

# DWR-925W user manual



## Table of Contents

<b>1. Starting Setup in the Web UI</b>	<b>8</b>
<b>2. button</b>	<b>8</b>
<b>3. Status</b>	<b>9</b>
3.1. Basic Info	9
3.2. Device Info	9
3.3. Clients List	10
3.4. Routing Table	10
<b>4. Network</b>	<b>11</b>
4.1. Lan	11
4.2. Wan	11
4.2.1 lan mode	11
4.2.2 WAN mode	11
4.2.3 DHCP	12
4.2.4 Static IP	12
4.2.5 PPPoE	12
4.3. WLAN	13
4.3.1 2.4G WLAN	13
4.3.2 5G WLAN	16
4.4. 3G/4G Modem	18
4.4.1 Summary Info	18
4.4.2 Edit modem config	20
4.4.3 Edit modem bridge config	21
4.5. Dns	21
4.6. Link Backup	21
4.6.1 Summary Info	21
4.6.2 Edit link backup config	22
4.7. Load Balance	23
4.7.1 Summary Info	23
4.7.2 Edit Load Balance config	23
4.8. DHCP Server	25
4.8.1 static ip for devices.	25
4.8.2 Custom dhcp server info	25
<b>5. Applications</b>	<b>26</b>
5.1. ICMP Check	26
5.2. Ddns	27
5.3. DTU	28
5.3.1 Dtu server work mode	28
5.3.2 Dtu client work mode	30

---

<b>5.4. Timing Task</b>	<b>32</b>
<b>5.5. SMS</b>	<b>33</b>
5.5.1 Inbox	33
5.5.2 Outbox	33
5.5.3 New Message	33
<b>5.6. Data Cap</b>	<b>34</b>
<b>5.7. USSD</b>	<b>35</b>
<b>6. VPN</b>	<b>36</b>
<b>6.1. VPND</b>	<b>36</b>
6.1.1 pptp or l2tp entry	36
6.1.2 Add tunnel entry	36
6.1.3 View tunnel entry	37
<b>6.2. Tunnel</b>	<b>38</b>
<b>6.3. IPsec</b>	<b>39</b>
6.3.1 View ipsec entry connect status	39
6.3.2 add ipsec entry connect status	40
<b>6.4. OpenVpn</b>	<b>44</b>
<b>7. Forward</b>	<b>46</b>
<b>7.1. nat</b>	<b>46</b>
7.1.1 view info	46
7.1.2 Add DNAT	46
7.1.3 Add SNAT	47
<b>7.2. Routing</b>	<b>48</b>
7.2.1 view info	48
7.2.2 Add Static Route	48
7.2.3 Add Policy Route	48
<b>7.3. RIP</b>	<b>50</b>
7.3.1 View RIP Info	50
7.3.2 Add Neighbor	50
7.3.3 Add Network	51
<b>7.4. OSPF</b>	<b>52</b>
7.4.1 View OSPF Info	52
7.4.2 Add OSPF Network	53
7.4.3 Add OSPF Neighbor	53
7.4.4 Add OSPF Interface	53
<b>7.5. Qos</b>	<b>55</b>
7.5.1 View Qos Info	55
7.5.2 Add Qos Entry	55
<b>8. Security</b>	<b>57</b>
<b>8.1. IP Filter</b>	<b>57</b>
8.1.1 View Filter Info	57

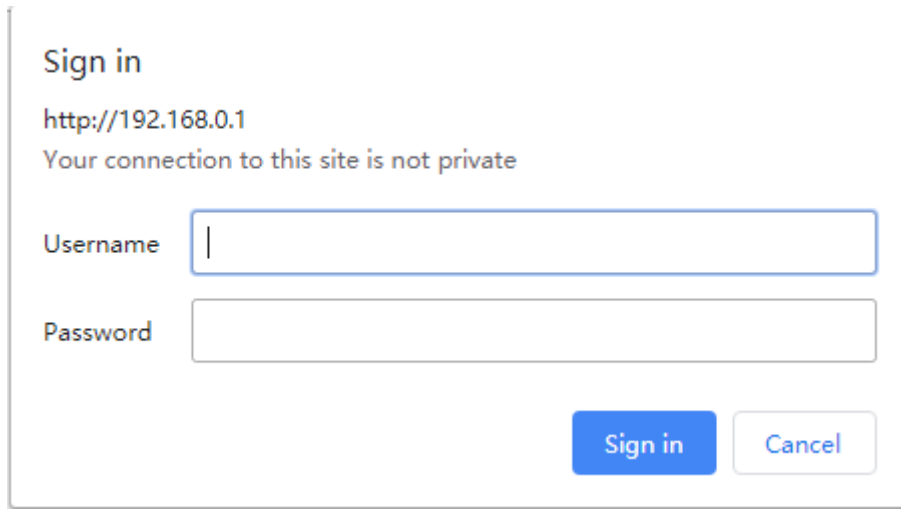
8.1.2	Add Filter Entry.....	57
<b>8.2.</b>	<b>Domain Filter .....</b>	<b>59</b>
8.2.1	View Domain Filter .....	59
8.2.2	Add Domain Filter .....	59
<b>8.3.</b>	<b>MAC Filter .....</b>	<b>60</b>
8.3.1	View MAC Filter.....	60
8.3.2	Add MAC Filter .....	60
<b>8.4.</b>	<b>DDOS .....</b>	<b>60</b>
<b>9.</b>	<b>Management.....</b>	<b>61</b>
9.1.	Local Log .....	61
9.2.	Remote Log .....	62
9.3.	NTP Server .....	62
9.3.1	Enable ntp system time .....	62
9.3.2	Enable manual system time.....	63
9.4.	Service Control .....	65
9.5.	Account .....	65
9.6.	Diagnostics .....	66
9.7.	Upgrade/Settings.....	66

# 1. Starting Setup in the Web UI

It is easy to configure and manage the DWR-925W with the web browser.

**Step1.** To access the configuration utility, open a web-browser and enter the default IP address <http://192.168.0.1> in the web address field of the browser.

After a moment, a login window will appear. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **Log In** button or press the **Enter** key.



**Figure 1-1** Login Window

Default IP Address: **192.168.0.1**

Default User Name: **admin**

Default Password: admin

## 2. button

Object	Description
<b>Add</b>	Add entry or config info.
<b>Mod</b>	Edit config
<b>Del</b>	Delect entry
<b>View</b>	View status
<b>En</b>	Enable this function
<b>Dis</b>	Disable this functon
<b>Enable</b>	Enable this function
<b>Disable</b>	Disable this functon

### 3. Status

#### 3.1. Basic Info

On this page, you can view information about the Internet status of the DWR-925W, include modem1 modem 2, lan,wan information.

