

comms
365

C365-4G-H900

COMMS365 H900 4G Router

(and C365-5G-H900 Options where applicable)

PART 2



USER MANUAL

Contents

3.5.7 SMS.....	3
3.5.8 VPN.....	11
3.5.8.1 IPSEC.....	11
3.5.8.2 PPTP.....	15
3.5.8.3 L2TP.....	18
3.5.8.4 OpenVPN.....	20
3.5.8.5 GRE Tunnel.....	21
3.5.9 DDNS.....	23
3.5.10 Connect Radio Module.....	27
3.6 Network Configuration.....	28
3.6.1 Operation Mode.....	28
3.6.1.1 LAN Ethernet Ports.....	29
3.6.2 Mobile Configuration.....	29
3.6.3 Cell Mobile Data Limitation.....	34
3.6.4 LAN Settings.....	35
3.6.5 Wired-WAN.....	38
3.6.6 Wi-Fi Settings.....	40
3.6.6.1 Wi-Fi General Configuration.....	40
3.6.6.2 Wi-Fi Advanced Configuration.....	41
3.6.6.3 Wi-Fi Interface Configuration.....	42
3.6.6.4 Wi-Fi AP Client.....	44
3.6.7 Interfaces Overview.....	46
3.6.8 Firewall.....	47
3.6.8.1 General Settings.....	47
3.6.8.2 Port Forwards.....	47
3.6.8.3 Traffic Rules.....	48
3.6.8.4 DMZ.....	51
3.6.8.5 Security.....	52
3.6.9 Static Routes.....	53
3.6.10 Switch.....	54
3.6.11 DHCP and DNS.....	55
3.6.12 Diagnostics.....	57
3.6.13 Loopback Interface.....	58
3.6.14 Dynamic Routing.....	58
3.6.15 QoS.....	61
3.6.16 Guest LAN (Guest Wi-Fi).....	62

3.5.7 SMS

SMS Command

SMS Command

Enable ☐

SMS ACK ☐

Fix error for some network ☐

Reboot Router Command

Get Cell Status Command

Set Cell link-up Command

Set Cell link-down Command

DIO_0 Set Command ▶ Set DIO0

DIO_0 Reset Command ▶ Reset DIO0

DIO_1 Set Command ▶ Set DIO1

DIO_1 Reset Command ▶ Reset DIO1

DIO_2 Set Command ▶ Set DIO2

DIO_2 Reset Command ▶ Reset DIO2

DIO_3 Set Command ▶ Set DIO3

DIO_3 Reset Command ▶ Reset DIO3

DIO Status Command

Wifi On Command

Wifi Off Command

Force Cellup Command

Operator List Command

Operator set Command

- **Enable:** Check the box to enable the SMS command feature.
- **SMS ACK:** If checked, the router will send the command feedback to the sender's phone number. If unchecked, the router will not send the command feedback to the sender's phone number.
- **Reboot Router Command:** Input the command for "reboot" operation, default is "reboot".
- **Get Cell Status Command:** Input the command for "router cell status checking" operation, default is "cell status". For example, if we send "cell status" to the router, the router will feedback the status to the sender such as "Router SN: 086412090002 cell_link_up", which identifies the router SN number and Cell Working Status.
- **Set cell link-up Command:** Input the command for the "router cell link up" operation, default is "cell up". If the router receives this command, the Router Cell will be online.
- **Set cell link-down Command:** Input the command for "router cell link down" operation, default is "cell down". If router gets this command, the Router Cell will be offline.
- **DIO_0 Set Command:** set I/O port 0 to high (1). For the SMS feature, please keep the parameter as default.
- **DIO_0 Reset Command:** set I/O port 0 to low (0). For the SMS feature, please keep the parameter as default.
- **DIO_1 Set Command:** set I/O port 1 to high (1). For the SMS feature, please keep the parameter as default.
- **DIO_1 Reset Command:** set I/O port 1 to low (0). For the SMS feature, please keep the parameter as default.
- **DIO_2 Set Command:** set I/O port 2 to high (1). For the SMS feature, please keep the parameter as default.
- **DIO_2 Reset Command:** set I/O port 2 to low (0). For the SMS feature, please keep the parameter as default.
- **DIO_3 Set Command:** set I/O port 3 to high (1). For the SMS feature, please keep the parameter as default.
- **DIO_3 Reset Command:** set I/O port 3 to low (0). For the SMS feature, please keep the parameter as default.
- **Button Set/Reset DIO:** Set the DIO to high or low immediately.
- **DIO Status Command:** Input the command for I/O port status. For the SMS feature, please keep the parameter as default.
- **Wi-Fi on Command:** Input the command for turning on the Wi-Fi. For the SMS feature, please keep the parameter as default.
- **Wi-Fi off Command:** Input the command for turning off the Wi-Fi. For the SMS feature, please keep the parameter as default.
- **Force Cellup Command:** If the cell is down due to traffic limitation, then it can be brought up by this command.
- **Operator List Command:** Send the modem operator list as SMS, it is only supported by some specific modems.
- **Operator set Command:** Set the modem to operator manually, it is only supported by some specific modems.

SMS Alarm

SMS Alarm

SMS Alarm ☐

RSSI Alarm Settings

Signal Alarm

Enable Signal Quality Alarm ☐

Signal Quality Threshold

Failed Times Threshold

Success Times Threshold

- **SMS Alarm:** Enable SMS alarm feature.
- **Enable Signal Quality Alarm:** Enable the signal quality alarm feature.
- **Signal Quality Threshold:** When the signal alarm is generated and the real time signal strength is lower than the signal quality threshold, then reset the success counter to 0. If the real time signal strength is bigger than this threshold, the success counter will add one.
- When the signal alarm is not generated and the real time signal strength is lower than the signal quality threshold, the failed counter will add one. If the real time signal strength is bigger than this threshold, reset the failed counter to 0.
- **Failed Times Threshold:** If the failed counter is more than this threshold, a signal alarm will be generated.
- **Success Times Threshold:** If a signal alarm is generated, and the success counter is bigger or equal to the success times threshold, a clear signal will alarm.

Phone Number

Phone Number

Phone Number Configuration

NUM1

Delete

SMS Command

☐

SMS Alarm

☐

DIO change

☐

Phone Number

New group name

Add

Save & Apply

Save

Reset

- **Add Phone number:** Input a name and click the “Add” button to add a new Phone number.
- **Delete Phone number:** Click the “Delete” button.
- **SMS command:** Enable the SMS command feature on this phone number.
- **SMS alarm:** This phone number can receive an SMS Alarm.
- **DIO change:** DIO change alarm can be sent to this phone number.

SMS Number

Send SMS

Receiver Phone Number

Message

Submit

Reset

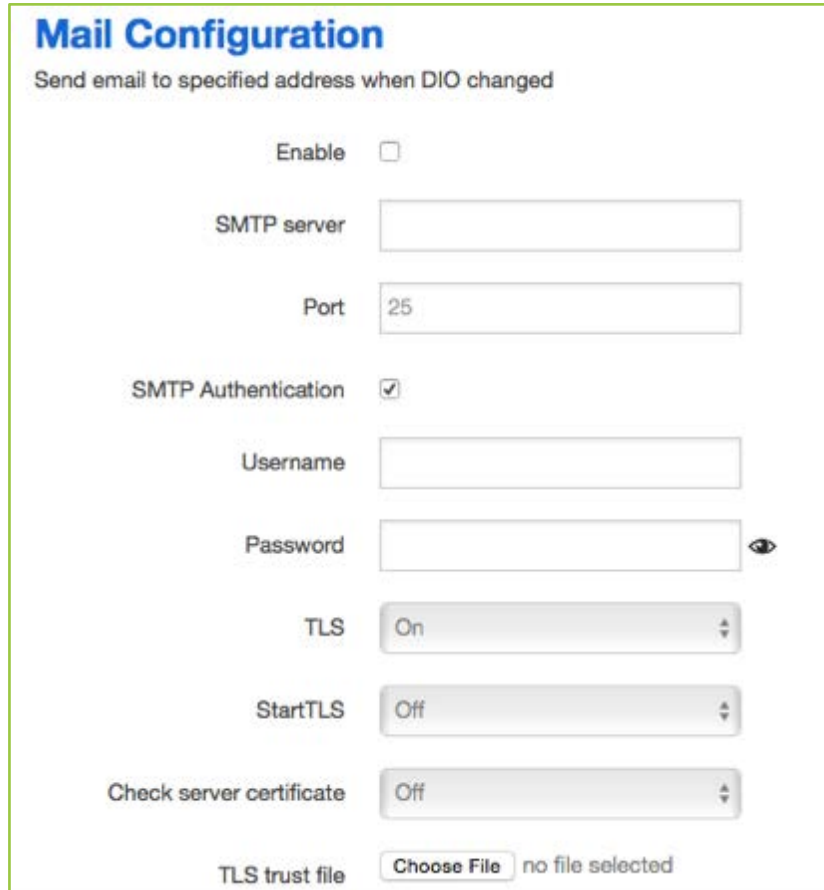
SMS Log

Received SMS: sender: 10010; time: 18-11-19 12:37:11; msg:
Received SMS: sender: 10010; time: 18-11-19 12:37:11; msg:

- **Receiver Phone Number:** The Phone number that receives the message.
- **Message:** The content of the message.
- **Submit:** Click the “Submit” button to send the message immediately.
- **SMS Log:** The SMS send and receive log.

DIO Mail

Send the email to the receiver when the DIO is changed.



Mail Configuration
Send email to specified address when DIO changed


Enable ☐

SMTP server

Port

SMTP Authentication ☒

Username

Password 

TLS

StartTLS

Check server certificate

TLS trust file no file selected

- **Enable:** Activate the DIO Mail functionality.
- **SMTP server:** SMTP server IP address or URL.
- **Port:** SMTP server port.
- **SMTP Authentication:** If SMTP server requires SMTP Authentication, enable it.
- **Username:** Username for the SMTP authentication.
- **Password:** Password for the SMTP authentication.
- **TLS:** Enable or disable TLS (also known as SSL) for secured connections.
- **StartTLS:** Choose the TLS variant: start TLS from within the session ('on', default), or tunnel the session through TLS ('off').
- **Check server certificate:** Activate server certificate verification using a list of trusted Certification Authorities (CAs).
- **TLS trust file:** Activate server certificate verification using trusted Certification Authorities (CAs).

