



Routeur industriel 4×Ethernet Gigabit, PoE passif, WiFi 5, Modbus, MQTT, DLMS, DNP3 | RUTM10

Référence GC-RUTM10000000

- 4× ports Gigabit Ethernet + PoE passif
- Wi-Fi 5 double bande MU-MIMO (802.11b/g/n/ac)
- 1× port USB 2.0
- Modbus TCP, DNP3, DLMS/COSEM, OPC UA
- Modbus-to-MQTT Gateway
- Capacités VPN étendues
- Dimensions : 115 × 32.2 × 95.2 mm
- Poids : 359 g

Destiné aux **applications IoT/M2M**, le **RUTM10** est un **routeur Wi-Fi 5** doté de **4 ports RJ45 Gigabit** avec VPN avancés et multiples protocoles industriels.

Il fournit des fonctions avancées de **segmentation réseau**, de **supervision et d'intégration Cloud** et assure le routage des flux entre interfaces Ethernet et Wi-Fi avec **gestion étendue du trafic** via QoS et Smart Queue Management.

Les **mécanismes de failover** permettent la **bascule automatique entre connexions WAN** et son architecture permet d'interconnecter équipements informatiques, automates, systèmes de mesure et plateformes IoT au sein d'une infrastructure unifiée.



Wi-Fi 5 jusqu'à 867 Mbps, double bande avec MU-MIMO.



Capacités sans fil jusqu'à 150 connexions simultanées



4x Ports Ethernet 10/100/1000 Mbps



PoE passif via port LAN



Boîtier en aluminium robuste



Système de gestion à distance



CONNECTIVITÉ

La connectivité repose sur un Wi-Fi 5 double bande (802.11b/g/n/ac Wave 2) atteignant jusqu'à 867 Mbps avec MU-MIMO, compatible modes point d'accès et station.

Les fonctions avancées incluent le **roaming rapide 802.11r**, la **gestion des ressources radio 802.11k** pour garantir la continuité de service dans des environnements multi-AP, tandis que le support du **mesh Wi-Fi (802.11s)** et d'un hotspot avec portail captif intégré, permet de déployer des réseaux distribués.

Il peut gérer jusqu'à **150 connexions Wi-Fi simultanées** et assure un haut niveau de sécurité grâce aux protocoles **WPA2-Enterprise, WPA3, EAP-TLS, OWE**, à l'isolation des clients, à la **protection des trames de gestion 802.11w** et au chiffrement **AES-CCMP**.

INTERFACES

Équipé de quatre ports Ethernet Gigabit, incluant un port WAN et trois ports LAN, compatibles avec les standards IEEE 802.3, 802.3u et 802.3az, il assure les fonctions d'auto-négociation et d'auto MDI/MDIX pour un déploiement réseau simple et rapide.

Une entrée et une sortie numériques intégrées permettent la surveillance d'événements externes et l'automatisation d'actions, répondant aux besoins des environnements industriels et professionnels.

Un port USB 2.0 permet la connexion de périphériques externes tels que stockage, imprimante ou adaptateur série.

L'ensemble est complété par 2 connecteurs RP-SMA pour les antennes Wi-Fi et un connecteur d'alimentation industriel.

PROTOCOLES

Le RUTM10 prend en charge le **routage statique** ainsi que de nombreux protocoles de **routage dynamique** tels que **BGP, OSPF v2, RIP v1/v2, EIGRP** et **NHRP**.

Conçu pour les usages Industrie 4.0 et IoT, il supporte nativement les **protocoles industriels Modbus TCP, OPC UA, DNP3 et DLMS/COSEM**.

GESTION, SUPERVISION ET INTÉGRATION IOT

Le système RutOS fournit une interface Web complète avec supervision, configuration, mises à jour firmware et journaux système.

L'intégration IoT est étendue avec **MQTT broker/publisher**, et une **compatibilité Azure IoT Hub** et **Cumulocity**.

Les fonctions Data to Server permettent d'agréger des données multi-protocoles, enrichies par scripting Lua.

CONTRÔLE À DISTANCE

La **gestion distante** du RUTM10 est assurée via **RMS (Teltonika Remote Management System), SNMP, TR-069** et **API JSON-RPC**.

Les fonctions de **gestion et de supervision à distance** sont assurées par une interface Web complète, l'accès **SSH**, la prise en charge de **SNMP v1, v2 et v3**, les notifications par e-mail, les mises à jour **FOTA**.



