TELTONIKA

RUT600 3G Wireless-N Router

User Manual v1.00

User manual

Dear Customer,

Thank you for choosing Teltonika!

RUT600 is a high speed Wireless Router, which complies with the latest standards and provides high wireless receiving and transmitting rates. It enhances your connectivity freedom wherever you are - in the office, at home or at the remote location.

The instructions bellow will help you to know-well your router.

Legal notice

Attention

Before using the device we strongly recommend to read this user manual carefully.

Do not disassemble the device.
Do not use the device if the device block is broken or its connecting wires are without isolation.

All wireless devices for data transfer may be susceptible to interference, which could affect performance.

The device is not water-resistant. Keep it dry.

The device requires 230V AC voltage. Be careful!

Please use cable and the adapter provided with RUT600 device. Teltonika is not responsible for any harm caused by using wrong cable or wrong adapter for connection

Any operation during a lightning storm is under your own risk and responsibility. It is strongly recommended to turn of the device during lightning storm.

IMPORTANT NOTES!

It is mandatory to read the notes and user manual carefully before starting to use the device.

Technical support contacts

If you face any problems related to the device, which you are not able to solve by yourself, you are always welcome to address our technical support department by e-mail support@teltonika.lt. We will do our best assisting you.

Table of Content

Chapter 1: Product overview

1.1 Introduction

Teltonika 3G Wireless-N Router provides WAN connectivity to wired and wireless clients using the 3G and Ethernet data network. 3G Wireless Router is extremely useful for mobile work teams or emergency crews that need access to the broadband Internet but have no permanent base. Quickly set up a IEEE802.11 hotspot Internet connection to check email and browse the web or share files.

1.2 Package Contents

- Teltonika Wireless-N 3G Router
- Power supply adapter
- WiFi antenna

Note: If any of the components is missing or damaged, please contact the retailer or reseller from which this product was purchased.

Chapter 2: RUT600 Hardware, LED's, connections and features

2.1 LED Indicator and Port Description

LED indicator description on front panel: (from R to L)

- **POWER**

  Always ON, indicates power connection.

- **WPS**

  Blinking indicates that device is negotiating with client in WPS mode.

- **SYS**

  Blinking indicates that system runs well.

- **USB**

  Always ON indicates successfully connected USB device; Blinking indicates data transmission through USB port.

- **WLAN**

  Wireless signal LED indicator. Blinking indicates that wireless function is enabled.

- **WAN**

  Wide area network LED indicator. Always ON indicates successfully connected Ethernet device; Blinking indicates data transmission through WAN port.

- **LAN (4, 3, 2, 1)**

  Wired local network LED indicator. Always ON indicates successfully connected Ethernet device; Blinking indicates data transmission through LAN port.

Ports and buttons description on back panel (from L to R)

- **POWER**

  The port is used for the power adapter connection. Please use only the included DC 9V 1A power adapter.

- **RESET**

  The system reset button. To restore settings to factory default, press this button and hold for 7 seconds.

- **USB**

  The USB2.0 port provided for 3G modem.

- **WAN**

  Modem, Switch, Router or other Ethernet device can be connected to the 100Mbps Ethernet port to access the Internet.

- **LAN (4, 3, 2, 1)**

  Ethernet switch, Ethernet router and NIC card can be connected to these 4 10/100Mbps Ethernet ports.

- **WPS**

  Wi-Fi Protected Setup button. Press it for 1 second to enable WPS.

2.2 Product Features

- ✓ Includes Wireless AP, Router, 4-Port Switch and Firewall in one
- ✓ WPS (Wi-Fi Protected Setup) encryption method
- ✓ IEEE 802.11b/g/n, IEEE 802.3, IEEE 802.3u standards
- ✓ 64/128-bit WEP, WPA, WPA2, WPA&WPA2 encryption methods
- ✓ RTS/CTS protocol and data partitioning function
- ✓ 1×10/100Mbps Ethernet WAN port
- ✓ 4×10/100Mbps Ethernet LAN ports
- ✓ 1 x USB2.0
- ✓ Supports xDSL/Cable Modem, static and dynamic IP
- ✓ Remote/local Web management
- ✓ WMM (Wireless MultiMedia)
- ✓ Wireless Roaming technology for high-efficient wireless connections
- ✓ SSID stealth mode and access control based over MAC address
- ✓ Auto MDI/MDIX
- ✓ System log to record the status of the Router
- ✓ Auto negotiation/manual mode for IEEE 802.11b/g/n
- ✓ UPnP and DDNS
- ✓ LAN access control over Internet connection
- ✓ SNTP
- ✓ Virtual server and DMZ host support
- ✓ Auto wireless channel selection
- ✓ WDS wireless network extension
- ✓ URL Monitor
- ✓ QoS function
- ✓ Firefox 1.0 and IE5.5 or above support

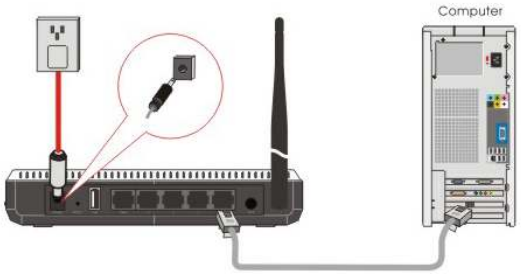
Chapter 3: Hardware Installation

After you unpack the box, please follow the steps below to connect the device. For better wireless performance, please put the device in the middle of wireless coverage area.

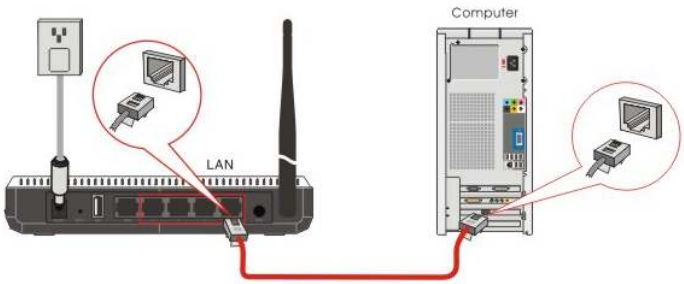
- Please use the included power adapter to power on the Router.

  ! (IMPORTANT: Use of a wrong power adapter could cause damage and void the warranty for this product).

  ! (IMPORTANT: when using 3G USB modem, first insert the modem and then power on the device).



