comnet
Communication Networks

QUICK START GUIDE

CNFE3TX2CXMS(U,E)

4G LTE Cellular VPN Gateway

This guide serves the following ComNet Model Numbers:

CNFE3TX2CXMSU
CNFE3TX2CXMSE

The ComNet CNFE3TX2CXMS(U,E) is an edge Cellular VPN Gateway with 2 10/100TX Ports and 1 SIM Card slot. It supports 802.1X and MAC filter for security control. The Gateway can be configured to operate in 3 modes: Dynamic/Static IP route, PPPoE authentication, and Modem dial up. The units can be powered by an IEEE 802.3af PoE compliant device on port 1 or through the 4-Pin terminal block with dual DC Inputs. The Gateways are DIN Rail mountable and feature a rigid IP-30 housing.

Contents

Regulatory Compliance Statement 3

Warranty 3

Disclaimer 3

Safety Information 4

Getting Started 5

1.1 About the CNFE3TX2CXMS(U,E) 5

1.3 Hardware Features 5

Hardware Overview 6

2.1 Front Panel 6

2.2 Front Panel LEDs 7

2.3 Rear Panel 8

2.4 Top Panel 9

Hardware Installation 10

3.1 DIN-rail Installation 10

3.2 Wall Mounting 11

3.3 Wiring 12

Cables and Antenna 13

4.1 Ethernet Cables 13

4.2 RJ-45 Pin Assignment 13

4.3 Cellular Antenna 14

Management Interface 15

5.1 Installation 15

5.2 Configuration 17

Regulatory Compliance Statement

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

Warranty

ComNet warrants that all ComNet products are free from defects in material and workmanship for a specified warranty period from the invoice date for the life of the installation. ComNet will repair or replace products found by ComNet to be defective within this warranty period, with shipment expenses apportioned by ComNet and the distributor. This warranty does not cover product modifications or repairs done by persons other than ComNet-approved personnel, and this warranty does not apply to ComNet products that are misused, abused, improperly installed, or damaged by accidents.

Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

Disclaimer

Information in this publication is intended to be accurate. ComNet shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ComNet reserves the right to revise the contents of this publication without notice.

Safety Information

» Only ComNet service personnel can service the equipment. Please contact ComNet Technical Support.

» The equipment should be installed in locations with controlled access, or other means of security, and controlled by persons of authority. When operating at temperatures above 60 °C, the equipment surfaces will be hot to the touch. Installation in restricted access location is required for this case.

Getting Started

1.1 About the CNFE3TX2CXMS(U,E)

The CNFE3TX2CXMS(U,E) is a reliable 4G LTE Cellular Router with two 10/100Base-T(X) ports where one is for LAN and the other one for WAN. It supports 802.1X and MAC filter for security control and can be operate in three routing modes: Dynamic/Static IP Route, PPPoE Authentication, and Modem Dial-up. In the mode of Modem Dial-up, it supports GPRS/3G/3.5G/LTE modem via the internal 4G module. You can set up a WLAN environment that fulfills demands of various applications by dialing up cellular modems. In addition, the LAN port of CNFE3TX2CXMS(U,E) is P.D.-enabled which is fully compliant with IEEE802.3af PoE specification. This feature extends the layout up to 100 meters.

1.2 Software Features

» Secure management by HTTPS
» Multiple WAN connection types supported: Dynamic/Static IP, PPPoE, Modem/Dial-up
» IP table to prevent access from unauthorized IP address
» Supports NAT setting (virtual server, port trigger, DMZ, and UPnP)
» Versatile modes & event alarm by e-mail
» Event warning by Syslog, e-mail, SNMP trap, relay output, and beeper

1.3 Hardware Features

» 2 × 10/100Base-T(X) Ethernet ports for WAN / LAN connection individually.
» 1 × SIM card slot
» 4G LTE dial-up modem included
» 1KV isolation for PoE P.D. port
» Dual DC inputs
» Operating temperature: -40 to 60 °C
» Storage temperature: -40 to 85 °C
» Operating humidity: 5% to 95%, non-condensing
» DIN-Rail and Wall-mount enabled
» Casing: IP-30
» Dimensions: 45(W) × 80.6(D) × 95(H) mm

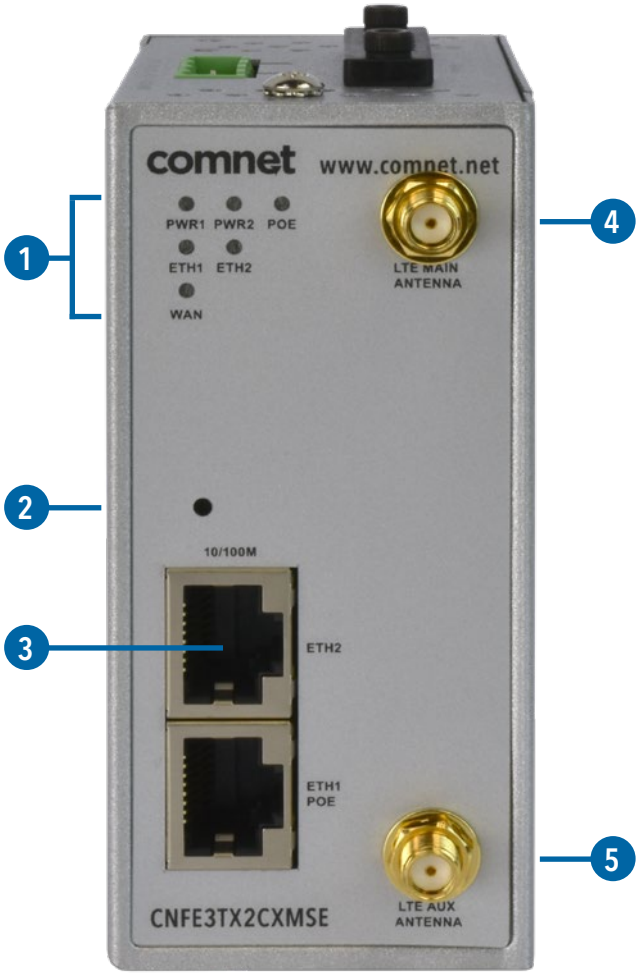
Hardware Overview

2.1 Front Panel

2.1.1 Ports and Connectors

The Router is equipped with the following ports and features on the front panel.

Port	Description
10/100Base-T(X) Fast Ethernet Ports	10/100Base-T(X) RJ-45 fast Ethernet ports supporting auto-negotiation. Default settings includes Speed: auto Duplex: auto ETH1 (LAN port) is IEEE802.3af PoE compliant PD
ANT.	2 × SMA connector for cellular antenna.



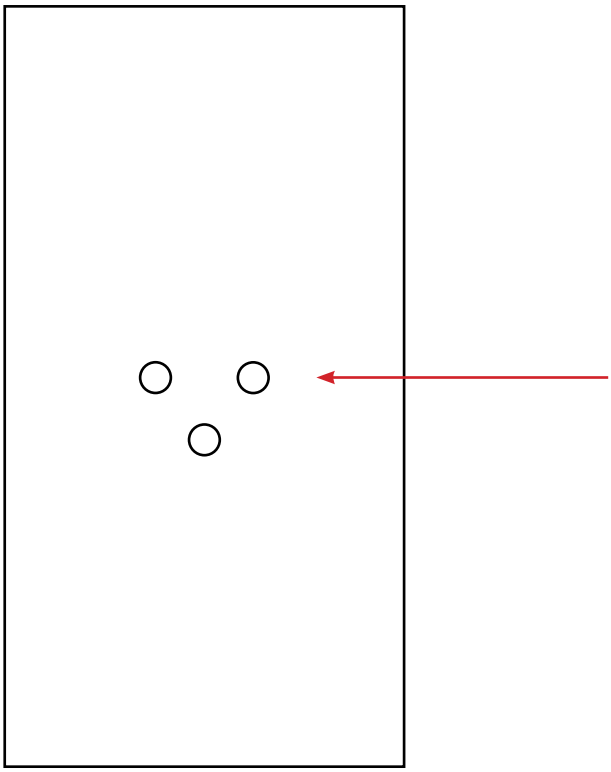
1	Indicating LEDs (see 2.2 Front Panel LEDs)
2	Reset
3	Ethernet Ports (ETH1 as LAN port; ETH2 as WAN port)
4	LTE main antenna connector
5	LTE auxilliary antenna connector

2.2 Front Panel LEDs

LED	Color	Status	Description
PWR1	Green	On	DC power 1 activated
PWR2	Green	On	DC power 2 activated
PoE	Green	On	Power is supplied over Ethernet cable
ETH1	Green	On	Port is linked and running at 100Mbps
		Blinking	Data being transmitted
ETH2	Green	On	Port is linked and running at 100Mbps
		Blinking	Data being transmitted
WAN	Green	On	Modem ready

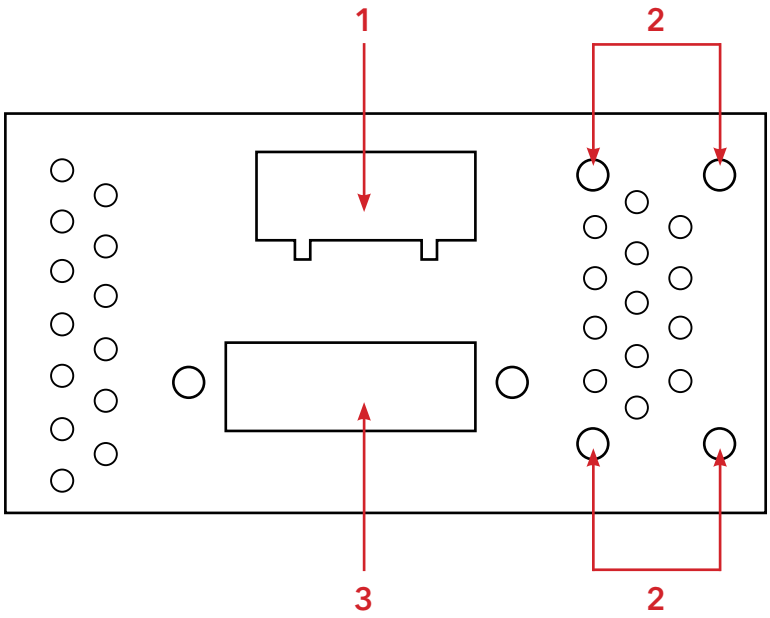
2.3 Rear Panel

On the rear panel of the router sit three sets of screw holes in the middle, used for DIN-rail installation.