DIO_0 name	<input type="text" value="DIO0"/>
DIO_0 high text	<input type="text" value="1"/>
DIO_0 low text	<input type="text" value="0"/>
DIO_1 name	<input type="text" value="DIO1"/>
DIO_1 high text	<input type="text" value="1"/>
DIO_1 low text	<input type="text" value="0"/>
DIO_2 name	<input type="text" value="DIO2"/>
DIO_2 high text	<input type="text" value="1"/>
DIO_2 low text	<input type="text" value="0"/>
DIO_3 name	<input type="text" value="DIO3"/>
DIO_3 high text	<input type="text" value="1"/>
DIO_3 low text	<input type="text" value="0"/>

The default email title is "[DIOx] changed", and content is SN:8600000000, [DIOx] is changed from [value0] to value [1]. Configure the email title and content, replace string in [].


Receiver Configuration

11

DIO change ☐

Email address

New group name

 Add

Delete

DIO Default

DIO Configuration

DIO trap ☐Set DIO to high for a period of time sDIO_0 default value DIO_1 default value DIO_2 default value DIO_3 default value

DIO_0 Value 0

DIO_1 Value 0

DIO_2 Value

DIO_3 Value

DIO_0 Function DIO_1 Function DIO_2 Function DIO_3 Function

- **DIO trap:** Send SNMP trap when DIO is changed from 1 to 0, or 0 to 1.
- **Set DIO to high for a period of time:** If setting DIO to high after a period of time, DIO will change to low automatically, value 0 means disable.
- **DIO_0 default value:** DIO default value is low (0). If set to high (1), when device is up, it will be set to high automatically.
- **DIO_1 default value:** DIO default value is low (0). If set to high (1), when device is up, it will be set to high automatically.
- **DIO_2 default value:** DIO default value is low (0). If set to high (1), when device is up, it will be set to high automatically.
- **DIO_3 default value:** DIO default value is low (0). If set to high (1), when device is up, it will be set to high automatically.

- **DIO_0 Value:** DIO current value, 0 means low, and 1 means high.
- **DIO_1 Value:** DIO current value, 0 means low, and 1 means high.
- **DIO_2 Value:** DIO current value, 0 means low, and 1 means high.
- **DIO_3 Value:** DIO current value, 0 means low, and 1 means high.
- **DIO_0 Function:** DIO function can be set to None, GPS and Wi-Fi. DIO value is set to high to turn on functionality, set it to low to turn it off. If the value is None, it will do nothing.
- **DIO_1 Function:** DIO function can be set to None, GPS and Wi-Fi. DIO value is set to high to turn on functionality, set it to low to turn it off. If the value is None, it will do nothing.
- **DIO_2 Function:** DIO function can be set to None, GPS and Wi-Fi. DIO value is set to high to turn on functionality, set it to low to turn it off. If the value is None, it will do nothing.
- **DIO_3 Function:** DIO function can be set to None, GPS and Wi-Fi. DIO value is set to high to turn on functionality, set it to low to turn it off. If the value is None, it will do nothing.

DIO SMS

DIO SMS configuration

send user defined SMS alarm when DIO changed

Enable user-defined DIO SMS alarm ☒

SMS text for DIO0 changed from low to high

SMS text for DIO0 changed from high to low

SMS text for DIO1 changed from low to high

SMS text for DIO1 changed from high to low

SMS text for DIO2 changed from low to high

SMS text for DIO2 changed from high to low

SMS text for DIO3 changed from low to high

SMS text for DIO3 changed from high to low

When the DIO value is changed, it sends an SMS text accordingly. It must enable the DIO change on the phone number. If the user-defined text is empty, it will send a system default SMS to the phone number. The default format is SN:[860000000000], [DIOx] is changed from [value1] to [value0].

3.5.8 VPN

3.5.8.1 ISPEC

Instance name	Enable	Exchange mode	Auth method	Operation level	
IPSec_base	Yes	IKEv1-Main	PSK Client	Main	Edit Delete

New instance name: Client [Add](#)

Enable Route-based IPsec ☐

[Save & Apply](#) [Save](#) [Reset](#)

This page is a list of configured IPsec instances and their state. Click the “**Edit**” button to modify it or click the “**Delete**” button to delete an instance.

The default setting is Policy-based IPsec, if Enabled the Route-based IPsec box is ticked, after click “**Save & Apply**”, it will then switch to Route-based IPsec.

IPSec Instance: IPSec_base

[Switch to advanced configuration »](#)

Enable ☒

Exchange mode

Operation Level

Authentication method

Remote VPN endpoint

Local endpoint

Local IKE identifier

Remote IKE identifier

Preshared Keys 

Perfect Forward Secrecy

DPD action

DPD delay seconds

DPD timeout seconds

NAT Traversal

- **Enable:** Enable the IPSEC feature.
- **Exchange mode:** IKEv1-Main, IKEv1-Aggressive, and IKEv2-Main modes are supported.
- **Operation Level:** For IPsec backup. One level is Main and the other is Backup. If the Main instance is down then switch to the backup instance.
- **Authentication method:** PSK Client, PSK Server, RSA X.509 Client and RSA X.509 Server. Client is the device which starts the IPSEC connection.
- **Remote VPN endpoint:** Domain name or IP address of the remote endpoint. It can be visited from the Internet.
- **Local endpoint:** Domain name or IP address or interface name of this device.
- **Local IKE identifier:** Identity the use of the local device authentication.
- **Remote IKE identifier:** Identity the use of the remote device authentication.
- **Preshared Keys:** Pre-shared key authentication, known as PSK.
- **Perfect Forward Secrecy:** Confirm whether Perfect Forward Secrecy of keys is desired on the connection's keying channel.
- **DPD action:** Controls the use of the Dead Peer Detection protocol (DPD, RFC 3706) where R_U_THERE notification messages (IKEv1) or empty INFORMATIONAL messages (IKEv2) are periodically sent in order to check the activeness of the IPsec peer. The values are clear, hold, and restart, all of which activate the DPD and determine the action to perform on a timeout. Clear: The connection is closed with no further actions taken. Hold: Installs a trap policy, which will catch matching traffic and tries to re-negotiate the connection on demand. Restart: Immediately triggers an attempt to re-negotiate the connection. The default is none which disables the active sending of DPD messages
- **DPD delay:** Defines the period time interval with which R_U_THERE messages/INFORMATIONAL exchanges are sent to the peer.
- **DPD timeout:** Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity.
- **NAT Traversal:** Indicates whether the device is behind a NAT device or not.

The screenshot shows a configuration window with the following fields:

- Local LAN bypass:** A checkbox that is checked.
- Local subnet:** A text input field containing "192.168.1.0/24" with a small blue icon to its right.
- Remote subnet:** A text input field containing "0.0.0.0/0" with a small blue icon to its right.
- Local source ip:** An empty text input field.
- Remote source ip:** An empty text input field.

- **Local subnet:** The local subnet which connects to the IPSEC VPN.
- **Remote subnet:** The remote subnet which connects to the IPSEC VPN.
- **Local source ip:** The internal source IP of the local device to use in a tunnel, also known as virtual IP.
- **Remote source ip:** The internal source IP of the remote device to use in a tunnel, also known as virtual IP.

Phase 1 Proposal

Enable ☒

Encryption algorithm 3DES ▼

Hash algorithm HMAC_MD5 ▼

DH group MODP1024/2 ▼

Life time 86400 seconds

Phase 2 Proposal

Enable ☐

Encryption algorithm AES 128 ▼

PFS group MODP1024/2 ▼

Authentication HMAC_SHA1 ▼

Life time 86400 seconds


Note: All the configurations in the Phase 1 Proposal and Phase 2 Proposal must match the remote endpoint to establish an IPSEC connection.

3.5.8.2 PPTP

Point-to-Point Tunneling Protocol

PPTP Configuration

Below is a list of configured PPTP instances and their state.

Name	Type	Enable	
	Server	No	 Edit  Delete

New instance name: Role:  Add New

PPTP NAT enable ☒


Save & ApplySaveReset

This page is a list of configured PPTP instances and their state. Click the **Edit** button to modify it or click the **Delete** button to delete an instance.

PPTP NAT enable: Enable PPTP interface NAT.

PPTP Client configuration

PPTP Client Instance: Client**Main Settings**

Enable	<input type="checkbox"/>
Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/> 
Remote LAN subnet	<input type="text"/>
Remote LAN netmask	<input type="text"/>
MTU	<input type="text" value="1500"/>
Keep Alive	<input type="text"/>
Use DNS servers advertised by peer	<input checked="" type="checkbox"/>
MPPE Encryption	<input checked="" type="checkbox"/>
Debug	<input type="checkbox"/>
Restart module when PPTP connects failed	<input checked="" type="checkbox"/>

- **Enable:** Enable this instance.
- **Server:** The domain name or IP address of the PPTP server.
- **Username:** Server authentication username.
- **Password:** Server authentication password.
- **Remote LAN subnet:** The remote subnet which can be accessed via the PPTP tunnel, such as 192.168.10.0
- **Remote LAN netmask:** The netmask for the remote LAN subnet, such as 255.255.255.0
- **MTU:** Maximum transmission unit.
- **Keep Alive:** Number of unanswered echo requests before considering the peer is dead. The interval between the echo requests is 5 seconds.
- **Use DNS servers advertised by peer:** If unchecked, the advertised DNS server addresses are ignored.

- **MPPE Encryption:** Microsoft Point-to-Point Encryption.
- **Debug:** Add verbose PPTP log in the system log.
- **Restart module when PPTP connects failed:** Some network PPTP cannot connect until module is restarted.

PPTP Server Configuration

PPTP Server Instance:

Main Settings

Enable ☐

PPTP Local IP

PPTP remote IP start

PPTP remote IP end

ARP Proxy

☐

MPPE Encryption

☒

Debug

☐

Username	Password	
admin	<input type="button" value="Delete"/>



- **PPTP Local IP:** Indicate server's IP address.
- **PPTP remote IP start:** The remote IP address leases start.
- **PPTP remote IP end:** The remote IP address lease end.
- **ARP Proxy:** If the remote IP has the same subnet as the LAN, check it for connecting one another.
- **MPPE Encryption:** Microsoft Point-to-Point Encryption.
- **Debug:** Add verbose PPTP log in the system log.
- **Username:** Server authentication username.
- **Password:** Server authentication password.

