Smarter. Greener. Together.

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-020BD20-02

2020-05-14

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

DX-3001**H9**-V **Industrial 3G/WAN VPN Router User Manual**

www.deltaww.com

Smarter. Greener. Together.

DX-3001H9-V Series
Industrial 3G/WAN VPN Router
User Manual

Revision History

Version	Revision	Date
1st	The first version was published.	2016/10/21
2nd	1. Chapter 3: Add new functions of Auto Detect/Dial Failure to Restart/Detect interval/WAN Backup/WAN Check Interval in section 3.2.1. 2. Add new function of PIN Management in section 3.2.4. 3. Add new function of Remote Web Manage Setting in section3.3.8.	2020/5/14

DX-3001H9-V Industrial 3G/WAN VPN Router User Manual

Table of Contents

1

Chapter 1 Product Introduction

Table of Contents

1

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

DX-3001H9-V is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility of Radio and Telecom device (1995/5/EC). For the evaluation regarding the Directives, the following standards were applied:

Test Items :

---EMC
EN 301 908-1 V7.1.1(2015-03)
EN 301 511 V12.1.1(2015-06)

---Radio
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)

---MPE
EN50385: 2002

---Safety
EN60950-1: 2006/A11:2009/A1:2010/A12:2011/A2:2013

EN 55022 Class A Warning:

Class A ITE is a category of all other ITE which satisfies the class A ITE limits but not the class B ITE limits.

The following warning shall be included in the instructions for use:

> **Notice**
>
> - This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

EN 55032 Class A Warning:

Class A ITE is a category of all other ITE which satisfies the class A ITE limits but not the class B ITE limits.

The following warning shall be included in the instructions for use:

Warning: This equipment is compliant with Class A of EN 55032. In residential environment this equipment may cause radio interference.

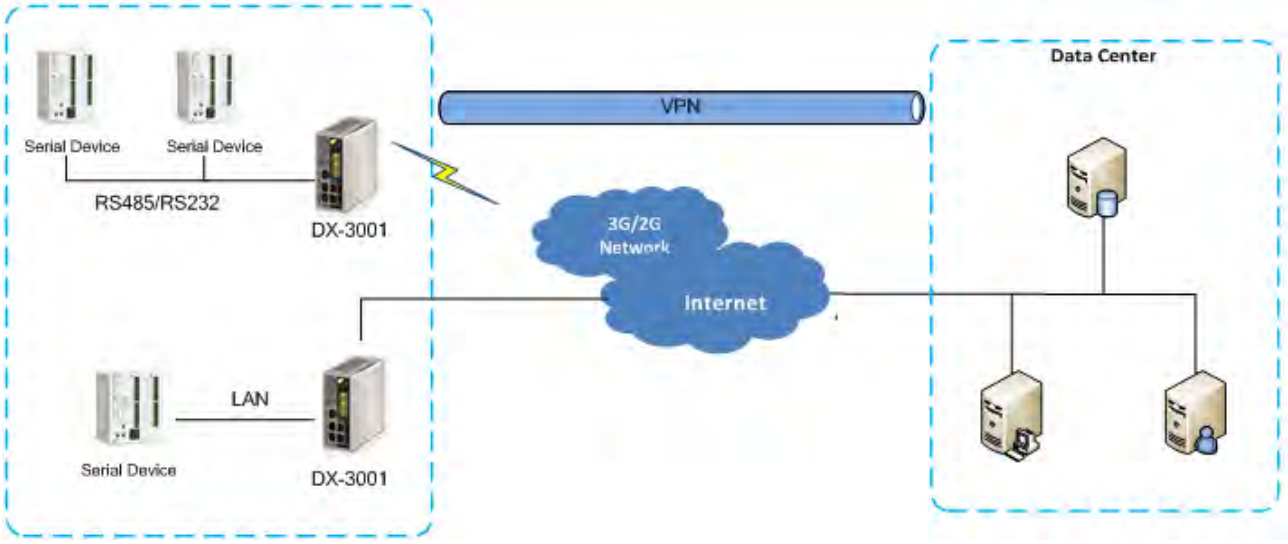
1.1 Product Overview

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.

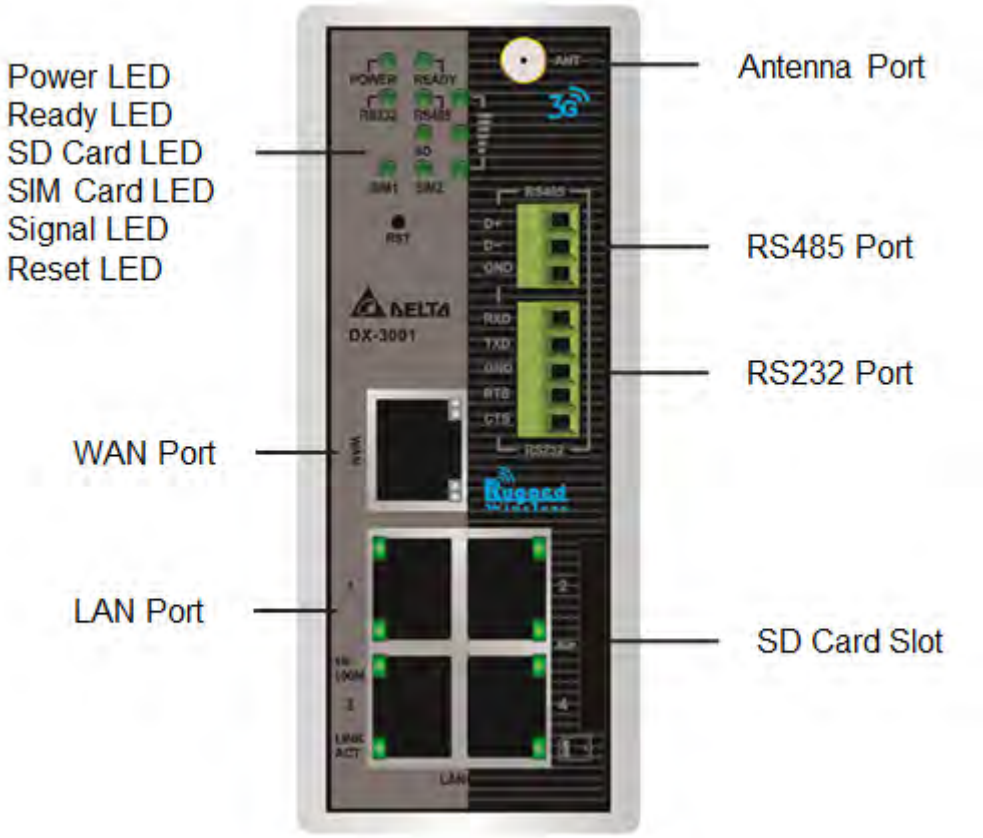
1.1.1 Network Design



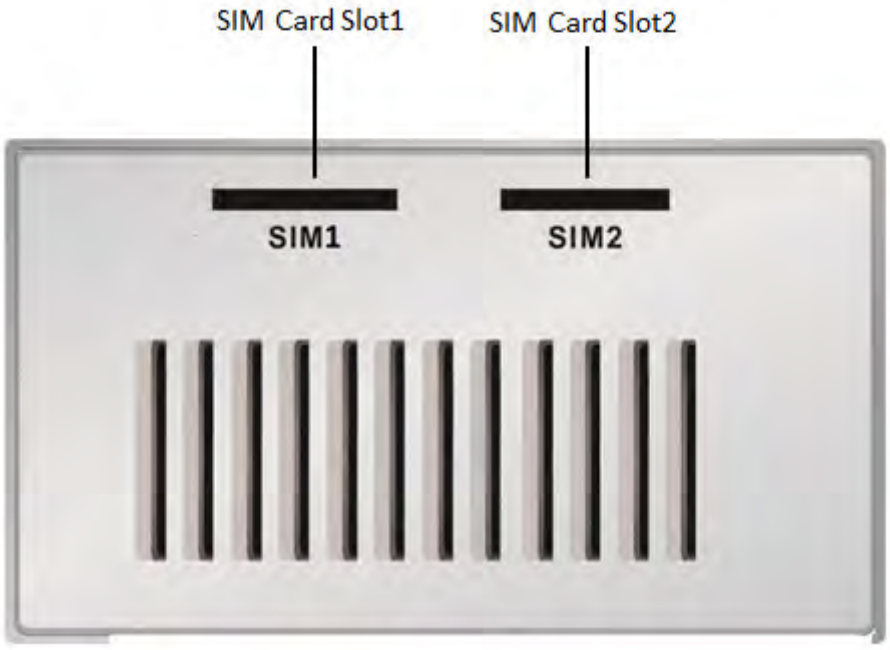
1.1.2 Features

- 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

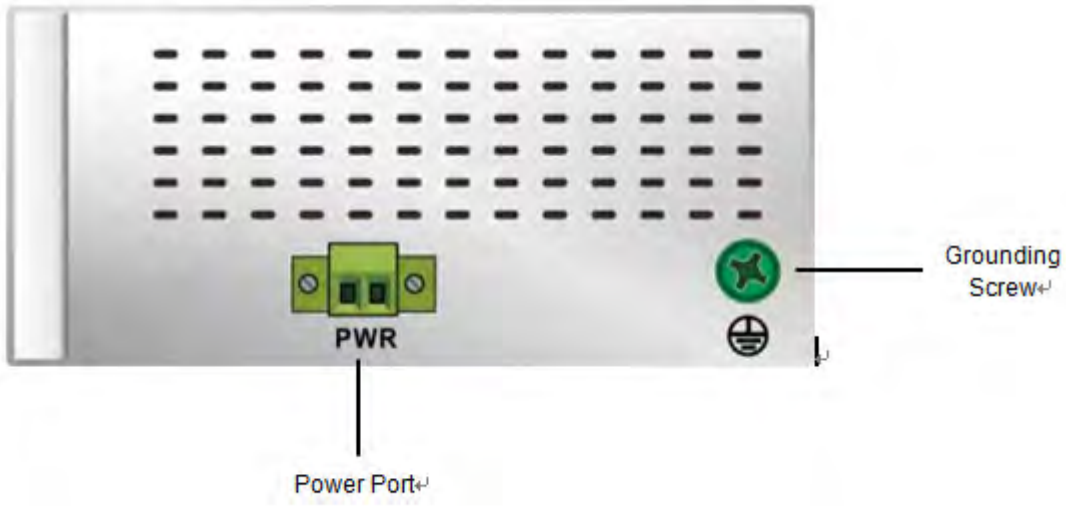
1.1.3 Front Panel Ports and LEDs



1.1.4 Top Panel



1.1.5 Bottom Panel

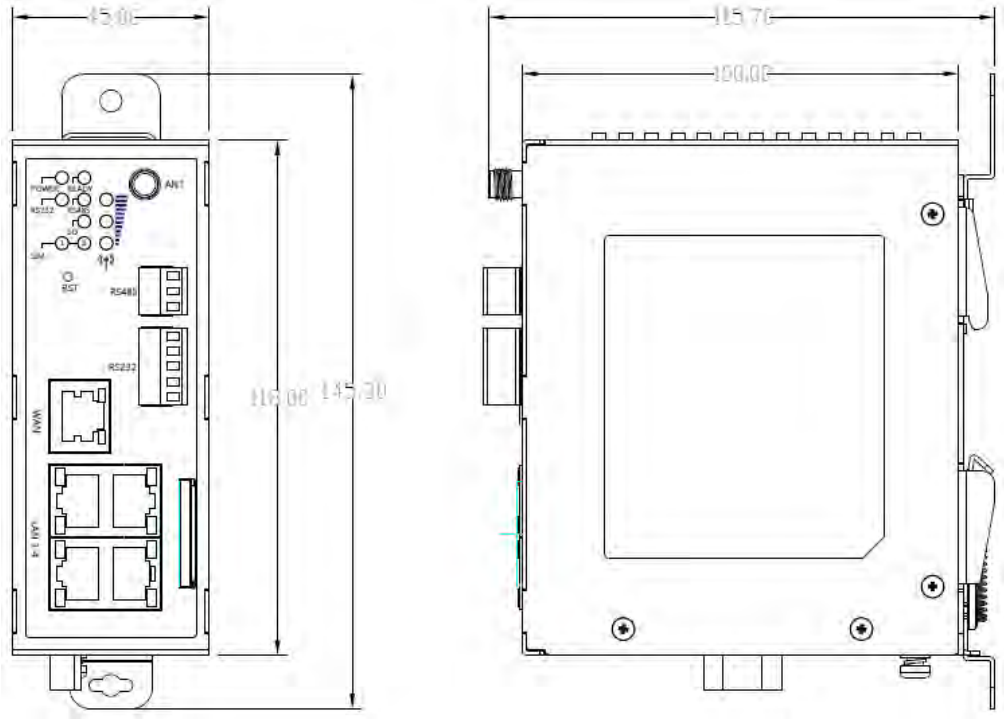


Notice

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

1.2 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.

2

Chapter 2 User Interface

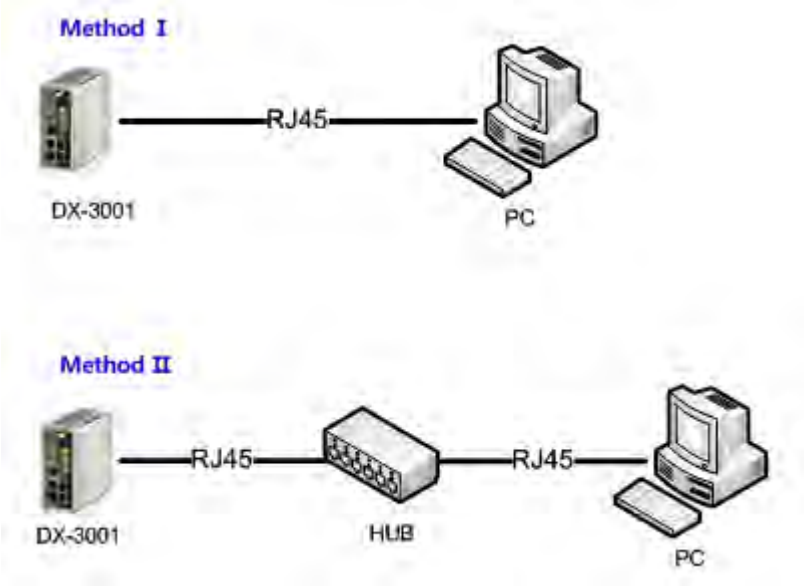
Table of Contents

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 intruitivly.