SÉCURITÉ

Le RUTM10 intègre des fonctions de sécurité avancées incluant un **pare-feu configurable**, la **gestion des VLAN**, le NAT, le filtrage web et la **protection contre les attaques réseau** telles que les DDoS, scans de ports et tentatives d'intrusion.

Il prend en charge des **mécanismes d'authentification** robustes avec certificats, RADIUS et TACACS+, ainsi qu'un large choix de technologies VPN comme OpenVPN, IPsec, WireGuard et Tailscale, tout en offrant des fonctions de **redondance réseau**, de basculement WAN, d'équilibrage de charge et de QoS pour garantir des communications sécurisées, stables et performantes.

ALIMENTATION

L'alimentation du routeur accepte une **large plage de tension continue de 9 à 50 VDC**, avec protections intégrées contre les inversions de polarité et les surtensions, et prend également en charge l'alimentation passive PoE via le port LAN1, tout en maintenant une **consommation maximale inférieure à 8,65 W**.

INSTALLATION

Son boîtier en aluminium anodisé est conçu pour les environnements industriels avec montage possible sur rail DIN, mur ou surface plane.

Ses dimensions compactes (115 × 32,2 × 95,2 mm) et son faible poids (359g) facilitent l'intégration dans des armoires techniques.

L'équipement fonctionne dans une plage de température étendue de -40 °C à +75 °C avec indice de protection IP30

Il est conçu pour fonctionner dans des conditions environnementales extrêmes, avec une **plage de température de -40 °C à +75 °C**, un **taux d'humidité jusqu'à 90 % sans condensation** et un indice de protection IP30.

CERTIFICATIONS

Le routeur est conforme aux principales normes et certifications internationales.

Il dispose des certifications CE, UKCA, RCM et CB, ainsi que de l'homologation UN ECE R10 (E-mark) pour les applications de transport, et respecte les exigences en matière de compatibilité électromagnétique, de sécurité électrique et de normes radio pour une conformité totale aux réglementations européennes et internationales.

EXEMPLES DE CAS D'USAGE

Dans une usine, un entrepôt ou un site industriel isolé, le RUTM10 est utilisé pour **connecter automates, équipements réseau et terminaux Wi-Fi** tout en séparant les flux grâce aux VLAN et en sécurisant les accès à distance par VPN.

Il joue également le rôle de routeur central ou de passerelle IoT, assurant la **collecte de données industrielles**, la **communication avec des centres de supervision** ou des plateformes cloud, et la gestion à distance de plusieurs sites via RMS.

Télégestion des réseaux d'eau



Automatisation des entrepôts



Smart Industry





SPÉCIFICATIONS

SANS FIL

MODE(S) SANS FIL	802.11b/g/n/ac Wave 2 (Wi-Fi 5) avec des débits de transmission de données allant jusqu'à 867 Mbps (Double bande, MU-MIMO), transition rapide 802.11r, point d'accès (AP), station (STA)
SÉCURITÉ WI-FI	WPA2-Enterprise : PEAP, WPA2-PSK, WPA-EAP, WPA-PSK, WPA3-SAE, WPA3-EAP, OWE ; AES-CCMP, TKIP, MODES DE CHIFFREMENT AUTOMATIQUE, SÉPARATION CLIENT, EAP-TLS AVEC CERTIFICATS PKCS#12, DÉSACTIVATION DE LA RECONNEXION AUTOMATIQUE, TRAMES DE GESTION PROTÉGÉES 802.11w (PMF)
SSID/ESSID	Mode(s) furtif SSID et contrôle d'accès basé sur l'adresse MAC
UTILISATEURS WI-FI	Jusqu'à 150 connexions simultanées
FONCTIONNALITÉS DE CONNECTIVITÉ SANS FIL	Maillage sans fil (802.11s), itinérance rapide (802.11r), gestion de la transition BSS (802.11v), mesure des ressources radio (802.11k)
FILTRE MAC SANS FIL	Liste des autorisants, liste de blocage
GÉNÉRATEUR DE CODES QR SANS FIL	Une fois scanné, un utilisateur accédera automatiquement à votre réseau sans avoir besoin de saisir ses informations de connexion
TRAVELMATE	Transférer la page d'atterrissage du point d'accès Wi-Fi vers un appareil connecté ultérieur

