

# Industrial Cellular VPN Router NR300 User Manual



**REVISION HISTORY**

Revision	Date	Firmware version	Revision Details
0	Oct 2019	1.0.0(337913f)	Initial release.
1	Dec 2019		Change home page layout of UM
2	Oct 2020	1.1.2(d9fbbdd)	<ol style="list-style-type: none"> <li>1. Change the Overview webpage to show the latest firmware</li> <li>2. Add OpenVPN Server</li> <li>3. Allow to import or download OpenVPN client file</li> <li>4. Add System Security: Local Telnet/Local HTTP/Local HTTPS/Local SSH/Ping request/DDoS Defense</li> <li>5. Add time synchronization from modem</li> <li>6. Add dd "NAT Enable" option on each uplink</li> <li>7. Add SMS Control</li> <li>8. Serial settings: Add the parity "Mark" and "Space"; Add "Sync to Secondary Address" option</li> <li>9. Add "MAC Binding IP" on LAN</li> <li>10. Change the layout of DDNS</li> <li>11. GRE VPN: Add "Enable Default Route", "Binding Interface" options</li> <li>12. Add the "Sniffer" for debugging</li> </ol>
3	July 2023	1.1.4(fb20324)	1. Add some VPNs and protocol converter software.
4	May 2024	1.1.4(fb20324)	Update Order Information

## Trademarks and copyright

Guangzhou Navigatworx Technologies Co, Ltd and  &  logo are the trademarks or registered trademarks in China mainland, HongKong and other countries worldwide. All other trademarks mentioned in this document are the property of their respective owners. ©2019 Navigatworx Technologies. All Rights Reserved.

## Disclaimers

Information in this document is subject to change without notice and does not represent a commitment on the part of Navigatworx Technologies.

Navigatworx Technologies provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Navigatworx Technologies may make improvements and/or changes in this manual, or in the product(s) and/or the program(s) described in this manual at any time.

Information provided in this manual is intended to be accurate and reliable. However, Navigatworx Technologies assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

## Technical Support

**E-mail:** support@navigatworx.com  
info@navigatworx.com

**Web:** www.navigatworx.com

## Interference Issues

Avoid possible radio frequency (RF) interference by following these guidelines:

- The use of cellular telephones or devices in aircraft is illegal. Use in aircraft may endanger operation and disrupt the cellular network. Failure to observe this restriction may result in suspension or denial of cellular services to the offender, legal action, or both.
- Do not operate in the vicinity of gasoline or diesel fuel pumps unless use has been approved or authorized.
- Do not operate in locations where medical equipment that the device could interfere with may be in use.
- Do not operate in fuel depots, chemical plants, or blasting areas unless use has been approved and authorized.
- Use care if operating in the vicinity of protected personal medical devices, i.e., hearing aids and pacemakers.
- Operation in the presence of other electronic equipment may cause interference if equipment is incorrectly protected. Follow recommendations for installation from equipment manufacturers.

## Declaration of Conformity

NR300 Series products are in conformity with the essential requirements and other relevant provisions of the CE and RoHS.



## Table of Contents

Chapter 1. Product Overview .....	6
1.1 Overview .....	6
1.2 Features and Benefits .....	6
1.3 General Specifications .....	7
1.4 Mechanical Specifications .....	9
1.5 Package Checklist .....	9
1.6 Order Information .....	11
Chapter 2. Installation .....	12
2.1 Product Overview .....	12
2.2 LED Indicators .....	13
2.3 Ethernet Port Indicator .....	14
2.4 PIN Definition of Terminal block .....	14
2.5 Reset Button .....	15
2.6 Insert SIM card .....	15
2.7 Install Antenna .....	16
2.8 DIN-rail Mounting .....	16
2.9 Power Supply Installation .....	17
2.10 Power On The Router .....	17
Chapter 3. Access to Web page .....	18
3.1 PC Configuration .....	18
3.2 Factory Default Settings .....	19
3.3 Login to Web Page .....	20
Chapter 4. Web Configuration .....	21
4.1 Web Interface .....	21
4.2 Overview .....	23
4.2.1 Status .....	23
4.2.2 Syslog .....	25
4.3 Link Management .....	26
4.3.1 Connection Manager .....	26
4.3.2 Cellular .....	29
4.3.3 Ethernet .....	32
4.4 Industrial Interface .....	37
4.4.1 Serial .....	37
4.5 Network .....	41
4.5.1 Firewall .....	41
4.5.2 Route .....	44
4.5.3 IP Passthrough .....	45
4.6 Applications .....	46
4.6.1 DDNS .....	46
4.6.2 SMS .....	47
4.6.3 Schedule Reboot .....	48
4.7 VPN .....	49

4.7.1 OpenVPN .....	49
4.7.2 GRE .....	54
4.8 Maintenance .....	56
4.8.1 Upgrade .....	56
4.8.2 Software .....	56
4.8.3 System .....	57
4.8.4 Configuration .....	62
4.8.5 Debug Tools .....	62
Appendix A -Glossary .....	65
Appendix B -Q&A .....	66
No Signal .....	66
Cannot detect SIM card .....	66
Poor Signal .....	66
IPSec VPN established, but LAN to LAN cannot communicate .....	67
Forget Router Password .....	67
Appendix D - CLI .....	68

# Chapter 1. Product Overview

## 1.1 Overview

Navigateworx NR300 series industrial cellular VPN router offers a single, flexible platform to address a variety of wireless communications needs with over-the-air configuration and system monitoring for optimal connectivity. This router enables wireless data connectivity over public and private LTE cellular networks at 4G speeds.

NR300 series router has dual SIM backup, 1 LAN ports. RS232 and RS485 interfaces are provided to support Serial to IP communication.

NR300 series router supports 9 to 36 VDC wide range power inputs, designed with reverse-voltage protection mechanism for greater reliability. It is an advanced choice for universal wireless M2M applications with reliable features for data transmission.

## 1.2 Features and Benefits

### **Industrial internet access**

- Wireless Mobile Broadband 2G / 3G / 4G Connection
- Remote access to SCADA System for Industrial Automation
- Reduce high costs for on-site maintenance

### **Designed for industrial usage**

- Power Input Range 9 to 36 VDC
- Industrial designed for harsh environment
- Aluminum casing

### **Secure and reliable remote connection**

- Connection manager ensure seamless communication
- Support Multiple VPN tunnels for data encryption
- Firewall prevents unsafe and unauthorized access

### **Easy to use and easy maintenance**

- User-friendly web interface for human interaction
- Easy configuration for deployment
- Support Web Management Platform

## 1.3 General Specifications

### Cellular Interface

- Standards: FDD-LTE, WCDMA/UMTS/HSPA/HSPA+/EDGE/GPRS,
- 2× SMA female antenna connector
- 2 x SIM (3.0V & 1.8V)

### Ethernet Interface

- Standard: IEEE 802.3, IEEE 802.3u
- Number of Ports:  
1 LAN x 10/100 Mbps, RJ45 connector
- 1.5KV magnetic isolation protection

### Serial Interface

- 1×RS232 (3 PIN): TX, RX, GND
- 1 x RS485 (2 PIN): Data+(A), Data-(B)
- Baud rate: 300 bps to 115200 bps
- Connector: terminal block
- 15KV ESD protection

### Other Interfaces

- 1× RST button
- LED instruction: 1 x SYS, 1 x NET, 1 x USR, 3 x RSSI

### Software

- Network protocols: TCP, UDP, IPv4, ICMP, NTP, DNS, HTTP, HTTPS, ARP, PPP, DHCP, IP Passthrough
- VPN: IPSec, GRE, OpenVPN, DMVPN, L2TP, PPTP, Wireguard, Zerotier
- Protocol Converter: Modbus Master, Modbus Slave, Modbus ID Mapping, Modbus Gateway, IEC101-104, Modbus to DNP3, DNP3 to IEC104, Modbus to SparkplugB, Modbus to LwM2M, Modbus to IEC104, DLMS Master, DLMS to IEC104, FTP Transfer
- Policy: RIPv1/RIPv2/OSPF/BGP dynamic route (optional)
- Firewall & Filter: Port forwarding, DMZ, anti-DoS, ACL
- Serial port: TCP server and client, UDP

- Management: Web, Devices Management Platform, CLI

### **Power Supply and Consumption**

- Connector: 7-pin 3.5 mm female socket
- Input voltage range: 9~36VDC
- Power consumption:

Idle: 50 mA@12V

Data link: 200 mA (peak) @12V

### **Physical Specification**

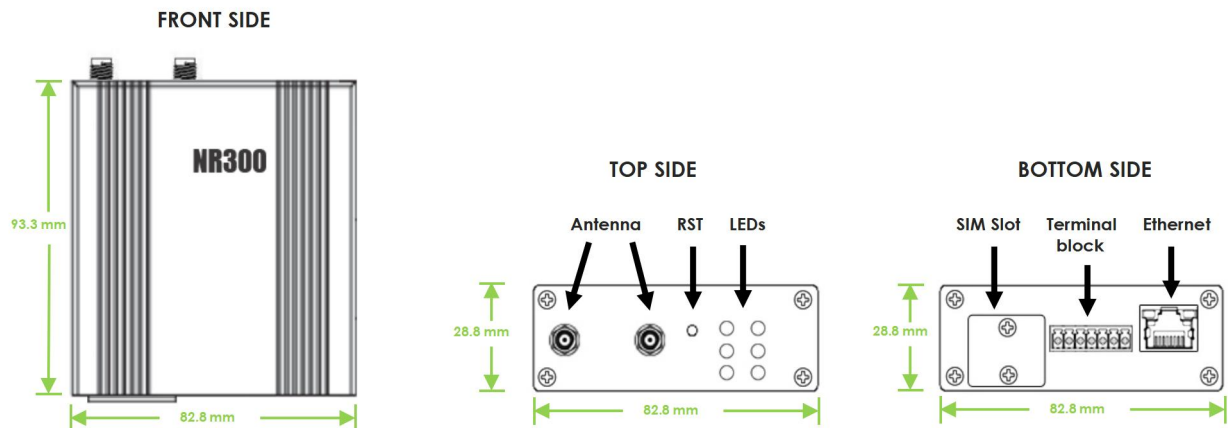
- Ingress Protection: IP30
- Housing & Weight: Aluminum, 200g
- Dimension: 82.8mm x 93.3mm x 28.8mm (excluding antenna)
- Installations: Din-rail mounting

### **Environmental**

- Operation temperature: -40~+75°C
- Store temperature: -40~+85°C
- Operation humidity: 5% to 95% non-condensing

## 1.4 Mechanical Specifications

**Dimension: 82.8mm x 93.3mm x 28.8mm**



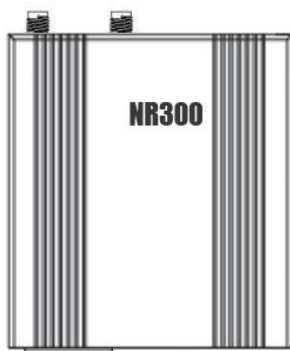
## 1.5 Package Checklist

NR300 series Router includes the parts shown in below, please verify your components.

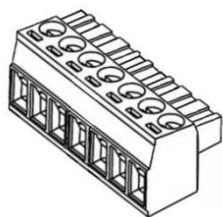
**NOTE:** if any of the below items is missing or damaged, please contact your sales representative.

