





- Litevská technologická firma se sídlem ve Vilniusu
- Od roku 1998
- **Výroba v Evropě:** Teltonika si zakládá na tom, že vyvíjí a vyrábí zařízení v Litvě
- **Globální dosah:** Firma působí ve více než 150 zemích
- **Inovace:** Investují do výzkumu a vývoje, zaměřují se na 5G, IoT a bezpečné síťové technologie
- **Spolehlivost:** Jejich produkty jsou oblíbené díky robustnosti (EN 55035)



Hlavní oblasti působení Teltoniky

1. Sítová zařízení (Networking)

- Silnou divizí je výroba **průmyslových switchů, routerů, přístupových bodů a modemů**.
- Jsou určeny pro stabilní a bezpečné připojení k internetu v **náročných podmínkách** – např. v dopravě, průmyslu nebo energetice.
- Produkty podporují 4G LTE, nově i **5G**, a mají **funkce pro vzdálenou správu, VPN** a zajištění **kybernetické bezpečnosti**.

2. Telematika a GPS sledování

- Teltonika patří mezi přední výrobce zařízení **pro sledování vozidel** a správy vozových parků.
- Jejich GPS jednotky se používají pro monitoring polohy, spotřeby paliva, stylu jízdy či pro zabezpečení automobilů.
- Typické využití najdeme u logistických firem, autopůjčoven, taxi služeb nebo třeba při správě stavebních strojů.

3. IoT a M2M řešení

- Teltonika se zaměřuje na technologie, které propojují zařízení mezi sebou – tzv. machine-to-machine komunikaci.
- Dodávají **kompletní IoT platformy**, které umožňují firmám sbírat, přenášet a vyhodnocovat data v reálném čase.
- Tato řešení se uplatňují například v energetice (chytré měření spotřeby), zdravotnictví, zemědělství nebo při budování chytrých měst.

Síťová zařízení

1. RUT série (routery)

- Patří k vlajkovým produktům.
- Modely **RUTX** a **RUT9** podporují 4G LTE/5G, VPN, failover, Wi-Fi.
- Určeny pro průmyslové prostředí, dopravní systémy, energetiku.

2. TRB série (IoT brány / modemy)

- Menší zařízení pro připojení jedné aplikace nebo stroje.
- Např. **TRB140**, **TRB500 (5G)** – vhodné pro průmyslovou automatizaci, SCADA systémy, vzdálený monitoring.

3. TSW série (switche)

- Průmyslové switche s PoE napájením, ideální pro CCTV, síťové prvky v terénu.

4. SWM série

- 19“ switche do racku

Každé zařízení s managementem podporuje **RMS (Remote Management System)**

- Cloudová platforma pro vzdálenou správu všech Teltonika zařízení – monitoring, aktualizace, konfigurace.