Din-rail screw holes

2.4 Top Panel

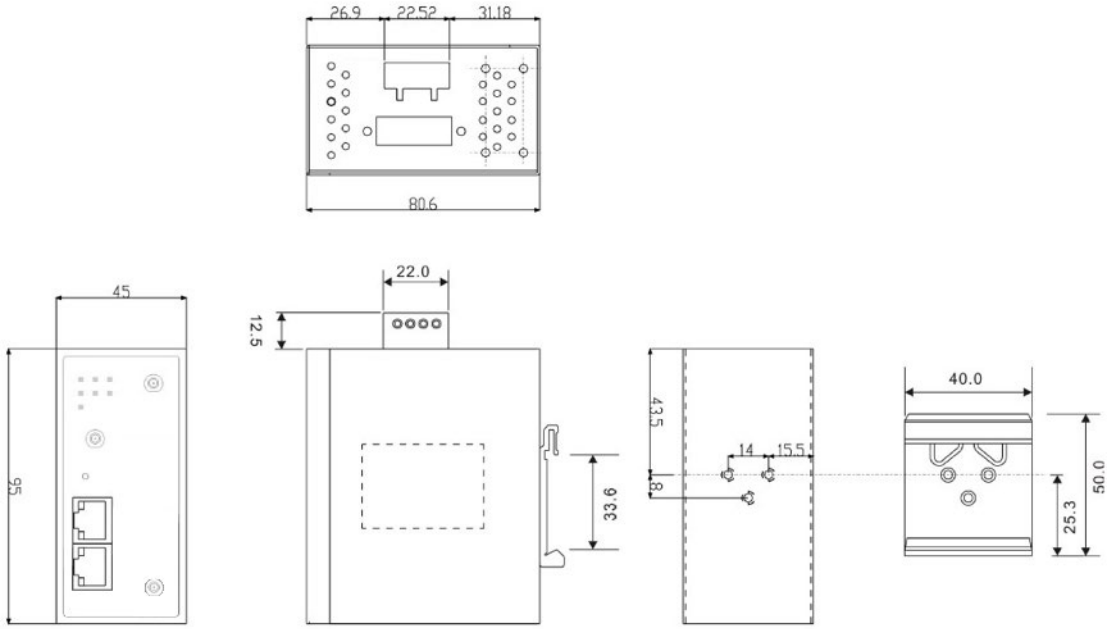


1. Terminal block
2. Wall-mount screw holes
3. SIM card slot

Hardware Installation

3.1 DIN-rail Installation

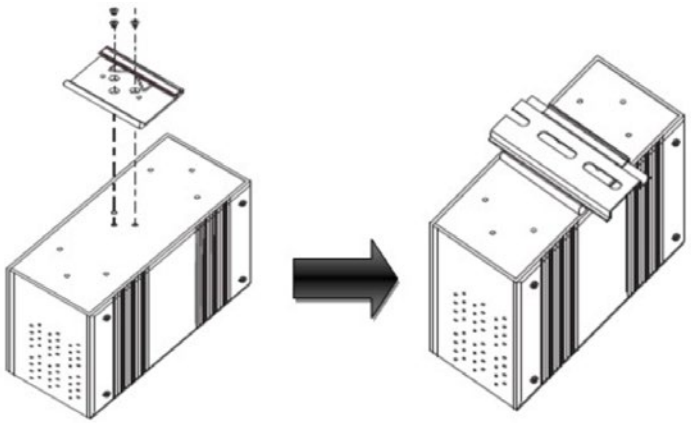
The router comes with a DIN-rail kit to allow you to fasten the router to a DIN-rail in any environment.



DIN-rail Kit Mechanical Drawing (Measurements in mm)

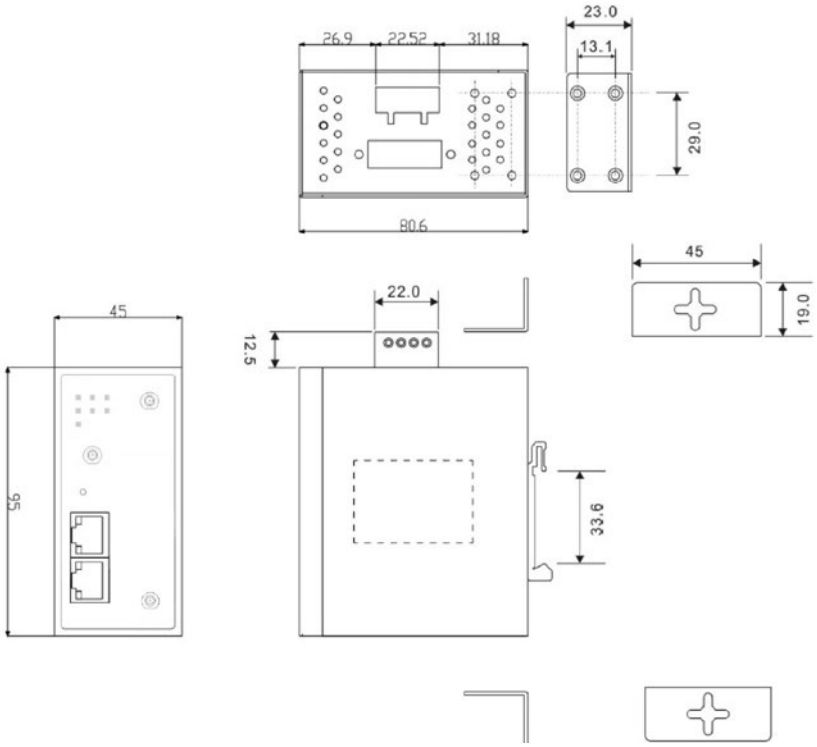
Step 1: Slant the router and screw the DIN-rail kit onto the back of the router, right in the middle of the back panel.

Step 2: Slide the router onto a DIN-rail from the DIN-rail kit and make sure the router clicks into the rail firmly.



3.2 Wall Mounting

Besides Din-rail, the router can be fixed to the wall via a wall mount panel, which can be found in the package.



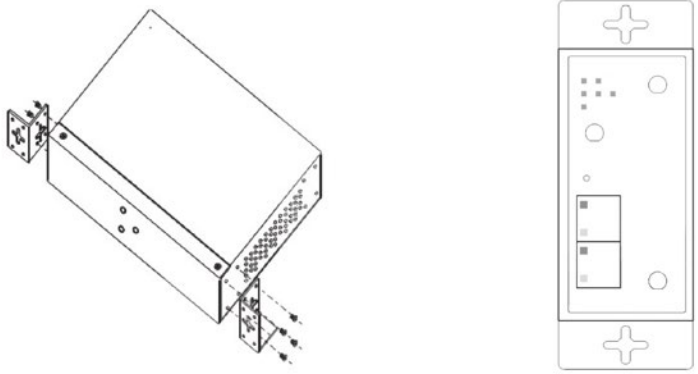
Wall-Mount Kit Drawing (Measurements in mm)

To mount the router onto the wall, follow the steps:

Step 1: Screw the two pieces of wall-mount kits onto both ends of the rear panel of the router. A total of eight screws are required, as shown below.

Step 2: Use the router, with wall mount plates attached, as a guide to mark the correct locations of the four screws.

Step 3: Insert a screw head through the large part of the keyhole-shaped aperture on the plate, and then slide the router downwards. Tighten the screw for added stability.



3.3 Wiring

WARNING: Be sure to switch off the power and make sure the area is not hazardous before disconnecting modules or wires. The devices may only be connected to the supply voltage shown on the type plate.

3.3.1 Grounding

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices.

3.3.2 Dual Power Inputs

The router has two sets of power inputs, power input 1 and power input 2, on a 4-pin terminal block on the router's top panel. Follow the steps below to wire redundant power inputs.

Step 1: insert the negative/positive DC wires into the V-/V+ terminals, respectively. Step 2: to keep the DC wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.

Note: besides power input, the router can also be powered by a PoE PSE such as switch via its PoE-enabled LAN port.

ATTENTION

1. *Be sure to disconnect the power cord before installing and/or wiring your routers.*
2. *Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.*
3. *If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.*
4. *Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.*
5. *Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.*
6. *You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring sharing similar electrical characteristics can be bundled together*
7. *You should separate input wiring from output wiring*
8. *It is advised to label the wiring to all devices in the system*

Cables and Antenna

4.1 Ethernet Cables

The device has two 10/100Base-T(X) Ethernet ports. According to the link type, the AP uses CAT 3, 4, 5, 5e, 6 UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-T(X)	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45

4.2 RJ-45 Pin Assignment

With 10/100Base-T(X) cables, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

10/100 Base-T(X) RJ-45 Pin Assignments :

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	P.O.E. power input +
5	P.O.E. power input +
6	RD-
7	P.O.E. power input -
8	P.O.E. power input -

The router also supports auto MDI/MDI-X operation. You can use a straight-through cable to connect PC and router. The following table below shows the 10/100BASE-T(X) MDI and MDI-X port pin outs.

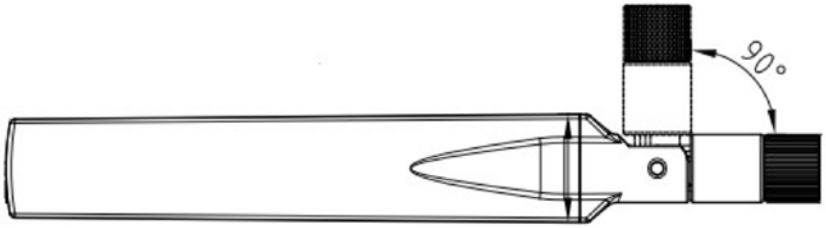
MDI/MDI-X pins assignment

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	P.O.E. power input +	P.O.E. power input +
5	P.O.E. power input +	P.O.E. power input +
6	RD-(receive)	TD-(transmit)
7	P.O.E. power input -	P.O.E. power input -
8	P.O.E. power input -	P.O.E. power input -

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

4.3 Cellular Antenna

The router provides two SMA connectors for cellular antennas. External RF cables and antennas can also be used with the connector.



Management Interface

5.1 Installation

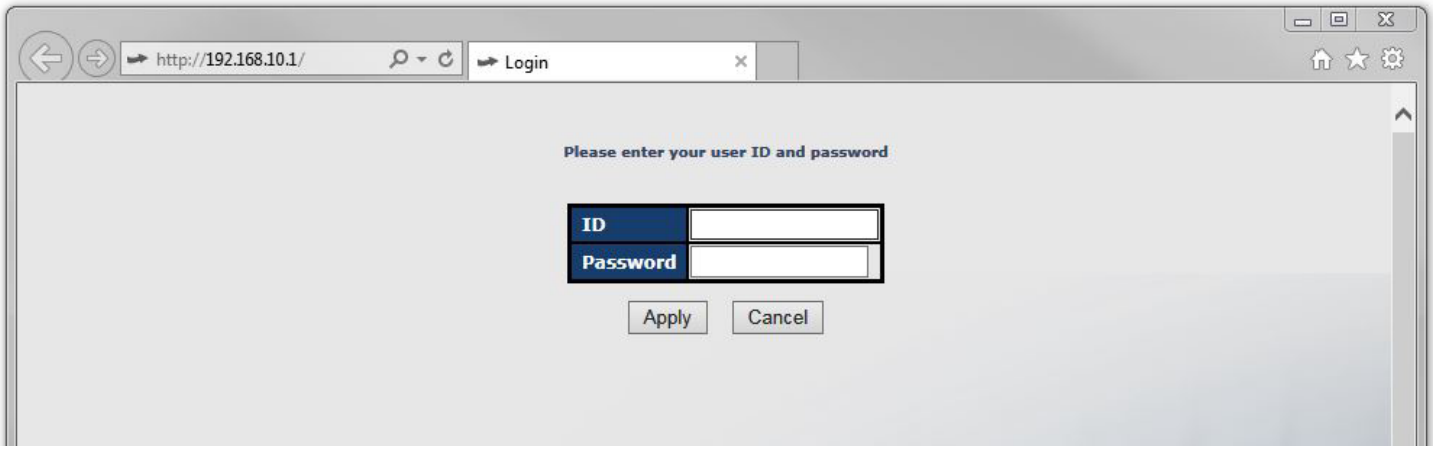
Before installing the router, you need to be able to access the router via a computer equipped with an Ethernet port.