SIM1	
SIM Status	NO CARD
SIM ICCID	
Up Time	
Modem Status	DISCONNECTED
Network Type	
Signal	
IP Address	
DNS	

SIM2	
SIM Status	NO CARD
SIM ICCID	
Up Time	
Modem Status	DISCONNECTED
Network Type	
Signal	
IP Address	
DNS	

LAN Status	
IP	192.168.0.1
Subnet Mask	255.255.255.0
MAC	00:11:22:33:44:55

WAN Status	
Wan Type	DHCP
IP	
Mask	
MAC	00:11:22:33:44:56

#### 3.2. Device Info

You can view base information about DWR-925W.

Product Type:	DWR-925W
Device ID:	001122334455
MAC Address:	001122334455
Hardware Version:	DWR-925W_A1
Software Version:	DWR-925W_A1_1.0.0_20191101
System Up Time	0 days, 13 hours, 33 mins, 53 secs

Refresh

### 3.3. Clients List

This page shows the IP addresses and host names of all the PCs in your network

client name	IP Address	MAC Address
---	192.168.0.101	08:57:00:ec:45:c0

Refresh

### 3.4. Routing Table

This page shows the system route info , include manual configuration static route and policy route

Network	Subnet Mask	Gateway	Interface	Metric
192.168.0.0	255.255.255.0	0.0.0.0	br0	0

Network	Subnet Mask	Gateway	Interface	Priority
---------	-------------	---------	-----------	----------

## 4. Network

### 4.1. Lan

On this page, you can configure the local network for router.

Host Name	<input type="text" value="DWR-925W"/>	* Max length is 32
LAN IP	<input type="text" value="192.168.0.1/24"/>	* eg. 192.168.1.1/24

Object	Description
Host Name	Router show host name inf dhcp.
LAN IP	Local network.

### 4.2. Wan

On this page, you can configure the parameters of the WAN interface.

<b>Status</b>					
<b>Network</b>					
LAN					
<b>WAN</b>	<table border="1"> <tr> <td>work mode</td> <td><input type="text" value="WAN"/></td> </tr> <tr> <td>Connection Type</td> <td><input type="text" value="dhcp"/></td> </tr> </table>	work mode	<input type="text" value="WAN"/>	Connection Type	<input type="text" value="dhcp"/>
work mode	<input type="text" value="WAN"/>				
Connection Type	<input type="text" value="dhcp"/>				
WLAN					
3G/4G Modem					
Optical And Dps					

#### 4.2.1 lan mode

When select lan mode, the wan port will work as a lan port. And select wan mode , you can configure

Dhcp , pppoe ,static ip for wan port.

work mode	<input type="text" value="LAN"/>
-----------	----------------------------------

#### 4.2.2 WAN mode

wan connection can be configured as difference mode, such as

DHCP router mode, PPPoE router mode, Static router mode, this will more helpful for user to meet different environment usage.



### 4.2.3 DHCP

Choose “**DHCP**” and the router will automatically obtain IP addresses, subnet masks and gateway addresses from your ISP.

work mode	WAN ▼
Connection Type	dhcp ▼

Save Refresh

### 4.2.4 Static IP

If your ISP offers you static IP Internet connection type, select “**Static IP** ” and then enter IP address, subnet mask, provided by your ISP in the corresponding fields.

Note:primary DNS and secondary DNS information and gateway you need to separate configuration on menu of Gateway And Dns.

work mode	WAN ▼
Connection Type	static ip ▼
IP	<input type="text"/> * eg. 192.168.10.1/24
Gateway	<input type="text"/> * eg. 192.168.10.1

Save Refresh

Object	Description
<b>IP</b>	Enter the WAN IP address/Subnet Mask provided by your ISP. Inquire your ISP if you are not clear.
<b>Gateway</b>	Enter the WAN Gateway IP address provided by your ISP. Inquire your ISP if you are not clear.

### 4.2.5 PPPoE

Select **PPPoE**, if your ISP is using a PPPoE connection and provide you with PPPoE user name and password information.

work mode	<input type="text" value="WAN"/>
Connection Type	<input type="text" value="pppoe"/>

**Basic Settings**

Service Name	<input type="text"/>	Max length is 64
Username	<input type="text"/>	* Max length is 64
Password	<input type="text"/>	* Max length is 64

Object	Description
<b>Username</b>	Enter the User Name provided by your ISP.
<b>Password</b>	Enter the password provided by your ISP.
<b>Service Name</b>	Type the name of this router.

### 4.3. WLAN

#### 4.3.1 2.4G WLAN

WLAN interface

Main Guest

WLAN Status

Enable Disable

**Basic Settings**

SSID	<input type="text" value="dlink-925W-2.4g-0001"/>	* Max length is 32
Wireless Mode	<input type="text" value="ap"/>	
Network Mode	<input type="text" value="bgn"/>	
Channel	<input type="text" value="auto"/>	
Bandwidth	<input type="text" value="20mhz"/>	
AP Isolate	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Broadcast Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	

**Encryption Settings**

Security Mode	<input type="text" value="wpa2"/>	
Algorithms	<input type="text" value="aes"/>	
WPA Shared Key	<input type="text" value="123456789"/>	* Length is between 8 to 63
WPA Renewal Interval	<input type="text" value="10800"/>	* 120-86400 s

Save

Refresh

WLAN interface  Main  Guest

WLAN Status  Enable  Disable

**Basic Settings**

SSID  \* Max length is 32

**Encryption Settings**

Security Mode

Algorithms

WPA Shared Key  \* Length is between 8 to 63

WPA Renewal Interval  \* 120-86400 s

Object	Description
<b>WLAN interface</b>	You may choose to Main or Guest interface, If select Guest interface, the Channel, Wireless mode and Bandwidth must be the same as the Main interface
<b>Enable</b>	You may choose to enable or disable Wireless function.
<b>SSID(Wi-Fi Name)</b>	Set a name (SSID) for your wireless network. The ID of the wireless network. User can access the wireless network through it only. However, if you switch to Client Mode, this field becomes the SSID of the AP you want to connect with.  Default: <b>DWR-925W-2.4G-XXXX</b> <b>("X" means the last 4 digits of the MAC address.)</b>
Wireless Mode	<b>Ap ,station or bridge mode.</b>
Network Mode	<b>IEEE 802.11 standard bgn ,bg, b</b>
Channel	For an optimal wireless performance, you may select the least interferential channel. It is advisable that you select an unused channel or "Auto" to let device detect and select the best possible channel for your wireless network to operate on from the drop-down list.
Bandwidth	20mhz or 40mhz
AP Isolate	isolate data between wifi 2.4g and 5g
Broadcast Status	Broadcast ssid