### Included equipment

- 1 x Navigatworx NR300 series Industrial Cellular VPN router



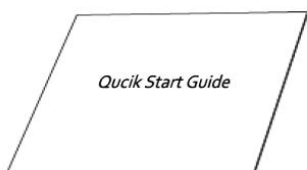
- 1 x 7-pin 3.5 mm male terminal block for Power Input/RS232/RS485



- 1 x Ethernet cable



- 1 x Quick Start Guide



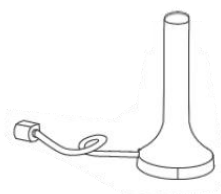
### Optional Accessories (sold separately)

- 3G/4G cellular antenna

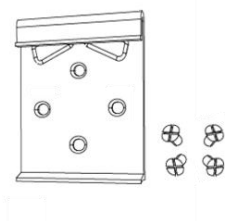
Stubby antenna



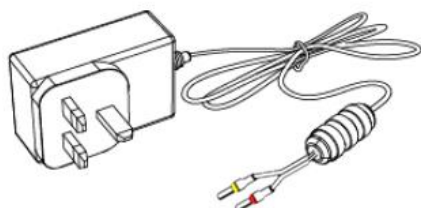
Magnet antenna



- 35mm Din-rail mounting kit



- AC/DC power adapter (12VDC, 1.5A; EU/US/UK/AU plug optional)



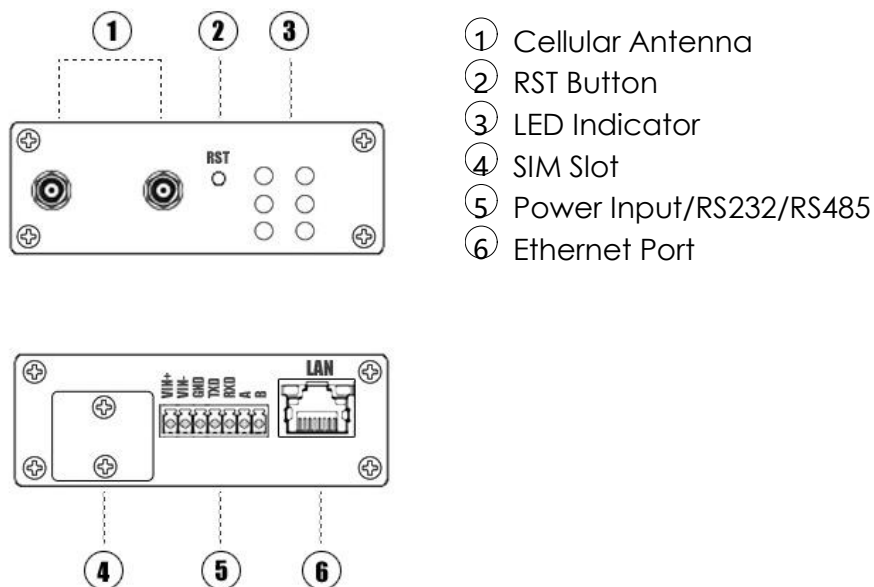
## 1.6 Order Information

MODEL	PN	Wi-Fi	GNSS	Frequency Bands	Description	Country
NR300-4G	B301403	-	-	<b>4G:</b> LTE FDD: B1/B3/B5/B8 LTE TDD: B34/B38/B39/B40/B41 <b>3G:</b> UMTS: B1/B5/B8 <b>2G:</b> GSM: B3/B8	4G LTE, Dual SIMs, 1 x Eth, 1 x RS232 (3 PIN), 1 x RS485, 9 - 36VDC	China
	B301404	-	-	<b>4G:</b> LTE FDD: B1/B3/B7/B8/B20/B28A <b>3G:</b> UMTS: B1/B8 <b>2G:</b> GSM: B3/B8	4G LTE, Dual SIMs, 1 x Eth, 1 x RS232 (3 PIN), 1 x RS485, 9 - 36VDC	EMEA
	B301405	-	-	<b>4G:</b> LTE FDD: B1/B2/B3/B4/B5/B7/B8/B28 LTE TDD: B40 <b>3G:</b> UMTS: B1/B2/B4/B5/B8 <b>2G:</b> GSM: B2/B3/B5/B8	4G LTE, Dual SIMs, 1 x Eth, 1 x RS232 (3 PIN), 1 x RS485, 9 - 36VDC	Latin America, Australia, New Zealand, Taiwan


# Chapter 2. Installation

## 2.1 Product Overview

- Front Panel



## 2.2 LED Indicators

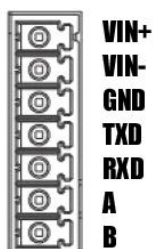
Name	Color	Status	Description
SYS	Green	Slow Blinking (500ms duration)	Operating normally
		Fast Blinking	System initialing
		Off	Power is off
NET	Green	On	Register to Highest priority network service (depend on Radio, e.g. Radio support LTE as Highest priority network).
		Fast Blinking (500ms duration)	Register to Non-Highest priority network service (depend on Radio, e.g. Radio support LTE as Highest priority network, then WCDMA and GPRS is non-highest priority network).
		Off	Register failed
USR: SIM	Green	On	Router is trying cellular connection with SIM1
		Fast Blinking (250ms duration)	Router is trying cellular connection with SIM2
		Off	No SIM detected
		Blinking	Wi-Fi is enabled and data transmission
		Off	Wi-Fi is disable or initialize failed
Signal Strength Indicator 	Green	On, 3 LED light up	Signal strength (21-31) is high
		On, 2 LED light up	Signal strength (11-20) is medium
		On, 1 LED light up	Signal strength (1-10) is low
		Off	No signal

## 2.3 Ethernet Port Indicator

Name	Status	Description
Link indicator	On	Connection is established
	Blinking	Data is being transmitted
	Off	Connection is not established

## 2.4 PIN Definition of Terminal block

- Power Input & Serial Port



PIN	RS232	RS485	Power Input	Direction
1	--	--	VIN+	Positive (Red Line)
2	--	--	VIN-	Negative (Yellow Line)
3	GND	--	--	--
4	TXD	--	--	Router-->Device
5	RXD	--	--	Router<--Device
6	--	A	--	Router<-->Device
7	--	B	--	Router<-->Device

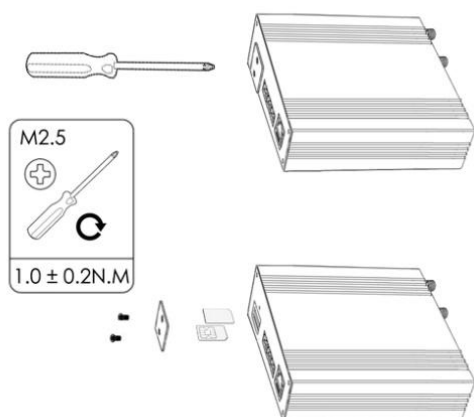
## 2.5 Reset Button

Function	Action
Reboot	Press the RST button within 3s under operation status
Factory Reset	Press the RST button between 3s to 10s, all LEDs blink few times then reboot the router manually.
Run Normally	Press the RST button more than 10s, router will run normally without reboot or factory reset.

## 2.6 Insert SIM card

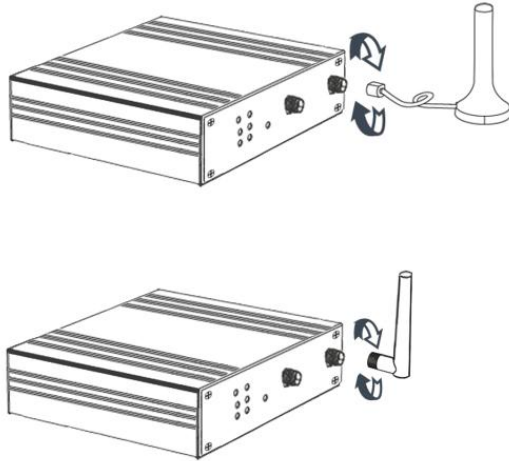
- **Insert / Remove SIM card**

1. Make sure the power is disconnected.
2. Use a Phillips-head screwdriver to remove SIM slot cover.
3. Insert the SIM card(s) in to the SIM sockets.
4. Replace the SIM slot cover.



## 2.7 Install Antenna

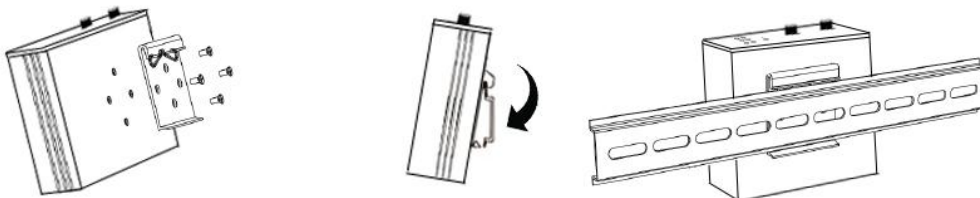
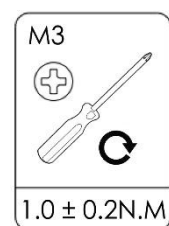
- Connect the cellular antenna to the MAIN and AUX connector on the unit.



**NOTE:** NR300 router supports dual antennas with MAIN and AUX connectors. MAIN connector is for data receiving and transmission. AUX connector is for enhancing signal strength, which cannot be used separately.

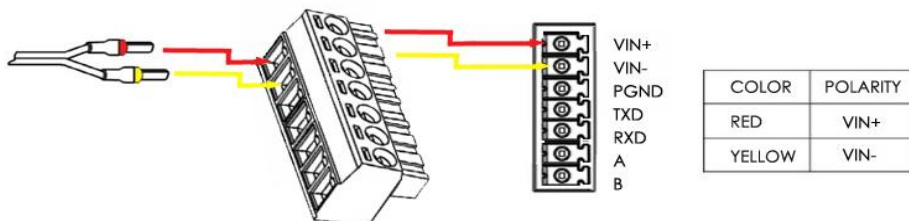
## 2.8 DIN-rail Mounting

1. Use 4 pcs of M3x6 flat head phillips screws to fix the DIN-rail to the router.
2. Insert the upper lip of the DIN-rail into the DIN-rail mounting kit.
3. Press the router towards the DIN-rail until it snaps into place.



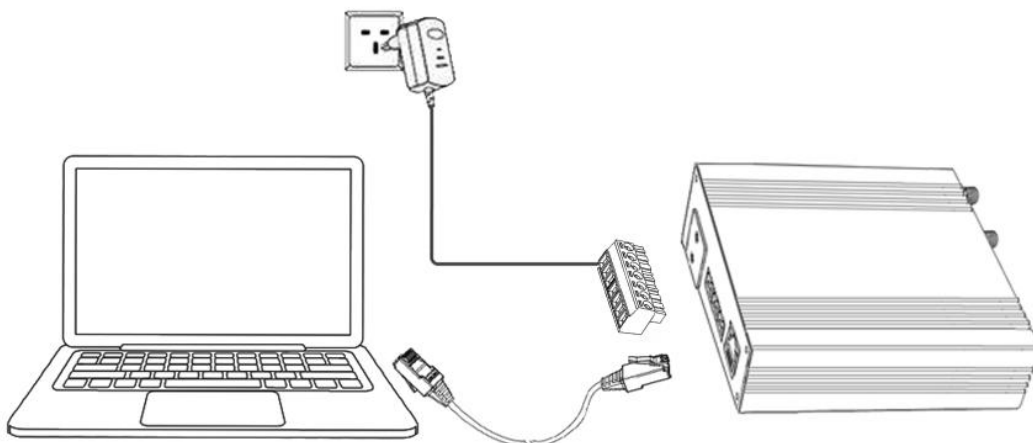
## 2.9 Power Supply Installation

1. Remove the pluggable connector from the unit, then loosen the screws for the locking flanges as needed.
2. Connect the wires of the power supply to the terminals.



## 2.10 Power On The Router

1. Connect one end of the Ethernet cable to the LAN port on the unit and the other end to a LAN port on a PC.
2. Connect the AC power to a power source.
3. Router is ready when SYS LED is blinking.