Follow the steps below to install and connect the Router to PCs:

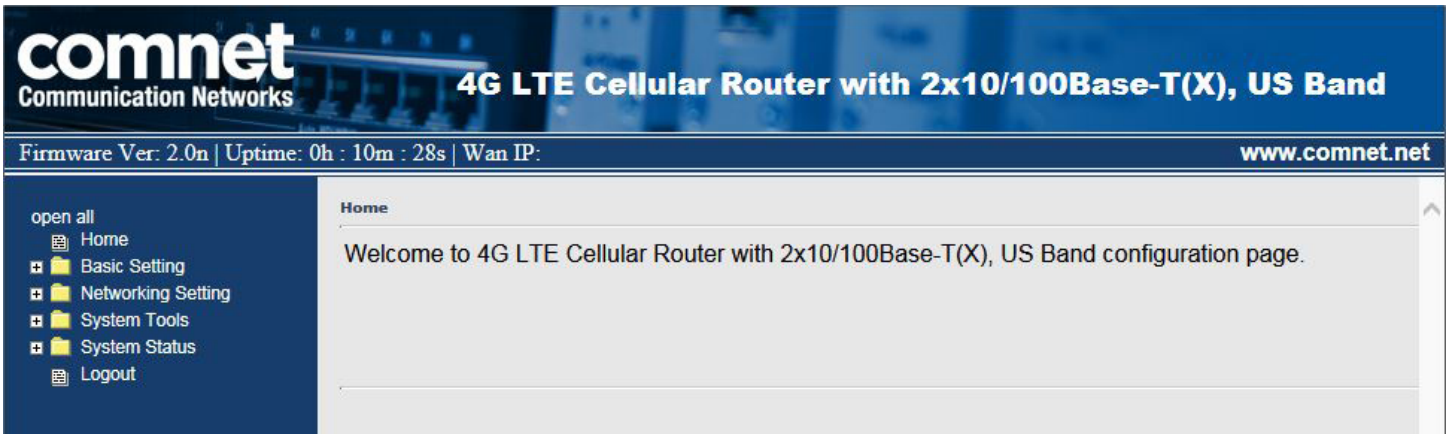
Step 1: Select power source. The router can be powered by +12~48V DC power input, or via a PoE (Power over Ethernet) PSE Ethernet switch.

Step 2: Connect a computer to the router. Use either a straight-through Ethernet cable or cross-over cable to connect the ETH1 port of the router to a computer. Once the LED of the LAN port lights up, which indicates the connection is established, the computer will initiate a DHCP request to retrieve an IP address from the AP router.

Step 3: Configure the router on a web-based management utility. Open a web browser on your computer and type http://192.168.10.1 (default router IP of the router) in the address box to access the webpage. A login window will pop up where you can enter the default login name admin and password admin. For security reasons, we strongly recommend you to change the password. Click on System Tools > Login Setting after logging in to change the password.

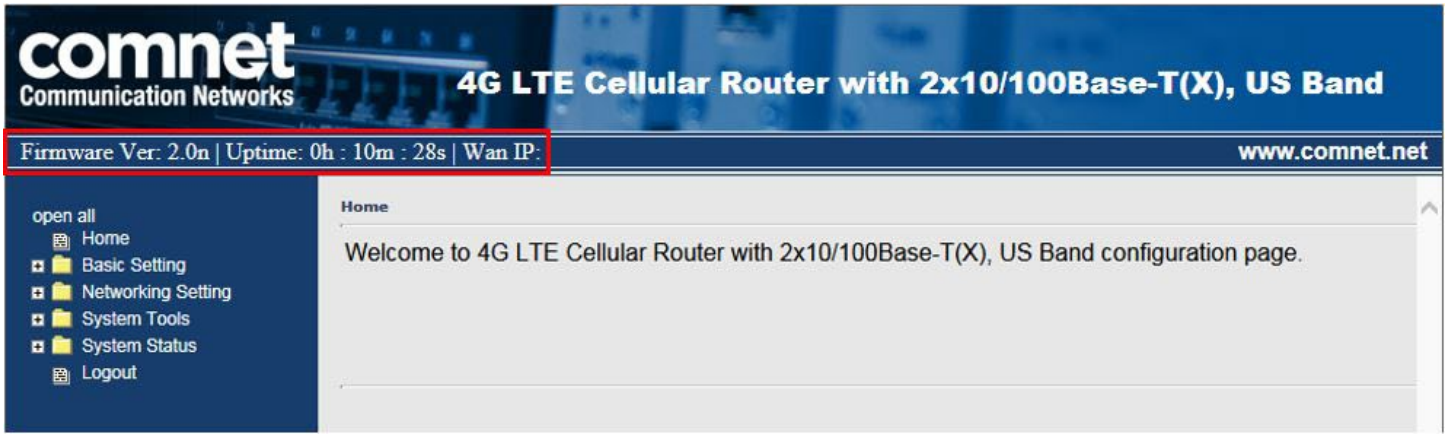


After you log in successfully, a Web interface will appear, as shown below. On the left hand side of the interface is a list of functions where you can configure the settings. The details of the configurations will be shown on the right screen.


comnet
Communication Networks
4G LTE Cellular Router with 2x10/100Base-T(X), US Band
Firmware Ver: 2.0n | Uptime: 0h : 10m : 28s | Wan IP:
www.comnet.net
open all
Home
Basic Setting
Networking Setting
System Tools
System Status
Logout
Home
Welcome to 4G LTE Cellular Router with 2x10/100Base-T(X), US Band configuration page.

5.2 Configuration

On top of the Home screen shows information about the firmware version, uptime, and WAN IP address.



Label	Description
Firmware	Shows the current firmware version
Uptime	Shows the elapsed time since the AP router is started
Wan IP	Shows WAN IP address

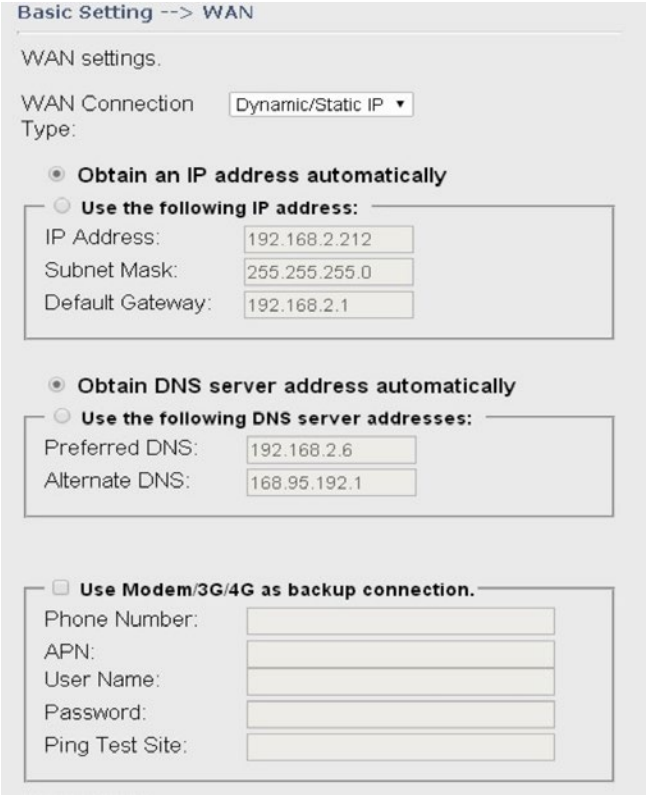
5.2.1 Basic Setting

This section will guide you through the general settings for the router.

WAN

This page allows you to configure WAN settings. Different WAN connection types will have different settings.

WAN Connection Type as Dynamic/Static IP:

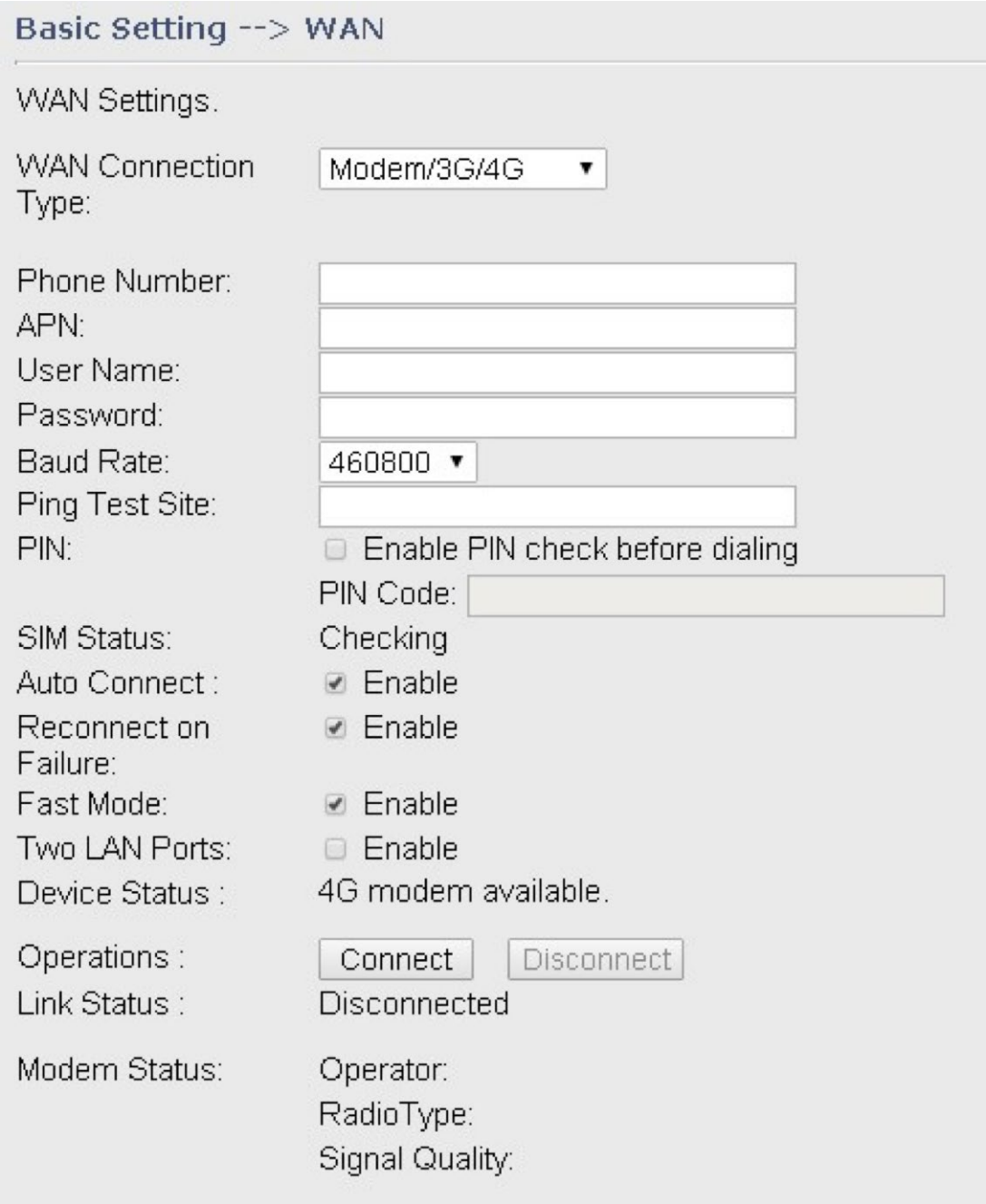


Label	Description
Obtain an IP address automatically	Select this option if you want the IP address of the WAN port to be assigned automatically by the DHCP server in your network.
Use the following IP address	Select this option if you want to assign an IP address to the WAN port manually. You should set IP Address, Subnet Mask, and Default Router according to IP rules.
Obtain DNS server address automatically	Obtains a DNS server address from a DHCP server. If you have chosen to obtain an IP address automatically, this option will be selected accordingly.
Use the following DNS server addresses	Specifies a DNS server address manually. You can enter two addresses as the primary and secondary options.
Use Modem/3G as backup connection	Enable this option if you want to use Modem/3G as a backup connection when main connection is lost. Enter your account username and password in the corresponding fields. Type a website address such as www.google.com in Ping Test Site to use it to check if the connection is alive or lost.

