RACOM

Manual de utilizare

M!DGE3
Router celular

fw 2.2.1.0
2025-02-11
versiunea 1.11

Quick start

Hardware

Configurare

Parametrii

RACOM sro| Mirova 1283 | 592 31 Nove Mesto na Morave | Cehia Tel.: +420 722 937 522 | E-mail: racom@racom.eu

www.racom.eu

Cuprins

Notă importantă

Produsele oferite pot conține software proprietar al RACOM. Oferta de furnizare a acestor produse și servicii nu include și nu deduce niciun transfer de proprietate.

Disclaimer

Deși au fost luate toate măsurile de precauție în pregătirea acestor informații, RACOM nu își asumă nicio responsabilitate pentru erori și omisiuni, sau orice daune rezultate din utilizarea acestor informații. Acest document sau echipamentul poate fi modificat fără notificare prealabilă, în interesul îmbunătățirii produsului.

RACOM își rezervă dreptul de a face modificări în specificațiile tehnice sau în această funcție a produsului sau de a opri producția acestui produs sau de a rezilia asistența de service fără notificarea prealabilă în scris a clienților.

Notă importantă

- Datorită naturii comunicațiilor fără fir, transmisia și recepția datelor nu pot fi niciodată garantate. Datele pot fi întârziate, corupte (adică au erori) sau se pot pierde total. Întârzierile sau pierderile semnificative de date sunt rare atunci când dispozitivele wireless, cum ar fi M!DGE3, sunt utilizate într-un mod adecvat într-o rețea bine construită. M!DGE3 nu trebuie utilizat în situații în care eșecul de a transmite sau de a primi date ar putea duce la daune de orice fel pentru utilizator sau orice altă parte, inclusiv, dar fără a se limita la vătămări personale, deces sau pierderea proprietății. RACOM nu își asumă răspunderea pentru daunele de orice fel rezultate din întârzieri sau erori ale datelor transmise sau primite folosind M!DGE3, sau pentru eșecul M!DGE3 de a transmite sau primi astfel de date.
- În niciun caz RACOM sau orice altă companie sau persoană nu este responsabilă pentru daune accidentale, accidentale sau asociate rezultate ca urmare a utilizării acestui produs. RACOM nu oferă utilizatorului nicio formă de garanție care să conțină asigurarea adecvării și aplicabilității pentru aplicarea sa.
- Produsele RACOM nu sunt dezvoltate, proiectate sau testate pentru a fi utilizate în aplicații care pot afecta în mod direct sănătatea și/sau funcțiile vieții oamenilor sau animalelor și nici pentru a fi o componentă a unor sisteme la fel de importante, iar RACOM nu oferă nicio garanție atunci când produsele companiei sunt utilizate în astfel de aplicații.

1. Ghid rapid

M!DGE3 este un router celular compact și configurabil pe scară largă. Tot ce trebuie să faceți pentru a-l pune în funcțiune este să îl conectați la o antenă și o sursă de alimentare și să îl configurați folosind un PC (tabletă, smartphone) și un browser web.

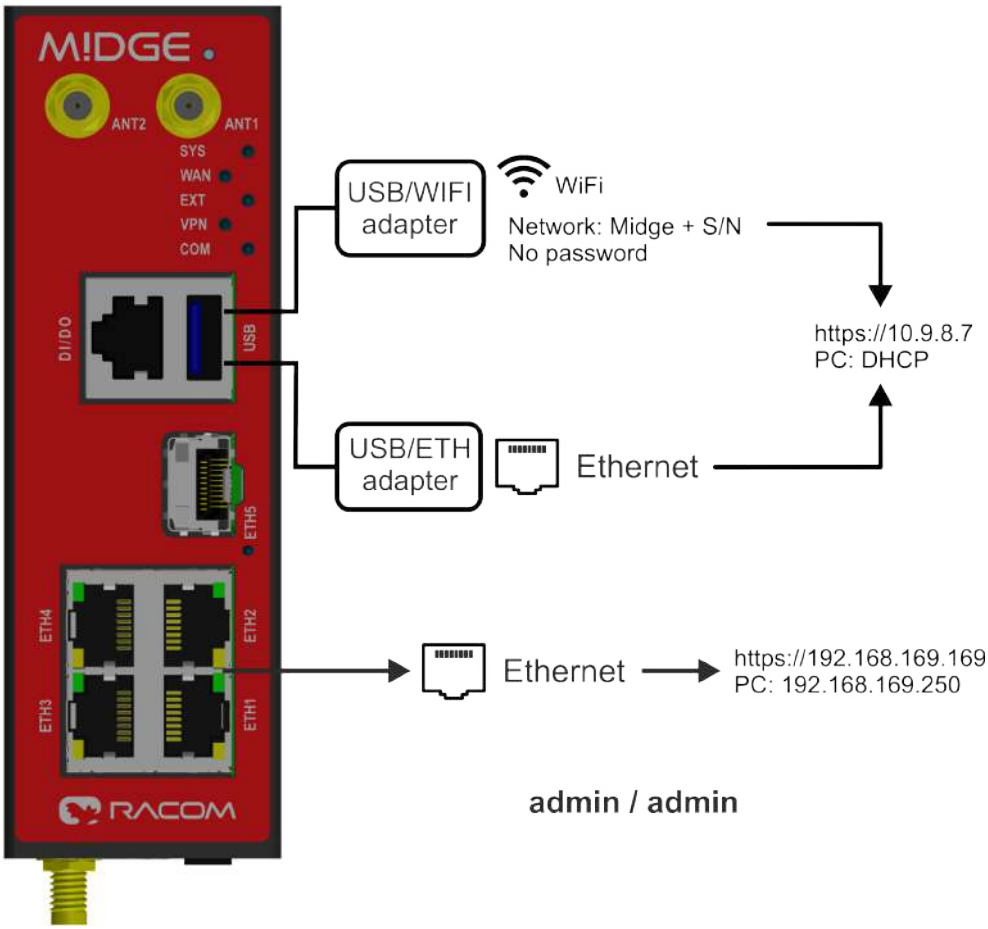


Fig. 1.1: Conectarea M!DGE3 la un PC prin WiFi, adaptor ETH/USB, interfață ETH

Parola implicită pentru contul „admin” este „admin”. Schimbați parola înainte de a instala unitatea într-o rețea.

Pentru a configura M!DGE3, îl puteți conecta la computer în trei moduri:

PC (tabletă, smartphone) conectat prin adaptor WiFi

Adaptor WiFi extern Cod piesa OTH-USB/WIFI-W2 (un accesoriu opțional al M!DGE3 vezi*adaptor USB*[1]) trebuie utilizat. Orice alt adaptor nu va funcționa corect atunci când este conectat la unitatea M!DGE3. Conectați mai întâi computerul, tableta sau smartphone-ul la M!DGE3 WiFi AP. SSID-ul său implicit este Midge S/N. În mod implicit, WPA2 PSK este dezactivat, deci nu este necesară nicio parolă. Adaptorul WiFi conține un server DHCP încorporat, așa că dacă aveți un client DHCP pe computer (cum o fac majoritatea utilizatorilor), nu trebuie să configurați nimic. Adresa IP implicită a unității M!DGE3, pentru acces prin adaptorul USB, este 10.9.8.7.

[1] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb

PC conectat prin adaptor ETH/USB

Adaptor extern ETH/USB Cod piesa OTH-USB/ETH-XR (un accesoriu optional al M!DGE3 vezi *Adaptor ETH/USB*[2]). ETH/USB conține un server DHCP încorporat, așa că dacă aveți un client DHCP în computer ca majoritatea utilizatorilor, nu trebuie să configurați nimic. Adresa IP implicită a unității M!DGE3, pentru acces prin adaptorul ETH/USB, este 10.9.8.7.

PC conectat direct la un port ETH

Adresa IP implicită pentru acces prin porturile ETH este 192.168.169.169.
Setați o adresă IP statică în PC în 192.168.169.0/24 (de exemplu, 192.168.169.250, masca de subrețea 255.255.255.0).

Important

Când schimbați adresa M!DGE3 ETH cu o altă adresă IP/mască, este posibil ca adresa IP a computerului dvs. să fie necesară pentru a fi actualizată pentru a se potrivi cu aceeași subrețea (mască).

Nota

HTTPS-Din motive de securitate, protocolul http cu criptare SSL poate fi utilizat pentru comunicarea dintre PC și M!DGE3. Protocolul HTTPS necesită un certificat de securitate. Trebuie să instalați acest certificat în browserul dvs. web. Prima dată când vă conectați la M!DGE3, computerul vă va cere autorizarea pentru a importa certificatul în computer. Certificatul este semnat de autoritatea de certificare RACOM sro. Îndeplinește toate reglementările de securitate și nu trebuie să vă faceți griji cu privire la importarea lui în computer. Confirmați importul cu toate avertismentele și excepțiile pe care browserul dvs. le poate afișa în timpul instalării.

Nota

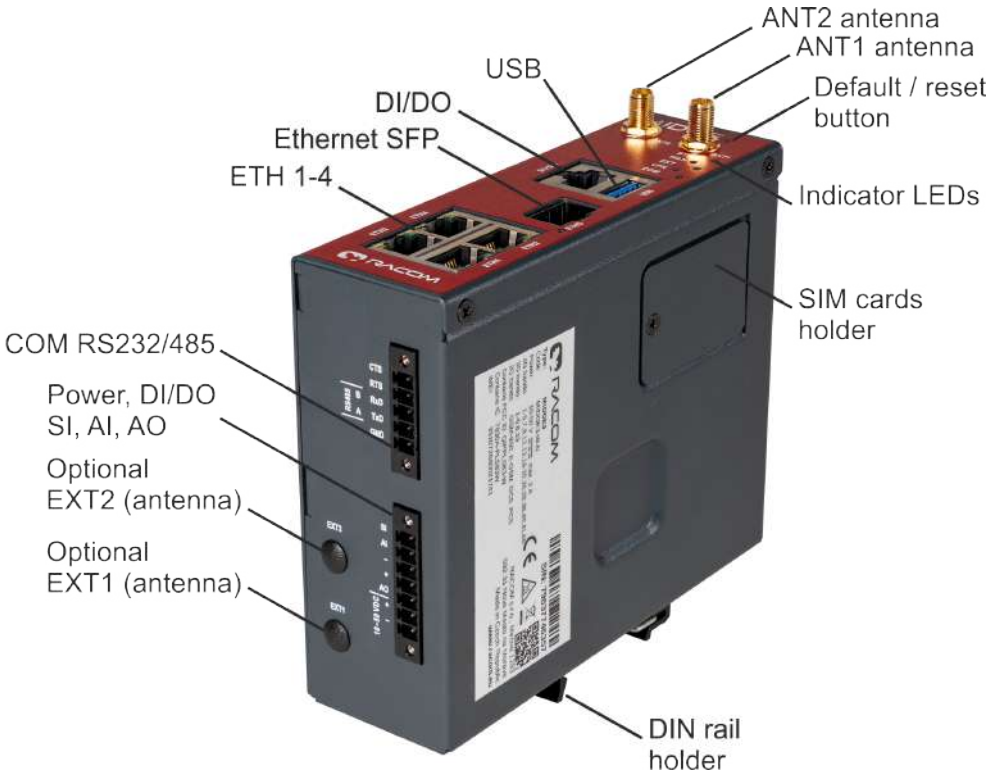
Dacă nu aveți adaptorul USB sau ați uitat parola, puteți reseta parametrii de acces la valorile implicite, consultați *Secțiunea 2.2.8, „Butonul HW”*.

Nota

Setări minime necesare pentru a configura conexiunea celulară.

[2] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb

2. Produs



M!DGE3 este o platformă de router celular concepută pentru orice mediu în timp real. Routerele celulare M!DGE3 sunt dispozitive IP native, cu sistem de operare Linux care au fost proiectate cu atenție la detalii, performanță și calitate.

M!DGE3 este încorporat într-o carcasă metalică robustă care permite posibilități multiple de instalare, vezi *Secțiunea 4.3, „Montarea”*.

Nota

Varianta M!DGE3e are unele limitări în ceea ce privește interfețele HW și caracteristicile SW. Detaliile sunt menționate în capitolele/descrierile respective.

2.1. Dimensiuni

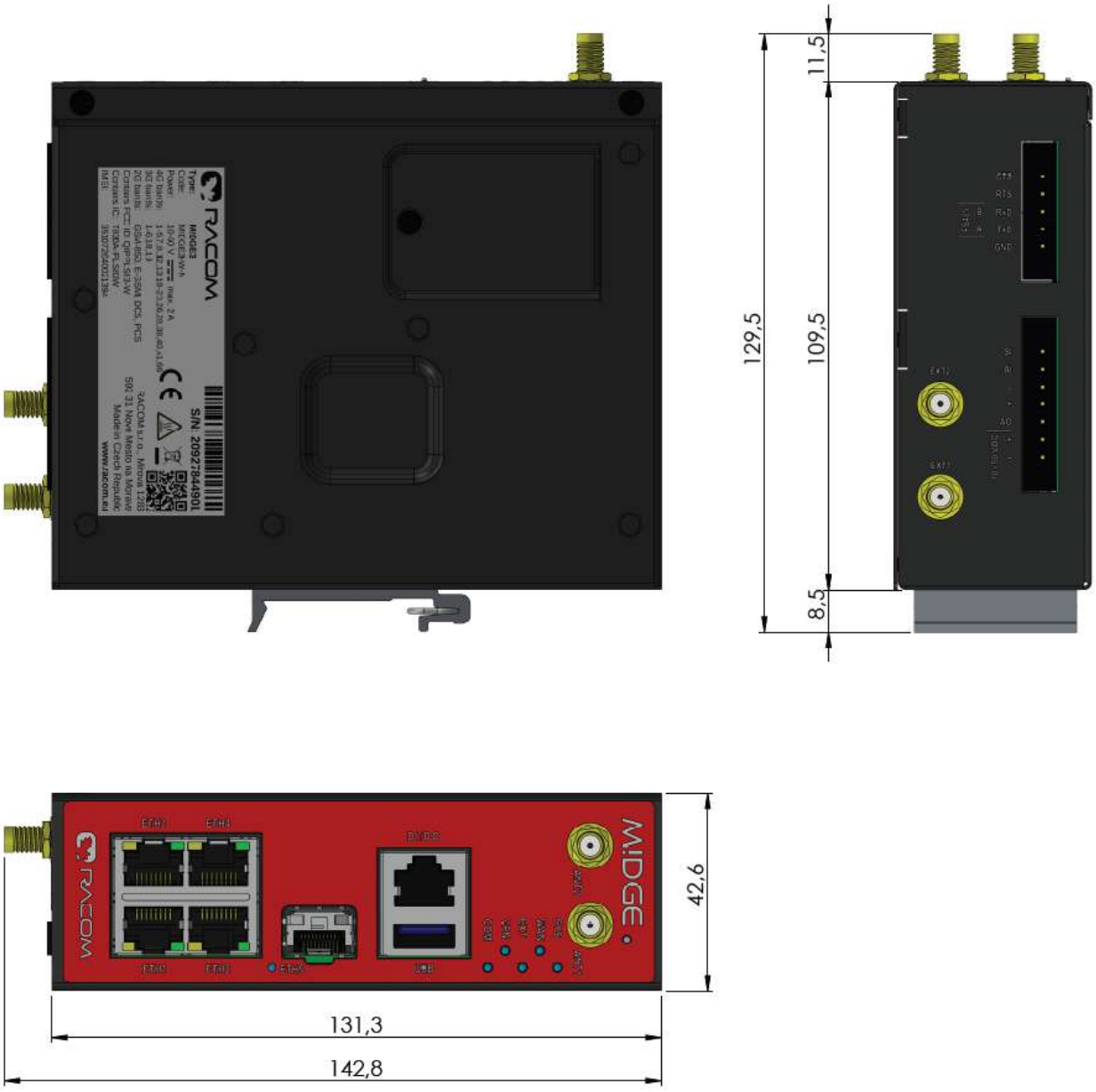


Fig. 2.1: Dimensiunile M!DGE3

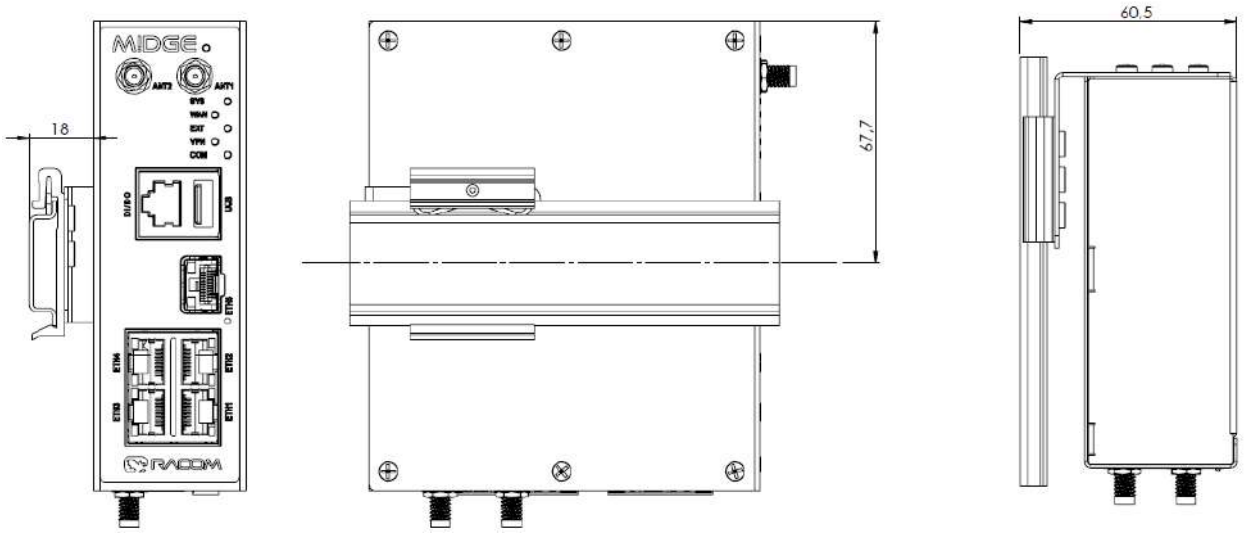


Fig. 2.2: M!DGE3 Dimensiuni suport de margine

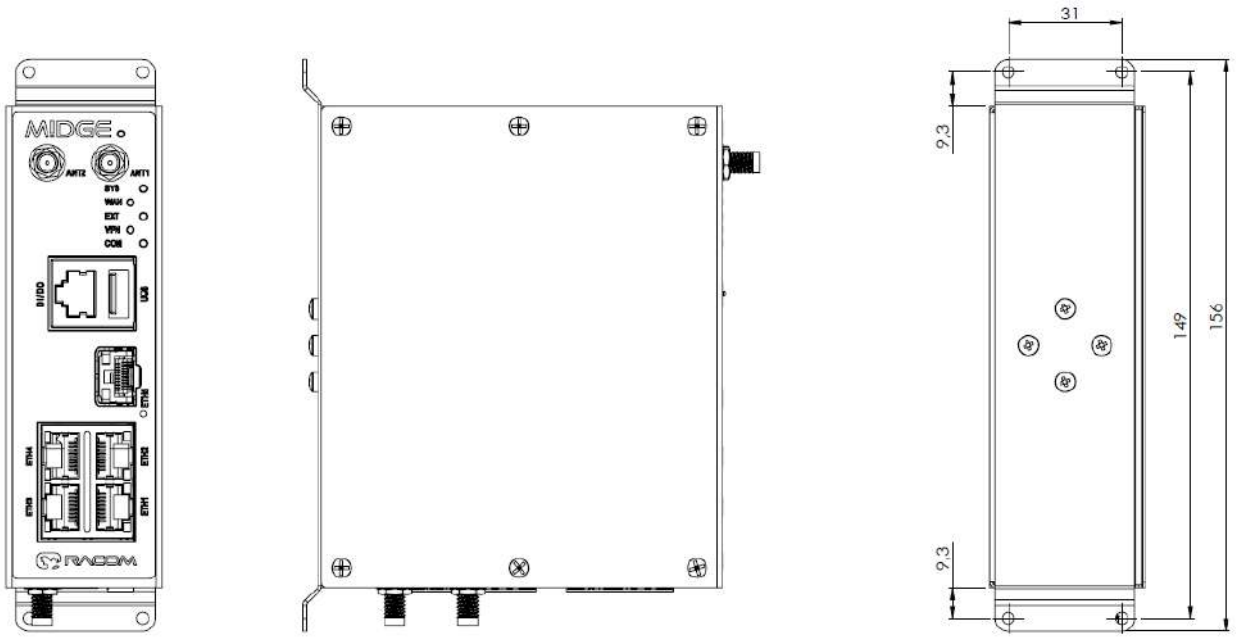


Fig. 2.3: Dimensiuni suport plat M!DGE3

Pentru mai multe informații vezi*Secțiunea 4.3.1, „Montarea șină DIN”*și*Secțiunea 4.3.2, „Montare plată”*.

2.2. Conectori

Toți conectorii sunt amplasați pe panoul frontal și inferior. Panoul frontal conține chiar și LED-uri. Butonul HW se află și pe panoul frontal (aproape de marginea superioară).

Fig. 2.4: Conectori

2.2.1. Antenă

O antenă poate fi conectată la M!DGE3 prin conectorul SMA mamă de 50 Ω.

M!DGE3 este echipat cu doi conectori. Conectorul ANT1 va fi folosit pentru transmisie și recepție comune. Conectorul ANT2 va fi folosit ca conector de diversitate Rx.

Fig. 2.5: Conectori antene

Nota

Pentru o conexiune LTE optimă, se recomandă utilizarea ambelor antene (diversitate Rx).
Dacă este utilizată o singură antenă, atașați-o la conectorul ANT1.

Avertizare

Routerul celular M!DGE3 poate fi deteriorat atunci când este utilizat fără antenă sau fără încărcătură.

2.2.2. Putere și control

Acest conector robust se conectează la o sursă de alimentare și conține semnale de control. O fișă cu terminale cu șuruburi și șuruburi de fixare pentru conectorul de alimentare și de control este furnizat cu fiecare M!DGE3. Este un mufă Tyco cu 7 pini, piesa nr. 1776192-7, pas de contact 3,81 mm. Conectorul este proiectat pentru fire electrice cu o secțiune transversală de 0,5 până la 1,5 mm2. Îndepărtați cablurile la 6 mm (1/4 inch). Cablurile izolate trebuie să primească manșoane PKC 108 sau mai puțin înainte de a fi introduse în clemă. Introduceți cablurile în porturile de sârmă, strângând bine.

Tab. 2.1: Atribuirea pinului

Pin	Etichetat	Semnal
1	SI	INTRARE SLEEP • trageți sub 1,1 VDC pentru a activa (histerezis prag de 1,1 VDC / 1,9 VDC) • max. 50 VDC
2	AI	INTRARE ALARMĂ HW • trageți sub 1,1 VDC pentru a activa (histerezis prag de 1,1 VDC / 1,9 VDC) • max. 50 VDC
3	−	− (GND) – pentru SLEEP IN, INTRARE ALARMĂ HW
4	+	+ (PUTERE) – pentru IEȘIRE ALARMĂ HW
5	AO	IEȘIRE ALARMĂ HW ieșire de scurgere deschisă max. 50 VDC, 1 A
6	+	+ POWER (10 până la 50 V) Prag de subtensiune 8,5 VDC Prag de supratensiune 55 VDC
7	−	− PUTERE (GND)

Pinii 3 și 7 sunt conectați intern. Pinii 4 și 6 sunt conectați intern.
Polul minus (GND) este conectat intern cu carcasa.

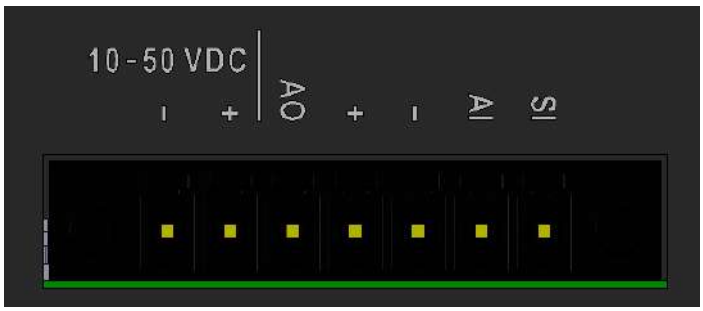


Fig. 2.6: Conector de alimentare

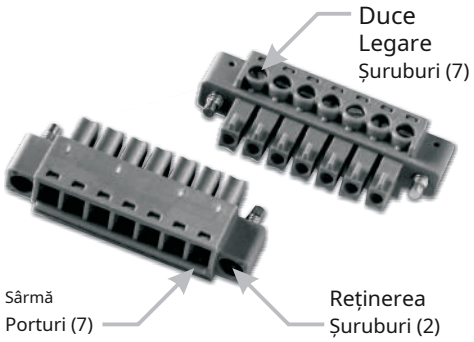


Fig. 2.7: Alimentare și control - mufa cablu

INTRARE ALARMĂ HW

HW ALARM INPUT este o intrare digitală. Dacă este împământat (de exemplu, prin conectarea la pinul 3), se declanșează o alarmă externă.

IEȘIRE ALARMĂ HW

HW ALARM OUTPUT este o ieșire digitală.

PUTERE

Pinii POWER etichetați + și - servesc la conectarea unei surse de alimentare de 10–50 VDC. Cerințele pentru o sursă de alimentare sunt definite în *Secțiunea 4.8, „Sursa de alimentare”* și *Capitolul 9, Parametrii tehnici*.

2.2.3. ETH1 - ETH4

Conectori RJ45 standard pentru conexiune Ethernet. M!DGE3 are interfețe 10/100/1000Base-T Auto MDI/MDIX, astfel încât se poate conecta la o rețea Ethernet de 10 Mb/s, 100 Mb/s sau 1000 Mb/s. Viteza poate fi selectată manual sau recunoscută automat de M!DGE3. M!DGE3 este prevăzut cu funcția Auto MDI/MDIX care îi permite să se conecteze atât prin cabluri standard, cât și prin cabluri transversale, adaptându-se automat.

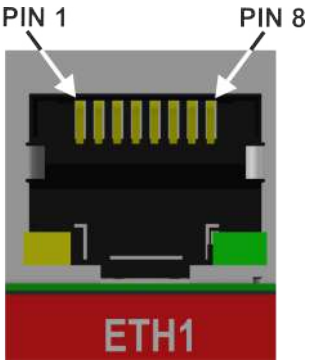
Nota

M!DGE3e are doar 2 porturi ETH.

Atribuirea PIN

Tab. 2.2: Conexiuni Ethernet la conectorul cablului

Pin	Semnal	Cablu direct	Cablu încrucișat
1	TX+	portocaliu – alb	verde – alb
2	TX-	portocale	verde
3	RX+	verde – alb	portocaliu – alb
4	—	albastru	albastru
5	—	albastru – alb	albastru – alb
6	RX-	verde	portocale
7	—	maro – alb	maro – alb
8	—	maro	maro



2.2.4. ETH5 (SFP)

ETH5 este un slot SFP standard pentru module Ethernet SFP 10/100/1000 Mb/s, care poate fi schimbat de utilizator cu un consum maxim de energie de 1,25 W. Sunt acceptate atât modulele SFP de fibră optică, cât și metalice Ethernet. Pentru fibră optică optică pot fi utilizate module Ethernet (= 2 sau 1 fibră optică). Modulele CSFP nu sunt acceptate. RACOM oferă toate tipurile menționate de module SFP, testate pentru a fi compatibile cu M!DGE3 ca accesoriu standard.

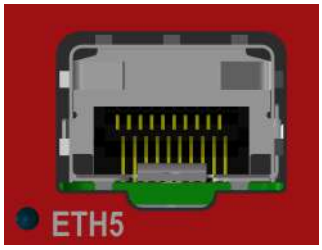


Fig. 2.8: Slot SFP

LED-ul de stare SFP este situat chiar lângă slot. Este controlat de modulul SFP. Funcția sa este specifică fiecărui modul SFP. Comportamentul tipic este o indicație că semnalul primit de la fibră optică sau legătura metalică se află în intervalul de funcționare.

Important

Este recomandat să utilizați un modul SFP de înaltă calitate cu interval de temperatură industrial. Modulele SFP enumerate în Accesorii sunt testate temeinic de RACOM și sunt garantate

pentru a funcționa cu unitățile M!DGE3. Este posibil să utilizați orice alt modul SFP, dar RACOM nu poate garanta că vor fi complet compatibile cu unitățile M!DGE3.

Nota

M!DGE3e nu are port SFP.

2.2.5. COM

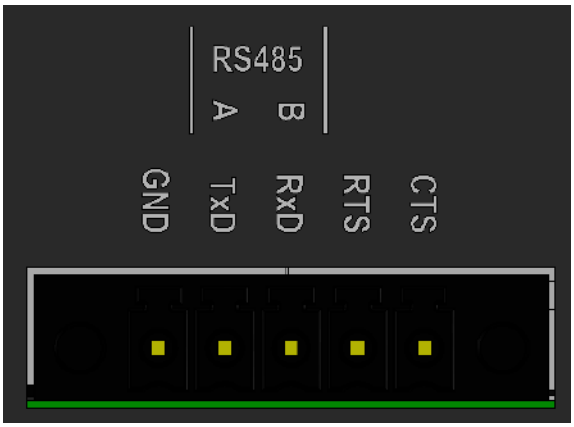
M!DGE3 oferă interfață serială COM terminată cu un conector terminal cu 5 pini care este furnizat cu fiecare unitate M!DGE3. Poate fi configurat ca RS232 sau RS485. Este un conector Tyco pentru bloc de borne cu 5 pini, piesa nr. 1776192-5, pas de contact 3,81 mm. Conectorul este proiectat pentru fire electrice cu o secțiune transversală de 0,5 până la 1,5 mm2. Îndepărtați cablurile la 6 mm (1/4 inch). Cablurile izolate trebuie să primească manșoane PKC 108 sau mai puțin înainte de a fi introduse în clemă. Introduceți cablurile în porturile de sârmă, strângând bine.

RS232 al M!DGE3 este un dispozitiv DCE (Data Communication Equipment) cu fir. Echipamentul conectat la portul serial al unității M!DGE3 trebuie să fie DTE (Echipament terminal de date).

RS485 al M!DGE3 nu este izolat galvanic și nu este terminat.

Tab. 2.3: Descrierea pinului COM

Terminal bloc	COM – RS232		COM – RS485	
Pin	**Semnal**	**In/Of**	**Semnal**	**In/Of**
1	CTS	Afară	—	
2	RTS	În	—	
3	RxD	Afară	linia B	Intrare/Ieşire
4	TxD	În	linia A	Intrare/Ieşire
5	GND		GND	



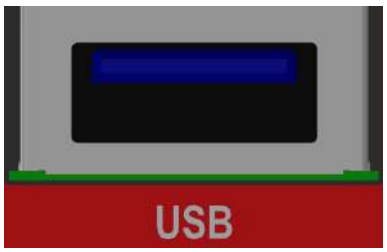
M!DGE3 menține pinul 6 DSR la nivelul 0 (stare ON, aprox. +6,2 V) conform standardului RS232 permanent.

2.2.6. USB

M!DGE3 folosește interfața USB 3.0, Host A. Interfața USB este cablată ca standard:

Tab. 2.4: Ansamblu cablu USB A Pinout

Pin	Semnal	Sârmă
1	VBUS	Roşu
2	D-	Alb
3	D+	Verde
4	GND	Negru
5	StdA_SSRX-	Albastru
6	StdA_SSRX+	Galben
7	GND_DRAIN	SOL
8	StdA_SSTX-	Violet
9	StdA_SSTX+	Portocale
Coajă	Scut	Carcasa conectorului



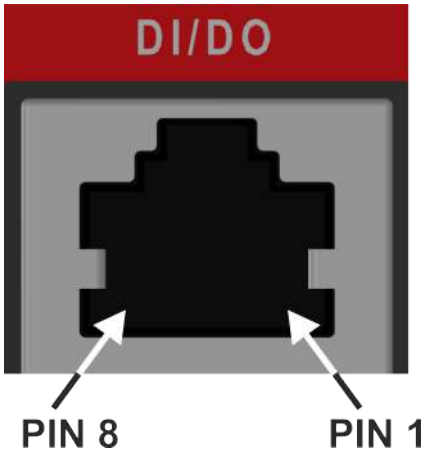
Interfața USB este proiectată pentru conectarea la un adaptor ETH/USB extern sau la un adaptor WiFi. Sunt accesorii opționale pentru M!DGE3, pentru mai multe detalii vezi *www/ripex/accesorii*[1]. Adaptoarele sunt utilizate pentru accesul de service la interfața de configurare web a unității M!DGE3.

Conectorul USB oferă și alimentare cu energie (5 V / 0,5 A). Poate fi folosit pentru a alimenta temporar un dispozitiv conectat, de exemplu un telefon. Conectorul USB nu trebuie utilizat ca sursă permanentă de alimentare cu energie.

2.2.7. DI/DO

Tab. 2.5: Intrări și ieșiri digitale

Pin	Descriere	Semnal
1	DI1+	Intrare digitală (diferențială) - Pozitivă - (P)
2	DI1-	Intrare digitală (diferențială) - Negativ - (N)
3	GND	Sol
4	DO1	Ieșire digitală 1
5	DO2	Ieșire digitală 2
6	GND	Sol
7	DI2	Intrare digitală 2
8	DI3	Intrare digitală 3



Ieșiri digitale:
• Ieșire de scurgere deschisă max. 50 VDC, 0,2 A

Intrare digitală diferențială izolată:
• Diferența de tensiune de intrare (PN) > 1,9 VDC logic „H”
• Diferența de tensiune de intrare (PN) < 1,1 VDC logic „L”
• Tensiune diferenţială maximă 50 V

Intrari digitale:
• Intrare inversată declanșată de Schmitt
• Trageți sub 1,1 VDC pentru a activa (histerezis prag de 1,1 VDC / 1,9 VDC)
• Max. 50 VDC

Nota

M!DGE3e nu are un conector DI/DO dedicat.

[1] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb

2.2.8. butonul HW

Fig. 2.9: Buton HW

Butonul HW este plasat în partea dreaptă a M!DGE3, lângă logo.

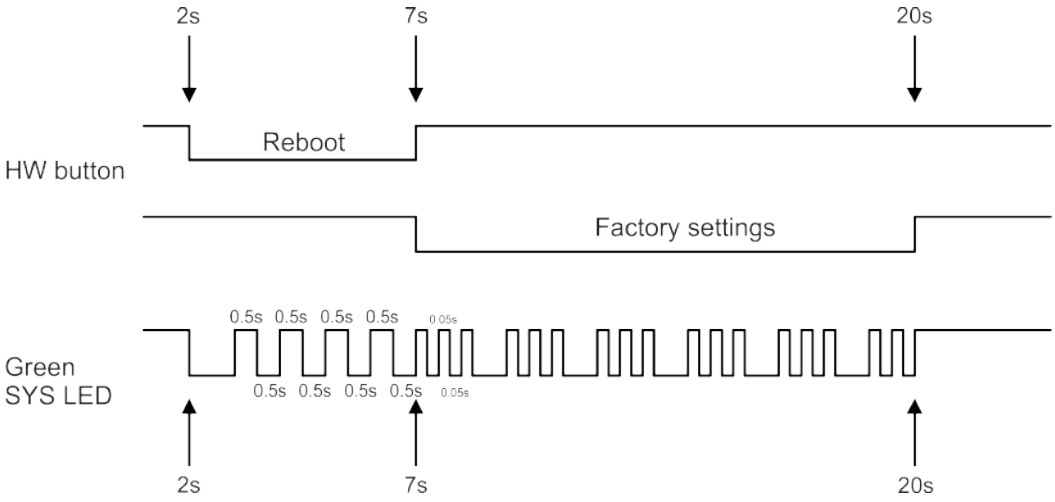


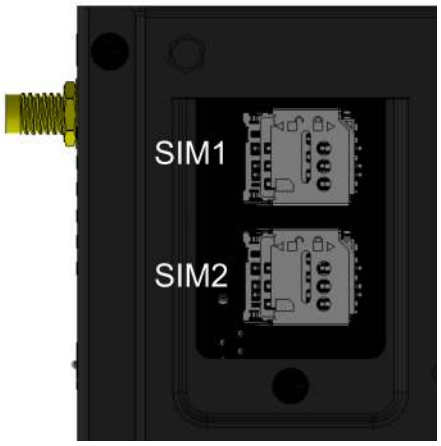
Fig. 2.10: Schema butoanelor HW

Operarea butonului HW

• Apăsați mai puțin de 2 secunde - Nu se întâmplă nimic
• Apăsați de la 2 la 7 secunde - Repornirea se efectuează la eliberarea butonului
• Apăsați de la 7 la 20 de secunde - Setările din fabrică sunt efectuate la eliberarea butonului
• Apăsați mai mult de 20 de secunde - Nu se întâmplă nimic

2.2.9. Cartele SIM

Două suporturi de cartelă SIM pentru Micro SIM (3FF) sunt disponibile sub capacul înșurubat de pe partea dreaptă a M!DGE3.



Avertizare

Deconectați unitatea M!DGE3 de la sursa de alimentare înainte de a deschide capacul și de a manipula cu cartelele SIM.

2.3. LED-uri de indicare

Indicatorul LED este plasat pe panoul frontal al M!DGE3.

Fig. 2.11: LED-uri de indicare

Tab. 2.6: Cheia LED-urilor

LED	Culoare	Stare	Funcţie
SYS	Verde	Aprins permanent	Sistem OK
		Clipire - perioada 500 ms	Apăsat butonul de resetare
		Trei clipiri rapide (50 ms) - pauză (500 ms)	Buton de resetare resetare din fabrică
		Clipește regulat - perioadă 2000 ms	Modul de repaus activat
	Roşu	Aprins permanent	Alarma
		Clipește regulat - perioadă 500 ms	Eroare gravă de sistem
	Portocale	Aprins permanent	Pornirea unității
		Trei clipiri rapide (75 ms).	Disc flash USB introdus
		Clipește rapid (75 ms) - perioadă 1000 ms	Interacțiune cu disc flash USB
	verde / Portocale	Clipește regulat - perioadă 300 ms	Activare FW - nu opriți dispozitivul
WAN	verde / Portocale / Roşu	Aprins permanent sau clipește la intervale de 1 secundă	Aprins permanent - conectat la rețeaua celulară. Culoarea semnalizează puterea semnalului Clipește - se conectează la rețeaua celulară.
EXT	Verde	Aprins permanent	Activitatea echipamentelor conectate mPCIe (cum ar fi GPS fix, LTE conectat, ...)
	Roşu	Aprins permanent	Alarma echipamentului conectat mPCIe
	Tabelul nivelurilor de semnal pentru serviciile individuale pentru interfața celulară		
	Tabelul activității GNSS		
VPN	Verde	Aprins permanent	Când toate serverele și clienții configurați sunt UP (ascultă sau conectate).
		Clipește regulat	Când cel puțin un server sau client este UP (ascultă sau conectat) și cel puțin un server sau client este DOWN (nu ascultă sau nu este conectat).
	Galben	Aprins permanent	Când toate serverele și toți clienții sunt INCHIS
	Nu aprins	-	Când nici serverul, nici clientul nu sunt setate.
COM	Verde	Aprins permanent	Primirea datelor
	Portocale	Aprins permanent	Transmiterea datelor

Alarma

O alarmă este declanșată de orice eveniment cu eroare de severitate sau mai mare (vezi *Secțiunea 8.4, „Evenimente”*).

2.4. Extensie

Routerul celular M!DGE3 poate fi livrat cu al doilea modul celular suplimentar (opțional), extensie GPS sau extensie COM. În cazul Cellular sau GPS vine cu doi conectori SMA suplimentari instalați pe panoul de jos (EXT1, EXT2). Activitatea oricărui modul de extensie este semnalizată pe panoul frontal al M!DGE3 (LED EXT).

Nota

Nu sunt disponibile extensii pentru versiunea M!DGE3e.

2.4.1. Celular

Se recomandă utilizarea ambelor antene (diversitate Rx) pentru conexiunea LTE. În cazul în care folosiți o singură antenă, atașați-o la conectorul EXT1. Conectorul EXT1 este folosit atât pentru transmisie, cât și pentru recepție sau pentru configurații cu o singură antenă. Conectorul EXT2 este special pentru diversitatea Rx.

Când 2nd este utilizat modulul celular, comportamentul LED-ului acestei extensii este semnalizat de LED-ul Verde / Portocaliu / Roșu

• Aprins permanent - Conectat la rețeaua celulară (intensitatea semnalului de semnalizare a culorii)

• Clipește la interval de 1 secundă - Se conectează la rețeaua celulară

2.4.2. Interfață WiFi

Routerul celular M!DGE3 poate fi livrat cu extensia Wi-Fi.

2.4.2.1. Antenă

Este posibil să utilizați una sau două antene. Configurarea antenei trebuie configurată corespunzător în parametrii de configurare a antenei EXT1 și EXT2 din meniul Setări > Interfețe > Wi-Fi.

2.4.3. GPS

Routerul celular M!DGE3 poate fi echipat cu receptor GPS cu iesire de impuls de timp. Conectorul EXT1 este utilizat pentru conectarea antenei GPS active, conectorul EXT2 este utilizat pentru ieșirea precisă a impulsului de timp.

2.4.4. COM2 - COM3

Al 2-lea și al 3-lea port COM sunt disponibile atunci când este instalat modulul de extensie „C” (2 x RS232). Într-un astfel de caz: conectorul DI/DO este utilizat ca conector pentru COM2 și COM3.

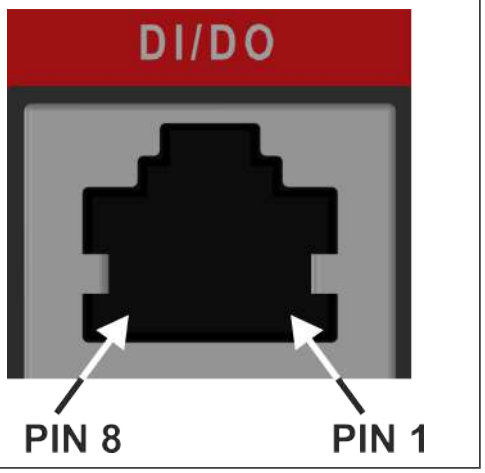
Parametri COM2 și COM3:

COM2: RS232 - 5 pini (RxD, TxD, GND, RTS, CTS) 600 b/s până la 2 Mb/s

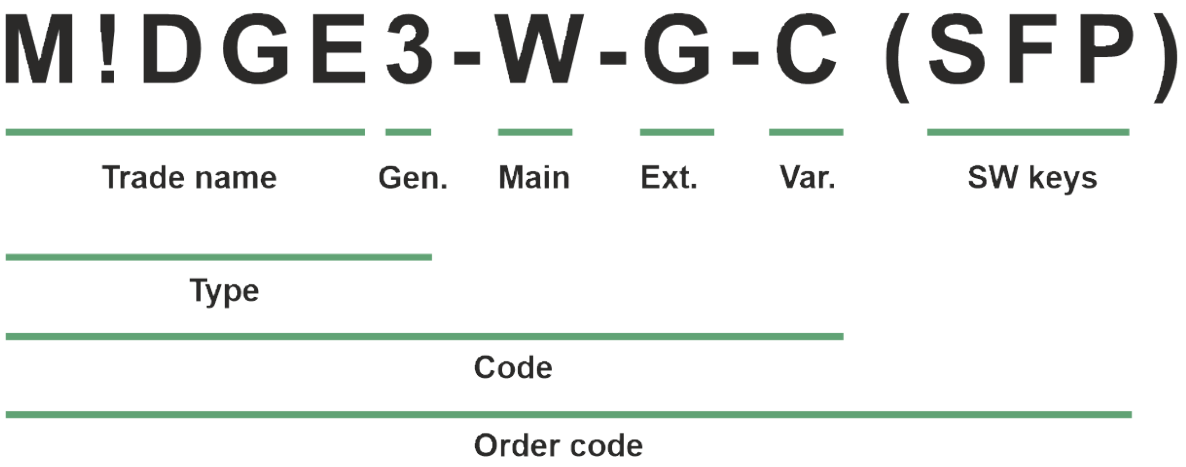
COM3: RS232 - 3 pini (RxD, TxD, GND) 2,4 kb/s până la 921,6 kb/s

Tab. 2.7: conector DI/DO utilizat de modulul de extensie „C”

Pin	Semnal	In / Out
1	RxD COM3	Afară
2	TxD COM3	În
3	GND	
4	CTS COM2	Afară
5	RTS COM2	În
6	GND	
7	RxD COM2	Afară
8	TxD COM2	În



2.5. Codurile de comandă



Nume comercial–denumirea comercială și comercială a produsului. Acest nume este folosit pentru toate produsele din aceeași familie de produse.

Valori posibile:**M!DGE**

Gen.–generarea produsului cu denumirea comercială specifică. Prima generație nu are niciun număr în această poziție.

Valori posibile:**3**

Principal

Valori posibile:
N–nefolosit
W–Modul celular principal; Nr. parte: mPCIe-W
Benzile W-4G/3G/2G, global

Ext.–Modul de extensie încorporat în slotul mPCIe
Valori posibile:
N–nefolosit
W–Extensie modul celular; Nr. parte: mPCIe-W
Benzile W-4G/3G/2G, global
M–Extensie modul celular; Nr. parte: mPCIe-M *Trupele M*–LTE Cat M1/NB1/NB2, global (inclusiv 450 MHz) **O**–Extensie modul celular; Nr. parte: mPCIe-O *Benzile O*–LTE Cat M1/NB1/NB2, global
G–Modul de extensie GPS (GNSS); Nr. parte: mPCIe-GPS **C**–Extensie 2× RS232; Nr. parte: mPCIe-COMS **F**–Modul de extensie Wi-Fi; Nr. parte: mPCIe-WIFI

Este posibilă o singură opțiune pentru slotul mPCIe.

Var.–Varianta hardware (nu este utilizată pentru M!DGE3)
Valori posibile:
C–M!DGE3e

Tastele SW–dacă unitatea este comandată cu chei SW, toate cheile sunt specificate în această paranteză. Cheia SW poate fi comandată independent pentru un anumit S/N oricând ulterior.
Valori posibile:
SFP–permite interfața SFP; Nr. piesa: M!DGE3-SW-SFP

Tip–tip specific de produs
Valori posibile:
M!DGE3

Cod–parte a codului de comandă care este imprimată pe eticheta produsului de pe carcasă (cheile SW nu depind de HW și pot fi comandate ulterior, deci nu sunt tipărite pe eticheta produsului).

Cod de comandă–codul complet al produsului, care este utilizat pe cotații, facturi, bonuri de livrare etc.

Pentru a afla codul de comandă corect, vă rugăm să utilizați*Magazin electronic*[2].

[2] https://webservice-new.racom.eu/main/eshop.list?t=10

3. Accesorii

Lista completă de accesorii este disponibilă pe *RACOM*[1] site-ul web.

1. Suport de margine

2. Suport plat

3. Adaptoare USB (ETH, WiFi) *https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb*

4. Caz demonstrativ
   https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_democase

[1] https://www.racom.eu/eng/products/cellular-router-midge.html#accessories

4. Instalare

4.1. Lista de verificare pas cu pas

1. Montați M!DGE3 în dulap (*Secțiunea 4.3, „Montarea”*).
2. Instalați antena (*Secțiunea 4.4, „Instalarea antenei”*).
3. Instalați linia de alimentare (*Secțiunea 4.5, „Linia de alimentare a antenei”*).
4. Asigurați-vă o împământare corespunzătoare (*Secțiunea 4.6, „Legătura la pământ”*).
5. Rulați cablurile și conectați toți conectorii, cu excepția echipamentului SCADA (*Secțiunea 2.2, „Conectori”*).
6. Aplicați sursa de alimentare la M!DGE3.
7. Conectați PC-ul de configurare (*Ripex2 „Conectare”*).
8. Configurați M!DGE3.
9. Testați calitatea conexiunii radio (de exemplu, folosind instrumentul de monitorizare).
10. Conectați echipamentul SCADA.
11. Testați aplicația.

4.2. Setări minime necesare pentru a configura conexiunea celulară

1. Introduceți codul PIN pentru cartela SIM anume, dacă este necesar (SETĂRI > Interfețe > Cellular > SIM1/SIM2).

2. Activați și configurați numele punctului de acces (APN) (SETĂRI > Interfețe > Cellular > MAIN/EXT > Activați și adăugați/editați profilul celular).

3. Adăugați ruta implicită 0.0.0.0/0 prin WWAN (MAIN sau EXT) (SETĂRI > Rutare > Static) sau altă regulă de rutare necesară.

   • Nicio rută nu este adăugată automat, rutele necesare trebuie adăugate manual.

   • Fără astfel de rute, unitatea va fi conectată la rețeaua celulară, dar nu va comunica cu niciun alt dispozitiv/IP.

4. Salvați modificările.

5. Verificați funcționalitatea

   • SETĂRI > Interfețe > Cellular > Stare > Afișați mai multe (<)

   • DIAGNOSTICĂ > Instrumente > ping ICMP

   • DIAGNOSTICĂ > Statistici > Tabele statistice celulare (Interfață, Stare, Semnal)

6. În cazul oricăror probleme, descărcați un pachet de diagnosticare detaliat (DIAGNOSTICS > Informații > Pachet de diagnosticare), includeți toate informațiile, cu excepția acreditărilor de utilizator și trimiteți-l la *support@racom.eu*[1].

[1] mailto: support@racom.eu

4.3. Montare

4.3.1. Montare pe șină DIN

Modemul celular M!DGE3 este montat direct pe șina DIN printr-un suport (care vine împreună cu modemul).

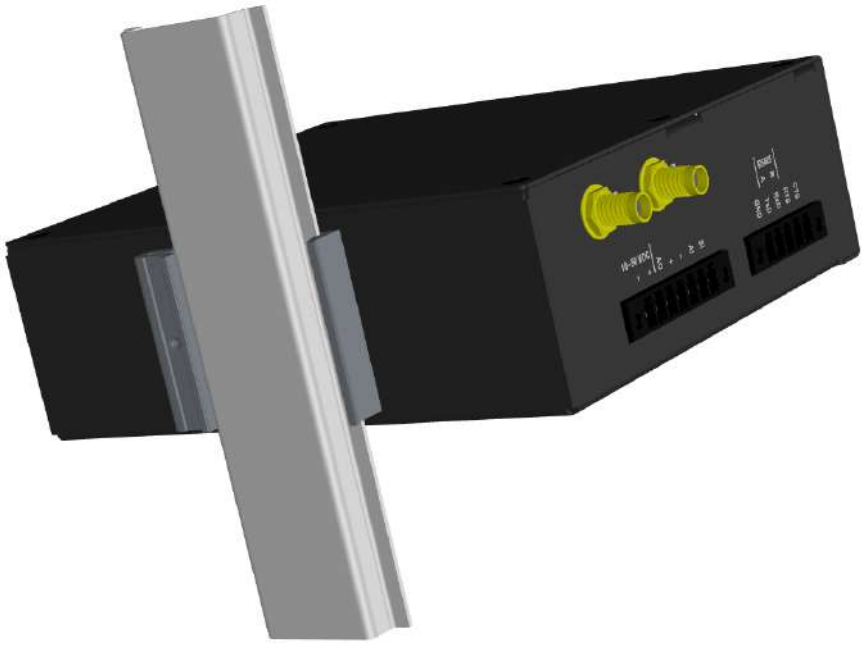


Fig. 4.1: șină DIN

Folosind acest suport M!DGE3 poate fi montat în diferite unghiuri (cu 90° în sensul acelor de ceasornic/în sens invers acelor de ceasornic).

Pentru montarea pe margine pe șina DIN, se folosește suportul de margine (accesoriu opțional). Utilizați numai șuruburile M4×5 mm care sunt furnizate.

Fig. 4.2: Montare cu muchii pe șina DIN

4.3.2. Montaj plat

Pentru montarea plată direct pe suport trebuie să utilizați suportul plat (un accesoriu opțional). Utilizați numai șuruburile M4×5 mm care sunt furnizate.

Fig. 4.3: Montare plat cu suport plat

4.4. Instalarea antenei

Tipul de antenă cel mai potrivit pentru site-urile individuale ale rețelei dvs. depinde de aspectul rețelei și de cerințele dumneavoastră pentru nivelul de semnal la fiecare site.

Antena nu trebuie instalată niciodată în apropierea unor potențiale surse de interferență, în special dispozitive electronice precum computere sau surse de alimentare comutatoare.

Recomandări suplimentare de siguranță

Numai personalul calificat cu autorizație de lucru la înălțime are dreptul să instaleze antene pe catarge, acoperișuri și pereți ai clădirilor. Nu instalați antena în apropierea liniilor electrice. Antena și suporturile nu trebuie să intre în contact cu cablurile electrice în niciun moment.

Antena și cablurile sunt conductori electrici. În timpul instalării, se pot acumula încărcări electrostatice care pot duce la vătămări. În timpul lucrărilor de instalare sau reparare, toate piesele metalice deschise trebuie să fie temporar împământate.

Antena și linia de alimentare a antenei trebuie să fie împământate în orice moment.

Nu montați antena în condiții de vânt sau ploaie sau în timpul unei furtuni sau dacă zona este acoperită cu zăpadă sau gheață. Nu atingeți antena, suporturile antenei sau conductorii în timpul unei furtuni.

4.5. Linie de alimentare a antenei

Linia de alimentare a antenei trebuie aleasă astfel încât atenuarea sa să nu depășească 3 până la 6 dB, ca regulă generală. Utilizați numai cabluri de impedanță de 50 Ω.

Cu cât linia de alimentare este mai scurtă, cu atât mai bine. Dacă M!DGE3 este instalat aproape de antenă, cablul de date poate fi înlocuit cu un cablu Ethernet pentru alte protocoale care utilizează portul serial, vezi *Secțiunea 7.1.3, „Servere terminale”*.

Respectați întotdeauna recomandările de instalare furnizate de producătorul cablului (raza de îndoire etc.). Folosiți conectori corespunzători și instalați-i cu grijă. Conectorii atașați prost cresc interferența și pot cauza instabilitate legăturii.

4.6. Împământare

Pentru a minimiza șansele ca transceiver-ul și echipamentul conectat să primească orice deteriorare, ar trebui utilizată o masă de siguranță (conform NEC Clasa 2), care leagă sistemul de antenă, transceiver-ul, sursa de alimentare și echipamentul de date conectat la o masă într-un singur punct, menținând cablurile de împământare scurte.

Routerul celular M!DGE3 este, în general, considerat împământat corespunzător dacă suporturile de montare plate furnizate sunt utilizate pentru a monta routerul celular pe o suprafață metalică împământată corespunzător. Dacă routerul celular nu este montat pe o suprafață cu împământare, ar trebui să atașați un fir de împământare de siguranță la unul dintre suporturile de montare sau un șurub pe carcasa routerului celular.

Dacă antena este instalată în afara clădirii, se recomandă insistent să instalați un sistem adecvat de protecție împotriva trăsnetului acolo unde cablul antenei intră în clădire.

Nota

Toate cablurile, împământarea și protecția la trăsnet trebuie să respecte standardele și reglementările aplicabile.

4.7. Conectori

M!DGE3 utilizează conectori standard. Utilizați numai omologi standard la acești conectori.

Veți găsi pin-out-urile conectorilor în *Secțiunea 2.2, „Conectori”*.

4.8. Alimentare electrică

Nu recomandăm pornirea sursei de alimentare a unității M!DGE3 înainte de a conecta antena și alte dispozitive. Conectarea RTU și a altor dispozitive la M!DGE3 în timp ce este alimentat crește probabilitatea de deteriorare din cauza descărcării diferenței de potențial electric.

M!DGE3 poate fi alimentat de la orice sursă de alimentare bine filtrată de la 10 la 50 VDC. Pentru a evita interferența canalului radio, sursa de alimentare trebuie să îndeplinească toate standardele EMC relevante. Nu instalați niciodată o sursă de alimentare aproape de antenă. Conectorul (- pini) este conectat intern la carcasa unității M!DGE3.

5. M!DGE3 în detaliu

5.1. Combinație de comunicații IP și seriale

M!DGE3 permite combinarea protocoalelor IP și seriale într-o singură aplicație.

Cinci servere terminale independente sunt disponibile în M!DGE3. Serverul terminal este un înlocuitor virtual pentru dispozitivele utilizate ca convertoare serial la TCP (UDP). Acesta încapsulează protocolul serial la TCP(UDP) și invers, eliminând transferul de**TCP overhead**.

Dacă structura de date a unui pachet este identică pentru IP și protocoalele seriale, serverul terminal poate servi ca convertor între TCP(UDP)/IP și protocoalele seriale (RS232, RS485).

5.1.1. Descriere detaliată

În general, un server Terminal (denumit și server serial) permite conectarea dispozitivelor cu o interfață serială la un M!DGE3 prin rețeaua locală (LAN). Este un înlocuitor virtual pentru dispozitivele utilizate ca convertoare serial-to-TCP(UDP).

Exemple de utilizare:

O aplicație SCADA din centru ar trebui să fie conectată la rețea prin interfață serială, totuși, din anumite motive, această interfață serială nu este utilizată. Sistemul de operare (de exemplu Windows) poate furniza o interfață serială virtuală unei astfel de aplicații și convertește datele seriale în datagrame TCP (UDP), care sunt apoi primite de serverul terminal în M!DGE3. Acest tip de conexiune între M!DGE3 SCADA și aplicație este benefic în următoarele circumstanțe:

- Nu există nicio interfață serială hardware pe computer
- Cablul serial între M!DGE3 și computer ar fi prea lung. De exemplu, M!DGE3 este instalat foarte aproape de antenă pentru a reduce pierderea liniei de alimentare.
- LAN există deja între computer și punctul de instalare

În cazuri speciale, serverul Terminal poate reduce încărcarea rețelei din aplicațiile TCP. O sesiune TCP poate fi terminată local la serverul Terminal din M!DGE3. Datele utilizatorului sunt extrase din mesajele TCP și procesate ca și cum ar proveni dintr-un port COM. Când datele ajung la destinația M!DGE3, pot fi transferate la RTU fie prin interfața serială, fie prin TCP (UDP), folosind din nou serverul Terminal. Vă rugăm să rețineți că implementarea serverului terminal M!DGE3 acceptă, de asemenea, modificarea dinamică a portului IP în fiecare datagramă de aplicație primită. Într-un astfel de caz, M!DGE3 trimite răspunsul către portul de la care a fost primit ultimul răspuns. Această caracteristică permite extinderea numărului de conexiuni TCP deschise simultan între M!DGE3 și aplicația conectată local până la 10 pe fiecare server Terminal.

6. Interfață web

M!DGE3 poate fi gestionat cu ușurință de pe computer folosind un browser web. Dacă există o conexiune IP între computer și respectivul M!DGE3, puteți pur și simplu să introduceți adresa IP a oricărui M!DGE3 din rețea direct în linia de adresă a browserului și să vă conectați. Cu toate acestea, nu este recomandat să gestionați un M!DGE3 conectat prin aer, deoarece ar trebui transferate cantități mari de date pe canalul celular.

Când trebuie să gestionați un M!DGE3 conectat prin aer (recomandat), conectați-vă la un M!DGE3, la care computerul dvs. este conectat folosind fie un cablu (prin LAN), fie un WAN de mare viteză. M!DGE3 la care sunteți autentificat în acest fel se numește Local. Apoi puteți gestiona orice M!DGE3 la distanță din rețea prin aer, într-un mod care economisește debitul: toate datele statice (de exemplu, obiectele grafice ale paginii Web) sunt descărcate din M!DGE3 Local și numai informațiile specifice unității la distanță sunt transferate pe canalul celular. M!DGE3 accesat în acest fel se numește Remote.

De asemenea, vă puteți conecta la o unitate RipEX2 la rețelele hibride în același mod.

Din motive de securitate, numai protocolul HTTPS este utilizat pentru conexiunea dintre browserul web și unitatea M!DGE3. Dacă http://... este folosit în linia de adresă a browserului web, comunicarea este imediat redirecționată automat către protocolul HTTPS.

Pentru o mai bună protecție împotriva accesului neautorizat la rețea, există un timer construit în unitatea M!DGE3 și interfața web (setat la 24 de ore în mod implicit), care monitorizează activitatea utilizatorului. În cazul inactivității utilizatorului, conexiunea dintre interfața web și unitate va fi întreruptă (adică deconectare automată). Cronometrul este lansat automat în paralel atât în unitate, cât și în browserul web. În cazul modificării setării temporizatorului, vă recomandăm să vă deconectați și să vă autentificați, astfel încât să se poată produce inițializarea corectă a inactivității timeout-ului.

Pagina de conectare

Nota
Interfața web pentru M!DGE3 este identică cu RipEX2.

Pagina de conectare vă informează despre numele unității și adresa IP a unității M!DGE3 la care încercați să vă conectați.
Pagina de autentificare permite vizualizarea și copierea parolei.
Pagina de autentificare permite schimbarea limbii întregii interfețe web (limba engleză este implicită).
Interfața web este concepută pentru utilizare pe toate tipurile de echipamente - cu diferite dimensiuni și rezoluții ale ecranului. Majoritatea imaginilor prezentate în acest manual de utilizare sunt realizate pe tipul de rezoluție a ecranului desktop.

Nota
Este implementat un mecanism împotriva atacului cu forță brută. Când este introdusă o combinație greșită a Contului/Parola, trebuie să așteptați un timp pentru următoarea încercare. Timpul crește cu fiecare încercare greșită.

Antetul paginii web

Antetul fiecărei pagini web conține:

• Numele unității

• Adresa IP a unității M!DGE3 la care sunteți conectat

• Buton de acces la distanță

• Identificarea paginii web curente (2ndsau 3rdnivelul meniului)

• Modificări la butonul de comitere

• Butonul Notificări

• Butonul de reîmprospătare a setărilor

• Butonul meniu utilizator

6.1. Browsere web acceptate

Browserele web acceptate pentru desktop sunt versiunile actuale ale:

• Marginea

• Chrome

• Firefox

• Safari

Browserele Web acceptate pentru echipamentele mobile sunt versiunile actuale ale:

• Safari pentru iOS

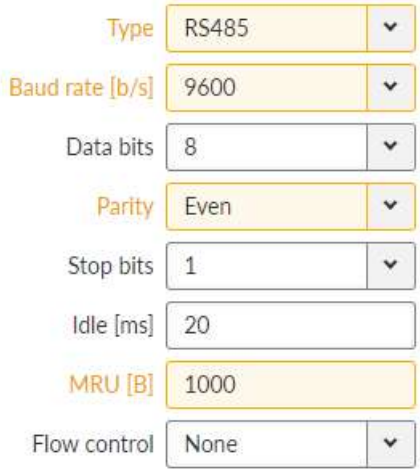
• Chrome pentru Android

Nota

Din motive de siguranță, se recomandă utilizarea unui browser web fără extensii (în special extensii, care ar putea avea acces la date).

6.2. Modificări de comis

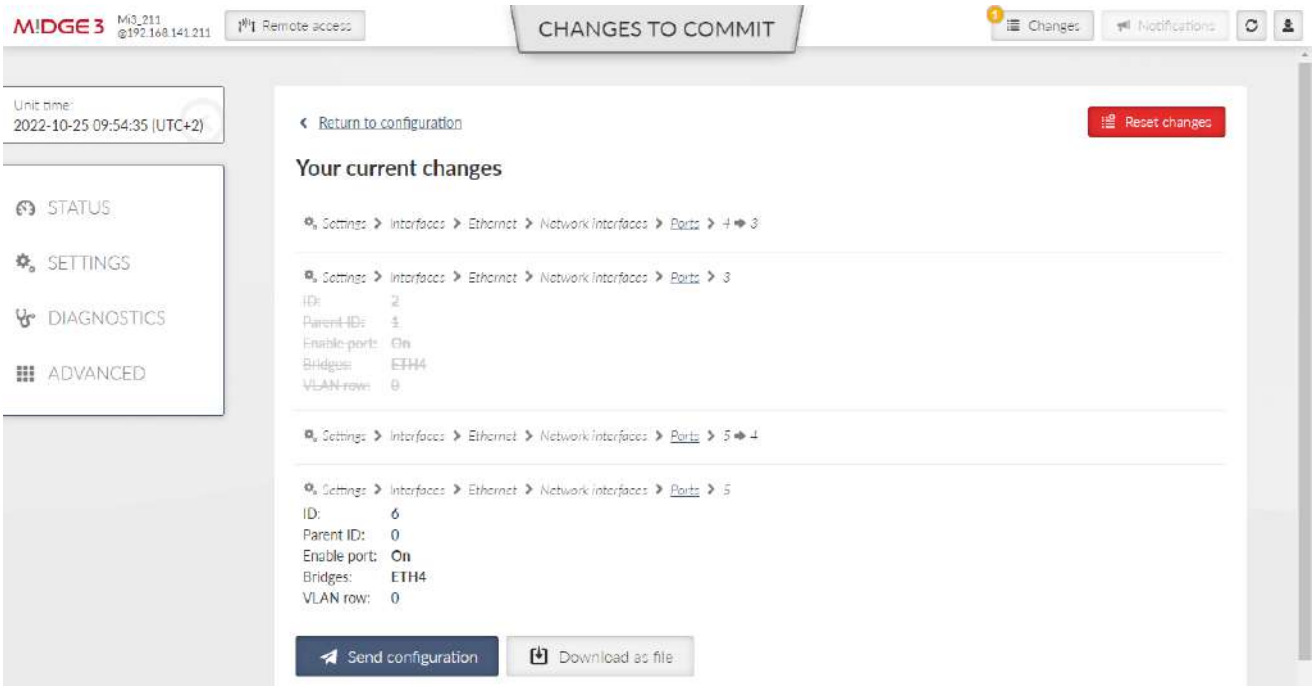
M!DGE3 este capabil să rețină modificările, care au fost făcute în configurația sa și să le colecteze într-un „coș” de modificări. Toate modificările parametrilor de configurare sunt evidențiate cu o culoare diferită.



Pentru a accesa „Coșul de modificări pentru comite”, faceți clic pe butonul Modificări (colțul din dreapta sus în antetul paginii Web) sau utilizați comanda rapidă „Ctrl+Alt+C”.

Modificările aduse „coșului” de comitere colectează toate setările modificate, care:

- Sunt separate în meniu alfabetic. Separarea alfabetică este sortată ierarhic în funcție de numele elementelor din meniu.
- Sunt afișate în meniu (inclusiv calea plasării lor) și sunt prevăzute cu un link pentru un transfer rapid la plasarea inițială.
- Transportați informații despre valorile lor modificate („Valoare veche” → „Valoare nouă”).

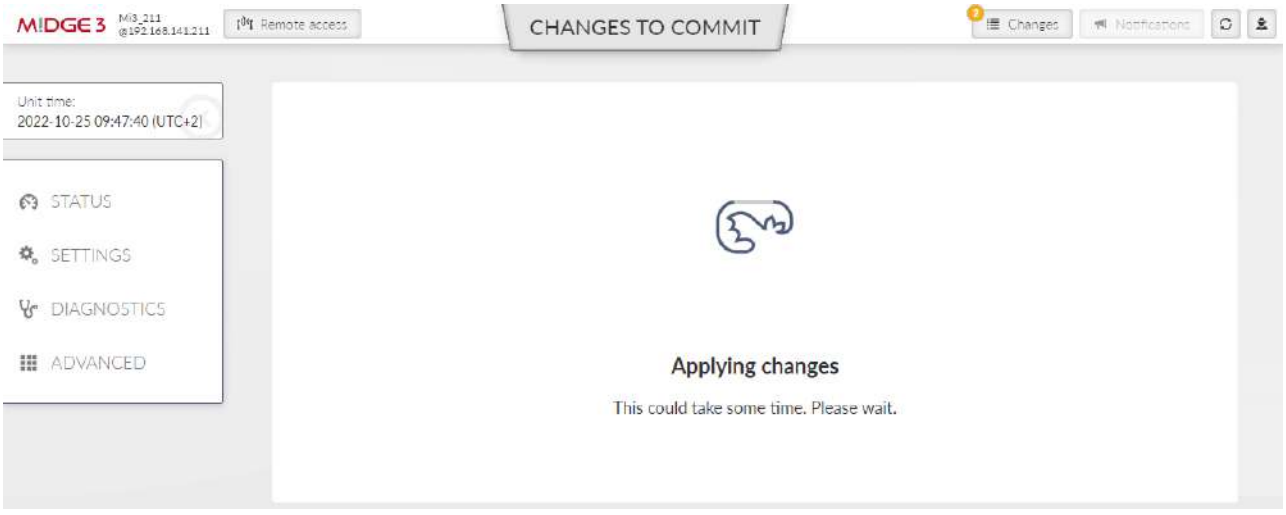


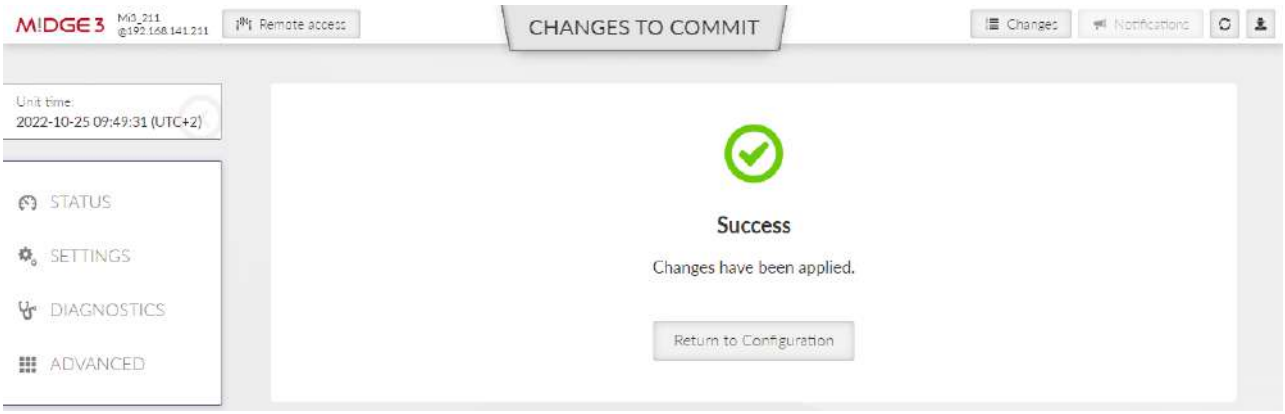
Din această pagină, este posibil să:

• Revenire la configurare - revenirea la meniul de configurare al ultimei valori modificate.

• Resetare modificări - toate modificările vor fi resetate la valoarea setată anterior (nu implicit).

• Trimiteți configurația - Aplicați (Salvați în unitate) toate modificările.





6.3. Notificări

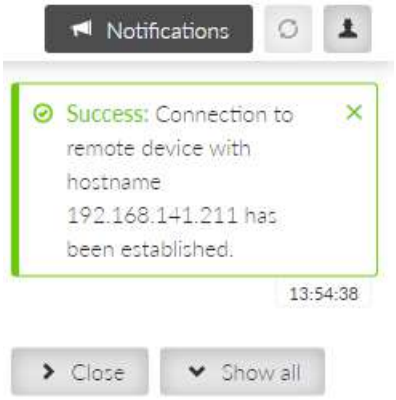
Cu M!DGE3 este introdus un nou mod de a arăta utilizatorului evenimentele importante ale sistemului. Se numește Centru de notificare și este utilizat în mod constant în întreaga interfață. Centrul de notificare este situat în colțul din dreapta sus al interfeței. Există în două forme: afișare activă a notificărilor și Centru de notificare complet. Atât afișajul de notificare activ, cât și Centrul de notificare complet sunt afișate fie sub antetul de sus al interfeței, fie în bara laterală din dreapta, în funcție de dimensiunea afișajului utilizatorului. Comportamentul este receptiv, astfel încât în cazul în care utilizatorul trebuie să îngusteze fereastra browserului, centrul de notificare își schimbă automat locul pentru a utiliza cea mai eficientă locație.

Nota

Pentru a accesa Centrul de notificări este posibil să utilizați comanda rapidă „Ctrl+Alt+N”.

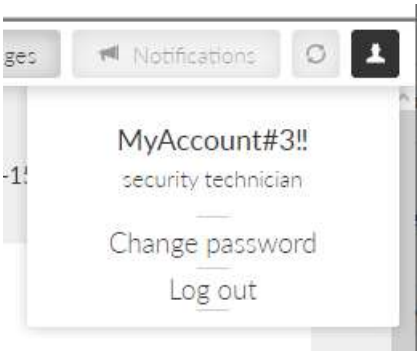
Notificările sunt declanșate în mare parte de acțiunile utilizatorului în interfață, de exemplu succesul sau eșecul conexiunii Fast Remote Access. Ele nu trebuie confundate cu Evenimente, care sunt declanșate în principal de sistem și nu sunt afișate în Centrul de notificări, ci pe pagina Diagnosticare > Evenimente. Cu alte cuvinte, notificările sunt cauzate de utilizator, evenimentele sunt cauzate de schimbarea stării unității.

Fiecare notificare nouă este afișată în sertarul Centrului de notificări. Utilizatorul poate fie să respingă notificarea făcând clic pe cruce din corpul notificării, să închidă toate notificările afișate în sertar sau să extindă complet Centrul de notificări folosind butoanele („Închideți tot” și „Afișați tot”) din partea dreaptă a sertarului Centrului de notificări.



Centrul de notificări colectează toate notificările care nu au fost respinse și le permite utilizatorilor să le răsfoiască.

6.4. Meniul utilizatorului



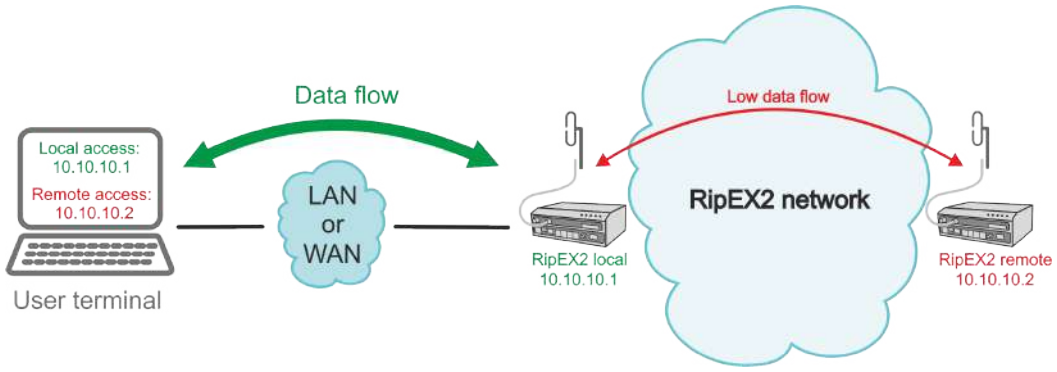
Este recomandat să schimbați parola implicită.

6.5. Acces de la distanță

Managementul unității M!DGE3 este proiectat să funcționeze fără probleme chiar și atunci când unitatea aflată în configurație este conectată printr-un canal relativ lent. În cazul unității conectate local - configurarea directă a unității (accesarea adresei IP a unității direct din browserul web) funcționează bine. Dacă unitatea ar trebui să fie conectată de la distanță prin intermediul rețelei, așa-numitul „Acces la distanță” trebuie utilizat pentru a configura și gestiona unitatea la distanță utilizând volume de date transmise prietenoase cu lățimea de bandă. Deschideți browserul web, introduceți adresa IP a unei unități conectate local și conectați-vă la o unitate la distanță (care trebuie să fie accesibilă de la unitatea conectată local prin intermediul rețelei).

Nota

Pentru a accesa accesul de la distanță este posibil să utilizați comanda rapidă „Ctrl+Alt+R”.



M!DGE3 localunitatea trebuie să aibă cea mai nouă versiune de firmware din întreaga rețea pentru a asigura funcționalitatea adecvată de acces la distanță. Cu toate acestea, se recomandă să păstrați aceeași versiune de firmware în întreaga rețea. Vezi detalii in capitol*Secțiunea 7.6.5, „Firmware”*

Accesul la distanță poate fi activat făcând clic pe butonul Conectare acces.

Odată ce accesul de la distanță are succes, linia adresei IP își schimbă culoarea în negru împreună cu identificarea paginii web.

Adresa IP a unității M!DGE3 conectată în prezent este afișată ca parte a butonului de acces la distanță. Toate setările de configurare sunt disponibile de la distanță folosind interfața web standard. Unele dintre funcțiile de diagnosticare sunt disponibile numai prin conexiune locală.

Conexiunea de acces la distanță poate fi stabilită direct prin introducerea adresei IP a unității de la distanță ca parametru suplimentar în adresa URL. Formatul necesar este:
https://LOCAL_UNIT_IP_ADDRESS?remoteAccessTarget=REMOTE_UNIT_IP_ADDRESS

de exemplu: https://192.168.141.210?remoteAccessTarget=10.10.10.212

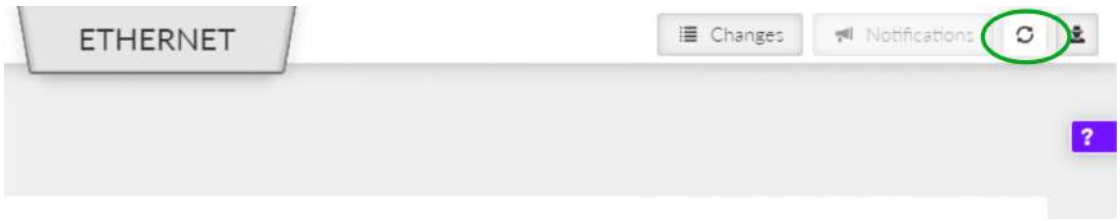
Nota

Este posibil să utilizați acest format URL pentru a crea marcajul unui browser web. Astfel de marcaje pot fi folosite pentru un acces mai rapid la unitățile de la distanță.

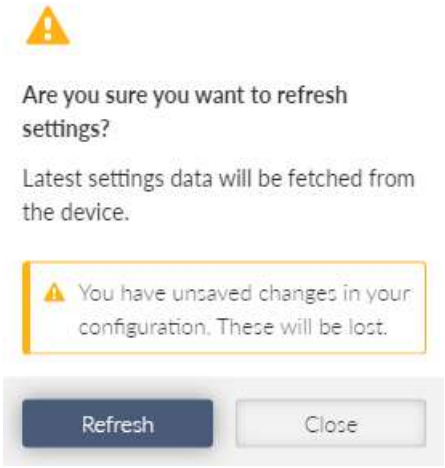
În mod implicit, accesul de la distanță utilizează**RO_Rmt_Access_Host_Key**pentru stabilirea conexiunilor la unități la distanță. Cu toate acestea, în scopuri de securitate îmbunătățită, vă recomandăm cu tărie utilizarea unui personalizat**Cheia RMTACCESS**(meniul SETĂRI > Securitate > Acreditări).

6.6. Actualizează setările

Butonul de reîmprospătare a setărilor (plasat în colțul din dreapta al antetului paginii web) declanșează o funcție care asigură utilizatorul că lucrează cu datele curente.



Declanșarea reîmprospătării va încărca datele curente de la unitate pe clientul web.



Nota

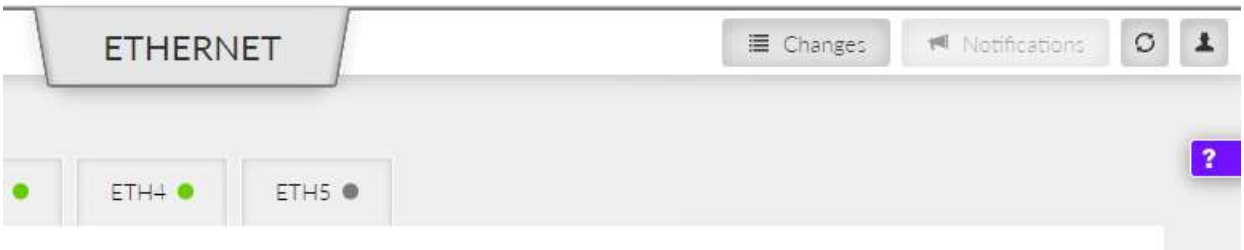
Actualizează șterge toate modificările nesalvate care au fost făcute în client.

6.7. Zona de informații despre stare

Zona de informații despre stare oferă o prezentare generală a secțiunii individuale de SETĂRI (sau DIAGNOSTICĂ) a M!DGE3 prin afișarea datelor de diagnosticare relevante pentru secțiune. Pentru a actualiza datele este necesar să faceți clic pe butonul Reîmprospătare. De asemenea, este posibil să utilizați funcția de reîmprospătare automată (butonul Start auto reîmprospătare), care declanșează automat reîmprospătarea după o perioadă de timp definită (3, 4, 5... 300 de secunde).

6.8. Ajutor

Această caracteristică este disponibilă pe paginile web individuale ale interfeței grafice cu utilizatorul făcând clic pe caseta violet cu semnul întrebării în colțul din dreapta sus (sau în mijlocul) ecranului (în funcție de lățimea ecranului).



Conținutul ajutorului este identic cu sub-capitolul respectiv al manualului de utilizare.

6.9. Comenzi rapide

Tab. 6.1: Tabel de comenzi rapide

Comandă rapidă	Acces la
Ctrl+Alt+C	Modificări de comis
Ctrl+Alt+N	Centru de notificare
Ctrl+Alt+R	Acces de la distanță

7. Setări

Informațiile furnizate în acest capitol sunt identice cu conținutul Ajutoare pentru meniul individual. care vor fi adăugate treptat pe toate ecranele.

7.1. Interfețe

7.1.1. Ethernet

M!DGE3 oferă 5 porturi Ethernet fizice ETH1, ETH2, ETH3, ETH4 și ETH5. Porturile ETH1 - ETH4 sunt metalice. Portul ETH5 este un port SFP. Există posibilitatea de a defini o punte Ethernet - o interfață logică de rețea - prin unirea (unirea) mai multor interfețe Ethernet fizice. Toate interfețele conectate împreună împărtășesc același trafic.

7.1.1.1. Interfețe de rețea

Interfața de rețea (din punct de vedere tehnic - o punte Ethernet) este identificată printr-un nume. Numele începe întotdeauna cu un prefix „LAN-”. Pot fi definite mai multe interfețe de rețea. Mai multe interfețe Ethernet fizice pot fi conectate împreună prin utilizarea unei singure interfețe de rețea.

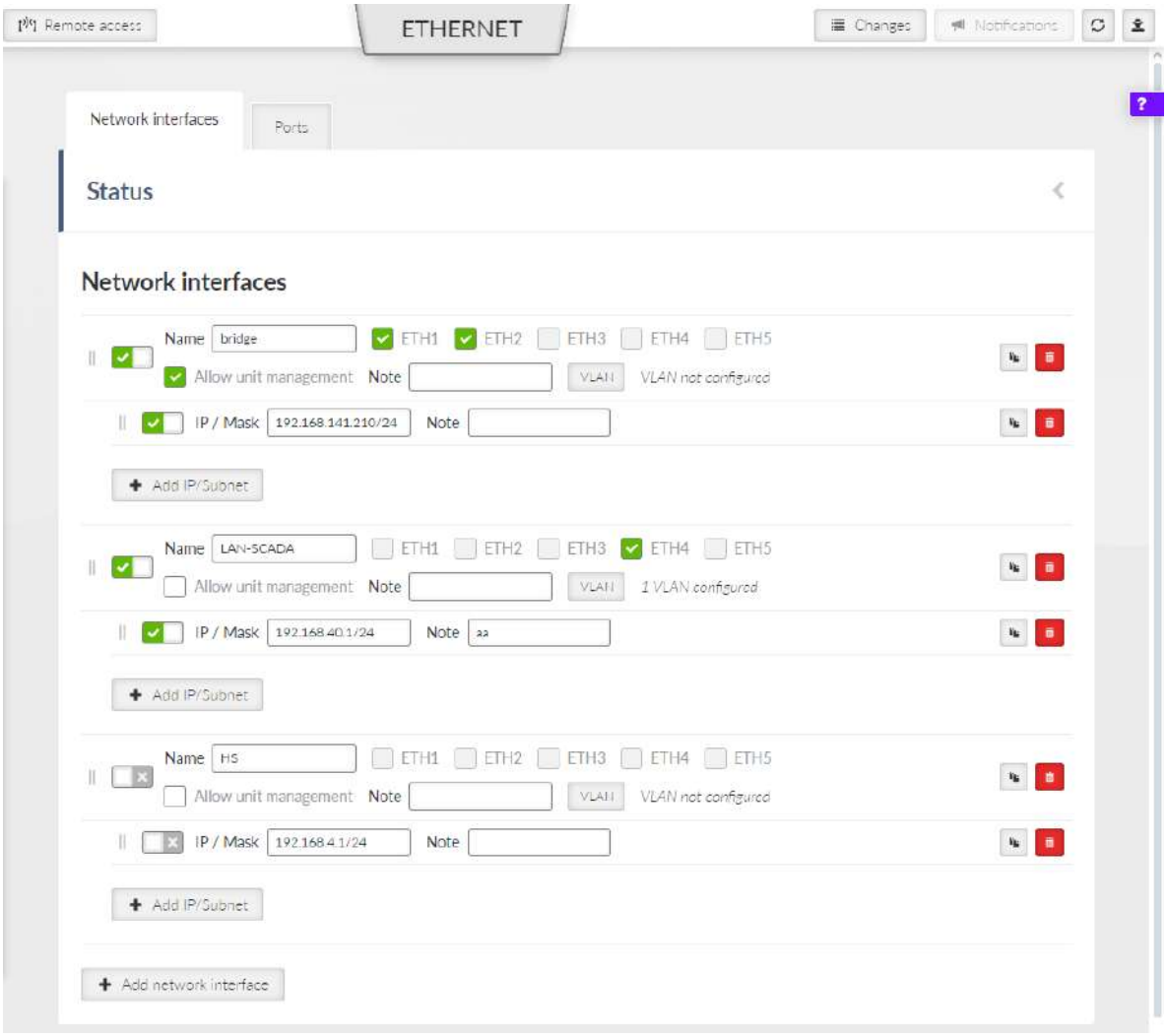


Fig. 7.1: SETĂRI > Interfață > Ethernet > Interfețe de rețea

Setarea implicită a unității celulare unește toate porturile Ethernet împreună. Pot fi definite noi interfețe de rețea pentru a împărți traficul Ethernet al porturilor individuale. Orice port Ethernet poate fi detașat dintr-o interfață de rețea existentă și adăugat la o altă interfață de rețea.

Subrețele Ethernet simple sau multiple pot fi definite într-o interfață de rețea. Fiecare subrețea este identificată prin IP/masca sa. Utilizați parametrul opțional Notă pentru a vă menține configurația rețelei într-un mod ușor de citit.

Activați / Dezactivați
Activează/dezactivează interfața de rețea.

Nume
Numele obligatoriu al interfeței de rețea.

ETH1 - ETH5
Interval pe porturile Ethernet selectate în interfața de rețea specifică.

Nota
Dacă interfața de rețea a configurat fie o interfață radio, fie un tunel GRE L2, nu necesită porturi ETH.

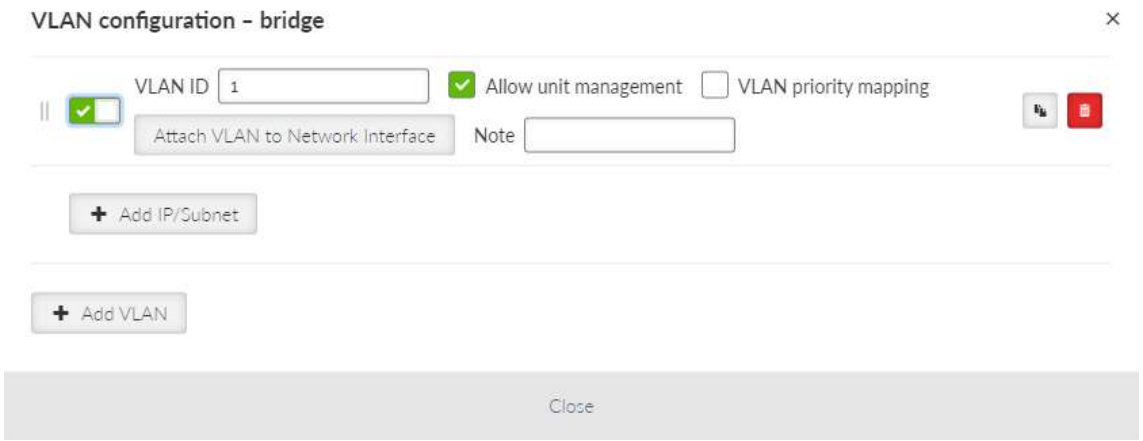
Permite gestionarea unității
Activează/dezactivează gestionarea unității pentru interfața de rețea specifică.

