

Item no.: 395768

RUT240 - INDUSTRIAL CELLULAR ROUTER

from **148,29 EUR**

Item no.: 395768
shipping weight: 0.20 kg
Manufacturer: Teltonika



 Product Description

RUT240I INDUSTRIAL CELLULAR ROUTER CONNECTIVITY- 4G LTE (Cat 4), 3G, 2G/WI-FI- Wireless Access Point with Hotspot functionality WAN FAILOVER- Automatic switching to available Backup connection RMS- For remote management, access & VPN services FEATURES MOBILE module- 4G LTE Cat 4 up to 150 DL/50 UL Mbps; 3G up to 21 DL/5.76 UL Mbps; 2G up to 236.8 DL/236.8 UL kbps 3GPP Release- Release 10/11 depending on the hardware version Status- IMSI, ICCID, operator, operator state, data connection state, network type, bandwidth, connected band, signal strength (RSSI), SINR, RSRP, RSRQ, EC/IO, RSCP, data sent/received, LAC, TAC, cell ID, ARFCN, UARFCN, EARFCN, MCC, and MNCSMS- SMS status, SMS configuration, send/read SMS via HTTP POST/GET, EMAIL to SMS, SMS to EMAIL, SMS to HTTP, SMS to SMS, scheduled SMS, SMS autoreply, SMPP USSD- Supports sending and reading Unstructured Supplementary Service Data messages Black/White list- Operator black/white list (by country or separate operators) Multiple PDN- Possibility to use different PDNs for multiple network access and services Band management- Band lock, Used band status display APN- Auto APN Bridge- Direct connection (bridge) between mobile ISP and device on LAN Pass through- Router assigns its mobile WAN IP address to another device on LAN WIRELESS Wireless mode- 802.11b/g/n (Wi-Fi 4), Access Point (AP), Station (STA) Wi-Fi security- WPA2-Enterprise - PEAP, WPA2-PSK, WPA-EAP, WPA-PSK, WPA3-SAE, WPA3-EAP, OWE; AES-CCMP, TKIP, Auto-cipher modes, client separation, EAP-TLS with PKCS#12 certificates, disable auto-reconnect SSID/ESSID- SSID stealth mode and access control based on MAC address Wi-Fi users- Up to 50 simultaneous connections Wireless Connectivity Features- Wireless mesh (802.11s), fast roaming (802.11r), Relay, BSS transition management (802.11v), radio resource measurement (802.11k) Wireless MAC filter- Whitelist, blacklist NETWORK Hotspot- Captive portal (hotspot), internal/external Radius server, Radius MAC authentication, SMS authorisation, SSO authentication, internal/external landing page, walled garden, user scripts, URL parameters, user groups, individual user or group limitations, user management, 9 default customisable themes and optionality to upload and download customised hotspot themes Routing- Static routing, Dynamic routing (BGP, OSPF v2, RIP v1/v2, EIGRP, NHRP), Policy based routing Network protocols- TCP, UDP, IPv4, IPv6, ICMP, NTP, DNS, HTTP, HTTPS, SFTP, FTP, SMTP, SSL/TLS, ARP, VRRP, PPP, PPPoE, UPNP, SSH, DHCP, Telnet, SMPP, SNMP, MQTT, Wake On Lan (WOL) VoIP pass through support- H.323 and SIP- alg protocol NAT helpers, allowing proper routing of VoIP packets Connection monitoring- Ping Reboot, Wget Reboot, Periodic Reboot, LCP and ICMP for link inspection Firewall- Port forward, traffic rules, custom rules DHCP- Static and dynamic IP allocation, DHCP relay, DHCP server configuration, status, static leases: MAC with wildcards QoS / Smart Queue Management (SQM)- Traffic priority queuing by source/destination, service, protocol or port, WMM, 802.11e DNS- Supported >25 service providers, others can be configured manually Network backup- Wi-Fi WAN, Mobile, VRRP, Wired options, each of which can be used as an automatic Failover Load balancing- Balance Internet traffic over multiple WAN connections SSHFS- Possibility to mount remote file system via SSH protocol ETHERNET WAN- 1 x WAN port 10/100 Mbps, compliance IEEE 802.3, IEEE 802.3u, IEEE 802.3z standards, supports auto MDI/MDIX LAN- 1 x LAN port, 10/100 Mbps, compliance with IEEE 802.3, IEEE 802.3u standards, supports auto MDI/MDIX SECURITY Authentication- Pre-shared key, digital certificates, X.509 certificates, TACACS+, Internal & External RADIUS users authentication, IP & login attempts