## Chapter 3. Access to Web page

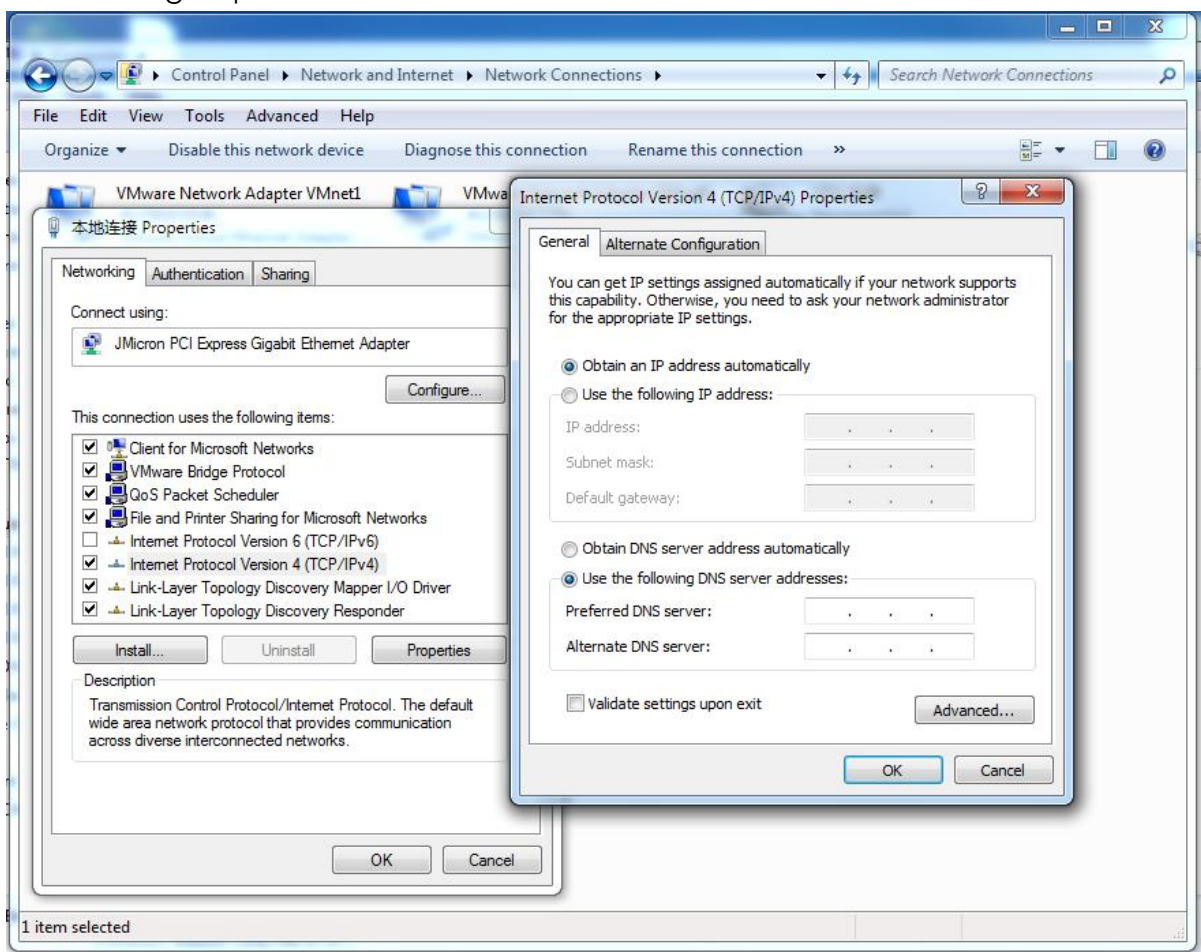
### 3.1 PC Configuration

NR300 router contains a DHCP server which will automatically assign an IP address to your PC, however in some cases the user may need to change the network settings on their PC to accept the IP address from the N300. or you can configure a static IP address manually.

- **Obtain an IP address automatically**

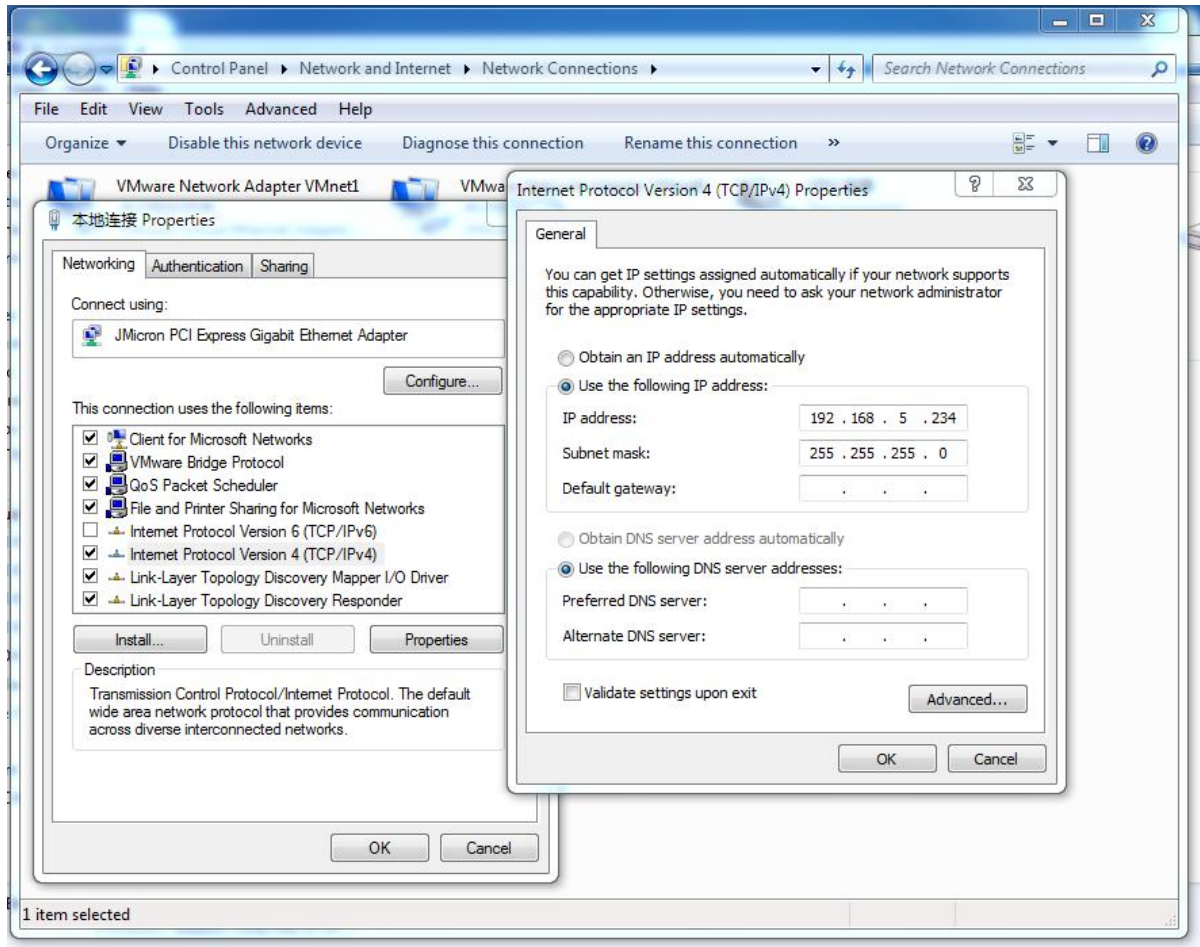
The process required to do this differs depending on the version of Windows you are using.

**NOTE:** The following steps are based on Windows 7.



select **Start » Control Panel » Network Connections**. Right click **Local Area Connection** and select **Properties** to open the configuration dialog box for Local Area Connection. Select **Internet Protocol (TCP/IP)** and click **Properties** to open the TCP/IP configuration window. On the General tab, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Click **OK** to complete TCP/IP configuration.

- **Set to a static IP address**



click "**Use the following IP address**" to assign a static IP manually within the same subnet of the router.

**NOTE:** *Default gateway* and *DNS server* is not necessary if PC not routing all traffic go through NR500 router.

## 3.2 Factory Default Settings

NR300 router supports Web-based configuration interface for management. If this is the first time for you to configure the router, please refer to below default settings.

Username: **admin**

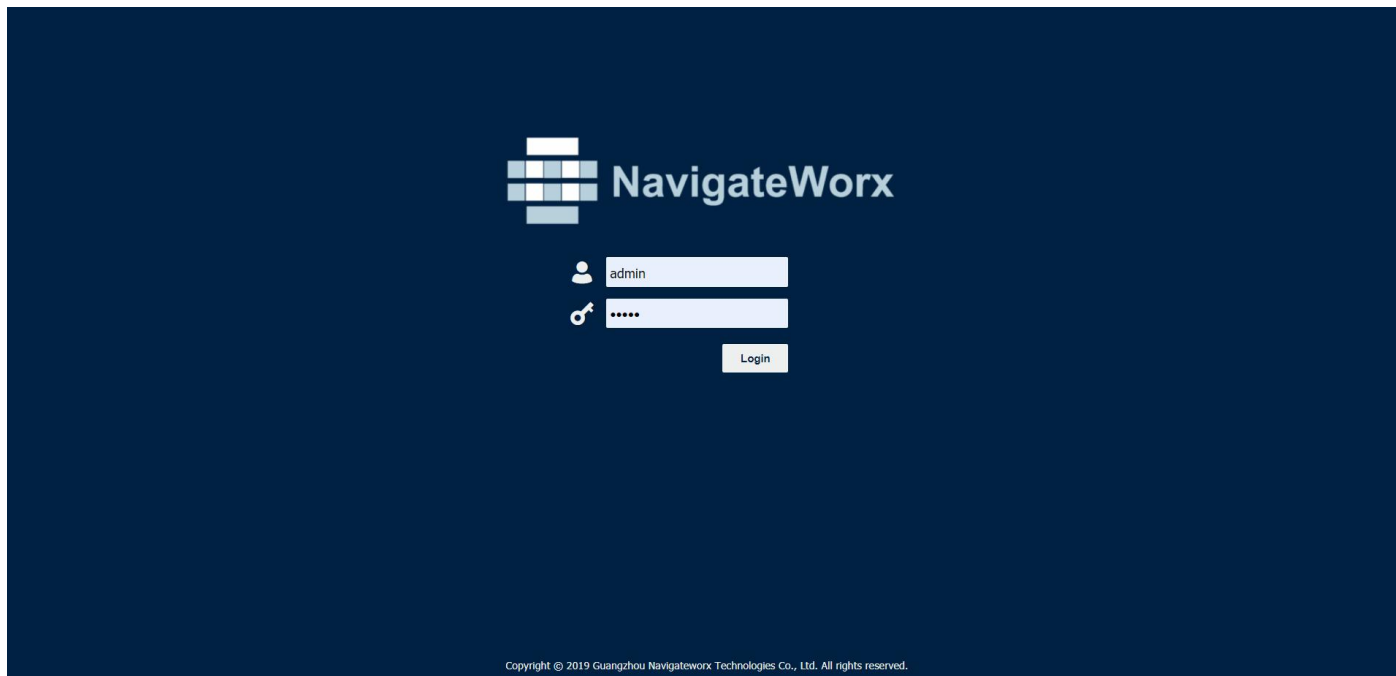
Password: **admin**

LAN IP Address: **192.168.5.1**

DHCP Server: **Enabled**

### 3.3 Login to Web Page

1. Start a Web browser on your PC (Chrome and IE are recommended), enter 192.168.5.1 into the address bar of the web browser.
2. Then use the default username and password(admin/admin), to log in to the router.



# Chapter 4. Web Configuration

## 4.1 Web Interface

The N300 router Web interface is divided into two sections. In the left pane is the main navigation menu. On the right is the content area for each page.

The screenshot displays the NavigateWorx web interface. On the left is a dark blue navigation menu with the following items: Overview, Overview (with a sub-item Syslog), Link Management, Industrial Interface, Network, Applications, VPN, and Maintenance. The main content area is titled 'Status' and contains two sections: 'System Information' and 'Active Link Information'. The 'System Information' section lists: Device Model (NR300-4G), System Uptime (00:06:10), System Time (2020-10-22 13:56:59), RAM Usage (31M Free/16M Shared/64M Total), Firmware Version (1.1.2 (d9fbdd)), Kernel Version (4.4.92), and Serial Number (19015124330001). The 'Active Link Information' section lists: Link Type (WWAN1), IP Address (10.35.221.184), Netmask (255.255.255.240), Gateway (10.35.221.185), Primary DNS Server (120.80.80.80), and Secondary DNS Server (221.5.88.88). At the top right, there is a login status 'Login: admin' and buttons for 'Reboot' and 'Logout'. At the bottom, a copyright notice reads: 'Copyright © 2019 Guangzhou Navigateworx Technologies Co., Ltd. All rights reserved.'