<b>Security Mode</b>	Select the security mode from the <b>Security Mode</b> dropdown list. There are 3 options in the Security Mode dropdown list: <ul style="list-style-type: none"> <li>■ <b>disable</b></li> <li>■ <b>WPA</b></li> <li>■ <b>WPA2</b></li> </ul>
Algorithms	aes or tkip
WPA Shared Key	Enter the Wi-Fi password
WPA Renewal Interval	Key renew time

### 4.3.2 5G WLAN

WLAN interface

WLAN Status

#### Basic Settings

SSID  \* Max length is 32

Wireless Mode

Channel

Bandwidth

Broadcast Status  Enable  Disable

#### Encryption Settings

Security Mode

Algorithms

WPA Shared Key  \* Length is between 8 to 63

WPA Renewal Interval  \* 120-86400 s

WLAN interface  Main  Guest

WLAN Status  Enable  Disable

**Basic Settings**

SSID  \* Max length is 32

**Encryption Settings**

Security Mode

Algorithms

WPA Shared Key  \* Length is between 8 to 63

WPA Renewal Interval  \* 120-86400 s

Object	Description
<b>WLAN interface</b>	You may choose to Main or Guest interface, If select Guest interface, the Channel, Wireless mode and Bandwidth must be the same as the Main interface
<b>Enable</b>	You may choose to enable or disable Wireless function.
<b>SSID(Wi-Fi Name)</b>	Set a name (SSID) for your wireless network. The ID of the wireless network. User can access the wireless network through it only. However, if you switch to Client Mode, this field becomes the SSID of the AP you want to connect with.  Default: <b>DWR-925W-5.8G-XXXX</b> <b>("X" means the last 4 digits of the MAC address.)</b>
Wireless Mode	<b>Ap ,station or bridge mode.</b>
Channel	For an optimal wireless performance, you may select the least interferential channel. It is advisable that you select an unused channel or "Auto" to let device detect and select the best possible channel for your wireless network to operate on from the drop-down list.
Bandwidth	20mhz , 40mhz or 80mhz
Broadcast Status	Broadcast ssid
Security Mode	Select the security mode from the <b>Security Mode</b> dropdown list. There are 4 options in the Security Mode dropdown list: <ul style="list-style-type: none"> <li>■ <b>wep</b></li> <li>■ <b>disable</b></li> <li>■ <b>WPA</b></li> <li>■ <b>WPA2</b></li> </ul>
Algorithms	aes or tkip
WPA Shared Key	Enter the Wi-Fi password
WPA Renewal Interval	Key renew time

## 4.4. 3G/4G Modem

### 4.4.1 Summary Info

This page is used to configure the parameters for LTE network .

Mode Select

Basic Bridge

Modem 1

APN	Network Type	PIN	Operation		
----	auto	----	Mod	En	Dis

Modem 2

APN	Network Type	PIN	Operation		
----	auto	----	Mod	En	Dis

Refresh



4.4.2 Edit modem config

Auto-Dialup

**Basic Settings**

Module Type

APN  Max length is 64

Username  Max length is 64

Password  Max length is 64

PIN  Max length is 64

Network Type

Object	Description
<b>Enable</b>	Enable or disabled mobile network
<b>APN</b>	Enter the APN from ISP. If not set ,system will try to auto get apn
<b>Username</b>	Enter the user name.
<b>Password</b>	Enter the password
<b>PIN</b>	If the SIM card has set PIN, please enter the PIN here.
<b>Network Type</b>	atuo ,lte, 3g,2g mode.

### 4.4.3 Edit modem bridge config

Mode Select	<input type="button" value="Basic"/> <input type="button" value="Bridge"/>
LTE Bridge Server	<input type="button" value="Enable"/> <input type="button" value="Disable"/>
Module Type	<input type="text" value="Modem 1"/>
MAC	<input type="text"/> * eg. 00:1A:4D:34:B1:8E

Object	Description
<b>Enable</b>	Enable or disabled mobile bridge network
<b>Module Type</b>	Which 4g interface is associated to select the bridge mode
<b>MAC</b>	The host Mac that needs to bridge the Internet, such as a PC, or a connected router

### 4.5. Dns

Select the system default gateway and dns information. This can manual setup static dns.

DNS Type	<input type="text" value="Custom"/>
DNS1	<input type="text" value="Custom"/> * eg. 192.168.1.1
DNS2	<input type="text"/> eg. 192.168.1.254

Object	Description
<b>DNS Type</b>	If auto , system dns will using default gateway wan'dns, Custom will manual set system dns
<b>DNS1</b>	Manual set system dns1
<b>DNS2</b>	Manual set system dns2

### 4.6. Link Backup

#### 4.6.1 Summary Info

This page is used to display status information for multi wan network link backup.

Work mode	Running Mode	Interface Name	Operation			
failover	main	WAN	Mod	Up	Down	Del
	backup	Modem 1	Mod	Up	Down	Del
	backup	Modem 2	Mod	Up	Down	Del

#### 4.6.2 Edit link backup config

This page is used to configure the parameters for multi wan network link backup .

Status

Rule Name  \* 0-9  
 Running Mode  ▾  
 Running Timeout  \* 1-65535 s  
 Interface Name  ▾  
 Check IP or Domain  \* Max length is 64  
 Normal Interval  \* 1-65535 s  
 Retry Times  \* 1-65535

Object	Description
<b>Rule name</b>	Entry name.
Running Mode	Work as main or backup link.
<b>Running Timeout</b>	If the main link, the stable time of the main link; If for the backup link, said the link the shortest working hours.
<b>Interface name</b>	Which interface working
<b>Check ip or domain</b>	Icmp to check ip or domain
<b>Normal interval</b>	How long to a time
<b>Retry times</b>	Try fail times.

## 4.7. Load Balance

### 4.7.1 Summary Info

This page is used to display status information for Load Balanced.

Interface Name	Work	Weight	Status	Real Weight percent	Operation
WAN	disable	-	-	-	Mod
Modem1	disable	-	-	-	Mod
Modem2	disable	-	-	-	Mod

Refresh

### 4.7.2 Edit Load Balance config

This page is used to configure the parameters for Load Balance config .

Status	<input checked="" type="button" value="Enable"/> <input type="button" value="Disable"/>
Rule Name	<input type="text" value="0"/> * 0-9
Interface Name	<input type="text" value="WAN"/>
Weight	<input type="text" value="5"/> * 1-100
Track IP or Domain	<input type="text"/> * Max length is 64
Timeout	<input type="text" value="3"/> * 1-65535 s
Interval	<input type="text" value="5"/> * 1-65535 s
Count	<input type="text" value="1"/> * 1-65535

Save

Return

Object	Description
Status	Enable or disabled Current network interface load balanaced
Rule name	Entry name.
Interface name	Which interface working
Weight	Setting current network interface weight load

---

	balanced
<b>Timeout</b>	If the main link, the stable time of the main link; If for the backup link, said the link the shortest working hours.
<b>ip or domain</b>	Icmp to check ip or domain
<b>interval</b>	How long to a time
<b>Count</b>	Try fail times.