Adăugați IP/Subrețea
Adaugă o subrețea definită la interfața de rețea.

IP/Mască
IP/masca subrețelei Ethernet specifice (în notație CIDR). Adresa IP reprezintă interfața de rețea în rețeaua Ethernet Layer 3.

Nota
Comentariu optional.

VLAN
Fiecare interfață de rețea poate avea unul sau mai multe VLAN-uri atașate cu una sau mai multe subrețele.



Activați / Dezactivați
Activează/dezactivează VLAN.

ID VLAN

Număr {0 – 4094}, implicit = 1

Specifică ID-ul VLAN în conformitate cu IEEE 802.1Q

Permite gestionarea unității

Permite / interzice gestionarea unității pentru VLAN-ul specific. Acest comutator nu este conectat la comutatorul de interfață de rețea cu același nume, așa că numai acest VLAN poate fi utilizat pentru diagnosticare.

Maparea priorității VLAN

Se referă la QoS

Atașați VLAN la interfața de rețea

Atașează VLAN la interfața de rețea definită

Nota

Comentariu optional.

Adăugați IP/Subrețea

Adaugă o subrețea definită la VLAN.

7.1.1.2. Porturi

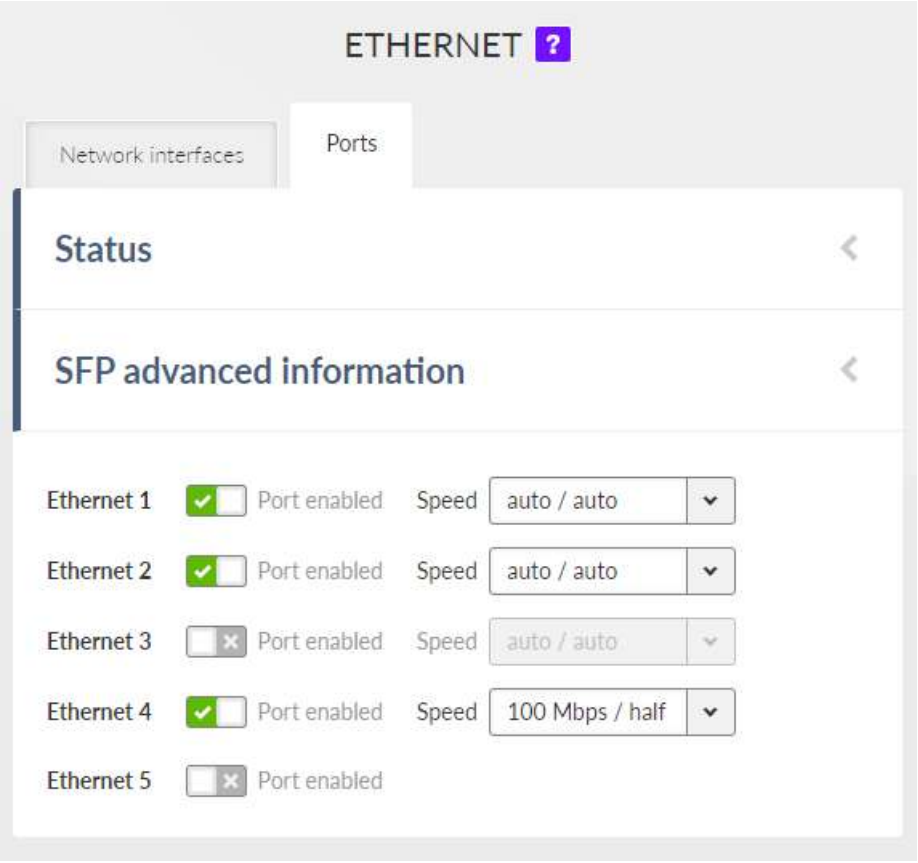


Fig. 7.2: SETĂRI > Interfață > Ethernet > Porturi

Activați / Dezactivați

Activează / dezactivează porturile ETH (1 - 5) control SW.

Viteza ETH1 - ETH4

Caseta listă {auto / auto; automat / complet; auto / jumătate; 1000 Mbps / automat; 1000 Mbps / complet; 1000 Mbps / jumătate; 100 Mbps / automat; 100 Mbps / complet; 100 Mbps / jumătate; 10 Mbps / automat; 10 Mbps / complet; 100 Mbps/jumătate}, implicit = „auto/auto”

Definește viteza și traficul half/full duplex.

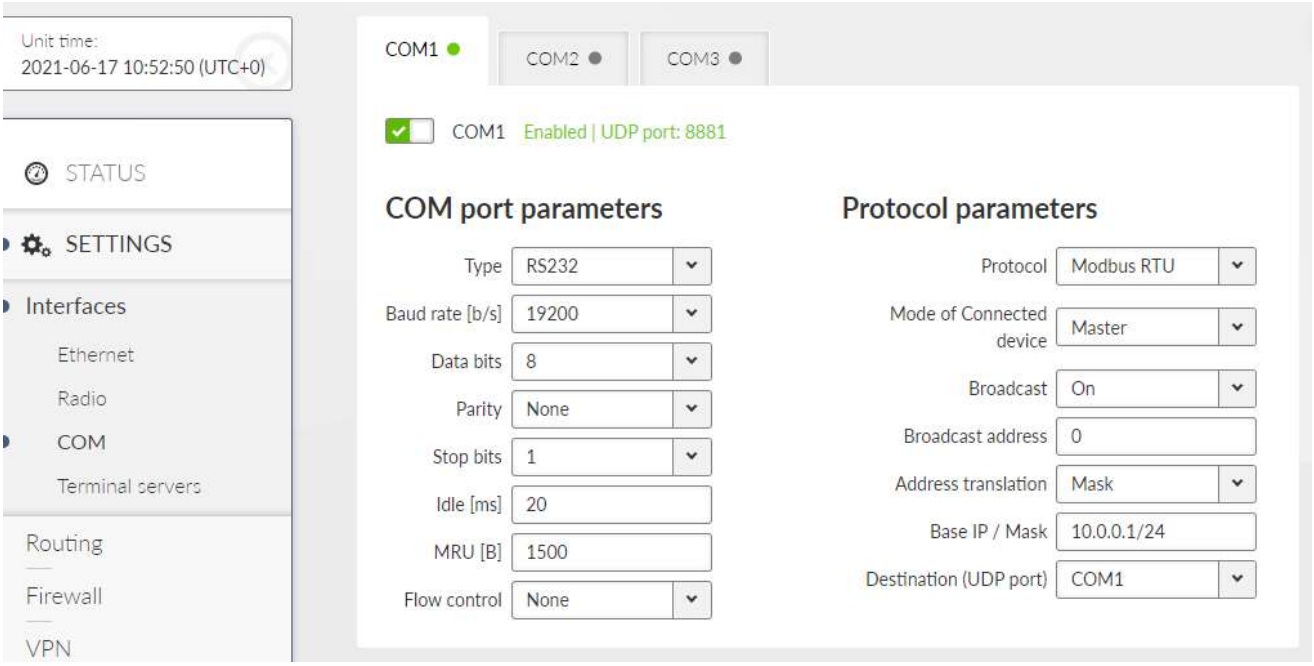
Nota

Atunci când mai multe punți sunt interconectate în rețea, este adecvat să porniți Protocolul Spanning Tree (AVANSAT > Interfețe > Ethernet > STP) pentru a preveni buclele de punte și pentru a construi o topologie logică fără bucle.

7.1.2. COM

Datele care intră în unitatea M!DGE3 de la portul COM sunt primite de modulul Protocol. Comportamentul modulului Protocol depinde de protocolul selectat. cadrul de intrare din portul COM este procesat de modulul Protocol, tradus în cadru UDP, redirecționat către modulul router M!DGE3 și procesat în continuare conform regulilor routerului. Astfel de cadre UDP primite de unitatea M!DGE3 din rețeaua M!DGE3 (pe baza adresei IP a unității și a portului UDP al modulului Protocol) sunt traduse în formatul de cadru original (de către modulul Protocol) și trimise prin portul COM.

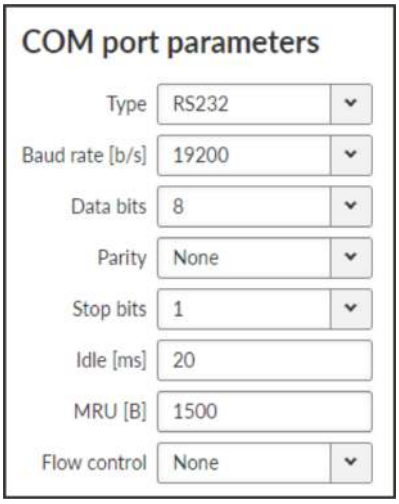
Când este instalat modulul de extensie „C”, sunt disponibile două porturi COM suplimentare (RS232). Setarea lor este similară cu portul COM1.



Meniul este împărțit în două părți:

7.1.2.1. Parametrii portului COM

Aceste setări de viteză de transmisie, biți de date, paritate și biți de oprire ai portului COM și setările dispozitivului conectat trebuie să se potrivească.



Tip

Caseta listă {valori posibile}, implicit = „RS232”
Portul COM poate fi configurat fie la RS232, fie la RS485.

Rata de transmisie [b/s]

Casetă listă {serie standard de rate de la 600 la 1152000 b/s}, implicit = „19200” Selectați Viteza de transmisie din caseta listă: sunt disponibile rate de la 600 la 1152000 b/s.
Porturile seriale folosesc semnalizare pe două niveluri (binară), astfel încât rata de date în biți pe secundă este egală cu rata simbolului în baud.

Biți de date

Caseta listă {5; 6; 7; 8}, implicit = 8, numai pentru COM3 (opțional) 8
Numărul de biți de date din fiecare caracter.

Paritate

Caseta listă: {Niciuna; Ciudat; Even}, implicit = „Niciunul”
Wikipedia: Paritatea este o metodă de detectare a erorilor de transmisie. Când paritatea este utilizată cu un port serial, un bit de date suplimentar este trimis cu fiecare caracter de date, aranjat astfel încât numărul de 1 biți din fiecare caracter, inclusiv bitul de paritate, să fie întotdeauna impar sau întotdeauna par. Dacă un octet este primit cu un număr greșit de 1 biți, atunci trebuie să fi fost corupt. Cu toate acestea, un număr par de erori poate trece de verificarea parității.

Opriți biți

Caseta listă {1; 2 (1.5)}, implicit = 1, pentru COM3 (opțional) doar 1, pentru 5 biți de date se utilizează 1,5 lungime a biților de oprire în loc de 2
Wikipedia: Biții de oprire trimiși la sfârșitul fiecărui caracter permit hardware-ului semnalului de recepție să detecteze sfârșitul unui caracter și să se resincronizeze cu fluxul de caractere.

Inactiv [ms]

Numărul {10 – 16383}, implicit = 20
Acest parametru definește intervalul maxim (în milisecunde) în fluxul de date primit. Dacă decalajul depășește valoarea setată, legătura este considerată inactivă, cadrul primit este închis și redirecționat către rețea.

MRU [B]

Număr {1 – 2047}, implicit = 1500
MRU (Unitate de recepție maximă) — un cadru de intrare este închis la această dimensiune chiar dacă fluxul de octeți continuă. În consecință, un flux de date permanent care vine la un COM are ca rezultat o secvență de cadre de dimensiunea MRU trimise prin rețea.

Nota
2. Acest MRU și MTU în setările celulare sunt independente, totuși MTU ar trebui să fie mai mare sau egal cu MRU.

Controlul fluxului

Caseta listă {Niciuna; RTS/CTS}, implicit = „Niciunul”
Controlul fluxului hardware RTS/CTS (Request To Send / Clear To Send) (strângere de mână) între DTE (Data Terminal Equipment) și M!DGE3 (DCE - Data Communications Equipment) poate fi activat pentru a întrerupe și a relua transmiterea datelor. Dacă tamponul RX al M!DGE3 este plin, CTS se stinge.

Nota
Controlul fluxului RTS/CTS necesită o conexiune cu 5 fire la portul COM.

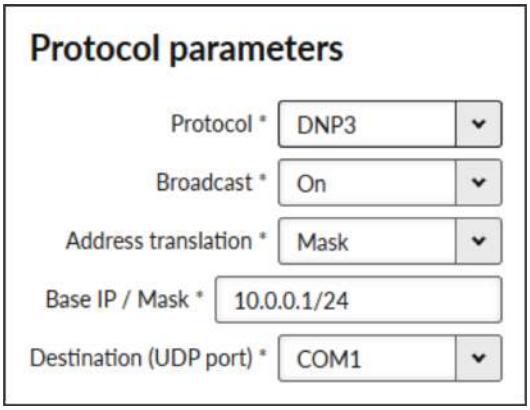
Timp de spălare a tamponului [ms]

Număr {0 – 65535}, implicit = 0

Acest parametru poate fi utilizat pentru a preveni blocarea nedorită a comunicației seriale. Temporizatorul este resetat de fiecare pachet primit sau transmis prin portul COM. Când cronometrul expiră, starea protocolului este resetată și tamponul de pachete este șters. Setarea parametrului la 0 dezactivează caracteristica. Acest parametru este disponibil numai prin meniul AVANZAT.

7.1.2.2. Parametri comuni ai protocolului

Fiecare protocol SCADA utilizat pe interfața serială este mai mult sau mai puțin unic. Modulul de protocol al portului COM realizează conversia în datagrame UDP standard pentru a călători prin rețeaua celulară M!DGE3. Aceleași setări sunt valabile și pentru serverele Terminal (pentru mai multe detalii despre TS vezi *Secțiunea 7.1.3, „Servere terminale”*).



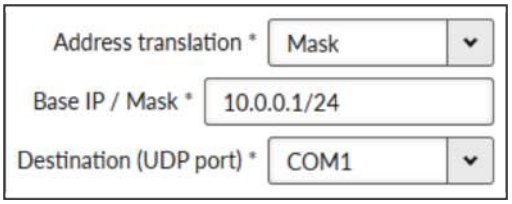
Protocol

Caseta listă {Niciuna; Legătură asincronă; COMLI; DNP3; DF1; IEC101; Marte-A; Modbus RTU; PR2000; RDS; S3964R; SAIA S-BUS; UNI}, implicit = „Niciunul”

Traducerea adresei

Caseta listă {Mască; Table}, implicit = „Mască”

Adresa de protocol SCADA este tradusă la adresa IP utilizând fie tipul de conversie Mask (regulă comună pentru toate adresele) fie Tabel (regula specifică pe adresă).



IP de bază / Mască

O parte din adresa IP de bază definită de această mască este înlocuită cu „Adresă de protocol”. Adresa de protocol SCADA are de obicei 1 octet, astfel încât Masca 24 (255.255.255.0) este folosită cel mai frecvent. Această adresă IP este utilizată ca adresă IP de destinație a datagramei UDP în care este încapsulat pachetul serial SCADA primit de la COM.

Portul UDP de destinație

Caseta listă {Manual; COM1 – COM3; TS1 – TS5}, implicit = „COM1”

Același port UDP va fi utilizat pentru toate destinațiile. Acest port UDP este utilizat ca port UDP de destinație în datagrama UDP în care pachetul serial SCADA primit de la COM este încapsulat. Porturile UDP implicite pentru serverele COM sau Terminal Server pot fi utilizate sau portul UDP poate fi setat manual. Dacă des-

adresa IP aparține unui M!DGE3 și portul UDP nu este atribuit COM sau unui server Terminal sau oricărui alt modul SW special care rulează în destinația M!DGE3, pachetul este aruncat.

Nota
Portul UDP implicit pentru interfața serială în M!DGE2 este 8882. Țineți cont de acest lucru dacă combinați M!DGE2 cu M!DGE3/RipEX2.

Adresă de protocol (de la)
Aceasta este adresa care este utilizată de protocolul SCADA.
Lungimea tipică a adresei de protocol este de 1 octet. Unele protocoale, de exemplu DNP3, folosesc adrese lungi de 2 octeți.

Adresă de protocol (către)
Mai multe adrese SCADA consecutive vor fi traduse folosind o singură regulă.

adresa IP (baza)
Adresă IP la care va fi tradusă adresa de protocol. Această adresă IP este utilizată ca adresă IP de destinație a datagramei UDP în care este încapsulat pachetul serial SCADA primit de la COM. Când sunt folosite mai multe adrese, aceasta va fi prima adresă IP, următoarea va avea +1 etc.

Destinație (port UDP)
Caseta listă {MANUAL; COM1 – COM3; TS1 – TS5}, implicit = „COM1”
Acesta este numărul portului UDP care este utilizat ca port UDP de destinație în datagrama UDP în care este încapsulat mesajul serial SCADA, primit de la COM. Porturile UDP de destinație diferite pot fi utilizate în reguli diferite.

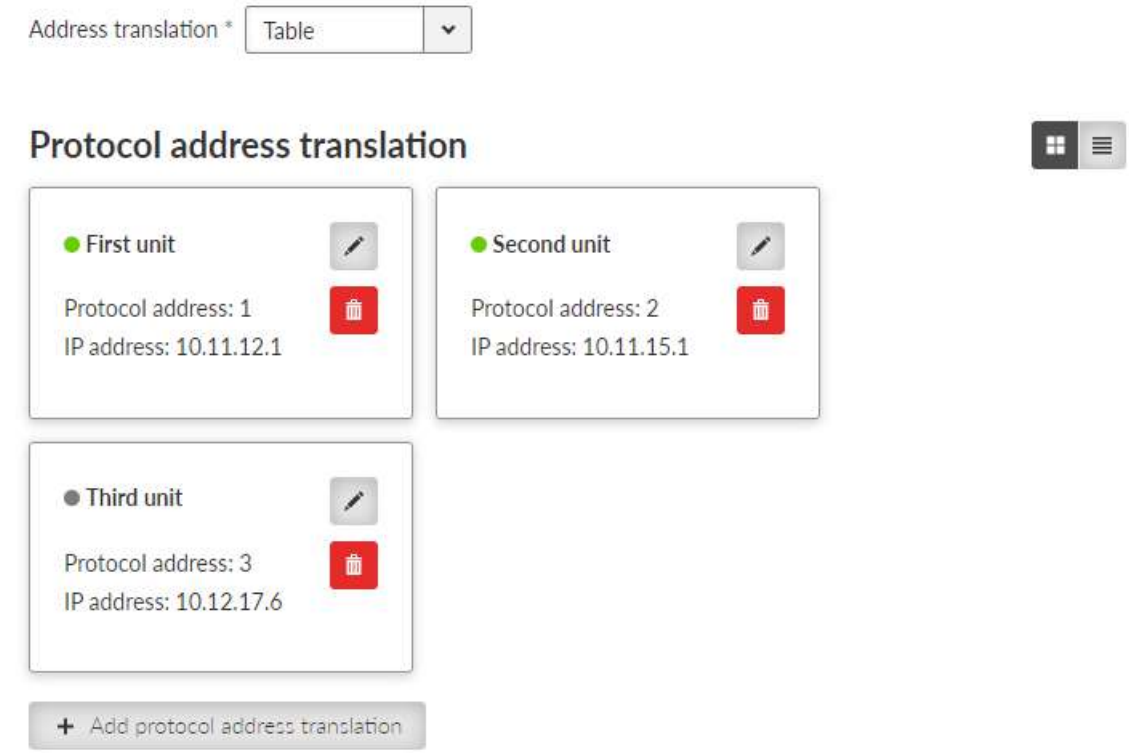
Traducere adresa: Masca

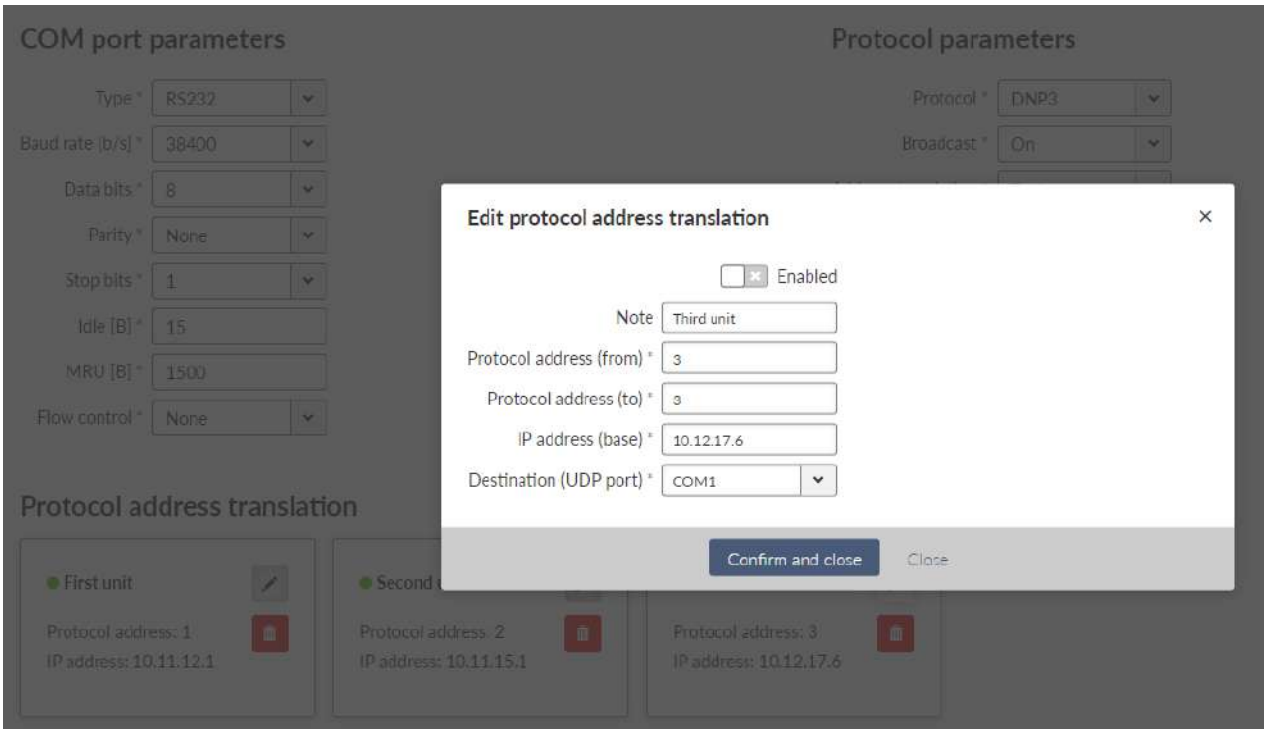
Nota
Toate adresele IP utilizate trebuie să fie în aceeași subrețea, care este definită de această mască. Același port UDP este utilizat pentru toate unitățile SCADA, ceea ce are ca rezultat următoarele limitări:

Dispozitivele SCADA de pe toate site-urile trebuie să fie conectate la aceeași interfață

Doar un dispozitiv SCADA la un port COM poate fi conectat, chiar dacă este utilizată interfața RS485.

Traducere adrese: Tabel
Traducerea adresei este definită într-un tabel. Nu există limitări, cum ar fi atunci când este utilizată traducerea „Mască”. Dacă există mai multe unități SCADA conectate prin interfața RS485, multiplele „adrese de protocol” ale acestora sunt traduse în aceeași adresă IP și pereche de porturi UDP.





Nota
Puteți adăuga o notă la fiecare adresă cu comentariile dvs. (UTF8 este acceptat) pentru confortul dvs.

7.1.2.3. Parametrii individuali ai protocolului

Unele dintre protocoalele SCADA pot configura un comportament suplimentar de răspuns al dispozitivului Slave.

Modul țintă de răspuns

Caseta listă {LASRCV; ȚINTĂ}, implicit = „LASRCV”
Răspunsul pentru cadrul de intrare va fi direcționat către adresa IP a masterului care a trimis cadrul (LASTRCV) sau către o adresă IP specificată (TARGET).

IP țintă de răspuns

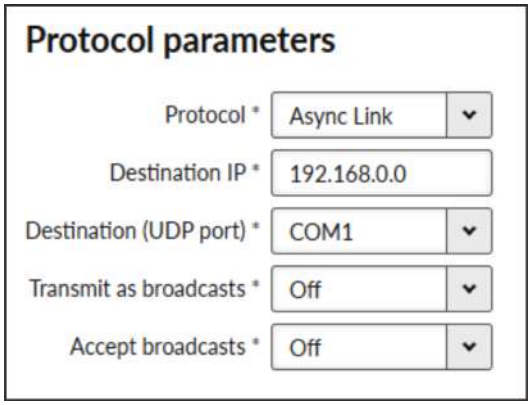
Adresă IP la care este trimis răspunsul atunci când este aleasă TARGET în modul țintă răspuns.

7.1.2.3.1. Nici unul

Protocolul None dezactivează portul COM. Toate datele primite vor fi aruncate, nu vor fi trimise date în interfața COM.

7.1.2.3.2. Legătură asincronă

Legătura asincronă creează o legătură asincronă între două porturi COM pe unități RipEX2 sau M!DGE3 diferite. Cadrele primite de la portul COM sau de la un server Terminal sunt trimise fără nicio prelucrare în mod transparent prin router către destinația IP și portul UDP setat. Cadrele primite din rețea sunt trimise către COM sau serverul Terminal în funcție de parametrul Destinație (port UDP).



IP de destinație

Definește adresa IP de destinație a lui RipEX2 sau M!DGE3).

7.1.2.3.3. COMLI

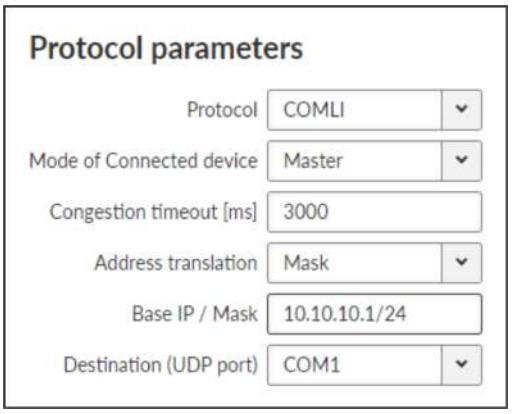
COMLI este un protocol de comunicare de tip polling serial utilizat de aplicația Master-Slave. Într-o rețea M!DGE3 pot fi angajați mai mulți Master COMLI și un Slave poate fi interogat de mai mulți Master. Pachetele de difuzare nu sunt utilizate.

Cadrul protocolului COMLI este trimis transparent, dar fără STX, ETX și BCC. STX (începutul datelor), ETX (sfârșitul datelor) și BCC (XOR de 8 biți) sunt adăugate la participantul care primește. În timpul transferului, integritatea datelor este securizată corespunzător prin sume de control individuale ale protocolului.

Nota

Protocolul COMLI din RipEX2 sau M!DGE3 nu este pe deplin compatibil pe portul COM cu modemurile RipEX și MR. Implementarea M!DGE3 nu acceptă „întârziere intercaracter tx”.

Mod de dispozitiv conectat: MASTER

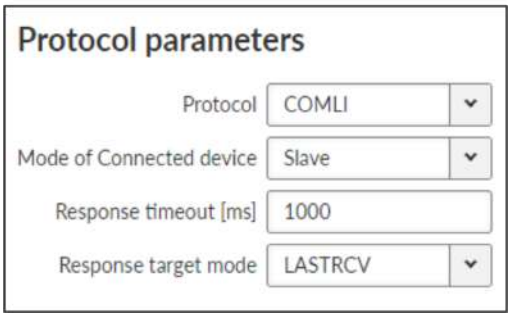


Timeout congestionare [ms]

Numărul {0 – 65535}, implicit = 3000, 0 dezactivează această funcționalitate

Timeout pentru verificarea duplicității celor două cadre următoare. Folosit atunci când același cadru este primit prin portul COM în timpul de expirare măsurat din momentul expedierii cadrului anterior.

Mod de dispozitiv conectat: SLAVE



Timp de expirare a răspunsului [ms]

Număr {0 – 16383}, implicit = 1000

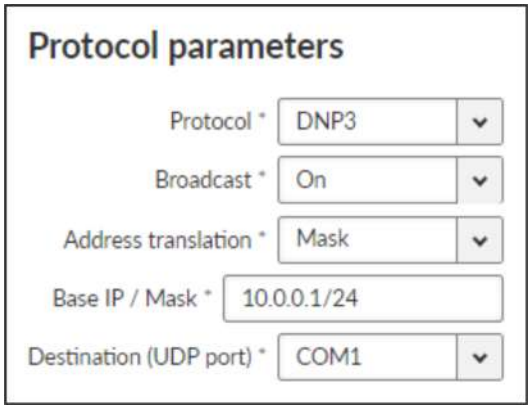
Timpul de expirare a răspunsului protocolului COMLI este utilizat pentru așteptarea pe portul COM pentru răspunsul dispozitivului conectat.

Modul țintă de răspuns

Caseta listă {LASRCV; ȚINTĂ}, implicit = ”LASRCV”
Răspunsul slave va fi trimis la adresa ultimei solicitări primite (LASRCV) sau la adresa specificată**IP țintă de răspuns**adresa (TARGET).

7.1.2.3.4. DNP3

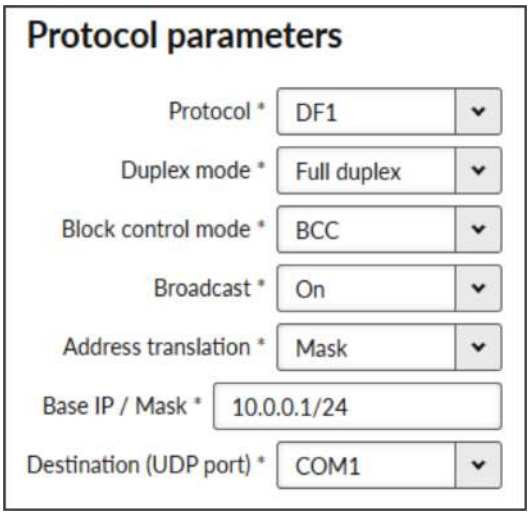
Fiecare cadru din protocolul DNP3 conține adresele sursă și destinație în antetul său, deci nu există nicio diferență între Master și Slave în ceea ce privește configurația M!DGE3. DNP3 permite atât sondarea Master-Slave, cât și comunicarea raport cu excepție de la unitățile de la distanță.



Parametrii comuni (de exemplu, traducerea adresei) trebuie setati.

7.1.2.3.5. DF1

Fiecare cadru din protocolul Allen-Bradley DF1 conține adresele sursă și destinație în antetul său, deci nu există nicio diferență între Master și Slave în modul Full duplex în ceea ce privește configurația M!DGE3.



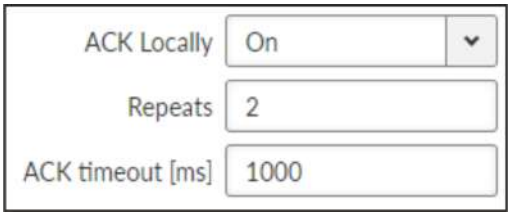
Modul duplex

Caseta listă {Full duplex; Half duplex}, implicit = „Full duplex“

Mod de operare a protocolului DF1: Numai modul Full duplex este implementat acum.

Parametri avansați DF1

Protocolul DF1 acceptă confirmarea locală a protocolului. De obicei, se utilizează setarea implicită. În cazul în care este nevoie, este posibilă modificarea parametrilor ACK în meniul AVANZAT > Generic > com_x_prot/Protocol_DF1.



ACK la nivel local

Caseta listă {On; Oprit}, implicit = „Pornit”

Permite pornirea/activarea ACK-ului local

Se repetă

Numărul {0 – 31}, implicit = 2

Setează numărul de repetări când ACK local nu este primit.

Timeout ACK [ms]

Număr {0 – 1683}, implicit = 1000

Timeout de așteptare pentru ACK.

Modul de control bloc

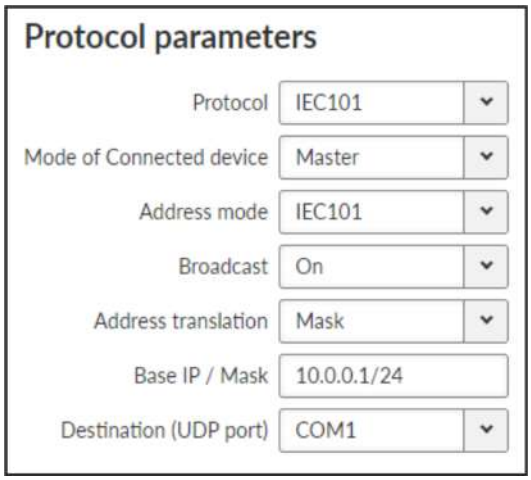
Caseta listă {BCC; CRC}, implicit = „BCC”

Conform specificației DF1, poate fi utilizat fie BCC, fie CRC pentru modul de control bloc (integritatea datelor).

Nota

Conform specificației DF1, pachetele pentru adresa de destinație 0xFF sunt considerate transmisii. Prin urmare, când Broadcast este activat, pachetele cu această destinație sunt tratate ca transmisii.

7.1.2.3.6. IEC101



Modul dispozitiv conectat

Caseta cu listă {Master; Sclav; Combinat}, implicit = „Maestru”

Nota
Pentru SCADA Master set Master conectat, pentru SCADA Slave Set Slave conectat.

Modul adresa

Caseta listă {IEC101; 2B ADDR; TELEGYR; SINAUT; Fără adresă}, implicit = „IEC101”

7.1.2.3.7. Marte-A

MARS-A este un protocol full duplex care include:

- adrese lungi de 32 de biți

- detectarea erorilor (pe baza unei sume de control pe 16 biți (XOR) sau pe 16 biți CRC)

- corectarea erorilor

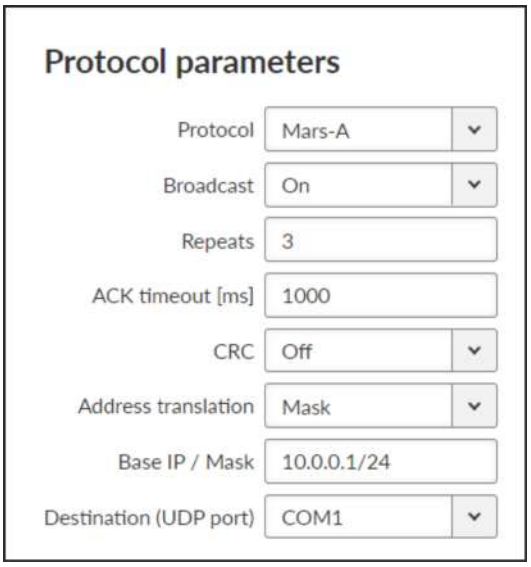
MARS-A a fost utilizat pe scară largă de către modemurile radio RACOM vechi în sistemul MORSE din anul 1999.

Noua implementare a acestui protocol în M!DGE3 sau M!DGE3 este limitată la părțile protocolului complex care pot fi utilizate împreună cu tipul modern de pachete ale acestor routere:

DATE UTILIZATOR (0x09) de la router la interfața serială (de exemplu, la RTU),

DATE UTILIZATOR (0x09) și DATE PROT (0x0A) de la interfața serială (de ex. de la RTU) la router.

Antetele Mars-A sunt eliminate din pachet înainte de a fi transmise în rețea - sunt transmise doar datele.



Timeout ACK [ms]

Număr {0 – 16383}, implicit = 1000 Timp de expirare pentru confirmarea interfeței seriale.

Se repetă

Numărul {0 – 31}, implicit = 3

Numărul de repetări. Repetarea este declanșată atunci când se primește cadrul NAK sau dacă cadrul ACK nu a fost primit în timpul expirării ACK.

Bit de securitate

Caseta listă {On; Off}, implicit = „Dezactivat”

Necesar pentru compatibilitate cu implementările vechi ale rețelei MORSE. Acest parametru nu modifică comportamentul protocolului.

CRC

Caseta listă {On; Off}, implicit = „Off”

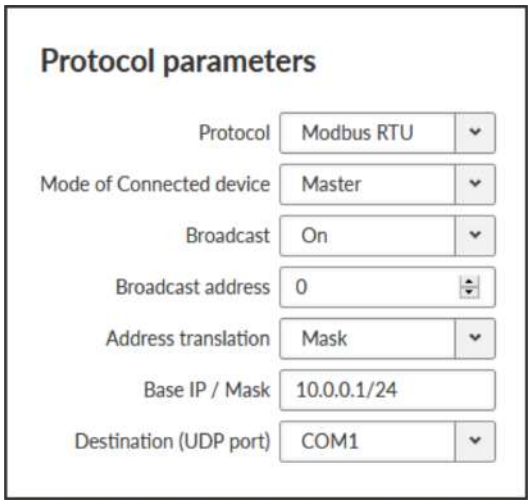
Algoritm de detectare a erorilor:

• Pornit - se utilizează algoritmul CRC

• Oprit - se utilizează algoritmul XOR

7.1.2.3.8. Modbus RTU

Modbus RTU este un protocol de comunicație de tip polling serial utilizat de aplicația Master-Slave.

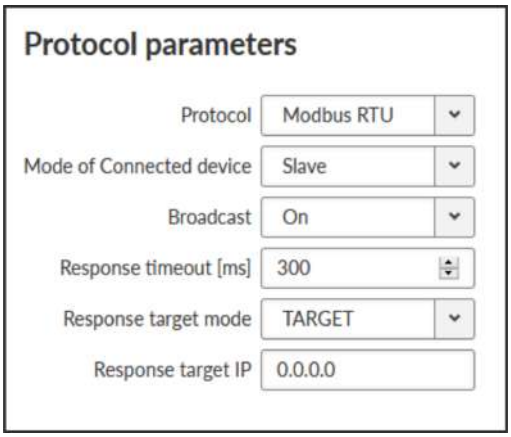


Modul dispozitiv conectat

Caseta cu listă {Master; Slave}, implicit = „Maestru”

Modul dispozitiv conectat: MASTER

Modul dispozitiv conectat: SLAVE



Timp de răspuns

Număr { 0 – 8190}, implicit = 300

Parametrul Response timeout controlează cât timp așteaptă unitatea pentru un cadru de confirmare. Timeout-ul începe când cadrul original primit de la canalul celular este transmis către dispozitivul conectat (prin canalul serial). Transmiterea oricărui alt cadru către dispozitivul conectat este blocată temporar, în timp ce Timeout de răspuns este activ. Timpul de expirare a răspunsului = 0 dezactivează această caracteristică.

7.1.2.3.9. Protocolul PPP

Protocolul PPP (Point-to-Point Protocol, specificat în RFC 1661) este destinat unei conexiuni duplex direct între două puncte de rețea. Funcționează la nivelul de legătură ca o extensie a protocolului HDLC. Ambele puncte de rețea primesc o configurație pe baza căreia negociază proprietățile de conectare între ele prin linia serială. Consecința unei negocieri de succes este crearea de interfețe de rețea de ambele părți. În funcție de protocolul de rețea selectat, acestea pot fi interfețe de diferite tipuri. În cazul nostru, se folosește protocolul IPCP (IPV6CP), iar interfața rezultată este de tip TUN (ex. ppp1). Interfeței i se atribuie o adresă IP în funcție de configurație și utilizator

datele sunt transferate prin intermediul acestuia. Încapsularea PPP este utilizată pentru încapsularea pachetelor IP în cadre transmise pe o linie serială (vezi Formatul cadru, RFC 1662).

7.1.2.3.9.1. Curs tipic de stabilire a unei conexiuni

Negocierea parametrilor de linie (LCP)

Parametrii de bază de conectare la nivelul liniei seriale
LCP (Link Control Protocol, RFC 1661)
Parametrii negociați:
• Unitate maximă de recepție (MRU)
• Harta caracterelor de control asincron (ACCM)
• Protocol de autentificare
• Comprimarea câmpului de protocol în antetul cadrului PPP
• Comprimarea câmpurilor de adresă și de control din antetul cadrului PPP

Autentificare

Opțional, dacă se negociază, se va folosi protocolul corespunzător
Poate fi cu două fețe, unde fiecare parte poate necesita un protocol diferit
Protocoale:
• PAP (protocol de autentificare prin parolă)
• CHAP (Challenge Handshake Authentication Protocol)

Negocierea parametrilor de compresie a datelor (CCP)

Tipul de compresie a datelor și parametrii Protocolul
de control al compresiei (CCP, RFC 1962)

Negocierea protocolului de rețea (NCP).

Parametri de conexiune la nivel de rețea
Protocolul de control al rețelei (NCP):
• IPCP (Internet Protocol Control Protocol, RFC 1332)
• IPv6CP (Protocol de control IPv6, RFC 5072)

7.1.2.3.9.2. Formatul cadrelor

Formatul cadrelor PPP (RFC 1661, RFC 1662) se bazează pe standardul de protocol HDLC.

7.1.2.3.9.3. Format de cadru comun

Pavilion	Adresa	Controla	Protocol	informa-ție	Captuseala	FCS	Pavilion
0x7E	0xFF	0x03	8/16 biți	*	*	16/32 de biți	0x7E

7.1.2.3.9.4. Înțelesul individual fields

- **Pavilion**: valoarea 0x7E definită în specificația protocolului
- **Câmp de adresă**: câmp de adresă, valoarea 0xFF definită în specificația protocolului
- **Câmp de control**: câmp de control, valoarea 0x03 definită în specificația protocolului
- **Câmpul protocolului**: câmpul protocol, indică tipul de date din câmpul Informații
  - Exemplu: 0xC021 pentru LCP, 0xC023 pentru PAP
- **Informaţii**: date încapsulate

○ Exemplu: pachet IP

- **Captuseala**
- **Câmpul Frame Check Sequence (FCS).**: secvență de control pentru detectarea erorilor de transmisie

7.1.2.3.9.5. Configurare

Unele elemente de configurare sunt strâns legate de parametrii nativi ai demonului pppd. Parametrii individuali sunt listați în textul de mai jos în puncte marcate cu „pppd:” și informații detaliate despre aceștia pot fi găsite în paginile de manual ale demonului.

„<NR>” este folosit pentru a indica indicele PPP (1/2/3).

7.1.2.3.9.6. Parametrii protocolului

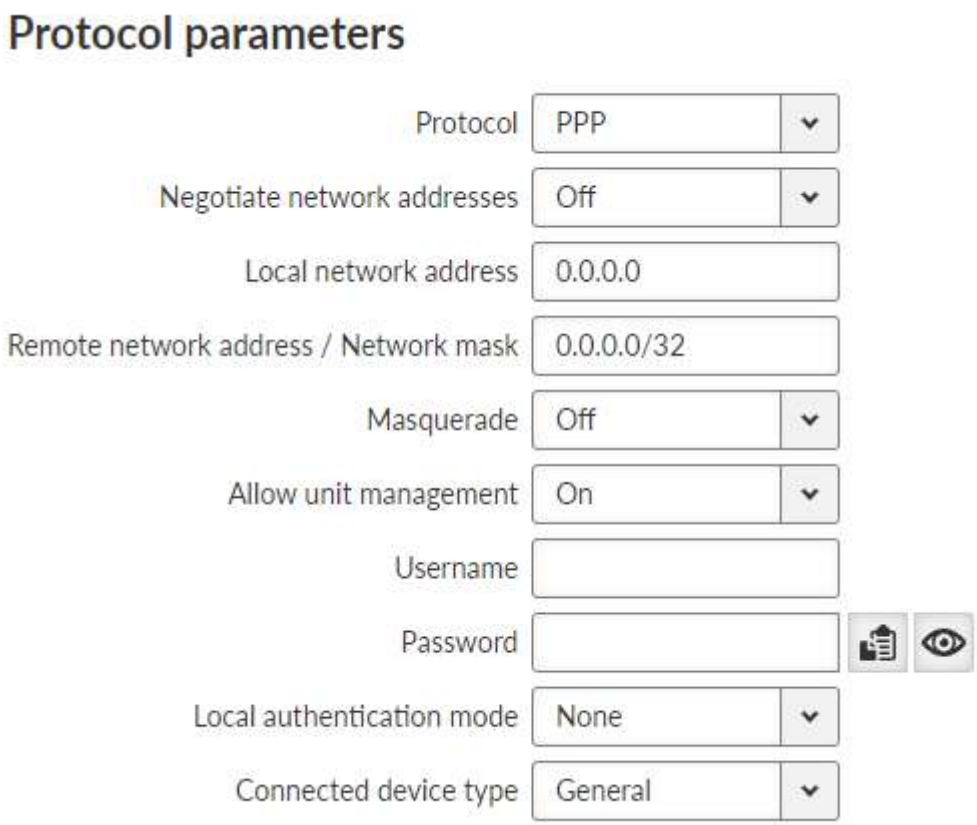


Fig. 7.3: SETĂRI>Interfețe>COM

Negociați adresele de rețea

Caseta listă {On; Off}, implicit = „Dezactivat”

Activează negocierea adresei interfeței PPP local/la distanță.

Dacă sunt dezactivate, Adresa rețelei locale și Adresa rețelei la distanță trebuie setate manual.

Adresa rețelei locale

adresa IP; implicit = 0.0.0.0 Adresa IP locală a interfeței PPP

Adresă de rețea la distanță / Mască de rețea

adresa IP; implicit = 0.0.0.0/32

Adresa IP de la distanță și masca interfeței PPP. Adresa și Masca sunt folosite pentru a determina intervalul țintă al unei reguli de rutare către interfața PPP

Mascaradă

Caseta listă {On; Off}, implicit = „Dezactivat”

Activează/dezactivează Sursa NAT (masquerade) pe pachetele trimise prin interfața PPP.

Cu masquerade activată, pachetele care părăsesc stația prin interfața PPP sunt rescrise cu adresa sursă la adresa atribuită acelei interfețe

Permite gestionarea unității

Caseta listă {On; Off}, implicit = „Activat”

Permite accesul la managementul unității prin interfața PPP

Nume de utilizator

Șir {până la 50 de caractere}, implicit = <gol>

Numele de utilizator de utilizat la autentificarea la contraparte, indiferent de protocolul care este necesar.

Caracterele ASCII imprimabile sunt permise, cu excepția caracterelor interzise „, `, \, $, ;

Parolă

Șir {până la 50 de caractere}, implicit = <gol>

Parola de utilizat la autentificarea la contraparte, indiferent de protocolul care este necesar.

Caracterele ASCII imprimabile sunt permise, cu excepția caracterelor interzise „, `, \, $, ;

Mod de autentificare locală

Selectarea protocolului cu care contrapartea urmează să fie autentificată la stabilirea conexiunii.

Pentru opțiunile PAP (moștenire) și CHAP, acreditările stabilite de**Nume de utilizator de autentificare locală**și **Parola de autentificare locală**sunt folosite

Nume de utilizator de autentificare locală

Șir {până la 50 de caractere}, implicit = <gol>

Numele de utilizator pe care contrapartea ar trebui să-l folosească în timpul autentificării (a se vedea**Mod de autentificare locală**).

Caracterele ASCII imprimabile sunt permise, cu excepția caracterelor interzise „, `, \, $, ;

Parola de autentificare locală

Șir {până la 50 de caractere}, implicit = <gol>

Parola pe care contrapartea ar trebui să o folosească în timpul autentificării (vezi**Mod de autentificare locală**).

Caracterele ASCII imprimabile sunt permise, cu excepția caracterelor interzise „, `, \, $, ;

Tip de dispozitiv conectat

Caseta listă {General; Terminal TETRA (Motorola MTM5x00)}, implicit = ”General”

Tip de dispozitiv conectat. Setează secvența de comandă corespunzătoare pentru a comuta dispozitivul conectat în modul PPP.

Negocierea adreselor de rețea trebuie să fie activată pentru TETRA.

Parametri de meniu avansati:

Harta caracterelor de control asincron

Număr {0 – 65535}, implicit = 0 setări Async-Control-Character-Map (ACCM).

O valoare diferită de zero poate fi utilizată pentru a selecta caractere de control pe care contrapartea nu ar trebui să le includă în pachetele PPP trimise.

Număr de erori LCP Keepalive

Număr {0 – 255}, implicit = 0

O valoare diferită de zero înseamnă numărul maxim de mesaje de solicitare eco LCP trimise înainte ca peer-ul să fie marcat ca deconectat și conexiunea să fie închisă (vezi**Interval de menținere LCP**[s]). O valoare zero dezactivează funcția.

Interval de menținere LCP [s]

Număr {0 – 255}, implicit = 10

Intervalul de trimitere a mesajelor de solicitare eco LCP, la care contrapartea răspunde cu un mesaj de răspuns eco LCP în stare normală.

Odata cu acea intrare**Număr de erori LCP Keepalive**poate fi folosit pentru a detecta dacă o parte este conectată

Activ dacă**Număr de erori LCP Keepalive**este mai mare decat 0

Activați utilizarea liniilor de control modem

Caseta listă {On; Off}, implicit = „Dezactivat”

Opțiunea de utilizare a „liniilor de control modem” (semnale portului serial DTR/DSR).

Activați înregistrarea mesajelor de control

Caseta listă {On; Off}, implicit = „Dezactivat”

Opțiunea de a descrie mesajele de control daemon pppd.

Mesajele sunt scrise în jurnalul standard /var/log/pppd_<NR>/log, care este disponibil într-un pachet de diagnosticare.

Modul de negociere de compresie

Caseta listă {Automatic; Manual}, implicit = „Automat”

Mod pentru selectarea parametrilor de configurare legati de compresie (toate elementele rămase de mai jos). Când este selectat Automat, elementele de configurare de mai jos sunt ignorate și demonul pppd își folosește valorile implicite. Când este selectat Manual, elementele de configurare de mai jos sunt active, iar valorile lor sunt folosite de demonul pppd atunci când negociază cu contrapartea.

Activați comprimarea adresei și a câmpului de control

Caseta listă {On; Off}, implicit = „Activat”

Alegerea de a negocia adresa și comprimarea câmpului de control în antetul cadrului PPP (comprimarea câmpului Adresă/Control, vezi Formatul cadru), în ambele direcții de transfer de date.

Activ dacă**Modul de negociere de compresie**este Manual.

Activați compresia câmpului de protocol

Caseta listă {On; Off}, implicit = „Activat”

Alegerea de a negocia compresia câmpului de protocol în antetul cadrului PPP (comprimarea câmpului de protocol, vezi Formatul cadru), în ambele direcții de transfer de date.

Activ dacă**Modul de negociere de compresie**este Manual.

Sloturi maxime de compresie antet IP Van Jacobson

Numărul {0; 2 – 16}, implicit = 16

Opțiunea de compresie Van Jacobson a antetelor IP.

O valoare diferită de zero este un parametru al algoritmului de compresie (numărul de sloturi de conexiune). O valoare zero dezactivează funcția.

Activ dacă**Modul de negociere de compresie**este Manual.

Activați protocolul de control al compresiei

Caseta listă {On; Off}, implicit = „Activat”

Opțiunea de a utiliza CCP (Compression Control Protocol) pentru a negocia parametrii de compresie a datelor. Opțiunea de a dezactiva CCP este oferită pentru compatibilitatea cu clienții PPP vechi care nu acceptă compresia datelor.
Activ dacă**Modul de negociere de compresie**este Manual.

Comprimarea datelor BSD primiți dimensiunea codului

Numărul {0; 9 – 15}, implicit = 15
O valoare diferită de zero este un parametru al algoritmului „BSD-Compress” pentru compresia datelor în direcția de intrare.
O valoare zero dezactivează funcția.
Activ dacă**Modul de negociere de compresie**este manuală și**Activați protocolul de control al compresiei** este dezactivat.

Comprimarea datelor BSD transmite dimensiunea codului

Numărul {0; 9 – 15}, implicit = 15
O valoare diferită de zero este un parametru al algoritmului „BSD-Compress” pentru compresia datelor în direcția de ieșire.
O valoare zero dezactivează funcția.
Activ dacă**Modul de negociere de compresie**este manuală și**Activați protocolul de control al compresiei** este dezactivat.

Dezumflați compresia datelor primiți dimensiunea codului

Numărul {0; 9 – 15}, implicit = 15
O valoare diferită de zero este un parametru al algoritmului „Deflate” pentru compresia datelor în direcția de intrare.
O valoare zero dezactivează funcția.
Activ dacă**Modul de negociere de compresie**este manuală și**Activați protocolul de control al compresiei** este dezactivat.

Dezumflați dimensiunea codului de transmisie de compresie a datelor

Numărul {0; 9 – 15}, implicit = 15
O valoare diferită de zero este un parametru al algoritmului „Deflate” pentru compresia datelor în direcția de ieșire.
O valoare zero dezactivează funcția.
Activ dacă**Modul de negociere de compresie**este manuală și**Activați protocolul de control al compresiei** este dezactivat.

7.1.2.3.9.7. Dirijare

Modul de rutare

Listbox este extinsă cu opțiuni PPP <NR>
Dacă regula de rutare are selectată una dintre opțiunile PPP <NR>, rutarea se face către interfața PPP corespunzătoare.

Rutare persistentă

Caseta listă {On; Off}, implicit = „Dezactivat”
Regula de rutare este persistentă (consultați Configurația celulară pentru explicații detaliate).

7.1.2.3.9.8. Starea protocolului

Informațiile despre starea PPP sunt disponibile în meniul Diagnosticare > Informații > Interfețe > PPP. Stare oferă următoarele informații

• Interfaţă

  ○ Numele interfeței PPP.

• Statul

  ○ Starea curentă a demonului interfeței PPP.

• Peer MRU

  ○ Unitatea maximă de primire (MRU) în octeți solicitată în timpul negocierii de către contraparte.

• Peer Auth. modul

  ○ Protocol de autentificare solicitat de contraparte.

• Peer ACCM

  ○ Setarea ACCM solicitată de contraparte.

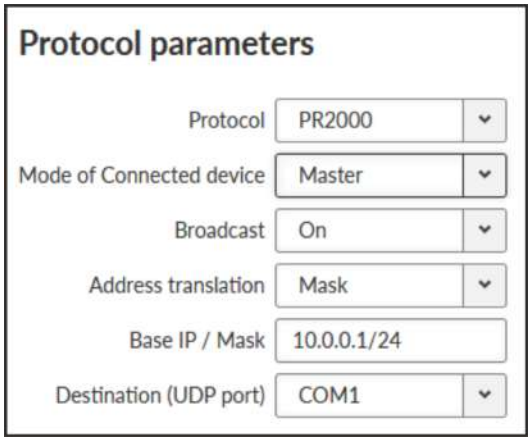
• Opțiuni de compresie negociate

  ○ Opțiuni negociate de compresie PPP.

7.1.2.3.10. PR2000

PR2000 este o abreviere pentru protocolul SCADA PROTEUS 2000. Acest protocol este utilizat în aplicațiile Master-Slave.

Protocolul PR2000 este implementat într-o manieră complet transparentă. Cadrele originale de protocol sunt transportate prin rețeaua RipEX în întregime.



7.1.2.3.11. Siemens 3964(R)

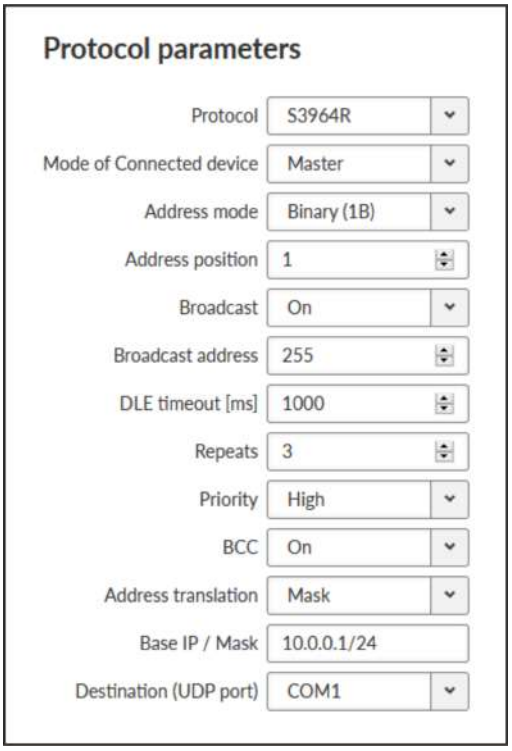
Protocolul 3964 este utilizat de compania Siemens ca o conexiune punct la punct între două controlere. Între timp, s-a dezvoltat într-un standard industrial care poate fi găsit pe multe dispozitive ca interfață de comunicații universală. 3964R este același cu 3964, în plus, folosește doar BCC (Block Check Character). 3964(R) gestionează numai stratul de legătură (L2 în modelul OSI), prin urmare RipEX folosește un mod similar de a citi „adresa SCADA” ca în protocolul UNI.

Există o strângere de mână STX(0x02) – DLE(Ox10) la începutul comunicării și DLE+ETX – DLE la sfârșit. Această strângere de mână este efectuată de RipEX local, nu este transferată prin rețeaua RipEX.

Comunicarea se desfășoară după cum
urmează: LocalRTU -> STX -> LocalRipEX
LocalRipEX -> DLE -> LocalRTU
LocalRTU -> DATE+DLE+ETX+BCC -> LocalRipEX
LocalRipEX -> DATE -> RemoteRipEX*
LocalRipEX -> DLE -> LocalRTU RemoteRipEX -> STX ->
RemoteRTU RemoteRTU -> DLE -> RemoteRipEX
RemoteRipEX -> DATA+DLE+ETX+BCC -> RemoteRTU
RemoteRTU -> DLE -> RemoteRipEX

* doar acest pachet este transferat prin rețeaua RipEX, toate celelalte sunt gestionate local.

Maestru



Modul adresa

Caseta listă {Binar (1 B); Binar (2B LSB mai întâi); Binar (2B MSB mai întâi)}, implicit = „Binar (1 B)”
RipEX citește adresa protocolului în formatul și lungimea setate (în octeți).

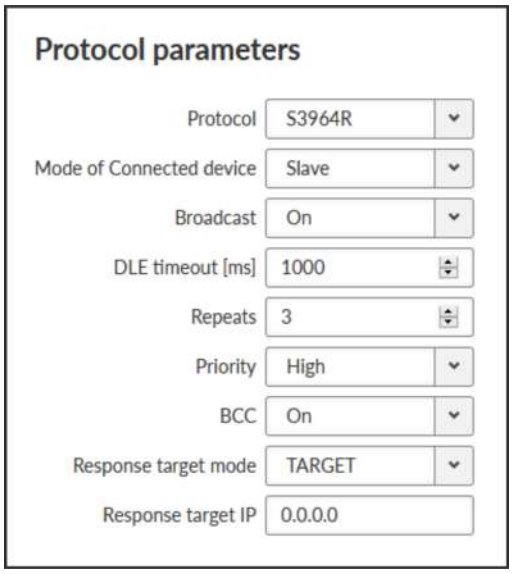
Poziția adresei

Specificați numărul de secvență al octetului, unde începe adresa de protocol.

Nota
Protocolul 3964(R) folosește secvența de evacuare (secvența de control) pentru DLE(0x10). Adică, când 0x10 este în datele utilizatorului, 0x1010 este trimis în schimb. Când se calculează poziția adresei, octeții adăugați de algoritmul secvenței de evacuare nu sunt luați în considerare.

Nota
Primul octet din pachet are numărul de secvență 1, nu 0.

Sclav



Timeout DLE [ms]

Număr {300 – 8190}, implicit = 1000

RipEX așteaptă un răspuns (DLE) de la dispozitivul conectat (RTU) în intervalul de timp stabilit. Dacă nu este primit, RipEX repetă cadrul conform setării „Reîncercări”.

Reîncercări [Nu]

Numărul {0 – 7}, implicit = 3

Când pachetul DLE nu este primit de la dispozitivul conectat (RTU) în timpul de expirare DLE setat, RipEX retransmite cadrul. Este specificat numărul de reîncercări posibile.

Prioritate

Caseta listă {Low; High}, implicit = „Scăzut”

Când echipamentul trimite STX și primește STX în loc de DLE, are loc o coliziune, ambele echipamente vor să înceapă comunicarea. Într-un astfel de caz, o unitate trebuie să aibă prioritate. Dacă Prioritatea este ridicată, RipEX așteaptă DLE. Când este scăzut, RipEX trimite DLE.

Nota

Evident, două echipamente care comunică împreună trebuie setate astfel încât una să aibă prioritate înaltă, iar cealaltă să aibă prioritate scăzută.

BCC

Caseta listă {On; Off}, implicit = „Activat”

BCC (Block Check Character) este un octet de control utilizat pentru controlul integrității datelor, ceea ce face ca fiabilitatea să fie mai mare. BCC este folosit de 3964R, 3964 nu îl folosește.

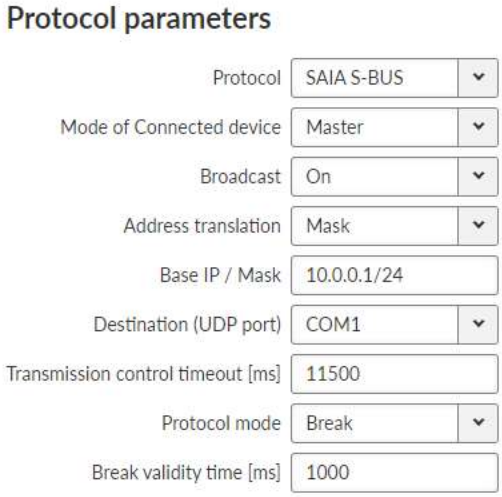
RipEX verifică (se calculează singur) acest octet în timp ce primește un pachet pe COM. RipEX transmite DLE (acceptă cadrul) numai când rezultatul verificării este OK. Octetul BCC nu este transferat prin rețeaua RipEX, este calculat local în final RipEX și atașat la datele primite.

7.1.2.3.12. SAIA S-Bus

Protocolul SAIA S-Bus a fost utilizat pe scară largă de modemurile radio RACOM vechi din sistemul MORSE. Protocolul S-Bus este implementat ca modul de acces pentru comunicarea cu dispozitivul SAIA PCD. Protocolul este de tip MASTER/SLAVE; MASTERUL nu are adresa proprie. Pot exista cel mult 254 de SLAVE-uri, adresa 255 este rezervată transmisiei transmise care nu este confirmată.

Stratul fizic al protocolului S-Bus utilizează interfața RS232 sau RS485. Adresa de difuzare 255 nu este acceptată pentru M!DGE3.

Cadrul de protocol trebuie să fie recepționat în întregime într-un singur buffer, deci parametrul IDLE ar trebui setat corect. Antetul protocolului S-bus nu conține întotdeauna lungimea datelor, așa că nu este posibil să lucrați cu cadre fragmentate și defragmentate.



Modul dispozitivului conectat

Caseta cu listă {Master; Sclav; Slave Plus}, implicit= „Master”

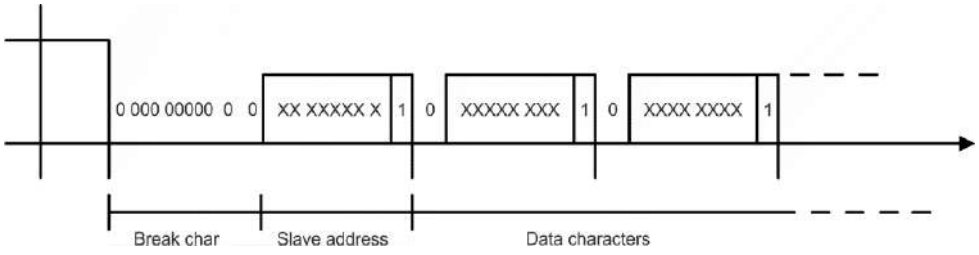
Maestruşi**Sclav**se comportă ca standard Master sau Slave Saia PCD. The**Slave Plus**modul permite să se comporte în mod limitat ca un Master și trimite către alt Slave/Slave Plus comanda de scriere (comanda de citire nu este permisă).

Mod protocol

Caseta cu listă {Break; Data}, implicit = „Break” Break sau modurile de protocol de date pot fi utilizate.

Mod pauză (SM0)

Cadrele sunt sincronizate de caracterele de pauză de o lungime configurată care sunt trimise înaintea comenzii adresate.

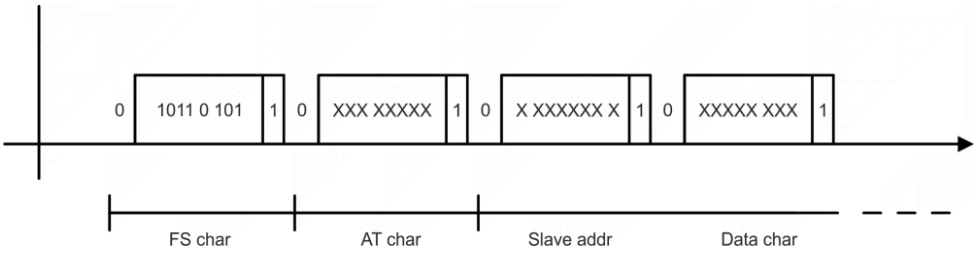


Modul Break este disponibil doar cu portul COM, nu este implementat pe TS (semnalul break nu este disponibil acolo). Verificarea semnalului de întrerupere este foarte dur (cu un pas de 100 ms) din cauza limitărilor nucleului Linux.

Modul de date (SM2)

Sincronizarea cadrelor se realizează prin inserarea caracterului 0xB5 la începutul cadrului. Dacă un alt caracter 0xB5 ar trebui să apară în cadru, atunci acesta este înlocuit cu următoarea secvență DLE:

Caracter	secvență DLE
0x85	0xC500
0xC5	0xC501



Nota
Vezi detalii despre implementarea RACOM pe*https://www.racom.eu/eng/support/prot/sbus/index.html*[1]

Mod de dispozitiv conectat: MASTER

Timeout control transmisie [ms]

Număr {0 – 65535}, implicit = 11500

Timeout master. Acest timeout este resetat după primirea unui răspuns de la Slave sau a unui cadru primit de la masterul conectat.

Mod de dispozitiv conectat: SLAVE

Timp de expirare a răspunsului [ms]Număr {0 – 16383}, implicit = 300

Timpul de răspuns al slavei - se așteaptă răspuns, altfel răspunsul către master este retrimis.

Se repetă

Numărul {0 – 7}, implicit = 3

Numărul de repetări când răspunsul de la master nu este primit.

Modul pauză

(parametru suplimentar)

Stăpân, Sclav Plus

Timp de valabilitate întrerupere [ms]

Număr {0 – 5000}, implicit = 1000 **Sclav,**

Sclav Plus

Lungimea pauzei [ms]

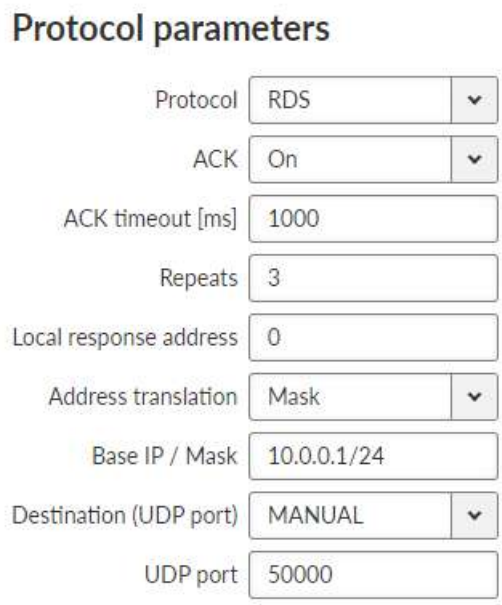
Număr {0 – 128}, implicit = 2

Lungimea pauzei în ms.

7.1.2.3.13. RDS

Protocolul RDS este un protocol utilizat în rețelele MRxx. Suportă comunicarea în rețea; orice nod din rețea poate vorbi cu oricare altul (spre deosebire de tipul de protocoale Master-Slave). Protocolul RDS este utilizat de obicei atunci când se combină rețelele RipEX și MRxx sau rețelele SCADA adaptate rețelelor MRxx. Cadrele sunt primite de la canalul celular și trimise către COM1-3 sau serverul Terminal 1-5 conform setărilor portului UDP și invers - de la fir la canalul celular.

[1] https://www.racom.eu/eng/support/prot/sbus/index.html



ACK

Caseta listă {On; Off}, implicit = „Activat”

Confirmare cadru atunci când este transmis prin interfață fir (COM sau Ethernet). Cadrele ACK (0x06) sunt transmise la recepția cu succes și NAK (0x15) la recepția nereușită.

Timeout ACK [ms]

Număr {0 – 16383}, implicit = 1000

Nota
Timeout ACK este măsurat de la începutul transmisiei pachetului.

Când „ACK” este activat, RipEX așteaptă „ACK timeout [ms]” după transmiterea cadrului pentru a primi confirmarea. Dacă cadrul ACK nu este primit, cadrul este retransmis. Retransmisia cadrelor are loc de până la „Repetări” de un număr de ori.

Se repetă

Număr {0 – 31}, implicit = 3 Număr de retransmisii de cadre.

Adresă locală de răspuns

Număr {0 – 255}, implicit = 0

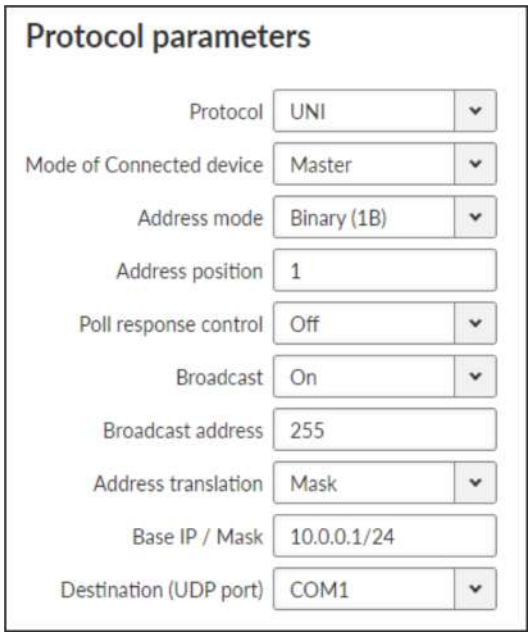
Această adresă este utilizată numai cu interogarea de stare (0x51). Răspunsul M!DGE3 este „0x54 <Local response address> 0x00”.

7.1.2.3.14. UNI

UNI este utilitarul de protocol „Universal” conceput pentru RipEX. Acesta ar trebui să fie utilizat atunci când protocolul de aplicație necesar nu este disponibil în RipEX și comunicarea în rețea utilizează modul adresat (care este un scenariu tipic). Condiția cheie este: mesajele generate de dispozitivul aplicației Master trebuie să conțină întotdeauna adresa Slave respectivă și poziția adresei, raportată la începutul mesajului (pachet, cadru), este întotdeauna aceeași (**Poziția adresei**). În general, două moduri de comunicare sunt tipice pentru protocolul UNI: În primul, comunicarea este întotdeauna inițiată de către Master și este acceptat un singur răspuns la o cerere; în al doilea mod, Master-Master

este posibilă comunicarea sau combinarea protocolului UNI cu protocolul ASYNC LINK și generarea spontană de pachete pe site-uri la distanță.

Protocolul UNI este complet transparent, adică toate mesajele sunt transportate și livrate fără nicio modificare.



Modul dispozitiv conectat

Casetă listă: {Master, Slave}, implicit = Master

Modul adresa

Caseta listă {Binar (1B); ASCII (2B); Binar (2B LSB mai întâi); Binar (2B MSB mai întâi)}, implicit = „Binar (1B)”

Formatul și lungimea adresei de protocol (în octeți). Formatul ASCII de 2 octeți este citit ca reprezentare hexazecimală de 2 caractere a valorii de un octet. De exemplu, caracterele ASCII AB sunt citite ca valoare 0xAB hex (10101011 binar, 171 zecimal) (funcția de format ASCII-2-Byte va fi disponibilă într-o versiune FW viitoare).

Poziția adresei

Numărul {1 – 255}, implicit = 1

Specificați numărul de secvență al octetului, unde începe adresa de protocol. Rețineți că primul octet din pachet are numărul de secvență 1, nu 0.

Controlul răspunsului la sondaj

Caseta listă {On; Off}, implicit = „Activat”

„Activat” – Master acceptă un singur răspuns pentru o cerere și trebuie să provină de la telecomanda specifică la care a fost trimisă cererea. Toate celelalte pachete sunt aruncate. Acest lucru se aplică schemei de comunicare Master - Slave.

Nota

Se poate întâmpla ca un răspuns de la un slave (Nr.1) să fie livrat după expirarea intervalului de timp respectiv și Masterul să genereze între timp cererea pentru următorul slave (Nr.2). În acest caz, răspunsul întârziat de la nr. 1 ar fi fost considerat răspuns de la nr.2. Când controlul răspunsului la sondaj este Activat, răspunsul întârziat de la slave nr.1 este renunțat și masterul rămâne pregătit pentru răspunsul de la nr.2.

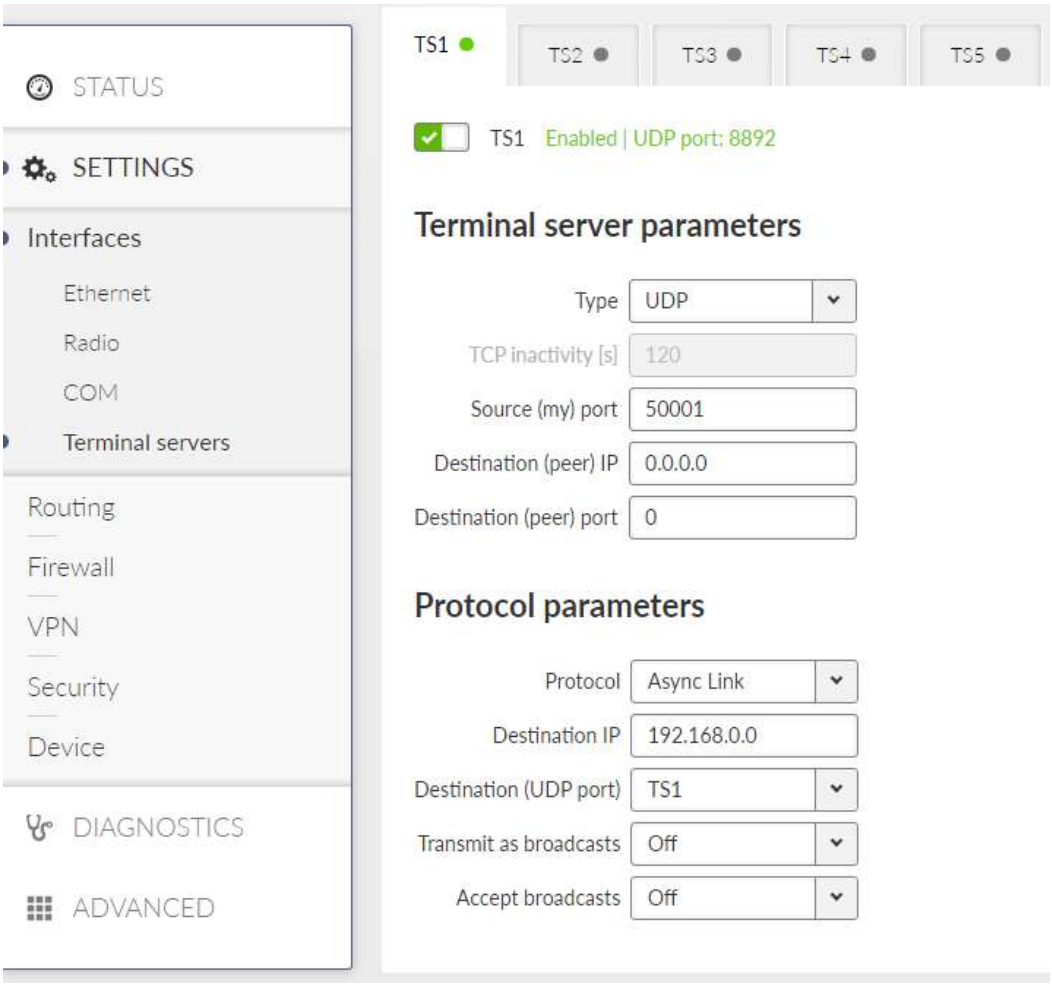
„Oprit” – Masterul nu verifică pachetele primite de la canalul RF - toate pachetele sunt transmise aplicației, inclusiv transmisiile. Acest lucru permite, de exemplu, să fie generate pachete spontane pe site-uri la distanță. Acest mod este potrivit pentru schema de comunicare Master-Master sau o combinație a protocoalelor UNI și ASYNC LINK.

Mod de dispozitiv conectat: SLAVE

7.1.3. Servere terminale

În general, un server terminal (denumit și server serial) permite conectarea dispozitivelor cu interfață serială la un M!DGE3 prin rețeaua locală (LAN). Este un înlocuitor virtual pentru dispozitivele utilizate ca convertoare serial-to-TCP (UDP).

În unele cazuri speciale, serverul Terminal poate fi utilizat și pentru reducerea încărcării rețelei de la aplicațiile care utilizează TCP. O sesiune TCP poate fi terminată local la serverul Terminal din M!DGE3, datele utilizatorului sunt extrase din mesajele TCP și procesate ca și cum ar veni dintr-un port COM. Când datele ajung la destinația M!DGE3, acestea pot fi transferate la RTU fie printr-o interfață serială, fie prin TCP (UDP), folosind din nou serverul Terminal.



Pot fi configurate până la 5 servere terminale independente. Fiecare poate fi de tip TCP sau UDP,**Inactivitate TCP**este timpul de expirare în secunde pentru care socket-ul TCP din M!DGE3 este menținut activ după ultima recepție sau transmisie de date. Ca adresă IP sursă a unui server Terminal va fi folosită adresa IP a interfeței M!DGE3 ETH (**Adresă locală de sursă preferată**daca exista vezi*Secțiunea 7.2.1, „Static”*), **Portul sursă (meu).** poate fi setat după cum este necesar.**IP de destinație (peer).**și**Port de destinație (peer).**valorile aparțin aplicației conectate local (de exemplu, o interfață serială virtuală). În unele cazuri, aplicațiile schimbă dinamic portul IP cu fiecare datagramă. Într-un astfel de caz setați Destination port=0. M!DGE3 va trimite apoi răspunsuri către portul de la care a fost primit ultimul răspuns. Această caracteristică permite extinderea numărului de conexiuni TCP deschise simultan între un M!DGE3 și o aplicație conectată local la orice valoare până la 10 pe fiecare server Terminal.**Protocol**urmează aceleași principii ca un protocol pe interfața COM.

Pentru detalii despre setări vezi*Secțiunea 7.1.2.2, „Parametri comuni ai protocolului”*.

Nota

Max. lungimea datelor utilizator într-o singură datagramă procesată de serverul Terminal este de 8192 de octeți.

Nota

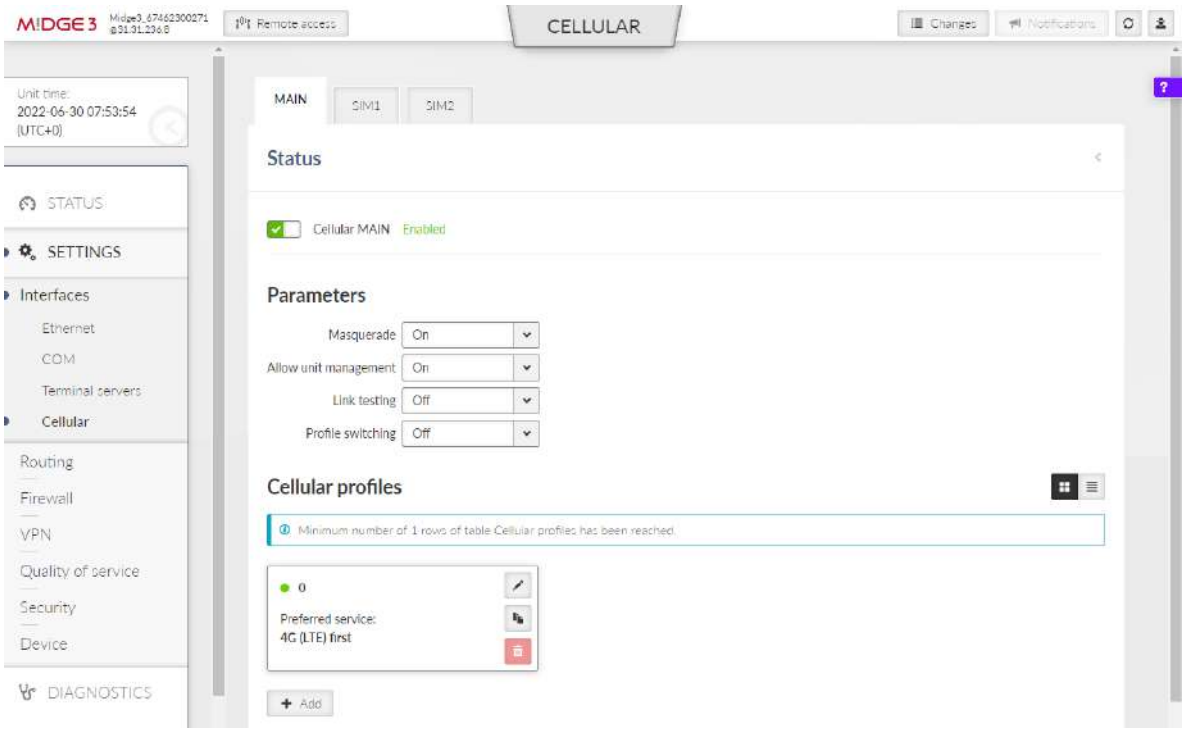
Intervalul de porturi 0-1023 este rezervat și interzis pentru Terminal Server. Portul 502 este o excepție pentru ModbusTCP.

7.1.4. Celular

M!DGE3 poate avea până la două module celulare (MAIN și EXT opțional). Toate caracteristicile sunt identice pentru ambele. Dacă sunt utilizate ambele module, fiecare cartelă SIM trebuie alocată unui anumit modul.

APN trebuie întotdeauna configurat, toți ceilalți parametri își pot păstra valorile implicite.

7.1.4.1. MAIN/EXT



Activați/dezactivați telefonul MAIN/EXT:

Activează/dezactivează telefonul MAIN/EXT. Când este dezactivat (implicit), modulul este oprit.

Nota

Dirijare**Modul**„WWAN MAIN/EXT” este adăugat la definiția regulilor de rutare statică. Când acest mod este selectat, parametrul Gateway de rutare este ignorat. În schimb, pachetul este redirecționat către interfața celulară (WWAN).

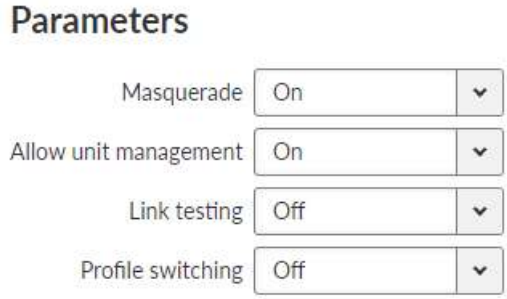
Regulile de rutare sunt activate/dezactivate automat atunci când interfața celulară (WWAN) este deschisă/închisă.

Nu sunt adăugate automat reguli de rutare după configurarea unui nou profil celular. Adăugați manual toate rutarea corespunzătoare (de exemplu, ruta implicită 0.0.0.0/0 prin interfața WWAN).

Nota

Această secțiune cooperează strâns cu*Secțiunea 7.7.5, „SMS”*.

7.1.4.1.1. Parametrii



Mascaradă

Caseta listă {On; Off}, implicit = „Activat”

Activează/dezactivează SNAT (MASQUERADE) pentru pachetele care ies din interfața WWAN. Când este activată, adresa sursă a pachetelor de ieșire prin interfața WWAN celulară va fi schimbată cu adresa atribuită acestei interfețe (adresa IP WWAN este utilizată în locul adreselor IP interne/LAN). Pachetele returnate vor fi direcționate corect înapoi la sursa inițială (dispozitivul intern).

Permite gestionarea unității

Caseta listă {On; Off}, implicit = „Activat”

Permite gestionarea unității prin interfața WWAN.

Testarea linkurilor

Caseta listă {On; Off}, implicit = „Dezactivat”

Activează/Dezactivează testarea legăturilor.

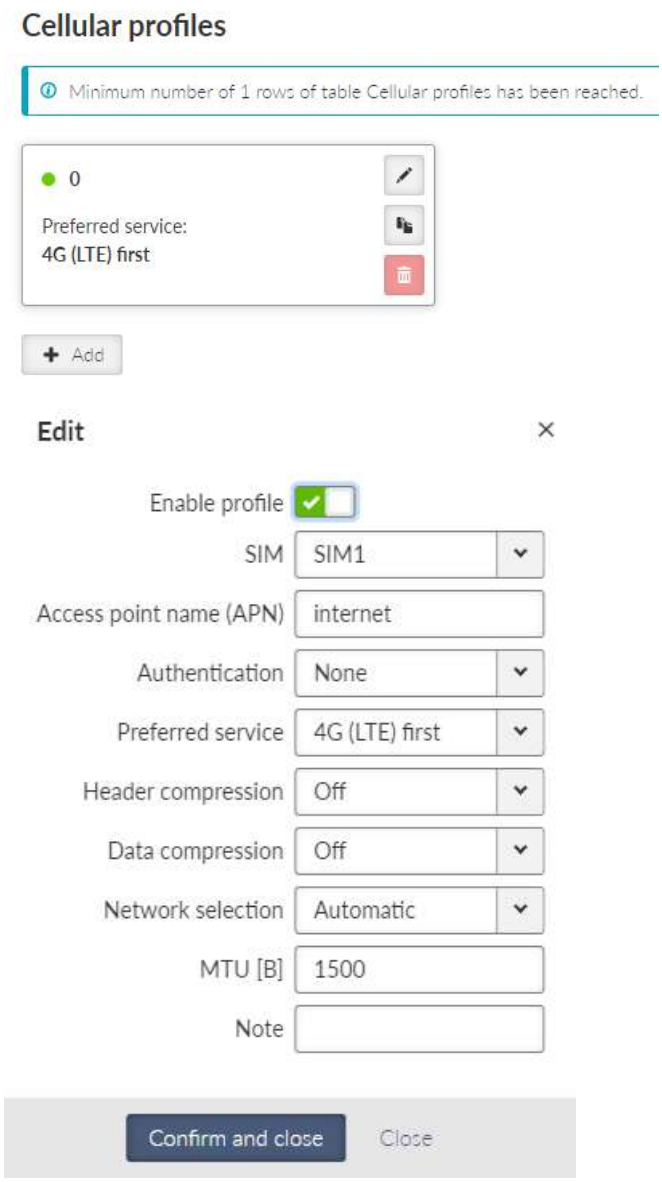
Schimbarea profilului

Caseta listă {On; Off}, implicit = „Dezactivat”

Activează/dezactivează comutarea automată a profilului.

7.1.4.1.2. Profiluri celulare

Set de profiluri definite (este necesar cel puțin un profil), care sunt parametrii de setare ai serviciului solicitat al rețelei (ex. APN).



Activați profilul

Activează/Dezactivează un profil specific.

Nume punct de acces (APN)

Șir {până la 99 de caractere}, implicit = <gol>

APN pentru acces în rețeaua celulară. APN valid este furnizat de clienții Furnizorul celular.

Autentificare

Caseta listă {Niciuna; PAP (moștenire); CHAP}, implicit =
"Niciuna" Selectează metoda de autentificare în APN.

Nici unul

Nu se utilizează autentificare pentru accesul APN.

PAP (moștenire)

Autentificare PAP (Password Authentication Protocol). Nu vă recomandăm să utilizați această opțiune din cauza problemelor de securitate (opțiunea este furnizată pentru a oferi compatibilitate cu sistemele vechi). Numele de utilizator și parola sunt necesare.

CAP

Autentificare CHAP (Challenge-Handshake Authentication Protocol). Numele de utilizator și parola sunt necesare.

Serviciu preferat

Caseta listă {2G (GSM) mai întâi; Doar 2G (GSM); 3G (UMTS) mai întâi; Numai 3G (UMTS); Doar 2G/3G (GSM/UMTS); 4G (LTE) mai întâi; Numai 4G (LTE); Numai 3G/4G (UMTS/LTE)}, implicit = „4G (LTE) primul”
Setează preferințele și/sau permisiunea pentru serviciile individuale ale rețelei celulare.

Comprimarea antetului

Caseta listă {On; Off}, implicit = „Dezactivat”
Activează/Dezactivează compresia antetelor IP de trafic de date utilizator. Nu este utilizat cu serviciul 4G.

Comprimarea datelor

Caseta listă {On; Off}, implicit = „Dezactivat”
Activează/Dezactivează compresia datelor despre traficul de date utilizator. Nu este utilizat cu serviciul 4G.

Selectarea rețelei

Caseta listă {Automatic; Prefer manualul; Blocare la manual; Lock to home}, implicit = „Automat”
Definește preferințele de selecție a rețelei:

Automat

Rețeaua este selectată automat.

Prefer manualul

Rețeaua conform**Identitatea zonei de locație (LAI)**este de preferat. O altă rețea va fi selectată atunci când rețeaua preferată nu este disponibilă.

Blocați la manual

Doar LAI a completat**Identitatea zonei de locație (LAI)**va fi utilizat parametrul.