System Information	
Device Model	NR300-4G
System Uptime	00:06:10
System Time	2020-10-22 13:56:59
RAM Usage	31M Free/16M Shared/64M Total
Firmware Version	1.1.2 (d9fbdd)
Kernel Version	4.4.92
Serial Number	19015124330001

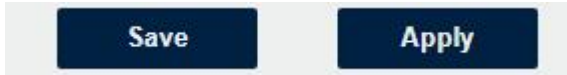
Active Link Information	
Link Type	WWAN1
IP Address	10.35.221.184
Netmask	255.255.255.240
Gateway	10.35.221.185
Primary DNS Server	120.80.80.80
Secondary DNS Server	221.5.88.88

**NOTE:** The navigation menu may contain fewer sections than shown here depending on which options are installed in your unit.

- **Reboot:** reset the router within power disconnect.
- **Logout:** logout to web authorization page.



- **Save:** save the configuration on current page.
- **Apply:** apply the changes on current page immediately.



- **Close:** exit without changing the configuration on current page.



## 4.2 Overview

### 4.2.1 Status

You can view the system information of the router on this page.

Status		
System Information		
Device Model	NR300-4G	
System Uptime	00:06:10	
System Time	2020-10-22 13:56:59	
RAM Usage	31M Free/16M Shared/64M Total	
Firmware Version	1.1.2 (d9fbdd)	
Kernel Version	4.4.92	
Serial Number	19015124330001	

#### System Information

- **Device Module**  
Displays the model name of router
- **System Uptime**  
Displays the duration the system has been up in hours, minutes and seconds.
- **System Time**  
Displays the current date and time.
- **RAM Usage**  
Displays the RAM capacity and the available RAM memory.
- **Firmware Version**  
Displays the current firmware version of router.
- **Kernel Version**  
Displays the current kernel version of router.
- **Serial Number**  
Display the serial number of router.

Active Link Information		
Link Type	WWAN1	
IP Address	10.146.236.12	
Netmask	255.255.255.248	
Gateway	10.146.236.13	
Primary DNS Server	120.80.80.80	
Secondary DNS Server	221.5.88.88	

Active Link Information

- **Link Type**  
Current interface for internet access.
- **IP Address**  
Displays the IP address assigned to this interface.
- **Netmask**  
Displays the subnet mask of this interface.
- **Gateway**  
Displays the gateway of this interface. This is used for routing packets to remote networks.
- **Primary DNS Server**  
Displays the primary DNS server of this interface.
- **Secondary DNS Server**  
Displays the secondary DNS server of this interface.

## 4.2.2 Syslog

**Syslog**

**Syslog Information**

```

Aug 17 20:18:24 navigateworx user.err modem[4039]: error in modem c, modem_get_at_cmd_response.r12
Aug 17 20:18:24 navigateworx user.debug connection_manager[6588]: connection_manager proc_disconnected
Aug 17 20:18:24 navigateworx user.debug connection_manager[6588]: cancel timer by disconnected action
Aug 17 20:18:24 navigateworx user.debug connection_manager[6588]: connection of wwan1 is disconnected
Aug 17 20:18:24 navigateworx user.debug connection_manager[6588]: optimal connection wwan health state 0 cs 2, current connection wwan1
health state 16 cs 0
Aug 17 20:18:24 navigateworx user.warn connection_manager[6588]: wwan1 is unusable
Aug 17 20:19:52 navigateworx authpriv.info webserver: pam_unix(login:session): session opened for user admin by (uid=0)
Aug 17 20:19:52 navigateworx authpriv.info webserver: pam_unix(login:session): session closed for user admin
Aug 17 20:20:07 navigateworx authpriv.info webserver: pam_unix(login:session): session opened for user admin by (uid=0)
Aug 17 20:20:07 navigateworx authpriv.info webserver: pam_unix(login:session): session closed for user admin
Aug 17 20:20:12 navigateworx authpriv.info webserver: pam_unix(login:session): session opened for user admin by (uid=0)
Aug 17 20:20:12 navigateworx authpriv.info webserver: pam_unix(login:session): session closed for user admin
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 available DHCP range: 192.168.5.2 -- 192.168.5.200
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 vendor class: MSFT 5.0
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 client provides name: Chen
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 DHCPREQUEST(lan0) 192.168.5.2 f0:76:1c:5a:4e:cc
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 tags: lan0
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 DHCPACK(lan0) 192.168.5.2 f0:76:1c:5a:4e:cc Chen
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 requested options: 1:netmask, 3:router, 6:dns-server, 15:domain-name,
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 requested options: 31:router-discovery, 33:static-route, 43:vendor-
encap,
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 requested options: 44:netbios-ns, 46:netbios-nodetype, 47:netbios-
scope,
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 requested options: 119:domain-search, 121:classless-static-route,
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 requested options: 249, 252
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 next server: 192.168.5.1
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 1 option: 53 message-type 5
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 54 server-identifier 192.168.5.1
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 51 lease-time 2h
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 58 T1 54m43s
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 59 T2 1h39m43s
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 1 netmask 255.255.255.0
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 28 broadcast 192.168.5.255
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 7 option: 81 PQDN 03:ff:ff:43:68:65:6e
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 6 dns-server 192.168.5.1
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 3 router 192.168.5.1
Aug 17 21:09:57 navigateworx daemon.err udhcpd[6639]: sending renew
Aug 17 21:09:57 navigateworx daemon.err udhcpd[6639]: lease of 192.168.111.33 obtained, lease time 7200
Aug 17 21:09:57 navigateworx user.debug udhcpd: dhcpd update configuration of wan
Aug 17 21:09:57 navigateworx user.debug connection_manager[6588]: connection_manager proc_connected

```

Download Diagnosis

Download Syslog

Clear

Refresh

### Syslog Information

- **Download Diagnosis**  
Download the Diagnosis file for analysis.
- **Download Syslog**  
Download the complete syslog since last reboot.
- **Clear**  
Clear the current page syslog printing.
- **Refresh**  
Reload the current page with latest syslog printing.

## 4.3 Link Management



This section shows you the setup of link management.


### 4.3.1 Connection Manager

Status		Connection			
Connection Information					
Index	Type	Status	IP Address	Netmask	Gateway
1	WWAN1	Connected	10.146.236.12	255.255.255.248	10.146.236.13
2	WWAN2	Disconnected			

#### Connection Manager->Status

- **Type**  
Displays the connection interface
- **Status**  
Displays the connection status of this interface.
- **IP Address**  
Displays the IP Address of this interface.
- **Netmask**  
Displays the subnet mask of this interface.
- **Gateway**  
Displays the gateway of this interface. This is used for routing packets to remote networks.

Status	<u>Connection</u>		
General Settings			
Priority	Enable	Connection Type	Description
1	true	WWAN1	
2	true	WWAN2	

Click  to add a new priority interface.

Click  to edit current interface settings.

Click  to delete current interface.

Connection Manager->Connection

- **Priority**  
Displays the priority list of default routing selection.
- **Enable**  
Displays the connection enable status.
- **Connection Type**  
Displays the name of this interface.
- **Description**  
Displays the description of this connection.

Connection Settings

General Settings

Priority

1

Enable

☒

Connection Type

WWAN1

?

Description

NAT Enable

☒

ICMP Detection Settings

Enable

☒

Primary Server

8.8.8.8

Secondary Server

114.114.114.114

Interval

300

?

Retry Interval

5

?

Timeout

3

?

Retry Times

3

?

Save

Close

Connection Settings

- **Priority**  
Displays current index on priority list.
- **Connection Type**  
Select the available interface as outbound link.  
**NOTE:** specify SIM1 carrier link as WWAN1, SIM2 carrier link as WWAN2.

- **NAT Enable**  
Check this box to enable NAT (Network Address Translation) on the current link.
- **ICMP Detection Settings->Enable**  
Check this box to detect link connection status based on pings to a specified IP address.
- **Primary Server**  
Enter the primary IP address that pings will be sent to, to detect the link state. Recommend entering the IP address of known external reachable server or network (e.g. 8.8.8.8).
- **Secondary Server**  
Enter the secondary IP address that pings will be sent to, when the primary server is ping failed, router would try to ping the secondary server.
- **Interval**  
The duration of each ICMP detection in seconds.
- **Retry Interval**  
The interval in seconds between each ping if no packets have been received.
- **Timeout**  
Enter timeout for received ping reply to determine the ICMP detection failure.
- **Retry Times**  
Specify the retry times for ICMP detection.

## 4.3.2 Cellular

NR300 Router main function is connecting to Internet by cellular modem.

Status

Cellular

Cellular Information

Index	Modem	Registration	CSQ	Operator	Netwok Type	IMEI	IMSI	TX Bytes	RX Bytes
1	EC25	Registered	31 (-51dBm)	CHN-UNICOM	LTE	861107038049871	460015956236598	2992	2748
				Index	1				
				Modem	EC25				
				Registration	Registered				
				CSQ	31 (-51dBm)				
				Operator	CHN-UNICOM				
				Netwok Type	LTE				
				IMEI	861107038049871				
				PLMN ID	46001				
				Local Area Code	2508				
				Cell ID	6016C02				
				IMSI	460015956236598				
				TX Bytes	2992				
				RX Bytes	2748				
				Modem Firmware	EC25EFAR06A01M4G				

Copyright © 2018 Guangzhou Navigatexorx Technologies Co., Ltd. All rights reserved.

Copyright © 2018 Guangzhou Navigatowx Technologies Co., Ltd. All rights reserved.

### Cellular->Status

- **Modem**  
Displays the module of the modem used by this WWAN interface.
- **Registration**  
Displays the registration status of SIM card.
- **CSQ**  
Displays the signal strength of the carrier network.
- **Operator**  
Displays the wireless network provider.
- **Network Type**  
Displays the RF technology currently active. Example: LTE, UMTS, or CDMA.
- **IMEI**  
International Mobile Electronic Identifier. Depending on the carrier and technology used, this may be required for the carrier when activating the data contract. In some cases this will be blank.

- **PLMN ID**

Displays the current PLMN ID, including MCC, MNC, LAC and Cell ID.

- **Local Area Code**

Displays the location area code of the SIM card.

- **Cell ID**

Displays the Cell ID of the SIM card location.

- **IMSI**

International Mobile Subscriber Identity, as read from the SIM. This is the user's network subscription.

- **TX Bytes**

Displays the total bytes transmitted since the time the unit was connected. NR300 router would record this data with same SIM card, reboot would not erase this data.

- **RX Bytes**

Displays the total bytes received since the time the unit was connected. NR300 router would record this data with same SIM card, reboot would not erase this data.

- **Modem Firmware**

Displays firmware version of the module used by the WWAN interface.

Status	<u>Cellular</u>	
Modem General Settings		
Index	SIM Card	Auto APN
1	SIM1	true
2	SIM2	true

## Cellular

- **SIM Card**

Displays the SIM card support on this unit.

- **Auto APN**

Displays the Enable status of auto APN function.

SIM Card Settings	
<b>Modem General Settings</b>	
Index	1
SIM Card	SIM1
Auto APN	<input checked="" type="checkbox"/>
Dial Number	*99#
Authentication Type	Auto
PIN Code	<input type="text"/> ?
Monthly Data Limitation	0 ?
Monthly Billing Day	1 ?
Data Roaming	<input checked="" type="checkbox"/>
Override Primary DNS	<input type="text"/>
Override Secondary DNS	<input type="text"/>
<b>Modem Network Settings</b>	
Network Type	Auto
Use All Bands	<input checked="" type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

## SIM Card Settings

- **SIM Card**  
Displays the current SIM card settings.
- **Auto APN**  
Check this box enable auto checking the Access Point Name provided by the carrier.
- **Dial Number**  
Enter the dial number of the carrier.
- **Authentication Type**  
Authentication method used by the carrier. Possible selections are Auto, PAP, CHAP.
- **PIN Code**  
Enter a 4-8 characters PIN code to unlock the SIM.
- **Monthly Data Limitation**  
Enter the data total amount for SIM card, SIM card switchover when data reach limitation.
- **Monthly Billing Day**  
Enter the date of renew data amount every month.
- **Data Roaming**  
Enable or disable the data roaming function on the router.
- **Override Primary DNS**  
Enter the primary DNS server will override the automatically obtained DNS.
- **Override Secondary DNS**  
Enter the secondary DNS server will override the automatically obtained DNS.
- **Network Type**  
Select the mode of operation of the cell module (Auto, 4G Firstly, 4G Only, etc.).
- **Use All Bands**  
Check this box to enable all bands selection or choose specified bands.