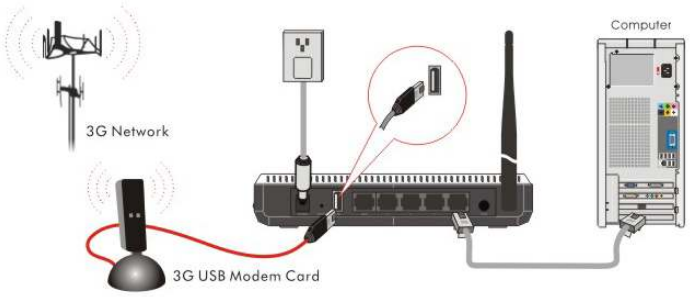
- Please connect the LAN port of the Router to the network adapter of your computer with a cable.



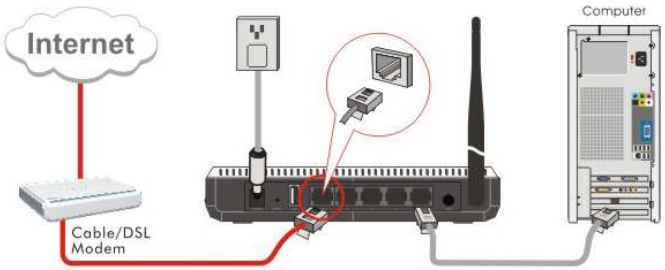
- Connection between the Router and Network

  ➔ If you have a 3G USB modem card, please connect it to the Router's USB port.

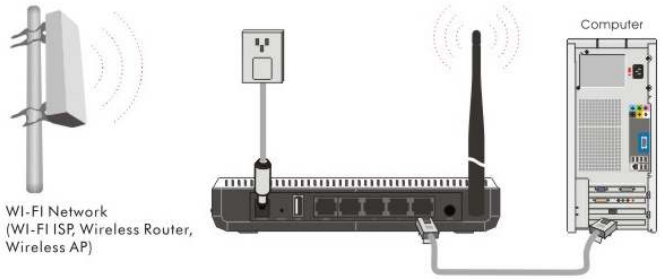
  ! (**IMPORTANT: when using 3G USB modem, first insert the modem and then power on the device**)



➔ If you are provided with the wired broadband by your ISP to access the Internet, please connect the Router's WAN port to the Internet access line.



➔ If you are provided with the wireless broadband by your ISP to access the Internet or you want to amplify wireless signals, please set the Router's wireless WAN feature.



Chapter 4: Router configuration

4.1 Connect to router WEB configuration page using wired connection

Step 1 Connect 3G Router to your PC using LAN cable.
Step 2 Setup Local Area Network adapter's IP address.

- Automatically obtain IP address and DNS server address or
- Assign static IP address manually within 192.168.0.2 – 192.168.0.254 range.

Step 3 Open the Web browser and type the IP address of the router (Default: 192.168.0.1) and enter Router administrator login details to access the Web management tool.

Note The default administrator login settings are:
Login: admin
Password: admin

Note It is strongly recommended to change the password after the first router configuration.

Step 4 After successful logon you will see the main page of the Router Web configuration interface. The device now is ready for configuration.

4.2 Connect to router WEB configuration page using wireless connection

Step 1 Setup the wireless network adapter's IP address on your computer.

- Automatically obtain IP address and DNS server address or
- Assign static IP address manually within 192.168.0.2 – 192.168.0.254 range

Step 2 Choose the wireless network (**RUT600** by default) from the list of available wireless networks.
Step 3 Open the Web browser and type the IP address of the router (Default: 192.168.0.1) and enter Router administrator login details to access the Web management tool.

Note The default administrator login settings are:
Login: admin
Password: admin

Step 4 After successful logon you will see the main page of the Router Web configuration interface. The device now is ready for configuration.

Chapter 5: WEB configuration page interface structure

After the successful login you will see the WEB configuration page with the following structure:

- **System Status**
- **WAN Medium**
- **Setup Wizard**
- **Advanced Settings**
  - **LAN Settings**
  - **WAN Settings**
  - **MAC Address Clone**
  - **DNS Settings**
- **WLAN Settings**
  - **Basic Settings**
  - **Security Settings**
  - **Advanced Settings**
  - **WPS Settings**
  - **WDS Settings**
  - **Access Control**
  - **Connection Status**
- **DHCP Server**
  - **DHCP Settings**
  - **DHCP List&Binding**
- **Virtual Server**
  - **Single Port Forwarding**
  - **Port Range Forwarding**
  - **ALG Service**
  - **DMZ Settings**
  - **UpnP Settings**
- **Traffic Control**
  - **Traffic Control**
  - **Traffic Statistic**
- **URL Monitor**
- **Security Settings**
  - **Client Filter**
  - **URL Filter**
  - **MAC Filter**
  - **Prevent Network Attack**
  - **Remote WEB Management**
  - **Local WEB Management**
  - **WAN PING**
- **Routing Settings**
  - **Routing Table**
  - **Static Route**
- **System Tools**
  - **Time Settings**
  - **DDNS**
  - **Backup/Restore**
  - **Upgrade**
  - **Restore to Factory**
  - **Reboot**
  - **Change Password**
  - **System Log**
- **Logout**

5.1 WAN Medium Type

The Router provides three access medium types. If you are provided with the 3G broadband by your ISP to access the Internet, you can connect the 3G USB modem card to the Router's USB port and select 3G WAN to set the device. If you are provided with the wired WAN access broadband such as ADSL Modem, Cable Modem or ISP broadband access line, you can connect the access line directly to the WAN port on the Router's rear panel. In addition, if you are provided with the wireless broadband by your ISP, you can access the Internet conveniently.

- **3G WAN:** If you have a 3G USB modem card and you want to share 3G Internet, please select this type.
- **Wired WAN:** In this type the WAN link line must be wired. Please connect the access line to the WAN port on the Router's rear panel. The default type is wired WAN.
- **Wireless WAN:** If you are provided with the wireless WAN to access the Internet or you want to amplify the wireless signals, you can use this type.

Please select the appropriate WAN medium type according to the access way provided by your ISP. After saving and rebooting the device, you can enter the "Setup Wizard" menu to set the connection type.

5.2 Setup Wizard

1. 3G Broadband Connection

If you have a 3G USB modem card and you want to share 3G Internet, please select "3G WAN" in "WAN Medium" after you enter the Router's Web-interface.

