KORTEX

KX 4G INDUS ROUTER

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

Content

CHAPTER 1 INTRODUCTION **3**

1.1 PURPOSE 3
1.2 APPLICATION RANGE 3
1.3 VERSION 3
1.4 TECHNICAL SUPPORT 3

CHAPTER 2 PRODUCT SPECIFICATION **4**

2.1 OVERVIEW 4
2.2 SPECIFICATIONS 5
3.1 ACCESSORIES 8
3.2 INSTALLATION 9

CHAPTER 4 CONFIGURE **9**

4.1 OVERVIEW 9
4.2 CONNECTION 9
4.2.1 Computer network configuration *9*
4.2.2 Login the router *10*
4.3 TOP LEDS 11
4.4 REAR PANEL & FRONT PANEL 13
4.5 CONFIGURE PARAMETERS 14
4.5.1 Internet Settings *14*
4.5.2 WAN settings *15*
4.5.3 LAN settings *16*
4.5.4 VPN *18*
4.5.5 Static Routes *24*
4.5.6 Wireless settings *25*
4.5.6.1 Interface Configuration/ Wireless Security *27*
4.5.7 Firewall *31*
4.5.8 SMS *33*
4.5.9 Management *33*
4.5.10 Firmware & Backup / Restore *35*
4.5.11 Status *37*
4.5.12 Reboot *38*
4.5.13 Remote Sms *38*
4.5.14 Telnet *39*

CHAPTER 5 FAQ **40**

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

Chapter 1 Introduction

Here to introduce the KX 4G INDUS ROUTER, it will be much helpful during your application.

1. Purpose
2. Application range
3. Version
4. Technical support

1.1 Purpose

The user manual will be used for your installation and test.

1.2 Application range

This manual is intended for persons with certain computer networks and electronic technical knowledge, network administrators, and other related equipment managers who need to use the KX 4G INDUS ROUTER.

1.3 Version

According to the market and the needs of users, the router products will make adjustments on related features and technical improvements. The following table explains product specifications and amendments in the revised version of the reasons described in different periods.

Version No.	Amendment	Participation	Date	Details
V1.0	R&D	Market, Technical Dep.	2019.02	First Version

1.4 Technical support

To enable users to quickly solve problems encountered in the course, and get the right solution on hardware, operating system and installation, please contact customer service staff: **France : 0820 69 00 42 International : +33134043760**

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

Chapter 2 Product specification

2.1 Overview

With the development of mobile communication technology, the mobile data communication network using GPRS/CDMA/EDGE/EVDO/HSDPA/HSUPA/HSPA+/LTE has covered many regions in the world. And network is very stable.

All these make a large market for wireless terminals. Different industries have different applications and different information needs, so the industry application solutions provided by the mobile communication operators must satisfy both the common needs and the special individual needs of the industry users perfectly.

Therefore, in recent two years, based on the needs of industry users, Telecommunication, Telecom Operator do innovative practice energetically in mobile application and provide solutions to meet the unique needs of the users.

Being different with the popular data requirements, industry application is very professional. Different industry users need different terminals. So hardware and software development and system integration must be accord with different industry needs.

By analyzing the different industry application features in recent years and according to the network features and the actual condition of the network operators, we launched the individually designed KX 4G INDUS ROUTER.

KX 4G INDUS ROUTER provide users the high-speed, the security with VPN, always-online and transparent-data-transmission communication network, to meet the needs of Electronic Power System Automation, Industry Monitoring, Transportation Management, Weather, Environment Protection, Pipe Network Monitoring, Finance, Bond industries and pos terminals.

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

2.2 Specifications

- **4G Router CPU MT7620 :**
  - RAM : 128 Mo (64Mo x 16)
  - FLASH :16 Mo
- **4G Module cellular characteristics :**
  - 4G LTE FDD frequencies
    - Lane 1: 2100 MHz
    - Band 3: 1800 MHz
    - Lane 7: 2600 MHz
    - Lane 8: 900 MHz
    - Strip 20: 800 MHz
  - 4G LTE TDD frequency
    - Strip 40 2600 MHz other countries (Lithuania (Mezon), Russia (Tele2, Telecom Vainah)
  - LTE-FDD Flow
    - Up to 100 Mbps downstream and 50Mbps transmission
  - LTE-TDD Flow
    - Up to 61 Mbps downstream and 18Mbps for transmission
- **WIFI CPU integrated :**
  - Wi-Fi: b/g/n ISM Band: 2.400GHz ~ 2.4835GHz
  - 802.11a : 6, 9, 12, 18, 24, 36, 48, 54 Mb/s
  - 802.11b : 1, 2, 5.5, 11 Mb/s
  - 802.11g : 6, 9, 12, 18, 24, 36, 48, 54 Mb/s
  - 802.11n : up to 300 Mb/s
  - 802.11ac : up to 433 Mb/s
  - **Output Power & Sensitivity Gain (5GHz)**
    - 11a(6bps): 18±1.5dBm
    - 11a(54bps): 14±1.5dBm
    - 11n(20MHz, MCS7): 13±1.5dBm
    - 11n(40MHz, MCS7): 13±1.5dBm
    - 11ac(80MHz, MCS9): 13±1.5dBm
    - Receive Sensitivity
      - 11a(6Mbps): - 90±2dBm
      - 11a(54Mbps): - 71±2dBm
      - 11n(20MHz, MCS7): - 69±2dBm
      - 11n(40MHz, MCS7): - 65±2dBm
      - 11ac(80MHz, MCS9): -55±2dBm
  - **Output Power & Sensitivity Gain (2,4GHz)**
    - 11b (1Mbps): 18±1.5dBm
    - 11b (11Mbps): 16±1.5dBm
    - 11g (54Mbps): 14±1.5dBm

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

- 11n (20MHz, MCS7): 13±1.5dBm
- 11n (40MHz, MCS7): 13±1.5dBm
- Receive Sensitivity
  - 11b(1Mbps): - 91±2dBm
  - 11b(11Mbps): - 87±2dBm
  - 11g (54Mbps): - 71±2dBm
  - 11n(20MHz, MCS7): - 68±2dBm
  - 11n(40MHz, MCS7): - 65±2dBm
- Security:
  - 64/128-bits WEP, WPA, WPA2

4G Router Power Input :

- Input DC 8-30V, standard DC 12V adapter
- Power consumption Block 12V DC 2A 5% 24.0W (max)/Input 100 to 240VAC
- Frequency 50/60 Hz / Power range 8V to 30V 24.0W max
- Low-voltage, over current, over voltage, anti-reverse protection

4G Router Environment :

- Storage Temperature：-40℃～85℃
- Work Temperature：-40℃～70℃
- Humidity：5%～95 relative 10%～90

4G Router Volume :

- L*W*H：73.4*125*27.6mm (without antenna)

4G Router Weight :

- Net weight（no accessories）:275g

4G Router Data Interface :

- 1 WAN, 1 LAN or 2 LAN 10/100Mb RJ45

4G Router EMC

- Electrostatic discharge immunity：EN6100-4-2，level 2
- RFEMS： EN6100-4-3, level 2
- Surge：EN6100-4-3, level 2
- PFMF：EN6100-4-6, level 2
- Shockwave immunity：EN6100-4-8, Horizontal / vertical direction 400A/m (>level 2)

4G Router Physical property

- Shockproof：IEC60068-2-27
- Drop test：IEC60068-2-32
- Vibration test：IEC60068-2-6

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

- **4G Router Applications area**
  - Pos terminals
  - Urban Smart Panels
  - ATM terminals access internet
  - Video surveillance
  - Environment monitor
  - Remote meter reading
  - Distribution automation
  - Outdoor LED
  - Smart home
  - Oil monitor
  - Car video surveillance (Coach, bus)
  - Road Traffic

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

Chapter 3 Installation

Here you can see the appearance of KX 4G INDUS ROUTER, and how to install.

3.1 Accessories

Name	Unit	No.	Description	Photo
KX 4G INDUS ROUTER	pc	1	router	
Power	pc	1	standard	
Antenna	pc	4	2 External for Wi-Fi and 2 for 3G / 4G. SMA connectors.	
RJ45 cable	pc	1	standard	
User manual	pc	1	standard	PDF Format on www.kortex-psi.fr

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

3.2 Installation

KX 4G INDUS ROUTER must be properly installed and configured to meet the design features.

Note: Please install the router and SIM card before inputting power.

Chapter 4 Configure

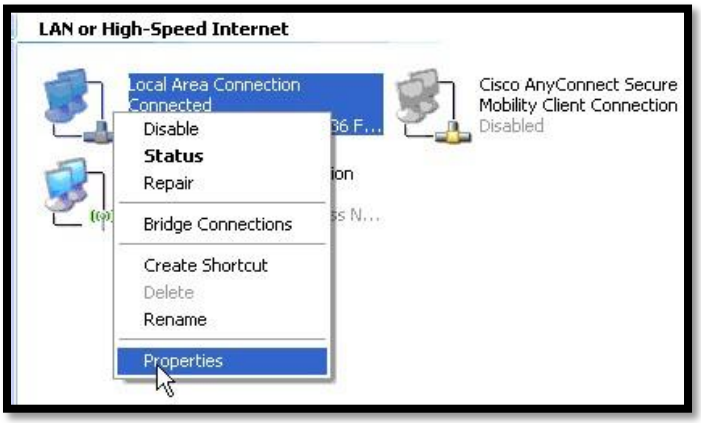
4.1 Overview

The router has its own webpage for parameter settings. You can access the router by the following way.

4.2 Connection

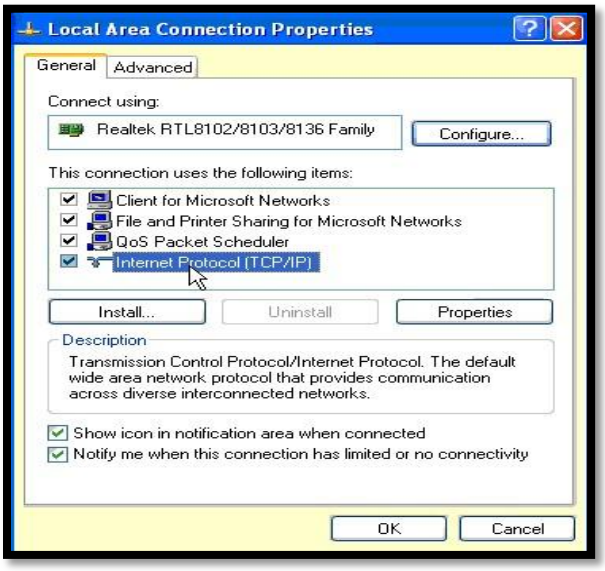
4.2.1 Computer network configuration

Find “Local Area Connection”, and choose “Properties”.

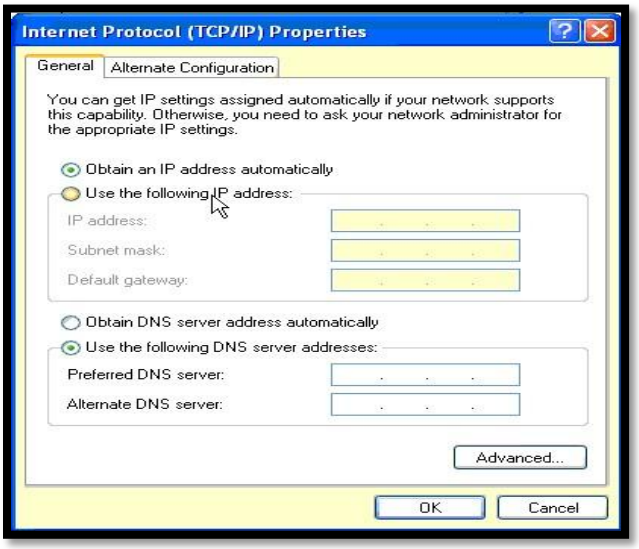


Choose “Internet Protocol”.

