Manuale di configurazione

Revisione N.30 del 09/01/2018

Indice

1. Note introduttive

Questo manuale illustra le principali e più comuni attività applicambili agli apparati Townet.
Per ogni approfondimento in merito a particolari configurazioni o proprietà del software Mikrotik si rimanda ad altri manuali forniti da Townet o alla manualistica Mikrotik.

La manualistica originale Mikrotik è disponibile on-line al seguente indirizzo: https://wiki.mikrotik.com/wiki/

Raccomandazioni

Questo apparato è conforme alla direttiva europea RED 2014/53/EU e successive integrazioni, pertanto l'uso è soggetto all'ottemperanza al D.Lgs 128/2016 e successive modifiche e integrazioni, ed è soggetto a limitazioni d’uso

Riportiamo, inoltre, una serie di raccomandazioni per il corretto settaggio del software al fine di rispettare la normativa vigente.

Il DFS deve essere obbligatoriamente impostato e mai disattivato per essere compatibile con la normativa.

Il valore di Antenna Gain deve essere settato in modo che la potenza in uscita all'antenna non superi i limiti previsti dalla normativa.

Impostare il valore di Frequency Mode a Regulatory domain e settare il campo Country a Italy. Tale configurazione abiliterà il software a lavorare nel rispetto della normativa italiana.

Impostare il parametro Installation in Indoor oppure Outdoor in base al tipo di installazione.

La configurazione deve essere eseguita da tecnici qualificati con specifiche competenze in radiofrequenza.

2. Accesso in configurazione

Applicabile a: Tutti gli apparati

Neighbor Viewer

NeighborViewer è un software che identifica tutti gli apparati townet presenti nella rete all'interno dello stesso dominio di collisione.

Neighbor Viewer permette di accedere all'interfaccia telnet dell'apparato tramite MAC Telnet. Cliccando sull'apparato si aprirà la finestra del terminale dove verrà chiesta user e password.

Accesso con Winbox

L'applicazione winbox fornita con il CD rappresenta un loader dell'applicazione che risiede sulla board. Il loader infatti si allinea con la versione di firmware caricata sull'apparato e scarica, se necessario, l'applicazione con la revisione corretta.

L'accesso è possibile sia utilizzando l'indirizzamento ip che utilizzando l'accesso con Mac address.

Utilizzando il pulsante "…" viene visualizzata una lista di tutti gli apparati presenti nello stesso dominio di collisione dai quali è possibile selezionare l'apparato da configurare.

Consigliamo di utilizzare l'accesso via mac address perché rende indipendente l'operatore dall'ip assegnato e quindi da eventuali di sconnessioni in caso di configurazione delle interfacce.

Si consiglia di utilizzare sempre l'accesso "Secure mode" che garantisce un livello di crittografia dei dati passanti fra l'apparato e il pc con cui si sta operando.

E' inoltre possibile salvare la password e salvare i dati di connessione per un veloce accesso.

Console Winbox

WinBox rappresenta un potentissimo tool di configurazione ed è strutturato con una pulsantiera che rispecchia la struttura gerarchica dei menù dell'interfaccia CLI.

Ogni maschera rappresenta i dati in un formato a tabelle e possiede dei pulsanti comuni che abilitano l'esecuzione di alcuni comandi standard come l'inserimento, la modifica ecc… Di seguito è riportata la lista di tali comandi:

per inserire una nuovo elemento
per cancellare un elemento
per abilitare un elemento
per disabilitare un elemento
per inserire una nota o un commento
per filtrare la vista

Fare particolare attenzione a non confondere il tasto "X" con il tasto "-" perché il primo disabilita e il secondo cancella senza chiedere alcuna conferma!

Per verificare se la connessione è protetta da crittografia fare riferimento all'icona in alto a destra rappresentata da un lucchetto, che se è chiuso rappresenta la connessione sicura altrimenti no.

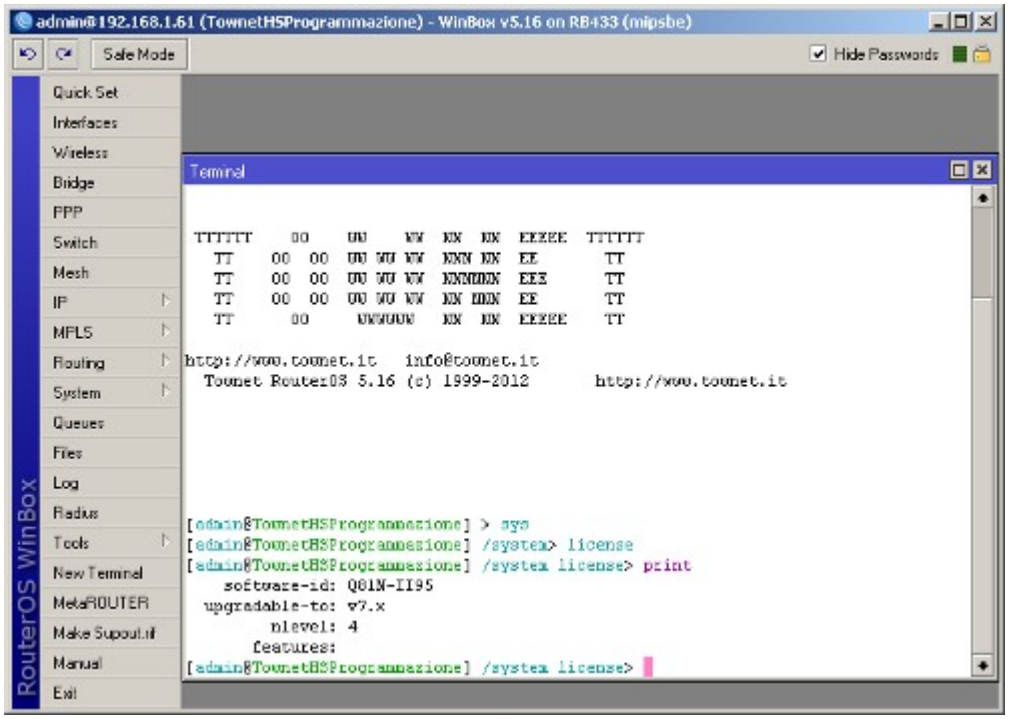
E' inoltre possibile utilizzare l'interfaccia CLI anche all'interno di WinBox premendo il pulsante "New Terminal" come indicato nella seguente figura.

Winbox è un'ambiente in cui è possibile aprire diverse finestre allo stesso tempo come indicato di seguito.

Accesso in Command Line Interface

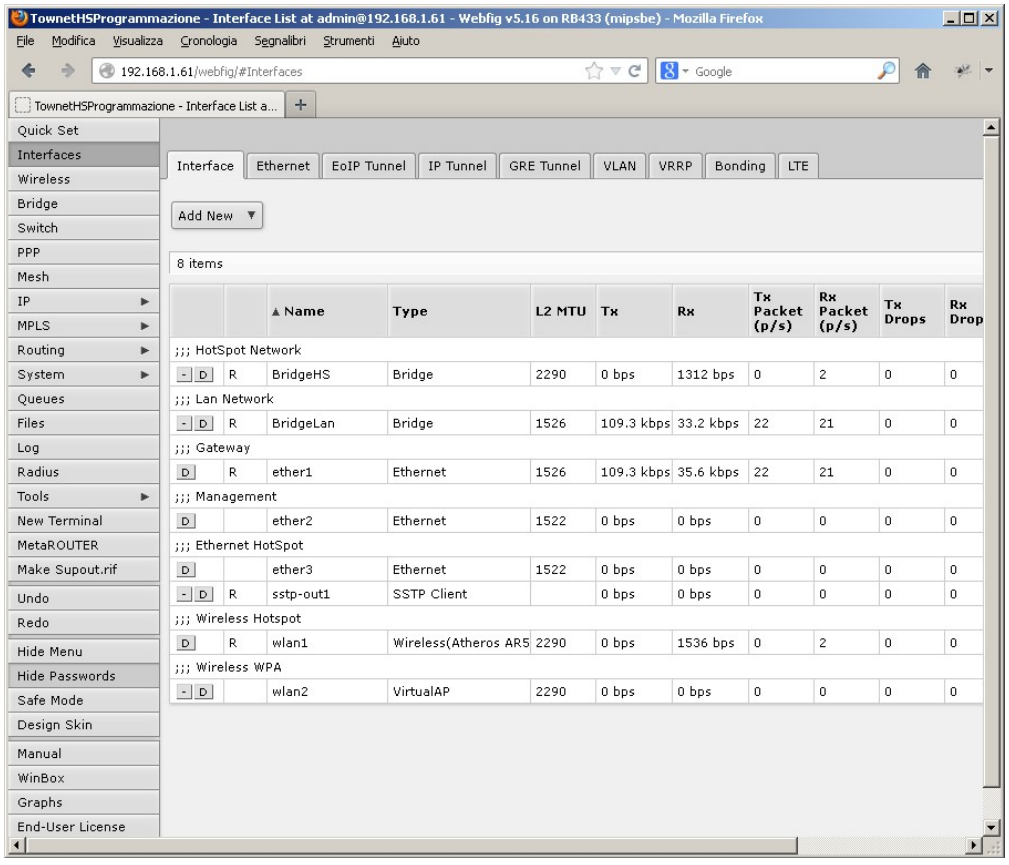
Tutti gli apparati townet sono dotati di una potente interfaccia testuale raggiungibile tramite Neighbor Viewer o utilizzando un comune client telnet.

La shell è costituita da una serie di directory che rappresentano ciascuna un'area di applicazione di comandi.



Interfaccia Web

collegandosi all'indirizzo http://[ip_router]/webfig è possibile accedere alla configurazione dell'apparato con l'interfaccia web.



