SheRink Industrial Router



Contents

1.	Product Introduction
	1.1 Product overview
	1.2 Model introduction 3
	1.3 Product Appearance
	1.4 Typical Application Diagram4
	1.5 Features
2.	Hardware Installation
	2.1 Panel
	2.2 LED Status7
	2.3 Dimension7
	2.4 How to Install
3.	Router Configuration9
	3.1 Local Configure9
	3.2 Basic Configuration10
	3.3 Advanced Network Setting16
	3.4 Firewall
	3.5 VPN Tunnel26
	3.6 Administration35
	3.7 Debugging Setting
	3.8 "RST" Button for Restore Factory Setting 44
	3.9 Appendix45

1 Product Introduction

1.1 Product overview

SheRink industrial Router is based on industrial grade design, built-in high-powered 32bit MIPS processor, and multi-band 4G/3G communication module, support WCDMA,HSPA+, 4G FDD/TDD etc., provide quick and convenient internet access or private network transmission to customer, provide wire-line network or wireless WLAN share high speed access, meanwhile, customized high security VPN (Open VPN、IPSec、SSL), to construct safe channel, widely used in financial, electric power, environment, oil, transportation, security, etc..

SheRink industrial series router provide GUI, optional CLI configuration interface, customer can configure by IE explore or Telnet/SSH, various configuration method, concise and friendly interface make configuring and managing of all router terminal easier ,meanwhile, SheRink provide M2M terminal management platform to manage all router terminal with remote management. User can monitor all terminals which connected to platform successfully by this platform, provide long-distance control, parameter configuration, and long-distance upgrade service.

1.2 Model introduction

SheRink industrial grade router series have single module / single SIM card, single module / double SIM card, double module / double SIM card design, support multi-band frequency WCDMA, HSPA+, 4G FDD/TDD etc., and downward compatibility to GPRS, EDGE, CDMA 1x, etc., optional GPS module Expansion positioning function, to suit different requirement and different network environment of different operators. Our Router series have many model for option, below is the product model indications in detail.

Model	4 G	3 G	Interface	WiFi	4 G
R1L1H	FDD 2600/2100/1900/1800/900/800MHz	HSPA+/HSPA/HSDPA 850/900/1900/2100MHz	1xLAN 1xRS-232	No	Yes
R1L1	FDD 2600/2100/1800/900/800MHz	HSPA+/HSPA/HSDPA 800/850/900/1900/2100MHz	1xLAN 1xRS-232	No	Yes
R1L1F	FDD:1800/2100/2600MHz TDD:1900/2300/2600MHz	HSPA+/HSPA/HSDPA 2100/1900/850/900MHz	1xLAN 1xRS-232	No	Yes
R1L1H2	FDD:700/850/1700/1900MHz	DC-HSPA+/HSPA/HSDPA 2100/1900/850/900MHz	1xLAN 1xRS-232	No	Yes
R1L1-H	-	HSPA+ 2100/1900/850MHz	1xLAN 1xRS-232	No	No
R1L1-H2	-	HSPA+ 2100/1900/900/850MHz	1xLAN 1xRS-232	No	No
R1L1-H232	-	HSPA+ 900/2100MHz or 850/1900MHz	1xLAN 1xRS-232	No	No
R1L1-H485	-	HSPA+ 900/2100MHz or 850/1900MHz	1xLAN 1xRS-485	No	No
R1L1E	-	EVDO 800MHz	1xLAN 1xRS-232	No	No

1.3 Product Appearance

Series	R1	R2	R20	R52
Appearance			Upper	
Ports	1xLAN 1xRS-232/RS485	2xLAN/1xLAN+ 1xWAN GPS or WLAN	2xLAN(deafult) + dual SIM GPS, WLAN	1xWAN, 4xLAN + single module / dual SIM or dual module / dual SIM
Product category	Single port router	Dual-port WiFi router	Multi-port WiFi router	Multi- functional WiFi router

Table 1-1 SheRink Router Appearance

1.4 Typical Application Diagram

SheRink 4G/3G Router widely used in Telecom, economic, advertisement, traffic, environment protection business area. For example, in economic area, R100 Series Router connect server by IPSec & GRE to ensure data security, tiny design makes it could installed into ATM machine. All these technology ensured safe and reliable data transmission, and minimize the probability of network disconnection, and maximize the usability of economic business like ATM, POS .etc.



Figure 1-1 Network Topology

SheRink industrial router is based on mobile wireless public network or private network, build wireless data channel in mature network, to lower down the cost of wireless data transmission and technique.

1.5 Features

- Various cellular module optional, LTE/HSPA+/EVDO/CDMA2000 optional

- Support virtual data and private network (APN/VPDN)

- Optional support RS-232/RS-485 interface data transparent transmission and protocol conversion

- Support on-demand dialing, include timing on/off-line, voice or SMS control on/off-line, data trigger online or link idle offline

- Support TCP/IP protocol stack, support Telnet, HTTP, SNMP, PPP, PPPoE, etc., network protocol

- Support VPN (Client PPTP), L2TP, optional support Open VPN, IPSec, HTTPs, SSH, advanced VPN function

- Provide friendly user interface, use normal web internet explorer to easily configure and manage, long-distance configure Telnet/SSH.

- Optional IPv6 protocol stack
- Optional support M2M terminal management platform
- WDT watchdog design, keep system stable

2 Hardware Installation

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

2.1 Panel

Table 1-1 R1 – Structure

	R1 series		
Front			
Rear	V+ V- GND RX TX LAN		

There are some different for Antenna interface and indicator light for the expanded GPS series.

Table 2-1 Router Interface

Port	Instruction
USIM	Plug type SIM Slot, support 1.8/3V/5V automatic detection
Main	4G/3G antenna, SMA connector, 50Ω

Port	Instruction	
Aux/GPS	4G Aux Antenna or GPS Antenna, SMA connector, 50Ω	
LAN	10/100Base-TX, MDI/MDIX self-adaption,	
RST	Reset button, (press on button 5 seconds)	
PWR	Power connector	
СОМ	Three pins serial port, suitable for collection devic with RS-232 or RS-485 interface, for wireless dat transmission.	

2.2 LED Status

silk-screen	color	status	Indication
	Green		Strong Signal
	Orange		Normal Signal
NET	Red		Weak Signal
		Solid light	Connected 4G successfully
		Blinking quickly(0.5s)	Dialing
	Green	Solid light	Connected
LAN	Green	Blinking	Data Sending
	Green	Dark	Not connected
PWR	Green	Solid light	Router OS is running.

Table 2-2 Router LED indictor Status

2.3 Dimension



Figure 2-2 R1 Series Router Dimension Figure

2.4 How to Install

2.4.1 SIM/UIM card install

If use dual SIM/UIM card router, you may need insert dual SIM before configure it. After installation, please follow below steps to connect the router.

!!! Before connecting, please disconnect any power resource of router

2.4.2 Ethernet Cable Connection

Use the Ethernet cable to connect the cellular Router to computer directly, or transit by a switch.