Blocați acasă

Va fi utilizată doar rețeaua de domiciliu (dacă SIM-ul acceptă citirea PLMN). Această opțiune poate fi folosită și ca „oprire” pentru roaming.

Identitatea zonei de locație (LAI)

Șir {00000 – 999999}, implicit = 00000
Numărul de identificare al rețelei de telefonie mobilă public Land Mobile Network (PLMN).
Acest parametru apare numai dacă este parametru**Selectarea rețelei**este setat la „Prefer manual” sau „Lock to manual”.

MTU [B]

Număr {70 – 1500}, implicit = 1430
Pachete de ieșire MTU. Valoarea implicită se potrivește cu valoarea modulului mPLS83W și este cea mai comună valoare în rețelele celulare.
Valoarea MTU minimă pentru IPv6 (Babel) = 1280 B.

Nota

Comentariu optional.

7.1.4.1.3. Testarea linkurilor

Testarea nu numai a conexiunii la rețeaua celulară (verificarea conexiunii), ci și a conexiunii cu adresa(e) de destinație (testare link). Testele sunt sub forma trimiterii unui ping ICMP la adresa (adresele) definite și așteptarea unui răspuns. Această secțiune apare numai dacă este parametru ***Testarea linkurilor*** este setat pe „Pornit”.

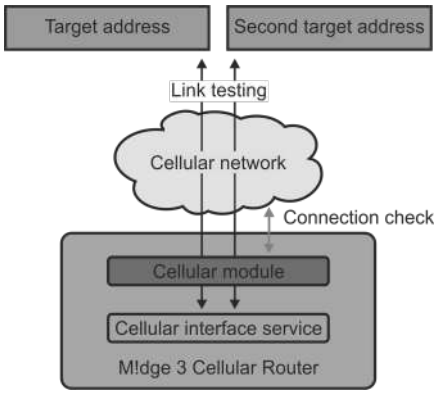
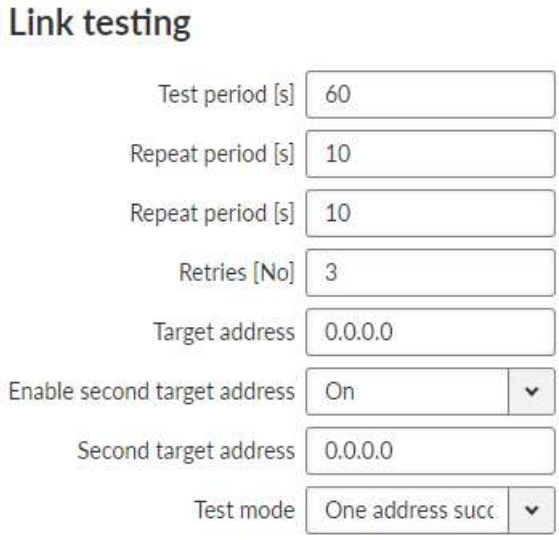


Fig. 7.4: Schema de testare a legăturilor

Setări de testare a legăturilor pentru MAIN (EXT):



Perioada de testare [s]

Număr {3 – 3600}, implicit = 60
Perioada de timp în care conexiunea este testată.

Perioada de repetare [s]

Număr {3 – 3600}, implicit = 10
Dacă testul nu a reușit, conexiunea este testată din nou după o perioadă de timp definită.

Reîncercări [Nu]

Numărul {1 – 20}, implicit = 3
Numărul de teste eșuate, după care linkul este declarat nefuncțional.

Adresa țintă

Adresă IP, implicită = 0.0.0.0
Adresă IP primară testată.

Activați a doua adresă țintă

Caseta listă {On; Off}, implicit = „Activat”

Activează/dezactivează testarea celei de-a doua adrese IP.

A doua adresă țintă

Adresă IP, implicită = 0.0.0.0

Adresă IP secundară testată.

Modul de testare

Caseta listă {One address succeeds; Ambele adrese reușesc}, implicit = „O adresă reușește”

Definește succesul testului:

• O singură adresă reușește - o singură adresă este suficientă pentru a trece testul.

• Ambele adrese au succes - ambele adrese trebuie să treacă testul.

Nota

Dacă conexiunea la cartela SIM eșuează (lipsă SIM, PIN greșit), toate profilurile care folosesc acel SIM vor fi blocate. Dacă toate profilurile sunt blocate, întregul serviciu de interfață celulară va fi blocat.

7.1.4.1.4. Schimbarea profilului

În cazul unei defecțiuni a profilului de rulare curent, modulul comută automat la altul (dacă este definit). Dacă modulul nu mai are profiluri definite la care să comutați, se comută înapoi la primul. După o perioadă de timp definită, modulul poate încerca din nou să se reconecteze prin primul profil (independent de coada de profil). Această secțiune apare numai dacă este parametru ***Schimbarea profilului*** este setat pe „Pornit”.

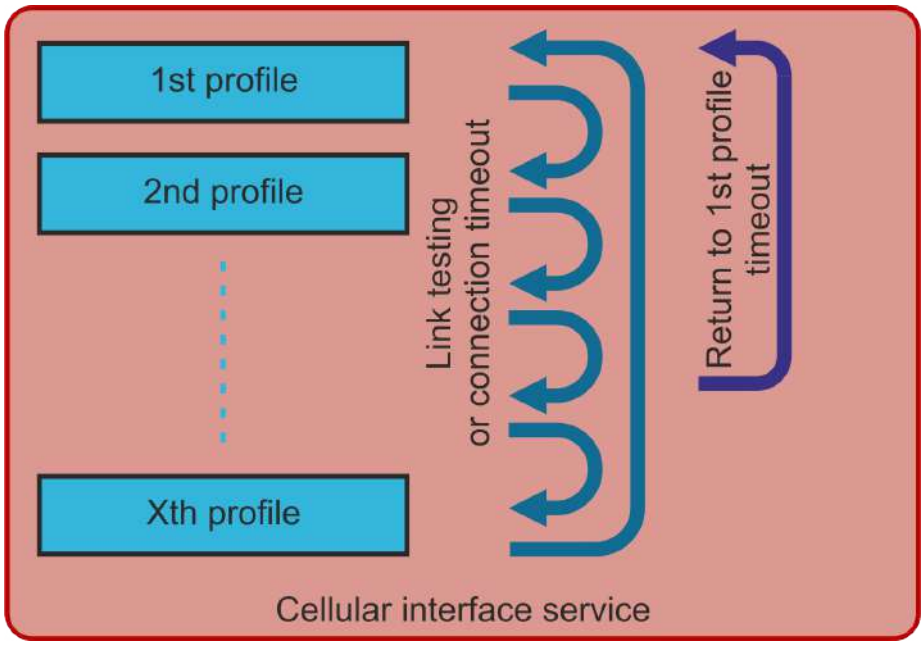
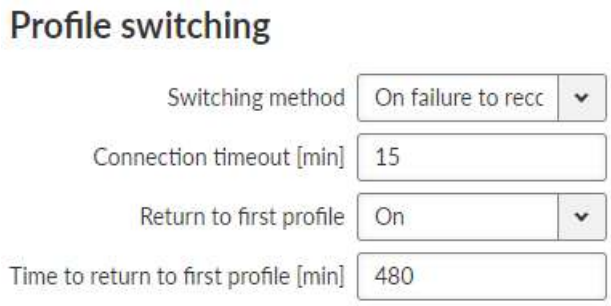


Fig. 7.5: Schema de testare a legăturilor



Metoda de comutare

Caseta listă {La prima eșec; La eșec la reconectare, On timeout}, implicit = „La prima eșec” Definește modul de comutare la următorul profil, atunci când conexiunea eșuează.

- La prima defecţiune - după prima defecţiune, modulul comută la alt profil.
- La eșec la reconectare - după defecțiune, modulul încearcă să se reconecteze. Dacă reconectarea nu reușește, modulul comută la alt profil.
- On timeout - modulul continuă să se reconecteze la profilul său curent pentru perioada de timp în care expiră (parametrul**Timeout conexiune [min]**).

Timeout conexiune [min]

Numărul {3 – 60}, implicit = 15

Perioada de timp în care modulul așteaptă conectarea (după deschiderea inițială a interfeței).

Reveniți la primul profil

Caseta listă {On; Off}, implicit = „Activat”

Când este activat, modulul va reveni la primul său profil după o perioadă de timp definită.

Timp pentru a reveni la primul profil [min]

Numărul {5 – 10080}, implicit = 480

Perioada de timp, după care profilul actual este comutat înapoi la primul.

7.1.4.2. SIM1 și SIM2

Filele SIM1 și SIM2 conțin aceeași setare pentru SIM1 și, respectiv, SIM2.

Protecție PIN

Caseta listă {On; Off}, implicit = „Dezactivat”

Activează/Dezactivează protecția PIN al modulului SIM. Trebuie să fie pornit dacă este necesar codul PIN. Parametrul este ignorat dacă SIM-ul nu necesită un PIN.

codul PIN

Șir {0000 – 9999}, implicit = „0000”

PIN-ul este utilizat numai când protecția PIN este Activată și modulul necesită codul PIN.

7.1.4.3. Cooperare cu alte servicii

Firewall L3

Parametrii**Interfață de intrare**şi**Interfață de ieșire**poate filtra traficul fie care vine în WWAN, fie care pleacă în WWAN (List box WWAN sau EXT).

NAT

- SNAT - parametru**Interfață de ieșire**poate filtra traficul (List box WWAN sau EXT).
  Regulile SNAT (setările utilizatorului) au prioritate mai mare decât regulile MASQUERADE în această secțiune (parametru**Mascaradă**).

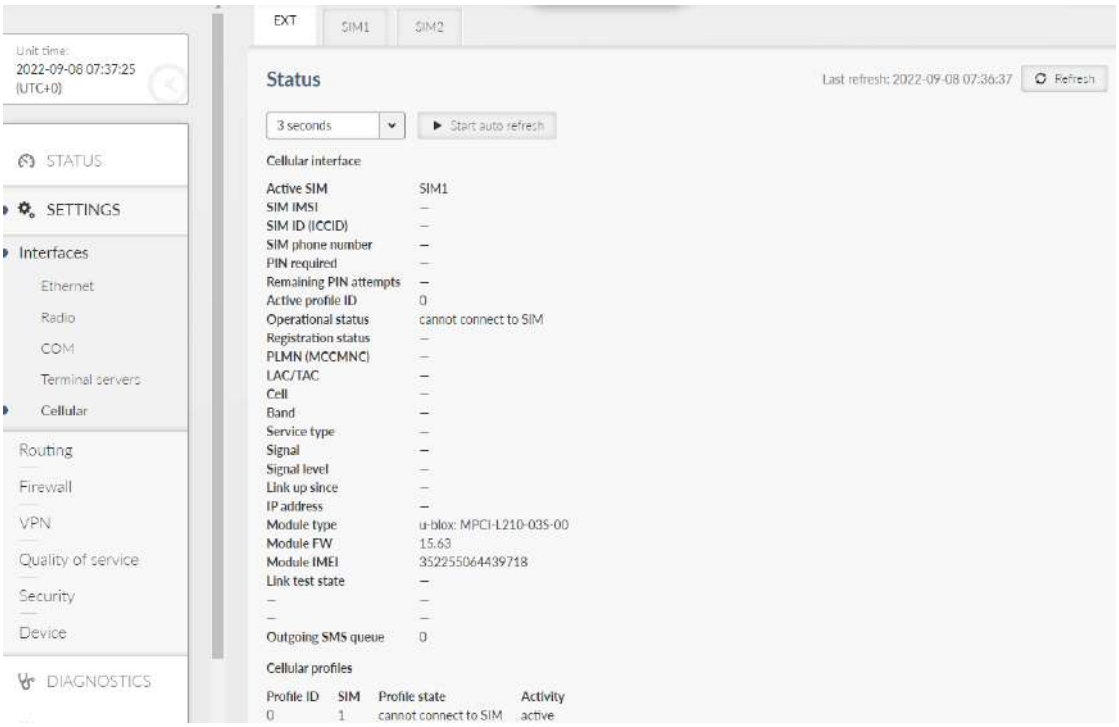
- DNAT - parametru**Interfață de intrare**poate filtra traficul (List box WWAN sau EXT).

IPsec

Regulile automate ale MASQUERADE nu suprascriu adresa sursă a pachetelor, care sunt încapsulate în IPsec.
Se recomandă ca IPsec să activeze MOBIKE, dacă este ghidat prin Cellular.

7.1.4.4. Stare

Valorile sunt afișate din momentul deschiderii meniului SETĂRI. Valorile pot fi actualizate folosind butonul Refresh.



Sunt disponibile informații comune de stare și informații despre SIM-uri.

Tab. 7.1: Niveluri de semnal pentru servicii individuale

Nivelul semnalului	Culoare LED	2G: RSSI	3G: RSCP	4G: RSRP
Slab / Fără semnal	Roşu	<= -95 dBm	<= -100 dBm	<= -100 dBm
Mediu	Portocale	- 95 până la -84 dBm	- 100 până la -89 dBm	- 100 până la -80 dBm
Bun	Verde	- 84 dBm <=	- 89 dBm <=	- 80 dBm <=

Nota

Când se utilizează ambele antene, sistemul măsoară nivelul semnalului pe fiecare antenă și folosește semnalul mai puternic. Dacă ANT1 este deconectat, deteriorat și ANT2 este conectat, meniul

(culoarea LED-ului) va afișa nivelul semnalului de la ANT2, dar comunicarea de transmisie (Tx) nu va fi posibilă. Consultați *subcapitolul 7.1.4.1.3* pentru instrucțiuni de testare a legăturilor.

7.1.5. Client PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) este un protocol de rețea care încapsulează cadre PPP în cadre Ethernet. Protocolul PPP în sine este deja descris printre *protocoale seriale*. Cu PPPoE, distingem între două faze de bază: „Descoperire” și „Sesiune PPP”.

Faza de descoperire
Scopul principal al fazei de descoperire PPPoE este de a obține informații esențiale pentru stabilirea fazei de sesiune PPP. Aceste informații includ adresa MAC a dispozitivului peer și ID-ul sesiunii PPPoE.

Faza de sesiune PPP
Scopul principal al fazei de sesiune PPP este de a stabili și menține o conexiune între client și server. Această fază utilizează cadre PPP standard pentru schimbul de date. Toate cadrele din această fază poartă o valoare ETHER_TYPE de 0x8864 și sunt considerate unicast Ethernet.

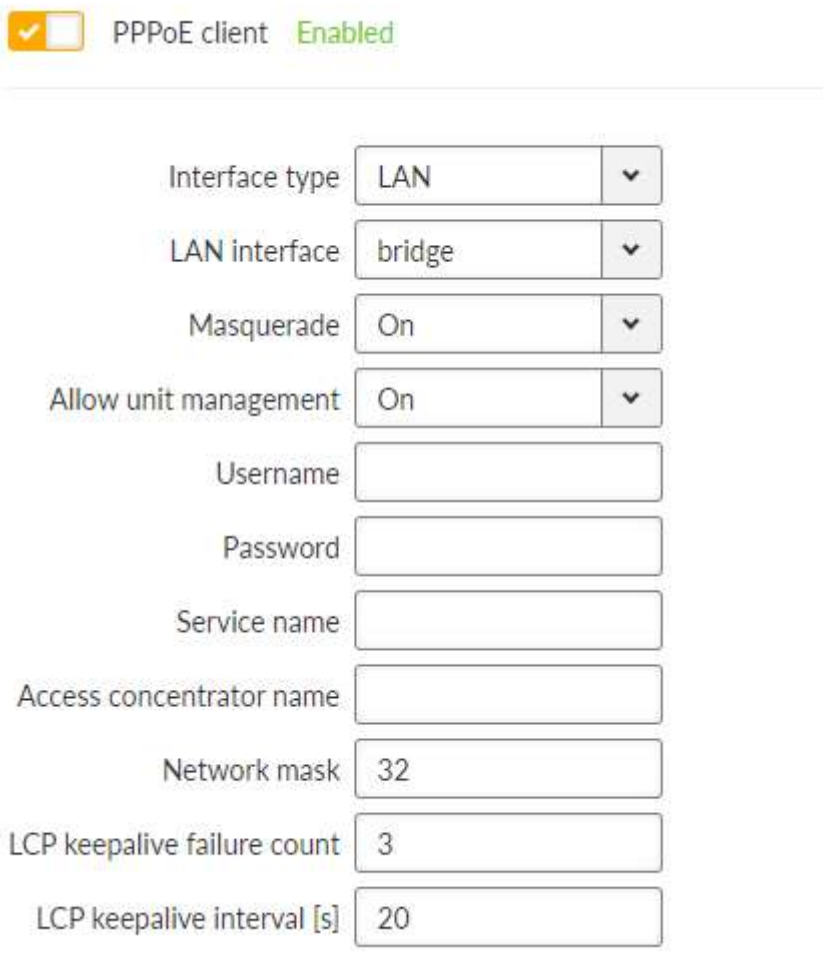


Fig. 7.6: SETĂRI>Interfețe>Client PPPoE

Tipul de interfață
Caseta listă {LAN; VLAN}, implicit = „LAN”

Acest parametru specifică din ce tabel va fi selectată interfața folosind un nume.

• LAN - Numele interfeței LAN care va fi utilizată pentru stabilirea conexiunii PPPoE.

• VLAN - Numele interfeței VLAN care va fi utilizată pentru stabilirea conexiunii PPPoE.

Mascarade

Caseta listă {On; Off}, implicit = „Activat”

Activează/dezactivează SNAT (mascarade) pe pachetele trimise prin interfața PPP.

Cu masquerade, pachetele de ieșire de la stație prin interfața PPP au adresa sursă rescrisă la adresa atribuită acestei interfețe. Pachetele returnate sunt apoi direcționate corect înapoi prin stație.

Permite gestionarea unității

Caseta listă {On; Off}, implicit = „Activat”

Permite gestionarea unității prin interfața PPP.

Nume de utilizator

Șir {până la 64 de caractere}, implicit = <gol>

Numele de utilizator care va fi folosit pentru autentificarea cu peer-ul, indiferent de protocolul necesar.

Parolă

Șir {până la 64 de caractere}, implicit = <gol>

Parola care trebuie utilizată pentru autentificarea cu peer-ul, indiferent de protocolul necesar.

Nume serviciu

Șir {până la 64 de caractere}, implicit = <gol>

Numele serviciului care va fi folosit la căutarea serverului la care să se conecteze.

Accesați numele concentratorului

Șir {până la 64 de caractere}, implicit = <gol>

Numele serverului la care să se conecteze.

Mască de rețea

Număr {0 – 32}, implicit = 0

Folosit împreună cu adresa IP a peer-ului pentru a determina intervalul de destinație al regulii de rutare care indică către interfața PPP.

Număr de erori LCP Keepalive

Număr {0 – 255}, implicit = 3 (dezactivat dacă 0)

O valoare diferită de zero specifică numărul maxim de mesaje de solicitare LCP trimise înainte ca peer-ul să fie considerat deconectat și conexiunea să fie terminată.

Interval de menținere LCP

Număr {0 – 255}, implicit = 10

Intervalul pentru trimiterea mesajelor de solicitare LCP, la care peer-ul răspunde în mod normal cu un mesaj de răspuns LCP.

Acest parametru poate fi utilizat împreună cu numărul de erori LCP keepalive pentru a detecta dacă peer-ul este conectat.

Acest parametru este activ numai atunci când numărul de erori LCP keepalive este mai mare de 0.

7.1.6. Wifi

M!DGE3 oferă opțional o interfață Wi-Fi celulară folosind modulul Wi-Fi încorporat. Interfața Wi-Fi poate fi utilizată în**Mod punct de acces (AP).**numai. Modul client nu este implementat.

7.1.6.1. Setări

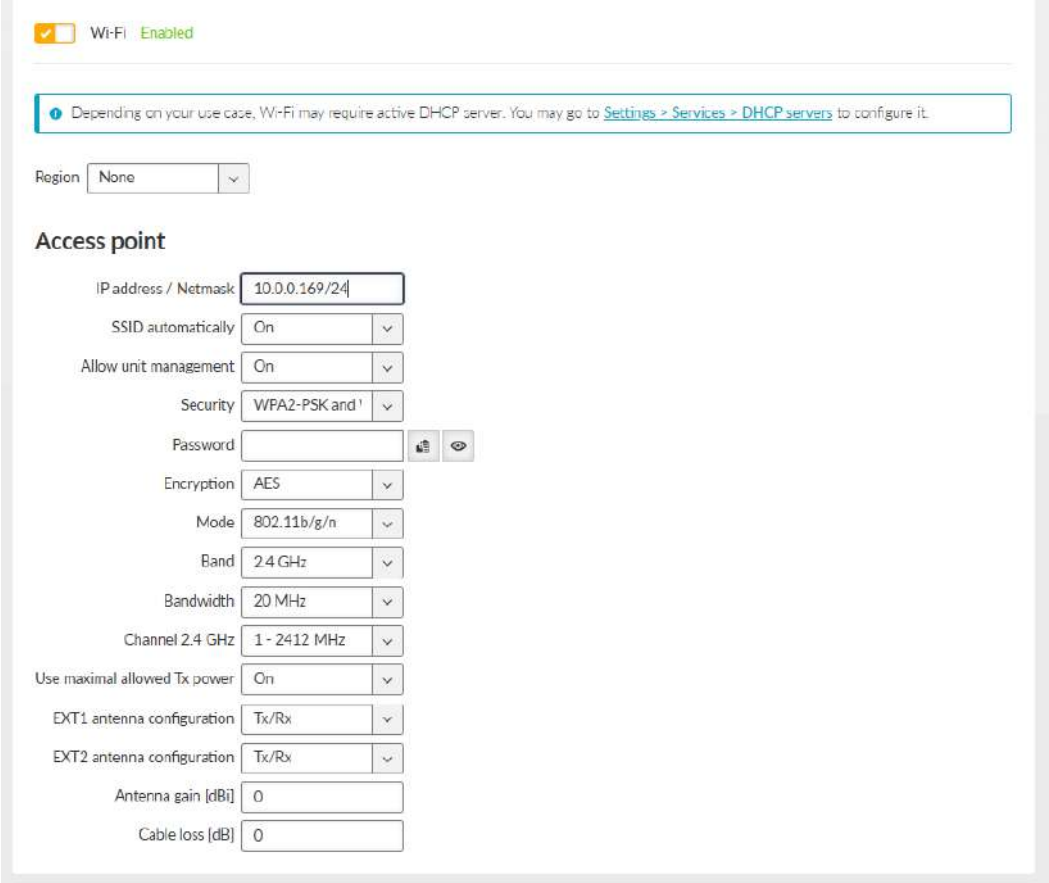


Fig. 7.7: SETĂRI>Interfețe>Wi-Fi

Activați/Dezactivați wifi

Caseta de selectare {On; Off}, implicit =
„Off” Activează/Dezactivează Wi-Fi.

Regiune

Casetă listă {Țări ISO 3166-1 alpha-2}, implicit = „Niciuna”
Setarea regiunii în care este operată unitatea. Scopul este de a activa orice restricții regionale privind puterea de transmisie. Aceste restricții variază în funcție de regiune și de banda de transmisie. Valoarea specifică a EIRP maxim permisă în regiunea selectată poate fi verificată în Status - valoarea „PII maxim permis [dBm]”.

Adresă IP/Mască de rețea

Adresă IP, implicită = „10.0.0.169”
Mască de rețea {0-32}, implicită = „24”
Adresa IP a interfeței Wi-Fi nu trebuie să intre în conflict cu un alt interval de adrese.

Permite gestionarea unității

Caseta listă {On; Off}, implicit = „Activat”

Permite accesul la gestionarea unității prin interfața Wi-Fi.

Securitate

Casetă listă {Dezactivat, WPA-PSK (vehicul), WPA2-PSK, WPA-PSK (vehicul) și WPA2-PSK, WPA3-SAE, WPA2-PSK și WPA3-SAE}, implicit = „WPA2-PSK și WPA3-SAE”
Securitatea rețelei Wi-Fi.

Parolă

Șir {până la 63 de caractere}, implicit = <gol> Parolă
pentru a vă conecta la punctul de acces Wi-Fi.

Criptare

Caseta de listă {TKIP (vehicul), AES (implicit), TKIP (vehicul) și AES}, implicit =
criptare AES rețelei Wi-Fi.

Modul

Caseta listă {802.11a, 802.11b, 802.11b/g, 802.11b/g/n, 802.11a/n, 802.11a/n/ac}, implicit = 802.11b/g/n
IEEE 802.11 modulul în care va funcționa modulul Wi-Fi

Bandă

Caseta listă {2,4 GHz, 5 GHz}, implicit = Banda de
2,4 GHz în care va funcționa modulul Wi-Fi.

Bandwitdh

Caseta listă {20 MHz ,40 MHz, 80 MHz}, implicit = 20 MHz
lățime de bandă a rețelei Wi-Fi.

Canal 2,4 GHz

Casetă listă {1 - 2412 MHz, 2 - 2417 MHz, 3 - 2422 MHz, 4 - 2427 MHz, 5 - 2432 MHz, 6 - 2437 MHz, 7 - 2442 MHz, 8 - 2447 MHz, 9 - 2452 MHz, 9 - 2452 MHz, 10 - 2452 MHz, 10 - 2432 MHz, 10 - 2437 MHz - 2467 MHz, 13 - 2472 MHz, 14 - 2484 MHz}, implicit = 1 - 2412 MHz
Canal de rețea Wi-Fi de 2,4 GHz. Opțiunile disponibile depind de setările lățimii de bandă Wi-Fi.

Canal 5 GHz

Casetă listă {36 - 5180 MHz , 40 - 5200 MHz, 44 - 5220 MHz, 48 - 5240 MHz, 52 - 5260 MHz, 56 - 5280 MHz, 60 - 5300 MHz, 64 - 5320 MHz, 100 - 520 MHz, 100 - 5260 MHz 108 - 5540 MHz, 112 - 5560 MHz, 116 - 5580 MHz, 120 - 5600 MHz, 124 - 5620 MHz, 128 - 5640 MHz, 132 - 5660 MHz, 136 - 5680 MHz, 57040 MHz, 517040 MHz, 128 - 5640 MHz MHz, 149 - 5745 MHz, 153 - 5765 MHz, 157
- 5785 MHz, 161 - 5805 MHz, 165 - 5825 MHz}, implicit = 36 - 5180 MHz
Canal de rețea Wi-Fi de 5 GHz. Opțiunile disponibile depind de setările lățimii de bandă Wi-Fi.

Nota
Canalele care necesită DFS nu pot fi utilizate.

Utilizați puterea Tx maximă permisă

Caseta listă {On; Off}, implicit = „Activat”
Selectarea automată a puterii de transmisie a modulului Wi-Fi. Dacă
opțiunea este dezactivată:

Putere Tx maximă

Număr complet {0-16}, implicit = „16” [dBm]
Puterea de transmisie a modulului Wi-Fi.

Configurarea antenei EXT1

Caseta listă {Off, Tx, Rx, Tx/Rx}, implicit = „Tx/Rx”

Determină funcționalitatea antenei conectate la modulul Wi-Fi prin portul EXT1.

Configurarea antenei EXT2

Caseta listă {Off, Tx, Rx, Tx/Rx}, implicit = „Tx/Rx”

Determină funcționalitatea antenei conectate la modulul Wi-Fi prin portul EXT2.

Câștig antenă

Număr complet {0-30}, implicit = „0” [dBi]

Câștig al antenei conectate la modulul Wi-Fi.

Folosit la calculul puterii de transmisie a modulului Wi-Fi cu semn pozitiv.

Pierderea cablului Număr complet {0-30}, implicit = „0” [dB]

Folosit la calculul puterii de transmisie a modulului Wi-Fi cu semn negativ.

7.1.6.2. Control acces

Tabelul de control acces vă permite să controlați accesul clientului pe baza adreselor MAC ale acestora.

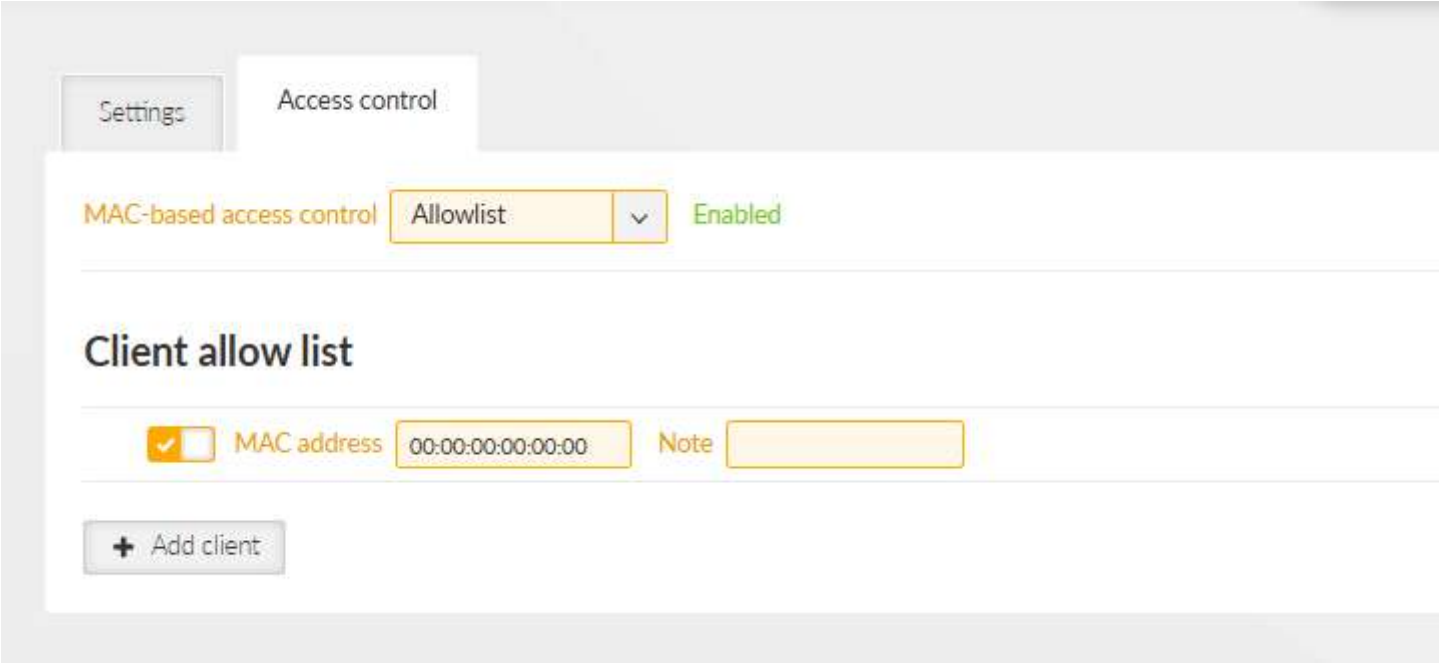


Fig. 7.8: SETĂRI>Interfețe>Wi-Fi>Control acces

Controlul accesului bazat pe MAC

Caseta listă {Off, Allowlist, Blocklist}, implicit = „Dezactivat”

Gestionați accesul clientului după adresa MAC.

Lista permisă

Permite doar clienții cu adrese MAC în listă, alții sunt blocați.

Lista blocată

Blochează clienții cu adrese MAC în listă, altele sunt permise

Activați/Dezactivați clientul

Caseta listă {On; Off}, implicit = „Pornit” Activează o regulă pentru o anumită adresă MAC.

adresa MAC Adresă MAC , implicită = 00:00:00:00:00:00

adresa MAC a clientului

7.1.6.3. Cooperare cu alte servicii

Server DHCP

Este posibil să rulați un server DHCP prin interfața Wi-Fi.
Serverul DHCP trebuie configurat să aloce adrese IP din intervalul de adrese specificat de configurare**Adresă IP/Mască de rețea**în interfața Wi-Fi.

Evenimente

Conexiunea și deconectarea clienților la Wi-Fi AP este raportată de evenimentele „WiFi AP (EXT) raportează clientul conectat” și „WiFi AP (EXT) raportează clientul deconectat”

Firewall L3

Firewall-ul poate filtra traficul care vine de la interfața Wi-Fi utilizând opțiunea „EXT” din setările interfeței I/O.

HotStandby

Wi-Fi este dezactivat în modul pasiv și activat în modul activ.
În modul pasiv, sursa de alimentare a modulului este activă, dar interfața Wi-Fi nu este activă.

Manager de linkuri

Interfața Wi-Fi poate fi utilizată în Link Manager ca interfață WWAN (EXT) la configurarea conexiunii.

NAPT

Regulile SNAT și DNAT pot modifica traficul care trece prin interfața Wi-Fi utilizând opțiunea „EXT” din setările interfeței I/O.
Numele interfeței Wi-Fi poate fi utilizat la setarea manuală a numelui interfeței I/O ("Altele"), dar numai dacă Wi-Fi (EXT) este activ.

Modul de repaus

Când modul de repaus este activ, este posibil să amânați punerea dispozitivului în stare de repaus dacă traficul utilizatorului este detectat pe interfața Wi-Fi.

7.2. Dirijare

Routerul M!DGE3 acceptă atât rutare IP statică, cât și dinamică.

Rutarea statică se bazează pe definiția fixă – statică – a tabelelor de rutare. Rutarea dinamică se bazează pe crearea și actualizarea automată a tabelelor de rutare. În acest scop sunt utilizate diverse metode și protocoale. Protocoalele standard de rutare Babel, OSPF și BGP sunt disponibile în rețelele M!DGE3.

A fost adăugată opțiunea de gestionare a legăturilor permițând setarea trecerii legăturii principale (în cazul eșecului acesteia) la o legătură de rezervă existentă prin modificări automate ale regulilor de rutare.

Nota

Datorită rutării interne statice către clienți, OpenVPN L3 este incompatibil cu protocoalele de rutare dinamică. Rutarea dinamică prin interfața OpenVPN L3 nu va funcționa.

Nota

M!DGE3e nu acceptă funcționalități de rutare dinamică (Gestionare link, Babel, OSPF, BGP).

7.2.1. Static

M!DGE3 funcționează ca un router IP standard cu mai multe interfețe independente: interfețe de rețea (unând interfețe Ethernet fizice), porturi COM, servere terminale, interfață celulară etc. Fiecare dintre interfețe are propriile adrese IP și măști. Toate pachetele IP sunt procesate conform tabelului de rutare.

Pe interfața de rețea poate fi definit un număr nelimitat de subrețele. Ele sunt direcționate independent.

Porturile COM sunt tratate în mod standard ca dispozitive router, mesajele le pot fi livrate ca datagrame UDP către numerele de porturi UDP selectate. Adresa IP de destinație a portului COM este IP-ul unei interfețe de rețea (interfețe Ethernet). Sursa adresei IP a pachetelor de ieșire din porturile COM este egală cu adresa IP a interfeței (interfața de rețea) prin care a fost trimis pachetul. Adresa sursă poate fi, de asemenea, atribuită**Adresă locală de sursă preferată**valoare - vezi descrierea de mai jos. Interfața de ieșire este determinată în tabelul de rutare în funcție de IP-ul de destinație.

Schema de adresare IP poate fi aleasă în mod arbitrar, se aplică doar restricția 127.0.0.0/8 și 192.0.2.233/30 și 192.0.2.228/30. Se poate întâmpla ca și adresele ulterioare din Subrețeaua 192.0.2.0/24 conform RFC5737 poate fi rezervată pentru utilizare internă în viitor.

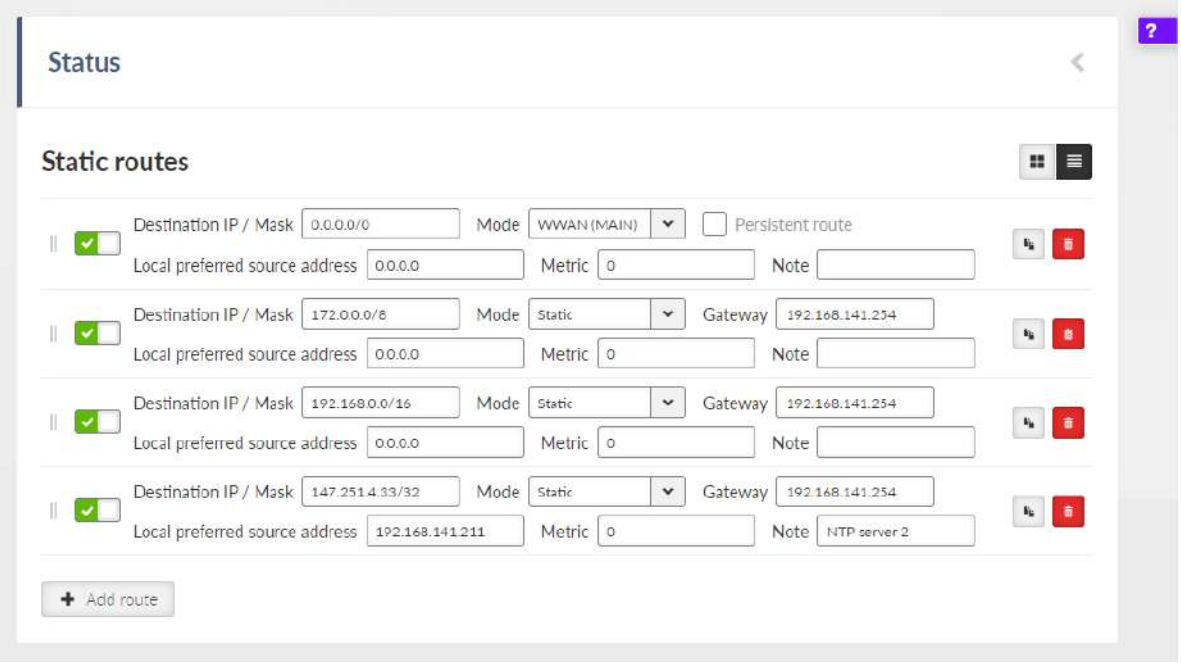


Fig. 7.9: SETĂRI > Rutare > Static

Activ

{Activat/Dezactivat}

Activează / dezactivează regula.

IP de destinație / mască

Adresă IP, implicită = 0.0.0.0/0

Fiecare pachet IP, primit de M!DGE3 prin orice interfață (ETH, COM, ...), are o adresă IP de destinație. M!DGE3 (router) redirecționează pachetul primit fie direct către adresa IP de destinație, fie către Gateway-ul respectiv, conform tabelului de rutare. Orice Gateway trebuie să fie în rețeaua definită de IP și Masca uneia dintre interfețe, altfel pachetul este aruncat.

Fiecare element din tabelul de rutare definește un Gateway (ruta, următorul hop) pentru rețea (grup de adrese) definit de IP-ul de destinație și Masca. Când Gateway-ul pentru adresa IP de destinație respectivă nu este găsit în tabelul de rutare, pachetul este redirecționat către gateway-ul implicit, când gateway-ul implicit (0.0.0.0/0) nu este definit, pachetul este aruncat.

Rețeaua (Destination IP și Mask) este scrisă în format CIDR, de exemplu 10.11.12.0/24.

Nota

Rețeaua definită prin aceeași combinație de IP de destinație și Mască nu poate fi utilizată pentru două reguli diferite.

Modul

Caseta listă {Static; WWAN (PRINCIPALA); WWAN (EXT); PPP1; PPP2; PPP3; Manager link; PPPoE Client}, implicit = Static

- Static - Folosit pentru regulile de rutare IP statică.
- WWAN (PRINCIPALA); WWAN (EXT) - Regulă de rutare către WWAN primar/secundar, care are o adresă alocată dinamic. Următorul hop va fi direcționat prin interfața „wwan” atunci când este deschis.
- PPP1; PPP2; PPP3 - Regulă de rutare către interfața PPP asociată cu protocolul COM. Interfața poate avea o adresă alocată dinamic. Poate fi setat doar dacă portul COM corespunzător este activat și cu protocolul PPP.
- Manager link - Regulă de rutare prin link activ selectat de Manager link. Regula va fi schimbată dinamic în cazul unei modificări sau pierderi a legăturii. Poate fi setat dacă Managerul de legături este activat.
- Client PPPoE - Regulă de rutare către interfața PPP creată de clientul PPPoE. Interfața are o adresă alocată dinamic. Poate fi setat doar dacă clientul PPPoE este activ.

Adresă locală de sursă preferată

Adresă IP, implicită = 0.0.0.0

Adresă IP locală utilizată ca adresă sursă pentru pachetele care provin din unitatea locală M!DGE3 care sunt rutate prin această regulă de rutare. Ar putea fi, de exemplu, pachete care provin de la portul COM sau de la Terminal Server. Dacă adresa este setată la 0.0.0.0, aceasta nu este considerată activă. Adresa IP trebuie să aparțină interfețelor de rețea.

Metric

Număr {0 – 4294967294}, implicit = 0

Valoarea valorii regulii de rutare.

Nota

Puteți adăuga un nume la fiecare rută cu comentariile dvs. de până la 16 caractere (UTF8 este acceptat) pentru confortul dvs.

Traseu persistent

Caseta listă {On; Off}, implicit = Off

Setează persistența (timpul prezenței) regulii de rutare dinamică.

Acest parametru este disponibil numai dacă este parametru**Modul**este setat la „WWAN (MAIN)” sau „WWAN (EXT)”.

• Pornit - Regula de rutare este întotdeauna prezentă. Când interfața WWAN este închisă, raportează mesaje „inaccesibile” (prin ICMP) și traficul nu poate fi prins de o altă regulă.

• Off - Regula de rutare există numai dacă interfața WWAN este deschisă. Dacă este închis, traficul poate fi prins de o altă regulă.

7.2.1.1. Adrese loopback

Tabelul de adrese de loopback conține adrese IP ale M!DGE3, care sunt setate pe interfața de loopback ca adrese „suport” independente de interfața specifică. Numărul maxim de adrese este 256. Adresele loopback pot fi utile, de exemplu, pentru scopuri specifice de rutare sau trafic de date specifice utilizatorului. De exemplu, folosind reguli de rutare diferite pentru trafic diferit.

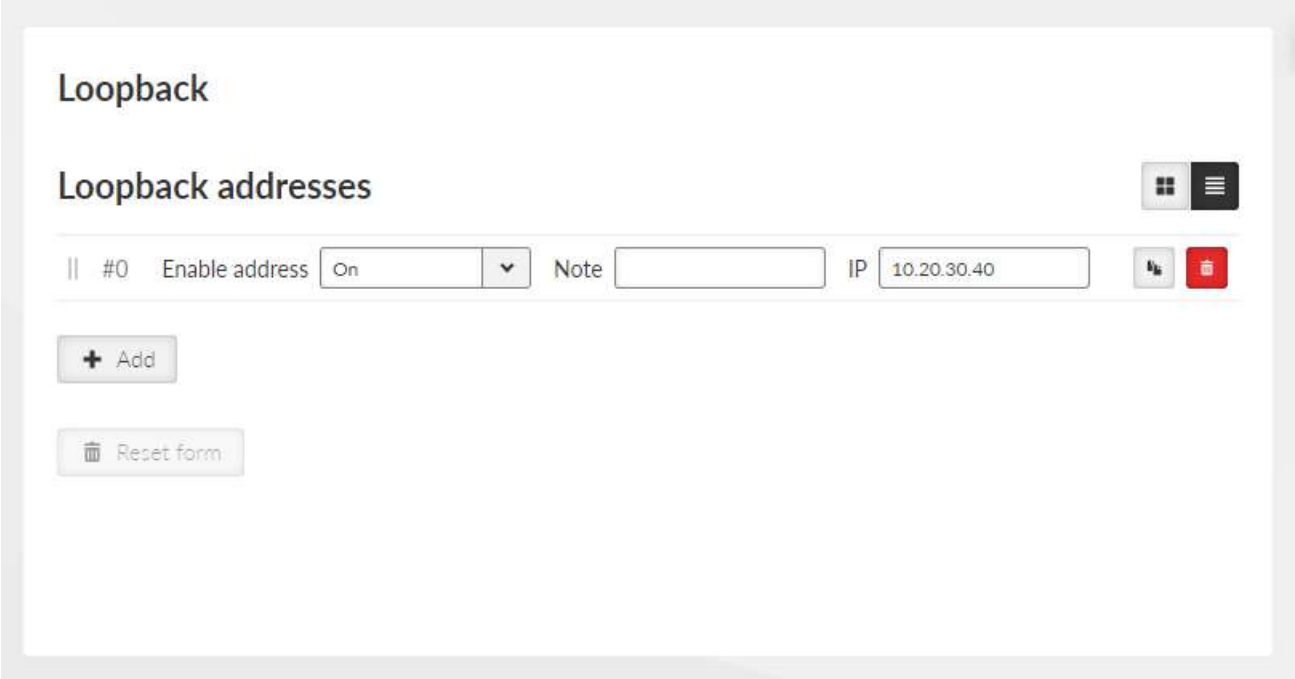


Fig. 7.10: AVANZAT > Interfețe > Loopback

Activați adresa
Caseta listă {On; Off}, implicit = „Activat”

Nota
Comentariu optional.

IP
Adresă IP, implicită = 0.0.0.0
Definește adresa IP care va fi setată pe interfața de loop-back. Masca este automat /32.

7.2.2. Gestionarea linkurilor

Managerul de legături este un mecanism care oferă comutarea mai multor legături alternative preconfigurate (rute alternative). Comutatorul de legătură este declanșat în cazul eșecului legăturii active. Eșecul legăturii poate fi detectat pasiv – prin verificarea stării interfeței legăturii (vezi**Interfață urmărită**parametru) și activ prin ping ICMP (vezi **Testarea linkurilor**parametru).

Testarea legăturilor este activă pe legătura activă în prezent și pe toate linkurile cu prioritate mai mare (pentru a detecta când sunt disponibile din nou). Legăturile cu prioritate inferioară pot fi, de asemenea, testate (vezi**Testați linkul de rezervă**parametru). Când legătura curentă eșuează, managerul de legături trece la următoarea legătură funcțională cu prioritate inferioară. Dacă legătura nu este verificată (parametrul de testare a legăturii de rezervă este dezactivat), se presupune că este funcțional. Regulile de rutare sunt actualizate automat la comutarea legăturii.

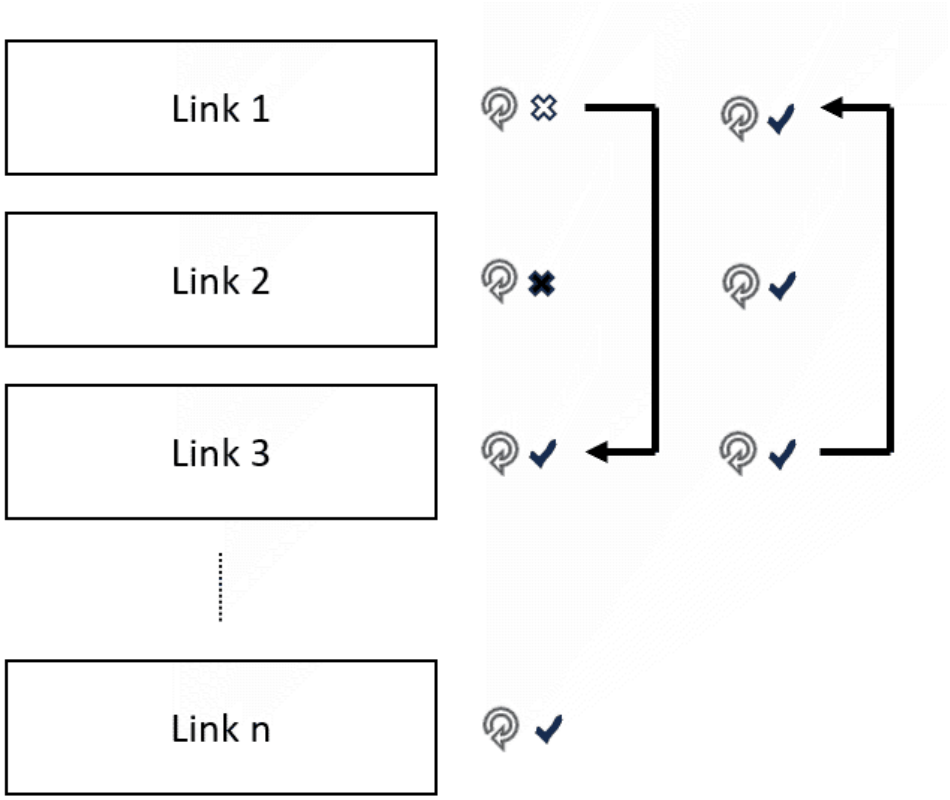


Fig. 7.11: Schema de gestionare a legăturilor

7.2.2.1. Parametrii

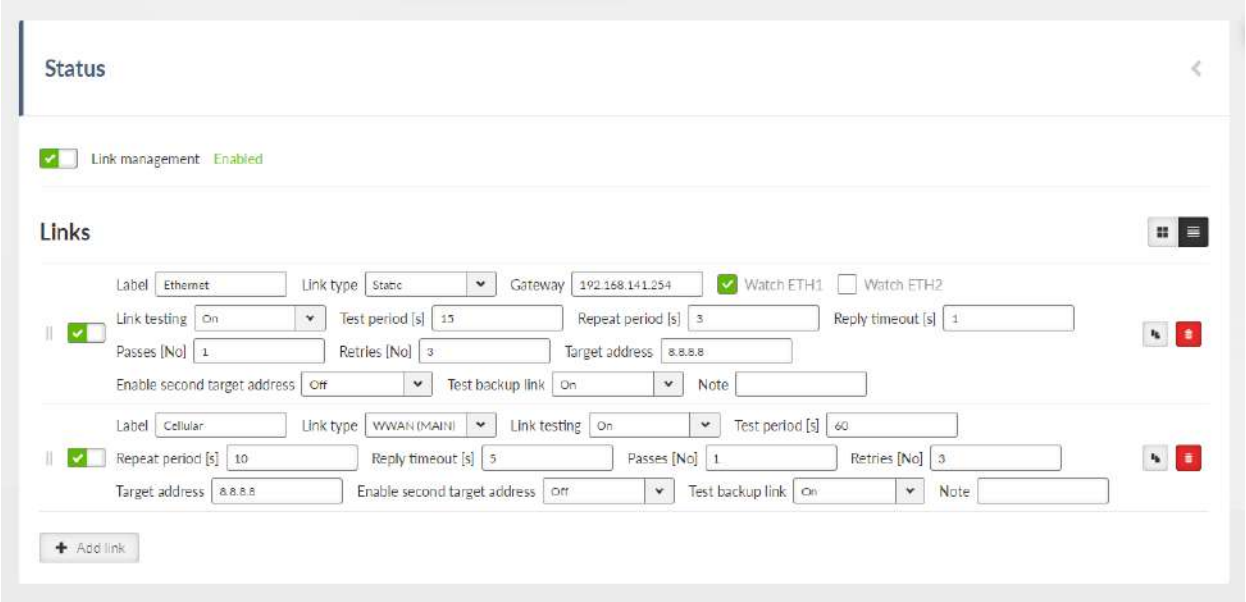


Fig. 7.12: SETĂRI > Rutare > Gestionare legături

Activați Managerul de linkuri

Activează/dezactivează Managerul de legături

control IPsec

Caseta listă {Off; Activat}, implicit = „Dezactivat”

Activează/dezactivează legarea între o legătură și un anumit tunel IPsec. Această opțiune este disponibilă numai când IPsec este activat și configurat. Parametru de configurare: SETĂRI > VPN > IPsec > Asocieri IPsec >**Modul de management**oferă două opțiuni:

Manager link (Master)

Una dintre asociațiile IPsec este declarată ca**Maestru**. Selectorii de trafic (CHILD SA) definesc traficul de criptat.

Manager link (Sclav)

Toate celelalte asociații sunt declarate ca**Sclav**. Nu sunt definiți selectori de trafic pentru un astfel de tunel. Se folosesc selectoarele de trafic ale Masterului.

7.2.2.2. Legături

Fiecare link alternativ este configurat separat. Prioritatea legăturilor individuale este determinată de ordinea acestora. Numărul maxim de linkuri este 16.

Stările posibile ale link-ului:

- **jos**: linkul nu este prezent
- **netestată**: linkul este prezent, nu este disponibil încă un rezultat al testului de link
- **Sus**: link-ul este prezent și funcțional. Dacă testul Link este activat, rezultatul testului este de succes
- **testul eșuat**: linkul este prezent, testul Link a eșuat

Roluri posibile de link:

- **activ**: link-ul este selectat ca fiind activ. Doar unul dintre linkuri poate fi activ
- **backup**: linkul are o prioritate mai mică în comparație cu linkul activ

- **respins**: linkul are o prioritate mai mare în comparație cu linkul activ, dar nu poate fi utilizat

Activați linkul

Activează/dezactivează legătura individuală

Eticheta

Șir {a..z A..Z 0..9 @ _ -}, max 42 caractere, implicit = „LINK” Numele linkului care este utilizat în informațiile de stare și jurnalele de sistem

Tip link

Caseta listă {Static; WWAN (PRINCIPALA); WWAN (EXT)}, implicit = „Static”

- Static – interfețe LAN, GRE sau radio
  Gateway-ul trebuie configurat. Interfețele urmărite pot fi selectate.

- WWAN (atât MAIN, cât și EXT)
  Starea interfeței celulare este verificată automat (inclusiv Cellular Link tester – când este activată). Starea conexiunii este activată în cazul în care interfața celulară este activată și testul conexiunii a reușit. IP-ul gateway-ului nu este configurat manual - este utilizată adresa IP atribuită de rețeaua celulară.

Poarta de acces

Adresă IP, implicită = 0.0.0.0

Adresă de hop următor (gateway) pentru tipul static al conexiunii

Interfață urmărită (ETH1 .. ETH5, Radio)

Activează/dezactivează verificarea interfeței individuale. Când toate interfețele verificate sunt oprite, starea conexiunii este**jos**

Starea conexiunii ETHxeste verificat pentru opțiunile ETH1-ETH5. Stabilirea cu succes a interfeței Radio este verificată pentru opțiunea Radio

Asocierea IPsec

Caseta listă {lista de ID-uri de egalitate disponibile}, implicit = primul ID de egalitate

Când**control IPsec**este Activat, legătura individuală este asociată cu un tunel IPsec individual definit de acesta**ID peer**. În acest caz, tunelul IPsec individual este activat/dezactivat împreună cu legătura respectivă. Este comutat automat înapoi la legătura cu prioritate mai mare odată ce este restaurată.

Testarea linkurilor

Caseta listă {Off; Activat}, implicit = „Dezactivat”

Activează testarea legăturilor active. Legăturile sunt testate folosind pachete de eco ICMP

Perioada de testare [s]

Număr {3 – 3600}, implicit = 60

Perioada de testare a unui link care se află în**Sus**stat

Perioada de repetare [s]

Număr {3 – 3600}, implicit = 10

Perioada de testare a unei legături care trebuie testată (deasupra legăturii active) și în mod normal nu este testată sau testul a eșuat

Timp expirat răspuns [s]

Număr {1 – 60}, implicit = 5

ICMP ping răspuns timeout

Treci [Nu]

Numărul {1 – 20}, implicit = 1

Număr neîntrerupt de teste (ping-uri) reușite după care starea legăturii este în sus

Reîncercări [Nu]

Numărul {1 – 20}, implicit = 3

Număr neîntrerupt de teste eșuate (ping-uri) după care este starea conexiunii**testul eșuat**

Adresa țintă

Adresă IP, implicită = 0.0.0.0

Adresă IP primară testată

Activați a doua adresă țintă

Caseta listă {Off; Activat}, implicit = „Dezactivat”

Activează/dezactivează testarea celei de-a doua adrese IP

A doua adresă țintă

Adresă IP, implicită = 0.0.0.0

Adresă IP secundară testată.

Modul de testare

Caseta listă {One address succeeds; Ambele adrese reușesc}, implicit = „O adresă reușește”

• O singură adresă reușește - o singură adresă este suficientă pentru a trece testul

• Ambele adrese au succes - ambele adrese trebuie să treacă testul

Testați linkul de rezervă

Caseta listă {Off; Activat}, implicit = „Dezactivat”

Permite testarea legăturii active a unei legături cu prioritate mai mică în comparație cu**activ**legătură

Nota

Șir {0–42 caractere}, implicit = <gol>

NOTĂ: Managerul de legături nu este un protocol de rutare dinamică complet (cum ar fi Babel, OSPF sau BGP). Protocoalele de rutare dinamică asigură sincronizarea rutelor alternative de pachete în întreaga rețea. Managerul de legături funcționează local – nu există nicio sincronizare a legăturii (rutei) selectate cu alte unități din rețea. Rețineți acest fapt atunci când planificați configurarea Managerului de legături în rețeaua dvs. și păstrați comportamentul simetric. Un efect al faptului că fiecare instanță Link Manager din rețea funcționează independent este traficul asimetric ocazional la comutarea rutelor alternative.

NOTĂ: Pachetele de testare a legăturii (ecou ICMP la adresele de testare) trebuie să testeze de fapt legătura individuală (să fie direcționată prin aceasta). În combinație cu controlul IPsec, nu trebuie să se întâmple ca tunelul IPsec să capteze și să cripteze aceste pachete. În caz contrar, poate apărea un comportament nestandard (oscilație, testul nu reușește niciodată, blocat pe o legătură ruptă).

7.2.2.3. Stare

Zona de informații despre stare oferă o listă cu toate linkurile activate. Starea legăturii și rolul legăturii (vezi descrierea de mai sus) oferă informații despre starea individuală a fiecărei legături și care dintre legături este cea activă.

7.2.3. Babel

Babel este un protocol de rutare cu vector de distanță care evită buclele, care este proiectat să fie robust și eficient atât în rețelele care utilizează rutarea bazată pe prefixe, cât și în rețelele care utilizează rutarea plată („rețele mesh”), precum și ambele

în rețelele cu fir relativ stabile și în rețelele fără fir foarte dinamice (pentru mai multe informații vezi *RFC 6126*[2]).

Babel este, de asemenea, un protocol de rutare dinamică pentru rețelele IP (Internet Protocol). Este un Protocol Gateway Interior (IGP) care funcționează într-un sistem autonom. Se bazează pe protocolul OSPF (vezi capitolul următor pentru descrierea protocolului OSPF) cu următoarele diferențe:

• Funcționează într-un singur sistem autonom

• Babel oferă atât interfața de rețea cu fir, cât și fără fir

Protocolul Babel este utilizat în mod obișnuit în cadrul hopurilor de rețea sau al altor rețele cu debit limitat de date.

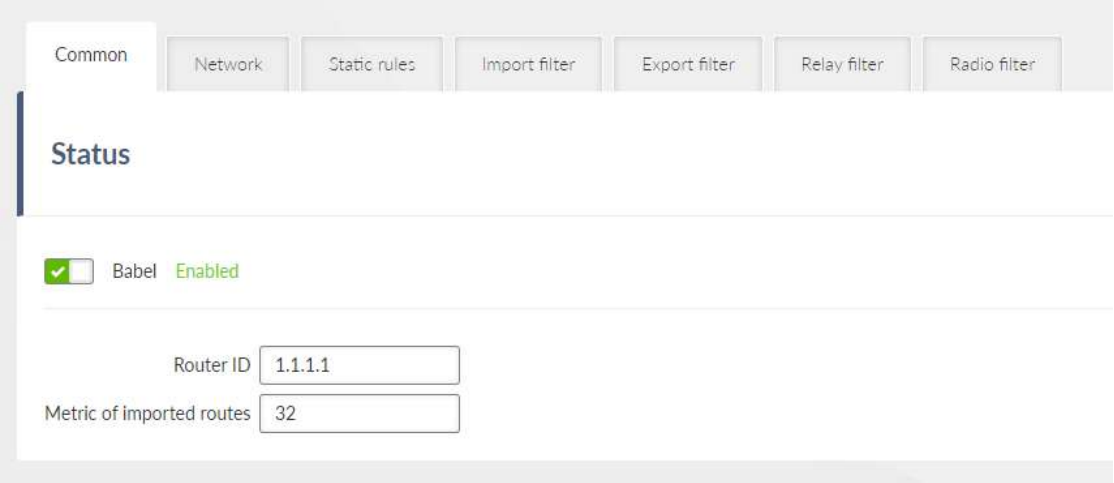


Fig. 7.13: SETĂRI > Rută > Babel

Parametrii de configurare sunt descriși în capitolele următoare. Mai multe scenarii de cazuri de utilizare și exemple de configurare sunt descrise în *Notă de aplicare Babel*[3].

7.2.3.1. Descriere

Fiecare router definește ce interfețe sunt folosite pentru protocolul Babel pentru a căuta vecinii de rețea disponibili.

Fiecare router transmite și primește periodic pachete Hello pentru a determina existența și calitatea unei conexiuni la nodurile rețelei vecine. Informațiile rezultate despre rutele (căile) disponibile și calitatea acestora sunt partajate în rețea. Tabelele de rutare sunt schimbate periodic și, de asemenea, după actualizarea lor.

Decizia căii de rutare se bazează pe o „metrică”:

• Metrica este setată pe fiecare interfață. Acesta reflectă un „preț” pentru recepția pachetului. Cu cât valoarea metricii este mai mare, cu atât este mai dezavantajoasă utilizarea unei astfel de căi.

• Valoarea maximă este 65535.

Există două tipuri de interfețe:

[2] https://datatracker.ietf.org/doc/html/rfc6126.html#section-1.1
[3] https://www.racom.eu/download/hw/ripex/free/eng/1_application/ripex2-app-bab-en.pdf

• Cablat: presupune o legătură fiabilă. Calitatea este evaluată în funcție de numărul de pachete Hello primite. Dacă limita configurată de pachete pierdute este depășită, linia este considerată ca fiind în jos.

• Wireless: presupune o calitate variabilă a conexiunii. Prețul interfeței crește treptat cu fiecare pachet Hello pierdut, până când linia este declarată în jos.

Decizia de rutare:

• SETĂRI > Rutare > Rute statice sunt valide chiar dacă rutarea dinamică este activată. Protocoalele de rutare dinamică „exportă" regulile de rutare rezultate în Linux și sunt adăugate regulilor de rutare existente (statice).

• Decizia particulară de rutare ia masca IP ca regulă de decizie primară (masca mai îngustă are o prioritate mai mare) și metrica ca regulă de decizie secundară. Regulile primite de la protocoalele dinamice au o metrică mai mare în comparație cu rutele statice (au întotdeauna cea mai mare metrică posibilă).

• Valorile interne ale protocoalelor dinamice sunt procesate numai în interiorul acestora. Doar setul final de reguli de rutare este exportat către routerul Linux.

Exemplul 1:

• SETĂRI > Rută > Regulă rute statice: 0.0.0.0/0 → 10.10.1.11

• Regula dinamică: 192.168.1.0/24 → 192.168.11.1 metric 32

• Pachetul cu DST 192.168.1.42 va fi direcționat către 192.168.11.1 deoarece regula dinamică are o mască mai îngustă.

Exemplul 2 – situație similară cu o regulă statică suplimentară:

• SETĂRI > Rută > Regulă rute statice: 0.0.0.0/0 → 10.10.1.11

• SETĂRI > Rută > Regulă rute statice: 192.168.1.0/24 → 192.168.22.1

• Regula dinamică: 192.168.1.0/24 → 192.168.11.1 metric 32

• Pachetul cu DST 192.168.1.42 va fi direcționat către 192.168.22.1 deoarece regula statică are aceeași mască, dar o metrică mai bună.

7.2.3.2. Comun - Setări comune

ID router

Adresă IP, implicită = 0.0.0.0

Unitatea M!DGE3 acționează în rețeaua Babel ca un router dinamic. Fiecare router este identificat printr-un ID având formatul adresei IP. Această adresă IP nu trebuie să fie „reală”.

ID-ul routerului este partajat în toate protocoalele dinamice.

ID aleator

Caseta listă {On; Off}, implicit = „Dezactivat”

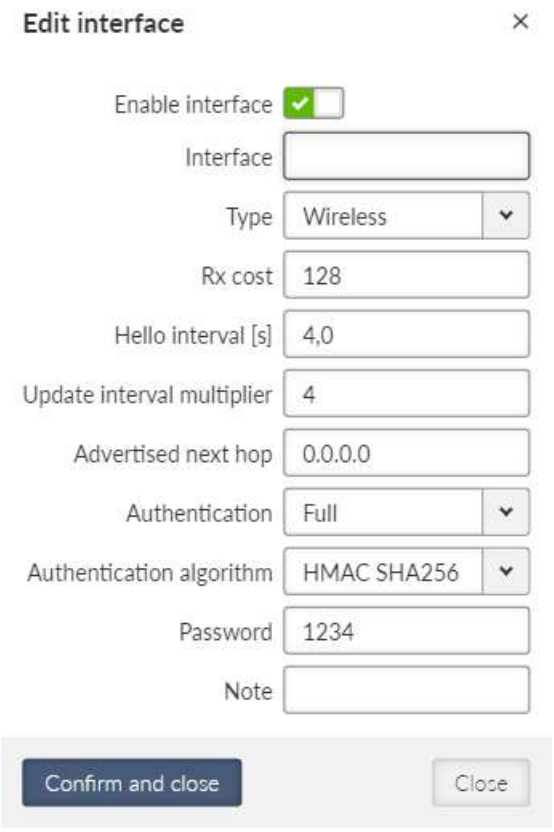
Funcție avansată: Permite randomizarea celor 4 octeți superiori ai identificării routerului. Cei 4 octeți inferiori sunt setați de a**ID router**parametru. Această caracteristică poate fi utilizată în cazul în care nodul Babel este adesea repornit, ceea ce duce la refuzul mesajelor sale de către vecinii săi.

Oferta de rutare

Caseta listă {On; Off}, implicit = „Activat”

Permite propagarea regulilor de rutare dobândite de la vecini. Când sunt dezactivate, regulile de intrare nu sunt propagate către alte routere și acest router se comportă ca un terminal de punct final - căile de rețea sunt pornite sau terminate într-un astfel de punct, dar nu traversează.

7.2.3.3. Rețea - Interfețe



Activ

Caseta listă {On; Off}, implicit = „Off”

Activează/dezactivează interfața.

Interfață

String {a..z A..Z 0..9}, max 16 caractere, implicit = <empty>Interfețe care vor fi folosite de Babel pentru căutarea conexiunilor disponibile. Trebuie folosit numele unei interfețe de unitate existentă. Pot fi utilizate următoarele interfețe:

LAN – trebuie folosit prefixul „if_” urmat de numele interfeței de rețea, de exemplu „if_LAN-141”

VLAN – trebuie folosit prefixul „dacă_”, urmat de numele interfeței de rețea, „.' punct și numărul VLAN, de exemplu, „if_LAN-141.29”

GRE L3 – „gre_tunX” unde „X” este numărul tunelului, începând de la zero

Cellular – „wwan”, „ext”

MTU de interfață trebuie să fie de 1280 de octeți sau mai mare pentru a opera corect protocolul Babel.

Tip

Caseta listă {Wired; Wireless}, implicit = „Wireless”

Tipul de interfață de rețea și, de asemenea, tipul de evaluare a stării legăturii. Starea legăturii „prin cablu” este evaluată prin verificarea limitei de pachete Hello primite – dacă nu este îndeplinită, legătura este considerată ca fiind inactivă. Starea conexiunii „Wireless” este evaluată folosind criteriile ETX – fiecare pachet Hello pierdut scade treptat valoarea conexiunii.

Costul Rx

Număr {1 – 65534}, implicit = 128

Costul utilizării acestei interfețe pentru a primi pachete de la un vecin. Se adaugă la metrica cale Babel.

Salut limită

Numărul {1 – 16}, implicit = 12

Numai pentru interfața „cablată”: limită de pachete Hello primite din cele 16 așteptate; dacă nu este îndeplinită, linkul este considerat ca fiind inactiv.

Salut interval

Număr {0,1 – 327,0}, implicit = 4,0 Interval (în secunde) de trimitere a pachetelor Hello.

Actualizați multiplicatorul de intervale

Numărul {2 – 30}, implicit = 4

Intervalul de trimitere a pachetelor de actualizare a tabelului de rutare – pentru a partaja informațiile despre topologia rețelei în rețeaua Babel. Intervalul de actualizare se calculează ca o multiplicare a acestui parametru și **Salut interval**. Durata maximă a intervalului de actualizare (după înmulțire) este de 655 de secunde.

Anunțul următor hop

Adresă IP, implicită = 0.0.0.0

Aceasta este adresa Următorul hop care este anunțată vecinilor pentru a fi direcționată prin această interfață. În cazul în care această interfață deservește mai multe adrese IP, acest parametru permite selectarea care dintre adrese ar trebui să fie utilizate pentru această stație în tabelele de rutare a vecinilor de rețea.

Autentificare

Caseta listă {Niciuna; Deplin; Numai semn}, implicit = „Niciunul”

Activează autentificarea pachetelor de protocol Babel.

- Complet - pachetele sunt semnate în timpul transferului și semnătura este validată la primirea pachetelor primite. Pachetele cu semnătură nevalidă sunt raportate în jurnal și aruncate.

- Semnează doar - Pachetele sunt semnate în timpul transferului și semnătura este validată la primirea pachetelor primite. Pachetele cu semnătură nevalidă sunt raportate în jurnal și acceptate. Aceste setări sunt destinate comutării treptate a rețelei în modul sigur.

Algoritm de autentificare

Caseta listă {HMAC SHA256; HMAC SHA384; HMAC SHA512; BLAKE2s-128; BLAKE2s-256; BLAKE2b-256; BLAKE2b-512}, implicit = „HMAC SHA256”

Selectează algoritmul de autentificare. Acest parametru apare numai dacă este parametru**Autentificare**este setat fie la „Complet” fie la „Doar semn”.

Fiecare algoritm are propria sa limită de lungime a parolei.

HMAC SHA256 - lungime șir de până la 128 de caractere HMAC SHA384 - lungime de șir de până la 128 de caractere HMAC SHA512 - lungime de șir de până la 128 de caractere BLAKE2s-128 - lungime de șir de până la 32 de caractere BLAKE2s-256 - lungime de șir de până la 32 de caractere Lungime de șir de până la 32 de caractere BLAKE2s-26 de caractere BLAKE2b-512 - lungime șir de până la 64 de caractere

Parolă

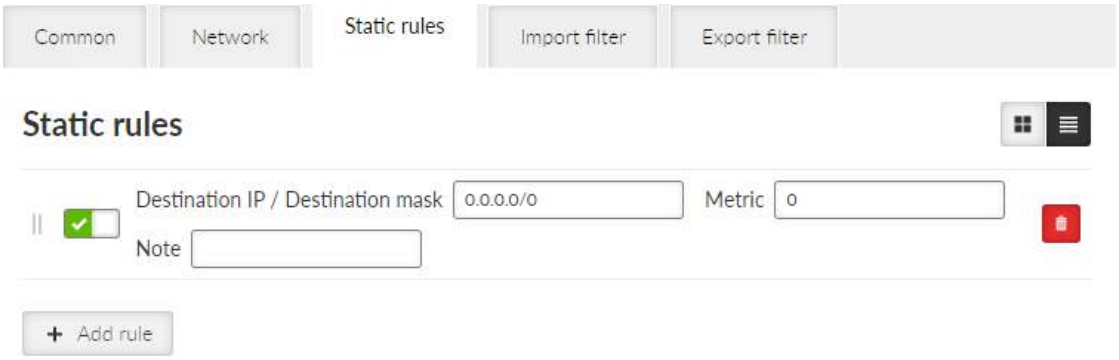
Șir {până la 128 de caractere}

Definește parola pentru autentificarea pachetelor.

Nota

Comentariu optional.

7.2.3.4. Reguli statice



Reguli de rutare statică predefinite pentru a fi exportate prin protocolul Babel. Numărul maxim de reguli este 256.

Activ

Caseta listă {On; Off}, implicit = „Pornit” Activează/ dezactivează regula de rutare statică.

Destination IP / Destination mask

Adresă IP, implicită = 0.0.0.0/0

Adresa IP și masca care definesc intervalul de adrese ale regulii de rutare exportate.

Metric

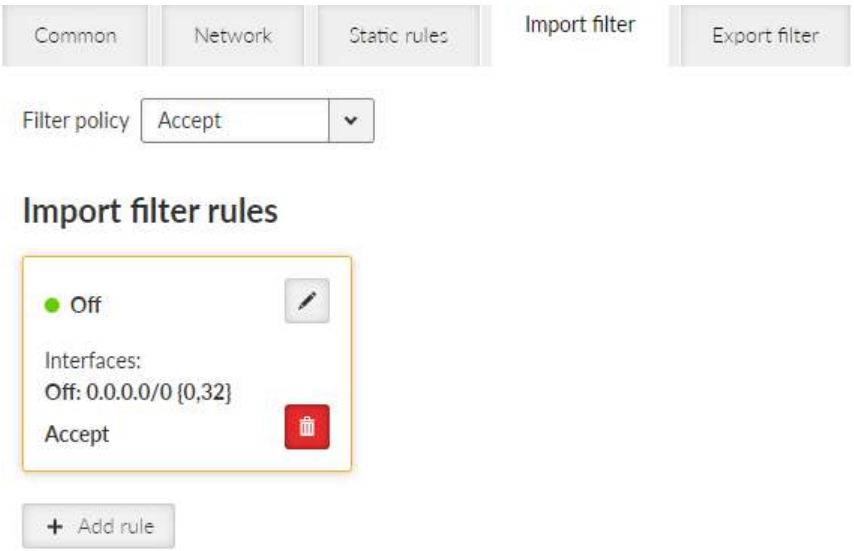
Număr {0 – 65534}, implicit = 0

Valoarea valorii regulii de rutare. Cu cât valoarea este mai mare, cu atât calea este mai „scumplă”.

Nota

Comentariu optional.

7.2.3.5. Filtru de import



Reguli de filtru de import Babel. Ordinea regulilor contează. Fiecare regulă de rutare de intrare este procesată de acele filtre de import. Numărul maxim de reguli de filtrare este 256.

Activ

Caseta listă {On; Off}, implicit = „Pornit”
Activează/dezactivează regula de filtrare.

Rețeaua de filtrare

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”
Metoda de comparare a intervalului țintă al regulii de rutare.

Adresă IP / mască

Adresă IP / mască, implicit = 0.0.0.0/0
Adresa IP și masca care definesc intervalul de rețea de comparat.

Masca de la

Număr {0 – 32}, implicit = 0

Masca la

Număr {0 – 32}, implicit = 32
Definirea intervalului activat al lungimii măștii regulii de rutare procesată.
Exemple:

Regula 0.0.0.0/0 {0,32} captează toate intervalele IP

Regula 192.168.1.0/24 {24,32} captează 192.168.1.0/24 și toate subrețelele (de exemplu 192.168.1.1/32)

Regula 10.9.8.7/32 {8,32} captează toate intervalele cu masca mai lungă de 8 care acoperă adresa 10.9.8.7 (de ex. 10.9.0.0/16)

Acţiune

Caseta listă {Accept; Respinge; Pass}, implicit = „Accept”
Tip de acțiune care trebuie efectuată atunci când regulile de filtrare de mai sus se potrivesc cu regula de rutare de intrare.
Când este selectat „Pass”, procesarea pachetului continuă.

Setați preferința

Caseta listă {On; Off}, implicit = „Dezactivat”

Când este activată, Preferința (vezi parametrul următor) va fi setată la această regulă.

Preferinţă

Număr {0 – 65535}, implicit = 210

Preferința regulilor de rutare din tabelul de rutare (a fi utilizat când Setați preferința este activată). Cu cât numărul este mai mare, cu atât preferința este mai bună.

Adresă locală de sursă preferată

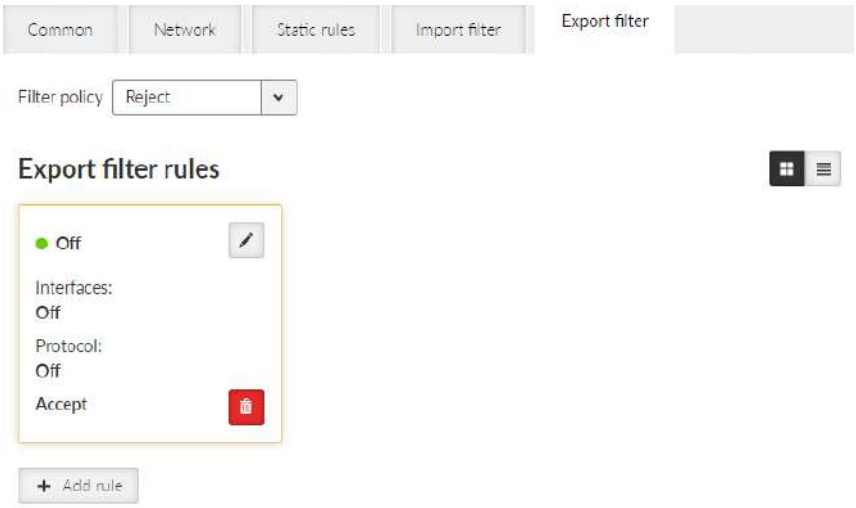
Adresă IP, implicită = 0.0.0.0

Adresă IP sursă preferată pentru pachetele generate local. Când este dezactivată (este utilizată valoarea implicită 0.0.0.0), adresa IP sursă este setată în funcție de interfața de ieșire.

Nota

Comentariu optional.

7.2.3.6. Export filtru



Regulile de filtru de export Babel definesc un set de reguli de rutare care urmează să fie exportate de la unitate către alte routere Babel. Ordinea regulilor contează. Numărul maxim de reguli de filtrare este 256.

Activ

Caseta listă {On; Off}, implicit = „Pornit”

Activează/dezactivează regula de filtrare.

Rețeaua de filtrare

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

Metoda de comparare a intervalului țintă al regulii de rutare.

Adresă IP / mască

Adresă IP / mască, implicit = 0.0.0.0/0

Adresa IP și masca care definesc intervalul de rețea de comparat.

Masca de la

Număr {0 – 32}, implicit = 0

Masca la

Număr {0 – 32}, implicit = 32

Definirea intervalului activat al lungimii măștii regulii de rutare procesată.

Protocol de filtrare

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

Selectează modul în care este comparat protocolul sursă a regulii de rutare.

Protocol

Caseta listă {System; BGP; BGP extern; BGP intern; OSPF}, implicit = „Sistem” Selectarea originii protocolului. „Sistem” – reprezintă regulile din tabelul obișnuit de rutare.

Filtrați calea BGP

Caseta listă {Off; Este gol; Nu este gol}, implicit = „Dezactivat”

Compară calea regulii de rutare BGP dacă este goală (adică regula provine din acest AS).

Filtrați sursa OSPF

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

Selectează modul în care este comparată regula de rutare din protocolul OSPF.

sursa OSPF

Caseta listă {Internă; Inter-zonă; Tip extern 1; Tip extern 2}, implicit = surse OSPF „Tip extern 2”. „Internă” – înseamnă o regulă generată intern (de exemplu, intervalul de interfață). „Inter-zonă” – reprezintă regula generată la granițele zonei.

Filtrați eticheta OSPF

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

metoda de filtrare bazată pe etichete OSPF.

Eticheta OSPF

Numărul {0 – (2^{32}-1)}, implicit = 0

etichetă OSPF de comparat.

Acțiune

Caseta listă {Accept; Respinge; Pass}, implicit = „Accept”

Definește ce acțiune este întreprinsă cu privire la regula de rutare. Când este selectat „Pass”, procesarea pachetului continuă.

Metric din alt protocol

Caseta listă {Off; BGP MED; OSPF Metrica 1; OSPF Metric 2; Suma metrice OSPF}, implicit = „Dezactivat”

Definește sursa valorii.

Off: static**Metric**este utilizată valoarea (vezi următorul parametru).

BGP MED: reguli MED (Multi-Exit Discriminator) din protocolul BGP. Dacă regula nu are o valoare MED completată, este utilizată valoarea metrică statică.

Valoarea OSPF 1: Metrica de tip OSPF 1. Dacă regula nu are o valoare de măsurare completată, este utilizată valoarea statică a Metricii.

Măsură OSPF 2: Metrica de tip OSPF 2. Dacă regula nu are o valoare de metrică completată, este utilizată valoarea Metric statică.

Suma metric OSPF: Suma metricilor OSPF de tip 1 a tip 2. Dacă regula nu are ambele valori completate de metrică, este utilizată valoarea statică a metricii.

Metric

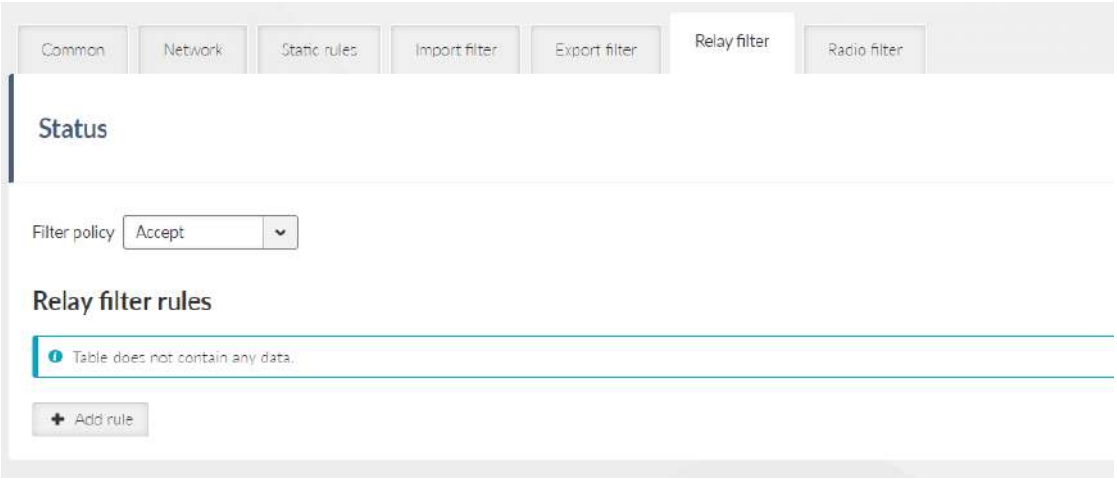
Număr {0 – 65534}, implicit = 0

Valoarea valorii regulii de rutare. Cu cât valoarea este mai mare, cu atât calea este mai „scumplă”.

Nota

Comentariu optional.

7.2.3.7. Filtru releu



Filtrul releu selectează ce se întâmplă cu o regulă primită de la o altă instanță Babel care nu a fost capturată în filtru. Când sunt dezactivate, regulile nu vor fi redirecționate către alte routere și această stație va acționa ca un terminal unde căile încep și se termină în rețeaua Babel, dar nu trec prin ea.

Politica de filtrare — Caseta listă {Accept; Reject}, implicit = „Accept”

Activați regula — Caseta de selectare {On; Off}, implicit = „Activat”

Activează/dezactivează regula

Rețeaua de filtrare — Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

Selectează o modalitate de a compara intervalul țintă al regulii

IP de rețea/Mască de rețea — Adresă IP / mască, implicit = 0.0.0.0/0

Compară prefixul rețelei

Masca de la — Număr {0 – 32}, implicit = 0

Definește intervalul de lungime permis al măștii pentru regula comparată

Masca la — Număr {0 – 32}, implicit = 32

Definește intervalul de lungime permis al măștii pentru regula comparată

Acţiune — Caseta listă {Accept; Respinge; Pass}, implicit = „Accept”

Alege ce să facă cu regula

Valoarea filtrului — Caseta listă {Off; <; <=; >=; >}, implicit = „Dezactivat”

Selectează o modalitate de a compara regulile de valori Babel

Valoare metrică — Număr {0 – 65534}, implicit = 0

Valoarea comparată a valorii regulii

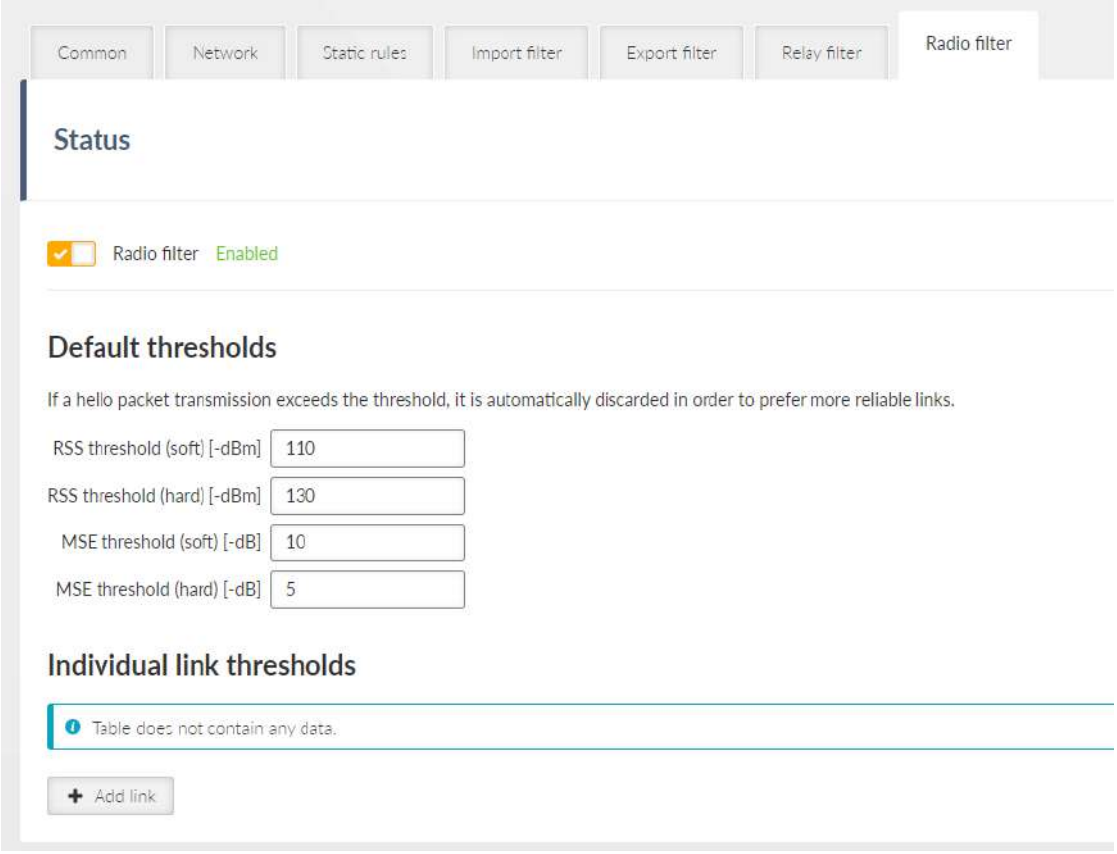
Măriți valoarea — Caseta listă {Off; Activat}, implicit = „Dezactivat”

Permite creșterea valorilor regulilor Babel la redirecționare. Este folosit pentru a penaliza căile prin acest router. Numai când Acțiune este Accept sau Treci.

Valoare adăugată — Număr {1 – 65534}, implicit = 1

Valoarea adăugată la valoarea regulii

7.2.3.8. Filtru radio



Conține setările globale ale filtrului de pachete Babel Hello în protocolul radio. Această funcție este utilizată pentru a exclude legăturile radio care nu au o putere sau o calitate a semnalului suficientă pentru a transmite pachete standard, deși pachetele scurte de salut vin bine.

prag RSS (soft) — Număr {50 – 150}, implicit = 110

Limitele nivelului RSS [-dBm] ale pachetului Hello primit

Limita soft este cea mai proastă valoare sub care pachetul nu este aruncat

prag RSS (hard) — Număr {50 – 150}, implicit = 130

Limitele nivelului RSS [-dBm] ale pachetului Hello primit

Limita rigidă este cea mai bună valoare pentru a arunca întotdeauna pachetul

Nota

Trebuie să fie Soft Threshold <= Hard Threshold

Pragul MSE (soft) — Număr {0 – 60}, implicit = 10

Limitele nivelului de date MSE [-dB] ale pachetului Hello primit

Limita soft este cea mai proastă valoare sub care pachetul nu este aruncat

Pragul MSE (dur) — Număr {0 – 60}, implicit = 5

Limitele nivelului de date MSE [-dB] ale pachetului Hello primit

Limita rigidă este cea mai bună valoare pentru a arunca întotdeauna pachetul

Nota

Trebuie să fie Soft Threshold >= Hard Threshold

Activați configurarea linkului — Caseta listă {Off; Activat}, implicit = „Activat”

Activează setările individuale

IP radio omologul — Adresă IP, implicită = 0.0.0.0

	Adresa IP radio a sursei pachetului Hello pentru care se aplică setarea de filtru individual
prag RSS (soft)	Număr {50 – 150}, implicit = 110 Limitele nivelului RSS [-dBm] ale pachetului Hello primit Limita soft este cea mai proastă valoare sub care pachetul nu este aruncat
prag RSS (hard)	Număr {50 – 150}, implicit = 130 Limitele nivelului RSS [-dBm] ale pachetului Hello primit Limita rigidă este cea mai bună valoare pentru a arunca întotdeauna pachetul **Nota** Trebuie să fie Soft Threshold <= Hard Threshold
Pragul MSE (soft)	Număr {0 – 60}, implicit = 10 Limitele nivelului de date MSE [-dB] ale pachetului Hello primit Limita soft este cea mai proastă valoare sub care pachetul nu este aruncat
Pragul MSE (dur)	Număr {0 – 60}, implicit = 5 Limitele nivelului de date MSE [-dB] ale pachetului Hello primit Limita rigidă este cea mai bună valoare pentru a arunca întotdeauna pachetul **Nota** Trebuie să fie Soft Threshold >= Hard Threshold
Nota	Notă opțională

7.2.4. OSPF

Open Shortest Path First (OSPF) este un protocol de rutare pentru rețelele IP (Internet Protocol). Utilizează un algoritm de rutare a stării de legătură (LSR) și se încadrează în grupul de protocoale de gateway interior (IGP), care funcționează într-un singur sistem autonom (AS). OSPF Versiunea 2 definită în RFC 2328 (1998) pentru IPv4 este implementată în routerul RipEX. OSPF oferă rutare dinamică Layer 2. În contextul rețelelor RipEX, este utilizat de obicei pentru rutarea rețelei de backhaul.