WAN Connection Type as PPPoE:

Label	Description
User Name / Password	Enter the username & password provided by your ISP.
AC Name	Enter the name of the access concentrator provided by your ISP
Service Name	Enter the service name provided by your ISP
Specify the IP & DNS provided by ISP	Enter a static IP and DNS address required by other ISPs.
Connection Mode	Auto: connect automatically when the router boots up Connect on Demand: disconnect the PPP session if the router has had no traffic for a specified amount of time. Fill a number in the Max Idle Time field. Manual: connects or disconnects manually via the Connect/Disconnect buttons at the end of the page
Use Modem/3G/4G as backup connection	Enable this option if you want to use modem/3G/4G as a backup connection when main connection is lost. Enter your account username and password in the corresponding fields. Type a website address such as www.google.com in Ping Test Site to use it to check if the connection is alive or lost.

WAN Connection Type as Modem/3G/4G

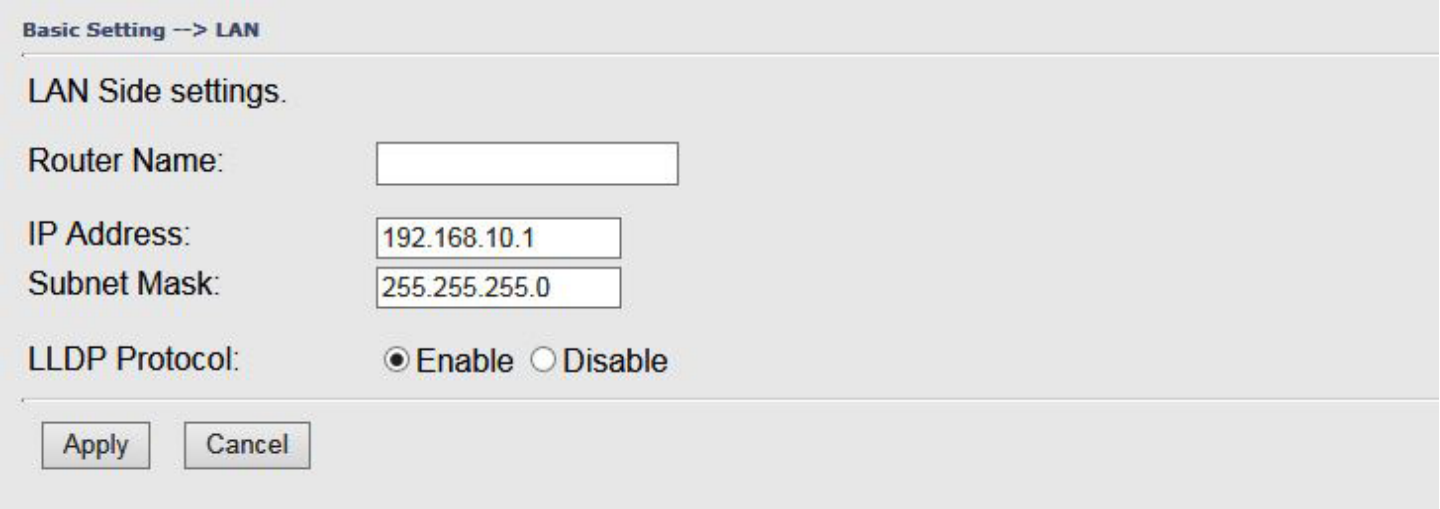


Label	Description
APN	Enter the APN value (optional)
User Name	Enter the user name provided by your ISP
Password	Enter the password provided by your ISP
Baud Rate	Select a Baud Rate from the drop-down list
Ping Test Site	Type a website address the field to use it to check if the connection is alive or lost.
PIN	Enter a PIN code if you want to perform PIN check

Label	Description
Auto Connect	Check to start connections when the router boots up
Reconnect on Failure	Check to allow for reconnection when links fail
Two LAN Ports	When connecting to a WAN network through wireless Connections such as a 3G SIM card, you can turn the idling WAN port to act as a LAN port by checking the box.
Device Status	Shows the status of the device
Operations	Click Connect to start modem/3G connections or Disconnect to shut down connections
Link Status	Shows the status of connections
Modem Status	Shows information about the modem

LAN

This page allows you to configure the IP settings of the LAN for the router. The LAN IP address is private to your internal network and is not visible to Internet.



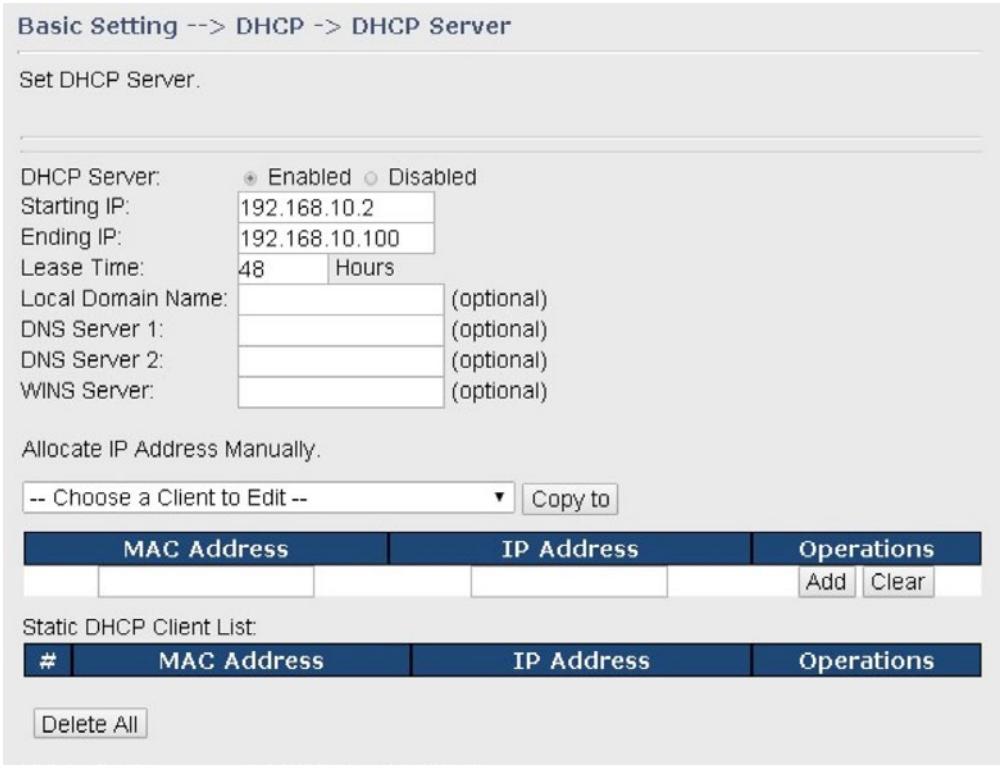
Label	Description
Router Name	Enter the name of your router
IP Address	The IP address of the LAN. The default value is 192.168.10.1
Subnet Mask	The subnet mask of the LAN. The default value is 255.255.255.0
LLDP Protocol	LLDP is a vendor-neutral protocol used by network devices for advertising their identity, capabilities, and neighbors on a LAN. You can enable or disable LLDP protocol.

DHCP

DHCP is a network protocol designed to allow devices connected to a network to communicate with each other using an IP address. The connection works in a client-server model, in which DHCP clients request an IP address from a DHCP server. The router comes with a built-in DHCP (Dynamic Host Control Protocol) server which assigns an IP address to a computer (DHCP client) on the LAN automatically. The router can also serve as a relay agent which will forward DHCP requests from DHCP clients to a DHCP server on the Internet.

The IP allocation provides one-to-one mapping of MAC address to IP address. When a computer with a MAC address requesting an IP address from the router, it will be assigned with the IP address according to the mapping. You can choose one from the client list and add it to the mapping list.

DHCP Server

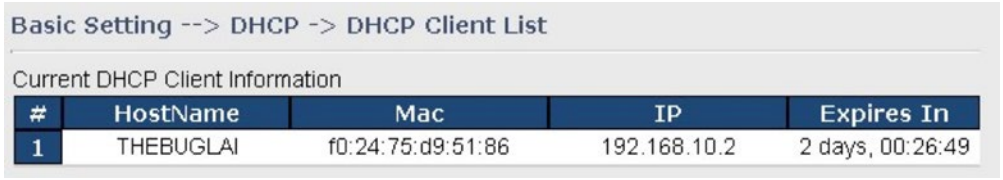


Label	Description
DHCP Server	Enables or disables the DHCP server function. The default setting is Enabled.
Starting IP	The starting IP address of the IP range assigned by the DHCP server
Ending IP	The ending IP address of the IP range assigned by the DHCP server
Lease Time	The period of time for the IP address to be leased. During the lease time, the DHCP server cannot assign that IP address to any other clients. Enter a number in the field. The default setting is 48 hours.
Local Domain Name	Enter the local domain name of a private network (optional)
DNS Server 1&2	Enter the IP address for the DNS server (optional)

Label	Description
WINS Server	Enter the WINS server (optional)
Allocate IP Address Manually	The IP Allocation section provides one-to-one mapping of MAC address to IP address. When a computer with the MAC address requests an IP from the router, it will be assigned with the IP address according to the mapping. You can choose one from the client list and add it to the mapping relationship.
Static DHCP Client List	The list shows the one-to-one relationship of the MAC address and IP address.

DHCP Client List

This page will show the DHCP client information including the host name, MAC address, IP address, and the expiration date of the address.



