



Industrial Automation Headquarters

Delta Electronics, Inc.
Taoyuan Technology Center
No.18, Xinglong Rd., Taoyuan City,
Taoyuan County 33068, Taiwan
TEL: 886-3-362-6301 / FAX: 886-3-371-6301

Asia

Delta Electronics (Jiangsu) Ltd.
Wujiang Plant 3
1688 Jiangxing East Road,
Wujiang Economic Development Zone
Wujiang City, Jiang Su Province, P.R.C. 215200
TEL: 86-512-6340-3008 / FAX: 86-769-6340-7290

Delta Greentech (China) Co., Ltd.
238 Min-Xia Road, Pudong District,
ShangHai, P.R.C. 201209
TEL: 86-21-58635678 / FAX: 86-21-58630003

Delta Electronics (Japan), Inc.
Tokyo Office
2-1-14 Minato-ku Shibadaimon,
Tokyo 105-0012, Japan
TEL: 81-3-5733-1111 / FAX: 81-3-5733-1211

Delta Electronics (Korea), Inc.
1511, Byucksan Digital Valley 6-cha, Gasan-dong,
Geumcheon-gu, Seoul, Korea, 153-704
TEL: 82-2-515-5303 / FAX: 82-2-515-5302

Delta Electronics Int'l (S) Pte Ltd.
4 Kaki Bukit Ave 1, #05-05, Singapore 417939
TEL: 65-6747-5155 / FAX: 65-6744-9228

Delta Electronics (India) Pvt. Ltd.
Plot No 43 Sector 35, HSIIDC
Gurgaon, PIN 122001, Haryana, India
TEL : 91-124-4874900 / FAX : 91-124-4874945

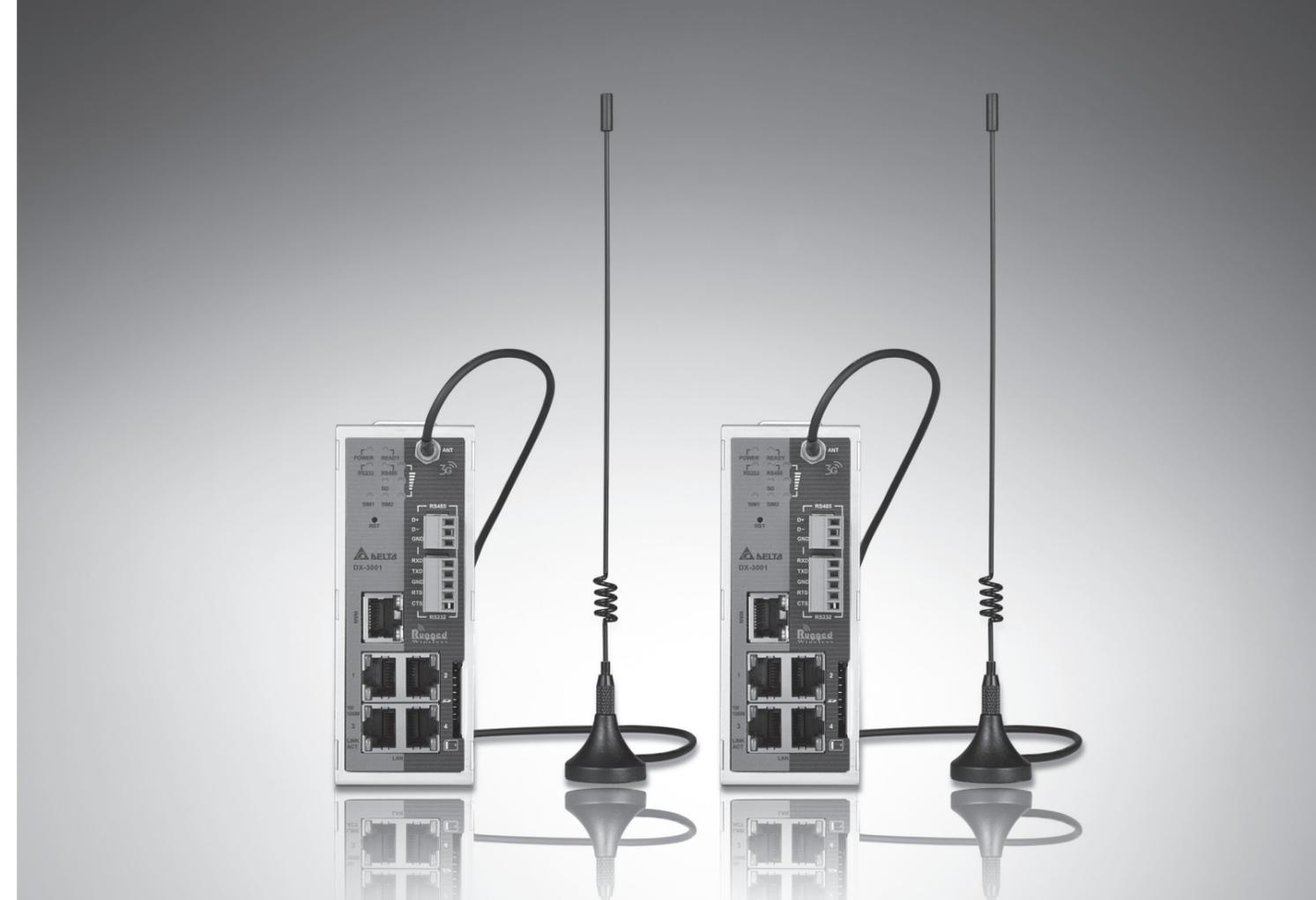
Americas

Delta Products Corporation (USA)
Raleigh Office
P.O. Box 12173, 5101 Davis Drive,
Research Triangle Park, NC 27709, U.S.A.
TEL: 1-919-767-3800 / FAX: 1-919-767-8080

Delta Greentech (Brasil) S.A.
Sao Paulo Office
Rua Itapeva, 26 - 3° andar Edificio Itapeva One-Bela Vista
01332-000-São Paulo-SP-Brazil
TEL: 55 11 3568-3855 / FAX: 55 11 3568-3865

Europe

Delta Electronics (Netherlands) B.V.
Eindhoven Office
De Witbogt 20, 5652 AG Eindhoven, The Netherlands
TEL : +31 (0)40-8003800 / FAX : +31 (0)40-8003898



DX-3001-V Series Industrial 3G/WAN VPN Router User Manual

2016-10-19

*We reserve the right to change the information in this manual without prior notice.

www.deltaww.com



DX-3001H9-V Industrial 3G-WAN VPN

Router User Manual

Table of Contents

Chapter 1 Introduction

1.1	Product Overview.....	1-3
1.1.1	Network Design	1-3
1.1.2	Features.....	1-4
1.1.3	Front Panel Ports and LEDs.....	1-5
1.1.4	Top Panel	1-5
1.1.5	Bottom Panel	1-6
1.1.6	Dimension	1-7
1.2	Package Checklist	1-7

Chapter 2 User Interface

2.1	Web-based GUI Configuration	2-2
2.1.1	System Connection	2-2
2.1.2	Default IP Address/Account/Password	2-2
2.1.3	Local Network Setups.....	2-2
2.1.4	Logging in	2-4

Chapter 3 Functions

3.1	Status	3-3
3.1.1	Network Status	3-3
3.1.2	Device	3-3
3.1.3	Log.....	3-5
3.2	Network.....	3-5
3.2.1	Connection	3-6
3.2.2	Cellular Link1.....	3-7
3.2.3	Cellular Link2.....	3-9
3.2.4	WAN	3-11

3.2.5	LAN	3-13
3.3	Firewall.....	3-14
3.3.1	Basic	3-14
3.3.2	DMZ	3-15
3.3.3	Port Forward.....	3-15
3.3.4	Port Trigger	3-17
3.3.5	URL Filter	3-19
3.3.6	MAC Filter	3-20
3.3.7	IP Filter.....	3-20
3.4	VPN.....	3-21
3.4.1	IPSec.....	3-21
3.4.2	OPENVPN	3-25
3.4.3	PPTP	3-27
3.4.4	L2TP	3-29
3.4.5	GRE.....	3-31
3.4.6	Certificate	3-33
3.4.7	VPN Log	3-34
3.5	Interface.....	3-34
3.5.1	RS232	3-34
3.5.2	RS485	3-36
3.5.3	Profile Management.....	3-37
3.5.4	FTP/SFTP Server	3-38
3.6	System.....	3-38
3.6.1	Name and Password	3-39
3.6.2	NTP Server	3-39
3.6.3	Firmware Upgrade.....	3-40
3.6.4	Backup & Restore	3-41
3.6.5	System Reboot	3-41
3.6.6	SD Card	3-41
3.6.7	Network Diagnosis.....	3-42

Chapter 1 Product Introduction

Table of Contents

- 1.1 Product Overview 1-3**
 - 1.1.1 Network Design 1-4
 - 1.1.2 Features 1-4
 - 1.1.3 Front Panel Ports and LEDs 1-5
 - 1.1.4 Top Panel 1-5
 - 1.1.5 Bottom Panel 1-6
 - 1.1.6 Dimension 1-7
- 1.2 Package Checklist 1-7**

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates radio frequency signal and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Declaration of Conformity

In accordance with the Directives 2004/108/EC*, 2014/30/EU, 2006/95/EC*, 2014/35/EU and 1999/5/EC. The test record, data evaluation and DX-2100RW-WW configurations represented herein are true and accurate under the standards herein specified.

EN 301 511 V9.0.2 (2003-3)

Test Items :

Radiated spurious emissions – MS allocated channel (Clause 4.2.16)

Radiated spurious emissions – MS in idle mode (Clause 4.2.17)

EN 301 908-1 V7.1.1 (2015-03)

EN 301 489-1 V1.9.2 (2011-09)

EN 301 489-7 V1.3.1 (2005-11)

EN 301 489-24 V1.5.1 (2010-10)

1.1 Product Overview

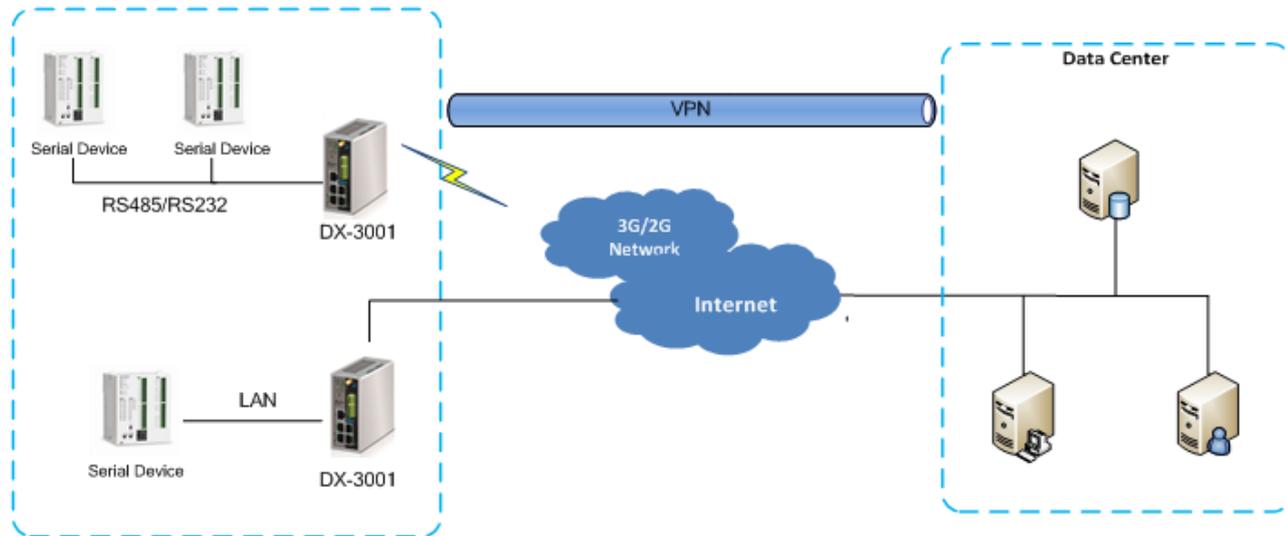
DX-3001H9-V is an industrial VPN router, it has 2 SIM card slots and supports multiple mobile networks like WCDMA, UMTS, HSUPA, GSM, GPRS, and EDGE. When one cellular network fails to work, the device will automatically switch to the other cellular network. Besides the two cellular network connections, the WAN port can be another connection to Internet. Priorities of the connection to Internet over WAN and 2 cellular networks are configurable. As there is only one 3G module in the device, the two cellular networks cannot be active at the same time.