2.1.1 System Connection

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



2.1.2 Default IP Address/Account/Password

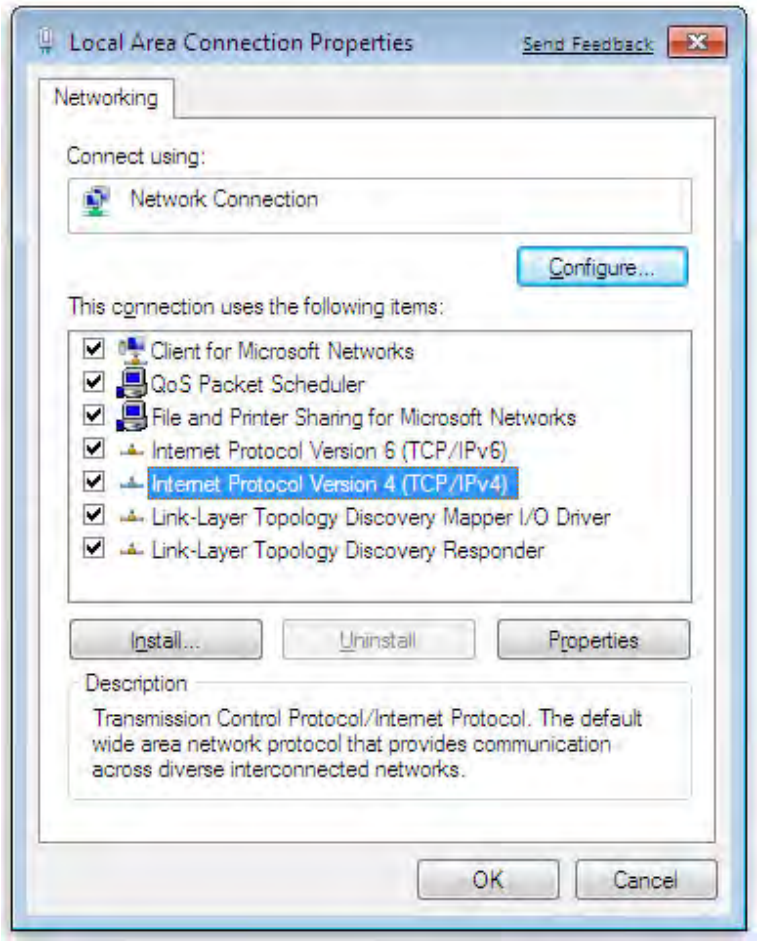
The default IP address of router is 192.168.1.1. The initial account and password is admin/admin

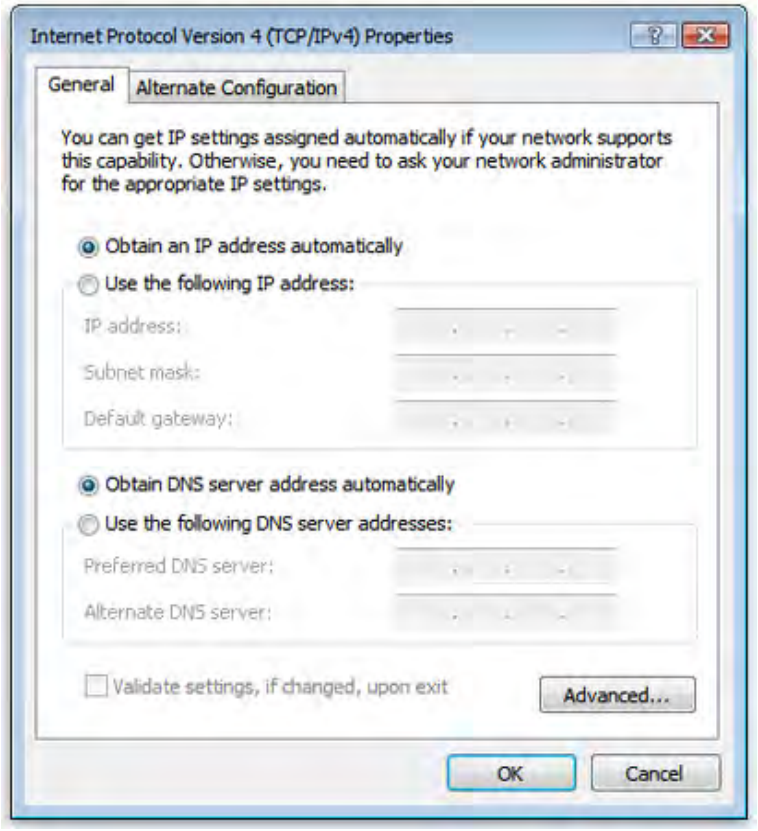
2.1.3 Local Network Setups

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

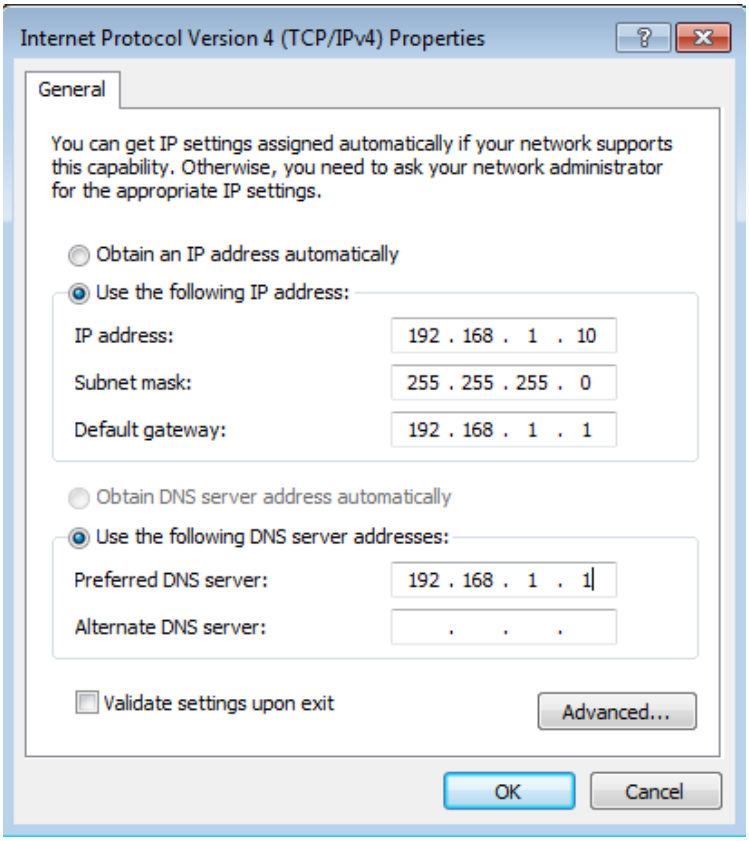

Local Area Connection Properties
Send Feedback
Networking
Connect using:
Network Connection
Configure...
This connection uses the following items:
Client for Microsoft Networks
QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings, if changed, upon exit
Advanced...
OK
Cancel

- **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.

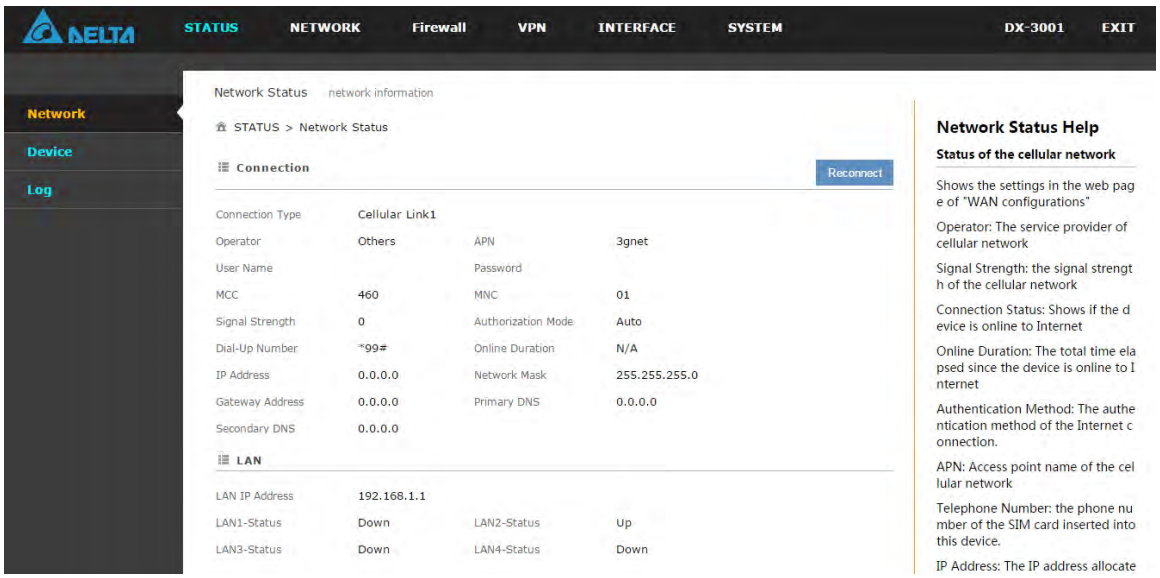


2.1.4 Logging in

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.



Notice

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

MEMO

3

Chapter 3 Functions

Table of Contents

3.1 Status

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

3.1.1 Network Status

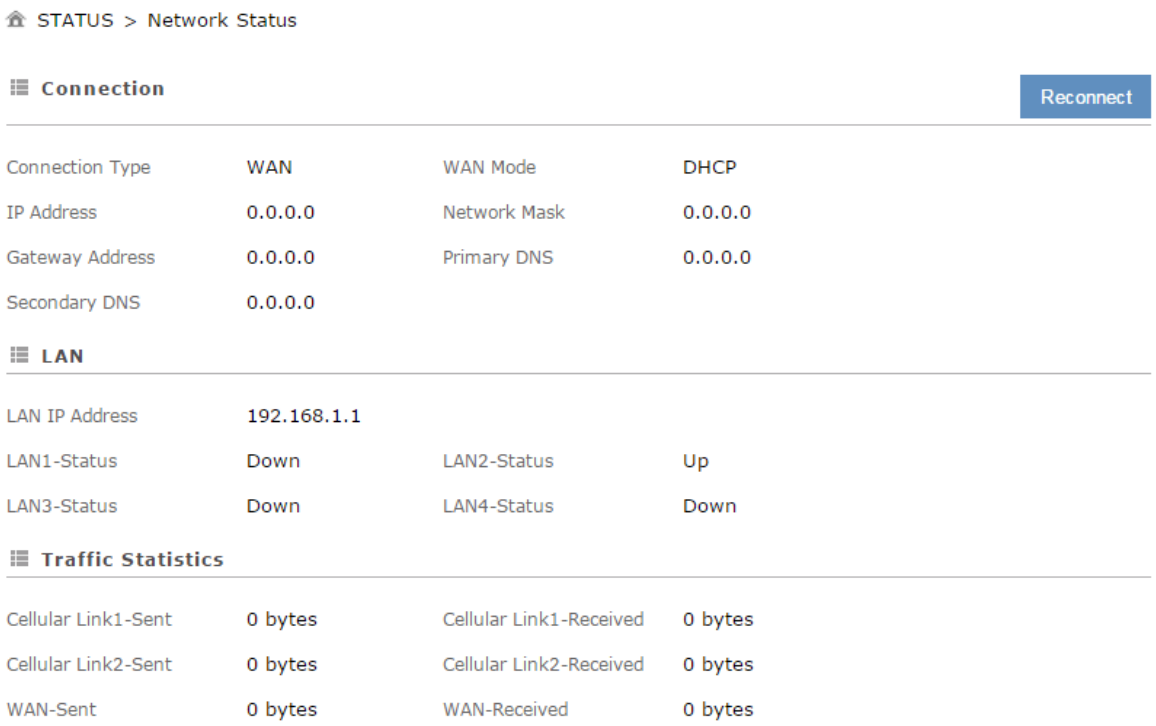
This page shows basic information on Network Status, LAN Status and traffic.

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, Signal Strength, Connection Status, Online Duration, Authorization Mode, APN, Telephone Number, IP Address Network Mask, Gateway Address, primary DNS, and Secondary DNS.

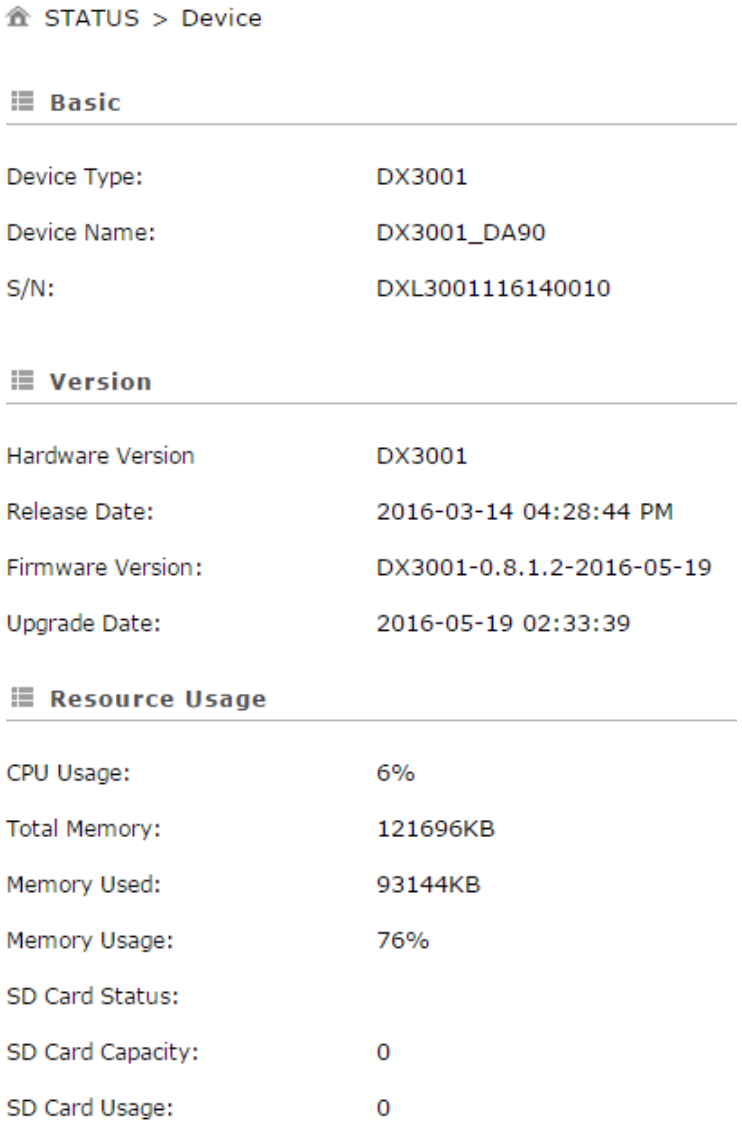
LAN includes the LAN IP Address, and connection status of 4 LAN port. Up means connected, down means disconnected.

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



3.1.2 Device

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



- 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

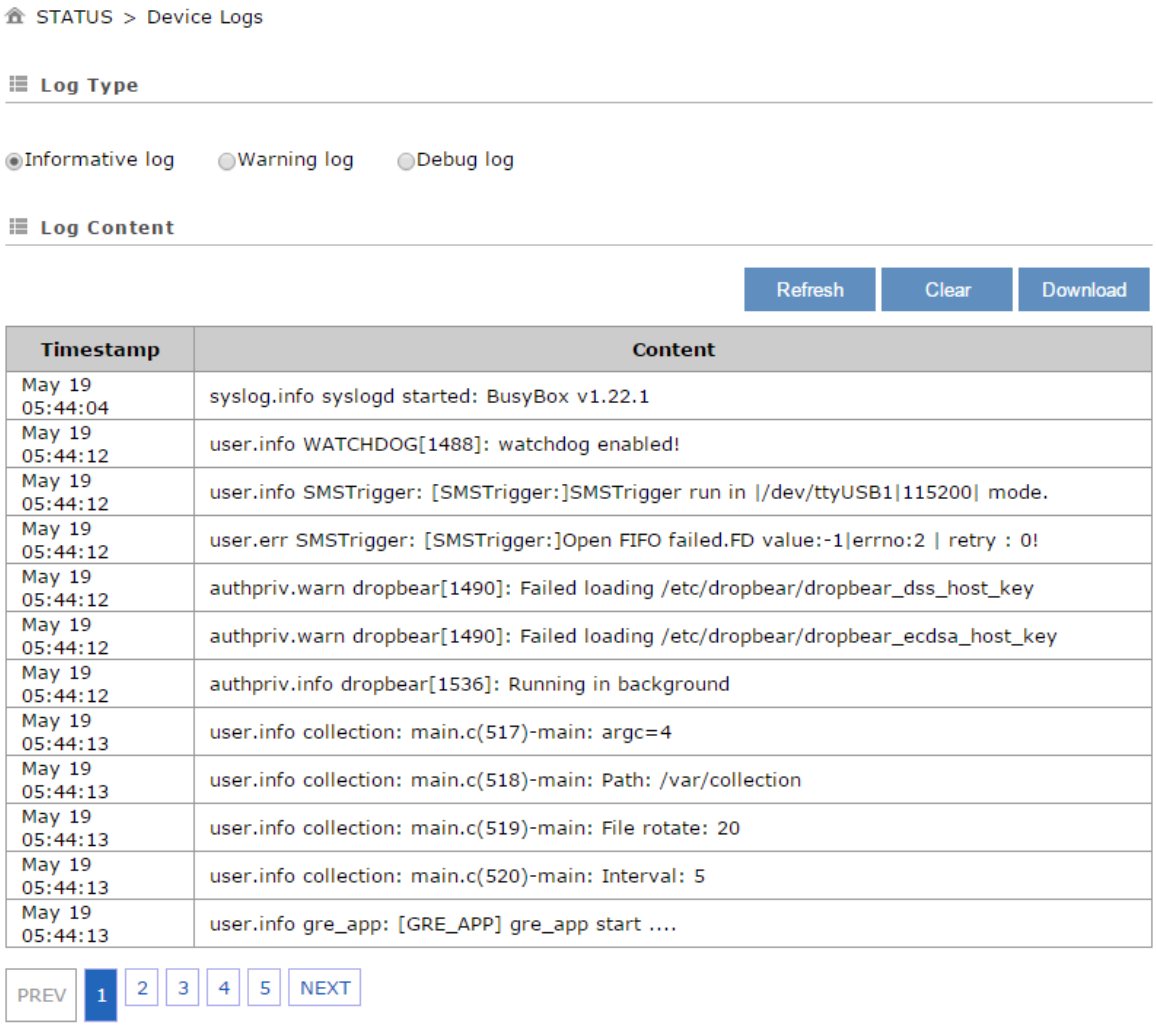
Item	Description
Hardware Version	Version number of the hardware currently used on the router
Release Date	Hardware release date
Current Version	Version number of the software currently used on the router
Upgrade Date	Upgrade time of the software currently used on the router

- 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 lot and the Debug log. You can use the buttons on the right hand side to refresh, clear or download the displayed logs.