### 4.3.3 Ethernet

The same instructions apply to settings for all Ethernet interfaces.

Status	Port Assignment	LAN	VLAN	
Ethernet Port Information				
Index	Name	Status		
1	ETH0	Up		
Interface Information				
Index	Name	MAC Address		
1	lan0	A8:3F:A1:E7:00:00		
DHCP Lease Table				
Index	MAC Address	IP Address	Lease Expires	Hostname

#### Ethernet->Status

- **Ethernet Port Information**  
Displays the port physical connected states.
- **Interface Information**  
Displays the name and MAC address of Ethernet interface.
- **DHCP Lease Table**  
Displays the current IP address assigned to DHCP client.

Status	Port Assignment	LAN	VLAN
<b>General Settings</b>			
Index	Port	Interface	
1	Eth0	LAN0	

#### Ethernet->Port Assignment

- **Port**  
Displays the port states and numbers of this unit.
- **Interface**  
Displays the port states of belong subnet.

Port Settings

General Settings

Index

1

Port

Eth0

Interface

LAN0

Save

Close

Ethernet->Port Settings

- Port**  
Indicate the current configure port.
- Interface**  
Select belong subnet for current configure port.

Status	Port Assignment	LAN	VLAN
General Settings			
Index	Interface	IP Address	Netmask
1	LAN0	192.168.5.1	255.255.255.0
Multiple IP Settings			
Index	Interface	IP Address	Netmask

Ethernet->LAN

- Interface**  
Displays current name of LAN subnet.
- IP Address**  
Displays LAN IP address of this subnet.
- Netmask**  
Displays subnet mask for this subnet.

LAN Settings	
<b>General Settings</b>	
Index	1
Interface	LAN0
IP Address	192.168.5.1
Netmask	255.255.255.0
MTU	1500
<b>DHCP Settings</b>	
Enable	<input checked="" type="checkbox"/>
Mode	Server
IP Pool Start	192.168.5.2
IP Pool End	192.168.5.200
Netmask	255.255.255.0
Lease Time	120
Gateway	
Primary DNS	
Secondary DNS	
WINS Server	
<div>Save</div> <div>Close</div>	
<b>DHCP Settings</b>	
Enable	<input checked="" type="checkbox"/>
Mode	Relay
Relay Server	
<div>Save</div> <div>Close</div>	

## Ethernet->LAN

- **Interface**  
Select the configure LAN port of this subnet.
- **IP Address**  
Enter LAN IP address for this interface.
- **Netmask**  
Enter subnet mask for this subnet.
- **MTU**  
Maximum Transmission Unit, maximum packet size allowed to be transmitted. Should be left as default value of 1500 in most cases.
- **Enable**  
Check this box to enable DHCP feature on current LAN port.
- **Mode**

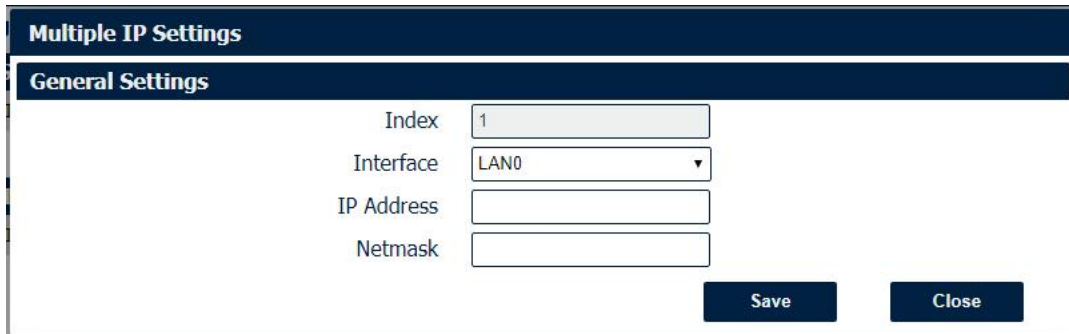
Select the DHCP working mode from "Server" or "Relay".

- **Relay Server**  
Enter the IP address of DHCP relay server.
- **IP Pool Start**  
External LAN devices connected to this unit will be assigned IP address in this range when DHCP is enabled. This is the beginning of the pool of IP addresses.
- **IP Pool End**  
This is the end of the pool of IP addresses.
- **Netmask**  
Subnet mask of the IP address obtained by DHCP clients from DHCP server.
- **Lease Time**  
The lease time of the IP address obtained by DHCP clients from DHCP server.
- **Gateway**  
The gateway address obtained by DHCP clients from DHCP server.
- **Primary DNS**  
Primary DNS server address obtained by DHCP clients from DHCP server.
- **Secondary DNS**  
Secondary DNS server address obtained by DHCP clients from DHCP server.
- **WINS Server**  
Windows Internet Naming Service obtained by DHCP clients from DHCP server.

MAC Binding IP Settings									
MAC Binding IP Settings									
Index	1	Enable	<input checked="" type="checkbox"/>	Description		Host MAC Address		Host IP Address	

### Ethernet->LAN->MAC Binding IP Settings

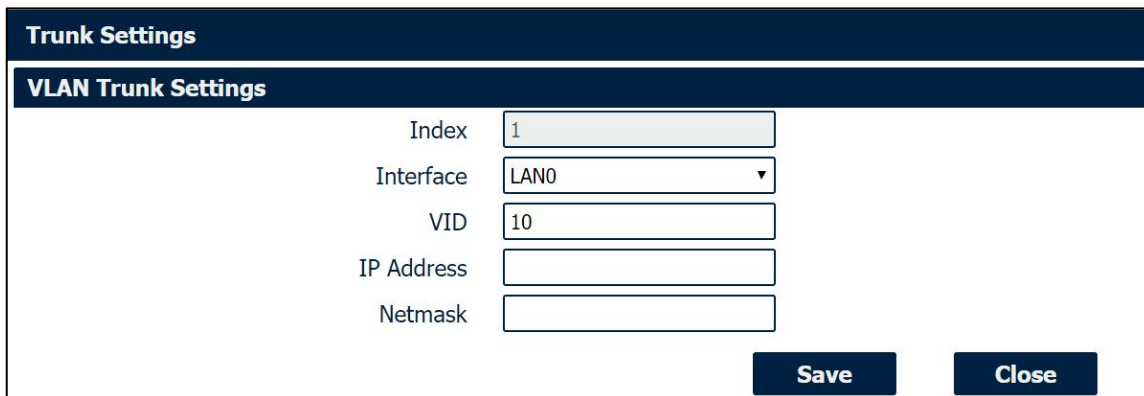
- **Enable**  
Check this box to enable MAC binding IP feature.
- **Description**  
Enter the description for MAC binding IP feature.
- **Host MAC Address**  
Enter the host MAC address.
- **Host IP Address**  
Enter the host IP address.



Multiple IP Settings	
General Settings	
Index	1
Interface	LAN0
IP Address	
Netmask	
<div>Save Close</div>	

### Ethernet->LAN->Multiple IP Settings

- **Interface**  
Select the configurate LAN port of this subnet.
- **IP Address**  
Enter multiple IP address for this interface.
- **Netmask**  
Enter subnet mask for this subnet.



Trunk Settings	
VLAN Trunk Settings	
Index	1
Interface	LAN0
VID	10
IP Address	
Netmask	
<div>Save Close</div>	

### Ethernet->VLAN->VLAN Trunk Settings

- **Interface**  
Select the LAN port for VLAN trunk.
- **VID**  
Specify the VLAN ID for VLAN trunk.
- **IP Address**  
Enter IP address for this VLAN trunk.
- **Netmask**  
Enter subnet mask for this VLAN trunk.

## 4.4 Industrial Interface

The Industrial page contains tabs for making configuration settings for Serial RS232 and RS485. Select Serial from the main navigation menu to navigate to this page.

### 4.4.1 Serial

You could review the status of serial connection.

<u>Status</u>		Connection			
Serial Information					
Index	Enable	Serial Type	Transmission Method	Protocol	Connection Status
1	false	RS485	Transparent	TCP Client	Disconnected
2	false	RS232	Transparent	TCP Client	Disconnected

#### Serial->Status

- **Enable**  
Displays status of current serial function.
- **Serial Type**  
Displays the serial type of COM port.
- **Transmission Method**  
Displays the transmission method of this serial port.
- **Protocol**  
Displays the protocol used by this serial port.
- **Connection Status**  
Displays the connection status of this serial port.

Status		<u>Connection</u>				
Serial Connection Settings						
Index	Enable	Port	Baud Rate	Data Bits	Stop Bits	Parity
1	false	COM1	115200	8	1	None
2	false	COM2	115200	8	1	None

#### Serial->Connection

- **Enable**  
Displays status of current serial function.

- **Port**  
Displays the serial type of COM port.
- **Baud Rate**  
Displays the serial port baud rate.
- **Data Bits**  
Displays the serial port Data Bits.
- **Stop Bits**  
Displays the serial port Stop Bits.
- **Parity**  
Displays the serial port parity.

Connection Settings	
Serial Connection Settings	
Index	1
Enable	<input type="checkbox"/>
Port	COM1
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None
Transmission Settings	
Transmission Method	Transparent
MTU	1024
Protocol	TCP Client
Remote Address	
Remote Port	2000
Sync to Secondary Address	<input checked="" type="checkbox"/>
Remote Secondary Address	
Remote Secondary Port	2000
<div>Save</div> <div>Close</div>	

### Serial->Connection Settings

- **Baud Rate**  
Select the serial port baud rate. Supported values are 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200.
- **Data Bits**  
Select the values from 7 or 8.
- **Stop Bits**  
Select the values from 1 or 2.
- **Parity**  
Select values from none, even, odd, mark, space.
- **Transmission Method**

Select the transmission method for serial port. Optional for "Transparent", "Modbus RTU Gateway" and "Modbus ASCII Gateway".

- **MTU**  
Maximum Transmission Unit, maximum packet size allowed to be transmitted. Should be left as default value of 1024 in most cases.
- **Protocol**  
Select the mode for Serial IP communication. Supported modes are UDP, TCP Server, or TCP Client.
- **Remote IP Address**  
Enter the IP address of the remote server.
- **Remote Port**  
Enter the port number of the remote server.
- **Sync to Secondary Address**  
Check this box to enable the data send to secondary remote server for data backup.
- **Remote Secondary Address**  
Enter the remote backup server IP address.
- **Remote Secondary Port**  
Enter the remote backup server port.

Below window displays different settings when you select **TCP Server** on Protocol.

Transmission Settings	
Transmission Method	Transparent ▼
MTU	1024 ⓘ
Protocol	TCP Server ▼
Local IP Address	
Local Port	2000

### Serial->Connection Settings

- **Local IP Address**  
Enter the IP Address of the local endpoint.
- **Local Port**  
The port number assigned to the serial IP port on which communications will take place.

Below window displays different settings when you select **UDP** on Protocol.

Transmission Settings	
Transmission Method	Transparent ▼
MTU	1024 ⓘ
Protocol	UDP ▼
Local IP Address	
Local Port	2000
Remote IP Address	
Remote Port	2000

### Serial->Connection Settings

- **Local IP Address**  
Enter the IP Address of the local endpoint.
- **Local Port**  
The port number assigned to the serial IP port on which communications will take place.
- **Remote IP Address**  
Enter the IP address of the remote server.
- **Remote Port**  
Enter the port number of the remote server.

## 4.5 Network

### 4.5.1 Firewall

Firewall rules are security rulesets to implement control over users, applications or network objects in an organization. Using the firewall rule, you can create blanket or specialized traffic transit rules based on the requirement.

ACLPort MappingDMZ

General Settings

Default PolicyAccept

ACL rule Settings

Index	Description	Protocol	Source Address	Source Port	Destination Address	Destination Port
-------	-------------	----------	----------------	-------------	---------------------	------------------

#### Firewall->ACL

- Default Policy

Select the “Accept” or “Drop” from the list, the packets which are not included in the access control list will be processed by the default filter policy.