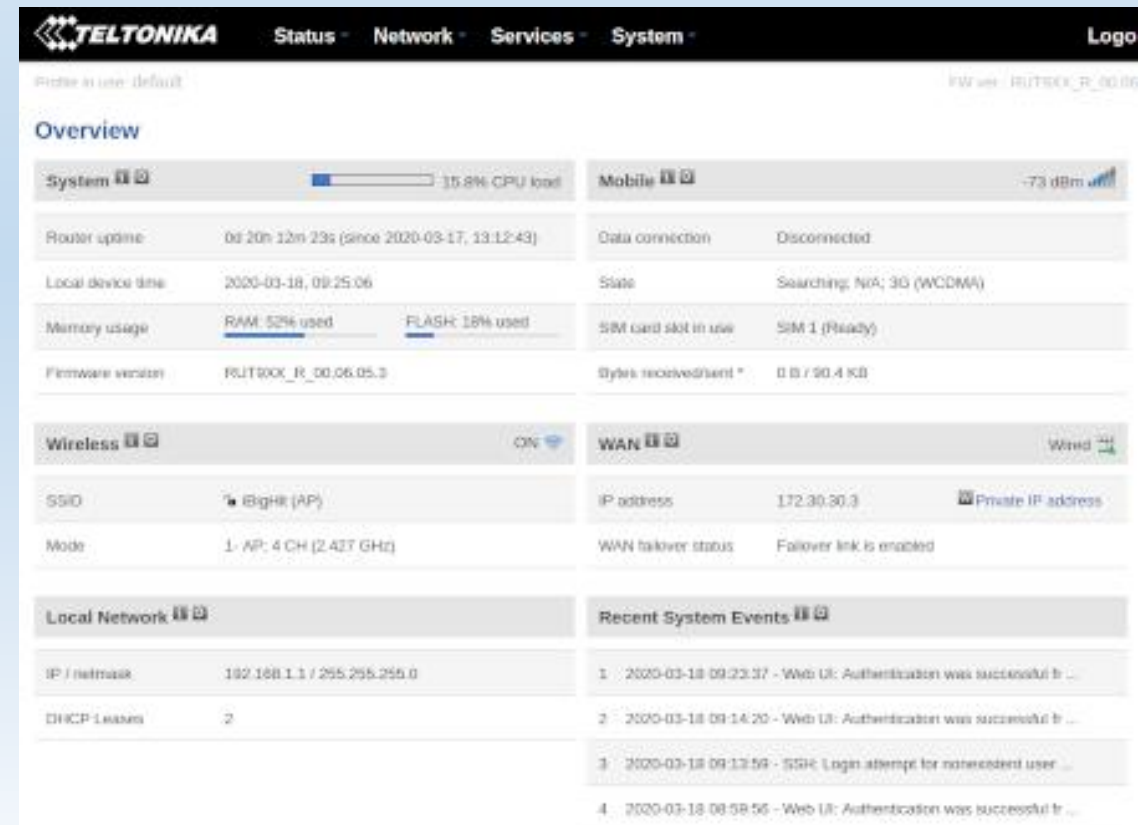


RutOS – Router Operating System

- Vychází z OpenWRT
- Používá se na všech zařízeních **RUT, TRB, TSW** (routery, brány, switche)
- Rozšířený o průmyslové funkce, bezpečnostní prvky a integraci s RMS
RUTOS = OpenWrt + průmyslové funkce + bezpečnost + RMS integrace.

