



Distribuitor autorizat Teltonika in Romania: **Topalis Engineering srl**

email: teltonika@topalis.ro

Notă juridică

Copyright © 2015 TELTONIKA Ltd. Toate drepturile rezervate. Sunt interzise reproducerea, transferul, distribuirea sau stocarea parțială sau integrală, sub orice formă, a conținutului acestui document fără acordul prealabil scris al TELTONIKA Ltd. Producătorul își rezervă dreptul de a modifica produsul și manualul în scopul perfecționării tehnice, fără notificare prealabilă.

Alte denumiri de produse și companii menționate aici pot fi mărci sau denumiri comerciale ale titularilor acestora.

Atenție



Vă recomandăm cu tărie să citiți acest manual de utilizare înainte de a folosi dispozitivul.



Nu dezmembrați dispozitivul. Nu atingeți dispozitivul dacă șasiul acestuia este crăpat.



Toate dispozitivele fără fir pentru transfer de date pot fi susceptibile la interferențe, ceea ce le-ar putea afecta performanțele.



Dispozitivul nu este rezistent la apă. Păstrați-l uscat.



Dispozitivul este alimentat prin un adaptor de joasă tensiune de +9 V c.c.

Cuprins

Notă juridică	2
Atenție	2
INFORMAȚII PRIVIND SIGURANȚA	9
Conecțarea dispozitivului	10
1 Introducere	11
2 Specificații	11
2.1 Ethernet	11
2.2 Wi-Fi	11
2.3 Hardware	11
2.4 Specificații electrice, fizice și de mediu	12
2.5 Utilizări	12
3 Configurarea routerului Dvs.	13
3.1 Instalare	13
3.1.1 Panoul frontal și panoul posterior	13
3.1.2 Indicatorul LED al stării conexiunii	14
3.1.3 Instalarea componentelor hardware	14
3.2 Logarea	15
4 Moduri de operare	18
5 Opțiuni de alimentare cu energie electrică	19
5.1 Alimentarea dispozitivului cu o tensiune mai mare	19
6 Stare	20
6.1 Imagine de ansamblu	20
6.2 Informații de sistem	21
6.3 Informații despre rețele	22
6.4 Informații despre dispozitiv	34
6.5 Servicii	35
6.6 Rute	36
6.6.1 ARP	36
6.6.2 Rute IP active	36
6.6.3 Rute IPv6 active	37
6.7 Grafice	38

6.7.1	Intensitatea semnalului rețelei de telefonie mobilă	38
6.7.2	Încărcarea în timp real	39
6.7.3	Traficul în timp real	40
6.7.4	Semnalul wireless în timp real	41
6.7.5	Conexiuni în timp real	42
6.8	Traficul prin rețeaua de telefonie mobilă	43
6.9	Jurnalul de evenimente	44
6.9.1	Toate evenimentele	44
6.9.2	Evenimente de sistem	45
6.9.3	Evenimente de rețea	46
6.9.4	Raportarea evenimentelor	47
6.9.5	Configurarea raportării	52
7	Rețea	57
7.1	Rețeaua de telefonie mobilă	57
7.1.1	Setări generale	57
7.1.2	Gestionarea cartelelor SIM	60
7.1.3	Operatori de rețele	61
7.1.4	Limita pentru date mobile	63
7.1.5	Protecția SIM-ului inactiv	64
7.2	WAN	66
7.2.1	Modul de operare	66
7.2.2	Configurare comună	66
7.2.3	Cum configerez o conexiune de backup?	74
7.3	LAN	75
7.3.1	Configurare	75
7.3.2	Server DHCP	76
7.3.3	Închirieri statice	77
7.3.4	Aliasuri IP	78
7.4	VLAN	79
7.4.1	Rețele VLAN	79
7.4.2	Rețele LAN	80
7.5	Wireless	81
7.5.1	Punct de acces wireless	81
7.5.2	Stație wireless	85
7.6	Firewall	86
7.6.1	Setări generale	86
7.6.2	DMZ	87

7.6.3	Forwardarea între zone	87
7.6.4	Forwardarea porturilor	88
7.6.5	Reguli pentru trafic	91
7.6.6	Reguli personalizate	97
7.6.7	Prevenirea atacurilor de blocare distribuită a serviciului (DDOS)	98
7.6.8	Prevenirea scanării porturilor	101
7.7	Rutarea.....	102
7.7.1	Rute statice	102
7.7.2	Rute dinamice	103
7.7.1	105
7.7.2	105
7.8	Echilibrarea încărcării	112
8	Monitorizarea și administrarea de la distanță.....	113
9	Servicii.....	115
9.1	VRRP.....	115
9.1.1	Setările de configurare a rețelei LAN în VRRP	115
9.1.2	Verificarea conexiunii la internet.....	115
9.2	TR-069	116
9.2.1	Configurarea parametrilor TR-069.....	116
9.3	Filtrul web	117
9.3.1	Blocarea site-urilor.....	117
9.3.2	Blocarea conținutului prin servere proxy	117
9.4	MQTT	118
9.4.1	Brokerul MQTT.....	118
9.4.2	Publisher-ul MQTT	121
9.5	NTP.....	123
9.6	RS-232/RS-485	124
9.6.1	RS-232	124
9.6.2	RS-485	126
9.6.3	Modurile diferitelor tipuri de interfețe seriale RS-232 și RS-485	130
9.7	VPN	133
9.7.1	OpenVPN.....	133
9.7.1	136
9.7.2	IPsec	139
9.7.3	Tunel GRE	142
9.7.4	PPTP	144
9.7.5	L2TP	146

9.8	Dynamic DNS	148
9.9	Utilitare SMS	149
9.9.1	Utilitare SMS	149
9.9.1	150
9.9.2	Utilitare prin apel	159
9.9.3	Grupuri de utilizatori.....	160
9.9.4	Gestionarea SMS-urilor.....	161
9.9.5	Configurarea de la distanță.....	163
9.9.6	Statistici.....	166
9.10	SNMP	167
9.10.1	Setări SNMP.....	167
9.10.2	Setări TRAP	168
9.11	Gateway SMS	169
9.11.1	Configurarea metodelor POST/GET.....	169
9.11.2	E-mail prin SMS	171
9.11.3	Mesaje programate	172
9.11.4	Răspuns automat.....	173
9.11.5	Forwardarea SMS-urilor	174
9.11.6	SMPP.....	177
9.12	GPS.....	178
9.12.1	GPS	178
9.12.2	Setări GPS	178
9.12.1	179
9.12.2	179
9.12.3	Mod GPS	180
9.12.4	Intrările și ieșirile GPS.....	181
9.12.5	Geofencing prin GPS.....	182
9.13	Hotspot	183
9.13.1	Setări generale	183
9.13.2	Setări de restrictionare a accesului la internet	185
9.13.3	Jurnalizarea.....	185
9.13.4	Pagina de destinație	186
9.13.5	Configurarea serverului RADIUS.....	188
9.14	CLI.....	189
9.15	Reporning automată.....	190
9.15.1	Reporning pe baza comenzi ping	190
9.15.2	Reporning periodică.....	191

9.16	Resurse partajate în rețea	191
9.16.1	Sisteme de fișiere montate	191
9.16.2	Samba	192
9.16.3	Utilizatori Samba	192
9.17	Interfață Modbus TCP	194
9.18	UPnP	195
9.18.1	Setări generale	195
9.18.2	Setări avansate	195
9.18.3	Liste de control acces UPnP	196
9.18.4	Redirecționări UPnP active	196
9.19	QoS	196
9.20	Intrări/ieșiri	197
9.20.1	Stare	197
9.20.2	Intrări	198
9.20.3	Ieșiri	201
9.20.4	Informații despre componente hardware ale intrărilor și ieșirilor	204
10	Sistem	210
10.1	Asistentul de configurare	210
10.2	Profiluri	212
10.3	Administrare	213
10.3.1	Setări generale	213
10.3.2	Remedierea defectiunilor	214
10.3.3	Backup	215
10.3.4	Diagnoză	217
10.3.5	Clonarea adresei MAC	218
10.3.6	Configurarea paginii Overview Imagine de ansamblu 	218
10.3.7	Monitorizare	219
10.4	Script-uri scrise de utilizatori	219
10.5	Punct de restaurare	220
10.5.1	Crearea unui punct de restaurare	220
10.5.2	Încărcarea unui punct de restaurare	220
10.6	Firmware	221
10.6.1	Firmware	221
10.6.2	Firmware over the air (FOTA)	222
10.7	Repornirea routerului	222
11	Recuperarea dispozitivului	222
11.1	Butonul de resetare	223

RUT955 - Manual de utilizare

11.2	Interfața web a bootloader-ului	223
12	Glosar.....	223
13	Evidența modificărilor.....	226

INFORMAȚII PRIVIND SIGURANȚA

În acest document vi se va prezenta modul în care să utilizați în siguranță routerul. Vă sugerăm să respectați recomandările de mai jos pentru a evita vătămările corporale și/sau daunele materiale.

Trebuie să vă familiarizați cu cerințele de siguranță înainte de a utiliza dispozitivul!

Pentru a evita arsurile și electrocutarea personalului care lucrează cu dispozitivul, respectați aceste cerințe de siguranță.



Dispozitivul este destinat alimentării de la o sursă de putere limitată (LPS) al cărei consum de energie nu trebuie să depășească 15 VA, iar pentru dispozitivul de protecție la supracuret valoarea nominală a curentului nu trebuie să depășească 2 A.



Supratensiunea tranzitorie maximă în circuitul de ieșire (secundar) al sursei de alimentare utilizate nu trebuie să depășească 36 V.



Dispozitivul poate fi utilizat cu un computer personal (prima clasă de siguranță) sau cu un notebook (a doua clasă de siguranță). Echipamente asociate: o sursă de alimentare cu energie electrică (PSU) (LPS) și un calculator personal care să respecte cerințele standardului EN 60950-1.



Nu montați și nu reparați dispozitivul în timpul unei furtuni.



Pentru a evita deteriorarea mecanică a dispozitivului, se recomandă să îl transportați într-un ambalaj rezistent la deteriorări.



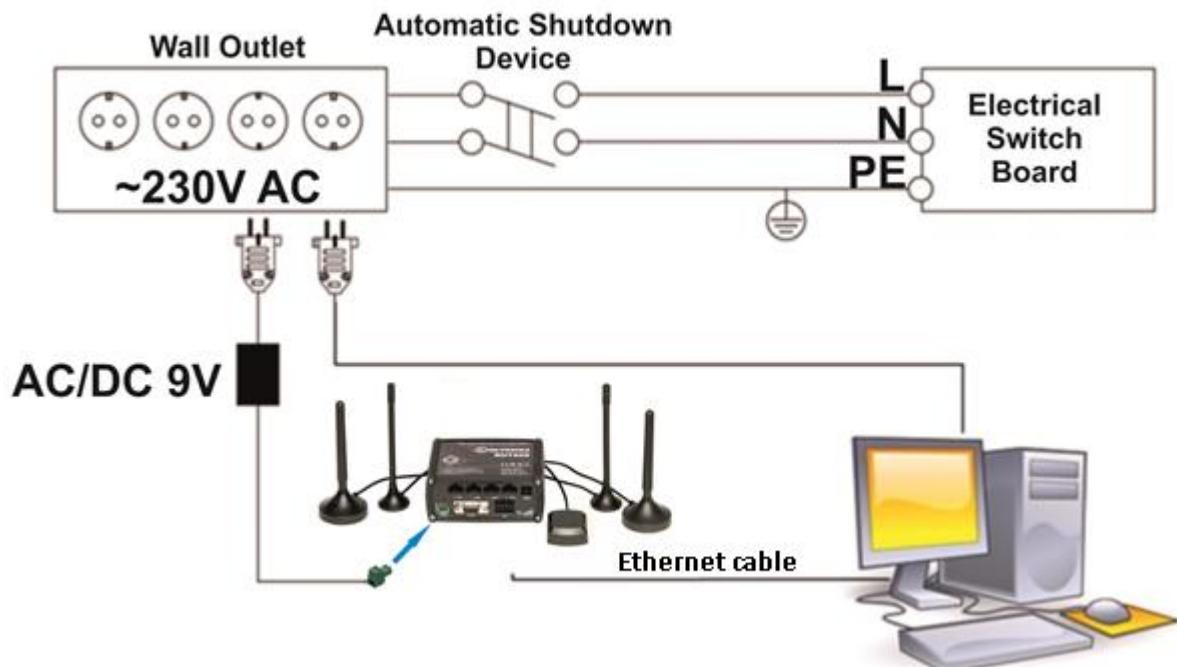
Protecția circuitelor primare ale PC-ului și sursei de alimentare asociate împotriva scurtcircuitelor și protecția împotriva împământării defectuoase a PC-ului asociat va fi asigurată ca parte a instalației clădirii.

Pentru a evita deteriorarea mecanică a dispozitivului, se recomandă să îl transportați într-un ambalaj rezistent la deteriorări. În timpul utilizării dispozitivului, acesta trebuie plasat astfel încât indicatoarele sale cu LED-uri să fie vizibile, deoarece acestea vă informeză cu privire la modul de operare a dispozitivului și dacă acesta are probleme de funcționare.

Protecția împotriva supracurenților, a scurtcircuitelor și a împământării defectuoase trebuie asigurată ca parte a instalației clădirii.

Nivelul semnalului dispozitivului depinde de mediul în care funcționează. Dacă dispozitivul începe să funcționeze necorespunzător, vă rugăm să vă adresați personalului calificat în vederea reparării produsului, respectiv unui service sau producătorului. Dispozitivul nu conține componente înlocuibile.

Conecțarea dispozitivului



1 Introducere

Vă mulțumim că ați achiziționat un router LTE RUT955!

RUT955 face parte din seria RUT9xx de routere mobile compacte cu conexiuni wireless și Ethernet de mare viteză.

Acest router este ideal pentru persoanele care doresc să-și partajeze internetul în mișcare, fără restricțiile impuse de o conexiune de cablu greoaie. Fără să impună restricții, dar nu fără a fi luată în calcul: routerul suportă, totuși, distribuția conexiunii la internet printr-un cablu de bandă largă; trebuie doar să conectați cablul la portul WAN, să setați routerul la un mod de operare corect și sunteți gata să navigați.

2 Specificații

2.1 Ethernet

- Respectă standardele IEEE 802.3, IEEE 802.3u
- 3 porturi LAN 10/100Mbps
- 1 port WAN 10/100Mbps
- Suportă Auto MDI/MDIX

2.2 Wi-Fi

- Respectă standardele IEEE 802.11b/g/n
- 2x2 MIMO
- Moduri AP și STA
- Metode de criptare: 64/128-bit WEP, WPA, WPA2, WPA&WPA2
- Domeniul de frecvențe: 2,401 – 2,495 GHz
- Putere de emisie maximă: 20 dBm
- Mod SSID ascuns și controlul accesului pe baza adresei MAC

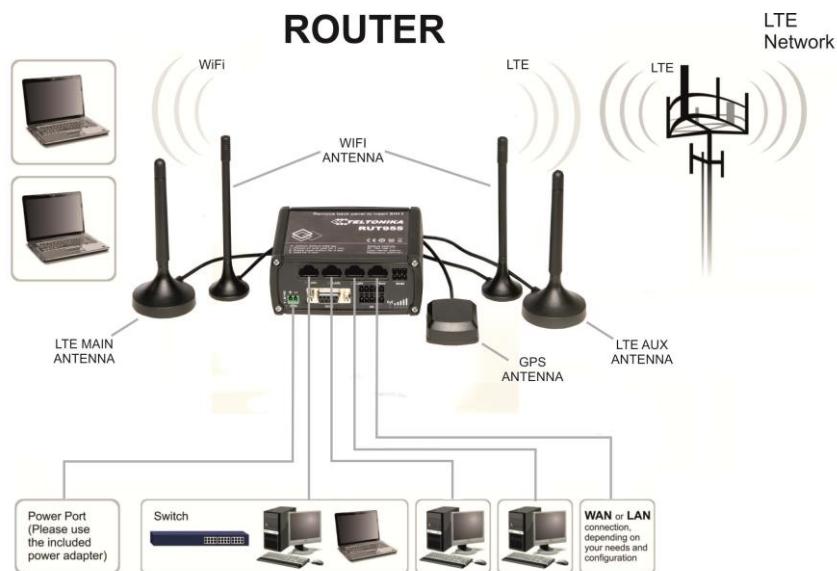
2.3 Hardware

- Unitate centrală de procesare de 560 MHz de înaltă performanță, cu memorie DDR2 de 128 MB
- Priză industrială de alimentare cu curent continuu cu 2 pini
- Adaptor atașabil pentru montare pe șină DIN
- Bloc teminal industrial cu 4 pini pentru conector RS-485 cu 2 sau 4 fire
- Mufă DB9 pentru conector RS-232
- USB tip A pentru dispozitive externe
- Bloc teminal industrial cu 4 pini pentru conector RS-485 cu 2 sau 4 fire
- Buton de resetare/revenire la setările implice
- Conectori pentru antene: 2 x SMA for LTE , 2 x RP-SMA pentru WiFi
- 4 LED-uri Ethernet, 1 LED pentru alimentare
- 1 LED bicolor pentru starea conexiunii, 5 LED-uri pentru intensitatea conexiunii
- Bloc teminal industrial cu 10 pini pentru intrări/ieșiri:
 - intrare digitală de 0 – 3 V
 - intrare digitală izolată galvanic de 0 – 30 V
 - intrare analogică de 0 – 24 V;
 - ieșire digitală cu colector în gol de 30 V, 250 mA
 - ieșire relee SPST de 40 V, 4 A

2.4 Specificații electrice, fizice și de mediu

• Dimensiuni (l x l x A)	80 mm x 106 mm x 46 mm
• Masă	250 g
• Alimentare	100 – 240 V c.a. -> adaptor de perete de 9 V c.c.
• Tensiune intrare	9 – 30 V c.c.
• Putere consumată	< 7 W
• Temperatură de funcționare	-40° ... 75° C
• Temperatură de depozitare	-45° ... 80° C
• Umiditate de funcționare	10% ... 90% fără condens
• Umiditate de depozitare	5% ... 95% fără condens

2.5 Utilizări



3 Configurarea routerului Dvs.

3.1 Instalare

După ce despachetați produsul, urmați pașii detaliați mai jos pentru a conecta corect dispozitivul. Pentru o mai bună performanță Wi-Fi, așezați dispozitivul într-un loc vizibil, deoarece obstacolele precum peretii și ușile afectează semnalul.

1. Întâi asamblați routerul prin atașarea antenelor necesare și prin introducerea cartelei/cartelelor SIM.
2. Pentru a porni routerul, folosiți adaptorul de alimentare inclus (IMPORTANT: utilizarea unui adaptor de alimentare diferit poate duce la deteriorarea produsului și la pierderea garanției).
3. Dacă aveți o conexiune de bandă largă prin cablu, va trebui să o conectați la portul WAN al routerului.

3.1.1 Panoul frontal și panoul posterior



1	Porturi Ethernet LAN
2	Port Ethernet WAN
3	LED-uri LAN
4	LED WAN
5	Conector RS-485
6	Priză alimentare
7	Conector RS-232
8	Conector pt. intrări și ieșiri
9	LED alimentare
10	LED conexiune
11	LED intensitate conexiune

1	Conector pt. antena auxiliară LTE*
2	Conector pt. antena GPS
3	Conector pt. antena principală LTE*
4	Conector USB
5	Conektori pt. antena WiFi
6	Buton resetare

* Poziționarea conectorilor pt. antena principală/auxiliară depinde de modemul routerului :
Quectel: 1 – PRINCIPALĂ; 3 – AUXILIARĂ
Huawei: 1 – AUXILIARĂ; 3 – PRINCIPALĂ
Telit: 1 – AUXILIARĂ; 3 – PRINCIPALĂ

Pentru a identifica marca modemului routerului Dvs., verificați față de jos a routerului. Ar trebui să găsiți un autocolant cu informații despre router (nr. serie, IMEI, MAC LAN etc.). Primul rând este codul de produs al routerului. Al săptalea caracter din cod indică modemul routerului:

- Quectel: A, H, J, K, L, M, P
- Huawei: 1, 3, 5, 7, 9, B, F
- Telit: 0, 2, G

Mai jos este un exemplu de autocolant cu un modem **Huawei** (caracterul aferent modemului este indicat cu galben)



3.1.2 Indicatorul LED al stării conexiunii

Clipire constantă (cca 2 Hz) – routerul pornește

LED stins – nu există conexiune de date 4G

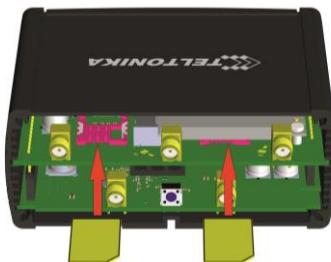
LED aprins – există conexiune de date 4G.

Explicarea indicațiilor LED-ului de stare a conexiunii:

1. Verde și roșu clipind alternativ la fiecare 500 ms: fără cartela SIM ori PIN incorrect;
2. Verde, roșu și galben clipind alternativ la fiecare 500 ms: în curs de conectare la GSM;
3. Roșu clipind la fiecare 1 s: conectat la 2G, dar nu s-a stabilit nicio sesiune de date;
4. Galben clipind la fiecare 1 s: conectat la 3G, nu s-a stabilit nicio sesiune de date;
5. Verde clipind la fiecare 1 s: conectat la 4G, nu s-a stabilit nicio sesiune de date;
6. Roșu aprins și clipind rapid când sunt transferate date: conectat la 2G cu sesiune de date;
7. Galben aprins și clipind rapid când sunt transferate date: conectat la 3G cu sesiune de date;
8. Verde aprins și clipind rapid când sunt transferate date: conectat la 4G cu sesiune de date.

3.1.3 Instalarea componentelor hardware

1. Scoateți panoul posterior și introduceți cartela/cartelele SIM oferită/e de furnizorul Dvs. de servicii de acces la internet. În imagine se arată poziția corectă a cartelei SIM.



SIM 1 (principal) SIM 2 (secundar)

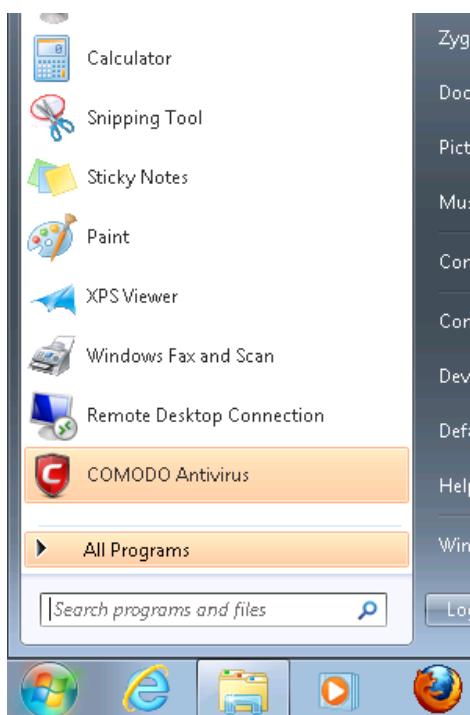
2. Ataşați antena LTE principală și antena Wi-Fi.
3. Conectați adaptorul de alimentare la priza de pe panoul frontal al dispozitivului, apoi conectați celălalt capăt al adaptorului la priza de rețea.
4. Conectați-vă la dispozitiv în mod wireless (SSID: **Teltonika_Router**) sau folosiți un cablu Ethernet introdus într-unul din porturile Ethernet pt. LAN.

3.2 Logarea

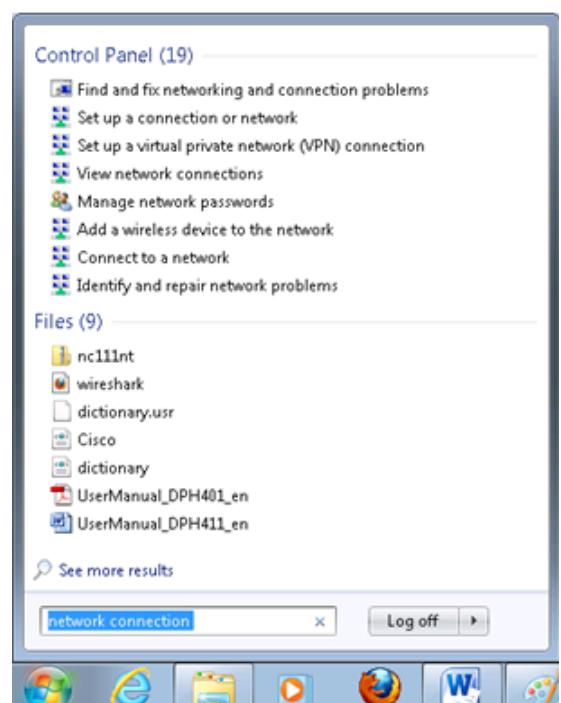
După ce ați finalizat configurarea ca în secțiunea de mai sus, sunteți gata să vă logați la router și să începeți să îl configurați. Acest exemplu arată modul de conectare în Windows 7. În Windows Vista: dați clic pe Start-> Control Panel -> Network and Sharing Centre -> Manage network Connections -> (treceți la pasul 4). În Windows XP: dați clic pe Start -> Settings -> Network Connections -> (vezi pasul 4). Nu se va afișa "Internet protocol version 4(TCP/IPv4)", ci va trebui să selectați "TCP/IP Settings" și să dați clic pe Options-> (treceți la pasul 6). În Windows 10 tastați "Network and Sharing Center" în bara de căutare și accesați. În bara de navigare din partea stângă a ferestrei, dați clic pe "Change adapter settings" -> (treceți la pasul 4).

Mai întâi trebuie configurată placa de rețea astfel încât aceasta să poată comunica în mod corespunzător cu routerul.

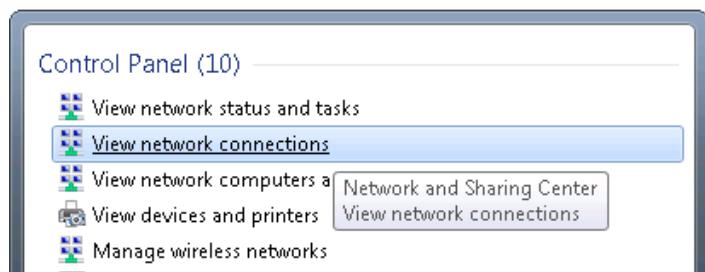
1. Apăsați butonul de pornire



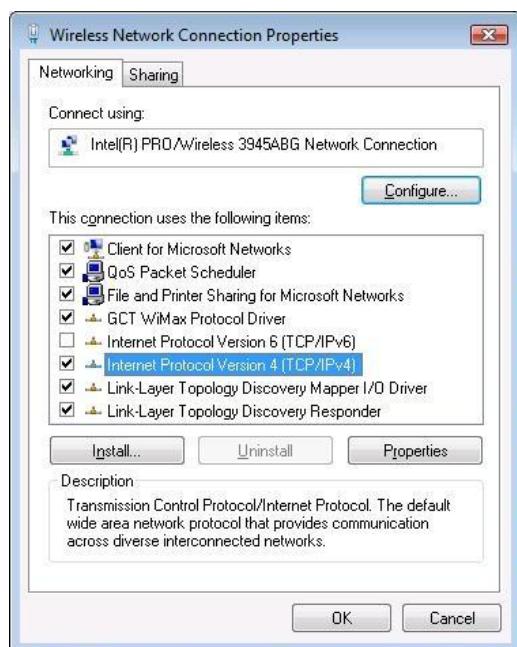
2. Tastați "network connections" și așteptați să apară rezultatele



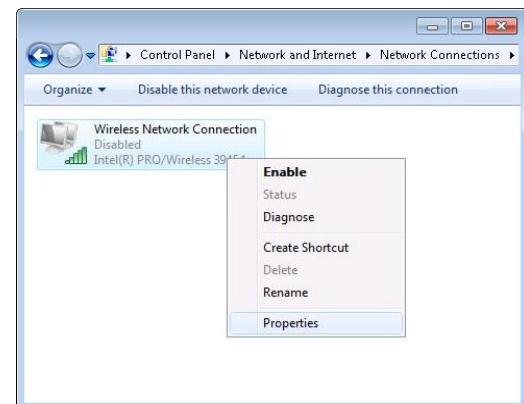
3. Dați clic pe “View network connections”



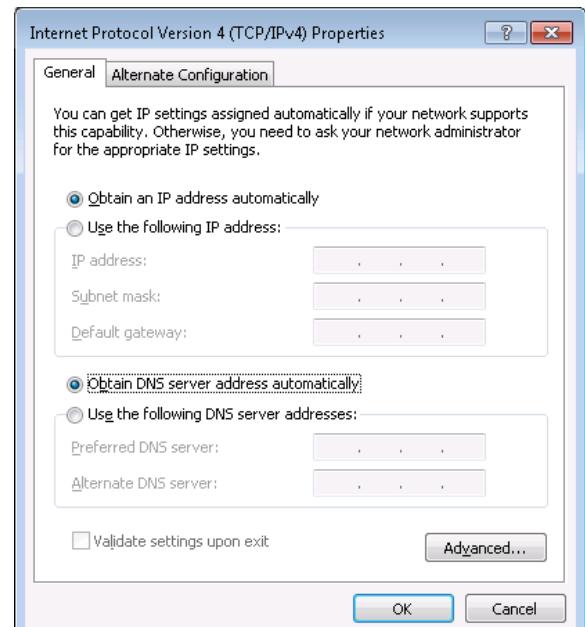
5. Selectați Internet Protocol Version 4 (TCP/IPv4) și apoi dați clic pe Properties



4. Apoi dați clic dreapta pe dispozitivul Dvs. wireless pe care îl folosiți pentru a vă conecta la alte puncte de acces (cel denumit “Wireless Network Connection” și care are bare indicatoare de semnal în pictogramă)

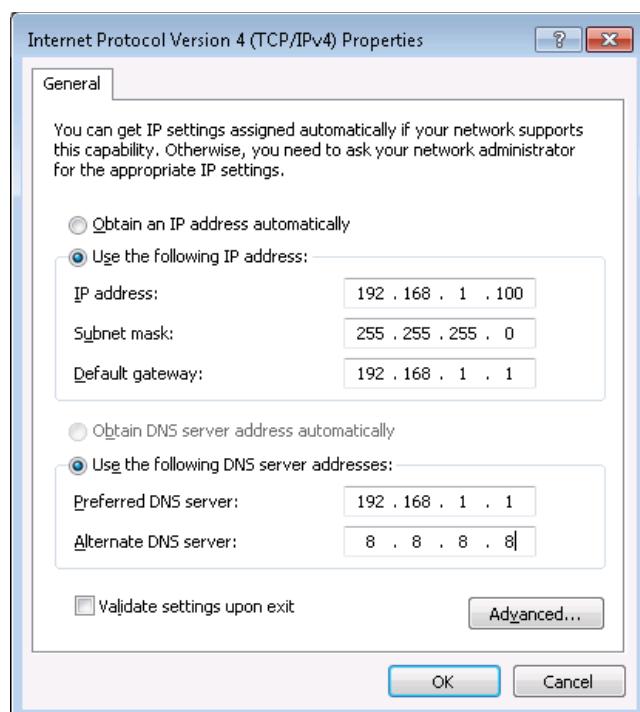


6. În mod implicit routerul va avea protocolul DHCP activat, astfel încât dacă selectați “Obtain an IP address automatically” și “Obtain DNS server address automatically”, routerul vă va aloca o adresă IP și veți fi gata să vă logați.



7. Dacă doriți configurarea manuală, procedați astfel:

Întâi selectați o adresă IP. Datorită setările din fabrică ale routerului, puteți introduce doar un IP de forma 192.168.1.XXX , cu XXX în intervalul 2-254 (192.168.1.2, 192.168.1.254, 192.168.1.155 și.m.d. sunt valide; 192.168.1.0, 192.168.1.1, 192.168.1.255, 192.168.1.699 și.m.d. nu sunt valide). Apoi introduceți masca de subrețea: "255.255.255.0" și gateway-ul implicit: "192.168.1.1", iar la final introduceți adresele IP ale serverului DNS principal și secundar. Unul este de ajuns, deși este bine să aveți și unul secundar, ca rezervă în cazul în care primul eșuează. DNS-ul poate fi IP-ul Dvs. (192.168.1.1), dar poate fi și un server DNS extern (precum cel oferit de Google: 8.8.8.8).



Dați clic dreapta pe pictograma rețelei wireless și selectați Connect / Disconnect. Va apărea o listă cu toate rețelele wireless disponibile. Selectați "Teltonika" și dați clic pe Connect. Apoi lansați browserul preferat și tastați IP-ul routerului în câmpul de adresă:



Apăsați Enter. Dacă nu sunt probleme, veți fi întâmpinat cu un ecran de logare precum cel de mai jos:



Introduceți parola implicită, care este "admin01", în câmpul "Password" și apoi fie dați clic pe Login | Logare|, fie apăsați tasta Enter. Acum v-ați logat cu succes la RUT955!

De aici înainte puteți configura aproape orice setare a routerului Dvs.

4 Moduri de operare

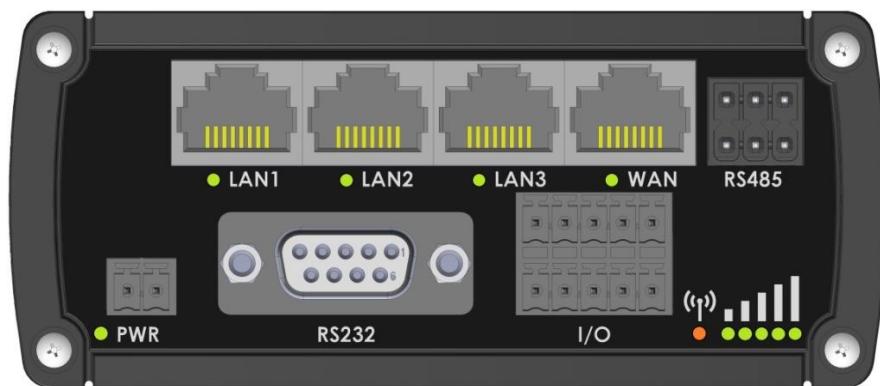
Routerul din seria RUT9xx suportă diferite moduri de operare. Poate fi conectat la internet (WAN) prin rețea de telefonie mobilă, prin cablu Ethernet standard sau printr-o rețea wireless. Când vă conectați la internet puteți, de asemenea, să stabiliți una sau două conexiuni de backup la conexiunea principală WAN. Orice interfață poate acționa ca backup dacă este configurață astfel. Inițial routerul folosește conexiunea sa principală WAN; dacă aceasta se pierde, routerul încearcă să se conecteze prin conexiunea de backup cu prioritatea mai mare și, dacă nici aceasta nu reușește, routerul încearcă și a doua opțiune de backup.

Conexiune WAN	Conexiune WAN principală	Conexiune WAN de backup	LAN
Rețea mobilă	✓	✓	X
Ethernet	✓	✓	✓
Wi-Fi	✓	✓	✓

Modurile de operare vor fi explicate detaliat în această [secțiune](#).

5 Opțiuni de alimentare cu energie electrică

Routerul RUT9xx poate fi alimentat de la o priză de rețea sau printr-un port Ethernet. În funcție de arhitectura rețelei Dvs., puteți utiliza portul LAN1 pentru alimentarea dispozitivului.



Routerul RUT9xx poate fi alimentat simultan de la o priză de rețea și prin Ethernet. Priza de rețea are o prioritate mai mare, ceea ce înseamnă că dispozitivul se va alimenta de la rețea atât timp cât este posibil.

Când routerul RUT9xx trece de la o sursă de alimentare la alta, alimentarea se întrerupe pentru o fracțiune de secundă și routerul poate reporni. Dispozitivul va funcționa corect după repornire.

Pin	Signal ID	T568A Color	T568B Color	Pins on plug face (socket is reversed)
1	TX+	white/green stripe	white/orange stripe	
2	TX-	green solid	orange solid	
3	RX+	white/orange stripe	white/green stripe	
4		blue solid	blue solid	
5	7 - 30VDC	white/blue stripe	white/blue stripe	
6	RX-	orange solid	green solid	
7	GROUND	white/brown stripe	white/brown stripe	
8	GROUND	brown solid	brown solid	

Deși dispozitivul poate fi alimentat printr-un port Ethernet, nu este compatibil cu standardul IEEE 802.3af-2003. Alimentarea routerului RUT9xx dintr-o sursă de alimentare IEEE 802.3af-2003 **va deteriora dispozitivul** deoarece nu este dimensionat pentru tensiunile de intrare ale standardului PoE.

5.1 Alimentarea dispozitivului cu o tensiune mai mare

Dacă decideți să nu folosiți adaptoarele de perete standard de 9 V c.c. oferite de noi și doriți să alimentați dispozitivul de la o tensiune mai mare (15 – 30 V c.c.), asigurați-vă că alegeti o sursă de alimentare de înaltă calitate. Unele surse de alimentare pot produce vârfuri de tensiune semnificativ mai mari decât tensiunea de ieșire declarată, în special în timpul procesului de conectare și deconectare.

Deși dispozitivul este proiectat să accepte tensiuni de intrare de până la 30 V c.c., supratensiunile de la surse de alimentare cu tensiune mare pot dăuna dispozitivului. Dacă doriți să utilizați surse de alimentare cu tensiune mare, vă recomandăm să folosiți și echipamente de siguranță suplimentare pentru suprimarea supratensiunilor.

6 Stare

Secțiunea de stare conține diferite informații, cum ar fi adresele IP ale diferitelor interfețe de rețea, starea memoriei routerului, versiunea de firmware, închirierile DHCP, stațiile wireless asociate, grafice care indică încărcarea, traficul și multe altele.

6.1 Imagine de ansamblu

Fereastra Overview |Imagine de ansamblu| afișează diferite informații generale.

The screenshot shows the 'Overview' page of the Teltonika RUT955 web interface. The top navigation bar includes the Teltonika logo, Status, Network, Services, System, and Logout. The main content is organized into several sections:

- System:** Shows Router uptime (0d 0h 4m 9s since 2017-06-05, 08:38:38), Local device time (2017-06-05, 08:42:47), Memory usage (RAM: 34% used, FLASH: 7% used), and Firmware version (RUT9XX_R_00.03.357). A CPU load bar indicates 9.0%.
- Mobile:** Shows Data connection (0d 0h 0m 31s since 2017-06-05, 08:42:16), State (Registered (home); LT BITE GSM; 4G (LTE)), SIM card slot in use (SIM 1 (Ready)), and Bytes received/sent* (3.1 MB / 138.4 KB). Signal strength is -67 dBm.
- Wireless:** Shows SSID (HAL10000 (AP)) and Mode (1- AP; 7 CH (2.442 GHz)). The wireless icon shows 'ON' with a signal strength bar.
- WAN:** Shows IP address (84.15.198.92) and Backup WAN status (Backup link is disabled). A mobile signal icon is shown.
- Local Network:** Shows IP / netmask (192.168.56.1 / 255.255.255.0) and Clients connected (2).
- Access Control:** Shows LAN (SSH; HTTP; HTTPS) and WAN (No access).
- Recent System Events:** Lists four events:
 - 1 2017-06-05 08:42:07 - DHCP: Leased 192.168.56.235 IP address f ...
 - 2 2017-06-05 08:42:07 - DHCP: Leased 192.168.56.124 IP address f ...
 - 3 2017-06-05 08:42:06 - DHCP: Leased 192.168.56.124 IP address f ...
 - 4 2017-06-05 08:41:59 - Port: Wired WAN connection non operation ...
- Recent Network Events:** Lists four events:
 - 1 2017-06-05 08:41:55 - Mobile data connected: LT BITE GSM
 - 2 2017-06-05 08:39:53 - WiFi client connected: 1C:7B:21:58:69:C3 ...
 - 3 2017-06-05 08:39:11 - Joined 4G LTE
 - 4 2017-06-05 08:39:02 - Joined 3G WCDMA

* Your carrier's data usage accounting may differ. Teltonika is not liable should any accounting discrepancies occur.

6.2 Informații de sistem

Fereastra System Information | Informații de sistem| afișează date despre sistemul de operare al routerului.

The screenshot shows the 'System Information' page with the following sections:

- System** section:

Router name	RUT955
Host name	Teltonika-RUTm.com
Router model	?
Firmware version	RUT9XX_R_00.03.539
Kernel version	3.10.36
Bootloader version	3.0.1
Local device time	2017-07-21, 12:43:56
Uptime	0d 4h 31m 29s (since 2017-07-21, 08:12:27)
Load average	1 min: 9%; 5 mins: 15%; 15 mins: 13%
Temperature	N/A ° C
- Memory** section:

Free	76312 kB / 126556 kB (60%)
Cached	17168 kB / 126556 kB (13%)
Buffered	6568 kB / 126556 kB (5%)

Detalierea secțiunii System | Sistem |:

	Nume câmp	Valoare în exemplu	Explicație
1.	Router Name	RUT955	Numele routerului (numele de gazdă al sistemului routerului)
2.	Host name Nume gazdă	Teltonika-RUT955.com	Arată cum va fi văzut routerul de alte dispozitive din rețea
3.	Router Model	Teltonika RUT955 LTE	Modelul routerului
4.	Firmware Version	RUT9XX_R_00.02.376	Versiunea firmware-ului cu care funcționează routerul la momentul respectiv
5.	Kernel Version	3.10.36	Versiunea nucleului Linux ce rulează pe router la momentul respectiv
6.	Local Time Ora locală	2016-05-24, 11:01:14	Arată data și ora curente ale sistemului
7.	Uptime Durată funcționare	0d 0h 42m 1s (since 2016-05-24, 10:19:03)	Arată cât timp a trecut de la pornirea routerului. Repornirile resetează acest cronometru la 0
8.	Load Average Încărcare medie	1 min: 99%; 5 mins: 63%; 15 mins: 35%	Arată cât de ocupat este routerul
9.	Temperature	34,9° C	Temperatura dispozitivului

Detalierea secțiunii Memory | Memorie |:

	Nume câmp	Valoare în exemplu	Explicație
1.	Free	84868 kB / 126556 kB (67%)	Câtă memorie este liberă
2.	Cached În cache	14740 kB / 126556 kB (11%)	Memoria dedicată stocării datelor accesate frecvent
3.	Buffered În buffer	5476 kB / 126556 kB (4%)	Dimensiunea zonei în care datele sunt stocate temporar înainte de mutarea în altă locație

6.3 Informații despre rețele

6.3.1 Rețeaua de telefonie mobilă

Fereastra Mobile Information | Informații rețea telefonie mobilă | afișează informații despre conexiunea la rețeaua de telefonie mobilă.

The screenshot shows the 'Mobile' tab selected in the navigation bar. The main section is titled 'Mobile Information' and displays the following data:

Mobile		SIM card slot in use: SIM 1
Data connection state	Connected	
IMEI	861107030078134	
IMSI	246012101922859	
ICCID	89370010100019228599	
Sim card state	Ready	
Signal strength	-59 dBm	
Cell ID	46479903	
RSRP	-86 dBm	
RSRQ	-11 dB	
SINR	12.9 dB	

Informații despre rețeaua de telefonie mobilă:

	Nume câmp	Valoare în exemplu	Explicație
1.	Data connection state	Connected Conectată	Starea conexiunii de date mobile
2.	IMEI	861107030078134	Numărul IMEI (International Mobile Equipment Identity) al modemului
3.	IMSI	246020100944448	IMSI (International Mobile Subscriber Identity) se folosește pentru identificarea utilizatorului într-o rețea celulară
4.	SIM card state	Ready Pregătită	Indică starea cartelei SIM, de ex. PIN required Introduceți PIN , Not inserted Inserați cartela etc.
5.	Signal strength Intensitate semnal	-67 dBm	Indicatorul intensității semnalului recepționat (RSSI). Intensitatea semnalului este măsurată în dBm
6.	Cell ID ID celulă	1037079	Identifierul celulei operatorului la care dispozitivul este conectat la momentul respectiv
7.	RSRP	-95 dBm	Indică puterea recepționată a semnalului de referință
8.	RSRQ	-8 dBm	Indică calitatea recepționată a semnalului de referință
9.	SINR	16.3 dBm	Indică raportul semnal/interferențe plus zgomot

Operator	OMNITEL LT
Operator state	Registered (home)
Connection type	4G (LTE)
Bytes received *	2.1 MB (2244660 bytes)
Bytes sent *	632.0 KB (647137 bytes)

Reboot modem **Restart connection** **(Re)register** **Refresh**

*Your carrier's data usage accounting may differ. Teltonika is not liable should any accounting discrepancies occur.

Teltonika solutions

www.teltonika.lt

10.	Operator	LT BITE GSM	Denumirea operatorului de telefonie mobilă
11.	Operator state Stare operator	Registered (home) Înregistrat (rețea proprie)	Starea rețelei GSM
12.	Connection type Tip conexiune	4G (LTE)	Indică tehnologia de acces a rețelei GSM
13.	Bytes received	15.7 MB (16453520 bytes)	Numărul de octeți recepționați prin conexiunea de date mobilă
14.	Bytes sent	624.0 KB (638962 bytes)	Numărul de octeți transmiși prin conexiunea de date mobilă
15.	Reboot modem Reporuire modem	-	Repornește modemul
16.	Restart connection	-	Restartează conexiunea mobilă
17.	(Re)register	-	Reînregistrează cartela SIM la un operator de rețea
18.	Refresh	-	Reîmprospătează fereastra Mobile Information

6.3.2 WAN

Fereastra WAN Information | Informații WAN| afișează informații despre conexiunea WAN curentă.

Nume câmp	Valoare în exemplu	Explicație
1. Interface	Mobile	Specifică interfața prin care routerul se conectează la internet. Aceasta poate fi Wired Cablu , Mobile Telefonie mobilă ori Wi-Fi
2. Type* Tip	Qmi2	Specifică tipul conexiunii
3. IP address	188.69.245.225	Adresa IP folosită de router pentru a se conecta la internet
4. Netmask Mască rețea	255.255.255.252	Specifică o mască folosită pentru a defini dimensiunea rețelei WAN
5. Gateway	188.69.245.226	Adresa la care este rutat traficul către internet
6. DNS 1 DNS 2	194.176.32.129 195.22.175.1	Serverul/serverele de nume de domeniu
7. Connected Conectat	0h 0m 56s	Timpul cât conexiunea a fost menținută cu succes
8. Ports	-	O indicare vizuală a porturilor folosite la momentul respectiv
9. Backup WAN Status	READY Pregătită	Indică starea rețelei WAN de backup
10. Refresh	-	Reîmprospătează fereastra WAN Information

Informații despre WAN:

	Nume câmp	Valoare în exemplu	Explicație
1.	Interface	Mobile	Specifică interfața prin care routerul se conectează la internet. Aceasta poate fi Wired Cablu , Mobile Telefonie mobilă ori Wi-Fi
2.	Type* Tip	Qmi2	Specifică tipul conexiunii
3.	IP address	188.69.245.225	Adresa IP folosită de router pentru a se conecta la internet
4.	Netmask Mască rețea	255.255.255.252	Specifică o mască folosită pentru a defini dimensiunea rețelei WAN
5.	Gateway	188.69.245.226	Adresa la care este rutat traficul către internet
6.	DNS 1 DNS 2	194.176.32.129 195.22.175.1	Serverul/serverele de nume de domeniu
7.	Connected Conectat	0h 0m 56s	Timpul cât conexiunea a fost menținută cu succes
8.	Ports	-	O indicare vizuală a porturilor folosite la momentul respectiv
9.	Backup WAN Status	READY Pregătită	Indică starea rețelei WAN de backup
10.	Refresh	-	Reîmprospătează fereastra WAN Information

* Când folosiți o interfață WAN diferită, acest câmp arată tipul de protocol utilizat. Poate fi DHCP, Static sau PPPoE.

6.3.3 LAN

Fereastra LAN Information | Informații LAN| afișează informații despre conexiunile LAN.

Secțiunea LAN Information:

	Nume câmp	Valoare în exemplu	Explicație
1.	Name	Lan	Numele instanței LAN
2.	IP address	192.168.56.1	Adresa utilizată de router în rețeaua LAN
3.	Netmask	255.255.255.0	O mască folosită pentru a defini dimensiunea rețelei LAN
4.	Ethernet MAC address	00:51:33:77:56:16	Adresa MAC (Media Access Control) folosită pentru comunicare în cadrul unei rețele LAN Ethernet
5.	Connected for Conectată timp de	4h 38m 24s	Timpul cât rețeaua LAN a fost menținută cu succes

Secțiunea DHCP Leases / Închirieri DHCP

Dacă serverul Dvs. DHCP este activat, acest câmp va arăta câte dispozitive au primit o adresă IP, precum și adresele IP respective.

	Nume câmp	Valoare în exemplu	Explicație
1.	Hostname	DESKTOP-69EIUGN	Numele de gază al clientului DHCP
2.	IP address	192.168.56.124	Adresa IP a unuia dintre dispozitivele conectate la LAN
3.	LAN name	Lan	Numele instanței LAN
4.	MAC address	18:66:DA:28:6A:34	Adresa MAC a interfeței de rețea pe care va fi folosită închirierea
5.	Lease time remaining	11h 52m 57s	Perioada de închiriere rămasă pentru adresele alocate clientilor
6.	Ports	-	O indicare vizuală a porturilor folosite la momentul respectiv
7.	Refresh Reîmprospătare	-	Reîmprospătează fereastra LAN Information

6.3.4 Wireless

Conexiunea wireless poate opera în două moduri: Access Point (AP) |Punct acces| ori Station (STA) |Stație|. În modul AP conexiunea radio wireless este utilizată pentru a crea un punct de acces la care se pot conecta alte dispozitive. În modul STA conexiunea radio a routerului este utilizată pentru conectarea la alt punct de acces prin WAN.

6.3.4.1 Modul Station

Fereastra Wireless Information |Informații wireless| afișează informații despre conexiunile wireless (în modul Station).

The screenshot shows the 'Wireless Information' section of the Teltonika RUT955 web interface. At the top, there's a navigation bar with tabs: Mobile, WAN, LAN, **Wireless**, OpenVPN, VRRP, Topology, and Access. The 'Wireless' tab is selected. Below the navigation bar, the title 'Wireless Information' is displayed. The page is divided into several sections:

- Wireless Information:** Shows Channel (6 (2.44 GHz)) and Country code (00 (World)).
- Wireless Status:** A table showing two entries:

SSID	Mode	Encryption	Wireless MAC	Signal quality	Bit rate
GG	Station (STA)	WPA2 PSK (CCMP)	C0:11:73:94:E8:E5	100%	72.2 Mbit/s
HAL10000	Access Point (AP)	mixed WPA/WPA2 PSK (CCMP)	02:51:33:77:56:18	0%	N/A
- Associated Stations:** A table showing one entry:

MAC address	Device name	Signal	RX rate	TX rate
C0:11:73:94:E8:E5	?	-50 dBm	72.2 Mbit/s, MCS 7, 20MHz	72.2 Mbit/s, MCS 7, 20MHz

At the bottom right of the main content area is a 'Refresh' button.

Informații în modul client

	Nume câmp	Valoare în exemplu	Explicație
1.	Channel	6 (2.44 GHz)	Canalul utilizat de punctul de acces la care este conectat routerul. Interfața Dvs. radio wireless este forțată să opereze pe acest canal pentru a menține conexiunea
2.	Country code	00 (World)	Codul de țară
3.	SSID	GG	SSID-ul utilizat de punctul de acces la care este conectat routerul
4.	Mode	Station (STA)	Indică dacă routerul este clientul vreunui punct de acces local
5.	Encryption	WPA2 PSK (CCMP)	Tipul de criptare utilizată de punctul de acces
6.	Wireless MAC	C0:11:73:94:E8:E5	Adresa MAC a interfeței radio a punctului de acces
7.	Signal Quality	100%	Calitatea semnalului între interfața radio a routerului și un alt dispozitiv care se conectează la router. Se va afișa 0% dacă niciun dispozitiv nu încearcă să se conecteze sau nu menține o conexiune la momentul respectiv
8.	Bit rate Rată de biți	72.2 Mbit/s	Traficul maxim pe care îl poate gestiona interfața radio a routerului. Tineți cont că această valoare este cumulativă – rata de biți va fi împărțită între router și orice alte dispozitive care se conectează la punctul de acces local

6.3.4.2 Modul Access Point

Fereastra Wireless Information afișează informații despre conexiunile wireless (în modul Access Point).

The screenshot shows the 'Wireless Information' page of the Teltonika RUT955 interface. It includes sections for 'Wireless Information' (Channel: 11 (2.46 GHz), Country code: 00 (World)), 'Wireless Status' (SSID: HAL10000, Mode: Access Point (AP), Encryption: mixed WPA/WPA2 PSK (CCMP), Wireless MAC: 00:51:33:77:56:18, Signal quality: 73%, Bit rate: 57.8 Mbit/s), and 'Associated Stations' (MAC address: 1C:7B:21:58:69:C3, Device name: android-3757690c5aecac34, Signal: -59 dBm, RX rate: 6.0 Mbit/s, MCS 0, 20MHz, TX rate: 57.8 Mbit/s, MCS 5, 20MHz). A 'Refresh' button is located at the bottom right.

Informații despre punctul de acces wireless

	Nume câmp	Valoare în exemplu	Explicație
1.	Channel	11 (2.46 GHz)	Canalul utilizat pentru difuzarea SSID-ului și pentru stabilirea de noi conexiuni către dispozitive
2.	Country code	00 (World)	Codul de țară
3.	SSID	HAL10000	SSID-ul este un nume prin care alte dispozitive vor recunoaște routerul
4.	Mode	Access Point (AP)	Indică faptul că routerul Dvs. este un punct de acces
5.	Encryption	Mixed WPA/WPA2 PSK (CCMP)	Tipul de criptare utilizată de router pentru autentificarea, stabilirea și menținerea conexiunilor
6.	Wireless MAC	00:51:33:77:56:18	Adresa MAC a interfeței radio a punctului de acces
7.	Signal Quality	73%	Calitatea semnalului între interfața radio a routerului și un alt dispozitiv conectat la router. Se va afișa 0% dacă niciun dispozitiv nu încearcă să se conecteze sau nu menține o conexiune la momentul respectiv
8.	Bit rate	57.8 Mbit/s	Rata de biți împărțită între toate dispozitivele conectate la rețea wireless a routerului

Stații asociate -Associated stations-*

	Nume câmp	Valoare în exemplu	Explicație
1.	MAC Address	1C:7B:21:58:69:C3	Adresa MAC a stației asociate
2.	Device Name Nume dispozitiv	android-3757690c5aecac34	Numele de gază al clientului DHCP
3.	Signal	-59 dBm	Indicatorul intensității semnalului recepționat (RSSI)
4.	RX Rate Rată recepție	6.0Mbit/s, MCS 5, 20MHz	Rata la care sunt recepționate pachetele de la stația asociată
5.	TX Rate Rată transmisie	57.8Mbit/s, MCS 5, 20MHz	Rata la care sunt transmise pachetele către stația asociată

* Fie informații despre punctul de acces la care este conectat routerul în modul STA, fie lista tuturor dispozitivelor conectate la punctul de acces al routerului.

6.3.5 Clientul OpenVPN

Fereastra OpenVPN Information | Informații OpenVPN | afișează informații despre clientul ori serverul OpenVPN.

OpenVPN Information

Client_Client1

OpenVPN	
Enabled	Yes
Status	Connected
Type	Client
IP	10.0.0.6
Mask	255.255.255.255
Time	0h 0m 16s

Refresh

	Nume câmp	Valoare în exemplu	Explicație
1.	Enabled Activat	Yes Da	Starea OpenVPN
2.	Status	Connected Conectat	Starea conexiunii
3.	Type	Client	Tipul instanței OpenVPN care a fost creată
4.	IP	10.0.0.6	Adresa IP a rețelei virtuale de la distanță
5.	Mask	255.255.255.255	Masca de subretea a rețelei virtuale de la distanță
6.	Time	0h 0m 16s	Durata conexiunii

6.3.6 Serverul OpenVPN

 [Status](#) [Network](#) [Services](#) [System](#) [Logout](#)

[Mobile](#) [WAN](#) [LAN](#) [Wireless](#) [OpenVPN](#) [VRRP](#) [Topology](#) [Access](#)

OpenVPN Information

[Server_Server](#)

OpenVPN	
Enabled	Yes
Status	Connected
Type	Server
IP	10.0.0.1
Mask	255.255.255.255
Time	0h 0m 24s

Clients Information			
Common Name	Real Address	Virtual Address	Connection Since
			Refresh

	Nume câmp	Valoare în exemplu	Explicație
1.	Enabled	Yes	Starea OpenVPN
2.	Status	Connected	Starea conexiunii
2.	Type	Server	Tipul instanței OpenVPN care a fost creată
3.	IP	10.0.0.1	Adresa IP a rețelei virtuale de la distanță
4.	Mask	255.255.255.255	Masca de subreștea a rețelei virtuale de la distanță
5.	Time	0h 0m 28s	Durata conexiunii

Informații despre clienti -Clients Information-*

	Nume câmp	Valori posibile	Explicație
1.	Common Name	Test001	Numele obișnuit al clientului
2.	Real Address Adresă reală	212.59.13.225:52638	Adresa IP a clientului și numărul portului
3.	Virtual Address	10.0.0.6	Adresa virtuală alocată unui client
4.	Connection Since Conexiune de la	Thu May 05 2016 07:46:29 GMT + 0300 (FLE Standard Time)	Momentul stabilirii conexiunii

* Fereastra OpenVPN Information afișează și informații privind clienții conectați atunci când o instanță de server TLS OpenVPN este online.

6.3.7 VRRP

Fereastra VRRP Information | Informații VRRP| afișează starea rețelei LAN ce utilizează protocolul VRRP (Virtual Router Redundancy Protocol).

