

HYTTHDRM100 3G/4G wireless router user guide

V1.01



Content

Content	2
Chapter 1 Install machine	4
1.1 Overview	4
1.2 Package list.....	4
1.3 Dimensions and mounting holes (Unit : mm)	5
1.4 LED Indication	5
1.5 Adapter,Atenna and SIM card	6
Chapter 2 Installation and configuration	6
2.1 Wiring method.....	6
2.2 Configuration	8
2.2.1 IP address setting	8
2.2.2 Routing configuration management UI	8
2.2.3 Working mode.....	8
2.3 Network setting	9
2.3.1 WAN setting	9
2.3.2 LAN setting.....	13
2.3.3 DHCP client list.....	13
2.3.4 VPN setting.....	14
2.3.5 Advanced routing configuration	17
2.3.6 QoS setting.....	18
2.3.7 IPv6 setting.....	19
2.3.7 DTU setting.....	19
2.3.8 SNMP setting.....	20
2.3.9 TR069 setting	22
2.4 WIFI setting	22
2.4.1 Basic setting	22
2.4.2 Advanced setting.....	23
2.4.3 Security setting	24
2.4.4 Linked device list.....	25
2.4.5 Wireless status.....	26
2.5 Firewall.....	26
2.5.1 MAC/IP/Port filter	26
2.5.2 System security setting	27
2.5.3 Content filtering.....	28

2.5.4	Port forwarding	29
2.5.5	Port trigger	31
2.5.6	DMZ.....	32
2.6	SMS setting	32
2.6.1	Inbox.....	32
2.6.2	Send SMS	33
2.6.3	Advanced setting.....	33
2.7	DDNS	34
2.8	GPS	34
2.8.1	GPS status	34
2.8.2	GPS information unload setting.....	35
2.9	System management.....	36
2.9.1	Management.....	36
2.9.2	Firmware updating.....	37
2.9.3	Setting management.....	37
2.9.4	System information.....	38
2.9.5	System status	39
2.9.6	System command.....	39
2.9.7	System log	40

Chapter 3 Environmental performance..... 41

Chapter 1 Install machine

1.1 Overview

Thank you for choosing IOT routing broadband products!

This manual will guide you how to use the 3G/4G LTE router and connect to the internet.

HYTTHDRM100 should be installed correctly, in order to get good performance. Usually, the installation should be under the guidance of engineers.

※Note. Please install the router and plug SIM card without power supply.

1.2 Package list.

Recommend you reserve the package box, in order to re-use when transfer. The box is environment protected material.

※HDRM100 3G/4G LTE router, 1 unit.

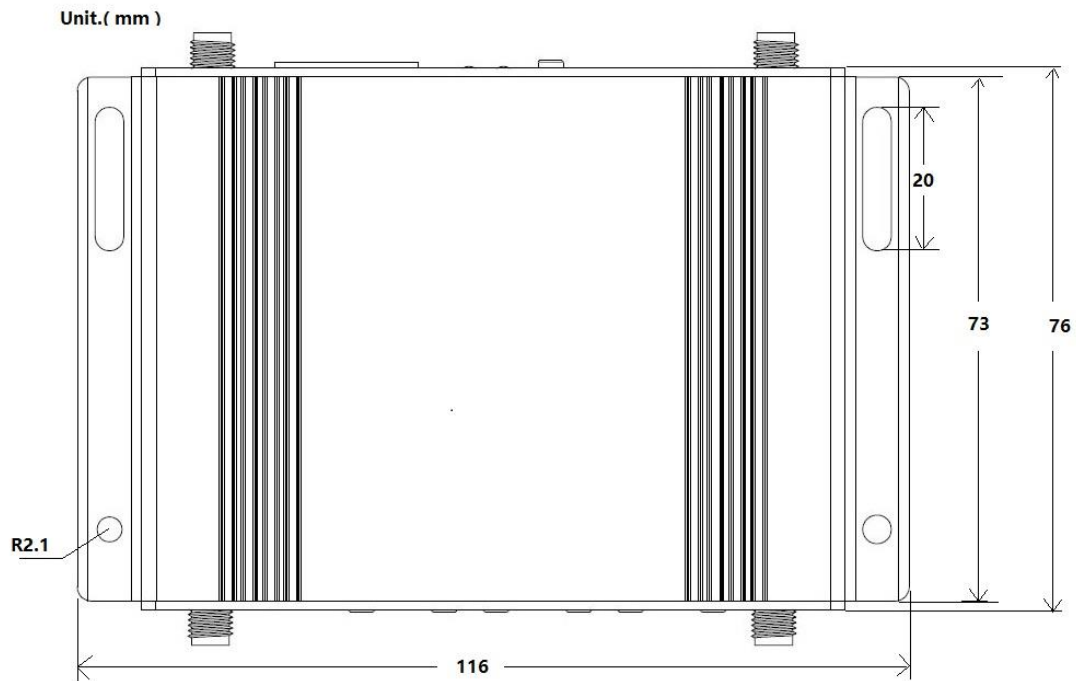
※4G LTE antenna, 2 units (Or 1 unit.)

※WIFI antenna, 2 units

※GPS antenna, 1 unit (Optional)

※ Standard 12V/1A power adapter, 1 unit. Note. If you want to choose other power adapter, such as Vehicular power supply .Welcome to inquiry our colleague in advance.

1.3 Dimensions and mounting holes (Unit : mm)



1.4 LED indication.

For the status of LED, please refer to the following description.

LED	Operating Status	Description
RSSI	Green	Strong 4G LTE signal
	Red	Weak 4G LTE signal
System	Every one second on	System Normal
	off	System abnormal or rebooting.
NET	Every three second on	Registered without data transmission
	Every one second on	Registered with data transmission

	off	Un-registration
LAN1	On	LAN1 device available
	Every three second on	Data transmission
	off	LAN device unavailable
WAN/LAN2	on	WAN device available
	Every three second on	Data transmission
	off	WAN device unavailable

1.5 Adapter, Antenna, SIM card.

Adapter in box is Standard power adapter +12V/1A. But customers can choose different one according to the wide power supply range of HYTTHDRM100 Series router, the input range is from DC 5V/2.5A to DC 48V/0.5A

HYTTHDRM100 Series router requires 2 units of 4G antenna, standard female SMA connector, 50 ohm impedance; 2 units WIFI 2.4G antenna, standard male SMA connector, 50 ohm impedance.

HYTTHDRM100 Series router uses Push-button SIM card holder, supports 1.8V/3V SIM/USIM card, ESD protection inside.

Chapter 2 Installation and configuration

2.1 Wiring methods

Insert the SIM card into the SIM card slot beneath the HYTTHDRM100 Series 4G LTE router. Press carefully until it 'clicks' into place.