3.5.8.3 L2TP

This page is a list of configured L2TP instances and their state. The user can click the “**Edit**” button to modify it or click the “**Delete**” button to delete an instance.

Layer 2 Tuneling Pprotocol

L2TP Configuration

Name	Type	Enable	
L2tpd_server	Server	No	 


New instance name:

Role:

Client

Client

Server

 Add New

L2TP Client configuration

L2TP Client Instance: Cli

Main Settings


Enable

☐

Server

Username

Password



Remote LAN subnet

Remote LAN netmask

MTU

Keep Alive

Debug

☐

- **Enable:** Enable this L2TP instance.
- **Server:** Domain name or IP address of L2TP server.
- **Username:** Server authentication username.
- **Password:** Server authentication password.
- **Remote LAN subnet:** The remote LAN subnet can be accessed via the L2TP tunnel, such as 192.168.10.0.
- **Remote LAN netmask:** The netmask for remote LAN subnet, such as 255.255.255.0
- **MTU:** Maximum transmission unit.
- **Keep Alive:** Number of unanswered echo requests before considering the peer is dead. The interval between the echo requests is 5 seconds.
- **Checkup Interval:** Number of seconds passed before checking if the interface is not up since the last setup attempt and retrying the connection. Set it to a value sufficient for a successful L2TP connection for you. It's because the netifd sent the connect request yet the xl2tpd failed to complete it without the notice of netifd.
- **Debug:** Add L2TP verbose log into the system log.

L2TP Server configuration

L2TP Server Instance: L2tpd_server

Main Settings

Enable

☐

L2TP Local IP

Remote IP range begin

Remote IP range end

Remote LAN IP

Remote LAN netmask

ARP Proxy

☐

Debug

☐

Username	Password
admin

Add

- **Local IP:** Indicate the server's IP address.
- **Remote IP range begin:** The remote IP address leases start.
- **Remote IP range end:** The remote IP address lease end.
- **Remote LAN IP:** The remote LAN subnet can be accessed via the L2TP tunnel, such as 192.168.10.0.
- **Remote LAN netmask:** The mask of the L2TP client IP, the default value is 255.255.255.0.
- **ARP Proxy:** It allows the remote L2TP client to access the local LAN subnet. The remote IP range should be included in the LAN subnet, for example if the local LAN subnet is 192.168.1.0/24, then configure the remote IP range starting with 192.168.1.20 and the remote IP range ending in 192.168.1.30, and enable the ARP Proxy.
- **Debug:** Add the L2TP verbose log into system log.
- **Username:** Server authentication username
- **Password:** Server authentication password.

3.5.8.3 Open VPN

This page is a list of the configured OpenVPN instances and their states. You can click the “**Edit**” button to modify it or click the “**Delete**” button to delete an instance. You can click the “**Start**” button to start or “**Stop**” button stop a specific instance.

OpenVPN

OpenVPN instances

Please goto overview page to restart openVPN instance manually after Save&Apply

	enabled	Started	Start/Stop	Tun/Tap	Port	Protocol	
custom_config	No	no	start	tun	1194	udp	Edit Delete
sample_server	No	no	start	tun	1194	udp	Edit Delete
sample_client	No	no	start	tun	1194	udp	Edit Delete

Client configuration for an ethernet Add

Save & Apply **Save** **Reset**

Note: For the OpenVPN configuration page, you can put the mouse on the title of the item to get more help information.

If the item you needed is not shown on the main page, please check the “**Additional Field**” dropdown list at the bottom of the page.

Overview » Instance "sample_server"

[« Switch to basic configuration](#)

Configuration category: **Service** | Networking | VPN | Cryptography

Service

enabled ☐

verb

mlock ☐

disable_occ ☐

-- Additional Field --

- cd
- chroot
- log
- log_append
- nice
- echo
- remap_usr1
- status_version
- mute
- up
- up_delay
- down
- route_up
- setenv
- tls_verify
- client_connect
- learn_address
- auth_user_pass_verify**

-- Additional Field --

3.5.8.5 GRE Tunnel

IPSec | PPTP | L2TP | **OpenVPN** | GRE Tunnel

GRE Tunnel Configuration

Instance name	Enable	Peer IP addr	Remote network	Local tunnel IP
GRE	No			

New instance name:

GRE Tunnel

GRE Instance: Gre_tunnel

Enable ☐

TTL

255

MTU

1500

Peer IP Address

Remote LAN subnet

Remote LAN netmask

Metric

0

Local Interface

All ▼

Local Tunnel IP

Local Tunnel Mask

Keepalive

None ▼

- **Enable:** Enable the GRE tunnel feature.
- **TTL:** Time-to-live.
- **MTU:** Maximum transmission unit.
- **Peer IP address:** The remote WAN IP address.
- **Remote Network IP:** The remote LAN subnet address that can be accessed via the GRE tunnel, such as 192.168.10.0.
- **Remote Netmask:** The remote LAN subnet mask. Such as 255.255.255.0.
- **Local Tunnel IP:** Virtual IP address. It cannot be in the same subnet as the LAN network.
- **Local Tunnel Mask:** Virtual IP mask.
- **Local Interface:** Bond a specific interface for the GRE tunnel.
- **Keepalive:** Options are None, receive only, send and receive. If the value is None, the GRE tunnel will remain up, if the value is receive only and if no GRE keepalive message is received for the peer device, it will set the tunnel to up. If the value is send and receive, it will send a keepalive message to the remote peer and it will receive a keepalive message from the peer.

3.5.9 DDNS

DDNS allows the router to be reached with a fixed domain name while having a dynamically changing IP address.

Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Overview

Below is a list of configured DDNS configurations and their current state.
If you want to send updates for IPv4 and IPv6 you need to define two separate Configurations i.e. 'myddns_ipv4' and 'myddns_ipv6'

Configuration	Hostname/Domain Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop	
example_ipv4	1534I9866a.iok.la <i>No data</i>	<input checked="" type="checkbox"/>	Never Verify	● PID: 3229	Edit Delete
myddns_ipv6	yourhost.example.com <i>No data</i>	<input type="checkbox"/>	Never Disabled	Edit Delete

[Add](#)

[Save & Apply](#)
[Save](#)
[Reset](#)

Details for: example_ipv4

[Basic Settings](#)
[Advanced Settings](#)
[Timer Settings](#)
[Log File Viewer](#)


Enabled ☒

IP address version ☒ IPv4-Address ☐ IPv6-Address

DDNS Service provider [IPv4] oray.com ▼

Hostname/Domain

Username

Password 

- **Enabled:** Enable this instance.
- **IP address version:** IPv4 and IPv6 supported.
- **DDNS Service provider:** Select a suitable provider.
- **Hostname/Domain:** The domain name that you can access the router by.

Basic Settings Advanced Settings Timer Settings Log File Viewer

IP address source [IPv4]

Network [IPv4]

DNS-Server

PROXY-Server

Log to syslog

Log to file ☒

- **IP address source:** Defines the source that reads the systems IPv4-Address from and that will be sent to the DDNS provider. The recommended option is network.
- **Network:** Defines the network that reads the systems IPv4-Address from.
- **DNS-server:** OPTIONAL: Use the non-default DNS-Server to detect 'Registered IP'. IP address and domain name is required.
- **Log to syslog:** Writes log messages to syslog. Critical Errors will always be written to syslog.
- **Log to file:** Writes detailed messages to the log file. The file will be truncated automatically.

Basic Settings Advanced Settings Timer Settings Log File Viewer

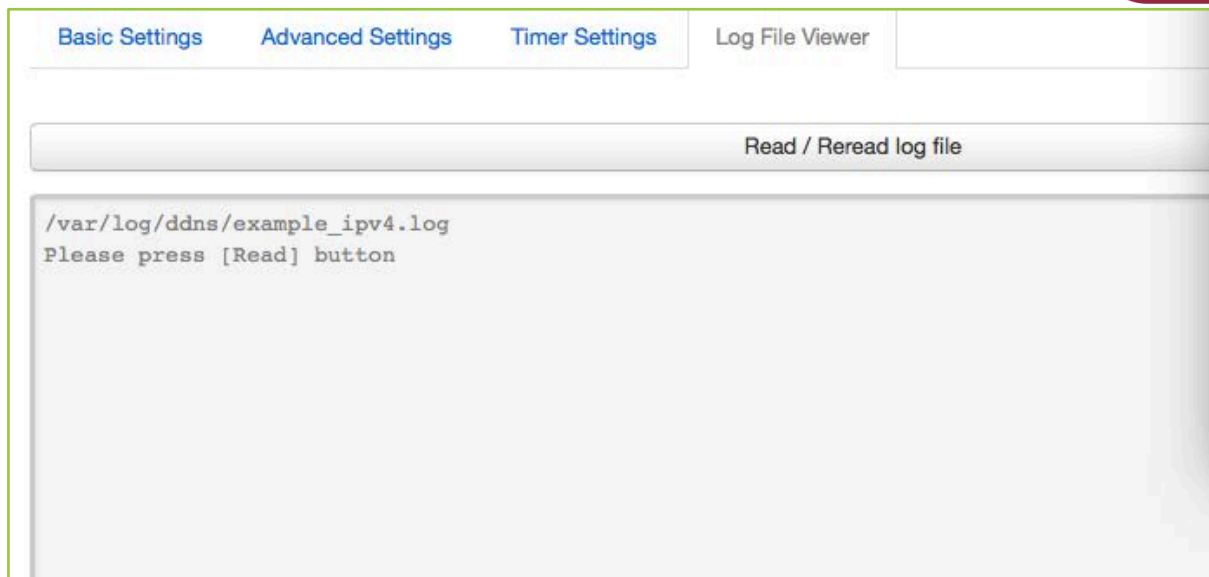
Check Interval

Force Interval

Error Retry Counter

Error Retry Interval

- **Check Interval:** The minimum check interval is 1 minute=60seconds.
- **Force interval:** The minimum check interval is 1 minute=60seconds.
- **Error Retry Counter:** On Error the script will stop execution after a given number of retries. The default setting of '0' will retry infinitely.