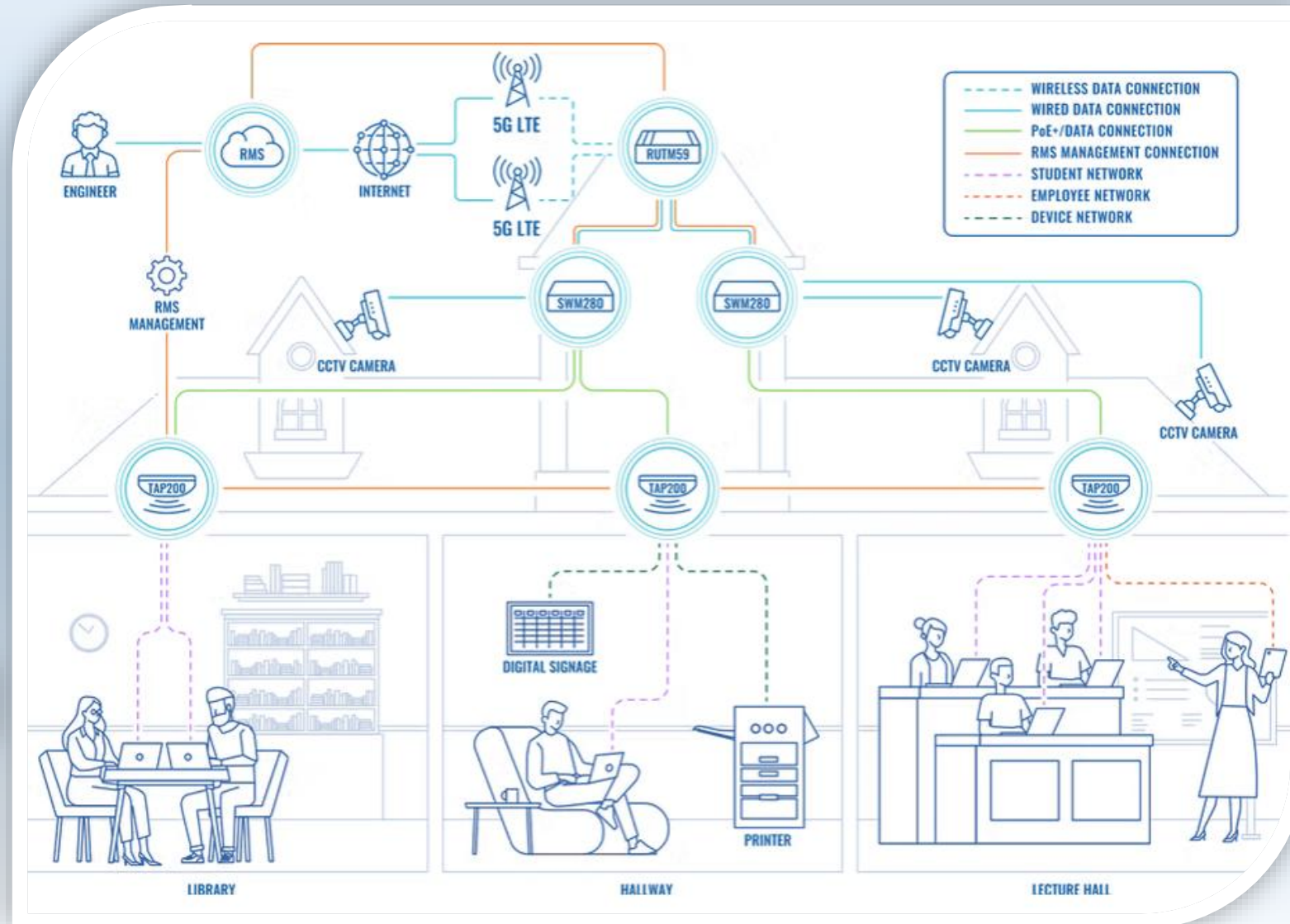
• Typické scénáře nasazení RUTOS

- Záložní internetové připojení pro pobočky firem.
- Průmyslová automatizace – připojení PLC přes Modbus a monitoring.
- IoT brány – sběr dat ze senzorů a přenos přes MQTT do cloudu.
- Doprava – mobilní Wi-Fi, GPS tracking, připojení k RMS.
- Retail – hotspots s captive portálem pro zákazníky.



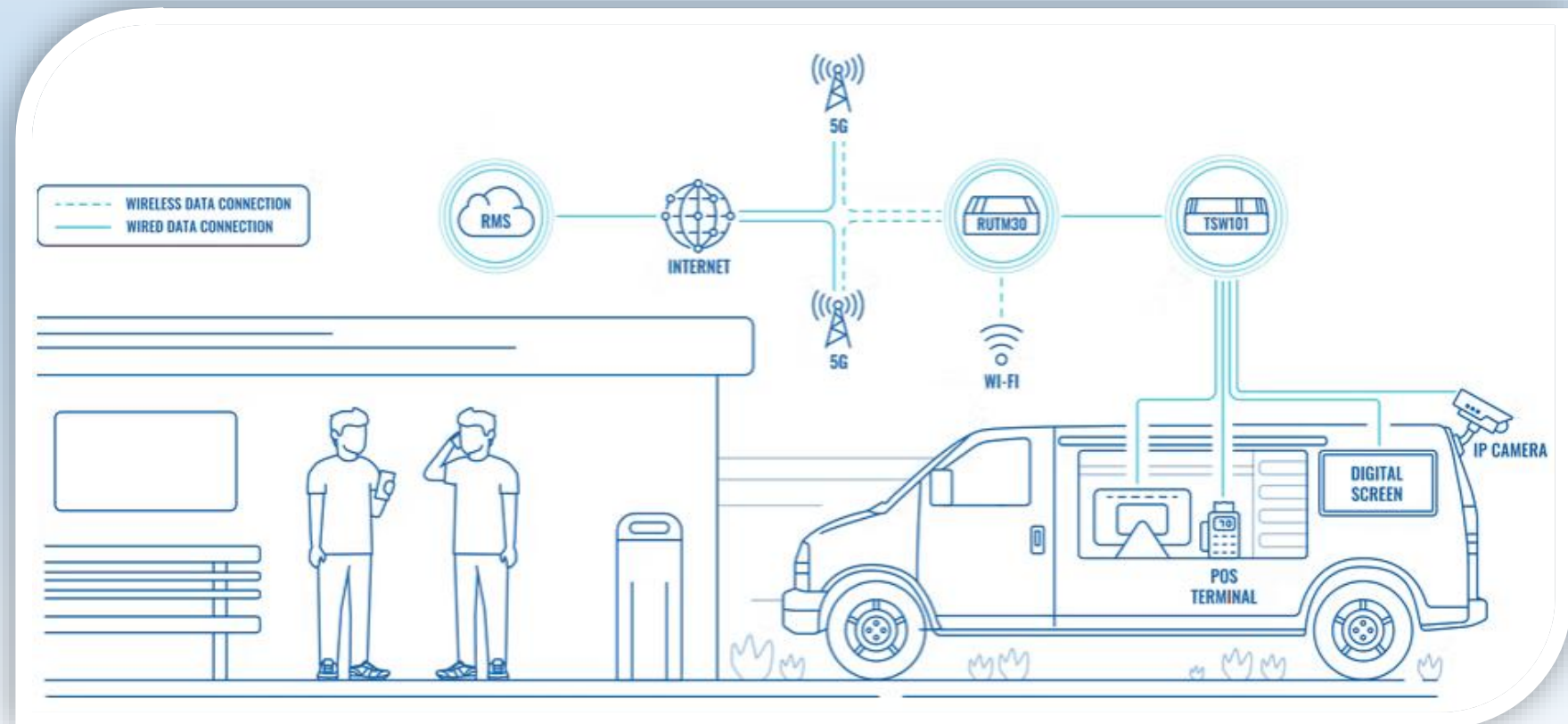
Novinky 2026 ~ SWM280 série

- ✓ 19" switche
- ✓ 24 portů
- ✓ Možné PoE 802.3at až 300W
- ✓ L2+ (static routing)
- ✓ Cloud správa a monitoring