ETHERNET

WAN	1 × port WAN 10/100/1000 Mbps, conforme aux normes IEEE 802.3, IEEE 802.3u, 802.3az, prend en charge le crossover automatique MDI/MDIX
LAN	3 × ports LAN, 10/100/1000 Mbps, conformité aux normes IEEE 802.3, IEEE 802.3u, 802.3az, prise en charge du crossover automatique MDI/MDIX

RÉSEAU

ROUTAGE	Routage statique, routage dynamique (BGP, OSPF v2, RIP v1/v2, EIGRP, NHRP), routage basé sur des politiques
PROTOCOLE(S) RÉSEAU	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), VXLAN
PRISE EN CHARGE DU PASSTHROUGH VOIP	H.323 et les protocoles SIP-alg NAT helpers, permettant un routage correct des paquets VoIP
SURVEILLANCE DES CONNEXIONS	Redémarrage Ping, Redémarrage Wget, Redémarrage périodique, LCP et ICMP pour l'inspection des liens
PARE-FEU	Redirection de port, règles de circulation, règles personnalisées, personnalisation de la cible TTL
PAGE D'ÉTAT DU PARE-FEU	Consultez toutes vos statistiques de pare-feu, règles et compteurs de règles
GESTION PORTUAIRE	Visualiser les ports de périphériques, activer et désactiver chacun d'eux, activer ou désactiver la configuration automatique, modifier leur vitesse de transmission, etc.
TOPOLOGIE DU RÉSEAU	Représentation visuelle de votre réseau, montrant quels appareils sont connectés à quels autres appareils



DHCP	Allocation IP statique et dynamique, relais DHCP, configuration du serveur DHCP, statut, baux statiques : MAC avec jokers
(QOS / SQM)	Mise en file d'attente de priorité au trafic par source/destination, service, protocole ou port, WMM, 802.11e
DDNS	Pris en charge par les fournisseurs de services >77, d'autres peuvent être configurés manuellement
DNS SUR HTTPS	Le DNS sur proxy HTTPS permet une résolution DNS sécurisée en routant les requêtes DNS via HTTPS
SAUVEGARDE RÉSEAU	Wi-Fi WAN, VRRP, options filaires, chacune pouvant être utilisée comme basculement automatique
RÉPARTITION DE CHARGE	Équilibrer le trafic Internet sur plusieurs connexions WAN
HOTSPOT	Portail captif (point d'accès), serveur Radius interne/externe, authentification MAC Radius, autorisation SMS, authentification SSO, page d'atterrissage interne/externe, jardin fermé, scripts utilisateurs, paramètres URL, groupes d'utilisateurs, limitations individuelles ou de groupes, gestion des utilisateurs, 9 thèmes personnalisables par défaut et possibilité de télécharger des thèmes de points d'accès personnalisés
SSHFS	Possibilité de monter un système de fichiers distant via le protocole SSH
PRISE EN CHARGE DU VRF	Prise en charge initiale du routage et du transfert virtuels (VRF)
GESTION DU TRAFIC	Surveillance en temps réel, cartes de feux sans fil, historique de la consommation du trafic

SÉCURITÉ

802.1X	Client de contrôle d'accès réseau basé sur des ports
AUTHENTIFICATION	Clé pré-partagée, certificats numériques, certificats X.509, TACACS+, authentification des utilisateurs RADIUS internes et externes, blocage des tentatives IP et de connexion, blocage de la connexion basée sur le temps, générateur de mots de passe aléatoires intégré
PARE-FEU	Les règles de pare-feu préconfigurées peuvent être activées via WebUI, une configuration illimitée via CLI, DMZ, NAT, NAT-T, NAT64
PRÉVENTION DES ATTAQUES	Prévention DDOS (protection contre les inondations SYN, prévention des attaques SSH, prévention des attaques HTTP/HTTPS), prévention du balayage des ports (SYN-FIN, SYN-RST, X-MAS, flags NULL, attaques par balayage FIN)
VLAN	Séparation VLAN basée sur les ports et les balises
FILTRE WEB	Liste de blocage pour bloquer les sites indésirables, liste de permis uniquement pour spécifier les sites autorisés
CONTRÔLE D'ACCÈS	Contrôle d'accès flexible du SSH, de l'interface Web, de la CLI et du Telnet
GESTIONNAIRE DE CERTIFICATS	L'outil de création de certificats permet de créer des certificats CA, serveur, client, let's encrypt, certificats SCEP
VPN	
OPENVPN	Plusieurs clients et un serveur peuvent fonctionner simultanément, 27 méthodes de chiffrement



