

# **WiMAX Outdoor Router**

# **User Manual**

Version 1.07 Applies to: RUT723, RUT725, RUT735 and RUT738

### **LEGAL NOTICE**

Copyright © 2012 TELTONIKA Ltd. All rights reserved. Reproduction, transfer, distribution or storage of part or all of the contents in this document in any form without the prior written permission of TELTONIKA Ltd is prohibited. The manufacturer reserves the right to modify the product and manual for the purpose of technical improvement without prior notice.

Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

# **ATTENTION**



Before using the device we strongly recommend reading this user manual first.



Do not rip open the device. Do not touch the device if the device block is broken.



The device should only be serviced by qualified personel.



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



The device is water-resistant (IP65) and can be mounted outdoor, though power adapter must be kept dry.

# Table of contents

00010 00000

LEGAL NOTICE	2
ATTENTION	2
TABLE OF CONTENTS	3
SAFETY INFORMATION	4
DEVICE SERVICE	5
PRODUCT OVERVIEW	6
INTRODUCTION	6
Package contents	6
System requirements	6
INSTALLATION GUIDELINES	7
Surge Protection Recommendations	7
Preparing an Ethernet Cable	7
Mounting device	9
WEB GUI OVERVIEW	10
CONNECTING TO THE WEBUI	10
WEBUI STRUCTURE	11
Status	11
Network	12
IP address	
DHCP server	
Dynamic DNS	
OpenVPN	
FIREWALL	15
Port joi waraing Mac filterina	15
IP filtering	
Demilitarization zone	
Administration	
Settings	
Firmware	19
Password	19
Авоит	19
TROUBLESHOOTER:	20
Under Windows 7	20
UNDER MAC OS	21
Under Linux (GNOME 3)	22
TECHNICAL SPECIFICATIONS:	23
Electrical, Mechanical & Environmental:	23

## **SAFETY INFORMATION**

In this section you will be introduced on how to use a WiMAX Outdoor Router safely. You have to be familiar with the safety requirements before using the device! We suggest you to adhere to the following recommendations in order to avoid personal injuries and or property damage.



The device is intended for supply from a Limited Power Source (LPS) that power consumption should not exceed 15VA and current rating of overcurrent protective device should not exceed 2A.



The highest transient overvoltage in the output (secondary circuit) of used PSU shall not exceed 71V peak.



The device can be used with the Personal Computer (first safety class) or Notebook (second safety class). Associated equipment: PSU (power supply unit) (LPS) and personal computer (PC) shall comply with the requirements of standard EN 60950-1.



Do not mount or serve device during a thunderstorm.



Device is mounted in limited access areas.



To avoid mechanical damages to the device it is recommended to transport it packed in a damage-proof pack.



<u>Protection in primary circuits of associated PC and PSU (LPS)</u> against short circuits and earth faults of associated PC shall be provided as part of the building installation.



When installing the WiMAX router outdoor, make sure that proper lightning surge protection and grounding precaution are taken according to local electrical code. Failure it do so may result in personal injury, fire or equipment damage. This automatic two pole protective device disconnects all the associated equipment (fig 1). To disconnect the device plug off the AC-DC power adapter from the wall outlet or power strip. The gap between contacts should be no less than 3mm.



1 Figure: Building installation scheme

### **Device service**

Signal level of the device depends on the working environment. In case the device starts working insufficiently, please refer to qualified personnel in order to repair this product.

There are no exchangeable parts within the device including 2A quick acting fuse.

Device should be serviced only by qualified personel. Opening the device will void the warranty for this product. We recommend forward it to a repair center or to the manufacturer.

Labels with product information (serial number and MAC address) can be found on the bottom side of the device as well as on the packaging.

# **PRODUCT OVERVIEW**

#### Introduction

Teltonika RUT723, RUT725, RUT735 and RUT738 are outdoor routers offering high speed data rate connectivity to the WiMAX networks. Router is compliant with IEEE802.16e-2005 WiMAX Wave 2. 10/100 Base-T interface and integrated DHCP server allow easy connection to any device with Ethernet cable. Teltonika outdoor WiMAX router is ideal for distant locations. High gain MIMO antenna improves coverage and pole mounting kit ensures stable signal conditions. Included POE adapter allows the device to function with only Ethernet cable connected.