3. Configurazione di base

Applicabile a: Tutti gli apparati radio tranne

Tutti gli apparati vengono forniti con una configurazione di base in modalità "Bridge". Tale modalità permette di agganciare gli apparati e far passare qualsiasi traffico attraverso tutte le interfacce. Inoltre gli apparati vengono forniti con la parte radio configurata per cui è possibile utilizzarli subito senza alcun intervento di configurazione. Di seguito viene riportata una tabella che elenca gli elementi significativi di una configurazione base

Apparati serie BS
Modalità: AP (Master)
IP: 10.10.10.1/24

Apparati Serie BR
Modalità: Bridge (Master)
IP: 10.10.10.1/24

Apparati Serie SU
Modalità: Station-Wds (Slave)
IP: 10.10.10.2/24

Apparati serie HS
Modalità: AP (Master) (2.4 ghz.)
Modalità: AP (Master) (5 ghz.)
IP: 10.10.10.1/24

Utenti di default

Ogni apparato viene fornito con tre tipologie di utenza di default come segue:

Nome Utente	**Password**	Tipo Account
admin	rtmtc	Full
manager	manager	Write
user	user	Read

Ripristino configurazione originale

All'interno di ogni apparato viene fornita è presente un file di configurazione con il nome dell'apparato ed estension rsc. Tale file può essere utilizzato per ripristinare la configurazione originale dell'apparato.

Per poter caricare la configurazione è necessario resettare l'apparato con il comando /system reset-configuration. L'apparato sarà poi raggiungibile solo via MAC.
ATTENZIONE! Dopo il reset se l'apparato non viene riconfigurato con un appropriato script avrà user admin e password vuota.
Eseguire il seguente comando per ripristinare la configurazione: `/import file-name=[nome_file].rsc`
L'operazione è possibile solo utilizzando comandi a terminale.

E' inoltre possibile accorpare le due operazioni con il seguente comando:
`/system reset-configuration run-after-reset=[nome_file].rsc`

L'apparato ripartirà con la configurazione del file.

4. Configurazione interfaccia radio

Applicabile a: Tutti gli apparati radio
Con l'evoluzione della tecnologia i prodotti Townet si aggiornano introducendo la tecnologia MiMo ai propri apparati.
MiMo (multi imput multi output) appartiene allo standard 802.11 n e permette di raggiungere velocità di trasmissioni prossime ai 300 Mbit al secondo sfruttando allo stesso tempo la doppia polarizzazione delle antenne. Mikrotik supporta questa tecnologia ed dagli ultimi firmware è stata aggiunta una voce al menu di *configurazione della parte Wireless (vedere la configurazione sotto la voce HT)* che permette di sfruttare al pieno questa tecnologia. Le antenne delle versioni di apparati MiMo hanno *sia una polarizzazione orizzontale sia una polarizzazione verticare* che tramite i pigtail vengono collegate alle schede radio MiMo che hanno a loro volta due connettori creando così un sistema MiMo aumentando le prestazioni del link radio.

Finestra Wireless
Tutte le interfacce radio dell'apparato sono visibili premendo il tasto "Wireless" dal menù principale di Winbox.

Wireless Tables

Interfaces

	Name	Type	MTU	MAC Address	Mode	Band	Frequency	SSID
R	Wlan1	Wireless (Atheros AR5213)	1500	00:80:48:41:55:FB	Station-wds	5Ghz.	5600Mhz.	Townet

La lista riporta i dati principali di configurazione della scheda radio. Notare la lettera "R" che indica lo stato "Running" dell'interfaccia. Le possibili impostazioni sono:
X – Interfaccia disabilitata
R – Interfaccia running, la radio è associata ad un altro apparato.

Finestra General
Name: nome dell'interfaccia
MTU: unità massima di trasmissione il cui valore deve essere un intero compreso tra 68 e 1660, di default è pari a 1500 byte.
MAC Address: Il mac address della scheda radio.
Arp: può essere abilitato, disabilitato, impostato su Proxy Arp o Reply Only . Il Proxy ARP è una tecnica di utilizzo del protocollo ARP per fornire un meccanismo ad hoc di routing, che non richiede la configurazione dell'indirizzo IP del router sugli host. Di default è impostato su Enable.

Finestra Wireless
Radio Name: Nome descrittivo .
Mode: modalità di funzionamento, può essere impostata su alignment-only, usato solo per il posizionamento dell'antenna, ap-bridge, se il dispositivo deve funzionare da Access Point, bridge, se il dispositivo deve funzionare come bridge, nstreme-dual-slave, se l'interfaccia è usata in estreme-dual mode, sniffer, è un modo misto di operare in cui il dispositivo è in grado di catturare pacchetti da tutte le trasmissioni esistenti, station-wds, l'interfaccia lavora come una stazione ma può comunicare con apparati WDS, WDS Slave, l'interfaccia lavora in modalità bridge, ma si adatta alla frequenza dell'altro apparato WDS se questa cambia. Di default è impostato su bridge.
E' ora disponibile una nuova modalità chiamata station-bridge che viene utilizzata per realizzare delle reti trasparent bridged, ossia non ruotate. In questa modalità non sarà necessario utilizzare il WDS che può essere

ignorato.
SSID (Service Set Identifier): Nome della rete collegata al bridge.
Band: Banda di lavoro, può essere impostato su 2.4 GHz-b (IEEE 802.11 b), 2.4 GHz-b/g (IEEE 802.11 g e IEEE 802.11b), , 2.4 Ghz-only g (IEEE 802.11 g), 5 GHz (IEEE 802.11 a fino a 300 Mbit con tecnologia MiMO) . Di default è 5 Ghz.
Frequency: Frequenza di lavoro dell'apparato. Questo valore è ininfluente se abilitato il DFS.
Scan List: Comprende la lista dei canali da poter utilizzare per il collegamento, sono dei valori interi che dipendono dal tipo di banda scelta e dal paese in cui dovrà essere effettuata l'installazione. Di default sono impostati i seguenti valori, 5500, 5520, 5540, 5560, 5580, 5600, 5620, 5640, 5660, 5680, 5670.
Security Profile: E' il profilo di sicurezza che si vuole adottare, inizialmente si può scegliere tra quello di default o l'AES256 . E' possibile crearne anche uno nuovo, per maggiore dettagli vedi la sezione creazione nuovo profilo di sicurezza.
Frequency Mode: definisce quali canali di frequenza sono permessi e la massima potenza erogabile; Può essere impostato su regulatory domain, in questo modo possono essere usati solo i canali previsti e la potenza irradiata non potrà mai superare quella imposta dalle leggi del paese. Con l'impostazione manual-tx-power, la potenza di trasmissione è stabilita dai settaggi nella sezione Tx Power mentre i canali utilizzati sono quelli regolamentati dallo stato considerato. L'opzione Superchannel non può essere attivata. Questo parametro deve essere sempre impostato su regulatory domain.
County: è impostato sul paese in cui viene installato l'apparato. Per installazioni nel territorio nazionale deve essere obbligatoriamente impostato su Italy.
Antenna Gain: E' il guadagno dell'antenna espresso in dBi, questo deve essere impostato in modo tale che vengano rispettate i valori di massima potenze erogabile.
Questo valore va calcolato considerando il gain reale dell'antenna -1/2 db di perdita cavo.
Ad esempio apparati con antenna integrata da 20dbi avranno un gain impostato a 18, mentre apparati con antenna da 23db dovranno avere una valore settato a 21.
⚠Attenzione che la potenza deve essere impostata per rispettare i seguenti valori di potenza all'antenna:
5Ghz. Hiperlan: 30 dBm EIRP
2.4Ghz. WiFi: 20 dBm EIRP
Per maggiori dettagli sul settaggio di questo parametro si veda il manuale di installazione dell'apparato.
Inoltre ci sono limitazioni nell'uso delle frequenze a 5ghz. Infatti i canali compresi tra 5200 e 5300 sono solo per installazioni indoor.
Per installazioni outdoor utilizzare canali da 5500 a 5700.
DFS Mode e TPC: Sono abilitati di default e non disattivabili
Installation: Questo parametro determina la selezione dei canali da utilizzare. Settare su outdoor per installazioni all'aperto, viceversa indoor per installazioni in ambienti chiusi.

Finestra Data Rates
Nella pagina DataRate è possibile impostare le velocità di trasmissione, di norma si lascia impostato il valore di default.

Per trasmissioni MiMo impostare la parte Wireless come di seguito:

```
Wireless
Mode: bridge
Band: 5GHz-only-N
Scan List: 5475-5725
Wireless Protocol: nv2
```

Finestra Advanced

Max Station Count: massimo numero di client a cui è permesso connettersi al bridge, può variare tra 1 e 2007, di default è impostato su 2007.

Ack Timeout (Acknowledgement code timeout): tempo di attesa per l'invio di un frame in cui si trasporta un ack. Può essere impostato in dynamic, quindi il timeout è scelto automaticamente, oppure in indoors, in questo caso il valore di attesa è costante e standard. Di default è impostato su dynamic.

Periodic Calibration: permette di calibrare le prestazioni dei chipset periodicamente in base ai cambiamenti della temperatura e delle condizioni ambientali. Può essere impostato su enable, attivo, disabled, disattivato o default. E' impostato su enable.

Burst Time: tempo, espresso in microsecondi, in cui verranno inviati i dati senza interruzione. Impostato di default a 4 microsecondi.

Hw. retries: Numero di volte che l'invio di frame viene ripetuta senza ritenere un errore di trasmissione. Importante lasciare questo valore impostato a 15.

Adaptive noise immunity: parametro di ottimizzazione anti-disturbo, settarlo su: "ap and client mode"

Preamble mode: definisce la lunghezza del campo di sincronizzazione in un pacchetto wireless. Può essere impostato in long, 128 bit, short, 56 bit, both supporta entrambe le soluzioni. Di default è selezionata la lunghezza short.

Compression: se selezionata attiva la compressione hardware dei dati. E' impostata di default.

Disconnect Timeout: se tale valore è superato, il client si considera disconnesso. Impostato di default a 3 s.

On Fail Retry Time: è l'intervallo di tempo superato il quale si ripete la comunicazione con il dispositivo wireless se la trasmissione dei dati è fallita. Di default è impostato a 100 ms.

Finestra HT

Le voci HT indicano quali antenna Ricevono e quali Trasmettono il segnale.
Per apparati SiSo lasciare di default.