During the installation, please select the type of 3G modem card and enter the basic parameters provided by your 3G ISP.

2. Wired Broadband Connection (Wired WAN)

If you are provided with the wired broadband by your ISP to access the Internet, please select "Wired WAN" in the "WAN Medium" setup page after you enter the Router's Web-interface. It takes effect after saving and rebooting the device.

The Router supports multiple access ways such as ADSL PPPOE Dial, Dynamic IP, static IP, etc. If you are not sure of your access way, you can enable the auto-detect function to select your access way.

- ADSL Virtual Dial-up (via PPPoE).
  Enter the Account and Password provided by your ISP and click "Next".
- Dynamic IP (via DHCP).
  If your connection mode is Dynamic IP, it means your IP address keeps changing every time you connect. You do not need to enter the information like for other modes. Click "Next" and "Apply" to save the settings.
- Static IP.
  In this screen, fill the network address information from your ISP in the IP address, Subnet Mask, Gateway and Primary DNS server fields and click "Next". Click "Apply" to complete the setup wizard. The Router will save the settings you made. To activate the settings, it is recommended to select "Reboot the Router" from the "System Tools" on the left menu. Please, DO NOT power off the router during the reboot.

3. Wireless Broadband Connection (Wireless WAN)

If you are provided with the wireless broadband by your ISP to access the Internet or you want to amplify wireless signals, please select "Wireless WAN" in "WAN Medium" page after you enter the Router's setup page.

Please enter the wireless SSID, Mac address, channel, security mode parameters provided by your Wi-Fi ISP. It is also possible to click "Auto Scan" to find ISP automatically. Select and save the settings, and you will enter the Router's Web interface again after rebooting the Router.

Note: When you open the wireless WAN feature or when you have another wireless router and you want to amplify wireless signals, please pay attention to the IP address the previous router distributed. If the IP address belongs to the range: 192.168.0.x, you need to change the LAN IP address to different range such as 192.168.2.1. Only this way, you can amplify the wireless signals and access the Internet. Please refer to chapter 6.1 for changing method.

You do not need to change LAN IP range if the router was connected to your wireless broadband ISP.

5.3 Advanced Settings

1. LAN Settings

LAN Settings are used to configure the basic TCP/IP parameters of LAN ports.

- **MAC Address:** The Router's physical MAC address as seen on your local network is unchangeable.
- **IP Address:** The Router's LAN IP addresses (not your PC's IP address). 192.168.0.1 is the default value.
- **Subnet Mask:** Router's subnet mask is used for setting the network size. 255.255.255.0 is the default value.

Note: Once you modify the IP address, you need to remember it for future logins.

2. WAN Settings

This section is used to modify and configure WAN settings in details after you have selected the ISP connection type in "Setup Wizard".

Virtual Dial-up (PPPoE)

- **WAN Connection Mode:** Shows your current connection mode.
- **Account:** Enter as provided by your ISP.
- **Password:** Enter as provided by your ISP.
- **MTU:** Maximum Transmission Unit. Is the size of the largest datagram that can be sent over a network. The default value is 1492. Do NOT modify it unless necessary. If some specific website or web-application software cannot be opened or enabled, you can have a try changing the MTU value to 1450, 1400, etc.
- **Service Name:** It is defined as a set of characteristics that are applied to a PPPoE connection. Enter it if provided. Do NOT modify it unless necessary.
- **AC Name:** Enter it if provided. Do NOT modify it unless necessary.

- **Connect Automatically:** Connect automatically to the Internet after rebooting the system or on connection failure.
- **Connect Manually:** Connect to the Internet manually.
- **Connect on Demand:** Re-establish your connection to the Internet after the specific time (Max Idle Time). Zero means your Internet connection is ON all the time. Otherwise, enter the minutes to be elapsed before you want to be disconnected from the Internet.
- **Connect on Fixed Time:** Connect to the Internet during the time you set.

Notice:

The "Connect on Fixed Time" can be used only when you have set the current time in "Time Settings" in "System Tools".

Static IP

If the static IP is chosen for your connection, you can modify the following address information.

- **IP Address:** Enter the WAN IP address as provided by your ISP.
- **Subnet Mask:** Enter the WAN Subnet Mask here.
- **Gateway:** Enter the WAN Gateway here.
- **Primary DNS Server:** Enter the Primary DNS server as provided by your ISP.
- **Secondary DNS Server:** Enter the secondary DNS.

For PPTP and L2TP connection settings please refer to the "Wizard Setup" in chapter 5.

3G Broadband:

Network settings

- **PIN code:** SIM card personal identification code. Enter as provided by your ISP.
- **Access Point Name:** Enter as provided by your ISP.
- **Dial:** Enter dialing number as provided by your ISP (default is *99#).

Advanced PPP Settings

- **User Name:** PPP Authentication User Name.
- **Password:** PPP Authentication Password.

After configuring the settings correctly, click "Apply" button and wait for 60 seconds. Then you can access the Internet.

Note: Please enter the correct parameters according to the requirements of your ISP. After finishing and saving the settings, please check the connection status on the status page.

3. MAC Address Clone

This page is used to set the Router's MAC address for WAN.
Some ISPs require end-user's MAC address to access their network. This feature copies the MAC address of your network device to the Router.

- **MAC Address:** The MAC address to be registered with your Internet service provider.
- **Clone MAC Address:** Register your MAC address.
- **Restore Default MAC Address:** Restore to the default hardware MAC address.

4. DNS Settings

DNS (Domain Name System (or Service)) – is an Internet service that translates domain names into IP addresses which are provided by your Internet Service Provider. Please contact your Internet Service Provider for details if needed.

- **DNS:** Check the checkbox to enable the DNS server. The Router's DHCP sever will answer to the clients requests and will distribute DNS address.
- **Primary DNS Address:** Enter the necessary address as provided by your ISP.
- **Secondary DNS Address:** Enter the second address if needed (optional).

Note: After you have finished with the settings, please reboot the device to activate the modified settings.

5.4 WLAN Setting

1. Basic Settings

- **Enable Wireless:** Check to enable the Router's wireless features; uncheck to disable it.
- **Network Mode:** Select one mode from the following. The default is 11b/g/n mode.