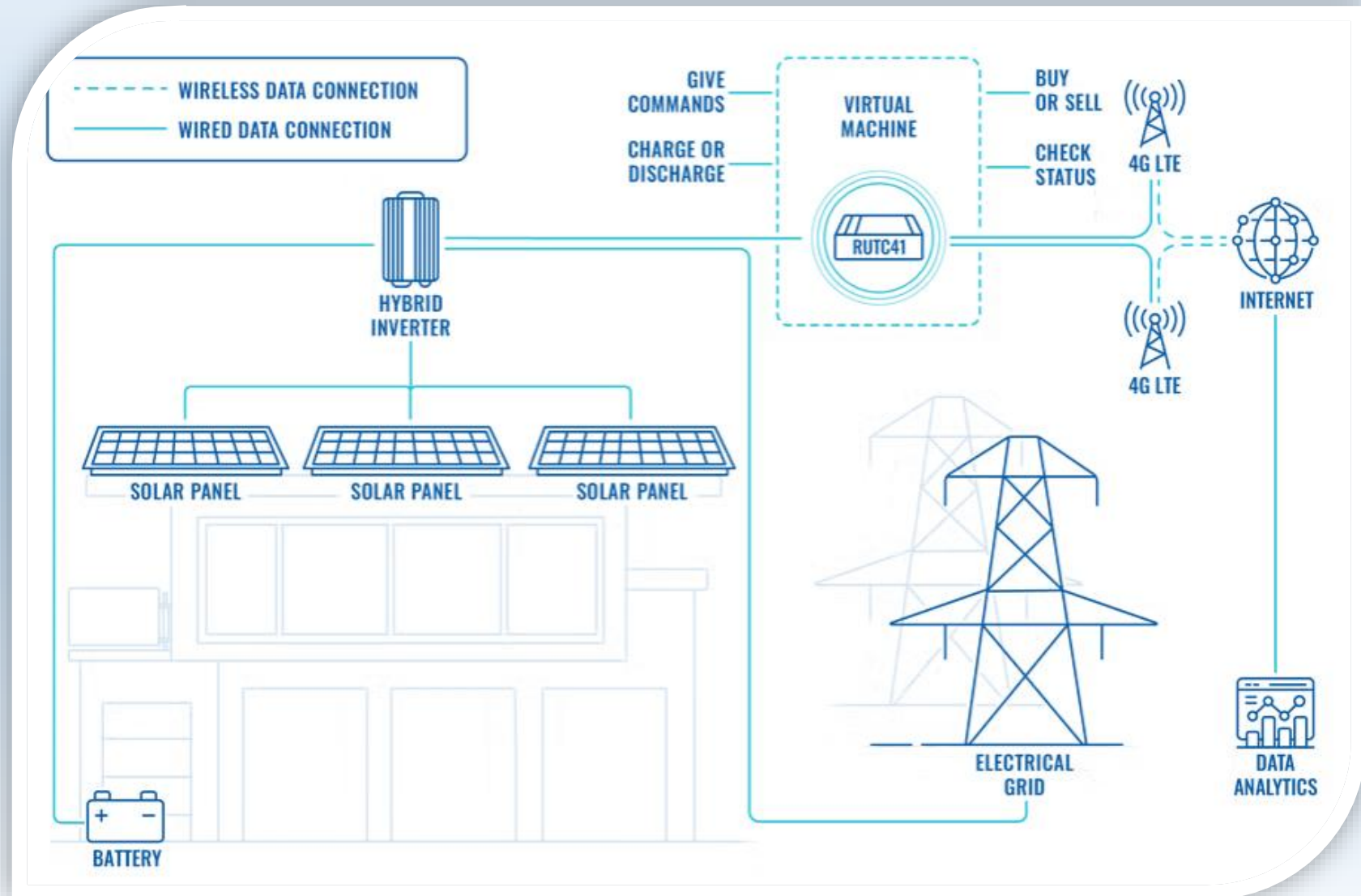
Novinky 2026 ~ RUTM20

- ✓ 5G router SA/NSA
- ✓ 4x4 MIMO antény
- ✓ Dual SIM+ eSIM
- ✓ PoE in/out
- ✓ WiFi 802.11ac