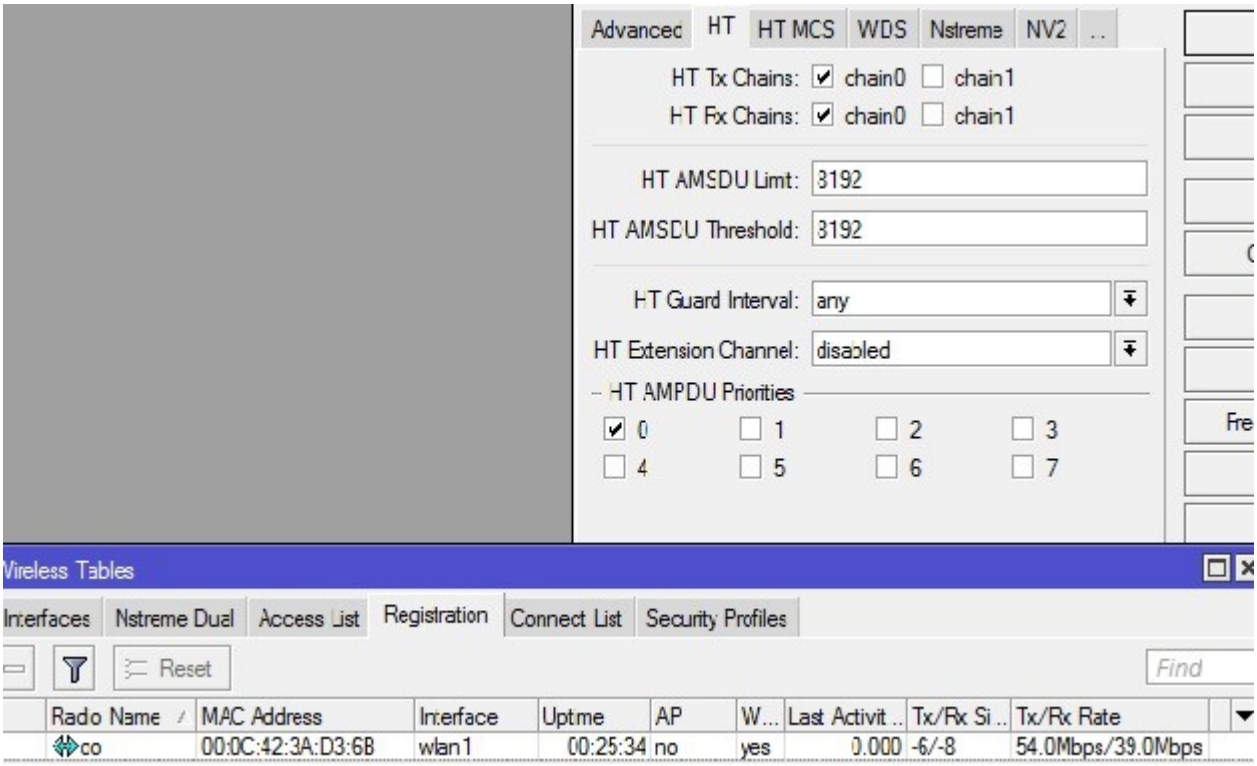
```
Interface <wlan1>

 HT
 Ht Tx Chains [X] 0 (Chain0)
 Ht Rx Chains [X] 0 (Chain0)
```

Per apparati MiMo impostare nel modo seguente per poter utilizzare il protocollo 802.11 n con massime prestazioni.

```
Interface <wlan1>

 HT
 Tx Chains [X] 0 [X] 1
 Rx Chains [X] 0 [X] 1
```

E' possibile allineare separatamente le due chain, basta spuntare su entrambi gli apparati una chain alla volta e cercare di allinearle il meglio possibile in modo di avere il massimo bitrate dal canale.

Di seguito un esembio di allineamento chain0, da notare il valore di segnale troppo basso in quanto era una prova in laboratorio con le antenne molto vicine; ma quest'immagine fa capire l'effettiva possibilità di allineare le chain separatamente ed il rispettivo bitrate del canale



Attenzione!

Abilitare comunque il valore HT Rx su chain 0 qualora si utilizzi solo la chain 1

Finestra WDS

WDS Mode: può essere impostato in disabled, quando le interfacce WDS sono disabilitate, dynamic, quando le interfacce sono create dinamicamente , static, quando le interfacce sono create manualmente. Di defualt è impostato in dynamic.

WDS Default Bridge: imposta le interfacce WDS come bridge. Può essere settato in none, o in bridge1 (default).

Per trasmissioni MiMo impostare il WDS come di seguito:

```
WDS

 WDS Mode:  dynamic
 WDS Default bridge:  bridge1
```

Finestra Nstreme

enable-nstreme: Abilitazione della modalità nstreme.

enable-polling: Utilizzo del polling dei clients.

framer-limit: Dimensione massima del frame.

framer-policy: Politica di accodamanto dei frame. Il protocollo estreme permette di conbinare più pacchetti piccoli all'interno di un singolo pacchetto. Di seguito sono riportate le possibili combinazioni:

none: non combina I pacchetti.

best-fit: inserisce più pacchetti possible all'interno dello stesso frame finchè il limite del frame non è raggiunto. Non frammenta i pacchetti in più frame.

exact-size: inserisce più pacchetti possibili in un frame. Esegue la frammentazione dei pacchetti.
dynamic-size: seleziona la migliore dimensione dinamicamente .
name: nome dell'interfaccia.

Tx Power

Tx-power-mode: indica il modo in cui viene scelto il valore della potenza di trasmissione. Deve essere sempre impostato in default.

Gestione dei profili di sicurezza

Aprire la maschera Wireless Tables->Security Profiles e verificare la presenza dei due profili di default: AES256 e default.

Di seguito viene riportata la configurazione del profilo AES256:

```
Security Profile

 General                          Static Keys
 Name: AES256                     Key 0: aes-ccm
 Mode: static keys required       0x: 6C6163686961766541455 3E86C756E
 RADIUS Mac Authentication:       676133326361726174746572694153434 9
 [  ]                             Key 1: aes-ccm
                                  0x:
                                  Key 2: aes-ccm
                                  0x:
                                  Key 3: aes-ccm
                                  0x:
                                  Trasmit Key: Key 0
                                  St. Private Key: aes-ccm
                                  0x: 6C6163686961766541455 3E86C756E
                                  676133326361726174746572694153434 9
```

Di seguito viene riportata la configurazione dei un profilo WPA-PSK:

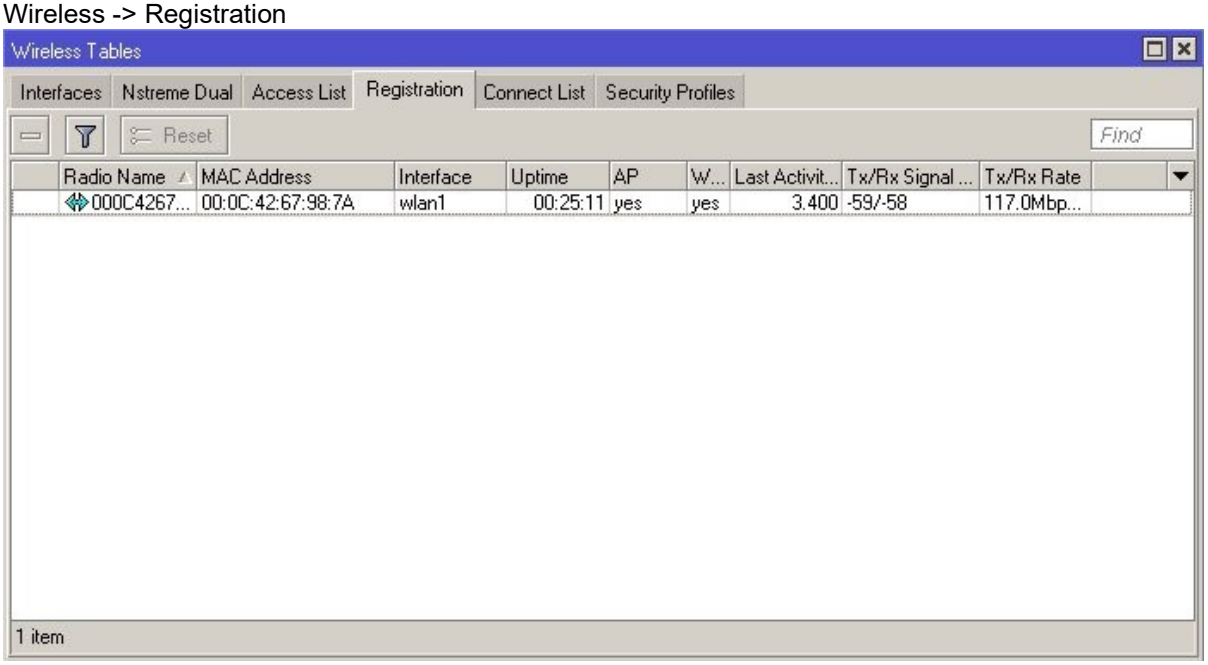
```
Security Profile

 General
 Name: WPA-PSK
 Mode: dynamic-keys
 WPA-PSK: [X]
 WPA-EAP: [  ]
 WPA2-PSK: [  ]
 WPA2-EAP: [  ]
 Unicast chipers tkip: [  ]
 Unicast chipers aes ccm: [X]
 Group chipers tkip: [  ]
 Group chipers aes ccm: [X]
 WPA Pre-Shared Key: a_key
 Group Key Update: 00:05:00
 RADIUS Mac Authentication: [  ]
```

Rimandiamo alla documentazione Mikrotik per una trattazione più approfondita dei singoli parametri.

