting time to transmit data to serial port.
Serial Timeout	Serial Timeout is the waiting time for transmitting the data package that is less the Packet payload. If the last package equals to the Packet payload, Serial port will transmit it immediately. The default setting is 500ms.
Packet payload	Packet payload is the maximum transmission length for serial port data packet. The default setting is 1024bytes.



Heart-beat	Send heart beat to the defined server to keep router online.			
Content	Meantime, it's convenient to monitor router from server.			
Heart beat	Heart beat interval time			
Interval				
Baud Rate	115200 as default			
Parity Bit	None as default			
Data Bit	8bit as default			
Stop Bit	1bit as default			

Step 2 Please click "Save" to finish.

----End

2.5.7 UPnp/NAT-PMP Setting

Step 1 Advanced Network> Upnp/NAT-PMP to check or modify the relevant parameter.

Status	>	Forwarded Ports					
Basic Network	>	Ext Ports	Int Port		Internal Address	Protocol	Description
WLAN	>						Delete All× C Refresh
Advanced Network	•						Delete All & O Reliesh
Port Forwarding Port Redirecting		Settings					~
··· DMZ ··· IP Passthrough		Enable UPnP	~				
Triggered Captive Portal		Enable NAT-PMP	<u></u>				
Serial App. GPS		Inactive Rules Cleaning	<u>~</u>				
···· UPnP/NAT-PMP ···· Bandwidth Limiter		Cleaning Interval	60	0	seconds		
VRRP Static DHCP		Cleaning Threshold	20		redirections		
🐼 Firewall	*	Secure Mode	Z	when ena	bled, UPnP clients are allowed to add mappings only to their IP)		
VPN Tunnel Administration	> >	Show In My Network Places					
③ More Info		Save ✓ Cancel ×					

Figure 3-16 UPnp/NAT-PMP Setting GUI

Step 2 Please click "Save" to finish.

2.5.8 Bandwidth Control Setting

Step 1 Advanced Network> Bandwidth Control to check or modify the relevant parameter.



0	Status	>			Already change	ed login password succe	ssfully.		
	Basic Network	>	Bandwidth Control						
	WLAN Advanced Network	•	Enable Control						
	Port Forwarding								
	Port Redirecting DMZ		IP IP Range MAC Address	C	DLRate	DLCeil	ULRate	ULCeil	Priority
-	IP Passthrough Triggered								Normal 🔻
	Captive Portal		Add+						
	Serial App. UPnP/NAT-PMP								
	Bandwidth Limiter		Default Class						
	Static DHCP		Enable Default Class						
1	Firewall	>							
	VPN Tunnel	>	Save ✓ Cancel ×						
黒	Administration	>							

Figure 3-17 Bandwidth Control Setting GUI

Step 2 Please click "Save" to finish.

----End

2.5.9 VRRP Setting

Step 1 Advanced Network> Static DHCP to check or modify the relevant parameter.

	Status	>		Already changed login password successfully.
	Basic Network	>	VRRP	
	Advanced Network	•	Enable VRRP	
	Port Forwarding Port Redirecting		Mode	backup *
-	DMZ IP Passthrough		Virtual IP	192.168.1.3
-	Triggered		Virtual Router ID	
-	Captive Portal Serial App.		Priority	100
-	UPnP/NAT-PMP Bandwidth Limiter		Authentication	
	VRRP Static DHCP		Script Type	Default *
	Firewall	>	Check Interval	3
	VPN Tunnel Administration	>	Weight	10
	 More Info 	1	Save Cancel ×	

Figure 3-18 VRRP Setting GUI

Step 2 Please click "Save" to finish.

----End

2.5.10 Static DHCP Setting

Step 1 Advanced Network> Static DHCP to check or modify the relevant parameter.



© Status	>	Already changed login password successfully.				
Basic Network	>	Static DHCP				
🗟 WLAN	>	Static DHCP				
Advanced Network	~	MAC Address	IP Address	Hostname 🔨	Description	
Port Forwarding		00:00:00:00:00	192.168.2.2			
- Port Redirecting		00:00:00:00:00:00	192.106.2.2			
DMZ IP Passthrough		Add +				
Triggered						
Captive Portal						
Serial App.		Save ✓ Cancel ×				
UPnP/NAT-PMP						



Step 2 Please click "Save" to finish.

----End

2.6 Firewall

2.6.1 IP/URL Filtering

Step 1 Firewall> IP/URL Filtering to check or modify the relevant parameter.

Status	>	IP/MAC/Port Filte	ring					
Basic Network	>	On Src MAC	Src IP	Dst IP	Protocol Src Po	ort	Dst Port	Policy Description
🗟 WLAN	>				NONE *			Accept 🔻
Advanced Network	>							
G Firewall		Add +						
IP/URL Filtering Domain Filtering		Key Word Filterin	g					
O VPN Tunnel	>	On	Key Word			Description		
R Administration	>							
		Add +						
		URL Filtering						
		On	URL			Description		
		Add+						
 More Info 		Access Filtering						

Parameter	Instruction
IP/MAC/Port	Support IP address, MAC address and port filter.
Filtering	Accept/Drop options for filter policy.
Key Word	Support key word filter.
Filtering	
URL Filtering	Support URL filter.
Access Filtering	Support Access Filter.

Step 2 Please click "Save" to finish.



---End

2.6.2 Domain Filtering

Step 1 Firewall> Domain Filtering to check or modify the relevant parameter

© Status	>	Already changed login password successfully.
Basic Network	>	Domain Filtering
WLAN	>	
Advanced Network	>	On
🔞 Firewall		Default Policy White List *
IP/URL Filtering Domain Filtering		On Domain Description
C VPN Tunnel	>	
R Administration	>	Add +
		Save ✓ Cancel X

Figure 3-20 Domain Filtering Setting GUI

Table 3-14 "Domain Filtering" Instruction

Parameter	Instruction
Default Policy	Support black list and white list
Local IP Address	Local IP address for LAN.
Domain	Support Domain filter.

Step 2 Please click "Save" to finish.

----End

2.7 VPN Tunnel

2.7.1 GRE Setting

Step 1 VPN Tunnel> GRE to check or modify the relevant parameter.



GRE Tunnel							~
On Idx ^	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive Interva	al Retries	Description	
Add+							
RE Route							~
On	Tunnel Index 🔨	Destination Add	dress		Description		
~	1	Ŧ					
Add+							

Figure 3-21 GRE Setting GUI

Table 3-15 "GRE" Instruction

Parameter	Instruction					
IDE	GRE tunnel number					
Tunnel Address	GRE Tunnel local IP address which is a virtual IP address.					
Tunnel Source	Router's 3G/WAN IP address.					
Tunnel Destination	GRE Remote IP address. Usually, it's a public IP address					
Keep alive	GRE tunnel keep alive to keep GRE tunnel connection.					
Parameter	Instruction					
Interval	Keep alive interval time.					
Retries	Keep alive retry times. After retry times, GRE tunnel will be re-established.					
Description						

Step 2 Please click "Save" to finish.