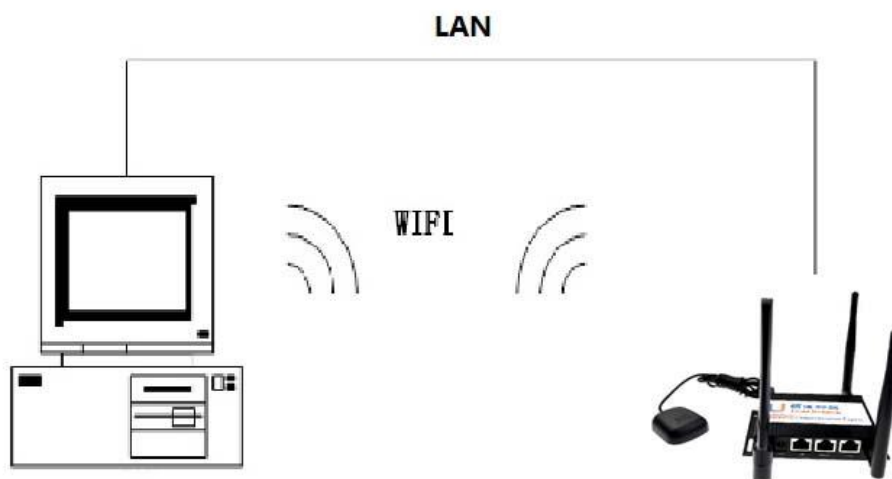
Plug the power adapter into the AC mains and plug the DC cable firmly into the +5V/2.5A~+48V/0.5A DC input of the HYTTHDRM100 Series 4G LTE router. Power light is working. User should choose PPP or NDIS dialing mode. It will start to work automatically.

Before configuration, HYTTHDRM100 Series router should be connected to PC via Ethernet cable or Wi-Fi network.

1) With Ethernet cable. One connector of Ethernet cable insert to LAN port, another connector of Ethernet connects to PC Ethernet port.

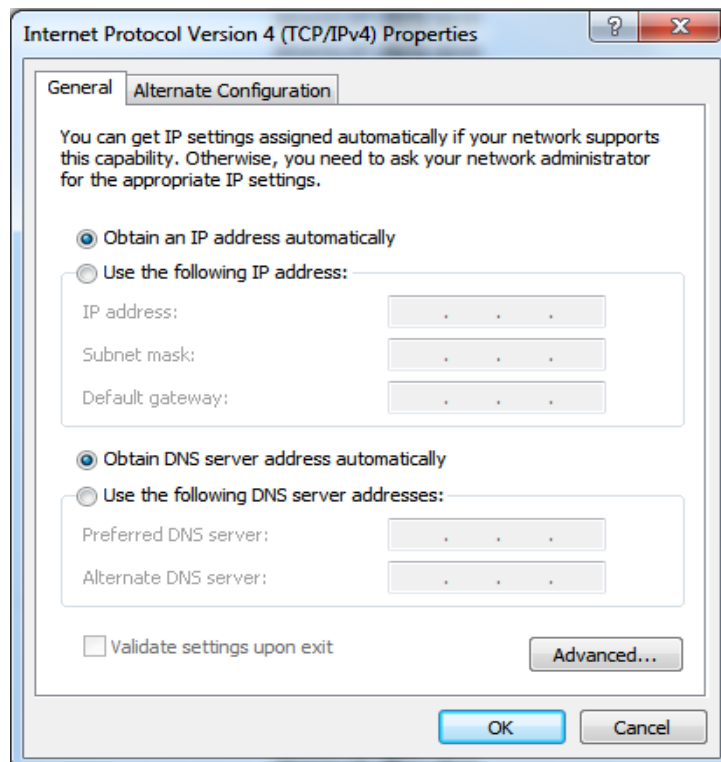
2) With Wi-Fi network. SSID of HYTTHDRM100 SERIES is "XXXXXXXX" default without password.

3) If user want to connect WLAN via cable. Please connect to HYTTHDRM100 WAN port. And setup parameter of WLAN connect method.



2.2 Configuration.

2.2.1 IP address setting.



2.2.2 Routing configuration management UI.

PC could access the configuration pages after connected to HYTTHDRM100 Series router via IE explorer or other browser tools. Default IP address is 192.168.0.1

There have 8 pages for setting, Operating mode configuration, network setting, 2.4G WIFI setting, firewall setting, SMS setting, DDNS setting , GPS setting, management and Status pages. You can get details information from each page.

Default user name is **admin** and the default password is **admin**

2.2.3 Working mode.

It can provide two operation mode, Bridge mode and Gateway mode.


Bridge is two layer network equipment. It's a device for connecting different network segments.

HYTTHDRM100 default operation mode is Gateway mode. It can be used to provide

network compatibility functions such as protocol conversion, routing, data exchange and so on when interworking between networks with different architectures or protocols.

The default configuration parameters of the system are as follows.

Operation Mode Configuration

 You may configure the operation mode suitable for you environment.

Bridge:
All ethernet and wireless interfaces are bridged into a single bridge interface.

Gateway:
The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

NAT Enabled:	<input type="text" value="Enable"/>
TCP Timeout:	<input type="text" value="180"/>
UDP Timeout:	<input type="text" value="180"/>
ALL LAN Enabled:	<input type="text" value="Disable"/>

NAT enable. Open or close the network address translation.

TCP Timeout. TCP Send Protocol timeout retransmission, timeout setting.

UDP Timeout. UDP Send Protocol timeout retransmission, timeout setting.

ALL LAN enable. After this function is enable, the WAN port can be switched to LAN port. HYTTHDRM100 will be switched to 2 LAN ports. The default is 1 WAN/1 LAN port.

2.3 Network setting.


2.3.1 WAN setting.

WAN connection types include. Automatic, Static IP, dynamic IP, PPPoE, 3G /4G PPP, 3G /4G NDIS.

Option 1. Static IP

Usually, this option will be used in optical networks. The service provider will provide the IP address, subnet mask, gateway and DNS information. Please add the configuration parameters of service providers to the HYTTHDRM100.

Wide Area Network (WAN) Settings

 You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type:	STATIC (fixed IP)
Static Mode	
IP Address	192.168.1.5
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Primary DNS Server	192.168.1.1
Secondary DNS Server	192.168.1.1
MAC Clone	
MAC Clone Setting	Disable

IP address. User owner IP address


Subnet mask. User owner subnet mask.

Default gateway. User owner gateway.

Option 2. Dynamic IP

Dynamic IP is DHCP service. Assign the IP address to the internal network or the network service provider automatically. Connect Ethernet cable to WAN port, configure as follow. Router uses this dynamic IP as WAN connection type.

Wide Area Network (WAN) Settings


 You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type:	DHCP (Auto config)
DHCP Mode	
Hostname (optional)	
MAC Clone	
MAC Clone Setting	Disable

Option 3. PPPoE

Usually, the ADSL service will use this option. PPPoE connection to the Internet service provider that it should has service provider name, username and password.