5. Gestione segnale radio

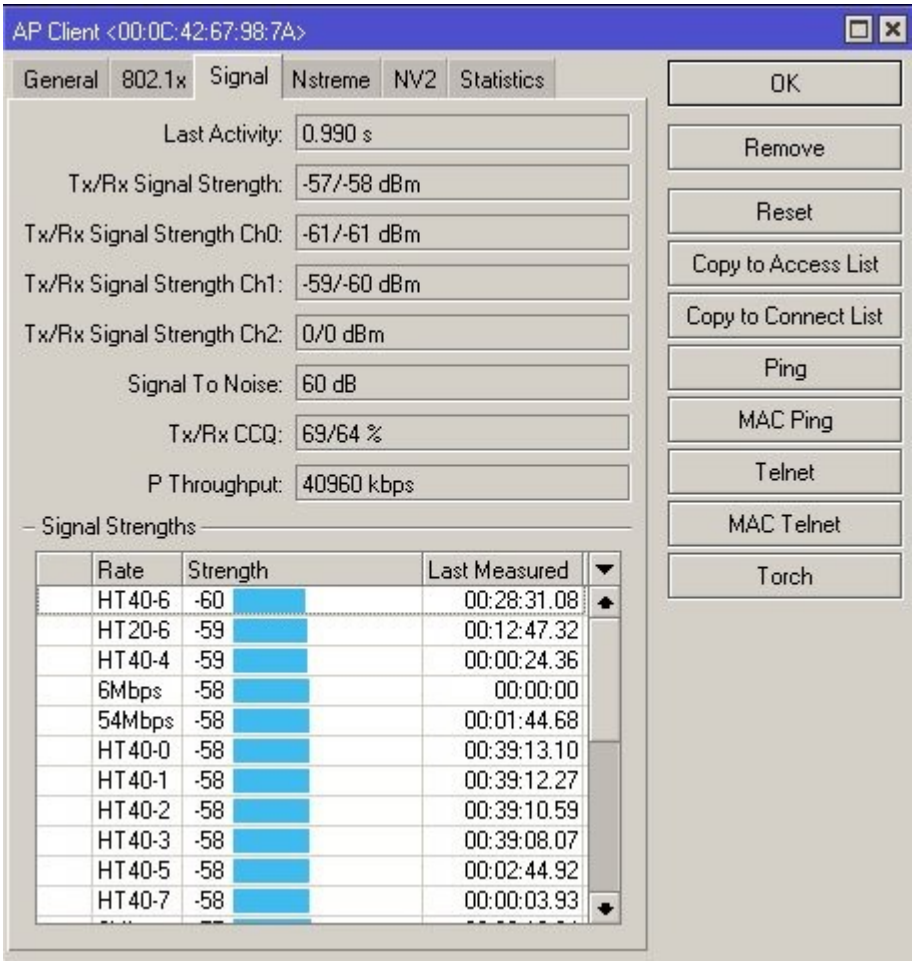
Un buon allineamento è la base per un ponte radio efficace.
Di seguito sono riportate informazioni su come valutare la qualità di un link.

Registration Table
Wireless -> Registration



La tabella della registration table riporta la lista degli apparati collegati ed è il punto di partenza per verificare se il link che si stà realizzando funziona correttamente.
Nell'immagine sopra riportata si può vedere un link con buone caratteristiche di registrazione.
E' importante considerare che le schede radio hanno una sensibilità di circa -90db. Tale valore rappresenta il minimo livello oltre il quale in ponte viene sganciato.
Utilizzare sempre un margine minimo di 10db. per considerare un link fattibile.

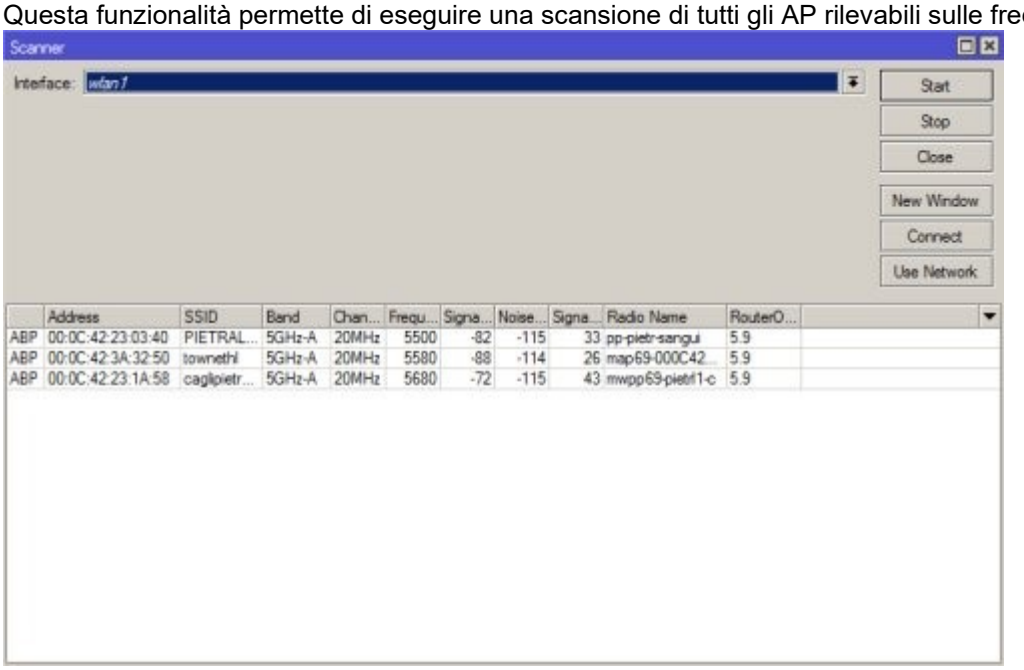
Cliccando due volte sulla riga della registration table si possono osservare maggiori dettagli.



La maschera riporta il segnale ricevuto e trasmesso per ogni chain e, molto importante, il valore CCQ.
Questo valore indica la qualità generale del link ed è un valore percentuale e può essere indicatore di eventuali anomalie o problemi. Un link perfetto deve tendere al 100%.

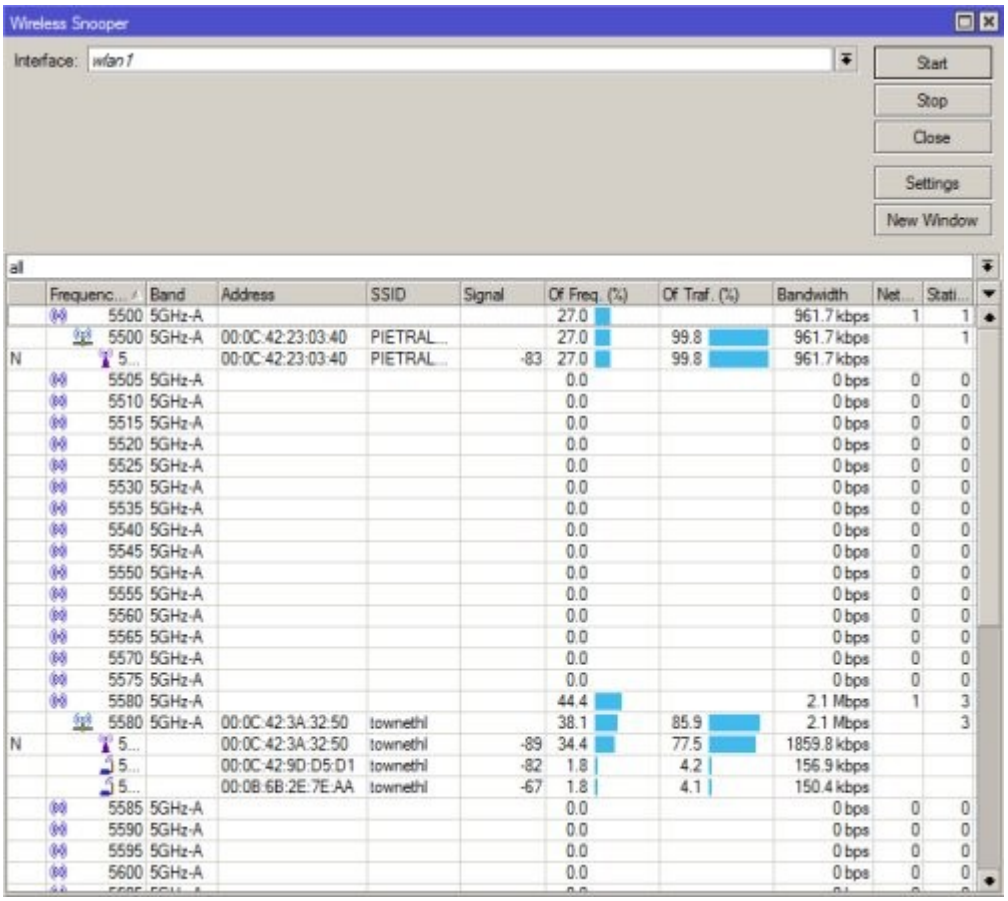
Scan
Wireless -> Interfaces -> Scanner

Questa funzionalità permette di eseguire una scansione di tutti gli AP rilevabili sulle frequenze impostate.



Snooper
Wireless -> Interfaces -> Wireless Snooper

A differenza della funzionalità scan, snooper permette un'analisi più dettagliata di quanto rilevato in aria, comprendente le stazioni client.



Spectral History

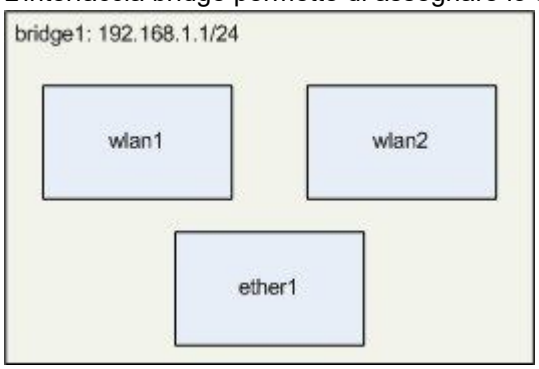
Questo comando è utilizzabile solo da console ed è richiamabile con il seguente comando.
/interface wireless spectral-history range=5500-5700
Permette di eseguire un'analisi di quanto rilevato in aria nel dominio del tempo.
Per essere eseguito richiede il range di frequenze da utilizzare.