## 4.8. DHCP Server

### 4.8.1 static ip for devices.

DHCP Server

**Basic Settings**

Domain Name  Max length is 32

IP Pool

Gateway Type

DNS Type

Lease Time  \* 120-86400 s

IP  \* eg. 192.168.1.1

MAC  \* eg. 00:1A:4D:34:B1:8E

IP	MAC	Operation

Object	Description
<b>Ip</b>	Ip binding to mac.
<b>MAC</b>	Device of this Mac will give static ip

### 4.8.2 Custom dhcp server info

DHCP Server

**Basic Settings**

Domain Name  Max length is 32

IP Pool

Start  \* eg. 192.168.1.1

End  \* eg. 192.168.1.254

Gateway Type

Gateway  \* eg. 192.168.1.1

DNS Type

DNS1  \* eg. 192.168.1.1

DNS2  eg. 192.168.1.254

Lease Time  \* 120-86400 s

Object	Description
<b>Ip Pool</b>	custom
<b>Start</b>	Dhcp server pool start address
<b>End</b>	Dhcp server pool end address
<b>Gateway Type</b>	custom
<b>Gateway</b>	Dhcp Lease for devices gateway
<b>DNS Type</b>	custom
<b>DNS1</b>	Dhcp Lease for devices dns
<b>DNS2</b>	Dhcp Lease for devices dns
<b>Lease Time</b>	Dhcp lease time

## 5. Applications

### 5.1. ICMP Check

Icmp check network status and do action.

ICMP Check Service

**Basic Settings**

Rule Name  \* Max length is 12

Check Type  ▼

Destination Address  \* Max length is 64

Destination Backup  Max length is 64

Normal Interval  \* 1-65535 s

Retry Times  \* 1-65535

Source Interface  ▼

Timeout Action  ▼

Object	Description
Rule Name	Entry name
Check Type	Icmp or domain
Destination Address	Ping main address
Destination Backup	If main address icmp fail , check backup address
Normal Interval	Ping period
Retry Times	Ping fail retry times
Source Interface	Check interface
Timeout Action	Executive action

## 5.2. Ddns

The dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, and allows access to a specified host from various locations on the Internet.



DDNS Service

**Basic Settings**

Service Provider

Server Port  1-65535

Username  \* Max length is 64

Password  \* Max length is 64

User Domain  \* Max length is 64

Update Interval  120-86400 s

Object	Description
Service Provider	Select server from the drop-down list
Server Port	port
Username	Server login username
Password	Server login password
User Domain	Domain need to translate
Update Interval	Period time to update

### 5.3. DTU

#### 5.3.1 Dtu server work mode

DTU Service

**Basic Settings**

Work Mode

Local Port  \* 1-65535

Protocol  TCP  UDP

Received Timeout  \* 1-65535 ms

RS232 Data Timeout  \* 1-65535 ms

**Reconnect**

Connect Interval  1-65535 s

Retry Times  1-65535

**Rs232 Setting**

Rate

Parity

Databits

Stopbits

Object	Description
Work Mode	server
Local Port	Server work port
Protocol	Tcp or udp
Received Timeout	Data received timeout
RS232 Data Timeout	Serial port data received timeout
Connect Interval	Try interval time if fail.
Retry Times	Fail times
Rate	Serial port data rate

Parity	Serial port data parity
Databits	Serial port data databits
Stopbits	Serial port data stopbits

### 5.3.2 Dtu client work mode

DTU Service

**Basic Settings**

Work Mode

Local Port  1-65535

Protocol  TCP  UDP

Channel Type  TREBLE  BACKUP

Received Timeout  \* 1-65535 ms

RS232 Data Timeout  \* 1-65535 ms

**Data Center Configure**

Server IP or Domain  Max length is 64

Server Port  1-65535

Server IP or Domain 2  Max length is 64

Server Port 2  1-65535

Server IP or Domain 3  Max length is 64

Server Port 3  1-65535

**Reconnect**

Connect Interval  1-65535 s

Retry Times  1-65535

**Login packets Settings**

Login Data  Max length is 64

**Heartbeat Settings**

Heartbeat Data  Max length is 64

Heartbeat Interval  1-65535 s

**Rs232 Setting**

Rate

Parity

Databits

Stopbits

[Save](#) [Refresh](#)

Object	Description
Work Mode	Client mode
Local Port	Client port
Protocol	Tcp or udp
Channel Type	Multi server type
Received Timeout	Data received timeout
RS232 Data Timeout	Serial port data received timeout
Server IP or Domain	Server 1 ip or domain
Server Port	Server 1 port
Server IP or Domain 2	Server 2 ip or domain
Server Port 2	Server 2 port
Server IP or Domain 3	Server 3 ip or domain
Server Port 3	Server 2 port
Connect Interval	Connect timeout
Retry Times	Fail retry times

Login Data	If server need login check
Heartbeat Data	Keep alive data
Heartbeat Interval	Keep alive time
Rate	Serial port data rate
Parity	Serial port data parity
Databits	Serial port data databits
Stopbits	Serial port data stopbits

### 5.4. Timing Task

This page is used to definition Timing task.

Status	<input type="button" value="Enable"/> <input type="button" value="Disable"/>
--------	--

Basic Settings	
Task Name	<input type="text"/> * Max length is 12
Task Type	<input type="text" value="custom"/> ▼
Schedule	<input type="text"/> * Max length is 64

Set Time	
Time Type	<input type="text" value="interval"/> ▼
Interval	<input type="text"/> * 1-65535 min

<input type="button" value="Save"/>	<input type="button" value="Return"/>
-------------------------------------	---------------------------------------

Object	Description
Task Name	name.
Task Type	Reboot or custom
Schedule	If select custom, manual set cmd to exc
Time Type	Time count
Interval	How many min will exc cmd

## 5.5. SMS

### 5.5.1 Inbox

This page is show inbox message for SMS.

Interface	<input type="radio"/> SIM1 <input checked="" type="radio"/> SIM2		
Classification	<input checked="" type="radio"/> Inbox <input type="radio"/> Outbox <input type="radio"/> New Message		
SMS List			
<input type="checkbox"/>	Number	Content	Time

### 5.5.2 Outbox

This page is show Outbox message for SMS.