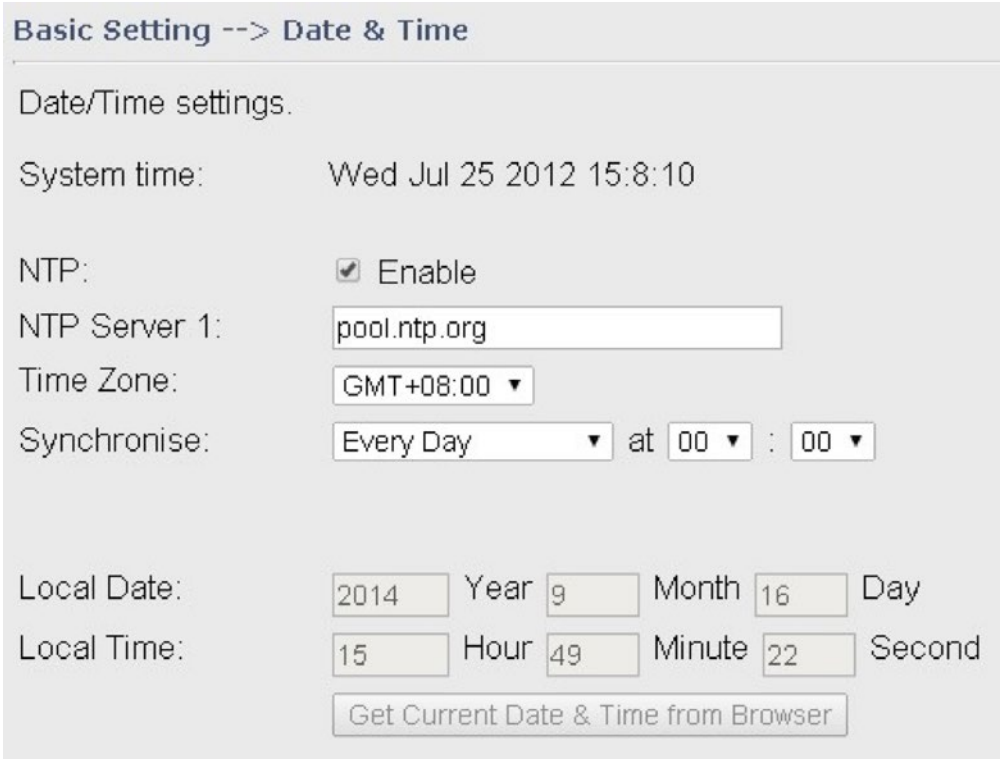
DDNS

DDNS (Dynamic Domain Name System) allows you to configure a domain name for your IP address which is dynamically assigned by your ISP. Therefore, you can use a static domain name that always points to the current dynamic IP address.

Label	Description
DDNS Service	Choose a DDNS service provider from the list
User Name	Enter the user name of your DDNS account
Password	Enter the password of your DDNS account
Domain	Enter the domain name provided by your dynamic DNS service provider

Date & Time

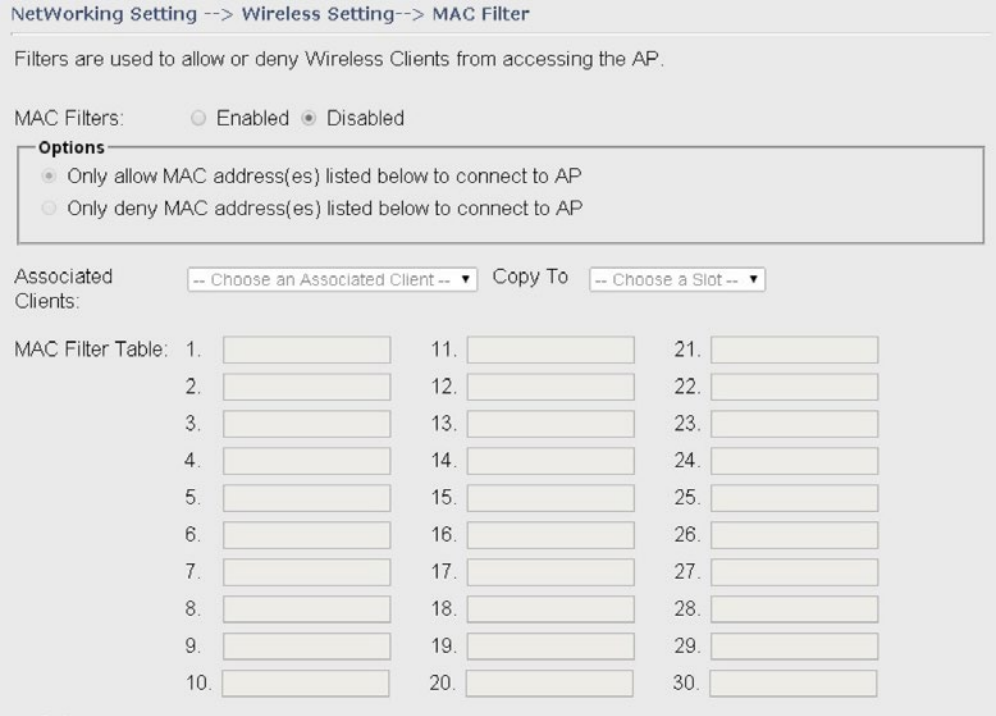
In this page, you can set the date & time of the device. A correct date and time will help the system log events. You can set up a NTP (Network Time Protocol) client to synchronize date & time with a NTP server on the Internet.



Label	Description
NTP	Enables or disables NTP function
NTP Server 1	The primary NTP server
Time Zone	Select the time zone you are located in
Synchronize	Specify the scheduled time for synchronization
Local Date	Set a local date manually
Local Time	Set a local time manually

MAC Filter

This page allows you to set up MAC filters to allow or deny wireless clients to connect to the router. You can manually add a MAC address or select a MAC address from the Associated Clients list currently associated with the router.

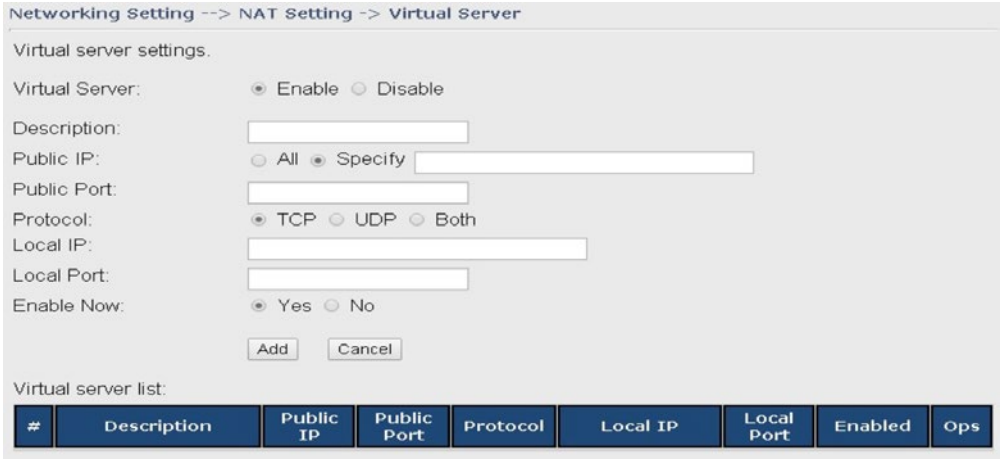


Label	Description
MAC Filter	Select Enabled or Disabled to activate or deactivate MAC filters
Options	Select one of the options to allow or deny the MAC address in the list
Associated Clients	Shows the wireless MAC addresses associated with the router
MAC Filter Table	You can edit up to MAC addresses in these fields
Apply	Click to activate the configurations

NAT Setting

Virtual Server

This page allows you to set up virtual server setting. A virtual server allows Internet users to access services on your LAN. This is a useful function if you host services online such as FTP, Web or game servers. A public port must be defined for the virtual server on your router in order to redirect traffic to an internal LAN IP address and LAN port. Any PC used as a virtual server must have a static or reserved IP address.

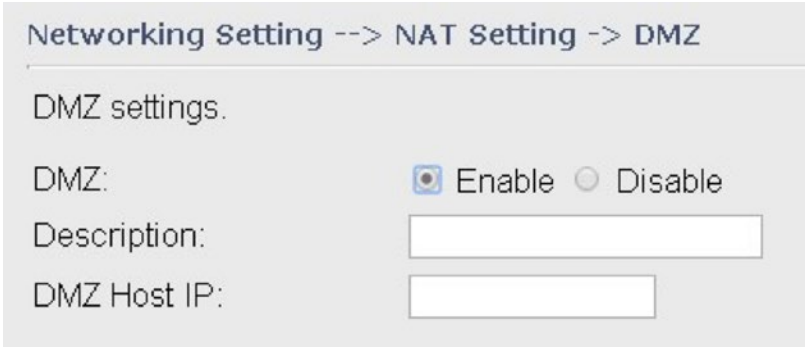


Label	Description
Virtual Server	Select Enabled or Disabled to activate or deactivate virtual server
Description	Enter the description of the entry. Acceptable characters are 0-9, a-z, and A-Z. A null value is allowed.
Public IP	Enter a public IP allowed to access the virtual service. If not specified, choose All.
Public Port	The port number to be used to access the virtual service on the
WAN (Wide Area Network) Protocol	The protocol used for the virtual service
Local IP	The IP address of the computer that will provide virtual service
Local Port	The port number of the service used by the private IP computer
Enable Now	Enables the virtual server entry after adding it
Virtual server list	Click Edit to edit the virtual service entry and Del to delete the entry.

DMZ

DMZ (Demilitarized Zone) allows a computer to be exposed to the Internet without passing through the security settings and therefore is unsecured. This feature is useful for special purposes such as gaming.

To use this function, you need to set an internal computer as the DMZ host by entering its IP address. Adding a client to the DMZ may expose your local network to a variety of security risks, so use this function carefully.



Label	Description
DMZ	Enables or disables DMZ
Description	Enter a description for the DMZ host entry
DMZ Host IP	Enter the IP address of the computer to act as the DMZ host

UPnP

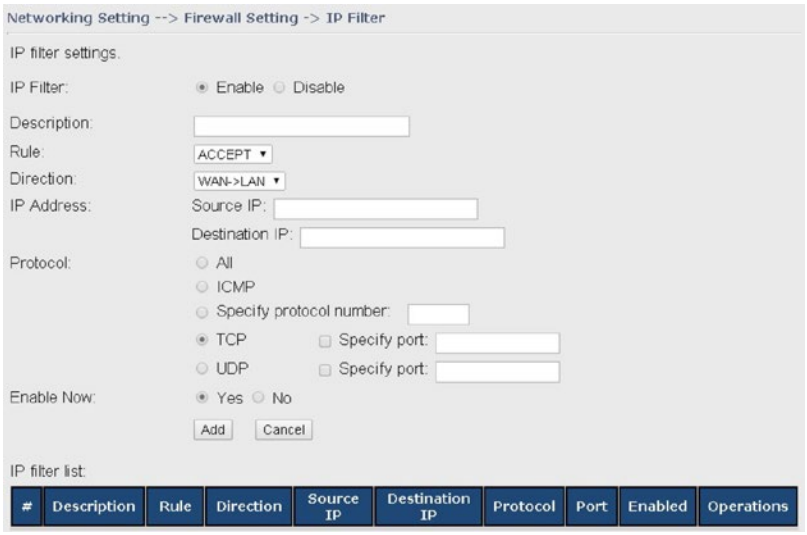
The UPnP (Universal Plug and Play) feature allows Internet devices to access local host resources or devices as needed. UPnP-enabled devices can be automatically discovered by the UPnP service application on the LAN.