#### Package contents

WiMA	WiMAX Outdoor Router					
•	WiMAX Outdoor Router					
•	Pole mounting kit					
•	POE Adapter					
٠	2 x LAN cable					

- Waterproof RJ45 connector kit
- Quick Start Guide

**Note**: The provisioning information is provided by your service provider, therefore any questions regarding connectivity problems should be addressed to it.

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

**Note**: Using a not IEEE 802.3af-2003 compliant POE adapter with the WiMAX Outdoor Router will cause damage and void the warranty for this product.

#### System requirements

- Wired network connection.
- Windows XP, Windows Vista, Windows 7, MAC OS X, or a Linux-based operating system.
- A web browser must have a flash player plug-in (version 10 or higher) in order to access the Web GUI for network configuration.

# **Installation guidelines**

#### **Surge Protection Recommendations**

Antenna should be placed on the mast on the level that is at least 1 meter lower than the mast's top. In this case lightning is more likely to strike the mast instead of the antenna. The mast is to be grounded on the grounding contour according to your local standards. Grounding will protect your equipment from voltage surges created by nearby lightning strikes but will not protect from a direct strike.

- Mount lightning arrestor as close as possible to where the lead-in enters the house.
- Grounding wires for both mast and leadin should either be a copper or an aluminum wire, number #8 or larger.
- Lead-in wire from antenna to lightning arrestor and mast ground wire should be secured to the house with stand-off insulators, spaced 1.2 to 1.8 meter apart.
- In the case of a "ground up" antenna installation, it may not be necessary to ground the mast if the mast extends 1.2 meter or more into the earth.



#### **Preparing an Ethernet Cable**

To provide waterproof seal, the Ethernet port use custom waterproof cable connector. Terminate your Ethernet cable with this connector as described in the following procedure. Use ruggedized, shielded, outdoor-rated CAT5 Ethernet cable. The cable length should not exceed 100 meters (300 feet).

Device has included waterproof RJ45 connector kit. Use it together with LAN cable and assemble as shown in the picture below. In order to connect the LAN cable to the router:

- 1. Plug the cable into the RJ45 socket
- 2. Tighten the screw around the RJ45 socket
- 3. Tighten the nut around the LAN cable





Pin	Signal ID	T568A Color	T568B Color	Pins on plug face (socket is reversed)
1	TX+	white/green stripe	white/orange stripe	
2	TX-	green solid	orange solid	Pin Position
3	RX+	white/orange stripe	white/green stripe	76 - 554 - 32
4	48V out	Due solid	0 blue solid	
5	48V out	white/blue stripe	white/blue stripe	
6	RX-	orange solid	green solid	
7	48V return	white/brown stripe	white/brown stripe	
8	48V return	brown solid	brown solid	

Cabling and powering colors are listed in a table below.

The device is powered by the included POE adapter. Connect the Outdoor WiMAX router to the PoE adapter's "Data & Power Out" port via an Ethernet cable. Connect the "**Data In**" port to your computer or switch. Plug the POE adapter into an AC socket to power the device up. The Green light on the bottom left corner of the Outdoor Router (just above RJ45 socket) indicates that the device is powered.





#### **Mounting device**

Device pole mounting kit contains these elements:



STEP 1	STEP 2	STEP 3
Fix "L" bracket to the router	Assemble pole bracket clamp and	Adjust right direction and
	"U" bolt on a pole	tighted the nuts.

Install Router as high as possible over specific level (at least 1 meter lower than a mast's top). Proximity of other antennas should be avoided. Avoid reflecting surfaces like: building with reflective windows, water surfaces or wet grounds. To obtain the best performance results, it is necessary to perform a precise analysis of a signal loss conditions, signal propagation path zone and possible obstructions. Antennas can be installed either with vertical or horizontal polarization (depends on network provider). Device position and angle of antenna has big impact on performance. To achieve the best link quality on the radio link, connect to web user graphical interface (WebUI). By monitoring **Status** window in WebUI rotate (and/or) tilt the antenna to achieve the best signal levels and fix the antenna.

# Web GUI OVERVIEW

In this section you will be briefly introduced to our user interface.

**Note:** we use an intuitive tool tip system in our web user interface which displays additional data for the user. To see this data hover your mouse cursor above the field. Also, if the frame of the field becomes red, it usually means that the data in the field is incorrect, in this case look into red tool tip for more information.

#### **Connecting to the WebUI**

To connect to the configuration web page do the following steps:

- 1. Make sure that IP address is set to be obtained automatically via DHCP on your computer.
- 2. Type **192.168.0.1** to your favorite internet browser. Skip the step 2 if the password is disabled.
- 3. Window asking for authentication will pop up. Enter your username and password (default: username: user, password: user) and press enter.