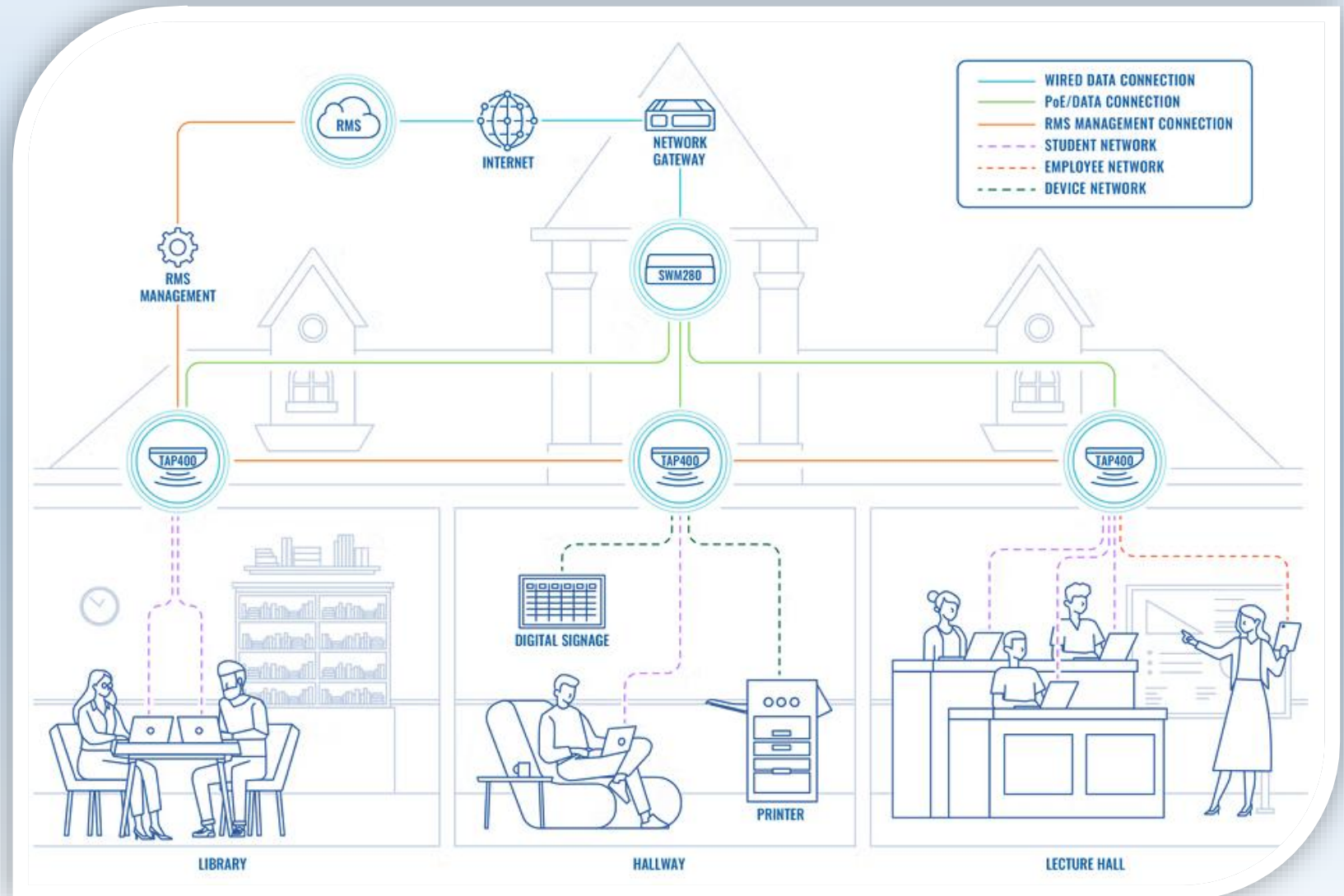
Novinky 2026 ~ RUTC41 / RUTC50

- ✓ 4G-LTE / 5G router
- ✓ Dual SIM+ eSIM
- ✓ WiFi 802.11ax
- ✓ **Docker aplikace v zařízení**



Novinky 2026 ~ TAP400

- ✓ **WiFi Access point**
- ✓ **Dual band 2,4+5GHz**
- ✓ **IEEE 802.11ax**
- ✓ **2,5GBASE-T RJ-45 LAN**
- ✓ **Podpora MESH**



Novinky 2026 ~ Altos CAP700

- ✓ **Domácí 5G-NR router**
- ✓ **WiFi IEEE 802.11be**
- ✓ **2,5GBASE-T RJ-45**
- ✓ **MODBUS client, server, database registers, gateway, alarmy**
- ✓ **Přímá podpora BACnet (Building Automation and Control Network)**
 - HVAC (topení, větrání, klimatizace)
 - osvětlení,
 - měření energií
 - zabezpečení
 - řízení přístupu
 - průmyslových a komerčních budovách



Novinky 2026 ~ OTD140 a OTD500

- ✓ Outdoor routery pro 4G-LTE a 5G-NR
- ✓ IP55 – odolnost proti dešti, prachu, UV
- ✓ Dual SIM – automatické přepínání
- ✓ 2× Ethernet (LAN/WAN)
- ✓ PoE-in + PoE-out (napájení kamer / IoT)
- ✓ RutOS – VPN, firewall, RMS, SNMP, MQTT
- ✓ Teploty -40 až +75 °C
- ✓ Montáž na stožár/stěnu



Novinky 2026 ~ 5G RedCap

- ✓ **Reduced Capability - odlehčené ale stále plnohodnotné 5G**
- ✓ **nižší cena, nižší spotřeba, nízká latence**
- ✓ **Down 223 x Up 123 Mb/s**
- ✓ **IoT a průmysl, SCADA, M2M**