Interface	<input type="radio"/> SIM1 <input checked="" type="radio"/> SIM2		
Classification	<input type="radio"/> Inbox <input checked="" type="radio"/> Outbox <input type="radio"/> New Message		
SMS List			
<input type="checkbox"/>	Number	Content	Time

### 5.5.3 New Message

This page is send a new message for SMS.

Interface SIM1 SIM2

Classification Inbox Outbox New Message

**Message**

Country Code

Phone Number  \* Max length is 64

**Send**

Object	Description
Country Code	Enter the country code.
Phone Number	Enter the phone number.
Text Area	Enter content in text area.

### 5.6. Data Cap

This page is used to definition Use Data cap.

Modem Select

Service Status

**Basic Settings**

Data Cap Allowance  MB

Data Cap Alert  (1-99)%

Alert Interval

Country Code

Phone Number

Monthly Cellular Data Statistics  Enable  Disable

Period Start Date  (1-28)

Cellular Data Used **0 MB**

Object	Description
Data Cap Allowance	Enter the maximum allowable cap value
Data Cap Alert	Enter the maximum allowable cap percentage
Alert Interval	Select once,once a day and once a week for power on alert interval
Country Code	Enter the country code
Phone Number	Enter the phone number
Monthly Cellular Data Statistics	Enable or disable Monthly Cellular Data Statistics
Period Start Date	Which days for period start Date
Cellular Data Used	Show the Cellular Data Used, and reset the data

### 5.7. USSD

This page is used to definition USSD(Unstructured Supplementary Service Data Settings).



Interface

Send to

Object	Description
Send to	Enter the data for USSD

## 6. VPN

### 6.1. VPND

#### 6.1.1 pptp or l2tp entry

Tunnel secrets  Max length is 64

Interface Name	Protocol	Server IP or Domain	Username	Operation				
pptptest	pptp	172.20.20.25	test	<input type="button" value="Mod"/>	<input type="button" value="Del"/>	<input type="button" value="View"/>	<input type="button" value="En"/>	<input type="button" value="Dis"/>
l2tptest	l2tp	172.20.20.25	test	<input type="button" value="Mod"/>	<input type="button" value="Del"/>	<input type="button" value="View"/>	<input type="button" value="En"/>	<input type="button" value="Dis"/>

#### 6.1.2 Add tunnel entry

VPDN Service

**Basic Settings**

Interface Name  \* Max length is 8

Protocol

Server IP or Domain  \* Max length is 64

Username  Max length is 64

Password  Max length is 64

Object	Description
Interface Name	Name of entry
Protocol	L2tp or pptp option select.
Server IP or Domain	Peer ip or domain
Username	username
Password	password

### 6.1.3 View tunnel entry

Interface Name	l2tptest
Status	disconnected
Protocol	l2tp
Local IP Address	
Remote IP	

Object	Description
Interface Name	Entry name
Status	Disconnected or connected
Protocol	L2tp or pptp
Local IP Address	Local ip

Remote IP	Remote ip
-----------	-----------

## 6.2. Tunnel

IP Tunnel Service

**Basic Settings**

Tunnel Name  \* Max length is 8

Tunnel Mode

Local Virtual IP  \* eg. 10.1.1.1

Peer Virtual IP  \* eg. 10.1.1.2

Interface Type

Local Extern Interface

Peer Extern IP  \* eg. 192.168.1.1

Object	Description
Tunnel Name	Entry name
Tunnel Mode	Ipip , gre ,grem
Local Virtual IP	Local network ip
Peer Virtual IP	Peer network ip
Interface Type	Static ip or interface
Local Extern IP	If select static ip ,manual setup wan ip. Else select which interface
Peer Extern IP	Peer wan ip

### 6.3. IPsec

Show ipsec config infomation

Phase1

Policy Name	Encrypt	Hash	Authentication	Operation	
11	des	md5	psk	Mod	Del

Phase2

Policy Name	Encrypt	Hash	Remote Subnet	Operation	
22	des	md5	192.168.0.0/24	Mod	Del

IPSec Interface

Interface Name	Encrypt Interface	Destination IP or Domain	Operation				
33	WAN	www.test.com	Mod	Del	View	En	Dis

Add   Refresh

#### 6.3.1 View ipsec entry connect status

Interface Name	22
Status	disconnected
Local Subnet	192.168.1.0/24
Remote Subnet	192.168.0.0/24

Refresh
Return

Object	Description
interfacel Name	Entry name
status	Connected or disconnected
Local subnet	Local network
<b>Remote subnet</b>	Peer network

### 6.3.2 add ipsec entry connect status

## Basic Settings

## Phase1

Policy Name	<input type="text"/>	* Max length is 12
Initiate Mode	<input type="text" value="main"/>	
Encrypt	<input type="text" value="des"/>	
Hash	<input type="text" value="md5"/>	
Authentication	<input type="text" value="psk"/>	
Pre Share Key	<input type="text"/>	* Max length is 64
Self Identify	<input type="text"/>	Max length is 64
Match identify	<input type="text"/>	Max length is 64
IKE Lifetime	<input type="text" value="28800"/>	* 120-86400 s
Group Name	<input type="text" value="group768"/>	
DPD Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
DPD Delay	<input type="text" value="30"/>	1-512 s
DPD Retry Times	<input type="text" value="4"/>	1-512 times

## Phase2

Policy Name	<input type="text"/>	* Max length is 12
Encryption Protocol	<input type="text" value="esp"/>	
Encrypt	<input type="text" value="des"/>	
Hash	<input type="text" value="md5"/>	
PFS	<input type="text" value="open"/>	
Group Name	<input type="text" value="group768"/>	

Lifetime	<input type="text" value="3600"/>	* 120-86400 s
Local Protoport	<input type="text"/> : <input type="text"/>	eg. 47:0
Remote Protoport	<input type="text"/> : <input type="text"/>	eg. 47:0
Transport Mode	<input type="text" value="auto"/>	
Local Subnet	<input type="text"/>	* eg. 192.168.1.0/24
Remote Subnet	<input type="text"/>	* eg. 192.168.1.0/24

## Ipssec

Interface Name	<input type="text"/>	* Max length is 12
Destination IP or Domain	<input type="text"/>	* Max length is 64
Encrypt Interface	<input type="text" value="br0"/>	