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62



Choose automatically or input IP manually.

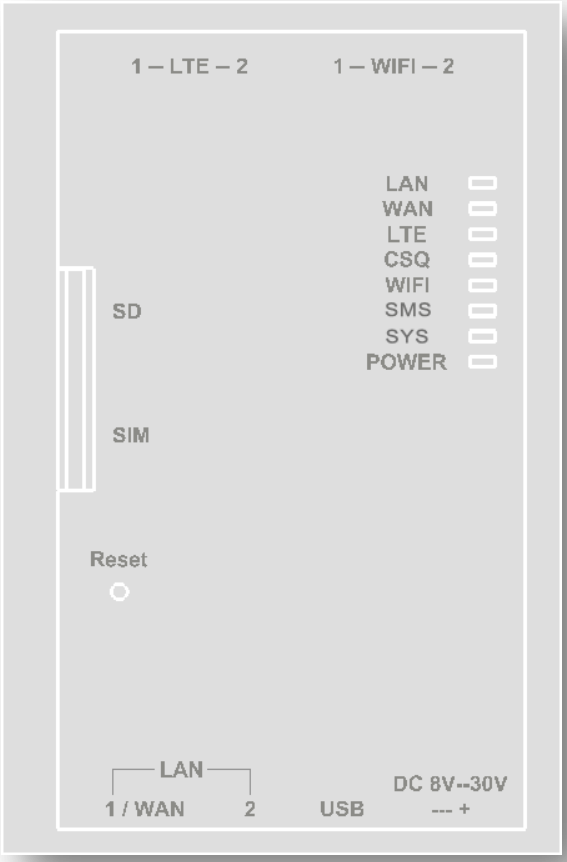


4.2.2 Login the router

- Open the Web browser, and type **http://192.168.8.1** into the address field and press Enter button in your computer keyboard.
- Type User Name "root" and Password "kxpro75002" in the pop-up Login Window, and then press the "OK" button. We strongly recommend that you change the default username and password.

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.3 Top LEDs

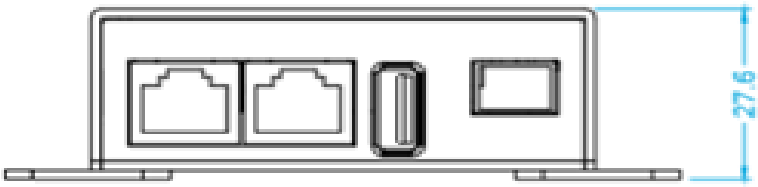


91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

LED		Meaning
1	**POWER**	Lit when power is ON.
2	**SYS**	Flash when the firmware is running.
3	**SMS**	Lit when a SMS is received. Used for remote monitoring.
4	**WIFI**	Lit when the Wi-Fi function is enabled (default). Flash when the data is transmitting. Off when the Wi-Fi function is disabled.
5	**CSQ**	Lit when the signal level is more than 15 Db.
6	**LTE**	Lit when the router is attached to the networks. Flash when the data is transmitting in 3G/4G networks. Off when dialup is disconnected.
5	**WAN**	Lit when the cable connection with device exists. Flash when the data is transmitting. Off when no cable connection exists.
5	**LAN**	Lit when the cable connection with device exists. Flash when the data is transmitting. Off when no cable connection exists.
2	**RESET**	After the device is powered on, press the reset button to restore to factory default settings. **10 seconds above**: restore to factory default settings (this is used when you cannot login to the router. **E.g. forgot the password**).

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.4 Rear Panel & Front Panel



Items		Meaning
1	**1/ WAN (RJ-45 connector)**	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to the WAN ports when connecting to a xDSL router or an office/home network of 10Mbps, 100Mbps.
2	**LAN 1X — 2X (RJ-45 connector)**	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
3	**USB**	Connect a USB Slave.
4	**DC 8V-30V**	Connect the supplied power adapter to this industrial connector.
5	**ANTENNA CONNECTOR**	Connect 2 SMA antennas for 3G/4G and WIFI.
6	**SD / SIM**	Insert a SIM into the SIM card holder. SD card is an option to store Data. Depend of the firmware.

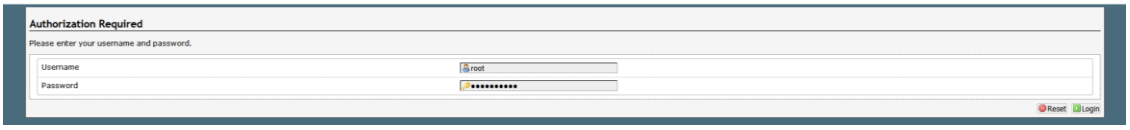
91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

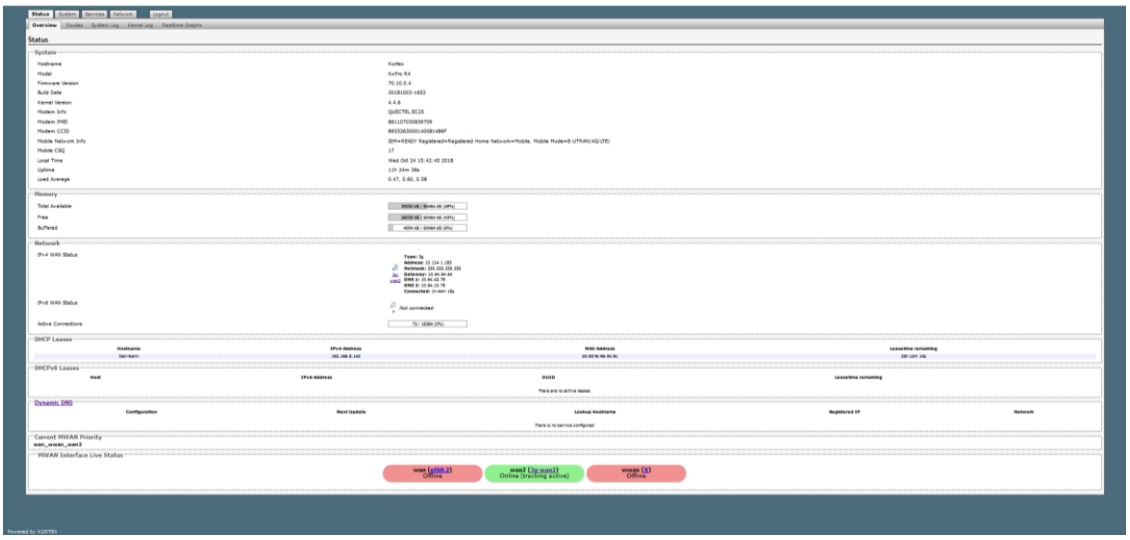
4.5 Configure Parameters

4.5.1 Internet Settings

After entering the "Username" and "password", click on the "Login" Button, then you can display the status page.

At the bottom, the MWAN Interface Live Status indicate witch WAN is active. Report to the next Wan Setting section in order to configure the connection parameters.

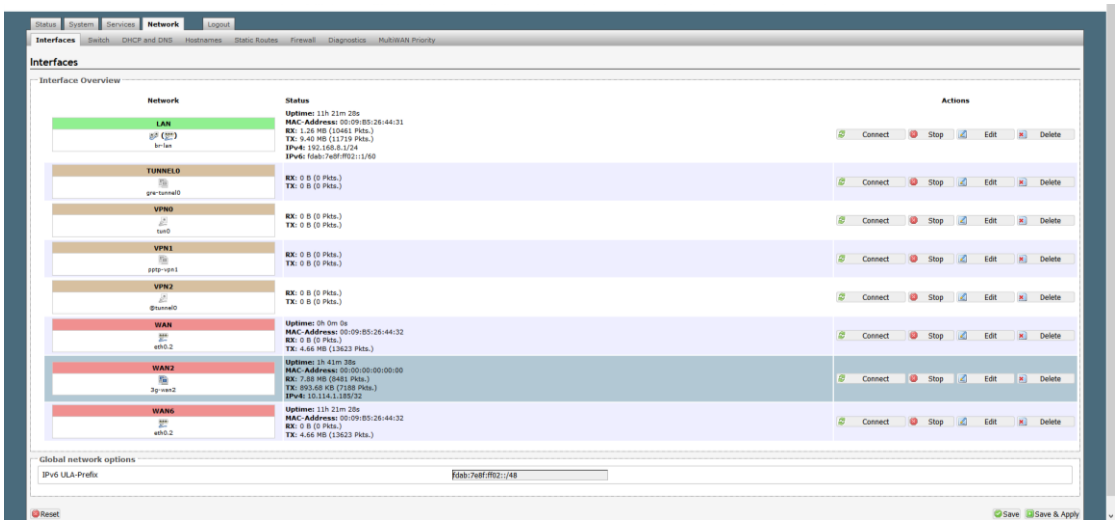


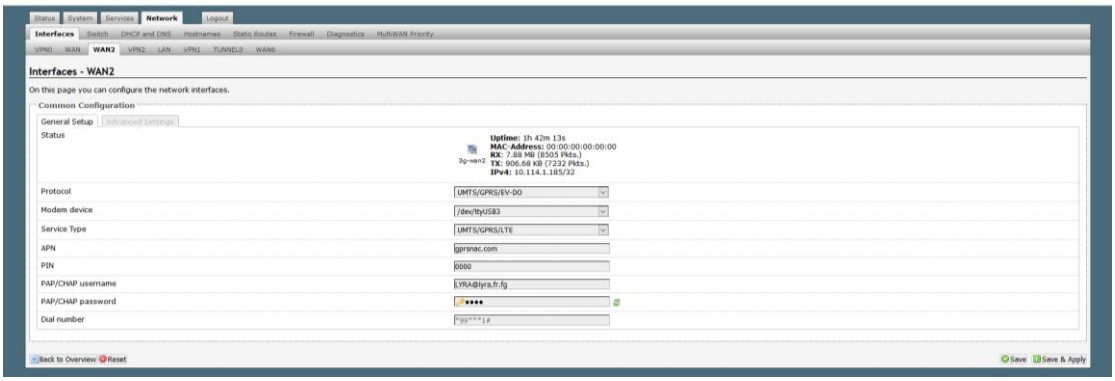


91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.5.2 WAN settings

The WAN (Wide Area Network) section is where you configure your Internet connection type. The KX 4G INDUS ROUTER supports 3G / 4G dialup connection type to access Internet. Please contact your Internet Service Provider before configuring the required parameters.