OSPF împarte rețeaua în „zone” pentru a simplifica topologia rețelei. Există o zonă principală de „coloană vertebrală” (0.0.0.0), iar celelalte zone sunt conectate la această zonă principală prin routere de graniță.

Procesul de decizie a rutei este afectat de calea „metrică”. Există două tipuri de valori:

- Tipul Metric 1 – lungimea traseului; Se adaugă costurile de trecere a interfețelor individuale.
- Tipul Metric 2 – este configurat pe regulile care sunt exportate către OSPF din exterior. Regulile care au metrica „Tipul 2” sunt întotdeauna tratate ca fiind mai proaste (adică calea mai lungă) în comparație cu metrica „Tipul 1”.

Routerele dintr-o anumită zonă sunt întotdeauna conectate prin interfețe.

• Un interval de adrese poate fi definit pentru o interfață în care funcționează OSPF. Pot fi definite mai multe intervale de adrese (comportându-se ca o altă interfață).

• Interconectarea router la router poate fi protejată prin criptare cu parolă.

• „Cost" specific este definit pentru fiecare interfață care este adăugată la valoarea „Tip 1".

• Există mai multe tipuri de interfețe:

  ○ Stub – interfața anunță doar către OSPF: prezența și intervalele sale de adrese vor fi propagate mai departe în rețea.

  ○ Broadcast – pentru a fi utilizat în rețea în care toți participanții se aud mereu între ei (Ethernet). Routerul desemnat (DR) și DR de rezervă (BDR) sunt configurate între vecini. Ei sunt responsabili pentru propagarea actualizării (difuzare).

  ○ NBMA (Non-Broadcast Multiple Access) – pentru a fi utilizat în rețea în care doar anumiți participanți pot comunica între ei; toți participanții se aud, dar multicast nu este disponibil. DR și BDR sunt configurate.

  ○ Point2Point – rețea având doar doi participanți. Se descoperă reciproc folosind multicast.

  ○ Point2Multipoint – rețea în care doar perechile predefinite de participanți se pot auzi între ei (de exemplu, topologia în stea); multicast nu este disponibil.

• Pot fi definite reguli statice. Astfel de reguli de rutare sunt propagate în rețea de pe acest router.

• Este posibil să definiți agregarea regulilor de rutare exportate sau ascunderea regulilor de rutare specifice.

• Este posibil să se controleze regulile de rutare care sunt importate în unitatea RipEX din protocolul OSPF și pe cele care sunt exportate în protocolul OSPF de la unitate folosind „filtre".

  ○ Export filtre – pentru a controla regulile exportate de la unitate către protocolul OSPF care le propaga în continuare.

  ○ Import filtre – pentru a controla regulile importate din OSPF în unitate.

7.2.4.1. OSPF Common - Setări comune

Activ

Caseta listă {On; Off}, implicit = „Dezactivat"

Activează rutarea dinamică și protocolul OSPF.

ID router

Adresă IP, implicită = 0.0.0.0

Unitatea M!DGE3 acționează în rețeaua OSPF ca un router dinamic. Fiecare router este identificat printr-un ID având formatul adresei IP. Această adresă IP nu trebuie să fie „reală". ID-ul routerului este partajat în toate protocoalele dinamice.

ID de instanță

Număr {0 – 255}, implicit = 0

Numărul instanței protocolului OSPF. Acest număr este necesar în cazul rulării mai multor protocoale OSPF (de exemplu la granița a 2 rețele OSPF independente).

7.2.4.2. Rețea OSPF - Zone și interfețe

7.2.4.2.1. Zone și interfețe

Zonele OSPF din care face parte unitatea RipEX sunt descrise aici. Numărul maxim de zone este de 32.

Activați / Dezactivați
Activează/dezactivează zona specifică.

ID zona
Adresă IP, implicită = 0.0.0.0
Identificator de zonă OSPF. ID-ul are formatul unei adrese IP. Această adresă IP nu trebuie să fie „reală”. Valoarea „Router ID” este utilizată de obicei. Valoarea implicită de 0.0.0.0 se numește „backbone” și trebuie să fie prezentă undeva în rețeaua OSPF.

Zona stub
Faceți clic pe caseta {On; Off}, implicit = „Dezactivat”
Definește dacă zona este de tip „stub” – ceea ce înseamnă că traficul nu este direcționat printr-o astfel de zonă. Fiecare trafic este originar sau terminat în zona „stub”.

GW prestabilit stub (parametru AVANSAT)
Caseta listă {On; Off}, implicit = „Activat”
Dacă „Activat” – numai GW implicit este direcționat către zona „stub”. Din „Oprit” – rutele individuale direcționează traficul în zonă. Poate fi eficient să dezactivați acest parametru atunci când sunt prezente mai multe routere de frontieră.

Nota
Comentariu optional. Este o bună practică să introduceți un nume descriptiv pentru zonă, deoarece această valoare este afișată (când este completată) în loc de**ID zona**ca un**Zonă**nume în alte casete de dialog de configurare (de exemplu, Configurarea rețelelor).

Interfețele OSPF ale zonei OSPF respective sunt definite aici. Numărul maxim de interfețe este 128.

Activ
Caseta listă {On; Off}, implicit = „Off”
Activează/dezactivează interfața.

Interfață
Șir {a..z A..Z 0..9}, maxim 16 caractere, implicit = <gol>
Numele interfeței OSPF. Trebuie folosit numele unei interfețe de unitate existentă. Pot fi utilizate următoarele interfețe:

- LAN – trebuie folosit prefixul „if_” urmat de numele interfeței de rețea, de exemplu „if_LAN-141”
- VLAN – trebuie folosit prefixul „dacă_”, urmat de numele interfeței de rețea, „.' punct și numărul VLAN, de ex. „if_LAN-141.29”
- GRE L3 – „gre_tunX” unde „X” este numărul tunelului, începând de la zero
- Cellular – „wwan”, „ext”

Adresă IP / mască
Adresă IP / mască, implicit = 0.0.0.0/0

Adresa IP și masca intervalului de adrese peste care protocolul OSPF va funcționa pe această interfață. Valoarea implicită este 0.0.0.0/0, ceea ce înseamnă că întregul interval de adrese de pe această interfață este disponibil pentru protocolul OSPF.

Tip de rețea

Caseta listă {Broadcast; Point2Point; Punct2Multipunct; NBMA; Stub}, implicit = „Difuzare”
Definește tipul de rețea din spatele interfeței.

Cost

Număr {1 – 65535}, implicit = 10

Costul traficului prin această interfață. Cu cât costul este mai mare, cu atât este mai rău calea. Este adăugată la valoarea OSPF „Tipul 1”.

Salut interval

Număr {1 – 3600}, implicit = 10
Intervalul (în secunde) de trimitere a pachetelor Hello. Intervalul trebuie să fie același pentru toți participanții la interfața dată.

Interval de sondaj

Număr {1 – 3600}, implicit = 20
Intervalul (în secunde) de trimitere a pachetelor Hello către vecinii inactivi în interfața de tip NMBA.

Interval de retransmitere

Număr {1 – 3600}, implicit = 5
Intervalul (în secunde) de repetare a pachetelor neconfirmate.

Număr de morți

Numărul {2 – 64}, implicit = 4
Numărul de pachete Hello pierdute de la vecin pentru a trata conexiunea ca fiind întreruptă.

Securitate TTL

Caseta listă {On; Off}, implicit = „Activat” Protecție
împotriva falsificării pachetelor OSPF.

Autentificare, Parolă

Caseta listă {Niciuna; MD5 cu cheie (OSPFv2); HMAC SHA256; HMAC SHA384; HMAC SHA512}, implicit = „Niciunul”
Selectarea unei metode de autentificare a mesajelor OSPF. Parola este folosită ca cheie secretă pentru funcția hash selectată. Lungimea maximă a parolei este de 128 de caractere.

Prioritate

Număr {0 – 255}, implicit = 1

Prioritatea este utilizată pentru a selecta routerul principal sau de rezervă responsabil pentru propagarea actualizărilor de rutare. Cu cât numărul este mai mare, cu atât este mai mare prioritatea. „0” indică că routerul nu poate fi utilizat ca router principal sau de rezervă.

Utilizați difuzarea

Caseta listă {On; Off}, implicit = „Dezactivat”
Definește dacă distribuția de pachete OSPF este furnizată folosind multicast-uri (comportament implicit) sau transmisii (comportament nestandard).

Nota

Comentariu optional. Este posibil să introduceți un nume descriptiv al interfeței OSPF. Această valoare este utilizată (când este completată) în locul originaluluiInterfațăidentificarea ca anInterfațănume în alte casete de dialog de configurare (de exemplu, configurarea vecinilor).

7.2.4.2.2. Vecinii

Aici sunt definiți vecinii de rețea ale tipurilor Point2Multipoint și NBMA de interfețe OSPF. Numărul maxim de vecini este de 512.

Activ

Caseta listă {On; Off}, implicit = „Off”
Activează/dezactivează interfața.

Interfață

Caseta listă {lista interfețelor OSPF existente}
Interfața OSPF căreia îi aparține vecinul. Interfata -**Nota**valoarea este utilizată atunci când este definită. Interfata -**Interfață**valoarea este folosită altfel.

IP

Adresă IP, implicită = 0.0.0.0
Adresa IP a vecinului.

Nota

Comentariu optional.

7.2.4.2.3. Rețele

Tabelul Rețele modifică rețelele anunțate în afara zonei. Permite agregarea parțială a rețelelor în prefixele comune sau ascunderea rețelei specifice. Numărul maxim de reguli este 256.

Activ

Caseta listă {On; Off}, implicit = „Off”
Activează/dezactivează interfața.

Zonă

Caseta listă {lista zonelor OSPF existente}
Zona OSPF căreia îi aparține înregistrarea.

Adresă IP / mască

Adresă IP / mască, implicit = 0.0.0.0/0
Adresa IP și masca intervalului (adică rețeaua) care vor fi agregate sau ascunse.

Acţiune

Caseta listă {Aggregate; Ascunde}, implicit = „Agregat”

- Agregat – prefixele mici de rețea vor fi exportate din această zonă agregate în acest interval (definit de**IP/mască**)

- Ascunde – acest prefix de rețea va fi ascuns și nu va fi exportat

Exemplu:
Zona 0.0.0.1 exportă două subrețele: 192.168.1.0/24 și 192.168.2.0/24. Routerul de graniță de zonă între Zona 0.0.0.1 și 0.0.0.0 definește o regulă pentru agregarea rețelei: 192.168.0.0/16. Ca urmare a acestui fapt,

routerul de frontieră de zonă anunță zonei 0.0.0.0 un singur traseu 192.168.0.0/16 în locul celor două rute individuale.

Nota
Comentariu optional.

7.2.4.3. Reguli statice OSPF

Reguli de rutare statică predefinite pentru a fi exportate prin protocolul OSPF. Numărul maxim de reguli este 256.

Activ
Caseta listă {On; Off}, implicit = „Off" Activează/
dezactivează regula de rutare statică.

Destination IP / Destination mask
Adresă IP, implicită = 0.0.0.0/0
Adresa IP și masca care definesc intervalul de adrese ale regulii de rutare exportate.

Tip metric
Caseta listă {Tip 1; Tip 2}, implicit = „Tip 1"
Tipul de metrică al regulii de rutare. Valoarea 1 este adăugată la costul căii. Valoarea 2 rămâne separată și, în comparație cu valoarea 1, este întotdeauna mai mare.

Metric
Număr {1 – 65535}, implicit = 1000
Valoarea valorii regulii de rutare.

Eticheta OSPF
Numărul {0 – (2^{32}-1)}, implicit = 0
Eticheta OSPF este adăugată la o regulă în momentul inserării acesteia în rețea. Eticheta trece prin OSPF fără nicio modificare, astfel încât poate fi folosită pentru a distinge regula în filtre.

Nota
Comentariu optional.

7.2.4.4. Filtru de import OSPF

Reguli de filtru de import OSPF. Ordinea regulilor contează. Fiecare regulă de rutare de intrare este procesată de acele filtre de import. Numărul maxim de reguli de filtrare este 256.

Activ
Caseta listă {On; Off}, implicit = „Off"
Activează/dezactivează regula de filtrare.

Rețeaua de filtrare
Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat"
Metoda de comparare a intervalului țintă al regulii de rutare.

Adresă IP / mască
Adresă IP / mască, implicit = 0.0.0.0/0
Adresa IP și masca care definesc intervalul de rețea de comparat.

Masca de la

Număr {0 – 32}, implicit = 0

Masca la

Număr {0 – 32}, implicit = 32

Definirea intervalului activat al lungimii măștii regulii de rutare procesată.

Exemple:

• Regula 0.0.0.0/0{0,32} captează toate intervalele IP

• Regula 192.168.1.0/24{24,32} captează 192.168.1.0/24 și toate subrețelele (de exemplu 192.168.1.1/32)

• Regula 10.9.8.7/32{8,32} captează toate intervalele cu masca mai lungă de 8 care acoperă adresa 10.9.8.7 (de ex. 10.9.0.0/16)

Sursa de filtrare

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

Metoda comparației sursei regulii de rutare OSPF.

Sursă

Caseta listă {Internă; Inter-zonă; Tip extern 1; Tip extern 2}, implicit = „Tip extern 1”

Comentarii tip sursă:

• Intern – regulă generată intern, de exemplu intervalul de interfață

• Inter-zonă – regulă generată la granița zonei

Filtrați eticheta OSPF

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat” Metoda de comparare a etichetelor OSPF a regulii de rutare OSPF

Eticheta OSPF

Numărul {0 – (2^{32}-1)}, implicit = 0

etichetă OSPF de comparat.

Acţiune

Caseta listă {Accept; Respinge; Pass}, implicit = „Accept”

Tip de acțiune care trebuie efectuată atunci când regulile de filtrare de mai sus se potrivesc cu regula de rutare de intrare.

Setați preferința

Caseta listă {On; Off}, implicit = „Dezactivat”

Când este activat,**Preferinţă**(vezi următorul parametru) va fi setat la această regulă.

Preferinţă

Număr {0 – 65535}, implicit = 200

Preferința regulilor de rutare în tabelul de rutare (a fi folosit când**Setați preferința**este activat). Cu cât numărul este mai mare, cu atât preferința este mai bună.

Adresă locală de sursă preferată

Adresă IP, implicită = 0.0.0.0

Adresă IP sursă preferată pentru pachetele generate local. Când este dezactivată (este utilizată valoarea implicită 0.0.0.0), adresa IP sursă este setată în funcție de interfața de ieșire.

Nota

Comentariu optional.

7.2.4.5. Filtru de export OSPF

Regulile de filtru de export OSPF definesc un set de reguli de rutare care trebuie exportate din unitate în zona OSPF. Ordinea regulilor contează. Numărul maxim de reguli de filtrare este 256.

Activ

Caseta listă {On; Off}, implicit = „Off”

Activează/dezactivează regula de filtrare.

Nota

Comentariu optional.

Rețeaua de filtrare

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

Selectează o metodă de comparare a intervalului de destinație al regulii de rutare.

Adresă IP / mască

Adresă IP / mască, implicit = 0.0.0.0/0

Adresa IP și masca definesc prefixul de rețea care trebuie comparat.

Masca de la

Număr {0 – 32}, implicit = 0

Masca la

Număr {0 – 32}, implicit = 32

Definirea intervalului activat al lungimii măștii regulii de rutare procesată.

Protocol de filtrare

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

Selectează modul în care este comparat protocolul sursă a regulii de rutare.

Protocol

Caseta listă {System; BGP; BGP extern; BGP intern}, implicit = „Sistem”

Selectarea originii protocolului. „Sistem” – reprezintă regulile din tabelul obișnuit de rutare.

Filtrați calea BGP

Caseta listă {Off; Este gol; Nu este gol}, implicit = „Dezactivat”

Compară calea regulii de rutare BGP dacă este goală (adică regula provine din acest AS).

Acţiune

Caseta listă {Accept; Respinge; Pass}, implicit = „Accept”

Definește ce acțiune este întreprinsă cu privire la regula de rutare. „Pass” continuă în procesare.

7.2.5. BGP

Border Gateway Protocol (BGP) este un protocol de gateway exterior standardizat conceput pentru a schimba informații de rutare și accesibilitate între sistemele autonome. BGP este clasificat ca un protocol de rutare vector cale și ia decizii de rutare bazate pe căi, politici de rețea sau seturi de reguli configurate de un administrator de rețea.

BGP împarte rețeaua în sisteme autonome (AS) care sunt identificate printr-un anumit număr. Routerele BGP individuale sunt interconectate cu vecinii lor folosind conexiuni TCP. Orice conexiune poate călători prin mai multe hopuri. Orice conexiune poate fi securizată folosind semnăturile MD5.

Conexiunile din interiorul AS sunt numite „interne” (iBGP):

• Toate routerele BGP din AS dat trebuie să fie complet interconectate – fiecare router trebuie să aibă conexiune la toate celelalte routere.

• Este posibil să se definească „reflectori de traseu” – aceștia trebuie să fie complet interconectați. Celelalte routere se comportă ca clienți Route reflector și au nevoie doar de o conexiune la reflectorul lor. Route reflector și clienții săi formează un „cluster”. Este posibil să se creeze un cluster cu mai multe reflectoare de rută în scopul rezervării.

• Routerul iBGP care are o preferință locală mai mare va fi preferat în timpul selecției interne a căii AS.

Conexiunile la un alt AS se numesc „externe” (eBGP):

• Este posibil să se comunice de la router către vecinul AS metrica MED (Multi-Exit Discriminator) care desemnează care dintre routerele de frontieră AS va fi folosit ca punct de intrare.

Când regulile de rutare sunt răspândite pe mai multe AS, acele AS sunt adăugate în calea acumulată (cale BGP). Lungimea căii este criteriul principal în timpul deciziei care dintre regulile de rutare va fi utilizată.

Este posibil să prescrii reguli de rutare către acest router care va fi răspândit în rețea (reguli statice).

Este posibil să se controleze regulile de rutare care sunt importate în unitatea RipEX din protocolul BGP și pe cele care sunt exportate în protocolul BGP de la unitate utilizând „filtre”.

Import IGP filter – controlează care dintre regulile de rutare din BGP sunt acceptate în tabelul de rutare dinamică și cum

Export IGP filter – controlează care dintre regulile de rutare din tabelul de rutare dinamică sunt exportate în BGP și cum

Filtrul Import OUT – controlează care dintre regulile de rutare de la celălalt AS sunt acceptate în BGP și cum

Filtrul Export OUT – controlează care dintre regulile de rutare sunt exportate din BGP către alte AS și cum

Regulile de rutare transmise între tabelele iBGP și BGP nu sunt filtrate

7.2.5.1. BGP Common - Setări comune

Activ

Caseta listă {On; Off}, implicit = „Dezactivat”

Activează rutarea dinamică și protocolul BGP.

ID router

Adresă IP, implicită = 0.0.0.0

Unitatea RipEX acționează în rețeaua BGP ca un router dinamic. Fiecare router este identificat printr-un ID având formatul unei adrese IP. Această adresă IP nu trebuie să fie „reală”. ID-ul routerului este partajat cu protocolul OSPF.

AS local

Numărul {0 – (2^{32}-1)}, implicit = 65000

Numărul de identificare al Sistemului Autonom Local. Numerele AS sunt atribuite de IANA. O parte a gamei este rezervată utilizării rețelei private: 64512 – 65534 și 4200000000 – 4294967294. Numerele AS din această gamă pot fi folosite în siguranță de oricine.

Preferinţă

Numărul {0 – (2^{32}-1)}, implicit = 100

Preferința routerului în AS local. Cu cât numărul este mai mare, cu atât preferința este mai mare.

MED (discriminator cu mai multe ieșiri)

Caseta listă {Off; Static; Valoarea OSPF 1}, implicit = „Dezactivat”

Setarea MED (Multi-Exit Discriminator) pentru regulile de rutare care sunt exportate către alte AS. MED face posibilă publicitatea care dintre routerele din AS local este punctul de intrare preferat pentru AS. Opțiunea „Static” setează valoarea fixă pentru toate regulile (**MED static**). „Metrica OSPF 1” copiază metrica OSPF în MED; pentru regulile care nu sunt din OSPF se introduce valoarea fixă**MED static**.

MED static

Numărul {0 – (2^{32}-1)}, implicit = 0

Metrica care trebuie utilizată pentru punctul de intrare preferat pentru selecția AS (consultați descrierea MED (Discriminator Multi-Exit)). Cu cât numărul este mai mare, cu atât preferința este mai mică.

Reflector de traseu

Caseta listă {Off; Activat}, implicit = „Dezactivat”

Activează funcția Route reflector pe acest router. iBGP necesită conexiune între toate routerele în circumstanțe normale. Route reflector face posibilă evitarea acestei cerințe prin distribuirea actualizărilor de rutare către toți clienții săi. Astfel de clienți nu au nevoie de altă conexiune, cu excepția conexiunii la acest reflector de rută. Route reflector și clienții săi formează un „cluster”. Vedeți mai multe detalii la începutul capitolului BGP.

Tip de ID cluster

Caseta listă {Router ID; Manual}, implicit = „ID router”

Controlează identificarea clusterului iBGP. Identificarea clusterului trebuie să fie aceeași în interiorul clusterului și trebuie să fie diferită în alt cluster. Dacă este selectat „ID-ul routerului”, acesta**ID router**valoare este folosită ca id de cluster.

ID-ul clusterului

Adresă IP, implicită = 0.0.0.0

Identificarea clusterului în formatul unei adrese IP. Această adresă IP nu trebuie să fie „reală” (validă).

7.2.5.2. Vecinii BGP

Routere BGP vecine. Numărul maxim de vecini este de 256.

Activ

Caseta listă {On; Off}, implicit =

„Pornit” Activează vecinul specific.

Nota

Comentariu optional.

Tipul de vecin

Caseta listă {Internă; Extern}, implicit = „Extern”

Selectarea tipului de router vecin. Vecinul „intern” aparține aceluiași AS (iBGP). „Extern” aparține altor AS (eBGP).

Vecinul AS

Numărul {0 – (2^{32}-1)}, implicit = 65000
număr AS vecin.

IP vecin

Adresă IP, implicită = 0.0.0.0
Adresa IP a routerului vecin.

IP local al conexiunii

Adresă IP, implicită = 0.0.0.0
Adresa IP locală a conexiunii. Valoarea implicită 0.0.0.0 asigură configurarea automată a acestei adrese – de la rutare.

Conexiune cu vecinul

Caseta listă {Direct; Multihop}, implicit = „Direct”
Tipul de conexiune la rețea între vecini. „Direct” înseamnă conexiune directă – un hop. Acest lucru este tipic pentru routerele eBGP. „Multihop” înseamnă conexiune prin mai multe routere. Acest lucru este tipic pentru routerele iBGP.

Autentificare MD5

Caseta listă {On; Off}, implicit = „Dezactivat”
Activează autentificarea pachetelor BGP folosind extensia de semnătură TCP MD5.

Parolă

Șir {până la 128 de caractere}
Parola pentru**Autentificare MD5**.

Pasiv

Caseta listă {On; Off}, implicit = „Dezactivat”
Routerul BGP pasiv nu inițiază conexiunea la un vecin, acesta așteaptă activitatea vecinului.

Interval de menținere [s]

Număr {3 – 10800}, implicit = 240
Timp (în secunde) pentru a aștepta mesajul keepalive de la vecin. Se negociaza cu vecinul. Când expiră, conexiunea este tratată ca întreruptă.

Interval de menținere a vieții [s]

Număr {1 – 3600}, implicit = 80
Perioada (în secunde) de trimitere a mesajelor keepalive. Nu ar trebui să fie mai mare de 1/3 din**Țineți intervalul**.

Interval de reîncercare a conexiunii [s]

Număr {1 – 3600}, implicit = 120
Timp (în secunde) de așteptat înainte de a încerca să reconectați conexiunea întreruptă.

Securitate TTL

Caseta listă {On; Off}, implicit = „Activat”
Protecție împotriva falsificării pachetelor BGP. [PP1] Mecanismul generalizat de securitate TTL (GTSM – RFC 5082) este utilizat. BGP transmite pachete cu valoare TTL cunoscută. Pachetele primite care au o valoare mai mică decât cea așteptată (număr așteptat de hopuri) sunt aruncate.

Hamei așteptat

Numărul {2 – 32}, implicit = 2
Numărul de hopuri așteptate între vecini.

Client reflector de traseu

Caseta listă {On; Off}, implicit = „Dezactivat”

Definește dacă acest vecin este un client al acestui reflector de rută.

Setați costul

Caseta listă {On; Off}, implicit = „Dezactivat”

Permite setarea unui anumit**Cost**a conexiunii BGP.

Cost

Numărul {0 – (2_{32}-1)}, implicit = 10

Costul conexiunii la acest vecin. Cu cât numărul este mai mare, cu atât costul este mai mare. Vă permite să luați decizii în interiorul routerului între mai multe căi de la același vecin.

Următorul hop de sine

Caseta listă {Off; Întotdeauna; Intern; Extern}, implicit = „Dezactivat”

Definește că regulile de rutare exportate ar trebui să aibă adrese „next hop” suprascrise la adresa acestui router. „Intern” suprascrie numai regulile din AS local. „Extern” suprascrie doar regulile din celălalt AS.

7.2.5.3. BGP Reguli statice

Reguli de rutare statică predefinite pentru a fi exportate prin protocolul BGP. Numărul maxim de reguli este 256.

Activ

Caseta listă {On; Off}, implicit = „Off” Activează/
dezactivează regula de rutare statică.

Destination IP / Destination mask

Adresă IP, implicită = 0.0.0.0/32

Adresa IP și masca care definesc intervalul de adrese de destinație a regulii de rutare exportate.

Nota

Comentariu optional.

7.2.5.4. BGP Import IGP filtru

Importați regulile filtrului IGP [PP1]. Ordinea regulilor contează. Numărul maxim de reguli de filtrare este 256.

Politica de filtrare

Caseta listă {Accept; Respingere}, implicit = „Respingere”

Definește ce acțiune este întreprinsă cu privire la regulile de rutare care nu au fost capturate (adică fallback) în**Import filtru IGP**.

Activ

Caseta listă {On; Off}, implicit = „Pornit”

Activează/dezactivează regula de filtrare.

Nota

Comentariu optional.

Rețeaua de filtrare

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

Selectează o metodă de comparare a intervalului de destinație al regulii de rutare.

Adresă IP / mască

Adresă IP / mască, implicit = 0.0.0.0/0

Adresa IP și masca definesc prefixul de rețea care trebuie comparat

Masca de la

Număr {0 – 32}, implicit = 0

Masca la

Număr {0 – 32}, implicit = 32

Definirea intervalului activat al lungimii măștii regulii de rutare procesată.

Sursa de filtrare

Caseta listă {Off; Intern; Extern}, implicit = „Dezactivat”

Selectare bazată pe sursa regulii de rutare. „Intern” selectează regulile primite de la conexiunea internă (iBGP). „Extern” selectează regulile primite de la celălalt AS (eBGP).

Filtrați calea BGP

Caseta listă {Off; Este gol; Nu gol; Conține; Nu conține}, implicit = „Dezactivat”

Filtrarea bazată pe calea BGP (calea regulii de rutare pe AS diferite). „Este gol” – definește o cale goală (regula de rutare din AS local). „Conține” – definește căile care conțin AS specific.

Poziția traseului

Caseta listă {Orice; Vecin; Sursă}, implicit = „Orice”

Selectează poziția AS specific (**Calea AS**). „Orice” – oriunde pe potecă. „Vecin” – calea a fost primită de la acest AS (ultimul pe potecă). „Sursă” – regula de rutare a fost originată din acest AS (primul pe cale).

Calea AS

Numărul {0 – (2^{32}-1)}, implicit = 65000

Numărul AS căutat.

Acţiune

Caseta listă {Accept; Respinge; Pass}, implicit = „Accept”

Definește ce acțiune este întreprinsă cu privire la regula de rutare [PP1] capturată. „Pass” continuă în procesare.

Setați preferința

Caseta listă {Off; Activat}, implicit = „Dezactivat”

Definește dacă specificul**Preferinţă**va fi stabilit pentru această regulă.

Preferinţă

Număr {0 – 65535}, implicit = 100

Preferința regulilor de rutare în tabelul de rutare. Cu cât numărul este mai mare, cu atât preferința este mai mare.

Adresă locală de sursă preferată

Adresă IP, implicită = 0.0.0.0

Adresă IP sursă preferată pentru pachetele generate local. Când este dezactivată (este utilizată valoarea implicită 0.0.0.0), adresa IP sursă este setată în funcție de interfața de ieșire.

7.2.5.5. BGP Export filtru IGP

Exportați regulile de filtru IGP. Ordinea regulilor contează. Numărul maxim de reguli de filtrare este 256.

Politica de filtrare

Caseta listă {Accept; Respingere}, implicit = „Respingere”

Definește ce acțiune este întreprinsă cu privire la regulile de rutare care nu au fost capturate (adică fallback) în**Exportați filtrul IGP**.

Activ

Caseta listă {On; Off}, implicit = „Pornit”
Activează/dezactivează regula de filtrare.

Nota

Comentariu optional.

Rețeaua de filtrare

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”
Selectează o metodă de comparare a intervalului de destinație al regulii de rutare.

Adresă IP / mască

Adresă IP / mască, implicit = 0.0.0.0/0
Adresa IP și masca definesc prefixul de rețea care trebuie comparat

Masca de la

Număr {0 – 32}, implicit = 0

Masca la

Număr {0 – 32}, implicit = 32
Definirea intervalului activat al lungimii măștii regulii de rutare procesată.

Protocol de filtrare

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”
Selectează modul în care este comparat protocolul sursă a regulii de rutare.

Protocol

Caseta listă {System; OSPF}, implicit = „Sistem”
Selectarea originii protocolului. „Sistem” – reprezintă regulile din tabelul obișnuit de rutare. „OSPF” înseamnă reguli din protocolul OSPF.

Filtrați sursa OSPF

Caseta listă {Off; Meci; Not match}, default = "Off" Selectează
modul de comparare a sursei regulii de rutare OSPF.

sursa OSPF

Caseta listă {Internă; Inter-zonă; Tip extern 1; Tip extern 2}, implicit = surse OSPF „Tip extern 2”. „Internă” – înseamnă o regulă generată intern (de exemplu, intervalul de interfață). „Inter-zonă”
– reprezintă regula generată la granițele zonei.

Filtrați eticheta OSPF

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”
Selectează modul de filtrare pe baza etichetei OSPF.

Eticheta OSPF

Numărul {0 – (2^{32}-1)}, implicit = 0
Eticheta OSPF de comparat. Eticheta este adăugată la o regulă atunci când este inserată în OSPF.

Acțiune

Caseta listă {Accept; Respinge; Pass}, default = „Accept”Definește ce acțiune este întreprinsă asupra regulii de rutare. „Pass” continuă în procesare.

7.2.5.6. Reguli BGP Import OUT

Importă regulile filtrului OUT [PP1]. Ordinea regulilor contează. Numărul maxim de reguli de filtrare este 256.

Politica de filtrare

Caseta listă {Accept; Reject}, implicit = „Accept”

Definește ce acțiune este întreprinsă cu privire la regulile de rutare care nu au fost capturate (adică fallback) în**Import OUT filtru**.

Limita filtrului

Număr {1 – 65535}, implicit = 1024

Limita regulilor de rutare acceptate de la vecin. Limita se aplică înainte de acest filtru Import OUT. Regulile în exces sunt eliminate.

Activ

Caseta listă {On; Off}, implicit = „Pornit”

Activează/dezactivează regula de filtrare.

Nota

Comentariu optional.

Rețeaua de filtrare

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

Selectează o metodă de comparare a intervalului de destinație al regulii de rutare.

Adresă IP / mască

Adresă IP / mască, implicit = 0.0.0.0/0

Adresa IP și masca definesc prefixul de rețea care trebuie comparat

Masca de la

Număr {0 – 32}, implicit = 0

Masca la

Număr {0 – 32}, implicit = 32

Definirea intervalului activat al lungimii măștii regulii de rutare procesată.

Filtrați calea BGP

Caseta listă {Off; Este gol; Nu gol; Conține; Nu conține}, implicit = „Dezactivat”

Filtrarea bazată pe calea BGP (calea regulii de rutare pe AS diferite). „Este gol” – definește o cale goală (regula de rutare din AS local). „Conține” – definește căile care conțin AS specific.

Poziția traseului

Caseta listă {Orice; Vecin; Sursă}, implicit = „Orice”

Selectează poziția AS specific (**Calea AS**). „Orice” – oriunde pe potecă. „Vecin” – calea a fost primită de la acest AS (ultimul pe potecă). „Sursă” – regula de rutare provine din acest AS (primul pe cale).

Calea AS

Numărul {0 – (2^{32}-1)}, implicit = 65000

Numărul AS căutat.

Acţiune

Caseta listă {Accept; Respinge; Pass}, implicit = „Accept”

Definește ce acțiune este întreprinsă cu regula de rutare de potrivire. „Pass” continuă în procesare.

Adăugați AS local

Număr {0 – 8}, implicit = 0

Permite adăugarea (chiar și de mai multe ori) număr AS local la capătul căii BGP - făcând calea practic mai lungă. Calea mai lungă este handicapată în timpul comparațiilor și selecțiilor.

7.2.5.7. Filtrul BGP Export OUT

Exportați regulile de filtru OUT. Ordinea regulilor contează. Numărul maxim de reguli de filtrare este 256.

Politica de filtrare

Caseta listă {Accept; Reject}, implicit = „Accept”

Definește ce acțiune este întreprinsă cu privire la regulile de rutare care nu au fost capturate (adică fallback) în**Exportați filtrul OUT**.

Activ

Caseta listă {On; Off}, implicit = „Pornit”

Activează/dezactivează regula de filtrare.

Nota

Comentariu optional.

Rețeaua de filtrare

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

Selectează o metodă de comparare a intervalului de destinație al regulii de rutare.

Adresă IP / mască

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

Adresa IP și masca definesc prefixul de rețea care trebuie comparat

Masca de la

Număr {0 – 32}, implicit = 0

Masca la

Număr {0 – 32}, implicit = 32

Definirea intervalului activat al lungimii măștii regulii de rutare procesată.

Protocol de filtrare

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

Selectează modul în care este comparat protocolul sursă a regulii de rutare.

Protocol

Caseta listă {System; OSPF; BGP; BGP extern; BGP intern}, implicit = „Sistem” Selectarea originii protocolului. „Sistem” – reprezintă regulile din tabelul obișnuit de rutare.

Filtrați eticheta OSPF

Caseta listă {Off; Meci; Nu se potrivește}, implicit = „Dezactivat”

Selectează modul de filtrare pe baza etichetei OSPF.

Eticheta OSPF

Numărul {0 – (2_{32}-1)}, implicit = 0

Eticheta OSPF de comparat. Eticheta este adăugată la o regulă atunci când este inserată în OSPF.

Filtrați calea BGP

Caseta listă {Off; Este gol; Nu gol; Conţine; Nu conține}, implicit = „Dezactivat”

Filtrarea bazată pe calea BGP (calea regulii de rutare pe AS diferite). „Este gol” – definește o cale goală (regula de rutare din AS local). „Conține” – definește căile care conțin AS specific.

Poziția traseului

Caseta listă {Orice; Vecin; Sursă}, implicit = „Orice”

Selectează poziția AS specific (**Calea AS**). „Orice” – oriunde pe potecă. „Vecin” – calea a fost primită de la acest AS (ultimul pe potecă). „Sursă” – regula de rutare a fost originată din acest AS (primul pe cale).

Calea AS

Numărul {0 – (2^{32}-1)}, implicit = 65000

Numărul AS căutat.

Acţiune

Caseta listă {Accept; Respinge; Pass}, implicit = „Accept”

Definește ce acțiune este întreprinsă cu privire la regula de rutare. „Pass” continuă în procesare.

7.3. Firewall

7.3.1. Firewall L2

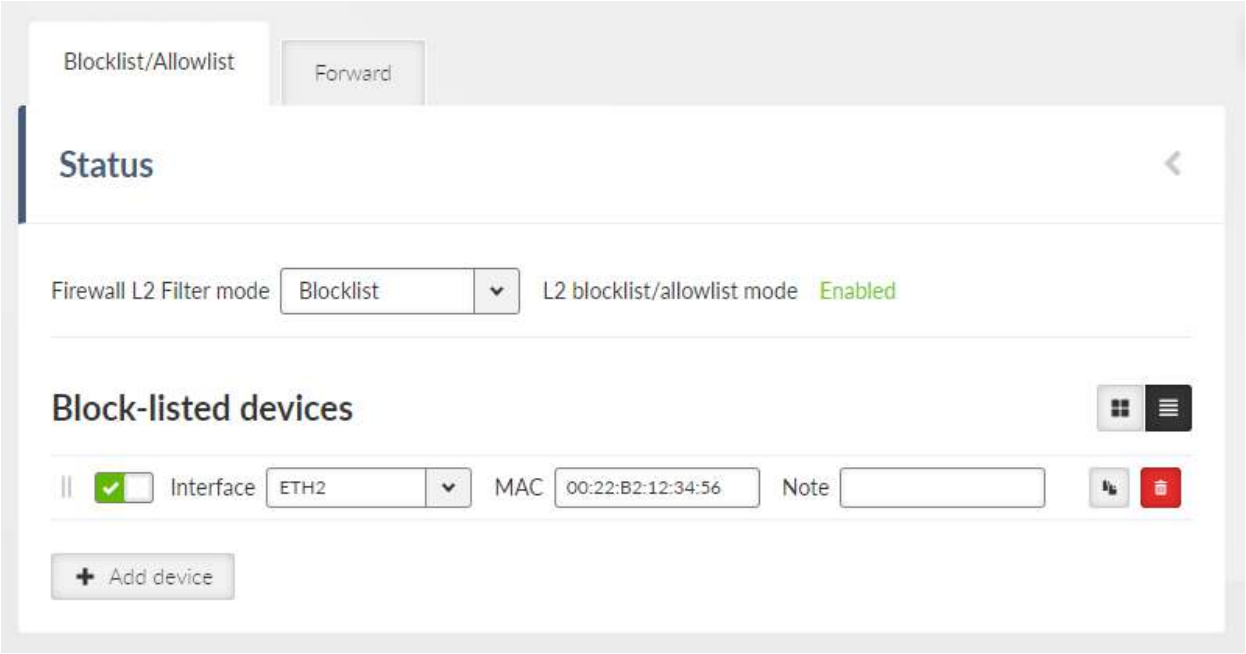


Fig. 7.14: SETĂRI > Firewall > L2

Modul de filtrare

Caseta listă {Off; Blocklist; Lista permisă}, implicit = „Dezactivat”

Lista blocată

Adresele MAC listate în tabel sunt blocate, adică toate pachetele către/de la acestea sunt aruncate. Traficul către/de la alte adrese MAC este permis.

Lista permisă

Sunt permise doar adresele MAC enumerate în tabel, adică sunt permise numai pachetele către/de la acestea. Traficul către/de la alte adrese MAC este blocat.

Activ

Caseta listă {Off; Activat}, implicit = „Activat”

Dacă este „Pornit”, regula de firewall Linux de nivel 2 este activată.

Interfață

Caseta listă {Toate; ETH1..ETH5}, implicit = „Toate”

MAC

Adresa MAC IPv4

Nota

Setările firewall-ului L2 nu afectează accesul local ETH, adică setările nu interzic niciodată accesul la un M!DGE3 conectat local (interfață web, ping, ...).

7.3.1.1. Redirecţiona

L2 Forward filtrează pachetele care trec printr-o punte de la un port la altul. Nu filtrează pachetele care provin de la sau care se termină la stație sau direcționate între diferite interfețe.

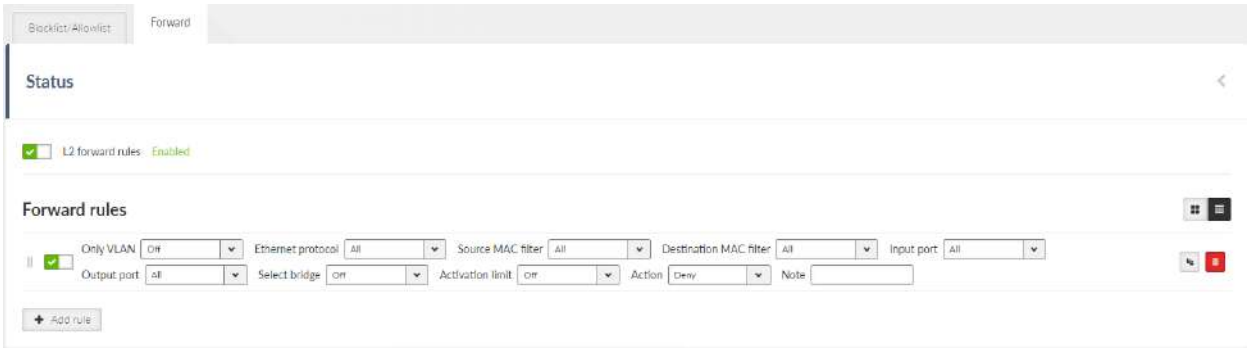


Fig. 7.15: SETĂRI > Firewall > L2

Reguli înainte L2

Activează/dezactivează regulile înainte L2; implicit = „Dezactivat”

Fiecare regulă de firewall individuală este descrisă de următorii parametri:

Doar VLAN

Caseta listă {Off; Activat}, implicit = „Dezactivat”

Permite filtrarea pachetelor pentru un anumit VLAN și inspecția profundă a pachetelor. Dacă este activat:

VLAN

Număr (0-4094), implicit = 1

ID al VLAN-ului filtrat

protocol Ethernet

Caseta listă {Toate; Nu VLAN; Toate VLAN-urile; IPv4; IPv6; ARP; Other}, implicit = "Toate" Filtru bazat pe EtherType (protocol purtat în cadrul Ethernet).

Filtru MAC sursă

Caseta listă {Toate; Masca; Unicast; Multicast-uri; Broadcasts}, implicit = „Toate” Activează filtrarea pe baza adresei MAC sursă a pachetului. Pentru opțiunea Mască:

Adresă MAC sursă

Adresă utilizată pentru a compara cu adresa MAC sursă a pachetelor.

Mască MAC sursă

Masca folosită pentru a compara cu adresa MAC sursă a pachetelor.

Filtru MAC de destinație

Caseta listă {Toate; Masca; Unicast; Multicast-uri; Broadcasts}, implicit = „Toate”
Permite filtrarea pe baza adresei MAC de destinație a pachetului. Pentru opțiunea Mască:

Adresă MAC de destinație

Adresă utilizată pentru a compara cu adresa MAC de destinație a pachetelor.

Mască MAC de destinație

Masca folosită pentru a compara cu adresa MAC de destinație a pachetelor.

Port de intrare

Caseta listă {Toate; Radio; Toate ETH; ETH1; ETH2; ETH3; ETH4; ETH5; GRE L2; OpenVPN L2; Altele"}, implicit = "Toate"
Filtrele bazate pe portul prin care pachetul a intrat în punte. Pentru altă opțiune:

Introduceți numele portului

Șir {0–16 caractere}, implicit = <gol>
Numele portului de intrare. Trebuie să fie numele unei interfețe existente, folosită ca port bridge.

Port de ieșire

Caseta listă {Toate; Radio; Toate ETH; ETH1; ETH2; ETH3; ETH4; ETH5; GRE L2; OpenVPN L2; Altele"}, implicit = "Toate"
Filtre în funcție de portul prin care iese pachetul de pe punte.
Pentru altă opțiune:

Numele portului de ieșire

Șir {0–16 caractere}, implicit = <gol>
Numele portului de ieșire. Trebuie să fie numele unei interfețe existente, folosită ca port bridge.

Selectați podul

Caseta listă {Off; Activat}, implicit = „Dezactivat”
Permite limitarea regulii la un anumit pod. Regula se va aplica numai pachetelor care trec prin puntea selectată.

Limită de activare

Caseta listă {Off; Activat}, implicit = „Dezactivat”
Permite limitarea numărului de declanșări ale regulii pe unitate de timp. Dacă este activat:

Număr de cadre

Număr (1-10000), implicit = 3
Limită medie de pachete/rata de activare pe unitate de timp.

Perioada de măsurare

Caseta de listă {Secund, Minut, Hour, Day}, implicit = „Minut” Unitate de timp pentru limitarea ratei de pachet/activare.

Dimensiunea exploziei

Număr (1-10000), implicit = 3

Numărul inițial și maxim de jetoane TBF. După o perioadă de inactivitate, TBF permite o explozie de trafic să treacă dintr-o dată. Trebuie să fie mai mare sau egal cu numărul de cadre.

Acțiune

Caseta listă {Deny; Permite}, implicit = „Refuză”

Selectează acțiunea care trebuie întreprinsă asupra unui pachet care se potrivește cu filtrul configurat.

7.3.2. Firewall L3

7.3.2.1. Redirecţiona

Set de reguli care se aplică pentru traficul care vine prin routerul celular2.

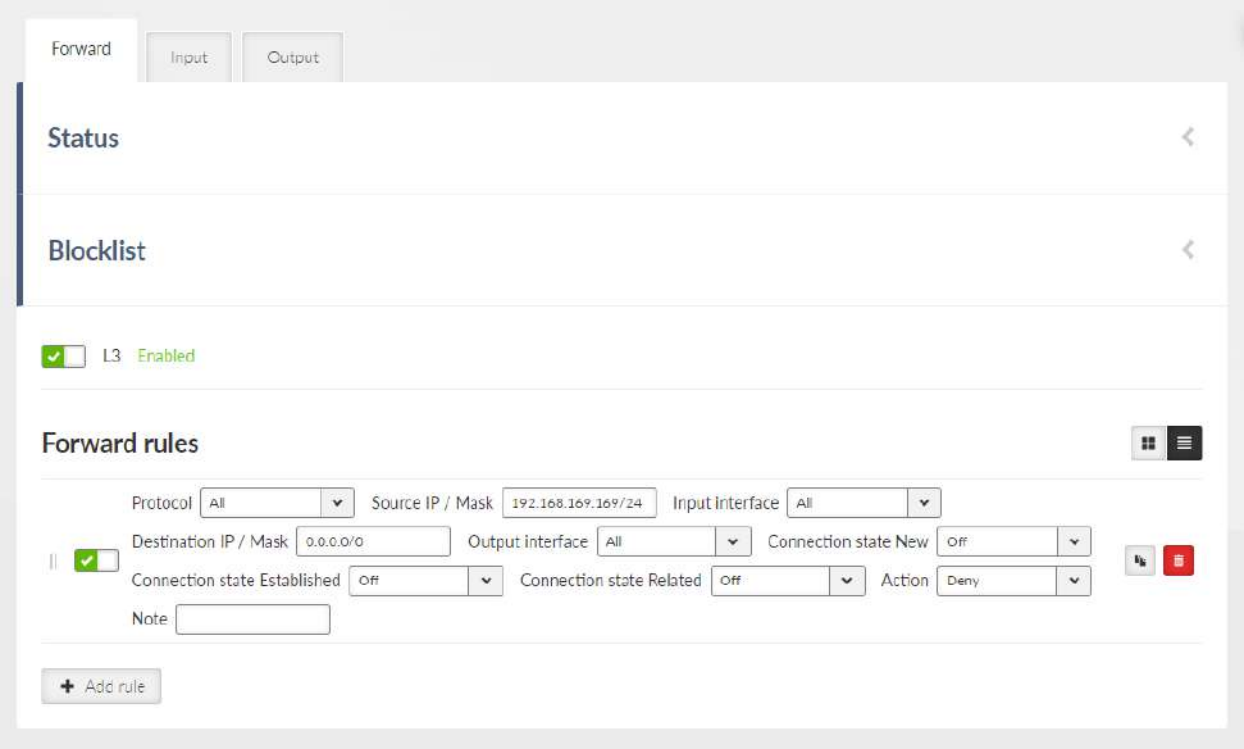


Fig. 7.16: SETĂRI > Firewall > L3

L3

Activează/dezactivează firewall L3; implicit = „Dezactivat”

Fiecare regulă de firewall individuală este descrisă de următorii parametri:

Protocol

Caseta listă {Toate; ICMP; UDP; TCP; GRE; ESP; Altele}, implicit = „Toate”

IP sursă / Mască

Regula cu mască mai îngustă are prioritate mai mare. Ordinea regulii afectează prioritatea.

Port sursă (de la) / Port sursă (către)

Intervalul porturilor sursă. Acest parametru apare numai când parametrul**Protocol**este setat fie la „UDP”, fie la „TCP”.

Interfață de intrare

Caseta listă {Toate; WWAN; Toate ETH; EXT; ETH1..ETH5; GRE L2; GRE L3; Altele}, implicit = „Toate”

IP de destinație / Mască

Definește subrețeaua IP de destinație.

Port de destinație (de la) / Port de destinație (la)

Intervalul porturilor de destinație.

Interfață de ieșire

Caseta listă {Toate; WWAN; Toate ETH; EXT; GRE L3; Altele}, implicit = „Toate”

Starea conexiunii Nou

Caseta listă {Off; Activat}, implicit = „Dezactivat”

Se referă la primul pachet când începe o conexiune TCP (Solicitare de la clientul TCP la serverul TCP pentru deschiderea unei noi conexiuni TCP). Folosit de exemplu pentru a permite deschiderea TCP numai din rețeaua M!DGE3 către exterior.

Starea conexiunii stabilită

Caseta listă {Off; Activat}, implicit = „Dezactivat”

Se referă la o conexiune TCP deja existentă. Folosit de exemplu pentru a permite obținerea de răspunsuri pentru conexiunile TCP create din rețeaua M!DGE3 către exterior.

Starea conexiunii Legat

Caseta listă {Off; Activat} implicit = „Dezactivat”

O conexiune legată de cea „stabilită”, de exemplu, FTP utilizează de obicei 2 conexiuni TCP de control și date, unde conexiunea de date este creată automat folosind porturi dinamice.

Nota

Conexiunea de gestionare la un M!DGE3 la distanță poate fi pierdută, atunci când un alt M!DGE3 acționează ca un router de-a lungul căii pachetelor de gestionare și portul TCP 8889 (Acces la distanță) este dezactivat (regula DENY) în setările firewall-ului L3 ale acelei M!DGE3 (lanț FORWARD).

Acţiune

Caseta listă {Deny; Permite}, implicit = „Refuză”

7.3.2.2. Intrare

Set de reguli care se aplică traficului care se îndreaptă către routerul celular2. Traficul de intrare de la adresele sursă nedorite poate fi blocat prin setarea parametrului *Acţiune* la „Refuză, adaugă la lista blocată”.

L3

Activează/dezactivează firewall L3; implicit = „Dezactivat”

Fiecare regulă de firewall individuală este descrisă de următorii parametri:

Serviciu

Reguli, care deschid accesul de management prin interfețele de servicii.

Caseta listă {Altele; COM1; COM2; COM3; TS1; TS2; TS3; TS4; TS5; SSH; HTTP; HTTPS; Acces de la distanță; SNMP; NTP}, implicit = „Altele”

Protocol

Caseta listă {Toate; ICMP; UDP; TCP; GRE; ESP; Altele}, implicit = „Toate”

IP sursă / Mască

Adresă IP sursă și mască. Regula cu mască mai îngustă are prioritate mai mare. Ordinea regulii afectează prioritatea.

Port sursă (de la) / Port sursă (către)

Intervalul porturilor sursă. Acest parametru apare numai când parametrul**Protocol**este setat fie la „UDP”, fie la „TCP”.

Interfață de intrare

Caseta listă {Toate; WWAN; Toate ETH; EXT; ETH1..ETH5; GRE L2; GRE L3; Altele}, implicit = „Toate”

Port de destinație (de la) / Port de destinație (la)

Intervalul porturilor de destinație.

Starea conexiunii Nou

Caseta listă {Off; Activat}, implicit = „Dezactivat”

Se referă la primul pachet când începe o conexiune TCP (Solicitare de la clientul TCP la serverul TCP pentru deschiderea unei noi conexiuni TCP). Folosit de exemplu pentru a permite deschiderea TCP numai din rețeaua M!DGE3 către exterior.

Starea conexiunii stabilită

Caseta listă {Off; Activat}, implicit = „Dezactivat”

Se referă la o conexiune TCP deja existentă. Folosit de exemplu pentru a permite obținerea de răspunsuri pentru conexiunile TCP create din rețeaua M!DGE3 către exterior.

Starea conexiunii Legat

Caseta listă {Off; Activat} implicit = „Dezactivat”

O conexiune legată de cea „Inființată”. de exemplu, FTP utilizează de obicei 2 conexiuni TCP de control și date, unde conexiunea de date este creată automat prin utilizarea porturi dinamice.

Nota

Conexiunea de gestionare la un M!DGE3 la distanță poate fi pierdută, atunci când un alt M!DGE3 acționează ca un router de-a lungul căii pachetelor de gestionare și portul TCP 8889 (Acces la distanță) este dezactivat (regula DENY) în setările firewall-ului L3 ale acelei M!DGE3 (lanț FORWARD).

Acţiune

Caseta listă {Deny; Permite; Deny, Add to Blocklist}, implicit = „Deny”

Deny, Add to Blocklist - tot traficul de la adresa anume va fi eliminat automat. Lista blocată are o capacitate limitată de 512 adrese. Odată ce capacitatea sa este depășită, cea mai veche adresă este suprascrisă. Adresele adăugate la lista blocată rămân timp de o săptămână (604.800 de secunde) și sunt șterse ulterior din aceasta. Schimbarea configurației, inclusiv firewall-ul sau repornirea unității, vor șterge și acele adrese.

7.3.2.3. Ieșire

Set de reguli aplicabile pentru traficul care pleacă de la routerul celular2.

L3

Activează/dezactivează firewall L3; implicit = „Dezactivat”

Fiecare regulă de firewall individuală este descrisă de următorii parametri:

Serviciu

Reguli, care permit returnarea pachetelor de management (răspunsuri) prin interfața de serviciu.
Caseta listă {Altele; COM1; COM2; COM3; TS1; TS2; TS3; TS4; TS5; SSH; HTTP; HTTPS; Acces de la distanță; SNMP; NTP}, implicit = „Altele”
Ordinea regulii afectează prioritatea.

Protocol

Caseta listă {Toate; ICMP; UDP; TCP; GRE; ESP; Altele}, implicit = „Toate”

Port sursă (de la) / Port sursă (către)

Intervalul porturilor sursă. Acest parametru apare numai când parametrul**Protocol**este setat fie la „UDP”, fie la „TCP”.

IP de destinație / Mască

Definește IP/subrețea de destinație.

Port de destinație (de la) / Port de destinație (la)

Intervalul porturilor de destinație.

Starea conexiunii Nou

Caseta listă {Off; Activat}, implicit = „Dezactivat”
Se referă la primul pachet când începe o conexiune TCP (Solicitare de la clientul TCP la serverul TCP pentru deschiderea unei noi conexiuni TCP). Folosit de exemplu pentru a permite deschiderea TCP numai din rețeaua M!DGE3 către exterior.

Starea conexiunii stabilită

Caseta listă {Off; Activat}, implicit = „Dezactivat”
Se referă la o conexiune TCP deja existentă. Folosit de exemplu pentru a permite obținerea de răspunsuri pentru conexiunile TCP create din rețeaua M!DGE3 către exterior.

Starea conexiunii Legat

Caseta listă {Off; Activat} implicit = „Dezactivat”
O conexiune legată de cea „Inființată”. De exemplu, FTP utilizează în mod obișnuit două conexiuni TCP de control și date, unde conexiunea de date este creată automat utilizând porturi dinamice.

Nota

Conexiunea de gestionare la un M!DGE3 la distanță poate fi pierdută, atunci când un alt M!DGE3 acționează ca un router de-a lungul căii pachetelor de gestionare și portul TCP 8889 (Acces la distanță) este dezactivat (regula DENY) în setările firewall-ului L3 ale acelei M!DGE3 (lanț FORWARD).

Acțiune

Caseta listă {Deny; Permite}, implicit = „Refuză”

Nota

Comentariu optional.

7.3.3. NAT - Traducere adrese de rețea

Adresa de rețea și traducerea portului(**NAPT**) este o metodă de mapare a unui spațiu de adresă IP (sau port) într-un altul prin modificarea informațiilor despre adresa de rețea din antetul IP al pachetelor în timp ce acestea sunt în tranzit printr-un dispozitiv de rutare a traficului.

7.3.3.1. Sursa NAT

Source Network Address Translation (SNAT) - rescrie adresa sursă și/sau portul din conexiunea de părăsire și efectuează modificări opuse pentru pachetele returnate.

SNAT:

• Permite pretinderea că pachetele provin de la un dispozitiv care realizează SNAT.

• Funcționează în timpul ieșirii pachetelor de la un dispozitiv (după rutare și filtrare în firewall).

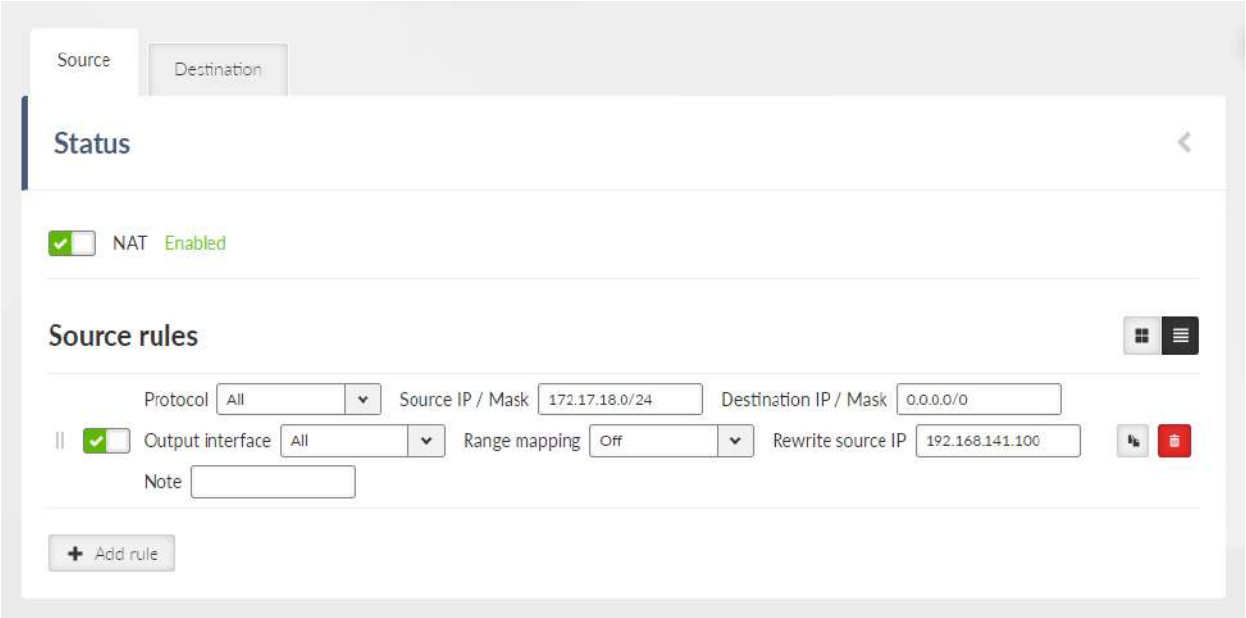


Fig. 7.17: SETĂRI > Firewall > NAT

Permite

Caseta listă {Activare; Disable}, implicit = "Disable"
Activează/dezactivează toate regulile NAT sursă.

Parametrii „**Protocol**”, “**IP sursă / Mască**”,„**IP de destinație / Mască**”, „**Interfață de ieșire**”,“**Port sursă de la** ”, “**Port sursă către**”, “**Port de destinație din**”, “**Port de destinație către**” și ”**Numărul protocolului**” definiți un filtru, care captează pachetele specificate. Regula SNAT se aplică pentru acele pachete.

Parametrii „**Port sursă de la**”, “**Port sursă către**”, “**Port de destinație din**” și ”**Port de destinație către** „ apare numai dacă parametrul „**Protocol**” este setat la „UDP” sau „TCP”.

Parametrul „**Numărul protocolului**” apare numai dacă parametrul “**Protocol**” este setat la „Altele”.

Protocol

Caseta listă {Toate; ICMP; UDP; TCP; GRE; ESP; Altele}, implicit = „Toate”
Filtrează protocolul selectat. Dacă niciuna dintre valorile menționate nu se potrivește, selectați „Altele”.

Numărul protocolului

Număr {0 – 255}, implicit = 1
Acest parametru apare numai dacă parametrul „**Protocol**” este setat la „Altele”.

IP sursă / Mască

Adresă IP, implicită = 0.0.0.0/0

Definește subrețeaua IP sursă.

Port sursă (de la) / Port sursă (către)

Număr {0 - 65535}, implicit = 0

Definește intervalul de valori al portului sursă. Valoarea 0 înseamnă că nu este filtrată în funcție de portul sursă. Dacă este necesar un singur port, setați ambii parametri la același număr. Acești parametri apar numai dacă parametrul „**Procotol**” este setat la „UDP” sau „TCP”.

IP de destinație / Mască

Adresă IP, implicită = 0.0.0.0/0

Definește subrețeaua IP de destinație.

Port de destinație (de la) / Port de destinație (la)

Număr {0 - 65535}, implicit = 0

Definește intervalul de valori al portului de destinație. Valoarea 0 înseamnă că nu este filtrată în funcție de portul de destinație. Acești parametri apar numai dacă parametrul „**Procotol**” este setat la „UDP” sau „TCP”.

Interfață de ieșire

Caseta listă {Toate; ; ;WWANAll ETH; EXT; GRE L3; Altele}, implicit = „Toate”

Filtrează interfețele selectate.

Numele interfeței de ieșire

Trebuie setat ca una dintre interfețele existente (numele interfeței LAN (sau VLAN), numele tunelului GRE etc.). Acest parametru apare numai dacă parametrul „**Interfață de ieșire**” este setat la „Altele”.

Maparea intervalului

Caseta listă {Off; Adresă IP la adresa IP}, implicit = „Dezactivat”

Off-Adresa sursă și (sau) portul vor fi înlocuite cu valorile din parametrii „**Rescrie IP-ul sursă**” și "**Rescrie portul sursă**”. Acest lucru se aplică numai dacă acești parametri sunt setați (nu sunt setați ca 0.0.0.0).

Adresă IP la adresa IP (NETMAP)-Rescrierea maparii intervalului adresei IP sursei. Noua adresă sursă va conține prefixul de la parametrii „**Rescrie IP sursă**" și "**Rescrie IP/Mască sursă**". Restul adresei sursă va fi completată de adresa sursă inițială.

Rescrie IP-ul sursă

Adresă IP, implicită = 0.0.0.0/0

Definește o nouă adresă sursă. Valoarea 0.0.0.0/0 înseamnă că adresa sursă nu este modificată.

Rescrie portul sursă

Număr {0 - 65535}, implicit = 0

Definește un nou port sursă (rescrierea mai multor porturi definite într-unul singur). Valoarea 0 înseamnă că portul sursă nu este schimbat.

Nota

Comentariu optional.

7.3.3.2. Destinație NAT

Destination Network Address Translation (DNAT) - rescrie adresa de destinație și/sau portul în conexiunea de intrare și efectuează modificări opuse pentru pachetele returnate.

DNAT:

• Permite redirecționarea destinației conexiunii către un dispozitiv care efectuează DNAT.

• Se efectuează în timpul introducerii pachetelor pe un dispozitiv (înainte de redirecționare și filtrare în firewall).

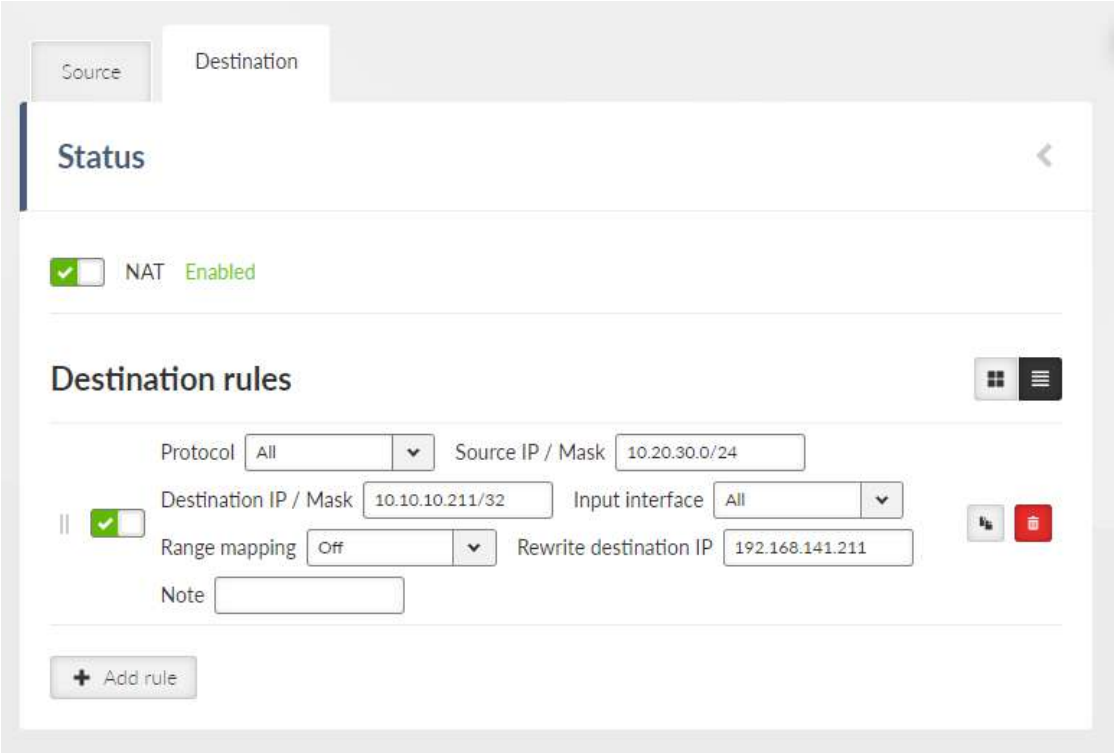


Fig. 7.18: SETĂRI > Firewall > NAT

Permite

Caseta listă {Activare; Disable}, implicit = "Disable"
Activează/dezactivează toate regulile Destination NAT.

Parametrii „**Protocol**”, “**IP sursă / Mască**”,„**IP de destinație / Mască**”, „**Interfață de ieșire**”,“**Port sursă de la** ”, “**Port sursă către**”, “**Port de destinație din**”, “**Port de destinație către**” și ”**Numărul protocolului**” definiți un filtru, care captează pachetele specificate. Regula SNAT se aplică pentru acele pachete.

Parametrii „**Port sursă de la**”, “**Port sursă către**”, “**Port de destinație din**” și ”**Port de destinație către**” apar numai dacă parametrul „Protocol” este setat la „UDP” sau „TCP”.

Parametrul „**Numărul protocolului**” apare numai dacă parametrul “**Protocol**” este setat la „Altele”.

Protocol

Filtrează protocolul selectat. Dacă niciuna dintre valorile menționate nu se potrivește, selectați „Altele”.

Numărul protocolului

Număr {0 – 255}, implicit = 1
Acest parametru apare numai dacă parametrul „**Protocol**” este setat la „Altele”.

IP sursă / Mască

Adresă IP, implicită = 0.0.0.0/0
Definește subrețeaua IP sursă.

Port sursă (de la) / Port sursă (către)

Număr {0 – 65535}, implicit = 0
Definește intervalul de valori al portului sursă. Valoarea 0 înseamnă că nu este filtrată în funcție de portul sursă. Dacă este necesar un singur port, setați ambii parametri pe același număr. Acești parametri apar numai dacă parametrul „**Procotol**” este setat la „UDP” sau „TCP”.

IP de destinație / Mască

Adresă IP, implicită = 0.0.0.0/0
Definește subrețeaua IP de destinație.

Port de destinație (de la) / Port de destinație (la)

Definește intervalul de valori al portului de destinație. Valoarea 0 înseamnă că nu este filtrată în funcție de portul de destinație. Acești parametri apar numai dacă parametrul „**Procotol**” este setat la „UDP” sau „TCP”.

Interfață de intrare

Caseta listă {Toate; WWAN; Toate ETH; EXT; GRE3; Altele}, implicit = „Toate”
Filtrează interfețele selectate.

Introduceți numele interfeței

Trebuie setat ca una dintre interfețele existente (numele interfeței LAN (sau VLAN), numele tunelului GRE etc.). Acest parametru apare numai dacă parametrul „**Interfață de intrare**” este setat la „Altele”.

Maparea intervalului

Caseta listă {Off; Adresă IP la adresa IP}, implicit = „Dezactivat”

- Off – Adresa de destinație și (sau) portul vor fi înlocuite cu valorile din parametrii „**Rescrieți IP-ul de destinație** ” și ”**Rescrieți portul de destinație**”. Acest lucru se va aplica numai dacă acești parametri sunt setați (nu sunt setați ca 0.0.0.0).
- Adresă IP la adresa IP (NETMAP) – Rescrierea maparii intervalului adresei IP sursei. Noua adresă sursă va conține prefixul de la parametrii „**Rescrie IP sursă**” și ”**Rescrie IP/Mască sursă**”. Restul adresei sursă va fi completată de adresa sursă inițială.
- Port la adresa IP (PORTMAP): maparea intervalului de porturi de destinație (parametrii „**Port de destinație din** ”, “**Port de destinație către**”). Noua mapare a zonei a originilor porturilor de destinație în parametrul „ **Rescrieți IP-ul de destinație**”. Poate fi suprascris suplimentar la parametrul „**Rescrieți portul de destinație** ”.

Exemplu:

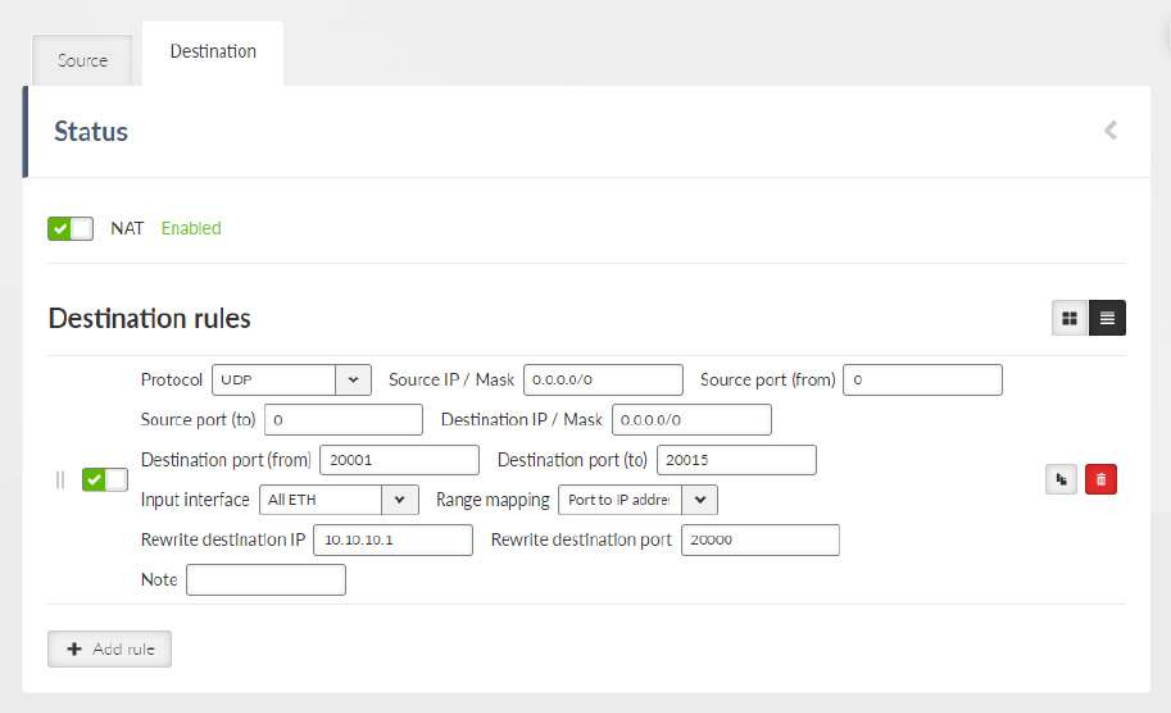


Fig. 7.19: SETĂRI > Firewall > NAT

Explicația parametrilor netipici și interesanți:

Port de destinație (de la) și Port de destinație (la)

Regula DNAT se aplică numai datelor UDP cu porturi de destinație în intervalul 20001-20015

Interfață de intrare

Datele trebuie primite pe orice port ETH

Maparea intervalului

Setați la „Port la adresa IP" - adică, porturile de destinație modifică adresa(ele) IP de destinație în consecință.

Rescrieți IP-ul de destinație și Rescrieți portul de destinație

Setați la IP 10.10.10.1 și la portul 502 - rezultând un interval de IP-uri 10.10.10.1 - 10.10.10.15 datorită porturilor de destinație ale datelor UDP primite într-un interval de 20001-20015 (15 porturi = 15 adrese IP). Un port nou este întotdeauna 20000 (adică, portul implicit DNP3).

Rescrieți IP-ul de destinație

Adresă IP, implicită = 0.0.0.0/0

Definește o nouă adresă de destinație. Valoarea 0.0.0.0/0 înseamnă că adresa de destinație nu este schimbată.

Rescrieți portul de destinație

Număr {0 – 65535}, implicit = 0

Definește un nou port de destinație (rescrierea mai multor porturi definite într-unul singur). Valoarea 0 înseamnă că portul de destinație nu este schimbat.

Nota

Comentariu optional.

Nota

Conexiunea FTP este un tip special de TCP cu sesiuni multiple deschise și funcționalitate internă. Dacă configurați DNAT pentru serverul FTP conectat, activați parametrul „FTP connection tracker” și specificați un port corect (implicit este 21). Acești parametri pot fi setați numai în meniul Avansat.

7.3.3.3. Cooperare cu alte servicii

• Regula MASQUERADE pentru conexiunea celulară are prioritate mai mică decât NAT-ul utilizatorului (este testat după NAT), astfel încât este posibil să se creeze excepții în setările NAT.

• Prin utilizarea DNAT este posibil să interceptați o conexiune care trece și să o redirecționați în M!DGE3 (similar cu un comportament proxy).

• Pentru redirecționare

  ○ Adresa IP locală va fi completată în „**Rescrieți IP-ul de destinație**” parametru.

  ○ Portul de serviciu, către care este redirecționată adresa locală va fi completat în „**Rescrieți portul de destinație**” parametru.

NAT și IPsec

• DNAT poate fi utilizat înainte de a împacheta un pachet în IPsec. Pentru mai multe informații vezi*Secțiunea 7.4.1.3, „Interacțiunea cu DNAT”*.

• SNAT funcționează pe pachete dezambalate din IPsec.

• SNAT poate fi folosit înainte de a împacheta un pachet în IPsec (parametrul „**Interfață de ieșire**” trebuie setat la „Toate”)

• Regulile SNAT și MASQUERADE (de la Cellular) modifică adresele pachetelor înainte de capturarea prin selector de trafic IPsec.

7.4. VPN

VPN (Virtual Private Network) extinde o rețea privată într-o rețea publică și permite utilizatorilor să trimită și să primească date prin rețele partajate sau publice, ca și cum dispozitivele lor de calcul ar fi conectate direct la rețeaua privată. Prin urmare, aplicațiile care rulează prin VPN pot beneficia de funcționalitatea, securitatea și managementul rețelei private.

7.4.1. IPsec

Internet Protocol Security (IPsec) este o suită de protocoale de rețea care autentifică și criptează pachetele de date trimise printr-o rețea. IPsec include protocoale pentru stabilirea autentificării reciproce între agenți la începutul sesiunii și negocierea cheilor criptografice pentru utilizare în timpul sesiunii. IPsec folosește servicii de securitate criptografică pentru a proteja comunicațiile prin rețele IP (Internet Protocol). IPsec acceptă autentificarea peer la nivel de rețea, autentificarea de origine a datelor, integritatea datelor, confidențialitatea datelor (criptare) și protecția la reluare. IPsec este o schemă de securitate end-to-end care funcționează

în stratul Internet al Internet Protocol Suite. IPsec este recunoscut ca o soluție sigură, standardizată și bine dovedită de către publicul profesionist.

Deși există 2 moduri de funcționare, M!DGE3 oferă doar un mod Tunel. În modul Tunnel, întregul pachet IP este criptat și autentificat. Acesta este apoi încapsulat într-un nou pachet IP (ESP – Encapsulating Security Payloads) cu un nou antet IP.

Criptografia simetrică este utilizată pentru a cripta pachetele. Cheile simetrice trebuie să fie livrate în siguranță către egal. Pentru a menține o conexiune sigură, cheile simetrice trebuie schimbate în mod regulat. Protocolul utilizat pentru schimbul securizat de chei este IKE (Internet Key Exchange). Atât versiunea IKE 1, cât și versiunea mai nouă 2 sunt disponibile în M!DGE3.

Comunicarea protocolului IKE cu peer-ul este stabilită folosind cadre UDP pe portul 500. Cu toate acestea, dacă sunt active NAT-T (NAT Traversal) sau MOBIKE (MOBILE IKE), se folosește în schimb portul UDP 4500.

Nota

NAT-T este recunoscut automat de implementarea IPsec în M!DGE3.

Tunelul IPsec este furnizat de Asociația de Securitate (SA). Există 2 tipuri de SA:

• IKE SA: Asociația de securitate IKE care oferă schimb de chei SA cu peer-ul.

• CHILD SA: Asociația de Securitate IPsec care asigură criptarea pachetelor.

Fiecare tunel IPsec conține 1 IKE SA și cel puțin 1 CHILD SA. În M!DGE3 pot fi setate maxim 24 IKE_SA și 48 CHILD_SA (TS).

Autentificarea securizată a partenerului de legătură (peer) este asigurată prin metoda de autentificare cu cheie pre-partajată (PSK): ambii parteneri de legătură au aceeași cheie (parolă).

Pe măsură ce CHILD SA expiră, noi chei sunt generate și schimbate folosind IKE SA.

Pe măsură ce versiunea IKE SA IKEv1 expiră - are loc o nouă autentificare și schimb de chei și este creat un nou IKE SA. Orice SA CHILD aparținând acestei IKE SA este de asemenea recreată.

Pe măsură ce versiunea IKE SA IKEv2 expiră, poate apărea unul dintre cele două scenarii diferite:

• Dacă este necesară re-autentificarea - comportamentul este similar cu IKEv1 (vezi mai sus).

• Dacă re-autentificarea nu este necesară - sunt generate și schimbate doar cheile IKE SA noi.

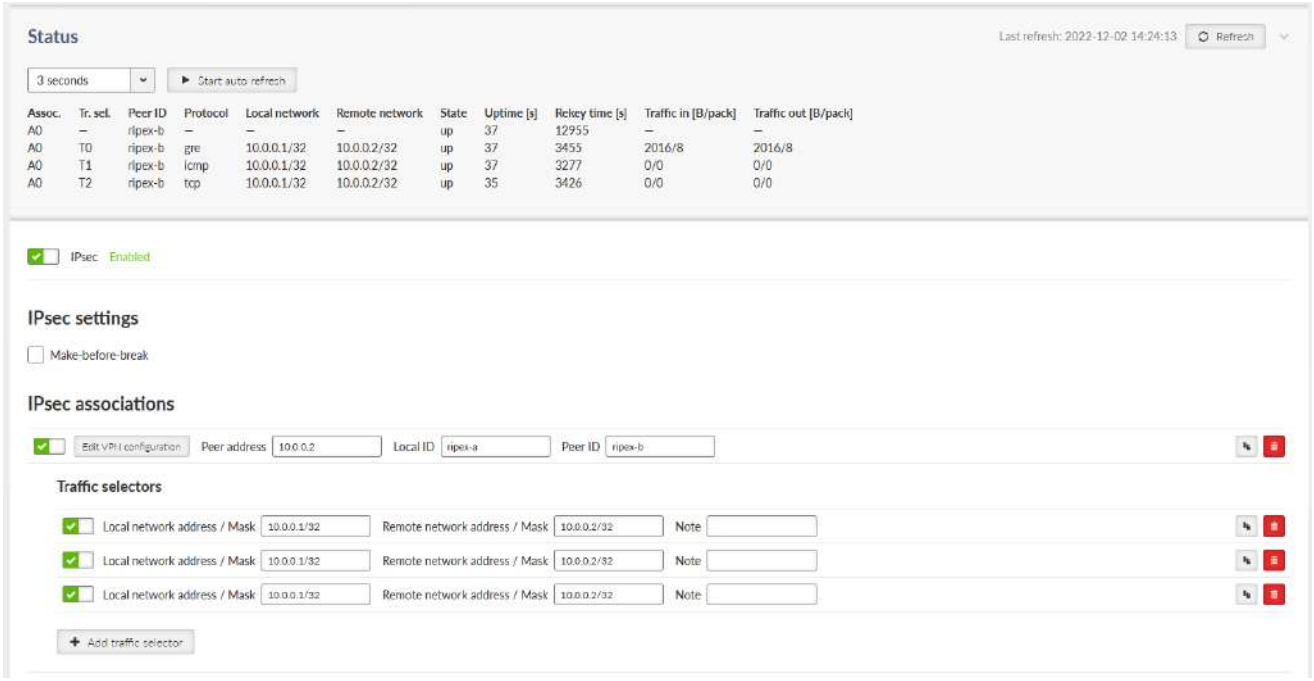


Fig. 7.20: SETĂRI > VPN > IPsec

IPsec

{Permite; Dezactivați}, implicit = „Dezactivați”

sistemul IPsec pornește/dezactivează

Pot exista maximum 16 CHILD SA active (în total peste toate Active IKE SA).

Fiecare linie „Activă” trebuie să aibă un echivalent pe partea egală cu câmpurile inversate „Rețea locală...” și „Rețea la distanță...”.

Câmpurile „Rețea locală...” și „Rețea la distanță...” trebuie să conțină diferite intervale de adrese și nu trebuie să interfereze cu conexiunea de serviciu USB (10.9.8.7/28) sau cu conexiunea internă la FPGA (192.0.2.233/30).

Fiecare selector de trafic „Activ” din tabelul de configurare trebuie să fie unic.

7.4.1.1. Setări IPsec

Faceți înainte de pauză

{Pe; Off}, implicit = „Dezactivat”

Acest parametru este valabil pentru toate IKE SA care utilizează IKEv2 cu re-autentificare. O conexiune temporară întreruptă în timpul re-autentificării IKE_SA este suprimată de acest parametru. Este posibil ca această funcție să nu funcționeze corect cu unele implementări IPsec (pe peer side).

7.4.1.2. Asociații IPsec

Pentru a configura în continuare tunelul VPN IPsec, faceți clic pe**Adăugați configurația VPN**buton.

Adăugați / Editați asocierile de tunel VPN IPsec

Fiecare articol din tabel reprezintă un IKE SA. Pot exista maximum 24 IKE SA active (limitate de resursele sistemului).

Stare de pornire

Caseta listă {Pasiv; La cerere; Start}, implicit = „Pasiv”

MOBIKE

Caseta listă {On; Off}, implicit = „Activat”

Activează MOBIKE pentru IKEv2 care acceptă mobilitatea sau migrarea tunelurilor. Vă rugăm să rețineți că IKE este mutat de la portul 500 la portul 4500 când MOBIKE este activat. Configurația peer trebuie să se potrivească. Este recomandat să folosiți modul MOBIKE în cazul direcționării traficului prin interfața celulară.

Detectarea egalilor morți

Caseta listă {On; Off}, implicit = „Activat”

Detectarea conexiunii pierdute cu peer-ul. Pachetele de testare IKE sunt trimise periodic. Când pachetele nu sunt confirmate după mai multe încercări, conexiunea este închisă (acțiunile corespunzătoare sunt inițializate). În cazul în care Detectarea nu este activată, se descoperă o pierdere a conexiunii atunci când este inițiat procesul obișnuit de schimb de chei.

Perioada DPD [e]

Număr {5 - 28800}, implicit = 30

Perioada de verificare a detectării de peer mort. Acest parametru este disponibil numai dacă este parametru**Detectarea egalilor morți**este setat pe „Pornit”.

Acțiunea DPD

Caseta listă {Clear; Țineți; Restart}, implicit = „Hold”

Una dintre cele trei stări de conectare se activează automat când se detectează pierderea conexiunii:

Clear – conexiunea este închisă și așteaptă

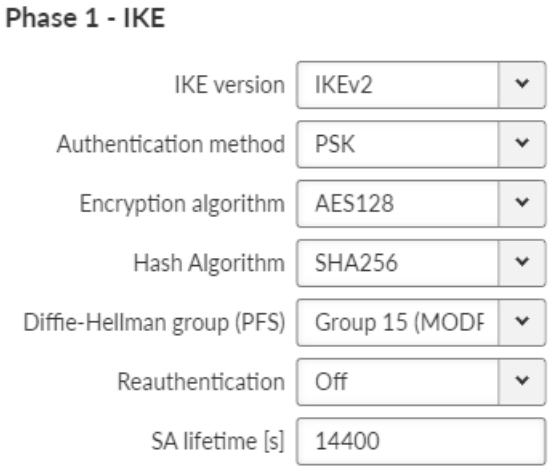
Hold – conexiunea este închisă. Conexiunea este stabilită atunci când se încearcă primul pachet de transmisie prin tunel.

Restart – conexiunea este stabilită imediat

Acest parametru este disponibil numai dacă este parametru**Detectarea egalilor morți**este setat pe „Pornit”.

Faza 1 IKE

Parametrii legați de IKE SA (IKE Security Association) asigură schimbul de chei SA cu peer-ul.



Metoda de autentificare

Caseta listă {PSK}

Metoda de autentificare peer. Configurația peer trebuie să se potrivească.

Negocierea „modul principal” este singura opțiune acceptată. „Modul agresiv” nu este acceptat; este recunoscut ca nesigur atunci când este combinat cu tipul de autentificare PSK.

Algoritm de criptare IKE

Caseta listă {3DES (moștenire); AES128; AES192; AES256; AES128CCM (AEAD); AES192CCM (AEAD); AES256CCM (AEAD); AES128GCM (AEAD); AES192GCM (AEAD); AES256GCM (AEAD); ChaCha20Poly1305 (AEAD)}, implicit = „AES128”

Algoritm de criptare IKE SA. Metodele marcate „moștenire” sunt recunoscute ca fiind nesigure. Configurația peer trebuie să se potrivească.

Algoritm de integritate IKE

Caseta cu listă {MD5 (moștenire); SHA1 (moștenire); SHA256; SHA384; SHA512}, implicit = "SHA256" algoritm de integritate IKE SA. Metodele marcate „moștenire” sunt recunoscute ca fiind nesigure. Configurația peer trebuie să se potrivească.

Valoarea de verificare a integrității IKE

Caseta listă {64b; 96b; 128b}, implicit = „96b”

Lungimea valorii de verificare a integrității IKE (ICV) pentru algoritmii de criptare AEAD din IKE SA. Activ numai pentru criptarea AES AEAD (AES-CCM și AES-GCM), „ChaCha20Poly1305” are o lungime ICV fixă de 128 de biți.

IKE Funcție pseudo-aleatorie

Caseta listă {SHA256; SHA384; SHA512}, implicit = „SHA256”

algoritm IKE SA pentru generarea de date pseudoaleatoare.

Grupul IKE Diffie-Hellman (PFS)

Caseta listă {Niciuna (moștenire); Grupa 2 (MODP1024, moștenire); Grupa 5 (MODP1536, moștenire); Grupa 14 (MODP2048); Grupa 15 (MODP3072); Grupa 25 (ECP192); Grupa 26 (ECP224); Grupa 19 (ECP256); Grupa 20 (ECP384); Grupa 21 (ECP521); Grupa 27 (ECP224BP); Grupa 28 (ECP256BP); Grupa 29 (ECP384BP); Grupa 30 (ECP512BP); Grupa 31 (X25519); Grupul 32 (X448)}, implicit = „Grupul 15 (MODP3072)”

Caracteristica PFS (Perfect Forward Secrecy) este realizată folosind metoda grupului Diffie-Hellman.