VRRP LAN Status

Status	Enabled
Virtual ip	192.168.1.253
Priority	100
Router	Master

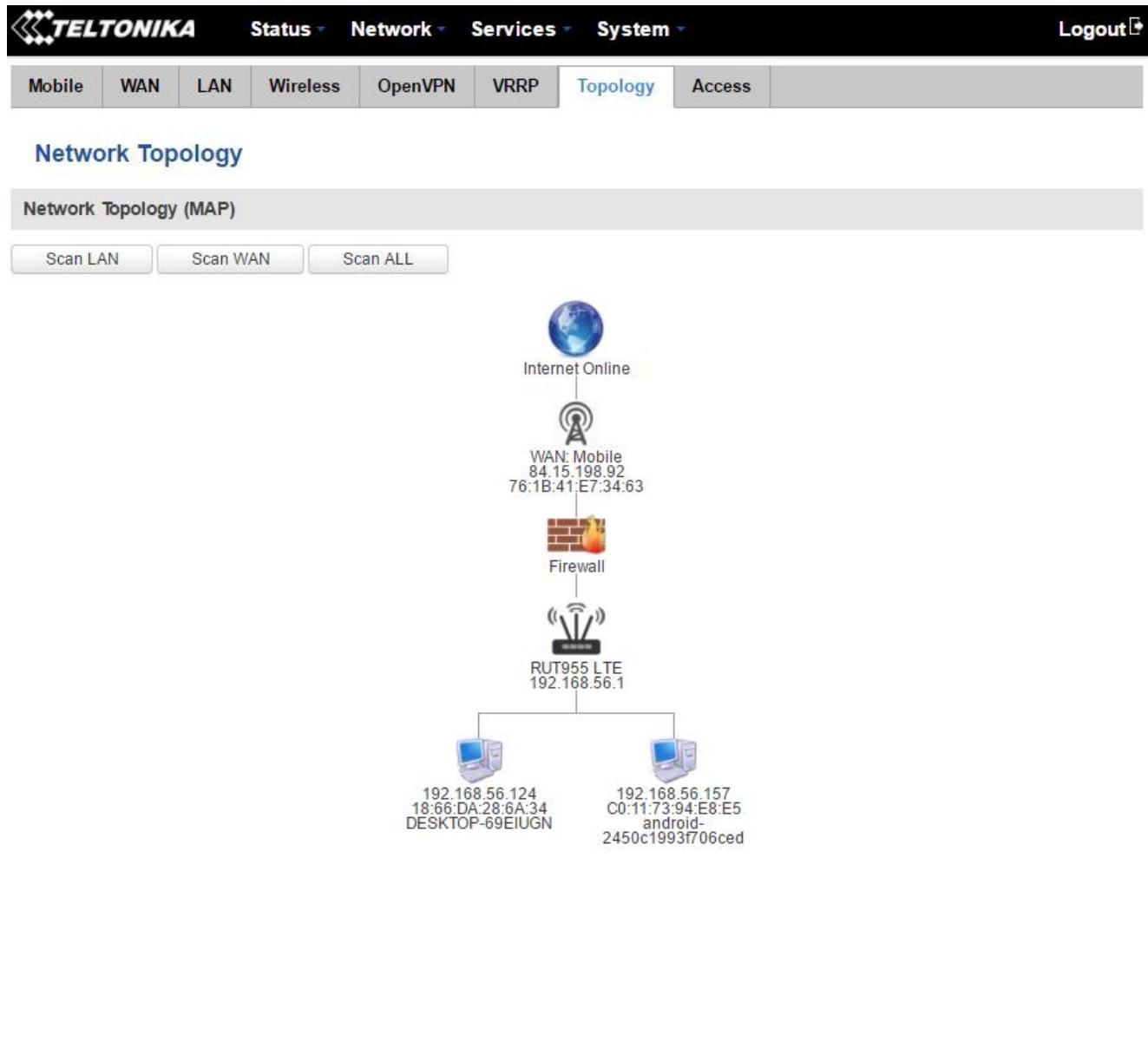
Refresh

	Nume câmp	Valoare în exemplu	Explicație
1.	Status	Enabled Activat	Starea protocolului VRRP
2.	Virtual IP	192.168.1.253	Adresa/adresele IP virtuală/e pentru clusterul VRRP al rețelei LAN
3.	Priority Prioritate	100	Routerul cu cea mai mare valoare a priorității din același cluster VRRP va acționa ca master; domeniul [1 – 255]
4.	Router*	Master	Modul de conectare

*Exclusiv în alte moduri cu slaves

6.3.8 Topologia

Fereastra Network Topology |Topologie rețea| vă oferă posibilitatea să scanați și să obțineți rapid informații despre dispozitivele din rețeaua Dvs. Când routerul folosește rețeaua de telefonie mobilă pentru WAN iar tipul de conexiune selectat este „PPP“, puteți scana numai partea de LAN.



6.3.9 Acces

6.3.9.1 Starea accesului

Fereastra Access Status |Stare acces| afișează informații despre conexiunile SSH, HTTP și HTTPS active, locale și la distanță.

The screenshot shows the 'Access Status' section of the Teltonika RUT955 web interface. It includes tabs for 'Access Information' and 'Last Connections'. The 'Access Information' tab is selected, displaying two tables: 'Local Access' and 'Remote Access'. Both tables have columns for Type, Status, Port, and Active connections. In the 'Local Access' table, all three types (SSH, HTTP, HTTPS) are enabled. In the 'Remote Access' table, all three types are disabled. A 'Refresh' button is located at the bottom right of the table area.

Local Access			
Type	Status	Port	Active connections
SSH	Enabled	22	0 (0.00 B)
HTTP	Enabled	80	1 (53.28 KB)
HTTPS	Enabled	443	0 (0.00 B)

Remote Access			
Type	Status	Port	Active connections
SSH	Disabled	22	0 (0.00 B)
HTTP	Disabled	80	0 (0.00 B)
HTTPS	Disabled	443	0 (0.00 B)

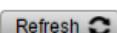
	Nume câmp	Valori posibile	Explicație
1.	Type	SSH; HTTP; HTTPS	Tipul de protocol de conectare
2.	Status	Disabled/Enabled Dezactivat/Activat	Starea conexiunii
3.	Port	22; 80; 443	Portul utilizat pentru conectare
4.	Active connections Conexiuni active	0(0.00B);1(53.28 KB); 0(0.00 B)	Numărul conexiunilor active și cantitatea de date transmise

6.3.9.2 Ultimele conexiuni

Fereastra Last Connections |Ultimele conexiuni| afișează informații despre ultimele 3 conexiuni pentru fiecare dintre diferitele tipuri de conexiuni.

Last Local Connections			
Type	Date	IP	Authentications Status
SSH	2017-06-07 14:04:28 2017-06-07 14:52:16 2017-06-07 15:06:51	192.168.56.205 192.168.56.124 192.168.56.124	Succeeded Succeeded Succeeded
HTTP	2017-06-07 15:06:17 2017-06-08 07:33:25 2017-06-08 13:50:09	192.168.56.124 192.168.56.124 192.168.56.124	Succeeded Succeeded Succeeded
HTTPS	<i>There are no records yet.</i>		

Last Remote Connections			
Type	Date	IP	Authentications Status
SSH	2017-06-07 14:06:08 2017-06-07 14:06:09 2017-06-07 14:06:10	171.109.105.59 171.109.105.59 171.109.105.59	Failed Failed Failed
HTTP	2017-05-24 16:14:37 2017-05-25 14:54:19 2017-06-01 13:16:30	158.129.22.189 188.69.236.204 88.119.152.93	Failed Succeeded Succeeded
HTTPS	<i>There are no records yet.</i>		



	Nume câmp	Valori posibile	Explicație
1.	Type	SSH; HTTP; HTTPS	Tipul de protocol de conectare
2.	Date	2016-03-03, 13:40:59	Data și ora conectării
3.	IP	192.168.56.205	Adresa IP de la care s-a realizat conectarea
4.	Authentications Status Stare autentificări	Failed Eșuată ; Succeeded Cu succes	Rezultatul încercării de autentificare

6.4 Informații despre dispozitiv

Pagina Device Information | Informații dispozitiv| afișează informațiile din fabrică care au fost scrise în dispozitiv în timpul procesului de fabricare.

The screenshot shows the 'Device Information' page from the Teltonika web interface. It includes sections for 'Device' and 'Modem' with various configuration parameters.

Device	
Serial number	54656555
Product code	RUT955H7V020
Batch number	0001
Hardware revision	0002
IMEI	861107030078134
IMSI	246012101922859
Ethernet LAN MAC address	00:51:33:77:56:16
Ethernet WAN MAC address	00:51:33:77:56:17
Wireless MAC address	00:51:33:77:56:18

Modem	
Model	EC25
FW version	EC25EFAR02A03M4G

	Nume câmp	Valoare în exemplu	Explicație
1.	Serial number	54656	Numărul de serie al dispozitivului
2.	Product code	RUT955H7V020	Codul de produs al dispozitivului
3.	Batch number	0001	Numărul de lot folosit în cursul procesului de fabricare a produsului
4.	Hardware revision	0002	Revizia hardware a dispozitivului
5.	IMEI	861107030078134	Numărul de identificare a modemului intern
6.	IMSI	246020100944448	Numărul de identificare al abonatului al modemului intern
6.	Ethernet LAN MAC	00:51:33:77:56:16	Adresa MAC a porturilor Ethernet pentru LAN
7.	Ethernet WAN MAC	00:51:33:77:56:17	Adresa MAC a portului Ethernet pentru WAN
8.	Wireless MAC	00:51:33:77:56:18	Adresa MAC a interfeței Wi-Fi
9.	Model	EC25	Modelul modemului routerului
10.	FW version	EC25EFAR02A03M4G	Versiunea de firmware a modemului routerului

6.5 Servicii

Pagina Services |Servicii| afișează starea serviciilor disponibile și vă oferă posibilitatea să le porniți/opriți ori să le reporniți.

The screenshot shows the 'Services' section of the Teltonika RUT955 web interface. At the top, there is a navigation bar with the Teltonika logo, 'Status', 'Network', 'Services', 'System', and 'Logout'. Below the navigation bar, the title 'Services' is displayed. A table titled 'Services Status' lists various services with their current status and a 'Restart' button. The table is divided into two columns. The first column contains: VRRP LAN (Disabled), OpenVPN servers (Enabled), OpenVPN clients (Disabled), SNMP agent (Disabled), SNMP trap (Disabled), NTP client (Enabled), IPsec (Disabled), Ping reboot (Disabled), and Input/Output rules (Disabled). The second column contains: DDNS (Disabled), Site blocking (Disabled), Content blocker (Disabled), SMS utils rules (Enabled), Hotspot (Disabled), Hotspot logging (Disabled), GRE tunnel (Disabled), QoS (Disabled), and GPS (Disabled). A 'Refresh' button is located at the bottom right of the table area.

Services Status		
VRRP LAN	Disabled	Restart
OpenVPN servers	Enabled	Restart
OpenVPN clients	Disabled	Restart
SNMP agent	Disabled	Restart
SNMP trap	Disabled	Restart
NTP client	Enabled	Restart
IPsec	Disabled	Restart
Ping reboot	Disabled	Restart
Input/Output rules	Disabled	Restart
DDNS	Disabled	Restart
Site blocking	Disabled	Restart
Content blocker	Disabled	Restart
SMS utils rules	Enabled	Restart
Hotspot	Disabled	Restart
Hotspot logging	Disabled	Restart
GRE tunnel	Disabled	Restart
QoS	Disabled	Restart
GPS	Disabled	Restart

[Refresh](#)

6.6 Rute

Pagina Routes | Rute| afișează tabela ARP a routerului și rutele IP și IPv6 active.

6.6.1 ARP

Tabela ARP conține adresele MAC ale fiecărui dispozitiv imediat care a comunicat cu routerul, stocate recent în memoria cache.



Routes

ARP		
IP address	MAC address	Interface
192.168.90.230	D0:50:99:40:91:CE	eth1
192.168.90.254	F0:9F:C2:10:A2:78	eth1
192.168.56.124	18:66:DA:28:6A:34	br-lan

	Nume câmp	Valoare în exemplu	Explicație
1.	IP address	192.168.56.235	Adresele IP ale fiecărui dispozitiv imediat care a comunicat cu routerul, stocate recent în memoria cache
2.	MAC address	1C:7B:21:58:69:C3	Adresele MAC ale fiecărui dispozitiv imediat care a comunicat cu routerul, stocate recent în memoria cache
3.	Interface	br-lan	Interfață utilizată de dispozitiv pentru conectare

6.6.2 Rute IP active

Secțiunea Active IP Routes | Rute IP active| afișează tabela de rutare a routerului. Tabela de rutare indică unde va fi direcționat un pachet TCP/IP cu o anumită adresă IP.

Active IP Routes			
Network	Target	IP gateway	Metric
wan	0.0.0.0/0	192.168.90.254	0
tun_rms	10.100.96.0	0.0.0.0	0
tun_rms	10.100.96.0/19	10.100.96.0	0
lan	192.168.56.0/24	0.0.0.0	0
wan	192.168.90.0/24	0.0.0.0	0

	Nume câmp	Valoare în exemplu	Explicație
1.	Network Rețea	wan	Interfață prin care se transmit pachetele TCP/IP
2.	Target Tintă	0.0.0.0	Indică unde va fi direcționat un pachet TCP/IP cu o anumită adresă IP
3.	IP gateway	192.168.90.254	Indică prin ce gateway va fi direcționat un pachet TCP/IP
4.	Metric	0	Indică prioritatea în utilizare a interfeței

6.6.3 Rute IPv6 active

Tabela Active IPv6-Routes | Rute IPv6 active| conține rutele IPv6 active pentru tranzitul pachetelor de date.

Active IPv6-Routes			
Network	Target	IPv6 gateway	Metric
loopback	0:0:0:0:0:0:0/0	0:0:0:0:0:0:0/0	FFFFFFFFF
loopback	0:0:0:0:0:0:0/0	0:0:0:0:0:0:0/0	FFFFFFFFF
loopback	0:0:0:0:0:0:1	0:0:0:0:0:0:0/0	00000000
wan	FF02:0:0:0:0:0:C	0:0:0:0:0:0:0/0	00000000
wan	FF02:0:0:0:0:0:FB	0:0:0:0:0:0:0/0	00000000
wan	FF02:0:0:0:0:1:2	0:0:0:0:0:0:0/0	00000000
wan	FF02:0:0:0:0:1:3	0:0:0:0:0:0:0/0	00000000
wan	FF02:0:0:0:1:FF9C:DCEF	0:0:0:0:0:0:0/0	00000000
wan	FF02:0:0:0:1:FFE5:F7AD	0:0:0:0:0:0:0/0	00000000
wan	FF00:0:0:0:0:0:0/8	0:0:0:0:0:0:0/0	00000100
loopback	0:0:0:0:0:0:0/0	0:0:0:0:0:0:0/0	FFFFFFFFF

Teltonika solutions

www.teltonika.lt

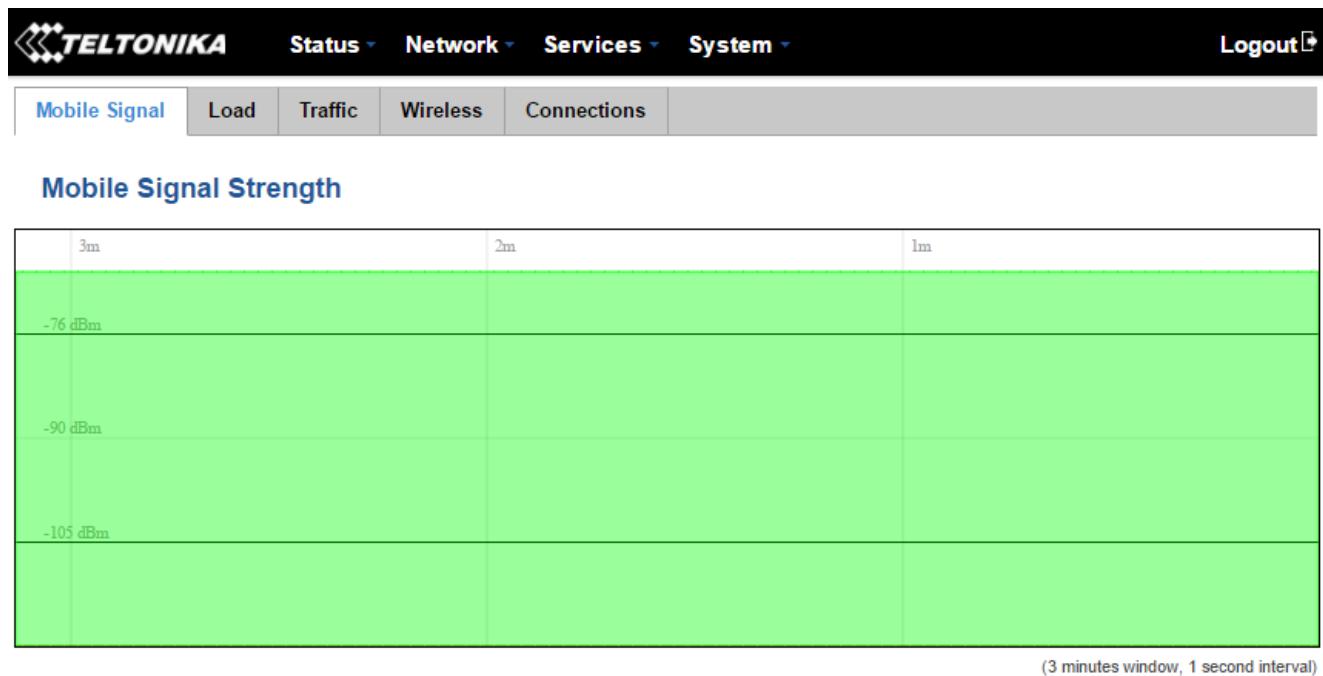
	Nume câmp	Valoare în exemplu	Explicație
1.	Network	loopback	Interfața de rețea folosită
2.	Target	0:0:0:0:0:0:0/0	Indică unde va fi direcționat un pachet TCP/IP cu o anumită adresă IP
3.	IPv6 gateway	0:0:0:0:0:0:0/0	Indică prin ce gateway va fi direcționat un pachet TCP/IP
4.	Metric	FFFFFFFFF	Indică prioritatea în utilizare a interfeței

6.7 Grafice

Fereastra Real-time graph |Grafice în timp real| prezintă sub formă de grafice modificările în timp ale diverselor date statistice.

6.7.1 Intensitatea semnalului rețelei de telefonie mobilă

Graficul Mobile Signal Strength prezintă variația în timp a intensității semnalului rețelei de telefonie mobilă (măsurată în dBm).



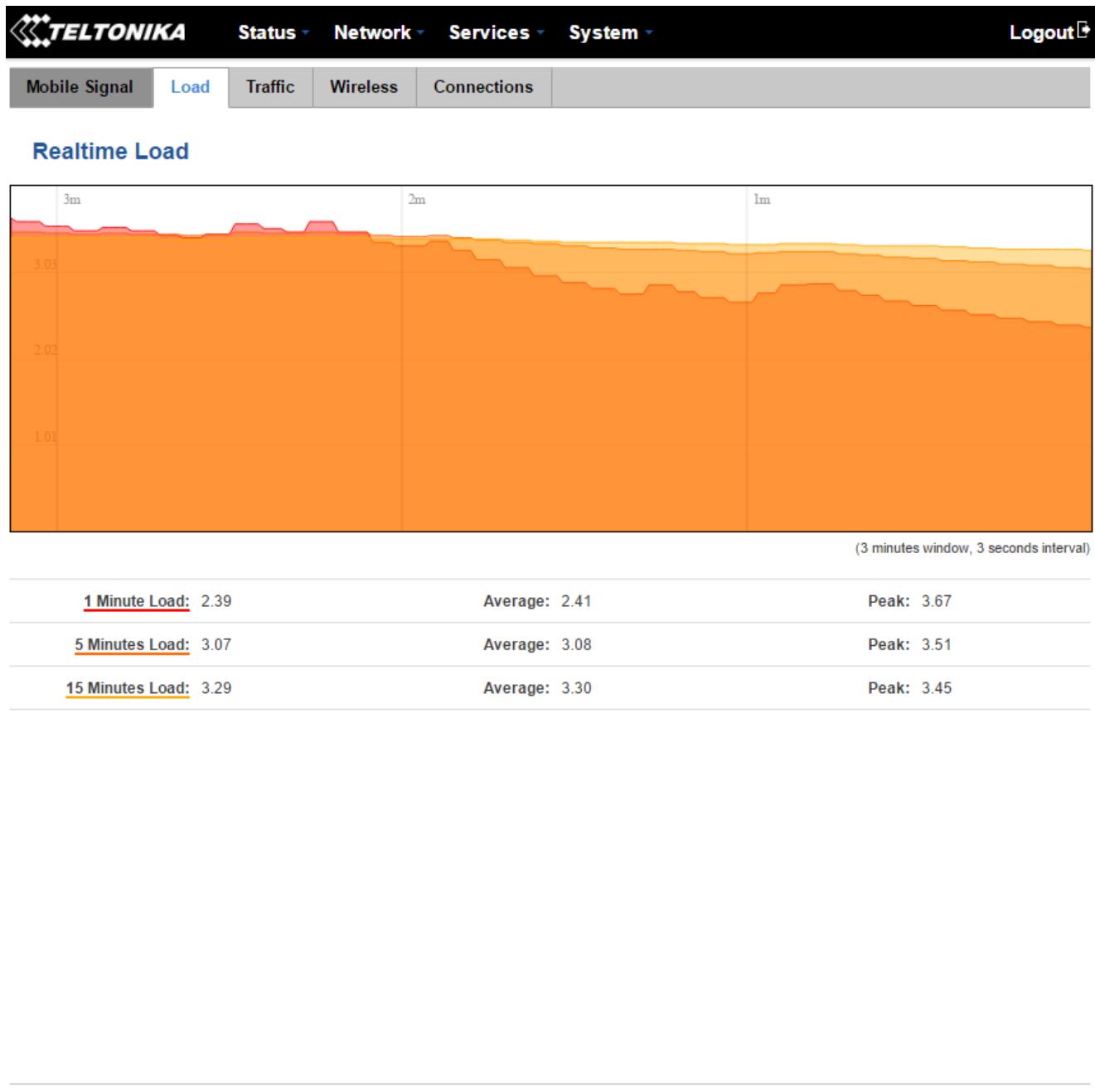
2G (GSM) 2G (GPRS) 2G (EDGE) 3G (WCDMA) 3G (HSDPA)

3G (HSUPA) 3G (HSPA) 3G (HSPA+) 3G (DC-HSPA+) 4G (LTE)

	Nume câmp	Valoare în exemplu	Explicație
1.	Connection type	4G (LTE)	Tipul conexiunii folosite
2.	Signal	-67 dBm	Valoarea curentă a intensității semnalului
3.	Average	-68.2 dBm	Valoarea medie a intensității semnalului
4.	Peak	-61 dBm	Valoarea de vârf a intensității semnalului

6.7.2 Încărcarea în timp real

Fereastra Realtime Load prezintă un grafic triplu ce ilustrează valorile în timp real ale încărcării CPU. Graficul constă în trei grafice de culori diferite, fiecare corespunzând unei încărcări medii a CPU în ultimele 1 (roșu), 5 (portocaliu) și 15 (galben) minute.



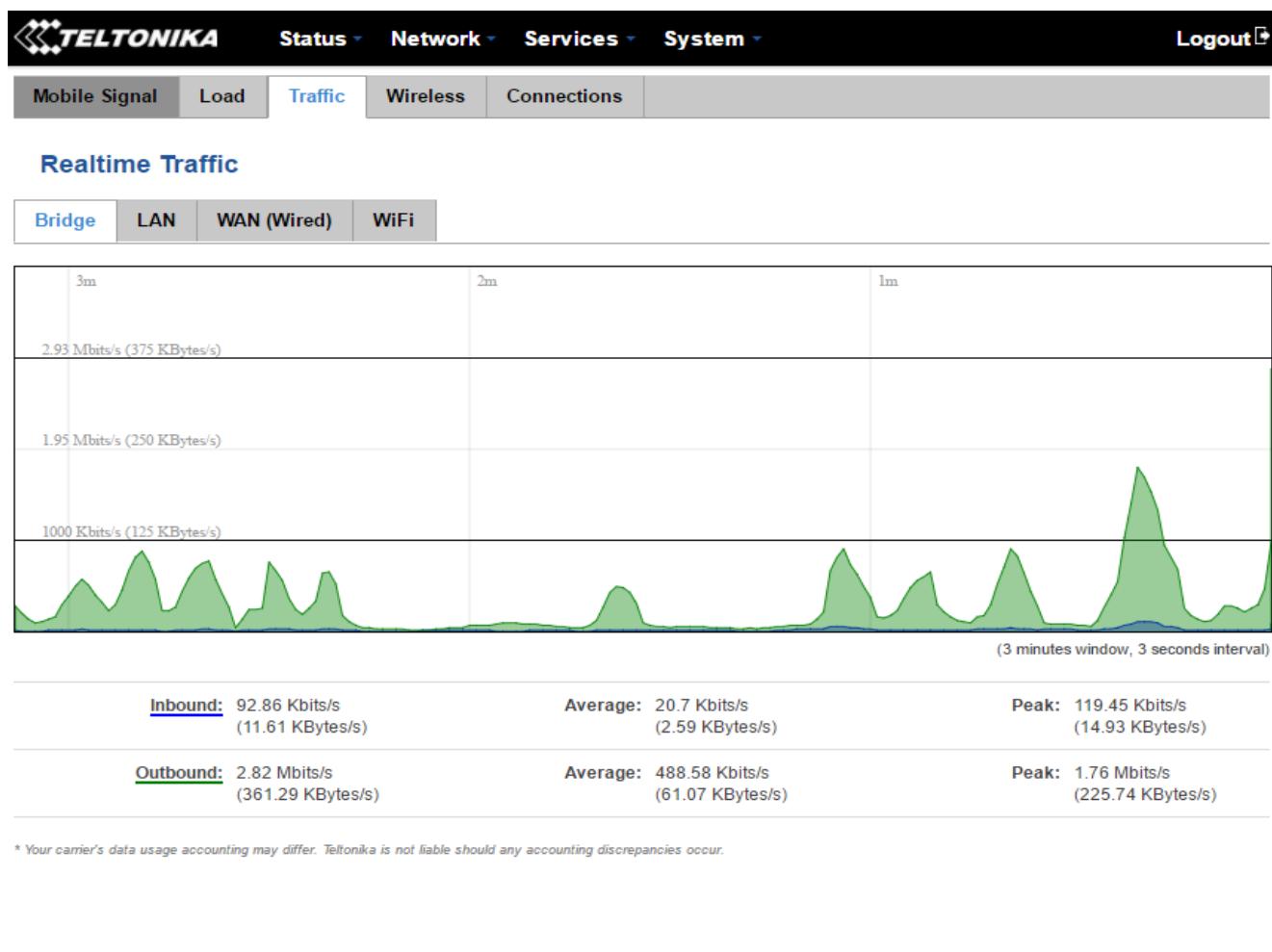
Teltonika solutions

www.teltonika.it

	Nume câmp	Valoare în exemplu	Explicație
1.	1/5/15 Minute Load Încărcare pe 1/5/15 minute	2.39	Intervalul de timp pe care se realizează media, culoarea graficului
2.	Average	2.41	Valoarea medie a încărcării CPU într-un interval de timp (1/5/15 minute)
3.	Peak	3.67	Valoarea de vârf a încărcării CPU în intervalul de timp

6.7.3 Traficul în timp real

Fereastra Realtime Traffic | Trafic în timp real| vă permite să monitorizați traficul mediu de intrare și de ieșire într-un interval de 3 minute; fiecare măsurare nouă se realizează la 3 secunde. Graficul constă în două grafice de culori diferite: graficul verde prezintă traficul de ieșire iar graficul albastru prezintă traficul de intrare. Fără a fi incluse în grafic, pagina afișează și valorile de vârf și medii ale traficului de intrare și de ieșire.



Teltonika solutions

www.teltonika.lt

	Nume câmp	Explicație
1.	Bridge	Grafic cumulativ, cuprinzând rețeaua LAN prin cablu Ethernet și rețeaua wireless
2.	LAN	Prezintă sub formă de grafic traficul total care a trecut prin ambele interfețe ale rețelei LAN
3.	WAN (Wired) (Prin cablu)	Prezintă sub formă de grafic traficul care a trecut prin conexiunea WAN activă la momentul respectiv
4.	Wi-Fi	Prezintă traficul transmis și receptionat prin conexiunea radio wireless

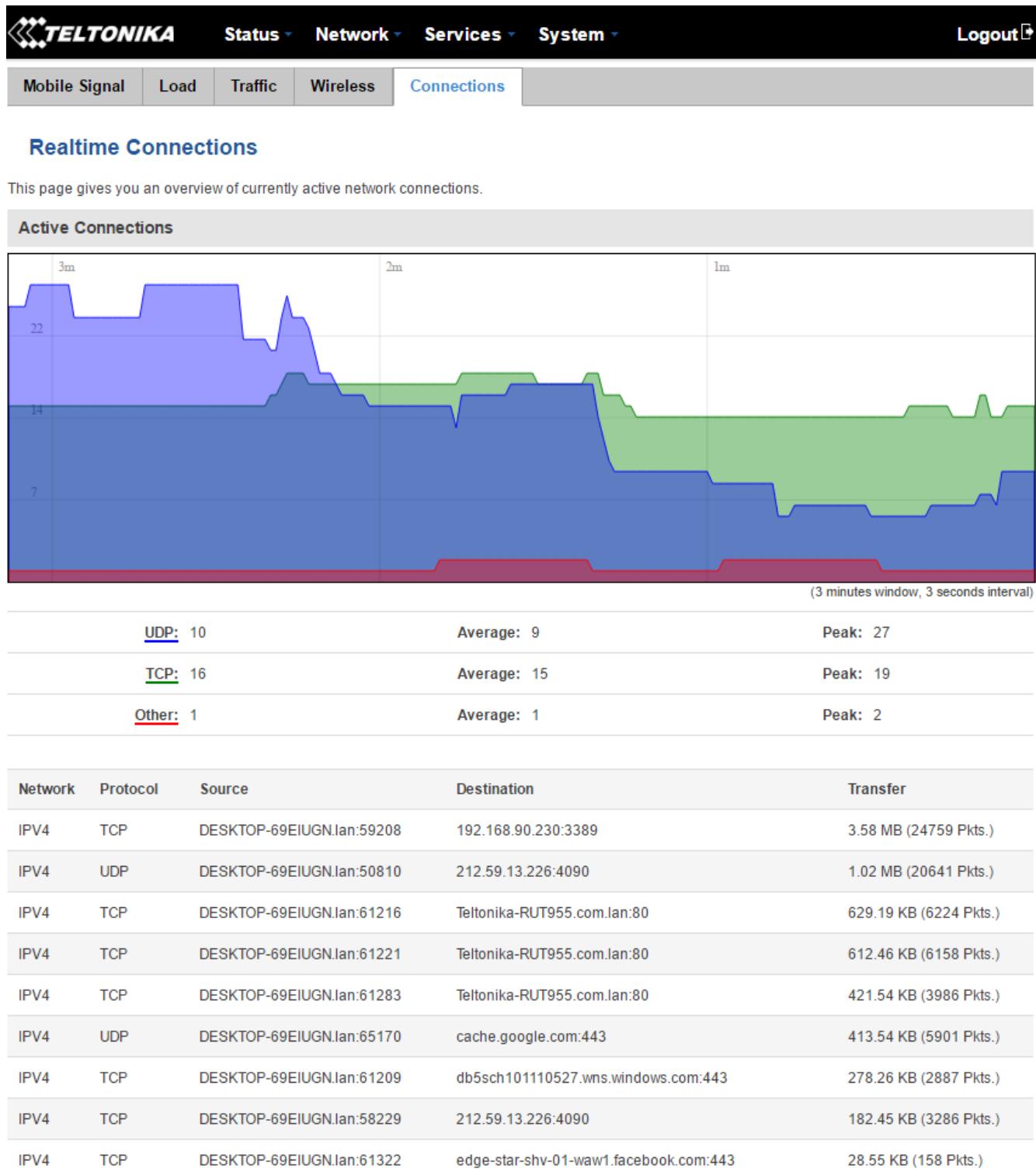
6.7.4 Semnalul wireless în timp real

Fereastra Realtime Wireless afișează intensitatea semnalului radio wireless, zgomotul semnalului, nivelurile medii și de vârf ale semnalului, precum și permeabilitatea maximă teoretică a canalului.



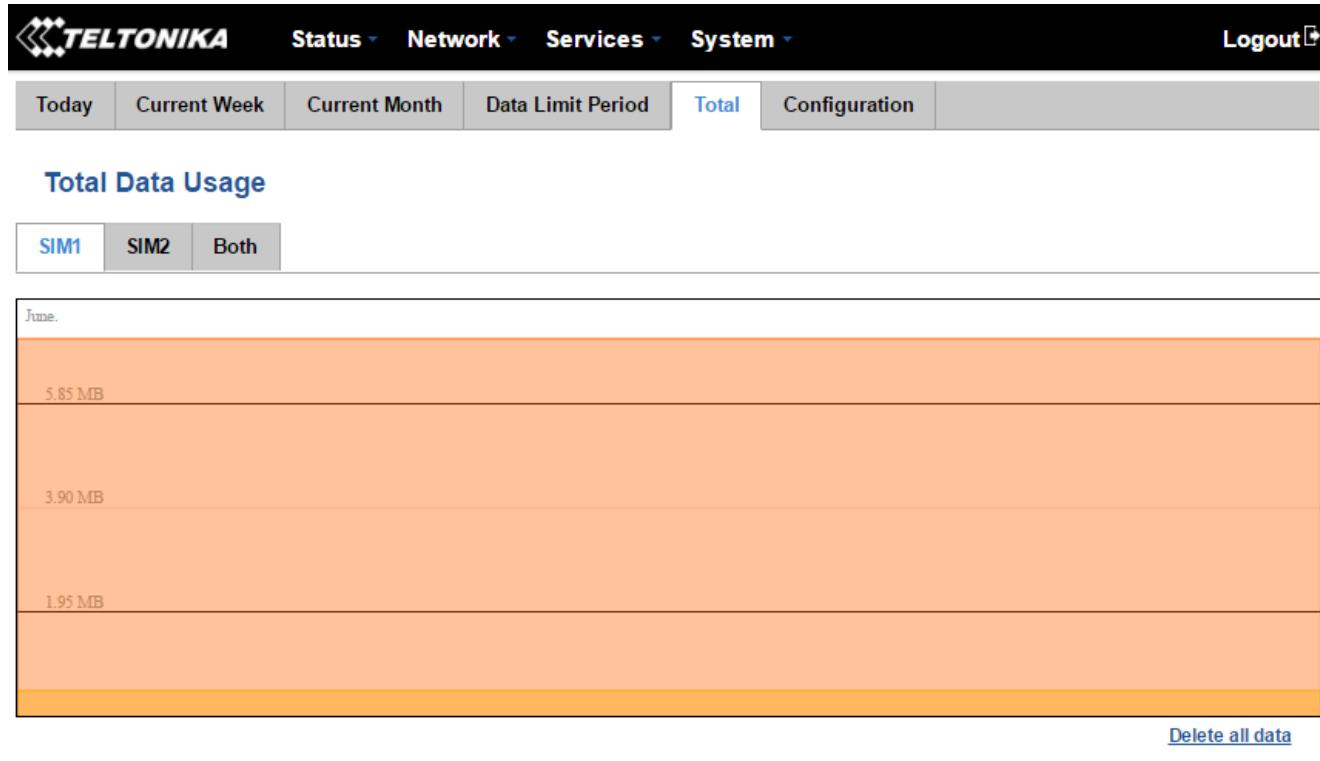
6.7.5 Conexiuni în timp real

Fereastra Realtime Connections afișează conexiunile de rețea active la momentul respectiv, cu informații despre rețea, protocol, adresele sursei și destinației, precum și viteza de transfer.



6.8 Traficul prin rețeaua de telefonie mobilă

Graficele Mobile Traffic |Trafic rețea telefonie mobilă| afișează datele transmise în ziua, săptămâna ori luna curente prin conexiunea la rețeaua de telefonie mobilă, pentru fiecare sau ambele cardurile SIM.



În mod implicit, jurnalizarea traficului prin rețeaua de telefonie mobilă este dezactivată. Pentru a putea folosi această funcție, trebuie să o activați în tab-ul Configuration |Configurare|.

Mobile Traffic Usage Logging

Enable

Interval between records (sec)

[Save](#)

	Nume câmp	Valori posibile	Explicație
1.	Enable	Activare / Dezactivare	Activează sau dezactivează funcția
2.	Interval between records (sec)	(minimum) 60 (sec)	Intervalul în secunde între înregistrările din jurnal

6.9 Jurnalul de evenimente

Ferestrele Events Log | Jurnal evenimente| afișează evidențe ale unor evenimente precum logări, reporniri, resetări, conexiuni și modificări de configurație.

6.9.1 Toate evenimentele

Fereastra All Events afișează toate evenimentele routerului înregistrate, tipurile acestora și momentul producerii.

The screenshot shows the 'Events Log' section of the Teltonika RUT955 web interface. At the top, there's a navigation bar with the Teltonika logo, 'Status', 'Network', 'Services', 'System', and 'Logout'. Below the navigation is a horizontal menu bar with tabs: 'All Events' (selected), 'System Events', 'Network Events', 'Events Reporting', and 'Reporting Configuration'. The main area is titled 'Events Log' and contains a table of network events. The table has columns: ID, Date, Event type, and Event details. The data shows various DHCP lease events and WiFi client connections. At the bottom of the table, it says 'Showing 1 to 10 of 7454 entries' and has a 'Next >>' link.

ID *	Date *	Event type *	Event *
5661N	2017-06-15 08:30:22	WiFi	WiFi client connected: 70:8A:09:1D:81:46 HUAWEI_P9
12597S	2017-06-15 08:30:22	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi
12596S	2017-06-15 08:30:22	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi
5660N	2017-06-15 08:28:01	WiFi	WiFi client disconnected: 70:8A:09:1D:81:46 HUAWEI_P9
12595S	2017-06-15 08:26:31	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi
12594S	2017-06-15 08:26:29	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi
12593S	2017-06-15 08:26:29	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi
5659N	2017-06-15 08:21:07	WiFi	WiFi client connected: 70:8A:09:1D:81:46 HUAWEI_P9
12592S	2017-06-15 08:21:04	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi
12591S	2017-06-15 08:21:03	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi

6.9.2 Evenimente de sistem

Fereastra System Events afișează toate evenimentele de sistem, tipurile acestora și momentul producerii. Aceste evenimente includ: autentificări, solicitări de repornire, mesaje SMS și apeluri primite și efectuate, e-mailuri, modificări de configurație și evenimente DHCP.

ID *	Date *	Event type *	Event *
12601	2017-06-15 08:41:28	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi
12600	2017-06-15 08:41:28	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi
12599	2017-06-15 08:33:55	CONFIG	Mobile Traffic configuration has been changed
12598	2017-06-15 08:33:55	CONFIG	Data Limit configuration has been changed
12597	2017-06-15 08:30:22	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi
12596	2017-06-15 08:30:22	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi
12595	2017-06-15 08:26:31	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi
12594	2017-06-15 08:26:29	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi
12593	2017-06-15 08:26:29	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi
12592	2017-06-15 08:21:04	DHCP	Leased 192.168.56.210 IP address for client 70:8A:09:1D:81:46 - HUAWEI_P9 in WiFi

6.9.3 Evenimente de rețea

Fereastra Network Events afișează informații despre evenimentele de rețea recente, precum noi conectări, modificări ale stării închirierilor, schimbările tipurilor de rețea ori ale operatorilor.

The screenshot shows the Teltonika Network Events interface. At the top, there's a navigation bar with the Teltonika logo, Status, Network, Services, System, and Logout options. Below the navigation bar is a menu bar with All Events, System Events, Network Events (which is highlighted in blue), Events Reporting, and Reporting Configuration. The main content area is titled "Connections Log". It includes a header with "Events per page" set to 10 and a "Search" input field. The data table has columns for ID, Date, Action, and Result. The table lists 10 entries of WiFi client activity from June 15, 2017, at 08:19:45 to 08:41:29, all involving the same HUAWEI_P9 device.

ID *	Date *	Action *	Result *
5663	2017-06-15 08:41:29	WiFi	WiFi client connected: 70:8A:09:1D:81:46 HUAWEI_P9
5662	2017-06-15 08:36:57	WiFi	WiFi client disconnected: 70:8A:09:1D:81:46 HUAWEI_P9
5661	2017-06-15 08:30:22	WiFi	WiFi client connected: 70:8A:09:1D:81:46 HUAWEI_P9
5660	2017-06-15 08:28:01	WiFi	WiFi client disconnected: 70:8A:09:1D:81:46 HUAWEI_P9
5659	2017-06-15 08:21:07	WiFi	WiFi client connected: 70:8A:09:1D:81:46 HUAWEI_P9
5658	2017-06-15 08:20:52	WiFi	WiFi client disconnected: 70:8A:09:1D:81:46 HUAWEI_P9
5657	2017-06-15 08:20:01	WiFi	WiFi client connected: 70:8A:09:1D:81:46 HUAWEI_P9
5656	2017-06-15 08:19:56	WiFi	WiFi client disconnected: 70:8A:09:1D:81:46 HUAWEI_P9
5655	2017-06-15 08:19:50	WiFi	WiFi client connected: 70:8A:09:1D:81:46 HUAWEI_P9
5654	2017-06-15 08:19:45	WiFi	WiFi client disconnected: 70:8A:09:1D:81:46 HUAWEI_P9

Showing 1 to 10 of 3463 entries [Next >>](#)

6.9.4 Raportarea evenimentelor

Pagina Events Reporting | Raportare evenimente| vă permite să configurați reguli pentru a fi informați prin SMS sau e-mail atunci când se produc anumite evenimente în routerul Dvs. Aceste evenimente pot fi aproape orice – modificări de configurație, conectări noi, diverse actualizări de stare, comutări între cartelele SIM etc.

Event type	Event subtype	Action	Enable	Sort
FW upgrade	From file	Send SMS	<input checked="" type="checkbox"/>	Edit Delete
Reboot	After unexpected shut down	Send email	<input checked="" type="checkbox"/>	Edit Delete
SSH	All	Send SMS	<input checked="" type="checkbox"/>	Edit Delete
Config change	OpenVPN	Send SMS	<input checked="" type="checkbox"/>	Edit Delete
Backup	Switched to backup	Send SMS	<input checked="" type="checkbox"/>	Edit Delete

6.9.4.1 Configurarea raportării evenimentelor

Tab-ul Events Reporting Configuration este folosit pentru personalizarea regulilor de raportare a evenimentelor. Aici puteți să specificați orice tip și subtip de eveniment, să alegeti dacă dorîți să fiți informați prin SMS sau e-mail și să modificați tipul de informații pe care dorîți să le primiți la producerea unui eveniment. Pentru a deschide această fereastră, creați o regulă și apăsați “Edit” | Editare|.

Event type	Event subtype	Action	Enable	Sort
Reboot	All	Send SMS	<input type="checkbox"/>	Edit Delete

6.9.4.1.1 Trimitere SMS

Event Reporting Configuration

Modify Event Reporting Rule

Enable

Event type: Reboot

Event subtype: After unexpected shut down

Action: Send SMS

Enable delivery retry

Retry interval: 5 min.

Retry count: 2

Message text on Event:

Router name - %rn; Event type - %et; Event text - %ex; Time stamp - %ts;	Time stamp - %ts Serial number - %sn LAN MAC address - %lm Connection state - %cs Connection type - %ct SIM slot in use - %su Event type - %et FW available on server - %fs Network state - %ns New line - %nl	Router name - %rn WAN MAC address - %wm Curren FW version - %fc Operator name - %on Signal strength - %ss IMSI - %im Event text - %ex LAN IP - %li WAN IP address - %wi
---	---	---

Get status after reboot

Status message after reboot:

Router name - %rn; WAN IP - %wi; Data Connection state - %cs; Connection type - %ct; Signal strength - %ss; New FW available - %fs;	Time stamp - %ts Serial number - %sn LAN MAC address - %lm Connection state - %cs Connection type - %ct SIM slot in use - %su Event type - %et FW available on server - %fs Network state - %ns New line - %nl	Router name - %rn WAN MAC address - %wm Curren FW version - %fc Operator name - %on Signal strength - %ss IMSI - %im Event text - %ex LAN IP - %li WAN IP address - %wi
---	---	---

Recipient's phone number: +37061111111

Back to Overview **Save**

Nume câmp	Valoare în exemplu	Explicație
1. Enable	Activat	Activăți/dezactivați o regulă
2. Event type	Reboot Repornire	Selectați tipul evenimentului despre care doriți să fiți informat
3. Event subtype	After unexpected shut down După oprire neașteptată	Specificați subtipul evenimentului
4. Action	Send SMS Trimite SMS	Acțiunea de executat la producerea evenimentului specificat
5. Enable delivery retry	Activat	Activăți reîncercările de trimitere a SMS-ului în caz de trimitere eşuată

6.	Retry interval Interval reîncercare	5 min.	La cât timp după o trimitere eșuată se inițiază reîncercarea trimiterii
7.	Retry count Număr reîncercări	2	De câte ori se reîncercă trimiterea
8.	Message text on Event Text mesaj la eveniment	Router name Nume router - %rn; Event type Tip eveniment - %et; Event text Text eveniment - %ex; Time stamp Marcă temporală - %ts;	Conținutul mesajului
9.	Get status after reboot	Activat	Indicați dacă doriți să primiți sau nu informații despre starea routerului după repornire
10.	Status message after reboot	Router name - %rn; WAN IP - %wi; Connection state Stare conexiune - %cs; Connection type Tip conexiune - %ct; Signal strength Intensitate semnal - %ss; New FW available Firmware nou disponibil - %fs;	Conținutul mesajului cu starea routerului după repornire
11.	Recipient's phone number Nr. telefon destinatar	+37061111111	Numărul de telefon care va primi mesajul după producerea evenimentului specificat

6.9.4.1.2 Trimitere e-mail

 Status ▾ Network ▾ Services ▾ System ▾ Logout ▾

All Events System Events Network Events **Events Reporting** Reporting Configuration

Event Reporting Configuration

Modify Event Reporting Rule

Enable

Event type **Reboot**

Event subtype **After unexpected shut down**

Action **Send email**

Enable delivery retry

Retry interval **5 min.**

Retry count **2**

Subject **Reboot**

Message text on Event

Router name - %rn;
Event type - %et; Event
text - %ex; Time stamp -
%ts;

Time stamp - %ts
Serial number - %sn
LAN MAC address - %lm
Connection state - %cs
Connection type - %ct
SIM slot in use - %su
Event type - %et
FW available on server - %fs
Network state - %ns
New line - %nl

Router name - %rn
WAN MAC address - %wm
Current FW version - %fc
Operator name - %on
Signal strength - %ss
IMSI - %im
Event text - %ex
LAN IP - %li
WAN IP address - %wi

Get status after reboot

SMTP server **mail.hostname.com**

SMTP server port **12345**

Secure connection

User name **user_name**

Password ********* 

Sender's email address **sender@email.com**

Recipient's email address **recipient@email.com** 

Send test email **Send**

	Nume câmp	Valoare în exemplu	Explicație
1.	Enable	Activat	Activăți sau dezactivați regula
2.	Event type	Reboot Repornire	Selectați tipul evenimentului despre care dorîți să fiți informat
3.	Event subtype	After unexpected shut down	Specificați subtipul evenimentului
4.	Action	Send email Trimitere e-mail	Acțiunea de executat la producerea evenimentului specificat
5.	Enable delivery retry	Activare	Activăți reîncercările de trimitere a e-mailului în caz de trimitere eşuată
6.	Retry interval	5 min.	La cât timp după o trimitere eşuată se inițiază reîncercarea trimiterii
7.	Retry count	2	De câte ori se reîncearcă trimiterea
8.	Subject	Reboot	Subiectul e-mailului
9.	Message text on Event	Router name - %rn; Event type - %et; Event text - %ex; Time stamp - %ts;	Conținutul mesajului
10.	Get status after reboot	Dezactivat	Indicați dacă dorîți să primiți sau nu informații despre starea routerului după repornire
11.	SMTP server	mail.hostname.com	Adresa serverului SMTP al furnizorului serviciului de e-mail al expeditorului
12.	SMTP server port	12345	Numărul portului serverului SMTP al furnizorului serviciului de e-mail al expeditorului
13.	Secure connection	Activat	Activăți sau dezactivați conexiunea securizată (folosiți numai dacă serverul are SSL sau TLS)
14.	User name	user_name	Numele de utilizator al contului de e-mail al expeditorului
15.	Password	*****	Parola contului de e-mail al expeditorului
16.	Sender's email address	sender@email.com	Adresa de e-mail a expeditorului
17.	Recipient's email address	recipient@email.com	Adresa de e-mail a destinatarului
18.	Send test email Trimitere e-mail de test	Send Trimitere	Transmite un mesaj de test simulat, conform datelor introduse de Dvs.

6.9.5 Configurarea raportării

Fereastra Reporting Configuration vă permite să creați reguli de transmitere a jurnalelor prin e-mail ori FTP.

The screenshot shows the Teltonika Reporting Configuration interface. At the top, there is a navigation bar with links for Status, Network, Services, System, and Logout. Below the navigation bar, there are tabs for All Events, System Events, Network Events, Events Reporting (which is selected), and Reporting Configuration. The main content area is titled "Events Log Files Report" and contains instructions to "Create rules for Events Log reporting." It displays two rules in a table:

Events log	Transfer type	Enable	Sort
Network	Email	<input checked="" type="checkbox"/>	Edit Delete
System	FTP	<input checked="" type="checkbox"/>	Edit Delete

Below this, there is a section titled "Events Log Reporting Configuration" with a table:

Events log	Transfer type
System	Email

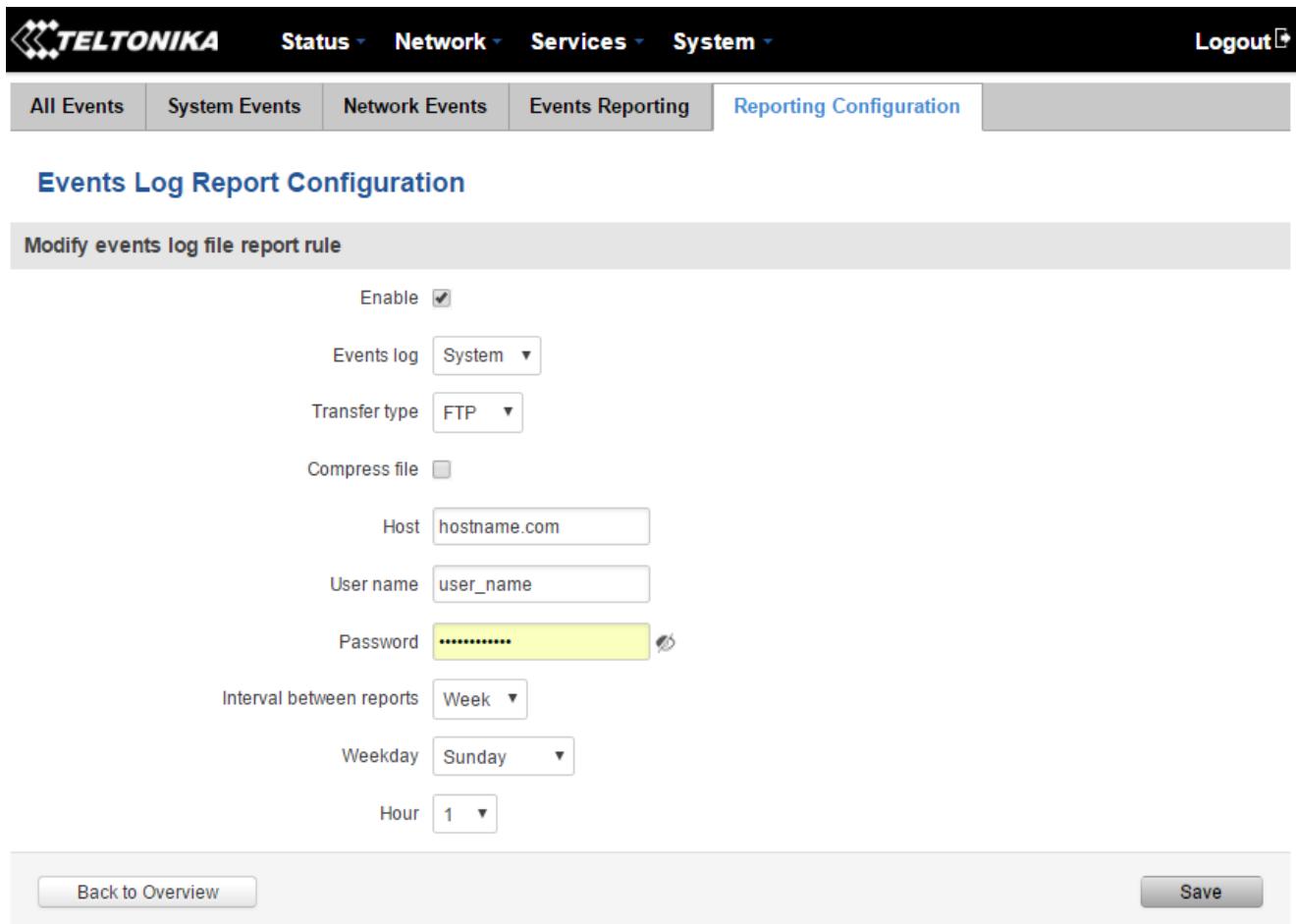
At the bottom right of this section is a "Save" button.

6.9.5.1 Configurarea raportării jurnalului de evenimente

Fereastra Events Log Report Configuration vă permite să modificați configurarea raportării periodice a evenimentelor prin e-mail ori FTP. Pentru a o accesa, creați o regulă și apăsați butonul "Edit" | Editare| alăturat, la fel ca la configurarea raportării evenimentelor.

Events log	Transfer type	Enable	Sort
System	FTP	<input type="checkbox"/>	 

6.9.5.1.1 FTP



The screenshot shows the Teltonika RUT955 web interface with the following navigation path: Status > Network > Services > System > Events Reporting > Reporting Configuration. The 'Events Reporting' tab is active. A modal dialog is open under 'Events Log Report Configuration' with the title 'Modify events log file report rule'. The configuration fields include:

- Enable: checked
- Events log: System
- Transfer type: FTP
- Compress file: unchecked
- Host: hostname.com
- User name: user_name
- Password: [REDACTED]
- Interval between reports: Week
- Weekday: Sunday
- Hour: 1

At the bottom of the modal are 'Back to Overview' and 'Save' buttons.

	Nume câmp	Valoare în exemplu	Explicație
1.	Enable	Activat	Activăți sau dezactivați regula
2.	Events log	System Sistem	Jurnalul de evenimente căruia î se aplică regula
3.	Transfer type Tip transfer	FTP	Modul de transfer al jurnalului de evenimente: e-mail ori FTP
4.	Compress file	Dezactivat	Activăți sau dezactivați comprimarea fișierului jurnalului de evenimente cu ajutorul gzip
5.	Host Gazdă	hostname.com	Numele gazdei FTP, de ex. ftp.example.com, 192.168.123.123. Caractere permise: (a-z-A-Z0-9!@#\$%^&*+-=?_`{ }~.)
6.	User name	user_name	Numele de utilizator folosit pentru autentificare pe serverul SMTP sau FTP. Caractere permise: (a-z-A-Z0-9!@#\$%^&*+-=?_`{ }~.)
7.	Password	*****	Parola pentru autentificare pe serverul SMTP sau FTP. Caractere permise: (a-z-A-Z0-9!@#\$%^&*+-=?_`{ }~.)
8.	Interval between reports Interval între raportări	Week Săptămână	Frecvența cu care va fi raportat jurnalul de evenimente
9.	Weekday	Sunday Duminică	Ziua din săptămână în care va fi raportat jurnalul de evenimente
10.	Hour	1	Ora la care va fi raportat jurnalul de evenimente

6.9.5.1.2 E-mail

Events Log Report Configuration

Modify events log file report rule

Enable

Events log

Transfer type

Compress file

Subject

Message

SMTP server

SMTP server port

Secure connection

User name

Password

Sender's email address

Recipient's email address

Interval between reports

Weekday

Hour

[Back to Overview](#)

	Nume câmp	Valoare în exemplu	Explicație
1.	Enable	Activare	Activăți sau dezactivați regula
2.	Events log	Network Rețea	Jurnalul de evenimente căruia i se aplică regula
3.	Transfer type	Email	Tipul de transferare a jurnalului de evenimente: Email ori FTP
4.	Compress file	Dezactivare	Activăți sau dezactivați comprimarea fișierului jurnalului de evenimente cu ajutorul gzip
5.	Subject	Test	Subiectul e-mailului
6.	Message	text message	Mesajul e-mailului
7.	SMTP server	mail.email.com	Adresa serverului SMTP al furnizorului serviciului de e-mail al expeditorului
8.	SMTP server port	12345	Numărul portului serverului SMTP al furnizorului serviciului de e-mail al expeditorului
9.	Secure connection	Activare/Dezactivare	Activăți sau dezactivați conexiunea securizată (folosiți numai dacă serverul are SSL sau TLS)
10.	User name	User	Numele de utilizator al contului de e-mail al expeditorului
11.	Password	*****	Parola contului de e-mail al expeditorului
12.	Sender's email address	sendersemail@example.com	Adresa de e-mail a expeditorului
13.	Recipient's email address	recipientemail@example.com	Adresa de e-mail a destinatarului
14.	Interval between reboots	Week	Frecvența cu care va fi raportat jurnalul de evenimente
15.	Weekday	Sunday	Ziua din săptămână în care va fi raportat jurnalul de evenimente
16.	Hour	1	Ora la care va fi raportat jurnalul de evenimente

7 Rețea

7.1 Rețeaua de telefonie mobilă

7.1.1 Setări generale

În fereastra Mobile Configuration |Configurare conexiune telefonie mobilă| puteți configura diverse setări pentru conectarea la rețeaua Dvs. locală de telefonie mobilă 2G/3G/LTE.