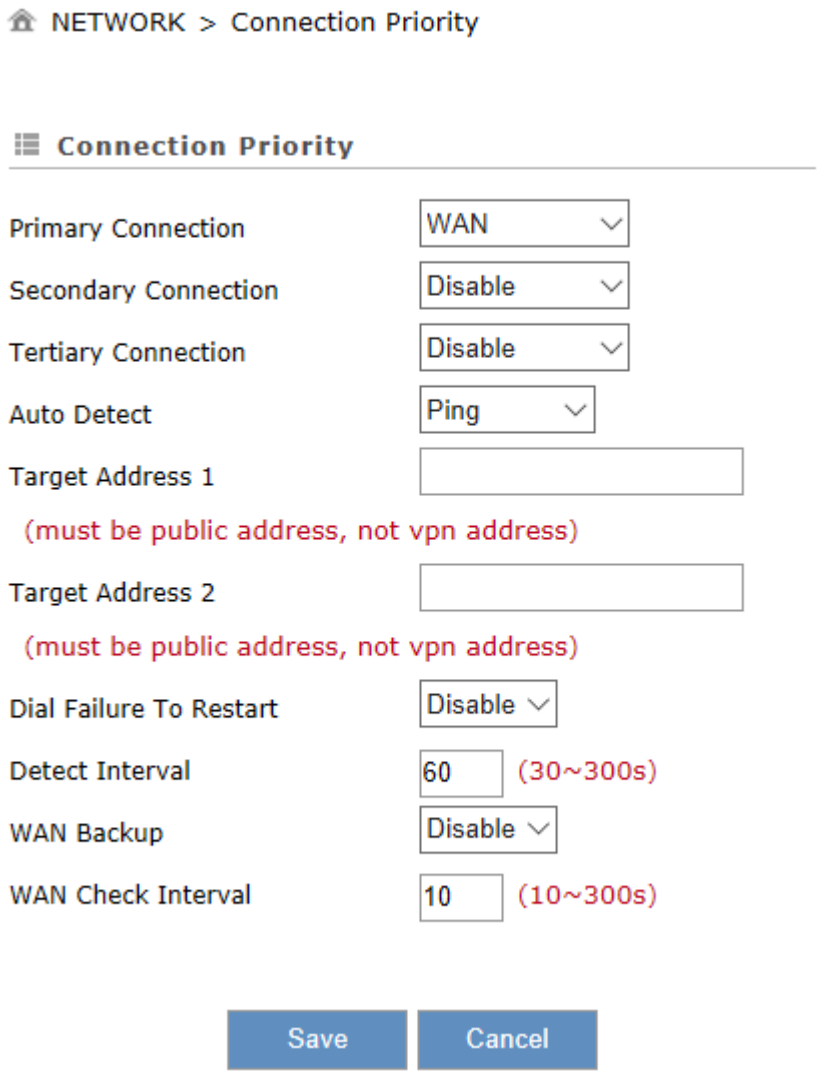


3.2 Network

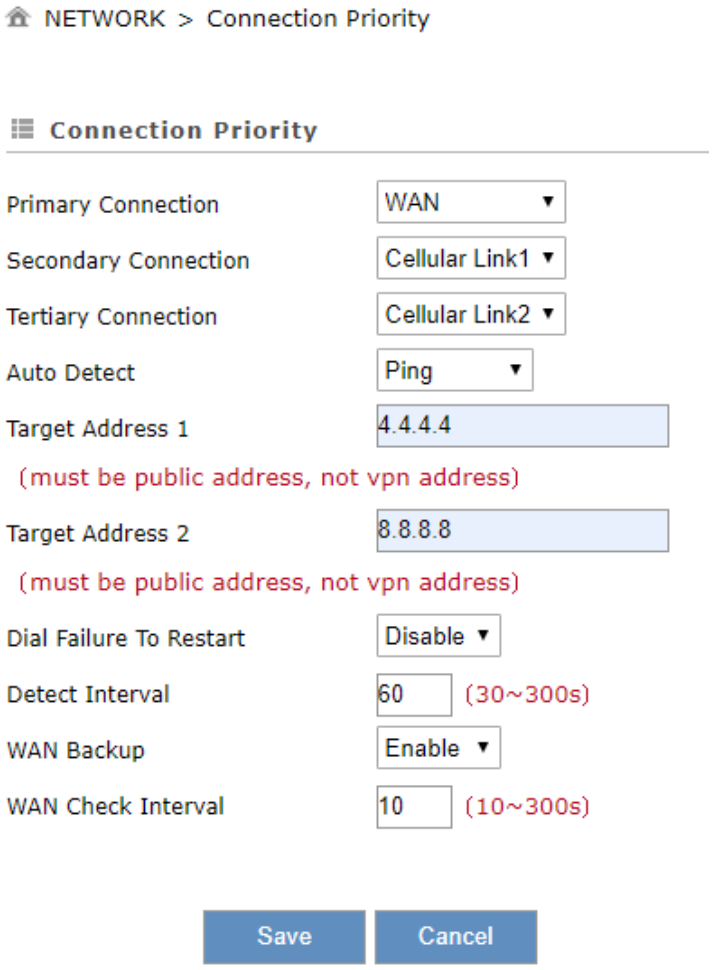
You can set up networks configuration, including the connection priority, Cellular network, WAN and LAN Configurations.

3.2.1 Connection Priority

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

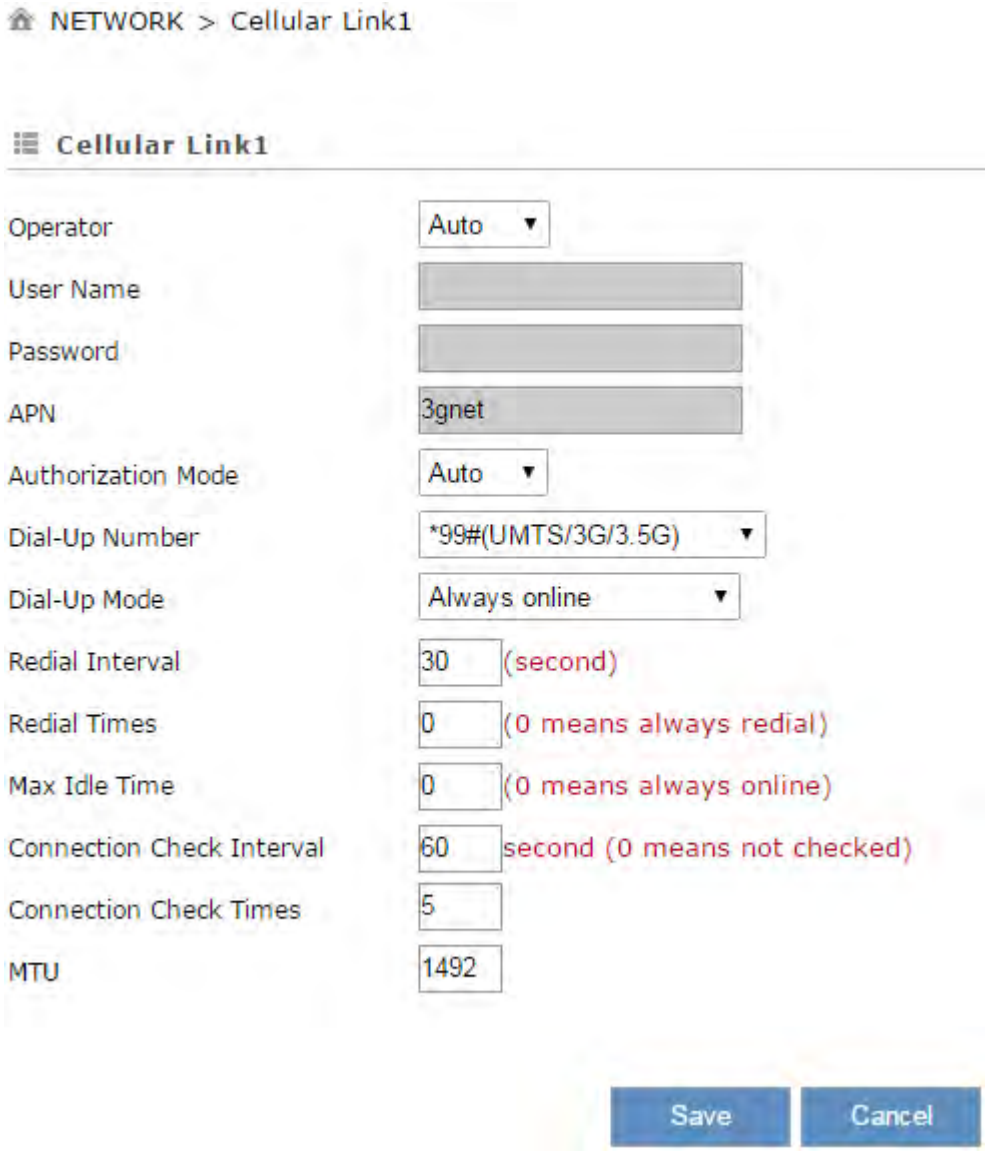


Description	Default
Primary Connection	
The first priority network interface connects to the Internet	WAN
Secondary Connection	
The second priority network interface connects to the Internet	Disable
Tertiary Connection	
Third priority network interface to connect to the Internet	Disable
Auto Detect	
● Enabled: The connection priority is enabled. Switch to the Secondary Connection automatically after the third failed attempt of testing on target address 1 and 2 with PING, FTP or SFP Ping during the Primary Connection. Switch to Tertiary Connection after another third attempt failed during the Secondary Connection. ● Disabled: The connection priority WON'T be enabled.	Disabled
Target Address 1	
Set the first IP of the server that program will do a ping testing. **Notice** ● Make sure the target IP address allows to be pinged. ● Does not support Domain Name input.	N/A
Target Address 2	
Set the second IP of the server that program will do a ping testing. **Notice** ● Make sure the target IP address allows to be pinged. ● Does not support Domain Name input.	N/A
Dial Failure To Restart	
DX devices will be restarted if the network connection has been continuously failed for 10minures with the Primary/ Secondary/ Tertiary Connection.	Disable
Detect Interval	
Set the retry interval for PING/ FTP/ SFTP connection testing. (Range: 30 to 300 sec.)	60s
WAN Backup	
Activated when the setting of Primary Connection is WAN. ● **Enable**: Even if the Secondary or Tertiary Connection is currently used for the loss of the Primary Connection. WAN will be forced to switch back to the Primary Connection after the recovery. ● **Disable**: The Secondary Connection or Tertiary Connection would still be activated after the Primary connection recovers.	Disable
WAN Check Interval	
Set the interval (30 to 300 sec.) for inspection of WAN connection status. (Range: 30 to 300 sec.)	10s

Operation Instruction	**Example: Activate WAN Backup** 1. Login to DX system. 2. Follow the path: Network -> Connection 3. Set Primary Connection as “WAN” 4. Set Secondary Connection as “Celluar1” 5. Set Tertiary Connection as “Celluar2” 6. Set Ping or FTP/ SFTP for Auto Detect. Input the target IP addresses. **Notice** ● Make sure the target IP address allows to be pinged. ● Does not support Domain Name input. 7. Set WAN Backup as “Enable” 8. Set WAN Check Interval as 10 seconds (Default setting is 10s) 9. Click “Save”
Illustration	

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.

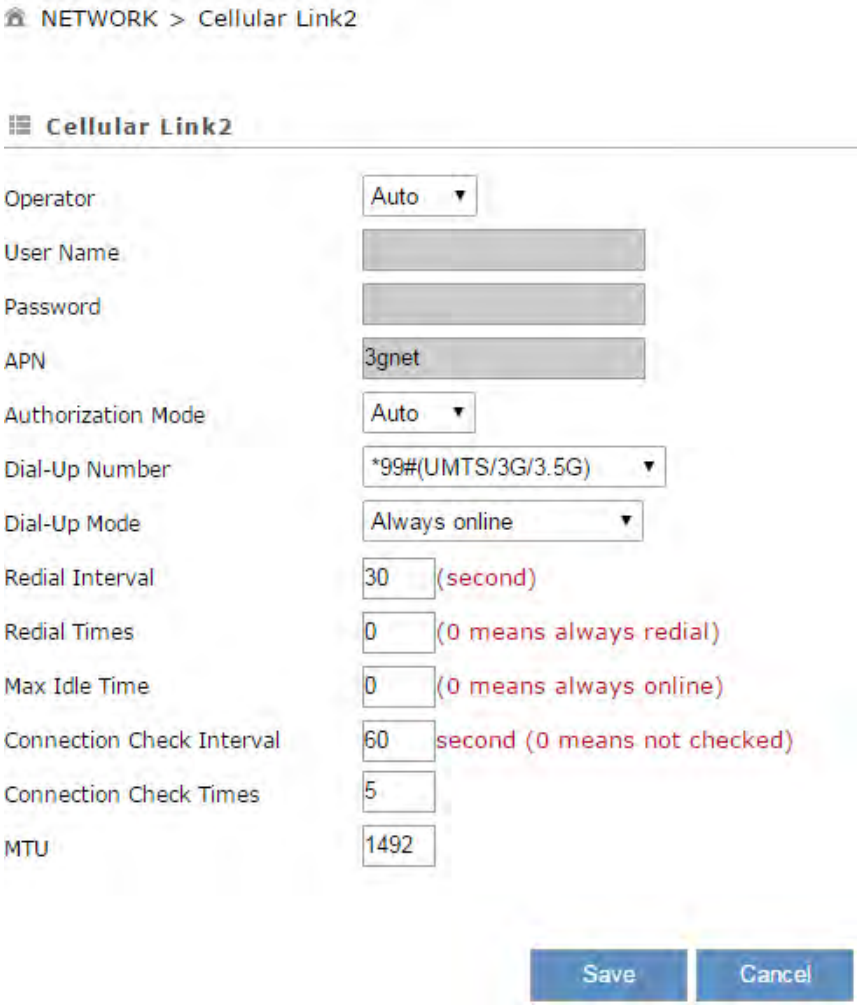


Description	Default
Operator	
Select Auto or Others for the Operator from the dropdown list. ● **Auto:** the system will detect the operator from the inserted SIM card and set up accordingly. ● **Others**: users can set up the operator manually.	AUTO
User Name	
This name is provided by the operator. When “Auto” is selected, the system will set the name up automatically and users cannot change the setting.	N/A
Password	

Description	Default
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 and users cannot change the setting.	*99#
Dial-Up Mode	
Options are : ● **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

3.2.3 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.