Save

Return

Object	Description
Phase1	Show the phase1 parameter
Policy Name	Name of entry
Initiate Mode	lpip , gre or grem tunnel mode
Encrypt	Select encrypt type,des 3des aes256/192/128
Hash	Md5,sha1,sha2_256
Authentication	Static ip or interface , if static ip ,manual config option Local Extern Ip. If interface, need select which interface on option Local Extern Interface.
Pre Share Key	Enter the pre share key
Self Identify	Enter the Self Identify
Match identify	Enter the match Identify
IKE Lifetime	Enter the IKE Lifetime
Group Name	Select group name
DPD Service	Enable or disable service
DPD Delay	Enter the delay
DPD Retry Times	Enter the retry times
Phase2	Show the phase2 parameter
Policy Name	Name of entry
Encryption Protocol	Esp,ah ,ah+esp
Encrypt	des 3des aes256/192/128
Hash	Md5,sha1,sha2_256
PFS	Open or close
Group Name	Select group name
Lifetime	Enter the Lifetime
Local Protoport	Enter the local port
Remote Protoport	Enter the remote port
Transport Mode	Auto, transport, tunnel

---

Local Subnet	Enter the local subnet network
Remote Subnet	Enter the remote subnet network
Ipssec	Show the ipsec parameter
Interface Name	Name of interface
Destination IP or Domain	Enter the ip address or domain
Encrypt Interface	Select the interface



## 6.4. OpenVpn

OPENVPN Service	<input type="button" value="Enable"/> <input type="button" value="Disable"/>
-----------------	--

Service Status	DISCONNECTED
----------------	--------------

Basic Settings	
Work Mode	<input type="text" value="client"/>
Dev	<input type="text" value="tap"/>
Protocol	<input type="text" value="tcp"/>
Destination IP or Domain	<input type="text"/> * Max length is 32
Port	<input type="text"/> * 1-65535
Compress	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
nobind	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Authentication	<input type="text" value="ssl"/>
Ca Path:	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Import"/> *
Key Path:	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Import"/> *
Cert Path:	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Import"/> *
Tls Path:	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Import"/> <input type="button" value="Del."/>
Cipher	<input type="text" value="NONE"/>

Object	Description
Openvpn service	Enable or Disable the openvpn service
Work Mode	client or multi
Dev	tap or tun,network interface type,tun(OSI Layer 3),tap(OSI Layer 2)
Protocol	tcp or udp
Destination IP or Domain	Enter the ip address or domain
Port	Enter the port
Compress	Enable or disable compress th data

---

nobind	Enable or disable specific local port
Authentication	ssl or text
Ca	Select a ca file to import ,if not
Key	Select a key file to import ,if not
Cert	Select a cert file to import ,if not
Tls	Select a tls file to import ,if not
Cipher	NONE,BF-CBC,DES-CBC,RC2-CBC,DES-EDE-CBC,DES-EDE3-CBC,DESX-CBC,RC2-40-CBC,CAST5-CBC,RC2-64-CBC,AES-128-CBC,AES-192-CBC,AES-256-CBC,SEED-CBC

## 7. Forward

### 7.1. nat

#### 7.1.1 view info

SNAT					
Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation
all	192.168.0.101	80	WAN	8080	Del

DNAT					
Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation
all	WAN	80	192.168.0.101	8080	Del

Add

Refresh

#### 7.1.2 Add DNAT

Basic Settings	
NAT Type	<input checked="" type="radio"/> DNAT <input type="radio"/> SNAT
Protocol	all ▼
Original Address Type	interface ▼
Interface	br0 ▼
Original Port	<input type="text"/> 1-65535 or [1-65535]
Mapping Address	<input type="text"/> * eg. 192.168.1.1
Mapping Port	<input type="text"/> 1-65535 or [1-65535]

Save

Return

Object

Description

NAT Type	DNAT or SNAT
Protocol	all , tcp ,udp ,icmp
Original Address Type	Interface or static ip
Interface	tcp or udp
Original Address	Enter the original address for wan interface
Original Port	Enter the original port for wan interface
Mapping Address	Enter the mapping ip address
Mapping Port	Enter the mapping port

### 7.1.3 Add SNAT

**Basic Settings**

NAT Type  DNAT  SNAT

Protocol

Original Address  \* 192.168.1.1 or 192.168.1.0/24

Original Port  1-65535 or [1-65535]

Mapping Address Type

Interface

Mapping Port  1-65535 or [1-65535]

Save

Return

Object	Description
NAT Type	DNAT or SNAT
Protocol	all , tcp ,udp ,icmp
Original Address	Interface or static ip
Original Port	tcp or udp
Mapping Address Type	Select Interface or static ip
Interface	Select the interface
Mapping Address	Enter the mapping ip address
Mapping Port	Enter the mapping port

## 7.2. Routing

### 7.2.1 view info

Route Type	Network	Gateway	Priority	Operatio
Policy Route	WAN	192.168.1.1	4	Delete
Static Route	0.0.0.0/0	WAN		Delete
Static Route	192.168.1.0/24	192.168.1.1		Delete

Add Refresh

### 7.2.2 Add Static Route

**Basic Settings**

Route Type  Static Route  Policy Route

Network  \* eg. 192.168.1.0/24

Gateway Type  ▼

Gateway  \* eg. 192.168.1.1

Save Return

Object	Description
Route Type	Static Route
Network	all , tcp ,udp ,icmp
Gateway Type	Interface or static ip
Gateway	Ip address or interface

### 7.2.3 Add Policy Route

Basic Settings

Route Type	<input type="radio"/> Static Route <input checked="" type="radio"/> Policy Route
Source Type	interface ▼
Source Interface	Modem 1 ▼
Gateway Type	interface ▼
Gateway	WAN ▼
Priority	4 * 3-252

Save Return

Object	Description
Route Type	Policy Route
Source Type	Interface or static ip
Source Interface	Interface
Network	Ip address
Gateway Type	Interface or static ip
Gateway	Interface or static ip
Priority	cost

### 7.3. RIP

Routing Information Protocol (RIP) is a standard for exchanging routing information between gateways and hosts. RIP is an interior gateway protocol.

Only exchange information with neighboring routers. If the communication between two routers does not pass through the other router, then the two routers are adjacent. The RIP protocol stipulates that no information is exchanged between non-adjacent routers.

- The information exchanged by the router is all the information known by the router. That is, its own routing table.
- Exchange routing information at a fixed time (for example, every 30 seconds), and then the router updates the routing table based on the received routing information.

The "distance" of the RIP protocol is also called "hop count" because the hop count is increased by 1 each time a router passes. RIP believes that a good route is that the number of routers it passes is small, that is, "short distance". RIP allows a path to contain up to 15 routers. Therefore, when "distance" is equal to 16, it is equivalent to unreachable. It can be seen that RIP is only suitable for small Internet.