The screenshot shows the 'Mobile Configuration' page for SIM 2. The top navigation bar includes 'TELTONIKA', 'Status', 'Network', 'Services', 'System', and 'Logout'. Below the navigation is a tab bar with 'General', 'SIM Management', 'Network Operators', 'Mobile Data Limit', and 'SIM Idle Protection'. The main content area is titled 'Mobile Configuration' and contains tabs for 'SIM 1' and 'SIM 2' (which is selected). The configuration fields for SIM 2 include:

- Connection type:** QMI
- Mode:** NAT
- APN:** APN
- PIN number:** 1234
- Dialing number:** *99#
- Authentication method:** CHAP
- Username:** user_name
- Password:** (redacted)
- Service mode:** Automatic
- Deny data roaming:** (unchecked)
- Use IPv4 only:** (checked)

Below this is the 'Mobile Data On Demand' section with 'Enable' (unchecked) and 'No data timeout (sec)' set to 10. The final section is 'Force LTE network' with 'Enable' (unchecked), 'Reregister' (unchecked), and 'Interval (sec)' set to 300. A 'Save' button is located at the bottom right.

	Nume câmp	Valori posibile	Explicație
1.	Connection type Tip conexiune	PPP / QMI	Definește modul cum modemul routerului se va conecta la internet. Modul PPP utilizează un număr apelant pentru stabilirea unei conexiuni de date. Modul QMI (implicit) nu utilizează apelarea sau protocolul PPP pentru stabilirea unei conexiuni de date și este, de obicei, mai rapid decât modul PPP
2.	Mode Mod	NAT / Passthrough / Bridge	Modul NAT permite translatarea adresei de rețea pe router. Modul Bridge realizează o punte între conexiunea de date LTE și rețeaua LAN. În acest mod routerul nu are o conexiune la internet, întrucât furnizorul serviciului de acces la internet alocă o adresă IP direct dispozitivului terminal. Utilizarea modului Bridge va dezactiva majoritatea capabilităților routerului și vă va permite să accesați setările routerului Dvs. numai cu o adresă IP statică. Modul Passthrough funcționează similar modului Bridge, cu excepția faptului că routerul are o conexiune la internet
3.	APN	"APN"	Un Access Point Name nume de punct de acces este un gateway între o rețea mobilă GSM, GPRS, 3G ori 4G și o altă rețea informatică
4.	PIN number *	Orice număr între 0000 și 9999	Un PIN – număr de identificare personal – este o parolă numerică folosită pentru autentificarea unui utilizator într-un sistem
5.	Dialing number	*99#	Un Număr apelant este folosit pentru stabilirea unei conexiuni mobile PPP
6.	Authentication method	CHAP, PAP sau None Niciuna	Metoda de autentificare folosită de furnizorul Dvs. GSM pentru autentificarea noilor conexiuni în rețeaua sa
7.	Username	user_name	Numele de utilizator folosit pentru a vă conecta la rețeaua furnizorului Dvs. Acest câmp devine disponibil dacă ați selectat o metodă de autentificare (respectiv metoda de autentificare selectată nu este "None" Niciuna)
8.	Password	*****	Parola folosită pentru a vă conecta la rețeaua furnizorului Dvs.
9.	Service mode Mod serviciu	2G only Numai 2G , 3G only Numai 3G , 4G (LTE) only Numai 4G (LTE) ori Automatic Automat	Modul serviciului preferat de Dvs. Dacă rețeaua Dvs. locală de telefonie mobilă suportă 2G, 3G și 4G (LTE), puteți specifica la ce tip de rețea dorîți să vă conectați; de ex., dacă alegeți 2G, routerul se va conecta la o rețea 2G cât timp cât este disponibilă, altfel se va conecta la o rețea cu conectivitate mai bună. Dacă selectați Automat, routerul se va conecta la rețeaua cu cea mai bună conectivitate
10.	Deny data roaming Refuz roaming de date	Activare/Dezactivare	Când este activată, această funcție împiedică dispozitivul să stabilească o conexiune mobilă de date în afara rețelei Dvs. proprii
11.	Use IPv4 only Utiliz. doar IPv4	Activare/Dezactivare	Când este activată, această funcție face ca dispozitivul să utilizeze numai setările IPv4 atunci când se conectează la un operator
12.	Mobile Data On Demand	Activare/Dezactivare	Când este activată, funcția Date mobile la cerere menține conexiunea mobilă de date deschisă numai când este folosită
		No data timeout Expirare fără date (sec) – 10-99999999	Conexiunea mobilă de date va fi terminată dacă nu se transferă date în perioada de expirare specificată în acest câmp
13.	Force LTE network Forțare rețea LTE	Activare/Dezactivare	Când este activată, această funcție face ca routerul să se conecteze la o rețea LTE după numărul de secunde specificat
		Activare/Dezactivare	Când este activată, modemul se va reînregistra înainte de a încerca să se conecteze la o rețea LTE
		180 – 3600	Timpul în secunde între încercările de conectare la o rețea LTE

*Avertisment: Dacă introduceți un PIN invalid (adică dacă PIN-ul introdus nu se potrivește cu cel folosit în cartela SIM), cartela Dvs. SIM va fi blocată. Pentru a evita astfel de situații neplăcute, vă recomandăm cu tărie să folosiți un SIM neprotejat. Dacă se întâmplă să introduceți un SIM protejat și PIN-ul este incorrect, cartela Dvs. nu va fi blocată imediat, ci după două reporniri SAU salvări ale configurației.

7.1.1.1 Modul Passthrough

Modul Passthrough este folosit pentru redirecționarea întregului trafic către un alt dispozitiv. În cursul acestui proces routerul devine "transparent", întrucât întregul trafic va fi redirecționat către un alt dispozitiv care va avea alocată și adresa IP publică a routerului.

Using Passthrough Mode will disable most of the router capabilities.

Mobile Configuration

SIM 1

Connection type: QMI

Mode: Passthrough

APN: APN

PIN number: 1234

Dialing number: *99#

Authentication method: None

Service mode: Automatic

Deny data roaming:

Use IPv4 only:

DHCP mode: Static

MAC Address: 11:22:33:44:55:66

Lease time: 12 Hours

Nume câmp	Valori posibile	Explicație
DHCP mode Mod DHCP *	Static	În modul Static trebuie să introduceți adresa MAC a computerului Dvs. (xx:xx:xx:xx:xx:xx) și să selectați o perioadă de închiriere (perioada după care va expira adresa închiriată). Dispozitivul va obține o adresă IP de la operatorul Dvs. GSM. Alte dispozitive conectate la router vor obține adrese IP de la serverul DHCP al routerului, dar nu vor avea acces la internet
	Dynamic	În modul Dynamic operatorul GSM se va conecta întâi la router și va aloca o adresă IP calculatorului Dvs. Serverul DHCP LAN al routerului va fi dezactivat, dar va fi reactivat automat când treceți în alt mod
	No DHCP	În modul No DHCP adresa IP, masca de subreșea, gateway-ul implicit și DNS-ul de la operatorul GSM vor trebui introduse manual în calculatorul Dvs. Serverul DHCP LAN al routerului va fi dezactivat, dar va fi reactivat automat când treceți în alt mod

* Utilizarea modului Passthrough va dezactiva majoritatea capabilităților routerului!

7.1.2 Gestionarea cartelelor SIM

În fereastra SIM Management vă definiți cartela SIM principală și configurați scenariile în care routerul va executa o comutare între cartelele SIM.

The screenshot shows the SIM Management section of the Teltonika RUT955 web interface. At the top, there are tabs for General, SIM Management (which is selected), Network Operators, Mobile Data Limit, and SIM Idle Protection. Below the tabs, the "SIM Switching" section is displayed. Under "Primary Card", the "Primary SIM card" dropdown is set to "SIM 1". In the "SIM Switching" section, "Enable automatic switching" is checked, and the "Check interval" is set to 4 seconds. The "SIM1 To SIM2" tab is active, showing various triggers for switching: "On weak signal", "On data limit", "On sms limit", "On roaming", "No network", "On network denied", and "On data connection fail". A "Save" button is located at the bottom right of this section.

* Your carrier's data usage accounting may differ. Teltonika is not liable should any accounting discrepancies occur.

	Nume câmp	Valori posibile	Explicație
1.	Primary SIM card SIM principal	SIM 1 / SIM 2	Care cartelă SIM va fi folosită de sistem ca și cartelă principală
2.	Enable automatic switching Activare comutare automată	Activare/Dezactivare	Comută automat între cartelele SIM principală și secundară pe baza diferitelor reguli și criterii definite mai jos
3.	Check interval	1-3600	Intervalul de verificare, în secunde
4.	On weak signal La semnal slab	Activare/Dezactivare	Comută între cartelele SIM când intensitatea semnalului scade sub pragul specificat
5.	On data limit La limita de date *	Activare/Dezactivare	Comută între cartelele SIM când este atinsă limita pentru datele mobile
6.	On SMS limit La limita de SMS-uri *	Activare/Dezactivare	Comută între cartelele SIM când este atinsă limita pentru SMS-uri
7.	On roaming În roaming	Activare/Dezactivare	Comută între cartelele SIM când este detectat roamingul
8.	No network Fără rețea	Activare/Dezactivare	Comută între cartelele SIM când nu este detectat niciun operator

9.	On network denied La refuzare rețea	Activare/Dezactivare	Comută între cartelele SIM când este refuzat accesul într-o rețea
10.	On data connection fail La eşuare conexiune date	Activare/Dezactivare	Comută între cartelele SIM când conexiunea de date eşuează

* Modul în care operatorul Dvs. contabilizează utilizarea datelor poate dифri. Teltonika nu este responsabilă pentru nicio neconcordanță de contabilizare.

7.1.3 Operatori de rețele

Fereastra Network Operators vă permite să scanați, să selectați și să introduceți manual coduri de operatori de rețele. Această funcție este extrem de utilă atunci când routerul este în roaming. Selectarea operatorului este disponibilă doar pentru cartela SIM principală. Pentru a specifica un operator pentru cealaltă cartelă SIM, aceasta trebuie întâi selectată ca și cartela principală în secțiunea "SIM Management".

	Nume câmp	Valoare în exemplu	Explicație
1.	SIM card in use	SIM 1	Afișează cartela SIM folosită
2.	Current operator	LT BITE GSM	Denumirea operatorului GSM curent
3.	Scan for operators*	-	Inițiază o scanare a operatorilor disponibili în zona Dvs.
4.	Connection mode Mod conectare	Auto	Vă permite să alegeti dacă doriti să va selectati operatorul manual sau automat

*În timp ce se scană, conexiunea la rețeaua de telefonie mobilă curentă va fi pierdută!

7.1.3.1 Lista operatorilor

Fereastra Operators List vă permite să creați fie o listă albă, fie o listă neagră, pentru a vă ajuta să diferențiați operatorii preferați de cei nedoriți. Este utilă în special când călătoriți în străinătate, pentru că vă protejează împotriva costurilor nedorite de utilizare a datelor, împiedicând cartela SIM să acceseze operatori necunoscuți ori nedoriți.

The screenshot shows the Teltonika RUT955 web interface. At the top, there is a navigation bar with the Teltonika logo, Status, Network, Services, System, and Logout. Below the navigation bar, there is a horizontal menu with tabs: General, SIM Management, Network Operators (which is selected), Mobile Data Limit, and SIM Idle Protection. Under the Network Operators tab, there is a sub-menu with Network Operators and Operators List. The main content area is titled "Operators list". It has a "Settings" section with "Enable" checked and "Mode" set to "Blacklist". Below this is a table titled "Operators List" with columns: Name, Operator code, and Sort. There is one entry: TELE2 (operator code 24603). To the right of this entry are edit and delete buttons. At the bottom left is an "Add" button, and at the bottom right is a "Save" button.

	Nume câmp	Valori posibile	Explicație
1.	Enable	Activare/Dezactivare	Activează/dezactivează blocarea operatorilor
2.	Mode	Whitelist Listă albă /Blacklist Listă neagră	Listă albă – permite fiecare operator din listă, blochează orice alt operator Listă neagră – blochează fiecare operator din listă, permite orice alt operator
3.	Name	TELE2	Denumirea operatorului
4.	Operator code	24603	Codul operatorului

7.1.4 Limita pentru date mobile

Fereastra Mobile Data Limit vă permite să definiți limite de date pentru cartelele Dvs. SIM pentru a vă proteja împotriva costurilor nedorite.

Data Connection Limit Configuration Configurare limită conexiune date			
	Nume câmp	Valoare în exemplu	Explicație
1.	Enable data connection limit Activare limită conexiune date	Activare/Dezactivare	Dezactivează conexiunea mobilă de date când se atinge limita pentru perioada curentă
2.	Data limit * (MB)	10	Limita pentru date ce declanșează deconectarea datelor mobile
3.	Period	Month Lună	Perioada pentru care se va aplica limitarea datelor mobile
4.	Start day Zi început / Start hour Oră început	1	Momentul de început al perioadei de limitare a datelor mobile
SMS Warning Configuration Configurare avertizare prin SMS			
1.	Enable SMS warning	Activare/Dezactivare	Activează trimiterea unui mesaj SMS de avertizare înainte de sau la atingerea limitei pentru datele mobile pentru perioada curentă
2.	Data limit* (MB)	5	Limita pentru date care declanșează mesajul de avertizare
3.	Period	Month	Perioada pentru care se va aplica limitarea datelor mobile
4.	Start day/ Start hour	1	Momentul de început al perioadei de limitare a datelor mobile
5.	Phone number	+37012345678	Numărul de telefon la care va fi transmis SMS-ul de avertizare
Clear Data Limit Resetare limită date			
1.	Clear data limit	-	Șterge toate datele transmise și receptionate pentru perioada selectată

* Modul în care operatorul Dvs. contabilizează utilizarea datelor poate diferi. Teltonika nu este responsabilă pentru nicio neconcordanță de contabilizare.

7.1.5 Protecția SIM-ului inactiv

Unii operatori blochează cartelele SIM după o perioadă de inactivitate a utilizatorului. Fereastra SIM Idle Protection vă permite să configurați routerul să comute automat la cartela SIM secundară și să stabilească o conexiune de date cu o rețea mobilă pentru a preveni blocarea cartelei SIM.

7.1.5.1 Setări

SIM Idle Protection Configuration

SIM1 **SIM2**

Enable

Period Month

Day 1

Hour 1

Minute 0

Host to ping 127.0.0.1

Ping package size 56

Ping requests 2

Save

	Nume câmp	Valori posibile	Explicație
1.	Enable	Activare/Dezactivare	Activează protecția SIM-ului inactiv
2.	Period	Month Lună /Week Săptămână	Frecvența inițierii comutării între cartelele SIM
3.	Day	1-31 / Monday – Sunday Luni-duminică	Specifică ziua în care va fi activată protecția SIM-ului inactiv. 1-31 dacă perioada este luna. Luni-duminică dacă perioada este săptămâna
4.	Hour	1 – 24	Specifică ora la care va fi activată protecția SIM-ului inactiv
5.	Minute	0 – 60	Specifică minutul în care va fi activată protecția SIM-ului inactiv
6.	Host to ping Gazda vizată de ping	127.0.0.1	Specifică adresa IP sau numele de domeniu la care vor fi trimise pachetele de date
7.	Ping package size	56	Specifică dimensiunea în octeți a pachetului cu care se efectuează ping
8.	Ping requests	2	Numărul de solicitări de ping ce vor fi trimise

7.1.5.2 Test

Fereastra SIM Idle Protection Test |Testare protecție SIM inactiv| vă permite să testați funcția de protecție a SIM-ului inactiv cu parametrii setați în tab-ul Settings |Setări|. La apăsarea butonului ‘Test’* se va simula un scenariu de protecție a SIM-ului pentru ambele cartele SIM. Nu efectuați alte acțiuni între inițierea și finalizarea testării; în caz contrar vor apărea erori ce pot fi remediate numai prin resetarea dispozitivului Dvs.

SIM	SIM state	IMSI	ICCID	Host IP	WAN ip	Ping
SIM2	OK (inserted)	246012101922859	89370010100019228599	8.8.8.8	188.69.236.204	Success
SIM1	OK (inserted)	246020100944448	8937002160600414481F	8.8.8.8	84.15.198.92	Success

	Nume câmp	Valoare în exemplu	Explicație
1.	SIM	SIM1	Numărul cartelei SIM
2.	SIM state	OK (inserted) OK (introdusă)	Starea cartelei SIM
3.	IMSI	246020100944448	Identifierul IMSI folosit pentru identificarea utilizatorului în cadrul unei rețele celulare
4.	ICCID	8937002160600414481	Identifierul ICCID folosit pentru identificarea cartelei SIM pe plan internațional
5.	Host IP	8.8.8.8	Adresa IP a gazdei
6.	WAN IP	84.15.198.92	Adresa IP publică a cartelei SIM
7.	Ping	Success	Starea încercării de ping

*În timpul testării nu efectuați nicio acțiune; așteptați finalizarea testului

7.2 WAN

7.2.1 Modul de operare

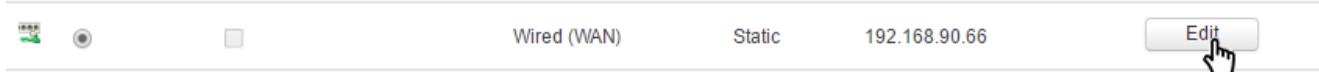
Fereastra WAN vă permite să determinați modul în care routerul se va conecta la internet. Puteți alege între trei tipuri de WAN – Mobile, Wired | Prin cablu | și Wi-Fi.

Main WAN	Backup WAN	Interface Name	Protocol	IP Address	Sort
<input checked="" type="radio"/>	<input type="checkbox"/>	Wired (WAN)	Static	192.168.90.66	
<input type="radio"/>	<input type="checkbox"/>	WiFi (WAN3)	DHCP	-	
<input type="radio"/>	<input checked="" type="checkbox"/>	Mobile (WAN2)	None	84.15.198.92	

	Nume câmp	Valori posibile	Explicație
1.	Main WAN	Wired/Mobile/Wi-Fi	Vă permite să selectați rețeaua WAN principală
2.	Backup WAN WAN de backup / Load Balancing / Echilibrare încărcare	Activare/Dezactivare	Vă permite să selectați una sau două interfețe pentru a servi ca rețea WAN de backup
3.	Interface Name	WAN/WAN2/WAN3	Numele interfețelor WAN
4.	Protocol	Static/DHCP/PPPoE	Protocolul folosit de o interfață WAN
5.	IP Address	192.168.90.66	Adresa IP a rețelei WAN
6.	Sort	-	Vă permite să sortați rândurile din tabel și să modificați prioritatea interfețelor (adică, prima interfață din listă are cea mai mare prioritate)

7.2.2 Configurare comună

Puteți configura mai departe fiecare dintre interfețele WAN dând clic pe butonul "Edit" aflat în extremitatea dreaptă a tabelului WAN în dreptul fiecărei interfețe:



Se va deschide fereastra Common Configuration unde puteți să selectați protocolul ce va fi folosit de interfața WAN, să configurați rețeaua WAN de backup, să definiți aliasuri IP, servere DNS particularizate și altele.

7.2.2.1 Setări generale

Puteți comuta între protocolele Static, DHCP ori PPPoE selectându-l pe cel pe care doriți să îl folosiți și apoi apăsând butonul ‘Switch Protocol’* |Comutare protocol|.



*Butonul “Switch protocol” nu aplică nicio modificare. Pentru a salva modificările, trebuie să dați clic pe butonul “Save” din colțul stânga-jos al ferestrei după ce ați terminat de făcut modificările.

7.2.2.1.1 Static

Protocolul Static este utilizat când sursa Dvs. de internet nu are un server DHCP activat. Deci, pentru a vă conecta la internet, trebuie să efectuați configurațiile aferente sursei (similar cu secțiunea [Logare](#) din acest manual.)

	Nume câmp	Valoare în exemplu	Explicație
1.	Protocol	Static	Protocolul folosit de interfața WAN
2.	IPv4 address	192.168.90.66	Adresa IPv4 a routerului Dvs. în rețea WAN
3.	IPv4 netmask	255.255.255.0	O mască de rețea folosită pentru definirea dimensiunii rețelei WAN
4.	IPv4 gateway	192.168.90.254	Adresa unde routerul va trimite tot traficul de ieșire
5.	IPv4 broadcast	192.168.90.255	Adresa de broadcast (generată automat dacă nu este setată). Dacă nu sunteți sigur, lăsați acest câmp necompletat
6.	Use custom DNS servers Utilizare servere DNS particularizate	8.8.8.8 8.8.4.4	De regulă gateway-ul are servere DNS predefinite. Astfel, când routerul trebuie să asocieze un nume de gazdă (“www.google.com”, “www.cnn.com” etc...) unei adrese IP, va redirecționa toate solicitările DNS către gateway. Prin introducerea de servere DNS particularizate, routerul se va ocupa de rezoluția numelui de gazdă. Puteți introduce mai multe servere DNS pentru a asigura redundanță în cazul căderii uneia dintre servere

7.2.2.1.2 DHCP

Protocolul DHCP ar trebui utilizat când sursa Dvs. de internet are un server DHCP activat. În acest caz, atunci când selectați protocolul DHCP, îl puteți folosi imediat, întrucât majoritatea rețelelor nu vor solicita alte setări avansate.

Common Configuration

General Setup Advanced Settings

Protocol: DHCP

Hostname to send when requesting DHCP: Teltonika

7.2.2.1.3 PPPoE

Protocolul PPPoE este folosit de regulă dacă aveți un furnizor de internet prin DSL.

Common Configuration

General Setup Advanced Settings

Protocol: PPPoE

PAP/CHAP username: user_name

PAP/CHAP password: *****

Access Concentrator: auto

Service Name: auto

	Nume câmp	Valoare în exemplu	Explicație
1.	Protocol	PPPoE	Protocolul folosit de interfața WAN
2.	PAP/CHAP username Nume utilizator PAP/CHAP	user_name	Numele de utilizator pe care l-ați folosi pentru a vă conecta la rețea furnizorului Dvs.
3.	PAP/CHAP password Parolă PAP/CHAP	*****	Parola pe care ați folosi-o pentru a vă conecta la rețea furnizorului Dvs.
4.	Access Concentrator	auto	Numele concentratorului de acces. Lăsați gol pentru detectare automată
5.	Service Name	auto	Numele serviciului. Lăsați gol pentru detectare automată

7.2.2.2 Setări avansate

Tab-ul Advanced Setting vă permite să efectuați setări avansate pentru fiecare dintre protocole. Dacă nu sunteți sigur cum trebuie modificate aceste setări, vă recomandăm cu tărie să le lăsați nemodificate ori să consultați un specialist.

7.2.2.2.1 Static

Tab-ul Advanced Settings se va modifica în funcție de protocolul de rețea selectat. Pentru protocolul Static puteți să porniți/opriți funcția NAT, să ignorați adresa MAC a routerului și MTU și să definiți o metrică pentru gateway. Mai jos găsiți informații suplimentare privind aceste setări.

Common Configuration			
	General Setup	Advanced Settings	
Disable NAT	<input type="checkbox"/>		
Override MAC address	00:51:33:77:56:17		
Override MTU	1500		
Use gateway metric	0		

	Nume câmp	Valoare în exemplu	Explicație
1.	Disable NAT	Pornit/Oprit	Porniți/opriți translatarea adresei de rețea (NAT) pentru interfața de rețea selectată
2	Override MAC address	00:51:33:77:56:17	Ignorați adresa MAC a interfeței WAN. Dacă furnizorul Dvs. de internet vă alocă o adresă IP statică, o poate și lega de adresa MAC a calculatorului Dvs. (adică acel IP va funcționa numai cu calculatorul, nu și cu routerul Dvs.). În acest câmp puteți să introduceți adresa MAC a calculatorului Dvs. și să păcăliți gateway-ul să credă că comunică cu calculatorul Dvs.
3.	Override MTU Ignorare MTU	1500	Maximum Transmission Unit (MTU) – specifică dimensiunea maximă posibilă a unui pachet de date
4.	Use gateway metric Utilizare metrică gateway	0	În mod implicit configurația rețelei WAN generează o intrare în tabela de rutare. În acest câmp puteți modifica metrica acelei intrări

7.2.2.2.2 DHCP

Pentru protocolul DHCP puteți să porniți/opriți funcția NAT, să specificați servere DNS particularizate, să definiți o metrică pentru gateway, să ignorați adresa MAC a routerului, să setați MTU și altele. Mai jos găsiți informații suplimentare privind aceste setări.

Common Configuration

General Setup **Advanced Settings**

Disable NAT

Use broadcast flag

Use default gateway

Use DNS servers advertised by peer

Use custom DNS servers

Use gateway metric

Client ID to send when requesting DHCP

Vendor class to send when requesting DHCP

Override MAC address

Override MTU

	Nume câmp	Valoare în exemplu	Explicație
1.	Disable NAT	Pornit/Oprit	Porniți/opriți translatarea adresei de rețea (NAT) pentru interfața de rețea selectată
2	Use broadcast flag	Activare/Dezactivare	Necesară pentru unii furnizori de servicii internet, de ex. Charter cu DOCSIS 3
3.	Use default gateway Utilizare gateway implicit	Activare/Dezactivare	Dacă lăsați căsuța nebifată, nu este configurată nicio rută implicită
4.	Use DNS servers advertised by peer Utilizare servere DNS anunțate de peer	Activare/Dezactivare	Dacă lăsați căsuța nebifată, adresele de servere DNS anunțate sunt ignorete
5.	Use custom DNS Servers	8.8.8.8 8.8.4.4	Vă permite să vă alegeti propriile Dvs. servere DNS preferate
6.	User gateway metric	0	În mod implicit configurația rețelei WAN generează o intrare în tabela de rutare. În acest câmp puteți modifica metrica acelei intrări
7.	Client ID to send when requesting DHCP		ID-ul de client ce va fi transmis când se solicită o închiriere DHCP
8.	Vendor Class to send when requesting DHCP		Clasa vânzătorului ce va fi transmisă când se solicită o închiriere DHCP

9.	Override MAC address	00:51:33:77:56:17	Ignorați adresa MAC a interfeței WAN. Dacă furnizorul Dvs. de internet vă alocă o adresă IP statică, o poate și lega de adresa MAC a calculatorului Dvs. (adică acel IP va funcționa numai cu calculatorul, nu și cu routerul Dvs.). În acest câmp puteți să introduceți adresa MAC a calculatorului Dvs. și să păcăliți gateway-ul să credă că comunică cu calculatorul Dvs.
10.	Override MTU	1500	Maximum Transmission Unit (MTU) – specifică dimensiunea maximă posibilă a unui pachet de date

7.2.2.2.3 PPPoE

Pentru protocolul PPPoE puteți să porniți/opriți funcția NAT, să specificați servere DNS particularizate, să definiți o metrică pentru gateway, să configurați setările ecoului LCP și altele. Mai jos găsiți informații suplimentare privind aceste setări.

Common Configuration

General Setup Advanced Settings

Disable NAT

Use default gateway

Use gateway metric

Use DNS servers advertised by peer

Use custom DNS servers

LCP echo failure threshold

LCP echo interval

Inactivity timeout

	Nume câmp	Valoare în exemplu	Explicație
1.	Disable NAT	Activare/Dezactivare	Porniți/opriți translatarea adresei de rețea (NAT) pentru interfața de rețea selectată
2	Use default gateway	Activare/Dezactivare	Dacă lăsați căsuța nebifată, nu este configurată nicio rută implicită
3.	Use gateway metric	0	În mod implicit configurația rețelei WAN generează o intrare în tabela de rutare. În acest câmp puteți modifica metrica acelei intrări
4.	Use DNS servers advertised by peer	Activare/Dezactivare	Dacă lăsați căsuța nebifată, adresele de servere DNS anunțate sunt ignorate
5.	Use Custom DNS Servers	8.8.8.8 8.8.4.4	Vă permite să vă alegeți propriile Dvs. servere DNS preferate
5.	LCP echo failure threshold Prag eșecuri cereri ecou LCP	0	Se prezumă că peer-ul este inactiv după numărul dat de cereri de ecou eșuate. Lăsați la valoarea 0 pentru a ignora eșecurile
6.	LCP echo interval Interval cereri ecou LCP	5	Se trimit cereri de ecou LCP la intervalul în secunde stabilit. Această funcție este eficace numai împreună cu pragul de eșecuri
7.	Inactivity timeout Expirare la inactivitate	0	Închide conexiunea inactivă după numărul de secunde specificat. Lăsați la valoarea 0 pentru a menține conexiunea

7.2.2.3 Aliasuri IP

7.2.2.3.1 Setări generale

Aliasurile IP sunt un mod de a defini ori de a accesa o subretea care funcționează în același spațiu ca și rețeaua obișnuită. Aceasta vă este de ajutor când doriți să accesați routerul în aceeași rețea, dar într-o subrețea diferită. Dacă aveți pe calculatorul Dvs. o configurație IP statică și nu doriți să o modificați de fiecare dată când trebuie să accesați un router într-o subrețea diferită, puteți configura în acest scop un alias IP.

The screenshot shows the 'IP Aliases' configuration page. At the top, there are two tabs: 'General Setup' (which is selected) and 'Advanced Settings'. Below the tabs, there are three input fields: 'IP Address' (192.168.99.60), 'Netmask' (255.255.255.0), and 'Gateway' (192.168.90.254). At the bottom left are two buttons: 'Delete' and 'Add'.

După cum vedeti, configurarea este foarte asemănătoare cu protocolul Static; în exemplu diferă doar faptul că este definită o adresă IP cu o a 99-a subrețea. Dacă un dispozitiv are un IP în a 99-a subrețea (de ex., 192.168.99.xxx), iar metrica gateway-ului subrețelei este "mai mare", iar dispozitivul încearcă să acceseze internetul, își va reruta traficul nu către gateway-ul definit în configurarea comună, ci către cel specificat în aliasurile IP.

7.2.2.3.2 Setări avansate

Puteți, de asemenea, să definiți o adresă de broadcast și un server DNS particularizat pentru aliasurile Dvs. IP în tab-ul Advanced Settings.

The screenshot shows the 'IP Aliases' configuration page with the 'Advanced Settings' tab selected. Below the tabs, there are two input fields: 'IP Broadcast' (192.168.99.255) and 'DNS Server' (8.8.8.8). At the bottom left are two buttons: 'Delete' and 'Add'.

7.2.2.4 Configurarea rețelei WAN de backup

Funcția rețea WAN de backup vă permite să supliniți conexiunea principală când aceasta cade. La un moment dat pot fi selectate două conexiuni de backup. În acest caz, când conexiunea principală cade, routerul încearcă să încearcă să folosească conexiunea de backup cu prioritatea mai mare, iar dacă aceasta este indisponibilă sau cade și ea, atunci routerul încearcă conexiunea de backup cu prioritatea mai mică.

Backup Configuration

Timing and other parameters will indicate how and when it will be determined that your conventional connection has gone down.

Health monitor interval	10 sec.
Health monitor ICMP host(s)	8.8.4.4
Health monitor ICMP timeout	3 sec.
Attempts before failover	3
Attempts before recovery	3

Save

Teltonika solutions

www.teltonika.lt

Majoritatea opțiunilor privesc setări de timp și alți parametri importanți ce ajută la stabilirea sănătății conexiunii Dvs. principale. Sunt efectuate periodic verificări de sănătate ale conexiunii Dvs. principale sub formă de pachete ICMP (ping-uri). Când starea conexiunii începe să se schimbe (READY->NOT READY și viceversa), trebuie să se atingă un anumit număr de verificări de sănătate eșuate sau trecute, înainte ca starea să se schimbe complet. Această întârziere este impusă pentru a se minimiza "vârfurile" disponibilității conexiunii, dar se și prelungesc perioada până la activarea sau dezactivarea conexiunii de backup.

Nume câmp	Valori posibile	Explicație
1. Health monitor interval Interval monitorizare sănătate	Disable/5/10/20/30/60/120 Seconds	Intervalul la care sunt efectuate verificările de sănătate
2. Health monitor ICMP host(s) Gazdă/e ICMP pentru monitorizare sănătate	8.8.4.4 / Disable / DNS Server(s) / WAN Gateway / custom	Indică unde vor fi transmise solicitările de ping pentru verificarea sănătății. Întrucât nu există o modalitate absolută de a determina când conexiunea la internet este pierdută definitiv, cel mai bine este să definiți o gazdă a cărei disponibilitate este cea a internetului în ansamblu (de ex. 8.8.8, 8.8.4.4)
3. Health monitor ICMP timeout Expirare cereri ICMP pentru monitorizare sănătate	1/2/3/4/5/10 Seconds	Frecvența cu care vor fi transmise solicitările ICMP. Recomandăm să setați o valoare mai mare atunci când conexiunea Dvs. are o latență sau jitter (vârfuri ale latenței) ridicate
4. Attempts before failover Încercări înainte de failover	1/3/5/10/15/20	Numărul de încercări de ping eșuate după care conexiunea este declarată ca "pierdută"
5. Attempts before recovery Încercări înainte de recuperare	1/3/5/10/15/20	Numărul de încercări de ping efectuate cu succes după care conexiunea este declarată ca "existență"

7.2.3 Cum configurați o conexiune de backup?

Mai întâi trebuie să selectați o conexiune principală și una sau două conexiuni de backup în secțiunea WAN. Apoi apăsați butonul "Edit" și configurați setările pentru rețelele Dvs. WAN principală și de backup după cum dorîți.

WAN

Your WAN configuration determines how the router will be connecting to the internet.

Main WAN	Backup WAN	Interface Name	Protocol	IP Address	Sort
	<input checked="" type="radio"/>	Wired (WAN)	Static	192.168.90.66	<button>Edit</button>
	<input checked="" type="radio"/>	Mobile (WAN2)	None	-	
	<input checked="" type="radio"/>	WiFi (WAN3)	DHCP	-	<button>Edit</button>



Backup Configuration

Timing and other parameters will indicate how and when it will be determined that your conventional connection has gone down.

Health monitor interval	5 sec.
Health monitor ICMP host(s)	DNS Server(s)
Health monitor ICMP timeout	1 sec.
Attempts before failover	1
Attempts before recovery	1

Dați clic pe Save după ca ați efectuat modificările și așteptați până când setările sunt aplicate. Puteți monitoriza starea rețelelor WAN principală/de backup în pagina Status -> Network Information -> WAN. Dacă totul funcționează corect ar trebui să vedeți ceva de genul:

Backup WAN Status

WAN: [Wired] IN USE Backup WAN: [Mobile] READY

Imaginea de mai sus prezintă starea rețelei WAN de backup mobile configurată pentru o conexiune principală prin cablu. Acum puteți simula o conexiune pierdută scoțând cablul Ethernet al rețelei WAN. După aceasta ar trebui să vedeți aceasta:

Backup WAN Status

WAN: [Wired] NOT READY Backup WAN: [Mobile] IN USE

Când conexiunea principală este pierdută, întregul trafic va trece prin interfața WAN de backup (în acest caz, mobilă). Când reintroduceți cablul, conexiunea va fi restabilită iar traficul va trece din nou prin interfața WAN principală (în acest caz, prin cablu).

7.3 LAN

Această pagină servește la configurarea rețelei LAN, în care se vor găsi toate dispozitivele și calculatoarele Dvs. pe care le conectați la router.

7.3.1 Configurare

7.3.1.1 Setări generale

The screenshot shows the 'General Setup' tab selected under the 'Configuration' section. It displays three input fields: 'IP address' (192.168.56.1), 'IP netmask' (255.255.255.0), and 'IP broadcast' (192.168.56.255).

	Nume câmp	Valoare în exemplu	Explicație
1.	IP address	192.168.56.1	Adresa IP folosită de router în rețeaua LAN
2.	IP netmask Mască rețea IP	255.255.255.0	O mască folosită pentru a defini dimensiunea rețelei LAN
3.	IP broadcast Difuzare IP	192.168.56.255	Difuzările sunt utilizate de clienții BOOTP și DHCP pentru a găsi și pentru a trimite solicitări către serverele respective

7.3.1.2 Setări avansate

The screenshot shows the 'Advanced Settings' tab selected under the 'Configuration' section. It includes several configuration options: 'Accept router advertisements' (checkbox), 'Override MTU' (input field set to 1500), 'Use gateway metric' (input field set to 0), and a note 'Use WAN port as LAN' with a checkbox and a tooltip 'WAN Ethernet port selected as LAN'.

	Nume câmp	Valori posibile	Explicație
1.	Accept router advertisements Acceptare RA-uri	Activare/Dezactivare	Când este activată, această funcție permite acceptarea RA-urilor (este dezactivată în mod implicit)
2.	Override MTU	0 – 1500	MTU (Maximum Transmission Unit) specifică dimensiunea maximă posibilă a unui pachet de date
3.	Use gateway metric	Orice număr întreg	În mod implicit configurația rețelei LAN generează o intrare în tabela de rutare. În acest câmp puteți modifica metrica acelei intrări. O metrică mai mare înseamnă o prioritate mai mare
4.	Use WAN port as LAN Utilizare port WAN ca LAN	Activare/Dezactivare	Vă permite să folosiți portul WAN ca și când ar fi fost un port LAN

7.3.2 Server DHCP

Serverul DHCP este serviciul secundar al routerului ce poate configura automat setările TCP/IP ale oricărui dispozitiv care solicită acest serviciu. Când conectați un dispozitiv configurat să obțină o adresă IP automat, serverul DHCP va închiria o adresă IP și dispozitivul va putea comunica cu routerul.

7.3.2.1 Setări generale

DHCP	Enable
Start	100
Limit	150
Lease time	12
	Hours

	Nume câmp	Valoare în exemplu	Explicație
1.	DHCP	Enable Activare / Disable Dezactivare / DHCP Relay Releu DHCP	Activează sau dezactivează serverul DHCP. Dacă selectați DHCP Relay, vi se va cere să introduceți o adresă IP a unui alt server DHCP din rețeaua Dvs. LAN. În acest caz, de fiecare dată când un nou dispozitiv se conectează la router, routerul va redirecționa toate solicitările DHCP către serverul DHCP specificat
2.	Start	100	Valoarea de pornire a adresei IP. De ex., dacă IP-ul din rețeaua LAN a routerului Dvs. este 192.168.2.1 iar masca Dvs. de subreșea este 255.255.255.0, atunci în rețeaua Dvs. o adresă IP validă trebuie să fie în domeniul [192.168.2.1 – 192.168.2.254] (192.168.2.0 și 192.168.2.255 sunt adrese speciale indisponibile). Dacă valoarea de start este setată la 100, atunci serverul DHCP va închiria numai adrese începând cu 192.168.2.100
3.	Limit Limită	150	Câte adrese poate închiria serverul DHCP. Continuând cu exemplul de mai sus: dacă adresa de start este 192.168.2.100 iar serverul poate închiria 150 (valoarea din exemplu) de adrese începând cu 192.168.2.100 și până la 192.168.2.249 (100 + 150 – 1 = 249; aceasta din cauză că prima adresă este inclusă)
4.	Lease time Durată închiriere	12	Durata unei închirieri IP. Adresele închiriate vor expira după perioada specificată în acest câmp iar dispozitivul care utiliza închirierea va trebui să trimită o nouă cerere DHCP serverului DHCP al routerului. Totuși, dacă dispozitivul rămâne conectat, închirierea sa va fi reînnoită după trecerea jumătății perioadei specificate; de ex.: dacă durata închirierii este 12 ore, atunci din 6 în 6 ore dispozitivul va transmite routerului o cerere de reînnoire a închirierii. Durata închirierii poate fi setată în ore ori minute. Durata minimă ce poate fi specificată este 2 minute

7.3.2.2 Setări avansate

Puteți, de asemenea, să definiți opțiuni avansate care specifică modul în care serverul DHCP va funcționa în rețeaua Dvs. LAN.

DYNAMIC DHCP

Enable DNS rebind protection

Force

IP netmask

DHCP Options

	Nume câmp	Valoare în exemplu	Explicație
1.	Dynamic DHCP DHCP dinamic	Activat/Dezactivat	Activează alocarea dinamică a adreselor clientilor. Dacă opțiunea este dezactivată, vor fi servite numai clientii care au închirieri de adrese IP statice
2.	Enable DNS rebind protection	Activat/Dezactivat	Activează protecția împotriva atacurilor de tip DNS rebinding prin eliminarea răspunsurilor RFC1918 din amonte (lăsați valoarea implicită dacă nu este necesar altfel)
3.	Force Forțare	Activat/Dezactivat	În mod implicit, serverul DHCP al routerului nu va porni atunci când este conectat la un segment de rețea unde există deja un server DHCP în funcțiune. Dacă este activată, funcția de forțare DHCP va face ca routerul să își pornească întotdeauna serverul DHCP, chiar dacă există un alt server DHCP care rulează deja în rețeaua routerului
4.	IP netmask	255.255.255.0	Înlătură masca de rețea a rețelei LAN, făcând astfel serverul DHCP să credă că deservește o rețea mai mare sau mai mică decât în realitate
5.	DHCP Options Opțiuni DHCP	6,8.8.8.8,8.8.4.4	Opțiuni suplimentare ce vor fi adăugate la serverul DHCP. De ex., cu '26,1470' ori 'option:mtu, 1470' puteți aloca MTU pentru DHCP

7.3.3 Închirieri statice

Închirierile de adrese IP statice sunt folosite pentru rezervarea anumitor adrese IP pentru anumite dispozitive prin legarea lor de adresele MAC. Această funcție este utilă când în rețeaua Dvs. aveți conectat un dispozitiv fix pe care trebuie să îl accesați frecvent, de ex. imprimantă, fax etc.

Static Leases		
Hostname	MAC address	IP address
Printer	70:8a:09:1d:81:46 (192.168.56.210)	192.168.56.210

Add Delete

	Nume câmp	Valoare în exemplu	Explicație
1.	Hostname	Printer Imprimantă	Un nume particularizat ce va fi asociat dispozitivului
2.	MAC address	10:a5:d0:70:9c:72 (192.168.1.104)	Adresa MAC a dispozitivului
3.	IP address	192.168.1.104	Adresa IP dorită ce va fi rezervată pentru dispozitivul specificat

7.3.4 Aliasuri IP

7.3.4.1 Setări generale

Aliasurile IP sunt un mod de a defini ori de a accesa o subrețea care funcționează în același spațiu ca și rețeaua obișnuită. Aceasta vă este de ajutor când doriți să accesați routerul care se află în aceeași rețea, dar într-o subrețea diferită. Dacă aveți pe calculatorul Dvs. o configurație IP statică și nu doriți să o modificați de fiecare dată când trebuie să accesați un router într-o subrețea diferită, puteți configura în acest scop un alias IP.

IP Address	192.168.14.1
Netmask	255.255.255.0
Gateway	192.168.90.254

Delete **Add**

7.3.4.1 Setări avansate

Puteți, de asemenea, să definiți o adresă de broadcast și un server DNS particularizat.

IP Broadcast	192.168.14.255
DNS Server	8.8.8.8

Delete **Add**

Puteți găsi indicațiile pentru configurarea aliasurilor IP în secțiunea [WAN](#) a acestui document.

7.4 VLAN

Fereastra VLAN vă permite să vă creați și să vă configurați propriile Dvs. rețele LAN virtuale, ce pot fi fie bazate pe porturi, fie bazate pe taguri.

7.4.1 Rețele VLAN

7.4.1.1 Funcția VLAN

VLAN Networks **LAN Networks**

Virtual LAN

VLAN Functionality

VLAN mode: **Disabled**

Save

	Nume câmp	Valori posibile	Explicație
1.	VLAN mode Mod VLAN	Disabled Dezactivată / Port based Bazată pe porturi / Tag based Bazată pe taguri	Vă permite să selectați modul VLAN sau să dezactivați funcția VLAN

7.4.1.2 Rețea VLAN bazată pe porturi

VLAN mode: **Port based**

VLAN Networks List

	LAN ports			Wireless access points	
VLAN ID	1	2	3	HAL9000	LAN
1	On	On	On	<input type="checkbox"/>	None

Add **Delete** **Save**

	Nume câmp	Valori posibile	Explicație
1.	VLAN ID	1-4094	Numărul de identificare al rețelei VLAN
2.	LAN ports 1 / 2 / 3	On / Off / Tagged	Schimbă starea portului LAN
3.	Wireless access points Puncte acces wireless	Activat/Dezactivat	Asignați punctul/punctele de acces selectat/e rețelei LAN selectate
4.	LAN	None Niciuna / lan (numele implicit al LAN)	Asignați porturile LAN și punctul/punctele de acces wireless selectate unei rețele LAN

7.4.1.3 Rețea VLAN bazată pe tag-uri

Virtual LAN

VLAN Functionality

VLAN mode

VLAN Networks List

Wireless access points		
VLAN ID	HAL9000	LAN
1	<input type="checkbox"/>	<input type="button" value="None ▾"/> <input type="button" value="Delete"/>

	Nume câmp	Valori posibile	Explicație
1.	VLAN ID	1-4094	Numărul de identificare al rețelei VLAN
2.	Wireless access points	Activat/Dezactivat	Asignați punctul/punctele de acces selectat/e rețelei LAN selectate
3.	LAN	None / lan	Asignați punctul/punctele de acces wireless selectat/e unei rețele LAN

7.4.2 Rețele LAN

În pagina LAN Networks puteți crea rețele LAN suplimentare și le puteți aloca porturi și puncte de acces wireless. Putem găsi mai multe informații privind oricare dintre setările LAN în secțiunea [7.3 LAN](#).

[Status](#) [Network](#) [Services](#) [System](#) [Logout](#)

[VLAN Networks](#) [LAN Networks](#)

LAN

LAN Networks List

LAN name	Interface name	
Lan	eth0 tap0	<input type="button" value="Edit"/>
Lan_Lan2	bri-lan	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

LAN name:

	Nume câmp	Valoare în exemplu	Explicatie
1.	LAN name	Lan	Specifică numele rețelei LAN
2.	Interface name	eth0 tap0	Specifică numele interfeței LAN

7.5 Wireless

Fereastra Wireless Configuration |Configurare wireless| vă permite să vă configurați punctele de acces wireless și stațiile wireless. Fereastra Wireless Station Mode |Mod stație wireless| va deveni activă numai după ce Wi-Fi va fi configurat ca interfață WAN activă (fie principală, fie de backup).

The screenshot shows the 'Wireless Configuration' page with two main sections:

- Wireless Access Points:** Shows a single entry for 'SSID: HAL9000' with 'Encryption: WPA-PSK/WPA2-PSK mixed mode'. Buttons for 'Disable', 'Edit', and 'Remove' are available.
- Wireless Station Mode:** Shows a single entry for 'SSID: GUEST_TELTONIKA' with 'Encryption: WPA2-PSK'. Buttons for 'Disable', 'Edit', and 'Remove' are available.

Mai sus este aspectul general al fereastrii Wireless Configuration, ce afișează punctele de acces și stațiile active. Aici puteți să vă dezactivați sau activați interfețele Wi-Fi, să eliminați punctele de acces sau stațiile nedorite sau să accesați o fereastră de configurare suplimentară pentru fiecare interfață Wi-Fi.

7.5.1 Punct de acces wireless

Fereastra de configurare Wireless Access Points |Puncte de acces wireless| este folosită pentru modificarea diferitelor puncte de acces. Este împărțită în două mari secțiuni – dispozitiv și interfață. Una este dedicată configurării parametrilor hardware, celalătă – parametrilor software. Pentru a accesa această fereastră, dați clic pe butonul "Edit" din dreptul interfeței pe care doriți să o configurați:

The screenshot shows the 'Wireless Access Points' section of the configuration page. It lists one entry: 'SSID: HAL9000' with 'Encryption: WPA-PSK/WPA2-PSK mixed mode'. Below the list are three buttons: 'Disable', 'Edit', and 'Remove'. A hand cursor is positioned over the 'Edit' button.

7.5.1.1 Configurarea dispozitivului

Secțiunea Device Configuration |Configurare dispozitiv| este folosită pentru configurarea parametrilor hardware Wi-Fi.

7.5.1.1.1 Setări generale

Aici puteți stabili disponibilitatea conexiunii wireless și frecvența canalului fizic.

The screenshot shows the 'Device Configuration' section for a 'Wireless Access Point'. It includes the following elements:

- A message: "Here you can configure your wireless settings like radio frequency, mode, encryption etc..."
- A tab bar with 'General Setup' (selected) and 'Advanced Settings'.
- Configuration fields:
 - 'Enable wireless' checkbox (checked).
 - 'Channel' dropdown set to '4 (2.427 GHz)'.

7.5.1.1.2 Setări avansate

Device Configuration

General Setup **Advanced Settings**

Mode	802.11g+n
HT mode	20MHz
Country code	00 - World
Transmit power	100 %
Fragmentation threshold	
RTS/CTS threshold	

	Nume câmp	Valori posibile	Explicație
1.	Mode	Auto, 802.11b, 802.11g, 802.11g+n	Diferitele moduri suportă standarde wireless diferite, ce afectează în mod direct capacitatea conexiunii radio
2.	HT mode	20MHz / 40MHz 2nd channel above Al 2-lea canal de mai sus	Modul HT (High Throughput) Capacitate mare . Banda de frecvență de 40 MHz oferă performanțe superioare
3.	Country code	Orice cod de țară conform ISO/IEC 3166	Coduri de țară alpha-2 astfel cum sunt definite de standardul ISO 3166-1
4.	Transmit power Putere emisie	20% / 40% / 60% / 80% / 100 %	Puterea semnalului Wi-Fi
5.	Fragmentation threshold Prag fragmentare	256-2346	Cel mai mic pachet ce poate fi fragmentat și transmis în mai multe cadre. În zonele în care interferențele creează probleme, setarea unui prag de fragmentare mai scăzut poate reduce probabilitatea eșuării transferului pachetelor, crescând astfel viteza
6.	RTS/CTS threshold Prag RTS/CTS	0-2347	RTS/CTS (Request to Send/Clear to Send) sunt mecanisme folosite pentru reducerea coliziunilor create de problema nodului ascuns. Acestea pot ajuta la rezolvarea problemelor apărute când mai multe puncte de acces concurează în aceeași zonă

7.5.1.2 Configurarea interfeței

7.5.1.2.1 Setări generale

Interface Configuration

General Setup **Wireless Security** **MAC Filter** **Advanced Settings**

SSID	HAL9000
Hide SSID	<input type="checkbox"/>

	Nume câmp	Valori posibile	Explicație
1.	SSID	Orice nume	Numele interfeței Dvs. Wi-Fi. Când alte calculatoare sau dispozitive cu capabilități Wi-Fi scană zona pentru rețele Wi-Fi, acestea vor vedea rețeaua Dvs. cu acest nume
2.	Hide SSID	Activat/Dezactivat	Va ascunde SSID-ul Dvs. altor dispozitive ce încearcă să scanzeze zona

7.5.1.2.2 Securitate wireless

Tab-ul Wireless Security |Securitate wireless| este folosit pentru a determina tipul criptării utilizate de rețeaua Dvs. WLAN. Puteți alege dintre diferitele tipuri de WEP (Wireless Encryption Protocol) sau WPA (Wi-Fi Protected Access). WPA oferă o securitate crescută întrucât folosește o mai bună criptare a datelor prin protocolul TKIP, însă nu toate dispozitivele suportă WPA, ci funcționează numai cu criptarea de tip WEP.

7.5.1.2.2.1 WEP

Interface Configuration

General Setup **Wireless Security** **MAC Filter** **Advanced Settings**

Encryption	WEP open system
Used key slot	Key #1
Key #1
Key #2
Key #3
Key #4

	Nume câmp	Valoare în exemplu	Explicație
1.	Encryption*	WEP open system Sistem deschis WEP	Tipul de criptare Wi-Fi folosită
2.	Used key slot	Key #1 Cheie#1	Ce cheie este folosită pentru autentificare
3.	Key #1 / Key #2 / Key #3 / Key #4	*****	O cheie personalizată din 10 caractere folosită pentru autentificare

7.5.1.2.2.2 WPA

Interface Configuration

General Setup **Wireless Security** **MAC Filter** **Advanced Settings**

Encryption	WPA-PSK/WPA2-PSK mixed mode
Cipher	Auto
Key

	Nume câmp	Valoare în exemplu	Explicație
1.	Encryption*	WPA-PSK/WPA2-PSK mixed mode	Tipul de criptare Wi-Fi folosită
2.	Cipher Cifru	Auto	Algoritmul folosit pentru criptare sau decriptare
3.	Key	*****	Parolă personalizată folosită pentru autentificare (de cel puțin 8 caractere)

*Unele metode de autentificare nu vor suporta criptarea TKIP (și TKIP&CCMP)

7.5.1.2.3 Filtrarea adreselor MAC

Tab-ul MAC Filter |Filtrare adrese MAC| este folosit pentru stabilirea de reguli ce permit sau interzic dispozitivelor cu adresele MAC specificate să acceseze rețeaua Dvs. Wi-Fi.

The screenshot shows the 'Interface Configuration' interface with the 'MAC Filter' tab selected. Under 'MAC address filter', the dropdown is set to 'Allow listed only'. The 'MAC list' contains two entries: 'C0:11:73:94:E8:E5' (with a delete icon) and '18:66:da:28:6a:34' (which is highlighted with a yellow background and has a delete and add icon below it).

	Nume câmp	Valoare în exemplu	Explicație
1.	MAC address filter	Allow listed only Permite numai cele din listă /Allow all except listed Permite toate fără cele din listă	Allow listed only – permite doar dispozitivelor care au adresele MAC specificate în listă să se conecteze la rețeaua Dvs. Wi-Fi Allow all except listed – interzice dispozitivelor care au adresele MAC specificate în listă să se conecteze la rețeaua Dvs. Wi-Fi
2.	MAC list	C0:11:73:94:E8:E5	Lista de adrese MAC cărora li se permite sau nu conectarea la rețeaua Dvs. Wi-Fi

7.5.1.2.4 Setări avansate

The screenshot shows the 'Interface Configuration' interface with the 'Advanced Settings' tab selected. It displays two settings: 'Separate clients' (checkbox checked) and 'Increase TTL packet size' (checkbox checked).

	Nume câmp	Valoare în exemplu	Explicație
1.	Separate clients Separare clienti	Activat/Dezactivat	Împiedică clientii Wi-Fi să comunice între ei în aceeași subrețea
2.	Increase TTL packet size	Activat/Dezactivat	Mărește dimensiunea TTL pentru pachetele recepționate

7.5.2 Stație wireless

Routerul RUT955 poate funcționa și ca un client Wi-Fi. Configurarea modului client este aproape identică cu configurarea punctului de acces, cu excepția faptului că majoritatea opțiunilor sunt dictate de punctul de acces wireless la care se conectează routerul. Modificarea lor poate duce la întreruperea conexiunii cu punctul de acces respectiv.

Pe lângă opțiunile standard, puteți și să dați clic butonul **Scan** pentru a scana zona înconjurătoare și a încerca conectarea la un nou punct de acces wireless.

WAN

Your WAN configuration determines how the router will be connecting to the internet.

Operation Mode					
Main WAN	Backup WAN	Interface Name	Protocol	IP Address	Sort
	<input checked="" type="radio"/>	WiFi (WAN)	DHCP	-	Edit Scan
	<input checked="" type="radio"/>	Wired (WAN2)	Static	192.168.90.66	Edit
	<input type="radio"/>	Mobile (WAN3)	None	188.69.245.225	Edit

[Save](#)

După care veți fi redirecționat la fereastra de mai jos.

Site Survey

Warning! During scan wireless will be temporarily shutdown. If you are connecting to the router via its wireless Access Point or via its wireless WAN you will lose the connection and won't be able to inspect the result of the scan.

[Start scan](#)

Apăsarea butonului **Start scan** |Pornire scanare| va iniția scanarea punctelor de acces Wi-Fi disponibile în zonă. După finalizarea scanării, veți vedea lista acestor puncte de acces. Alegeti punctul de acces dorit și apăsați butonul **Join Network** |Accesare rețea| din dreptul acestuia.

Teltonika_Pardavimai 55% Channel: 1 Mode: Master BSSID: 00:1E:42:9A:70:A3 Encryption: WPA2 PSK (CCMP)	Join Network
GUEST_TELTONIKA 50% Channel: 1 Mode: Master BSSID: 00:F1:02:10:34:23 Encryption: WPA2 PSK (CCMP)	Join Network
GUEST_TELTONIKA 42% Channel: 4 Mode: Master BSSID: 00:F1:02:FF:BA:FC Encryption: WPA2 PSK (CCMP)	Join Network
RUT240_001E42190D8B 77% Channel: 8 Mode: Master BSSID: 00:1E:42:19:0D:8B Encryption: None	Join Network

[Repeat scan](#)

7.6 Firewall

În această secțiune vom examina diversele funcții de firewall ale routerului RUT955.

7.6.1 Setări generale

Firewall-ul routerului este un pachet iptables standard în Linux, ce folosește lanțuri și politici de rutare pentru a facilita controlul traficului de intrare și ieșire.

The screenshot shows the Teltonika RUT955 web interface. At the top, there's a navigation bar with the Teltonika logo, Status, Network, Services, System, and Logout. Below the navigation bar, a horizontal menu bar has tabs for General Settings (which is selected), Port Forwarding, Traffic Rules, Custom Rules, DDOS Prevention, and Port Scan Prevention. The main content area is titled "Firewall" and contains a sub-section titled "General Settings". It includes a checkbox for "Drop invalid packets" and four dropdown menus for "Input" (set to "Accept"), "Output" (set to "Accept"), and "Forward" (set to "Reject").