An access control list (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

ACL Settings

General Settings

Index1

Description

ProtocolAll

Source Address

Destination Address

?

?

Save

Close

## Firewall->ACL

- **Description**  
Add a description for this rule.
- **Protocol**  
All: Any protocol number.  
TCP: The TCP protocol.  
UDP: The UDP protocol.  
TCP & DUP: both TCP and UDP protocol  
ICMP: The ICMP protocol.
- **Source Address**  
A specific host IP address can also be specified, or a range of IP addresses via a bitmask (the box following the /).
- **Destination Address**  
A specific IP address can also be specified, or a range of IP addresses via a bitmask (the box following the /).

Port Mapping Settings

Port Mapping rule Settings

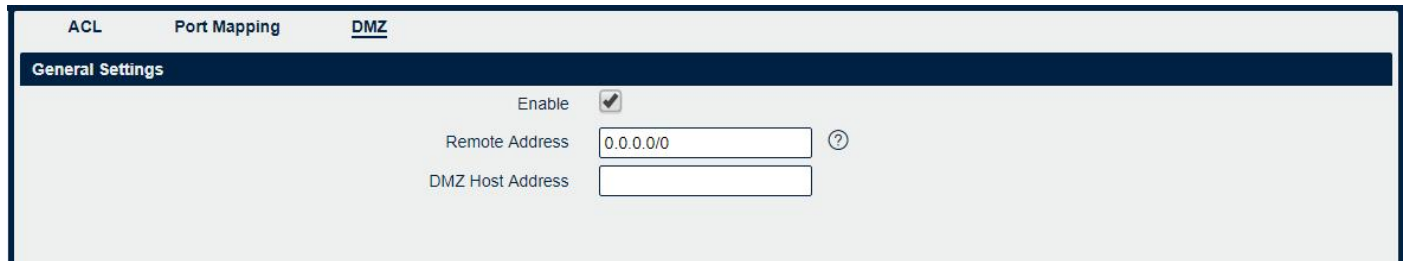
Index	<input type="text" value="1"/>	
Description	<input type="text"/>	
Protocol	<input type="text" value="All"/>	<input style="border: none;" type="button" value="?"/>
Remote Address	<input type="text"/>	<input style="border: none;" type="button" value="?"/>
Remote Port	<input type="text"/>	<input style="border: none;" type="button" value="?"/>
Local Address	<input type="text"/>	<input style="border: none;" type="button" value="?"/>
Local Port	<input type="text"/>	<input style="border: none;" type="button" value="?"/>

## Firewall->Port Mapping

- **Description**  
Add a description for this rule.
- **Protocol**  
All: Any protocol number.  
TCP: The TCP protocol.  
UDP: The UDP protocol.
- **Remote Address**  
Enter a WAN IP address that is allowed to access the unit.
- **Remote Port**  
Enter the external port number range for incoming requests.
- **Local Address**  
Sets the LAN address of a device connected to one of the Fusion's LAN interfaces. Inbound requests will be forwarded to this IP address.

- **Local Port**

Sets the LAN port number range used when forwarding to the destination IP address.



The screenshot shows the 'DMZ' configuration page. At the top, there are tabs for 'ACL', 'Port Mapping', and 'DMZ'. Below the tabs is a 'General Settings' section. It contains an 'Enable' checkbox which is checked. Below that is a 'Remote Address' field with the value '0.0.0.0/0' and a help icon. At the bottom is a 'DMZ Host Address' field which is empty.

## Firewall->DMZ

- **Enable**

Check this box to enable DMZ function.

- **Remote Address**

Optionally restricts DMZ access to only the specified WAN IP address.

**NOTE:** If set to 0.0.0.0/0, the DMZ is open to all incoming WAN IP addresses.

- **DMZ Host Address**

The WAN IP address which has all ports exposed except ports defined in the Port Forwarding configuration.

## 4.5.2 Route

Static Routing refers to a manual method of setting up routing between networks. Select the Static Routing tab to add static routes to the Static Route Table.

Please refer current route table as below.

Status Static Route					
Route Table Information					
Index	Destination	Netmask	Gateway	Metric	Interface
1	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0

### Route->Route Table Information

- **Destination**  
Displays the destination of routing traffic.
- **Netmask**  
Displays the subnet mask of this routing.
- **Gateway**  
Displays the gateway of this interface. This is used for routing packets to remote networks.
- **Metric**  
Displays the metric value of this interface.
- **Interface**  
Displays the outbound interface of this route.

Static Route Settings	
Route Table Information	
Index	<input type="text" value="1"/>
Description	<input type="text"/>
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Gateway	<input type="text"/>
Interface	<input type="text"/> ?
<input type="button" value="Save"/> <input type="button" value="Close"/>	

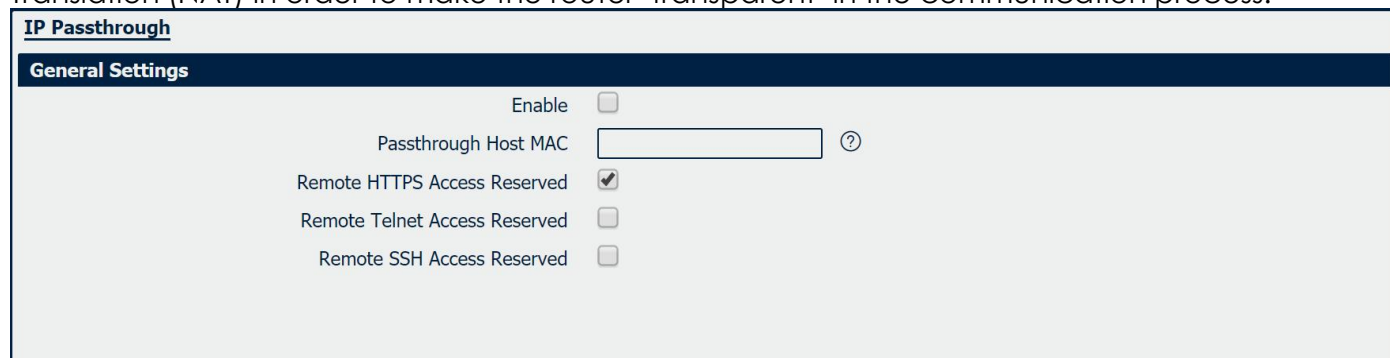
### Route->Static Route Settings

- **Description**  
Enter the description of current static route rule.

- **IP Address**  
Enter the IP address of the destination network.
- **Netmask**  
Enter the subnet mask of the destination network.
- **Gateway**  
Enter the IP address of the local gateway.
- **Interface**  
Please refer to the Network->Route->Status interface.

### 4.5.3 IP Passthrough

IP Passthrough mode, disables NAT and routing and passes the WAN IP address from the WAN interface to the device connected on the local Interface. It is used instead of Network Address Translation (NAT) in order to make the router "transparent" in the communication process.



The screenshot shows the 'IP Passthrough' configuration page. At the top, there is a tab labeled 'IP Passthrough'. Below it is a section titled 'General Settings'. The settings include: 'Enable' with an unchecked checkbox; 'Passthrough Host MAC' with a text input field and a help icon; 'Remote HTTPS Access Reserved' with a checked checkbox; 'Remote Telnet Access Reserved' with an unchecked checkbox; and 'Remote SSH Access Reserved' with an unchecked checkbox.

#### Network->IP Passthrough

- **Enable**  
Check this box will enable IP Passthrough.
- **Passthrough Host MAC**  
Enter the MAC of passthrough host to receive the WAN IP address.
- **Remote HTTPS Access Reserved**  
Check this box to allow to remote access the router via https while enable IP Passthrough mode.
- **Remote Telnet Access Reserved**  
Check this box to allow to remote telnet to the router while enable IP Passthrough mode.
- **Remote SSH Access Reserved**  
Check this box to allow to remote SSH to the router while enable IP Passthrough mode.

## 4.6 Applications

### 4.6.1 DDNS

DDNS is a system that allows the domain name data of a computer with a varying (dynamic) IP addresses held in a name server to be updated in real time in order to make it possible to establish connections to that machine without the need to track the actual IP addresses at all times. A number of providers offer Dynamic DNS services (DDNS), free or for a charge.

You could review the status of DDNS as below.

Status

DDNS

DDNS Status

Index	Status	Hostname	Public IP Address
-------	--------	----------	-------------------

Status

DDNS

General Settings

Check IP Interval300

Log LevelError

DDNS Settings

Index	Enable	Provider	Hostname	Username
-------	--------	----------	----------	----------

DDNS Settings

Index1

Enable☒

Providerno-ip

Hostname

Enable SSL☒

Username

Password

Save

Close

#### DDNS

- Status**  
Display the DDNS status.
- Hostname**  
Display the hostname of DDNS.
- Public IP Address**  
Display the public IP address.
- Check IP Interval**

Enter the interval, the modem will update the Dynamic DNS server of its carrier assigned IP address.

- **Log Level**  
Select the log output level from “none”, “Error”, “Notice”, “Info” and “Debug”.
- **Enable**  
Check this box to enable the DDNS service.
- **Provider**  
Select the DDNS provider from the list, options from “DynDNS”, “no-ip”, “3322” and custom.
- **DDNS Server**  
The internet address to communicate the Dynamic DNS information to. This option is available after you select **custom** on DDNS Provider.
- **DDNS Path**  
DDNS path for custom type.
- **Check IP Server**  
Check IP Server for custom type
- **Check IP Path**  
Check IP Path for custom type.
- **Enable SSL**  
Enable SSL for connection.
- **Username**  
Enter the username used when setting up the account. Used to login to the Dynamic DNS service.
- **Password**  
Enter the password associated with the account.
- **Hostname**  
Enter the hostname associated with the account.

## 4.6.2 SMS

SMS allows user to send the SMS to control the router or get the running status of the router.

SMS		
<b>General Settings</b>		
Enable	<input checked="" type="checkbox"/>	
Enable SMS Control	<input checked="" type="checkbox"/>	
Authentication Type	Password ▼	
<b>Allow Phone Book</b>		
Index	Description	Phone Number
		⊕

Phone Number Settings	
Allow Phone Book	
Index	<input type="text" value="1"/>
Description	<input type="text"/>
Phone Number	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

#### Application->SMS

- **Enable**  
Check this box to enable SMS feature.
- **Authentication Type**  
Specify the authentication mode for SMS, optional for "None" and "Password".
- **Description**  
Enter the description of the Phone Book
- **Phone Number**  
Enter the special phone number and only allow this phone number to send SMS to the router

## 4.6.3 Schedule Reboot

Schedule reboot allows user to define the time for router reboot itself.

Schedule Reboot	
General Settings	
Enable	<input type="checkbox"/>
Time to Reboot	<input type="text" value="00:00"/> ?
Day to Reboot	<input type="text" value="0"/> ?

#### Application->Schedule Reboot

- **Enable**  
Check this box to enable schedule reboot feature.
- **Time to Reboot**  
Enter the time of each day to reboot device. Format: HH(00-23):MM(00-59).
- **Day to Reboot**  
Enter the day of each month to reboot device. 0 means every day.

## 4.7 VPN

### 4.7.1 OpenVPN

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability.

You could review all OpenVPN connection as below.

<u>Status</u>	OpenVPN	X.509 Certificate	Configuration Files			
OpenVPN Information						
Index	Enable	Description	Mode	Status	Uptime	Local Virtual IP
OpenVPN Server Status						
Index	Common Name	Status	Uptime	Remote Virtual IP	Remote IP	Remote Port

#### VPN->OpenVPN->Status>OpenVPN Information

- **Enable**  
Displays current OpenVPN settings is enable or disable.
- **Mode**  
Displays current working mode of OpenVPN.
- **Status**  
Displays the current VPN connection status.
- **Uptime**  
Displays the connection time since VPN is established.
- **Local Virtual IP**  
Displays the virtual IP address obtain from remote side.

#### VPN->OpenVPN->Status>OpenVPN Server Status

- **Common Name**  
Displays the common name of OpenVPN client.
- **Status**  
Displays the current VPN connection status.
- **Uptime**  
Displays the connection time since VPN is established.
- **Remote Virtual IP**  
Displays the virtual IP address of OpenVPN client.
- **Remote IP**  
Displays the remote IP address of OpenVPN client.
- **Remote Port**  
Displays the remote port obtain of OpenVPN client.