6. Configurazione Interfaccia bridge

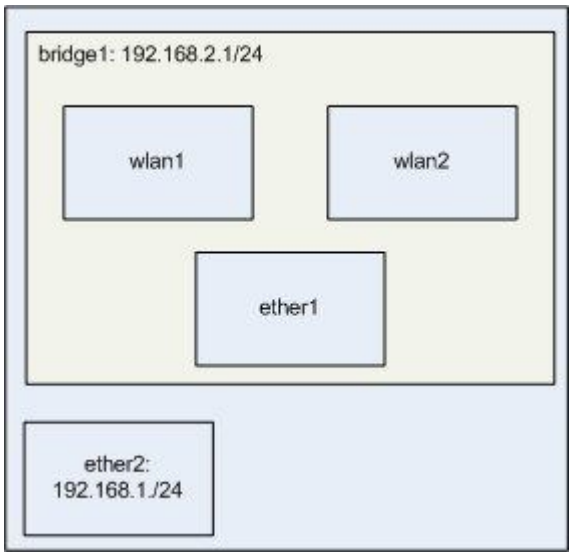
Configurazione Interfaccia Bridge

Applicabile a: Tutti gli apparati

L'interfaccia bridge permette di assegnare lo stesso indirizzo ip a più interfacce.



Esempio 1



Esempio 2

Nell'esempio 1 è stato assegnato un indirizzo ip al bridge che contiene le interfacce wlan1, wlan2 e ether1. In questo tipo di configurazione tutti i pacchetti che entrano in una delle interfacce viene rimandato alle altre interfacce, indipendentemente dall'indirizzamento assegnato agli apparati connessi.
Nell'esempio 2 è stato aggiunto un indirizzo sull'interfaccia ether2. I pacchetti provenienti in quest'ultima interfaccia non verranno smistati nell'interfaccia bridge a meno di configurare un routing tra le due interfacce bridge1 e ether2. Tutto il traffico all'interno dell'interfaccia bridge1 verrà smistato fra i componenti del bridge stesso.

Per configurare un'interfaccia bridge procedere come segue:
Selezionare "Bridge" dal menù principale e premere "+" nella pagina "Bridges". In seguito premere "Ok" confermando i parametri di default.
A questo punto nella pagina "Bridges" comparirà una riga come segue:

Bridge

Bridges

	Name	MAC Address	STP
R	bridge1	00:0C:42:10:80:9A	No

La seconda operazione da eseguire è quella di associare le interfacce al bridge.
Aprire la maschera Bridge->Port->+

Bridge Port

Interface: ether1
Bridge: bridge1
Priority: 128
Path Cost: 10

Nel presente esempio è stata associata l'interfaccia ether1 al bridge1. Nella maschera "Port" comparirà la seguente riga:

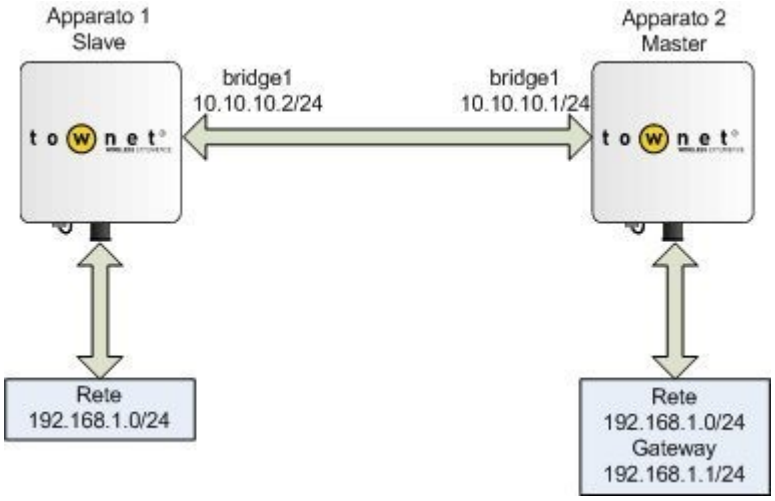
Bridge

Bridges

Interface	Bridge	Priority	Path cost	Status
ether1	bridge1	128	10	Forwarding

Procedere in maniera analoga per tutte le interfacce da inserire nel bridge.

Esempio Bridge con due apparati P-P
L'esempio riporta la configurazione di due apparati P-P in modalità Bridge (configurazione di default).



In una configurazione di questo tipo, come esposto nei paragrafi precedenti, ogni host collegato alla rete dietro l'apparato 1 appartiene allo stesso dominio di collisione degli host collegati a valle dell'apparato 2, come se vorremo collegati con due switch.
Di seguito viene riportata la configurazione di uno degli apparati. L'unica differenza tra i due apparati è posta nella configurazione della scheda radio che deve essere impostata in modalità "Bridge" (P-P Master) o "Ap-Bridge" (Base Station) nell'apparato master e "Station-Wds" nell'apparato slave. Ambedue gli apparati devono avere il Wds abilitato sull'interfaccia bridge.

Apparato 1

Address List

Port

Address	Network	Broadcast	Interface
10.10.10.2/24	10.10.10.0	10.10.10.255	bridge1

Route List

Router

	Destination	Gateway	Pref.Source	Distance	Interface	RouteMask
DAC	10.10.10.0/24		10.10.10.2		bridge1	

Come si vede dalla configurazione sopra riportata, in una situazione del genere non è necessario specificare alcuna rotta statica o gateway.

7. Configurazione indirizzi IP

Applicabile a: Tutti gli apparati

Il software permette di inserire un numero qualsiasi di indirizzi ip assegnati alle interfacce fisiche o virtuali dell'apparato.

Per inserire un indirizzo ip
Aprire la maschera Ip->Address List->+

New Address

address: 192.168.1.10/24

Network:

Broadcast:

Interface: ether1

Come indicato nell'esempio sopra riportato non è necessario specificare il parametro Network e Broadcast che verrà calcolato dal sistema. Il risultato del precedente esempio sarà il seguente:

Address List

	Address	Network	Broadcast	Interface
	192.168.1.10/24	192.168.1.0	192.168.1.255	ether1
D	83.211.20.126	83.211.20.2	0.0.0.0	pppoe-out1

In questo esempio è riportato anche un indirizzo dinamico acquisito dall'interfaccia pppoe. Si veda la sezione di configurazione di un client in modalità pppoe per maggiori dettagli.

Utilizzare il tasto "-" per eliminare l'indirizzo dalla lista.

⚠Fare attenzione perché il software non chiede alcuna conferma e la modifica è immediatamente attiva.

8. Configurazione del Routing

Applicabile a: Tutti gli apparati

Routing Table
Aprire la maschera Ip->Routes

Route List

Routes

	Destination	Gateway	Pref.Source	Distance	Interface	Routing Mask
AS	0.0.0.0/24	10.10.10.2		1	bridge1	
DAC	10.10.10.0/24		10.10.10.5		bridge1	

Il precedente esempio riporta l'assegnazione di un gateway e una rotta dinamica creata dal sistema. La rotta dinamica 10.10.10.0/24 viene aggiunta in automatico dopo aver configurato l'indirizzo ip.

Rotte statiche e gateway
Per aggiungere una rotta statica alla routine table procedere come segue:
Aprire la maschera Ip->Routes->+

New Address

Destination: 0.0.0.0/24
Gateway: 10.10.10.2
Check Gateway:
Distance:
Mark:
Pref.Source:

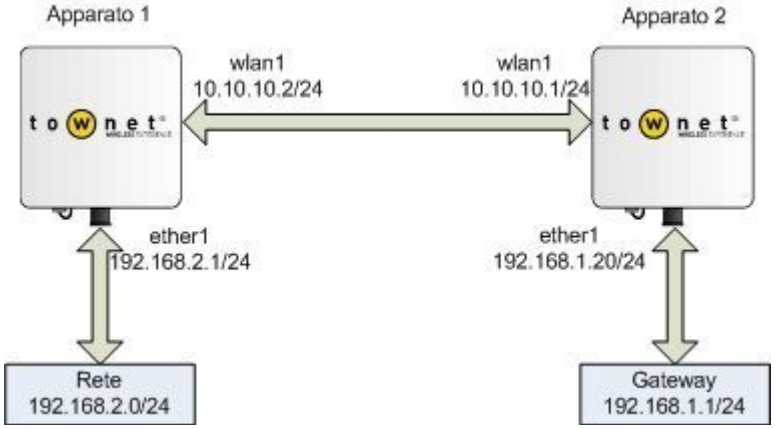
Nell'esempio è stato inserito un gateway verso l'indirizzo 10.10.10.2.
Analogamente al gateway, possono essere inserite anche rotte statiche verso altre reti. Ad esempio supponiamo di voler inserire una rotta verso la rete 10.10.9.0/24:

New Route

Destination: 10.10.9.0/24
Gateway: 10.10.8.2
Check Gateway:
Distance:
Mark:
Pref.Source:

Ovviamente per rendere operativa questa rotta deve essere assegnato un indirizzo della classe 10.10.8.0/24 in una delle interfacce del sistema.

Esempio Routing con due apparati P-P
Di seguito si riporta un esempio di configurazione di due apparati Punto Putno (108-20-BR) in modalità ruotata.



Apparato 1

Address List

Port

Address	Network	Broadcast	Interface
10.10.10.2/24	10.10.10.0	10.10.10.255	wlan1
192.168.2.1/24	192.168.2.0	192.168.2.255	ether1

Route Listo

Routes

	Destination	Gateway	Pref.source	Distance	Interface	Routing Mask
AS	0.0.0.0/0	10.10.10.1			wlan1	
DAC	10.10.10.0/24		10.10.10.2		wlan1	
DAC	192.168.2.0/24		192.168.2.1		ether1	

Apparato 2

Address List

Port

Address	Network	Broadcast	Interface
10.10.10.1/24	10.10.10.0	10.10.10.255	wlan1
192.168.1.20/24	192.168.1.0	192.168.1.255	ether1

Route Listo

Routes

	Destination	Gateway	Pref.source	Distance	Interface	Routing Mask
AS	0.0.0.0/0	10.10.10.1			wlan1	
DAC	10.10.10.0/24		10.10.10.1		wlan1	
DAC	192.168.1.0/24		192.168.1.20		ether1	
AS	192.168.2.0/24	10.10.10.2			wlan1	

⚠E’ importante precisare che in una configurazione ruotata l’interfaccia radio va configurata diversamente rispetto ad una configurazione in bridge, come di seguito riportato:

Apparato Master
Modificare l’impostazione WDS a "disabled” e l’impostazione WDS Default Bridge a "none”.