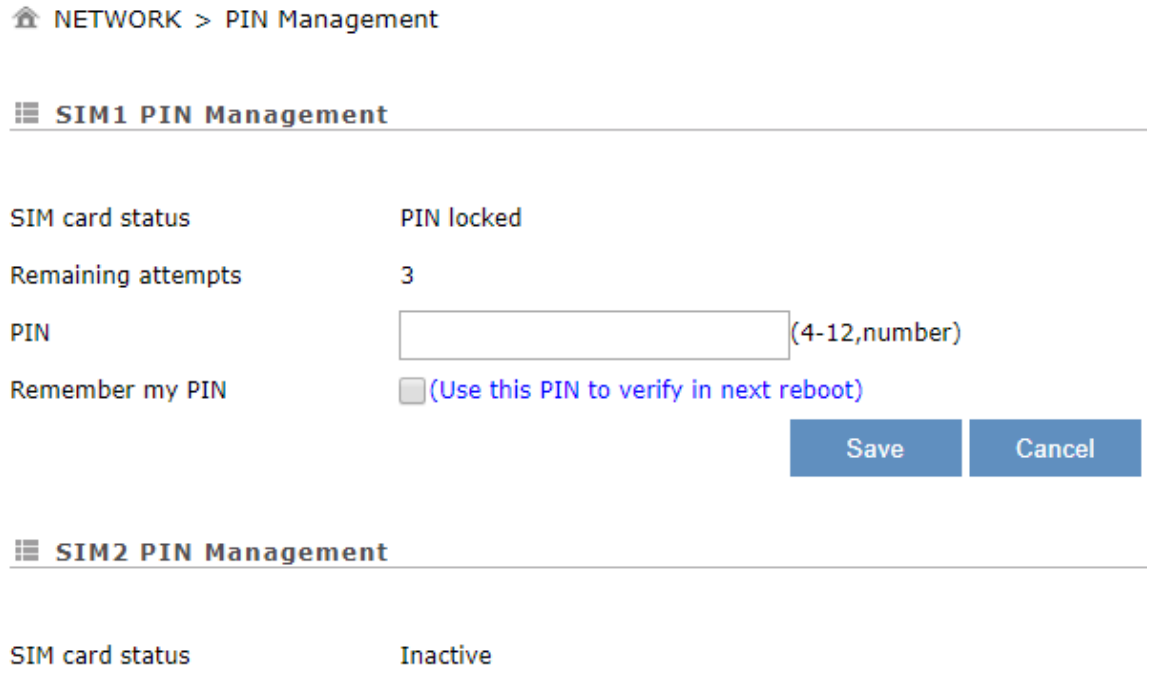


Description	Default
Operator	
Select Auto or Others for the Operator from the dropdown list. ● **Auto:** the system will detect the operator from the inserted SIM card and set up accordingly. ● **Others**: users can set up the operator manually.	AUTO
User Name	
This name is provided by the operator. 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 and users cannot change the setting.	*99#
Dial-Up Mode	
Options are : ● **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 PIN Management

Users can unlock SIM card locked by PIN code and save the code in DX device and check the PIN status.

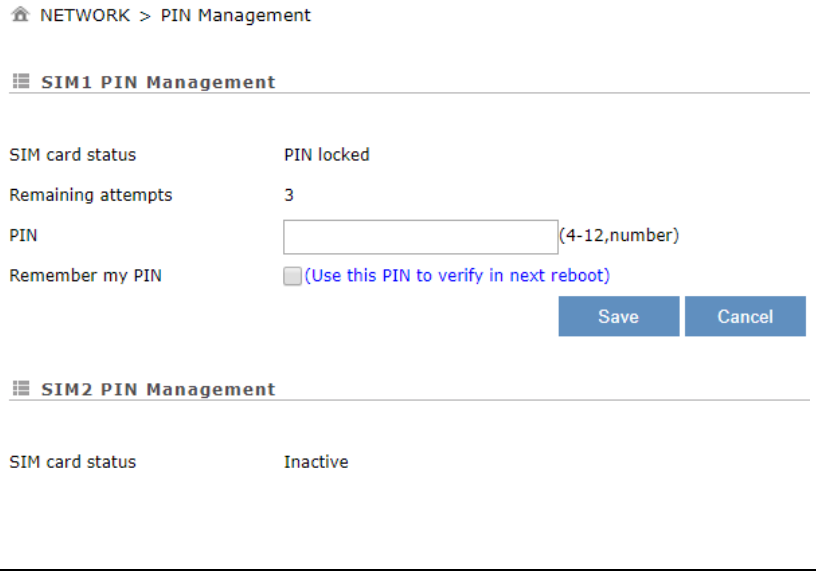


Description	Default
SIM card status	
● Inactive: SIM Card is inserted but communication module has not been activated. **Notice** ● DX3001 supports dual SIM with the condition that two SIM cards cannot be activated at the same time. ◦ ● No Sim: No SIM cards detected in the slot. ● Normal: SIM Card is inserted correctly and functions normally. ● PIN Locked: SIM Card is in the slot. Need the associated PIN code to function. ● PUK Locked: Exceed the maximum PIN code input tries. Need the correct PUK (Personal Unlocking Key) to unlock and resume normal operation.	N/A
Remaining attempts	
The allowable entry attempts is normally 3 times. When the remaining attempts is zero and the SIM card is locked, users must ask for help from operators or unlock it with PUK code.	3
PIN	
A personal identification number used in SIM card is a security measure to protect SIM card from being stolen.	N/A

Description	Default
Remember my PIN	
Enable this function to remember the PIN code in the system and the code would be input automatically every time after booting.	Uncheck

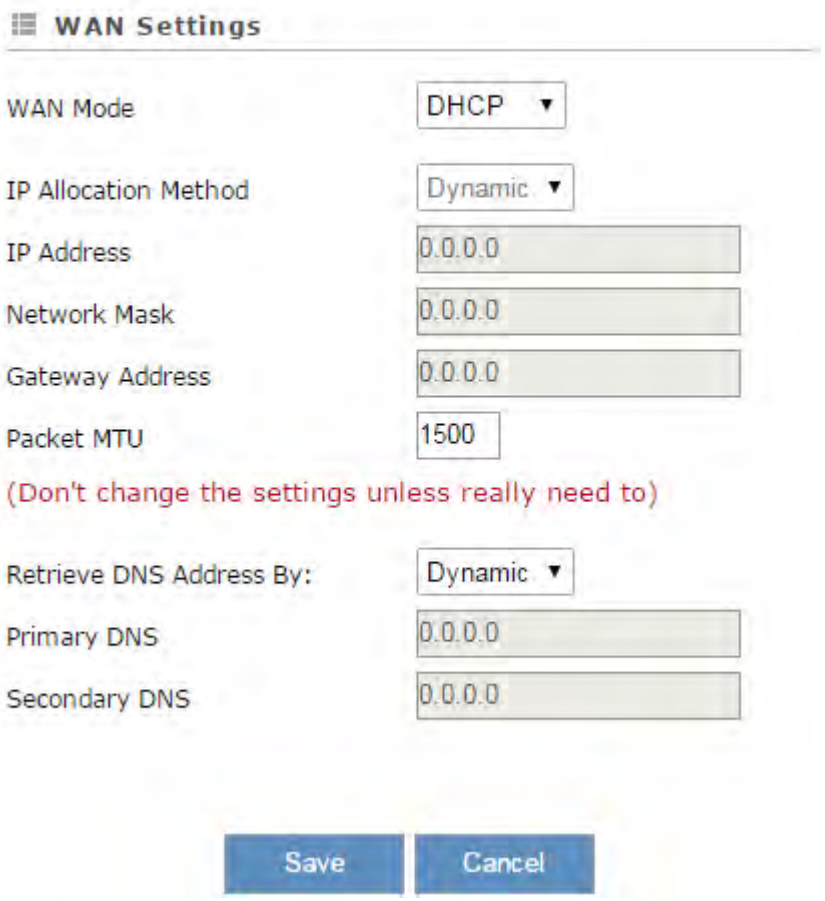
Notice

- If you enter the wrong PIN three times, your SIM card will be locked. Once SIM card is blocked, you will need PUK code to unlock it or find operator's help

Operation Instruction	**Example: Insert and unlock a PIN-locked SIM card** 1. Insert a SIM card locked by PIN codes into the SIM1 slot of the DX Shell. 2. Login to DX system. 3. Follow the path: Network -> PIN Management to access "SIM1 PIN Management". 4. Enter the correct PIN code. 5. Click "Save" and a "unlock successful" message would be displayed.
Illustration	

3.2.5 WAN Setting

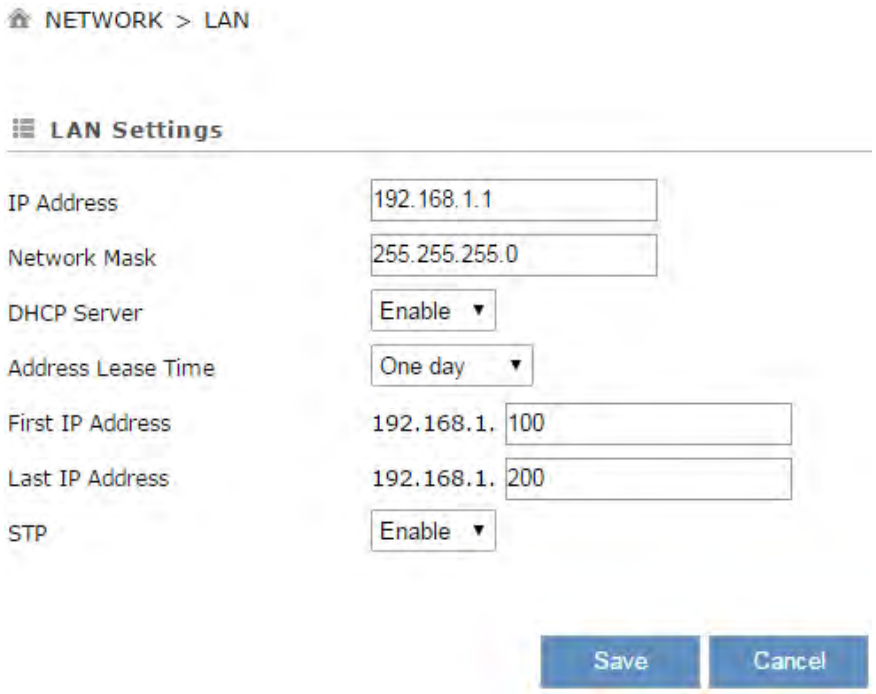
NETWORK > WAN



Description	Default
WAN Mode	
Your device can connect to the internet via the WAN port with a Dynamic IP or Static IP. ● 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. ● 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	
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	
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. DNS address can be retrieved by DHCP setup or manually set. ● 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

3.2.6 LAN

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



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	
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.

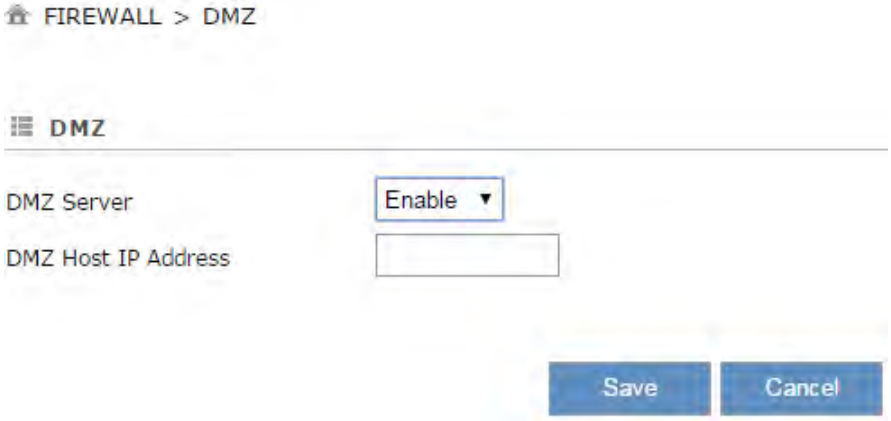
3.3.1 Basic

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.

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

3.3.2 DMZ

This page is used for setting up the DMZ server.



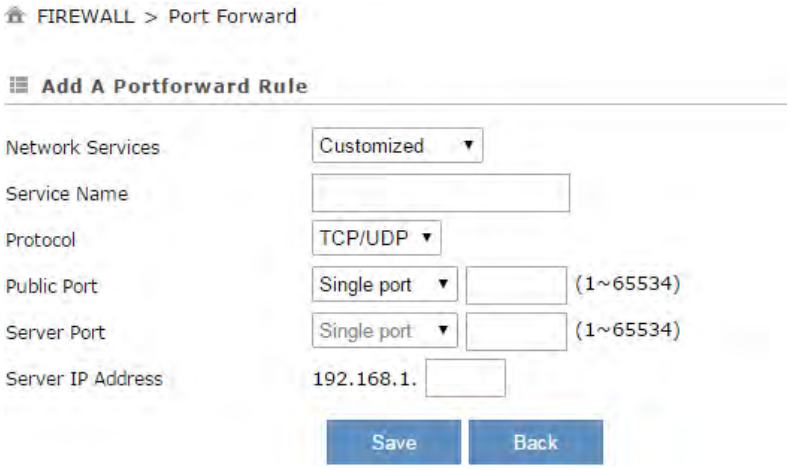
Description	Default
DMZ Server	
Demilitarized zone (DMZ) is a special segment of the local network reserved for servers accessible from the Internet, adding an additional layer of security.	Disable
DMZ Host IP Address	
Set up the IP address for the DMZ host.	N/A

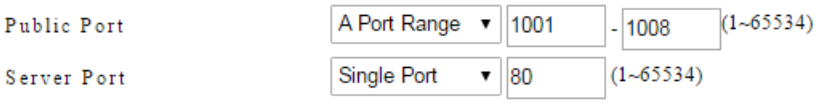
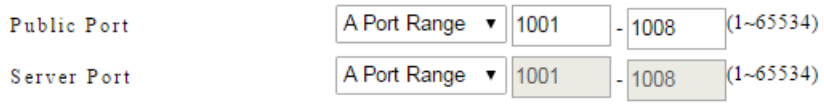
3.3.3 Port Forward

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.

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



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  N:1  N:N 	Single Port
Server IP Address	
Set up the server IP address that applies to the port mapping rule.	192.168.1.*

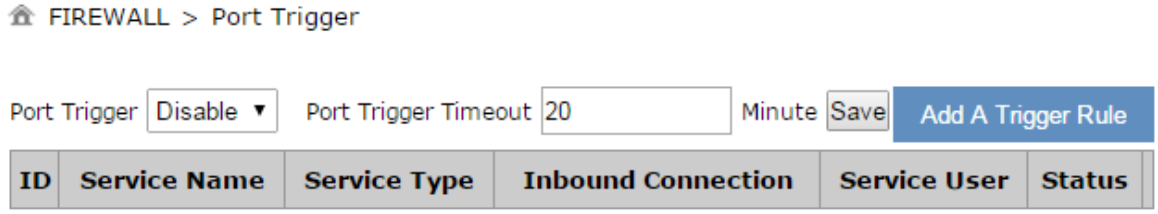
Common Service List for Port Forwarding			
Service name	**Protocol**	**Starting Port**	**Ending Port**
Customized	TCP, UDP, TCP/UDP	1~65534	1~65534
FTP	TCP	20	21
HTTP	TCP	80	80
ICUII	TCP	23566	23566
IP_PHONE	TCP	6670	6670
NetMeeting	TCP	1720	1720
News	TCP	119	119
PPTP	TCP/UDP	1723	1723
Telnet	TCP	23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

3.3.4 Port Trigger

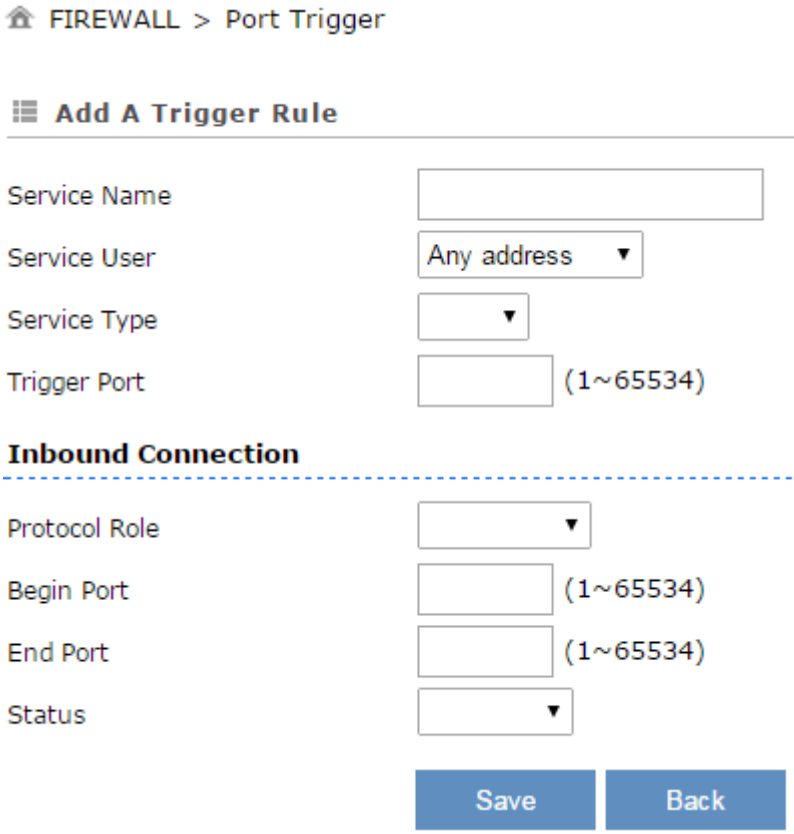
This page is used for setting up the port trigger, including configuring the Service Name, Service User, Service Type, Trigger Port, Protocol Role, Begin Port, End Port, and Status.