Note: If using the DDNS server no-ip.com, please check that the "Use HTTP Secure" box and put "8.8.8.8" for the DNS-Server, referring to the following picture.

Details for: example_ipv4

Basic Settings Advanced Settings Timer Settings Log File Viewer

Enabled ☐

IP address version

☒ IPv4-Address
☐ IPv6-Address

DDNS Service provider [IPv4]

No-IP.com ▼

Hostname/Domain


yourhost.example.com

Username

your_username

Password

.....



Use HTTP Secure ☒

Path to CA-Certificate

/etc/ssl/certs

Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Details for: example_ipv4

[Basic Settings](#)[Advanced Settings](#)[Timer Settings](#)[Log File Viewer](#)

IP address source [IPv4]

Network [IPv4]

DNS-Server

PROXY-Server

Log to syslog

Log to file ☒

Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Details for: example_ipv4

[Basic Settings](#)[Advanced Settings](#)[Timer Settings](#)[Log File Viewer](#)

IP address source [IPv4]

Network [IPv4]

DNS-Server

PROXY-Server

Log to syslog

Log to file ☒

3.5.10 Connect Radio Module

Connect the Radio Module feature is used for exchanging data between the Radio module and the serial.

Notes: This feature conflicts with the DTU and “GPS sent to serial”. Please make sure that the other two features are disabled before enabling the Connect Radio Module. Otherwise this error will occur.

Connect Radio Module Configuration

Exchange data between radio module and serial

Enable ☒

Connect mode

Serial baudrate

Serial parity

Serial databits

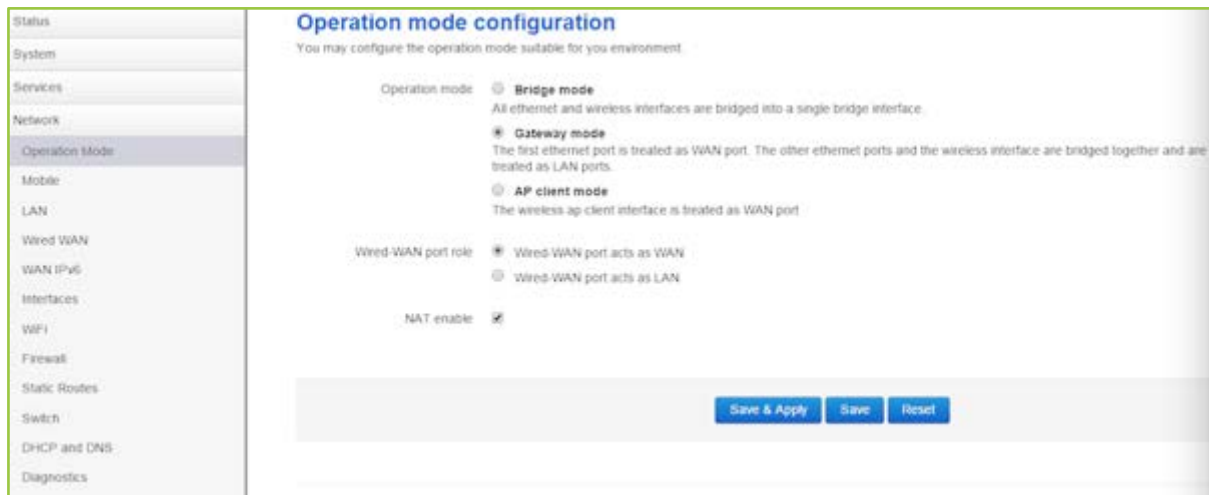
Serial stopbits

• Enable: conflict with DTU, please disable DTU firstly

- **Connect Mode:** Serial only.
- Modem to Serial Settings
- **Serial baudrate:** Supports 9600/19200/38400/57600/115200bps
- **Serial parity:** Supports none/odd/even
- **Serial databits:** Supports 7 bits and 8 bits
- **Serial stopbit:** Supports 1 bits and 2 bits
- **Serial Flow Control:** Supports none/hardware/software

3.6 Network Configuration

3.6.1 Operation Mode



Operation mode

- **Bridge:** All Ethernet and wireless interfaces are bridged into a single bridge interface.
- **Gateway:** The first Ethernet port is treated as a WAN port. The other Ethernet ports and the wireless interface are bridged together and are treated as LAN ports.
- **AP Client:** The wireless apcli interface is treated as a WAN port and the wireless AP interface and the Ethernet ports are LAN ports.

NAT Enabled

Network Address Translation. Default is Enabling.

Ethernet wan port role:

Wired-WAN port acts as WAN.

The Ethernet WAN port is used as the WAN. Default is Checked.

Wired-WAN port acts as LAN.

The Ethernet WAN port is used as the LAN port to get 2 LAN Ethernet ports. If the WAN RJ45 Ethernet port is used for the WAN, please do not check this feature.

Default setting is "**Gateway mode**". Keep all other parameters as default.

3.6.1.1 LAN Ethernet Ports

Check the "Wired-WAN port acts as LAN".

Note:

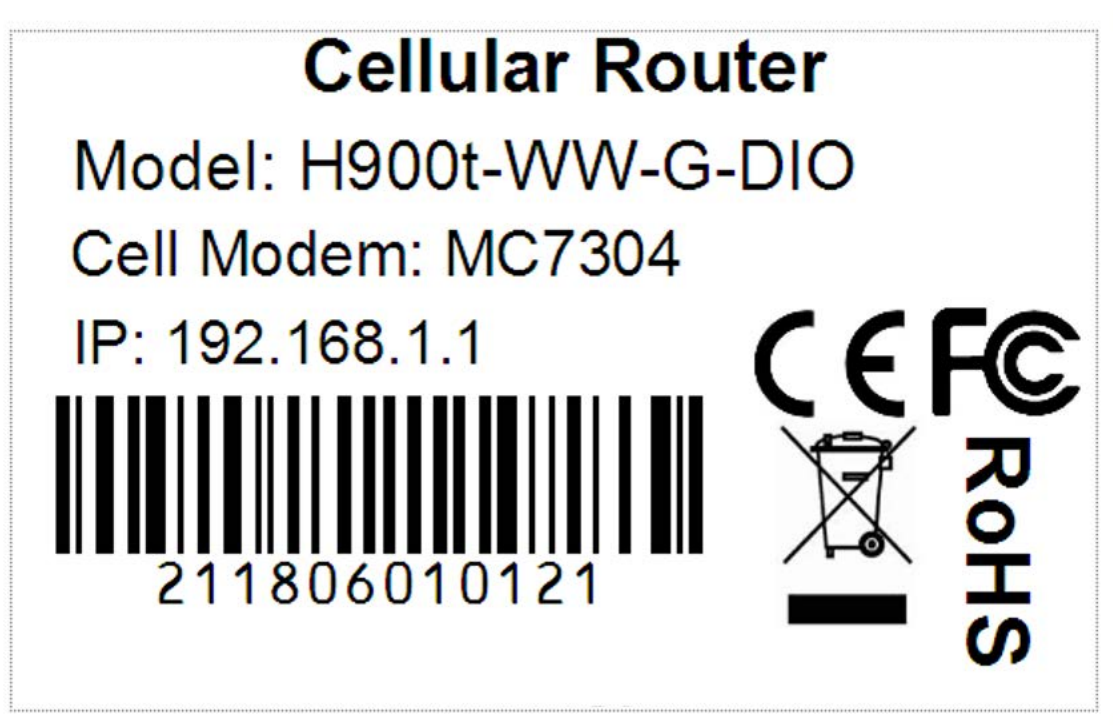
- 1) If checked the **"Wired-WAN port acts as LAN"**, the C365-4G-H900 will not have a WAN RJ45 port.
- 2) Please do not use any features for WAN RJ45 if the **"Wired-WAN port acts as LAN"** is checked.

3.6.2 Mobile Configuration

Systems support different cell modems. By default, the router is set to the correct Cell Modem name before shipment. If you replace it with another Cell Modem and it is not supported, the router will automatically detect the Cell Modem.

Note: The Cell Modem Type was marked on the back of the router.

For example, it shows the following picture. H900 is the router series name, H900t-WW-G-DIO is the part number name. And the MC7304 Cell Modem is the Cell Modem name.



Configure the parameters for SIM1 and SIM2.

General

SIM Switch

Mobile Configuration

SIM 1

SIM 2

Enable

☒

Mobile connection

DHCP mode

▼

PIN code

Dialing number

*99#

APN

3gnet

Authentication method

None

▼

Dual APN support

☐

Network Type

automatic

▼

MTU

1500

Save & Apply

Save

Reset

SIM 1

SIM 2

Mobile Configuration

Enable

☒

Mobile connection

DHCP mode

▼

PIN code

Dialing number

*99#

APN

3gnet

Authentication method

None

▼

Dual APN support

☐

Lock to network

All

▼

Network Type

automatic

▼

MTU

1500

Save & Apply

Save

Reset

Item	Description	
Enable	Check it	
Mobile connection	DHCP mode or PPP mode. Normally system will be automatically selected.	
PIN code	If the SIM card uses a PIN code, please put it here. The wrong PIN code will prevent the router from working. If the SIM card doesn't use a PIN code, please keep it blank.	
Dialing number	Fill in the right parameters. Get this parameter from the Sim Card Provider or Carrier. With experience, most of the time, 2G/3G/4G uses *99#, and CDMA/EVDO use #777.	
APN	Fill in the right parameters. Get this parameter from the Sim Card Provider or Carrier;	
Authentication method	Fill in the right parameters. Get this parameter from the Sim Card Provider or Carrier;	
	None	No more settings.
	CHAP	Username and Password required.
	PAP	Username and Password required.
Dual APN support	<p>Most of the SIM cards or Carriers/Operators use just one APN, but some use two APNs. Check this feature to before use.</p> <p>Second APN: configure it referring to APN; Second Authentication method: configure it referring to Authentication method;</p>	
Lock to network	Normally keep default settings.	
Network Type	Select the network you want to use or use default settings.	
Demand	Use default settings.	
MTU	Use default settings.	
Item	Description.	
Enable	Check it.	
Mobile connection	DHCP mode or PPP mode. The system will automatically select.	
PIN code	If the SIM card uses a PIN code, please put it here. The wrong PIN code will prevent the router from working. If the SIM card doesn't use the PIN code, please keep blank.	
Dialing number	Fill in the right parameters. Get this parameter from the Sim Card Provider or Carrier. With experience, most of the time, 2G/3G/4G uses *99#, and CDMA/EVDO use #777.	
APN	Fill in the right parameters. Get this parameter from the Sim Card Provider or Carrier;	
Authentication method	Fill in the right parameters. Get this parameter from the Sim Card Provider or Carrier;	
	None	No more settings
	CHAP	Username and Password required.
	PAP	Username and Password required.
Dual APN support	<p>Most of the SIM cards or Carriers/Operators use just one APN, but some use two APNs. Check this feature to use.</p> <p>Second APN: configure it referring to APN; Second Authentication method: configure it referring to Authentication method</p>	
Lock to network	Normally keep default settings. For some models, there is no this option.	
Network Type	Select the network you want to use. Normally keep default settings	
Demand	Use default settings.	
MTU	Use default settings.	