Router support standard VPN protocols include PPTP, L2TP, OPENVPN, IPSec and GRE. With interfaces like Ethernet ports, RS232 and RS485, multiple peripheral devices can be connected to the device.

The product can be widely used on the M2M fields, such as industrial automation, smart power grids, finance, environment protection, intelligent building, intelligent transportation, video surveillance, intelligent self-service and so on.



1.1.1 Network Design

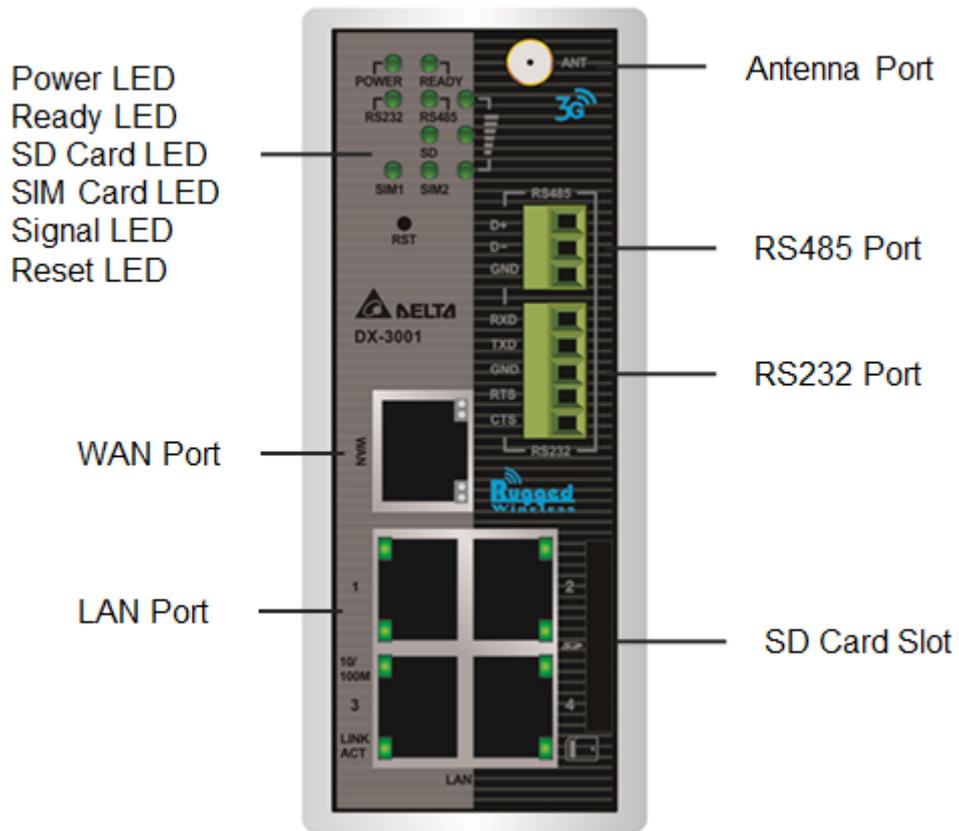


1.1.2 Features

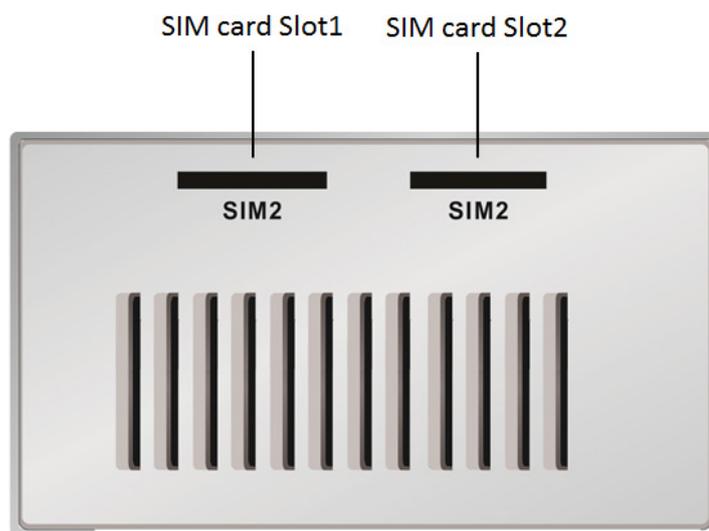
- Support HSPA+/HSUPA/HSDPA/UMTS: 800/850/900/AWS1700/1900/2100 MHz
- Support GSM/GPRS/EDGE: 850/900/1800/1900 MHz
- Support CHAP / PAP authentication
- Support APN access
- Support automatic redial when connection is broken
- WAN port access mode(static IP , DHCP client)
- Dual SIM card slots, support auto-switching between the cellular operators
- Provides dual serial ports (RS232 and RS485) and 4 LAN port to meet the needs of different devices connected
- Support PPTP/L2TP/OPENVPN/IPSec/GRE VPN
- Support LED status display
- Provides reset function
- Support NTP client, built-in independent RTC
- Support DHCP server
- Support Dynamic DNS

1.1.3 Front Panel Ports and LEDs

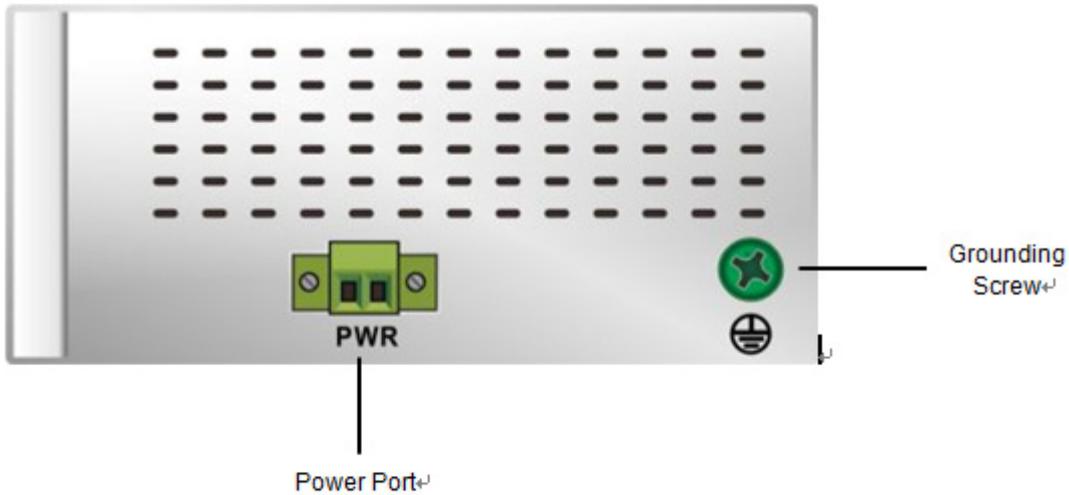
1



1.1.4 Top Panel



1.1.5 Bottom Panel



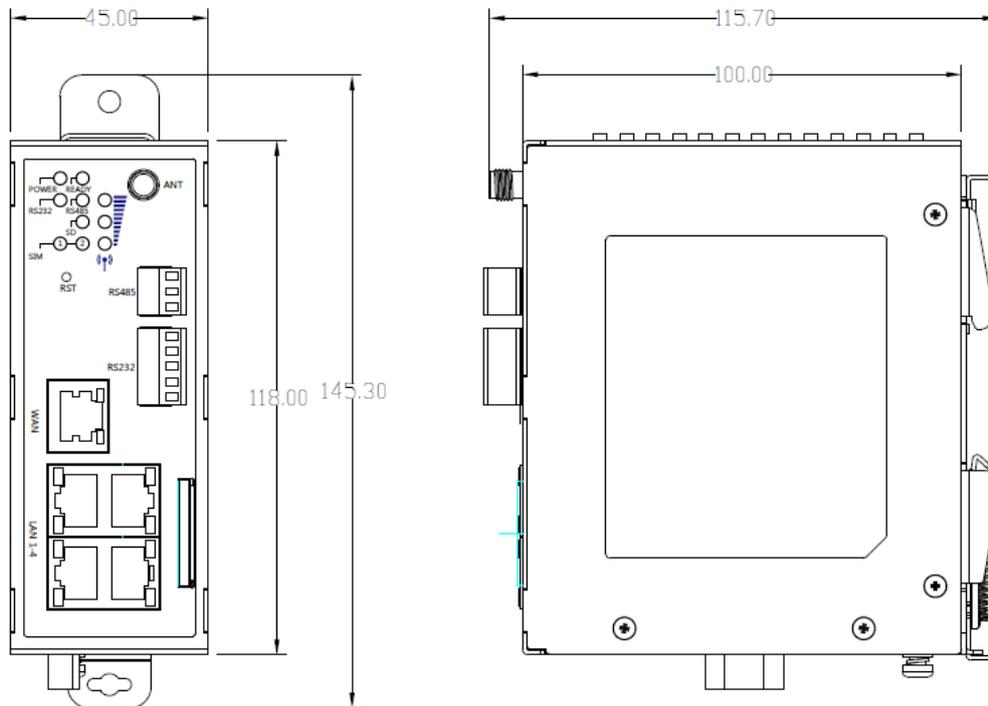
Notice

This router's reset button is on the front panel. By pressing the Reset button, users can reset the router or reset the router to factory default settings. See the instruction below:

- Reset the Router: With the router powered on, press the Reset button and release the button right away.
- Reset to Factory Defaults: With the router powered on, press and hold the Reset button for 3~6 seconds and then release the button.
 - Reset can only be done when the device is running properly.
 - With the router powered on, press and hold the Reset button until all the LEDs go out (except the Power LED). Then release the button and wait the router to reboot to its factory default settings.

1.1.6 Dimension

Unit = mm

1

1.2 Package Checklist

Unpack the package carefully and check the package contents. The package should contain the following items:

- DX-3001H9-V Industrial 3G VPN Router x 1
- Quick Installation Guide x 1
- SMA Antenna (300cm) x 1



Notice

Verify that nothing is missing from the DX-3001H9-V package by using the check list above. If any item is found missing or damaged, please contact your local sales representative for support.

Chapter 2 User Interface

Table of Contents

2.1	Web-based GUI Configuration	2-2
2.1.1	System Connection	2-2
2.1.2	Default IP Address/Account/Password	2-2
2.1.3	Local Network Setups	2-2
2.1.4	Logging in	2-4

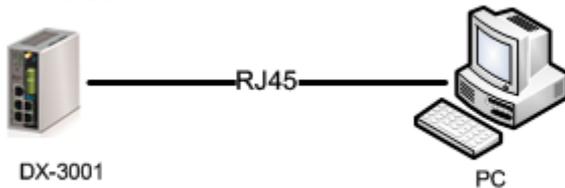
2.1 Web-based GUI Configuration

The DX-3001 Industrial Ethernet Cloud Router provides a friendly Web Browser Configuration for users to set up and operate more intuitively.