Apparato Slave
Modificare l’impostazione WDS a "disabled” e l’impostazione WDS Default Bridge a "none”.
Modificare l’impostazione Wireless Mode a "station”.

9. Configurazione del Firewall

Applicabile a: Tutti

Ogni apparato townet è fornito di un potente firewall. Di seguito verranno illustrate le principali procedure adottate nell'utilizzo del firewall. Per una trattazione più approfondita si rimanda alla documentazione Mikrotik.

Il firewall è suddiviso in tre diverse sezioni: Filter Rules, NAT e Mangle. Il primo permette di filtrare i pacchetti che passano attraverso il router ed effettuare delle azioni in funzione del filtro. Il secondo permette di eseguire il nat degli indirizzi e il terzo permette di marchiare i pacchetti per riconoscerli in altre operazioni.
Tutte le righe di ogni regola vengono processate nell'ordine in cui sono inserite dall'alto verso il basso, ma possono essere modificate trascinando con il mouse la riga desiderata nella posizione corretta.

Filter Rules
Le regole di filtro permettono di eseguire delle azioni in funzione di un filtro di ricerca impostabile dall'utente.
Premendo il puldante "+" si apre la finestra Firewall Rule che è suddivisa in 5 schede. Le schede "General", "Advanced" e "Extra" permettono di individuare i pacchetti. La scheda "Action" permette di definire l'azione che deve essere intrapresa in funzione del filtro. La scheda "Statistics" rappresenta il grafico dell'attività della regola ed è estremamente utile per verificare il funzionamento della stessa.

Di seguito viene riportato un esempio di applicazione di due regole.
Aprire la maschera Ip->Firewall->Filter Rules->+

New Firewall Rule

General	**Action**
Chain: input Protocol: 6 (tcp) Dst. Port: 80 In. Interface: ether2	Action: accept

New Firewall Rule

General	**Action**
Chain: input Protocol: 6 (tcp) Dst. Port: 0-65535 In. Interface: ether2	Action: drop

Aprendo la maschera Ip->Firewall->Filter Rules verranno visualizzate due righe che identificano le due regole che operano come segue:
Ragola 1
Accetta tutti i pacchetti nella catena di input, sul protocollo tcp, destinati alla porta 80 e provenienti dall'interfaccia ether2.
Regola 2
Scarta tutte le richieste nella catena di input, sul protocollo tcp, su tutte le porte e provenienti dall'interfaccia ether2.

NAT

Le operazioni prevalentemente attivate su questa scheda sono di “Masquerade” e di “Nat”.
Premendo il puldante “+” si apre la finestra New NAT Rule che è suddivisa in 5 schede. Le schede “General”, “Advanced” e “Extra” permettono di individuare i pacchetti. La scheda “Action” permette di definire l’azione che deve essere intrapresa in funzione del filtro. La scheda “Statistics” rappresenta il grafico dell’attività della regola ed è estremamente utile per verificare il funzionamento della stessa.

Di seguito riportiamo due esempi:

Aprire la maschera Ip->Firewall->NAT->+

New NAT Rule

General	**Action**
Chain: srcnat	Action: masquerade

Aprire la maschera Ip->Firewall->NAT->+

New NAT Rule

General	**Action**
Chain: dstnat Protocol: 6 (tcp) Dst. Port: 22 In. Interface: pppoe-out1	Action: masquerade To Addresses: 192.168.1.100 To Ports: 22

Aprire la maschera Ip->Firewall->NAT->+

New NAT Rule

General	**Action**
Chain: dstnat Protocol: 17 (udp) Dst. Port: 514 In. Interface: pppoe-out1	Action: masquerade To Addresses: 192.168.1.100 To Ports: 514

Gli esempi sopra riportato operano come segue:
Regola 1
Esegue il “Masquerade” di tutti i pacchetti in uscita. Questa regola è fondamentale quando l’apparato è un gateway di rete, infatti tutti i pacchetti che escono verso l’esterno avranno come mittente l’indirizzo (esterno) dell’apparato e non della macchina che l’ha generato.
Regola 2
Apre la porta 22 (ssh) verso una macchina interna (192.168.1.100) sul protocollo tcp.
Regola 3
Apre la porta 514 (logs) verso una macchina interna (192.168.1.100) sul protocollo udp.

Notare che l’interfaccia di entrata delle regole 2 e 3 è la pppoe-out1. Ciò indica che il router possiede una connessione pppoe verso l’esterno. Qualora il router sia connesso direttamente ad un’altra rete senza pppoe si utilizzerà una delle interfacce fisiche dell’apparato come ad esempio ether1 o wlan1.

 Affinché le regole di Nat operino correttamente accertarsi che sia abilitata la funzionalità “Connection Tracking” abilitabile sulla maschera Ip->Firewall->Connections->Tracking, Enabled = on.

Mangle
La funzionalità di Mangle viene utilizzata per marchiare dei pacchetti o per modificare l’header del pacchetto IP come ad esempio il TOS o il TTL. Questo tipo di marchiatura viene eseguita all’interno del router e la modifica del pacchetto non viene trasmessa fuori dall’apparato.
Questo tipo di marchiatura viene in seguito elaborata da altri processi come ad esempio il NAT e la gestione delle code, che la utilizzano per riconoscere particolari pacchetti.
Di seguito si riporta un esempio di marchiatura pacchetti sul protocollo ICMP:

Aprire la maschera Ip->Firewall->Mangle->+

New Mangle Rule

General	**Action**
Chain: prerouting Protocol: 1 (icmp) Dst. Port: 514 In. Interface: pppoe-out1	Action: mark connection New Connection Mark: Ping-Conn Passthrough: [X]

Aprire la maschera Ip->Firewall->Mangle->+

New Mangle Rule

General	**Action**
Chain: prerouting Connection Mark: Ping-conn	Action: mark_packet New Packet Mark: Ping Passthrough: [ ]

Le due regole appena definite agiscono comee di seguito indicato:
La prima identifica la connessione icmp e la marchia con nome Ping-Conn.
La seconda marchia il pacchetto con il nome Ping in base alla regola sopra definita.
Il valore Passthrough, quando selezionato, indica al processore di continuare a controllare le regole seguenti altrimenti termina il lavoro in quella regola.

Come già illustrato in precedenza le tab General, Advanced e Extra servono per definire le regole di individuazione e la tab Action per definire l'azione da intraprendere.

10. Configurazione di un client in modalità PPPoE

Applicabile a: 108-40-SU, 108-30-SU

Si seguito viene illustrata la procedura di configurazione di un ClientCPE 108-30-SU in modalità Client PPPoE.

Il modello client PPPoE viene essenzialmente utilizzato da reti gestite da WISP dove la banda ad ogni punto terminale è gestita da un Subscriber Server, o anche definito concentratore.
Gli scenari applicativi ove localizzare il subscriber Server possono essere molteplici, in funzione del risultato da raggiungere.
La configurazione che segue risulta comunque comune a qualsiasi modello di concentratore utilizzato.
L'esempio utilizzerà il client come gateway della rete interna sulla classe 192.168.1.0/24, con server DHCP abilitato.

Ogni 108-30-SU viene rilasciato con una configurazione che gli permette di agganciarsi a qualsiasi Base Station con SSID Townet, Nstream abilitato e modalità di lavoro dell'interfaccia wireless settata a station WDS.
Si presuppone che la macchina in dotazione sia configurata in modalità standard. Qualora non lo fosse si consiglia di leggere la parte del manuale che spiega come resettare l'apparato ai parametri di default.

```
Addresses: 192.168.1.1/24
Interface: Ether1
```

Configurazione generale
Indirizzo IP della rete interna
Aprire la maschera IP->Addresses ed aggiungere l'indirizzo IP 192.168.1.1/24 con i parametri seguenti:

```
admin@108-30-SU>ip address add
address: 192.168.1.1/24
interface: ether1
```

Definizione di un pool di indirizzi
Al fine di utilizzare il server DHCP è necessario definire un pool di indirizzi ip da rilasciare alle macchine che ne fanno richiesta.
Aprire la maschera IP->Pool ed aggiungere un pool di indirizzi che va da 192.168.1.20 a 192.168.1.100

```
Name: pool1
Interface: 192.168.1.20-192.168.1.100
Next pool: none
```

Configurazione DNS
Aprire la maschera IP->DNS->Settings ed inserire I seguenti valori

```
Primary DNS:
Secondary DNS:
Allow Remote Requests: [ ]
Cache Size: 2048
```

Server DHCP
Aprire la maschera IP->DHCP Server.
Nella Tab DHCP, inserire un nuovo server con i seguenti valori:

```
Name: server1
Interface: ether1
Relay: [ ]
Lease Time: 3d 00:00:00
Address Pool: static-only
Authoritative: after 2s delay
Bootp support: [v]
Add ARP For Lease: [ ]
Always Broadcast: [ ]
Use RADIUS: [ ]
```

Nella Tab Networks aggiungere una nuova DHCP Network:

```
Addresses: 192.168.1.0/24
Gateway: 192.168.1.1
Netmask: 24
DNS servers:
DNS servers:
```

Firewall
Affinchè i pacchetti passino attraverso il router ed abbiano la strada per tornare indietro è necessario attivare la funzionalità di NAT Masquerading.
Aprire la maschera IP->Firewall ed aggiungere una nuova regola nella Tab NAT con i seguenti valori:

```
Chain: srcnat
Action: masquerade
```

E' fondamentale abilitare la funzione Connection Tracking nella maschera:
IP->Firewall->Connections->Tracking

Configurazione del Client PPPoE
Dal menù PPP creare una nuova interfaccia PPPoEClient con i seguenti parametri:

```
Name: pppoe-out2
Max MTU: 1480
Max MRU: 1480
Interface: wlan1
User:
Password:
Profile: Default
Add Default Route: [v]
Pap: [v]
Chap: [v]
Mschap1: [v]
Mschap2: [v]
```

Nella lista comparirà la dicitura pppoe-out2 relativa all'interfaccia client appena configurata. Se tutte le operazioni sono state condotte correttamente, il sistema è ora in grado di connettersi al concentratore più vicino utilizzando l'user name e la password forniti. Il sistema è inoltre in grado di rilasciare gli indirizzi per la rete privata e funzionare da gateway.