11b mode: Allows the wireless client equipment to be connected to the device in 11b mode at the maximum speed of 11Mbps.

11g mode: Allows the 11g/11n-compliant client equipment to be connected to the AP at the maximum speed of 54Mbps.

11b/g mode: Allows the 11b/g-compliant client equipment to be connected to the AP with auto-negotiation speed, and 11n wireless client equipment to be connected to the device with 11g speed.

11b/g/n mode: Allows 11b/g/n-compliant client equipment to be connected to the AP with auto-negotiation speed.

- **Main SSID:** SSID (Service Set Identifier) is the unique name of the wireless network. This device has two SSID's and the main SSID is necessary.
- **Minor SSID:** It is optional.
- **Broadcast (SSID):** Select "Enable" to enable the device's SSID to be visible by wireless client equipment. It is Enabled by default.
- **MBSSID AP Isolation:** the access control feature based on wireless MAC address. When this feature is enabled, wireless client equipment connected to the same SSID cannot communicate with each other. For example, configure main SSID as AP1, minor SSID as AP2. Connect PC1 and PC2 to AP1 via wireless adapter, and configure PC1 and PC2 in the same segment. After the feature is enabled, two PCs cannot communicate and share network resources with each other, but they can communicate with wireless clients connected with AP2.
- **AP Isolation:** the access control feature based on SSID. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. When this feature is enabled, wireless clients connected to the Main SSID and Minor SSID will not be able to communicate with each other, which can secure the wireless network strongly. For example, configure main SSID as AP1, minor SSID as AP2. Connect PC1 to AP1 via wireless adapter; connect PC2 to AP2. After the feature is enabled, two PCs will not be able to communicate and share network resources with each other. This feature is to isolate the communication of wireless clients connected with different SSID.

Tip: If you want to isolate all connected wireless client equipment communication, please enable MBSSID AP Isolation and AP Isolation simultaneously.

- **BSSID:** Basic Service Set Identifier of wireless network. In IEEE802.11, BSSID is the MAC address of wireless access point.
- **Standard Channel:** Specify the used channel (from 1 to 13 or Auto) for the wireless network.

- **Extension Channel:** To increase data throughput of wireless network, the extension channel range is used in 11n mode.
- **Channel Bandwidth:** Select the channel bandwidth to improve the wireless performance.

2. Security Settings

These settings are used to configure the AP's network security.

- **Select SSID:** Select the SSID (main SSID or minor SSID) to configure security settings from the drop-down menu.
- **Security Mode:** Please select the corresponding security encryption modes from the drop-down menu.

WPA-Personal

WPA (Wi-Fi Protected Access) - is a Wi-Fi standard encryption scheme, designed to improve the security features of WEP security. It applies more powerful encryption types (such as TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]) and can change the keys dynamically on every authorized wireless device.

- **WPA Algorithms:** Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard].
- **Pass Phrase:** Enter 8-63 ASCII characters.
- **Key Renewal Interval:** Set the key renewal period.

WPA2- Personal

WPA2 (Wi-Fi Protected Access version 2) provides higher security than WEP (Wireless Equivalent Privacy) or WPA (Wi-Fi Protected Access). Besides TKIP encryption, new AES encryption mode is provided.

- **WPA Algorithms:** Provides TKIP [Temporal Key Integrity Protocol], AES [Advanced Encryption Standard] or TKIP&AES mixed mode.
- **Pass Phrase:** Enter 8-63 ASCII characters.
- **Key Renewal Interval:** Set the key renewal period.

Mixed WEP

WEP (Wired Equivalent Privacy), a basic encryption method, usually encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). By using the same keys on each of your wireless network devices, you can prevent unauthorized wireless devices from monitoring your transmissions or using your wireless resources.

- **WEP Key:** Set the WEP key in the ASCII or Hex format.
- **Key Explanation:** You can enter ASCII code (5 or 13 ASCII characters. Illegal character as "/" are not allowed) or 10/26 hex characters.
- **Default Key:** Select one key from the four configured keys as the default one.

WPA- Enterprise / WPA2-Enterprise

This security mode is based on Radius authentication server and WPA/WPA2 encryption method. This security mode is used when a RADIUS server is connected to the device.

- **WPA Algorithms:** Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard].
- **Key Renewal Interval:** Set the key renewal period.
- **Radius Server Address:** Enter the IP address of the Radius server.
- **Radius Server port:** Enter the authentication port of the Radius server. The default is 1812.
- **Shared Key:** Enter the shared key for authentication server with 8~63 ASCII characters.
- **Session Timeout:** The authentication interval period between the Router and authentication server.

802.1X

This security mode is used when using a RADIUS server. 802.1x, is a Port-based authentication protocol. The port can be either a physical or logic port (such as VLAN). For wireless LAN users, a port is just a channel. The final purpose of 802.11x authentication is to check if the port can be used. If the port is authenticated successfully, you will be able to open this port which will allow all the messages to pass. If the port isn't authenticated successfully, you will be able to keep this port "disabled" which will just allow 802.1x authentication protocol message to pass.

- **WEP:** Click "Enable/Disable" to enable or disable the WEP security mode.
- **Radius Server Address:** Enter the IP address of the Radius server.
- **Radius Server Port:** Enter the authentication port of the Radius server. The default is 1812.
- **Shared Key:** Enter the shared key for authentication server (8~63 ASCII characters).
- **Session Timeout:** The session authentication interval period between AP and authentication server. The default is 3600s.

Note: To improve security level, do not use simple keys. If you are not familiar with these security modes, it is recommended to use the "WPA-Personal" mode.

Wireless Security Settings for 802.11n only define three standard encryption methods: Open-None (Disable), WPA-Personal-AES, PA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems between equipment of different manufacturers.

3. Advanced Settings

This section is used to configure the advanced wireless setting of the Router, including the BG Protection Mode, Basic Data Rates, Fragmentation Threshold, RTS Threshold, and WMM etc.