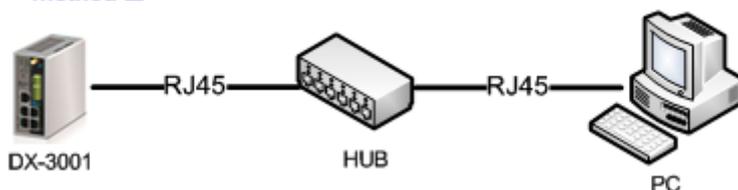
2.1.1 System Connection

First, connect the PC used for configuration with Ethernet interface of the router directly or through the switch/hub.

Method I



Method II



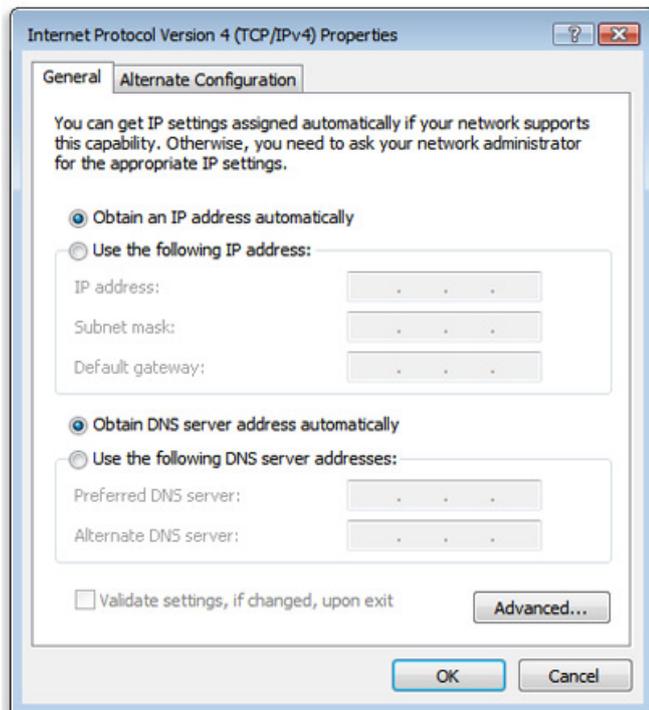
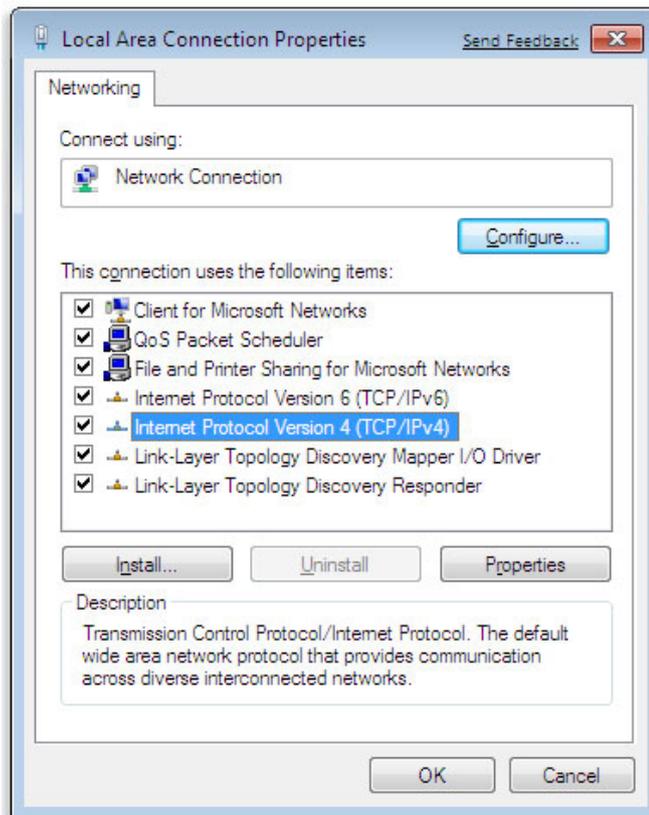
2.1.2 Default IP Address/Account/Password

The default IP address of router is 192.168.1.1. The initial account and password is admin/admin

2.1.3 Local Network Setups

After the connection of the local computer and the router is done, you will need to set the network configuration for your computer.

- **Obtain an IP address automatically by using the router as a DHCP server.**
 1. Open Network Connections by clicking the Start button , and then clicking Control Panel.
 2. Under Network and Sharing Center, click View network connections.
 3. Right-click the connection that you want to change, and then click Properties.  If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
 4. Click the Networking tab. Under This connection uses the following items, click either Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6), and then click Properties.
 5. Click Obtain DNS server address automatically and then click OK to get a DNS server address automatically using DHCP.

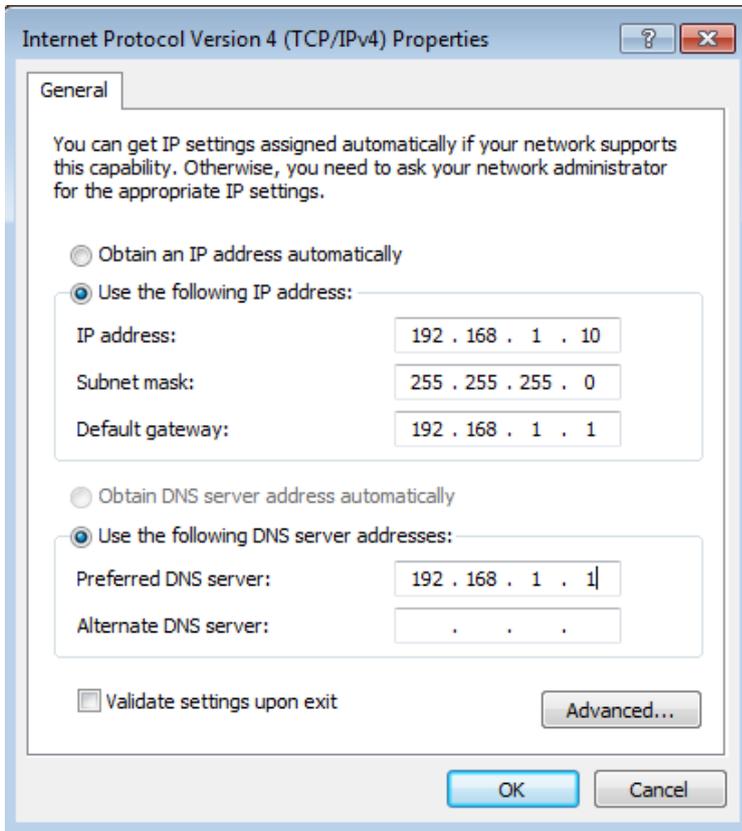


- **Set up the IP address manually.**

(The IP address of the computer should be in the same network segment as the router's.)

Since the router's default IP address is 192.168.1.1 and the subnet mask is 255.255.255.0, the computer's IP address can be set between 192.168.1.2 to 192.168.1.254. However, you'll need to make sure there are no IP conflicts.

Here, we set the address to 192.168.1.10 and the default gateway to 192.168.1.1. For DNS, the usable DNS address can be selected or the address can also be set to 192.168.1.1.



2

2.1.4 Logging in

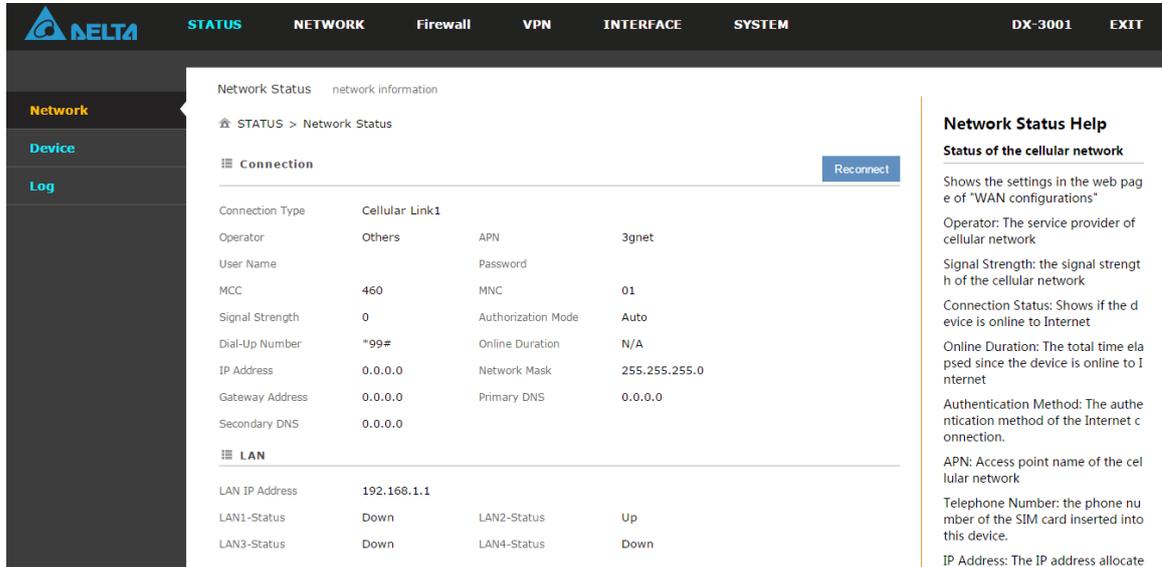
1. Open your Internet Explorer browser and input the router's LAN IP address (Default is 192.168.1.1) in the search bar and then press Enter.



2. You'll be prompted with the log-in page. Input the user name and the password (Default is admin/admin) and then press Enter to log in to the setup page.



3. After login, you can see the main selection area on the left hand side and the upper area of the page. The detailed settings can be seen on the right hand side of the page.



The screenshot displays the Delta network management interface. The top navigation bar includes 'STATUS', 'NETWORK', 'Firewall', 'VPN', 'INTERFACE', 'SYSTEM', 'DX-3001', and 'EXIT'. The left sidebar has 'Network', 'Device', and 'Log' options. The main content area is titled 'Network Status' and shows 'Cellular Link1' configuration. A 'Reconnect' button is visible. The LAN status is also shown at the bottom.

Connection			
Connection Type	Cellular Link1		
Operator	Others	APN	3gnet
User Name		Password	
MCC	460	MNC	01
Signal Strength	0	Authorization Mode	Auto
Dial-Up Number	*99#	Online Duration	N/A
IP Address	0.0.0.0	Network Mask	255.255.255.0
Gateway Address	0.0.0.0	Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0		

LAN			
LAN IP Address	192.168.1.1		
LAN1-Status	Down	LAN2-Status	Up
LAN3-Status	Down	LAN4-Status	Down

Network Status Help
Status of the cellular network
 Shows the settings in the web page of "WAN configurations"
 Operator: The service provider of cellular network
 Signal Strength: the signal strength of the cellular network
 Connection Status: Shows if the device is online to Internet
 Online Duration: The total time elapsed since the device is online to Internet
 Authentication Method: The authentication method of the Internet connection.
 APN: Access point name of the cellular network
 Telephone Number: the phone number of the SIM card inserted into this device.
 IP Address: The IP address allocated



Notice

For security, please modify the initial password as soon as possible.