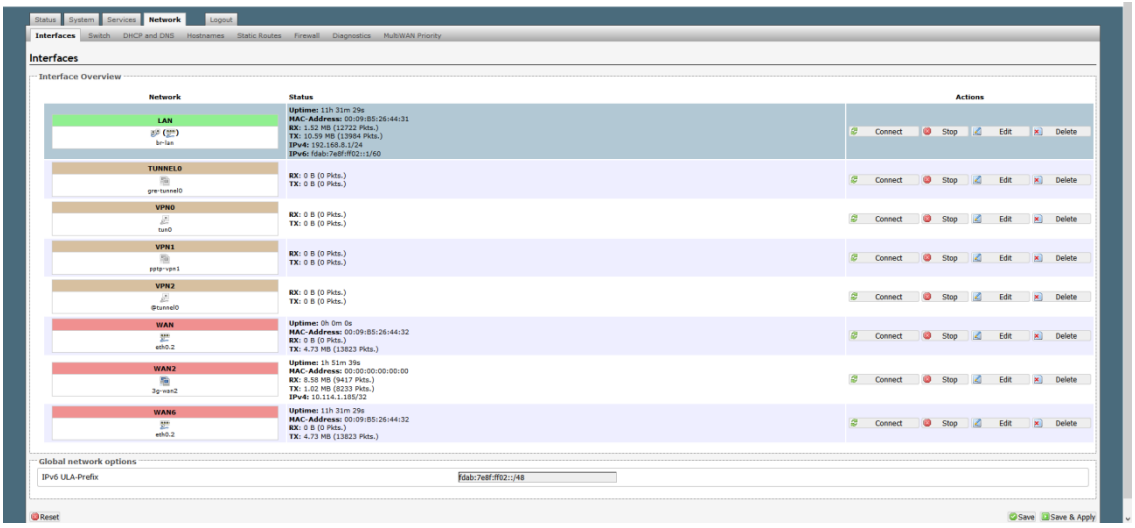
Interfaces - WAN2

- **Protocol:** UMTS/GPRS/EV-DO
- **Modem device:** /dev/ttyUSB3
- **Service Type:** UMTS/GPRS/LTE
- **APN:** (Access Point Name).This SIM Card APN name is from Mobile Management Service Provider.
- **PIN**: 0000 enter the Pin code of your SIM card
- **PAP / CHAP Username:** input it if ISP offers
- **PAP / CHAP Password:** input it if ISP offers
- **Dial Number**: Input the Dialing Number you get from ISP. Default is *99***1#.

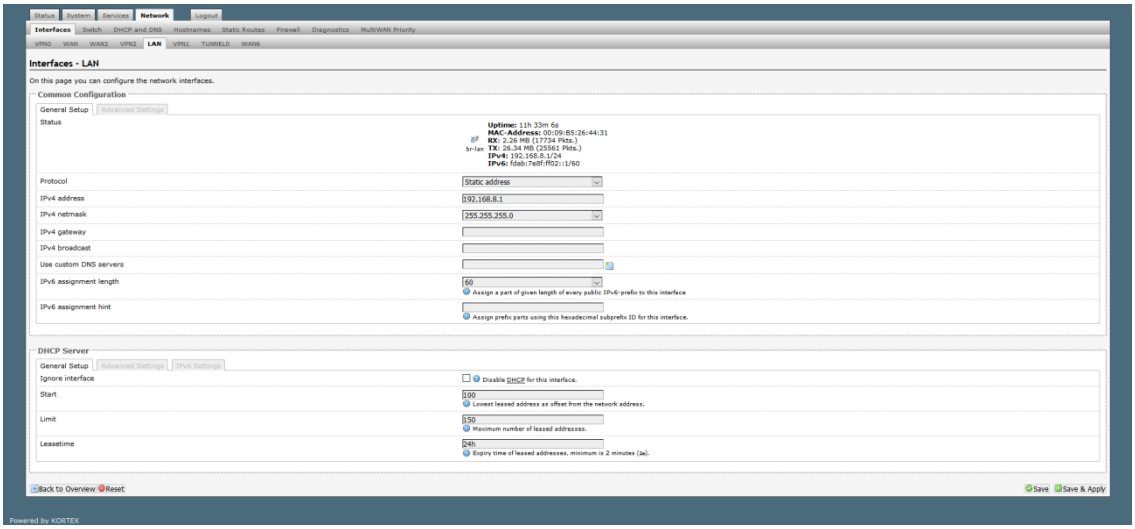
91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.5.3 LAN settings

These are the settings of the LAN (Local Area Network) interface for the router. The router's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this web-based management interface. It is recommended that you use the default settings if you do not have an existing network.



Setting the LAN parameters, include IP Address, Subnet Mask, DHCP, etc...



91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

Protocol: Static address (default). Choose the protocol you need.
IPv4 Address: The IP address of your router's LAN port. Default: **192.168.8.1**.
IPv4 netmask: Subnet Mask of your LAN. Default: 255.255.255.0.
IPv4 Gateway: Empty field.
IPv4 Broadcast: Empty field.
Use custom DNS servers: Empty field. Add your own DNS server.
IPv6 assignment length: 60. Assign a part of given length of every public IPv6-prefix to this interface.
IPv6 assignment hint: Empty field. Assign prefix parts using this hexadecimal sub prefix ID for this interface.

All devices on the network must have the same subnet mask to communicate on the network.

DHCP SERVER
DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN).

Start: Specify the DHCP Client IP address that will start.
Limit: Specify DHCP Client IP address that will end.

Note: The number of the "Limit" must be greater than "Start", and cannot be the same as the router's IP address.

Lease Time: Default 24 hours. Designate the amount of the time for the device to recycle and give out the IP addresses to the devices in your network. Expiry time of leased addresses, minimum is 2 minutes (2m).

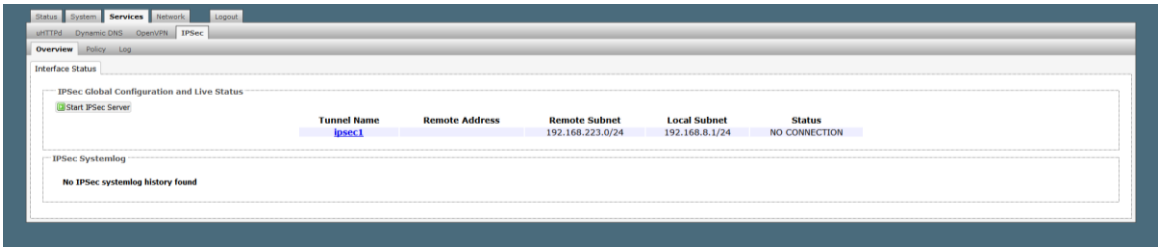
91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.5.4 VPN

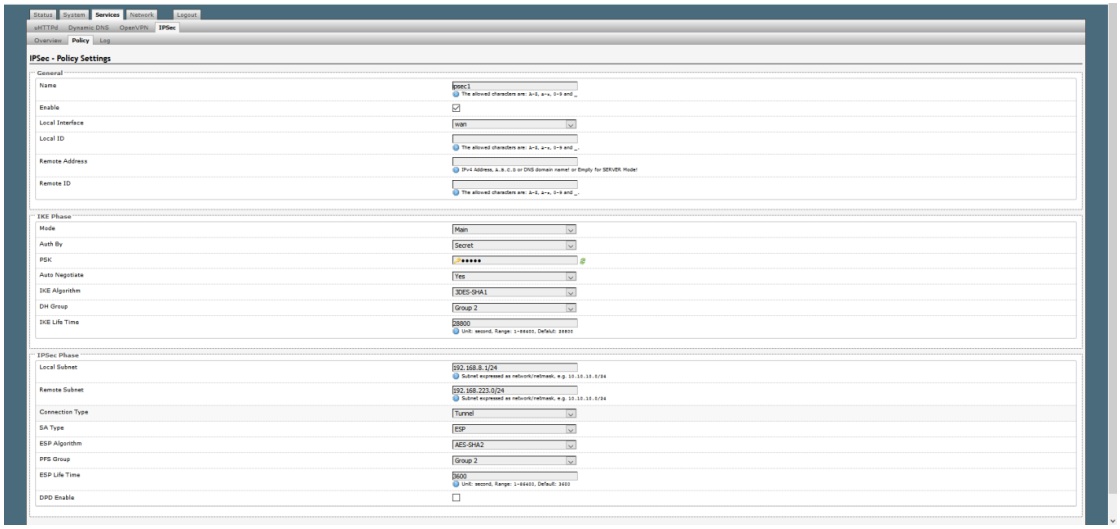
VPN (Virtual Private Network) is a method for secure data transfer through unsafe public network. This chapter explains how to configure IPSEC & Open VPN, which are integrated on the KX 4G INDUS ROUTER.

4.5.4.1 IPSEC

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).



Click on "Edit" to create the VPN Configuration.



General Settings

Name: Give a name to your VPN Tunnel (e.g. “KORTEX VPN OFFICE”).The allowed characters are: A-Z, a-z, 0-9 and _.

Enable: Check to activate the tunnel.

Local Interface: Select the set used interface for the IPSec connection, when you select WAN, WWAN, WAN2 interface, the IPSec tunnel would transmit data via this interface to connect to the remote peer.

Local ID: When the mode of IKE is aggressive, Local and Remote peers can be identified by other IDs. The allowed characters are: A-Z, a-z, 0-9 and _.

Remote Address: The WAN IP address of the remote VPN gateway that is to be connected, establishing a VPN tunnel.

Remote ID: When the mode of IKE is aggressive, Local and Remote peers can be identified by other IDs. The allowed characters are: A-Z, a-z, 0-9 and _.

IKE Phase

Mode: IKE, Internet Key Exchange, is the mechanism to negotiate and exchange parameters and keys between IPSec peers to establish security associations(SA). Select Main or Aggressive mode.

Auth By: Method of authentication, Secret.

PSK: Pre-Shared Key. This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Auto Negotiate: Default auto. Select from the drop-down menu if you want to change.

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

IKE Algorithm :

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are 3 options: 3DES, DES and AES 256. 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES 256:** Stands for Advanced Encryption Standards, 256 bits as encryption method.

Authentication Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA2). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.
- **SHA2:** A one-way hashing algorithm. It includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.

DH Group: Diffie-Hellman Group. It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). Select from the drop-down menu if you want to change the group 1, 2,5. DH Group 1: 768-bit group, DH Group 2: 1024-bit group, DH Group 5: 1536-bit group.

IKE Life Time: Specify the lifetime (in seconds) of an IKE security association (SA). When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated. Unit: second, Range: 1-86400, Default: 28800.

IPSec Phase :

Local Subnet: Set the IP address or subnet of the local network. Local Subnet expressed as network/netmask, e.g. 10.10.10.0/24.
Remote Subnet: Set the IP address or subnet of the remote network. Local Subnet expressed as network/netmask, e.g. 10.10.10.0/24.
Connection Type: VPN mode, Tunnel.
SA Type: Select the IPSec security method. There are two methods of verifying the authentication information, AH (Authentication Header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and the data origin be authenticated but using AH data origin will only be authenticated but not encrypted.

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

ESP Algorithm :

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are 3 options: 3DES, DES and AES. 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

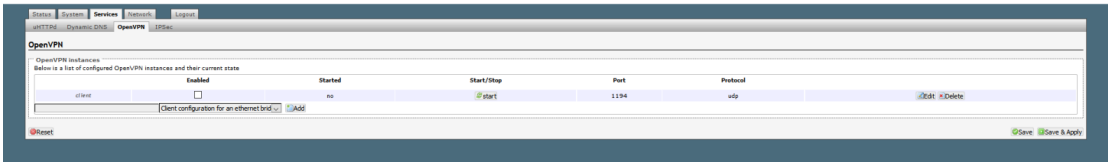
Authentication Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA2). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.
- **SHA2:** A one-way hashing algorithm. It includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.