	Nume câmp	Valori posibile	Explicație
1.	Drop Invalid packets	Bifat/Nebifat	Se efectuează o acțiune de "refuzare" asupra unui pachet determinat a fi invalid
2.	Input Intrare	Reject Respingere / Drop Refuzare / Accept Acceptare	Acțiunea IMPLICITĂ* ce va fi efectuată pentru pachetele care trec prin lanțul Input
3.	Output Ieșire	Reject/Drop/Accept	Acțiunea IMPLICITĂ* ce va fi efectuată pentru pachetele care trec prin lanțul Output
4.	Forward Forwardare	Reject/Drop/Accept	Acțiunea IMPLICITĂ* ce va fi efectuată pentru pachetele care trec prin lanțul Forward

*IMPLICIT: Când un pachet trece printr-un lanț al firewall-ului, acesta este raportat la regulile lanțului respectiv. Dacă nicio regulă nu se aplică pentru pachetul în cauză, se efectuează acțiunea respectivă (refuzare, respingere sau acceptare)

Acceptare – Pachetul continuă până la lanțul următor;

Refuzare – Pachetul este oprit și șters;

Respingere – Pachetul este oprit, șters și, spre deosebire de Refuzare, un pachet ICMP conținând un mesaj de respingere este trimis către **sursa** pachetului refuzat.

7.6.2 DMZ

Prin activarea zonei demilitarizate (DMZ) pentru o anumită gazdă internă (de ex., calculatorul Dvs.), veți expune acea gazdă și serviciile acesteia rețelei WAN a routerului (adică internetul).

DMZ Configuration			
	Nume câmp	Valori posibile	Explicație
1.	Enable	Bifat/Nebifat	Activează DMZ
2.	DMZ host IP address Adresă IP gazdă DMZ	Orice adresă IP din rețeaua Dvs. LAN	Gazda internă căreia îi va fi aplicată regula DMZ

7.6.3 Forwardarea între zone

O secțiune de tip zonă grupează una sau mai multe interfețe și servește drept sursă ori destinație pentru forwardări, reguli și redirecționări. Fereastra Zone Forwarding vă permite configurarea acestor forwardări.

Zone Forwarding			
Source zone	Destination zones	Default forwarding action	
lan:lan:		accept ▾	Edit
wan:ppp: wan: wan3:		reject ▾	Edit
vpn: openvpn:	lan	reject ▾	Edit
i2tp: i2tp:	lan	reject ▾	Edit
pptp: pptp:	lan	reject ▾	Edit
gre: gre tunnel:	lan	reject ▾	Edit
hotspot:		accept ▾	Edit
lan_Lan2:lan_Lan2:	wan	reject ▾	Edit

	Nume câmp	Valoare în exemplu	Explicație
1.	Source zone	vpn: openvpn	Zona-sursă din care vor fi redirecționate pachetele de date
2.	Destination zones Zone destinație	lan	Zona-destinație către care vor fi redirecționate pachetele de date
3.	Default forwarding action Acțiune forwardare implicită	reject	Acțiunea ce va fi efectuată asupra pachetelor redirecționate

7.6.4 Forwardarea porturilor

Fereastra Port Forwarding este folosită pentru configurarea serverelor și serviciilor pe mașini din rețeaua LAN locală. Imaginea de mai jos arată cum puteți crea o regulă care să permită unui site web găzduit la 192.168.1.109 să fie accesat din exterior, introducând <http://routersExternalIp:12345/>.

The screenshot shows the Teltonika RUT955 router's configuration interface under the 'Services' tab. The 'Port Forwarding' sub-tab is selected. The main area displays a table of existing port forwarding rules:

Name	Protocol	Source	Via	Destination	Enable	Sort	Action Buttons		
Enable_SSH_WAN_PASSTHROUGH	TCP	From any host in wan	To any router IP at port 22	Forward to IP 127.0.0.1, port 22 in lan	<input type="checkbox"/>			Edit	Delete
Enable_HTTP_WAN_PASSTHROUGH	TCP	From any host in wan	To any router IP at port 80	Forward to IP 127.0.0.1, port 80 in lan	<input type="checkbox"/>			Edit	Delete
Enable_HTTPS_WAN_PASSTHROUGH	TCP	From any host in wan	To any router IP at port 443	Forward to IP 127.0.0.1, port 443 in lan	<input type="checkbox"/>			Edit	Delete
Enable_CLI_WAN_PASSTHROUGH	TCP	From any host in wan	To any router IP at port 4200	Forward to IP 127.0.0.1, port 4200 in lan	<input type="checkbox"/>			Edit	Delete
Redirect_DNS	TCP, UDP	From any host in lan	To any router IP at port 53	Forward to IP 192.168.1.1, port 53 in lan	<input type="checkbox"/>			Edit	Delete

Below this is a section titled 'New Port Forward Rule' with fields for Name, Protocol, External port(s), Internal IP, and Internal port(s). A table below details the fields and their descriptions:

Nume câmp	Valori posibile	Explicație
1. Name	Numele noii reguli	Numele regulii, folosit exclusiv pentru facilitarea gestionării acesteia
2. Protocol	TCP/UDP/TCP+UDP/Other Altul	Tipul protocolului pachetului de intrare
3. External Port Port extern	1800 or 2000-2200	Traficul va fi forwardat de la acest port din rețeaua WAN
4. Internal IP address Adresă IP internă	Adresa unui dispozitiv din rețeaua Dvs. LAN	Adresa IP a mașinii interne care găzduiește un serviciu care dorîți să fie accesat din afară
5. Internal port Port intern	1800 sau 2000-2200	Regula va redirecționa traficul către acest port pe mașina internă

RUT955 Manual de utilizare

Dând clic pe butonul Edit puteți perfecționa o regulă, dacă doriti:

Name	Protocol	Source	Via	Destination	Enable	Sort
Enable_SSH_WAN_PASSTHROUGH	TCP	From any host in wan	To any router IP at port 22	Forward to IP 127.0.0.1, port 22 in lan	<input type="checkbox"/>	 



TELTONIKA Status ▾ Network ▾ Services ▾ System ▾ Logout

General Settings Port Forwarding Traffic Rules Custom Rules DDOS Prevention Port Scan Prevention

Firewall - Port Forwards - Enable_SSH_WAN_PASSTHROUGH

This page allows you to change advanced properties of the port forwarding entry. Although, in most cases there is no need to modify those settings.

Enable

Name

Protocol

Source zone gre: gre tunnel: 
 hotspot: 
 l2tp: l2tp: 
 lan: lan: 
 lan_Lan2: lan_Lan2: 
 pptp: pptp: 
 vpn: openvpn: 
 wan: ppp:  wan:  wan3: 

Source MAC address 

Source IP address

Source port

External IP address

External port

Nume câmp	Valori posibile	Explicație
1. Name	Numele regulii	Numele regulii
2. Protocol	TCP/UDP/TCP+UDP/ICMP/Custom	Puteți specifica mai multe selectând (custom) și apoi introducând protocolele separate prin spații
3. Source zone	gre/hotspot/l2tp/lan/pptp/vpn/wan	Aplicați regula numai traficului de intrare din această zonă
4. Source MAC address Adresă MAC sursă	Orice adresă MAC	Aplicați regula numai traficului de intrare de la aceste adrese MAC
5. Source IP address Adresă IP sursă	Orice adresă IP sau domeniu de adrese IP	Aplicați regula numai traficului de intrare de la această adresă IP/domeniu de adrese IP
7. Source port Port sursă	Orice port	Aplicați regula numai traficului de intrare cu originea în portul sau domeniul de porturi specificat de pe gazda client
8. External IP address Adresă IP externă	Orice adresă IP externă	Aplicați regula numai traficului de intrare direcționat către adresa IP specificată

9.	External port Port extern	Orice port extern	Aplicați regula numai traficului de intrare direcționat către portul sau domeniul de porturi de pe această gazdă
----	----------------------------	-------------------	--

Internal zone gre: gre tunnel:

hotspot:

l2tp: l2tp:

lan: lan:

lan_Lan2: lan_Lan2:

pptp: pptp:

vpn: openvpn:

wan: ppp: wan: wan3:

Internal IP address

Internal port

Enable NAT loopback

Extra arguments

[Back to Overview](#) **Save**

Teltonika solutions

www.teltonika.lt

10.	Internal zone Zonă internă	gre/hotspot/l2tp/lan/pptp/vpn/wan	Redirecționați traficul de intrare vizat de regulă către zona internă specificată
11.	Internal IP address	Orice adresă IP internă	Redirecționați traficul de intrare vizat de regulă către gazda internă specificată
12.	Internal port	Orice port	Redirecționați traficul de intrare vizat de regulă către portul specificat de pe gazda internă
13.	Enable NAT loopback	Activare/Dezactivare	NAT loopback permite rețelei Dvs. locale (adică aflată după routerul/modemul Dvs.) să se conecteze la o adresă IP orientată către înainte (de ex. 208.112.93.73) a unei mașini aflate de asemenea în rețeaua Dvs. locală
14.	Extra arguments Argumente suplimentare	-	Introduce argumente suplimentare în iptables. Folosiți cu atenție!

7.6.5 Reguli pentru trafic

Pagina Traffic Rules |Reguli trafic| conține opțiuni mai generalizate de definire a regulilor. Aici puteți bloca sau deschide porturi, puteți schimba modul în care traficul este forwardat între rețelele LAN și WAN, și multe altele.

Name	Protocol	Source	Destination	Action	Enable	Sort
Allow-DHCP-Relay	UDP	From any host in wan	To any router IP at port 67 on this device	Accept input	<input type="checkbox"/>	Edit Delete
Allow-DHCP-Renew	UDP	From any host in wan	To any router IP at port 68 on this device	Accept input	<input checked="" type="checkbox"/>	Edit Delete
Allow-Ping	ICMP with type echo-request	From any host in wan	To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	Edit Delete
Allow-vpn-traffic	TCP, UDP	From any host in wan	To any router IP at port 1194 on this device	Accept input	<input checked="" type="checkbox"/>	Edit Delete

	Nume câmp	Explicație
1.	Name	Numele regulii. Folosit pentru facilitarea gestionării acestor reguli
2.	Protocol	Tipul protocolului pachetului de intrare sau ieșire
3.	Source Sursă	Aplicați regula numai traficului de intrare de la această adresă IP/domeniu de adrese IP
4.	Destination Destinație	Redirecționați traficul vizat de regulă către adresa IP și portul de destinație specificate
5.	Action	ACTIONA ce va fi efectuată asupra pachetului dacă i se aplică regula
6.	Enable	Debifați pentru a dezactiva regula. Regula nu va fi ștersă, dar nici nu va fi încărcată în firewall
7.	Sort	Când un pachet sosește, se verifică dacă i se aplică vreo regulă. Dacă există mai multe reguli aplicabile, se aplică prima, adică ordinea din lista de reguli afectează modul de operare al firewall-ului Dvs., de aceea vi se permite să sortați lista după cum dorîți

Dând clic pe Edit puteți perfectiona o regulă, dacă doriți:

Traffic Rules						
Name	Protocol	Source	Destination	Action	Enable	Sort
Allow-DHCP-Relay	UDP	From any host in wan	To any router IP at port 67 on this device	Accept input	<input type="checkbox"/>	 



Firewall - Traffic Rules - Allow-DHCP-Relay

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Enable

Name

Restrict to address family

Protocol

Match ICMP type 

Source zone Any zone
 gre: gre tunnel:
 hotspot:
 l2tp: l2tp:
 lan: lan:
 lan_Lan2: lan_Lan2:
 pptp: pptp:
 vpn: openvpn:
 wan: ppp:  wan:  wan3: 

Source MAC address

Source address

Source port

	Nume câmp	Valori posibile	Explicație
1.	Name	Numele regulii	Folosit pentru facilitarea gestionării acestoră
2.	Restrict to address family Restrângere la familia de adrese	IPv4 and IPv6 / IPv4 only / IPv6 only	Aplicați regula numai traficului de la familia de adrese selectată
3.	Protocol	TCP / UDP / Any / ICMP / Custom	Protocolul pachetului care este verificat dacă i se aplică regulile de trafic
4.	Match ICMP type Potrivire cu tip ICMP	Any	Aplicați regula numai traficului cu tipul ICMP selectat
5.	Source zone	Any zone Orice zonă / gre / hotspot / l2tp / lan / pptp / vpn / wan	Aplicați regula numai traficului de intrare din zona selectată
6.	Source MAC address	Orice adresă MAC	Aplicați regula numai traficului de intrare de la aceste adrese MAC
7.	Source address Adresă sursă	Orice adresă IP sau interval de adrese IP	Aplicați regula numai traficului de intrare de la această adresă IP/domeniu de adrese IP

8.	Source port	Orice port	Aplicați regula numai traficului de intrare cu originea în portul sau domeniul de porturi specificat de pe gazda client
----	-------------	------------	---

Destination zone Device (input) Any zone (forward) gre: gre tunnel:  hotspot:  i2tp: i2tp:  lan: lan:    lan_Lan2: lan_Lan2:  pptp: pptp:  vpn: openvpn:  wan: ppp:  wan:   

Destination address

Destination port

Action

Extra arguments

[Back to Overview](#)

Teltonika solutions

www.teltonika.lt

9.	Destination zone	Device Dispozitiv /Any zone/LAN/VPN/WAN	Aplicați regula numai traficului forwardat către zona-destinație specificată
10.	Destination address	any	Aplicați regula numai traficului forwardat către adresa IP/domeniul de adrese IP specificate ca destinație
11.	Destination port	67	Aplicați regula numai traficului forwardat către portul sau domeniul de porturi specificat ca destinație
12.	Action	Drop/Accept/Reject + chain lanț + additional rules reguli suplimentare	Acțiunea ce va fi efectuată asupra pachetului dacă i se aplică regula. Puteți și să definiți opțiuni suplimentare precum limitarea volumului de pachete și definirea căruia lanț îi aparține regula

7.6.5.1 Porturi deschise pe router

Open Ports On Router

Name	Protocol	External port
------	----------	---------------

<input style="width: 150px; background-color: #ffffcc;" type="text" value="Open_Port_Rule"/>	<input style="width: 100px; height: 20px;" type="button" value="TCP+UDP"/>	<input style="width: 100px; margin-left: 10px;" type="text"/>	<input style="width: 50px; height: 20px; margin-left: 10px;" type="button" value="Add"/>
--	--	---	--

Nume câmp	Valoare în exemplu	Explicație
1. Name	Open_Port_Rule	Numele regulii, folosit pentru facilitarea gestionării
2. Protocol	TCP/UDP/Any/ICMP/Custom	Protocolul pachetului care este verificat dacă i se aplică regulile de trafic
3. External port	1-65535	Aplicați regula traficului de intrare direcționat către portul sau domeniul de porturi de pe această gazdă

7.6.5.2 Regulă de forwardare nouă

New Forward Rule

Name	Source	Destination
New_Forward_Rule	LAN	WAN
<input type="button" value="Add"/>		

Nume câmp	Valori posibile	Explicație
1. Name	Numele regulii	Numele regulii, folosit pentru facilitarea gestionării
2. Source	GRE / HOTSPOT / L2TP / LAN / PPTP / VPN / WAN	Aplicați regula numai traficului de intrare provenit de la familia de adrese selectată ca sursă
3. Destination	GRE / HOTSPOT / L2TP / LAN / PPTP / VPN / WAN	Forwardați traficul de intrare numai către familia de adrese selectată ca destinație

7.6.5.3 Translatarea adresei sursă

Source Network Address Translation (Source NAT/SNAT) este o formă specifică de mascaradare ce permite controlul detaliat al adresei IP sursă folosită pentru traficul de ieșire, de ex. pentru maparea mai multor adrese WAN în subrețele interne.

Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Protocol	Source	Destination	SNAT	Enable
New_SNAT_Rule	All	From any host in lan	To any host, port 15465 in wan	Rewrite to source IP 192.168.55.55, port 15465	<input type="checkbox"/>
<input type="button" value="Edit"/> <input type="button" value="Delete"/>					

New Source NAT

Name	Source	Destination	Source IP	Source port
New SNAT rule	LAN	WAN		<input type="button" value="Do not rewrite"/>
<input type="button" value="Add"/>				
<input type="button" value="Save"/>				

Nume câmp	Valori posibile	Explicație
1. Name	Numele regulii	Numele regulii, folosit pentru facilitarea gestionării
2. Protocol	TCP/UDP/Any/ICMP/Custom	Protocolul pachetului care este verificat dacă i se aplică regulile de trafic
3. Source	GRE / HOTSPOT / L2TP / LAN / PPTP / VPN / WAN	Aplicați regula numai traficului de intrare provenit de la familia de adrese selectată
4. Destination	GRE / HOTSPOT / L2TP / LAN / PPTP / VPN / WAN	Forwardați traficul de intrare numai către familia de adrese selectată
5. SNAT	Rewrite to source IP Rescriere la IP-sursă 192.168.55.55, port 15465	SNAT rescrie adresa IP sursă și portul-sursă ale pachetului
6. Enable	Activare/Dezactivare	Activează/dezactivează regula

Puteți configura regulile când clic pe butonul "Edit" din dreptul lor:

Source NAT						
Name	Protocol	Source	Destination	SNAT	Enable	
New_SNAT_Rule	All	From any host in lan	To any host, port 15465 in wan	Rewrite to source IP 192.168.55.55, port 15465	<input checked="" type="checkbox"/>	 



Firewall - Traffic Rules - SNAT New_SNAT_Rule

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Enable

Name

Protocol

Source zone gre: gre tunnel:
 hotspot:
 l2tp: l2tp:
 lan: lan:
 lan_Lan2: lan_Lan2:
 pptp: pptp:
 vpn: openvpn:
 wan: ppp: wan: wan3:

Source MAC address

Source IP address

Source port

	Nume câmp	Valoare în exemplu	Explicație
1.	Name	Numele regulii	Numele regulii, folosit pentru facilitarea gestionării
2.	Protocol	All protocols Toate protocolele / TCP / UDP / TCP+UDP / ICMP / Custom	Protocolul pachetului care este verificat dacă i se aplică regulile de trafic
3.	Source zone	Any zone/ gre / hotspot / l2tp / lan / pptp / vpn / wan	Aplicați regula numai traficului de intrare din această zonă
4.	Source MAC address	Orice adresă MAC	Aplicați regula numai traficului de intrare de la aceste adrese MAC
5.	Source address	Orice adresă IP sau domeniu de adrese IP	Aplicați regula numai traficului de intrare de la această adresă IP/domeniu de adrese IP
6.	Source port	Orice port	Aplicați regula numai traficului de intrare cu originea în portul sau domeniul de porturi specificat de pe gazdă client

Destination zone gre: gre tunnel:

hotspot:

l2tp: l2tp:

lan: lan:

lan_Lan2: lan_Lan2:

pptp: pptp:

vpn: openvpn:

wan: ppp: wan: wan3:

Destination IP address

Destination port

SNAT IP address

SNAT port

Extra arguments

[Back to Overview](#) Save

Teltonika solutions

www.teltonika.lt

7.	Destination zone	Device/Any zone/LAN/VPN/WAN	Aplicați regula numai traficului forwardat către zona-destinație specificată
8.	Destination address	Orice adresă IP	Aplicați regula numai traficului forwardat către adresa IP/domeniul de adrese IP specificate ca destinație
9.	Destination port	Orice port	Aplicați regula numai traficului forwardat către portul sau domeniul de porturi specificate ca destinație
10.	SNAT IP address	Orice adresă IP	Rescrieți traficul căruia i se aplică regula la adresa IP specificată
11.	SNAT port	Orice port	Rescrieți traficul căruia i se aplică regula la portul sursă specificat. Puteți lăsa gol pentru a rescrie numai adresa IP
12.	Extra arguments		Introduce argumente suplimentare în iptables. Folosiți cu atenție!

7.6.6 Reguli personalizate

Pagina Custom Rules |Reguli personalizate| vă oferă cea mai mare libertate în definirea regulilor – le puteți introduce direct în programul iptables. Doar tastați-le în câmpul de tip text și vor fi executate ca un shell script Linux. Dacă nu știți sigur cum să folosiți iptables, căutați pe internet manuale, exemple și explicații.

TELTONIKA Status ▾ Network ▾ Services ▾ System ▾ Logout

General Settings Port Forwarding Traffic Rules **Custom Rules** DDOS Prevention Port Scan Prevention