The server 192.168.0.1:80 requires a username and password. The server says: WiMAX.						
User Name:						
Password:						
	Cancel Log In					

4. Status window will appear in a few seconds:

	<b>X</b> TE	LTON	IIKA		
Status	Firewall	Network	Administration	About	Connected
Upti	ime		0:48:05		
Sigr	nal quality		88% (28	dB)	
Sigr	nal strength		-59 dBr	n	
Exte	ernal IP		88.88.2	22.88	
МАС	C address		00:1E:0	0:00:00:	00
BS	MAC addres	s	00:1E:0	0:00:00:	01
4	40 —				
3	30				
명 2	20				V-012 0
:	10				
	0				
	60				U Signal Quality
	-30				
Ē	-50				
ab .	-70				
-	-90				0
	00				Signal Strength



First page of WebUI



#### WebUI structure

Our modern web user interface provides you with all the tools needed within the five main pages: Status, Network, Firewall, Administration, About.

#### **Status**

Status	Firewall	Network	Administration	About	
Uptin	ie		0:48:05		
Signa	d quality		88% (28	dB)	
Signa	d strength		-59 dBm		
Exter	nal IP		88.88.2	22.88	
MAC	address		00:1E:0	0:00:00:00	
BS M	AC address	i	00:1E:0	0:00:00:01	
1					

#### Status page

The status page consists of 6 properties that define the current state of the WiMAX Outdoor Router:

- 1. Uptime amount of time since the last reboot (or plug in).
- 2. Signal quality the quality of a signal in percents (and decibels).
  - <30% poor >30% <50% decent >50% <90% good
  - >90% very good

**Note:** signal quality depends on the distance between the device and the base station, plus other factors: interference with other devices, etc.

- 3. Signal strength the strength of the signal in dBm.
- 4. External IP IP which was assigned by the base station to your device.
- 5. MAC address physical address of the WiMAX connection module.
- 6. BS MAC address physical address of the base station.



#### **Network**

Network settings page allows the user to change the IP address, net mask and DHCP server settings.

#### **IP** address

IP address	DHCP server	Dynamic DNS	OpenVPN	J
	LAN config	juration		
IP a	ddress 192	.168.0.1		
Ne	etmask 255	.255.255.0		
Apply				

IP address settings page

IP address – IP address of the router. Netmask – mask used to divide IP address into subnets.

#### **DHCP** server

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network.

IP address	DHCP server	Dynamic DNS	OpenVPN	
	DHCP s	erver settings		
	Enable	$\checkmark$		
	First IP address	192.168.0.1		]
	No. of users	200	*	]
	Lease time	6000	*	]
Apply				

#### DHCP server form

Enable – check to enable the DHCP server. First IP address – First IP from the range to be leased. No. of users – number of IP addresses to be leased. Lease time – time after the leased IP expires.



#### **Dynamic DNS**

Dynamic DNS (DDNS) is a domain name service allowing to link dynamic IP addresses to static hostname. To start using this feature firstly you should register to DDNS service provider.

IP address	DHCP server	Dynamic DNS	OpenVPN		
	Dynamic	DNS settings			
	$\checkmark$				
P	rovider no-ip	.org	•		
Use	rname				
Pas	sword				
Hos	tname				
Renew	period		÷.		
Apply					

#### DDNS form

**Provider** – your dynamic DNS service provider selected from the list.

Username – name of the user account.

Password – password of the user account.

Hostname – domain name that you will be able to use instead of your IP address. Renew period – time interval to check if IP address of the device have changed.



#### **OpenVPN**

VPN (virtual private network) is a secure network that provides remote offices or traveling users an access to a central organizational network.

IP address	DHCP server	Dynamic DNS	OpenVPN		
	Gen	eral settings		Loc	al network settings
Enable OpenVPN		$\checkmark$		Local tunnel IP	10.8.0.2
	VPN mode	P2P Server	•	Ren	note network settings
	Protocol	UDP	•	Endpoint IP	84.15.196.36
LZ	O compression	$\checkmark$		Tunnel IP	10.8.0.1
				Network IP	192.168.99.0
				Network mask	255.255.255.0
	Kee	ep alive settings		Stat	tic key
	Enable	$\checkmark$			Select key file
	Interval	10	* *		Upload key file
	Timeout	60	*		Download key file

Apply OpenVPN form

#### General:

Enable OpenVPN – enables VPN functionality.