2.4.3 Serial Port Connection

If you want to connect the router via serial port to laptop or other devices, you should prepare a serial port, this cable is optional. One end connect to computer serial port, the other end connects the RX/TX and GND of the router

!!! Before connecting, please disconnect any power resource of router

2.4.4 Power Supply

In order to get high reliability, SheRink Series Router adapt supports wide voltage input range: $+7.5V \sim +32VDC$, support hot plug and complex application environment.

2.4.5 Review

After insert the SIM/UIM card, connect Ethernet cable and necessary antenna, connect power cable.

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

Notice:

Step 1 Check antenna connection.

Step 2 Check SIM/UIM card, confirm SIM/UIM card is available.

Step 3 Power on the industrial Router

3. Router Configuration

This Chapter introduces the parameter configuration of the router, the router can be configured via IE, Firefox, or Chrome.

3.1 Local Configure

The router supports to be configured by local Ethernet port, you could specify a static IP or DHCP get IP for your computer. 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 3-3 Network Connection

Step 2 Obtain a IP address automatically 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 when log in for the first time

Connect to 19	2.168.8.1 🛛 🛛 🔀
R	GA
<u>U</u> ser name: <u>P</u> assword:	admin Remember my password
	OK Cancel

Figure 3-4 User Identify Interface

3.2 Basic Configuration

Different software version has different web configuration interface, below take WL-R100 as example. After access the WEB interface, you can check the current status of Router, or modify router configuration via web interface, below is the introduction for the common setting.

			Router
Status	System Status		
Overview			
LAN	Router Name	Router	
Device List	Hardware Verion		
Basic Network	Firmware Version	Router-4.2.2.3	
Advanced Network	Pouter Time	Tue 20 Mar 2016 20:40:06 ±0800 Clock Sync	
Firewall	Rodeer filme	00-01-0C	
VPN Tunnel	Tabl / Free Memory	00:01:30	
Administration	Total / Free Menory	00.00 MB / 35.35 MB (05.14 %)	
Debugging			
	Internet Status		
Logout			
	Connection Type	Cellular Network	
	MAC Address	00:90:4C:06:50:2E	
	Modem IMEI	864881021779259	
	Modem Status	Ready	
	Cellular ISP	"CHN-UNICOM"	
	Cellular Network	"WCDMA"	
	USIM Status	Ready	
	CSQ	9.	
	IP Address	10.232.200.48	
	Subnet Mask	255.255.255.255	
	Gateway	10.64.64	
	DNS	210.21.196.6:53, 221.5.88.88:53	
	Connection Status	Connected	
	Connection Uptime	00:00:45	

3.2.1 Cellular Network Configure

Step 1 Single Click Basic Network-> Cellular, you can modify relevant parameter

according to the application.

Status	Cellular Settings	i l	Router
Basic Network			
Cellular	Cellular Network	MU709S:WCDMA/HSPA+	
LAN	Type		
DDNS	ICMP Check	8	
Routing			
Advanced Network	Cellular Traffic Check	0	
Firewall	Connect Mode	Keep Alive(Auto-Online) 🔻	
VPN Tunnel	CIMI Send to	:	
Administration		1	
Debugging	SMS Code		
Logout	PIN Code		
cogout	Operator Lock	ex:46001	
	Dial Number	*99#	
	Mode	Auto 🔻	
	APN	3GNET	1
	User	CARD	3
	Password	****	
	Auth Type	Auto 🔻	
	Local IP Address		
		S	ave Cancel

Figure 3-1 Cellular Settings GUI

Table 3-1 Cellular Setting Parameter Instruction

Parameter	Instruction		
ICMP check	To enable or disable ICMP check rules. Enable the ICMP check and setup a reachable IP address as destination IP. Once ICMP check failed, router will reconnect/reboot system as optional		
Cellular Traffic Check	There is Rx/Tx as options. Once no Rx/Tx data, router will router will reconnect/reboot system as options.		
Connect Mode	 Keep alive (Auto-online). The router will automatically connect 3G/4G network and keep online. 		
	 Connect On Demand. Idle offline if no data from LAN to 3G/4G within defined time. 		

Parameter	Instruction		
	 Schedule, Define online and offline time. This function need to enable NTP function, Call/SMS Triggered. Call/SMS trigger router online. Manually. Connect 3G/4G network by manual. 		
CIMI Send	Send CIMI to defined IP and port by TCP protocol.		
SMS Code	SMS identifying code. Router just identifies the unique code to implement SMS command.		
PIN Code	Unlock the SIM PIN code.		
Operator Lock	Lock operators via MCC/MNC		
Service Code	The default service code as *99#.		
APN	APN, provided by local ISP, usually CDMA/EVDO network do not need this parameter.		
User	SIM card user name is provided by ISP		
Password	SIM card password is provided by ISP		
Auth Type	Support PAP/Chap/MS-Chap/MS-Chapv2		
Local IP Add	Defined SIM IP from operator.		

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	8.8.8.8	
Check IP (Optional)	4.4.4.4	4
Interval	60	(seconds)
Retries	3	(Times)
Fail Action	Reboo	t 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	•	
Check Interval	10	(minutes)Range: 1 ~ 1440	,
Fail Action	Cellula	ar Reconnect 🔻	

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

3.2.2 LAN Setting

Step 1 Single Click "Basic Network>LAN" to enter below interface

Status	LAN	Ro	uter
Basic Network			
Cellular	Router IP Address	192.168.1.1	
LAN	Subnet Mask	255 255 255 0	
DDNS	Sublict Mask	255,255,257,0	
Routing	DHCP Server	2	
Advanced Network	IP Pool	192.168.1.2 - 192.168.1.53 (52)	
Firewall	Lease	1440 (minutes)	
VPN Tunnel			
Administration			
Debugging			
Logout			
		Save	ol



Table 3-2 LAN Setting Instruction

Parameter	Instruction
Router 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	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

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

3.2.3 Dynamic DNS Setting

Step 1 Single click "Basic Network->DDNS to enter the DDNS setting GUI.

Status	Dynamic DNS		Router
Basic Network			
Cellular	IP Address	Use WAN IP Address 10.232.200.48 (recommended) V	
LAN	Auto refrech every	5 minutes $(0 = \text{Displied})$	
DDNS	Autorenesirevery	Disabled)	
Routing			
Advanced Network	Dynamic DNS 1		
Firewall			
VPN Tunnel	Service	None	
Administration	our vice	mene	
Debugging			
Logout	Dynamic DNS 2		
	Service	None	
		Save	e Cancel

Figure 3-3 Dynamic DNS Setting

Table 3-3 DDNS Setting Instruction

parameter	Instruction
IP Address	Default is standard DDNS protocol, for customized protocol, please contact Wlink engineer. Usually, use default IP 0.0.0.0
Auto refresh time	Set the interval of the DDNS client obtains new IP, suggest 240s or above
Service provider	Select the DDNS service provider that listed.

Step 2 Please Click "Save" to finish.