Chapter 3 Functions

Table of Contents

3.1	Status	3-3
3.1.1	Network Status	3-3
3.1.2	Device.....	3-4
3.1.3	Log.....	3-5
3.2	Network	3-6
3.2.1	Connection	3-6
3.2.2	Cellular Link1	3-7
3.2.3	Cellular Link2.....	3-9
3.2.4	WAN	3-12
3.2.5	LAN	3-13
3.3	Firewall	3-15
3.3.1	Basic.....	3-15
3.3.2	DMZ	3-16
3.3.3	Port Forward	3-16
3.3.4	Port Trigger	3-18
3.3.5	URL Filter	3-20
3.3.6	MAC Filter.....	3-21
3.3.7	IP Filter	3-21
3.4	VPN	3-22
3.4.1	IPSec	3-22
3.4.2	OPENVPN	3-26
3.4.3	PPTP	3-28
3.4.4	L2TP	3-30
3.4.5	GRE	3-32
3.4.6	Certificate.....	3-34
3.4.7	VPN Log	3-35
3.5	Interface	3-35
3.5.1	RS232.....	3-35
3.5.2	RS485.....	3-36
3.5.3	Profile Management	3-38
3.5.4	FTP/SFTP Server	3-42

3.6	System	3-43
3.6.1	Name and Password	3-43
3.6.2	NTP Server	3-44
3.6.3	Firmware Upgrade	3-45
3.6.4	Backup & Restore	3-46
3.6.5	System Reboot	3-46
3.6.6	SD Card	3-47
3.6.7	Network Diagnosis.....	3-47

3.1 Status

You can view summary or detailed information on the Device Information, Network Status, and Log.

3.1.1 Network Status

This page shows basic information on Network Status, LAN Status and traffic.

When router connects to internet by WAN port, the connection includes the connection type, WAN mode, IP Address, Network Mask, Gateway Address, primary DNS, and Secondary DNS.

When router connects to internet by Cellular, the connection includes the Operator, APN, User Name, Password, MCC, MNC, Signal Strength, Authorization Mode, Online Duration, IP Address, Network Mask, Gateway Address, primary DNS, and Secondary DNS.

LAN includes the LAN IP Address, and connection status of 4 LAN port. Up means connected, down means disconnected.

Traffic statistics shows network traffic information of the Cellular Link 1&2 and WAN port.

[STATUS](#) > Network Status

Connection Reconnect			
Connection Type	WAN	WAN Mode	DHCP
IP Address	0.0.0.0	Network Mask	0.0.0.0
Gateway Address	0.0.0.0	Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0		
LAN			
LAN IP Address	192.168.1.1		
LAN1-Status	Down	LAN2-Status	Up
LAN3-Status	Down	LAN4-Status	Down
Traffic Statistics			
Cellular Link1-Sent	0 bytes	Cellular Link1-Received	0 bytes
Cellular Link2-Sent	0 bytes	Cellular Link2-Received	0 bytes
WAN-Sent	0 bytes	WAN-Received	0 bytes

3.1.2 Device

This page shows basic information on the Hardware/Software version and Resource Usage Information

🏠 STATUS > Device

☰ Basic

Device Type: DX3001
 Device Name: DX3001_DA90
 S/N: DXL3001116140010

☰ Version

Hardware Version: DX3001
 Release Date: 2016-03-14 04:28:44 PM
 Firmware Version: DX3001-0.8.1.2-2016-05-19
 Upgrade Date: 2016-05-19 02:33:39

☰ Resource Usage

CPU Usage: 6%
 Total Memory: 121696KB
 Memory Used: 93144KB
 Memory Usage: 76%
 SD Card Status:
 SD Card Capacity: 0
 SD Card Usage: 0

● Basic

Item	Description
Device Type	Model type of the router
Device Name	Name of the router, the default is DX3001 + “_” + “the last four digits of Mac address”
S/N	Serial number of the router

● Version

Item	Description
Hardware Version	Version number of the hardware currently used on the router

Release Date	Hardware release date
Current Version	Version number of the software currently used on the router
Upgrade Date	Upgrade time of the software currently used on the router

- Resource Usage

Item	Description
CPU Usage	The CPU usage of current router
Total Memory	The total memory on the router
Memory Used	The memory currently used on the router.
Memory Usage	The current ratio of the router usage
SD Card Status	The SD card status in the router.
SD Card Capacity	The total storage of the SD card
SD Card Usage	The storage currently usage of SD card

3.1.3 Log

This page shows logs of the router, including the System log, Warning log and the Debug log. You can use the buttons on the right hand side to refresh, clear or download the displayed logs.

🏠 STATUS > Device Logs

☰ Log Type

Informative log Warning log Debug log

☰ Log Content

Refresh Clear Download

Timestamp	Content
May 19 05:44:04	syslog.info syslogd started: BusyBox v1.22.1
May 19 05:44:12	user.info WATCHDOG[1488]: watchdog enabled!
May 19 05:44:12	user.info SMSTrigger: [SMSTrigger:]SMSTrigger run in /dev/ttyUSB1 115200 mode.
May 19 05:44:12	user.err SMSTrigger: [SMSTrigger:]Open FIFO failed.FD value:-1 errno:2 retry : 0!
May 19 05:44:12	authpriv.warn dropbear[1490]: Failed loading /etc/dropbear/dropbear_dss_host_key
May 19 05:44:12	authpriv.warn dropbear[1490]: Failed loading /etc/dropbear/dropbear_ecdsa_host_key
May 19 05:44:12	authpriv.info dropbear[1536]: Running in background
May 19 05:44:13	user.info collection: main.c(517)-main: argc=4
May 19 05:44:13	user.info collection: main.c(518)-main: Path: /var/collection
May 19 05:44:13	user.info collection: main.c(519)-main: File rotate: 20
May 19 05:44:13	user.info collection: main.c(520)-main: Interval: 5
May 19 05:44:13	user.info gre_app: [GRE_APP] gre_app start

PREV 1 2 3 4 5 NEXT

3.2 Network

You can set up networks configuration, including the connection priority, Cellular network, WAN and LAN Configurations.

3.2.1 Connection

This page is used for setting up the connection priority. Router provide 3 links to connect to Internet, include cellular link 1&2 and WAN, user can appoint the connect order in this page.

[🏠 NETWORK](#) > Connection Priority

☰ Connection Priority

Primary Connection	<input type="text" value="WAN"/>
Secondary Connection	<input type="text" value="Disable"/>
Tertiary Connection	<input type="text" value="Disable"/>
Auto Detect	<input type="text" value="Ping"/>
Target Address 1	<input type="text" value="114.114.114.114"/>
Target Address 2	<input type="text" value="8.8.8.8"/>
Dial Failure To Restart	<input type="text" value="Enable"/>
Detect Interval	<input type="text" value="120"/> (5~300s)

Description	Default
Primary Connection	
Appoint the first interface for internet connection, user can choose WAN, cellular link1 or cellular link2	WAN
Secondary Connection	
Appoint the second interface for internet connection, user can choose one from the rest of the 2 interface, or disable it	Disabled
Tertiary Connection	
Appoint the third interface for internet connection, user can choose the rest of the interface, or disable it	Disabled
Auto Detect	
Check if the connection is dropped or not via PING or FTP/SFTP test.	Disabled
Target Address 1	
Set the first IP/domain of the server that program will do a ping testing.	N/A

Description	Default
Target Address 1	
Set the second IP/domain of the server that program will do a ping testing.	N/A
Dial Failure To Restart	
Enable or disable the function if the dial failure will be in the default time to restart device.	Disabled
Detect Interval	
Setup the interval time in seconds between two detect action	120

3.2.2 Cellular Link1

This page is used for setting up the Cellular Network for Link1(SIM1), including the Operator, User Name, Password, APN, Authorization Mode, Dial-Up Number, Dial-Up Mode, Redial Interval, Redial Times, Max Idle Time, Connection Check Interval, Connection Check Times, and MTU.

🏠 NETWORK > Cellular Link1

☰ Cellular Link1

Operator	Auto ▼
User Name	<input type="text"/>
Password	<input type="password"/>
APN	3gnet
Authorization Mode	Auto ▼
Dial-Up Number	*99#(UMTS/3G/3.5G) ▼
Dial-Up Mode	Always online ▼
Redial Interval	<input type="text" value="30"/> (second)
Redial Times	<input type="text" value="0"/> (0 means always redial)
Max Idle Time	<input type="text" value="0"/> (0 means always online)
Connection Check Interval	<input type="text" value="60"/> second (0 means not checked)
Connection Check Times	<input type="text" value="5"/>
MTU	<input type="text" value="1492"/>

Save

Cancel

Description	Default
Operator	
Select Auto or Others for the Operator from the dropdown list. <ul style="list-style-type: none"> ● Auto: the system will detect the operator from the inserted SIM card and set up accordingly. ● Others: users can set up the operator manually. 	AUTO
User Name	
This name is provided by the operator. When "Auto" is selected, the system will set the name up automatically and users cannot change the setting.	N/A
Password	
This password is provided by the operator. When "Auto" is selected, the system will set the password up automatically and users cannot change the setting.	N/A
APN (Access Point Name)	
This APN is provided by the operator. When "Auto" is selected, the system will set the APN up automatically and users cannot change the setting.	3gnet
Authorization Mod	
Options are "Auto", "PAP" and "CHAP".	Auto
Dial-Up Number	
This number is provided by the operator. When "Auto" is selected, the system will set the number up automatically.	*99#
Dial-Up Mode	
Options are : <ul style="list-style-type: none"> ● Always online: stay connected and once a disconnection is detected, the router will redial to connect automatically. ● On-demand connection: redial when connection to the internet is on demand. ● Manual connection: users dial to connect and when it fails to connect, it will not redial. 	Always online
Redial Interval	
Set up the time to redial when the system fails to connect. This will only be executed when the option "Always online" or "On-demand connection" is selected.	30
Redial Times	
Set up the maximum redial time, 0 indicating infinity. This will only be executed when the option "Always online" or "On-demand connection" is selected.	5
Max Idle Time	
Set up the maximum idle time. When the idle time exceeds the set value,	180

Description	Default
the router will disconnect and then redial, 0 indicating not to disconnect.	
Connection Check Interval	
Set up the connection check interval. Check the connectivity, if the connection is lost, it will redial automatically, 0 indicating not to check the connectivity.	60
Connection Check Times	
Set up the connection check times, 0 indicating infinity. Once a disconnection is detected, and the option “Always online” or “On-demand connection” is selected, the router will redial according to the set value in the Redial Times.	5
MTU	
Maximum Transmission Unit is the largest packet that can be transmitted over packet based networks.	1492

3.2.3 Cellular Link2

This page is used for setting up the Cellular Network for Link1(SIM2), including the Operator, User Name, Password, APN, Authorization Mode, Dial-Up Number, Dial-Up Mode, Redial Interval, Redial Times, Max Idle Time, Connection Check Interval, Connection Check Times, and MTU.