Wide Area Network (WAN) Settings

 You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type:		PPPoE (ADSL)
PPPoE Mode		
User Name	pppoe_user	
Password	*****	
Verify Password	*****	
Operation Mode	Keep Alive	
	Keep Alive Mode: Redial Period	50 seconds
	On demand Mode: Idle Time	minutes
MAC Clone		
MAC Clone Setting		Disable

User name. User name provided by ISP provider

Password. Password provided by ISP provider


Option 4 : 3G / 4G PPP

Using 3G / 4G PPP mode, users need to insert the SIM card into the card slot before booting. And then click the confirmation button to access the internet.

Note.

HYTTHDRM100 4G router system is set defaults parameters of the local operator network, such as user name, password, APN, access number(like *99#), DNS, etc. If we did not match the equipment data from network operators user data update. please contact with the operator and confirmed the parameters of SIM/USIM card and set the correct parameters on the HYTTHDRM100 settings interface to ensure normal access to the Internet.

Wide Area Network (WAN) Settings


 You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type:		3G/4G PPP
3G/4G PPP		
APN		
PIN		
Dial Number		
Username		
Password		
MAC Clone		
MAC Clone Setting		Disable

Option 5 : AUTO

Automatically connect to the Internet using the 4 options 1~4. You can choose the static IP or DHCP in the preferred connection type. The system will automatically select the priority of these two modes. The default configuration of the system is as follows.

Wide Area Network (WAN) Settings

 You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.


WAN Connection Type:		AUTO
Primary Connection Type		
Connection Type		DHCP (Auto config)
DHCP Mode		
Hostname (optional)		
3G/4G PPP		
APN		
PIN		
Dial Number		
Username		
Password		
MAC Clone		
MAC Clone Setting		Disable

In AUTO mode, if you want to use 3G/4G PPP mode. You should setup dialing number, user name and password of the service provider in the HYTTHDRM100 .

Option 6: 3G/4G NDIS

3G/4G NDIS is based on the SIM card, users need to insert the SIM card into the card slot before boot. Using the default configuration of the system and click OK to access the Internet.

Wide Area Network (WAN) Settings

 You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.


WAN Connection Type:		3G/4G NDIS
3G/4G NDIS		
APN		
PIN		
Username		
Password		
Authentication		None
MAC Clone		
MAC Clone Setting		Disable

2.3.2 LAN setting.

LAN is a group which is connected by a plurality of computers in a certain area. It can be easy to realize intercommunication inside the local area network

Note. The preset gateway of local area network must be connected with IP address and the start IP address of LAN, and the end of IP address is in the same network segment. Otherwise it can not access the Internet.

Local Area Network (LAN) Settings

 You may enable/disable networking functions and configure their parameters as your wish.

LAN Setup	
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
LAN 2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
LAN2 IP Address	
LAN2 Subnet Mask	
MAC Address	CD:4A:09:15:87:D4
DHCP Type	Server
Start IP Address	192.168.0.100
End IP Address	192.168.0.200
Subnet Mask	255.255.255.0
Primary DNS Server	168.95.1.1
Secondary DNS Server	8.8.8.8
Default Gateway	192.168.0.1
Lease Time	86400

Local IP. Local IP address.

Subnet Mask. Local subnet mask.


Gateway. Router internal gateway.

Start IP address and end IP address. The range IP address can be setted in the same network segment. And the IP address is the IP address of the LAN in this section.

2.3.3 DHCP Client list.

If DHCP services are enabled. All clients that connect to the DHCP will appear in this list, including the WIFI network client and the LAN client.

DHCP Client List

 You could monitor DHCP clients here.

DHCP Clients			
Hostname	MAC Address	IP Address	Expires in
Quzi-PC	70:85:C2:0F:2D:99	192.168.0.100	21:50:59
box-iPhone	A0:18:28:E0:EB:2A	192.168.0.101	23:12:37

2.3.4 VPN setting.

HYTTHDRM100 VPN. The client supports five mode, such as IPsec, PPTP, GRE, OPENVPN and L2TP etc.

VPN pass through.

When it is enabled, the penetration VPN service is allowed to pass through the HYTTHDRM100. And it is intercepted when it is stopped.

There are three kinds of L2TP penetration, IPsec penetration and PPTP penetration that can be passed or intercepted.

Select L2TP and PPTP operation mode.

PPTP, Point to Point Tunneling Protocol, is a new enhanced encryption protocol developed based on PPP protocol. PPTP supports VPN, PAP and EAP, etc.

Remote user is allowed to access safely local network via ISP, internet or other network.

L2TP, In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Server IP address of VPN server. The priority. User name for login of VPN server.

Password. Password for login of VPN server user name.

Note. Please check the VPN information in the system state to ensure that VPN starts successfully in the corresponding operation mode.

Select IPsec operation mode.

Name. Customize the name of VPN.

Local subnet. Can be empty, client local subnet.

The remote end of gateway gateway IP. VPN server gateway, required.

The remote terminal network. It can be empty. If you set up a local subnet, the remote terminal network must be the same as the local subnet.

IKE mode. Active or brutal mode can be set.

PSK. Pre shared key, consistent with the server's PSK.

Xauth. When the authentication enable, you need to enter a username and password.

Local identifier ID type. You can setup either default or customize.

Remote identifier ID type. You can setup either default or customize.

Hash algorithm. You can choose MD5 or SHA1.

Security protocols. AH or ESP. AH authentication, the packet will not be encrypted, only to provide IP and ensure data packets have not been modified. ESP, to support encryption and can adapt to the end to end between the presence of NAT, recommend using this method.

Other configuration can choose the default setting. Or according to the requirements of the user to set the parameters.

Note. Please check the VPN information in the system state to ensure that VPN starts successfully in the corresponding operation mode.

VPN Connection Type			
VPN Operation Mode		IPSec	
IPSec Mode			
Name	<input type="text"/>		
Local Subnet	Subnet	Subnet IP / Subnet Prefix Length	<input type="text"/>
Remote Secure Gateway IP	<input type="text"/>		
Remote Subnet	None	Subnet IP / Subnet Prefix Length	<input type="text"/>
IKE Mode	Main	Pre-Shared Key (PSK)	<input type="text"/>
Xauth	Disable		
User Name	<input type="text"/>	Password	<input type="text"/>
Local ID Type	Default	Local ID Content	<input type="text"/>
Remote ID Type	Default	Remote ID Content	<input type="text"/>
ISAKMP SA			
Hash Function	SHA1	Encryption	AES128
DH Group	MODP1024		
ISAKMP SA			
Hash Function	SHA1	Encryption	AES128
DH Group	MODP1024		
IPSec SA			
IPSec Proposal	ESP		
Authentication	SHA1	Encryption	AES128
Perfect Forward Secrecy (PFS)	None		
Other IPSec Settings			
Phase1 (IKE) SA Lifetime	480 min(s)	Phase2 (IPSec) SA Lifetime	480 min(s)
NAT-Traversal	Enable	Keepalive Frequency	1 seconds(0-60 sec)
Dead Peer Detection (DPD)	Enable		
DPD Delay	30 seconds	DPD Timeout	120 seconds

Apply Cancel

Select GRE operation mode.