Firewall - Custom Rules

Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
```

Reset Save

7.6.7 Prevenirea atacurilor de blocare distribuită a serviciului (DDOS)

Pagina DDOS Prevention |Prevenire atacuri DDOS| vă permite să instituiți metode de protecție împotriva diferitelor tipuri de atacuri. Mai jos veți găsi informații despre toate aceste metode.

7.6.7.1 Protectia împotriva atacurilor de tip SYN flood

Pagina SYN Flood Protection vă permite să vă protejați împotriva atacurilor ce exploatează o parte din handshake-ul tripartit normal din TCP pentru a consuma resursele serverului-țintă și a-l bloca. În esență, cu atacurile DDoS de tip SYN flood, atacatorul trimite solicitări de conectare TCP mai repede decât mașina-țintă la poate procesa, cauzând suprasaturarea rețelei.

The screenshot shows the Teltonika RUT955 web interface with the following details:

- Header:** TELTONIKA logo, Status, Network, Services, System, Logout.
- Navigation Bar:** General Settings, Port Forwarding, Traffic Rules, Custom Rules, **DDOS Prevention** (highlighted in blue), Port Scan Prevention.
- Section Title:** DDOS Prevention > SYN Flood Protection.
- Form Fields:**
 - Enable SYN flood protection:
 - SYN flood rate: 25
 - SYN flood burst: 50
 - TCP SYN cookies:

	Nume câmp	Valori posibile	Explicație
1.	Enable SYN flood protection	Activare/Dezactivare	Face routerul mai rezistent la atacuri de tip SYN flood
2.	SYN flood rate	Numere întregi	Setează rata maximă (în pachete pe secundă) pentru pachete SYN peste care traficul este considerat inundat
3.	SYN flood burst	Numere întregi	Setează numărul maxim de pachete inițiale pentru pachetele SYN peste care traficul este considerat inundat dacă depășește rata permisă
4.	TCP SYN cookies	Activare/Dezactivare	Activează folosirea de SYN cookies (alegeri de numere de secvență inițiale speciale efectuate de serverele TCP)

7.6.7.2 Cereri ICMP de la distanță

Unii atacatori folosesc pachete cu cereri de ecou ICMP direcționate către adrese de broadcast IP din locații îndepărte pentru a genera atacuri de blocare a serviciului (DoS).

Remote ICMP Requests

Enable ICMP requests	<input checked="" type="checkbox"/>
Enable ICMP limit	<input type="checkbox"/>
Limit period	Second <input type="button" value="▼"/>
Limit	<input type="text" value="10"/>
Limit burst	<input type="text" value="5"/>

	Nume câmp	Valori posibile	Explicație
1.	Enable ICMP requests	Activare/Dezactivare	Blochează cererile de ecou ICMP de la distanță
2.	Enable ICMP limit	Activare/Dezactivare	Activăți limita de cereri de ecou ICMP în perioada selectată
3.	Limit period Perioadă limitare	Second/Minute/Hour/Day	Selectați perioada pentru limitarea cererilor de ecou ICMP
4.	Limit Limită	Numere întregi	Numărul maxim de cereri de ecou ICMP în perioadă
5.	Limit burst	Numere întregi	Indicați numărul maxim de pachete inițiale înainte să se aplice limita de mai sus

7.6.7.3 Prevenirea atacurilor prin SSH

Preveniți atacurile prin SSH (permite unui utilizator să ruleze comenzi pe interpretorul liniei de comandă al unei mașini fără a fi prezent fizic lângă mașină) prin limitarea conexiunilor într-o perioadă specificată.

SSH Attack Prevention

Enable SSH limit	<input type="checkbox"/>
Limit period	Second <input type="button" value="▼"/>
Limit	<input type="text" value="10"/>
Limit burst	<input type="text" value="5"/>

	Nume câmp	Valori posibile	Explicație
1.	Enable SSH limit	Activare/Dezactivare	Activăți limita de conexiuni SSH într-o perioadă selectată
2.	Limit period	Second/Minute/Hour/Day	Perioada în care vor fi limitate conexiunile SSH
3.	Limit	Numere întregi	Numărul maxim de conexiuni SSH în perioada stabilită
4.	Limit burst	Numere întregi	Indicați numărul maxim de conexiuni inițiale înainte să se aplice limita de mai sus

7.6.7.4 Prevenirea atacurilor prin HTTP

Un atac HTTP trimite un antet HTTP complet, legitim, ce include un câmp Content-Length pentru specificarea dimensiunea corpului mesajului care urmează. Cu toate acestea, atacatorul trimite apoi corpul efectiv al mesajului la o viteză extrem de redusă (de ex. 1 octet la 110 secunde). Datorită faptului că mesajul întreg este corect și complet, serverul-țintă va încerca să respecte câmpul Content-Length din antet și să aștepte ca întreg corpul mesajului să fie transmis, încetinind astfel.

HTTP Attack Prevention

Enable HTTP limit

Limit period

Limit

Limit burst

	Nume câmp	Valori posibile	Explicație
1.	Enable HTTP limit	Activare/Dezactivare	Limitează conexiunile HTTP în perioada de timp stabilită
2.	Limit period	Second/Minute/Hour/Day	Perioada în care vor fi limitate conexiunile HTTP
3.	Limit	Număr întreg	Numărul maxim de conexiuni HTTP în perioada stabilită
4.	Limit burst	Număr întreg	Numărul maxim de conexiuni inițiale înainte să se aplice limita de mai sus

7.6.7.5 Prevenirea atacurilor prin HTTPS

HTTPS Attack Prevention

Enable HTTPS limit

Limit period

Limit

Limit burst

	Nume câmp	Valori posibile	Explicație
1.	Enable HTTPS limit	Activare/Dezactivare	Limitează conexiunile HTTPS în perioada de timp stabilită
2.	Limit period	Second/Minute/Hour/Day	Perioada în care vor fi limitate conexiunile HTTPS
3.	Limit	Număr întreg	Numărul maxim de conexiuni HTTPS în perioada stabilită
4.	Limit burst	Număr întreg	Numărul maxim de conexiuni inițiale înainte să se aplice limita de mai sus

7.6.8 Prevenirea scanării porturilor

7.6.8.1 Scanarea porturilor

The screenshot shows the Teltonika RUT955 web interface with the following navigation bar:

- TELTONIKA logo
- Status ▾
- Network ▾
- Services ▾
- System ▾
- Logout

The main menu bar includes the following tabs:

- General Settings
- Port Forwarding
- Traffic Rules
- Custom Rules
- DDOS Prevention
- Port Scan Prevention**

The current page is "Port Scan Prevention". Under the "Port Scan" section, there are three configuration fields:

- Enable: A checkbox.
- Interval: A text input field containing "30".
- Scan count: A text input field containing "10".

	Nume câmp	Valori posibile	Explicație
1.	Enable	Activare/Dezactivare	Activează prevenirea scanării porturilor
2.	Interval	10-60	Intervalul de timp în secunde în care sunt contorizate scanările porturilor
3.	Scan count Contor scanări	5-65534	Numărul de scanări ale porturilor înainte de a fi blocate

7.6.8.1 Tipul de apărare

The screenshot shows the Teltonika RUT955 web interface with the following navigation bar:

- TELTONIKA logo
- Status ▾
- Network ▾
- Services ▾
- System ▾
- Logout

The main menu bar includes the following tabs:

- General Settings
- Port Forwarding
- Traffic Rules
- Custom Rules
- DDOS Prevention
- Port Scan Prevention**

The current page is "Defending type". There are five checkboxes for different types of attacks:

- SYN-FIN attack
- SYN-RST attack
- X-Mas attack
- FIN scan
- NULLflags attack

	Nume câmp	Explicație
1.	SYN-FIN attack	Protejează împotriva atacurilor de tip SYN-FIN
2.	SYN-RST attack	Protejează împotriva atacurilor de tip SYN-RST
3.	X-Mas attack	Protejează împotriva atacurilor de tip X-Mas
4.	FIN scan	Protejează împotriva scanării FIN
5.	NULLflags attack	Protejează împotriva atacurilor de tip NULLflags

7.7 Rutarea

7.7.1 Rute statice

Rutele statice specifică prin ce interfață sau gateway poate fi accesată o anumită gazdă ori rețea. În pagina Static Routes vă puteți configura propriile Dvs. rute personalizate.

Routing table	Interface	Destination address	Netmask	Gateway	Metric
WAN	WAN (Wired)	0.0.0.0	0.0.0.0		0
WAN2	WAN2 (WiFi)	0.0.0.0	0.0.0.0		0
WAN3	WAN3 (Mobile)	0.0.0.0	0.0.0.0		0

Add

	Nume câmp	Valori posibile	Explicație
1.	Routing table Tabelă rutare	MAIN/WAN/WAN2/WAN3	Definește care tabelă va fi folosită pentru ruta în cauză
2.	Interface	MAIN/WAN/WAN2/WAN3	Zona în care rezidă rețeaua-țintă
3.	Destination address*	Adresă IP	Adresa rețelei-destinație
4.	Netmask*	Mască IP	Masca aplicată ţintei pentru a determina adresele IP efective căror li se aplică regula de rutare
5.	Gateway	Adresă IP	Unde trebuie să transmită routerul tot traficul căruia i se aplică regula
6.	Metric Metrică	Întreg	Folosită ca o măsură pentru ordonare. Dacă unui pachet care urmează să fie rutat i se aplică două reguli, se aplică regula cu metrica mai mare

*Note suplimentare privind destinația și masca de rețea:

Puteți defini o regulă care se aplică unei singure adrese IP astfel: Destination – **adresă IP oarecare**; Netmask – **255.255.255.255**. Mai departe, puteți defini o regulă care se aplică unui segment de adrese IP astfel: Destination – o adresă IP oarecare de la care **ÎNCEPE** segmentul; Netmask – mască de rețea ce definește mărimea segmentului. Exemplu:

192.168.55.161	255.255.255.255	Se aplică numai pentur 192.168.55.161
192.168.55.0	255.255.255.0	Se aplică adreselor IP din domeniul 192.168.55.0 – 192.168.55.255
192.168.55.240	255.255.255.240	192.168.55.240 – 192.168.55.255
192.168.55.161	255.255.255.0	192.168.55.0 – 192.168.55.255
192.168.0.0	255.255.0.0	192.168.0.0 – 192.168.255.255

7.7.1.1 Intrări ARP statice

Intrările ARP statice sunt folosite pentru a lege o adresă MAC de o anumită adresă IP. De exemplu, dacă doriți ca un dispozitiv oarecare să obțină aceeași adresă IP de fiecare dată când se conectează la router, puteți crea o intrare ARP statică prin legarea adresei MAC a respectivului dispozitiv de o adresă IP dorită. Apoi routerul va crea o intrare în tabela ARP, ceea ce asigură că respectivul dispozitiv va obține adresa IP specificată de fiecare dată.

Static ARP Entries		
IP address	MAC address	
192.168.56.56	11:22:33:44:55:66	<button>Delete</button>

Add

7.7.2 Rute dinamice

7.7.2.1 Aspecte generale

Rutarea dinamică permite routerului să selecteze căi în conformitate cu modificările în timp real ale topologiei logice a rețelei.

TELTONIKA Status Network Services System Logout

Static Routes Dynamic Routes

General OSPF Protocol General Protocols

Dynamic Routes

General Settings

Enable

Router ID 192.168.1.1

Save

	Nume câmp	Valoare	Explicație
1.	Enable	Activare/Dezactivare	Activăți ruturile dinamice
2.	Router ID	192.168.1.1	Identifierul routerului

7.7.2.2 Protocolul BGP

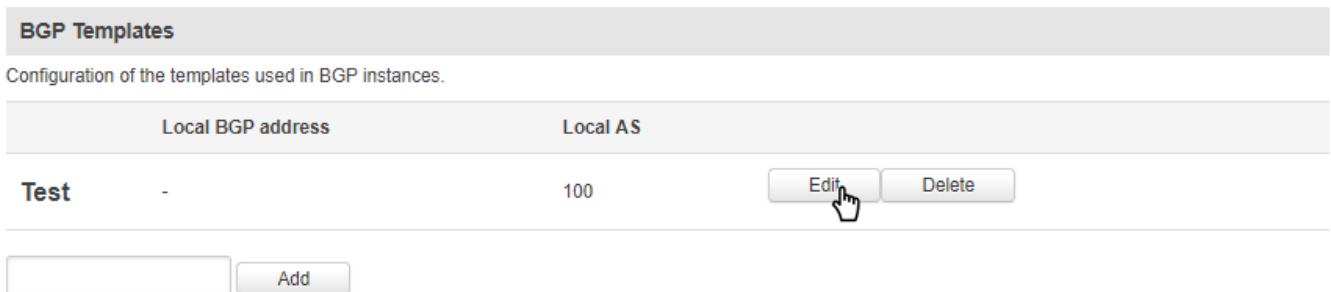
Border Gateway Protocol (BGP) este un protocol standard de exterior destinat schimbului de informații privind rutarea și accesibilitatea între sisteme autonome (AS) pe internet. Protocolul este clasificat deseori ca un protocol vector-cale, dar uneori și ca un protocol de rutare vector-distanță. Border Gateway Protocol ia decizii de rutare pe baza căilor, politicilor de rețea ori a seturilor de reguli configurate de un administrator de rețea și este implicat în luarea deciziilor de rutare în nucleu.

7.7.2.2.1 Şablonane BGP

Puteți crea un şablon BGP tastând un nume (numele de şablonane BGP pot conține numai litere) în bara de text și apăsând butonul “Add” |Adăugare| alăturat.



Această acțiune va crea un şablon nou cu numele dat de Dvs. Puteți apoi începe să vă configurați şablonul BGP apăsând butonul “Edit” alăturat.



După aceasta veți fi redirecționat către fereastra de configurare a protocolului BGP, unde vă puteți configura în detaliu noul Dvs. protocol.

7.7.2.2.2 Configurarea protocolului BGP Bird4

BGP Templates

Configuration of the templates used in BGP instances.

Local BGP address	<input type="text" value="192.168.56.1"/>
Local AS	<input type="text" value="100"/>
Import	<input type="text" value="All"/> ▾
Export	<input type="text" value="All"/> ▾
Source Address	<input type="text" value="192.168.1.1"/>
Next hop self	<input type="checkbox"/>
Next hop keep	<input type="checkbox"/>
Route Reflector server	<input type="checkbox"/>
Route Reflector Cluster ID	<input type="text"/>
Routes import limit	<input type="text" value="0"/>
Routes import limit action	<input type="text" value="warn"/> ▾
Routes export limit	<input type="text" value="0"/>
Routes export limit action	<input type="text" value="warn"/> ▾
Routes received limit	<input type="text" value="0"/>
Routes received limit action	<input type="text" value="warn"/> ▾

	Nume câmp	Valoare	Explicație
1.	Local BGP address	192.168.56.1	
2.	Local AS	100	
3.	Import	All Toate	
4.	Export	All	
5.	Source address	192.168.1.1	
6.	Next hop self	Activat/Dezactivat	
7.	Next hop keep	Activat/Dezactivat	
8.	Route Reflector server	Activat/Dezactivat	
9.	Route Reflector Cluster ID		
10.	Routes import limit	0	
11.	Routes import limit action	Warn Avertizare	
12.	Routes export limit	0	
13.	Routes export limit action	Warn	
14.	Routes received limit	0	
15.	Routes received limit action	warn	

7.7.2.3 Instanțe BGP

Puteți crea o instanță BGP tastând un nume (numele de instanțe BGP pot conține numai litere) în bara de text și apăsând butonul “Add” |Adăugare| alăturat.

BGP Instances

Configuration of the BGP protocol instances

Enable	Templates	Neighbor IP Address	Neighbor AS
<i>There are no BGP instances created yet.</i>			

Instance 

Instanța Dvs. este acum creată și ar trebui să fie vizibilă în tab-ul BGP Instances |Instanțe BGP|.

BGP Instances

Configuration of the BGP protocol instances

Enable	Templates	Neighbor IP Address	Neighbor AS	
Instance <input checked="" type="checkbox"/>	<input type="button" value="Test ▾"/>	192.168.90.66	100	<input type="button" value="Delete"/>
<input type="button" value=""/>		<input type="button" value="Add"/>		

	Nume câmp	Valoare	Explicație
1.	Enable	Activare/Dezactivare	Activăți sau dezactivați instanța BGP
2.	Template Şablon	Test	Selectați ce şablon BGP va folosi instanța
3.	Neighbour IP Address	192.168.90.66	Adresa IP a unui dispozitiv din vecinătate
4.	Neighbour AS	100	Sistemul autonom al dispozitivului din vecinătate

7.7.2.4 Protocolul OSPF

Open Shortest Path First (OSPF) este un protocol de rutare pentru rețele bazate pe Internet Protocol (IP). Acesta folosește un algoritm de rutare bazat pe starea legăturilor (link state) și aparține grupului de protocoale standard de interior (IGP), operând în interiorul unui singur sistem autonom. Este definit ca OSPF Version 2 în documentul RFC 2328 (1998) pentru IPv4.

7.7.2.4.1 Instanța generală a OSPF

General	OSPF Protocol	General Protocols
OSPF Protocol Configuration		
OSPF General Instance		
Enable	<input type="checkbox"/>	
Stub	<input type="checkbox"/>	
RFC1583 compatibility	<input type="checkbox"/>	
Import	All	<input type="button" value="▼"/>
Export	All	<input type="button" value="▼"/>

	Nume câmp	Valoare	Explicație
1.	Enable	Activare/Dezactivare	Activează protocolul OSPF
2.	Stub	Activare/Dezactivare	Schimbă zona în ciot
3.	RFC1583 compatibility	Activare/Dezactivare	Activează compatibilitatea OSPF cu specificația RFC1583
4.	Import	All Toate /None Niciuna / custom Particularizare	Setați dacă protocolul trebuie să importe rute
5.	Export	All/None/custom	Setați dacă protocolul trebuie să exporte rute

7.7.2.4.2 Zone OSPF

Rețeaua OSPF poate fi împărțită în subdomenii denumite zone.

OSPF Area			
Area name	Enable	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
1	No		
New area name:	<input type="text"/>	<input type="button" value="Add New"/>	<input type="button" value="Save"/>

	Nume câmp	Valoare	Explicație
1.	Area name	1	Numele zonei OSPF. Trebuie să fie un număr
2.	Enable	Yes/No Da/Nu	Activăți/dezactivați zona OSPF

Pentru a configura zona OSPF, apăsați butonul "Edit" alăturat.

OSPF Area

Area name	Value	
1	No	<input style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;" type="button" value="Edit"/> <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Delete"/>

Veți fi redirecționat către fereastra de configurare a zonei OSPF.

Area Instance: 1

Main Settings

Enabled	<input type="checkbox"/>	
Stub	<input type="checkbox"/>	

OSPF interface

Interface

Interface	Edit	Delete	
br-lan	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	

Interface
br-lan

OSPF networks

IP	Value	
192.168.56.0	<input type="checkbox"/>	<input type="button" value="Delete"/>

New IP:

	Nume câmp	Valoare	Explicație
1.	Enabled	Activare/Dezactivare	Activăți sau dezactivați zona OSPF
2.	Stub	Activare/Dezactivare	Activăți/dezactivați ciotul
3.	Interface	br-lan	O interfață pe care o va folosi zona
4.	New IP Adresă IP nouă	192.168.56.0	Adresele IP ale rețelelor OSPF ce aparțin zonei OSPF

7.7.2.2.2.1 Interfață OSPF

Interface: Brlan_1

Main Settings

Cost	10
Hello	10
Poll	20
Retransmit	5
Priority	1
Wait	40
Dead count	3
Dead	30
RX buffer	Normal ▾
TX length	100
Type	Broadcast ▾
Authentication	None ▾

	Nume câmp	Valoare	Explicație
1.	Cost	10	
2.	Hello	10	
3.	Poll	20	
4.	Retransmit	5	
5.	Priority	1	
6.	Wait	40	
7.	Dead count	3	
8.	Dead	30	
9.	RX buffer	Normal	
10.	TX length	100	
11.	Type	Broadcast	
12.	Authentication	None Niciuna	

7.7.2.5 Protocole generale

Fereastra General Protocols vă permite să configurați opțiunile pentru nucleu și pentru dispozitiv, precum și rutele statice.

7.7.2.5.1 Opțiuni pentru nucleu

Kernel Options

Enable	<input checked="" type="checkbox"/>
Learn	<input type="checkbox"/>
Persist	<input type="checkbox"/>
Scan time	20
Import	All
Export	All

	Nume câmp	Valoare	Explicație
1.	Enable	Activare/Dezactivare	Activăți/dezactivați setările
2.	Learn Învățare	Activare/Dezactivare	Activează învățarea rutelor
3.	Persist	Activare/Dezactivare	Stocați rutele. După o repornire, rutele vor fi configurate încă
4.	Scan time	20	Perioada de timp dintre scanări
5.	Import	All	Setați dacă protocolul trebuie să importe rute
6.	Export	All	Setați dacă protocolul trebuie să exporte rute

7.7.2.5.2 Opțiuni pentru dispozitiv

Device Options

Enable	<input checked="" type="checkbox"/>
Scan time	10

	Nume câmp	Valoare	Explicație
1.	Enable	Activare/Dezactivare	Dacă bifăți, protocolul nu va fi configurat
2.	Scan time	10	Perioada de timp dintre scanări

7.7.2.5.3 Rute statice

Static Routes

Prefix	Type	
Prefix	router	Edit Delete

New Static Route

Prefix	Type	
<input type="text"/>	Router ▾	Add

	Nume câmp	Explicație
1.	Prefix	Prefixul protocolului pachetului de intrare sau de ieșire
2.	Type	Tipul protocolului pachetului de intrare sau de ieșire
3.	Add Adăugare	Adăugați o nouă Rută Statică

7.7.2.2.2 Configurarea rutelor statice

Vă puteți configura în detaliu noile rute statice apăsând butonul “Edit” alăturat.

Prefix	Type	
Prefix	router	Edit  Delete

Veți fi redirectionat către fereastra de configurare a rutei statice.

Static Route - Prefix

Route configuration

Disabled

Route instance [static](#) ▾

Route prefix Prefix

Type of route [router](#) ▾

Via

Reject

	Nume câmp	Valoare	Explicație
1.	Disabled	Bifat/Nebifat	Dacă bifăți, protocolul nu va fi configurat
2.	Route instance Instanță rută	Static	
3.	Route prefix Prefix rută	Prefix	
4.	Type of route Tip rută	Router	
5.	Via		
6.	Reject Respingere	Bifat/Nebifat	

7.8 Echilibrarea încărcării

Echilibrarea încărcării permite utilizatorilor să creeze reguli ce împart traficul între diferite interfețe.

Policies

Policy	Members assigned	Ratio	Sort	Actions
balanced	Mobile Wired	3 2	Up/Down	Edit Delete

Add

Rules

Rule	Source address	Source port	Destination address	Destination port	Protocol	Policy assigned	Sort	Actions
default_rule	—	—	0.0.0.0/0	—	all	balanced	Up/Down	Edit Delete

Add

Save

Pentru a configura o regulă, dați clic pe butonul "Edit" din dreptul acesteia.

Policy	Members assigned	Ratio	Sort	Actions
balanced	Mobile Wired	3 2	Up/Down	Edit Delete

Veți fi redirecționat către fereastra de configurare a regulii.

WAN Policy Configuration - balanced

Interface	Ratio	Sort	Actions
Mobile	3	Up/Down	Delete
Wired	2	Up/Down	Delete

Add

Aici puteți defini proporția fiecărei interfețe WAN. În exemplul de mai sus vedem că proporția interfeței mobile este 3, iar proporția interfeței pe cablu este 2. Aceasta înseamnă că 3/5 din întreg traficul vor trece prin interfața mobilă, iar 2/5 prin interfața pe cablu. După ce ați finalizat configurarea regulilor de echilibrare a încărcării, mergeți în secțiunea WAN și activați echilibrarea încărcării pentru interfața dorită.

8 Monitorizarea și administrarea de la distanță

Routerul RUT955 suportă multiple posibilități de monitorizare și administrare. Informații despre router se pot obține prin SMS sau utilizând RMS (Remote Management System). Mai mult, unii parametri de sistem pot fi obținuți utilizând serviciile de publicare MQTT sau MODBUSD. Instrucțiuni privind modul de utilizare a acestora pot fi găsite în capitolele [9.19](#) și [9.20](#) de mai jos. Accentul principal se pune pe parametrii care se modifică în timp, precum intensitatea semnalului, numele operatorului (schimbarea numelui operatorului este des întâlnită în țările în care se utilizează roamingul intern) sau temperatura modulului. Este, totuși, posibilă și citirea valorilor statice, precum adresa MAC, numărul de serie al routerului și multe altele. Accesul la parametrii menționați este implementat în aplicațiile de publicare MODBUSD și MQTT. În afară de obținerea parametrilor, MODBUSD poate fi folosit și pentru setarea unor parametri de sistem; de exemplu, poate fi utilizat pentru a modifica valoarea ieșirii digitale.

Unele aplicații, precum MQTT sau RMS, permit monitorizarea sau administrarea simultană a mai multor routere. Aceasta este o funcționalitate foarte utilă atunci când doriți să modificați aceiași parametri pe mai multe routere simultan. RMS are unele similitudini cu SSH (Secure Shell) și una dintre caracteristicile RMS este de a permite accesul prin SSH la un router de la distanță. Acest manual nu are un capitol separat despre RMS, deoarece interfața RMS este foarte intuitivă și ușor de utilizat. Puteți accesa RMS din browserul Dvs. cu un nume de utilizator furnizat și o parolă la <http://rms.teltonika.lt>.

Prin trimitera de mesaje SMS către router, utilizatorul poate executa diferite comenzi precum repornirea, pornirea sau oprirea conexiunii Wi-Fi și multe altele. La fiecare SMS utilizatorul trebuie să specifice parola de administrator a routerului, pentru autentificare. Lista comenziilor care pot fi executate prin SMS este limitată. Lista completă a comenziilor poate fi găsită accesând Services-> SMS Utilities pe pagina web a routerului. Mai multe informații despre modul de gestionare prin SMS a routerului pot fi găsite mai jos în capitolul [9.8](#).

O altă soluție interesantă de monitorizare a routerului este SNMP (Simple Network Management Protocol). Fără a intra în detaliu, acest protocol este o altă modalitate de monitorizare a parametrilor routerului. Acesta permite utilizatorului să verifice operatorul curent, modelul de modem și alți parametri ai routerului. În comparație cu alte aplicații și servicii, numai SNMP are capacitatea de a informa utilizatorul despre producerea anumitor evenimente (denumite capcane) în sistem. Principalul dezavantaj al acestui protocol este că nu permite utilizatorului să schimbe nimic. Puteți citi mai multe despre SNMP în capitolul [9.9](#).

În afară de serviciile menționate mai sus, există un serviciu care este utilizat numai pentru comunicarea dintre router și un dispozitiv de tip Android (telefoane etc.). Se numește JSON-RPC și permite utilizatorului să seteze sau să citească diverse parametri ai sistemului. JSON-RPC permite utilizatorilor să execute aceleași comenzi ca și prin SSH. Pe scurt, această abordare deschide posibilități largi de comunicare între router și un dispozitiv Android. Totuși, acest manual nu tratează separat JSON-RPC, deoarece acest tip de comunicare nu este în general folosit de utilizatorii finali.

Fiecare abordare are avantajele și dezavantajele sale. În unele situații MQTT funcționează mai bine decât MODBUSD, în timp ce în altele MODBUSD este alegerea mai bună. Cea mai versatilă modalitate de monitorizare și administrare a sistemului este SSH. SSH oferă controlul complet al routerului. Utilizatorul poate să execute comenzi, să scrie shell script-uri și să facă multe alte lucruri. În acest caz, utilizatorul are nevoie doar de o aplicație pentru conectarea la router prin SSH. Cea mai populară aplicație utilizată în sistemele de operare Windows este Putty. Dacă încercați să vă conectați la router dintr-un sistem de operare UNIX, aveți nevoie doar de numele gazdei, numele de utilizator (în acest caz – root) și parolă.

Uneori utilizarea SSH nu este necesară, astfel încât sunt folosite alte servicii/aplicații mai conservatoare. Lista completă a aplicațiilor și serviciilor ce pot fi utilizate pentru administrarea și monitorizarea routerului este prezentată mai jos. Se poate observa că toate aplicațiile, cu excepția MQTT și a SNMP, suportă setarea/citirea unor parametri de sistem.

	Aplicație	Poate citi parametri	Poate seta parametri
1.	MQTT	•	○
2.	MODBUS Daemon	•	•
3.	SSH	•	•
4.	RMS	•	•
5.	SMS	•	•
6.	SNMP	•	○
7.	JSON-RPC	•	•
8.	TR-069	•	•

În concluzie, routerul RUT955 oferă mai multe soluții de gestionare. Fiecare utilizator poate alege ce soluție să folosească. Dacă funcționalitatea necesară nu este acceptată de un anumit serviciu, utilizatorul poate combina mai multe aplicații, de exemplu, să folosească MQTT împreună cu SNMP. În cele din urmă, dacă un utilizator are cerințe speciale, poate scrie shell script-uri și le poate executa prin SSH sau poate folosi JSON-RPC.

9 Servicii

9.1 VRRP

Virtual Router Redundancy Protocol (VRRP) este un protocol de rețea ce oferă alocarea automată a routerelor IP disponibile gazdelor participante. Astfel se mărește disponibilitatea și fiabilitatea căilor de rutare prin selecția automată a gateway-ului implicit într-o subrețea IP.

9.1.1 Setările de configurare a rețelei LAN în VRRP

VRRP Configuration

VRRP LAN Configuration Settings

Enable	<input type="checkbox"/>
IP address	192.168.1.253 <input type="button" value=""/>
Virtual ID	1
Priority	100

	Nume câmp	Valoare în exemplu	Explicație
1.	Enable	Activare/Dezactivare	Activăți sau dezactivați VRRP pentru LAN
2.	IP address	192.168.1.253	Adresă IP virtuală pentru clusterul VRRP al rețelei LAN
3.	Virtual ID Identificator virtual	1	Routerele cu același identificator vor fi grupate în același cluster VRRP, interval [1-255]
4.	Priority	100	Routerul cu cea mai mare valoare a priorității din același cluster VRRP va opera ca master, interval [1-255]

9.1.2 Verificarea conexiunii la internet

Check Internet Connection

Enable	<input type="checkbox"/>
Ping IP address	8.8.4.4
Ping interval	10
Ping timeout (sec)	1
Ping packet size	50
Ping retry count	100

	Nume câmp	Valori posibile	Explicație
1.	Enable	Activare/Dezactivare	Activăți monitorizarea conexiunilor rețelei WAN
2.	Ping IP address	8.8.4.4	Gazda unde vor fi trimise pachetele ICMP
3.	Ping interval	Orice număr întreg	Intervalul de timp, în secunde, dintre două comenzi ping
4.	Ping timeout (sec)	1 – 9999	Timpul cât se așteaptă răspunsul la ping
5.	Ping packet size	0 – 1000	Dimensiunea pachetului ICMP
6.	Ping retry count	1 – 9999	Numărul de încercări de ping eşuate înainte de a se stabili pierderea conexiunii

9.2 TR-069

TR-069 este un standard dezvoltat pentru configurarea și gestionarea automată a dispozitivelor aflate la distanță prin servere de configurare automată (ACS).

9.2.1 Configurarea parametrilor TR-069

TR-069 Client Configuration

TR-069 Parameters Configuration

Enable	<input type="checkbox"/>
Periodic enable	<input checked="" type="checkbox"/>
Accept server request	<input type="checkbox"/>
Sending interval	100
Username	easycwmp
Password	***** 
URL	http://192.168.1.110:8080/

	Nume câmp	Valori posibile	Explicație
1.	Enable	Activat/Dezactivat	Activați clientul TR-069
2.	Periodic enable Activare periodică	Activat/Dezactivat	Activați transmiterea periodică de date către server
3.	Accept server request Acceptare cerere server	Activat/Dezactivat	Bifați pentru a accepta cererile de conectare de la server
4.	Sending interval Interval transmitere	60-9999999	Intervalul la care se transmit periodic date
5.	User name	admin	Numele de utilizator folosit pentru autentificare pe un server TR-069
6.	Password	*****	Parola folosită pentru autentificare pe un server TR-069
7.	URL	http://192.168.1.110:8080/	Adresa URL a serverului TR-069

9.3 Filtrul web

9.3.1 Blocarea site-urilor

Aveți posibilitatea de a bloca site-urile web nedorite.

Site Blocking Settings

Site Blocking

Enable	Hostname	
<input checked="" type="checkbox"/>	www.facebook.com	Delete

[Add](#)

	Nume câmp	Valori posibile	Explicație
1.	Enable	Activare/Dezactivare	Activăți blocarea site-urilor web pe baza numelui gazdei
2.	Mode	Whitelist Listă albă /Blacklist Listă neagră	Listă albă: permite fiecare site din listă și blochează orice altceva. Listă neagră: blochează fiecare site din listă și permite orice altceva
3.	Enable	Activare/Dezactivare	Activăți blocarea/permisiunea pentru intrarea respectivă
4.	Host name	www.facebook.com	Blocați/permiteți site-urile cu acest nume de gazdă

9.3.2 Blocarea conținutului prin servere proxy

Blocarea conținutului printr-un server proxy funcționează asemănător cu blocarea site-urilor, cu excepția faptului că blocarea conținutului vă permite să filtrați conținutul cu mai multă versatilitate.

Proxy Based URL Content Blocker Configuration

Proxy Based URL Content Blocker

Enable	URL content	
<input checked="" type="checkbox"/>	*.facebook.*	Delete

[Add](#)

	Nume câmp	Valoare în exemplu	Explicație
1.	Enable	Activare/Dezactivare	Activăți blocarea conținutului URL-urilor prin intermediul unui server proxy. Funcționează numai cu protocolul HTTP
2.	Mode	Whitelist/Blacklist	Listă albă: permite fiecare parte a unui URL din listă și blochează orice altceva. Listă neagră: blochează fiecare parte a unui URL din listă și permite orice altceva
3.	URL content Conținut URL	*.facebook.*	Blocați/permiteți orice URL care conține acest sir. Asteriscul ține loc de orice, de ex. www.facebook.* va bloca www.facebook.net, www.facebook.org etc.

9.4 MQTT

9.4.1 Brokerul MQTT

MQTT (Message Queuing Telemetry Transport) este un protocol de mesagerie de tip publicare-abonare utilizat peste protocolul TCP/IP. Este destinat trimiterii de mesaje scurte de la un client (publisher) către altul (abonat) prin intermediul brokerilor, care sunt responsabili pentru livrarea mesajelor la punctul final. Routerele RUT955 suportă această funcționalitate prin intermediul unui broker open-source Mosquitto. Mesajele sunt trimise astfel: un client (abonat) se abonează la unul sau mai multe subiecte (topics); un publisher postează un mesaj pe subiectul/subiectele respectiv/e. Apoi brokerul verifică cine este abonat la subiectul/subiectele respectiv/e și transmite datele de la publisher la abonat.

Puteți activa brokerul MQTT bifând căsuța **Enable**. Brokerul va “asculta” după conexiuni pe **portul local** specificat. Pentru acceptarea conexiunilor din rețeaua WAN, trebuie să bifăți și **Enable Remote Access** |Activare acces la distanță|.

The screenshot shows a top navigation bar with two tabs: "Broker" (which is selected and highlighted in blue) and "Publisher". Below this is a section titled "MQTT Broker" containing configuration options:

- "Enable" checkbox (unchecked)
- "Local Port" input field with value "0"
- "Enable Remote Access" checkbox (unchecked)

MQTT Broker

Enable

Local Port

Enable Remote Access

	Nume câmp	Valori posibile	Explicație
1.	Enable	Activat/Dezactivat	Activați brokerul MQTT
2.	Local port Port local	0 – 65535	Specificați portul local pe care va asculta brokerul MQTT
3.	Enable remote access	Activat/Dezactivat	Dacă este activat, brokerul Dvs. MQTT va fi accesibil de către clienți de la distanță (WAN)

9.4.1.1 Securitatea brokerului MQTT

Pentru a folosi autentificarea TLS/SSL pentru comunicarea client-broker-client, trebuie să bifăți **Use TLS/SSL** |Utilizare TLS/SSL|. Ulterior, utilizatorului îi vor fi prezentate setări suplimentare, ca în figura de mai jos.

The screenshot shows a top navigation bar with three tabs: "Security" (selected), "Bridge", and "Miscellaneous". Below this is a section titled "Security" containing configuration options:

- "Use TLS/SSL" checkbox ()
- "CA File" button ("Choose File") with placeholder "No file chosen"
- "CERT File" button ("Choose File") with placeholder "No file chosen"
- "Key File" button ("Choose File") with placeholder "No file chosen"
- "TLS version" dropdown menu with option "Support all"

Use TLS/SSL

CA File No file chosen

CERT File No file chosen

Key File No file chosen

TLS version

	Nume câmp	Valoare în exemplu	Explicație
1.	Use TLS/SSL	Bifat/Nebifat	Activați autentificarea TLS/SSL pentru broker
2.	CA File	-	Încărcați un fișier conținând certificatul autoritatii de certificare
3.	CERT File	-	Încărcați un fișier conținând certificatul cleintului
4.	Key File	-	Încărcați un fișier conținând cheia
5.	TLS version Versiune TLS	tlsv1/tls1.1/tls1.2/ Support all	Selectați ce versiune a TLS va folosi brokerul

9.4.1.2 MQTT Bridge

Brokerul MQTT suportă și o funcționalitate denumită **Bridge**. O punte MQTT este folosită pentru comunicarea între doi brokeri MQTT. Fereastra parametrilor pentru această funcție este prezentată mai jos. Unii parametri sunt obligatorii, fiind necesari pentru crearea unei conexiuni: **Connection Name**, **Remote Address** și **Remote Port**. Pentru mai multe informații despre parametrii funcției bridge MQTT puteți consulta pagina oficială a manualului mosquitto.conf.

Enable

Connection Name

Remote Address

Remote Port

Use Remote TLS/SSL

Use Remote Bridge Login

Topic

Try Private

Clean Session

	Nume câmp	Valori posibile	Explicație
1.	Enable	Bifat/Nebifat	Activăți funcția Bridge MQTT
2.	Connection Name	Orice nume	Numele conexiunii bridge. Deși este folosit pentru facilitarea gestionării, acest câmp este obligatoriu
3.	Remote Address	Orice adresă IP la distanță	Adresa la distanță a brokerului
4.	Remote Port Port la distanță	0 – 65535	Selectați pe ce port va asculta brokerul după conexiuni
5.	Use Remote TLS/SSL	Bifat/Nebifat	Selectați pentru a folosi certificatele TSL/SSL ale brokerului de la distanță
6.	Use Remote Bridge Login Utilizare logare la distanță	Bifat/Nebifat	Selectați pentru a utiliza datele de logare la distanță. Dacă bifați, vi se va cere să introduceți identificatorul unui client la distanță, numele de utilizator și parola
7.	Topic Subiect	Numele oricărui subiect existent	Introduceți numele subiectelor la care se va abona brokerul Dvs.
8.	Try Private	Bifat/Nebifat	Bifați dacă brokerul la distanță este o altă instanță a unui daemon
9.	Clean Session	Bifat/Nebifat	Bifați pentru a elimina starea sesiunii după conectare ori deconectare

9.4.1.3 Diverse

Ultima secțiune a parametrilor brokerului MQTT este denumită **Miscellaneous | Diverse** și conține parametrii care nu privesc securitatea ori puntea.

The screenshot shows the Mosquitto configuration interface with the 'Miscellaneous' tab selected. The interface includes the following fields:

- ACL File:** A file selection field with a 'Choose File' button and the message 'No file chosen'.
- Password File:** A file selection field with a 'Choose File' button and the message 'No file chosen'.
- Persistence:** A checkbox labeled 'Persistence'.
- Allow Anonymous:** A checkbox labeled 'Allow Anonymous' with a checked status.

	Nume câmp	Valoare în exemplu	Explicație
1.	ACL File Fișier ACL	-	Conținutul acestui fișier este folosit pentru a controla accesul clientului la subiectele brokerului
2.	Password File Fișier parolă *	-	Stochează numele de utilizatori și parolele asociate, folosite pentru autentificare
3.	Persistence Persistență *	Bifat/Nebifat	Dacă bifăți, datele privind conexiunea, abonarea și mesajele vor fi scrise pe disc. În caz contrar, datele sunt stocate numai în memoria routerului
4.	Allow Anonymous	Bifat/Nebifat	Dacă bifăți, brokerul permite accesul anonim

* Puteți afla mai multe despre fișierele ACL și parolă în manualul de configurare Mosquitto.

9.4.2 Publisher-ul MQTT

Un publisher MQTT este un client care trimite mesaje brokerului, care apoi le redirecționează către abonat.

Broker	Publisher
--------	-----------

MQTT Publisher

Enable

Hostname

Port

Username

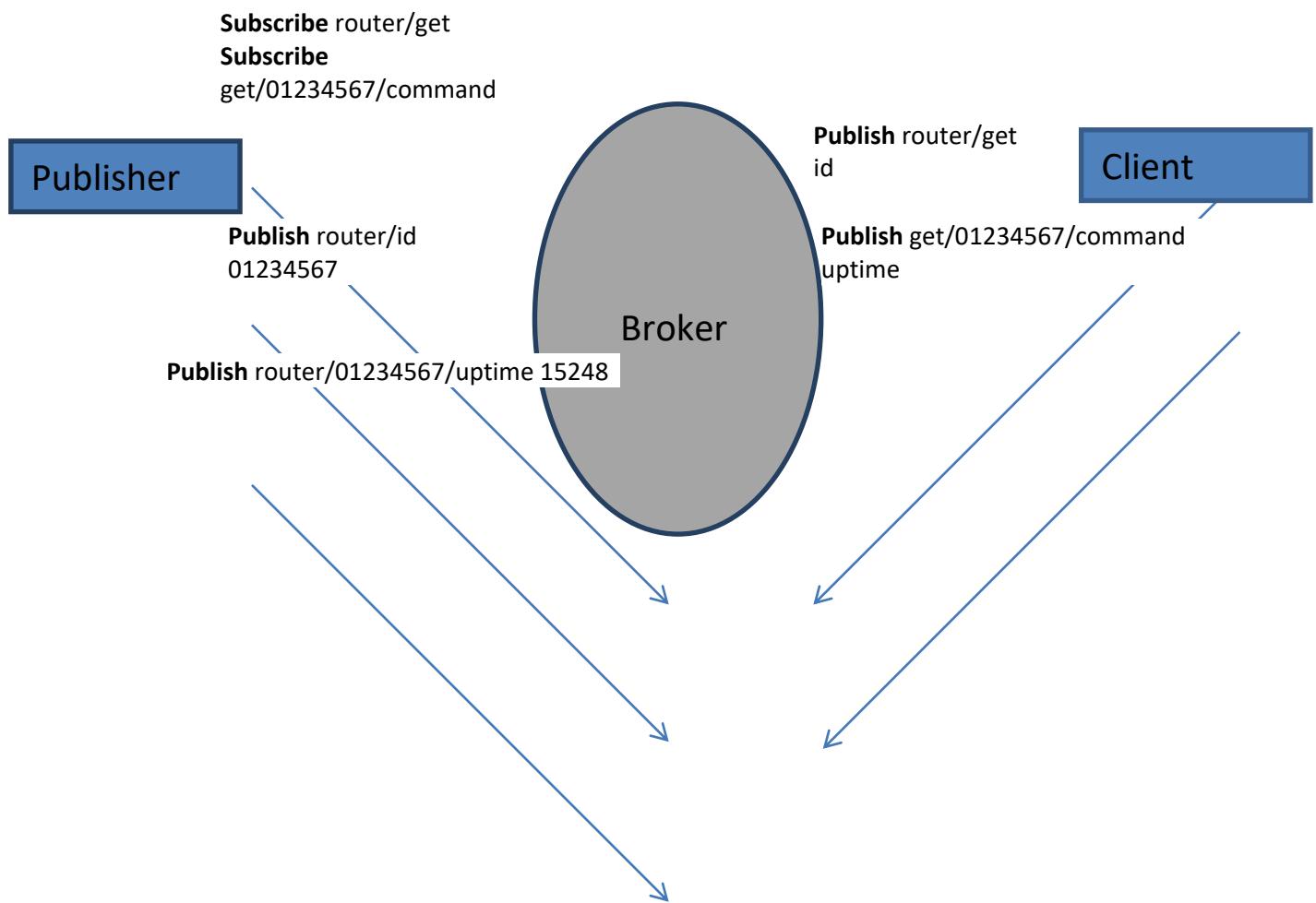
Password 

	Nume câmp	Valoare în exemplu	Explicație
1.	Enable	Bifat/Nebifat	Face ca routerul să opereze ca un publisher MQTT. Ceilalți parametri ai MQTT vor apărea numai dacă bifați această casuță
2.	Hostname	Adresa IP sau numele de gazdă	Adresa IP sau numele de gazdă ale brokerului
3.	Port	0 – 65535	Specificați portul folosit pentru conectarea la broker
4.	Username	Numele Dvs. de utilizator	Numele de utilizator folosit pentru autentificare la conectarea la broker
5.	Password	Parola Dvs.	Parola folosită pentru autentificare la conectarea la broker

Publisher-ul MQTT poate “publica” parametri de sistem către broker. Lista tuturor parametrilor de sistem ce pot fi publicați este dată în tabelul de mai jos.

Numele parametrului	Descrierea parametrului
temperature temperatură	Temperatura modulului în zecimi de grade Celsius
operator	Numele operatorului curent
signal semnal	Intensitatea semnalului în dBm
network rețea	Tipul rețelei curente (2G, 3G, 4G)
connection conexiune	Disponibilitatea conexiunii de date
wan	Adresa IP a rețelei WAN
uptime Durată funcționare	Durata de funcționare a sistemului, în secunde
name Nume	Numele routerului
digital1	Valoarea intrării digitale nr.1
digital2	Valoarea intrării digitale nr.2
analog	Valoarea intrării analogice

Pentru ca sistemul să funcționeze, brokerul MQTT trebuie configurat în prealabil. Puteti folosi brokerul instalat în router sau un alt broker independent. Mai jos este prezentată o schemă în care clientul încearcă să se aboneze la informații despre perioada de funcționare a routerului. Pentru aceasta, între client și publisher sunt transmise mai multe comenzi.



În general publisher-ul operează astfel: publisher-ul se conectează la broker și se abonează la subiectele **router/get** și **get/<SERIAL>/command**. <SERIAL> denotă numărul de serie al routerului clientului. Clientul trimite apoi un identificator de mesaj pe subiectul **router/get**. Mesajul următor este primit de publisher, întrucât este abonat la subiectul respectiv. Apoi publisher-ul trimite un răspuns cu numărul său de serie pe subiectul **router/id**. Acum clientul știe că există un publisher cu un număr de serie. Înseamnă că clientul poate trimite brokerului un mesaj cu numele parametrului din listă pe subiectul **get/<SERIAL>/command**. Mesajul va fi primit numai de către abonatul care are același număr de serie ca cel menționat în subiect. Acum publisher-ul poate trimite înapoi un răspuns cu subiectul **router/<SERIAL>/parameter_name** și un mesaj cu valoarea parametrului cerut. Țineți cont că, în conformitate cu protocolul MQTT, numele de subiecte disting între literele mari și mici, de ex. subiectul router nu este identic cu subiectul RoUtEr.

9.5 NTP

Cu ajutorul NTP (Network Time Protocol) vă puteți configura și sincroniza timpul routerului Dvs.

Time Synchronisation

General

Current system time 2017-08-30 14:05:23

Sync with browser

Time zone Europe/Vilnius

Enable NTP

Update interval (in seconds) 3660

Save time to flash

Count of time synchronizations

Clock Adjustment

Offset frequency 0

Save

Nume câmp	Descriere
1. Current System time Timp curent sistem	Timpul local al routerului
2. Time zone Fus orar	Fusul orar al țării în care se află routerul
3. Enable NTP Activare NTP	Activează sincronizarea cu serverul de timp prin NTP
4. Update interval Interval actualizare	Cât de des actualizează routerul timpul
5. Save time to flash Salvare timp în flash	Salvează ultimul timp sincronizat în memoria flash
6. Count of time synchronizations Număr sincronizări timp	Numărul total de sincronizări efectuate de router. Notă: dacă lăsați necompletat numărul va fi infinit
7. Offset frequency Decalaj frecvență	Ajustează miciile abateri ale ceasului pentru o funcționare mai precisă

Țineți cont că în secțiunea **Time Servers** |Servere de timp| trebuie să existe cel puțin unul; în caz contrar protocolul NTP nu vă va fi util.

9.6 RS-232/RS-485

Funcțiile RS-232 și RS-485 sunt proiectate să folosească interfețele seriale disponibile ale routerului. Interfețele seriale permit dispozitivelor de generație mai veche să obțină acces în rețelele IP.

9.6.1 RS-232

The screenshot shows the RS-232 configuration page. At the top, there are tabs for 'RS232' (selected) and 'RS485'. Below the tabs, the title 'RS232 Configuration' is displayed. Under the title, the 'RS232 Serial Configuration' section contains the following fields:

- Enabled: A checkbox that is checked.
- Baud rate: A dropdown menu set to 115200.
- Data bits: A dropdown menu set to 8.
- Parity: A dropdown menu set to None.
- Stop bits: A dropdown menu set to 1.
- Flow control: A dropdown menu set to None.
- Serial type: A dropdown menu set to Console.

Below this, the 'Interface' configuration section shows a table with one row:

Interface	Allow IP
LAN	192.168.1.124

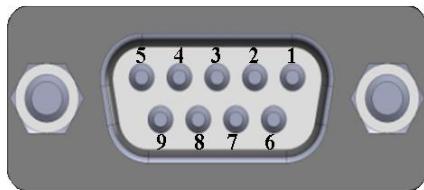
At the bottom of the interface configuration section, there are buttons for 'Add' and a dropdown menu set to 'LAN'.

At the very bottom of the page, there is a table with 9 rows, each containing a number from 1 to 9, a field name, possible values, and a detailed explanation:

	Nume câmp	Valori posibile	Explicație
1.	Enabled	Bifat/Nebifat	Bifați pentru a activa funcția port serial
2.	Baud rate	300/1200/2400/4800/9600/19200/38400/57600/115200	Selectați viteza comunicației interfeței seriale
3.	Data bits Biți date	5 – 8	Specifică câți biți vor fi folosiți pentru fiecare caracter
4.	Parity Paritate	None Niciuna /Odd Impar / Even Par	Selectați setarea bitului de paritate folosită pentru detectarea erorilor în timpul transferului de date
5.	Stop bits Biți stop	1 / 2	Specifică câți biți de stop vor fi folosiți pentru detecția sfărșitului caracterului
6.	Flow control Control flux	None/RTS– CTS/Xon-Xoff	Specifică ce tip de caractere vor fi folosite pentru controlul fluxului
7.	Serial type	Console/Over IP/Modem/Modbus Gateway/NTRIP Client	Specifică funcția interfeței seriale
8.	Interface	LAN/ WAN/VPN/L2TP/PPTP/GRE/HOTSPOT	Interfața folosită pentru conectare
9.	Allow IP Permisii IP	Orice adresă IP	Permiteți adresei IP să se conecteze la server

9.6.1.1 Funcțiile pinilor conectorului RS-232

Conectorul RS-232 al acestui dispozitiv este de tip DCE (Data Communication Equipment) mamă.



Pin	Nume*	Descriere*	Direcția pe acest dispozitiv
1	DCD	Detectare purtătoare semnal de date	Ieșire
2	RXD	Recepție de date	Ieșire
3	TXD	Transmisie de date	Intrare
4	DTR	Terminal de date pregătit	Intrare
5	GND	Masă	-
6	DSR	Echipament receptor pregătit	Ieșire
7	RTS	Pregătit pentru transmisie	Intrare
8	CTS	Gata de emisie	Ieșire
9	RI	Indicator apel	Ieșire (conectat permanent la +5 V printr-un rezistor de 4,7k)

*Numele și descrierile ce indică direcția semnalului (TXD, RXD, RTS, CTS, DTR și DSR) sunt din perspectiva dispozitivului DTE.

9.6.1.2 Cabluri

Routerul RUT955 are un conector DCE mamă. Pentru a conecta la router un dispozitiv DTE standard, folosiți un cablu direct RS-232 mamă/tată:



Pentru a conecta un alt dispozitiv DCE la routerul RUT955, trebuie folosit un cablu nul-modem (încrucisat) mamă/mamă:



Lungimea maximă a cablului este de 15 m sau lungimea egală cu o capacitate electrică de 2500 pF (pentru o rată de baud de 19200). Utilizarea de cabluri cu capacitate electrică mai redusă poate mări distanța. Reducerea vitezei comunicațiilor poate, de asemenea, mări lungimea maximă a cablului.

9.6.2 RS-485

RS-485 este un alt standard pentru transmisia serială de date, folosit pentru distanțe mari ori în medii zgomotoase.

RS232

RS485

RS485 Configuration

RS485 Serial Configuration

Enabled	<input type="checkbox"/>
Baud rate	115200
Parity	None
Flow control	None
Serial type	Console
Interface	Allow IP
LAN	192.168.1.124
<input type="button" value="Delete"/>	
Interface name:	Add
LAN	

	Nume câmp	Valori posibile	Explicație
1.	Enabled	Activare/Dezactivare	Bifați pentru a activa funcția port serial
2.	Baud rate	300/1200/2400/4800/9600/ 19200/38400/57600/115200	Selectați viteza comunicației interfeței seriale
3.	Parity	None / Odd / Even	Setarea bitului de paritate este folosită pentru detectarea erorilor în timpul transferului de date
4.	Flow control	None/RTS-CTS/Xon-Xoff	Specifică ce tip de caractere vor fi folosite pentru controlul fluxului
5.	Serial type	Console/Over IP/Modem/ Modbus Gateway/NTRIP Client	Specifică funcția interfeței seriale
6.	Interface	LAN/ WAN/ VPN/L2TP/PPTP/GRE/HOTSPOT	Interfața folosită pentru conectare
7.	Allow IP	192.168.1.102	Permiteți adresei IP să se conecteze la server

9.6.2.1 Viteza maximă de transfer al datelor raportată la lungimea liniei de transmisie

Standardul RS-485 poate fi folosit pentru rețele cu o lungime de până la 1200 m, dar viteza de date maximă scade odată cu creșterea lungimii liniei de transmisie. Un dispozitiv care funcționează la viteza maximă de transfer al datelor (10 Mbps) este limitat la o lungime a liniei de transmisie de cca 12 m, în timp ce viteza de 100 kbps poate acoperi o distanță de până la 1200 m. O relație aproximativă între lungimea maximă a liniei de transmisie și viteza de transfer al datelor poate fi calculată cu următoarea formulă:

$$L_{\max(m)} = \frac{10^8}{DR \left(\frac{\text{bit}}{\text{s}} \right)}$$

unde L_{\max} este lungimea maximă a liniei de transmisie în metri iar DR este viteza maximă de transfer al datelor în biți pe secundă.

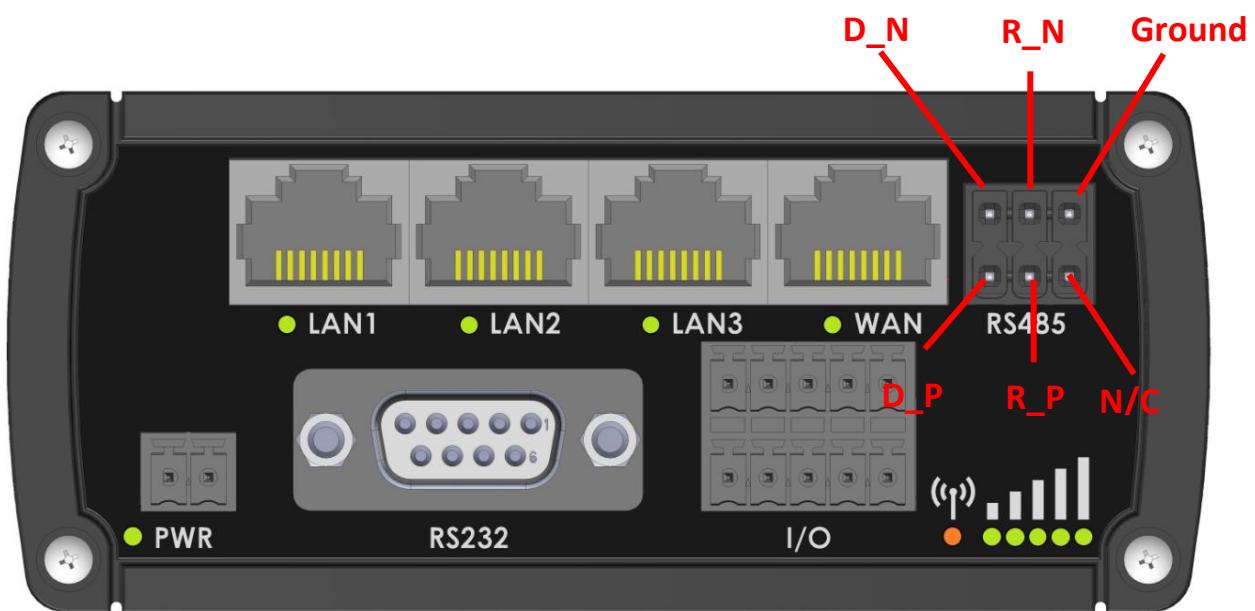
Perechea de fire torsadate este tipul de cablu preferat pentru rețelele RS-485. Cablurile cu pereche de fire torsadate captează zgomotul și alte tensiuni induse electromagnetic ca semnale de mod comun, care sunt respinse de receptoarele diferențiale.

9.6.2.2 Tipul de cablu

Parametrii recomandați pentru cablu:

Parametru	Valoare
Tip de cablu	22-24 AWG, cu 2 perechi (folosit pentru rețelele duplex) sau 1 pereche (folosit pentru rețelele semiduplex). Este necesar un fir suplimentar pentru împământare
Impedanță caracteristică a cablului	120 Ω @ 1 MHz
Capacitatea electrică (conductor la conductor)	36 pF/m
Viteză de propagare	78% (1,3 ns/ft)

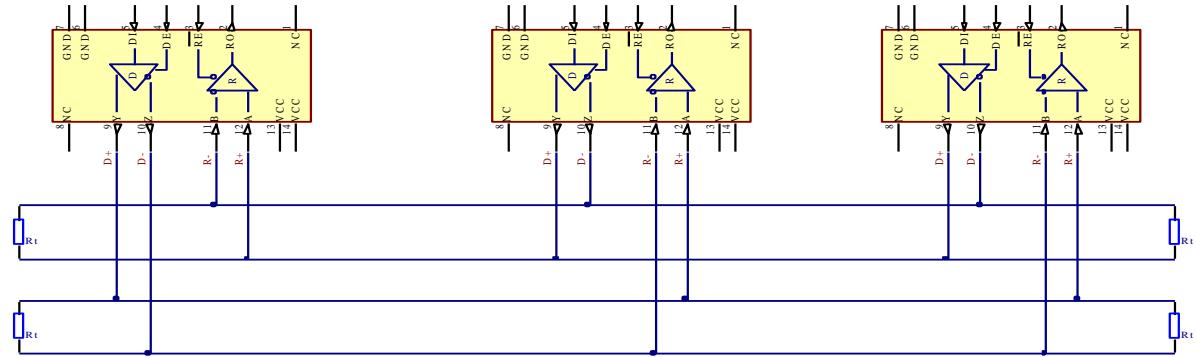
9.6.2.3 Funcțiile conectorilor RS-485



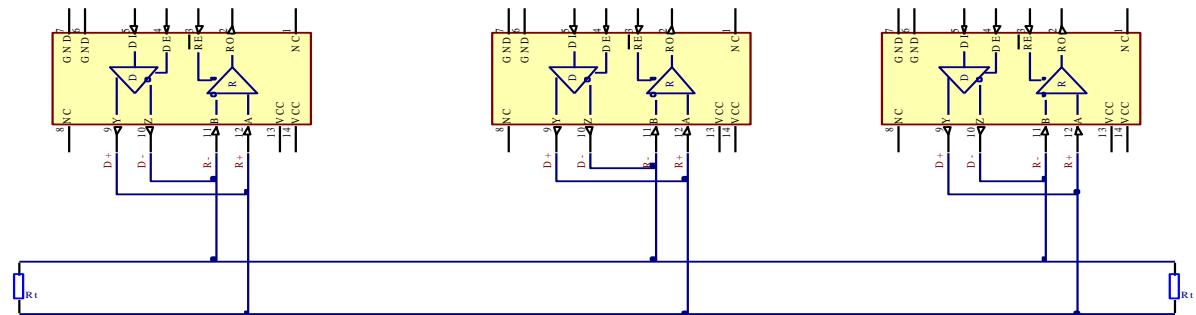
Nume	Descriere	Tip
D_P	Semnalul pozitiv al driver-ului	Ieșire diferențială
D_N	Semnalul negativ al driver-ului	Ieșire diferențială
R_P	Semnalul pozitiv al receptorului	Intrare diferențială
R_N	Semnalul negativ al receptorului	Intrare diferențială
Ground	Împământarea dispozitivului	Ieșire diferențială

9.6.2.4 Rețele pe 2 fire și rețele pe 4 fire

Mai jos este un exemplu de conexiune electrică într-o rețea pe 4 fire. În exemplu sunt prezentate 3 dispozitive, dintre care unul este "master" iar celelalte două sunt "sclavi". La fiecare capăt al cablului sunt amplasate rezistoare terminale. Rețelele pe 4 fire constau într-un „master” cu transmisițorul conectat la fiecare dintre receptoarele „slave” pe o pereche de fire torsadate. Transmisițioarele „slave” sunt toate conectate la receptorul „master” pe o a doua pereche de fire torsadate.



Exemplu de conexiune electrică într-o rețea pe 2 fire: pentru a permite o configurație RS-485 pe 2 fire pe un router Teltonika, trebuie să conectați D_P la R_P și D_N la R_N la priza RS-485 a dispozitivului. La fiecare capăt al cablului sunt amplasate rezistoare terminale.



9.6.2.5 Rezistorii terminatoare

Când să folosiți (amplasați jumperul)

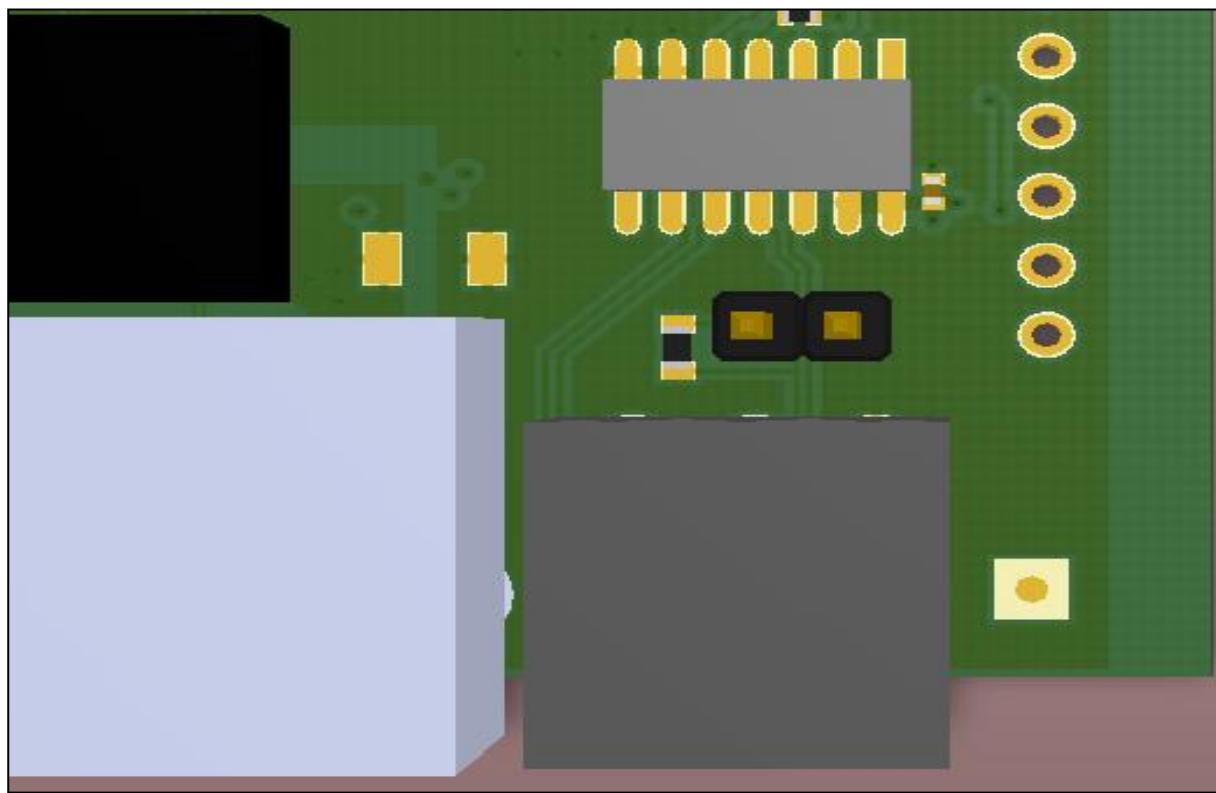
Rezistorii terminatoare, cu rezistență egală cu impedanța caracteristică a cablului, trebuie conectați la fiecare capăt al cablului pentru a reduce reflexia și oscilația semnalelor când cablul este relativ lung. Timpul de creștere al driverului RS-485 al routerului RUT955 este de cca 5 ns, astfel că lungimea maximă a cablului fără terminatoare este de cca 12 cm. Întrucât cablurile liniei de transmisie vor fi întotdeauna mai lungi de 12 cm, terminatoarele vor fi obligatorii întotdeauna când routerul RUT955 se află la capătul cablului.

Când să nu folosiți (îndepărtați jumperul)

Dacă rețeaua Dvs. de tip RS-485 constă în mai mult de două dispozitive iar routerul RUT955 se află nu la capătul liniei ci, de ex., la mijloc, rezistorul terminator trebuie dezactivat. În acest caz, amplasați terminatorul la alte dispozitive care sunt situate la capetele liniei.

Cum să activați terminatoarele

Un rezistor terminator de $120\ \Omega$ este inclus în circuitul imprimat al routerului RUT955 și poate fi activat prin scurtcircuitarea contactelor (ca în figura de mai jos), prin amplasarea unui jumper de 2,54 mm:



9.6.2.6 Numărul de dispozitive într-o rețea RS-485

Un driver RS-485 al routerului RUT955 poate acționa maxim 32 de receptoare, cu condiția ca impedanța de intrare a receptorului să fie $12\ k\Omega$. Dacă impedanța receptorului este mai mare, numărul maxim de receptoare din rețea crește. Pot fi conectate împreună tipuri de receptoare în orice combinație, cu condiția ca impedanța lor paralelă să nu depășească $R_{Load} > 375\ \Omega$.

9.6.3 Modurile diferitelor tipuri de interfețe seriale RS-232 și RS-485

9.6.3.1 Consolă

În acest mod interfața serială este configurață ca o consolă Linux a dispozitivului. Poate fi folosită pentru depanare, pentru citirea stării dispozitivului sau pentru controlul acestuia.

9.6.3.2 Over IP

În acest mod routerul asigură o conexiune la o rețea TPC/IP pentru dispozitivele conectate prin interfețe seriale.

Mod: Server

Serial type: Over IP

Protocol: TCP

Mode: Server

No leading zeros:

TCP port: _____

Timeout (s): _____

	Nume câmp	Valori posibile	Explicație
1.	Protocol	TCP	Protocolul folosit pentru transmisia de date
2.	Mode	Server / Client / Bidirect	Server – așteaptă conexiunea de intrare Client – inițiază conexiunea Bidirect – acționează în mod implicit ca un client, dar în același timp așteaptă conexiuni de intrare
3.	No leading zeros Fără zerouri inițiale	Bifat/Nebifat	Bifați pentru a sări zerourile inițiale la numerele hexazecimale
3.	TCP port Port TCP	0 – 65535	Numărul portului folosit pentru așteptarea conexiunilor de intrare
4.	Timeout (s)	Orice număr întreg	Deconectează clientul după perioada de inactivitate specificată

Mod: Client

Serial type: Over IP

Protocol: TCP

Mode: Client

No leading zeros:

Server Address: _____

TCP port: _____

Reconnect interval (s): _____

	Nume câmp	Valori posibile	Explicație
1.	Server Address	Nume de gazdă sau adresă IP	Adresa serverului la care va trebui să se conecteze clientul
2.	TCP port	0 – 65535	Numărul portului serverului de la distanță
3.	Reconnect intervals (s) Interval/e reconectare	Orice număr întreg	Indică perioada de timp între încercările de reconectare

Mod: Bidirect

Modul bidirecțional permite comunicarea bidirecțională prin interfața serială. În starea implicită aplicația acționează ca un client, dar în același timp așteaptă orice conexiuni de intrare pe portul dedicat. Când există o conexiune de intrare, aplicația renunță la conexiunea curentă la serverul de la distanță și acționează ca un server în noua conexiune. Se declanșează astfel o schimbare a ieșirii configurate ce poate fi folosită pentru a informa dispozitivele auxiliare despre schimbările de stare ale conexiunii. La terminarea conexiunii cu clientul, aplicația revine în modul său implicit și continuă să acționeze ca un client al serverului de la distanță.

Mode: Bidirect

No leading zeros:

Client settings:

- Server Address:
- TCP port:
- Reconnect interval (s):

Server settings:

- TCP port:
- Timeout (s):

Output: OC Output

Output state: 0

	Nume câmp	Valori posibile	Explicație
1.	Server Address	Nume de gazdă sau adresă IP	Adresa serverului la care va trebui să se conecteze clientul
2.	TCP port	0 – 65535	Numărul portului serverului de la distanță
3.	Reconnect intervals (s)	Orice număr întreg	Indică perioada de timp între încercările de reconectare
4.	TCP port	0 – 65535	Numărul portului folosit pentru așteptarea conexiunilor de intrare
5.	Timeout (s)	Orice număr întreg	Deconectează clientul după perioada de inactivitate specificată
6.	Output	OC Output ieșire cu colector în gol / Relay Output ieșire releu	Ieșirea ce indică faptul că aplicația a trecut din starea de client (implicită) în starea de server
7.	Output state Stare ieșire	0 ori 1	Valoarea stării ieșirii după ce aplicația revine în modul server

9.6.3.3 Modem

În acest mod, routerul imită un modem de dial-up. Conexiunile la rețelele TCP/IP pot fi stabilite prin comenzi AT. Conexiunea poate fi inițiată de dispozitivul conectat prin interfața serială cu o comandă ATD: ATD <gazdă>:<port>. Dacă au fost efectuate setări de conectare directă, conexiunea la server este întotdeauna activă. În modul date se poate intra prin emiterea comenzi ATD. Conexiunile de intrare sunt indicate prin trimiterea unui RING către interfața serială.

Serial type

Direct connect

TCP port

	Nume câmp	Valori posibile	Explicație
1.	Direct connect Conectare directă	Nume gazdă/adresă IP:port	Mențineți o conexiune constantă la gazda specificată. Lăsați necompletat pentru a folosi o comandă ATD pentru inițierea conexiunii
2.	TCP port	0 – 65535	Numărul portului folosit pentru așteptarea conexiunilor de intrare. Lăsați necompletat pentru a dezactiva conexiunile de intrare

Acesta este setul de comenzi AT folosit în modul **Modem** al interfețelor seriale:

Comandă	Descriere	Folosită pentru
A	Răspunde la un apel de intrare	Pentru a răspunde unei conexiuni de intrare: ATA
D	Formează un număr	Pentru a iniția conexiunea de date: ATD <gazdă>:<port> Pentru a intra în modul date cu setările Direct connect : ATD
E	Ecou local	Pornirea ecoului local: ATE1 ; Oprirea ecoului local: ATE0
H	Încheie apelul curent	Pentru a încheia conexiunea de date: ATH
O	Întoarcere în modul date	Pentru întoarcerea în modul date din modul comandă: ATO
Z	Resetare la configurația implicită	Pentru a reseta modemul la configurația implicită: ATZ

9.6.3.4 Gateway Modbus

Acest mod permite redirecționarea datelor TCP recepționate pe un port specificat către unitatea RTU specificată de identificatorul dispozitivului sclav. Identificatorul dispozitivului sclav poate fi specificat de utilizator sau poate fi obținut direct din antetul Modbus.

Serial type

Listening IP

Port

Slave ID configuration type

Slave ID

	Nume câmp	Valori posibile	Explicație
1.	Listening IP IP ascultat	Orice adresă IP	Adresa IP la care gateway-ul Modbus va aștepta conexiuni de intrare
2.	Port	0 – 65535	Numărul portului folosit pentru așteptarea conexiunilor de intrare
3.	Slave ID configuration type Tip configurare ID dispozitiv sclav	User defined / Obtained from TCP	Există două opțiuni disponibile pentru acest parametru: User defined – Definit de utilizator – redirecționează toate datele către identificatorul dispozitivului sclav specificat Obtain from TCP – Obținut din TCP – redirecționează datele către identificatorii dispozitivelor slave din Modbus TCP
4.	Slave ID / Permitted slave IDs	Orice număr întreg / Oricare câțiva întregi sau intervale de numere	Numele și valorile posibile ale acestui câmp se schimbă în funcție de tipul de configurare a identificatorului dispozitivului sclav: Slave ID – identificatorul dispozitivului sclav conectat la router Permitted slave IDs – ID-uri dispozitive slave permise – permite specificarea listei ID-urilor permise ale dispozitivelor slave pentru redirecționarea datelor Modbus TCP. Valorile individuale pot fi separate prin virgule (','), intervalul prin liniuțe ('-'), de ex.: 1, 2, 4-6. ID-urile dispozitivelor slave nelistate aici sunt ignorate

9.7 VPN

9.7.1 OpenVPN

VPN (Virtual Private Network) este o metodă de transfer securizat de date prin rețele publice nesigure. Această secțiune explică configurarea OpenVPN, care este o implementare de VPN suportată de routerele RUT.

Lista din fereastra de configurare OpenVPN este în mod implicit vidă, astfel încât trebuie să vă definiți propria configurație pentru a stabili orice tip de conexiune OpenVPN. Configurațiile OpenVPN pot avea unul din aceste două **roluri**: client și server. Vom începe cu un client OpenVPN. Pentru a-l crea, introduceți numele dorit al instanței în câmpul **“New configuration name”** |Numele noii configurații|, selectați rolul instanței din lista autoderulantă **“Role”** și apăsați butonul **“Add New”** |Adăugare instanță nouă|.

Tunnel name	TUN/TAP	Protocol	Port	Enable
<i>There are no openVPN configurations yet</i>				
Role:	Client	New configuration name:	demo	Add New
Save				

Tunnel name	TUN/TAP	Protocol	Port	Enable
client_demo	tun_c_demo	UDP	1194	<input type="checkbox"/>
<input style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px 10px; cursor: pointer; border-radius: 5px;" type="button" value="Edit"/> <input style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px 10px; cursor: pointer; border-radius: 5px;" type="button" value="Delete"/>				
Role:	Client	New configuration name:		
Add New				

După ce ași adăugat o instanță OpenVPN nouă, nu este nevoie să apăsați butonul **“Save”** |Salvare| întrucât butonul **“Add new”** creează, dar și salvează noua instanță. În mod implicit instanța va fi dezactivată și neconfigurată. Pentru a stabili o conexiune OpenVPN trebuie să vă activați instanța, să introduceți o adresă pentru serverul OpenVPN, să alegeți o metodă de autentificare și să parurgeți alți câțiva pași, toate în fereastra **Settings** |Setări|, ce poate fi accesată apăsând butonul **“Edit”** din dreptul instanței OpenVPN (după cum se arată în figura de mai sus).

9.7.1.1 Clientul OpenVPN

OpenVPN Instance: Client_demo

Main Settings

Enable	<input checked="" type="checkbox"/>
TUN/TAP	TUN (tunnel) <input type="button" value="▼"/>
Protocol	UDP <input type="button" value="▼"/>
Port	1194
LZO	<input checked="" type="checkbox"/>
Encryption	BF-CBC 128 (default) <input type="button" value="▼"/>
Authentication	TLS/Password <input type="button" value="▼"/>
TLS cipher	All <input type="button" value="▼"/>
Remote host/IP address	84.15.198.92
Resolve retry	infinite
Keep alive	10 120
Remote network IP address	10.0.0.0
Remote network IP netmask	255.255.255.0
User name	client
Password	***** <input type="password"/> <input type="button" value=""/>
Extra options	<input type="button" value=""/>
HMAC authentication algorithm	SHA1 (default) <input type="button" value="▼"/>
Additional HMAC authentication	<input type="checkbox"/>
Certificate authority	<input type="button" value="Choose File"/> ca.crt
Client certificate	<input type="button" value="Choose File"/> client1.crt
Client key	<input type="button" value="Choose File"/> client1.key

Figura de mai sus prezintă o instanță de client OpenVPN configurată, care utilizează protocolul UDP și metoda de autentificare TLS/parolă. Tabelul de mai jos explică pe larg configurarea fiecărui câmp.

	Nume câmp	Valori posibile	Explicație
1.	Enable	Bifat/Nebifat	Pornește sau oprește instanța OpenVPN
2.	TUN/TAP	TUN (tunnel) / TAP (bridged)	Tipul interfeței OpenVPN. TUN se folosește cel mai des în conexiunile VPN tipice, însă TAP este necesar în anumite configurații puncte Ethernet
3.	Protocol	UDP / TCP	Protocolul de transfer folosit de conexiune
4.	Port	0 – 65535	Numărul portului (asigurați-vă că acest port este permis de firewall)
5.	LZO	Bifat/Nebifat	Cu ajutorul compresiei LZO, conexiunea Dvs. VPN va genera mai puțin trafic în rețea. Cu toate acestea, activarea acestei opțiuni determină o încărcare mai mare a procesorului. Utilizați-o cu atenție în caz de trafic intens sau de resurse de procesare scăzute
6.	Encryption	BF-CBC 128 (default) / AES-128-CBC 128 / ...	Algoritmul de criptare a pachetelor
7.	Authentication	TLS / Static Key / Password / TLS/Password	Modul de autentificare, folosit pentru securizarea sesiunilor de date. Static key – Cheie statică – este o cheie secretă utilizată pentru autentificarea server-client. Modul de autentificare TLS utilizează certificate de tip X.509: autoritatea de certificare (CA), certificatul de client, cheia clientului . Toate certificatele menționate pot fi generate folosind utilitare OpenVPN sau Open SSL pe orice tip de mașină gazdă. Password – Parola este o autentificare simplă bazată pe nume de utilizator / parolă în care proprietarul serverului OpenVPN furnizează datele de logare. TLS/Password utilizează autentificarea atât prin TLS, cât și prin parolă
8.	TLS cipher Cifru TLS	All / DHE + RSA / Custom	Algoritmul de criptare a pachetelor (cifru)
9.	Remote host/IP address	Orice nume de gazdă sau adresă IP	Adresa IP sau numele de gază al unui server OpenVPN
10.	Resolve Retry Reîncercare rezoluțione	Infinite / orice număr întreg	Perioada de timp, în secunde, pentru rezoluțunea periodică a numelui de gazdă al serverului atunci când prima rezolvare a eșuat, înainte de generarea unei excepții privind serviciul
11.	Keep alive	Orice număr întreg *spațiu* orice număr întreg	Definește două intervale de timp: unul este folosit pentru a trimite periodic cererea ICMP către serverul OpenVPN, celălalt definește o fereastră de timp utilizată pentru repornirea serviciului OpenVPN, dacă nu se primește niciun răspuns ICMP în această fereastră. Ex.: "10 60"
12.	Remote network IP address	Orice adresă IP privată	Adresa IP a rețelei LAN de la distanță
13.	Remote network IP netmask	Orice mască de rețea	Masca de subrețea a rețelei LAN de la distanță
14.	User name	Numele de utilizator al clientului	Numele de utilizator folosit pentru autentificare
15.	Password	Parola clientului	Parola folosită pentru autentificare
16.	Extra options		Opțiunile suplimentare ce vor fi folosite de instanța OpenVPN
17.	HMAC authentication algorithm	none / SHA1(default) / SHA256 / SHA384 / SHA512	Tipul algoritmului de autentificare HMAC
18.	Additional HMAC authentication	Bifat/Nebifat	Un strat suplimentar de autentificare HMAC, deasupra canalului de control TLS, pentru protecția împotriva atacurilor de tip DoS
19.	Certificate authority	Fișier .ca	Autoritatea de certificare este o entitate care emite certificate digitale. Un certificat digital certifică deținerea unei chei publice de către titularul certificatului

20.	Client certificate	Fișier .crt	Certificatul de client este un tip de certificat digital care este utilizat de sistemele-client pentru a trimite cereri autentificate către un server de la distanță. Certificatele de client joacă un rol esențial în numeroase tipuri de autentificare reciprocă, oferind garanții solide cu privire la identitatea unui solicitant
21.	Client key	Fișier .key	Autentifică clientul pe server și îi stabilește cu precizie identitatea

După ce ați setat oricare dintre acești parametri, apăsați butonul "**Save**"; în caz contrar modificările nu vor fi aplicate. Unii dintre parametrii selectați vor fi afișați în lista de configurații. Trebuie să știți și că routerul va lansa un serviciu OpenVPN separat pentru fiecare configurație introdusă (dacă este definită ca fiind activă la acel moment, desigur), astfel încât routerul are capacitatea de a acționa ca server și client în același timp.

9.7.1.2 Serverul OpenVPN

OpenVPN Instance: Server_demo

Main Settings

Enable <input checked="" type="checkbox"/>
TUN/TAP <input type="button" value="TUN (tunnel)"/>
Protocol <input type="button" value="UDP"/>
Port <input type="text" value="1194"/>
LZO <input checked="" type="checkbox"/>
Encryption <input type="button" value="BF-CBC 128 (default)"/>
Authentication <input type="button" value="TLS"/>
TLS cipher <input type="button" value="All"/>
Client to client <input checked="" type="checkbox"/>
Keep alive <input type="text" value="10 120"/>
Virtual network IP address <input type="text" value="10.0.0.0"/>
Virtual network netmask <input type="text" value="255.255.255.0"/>
Push option <input type="text" value="route 192.168.1.0 255.255.255.0"/> <input type="button" value="+"/>
Allow duplicate certificates <input type="checkbox"/>
Certificate authority <input type="button" value="Choose File"/> ca.crt
Server certificate <input type="button" value="Choose File"/> server.crt
Server key <input type="button" value="Choose File"/> server.key
Diffie Hellman parameters <input type="button" value="Choose File"/> dh1024.pem

Figura de mai sus prezintă o instanță configurată de server OpenVPN ce utilizează protocolul UDP și metoda de autentificare TLS. După cum vedeați, configurarea este similară clientului OpenVPN, dar cu câteva diferențe esențiale. Tabelul de mai jos explică pe larg configurarea fiecărui câmp.

	Nume câmp	Valori posibile	Explicație
1.	Enable	Bifat/Nebifat	Pornește sau oprește instanța OpenVPN
2.	TUN/TAP	TUN (tunnel) / TAP (bridged)	Tipul interfeței OpenVPN. TUN se folosește cel mai des în conexiunile VPN tipice, însă TAP este necesar în anumite configurații Ethernet puncte
3.	Protocol	UDP / TCP	Protocolul de transfer folosit de conexiune
4.	Port	0 – 65535	Numărul portului (asigurați-vă că acest port este permis de firewall)
5.	LZO	Bifat/Nebifat	Cu ajutorul compresiei LZO, conexiunea Dvs. VPN va genera mai puțin trafic în rețea. Cu toate acestea, activarea acestei opțiuni determină o încărcare mai mare a procesorului. Utilizați-o cu atenție în caz de trafic intens sau de resurse de procesare scăzute
6.	Encryption	BF-CBC 128 (default) / AES-128-CBC 128 / ...	Algoritmul de criptare a pachetelor
7.	Authentication	TLS / Static Key / Password / TLS/Password	<p>Modul de autentificare, folosit pentru securizarea sesiunilor de date.</p> <p>Static key – Cheie statică – este o cheie secretă utilizată pentru autentificarea server-client.</p> <p>Modul de autentificare TLS utilizează certificate de tip X.509: autoritatea de certificare (CA), certificatul de server, cheia serverului, parametrii Diffie Hellman.</p> <p>Toate certificatele menționate pot fi generate folosind utilitate OpenVPN sau Open SSL pe orice tip de mașină gazdă.</p> <p>TLS/Password utilizează atât certificatele TLS, cât și o autentificare de tip utilizator/parolă</p>
8.	TLS cipher	All / DHE + RSA / Custom	Algoritmul de criptare a pachetelor (cifru)
9.	Client to client	Bifat/Nebifat	Activează comunicația client-la-client în rețeaua virtuală. Pentru a funcționa, trebuie utilizată secțiunea TLS Clients
10.	Keep alive	Orice număr întreg *spațiu* orice număr întreg	Definește două intervale de timp: unul este folosit pentru a trimite periodic cererea ICMP către serverul OpenVPN, celălalt definește o fereastră de timp utilizată pentru repornirea serviciului OpenVPN, dacă nu se primește niciun răspuns ICMP în această fereastră. Exemplu: "10 60"
11.	Virtual network IP address	Orice adresă IP privată	Adresa IP a rețelei LAN de la distanță
12.	Virtual network IP netmask	Orice mască de rețea	Masca de subrețea a rețelei LAN de la distanță
13.	Push option	route 192.168.1.0 255.255.255.0	Opțiunile de inserare forțată sunt o modalitate de a "împinge" rutele definite de utilizator în tabelele de rutare ale clientilor care se conectează. În exemplul dat, serverul va insera ruta rețelei 192.168.1.0 cu masca de rețea 255.255.255.0 la clienții care se conectează. Prin urmare, clientul va putea accesa dispozitivele din rețeaua 192.168.1.0. Acest lucru este util atunci când un client trebuie să acceseze dispozitive situate în rețeaua LAN a serverului OpenVPN.
14.	Allow duplicate certificates	Bifat/Nebifat	Dacă bifați, serverul permite conectarea clientilor cu certificate identice (duplicate)
15.	Certificate authority	Fișier .ca	Autoritatea de certificare este o entitate care emite certificate digitale. Un certificat digital certifică deținerea unei chei publice de către titularul certificatului
16.	Server certificate	Fișier .crt	Certificatul de server este un tip de certificat digital care este utilizat pentru identificarea serverului OpenVPN
17.	Server key	Fișier .key	Autentifică clienții pe server
18.	Diffie Hellman parameters	Fișier .pem	Parametrii Diffie-Hellman (DH) definesc modul în care OpenSSL realizează schimbul de chei DH

9.7.1.3 Clienți TLS

Clienții TLS reprezintă o modalitate de diferențiere avansată a clientilor prin numele lor comun (CN) găsit în fișierul certificatului de client. Se poate folosi pentru a atribui anumite adrese VPN anumitor clienți și pentru a le lega de adresele lor LAN, astfel încât alte dispozitive din rețeaua LAN a clientului să poată fi accesate de server sau alți clienți.

Secțiunea TLS Clients se află în fereastra de configurare a serverului OpenVPN, cu condiția ca serverul OpenVPN să utilizeze metode de autentificare TLS sau TLS/Password. Pentru a crea un client TLS nou, tastează numele noului client în câmpul de text de sub tab-ul TLS Clients și apăsați butonul "**Add**" alăturat, așa cum se arată în imaginea de mai jos.

TLS Clients

Here you can add your VPN clients so that they may be reachable from the server.

There are no values created yet

client1	Add
---------	------------

Această acțiune va crea un client TLS nou, neconfigurat. Imaginea de mai jos prezintă un client TLS configurat.

TLS Clients

Here you can add your VPN clients so that they may be reachable from the server.

client1	VPN instance name: server_demo
	Endpoint name:
	Common name (CN): client1
	Virtual local endpoint: 10.0.0.6
	Virtual remote endpoint: 10.0.0.5
	Private network: 192.168.1.0
	Private netmask: 255.255.255.0
Delete	Add

	Nume câmp	Valoare în exemplu	Explicație
1.	VPN instance name Nume instanță VPN	server_demo	Cu ce instanță VPN trebuie asociat clientul TLS
2.	Endpoint name		Numele punctului Dvs. terminal
3.	Common name (CN)	client1	Numele comun (CN) al clientului găsit în fișierul ce conține certificatul de client
4.	Virtual local endpoint	10.0.0.6	Adresa locală virtuală a clientului în rețeaua virtuală
5.	Virtual remote endpoint	10.0.0.5	Adresa la distanță virtuală a clientului în rețeaua virtuală
6.	Private network	192.168.1.0	Adresa privată de rețea a clientului
7.	Private netmask	255.255.255.0	Masca privată de rețea a clientului

9.7.2 IPsec

Protocolul IPsec permite routerului să stabilească o conexiune securizată cu un peer IPsec prin internet. IPsec este suportat în două moduri – transport și tunel. Modul transport creează un canal punct-la-punct securizat între două gazde. Modul tunel poate fi utilizat pentru a construi o conexiune securizată între două rețele LAN la distanță servind drept o soluție VPN.

Sistemul IPsec menține două baze de date: baza de date a politicilor de securitate (SPD) care definește dacă IPsec se aplică sau nu la un pachet și specifică ce asociere de securitate (IPsec-SA) se aplică și cum, precum și baza de date a asocierilor de securitate (SAD), care conține o cheie a fiecărei IPsec-SA.

Crearea asocierii de securitate între doi parteneri este necesară pentru comunicarea IPsec. Se poate efectua prin configurație manuală sau automată.

Notă: routerul începe să creeze un tunel atunci când datele sunt trimise de la router la distanță prin tunel. Funcția Keep Alive este utilizată pentru crearea automată a tunelului.

Pentru a crea o nouă instanță IPsec, accesați tab-ul IPsec, tastăți un nume pentru noua dvs. instanță în câmpul de text de sub tab-ul IPsec și apăsați butonul "**Add**" alăturat.

The screenshot shows the 'IPsec Configuration' section of the router's web interface. A table lists configurations with columns: Name, Enabled, Mode, Dead Peer Detection, and Remote VPN endpoint. A text message below the table says 'There are no IPsec configurations yet'. In the 'Name' column, the word 'demo' is typed. To the right of the table is a large blue downward-pointing arrow indicating the next step.

Name	Enabled	Mode	Dead Peer Detection	Remote VPN endpoint
demo				

The screenshot shows the 'IPsec Configuration' section after the 'demo' instance has been added. The table now includes a row for 'demo'. The 'Enabled' column has a checkbox that is unchecked. The 'Mode' column shows 'Main'. The 'Dead Peer Detection' column shows 'Disabled'. The 'Remote VPN endpoint' column shows a dash. To the right of the table are two buttons: 'Edit' and 'Delete', with a blue downward-pointing arrow indicating the next step.

Name	Enabled	Mode	Dead Peer Detection	Remote VPN endpoint
demo	<input type="checkbox"/>	Main	Disabled	-

Instanța nou-creată va fi dezactivată și neconfigurată. Pentru a o configura apăsați butonul "**Edit**" din dreptul său (vezi exemplul de mai sus). Această acțiune vă va redirecționa către fereastra de configurație a instanței IPsec.

IPsec

IPsec Configuration

Enable <input checked="" type="checkbox"/>
IKE version <input type="button" value="IKEv1"/>
Mode <input type="button" value="Main"/>
Type <input type="button" value="Tunnel"/>
My identifier type <input type="button" value="Address"/>
My identifier <input type="text" value="100.121.122.123"/>
Force encapsulation <input checked="" type="checkbox"/>
Dead Peer Detection <input checked="" type="checkbox"/>
Pre shared key <input type="text" value="password"/>
Remote VPN endpoint <input type="text" value="215.148.3.15"/>
IP address/Subnet mask <input type="text" value="192.168.1.0/24"/> <input type="button" value="+"/>
Enable keepalive <input checked="" type="checkbox"/>
Host <input type="text" value="192.168.1.125"/>
Ping period (sec) <input type="text" value="60"/>

	Nume câmp	Valori posibile	Explicație
1.	Enable	Bifat/Nebifat	Pornește sau oprește IPsec
2.	IKE version Versiune IKE	IKEv1 ori IKEv2	Metoda schimbului de chei
3.	Mode	Main Principal / Aggressive Agresiv	Modul de schimb din faza 1 a ISAKMP
4.	Type	Tunnel / Transport	Tipul de conexiune
5.	My identifier type Tipul meu de identificator	Adresă / FQDN / User FQDN	Tipul de identificator folosit pentru stabilirea unei conexiuni cu altă instanță de IPsec
6.	My identifier Identifierul meu	Depinde de tipul de identificator	In cazul în care routerul are o adresă IP privată, identificatorul său ar trebui să fie propria sa adresă de LAN. Astfel este posibilă abordarea Road Warrior
7.	Force encapsulation	Bifat/Nebifat	Forțați încapsularea UDP pentru pachetele ESP chiar dacă nu este detectată nicio situație de NAT
8.	Dead Peer Detection	Bifat/Nebifat	Valorile clear, hold și restart toate activează funcția DPD
9.	Pre shared key Cheie pre-partajată	Orice sir	O parolă partajată pentru autentificare între peers
10.	Remote VPN endpoint	Adresa gazdei	Adresa IP sau numele de gazdă al instanței IPsec de la distanță
11.	IP address / Subnet mask	Adresa IP/[0 – 32]	Adresa IP și masca grupului securizat din cadrul rețelei de la distanță folosite pentru a determina cărei subrețele aparține o adresă IP. Trebuie să fie diferită de adresa IP din LAN a dispozitivului
12.	Enable keep alive	Bifat/Nebifat	Activăți funcția de "menținere în viață" a tunelului
13.	Host	Adresa gazdei	Adresa gazdei la care vor fi trimise cererile de ecou ICMP
14.	Ping period (sec)	0 – 9999999	Trimiteți o cerere de ecou ICMP la fiecare x secunde