3.2.4 Routing Setting

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

atus	Current Routing	Table					
sic Network					-		
Cellular	Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface		
AN	10.64.64.64	*	255.255.255.255	0	pppO (WAN)		
	192. 168. 1. 0	*	255. 255. 255. 0	0	br0 (LAN)		
JUNS	127.0.0.0	*	255.0.0.0	0	10		
Routing	default	10.04.04.04	0.0.0.0	0	pppu (man)		
vanced Network		120					
wall	Static Routing T	able					
N Tunnel	Destination	Gateway	Subnat Mask	Hatric	Interface	Bargrintian	
ministration	1	7	Daniel C Basa				
buaaina	U			-			
pout	Miscellaneous						
gout	Miscellaneous	Gateway 🔻					
pout	Miscellaneous Mode	Gateway 🔻					
gout	Miscellaneous Mode RIPv1 & v2	Gateway 🔻 Disabled 🔻					
gout	Miscellaneous Mode RIPv1 & v2 Efficient Multicast Forwarding	Gateway V Disabled V					
pout	Miscellaneous Mode RIPv1 & v2 Efficient Multicast Forwarding DHCP Routes	Gateway ▼ Disabled ▼					
pout	Miscellaneous Mode RIPv1 & v2 Efficient Multicast Forwarding DHCP Routes Spanning-Tree Protoco	Gateway V Disabled V Oliable					
jout	Miscellaneous Mode RIPv1 & v2 Efficient Multicast Forwarding DHCP Routes Spanning-Tree Protoco	Gateway					
pout	Miscellaneous Mode RIPv1 & v2 Efficient Multicast Forwarding DHCP Routes Spanning-Tree Protoco	Gateway V Disabled V Ol					

Figure 3-4 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.

3.3 Advanced Network Setting

3.3.1 Port Forwarding

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

asic Network								
dvanced Network	On	Proto	Src Addr	ess Ext Ports	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		Both	1.1.1.0/2	4 1000-2000		192.168.1.2	ex: 1000 to 2000, restricted	
Triggered		TCP		1000	2000	192.168.1.2	ex: different internal port	
Serial App.		TCP	•					
UPnP/NAT-PMP Bandwidth Limiter VRRP								Å
UPnP/NAT-PMP Bandwidth Limiter VRRP Static DHCP rewall	:	Src Add Ext Por Int Por	iress (optiona ts - The ports t (optional)	() - Forward only if from to be forwarded, as see The destination port ins	this addre n from the ide the LAI	ss. ex: "1.2.3.4", "1. WAN. ex: "2345", "2 N. If blank, the destin	2.3.4 - 2.3.4.5", "1.2.3.0/24", "me.exa 200,300", "200-300,400". nation port is the same as <i>Ext Ports</i> . Only	mple.com' y one port
UPnP/NAT-PMP Bandwidth Limiter VRRP Static DHCP rewall PN Tunnel	:	Src Add Ext Por Int Por entry is Int Add	Iress (optiona ts - The ports t (optional) - , supported whe Iress - The desi	//- Forward only if from to be forwarded, as see The destination port ins n forwarding to a differ ination address inside ti	this addre n from the ide the LAI ent internal ne LAN.	ss. ex: "1.2.3.4", "1. WAN. ex: "2345", " N. If blank, the destir I port.	2.3.4 - 2.3.4.5", "1.2.3.0/24", "me.exa 200,300", "200-300,400". aation port is the same as <i>Ext Ports</i> . Only	A mple.com y one port
UPnP/NAT-PMP Bandwidth Limiter VRRP Static DHCP rewall PN Tunnel dministration	:	Src Add Ext Por Int Por entry is Int Add	Iress (optiona ts - The ports t (optional) supported whe Iress -The desi	// - Forward only if from to be forwarded, as see The destination port ins n forwarding to a differ tination address inside the tination address inside the second second second tination address inside the second second second second second tination address inside the second seco	this addre h from the ide the LAI ant internal he LAN.	ss. ex: "1.2.3.4", "1. WAN. ex: "2345", "3 N. If blank, the destir port.	2.3.4 - 2.3.4.5", "1.2.3.0/24", "me.exa 200,300", "200-300,400". nation port is the same as <i>Ext Ports</i> . Only	mple.com y one port
UPnP/NAT-PMP Bandwidth Limiter VRRP Static DHCP rewall PN Tunnel dministration ebugging	:	Src Add Ext Por Int Por entry is Int Add	iress (optiona ts - The ports t (optional) supported whe iress -The des	// - Forward only if from to be forwarded, as see The destination port ins n forwarding to a differ tination address inside to	this addre n from the de the LAI ent internal ne LAN.	ss. ex: "1.2.3.4", "1. WAN. ex: "2345", "; V. If blank, the destir I port.	2.3.4 - 2.3.4.5", "1.2.3.0/24", "me.exal 200,300", "200-300,400". ation port is the same as <i>Ext Port</i> s. Only	A mple.com y one port

Figure 3-5 Port Forwarding GUI

Table 3-5 "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

3.3.2 Port Redirecting

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

Proto TCP V	Int Port	Dat Address	Ext Port	Description	
TCP Y	Int Fort	JST Address		Jeser 1911on	
					1

Figure 3-6 Port Forwarding GUI

Table 3-6 "Port Redirecting" Instruction

Parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Int Port	Internal port.
Dst. Address	The redirecting IP address.
Ext. Ports	External port for redirection.
Description	Remark the rule

Step 2 Please click "save" to finish

3.3.3 DMZ Setting

Step 1 Please click "Advanced Network> DMZ" to check or modify the relevant parameter.

Status	DMZ		Router
Basic Network			
Advanced Network Port Forwarding Port Redirecting DMZ Triggered Serial App. UPnP/NAT-PMP	Enable DMZ Internel Address Source Address Restriction Leave Remote Access	192.168.1.0 (optional; ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" or "me.example.com") (Redirect remote access ports for SSH and HTTP(s) to router)	
Bandwidth Limiter VRRP Static DHCP Firewall VPN Tunnel Administration Debugging Logout			
		Figure 3-7 Port Redirecting GUI	Cancel

Table 3-7	"DMZ"	Instruction
-----------	-------	-------------

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

Step 2 Please click "save" to finish

3.3.4 IP Passthrough Setting

Step 1 Please click "Advanced Network> IP Passthrough" to check or modify the relevant parameter.

Status	IP Passthrough		Router
Basic Network	-		
WLAN	Enabled	•	
Advanced Network	MAC Address	24:00:00 40:52:22	
Port Forwarding	MAC Address	34.00.09.AC.32.23	
Port Redirecting	Gateway		
DMZ			
IP Passthrough			
Triggered			
Captive Portal			
Serial App.			
UPnP/NAT-PMP			
Bandwidth Control			
VRRP			
Static DHCP			
Firewall			
VPN Tunnel			
Administration			
Debugging			
Logout			
			save Cancel

Figure 3-8 IP Passthrough GUI

Table 3-8 "IP Passthrough" Instruction

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

Step 2 Please click "save" to finish

3.3.5 Triggered Setting

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

vanced Network	Un	TCP	3000-4000	Forwarded Forts	Description av: open 5000-6000 if 3000-4000	
Port Forwarding		TCD		3000 0000	ex. open 3000 0000 11 3000 4000	
Port Redirecting		TOP				
OMZ						A
nggered						
erial App.	•	(200-300).				
PnP/NAT-PMP	•	These ports a	are automatically closed a	fter a few minutes of inactivit	у.	
andwidth Limiter						
000						
KKP						
tatic DHCP						
KKP tatic DHCP wall						
kkp tatic DHCP wall i Tunnel						
kkp Satic DHCP wall I Tunnel ninistration						
tatic DHCP wall I Tunnel ninistration ugging						

Figure 3-9 Triggered GUI

Table 3-	-9 "Trigge	red" Instr	uction
----------	------------	------------	--------

parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Triggered Ports	Trigger Ports are the initial LAN to WAN "trigger".
Transferred Ports	Forwarded Ports are the WAN to LAN ports that are 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.