#### 7.3.1 View RIP Info

RIP Service

**Basic Settings**

Redistribute Connected  Enable  Disable

Redistribute Static  Enable  Disable

Redistribute Kernel  Enable  Disable

Network	Operation
192.168.2.0/24	<input type="button" value="Delete"/>

Neighbor	Operation
192.168.2.1	<input type="button" value="Delete"/>

Object	Description
Redistribute Connected	Advertising direct connect routing information
Redistribute Static	Advertising static routing information
Redistribute Kernel	Advertising kernel routing information
Network	display configure direct connect network info
Neighbor	display configure neighbor router ip address

#### 7.3.2 Add Neighbor

**Basic Settings**

Add Type  Network  Neighbor

Neighbor  \* eg. 192.168.1.1

**Save** **Return**

Object	Description
Add Type	Select network or Neighbor
Neighbor	Add a entry,for configure neighbor router ip address

### 7.3.3 Add Network

**Basic Settings**

Add Type  Network  Neighbor

Network  \* eg. 192.168.1.0/24

**Save** **Return**

Object	Description
Add Type	Select network or Neighbor
Network	Add a entry,for configure direct connect network info



## 7.4. OSPF

The OSPF routing protocol is a typical link-state routing protocol. It is generally used in the same routing domain. Here, a routing domain refers to an autonomous system, which refers to a group of networks that exchange routing information with each other through a unified routing policy or routing protocol. In this AS, all OSPF routers maintain an identical database describing the structure of the AS. This database stores the state information of the corresponding links in the routing domain. The OSPF router calculates its OSPF routing table through this database.

As a link-state routing protocol, OSPF transmits Link State Advertisement (LSA) to all routers in an area. This is different from distance vector routing protocols. The distance vector routing protocol is to pass part or all of the routing table to its neighboring routers.

### 7.4.1 View OSPF Info

OSPF Service

---

**Basic Settings**

Redistribute Connected  Enable  Disable

Redistribute Static  Enable  Disable

Redistribute Kernel  Enable  Disable

Interface Name	Cost	Operation
br0	43	<input type="button" value="Delete"/>

Interface Name	Network Type	Operation
br0	broadcast	<input type="button" value="Delete"/>

Network	Area Number	Operation
192.168.0.0/24	36	<input type="button" value="Delete"/>

Neighbor	Operation
192.168.0.1	<input type="button" value="Delete"/>

Object	Description
Redistribute Connected	Advertising direct connect routing information
Redistribute Static	Advertising static routing information
Redistribute Kernel	Advertising kernel routing information
Network	display configure direct connect network info
Neighbor	display configure neighbor router ip address

### 7.4.2 Add OSPF Network

**Basic Settings**

Add Type  Network  Neighbor  Interface

Network  \* eg. 192.168.1.0/24

Area Number  \* 0-65535

**Save** **Return**

### 7.4.3 Add OSPF Neighbor

**Basic Settings**

Add Type  Network  Neighbor  Interface

Neighbor  \* eg. 192.168.1.1

**Save** **Return**

### 7.4.4 Add OSPF Interface

**Basic Settings**

Add Type  Network  Neighbor  Interface

Interface Name

Interface Attribute  Cost  Network

Cost  \* 1-65535

**Save** **Return**

Object	Description
Add Type	Interface
Interface Name	Interface or static ip
Interface Attribute	Cost or network
cost	A cost value

---

Network Type	Broadcast,non-broadcast,point-to-multipoint,point-to-point
--------------	--

## 7.5. Qos

### 7.5.1 View Qos Info

Rule Name	Control Interface	Network	Rate	Operation			
22	Modem	----	2000	Mod	Del	En	Dis

### 7.5.2 Add Qos Entry

Configure QoS rules to evenly allocate or prioritize bandwidth usage by certain Internet users.

Status

**Basic Settings**

Rule Name  \* Max length is 12

Control Interface

Network  \* eg. 192.168.1.1/24

Port  1-65535

Rate  \* 1-65535 Kbps

Ceil Rate  1-65535 Kbps

Priority  1-30

Object	Description
Rule Name	Enter a name for the service
Control Interface	Output data interface
Network	Enter the network mask
Port	Data port
Rate	Limit speed

---

Ceil Rate	Max buffer speed
Priority	The rule priority

## 8. Security

### 8.1. IP Filter

#### 8.1.1 View Filter Info

**Local Filter**

Filter mode

Action	Protocol	SRC Address	Source Port	Destination IP	Destination Port	Operation
permit	udp	192.168.1.101	567	br0	1000-62520	<input type="button" value="Del"/>

**Internet Filter**

Filter mode

Action	Protocol	SRC Address	Source Port	Destination IP	Destination Port	Operation
deny	all	192.168.1.102	1-65535	172.20.20.32	---	<input type="button" value="Del"/>



#### 8.1.2 Add Filter Entry

**Basic Settings**

Type	<input checked="" type="radio"/> Local <input type="radio"/> Internet
Default Action	<input checked="" type="radio"/> Accept <input type="radio"/> Drop
Protocol	<input type="text" value="all"/> ▼
Source IP	<input type="text"/> * 192.168.1.1 or 192.168.1.0/24
Source Port	<input type="text"/> 1-65535 or [1-65535]
Destination Type	<input type="text" value="interface"/> ▼
Interface	<input type="text" value="br0"/> ▼
Destination Port	<input type="text"/> 1-65535 or [1-65535]

Object	Description
Type	Local or Internet
Default Action	Drop or Accept
Protocol	All, tcp,udp,icmp
Source IP	from ip
Source Port	From port
Destination Type	Interface or any
Interface	Data forward interface
Destination IP	to ip
Destination Port	To ip port

## 8.2. Domain Filter

### 8.2.1 View Domain Filter

Filter mode

Domain Address	Action	Operation
www.test.com	permit	<input type="button" value="Delete"/>

### 8.2.2 Add Domain Filter

**Basic Settings**

Domain Keyword  \* eg. facebook Max length is 64

Default Action  Accept  Drop

Object	Description
Domain Keyword	Domain string
Default Action	Accept or drop this domain



### 8.3. MAC Filter

#### 8.3.1 View MAC Filter

**Local Filter**

Filter mode

MAC Address	Action	Operation
00:1a:4d:34:b1:8e	Accept	<input type="button" value="Delete"/>

**Internet Filter**

Filter mode

MAC Address	Action	Operation
00:1a:4d:34:b1:8e	Accept	<input type="button" value="Delete"/>

#### 8.3.2 Add MAC Filter

**Basic Settings**

MAC  \* eg. 00:1A:4D:34:B1:8E

Default Action  Accept  Drop

Filter mode  Local  Internet  Both

Object	Description
MAC	Select server from the drop-down list
Default Action	Accept or Drop
Filter mode	Local,Internet,Both

### 8.4. DDOS

The page provides an anti-ddos attack function, which can control sync attacks and ping attacks functions.