OpenVPN Settings

General Settings

Index

1

Enable

☒

Description

Mode

Client

Protocol

UDP

Connection Type

TUN

Server Address

Server Port

1194

Authentication Method

X.509

?

Encryption Type

BF-CBC

Renegotiate Interval

3600

Keepalive Interval

20

Keepalive Timeout

60

Fragment

0

?

Private Key Password

Output Verbosity Level

3

Advanced Settings

Enable NAT

☐

## VPN->OpenVPN

- Enable**  
 Check this box to enable OpenVPN tunnel.
- Description**  
 Enter a description for this OpenVPN tunnel.
- Mode**  
 Select from "P2P", "Client" or "Server".
- Protocol**  
 Select from "UDP", "TCP Client" or "TCP Server"
- Connection Type**  
 Select from "TUN", "TAP" which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.
- Server Address**  
 Enter the IP address or domain of remote server.
- Server Port**

Enter the negotiate port on OpenVPN server.









- **Max Client**  
Allow max OpenVPN client connect to OpenVPN server.
- **Authentication Method**  
Select from "X.509", "Pre-shared", "Password", and "X.509 And Password".
- **Encryption Type**  
Select from "BF-CBC", "DES-CBC", "DES-EDE-CBC", "DES-EDE3-CBC", "AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".
- **Username**  
Enter the username for authentication when selection from "Password" or "X.509 And Password".
- **Password**  
Enter the password for authentication when selection from "Password" or "X.509 And Password".
- **Local IP Address**  
Enter the local virtual IP address when select "P2P" and "OpenVPN Server" mode.
- **Remote IP Address**  
Enter the remote virtual IP address when select "P2P" mode.
- **Local Port**  
Specify the OpenVPN Server port, default is 1194.
- **Topology**  
Select the possible topology from "Subnet" and "Net30"  
Subnet: The recommended topology for modern servers. Note that this is not the current default. Addressing is done by IP & netmask.  
Net30: This is the old topology for support with Windows clients running 2.0.9 or older clients. This is the default as of OpenVPN 2.3, but not recommended for current use. Each client is allocated a virtual /30, taking 4 IPs per client, plus 4 for the server.
- **Subnet**  
Specify the subnet for the OpenVPN client. Default is 10.8.0.0
- **Subnet Netmask**  
Specify the subnet netmasks for OpenVPN client. Default is 255.255.255.0
- **TAP Bridge**  
Select the specified LAN that bridge with OpenVPN tunnel when select "TAP" connection type.
- **Renegotiate Interval**  
Enter the renegotiate interval if connection is failed.
- **Keepalive Interval**  
Enter the keepalive interval to check the tunnel is active or not.
- **Keepalive Timeout**  
Enter the keepalive timeout, once connection is failed it will trigger the OpenVPN reconnect.
- **Fragment**  
Enter the fragment size, 0 means disable.
- **Private Key Password**  
Enter the private key password for authentication when selection from "X.509" or "X.509 And Password".

- **Output Verbosity Level**

Enter the level of the output log and values.

## VPN->OpenVPN->Advanced Settings

- **Enable NAT**  
Check this box to enable NAT, the source IP of host behind router will be disguised before accessing the remote end.
- **Enable Default Gateway**  
Check this box to enable default gateway, all the data traffic will go through the VPN tunnel.
- **Enable PKCS#12**  
It is an exchange of digital certificate encryption standard, used to describe personal identity information.
- **Enable CRL**  
Check this box to enable CRL(Certificate Revocation List).
- **Enable Client to Client**  
Check this box to allow client to communicate with each other.
- **Enable Duplicate CN**  
Check this box allow multiple clients connect to the server with the same certificate/key files or common names.
- **Enable IP Persist**  
Check this box to keep the IP address unchanged.
- **Enable X.509 Attribute nsCertType**  
Require that peer certificate was signed with an explicit nsCertType designation of "server".
- **Enable HMAC Firewall**  
Add additional layer of HMAC authentication on the top of the TLS control channel to protect against DoS attacks.
- **Enable Compression LZ0**  
Compress the data.
- **Additional Configurations**  
Enter some other options of OpenVPN in this field. Each expression can be separated by a ','.

Status	OpenVPN	<u>X.509 Certificate</u>	Configuration Files
<b>X.509 Certificate Import</b>			
OpenVPN Mode	Client ▾		
Connection Index	1 ▾		
CA Certificate	Choose File	No file chosen	
Local Certificate File	Choose File	No file chosen	
Local Private Key	Choose File	No file chosen	
HMAC Firewall Key	Choose File	No file chosen	
Pre-shared Key	Choose File	No file chosen	
PKCS#12 Certificate	Choose File	No file chosen	
User-Password File	Choose File	No file chosen	
Private Key Password File	Choose File	No file chosen	
<b>X.509 Certificate Files</b>			
Index	File Name	File Size	Date Modified

## VPN->OpenVPN->X.509 Certificate

- **OpenVPN Mode**  
Select OpenVPN working mode between Server and Client.
- **Connection Index**  
Displays the current connection index for OpenVPN channel.
- **CA Certificate**  
Import CA certificate file.
- **Local Certificate File**  
Import Local Certificate file.
- **Local Private Key**  
Import Local Private Key file.
- **DH File**  
Import DH file when works as OpenVPN server.
- **HMAC Firewall Key**  
Import HMAC Firewall Key file.
- **Pre-shared Key**  
Import the pre-shared key file.
- **PKCS#12 Certificate**  
Import PKCS#12 Certificate.
- **User-Password File**  
Import the username and password file when import the OpenVPN client file.
- **Private Key Password File**  
Import the private key password file when import the OpenVPN client file.
- **CRL File**  
Import CRL file.

## 4.7.2 GRE

Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route other protocols over IP networks. It's a tunneling technology that provides a channel through which encapsulated data message could be transmitted and encapsulation and decapsulation could be realized at both ends.

GRE				
GRE Information				
Index	Enable	Description	Mode	Status

### VPN->GRE->Status

- **Enable**  
Displays current GRE settings is enable or disable.
- **Description**  
Displays the description of current VPN channel.
- **Mode**  
Displays the current VPN mode.
- **Status**  
Displays the current VPN connection status.

GRE Settings

General Settings

Index

1

Enable

☒

Description

Mode

Layer 3

Remote Gateway

Local Virtual IP

Local Virtual Netmask

255.255.255.252

Tunnel key

?

Enable NAT

☐

Enable Default Route

☐

Advanced Settings

Binding Interface

?

Save

Close

## VPN->GRE

- **Enable**  
Check this box to enable GRE.
- **Description**  
Enter the description of current VPN channel.
- **Mode**  
Specify the running mode of GRE, optional are "Layer 2" and "Layer 3".
- **Remote Gateway**  
Enter the remote IP address of peer GRE tunnel.
- **Local Virtual IP**  
Enter the local tunnel IP address of GRE tunnel.
- **Local Virtual Netmask**  
Enter the local virtual netmask of GRE tunnel.
- **Tunnel Key**  
Enter the authentication key of GRE tunnel.
- **Enable NAT**  
Check this box to enable NAT function.
- **Bridge Interface**  
Specify the bridge interface work with Layer 2 mode.
- **Enable Default Route**  
Check this box to make all the traffic go through VPN tunnel.
- **Binding Interface**  
Only specified interface turn into active WAN will start the VPN tunnel.

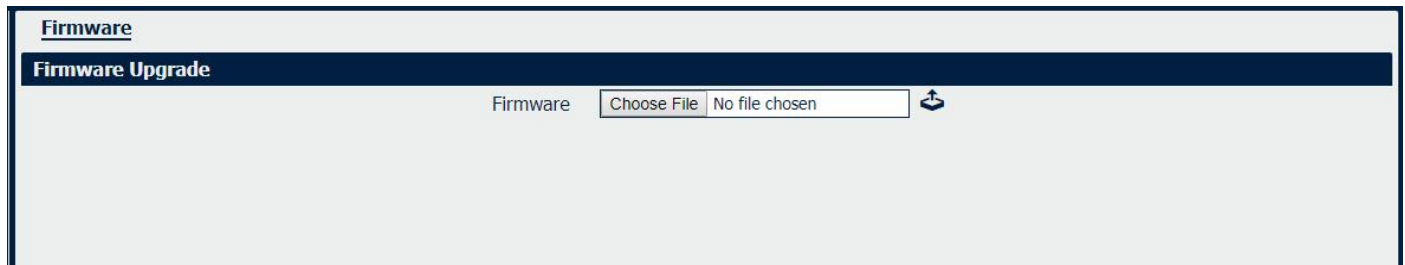
## 4.8 Maintenance

### 4.8.1 Upgrade

When newer versions of NR300 firmware become available, the user can manually update the unit by uploading a package to the unit.

**NOTE:** The unit need manually reboots once the upload completes, thus taking the NR300 router out of service during approximately 1 minute. Unless otherwise stated, the user is not expected to take any special precautions.

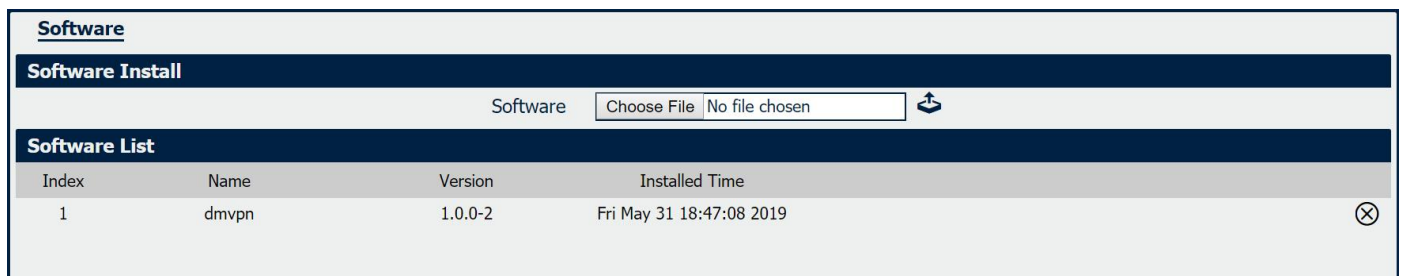
**CAUTION:** It is important to have a stable power source and ensure that power to the Fusion is not interrupted during a firmware upgrade.



### 4.8.2 Software

When release a new feature (APP Package) of NR300 router, the user can manually install to the unit by uploading a package. Or user can uninstall this feature (APP Package) from router.

**NOTE:** The unit need manually reboots once the upload/uninstall completes, thus taking the NR300 router out of service during approximately 1 minute. Unless otherwise stated, the user is not expected to take any special precautions.



Click  to upload the APP Package.

Click  to delete the APP Package.

*Note: We are working different kinds of the APP Packages. Please contact us to get them in case of you would like to test.*

## 4.8.3 System

This section allows you to review the device system settings.

<u>General</u>	Accounts	Syslog	Web Server	Telnet	SSH	Security
<b>General Settings</b>						
Hostname		novusautomation.com				
User LED Type		None ▼				
<b>Time Zone Settings</b>						
Time Zone		UTC+08:00 ▼				
Customized Time Zone		<input type="text"/> ?				
<b>Time Synchronisation</b>						
Enable		<input checked="" type="checkbox"/>				
Primary NTP Server		pool.ntp.org				
Secondary NTP Server		1.pool.ntp.org				
Synchronize Modem Time		<input type="checkbox"/>				

### System->General

- **Hostname**  
User-defined router name, which might be use for IPSec local ID identify.
- **User LED Type**  
Defined the User LED behavior.
- **Time Zone**  
Select the zone where the device is in use.
- **Customized Time Zone**  
Customized the zone where the device is in use.
- **Enable (NTP Client)**  
Selected Enabled to utilize the NTP client to synchronize the device clock over the network using a time server (NTP server).
- **Primary NTP Server**  
Enter the IP address (or host name) of the primary time server.
- **Secondary NTP Server**  
Enter the IP address (or host name) of the secondary time server.
- **Synchronize Modem Time**  
Synchronize the time from cellular module.