- **BG protection Mode:** the default value is "Auto". It is used for 11b/g wireless client equipment to connect to 11n wireless network smoothly in a complicated wireless area.
- **Basic Data Rates:** Depending on requirements, you can select one of the suitable Basic Data Rates. The default value is (1-2-5.5.-11Mbps…). It is recommended not to modify this value.
- **Beacon Interval:** Set the beacon interval of wireless radio. Default value is 100. It is recommended not to modify this value.
- **Fragment Threshold:** The fragmentation threshold defines the maximum transmission packet size in bytes. The packet will be fragmented if its size exceeds the threshold settings. The default size is 2346 bytes. It is recommended not to modify this value.
- **RTS Threshold:** RTS stands for "Request to Send". This parameter controls what data packet size the frequency protocol issues to RTS packet. The default value of the attribute is 2346. It is recommended not to modify this value in SOHO (small office and home) environment.
- **TX Power:** Set the output power of wireless radio. The default value is 100.
- **WMM Capable:** It will enhance the data transfer performance of multimedia data when they're being transferred over wireless network. It is recommended to enable this option.
- **APSD Capable:** It is used for auto power-saved service. The default is disabled.

4. WPS Settings

WPS (Wi-Fi Protected Setting) can be used for easy and quick connection setup between the wireless network client equipment and the device through encrypted contents. The users only enter PIN code or press WPS button on the panel to configure it without selecting encryption method and secret keys manually.

- **WPS settings:** Is used to enable or disable WPS function. The default is "Enable".
- **WPS mode:** Provides two ways: PBC (Push-Button Configuration) and PIN code.
- **PBC:** Select the PBC or press the WPS button on the front panel of the device for about one second. WPS indicator will be blinking for 2 minutes, which means the WPS is enabled. During the blinking time, you can enable another device to start the WPS/PBC negotiation between them. Two minutes later, the WPS indicator will be off, which means the WPS connection is completed. If additional client equipment is added, repeat the above steps. WPS supports up to 32 clients access.
- **PIN:** If this option is enabled, you will need to enter a wireless client equipment PIN code in the field.
- **WPS Summary:** Shows the current state of Wi-Fi protected settings, including authorized mode, encryption type, default key and other information.
- **WPS Current Status:** Idle means WPS is in idle state. Start WSC process means the process has been started and waits for being connected. Configured means the negotiation is successful between server and client equipment.
- **WPS Configured:** "Yes" means WPS feature is enabled and is effective. "Not used" means it is not used.
- **WPS SSID:** Shows the main SSID set by WPS.

- **WPS Auth. Mode:** The authorization mode deployed by WPS.
- **WPS Encryption Type:** The encryption type used by WPS.
- **WPS key:** The key generated by AP automatically.
- **AP PIN KEY:** The PIN code used by default.
- **Reset OOB:** When this button is pressed, the WPS client will be in the idle state, and WPS indicator will be turned off. AP will not respond to the WPS client equipment requests and the security mode will be set to WPA mode.

5. WDS Settings

WDS (Wireless Distribution System) is used to expand wireless coverage area. This Router provides three modes: Lazy, Bridge and Repeater.

- **Lazy:** In this mode, the connected device can be in Bridge or Repeater mode.
- **Bridge Mode:** You can wirelessly connect two or more wired networks using this mode. You need to add the Wireless MAC address of the connecting device to the Router's AP MAC address table or select the one from the table.
- **Repeater Mode:** in this mode, you need to add the MAC address of the connecting device into the Router's AP MAC address table and the connecting client should be in Lazy, Repeater or Client mode.
- **Encryption Type:** Select one from WEP, TKIP, AES here.
- **Pass phrase:** Enter the key.
- **AP MAC Address:** Input the MAC address of another wireless router you want to connect.

Note: It is recommended that two wireless routers keep the same bandwidth, channel number, and security settings. Apply the settings and reboot the Router to activate the settings.

6. Access Control

To secure your wireless LAN, the wireless access control is actually based on the MAC address management to allow or block the specific client equipment to access the wireless network.

- **MAC Address Filter:** Enable/disable MAC address filter. Select "Off" to exclude the MAC address; "Disable" to prevent the MAC addresses in the list from accessing the wireless network; "Allow" to allow the MAC address in the list to access the wireless network.
- **MAC Address Management:** Input the MAC address to implement the filter policy. Click "Add" to finish the MAC add operation.
- **MAC Address list:** Shows the added MAC addresses. You can add or delete them.

7. Connection Status

This page shows wireless client equipment connection status, including MAC address, Channel bandwidth, etc.

- **MAC Address:** Shows current MAC addresses of the hosts connected to the Router.
- **Bandwidth:** Shows current frequency bandwidth the wireless client equipment uses.

5.5 DHCP Server

1. DHCP Settings

DHCP (Dynamic Host Control Protocol) is used to assign an IP address to the computers on the LAN/private network. When you enable the DHCP Server, the DHCP Server will automatically allocate an unused IP address from the IP address pool and will assign it to the client equipment automatically. Hence, you need to specify the starting and ending address of the IP Address pool.

- **DHCP Server:** Activate the checkbox to enable DHCP server.
- **IP Address Start/End:** Enter the range of IP address pool for DHCP server distribution.
- **Lease Time:** The duration of the IP address lease.

2. DHCP List and Binding

The Static IP assignment is used to add a specific static IP address to the certain MAC address. You can view the related information in the DHCP server list.

- **IP Address:** Enter the IP address which needs to be bounded.
- **MAC Address:** Enter the MAC address of the computer you want to assign the above IP address. Click "Add" to add the entry to the list.
- **Hostname:** The name of the computer you wish to add the IP address.
- **Lease Time:** The duration of the IP address lease.

5.6 Virtual Server

1. Single Port Forwarding

The Router can be configured as a virtual server on behalf of local services behind the LAN port. The remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding. The Single Port Forwarding allows you to set up public services such as web servers, ftp, e-mail and other special Internet applications on your network.

- **External Port:** This is the external port number for the server or Internet application, for example, port 21 is used for ftp service.
- **Internal Port:** This is the port number set by the router for LAN computer. The Internet traffic from the external port will be forwarded to the internal port.
- **IP Address:** Enter the IP address of the PC where you want to set the applications.
- **Protocol:** Select the protocol (TCP/UDP/Both) for the application.
- **Delete/Enable:** Click to check it for corresponding operation.
- **Popular Service Ports:** the list of popular services such as DNS, FTP, etc. Please select from the drop-down menu to select the desired one.
- **Add:** Add a service port.

Note: If you set the virtual server on the service port 80, you will need to set the Web management port to any value except 80, i.e. 8080. Otherwise, there will be a conflict. Please use the Remote Web Management page to set the port value.