----End

2.7.2 OpenVPN Client Setting

Step 1 VPN Tunnel> OpenVPN Client to check or modify the relevant parameter.



OpenVPN Client	
Client 1 Client 2	
Basic Advanced Keys Status	
VPN Client #1 (Stopped)	×
Start with WAN	
Interface Type	TUN •
Protocol	UDP *
Server Address	1194
Firewall	Automatic *
Authorization Mode	TLS Y
Username/Password Authentication	
HMAC authorization	Disabled *
Create NAT on tunnel	

Figure 3-22 OpenVPN Setting GUI

Table 3-16 "OpenVPN" Instruction

Parameter	Instruction
Start with WAN	Enable the Openvpn feature for 4G/3G/WAN port.
Interface Type	Tap and Tun type are optional.
	Tap is for bridge mode and Tunnel is for routing mode
Protocol	UDP and TCP optional.
Server Address	The Openvpn server public IP address and port.
Parameter	Instruction
Firewall	Auto, External only and Custom are optional
Authorization	TLS, Static key and Custom are optional.
Mode	
User	As the configuration requested.
name/Password	
Authentication	
НМАС	As the configuration requested.
authorization	
Create NAT on	Configure NAT in Openvpn tunnel.
tunnel	



OpenVPN C	lient
-----------	-------

Client 1 Client 2		
Basic Advanced Keys Status		
VPN Client #1 (Stopped)		Þ
Poll Interval	0 (in minutes, 0 to disable)	
Redirect Internet traffic		
Accept DNS configuration	Disabled 💌	
Encryption cipher	Use Default •	
Compression	Adaptive *	
TLS Renegotiation Time	-1 (in seconds, -1 for default)	
Connection retry	30 (in seconds; -1 for infinite)	
Verify server certificate (tls-remote)		

Parameter	Instruction
Poll Interval	Openvpn client check router's status as interval time.
Redirect Internet Traffic	Configure Openvpn as default routing.
Access DNS	As the configuration requested.
Encryption	As the configuration requested.
Compression	As the configuration requested.
TLS Renegotiation Time	TLS negotiation time1 as default for 60s.
Connection Retry Time	OpenVPN retry to connection interval.
Parameter	Instruction
Verify server certificate	As the configuration requested.
Custom Configuration	As the configuration requested.



OpenVPN	Client
---------	--------

Client 1 Client 2		
Basic Advanced Keys Status		
VPN Client #1 (Stopped)		Þ
For help generating keys, refer to the OpenVPN HC	жто.	
Certificate Authority		
Client Certificate		
		//
Client Key		

Start Now

Parameter	Instruction
Certificate Authority	Keep certificate as the same as server
Client Certificate	Keep client certificate as the same as server
Client Key	Keep client key as the same as server

OpenVPN Client	
Client 1 Client 2	
Basic Advanced Keys Status	
VPN Client #1 (Stopped)	•
Client is not running or status could not be read.	
	Refresh Status
Start Now	
Save ∽ Cancel ×	

Step 2 Please click "Save" to check OpenVPN status and data statistics.

----End

.

2.7.3 VPN Client Setting

Step 1 VPN Tunnel> VPN Client to check or modify the relevant parameter



TP/PPTP Basi	c							
n	Protocol 🔨	Name	Server	Username Pa	assword Firew	all Default Rout	e Local IP	
<	L2TP *							
Add+								
TP Advanced								
i.	Name 🔨	Accept DNS	мти	MRU	Tunnel Auth	Tunnel Password	Custom Options	
·		NO	¥					
Add+								
P Advanced								
	Name ^	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options	

Table 3-17 "PPTP/L2TP Basic" Instruction

Parameter	Instruction
On	VPN enable
Protocol	VPN Mode for PPTP and L2TP
Name	VPN Tunnel name
Server Address	VPN Server IP address
User name	As the configuration requested
Password	As the configuration requested
Firewall	Firewall For VPN Tunnel
Local IP	Defined Local IP address for tunnel

Table 3-18 "L2TP Advanced" Instruction

Parameter	Instruction
On	L2TP Advanced enable
Name	L2TP Tunnel name
Accept DNS	As the configuration requested.
MTU	MTU is 1450bytes as default
MRU	MRU is 1450bytes as default
Tunnel Auth.	L2TP authentication Optional as the configuration requested.
Tunnel Password	As the configuration requested.
Custom Options	As the configuration requested.

Table 3-19 "PPTP Advanced" Instruction

Parameter	Instruction
On	PPTP Advanced enable
Name	PPTP Tunnel name



Accept DNS	As the configuration requested
MTU	MTU is 1450bytes as default
MRU	MRU is 1450bytes as default
MPPE	As the configuration requested
MPPE Stateful	As the configuration requested
Customs	As the configuration requested

Table 3-20 "SCHEDULE" Instruction

Parameter	Instruction
On	VPN SCHEDULE feature enable
Name1	VPN tunnel name
Name2	VPN tunnel name
Policy	Support VPN tunnel backup and failover modes optional
Description	As the configuration requested

Step 2 Please click "Save" to finish.

---End

2.7.4 IPSec Setting

Step 1 IPSec> Group Setup to check or modify the relevant parameter.

IPSec					
IPSec 1 IPSec 2 Schedule	IPSec 1 IPSec 2 Schedule				
Group Setup Basic Setup Advanced Setu	2				
Enable IPSec					
IPSec Extensions	Normal 💌				
Local Security Gateway Interface	3G Cellular 💌				
Local Security Group Subnet/Netmask	192.168.1.0/24	ex 192.168.1.0/24			
Local Security Firewalling					
Remote Security Gateway IP/Domain					
Remote Security Group Subnet/Netmask	10.0.0/24	ex 192.168.88.0/24			
Remote Security Firewalling					

Save ✓ Cancel ×

Table 3-21 "IPSec Group Setup" Instruction

Parameter	Instruction
IPSec	Support Standard IPSec, GRE over IPSec, L2TP over IPSec
Extensions	
Local Security	Defined the IPSec security interface
Interface	



Local	IPSec local subnet and mask
Subnet/Mask	
Local Firewall	Forwarding-firewalling for Local subnet
Remote	IPsec peer IP address/domain name
IP/Domain	
Remote	IPSec remote subnet and mask
Subnet/Mask	
Remote	Forwarding-firewalling for Remote subnet
Firewall	

Step 2 IPSec >Basic Setup to check or modify the relevant parameter

IPSec	
IPSec 1 IPSec 2 Schedule	
Group Setup Basic Setup Adv	anced Setup
Keying Mode	IKE with Preshared Key *
Phase 1 DH Group	Group 2 - modp1024 💌
Phase 1 Encryption	3DES (168-bit) •
Phase 1 Authentication	MD5 HMAC (96-bit)
Phase 1 SA Life Time	28800 seconds
Phase 2 DH Group	Group 2 - modp1024 💌
Phase 2 Encryption	3DES (168-bit) *
Phase 2 Authentication	MD5 HMAC (96-bit)
Phase 2 SA Life Time	3600 seconds

Table 3-22 "IPSec Basic Setup" Instruction

Parameter	Instruction
Keying Mode	IKE preshared key
Phase 1 DH	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec
Group	setting.
Phase 1	Support 3DES, AES-128, AES-192, AES-256
Encryption	
Phase 1	Support HASH MD5 and SHA
Authentication	
Phase 1 SA	IPSec Phase 1 SA lifetime
Life Time	
Phase 2 DH	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec
Group	setting.