PFS Group: PFS (Perfect Forward Secrecy) group must match with another incoming connection to establish IPSec. Select from the drop-down menu if you want to change the group 1, 2,5. DH Group 1: 768-bit group, DH Group 2: 1024-bit group, DH Group 5: 1536-bit group.
ESP Life Time: The time duration for phase.
DPD enable: Dead peer detection (DPD) is a keeping alive mechanism that enables the router to be detected lively when the connection between the router and a remote IPSec peer has lost. Please be noted, it must be enabled on the both sites.

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.5.4.2 OPEN VPN

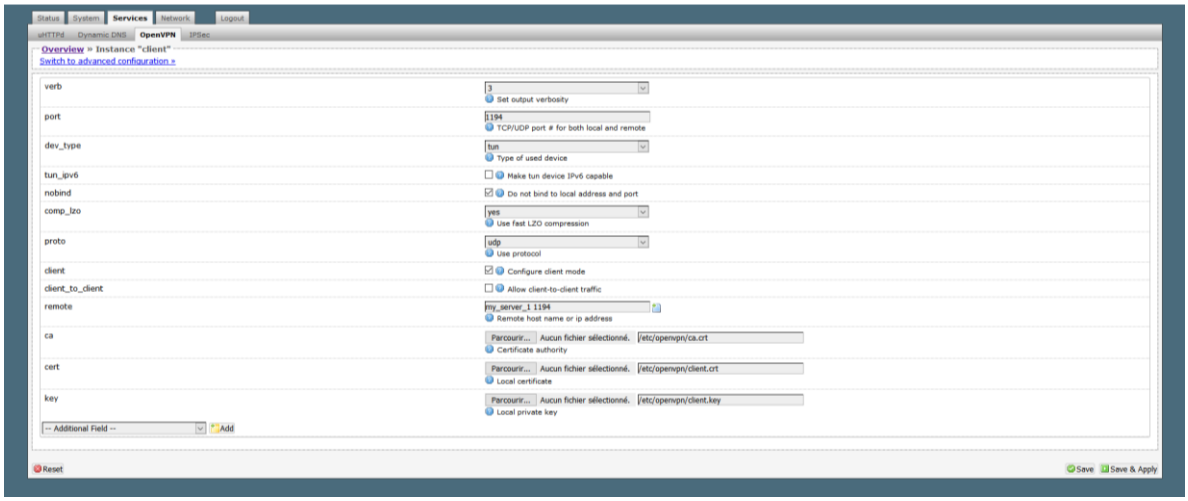


Click on "Edit" to create the VPN Configuration.

Default (TUN) Server: The simplest type of Open VPN server to configure, clients are exclusively managed by Open VPN and can be assigned IP addresses by the Open VPN server under their own distinct subnet.

Server-Bridge (TAP) Server: Also called an Ethernet-bridge, this configuration creates a virtual Ethernet cable between the server and client. This means that clients will be treated by the router as if they were plugged into it like any other computer. They will be assigned an IP address by the network's DHCP server (most commonly the router itself).

Client: Open VPN will act as a client and connect to a remote server.



Verb: Set output verbosity 0-11.
Port : Defines TCP or UDP port number (make sure, that this port allowed by firewall).
Dev_Type: Set output verbosity TUN or TAP.
Tun_ipv6: Make tun device IPv6 capable.
Nobind: Do not bind to local address and port.

Comp_lzo: Use fast LZO compression. Select yes, no or adaptive.
Use protocol, Proto: Udp, Udp6, Tcp,Tcp6.
Client: Configure client mode.

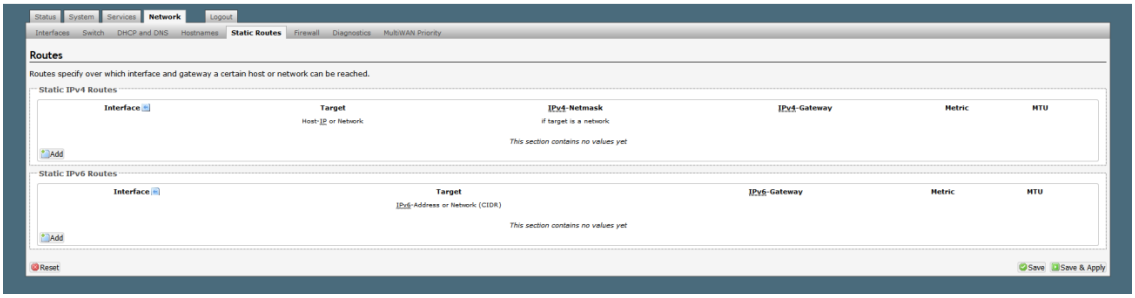
91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

Client_to_client: Allow client-to-client traffic.
Remote: Remote host name or IP address.
Ca: Certificate authority.
Cert: Local certificate.
Key: Local private key.
Additionnal Field: Select the field you need to add. (nice, ifconfig, Server, Server Bridge, Keepalive, secret, key_direction, pkcs12, dh).

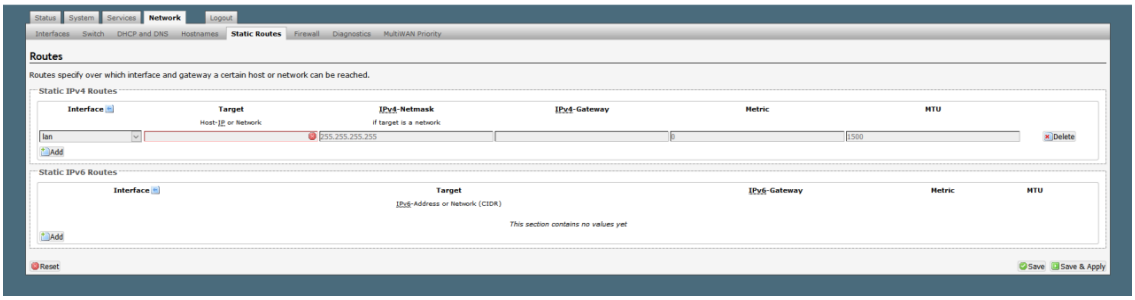
91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.5.5 Static Routes

This section mainly introduces what is Routing Table and how to configure static routing.

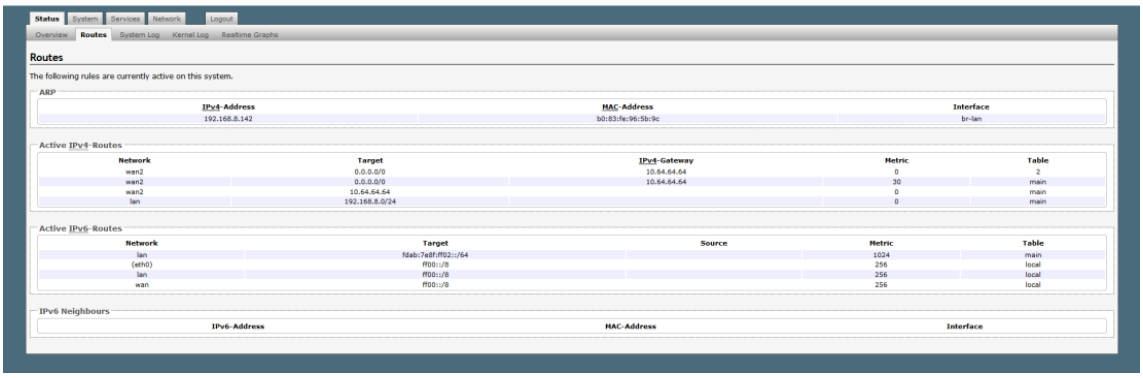


Click on Add to create the static routes.



4.5.5.1 Routing Table

This page shows the key routing table of this router. In Static Routing Settings, the user can set up a route rule (table) here. Refer to the description of the following parameters to set up the necessary route rule.



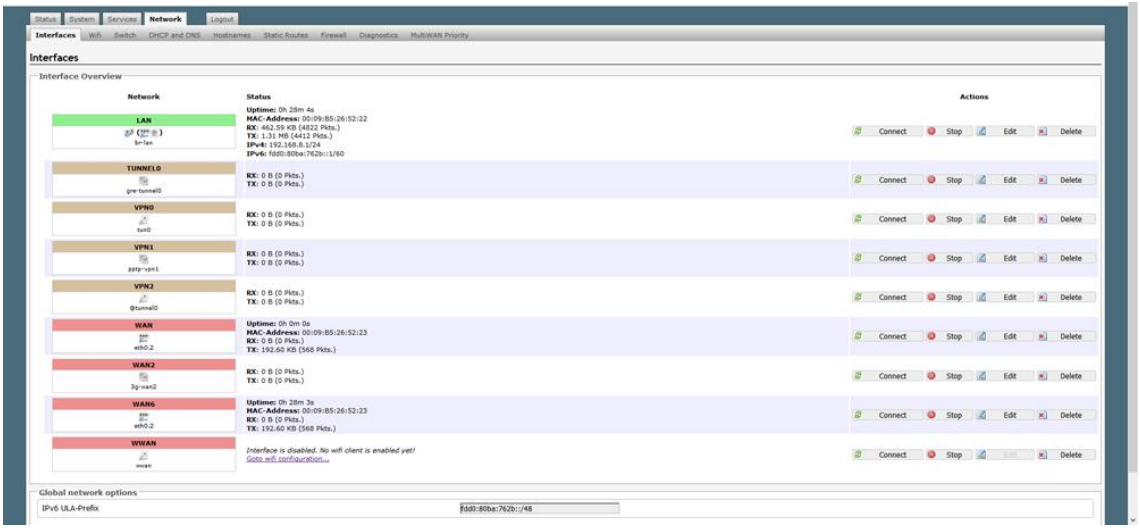
91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

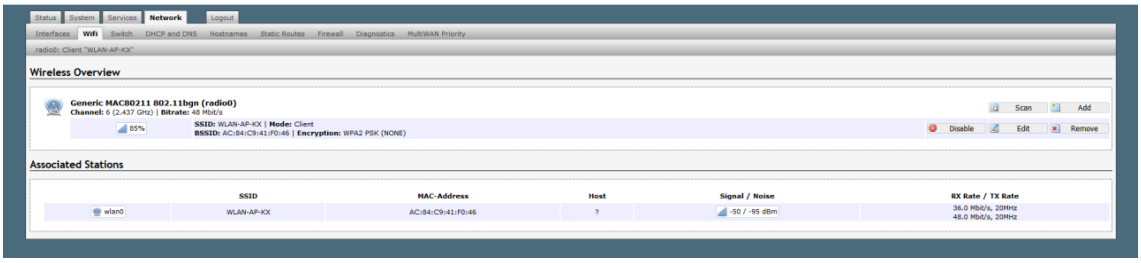
4.5.6 Wireless settings

4.5.6.1 Basic Wireless Settings

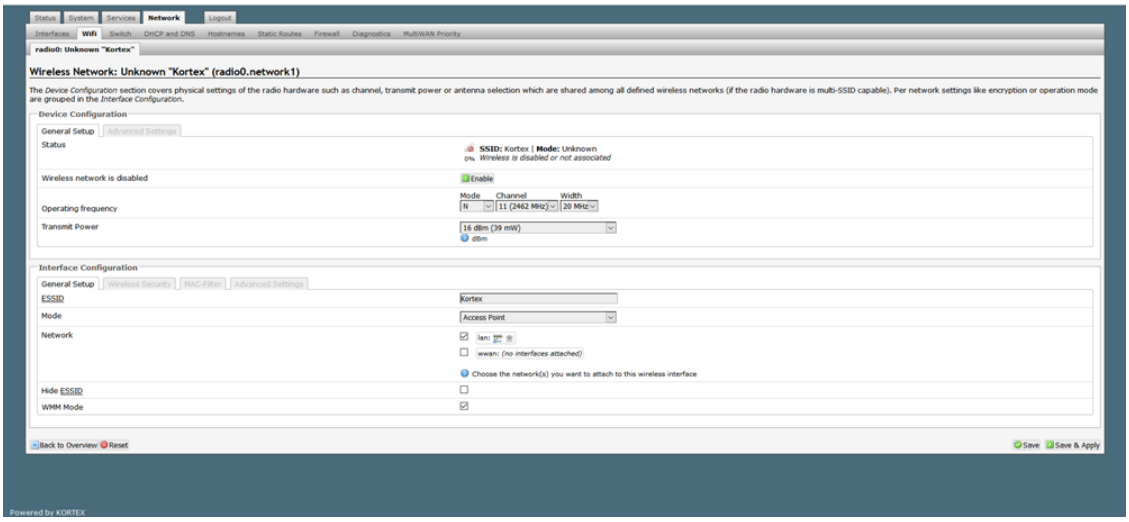
The wireless section is used to configure the wireless settings for your Company router. Please note that changes made on this section may also need to be duplicated on your Wireless Client. To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: WEP, WPA-PSK, and WPA2-PSK. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-PSK does not require an authentication server. The WPA2-PSK option does require a RADIUS authentication server.