2. Port Range Forwarding

This section is used to set the port range forwarding. The Port Range Forwarding allows you to set up public services such as web servers, ftp, e-mail and other special Internet applications on your network.

- **Start/End Port:** Enter the starting/ending port number which ranges the External ports used to set the server or Internet applications.
- **IP Address:** Enter the IP address of the PC where you want to set the applications.
- **Protocol:** Select the protocol (TCP/UDP/Both) for the application.
- **Delete/Enable:** Click to check it for corresponding operation.
- **Popular Service Ports:** the list of popular services such as DNS, FTP, etc. Please select from the drop-down menu to select the desired one.
- **Add:** Add a service port.

3. ALG Service Settings

ALG (Application Layer Gateway): An application layer gateway (ALG) allows customized NAT traversal filters to be applied on the gateway to support address and port translation for certain application layer protocols such as FTP, BitTorrent, SIP, RTSP, file transfer applications, etc.

In order for these protocols to work through NAT or a firewall, either the application has to know the address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open port mappings dynamically as required. Allowed application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its filter criteria.

Usually allows client applications to use dynamic TCP/ UDP ports to communicate with the known ports used by the server applications. In the absence of an ALG, either the ports would get blocked or the network administrator would need to open a large number of ports in the firewall; which can lead to the additional network vulnerabilities.

In the default ALG settings, the following protocols are enabled. It is recommended to keep the settings unchanged.

1. FTP
2. TFTP
3. PPTP
4. IPSec
5. L2TP

4. DMZ Settings

The DMZ function is used to allow one computer on the LAN to be exposed to the Internet for a special-purpose service such as Internet gaming or video conferencing.

- **DMZ Host IP Address:** The IP address of the computer you want to expose.
- **Enable:** Click the checkbox to enable the DMZ host.

IMPORTANT:
When the DMZ host is enabled, the firewall settings of the DMZ host will be disregarded.

5. UPNP Settings

UPnP (Universal Plug and Play) allows the system (Windows Me and Windows XP only) to configure the device for various Internet applications automatically.

- **Enable UPnP:** Click the checkbox to enable the UPnP.

5.7 Traffic Control

1. Traffic Control

Traffic control is used to limit communication speed over the LAN. Up to 20 entries can be supported to control a maximum of 254 PCs'.

- **Enable Traffic Control:** Is used to enable or disable the internal IP bandwidth control. The default is "Disabled".
- **Interface:** Is used to limit the uploading and downloading bandwidth on WAN port.
- **Service:** Is used to select the controlled service type, such as HTTP service.
- **IP Starting Address:** The first IP address for traffic control.
- **IP Ending Address:** The last IP address for traffic control.
- **Uploading/Downloading:** Specify the traffic direction for the selected IP addresses: upload or download.
- **Bandwidth:** Specify the upload/download Min./Max. traffic speed (KB/s). It cannot exceed the WAN speed.
- **Apply:** Enable the edited rule. If not, the rule will be disabled.
- **Add To List:** After editing the rule, click the "Add To List" button to add the current rule to rule list.
- **Apply:** Click "Apply" to activate the current rule.
- **Cancel:** Click "Cancel" to roll back to the last saved settings..

2. Traffic Statistics

Traffic statistics is used to show the LAN PC's traffic information.

- **Enable:** check to enable traffic statistics. By default traffic statistics is disabled, which can improve the Router's data handling. If it is enabled, the data traffic information page will be updated every 5 seconds.
- **IP address:** The IP address to be shown.
- **Upload rate:** the speed of upstream data per second (Kbyte/S).
- **Download rate:** the speed of downstream data per second (Kbyte/S).
- **Sent packets:** sent from the PC packets.
- **Sent bytes:** Sent from the PC information amount in Mbytes.
- **Received packets:** The number of packets received from the Router.
- **Received bytes:** The information amount in Mbytes received from the Router.

5.8 URL Monitor

1. URL Monitor

This feature is used to track users' Internet activity.

- **Enable URL Monitor:** After checking this feature, the Router will record LAN computer's URL information, including the visited Websites, LAN IP addresses and time. The Router can store up to 500 entries. After 500 entries, the counter will clear all the records and will restart the URL tracking again. If the Router is powered off and restarted, the records will be also lost. By default is disabled.
- **Enable Email:** When enabled, the URL records will be sent to the specified e-mail. This can be used as a workaround for saving the records without loosing them.
- **Receiving E-mail Address:** Enter the e-mail address you wish to receive the messages to.
- **SMTP Server Address:** Enter the SMTP server address here.
- **Sending Email Address:** Enter the e-mail address you wish to send from.
- **Username:** Enter the username for the e-mail account you wish to send from.
- **Email Password:** Enter the password for the e-mail account you wish to send from.
- **Time Triggering Interval:** is used to set e-mail sending time interval. The time can vary from 30 to 1440 minutes.

Example: if you set "30" for time triggering interval, the Router will be sending e-mail messages from "Sending Email Address" to "Receiving Email Address" every 30 minutes. After the message is sent the device will clear all the records and will start the logging again.

- **Entry Triggering Interval:** To set e-mail sending based on entry number. The entries number can vary from 100 to 500.

5.9 Security Settings

1. Client Equipment Filtering Settings

In order to better manage the network computers, you can use data packet filter function.

- **Client Equipment Filtering:** Check to enable client filter.
- **Access Policy:** Select one from the drop-down menu.
- **Enable:** Check to enable the access policy.
- **Delete the Policy:** Click "Clear" button to clear all settings for the selected policy.
- **Filtering Mode:** Check the corresponding radio button in order to enable or disable the Internet access.
- **Policy Name:** Enter a name for the selected access policy.
- **IP Start/End:** Enter the starting/ending IP address.

- **Port No.:** Enter the port range based on the protocol for access policy.
- **Protocol:** Select the desired protocol (TCP/UDP/Both) from the drop-down menu.
- **Time:** Select the time range for client filter to be enabled.
- **Days:** Select the day(s) to run the access policy on.

2. URL Filter Settings

In order to control computers' access to websites, you can use URL filtering. This way you can allow or forbid access to certain websites at the time you set.