CHIFFREMENT OPENVPN	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-OFB 128, AES-128-GCM 128, AES-192-CFB 192, AES-192-CFB1 192, AES-192-CFB8 192, AES-192-OFB 192, AES-192-CBC 192, AES-192-GCM 192, AES-256-GCM 256, AES-256-CFB 256, AES-256-CFB1 256, AES-256-CFB8 256, AES-256-OFB 256, AES-256-CBC 256
IPSEC	XFRM, IKEv1, IKEv2, avec 14 méthodes de chiffrement pour IPsec (3DES, DES, AES128, AES192, AES256, AES128GCM8, AES192GCM8, AES256GCM8, AES128GCM12, AES192GCM12, AES256GCM12, AES128GCM16, AES192GCM16, AES256GCM16)
GRE	Tunnel GRE, prise en charge du tunnel GRE sur IPsec
PPTP, L2TP	Les instances client/serveur peuvent s'exécuter simultanément, prise en charge L2TPv3, L2TP sur IPsec
STUNNEL	Proxy conçu pour ajouter des fonctionnalités de chiffrement TLS aux clients et serveurs existants sans aucune modification du code du programme
DMVPN	Méthode de création de VPN IPsec évolutifs, support des phases 2 et 3 ainsi que du double hub
SSTP	Prise en charge des instances client SSTP
ZEROTIER	Prise en charge du client VPN ZeroTier
WIREGUARD	Prise en charge des clients et serveurs VPN WireGuard
TINC	Tinc propose le chiffrement, l'authentification et la compression dans ses tunnels. Support client et serveur.
TAILSCALE	Tailscale offre vitesse, stabilité et simplicité par rapport aux VPN traditionnels. Connexions point à point chiffrées utilisant le protocole open source WireGuard
OPC UA	
MODES	Client, serveur
TYPES DE CONNEXION	TCP
MODBUS	
MODES	Serveur, client
TYPES DE CONNEXION	TCP, USB
REGISTRES PERSONNALISÉS	Requêtes de blocs de registres personnalisées MODBUS TCP, qui lisent/écrivent dans un fichier à l'intérieur du routeur, et peuvent être utilisées pour étendre la fonctionnalité du client TCP MODBUS
FORMATS DE DONNÉES	8 bits : INT, UINT ; 16 bits : INT, UINT (MSB ou LSB en premier) ; 32 bits : float, INT, UINT (ABCD (big-endian), DCBA (little-endian), CDAB, BADC), HEX, ASCII
DONNÉES VERS SERVEUR	
PROTOCOLE(S)	HTTP(S), MQTT, Azure MQTT



DONNÉES VERS SERVEUR

Extraire des paramètres de plusieurs sources et différents protocoles, et les envoyer tous à un seul serveur ; Scripting LUA personnalisé, permettant aux scripts d'utiliser la fonctionnalité Data to server du routeur

PASSERELLE MQTT

PASSERELLE MODBUS MQTT

Permet d'envoyer des commandes et de recevoir des données depuis le serveur MODBUS via le courtier MQTT

DNP3

MODES

Station, Avant-station

CONNEXION

TCP, USB

DLMS/COSEM

SOUTIEN DLMS

DLMS - protocole standard pour l'échange de données des compteurs de services publics

MODES

Client

TYPES DE CONNEXION

TCP, USB

SURVEILLANCE ET GESTION

INTERFACE WEB

HTTP/HTTPS, statut, configuration, mise à jour du firmware (CLI), dépannage de dépannage, plusieurs journaux d'événements, notifications de disponibilité des mises à jour du firmware, journal d'événements, journal système, journal du noyau, statut Internet

FOTA

Mise à jour du firmware depuis le serveur, notification automatique

SSH

SSH (v1, v2)

EMAIL

Recevez des alertes de statut par e-mail concernant divers services

TR-069

OpenACS, EasyCwmp, ACSLite, tGem, LibreACS, GenieACS, FreeACS, LibCWMP, Friendly tech, AVSystem

MQTT

Courtier MQTT, éditeur MQTT

SNMP

SNMP (v1, v2, v3), Piège SNMP, Protection contre la force brute

JSON-RPC

API de gestion sur HTTP/HTTPS

RMS

Système de gestion à distance Teltonika (RMS)