Through the wireless setting page, the user can control the Enable/Disable status of Wi-Fi function, and set up the 802.11 mode, Network Name (SSID) as well as Channel. Besides, you can do the further settings related to the HT Physical Mode.





91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62



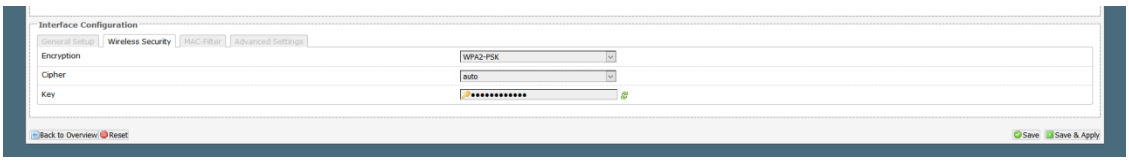
Wireless Network Settings:

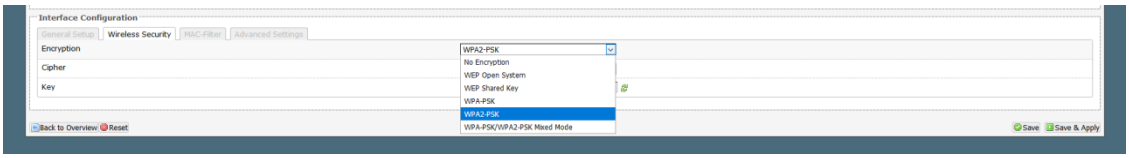
Status: Display the Wi-Fi status information SSID and Mode.
Wi-Fi Enable / Disable: This option turns on and off the wireless connection feature of the router. Simply click on the **Enable / Disable** button. The system will automatically detect the current status of the router and switch the button accordingly.
Operating Frequency: A wireless network uses specific channels in the 2.4GHz wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network. If you select **Auto**, the router automatically finds the channel with least interference and uses that channel for wireless networking.
Transmit Power: Adjust the transmit power from 0 dBm (1mw) to 16 dBm (39mw).
ESSID: (Network Name)**.** When you are browsing for available wireless networks, this is the name that will appear in the list (unless you set it to Hidden, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name. Kortex is Default Wi-Fi.
Mode: Choose the operation mode needed. Access Point (Default).
Network: Choose the network(s) you want to attach to this wireless interface..
Hide ESSID: The option allows you to hide your wireless network. When this option is unchecked, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When you click on this checkbox to enable this function, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.5.6.1 Interface Configuration/ Wireless Security

In this section, you can configure the wireless security and encryption to prevent from unauthorized access and monitoring.





There are 5 encryption modes, including **No Encryption**, **WEP OPEN SYSTEM**, **WEP SHARED KEY**, **WPA-PSK** and **WPA2-PSK, WPA-PSK/WPA2-PSK mixed Mode** offered for your selection. Please also pull down the **Cipher** list and select the desired mode for your router's wireless security. For more details about the setup in these different modes, please refer to the following sections.

(WEP) Mode

WEP is a method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F(a-f)) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network.

Examples:

- 64-bit hexadecimal keys are exactly 10 characters in length. (12345678FA is a valid string of 10 characters for 64-bit encryption.)
- 128-bit hexadecimal keys are exactly 26 characters in length. (456FBCDF123400122225271730 is a valid string of 26 characters for 128-bit encryption.)
- 64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.)
- 128-bit ASCII keys are up to 13 characters in length (2018HALOSWIN1 is a valid string of 13 characters for 128-bit encryption).

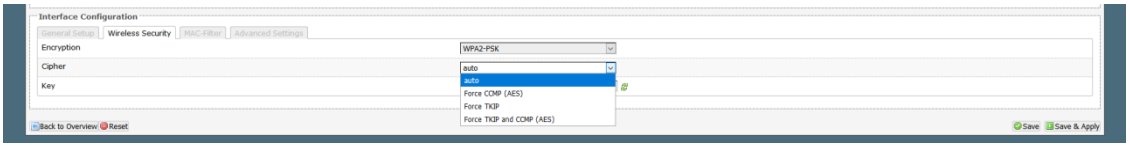
WPA-PSK / WPA2-PSK Mode

WPA (Wi-Fi Protected Access) is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard.

PSK (Pre-Shared Key) is the key which is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format or 64 digits in HEX format at both ends of the wireless connection.

When inputting ASCII strings, it cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase.

This phrase is used to generate session keys that are unique for each wireless client.



Cipher: Mark the option to enable modes of TKIP or AES.

Key: You must respect the Key Format, Length and Value. They must be as same as each wireless client in your wireless network. When Key format is Passphrase, the key value should have 8-63 ASCII characters or 64 digits in HEX format.

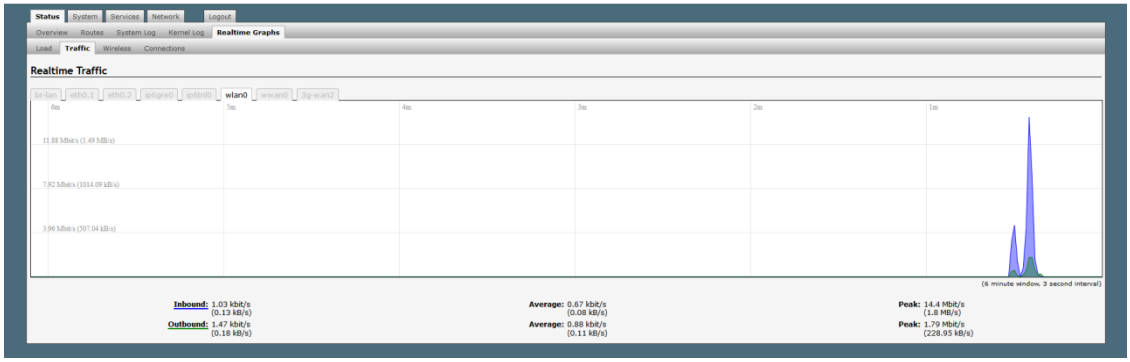
91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.5.6.3 Statistics Real-time Wireless Graph

The KX 4G INDUS ROUTER offers a real-time graph viewer function to collect all wireless traffic counting information about the transmitting / receiving packets and charge of this router. The system will automatically update these wireless data per 3 second interval during six minutes.

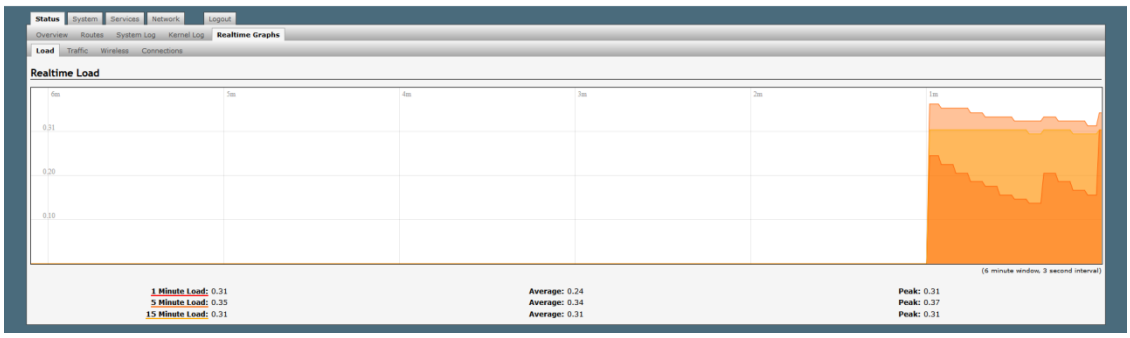
Real-time Traffic:

These graphs illustrate the average system inbound and outbound traffic over the course of 3 minutes; each new measurement is taken every 3 seconds. Each graph consists out of two colours coded graphs (green graph shows the outbound traffic, blue graph shows the inbound traffic). Although not graphed, the page also displays peak loads and averages of inbound and outbound traffic.



Real-time Load:

This tri-graph illustrates average CPU load values in real time. The graph consists out of three colours coded graphs, each one corresponding to the average CPU load over 1 (red), 5 (orange) and 15 (yellow) most recent minutes.

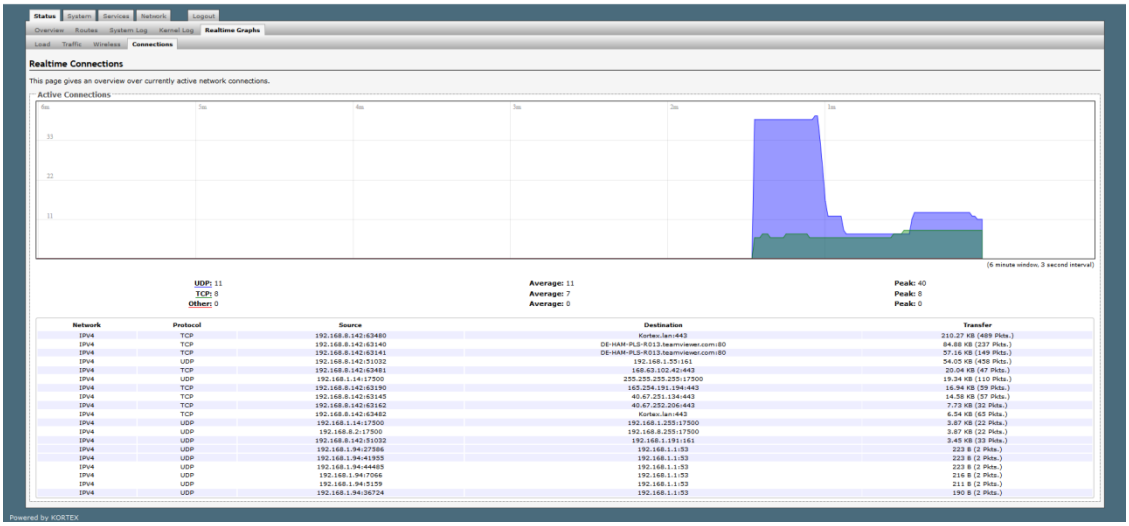


1.	1/5/15 Minutes Load	0.31	Time interval for load averaging, colour of the diagram
2.	Average	0.24	Average CPU load value over time interval (1/5/15 Minute)
3.	Peak	0.31	Peak CPU load value of the time interval