Label	Description
UPnP	Enable or disable UPnP.
Enable NAT-PMP	NAT-PMP allows a computer in a private network (behind a NAT router) to automatically configure the router to allow parties outside the private network to contact with each other. NAT-PMP operates with UDP. It essentially automates the process of port forwarding. Check the box to enable NAT-PMP.
UPnP List	This table lists the current auto port forwarding information. Application: The application that generates this port forwarding. Ext Port: The port opened on WAN Protocol: The protocol type Int Port: The port redirected to the local computer IP Address: The IP address of local computer to be redirected to

Firewall Setting

IP Filter

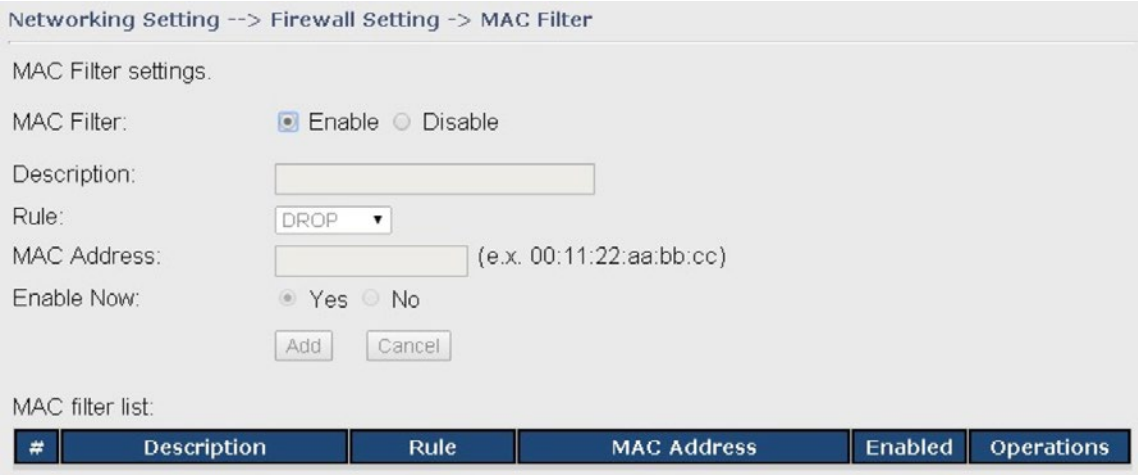
IP filters enable you to control the forwarding of incoming and outgoing data between your LAN and the Internet and within your LAN. This control is implemented via IP filter rules which are defined to block attempts by certain computers on your LAN to access certain types of data or Internet locations. You can also block incoming access to computers on your LAN.



Label	Description
IP Filter	Enables or disables the IP Filter
Description	Enter description for the entry.
Rule	Configures the rules to be applied to the IP filter. Available options include DROP, ACCEPT, and REJECT.
Direction	Specifies the direction of data flow to be filtered
IP Address	Enter the IP address of the source and destination computer
Protocol	Configures the protocol to be filtered
Enable Now	Click Yes to enable the entry after adding it
IP filter list	Shows the information of all IP filters. Click Edit to edit the entry or Del to delete the entry.

MAC Filter

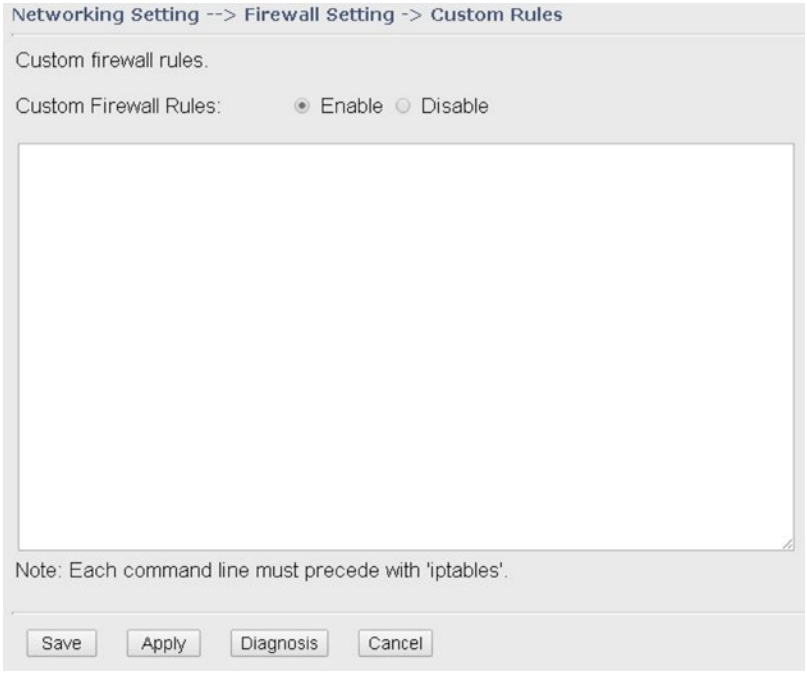
This page enables you to deny or allow LAN computers to access the Internet based on their MAC addresses.



Label	Description
MAC Filter	Enables or disables the MAC Filter
Description	Enter description for the entry
Rule	Configures the rules to be applied to the MAC filter. Available options include DROP, ACCEPT, and REJECT.
MAC Address	Enter the MAC address to be filtered
Enable Now	Click Yes to enable the entry after adding it
MAC filter list	Shows the information of all MAC filters. Click Edit to edit the entry or Del to delete the entry.

Custom Rules

Custom firewall rules provide more granular access control beyond LAN isolation. You can define a set of firewall rules that is evaluated for every request sent by a wireless user associated to that SSID. Firewall rules are evaluated from top to bottom. The first rule that matches is applied, and subsequent rules are not evaluated. If no rules match, the default rule (allow all traffic) is applied.



VPN Setting

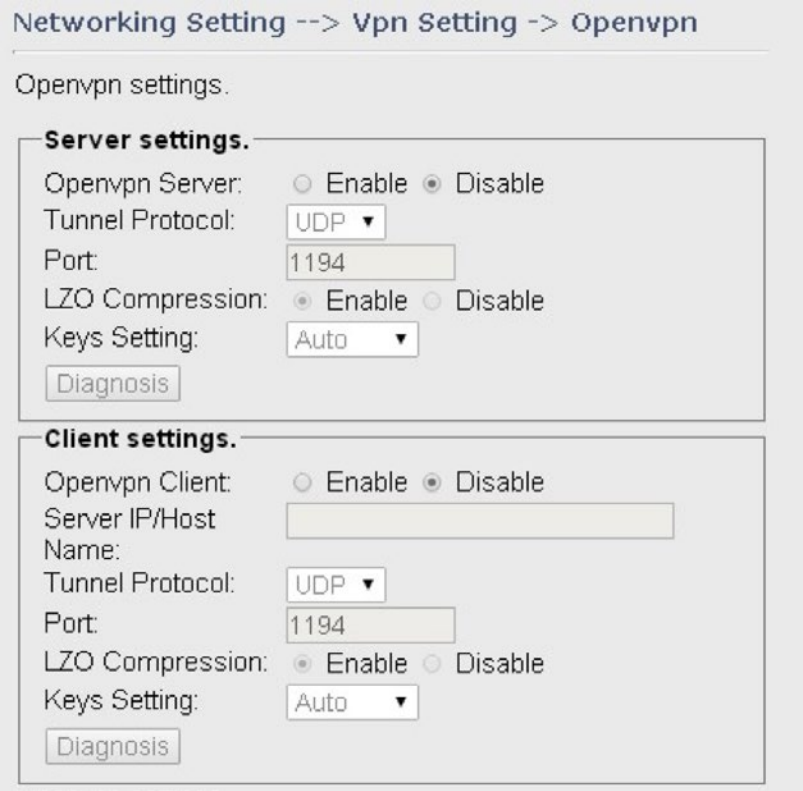
OpenVPN

A VPN is a method of linking two locations as if they are on a local private network to facilitate data transmission and ensure data security. The links between the locations are known as tunnels. VPN can achieve confidentiality, authentication, and integrity of data by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

Open VPN enables you to easily set up a virtual private network over an encrypted connection. It is a full-function SSL VPN solution which accommodates a wide range of configurations including remote access, site-to-site VPNs, WiFi security, and enterprise-level remote access with load balancing, failover, and fine-grained access control features.

To set up your router as an Open VPN server, you need to install OpenVPN client software for your Windows-based PC. You can download it from http://openvpn.net/download.html#stablel. The software version must match the current version of Openvpn used by the router which is version 2.0.9.

When you enable Open VPN Client, you need two routers to create site-to-site VPN connections. The server IP and client IP address should be within the same network domain.



Label	Description
OpenVPN Server	Enables or disables the function of Open VPN server
Tunnel Protocol	Select UDP or TCP protocol depending on your needs. TCP is more reliable than UDP, but UDP performs better than TCP. It is recommended to use UDP if the distance between VPN server and client is short; otherwise, use TCP.
Port	The number of the port (default is 1194).
LZO Compression	Enables or disables the function of LZO Compression
Keys Setting	Select Auto to use preset certificates or Manual to use your certificates. Please install OpenVPN client software to generate your certificates and paste them here. For more information, please visit OpenVPN website.
OpenVPN Client	Enables or disables the function of Open VPN client.
Server IP/Host Name	Enter the Open VPN server IP address
Tunnel Protocol	Select UDP or TCP protocol depending on your needs. TCP is more reliable than UDP, but UDP performs better than TCP. It is recommended to use UDP if the distance between VPN server and client is short; otherwise, use TCP.
Port	The number of the port (default is 1194).
LZO Compression	Enables or disables the LZO Compression
Keys Setting	Select Auto to use preset certificates or Manual to use your certificates. Please install OpenVPN client software to generate your certificates and paste them here. For more information, please visit OpenVPN website.

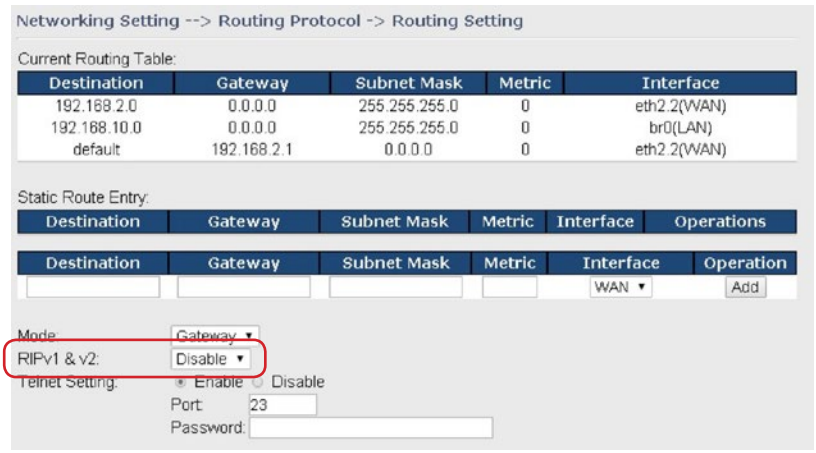
Routing Protocol

Routing Setting

This page shows the information of the routing table. You can configure static and dynamic routing settings in this page.