🏠 NETWORK > Cellular Link2

☰ Cellular Link2

Operator	<input type="text" value="Auto"/>
User Name	<input type="text"/>
Password	<input type="text"/>
APN	<input type="text" value="3gnet"/>
Authorization Mode	<input type="text" value="Auto"/>
Dial-Up Number	<input type="text" value="*99#(UMTS/3G/3.5G)"/>
Dial-Up Mode	<input type="text" value="Always online"/>
Redial Interval	<input type="text" value="30"/> (second)
Redial Times	<input type="text" value="0"/> (0 means always redial)
Max Idle Time	<input type="text" value="0"/> (0 means always online)
Connection Check Interval	<input type="text" value="60"/> second (0 means not checked)
Connection Check Times	<input type="text" value="5"/>
MTU	<input type="text" value="1492"/>

Description	Default
Operator	
Select Auto or Others for the Operator from the dropdown list. <ul style="list-style-type: none"> ● Auto: the system will detect the operator from the inserted SIM card and set up accordingly. ● Others: users can set up the operator manually. 	AUTO
User Name	
This name is provided by the operator. When “Auto” is selected, the system will set the name up automatically and users cannot change the setting.	N/A
Password	
This password is provided by the operator. When “Auto” is selected, the system will set the password up automatically and users cannot change the setting.	N/A

Description	Default
APN (Access Point Name)	
This APN is provided by the operator. When "Auto" is selected, the system will set the APN up automatically and users cannot change the setting.	3gnet
Authorization Mod	
Options are "Auto", "PAP" and "CHAP".	Auto
Dial-Up Number	
This number is provided by the operator. When "Auto" is selected, the system will set the number up automatically.	*99#
Dial-Up Mode	
Options are : <ul style="list-style-type: none"> ● Always online: stay connected and once a disconnection is detected, the router will redial to connect automatically. ● On-demand connection: redial when connection to the internet is on demand. ● Manual connection: users dial to connect and when it fails to connect, it will not redial. 	Always online
Redial Interval	
Set up the time to redial when the system fails to connect. This will only be executed when the option "Always online" or "On-demand connection" is selected.	30
Redial Times	
Set up the maximum redial time, 0 indicating infinity. This will only be executed when the option "Always online" or "On-demand connection" is selected.	5
Max Idle Time	
Set up the maximum idle time. When the idle time exceeds the set value, the router will disconnect and then redial, 0 indicating not to disconnect.	180
Connection Check Interval	
Set up the connection check interval. Check the connectivity, if the connection is lost, it will redial automatically, 0 indicating not to check the connectivity.	60
Connection Check Times	
Set up the connection check times, 0 indicating infinity. Once a disconnection is detected, and the option "Always online" or "On-demand connection" is selected, the router will redial according to the set value in the Redial Times.	5
MTU	
Maximum Transmission Unit is the largest packet that can be transmitted over packet based networks.	1492

3.2.4 WAN

🏠 NETWORK > WAN

☰ WAN Settings

WAN Mode

IP Allocation Method

IP Address

Network Mask

Gateway Address

Packet MTU

(Don't change the settings unless really need to)

Retrieve DNS Address By:

Primary DNS

Secondary DNS

Description	Default
WAN Mode	
Your device can connect to the internet via the WAN port with a Dynamic IP or Static IP. <ul style="list-style-type: none"> ● Static IP: Manually set up the IP address. ● Dynamic IP: DHCP (Dynamic Host Configuration Protocol) allows you to obtain an IP address automatically from your router. 	DHCP
IP Allocation Method	
The IP Allocation Method is the same as the WAN Connection Mode that you have set. You can apply to different option by modifying the WAN Connection Mode. <ul style="list-style-type: none"> ● Dynamic: Dynamic Host Configuration Protocol (DHCP) allows you to obtain an IP address automatically from your router. ● Manual: Manually set up the IP address (Static). 	DHCP
IP Address	

Description	Default
Set up an IP address for your device to connect to the internet via the WAN port. It's configurable when the mode is set to Static.	0.0.0.0
Network Mask	
Set up the WAN network mask. It's configurable when the mode is set to Static.	0.0.0.0
Gateway Address	
Set up the gateway address. It's configurable when the mode is set to Static.	0.0.0.0
MTU	
Maximum Transmission Unit is the largest packet that can be transmitted over packet based networks.	1500
Retrieve DNS Address By	
<p>The Retrieve DNS Address Method is the same as the WAN Connection Mode that you have set. You can apply to different option by modifying the WAN Connection Mode.</p> <p>DNS address can be retrieved by DHCP setup or manually set.</p> <ul style="list-style-type: none"> ● Dynamic: Dynamic Host Configuration Protocol (DHCP) allows you to obtain an IP address automatically from your router. ● Manual: Manually set up the IP address (Static). 	DHCP
Primary DNS	
Set up the primary DNS. It's configurable when the mode is set to Static.	0.0.0.0
Secondary DNS	
Set up the secondary DNS. It's configurable when the mode is set to Static.	0.0.0.0

3.2.5 LAN

This page is used for setting up the LAN, including IP Address, Network Mask, and DHCP Server.

🏠 NETWORK > LAN

☰ LAN Settings

IP Address

Network Mask

DHCP Server

Address Lease Time

First IP Address 192.168.1.

Last IP Address 192.168.1.

STP

Description	Default
IP Address	
Set up an IP address for your device.	192.168.1.1
Network Mask	
Set up the LAN network mask.	255.255.255.0
DHCP Server	
Dynamic Host Configuration Protocol allows you to obtain an IP address automatically from your router. You can enable or disable this functionality.	Enable
Address Lease Time	
To set up the address lease time so that a client doesn't hold an IP address indefinitely. It allows for a mechanism to gracefully reuse DHCP addresses. Options here are 1 to 3 days.	One day
First IP Address	
To increase the number of addresses available to clients, you can change the Start Address.	192.168.1.100
Last IP Address	
To increase the number of addresses available to clients, you can change the End Address.	192.168.1.200
STP	

Description	Default
Enable or disable STP(spanning tree protocol) function	Enable



Notice

STP is a network protocol that builds a logical loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Enable this option will increase traffic usage

3.3 Firewall

You can set up firewall configurations, including the Basic Configurations, DMZ Configurations, Port Forward, Port Trigger, URL Filter, MAC Filter, and IP Filter.

3.3.1 Basic

This page is used for setting up the basic firewall settings, including the SPI firewall switch, WAN Ping response, LAN SSH function and WAN SSH.

[🏠 FIREWALL > Basic](#)

☰ Basic Firewall Settings

SPI Firewall	Enable ▼
WAN Ping	Not response ▼
LAN SSH	Enable ▼
WAN SSH	Disable ▼

Save

Cancel

Description	Default
SPI Firewall	
The SPI Firewall keeps track of the state of network connections travelling across it, protecting your Internet connection against Internet threats and Denial of Service (DoS).	Disable
WAN Ping	
It creates a filter that your router not to respond to Ping command and prevents other users on the internet from pinging your pc and gaining your IP address.	Not responded
LAN SSH	
Set up whether to allow LAN end to connect with the router via SSH.	Enable

Description	Default
WAN SSH	
Set up whether to allow WAN end to connect with the router via SSH.	Disable



Notice
Please disable the SPI firewall function first when you enabled VPN function.

3.3.2 DMZ

This page is used for setting up the DMZ server.

[HOME](#) [FIREWALL](#) > [DMZ](#)

DMZ

DMZ Server

DMZ Host IP Address

Description	Default
DMZ Server	
Demilitarized zone (DMZ) is a special segment of the local network reserved for servers accessible from the Internet, adding an additional layer of security.	Disable
DMZ Host IP Address	
Set up the IP address for the DMZ host.	N/A

3.3.3 Port Forward

This page is used for setting up the port forward, including configuring the Network Services, Service Name, Protocol, Public Port, Server Port, and Server IP Address.

Click the "Add A Portforward Rule" to add port forwarding entries to the router.

[HOME](#) [FIREWALL](#) > [Port Forward](#)

ID	Service Name	Protocol	Public Port	Server Port	Server IP Address
----	--------------	----------	-------------	-------------	-------------------

After clicking the “Add A Portforward Rule” , you will see the following page.

🏠 FIREWALL > Port Forward

☰ Add A Portforward Rule

Network Services	<input type="text" value="Customized"/>
Service Name	<input type="text"/>
Protocol	<input type="text" value="TCP/UDP"/>
Public Port	<input type="text" value="Single port"/> <input type="text"/> (1~65534)
Server Port	<input type="text" value="Single port"/> <input type="text"/> (1~65534)
Server IP Address	192.168.1. <input type="text"/>

Description	Default
Network Services	
Select the common network services. Refer to the following common service list for optional values.	Customized
Service Name	
Set up the service name for port forwarding. The name is composed of letters, numbers and underline, starting with a letter or number. The maximum string length is 32 bytes.	N/A
Protocol	
Set up the protocol type for port forwarding.	TCP/UDP
Public Port	
Set up the public port for port forwarding. The port range is 1~65534. A Public port should be less than or equal to the server port.	Single Port
Server Port	
Set up the server port for port forwarding. The port range is 1~65534. A server port should be greater than or equal to the public port. When the public port is set to a Single Port, the server port can only be set to a Single Port. When the public port is set to a Port Range, the server port can be set to a Single Port or a Port Range. And when the public port is set to a single port, all the port will be forwarded to ONE single port. Examples of different port forwarding settings: 1:1	Single Port
Public Port	<input type="text" value="Single Port"/> <input type="text" value="1001"/> (1~65534)
Server Port	<input type="text" value="Single Port"/> <input type="text" value="80"/> (1~65534)

Description	Default
N:1 Public Port <input type="text" value="A Port Range"/> 1001 - 1008 (1~65534) Server Port <input type="text" value="Single Port"/> 80 (1~65534)	
N:N Public Port <input type="text" value="A Port Range"/> 1001 - 1008 (1~65534) Server Port <input type="text" value="A Port Range"/> 1001 - 1008 (1~65534)	
Server IP Address	
Set up the server IP address that applies to the port mapping rule.	192.168.1.*

Common Service List for Port Forwarding			
Service name	Protocol	Starting Port	Ending Port
Customized	TCP, UDP, TCP/UDP	1~65534	1~65534
FTP	TCP	20	21
HTTP	TCP	80	80
ICUII	TCP	23566	23566
IP_PHONE	TCP	6670	6670
NetMeeting	TCP	1720	1720
News	TCP	119	119
PPTP	TCP/UDP	1723	1723
Telnet	TCP	23	23
Quakell/III	TCP/UDP	27960	27960
Real-Audio	TCP	6970	7170

3.3.4 Port Trigger

This page is used for setting up the port trigger, including configuring the Service Name, Service User, Service Type, Trigger Port, Protocol Role, Begin Port, End Port, and Status.

Port triggering is port forwarding with an on/off switch for the ports that have been forwarded. Have data flow out of a trigger port or not by enabling or disabling this functionality. Set up the time for the Port Trigger Timeout and click "Save" to save the setting.

Click the "Add ATrigger Rule" to add port trigger entries to the router.

🏠 FIREWALL > Port Trigger

Port Trigger Port Trigger Timeout Minute

ID	Service Name	Service Type	Inbound Connection	Service User	Status
----	--------------	--------------	--------------------	--------------	--------

After clicking the "Add A Trigger Rule", you will see the following page.

🏠 FIREWALL > Port Trigger

☰ Add A Trigger Rule

Service Name

Service User

Service Type

Trigger Port (1~65534)

Inbound Connection

Protocol Role

Begin Port (1~65534)

End Port (1~65534)

Status

Description	Default
Service Name	
Set up the service name for port triggering. The name is composed of letters, numbers and underline, starting with a letter or number. The maximum string length is 32 bytes.	N/A
Service User	
Select the service user to apply the port triggering rule.	Any Address
Service Type	
Set up the protocol type for port triggering.	TCP
Triggering Port	
Set up the triggering port. The port range is 1~65534.	N/A
Protocol Role	
Set up the protocol type for the inbound connection.	TCP/UDP

Description	Default
Begin port	
Set up the starting port for the inbound connection. The port range is 1~65534.	N/A
End Port	
Set up the ending port for the inbound connection. The port range is 1~65534.	N/A
Status	
Enable/disable the port triggering functionality.	Enabled

3.3.5 URL Filter

This page is used for setting up the URL Filter, including configuring the URL Address, LAN IP Address and Status.