3.3.6 Serial App. Setting

Step 1 Please click "Advanced Network> Serial App" to check or modify the relevant parameter.

Status	Serial to TCP/IP				Notiter
Basic Network					
Advanced Network	Serial to TCP/IPMode	Client	•		
Port Forwarding	Server IP/Port	8.8.8.8		: 40002	
Port Redirecting				10002	
DMZ				: 40003	
Triggered	Socket Type	TCP 🔻			
Serial App.	Socket Timeout	500	(milliseconds)		
UPnP/NAT-PMP	Serial Timeout	500	(milliseconds)		
Bandwidth Limiter	Paket Pavload	1024	(hytes)		
VRRP	Faket Fayload	1024	10,000		
Static DHCP	Heart Beat Content				
Firewall	Heart-Beat Content				
VPN Tunnel	Heart-Beat Interval	2	(seconds)		
Administration					
Debugging	Baud Rate	115200	*		
	Parity Bit	none 🔻			
Logout	Data Bit	8 🔻			
	Stop Bit	1 🔻			

Save Cancel

Figure 3-10 Serial App Setting GUI

Table 3-10 "Serial App" Instruction

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

Serial port connection

PINs	DB9(male)
V+	
V-	
GND	 5
RX	 3
ТХ	 2

Step 2 Please click "save" to finish.

----End

3.3.7 UPnp/NAT-PMP Setting

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

Status	Forward	ed Ports						Router
Basic Network								
Advanced Network	Ext Ports	Int Port	Address		Protocol	Description		
Port Forwarding							Delete A	Refresh
Port Redirecting								
DMZ	Settings							
Triggered								
Serial App.	Enable UPn	p	4					
UPnP/NAT-PMP	Enable NAT							
Bandwidth Limiter	Enable NAT	-PMP	(*)					
VRRP	Inactive Ru	les Cleaning	4					
Static DHCP	Cleaning I	interval	600	seconds				
Firewall	Cleaning 1	Threshold	20	redirection	ons			
VPN Tunnel	Secure Mod	le	when ena	blad LID	D cliente a	re allowed to add mannings only to their I	D)	
Administration	Secure Hou		C WHEN ENd	bied, ori	IF CIEILS a	re allowed to add mappings only to clear I	r J	
Debugging	Chaus In M	. Maharada						
Logout	Places	Network						
							Save	Cancel

Figure 3-11 UPnp/NAT-PMP Setting GUI

Step 2 Please click "save" to finish.

3.3.8 Bandwidth Control Setting

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

Status	Bandwidth Control					Router
Basic Network						
WLAN	Enable Control					
Advanced Network						
Port Forwarding				202250 - 111		
Port Redirecting	IP IP Range MAC Address	DLEate	DLCeil	ULRate	WLCeil	Priority
DMZ						Normal 🔻
IP Passthrough						Add
Triggered						
Captive Portal	Default Class					
Serial App.						
UPnP/NAT-PMP	Enable Default Class					
Bandwidth Control						
VRRP						
Static DHCP						
Firewall						
VPN Tunnel						
Administration						
Debugging						
Logout						
					Si	ave Cancel

Figure 3-12 Bandwidth Control Setting GUI

Step 2 Please click "save" to finish. ---End

3.3.9 VRRP Setting

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

Status	VRRP		
Basic Network			
Advanced Network	Enable VRRP		
Port Forwarding	Mode	Backup Y	
Port Redirecting	No.		
DMZ	VITUAL IP	192.168.1.3	
Triggered	Virtual Router ID		
Serial App.	Priority	100	
UPnP/NAT-PMP	Authentication		
Bandwidth Limiter	Covint Tune	Default -	
VRRP	Script Type	Derault	
Static DHCP	Check Interval	3	
irewall	Weight	10	
/PN Tunnel			
dministration			
Debugging			
ogout			
			Save Cance

Step 2 Please click "save" to finish.

---End

3.3.10 Static DHCP Setting

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

	MAC Address	IP Address	Hostname	Description
dvanced Network	00:00:00:00:00:00		- Administration of the community of the	
Port Forwarding	00:00:00:00:00	192.168.1.2		
Port Redirecting				A
DMZ				
Triggered				
Serial App.				
UPnP/NAT-PMP				
Bandwidth Limiter				
VRRP				
Static DHCP				
ewall				
PN Tunnel				
dministration				
ebugging				

Figure 3-14 Static DHCP Setting GUI

Step 2 Please click "save" to finish.

3.4 Firewall

3.4.1 IP/URL Filtering

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

Status	IP/	MAC/Port	Filtering						PAU PAU
Basic Network	On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
WLAN	1				NONE T			Accs T	
dvanced Network					none			meet	
rewall									Ad
IP/URL Filtering									
Domain Filtering	Ke	y Word Filt	ering						
N Tunnel	0,	Key Ford			Descrip	tion			
Iministration)							
ebugging									a di
	0.	N URL			Descrip	tion			
	2								Ad
	Ace	cess Filteri	ng						6A
	Act	Cess Filterin Sro KAC	ng Sre IP	Dst IP	Protocol	Sre Port	Dst Port	Policy	Ad
		C ess Filteri i Sto BAC	ng Sre IP	Dst IP	Protocol NONE V	Src Port	Dst Port	Policy Acce V	Ad

Table 3-11 "IP/URL Filtering" Instruction

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

Step 2 Please click "save" to finish.

3.4.2 Domain Filtering

Step 1 Please click "Firewall> Domain Filtering" to check or modify the relevant parameter.

Domain Filte	ring			Koute
On	1			
Default Delige	Black List			
Default Policy	BIACK LISE			
On Domain		Description		
				Add
	On Default Policy	On Default Policy Black List On Demain	On Default Policy Black List On Description	On Default Policy Black List Dn Description Save

Figure 3-15 Domain Filtering Setting GUI

Table 3-12 "GRE" 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

3.5 VPN Tunnel

3.5.1 GRE Setting

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

	0	TBY	Tannal Address	Tanaa	1 Sanzas	Tunnal	Bertinstion	Verneline	Tatarral	Patriar	Decarintia
VLAN			Tumer Autress	Tume	I Source	1 onner	Destination	Meeparive	THEFTAR	Beliles	Description
dvanced Network								100			
irewall											Add
PN Tunnel											
GRE	GR	E Rou	ıte								
OpenVPN Client	On	Tunnel	Index		Destination	Addres	s	Desc	ription		
PPTP/L2TP Client		1		T							
IPSec	_										644
Iministration											Aud
ebugging											
ogout											

Table 3-13 "GRE" Instruction

	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 a public IP address
Keep alive	GRE tunnel keep alive to keep GRE tunnel connection.
Interval	Keep alive interval time.
Retries	Keep alive retry times. After retry times, GRE tunnel will be re-established.
Description	

Step 1 Please click "save" to finish.