Phase 2	Support 3DES, AES-128, AES-192, AES-256
Encryption	
Phase 2	Support HASH MD5 and SHA
Authentication	
Phase 2 SA	IPSec Phase 2 SA lifetime
Life Time	
Preshared Key	Preshared Key

Step 3 IPSec >Advanced Setup to check or modify the relevant parameter

IPSec		
IPSec 1 IPSec 2 Schedule		
Group Setup Basic Setup Advanced Setup	-	
Aggressive Mode	1	
Compress(IP Payload Compression)	1	
Dead Peer Detection(DPD)		
ICMP Check	1	
IPSec Custom Options 1		
IPSec Custom Options 2		
IPSec Custom Options 3		
IPSec Custom Options 4		

Table 3-23 "IPSec Advanced Setup" Instruction

Parameter	Instruction
Aggressive	Default for main mode
Mode	
ID Payload	Enable ID Payload compress
Compress	
DPD	To enable DPD service
ICMP	ICMP Check for IPSec tunnel
IPSec Custom Options	IPSec advanced setting such as left/right ID.

Step 4 Please click "Save" to finish.

---End

2.8 Administration



2.8.1 Identification Setting

Step 1 Please click "Administrator> Identification" to enter the GUI, you may modify the router name, Host name and Domain name according to self-requirement.

Statu	15	>	You have	en't changed the default password for this router. To change router password click here,
Basic	: Network	>	PRINT WAR AND AN	
🛜 WLAI	N	>	Router Identification	
😭 Adva	anced Network	>	Router Name	Router
🐼 Firew	vall	>	Hostname	Router
D VPN	Tunnel	>	Domain Name	
📕 Admi	inistration	~		
- Iden Time	ntification		Save ✓ Cancel ×	
Adm	nin Access			
Sche	eduled Reboot			
SNM				
	age Settings			
	M Settings			
	00 Setting			
	figuration			
- Logg	ging			
Upgi	rade			

Figure 3-23 Router Identification GUI

Table 3-24 "Router Identification" Instruction

Parameter	Instruction
Router name	Default is router, can be set maximum 32 character
Host name	Default is router, can be set maximum 32 character
Domain name	Default is empty, support maximum up to 32 characters, it is the domain of WAN, no need to configure for most application.

Step 2 Please click "Save" to finish

---End

2.8.2 Time Setting

Step 1 Please click "Administrator> time" to check or modify the relevant parameter.



Status	>	You ha	ven't changed the default password for this router. To change router password_click here,
Basic Network	>	Time	
🛜 WLAN	>		
Advanced Network	>	Router Time	Thu, 21 May 2020 17:05:09 +0800 Clock Sync.
B Firewall	>		
D VPN Tunnel	>	Time Zone	UTC+08:00 China, Hong Kong, Western Australia, Singapore, Taiwan 🔻
R Administration	~	Auto Daylight Savings Time	
Identification			
Time Admin Access		Auto Update Time	Every 4 Hours 🔻
Scheduled Reboot		Trigger Connect On Demand	
SNMP			Asia 🔻
Storage Settings M2M Settings		NTP Time Server	ASI8 *
DI/DO Setting			Oasia pool ntp.org, 1 asia.pool ntp.org 2 asia.pool ntp.org
Configuration			
Logging			
· Upgrade		Save ✓ Cancel ×	

Figure 3-24 System Configuration GUI

CAUTION:

If the device is online but time update is fail, please try other NTP Time Server.

Step 2 Please click "Save" to finish.

----End

2.8.3 Admin Access Setting

Step 1 Please click "Administrator>Admin Access" to check and modify relevant parameter. In this page, you can configure the basic web parameter, make it more convenient for usage. Please note the "password" is the router system account password.

Status		>		You haven't changed the default password for this router. To change router password click here,	
Basic Netwo	ork	>	WebAccess		~
🛜 WLAN		>	web the	GUI3.0 ¥	
Advanced N	Network	>	Web Style		
🐼 Firewall		>	Local Access	нттр	
VPN Tunnel	el	>	HTTP Access Port	80	
R Administrat		*	Remote Access	Disabled *	
Time	cess		Allow Wireless Access		
Scheduled SNMP	Reboot		Block WAN Ping		
Storage Se M2M Settin			SSH Enable at Startup		
DI/DO Sett	-		Allow Telnet Remote Access		
Logging					
I Upgrade			Password		~
(i) Mo	ore Info		Password (admin)		

Figure 3-25 Admin Setting GUI

Step 2 Please click "Save" finish the setting ----End

2.8.4 Schedule Reboot Setting

Step 1 Please click "Administrator>Schedule Reboot" to check and modify relevant



parameter.				
© Status	>		You haven't changed the default password for this router. To change router password click here.	
Basic Network	>	Scheduled Reboot		v
🛜 WLAN	>			
Advanced Network	>	Enabled		
G Firewall	>	Time	* MAX OD-1	
VPN Tunnel	>	Days	Sun Sun Tue Wed Thu Fri Sat Everyday	
R Administration	~			
Identification		Save ✓ Cancel ×		

Figure 3-26 Scheduler Reboot Setting GUI

Step 2 Please click "Save" to finish the setting

----End

2.8.5 SNMP Setting

Step 1 Please click "Administrator>SNMP" to check and modify relevant parameter.

Status	>	SNMP Settings		
Basic Network WLAN	>	Enable SNMP	<u>×</u>	
Advanced Network	>	Port	161	
Firewall	>	Port		
D VPN Tunnel	>	Remote Access		
R Administration	•	Allowed Remote IP Address		(optional; ex "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" ")
- Identification				
Admin Access		System Name	detran	
Scheduled Reboot		Location	W1908	
 Storage Settings M2M Settings 		Contact	root	
DI/DO Setting		RO Community	Monitoreo_Radiomodem	
Logging Upgrade		RW Community	Monitoreo_Radiomodem	
		SNMPv3 Authentication Type	NONE *	
③ More Info		SNMPv3 Privacy Type	NONE *	

Figure 3-27 SNMP Setting GUI

Step 2 Please click "Save" to finish the setting

----End

2.8.6 M2M Access Setting (Apply to M2M Management Platform

installation application only)

Step 1 Please click "Administrator>M2M Access" to check and modify relevant parameter.