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

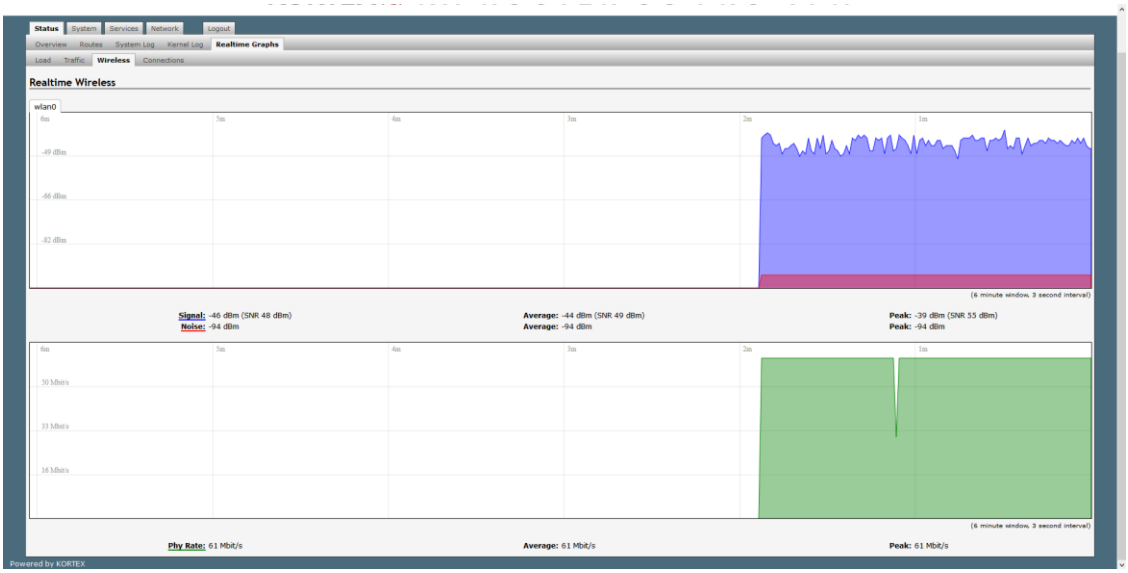
Connections:

Displays currently active network connections with the information about network, protocol, source and destination addresses, transfer speed.



Real-time Wireless :

Displays the wireless radio signal, signal noise and the theoretical maximum channel permeability. Average and peak signal levels are displayed.



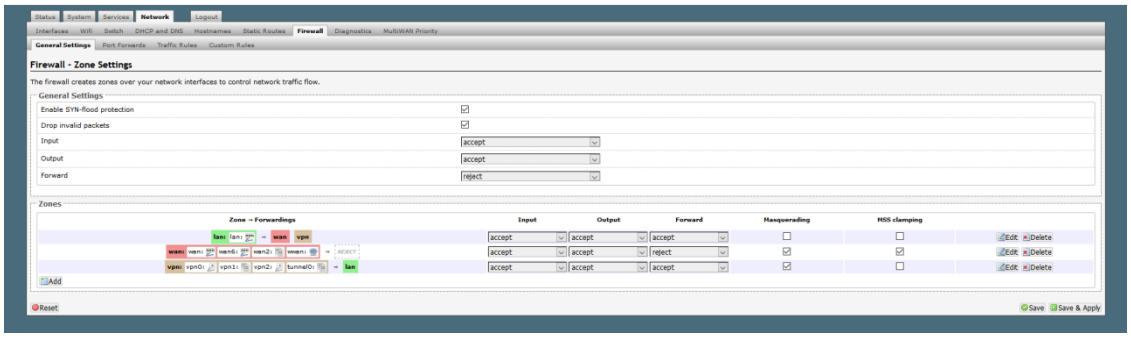
91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.5.7 Firewall

4.5.7.1 General Settings

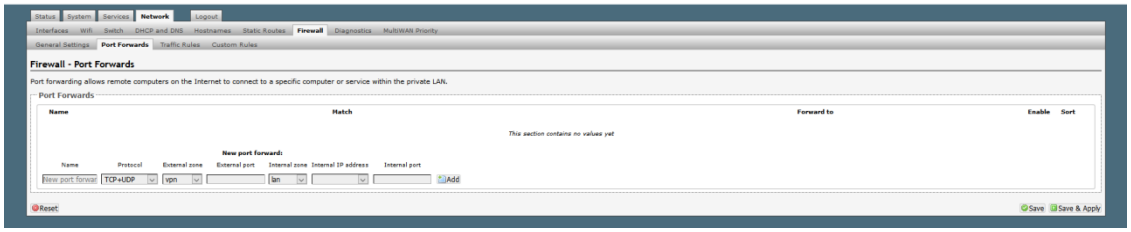
The router could filter the outgoing packets for security or management consideration. You can set up the filter against the IP addresses to block specific internal users from accessing the Internet. The firewall could not only obstruct outside intruders from intruding your system, but also restricting the LAN users. Port filter restricts certain type of data packets from your LAN to Internet through the router.

To improve the safety of the internal network environment, the KX 4G INDUS ROUTER offers a variety of basic firewall management functions, including Remote management (via WAN), Ping from WAN Filter, Block port scan, Block SYN Flood and SPI Firewall. By the configuration the following system security settings, you can protect the router itself from being attacked, scanned or intruded.



4.5.7.2 Port Forwarding

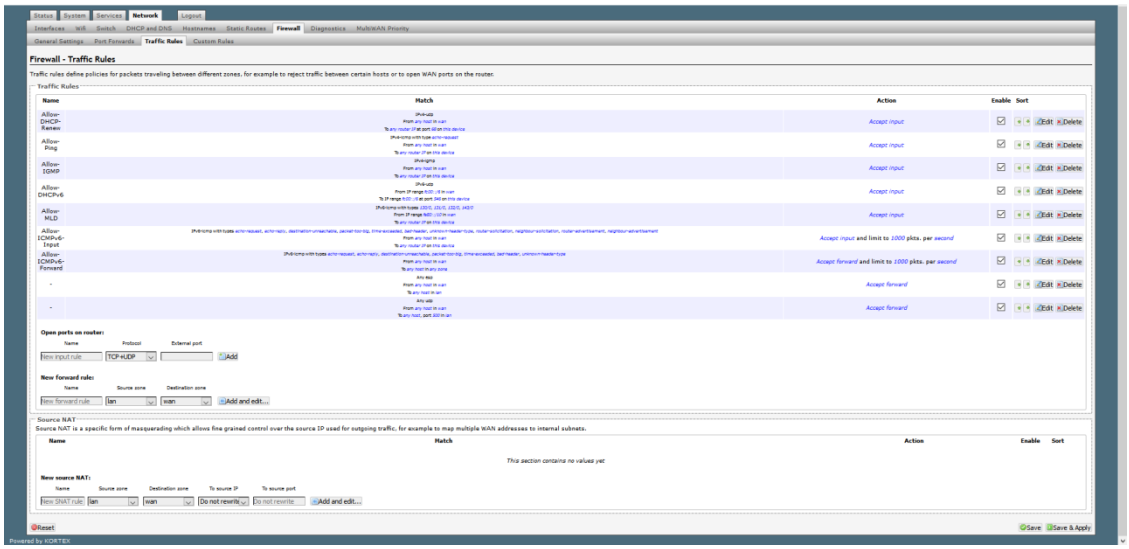
This function offers the way of Port Forwarding / Virtual Server in order to help redirect requests from computers on the LAN to a server set up on the LAN. You can set up an Internet service on the computer on local network, without exposing it on Internet directly. You can also build many sets of port redirection, to provide many different Internet services on different local computers via a single Internet IP address.



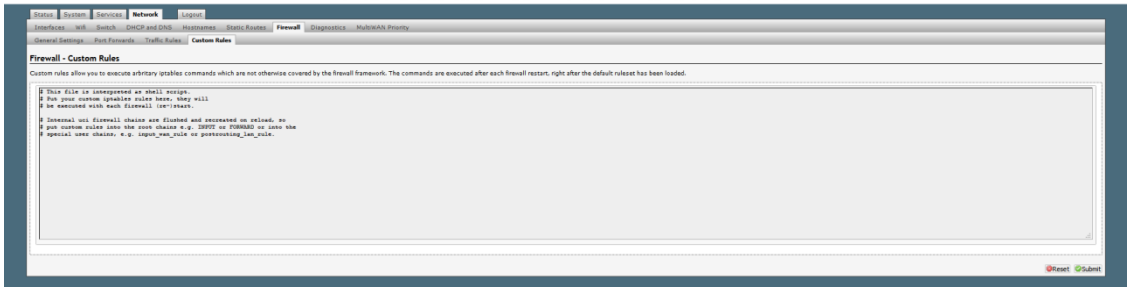
91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.5.7.3 Traffic & Custom rules

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



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

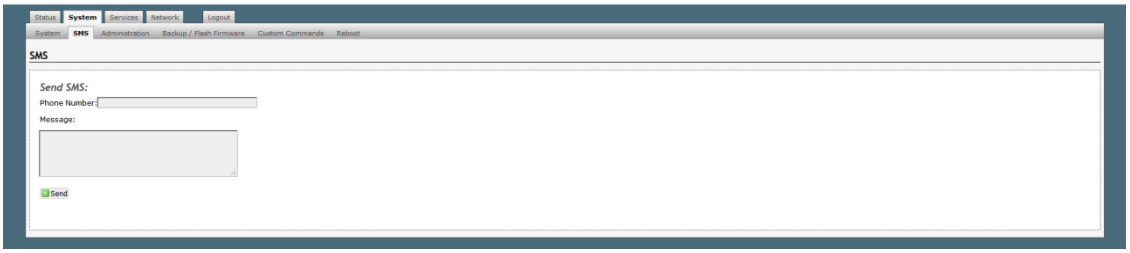


Custom rules allow you to execute arbitrary IP tables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default rule set has been loaded.

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.5.8 SMS

SMS offer the possibility to Send/Receive an SMS to/from an mobile phone number and to display in a list. You can also delete an SMS from the In Box or Sent Box windows.