A technology called tunnel is used between the protocol layers.

VPN Connection Type	
VPN Operation Mode	GRE
GRE mode	
Remote IP	<input type="text"/>
Local IP	<input type="text"/>
Remote Subnet	<input type="text"/>
Tunnel Remoteip	<input type="text"/>
Tunnel Localip	<input type="text"/>

You need to fill in remote VPN GRE IP, local VPN GRE IP, GRE remote subnet, GRE remote tunnel IP and local tunnel IP correctly. You can view the VPN information in the system state that it ensure VPN starts successfully in the corresponding running mode.

Select OpenVPN operation mode.

VPN Connection Type	
VPN Operation Mode	OPENVPN
OPENVPN mode	
Server IP	<input type="text"/>
Port	119
Tunnel Type	tun
Protocol	tcp
Auth mode	cert
CA Cert Location	<input type="button" value="浏览... 未选择文件"/> <input type="button" value="Upload"/>
Client Cert Location	<input type="button" value="浏览... 未选择文件"/> <input type="button" value="Apply"/>
Key Location	<input type="button" value="浏览... 未选择文件"/> <input type="button" value="Apply"/>

OpenVPN server IP. OpenVPN server IP address.

OpenVPN server port. VPN server monitor port.

OpenVPN tunnel. Select tunnel mode, tunnel(route IP tunnel),tap(Two layer communication channel)

OpenVPN port. VPN communication protocol, TCP or UDP

OpenVPN Authentication mode. password verification or certificate verification.

1. Select certificate validation mode, configure parameters as

follows.

OpenVPN cacert. Uploading CA server files.

OpenVPN clientcert. Uploading CA client files.

OpenVPN Key position. key files

2. Select password authentication mode

Fill in the OpenVPN user name and the OpenVPN user password.


VPN Connection Type	
VPN Operation Mode	OPENVPN
OPENVPN mode	
Server IP	<input type="text"/>
Port	119
Tunnel Type	tun
Protocol	tcp
Auth mode	password
Username	<input type="text"/>
Password	<input type="text"/>

You can view the VPN information in the system state to ensure that VPN is successfully started in the corresponding operation mode.

2.3.5 Advanced routing configuration.

Supports static mode, where you can add and remove customized static routing rules. The rules can be deleted and reset in the current routing list

Static Routing Settings

 You may add and remove custom Internet routing rules, and/or enable dynamic routing exchange protocol here.

Add a routing rule	
Destination	<input type="text"/>
Range	Host
Gateway	<input type="text"/>
Interface	LAN
Comment	<input type="text"/>

Current Routing table in the system:									
No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)	
2	192.168.1.0	255.255.255.0	0.0.0.0	1	0	0	0	WAN(eth2.2)	
3	192.168.0.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)	
4	0.0.0.0	0.0.0.0	192.168.1.1	3	1	0	0	WAN(eth2.2)	


2.3.6 QoS quality of service.

Service quality rules can be added and deleted on this page to ensure that different bandwidth and priorities are provided for each traffic.

Quality of service has four traffic direction mode:

1. disable
2. Internet upload and download
3. upload to Internet
4. download from Internet.

Quality of Service Settings

 You may setup rules to provide Quality of Service guarantees for specific applications.

QoS Setup	
Quality of Service	Upload to Internet ▾
Upload Bandwidth:	16M ▾ Bits/sec
Download Bandwidth:	20M ▾ Bits/sec
QoS Type:	MANUAL QoS ▾
QoS Model:	DRR ▾
Reserved bandwidth:	0% ▾ (10% is recommended)

QoS Upload Group Settings	
Highest	Rate: 10% ▾ Cell: 100% ▾
High	Rate: 10% ▾ Cell: 100% ▾
Default	Rate: 10% ▾ Cell: 100% ▾
Low	Rate: 10% ▾ Cell: 100% ▾

Upload bandwidth. Bits/S limit speed of different values can be selected. Custom input is also available.

Download bandwidth. Bits/S limit speed of different values can be selected. Custom input is also available.

Select QoS type.


1. QoS automatic service
2. QoS manual setup service

Reserved bandwidth. Recommended to retain 10%. Or other values can be set.

If you choose to set type QoS manually. There are four modes of QoS.

1. **DRR mode.** We can set up four levels of bandwidth utilization and maximum bandwidth utilization for the selected control bandwidth flow direction (upload, download, or Internet up and down).
2. **SPQ mode.** The bandwidth utilization rate cannot be set to the selected control bandwidth flow.
3. **SPQ+DRR mode.** For the selected control bandwidth flow direction can only be minimum and default two levels of bandwidth usage settings.
4. **Remark only mode.** Bandwidth utilization cannot be set.

Quality of Service Settings

 You may setup rules to provide Quality of Service guarantees for specific applications.


QoS Setup	
Quality of Service	Upload to Internet
Upload Bandwidth:	16M Bits/sec
Download Bandwidth:	20M Bits/sec
QoS Type:	MANUAL QoS
QoS Model:	DRR
Reserved bandwidth:	0% (10% is recommended)

QoS Upload Group Settings	
Highest	Rate: 10% Cell: 100%
High	Rate: 10% Cell: 100%
Default	Rate: 10% Cell: 100%
Low	Rate: 10% Cell: 100%

2.3.7 IPv6

Turn on or off the IPv6 connection type. At present, the default is disabled, and the user can open it according to his own needs.

IPv6

 IPv6 Setup

IPv6 Connection Type	
IPv6 Operation Mode	Static IP Connection

IPv6 Static IP Setup	
LAN IPv6 Address / Subnet Prefix Length	<input type="text"/> / <input type="text"/>
WAN IPv6 Address / Subnet Prefix Length	<input type="text"/> / <input type="text"/>
Default Gateway	<input type="text"/>

2.3.7 DTU

When the user sets the DTU function in the UI interface is enable. It sent and received data via RS232 serial port will be the default for IP packets. It can be achieved point-to-point transparent data transmission between single HYTTHDRM100 and server. Or achieved point-to-multiple points transparent data transmission between a server and a plurality of HYTTHDRM100. When the system is dormant, the user can also set up a heartbeat packet to maintain the link permanently online.

Data Transfer unit (DTU) Settings

 You may enable/disable DTU function and configure its parameters as your wish.