Status	>	m2m	
Basic Network	>	M2M Enabled	
 WLAN Advanced Network 	>	Fail Action	Restart M2M v
🔞 Firewall	>	Device ID	
VPN Tunnel	>		
R Administration	~	M2M Server/Port	: 8000
Identification		Heartbeat Intval	60 (seconds)
Admin Access		Heartbeat Retry	10 (Range:10-1000)
Scheduled Reboot SNMP Storage Settings		Named-Pipe Enabled	Remote Connect ·
M2M Settings DI/DO Setting		Named-Pipe Server Port	8002 (Bange1024-65535)
Configuration		Named-Pipe Status	Offline
Upgrade		Named-Pipe Address	0000

Figure 3-28 M2M Access Setting GUI

Step 2 Please click "Save" to finish the setting

----End

2.8.7 Configuration Setting

Step 1 Please click "Administrator> Configuration" to do the backup setting

0	Status	>	You haven't changed the default password for this router. To change router password <u>click here</u> .
Ø	Basic Network	>	
((*	WLAN	>	Backup Configuration
@	Advanced Network	>	router_015_m175101 .cfg Backup 🗛
1	Firewall	>	Save As Default Configuration
Ø	VPN Tunnel	>	Save
ѫ	Administration	*	Restore Configuration
H	Identification		Select the configuration file to restore:
	Time		No file chosen Choose File Restors
	Admin Access		
-	Scheduled Reboot		Restore Default Configuration
-	SNMP		Select V OX
-	Storage Settings		
-	M2M Settings		
	DI/DO Setting		Total / Free NVRAM: 64.00 KB / 39.50 KB (61.71%)

Figure 3-29 Backup and Restore Configuration GUI

CAUTION:

Restore Default would lose all configuration information, please be careful.

Step 2 After setting the backup and restore configuration. The system will reboot automatically.

----End

2.8.8 System Log Setting

Step 1 Please click "Administrator> Logging" to start the configuration, you can set the file path to save the log (Local or remote sever).



Status	>		You haven't changed the default password for this router. To change router password dick here.
Basic Networ	rk >		
🗟 WLAN	>	Syslog	v
Advanced Ne	etwork >	Log Internally	
G Firewall	>	Log To Remote System	
VPN Tunnel	>	Generate Marker	Every 1 Hour *
R Administratio	on 👻		
Identificatio	on	Limit	60 (messages per minute / 0 for unlimited)
- Time			
Admin Acces	155	Save Cancel X	
Scheduled R	Reboot		

Figure 3-30 System log Setting GUI

Step 2 After configure, please click "Save" to finish.

----End

2.8.9 Firmware upgrade

Step 1 Please click "Administrator>firmware upgrade" to open upgrade firmware tab.

0	Status	>		in a second company with the second state of the
~			Your	aven't changed the default password for this router. To change router password <u>click here</u> .
Q	Basic Network	>	Upgrade Firmware	
(WLAN	>		
	Advanced Network	>	Select the file to use:	
782	Advanced Network		No file chosen	Choose File Upgrade
1	Firewall	>	After flashing, erase all data in NVRAM m	emory
60	VPN Tunnel	>		
			Current Version:	G5.0.1.5-190801-095217
*	Administration	~	Free Memory:	98.86 M8 (aprox. size that can be buffered completely in RAM)
har	Identification		rice Menory.	30.00 mai (aprox size mar can be buriered completely in rxim)
	Time			
	Admin Access			
	Scheduled Reboot			
-	SNMP			
	Storage Settings			
	M2M Settings			
	DI/DO Setting			
-	Configuration			
	Logging			
har	Upgrade			

Figure 3-31 Firmware Upgrade GUI

CAUTION:

When upgrading, please don't cut off the power.

Step 2 After complete, you will see a button "Continue", click it to continue.

----End

2.9 System Reboot

Step 1 Please click "System >Reboot" to restart the router. System will popup dialog to remind "Yes" or "NO" before the next step.



Tools 🛠	Bandwidth 🞽	IP Traffic 📶	System 🏚
password <u>cliu</u>	Reboot 🗘	Hardware Reb	oot ტ
		Logout 🗗	

Step 2 If choose "yes", the system will restart, all relevant update configuration will be effective after reboot.

----End

2.10 Debugging Setting

2.10.1 Logs Setting

Step 1 Please click "Tools>Log" to check and modify relevant parameter.

		E Tools 🛠 Bandwidth 🗹 IP Traffic 💆 System 🗘
Status	>	You haven't changed the default password for this router. To change router password dick here.
Ø Basic Network	>	➢ Ping ⊘ Trace ♀ WOL ■ Log ▲ Capture
🛜 WLAN	>	
Advanced Network	>	Logs
G Firewall	>	View
O VPN Tunnel	>	Download Log File
R Administration	•	
Identification		* Logging Configuration
Admin Access		
SNMP		
Storage Settings		
 M2M Settings DI/DO Setting 		
Configuration		
Logging		
- Upgrade		

Figure 3-32 Logs GUI

----End

2.10.2 Ping Setting

Step 1 Please click "Tools >Ping" to check and modify relevant parameter.



	=	=			Tools 🛠	Bandwidth 🛃	IP Traffic 📶	System 🕻
Status	*	You have	n't changed the default passw	ord for this router. To change rou	ter password <u>click</u>	here.		
Basic Network	>	🎤 Ping 🖉 Trace 🖾 WOL 🖿 Log 🔒	Capture					
WLAN	>							
Advanced Network	>	Ping						
🐼 Firewall	>	IP Address	baidu.com	Ping				
O VPN Tunnel	>	Ping Count	5					
R Administration	~	Packet Size	56 (bytes)					
Time Admin Access Scheduled Reboot SNMP		Seq Address			RX Bytes	π	RTT (ms)	+/- (ms)
Storage Settings M2M Settings DI/DO Setting Configuration Logging Upgrade								

Figure 3-33 Ping GUI

----End

2.10.3 Trace Setting

Step 1 Please click "Debugging>Trace" to check and modify relevant parameter

				Tools 🛠 Bandwidth 🗹 🔅 Traffic 🔳	System 🐒
Status	>		You haven't cha	hanged the default password for this router. To change router password <u>click here.</u>	
Basic Network	>	➢ Ping Ø Trace S WOL ■ L	Log 🔒 Capture	re	
🗟 WLAN	>				
Advanced Network	>	Trace Route			
🕼 Firewall	>	IP Address		Trace	
O VPN Tunnel	>	Maximum Hops	20		
R Administration	*				
- Identification		Maximum Wait Time	3	(seconds per hop)	
Time					
Admin Access		Hop Address		min (ms) max (ms) avg (ms)	+/- (ms)
Scheduled Reboot				conclosed count food and food	
SNMP					

Figure 3-34 Trace GUI

----End

2.11 "Reset" Button for Restore Factory Setting

If you couldn't enter web interface for other reasons, you can also use this way. "Reset" button is near to Console port in G51 panel, This button can be used when the router is in use or when the router is turned on.

Press the "RST" button and keep more than 8 seconds till the NET light stopping blink. The system will be reverted to factory.

Table 3-27 System Default Instruction

Parameter	Default setting



LAN IP	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP server	Enable
User Name	admin
Password	admin

NOTE:

After reboot, the previous configuration would be deleted and restore to factory settings.