VPN mode – changes VPN mode Client/Server.

**Protocol** – use **TCP** or **UDP** for transmitting packets.

LZO compression – check the box to enable fast adaptive LZO compression.

#### Network:

**Local tunnel IP** – specifies the IP address of the local VPN tunnel endpoint. **Endpoint IP** – specifies server IP address.

Tunnel IP – specifies the IP address of the remote VPN tunnel endpoint.

**Network IP** – specifies the remote network IP.

Network mask – specifies the remote network subnet mask.

#### Keep alive:

Enable – turns on "Keep alive" feature.

Interval – specifies time interval to check if VPN connection is still alive.

**Timeout** – specifies time span for the network to respond.



#### **Firewall**

Firewall page lets you configure firewall settings to meet your requirements. It includes portforwarding, MAC filtering and IP filtering

#### Port forwarding

Port forwarding is the process of translating the address and port number of a packet to a new destination.

Follow these steps to add a port-forwarding rule:

- 1. Enable check to enable the Port forwarding.
- 2. Press the + button.

Port forwarding	MAC filtering	IP filtering DMZ						
Por	Port forwarding							
Ena	ble 🗹							
Name	Protoco	I Extern	al Port Destinatio	n IP Destination Port				
PPTP	tcp	1723	192.168.0.	8 1723				
+ .								

Apply

Port forwarding form

The following port-forwarding rule creation window will pop-up. Choose a rule type (single port or port range) and fill the fields in a window to define your rule:

- Predefined rule select from a list of most common rules.
- Name the name of the rule that will be visible in the list of your defined rules.
- External port from/to external port range to be redirected to an identical internal port range.
- External port external port to be redirected to Internal port.
- Internal port port used by the destination device to receive data.
- **Protocol** protocol in which rule operates.
- **Destination IP** the address of the device to which all the data coming to the selected external ports is forwarded to.

New port-forwarding rule	×	New port-forwarding rule	×
	Single port 💌		Port range 💌
Predefined rule	-	Predefined rule	
Name	Single forward #1	Name	Port Range forward #1
External port	80	External port from	80 *
Internal port	80	External port to	86
Protocol	TCP/UDP 💌	Protocol	TCP/UDP 💌
Destination IP	192.168.0.156	Destination IP	192.168.0.156
OK Cancel		OK Cancel	

New port-forwarding rule windows

- 3. Press **OK** button to accept the rule.
- 4. Press Apply to save the rules to the configuration.



#### Mac filtering

MAC filtering is a security access control method used to determine access to the network by physical address.

Follow these steps to add a MAC filtering rule:

- 1. Enable check to enable the MAC filtering.
- 2. Press the + button.

Port forwarding	MAC filtering	IP filtering	DMZ			
<b>MAC</b> Enat	filtering					
Name	1	MAC address		Filtering type	Chain	
MAC block #1	(	00:86:40:99:00	13	DENY	FORWARD	
MAC block #1	(	00:86:40:99:00	13	DENY	INPUT	
+ .					I	
Apply						

Mac filtering form

3. The following MAC filtering rule creation window will pop-up.

New MAC filtering rule	×
Name	MAC block #3
Filtering type	DENY -
MAC address	00:1E:44:82:45:11
OK Cancel	

New MAC filtering rule window

- Name MAC filtering rule name.
- MAC address physical address that you want to block from connecting to and/or through the router.
- 4. Press **OK** to add the rule.
- 5. After adding all the rules that you needed, press **Apply** to save the rules to the configuration.



#### IP filtering

IP filtering is a security access control method used to determine access to the network by IP address.

Follow these steps to add an IP filtering rule:

- 1. Enable check to enable the IP filtering.
- 2. Press the + button.

Port forwarding	MAC filtering	IP filtering	DMZ	
IP fil	terina			
	<b>T</b>			
Enar	ole 💌			
Name		lp add	ress	Chain
IP block #1		192.1	58.0.9	INPUT
IP block #1		192.1	68.0.9	FORWARD
+ .				
Apply				

IP filtering form

3. The following IP filtering rule creation window will pop-up.

New IP filtering rule	×
Name	IP block #1
lp address	192.168.0.123
OK Cancel	

New IP filtering rule window

- Name IP filtering rule name.
- IP address IP address that you want to block from connecting to and/or through the router.
- 4. Press **OK** to add the rule.
- 5. After adding all the rules that you needed, press **Apply** to save the rules to the configuration.