RUT976 – průmyslový router

- 5G RedCap + LTE Cat4 fallback
- 4× LAN, RS232/RS485, 7× I/O, GNSS
- Wi-Fi 4, až 100 klientů



RUT276 – kompaktní IoT router

- 5G RedCap + LTE fallback
- RS232/RS485
- Wi-Fi 4, Mesh, WPA3

	4G LTE-M (Cat-M1)	LTE (Cat-4)	5G RedCap	Plnohodnotné 5G
Download	~1 Mbps	až 150 Mbps (Cat-4)	150 – 220 Mbps	1 – 10+ Gbps
Upload	~1 Mbps	až 50 Mbps (Cat-4)	50 – 100 Mbps	100 – 1000+ Mbps
Latence	Vyšší (50–150 ms)	Střední (30–80 ms)	Nízká (10–20 ms)	Velmi nízká (1–10 ms)
Spotřeba	Extrémně nízká	Střední	Nízká až střední	Vysoká

RMS – Remote Management System

- **Cloudová služba** pro vzdálenou správu a monitoring síťových zařízení (routerů RUT, bran TRB, switchů TSW) a částečně i telematiky.
- Funguje jako **centrální řídicí panel**, kde má správce přehled o stovkách nebo tisících zařízení nasazených kdekoliv po světě.
- Přístup je přes **webové rozhraní** (bez nutnosti VPN či veřejné IP adresy).

Praktické příklady využití

- **Energetika**: dohled nad routery v trafostanicích, možnost vzdáleně restartovat či přenastavit.
- **Retail & banky**: správa stovek poboček bez nutnosti posílat techniky.
- **Doprava**: vzdálená správa routerů ve vozidlech (autobusy, vlaky, kamiony).
- **Průmysl**: přístup na PLC a SCADA přes RMS Connect, bez VPN a veřejných IP.

RMS – vrstvy systému

1. RMS Management

- Monitoring a konfigurace zařízení.
- Správa nastavení, aktualizace firmwaru, vzdálený reboot.

2. RMS Connect

- Umožňuje vzdálený přístup **k zařízením za routerem** – např. PLC, IP kamerám, serverům.
- Připojení přes **SSH, HTTP/HTTPS, RDP, VNC** bez veřejné IP.

3. RMS VPN

- Vytvoření **virtuální privátní sítě** mezi zařízeními Teltonika a uživateli.
- Nahrazuje složitou VPN konfiguraci na routerech – vše je spravováno z cloudu.

4. RMS API

- Umožňuje integraci RMS do vlastních IT systémů.
- Možnost automatizace (např. nasazení nových zařízení, sběr statistik, propojení s helpdeskem).

RMS – přístup a bezpečnost

1. Architektura a technologie

- **Cloud-first řešení** – RMS běží v cloudu (Teltonika používá evropská datová centra a partnery typu AWS pro vysokou dostupnost).
- **End-to-end šifrování** – komunikace mezi zařízením a RMS je zabezpečena (TLS, certifikáty, unikátní autentizace každého zařízení).
- **Bez veřejné IP adresy** – zařízení se připojuje samo k RMS, správce nepotřebuje složitě nastavovat NAT, port forwarding ani VPN.

2. Licencování

- RMS funguje na principu **kreditů** (1 kredit = 30 dní správy jednoho zařízení).
- Lze zakoupit balíčky kreditů a přidělovat je podle aktuálních potřeb.
- Díky tomu je škálovatelné – od malých projektů (jednotky zařízení) až po velké flotily (tisíce routerů).

3. Bezpečnostní aspekty

- Každé zařízení má **unikátní identitu** v RMS.
- Správci mohou využít **role a oprávnění** (např. operátor má jen čtení, admin plnou správu).
- Audit log – všechny akce uživatelů se zaznamenávají.

RMS - rozhraní

>

Management

Devices

Wi-Fi & Hotspots

Task manager

Reports

Alerts & Automations

Monitoring templates

RMS Connect

Remote access

Access history

RMS VPN

VPN hubs

VPN quick connect

Administration

Companies

Users

Tags

Files

Resources

Management > Devices

Devices

ACCOUNT SETTINGS AND MISC.

wikidemott@gmail.com

Status

Online 2

Device model

TRB143 1

RUTX11 1

Device firmware

TRB1_T_R713_00.07.12.1168 1

RUTX_R_00.07.12.3 1

ACTIONS MENU

Actions Filter Search table... Default Showing 2 of 2 items Page settings

Status	Actions	Name	Model	Company name	Tags	Serial	MAC	Created at
Online		RUTX11_LV	RUTX11	#10 Wiki	-	1113589121	00:1E:42:37:AF:5F	2025-02-24 09:48:18
Online		TRB143Mbus	TRB143	#10 Wiki	-	6000188028	4E:9B:9F:A6:1C:BF	2025-02-05 09:04:49