2.12 Appendix (For advanced optional features only)

2.12.1 GPS Setting

Step 1 Please click "Advanced Network> GPS" to view or modify the relevant parameter.

Status	>		You haven't changed the default password for thi	s router. To change router password <u>click here.</u>
Basic Network	>			
🗟 WLAN	>	GPS		
Advanced Networl		GPS Mode	Client *	
- Port Forwarding		Data Format	M2M_FMT	
Port Redirecting				
DMZ		Server IP/Port	192.168.1.2	: 40002
··· IP Passthrough				
Triggered				
Captive Portal		Heart-Beat Content		
Serial App.		Heart-Beat Interval	5 (seconds)	
GPS		Treat Deat Interval		
UPnP/NAT-PMP				
Bandwidth Limite	r	Save ✓ Cancel ×		
VRRP		Cancer A		
Static DHCP				

Figure 3-35 GPS Setting GUI

Table 3-28 "GPS" Instruction

Parameter	Instruction
GPS Mode	Enable/Diable
GPS Format	NMEA and M2M_FMT(HOMTECS)
Server IP/Port	GPS server IP and port
Heart-Beat	If choose M2M_FMT format, heart-beat ID will be packed into GPS data.
Interval	GPS data transmit as the interval time.



Step 2 Please click "Save" to finish

NOTE:

M2M_FMT Format as below.

1. GPS data structure:

Router ID, gps_date, gps_time, gps_use, gps_latitude, gps_NS, gps_longitude, gps_EW, gps_speed, gps_degrees, gps_FS, gps_HDOP, gps_MSL

2. Example:

0001_R081850ac,150904,043215.0,06,2234.248130,N,11356.626179,E,0.0,91.5,1,1.2,9 7.5

Field	d Name Format		Example	Description		
No.						
1	Router ID	String	0001_R081850 ac	0001-customizableproduct IDR-router indicator.081850ac-last 8digits ofrouters MAC address.		
2	gps_date	yymmdd	150904	Date in year,month,day		
3	gps_time	hhmmss.ss s	043215.0	UTC Time, Time of position fix.		
4	gps_use	numeric	06	Satellites Used, Range 0 to 12.		
5	gps_latitude	ddmm.mm mm	2234.248130	Latitude, Degrees + minutes.		
6	gps_NS	character	N	N/S Indicator,N=north or S=south.		
7	gps_longitude ddmm.mm 11356.626179 mm		Longitude, Degrees + minutes.			
8	gps_EW	character	E	E/W indicator, E=east or W=west		
9	gps_speed	numeric	0.0	Speed over ground, units is km/h.		
10	gps_degrees	numeric	91.5	Course over ground, unit is degree.		
11	gps_FS	digit	1	Position Fix Status Indicator,		
12	gps_HDOP	numeric	1.2 HDOP, Horizontal Dilution Precision			

3. GPS data description



	13	gps_MSL	numeric	97.5	MSL Altitude, unit is meter.
L					

----End

2.12.2 Captive Portal Setting

Step 1 Please click "Advanced Network> Captive Portal" to check or modify the relevant

parameter.

P			
Status	>	Captive Portal	
Basic Network	>	Enabled	
 WLAN Advanced Network 	•	Auth Type	NONE Y
Port Forwarding Port Redirecting		WEB Root	Default •
DMZ		WEB Host	
 IP Passthrough Triggered 		Portal Host	
Captive Portal Serial App.		Login Timeout	0 Minutes
- GPS - UPnP/NAT-PMP		Idle Timeout	0 Minutes
Bandwidth Limiter		Ignore LAN	
Static DHCP	>	Redirecting http://	www.google.com
VPN Tunnel	>	MAC Address Whitelist	
R Administration	>	Download QDS	

Figure 3-36 Captive Portal Setting GUI

ParameterInstructionEnableEnable Captive portal feature.Auth TypeReserved.Auth TypeReserved.Web RootChoose captive portal file storage path. Default: Captive portal file is in the firmware as default. In-storage: Captive portal file is in router's Flash. Ex-storage: Captive portal file is in extended storage such as SD card.Web HostConfigure domain name for the captive portal access. For example, Configure as www.homtecsm2m.com, we might directly access to captive portal page in the website as www.homtecsm2m.comPortal HostMaximum time user has connectivity. User need to re-login Captive Portal nage after defined time	Table 3-29 Serial Ap	p instruction
Auth TypeReserved.Web RootChoose captive portal file storage path. Default: Captive portal file is in the firmware as default. In-storage: Captive portal file is in router's Flash. Ex-storage: Captive portal file is in extended storage such as SD card.Web HostConfigure domain name for the captive portal access. For example, Configure as www.homtecsm2m.com, we might directly access to captive portal page in the website as www.homtecsm2m.comPortal HostReserved.Logged TimeoutMaximum time user has connectivity. User need to re-login Captive	Parameter	Instruction
Web RootChoose captive portal file storage path. Default: Captive portal file is in the firmware as default. In-storage: Captive portal file is in router's Flash. Ex-storage: Captive portal file is in extended storage such as SD card.Web HostConfigure domain name for the captive portal access. For example, Configure as www.homtecsm2m.com, we might directly access to captive portal page in the website as www.homtecsm2m.comPortal HostReserved.Logged TimeoutMaximum time user has connectivity. User need to re-login Captive	Enable	Enable Captive portal feature.
Default: Captive portal file is in the firmware as default.In-storage: Captive portal file is in router's Flash.Ex-storage: Captive portal file is in extended storage such as SD card.Web HostConfigure domain name for the captive portal access. For example, Configure as www.homtecsm2m.com, we might directly access to captive portal page in the website as www.homtecsm2m.comPortal HostReserved.Logged TimeoutMaximum time user has connectivity. User need to re-login Captive	Auth Type	Reserved.
In-storage: Captive portal file is in router's Flash. Ex-storage: Captive portal file is in extended storage such as SD card.Web HostConfigure domain name for the captive portal access. For example, Configure as www.homtecsm2m.com, we might directly access to captive portal page in the website as www.homtecsm2m.comPortal HostReserved.Logged TimeoutMaximum time user has connectivity. User need to re-login Captive	Web Root	Choose captive portal file storage path.
Ex-storage: Captive portal file is in extended storage such as SD card.Web HostConfigure domain name for the captive portal access. For example, Configure as www.homtecsm2m.com, we might directly access to captive portal page in the website as www.homtecsm2m.comPortal HostReserved.Logged TimeoutMaximum time user has connectivity. User need to re-login Captive		Default: Captive portal file is in the firmware as default.
Web Host Configure domain name for the captive portal access. For example, Configure as www.homtecsm2m.com, we might directly access to captive portal page in the website as www.homtecsm2m.com Portal Host Reserved. Logged Timeout Maximum time user has connectivity. User need to re-login Captive		In-storage: Captive portal file is in router's Flash.
Configure as www.homtecsm2m.com, we might directly access to captive portal page in the website as www.homtecsm2m.com Portal Host Reserved. Logged Timeout Maximum time user has connectivity. User need to re-login Captive		Ex-storage: Captive portal file is in extended storage such as SD card.
page in the website as www.homtecsm2m.com Portal Host Reserved. Logged Timeout Maximum time user has connectivity. User need to re-login Captive	Web Host	Configure domain name for the captive portal access. For example,
Portal Host Reserved. Logged Timeout Maximum time user has connectivity. User need to re-login Captive		Configure as www.homtecsm2m.com, we might directly access to captive portal
Logged Timeout Maximum time user has connectivity. User need to re-login Captive		page in the website as www.homtecsm2m.com
	Portal Host	Reserved.
Portal page after defined time	Logged Timeout	Maximum time user has connectivity. User need to re-login Captive
i ortal page arter defined time.		Portal page after defined time.
Idle Timeout Maximum time user has connectivity if no network activity from Wi-Fi	Idle Timeout	Maximum time user has connectivity if no network activity from Wi-Fi
User. If User need to re-login Captive page to surf internet.		User. If User need to re-login Captive page to surf internet.
Ignore LAN If enabled, LAN devices will bypass the Captive Portal page.	Ignore LAN	If enabled, LAN devices will bypass the Captive Portal page.