- **URL Filter:** Check to enable URL filter.
- **Access Policy:** Select the desired from the drop-down menu.
- **Enable:** Check to enable the access policy.
- **Delete the Policy:** Click "Clear" button to clear all the settings for the policy.
- **Filtering Mode:** Check the corresponding radio button in order to enable or disable the Internet access.
- **Policy Name:** Enter a name for the selected access policy.
- **Start/End IP:** Enter the starting/ending IP address.
- **URL Strings:** Specify the text strings or keywords needed to be filtered. If the URL contains these, the web page will not be accessible and displayed.
- **Time:** Select the time range for the filter to be enabled.
- **Days:** Select the day(s) to run the access policy on.
- **Apply:** Click "Apply" for the settings to take effect.

3. MAC Address Filter

In order to better manage the computers in LAN, you can control the network computers' access to Internet using MAC Address Filter.

- **MAC Address Filter:** Check to enable MAC address filter.
- **Access Policy:** Select the desired from the drop-down menu.
- **Enable:** Check to enable the access policy.
- **Delete the Policy:** Click "Clear" button in order to clear all settings for the policy.
- **Filtering Mode:** Check the corresponding radio button in order to enable or disable the Internet access.
- **Policy Name:** Enter a name for the access policy selected.
- **MAC Address:** Enter the MAC address you want to run the access policy for.
- **Time:** Select the time range for the filter to be enabled.
- **Days:** Select the day(s) to run the access policy on.
- **Apply:** Select "Apply" for the settings to take effect.

4. Prevent Network Attack

This section allows protection of the internal network from external attacks such as SYN Flooding attack, Smurf attack, LAND attack, etc. Upon detection of the unknown attack, the Router will reject the traffic automatically.
You will find the attacker's IP address in the "System Log".

- **Prevent Network Attack:** Check to enable the Attack Prevention.

5. Remote Web Management

This section allows the network administrator to manage the router remotely. If you want to access the router remotely, please select the "Enable".

- **Enable:** Check to enable remote web management.
- **Port:** The management port has to be open for external access. The default value is 8080.
- **WAN IP Address:** Specify the range of IP Addresses for remote management.

6. Local Web Management

Local web management is the alternative to the remote web management. It allows the network administrator to manage the router over LAN. Any network PC can access the Web management utility by default. Please set the MAC addresses of the network computers to have access to the management function.

- **Enable:** Check to enable the local web management.
- **MAC Address:** Enter the MAC addresses of network computers.

7. WAN Ping

The Ping application is used to check the status of your Internet connection. When disabling the test, the system will ignore the ping test from WAN.

- **Ignore Ping from WAN:** If this feature is enabled, the system will ignore pinging from WAN.

5.10 Routing Settings

1. Routing Table

The main router task is to set and use the best path for every data frame, and transfer this data frame to a destination point. So, it's essential for the router to select the optimal path, i.e. using routing calculations. In order to implement this function, the transferring paths, i.e. routing table, are saved in the router.

2. Static Routing

Static routing is used for the manual method of setting-up routing for successful packet forwarding.
This section is used to configure the Router's static routing.

- **Destination LAN IP:** The address of the remote host with which you want to make a static route.
- **Subnet Mask:** The logically visible subdivision of the Destination IP network.
- **Gateway:** The gateway of the next hop, usually the Router or host's IP address.

5.11 System Tools

1. Time Settings

This section is used to select the time zone for your location. If you turn off the Router, the time settings will reset. However, the Router will automatically obtain the correct time again once it is connected to the Internet.

- **Time Zone:** Select your time zone from the drop-down menu.
- **Customized time:** Enter the custom time you want to set.

Note: When the Router is powered off, the time settings will reset. For the router to obtain correct time automatically, you will need to connect it to the Internet. Otherwise, please set the time manually on this page. After the time is set you can use time-dependant features (e.g. filtering, etc.).

2. DDNS

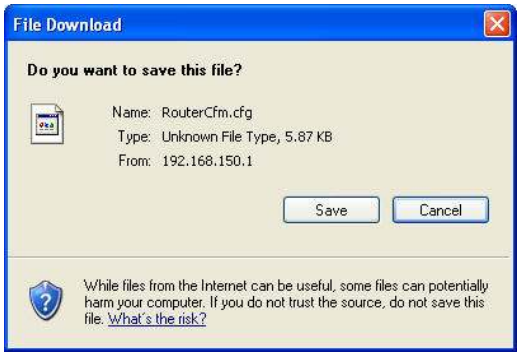
The router supports DDNS (Dynamic Domain Name System). It is used to assign a fixed host and domain name to a dynamic Internet IP address. If you want to activate this feature, please select "Enable" and set a DDNS service provider.

- **Main Features:** in some cases your ISP will provide dynamic IP address. DDNS is used for dynamic IP address to be linked with fixed domain. DDNS can help you establish connection to your home or company.
- **DDNS:** Check the radio button to enable or disable the DDNS service.
- **Service Provider:** Select the desired one from the drop-down menu and press "Sign up" for registration.
- **User Name:** Enter the user name which is the same as the registration name.
- **Password:** Enter the password you set.
- **Domain Name:** Enter the domain name which (optional).

3. Backup/Restore Settings

The device provides backup/restore settings, so you need set a directory to keep these parameters.

- **Backup Settings:** Click "Backup" button to back up the Router's settings. Select the path to save the configuration file to.



Click "Save" to save the configuration file.

- **Restore Settings:** Press "Browse" button to locate the backup files.

Select the needed configuration file and press "Restore" button to restore your saved settings.

4. Restore to Factory Default Settings

This function is used to reset all settings to the default (factory) values. This means the Router will lose all the settings you have set. So please write down the settings if necessary.

- **Restore:** Press this button to restore the settings to the default values.
- **Factory Default Settings:**

Username: admin
Password: admin
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0

Note: Please restart the device to roll back to the default settings.

5. Firmware Upgrade

The Router provides the firmware upgrade (update) capabilities.

- **Browse:** click this button to locate and select the firmware upgrade (update) file.
- **Upgrade:** press this button to start updating. After the upgrade is completed, the Router will reboot automatically.

6. Reboot the Router

Router reboot makes the newly applied settings to go into effect, also it can be used to restart the Router in case of operational failure.

Reboot the router: Press this button to reboot the device.

7. Password Change

This section is used to set a new username and password to better secure your router and network.

- **Username:** Enter a new user name.
- **Old Password:** Enter the old password.
- **New Password:** Enter a new password.
- **Re-enter to Confirm:** Re-enter to confirm the new password.