----End

3.5.2 OpenVPN Client Setting

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

Status	OpenVPN Client			Router
Basic Network				
WLAN	Client 1	Client 2		
Advanced Network	Basic	Advanced Keys Status		
Firewall	Start with WAN			
VPN Tunnel				
GRE	Interface Type	ION •		
OpenVPN Client	Protocol	UDP Y		
PPTP/L2TP Client	Server Address/Port		1194	
IPSec	Firewall	Automatic 💌		
Administration	Authorization Mode	TIS		
Debugging	Authorization Houe			
Logout	Username/Password Authentication			
	HMAC authorization	Disabled 💌		
	Create NAT on tunnel	8		
	Start Now			
			S	ave Cancel

Figure 3-17 OpenVPN Setting GUI

Table 3-14 "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.
Firewall	Auto, External only and Custom are optional
Authorization Mode	TLS, Static key and Custom are optional.
User name/Password Authentication	As the configuration requested.
HMAC authorization	As the configuration requested.
Create NAT on tunnel	Configure NAT in Openvpn tunnel.



Save Cancel

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

Status	OpenVPN Cli	ent			Router
Basic Network	Client 1	Client 2			
WLAN	Basic	Advanced	Keys	Status	
Advanced Network					
Firewall	Client is not running	or status could not be	e read.		
VPN Tunnel	Chart Mauri				Refresh Status
GRE	Start NOW				
OpenVPN Client					
PPTP/L2TP Client					
IPSec					
Administration					
Debugging					
Logout					
Logout					

Save Cancel

Parameter	Instruction
Status	Check Openvpn status and data statistics.

Step 1 Please click "save" to finish.

----End

3.5.3 VPN Client Setting

Step 1 Please click "VPN Tunnel> VPN Client" to check or modify the relevant parameter.

Status	L21	P/PPTP	Basic										
asic Network	On A	Protocol	Name	Server	r:		Usern	ame Po	assword	Firewall	Default	Local	[P
idvanced Network		1070	1							1.0	Koute		
rowall	۲	L2TP •									U		
PN Tunnel													Add
GRE													
OpenVPN Client	L21	P Advan	ced										
PPTP/L2TP Client	On 🔺	. Name	Accept DE	S III	IRU	Tunnel	Auth	Tunnel	Password	Custon (Options		
IPSec		A PARAZARONI	NO	•									
dministration													Ad
ebugging													
gout	PP.	TP Advar	nced										
	On 🛦	. Name	Accept DM	S ITU	REU	TPPE	IIPP1	E Statefu	d Custon	Options			
	2		NO	•				W					
													Ad
	sci												
	50	LUGLE											
	On 🔺	. Name 1	Name 2	Policy	•	Descrip	tion						
				FAILO	VER 🔻								
													Ad
											Sav	e	Canc

Table 3-15 "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 3-16 "L2TP Advanced" 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 3-17 "PPTP Advanced" Instruction

	· · · · · · · · · · · · · · · · · · ·	
On	PPTP Advanced enable	
Name	PPTP Tunnel name	
Accept DNS	As the configuration requested.	
ΜΤυ	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 3-18 "SCHEDULE" 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 1 Please click "save" to finish.

---End

3.5.4 IPSec Setting

11115	IFOLC				
sic Network	IPSEC 1 IP	SEC 2			
LAN	Group Setup	Basic Setup	Advanced Setup		
vanced Network					
rewall	Enable IPSec				
n Tunnel	IPSec Extensions	Normal	•		
VPN Client	Local Security Gateway	3G Cellular	Ŧ		
IPSec	Interface				
ministration	Subnet/Netmask	192.168.1.	0/24	ex. 192.168.1.0/24	
bugging	Local Security				
nout	Firewalling				
gour	Remote Security Gateway IP/Domain				
	Remote Security Group Subnet/Netmask	10.0.0/24	ł	ex. 192.168.88.0/24	
	Remote Security Firewalling				

3.5.4.1 IPSec Group Setup

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

Status	IPSEC			Router
Basic Network				
WLAN	IPSEC 1 IP	SEC 2		
Advanced Network	Group Setup	asic Setup Advanced Setup		
Firewall	Enable TPSec	a		
VPN Tunnel				
GRE	IPSec Extensions	Normal		
VPN Client	Local Security Gateway	3G Cellular 🔻		
IPSec	Interface			
Administration	Local Security Group Subnet/Netmask	192.168.1.0/24	ex. 192.168.1.0/24	
Debugging	Local Coqueity			
Logout	Firewalling	8		
	Remote Security Gateway IP/Domain			
	Remote Security Group Subnet/Netmask	10.0.0/24	ex. 192.168.88.0/24	
	Remote Security Firewalling	8		
				Save Cancel

Table 3-1 " IPSec Group Setup" Instruction

parameter	Instruction
IPSec Extensions	Support Standard IPSec, GRE over IPSec, L2TP over IPSec
Local Security Interface	Defined the IPSec security interface
Local Subnet/Mask	IPSec local subnet and mask.
Local Firewall	Forwarding-firewalling for Local subnet
Remote IP/Domain	IPsec peer IP address/domain name.
Remote Subnet/Mask	IPSec remote subnet and mask.
Remote Firewall	Forwarding-firewalling for Remote subnet

Step 2 Please click "save" to finish.

3.5.4.2 IPSec Basic Setup

Step 1 Please click "IPSec >Basic Setup " to check or modify the relevant parameter.

Status	IPSEC		Router
Basic Network	IPSEC 1 IP	SEC 2	
Advanced Network	Group Setup	Advanced Setup	
Firewall	Keving Mode	IKE with Preshared Key	
VPN Tunnel	Phase 1 DH Group	Group 2 - modp1024	
GRE	Phase I bit Group	Gloup 2 - Houp 1024	
VPN Client	Phase 1 Encryption	3DES (168-bit) *	
IPSec	Phase 1 Authentication	MD5 HMAC (96-bit)	
Administration	Phase 1 SA Life Time	28800 seconds	
Debugging			
Logout	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	
	Preshared Key		
			Save Cancel

Table 3-2 " IPSec Basic Setup" Instruction

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

Step 2 Please click "save" to finish.

3.5.4.3 IPSec Advanced Setup

Step 1 Please click "IPSec >Advanced Setup " to check or modify the relevant parameter.

Status	IPSEC	Router
Basic Network		
WLAN	IPSEC 2	
Advanced Network	Group Setup Basic Setup Advanced Setup	
Firewall	Anaressive Mode	
VPN Tunnel	Aggressive Houe	
GRE	Compress(IP Payload Compression)	
VPN Client	Dead Bear	
1PSec	Detection(DPD)	
Administration	ICMP Check	
Debugging	100 car Cardena Carlinare	
Logout	1 1	
	IPSec Custom Options 2	
	IPSec Custom Options 3	
	IPSec Custom Options 4	
		Save Cancel

Table 3-3 " IPSec Advanced Setup" Instruction

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

Step 2 Please click "save" to finish.