URL Filter is used to block particular website from the local network. Select Enable/Disable to activate/deactivate this functionality. Click the "Add An URL Address" to block the URL.

[🏠 FIREWALL > URL Filter](#)

URL Address Filter

ID	URL Address	LAN IP Address	Status
----	-------------	----------------	--------

After clicking the "Add An URL Address", you will see the following page.

[🏠 FIREWALL > URL Filter](#)

☰ Add URL

URL Address

LAN IP Address

Status

Description	Default
URL Address	
Manually input the URL address that you'd like to block, for example www.baidu.com.	
LAN IP Address	
Set up the LAN IP address that you'd like to block. Options are "Any Address", "Single Address" and "Address Range".	Any Address
Status	
Enable/disable the URL Filter functionality.	Enabled

3.3.6 MAC Filter

This page is used for setting up the MAC Filter, including configuring the MAC Address, Device Name and Status.

MAC Filter is used to block particular MAC address from the local network. Select Enable/Disable to activate/deactivate this functionality. Click the "Add A MAC Address" to block the MAC Address.

[🏠 FIREWALL > MAC Filter](#)

MAC Filter Disable ▾ Save Add A MAC Address

ID	MAC Address	Device Name	Status
----	-------------	-------------	--------

After clicking the "Add A MAC Address" , you will see the following page.

[🏠 FIREWALL > MAC Filter](#)

☰ Add A MAC Address

MAC Address

Device Name

Status Enabled ▾

Save Back

Description	Default
MAC Address	
Manually input the MAC address that you'd like to block.	
Device Name	
Set up the device name corresponding to the set MAC address.	
Status	
Enable/disable the MAC Filter functionality.	Enabled

3.3.7 IP Filter

This page is used for setting up the IP Filter, including configuring the Source IP, Source Port, Destination IP, Destination Port, Protocol and Status.

IP Filter is used to block particular IP address from the local network. Select Enable/Disable to activate/deactivate this functionality. Click the "Add An IP Address" to block the IP Address.

[🏠 FIREWALL > IP Filter](#)

IP Filter Disable ▾ Save Add An IP Address

ID	Source IP Address Range	Source Port Range	Range Of Destination IP Address	Range Of Destination Port	Protocol	Status
----	-------------------------	-------------------	---------------------------------	---------------------------	----------	--------

After clicking the "Add An IP Address" , you will see the following page.

🏠 FIREWALL > IP Filter

☰ Add An IP Address

Source IP	<input type="text" value="Any address"/>
Source Port	<input type="text" value="Any address"/>
Destination IP	<input type="text" value="Any address"/>
Destination Port	<input type="text" value="Any address"/>
Protocol	<input type="text" value="TCP/UDP"/>
Status	<input type="text" value="Enabled"/>

Save

Back

Description	Default
Source IP	
Set up the source IP.	Any Address
Source Port	
Set up the source port where the datagram came from.	Any Address
Destination IP	
Set up the destination IP.	Any Address
Destination Port	
Set up the destination port where the datagram is going to.	Any Address
Protocol	
Set up the protocol type for the IP Filter.	TCP/UDP
Status	
Enable/disable the URL Filter functionality.	Enabled

3.4 VPN

You can set up the configuration of VPN in this function, device support IPSec, OPENVPN, PPTL, L2TP and GRE VPN. This function also provides certificate management and VPN log download.

3.4.1 IPSec

This page is used for set up the parameters of the IPSec VPN. Currently system support IPSec client mode only.

🏠 VPN > IPsec Setting

☰ Connection Management

NAT Traversal:

Enabled ▾

Save

Name	Enabled	Status	Local Interface	Local Subnet	Peer Subnet	Operation
------	---------	--------	-----------------	--------------	-------------	-----------

Add

🏠 VPN > IPsec Setting

☰ IPsec Setting

Name:	<input type="text"/>	Enable:	False ▾
IPsec Type:	Net-to-Net ▾	IPsec Role:	Client ▾
Local WAN Interface:	WAN ▾	Peer WAN Address:	<input type="text"/>
Local Subnet:	<input type="text"/> / <input type="text"/>	Peer Subnet:	<input type="text"/> / <input type="text"/>
Local ID:	<input type="text"/>	Peer ID:	<input type="text"/>

☰ Phase1

IKE Encryption:	3DES ▾	IKE Integrity:	MD5 ▾
IKE DH Group:	Group2(1024) ▾	IKE Lifetime:	120 (120-86400sec.)

☰ Phase2

ESP Encryption:	3DES ▾	ESP Integrity:	MD5 ▾
PFS:	Enabled ▾	ESP Keylife:	120 (120-86400sec.)
DH Group:	Group2(1024) ▾		

☰ Advanced

Negotiation Mode:	Main Mode ▾	IP Compress:	Enabled ▾
DPD Detection:	Enabled ▾	Time Interval:	60 (Sec.)
Timeout:	60 (Sec.)	DPD Action:	Hold ▾

☰ Authentication

- Use A Pre-Shared Key:
- Use The X.509 Cert:

Add

Cancel

Description	Default
Name	
Input the name of IPSec connection, it cannot be repeated with other connection's name. Name can be up to 20 characters long.	
Enable	
Enable or disable this connection.	False
IPSec Type	
Set up the working mode of the IPSec, currently support "Net to Net" only	Net-to-Net
IPSec Role	
Set up the role of the router in IPSec, currently support "Client" only	Client
Local WAN Interface	
Local end WAN interface, system will auto assign it base on connection status	WAN
Peer WAN Address	
IP/domain name of end opposite	
Local Subnet	
IPSec local protects subnet and subnet mask, i.e. 192.168.1.0/24	
Peer Subnet	
IPSec opposite end protects subnet and subnet mask, i.e.192.168.7.0/24;	
Local ID	
Local end identification, IP and domain name are available	
Peer ID	
Opposite end identification, IP and domain name are available	
IKE Encryption	
IKE phase encryption mode. Options are "3DES", "DES", "AES(128bit)" and "AES(256bit)"	3DES
IKE Integrity	
IKE phase integrity solution. Options are "MD5","SHA1" and "SHA2(256)"	MD5
IKE DH Group	
DH exchange algorithm. Options are "Group1(768)", "Group2(1024)", "Group5(1536)", "Group14(2048)", "Group15(3072)", "Group16(4096)", "Group17(6144)" and "Group18(8192)"	Group2(1024)
IKE Lifetime	
Set up IKE life time, current unit is second, range is 120~86400s	120
ESP Encryption	
ESP phase encryption mode. Options are "3DES", "DES", "AES(128bit)" and	3DES

Description	Default
"AES(256bit)"	
ESP Integrity	
ESP phase integrity solution. Options are "MD5" and "SHA1"	MD5
PFS	
Enable or disable PFS(Perfect Forward Secrecy)	Enabled
ESP Keylife	
Set up ESP life time, current unit is second, range is 120~86400s	120
DH Group	
DH exchange algorithm in ESP phase. Options are "Group1(768)", "Group2(1024)", "Group5(1536)", "Group14(2048)", "Group15(3072)", "Group16(4096)", "Group17(6144)" and "Group18(8192)"	Group2(1024)
Negotiation Mode	
Set up the mode of the IKE negotiation, Options are "Main" and "Aggressive"	Main
IP Compress	
Enable or disable IP Payload compression	Enabled
DPD Detection	
Enable or disable DPD detection	Enabled
Time Interval	
Set time interval of DPD detection, current unit is second	60
Timeout	
Set timeout of DPD detection, current unit is second	60
DPD Action	
Set the action when detect the connection is drop	Hold
Authentication	
Choose use share encryption option (PSK) or certificate authentication option. PSK can be up to 24 characters long; Certificate can be maintain by Certificate function	

3.4.2 OPENVPN

This page is used for set up the parameters of the OPENVPN. Currently system support OPENVPN client mode only.

🏠 VPN > OpenVPN

☰ Basic Settings

OpenVPN Mode	<input type="text" value="Client"/>		
OpenVPN Server	<input type="text"/>		
Port	<input type="text" value="1194"/>	Protocol	<input type="text" value="UDP"/>
Tunnel Device	<input type="text" value="TUN"/>	Encryption	<input type="text" value="Blowfish CBC"/>
Hash Algorithm	<input type="text" value="SHA1"/>	NsCertType Verification	<input type="text" value="Disable"/>
LZO Compression	<input type="text" value="Disable"/>	NAT	<input type="text" value="Disable"/>
Remote Subnet	<input type="text"/>	MTU	<input type="text" value="1500"/>
Remote Subnet Mask	<input type="text"/>	Tunnel UDP Fragment	<input type="text"/>
Connect Check Interval	<input type="text" value="60"/>	Connect Check Times	<input type="text" value="5"/>
TLS Cipher	<input type="text" value="Disable"/>		

☰ Authentication

Authentication	<input type="text" value="Pre-Shared Key"/>
Use A Pre-Shared Key	<input type="text"/>
Local IP	<input type="text"/>
Remote IP	<input type="text"/>

☰ Status

Connection Status Inactive

Description	Default
OPENVPN Mode	
Set up the working mode of the OPENVPN, options are "Disabled" and "Client"	Disabled
OPENVPN Server	
Set up the IP/Domain name of the OPENVPEN server	
Port	
Set up the listen port of OPENVPN client	1194
Protocol	

Description	Default
Set up the protocol type, options are “UDP” and “TCP”	UDP
Tunnel Device	
Set up the interface type, options are “TUN” and “TAP” TUN – Router mode TAP – Bridge mode	TUN
Encryption	
Set up the encryption mode, options are “Blowfish CBC”, “AES-128 CBC”, “AES-192 CBC”, “AES-256 CBC” and “AES-512 CBC”	Blowfish CBC
Hash Algorithm	
Hash algorithm provides a method of quick access to data, options are “SHA1”, “SHA256”, “SHA512” and “MD5”	SHA1
NsCertType Verification	
Enable or disable the function support ns certificate type	Disable
LZO Compression	
Enable or disable use LZO compression for data transfer	Disable
NAT	
Enable or disable Network Address Translation	Disable
Remote Subnet	
Set up remote subnet IP	
MTU	
Set up the Maximum Transmission Unit of the tunnel	1500
Remote Subnet Mask	
Set up remote subnet mask	
Tunnel UDP Fragment	
Set up MSS(Maximum Segment Size) of UDP, Range is 1~65536	
TLS Cipher	
Set up TLS(Transport Layer Security) encryption standard, options are “Disable”, “Enable”	Disable
Import TLS Auth Key	
Import the authority key of Transport Layer Security	
Authentication	
Set up authenticate method, options are “Pre-Shared Key”, “User/Password” and “certificate authentication”.	

3.4.3 PPTP

This page is used for set up the parameters of the PPTP VPN. Currently system support PPTP client mode only.