Port triggering is port forwarding with an on/off switch for the ports that have been forwarded. Have data flown 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.



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

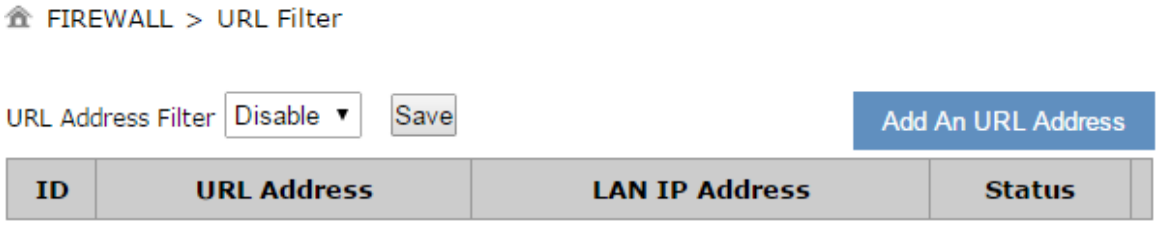


Description	Default
Service Name	
Set up the service name for port triggering. The name is composed of letters, numbers and underline, starting with a letter or number. The maximum string length is 32 bytes.	N/A
Service User	
Select the service user to apply the port triggering rule.	Any Address
Service 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
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.	Disable

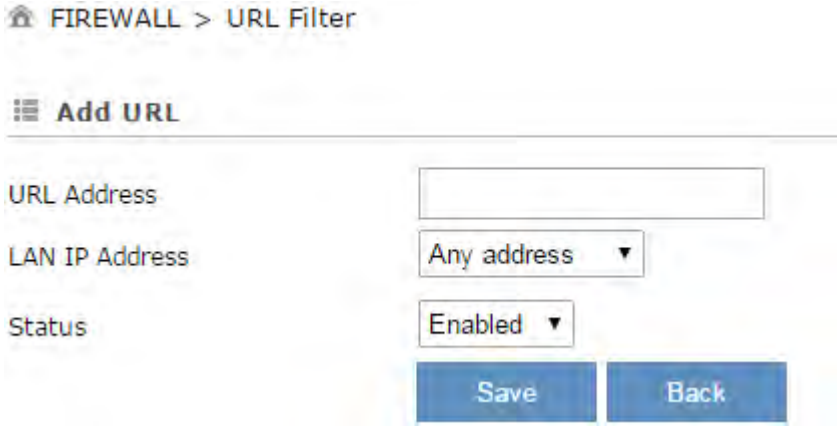
3.3.5 URL Filter

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.



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



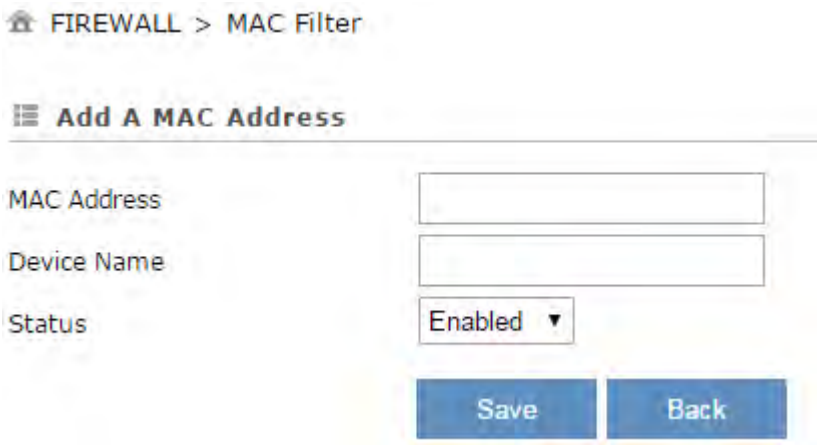
Description	Default
URL Address	
Manually input the URL address that you'd like to block, for example www.baidu.com.	
LAN IP Address	
Set up the LAN IP address that you'd like to block. Options are "Any Address", "Single Address" and "Address Range".	Any Address
Status	
Enable/disable the URL Filter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

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.

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

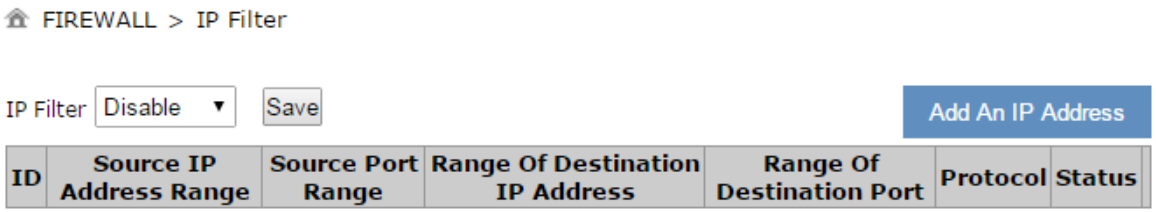


Description	Default
MAC Address	
Manually input the MAC address that you'd like to block.	
Device Name	
Set up the device name corresponding to the set MAC address.	
Status	
Enable/disable the MAC Filter functionality.	Enable

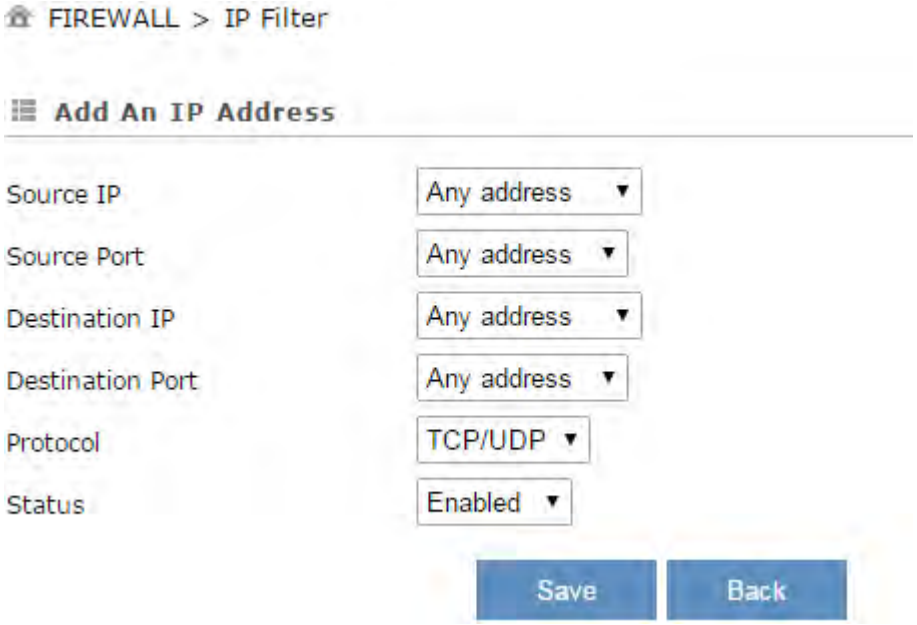
3.3.7 IP Filter

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.



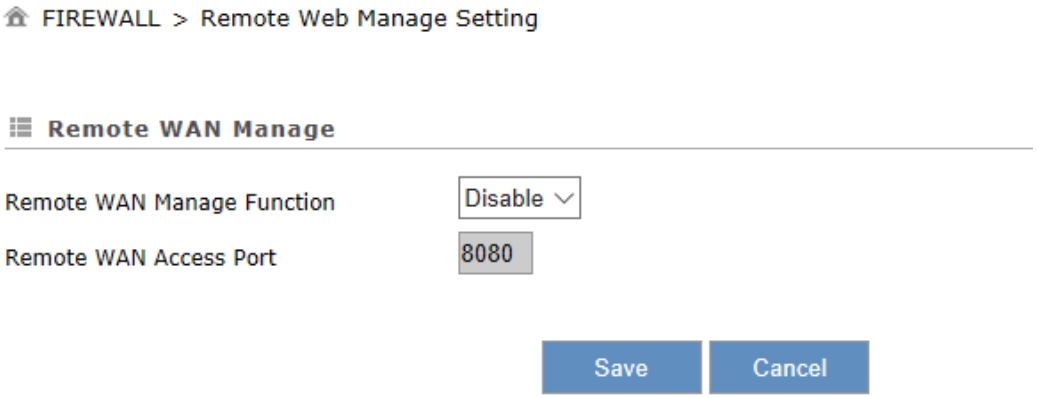
After clicking the "Add An IP Address", you will see the following page.



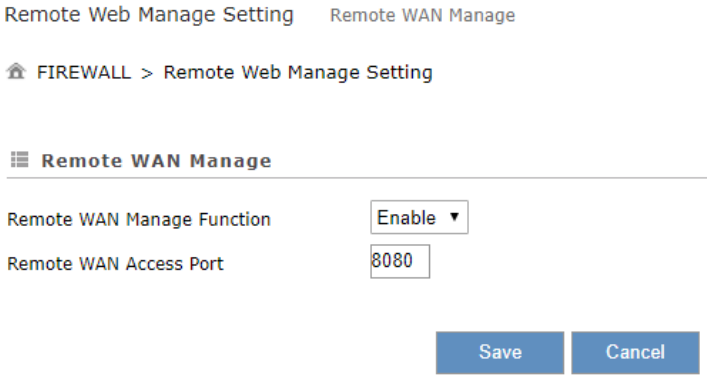
Description	Default
Source IP	
Set up the source IP.	Any Address
Source Port	
Set up the source port where the datagram came from.	Any Address
Destination IP	
Set up the destination IP.	Any Address
Destination Port	
Set up the destination port where the datagram is going to.	Any Address
Protocol	
Set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

3.3.8 Remote Web Manage Setting

Users can access DX webpage with a public IP address via WAN to configure remote web manage settings.



Description	Default
Remote WAN Manage Function	
Enable or disable Remote WAN Manage Function which allows users to access the management webpage and configure various parameters/ operating modes through WAN.	Disable
Remote WAN Access Port	
The default value of Remote WAN Access Ports is set as 880. Users can configure the value depending on their own needs, while the ports mostly used by other protocols are not recommended in order to prevent conflicts. ◦	8080

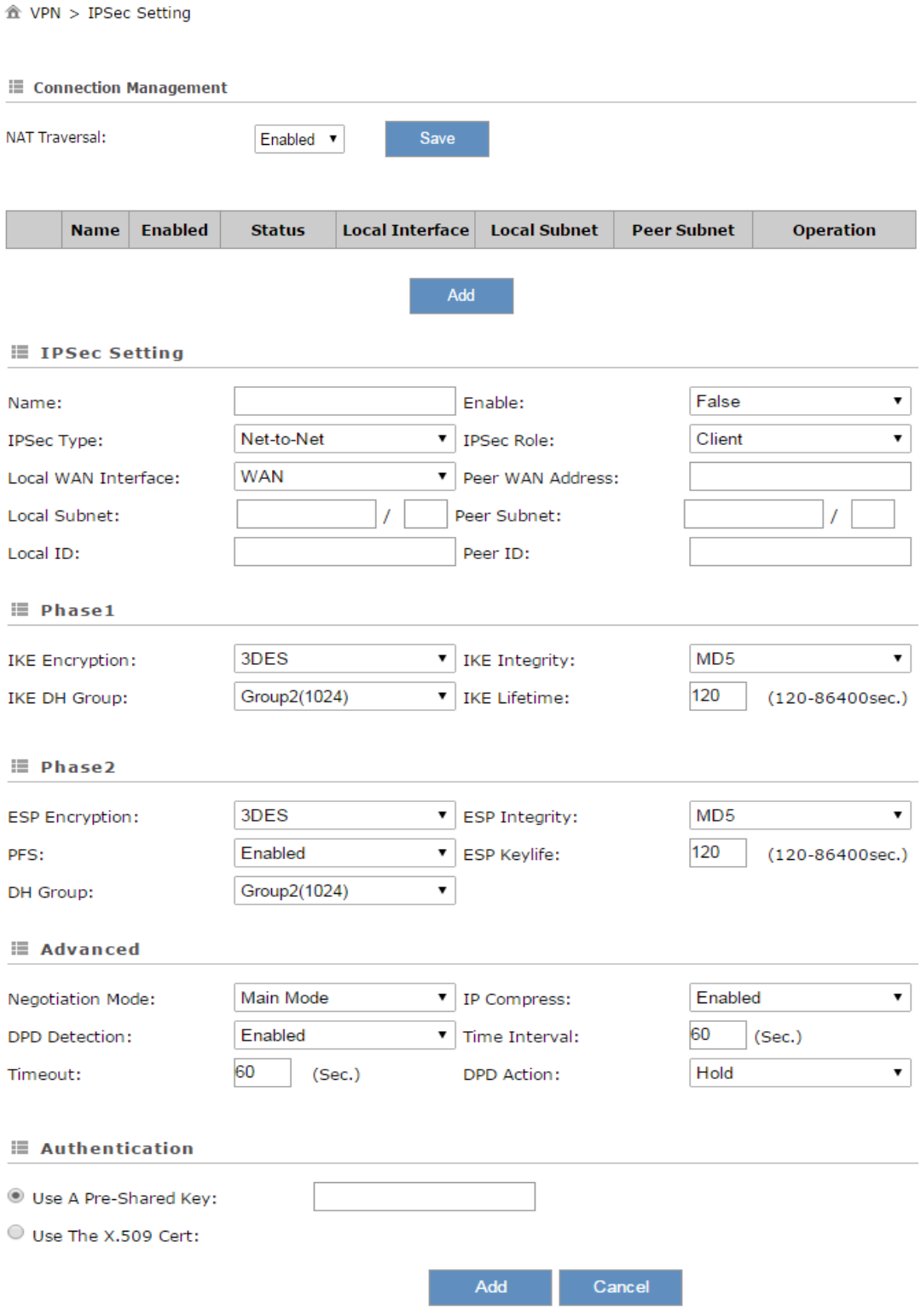
Operation Instruction	**Example: Access DX webpage with a public IP address via WAN** 1. Login to DX system. 2. Follow the path: NETWORK -> Connection 3. Set Primary Connection as WAN. 4. Obtain an IP address from the ISP.(e.g. 123.123.123.1) 5. Follow the path: FIREWALL -> Remote Web Manage 6. Set Remote WAN Manage Function as Enable 7. Set Remote WAN Access Port as 8080 8. Access DX Configuration webpage with http://123.123.123.1:8080 via Web browser on your PC. 
Illustration	

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.