DTU Status Option	
DTU Status	<input type="text" value="Disable"/>

Basic Settings	
Operation Mode	<input type="text" value="Client"/>
Transmission Protocol	<input type="text" value="TCP"/>
Serial Packet Idle Time	<input type="text" value="600"/> ms (range 1 - 65535, default 500)
Socket Packet Timeout	<input type="text" value="600"/> ms (range 1 - 65535, default 500)
Socket Buffer Length	<input type="text" value="1500"/> (range 100 - 1500, default 1500)

Server Settings	
Server IP/Domain Name	<input type="text"/>
Server Port	<input type="text"/> (range 1 - 65535)
Retry Interval	<input type="text" value="5000"/> ms (range 1 - 65535, default 5000)
Retry Count	<input type="text" value="10"/> (range 0 - 65535, default 10, 65535: keep trying)

Server Settings	
Server IP/Domain Name	<input type="text"/>
Server Port	<input type="text"/> (range 1 - 65535)
Retry Interval	<input type="text" value="5000"/> ms (range 1 - 65535, default 5000)
Retry Count	<input type="text" value="10"/> (range 0 - 65535, default 10, 65535: keep trying)

Heartbeat Settings	
Heartbeat Packet	<input type="text"/>
Heartbeat Interval	<input type="text" value="1000"/> ms (range 1 - 65535, default 1000)
Initial Packet	<input type="text"/>

Serial Settings	
Baudrate	<input type="text" value="57600"/>
Parity	<input type="text" value="None"/>
Data Bits	<input type="text" value="8"/>
Stop Bits	<input type="text" value="1"/>

DTU status. It can be set DTU enable and disable.

Operator mode. Set wireless terminal device to the client or server.

Transport protocol. Select transport protocol for DTU.

The server IP address / Domain Name. Set DTU server IP address and name.

Serial port settings: set the serial port parameters, baud rate etc.

2.3.8 SNMP

Network management. It can detect routing devices on the network.

Network management function operation mode. disable, SNMP V1/V2 and SNMP V3.


1. SNMP V1/V2 mode settings.

Community. SNMP community, No password is required, only a common name.

Access authority. SNMP access authority.

- 1) RO, read only.
- 2) RW, read and write.

Snmp Settings

 You may enable/disable Snmp function and configure its parameters as your wish.

Snmp Status	
Snmp Opmode	Snmpv1v2

Snmp Snmp V1 And Snmp V2 Setting	
Community	<input type="text"/>
Access Authority	ro

2. SNMP V3 mode settings.

User name. SNMP user name.

Access authority. User authority. 1, ro (read only) 2, rw (read and write)

Authentication method. SNMP authentication protection. 1, no. 2, MD5.

3, SHA.

When selecting no of verification method. There is no need to input the verification code. And when selecting MD5 or SHA, it need fill the corresponding verification code.

Authentication code. MD5 or SHA password that enters authentication protection.


Encryption methods. Private protection mode of SNMP. 1, no 2, DES 3, AES

When selecting on of encrypting. You don't need to add a password.

When selecting DES or AES. You need to add a password.

Add password: enter private protection password

Snmp Settings

 You may enable/disable Snmp function and configure its parameters as your wish.

Snmp Status	
Snmp Opmode	Snmpv3

Snmp V3 Setting	
User Name	<input type="text"/>
Access Authority	ro
Auth Password Encryption Algorithm	MD5
Auth Password	<input type="text"/>
Priv Password Encryption Algorithm	AES
Priv Password	<input type="text"/>

2.3.9 TR069

The WAN device management protocol can manage and configure routing devices in the home network or industrial network.


TR069 operation mode. Enable or disable function.

TR069 server. Enter TR069 server IP address.

TR069 user name. Enter TR069 user name.

TR069 password. Enter TR069 user password.

TR069 Settings

 You may enable/disable TR069 function and configure its parameters as your wish.

TR069 Status	
TR069 Opmode	<input type="text" value="Enable"/>


TR069 Setting	
ACS Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>

2.4 WIFI wireless settings.

2.4.1 Basic settings.

User can configure the WIFI general parameters here as follows.

Basic Wireless Settings

 You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network	
Driver Version	4.1.0.0
WiFi On/Off	<input type="button" value="WIFI OFF"/>
Network Mode	<input type="text" value="11b/g/n mixed mode"/>
Network Name(SSID)	<input type="text" value="Head_WebLink"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	C0:4A:09:15:87:D4
Frequency (Channel)	<input type="text" value="2412MHz (Channel 1)"/>

HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2432MHz (Channel 5)
Space Time Block Coding(STBC)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
HT Disallow TKIP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
HT LDPC	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Other	
HT TxStream	2
HT RxStream	2

SSID. User WIFI device name. This is a unique name, consisting of numbers and letters. It's case sensitive and length less than 32 characters.

Channel. ID from 1 to 14. In multiple wireless network, recommend different channels.

The wireless network On/off. This is a WIFI on/off button. Click button will switch to turn on or off.

The other set select the default profile can realize mobile device accessing internet.

The WIFI password is set in the security settings. Details refer to 2.4.3.

2.4.2 Advanced setting.

Advanced settings are setting the wireless network detailed parameters. Advanced settings include non-basic settings such as beacon spacing, control transfer rate, basic data transfer rate, and WIFI multimedia capabilities etc.

Usually, using system default configuration as shown below.

Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

Advanced Wireless	
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IEEE 802.11H Support	<input type="radio"/> Enable <input checked="" type="radio"/> Disable(only in A band)
Country Code	None
Support Channel	Ch1-14

Wi-Fi Multimedia	
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Parameters	WMM Configur...

2.4.3 Security setting.

Including OpenWEP,WPA,WPA-PSK,WPA2,WPA-PSK and other encryption methods. System default setting is no password. User can select the encryption mode. Also can set up your WIFI password.

For example. The 1:802.1X security mode.

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	Head_Weblink
"Head_Weblink"	
Security Mode	802.1X

802.1x WEP	
WEP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable


Radius Server	
IP Address	0
Port	1812
Shared Secret	
Session Timeout	0
Idle Timeout	

Access Policy	
Policy	Disable

Radius IP address. Radius server IP address.
 Port. Radius. Port of authentication server
 Share key. Share key of Radius authentication server.

Example 2. WPA2-PSK security mode.

Wireless Security/Encryption Settings

 Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID

SSID choice: test_host

"test_host"

Security Mode: WPA2-PSK

WPA

WPA Algorithms: TKIP AES TKIPAES

Pass Phrase: 1234w678

Key Renewal Interval: 3600 seconds (0 ~ 4194303)

Access Policy

Policy: Disable

Add a station Mac:

WPA-PSK/WPA2-PSK is the type of encryption that we set up usually. It's high performance of this encryption type. Also it is very easy to setup. But it's important to note that it has three encryption algorithms, AES, TKIP and TKIPAES.

If user want to achieve mobile device access the Internet via WIFI. It can do the following configuration.

Security mode. Select WPA2-PSK.

WPA algorithm. Select AES.


Password. Can be set by yourself. Usually, default password is 12345678.

The choice of the default configuration, click OK to set successfully.