PFS mărește securitatea schimbului de chei IKE SA. Metodele marcate „moștenire” sunt recunoscute ca fiind nesigure. Configurația peer trebuie să se potrivească.

Cu cât grupul Diffie-Hellman este mai mare, cu atât securitatea este mai mare, dar și sarcina de rețea și procesor este mai mare.

Reautentificare

Caseta listă {On; Off}, implicit = „Dezactivat”

Acest parametru este valid dacă este utilizat IKEv2. Acesta determină următoarea acțiune după expirarea IKE SA. Când este activat: noul IKE SA este negociat, inclusiv o nouă autentificare peer. Când este dezactivat: sunt schimbate doar cheile noi.

IKE SA durata de viață [s]

Număr {180 – 86400}, implicit = 14400 s (4 ore)

Timpul valabilității SA. Noul schimb de chei sau reautentificarea este declanșată imediat ce cheia expiră. Timpul real de expirare este selectat aleatoriu în intervalul 90-110%. Din păcate, cu cât schimbul de chei este mai frecvent, cu atât sarcina rețelei și procesorului este mai mare.

Nota

Dacă se utilizează un canal de capacitate mică, încărcarea canalului M!DGE3 poate fi afectată în timpul procesului de schimb de chei.

IKE Post-quantum PSK (PPK)

Caseta listă {On; Off}, implicit = „Dezactivat”

Permite protecție suplimentară folosind PPK atunci când utilizați IKEv2.

ID-ul IKE PPK

Șir {0–64 caractere}, implicit = <gol>

Identificatorul cheii PPK, care poate fi un FQDN. Nu trebuie să fie gol sau identic cu identificatorul din alt IKE SA. Este folosit pentru a identifica și selecta cheia PPK între egali, iar aceștia trebuie să aibă același identificator.

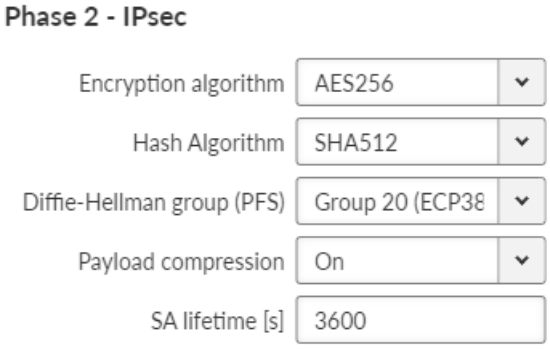
ID-ul cheii IKE PPK

Caseta listă {Niciuna; Cheie de criptare radio}, implicit = „Niciuna”

Identificatorul cheii în breloc. Cheia trebuie să existe și să fie populată cu tipul „psk” și o lungime de cel puțin 32B (256 de biți).

Faza 2 – IPsec

Anumiți parametri sunt împărtășiți de toți subordonații CHILD SA. IPsec Security Association oferă criptarea pachetelor (criptarea traficului utilizatorului).



Algoritm de criptare

Caseta listă {3DES (moștenire); AES128; AES192; AES256}, implicit = „AES128”

Algoritm de criptare IKE CHILD SA. Metodele marcate „moștenire” sunt recunoscute ca fiind nesigure. Configurația peer trebuie să se potrivească.

Algoritmul de integritate IPsec

Caseta cu listă {MD5 (moștenire); SHA1 (moștenire); SHA256; SHA384; SHA512}, implicit = "SHA256" algoritm de integritate IKE CHILD SA. Metodele marcate „moștenire” sunt recunoscute ca fiind nesigure. Configurația peer trebuie să se potrivească.

Aceeași valoare ca cea selectată pentru algoritmul Integrity, este utilizată pentru PRF (Funcția Pseudo-Random).

Valoarea de verificare a integrității IPsec

Caseta listă {64b; 96b; 128b}, implicit = „96b”

Lungimea valorii de verificare a integrității IPsec (ICV) pentru algoritmii de criptare AEAD din IKE SA. Activ numai pentru criptarea AES AEAD (AES-CCM și AES-GCM), „ChaCha20Poly1305” are o lungime ICV fixă de 128 de biți.

Grupul IPsec Diffie-Hellman (PFS)

Caseta listă {Niciuna (moștenire); Grupa 2 (MODP1024, moștenire); Grupa 5 (MODP1536, moștenire); Grupa 14 (MODP2048); Grupa 15 (MODP3072); Grupa 25 (ECP192); Grupa 26 (ECP224), Grupa 19 (ECP256); Grupa 20 (ECP384); Grupa 21 (ECP521); Grupa 27 (ECP224BP); Grupa 28 (ECP256BP); Grupa 29 (ECP384BP); Grupa 30 (ECP512BP); Grupa 31 (X25519); Grupul 32 (X448)}, implicit = „Grupul 15 (MODP3072)”

Caracteristica PFS (Perfect Forward Secrecy) este realizată folosind metoda grupului Diffie-Hellman.

PFS mărește securitatea schimbului de chei IKE CHILD SA. Metodele marcate „moștenire” sunt recunoscute ca fiind nesigure. Configurația peer trebuie să se potrivească.

Cu cât grupul Diffie-Hellman este mai mare, cu atât securitatea este mai mare, dar și sarcina de rețea și procesor este mai mare.

Comprimarea sarcinii utile

Acest parametru permite compresia sarcinii utile. Acest lucru are loc înainte de criptare. Configurația peer trebuie să se potrivească.

Durata de viață IPsec SA [s]

Număr {180 – 86400}, implicit = 3600 s (1 oră)

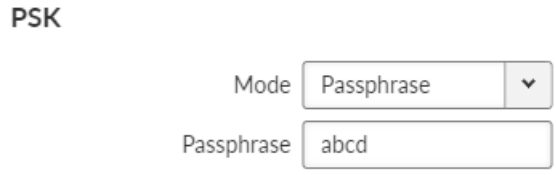
Timpul valabilității CHILD SA. Noul schimb de chei sau reautentificarea este declanșată imediat ce expiră cheia. Timpul real de expirare este selectat aleatoriu în intervalul 90-110%. Durata de viață SA pentru CHILD SA este în mod normal mult mai scurtă decât durata de viață SA pentru IKE SA deoarece CHILD SA transferă în mod normal mult mai multe date decât IKE SA (doar schimbul de chei). Schimbarea cheilor servește ca protecție împotriva spargerii cifrului prin analizarea unor cantități mari de date criptate de același cifr.

Nota

Dacă se utilizează un canal de capacitate mică, încărcarea canalului M!DGE3 poate fi afectată în timpul procesului de schimb de chei.

PSK

Autentificarea PSK (pre-shared key) este utilizată pentru autentificarea IKE SA. Peer-ul relevant este identificat folosind „Peer ID”. Cheia trebuie să fie aceeași atât pentru partea locală, cât și pentru partea de egalitate a IPsec-ului.



Modul

Caseta listă {Passphrase; ID cheie}, implicit = „Expresie de acces”

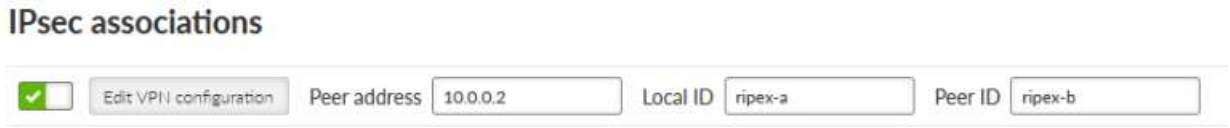
Fraza de acces

Cheia PSK este introdusă ca parolă. Nu este permisă o parolă goală (lungimea maximă este de 128 de caractere). Fraza de acces pentru versiunea FW 2.1.1.0 nu trebuie să conțină caractere neacceptate. Caracterele neacceptate sunt: ", `, \, $, ;. Setul complet de caractere UTF-8 este disponibil începând cu FW 2.1.2.0.

Nota: Dacă parola începe cu caracterele 0x sau 0s, atunci conexiunea între M!DGE3 cu FW 2.1.2.0 (și mai nou) și M!DGE3 cu FW 2.1.1.0 (și mai vechi) nu va fi stabilită. De asemenea, orice alt dispozitiv care scrie parola în configurația sa ca șir simplu (nu codificată „hexa” sau „base64”).

Cheie

Este posibil să setați o cheie de 256 de biți în loc de frază de acces. Acest parametru apare numai dacă este parametru**Modul**este setat la „Cheie”.



Adresa de la egal la egal

Implicit = 0.0.0.0

Adresă IP peer IKE.

ID local

Adresa IP sau FQDN (Nume de domeniu complet calificat) este utilizată ca identificare locală. Trebuie să fie identic cu „ID peer” al peer-ului IKE.

ID peer

Adresa IP sau FQDN (Nume de domeniu complet calificat) este utilizată ca identificare IKE peer. Trebuie să fie identic cu „ID local” al peer-ului IKE. „ID peer” trebuie să fie unic în întregul tabel.

7.4.1.2.1. Selector de trafic

Definește ce trafic este redirecționat către tunelul IPsec. Regula care definește această selecție potrivește un pachet de intrare cu intervalele de adrese „Rețea locală...” și „Rețea la distanță...”.

Adresa rețelei locale/Mască

Adresa IP sursă și masca pachetelor care urmează să fie capturate și redirecționate către tunelul criptat.

Adresă de rețea la distanță / Mască

Adresa IP de destinație și masca pachetelor care urmează să fie capturate și redirecționate către tunelul criptat.

Protocol

Caseta listă {Toate; ICMP; UDP; TCP; GRE; ESP; Altele}, implicit = "Toate" Definește protocolul de transport al pachetelor care vor fi capturate și criptate.

Numărul protocolului

Numărul {1 – 255}, implicit = 1

Definește numărul protocolului de transport al pachetelor care vor fi capturate și criptate. Acest parametru este disponibil numai dacă este parametru**Protocol**este setat la „Altele”.

7.4.1.3. Interacțiunea cu DNAT

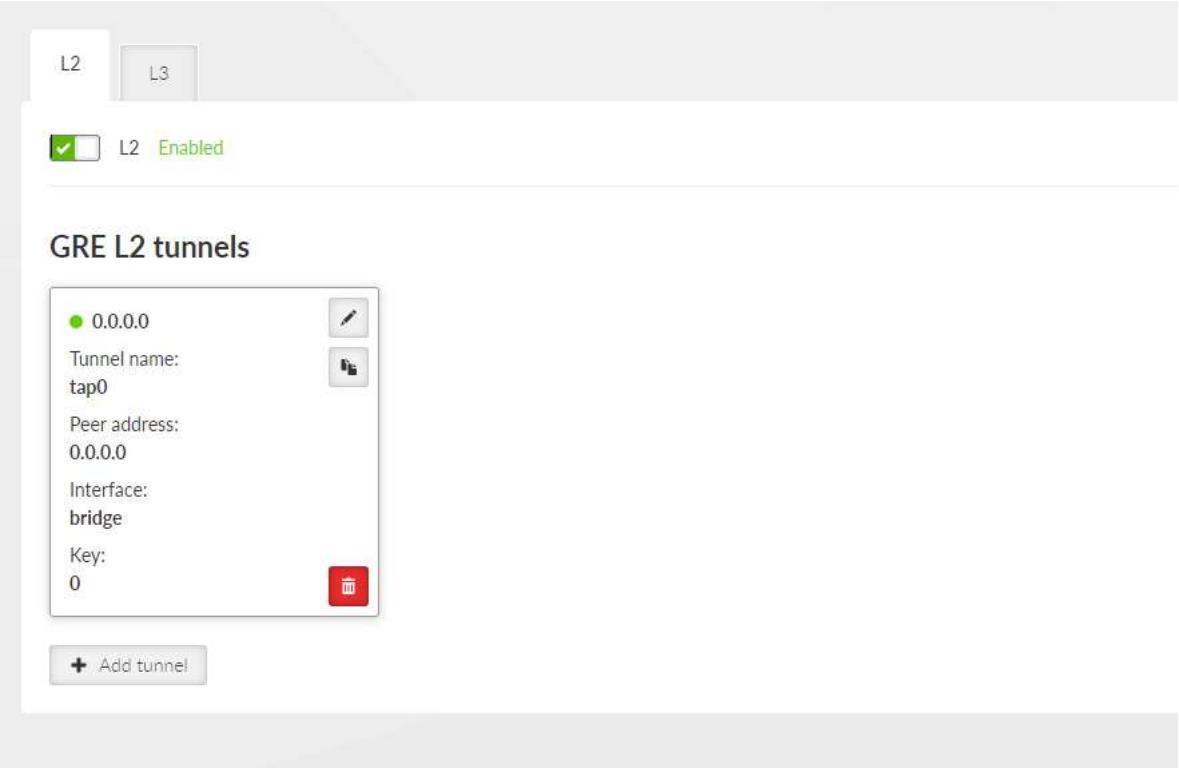
Dacă IPsec captează pachete care au fost modificate de DNAT, regulile de rutare create automat de regulile IPsec nu se vor aplica acestora, deoarece DNAT le rescrie adresa de destinație. Prin urmare, trebuie creată o nouă regulă de rutare statică (SETĂRI > Rutare > Static) pentru acele pachete.

7.4.2. GRE

7.4.2.1. GRE L2

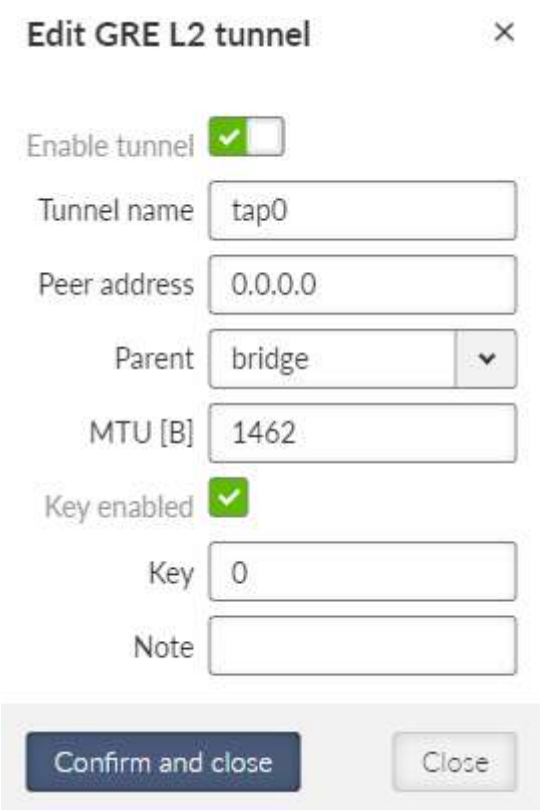
Tunelul GRE L2 este interconectat la pod (interfață LAN) ca unul dintre porturile podului, captează cadre Ethernet ale podului și le trimite la celălalt capăt al tunelului. Acesta permite construirea de punți prin intermediul rețelei complexe și combinarea rețelelor parțiale locale într-o singură rețea.

Tunelul GRE L2 poate fi folosit pentru a tunel traficul Q-in-Q și IPv6 prin rețeaua RipEX IPv4.



Activare GRE L2

Activează sau dezactivează toate tunelurile L2.



Tuneluri individuale L2:

Permite
Activează un anumit tunel L2. Numărul maxim de tuneluri configurabile este de 256.

Numele tunelului
Baza numelui interfeței tunelului, prefixat cu „gre_”.

Adresa de la egal la egal
Adresa IP a echipamentului cu al doilea capăt al tunelului. Această adresă este adresa sursă așteptată a pachetelor GRE primite de la peer.

Mamă
Trebuie setat ca unul dintre numele punții existente în SETARE/Interfețe/Ethernet/Nume interfață de rețea.

MTU [B]
MTU al tunelului L2. Numărul {74 – 1500}, implicit = 1430 B
Deasupra tunelului L2 este 38 B, deci ar trebui să fie GRE MTU = Path MTU - 38.
Valoarea MTU minimă pentru a stabili TCP între unitățile M!DGE3 = 576 B.

Nota
Pentru traficul în rețea cu punte (de exemplu, când se utilizează protocolul Transparent), este necesar să se seteze MTU-ul la o valoare adecvată, altfel există riscul fragmentării pachetelor și astfel să se compromită eficiența și fiabilitatea transferului.

Cheie activată
Permite utilizarea cheii de identificare a tunelului de la/la același peer.

Cheie

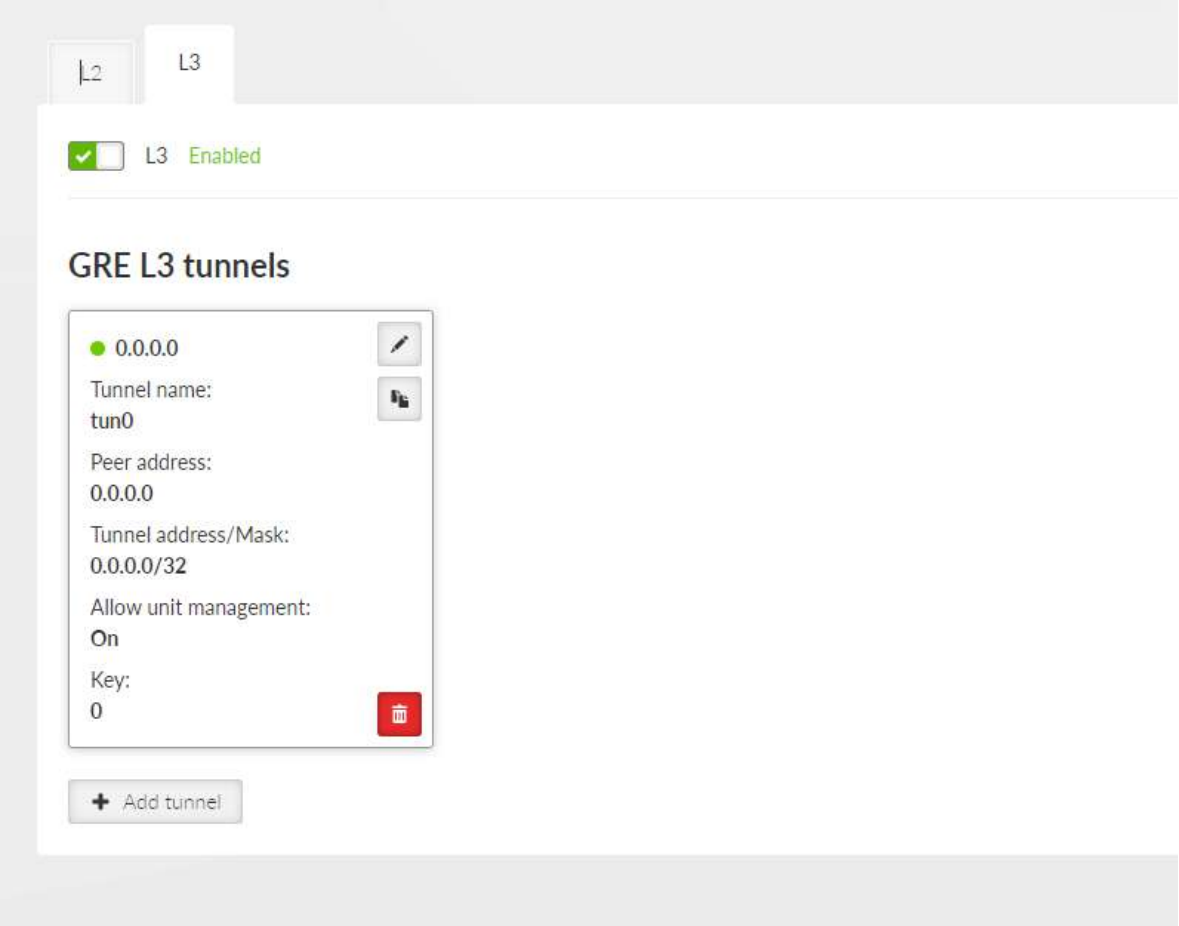
Numărul de identificare al tunelului Număr {0 – 4.294.967.295}, implicit = 0

Nota

Comentariu optional.

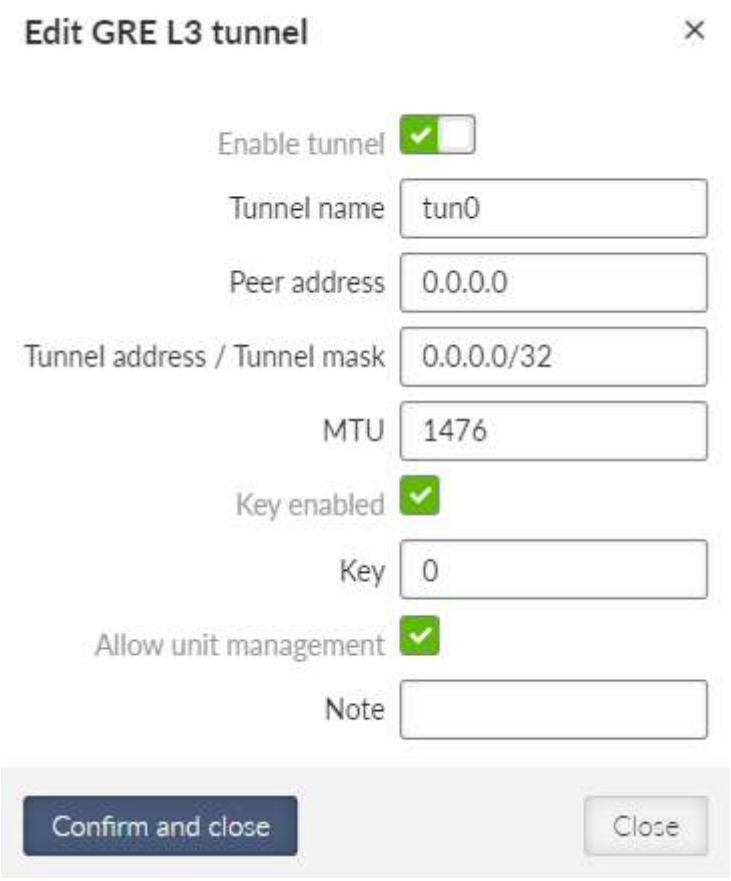
7.4.2.2. GRE L3

Tunelul GRE L3 funcționează ca interfață suplimentară a unității cu propria sa adresă IP (și mască). Regulile de rutare sunt folosite pentru trimiterea pachetelor către această interfață. Conectează o parte a rețelei, așa că pare să fie un singur salt pentru traficul de utilizatori.



Activare GRE L3

Activează sau dezactivează toate tunelurile L3.



Tuneluri individuale L3:

Permite
Activează un anumit tunel L3. Numărul maxim de tuneluri configurabile este de 256.

Numele tunelului
Baza numelui interfeței tunelului, prefixat cu „gre_”.

Adresa de la egal la egal
Adresa IP a echipamentului cu al doilea capăt al tunelului. Această adresă este adresa sursă așteptată a pachetelor GRE primite de la peer.

Adresa tunelului / Masca
Adresa IP și masca interfeței tunelului GRE

MTU

MTU al tunelului L2. Numărul {70 – 1476}, implicit = 1476
Deasupra tunelului L3 este 24 B, deci ar trebui să fie GRE MTU = Path MTU - 24. Dacă MTU este mai mare decât este permis pe traseu, pachetele GRE vor fi aruncate și raportul ICMP va fi trimis înapoi la sursa pachetului original (Path MTU discovery).
Valoarea MTU minimă pentru stabilirea TCP între unitățile M!DGE3 = 576 B.

Cheie activată
Permite utilizarea cheii de identificare a tunelului de la/la același peer.

Cheie
Numărul de identificare al tunelului Număr {0 – 4.294.967.295}, implicit = 0

Permite gestionarea unității
Permite/dezactivează gestionarea unității prin tunelul GRE.

Nota
Comentariu optional.

7.4.3. OpenVPN

OpenVPN este un sistem de rețea privată virtuală (VPN) care permite crearea de conexiuni punct-tomultipunct criptate sigure în moduri direcționate (TUN) sau cu punte (TAP). Până la patru instanțe (clienți și/sau servere) pot fi utilizate simultan într-o unitate. Fiecare server este capabil să stabilească conexiuni cu câteva zeci de clienți.

OpenVPN permite colegilor să se autentifice între ei folosind chei și certificate secrete pre-partajate. Un server OpenVPN este capabil să elibereze un certificat de autentificare pentru fiecare client, folosind semnături și autoritate de certificare (certificatele pot fi generate / încărcate în meniul SETĂRI>Securitate>Acreditări).

O sincronizare de timp a unităților individuale este necesară pentru funcționarea corectă a OpenVPN.

Link pentru *Notă privind aplicația OpenVPN*[4].

Avertizare

Este necesară atenția pentru a preveni buclele de rutare, unde traficul de la legătura dintre punctele finale OpenVPN este redirecționat înapoi în tunelul OpenVPN. Spre deosebire de IPsec, nu există niciun mecanism de protecție împotriva ambalării pachetelor.

7.5. Securitate

Autentificarea utilizatorului este necesară pentru a accesa managementul unității RipEX. Există două tipuri de autentificare a utilizatorului, care diferă în funcție de locația contului de utilizator:

Autentificare locală – conturile de utilizator sunt stocate direct în unitatea RipEX

Autentificare la distanță – conturile de utilizator sunt stocate pe un server de autentificare la distanță (este implementat RADIUS)

Există patru niveluri diferite de privilegii de acces de utilizator – acestea sunt legate de patru roluri diferite de acces de utilizator:

Invitat (role_guest)
Acces numai citire pentru parametrii de configurare (cu excepția părții securizate a configurației). Instrumente de diagnosticare sunt disponibile.

Tehnician (role_tech)
Toate privilegiile rolului Guest plus: acces de scriere pentru partea nesecurizată a configurației; firmware-ul unității up/downgrade.

Tehnician de securitate (role_secttech)
Toate privilegiile rolului de tehnician plus: acces de scriere pentru partea securizată a configurației (cu excepția părților legate de autentificarea unității).

[4] https://www.racom.eu/eng/products/m/ripex/app/openvpn/index.html

Administrator (role_admin)

Fără restricții de nivel de acces. Toate privilegiile rolului de tehnician de securitate plus: gestionarea conturilor de utilizator; configurație de autentificare la distanță.

Limitări:

Tab. 7.2: Prezentare generală a rolurilor și drepturilor din fiecare secțiune

Secțiune	Caracteristici		Roluri / Drepturi			
			Oaspete	Teh	Sec tech	Admin
SETĂRI	Interfețe	Ethernet, COM, Termin-toate serverele, Celular	Numai citire	Scrie	Scrie	Scrie
	Dirijare	Static	Numai citire	Scrie	Scrie	Scrie
		Babel, OSPF, BGP, Gestionarea linkurilor	Nevizibil	Nevizibil	Scrie	Scrie
	Firewall	L2, L3, NAT	Numai citire	Scrie	Scrie	Scrie
	VPN	IPsec	Nevizibil	Nevizibil	Scrie	Scrie
		OpenVPN	Nevizibil	Nevizibil	Scrie	Scrie
		GRE	Numai citire	Scrie	Scrie	Scrie
	Calitatea serviciului		Numai citire	Scrie	Scrie	Scrie
	Securitate	Politică	Nevizibil	Nevizibil	Nevizibil	Scrie
		Local autentificare	Nevizibil	Nevizibil	Nevizibil	Scrie
		Acreditări	Nevizibil	Nevizibil	Nevizibil	Scrie
		Acces de management	Nevizibil	Nevizibil	Nevizibil	Scrie
		RAZĂ	Nevizibil	Nevizibil	Nevizibil	Scrie
		Resetare tamper	Nevizibil	Nevizibil	Nevizibil	Scrie
	Dispozitiv	Unitate	Numai citire	Scrie	Scrie	Scrie
		Configurare	Numai citire	Scrie	Scrie	Scrie
		Evenimente	Numai citire	Scrie	Scrie	Scrie
		Chei software	Numai citire	Scrie	Scrie	Scrie
		Firmware	Nevizibil	Scrie	Scrie	Scrie
	Servicii	Distribuție de firmware	Nevizibil	Scrie	Scrie	Scrie
		SNMP	Nevizibil	Nevizibil	Scrie	Scrie
		SMS	Nevizibil	Nevizibil	Scrie	Scrie
		Standby fierbinte	Numai citire	Scrie	Scrie	Scrie
DIAGNOSTICĂ	Monitorizare		Nevizibil	Scrie	Scrie	Scrie
	Instrumente		Numai citire	Scrie	Scrie	Scrie

Cel puțin un tip de cont de administrator trebuie să fie definit în unitate.

Numărul maxim de sesiuni active simultan este de 64. Un utilizator poate avea mai multe sesiuni deschise în același timp. Dacă se atinge această limită și urmează să fie deschisă o nouă sesiune, cea mai veche sesiune activă este dezactivată și se deschide una nouă.

Numărul maxim de conturi de utilizator locale (toate rolurile împreună) este de 100.

Nota

The**Acces de la distanță**folosește identitatea locală și rolul utilizatorului – nu există autentificare suplimentară la unitatea de la distanță (autentificarea la unitatea locală servește ca conectare la întreaga rețea).

7.5.1. Politică

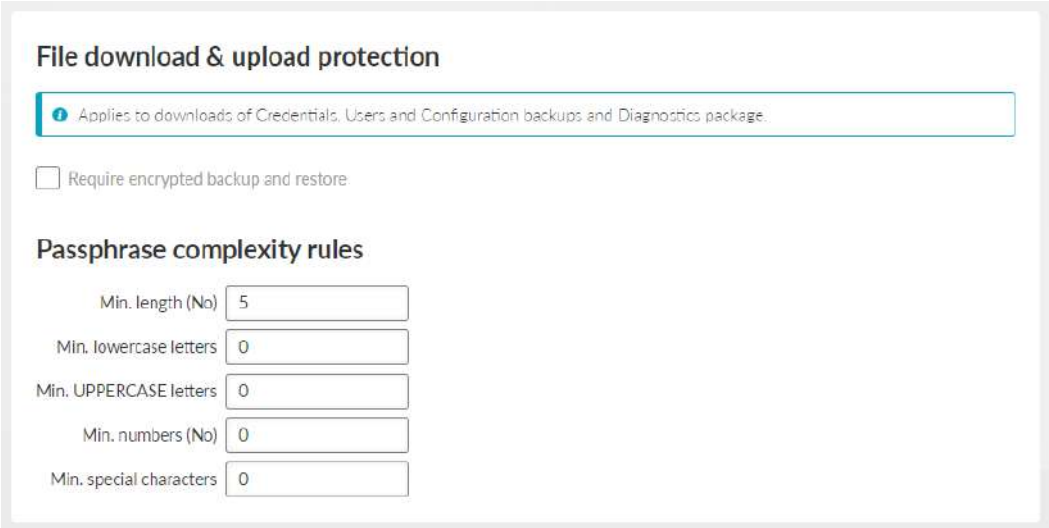


Fig. 7.21: SETĂRI > Securitate > Politică

Această setare se aplică pentru descărcarea de acreditări, utilizatori, copii de rezervă de configurare și pachete de diagnosticare. The**Necesită backup criptat și restaurare**parametrul impune utilizarea fișierelor criptate pentru toți utilizatorii. Următorii parametri vă permit să definiți regulile de complexitate a frazei de acces pentru criptare.

7.5.2. Autentificare locală

7.5.2.1. Conturi de utilizator

Următoarele setări sunt disponibile numai pentru utilizatorii cu rol de Administrator.

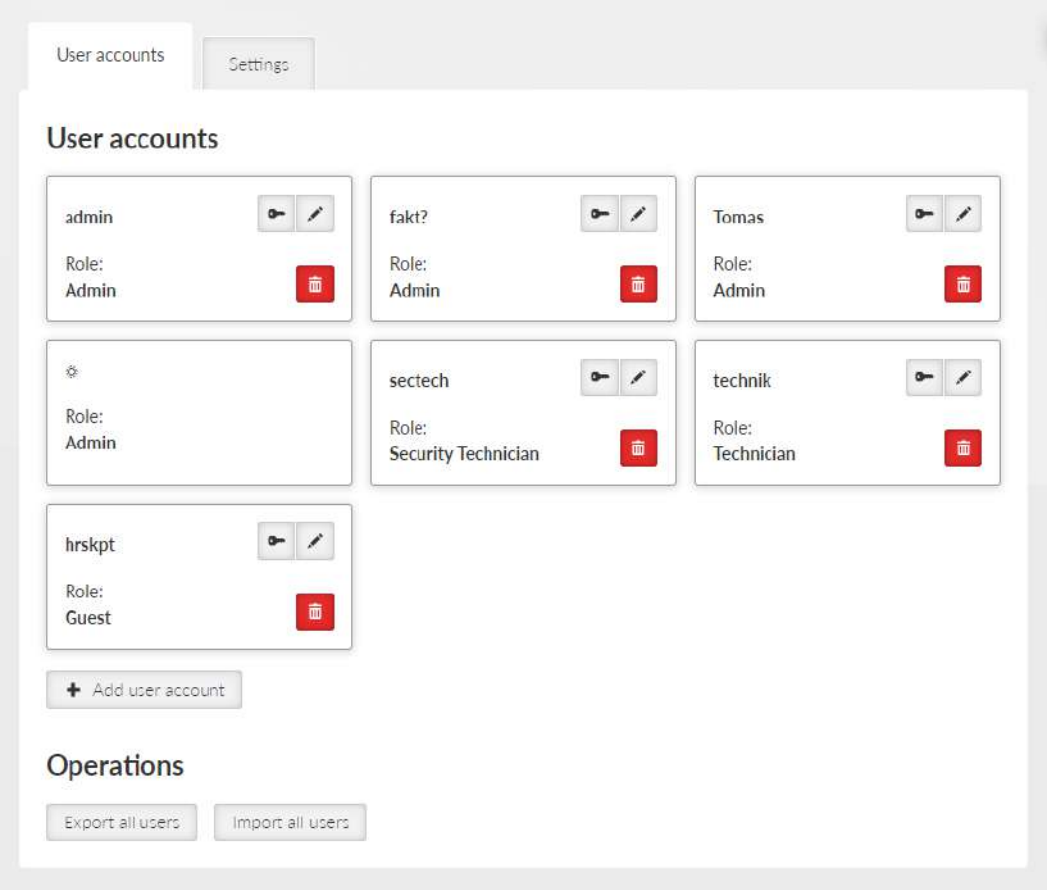


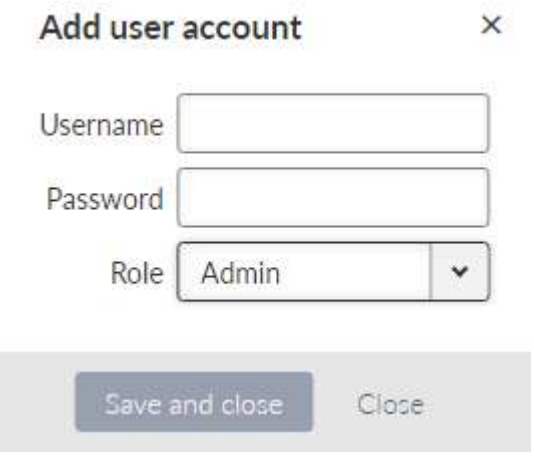
Fig. 7.22: SETĂRI > Securitate > Autentificare locală

Următorii parametri ai contului de utilizator pot fi modificați: parolă, rol de utilizator. Orice cont (așteptați-vă ultimul rol de Administrator) poate fi șters.

Exportați toți utilizatoriibutonul oferă backup pentru toate conturile de utilizator locale într-un fișier.

Importă toți utilizatoriibutonul oferă restaurarea tuturor conturilor de utilizator locale dintr-un fișier de rezervă. Sesiunea activă este deconectată automat după această comandă.

+ Adăugați un cont de utilizatorbutonul invocă dialogul de creare a unui cont de utilizator nou:



Nume de utilizator

Șir {1–128 caractere}, implicit = <gol>

Nume de utilizator nou. Fiecare nume de utilizator din unitate trebuie să fie unic.

Parolă

String {5–128 char}, default = <empty>

Parola este stocată într-un mod sigur.

Rol

Caseta listă {Admin; Tehnician de securitate; Tehnician; Guest}, implicit = „Administrator”

Nota

Este foarte recomandat să creați un nou tip de cont de administrator și să ștergeți contul implicit „Admin”.

Funcție avansată

Când contul de utilizator nu este activ de ceva timp, utilizatorul va fi deconectat automat. Timpul de inactivitate al contului este setat implicit pentru 1 zi. Este posibilă modificarea în intervalul de la 5 minute până la 2 zile (meniul AVANZAT > Generic > Acces utilizator >**Timeout inactivitate web**).

7.5.2.2. Setări

Permite setarea regulilor de complexitate a parolei.

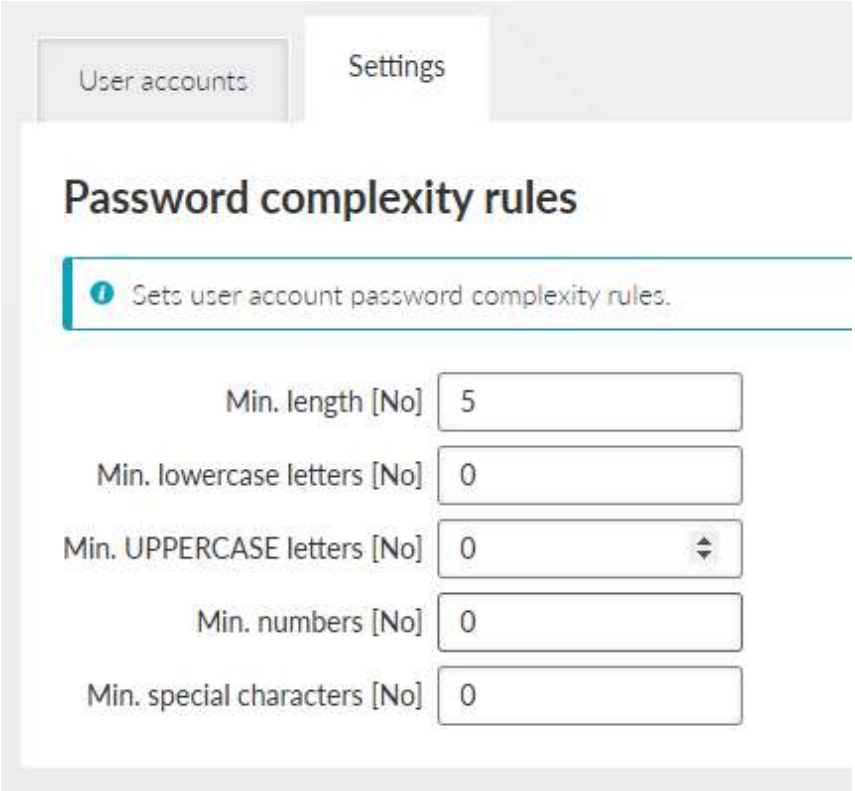


Fig. 7.23: SETĂRI > Securitate > Autentificare locală > Setări

Min. lungime [Nu]

Numărul {5 – 64}, implicit = 5

Lungimea minimă a parolei pentru toți utilizatorii.

Min. litere mici [Nu]
Număr {0 – 5}, implicit = 0
Numărul minim de litere mici (litere engleze) care sunt necesare în parola utilizatorului.

Min. Litere MAJUSCULE [Nu]
Număr {0 – 5}, implicit = 0
Numărul minim de litere mari (litere engleze) care sunt necesare în parola utilizatorului.

Min. numere [Nu]
Număr {0 – 5}, implicit = 0
Numărul minim de caractere numerice (de la 0 la 9) care sunt necesare în parola utilizatorului.

Min. caractere speciale [Nu]
Număr {0 – 5}, implicit = 0
Numărul minim de caractere speciale (nu majuscule sau minuscule în engleză sau numere) care sunt necesare în parola utilizatorului. Literele non-engleze (cum ar fi greacă, rusă, arabă) sunt considerate caractere speciale.

Nota
Setările sunt aplicabile numai pentru parolele noi, parolele deja existente nu vor fi afectate.

7.5.3. Acreditări

Unitățile M!DGE3 oferă o soluție de stocare unificată pentru chei, certificate și alte acreditări. Această stocare este securizată și accesibilă numai utilizatorilor cu permisiunea Sectech și mai mult.

Acreditările sunt separate de configurare pentru a îmbunătăți securitatea și, de asemenea, sunt protejate folosind suma de control pentru a preveni modificările neautorizate. Din acest motiv, toate modificările de depozit/cheie sunt executate imediat și nu trec prin fluxul de lucru „Modificări” ca configurația obișnuită.

Notă: În acest manual și în interfața cu utilizatorul, numim toate intrările de stocare a acreditărilor „Chei”. Deși aceasta este o simplificare, credem că este de înțeles. Mai departe, „Cheile” sunt toate cheile, certificatele publice și private, parametrii DH, lanțurile CA etc.

Avertisment: downgrade-ul unității va reseta întotdeauna toate acreditările la valorile implicite.

7.5.3.1. General

Acreditările sunt stocate în Arhive. Depozitul este un spațiu rezervat, care conține 0-1 Cheie și este adresabil prin intermediul ID-ului său în restul configurației unității. Acest construct, deși poate părea complicat la început, aduce beneficii majore. În principal, utilizatorul poate actualiza pur și simplu certificatele expirate într-un depozit fără a fi nevoie să schimbe configurația folosind acel depozit.

Există două tipuri de chei: Numai citire, ușor de identificat printr-o pictogramă de lacăt și prefixul „_RO_”. Aceste chei sunt încorporate în firmware sau generate automat pe dispozitiv. Restul sunt chei definite de utilizator.

Site-ul de administrare permite utilizatorilor să efectueze diverse operațiuni cu cheile și depozitele.

Folosind butoanele din partea de jos a paginii, le permitem utilizatorilor să descarce o copie de rezervă completă a acreditărilor.

Există două moduri de a restabili acreditările: Înlocuire, care înlocuiește toate cheile cu unele din fișier și Actualizare, care îmbină cheile actuale și noi.

7.5.3.2. Acreditări

Acreditările arată toate arhivele și cheile aflate în prezent pe dispozitiv. Utilizatorii le pot filtra după tip și pot afișa numai cheile valide sau toate. Chenarul cardului și eticheta de jos indică dacă arhiva este goală sau dacă cheia este validă sau invalidă.

Fiecare card reprezintă un Depozit. Titlul cardului este ID-ul depozitului. Toate arhivele definite de utilizator pot fi editate folosind butonul „Editare” și șterse folosind butonul roșu „Ștergere”.

ID
: Identificator unic folosit pentru a face referire la Repository în configurație.
Validat conform expresiei regulate: [a-zA-Z0-9_]\\{1.128\\}. ID-urile care încep cu liniuța de subliniere „_” sunt rezervate pentru cheile Numai citire.

Tip
: Definește tipul de cheie pe care o poate conține depozitul.

Nota
: Comentariu optional.
Există mai multe operații, care pot fi efectuate pe un depozit:

Info
: Afișează informațiile cheie, inclusiv sumele de control.

Genera
: Generează o cheie nouă folosind autoritatea locală de certificare (vezi mai jos).

Actualizare
: Actualizează cheia cu una nouă. Sunt acceptate atât cheile de fișiere, cât și de text, criptate și necriptate.

Descărcați
: Permite descărcarea cheii. Sunt acceptate atât descărcări criptate, cât și necriptate, conform setărilor (vezi mai jos).

Generați CSR (cerere de semnare a certificatului)
: Generează și descarcă CSR din cheile eligibile.

Semnează CSR (cerere de semnare a certificatului)
: Semnează CSR. Atât certificatele de fișiere, cât și certificatele text sunt acceptate. Certificatul semnat este descărcat automat. Este posibil să adăugați modificatorul de certificat „utilizare extinsă a cheii” pentru client/server OpenVPN.

Operația „Adăugați un depozit” creează un depozit gol.

Operațiunile de comandă rapidă „Generați cheia” și „Cheia de încărcare” permit utilizatorilor să creeze un depozit și să genereze/încărcare o cheie în acesta. Aceste butoane nu pot fi folosite pentru a modifica depozitele existente.

7.5.3.3. Chei numai pentru citire

_RO_Ssh_Host_Key
: Tip: cheie SSH (PRI)
Cheia gazdă SSH folosită pentru a autentifica serverul pe client. Dacă lipsește, este generat la pornirea stației.

_RO_Rmt_Access_Host_Key
: Tip: cheie RMTACCESS (PRI)

Cheie gazdă pentru serverul de acces la distanță (QSSH). Este folosit pentru autentificarea serverului. Dacă lipsește, este generat la pornirea stației.

_RO_Rmt_Access_Client_Key

Tip: cheie RMTACCESS (PRI)

Cheie pentru autentificarea clientului de acces la distanță (QSSH) la server. Trebuie să fie prezent pe ambele părți. Obținut de la FW. Dacă diferă de versiunea din FW, este actualizat.

_RO_Web_Private_Key

Tip: Certificat (PRI)

Cheie privată a serverului web (implicit).

Obținut de la FW. Dacă este diferită de versiunea din FW, este actualizată.

_RO_Web_Cert

Tip: Cheie de certificat (PUB)

Certificat de server web (implicit).

Obținut de la FW. Dacă este diferită de versiunea din FW, este actualizată.

_RO_Web_CA_Chain

Tip: CA Chain (PUB)

Șirul de certificat al autorității care a semnat certificatul serverului web. Dacă este autosemnat, acesta va fi gol.

Preluat de la FW. Dacă diferă de versiunea din FW, este actualizat.

_RO_Web_DH_Param

Tip: Parametri DH (PUB)

Parametri pentru schimbul de chei Diffie-Hellman în serverul Web.

Preluat de la FW. Dacă diferă de versiunea din FW, este actualizat.

_RO_File_Distribution_Key

Tip: cheie UFTP (PRI)

Cheie pentru autentificarea stațiilor în serviciul „Distribuire fișiere” (UFTP).

Obținut de la FW. Dacă diferă de versiunea din FW, este actualizat.

7.5.3.4. Setări

Această filă afișează setări suplimentare necesare pentru autoritatea CA locală și regulile de complexitate a frazei de acces pentru descărcările de chei.

Autoritatea locală

ID-ul cheii private

Cheie privată folosită pentru autoritatea locală de certificare.

ID certificat

Certificat public utilizat pentru autoritatea locală de certificare.

Algoritm de semnătură

Algoritm utilizat pentru semnarea certificatelor. Depinde de algoritmul cheie al autorității de certificare și este posibil să nu fie utilizat în cazul în care CA utilizează un anumit algoritm.

Perioada de expirare (zile)

Perioada de expirare în zile. Implicit 7300.

7.5.3.5. Organizare

Conține identificarea organizației utilizată pentru generarea certificatelor.

• Țara

• Cod de țară (precompletat automat, se poate seta manual folosind „Altele” în „Țară”)

• Organizare

• Departamentul

• Locație

• Statul

• Nume comun

• E-mail

7.5.3.6. Reguli de complexitate a frazei de acces

Este necesară o expresie de acces

Dacă este setată la „Nu”, utilizatorii pot descărca chei necriptate (fără parolă).

Fraza de acces - lungime minimă
Numărul {5 – 64}, implicit = 5
Lungimea minimă a parolei.

Fraza de acces - Număr minim de caractere minuscule
Număr {0 – 5}, implicit = 0
Numărul minim de litere mici (litere engleze) care sunt necesare în parolă.

Expresie de acces - Număr minim de caractere majuscule
Număr {0 – 5}, implicit = 0
Numărul minim de litere mari (litere engleze) care sunt necesare în parolă.

Fraza de acces - Număr minim de cifre
Număr {0 – 5}, implicit = 0
Numărul minim de caractere numerice (de la 0 la 9) care sunt necesare în parolă.

Fraza de acces - Număr minim de caractere speciale
Număr {0 – 5}, implicit = 0
Numărul minim de caractere speciale (nu majuscule sau minuscule în engleză sau numere) care sunt necesare în parolă. Literele non-engleze (cum ar fi greacă, rusă, arabă) sunt considerate caractere speciale.

7.5.3.7. Crearea autorității locale de certificare

Pentru a crea CA local, trebuie să urmați acești pași:

1. Generați un nou certificat privat „Cheie de certificat (PRI)”

2. Generați un nou „CA Chain (PUB)” folosind certificatul creat la pasul anterior ca „cheie de certificat”

3. Activați CA local accesând fila Setări și activând CA local, selectând „ID cheie privată” nou creat (= certificat privat nou „Cheie certificat (PRI)”) și „ID certificat” (= nou „LANț CA (PUB)”)

Nota

Cheia privată a serverului web trebuie să utilizeze algoritmi „RSA” sau „EC (ECDSA)”. Alți algoritmi nu sunt acceptați de browserele web.

7.5.4. Acces de management

7.5.4.1. Site-ul administrativ

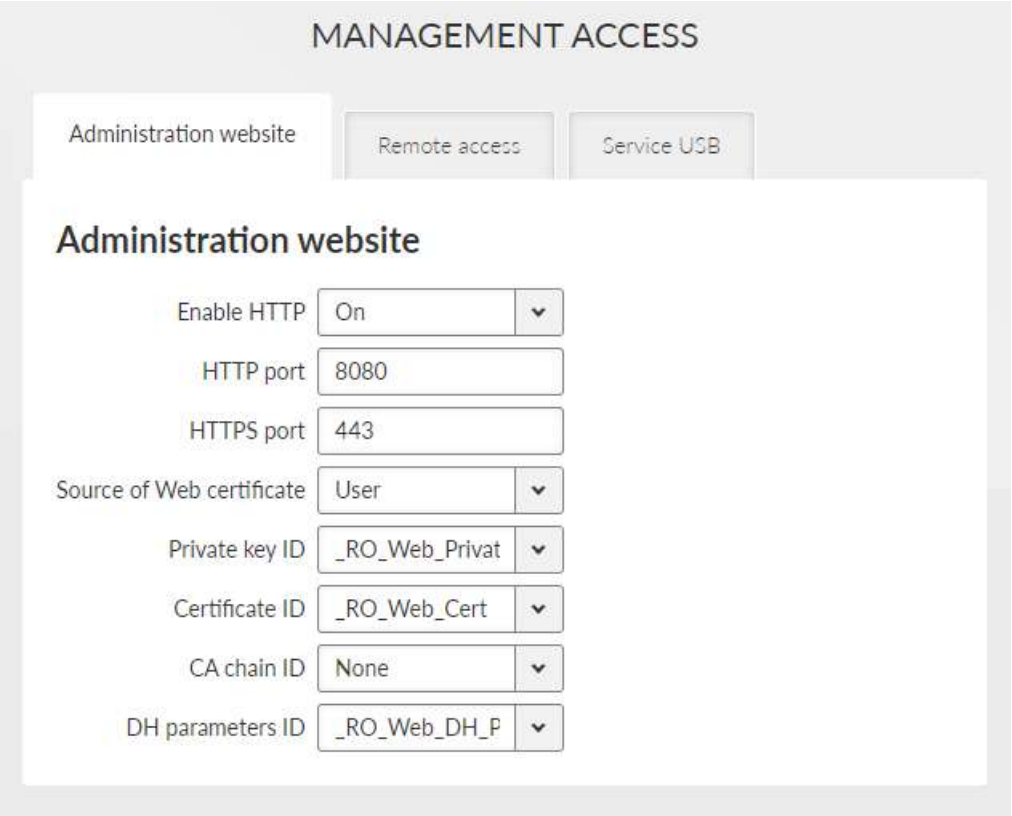


Fig. 7.24: SETĂRI > Securitate > Acces administrare > Site web de administrare

Activați HTTP — Caseta listă {On; Off}, implicit = „Activat”

Activează accesul HTTP la stație. Când este activat, HTTP redirecționează imediat către HTTPS.

Port HTTP — Număr {1 – 65535}, implicit = 80

Numărul portului TCP pe care este disponibil accesul HTTP.

Port HTTPS — Număr {1 – 65535}, implicit = 443

Numărul portului TCP pe care este disponibil accesul HTTPS.

Sursa certificatului Web

Caseta listă {Implicit; Utilizator}, implicit = „Implicit”

Alege sursa certificatului de server Web. „Implicit” folosește cheia, certificatul și parametrul DH distribuit în FW (consultați SETĂRI > Securitate > Acreditări), valorile implicite sunt următoarele:

• Cheie privată: _RO_Web_Private_Key

• Certificat : _RO_Web_Cert

• Lanț CA: _RO_Web_CA_Chain": Lanț CA, al CA care a semnat certificatul. Pentru certificatul autosemnat va rămâne necompletat - Nici unul).

• Parametri DH: _RO_Web_DH_Param

Timeout inactivitate web [min]

Număr {5 – 2880}, implicit = 1440

Când expirarea timpului de inactivitate este atins, sesiunea HTTPS se încheie.

Disponibil în meniul ADVANCED > Security > Management access.

„Utilizator” permite utilizarea cheii de utilizator și a certificatului incluse în stocarea de acreditări. Adăugați certificatul și alte fișiere folosind meniul SETĂRI > Securitate > Acreditări. În casetele de listă individuale vor fi afișate certificatele de chei disponibile pentru fiecare categorie și le puteți alege pe cele adăugate anterior.

7.5.4.2. Acces de la distanță

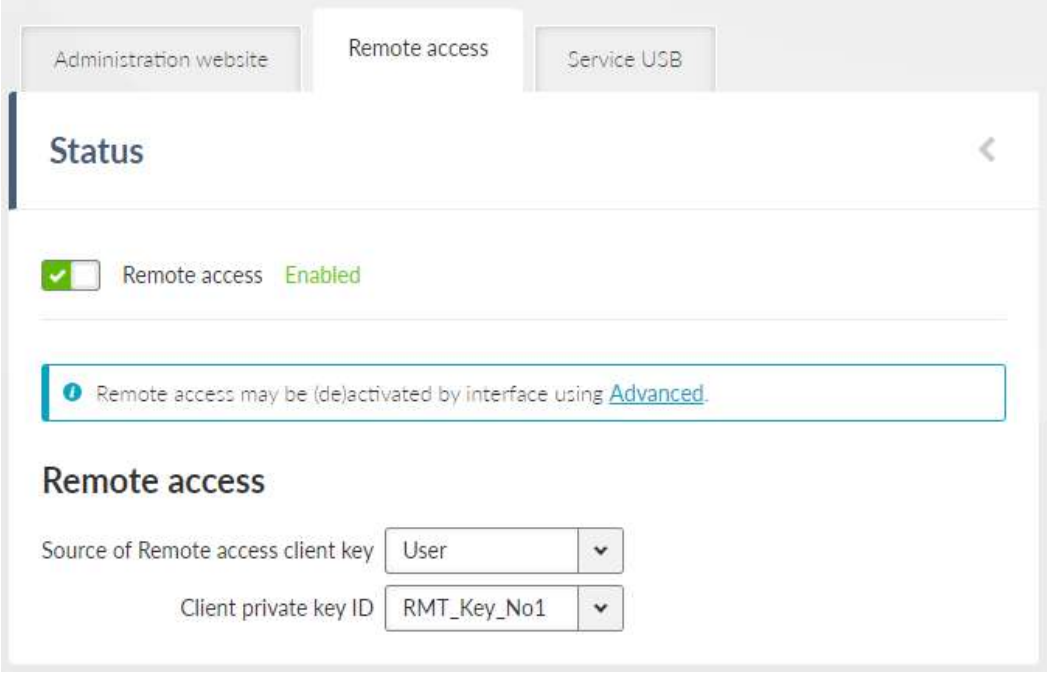


Fig. 7.25: SETĂRI > Securitate > Acces administrare

Activați/Dezactivați

Dacă este activat, permite accesarea unității prin intermediul funcției de acces la distanță.

Nota

Accesul de la distanță este activat sau dezactivat global în acest meniu. Setările individuale pentru fiecare interfață sunt disponibile în meniul AVANZAT. În mod implicit, interfețele Cellular și Ethernet sunt activate, în timp ce toate celelalte interfețe sunt dezactivate. Setările curente sunt afișate în zona Stare.

Sursa cheii clientului de acces la distanță

Caseta listă {Implicit; Utilizator}, implicit = „Implicit”

ID-ul cheii private ale clientului

Când este aleasă caseta de listă Utilizator în listă de mai sus, atunci puteți selecta o cheie descărcată anterior în spațiul de stocare a acreditărilor (SETĂRI > Securitate > Acreditări) sau sau generată în același meniu. Cheia de acces la distanță trebuie să fie aceeași pentru întreaga rețea (sau partea din aceasta pentru care veți utiliza accesul la distanță). Accesul de la distanță la unitate cu o cheie de acces la distanță diferită nu este posibil.

Nota

Utilizarea unui dedicat**Cheie privată a clientului**este foarte recomandat.

7.5.4.3. Serviciu USB

Scopul principal al interfeței de serviciu USB este de a oferi servicii de unitate și acces de gestionare. Conexiunea Ethernet sau WiFi poate fi stabilită folosind un adaptor ETH/USB sau WiFi extern.

În acest scop pot fi utilizați numai adaptoarele furnizate împreună cu produsul.

Vedea*lista de adaptoare disponibile*[5].

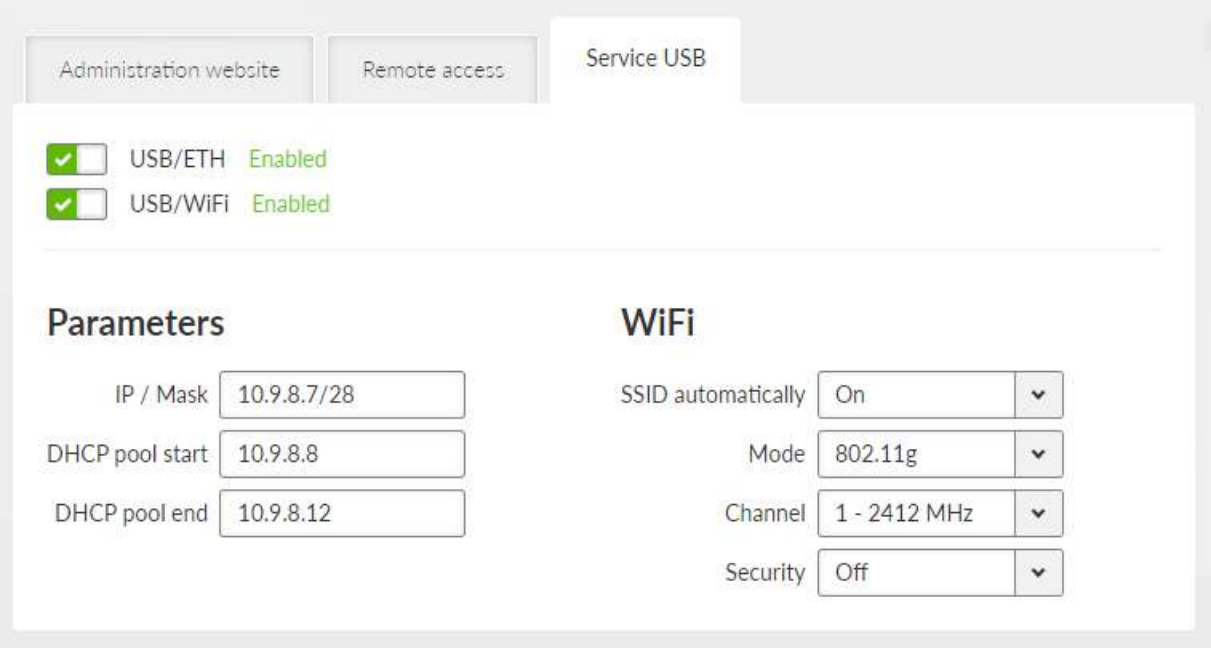


Fig. 7.26: SETĂRI > Securitate > Acces administrare

[5] https://www.racom.eu/eng/products/cellular-router-midge.html#usb_adapters

Serverul DHCP rulează pe această interfață de serviciu pentru a permite conectarea mai ușoară a dispozitivului de management (PC, tabletă sau telefon inteligent).

Activați / Dezactivați

Fiecare dintre serviciile ETH sau WiFi poate fi activat sau dezactivat separat. Când WiFi este activat, unitatea acționează ca un punct de acces WiFi (AP).

Adresă IP/Mască

Adresă IP, implicită = 0.0.0.0/0

Adresa IP a serverului DHCP. Aceasta este adresa IP care trebuie utilizată atunci când accesați gestionarea unității prin această interfață serială.

Pornirea pool-ului DHCP

Implicit = adresa IP a serverului DHCP + 1

Serverul DHCP atribuie adrese clienților conectați începând de la această adresă.

Sfârșitul pool-ului DHCP

Serverul DHCP atribuie adrese IP clienților conectați în intervalul definit de**Pornirea pool-ului DHCP** şi **Sfârșitul pool-ului DHCP**(inclusiv).

Wifi

Parametrii WiFi AP pot fi personalizați.

SSID automat

Caseta listă {On; Off}, implicit = „Activat”

Când este activată definirea automată a SSID, SSID-ul conține numărul de serie al unității.

SSID

SSID WiFi AP. Când este introdus manual, trebuie să respecte convențiile de denumire SSID.

Modul

Caseta listă {802.11g; 802.11g }, implicit = „802.11g”

Mod WiFi AP.

Canal

Canalul WiFi selectat.

Securitate

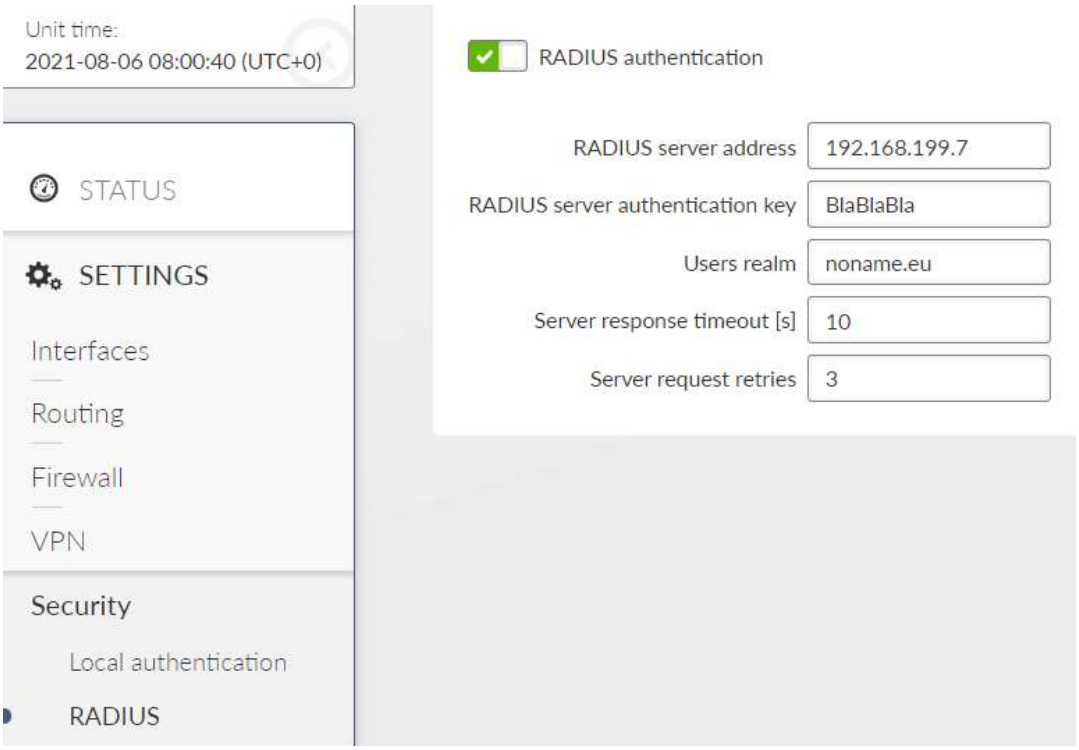
Caseta listă {Off; WPA2-PSK}, implicit = „Dezactivat”

Este o practică bună să utilizați conexiunea securizată WPA2-PSK împreună cu o parolă puternică. Este foarte recomandat în cazul instalării permanente a adaptorului WiFi.

7.5.5. RAZĂ

Conturile de utilizator pot fi gestionate central cu un server de autentificare. Protocolul RADIUS client-server este utilizat pentru autentificarea de la distanță. Conturile RADIUS pot fi mapate la unul dintre cele patru roluri de utilizator. Acesta este gestionat fie de serverul însuși, fie de setările locale M!DGE3.

Conturile locale sunt verificate mai întâi și dacă contul nu există, vor fi folosite conturile RADIUS. Dacă serverul RADIUS nu este accesibil, utilizatorii pot folosi numele de utilizator/parola local pentru a „reveni” la autentificarea locală.



Meniul SETĂRI > Securitate > RAZĂ permite setarea tuturor parametrilor principali.

Adresa serverului RADIUS

Adresa IP a serverului RADIUS utilizat pentru autentificare.

Cheia de autentificare a serverului RADIUS

Text {0 – 32 de caractere}

Parola pentru autentificare pe serverul RADIUS.

Domeniul utilizatorului

Textul {trebuie să conțină cel puțin un punct „.”}

Realm permite scurtarea numelui de conectare - de exemplu, atunci când numele complet de conectare este „ tech@noname.eu ” și domeniul este „noname.eu”, numele de utilizator completat în pagina de conectare este doar „tech”.

Timp de răspuns al serverului [s]

Numărul {1 – 30}, implicit = 10

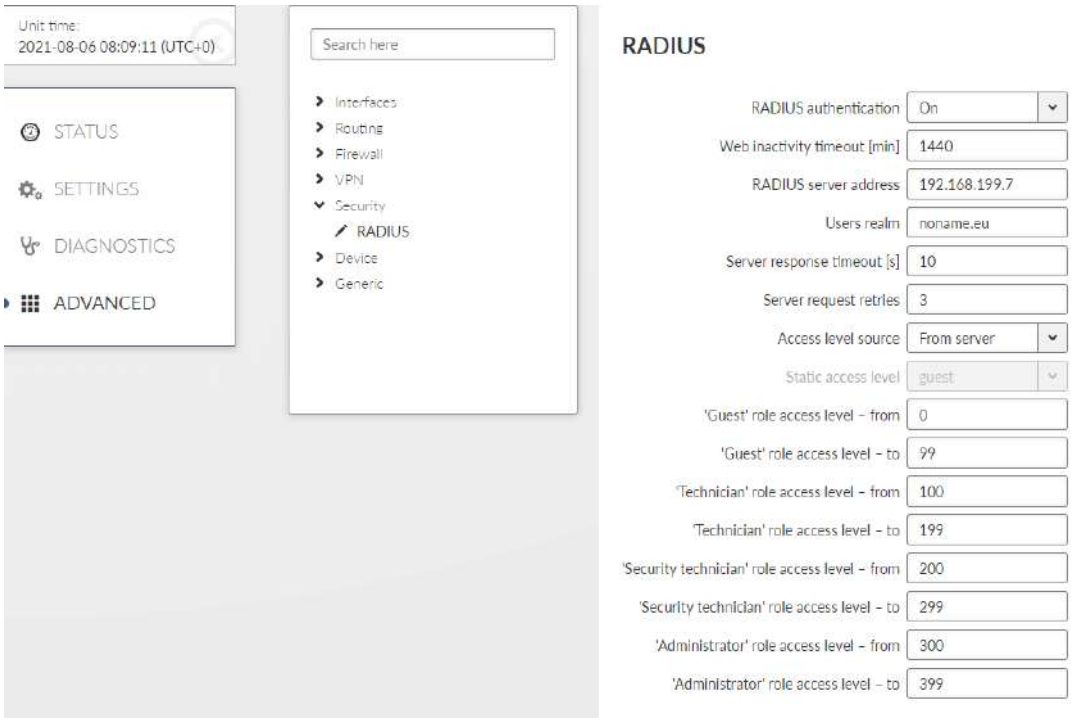
Timp măsurat în așteptarea răspunsului serverului înainte de a trimite o nouă încercare de solicitare.

Reîncercări de solicitare de server

Numărul {1 – 7}, implicit = 3

Numărul de încercări de solicitare în cazul M!DGE3 nu a primit un răspuns valid.

Parametrii experți suplimentari vor fi setați în meniul AVANZAT.



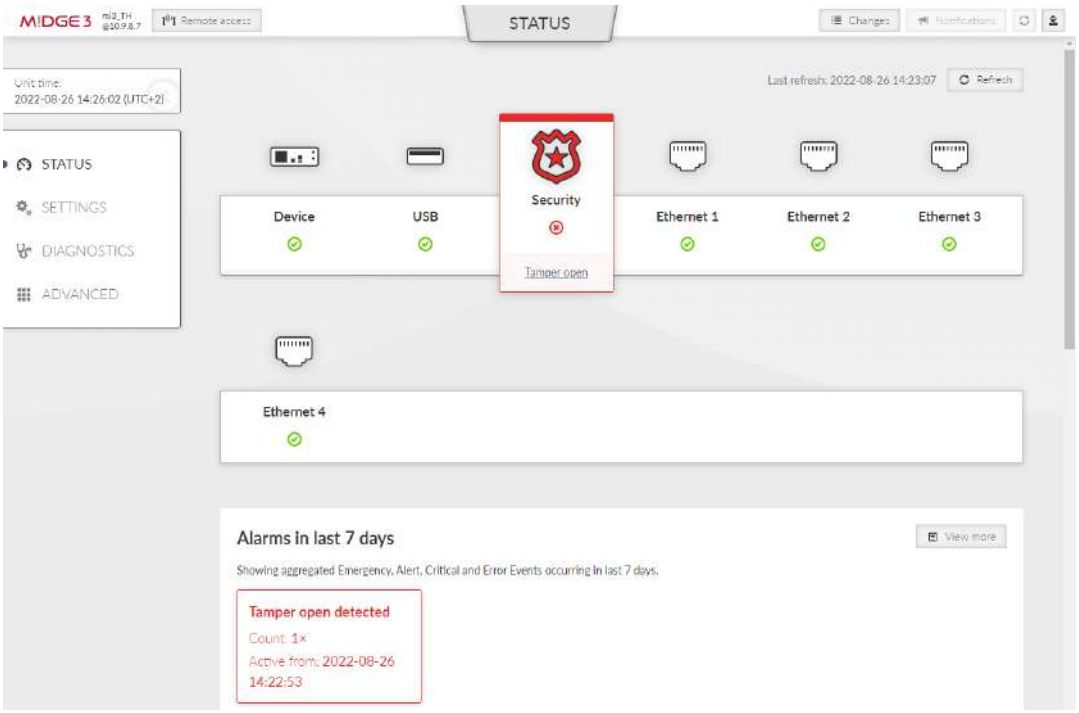
Nivelul de acces este realizat prin Management-Privilegiu-Level (RFC 5607, index 136, tip integer). Nivelul pentru fiecare cont va fi setat în timpul configurării serverului. Nivelul de acces utilizator va fi acordat în funcție de intervalele întregi pentru nivelurile individuale de rol. Când serverul nu permite setarea Management-Privilegie-Level, trebuie utilizată opțiunea de nivel de cont static (pentru toți utilizatorii).

7.5.6. Resetare tamper

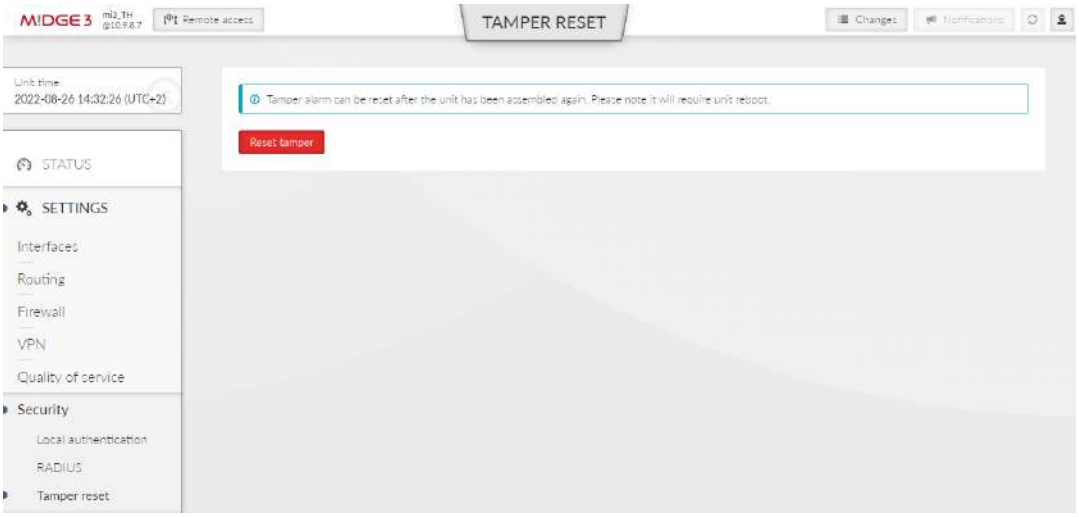
Tamper este un serviciu de detectare, care se declanșează atunci când șasiul M!DGE3 este deschis fizic. Există 2 contacte (securează carcasa superioară și inferioară) și evenimentul este declanșat chiar dacă unitatea este fără alimentare. Când șasiul este deschis, se declanșează o alarmă și este afișată în Raportul de stare. Triggered Tamper oprește RTC (ceasul în timp real), ceea ce înseamnă că fiecare repornire a unității resetează temporizatorul unității înapoi la momentul în care a fost declanșat Tamperul.

Nota

M!DGE3e nu are funcționalitatea de detectare a intervenției.

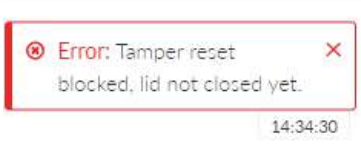


Pentru a rezolva alarma de manipulare, reasamblați unitatea, prin contul de utilizator de administrator, consultați SETĂRI/Securitate/Resetare manipulare din meniu și faceți clic pe butonul „Resetați manipularea”.



Nota

Unitatea trebuie reasamblată înainte de a face clic pe butonul „Resetare tamper”, altfel returnează o eroare.



Întregul proces poate dura ceva timp și se termină prin repornirea unității.

Dacă nu este setată o sincronizare automată a orei, ora din RTC trebuie setată manual.

7.6. Dispozitiv

7.6.1. Unitate

7.6.1.1. General

Setările generale care afectează întreaga unitate.

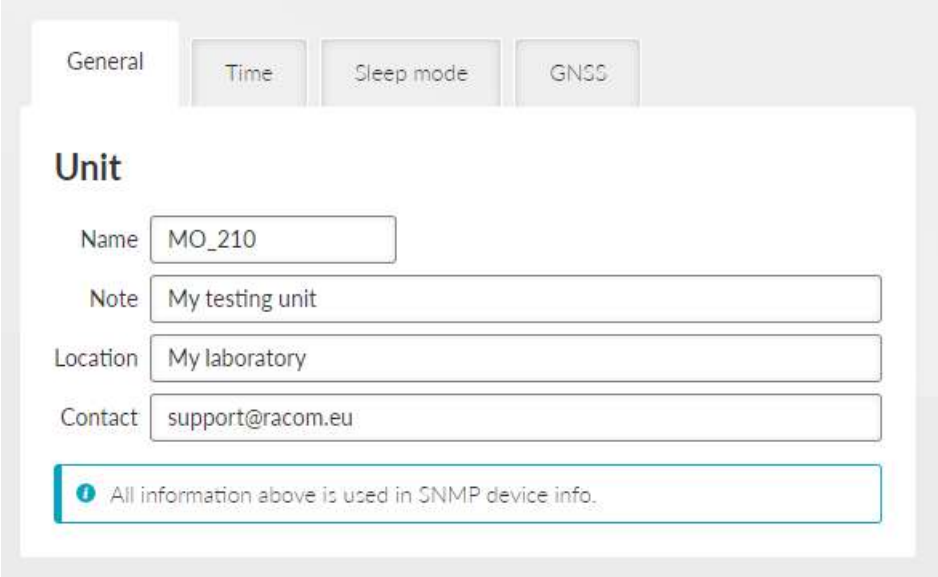


Fig. 7.27: SETĂRI > Dispozitiv > Unitate

Numele unității

Acest nume este folosit ca nume real al routerului Linux, astfel încât caracterele permise sunt strict limitate la:

Text; implicit = _a..zA..Z0..9

Nota de unitate

Text; implicit = _a..zA..Z0..9

Nume mai lung al unității, fără restricții de caractere speciale.

Locația unității, contactul unității

Text; implicit = _a..zA..Z0..9

Informații suplimentare SNMP. Toate câmpurile de mai sus sunt utilizate de obicei în sistemele NMS pentru a identifica unitatea specifică.

7.6.1.2. Timp

Marcajele de timp ale evenimentului unității, înregistrările statistice ale unității și jurnalele interne ale unității folosesc Timpul unității. Este o practică bună să păstrați ora unității sincronizată pentru a ușura diagnosticarea unității și a rețelei.

Unitatea de timp poate fi configurată manual sau poate fi sincronizată cu un server NTP. Se recomandă sincronizarea serverului NTP.

Unitatea în sine servește ca server NTP, oferind sincronizarea timpului către alți clienți IP. Dacă nu este definit niciun server NTP sau nu este nimeni disponibil, unitatea rulează într-un mod „orfan”. Serverul NTP intern al unității Stratum este setat la 8 în acest caz. Dacă unitatea este sincronizată cu un server NTP, serverul NTP al unității Stratum este setat cu 1 mai mare în comparație cu Stratum al serverului NTP care oferă sincronizarea timpului unității.

Dacă unitatea este sincronizată cu o sursă de timp și ora unității (sincronizate) diferă de ora RTC unității (cu mai mult de 8 secunde), ora RTC este actualizată.

Nota

Fiecare unitate poate servi ca server NTP pentru alte echipamente IP, această funcționalitate este întotdeauna activată.

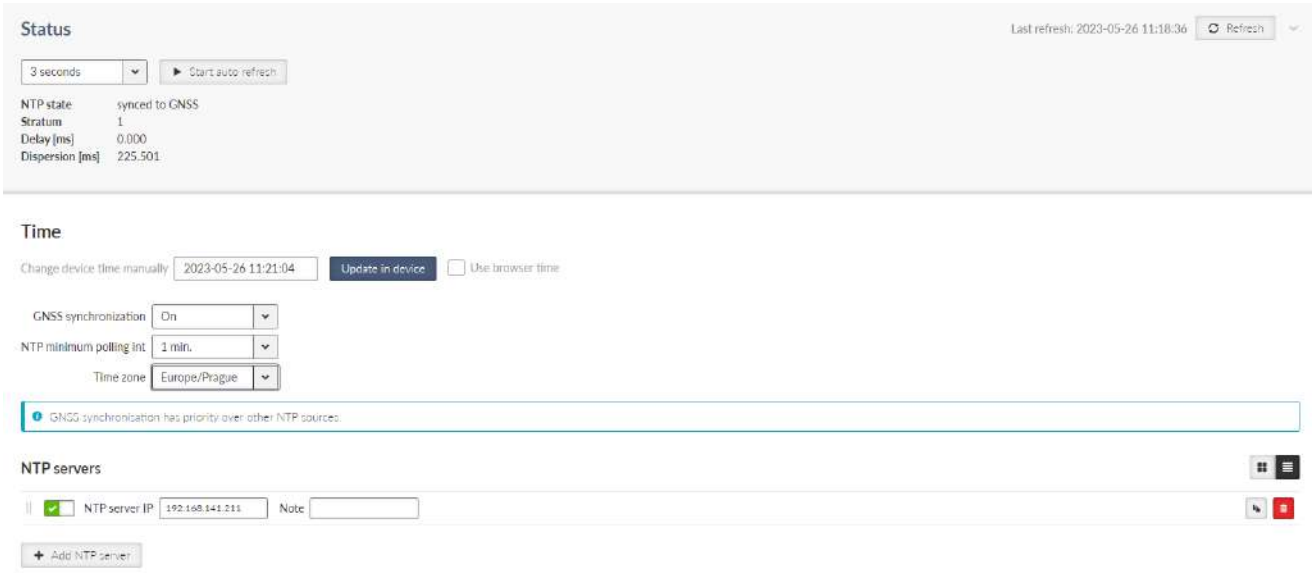


Fig. 7.28: SETĂRI > Dispozitiv > Unitate > Ora

Stare
: Câmpul Stare oferă informații despre starea sincronizării NTP. Butonul de reîmprospătare este utilizat pentru a actualiza informațiile de stare.

7.6.1.2.1. Timp

Schimbați manual ora dispozitivului
: Acest câmp este folosit pentru a seta manual ora unității.

Actualizare în dispozitiv
: Setează ora dată unității.

Caseta de selectare Utilizați ora browserului

Actualizează continuu câmpul Schimbați manual ora dispozitivului pentru a minimiza întârzierea dintre introducerea orei și momentul configurării orei.

Sursă de sincronizare client NTP

Sursa de sincronizare a clientului NTP. Singura opțiune „Server NTP” este implementată la această versiune de firmware.

Sincronizare GNSS

Caseta listă {On; Off }, implicit = „Dezactivat”

Activează/dezactivează sincronizarea cu GNSS (GPS) (când se utilizează modulul GNSS opțional). Sincronizarea GNSS (GPS) are prioritate față de alte surse NTP. Acest parametru apare numai dacă GNSS (GPS) este activat*Secțiunea 7.6.1.4, „GNSS (GPS)”*.

Durata minimă de interogare a serverului NTP

Perioada minimă a interogărilor serverului NTP. Clientului NTP i se permite să prelungească acest timp în caz de calitate proastă a serverului sau a conexiunii la server.

Fus orar

Fus orar pentru a reprezenta unitatea de timp intern. Toate marcajele de timp ale unității sunt afișate folosind acest fus orar. Modificarea fusului orar nu afectează înregistrările interne ale unității – acestea sunt întotdeauna înregistrate folosind fusul orar UTC.

Informațiile de stare NTP se bazează pe ieșirea standard de stare a demonului ntpq (ntpq -c lpeers, ntpq -c rv) - vezi*https://docs.ntpsec.org/latest/ntpq.html*(variabile de sistem, peer și ceas) pentru detalii.

7.6.1.2.2. servere NTP

Mai multe servere NTP pot fi configurate pentru a obține o sincronizare a timpului mai precisă sau pentru a avea o soluție de rezervă în cazul indisponibilității unui server NTP individual. Numărul maxim de înregistrări din listă este 32. Unitatea rulează într-un mod „orfan” dacă**Sursă de sincronizare client NTP**este setat la „Server NTP” și nu există niciun server NTP definit în această listă.

Activați / Dezactivați	Activează/dezactivează un server NTP.
IP server NTP	Definește adresa IP a serverului NTP.
Nota	Comentariu informativ.

7.6.1.3. Modul de repaus

M!DGE3 oferă un mod care comută periodic între modul de trafic complet și modul de consum redus de energie. Acest mod este potrivit, de exemplu, pentru aplicații sensibile la consumul de energie. În modul Sleep, M!DGE3 are un consum de energie extrem de scăzut (10 mW). Timpul necesar pentru o trezire completă din modul Sleep (timp de pornire) este de aprox. 30 de secunde sau mai mult - în funcție de configurație. Unitatea de dormit indică starea sa prin LED-ul SYS verde intermitent.

Fig. 7.29: SETĂRI > Dispozitiv > Unitate > Modul Sleep

Modul de repaus

Activare / dezactivare, implicit = dezactivare

Activează/dezactivează modul Sleep. Când este activată, unitatea va intra periodic în modul Sleep, în funcție de condițiile definite de următoarea configurație.

7.6.1.3.1. Parametrii de trezire

Trezirea M!DGE3 din modul Sleep este posibilă prin setarea orei de trezire a acestuia. De asemenea, este posibil să setați un interval în care unitatea va fi trezită în mod regulat. Limitele de timp ale modului de repaus sunt numărate într-un set**Fus orar**(SETĂRI > Dispozitiv > Unitate > Ora).

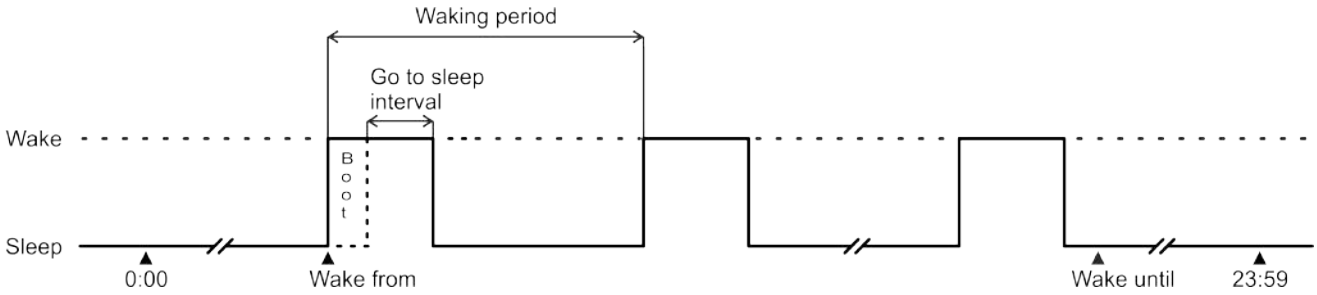


Fig. 7.30: Schema modului Sleep

Treziți-vă de la [h]

Numărul {0 – 23}, implicit = 0

Definește prima oră de trezire dintr-o zi - oră.

Treziți de la [min]

Numărul {0 – 59}, implicit = 0

Definește prima oră de trezire dintr-o zi - minut.

Perioada de veghe [min]

Număr {0 – 1439}, implicit = 60

Definește perioada de timp (min) dintre trezirile individuale.

Treziți-vă până la [h]

Număr {0 – 24}, implicit = 23

Definește timpul dintr-o zi după care unitatea nu va fi trezită - oră.

Treziți până la [min]

Număr {0 – 59}, implicit = 59

Definește timpul dintr-o zi după care unitatea nu va fi trezită - minut.

Nota

Setați timpul din parametri**Treziți-vă de la [h]**și**Treziți de la [min]**trebuie să fie mai mic sau egal cu timpul setat din parametri**Treziți până la [h]**și**Treziți până la [min]**.

7.6.1.3.2. Accesați parametrii de somn

M!DGE3 va intra în modul Sleep după trecerea timpului setat. Este posibil să amânați modul Sleep pentru a vă asigura că transferul de date este complet. Conectarea adaptoarelor USB-ETH sau USB-WIFI la portul de serviciu va întârzia și modul Sleep. Intrarea în modul Sleep va genera un eveniment în jurnalul de evenimente.

Nota

Dacă M!DGE3 este în modul Sleep și are loc o întrerupere a curentului (pentru aproximativ 10 secunde), modul Sleep va fi întrerupt și unitatea se va trezi (pornire).

Treci la interval de somn [min]

Numărul {5 – 1439}, implicit = 15

Definește durata de timp (min) după care unitatea va intra în modul Sleep. Numărătoarea inversă începe când unitatea este complet trează.

Intervalul de resetare

Caseta listă {On; Off }, implicit = „Dezactivat”

Permite setarea condițiilor care determină unitatea să întârzie tranziția în modul Sleep prin resetarea cronometrului înapoi la valoarea inițială**Treci la interval de somn [min]**.

Resetare la radio/activitate MAIN

Caseta listă {On; Dezactivat }, implicit = „Activat”

Dacă unitatea arată activitate pe interfața Cellular-MAIN, cronometrul de numărătoare inversă este resetat la valoarea inițială**Treci la interval de somn [min]**.

Nota

Ping-ul ICMP pe interfața Cellular-MAIN nu va declanșa**Resetare la radio/activitate MAIN**.

Resetare la activitatea EXT

Caseta listă {On; Dezactivat }, implicit = „Activat”

Dacă unitatea arată activitate pe interfața Cellular-EXT, cronometrul de numărătoare inversă este resetat la valoarea inițială**Treci la interval de somn [min]**.

Nota

Ping-ul ICMP pe interfața Cellular-EXT nu va declanșa**Resetare la activitatea Radio/EXT**.

Exemplul 1:

Cu următoarele setări, M!DGE3 va fi trezit periodic la fiecare oră timp de 10 minute (toată ziua):

Treziți-vă de la [h]=0 **Treziți de la [min]**=0 **Perioada de veghe [min]**=60 **Treziți până la [h]**=23

Treziți până la [min]=59
Treci la interval de somn [min]=10
Intervalul de resetare=Off

Exemplul 2:

Cu următoarele setări, M!DGE3 va fi trezit periodic de la 7:00 la 16:00 la fiecare 30 de minute timp de 10 minute:
Treziți-vă de la [h]=7 **Treziți de la [min]**=0 **Perioada de veghe [min]**=30 **Treziți până la [h]**=16 **Treziți până la [min]** =00
Treci la interval de somn [min]=10
Intervalul de resetare=Pe
Resetare la radio/activitate MAIN=Activat - acest parametru se va asigura că M!DGE3 rămâne treaz în cazul oricărei activități celulare la ora de somn programată.