Click the Save button for the next step;

Click the SIM Switch to configure the SIM working mode.

General

SIM Switch

Mobile Configuration

SIM 1

SIM 2

Cell Switch Configuration

Master SIM

SIM 1

Enable SIM switch ☒

Switch Rules

On Time

☐

On ICMP check

☐

On signal strength

☐

On dial fail

☐

On data limit

☐

Switch to master

☐

Save & Apply

Save

Reset

Item	Description	
Master SIM	Choose the SIM1 or SIM2 for the master SIM, the other SIM will automatically be a backup SIM.	
Enable SIM switch	Check this to enable the SIM switch feature. If unchecked, the router works with a single SIM.	
Switch Rules	On Time	Check this, the two SIMs switch with trigger at a scheduled time.
	On ICMP check	Check this, the two SIMs switch with trigger of cell alive. The data traffic goes via the Master SIM, once the Master SIM has failed, switch to the backup SIM. Once the backup SIM has failed, the data traffic switches to the Master SIM.
	On Signal strength	Set the signal ASU value from 1 to 30. For example, set the value as 10, the data traffic will switch from the Master SIM to the backup SIM if the master SIM signal value is less than 10.
	On dial fail	Master SIM and backup SIM switch with trigger, dialling a number of retries. For example, set the value as 5, the data traffic will switch from Master SIM to backup SIM if master SIM dial failure reaches 5.
	On data limit	Master SIM and backup SIM switch with trigger of SIM data limit.
	Switch to master	For example, check this feature and set the value as 3 minutes. With some issues, the data traffic goes via the backup SIM. The router will check the master SIMs working status. If the master SIM is working, the data traffic will switch to the master SIM after 3 minutes.
Notes: some trigger rules can be selected and used at the same time to meet different applications.		

- **Enable:** Enable mobile network;
- **Mobile connection:** Select a suitable mode for the mobile to connect, if the cell modem only supports 3G, the default mode is pppd mode, otherwise the default value is DHCP mode;
- **APN:** Fill in the related parameters. Get this parameter from the Sim Card Provider or Carrier;
- **PIN number:** If necessary, fill in the related parameters. If the SIM card has no PIN code, and then keep it as blank;
- **Dialing number:** Fill in the related parameters. Get this parameter from the SIM Card Provider or Carrier;
- **Authentication method:** Three options (None, PAP, CHAP). Please confirm your carrier, provide the types of authentication. Normally select None. If it is not working then try to use PAP or CHAP;
- **Username:** Fill in the related parameters. Get this parameter from the SIM Card Provider or Carrier. Notes: If your SIM card has no username, please input out default value, otherwise the router may not dialup. Note: if the authentication method is None, this parameter will not be displayed.
- **Password:** Fill in the related parameters. Get this parameter from the Sim Card Provider or Carrier.

Note: If your SIM card has no username, please input out default value, otherwise the router may not dialup.

Note: if the authentication method is None, this parameter will not be displayed.

- **Network Type:** Select the type. Different Cell Modems support different types. The default value is Automatic.
- **MTU:** Maximum Transmission Unit. This is the max size of packet transmitted on the network. The default value is 1500. Please configure it to optimize your own network.
- **Online Mode**
- **Keep Alive:** means always online. The router will keep online whenever there is data for transmission or not.
- **On Demand:** The router will dialup when there is data for transmission.
- **Idle time (minutes):** Fill in the time. For example, enter 5 and the router will be offline after 5 minutes

if there is no data for transmission.

- Scheduled: Router dialup or offline with schedule. One group is supported.

3.6.3 Cell Mobile Data Limitation

Data Limitation Configuration


Enable data limitation ☐


Period Month ▼


Start day 1 ▼

SIM data limit(MB) 0

Enable alarm ☐

Phone number 

Warning percent of Data Used(%) 90 

Used(Bytes) 0  Reset

Terminate 3G/4G connection until restart time ☒

- **Enable data limitation:**
- **Period:** Support periods are Month, Week and Day.
- **Start day:** The beginning day of period.
- **SIM data limit(MB):** The maximum data that can be used during this period. If it exceeds, the router will disable the cell mobile network during this period.
- **Enable alarm:** Enable the data limitation alarm.
- **Phone number:** The phone number that receives the data limitation alarm SMS.
- **Warning percent of data used:** If the used data arrives at this limit, a data limitation alarm SMS will be sent.
- **Used(MB):** The amount of data consumed during this period.
- **Reset:** Press this button to clear all used data.
- **Terminate 3G/4G connection until restart time:** If the max data is exceed, set the cell interface to down.

3.6.4 LAN Settings

Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of the interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

General Setup

Advanced Settings

Physical Settings

Firewall Settings

Status



Uptime: 0h 24m 3s

MAC-Address: 90:22:00:80:03:00

RX: 1.34 MB (13877 Pkts.)

TX: 4.46 MB (12981 Pkts.)

IPv4: 192.168.1.1/24

IPv6: fd35:ff0d:10d1::1/60

Protocol Static address ▼

Really switch protocol?

Switch protocol

IPv4 address 192.168.1.1

IPv4 netmask 255.255.255.0 ▼

IPv4 gateway

IPv4 broadcast

Use custom DNS servers





IPv6 assignment length 60 ▼

IPv6 assignment hint

- **Protocol:** Only static addresses are supported for LAN
- **Use custom DNS servers:** Multiple DNS server supported.
- **IPv6 assignment length:** Assign a part of a given length of every public IPv6-prefix to LAN interface.
- **IPv6 assignment hint:** Assign prefix parts using this hexadecimal subprefix ID for LAN interface.

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Bring up on boot	<input checked="" type="checkbox"/>		
Use builtin IPv6-management	<input checked="" type="checkbox"/>		
Override MAC address	<input type="text" value="90:22:06:80:02:01"/>		
Override MTU	<input type="text" value="1500"/>		
Use gateway metric	<input type="text" value="0"/>		

- **Bring up on boot:** If checked, the LAN interface will be set to up to when the system boots up. If unchecked, the LAN interface will be down. Don't set it to be unchecked if you don't have a specific purpose.
- **Use built-in IPv6-management:** The default is checked. If IPv6 is not needed, it can be set to unchecked.
- **Override MAC address:** Override LAN MAC address.
- **Override MTU:** Maximum Transmission Unit.
- **Use gateway metric:** The LAN subnet's metric gateway.

Common Configuration		General Setup	Advanced Settings	Physical Settings	Firewall Settings
Bridge interfaces	<input checked="" type="checkbox"/>				
Enable STP	<input type="checkbox"/>				
Interface	<input checked="" type="checkbox"/>  Wired-LAN (lan) <input type="checkbox"/>  Wired-WAN (wan, wan6) <input type="checkbox"/>  Mobile-eth <input checked="" type="checkbox"/>  WiFi (lan)				

- **Bridge interfaces:** LAN bridges wired-LAN and Wi-Fi in a same LAN subnet.
- **Enable STP:** Enable the Spanning Tree Protocol on the LAN. The default value is unchecked.

DHCP Server

General Setup **Advanced Settings** IPv6 Settings

Ignore interface ☐

Start

Limit

Leasetime

- **Ignore interface:** If it is unchecked, Disable DHCP on LAN.
- **Start:** Lowest leased address as offset from the network address.
- **Limit:** Maximum number of leased addresses.
- **Lease time:** Expiry time of leased addresses, minimum is 2 minutes(2m). 12H means 12 hours.


DHCP Server

General Setup Advanced Settings IPv6 Settings

Dynamic DHCP ☒

Force ☐

IPv4-Netmask

DHCP-Options 

- **Dynamic DHCP:** Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
- **Force:** Force DHCP on this network even if another server is detected.
- **IPv4-Netmask:** Override the netmask sent to clients. Normally it is calculated from the subnet that is served.
- **DHCP-Options:** Define additional DHCP options, for example '6,192.168.2.1,192.168.2.2' which advertises different DNS servers to clients.

DHCP Server

General Setup Advanced Settings IPv6 Settings

Router Advertisement-Service: server mode

DHCPv6-Service: server mode

NDP-Proxy: disabled

DHCPv6-Mode: stateless + stateful

Always announce default router: ☐

Announced DNS servers:


Announced DNS domains:

- **Router Advertisement-Service:** Four options: disabled, server mode, relay mode and hybrid mode.
- **DHCPv6-Service:** Has the same options with Router Advertisement-Service.
- **NDP-Proxy:** three options: Disabled, relay mode and hybrid mode.
- **Always announce default router:** Announce as the default router even if no public prefix is available.

3.6.5 Wired WAN

Common Configuration

General Setup Advanced Settings Physical Settings Firewall Settings

Status:  **Uptime:** 0h 0m 0s
MAC-Address: 90:22:06:C0:02:01
RX: 0.00 B (0 Pkts.)
TX: 332.81 KB (995 Pkts.)


Protocol: DHCP client

Hostname to send when requesting DHCP: Cell_Router

Protocol: the default protocol is DHCP client. If it should be changed to another protocol, such as PPPoE, select protocol PPPoE, then click button the “Switch protocol”.

Common Configuration

General Setup


Status  **Uptime:** 0h 0m 0s
MAC-Address: 90:22:06:C0:02:01
RX: 0.00 B (0 Pkts.)
TX: 346.66 KB (1036 Pkts.)