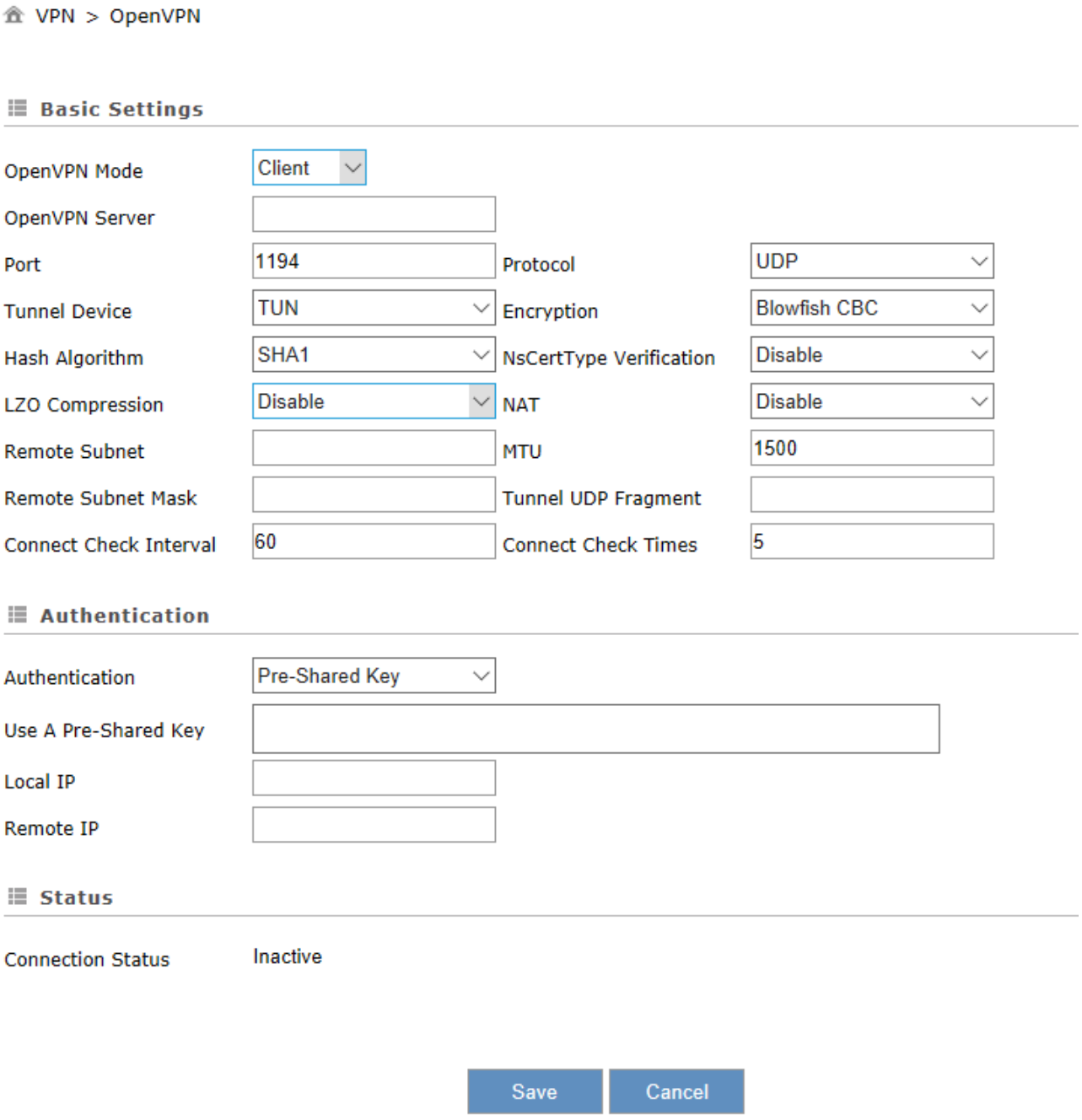


Description	Default
Name	
Input the name of IPSec connection, it cannot be repeated with other connection's name. Name can be up to 20 characters long.	
Enable	
Enable or disable this connection.	False
IPSec Type	
Set up the working mode of the IPSec, currently support "Net to Net" only	Net-to-Net
IPSec 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 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 "AES(256bit)"	3DES
ESP Integrity	
ESP phase integrity solution. Options are "MD5" and "SHA1"	MD5
PFS	
Enable or disable PFS(Perfect Forward Secrecy)	Enabled

Description	Default
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 maintained 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.

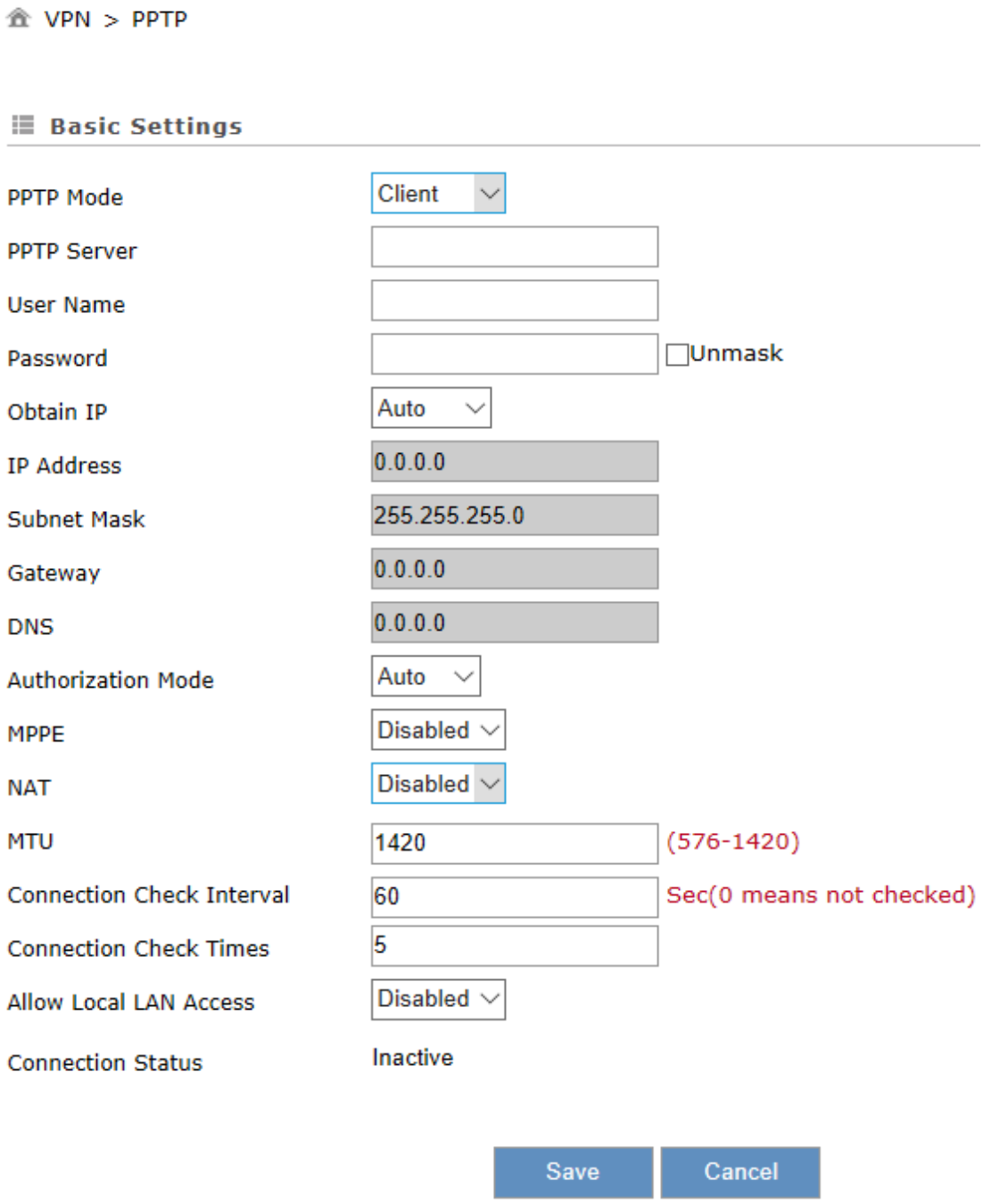


Description	Default
OPENVPN Mode	
Set up the working mode of the OPENVPN, options are “Disabled” and “Client”	Disabled
OPENVPN Server	
Set up the IP/Domain name of the OPENVPEN server	
Port	
Set up the listen port of OPENVPN client	1194
Protocol	
Set up the protocol type, options are “UDP” and “TCP”	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	
Set up hash algorithm, options are “None”, “SHA1” , “SHA256” , “SHA512” and “MD5”.	SHA1
nsCertType verification	
Enable or disable to support ns certificate type.	Disable
LZO Compression	
Enable or disable use LZO compression for data transfer	Disabled
NAT	
Enable or disable Network Address Translation	Disabled
Remote Subnet	
Set up remote subnet.	
MTU	
Set up the Maximum Transmission Unit of the tunnel	1500
Remote Subnet Mask	
Set up the remote subnet mask.	
Tunnel UDP Fragment	
Set the size of UDP packet fragment. Input range is 1~65536	
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

Description	Default
Authentication	
Choose use Pre-Shared key, username/password or certificate authentication option.	Pre-Shared key
Connection Status	
Display the current connection status	

3.4.3 PPTP

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

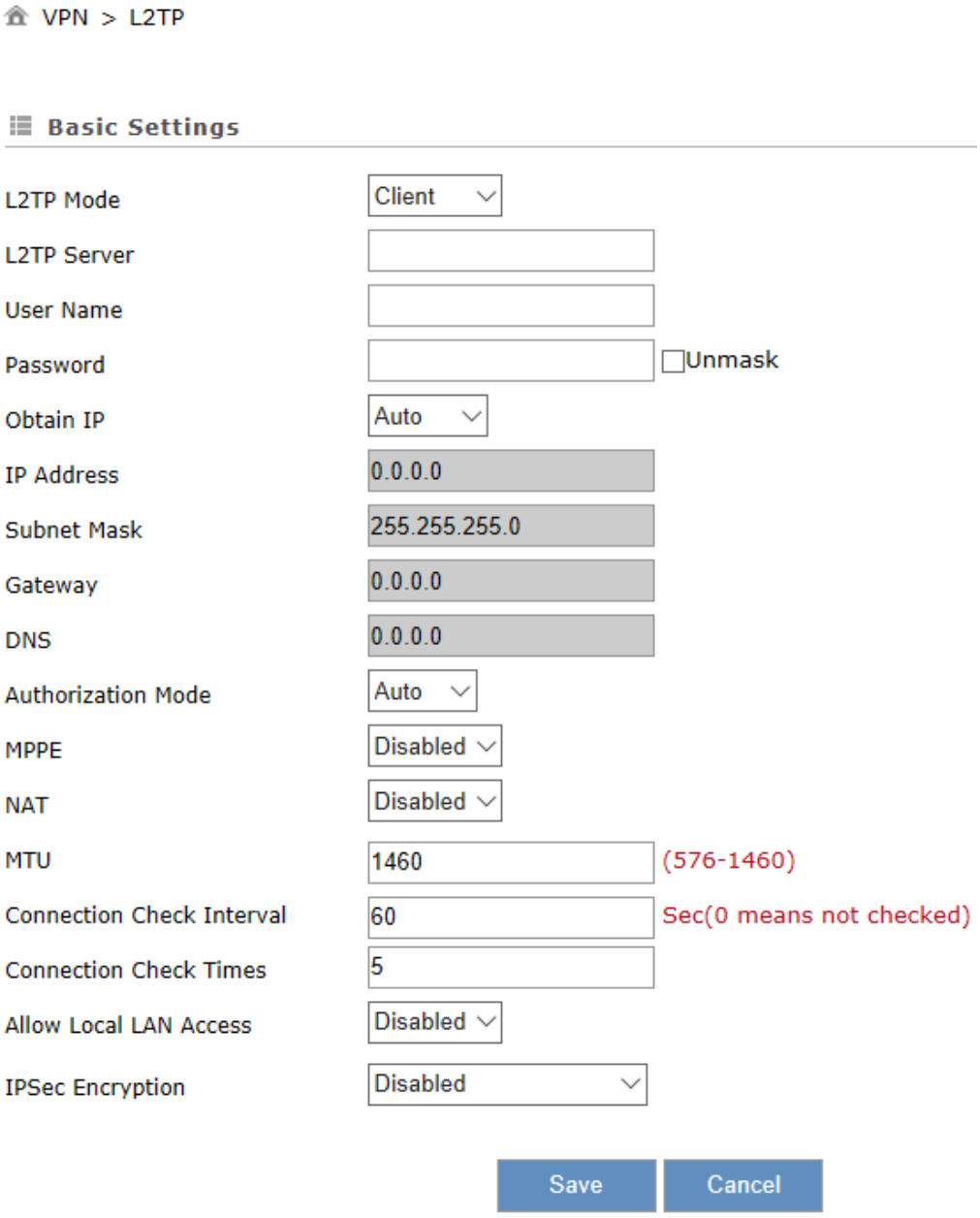


Description	Default
PPTP Mode	
Set up the working mode of the PPTP, options are “Disabled” and “Client”	Disabled
PPTP Server	
Set up the IP/Domain name of the PPTP server	
User Name	
Set up the username to login the PPTP server	
Password	
Set up the password to login the PPTP server	
Obtain IP	
Set up 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
Allow Local LAN Access	
Setup whether allow local LAN device access PPTP server	Disabled
PPTP Server Subnet	
Setup PPTP server subnet	

Description	Default
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.

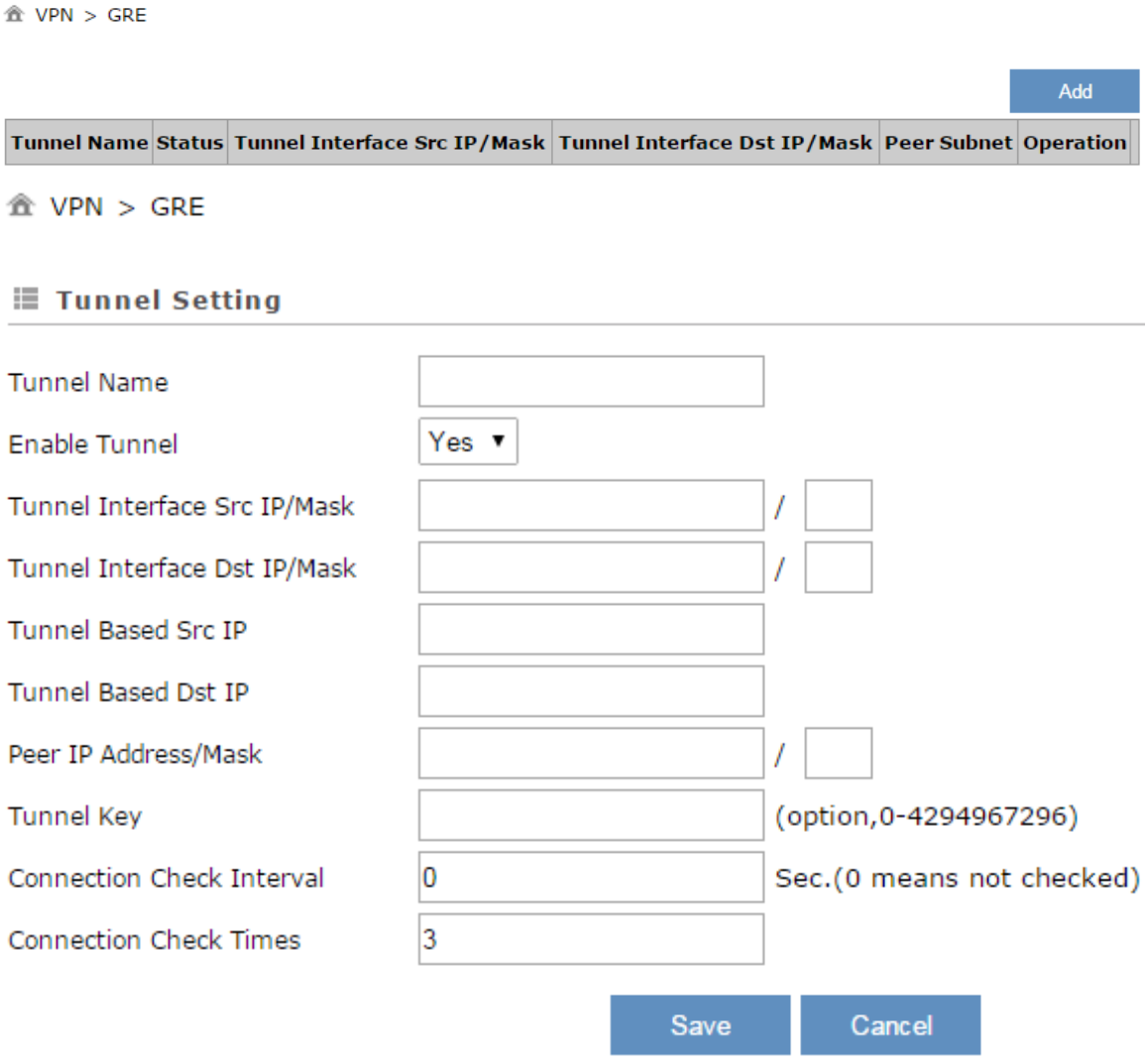


Description	Default
L2TP Mode	
Set up the working mode of the L2TP, options are “Disabled” and “Client”	Disabled
L2TP Server	
Set up the IP/Domain name of the L2TP server	
User Name	
Set up the username to login the L2TP server	
Password	
Set up the password to login the L2TP server	
Obtain IP	
Set up 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
Allow Local LAN Access	
Setup whether allow local LAN device access L2TP server	Disabled
L2TP Server Subnet	
Setup L2TP server subnet	