DDos Protect Service

Sync flood Limit Rate  \* 1-65535 s

Sync flood Limit Burst  \* 1-65535

Ping of Death Limit Rate  \* 1-65535 s

Object	Description
Sync flood Limit Rate	Select server from the drop-down list
Sync flood Limit Burst	Accept or Drop
Ping of Death Limit Rate	Local,Internet,Both

## 9. Management

### 9.1. Local Log

Local Log

Log Display Table

```
Nov 2 09:34:58 00:11:22:33:44:56 daemon.debug pppd[5146]: sent [LCP ConfReq id=0x1 <asynctest 0x0>
<magic 0xdf85f17>]
Nov 2 09:34:59 00:11:22:33:44:56 daemon.notice openvpn[5441]: OpenVPN 2.3.6 mipsel-openwrt-linux-gnu
[SSL (OpenSSL)] [LZO] [EPOLL] [MH] [IPv6] built on Nov 1 2019
Nov 2 09:34:59 00:11:22:33:44:56 daemon.notice openvpn[5441]: library versions: OpenSSL 1.0.2 22 Jan 2015,
LZO 2.08
Nov 2 09:34:59 00:11:22:33:44:56 daemon.err openvpn[5441]: ERROR: could not read Auth username from
stdin
Nov 2 09:34:59 00:11:22:33:44:56 daemon.notice openvpn[5441]: Exiting due to fatal error
Nov 2 09:35:01 00:11:22:33:44:56 daemon.info openvpn_init[18256]: openvpn exited!(openvpn_init.c, line 171)
Nov 2 09:35:01 00:11:22:33:44:56 daemon.debug pppd[5146]: sent [LCP ConfReq id=0x1 <asynctest 0x0>
<magic 0xdf85f17>]
Nov 2 09:35:04 00:11:22:33:44:56 daemon.debug pppd[5146]: sent [LCP ConfReq id=0x1 <asynctest 0x0>
<magic 0xdf85f17>]
Nov 2 09:35:05 00:11:22:33:44:56 daemon.notice openvpn[5587]: OpenVPN 2.3.6 mipsel-openwrt-linux-gnu
[SSL (OpenSSL)] [LZO] [EPOLL] [MH] [IPv6] built on Nov 1 2019
Nov 2 09:35:05 00:11:22:33:44:56 daemon.notice openvpn[5587]: library versions: OpenSSL 1.0.2 22 Jan 2015,
LZO 2.08
Nov 2 09:35:05 00:11:22:33:44:56 daemon.err openvpn[5587]: ERROR: could not read Auth username from
stdin
Nov 2 09:35:05 00:11:22:33:44:56 daemon.notice openvpn[5587]: Exiting due to fatal error
Nov 2 09:35:07 00:11:22:33:44:56 daemon.info openvpn_init[18256]: openvpn exited!(openvpn_init.c, line 171)
Nov 2 09:35:07 00:11:22:33:44:56 daemon.debug pppd[5146]: sent [LCP ConfReq id=0x1 <asynctest 0x0>
<magic 0xdf85f17>]
```

Object	Description
Local Log	Kernel,Application,Message
<b>View</b>	Show log
<b>Clear</b>	Clear log record
<b>Export</b>	Export log to save

## 9.2. Remote Log

Log Status	<input type="button" value="Enable"/> <input type="button" value="Disable"/>
Remote IP or Domain	<input type="text" value="192.168.1.100"/> * eg. 192.168.1.1
Remote Port	<input type="text" value="514"/> * 1-65535

Object	Description
<b>Log Status</b>	Enable or disable "Logging to Syslog Server"
<b>Remote IP or Domain</b>	Syslog server IP address
<b>Remote Port</b>	Server port

## 9.3. NTP Server

### 9.3.1 Enable ntp system time

Status

Time sync Type

NTP Server IP or Domain  \* Max length is 64

NTP Server BackUp  \* Max length is 64

NTP sync Interval  \* 1-65535 s

Time Zone

Object	Description
Time sync Type	Sync time from time server
NTP Server IP or Domain	First Time server
NTP Server BackUp	Swich to second time server when first time server sync fail
NTP sync Interval	How to get time from server
Time Zone	Fix time zone
Time Zone Number	If you select customer time zone , you can manual set time zone

### 9.3.2 Enable manual system time

Status

Time sync Type

Set Date  -  -  eg. 1970-01-01

Set Time  -  -  eg. 07:01:01

Object	Description
Time sync Type	Manual set system time
Set Date	Which date
Set Time	Which time

## 9.4. Service Control

Service	LAN	WAN	PORT	Access from network
TELNET	<input type="checkbox"/>	<input type="checkbox"/>	52323	<input type="text"/>
PING	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="text"/>
WEB	<input checked="" type="checkbox"/>	<input type="checkbox"/>	80	<input type="text"/>
SSH	<input type="checkbox"/>	<input type="checkbox"/>	22	<input type="text"/>

Save

Refresh

Object	Description
Service Type	The following services can be configured with access permissions
lan	Select to allow lan access
wan	Select to allowwan access
port	Enter the port to allow access
Access from network	Enter the ip to allow access, When multiple IP address are allowed, they can be separated by a separator character "/"

## 9.5. Account

Current Username	<input type="text" value="admin"/>
Admin Password	<input type="text"/> * Max length is 64
New Password	<input type="text"/>
New Password Confirm	<input type="text"/>

Save

Refresh

Object	Description
Account Type	Web login account
Current Username	username
Admin Password	password
New Password	New password
New Password Confirm	Confirm new password

## 9.6. Diagnostics

Destination  \* [Ping](#) [Trace](#)

---

**Result**

```

PING www.baidu.com (183.232.231.172): 56 data bytes
64 bytes from 183.232.231.172: seq=0 ttl=55 time=7.291 ms
64 bytes from 183.232.231.172: seq=1 ttl=55 time=7.323 ms
64 bytes from 183.232.231.172: seq=2 ttl=55 time=7.476 ms
64 bytes from 183.232.231.172: seq=3 ttl=55 time=7.165 ms
64 bytes from 183.232.231.172: seq=4 ttl=55 time=7.370 ms

--- www.baidu.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.165/7.325/7.476 ms

```

Object	Description
Destination	Ntp or manual
ping	Ping cmd to test network
trace	Trace cmd to test network
result	Show ping or trace cmd result

## 9.7. Upgrade/Settings

Firmware Setting  No file chosen   Reset

Backup setting  No file chosen

Factory setting

Object	Description
<b>Upgrade</b>	Click this button to start upgrade system
<b>Select</b>	Select the upgrade system bin file or config file
<b>Reset</b>	If select this option when upgrade system , syetem config will restore to factory.
<b>Import</b>	Import a backup config
<b>Export</b>	Export config to backup
<b>Factory Default</b>	Restore system config to factory mode
<b>Reboot</b>	Restart system