Note: It is strongly recommended to change the password to secure your network and the Router.

8. System Log

This section is used to view the system log. Click the "Refresh" button to update the log. Click "Clear" to clear all recorded information. The maximum length of the log is 150 records. Records are being cleared automatically after 150 entries are recorded.

- **Refresh:** Press this button to update the log.
- **Clear:** Press this button to clear the current log records.

5.12 Logout

After you are done with router settings, press "Yes" on the logout page, to logout from the web management page.

Chapter 6: Troubleshooting

This section provides answers to frequently asked questions. If your problems are not on the list, please contact your reseller or send your e-mail request to support@teltonika.eu.

1. I am unable to login to the Web-interface of the Router after entering the IP address in the address field.

Step 1: Check if the Router is working properly. Once the device is powered on, the SYS LED indicator on the top panel is turned on. If it is not, please contact us.

Step 2: Check the network cable connection and the corresponding LED indicator on the top panel – it should be either ON or blinking.

Run "Ping" application on the connected equipment and see if Ping requests get through to the Router's IP address (default: 192.168.0.1). If Ping works well, please check your proxy server settings. If Ping fails, please reset the router. You can also try resetting the router to the factory defaults by pressing and holding "RESET" button for 7 seconds. Then repeat the ping operation. If it still does not work, please contact us.

2. I forgot my login password and cannot enter the Web-interface. What should I do?

Press the "RESET" button for 7 seconds to restore the Router to factory defaults and then use the default login credentials (admin/admin).

3. The computer connected to the Router shows IP address conflict. What should I do?

Please check if there are other DHCP servers on the network. If there are, please disable them.

The default IP address of the Router is 192.168.0.1. Please make sure the same address is not used by other devices. If there are two computers with the same IP addresses on the network, please change one of them.

4. I am unable use E-mail service and access the Internet. What should I do?

For ADSL connection and Dynamic IP please try modifying the MTU value (default: 1492). Please go to the "WAN Settings" and change the MTU value to 1450 or 1400.

5. I am using Dynamic IP, how should I set it up?

Please enter the Web-Interface and go to the Setup Wizard. Select "Dynamic IP" connection type and click "Save" to activate it. In some cases (when required by ISP) you will need to assign certain MAC address to the router. Please use "MAC Address Clone" under "Advanced Settings" of the Web-interface to assign i.e. your computer's MAC address and click "Apply" to activate the changes.

6. How do I share my computer resources with other network/Internet users?

If you want network/Internet users to have access to the internal server via the Router, you can configure the "Virtual Server".

Step 1: setup the internal server, make sure local network users are able to access this server and know the service port used. For example: Web server port is 80; FTP is 21; SMTP is 25 and POP3 is 110.
Step 2: go to Router Web-Interface and enter "Virtual Server" section. Select "Single Port Forwarding".
Step 3: enter the external service port, for example: 80.
Step 4: enter the internal Web service port, for example: 80.
Step 5: Enter the internal server IP address.
Step 6: Select the communication protocol used by the internal server: TCP, UDP or ICMP.
Step 7: Press "Apply" to activate the settings.
The following table is listing the popular applications and their default service ports:

Server	Protocol	Service Port
WEB Server	TCP	80
FTP Server	TCP	21
Telnet	TCP	23
NetMeeting	TCP	1503、1720
MSN Messenger	TCP/UDP	File Send:6891-6900(TCP) Voice:1863-6901(TCP) Voice:1863-5190(UDP)
PPTP VPN	TCP	1723
SMTP	TCP	25
POP3	TCP	110

7. I am having issues connecting to Internet via 3G modem. What should I do?

a. Please make sure the SIM card is inserted to your 3G Modem Card, the 3G data is enabled. Try using your 3G Modem Card to access the Internet connecting it to the computer directly.
b. Please make sure your 3G Modem is properly connected to the Router's USB port.
c. Please make sure your 3G Modem is compatible with the Router. You can search the related model No. on the compatible product list (Chapter 7:).
d. Please make sure 3G settings are entered properly as provided by ISP.
e. Please download the latest firmware and upgrade the router. Try using your 3G modem with the router.
f. If you still can't access the Internet, please contact us.

8. I am having issues accessing Internet over wireless WAN. What should I do?

a. Please make sure you have entered valid settings (SSID, MAC address etc.).
c. Please make sure WAN IP address range differs from LAN IP address range.
d. Please make sure the antenna is properly mounted.

If you still can't access the Internet, please contact us.

9. How do I decrease 3G Internet expenses?

a. 3G ISP will charge you based either on traffic used or the time connected. It is recommended to remove your 3G Modem or turn the Router off if you do not use 3G Internet connection.

b. You can also track the connected network equipment to see the traffic activity.

Chapter 7: Compatible 3G Modems list

Brand	Model	Brand	Model
TELTONIKA	UM5100	HUAWEI	EC169
D-LINK	DWM_162U5	HUAWEI	EC1260
D-LINK	DWM_162	HUAWEI	EC1261
DCWL	390	HUAWEI	ET128
STAR-NET	EV2000	HUAWEI	E1750
GXZG	GX100C	HUAWEI	EC226
MACAO	CTM H21	HUAWEI	E1630 Tmobile
WEWINS	U602D	HUAWEI	E176G
HiNet	E220	HUAWEI	E176
TURKCELL	E176G	HUAWEI	E180
Vodafone	E220	HUAWEI	EC170BT
Vodafone	K3520	HUAWEI	EC168C
Cricket	UM185C	HUAWEI	E160E
Cricket	A600	HUAWEI	E1550
T-Mobile	UMG181	HUAWEI	EZ220 3G UK
AT&T	USBConnect mercury	ZTE	MU351
AT&T	GI0322	ZTE	AC580
Sprint	USB 598	ZTE	AC581
Sprint	U300	ZTE	AC560
Sprint	U760	ZTE	MF626 TMobile
Verizon	USB760	ZTE	AC2736
Verizon	UMW190VW	ZTE	AC2746
Verizon	UMW190	ZTE	AC8710
Verizon	UMW175VW	ZTE	MF637U
Ttec	WS119	ZTE	MU350
Ttec	WS220	ZTE	MF622
CCU	680	ZTE	MF627
CCU	650	ZTE	AC2726
Intertel leader	C810	ZTE	AC8700
Sierra	USB306	ZTE	AC8710
DTM	5731E		