#### Demilitarization zone

In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a private network and the outside public network.

Port forwarding	MAC filtering	IP filtering	DMZ
	Demilitariza	tion zone	
Enat	le 🗹		
Destination	IP 192.168.	0.8	

DMZ page

To set up DMZ, click the **Enable**checkbox and put in IP address of your destination in the **Destination IP** text field.

#### **Administration**

Administration page allows you to change the language of the WebUI, disable radio connection, reboot the router, save firmware to your computer (in a binary file format) or update it with the newer version. In addition, you can set up a new password for WebUI connection.

#### Settings

Settings	Firmware		Password			
Longua		5				
Langua	ige (	E	ngiisn		-	
Radio s	Radio state:		Disable r	adio		
Click to	reboot: (		Reboo	ot		

#### Settings page

Language – select a language from the drop down list.

Radio state – disables or enables radio (WiMAX) connection.

**Reboot button** – click to reboot this device. You will have to wait for a few seconds until it boots up again.

#### **Firmware**

Settings	Firmware	Password
Sav	e firmware to	file
Sel	ect firmware	file
U	oload firmwa	re

#### Firmware page

**To save firmware:** click **Save firmware to file** and at the following dialog browse to the directory you want to place binary file.

To update firmware:click Select firmware file and at the following dialog window select firmware file (note: file <u>must</u> be named firmware.bin). To start updating click: Update firmware. This process usually takes 5 to 10 minutes.

**Note:**A firmware backup is only suitable for the device from which it was downloaded. If a firmware backup is uploaded to another router, that device will malfunction.

#### Password

Password	Firmware	Settings		
Upprin				
User in				
sword 🗹	Enable user password			
sword	Password			
sword	Repeat pas			
fo	Password User info sword sword sword	Firmware Password User info ble user password Password Repeat password		

To set up or change a password check **Enable user password** and write a new one into two fields bellow. To disable user password simply uncheck **Enable user password** checkbox. You must click **Apply** if you want to save any of these to configuration.

**Note:** it is strongly not recommended to disable user password if a router is reachable from Local area network

#### About

Status	Firewall	Ethernet	Administration	About	Connected
Firm	ware versio	on 4.6.3.	0-40086		
Micro	ocode vers	ion 6.7.87	39		
Drive	er version	2.0.11	.141		
Daen	non versior	<b>1</b> 4.6.3.	0-40086		
OS v	ersion	Linux	(none) 2.6.25-uc0	-sqn #36	Mon Dec 5 13:57:37 EET 2011 armv5teb 64k
Serv	er version	4.6.3.	D-40086		
UI ve	rsion	2.0be	ta (2011/12/05-12	31)	

About page

The About page displays the versions of your firmware and software that are currently running on your device. This helps you decide whether or not you need to update your firmware.

**Note:** The last part in the OS version string refers to the sector size (64 kilobytes in this case) of the flash memory. It is important that the firmware you update is made for the same flash sector size as the flash memory in the device.

# Troubleshooter:

Q: I think my router is not working: can not acquire connection and WebUI is not reachable. A1: Check if green LED indicating that device is powered is lit on the bottom left corner of the Outdoor Router (just above RJ45 socket). If not, check if PoE adapter is plugged into AC socket and that it is connected by Ethernet cable to the device.

A2: Check if IP address is set to be obtained automatically via DHCP. Follow these steps:

#### **Under Windows 7**

- Go to Control panel ->Network and internet -> Network sharing center -> change adapter settings.
- Right click on a Local Area Connection which uses WiMAX Outdoor Router for connecting to the internet and click **Properties**.



• Check Internet Protocol IPv4 (TCP/IP) and click Properties.

Realtek PCIe GBE Family Controller #3           Configure	You can get IP settings assigned au this capability. Otherwise, you need for the appropriate IP settings.	tomatically if your network supports I to ask your network administrator
nis connection uses the following items:	Obtain an IP address automatic	ically
Client for Microsoft Networks	- Use the following IP address:	
ECOMODO Internet Security Firewall Driver     EQOS Packet Scheduler	IP address:	
File and Printer Sharing for Microsoft Networks	Subnet mask:	
Internet Protocol Version 6 (TCP/IPv6)     Internet Protocol Version 4 (TCP/IPv4)	Default gateway:	
Link-Layer Topology Discovery Mapper I/O Driver     Link-Layer Topology Discovery Responder	<ul> <li>Obtain DNS server address au</li> </ul>	tomatically
	Ouse the following DNS server a	addresses:
Install Uninstall Properties	Preferred DNS server:	
Transmission Control Protocol/Internet Protocol. The default	Alternate DNS server:	
across diverse interconnected networks.	Validate settings upon exit	Advanced

- Make sure that Obtain IP address automatically is checked in the General settings.
- Click OK

.....