Protocol PPPoE

Really switch protocol? ☒ Switch protocol


After, click the “Switch protocol” button, the below screen appears:

General Setup **Advanced Settings** Physical Settings Firewall Settings

Status  pppoe-wan

Protocol PPPoE

PAP/CHAP username

PAP/CHAP password 

Access Concentrator auto

Service Name auto

Note: for different protocols the Advanced Settings are different, please put the mouse over the title to receive help information, the recommend web browser is Google Chrome.

3.6.6 Wi-Fi Settings

The screenshot shows the 'Wireless Overview' section. At the top, it displays 'radio0: Master *Cell_AP_0002b2*'. Below this, the 'Generic MAC80211 802.11bgn (radio0)' is shown with 'Channel: 11 (2.462 GHz)' and 'Bitrate: 43.3 Mbit/s'. A signal strength indicator shows 45%. To the right are buttons for 'Wifi Restart', 'AP Client', and 'Add'. Below this, the 'SSID: Cell_AP_0002b2 | Mode: Master' and 'BSSID: 90:22:06:00:02:B2 | Encryption: None' are listed, with buttons for 'Disable', 'Edit', and 'Remove'. The 'Associated Stations' section features a table with the following data:

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
Cell_AP_0002b2	68:A8:6D:48:77:5E	192.168.1.105	-78 dBm	0 dBm	1.0 Mbit/s, MCS 0, 20MHz	43.3 Mbit/s, MCS 4, 20MHz

- **Wi-Fi Restart:** Turn off Wi-Fi, and then turn it on again.
- **AP Client:** Scan all frequencies to get the Wi-Fi network information.
- **Add:** Add a new Wireless network.
- **Disable:** Set the wireless network to down.
- **Edit:** Modify the detailed information of the wireless network.
- **Remove:** Delete a wireless network.
- **Associated Stations:** This is a list of connected wireless stations.

3.6.6.1. Wi-Fi General Configuration

The screenshot shows the 'Device Configuration' page with the 'Advanced Settings' tab selected. The 'Status' section displays a signal strength indicator at 54% and the following details: 'Mode: Master | SSID: Cell_AP_0002b2', 'BSSID: 90:22:06:00:02:B2 | Encryption: None', 'Channel: 11 (2.462 GHz) | Tx-Power: 20 dBm', 'Signal: -72 dBm | Noise: 0 dBm', 'Bitrate: 43.3 Mbit/s | Country: 00'. Below this, a toggle switch indicates 'Wireless network is enabled' with a 'Disable' button. The 'Operating frequency' section includes dropdowns for 'Mode' (set to 'N'), 'Channel' (set to '11 (2462 MHz)'), and 'Width' (set to '20 MHz'). The 'Transmit Power' dropdown is set to '20 dBm (100 mW)'.

- **Status:** Show the Wi-Fi signal strength, mode, SSID and so on.
- **Operating frequency Mode:** supports 802.11b/g/n/ac. the Legacy means 802.11b/g. "N" means 802.11n. "ac" means 802.11ac.
- **Channel:** Channel 1-11 supported.
- **Width:** 20MHz and 40MHz.
- **Transmit Power:** From 0dBm to 20dBm supported.

3.6.6.2 Wi-Fi Advanced Configuration

Device Configuration

General Setup | **Advanced Settings**

Country Code: 00 - World

Distance Optimization:

Fragmentation Threshold:

RTS/CTS Threshold:

- **Country Code:** Use ISO/IEC 3166 alpha2 country codes.
- **Distance Optimization:** Distance to the farthest network member in meters.
- **Fragmentation Threshold:**
- **RTS/CTS Threshold:**

3.6.6.3 Wi-Fi Interface Configuration

Interface Configuration

General Setup | **Wireless Security** | MAC-Filter

ESSID: Cell_AP_0002b2

Mode: Access Point

Network: ☐ ifmobile: ☐ ☒ lan: ☐ wan6: ☐ create:

Hide Extended Service Set Identifier: ☐

WMM Mode: ☒

- **ESSID:** Extended Service Set Identifier. This is the broadcast name.
- **Mode:** Supported options.

✓ Access Point

Client

Ad-Hoc

802.11s

Pseudo Ad-Hoc (ahdemo)

Monitor

Access Point (WDS)

Client (WDS)

- **Network:** Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.
- **Hide Extended Service Set Identifier:** Hide SSID means this Wi-Fi cannot be scanned by others.
- **WMM Mode:**

Interface Configuration

General Setup | **Wireless Security** | MAC-Filter

Encryption: WPA-PSK

Cipher: auto

Key:

Enable WPS pushbutton, requires WPA(2)-PSK ☒

- Encryption:

No Encryption
WEP Open System
WEP Shared Key
/ WPA-PSK
WPA2-PSK
WPA-PSK/WPA2-PSK Mixed Mode
WPA-EAP
WPA2-EAP

- **Key:** This is the password to join a wireless network. If the Encryption is set to “No Encryption”, no password is required.

Interface Configuration

General Setup | **Wireless Security** | MAC-Filter

MAC-Address Filter: Allow list

MAC-List:

00:1E:10:1F:00:00 (10.223.164	
68:A8:6D:48:77:5E (dentydeME	
90:22:06:80:02:01 (Cell_Router	

- **MAC-Address Filter:** MAC address access policy. Disabled: disable MAC-address filter functionality. Allow list: only the MAC address in the list is allowed to proceed. Deny list: all packets are allowed to proceed except the MAC address on the list.
- **MAC-List:** click button the button to delete the MAC address from the list, click the button to add to a new MAC address onto the list.

3.6.6.4 Wi-Fi AP Client

- **Step 1)** click the “AP Client” button on the wireless overview page, then the system will start to scan all Wi-Fi signals.

- **Step 2)** If the Wi-Fi you want to join is on the list, then click the “Join Network” button accordingly. If it is not, click “Repeat Scan” until you find the Wi-Fi that you want to join.

- **Step 3)** Join Network Settings
 Replace wireless configuration: An additional wireless network will be created if it is unchecked. Otherwise it will replace the old configuration.
WPA passphrase: Specify the secret encryption key here.
Name of the new network: The default value is wwan. If it conflicts with other interfaces, please change it. Otherwise don't change it.
- **Step 4)** Click Submit if everything is configured. The below is the Wi-Fi configuration page. Don't change the operating frequency, make sure the ESSID and BSSID is from the Wi-Fi you want to join.

Device Configuration

General Setup

Advanced Settings

Status



Mode: Client | **SSID:** MERCURY_FE2A
BSSID: 8C:F2:28:FD:FE:2A | **Encryption:** -
Channel: 11 (2.462 GHz) | **Tx-Power:** 0 dBm
Signal: 0 dBm | **Noise:** 0 dBm
Bitrate: 0.0 Mbit/s | **Country:** 00

Wireless network is enabled

Disable

Operating frequency

Mode

N

Channel

3 (2422 MHz)

Width

20 MHz

Transmit Power

20 dBm (100 mW)

Interface Configuration

General Setup

Wireless Security

ESSID

MERCURY_FE2A

Mode

Client

BSSID

8C:F2:28:FD:FE:2A

Network



ifmobile:



lan:



wan:



wan6:



wwan:



create:

- Step 5) Click the “Save & Apply” button to start the AP client.

Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 3 (2.422 GHz) | Bitrate: 150 Mbit/s

68% SSID: Cell_AP_0002b2 | Mode: Master
BSSID: 90:22:06:00:02:B3 | Encryption: None

65% SSID: MERCURY_FE2A | Mode: Client
BSSID: 8C:F2:28:FD:FE:2A | Encryption: WPA2 PSK (CCMP)

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
Cell_AP_0002b2	68:A8:6D:48:77:5E	?	-62 dBm	0 dBm	1.0 Mbit/s, MCS 0, 20MHz	58.5 Mbit/s, MCS 6, 20MHz
MERCURY_FE2A	8C:F2:28:FD:FE:2A	192.168.1.1	-50 dBm	0 dBm	135.0 Mbit/s, MCS 7, 40MHz	150.0 Mbit/s, MCS 7, 40MHz

3.6.7 Interfaces Overview

Interfaces overview shows all interfaces status, including uptime, MAC-address, RX, TX and IP address.

Interfaces

Interface Overview

Network	Status	Actions
LAN br-lan	Uptime: 0h 50m 35s MAC-Address: 90:22:06:80:02:01 RX: 945.69 KB (9759 Pkts.) TX: 2.35 MB (6976 Pkts.) IPv4: 192.168.10.1/24 IPv6: fd90:5065:78e::1/60	Connect Stop Edit
IFMOBILE eth1	MAC-Address: 00:00:00:00:00:00 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Stop Edit
WAN eth0.2	Uptime: 0h 0m 0s MAC-Address: 90:22:06:C0:02:01 RX: 0.00 B (0 Pkts.) TX: 480.27 KB (1433 Pkts.)	Connect Stop Edit
WAN6 eth0.2	Uptime: 0h 0m 0s MAC-Address: 90:22:06:C0:02:01 RX: 0.00 B (0 Pkts.) TX: 480.27 KB (1433 Pkts.)	Connect Stop Edit
WWAN Client "MERCURY_FE2A"	Uptime: 0h 5m 46s MAC-Address: 90:22:06:00:02:B2 RX: 243.14 KB (980 Pkts.) TX: 236.01 KB (1861 Pkts.) IPv4: 192.168.1.105/24	Connect Stop Edit

3.6.8 Firewall

3.6.8.1 General Settings

3.6.8.2 Port Forwards

This page includes the port forwards list and the add new port forwards rule functionality.

General Settings Port Forwards Traffic Rules DMZ Security

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable	Sort
This section contains no values yet				

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
New port forward	TCP+UDP	cpe		lan		

Add

Save & Apply Save Reset

- **Name:** Port forward instance name.
- **Protocol:** TCP+UDP, UDP and TCP can be chosen.
- **External zone:** The recommended option is wan.
- **External port:** Match incoming traffic directed at the given destination port on this host.
- **Internal zone:** The recommended zone is lan.
- **Internal IP address:** Redirect matched incoming traffic to the specific host.
- **Internal port:** Redirect matched incoming traffic to the given port on the internal host.