2.4.4 Terminals list.

You can see the client information of the current connection via WIFI in the list.

Station List


 You could monitor stations which associated to this AP here.

Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
A0:18:28:E0:EB:2A	1	1	0	7	20M	0	0

2.4.5 Wireless statistical data.

Looking at the statistics sent and accepted via WIFI. Also you can reset the counters and reset the statistics.

AP Wireless Statistics

 Wireless TX and RX Statistics

Transmit Statistics	
Tx Success	4714
Tx Retry Count	0, PER=13.8%
Tx Fail after retry	754, PLR=1.4e-01
RTS Successfully Receive CTS	0
RTS Fail To Receive CTS	0

Receive Statistics	
Frames Received Successfully	70208
Frames Received With CRC Error	89622, PER=56.1%

SNR	
SNR	34, n/a, n/a

[Reset Counters](#)

2.5 Firewall.

2.5.1 MAC/IP/Port filter.


Foundation setting.

This page is the firewall of each filter function to open and close settings. Only when the total filter switch of the firewall is enabled. The subsequent "MAC address filtering", "port filtering" and "IP address filtering" will be effective. Otherwise, the failure will be invalid.

Default rules option.

Setting default rules can discard or accept packets that are not in conformity with the rules.

MAC/IP/Port Filtering Settings

 You may setup firewall rules to protect your network from virus, worm and malicious activity on the Internet.

Basic Settings	
MAC/IP/Port Filtering	<input type="text" value="Disable"/>
Default Policy -- The packet that don't match with any rules would be:	<input type="text" value="Dropped"/>

[Apply](#) [Reset](#)

MAC/IP/Port filter setting.

The origin of MAC address. The MAC address of the computer you want to control.

The target of IP address. The downlink IP address you want to control.

The origin of IP address. The upstream IP address you want to control.

Protocol. Options are as follows. Such as None, TCP, UDP, ICMP etc. You want to filter the protocol.

The target of ports range. The downstream port range that you want to control.

The origin of ports range. The upstream port range that you want to control.

Execute action. You need to select accept or discard for the operation of this setting.

Note. How do you explain the filter settings?

MAC/IP/Port Filter Settings	
Source MAC address	<input type="text"/>
Dest IP Address	<input type="text"/>
Source IP Address	<input type="text"/>
Protocol	None <input type="button" value="v"/>
Dest Port Range	<input type="text"/> - <input type="text"/>
Source Port Range	<input type="text"/> - <input type="text"/>
Action	Accept <input type="button" value="v"/>
Comment	<input type="text"/>

(The maximum rule count is 32.)

MAC/IP/Port filtering rules for current systems.

You can see filter rules for each number and perform delete and reset operations.

Current MAC/IP/Port filtering rules in system:									
No.	Source MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Others would be dropped									-

2.5.2 System security setting.

This page can set up a system firewall to protect the router or the wireless access point itself.

Remote management.

Allow and prohibit remote management of routers through wide area networks. And specify remote management hosts IP and ports.

Remote management	
Remote management (via WAN)	Deny
Host IP	0.0.0.0
Port	80 (range 1 - 65535)

PING packet filtering over wide area networks.

Allows and prohibits access to routers over Wan PING packet.

Ping form WAN Filter	
Ping form WAN Filter	Disable

Port scannig.

Port scanning enable or disable.

Block Port Scan	
Block port scan	Disable

SYN FLOOD attack.

Block SYN flood attack enable or disable.

Block SYN Flood	
Block SYN Flood	Disable

Packet state detection(SPI)

SPI firewall enable or disable.

Stateful Packet Inspection (SPI)	
SPI Firewall	Disable

Apply
Reset

2.5.3 Content filtering.

Content filtering settings can set filter rules to limit inappropriate web content.

Page content filtering: you can filter proxy servers, Java pages, and ActiveX plug-in page content.

Webs Content Filter	
Filters:	<input type="checkbox"/> Proxy <input type="checkbox"/> Java <input type="checkbox"/> ActiveX

Apply
Reset

Page URL filter setting.

The current system of web page URL filtering rules: you can see the filter rules of the URL and its number. And can choose the corresponding number of URL delete and reset.

New URL filtering rules.

You can add URL that you want to filter.

Webs URL Filter Settings

Current Webs URL Filters:	
No	URL

Add a URL filter:	
URL:	<input type="text"/>

Web host filter settings.

The current system of web host filter rules. You can see key words and numbers in the web host filter rules of the routing system. And can be selected to delete and reset the operation

Current system web host filter rules.

You can add new web host keywords that need filtering.

Webs Host Filter Settings

Current Website Host Filters:	
No	Host(Keyword)

Add a Host(keyword) Filter:	
Keyword	<input type="text"/>

2.5.4 Port forwarding.

Port forwarding can transfer the external network port to another internal network node for external network connection.

Port forwarding. Can be enable or disabel.

IP address. IP address to be forwarded.

Ports range. Ports to be forwarded.

Protocol. Three protocol packets can be forwarded.

1) TCP&UDP.


2) TCP.

3) UDP.

Note: Comment on the set of virtual servers.

The port forwarding of the current system can view the number, IP address, port range, protocol and annotation to be forwarded. And the corresponding number can be selected to delete and reset the operation.

Virtual Server Settings

 You may setup Virtual Servers to provide services on Internet.

Port Forwarding	
Port Forwarding	Disable <input type="button" value="v"/>
IP Address	<input type="text"/>
Port Range	<input type="text"/> - <input type="text"/>
Protocol	TCP&UDP <input type="button" value="v"/>
Comment	<input type="text"/>

(The maximum rule count is 32.)

Current Port Forwarding in system:

No.	IP Address	Port Range	Protocol	Comment

Virtual server.

Virtual server. Enable or disable the virtual server function.

IP address. Virtual server's IP address.

Public port. Can be set to be accessed the port from wide area network users.

Private port. Can be set to private LAN access port.

Protocol. Virtual server transmission protocol

Note. Remarks for this virtual server.

The virtual server of the current system can view the IP address, common port, private port, protocol, annotation and its corresponding number of the virtual server of the current system. And can selected to delete and reset the operation.

Virtual Server	
Virtual Server	Disable
IP Address	
Public Port	
Private Port	
Protocol	TCP&UDP
Comment	

(The maximum rule count is 32.)

Apply Reset

Current Virtual Servers in system:						
No.	IP Address	Public Port	Private Port	Protocol	Comment	

Delete Selected Reset

2.5.5 Port triggering.

Port triggering is when an application specifies a port to open an input connection. The router will transfer an external connection to an internal designated port (transport port). The port ranges from 5000 to 6000.

Trigger protocol. The protocol triggered by a desired port.

Trigger port. Port number triggered by the desired port.

Incoming protocol. The incoming protocol triggered by the desired port .


Incoming port. The incoming port number triggered by the desired port.