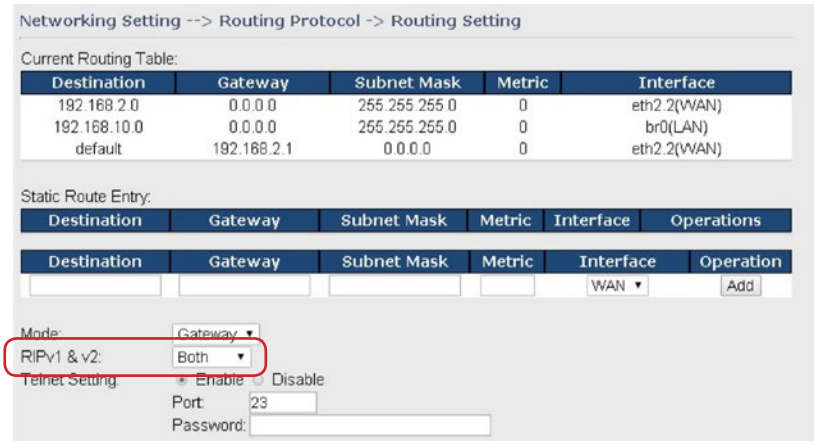
Static Routing

When RIPv1 & v2 is Disabled, the router will operate in static routing mode, which means routers forward packets using either route information from route table entries that you manually configure or the route information that is calculated using dynamic routing algorithms.

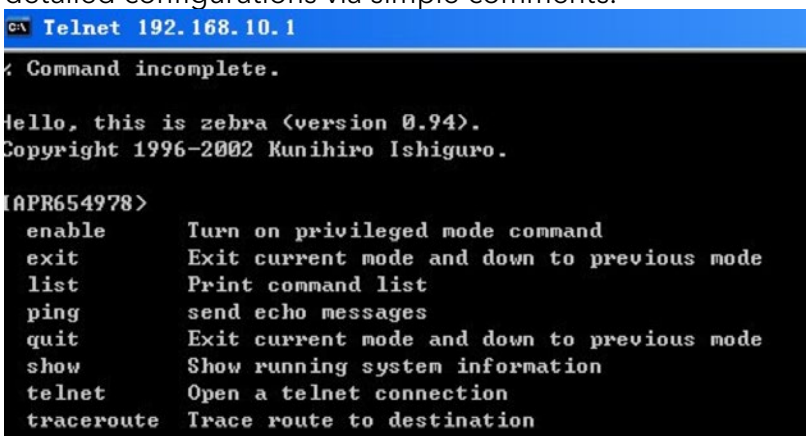


Dynamic routing lets routing tables in routers change as the routes change. If the best path to a destination cannot be used, dynamic routing protocols change routing tables when necessary to keep your network traffic moving. Dynamic routing protocols include RIP, OSPF, and BGP; however, the device only supports RIP (Routing Information Protocol).

Do not choose Disable in the RIPv1 & v2 list if you want to enable Dynamic Routing. After clicking Apply, more information will be displayed in Current Routing Table.



Label	Description
Current Routing Table	Shows all routing information, including static and dynamic routing (if enabled)
Static Route Entry	Fills in corresponding information to add new entries to the static routing tablet
Mode	Choose Router Mode if you want PCs in the LAN to visit external network, otherwise choose Router Mode
RIPv1 &v2	Choose Disable to disable dynamic routing or other options to configure the interfaces for dynamic routing
Telnet Setting	This option is only available when dynamic routing is enabled. It allows you to make detailed configurations via simple comments.



5.2.3 System Tools

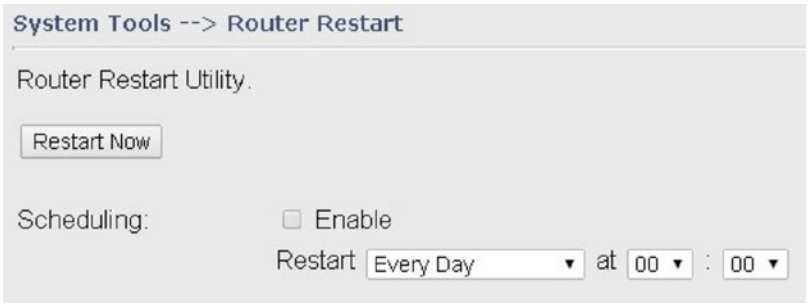
Login Setting

You can change login name and password in page. The default login name and password are both admin.

Label	Description
Old Name	Type in current login name
Old Password	Type in current password
New Name	Enter a new login name. Acceptable characters contain '0-9', 'a-z', 'A-Z' and the length must be 1 to 15 characters. An empty name is not acceptable.
New Password	Enter a new login password. Acceptable characters contain '0-9', 'a-z', 'A-Z' and the length must be 0 to 15 characters.
Confirm New Password	Retype the new password to confirm it.
Web Protocol	Choose a web management page protocol from HTTP and HTTPS. HTTPS (HTTP over SSL) encrypts data sent and received over the Web. Choose HTTPS if you want a secure connection.
Port	Choose a web management page port number. For HTTP, default port is 80. For HTTPS, default port is 443.

Router Restart

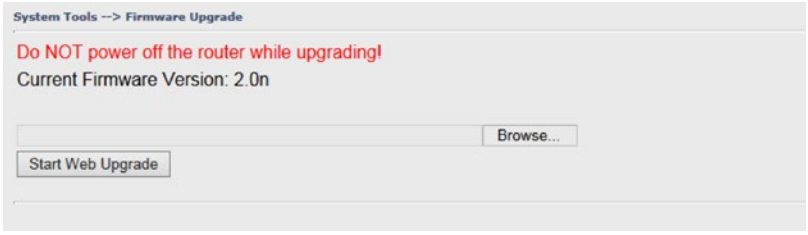
This page allows you to configure restart settings for the router.



Label	Description
Restart Now	Click to restart the router via warm reset
Scheduling	Enable: check to activate the setting Restart at: specify the time for resetting the router. You can configure the action to be performed periodically.

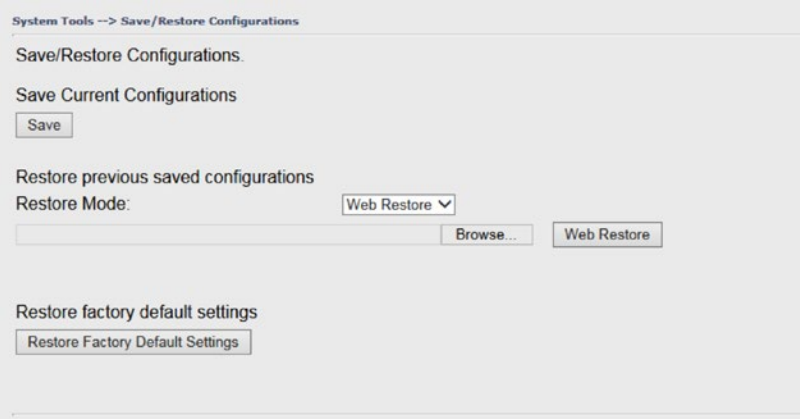
Firmware Upgrade

ComNet launches new firmware constantly to enhance router performance and functions. To upgrade firmware, download new firmware from ComNet's website to your PC and install it via Web upgrade. Make sure the firmware file matches the model of your router. It will take several minutes to upload and update the firmware. After upgrade completes successfully, reboot the router.



Save/Restore Configurations

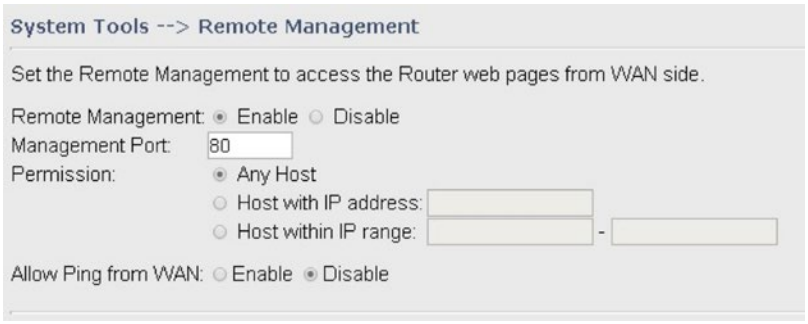
This page allows you to save configurations or return settings to previous status. You can download the configuration file from the Web. Note: users using old versions of Internet Explorer may have to click on the warning on top of the browser and choose Download File.



Label	Description
Save	Click to save existing configurations as a file for future usage.
Select File	You can restore configurations to previous status by installing a previous configuration file. To do this, choose Web Restore or TFTP Restore. If you choose Web Restore, you need to choose a file and click Web Restore. If you select TFTP Restore, fill in a TFTP server IP address and the file name before clicking TFTP Restore.
Restore Factory Default Setting	Click to reset the router to the factory settings. The router will reboot to validate the default settings.

Remote Management

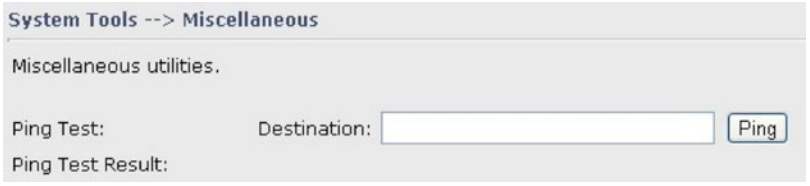
The page allows you to configure remote management settings.



Label	Description
Remote Management	Enables or disables remote management function
Management Port	Enter the port number that will be open to outside access. This port must be used when you establish a remote connection.
Permission	You can grant remote access to specific users. Tick Any Host or enter a hostname or IP address if you only want a specific computer or device to be able to access the device.
Allow Ping from WAN	Click Enable to allow system administrator to ping the router from WAN interface

Miscellaneous

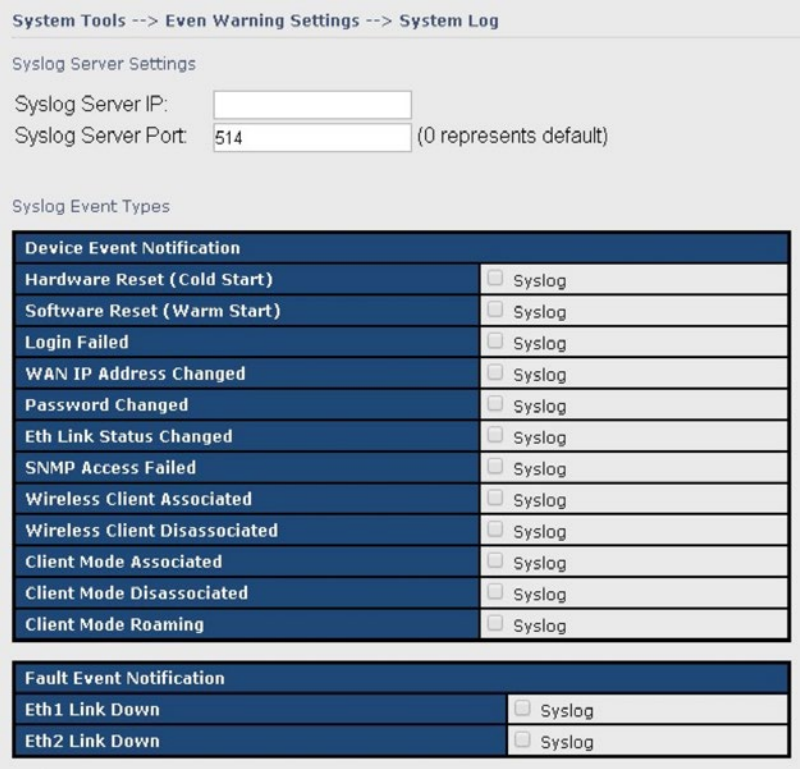
This page enables you to run ping test which will send out ping packets to test if a computer is on the Internet or if the WAN connection is OK. Enter a domain name or IP address in the destination box and click Ping to test.