#### **Under MAC OS**

Click on the Apple Menu and select System Preferences



- In the Internet & Network section, click on the Network icon.
- Select Built-in Ethernet.

Show All		0	, netw	- 0
Locatio	n: Automatic	:		
Built-in Ethernet     Connected     AirPort     Off	Status:	Connected Built-in Ethernet is currently a the IP address 192.168.0.21.	ictive and has	
Internal Modern C	Configure: IP Address: Subnet Mask: Router: DNS Server: Search Domains:	Using DHCP 192.168.0.21 255.255.255.0 192.168.0.1 192.168.0.1	\$	
+ - 0-		C	dvanced)	1

- Click on Advanced.
- In the TCP/IP tab, ensure that Configure is set to Using DHCP.
- Select the DNS tab. Ensure that DNS servers and Search Domains are empty.
- Click OK.



#### Under Linux (GNOME 3)

- Click on network interfaces icon in activity bar
- Select Network Settings



- Click Configure... to open network connection properties.
- Go to IPv4 tab.

	Editing V	Vired connecti	on 1	•	
Connection name:	Vired connection 1				
Connect automatically					
Wired 802.1x Security		IPv4 Settings IPv6 Settings			
Method: Automatic (DHCP)					
Addresses					
Address	Netmask	Gatewa	ау	Add	
				Delete	
DNS servers:				,	
Search domains:					
DHCP client ID:					
Require IPv4 addressing for this connection to complete					
				Routes	
💜 Available to all us	ers		Cancel	Save	

- Select Automatic (DHCP) from Method drop down menu.
- Click Save...

# **Technical Specifications:**

00010 00000

Standard Compliant	IEEE 802.16e-2005	
Air Interface	S-OFDMA	
Frequency Band	2.3 – 2.4 GHz (RUT723), 2.5 – 2.7 GHz (RUT725),	
	3.3 – 3.6 GHz (RUT735) or 3.3 – 3.8 GHz (RUT738)	
Channel Bandwidth	3 MHz, 3.5 MHz, 5 MHz, 6 MHz, 7 MHz, 8.75 MHz and 10 MHz	
Modulation Adaptive	QPSK, 16QAM, 64QAM	
MIMO	MRC, Matrix A + MRC, Matrix B	
Beamforming	All I/O Beamforming Items	
RF Output Power	2 x 23 dBm @ 3.3 – 3.8 GHz (RUT735, RUT738) or	
	2 x 25 dBm @ 2.3 – 2.7GHz (RUT723, RUT725)	
RX Sensitivity	QPSK1/2: -99 @ 3.5 GHz and 10 MHz BW	
	16QAM1/2: -93.8 @ 3.5 GHz and 10 MHz BW (RUT735)	
	QPSK1/2: -99.5 @ 2.5 GHz and 10 MHz BW	
	16QAM1/2: -94.29 @ 2.5 GHz and 10 MHz BW (RUT725)	
Antenna Gain	14 dBi dual-pol MIMO	
Antenna Type	Panel antenna with pole mounting kit	
Handover	Hard / Optimized Handover	
QoS Mechanism	UGS, Real-Time-VR, Non Real-Time-VR, Best Effort, ERT-VR	
Authentication	EAP-TLS, EAP-TTLS-MSCHAPv2	
Encryption	3 CCM-Mode 128-bit AES	
Throughput	HARQ UL and DL, up to Category 7	
	40 Mbps Total DL + UL	
LEDs	Power, LAN and WiMAX Activity	
LAN	1 x RJ45 10/100 Base-T Ethernet	
POE	IEEE 802.3af-2003 Compliant	

#### **Electrical, Mechanical & Environmental:**

Dimensions (H x W x D)	290mm x 240mm x 45mm
Mounting Pole Diameter	30 – 50 mm
Weight	1.3 kg
Power Supply	36 – 57VDC
Power Consumption	< 6W
Operating Temperature -	- 20º to 50º C
Storage Temperature -	- 20º to 70º C
IP Rating	IP65
Storage Humidity	5% to 95% Non-condensing