3.6.8.3 Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

The traffic rules overview page content provides the following functionalities.

Traffic rules list:

Traffic Rules				
Name	Match	Action	Enable	Sort
Allow-DHCP-Renew	IPv4-UDP From any host in wan To any router IP at port 58 on this device	Accept input	<input checked="" type="checkbox"/>	
Allow-Ping	IPv4-ICMP with type echo-request From any host in wan To any host in any zone	Accept forward	<input checked="" type="checkbox"/>	
Allow-IGMP	IPv4-IGMP From any host in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	
Allow-DHCPv6	IPv6-UDP From IP range fe80::/10 in wan with source port 547 To IP range fe80::/10 at port 546 on this device	Accept input	<input checked="" type="checkbox"/>	
Allow-MLD	IPv6-ICMP with types 130/0, 131/0, 132/0, 143/0 From IP range fe80::/10 in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	
Allow-ICMPv6-Input	IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-advertisement From any host in wan To any router IP on this device	Accept input and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	
Allow-ICMPv6-Forward	IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type From any host in wan To any host in any zone	Accept forward and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	

Open ports on the router and create new forward rules:

Open ports on router:

Name	Protocol	External port
<input type="text" value="New input rule"/>	TCP+UDP	<input type="text"/>

Add

New forward rule:

Name	Source zone	Destination zone
<input type="text" value="New forward rule"/>	lan	wan

Add and edit...

Source the NAT list and create the source NAT rule:

Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort
This section contains no values yet				

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port
<input type="text" value="New SNAT rule"/>	lan	wan	-- Please cho	Do not rewrite

Add and edit...

Traffic rule configuration page: This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Firewall - Traffic Rules - forwardtest

This page allows you to change advanced properties of the traffic rule entry, such as matched sou

Rule is enabled ☒ Disable

Name forwardtest

Restrict to address family IPv4 and IPv6

Protocol TCP+UDP

Match ICMP type any

Source zone ☐ Any zone

☒ lan: lan: 

☐ openvpn: (empty)

☐ vpnzone: (empty)

☐ wan: wan:  wan6:  ifmobile:  wwan: 

Source MAC address any

Source address any

Source port any





Destination zone ☐ Device (input)

☐ Any zone (forward)

☐ lan: lan: 

☐ openvpn: (empty)

☐ vpnzone: (empty)

☒ wan: wan:  wan6:  ifmobile:  wwan: 

Destination address	<input type="text" value="any"/>
Destination port	<input type="text" value="any"/>
Action	<input type="text" value="accept"/>
Extra arguments	<input type="text"/>

- **Name:** Traffic rule entry name
- **Restrict to address family:** IPv4+IPv6, IPv4 and IPv6 can be selected. Specify the matched IP address family.
- **Protocol:** Specify the protocol matched in this rule. "Any" means any protocol is matched.
- **Source zone:** This is the zone that the traffic comes from.
- **Source MAC address:** Traffic rule checks if the incoming packet's source MAC address is matched.
- **Source address:** Traffic rule checks if the incoming packet's source IP address is matched.
- **Source port:** Traffic rule checks if the incoming packet's TCP/UDP port is matched.
- **Destination zone:** The zone that the traffic will go to.
- **Destination address:** Traffic rule checks if the incoming packet's destination IP address is matched.
- **Destination port:** Traffic rule checks if the incoming packet's TCP/UDP port is matched.
- **Action:** If traffic is matched, the system will handle traffic according to the Action (accept, drop, reject, don't track).
- **Extra argument:** Passes additional arguments to iptable, use with care!

3.6.8.4 DMZ

General Settings	Port Forwards	Traffic Rules	DMZ	Security
----------------------------------	-------------------------------	-------------------------------	---------------------	--------------------------

DMZ Configuration

You may setup a Demilitarized Zone(DMZ) to separate internal network and Internet.

Enable DMZ ☐

IP address

Protocol

In computer networking, DMZ is a firewall configuration for securing local area networks (LANs).

- **IP Address:** Please Enter the IP address of the computer which you want to set as DMZ host
- **Protocol:** All protocols, TCP+UDP, TCP, UDP.

Note: When DMZ host is settled, the computer is completely exposed to the external network; the firewall will not influence this host.

3.6.8.5 Security

System Security Configuration

SSH access from WAN

Allow

Ping from WAN to LAN

Allow

Enable telnet

☐

HTTPS Access

HTTPS port

443

HTTPS access from WAN

Allow

Remote network

Any IP address

HTTP Access

HTTP port

80

HTTP access from WAN

Allow

Remote network

Any IP address

RFC1918 filter

☐

- **SSH access from WAN:** Allow or deny users access to the router from remote side.
- **Ping from WAN to LAN:** Allow or deny ping from remote side to internal LAN subnet.
- **Enable telnet:** Enable telnet connect. The default setting is disabled for security.
- **HTTPS port:** Set HTTPS port, the default port is 443.
- **HTTPS access from WAN:** Allow or deny access router web management page from remote side.
- **Remote network:** Any IP Address, Single IP address, Subnet.
- **IP address:** Fill a remote IP address that can access the router web management page.
- **Netmask:** 24 means net mask 255.255.255.0, 32 means 255.255.255.255, the legal value is from 1 to 32.
- **HTTP port:** Set HTTP port, the default port is 80.
- **HTTP access from WAN:** Allow or deny access router web management page from remote side.
- **Remote network:** Any IP Address, Single IP address, Subnet.
- **IP address:** Fill a remote IP address that can access router web management page.
- **Netmask:** 24 means net mask 255.255.255.0, 32 means 255.255.255.255, the legal value is from 1 to 32.
- **RFC1918 filter:** Reject requests from RFC1918 IPs to public server IPs

3.6.9 Static Routes

Routes
Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU	Table
lan	192.168.8.0	255.255.255.0	192.168.1.107	0	1500	128

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU	Table
This section contains no values yet					

Buttons: Add, Delete, Save & Apply, Save, Reset

- **Interface:** You can choose the corresponding interface type.
- **Target:** The destination host IP or network.
- **IPv4-Netmask:** The destination IP mask.
- **IPv4-Gateway:** IP address of the next hop.
- **Metric:** Used by router to make routing decisions.
- **MTU:** Maximum transmission unit
- **Table:** The route table ID, the default value is 254, valid table ID 1-254.

Notice:

- Gateway and LAN IP of this router must belong to the same network segment.
- If the destination IP address is the one of a host, and then the Netmask must be 255.255.255.255.
- If the destination IP address is IP network segment, it must match with the Netmask. For example, if the destination IP is 10.0.0.0, and the Netmask is 255.0.0.0.

3.6.10 Switch

VLANs on "switch0" (rt305x-esw)

VLAN ID	Port 0	Port 1	Port 2	Port 3	Port 4	Port 5	CPU
1	untagged	untagged	untagged	untagged	off	off	tagged
2	off	off	off	off	untagged	off	tagged

 Add

Note:

1. Port 4 is a Wired-WAN port, port 0, port 1, port 2, port 3 are LAN port.
2. “**Untagged**” means the Ethernet frame transmits from this port without VLAN tag.
3. “**Tagged**” means the Ethernet frame transmits from this port is with VLAN tag.
4. “**Off**” means this port does not belong to VLAN. For default setting, port 0 belongs to VLAN1, but not belong to VLAN 2.

3.6.11 DHCP and DNS

DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

General Settings

Resolv and Hosts Files

TFTP Settings

Advanced Settings

Domain required

☒

Authoritative

☒


Local server

Local domain

Log queries

☐

DNS forwardings




Rebind protection

☒

Allow localhost

☒

Domain whitelist

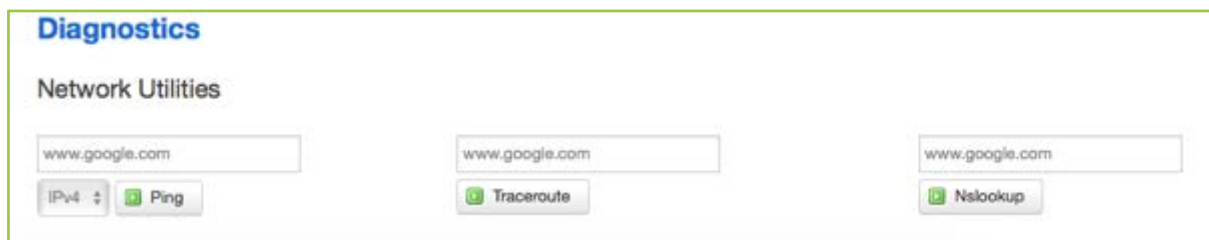


- **Domain required:** Don't forward DNS-requests without DNS-Name.
- **Authoritative:** This is the only DHCP on the local network.
- **Local server:** Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only.
- **Local domain:** Local domain suffix appended to DHCP names and hosts file entries.
- **Log queries:** Write received DNS requests to syslog.
- **DNS forwarding:** List of DNS servers to forward requests to.
- **Rebind protection:** Discard upstream RFC1918 responses.
- **Allow localhost:** Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services.
- **Domain whitelist:** List of domains to allow RFC1918 responses for.