7.6.1.3.3. Treziți-vă la intrarea în somn (SI)

Sleep Input (SI) este un semnal de declanșare care poate fi folosit pentru a trezi o stație din somn.

SI este declanșat/activat dacă este tras sub 1,1 VDC. Vedeți mai multe detalii în*Atribuirea PIN*

Dacă M!DGE3 este în modul Sleep și SI este declanșat, unitatea se va trezi pentru perioada de trezire setată și va reveni la somn. Semnalul de intrare Sleep nu este monitorizat în timp ce M!DGE3 este treaz, astfel încât orice declanșare suplimentară SI nu crește perioada de trezire.

Exemplu:

Unitatea este setat să se trezească la fiecare oră timp de 10 minute.
Dacă o unitate ar primi o comandă SI la 10:15, se va trezi și va fi treaz până la 10:25. Dacă nu se primește o altă comandă SI după ora 10:25, unitatea va rămâne adormită până la ora 11:00.

7.6.1.4. GNSS (GPS)

GNSS (sistemul global de navigație prin satelit) permite modulului de extensie opțional să ofere informații despre locația unităților și să permită o sincronizare precisă a timpului.

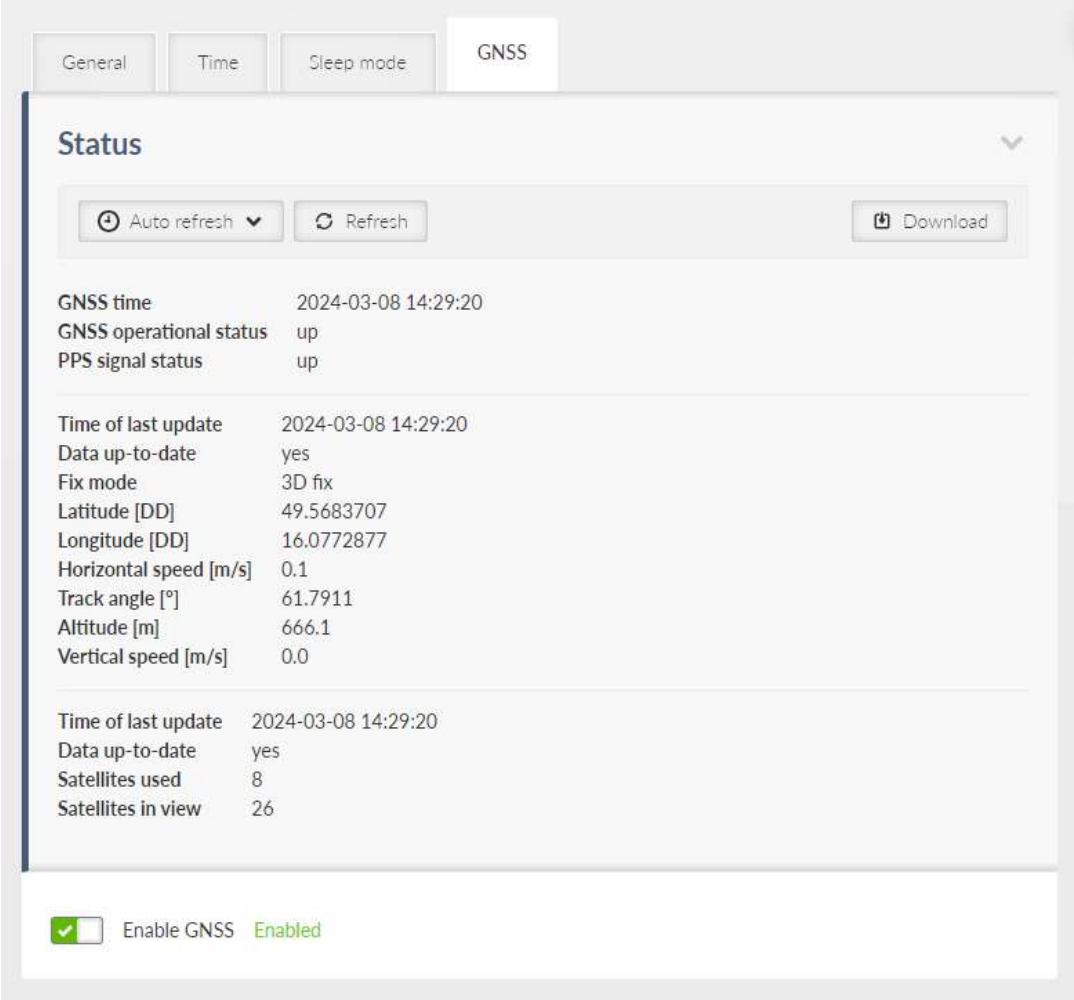


Fig. 7.31: SETĂRI > Dispozitiv > Unitate

Permite; Dezactivare, implicit = „Dezactivare”
Activează/dezactivează GNSS (GPS).

Pentru a configura GNSS (GPS), vezi *Secțiunea 7.7.6, „Server GNSS”*.

Tab. 7.3: Comportamentul LED-ului GNSS (GPS)

LED	Culoare	Stare	Funcţie
EXT	Verde	Clipește regulat - perioadă 1000 ms	GNSS (GPS) este activ, așteaptă date despre locație și semnal PPS.
EXT	Verde	Aprins permanent	GNSS (GPS) este activ, sunt disponibile date despre locație și semnal PSS.

7.6.1.4.1. Cooperare cu alte servicii

• HotStandby - GNNS (GPS) este deconectat în modul pasiv și activat în mod activ.

• Evenimente - TBD

• SNMP - TBD

7.6.2. Configurare

Configurația în M!DGE3 funcționează pe următorul sistem:

• Configurație curentă - configurație afișată, care este văzută în clientul web.

• Configurație de rulare - configurație reală, care rulează în unitatea M!DGE3.

• Configurație stocată - configurație stocată în unitatea M!DGE3. Această configurație este stocată în unitate, chiar și atunci când este oprită.

• Setări din fabrică - configurație implicită.

• Modificări - toate modificările efectuate în configurația curentă (în clientul web). Pentru mai multe informații vezi *Secțiunea 6.2, „Modificări de angajare”*.

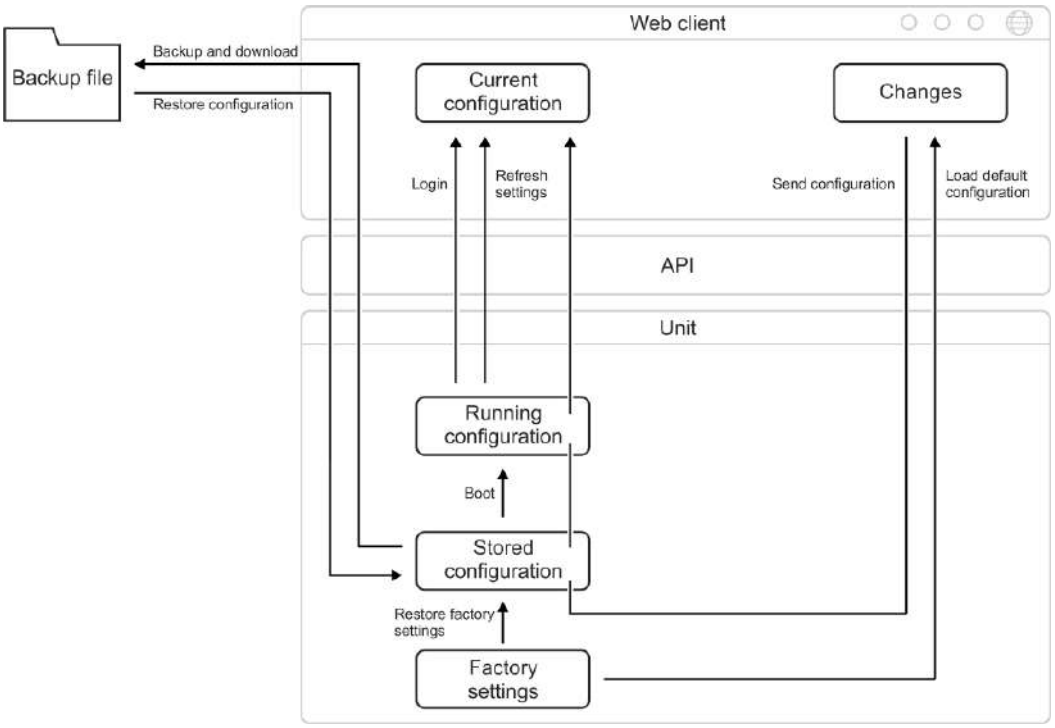
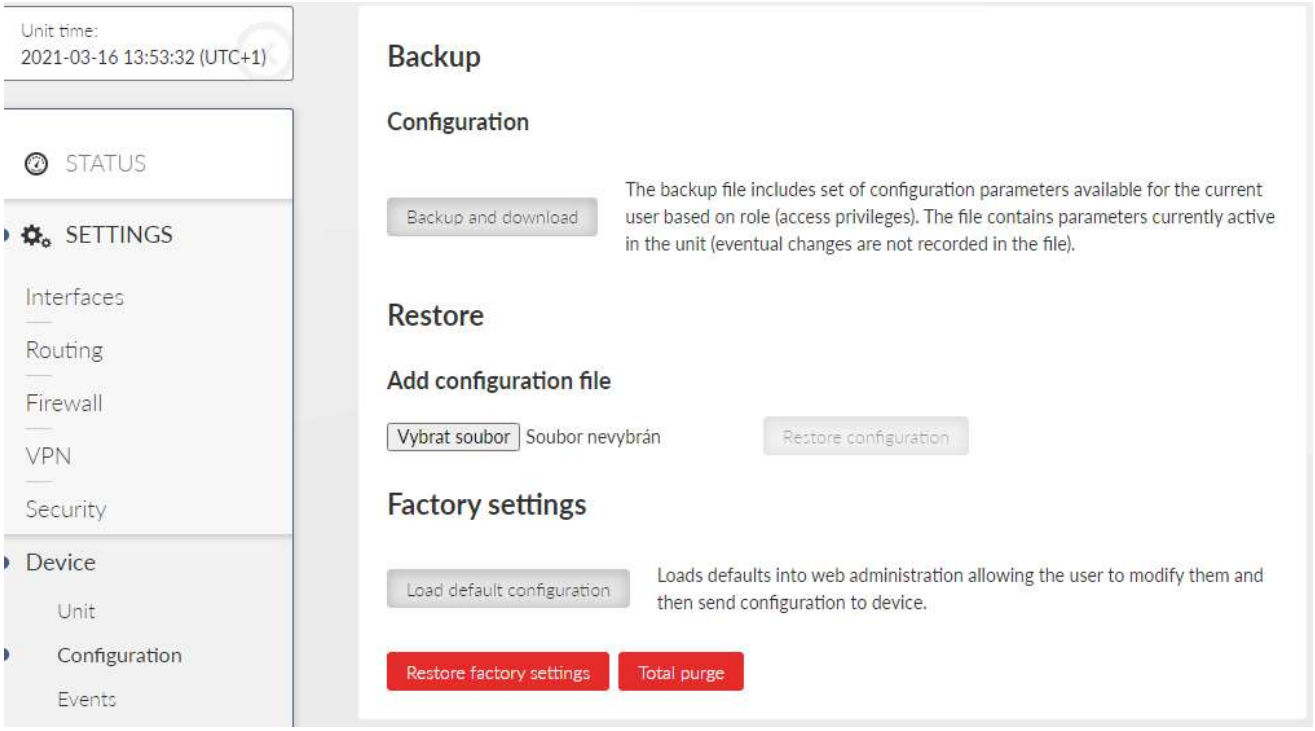


Fig. 7.32: Schema de configurare M!DGE3

Există mai multe instrumente pentru a opera configurația completă a unității:



Backup

Este o bună practică să faceți o copie de rezervă a configurației într-un fișier extern de fiecare dată când configurația este schimbată, pentru a putea restabili configurația într-o altă unitate în cazul întreținerii unității. **Backup și descărcare**butonul declanșează acțiunea de descărcare a browserului web. Comportamentul specific depinde de setările personale ale browserului dvs. web - dacă fișierul de backup de configurare este descărcat într-un folder de descărcare predefinit sau este afișat dialogul Descărcare fișier pentru a selecta folderul de destinație. Configurația este stocată într-un fișier text (tip de fișier .json).

Configurația de rezervă are următoarele limitări:

• Setul de date de configurare este limitat de privilegiile de acces ale utilizatorului care a efectuat backup-ul. Backup-ul complet al configurației poate fi eliberat numai de un utilizator cu privilegii de acces Administrator (role_admin). Aceeași limită de acces de utilizator se aplică atunci când configurația este restaurată (adică restaurarea completă a configurației poate fi emisă numai de un utilizator cu privilegii de acces Administrator (role_admin)).

Versiunea de configurare este stocată în parametrul numit „Versiune CNF” care poate fi verificat în meniul: DIAGNOSTICĂ > Informații > Dispozitiv > Informații avansate.

Restabili

Configurația poate fi restabilită dintr-un fișier de rezervă (care conține aceeași versiune de configurare ca versiunea de configurare care rulează în prezent în unitate - vezi mai sus).

Alegeți butonul File

Declanșează dialogul de selecție a fișierelor. Odată ce fișierul de rezervă de configurare este selectat, acesta este încărcat în unitate. Acțiunea de încărcare poate dura ceva timp - depinde de viteza conexiunii de serviciu la unitate.

Setări din fabrică

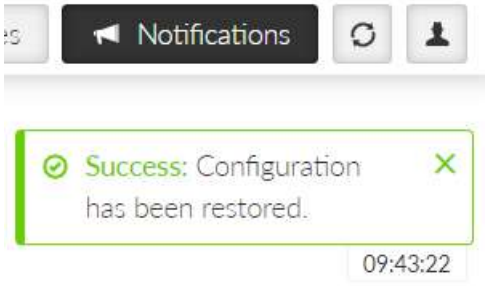
Încărcați configurația implicităbutonul încarcă valorile implicite ale tuturor parametrilor de configurare în interfața web. Toți parametrii a căror valoare curentă diferă de cea implicită sunt marcați ca modificați. Acestea sunt listate în caseta de dialog Modificări pentru comite. Acestea nu afectează unitatea care rulează până când sunt trimise în cele din urmă către unitate prin butonul de configurare Trimitere.

Nota

Această acțiune poate fi utilizată (de exemplu) pentru a verifica ce set de parametri diferă de valoarea implicită.

Butonul de restabilire a configurației

Activat după încărcarea configurației de rezervă. Apăsați butonul pentru a restabili configurația unității. Rezultatul restabilirii configurației este raportat ca mesaj de eroare (în caz de eșec) sau mesaj de succes al centrului de notificare:



Restabiliți setările din fabrică

Restabilește toți parametrii de configurare la configurația implicită (inclusiv setările de monitorizare). Se va aplica deconectarea de la stație.
Șterge baza de date a utilizatorilor (va rămâne doar utilizatorul implicit „admin” cu parola implicită).

Purjare totală

Restabilește toți parametrii de configurare la configurația implicită (inclusiv setările de monitorizare). Se va aplica deconectarea de la stație.
Șterge baza de date a utilizatorilor (va rămâne doar utilizatorul implicit „admin” cu parola implicită). Șterge toate jurnalele de diagnosticare și statisticile.

Nota

Datele de bază, cum ar fi cod, regiune, cheile SW vor rămâne întotdeauna în unitate.

Avertizare

Această acțiune poate dura până la două minute - nu opriți unitatea până când nu ați terminat.

Validarea configurației

FW din versiunea 2.2.0.0 introduce un proces îmbunătățit de validare a configurației. În versiunile FW mai vechi, unele validări ale elementelor de configurare (de exemplu, intervalul de valori permis, lungimea șirului) au fost validate numai în aplicația web (front-end). La modificarea configurației în alte moduri (apeluri API, editare directă a fișierului de configurare de rezervă), a fost posibilă introducerea unei valori într-un element de configurare care a cauzat ca configurația unității rezultată să fie invalidă. Recent, validarea completă a configurației este efectuată direct în unitate (back-end). Nicio metodă de modificare a configurației (interfață web, API, modificări de copiere a textului) nu poate determina unitatea să utilizeze o configurație nevalidă.

Notă pentru actualizarea FW de la versiunile mai vechi la versiunea 2.2.0.0 și o versiune ulterioară:
Este posibil ca unitățile cu FW mai vechi de 2.2.0.0 să fi funcționat cu o configurație care nu este complet validă. La actualizarea unității la FW 2.2.0.0 sau o versiune ulterioară, se va efectua o verificare a validității configurației în timpul pornirii unității. Dacă configurația nu reușește această verificare, utilizatorul va fi informat prin generarea evenimentului de sistem „EVENT_CNF_BOOT_ERROR”. Centrul de notificare va furniza mesaje de alarmă detaliate care fac referire la elemente individuale de configurare nevalide. Cu toate acestea, unitatea va continua să funcționeze cu această configurație așa cum a făcut înainte de upgrade-ul FW. Funcțiile unității nu sunt afectate de această situație.

Consecințele rulării unității cu o configurație nevalidă:

Evenimentul de sistem „EVENT_CNF_BOOT_ERROR” este activ. Evenimentul are o severitate implicită de alarmă, ceea ce face ca LED-ul de stare SYS să se aprindă roșu.

Până când toate elementele care au eșuat procesul de validare nu sunt corectate, nu pot fi salvate modificări de configurare. Configurația actualizată poate fi activată numai odată ce întreaga configurație a trecut cu succes validarea.

Tab. 7.4: Versiuni de configurare

Versiunea CNF	Versiunea FW
24	2.2.1.0
24	2.2.0.0
23	2.1.7.0
22	2.1.6.0
21	2.1.2.0
20	2.1.1.0
19	2.1.0.0
18	2.0.18.0
17	2.0.16.0
16	2.0.14.0
15	2.0.13.0

7.6.3. Evenimente

Setări ale severității evenimentelor individuale. Unele evenimente pot genera notificare SNMP și pot schimba nivelul ieșirilor de alarmă HW (AO, DO1, DO2) vezi *Secțiunea 2.2.2, „Putere și control”*. Evenimentele pot genera, de asemenea, notificări prin SMS, care sunt trimise la un număr de telefon definit (vezi *Secțiunea 7.7.5, „SMS”*).

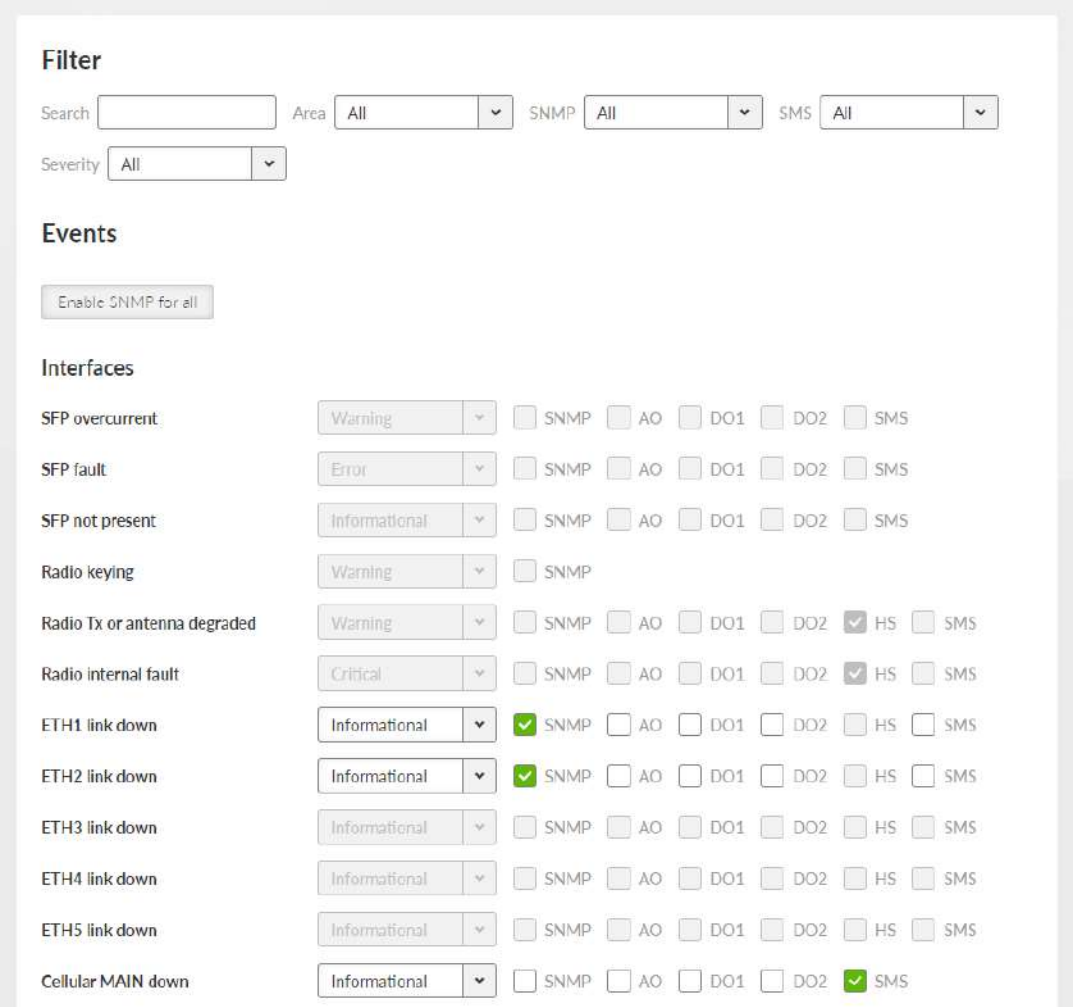


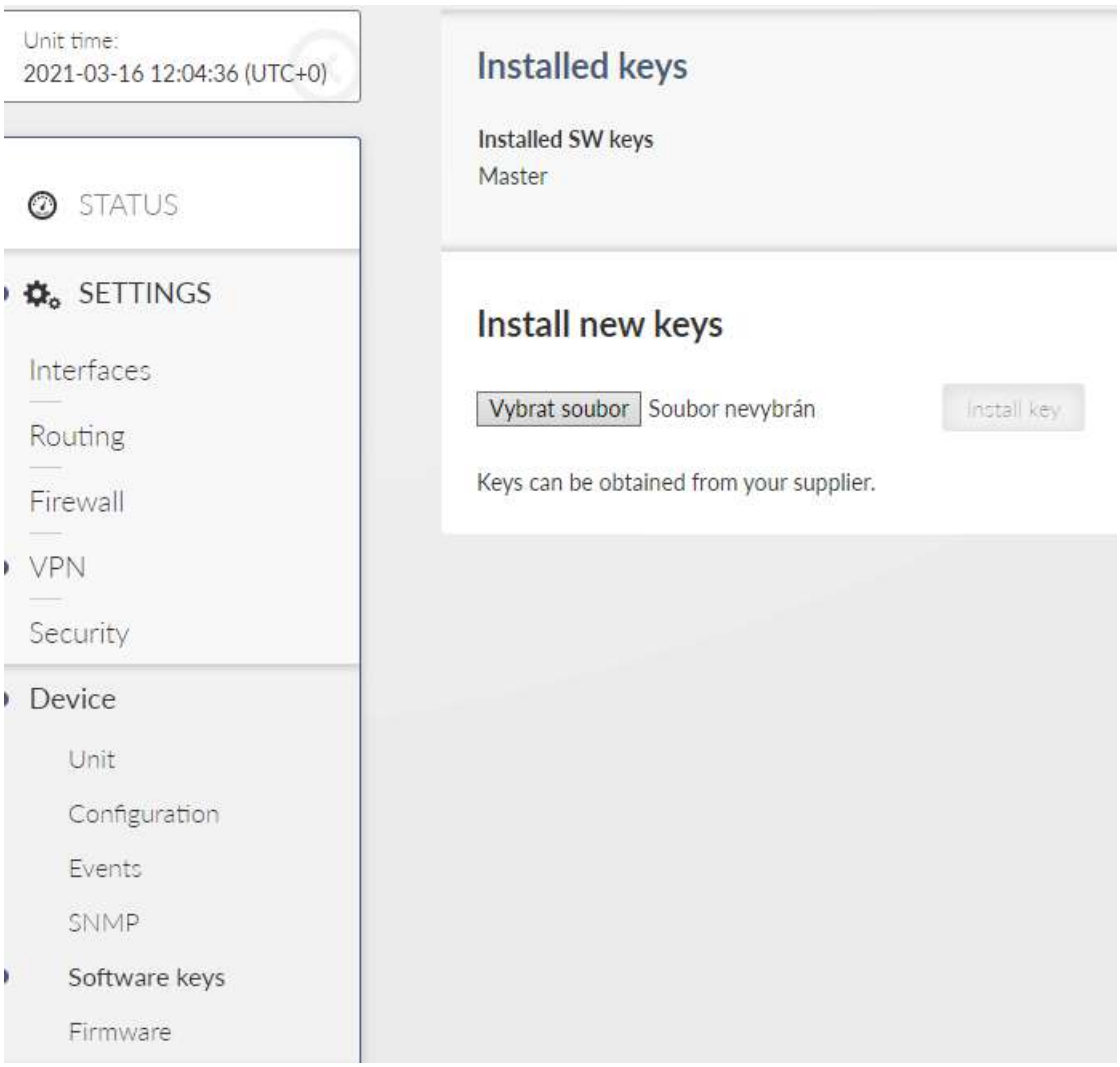
Fig. 7.33: SETĂRI > Dispozitiv > Evenimente

7.6.4. Tastele SW

Anumite funcții M!DGE3 trebuie activate de o cheie SW pentru a fi disponibile. Când tasta SW respectivă nu este prezentă, caracteristica nu poate fi configurată. Dacă funcția este activată într-un fișier de rezervă de configurare și fișierul este încărcat într-o unitate care nu este echipată cu cheia respectivă, configurația este refuzată (nu se fac modificări în unitate).

Aici este lista cheilor SW disponibile și atribuirea acestora la pachetele de chei SW oferite.

Cheile SW pot fi obținute de la furnizorul dvs. Este livrat ca un fișier text care conține cheia (cheile). Fiecare cheie SW este unică pentru unitatea specifică (număr de serie specific). Utilizați dialogul Alegeți fișierul pentru a selecta fișierul și butonul Instalare cheie pentru a instala cheile pe unitate.



Diferențele față de generația anterioară de RipEX:

- Tastele SW sunt întotdeauna instalate ca fișier (nu există o opțiune pentru clipboard)

- Un singur fișier poate conține mai multe chei SW

- Tastele SW nu sunt limitate în timp

Tab. 7.5: Lista tastelor SW atomice

Cheie atomică	Comandă rapidă	Tasta SW	Fără Cheie
BGP**	BGP	Implicit	N / A
OSPF**	OSPF		N / A
Babel**	Babel		N / A
Gestionarea linkurilor**	LMgmt		N / A
PPPoE*,**	PPPoE		N / A
IPsec	IPsec	Implicit	N / A
OpenVPN	OpenVPN		N / A
Utilizatori multipli	Utilizatori		Un singur utilizator
RAZĂ	Rază		N / A
Detectare manipulare**	Tamp		N / A
SFP**	SFP	SFP	N / A

* Implicit din 03/2024, dacă ați achiziționat M!DGE3 înainte de această dată și doriți să utilizați această funcționalitate, va trebui să solicitați cheia atomică de la furnizor.

* * Nu este disponibil pentru M!DGE3e

Nota

Cheile atomice nou adăugate nu sunt incluse în livrarea cheii SW comandate anterior (Gestionarea linkurilor pentru unitățile expediate înainte de 07/2023, OpenVPN pentru unitățile expediate înainte de 10/2023). Data de expediere face parte din Raportul de inspecție a calității, care este disponibil pentru fiecare S/N individual prin serviciul web RACOM.

Cheile atomice instalate le puteți verifica folosind meniul SETĂRI > Dispozitiv > Taste SW.

Cheia principală înlocuiește toate cheile atomice (chiar și acestea adăugate recent și în viitor)

7.6.5. Firmware

7.6.5.1. Local

Firmware-ul unității definește funcționalitatea unității. Există mai multe principii pentru gestionarea firmware-ului în rețeaua care rulează:

• Mențineți aceeași versiune de firmware în rețea (recomandat). Unitățile RipEX sunt capabile să coopereze cu diferite versiuni de firmware care rulează, dar utilizarea aceleiași versiuni de firmware în toate unitățile este cea mai bună modalitate de a menține simplă întreținerea rețelei.

• Actualizarea firmware-ului la o versiune mai nouă nu este obligatorie, cu excepția cazului în care există remedieri de erori/securitate etc.

• Problemele de securitate cibernetică pot forța actualizarea firmware-ului, de exemplu atunci când a fost remediată o vulnerabilitate serioasă de securitate.

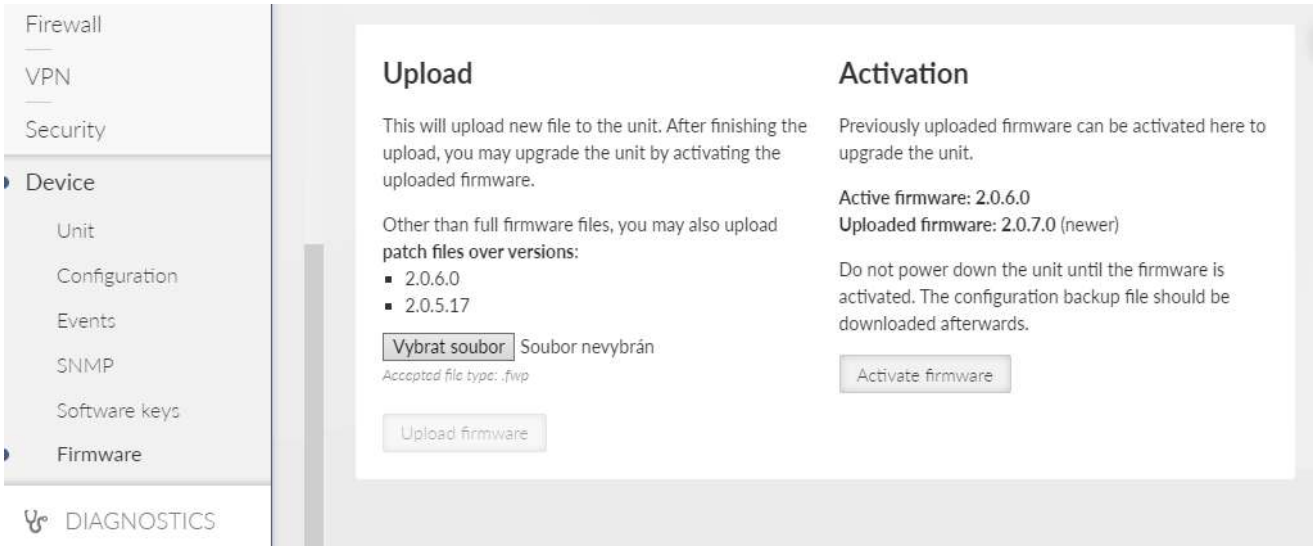
Există 3 etape ale procedurii de actualizare a firmware-ului:

• Alegerea unui firmware nou și încărcarea acestuia în browserul web.

• Încărcarea firmware-ului nou în arhiva internă a unității.

• Activarea firmware-ului unității.

Fiecare operație poate dura până la câteva zeci de secunde.



Nota

Este recomandată copierea de rezervă a configurației unității după actualizarea firmware-ului. Vedea *Secțiunea 7.6.2, „Configurare”* pentru detalii.

Pentru a actualiza firmware-ul:

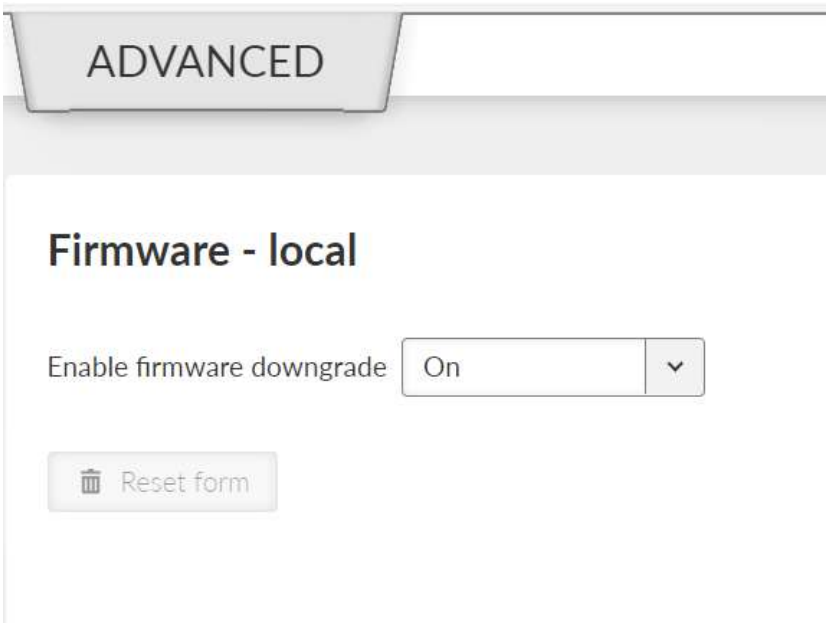
1. Opțional (recomandat): Efectuați o copie de rezervă a configurației curente a unității (meniul SETĂRI > Dispozitiv > Configurare – Backup și descărcare).

2. Descărcați firmware-ul necesar din *Racom web*[6]: Produse – M!DGE3 – Descărcare – Firmware M! DGE3 – midge3-fw-xxx0.fwp

3. Faceți clic pe **Alegeți Fișier** butonul (eticheta butonului poate diferi în funcție de localizarea browserului dvs. web) pentru a selecta fișierul firmware.

4. Faceți clic pe **Încărcați firmware** butonul pentru a transfera fișierul firmware în unitate. Încărcarea poate dura mult timp – în funcție de viteza conexiunii dintre PC-ul de management și unitatea M! DGE3. În cazul conexiunii lente și a transferului de fișiere mai mult de 120 s, browserul web va închide conexiunea și acțiunea nu se va finaliza cu succes. Această acțiune nu actualizează încă firmware-ul unității care rulează. Nu există nicio afecțiune asupra celorlalte comunicații care circulă prin această unitate. Încărcarea cu succes a noului firmware în arhivă este anunțată în Notificări, iar versiunea de firmware disponibilă este evidențiată sub titlul „Activare” ca „**Firmware încărcat:**".

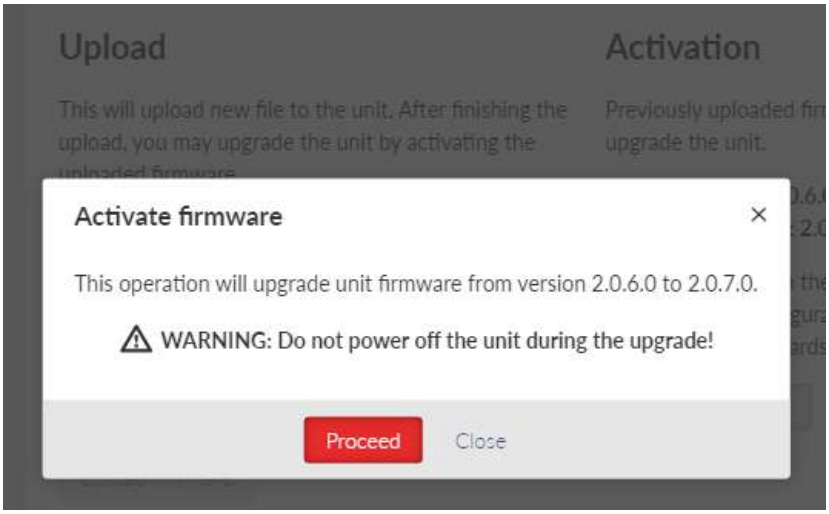
[6] https://www.racom.eu/eng/products/cellular-router-midge.html#dnl_fwr3



Nota

Contul la nivel de administrator are posibilitatea de a dezactiva downgrade-ul FW (meniul ADVANCED > Firmware > Firmware - local prin setarea**Activați downgrade-ul firmware-ului**la Off), în mod implicit, această funcționalitate este permisă.

5. Faceți clic pe**Activați firmware-ul**butonul pentru a actualiza (adică a reinstala) firmware-ul unității. Procesul de actualizare durează aprox. un minut. Comunicarea datelor utilizatorului care circulă prin această unitate este întreruptă pentru o perioadă. Toate procesele sunt repornite într-un anumit moment (de exemplu, tunelurile VPN trebuie restabilite).



Avertizare

Nu opriți unitatea în timpul procesului de actualizare a firmware-ului. Poate deteriora permanent unitatea.

6. Este posibil nu doar upgrade-ul versiunii de firmware, ci chiar downgrade-ul acesteia, deși această operațiune nu este recomandată. Fiți conștienți de eventualele probleme de securitate ale downgrade-ului firmware-ului ca

eventual codul de securitate învechit poate face parte dintr-un firmware vechi. După downgrade FW, toți parametrii unității vor fi setați la valorile implicite din fabrică.

Nota

Actualizarea directă a firmware-ului de la versiunea 2.0.3.0 (sau mai recentă) la versiunea 2.0.13.0 (sau mai mare) nu este posibilă. Trebuie să actualizați firmware-ul la orice versiune de la 2.0.5.0. la 2.0.10.0 înainte de actualizarea la 2.0.13.0 (sau mai mare).

Nota

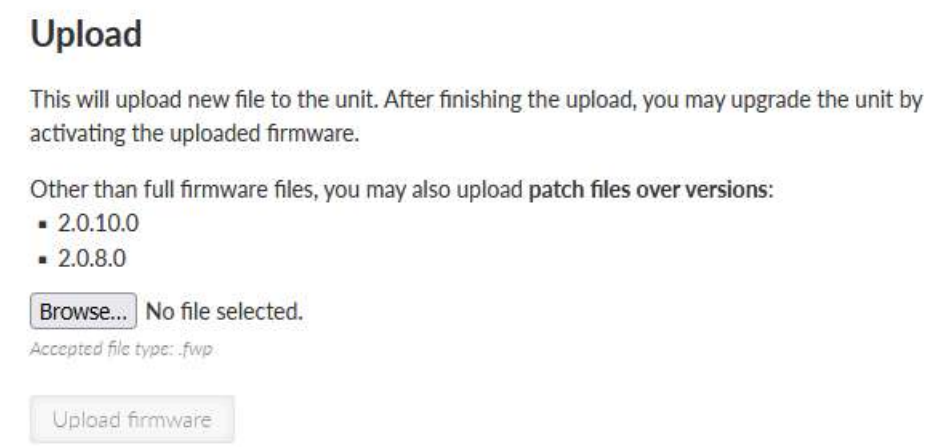
Actualizarea directă a firmware-ului la 2.1.1.0 sau mai nouă de la versiunea 2.0.18.0 sau mai veche este posibilă în unul din două moduri.

- Actualizați firmware-ul la versiunea 2.1.0.0 înainte de actualizarea la 2.1.1.0 sau mai nouă
- Utilizați un pachet special de upgrade care include abrevierea FWD în numele său. Vezi*Arhiva de firmware*[7] pentru opțiunile de descărcare.

7.6.5.1.1. Fișiere de corecție

În unele cazuri, în loc să încărcați și să activați versiunea completă FW, pot fi folosite fișiere de corecție. Avantajul fișierelor de corecție este că sunt mai mici în comparație cu fișierele cu versiunea completă. Pentru o activare cu succes, trebuie să se asigure compatibilitatea între fișierul de corecție și firmware-ul activ (sau firmware-ul încărcat). Fișierele de corecție pentru M!DGE3 pot fi descărcate de la*Site-ul web al RACOM*[8]. Versiunile FW stocate în M!DGE3 sunt afișate în SETĂRI > Dispozitiv > Firmware.

[7] https://www.racom.eu/eng/products/radio-modem-ripex.html#dnl_archive
[8] https://www.racom.eu/eng/products/cellular-router-midge.html#dnl_fwr3



Exemplu: Există 2 versiuni FW mai vechi (2.0.8.0 și 2.0.10.0) stocate în M!DGE3 (imaginea de mai sus).

Pentru activarea cu succes a versiunii FW mai noi (de ex. 2.0.13.0) folosind fișierul de corecție:

• Descărcați versiunea de actualizare a fișierelor de corecție de la 2.0.8.0 la 2.0.13.0 sau
• Descărcați versiunea de fișiere de corecție de la 2.0.10.0 la 2.0.13.0 (recomandat, deoarece acest fișier de corecție va fi mai mic).

Rezultatul va fi exact același în ambele cazuri.

Nota

Versiunile FW (atât fișierele de corecție, cât și versiunile complete) sunt stocate în*Arhiva M!DGE3*[9].

7.6.5.2. USB

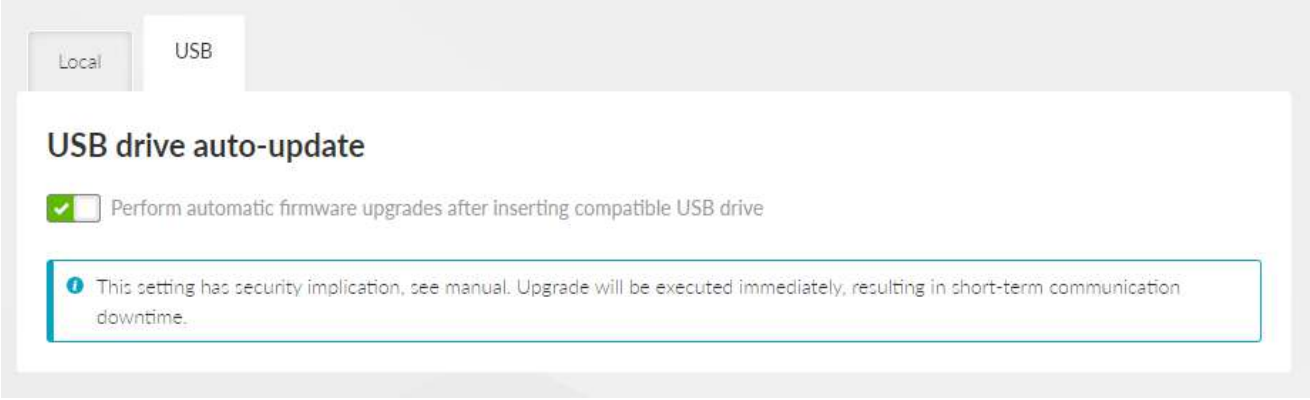


Fig. 7.34: SETĂRI > Dispozitiv > Firmware > USB

Comutator**Efectuați upgrade automate de firmware după ce ați introdus unitatea USB compatibilă**permițând actualizarea FW de pe un disc flash USB. Trecerea la o versiune superioară utilizând un disc USB nu este posibilă. Modificarea acestei setări este activată după un nou proces de pornire.

FW-ul unității în sine va fi actualizat (nu FW-ul unui eventual modul încorporat).

[9]https://www.racom.eu/eng/products/cellular-router-midge.html#dnl_archive

Când este permis, upgrade-ul FW (de pe discul flash USB) începe automat după introducerea discului flash USB în conectorul USB. Utilizatorul este informat despre proces prin intermediul semnalizării LED SYS (vezi capitolul 2.4.*LED-uri de indicare*).

Următoarele condiții se aplică procesării:

• Unitatea USB trebuie să conţină cel puţin o partiţie. Dacă există mai multe partiții, doar prima va fi conectată la dispozitiv.

• Prima partiție trebuie să fie primară (fizică) și trebuie să fie formatată cu sistemul de fișiere FAT12, FAT16 sau FAT32.

• Fișierele FW trebuie să fie localizate în directorul rădăcină. Subdirectoarele nu sunt căutate. Fișierele FW pot fi fie fișiere standard, fie legături soft.

• Numele fișierului FW trebuie să aibă extensia .fwp sau .cpio.enc. Nu contează dacă caracterele sunt litere mici sau majuscule (insensibile la majuscule).

• Nu există restricții privind numele fișierului FW, trebuie respectate doar regulile de extensie. Setul de caractere permis de sistemul de fișiere al unității USB date (dar recomandăm totuși utilizarea setului ASCII standard).

• Orice număr de fișiere FW (pachete FW) pot fi stocate pe unitatea USB (nu toate chiar trebuie să fie pentru un anumit dispozitiv). Dintre acestea, dispozitivul „alege” apoi FW-ul care se potrivește HW-ului dat și are cea mai înaltă versiune.

• Dacă pe disc se găsesc două sau mai multe FW-uri adecvate, care au aceeași versiune, primul este selectat în ordine în funcție de aranjamentul lexicografic (acest lucru se poate întâmpla, de exemplu, dacă un fișier este FW complet, în timp ce celălalt este FW-patch).

7.7. Servicii

7.7.1. Servere DHCP

Serverul DHCP ascultă pe interfețele selectate. Când un client de la o altă stație o solicită, acesta atribuie o adresă IP (închiriere DHCP) din intervalul specificat.

Interfața de rețea corespunzătoare trebuie să aibă un interval de rețea definit, care include intervalul alocat.

Serverul DHCP este apoi utilizat special pentru această interfață (ETH1 - ETH5, Wi-Fi).

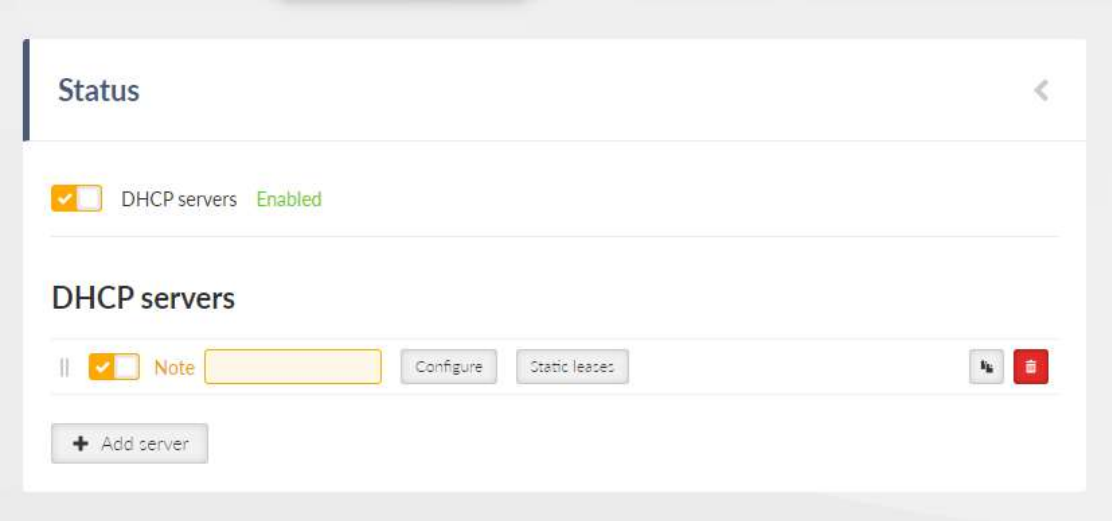


Fig. 7.35: SETĂRI > Servicii > Servere DHCP

7.7.1.1. Configurarea serverelor DHCP

Fig. 7.36: SETĂRI > Servicii > Servere DHCP > Configurare

Permite

{Permite; Dezactivare}, implicit = „Activare”
Activează serverul DHCP selectat în prezent.

Nota

Notă informativă.

Începe intervalul de adrese

Adresă IP, implicită = 0.0.0.0

Începutul intervalului de adrese IP alocate. Trebuie să fie cazul că**Începe intervalul de adrese**<= **Sfârșitul intervalului de adrese**.

Adresa trebuie să fie în domeniul de adrese al interfeței ETH, LAN, VLAN sau Wi-Fi.

Sfârșitul intervalului de adrese

Adresă IP, implicită = 0.0.0.0

Sfârșitul intervalului de adrese IP alocate. Trebuie să fie cazul că**Începe intervalul de adrese**<= **Sfârșitul intervalului de adrese**.

Adresa trebuie să fie în domeniul de adrese al interfeței ETH, LAN, VLAN sau Wi-Fi.

Nota

Intervalele de servere DHCP active nu trebuie să se suprapună.

Timp de închiriere [min]

Număr {2 – 10080}, implicit = 60

Adresa perioada de inchiriere. Se aplică atât adreselor dinamice, cât și statice.

Numai contracte de închiriere statice

Caseta listă {Off; Activat}, implicit = „Dezactivat”

Specifică dacă intervalul este utilizat numai pentru alocarea adreselor fixe (statice). Dacă este activat, trebuie să fie în tabelul Închirieri statice.

Anunțați gateway

Caseta listă {Off; Local; Manual}, implicit = "Local"

Configurați anunțarea routerului către clienți. Oprit:

Gateway-ul nu este anunțat.

Local: IP-ul routerului este anunțat ca gateway. Manual: Adresa

IP setată manual este anunțată ca gateway.

Adresa gateway-ului

Adresă IP, implicită = 0.0.0.0

Adresa IP a gateway-ului care se anunță.

Anunțați DNS

Caseta listă {Off; Local; Manual}, implicit = "Local"

Configurați anunțarea serverului DNS către clienți. Oprit:

serverul DNS nu este anunțat.

Local: IP-ul routerului este anunțat ca server DNS. Numai dacă**Redirecționare DNS**este activat.

Manual: Adresa IP setată manual este anunțată ca server DNS.

Server DNS primar

Adresă IP, implicită = 0.0.0.0

Se anunță adresa IP a serverului DNS principal.

Setați serverul DNS secundar

Caseta listă {Off; Activat}, implicit = „Dezactivat”

Stabilește dacă serverul DNS secundar este anunțat.

Server DNS secundar
Adresă IP, implicită = 0.0.0.0
Se anunță adresa IP a serverului DNS secundar.

Anunțați serverul NTP
Caseta listă {Off; Local; Manual}, implicit = "Oprit" Configurați anunțarea serverului NTP către clienți. Oprit: Serverul NTP nu este anunțat.
Local: IP-ul routerului este anunțat ca server NTP. Manual: Adresa IP setată manual este anunțată ca server NTP.

server NTP
Adresă IP, implicită = 0.0.0.0
Se anunță adresa IP a serverului NTP.

7.7.1.2. Leasing statice

Fig. 7.37: SETĂRI > Servicii > Servere DHCP > Închirieri statice

Fiecare linie definește o atribuire statică a unei adrese IP fixe către client pe baza adresei MAC.

Permite
Listbox {Activare; Dezactivare}, implicit = „Activare”
Activează/Dezactivează linia selectată.

adresa IP
Adresă IP, implicită = 0.0.0.0
Adresa IP fixă atribuită clientului. Trebuie să fie unic în tabelul Închirieri statice.
Trebuie să aparțină intervalului părinte din tabelul Servere DHCP. Nu trebuie să intre în conflict cu adresa postului local.

adresa MAC
Adresă MAC, implicită = 00:00:00:00:00:00
Adresa MAC a clientului pentru care este atribuită adresa IP fixă. Trebuie să fie unic în tabelul Închirieri statice.

Nota
Notă informativă.

7.7.2. DNS

Redirecționarea DNS funcționează ca un server proxy DNS. Primește interogări DNS de la clienți pe interfețele selectate. Filtrează interogările. Traducerea numelor selectate poate fi blocată. Trimite interogări personalizate către o listă specificată de servere. Menține un cache din care clientul poate răspunde imediat fără a interoga serverele părinte.

7.7.2.1. Configurare

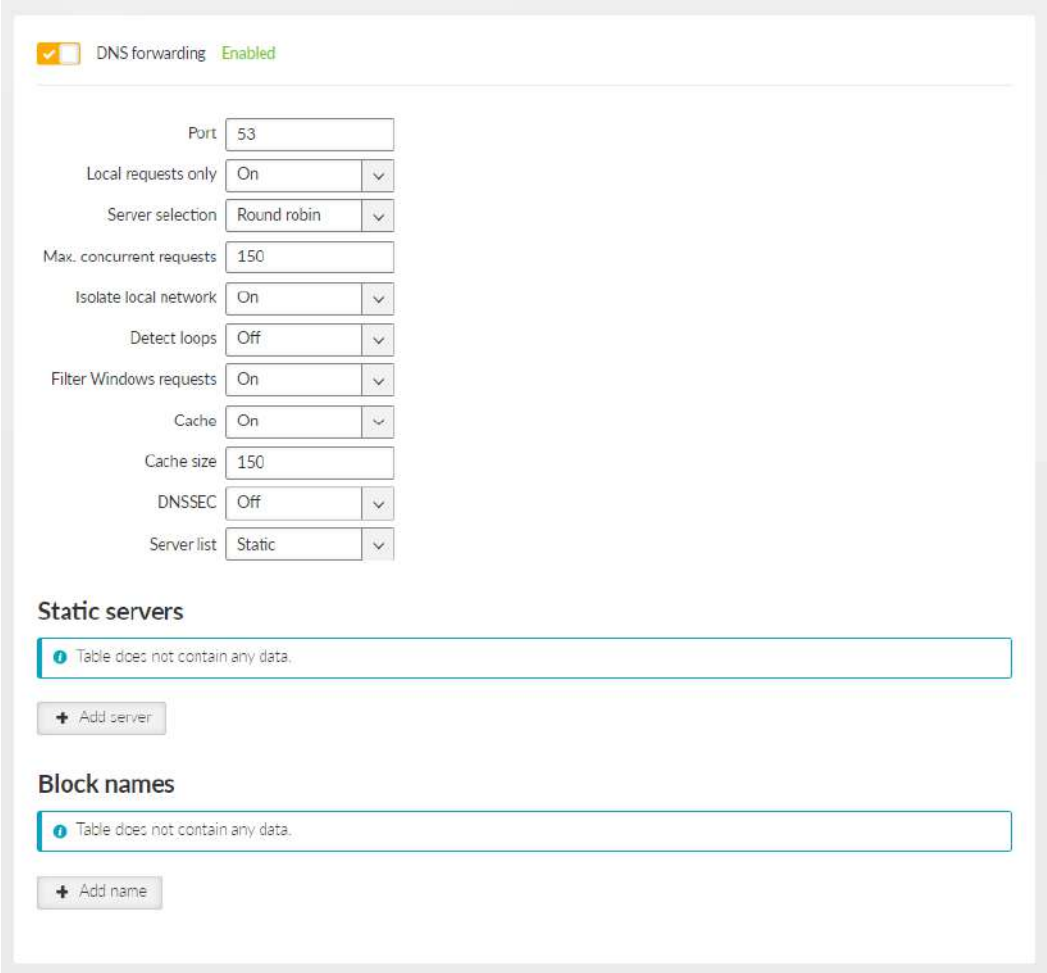


Fig. 7.38: SETĂRI > Servicii > Redirecționare DNS

Permite

Listbox {Activare; Dezactivare}, implicit = „Activare”
Activează/dezactivează redirecționarea DNS.

Port

Număr {1 – 65535}, implicit = 53
Numărul portului (atât UDP, cât și TCP) pe care serverul ascultă cererile clientului.

Doar cereri locale

Listbox {Dezactivat; Activat}, implicit = „Activat”
Stabilește dacă serverul servește numai cereri de la adrese din rețeaua locală (de la adrese din intervalele setate pe interfețe). Cererile de la alte adrese vor fi respinse.

Selectarea serverului

Caseta de listă {Round robin; Ordine strictă; Toate simultan}, implicit = „Round robin” Setează modul în care serverele sunt selectate pentru interogare.

Round robin

Selectează serverele unul câte unul, preferându-le pe cele care au răspuns.

Ordine strictă

Începe întotdeauna cu primul server din listă și încearcă următorul din secvență dacă nu reușește.

Toate simultan

Solicitarea este trimisă la toate serverele în același timp și se așteaptă primul răspuns.

Max. cereri concurente

Numărul {5 – 250}, implicit = 150
Numărul maxim de solicitări DNS care rulează simultan.

Izolați rețeaua locală

Listbox {Dezactivat; Activat}, implicit = „Activat”
Stabilește dacă serverul izolează rețeaua locală. Dacă este activat, blochează forțarea traducerii adreselor locale de la serverele părinte, nu trimite interogări inverse către adresele private către serverele părinte.

Detectează bucle

Listbox {Dezactivat; Activat}, implicit = „Dezactivat”
Activează detectarea buclei între serverele DNS.

Filtrați solicitările Windows

Listbox {Dezactivat; Activat}, implicit = „Activat”
Filtrează solicitările DNS periodice generate de Windows.

Cache

Listbox {Dezactivat; Activat}, implicit = „Activat”
Activează răspunsurile cache la solicitările DNS. Dacă răspunsul la cererea clientului este stocat în cache, acesta este returnat imediat și nu este nevoie să faceți alte cereri către serverele părinte.

Dimensiunea memoriei cache

Număr {50 – 10000}, implicit = 150
Număr maxim de intrări în cache.

DNSSEC

Listbox {Dezactivat; Activat}, implicit = „Dezactivat”
Permite autentificarea răspunsurilor de la serverele părinte folosind DNSSEC și lanțul de încredere (**Ancore de încredere DNS**masă).

Lista de servere

Listbox {Static; Dinamic}, implicit = „Static”

Static

Lista statică a serverelor din**Servere statice**masă.

Dinamic

Listbox {WWAN (MAIN); WWAN (EXT); PPP 1; PPP 2; PPP 3; Client PPPoE}, implicit = „Client PPPoE”

Lista de servere este obținută din parametrii interfeței WAN dinamice. Interfața corespunzătoare trebuie să fie activă.

7.7.2.1.1. Servere statice

Rândurile definesc adresele serverelor DNS părinte din lista statică.

Numărul maxim de servere DNS este de 32.

Activ numai dacă Lista de servere este setată la Static.

Fig. 7.39: SETĂRI > Servicii > Redirecționare DNS > Servere statice

Permite
Listbox {Activare; Dezactivare}, implicit = „Activare”
Activează/Dezactivează linia selectată.

Domeniu
Șir {0–128 char}, implicit = <gol> Nume domeniu.

adresa IP
Adresă IP, implicită = 0.0.0.0
Adresa IP a serverului static.

Port
Număr {1 – 65535}, implicit = 53
Portul de destinație pe care serverul ascultă cererile DNS.

Nota
Notă informativă.

7.7.2.1.2. Nume de bloc

Fiecare linie definește nume DNS a căror traducere este blocată.

Numărul maxim de nume blocate este 128. Ordinea nu contează.

Fig. 7.40: SETĂRI > Servicii > Redirecționare DNS > Nume blocate

Permite
Listbox {Activare; Dezactivare}, implicit = „Activare”
Activează/Dezactivează linia selectată.

Domeniu
Șir {0–128 char}, implicit = „example.com”
Nume de domeniu, a cărui traducere în adresă va fi blocată.

Nota
Notă informativă.

7.7.2.1.3. Ancore de încredere DNS

Fiecare linie definește un DNSSEC Trust Anchor.

Numărul maxim de ancore de încredere DNSSEC este 8. Ordinea nu contează.

Activ numai dacă Cache și DNSSEC sunt activate.

Fig. 7.41: SETĂRI > Servicii > Redirecționare DNS > Ancore de încredere DNS

Permite
Listbox {Activare; Dezactivare}, implicit = „Activare”
Activează/Dezactivează linia selectată.

Eticheta cheie
Număr {0 – 65535}, implicit = 0
Identificator cheie. Trebuie să fie unic printre liniile active din tabel.

Algoritm
Număr {0 – 255}, implicit = 0
Identificator algoritm cheie.

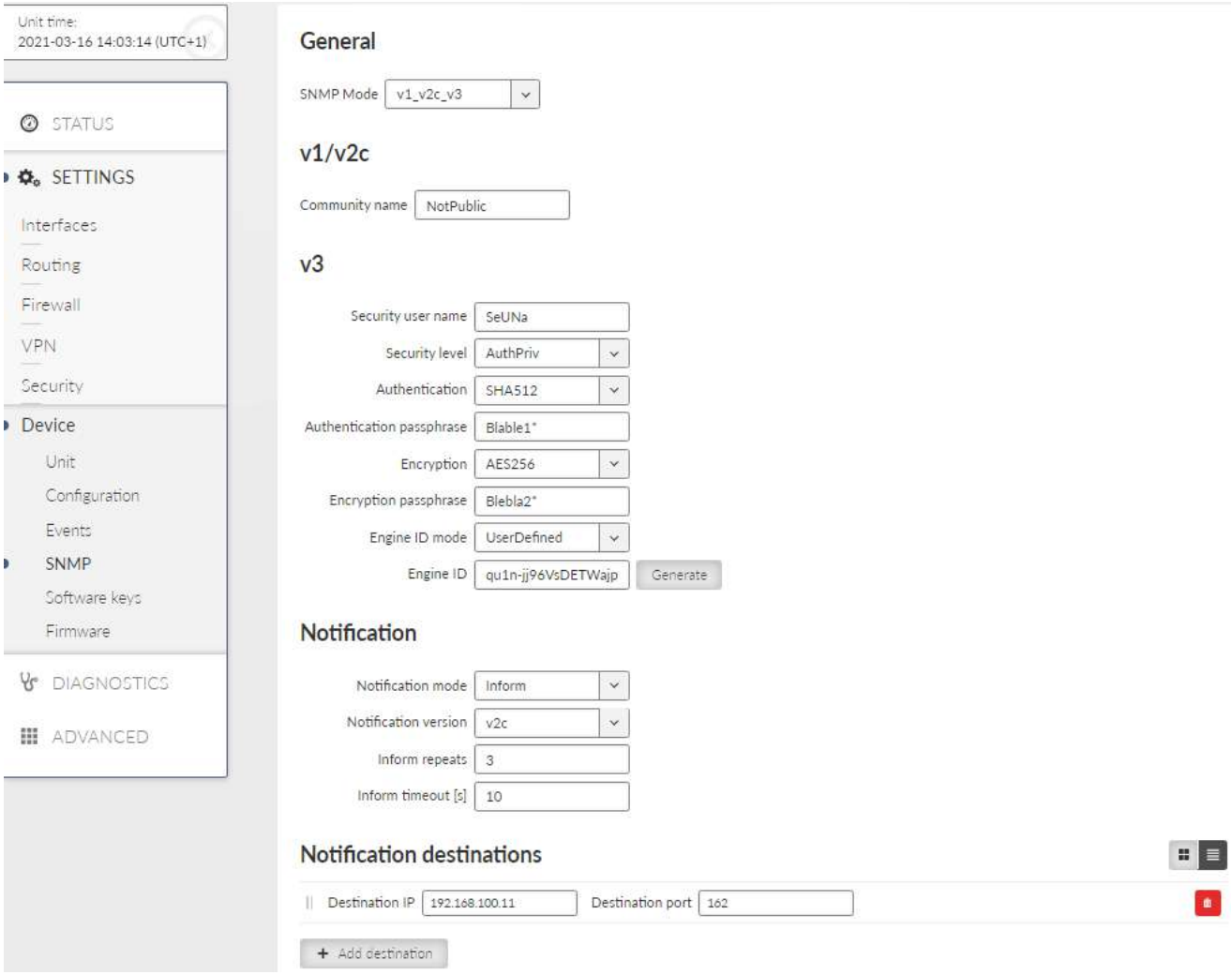
Tipul de digerare
Număr {0 – 255}, implicit = 0 Identificatorul
algoritmului de sinteza a cheilor.

Digera
Șir hexazecimal, implicit = <gol> Tasta
Digest (hash).

Nota
Notă informativă.

7.7.3. SNMP

Implementarea SNMP (Simple Network Management Protocol) în M!DGE3 oferă trei versiuni SNMP: v1, v2c și v3.



Nota

Următoarele caractere sunt interzise în comunicarea SNMP:
" (Citale duble) ` (Accent grav) \ (Bară inversă) $ (Simbol dolar) ; (Punt și virgulă)

Modul SNMP

Caseta listă {Off; v1_v2c_v3; v3}, implicit = „Dezactivat”

Activează SNMP și definește ce versiuni de protocol sunt disponibile.

Numele comunității

Șir {1–32 caractere}, implicit = „public”

Numele comunității folosit de v1 și v2c. Când se utilizează modul v1_v2c_v3, acest parametru este obligatoriu.

Setări versiunea 3

Nume de utilizator de securitate

Șir {1–32 caractere}, implicit = <gol>

Nume de utilizator pentru SNMPv3. Când este selectat protocolul v3, acest parametru este obligatoriu.

Nivel de securitate

Caseta listă {NoAuthNoPriv; AuthNoPriv; AuthPriv}, implicit = „NoAuthNoPriv”

Nivelul de securitate al protocolului v3. Activează/dezactivează autentificarea (Auth) și criptarea datelor SNMP (Priv).

Autentificare

Caseta listă {MD5_legacy; SHA1_legacy; SHA224; SHA256; SHA384; SHA512}, implicit = "SHA256" algoritm de autentificare. Nu se recomandă utilizarea algoritmilor vechi, sunt disponibili numai din motive de compatibilitate.

Fraza de acces pentru autentificare

Șir {8–128 char}, implicit = <empty> Fraza de acces utilizată pentru autentificare cu serverul SNMP.

Criptare

Caseta listă {DES_legacy; AES128; AES192; AES256}, implicit = "AES128"
Algoritm de criptare.

Fraza de acces de criptare

Șir {8–128 de caractere}
Fraza de acces utilizată pentru criptarea datelor atunci când comunicați cu serverul SNMP.

Modul ID motor

Caseta listă {Implicit; Definit de utilizator}, implicit = „Implicit”
ID-ul motorului servește pentru identificarea unică a instanței SNMP (adică unitatea M!DGE3) conform RFC3411. Când este selectat modul „Default” Engine ID, adresa MAC a interfeței ETH1 este utilizată pentru partea unică a ID-ului motorului (exemplul întreg ID-ul motorului: 800083130302a92006ef).

ID motor

Șir {1–27 caractere}
Când este selectat modul ID motor „Definit de utilizator”, partea diferențiată a ID-ului motor poate fi introdusă ca caractere ASCII sau generată (de exemplu, U3qPrisWoDYbBVNsAWluZYGL3M5). Acest șir este convertit în număr HEX (adică 55 33 71 50 72 69 73 57 6f 44 59 62 42 56 4e 73 41 57 6c 75 5a 59 47 4c 33 4d 35). ID-ul întregului motor pentru exemplul menționat: 800083130455337150726973576f44596242564e7341576c755a59474c334d35.

Notificare

Notificarea este utilizată pentru notificarea asincronă de la o unitate M!DGE3 în serverul SNMP.

Modul de notificare

Caseta listă {Off; Capcană; Inform}, implicit = „Dezactivat”
Modul de notificare; Inform nu este acceptat de SNMPv1.

Versiunea de notificare

Caseta listă {v1; v2c; v3}, implicit = „v2c”
Versiunea pachetelor de notificare.

Informați repetările

Numărul {0 – 10}, implicit = 3
Numărul de repetări utilizate atunci când confirmarea informării nu a fost primită.

Informare expirare [s]

Număr {1 – 20}, implicit = 10
Informați expirarea confirmării.

Destinații de notificare

IP de destinație

Adresă IP, implicită = 0.0.0.0

Adresa IP a serverului SNMP care primește pachete de notificare.

Port de destinație
Număr {1 – 65535}, implicit = 162 Port destinație pachete de notificare.

Pentru informații mai detaliate, consultați *Notă de aplicație SNMP*[10].

7.7.4. Syslog

Syslog permite înregistrarea evenimentelor pe un server la distanță. Mesajele Syslog sunt create în unitate în conformitate cu RFC5424 și trimise la un server la distanță. Mesajele pot fi trimise folosind UDP sau TCP.

Noile jurnale de sistem și evenimente încep să fie trimise la serverul de la distanță după pornirea stației. În caz de indisponibilitate a serverului la distanță, jurnalele sunt stocate în buffer-ul de disc și trimise la serverul de la distanță după restabilirea conexiunii cu acesta.

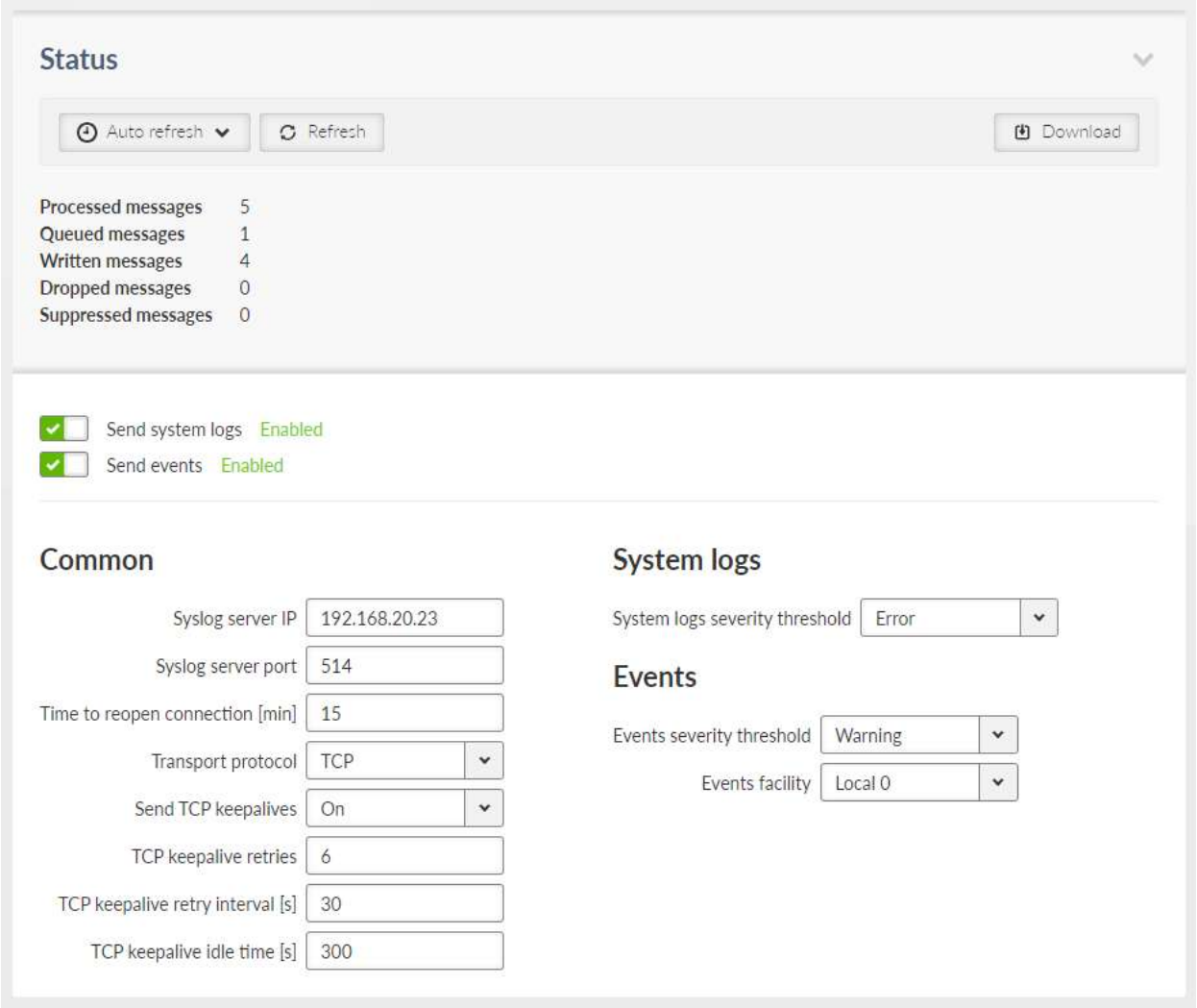


Fig. 7.42: SETĂRI > Servicii > Syslog

[10] https://www.racom.eu/eng/products/m/ripex/app/snmp-ripex2/index.html

Trimiteți jurnalele de sistem

{Permite; Dezactivați}, implicit = „Dezactivați”

Activează/Dezactivează trimiterea jurnalelor de sistem către serverul de la distanță

Trimite evenimente

{Permite; Dezactivați}, implicit = „Dezactivați”

Activează/Dezactivează trimiterea evenimentelor de sistem către serverul de la distanță

Comun

IP server Syslog

Adresă IP, implicită = 0.0.0.0

Adresa IP a serverului Syslog la distanță

Port server Syslog

Număr {1 – 65535}, implicit = 514

Număr port server la distanță Syslog

Timp pentru redeschiderea conexiunii [min]

Număr {1 – 240}, implicit = 15

Timp (în minute) de așteptat pentru a reîncerca conexiunea la serverul de la distanță când conexiunea a fost închisă

Protocolul de transport

Caseta listă {UDP; TCP}, implicit = "UDP" Tipul de protocol pentru transportul de date

Când TCP:

Trimiteți TCP keepalives

Caseta listă {Off; Activat}, implicit = „Activat”

Activează/Dezactivează trimiterea mesajelor TCP keepalives

Reîncercări TCP Keepalive

Numărul {1 – 15}, implicit = 6

Numărul de încercări keepalive când răspunsul nu a fost primit.

Interval de reîncercare TCP keepalive [s]

Număr {10 – 240}, implicit = 30

Intervalul (în secunde) la care un mesaj TCP keepalive este retrimis dacă nu se primește niciun răspuns.

Timp de inactivitate TCP keepalive [s]

Număr {60 – 64800}, implicit = 300

Timp de inactivitate a conexiunii (în secunde) în așteptarea trimiterii mesajului TCP keepalive.

Jurnalele de sistem

Pragul de severitate al jurnalelor de sistem

Caseta listă {Emergency; Alerta; Critic; Eroare}, implicit = „Urgență”

Mesajele de sistem cu această gravitate și mai mari vor fi trimise către serverul de la distanță. Mesajele cu severitate mai mică nu vor fi trimise.

Evenimente

Pragul de severitate al evenimentelor

Caseta listă {Emergency; Alerta; Critic; Eroare; Avertizare; Observa; Informațional}, implicit = „Urgență” Evenimentele de sistem cu această gravitate și mai mari vor fi trimise la serverul de la distanță. Evenimentele cu severitate mai mică nu vor fi trimise.

Facilitate de evenimente

Caseta listă {Local 0; Local 1; Local 2; Local 3; Local 4; Local 5; Local 6; Local 7}, implicit = "Local 7" Clasificarea evenimentelor de sistem în facilități conform RFC 5424 pentru uz local: Local 0 la Local 7 (coduri numerice de la 16 la 23) pot fi setate. Consultați-vă cu administratorul de server Syslog despre ce facilitate va fi utilizată pentru grupuri individuale de unități.

7.7.5. SMS

M!DGE3, complet conectat la rețeaua celulară (starea CONECTAT), este capabil să primească și să trimită SMS-uri.

• Primirea și trimiterea SMS-urilor este asigurată de un serviciu Linux.

• Coada de SMS-uri în așteptare pentru trimitere este controlată de serviciul Linux de diagnosticare adecvat.

• Lungimea SMS-ului depinde de tipul de modul și de codare. Dacă este necesar un SMS mai lung (numai **Notificări prin SMS**), este împărțit într-un SMS în lanț.

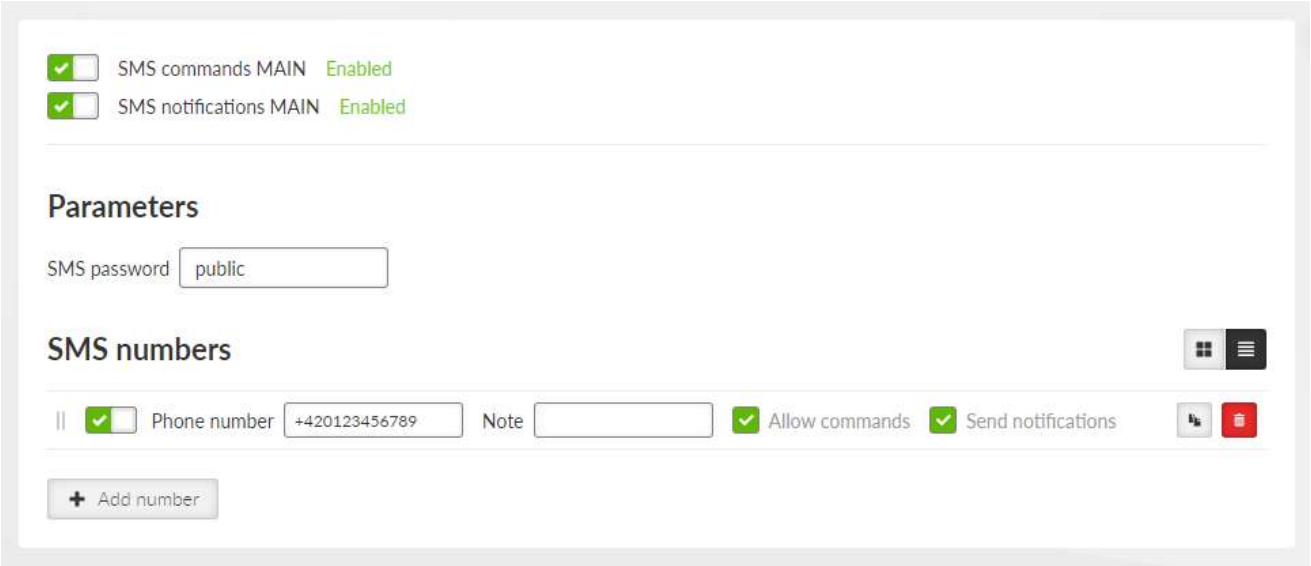


Fig. 7.43: SETĂRI > Servicii > SMS

Nota

Această secțiune cooperează strâns cu *Secțiunea 7.1.4, „Celular”*.

Comenzi SMS MAIN/EXT

{Permite; Dezactivați}, implicit = „Dezactivați”

Activează/Dezactivează comenzile SMS pentru Cellular MAIN/EXT. Când este activat, modulul software permite toate SMS-urile primite și începe să inițieze comenzile.

• Pentru a procesa o comandă SMS de la un număr de telefon:

○ Numărul de telefon specific trebuie definit în parametru**numere SMS**. Dacă numărul de telefon nu este definit, SMS-ul nu va fi procesat.

○ SMS-ul trebuie să conțină o parolă pentru a trece autentificarea (parametrul**parola SMS)**.

○ SMS-ul trebuie să conțină un mesaj valid*formatul unei comenzi*.

• Numai SMS-urile obișnuite sunt acceptate (SMS-urile în lanț nu sunt).

• Unele comenzi generează un răspuns automat, care este trimis la un(e) numere(e) de telefon definit(e), dacă această caracteristică este activată.

• Dacă acest parametru este dezactivat, toate SMS-urile primite vor fi șterse.

Notificări prin SMS MAIN/EXT

{Permite; Dezactivați}, implicit = „Dezactivați”

Activează/Dezactivează comenzile SMS pentru Cellular MAIN/EXT.

Când este activată, orice modificare (dacă este configurată în*Secțiunea 7.6.3, „Evenimente”*) va genera un SMS de notificare, care va fi trimis la toate numerele de telefon definite cu notificare activă.

• Pentru a trimite o notificare prin SMS la un număr de telefon:

○ Numărul de telefon specific trebuie definit în parametru**numere SMS**. Dacă numărul de telefon nu este definit, acesta nu va primi nicio notificare.

• SMS-urile înlănțuite sunt acceptate.

• Trimiterea notificărilor prin SMS poate fi activată în*Secțiunea 7.6.3, „Evenimente”*.

7.7.5.1. Parametrii

Parola SMS

Șir {2–16 caractere ASCII}, implicit = „public”

Setează o parolă pentru SMS, care servește drept autentificare pentru a trimite SMS-uri de la numerele de telefon definite. Intervalul de lungime a parolei este între 2 și 16 caractere. Parola SMS nu trebuie să conțină caractere neacceptate. Caracterele neacceptate sunt: ", `, \, $, ;.

7.7.5.2. numere SMS

Număr de telefon

{Permite; Dezactivați}, implicit = „Activați”

Activează/Dezactivează numărul de telefon. Când este activat, numărul de telefon definit poate trimite sau primi (sau ambele) SMS-uri. Numărul de numere de telefon care pot primi și trimite SMS-uri este limitat la 10.

Nota

Comentariu optional.

Permite comenzi

{Pe; Off}, implicit = „Activat”

Permite acceptarea comenzilor de la un număr de telefon definit.

Nota

Acest parametru va funcționa numai dacă parametrul Comenzi SMS MAIN/EXT este activat.

Trimite notificări

{Pe; Off}, implicit = „Activat”

Permite trimiterea notificărilor către numărul de telefon definit.

Nota

Acest parametru va funcționa numai dacă parametrul Notificări SMS MAIN/EXT este activat.

7.7.5.3. Comenzi SMS

Toate comenzile trebuie să se potrivească cu următorul format:

<parolă>„spațiu”<comandă>„spațiu”[<param1>...]

Comenzi SMS:

starea celulei

Exemplu: starea celulei publice

Solicitare SMS cu extras din starea celulară a modulului care a primit SMS-ul. **Răspuns la comanda „cellstatus”:** Statie: *<nume_stație>* *<tip_modul>* *<SIM>* Profil *<profile_id>*
Stare: *<stare_conexiune>* Reg: *<stare_înregistrare>* Net: *<PLMN>*

Svc: *<tip_serviciu>*
Bandă: *<banda>*
Semnal: *<puterea_semnalului>*
APN: *<username_APN>*
IP: *<IP_alocat>*

Exemplu de răspuns pentru comanda „cellstatus”:

Gara: Alef
EXT SIM2 Profil 1
Stare: CONECTAT
Reg: RegHome
Net: 23002
Svc: 2G_EDGE
Banda: ARFCN 77
Semnal: RSSI: >=-48 dBm
APN: internet
IP: 100.110.103.173

smsevent <param>

Exemplu: public smsevent raise

Această comandă este folosită pentru a activa/dezactiva alarmele care pot fi setate *Secțiunea 7.6.3, „Evenimente”* prin utilizarea parametrilor săi („creștere”, „ștergere”).

Această comandă nu generează un răspuns automat.

7.7.6. server GNSS

Serverul GNSS colectează date de la un receptor GNSS (GPS) și furnizează datele unor aplicații client potențial multiple într-o arhitectură de aplicație server-client. Intern este folosit de NTP.

Preluarea datelor este posibilă folosind o aplicație client gpsd (cum ar fi cgps sau gpspipe). Formatul de date JSON este acceptat și sunt disponibile cadre de date TPV, SKY și PPS.

Activați GNSS

Caseta listă {On; Off}, implicit = Off

Activează/dezactivează subsistemul GNSS. Acest parametru apare numai dacă modulul GNSS este disponibil în unitate.

Activați serverul GNSS - Meniu avansat

Caseta listă {On; Off}, implicit = Off

Activează/dezactivează serverul GNSS. Acest parametru poate fi setat numai dacă este parametru**Activați serverul GNSS**este setat pe „Pornit”.

Port server GNSS

Număr {1 – 65535}, implicit = 2947

Setează un număr de port TCP al serverului GNSS. Acest parametru poate fi setat numai dacă sunt parametri**Activați serverul GNSS**și**Port server GNSS**sunt setate la „Pornit”.

Timp maxim de oprire GNSS [min]

Număr {1 – 65535}, implicit = 15

Setează un temporizator care contează pentru cât timp unitatea nu are nevoie de date noi despre locație (când GNNS este activ). Dacă timpul expiră, sunt declanșate acțiuni de securitate (repornire serviciu linux, repornire modul). Acest parametru poate fi setat numai dacă este parametru**Activați serverul GNSS**este setat pe „Pornit”.

7.8. Avansat

M!DGE3 introduce un nou concept pentru setările expertului și implementarea rapidă a noilor funcții numite secțiunea „Avansat”. Secțiunea avansată afișează automat toate punctele de setare de configurare prezente în prezent în dispozitiv, fără a fi nevoie să proiectați o pagină de configurare specială (cum ar fi cele din „Setări”). Acest lucru ne permite să implementăm noi funcții rapid cu fiecare firmware nou și, de asemenea, permite utilizatorilor experimentați să-și ajusteze M!DGE3.

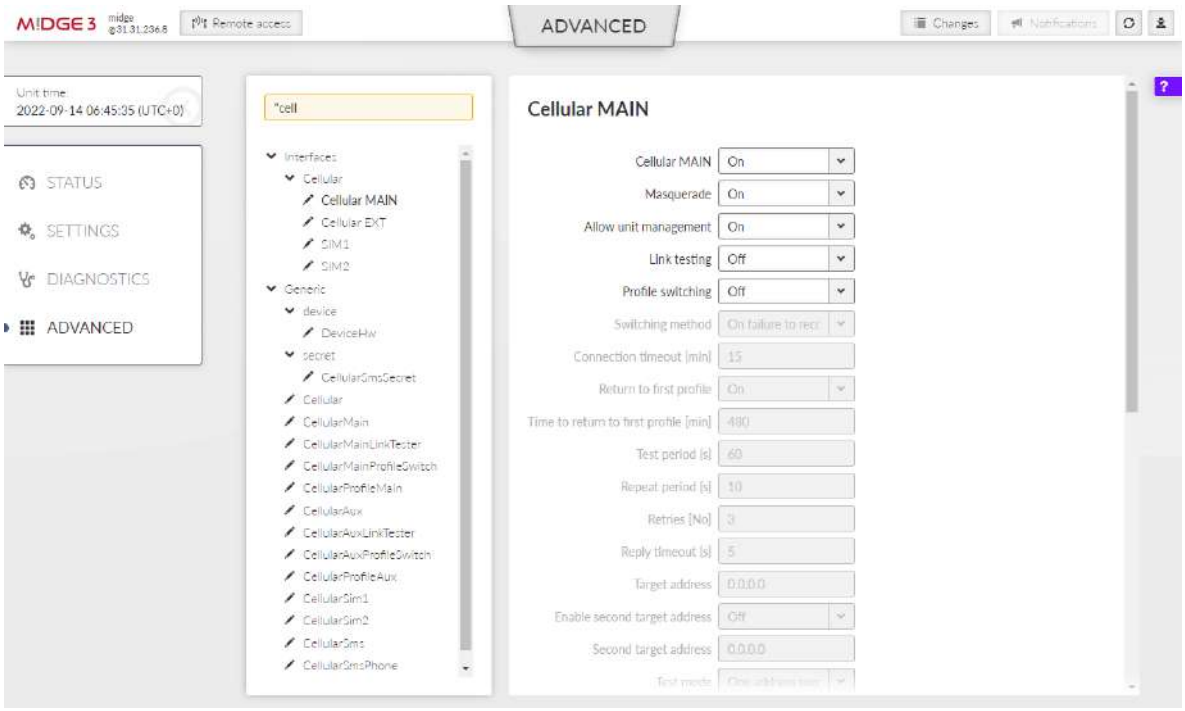
Vă rugăm să rețineți că M!DGE3 este un dispozitiv foarte puternic și chiar arată toți parametrii în secțiunea Avansat.

Când vizitați pagina pentru prima dată, veți vedea un câmp de căutare și sub un arbore de pagini de configurare.

Câmpul de căutare examinează toate etichetele și arborele în sine și este capabil să arate toate paginile de configurare relevante. Dispune de așa-numita căutare „fuzzy” capabilă să returneze răspunsurile corecte chiar și atunci când există o greșeală de scriere în interogarea de căutare. Încercați să căutați „Ethernet” sau „BGP” pentru a vedea funcția în acțiune. Pentru a utiliza din nou întregul arbore, pur și simplu ștergeți interogarea de căutare.

Arborele de configurare are două părți. Pentru confortul dvs., primele câteva elemente (Interfețe, Rutare, ...) folosesc o ierarhie similară cu „Setări”, dar includ toate setările avansate. Cele mai noi caracteristici pot fi găsite în ultimul articol numit „General”, care conține toate tabelele de configurare care există în unitate.

Prin selectarea unei pagini de configurare (marcată cu pictograma creion) este afișată o fereastră în partea dreaptă a ecranului care conține punctele de setare ale paginii de configurare selectate. Puteți modifica setările și apoi le puteți trimite către dispozitiv în același mod pe care îl știți din „Setări”.