MAIN CONTENT WINDOW

NAVIGATION PANEL

RMS - rozhraní

Devices > Wiki devices > Tagged devices > RUTX11_DN #18472

wikidemotit@gmail.com

RUTX11_DN - Device information

Actions ▾ General Monitoring history **Dashboards (Beta)** Data usage Location Ports Network Remote access Other services

< Meter1

 Save

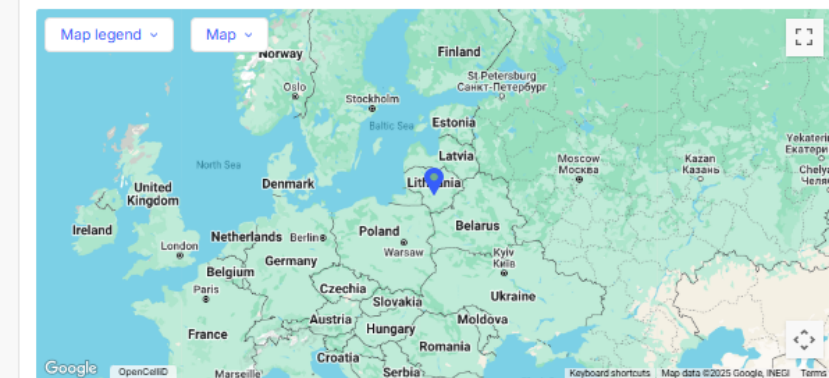
✕ Cancel

+ Add widget

2025-03-03 11:59 - Now

 κ^2

Current location



Embedded Controller

Sensor Data

Temperature: 23.1 °C

Humidity: 41.1 %

LED Control

LED 1

Status: **OFF**

Turn On Turn Off

LED 2

Status: **OFF**

Turn On Turn Off

Alerts

Status	Device name	Serial	MAC	Company	Created at
 Failure	RUTX1_DN			Wiki	2025-03-05 10:20:47
 Failure	RUTX1_DN			Wiki	2025-03-05 08:09:17
 Success	RUTX1_DN			Wiki	2025-03-04 11:10:14

Data: 1

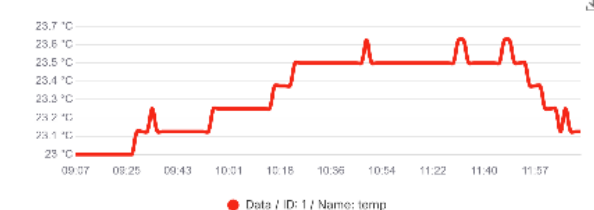
```
IF ( Data == 1 )
```

✓ Send notification

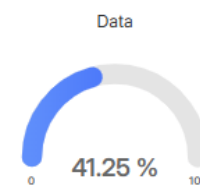
Temperature



⚠ Temperature data



Humidity



⚠ Humidity data



Temperature Table

Data	Created at
23.125000 °C	2025-03-05 12:13:52
23.125000 °C	2025-03-05 12:12:06
23.125000 °C	2025-03-05 12:10:19
23.250000 °C	2025-03-05 12:08:33