block, time-based login blocking, built-in random password generator Firewall- Pre-configured firewall rules can be enabled via WebUI, unlimited firewall configuration via CLI; DMZ; NAT; NAT-T Attack prevention- DDOS prevention (SYN flood protection, SSH attack prevention, HTTP/HTTPS attack prevention), port scan prevention (SYN-FIN, SYN-RST, X-mas, NULL flags, FIN scan attacks) VLAN- Port and tag-based VLAN separation Mobile quota control- Mobile data limit, customizable period, start time, warning limit, phone number WEB filter- Blacklist for blocking out unwanted websites, Whitelist for specifying allowed sites only Access control- Flexible access control of SSH, Web interface, CLI and Telnet VPN OpenVPN- Multiple clients and a server can run simultaneously, 27 encryption methods OpenVPN Encryption- DES-CBC 64, RC2-CBC 128, DES-EDE-CBC 128, DES-EDE3-CBC 192, DESX-CBC 192, BF-CBC 128, RC2-40-CBC 40, CAST5-CBC 128, RC2-64-CBC 64, AES-128-CBC 128, AES-128-CFB 128, AES-128-CFB1 128, AES-128-CFB8 128, AES-128-CFB16 128, AES-128-CFB8 128, AES-128-CFB16 128, AES-192-CFB 192, AES-192-CFB1 192, AES-192-CFB8 192, AES-192-CFB16 192, AES-192-CBC 192, AES-192-GCM 192, AES-256-GCM 256, AES-256-CBC 256, AES-256-CFB 256, AES-256-CFB1 256, AES-256-CFB8 256, AES-256-CFB16 256, AES-256-CBC 256, AES-256-CBC 256, AES-256-CBC 256, AES-256-GCM 128, AES-192-GCM 128, AES-256-GCM 128, AES-192-GCM 16, AES-256-GCM 16, AES-256-GCM 16, AES-256-GCM 16) GRE tunnel, GRE tunnel over IPsec support PPTP, L2TP- Client/Server instances can run simultaneously, L2TPv3, L2TP over IPsec support Stunnel- Proxy designed to add TLS encryption functionality to existing clients and servers without any changes in the program's code DMVPN- Method of building scalable IPsec VPNs SSTP- SSTP client instance support ZeroTier- ZeroTier VPN client support WireGuard- WireGuard VPN client and server support Tinc- Tinc offers encryption, authentication and compression in it's tunnels. Client and server support. MODBUS TCP SLAVE ID range- Respond to one ID in range [1;255] or any Allow Remote Access- Allow access through WAN Custom registers- MODBUS TCP custom register block requests, which read/write to a file inside the router, and can be used to extend MODBUS TCP Slave functionality MODBUS TCP MASTER Supported functions- 01, 02, 03, 04, 05, 06, 15, 16 Supported data formats- 8-bit: INT, UINT; 16-bit: INT, UINT (MSB or LSB first); 32-bit: float, INT, UINT (ABCD (big-endian), DCBA (little-endian), CDAB, BADC) DATA TO SERVER Protocol- HTTP(S), MQTT, Azure MQTT, Kinesis MQTT GATEWAY Modbus MQTT Gateway- Allows sending commands and receiving data from MODBUS Server through MQTT broker DNP3 Supported modes- TCP Master, DNP3 Outstation API Teltonika Networks Web API (beta) support- Expand your device's possibilities by using a set of configurable API endpoints to retrieve or change data. MONITORING & MANAGEMENT WEB UI- HTTP/HTTPS, status, configuration, FW update, CLI, troubleshoot, multiple event log servers, firmware update availability notifications, event log, system log, kernel log, Internet status FOTA- Firmware update from server, automatic notification SSH- SSH (v1, v2) SMS- SMS status, SMS configuration, send/read SMS via HTTP POST/GET Call- Reboot, Status, Mobile data on/off, Output on/off, answer/hang-up with a timer, Wi-Fi on/off FTTR-069- OpenACS, EasyCwmp, ACS Lite, tGem, LibreACS, GenieACS, FreeACS, LibCWMP, Friendly tech, AVSystem MQTT- MQTT Broker, MQTT publisher SNMP- SNMP (v1, v2, v3), SNMP Trap, Brute force protection JSON-RPC- Management API over HTTP/HTTPS RMS- Teltonika Remote Management System (RMS) IOT PLATFORMS Cloud of Things- Allows monitoring of: Device data, Mobile data, Network info, Availability ThingWorx- Allows monitoring of: WAN Type, WAN IP, Mobile Operator Name, Mobile Signal Strength, Mobile Network Type Cumulocity- Allows monitoring of: Device Model, Revision and Serial Number, WAN Type and IP, Mobile