Utilizzo del Firewall
Al fine di aumentare la sicurezza del sistema è bene adottare una serie di regole sul firewall che impediscano a malintenzionati di accedere alla rete interna.
Di seguito sono riportate una serie di regole basilari:
Rimozione della risposta al protocollo ICMP (Ping)
Blocco di tutte le attività in entrata.

Di seguito sono riportati i due esempi di configurazione.

Rimozione della risposta al protocollo ICMP (Ping)
Aprire la maschera IP->Firewall ed aggiungere una nuova regola sulla Tab Filter Rules:

```
Chain: input
Protocol: 1 (icmp)
Interface: wlan1

Action: drop
```

Blocco di tutte le attività TCP sull'interfaccia esterna
Aprire la maschera IP->Firewall ed aggiungere una nuova regola sulla Tab Filter Rules:

```
Chain: input
Protocol: 6 (tcp)
Dst. Port: 0-65535
Interface: wlan1
```

Action: drop

Qualora fosse necessario raggiungere una macchina nella rete interna, sarà necessario aprire le porte relative al servizio che si vuole erogare. Di seguito riportiamo un esempio dove viene aperta la porta per poter raggiungere un server https interno alla rete.

Aprire la maschera IP-Firewall->NAT ed aggiungere una nuova regola con la seguente configurazione:

Chain: dstnat
Protocol: 6 (tcp)
Dst. Port: 443
In. Interface:pppoe-out1
Dst. Port: 0-65535

Action: dst-nat
ToAddress:
To Ports: 443

11. Configurazione di un Hotspot

Applicabile a: 108-40-HS, 108-30-HS

Un sistema hotspot rappresenta il punto di accesso per utenze nomatiche. L'accesso alla rete è garantita dal'inserimento di una user name e una password.
Ogni utente può collegare il proprio terminale, di solito un portatile, alla rete wireless ma non può accedere ai serizi di rete se non inserisce i dati di autenticazione.
La configurazione di ogni parametro è abbastanza complessa soprattutto perché devono essere create numerose regole di firewall. Il metodo più semplice è senz'altro quello di utilizzare il Wizzard messo a disposizione che guida l'utente attraverso la configurazione del apparato HotSpot.

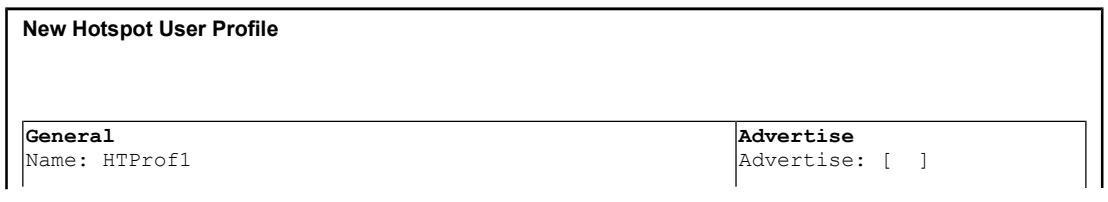
Configurazione Generale
Di seguito si riporta l'esempio a terminale:

```
[admin@108-40-HS] > ip hotspot
[admin@108-40-HS] ip hotspot> setup
hotspot interface: wlan1
local address of network: 10.5.50.1/24
masquerade network: yes
address pool of network: 10.5.50.20-10.5.50.254
select certificate: none
ip address of smtp server: 0.0.0.0
dns servers: 212.97.32.2
dns name:
[admin@108-40-HS] >
```

hotspot interface: E' l'interfaccia su cui si appoggia l'hotspot, generalmente wlan1.
local address of network: E' l'indirizzamento assegnato alla rete wireless.
masquerade network: Definisce se attivare il masuerade sui pacchetti in uscita dal router.
address pool of network: Definisce il pool di indirizzamento che il server DHCP rilascerà agli utenti connessi sull'interfaccia wireless.
select certificate: Seleziona un certificato dalla lista dei certificati importati, generalmente lasciato a none.
ip address of smtp server: Indirizzo del server smtp a cui ridirigere le richieste snmp.
dns servers: Indirizzo del server dns.
dns name: Nome del server dns.

Gestione Utenti
La seconda fase della creazione di un serizio hotspot è la gestione degli account utente che può essere gestita attraverso la maschera IP->Hotspot->Users.
Ogni utente è collegato ad un profilo che deve essere definito. Il software è dotato di un profilo già caricato che si chiama default. Questo profilo può essere modificato ma non deve essere cancellato.

Aprire la maschera IP->HotSpot->Users->Profiles->+



```
Address Pool: hs-pool-2
Session Timeout: [  ] [     ]
Idle timeout: none
Keepalive Timeout: [X] 00:02:00
Status autorefresh: 00:01:00
Shared Users: [X] 1
Rate Limit (tx/rx): 640k/256k
Open Status Page: always
Trasparent Proxy: [  ]
```

L'esempio sopra riportato illustra I parametri principali. Gli altri possono essere lasciati vuoti.

Name: Nome del profilo.
Address Pool: Nome del pool di indirizzamento definito con il wizzard.
Session Timeout: Tempo limite assegnato all'utente oltre il quale viene disconnesso.
Session Timeout: Tempo limite assegnato all'utente oltre il quale viene disconnesso.
Idle Timeout: Tempo limite di inattività dell'utentea oltre il quale viene disconnesso.
Keepalive timeout: Tempo limite entro il quale il computer dell'utente deve essere raggiungibile. Se viene superato l'utente è disconnesso.
Status Autorefresh: Intervallo di refresh della pagina di status che appare dopo il login al servizio.
Shared Users: Numero massimo di utenti simultanei con lo stesso nome. Di norma impostato a 1.
Rate Limit: Limite di banda assegnato all'utente. Il valore immesso è in bits/sec dove tx rappresenta il download per l'utente e rx l'upload per l'utente.
Open Status Page: Identifica se deve essere visualizzata la pagina di status anche per utenti autenticati con il solo mac-address. Di norma si imposta ad always.
Trasparent Proxy: Impostare se viene utilizzato un Trasparent Proxy per gli utenti autenticati.
Advertise: Abilita la possibilità di visualizzare delle pagine pubblicitare tramite finestre popup.

Aprire la maschera IP->HotSpot->Users->+

New Hotspot User

General	**Limits**
Server: All	Limit Uptime: [ ]
Name: test	Limit Bytes In: [ ]
Password: test	Limit Bytes Out: [ ]
Address: [ ]	
MAC Address: [ ]	
Profile: default	

L'esempio sopra riportato illustra I parametri principali per la configurazione di un utente.
Server: Nome del server hotspot a cui l'utente è collegato (si possono avere più server hotspot sulla stessa macchina).
Name: User Name.
Password: Password assegnata all'utente.
Address: Indirizzo statico assegnato all'utente.
MAC Address: Se viene specificato un mac address, l'utente può autenticarsi solo con quel mac address.
Profile: Nome del profilo assegnato all'utente.
Limit Uptime: Tempo limite di connessione per l'utente.
Limit Bytes In: Massima quantità di bytes ricevibile dall'utente.
Limit Bytes Out: Massima quantità di bytes inviabile dall'utente.

Walled Garden

Il Walled Garden permette di rendere raggiungibili alcuni servizi senza la necessità di autenticare l'utente. Ad esempio un operatore potrebbe rendere visibile il proprio sito internet o un'ammistrazione pubblica una serie di

servizi.

Aprire la maschera IP->HotSpot->Walled Garden->+

New Garden Entry

General
Action: Allow [X]
Dst. Host: www.google.com

L’esempio sopra riportato permette ad un utente non registrato di raggiungere il sito www.google.com. Non potrà raggiungere nessun altro dominio.
Il seguente esempio limita l’accesso al solo indirizzo ip

Aprire la maschera IP->HotSpot->Walled Garden->+

New Garden Entry

General
Action: Allow [X]
Dst. Address: 209.85.135.147

IP Accounting

L'ip accounting è il metodo per poter collezionare il traffico effettuato da un hotspot. I dati di traffico degli utenti vengono collezionati prelevando la lista da questo indirizzo: http://routerIP/accounting/ip.cgi.
Ad ogni lettura la memoria del router viene azzerata. E' importante definire bene la lunghezza dello spazio di memoria riservato al numero di righe registrate. Tale valore, ip->accounting->traffic_accounting è settato con il valore di Threshold. Impostare tale valoe ad almeno 3000 per essere certi di collezionare tutto il traffico.
Per abilitare questo servizio selezionare ip->accounting->traffic_accounting->enable_accounting e rendere disponibile il servizio sul web con ip->accounting->web_access->accessible_via_web.
fare attenzione che il servizio web sia abilitato nel menù ip-services.