Device tasks

Group name

#543 DN_LED1&LED2_TEST

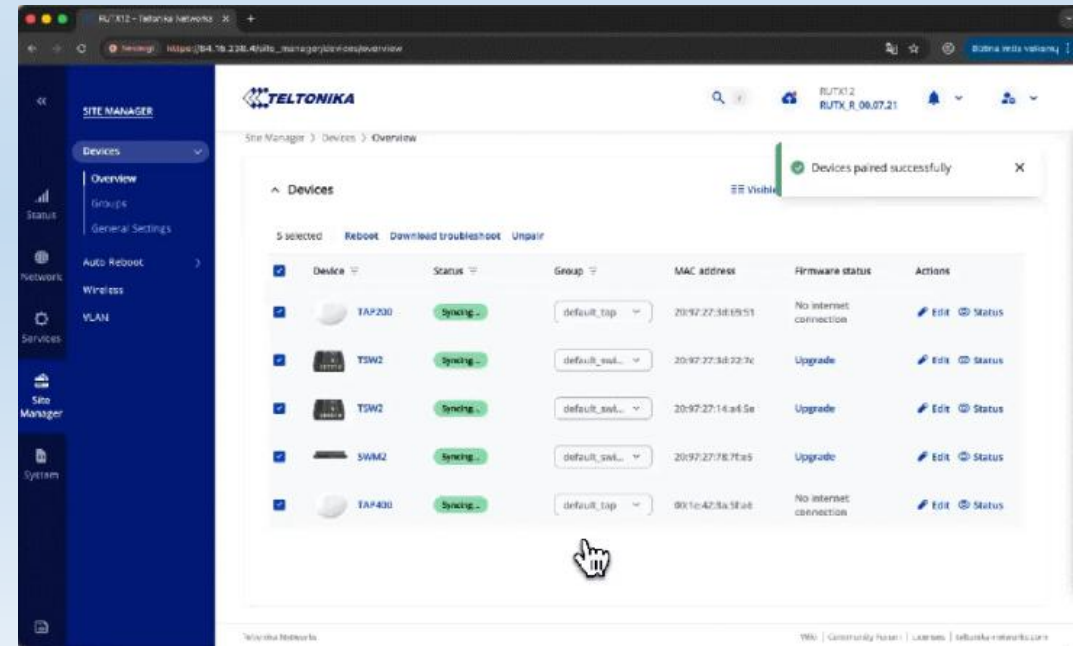
▶ Execute

Novinky 2026 ~ Site manager

- ✓ lokální centrální kontrolér
- ✓ běží přímo uvnitř Teltonika routeru (RutOS 7.21+)
- ✓ TSW switche a TAP access pointy bez RMS cloudu

Funkce:

- Lokální centrální správa – vše běží na routeru, žádný cloud
- Discovery zařízení – automaticky najde TAP AP a TSW switche v síti
- Párování zařízení – Unpaired → Pairing → Syncing → Paired
- Plná konfigurace připojených zařízení
- Skupiny zařízení – organizace podle typu nebo lokace
- Troubleshoot file – stažení diagnostiky zařízení
- Zákaz WebUI na zařízení po spárování



NIS2 - Network and Information Security

Teltonika i jako **dodavatel ICT zařízení a služeb pro kritickou infrastrukturu.**

Podle směrnice NIS2 (článek 6 a následující) musí poskytovatelé digitálních služeb a výrobci síťových zařízení dodržovat několik zásad kybernetické bezpečnosti.

- **Bezpečnostní aktualizace a správa zranitelností**

- Pravidelné firmware aktualizace pro RUTOS routery a TRB brány.
- Možnost rollbacku při chybné aktualizaci.
- RMS umožňuje hromadné aktualizace a centralizovaný dohled nad bezpečnostními patchemi.

- **Bezpečné protokoly a šifrovaná komunikace**

- VPN (WireGuard, OpenVPN, IPsec) a RMS Connect šifrovaně propojují zařízení s cloudem i vzdálenou správou.
- TLS a certifikáty na web UI a SSH pro zabezpečení managementu.

- **Monitoring a audit**

- RMS poskytuje audit logy, role-based access control (RBAC) a monitoring zařízení.
- Podpora SNMP, syslog a health checks umožňuje sledování bezpečnostních incidentů.

- **Segmentace a modulární architektura**

- IoT a průmyslové protokoly jsou odděleny od běžné sítě, RUTOS podporuje VLAN, NAT, firewall a QoS.

- **Dokumentace a reporting**

- RMS centralizuje konfigurace, aktualizace a provozní metriky, což podporuje povinnou evidenci a reportování podle NIS2.

NIS2 versus

RuTOS -----

- **Zabezpečení zařízení**
 - RuTOS je Linux-based OS s pravidelnými aktualizacemi a end-to-end šifrováním.
 - Firewall, VPN (WireGuard, OpenVPN, IPsec) a role-based access control pomáhají splnit požadavky na ochranu sítí a dat.
- **Správa zranitelností**
 - Teltonika poskytuje plánované **firmware aktualizace** a možnost rollbacku, což je klíčové pro NIS2 compliance.
 - Modulární architektura umožňuje rychlou reakci na bezpečnostní incidenty a zranitelnosti.
- **Audit a monitoring**
 - Audit logy, SNMP, syslog, monitoring zařízení a RMS agent umožňují sledování a hlášení bezpečnostních událostí, což je doporučeno NIS2.
- **IoT a průmyslové protokoly**
 - Podpora protokolů jako Modbus, MQTT a BACnet je důležitá pro kritické systémy, ale vyžaduje správnou segmentaci sítě a zabezpečené tunely (VPN).

RMS -----

- **Centrální správa a dohled**
 - RMS umožňuje centralizovanou správu zařízení, provisioning, firmware updates a vzdálenou konfiguraci, což zjednodušuje splnění NIS2 povinností.
- **Bezpečná komunikace**
 - RMS Connect a RMS VPN poskytují šifrovaný přístup k zařízení za NAT/firewallem bez veřejné IP, což minimalizuje riziko útoků.
- **Role-based přístup a audit**
 - Podpora více uživatelských rolí, audit logů a integrace s API umožňuje sledovat a kontrolovat činnosti uživatelů, což je kritické pro NIS2 compliance.
- **Škálovatelnost a dokumentace**
 - RMS umožňuje spravovat stovky až tisíce zařízení a dokumentovat aktualizace a změny konfigurací, což vyhovuje požadavkům na bezpečnostní záznamy.