GeneralAccountsSyslogWeb ServerTelnetSSHSecurity

Account Settings

Administrator

admin

Old Password

New Password

Confirm Password

Visitor Settings

Index

Username

Password

System->Account

- Administrator**  
Displays the name of current administrator, default as "admin".
- Old Password**  
Enter the old password of administrator.
- New Password**  
Enter the new password of administrator.
- Confirm Password**  
Confirm the new password of administrator.

Account Settings

Account Settings

Index

1

Username

Password

Save

Close

System->Account



- Username**  
Enter a username of visitor privilege
- Password**  
Enter the new password of current visitor account.

Syslog displays system logs that are stored in the log buffers.

General	Accounts	Syslog	Web Server	Telnet	SSH	Security
<b>General Settings</b>						
		Log Location	RAM ▼			
		Log Level	Debug ▼			
<b>Remote Syslog Settings</b>						
		Enable Remote Syslog	<input type="checkbox"/>			
		Remote Syslog Server	<input type="text"/>			
		Remote Syslog Port	514			

### System->Syslog

- **Log Location**  
Select the log store location to "RAM".
- **Log Level**  
Select the log output level from "Debug", "Notice", "Info", "Warning" or "Error".
- **Enable Remote Syslog**  
Check this box to enable remote syslog connection.
- **Remote Syslog Server**  
Enter the IP address of remote syslog server.
- **Remote Syslog Port**  
Enter the port for remote syslog server listening.

General	Accounts	Syslog	Web Server	Telnet	SSH	Security
<b>General Settings</b>						
		HTTP Port	80			
		HTTPS Port	443			
<b>Certificate Settings</b>						
		Private Key	Choose File	No file chosen		
		Certificate File	Choose File	No file chosen		

### System->Web Server

- **HTTP Port**  
Enter the port for Hypertext Transfer Protocol. A well-known port for HTTP is port 80.
- **HTTPS Port**  
Enter the port for HTTPS Protocol. A well-known port for HTTPS is port 443.
- **Private Key**  
Import private Key file for HTTPS connection.
- **Certificate File**  
Import certificate file for HTTPS connection.

General	Accounts	Syslog	Web Server	<u>Telnet</u>	SSH	Security
<b>General Settings</b>						
				Telnet Port	<input type="text" value="23"/>	

### System->Telnet

- **Telnet Port**  
Enter the port for telnet access. A well-known port for HTTP is port 23.

General	Accounts	Syslog	Web Server	Telnet	<u>SSH</u>	Security
<b>General Settings</b>						
				SSH Port	<input type="text" value="22"/>	
				Allow Password Authentication	<input checked="" type="checkbox"/>	
				Public Key	<input type="text"/>	

### System->SSH

- **SSH Port**  
Enter the port for SSH access. A well-known port for HTTP is port 22.
- **Allow Password Authentication**  
Check this box to enable SSH authentication.
- **Public Key**  
Enter the public Key SSH authentication.

General	Accounts	Syslog	Web Server	Telnet	SSH	<u>Security</u>
<b>Access Settings</b>						
				Remote HTTP Access	<input type="checkbox"/>	
				Remote HTTPS Access	<input checked="" type="checkbox"/>	
				Remote Telnet Access	<input type="checkbox"/>	
				Remote SSH Access	<input checked="" type="checkbox"/>	
				Local HTTP Access	<input checked="" type="checkbox"/>	
				Local HTTPS Access	<input checked="" type="checkbox"/>	
				Local Telnet Access	<input checked="" type="checkbox"/>	
				Local SSH Access	<input checked="" type="checkbox"/>	
<b>Ping Settings</b>						
				Remote Ping Request	<input checked="" type="checkbox"/>	
				Local Ping Request	<input checked="" type="checkbox"/>	
				DDoS Defense	<input checked="" type="checkbox"/>	

## System->Security

- **Remote HTTP Access**  
Check this box to allow remote HTTP access.
- **Remote HTTPS Access**  
Check this box to allow remote HTTPS access.
- **Remote Telnet Access**  
Check this box to allow remote Telnet access.
- **Remote SSH Access**  
Check this box to allow remote SSH access.
- **Local HTTP Access**  
Check this box to allow local HTTP access.
- **Local HTTPS Access**  
Check this box to allow local HTTPS access.
- **Local Telnet Access**  
Check this box to allow local Telnet access.
- **Local SSH Access**  
Check this box to allow local SSH access.
- **Remote Ping Request**  
Check this box to allow remote ping request.
- **Local Ping Request**  
Check this box to allow local ping request.
- **DDoS Defense**  
Check this box to enable DDoS defense.

## 4.8.4 Configuration

The Unit Configuration tab allows you to save parameters (settings in the Web interface) to a file. Conversely, if you have saved settings from the NR300 router to a file, you can Import these previously-saved configuration settings to the NR300 router as well.

**Configuration**

**Configuration Management**

Factory settings **Restore**

Configuration File Download **Download**

Configuration File Upload  No file chosen

### System->Configuration

- **Restore**  
Reset the unit to factory default settings.
- **Download**  
Download the configuration file from NR300 router.
- **Configuration File Upload**  
Import previously-saved configuration file.

## 4.8.5 Debug Tools

**Debug Tools**

**Ping** Traceroute AT Debug Sniffer

**Ping Settings**

Host Address

Ping Count

Local IP Address

### Debug Tools->Ping

- **Host Address**  
Enter a host IP address or domain name for ping.
- **Ping Count**  
Enter the ping times.
- **Local IP Address**  
Enter the ping source IP address or leave it blank.

Ping	<u>Traceroute</u>	AT Debug	Sniffer
<b>Traceroute Settings</b>			
		Host Address	<input type="text"/>
		Max Hops	<input type="text" value="30"/>

### Debug Tools->Traceroute

- **Host Address**  
Enter a host IP address or domain name for traceroute.
- **Max Hops**  
Enter the max hops for traceroute.

Ping	Traceroute	<u>AT Debug</u>	Sniffer
<b>AT Debug Settings</b>			
		AT Command	<input type="text"/>

### Debug Tools->AT Debug

- **AT Command**  
Enter the AT command of the module.

Ping	Traceroute	AT Debug	<u>Sniffer</u>
<b>Sniffer Settings</b>			
		Source Host	<input type="text"/>
		Source Port	<input type="text"/>
		Destination Host	<input type="text"/>
		Destination Port	<input type="text"/>
		Interface	<input type="text"/>
<b>Sniffer Files List</b>			
Index	File Name	File Size	Date Modified

### Debug Tools->Sniffer>Sniffer Settings

- **Source Host**  
Enter the source IP address.
- **Source Port**  
Enter the source port.
- **Destination Host**  
Enter the destination IP address.
- **Destination Port**  
Enter the destination port.
- **Interface**  
Enter the interface that the packages go through.

## Debug Tools->Sniffer>Sniffer Files List

- **File Name**  
Display the file name of package.
- **File Size**  
Display the file size of package.
- **Date Modified**  
Display the date of the package.

# Appendix A -Glossary

<b>APN:</b>	Access Point Name
<b>GPRS:</b>	General Packet Radio Service
<b>HSPA:</b>	High Speed Packet Access
<b>HSDPA:</b>	High-Speed Downlink Packet Access
<b>HSUPA:</b>	High-Speed Uplink Packet Access
<b>LTE:</b>	3GPP Long Term Evolution
<b>IMEI:</b>	International Mobile Equipment Identity
<b>ICCID:</b>	Integrated Circuit Card Identifier
<b>PIN:</b>	Personal Identification Number
<b>PPP:</b>	Point-to-Point Protocol
<b>RSSI:</b>	Received Signal Strength Indication
<b>SIM:</b>	Subscriber Identity Module
<b>SMS:</b>	Short Message Service
<b>DHCP:</b>	Dynamic Host Configuration Protocol
<b>LAN:</b>	Local Area Network
<b>LED:</b>	Light-Emitting Diode
<b>NTP:</b>	Network Time Protocol
<b>SMA:</b>	SubMiniature version A (connector)
<b>SSID:</b>	Service Set Identifier
<b>TCP/IP:</b>	Transmission Control Protocol / Internet Protocol
<b>UDP:</b>	User Datagram Protocol
<b>VPN:</b>	Virtual Private Network
<b>VDC:</b>	Voltage, Direct Current

# Appendix B -Q&A

## No Signal

### Phenomenon

NR300 Router modem status show no signal.

### Possible Reason

- Antenna installation is wrong.
- Modem failure.

### Solution

- Check the LTE antenna or replace with new one.
- Check the cellular page confirm modem is detected correctly or not.

## Cannot detect SIM card

### Phenomenon

NR300 Router cannot detect SIM card, cellular is not failed to connect to base station.

### Possible Reason

- SIM card damage.
- SIM bad contact.

### Solution

- Replace SIM card.
- Re-install SIM card.

## Poor Signal

### Phenomenon

NR300 Router no signal or poor signal.

### Possible Reason

- Antenna installation is wrong.
- Area signal weak.

### Solution

- Check the antenna and re-connect it.
- Contact Telecom Operator to confirm signal problem.
- Change to high-gain antenna.

## IPSec VPN established, but LAN to LAN cannot communicate

### Phenomenon

IPSec VPN established, but LAN to LAN cannot communicate

### Possible Reason

- Both subnets are not match the interested traffic.
- IPSec second phase (ESP) settings is not match.

### Solution

- Check the both subnet settings.
- Check IPSec second phase (ESP) setting.

## Forget Router Password

### Phenomenon

Forget router login password.

### Possible Reason

User has changed the password.

### Solution

After router power on, press RESET button between 3 to 10 seconds then release, router need manually reboot and reset to factory default settings (Username/Password is admin/admin).

# Appendix D - CLI

Command-line interface (CLI) is a software interface that provide another configurable way to set parameters on our router. We could use Telnet or SSH connect to our router for CLI input.

## NR300 CLI Access

navigateworx.router login: **admin**

Password: **admin**

>

## CLI reference commands

>?

config	Change to the configuration mode
exit	Exit this CLI session
help	Display an overview of the CLI syntax
ping	Ping
reboot	Reboot system
show	Show running configuration or running status
telnet	Telnet Client
traceroute	TraceRoute
upgrade	Upgrade firmware
version	Show firmware version

**e.g.**

> version

1.0.0 (337913f)

> ping www.baidu.com

PING www.baidu.com (14.215.177.38): 56 data bytes

64 bytes from 14.215.177.38: seq=0 ttl=54 time=10.826 ms

64 bytes from 14.215.177.38: seq=1 ttl=54 time=10.284 ms

64 bytes from 14.215.177.38: seq=2 ttl=54 time=10.073 ms

64 bytes from 14.215.177.38: seq=3 ttl=54 time=10.031 ms

64 bytes from 14.215.177.38: seq=4 ttl=54 time=10.347 ms

--- www.baidu.com ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 10.031/10.312/10.826 ms.

>

## How to Configure the CLI

### CONTEXT SENSITIVE HELP

[?] - Display context sensitive help. This is either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of this key, when a command has been resolved, will display a detailed reference.

### AUTO-COMPLETION

The following keys both perform auto-completion for the current command line. If the command prefix is not unique then the bell will ring and a subsequent repeat of the key will display possible completions.

[enter] - Auto-completes, syntax-checks then executes a command. If there is a syntax error then offending part of the command line will be highlighted and explained.

[space] - Auto-completes, or if the command is already resolved inserts a space.

### MOVEMENT KEYS

[CTRL-A] - Move to the start of the line

[CTRL-E] - Move to the end of the line.

[up] - Move to the previous command line held in history.

[down] - Move to the next command line held in history.

[left] - Move the insertion point left one character.

[right] - Move the insertion point right one character.

### DELETION KEYS

[CTRL-C] - Delete and abort the current line

[CTRL-D] - Delete the character to the right on the insertion point.

[CTRL-K] - Delete all the characters to the right of the insertion point.

[CTRL-U] - Delete the whole line.

[backspace] - Delete the character to the left of the insertion point.

### ESCAPE SEQUENCES

!! - Substitute the the last command line.

!N - Substitute the Nth command line (absolute as per 'history' command)

!-N - Substitute the command line entered N lines before (relative)