3.6 Administration

3.6.1 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.

Status	Router Identif	ication	Route
Basic Network			
Advanced Network	Router Name	Router	
Firewall	Hostname	Router	
VPN Tunnel	nostname	Noues	
Administration	Domain Name		
Identification			
Time			
Admin Access			
Scheduler Reboot			
SNMP			
M2M Settings			
Configuration			
Logging			
Upgrade			
Reboot			
Debugging			
Logout			

Save Cancel

Figure 3-2 Router Identification GUI

Table 3-4	"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 character, it is the domain of WAN, no need to configure for most application.

Step 2 Please click "save" to finish

3.6.2 Time Setting

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



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

Step 2 Please click "save to finish.

3.6.3 Admin Access Setting

Step 1 Please click "Administrator>Admin" 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.

WebAccess	Nour	20
Local Access	HTTP •	
HTTP Access Port	80	
IIII ACCOFTOR		
Remote Access	Disabled *	
Allow Wireless Access	8	
Open Menus		
Status		
Basic Network		
Firewall		
VPN Tunnel		
Advanced Network	0	
Administration		
Debugging		
Password		
Password		
(re-enter to confirm)		
	WebAccess Local Access HTTP Access Port Remote Access Allow Wireless Access Status Basic Network Firewall VPN Tunnel Advanced Network Administration Debugging Password (re-enter to confirm)	WebAccess Local Access HTTP • HTTP Access Port 80 Remote Access Disabled • Allow Wireless Access • Open Menus • Status • Basic Network • Firewall • Advanced Network • Advanced Network • Debugging •

Figure 3-4 Admin Setting GUI

Step 2 Please click save iron to finish the setting

3.6.4 Schedule Reboot Setting

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

Status	Scheduler Re	aboot	Rout
Basic Network Advanced Network	Enabled		
Hrewall	Time	1:00 AM 🔹	
Administration	Days	Sun Mon Tue Wed Thu Fri Sat Everyday	
Identification			
Time			
Admin Access			
Scheduler Reboot			
SNMP			
M2M Settings			
Configuration			
Logging			
Upgrade			
Reboot			
ebugging			
ogout			
		Save	Cance

Figure 3-5 Scheduler Reboot Setting GUI

Step 2 Please click save iron to finish the setting

3.6.5 SNMP Setting

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

Status	SNMP Settings		Router
Basic Network			
Advanced Network	Enable SNMP	0	
Firewall			
VPN Tunnel	Port	161	
Administration	Remote Access		
Identification	Remote Access		
Time	Allowed Remote	(antional: au "1 1 1 1" "1 1 1 0/24" "1 1 1 1	
Admin Access		(opuonal; ex. 1.1.1.1, 1.1.1.0/24, 1.1.1.1 - 2.2.2.2)	
Scheduler Reboot	Location	ros (for	
SNMP	LOCACIÓN	1000s	
M2M Settings	Contact	admin@router	
Configuration	R0 Community	rocommunity	
Logging			
Upgrade			
Reboot			
Debugging			
Logout			
			Save Cancel

Figure 3-6 SNMP Setting GUI

Step 2 Please click save iron to finish the setting

----End

3.6.6 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		Router
Basic Network			
Advanced Network	M2M Enabled	0	
Firewall	Fail Ashian	Desired MOM	
VPN Tunnel	Fall ACTION	Kestart M2M	
Administration	Device ID		
Identification			
Time	M2M Server/Port		
Admin Access	Heartbeat Intval	10 (seconds)	
Scheduler Reboot	Heartheat Retry	10 (Range:10-1000)	
SNMP	india di contracti (
M2M Settings			
Configuration			
Logging			
Upgrade			
Reboot			
Debugging			
Logout			
			Save Cancel

Step 2 Please click save iron to finish the setting

----End

3.6.7 Configuration Setting

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

Status	Backup Configur	ation	Router
Basic Network Advanced Network Firewall	Router_Router-4223_m0650 Link	2d .cfg Backup	
VPN Tunnel			
Administration	Restore Configur	ation	
Identification	Calash Han and Saure Kan King		
Time	Select the configuration file t	Bestore	
Admin Access	AGINALT PRODUCT	10.000	
Scheduler Reboot			
SNMP	Doctore Default	Configuration	
M2M Settings	Restore Default	configuration	
Configuration	Select	 Save 	
Logging			
Upgrade			
Reboot			
Debugging	Total / Free NVRAM:	32.00 KB / 14.11 KB (44.10%)	
Logout			



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

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

3.6.8 Logging 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	Syslog			Routa
Basic Network				
Advanced Network	Log Internally	2		
Firewall	Log To Remote System	(T)		
VPN Tunnel	Log to Remote System	1000 (2002)		
Administration	Generate Marker	Every 1 Hour •		
Identification	Limit	60 (messages p	er minute / 0 for unlimited)	
Time				
Admin Access				
Scheduler Reboot				
SNMP				
M2M Settings				
Configuration				
Logging				
Upgrade				
Reboot				
Debugging				
Logout				
				Save Cancel

Figure 3-9 System log Setting GUI

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

3.6.9 Firmware upgrade

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

Status	Upgrade Firmware
Basic Network Advanced Network Firewall	Select the file to use: 这择文件 未选择任何文件 Upgrade
VPN Tunnel	After flashing, erase all data in NVRAM memory
Administration	Current Version: Router-4.2.2.3-160329-114644
Identification	Free Henory: 53.52 MB (aprox. size that can be buffered completely in RAM)
Time	
Admin Access	
Scheduler Reboot	
SNMP	
M2M Settings	
Configuration	
Logging	
Upgrade	
Reboot	
Debugging	
Logout	

Figure 3-10 Firmware Upgrade GUI

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

3.6.10 System Reboot

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

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

3.7 Debugging Setting

3.7.1 Logs Setting

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

Status	Logs	
Basic Network	View	
Advanced Network	Download Lon File	
Firewall	Dominolog Log The	
VPN Tunnel		Find
Administration		
Debugging	» Logging Configuration	
Logs		
Ping		
Trace Route		
Longut		
toguat		

Figure 3-11 Logs GUI

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

----End

3.7.2 Ping Setting

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

Status	Ping						Router
Basic Network							
Advanced Network	IP Address	baidu.c	om	Ping			
Firewall	Ding Count	10					
VPN Tunnel	Ping Counc	10					
Administration	Packet Size	56	(bytes)				
Debugging							
Logs							
Ping	Seq Address			RI Bytes	TTL	ETT (as)	+/- (ns)
Trace Route							
Logout							

Figure 3-12 Ping GUI

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

3.7.3 Trace Setting

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

Status	Trace Route							Router
Basic Network								
Advanced Network	IP Address			Trace				
Firewall	Maximum Hops	20						
VPN Tunnel	Thuxing thops	20						
Administration	Maximum Wait Time	3	(seconds per hop)					
Debugging								
Logs								
Ping.	Nop Address				min (ms)	max (ms)	avg (ms)	+/- (ms)
Trace Route								
Logout								

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

----End

3.8 "RST" Button for Restore Factory Setting

If you couldn't enter web interface for other reasons, you can also use this way. For R100 Series, "RST" button is on the left or Ethernet port, for R100 Series, the button is on the left of NET light. 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 restored to factory.