Description	Default
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	
Select The Certificate	
Select the Certificate user maintain it by Certificate function	
IPSec Peer ID	
Input the peer ID of the IPSec	
Connection Status	
Display the current connection status	

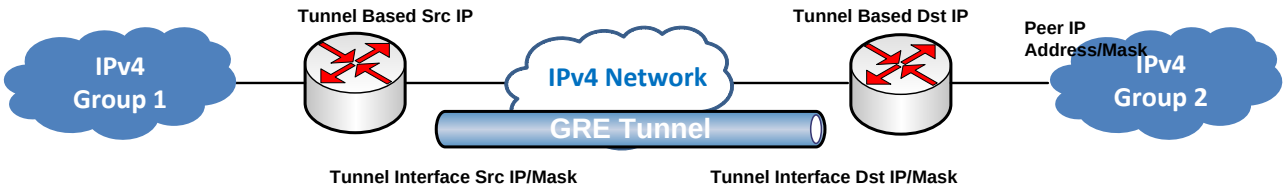
3.4.5 GRE

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



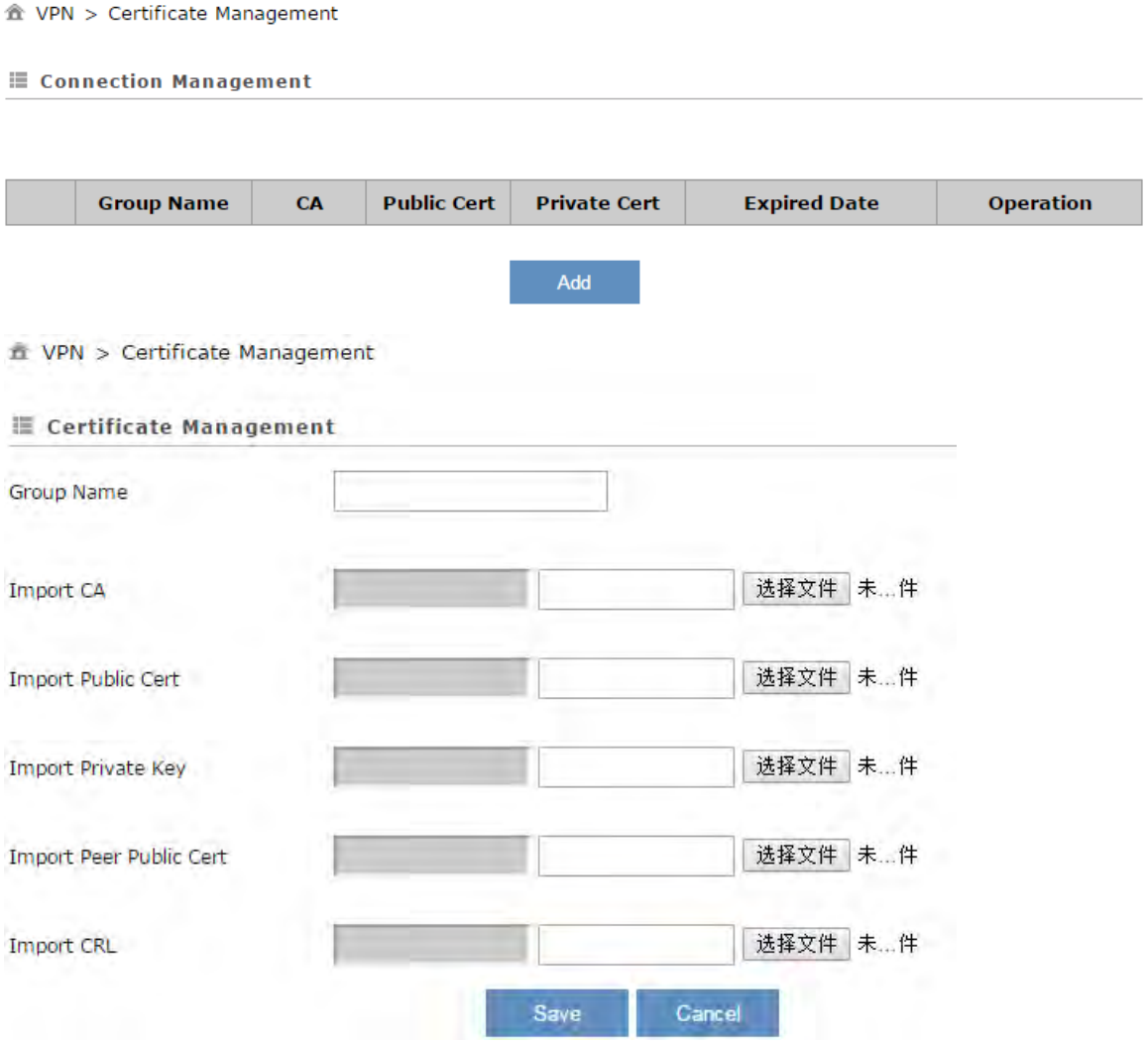
Description	Default
Tunnel Name	
Input the name of this tunnel, it can not be repeated with other tunnel's name.	
Enable Tunnel	
Enable or disable this tunnel.	Yes
Tunnel Interface Src IP/Mask	
The local tunnel IP address and mask	
Tunnel Interface Dst IP/Mask	
The remote tunnel IP address and mask	
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	
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.	3

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.

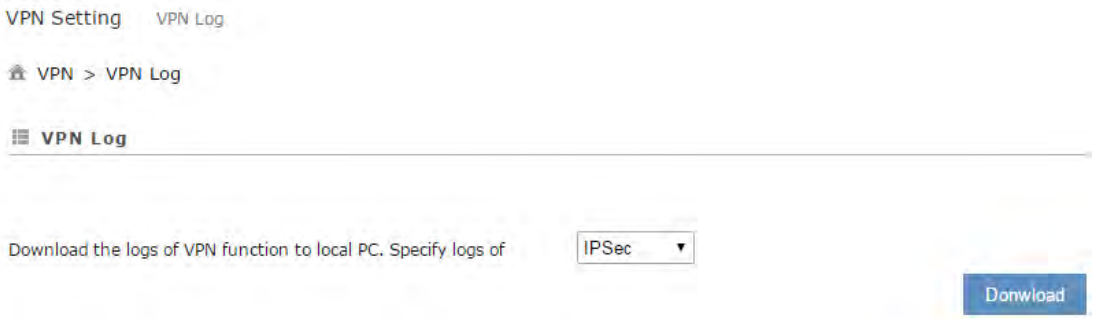


Description	Default
Group Name	
Setup the name of cert group, it cannot be repeated with other cert group.	
CA	
Import CA certificate file	
Public Cert	
Import public certificate file	
Private Cert	
Import public certificate file	
Peer Public Cert	
Import peer end public certificate file	

Description	Default
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

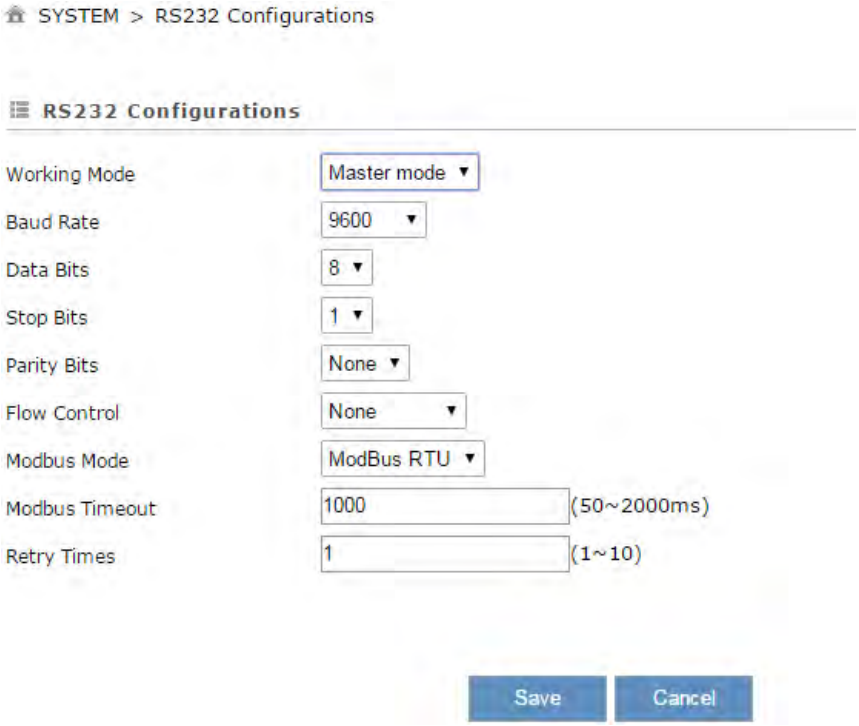
This page is used for download specified VPN log. Select the VPN type and click "Download" to save the log to local.



3.5 Interface

3.5.1 RS232

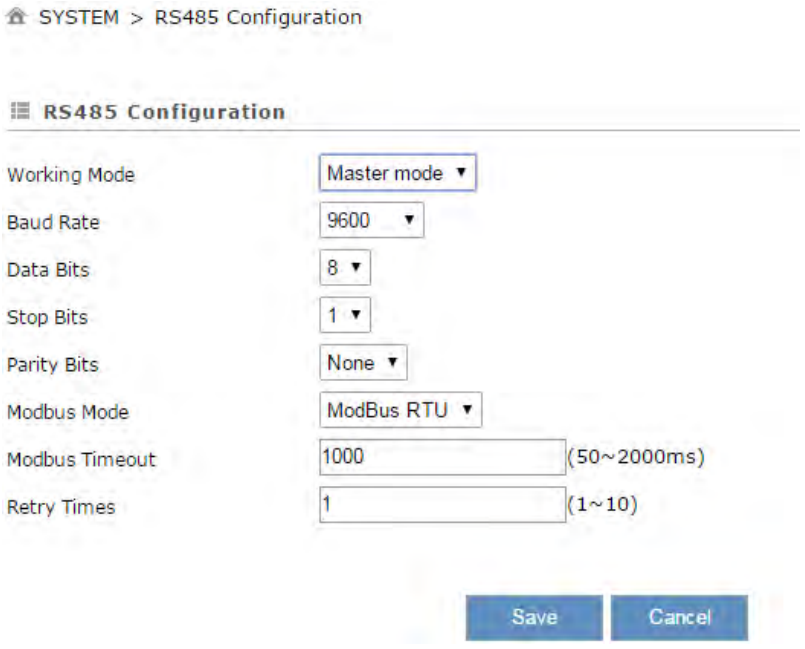
RS232 (Recommended Standard - 232) is a telecommunication standard for binary serial communications between devices. You can set up the configurations for RS232, including Baud Rate, Data Bits, Stop Bits, Parity Bits and Flow Control.



Description	Default
Working Mode	
Select the working mode for the current active serial port. ● **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

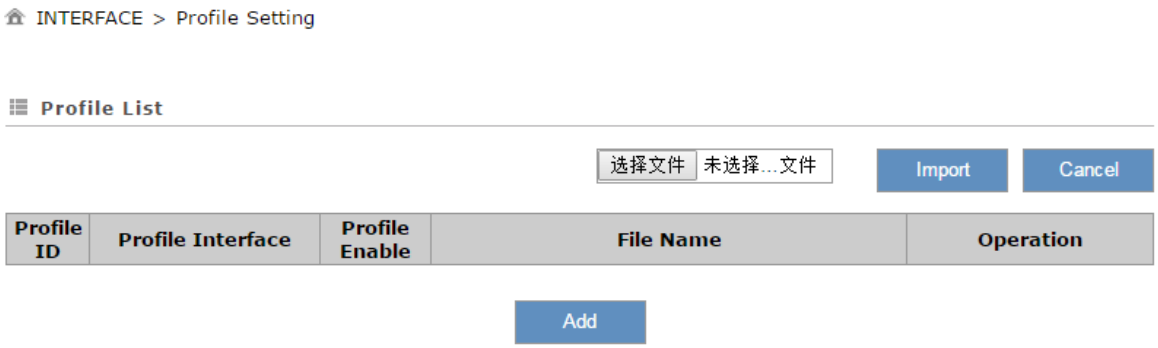
RS-485 (Recommended Standard - 485) is a telecommunication standard for binary serial communications between devices. You can set up the configurations for RS-485, including Baud Rate, Data Bits, Stop Bits, Parity Bits, and many more.

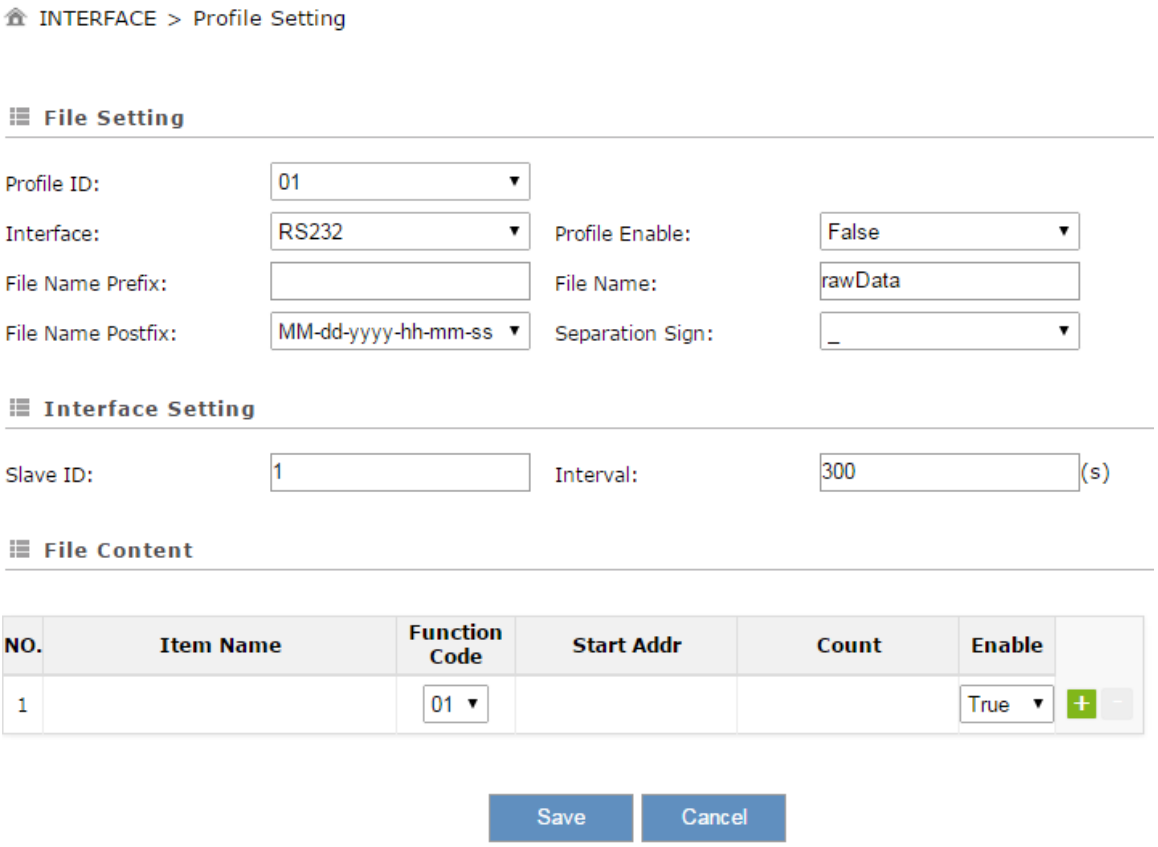


Description	Default
Working Mode	
Select the working mode for the current active serial port. ● **Master mode:** This mode is suitable for the DX-3001 to perform the read/write tasks on the open register of the Slave. ● **Close:** Disable this functionality.	Close
Baud Rate	
Set up the baud rate for 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