Faza 1 și Faza 2 trebuie configurate în conformitate cu configurația serverului IPsec, astfel încât algoritmii, autentificarea și duratele de viață ale celor două faze să fie identice.

Phase

The phase must match with another incoming connection to establish IPSec

Phase 1 **Phase 2**

Encryption algorithm	3DES	▼
Authentication	SHA1	▼
DH group	MODP1536	▼
Lifetime (h)	8	Hours

Phase

The phase must match with another incoming connection to establish IPSec

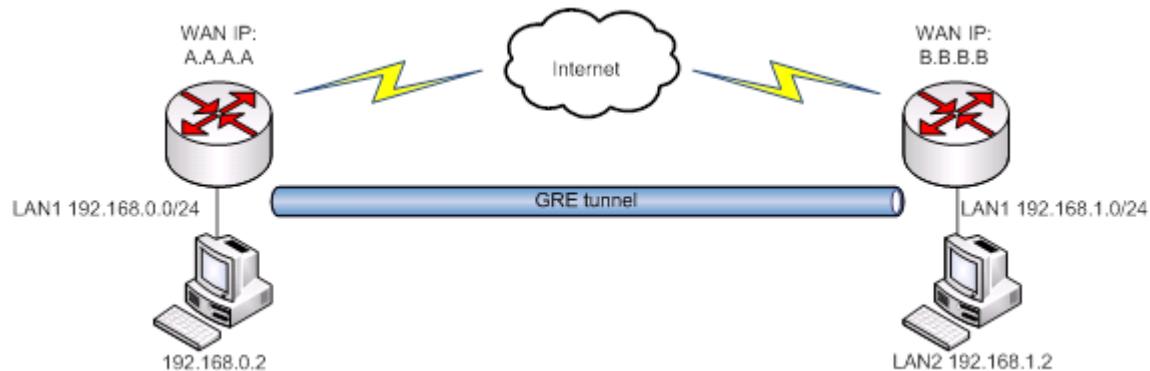
Phase 1 **Phase 2**

Encryption algorithm	3DES	▼
Hash algorithm	SHA1	▼
PFS group	MODP1536	▼
Lifetime (h)	8	Hours

	Nume câmp	Valori posibile	Explicație
1.	Encryption algorithm	DES, 3DES, AES 128, AES 192, AES256	Algoritmul de criptare trebuie să se potrivească cu altă conexiune de intrare
2.	Authentication	MD5, SHA1, SHA256, SHA384, SHA512	Algoritmul de autentificare trebuie să se potrivească cu altă conexiune de intrare
3.	Hash algorithm	MD5, SHA1, SHA256, SHA384, SHA512	Algoritmul hash trebuie să se potrivească cu altă conexiune de intrare
4.	DH group	MODP768, MODP1024, MODP1536, MODP2048, MODP3072, MODP4096	Grupul DH (Diffie-Helman) trebuie să se potrivească cu altă conexiune de intrare
4.	PFS group	MODP768, MODP1024, MODP1536, MODP2048, MODP3072, MODP4096, No PFS	Grupul PFS (Perfect Forward Secrecy) trebuie să se potrivească cu altă conexiune de intrare
5.	Lifetime Durată viață	Hours Ore , Minutes Minute , Seconds Secunde	Durata de timp pentru fază

9.7.3 Tunel GRE

GRE (Generic Routing Encapsulation, Încapsulare Generică pentru Rutare, conform RFC 2784) este o soluție de tunelare, conform RFC 1812, a traficului spațiului privat de adresare peste o rețea TCP/IP intermediară cum este internetul. Tunelarea GRE nu folosește criptarea, ci doar încapsulează datele și le transmite prin WAN.



În exemplul de rețea din schema de mai sus sunt conectate două rețele îndepărtate LAN1 și LAN2.

Pentru a crea un tunel GRE utilizatorul trebuie să cunoască următorii parametri:

1. Adresele IP ale sursei și destinației
2. Adresa IP locală a tunelului
3. Adresa IP și masca de subrețea a rețelei îndepărtate

Pentru a crea o nouă instanță GRE, accesați tab-ul GRE Tunnel, tastați un nume pentru noua dvs. instanță în câmpul de text de sub tab-ul GRE Tunnel și apăsați butonul “Add” alăturat.

Generic Routing Encapsulation Tunnel

GRE Tunnel Configuration

Disable NAT

Tunnel name	Enable
There are no GRE Tunnel configurations yet	

New configuration name: **Add New** 

↓

Tunnel name	Enable
Gre_demo	<input type="checkbox"/>
	Edit  Delete

Instanța nou-creată va fi dezactivată și neconfigurată. Pentru a o configura apăsați butonul “Edit” din dreptul său (vezi exemplul de mai sus). Această acțiune vă va redirecționa către fereastra de configurare a instanței GRE Tunnel.

GRE Tunnel Instance: Gre_demo**Main Settings**

Enabled	<input checked="" type="checkbox"/>
Remote endpoint IP address	84.148.7.87
Remote network	192.168.2.0
Remote network netmask	24
Local tunnel IP	10.0.0.1
Local tunnel netmask	24
MTU	1500
TTL	255
PMTUD	<input checked="" type="checkbox"/>
Redirect LAN to GRE	<input type="checkbox"/>
Enable Keep alive	<input checked="" type="checkbox"/>
Keep Alive host	8.8.8.8
Keep Alive interval	60

	Nume câmp	Valori posibile	Explicație
1.	Enabled	Bifat/Nebifat	Bifați pentru a activa funcția tunel GRE
2.	Remote endpoint IP address	Adresa IP sau numele de gazdă ale rețelei îndepărtate	Specificați adresa IP sau numele de gazdă ale rețelei WAN de la distanță
3.	Remote network Rețea la distanță	O adresă IP privată	Adresa IP din LAN a dispozitivului de la distanță
4.	Remote network netmask Mască rețea la distanță	0 – 32	Rețeaua LAN a dispozitivului de la distanță
5.	Local tunnel IP Adresă IP locală tunel	O adresă IP privată	Adresa IP locală virtuală. Nu poate fi în aceeași subrețea ca rețeaua LAN
6.	Local tunnel netmask Mască rețea locală tunel	0 – 32	Rețeaua adresei IP locale virtuale
7.	MTU	0 – 1500	Unitatea maximă de transmisie (MTU) în octeți
8.	TTL	0 – 255	Specificați valoarea fixă a duratei de viață (TTL) a pachetelor tunelate. 0 este o valoare specială ce înseamnă că pachetele moștenesc valoarea TTL
9.	PMTUD	Bifat/Nebifat	Bifați pentru a activa Path Maximum Transmission Unit Discovery (PMTUD) pentru acest tunel.
10.	Redirect LAN to GRE	Bifat/Nebifat	Bifați pentru a redirecționa traficul din LAN către interfața GRE
10.	Enable Keep alive	Bifat/Nebifat	Permite uneia dintre părți să transmită și să recepționeze pachete de "menținere în viață" către și de la un router îndepărtat
11.	Keep Alive host	IP address	Adresa IP a gazdei funcției Keep Alive. De preferat o adresă IP ce aparține rețelei LAN a dispozitivului de la distanță
12.	Keep Alive interval	0 – 255	Intervalul de timp, în secunde, pentru funcția Keep Alive

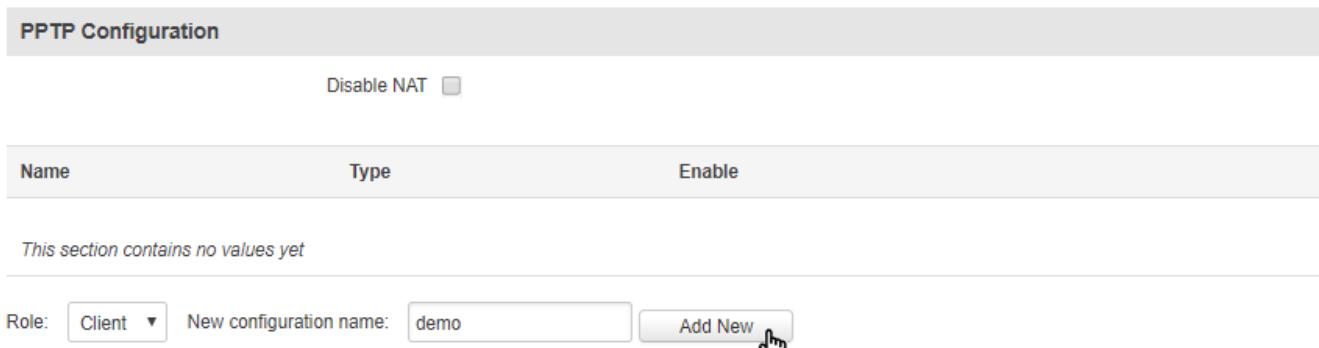
9.7.4 PPTP

Point-to-Point Tunneling Protocol (PPTP) – Protocolul de tunelare punct-la-punct este un protocol (set de reguli de comunicație) ce permite corporațiilor să-și extindă propriile rețele prin "tunele" private prin internetul public. Efectiv, o corporație utilizează o rețea cu o arie largă ca o singură rețea locală mare. O companie nu mai are nevoie să-și închirieze propriile linii pentru comunicații pe arie largă, ci poate utiliza în siguranță rețelele publice.

9.7.4.1 Clientul PPTP

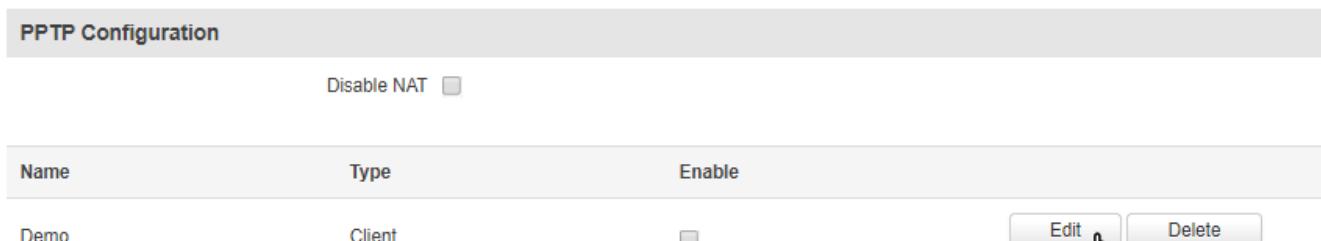
Pentru a crea o nouă instanță PPTP, accesați tab-ul PPTB, selectați **Rolul** (server sau client) instanței Dvs., introduceți un nume în câmpul **"New configuration name"** |Numele noii configurații| și apăsați butonul **"Add"** alăturat.

Point-to-Point Tuneling Protocol



This screenshot shows the 'PPTP Configuration' section of a web-based interface. At the top, there is a 'Disable NAT' checkbox. Below it is a table with columns 'Name', 'Type', and 'Enable'. A message 'This section contains no values yet' is displayed. At the bottom, there is a 'Role' dropdown set to 'Client', a 'New configuration name' input field containing 'demo', and an 'Add New' button. A blue arrow points downwards from the 'Add New' button towards the second screenshot.

Point-to-Point Tuneling Protocol



This screenshot shows the 'PPTP Configuration' section after a new entry has been added. The table now includes a row for 'Demo' (Type: Client). To the right of this row are 'Edit' and 'Delete' buttons, with a hand cursor hovering over the 'Edit' button. Below the table is a 'Role' dropdown and a 'New configuration name' input field, along with an 'Add New' button. A blue arrow points upwards from the 'Edit' button towards the first screenshot.

Instanța nou-creată va fi dezactivată și neconfigurată. Pentru a o configura apăsați butonul **"Edit"** din dreptul său (vezi exemplul de mai sus). Această acțiune vă va redirecționa către fereastra de configurare a instanței PPTP.

PPTP Client Instance: Demo**Main Settings**Enable Use as default gateway Client to client

Server 84.15.198.92

User name user

Password 

	Nume câmp	Valori posibile	Explicație
1.	Enable	Bifat/Nebifat	Bifați pentru a activa configurația curentă
2.	Use as default gateway	Bifat/Nebifat	Utilizați această instanță PPTP ca gateway implicit
3.	Client to client	Bifat/Nebifat	Bifați pentru a activa comunicația client-la-client
4.	Server	Adresă IP sau nume de gazdă	Adresa IP sau numele de gazdă ale serverului PPTP
5.	Username	Orice nume	Numele de utilizator pentru autorizarea pe server
6.	Password	Orice parolă	Parola pentru autorizarea pe server

9.7.4.2 Serverul PPTP**PPTP Server Instance: Demo****Main Settings**Enable

Local IP 192.168.0.1

Remote IP range start 192.168.0.20

Remote IP range end 192.168.0.30

User name	Password	PPTP Client's IP	
user1 	192.168.0.21	Delete
user2 	192.168.0.22	Delete
Add			

	Nume câmp	Explicație
1.	Enable	Bifați căsuța pentru a activa funcția PPTP
2.	Local IP	Adresa IP virtuală a acestui dispozitiv (RUT)
3.	Remote IP range start	Începutul intervalului de adrese IP închiriate
4.	Remote IP range end	Sfârșitul intervalului de adrese IP închiriate
5.	Username	Numele de utilizator pentru conectarea la acest server PPTP
6.	Password	Parola pentru conectarea la acest server PPTP
7.	PPTP Client's IP Adresă IP client PPTP	Adresa IP a utilizatorului. Lăsați necompletat pentru a aloca o adresă aleatorie din intervalul specificat mai sus

9.7.5 L2TP

În domeniul rețelelor de calculatoare, Layer 2 Tunneling Protocol (L2TP) – Protocolul de tunelare nivel 2 – este un protocol de tunelare folosit pentru a suporta rețele private virtuale (VPN). Este mai sigur decât PPTP însă, întrucât încapsulează de două ori datele transferate, este mai lent și folosește mai multă putere de procesare.

9.7.5.1 Clientul L2TP

Pentru a crea o nouă instanță L2TP, accesați tab-ul L2TP, selectați **Rolul** (server sau client) instanței Dvs., introduceți un nume în câmpul **“New configuration name”** |Numele noii configurații| și apăsați butonul **“Add”** alăturat.

The screenshot shows two instances of the 'Layer 2 Tuneling Protocol' configuration page. The top instance is for creating a new configuration, and the bottom instance shows the newly created 'Demo' configuration.

Top Instance (Creating New Configuration):

- L2TP Configuration:** A section with a 'Disable NAT' checkbox.
- Name:** A field containing 'demo'.
- Type:** A dropdown menu set to 'Client'.
- Add New:** A button with a hand cursor icon, highlighted by a blue arrow pointing downwards.

Bottom Instance (Existing Configuration):

- L2TP Configuration:** A section with a 'Disable NAT' checkbox.
- Name:** 'Demo'.
- Type:** 'Client'.
- Enable:** An unchecked checkbox.
- Edit:** A button with a hand cursor icon, highlighted by a blue arrow pointing downwards.
- Delete:** A button.

Common Interface Elements:

- Role:** A dropdown menu set to 'Client'.
- New configuration name:** A field containing 'demo'.
- Add New:** A button.

Instanța nou-creată va fi dezactivată și neconfigurată. Pentru a o configura apăsați butonul **“Edit”** din dreptul său (vezi exemplul de mai sus). Această acțiune vă va redirecționa către fereastra de configurare a instanței L2TP.

L2TP Client Instance: Demo**Main Settings**Enable

Server 84.15.66.47

Username user1

Password 

	Nume câmp	Explicație
1.	Enable	Bifați pentru a activa instanța tunelului L2TP
2.	Server	Adresa IP sau numele de gazdă ale serverului L2TP
3.	Username	Numele de utilizator folosit pentru a vă autentifica pe server
4.	Password	Parola folosită pentru a vă autentifica pe server

9.7.5.2 Serverul L2TP**L2TP Server Instance: Demo****Main Settings**Enable

Local IP 192.168.0.1

Remote IP range begin 192.168.0.20

Remote IP range end 192.168.0.30

User name	Password	
user1	<input type="password"/> 	Delete
user2	<input type="password"/> 	Delete
<input type="button" value="Add"/>		

	Nume câmp	Explicație
1.	Enable	Bifați pentru a activa instanța tunelului L2TP
2.	Local IP	Adresa IP locală a serverului Dvs. L2TP
3.	Remote IP range begin	Începutul domeniului de adrese IP pentru conectarea clientilor
4.	Remote IP range end	Sfârșitul domeniului de adrese IP pentru conectarea clientilor
5.	Username	Numele de utilizator al clientului folosit pentru autentificarea pe acest server L2TP
6.	Password	Parola clientului folosită pentru autentificarea pe acest server L2TP

9.8 Dynamic DNS

Dynamic DNS (DDNS) – sistem dinamic de nume de domeniu – este un serviciu de nume de domeniu care permite legarea adreselor IP dinamice de un nume de gazdă static. Pentru a începe să utilizați această funcție, trebuie mai întâi să vă înregistrați la un furnizor de servicii DDNS (lista de exemple este dată în descriere).

În mod implicit, va fi prezentă o instanță DDNS neconfigurată, prezentată în imaginea de mai jos. Dacă doriți, puteți crea mai multe instanțe DDNS.

Dynamic DNS

Dynamic DNS allows you to reach your router using a fixed hostname while having a dynamically changing IP address.

The screenshot shows the 'DDNS' configuration page. It includes the following fields:

- Enable:** Unchecked checkbox.
- Use HTTPS:** Unchecked checkbox.
- Status:** N/A
- Service:** A dropdown menu set to 3322.org.
- Hostname:** A text input field containing yourhost.example.org.
- User name:** A text input field containing your_username.
- Password:** A redacted text input field.
- IP source:** A dropdown menu set to Custom.
- Network:** A dropdown menu set to WAN.
- IP renew interval (min):** A text input field containing 10.
- Force IP renew (min):** A text input field containing 472.

	Nume câmp	Valori posibile	Explicație
1.	Enable	Bifat/Nebifat	Activează configurarea instanței DDNS curente
2.	Use HTTPS	Bifat/Nebifat	Activează criptarea de date SSL
3.	Status		Marca temporală a ultimei verificări sau actualizări de IP
4.	Service	1. dydns.org 2. no-ip.com 3. ...	Furnizorul Dvs. de servicii DDNS selectat din listă. În cazul în care furnizorul Dvs. DDNS nu este prezent printre cele furnizate, puteți folosi "custom" personalizat
5.	Hostname	Orice nume de gazdă	Numele de domeniu care va fi legat de adresa IP dinamică
6.	Username	Numele Dvs. de utilizator	Numele contului de utilizator (de la înregistrare)
7.	Password	Parola Dvs.	Parola contului de utilizator (de la înregistrare)
8.	IP Source	Public Private Custom	Această opțiune vă permite să selectați o anumită interfață a routerului și apoi să trimiteți adresa IP a interfeței respective către serverul DDNS. Deci, dacă, de exemplu, routerul Dvs. are o adresă IP privată (adică 10.140.56.57) la interfața sa WAN (3G), atunci puteți trimite acest IP exact către serverul DDNS selectând "Private" sau selectând "Custom" și interfața "WAN"
9.	Network	WAN / WAN2 / WAN3 / LAN / PPP	Rețeaua sursă
10.	IP renew interval Interval reînnoire IP (min)	5 – 600000	Intervalul de timp pentru verificarea schimbării adresei IP a dispozitivului
11.	Force IP renew Forțare reînnoire IP (min)	5 – 600000	Intervalul de timp pentru forțarea reînnoirii adresei IP

9.9 Utilitare SMS

RUT955 dispune de un număr mare de diverse utilitare SMS. Secțiunea SMS Utilities este împărțită în 6 subsecțiuni: SMS Utilities |Utilitare SMS|, Call Utilities |Utilitare apeluri|, User Groups |Grupuri utilizatori|, SMS Management |Gestionare SMS|, Remote Configuration |Configurare de la distanță| și Statistics |Statistici|.

9.9.1 Utilitare SMS

Tab-ul SMS Utilities conține o listă de reguli ce execută anumite acțiuni când sunt activate prin mesaje SMS.

SMS Utilities

SMS Rules				
Enable	Action	SMS Text	Authorization method	Sort
<input checked="" type="checkbox"/>	Reboot	reboot	By router admin password	
<input checked="" type="checkbox"/>	Get status	status	By router admin password	
<input checked="" type="checkbox"/>	Get I/O status	iostatus	By router admin password	

Figura de mai sus prezintă o parte din lista de reguli aferente utilitarelor SMS. Întreaga listă conține 26 de reguli, dar aveți și posibilitatea de a configura reguli personalizate.

Toate opțiunile de configurare implicate sunt enumerate mai jos:

- Reboot | Repornire|
- Get status |Obținere stare|
- Get I/O status |Obținere stare intrări/ieșiri|
- Get OpenVPN status |Obținere stare OpenVPN|
- Switch WiFi on/off |Pornire/oprire WiFi|
- Switch mobile data on/off |Pornire/oprire date mobile|
- Switch OpenVPN on/off |Pornire/oprire OpenVPN|
- Change mobile data settings |Modificare setări date mobile|
- Get list of profiles |Obținere listă profiluri|
- Change profile |Modificare profil|
- SSH access control |Control acces SSH|
- Web access control |Control acces web|
- Restore to default |Restabilire setări implicate|
- Force SIM switch |Forțare comutare SIM-uri|
- GPS coordinates |Coordonate GPS|
- GPS on/off |Pornire/oprire GPS|
- FW upgrade from server |Upgradare firmware de pe server|
- Config update from server |Actualizare configurații de pe server|
- Switch monitoring on/off |Pornire/oprire monitorizare|
- Monitoring status |Stare monitorizare|
- Interfața de programare a aplicațiilor (API) UCI

Cum să executați o regulă:

Pentru a executa o regulă trebuie doar să trimiteți la numărul cartelei SIM a routerului un mesaj SMS cu textul SMS al regulii; de exemplu, dacă trimiteți un mesaj cu textul "**reboot**", routerul va reporni, cu condiția ca metoda de autorizare selectată să fie "**No authorization**" |Fără autorizare|. Totuși, dacă există o metodă de autorizare, va trebui să includeți în mesaj "**cheia de autorizare**". Această cheie de autorizare depinde de metoda de autorizare aleasă, adică: dacă metoda este "By serial" |Prin număr serie|, "**cheia de autorizare**" este numărul de serie al routerului; dacă metoda este "By router admin password" |Prin parolă administrator router|, "**cheia de autorizare**" este parola de administrator al routerului. Cheia de autorizare trebuie să preceadă textul de activare, de care trebuie să fie separată de un **spațiu**. De exemplu, dacă metoda de autorizare aleasă este "**By router admin password**" și parola este "**admin01**", întregul mesaj ar trebui să arate astfel: "admin01 reboot". Același lucru este valabil și pentru autorizarea "By serial".

9.9.1.1 Reguli SMS implicate

Această secțiune prezintă tabelul ce conține toate regulile implicate și explicații pentru acestea.

	Nume câmp	Explicație	Note
1.	Reboot Repornire		
	Enable	Această căsuță va activa ori dezactiva funcția SMS de repornire	Permite repornirea routerului prin SMS
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, repornirea routerului	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method Metodă autorizare	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization Fără autorizare , By serial Prin număr serie sau By router admin password Prin parolă administrator router
	Allowed users Utilizatori permisi	Lista albă a utilizatorilor permisi	From all numbers De la toate numerele , From group De la grup sau From single number De la un singur număr
	Get status via SMS after reboot Obținere stare prin SMS după repornire	Bifați pentru a obține starea conexiunii prin SMS după repornire	Dacă ați bifat, routerul va trimite un mesaj de stare după ce a repornit și este din nou funcțional. Aceasta este atât o regulă SMS separată, cât și o opțiune în cadrul regulii Repornire prin SMS. După ce ați bifat, câmpul „Send status SMS to other number“ va deveni disponibil
	Send status SMS to other number Trimitere SMS stare către alt număr	Activăți dacă dorîți ca mesajul de stare să fie transmis la unul sau mai multe numere de telefon (diferit/e de numărul expeditorului)	Dacă ați bifat, vi se va cere să introduceți unul sau mai multe numere de telefon Acest câmp este vizibil numai dacă ați bifat „Get status via SMS after reboot“
	Message text Text mesaj	Ce informații de stare vor fi incluse în SMS: Data state Stare date , Operator, Connection type Tip conexiune , Signal Strength Intensitate semnal , Connection State Stare conexiune , IP	Puteți selecta ce elemente de stare să fie afișate
2.	Get status Obținere stare 		
	Enable	Această căsuță va activa ori dezactiva funcția SMS de stare	Vă permite să obțineți prin SMS starea routerului. Aceasta este atât o regulă SMS separată, cât și o opțiune în cadrul regulii Repornire
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, să vă fie transmisă starea routerului	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password.
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number

	Send status SMS to other number	Activări dacă doriți ca mesajul de stare să fie transmis la unul sau mai multe numere de telefon (diferit/e de numărul expeditorului)	Dacă ați bifat, vi se va cere să introduceți unul sau mai multe numere de telefon
	Message text	Ce informații de stare vor fi incluse în SMS: Data state, Operator, Connection type, Signal Strength, Connection State, IP	Puteți selecta elementele de stare ce vor fi incluse în mesaj
3.	Get I/O status Obținere stare intrări/ieșiri 		
	Enable	Această căsuță va activa ori dezactiva funcția SMS de stare a intrărilor/ieșirilor	Vă permite să obțineți prin SMS starea intrărilor/ieșirilor routerului
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, să vă fie transmisă starea intrărilor/ieșirilor routerului	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password.
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
	Send status SMS to other number	Activări dacă doriți ca mesajul de stare să fie transmis la unul sau mai multe numere de telefon (diferit/e de numărul expeditorului)	Dacă ați bifat, vi se va cere să introduceți unul sau mai multe numere de telefon
4.	Get OpenVPN status Obținere stare OpenVPN 		
	Enable	Această căsuță va activa ori dezactiva funcția de stare a OpenVPN	Vă permite să obțineți prin SMS starea conexiunii OpenVPN a routerului
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, să vă fie transmisă starea OpenVPN a routerului	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
	Send status SMS to other number	Activări dacă doriți ca mesajul de stare să fie transmis la unul sau mai multe numere de telefon (diferit/e de numărul expeditorului)	Dacă ați bifat, vi se va cere să introduceți unul sau mai multe numere de telefon
5.	Switch WiFi On/Off Pornire/oprire WiFi 		
	Enable	Această căsuță va activa ori dezactiva funcția de pornire/oprire WiFi	Permite controlul conexiunii Wi-Fi prin SMS

Action	Acțiunea ce va fi efectuată când această regulă se aplică	Pornește sau oprește conexiunea WiFi
SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, pornirea/oprirea conexiunii Wi-Fi	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
Write to config Scriere în configurație	Salvează permanent starea conexiunii Wi-Fi	Dacă această setare este activată, routerul va menține noua stare a conexiunii Wi-Fi chiar și după repornire. Dacă nu ati selectat această setare, routerul va schimba înapoi starea conexiunii Wi-Fi după repornire

6. Switch mobile data on/off |Pornire/oprire date mobile|

Enable	Această căsuță va activa oridezactiva funcția de pornire/oprire a datelor mobile	Permite controlul datelor mobile prin SMS
Action	Acțiunea ce va fi efectuată când această regulă se aplică	Pornește sau oprește datele mobile
SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, pornirea/oprirea datelor mobile	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
Write to config	Salvează permanent starea rețelei de telefonie mobilă	Dacă această setare este activată, routerul va menține noua stare a datelor mobile chiar și după repornire. Dacă nu ati selectat această setare, routerul va schimba înapoi starea datelor mobile după repornire

7. Manage OpenVPN |Gestionare OpenVPN|

Enable	Această căsuță va activa oridezactiva funcția de gestionare a OpenVPN	Permite controlul OpenVPN prin SMS control
Action	Acțiunea ce va fi efectuată când această regulă se aplică	Pornește sau oprește OpenVPN
SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, pornirea/oprirea OpenVPN	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează După textul SMS-ului trebuie să scrieți numele instanței OpenVPN
Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number

8. Change mobile data settings |Modificare setări date mobile|

Enable	Această căsuță va activa oridezactiva funcția de modificare a setărilor datelor mobile	Vă permite să modificați setările datelor mobile prin SMS
--------	--	---

Action	Acțiunea ce va fi efectuată când această regulă se aplică	
SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, modificarea setărilor specificate ale datelor mobile	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează. Utilizarea acestei funcții va fi explicată detaliat în tabelul de mai jos
Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number

Setări ale datelor mobile prin parametri SMS:

	Parametru	Valoare/valori	Explicație
1.	apn=	De ex., internet.gprs	Setează numele punctului de acces (APN)
2.	dialnumber=	De ex., *99***1#	Setează numărul de apelare
3.	auth_mode=	none pap chap	Setează modul de autentificare
4.	service=	Auto 4gonly 3gonly 2gonly	Setează modul serviciului de telefonie mobilă
5.	username=	De ex., user	Folosit numai dacă modul de autentificare selectat este PAP sau CHAP
6.	password=	De ex., pass	Folosit numai dacă modul de autentificare selectat este PAP sau CHAP

Toate aceste setări pot fi schimbate într-un singur SMS. Este necesară introducerea unui spațiu între perechile <parametru=valoare>.

Exemplu: `cellular apn=internet.gprs dialnumber=*99***1# auth_mode=pap service=3gonly username=user password=user`

	Nume câmp	Explicație	Note
9.	Get list of profiles Obținere listă profiluri		
	Enable	Această căsuță va activa ori dezactiva funcția de obținere a listei profilurilor	Vă permite să obțineți lista profilurilor prin SMS
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, să vă fie transmisă lista profilurilor	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
10.	Change profile Schimbare profil		
	Enable	Această căsuță va activa ori dezactiva funcția de schimbare a profilului	Vă permite să schimbați profilurile prin SMS
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	

	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, să transmită schimbarea de profil	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează. După textul SMS-ului trebuie să scrieți numele instanței OpenVPN
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
11.	SSH access Control Control acces SSH 		
	Enable	Această căsuță va activa ori dezactiva funcția de control al accesului prin SSH	Permite controlul accesului prin SSH prin SMS
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, pornirea/oprirea accesului prin SSH	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
	Enable SSH access Activare acces SSH	Activăți pentru a accesa routerul prin SSH din rețeaua LAN	Dacă bifați, SMS-ul va activa accesul prin SSH din LAN; dacă nu bifați, SMS-ul va dezactiva accesul prin SSH din LAN
	Enable remote SSH access Activare acces SSH la distanță	Activăți pentru a accesa routerul prin SSH din rețeaua WAN	Dacă bifați, SMS-ul va activa accesul prin SSH din WAN; dacă nu bifați, SMS-ul va dezactiva accesul prin SSH din WAN
12.	Web access Control Control acces web 		
	Enable	Această căsuță va activa ori dezactiva funcția control al accesului web	Permite controlul accesului web prin SMS
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, pornirea/oprirea accesului web	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
	Enable HTTP access Activare acces HTTP	Activăți pentru a accesa routerul prin HTTP din rețeaua LAN	Dacă bifați, SMS-ul va activa accesul prin HTTP din LAN; dacă nu bifați, SMS-ul va dezactiva accesul prin HTTP din LAN
	Enable remote HTTP access Activare acces HTTP la distanță	Activăți pentru a accesa routerul prin HTTP din rețeaua WAN	Dacă bifați, SMS-ul va activa accesul prin HTTP din WAN; dacă nu bifați, SMS-ul va dezactiva accesul prin HTTP din WAN
	Enable remote HTTPS access Activare acces HTTPS la distanță	Activăți pentru a accesa routerul prin HTTPS din rețeaua WAN	Dacă bifați, SMS-ul va activa accesul prin HTTPS din WAN; dacă nu bifați, SMS-ul va dezactiva accesul prin HTTPS din WAN
13.	Restore to default Restabilire setări implicate 		
	Enable	Această căsuță va activa ori dezactiva funcția de restabilire a setărilor implicate	Vă permite să reduceți prin SMS routerul la setările sale implicate
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	Routerul va reporni după executarea acestei reguli și toate configurațiile vor fi sterse

	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, readucerea routerului la setările sale implicate	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
14.	Force SIM switch Forțare comutare SIM-uri 		
	Enable	Această căsuță va activa ori dezactiva funcția de comutare între cartelele SIM	Permite comutarea între cartelele SIM prin SMS
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, forțarea unei comutări între cartelele SIM	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
15.	GPS coordinates Coordonate GPS 		
	Enable	Această căsuță va activa ori dezactiva funcția de obținere a coordonatelor GPS	Vă permite să obțineți coordonatele GPS prin SMS
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, transmiterea coordonatelor GPS	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
16.	GPS		
	Enable	Această căsuță va activa ori dezactiva funcția de pornire/oprire a GPS-ului	Vă permite să controlați GPS-ul prin SMS
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	Pornește sau oprește GPS-ul
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, pornirea/oprirea GPS-ului	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Lista albă a utilizatorilor permisi	From all users, From group sau From single number
17.	Force FW upgrade from server Forțare upgrade firmware de pe server 		
	Enable	Această căsuță va activa ori dezactiva funcția de upgradare a firmware-ului de pe server	Vă permite să upgradați firmware-ul routerului prin SMS
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	Routerul va reporni după executarea acestei reguli

	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, forțarea unui upgrade de firmware de pe server	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
18.	Force Config update from server Forțare actualizare configurări de pe server 		
	Enable	Această căsuță va activa ori dezactiva funcția de actualizare a configurărilor de pe server	Vă permite să actualizați configurările routerului prin SMS
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	Routerul va reporni după executarea acestei reguli
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, forțarea unei actualizări a configurărilor de pe server	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
19.	Switch monitoring on/off Pornire/oprire monitorizare 		
	Enable	Această căsuță va activa ori dezactiva funcția de pornire/oprire a monitorizării	Vă permite să controlați starea monitorizării prin SMS
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	Pornirea sau oprirea monitorizării
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, pornirea/oprirea monitorizării	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
20.	Monitoring status Stare monitorizare 		
	Enable	Această căsuță va activa ori dezactiva funcția de stare a monitorizării	Vă permite să obțineți starea monitorizării prin SMS
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, trimiterea stării monitorizării	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Lista albă a utilizatorilor permisi	From all numbers, From group sau From single number
21.	Interfața de programare a aplicațiilor (API) UCI		
	Enable	Această căsuță va activa ori dezactiva funcția API UCI	Vă permite să setați sau să obțineți orice configurații de pe router
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, setarea/trimiterea parametrilor routerului	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează

	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Listă albă a utilizatorilor permisi	From all numbers, From group sau From single number
22.	Switch output on / off Pornire/oprire ieșire 		
	Enable	Această căsuță va activa ori dezactiva funcția de pornire/oprire a ieșirii	Permite controlul ieșirii prin SMS
	Action	Acțiunea ce va fi efectuată când această regulă se aplică	Pornirea sau oprirea ieșirii
	Active timeout	Regulă activă pentru o anumită perioadă, format – secunde	
	SMS text	Textul SMS ce va declanșa aplicarea regulii. În acest caz, pornirea/oprirea ieșirii	Textul SMS-ului poate conține litere, cifre, spații și simboluri speciale. Literele mari contează
	Authorization method	Ce tip de autorizare va fi folosit pentru gestionarea SIM-urilor	No authorization, By serial sau By router admin password
	Allowed users	Listă albă a utilizatorilor permisi	From all numbers, From group sau From single number
	Output type Tip ieșire	Ce ieșire (ieșirea digitală cu colector în gol sau ieșirea releu) va fi activată	

Parametrii UCI prin SMS:

UCI vă permite să setați sau să obțineți orice parametru din fișierele de configurare ale routerului. Exemple de sintaxă:

1.	uci get config.section.option"	Obțineți valoarea opțiunii de configurare
2.	uci set config.section.option=value"	Setați opțiunea de configurare
3.	uci show config	Afișează fișierul de configurare
4.	uci show config.section	Afișează o anumită secțiune din fișierul de configurare (de ex.: uci show network.ppp.apn")

Note importante:

- Setările privind conexiunea de telefonie mobilă trebuie efectuate corect. Dacă cartela SIM are un PIN, trebuie să îl introduceți în "Network" > "3G" settings. În caz contrar funcția de repornire prin SMS nu va funcționa.
- Numărul de telefon al expeditorului trebuie să conțină codul de țară. Puteți verifica formatul numărului de telefon al expeditorului citind detaliile mesajelor SMS vechi de pe telefonul Dvs.

9.9.1.2 Reguli SMS personalizate

Pe lângă regulile implicite, puteți și să configurați reguli personalizate. Pentru aceasta, mergeți în partea inferioară a paginii SMS Utilities. Acolo veți găsi tab-ul **“New SMS Rule”** |Regulă SMS nouă|. Selectați o acțiune și apăsați butonul **“Add”** din dreptul acesteia.



Configurarea acestor reguli personalizate este identică cu configurarea regulilor implicite. În consecință, instrucțiunile din secțiunea de mai sus se aplică și aici.

9.9.2 Utilitate prin apel

La fel ca și utilitarele SMS, utilitarele prin apel vă oferă posibilitatea să emiteți anumite comenzi pentru router de pe telefonul Dvs. mobil. Lista regulilor posibile este, desigur, mai scurtă, deoarece puteți efectua doar un singur tip de apel. Țineți cont de acest lucru atunci când creați reguli pentru utilitate prin apel, deoarece un apel va declanșa simultan toate regulile activate.

Există o singură regulă implicită (Reboot) configurață, și este dezactivată. Pentru a crea o nouă regulă, dați clic pe butonul “Edit” din dreptul singurei reguli implicite (după cum se arată în exemplul de mai jos) sau creați o intrare complet nouă în lista Dvs. de reguli pentru apeluri prin adăugarea unei reguli în tab-ul **New Call Rule |Regulă apeluri nouă|**.

Call Utilities

Action	Enable	Sort
Reboot	<input type="checkbox"/>	



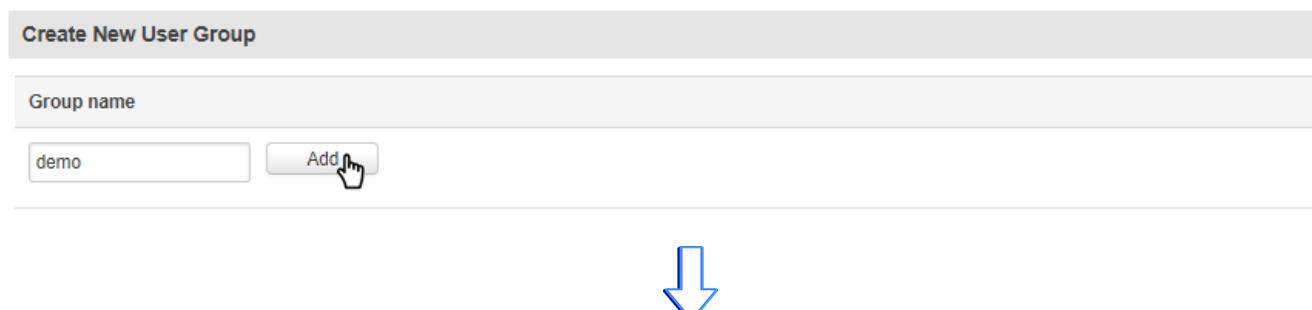
Call Configuration

Modify Call Rule	
Enable	<input type="checkbox"/>
Action	Reboot
Allowed users	From all numbers
Get status via SMS after reboot <input type="checkbox"/>	

	Nume câmp	Valori posibile	Explicație
1.	Enable	Bifat/Nebifat	Activează regula
2.	Action	Reboot / Get Status / Turn WiFi on/off / Turn mobile data on/off / Turn Output on/off	Acțiunea ce va fi efectuată după primirea unui apel
3.	Allowed users Utilizatori permisi	From all numbers / From group / From single number	Limităază declanșarea acțiunii. Dacă ați selectat From group De la grup , vi se va cere să selectați un Grup de utilizatori (informații privind configurarea grupurilor de utilizatori puteți găsi mai jos în secțiunea 9.9.3). Dacă ați selectat From single number De la un singur număr , vi se va cere să introduceți numărul expeditorului
4.	Get status via SMS after reboot	Bifat/Nebifat	Activează transmiterea automată a unui mesaj conținând informații despre starea routerului după repornire. Dacă bifăți, vi se va cere să introduceți numărul de telefon al destinatarului

9.9.3 Grupuri de utilizatori

Grupurile de utilizatori vă permit să grupați numere de telefon în scopul gestionării SMS-urilor. Ulterior puteți folosi aceste grupuri în cadrul tuturor funcțiilor relevante legate de SMS și de apeluri. Această opțiune este utilă în cazul în care există mai mulți utilizatori care ar trebui să aibă aceleași roluri atunci când gestionează routerul prin SMS sau prin apeluri. Puteți crea un grup nou de utilizatori introducând un nume în câmpul de text **Group name** și dând clic pe butonul “**Add**” alăturat din secțiunea “**Create New User Group**” |Creare grup utilizatori nou|. După aceasta, veți fi redirectionat la secțiunea “**Modify User Group**” |Modificare grup utilizatori|.



Create New User Group

Group name

demo

User Group Configuration

Modify User Group

Group name	<input type="text" value="demo"/>
Phone number	<input type="text" value="+37061111111"/> <input type="button" value="x"/>
	<input type="text" value="+37062222222"/> <input type="button" value="x"/>
	<input type="text" value="+37063333333"/> <input type="button" value="x"/> <input type="button" value="+"/>

[Back to Overview](#)

	Nume câmp	Valoare în exemplu	Explicație
1.	Group name	demo	Numele grupului de numere de telefon. Folosit pentru facilitarea gestionării
2.	Phone number	+37061111111, +37062222222, +37063333333	Adăugați numere de telefon la grupul de utilizatori. Trebuie respectat formatul internațional. Puteți adăuga mai multe câmpuri pentru numere de telefon dând clic pe simbolul “+” verde

9.9.4 Gestionarea SMS-urilor

Cu ajutorul tab-ului SMS Management |Gestionare SMS| puteți citi și trimite mesaje SMS.

9.9.4.1 Citirea SMS-urilor

În pagina Read SMS |Citire SMS| puteți citi și șterge mesajele SMS primite/memorate. Aspectul paginii este simplu, există o listă a mesajelor SMS primite și puteți alege câte intrări din această listă să fie vizibile simultan din lista autoderulantă **SMS per page** |SMS-uri pe pagină| din colțul stânga-sus al paginii, iar în colțul dreapta-sus al paginii există un câmp **Search** |Căutare| ce vă ajută să navigați mai eficient în lista de mesaje.

The screenshot shows the 'Read SMS' interface. At the top, there are three tabs: 'Read SMS' (selected), 'Send SMS', and 'Storage'. Below the tabs is a search bar labeled 'SMS Messages' with a dropdown for 'SMS per page' set to 10, and a 'Search' input field. The main area displays a table of messages with columns: Date, Sender, Message, and a checkbox column. One message is listed: '2017-09-22 09:13:06' from '+37065259965' with the message 'Hello'. At the bottom, it says 'Showing 1 to 1 of 1 entries' and has buttons for 'Refresh', 'Delete', and 'Select all'.

9.9.4.2 Trimiterea SMS-urilor

Pagina Send SMS |Trimitere SMS| vă permite să trimiteți mesaje SMS de pe cartela SIM a routerului.

Send SMS

The screenshot shows the 'Send SMS' page. It has a header 'Send SMS Message'. Below it, there are two input fields: 'Phone Number' containing '+37061111111' and 'Message' containing 'Hello'. A note below the message box says 'SMS 1 (155 characters left)'. At the bottom right is a 'Send' button.

Tot ce trebuie să faceți este să introduceți numărul de telefon al destinatarului, să tasteți mesajul și să apăsați butonul **"Send"**. Dacă totul a mers bine, ar trebui să apară o bară verde cu mesajul **"Message sent"** |Mesaj trimis|.

Message sent

9.9.4.3 Stocarea SMS-urilor

Tab-ul Storage |Stocare| vă arată cât spațiu de memorie este utilizat și cât este disponibil pe cartela SIM. De asemenea, puteți alege opțiunea ca routerul să nu șteargă mesajele. Dacă nu folosiți această opțiune, routerul va șterge automat toate mesajele primite, după ce au fost citite. Starea mesajului "read/unread" |citit/necitit| este examinată la fiecare 60 de secunde. Toate mesajele "citite" sunt șterse.

SMS Storing

Configuration

Save messages on SIM

SIM card memory Used:1 Available: 50

Leave free space

	Nume câmp	Valoare în exemplu	Explicație
1.	Save messages on SIM	Bifat/Nebifat	Activează salvarea pe cartela SIM a mesajelor primite
2.	SIM card memory	Used Folosită : 1 Available Disponibilă : 50	Informații despre memoria folosită/disponibilă pe cartela SIM
3.	Leave free space Lăsare spațiu liber	1	Câtă memorie (număr de mesaje) ar trebui lăsată liberă

9.9.5 Configurarea de la distanță

Routerul RUT955 poate fi configurat prin SMS de pe un alt router RUTxxx. Trebuie doar să selectați detaliile de configurare care trebuie trimise și să tastezi numărul de telefon al celuilalt router. Routerul va genera textul SMS necesar pentru ca configurațiile să fie aplicate.

Numărul total de SMS-uri este gestionat automat. Trebuie să cunoașteți numărul de SMS-uri posibil și să utilizați această caracteristică pe propria răspundere. În general, aceasta nu ar trebui folosită dacă trimiterea de SMS-uri este scumpă. Acest lucru este valabil în special dacă încercați să trimiteți o întreagă configurație OpenVPN, care poate cumula aproximativ 40 de mesaje SMS.

9.9.5.1 Primirea configurațiilor

Această secțiune controlează modul în care trebuie să se identifice partea care inițiază configurarea. În acest scenariu este configurat routerul RUT955 însuși.

Receive	Send
---------	------

Receive Configuration

Receive Configuration	
<input checked="" type="checkbox"/> Enable	
Authorization method <input style="border: 1px solid #ccc; padding: 2px;" type="button" value="By router admin password"/>	
Allowed users <input style="border: 1px solid #ccc; padding: 2px;" type="button" value="From all numbers"/>	

	Nume câmp	Valori	Note
1.	Enable	Bifat/Nebifat	Permite routerului să primească configurația
1.	Authorization method*	No authorization / By serial / By router admin password	Descrie tipul de autorizare folosit pentru gestionarea SMS-urilor. Metodele folosite de destinatar și de expeditor trebuie să fie identice
2.	Allowed users	From all numbers From group From single number	Căror numere le este permis să transmită configurații

*Țineți cont că, din motive de securitate, metoda de autorizare trebuie configurată înainte de utilizarea routerului.

9.9.5.2 Trimiterea configurațiilor

Această secțiune vă permite să configurați dispozitive RUTxxx de la distanță. Setările de autorizare trebuie să se potrivească cu cele stabilite pentru destinatar. Trimiterea unei configurații de rețea noi cu setări pentru WAN și LAN este prezentată cu titlu de exemplu mai jos.

Send Configuration

Setup Configuration Message

Network **VPN**

Generate SMS	New
WAN	<input checked="" type="checkbox"/>
Interface	Mobile
Primary SIM card	SIM1
Mobile connection	Use PPP mode
APN	gprs.fix-ip.omnitel1.net
Dialing number	*99#
Authentication method	CHAP
User name	admin
Password	*****
Service mode	3G preferred
LAN	<input checked="" type="checkbox"/>
IP address	192.168.1.1
IP netmask	255.255.255.0
IP broadcast	192.168.1.255

Send Message Settings

Phone number	+37061111111
Authorization method	By router admin password
Router admin password	admin01

Send

	Nume câmp	Valori	Note
Setările mesajului de configurare			
1.	Generate SMS Generare SMS	New Nou / From current configuration Cu configurația curentă	Generați noi setări sau folosiți configurația curentă a dispozitivului
2.	WAN	Bifat/Nebifat	Includefă configurații pentru rețeaua WAN
3.	Interface	Mobile / Wired Prin cablu	Tipul de interfață folosit pentru conexiunea WAN
4.	Primary SIM card	SIM1 / SIM2	Cartela SIM principală
5.	Mobile connection Conexiune mobilă	PPP / NDIS / NCM / QMI	Un agent de bază ce va fi folosit pentru crearea și gestionarea conexiunii mobile de date
6.	APN	Numele punctului de acces al operatorului	(APN) este numele unui gateway între o rețea mobilă GPRS ori 3G și o altă rețea de calculatoare, în mod frecvent internetul public
7.	Dialing number	*99#	Un număr de telefon ce va fi folosit pentru stabilirea unei conexiuni mobile prin PPP
8.	Authentication method	CHAP / PAP / None Niciuna	Selectați o metodă de autentificare ce va fi folosită pentru autentificarea noilor conexiuni în rețeaua furnizorului Dvs. GSM
9.	User name	“admin”	Numele de utilizator folosit pentru autentificare în rețeaua furnizorului Dvs. GSM
10.	Password	“•••••”	Parola folosită pentru autentificare în rețeaua furnizorului Dvs. GSM
11.	Service mode Mod serviciu	Auto 4G (LTE) only 3G only 2G only	Preferința Dvs. pentru rețea. Dacă rețeaua locală de telefonie mobilă suportă GSM (2G), UMTS (3G) ori LTE (4G), puteți specifica la care rețea preferați să vă conectați
12.	LAN	Activare/Dezactivare	Includefă configurații pentru LAN
13.	IP address	“192.168.1.1”	Adresa IP pe care o va folosi în LAN routerul de la distanță
14.	IP netmask	“255.255.255.0”	O mască de subrețea pe care o va folosi routerul de la distanță pentru a defini dimensiunea rețelei LAN
15.	IP broadcast	“192.168.1.255”	O adresă logică la care pot primi datagrame toate dispozitivele conectate la o rețea de comunicații cu acces multiplu
Setări pentru trimiterea mesajului			
16.	Phone number	“+37061111111”	Numărul de telefon al routerului care va primi configurația
17.	Authorization method	No authorization By serial By router admin password	Ce tip de autorizare va fi folosit pentru configuraarea de la distanță

Acesta este un exemplu de scenariu, dar puteți trimite și alte setări pentru rețea și VPN. Setările trimise sunt identice cu cele pe care le-ați configura local pe routerul Dvs., deci puteți găsi informații despre funcțiile diferențiale parametri de rețea și VPN în secțiunile [7](#) și [9.7](#) ale acestui document.

9.9.6 Statistici

Pagina Statistics | Statistici prezintă numărul de mesaje SMS trimise și primite.

Statistics

SMS Statistics			
SIM Card	Sent SMS	Received SMS	
SIM 1	4	1	<button>Reset</button>
SIM 2	0	0	<button>Reset</button>

9.10 SNMP

Simple Network Management Protocol (SNMP) este un protocol des folosit pentru administrarea rețelelor. Este folosit pentru colectarea de informații de la dispozitivele din rețea și la configurarea acestora.

9.10.1 Setări SNMP

SNMP Configuration

SNMP Service Settings

Enable SNMP service	<input type="checkbox"/>
Enable remote access	<input type="checkbox"/>
Port	161
Community	Public ▾
Location	Location
Contact	email@example.com
Name	Name

	Nume câmp	Valori posibile	Explicație
1.	Enable SNMP service	Bifat/Nebifat	Lansați serviciul SNMP la pornirea sistemului
2.	Enable remote access Activare acces la distanță	Bifat/Nebifat	Deschideți un port în firewall astfel încât serviciul SNMP să poată fi accesat din WAN
3.	Port	0 – 65535	Portul serviciului SNMP
4.	Community Comunitate	Public / Private / Custom	Comunitatea SNMP este un identificator ce permite accesul la datele SNMP ale routerului
6.	Location	Locație	Capcana denumită sysLocation
7.	Contact	Adresă de e-mail	Capcana denumită sysContact
8.	Name	Orice nume	Capcana denumită sysName

Variabile SNMP/OID identificatoare de obiecte (OID)

	OID	Descriere
1.	1.3.6.1.4.1.99999.1.1.1	Modem IMEI-ul modemului
2.	1.3.6.1.4.1.99999.1.1.2	Modelul modemului
3.	1.3.6.1.4.1.99999.1.1.3	Producătorul modemului
4.	1.3.6.1.4.1.99999.1.1.4	Revizia modemului
5.	1.3.6.1.4.1.99999.1.1.5	Numărul de serie al modemului
6.	1.3.6.1.4.1.99999.1.1.6	Starea cartelei SIM
7.	1.3.6.1.4.1.99999.1.1.7	Starea codului PIN
8.	1.3.6.1.4.1.99999.1.1.8	IMSI
9.	1.3.6.1.4.1.99999.1.1.9	Starea înregistrării în rețeaua de telefonie mobilă
10.	1.3.6.1.4.1.99999.1.1.10	Nivelul semnalului
11.	1.3.6.1.4.1.99999.1.1.11	Operatorul folosit la momentul respectiv
12.	1.3.6.1.4.1.99999.1.1.12	Numărul operatorului (MCC+MNC)
13.	1.3.6.1.4.1.99999.1.1.13	Starea conексiunii sesiunii de date
14.	1.3.6.1.4.1.99999.1.1.14	Tipul conексiunii sesiunii de date
15.	1.3.6.1.4.1.99999.1.1.15	Capcana intensitate semnal
16.	1.3.6.1.4.1.99999.1.1.16	Capcana tip de conexiune

9.10.2 Setări TRAP

Trap Configuration

Trap Service Settings

SNMP Trap

Host/IP

Port

Community

Trap Rules

Action	Enable
Signal strength trap	<input type="checkbox"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Connection type trap	<input type="checkbox"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

New Trap Rule

Action

	Nume câmp	Valori posibile	Explicație
1.	SNMP Trap	Bifat/Nebifat	Activează funcția capcane SNMP
2.	Host/IP	Adresa IP sau nume de gazdă	Gazda unde va fi transferat traficul SNMP
3.	Port	0 – 65535	Port pentru gazda capcanei
4.	Community	Public/Private	Comunitatea SNMP este un identificator ce permite accesul la datele SNMP ale routerului

9.11 Gateway SMS

9.11.1 Configurarea metodelor POST/GET

Pagina POST/GET Configuration |Configurare POST/GET| vă permite să efectuați cereri de acțiuni prin scrierea lor în URL după adresa IP a dispozitivului Dvs.

Post/Get Configuration

SMS Post/Get Settings

Enable	<input checked="" type="checkbox"/>
User name	user1
Password

	Nume câmp	Valori posibile	Note
1.	Enable	Bifat/Nebifat	Activăți funcția de gestionare a SMS-urilor prin intermediul POST/GET
2.	User name	Orice nume de utilizator	Numele de utilizator folosit pentru autorizare
3.	Password	Orice parolă	Parola folosită pentru autorizare (valoare implicită: user1)

Nu uitați să modificați parametrii în URL conform configurației POST/GET!

9.11.1.1 SMS prin HTTP – metodele POST/GET

Puteți să citiți și să trimiteți SMS-uri utilizând o sintaxă HTTP POST / GET validă. Folosiți un browser web sau orice alt software compatibil pentru a trimite routerului șiruri HTTP POST / GET. Routerul trebuie să fie conectat la o rețea GSM atunci când utilizează funcția de trimitere SMS.

	Acțiune	Exemplu de URL POST/GET
1.	Vizualizarea listei de SMS-uri	/cgi-bin/sms_list?username=admin&password=admin01
2.	Citire SMS	/cgi-bin/sms_read?username=admin&password=admin01&number=1
3.	Trimitere SMS-uri	/cgi-bin/sms_send?username=admin&password=admin01&number=0037060000001&text=testmessage
4.	Vizualizarea numărului total de SMS-uri	/cgi-bin/sms_total?username=admin&password=admin01
5.	Ștergere SMS	/cgi-bin/sms_delete?username=admin&password=admin01&number=1

9.11.1.2 Sintaxa șirului HTTP POST/GET

Șirul HTTP POST/GET		Explicație
http://{ADRESĂ_IP}	/cgi-bin/sms_read? username={numele_dvs_de_utilizator}&password={parola_dvs}&number={INDEX_MESAJ}	Citire mesaj
	/cgi-bin/sms_send? username={numele_dvs_de_utilizator}&password={parola_dvs}&number={NUMĂR_TELEFON}&text={TEXT_MESAJ}	Trimitere mesaj
	/cgi-bin/sms_delete? username={numele_dvs_de_utilizator}&password={parola_dvs}&number={INDEX_MESAJ}	Ștergere mesaj
	/cgi-bin/sms_list? username={numele_dvs_de_utilizator}&password={parola_dvs}	Listarea tuturor mesajelor
	/cgi-bin/sms_total? username={numele_dvs_de_utilizator}&password={parola_dvs}	Numărul de mesaje în memorie

Notă: parametrii șirurilor HTTP POST/GET sunt scriși cu litere mari între acolade. Acoladele ("{ }") nu sunt necesare când trimiteți șirul HTTP POST/GET.

9.11.1.3 Parametrii șirului HTTP POST/GET

	Parametru	Explicație
1.	ADRESĂ_IP	Adresa IP a routerului Dvs.
2.	INDEX_MESAJ	Numărul de ordine al SMS-ului în memorie
3.	NUMĂR_TELEFON	Numărul de telefon al destinatarului mesajului. Notă: Numărul de telefon trebuie să conțină prefixul de țară. Formatul numărului de telefon: 00{COD_ȚARĂ} {NUMĂR_DESTINATAR}. De ex.: 0037062312345 (370 este codul de țară și 62312345 este numărul de telefon al destinatarului)
4.	TEXT_MESAJ	Textul mesajului SMS. Notă: Nr. maxim de caractere per SMS este 160. Nu puteți trimite mesaje mai lungi. Se recomandă să folosiți numai caractere alfanumerice

După fiecare comandă executată routerul va răspunde comunicând starea.

9.11.1.4 Răspunsuri posibile după executarea comenziilor

	Response	Explicație
1.	OK	Comandă executată cu succes
2.	ERROR Eroare	S-a produs o eroare în cursul executării comenzi
3.	TIMEOUT Expirare durată	Nu s-a primit niciun răspuns de la modul
4.	WRONG_NUMBER Număr greșit	Formatul numărului destinatarului SMS-ului este incorrect sau numărul de ordine al SMS-ului este incorrect
5.	NO MESSAGE Niciun mesaj	În memorie nu există niciun mesaj cu numărul de ordine specificat
6.	NO MESSAGES Fără mesaje	În memorie nu sunt stocate mesaje

9.11.1.5 Exemple de șiruri HTTP POST/GET

http://192.168.1.1/cgi-bin/sms_read?username=admin&password=admin01&number=2

http://192.168.1.1/cgi-bin/sms_send?username=admin&password=admin01&number=0037060000001&text=message

http://192.168.1.1/cgi-bin/sms_delete?username=admin&password=admin01&number=4

http://192.168.1.1 /cgi-bin/sms_list?username=admin&password=admin01

9.11.2 E-mail prin SMS

Funcția E-mail to SMS |E-mail prin SMS| vă verifică inbox-ul de e-mail după o perioadă de timp specificată și, dacă există mesaje noi primite, le convertește în mesaje SMS.

POP3 Email To SMS Configuration

Email To SMS Settings

Enable

POP3 server

Server port

User name

Password 

Secure connection (SSL)

Check email every Minutes

	Nume câmp	Valori	Note
1.	Enable	Bifat/Nebifat	Permite convertirea e-mailurilor primite în SMS-uri
2.	POP3 server	“pop.gmail.com”	Adresa serverului POP3
3.	Server port	0 – 65535	Portul de autentificare al serverului
4.	User name	Orice nume de utilizator	Numele de utilizator al contului Dvs. de e-mail
5.	Password	Orice parolă	Parola contului Dvs. de e-mail
6.	Secure connection (SSL)	Bifat/Nebifat	SSL este un protocol pentru transmiterea documentelor private prin internet. SSL folosește un sistem criptografic care utilizează două chei pentru a cripta datele – o cheie publică cunoscută tuturor și o cheie privată sau secretă cunoscută numai destinatarului mesajului
7.	Check e-mail every Verificare e-mail la fiecare	Minutes Minute Hours Ore Days Zile	Perioada de verificare a inbox-ului

9.11.3 Mesaje programate

Mesajele programate vă permit să trimiteți periodic mesaje SMS către un număr specificat. Mesajele programate sunt gestionate prin reguli, similar cu raportarea evenimentelor, utilitarele SMS etc. De aceea, pentru a configura un nou mesaj programat, trebuie mai întâi creată o regulă. Pentru a crea o nouă regulă, tastați un număr de telefon în câmpul **Phone number** din secțiunea “Scheduled Messages Configuration” | Configurare mesaje programate și apăsați pe butonul “Add” | Adăugare| alăturat.

The screenshot shows the 'Scheduled Messages Configuration' section. A yellow box highlights the 'Phone number' field containing '+37061111111'. To its right is a dropdown menu set to 'Day'. Below these is a large 'Add' button with a hand cursor icon. A blue arrow points downwards from this section to the 'Messages To Send' section below.

Recipients number	Sending Interval	Enable	Sort
+37061111111	day	<input type="checkbox"/>	

După aceasta, noua dvs. regulă va apărea în secțiunea “Messages To Send” | Mesaje de trimis|. În afară de numărul de telefon, noua regulă va fi dezactivată și neconfigurată. Pentru a vă configura regula, dați clic pe butonul “Edit” din dreptul acesteia, aşa cum se arată în exemplul de mai sus.

9.11.3.1 Configurarea mesajelor programate

Scheduled Messages Configuration

The screenshot shows the 'Modify scheduled message' dialog. It includes fields for 'Recipient's phone number' (+37061111111), 'Message text' (Hello), and a character count indicator 'SMS 1 (155 characters left)'. Below these are dropdown menus for 'Message sending Interval' (set to 'Day'), 'Hour' (12), and 'Minute' (45).

	Nume câmp	Valori posibile	Note
1.	Enable	Bifat/Nebifat	Activează trimitera periodică de mesaje
2.	Recipient's phone number Număr telefon destinatar	Orice număr de telefon	Numărul de telefon care va primi mesajele programate
3.	Message text	Orice text	Mesajul care va fi trimis
4.	Message sending interval Interval trimitere mesaje	Day Zi / Week Săptămână / Month Lună / Year An	Perioada dintre mesajele trimise

9.11.4 Răspuns automat

Funcția Auto reply vă permite să configurați răspunsul automat la mesajele SMS primite de router de la oricine ori doar de la numerele din listă.

Auto Reply Configuration

Reply Configuration

Enable

Reply SMS-Utilities rules

Don't save received message

Mode

Message

Recipient's phone number

	Nume câmp	Valori	Note
1.	Enable	Bifat/Nebifat	Activări răspunsul automat la fiecare SMS primit
2.	Reply SMS-Utilities rules	Bifat/Nebifat	Dacă bifați, routerul va răspunde automat și la regulile utilitarelor SMS
3.	Don't save received message	Bifat/Nebifat	Dacă bifați, mesajele primite nu vor fi salvate
4.	Mode	Everyone Oricine / Listed numbers Numere listate	Selectați care mesaje vor primi răspuns automat. Fie toate mesajele, fie cele de la numerele specificate
5.	Message	Orice mesaj text	Textul mesajului de răspuns
6.	Recipient's phone number	Orice număr de telefon	Numerele de telefon la care va fi trimis răspunsul automat

9.11.5 Forwardarea SMS-urilor

9.11.5.1 Forwardarea SMS-urilor prin HTTP

Funcția SMS Forwarding To HTTP forwardează mesajele SMS prin HTTP, folosind fie metoda POST, fie GET.

SMS Forwarding To HTTP Configuration

SMS Forwarding To HTTP Settings

Enable

Forward SMS-Utilities rules

Use HTTPS

Method

URL

Number value name

Message value name

Extra data pair 1

Extra data pair 2

Mode

Sender's phone number(s)

	Nume câmp	Valori posibile	Note
1.	Enable	Bifat/Nebifat	Activăți forwardarea SMS-urilor prin HTTP
2.	Forward SMS-Utilities rules	Bifat/Nebifat	Dacă bifăți, routerul va forwarda prin HTTP și utilitarele SMS
3.	Use HTTPS	Bifați/Nebifați	Bifați pentru a folosi HTTPS
4.	Method	Post / Get	Definește metoda de transfer HTTP
5.	URL	192.168.99.250/getpost/index.php	Adresa URL către care vor fi forwardate mesajele
6.	Number value name Nume valoare număr	Orice nume	Numele ce va fi alocat valorii numărului de telefon al expeditorului în sirul de interogare
7.	Message value name Nume valoare mesaj	Orice text	Numele ce va fi alocat valorii textului mesajului în sirul de interogare
8.	Extra data pair 1 Pereche date suplimentare 1	Var1 – 17	Dacă dorîți să transferați informații suplimentare prin cererea HTTP, introduceți numele variabilei în câmpul din stânga și valoarea acesteia în dreapta
9.	Extra data pair 2	Var2 – “go”	
10.	Mode	All messages Toate mesajele / From listed numbers De la numerele listate	Specifică expeditorul mesajelor ce vor fi forwardate
11.	Sender's phone number(s)	Orice număr/numere de telefon	Specifică numerele de telefon care au trimis mesajele SMS ce vor fi forwardate

9.11.5.2 Forwardarea SMS-urilor prin SMS

Funcția SMS Forwarding To SMS forwardează mesajele SMS către unul sau mai mulți destinatari.

SMS Forwarding To SMS Configuration

SMS Forwarding To SMS Settings

Enable

Forward SMS-Utilities rules

Add sender number

Mode

Sender's phone number(s)

recipients phone numbers

	Nume câmp	Valori	Note
1.	Enable	Bifat/Nebifat	Activăți forwardarea SMS-urilor
2.	Forward SMS-Utilities rules	Bifat/Nebifat	Dacă bifați, routerul va forwarda prin SMS și utilitarele SMS
3.	Add sender number Adăugare număr expeditor	Bifat/Nebifat	Dacă bifați, numărul expeditorului inițial va fi adăugat la sfârșitul mesajului forwardat
4.	Mode	All messages / From listed numbers	Specifică expeditorii mesajelor primite ce vor fi forwardate
5.	Sender's phone numbers(s)	Orice număr/numere de telefon	Specifică numerele de telefon care au trimis mesajele SMS ce vor fi forwardate
6.	Recipient's phone numbers	Orice număr/numere de telefon	Numerele de telefon la care vor fi forwardate mesajele SMS

9.11.5.3 Forwardarea SMS-urilor prin e-mail

Funcția SMS Forwarding To Email forwardează mesajele SMS prin e-mail.

SMS Forwarding To Email Configuration

SMS Forwarding To Email Settings

Enable <input checked="" type="checkbox"/>
Forward SMS-Utilities rules <input checked="" type="checkbox"/>
Add sender's number <input checked="" type="checkbox"/>
Subject <input type="text" value="forwarded message"/>
SMTP server <input type="text" value="mail.gmail.com"/>
SMTP server port <input type="text" value="995"/>
Secure connection <input checked="" type="checkbox"/>
User name <input type="text" value="gmail@gmail.com"/>
Password <input type="password" value="emailpwd"/>
Sender's email address <input type="text" value="gmail@gmail.com"/>
Recipient's email address <input type="text" value="gmail2@gmail.com"/>
Mode <input type="button" value="From listed numbers"/>
Sender's phone number(s) <input type="text"/>

	Nume câmp	Valori posibile	Explicație
1.	Enable	Bifat/Nebifat	Activăți forwardarea SMS-urilor prin e-mail
2.	Forward SMS-Utilities rules	Bifat/Nebifat	Dacă bifați, routerul va forwarda prin e-mail și utilitarele SMS
3.	Add sender number	Bifat/Nebifat	Dacă bifați, numărul expeditorului inițial va fi adăugat la sfârșitul mesajului forwardat
4.	Subject	Orice text	Textul ce va fi introdus în câmpul subiectului e-mailului
5.	SMTP server	"mail.teltonika.lt"	Adresa serverului Dvs. SMTP
6.	SMTP server port	0 – 65535	Numărul portului serverului Dvs. SMTP
7.	Secure connection	Bifat/Nebifat	Activează utilizarea protocolelor criptografice. Activăți numai dacă serverul Dvs. SMTP suportă SSL ori TLS
7.	User name	Orice nume de utilizator	Numele de logare al contului Dvs. de e-mail
8.	Password	Orice parolă	Parola contului Dvs. de e-mail
9.	Sender's email address	Orice adresă de e-mail	Adresa Dvs. de la care vor fi trimise e-mailurile
10.	Recipient's email address	Orice adresă de e-mail	Adresa către care dorîți să vă forwardați mesajele
11.	Mode	All messages / From listed numbers	Specificați expeditorii mesajelor ce vor fi forwardate prin e-mail
12.	Sender's phone number(s)	Orice număr/numere de telefon	Specifică numerele de telefon care au trimis mesajele SMS ce vor fi forwardate

9.11.6 SMPP

Short Message Peer-to-Peer (SMPP) este un protocol folosit pentru schimbul de mesaje SMS între centre SMS (SMSC) și/sau entități (ESME)

SMPP Server Configuration

Transmitter Configuration

Enable	<input checked="" type="checkbox"/>
User name	admin
Password	password 
Server port	7777

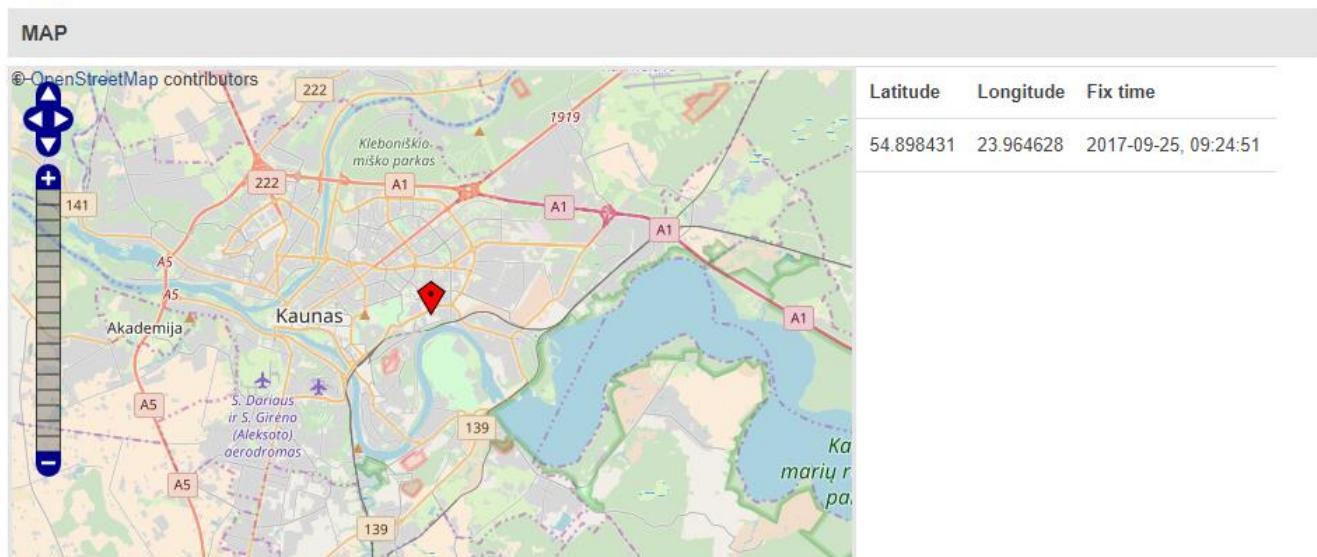
	Nume câmp	Valori	Explicație
1.	Enable	Bifat/Nebifat	Activează serverul SMPP
2.	User name	Orice nume de utilizator	Numele de utilizator pentru autentificarea pe serverul SMPP
3.	Password	Orice parolă	Parola pentru autentificarea pe serverul SMPP
4.	Server port	0 – 65535	Un port ce va fi folosit pentru comunicațiile serverului SMPP

9.12 GPS

9.12.1 GPS

Fereastra GPS afișează coordonatele Dvs. curente și poziția pe hartă.

GPS



9.12.2 Setări GPS

Aceasta este fereastra de configurare a parametrilor GPS.

GPS Configuration

GPS Settings

Enable GPS service

Enable GPS Data to server

Remote host/IP address:

Port:

Protocol:

	Nume câmp	Valori	Note
1.	Enable GPS service	Bifat/Nebifat	Activează funcția GPS
2.	Enable GPS Data to server	Bifat/Nebifat	Activează transferul automat al datelor GPS către un server la distanță
3.	Remote host / IP address	Orice adresă IP sau nume de domeniu către care vor fi trimise coordonatele	Adresa IP a serverului sau numele de domeniu către care vor fi trimise coordonatele
4.	Port	0 – 65535	Portul serverului folosit pentru transferul datelor
5.	Protocol	TCP / UDP	Protocol ce va fi folosit pentru transferul datelor către server

9.12.2.1 Setări TAVL

TAVL Settings

Send GSM signal Send analog input Send digital input (1) Send digital input (2)

	Nume câmp	Valori	Note
1.	Send GSM signal Trimitere semnal GSM	Bifat/Nebifat	Bifați pentru a include informații despre intensitatea semnalului GSM în pachetul de date GPS ce va fi trimis serverului
2.	Send analog input Trimitere intrare analogică	Bifat/Nebifat	Bifați pentru a include starea intrării analogice în pachetul de date GPS ce va fi trimis serverului
3.	Send digital input Trimitere intrare digitală (1)	Bifat/Nebifat	Bifați pentru a include starea intrării digitale #1 în pachetul de date GPS ce va fi trimis serverului
4.	Send digital input (2)	Bifat/Nebifat	Bifați pentru a include starea intrării digitale #2 în pachetul de date GPS ce va fi trimis serverului

9.12.3 Mod GPS

Gps Mode Configuration

Data sending parameters

Min period	5
Min distance	200
Min angle	30
Min saved records	20
Send period	60

Rules

Wan	Type	Digital isolated input	Min period	Min saved records	Send period	Enable	Sort
Mobile	Home	Low	5	20	60	<input checked="" type="checkbox"/>	

GPS Configuration

Wan	Type	Digital Isolated Input
-----	------	------------------------

Mobile ▾ Home ▾ Low ▾ Add

Transmiterea datelor

	Nume câmp	Valoare în exemplu	Note
1.	Min period	5	Perioada minimă (în secunde) pentru colectarea datelor
2.	Min distance Distanță minimă	200	Distanța minimă (în metri) între ultimele coordonate înregistrate și coordonatele curente pentru colectarea datelor (chiar dacă perioada specificată nu a trecut încă)
3.	Min angle Unghi minim	30	Diferența angulară minimă între ultimele coordonate înregistrate și coordonatele curente pentru colectarea datelor (chiar dacă perioada specificată nu a trecut încă)
4.	Min saved records Nr. min. înregistrări salvate	20	Volumul minim de coordonate înregistrate ce va fi trimis imediat către server (chiar dacă perioada de trimitere specificată nu a trecut încă)
5.	Send period	60	Perioada pentru trimiterea datelor colectate către server

Rules | Reguli|

Acest tabel conține regulile create pentru trimiterea datelor GPS.

Configurarea GPS

Secțiunea GPS Configuration permite salvarea mai multor configurații pentru colectarea datelor GPS. Configurația activă este selectată automat când sunt îndeplinite condițiile configurate.

	Nume câmp	Valori	Note
1.	WAN	Mobile / Wired / WiFi	Interfața ce trebuie folosită pentru activarea acestei configurații
2.	Type	Home / Roaming / Both	Starea conexiunii la rețeaua de telefonie mobilă necesară pentru activarea acestei configurații
3.	Digital Isolated Input Intrare digitală izolată	Low Nivel logic 0 / High Nivel logic 1 / Both Ambele	Starea intrării necesară pentru activarea acestei configurații

9.12.4 Intrările și ieșirile GPS

Fereastra GPS I/O |Intrări/ieșiri GPS| vă permite să setați reguli pentru intrările GPS. Pentru a crea o nouă regulă pentru intrări selectați tipul de intrare – **Input type** – și declanșatorul – **Trigger** –, ce pot fi găsite ambele în secțiunea **GPS Input Configuration** |Configurare intrări GPS|, apoi dați clic pe butonul **Add**.

GPS Input Configuration

Input type	Trigger
Digital	Input open

Add

Input Rules

Input	Priority	Generate event	Enable	Sort
Digital input	Low	Input open	<input checked="" type="checkbox"/>	

Edit

Se va crea o regulă pentru intrări nouă și neconfigurată. Pentru a configura apăsați butonul **Edit** din dreptul regulii nou-create.

GPS Data Configuration

Enable	<input checked="" type="checkbox"/>
Input type	Digital
Trigger	Input open
Priority	Low

	Nume câmp	Valori	Note
1.	Enable	Bifat/Nebifat	Activează regula
2.	Input Type	Digital / Digital isolated / Analog	Căruia tip de intrare i se va aplica regula
3.	Trigger	Input open Intrare deschisă / Input shorted Intrare scurtcircuitată / Both Ambele	Evenimentul declanșator pentru configurația dorită
4.	Priority Prioritate	Low / High / Panic Scăzută/Ridicată/Panică	Setările de prioritate diferite adaugă flag-uri de prioritate diferite pachetelor evenimentului, și acestea pot fi afișate diferit

9.12.5 Geofencing prin GPS

The screenshot shows the 'GPS Geofencing' configuration page. At the top, there are tabs for GPS, GPS Settings, GPS Mode, GPS I/O, and GPS Geofencing (which is currently selected). Below the tabs, there's a section titled 'Geofencing' with an 'Enable' checkbox. Underneath are input fields for 'Longitude (X)' (0.000000), 'Latitude (Y)' (0.000000), and 'Radius' (200). Below these fields are two buttons: 'Get current coordinates' and 'Get'. To the right of these buttons is a map preview showing a circular geofence centered at the specified coordinates with a radius 'r'.

Geofencing este o funcție ce poate detecta toate dățile în care un dispozitiv intră în sau ieșe din zona definită.

	Nume câmp	Note
1.	Enable	Activăți/dezactivați funcția de geofencing GPS
2.	Longitude (X)	Longitudinea punctului selectat
3.	Latitude (Y)	Latitudinea punctului selectat
4.	Radius	Raza zonei selectate
5	Get current coordinates	Obțineți coordonatele curente ale dispozitivului prin GPS

Pentru a primi un SMS or e-mail în cazul intrării în sau ieșirii din zona de geofencing, accesați Status -> Events Log -> Events reporting și configurați tipul de eveniment GPS!

9.13 Hotspot

Hotspot-ul wireless oferă funcționalități esențiale pentru gestionarea unei rețele wireless cu acces deschis. Pe lângă autentificarea standard pe serverul RADIUS, există și posibilitatea de colectare și de încărcare a unor jurnale detaliate ale acțiunilor efectuate de fiecare dispozitiv (determinat printr-o adresă MAC) în rețea (ce site-uri au fost traversate etc.).

9.13.1 Setări generale

9.13.1.1 Setări principale

Wireless Hotspot Configuration

General Settings

Main Settings **Session Settings**

Enable

AP IP: 192.168.2.254/24

Authentication mode: Without radius

External landing page:

Landing page address:

Protocol: HTTP

HTTPS redirect:

Users Configuration

User name	Password	Idle timeout	Session timeout	Download bandwidth	Upload bandwidth
There are no users created yet.					
Username	Password	<input type="text"/> <input type="password"/> <input type="button" value="Add"/>			

	Nume câmp	Explicație
1.	Enabled	Bifați pentru a activa pe router funcția de hotspot.
2.	AP IP	Adresa IP a punctului de acces. Aceasta va fi adresa routerului din rețeaua hotspot. Routerul va crea automat o rețea în funcție de propriul IP și de numărul CIDR pe care îl specificați după slash. De exemplu, "192.168.2.254/24" înseamnă că routerul va crea o rețea cu adresa IP 192.168.182.0 și masca de rețea 255.255.255.0 în scopul explicit de a include toți clienții wireless. O astfel de rețea va putea avea 253 de clienți (adresele IP le vor fi atribuite automat în intervalul de 192.168.2.1 la 192.168.2.253)

Mod autentificare: External radius | Server RADIUS extern|

1.	Radius server #1	Adresa IP a serverului RADIUS ce va fi folosit pentru autentificarea clientilor Dvs. wireless
2.	Radius server #2	Adresa IP a celui de-al doilea server RADIUS
3.	Authentication port	Portul de autentificare al serverului RADIUS
4.	Accounting port	Portul de contabilizare al serverului RADIUS

5.	Radius secret key	Cheia secretă folosită pentru autentificarea pe serverul RADIUS
6.	UAM port	Portul pentru autentificarea clientilor
7.	UAM UI port	Portul interfeței cu utilizatorul UAM
8.	UAM secret	Secretul partajat între serverul UAM și hotspot
9.	NAS Identifier	Identifierul serverului de acces la rețea
10.	Swap octets	Interschimbați sensul octetilor de intrare și de ieșire în legătură cu atributele RADIUS
11.	Location name	Numele locației

Mod autentificare: Internal radius |Server RADIUS intern|/Without radius |Fără server RADIUS|

1.	External landing page	Activează utilizarea paginii de destinație externe
2.	Landing page address	Adresa paginii de destinație externe
3.	HTTPS redirect	Redirectionează paginile HTTP către pagina de destinație

Mod autentificare: SMS OTP**9.13.1.2 Setări pentru sesiune**

Wireless Hotspot Configuration

General Settings

Main Settings Session Settings

Logout address 1.1.1.1

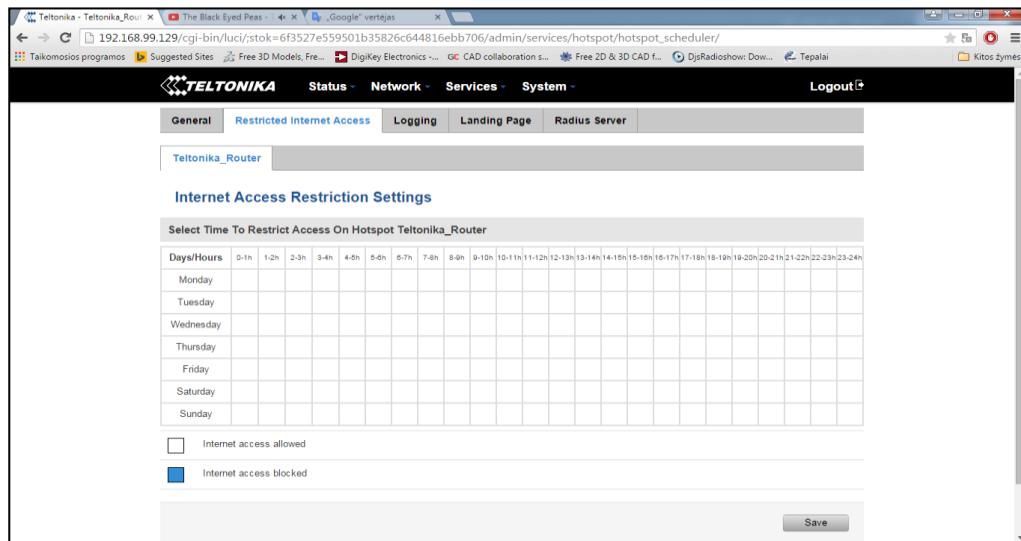
List Of Addresses The Client Can Access Without First Authenticating

Enable	Address	Port	Allow subdomains	
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Delete
Add				

	Nume câmp	Explicație
1.	Logout address Adresă delegare	Adresa IP pentru delegarea instantanee a unui client care o adresează
2.	Enable	Activăți accesarea adresei fără autentificare prealabilă
3.	Address	Numele de domeniu, adresa IP sau segmentul de rețea
4.	Port	Numărul portului
5.	Allow subdomains	Activăți/dezactivați subdomeniile

9.13.2 Setări de restricționare a accesului la internet

Permit dezactivarea accesului la internet într-o zi și la o oră specificate din fiecare săptămână.



9.13.3 Jurnalizarea

9.13.3.1 Configurare

This screenshot shows the 'Wireless Hotspot Logging Settings' page. It includes a 'Logging To FTP Settings' section with the following fields: 'Enable' (checkbox checked), 'Server address' (text input: 'your.ftp.server'), 'User name' (text input: 'username'), 'Password' (text input: '*****' with a visibility icon), and 'Port' (text input: '21').

	Nume câmp	Explicație
1.	Enable	Bifați această casetă dacă doriți să activați jurnalizarea traficului wireless. Această funcție va crea jurnale care conțin date despre site-urile pe care le-a vizitat fiecare client pe durata conectării la hotspotul Dvs.
2.	Server address	Adresa IP a serverului FTP unde doriți să fie încărcate jurnalele
3.	Username	Numele de utilizator al utilizatorului serverului FTP sus-menționat
4.	Password	Parola utilizatorului
5.	Port	Portul TCP/IP al serverului FTP

FTP Upload Settings

You can configure your timing settings for the log upload via FTP feature here.

Mode	Fixed
Hours	8
Minutes	15
Days	<input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday <input type="checkbox"/> Sunday

	Nume câmp	Explicație
1.	Mode	Modul programului. Utilizați opțiunea "Fixed" Fix dacă doriți ca încărcarea să se realizeze la o anumită oră a zilei. Utilizați "Interval" dacă doriți ca încărcarea să se facă la un interval fix
2.	Interval	Se afișează numai când modul este setat ca interval. Specifică intervalul încărcărilor obișnuite într-o anumită zi. De exemplu, dacă alegeti 4 ore, încărcarea se va face la miezul noptii, la 4:00, 8:00, 12:00, 16:00 și 20:00
3.	Days	Încărcarea va fi efectuată numai în aceste zile
4.	Hours, Minutes	Se afișează numai când modul este setat ca fix. Încărcarea se va face la acel moment al zilei. De exemplu, dacă doriți să vă încărcați jurnalele la 6:48, va trebui doar să introduceți Hours: 6 și Minutes: 48

9.13.3.2 Jurnalul

Configuration Log

Wifi Log

Wifi Log

Events per page	10	Search
-----------------	----	--------

MAC	IP	Port	Date	Time
-----	----	------	------	------

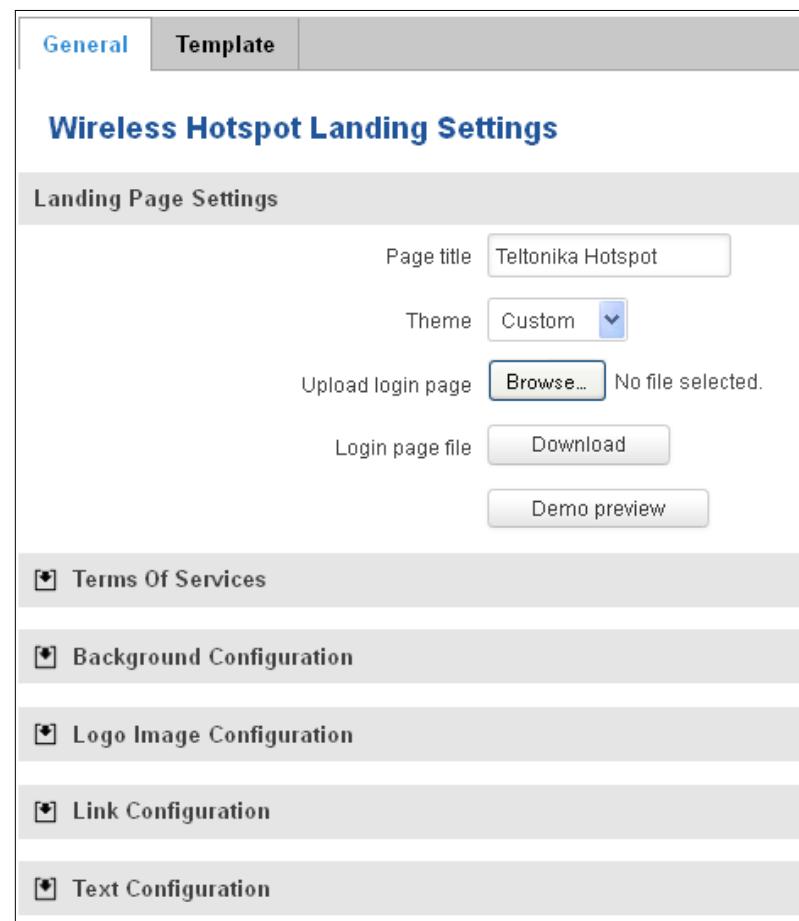
There are no records yet.

Showing 1 to 1 of 1 entries

9.13.4 Pagina de destinație

9.13.4.1 Setări generale pentru pagina de destinație

Cu ajutorul acestei funcții puteți personaliza pagina de destinație a hotspotului Dvs.



Nume câmp	Explicație
1. Page title	Va fi văzut ca titlul paginii de destinație
2. Theme Temă	Selectarea temei paginii de destinație
3. Upload login page Încărcare pagină logare	Permite încărcarea unei teme personalizate a paginii de destinație
4. Login page file Fișier pagină logare	Permite descărcarea și salvarea fișierului paginii Dvs. de destinație

În secțiunile “Terms Of Services” |Termeni servicii|, “Background Configuration” |Configurare fundal|, “Logo Image Configuration” |Configurare logo|, “Link Configuration” |Configurare link|, “Text Configuration” |Configurare text| puteți particulariza diversi parametri ai componentelor paginii de destinație.

9.13.4.2 Şablon

În această pagină –Template– puteți să revedeți codul HTML al paginii de destinație și să îl modificați.

The screenshot shows a web-based configuration interface for a landing page template. At the top, there are two tabs: "General" and "Template". The "Template" tab is currently selected, indicated by a blue background and white text. Below the tabs, the title "Landing Page Template Editor" is displayed in a bold, dark blue font. A sub-instruction "Modify login page template by your needs" is present. The main area is a code editor containing the following HTML and CSS:

```

<html lang="en">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>$pageTitle$</title>
    <link rel="stylesheet" href="/luci-static/teltonikaExp/style.css">
    <link rel="stylesheet" href="/luci-static/resources/loginpage.css">
    <link rel="shortcut icon" href="/luci-static/teltonikaExp/favicon.ico">
    <style>
        .login_button {
            margin-top: 15px;
            text-align: center
        }

        .cbi-map-descr {
            text-align: center;
        }
    </style>

```

At the bottom left of the editor area, there is a "Reset" button.

9.13.5 Configurarea serverului RADIUS

Un sistem de autentificare și contabilizare utilizat de mulți furnizori de servicii de acces la internet (ISP). Când vă conectați la ISP, trebuie să vă introduceți numele de utilizator și parola. Aceste informații sunt transmise unui server RADIUS, care verifică dacă informațiile sunt corecte și apoi autorizează accesul la sistemul ISP-ului.

The screenshot shows the "Radius Server" configuration page within the Teltonika RUT955 web interface. The top navigation bar includes "TELTONIKA", "Status", "Network", "Services", "System", and "Logout". The "Radius Server" tab is active, highlighted in blue. The main content area is titled "Radius Server Configuration".

- General Settings:** Contains fields for "Enable" (checkbox), "Remote access" (checkbox), "Accounting port" (set to 1813), and "Authentication port" (set to 1812).
- Users Configuration Settings:** Shows a message: "There are no users created yet." Below this is a table with columns: "Username" (input field), "Password" (input field), and "Add" (button).
- Clients Configuration Settings:** Shows a message: "There are no clients created yet." Below this is a table with columns: "Enable", "Client name", "IP address", "Netmask", and "Radius shared secret".

At the bottom right of the configuration area, there are "Save" and "Cancel" buttons.

	Nume câmp	Explicație
1.	Enable	Activează un sistem de autentificare și contabilizare
2.	Remote access	Activează accesul de la distanță la serverul RADIUS
3.	Accounting port	Portul pe care se ascultă pentru contabilizare
4.	Authentication port	Portul pe care se ascultă pentru autentificare

9.13.5.1 Statistici

În pagina de statistici despre hotspot –Statistics– puteți vizualiza informații statistice despre instanțele hotspotului.

The screenshot shows the 'Hotspot Statistics' section of the Teltonika RUT955 web interface. At the top, there is a navigation bar with tabs: General, Restricted Internet Access, Logging, Landing Page, Radius Server, and Statistics (which is highlighted in blue). Below the tabs, the title 'Hotspot Statistics' is displayed. Underneath the title, there is a search bar with the placeholder 'Search' and a dropdown menu for 'Events per page' set to 10. A table header row is shown with columns: Username, IP, MAC, Start time, End time, Use time, Download, and Upload. Below the table, a message states 'There are no records yet.' and indicates 'Showing 1 to 1 of 1 entries'.

9.14 CLI

Comand Line Interface (CLI) – interfața liniei de comandă – vă permite să introduceți și să executați comenzi în terminalul routerului.

The screenshot shows the CLI terminal window of the Teltonika RUT955 web interface. The terminal prompt is 'Teltonika login: root'. It then asks for a password. After logging in, it displays the BusyBox shell version: 'BusyBox v1.19.4 (2016-05-05 14:14:22 EEST) built-in shell (ash)'. It also provides a help message: 'Enter 'help' for a list of built-in commands.'. Below the shell, there is a small graphic of a tree made of ASCII characters. The terminal then shows the text 'Teltonika 2014' and 'root@Teltonika:~#'. A red question mark character is visible at the end of the command line.

Use "CTRL + ALT + SHIFT + T" keyboard shortcut to open CLI in new tab

9.15 Repornire automată

9.15.1 Repornire pe baza comenzi ping

Funcția Ping Reboot |Reporning prin ping| va trimite periodic comanda ping către server și va aștepta primirea ecoului. Dacă nu este primit niciun ecou, routerul va încerca din nou să trimită comanda ping de numărul de ori definit, după intervalul de timp definit. Dacă nu se primește un ecou după numărul definit de încercări nereușite, routerul va reporni. Puteți opri repornirea routerului după numărul definit de reîncercări nereușite. Astfel, această funcție poate fi folosită ca o funcție "Keep Alive", când routerul trimite un număr nelimitat de comenzi ping către gazdă. Acțiuni posibile dacă nu se primește ecou: repornire, restartare modem, restartare conexiune mobilă, (re)înregistrare, niciuna.

Ping Reboot

Ping Reboot Settings

- Enable
- Action if no echo is received: Reboot
- Interval between pings: 5 mins
- Ping timeout (sec): 5
- Packet size: 56
- Retry count: 2
- Interface: Ping from mobile
- Host to ping from SIM 1: 127.0.0.1
- Host to ping from SIM 2: 127.0.0.1

Nume câmp	Explicație	Note
1. Enable	Această căsuță va activa ori dezactiva funcția de repornire prin ping	În mod implicit, funcția este dezactivată
2. Action if no echo is received	Acțiunea după numărul definit de reîncercări nereușite	Niciun răspuns de ecou primit pentru pachetul ICMP trimis
3. Interval between pings	Intervalul de timp, în minute, între două comenzi ping	Intervalul de timp minim este 5 minute
4. Ping timeout (sec)	Timpul în secunde după care comanda ping se consideră că a eşuat	Interval (1-9999)
5. Packet size	Acest câmp vă permite modificarea dimensiunii pachetului trimis	Trebuie lăsată valoarea implicită, dacă nu este necesar altfel
6. Retry count	Numărul de încercări de trimitere a comenzi ping către server după intervalul de timp specificat, dacă nu s-a primit ecou	Numărul minim de reîncercare este 1. A doua reîncercare va fi efectuată după intervalul de timp definit
8. Interface	Interfața folosită pentru conectare	
7. Host to ping from SIM 1	Adresa IP sau numele de domeniu către care vor fi trimise pachetele ping. De ex. 127.0.0.1 (ori www.host.com dacă serverul DNS este configurat corect)	Pachetele de ping vor fi trimise de pe cartela SIM1.
8. Host to ping from SIM 2	Adresa IP sau numele de domeniu către care vor fi trimise pachetele ping. De ex. 127.0.0.1 (ori www.host.com dacă serverul DNS este configurat corect)	Pachetele de ping vor fi trimise de pe cartela SIM2.

9.15.2 Repornire periodică

Periodic Reboot

Periodic Reboot Setup

Enable

Days Sunday
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday

Hours

Minutes

	Nume câmp	Explicație
1.	Enable	Această căsuță va activa ori dezactiva funcția de repornire periodică
2.	Days	Această căsuță va activa repornirea routerului în ziua definită
3.	Hours, Minutes	Încărcarea va fi realizată la ora respectivă (ore, minute) a zilei

9.16 Resurse partajate în rețea

9.16.1 Sisteme de fișiere montate

În pagina Mounted file systems puteți vizualiza sistemele de fișiere montate (de exemplu o unitate flash USB).

Network Shares

Mounted file systems

Filesystem	Mount Point	Available	Used	
/dev/sda1	/mnt/sda1	7.84 GB / 14.65 GB	47% (6.81 GB)	Safely Remove Disk
				Refresh

	Nume câmp	Explicație
1.	File System	Sistemul de fișiere pe care este montat sistemul de fișiere suplimentar
2.	Mount Point Punct montare	Director disponibil pentru montarea sistemului de fișiere suplimentar
3.	Available	Memoria totală disponibilă în sistemul montat
4.	Used	Memoria ocupată în sistemul montat

9.16.2 Samba

Funcția Samba permite partajarea în rețea a directoarelor specificate.

Name	Path	Allow guests	Allowed users	Read-only
my_dir	/mnt/sda1	<input type="checkbox"/>	root	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="button" value="Delete"/>

	Nume câmp	Valori	Note
1.	Enable	Activare / Dezactivare	Activează serviciul Samba
2.	Hostname	Router_Share	Numele serverului Samba
3.	Description	Teltonika_Router_Share	Scurtă descriere a serverului
4.	Workgroup	WORKGROUP	Numele grupului de lucru

În secțiunea Shared Directories | Directoare partajate| puteți să adăugați directoare pentru a fi partajate și să configurați unii parametri de utilizare:

	Nume câmp	Valori	Note
1.	Name	My_dir	Numele directorului partajat
2.	Path	/mnt/sda1	Calea către directorul ce va fi partajat
3.	Allow guests	Activare / Dezactivare	Permite vizualizarea directorului ca guest
4.	Allowed users	root	Specificați utilizatorii cărora li se va permite să partajeze acest director
5.	Read-only	Activare / Dezactivare	Setează ca utilizatorul să aibă drepturi doar-în-citire în directorul specificat

9.16.3 Utilizatori Samba

În pagina Samba users puteți adăuga noi utilizatori Samba.

Samba users

Users

Username

This section contains no values yet

Add user:

Username	Password
user	pass1

	Nume câmp	Valori	Note
1.	Username	user	Numele noului utilizator
2.	Password	Pass1	Parola noului utilizator

9.17 Interfață Modbus TCP

Modbus TCP

The screenshot shows a configuration page for Modbus TCP. At the top left is a checkbox labeled "Enable". Below it is a text input field labeled "Port" with a placeholder value of "0". Underneath the port field is another checkbox labeled "Allow Remote Access". In the bottom right corner of the form area is a large, rounded rectangular button with the word "Save" in white text.

Interfața Modbus TCP permite utilizatorului să seteze sau să obțină de la router parametri precum temperatura modulului, intensitatea semnalului etc. Cu alte cuvinte, Modbus TCP permite controlul comportamentului routerului și obținerea informațiilor sale de stare. Pentru a utiliza capabilitățile Modbus TCP, această funcție trebuie să fie activată accesând Services-Modbus. După ce apăsați butonul "Save", daemonul Modbus va fi lansat pe portul selectat al sistemului. Daemonul Modbus acționează ca un dispozitiv de tip sclav, ceea ce înseamnă că acceptă conexiunea de la master (client) și trimit un răspuns sau setează un parametru legat de sistem. În mod implicit, Modbus va accepta conexiuni numai prin interfața LAN. Pentru a accepta și conexiunile prin interfața WAN, trebuie să fie bifată căsuța Allow Remote Access |Permitere acces de la distanță|.

Pentru a obține un anumit parametru din sistem, se folosește comanda read holding registers |citire registri memorare|. Numărul de regisztr și valorile din sistem corespunzătoare sunt descrise mai jos. Fiecare regisztr conține 2 octeți. Pentru simplificare, numărul de regisztri pentru stocarea numerelor este 2, în timp ce pentru stocarea informațiilor de tip text numărul de regisztri este de 16.

Valoarea cerută	Reprezentare	Număr regisztr	Număr de regisztri
System uptime Durata de funcționare a sistemului	Întreg fără semn pe 32 biți	1	2
GSM signal strength (dBm) Intensitatea semnalului GSM	Întreg pe 32 biți	3	2
System temperature in 0.1 degrees Celcius Temperatura sistemului în zecimi de grad Celsius	Întreg pe 32 biți	5	2
System hostname Numele de gazdă al sistemului	Text	7	16
GSM operator name Numele operatorului GSM	Text	23	16
Router serial number Numărul serial al routerului	Text	39	16
Router MAC address Adresa MAC a routerului	Text	55	16
Router name Numele routerului	Text	71	16
Current SIM card Cartela SIM curentă	Text	87	16
Network registration Înregistrarea în rețea	Text	103	16
Network type Tipul rețelei	Text	119	16
Digital input 1 Intrarea digitală 1	Întreg pe 32 biți	135	2
Digital input 2 Intrarea digitală 2	Întreg pe 32 biți	137	2
Current WAN IP address Adresa IP WAN curentă	Întreg fără semn pe 32 biți	139	2
Analog input Intrare analogică	Întreg pe 32 biți	141	2

Daemonul Modbus acceptă și setarea unor parametri de sistem. Pentru această sarcină se utilizează comanda write holding register |scriere regisztr memorare|. Parametrii de sistem și modul de utilizare a acestora sunt descrise mai jos. Numărul regisztrului se referă la numărul de regisztr de unde se începe scrierea valorilor solicitate. Toate comenziile, cu excepția "Change APN" |Schimbare nume punct acces|, acceptă doar un singur parametru de intrare.

RUT955 Manual de utilizare

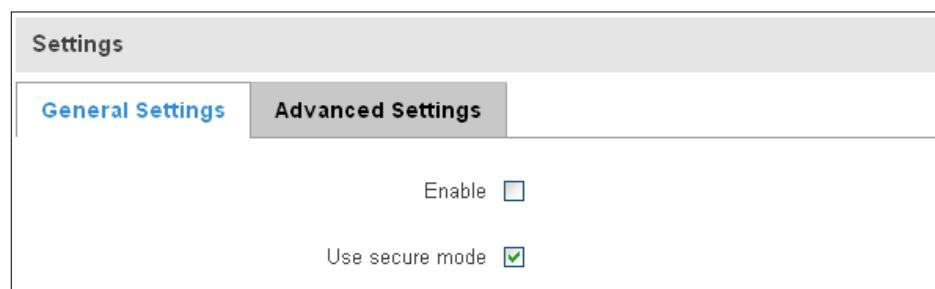
Pentru APN numărul de registri de intrare poate varia. Primul octet al comenzi APN desemnează numărul de cartela SIM pentru care a fost setat APN. Acest octet trebuie să fie setat la 1 (pentru a schimba APN pentru cartela SIM numărul 1) sau la 2 (pentru a schimba APN pentru cartela SIM nr. 2).

Valoarea de setat	Descriere	Număr registru	Valoare registru
Digital output 1 (on/off)	Modifică starea (pornită/oprită) ieșirii digitale nr.1	201	1/0
Digital output 2 (on/off)	Modifică starea (pornită/oprită) ieșirii digitale nr.2	202	1/0
Switch WiFi (on/off)	Permite pornirea sau oprirea conexiunii WiFi	210	1/0
Switch mobile data connection (on/off)	Pornește sau oprește conexiunea de date mobile	211	1/0
Switch SIM card (SIM1, SIM2, SIM1->SIM2 and SIM2->SIM1)	Permite schimbarea cartelei SIM folosite; sunt suportate 3 opțiuni posibile	212	0/1/2
Change APN	Permite schimbarea numelui punctului de acces	213	Cod APN
Reboot	Repornește routerul	220	1

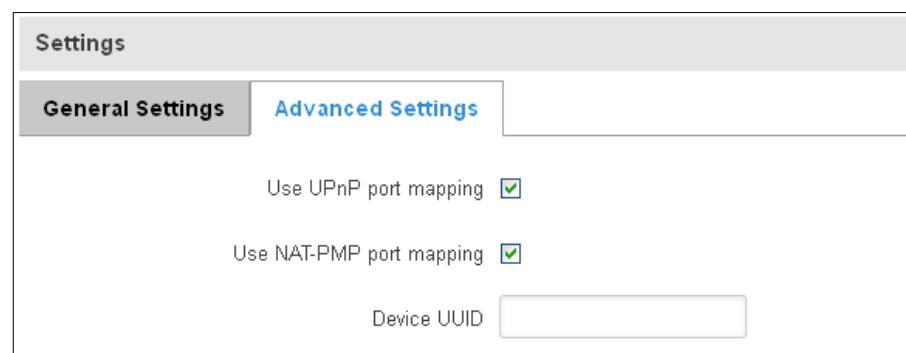
9.18 UPnP

9.18.1 Setări generale

UPnP permite clienților din rețeaua locală să configureze automat routerul.



9.18.2 Setări avansate



	Nume câmp	Explicație
1.	Use UPnP port mapping	Activăți funcția de mapare a porturilor UPnP
2.	Use NAT-PMP port mapping	Activăți funcția de mapare a porturilor NAT-PMP
3.	Device UUID	Specificați identificatorul universal unic al dispozitivului

9.18.3 Liste de control acces UPnP

Listele de control al accesului (ACL) specifică ce porturi externe pot fi redirecționate către adresele și porturile interne specificate.

UPnP ACLs					
ACLs specify which external ports may be redirected to which internal addresses and ports					
Comment	External ports	Internal addresses	Internal ports	Action	Sort
Allow high ports	1024-65535	0.0.0.0/0	1024-65535	allow	
<input type="button" value="Delete"/> <input type="button" value="Add"/>					

	Nume câmp	Explicație
1.	Comment	Adăugați un comentariu la această regulă
2.	External ports	Porturile externe care pot fi redirecționate
3.	Internal addresses	Adresele interne unde se va realiza redirecționarea
4.	Internal ports	Porturile interne unde se va realiza redirecționarea
5.	Action	Acțiune: permite -allow- ori interzice -forbid- serviciului UPNP să deschidă portul specificat

9.18.4 Redirecționări UPnP active

Active UPnP Redirects			
Protocol	External Port	Client Address	Client Port
There are no active redirects.			

9.19 QoS

QoS (Quality of Service, calitatea serviciilor) este ideea că vitezele de transmisie, ratele de eroare și alte caracteristici pot fi măsurate, îmbunătățite și, într-o anumită măsură, garantate în avans. QoS este importantă în special pentru transmiterea continuă a semnalului video în bandă largă și a informațiilor multimedia.

QoS poate fi îmbunătățită prin tehnici de modelare a traficului, cum ar fi prioritizarea pachetelor, a traficului de rețea și a porturilor.

Interfaces					
Interface	Enable	Calculate overhead	Half-duplex	Download speed (kbit/s)	Upload speed (kbit/s)
WAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1024	128
Interface name:	<input type="button" value="WAN"/>	<input type="button" value="Add"/>	<input type="button" value="Delete"/>		

	Nume câmp	Valoare	Explicație
1.	Interface Interfață	WAN/LAN/PPP	

2.	Enable	Activare/Dezactivare	Activăți/dezactivați setările
3.	Calculate overhead	Activare/Dezactivare	Bifați pentru a micșora raportul dintre încărcare și descărcare pentru a preveni saturarea conexiunii
4.	Half-duplex Semiduplex	Activare/Dezactivare	Bifați pentru a activa transmiterea bidirectională a datelor cu un singur operator
5.	Download speed (kbit/s)	1024	Specificați viteza maximă de descărcare
6.	Upload speed (kbit/s)	128	Specificați viteza maximă de încărcare

Classification Rules

Target	Source host	Destination host	Service	Protocol	Ports	Number of bytes	Sort	
Priority	All	All	All	All	22,53			Delete
Normal	All	All	All	TCP	20,21,25,80			Delete
Express	All	All	All	All	5190			Delete

	Nume câmp	Explicație
1.	Target	Selectați ținta pentru care se va aplica regula
2.	Source host Gazdă-sursă	Selectați gazda de pe care vor fi transmise datele
3.	Destination host Gazdă-destinație	Selectați gazda către care vor fi transmise datele
4.	Service	Selectați serviciul pentru care se va aplica regula
5.	Protocol	Selectați protocolul de transmisie de date
6.	Ports	Selectați portul folosit pentru transmitere
7.	Number of bytes	Specificați numărul maxim de octeți pentru conexiune

9.20 Intrări/ieșiri

9.20.1 Stare

În această pagină – Status – puteți vizualiza starea curentă a tuturor intrărilor și ieșirilor routerului.

TELTONIKA Status Network Services System Logout

Status Input Output

Input/Output Status

Type	Associated pins	State
Digital input	1,6	Open
Digital galvanically isolated input	2,7	Low level
Analog input	9,6	0.19 V
Open collector output	3,4,8	Inactive (High level)
Relay output	5,10	Inactive (Contacts open)

1. Intrare digitală (numai pentru senzori pasivi)	6. Masă (intrare digitală & analogică)
2. Intrare digitală izolată (0...4 V: nivel inferior / 9...30 V: nivel superior)	7. Masă (intrare digitală izolată)
3. Ieșire cu colector în gol (max. 0,3 A)	8. Ieșire colector în gol
4. Tensiune de curent continuu externă (0-30 V)	9. Intrare analogică (0-24 V)
5. Ieșire releu (COM) (24 V, 2 A)	10. Ieșire releu (NO)

9.20.2 Intrări

Această pagină – Input – vă permite să configurați parametrii intrărilor și să specificați acțiunile ce vor fi efectuate după producerea evenimentului declanșator al oricărei intrări. În secțiunea Check analog | Verificare intrare analogică| puteți modifica intervalul de verificare a intrării analogice.

Create rules for Input/Output configuration.

Check Analog

Interval [sec] 3

Input Rules

Type	Trigger	Action	Enable	Sort
There are no input rules created yet				

Input Configuration

Input type	Analog type	Trigger	Action	
Analog	Analog Voltage	Inside range	Send SMS	Add
	Analog Voltage			
	Analog Current			

Save

În secțiunea Input rules |Reguli intrare| puteți crea și modifica reguli pentru acțiunea ce va fi efectuată după declanșarea unei anumite intrări.

Input Rules				
Type	Trigger	Action	Enable	Sort
Digital	Input open	Send SMS	<input checked="" type="checkbox"/>	Edit Delete

	Nume câmp	Valoare în exemplu	Explicație
1.	Type	Digital/Digital isolated Digitală izolată /Analog	Specifică tipul de intrare
2.	Trigger	Input open Intrare deschisă	Specifică pentru ce eveniment declanșator se aplică regula
3.	Action	Send SMS Trimitere SMS	Specifică ce acțiune se efectuează
4.	Enable	Activare/Dezactivare	Activăți configurația intrării

Input Configuration

Input type	Analog type	Trigger	Action	
Analog	Analog Voltage	Inside range	Send SMS	Add
	Analog Voltage			
	Analog Current			

Save

	Nume câmp	Valori	Explicație
1.	Input type	Digital/Digital isolated/Analog	Specificați tipul de intrare
1.a	Analog type Tip intrare analogică	Analog Voltage Tensiune analogică /Analog Current Intensitate analogică	Specificați măsurarea tensiunii ori intensității
2.	Trigger	Input open Intrare deschisă / Input shorted Intrare scurtcircuitată / both Ambele	Specificați pentru ce eveniment declanșator se aplică regula
3.	Action	Send SMS Trimitere SMS / Change SIM card Schimbare SIM / Send email Trimitere e-mail / Change profile Schimbare profil / Turn WiFi ON or OFF Pornire/oprire WiFi /Reboot Reporuire / Activate Output Activare ieșire	Alegeți ce acțiune se va efectua după declanșarea intrării

După ce dați clic pe butonul Add |Adăugare| (sau pe Edit |Editare|, dacă regula este deja creată), se afișează a doua pagină de configurare a intrărilor – Input configuration –, cu parametri suplimentari.

The screenshot shows the 'Input Configuration' page of the Teltonika RUT955 web interface. The page has a header with the Teltonika logo and navigation links for Status, Network, Services, System, and Logout. Below the header, there are tabs for Status, Input (which is selected), and Output. The main content area is titled 'Input Configuration'. It contains several input fields: 'Enable' (checkbox checked), 'Input type' (dropdown set to 'Analog'), 'Analog type' (dropdown set to 'Voltage (up to 24V)'), 'Min [V]' (text input set to '10'), 'Max [V]' (text input set to '15'), 'Trigger' (dropdown set to 'Inside range'), 'Action' (dropdown set to 'Activate output'), 'Output activated' (dropdown set to 'While exist'), and 'Output type' (dropdown set to 'Relay output'). At the bottom left is a 'Back to Overview' button, and at the bottom right is a 'Save' button.

	Nume câmp	Valoare în exemplu	Explicație
1.	Enable	Activare/Dezactivare	Activați această regulă pentru intrare
2.	Input type	Digital/Digital isolated/Analog	Specificați tipul de intrare
3.	Min V/mA	10	Specificați tensiunea/intensitatea minimă. Se afișează doar pentru intrarea analogică
4.	Max V/mA	20	Specificați tensiunea/intensitatea maximă. Se afișează doar pentru intrarea analogică
5.	Trigger	Input open	Specificați pentru ce eveniment declanșator se aplică regula
6.	Action	Send SMS Trimitere SMS	Specificați ce acțiune se va efectua
7.	SMS text	Input	Specificați mesajul ce va fi trimis prin SMS
8.	Recipients phone number Nr. telefon destinatar	+37012345678	Numărul de telefon la care veți trimite SMS-ul. Se afișează doar pentru acțiunea Trimitere SMS
9.	Subject	Input	Specificați subiectul e-mailului. Se afișează doar pentru acțiunea Trimitere e-mail
10.	Message	Input	Specificați mesajul ce va fi trimis prin e-mail. Se afișează doar pentru acțiunea Trimitere e-mail
11.	SMTP server	mail.example.com	Specificați serverul SMTP. Se afișează doar pentru acțiunea Trimitere e-mail

12.	SMTP server port	123	Specificați portul serverului SNMP. Se afișează doar pentru acțiunea Trimite e-mail
13.	Secure connection	Activare/Dezactivare	Specificați dacă serverul suportă SSL ori TLS. Se afișează doar pentru acțiunea Trimite e-mail
14.	User name	username	Specificați numele de utilizator pentru conectare la serverul SNMP. Se afișează doar pentru acțiunea Trimite e-mail
15.	Password	password	Specificați parola utilizatorului. Se afișează doar pentru acțiunea Trimite e-mail
16.	Sender's email address	sender@example.com	Specificați adresa Dvs. de e-mail. Se afișează doar pentru acțiunea Trimite e-mail
17.	Recipient's email address	recipient@example.co m	Specificați cui doriți să trimiteți e-mailul. Se afișează doar pentru acțiunea Trimite e-mail
18.	Sim	Primary Principală Secondary Secundară	Specificați care cartelă SIM va fi schimbată. Se afișează doar pentru acțiunea Schimbare SIM
19.	Profile	Admin	Specificați ce profil va fi setat și folosit. Se afișează doar pentru acțiunea Schimbare profil
20.	Reboot after Repornire după (s)	4	Dispozitivul va reporni după o perioadă specificată (în secunde). Se afișează doar pentru acțiunea Repornire
21.	Output activated Ieșire activată	10	Ieșirea va fi activată pentru o perioadă specificată (în secunde) sau pentru cât timp există – While exist –
22.	Output type	Digital OC output Ieșire digitală cu colector în gol/ Relay output ieșire releu	Specificați tipul ieșirii care va fi activată, în funcție de durata ieșirii. Se afișează doar pentru acțiunea Activare ieșire

9.20.3 Ieșiri

9.20.3.1 Configurarea ieșirilor

Output Configuration ON/OFF Post/Get Configuration Periodic Control Scheduler

Output Configuration

Output configuration in active state

Open collector output	<input type="button" value="Low level"/>
Relay output	<input type="button" value="Contacts closed"/>
<input type="button" value="Save"/>	

	Nume câmp	Valoare în exemplu	Explicație
1.	Open collector output Ieșire cu colector în gol	Low level Nivel superior / High level Nivel inferior	Alegeți care ieșire cu colector în gol va fi în starea activă
2.	Relay output Ieșire releu	Contacts closed Contacte închise / Contacts open Contacte deschise	Alegeți care ieșire releu va fi în starea activă

9.20.3.2 Pornire/oprire

Output Configuration	ON/OFF	Post/Get Configuration	Periodic Control	Scheduler
----------------------	--------	------------------------	------------------	-----------

Output

Output

Digital OC output	<input type="button" value="Turn on"/>
Digital relay output	<input type="button" value="Turn on"/>

	Nume câmp	Valoare în exemplu	Explicație
1.	Digital OC output Ieșire cu colector în gol digitală	Turn on Pornire / Turn Off Oprire	Comutați manual ieșirea cu colector în gol digitală
2.	Digital relay output Ieșire releu digitală	Turn on / Turn Off	Comutați manual ieșirea releu digitală

9.20.3.3 Configurarea prin metodele POST/GET

Output Configuration	ON/OFF	Post/Get Configuration	Periodic Control	Scheduler
----------------------	--------	------------------------	------------------	-----------

Post/Get Configuration

Output Post/Get Settings

Enable	<input type="checkbox"/>
Username	user1
Password	pass1 

	Nume câmp	Exemplu	Explicație
1.	Enable	Activare / Dezactivare	Activați funcția de configurare a ieșirii prin metodele POST/GET
2.	Username	User1	Numele de utilizator pentru serviciu
3.	Password	Pass1	Parola pentru autentificare a utilizatorului

9.20.3.4 Sintaxa șirului HTTP POST/GET pentru ieșiri

Puteți gestiona numai ieșirile (ieșirea cu colector în gol și ieșirea releu digitală).

	Nume câmp	Exemplu	Explicație
1.	IP_ADDRESS	192.168.1.1	Adresa IP a routerului Dvs.
2.	action	on Pornire și off Oprire	Specificați acțiunea ce va fi efectuată
3.	pin	oc Cu colector în gol și relay Releu	Specificați ieșirea
4.	delay (sec)	15	Întârzierea în secunde după care va fi pornită acțiunea
5.	time (sec)	10	Perioada în secunde după care va fi oprită acțiunea. (dacă acțiunea este Pornire, va reveni la Oprire după această perioadă)

Rețineți:

Parametrii Întârziere și Perioadă pot fi utilizați împreună. Exemplu: Întârzierea este de 10, perioada este 5, acțiunea este "pornire". La 10 secunde după executarea comenzi, ieșirea va trece în starea "pornită" (sau va rămâne în starea "pornită" dacă este deja pornită), apoi după încă 5 secunde va trece în starea oprită. Perioada totală de execuție a comenzi este de 15 secunde.

Acțiunile "pornire" și "oprire" depind de ieșirea configurată în starea activă (pornită înseamnă în starea activă), în secțiunea „Output configuration in active state”, care poate fi accesată prin Services > Input/Output > Output

9.20.3.5 Exemple de șiruri HTTP POST/GET pentru ieșiri