PLATEFORMES IOT

CUMULOCITÉ

Permet la surveillance de : modèle de dispositif, révision et numéro de série, type WAN et IP. Comporte des actions de redémarrage et de mise à jour du firmware

AZURE IOT HUB

Peut être configuré avec Data to Server pour envoyer tous les paramètres disponibles au cloud. Prend en charge la méthode Direct, ce qui permet d'exécuter des appels API RutOS sur l'IoT Hub. Dispose également d'une intégration Plug and Play avec le service de provisionnement d'appareils qui permet un provisionnement sans contact direct vers les IoT Hubs

CARACTÉRISTIQUES DU SYSTÈME



CPU MediaTek, Dual-Core, 880 MHz, MIPS1004Kc

RAM 256 Mo, DDR3

STOCKAGE FLASH 16 Mo de mémoire NOR série, 256 Mo de mémoire NAND série

FIRMWARE/CONFIGURATION

INTERFACE WEB Mise à jour du firmware à partir du fichier, vérifier le firmware sur le serveur, profils de configuration, sauvegarde de configuration

FOTA Mise à jour FW

RMS Mise à jour du firmware / la configuration pour plusieurs appareils simultanément

CONSERVEZ LES RÉGLAGES Mise à jour du firmware sans perdre la configuration actuelle

RÉINITIALISATION PARAMÈTRES D'USINE Une réinitialisation complète d'usine restaure tous les paramètres système, y compris l'adresse IP, le code PIN et les données utilisateur, dans la configuration par défaut du fabricant

PERSONNALISATION DU FIRMWARE

SYSTÈME D'EXPLOITATION RutOS (système Linux basé sur OpenWrt)

LANGUES Shell Busybox, Lua, C, C++

OUTILS DE DÉVELOPPEMENT Package SDK avec environnement de compilation fourni

PERSONNALISATION GPL Vous pouvez créer votre propre firmware personnalisé et une application de page web en modifiant les couleurs, les logos et d'autres éléments de notre firmware pour répondre à vos besoins ou à ceux de vos clients

GESTIONNAIRE DE PAQUETS Le gestionnaire de paquets est un service utilisé pour installer des logiciels supplémentaires sur l'appareil

USB

DÉBIT DE DONNÉES USB 2.0

APPLICATIONS Partage Samba, USB-vers-série

DISPOSITIFS EXTERNES Possibilité de connecter un disque dur externe, une clé USB, un modem supplémentaire, une imprimante, un adaptateur série USB

FORMATS DE STOCKAGE FAT, FAT32, exFAT, NTFS (lecture seule), ext2, ext3, ext4

ENTRÉE(S)/SORTIE(S)

ENTRÉE(S) 1× Entrée(s) numérique, 0 - 6 V détecté comme faible logique, 8 - 50 V détecté comme haut logique

SORTIE(S) 1× Sortie numérique et sortie à collecteur ouvert, sortie maximale 50 V, 300 mA

ÉVÉNEMENTS Email, RMS

JUGGLER I/O Permet de définir certaines conditions d'E/S pour initier un événement

ALIMENTATION



CONNECTEUR	Prise électrique industrielle DC à 4 broches
PLAGE DE TENSION D'ENTRÉE	9 – 50 VDC, protection contre la polarité inverse, protection contre les surtensions >51 VDC 10us max
POE (PASSIF)	Possibilité d'alimentation via un port LAN1, non compatible avec les normes IEEE802.3af, 802.3at et 802.3bt, mode B, 9 - 50 VDC
CONSUMMATION D'ÉNERGIE	• Ralenti : < 3,51 W • Max : < 8,65 W

INTERFACES PHYSIQUES

ETHERNET	4× ports RJ45, 10/100/1000 Mbps
ENTRÉE(S)	• 1× entrée numérique • 1× sortie numérique sur un connecteur d'alimentation 4 broches
LED(S) D'ÉTAT	• 8× état LAN • 1× LED(s) d'alimentation • 2× LED Wi-Fi 2,4G et 5G
ALIMENTATION	1× connecteur d'alimentation 4 broches
ANTENNES	2× RP-SMA pour Wi-Fi
USB	1× port USB A pour périphériques externes
RÉINITIALISATION	• Redémarrage • Bouton de réinitialisation par défaut utilisateur • Réinitialisation d'usine
AUTRES	1 × vis de mise à la terre