Cell ID, ICCID, IMEI, Connection Type, Operator, Signal Strength Azure IoT Hub- Can be configured with Data to Server to send all the available parameters to the cloud. Has Direct method support which allows to execute RutOS API calls on the IoT Hub. Also has Plug and Play integration with Device Provisioning Service that allows zero-touch device provisioning to IoT Hubs SYSTEM CHARACTERISTICS CPU- Atheros Hornet, MIPS 24Kc, 400 MHz RAM- 64 MB, DDR2 FLASH storage- 16 MB, SPI Flash FIRMWARE / CONFIGURATION WEB UI- Update FW from file, check FW on server, configuration profiles, configuration backup FOTA- Update FWRMS- Update FW/configuration for multiple devices at once Keep settings- Update FW without losing current configuration Factory settings reset- A full factory reset restores all system settings, including the IP address, PIN, and user data to the default manufacturer's configuration FIRMWARE CUSTOMISATION Operating system- RutOS (OpenWrt based Linux OS) Supported languages- Busybox shell, Lua, C, C++ Development tools- SDK package with build environment provided INPUT / OUTPUT Input- 1 x Digital Input, 0 - 6 V detected as logic low, 8 - 30 V detected as logic high Output- 1 x Digital Output, Open collector output, max output 30 V, 300 mA Events- Email, RMS, SMS/I/O juggler- Allows to set certain I/O conditions to initiate event POWER Connector- 4-pin industrial DC power socket Input voltage range- 9 - 30 VDC, reverse polarity protection; surge protection >31 VDC 10us max PoE (passive)- Passive PoE over spare pairs. Possibility to power up through LAN1 port, not compatible with IEEE802.3af, 802.3at and 802.3bt standards, Mode B, 9 - 30 VDC Power consumption- < 6.5 W Max PHYSICAL INTERFACES Ethernet- 2 x RJ45 ports, 10/100 Mbps/O's- 1 x Digital Input, 1 x Digital Output on 4-pin power connector Status LEDs- 3 x Connection type status LEDs, 5 x Connection strength LEDs, 2 x LAN status LEDs, 1 x Power LED SIM- 1 x SIM slot (Mini SIM - 2FF), 1.8 V/3 V, external SIM holder Power- 1 x 4-pin power connector Antennas - 2 x SMA for LTE, 1 x RP-SMA for Wi-Fi antenna connectors Reset- Reboot/User default reset/Factory reset button PHYSICAL SPECIFICATION Casing material- Aluminium housing, plastic panels Dimensions (W x H x D)- 83 x 25 x 74 mm Weight- 125 g Mounting options- DIN rail, wall mount, flat surface (all require additional kit) OPERATING ENVIRONMENT Operating temperature- -40 °C to 75 °C Operating humidity- 10% to 90% non-condensing Ingress Protection Rating- IP30 Operating humidity- 10% to 90% non-condensing REGULATORY & TYPE APPROVALS Regulatory- CE/RED, FCC, IC/ISED, EAC, RCM, PTCRB, RoHS, WEEE, Wi-Fi Certified, Anatel, GCF, REACH, Thailand NBTC, Ukraine UCRF, SDPPI (POSTEL) Operator- AT&T, Verizon EMC EMISSIONS & IMMUNITY IMMUNITY Standards- Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, Draft EN 301 489-52 V1.1.0- FCC 47 CFR Part 15B (2017), ANSI C63.4 (2014) ESD- EN 61000-4-2:2009 Radiated Immunity- EN 61000-4-3:2006 + A1:2008 + A2:2010 EFT- EN 61000-4-4:2012 Surge immunity (AC Power Line)- EN 61000-4-5:2006 Surge immunity (Ethernet ports)- EN 61000-4-5:2014, clause 7.1 of ITU-T K21CS- EN 61000-4-6:2009 DIP- EN 61000-4-11:2004 RF Standards- EN 300 328 V2.1.1, EN 301 511 V12.5.1, EN 301 908-1 V11.1.1, EN 301 908-2 V11.1.1, EN 301 908-13 V11.1.1- FCC 47 CFR Part 15C (2017), FCC 47 CFR Part 2 (2017), FCC 47 CFR Part 22H (2017), FCC 47 CFR Part 24E (2017), FCC 47 CFR Part 27C (2017)- RSS-Gen Issue 4 (2014), RSS-247 Issue 2 (2017), RSS-132 Issue 3 (2013), RSS-133 Issue 6 (2013), RSS-139 Issue 3, RSS-130 Issue 1- AS/CA S042.1:2018, AS/ACIF S042.3:2005, AS/CA S042.4:2018, AS/NZS 4268:2017 SAFETY Standards- IEC 60950-1:2005 (Second Edition) + Am 1:2009 + Am 2:2013- AS/NZS 60950.1:2015- EN 50665:2017, EN 62311:2008- FCC 47 CFR Part 1.1310- RSS-102 Issue 5 (2015)

Specifications

Scan this QR code to
view the product
All details, up-to-date
prices and availability