```
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=on&pin=relay
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=on&pin=relay&delay=10
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=on&pin=relay&time=5
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=on&pin=relay&delay=15&time=5
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=off&pin=relay&delay=15&time=5
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=on&pin=oc
http://192.168.1.1/cgi-bin/output?username=User1&password=Pass1&action=off&pin=oc
```

9.20.3.6 Controlul periodic al ieșirilor

Funcția de control periodic permite utilizatorului să creeze un orar pentru pornirea sau oprirea ieșirilor la anumite ore.

Action	Mode	Action timeout	Days	Enable
On	Fixed	10	Wed	<input checked="" type="checkbox"/>

Add Save

După ce dați clic pe butonul Add |Adăugare| (sau Edit |Editare|, dacă regula este deja creată), se afișează a doua pagină de configurare a controlului periodic al ieșirilor – Periodic output control –, cu parametri suplimentari.

Enable

Output Digital OC output

Action On

Action timeout

Timeout (sec)

Mode Fixed

Hours 1

Minutes 0

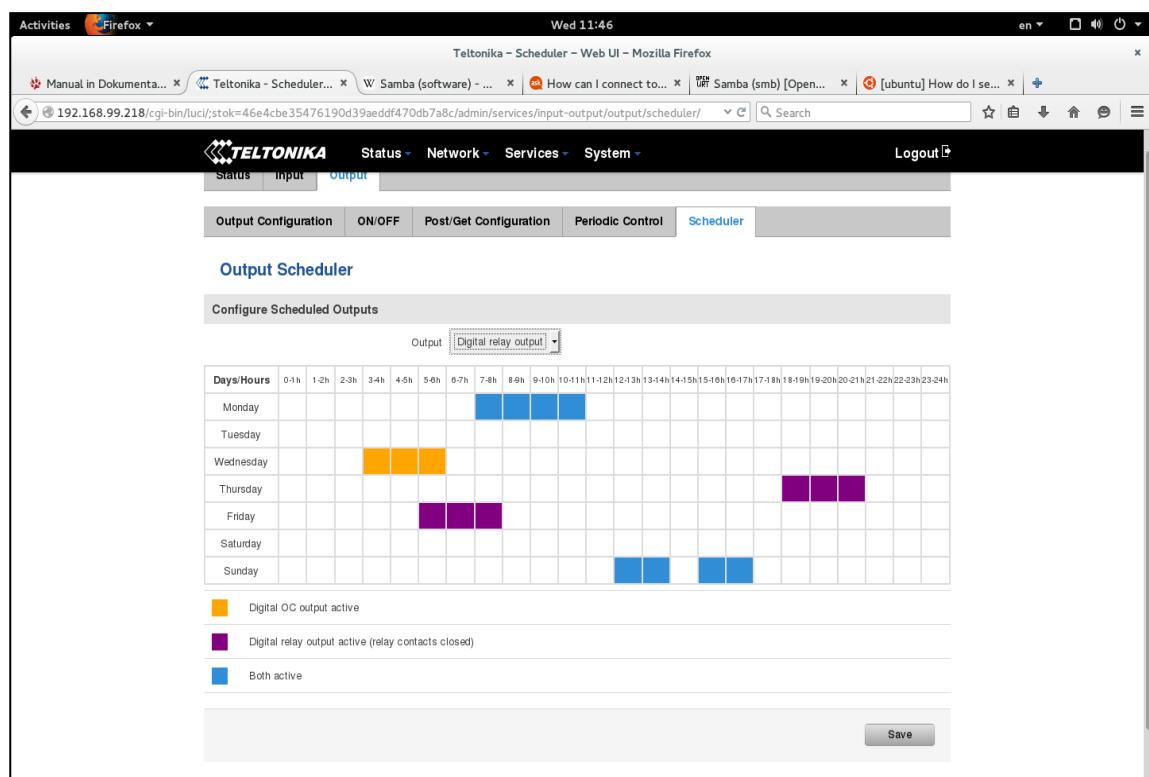
Days Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday
 Sunday

Back to Overview Save

	Nume câmp	Valoare în exemplu	Explicație
1.	Enable	Activare/Dezactivare	Activați această regulă pentru ieșiri
2.	Output	Digital/Digital isolated/Analog	Specificați tipul de ieșire
3.	Action	On / Off	Specificați acțiunea ce va fi efectuată
4.	Action timeout	Activare/Dezactivare	Activați perioada de expirare pentru această regulă
5.	Timeout (sec)	10	Specifică după cât timp se va încheia această acțiune
6.	Mode	Fixed / Interval	Specificați modul de activare a ieșirii
7.	Hours	15	Specificați ora la care va fi activată regula
8.	Minutes	25	Specificați minutul la care va fi activată regula
9.	Days	Monday Luni	Selectați zilele săptămânii în care va fi activată regula

9.20.3.7 Orar

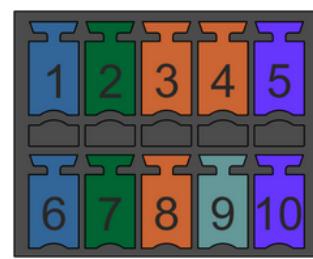
Această funcție –Output scheduler– vă permite să configurați programul periodic, pe ore, al ieșirilor. Puteți selecta în ce zile ale săptămânii vor fi pornite sau opriate ieșirile.



9.20.4 Informații despre componente hardware ale intrărilor și ieșirilor

Conectorul pentru intrări/ieșiri (I/O) se află pe panoul frontal lângă LED-uri. Schema pinilor conectorului I/O:

1	Intrare digitală (numai pentru senzori pasivi)	6	Masă (intrare digitală & analogică)
2	Intrare digitală izolată (0...4 V: nivel inferior / 9...30 V: nivel superior)	7	Masă (intrare digitală izolată)
3	Ieșire cu colector în gol (max. 0,3 A)	8	Ieșire colector în gol
4	Tensiune de curent continuu externă (0-30 V)	9	Intrare analogică (0-24 V)
5	Ieșire relee (COM) (24 V, 2 A)	10	Ieșire relee (NO)



Tip	Descriere	Valori nominale	Cantitate
Intrare (digitală)	Intrare digitală neizolată pentru senzori pasivi	Max. 3 V	1
Intrare (digitală)	Intrare digitală izolată galvanic	0...4 V – nivel inferior 9...30 V – nivel superior	1
Intrare (analogică tensiune/intensitate)	Intrare analogică (0-24 V/0-20 mA)	Max. 24 V/20 mA (cu şunt de 1,2 kΩ)	1
Ieşire (cu colector în gol)	Ieşire cu colector în gol	30 V, 0,3 A	1
Ieşire (releu)	Ieşire releu monopolar pentru un singur circuit (SPST)	24 V, 4 A	1

9.20.4.1 Intrare digitală pentru senzori pasivi

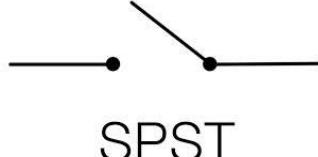
Valori nominale maxime absolute:

Tensiunea maximă la pinul 1 al intrării raportată la pinul 6: **3 V**

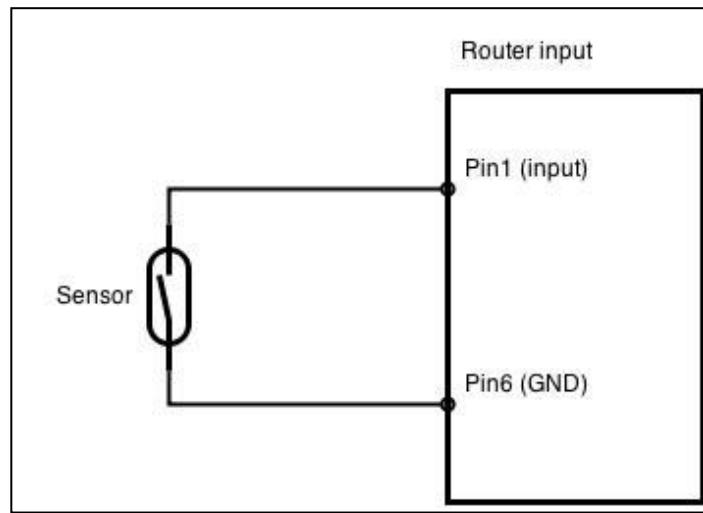
Tensiunea minimă la pinul 1 al intrării raportată la pinul 6: **0V**

Intrarea este protejată împotriva curenților tranzistorii scurți pozitivi sau negativi produși de descărcări electrostatice

Această intrare este destinată conectării senzorilor cu ieșire pasivă (fără tensiune de ieșire), precum:

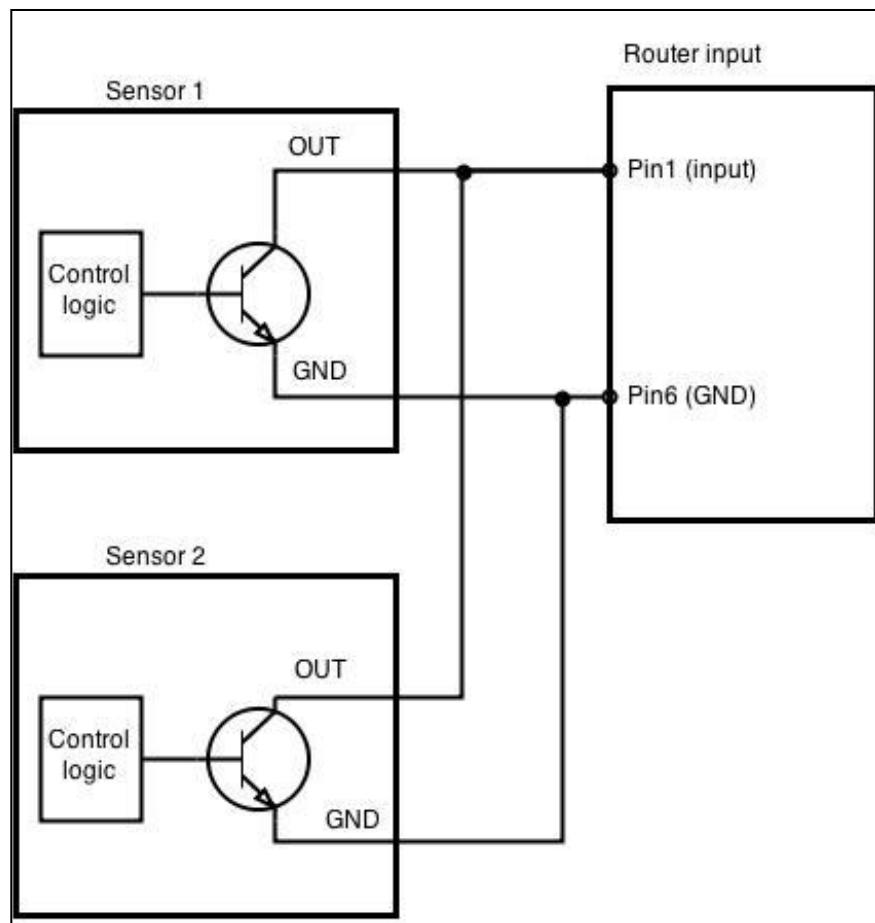
Senzori pasivi cu infraroșu (PIR) pentru detectarea mișcării (pot fi utilizați senzori cu ieșiri cu colector în gol sau cu ieșiri releu)	
Comutatoare mecanice, butoane	 SPST
Comutatoare reed, care își deschid sau închid contactele în apropierea unui câmp magnetic	
Orice senzor cu ieșire cu colector în gol sau cu ieșire de tip open drain (utilizare fără rezistor pull-up)	

Exemplu de schemă în care sunt folosiți senzori PIR, comutatoare mecanice, comutatoare reed:



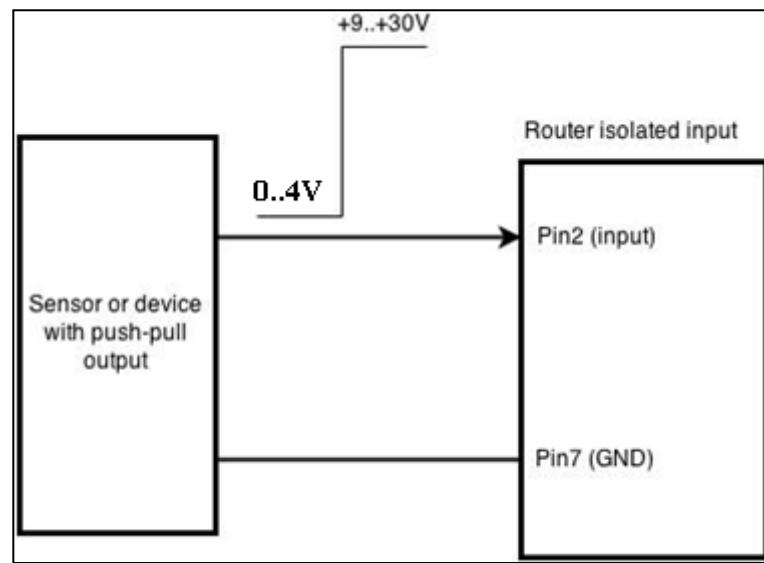
Exemplu de schemă în care sunt conectați mai mulți senzori cu ieșiri cu colector în gol:

Mai mulți senzori pot fi conectați în paralel ca în schema de mai jos. În această configurație orice senzor va activa intrarea. De exemplu, mai mulți senzori de mișcare amplasați în mai multe locuri. Dacă oricare dintre ei va detecta mișcare, evenimentul configurat (de exemplu, alarma) va fi activat. Acest lucru este util atunci când trebuie doar să știți că alarma este declanșată, dar nu și care senzor a activat-o.



9.20.4.2 Intrare digitală izolată galvanic

La această intrare pot fi conectați senzori cu etaje de ieșire în contratimp (push-pull). Un exemplu de astfel de circuit este prezentat în imaginea de mai jos. Circuitul utilizează un optocuplător pentru izolarea intrării. În cazul unei avariile la intrare, restul circuitului rămâne în siguranță.



Rezistența sursei semnalului trebuie să fie sub $100\ \Omega$.

Niveluri ale tensiunii de intrare:

- Nivel inferior: **0...+4 V**
- Nivel superior: **+9...30 V**

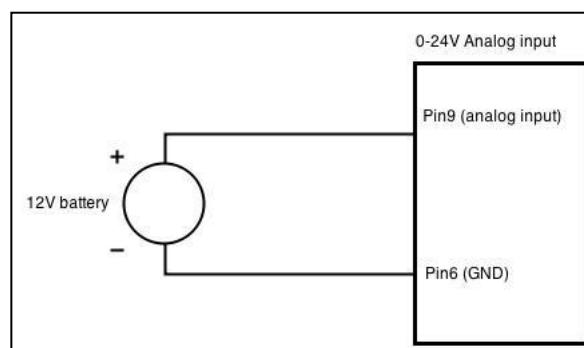
Valori nominale maxime:

- Tensiunea maximă ce poate fi aplicată la pinul 2 raportată la pinul 7 este de **30 V**. Nu depășiți această tensiune!
- Intrarea este protejată împotriva unei tensiuni inverse de până la -200 V.

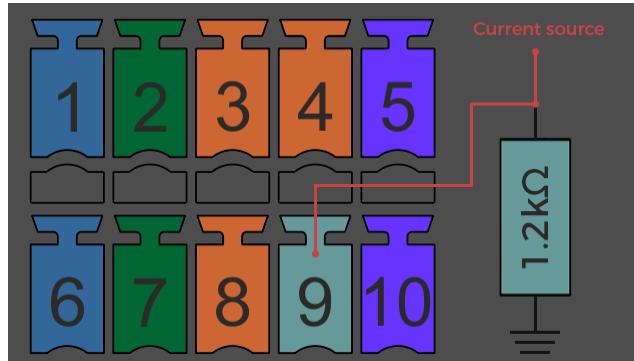
9.20.4.3 Intrarea analogică

Intrarea analogică este destinată măsurării tensiunilor analogice în intervalul 0-24 V și conversiei acestora în domeniul digital. Această intrare poate fi utilizată și pentru măsurarea intensității curentului până la 20 mA.

Exemplu de monitorizare a tensiunii unei baterii de 12 V:



Când tipul intrării analogice este „Intensitate analogică” - Analog Current -, trebuie conectat un şunt cu rezistor de $1,2\text{ k}\Omega$, ca mai jos:



Caracteristicile electrice ale intrării:

Parametru	Valoare
Tensiune maximă	24 V
Tensiune minimă	0 V
Rezoluție	5,859 mV
Frecvența de tăiere a filtrului trece-jos al intrării (-3dB)	10 Hz
Rezistența intrării (între pinii 9 și 6 ai blocului terminal I/O)	131 k Ω

Precizia intrării:

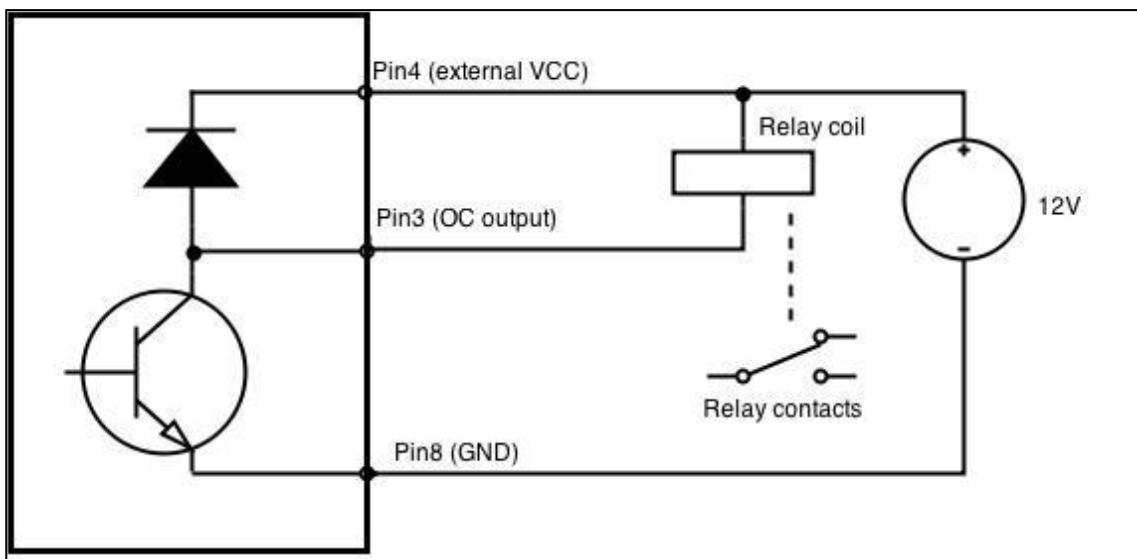
Interval tensiuni intrare, în V	Eroare măsurare, %
$0 < \text{Vin} \leq 1$	<20
$1 < \text{Vin} \leq 2$	<10
$2 < \text{Vin} \leq 5$	<5
$5 < \text{Vin} \leq 24$	<3

9.20.4.4 Ieșirea cu colector în gol

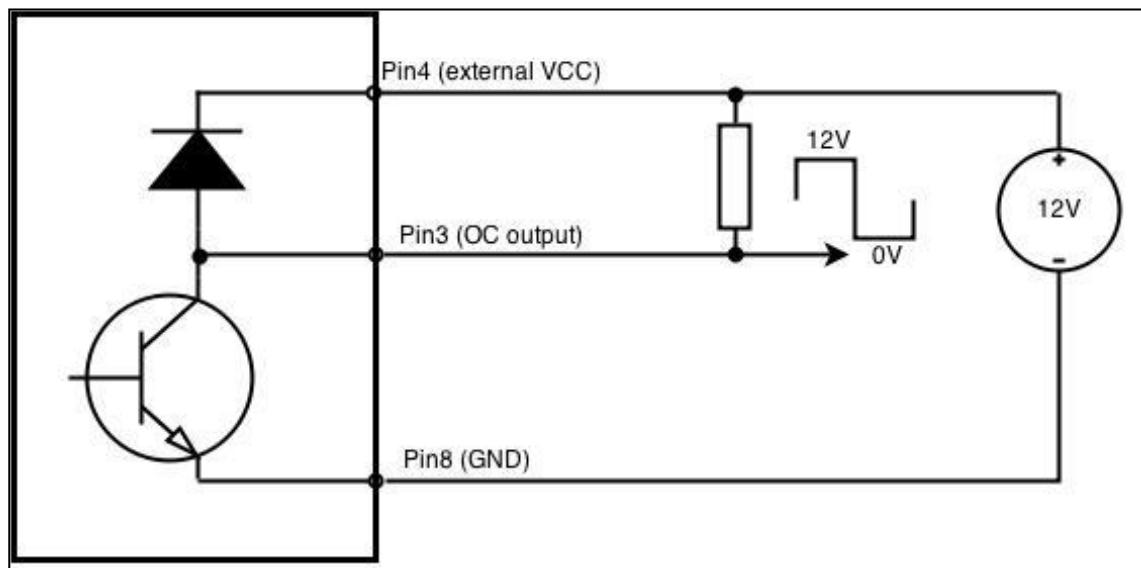
Această ieșire poate fi utilizată pentru acționarea releului extern. Pentru ca ieșirea să funcționeze corect, tensiunea externă care este conectată la un releu trebuie, de asemenea, să fie conectată la pinul 4 al blocului terminal I/O. În interiorul dispozitivului se află o diodă flyback pentru a-l proteja de vârfurile de tensiune care se produc când sarcina inductivă (bobina releului) este oprită brusc, astfel încât nu este necesară conectarea unei diode externe. Ieșirea este izolată de restul circuitului printr-un optocuplător. În cazul unei avarii la ieșire, restul circuitului va rămâne protejat.

Tensiunea externă c.c. maximă	30 V
Curentul absorbit maxim	0,3 A

Exemplu de acționare a unui releu:



Ieșirea poate fi folosită și pentru generarea de semnale cu amplitudinea dorită. Rezistorul ar putea fi, de ex., de 4,7 kΩ.

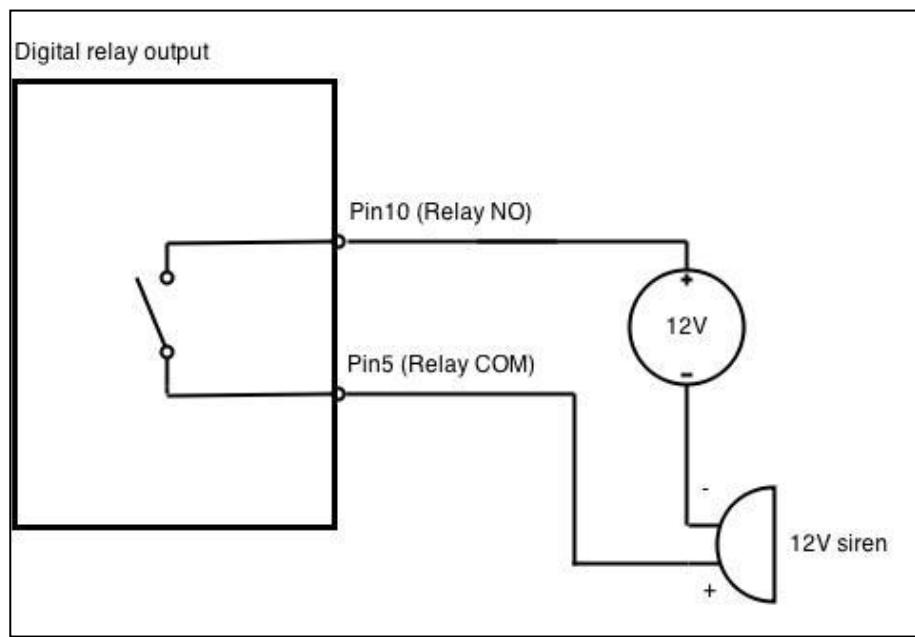


9.20.4.5 Ieșirea releu

Ieșirea releu are doi pini: COM și NO. Când releul nu este alimentat (ieșirea nu este activă), acești pini sunt deconectați. Când releul este alimentat (ieșirea este activă), acești pini se unesc. Ieșirea releu nu este destinată tensiunilor de curent alternativ.

Tensiunea de c.c. maximă între contactele releului	24 V
Intensitatea de c.c. maximă	4 A

Exemplu de conectare a unei sirene de alarmă la ieșirea relee:



10 Sistem

10.1 Asistentul de configurare

Asistentul de configurare oferă o modalitate simplă de configurare rapidă a funcțiilor de bază ale dispozitivului. Asistentul conține 4 pași, după cum urmează:

Pasul 1 (Modificări generale)

La început, asistentul vă va solicita să schimbați parola implicită. Trebuie doar să introduceți aceeași parolă în ambele câmpuri (parolă nouă și confirmare) și apoi să apăsați **Next**.

Step 1 - General	Step 2 - Mobile	Step 3 - LAN	Step 4 - WiFi
<h3>Step - General</h3> <p>First, let's change your router password from the default one.</p> <p>Password Settings</p> <p>New password: <input type="password"/> </p> <p>Confirm new password: <input type="password"/> </p> <p>Time Zone Settings</p> <p>Current system time: 2016-03-16 09:27:33 Sync with browser</p> <p>Time zone: <input type="button" value="UTC"/></p>			

Pasul 2 (Configurarea conexiunii de telefonie mobilă) – Mobile Configuration –

Apoi este necesar să vă configurați conexiunea la rețeaua de telefonie mobilă. Pentru instrucțiuni detaliate accesați secțiunea Rețeaua de telefonie mobilă din capitolul Rețea.

Step 1 - General	Step 2 - Mobile	Step 3 - LAN	Step 4 - WiFi
<h3>Mobile Configuration</h3> <p>Next, let's configure your mobile settings so you can start using internet right away.</p> <p>Mobile Configuration (SIM1)</p> <p>Operator profile: <input type="button" value="None"/></p> <p>APN: <input type="text"/></p> <p>PIN number: <input type="text"/></p> <p>Dialing number: <input type="text"/> *99#</p> <p>Authentication method: <input type="button" value="None"/></p> <p>Service mode: <input type="button" value="4G (LTE) preferred"/></p> <p>Show mobile info at login page: <input type="checkbox"/></p>			

Pasul 3 (LAN)

Aici vă puteți configura opțiunile privind rețeaua LAN și serverul DHCP. Pentru instrucțiuni detaliate accesați secțiunea LAN din capitolul Rețea.

Step - LAN

Here we will setup the basic settings of a typical LAN configuration. The wizard will cover 2 basic configurations: static IP address LAN and DHCP client.

General Configuration

IP address	192.168.1.1
Netmask	255.255.255.0
Enable DHCP	<input checked="" type="checkbox"/>
Start	100
Limit	150
Lease time	12h

Skip Wizard **Save**

Pasul 4 (Wi-Fi)

Pasul final vă permite să vă efectuați setările pentru conexiunea wireless în scopul creării unui punct de acces (AP) simplu.

Step 1 - General **Step 2 - Mobile** **Step 3 - LAN** **Step 4 - WiFi**

Step - Wireless

Now let's configure your wireless radio. (Note: if you are currently connecting via wireless and you change parameters, like SSID, encryption, etc. your connection will be dropped and you will have to reconnect with a new set of parameters.)

WiFi Configuration

Enable wireless	<input checked="" type="checkbox"/>
SSID	Teltonika_Router
Mode	802.11g+n
Channel	Auto
Encryption	No encryption
Country Code	00 - World

Skip Wizard **Save**

Când ați terminat de folosit asistentul de configurare, apăsați **Save**.

10.2 Profiluri

Routerul poate avea 5 profiluri de configurare, pe care le puteți aplica ulterior fie prin interfața web, fie prin SMS. Când adăugați un profil nou, salvați configurația completă **currentă** a routerului. Notă: numele profilurilor nu pot depăși 10 caractere.

Configuration Profiles

Manage Profiles

Profile name	Created	Action
Profile	2016-03-15	<button>Apply</button> <button>Delete</button>

10.3 Administrare

10.3.1 Setări generale

Administration Settings

Router Name And Host Name

Router name: Teltonika
Host name: Teltonika

Administrator Password

New password:
Confirm new password:

Language Settings

Language: English

IPv6 Support

Enable:

Login Page

Show mobile info at login page:
Show WAN IP at login page:

Leds indication

Enable:

Restore Default Settings

Restore to default Restore

Save

	Nume câmp	Explicație
1.	Router name	Introduceți noul nume al routerului Dvs.
2.	Host name	Introduceți noul Dvs. nume de gazdă
3.	New Password	Introduceți-vă noua parolă de administrator. Schimbarea acestei parole va schimba și parola SSH
4.	Confirm new password	Introduceți-vă din nou noua parolă de administrator

5.	Language Limbă	Website-ul va fi tradus în limba selectată
6.	IPv6 support	Activăți suportul IPv6 pe router
7.	Show mobile info at login page	Afișați operatorul de telefonie mobilă și intensitatea semnalului pe pagina de logare
8.	Show WAN IP at login page	Afișați adresa IP a rețelei WAN pe pagina de logare
9.	On/Off LEDs Activare/dezactivare LED-uri	Dacă nu bifați, toate LED-urile routerului sunt dezactivate
10.	Restore to default	Routerul va reveni la setările implicite din fabrică

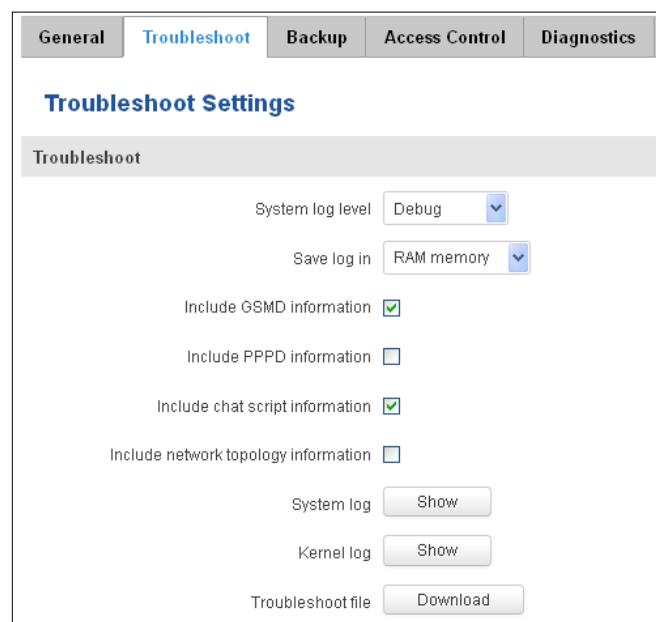
Note importante:

Singura modalitate de a obține acces la administrarea web dacă v-ați uitat parola de administrator este prin revenirea la setările implicite din fabrică ale dispozitivului. Setările implicite de logare ale administratorului sunt:

Nume utilizator: **admin**

Parolă: **admin01**

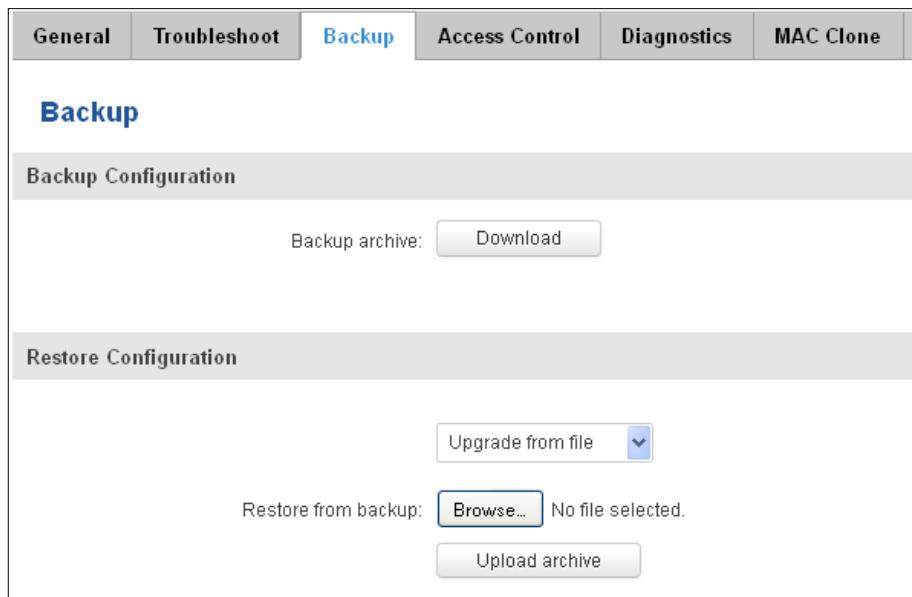
10.3.2 Remedierea defecțiunilor



	Nume câmp	Explicație
1.	System log level Nivel jurnal sistem	Nivelul Debug trebuie folosit întotdeauna, dacă nu vi se cere altfel
2.	Save log in Salvare jurnal în	Memoria RAM (setare implicită) trebuie folosită întotdeauna, dacă nu vi se cere altfel
3.	Include GSMD information Includere informații GSMD	Setare implicită – trebuie folosită activată, dacă nu vi se cere altfel
4.	Include PPPD information Includere informații PPPD	Setare implicită – trebuie folosită dezactivată, dacă nu vi se cere altfel
5.	Include chat script Includere informații script-uri chat	Setare implicită – trebuie folosită activată, dacă nu vi se cere altfel
6.	Include network topology information Includere informații topologie rețea	Setare implicită – trebuie folosită dezactivată, dacă nu vi se cere altfel
7.	System Log Jurnal sistem	Afișează pe ecran informații din jurnalul de sistem. Totuși, nu înlocuiește fișierul cu instrucțiuni de depanare, care poate fi descărcat din meniul System -> Backup and Firmware.

8.	Kernel Log Jurnal nucleu	Afișează pe ecran informații din jurnalul nucleului. Totuși, nu înlocuiește fișierul cu instrucțiuni de depanare, care poate fi descărcat din meniul System -> Backup and Firmware.
9.	Troubleshoot file Fișier remediere defectiuni	Arhivă descărcabilă ce conține toate fișierele de configurare ale routerului și întregul Jurnal de sistem.

10.3.3 Backup



	Nume câmp	Explicație
1.	Backup archive Arhivă backup	Descărcați în calculatorul personal fișierul cu setările curente ale routerului. Acest fișier poate fi încărcat în alt router RUT955 cu aceeași versiune de firmware, pentru a-l configura rapid
2.	Restore from backup Restabilire din backup	Selectați, încărcați și restabiliți fișierul cu setările ale routerului din calculatorul personal

10.3.3.1 Controlul accesului

10.3.3.1.1 Setări generale

	Nume câmp	Explicație
1.	Enable SSH access	Bifați pentru a activa accesul prin SSH
2.	Remote SSH access	Bifați pentru a activa accesul de la distanță prin SSH
3.	Port	Portul care va fi folosit pentru conectarea prin SSH
4.	Enable HTTP access	Activează accesul la router prin HTTP
5.	Enable remote HTTP access	Activează accesul la router de la distanță prin HTTP
6.	Port	Portul care va fi folosit pentru comunicația HTTP
7.	Enable remote HTTPS access	Activează accesul la router de la distanță prin HTTPS
8.	Port	Portul care va fi folosit pentru comunicația HTTPS
9.	Enable CLI	Activează interfața linie de comandă (CLI)
10.	Enable remote CLI	Activează interfața linie de comandă (CLI) de la distanță
11.	Port	Portul care va fi folosit pentru comunicația CLI

Note: Routerul are 2 utilizatori: “**admin**” pentru interfața web și “**root**” pentru SSH. Când vă logați prin SSH folosiți “**root**”.

10.3.3.1.2 Setări de siguranță

SSH Access Secure

Enable
Clean after reboot
Fail count

WebUI Access Secure

Enable
Clean after reboot
Fail count

List Of Blocked Addresses

Events per page: 10 Search

Service *	Blocked address *	Blocked date *
There are no addresses blocked		

Showing 1 to 1 of 1 entries

	Nume câmp	Explicație
1.	SSH access secure enable	Bifați pentru a activa funcția securizare acces SSH
2.	Clean after reboot	Dacă ati bifat – adresele blocate sunt eliminate după fiecare repornire
3.	Fail count Număr încercări eşuate	Specifică numărul maxim de încercări de conectare înainte de blocarea accesului
4.	WebUI access secure enable	Bifați pentru a activa accesul securizat prin interfața web

10.3.4 Diagnoză

Diagnostics

Network Utilities

Host

Action

	Nume câmp	Explicație
1.	Host	Introduceți adresa IP sau numele de gazdă ale serverului

2.	Ping	Utilitar folosit pentru a testa posibilitatea de accesare a unei gazde dintr-o rețea IP și pentru a măsura timpul dus-întors pentru mesajele trimise de la gazda-sursă la un server de destinație. Răspunsul-ecou al serverului va fi afișat după câteva secunde dacă serverul este accesibil
3.	Traceroute	Instrument de diagnosticare pentru afișarea rutei (căii) și pentru măsurarea întârzierilor de tranzit ale pachetelor printr-o rețea IP. Jurnalul care conține informații despre traseu va fi afișat după câteva secunde
4.	Nslookup	Instrument la nivel de linie de comandă de administrare a rețelei pentru interogarea sistemului de nume de domeniu (DNS) în vederea obținerii numelui de domeniu sau mapării adresei IP sau pentru orice altă înregistrare DNS specifică. Jurnalul care conține informațiile DNS specificate despre server va fi afișat după câteva secunde

10.3.5 Clonarea adresei MAC

	Nume câmp	Explicație
1.	WAN MAC address	Introduceți noua adresă MAC a rețelei WAN

10.3.6 Configurarea paginii Overview |Imagine de ansamblu|

Selectați informațiile care doriți să fie afișate în fereastra Overview (Status -> Overview).

	Nume câmp	Explicație
--	-----------	------------

1.	Mobile	Bifați pentru a afișa tabelul Mobile Rețea telefonie mobilă
2.	SMS counter	Bifați pentru a afișa tabelul SMS counter Număr SMS-uri în pagina Overview
3.	System	Bifați pentru a afișa tabelul System în pagina Overview
4.	Wireless	Bifați pentru a afișa tabelul Wireless în pagina Overview
5.	WAN	Bifați pentru a afișa tabelul WAN în pagina Overview
6.	Local network	Bifați pentru a afișa tabelul Local network Rețea locală în pagina Overview
7.	Access control	Bifați pentru a afișa tabelul Access control Control Acces în pagina Overview
8.	Recent system events	Bifați pentru a afișa tabelul Recent system events Evenimente sistem recente în pagina Overview
9.	Recent network events	Bifați pentru a afișa tabelul Recent network events Evenimente rețea recente în pagina Overview
10.	<Nume hotspot> Hotspot	Bifați pentru a afișa tabelul Hotspot instance Instanță hotspot în pagina Overview
11.	VRRP	Bifați pentru a afișa tabelul VRRP în pagina Overview
12.	Monitoring	Bifați pentru a afișa tabelul Monitoring Monitorizare în pagina Overview

10.3.7 Monitorizare

Funcția de monitorizare permite conectarea routerului Dvs. la sistemul de monitorizare la distanță (RMS).

De asemenea, este utilă afișarea în această pagină a adresei MAC și a numărului de serie ale routerului, deoarece sunt necesare atunci când se adaugă dispozitivul în sistemul de monitorizare.

The screenshot shows the Teltonika RMS interface with the following details:

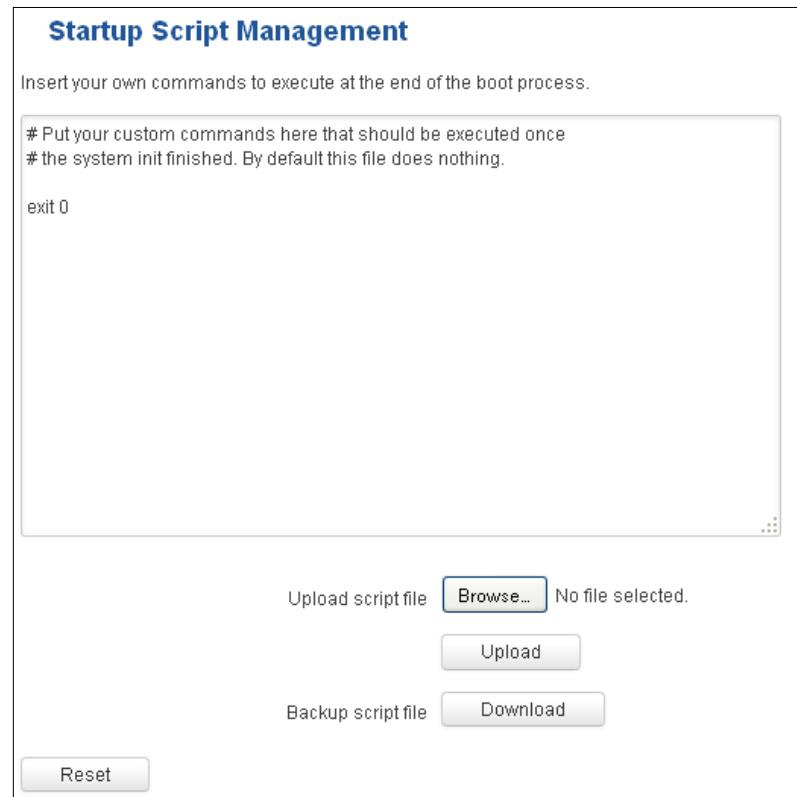
- Header:** TELTONIKA logo, Status, Network, Services, System dropdown menus, Logout button.
- Navigation Bar:** General, Troubleshoot, Backup, Access Control (highlighted), Diagnostics, MAC Clone, Overview, Monitoring (highlighted).
- Section:** Remote Monitoring
- Sub-section:** Remote Access Control
- Form Fields:**
 - Enable remote monitoring
- Status Table:**

Status	
Monitoring	Enabled
Connection state	Connected to monitoring system
Router LAN MAC address	00:1E:42:1E:42:10
Router serial number	77885555
- Buttons:** Refresh, Save.

	Nume câmp	Explicație
1.	Enable remote monitoring	Bifați pentru a activa/dezactiva monitorizarea la distanță
2.	Monitoring	Afișează starea monitorizării
3.	Router LAN MAC address Adresă MAC router în LAN	Adresa MAC a porturilor din rețeaua LAN Ethernet
4.	Router serial number	Numărul de serie al routerului

10.4 Script-uri scrise de utilizatori

Utilizatorii avansați își pot insera propriile comenzi ce vor fi executate la finalul procesului de pornire.



În fereastra *Script Management* |Gestionare script-uri| este afișat conținutul unui fișier /etc/rc.local. Acest fișier este executat la sfârșitul procesului de pornire, executându-se linia: sh /etc/rc.local. În acest script este necesar să folosiți comenziile sh (ash). Trebuie remarcat faptul că acesta este un dispozitiv încorporat, iar funcția sh nu este deplină.

10.5 Punct de restaurare

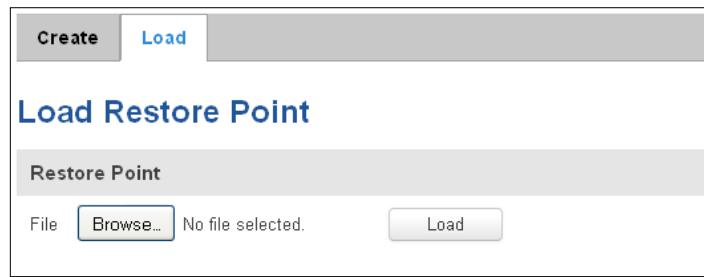
10.5.1 Crearea unui punct de restaurare

Pagina Create restore point permite crearea de puncte de restaurare a firmware-ului cu toate configurările personalizate. Puteți descărca în calculatorul Dvs. punctele de restaurare create.



10.5.2 Încărcarea unui punct de restaurare

Pagina Load restore point permite restabilirea configurației pe baza unui punct de restaurare salvat anterior. Puteți încărca punctul de restaurare din calculatorul Dvs.



10.6 Firmware

10.6.1 Firmware

Current Firmware Information		Firmware Available On Server	
Firmware version	RUT9XX_R_00.02.341	Firmware version	RUT9XX_R_00.02.345
Firmware build date	2016-05-04, 15:12:44		
Kernel version	3.10.36		

Firmware Upgrade Settings

Keep all settings Keep dynamic DNS settings
 Keep network settings Keep wireless settings
 Keep mobile settings Keep firewall settings
 Keep LAN settings Keep OpenVPN settings

Upgrade from file No file selected.

Keep all settings | Păstrați toate setările | – dacă bifăți, routerul va păstra setările efectuate de utilizatorii salvate după upgradarea firmware-ului. Dacă nu bifăți, toate setările routerului vor fi restabilite la valorile implicate din fabrică după upgradarea firmware-ului. Când upgradați firmware-ul, puteți alege setările pe care dorîți să le păstrați după upgrade. Această funcție este utilă atunci când firmware-ul este upgradat prin internet (de la distanță) și nu trebuie să pierdeți ulterior conexiunea la router.

FW image file – fișierul de upgradare a firmware-ului routerului.

Avertisment: Nu întrerupeți niciodată alimentarea routerului și nu apăsați butonul de resetare în timpul procesului de upgradare! Routerul va fi grav deteriorat și va deveni inaccesibil. Dacă aveți probleme legate de upgradarea firmware-ului, trebuie să consultați întotdeauna distribuitorul local.

10.6.2 Firmware over the air (FOTA)

Firmware Over The Air Configuration

Server Settings

Server address: http://rms.teltonika.lt/fota

User name: admin

Password:

Enable auto check:

Auto check mode: On router startup

WAN wired:

	Nume câmp	Explicație
1.	Server address	Specificați adresa serverului pentru a verifica dacă există actualizări de firmware. De ex. "http://teltonika.sritis.lt/rut9xx_auto_update/clients/"
2.	User name	Nume de utilizator pentru autorizarea pe server
3.	Password	Parola pentru autorizarea pe server
4.	Enable auto check Activare verificare automată	Bifați pentru a activa verificarea automată a existenței unor noi actualizări de firmware
5.	Auto check mode Mod verificare automată	Selectați când se va realiza verificarea automată
6.	WAN wired WAN pe cablu	Permite actualizarea de pe server a firmware-ului numai dacă rețeaua WAN a serverului este pe cablu (dacă este bifată căsuța).

10.7 Repornirea routerului

Router reboot

Warning! During reboot you will temporarily lose the connection.

Reboot

Reporniți routerul apăsând butonul "Reboot".

11 Recuperarea dispozitivului

Următoarea secțiune descrie opțiunile disponibile pentru recuperarea dispozitivului defect. De obicei, dispozitivul poate deveni inaccesibil din cauza unei căderi a alimentării în timpul actualizării firmware-ului sau dacă fișierele sale de bază au fost modificate în mod eronat în sistemul de fișiere. Rutele Teltonika oferă mai multe opțiuni pentru

11.1 Butonul de resetare

Butonul de resetare este situat pe panoul din spate al dispozitivului. Butonul de resetare are mai multe funcții:

Reporarea dispozitivului. După ce dispozitivul a pornit și dacă butonul de resetare este apăsat timp de până la 4 secunde, dispozitivul va reporni. Începutul reporirii va fi indicat prin clipirea tuturor celor 5 LED-uri de intensitate a semnalului, împreună cu LED-ul verde de stare a conexiunii.

Resetare la valorile implicate. După ce dispozitivul a pornit, dacă butonul de resetare este apăsat timp de cel puțin 5 secunde, dispozitivul va reseta toate modificările efectuate de utilizator la valorile implicate din fabrică și va reporni. Pentru a ajuta utilizatorul să știe cât timp trebuie apăsat butonul de resetare, LED-urile de intensitate a semnalului indică timpul scurs. Toate cele 5 LED-uri aprinse înseamnă că au trecut 5 secunde și că butonul de resetare poate fi eliberat. Începutul resetării la valorile implicate va fi indicat prin aprinderea tuturor celor 5 LED-uri de intensitate a semnalului, împreună cu LED-ul roșu de stare a conexiunii. PIN-ul cartelei SIM principale este singurul parametru de utilizator care este păstrat după resetarea la valorile implicate.

11.2 Interfața web a bootloader-ului

Bootloader-ul este o altă modalitate de recuperare a funcționalității routerului atunci când firmware-ul este deteriorat. Pentru o mai ușoară utilizare, bootloader-ul are propriul său server web care poate fi accesat cu orice browser web.

Procedura de pornire a serverului web al bootloader-ului:

În mod automat. Se întâmplă când bootloader-ul nu detectează firmware-ul master. Clipirea tuturor celor 4 LED-uri Ethernet indică faptul că serverul web al bootloader-ului a pornit.

Manual. Serverul web al bootloader-ului poate fi solicitat ținând apăsat butonul de resetare timp de 3 secunde în timp ce porniți dispozitivul. Clipirea tuturor celor 4 LED-uri Ethernet indică faptul că serverul web al bootloader-ului a pornit.

Interfața web a bootloader-ului poate fi accesată prin tastarea acestei adrese în browser-ul web:

<http://192.168.1.1/index.html>

Notă: poate fi necesar să ștergeți memoria cache a browser-ului web și să utilizați o fereastră incognito / anonimă pentru a accesa interfața web a bootloader-ului.

12 Glosar

WAN – Wide Area Network – este o rețea de telecomunicații care acoperă o arie largă (adică orice rețea la nivel de oraș, regiune sau țară). Aici folosim termenul WAN pentru rețeaua externă pe care routerul o utilizează pentru a accesa internetul.

LAN – Local Area Network – o rețea locală este o rețea de calculatoare care interconectează calculatoarele într-o zonă limitată, cum ar fi o casă, o școală, un laborator informatic sau o clădire de birouri.

DHCP – Dynamic Host Configuration Protocol – Protocolul de configurare a gazdei dinamice este un protocol de configurare a rețelei pentru gazde în rețelele IP (Internet Protocol). Computerele care sunt conectate la rețele IP trebuie configurate înainte de a putea comunica cu alte gazde. Cele mai importante informații necesare sunt o adresă IP, o rută implicită și un prefix de rutare. DHCP elimină activitatea manuală a unui administrator de rețea. De asemenea,

furnizează o bază de date centrală a dispozitivelor conectate la rețea și elimină alocările duplicate de resurse.

CABLU ETHERNET – Se referă la cablul CAT5 UTP cu conector RJ-45.

AP – Access Point – Punct de acces. Un punct de acces este orice dispozitiv care oferă conectivitate wireless pentru clienții wireless. În acest caz, când activați conexiunea Wi-Fi pe routerul Dvs., acesta devine un punct de acces.

DNS – Domain Name Resolver. Resolver de nume de domeniu. Un server care translatează nume precum www.google.lt la adresele IP respective. Pentru ca computerul sau routerul Dvs. să comunice cu un server extern, trebuie să îi cunoască adresa IP; numele său "www.something.com" nu este suficient. Există servere speciale care execută această sarcină specifică de rezoluție a numelor în IP-uri, denumite servere de nume de domeniu. Dacă nu ati specificat niciun DNS, puteți naviga în continuare pe web, cu condiția să cunoașteți adresa IP a site-ului pe care încercați să îl accesați.

ARP – Adress Resolution Protocol – un protocol de strat de rețea folosit pentru convertirea unei adrese IP într-o adresă fizică (denumită adresă DLC), cum ar fi o adresă Ethernet.

PPPoE – Point-to-Point Protocol over Ethernet – Protocol punct-la-punct prin Ethernet. PPPoE este o specificație pentru conectarea utilizatorilor dintr-o rețea Ethernet la internet printr-un mediu comun de bandă largă, cum ar fi o linie DSL, un dispozitiv wireless sau un modem de cablu.

DSL – Digital Subscriber Line – linie digitală de abonat – este o familie de tehnologii care oferă acces la internet prin transmiterea datelor digitale printr-o rețea telefonică locală care utilizează rețeaua publică de telefonie comutată.

NAT – Network Address Translation – translatarea adresei de rețea – un standard internet care permite unei rețele locale (LAN) să utilizeze un set de adrese IP pentru traficul pe internet și un alt doilea set de adrese pentru traficul extern.

LCP – Link Control Protocol – un protocol care face parte din PPP (Point-to-Point Protocol). LCP verifică identitatea dispozitivului conectat și fie acceptă, fie respinge dispozitivul partener, determină dimensiunea acceptabilă a pachetului pentru transmisie, caută erori în configurație și poate termina legătura dacă parametrii nu sunt îndepliniți.

BOOTP – Bootstrap Protocol – un protocol de internet care permite unei stații de lucru fără disc să-și descopere propria adresă IP, adresa IP a unui server BOOTP din rețea și un fișier care trebuie încărcat în memorie pentru a porni mașina. Astfel se permite stației de lucru să pornească fără a necesita o unitate hard disk sau unitate floppy.

TCP – Transmission Control Protocol – Protocol de control al transmisiei. Unul dintre protocolele principale din rețelele TCP/IP. În timp ce protocolul IP lucrează numai cu pachete, TCP permite celor două gazde să stabilească o conexiune și să schimbe fluxuri de date. TCP garantează livrarea datelor și garantează că pachetele vor fi livrate în același ordine în care au fost trimise.

TKIP – Temporal Key Integrity Protocol – efectuează scramblarea cheilor folosind algoritmul hash și, adăugând o caracteristică de verificare a integrității, asigură că cheile nu au fost compromise.

CCMP – Counter Mode Cipher Block Chaining Message Authentication Code Protocol – protocol de criptare conceput pentru produsele LAN wireless care implementează amendamentul IEEE 802.11i la standardul IEEE 802.11 original. CCMP este o encapsulare criptografică a datelor schimbate concepută pentru asigurarea confidențialității datelor și bazată pe modul Counter with CBC-MAC (CCM) al standardului AES (Advanced Encryption Standard).

MAC – Media Access Control – adresa hardware care identifică în mod unic fiecare nod dintr-o rețea. În rețelele IEEE 802, stratul de control al legăturii de date (DLC) al modelului de referință al PSO este împărțit în două substraturi: stratul LLC și stratul MAC. Stratul MAC interfațează direct cu mediul de rețea. În consecință, fiecare tip de mediu de

rețea necesită un strat MAC diferit.

DMZ – Demilitarized Zone – zonă demilitarizată – un computer sau o subrețea mică situată între o rețea internă de încredere, cum ar fi o rețea LAN privată, și o rețea externă nesigură, cum ar fi internetul public.

UDP – User Datagram Protocol – un protocol fără conexiune care, la fel ca TCP, rulează peste rețele IP. Oferă foarte puține servicii de recuperare a erorilor, oferind în schimb un mod direct de a trimite și primi datagrame prin rețeaua IP.

VPN – Virtual Private Network – rețea privată virtuală – o rețea construită utilizând rețele publice – de obicei internetul – pentru conectarea la o rețea privată, cum ar fi rețeaua internă a unei companii.

VRRP – Virtual Router Redundancy Protocol – un protocol de selecție care atribuie dinamic routerului/routerelor VRRP dintr-o rețea LAN responsabilitatea unuia sau mai multor routere virtuale, permitând mai multor routere pe o legătură multiacces să utilizeze aceeași adresă IP virtuală.

Tunel GRE – Generic Routing Encapsulation – Încapsularea generică pentru rutare – un protocol de tunelare dezvoltat de Cisco Systems, care poate încapsula o mare varietate de protocoale de straturi de rețea în interiorul unor legături virtuale punct-la-punct într-o rețea de rețele ce folosesc protocolul IP.

PPPD – Point to Point Protocol Daemon – este folosit pentru gestionarea conexiunilor de rețea între două noduri pe sistemele de operare de tip Unix. Este configurațat folosind argumente în linia de comandă și fișiere de configurație.

SSH – Secure SHell – un program pentru logarea la alt computer printr-o rețea, pentru executarea de comenzi într-o mașină la distanță și pentru mutarea de fișiere de pe o mașină pe alta. Oferă o autentificare puternică și comunicații sigure pe canale nesigure.

VRRPD – Virtual Router Redundancy Protocol Daemon – este conceput pentru a elimina punctul unic de eșec asociat rețelelor rutate în mod static asigurând automat failover-ul prin folosirea mai multor căi LAN prin routere alternative.

SNMP – Simple Network Management Protocol – un set de protocoale pentru gestionarea rețelelor complexe. SNMP funcționează prin trimiterea de mesaje, numite unități de date de protocol (PDU), către diferite părți ale unei rețele.

13 Evidență modificărilor

Nr.	Data	Versiune	Observații
1	2018-02-05	1.26.1	Traducere in limba romana a versiunii 1.26 – Topalis Engineering

Distribuitor autorizat Teltonika în România: **Topalis Engineering srl**

email: teltonika@topalis.ro