Note: Remarks on rules for port triggered settings.

Port trigger of current system.

We can check the trigger service number, trigger protocol, trigger port, import protocol, import port and annotation. And select the corresponding number to execute delete and reset operation.

Port Trigger Setting

 You may setup Port Trigger services on Internet.

Port Trigger		
Port Trigger		Disable
Trigger Protocol		TCP
Trigger Port		
Incoming Protocol		TCP
Incoming Port		
Comment		

(The maximum rule count is 32.)

Current Port Trigger in system:					
No.	Current Trigger Protocol	Current Trigger Port	Current Incoming Protocol	Current Incoming Port	Comment


2.5.6 DMZ

DMZ can be understood as the network from outside the pass through. It will put all the ports open to the network on your computer.

DMZ setting. DMZ can set to be enable or disable.

DMZ address. Please set the internal IP address for the DMZ host.

DMZ Settings

 You may setup a De-militarized Zone(DMZ) to separate internal network and Internet.

DMZ Settings	
DMZ Settings	Enable
DMZ IP Address	

Except TCP port 80

2.6 SMS setting.


2.6.1 Inbox.

Inbox. Inbox can see the messages received of SIM card.

Inbox setting. Inbox functions can be enabled or disable.

Inbox list. You can view the received SMS sender, message content and delivery time. And you can choose to delete and refresh.

SMS Inbox

 You can take a look at the short messages received by the SIM card.

SMS Inbox Setting

SMS Inbox

Apply

Inbox List


Sender	Content	Time
--------	---------	------

Delete Refresh

2.6.2 Send SMS.

You can send text messages here. And edit SMS recipient, SMS content and send.

Send Message

 You can send short messages here.

Edit a message

Receiver	<input type="text"/>
Content	<input type="text"/>

Apply Cancel

2.6.3 Advanced setting.

Advanced settings can set SMS automatic reporting and control command parameters.

Set the automatic report / SMS control command function to enable and disable.

Advanced

 You can setup SMS auto report and control command parameters here.

Advanced Settings	
Auto Report/SMS Control Command	Disable ▾

Apply

Cancel

2.7 DDNS

DDNS settings can configure DDNS connection types and related parameters here.

DDNS connection type. DDNS operation mode is disable,peanut shell,noip.

Only when you have peanut shell and noip account number that you can use DDNS service.

DDNS state. Check existing DDNS running mode and running state.

DDNS Setting

 You may enable/disable DDNS function and configure its parameters as your wish.

DDNS Connection Type	
DDNS Operation Mode	disable ▾

Apply

DDNS Status	
ddns setting mod	
ddns setting Status	

2.8 GPS information.

2.8.1 GPS status

This page allows you to view GPS status information here. The premise is to assemble the GPS antenna and enable the GPS function.

Positioning status. A, effective location. V, invalid location. Disable, GPS function is disabled.

Positioning date. The date of the last GPS positioning.

Positioning time. The last time of GPS positioning.


Longitude. The longitude of the last GPS location.

Latitude. The latitude of the last GPS location.

Speed. The speed of the last GPS positioning.

GPS operation mode. GPS function can be turned on or off.

GPS Status

 You can take a look at information of GPS

GPS status	
Status	Disable (A:effective positioning V:invalid positioning Disable: Operation state disable)
Date	
Time	
Latitude	
Longitude	
Speed	
GPS Operation Mode	<input type="text" value="Disable"/>

2.8.2 GPS information setting.

This page can upload GPS status information to the specified server.

Destination server. Server to receive GPS status information.


Port number. Port of receiving information service.

Sending interval (s). The time interval for uploading GPS status information.

Protocol. The selected protocol for uploading GPS information.

Upload status. The status of uploading GPS information at this time.

GPS Information Setting

 You can upload information of GPS here.

GPS Information Setting	
Server	<input type="text"/>
Port	<input type="text"/>
Transport Interval (s)	<input type="text"/>
Protocol	<input type="text" value="UDP"/>
Status	Upload stopped

2.9 System management.

2.9.1 Management.

System management interface can set the system administrator password, and network time and module settings.

Language settings. You can choose Chinese simplified, traditional Chinese and English

System Management



You may configure administrator account and password, NTP settings, and Dynamic DNS settings here.

Language Settings	
Select Language	<input type="text" value="English"/>
	<input type="text" value="English"/> <input type="text" value="繁體中文"/> <input type="text" value="简体中文"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Manager settings. You can set or modify the router administrator's account number and password.

Administrator Settings	
Account	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Network time settings. You can view the current system time. Also you can set host synchronization to update the time, set the system time zone, set the network time server, and Calibrating network time in hours.

NTP Settings	
Current Time	<input type="text" value="Fri Oct 20 11:09:38 UTC 2017"/> <input type="button" value="Sync with host"/>
Time Zone:	<input type="text" value="(GMT-11:00) Midway Island, Sa"/>
NTP Server	<input type="text"/> ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw
NTP synchronization(hours)	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Module setting.

The automatic restart function module. Enable and disable selection
Automatic restart time interval (Hour). Restart time interval

Module Settings	
Module Auto Reboot	<input type="text" value="Disable"/>
Auto Reboot Interval (hours)	<input type="text" value="24"/>

Apply

Cancel

Restart the router. Can reboot the router immediately.

Router Reboot	
Reboot	<input type="button" value="Reboot"/>

2.9.2 Firmware upgrade.


Firmware update page, upload update firmware takes about 1 minutes. Please be patient. Warning!

Abnormal Image will interrupt system operation.

Upgrade mode has local upgrade and remote upgrade. Generally default to local upgrade.

Firmware upgrade. Click on the selection file, select the firmware version file you want to upgrade. And then confirm and wait for the system to restart, you can upgrade successfully.

Upgrade Firmware

 Upgrade the Head Weblink firmware to obtain new functionality. It takes about 1 minute to upload, upgrade flash and be patient please. Caution! A corrupted image will hang up the system.

Upgrade Way	<input type="text" value="Local Upgrade"/>
Update Firmware	
Location:	<input type="button" value="浏览..."/> 未选择文件*

Apply

2.9.3 Setting management.

Setting management can save system settings by exporting settings. Or restoring system settings by importing settings, and even resetting default values to the system.

Settings Management

 You might save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to factory default.

Export Settings	
Export Button	<input type="button" value="Export"/>

Import Settings	
Settings file location	<input type="text" value="浏览 未选择文件"/>
<input type="button" value="Import"/>	<input type="button" value="Cancel"/>

Load Factory Defaults	
Load Default Button	<input type="button" value="Load Default"/>

2.9.4 System status.

The system information, Internet configuration and LAN status information of the routing platform can be seen on this page.

System Status

 Let's take a look at the status of Head Weblink Platform.