Table 3-29 "Serial App" Instruction



Redirecting	Router will redirect to the defined link after accepting the terms and
	conditions on the Captive Portal page
MAC Whitelist	No captive portal page for Wi-Fi device.
Download QoS	Enable to apply the Download and Upload per user limits.
Upload Qos	Maximum download speed available to each user.

NOTE:

1) Upload Portal file and Splash.html by local

Upload portal images and splash.html in router for the Slider (0001_portal.png, 0002_portal.png and

0003_portal.png) to the Router under the "Administration / Storage Settings" menu.

Furthermore, also might upload splash with images together.

	Status	>	You have	ren't changed the default password for this router. To change router password_ <u>click here</u> ,	
(i+ (j)	Basic Network WLAN Advanced Network Firewall	> > >	Storage settings Storage	Router Total 5,248.00 K3 Free4,988.00 K3	~
ø	VPN Tunnel	>	Upload new file		~
*	Administration Identification Time	.*	No file chosen Ch	noose File Upload	
	Admin Access Scheduled Reboot SNMP		Current file list	File size File operation	~
	Storage Settings		sms.list	rile size File operation	
	M2M Settings DI/DO Setting Configuration		SITISAISA	010	
-	Logging		Save - Cancel ×		
i	Upgrade				
0	Status	,	Captive Portal		
	busic rection.	>	Enabled		
	Advanced Network		Auth Type	NONE *	
	Port Forwarding Port Redirecting		WEB Root	In-storage 💌	
	DMZ IP Passthrough		WEB Host		
	Triggered Captive Portal		Portal Host		
	Serial App.		Login Timeout	0 Minutes	
	GPS UPnP/NAT-PMP		Idle Timeout	0 Minutes	
	Bandwidth Limiter VRRP		Ignore LAN		
	Static DHCP	>	Redirecting http://	www.google.com	
۵	VPN Tunnel	>	MAC Address Whitelist		
	Administration	>	Download QOS		



```
<!-- <hr> -->
<div id="myCarousel" class="carousel slide marketing">
   data-target="#myCarousel" data-slide-to="0" class="active">
      data-target="#myCarousel" data-slide-to="1">
      data-target="#myCarousel" data-slide-to="2">
   </01>
   <div class="carousel-inner">
       <div class="item_active">
          <img src="0001_portal.png")alt="">
       </div>
      <div class="item">
          <img src="0002 portal.png" alt="">
      </div>
       <div class="item">
          <img sro="0003_portal.png" alt="">
       </div>
   </div>
   <a class="left carousel-control" href="#myCarousel" data-slide="prev">&lsaquo;</a>
   <a class="right carousel-control" href="#myCarousel" data-slide="next">&rsaquo;</a>
</div>
<!-- <hr>>
```

----End

2.12.3 VLAN

Virtual local area network (VLAN) is a set of logical devices and users that are not limited by physical location, and can be organized according to factors such as functionality, and application, as if they were in the same network segment, Thereby getting the name of the department, virtual local area network. A VLAN is a new technology that works on Layer 2 and Layer 3 of the OSI reference model, a VLAN is a broadcast domain, and the communication between VLANs is done through a Layer 3 router. Compared with the traditional LAN technology, the VLAN technology is more flexible, it has the following advantages: the movement of network devices, the management cost of adding and modifying is reduced; the broadcast activity can be controlled, and the security of the network can be improved.

Select "Base Network > VLAN" in the navigation bar. In the open page, you can modify the relevant parameters to configure the dynamic domain name. As shown:

Status	>			You ha	ven't chang	ed the defaul	t password f	or this router	. To change	router passw	ord <u>click here</u>			
Basic Network	•	VLAN												,
Cellular		VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge	
- LAN - VLAN		1	~	×	~	×	~	×	~	×	~	×	br0	
Schedule		2	×	×	×	×	×	×	×	×	×	×	WAN	
- DDNS - Routing		0 *						10					none	٣
WLAN	>	Add+												
Advanced Network	>													
Firewall	>	Save 🗸 🛛 Cancel	×											
VPN Tunnel	>													
Administration	>													

Table 3-30 "VLAN" Instruction

Parameter	Instruction



VID	Each VLAN switch port needs to be bound to a
	VID; (VID range: 0 - 15).
LAN	Interface, 1*LAN
Тад	Trunk port (equivalent to checking the tagged-tag check) the
	data frame received from this port is typed by the tag, and the
	data frame sent by the tag, from this type of port requires tag
	(regardless of the default VLAN).

Example:

- 1. Each VLAN switch port needs to be bound to a VID; (VID range: 0 15).
- 2. Each VLAN switch port is in one of the following three categories: access, trunk.
 - 2.1. Access port (equal to or not checked): The data frame received from such port is not tag, and the data frame sent from such port is not tag;
 - 2.2. Trunk port (equal to the check-tagged-tag): The data frame received from such a port is tag, and the data frame sent from such a port needs to be tag (the default VLAN is not considered);
- 3. LAN port default is br0192.168.1.1 segment, can add 4 address segments on different interfaces.

Status	>		You haven't changed the	default password for this rou	iter. To change router passw	ord <u>click here.</u>	
Q Basic Network							
- WAN		LAN					~
Cellular		Bridge 🔨	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
LAN		br0	192.168.1.1	255.255.255.0	~	192.168.1.2 - 51	1440
VLAN			131100111	2551255125515		131100112 51	1440
Schedule		1					
DDNS Routing		· · ·					
		_					
🛜 WLAN	>	Add+					
Advanced Network	>						
🔞 Firewall	>	DNS					~
O VPN Tunnel	>	Use Custom DNS					
果 Administration	>						
		Save ✓ Cancel ×					

4. Set up 4 LANs, one WAN with the following diagram, assign the WAN to the VID 2, that is to bridge the WAN, and to assign the other interfaces to the br0 interface.