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

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

3.9 Appendix (GPS&OpenVPN only)

3.9.1 GPS Setting

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

Status	GPS		Router
Basic Network			
Advanced Network	GPS Mode	Client 🔻	
Port Forwarding	Data Format	M2M ENT Y	
Port Redirecting	Data Format		
DMZ	Server IP/Port	192.168.1.Z	: 40002
Triggered			
Serial App.	Heart-Beat Content		
GPS	Heart-Beat Interval	5 (seconds)	
UPnP/NAT-PMP			
Bandwidth Limiter			
VRRP			
Static DHCP			
Firewall			
VPN Tunnel			
Administration			
Debugging			
Logout			

Figure 3-14 GPS Setting GUI

Table 3-6 "GPS" Instruction

parameter	Instruction
GPS Mode	Enable/Disable
GPS Format	NMEA and M2M_FMT(WLINK)
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

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

Save Cancel

3. GPS data description

Field No.	Name	Format	Example	Description		
1	Router ID	String	0001_R081850 ac	0001 customizable product ID. _R router indicator. 081850ac Last 8digits of routers 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 mm	11356.626179	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 of Precision		
13	gps_MSL	numeric	97.5	MSL Altitude, units is meter.		

3.9.2 OpenVPN Demo (TAP Mode)

1) Network topology



2) OpenVPN Server Config Demo

Status	OpenVPN Server (Configuration	Router
Basic Network	Convor 1 Co	-	
WLAN	Basic	idvanced Keys Status	
Advanced Network	Sectore Control of Con		
Firewall	Start with WAN		
OPE CPE	Interface Type	TUN ¥	
OpenVPN Server	Protocol	UDP V	
OpenVPN Client	Port	1194	
VPN Client	Firewall	Automatic X	
Administration	Authorization Mode		
Debugging	Authorization Mode	ILS Y	
Logout	Extra HMAC authorization (tls-auth)	Disabled •	
	VPN subnet/netmask	10.8.0.0 255.255.255.0	
	Start Now		
			Save Cancel
Status Basic Natwork	OpenVPN Server (Configuration	Router
WIAN	Server 1 Se	ver 2	
Advanced Network	Basic	dvanced Keys Status	
Firewall	Dell Internal	0 (in minutes 0 to distribut)	
VPN Tunnel	Poli Interva		
GRE	Push LAN to clients		
OpenVPN Server	Direct clients to redirect Internet traffic	0	
OpenVPN Client	Respond to DNS		
VPN Client	Respond to bits		
Administration	Encryption cipher	Use Default	
Debugging	Compression	Adaptive •	
ogout	TLS Renegotiation Time	-1 (in seconds, -1 for default)	
	Manage Client-Specific Options	8	
	Allow User/Pass Auth	0	
	Custom Configuration		
	Start Now		A

Save Cancel

Status	OpenVPN Ser	ver C	onfigu	ration				
Basic Network	Danimi t		and the					
WLAN	Basir	Ser	dvanced	Ken	-	Status		
Advanced Network	- unarc	-	arenteet.	integration of the second seco	-	Juctury		
Firewall	For help generating	keys, re	efer to the	OpenVPN H	owto.			
VPN Tunnel			yyyyyypco		001140700	(yogwjooch re	DUILVIMCAWEAR4OB+1C89JAUBUIV	-
GRE			HQ4EFg	QUh18dizrp+Z	C7mO8L/u	QFORWqOjgw	gcYGA1UdIwSBvjCBu4AUh18dzrp	-
OpenVPN Server			RDELMA	KGA1UEBXMC	U10xDTALE	I GWGZERCZAJE I GNVBAOTBFRI	U1QxFDASBgNVBAsTC29wZW52cG50	
OpenVPN Client	Certificate Auth	ority	ZXNOMR	AWDgYDVQQ	DEwdURVN GV4 YW1M	UIENBMRAWD	g YDVQQpEwdFYXN5UINBMR8wHQ Y3KoZ	I
VPN Client			/zANBgk	ghkiG9w0BAC	SFAAOCAC	EASbzApdBK2	v7bz8wzryoX2yZ6XYJ3hWz9o0WJ	
Administration			F73ISsnD 03R5304	IZUJKUgb5sfPl -MXaiSeN8vvt	JW4W3Uir OICPbloK5	TdBwLlQQkpjh cvaahFaaOoel	30hAyGdgfQP7fxJ2J0xI6Mkr)+iceSNUFA1U1Fm]A0viupR6S	-
Debugging			DECT		TERC		nt na cina n'a ém	10
Logout	Server Certificat	e	MIIBCAK wNNr8dł ofqaknbł VkgHHcz +b/wEw W9Tugc END	CAQEA8FSJV; iZR8kKhpKW; iKZb/Wcm61 CTJBNjaoore7 O41NMBO6dv ABXoR0kgb1; DH PARAMET	pA0MKwB+ z9sRpSXfE8 IpwBxeBoz K50c2/Guh /JB95TsdVa p7awbITgp ERS	GShyF17hN4N IoX/Idscto61fr JARVIuG1NSAC LIr+tHIP1qQ0/ ad8k2Qgi8CWf HjL1gP/gwIBA	MNM/kI0kYog+d5NEsp+Y7HY6+tn1 18I2pLMvIs0QEbtEVh53nkWwV AAQpk2cqW/LVA+3Yh64g05pHzsd JhBeRG9+paVjdc2vQmkVh5TA +oX8Xt9vm8yf/Ul6UBLXFF5U0SfV g==	
	Server Key Diffie Hellman parameters		DCBkTEI A1UEChT Q0ExED/ Z55jb22/ BaAwEQ u2rtX+SJ v4IC88af GF5id8CI 45Js22tC v1rBnpt/ X5SyLo: eLbhnv// K1+Sula2 94iYUdy; GoZ3G/c E55gM/jJ EV/IP4UL	MAKGA1UEB MEVEVTVDEL COQDh17dy/X YDVR0RBA00 WR03BA00400 H-A4Hu52J85 f7tG5hmg4rH 2W90-y2wW 2Y10xNGnoKJ N6wKBg0Die, 2J170hxVEvLx 255cWaWcPf ISRx47yVb2D6 S7E42Meqm72	hMCQ04xC. IMBIGA1UE B0Vhc3lSU 2A5jATBg1 vcIIGc2Vyd sLWUD7/JC th9j5Fx2NR IbLWgLC2r Xs0d25Kff K05015aj00 WGtoN7aM /9uq+3klV (35Vl5V00 Rg1Y0y2Mi EHuJ05vv6i Dv2/LW5fb /nDV2/LW5fb	zAJBgNVBAgT. CxMLb3BlbnZv DExHzAdBgkql VIHSUEDDAKB mVVMA0GCSq IxbY6Hld0J2CS Elm84MlvZ+AA pemVQranXau W0vRZVhD095 lmRCdKrACaisd Bu4X3D0SfnH kRCdKrACaisd Bu4X3D0SfnH kRCdKrACaisd Bu4X3D0SfnH zZNg8b0HLV0 Ld3Jr40HV/e lq2lADg6+/jb.	AkdEMQswCQYDVQQHEwJTWJENMAsG /bnRlc3QxEDAOBgNVBAMTB1RFU1Qg kiG9w0BCQEVVEHRIc3RAZXhhbXBs ggrBgEFBQcDATALBgNVHQ8EBAMC GSIb3DQEBCwUAA4IBAQApMOqOVbJ7 ibH9IHX2nkrOACB2S11fbMsCN uaxsp4YwD7eeOvfne1dKiq0Ld 2b982/2j3/h+qp8LJ8iZI2h0V nx8Gc1s8eift.d0N3ZuCO4zMKyp3 mcg2r1x0umasbsc2nrentertzA19x Lt5KrgP3plywdguJhXIAMk1S9c LBwVDFdbhHJZbvb+QJ08Nf0JYag PCtkkgFLrbGXMEkQCR9+z EirC2M3/VxoW+Hq2TGQKBgBxp BwbMTBN6EAqUM97hK9wNUX/Wn YguUa4h0PWSbYhrloxGJ2bWG AoGAZw+VJSEpvvBwnOg83r8	•