General Settings	Resolv and Hosts Files	TFTP Settings	Advanced Settings
Suppress logging	<input type="checkbox"/>		
Allocate IP sequentially	<input type="checkbox"/>		
Filter private	<input checked="" type="checkbox"/>		
Filter useless	<input type="checkbox"/>		
Localise queries	<input checked="" type="checkbox"/>		
Expand hosts	<input checked="" type="checkbox"/>		
No negative cache	<input type="checkbox"/>		
Strict order	<input type="checkbox"/>		
Bogus NX Domain Override	<input type="text" value="67.215.65.132"/>		
DNS server port	<input type="text" value="53"/>		
DNS query port	<input type="text" value="any"/>		
Max. DHCP leases	<input type="text" value="unlimited"/>		
Max. EDNS0 packet size	<input type="text" value="1280"/>		
Max. concurrent queries	<input type="text" value="150"/>		

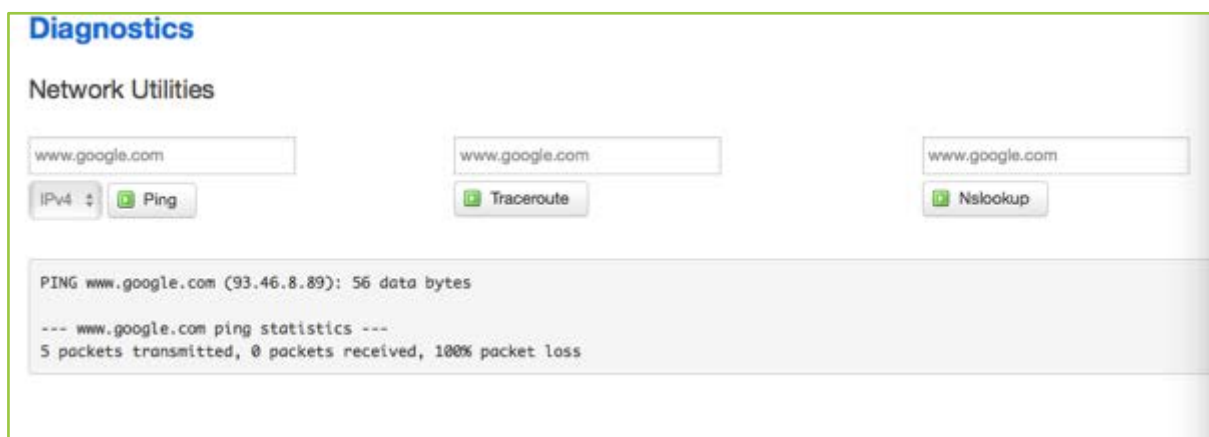
- **Suppress logging:** Suppress logging of the routine operation of these protocols.
- **Allocate IP sequentially:** Allocate IP addresses sequentially, starting from the lowest available address.
- **Filter private:** Do not forward reverse lookups for local networks.
- **Filter useless:** Do not forward requests that cannot be answered by public name servers.
- **Localize queries:** Localize hostname depending on the requesting subnet if multiple IPs are available.
- **Expand hosts:** Add local domain suffix to names served from hosts files.
- **No negative cache:** Do not cache negative replies, e.g. for not existing domains.
- **Strict order:** DNS servers will be queried in the order of the resolve file.
- **Bogus NX Domain Override:** List of hosts that supply bogus NX domain results.
- **DNS server port:** Listening port for inbound DNS queries
- **DNS query port:** Fixed source port for outbound DNS queries
- **Max DHCP leases:** Maximum allowed number of active DHCP leases
- **Max edns0 packet size:** Maximum allowed size of EDNS.0 UDP packets.
- **Max concurrent queries:** Maximum allowed number of concurrent DNS queries.

3.6.12 Diagnostics



The screenshot shows the 'Diagnostics' section of a network utility interface. Under the 'Network Utilities' heading, there are three identical input fields, each containing the text 'www.google.com'. Below each input field is a button: the first has a dropdown menu set to 'IPv4' and a 'Ping' button; the second has a 'Traceroute' button; and the third has an 'Nslookup' button.

- **Ping**: This is a tool that is used to test the reachability of a host on an Internet Protocol (IP) network.
- **Traceroute**: it is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.
- **Nslookup**: This is a network administration command-line tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.
- For example if you want to ping `www.google.com`, type the target domain name or IP address, then click the “**Ping**” button. Wait a couple of seconds, then the result will be shown below.



This screenshot shows the same interface as the previous one, but with the results of a ping command displayed in a text area below the buttons. The text reads: 'PING www.google.com (93.46.8.89): 56 data bytes', followed by a separator line '--- www.google.com ping statistics ---', and finally '5 packets transmitted, 0 packets received, 100% packet loss'.

3.6.13 Loopback Interface

Loopback Interface Configuration

IP address	<input type="text" value="172.16.99.99"/>
Netmask	<input type="text" value="255.255.255.255"/>
IP address 2	<input type="text"/>
Netmask 2	<input type="text"/>

The default Loopback interface has the IP address 127.0.0.1, the user can change it here. The first IP address can be used in IPsec. The secondary can be used as management.


3.6.14 Dynamic Routing

Dynamic Routing is implemented by quagga-0.99.22.4. Dynamic Routing services can be enabled here:

Dynamic Routing

Zebra

Enable ☐

Password 

OSPF

Enable ☐

Password 

OSPF6

Enable ☐

Password 

RIP

Enable ☐

Password 

RIPng

Enable ☐

Password 

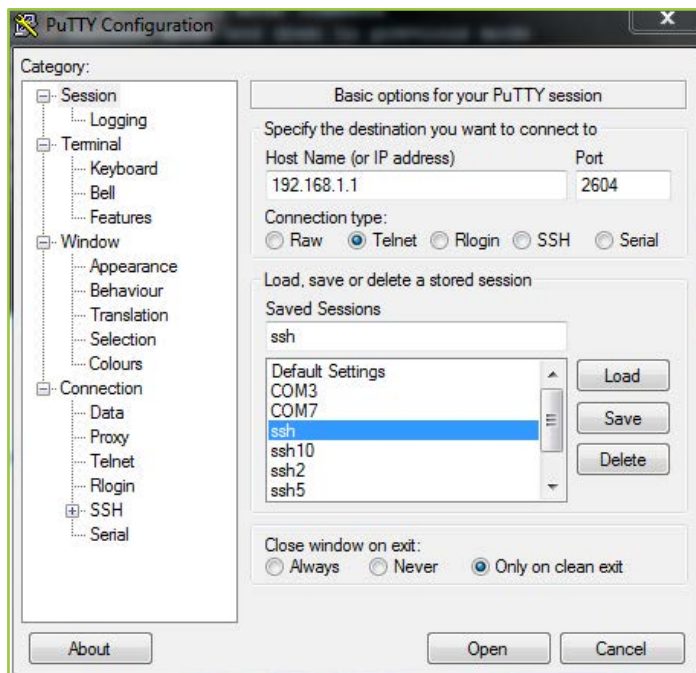
BGP

Enable ☐

Password 

- **Zebra:** Zebra is an IP routing manager. Telnet port number is 2601.
- **OSPF:** Open Shortest Path First. Telnet port number is 2604.
- **OSPF6:** Open Shortest Path First for IPv6. Telnet port number is 2606.
- **RIP:** Routing Information Protocol. Telnet port number is 2602.
- **RIPng:** This is an IPv6 reincarnation of the RIP protocol. Telnet port number is 2603.
- **BGP:** Border Gateway Protocol. Telnet port number is 2605.

Note: How to configure these services? For example, the router's LAN IP is 192.168.10.1. If we want to configure OSPF, we need to set OSPF to **"Enable"** firstly, then open putty in windows:



Input the password of OSPF. Then press the "?" for help.

```

Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
Cell_Router>
Cell_Router>
  echo      Echo a message back to the vty
  enable    Turn on privileged mode command
  exit      Exit current mode and down to previous mode
  help      Description of the interactive help system
  list      Print command list
  quit      Exit current mode and down to previous mode
  show      Show running system information
  terminal   Set terminal line parameters
  who       Display who is on vty
Cell_Router>

```

3.6.15 QoS

QoS (Quality of Service) can prioritize network traffic selected by addresses, ports or services.

Quality of Service

With QoS you can prioritize network traffic selected by addresses, ports or services.

Interfaces

WAN

Delete

Enable ☒

Classification group

default

Calculate overhead

☐

Half-duplex

☐

Download speed (kbit/s)

1024

Upload speed (kbit/s)

128

Add

- **Enable:** Enable QoS on this interface.
- **Classification group:** Specify class group used for this interface.
- **Calculate overhead:** Decrease upload and download ratio to prevent link saturation.
- **Download speed:** Download limit in kilobits/second.
- **Upload speed:** Upload limit in kilobits/second.

Target	Source host	Destination host	Service	Protocol	Ports	Number of bytes	Comment	Sort
priority	all	all	all	all	22,53		ssh, dns	
normal	all	all	all	TCP	20,21,25,80,110,443,993,995		ftp, smtp, http(s), imap	
express	all	all	all	all	5190		AOL, iChat, ICQ	
normal	all	all	all	all	all			

Add

Each classification section defines one group of packets and which target (i.e. bucket) this group belongs to. All the packets share the bucket specified.

- **Target:** The four defaults are: priority, express, normal, low.
- **Source host:** Packets matching this source host(s) (single IP or in CIDR notation) belong to the bucket defined in the target.
- **Destination host:** Packets matching this destination host(s) (single IP or in CIDR notation) belong to the bucket defined in the target.
- **Protocol:** Packets matching this protocol belong to the bucket defined in the target.
- **Ports:** Packets matching this, belong to the bucket defined in the target. If more than 1 port is required, they must be separated by a comma.
- **Number of bytes:** Packets matching this, belong to the bucket defined in target.

3.6.16 Guest LAN (Guest Wi-Fi)

Guest Wi-Fi is a specific Wi-Fi that can only access internet bots not the local LAN.

Guest LAN(Guest Wi-Fi) Configuration

Enable ☐

LAN IP address

LAN mask

Wi-Fi ssid

Wi-Fi device name

- **Enable:** Enable Guest Wi-Fi.
- **LAN IP address:** This LAN IP address must be different than the LAN interface IP address.
- **LAN mask:** Packets matching this destination host(s) (single IP or in CIDR notation) belong to the bucket defined in the target.
- **Wi-Fi ssid:** The ssid of the guest Wi-Fi.
- **Wi-Fi device name:** Choose one Wi-Fi device to carry the Guest Wi-Fi, the available device name is radio0 and radio1. Check the Wi-Fi overview page for the device name. for example:

Wi-Fi Overview



Qualcomm Atheros QCA9880 802.11bgnac (radio0)
Channel: 149 (5.745 GHz) | Bitrate: ? Mbit/s



Wifi Restart



AP Client



Add



0%

SSID: SPEEDROUTE H820Q 5GHz | Mode: Master
BSSID: 04:F0:21:1A:D8:35 | Encryption: WPA2 PSK (CCMP)



Disable



Edit



Remove



Generic MAC80211 802.11bgn (radio1)
Channel: 5 (? GHz) | Bitrate: ? Mbit/s



Wifi Restart



AP Client



Add



0%

SSID: Cell_AP_007622 | Mode: Client
BSSID: 90:22:06:00:76:22 | Encryption: -



Disable



Edit



Remove