🏠 VPN > PPTP

☰ Basic Settings

PPTP Mode	<input type="text" value="Client"/>	
PPTP Server	<input type="text"/>	
User Name	<input type="text"/>	
Password	<input type="text"/>	<input type="checkbox"/> Unmask
Obtain IP	<input type="text" value="Auto"/>	
IP Address	<input type="text" value="0.0.0.0"/>	
Subnet Mask	<input type="text" value="255.255.255.0"/>	
Gateway	<input type="text" value="0.0.0.0"/>	
DNS	<input type="text" value="0.0.0.0"/>	
Authorization Mode	<input type="text" value="Auto"/>	
MPPE	<input type="text" value="Disabled"/>	
NAT	<input type="text" value="Disabled"/>	
MTU	<input type="text" value="1420"/>	(576-1420)
Connection Check Interval	<input type="text" value="60"/>	Sec(0 means not checked)
Connection Check Times	<input type="text" value="5"/>	
Connection Status	Inactive	

Description	Default
PPTP Mode	
Set up the working mode of the PPTP, options are “Disabled” and “Client”	Disabled
PPTP Server	
Set up the IP/Domain name of the PPTP server	

Description	Default
User Name	
Set up the username to login the PPTP server	
Password	
Set up the password to login the PPTP server	
Obtain IP	
Set up the method of obtain IP, options are "Auto" and "Manual" Auto – Obtain IP from PPTP server automatically Manual – assign IP address manual	Auto
IP Address	
PPTP Client IP address	
Subnet Mask	
PPTP Client subnet mask	
Gateway	
PPTP Client gateway address	
DNS	
PPTP Client DNS server address	
Authorization Mode	
Options are "Auto", "PAP" and "CHAP".	Auto
MPPE	
Enable or disable Microsoft Point-to-Point Encryption	Disabled
NAT	
Enable or disable Network Address Translation	Disabled
MTU	
Set up the Maximum Transmission Unit of the tunnel	1420
Connection Check Interval	
Set up the connection check interval. Check the connectivity, if the connection is lost, it will redial automatically, 0 indicating not to check the connectivity.	60
Connection Check Times	
Set up the connection check times, 0 indicating infinity. Once a disconnection is detected, the router will redial according to the set value in the Redial Times.	5
Connection Status	
Display the current connection status	

3.4.4 L2TP

This page is used for set up the parameters of the L2TP VPN. Currently system support L2TP client mode only.

🏠 VPN > L2TP

Basic Settings

L2TP Mode	<input type="text" value="Client"/>	
L2TP Server	<input type="text"/>	
User Name	<input type="text"/>	
Password	<input type="password"/>	<input type="checkbox"/> Unmask
Obtain IP	<input type="text" value="Auto"/>	
IP Address	<input type="text" value="0.0.0.0"/>	
Subnet Mask	<input type="text" value="255.255.255.0"/>	
Gateway	<input type="text" value="0.0.0.0"/>	
DNS	<input type="text" value="0.0.0.0"/>	
Authorization Mode	<input type="text" value="Auto"/>	
MPPE	<input type="text" value="Disabled"/>	
NAT	<input type="text" value="Disabled"/>	
MTU	<input type="text" value="1460"/>	(576-1460)
Connection Check Interval	<input type="text" value="60"/>	Sec(0 means not checked)
Connection Check Times	<input type="text" value="5"/>	
IPSec Encryption	<input type="text" value="Disable"/>	
Connection Status	Inactive	

Description	Default
L2TP Mode	
Set up the working mode of the L2TP, options are "Disabled" and "Client"	Disabled
L2TP Server	
Set up the IP/Domain name of the L2TP server	

Description	Default
User Name	
Set up the username to login the L2TP server	
Password	
Set up the password to login the L2TP server	
Obtain IP	
Set up the method of obtain IP, options are "Auto" and "Manual" Auto – Obtain IP from PPTP server automatically Manual – assign IP address manual	Auto
IP Address	
PPTP Client IP address	
Subnet Mask	
PPTP Client subnet mask	
Gateway	
PPTP Client gateway address	
DNS	
PPTP Client DNS server address	
Authorization Mode	
Options are "Auto", "PAP" and "CHAP".	Auto
MPPE	
Enable or disable Microsoft Point-to-Point Encryption	Disabled
NAT	
Enable or disable Network Address Translation	Disabled
MTU	
Set up the Maximum Transmission Unit of the tunnel	1460
Connection Check Interval	
Set up the connection check interval. Check the connectivity, if the connection is lost, it will redial automatically, 0 indicating not to check the connectivity.	60
Connection Check Times	
Set up the connection check times, 0 indicating infinity. Once a disconnection is detected, the router will redial according to the set value in the Redial Times.	5
IPSec Encryption	
Set up the encryption solution of L2TP. Options are "Disabled", "Use a Pre-Shared Key" and "Use the Certificate".	Disabled
Input The PSK	
Input the Pre-Shared Key. When IPSec Encryption setup to "Use a Pre-Shared	

3

Description	Default
Key”, it will display.	
Select The Certificate	
Select the Certificate user maintain it by Certificate function. When IPSec Encryption setup to “Use the Certificate”, it will display.	
IPSec Peer ID	
Input the peer ID of the IPSec	
Connection Status	
Display the current connection status	

3.4.5 GRE

This page is used for set up the parameters of the GRE VPN. User can create up to 10 GRE tunnels.

🏠 VPN > GRE

Add

Tunnel Number	Enabled	Status	Tunnel Interface Src IP/Mask	Tunnel Interface Dst IP/Mask	Peer Subnet	Operation
---------------	---------	--------	------------------------------	------------------------------	-------------	-----------

🏠 VPN > GRE

☰ Tunnel Setting

Tunnel Number

Enable Tunnel

Tunnel Interface Src IP/Mask /

Tunnel Interface Dst IP/Mask /

Tunnel Based Src IP

Tunnel Based Dst IP

Peer IP Address/Mask /

Tunnel Key (option,0-4294967295)

Connection Check Interval Sec.(0 means not checked)

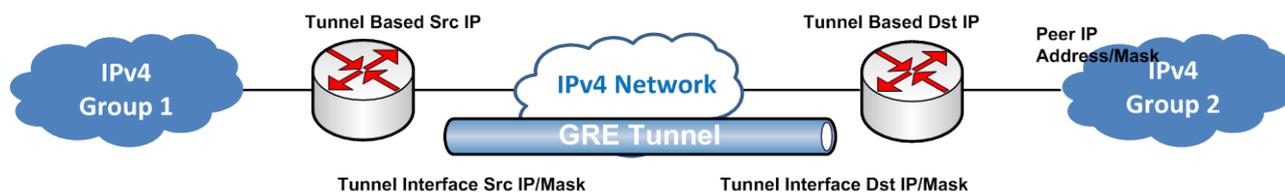
Connection Check Times

Save Cancel

Description	Default
-------------	---------

Description	Default
Tunnel Number	
Input the number as the name of this tunnel, it can not be repeated with other tunnel's name. Rang is 0-1023	
Enable Tunnel	
Enable or disable this tunnel.	Yes
Tunnel Interface Src IP/Mask	
The local tunnel IP address and mask	
Tunnel Interface Dst IP/Mask	
The remote tunnel IP address and mask	
Tunnel Based Src IP	
The Local WAN IP address	
Tunnel Based Dst IP	
The remote WAN IP address	
Peer IP Address/Mask	
The remote gateway local subnet IP and Mask	
Tunnel Key	
Input the secret key of the tunnel, number only, range is from 0 to 4294967296	
Connection Check Interval	
Set up the connection check interval. Check the connectivity, if the connection is lost, it will redial automatically, 0 indicating not to check the connectivity.	0
Connection Check Times	
Set up the connection check times, 0 indicating infinity. Once a disconnection is detected, the router will redial according to the set value in the Redial Times.	5

Network diagram as below:



3.4.6 Certificate

This page is used for user import the certificate which will use in IPSec or OPENVPN function.

🏠 VPN > Certificate Management

☰ Certificate Management

Group Name	CA	Public Cert	Private Cert	Expired Date	Operation
<input type="button" value="Add"/>					

🏠 VPN > Certificate Management

☰ Certificate Management

Group Name

Password

Import CA	<input type="text"/>	<input type="text"/>	<input type="button" value="选择文件"/> 未选择任何文件
Import Public Cert	<input type="text"/>	<input type="text"/>	<input type="button" value="选择文件"/> 未选择任何文件
Import Private Key	<input type="text"/>	<input type="text"/>	<input type="button" value="选择文件"/> 未选择任何文件
Import Peer Public Cert	<input type="text"/>	<input type="text"/>	<input type="button" value="选择文件"/> 未选择任何文件
Import CRL	<input type="text"/>	<input type="text"/>	<input type="button" value="选择文件"/> 未选择任何文件

Description	Default
Group Name	
Setup the name of cert group, it cannot be repeated with other cert group.	
Import CA	
Import CA certificate file	
Import Public Cert	
Import public certificate file	
Import Private Cert	
Import public certificate file	
Import Peer Public Cert	
Import peer end public certificate file	
Import CRL	
Import certificate revocation list	
Password	
Input the password about the certificate file if the file with a password	
Expired Date	
Show the expired date of the cert.	

3.4.7 VPN Log

This page is used for download specified VPN log. Select the VPN type and click “Download” to save the log to local.

VPN Setting VPN Log

VPN > VPN Log

VPN Log

Download the logs of VPN function to local PC. Specify logs of

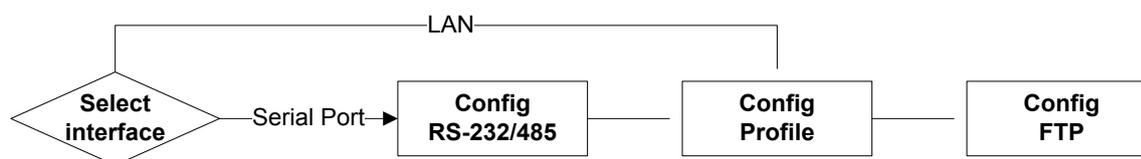
IPSec ▼

Download

3.5 Interface

This device can be used as data collector to gather data from slave via LAN port and serial port, user can set up the interface parameter by this function.

Config process as below normally.



3.5.1 RS232

RS232 (Recommended Standard - 232) is a telecommunication standard for binary serial communications between devices. You can set up the configurations for RS232, including Baud Rate, Data Bits, Stop Bits, Parity Bits and Flow Control.

SYSTEM > RS232 Configurations

RS232 Configurations

Working Mode	Master mode ▼
Baud Rate	9600 ▼
Data Bits	8 ▼
Stop Bits	1 ▼
Parity Bits	None ▼
Flow Control	None ▼
Modbus Mode	ModBus RTU ▼
Modbus Timeout	1000 (50~2000ms)
Retry Times	1 (1~10)

Save

Cancel

Description	Default
Working Mode	
Select the working mode for the current active serial port. <ul style="list-style-type: none"> ● Master mode: This mode is suitable for the DX-3001 to perform the read/write tasks on the open register of the Slave. ● Close: Disable this functionality. 	Close
Baud Rate	
Set up the baud rate for the serial port. Options are 2400, 4800, 9600, 19200, 38400, 57600 and 115200.	9600
Data Bits	
Set up the data bits for the serial port.	8
Stop Bits	
Set up the stop bits for the serial port. Options are 1 and 2.	1
Parity Bits	
Set up the parity bits for the serial port. Options are None, Odd and Even.	None
Flow Control	
Set up the flow control. Options are None, XON, XOFF, RTS, and CTS.	None
MODBUS Mode	
Set up the communication mode for the device.	MODBUS RTU
MODBUS Timeout	
Set up the timeout timer from 50ms to 2000ms. If the set value is out of range, it will be automatically changed to its maximum or minimum value.	1000ms

3.5.2 RS485

RS-485 (Recommended Standard - 485) is a telecommunication standard for binary serial communications between devices. You can set up the configurations for RS-485, including Baud Rate, Data Bits, Stop Bits, Parity Bits, and many more.