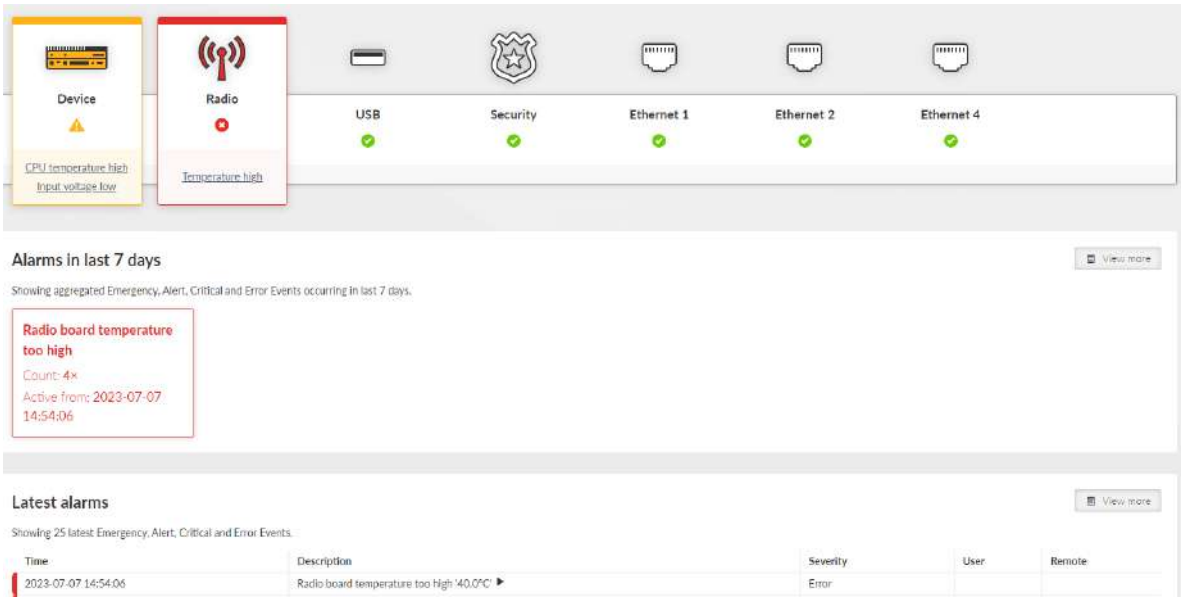


Fiți atenți când ajustați setările în secțiunea Avansat și examinați pagina „Modificări” în detaliu înainte de a trimite modificări la dispozitiv.

8. Diagnosticare

8.1. Prezentare generală STATUS

Oferă informații de ansamblu despre secțiunile individuale ale unității. fiecare secțiune este legată de o zonă de Evenimente (vezi Secțiunea 8.4,*„Evenimente”*).



Atunci când în unitate are loc orice eveniment cu severitate mai mare decât Notice, pictograma corespunzătoare va schimba culoarea în funcție de gravitatea evenimentului, linkul duce la informații suplimentare despre eveniment în meniul DIAGNOSTIC. STARE afișează și descrie, de asemenea, alarmele din ultima săptămână, care sunt evidențiate sub pictograme. Ultimele 25 de evenimente de urgență, alertă, critice și eroare sunt afișate în partea de jos a paginii.

Tab. 8.1: Pictogramele secțiunii unității

	Dispozitiv
	USB
	Securitate
	Ethernet 1-5

Nota

Numărul de pictograme Ethernet vizibile depinde de setările unității. (SETĂRI > Interfețe > Ethernet > Porturi)

Fiecărui eveniment i se poate atribui o gravitate individuală. Când mai multe evenimente cu gravitate diferită sunt declanșate în aceeași secțiune, prioritatea este: Eroare > Avertisment > Notă.

Tab. 8.2: Pictograme de severitate

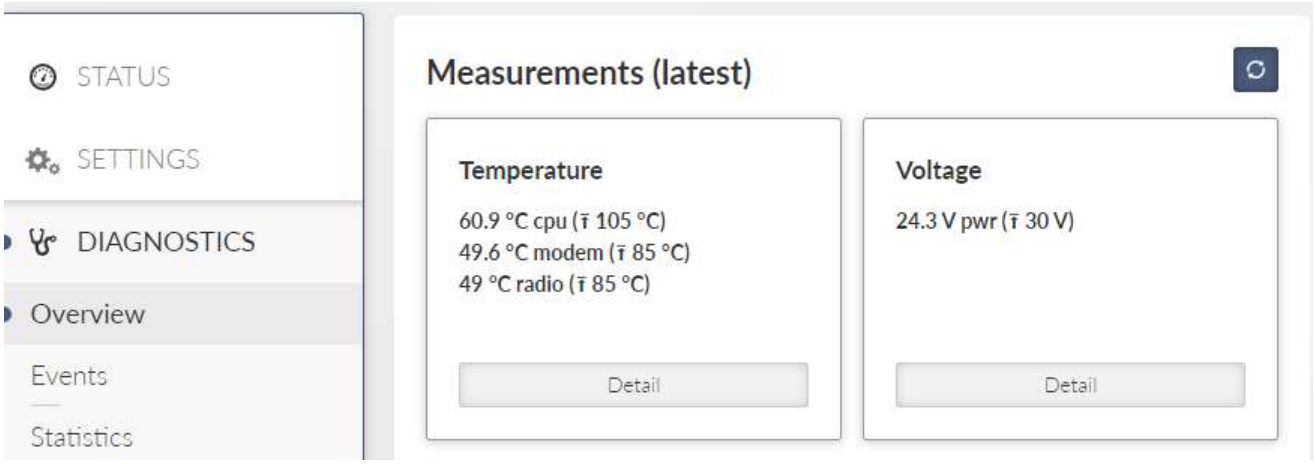
	Unitatea funcționează impecabil
	Informațional, Notă
	Avertizare
	Eroare, critică, alertă, urgență

8.2. Prezentare generală

Secțiunea Prezentare generală servește pentru a oferi informații generale despre M!DGE3.

8.2.1. Măsurătorile

Prezentare generală a secțiunii - Măsurători conține măsurarea datelor curente (obținute de la senzori).



• Temperatura cardului - furnizează date despre temperatură (pe CPU, modem).

• Tensiune card - furnizează date despre tensiunea măsurată pe conectorul de intrare.

Simbolurile cu cap de săgeată (↑, ↓, →) au următoarea semnificație:

• ↑ - Valoarea limită maximă. Se declanșează o alarmă când valoarea (afișată între paranteze) este depășită.

• ↓ - Valoarea minimă-limită. Se declanșează o alarmă când valoarea scade sub valoarea, care este afișată între paranteze.

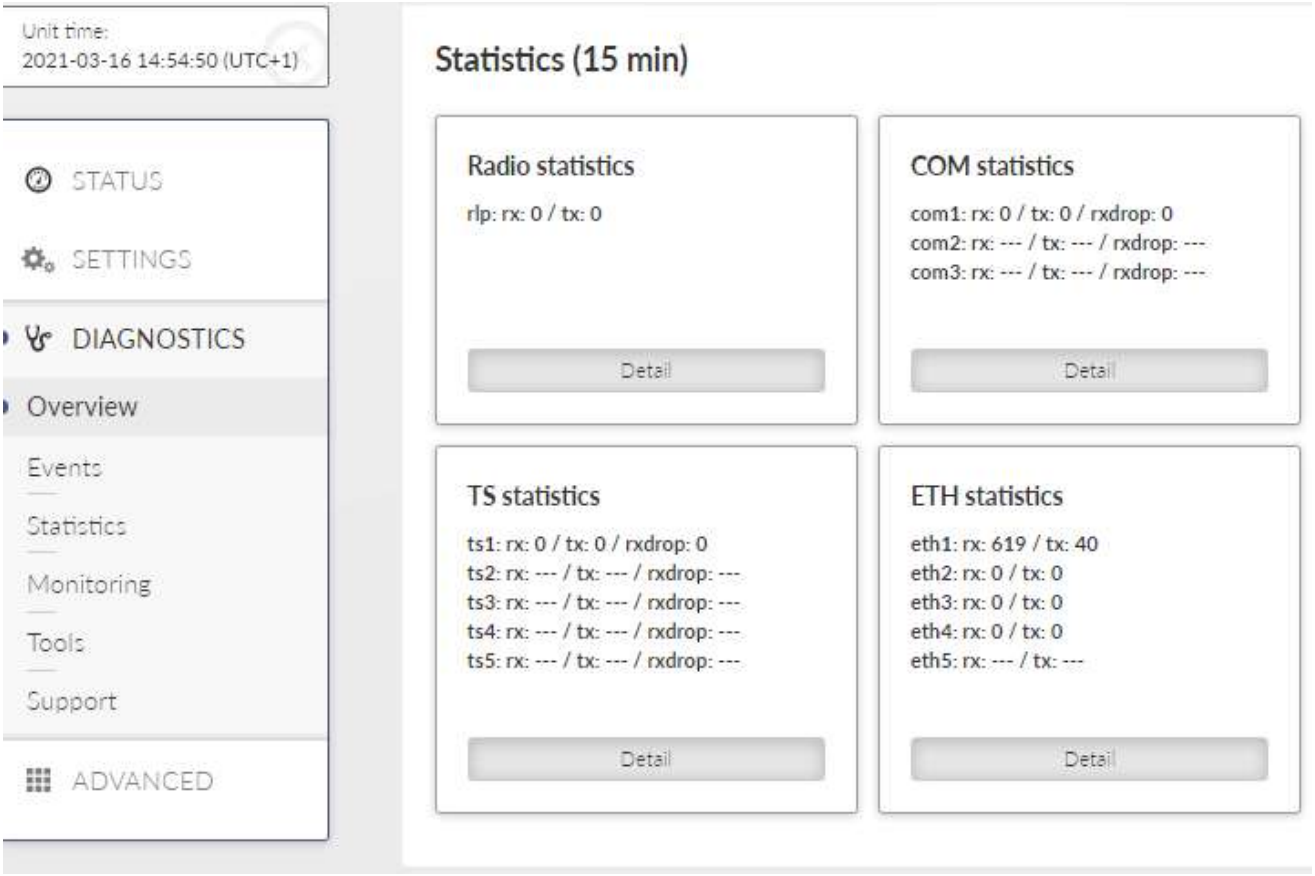
• → - Valoarea ar trebui să se îndrepte către alta.

Nota

Măsurătorile de valoare sunt colectate o dată la 10 secunde.

8.2.2. Statistici

Prezentare generală a secțiunii - Statistici arată o scurtă vizualizare a statisticilor din ultimele 15 minute (din momentul deschiderii ferestrei sau apăsarea butonului Reîmprospătare).



• Statisticile cardurilor sunt întotdeauna afișate pentru toate interfețele.

• Dacă interfața este dezactivată, statisticile sale (înregistrarea) sunt afișate ca „-“.

• Colectarea statisticilor este actualizată la fiecare 1 s (în fiecare secundă este posibil să se vadă noi valori).

• Intervalul de 15 minute este colectat luând 14 minute din istoric + secunde trecute din minutul curent.

8.3. Informaţii

Această secțiune oferă informații mai detaliate (extras de date) despre setările unității M!DGE3. Oferă, de asemenea, o explicație mai profundă despre unele dintre valorile și interfețele setate. Sunt furnizate și date de diagnosticare.

8.3.1. Interfețe

Oferă un extras complet de informații despre toate interfețele active (adrese, detalii și statistici incluse). Toate interfețele utilizate de routerul Linux (inclusiv toate interfețele interne precum npi, loop, ag, ip6tnl etc.) sunt afișate în această secțiune.

8.3.1.1. Interfețe Ethernet

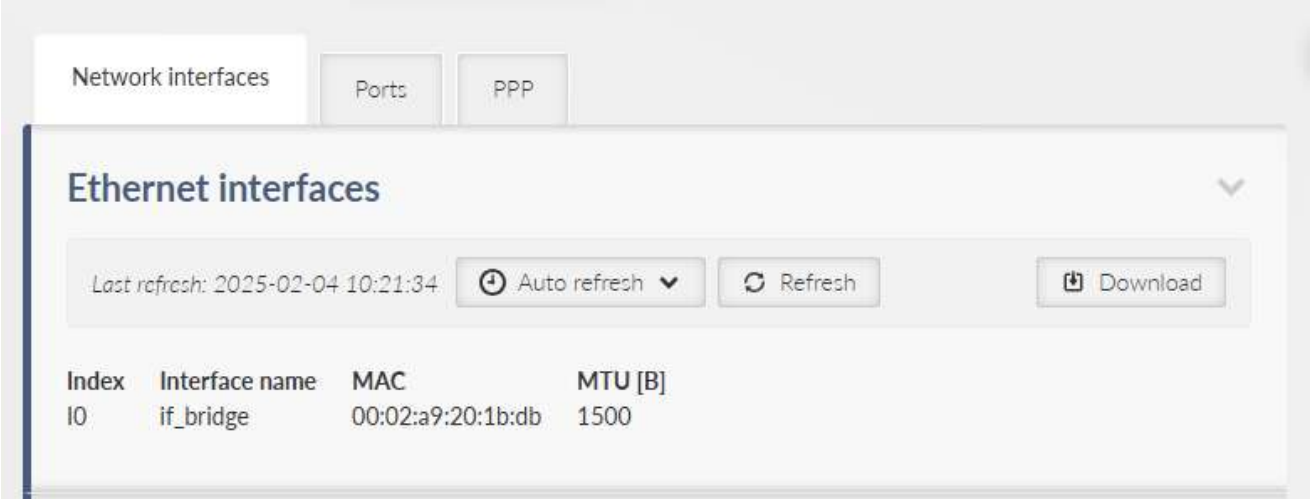


Fig. 8.1: DIAGNOSTICĂ > Informații > Interfețe > Ethernet

Interfețele utilizate în unitățile M!DGE3 sunt, în general, fie porturi Bridged (BP-L2) fie interfețe rutate (RI-L3).

Toate interfețele utilizate de routerul Linux (excluse interfețele interne) sunt afișate în următoarea listă.

dacă_*<LanIface_Name>*
: Interfață punte LAN tip RI-L3
(SETĂRI > Interfețe > Ethernet > Interfețe de rețea)

dacă_*<LanVlan_IfName>.<LanVlan_VlanId>*

- Tip de interfață VLAN BP-L2 (dacă este utilizat ca port în podul LAN) (SETĂRI > Interfețe > Ethernet > Interfețe de rețea>VLAN)
- Tip de interfață VLAN RI-L3 (dacă nu este utilizat ca port în podul LAN) (SETĂRI > Interfețe > Ethernet > Interfețe de rețea > IP/Subrețea > VLAN)

8.3.1.2. Interfețe de rețea

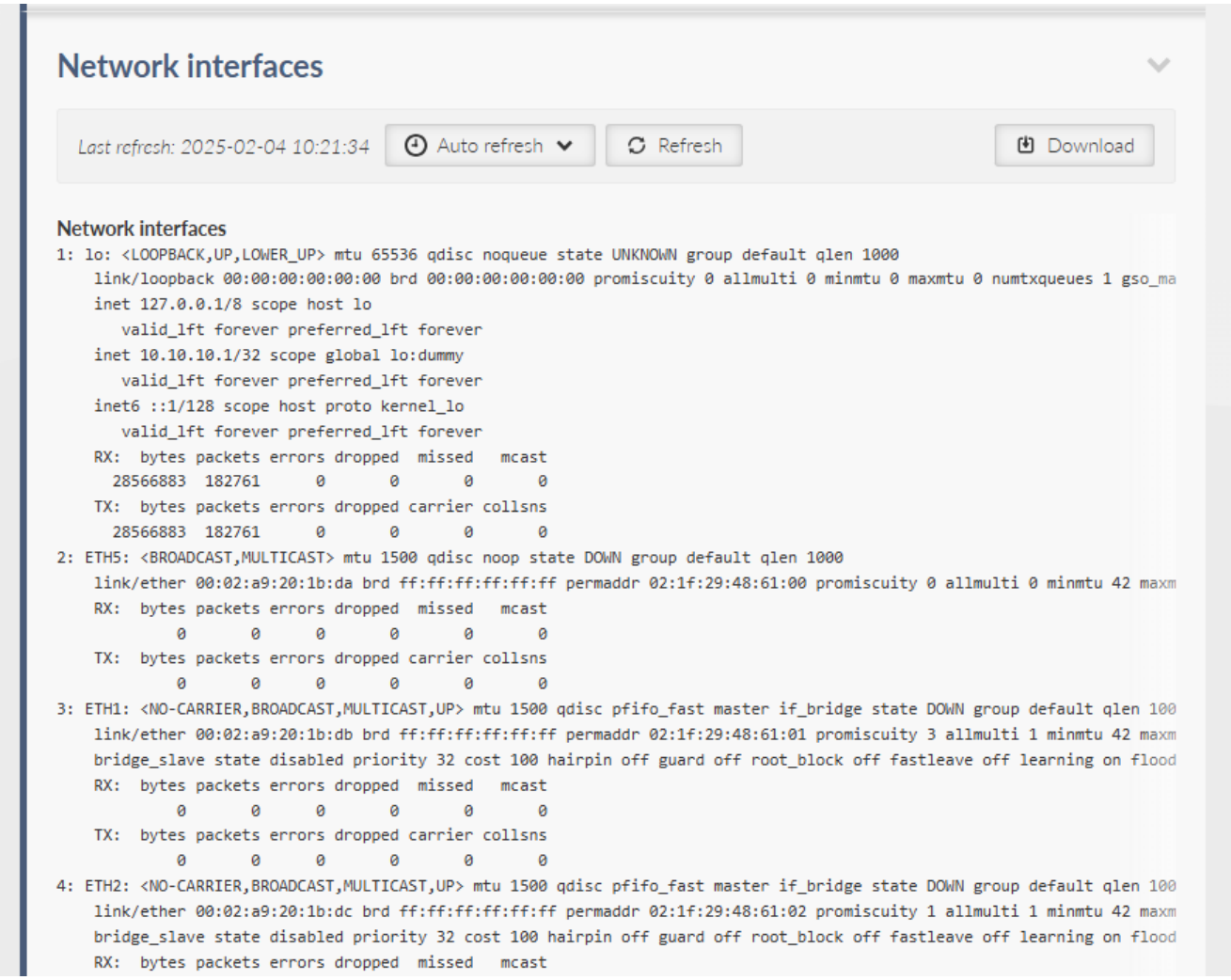


Fig. 8.2: DIAGNOSTICĂ > Informații > Interfețe > Ethernet

eth1, eth2, eth3, eth4
Interfață porturi Ethernet fizice ETH1 – ETH4, tip interfață BP-L2

eth0
Interfața portului fizic SFP (ETH5), tip interfață BP-L2

wwan
Interfață bridge a modulului celular principal, tip interfață RI-L3 (SETĂRI > Interfață > Cellular > PRINCIPALA)

ext
Interfață bridge a modulului celular EXT, tip interfață RI-L3 (SETĂRI > Interfață > Cellular > EXT)

gre_tap*<INDEX>*
Interfață tunel GRE L2, tip interfață BP-L2 (SETĂRI > VPN > GRE > L2)

gre_tun*<INDEX >*
Interfață tunel GRE L3, tip interfață RI-L3 (SETĂRI > VPN > GRE > L3)

uite

Interfață Loopback Tipul de interfață RI-L3 – Adresele IP ale loopback-ului (AVANZAT > Interfețe > Loopback).

8.3.1.3. Interfețe celulare

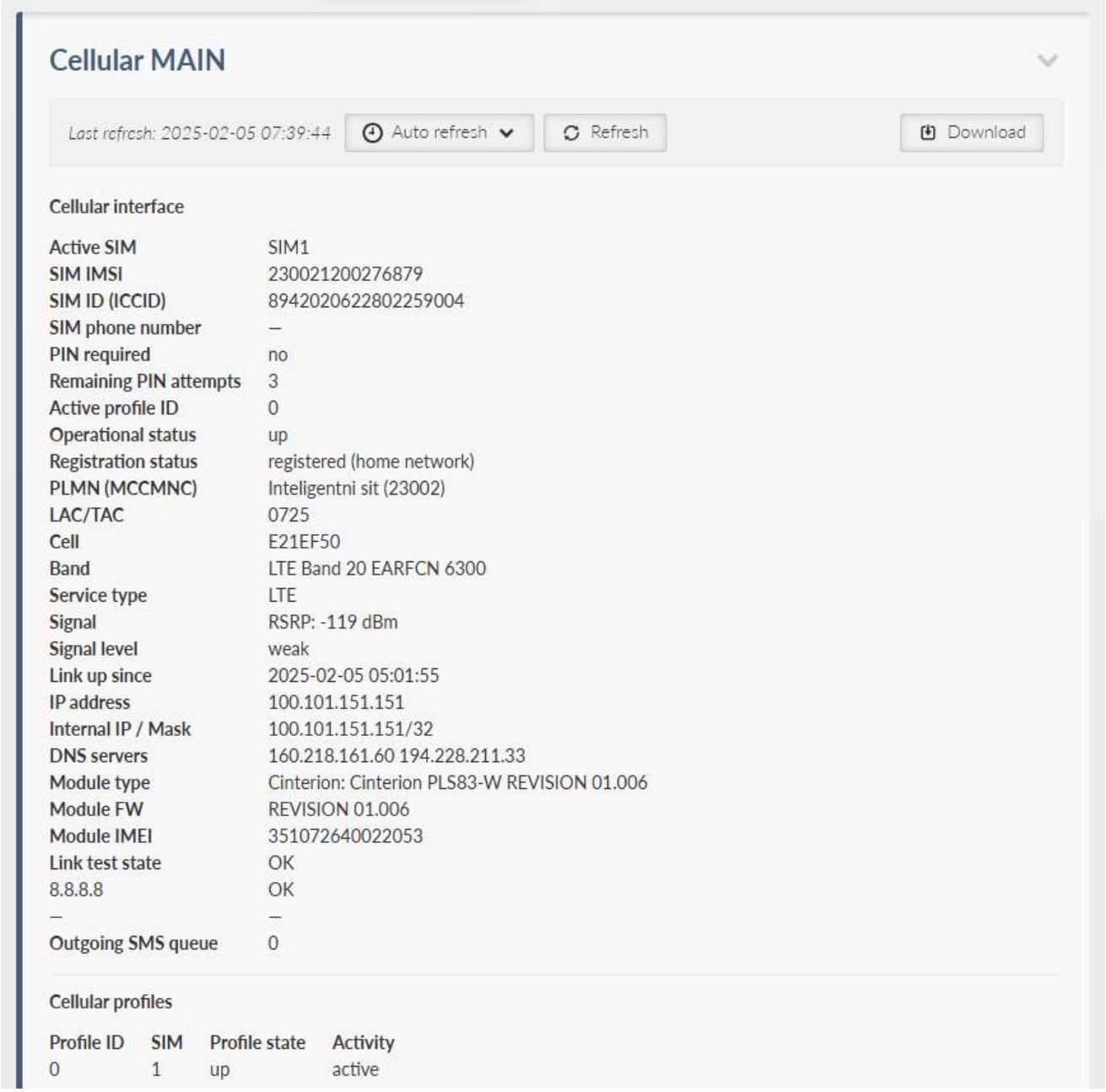


Fig. 8.3: DIAGNOSTICĂ > Informații > Interfețe > Cellular

SIM activ

SIM utilizat în prezent

SIM IMSI

Identitatea stației mobile internaționale a SIM-ului activ

ID SIM (ICCID)
ID-ul cardului de circuit integrat al SIM-ului activ

Număr de telefon SIM
Număr de telefon SIM, dacă este stocat în SIM

PIN necesar
Dacă SIM-ul pe care îl utilizați în prezent necesită un PIN

Încercări de PIN rămase
Numărul rămas de încercări de a introduce codul PIN în SIM

ID de profil activ
ID-ul profilului SIM utilizat în prezent

Starea operațională
Starea conexiunii

Starea de înregistrare
Starea de înregistrare

PLMN (MCCMNC)
Numele furnizorului și PLMN al rețelei conectate

LAC/TAC
LAC (2G, 3G) sau TAC (4G, LTE Cat. M/NB) al locației la care este conectat modulul

Celulă
ID-ul celulei

Bandă
Banda folosita. Nu este completat pentru 2G
Întotdeauna adăugat ARFCN (2G), UARFCN (3G) sau EARFCN (4G, LTE Cat. M/NB) - numărul canalului

Tipul serviciului
Serviciu conectat

Semnal
Puterea semnalului curent

Nivelul semnalului
Nivelul curent al puterii semnalului

Conectați-vă de atunci
Marca temporală (cu UTC) a deschiderii conexiunii

adresa IP
Adresă IP atribuită interfeței când este deschisă (din APN)

IP intern/Mască
Adresa IP atribuită interfeței atunci când aceasta este deschisă (internă, din modul)

servere DNS
Adresele IP ale serverelor DNS, separate printr-un spațiu

Tipul de modul
Numele modulului și producătorul

Modulul FW
Versiunea de firmware a modulului

Modulul IMEI
Identitatea International Mobile Equipment a modulului

Stare de testare a legăturii
*Testarea linkurilor*stare, dacă este activată

Coada de SMS-uri de ieșire
SMS-ul în coadă, așteaptă să fie trimis

Profiluri celulare
Starea profilurilor

ID de profil
ID de profil în tabelul de profil

SIM
SIM utilizat de profil

Starea profilului
Cel mai recent statut al profilului

Activitate
Dacă profilul este activ în prezent

8.3.1.4. Client PPPoE

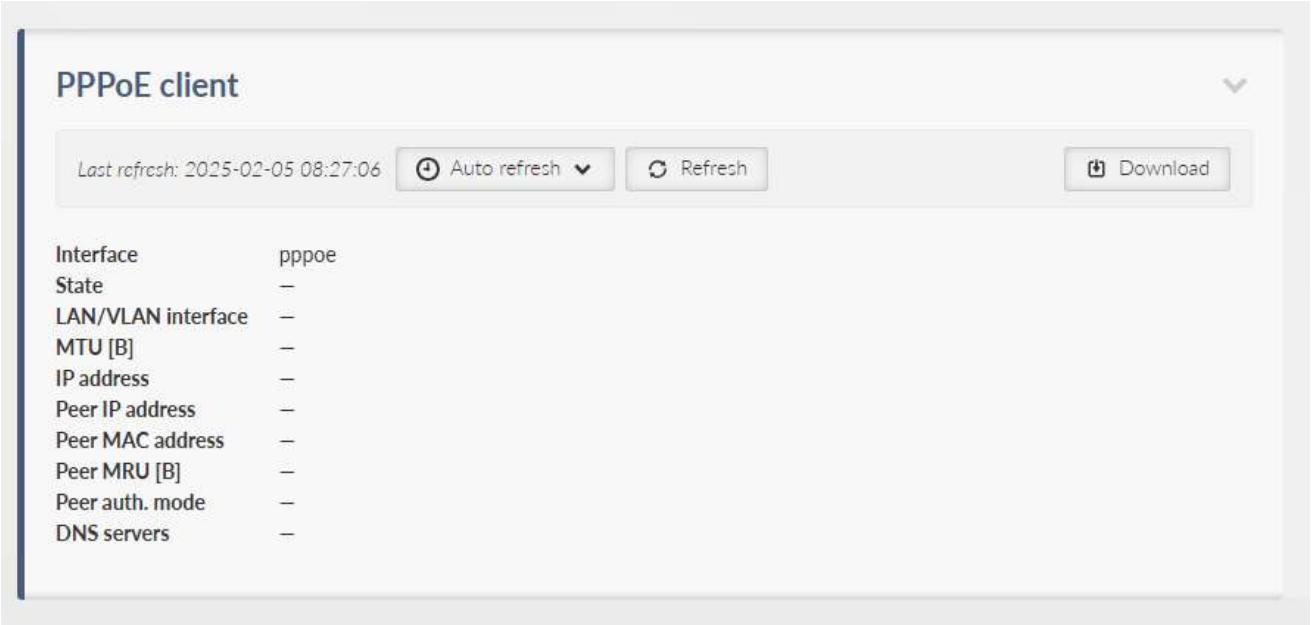


Fig. 8.4: DIAGNOSTICĂ > Informații > Interfețe > Client PPPoE

Interfață Numele interfeței PPPoE

Stat	Starea actuală a interfeței
Interfață LAN/VLAN	Numele interfeței LAN/VLAN pe care rulează clientul PPPoE
MTU [B]	MTU al interfeței LAN/VLAN pe care rulează clientul PPPoE
adresa IP	Adresă IP atribuită
Adresă IP peer	Adresa IP a peer-ului (server)
Adresă MAC peer	Adresa MAC a peer-ului (server)
Peer MRU [B]	Maximum Receive Unit (MRU) în octeți solicitați de peer-ul de negociere
Autentificare de la egal la egal. modul	Protocolul de autentificare solicitat de peer
servere DNS	Adresele IP ale serverelor DNS, separate printr-un spațiu

8.3.1.5. Wifi

Oferă informații detaliate despre punctul de acces Wi-Fi și clienții Wi-Fi conectați.

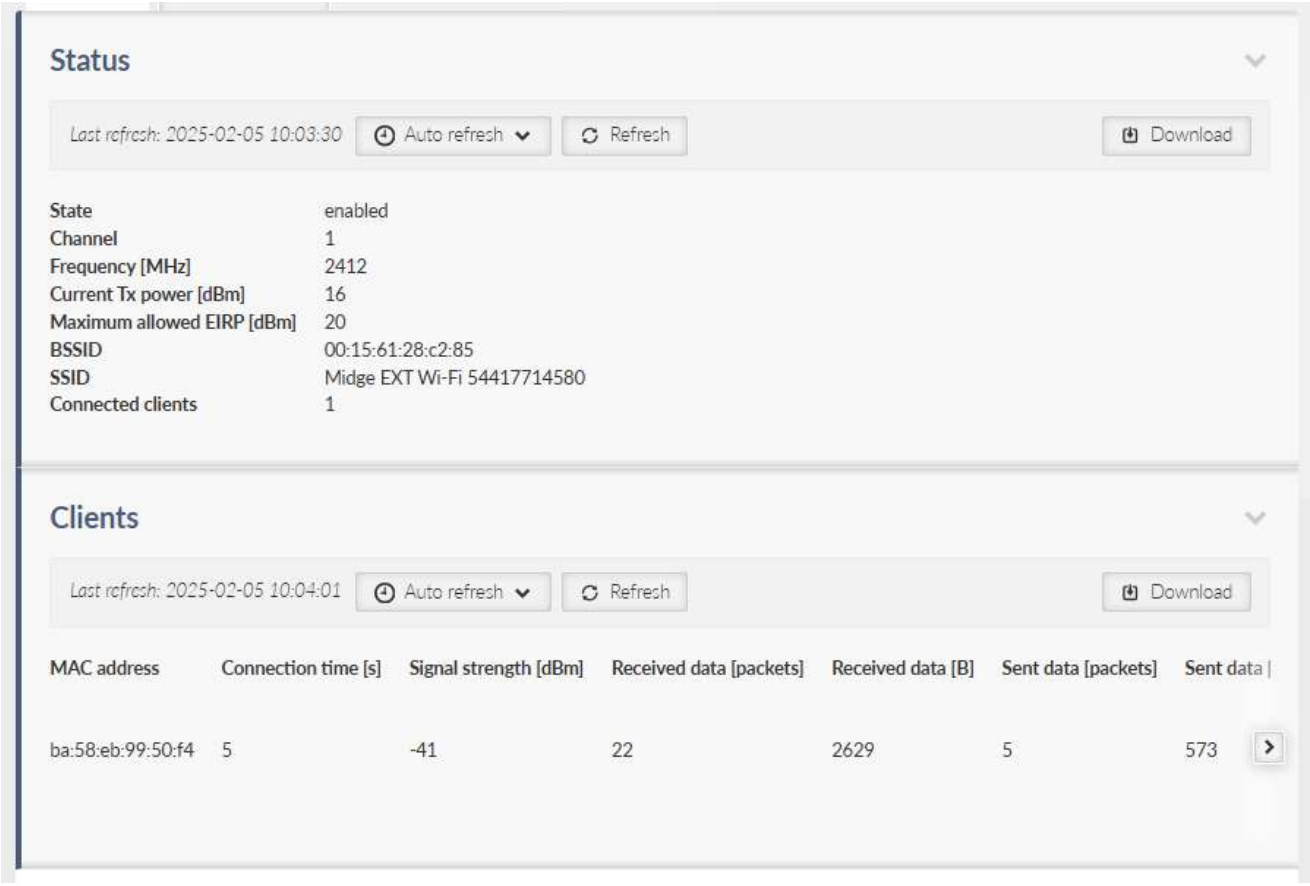


Fig. 8.5: DIAGNOSTICĂ > Informații > Interfețe > Wi-Fi

8.3.2. Dirijare

Oferă informații despre extragerea datelor din secțiunea Rutare.

Fig. 8.6: DIAGNOSTICĂ > Informații > Rutare

Această secțiune este împărțită în următoarele părți:

• Sistem - extras complet de date din tabelul de rutare a sistemului. Afișează datele apelate de comanda Linux „ip route show”.

• Dynamic - extras complet de date din tabelul de rutare intern al serviciului de rutare dinamică bird master4. Afișează datele apelate de comanda linux „birdcl show route all table master4”.

• Babel - extras de date privind starea protocolului Babel. Afișează datele apelate de următoarele comenzi Linux: „birdcl show babel interfaces”, „birdcl show babel neighbors”, „birdcl show babel routes”, „birdcl show babel entries”, „birdcl show babel route all table babel_ipv4”.

• OSPF- extras de date a stării protocolului OSPF. Afișează datele apelate de următoarele comenzi Linux: „birdcl show ospf neighbors”, „birdcl show ospf state”, „birdcl show ospf interface”, „birdcl show route all table ospf_ipv4”.

• BGP - extras de date a stării tuturor instanțelor protocolului BGP. Afișează datele apelate de următoarele comenzi Linux: „birdcl show protocol '"bgp*"'", "birdcl show protocol all '"bgp*"'", "birdcl show route all table bgp_ipv4".

8.3.3. Firewall

Oferă o prezentare generală despre extragerea datelor din secțiunile L2, L3 și NAT.

8.3.3.1. Firewall L2

Afișează datele numite de comanda Linux „iptables -L”.

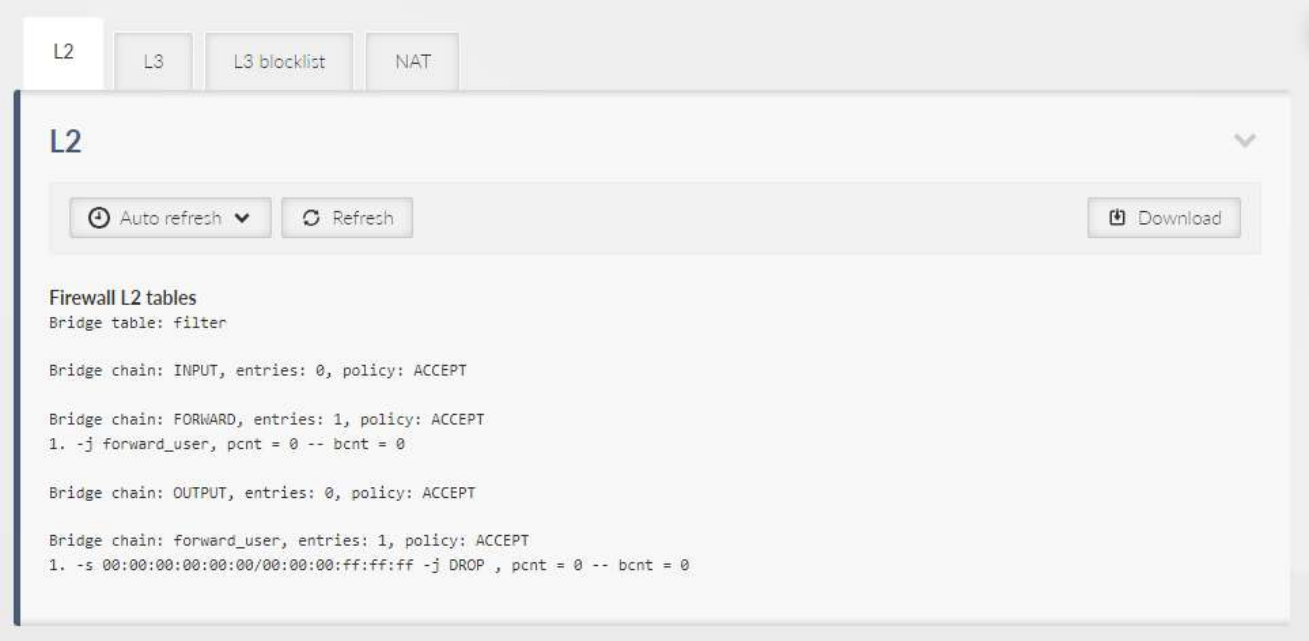


Fig. 8.7: DIAGNOSTICĂ > Informații > Firewall > L2

8.3.3.2. Firewall L3

Afișează datele apelate de următoarele comenzi Linux „iptables -nvL --line-numbers”.

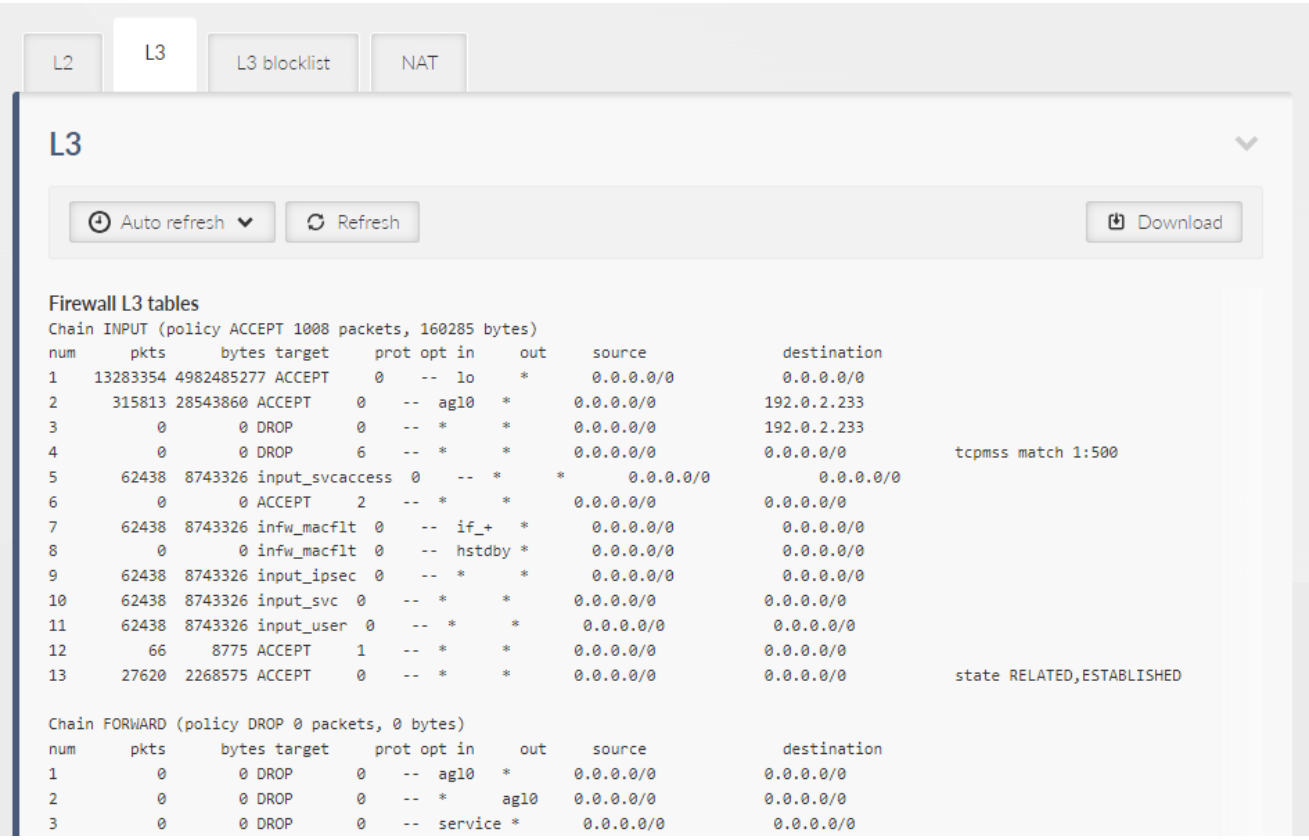


Fig. 8.8: DIAGNOSTICĂ > Informații > Firewall > L3

8.3.3.3. Lista blocată pentru firewall L3

Listarea listei de adrese interzise. Adresele sunt adăugate la listă dacă acțiunea: „Refuză, adaugă la lista de blocare” (adăugarea adresei sursă a pachetului primit la lista interzisă) este configurată în Firewall L3 - Reguli de intrare

8.3.3.4. NAT

Afișează datele apelate de următoarele comenzi Linux:

• „iptables -t nat -nvL postrouting_user” – date despre SNAT

• „iptables -t nat -nvL prerouting_user” – date despre DNAT

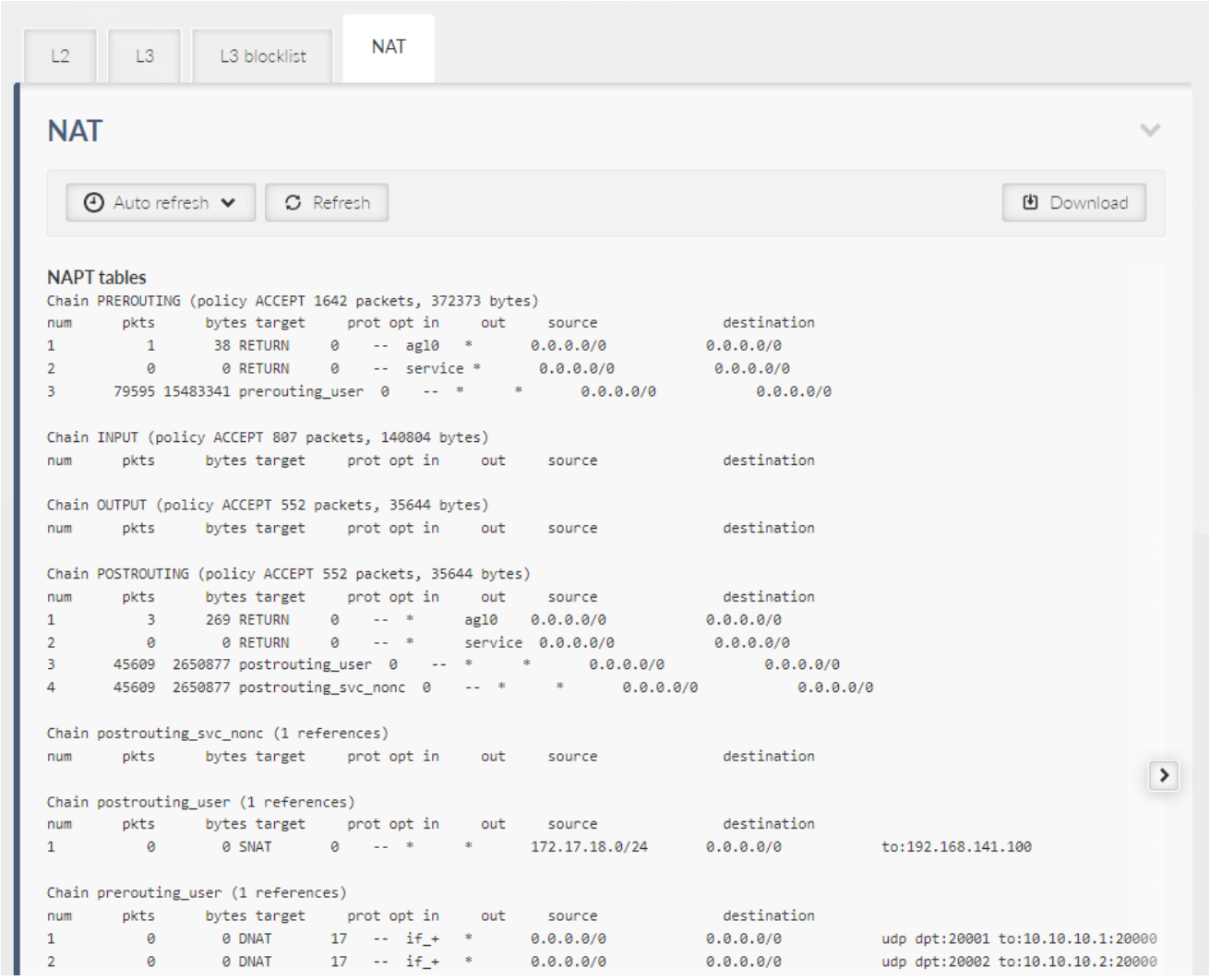


Fig. 8.9: DIAGNOSTICĂ > Informații > Paravan de protecție > NAT

8.3.4. Calitatea serviciului

Creează un tabel despre obiect și extras de statistici pentru fiecare interfață dată. Acest tabel conține:

• Numele unei interfețe.

• Starea și statisticile disciplinelor frontale - afișează datele numite de comanda linux „tc qdisc show”.

• Starea și statisticile claselor - afișează datele numite de comanda linux „tc class show”.

• Starea și statisticile filtrului - afișează datele numite de comanda linux „tc filter show”.

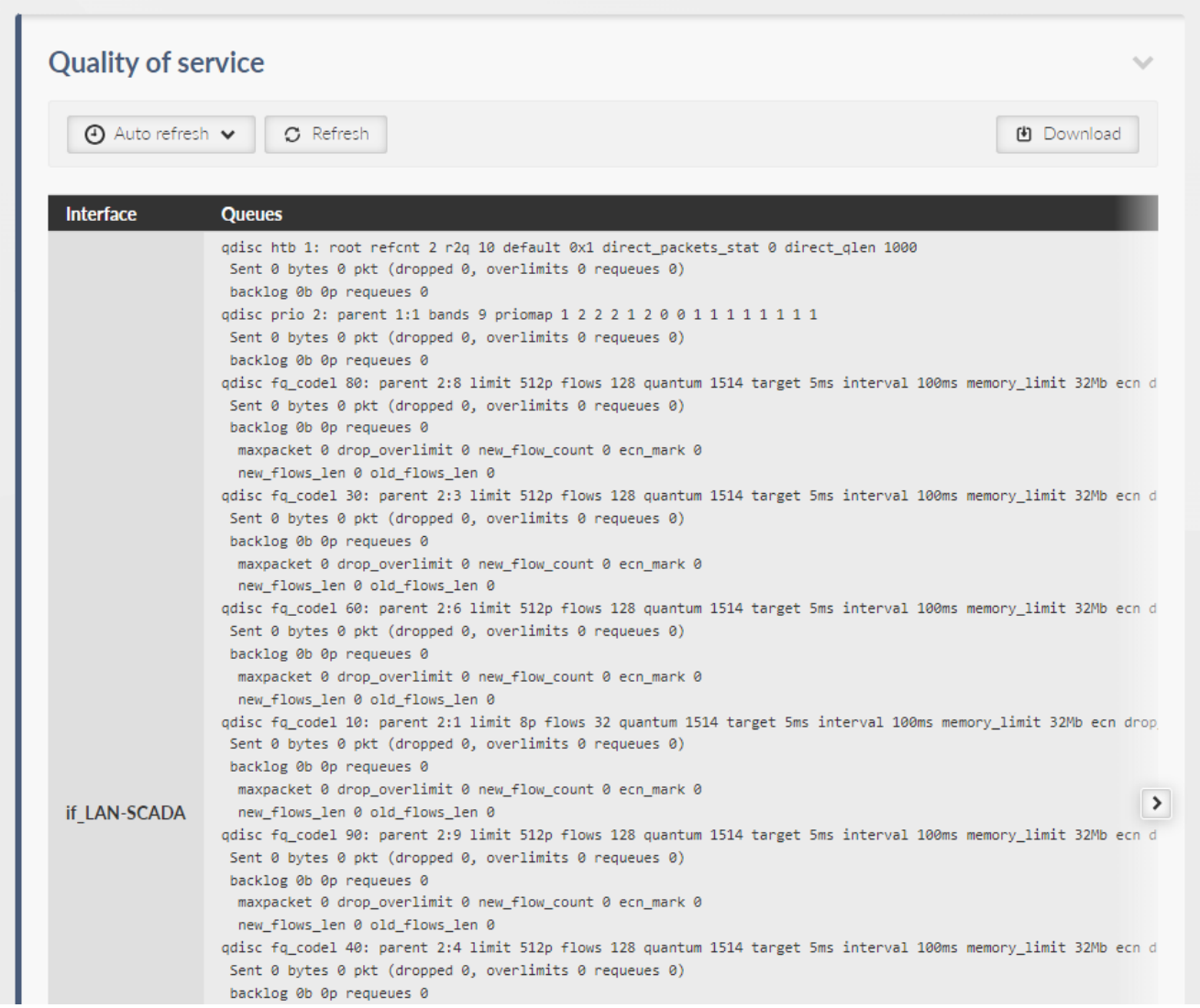


Fig. 8.10: DIAGNOSTICĂ > Informații > Calitatea serviciului

8.3.5. Servere DHCP

Lista adreselor atribuite de serverul DHCP.

adresa IP	Adresa IP atribuită clientului
adresa MAC	adresa MAC a clientului
Închiriază până la	Ora la care expiră contractul de închiriere

8.3.6. SNMP

Afișarea valorii ID-ului motorului. ID-ul motorului este utilizat pentru a identifica în mod unic stația atunci când comunicați cu managerul SNMP.

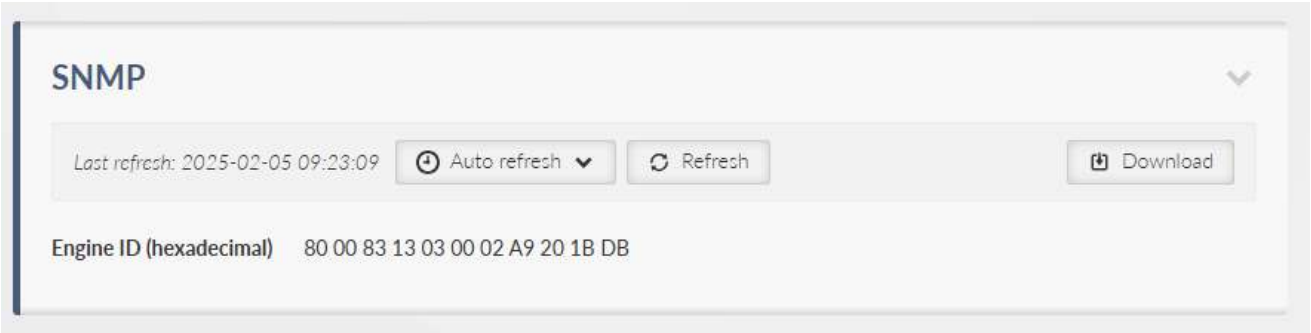


Fig. 8.11: DIAGNOSTICĂ > Informații > Servicii > SNMP

8.3.7. Syslog

Listarea contoarelor de mesaje către un server Syslog la distanță.

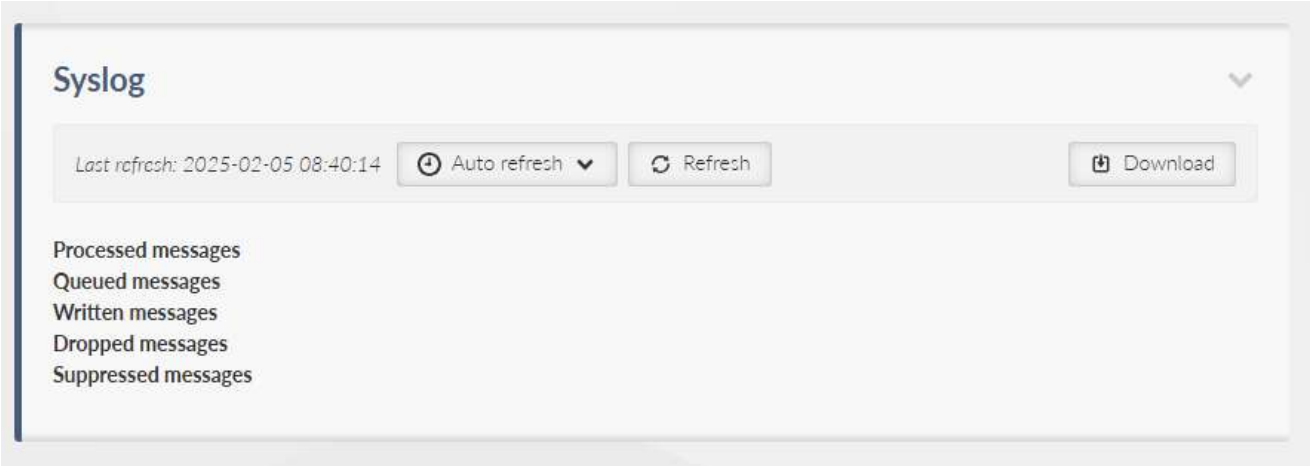


Fig. 8.12: DIAGNOSTICĂ > Informații > Servicii > Syslog

8.3.8. SMS

Oferă informații despre mesajele SMS trimise și primite.

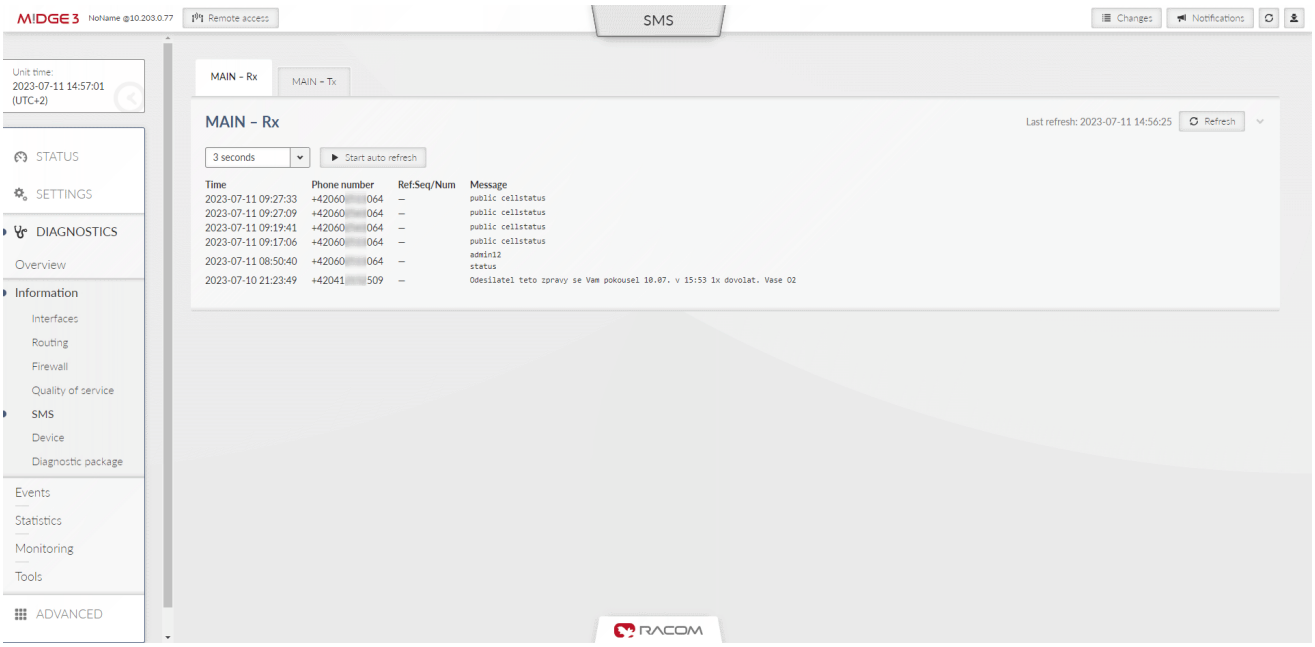


Fig. 8.13: DIAGNOSTICĂ > Informații > SMS > MAIN - Rx

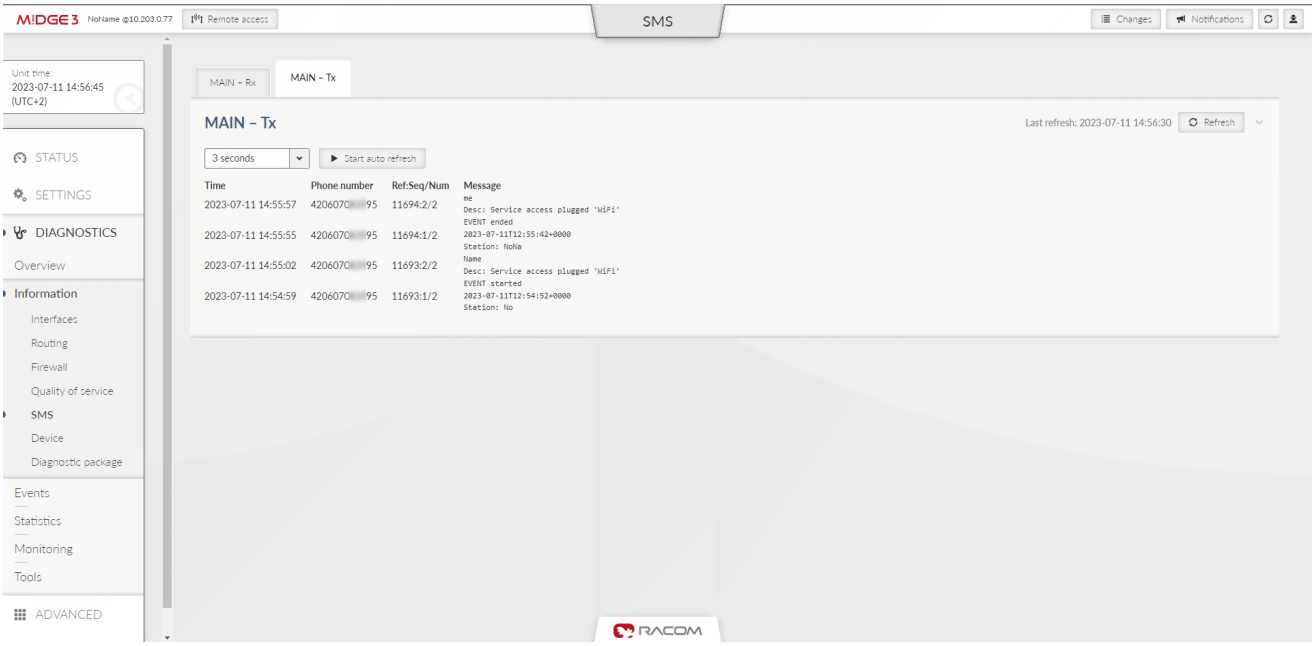


Fig. 8.14: DIAGNOSTICĂ > Informații > SMS > MAIN - Tx

8.3.9. Dispozitiv

Oferă informații generale despre unitate (dispozitiv).

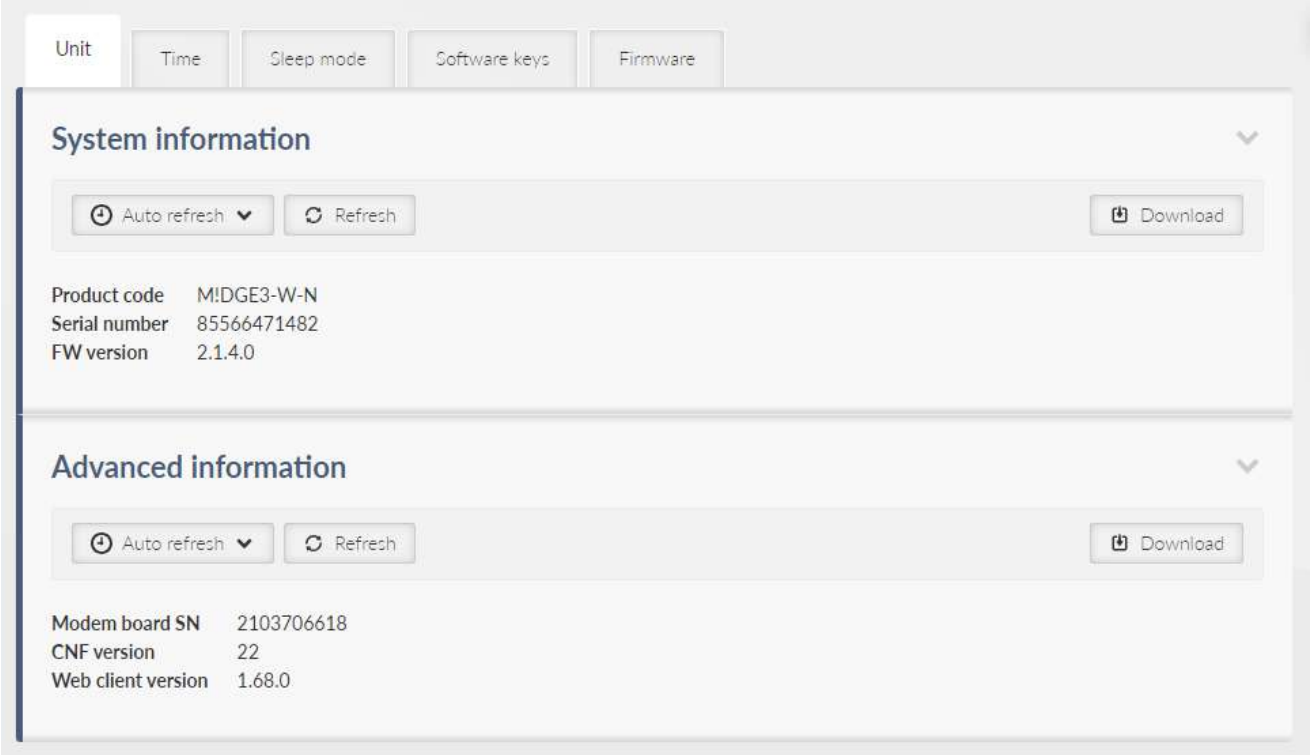


Fig. 8.15: DIAGNOSTICĂ > Informații > Dispozitiv

8.3.9.1. Informații despre sistem

Sunt furnizate informații de bază ale unității.

• Cod produs - Identifică hardware-ul unității.

• Număr de serie - Număr unic de identificare a unității.

• Versiune FW - Firmware-ul unității instalat în prezent.

8.3.9.2. Informații avansate

Sunt furnizate informații suplimentare despre unitate, care ar putea fi solicitate pentru diagnosticare avansată. Descriere parțială:

• SN plăci modem - Numărul sistemului plăcilor modem.

• Versiune CNF - Versiunea configurației unității.

• Versiune web client - Versiunea clientului web curent.

8.3.10. Pachet de diagnosticare

Acest meniu servește pentru colectarea datelor, fie de la stația locală, fie de la distanță și stocarea lor într-un pachet (fișier). Pachetul de diagnosticare servește în primul rând ca instrument de ajutor, pentru suportul tehnic al RACOM în cazul oricăror probleme potențiale ale unității. Dimensiunea minimă a unui pachet este de 5 kB. Pachetul de diagnosticare este descărcat deja comprimat, ceea ce economisește aprox. 1/3 din dimensiunea sa originală.

Este acceptată o singură colectare de pachete (se aplică atât la nivel local, cât și la distanță).

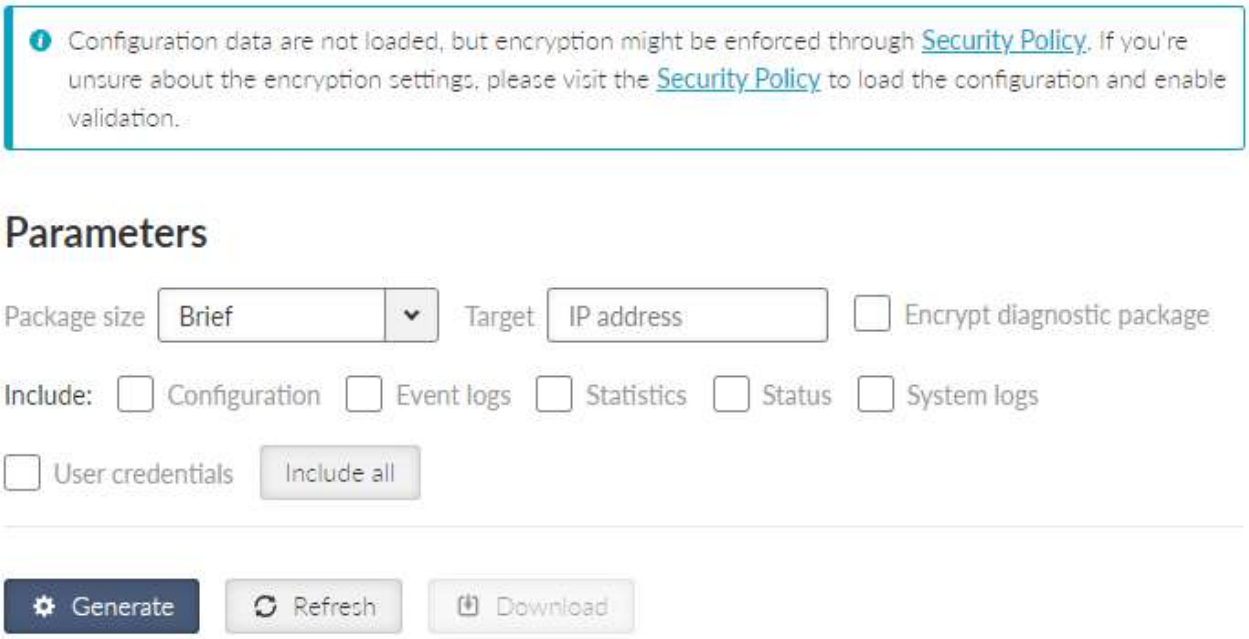


Fig. 8.16: DIAGNOSTICĂ > Informaţii > Pachet de diagnosticare

Dimensiunea pachetului

Caseta listă {Brief; Detaliat}, implicit = „Scurt”
Definește dimensiunea pachetului generat.

Ţintă

Definește stația de la care se colectează pachetul de diagnosticare.

• Pachetul de diagnosticare de la o stație locală - acest parametru rămâne gol.

• Pachetul de diagnosticare de la o stație la distanță - trebuie utilizată adresa IPv4 de destinație a stației solicitate.

Criptați pachetul de diagnosticare

Permite generarea pachetului de diagnosticare ca fișier .zip criptat. Regulile pentru complexitatea parolei sunt stabilite în meniul SETĂRI > Securitate > Politică. În același meniu, este posibil să setați criptarea să fie întotdeauna necesară.

Nota
Nu puteți utiliza Windows Explorer pentru a extrage pachetul. Trebuie să utilizați un software care poate funcționa cu fișiere criptate cu algoritmul AES-256 (de ex. WinZip, WinRAR, 7-zip, Total commander).

Include

• Configurare - configurația unității este adăugată la pachet (format json)

• Jurnalele evenimentelor - adaugă o listă de evenimente exportate în csv

○ Scurtă: Ultimele 50 de evenimente

○ Detaliat: ultimele 500 de evenimente

- Statistici - adaugă lista de statistici exportate în csv
  - ○ Intervalul statisticilor cadrelor: 30 min
  - ○ Scurtă: 10 cadre
  - ○ Detaliat: 24 de cadre
- Stare - listează starea detaliată a dispozitivelor și serviciilor din rețea
- Jurnalele de sistem - adaugă ultimele jurnalele de sistem
  - ○ Scurtă: 100 de linii curente din toate jurnalele
  - ○ Detaliat: întreg conținut de jurnal
- Acreditări utilizator - adaugă o listă de conturi de utilizator

După setarea tuturor parametrilor, faceți clic pe butonul „Generare”. Făcând clic pe butonul „Actualizați”, actualizați starea de procesare a pachetului. Odată ce pachetul este gata, acesta poate fi descărcat făcând clic pe butonul „Descărcare”. După descărcarea acestuia, pachetul este șters din unitate. Pachetul va fi șters chiar dacă descărcarea lui nu reușește și dacă descărcarea nu este inițiată, pachetul va fi șters automat după 24 de ore.

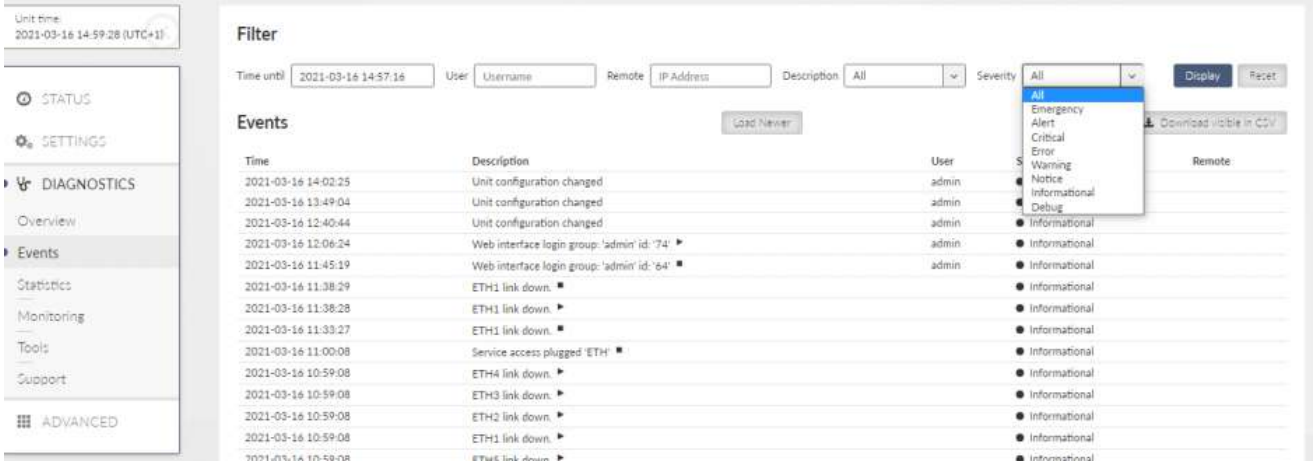
8.4. Evenimente

Acest meniu arată toate evenimentele care au loc în istoricul unității.

Pentru filtrarea evenimentelor puteți folosi instrumentul de filtrare. Când nu sunt utilizate reguli de filtrare, ultimele 30 de evenimente vor fi afișate după ce faceți clic pe butonul Afișare.

Evenimentele mai vechi ar trebui să fie afișate utilizând butonul Încărcare mai mult clic, evenimentele care apar în timpul vizualizării acestei ferestre pot fi încărcate utilizând butonul Încărcare mai nou.

Alarmele sunt afișate în roșu, avertismentele în portocaliu, avizele în negru și depanările în gri.



Este posibil să modificați gravitatea evenimentelor individuale în meniul SETĂRI > Dispozitiv > Evenimente.

Tab. 8.3: Descrierea nivelului de evenimente implicite

Severitate grup	Nivel	Severitate	Culoare cod	Descriere	Acţiune
ALARMA	0	Urgență	Roşu	Unitate defectă. Este probabil necesară reparația HW.	Înlocuiți unitatea. Contactați asistența tehnică.
	1	Alerta	Roşu	Unitatea nu funcționează. Problema HW sau SW.	Verificați unitatea. Consultați asistența tehnică.
	2	Critic	Roşu	Eroare gravă. Comunicarea nu funcționează.	Verificați imediat unitatea.
	3	Eroare	Roşu	Eroare. Comunicarea poate funcționa.	Verificați unitatea.
AVERTIZARE	4	Avertizare	Portocale	Comunicarea este OK. Acțiunea de autovindecare a continuat.	Când des, consultați asistența tehnică.
	5	Observa	Albastru	Acțiune importantă de securitate a continuat sau acțiune I/O.	Verificarea securității, verificarea stării I/O.
INFO	6	Informațional	-	Element informativ	Comportament standard
	7	Depanați	-	Informații de depanare, dacă se setează astfel.	Depanați

8.5. Statistici

Unitatea M!DGE3 monitorizează permanent diverse „canale” ale sistemului. Există mai multe tipuri de acele canale: interfețe fizice (porturi Ethernet, porturi seriale, MAIN, interfață modul suplimentar (de exemplu modul LTE) când este instalat), interfețe virtuale (de exemplu interfețe VLAN) și senzori HW (temperatura CPU, tensiunea de alimentare, ...). Valorile monitorizate sunt stocate în baza de date internă.

Pagina Statistici oferă date statistice agregate din această bază de date internă. Datele pot fi atât afișate, cât și descărcate în format CSV. Acest format de fișier este potrivit pentru a fi importat în orice program de foaie de calcul terță parte pentru analize ulterioare.

Există două opțiuni diferite de afișare a datelor statistice:

Istoric
: Contoarele statistice sunt agregate pe intervalul de timp definit. Intervalul este definit de două mărci temporale „De la” și „Către”.

Diferenţial
: Contoarele statistice sunt agregate între resetarea contorului și ora curentă (momentul în care a fost apăsat butonul Display). Resetarea este declanșată de o repornire a unității sau de butonul Resetare statistici.
Butonul de resetare a statisticilor-inițiază resetarea contoarelor statistice diferențiale. O astfel de resetare nu afectează contoarele statistice normale - adică statisticile istorice nu sunt deloc afectate de o astfel de resetare.

Lungimea datelor statistice

Datele statistice sunt stocate în baza de date internă. Există o dimensiune fixă de memorie alocată pentru datele statistice - baza de date este limitată de numărul de înregistrări. Ca urmare a acestui fapt, lungimea istoricului statisticilor - cât de vechi sunt disponibile înregistrările - depinde de configurația reală a rețelei: cu cât sunt mai multe valori monitorizate, cu atât este mai mare rata noilor valori înregistrate, cu atât istoricul disponibil este mai scurt.

Unele seturi de valori monitorizate sunt constante (porturile Ethernet și contoarele acestora) sau nu se ridică la valori ridicate (porturile COM, serverele terminale și contoarele acestora).

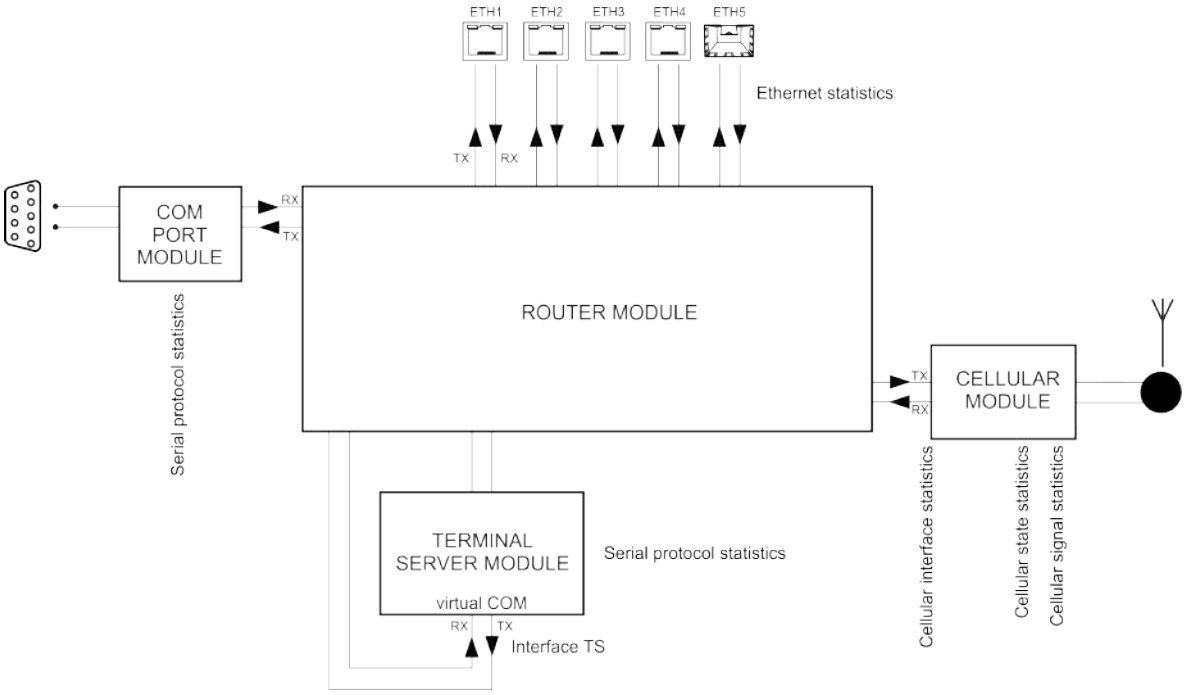


Fig. 8.17: Date statistice în contextul interfețelor unităților

8.5.1. Parametrii

Datele statistice sunt întotdeauna preluate ca agregate pentru un anumit interval de timp. Acest interval poate fi setat prin introducerea unei date și ore specifice în câmpurile „De la” și „Către” sau folosind butoanele „Ultima zi”, „Ultima oră” sau „Mai multe opțiuni” presetări rapide (de la câteva minute la câteva zile). Butonul „Setați ora curentă” setează ora curentă atât în câmpurile De la și Către pentru a ușura diagnosticarea stării curente a unității.

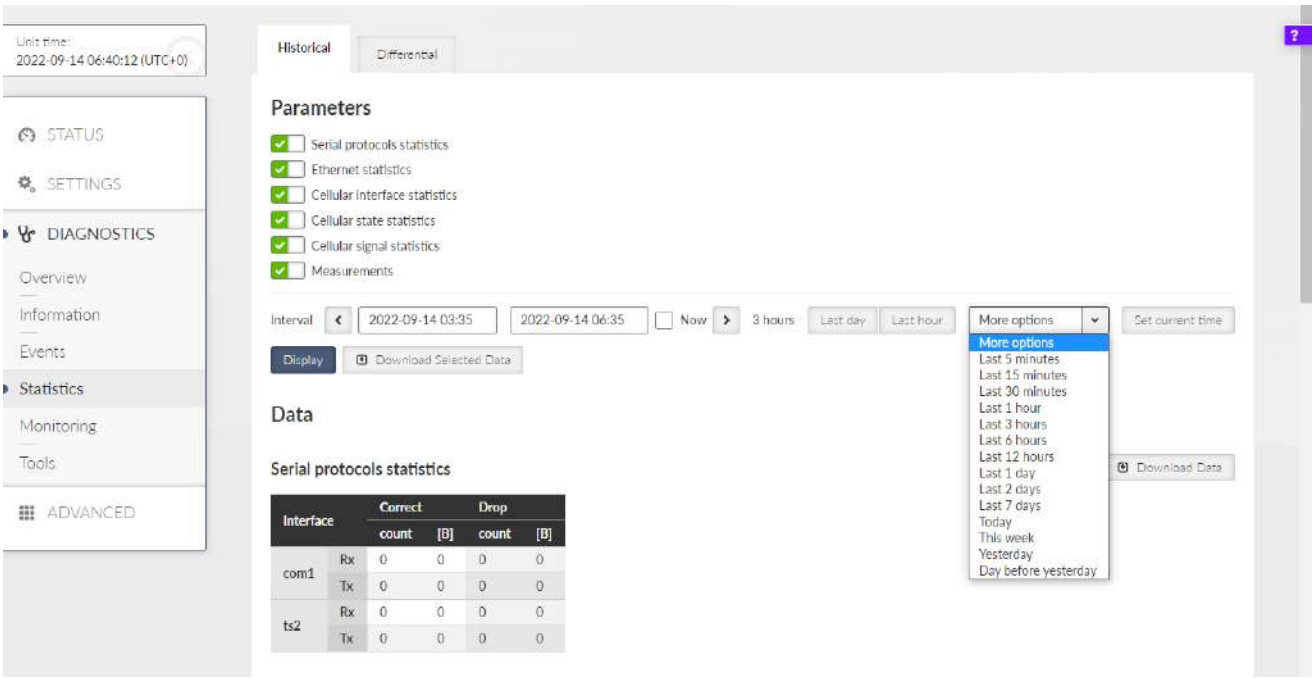
Există următoarele seturi de date statistice disponibile în unitate:

• Statistici protocoale seriale

• Statistici Ethernet

• Statistică celulară

• Măsurători



Butonul „Afișare” arată apoi datele alese de mai jos. Butonul „Descărcați datele selectate” generează fișierul CSV (codificat UTF-8) cu datele tuturor sistemelor alese și le descarcă ca fișiere fără a le afișa. Ambele butoane „Afișare” și „Descărcare...” trimit o solicitare pentru setul necesar de date statistice către unitate. Preluarea și transferul datelor durează ceva timp. Descărcarea datelor este practică atunci când utilizatorul trebuie să le proceseze într-o foaie de calcul și dorește să economisească o anumită lățime de bandă. De asemenea, se recomandă utilizarea editorului de foi de calcul precum Microsoft Excel sau Apple Numbers pentru a procesa statistici pe dispozitivele mobile, datorită experienței de utilizare mai bune oferite de aplicațiile specializate.

8.5.2. Statistica protocolului serial

Statisticile protocoalelor seriale oferă un set de date care monitorizează porturile COM și serverele terminale. Sunt afișate doar interfețele activate. Contoarele de statistici se bazează pe pachetele care intră sau ies din portul COM sau din modulul serverului Terminal. Ca rezultat, valorile „numărului” corespund mesajelor de protocol („Protocolul” selectat pe portul COM specific sau pe serverul terminal). Dacă pachetul este „lipit” din mai multe cadre, acesta este evaluat ca un singur pachet. În cazul statisticilor portului COM, rezumatul octeților „Corect” și „Renunțare” furnizează cantitatea totală de octeți de pe interfața fizică.

Direcția Rx: de la dispozitivul extern conectat (la portul COM sau ETH) la unitatea M!DGE3 (adică de la modulul portului COM sau modulul server terminal la modulul Router). Direcția Tx: de la unitatea M! DGE3 la dispozitivul extern.

Serial protocols statistics

Download Data

Interface		Correct		Drop	
		count	[B]	count	[B]
com1	Rx	0	0	0	0
	Tx	0	0	0	0
ts1	Rx	0	0	0	0
	Tx	0	0	0	0

Interfață–Numele interfeței

Corect (Rx, Tx)–Numărul de pachete recepționate/transmise corect și cantitatea de date în octeți. Acceptat de portul COM sau modulul server terminal - pe baza procesării protocolului selectat. Suma de

datele - atât pentru contoarele de corectare, cât și pentru contoarele Drop - sunt afectate numai de datele portului COM (adică anteturile IP ale cadrelor UDP create în modulul portului COM NU sunt numărate).

Drop (Rx, Tx)-Pachete primite/transmise abandonate - motiv: cadru corupt, eroare CRC, mesaj de protocol greșit, mesaj de protocol neacceptat.

8.5.3. Statistici Ethernet

Statisticile Ethernet oferă un set de date care monitorizează porturile Ethernet fizice. Sunt afișate doar interfețele activate.

Sunt tratate numai cadrele primite corect. Contoarele corespund tipurilor specifice de protocol IP.

Direcția Rx: de la portul fizic Ethernet la unitatea M!DGE3 (adică la modulul Router). Direcția Tx: de la unitatea M!DGE3 la portul fizic Ethernet.

Ethernet statistics

Download Data

Interface		UDP		TCP		ICMP		ARP		VLAN		Multicast		IPv4 other		IPv6		Other	
		count	[B]	count	[B]	count	[B]	count	[B]	count	[B]	count	[B]	count	[B]	count	[B]	count	[B]
eth1	Rx	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Tx	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth2	Rx	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Tx	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth3	Rx	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Tx	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth4	Rx	321	70354	5204	551424	0	0	2425	111550	0	0	43244	1989224	2	92	42	5141	0	0
	Tx	0	0	4386	7950627	0	0	22	616	0	0	0	0	0	0	0	0	0	0

Interfață–Numele interfeței.

UDP, TCP, ICMP, ARP, VLAN, Multicast-Numărul de pachete și cantitatea de date în octeți [B] pentru diferite tipuri de protocol - trafic IPv4. Cantitatea de date - pentru toate contoarele - este însumată pe întregul cadru Ethernet Layer 2 (adică toate anteturile IP sunt contorizate).

IPv4 altul-Traficul IPv4 nu este gestionat de contoarele anterioare

IPv6-Contor de trafic IPv6

Alte-Contor însumând cadrele care nu au fost gestionate de contoarele anterioare - de exemplu protocoalele MPLS și GOOSE.

8.5.4. Statistici celulare

Statisticile celulare sunt disponibile pentru modulul celular principal și, eventual, pentru modulul de extensie opțional, dacă este utilizat.

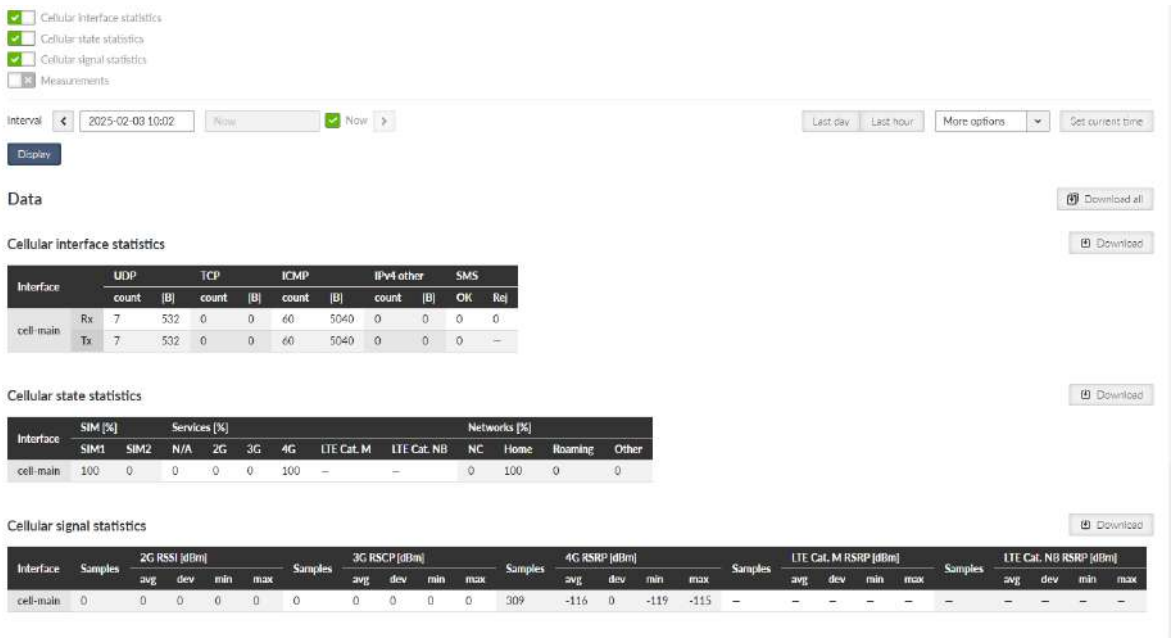


Fig. 8.18: DIAGNOSTIC>Statistici

8.5.4.1. Statisticile interfeței celulare

Statisticile interfeței celulare furnizează un set de date colectate de la interfața dintre modulul Router (motorul de rutare IP din unitate) și modulul Cellular. Acesta corespunde monitorizării Cellular - Interfață.

Direcția Tx: de la modulul Router la modulul Cellular.
Direcția Rx: de la modulul Cellular la modulul Router.

Cellular interface statistics

Interface		UDP		TCP		ICMP		IPv4 other		SMS	
		count	[B]	count	[B]	count	[B]	count	[B]	OK	Rej
cell-main	Rx	7	532	0	0	60	5040	0	0	0	0
	Tx	7	532	0	0	60	5040	0	0	0	–

Interfață

– interfața „celulă-principală” este utilizată pentru modulul celular M!DGE3 MAIN.
– Interfața „cell-ext” este utilizată pentru modulul celular de extensie opțional M!DGE3.

UDP, TCP, ICMP

- Numărul de pachete și cantitatea de date în octeți [B] pentru diferite tipuri de protocol. Cantitatea de date este însumată pe întregul cadru Ethernet Layer 2 (adică toate anteturile IP sunt contorizate).

IPv4 altul

- Pachete care nu sunt gestionate de contoarele anterioare (ex. VLAN, servicii, GRE, IPsec (ESP), ...).

SMS

Rx OK

Numărul de SMS-uri primite

SMS cu formatul corect, parola și de la numărul corect. Aici sunt incluse și comenzi invalide sau parametri greșiți (sunt recepționați corect de demon, respinși doar în sistemul de execuție a comenzilor).

Rx Rej

Numărul de SMS-uri primite respinse

SMS. În cazul dezactivării recepționării SMS-urilor de comandă, toate SMS-urile primite sunt incluse aici.

Tx OK

Numărul de SMS-uri trimise

8.5.4.2. Statistica stării celulare

Cellular state statistics

Interface	SIM [%]		Services [%]						Networks [%]			
	SIM1	SIM2	N/A	2G	3G	4G	LTE Cat. M	LTE Cat. NB	NC	Home	Roaming	Other
cell-main	100	0	0	0	0	100	–	–	0	100	0	0

Interfață

– interfața „celulă-principală” este utilizată pentru modulul celular M!DGE3 MAIN.

– Interfața „cell-ext” este utilizată pentru modulul celular de extensie opțional M!DGE3.

SIM [%]

– informații despre utilizarea cartelelor SIM individuale în timpul afișat în %.

Servicii [%]

– N/A (nu este disponibil), 2G (de ex. GPRS, EDGE), 3G (de ex. UMTS), 4G (de ex. LTE), LTE Cat. M, LTE Cat. NB utilizarea serviciilor este afișată în % din timp.

Rețele [%]

– NC (neconectat), Acasă (rețea de domiciliu), Roaming (rețea de roaming), Altele (care nu se potrivesc cu tipul de rețele anterior) afișate în % din timp.

Nota

Valorile sunt rotunjite la un număr întreg (în %).