SPÉCIFICATIONS PHYSIQUES

MATÉRIAU	Boîtiers et panneaux en aluminium anodisé
DIMENSIONS	115 × 32,2 × 95,2 mm
POIDS	359 g
OPTIONS DE MONTAGE	• Rail DIN • Support mural • Surface plane (tous nécessitent un kit supplémentaire)

ENVIRONNEMENT OPÉRATIONNEL

T° DE FONCTIONNEMENT	-40 °C à 75 °C
HUMIDITÉ DE FONCTIONNEMENT	10 % à 90 % non condensant
INDICE DE PROTECTION	IP30

RÉGLEMENTATION(S)

RÉGLEMENTATION(S)	CE, UKCA, RCM, CB, UN ECE R10 (E-mark)
-------------------	--

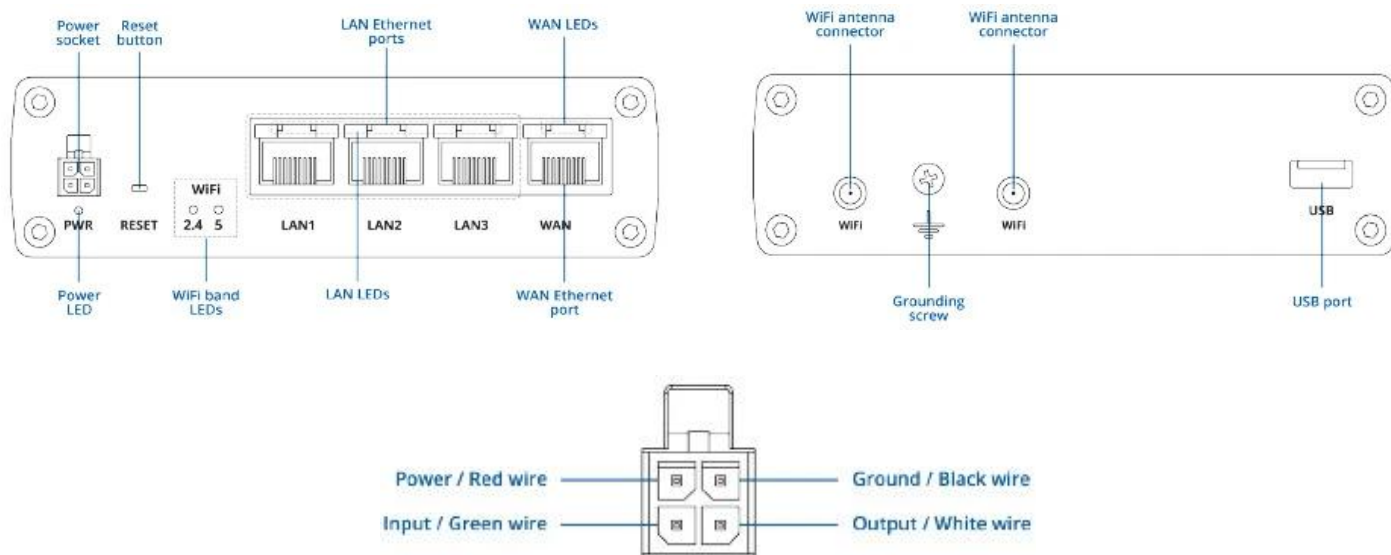
ÉMISSIONS ET IMMUNITÉ EMC

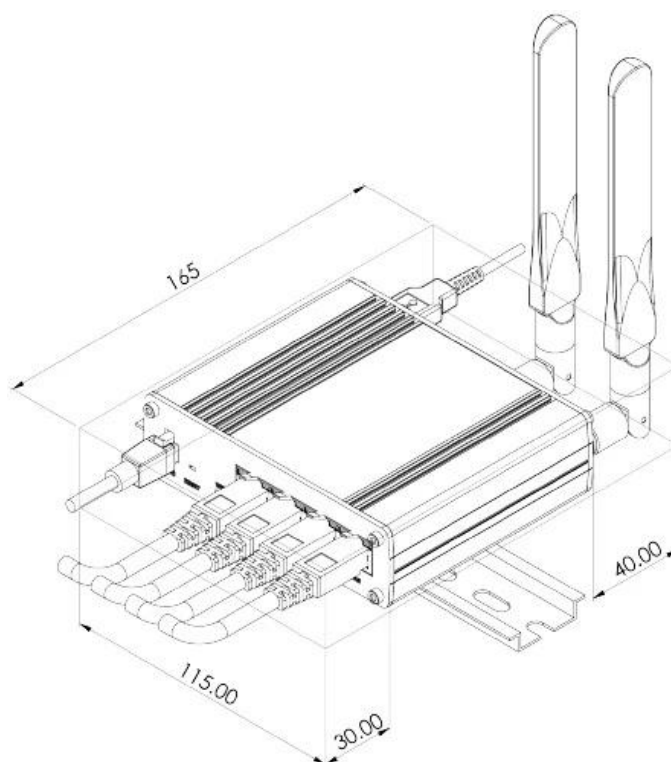
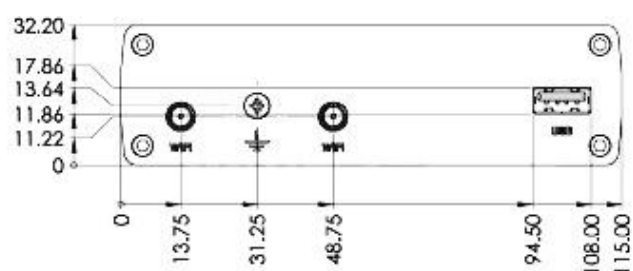
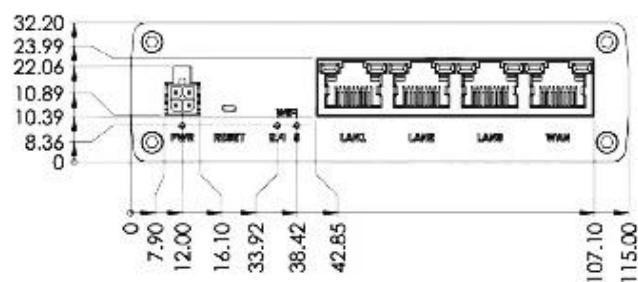
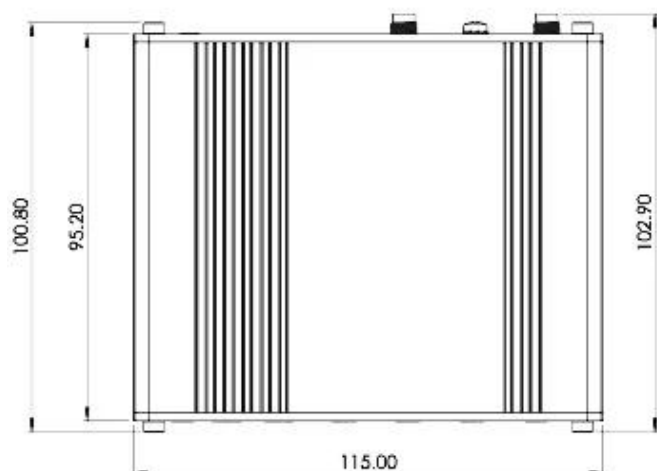