Event Warning Setting

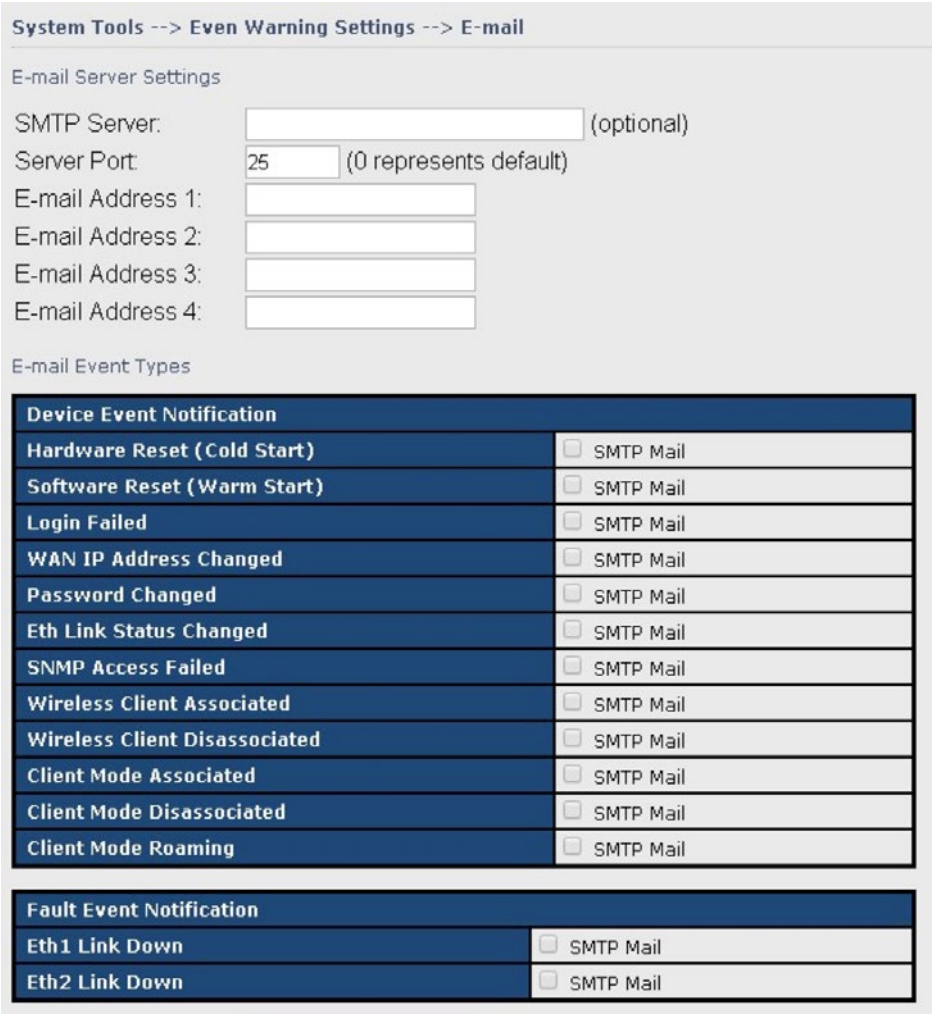
When an error occurs, the device will notify you through system log, and SNMP messages. You can configure the system to issue a notification when specific events occur by checking the box next to the event.

Syslog Server Settings



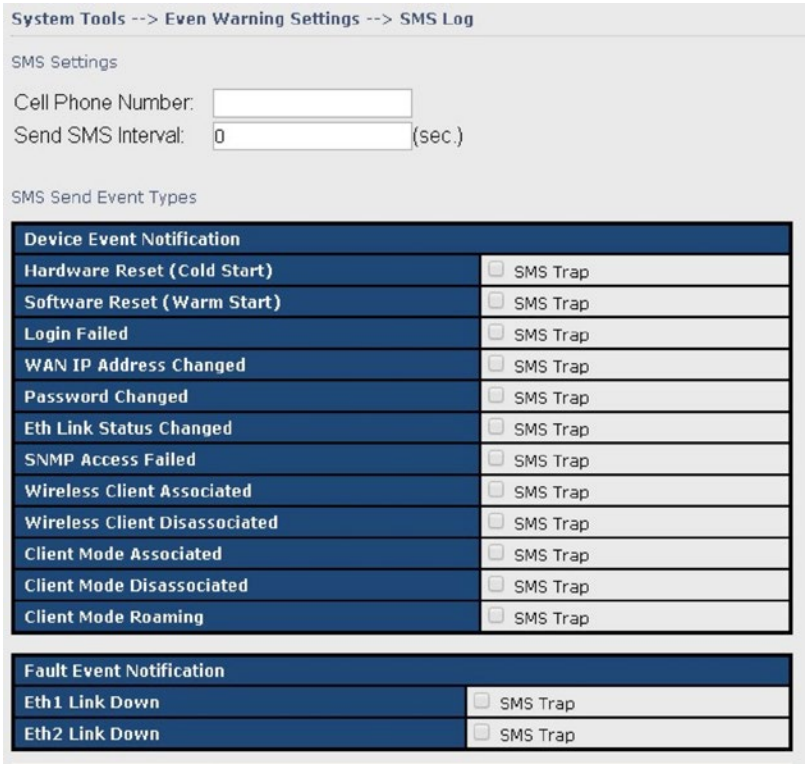
Label	Description
Syslog Server IP	Enter the IP address of a remote server if you want the logs to be stored remotely. Leave it blank will disable remote syslog.
Syslog Server Port	Specifies the port to be logged remotely. Default port is 514.

E-Mail



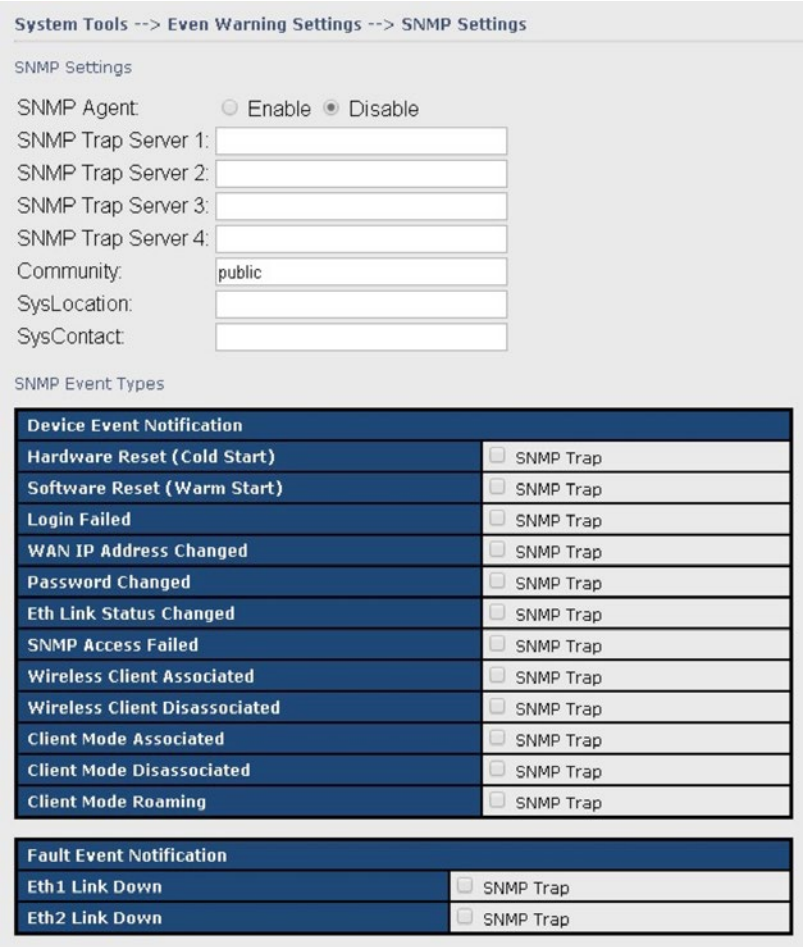
Label	Description
SMTP Server	Enter a backup host to be used when the primary host is unavailable.
Server Port	Specifies the port where MTA can be contacted via SMTP server
E-mail Address 1-4	Enter the mail address that will receive notifications

SMS



Label	Description
Cell Phone Number	Set Cell Phone Number.
Send SMS Interval	Set send interval

SNMP Settings

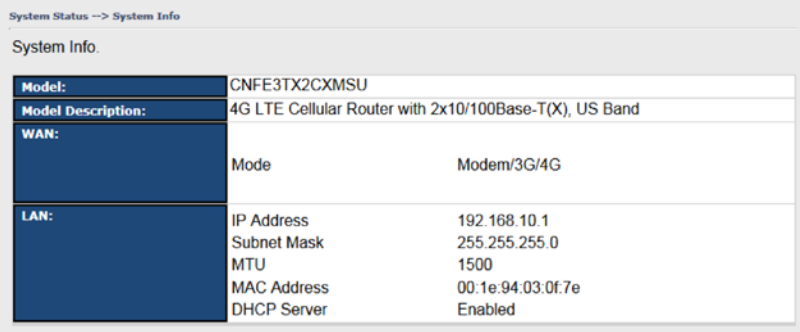


Label	Description
SNMP Agent	SNMP (Simple Network Management Protocol) Agent is a service program that runs on the access point. The agent provides management information to the NMS by keeping track of various operational aspects of the AP system. You can enable or disable the function.
SNMP Trap Server 1-4	Enter the IP address of the SNMP server which will send out traps generated by the AP.
Community	Community is a password to establish trust between managers and agents. Normally, public is used for read-write community.
SysLocation	Specifies sysLocation string
SysContact	Specifies sysContact string

5.2.4 System Status

System Info

This page displays the detailed information of the router including model name, description, firmware version, WAN, and LAN settings.

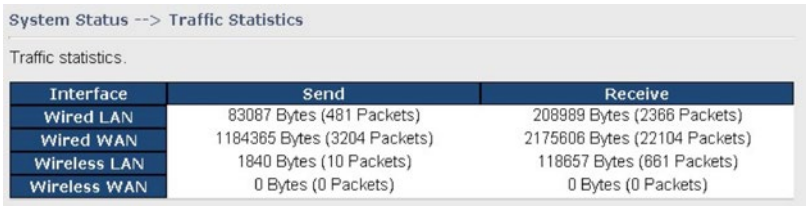


System Log

By checking in a specific box, the router will constantly log the events and provide the files for you to review. You can click Refresh to renew the page or Clear Logs to clear all or certain log entries.

Traffic Statistics

This page displays network traffic statistics for packets both received and transmitted through Ethernet ports and wireless connections.



ComNet Customer Service
Customer Care is ComNet Technology's global service center, where our professional staff is ready to answer your questions at any time.
Email ComNet Global Service Center: customercare@comnet.net

comnet
Communication Networks

3 CORPORATE DRIVE | DANBURY, CT 06810 | USA
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET
8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET

© 2018 Communications Networks Corporation. All Rights Reserved. "ComNet" and the "ComNet Logo" are registered trademarks of Communication Networks, LLC.