Status	>			You ha	ven't chang	ed the defaul	t password f	for this router	. To change	router passw	ord <u>click here</u>	1		
Basic Network	*	VLAN												~
Cellular		VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge	
- LAN - VLAN		1	~	×	~	×	~	×	~	×	×	×	br0	
Schedule		2	×	×	×	×	×	×	×	×	~	×	WAN	
DDNS Routing		0 *											none	v
🗟 WLAN	>	Add+												
Advanced Netw	ork >													
🔞 Firewall	>	Save ✓ Cance	l×											

5. With the increase of br1, br2, br3 in LAN, VLAN can be divided into four LAN ports with different IP segments independently for WAN ports, as shown in the following figure.



Status	>		You haven't changed the	default password for this rou	ter. To change router pass	word <u>click here.</u>	
Basic Network WAN	*	LAN					~
Cellular		Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
VLAN		br0	192.168.1.1	255.255.255.0	~	192.168.1.2 - 51	1440
Schedule		br1	192.168.2.1	255.255.255.0	~	192.168.2.2 - 254	1440
DDNS Routing		br2	192.168.3.1	255.255.255.0	~	192.168.3.2 - 254	1440
🕆 WLAN	>	br3	192.168.4.1	255.255.255.0	~	192.168.4.2 - 254	1440
Advanced Network	>	3					
🐼 Firewall	>						
🖾 VPN Tunnel	>	Add+					

6. Four LAN ports and WAN ports are configured independently.

VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	~	×	×	×	×	×	×	×	×	×	br0
2	×	×	~	×	×	×	×	×	×	×	br1
3	×	×	×	×	~	×	×	×	×	×	br2
4	×	×	×	×	×	×	~	×	×	×	br3
5	×	×	×	×	×	×	×	×	~	×	WAN
×										10.0	none

7. WAN uses the configuration as one of the LAN ports on the same network segment.

VID ^											
	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	~	×	×	×	×	×	×	×	×	×	br0
2	×	×	4	×	×	×	×	×	×	×	br1
3	×	×	×	×	4	×	×	×	×	×	br2
4	×	×	×	×	×	×	~	×	~	×	br3
5	×	×	×	×	×	×	×	×	×	×	WAN
0 *				11				11		10.0	none *

8. The VLAN divides a group of LAN1 and LAN2, a group of LAN3 and LAN4, and the independent WAN port is shown in the following figure. One IP segment of LAN1 and LAN2, one IP segment of LAN3 and LAN4, and the WAN port is configured independently.

VLAN											~
VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	~	×	~	×	×	×	×	×	×	×	br0
2	×	×	×	×	×	×	×	×	~	×	WAN
3	×	×	×	×	~	×	~	×	×	×	br1
0 *											none v
Add+											

9. The WAN port and one of the LAN ports are configured with the IP section.



AN											~
VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	~	×	~	×	×	×	×	×	~	×	br0
2	×	×	×	×	×	×	×	×	×	×	WAN
3	×	×	×	×	~	×	~	×	×	×	br2
• •		100		100						100	none 🔻

10.VLAN tagging trunk requires setting the accessed device to the same VID of 1.

VLAN											~
VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	~	~	~	~	~	~	~	~	×	×	br0
2	×	×	×	×	×	×	×	×	~	×	WAN
0 *											none 🔻
Add +											

----End

2.12.4 Schedule

Select "Basic Network > Schedule" in the navigation bar. On the open page, you can configure link scheduling WAN and 3G/4G backup or mutual standby mode.

NOTE:

The version of the 3G/ 4G and the wired network backup is only available for this feature, depending on the actual product version.

Features:

1, The ICMP link detection determines whether the link is normal through the IP address, and if the PING checks the IP block abnormal trigger switching mechanism.

2, The link scheduling strategy can be selected in BACKUP mode: link 1 fills in "WAN", WAN network is dominant, link 2 is filled with "modem", link 1 is filled in "modem", 4G network is dominant, link 2 is filled in "WAN", link 1 is standby, in BACKUP mode, link 1 is dominant when link 1 is online, link 1 is switched to link 2 when link 1 fails after ICMP detection. Link 1 is switched back to link 1 after ICMP detection recovery takes effect.

3, The link scheduling policy is an optional FAILOVER mode, which refers to the backup mode of the link 1 and the link 2; when the link 1 is on-line, the link 1 is the main link; after the link 1 fails, the link 1 is switched to the link 2 through the ICMP detection, and the link 2 is the main link; and when the link 1 is in effect, the link 2 is still the primary link and does not switch back link 3.to the link 1; after the link 2 fails, the ICMP detection is switched to the link 1, where the link 1 is the primary link.



4, WAN port supports DHCP automatic acquisition and static address, PPPoE fixed network access, WAN default shutdown needs to be enabled.

Status	>	Enabled Link	s					~
Basic Network WAN	*	Link Name		Link Type		Description		
Cellular LAN		modem		ECM/QMI				
VLAN Schedule		ICMP Check						~
DDNS Routing		On Link		Destination	Interval	Retries	Description	
	>							
Advanced Network	>	Add+						
B Firewall	>							
O VPN Tunnel	>	Schedule						~
R Administration	>	On	Link 1	Link 2	Policy	Description		
		<u>~</u>	modem	• modem	* FAILOVER	*		
		Add+						
		Save ✓ Car	ncel×					
 More Info 								

Table 3-30 "Schedule" Instruction

Parameter	Instruction
ICMP Link Detection-Link	Link,"modem, wan"
ICMP Link Detection-Destination	The IP address or domain name that the link needs to detect,
Address	whether the host is reachable and whether the route is available
ICMP Link Detection-Interval	The time interval for detecting the IP address
ICMP Link Detection-retry	Retry the secondary consecutive failure after the failure has failed to set the number of setting times.
Link scheduling-Link 1	Link,"modem, wan"
Link scheduling-Link 2	Link,"modem, wan"
Link scheduling-Policy	Link scheduling policy can be selected in BACKUP mode, "Link 1 is
	WAN, Link 2 is 4G" or "Link 1 is 4G, Link 2 is WAN" these two modes.
	Or in FAILOVER mode, refers to do backup
	between the link 1 and the link 2

Example:

Step 1:

Select "Basic Network > WAN" in the navigation bar. In the open page, the drop-down box selects the static address, configure the parameters of the static address, and click on the save settings; as shown in the following figure (note: the parameter configuration is an example that actually needs to be configured according to the field situation)



© Status	>	You have	n't changed the default password for this router. To change router password <u>click here</u> ,
Basic Network WAN	~	WAN / Internet	
- Cellular LAN		Туре	Static Address
VLAN		IP Address	192.168.10.64
DDNS Routing		Subnet Mask	255.255.255.0
	>	Gateway	192.168.10.1
Advanced Network	>	MTU	Default 🔻 1500
G Firewall	>		
C VPN Tunnel	>	Primary DNS	192.168.10.1
R Administration	>	Secondary DNS	114114.114.114
		Save ✓ Cancel ×	

Step 2:

Select "Basic Network > VLAN" in the navigation bar. On the open page, remove the WAN, click OK that checks VID1, as shown in the following figure:

VLAN												~
VID) ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
	1	1	×	~	×	~	×	~	×	×	×	br0
	2	×	×	×	×	×	×	×	×	×	×	WAN
0												none 🔻
Add +												

In the page of the VLAN, add the VID2, check the WAN, click OK, and click Save Settings after the setting is complete, as shown in the following figure:

	N 2 Taggeo	i LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
*								bridge
· ·	× ×	~	×	~	×	×	×	br0
×	× ×	×	×	×	×	~	×	WAN
								none 🔻
	×							

Step 3:

Select the "Status> Overview" in the navigation bar. In the open page, view the WAN network status and access the external network, as shown in the figure:



GPS Status Device List Image: Network > Image: Network >	Router Sn Chipset Router Time Uptime Memory Usage NVRAM Usage Ethernet Ports Status	G5.0.15 1120G512004170001 ARMv7 Processor rev 5 (v7) More, 25 May 2020 09:25:5 00:01:37 <u>33.27 M8 / 122.22</u> M8 (27.2 <u>31.38 K8 / 64.00 K8 (49.03%</u>	1 +0800 Clock Sync. 296)	~	Modem IMEI Modem Status Cellular ISP Cellular Network USIM Status CSQ IP Adress Subnet Mask Gateway DNS Connection Status Connection Uptime	88704042207165 Ready "CHINA MOBILE" LTE Ready 25		
() More Info		LAN1 LAN2	LAN3 LOOM Full		Wireless (2.4 GHz) MAC Address Wireless Mode Wireless Network Mode Interface Status Radio	340A:A417:51:03 Access Point Auto Up (LAN) Enabled γ	۵	~

Step 4:

Select "Basic Network> Schedule", configure the ICMP link detection item and the link scheduling item (note: link 1 is WAN, link 2 is modem), and the policy is backup; configure to complete the click save and wait for the device to restart.

Status	>	Enabled Links							
Basic Network	*	Link Name	Link Type		Description	Description			
- WAN		modem	ECM/QMI						
Cellular LAN		wan	WAN(STAT	IC)					
···· VLAN									
DDNS		ICMP Check					~		
Routing		On Link	Destination	Interval	Retries	Description			
🗇 WLAN	2	🗸 wan	114.114.114.114	5	3		×		
Advanced Network	>	✓ modem	114.114.114.114	5	3				
🐼 Firewall	>								
D VPN Tunnel	>	Add +							
R Administration	>	Add+							
		Schedule					~		
		On Link 1	Link 2	Policy	Description				
		✓ wan	modem	BACKUP					
(i) More Info		mode	m • modem	* FAILOVER	×				

NOTE:

WAN prefer, Modem backup

Step 5:

Click "Status> Overview" to view the WAN connection status (the WAN is the main), as shown in the following figure:



 Status Overview Traffic Status GPS Status Device List Basic Network WLAN Advanced Network Firewall VPN Tunnel Administration 	• • • •	System Router Name Hardware Version Firmware Version Router 5n Chipset Router Time Uptime Memory Usage NVRAM Usage	Mon, 25 May 00:01:24 33.21 M8 / 12	4170001 ssor rev 5 (v71) 2020 09:29:17 +0800 22.22 MB (27.17%) 20 KB (49.26%)	Clock Sync.	~	WAN Connection Type Modem IMEI Modem Status Cellular ISP Cellular Network USIN Status CSQ IP Address Subnet Mask. Gateway DNS Connection Status	WAN 868704042207165 Ready "CHINA MOBILE" LTE Ready 26 m 192168.10.64 253252520 192168.10.13 192168.10.13 192168.10.13	٥	~
							Connection Uptime	00:00:59		
		Ethernet Ports Status				~				
		WAN/LAN	LAN1	LAN2	LAN3		Wireless (2.4 GHz)		۵	~
		Lunni I	F				MAC Address	34:0A:A4:17:51:03		
		1000M Full U	Jnplugged	Unplugged	100M Full		Wireless Mode	Access Point		
		200001100	, proggeo	onproggeo	2001110		Wireless Network Mode	Auto		
							Interface Status	Up (LAN)		
		VPN Status			\$	~	Radio	Enabled 🗸		
(i) More Info		No Active VPN					SSID	router-wifi_175103		

Step 6:

Disconnect the network cable from the WAN port and look again at the connection status of the WAN (this is the line on the card), as shown in the following figure:

Status Overview Traffic Stats. GPS Status Device List Easic Network WILAN Advanced Network Firewall VYN Tunnel	> > > >	Hardware Version Firmware Version Router Sn Chipset Router Time Uptime Memory Usage NVRAM Usage	ARMv7 Pro Mon, 25 M 00:03:15 <u>33.27 MB /</u>	004170001 ocessor rev 5 (v7l) 1ay 2020 09:31:10 +0800 <u>122:22 1M8 (27.22%)</u> 64.00 KB (49.26%)	Clock Sync.			Modem IMEI Modem Status Cellular ISP Cellular Network USIM Status CSQ IP Address Subnet Mask Gateway DNS Connection Status Connection Uptime	868704042207165 Ready "C-HINA MOBILE" LTE Ready 26		
Administration Administration	>	Ethernet Ports Status WAN/LAN Unplugged VPN Status No Active VPN	LAN1 Unplugged	LAN2	LAN3	۰	× ;	Wireless (2.4 GHz) MAC Address Wireless Mode Wireless Network Mode Interface Status Radio SSID Broadcast Security Channel	340A4A417:51:03 Access Point Auto Up (LAN) Foulder J Foulder J Isabled J disabled 7 - 2:442 CH:	\$ ~	<i>.</i>

Step 7:

When you insert the network cable into the router's WAN port again, check the connection status of the WAN (at this time static Internet access), as shown in the following figure:

Status Overview Traffic Stats. GPS Status Device List Desice List WLAN Advanced Network Firewall VPN Tunnel Administration	> > > >	System Router Name Hardware Version Firmware Version Router 5n Chipset Router Time Uptime Memory Usage NVRAM Usage	ARMv7 P Mon, 25 00:04:02 <u>33.49 MB</u>	2004170001 rocessor rev 5 (v7l) May 2020 09:31:57 +08 / 122.22 M8 (27.40%) / 122.22 M8 (27.40%) / 64.00 K8 (49.26%)	00 Clock Sync.	~	WAN Connection Type Modem MEI Modem Status Cellular ISP Cellular Network USIM Status CSQ IP Address Subnet Mask Gatevay DNS Connection Status Connection Uptime	WAN 868704042207165 Ready "CHINA MOBILE" LTE Ready 26 art 1921661064 2552550 192166101 19216610153,11411411411453 Connected 000013	٥	~
		WANLAN	LAN1 Unplugged	LAN2	LAN3 100M Full	¢ ~	Wireless (2.4 GHz) MAC Address Wireless Mode Wireless Network Mode Interface Status Radio	340A.4417.51.03 Access Point Auto Up (LAN) Enabled ~	٥	×
③ More Info		No Active VPN					SSID	router-wifi_175103		