NORMES	EN 55032:2015 + A11:2021 EN 55035:2017 + A11:2020 EN IEC 61000-3-2:2019 + A1:2021 EN 61000-3-3:2013 + A1:2019 + A2:2021 EN 301 489-1 V2.2.3 EN 301 489-3 V2.1.1 EN 301 489-17 V3.2.4 EN 301 489-52 V1.2.1
ESD	EN 61000-4-2:2009
IMMUNITÉ AUX RADIATIONS	EN IEC 61000-4-3:2020
EFT	EN 61000-4-4:2012
IMMUNITÉ AUX SURTENSIONS	EN 61000-4-5:2014 + A1:2017
CS	EN 61000-4-6:2014
DIP	EN IEC 61000-4-11:2020
RF	
NORMES	EN 301 908-1 V15.2.1 EN 301 908-2 V13.1.1 EN 301 908-13 V13.2.1 EN 300 328 V2.2.2 EN 301 893 V2.1.1 EN 300 440 V2.2.1
SÉCURITÉ	
NORMES	CE : EN IEC 62368-1:2020 + A11:2020, EN IEC 62311:2020 RCM : AS/NZS 62368.1:2022 CB : IEC62368-13:2018



SCHÉMA(S)







CONTENU DU PACK



RUTM10



PSU 18W



2× antennes Wi-Fi dual bande SMA mâle



Câble Ethernet (1,5 m)