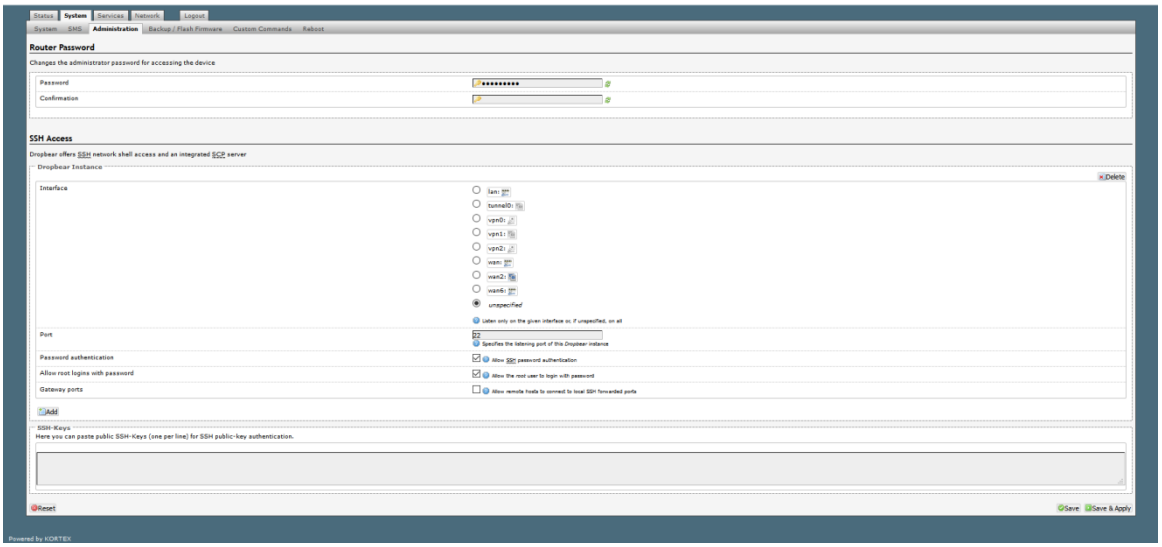


Phone Number: Enter the exact phone number with international code if necessary.
Message: Enter the SMS message (Max 160 characters)

4.5.9 Management

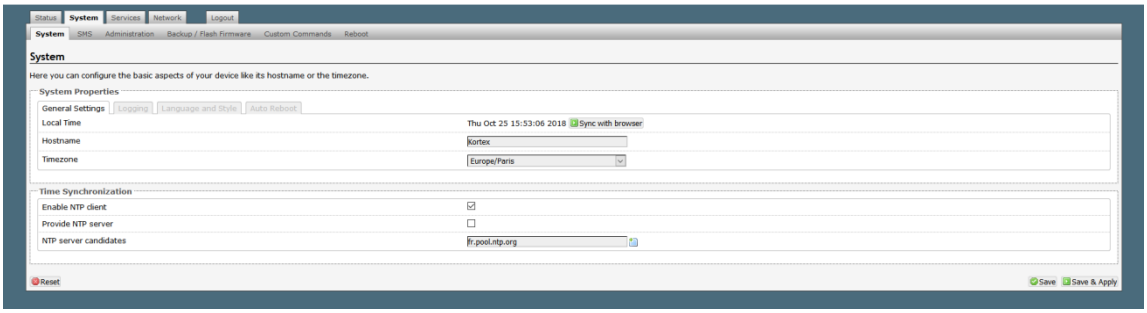
4.5.9.1 Administration

You may configure administrator's account and password, SSH Access here. We strongly recommend that you change the default username and password.

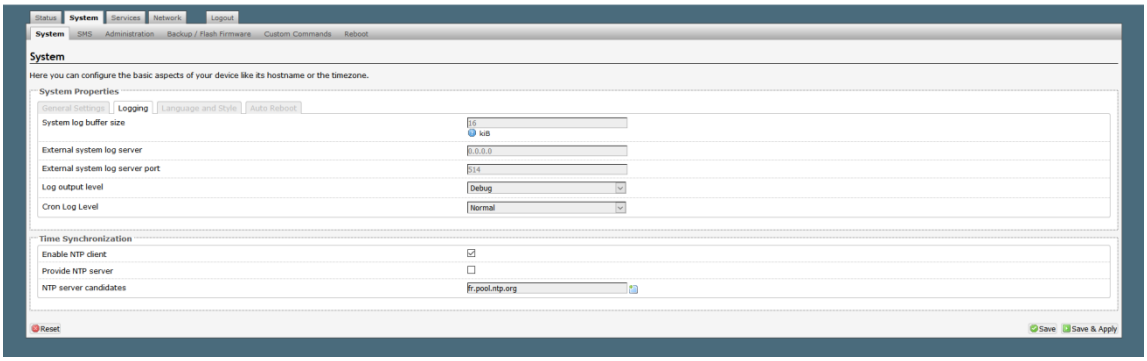


Here you can configure the basic aspects of your device like its hostname or the time zone.

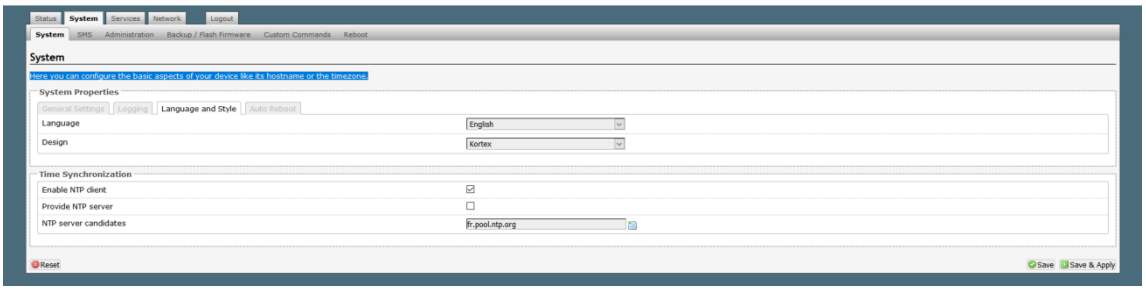
91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62



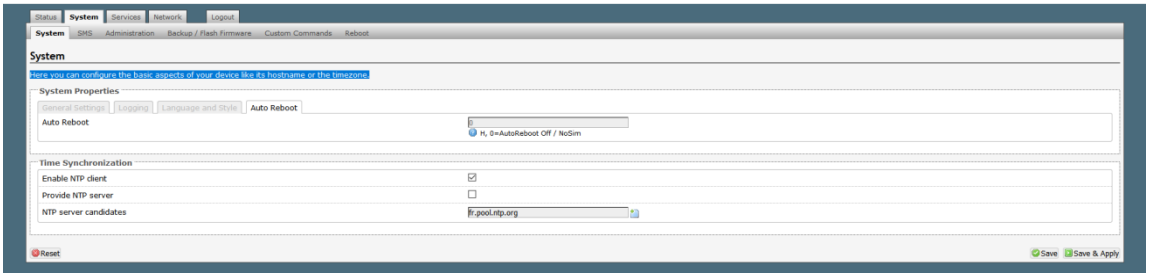
Here you can send the log to a remote server.



Here you can change the language and the interface of the design of the web interface.



Here you can use the keyword "NoSim" to avoid that the router reboot (watchdog) when no SIM is inserted on it.

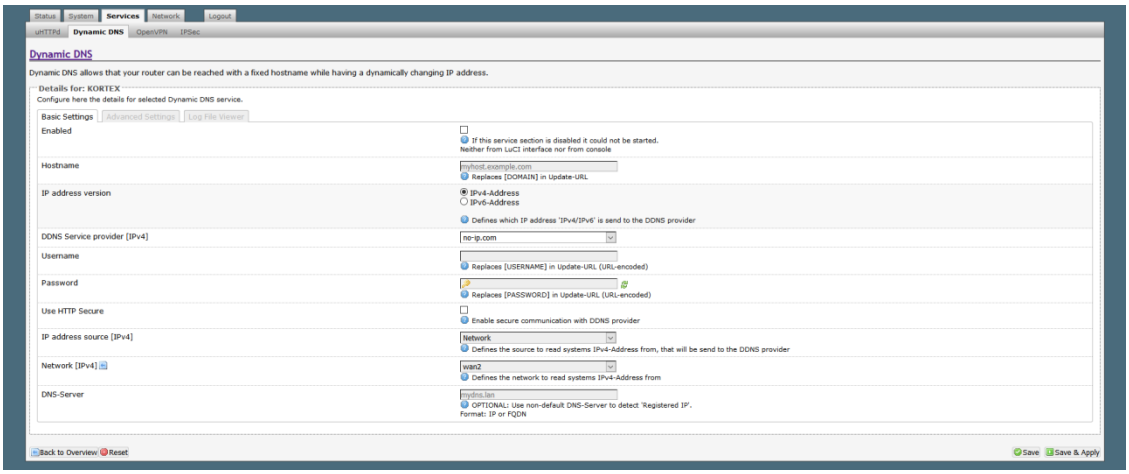


4.5.9.2 DynDNS (Basic Settings)

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc.) using a domain name that you have registered (www.dyndns.com or www.no-ip.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

dynamic (changing) IP addresses. When you use a Dynamic DNS service provider, your friends can enter your domain name to connect to your server, no matter what your IP address is. Enter a name ex. KORTEX.



Enable: If this service section is disabled it could not be started. Neither from web interface nor from console.
Host Name: Enter your host name.
IP address version: Defines which IP address 'IPv4/IPv6' is send to the DDNS provider
Dynamic DNS Provider: Select a dynamic DNS service provider from the pull-down list.
Username: Enter the username or key provided by your service provider.
Password: Enter the password or key provided by your service provider.
Use HTTP Secure: Enable secure communication with DDNS provider
IP address source [IPv4]: Defines the source to read systems IPv4-Address from, that will be send to the DDNS provider.
Network [IPv4]: Defines the network to read systems IPv4-Address from.
DNS-Server: OPTIONAL: Use non-default DNS-Server to detect 'Registered IP'.
Format: IP or FQDN.

Note: After configuring the router for dynamic DNS, you can open a browser and navigate to the URL for your domain (for example **http://www.mydomain.info**) and KX 4G INDUS ROUTER will attempt to forward the request to port 80 on your LAN.

4.5.10 Firmware & Backup / Restore

Software upgrade tool is used to help upgrade the software function in order to fix or improve the function. User can upgrade the firmware in this page. Please note that power

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

cannot be off in the process of the software upgrade. You must do it carefully. Specify the filename and directory where the file is located via the **Browse**…button, and click on the **Flash Image** button when it is completed. When the upload is finished, the router will start upgrading software. A reboot message will be prompted after completing upgrading software. At this time, you must reboot the router to have the new software worked. If your upload is unsuccessful, an error message will be shown in the webpage, and it will not upgrade the software as well.

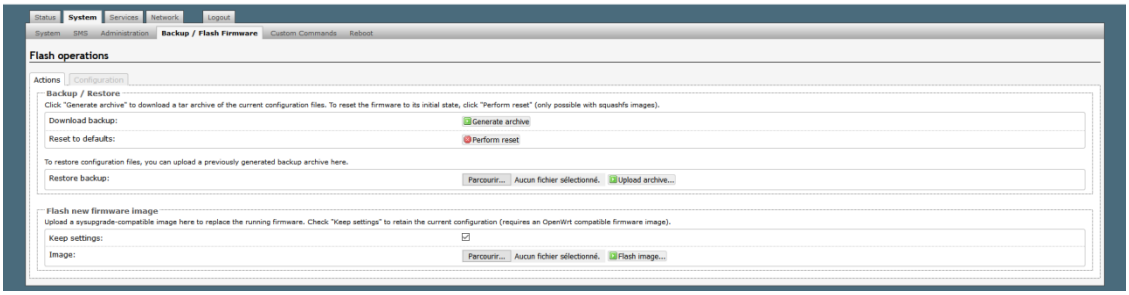


Image: File path and filename stored the image file you would like to upgrade.

Upgrade the firmware to obtain new functionality. It takes about 2 minutes.

Backup / Restore

With this function, user can back up or reload the config files by exporting/ importing settings. Besides through the press of the **Reset** button in the rear panel to execute the hardware reset function as we had mentioned before for the router.

The software reset function provided here takes the same effect as the **Perform Reset** button on the front panel of the router. It will take about 30~60 seconds to complete the system boot.