System Info		
Kernal Version	2.6.36 (Oct 24 2017)	
System Up Time	2 hours, 41 mins, 36 secs	
System Platform	RT2880 embedded switch	
Operation Mode	Gateway Mode	
FW Version	V 2.1	
Modification Times	2017-10-23 17:09	


Internet Configurations		
Connected Type	DHCP	
WAN IP Address	192.168.1.5	
Subnet Mask	255.255.255.0	
Default Gateway	192.168.1.1	
Primary Domain Name Server	192.168.1.1	
Secondary Domain Name Server	192.168.1.1	
MAC Address	C0:4A:09:15:87:D5	

Local Network		
Local IP Address	192.168.0.1	
Local Netmask	255.255.255.0	
MAC Address	C0:4A:09:15:88:98	

2.9.5 Statistical information

You can view platform statistics, such as memory, Wan, LAN, and all interface information.

Statistic

 Take a look at the SIMCOM SoC statistics

Memory		
	Memory total:	59120 kB
	Memory left:	21752 kB
WAN/LAN		
	WAN Rx packets:	223883
	WAN Rx bytes:	246550913
	WAN Tx packets:	117360
	WAN Tx bytes:	8811614
	LAN Rx packets:	132940
	LAN Rx bytes:	8735939
	LAN Tx packets:	197169
	LAN Tx bytes:	261434623
All interfaces		
	Name	eth2
	Rx Packet	357025
	Rx Byte	261129077
	Tx Packet	314517
	Tx Byte	270706226
	Name	imq0
	Rx Packet	179479
	Rx Byte	243561106
	Tx Packet	179479
	Tx Byte	243561106
	Name	imq1
	Rx Packet	109558
	Rx Byte	6598312
	Tx Packet	109558
	Tx Byte	6598312
	Name	ra0
	Rx Packet	5385

2.9.6 System comman.

Execute a system command as root. And you can view the results of the implementation of feedback, or repeat last instruction operation.

System Command

Run a system command as root:

System command

Command:

ifconfig

```
br0: Link encap:Ethernet HWaddr C0:4A:09:15:87:D4
      inet addr:192.168.0.1 Bcast:192.168.0.255 Mask:255.255.255.0
      inet6 addr:fe80::c24a:9f:fe15:874a:64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:118039 errors:0 dropped:0 overruns:0 frame:0
      TX packets:185274 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:7274020 (6.9 MiB) TX bytes:252110427 (240.4 MiB)

eth2: Link encap:Ethernet HWaddr C0:4A:09:15:87:D4
      inet addr:fe80::c24a:9f:fe15:874a:64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:325503 errors:0 dropped:0 overruns:0 frame:0
      TX packets:293166 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:254991031 (243.1 MiB) TX bytes:261360439 (249.2 MiB)
      Interrupt:3

eth2:1 Link encap:Ethernet HWaddr C0:4A:09:15:87:D4
      inet addr:fe80::c24a:9f:fe15:874a:64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Apply

Repeat Last Command

2.9.7 System log.

You can view the system log . And refresh or clear the current record.

System Log

Syslog:

Refresh

Clear

System Log

```
Oct 20 08:34:42 Weblink syslog.info syslogd started: BusyBox v1.12.1
Oct 20 08:34:42 Weblink kern.notice kernel: klogd started: BusyBox v1.12.1 (2017-09-14 11:22:17 CST)
Oct 20 09:03:22 Weblink user.err syslog: ERRO: MRT_INIT failed; Errno(99): Protocol not available
Oct 20 09:03:25 Weblink kern.warn kernel: [66909,156000] AP SETKEYS DONE - WPA2, AuthMode(7)=WPA2PSK, WepStatus(6)=AES, GroupWepStatus(6)=AES
Oct 20 09:03:25 Weblink kern.warn kernel: [66909,156000]
Oct 20 09:03:27 Weblink kern.warn kernel: [66911,048000] MtAsicAddSharedKeyEntry(1343): Not support for HIF_MT yet!
Oct 20 09:03:27 Weblink user.err syslog: ERRO: MRT_INIT failed; Errno(99): Protocol not available
Oct 20 10:03:22 Weblink user.err syslog: ERRO: MRT_INIT failed; Errno(99): Protocol not available
Oct 20 10:03:26 Weblink kern.warn kernel: [70510,160000] AP SETKEYS DONE - WPA2, AuthMode(7)=WPA2PSK, WepStatus(6)=AES, GroupWepStatus(6)=AES
Oct 20 10:03:26 Weblink kern.warn kernel: [70510,160000]
Oct 20 10:03:28 Weblink kern.warn kernel: [70512,060000] MtAsicAddSharedKeyEntry(1343): Not support for HIF_MT yet!
Oct 20 10:03:28 Weblink user.err syslog: ERRO: MRT_INIT failed; Errno(99): Protocol not available
Oct 20 10:47:18 Weblink kern.warn kernel: [73141,972000] ageout a0:18:28:e0:eb:2a after 300-sec silence
Oct 20 10:47:18 Weblink kern.warn kernel: [73141,980000] Send DEAUTH - Reason = 3 frame TO a0:18:28:e0:eb:2a
Oct 20 10:55:06 Weblink kern.warn kernel: [73610,420000] PeerAssocReqSanity - IE_HT_CAP
Oct 20 10:55:06 Weblink kern.warn kernel: [73610,536000] Rcv Wcid(1) AddBAReq
Oct 20 10:55:06 Weblink kern.warn kernel: [73610,544000] Start Seq = 00000000
Oct 20 10:55:06 Weblink kern.warn kernel: [73610,556000] AP SETKEYS DONE - WPA2, AuthMode(7)=WPA2PSK, WepStatus(6)=AES, GroupWepStatus(6)=AES
Oct 20 10:55:06 Weblink kern.warn kernel: [73610,556000]
Oct 20 10:55:14 Weblink kern.warn kernel: [73618,232000] Rcv Wcid(1) AddBAReq
Oct 20 10:55:14 Weblink kern.warn kernel: [73618,240000] Start Seq = 00000000
Oct 20 11:03:23 Weblink user.err syslog: ERRO: MRT_INIT failed; Errno(99): Protocol not available
Oct 20 11:03:28 Weblink kern.warn kernel: [74111,976000] AP SETKEYS DONE - WPA2, AuthMode(7)=WPA2PSK, WepStatus(6)=AES, GroupWepStatus(6)=AES
Oct 20 11:03:28 Weblink kern.warn kernel: [74111,976000]
Oct 20 11:03:29 Weblink kern.warn kernel: [74113,072000] MtAsicAddSharedKeyEntry(1343): Not support for HIF_MT yet!
Oct 20 11:03:29 Weblink user.err syslog: ERRO: MRT_INIT failed; Errno(99): Protocol not available
```


Chapter 3 Environmental performance.

HYTTHDRM100 4G router environmental performance.

Item	Specifications
Storage temperature	-40°C~+85°C
Working temperature	-30°C~+75°C
Working humidity	5%~90% (Non condensation)