SYSTEM > RS485 Configuration

RS485 Configuration

Working Mode	Master mode ▼
Baud Rate	9600 ▼
Data Bits	8 ▼
Stop Bits	1 ▼
Parity Bits	None ▼
Modbus Mode	ModBus RTU ▼
Modbus Timeout	1000 (50~2000ms)
Retry Times	1 (1~10)

Save

Cancel

Description	Default
Working Mode	
Select the working mode for the current active serial port. <ul style="list-style-type: none"> ● Master mode: This mode is suitable for the DX-3001 to perform the read/write tasks on the open register of the Slave. ● Close: Disable this functionality. 	Close
Baud Rate	
Set up the baud rate for the serial port. Options are 2400, 4800, 9600, 19200, 38400, 57600 and 115200.	9600
Data Bits	
Set up the data bits for the serial port.	8
Stop Bits	
Set up the stop bits for the serial port. Options are 1 and 2.	1
Parity Bits	
Set up the parity bits for the serial port. Options are None, Odd and Even.	None
Flow Control	
Set up the flow control. Options are None, XON, XOFF, RTS, and CTS.	None
MODBUS Mode	
Set up the communication mode for the device.	MODBUS RTU
MODBUS Timeout	
Set up the timeout timer from 50ms to 2000ms. If the set value is out of range, it will be automatically changed to its maximum or minimum value.	1000ms

3.5.3 Profile Management

This page is used for setup the parameter about data collect. User can appoint the interface (RS-232/RS-485/LAN etc.) which will use to collect data, setup the file name which data will save to, and collect data from which address of the Slave

User can create up to 5 instances to collect data from Slave.

🏠 INTERFACE > Profile Setting

☰ Profile List

选择文件 未选择...文件

Import

Cancel

Profile ID	Profile Interface	Profile Enable	File Name	Operation
------------	-------------------	----------------	-----------	-----------

Add

🏠 INTERFACE > Profile Setting

☰ File Setting

Profile ID:

Interface: Profile Enable:

File Name Prefix: File Name:

File Name Postfix: Separation Sign:

☰ Interface Setting

Slave ID: Interval: (s)

☰ File Content

NO.	Item Name	Function Code	Start Addr	Count	Enable	
1		<input type="text" value="01"/>			<input type="text" value="True"/>	<input type="button" value="+"/> <input type="button" value="-"/>

Save

Cancel

RS-232 interface

🏠 INTERFACE > Profile Setting

☰ File Setting

Profile ID:

Interface: Profile Enable:

File Name Prefix: File Name:

File Name Postfix: Separation Sign:

☰ Interface Setting

Interval: (s)

☰ File Content

NO.	Slave ID	Item Name	Function Code	Start Addr	Count	Enable	
1			<input type="text" value="01"/>			<input type="text" value="True"/>	<input type="button" value="+"/> <input type="button" value="-"/>

RS-485 interface

🏠 INTERFACE > Profile Setting

☰ File Setting

Profile ID:

Interface: Profile Enable:

File Name Prefix: File Name:

File Name Postfix: Separation Sign:

☰ Interface Setting

Target IP Address: Port:

Interval: (s)

☰ File Content

NO.	Slave ID	Item Name	Function Code	Start Addr	Count	Enable	
1			<input type="text" value="01"/>			<input type="text" value="True"/>	<input type="button" value="+"/> <input type="button" value="-"/>

LAN.Modbus.TCP interface

🏠 INTERFACE > Profile Setting

☰ File Setting

Profile ID:

Interface: Profile Enable:

File Name Prefix: File Name:

File Name Postfix: Separation Sign:

☰ Interface Setting

Target IP Address: Port:

Read Community: Write Community:

Protocol: Time Out: (s)

Interval: (s)

☰ File Content

NO.	Item Name	OIDS	Enable
1			True <input type="button" value="+"/> <input type="button" value="-"/>

LAN.SNMP interface

Description	Default
Profile ID	
Setup instance ID, options are 01,02,03,04,05	01
Interface	
Setup the interface connect to Slave, options are "RS-232", "RS-485", "LAN.SNMP" and "LAN.Modbus.TCP.Master"	RS-232
Profile Enable	
Enable or disable this instance	False
File Name Prefix	
Set the prefix name of the data file.	
File Name	
Set the name of the data file	rawData
File Name Postfix	
Set the postfix name of the data file.	
Separation Sign	
Set the sign to separate the file name, for example "_", then the file name will be "prefix_file name_postfix.csv"	_

	Description	Default
RS-232/ RS-485/ LAN.Modbus.TCP. Master	Target IP Address (only for LAN.Modbus.TCP.Master)	
	Set up the IP address of the Slave	
	Port (only for LAN.Modbus.TCP.Master)	
	Set up the port of the Slave. Ranging from 1 to 65535	502
	Interval	
	Set up the time for scan interval. Ranging from 10s to 86400s.	300s
	Slave ID	
	Set up the corresponding slave communication port. Ranging from 1 to 255.	
	Item Name	
	Set up the name of this data item	
	Function Code	
	Set up the Modbus function code, options are 01,02,03,04	01
	Start Addr.	
	Set up the slave starting address (decimal) for read/write the registers. Ranging from 0 to 65535	
	Count	
	Set up how many registers will be read continuous from start address. Ranging from 1 to 255	
	Enable	
Enable or disable this setting		
Operation		
 Click it to add a new setting		
 Click it to delete the setting		
LAN.SNMP	Target IP Address	
	Set up the IP address of the Slave	
	Port	
	Set up the port of the Slave. Ranging from 1 to 65535	161
	Read Community	
	Set up the read community of SNMP	public
	Write Community	
Set up the write community of SNMP	private	

Description		Default
Protocol		
Set up the version of SNMP are supported		V2
Time Out		
Set up time out of the connection, Ranging from 0 to 120s		60s
Interval		
Set up the time for scan interval. Ranging from 10s to 86400s.		300s
Item Name		
Set up the name of this data item		
OIDs		
Set up which OID (Object Identifier) user intends to gather data from.		
Enable		
Enable or disable this setting		
Operation		
 Click it to add a new setting		
 Click it to delete the setting		

**Notice**

DX-3001 support to gather data from Slave by the SNMP V1/V2 protocol , however, does not support the user through the SNMP to manage DX-3001

3.5.4 FTP/SFTP Server

After the system collects the data and save to file, it can be upload to specified server by FTP/SFTP. Users can config the related parameter of the FTP/SFTP here.

🏠 INTERFACE > FTP/SFTP Server Setting

FTP/SFTP Server

Upload Mode	<input type="text" value="FTP"/>	
Target Server	<input type="text"/>	(IP or domain name)
Port	<input type="text" value="21"/>	
File Path	<input type="text" value="/"/>	
Account	<input type="text" value="deltauser"/>	
Password	<input type="password" value="....."/>	<input type="checkbox"/> Unmask

Save

Cancel

Description	Default
Upload Mode	
Set the method of the data upload to server, options are FTP and SFTP	Disabled
Target Server	
Set up the FTP/SFTP server IP/domain name	
Port	
Set up the listen port of server	
File Path	
Set up the file save path in server	/
Account	
Set up the FTP/SFTP account	
Password	
Set up the FTP/SFTP password	

3.6 System

You can set up the system configurations, including the User and device Management, Time Configurations, Firmware Upgrade, Backup & Restore, System Reboot, SD Card, and Network Diagnosis.

3.6.1 Name and Password

This page is used for reset router name and change the administrator password. The password must be a combination of 5 to 12 characters, numbers and/or underline symbols.

SYSTEM > Administrator Password

Device Name Setting

Device Name

Change Administrator Password

Old Password

New Password

The password must be a combination of 5 to 12 characters, numbers and underline marks

Confirm Password

Description	Default
Device Name	
Input the new name of this router.	DX3001 + “_” + “the last four digits of Mac”
Old Password	
Input the original password of admin.	admin
New Password	
Input the new password you’d like to use. The password length should be 5-12 digits and is composed of lowercase letters, uppercase letters (case sensitive), numerals 0-9 and underline.	N/A
Confirm Password	
Again input the password you’d like to use to double confirm there is no typo.	A/A

3.6.2 NTP Server

This page is used for set the NTP server to synchronizing router clocks over network. Use the dropdown list to select the server or manual input server IP/domain.

🏠 SYSTEM > Time Settings

The current time of device 2016-05-19 09:38:56

NTP Server:

Save

Cancel

Description	Default
The current time of device	
Here shows the current time of your device.	N/A
NTP Server	
Select the operating time zone of your device: GMT-12:00 - GMT+13:00.	N/A
Main NTP Server	
Manual input the primary NTP server Domain/IP when “Others” was selected	N/A
Backup NTP Server	
Manual input the secondary NTP server Domain/IP when “Others” was selected	N/A

3.6.3 Firmware Upgrade

This page is used for upgrading the system.

🏠 SYSTEM > Software Upgrade Settings

☰ System Upgrade

DO NOT turn off the power supply or reboot the device during the upgrade process. Please select the correct firmware package which is consistent with the device model, otherwise the device may be damaged !

(Before upgrade the firmware, please backup the settings and data. Please contact the local dealers or manufacturers when failed to upgrade the firmware)

Select Firmware 未选择任何文件

Upgrade

Cancel

Description	Default
Chose file	
Click “Choose file” to select the new firmware file.	N/A
Upgrade	
Click “Upgrade” to upgrade firmware. The device will reboot after the upgrade is done.	N/A

3.6.4 Backup & Restore

This page is used for backing up and restoring the configurations.

🏠 SYSTEM > Backup & Restore

☰ Backup & Restore

Device configurations can be backed up and saved to local PC

Backup

Configuration restoration will remove the current settings in the device and restore the configurations in your .cfg file

Select .Cfg File

Browse...

Restore

Configurations will be reset to the factory default settings, device will be reboot after the reset

Reset To Factory Default

Description	Default
Backup	
Click "Backup" to save the device configurations on your computer.	N/A
Restore	
Click "Chose file" to select the backup file and then click "Restore" to restore the configurations. The device configuration will be restored to the previous version and the device will reboot after the restoring is done.	N/A
Restore To Factory Default	
Click "Restore To Factory Default" to reset the configurations to the factory defaults. The device will reboot after the reset is done.	N/A

3.6.5 System Reboot

This page is used for manually rebooting the system. Click "Restart Device" and the system will reboot.

🏠 SYSTEM > System Reboot

☰ System Reboot

The network will be temporarily shut down during system reboot, please wait!

Restart Device

3.6.6 SD Card

This page is used for manage SD card.

🏠 SYSTEM > SD Card

☰ SD Card Setting

Storage Limit

 %

Save

☰ Format SD Card

Format the SD card, the data will be completely removed!

Format SD Card

Description	Default
Storage Limit	
Set the storage usage limitation of the SD card. The oldest data will be overwriting when the storage usage matches the configured value	90%
Format SD Card	
Click on the button to perform formatting SD card	N/A

3.6.7 Network Diagnosis

This page is used for diagnosing the network status; methods are Ping Test and Route Trace.

🏠 SYSTEM > Network Diagnosis

☰ Network Diagnosis

Diagnosing Method

Ping Test ▼

Host Name/IP Address

Start

Description	Default
Diagnosing Method	
Select the Diagnosing Method; options are Ping Test and Route Trace.	Ping Test
Host Name/IP Address	
Input the Host Name or the IP Address.	N/A
Start	
Click "Start" to start the network diagnosing. While running the network diagnosing, the settings cannot be changed.	N/A