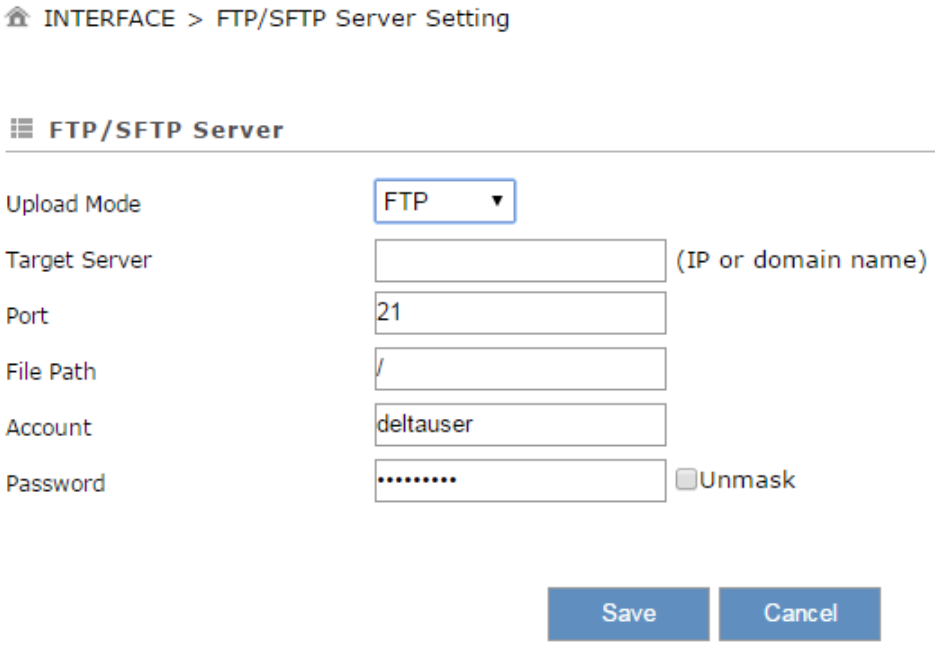
This page is used for setup the parameter about data collect.





3.5.4 FTP / SFTP Server

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



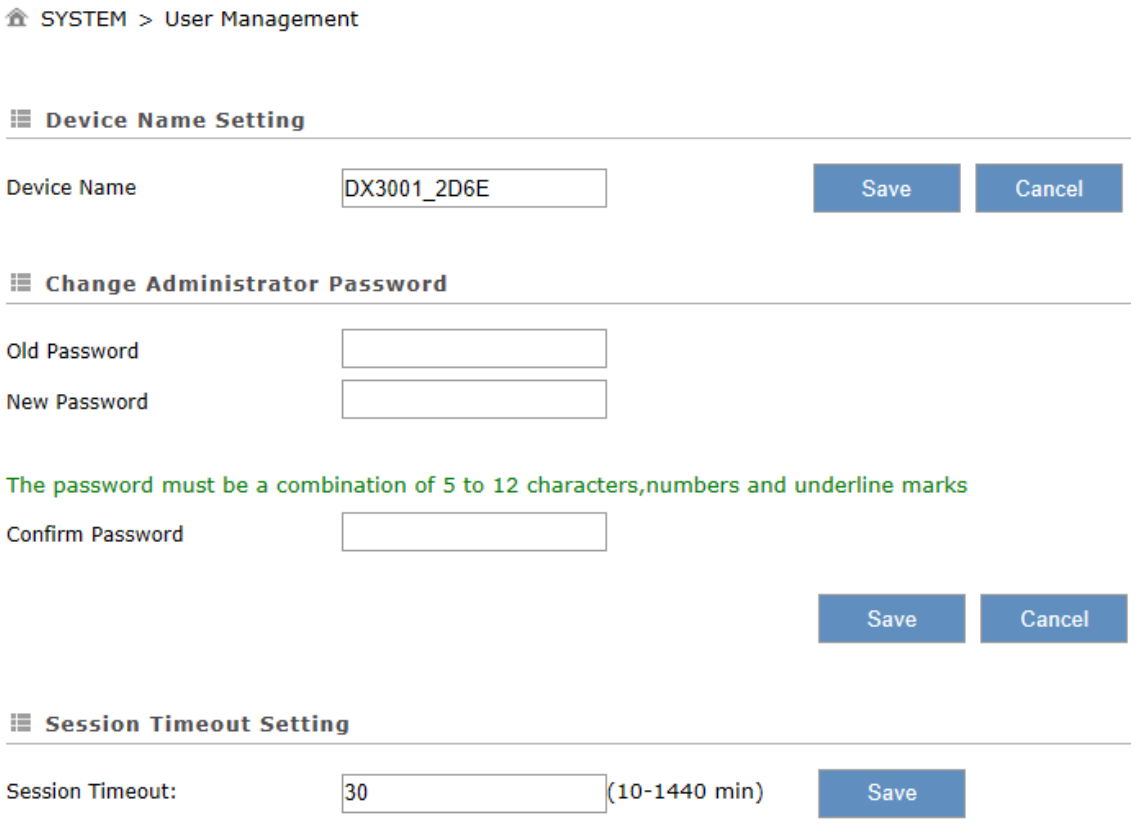
Description	Default
Upload Mode	
Set the method of the data upload to server, options are FTP and SFTP	Disabled
Target Server	
Set up the FTP/SFTP server IP/domain name	
Port	
Set up the listen port of server	
File Path	
Set up the file save path in server	/
Account	
Set up the FTP/SFTP account	
Password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

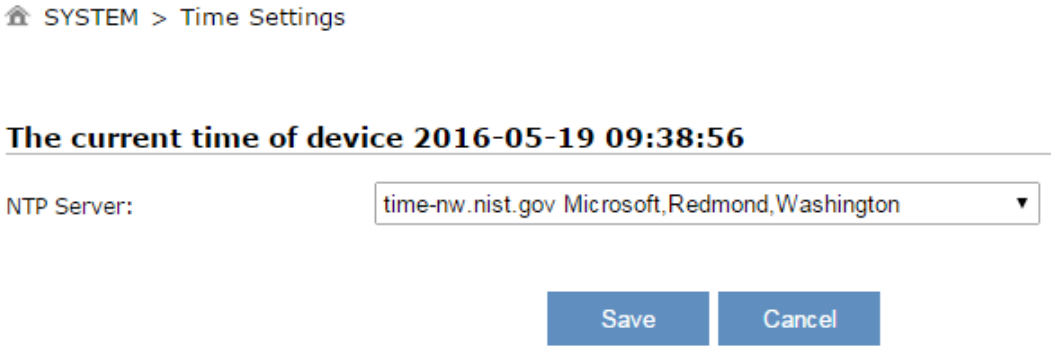
This page is used for reset router name and change the administrator password. The password must be a combination of 5 to 12 characters, numbers and/or underline symbols.



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.	N/A
Session Timeout	
Session timeout is an expired time limit for a logged in user which has been inactive for a period of time. Setting range is from 10 to 1440 minutes	30

3.6.2 Time Zone Settings

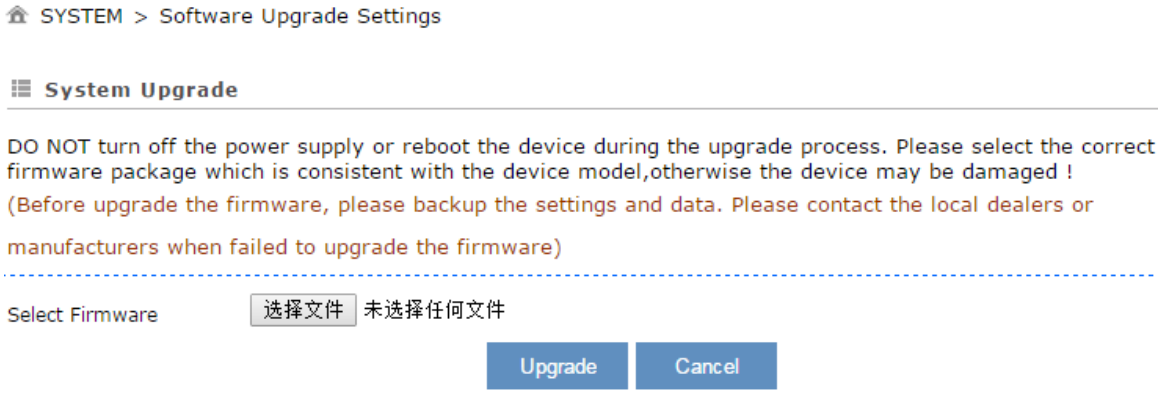
This page is used for set the NTP server to synchronizing router clocks over network. Use the dropdown list to select the server or manual input server IP/domain.



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

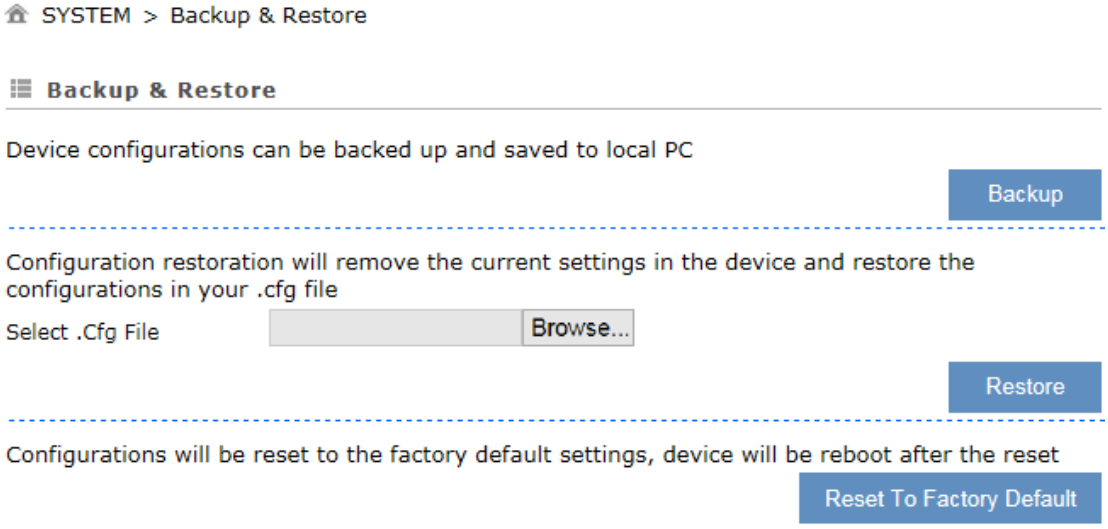
This page is used for upgrading the system.



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.

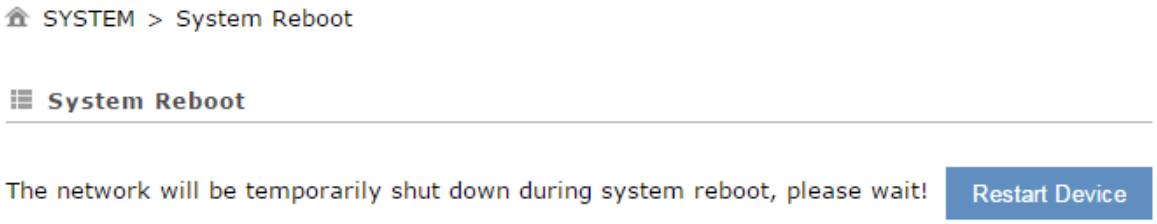


Description	Default
Backup	
Click “Backup” to save the device configurations on your computer.	N/A
Restore	
Click “Chose file” to select the backup file and then click “Restore” to restore the configurations. The device configuration will be restored to the previous version and the device will reboot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

Description	Default
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

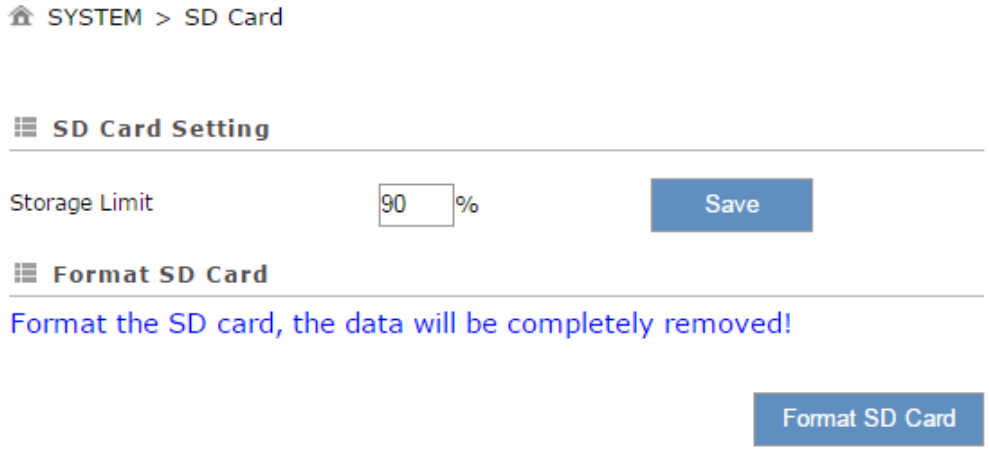
3.6.5 System Reboot

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



3.6.6 SD Card

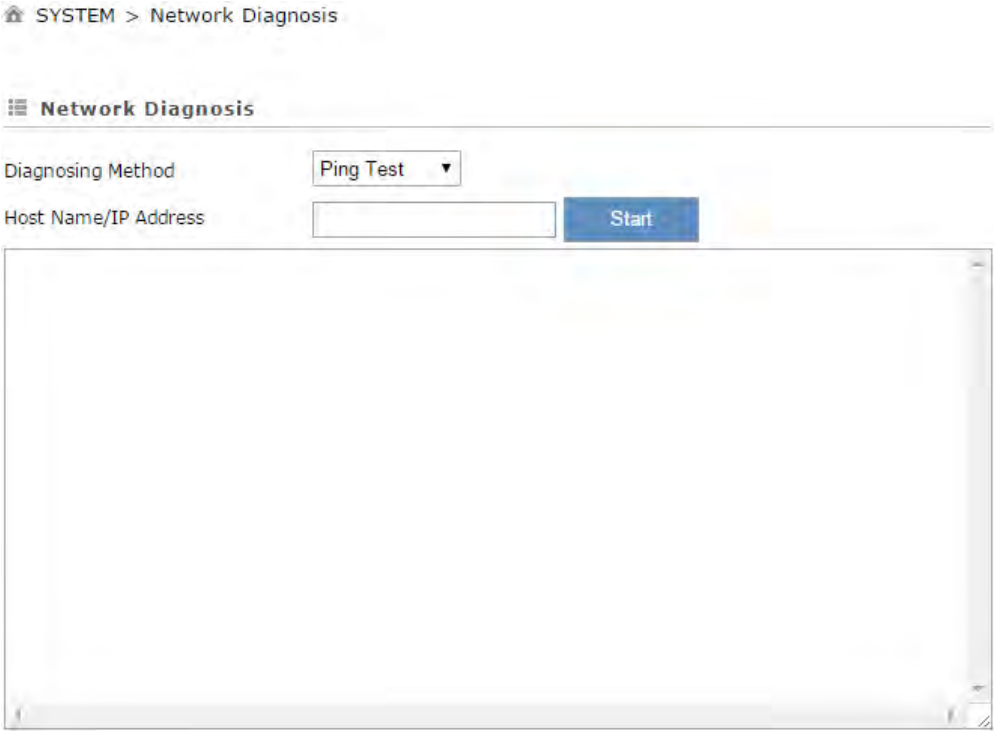
This page is used for manage SD card.



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.



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