3) OpenVPN Client Config Demo

Status	OpenVPN Client				Route
lasic Network					
VLAN	Cient 1	Rent 2	Philippin		
Advanced Network	Basic	Advanced Neys	Status		
irewall	Start with WAN	×			
PN Tunnel	Take fees Tone	77.001			
GRE	Interface Type	TON +			
OpenVPN Client	Protocol	UDP			
PPTP/L2TP Client	Server Address/Port	211.165.59.162		1194	
IPSec .	Firewall	Automatic 🔻			
dministration	Authorization Mode	TIS .			
ebugging		10			
ogout	Osername/Password Authentication	120			
	HMAC authorization	Disabled 🔹			
	Create NAT on tunnel	×			
	Start Now				
					mo Cancol

Status	OpenVPN Client	Router
Basic Network	Cleart 1 Cleart 2	
WLAN	Bacir Advanced Keys Status	
Advanced Network	Done. Developming Reas	
Firewall	Poll Interval 0 (in minutes, 0 to disable)	
VPN Tunnel		
GRE	traffic	
OpenVPN Client	Accent DNS	
PPTP/L2TP Client	configuration Disabled V	
IPSec	Encryption cipher Use Default 🔻	
Administration	Compression Adaptive V	
Debugging	- Augure -	
	TLS Renegotiation Time -1 (in seconds, -1 for default)	
Logout	Connection retry 30 (in seconds; -1 for infinite)	
	Verify server certificate (tls-remote)	
	Custom Configuration	
	Start Now	

Save Cancel

Status	OpenVPN Client					Router
Basic Network	Charles 1	Client 2				
WLAN	Clent 1	Client 2	Koura	Chattain		
Advanced Network	DdbK.	Auvanceu	Reys	Status		
Firewall	For help generating keys, re	efer to the OpenVF	N HOWTO.			
VPN Tunnel		1-002-0010-25-00	The Color Discontinues and T		nd a link life (Ala ad als Vici int	
GRE		Ycvq1hixgw+	Ycvq1hixqw+8EJy73Eeqip42E5SL7Q1kEV9K1U28oZYYCO59b155KPqtAoGBAKwr			
OpenVPN Client		RmzplwF2jvy1 gc5R+3AgKB6	isgV6W1A4VkII67sTF 5W/+oaNfP7mMHE5gk	VOL9LXgI/VYY7CihlKr GPe01Vv34Ncu+B1E	0aIZ8d0ZSIMBH976 89arWBMIZ5BWignWAlKDf	
PPTP/L2TP Client	Certificate Authority	e1wAEHzWXF	e1wAEHzWXFrxb9z25)RZZ7AHnCAzc4o4F4)YrcpHAoGAA15IOjfrcNakvTs8o1dZ EQKAKWrl3QbhJIWaMOjSho65EQFXUv9GCVkr5g39mY1tR+HZzNacez9tnKfiuHaG HhnX3fNeBREQRue8P+vQC9Udc9Bucrwq5gURZbOC0aVgE4fHvPJgcq27IIVjrZvR			
₽Sec (HhnX3fNeBRE				
Administration		uHpog1CBOD		-		
Debugging	Client Certificate	CSGGSIDSDQEJARYQGGYZGEBIeGFtcGxILmNvbYJJAOEnt3L9rYDmM8MGA1UdJQQM			*	
Logout		MAGCCSGAQQUFWMGHASAF10DWQEAWIHgUASBgNVHKEEC2AJgg0j0GinQMAGG CSqGSIb3DQEBCWUAA4IBAQ8988T8yPS6d2uwNtymscEEL8E5e3SSuGdvJR2ORn ZK6T9taJVaWCohhkgxe5yNlyX7Da12oyggrgpxUT5FzE3LynbcCsc37ovWyhC0re KCcbJWkYFgDpzxVrhob6up+R3L8TIbSCtirwKt53/q+uAaWatVyrvgzPsYCr3J/3 hq8nV2gdc02UhGwk+o06jp23bLNRvINgLYUQ0K7m9FqYLXdTuDiVV7ZgnpdWs8nX 4umRHpGWTJM2fnVEMIx45rD6ELQBbLDYDMeWGAQ0/fM62B+qI9VmgusKremgDRZI 8NgjdyvOv0n7WRtnWJ/ZhRFBmWhUSaIn3ai+szlX/ END CERTIFICATE				
	Client Key	QKIWarPufRC bH9pFqrAbvq; WIuJfct+L+DJ yJyWpCouTP' HQ4EFgQUh1 +ZC7m08L/ut RDELMAKGA1 ZXN0MRAWDQ hvcNAQkBFhE	MJqVILzbal92+69cx3r zcxl+Yh/9WGwvRNUD Ef3TEKFTBij5qNK7B90 YcGwxYQI0P14C76xyH 8dizrp+ZC7m08L/uQf QF0RWq0JihgZekgZQ UEBxMCU1oxDTALBgI yDVQQDEwdURVNU 10ZXN0QGV4YW1wb0	q1PMpYpHtzuxuW0X ye9B96skashD03286 y0C695Lf10M7mPNG1 y0wf66cHY08mcv1M GRWq0jgwgcYGA1U wgZExCzA3BghVBAY WBAoTBFRFU1QxFD/ IENBMRAwDgYDVQQ JUUY29tggkA4Se3cv	4Xh3e7r37b7ppvGTMq nUNV0+peNNruuySwHTk dhejA4kx1B2TiJJ/Pu CAwEAAaOB+TCB9jAdBgNV dIwSBvjCBu4AUh18dizrp TAkNOMQswCQYDVQQIEwJH ASBgNVBASTC29wZW52cG50 DewdFYXNSUINBMRSwHQYJKoZI 19gOYwDAYDVR0TBAUwAwEB	•
	Start Now					