8.5.4.3. Statistica semnalului celular

Cellular signal statistics

Download

Interface	Samples	2G RSSI [dBm]				Samples	3G RSCP [dBm]				Samples	4G RSRP [dBm]				Samples	LTE Cat. M RSRP [dBm]				Samples	LTE Cat. NB RSRP [dBm]			
		avg	dev	min	max		avg	dev	min	max		avg	dev	min	max		avg	dev	min	max		avg	dev	min	max
cell-main	0	0	0	0	0	0	0	0	0	0	309	-116	0	-119	-115	–	–	–	–	–	–	–	–	–	–

Interfață

– interfața „celulă-principală” este utilizată pentru modulul celular M!DGE3 MAIN

– Interfața „cell-ext” este utilizată pentru modulul celular de extensie opțional M!DGE3

2G RSSI / 3G RSCP / 4G RSRP/ LTE Cat. M RSRP/ LTE Cat. NB RSRP

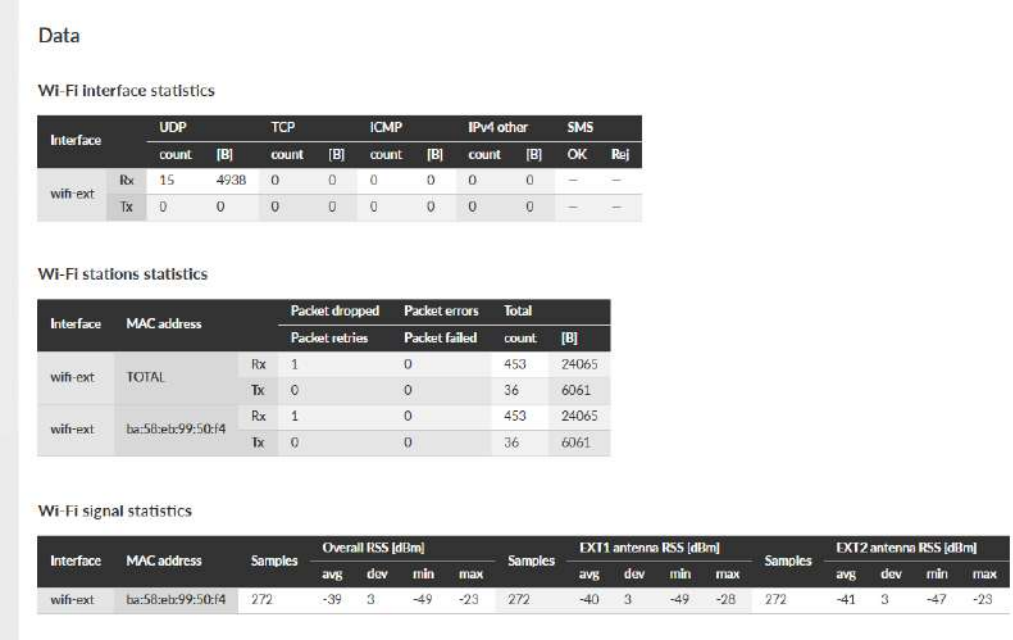
Nivelurile semnalului în dBm

Mostre

Numărul de eșantioane utilizate pentru statisticile individuale

medie / dev / min / max
Valoare medie / abatere standard / minim / maxim

8.5.5. Statistici Wi-Fi



Data

Wi-Fi interface statistics

Interface		UDP		TCP		ICMP		IPv4 other		SMS	
		count	[B]	count	[B]	count	[B]	count	[B]	OK	Rej
wifi-ext	Rx	15	4938	0	0	0	0	0	0	–	–
	Tx	0	0	0	0	0	0	0	0	–	–

Wi-Fi stations statistics

Interface	MAC address		Packet dropped / Packet retries	Packet errors / Packet failed	Total count	Total [B]
wifi-ext	TOTAL	Rx	1	0	453	24065
		Tx	0	0	36	6061
wifi-ext	ba:58:eb:99:50:f4	Rx	1	0	453	24065
		Tx	0	0	36	6061

Wi-Fi signal statistics

Interface	MAC address	Samples	Overall RSS [dBm] avg	dev	min	max	Samples	EXT1 antenna RSS [dBm] avg	dev	min	max	Samples	EXT2 antenna RSS [dBm] avg	dev	min	max
wifi-ext	ba:58:eb:99:50:f4	272	-39	3	-49	-23	272	-40	3	-49	-28	272	-41	3	-47	-23

Statisticile interfeței Wi-Fi

Interfață
Interfața „wifi-ext” este utilizată pentru modulul Wi-Fi de extensie opțional M!DGE3

UDP, TCP, ICMP
Numărul de pachete și cantitatea de date în octeți [B] pentru diferite tipuri de protocol. Cantitatea de date este însumată pe întregul cadru Ethernet Layer 2 (adică toate anteturile IP sunt contorizate)

IPv4 altul
Pachete care nu sunt gestionate de contoarele anterioare (de exemplu, VLAN, servicii, GRE, IPsec (ESP), ...)

SMS

Rx OK
Numărul de SMS-uri primite
SMS cu formatul corect, parola și de la numărul corect. Aici sunt incluse și comenzi nevalide sau parametri greșiți (sunt recepționați corect de demon, respinși doar în sistemul de execuție a comenzilor)

Rx Rej
Numărul de SMS-uri primite respinse
SMS. În cazul dezactivării recepționării SMS-urilor de comandă, toate SMS-urile primite sunt incluse aici

Tx OK
Numărul de SMS-uri trimise

Statistici stații Wi-Fi

Interfață
Interfața „wifi-ext” este utilizată pentru modulul Wi-Fi de extensie opțional M!DGE3

adresa MAC
Statistici disponibile pentru interfața ext și stațiile conectate (după adresa MAC)

Pachetul scăpat Rx
Numărul de pachete abandonate fără a specifica motivul

Erori de pachete Rx
Numărul de pachete cu eroare FCS

Număr total Rx
Numărul total de pachete primite

Total octeți Rx
Dimensiunea totală a datelor primite în octeți

Reîncercări de pachete Tx
Numărul de pachete trimise în mod repetat

Pachetul a eșuat Tx
Numărul de pachete trimise fără succes

Număr total Tx
Numărul total de pachete trimise

Total octeți Tx
Dimensiunea totală a datelor trimise în octeți

Statistici semnal Wi-Fi

adresa MAC
Statistici disponibile pentru interfața ext și stațiile conectate (după adresa MAC)

RSS general
Nivelurile semnalului în dBm

medie / dev / min / max
Valoare medie / abatere standard / minim / maxim

Mostre
Numărul de eșantioane utilizate pentru statisticile individuale

Antena EXT1 RSS
Puterea semnalului la antena EXT1 în dBm

Antena EXT2 RSS
Puterea semnalului la antena EXT2 în dBm

8.5.6. Măsurătorile

Measurements

Sensor	count	avg	min	max
CPU [°C]	8478	52.9	52.1	54.3
Modem board [°C]	8478	38.1	37.6	39.1
Radio board [°C]	0	0	0	0
Input [V]	8478	13.3	13.3	13.4

Senzor
Valori măsurate pe M!DGE3.

conta
De câte ori senzorul a măsurat valoarea dată (contor).

medie / min / max
Valoare medie / minimă / maximă.

8.6. Monitorizare

Monitorizarea este un instrument avansat de diagnosticare on-line, care permite o analiză detaliată a comunicației prin oricare dintre interfețele routerului M!DGE3. Pe lângă toate interfețele fizice (MAIN, EXT, ETH, COM, TS), unele interfețe interne dintre modulele software pot fi monitorizate atunci când este nevoie de o astfel de diagnosticare avansată.

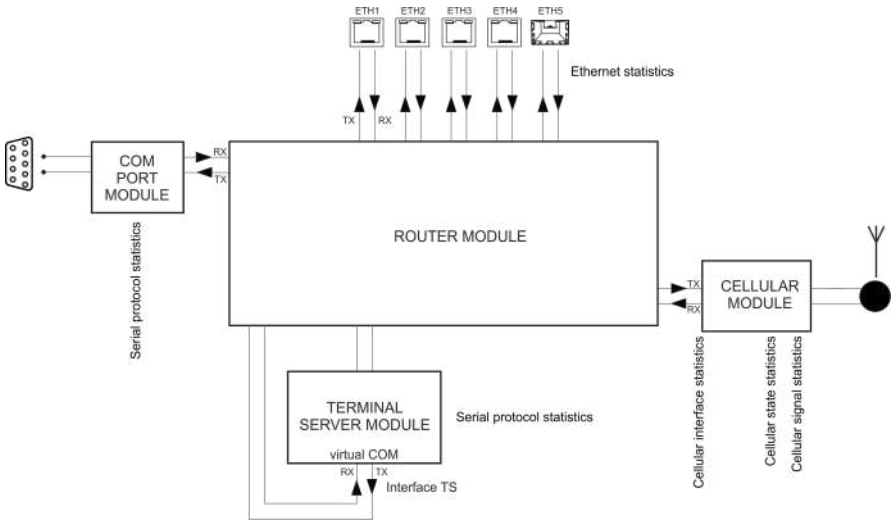
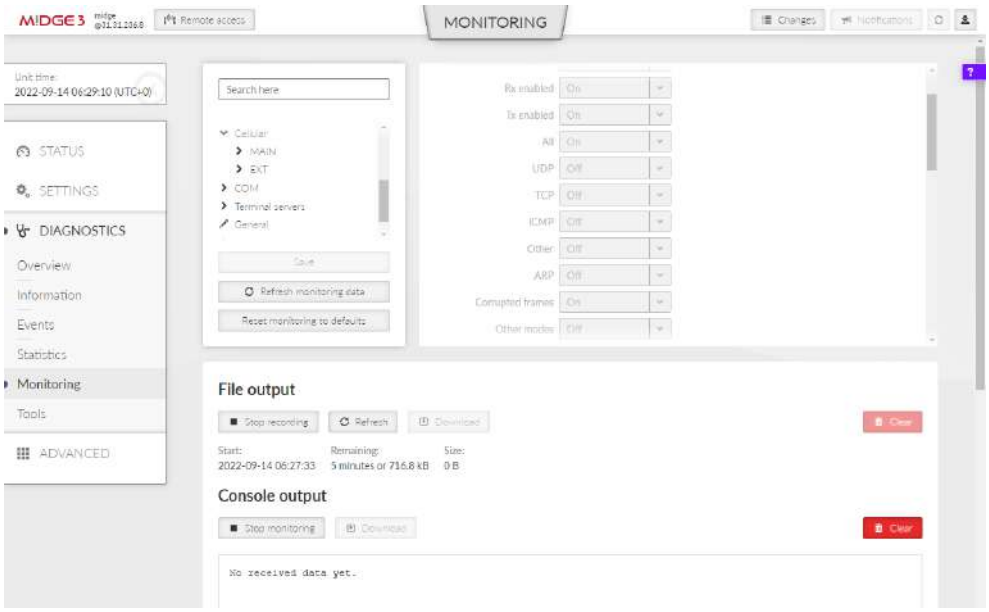


Fig. 8.19: Interfețe în contextul monitorizării unității

Monitorizarea constă din două procese independente: setările elementelor monitorizate și ieșirile. Vă rugăm să rețineți că, chiar dacă ambele ieșiri sunt oprite și unele interfețe sunt setate la Activat, monitorizarea rulează în continuare în fundal.

Ecranul de monitorizare are două părți principale - Setări și Ieșire



8.6.1. Setări

Salvabutonul - salvează noile setări ale parametrilor de monitorizare.

Actualizează datele de monitorizarebutonul - reîmprospătează meniul de setări în funcție de starea statisticilor salvate în unitate. Diferența dintre starea afișată și cea salvată poate apărea, de exemplu, atunci când starea este schimbată în filă diferită de browser.

8.6.1.1. Prezentare generală

Toate stările (Pornit/Oprit) ale interfețelor individuale sunt afișate în acest loc pentru o privire de ansamblu rapidă asupra setărilor de monitorizare.

8.6.1.2. Interfețe

Această secțiune permite setări detaliate ale anumitor parametri de monitorizare pentru toate interfețele.

Parametri comuni pentru mai multe interfețe:

Rx activat, Tx activat

Caseta listă {On; Off}, implicit = „Activat”

Un pachet este considerat unul Tx atunci când iese din modulul software respectiv (ex. Terminal Server) și invers. Când este monitorizată o interfață externă (de ex. Interfața COM), Tx înseamnă și pachete care sunt transmise de la M!DGE3 prin interfața respectivă (Rx înseamnă „primit”). Înțelegerea indicațiilor prin interfețele interne poate să nu fie atât de simplă, vă rugăm să vedeți *Fig. 8.19, „Interfețe în contextul monitorizării unității”*mai sus pentru clarificare.

Toate

Caseta listă {On; Off}, implicit = „Activat”

Ieșirea de monitorizare poate fi limitată și de tipul de protocol IP. Selectați Off pentru a putea activa/dezactiva individual ieșirea de protocol specific - vedeți următorul(i) parametru(i).

UDP / TCP / ICMP / Altele / ARP

Caseta listă {On; Off}, implicit = „Dezactivat”

Ieșirea de monitorizare a limitării protocolului IP specific.

Offset [B]

Implicit = 0

Numărul de octeți de la începutul pachetului/cadrului, care nu vor fi afișați - ieșirea de monitorizare este trunchiată de octeți „Offset” la începutul mesajului.

Lungime [B]

Implicit = 32

Numărul de octeți care urmează să fie afișați din fiecare pachet/cadru.

Exemplu: Offset=2, Length=4 înseamnă că vor fi afișați octeți de la al 3-lea octet la al 6-lea (inclusiv):

Date (HEX): 01AB**3798 A285**93CD 6B96

Ieșire de monitorizare: 3798 A285

Lățimea de bandă

Caseta listă {LOW; NORMAL; RIDICAT; NELIMITAT}, implicit = „NORMAL”

Monitorizarea limitei lățimii de bandă pentru a preveni supraîncărcarea conexiunii de gestionare între PC-ul client și unitatea M!DGE3. SCĂZUT (până la ~300 kb/s), NORMAL (până la ~800 kb/s), MARE (până la ~2 Mb/s), NELIMITAT (până la ~8 Mb/s)

Port sursă (de la) / Port sursă (către)

Portul sursă TCP/UDP să fie activat/dezactivat în ieșirea de monitorizare. Utilizați acești parametri pentru a specifica intervalul sursă de porturi <de la - la>.

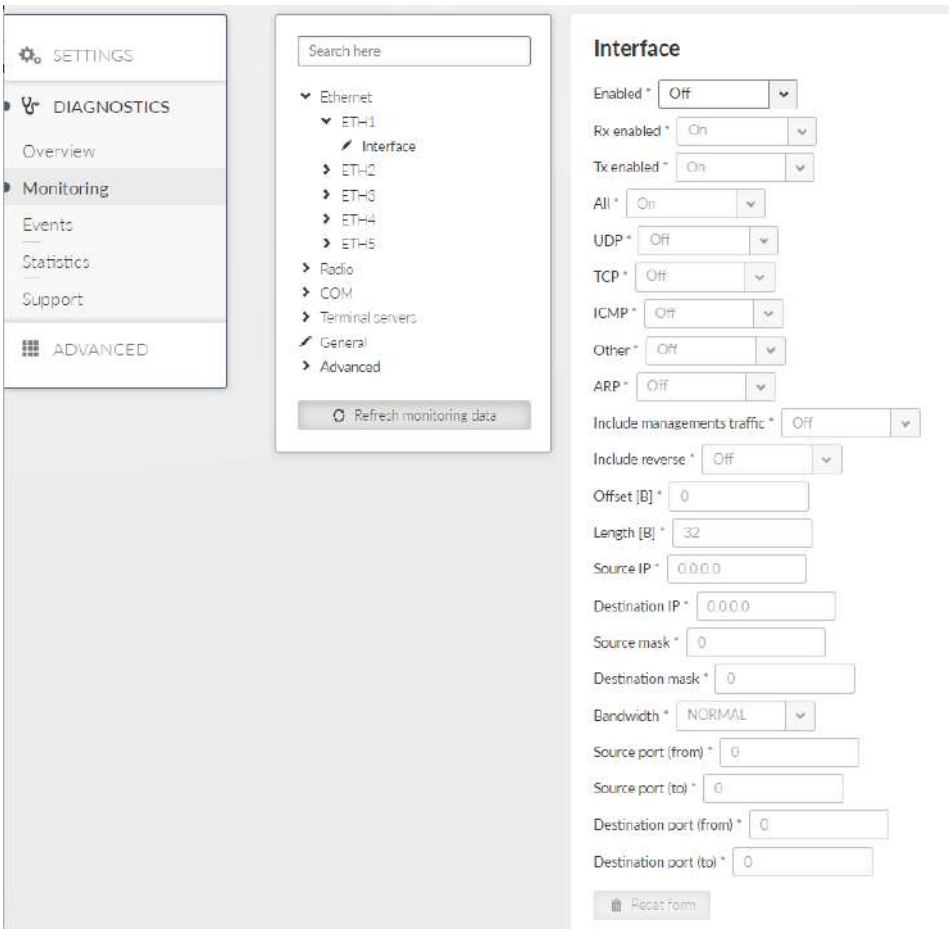
Port de destinație (de la) / Port de destinație (la)

Portul de destinație TCP/UDP să fie activat/dezactivat în ieșirea de monitorizare. Utilizați acești parametri pentru a specifica intervalul de destinație al porturilor <de la - la>.

Cadre scăpate

Caseta listă {On; Off}, implicit = „Dezactivat”

Când este activată, monitorizarea arată cadrele care sunt abandonate (de exemplu, CRC nu este valid, buffer overflow, ...).



interfețe ETH

Includeți traficul de gestionare

Caseta listă {On; Off}, implicit = „Dezactivat”

Activați/dezactivați ieșirea de monitorizare a pachetelor de management.

Includeți antetele ETH

Caseta listă {On; Off}, implicit = „Dezactivat”

Afișează (activează)/omite (dezactivează) anteturile L2 în ieșirea de monitorizare.

Includeți reversul

Caseta listă {On; Off}, implicit = „Dezactivat”

Activați/dezactivați monitorizarea traficului invers (de exemplu, răspunsul TCP la o solicitare).

IP sursă / mască, IP / mască de destinație

Ieșirea de monitorizare poate fi, de asemenea, limitată la un anumit interval de adrese - Adresa IP și masca sursă și destinație pot fi utilizate pentru a defini intervalul necesar.

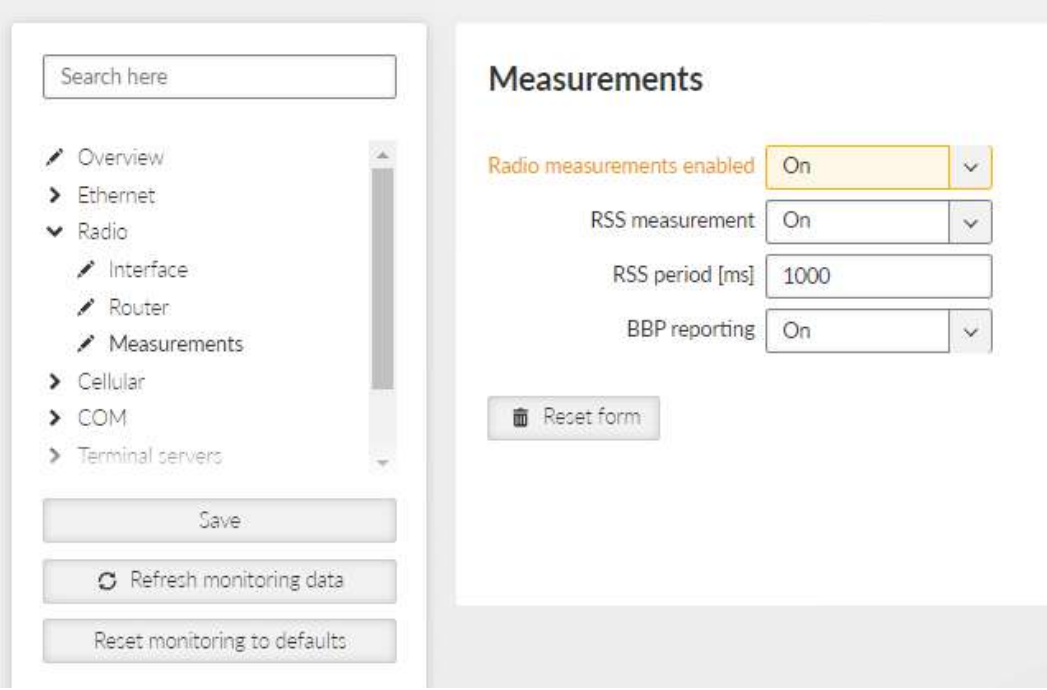


Fig. 8.20: Diagnosticare > Monitorizare > Radio > Măsurători

Monitorizarea include acum parametri suplimentari, cum ar fi tipul de modulație, codul FEC, puterea RF și temperatura pentru TX, precum și tipul de modulație, codul FEC, offset de frecvență și RSS pre-pachet pentru RX.

Monitorizează măsurătorile regulate ale variabilelor canalului radio și HW.

Măsurătorile individuale pot fi pornite și oprite sau perioada de măsurare poate fi modificată.

Puterea semnalului este măsurată la receptor la intervalul stabilit, indiferent de orice activitate în desfășurare, chiar și în timpul transmisiei.

Funcția de raportare BBP este inclusă, oferind nivelul de putere integrat măsurat pe întreaga lățime de bandă.

Interfețe celulare

Modulul celular Cinterion PLS83-W este conectat la stratul L3, astfel că cadrele capturate nu conțin antet(e) L2. Din motive de coerență, sunt adăugate următoarele valori la cadru:

• SRC mac: 0x0 0x0 0x0 0x0 0x0 0x0

• Dst mac: 0x0 0x0 0x0 0x0 0x0 0x0

• Ethertype: 0x0800

Interfață celulară MAIN activată (MAIN)

Caseta listă {On; Off}, implicit = „Dezactivat”

Interfață celulară EXT activată (EXT)

Caseta listă {On; Off}, implicit = „Dezactivat”

8.6.1.3. General

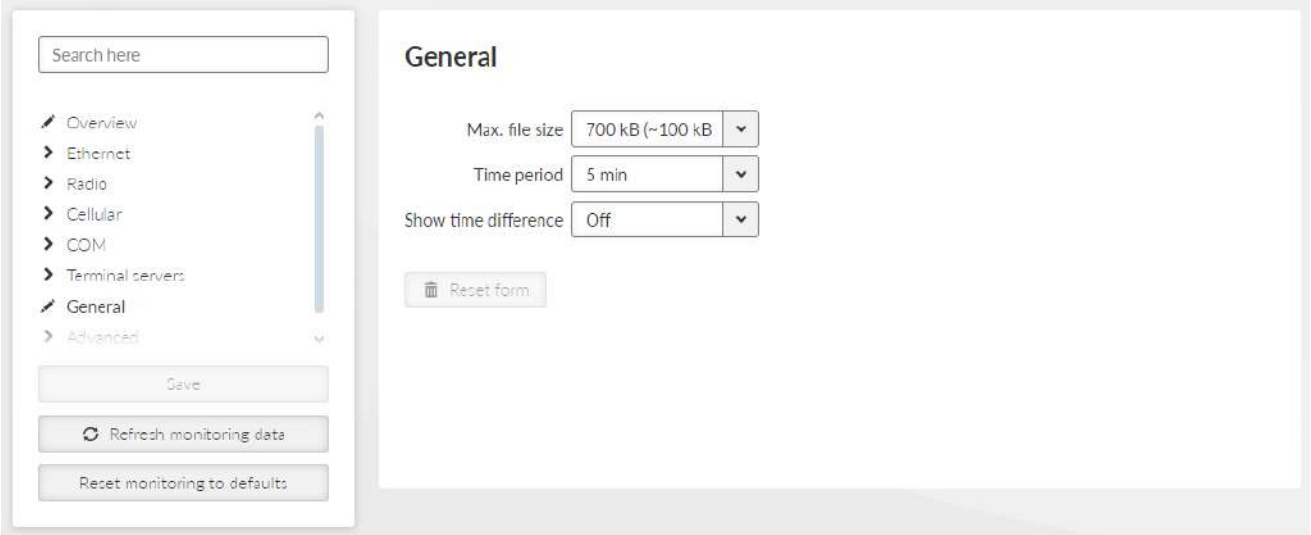


Fig. 8.21: DIAGNOSTICĂ > Monitorizare

Setările parametrilor de ieșire pentru fișierele de ieșire –**Max. dimensiunea fișieruluişiPerioada de timp**, primul parametru potrivit închide fișierul de monitorizare. Fișierul este salvat în mod comprimat, astfel încât dimensiunea comprimată necomprimată și aproximativă este afișată în caseta de listă.

Max. dimensiunea fișierului

Caseta listă {7 kB (~1 kB); 70 kB (~10 kB); 358 kB (~50 kB); 700 kB (~100 kB); 3 MB (~500 kB); 7 MB (~1 MB); max (~2 MB)}, implicit = „700 kB (~100 kB)”

Perioada de timp

Caseta listă {1 min; 2 min; 5 min; 10 min; 20 min; 30 min; 1 oră; 3 ore; 24 de ore; Off}, implicit = „5 min”

Arată diferența de timp

Caseta listă {On; Off}, implicit = „Dezactivat”

Când este activat, diferența de timp dintre pachetele ulterioare este afișată în ieșirea de monitorizare.

8.6.2. Ieșire fișier

Înregistrabutonul – începe înregistrarea în fișier. Declanșează un proces, care este setat de parametrii din capitolul de mai sus (*Secțiunea 8.6.1.3, „General”*).

Opriți înregistrareabutonul – oprește înregistrarea în fișier. Înregistrarea va fi oprită imediat, indiferent de dimensiunea și timpul înregistrării. Când butonul Înregistrare este apăsat pentru a doua oară, datele înregistrate anterior vor fi șterse.

Reîmprospătabutonul – reîmprospătează informațiile despre timpul rămas și dimensiunea datelor înregistrate (în mod necomprimat).

Descărcațibutonul – descarcă fișierul pe un computer conectat. Numele implicit conține numele unității, data și ora începerii și ziua și ora sfârșitului monitorizării. Înainte de descărcare, trebuie să opriți înregistrarea.

Clarbutonul – permite ștergerea datelor de monitorizare stocate în unitate – atât descărcate, cât și nedescărcate.

8.6.3. Ieșire de consolă

Monitorizare/Oprire monitorizarebuton

Descărcațibutonul – descarcă conținutul ieșirii consolei ca fișier

ClarButon - șterge ecranul de ieșire al consolei

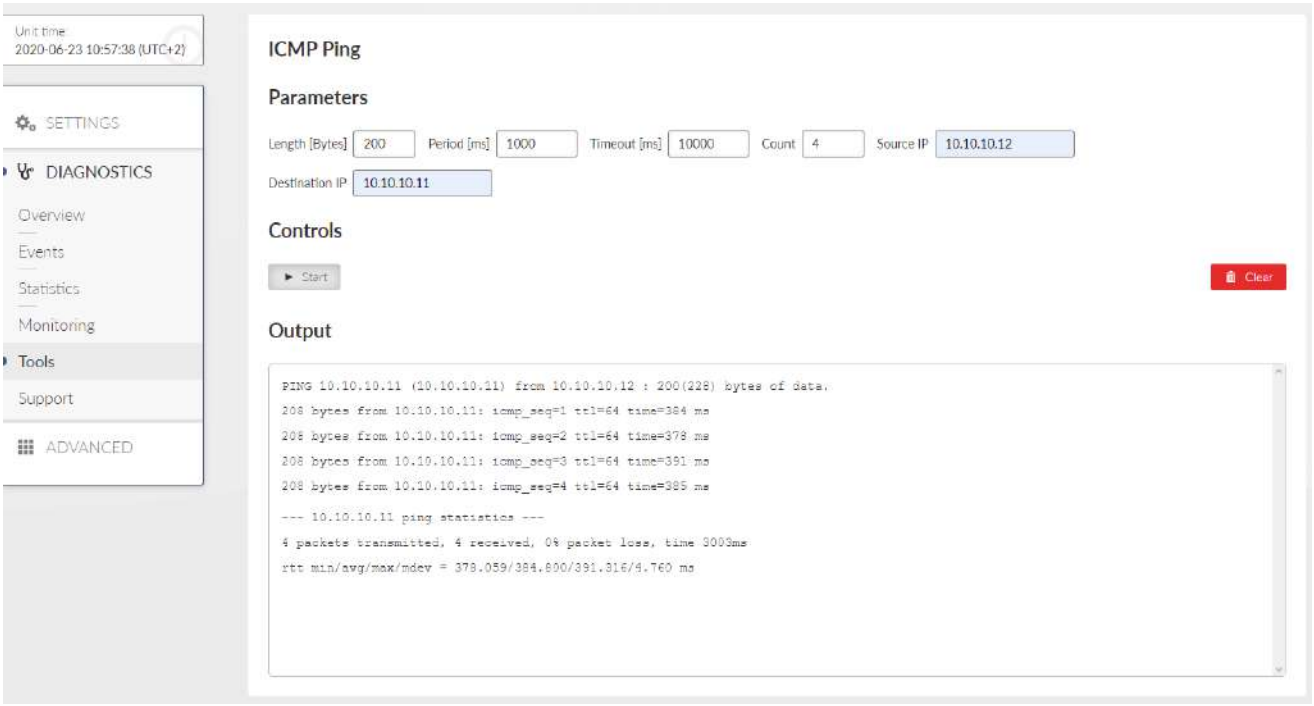
Nota

Dacă cantitatea de date monitorizate depășește limita (2,7 kB pentru monitorizare la distanță și 32 kB pentru monitorizare locală) pentru o perioadă de timp (aproximativ 1 s), unele date nu vor fi afișate în ieșirea consolei. O notă despre datele omise va fi inserată în ieșirea consolei în poziția datelor neafișate.

8.7. Instrumente

Set de instrumente de diagnosticare

8.7.1. Ping ICMP

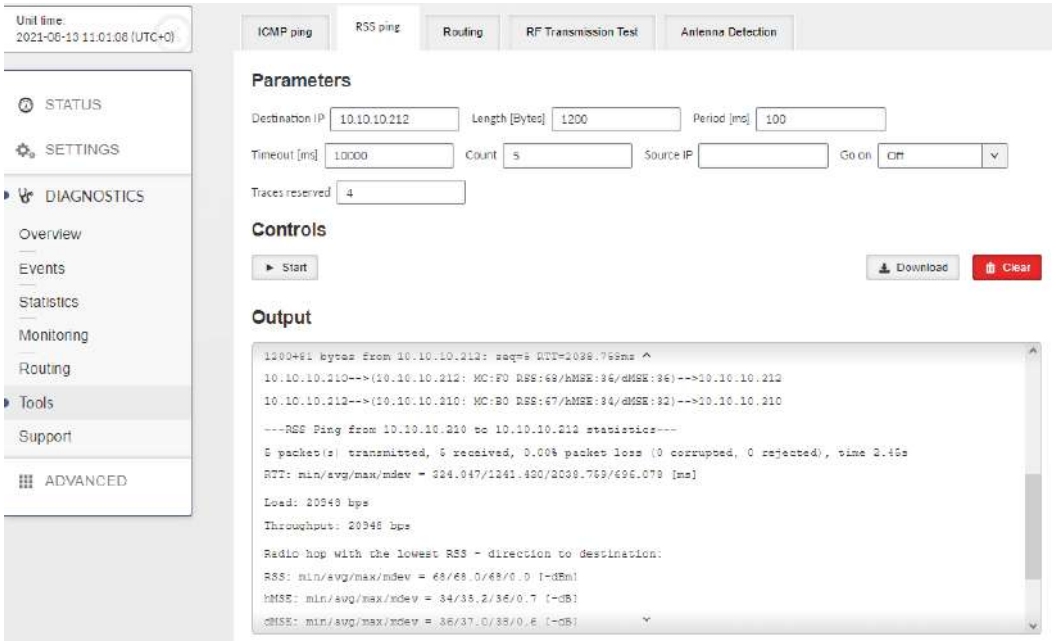


Toți parametrii utilizați de ping-ul ICMP standard sunt disponibili. Butonul Start/Oprire pornește/oprește ping-ul.

8.7.2. Ping RSS

RSS ping poate fi utilizat pentru monitorizarea canalului radio în cazul rețelelor hibride (combinație RipEX2 / M!DGE3). În astfel de rețele, ping-ul RSS vine prin întreaga rețea, dar informațiile despre RSS/MSE sunt evaluate doar pentru hopurile radio.

RSS ping este un instrument de diagnosticare pentru măsurarea performanței radio (Intensitatea semnalului radio și Eroare pătrată medie de modulare) a hopurilor radio individuale dintr-o rețea RipEX2. Sunt acceptate rețelele hibride. Formatul de ieșire de tip diferit (altul decât radio) de hop este similar cu ping ICMP.



IP de destinație

Adresa IP de destinație. Această adresă trebuie să aparțină unei unități RipEX2, deoarece ping-ul RSS poate fi inițiat doar între două unități RipEX2.

Lungime [B]

Număr {8 – 1500}, implicit = 10

Lungimea datelor utilizate de ping RSS. În cazul în care lungimea pachetului ping RSS este mai mare decât lungimea lui**Interfață radio MTU**, primul pachet ping RSS va fi pierdut și va determina scăderea lungimii pachetului la valoarea care se potrivește cu MTU-ul radio curent. Datele aleatorii sunt folosite ca sarcină utilă.

Perioada [ms]

Număr {100 – 3 600 000}, implicit = 1000

Perioada de trimitere a pachetelor ping RSS

Când perioada este setată la un număr mai scurt decât RTT real, pot apărea coliziuni (depinde de protocolul radio selectat). Pentru a ajunge la cea mai scurtă perioadă posibilă, activați**Continuă** modul.

Timeout [ms]

Număr {100 – 3 600 000}, implicit = 10000 Timp

expirat răspuns

Conta

Număr {1 – 10000}, implicit = 5

Număr de ping-uri RSS de trimis

IP sursă

Adresa IP locală a unității M!DGE3 care generează ping RSS. Câmpul necompletat (egal cu adresa 0.0.0.0) este utilizat pentru a atribui automat adresa sursă - adresa este atribuită automat conform regulilor de rutare.

Continuă

Caseta listă {On; Off}, implicit = „Dezactivat”
Treci pe modul. Când este activat, ping-urile RSS sunt trimise imediat după primirea răspunsului RSS ping (parametrul Perioad este ignorat).

Urme rezervate

Ping-ul RSS conține și date despre rută (RSS, MSE), acest parametru permite setarea numărului de hop-uri radio în cadrul rețelei de măsurat. Saltul radio se măsoară în ambele direcții, astfel încât numărul trebuie să fie mai mare decât numărul de sărituri în rută înmulțit cu 2 (de exemplu: legătura formată din 2 sărituri radio necesită 5 urme pentru a fi rezervată).

Ieșire:

- **MC**–Codifică modularea și codificarea - vezi tabelul de transcriere:

Tab. 8.4: Tabel de translație pentru Ratele de modulare și FEC

	Modulare	**FEC**
00	2CPFSK	FEC oprit
01		FEC 3/4
10	4CPFSK	FEC oprit
11		FEC 3/4
80	DPSK	FEC oprit
81		FEC 3/4
90	pi/4 DQPSK	FEC oprit
91		FEC 3/4
A0	D8PSK	FEC oprit
A1		FEC 3/4
B0	16DEQAM	FEC oprit
B1		FEC 3/4
C0	64QAM	FEC oprit
C1		FEC 3/4
D0		FEC 5/6
D1		FEC 2/3
E0	256QAM	FEC oprit
E1		FEC 3/4
F0		FEC 5/6
F1		FEC 2/3

- **RSS**–Puterea semnalului radio [dBm] - măsurată în recepția antetului
- **hMSE**–Eroare pătrată medie a modulării antetului phy [dB] - măsurată în recepția antetului
- **dMSE**–Eroare medie pătratică de modulare a datelor [dB] - măsurată în recepția părții de date cadru

8.7.3. Dirijare

Instrumentul de rutare oferă următoarele informații de rutare a hopului pentru adresa IP dată.

IP de destinație
Adresa IP examinată.

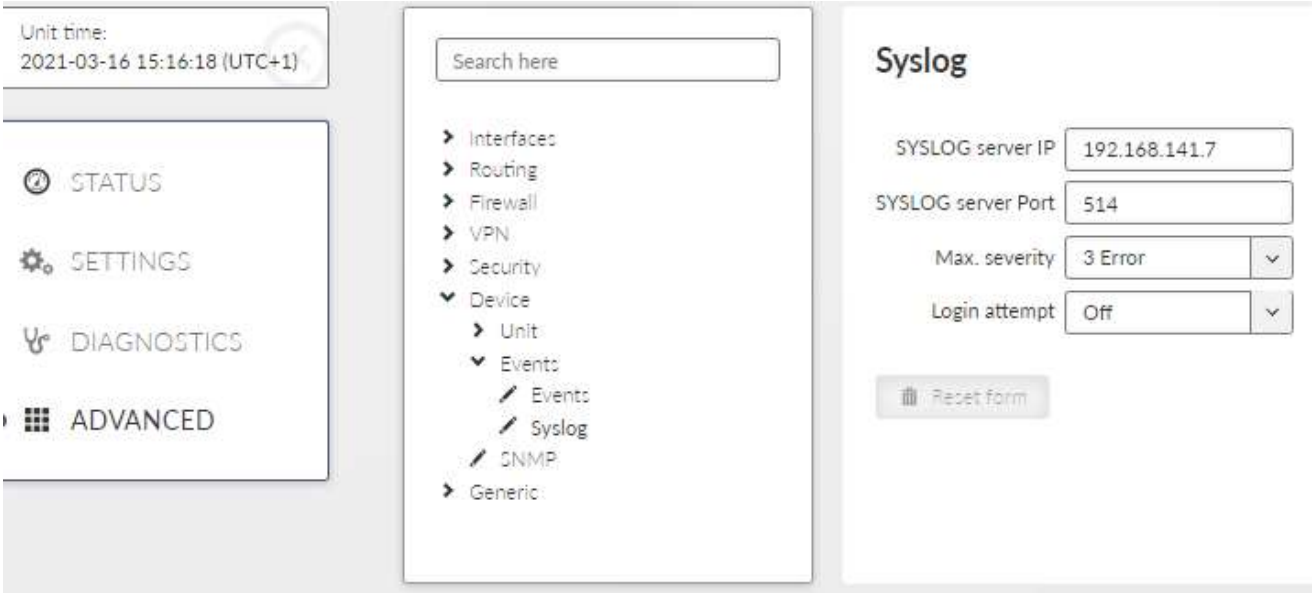
Ieșire
Secțiunea de ieșire oferă următoarele detalii:

- Adresă examinată (exemplu: 8.8.8.8)
- Următorul hop (gateway) adresă (exemplu: prin 192.168.141.254)
- Interfața hop următor (exemplu: dev if_bridge)
- Adresă sursă pachet de ieșire (exemplu: src 192.18.141.210)

8.7.4. Sistem

Butonul de repornire
Efectuează repornirea la rece a unității (echivalent ciclu de alimentare).

8.8. Syslog



IP server SYSLOG

Adresa IP a serverului Syslog la distanță către care vor fi trimise jurnalele cu o severitate mai mare decât severitatea setată în Max. severitate

Port server SYSLOG

Portul utilizat de serverul Syslog

Max. severitate

Caseta listă {Off; 0 Urgență; 1 Alertă; 2 Critic; 3 Error}, default= ”Off”

Off - dezactivează funcționalitatea SYSLOG

Doar evenimentele cu severitatea setată (și mai mare) vor fi trimise la serverul Syslog. Pot fi setate severități pentru evenimente individuale*Secțiunea 7.6.3, „Evenimente”*.

Încercarea de conectare

Caseta listă {Off; Web}, implicit = „Dezactivat”

Comută dacă încercările de conectare (atât reușite, cât și nereușite) vor fi trimise către serverul SYSLOG.

9. Parametri tehnici

Electric	**M!DGE3**	**M!DGE3e**
Putere primară	10 până la 50 VDC, GND negativ	
Rx	4,8 W / 24 V, *vezi detalii*	
Tx	7,8 W / 24 V, *vezi detalii*	
Modul de repaus	0,01 W	
Interfețe		
Sloturi SIM	2× Micro SIM + 1× eSIM1)	2× Micro SIM
Ethernet	10/100/1000 Base-T, Auto MDX, 4× RJ45 în punte sau direcționat	10/100/1000 Base-T, 2× RJ45 Auto MDX, în punte sau dirijate
SFP	10/100/1000Base-T sau 1× SFP 1000Base-SX sau 1000Base-LX	Fără SFP
Serial	1× RS232/RS485 Terminale configurabile SW 2× RS232 (extensiune mPCIe 1× placă RJ45) 600 b/s – 1 Mb/s	1× terminale RS232/RS485 SW configurabile 600 b/s – 1 Mb/s
USB	USB 3.0/gazdă A	
Intrări/Ieșiri	1× intrare alarmă HW, 1× ieşire alarmă HW, 1× intrare Sleep - Conector de alimentare RJ45	
	2× DI, 2× DO, 1× difDI (când nu se utilizează mPCIe-COMS)	Nu
Antenă	2× SMA femelă – diversitate receptor (2×2 MIMO)	
Expansiuni opționale	1× mPCIe: modul celular („W” sau „M” sau „O”) sau 2× RS232 sau GPS	Nu
1) eSIM numai pentru 5G		

Interfață celulară	
5G2)	
Disponibil pe placa de bază M!DGE3	
Benzi de frecvență pentru modulul de extensie „Q” Cellular	5G (SA și NSA) n1, n2, n3, n5, n7, n8, n12, n13, n14, n18, n20, n25, n26, n28, n30, n38, n40, n41, n48, n53, n66, n70, n71, n75, n76, n77, n77, n77, n77
	4G LTE Advanced-Pro B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B34, B38, B39, B40, B41, B43, B42, B44, B41, B41, B42, B41, B42, B41, B44 B75, B76
	3G UMTS/HSPA+ B1, B2, B4, B5, B8
	Cinterion MV32-WA ID FCC QIPMV32-WA
Specificații pentru modulul „Q” Cellular	4 × antenă SMA
	5G NR 3GPP Versiunea 16 FR1 (Sub 6G) Debit de date (max. @ 5G FR1 SA) DL 3,5 Gb/s , UL 900 Mb/s DL 4×4 MIMO / UL 2×2 MIMO
	4G LTE 3GPP Versiunea 15 Evoluție pe termen lung (LTE) UE Cat 19 (DL 1,6 Gb/s, UL 211 Mb/s) 7× DL CA, 2× UL CA (intra-bandă), 5× DL CA+ 4 × 4 MIMO (până la UE Cat 20)
	3G UMTS/HSDPA/HSUPA 3GPP Versiunea 8 DC-HSPA+ – DL Cat 24 (42 Mb/s) / UL Cat 6 (5,76 Mb/s) HSUPA – UL 5,76 Mb/s
4G	
Disponibil pe placa de bază M!DGE3, M!DGE3e2)sau placa de extensie mPCIe	

Benzi de frecvență pentru modulul de extensie „W” Cellular	4G LTE (de asemenea, 5G NSA) Banda 1 (2100 MHz), Banda 2 (1900 MHz), Banda 3 (1800 MHz), Banda 4 (2100 MHz), Banda 5 (850 MHz), Banda 7 (2600 MHz), Banda 8 (900 MHz), Banda 12 (700 MHz), Banda 13 (700 MHz)**, Banda 18 (850 MHz), Banda 18 (850 MHz), Banda 18 (850 MHz), Banda 18 (85 MHz) (800 MHz), Banda 26 (850 MHz), Banda 28 (700 MHz), Banda 38 (2600 MHz), Banda 40 (2300 MHz), Banda 41 (2500 MHz), Banda 66 (2100 MHz) * * O problemă de sensibilitate va apărea în GNSS la transmiterea în banda 13	
	3G UMTS/HSDPA/HSUPA Banda 1 (2100 MHz), Banda 2 (1900 MHz), Banda 3 (1800 MHz), Banda 4 (2100 MHz), Banda 5 (850 MHz), Banda 6 (850 MHz), Banda 8 (900 MHz), Banda 19 (850 MHz)	
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz	
	Cinterion PLS83-W	ID FCC QIPPLS83-W TAC 35107264
Specificații pentru modulul „W” Cellular	ANT1, ANT2 - diversitate spațială	2 × antenă SMA
	4G LTE (și 5G NSA) 3GPP Versiunea 10 Evoluție pe termen lung (LTE) Uni evoluat. Acces radio terestre (E-UTRA) Duplex cu diviziune de frecvență (FDD) DL Multi-Input Multi-Output (MIMO) 2×2	
	3G UMTS/HSDPA/HSUPA 3GPP Versiunea 7 Acces de pachete HS cu două celule (DC-HSPA+) Acces radio terestre UMTS (UTRA) Duplex cu diviziune în frecvență (FDD) Diversitate DL Rx	
	2G GSM/GPRS/EDGE 3GPP Versiunea 4 Rată de date îmbunătățită GSM Evolution (EDGE) Acces radio GSM EGPRS (GERA) Time Division Multiple Access (TDMA) DL Advanced Rx Performance Faza 1	
	Rate de date de până la 150 Mb/s pe legătură în jos / 50 Mb/s pe legătura în sus	
LTE 450 NB IoT		
Disponibil pe placa de bază M!DGE3, M!DGE3e2)sau placa de extensie mPCIe		
Benzi de frecvență pentru modulul de extensie „M” Cellular	LTE Cat M1: Banda 1 (2100 MHz), Banda 3 (1800 MHz), Banda 8 (900 MHz), Banda 20 (800 MHz), Banda 28 (700 MHz), Banda 31 (450 MHz), Banda 72 (450 MHz)	
	LTE Cat NB1/2: Banda 1 (2100 MHz), Banda 3 (1800 MHz), Banda 8 (900 MHz), Banda 20 (800 MHz), Banda 28 (700 MHz), Banda 31 (450 MHz), Banda 72 (450 MHz)	
	Cinterion TX62-WC	

Benzi de frecvență pentru modulul de extensie „O” Cellular	LTE Cat M1: Banda 1 (2100 MHz), Banda 2 (1900 MHz), Banda 3 (1800 MHz), Banda 4 (AWS-1), Banda 5 (850 MHz), Banda 8 (900 MHz), Banda 12 (700 MHz), Banda 13 (700 MHz), Banda 18 (800 MHz), Banda 18 (800 MHz), Banda 18 (800 MHz), Banda 180 MHz, Banda 19080 MHz (1900 MHz), Banda 26 (800 MHz), Banda 27 (800 MHz), Banda 28 (700 MHz), Banda 66 (AWS-3), Banda 85 (700 MHz)	
	LTE Cat NB1/2: Banda 1 (2100 MHz), Banda 2 (1900 MHz), Banda 3 (1800 MHz), Banda 4 (AWS-1), Banda 5 (850 MHz), Banda 8 (900 MHz), Banda 12 (700 MHz), Banda 13 (700 MHz), Banda 18 (800 MHz), Banda 08 MHz (Banda 0 MHz), Banda 08 MHz 25 (1900 MHz), Banda 26 (800 MHz), Banda 28 (700 MHz), Banda 66 (AWS-3), Banda 71 (600 MHz), Banda 85 (700 MHz)	
	Cinterion TX62-WB	FCC QIPTX62-WB
Specificații pentru modulul de extensie „M” și „O” Cellular	ANT1	1 × antenă SMA
	LTE Cat M1 - DL: max. 300 kb/s, UL: max. 1,1 Mb/s LTE Cat NB 1 - DL: max. 27 kb/s, UL: max. 63 kb/s LTE Cat NB 2 - DL: max. 124 kb/s, UL: max. 158 kb/s	
	3GPP Versiunea 14	
	Half Duplex - Duplex cu diviziunea în frecvență (HD-FDD)	
2) În așteptare		

LED-uri de indicare	
Panou LED	5 LED-uri de stare tricolore (SYS, WAN, EXT, VPN, COM)
ETH	4× RJ45 (LED-uri de legătură și activitate), 1× SFP (LED-uri de stare)
de mediu	
Cod IP (protecție la intrare)	IP40, numai pentru uz interior
MTBF (Timp mediu între eșecuri)	> 900 000 de ore (> 100 de ani)
Durata de viață a sistemului	> = 15 ani
Temperatura de functionare	−40 la +70 °C (de la −40 la +158 °F)
Umiditatea de funcționare	5 până la 95 % fără condensare
Depozitare	− 40 până la +85 °C (-40 până la +185 °F) / 5 până la 95 % fără condensare
Mecanic	
Carcasa	Metal
Dimensiuni	Înălțime×L×D: 132×43×110 mm (5,20×1,69×4,33 inchi)
Greutate	0,50 kg (1,1 lbs)
Montare	Sină DIN, opțional: suport plat sau colț
SW	
Protocoale utilizator pe COM	DNP3, DF1, IEC101, Modbus RTU, PR2000, RDS, Siemens 3964(R), COMLI, SAIA S-bus, Mars-A, PPP, UNI, Async Link
Protocoale utilizator pe Ethernet	Modbus TCP, IEC104, DNP3 TCP, Comli TCP, server terminal...
Convertoare seriale la IP	DNP3 / DNP3 TCP, Modbus RTU / Modbus TCP
Securitate	
management	HTTPS (interfață web sau interfață de programare a aplicațiilor)
Controlul accesului bazat pe rol (RBAC)	4 niveluri (Guest, Tech, SecTech, Admin)
Acces de gestionare WiFi (opțional)	Securizat WPA2-PSK
VPN	IPsec, OpenVPN, GRE
VLAN	IEEE 802.1Q (etichetare)
protocol AAA	RAZĂ
Firewall	Layer 2 - MAC, Layer 3 - IP, Layer 4 - TCP/UDP
FW	Semnat digital
Tamper HW	Dovezi de deschidere a cazului (N/A pentru M!DGE3e)

Diagnostic și management	
Testarea linkurilor	Ping ICMP
Informații despre stare	Interfețe cu utilizatorul
Statistici	Statistici istorice și diferențiale pentru pachetele Rx / Tx pe toate interfețele utilizator (de ex. ETH 1-5, COM 1-3, TS 1-5)
Istoricul statisticilor	Câteva săptămâni
Jurnalul evenimentelor	Evenimente filtrate în funcție de timp, gravitate, utilizator, adresă IP de la distanță și tip de eveniment
SNMP	SNMPv1, SNMPv2c, SNMPv3 Capcană / Informați generarea notificărilor conform setărilor
NTP	Client/Server
Monitorizare	Analiza în timp real a tuturor interfețelor (de ex. ETH 1-5, COM 1-3, TS 1-5) și interfețelor interne între modulele software, *vezi detalii*

Standarde	
CE, FCC	*ROȘU, RoHS, DEEE*
Spectru	ETSI EN 301 511 V12.5.1 ETSI EN 301 908-01 V13.1.1 ETSI EN 301 908-02 V11.1.2 ETSI EN 301 908-13 V13.1.1 ETSI EN 303 413 V1.1.
EMC (compatibilitate electromagnetică)	ETSI EN 301 489-1 V2.2.3 ETSI EN 301 489-5 V3.2.1 ETSI EN 301 489-19 V2.1.0 ETSI EN 301 489-52 V1.1.0
Siguranța produsului	EN 62368-1:2014 + A11:2017
Siguranța sănătății RF	EN 62311:2008
Mediul substațiilor electrice	IEEE 1613:2009 IEEE 1613.1:2013 EN 61850-3:2014
de mediu	EN 61850-3: 2014
Vibrații și șoc	EN 60068-2-6:2008 ETS 300 019-2-3:1994, Clasa 3.4 EN 61850-3:2014
Calificare seismică	EN 60068-2-27:2010
Evaluare IP	EN 60529:1993 + A1:2001 + A2:2014

Interfețe opționale	
Modul de extensie „G” GPS (GNSS)	Antenă activă 3,3 VDC SMA mamă (EXT1 în partea de jos)
	Motor u-blox M8 cu 72 de canale GPS/QZSS L1 C/A, GLONASS L10F, BeiDou B1I, Galileo E1B/C, SBAS L1 C/A: WAAS, EGNOS, MSAS, GAGAN
Modulul de extensie „C” porturi COM	COM2: RS232 - 5 pini (RxD, TxD, GND, RTS, CTS) 600 b/s până la 2 Mb/s COM3: RS232 -3 pini (RxD, TxD, GND) 2,4 kb/s până la 921,6 kb/s RJ45 (DI/DO pe panoul frontal)
Modulul de extensie „W”, „M”, „O” Cellular	vedea*Interfață celulară*
Modul de extensie „F” Wifi	IEEE 802.11a/b/g/n/ac 2x2 MIMO 20 MHz / 40 MHz pentru 2,4 GHz 20 MHz / 40 MHz / 80 MHz pentru 5 GHz WPA/WPA2 PSK WPA3-SAE Criptare hardware AES/TKIP Putere de ieșire de până la 16 dBm Realtek RTL8822CE

Lista cablurilor conectate			
Intrare / Ieșire	**Lungimea specificată pentru EN 61850-3**	**Ecrat / Neecranat**	**Recomandat tip cablu**
Alimentare DC 10 – 50 V	La nevoie	N	V03VH-H 2×0,5
GPIO (intrare de repaus, intrare de alarmă HW, ieșire de alarmă HW)	La nevoie	S	LiYCY 6×0,14
Conexiune antenă	La nevoie	S	coaxiale
COM (RS232/485)	După cum este necesar, de obicei până la 15 m (RS232) sau până la 400 m (RS485)	S	LiYCY 4×0,14
EXT1	După cum este necesar (pentru celular) Max. 2 m (antenă GPS)	S	coaxiale
EXT2	După cum este necesar (pentru celular) Max. 2 m (ieșire impuls de timp)	S	coaxiale
ETH (4 porturi)	După cum este necesar, de obicei până la 100 m	S	STP CAT 5e
Ethernet optic	După nevoie, de obicei până la 2 km	N / A	Fibră optică
USB	Max. 2 m	S	USB3
DI / DO	La nevoie	S	STP CAT 5e

Rx Consumul de energie @24Vdc	
Rx	4,8 W
LTE Tx	+ 3,0 W
+ Ethernet	+ 0,1 W @ 10BaseT + 0,12 W @ 100BaseT + 0,5 W @ 1000BaseT per interfață Eth cu echipamentele conectate
+ primul COM	+ 0,2 W
+ GNSS	+ 0,15 W
+ 2ndCOM	+ 0,1 W
+ 2ndLTE	Rx +0,3, Tx +3,0 W
+ Modul SFP tip.	+ 1,0 W
+	+ 3,0 W max.

10. Siguranță, reglementări, garanție

10.1. Instrucțiuni de siguranță

Routerul wireless M!DGE3 trebuie utilizat în conformitate cu toate legile internaționale și naționale aplicabile și cu orice restricții speciale care reglementează utilizarea modulului de comunicație în aplicații și medii prescrise.

Pentru a preveni eventualele vătămări ale sănătății și deteriorarea aparatelor și pentru a vă asigura că au fost respectate toate prevederile relevante, utilizați numai accesoriile originale. Modificările neautorizate sau utilizarea accesoriilor care nu au fost aprobate pot duce la încetarea valabilității garanției.

Routerele celulare M!DGE3 nu trebuie deschise. Este permisă doar înlocuirea cartelei SIM.

Tensiunea la toți conectorii modulului de comunicație este limitată la SELV (Safety Extra Low Voltage) și nu trebuie depășită.

Pentru utilizare cu surse de alimentare certificate (CSA sau echivalente), care trebuie să aibă o ieșire limitată și circuit SELV. M!DGE3 este proiectat numai pentru utilizare în interior. Nu expuneți modulul de comunicație la condiții ambientale extreme. Protejați modulul de comunicație împotriva prafului, umidității și temperaturii ridicate.

Reamintim utilizatorilor obligația de a respecta restricțiile privind utilizarea dispozitivelor radio la benzinării, în uzinele chimice sau în derularea lucrărilor de detonare în care se folosesc explozivi. Opriți modulul de comunicare când călătoriți cu avionul.

Când utilizați modulul de comunicație în imediata apropiere a dispozitivelor medicale personale, cum ar fi stimulatoare cardiace sau aparate auditive, trebuie să procedați cu precauție sporită.

Dacă se află în apropierea televizorului pentru a preveni posibile răni ale aparatelor medicale, receptoarelor radio și computerelor personale, routerul wireless M!DGE3 poate provoca interferențe.

Se recomandă să creați o copie sau o copie de rezervă aproximativă a tuturor setărilor importante care sunt stocate în memoria dispozitivului.

Nu trebuie să lucrați la instalarea antenei în timpul unui fulger.

Păstrați întotdeauna o distanță mai mare de 40 cm față de antenă pentru a vă menține expunerea la câmpurile electromagnetice sub limitele legale. Această distanță se aplică antenelor Lambda/4 și Lambda/2. Distanțele mai mari se aplică pentru antenele cu câștig mai mare.

Respectați instrucțiunile documentate în acest manual de utilizare.

10.2. Temperatură ridicată

Dacă M!DGE3 este utilizat într-un mediu în care temperatura ambientală depășește 55 °C, M!DGE3 trebuie instalat într-o locație cu acces restricționat pentru a preveni contactul uman cu radiatorul carcasei.

10.3. Eliminarea bateriilor

Eliminarea bateriei - Acest produs poate conține o baterie (de exemplu, CRC1225, 3V, 48 mAh). Bateriile trebuie aruncate în mod corespunzător și nu pot fi aruncate ca deșeuri municipale nesortate. Bateriile sunt marcate cu un simbol, care poate include litere pentru a indica cadmiul (Cd), plumbul (Pb) sau mercurul (Hg). Pentru o reciclare adecvată, returnați bateria furnizorului dumneavoastră sau la un punct de colectare desemnat.

10.4. Instrucțiuni pentru funcționarea în siguranță a echipamentului

Vă rugăm să citiți cu atenție aceste instrucțiuni de siguranță înainte de a utiliza produsul:

• Echipamentul radio poate fi operat numai pe frecvenţele stipulate de organismul autorizat de administraţia de operare radio din ţara respectivă şi nu poate depăşi puterea maximă de ieşire admisă. RACOM nu este responsabil pentru produsele utilizate într-un mod neautorizat.

• Echipamentul menționat în acest manual de utilizare poate fi utilizat numai în conformitate cu instrucțiunile conținute în acest manual. Funcționarea fără erori și în siguranță a acestui echipament este garantată numai dacă acest echipament este transportat, depozitat, operat și controlat în mod corespunzător. Același lucru este valabil și pentru întreținerea echipamentelor.

• Pentru a preveni deteriorarea routerului celular și a altor echipamente terminale, alimentarea trebuie să fie întotdeauna deconectată la conectarea sau deconectarea cablului la interfața de date a routerului celular. Este necesar să vă asigurați că echipamentul conectat a fost împământat la același potențial.

• Numai producătorul menționat mai jos are dreptul să repare orice dispozitiv.

10.5. Licență SW

Condițiile de utilizare a acestui produs software respectă licența menționată mai jos. Programul răspândit prin această licență a fost eliberat cu scopul de a fi util, dar fără nicio garanție specifică. Autorul sau o altă companie sau persoană nu este responsabilă pentru daune secundare, accidentale sau conexe rezultate din aplicarea acestui produs în nicio circumstanță.

Licență software deschisă RACOM

Versiunea 1.0, noiembrie 2009

Copyright (c) 2001, RACOM sro, Mírová 1283, Nové Město na Moravě, 592 31

Toată lumea poate copia și răspândi copii cuvânt cu cuvânt ale acestei licențe, dar orice modificare nu este permisă.

Programul (versiune binară) este disponibil gratuit la contactele listate pe https://www.racom.eu. Acest produs conține software open source sau alt software care provine de la terțe părți care fac obiectul Licenței Publice Generale GNU (GPL), Bibliotecii GNU/Licenței Publice Generale Inferioare (LGPL) și/sau altor licențe de autor, excluderii declarațiilor de responsabilitate și notificărilor. Termenii exacti de GPL, LGPL și unii

licențe suplimentare sunt menționate în pachetele de cod sursă (de obicei fișierele COPYING sau LICENSE). Puteți obține copii aplicabile, care pot fi citite de mașină, ale codului sursă ale acestui software sub licențe GPL sau LGPL, de la contactele enumerate pe https://www.racom.eu. Acest produs include, de asemenea, software dezvoltat de Universitatea din California, Berkeley și colaboratorii săi.

10.6. Conformitatea UE

10.6.1. RoHS, DEEE și WFD

RACOM
www.racom.eu

EU DECLARATION OF CONFORMITY

Equipment	RipEX, RipEX2 RAy2, RAy3 M!DGE2, M!DGE3 RipEX-HS, RipEX2-HS
Manufacturer	RACOM s.r.o. Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic

This declaration of conformity is issued under the sole responsibility of the manufacturer.

The equipment described above is in conformity with the Directive 2011/65/EU of the European Parliament and of the Council on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS), as amended by Directive (EU) 2015/863, Directive 2012/19/EU of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE) and Regulation (EC) No 1907/2006 of the European Parliament and of the Council concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH).

REACH: Equipment mentioned above do not contain any substances from the "Candidate List of Substances of Very High Concern" with more than 0.1% of the global weight of the delivered item (without packaging of the item)

Compliance has been verified via internal design controls, supplier declarations and/or analytical test data.

Signed for and on behalf of the manufacturer:

Nove Mesto na Morave, 3rd May 2024
Marek Bobula, Technical director

RACOM s.r.o. | Mirova 1283 | 592 31 Nove Mesto na Morave | Czech Republic
Tel.: +420 722 937 522 | E-mail: racom@racom.eu

www.racom.eu

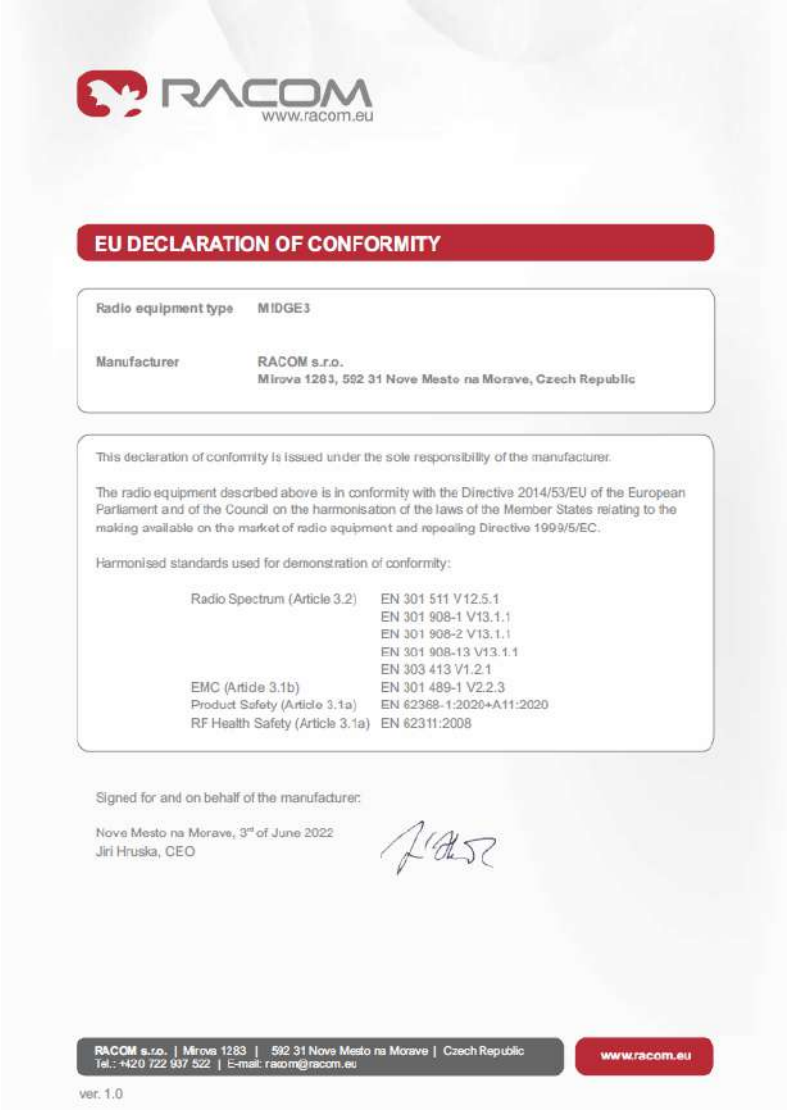
ver. 1.4

Fig. 10.1: Declarație de conformitate UE RoHS, DEEE

Declarație privind Directiva-cadru privind deșeurile

În conformitate cu Directiva 2008/98/CE privind deșeurile modificată prin Directiva (UE) 2015/1127 și Directiva (UE) 2018/851 (Directiva-cadru privind deșeurile), declarăm prin prezenta că produsele noastre nu conțin substanțe de foarte mare îngrijorare (SVHC) listate pe agenția chimică europeană (ECHA) în concentrații SCIP de mai sus cu lista de 1 % cu baza de date de candidati.

10.6.2. Declaratie de conformitate UE RED



RACOM
www.racom.eu

EU DECLARATION OF CONFORMITY

Radio equipment type M!DGE3

Manufacturer RACOM s.r.o.
Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic

This declaration of conformity is issued under the sole responsibility of the manufacturer.

The radio equipment described above is in conformity with the Directive 2014/53/EU of the European Parliament and of the Council on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

Harmonised standards used for demonstration of conformity:

Radio Spectrum (Article 3.2)	EN 301 511 V12.5.1
	EN 301 908-1 V13.1.1
	EN 301 908-2 V13.1.1
	EN 301 908-13 V13.1.1
	EN 303 413 V1.2.1
EMC (Artide 3.1b)	EN 301 489-1 V2.2.3
Product Safety (Article 3.1a)	EN 62368-1:2020+A11:2020
RF Health Safety (Article 3.1a)	EN 62311:2008

Signed for and on behalf of the manufacturer:

Nove Mesto na Morave, 3rd of June 2022
Jiri Hruska, CEO

RACOM s.r.o. | Mirova 1283 | 592 31 Nove Mesto na Morave | Czech Republic
Tel.: +420 722 937 522 | E-mail: racom@racom.eu

www.racom.eu

ver. 1.0

Fig. 10.2: Declarația de conformitate UE ROȘU

10.6.3. Declarație simplificată de conformitate UE

BG
С настоящото RACOM SRO декларира, че този тип радиосъоръжение m! DGE3 е в ъ ъответствие с директива 2014/53/e.

ES
Por la prezent, RACOM sro declara că tipul de echipament radioeléctrico M!DGE3 este conform cu Directiva 2014/53/UE.

CS
Tímto RACOM sro prohlašuje, že typ rádiového zařízení M!DGE3 je v souladu se směrnicí 2014/53/UE.

DA
Hermed erklærer RACOM sro, la radioudstyrstypen M!DGE3 er i overensstemmelse med direktiv 2014/53/EU.

DE
Hiermit erklärt RACOM sro, dass der Funkanlagentyp M!DGE3 der Richtlinie 2014/53/EU entspricht.

ET
Käesolevaga declaraerib RACOM sro, et käesolev raadioseadme tüüp M!DGE3 vastab direktiivi 2014/53/EL nõuetele.

EL
Με την παρούσα ο/η RACOM sro, δηλώνει ότι ο ραδιοεξοπλισμός M!DGE3 πληροί την οδηγία 2014/53/ΕΕ.

RO
Prin prezenta, RACOM sro declară că echipamentul radio de tip M!DGE3 este în conformitate cu Directiva 2014/53/UE.

FR
Le soussigné, RACOM sro, declara că echipamentul radioélectrique de tip M!DGE3 este conform directivei 2014/53/UE.

HR
RACOM sro ovime izjavljuje da je radijska oprema tipa M!DGE3 u skladu s Direktivom 2014/53/EU.

IT
Il fabbricante, RACOM sro, declara che il tipul de aparatura radio M!DGE3 este conform cu directiva 2014/53/UE.

LV
Ar šo RACOM sro deklarē, ka radioiekārta M!DGE3 atbilst Direktīvai 2014/53/ES.

LT
Aš, RACOM sro, patvirtinu, kad radijo įrenginių tipas M!DGE3 atitinka Direktyvą 2014/53/ES.

HU
RACOM sro igazolja, hogy a M!DGE3 típusú rádióberendezés megfelel a 2014/53/EU irányelvnek.

MT
B'dan, RACOM sro, niddeks li dan it-tip ta' echipament tar-radju M!DGE3 este conform mad-Direttiva 2014/53/UE.

NL
Hierbij verklaar ik, RACOM sro, dat het tip radio aparatuur M!DGE3 conform este îndeplinită Richtlijn 2014/53/EU.

PL
RACOM sro niniejszym oświadcza, że typ urządzenia radiowego M!DGE3 jest zgodny z dyrektywą 2014/53/UE.

PT

O(a) abaixo assinado(a) RACOM sro declara că o prezintă tipul de echipament de radio M!DGE3 este conform cu Directiva 2014/53/UE.

RO
Prin prezenta, RACOM sro declară că tipul de echipamente radio M!DGE3 este în conformitate cu Directiva 2014/53/UE.

SK
RACOM sro týmto vyhlasuje, že rádiové zariadenie typu M!DGE3 je v súlade so smernicou 2014/53/EÚ.

SL
RACOM sro potrjuje, da je tip radijske opreme M!DGE3 skladen z Direktivo 2014/53/EU.

FI
RACOM sro vakuuttaa, että radiolaitetyyppi M!DGE3 on direktiivin 2014/53/EU mukainen.

SV
Härmed försäkrar RACOM sro att denna typ av radioutrustning M!DGE3 överensstämmer med direktiv 2014/53/EU.

10.7. Conformitate COMISIA FEDERALĂ DE COMUNICAȚII ȘI INOVAȚIE, ȘTIINȚĂ ȘI DEZVOLTARE ECONOMICĂ CANADA

M!DGE3 îndeplinește FCC - Titlul 47 CFR Part 15 și ICES-003, Issue 7.

Modul	**Conține ID-ul FCC**	**Conține IC**
W	QIPPLS83-W	7830A-PLS83W
Q*	QIPMV32-WA	7830A-MV32W-A
M	---	---
O	QIPTX62-WB	7830A-TX62WB

* în așteptare

10.8. garanție

Piesele sau echipamentele furnizate de RACOM („echipamente”) sunt acoperite de garanție pentru piesele și manopera defecte inerent pentru o perioadă de garanție, așa cum este menționat în documentația de livrare de la data expedierii către client. Garanția nu acoperă modificările personalizate ale software-ului. Pe durata perioadei de garanție, RACOM va monta, repara sau înlocui echipamentul defecte („serviciu”), întotdeauna cu condiția ca în timpul utilizării normale să fi apărut o defecțiune, nu din cauza utilizării necorespunzătoare, fie deliberată sau accidentală, cum ar fi încercarea de reparare sau modificare de către orice persoană neautorizată; nici din cauza acțiunii unor condiții de mediu anormale sau extreme, cum ar fi supratensiune, scufundare în lichid sau lovire de fulger.

Orice echipament supus reparației în garanție trebuie să fie returnat cu transport preplătit către RACOM direct. Echipamentul deservit va fi returnat de către RACOM clientului prin transport preplătit. Dacă circumstanțele nu permit returnarea echipamentului către RACOM, atunci clientul este responsabil și este de acord să ramburseze RACOM pentru cheltuielile suportate de RACOM în timpul întreținerii echipamentului la fața locului. Atunci când echipamentul nu se califică pentru service în condiții de garanție, RACOM va percepe clientul și va fi rambursat pentru costurile suportate pentru piese și forță de muncă la tarifele în vigoare.

Acest contract de garanție reprezintă întreaga acoperire a garanției oferite de RACOM clientului, ca un acord încheiat liber de ambele părți.

RACOM garantează că echipamentul funcționează conform descrierii, fără a garanta că se potrivește intenției sau scopului clientului. În nicio circumstanță, răspunderea RACOM nu se va extinde dincolo de cele de mai sus și nici RACOM, directorii, angajații sau agenții săi nu vor fi răspunzători pentru orice pierdere sau daune consecințe cauzate direct sau indirect prin utilizarea, utilizarea greșită, funcționarea sau funcționarea defectuoasă a echipamentului, întotdeauna sub rezerva protecției statutare care se poate aplica în mod explicit și inevitabil aici.

10.9. Întreținere M!DGE3

Acţiune	Perioadă	Nota
Verificare vizuală – Antenă: Orificiul de scurgere de pe dipol trebuie să fie îndreptat în jos Nu ar trebui să existe elemente deteriorate pe antenă Unghiul de înălțime al antenei Azimut (unghiul deviației orizontale) în conformitate cu proiectarea	Trimestrial	
Verificare vizuală – Cablu coaxial: Deteriorări mecanice Degradarea solară Întregul cablu montat corect pe suprafață Conectori strânși pentru a funcționa optim Banda autovulcanizantă utilizată pentru toate conexiunile care necesită măsurători de izolare PSV și RF	Anual	
Verificare vizuală – Cabinet: Deteriorări mecanice Deteriorări care au ca rezultat o clasificare mai scăzută pentru acoperirea dulapului Bucșe pentru cablurile de rulare	Anual	
Verificare vizuală – Alimentare cu energie electrică: Deteriorări ale izolației Conexiune la terminale	Anual	
Verificare vizuală – Acumulator: Capacitate în conformitate cu cerințele clientului Starea acumulatorului	Anual	
Verificare funcționalitate – sursă de alimentare: Supraîncărcare Deteriorarea acumulatorului	Anual	
Utilizare deplinăa învelișurilor de protecție prevăzute	Anual	
Eliminaorice elemente care nu fac parte din instalație	Anual	
Fixși securizați corect instalațiile improvizate	Anual	
Verificaconexiuni de împământare	După cum este necesar	
Verificaparatrăsnet : conectorii trebuie strânși	După cum este necesar	
Verificaconectori de date conectați inclusiv șuruburi de fixare	Anual	
Evaluavalorile intensității semnalului conexiunii celulare ca măsură preventivă împotriva eșecul conexiunii.	Lunar	*Secțiune 8.5.4.3, "Celular semnal statistici"*
Verificajurnalele de activitate pentru a detecta anomalii în transmisiile de date	Lunar	*Secțiune 8.5.4.2, "Celular stat statistici"*

Acţiune	Perioadă	Nota
Verificadacă alarma de temperatură internă a fost declanșată	Lunar	*Secțiune 8.4, „Evenimente”* *Secțiune 8.2.1, „Măsurători”*
Verificaacel firmware este cea mai recentă versiune stabilă – upgrade FW recomandat atunci când sunt necesare funcții noi	După cum este necesar	*Firmware M!DGE3*[1]

Dacă nu sunteți sigur de oricare dintre cele de mai sus, vă rugăm să contactați asistența tehnică RACOM.

[1] https://www.racom.eu/eng/products/cellular-router-midge.html#dnl_fwr3

Anexa A. Procedura de întărire a securității

RipEX2/M!DGE3 sunt dispozitive de telecomunicații IP celulare fără fir, care oferă un serviciu de încredere 24/7 pentru transferul de date fără fir în aplicații critice, cum ar fi sistemele de control industrial (ICS) și sistemele de control și achiziție de date (SCADA).

Acest apendice conține câțiva pași care pot fi luați în considerare la implementarea infrastructurilor de telecomunicații fără fir.

A.1. Parola si contabilitate

Creați o**cont nou cu rol de „administrator”.**(acces complet) și ștergeți utilizatorul „admin” implicit
• SETĂRI > Securitate > Autentificare locală > Conturi de utilizator
Configurați**o parolă puternică**pentru acest utilizator nou creat cu rol „Admin”. Luați în considerare activarea funcției „Reguli de complexitate a parolei”.
• SETĂRI > Securitate > Autentificare locală > Setări
• Acreditările implicite nesigure sunt:
utilizator: admin
parola: admin
• Utilizarea parolelor complexe este prima ta linie de apărare în protejarea dispozitivului.Luați în considerare actualizările periodice
• Lungimea recomandată este de cel puțin 8-10 caractere, inclusiv Az, 0-9 și caractere speciale (@?* etc.)

Controlul accesului bazat pe rol (RBAC)vă permite să atribuiți privilegii și drepturi de acces utilizatorilor administrativi/numai citire prin atribuirea rolurilor. Creați conturi de utilizator (**autentificare locală** sau la distanță**RAZĂ**) și atribuiți-le roluri prin care pot accesa GUI sau API-ul RipEX2/M!DGE3.
• Există patru niveluri diferite de privilegii de acces utilizator – acestea sunt legate de patru roluri diferite de acces de utilizator:
Oaspete
Tehnician
Tehnician de securitate
Administrator
- *Nota*: Puteți exporta utilizatori de autentificare locală și îi puteți importa în alte unități din rețeaua dvs. Nu trebuie să le creați separat în fiecare dispozitiv
  Fișierul constă din parole hashed/sărate, adică nu pot fi citite și nu sunt deductibile înapoi

Timeout inactivitate web
- Când contul de utilizator nu este activ de ceva timp, utilizatorul va fi deconectat automat. Timpul de inactivitate al contului este setat implicit pentru 1 zi. Este posibil să se schimbe în intervalul de la 5 minute până la 2 zile
- AVANZAT > Generic > Acces utilizator > Timeout inactivitate web
- *Nota:*Este implementat un mecanism împotriva atacurilor cu forță brută. Când este introdusă o combinație greșită de Cont/Parolă, trebuie să așteptați un timp pentru următoarea încercare. Timpul crește cu fiecare încercare greșită.

A.2. Acces fizic

Limitați accesul fizic la dispozitiv numai personalului autorizat.

Dezactivați porturile fizice care nu sunt utilizate
Ethernetporturi

• SETĂRI > Interfețe > Ethernet > Porturi
Serialporturi
• SETĂRI > Interfețe > COM **USB**
port
• pentru acces de gestionare USB/ETH și USB/WiFi
• SETĂRI > Dispozitiv > Unitate > Service USB **Celular**
porturi (dacă există)
• SETĂRI > Interfețe > Cellular > MAIN/EXT **Wifi**(daca
este cazul)
• SETĂRI > Interfețe > Wi-Fi
Detectare manipulare
Unitățile RipEX2 și M!DGE3 sunt echipate cu detectarea deschiderii carcasei. Comportamentul în cazul acestui eveniment va fi setat în meniul SETĂRI > Dispozitiv > Evenimente > Tamper.

A.3. Criptați datele în rețeaua radio (RipEX2)

Criptarea datelor radio wireless împiedică oricine care ar putea accesa rețeaua dvs. să le vadă. Traficul radio poate fi criptat prin AES-256-CCM (frază de acces sau cheie) sau utilizând opțiuni VPN securizate IPsec/OpenVPN (dar acestea nu sunt opțiuni optimizate pentru lățimea de bandă pentru un canal radio).

Radio AES256
Pentru criptare este posibil să setați o frază de acces sau o cheie primară și secundară. Această opțiune permite schimbarea acreditărilor în întreaga rețea fără întrerupere a serviciului.
Criptarea traficului radio are o opțiune suplimentară AES-256-CCM + KEX, care permite înlocuirea periodică a cheilor.
• SETĂRI > Interfețe > Radio > Criptare **VPN**

• SETĂRI > VPN > IPsec
• SETĂRI > VPN > OpenVPN

A.4. Criptați datele în rețeaua celulară

Rețelele celulare sunt în controlul operatorilor, iar APN-urile publice sunt conectate la internetul public. Orice date trimise sau primite de RipEX2 (EXT) sau M!DGE3 (MAIN, EXT) pot fi capturate de hackeri experimentați. Dacă astfel de date nu sunt criptate, datele sensibile pot fi citite de acești hackeri și utilizate greșit.

Este foarte recomandat să**criptați toate datele sensibile**prin opțiuni VPN acceptate -**IPsec sau OpenVPN**.

*Nota:*APN-urile private seamănă cu rețelele radio private. Astfel de APN-uri sunt restricționate de pe Internet de firewall-urile operatorului și ar trebui să fie mai sigure. Cu toate acestea, este încă recomandat să criptați datele dvs. sensibile.

*Nota:*Dirijarea datelor LAN2LAN (end2end) prin APN/rețeaua operatorului este blocată de firewall-urile acestora, iar tunelul sau redirecționarea porturilor sunt singurele modalități de a transmite cu succes datele end2end.

A.5. Dezactivați accesul la distanță sau configurați-l în siguranță

Accesul de la distanță este utilizat pentru a configura și gestiona unitățile de la distanță prin volume de date transmise care permit lățimea de bandă. Trebuie să vă conectați la unitatea locală prin nume de utilizator și parolă. Nu este nevoie să furnizați alte acreditări pentru a accesa alte unități de la distanță prin acces la distanță. Securitatea se bazează pe protocolul QSSH (port TCP 8889) și o cheie privată. Activați numai interfețele pe care le veți folosi pentru acces la distanță:

• AVANZAT > Interfețe > Ethernet > Interfață de rețea
• AVANZAT > Interfețe > Radio > Interfață radio

Sau opriți-l complet:

• SETĂRI > Securitate > Acces administrare > Acces la distanță

Sfaturi pentru setarea într-un mod sigur pentru interfețele activate:

Cheie de acces la distanță generată de utilizator

Cheia privată este aceeași pentru TOATE unitățile fabricate. Este foarte recomandat să generați o astfel de cheie într-o unitate și să o distribuiți tuturor celorlalte din rețeaua dumneavoastră. Nicio altă unitate cu cheie implicită (sau altă cheie de utilizator) nu poate accesa unitățile dvs. prin acces de la distanță.

- SETĂRI > Securitate > Acreditări
  - pentru a genera/descărca/încărca cheia
- SETĂRI > Securitate > Acces administrare > Acces la distanță
  - pentru a seta cheia „utilizator” pentru acces la distanță
  - pentru a defini ID-ul cheii de utilizator

A.6. Schimb de certificate

Se recomandă schimbarea certificatelor pentru certificatele de încredere de către utilizatorul M!DGE3.

Certificatele implicite fac parte din instalarea tuturor unităților, astfel încât înlocuirea propriilor certificate va crește securitatea tuturor proceselor și serviciilor (de ex. acces web, criptare radio), care utilizează certificate (vezi SETĂRI > Securitate > Acreditări).

De asemenea, este posibil să se genereze certificate cu parametri solicitați de aplicația utilizator (vezi parametrii în SETĂRI > Securitate > Acreditări > Setări).

A.7. Servicii

Activați numai**servicii**utilizat pe dispozitiv și dezactivați toate celelalte servicii

Dezactivați neutilizat**SSH**

• AVANZAT > Securitate > Acces administrare > Site web de administrare > Activare SSH → Dezactivat

Dezactivați SNMPv2c, dacă este necesar SNMP,**utilizați SNMPv3**

• SETĂRI > Servicii > SNMP
• sau folosiți „SNMPv3”
  - nivel de securitate: AuthPriv
  - Utilizați algoritmi siguri de autentificare și criptare
  - Setați fraze de acces puternice

Schimbați implicit**HTTP-uri**port

• SETĂRI (sau AVANSAT) > Securitate > Acces administrare > Site web de administrare > Port HTTPS

Dezactivați**HTTP**acces

• SETĂRI (sau AVANSAT) > Securitate > Acces administrare > Site web de administrare > Activare HTTP → Dezactivat

Dezactivați**SMS**sau ajustați numerele de telefon permise

• SETĂRI > Servicii > SMS
  ○ Setați o expresie de acces SMS puternică

Wifi

• Disponibil numai dacă este utilizat adaptorul USB/WiFi pentru accesul de gestionare (conectat)
• Activați WPA2-PSK cu parolă puternică pentru a asigura securitatea WiFi
  ○ SETĂRI > Securitate > Acces administrare > Serviciu USB > Wi-Fi > Securitate, expresie de acces
• Dacă nu este utilizată, funcția poate fi dezactivată complet în cadrul aceluiași meniu

A.8. Firewall

Protejați unitatea prin**Firewall**setări

• SETĂRI > Firewall > L2 / L3 / NAT
• Mai ales important dacă RipEX2/M!DGE3 are o adresă IP publică!

Limitați accesul la GUI RipEX2/M!DGE3

• Permite numai**adrese IPv4 autorizate**pentru a vă accesa rețeaua. Fiecare componentă hardware conectată la o rețea are o adresă IPv4 atribuită. Puteți restricționa accesul la rețea prin filtrarea acestor adrese IPv4 în firewall-ul L3.
• Accesul local poate fi restricționat prin filtrarea adreselor MAC prin firewall L2 (listă neagră, listă albă).
• SETĂRI > Firewall > L2 / L3

A.9. Certificat HTTPS

De la FW 2.1.0.0 și de caracteristicile sale Acreditări, puteți genera sau încărca propriile certificate și chei, inclusiv**HTTP-uri**.

• SETĂRI > Securitate > Acreditări
• SETĂRI > Securitate > Autentificare locală > Setări

A.10. Fișiere de configurare

Fișierele de configurare sunt stocate ca**fișiere JSON necriptate**sau fișiere zip criptate. Este posibil să setați ca numai fișierele criptate să fie permise și regulile pentru parolă pot fi, de asemenea, setate.

• AVANZAT > Generic > CnfSecurity

Puteți descărca fără probleme fișierele de configurare din întreaga rețea prin instrumentul NetSPIDER.

*Nota:*Fiecare utilizator poate descărca doar un fișier de configurare care include parametrii de configurare disponibili pentru un anumit rol de nivel de utilizator.

A.11. Firmware

Păstrați**firmware actualizat**.

Cel mai recent FW poate fi descărcat de pe site-ul RACOM:

RipEX2 FW:*https://www.racom.eu/eng/products/radio-modem-ripex.html#dnl_fwr2*

M!DGE3 FW:*https://www.racom.eu/eng/products/cellular-router-midge.html#dnl_fwr3*

Utiliza**Încărcare și activare directă**pentru dispozitivele RipEX2/M!DGE3 conectate local.

• SETĂRI > Dispozitiv > Firmware > Local

Utiliza**unitate flash USB**-pentru upgrade FW prin disc USB - acest serviciu este activat implicit, poate fi dezactivat.

• SETĂRI > Dispozitiv > Firmware > USB

Utiliza**Distribuție de firmware**pentru rețelele RipEX2 într-un mod optimizat pentru lățimea de bandă.

• Distribuția FW folosește cheia de autentificare în timpul procesului - cheia este aceeași în toate unitățile fabricate - puteți genera și utiliza propria dvs.
• SETĂRI > Servicii > Distribuție firmware
• SETĂRI > Dispozitiv > Firmware > Distribuit
• AVANZAT > Dispozitiv > Distr. firmware - receptor

Utiliza**NetSPIDER**pentru a accelera procesul de distribuție FW în întreaga rețea.

Istoricul revizuirilor

Revizuire
Acest manual a fost pregătit pentru a acoperi o anumită versiune a codului de firmware. În consecință, unele ecrane și caracteristici pot diferi de unitatea reală cu care lucrați. Deși s-au depus toate eforturile rezonabile pentru a asigura acuratețea acestei publicații, îmbunătățirile produsului pot duce, de asemenea, la diferențe minore între manual și produsul livrat.

Revizia 1.0 2022-09-12
Prima problemă

Revizia 1.01 2022-11-16
Îmbunătățiri generale

Revizia 1.01 2022-12-16
A fost adăugată secțiunea Modul Sleep

Revizia 1.02 24-02-2023
Îmbunătățiri minore ale capitolului SETĂRI

Revizia 1.03 2023-05-11
Îmbunătățiri minore ale capitolului SETĂRI

Revizia 1.04 28-07-2023
Secțiune*Acreditări*Secțiunea adăugată
*Gestionarea linkurilor*adăugat

Revizia 1.05 23-10-2023
Secțiunea OpenVPN a fost adăugată
Anexă Procedura de întărire a securității a fost adăugată

Revizia 1.06 2023-12-15
Au fost adăugate funcții noi pentru versiunea FW 2.1.2.0

Revizia 1.07 2024-03-05
Au fost adăugate funcții noi pentru versiunea FW 2.1.6.0

Revizia 1.08 2024-06-05
Au fost adăugate funcții noi pentru versiunea FW 2.1.7.0

Revizia 1.09 29-08-2024
Au fost adăugate funcții noi pentru versiunea FW 2.2.0.0

Revizia 1.10 2024-10-07
Extinderea protocolului PPP pentru a include Tetra

Revizia 1.11 28-11-2024
Au fost adăugate funcții noi pentru versiunea FW 2.2.1.0

****

TRADUCĂTOR

Subsemnata, **ALBU MARIA CAMELIA,** interpret şi traducător autorizat pentru limba engleză în temeiul autorizaţiei nr. 8963/2003, certific exactitatea traducerii documentului din limba engleză în limba română, care a fost văzut de mine, că textul prezentat a fost tradus complet, fără omisiuni, şi că, prin traducere, înscrisului nu i-au fost denaturate conţinutul şi sensul.

TRADUCĂTOR

ALBU MARIA CAMELIA