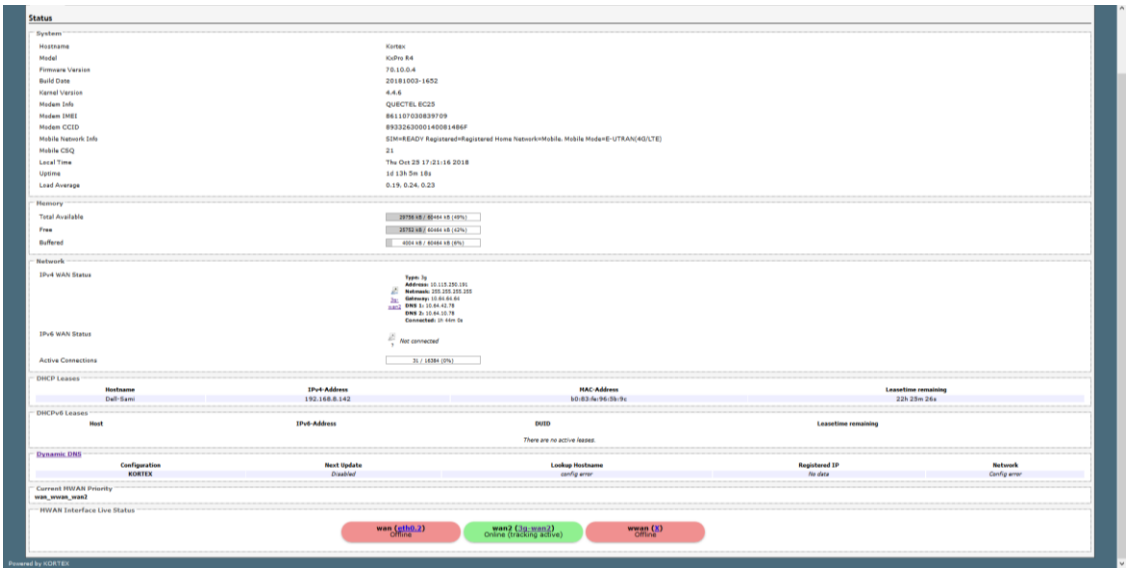
Generate Archive: To export the current settings stored in the flash to a config file, just press the **Generate archive** button.

Restore backup: Import the configuration file into your router. Specify the filename and directory where the file is located via the **Browse**…button, and press the **Upload archive...** button when completed.

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.5.11 Status

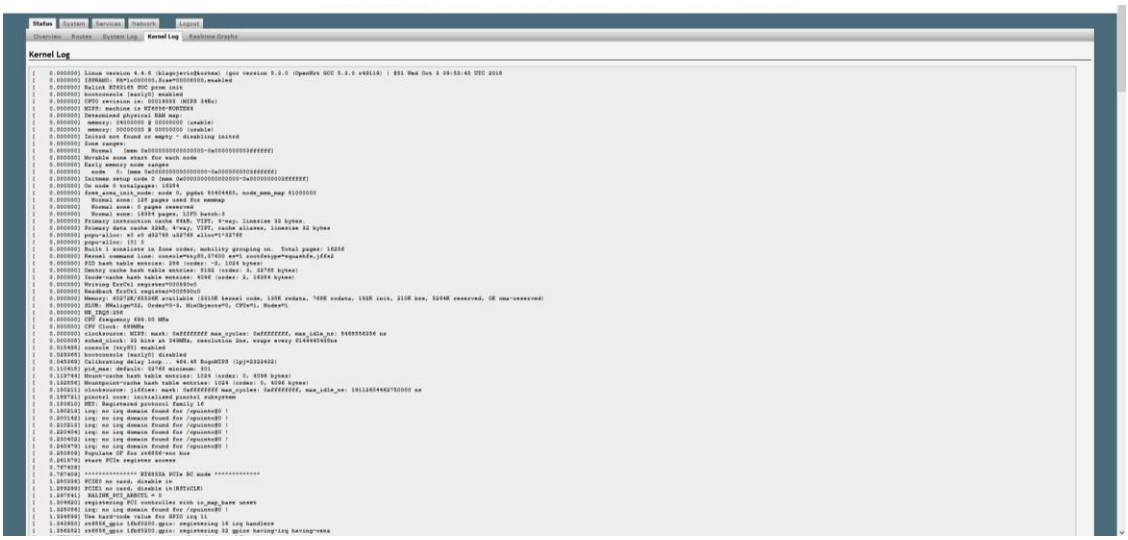
In the Status page, it tells you the basic information of the system. You can check the device status, including the firmware version, system up time, current operation mode, WAN/Local IP address, MAC address and so on. They will be refreshed per 3 seconds. With these information, it is helpful while malfunctioning.



From the Status Windows you can read the various informations after the system is connected.

4.5.11.1 Logs

The KX 4G INDUS ROUTER offers a system & a kernel log.

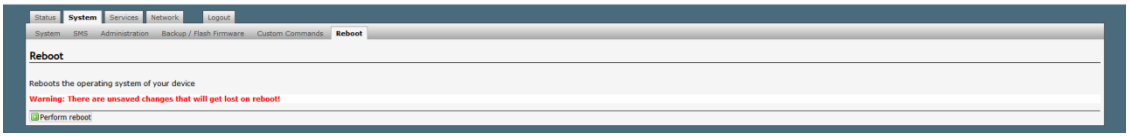


Display the log information of system or kernel flow. From the system log you can read the various situations after the system starts.

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.5.12 Reboot

The KX 4G INDUS ROUTER offers the possibility to be rebooted.



4.5.13 Remote Sms

The KX 4G INDUS ROUTER has a function to be controlled via SMS.
You can send a SMS to the number of the M2M SIM card in the KX 4G INDUS ROUTER router; a reply SMS will then be sent back (if the issuance SMS are allowed on the SIM card).

You must first, make sure with the operator company, it is able to provide this service and transmit SMS reception. The cost applied for such a service may be charged a flat rate penalty or unit basis.

Two commands are available for use by SMS. These can be entered in upper or lower case.
MS is the last 4 digits of the IMEI (password) and the command.

Connect or **go** orders
you can view the IMEI number, IP address received from the GPRS / 3G / 4G and the module reception level (CSQ). The answer is done only on the number of the SMS sender.

Order **bb**
Reboot the router.

Examples of SMS with the IMEI 358178041055718:
- 5718connect or 5718go
- 5718bb

SMS return will consist of the IMEI (unique number of the module), public or private IP address and module reception level (CSQ).

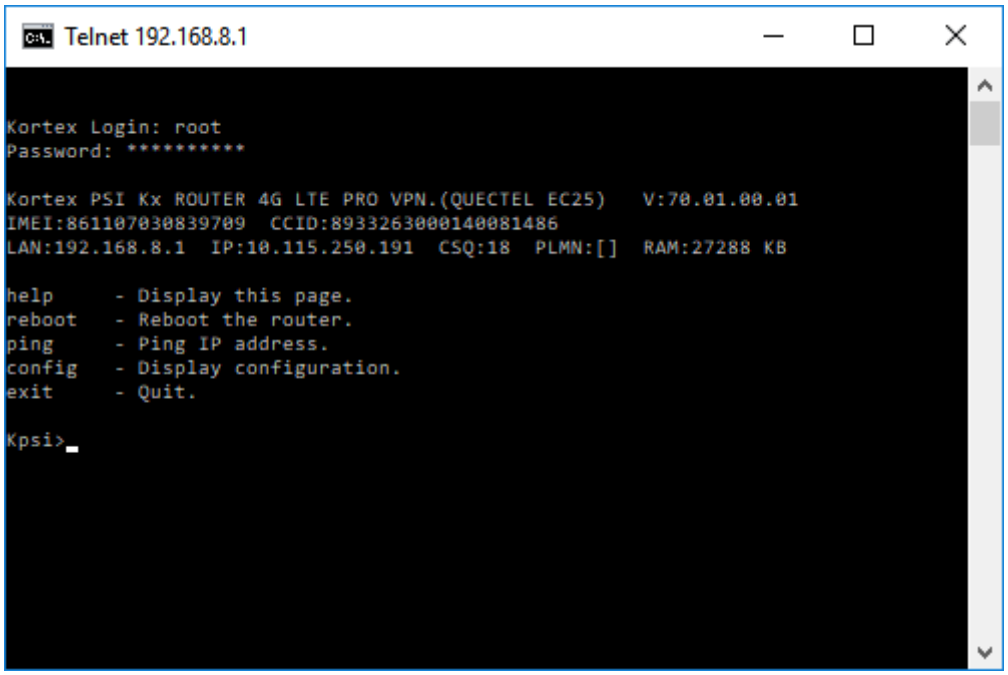
Example:
http://80.214.118.34
IMEI = 352347031832032
CSQ = 22

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

4.5.14 Telnet

The KX 4G INDUS ROUTER has a control interface "Telnet" on port 2000 accessible from the LAN ports or remote. Locally, you must type in command mode "cmd" Telnet "IP of the router" 2000.

Default: Telnet 192.168.8.1 2000 or 2000 (if the initial configuration has been loaded into the KX 4G INDUS ROUTER). The login is **root** and default password is **kxpro75002**. We strongly recommend that you change the default username and password.



This interface allows among others:

- Display the IP address and others information
- Reboot the box KX 4G INDUS ROUTER locally or remotely.
- This interface allows among others: Ping a specific host...

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62

Chapter 5 FAQ

SIM Card Status shows "Not Ready"

It means the SIM card is not found, you can take SIM card out, and insert it again.

Signal Strength is normal, but can't get WAN IP

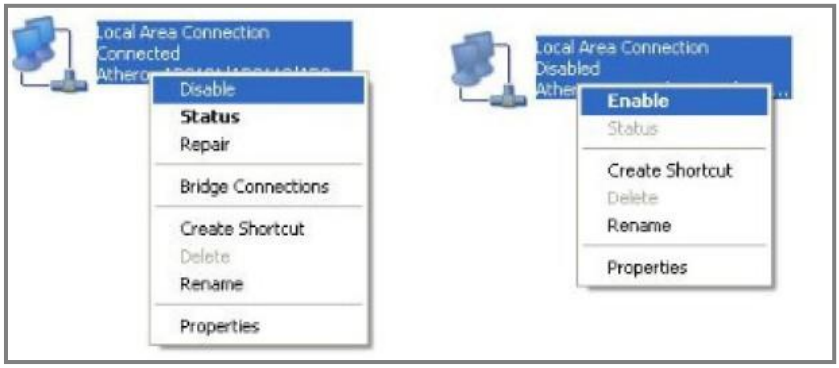
Check the APN parameters in WAN settings.

Can't visit the router from remote side

1) Make a ping to the WAN IP to check whether it is successful.
2) We are using 80 as router's default port, but some ISP block the 80 port, you can confirm with local ISP which ports are open, and change port to try.

LAN fails

1. Check RJ45 cable; make sure it is correctly connected.
2. Make sure the PC and router are in same network segment.
3. Disable the PC network card, and re-enable it.



4) Reset the router. Press Reset button for several seconds, it will load to factory settings.

Get WAN IP, but PC can't access internet.

1. Check the DNS, you can make a ping to a normal IP (e.g. 8.8.8.8), if ping IP is ok, the question must be caused by DNS.
2. Make sure the SIM card support data service, you can try it in your cell phone.
3. Signal is too weak. Move antenna or change position to get better signal.

Port forwarding not working

1) Check with ISP which ports are open by them.
2) More than 1 router. The most common problem we come across is people who are behind 2 or more routers and don't realize it.

91 rue Réaumur
75002 PARIS
Tel: 01 34 04 37 62