12. Guida passo passo configurazione HotSpot

Per una corretta installazione e configurazione di un Hotspot seguire le indicazioni riportate di seguito

1
Aggiornare RouterOS all'ultima versione.

2
Resetta il router

3
Accedi in mac-winbox

4
Se sulla rete è presente un DHCP server continua, altrimenti passa al punto 6

5
Imposta un DHCP client sulla porta connessa al tuo router gateway (WAN) tramite il comando:
`/ip dhcp-client add interface=[interfaccia WAN] disabled=no`
passa al punto 8

6
Aggiungi sulla porta connessa al tuo router (WAN) un indirizzo corretto e libero sulla tua rete tramite il comando:
`/ip address add address=x.x.x.x netmask=x.x.x.x interface=[interfaccia WAN]`

7
Aggiungi una default route per raggiungere internet tramite il seguente comando:
`/ip route add dst-address=0.0.0.0/0 gateway=[indirizzo del gateway]`

8
Aggiungi il DNS e imposta il DNS caching tramite questo comando:
`/ip dns set servers=8.8.8.8,8.8.4.4 allow-remote-requests=yes`

9
Aggiungi la VPN SSTP per raggiungere il radius server OOrl/Waver con il seguente comando:
`/interface sstp-client add connect-to=212.104.1.244 user=[tuo utente vpn] password=[tua password vpn]`

10
Definisci una rotta per raggiungere il radius server con il seguente comando:
`/ip route add dst-address=10.10.0.0/16 gateway=10.10.0.1`

11
Attiva la funzionalità HotSpot tramite il wizard seguente:
`/ip hotspot setup`

Rispondi ai vari steps come qui di seguito:
Select interface to run HotSpot on

hotspot interface: [interfaccia dove vuoi abilitare l'HotSpot]
Set HotSpot address for interface

local address of network: 10.5.50.1/24
masquerade network: yes
Set pool for HotSpot addresses

address pool of network: 10.5.50.10-10.5.50.250
Select hotspot SSL certificate

select certificate: none
Select SMTP server

ip address of smtp server: 0.0.0.0
Setup DNS configuration

dns servers: 10.5.50.1
DNS name of local hotspot server

dns name:

Finito !

12
Una volta creato l'hotspot cambiagli il nome con uno + specifico, per esempio "ristorante_pino"
```
/ip hotspot set name=ristorante_pino
```

13
Aggiungi il server RADIUS al router con il seguente comando:
```
/radius add address=10.10.0.2 service=hotspot secret=[quella impostata]
authentication-port=1812 accounting-port=1813 timeot=3s
/radius incoming set accept=yes port=1700
```

* Attenzione! le porte di autenticazione e di accounting potrebbero essere diverse in accordo con la piattaforma radius

14
Abilita l'HotSpot ad usare il server radius esterno ed abilita il radius accounting:
```
/ip hotspot profile set hsprof1 use-radius=yes radius-accounting=yes radius-interim-
update=00:01:00
```
* Attenzione! assumendo che "hsprof1" sia il profilo attualmente collegato all'hotspot.

15
Abilita IP accounting per loggare le sessioni nattate con i seguenti comandi:
```
/ip accounting set enabled=yes threshold=8000
/ip accounting web-access set accessible-via-web=yes address=10.10.0.2
```

16
Popola il walled-garden con tutte le destinazioni comunque accessibili anche senza autenticazione, sia quelli obbligatori che quelli facoltativi (es www.townet.it):
```
/ip hotspot walled-garden
add action=allow comment=Townet disabled=no dst-host=www.townet.it

/ip hotspot walled-garden ip
add action=accept comment="Server Radius" disabled=no dst-address=10.10.0.2
```

se utilizzi OOrl passa al punto 18, altrimenti continua

17
Ricorda di aggiungere al walled garden l'IP oppure il dominio/host del server web che ospita il tuo captive-portal personalizzato nella seguente forma:
```
/ip hotspot walled-garden ip
add action=accept comment="captive-esterno" disabled=no dst-address=x.x.x.x
```
oppure
```
/ip hotspot walled-garden
add action=allow comment=captive-esterno disabled=no dst-host=www.miosito.it
```

18
Sostituisci la pagina di default del captive portal (login.html) con la versione corretta.
Caricala con FTP, oppure trascinala nella finestra files della winbox, ma fai attenzione a caricarla sulla radice della cartella hotspot.
Ricordati di cambiare i riferimeti di redirect con l'esatta ubicazione del tuo portale, e se dovesse essere su un server esterno aggiungi il suo indirizzo al walled garden (punto 16)

19
Imposta il client NTP e il fuso orario corretto per allineare i log al radius.
```
/system ntp client
```

```
set enabled=yes mode=unicast primary-ntp=10.10.0.1 secondary-ntp=193.204.114.233
/system clock
set time-zone-name=Europe/Rome
```

20

Assicurati che le seguenti impostazioni siano abilitate/corrette:

```
/ip service
set www address=0.0.0.0/0 disabled=no port=80
set www-ssl address=0.0.0.0/0 certificate=none disabled=yes port=443
set api address=0.0.0.0/0 disabled=no port=8728
```

*il servizio SSL ha bisogno di un certificato, altrimenti disabilitalo.

```
  set winbox address=0.0.0.0/0 disabled=no port=8291

/ip firewall connection tracking
set enabled=yes
```

21

Dai un nome al router:

```
/system identity
set name="OOrl_albergo_pio"
```

13. Utilizzo Certificati SSL

Creazione del certificato
Di seguito viene riportato un esempio di importazione di un certificato per accesso SSL utilizzando il servizio gratuito rilasciato da www.cacert.org.

La prima operazione da eseguire è quella di esportare la richiesta di certificato:

```
Creazione richiesta
/certificate create-certificate-request
```

Il sistema richiederà l'inserimento di una serie di informazioni relative al certificato. Utilizzare Townet come Passphrase.
Una volta terminata la procedura verrà creato il file certificate-request.pem che dovrà essere scaricato dall'apparato via FTP o trascinando il file stesso su una cartella del proprio pc.

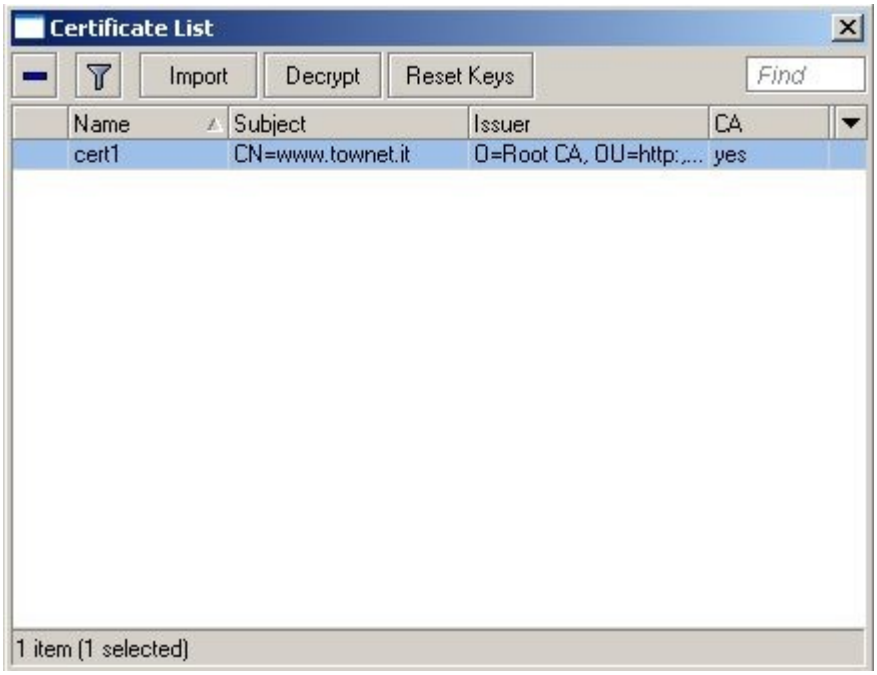
Collegarsi al sito www.cacert.org ed accedere al proprio account.
Cliccare nel link "New Server certificates" e copiare il contenuto del file certificate-request.pem all'interno della maschera di richiesta del sito web.
Alla fine dell'operazione il sistema proporrà un risultato che apparirà simile a quanto riportato di seguito.

Copiare il testo all'interno di un nuovo file che potremo chiamare certificate-response.pem. Caricare questo file all'interno dell'apparto con uno dei metodi conosciuti.

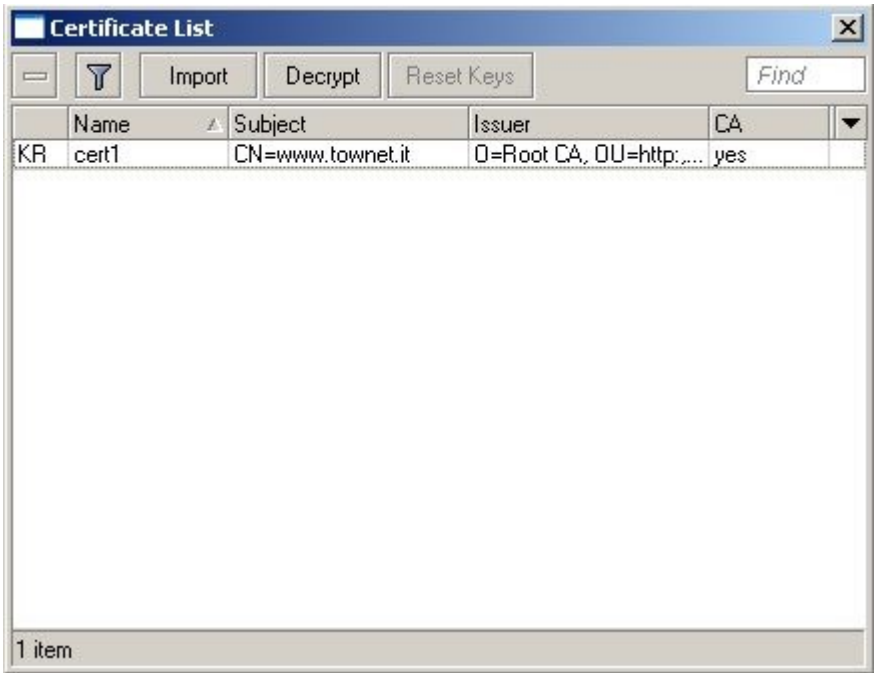
Importazione del certificato
Una volta caricato il file certificate-response.pem accedere al seguente menù:

```
Certificates
Import
Only File: certificate-response.pem
Pssphrase: Townet
```

Di seguito un esempio del certificato caricato.



Importare infine il file private-key.pem generato durante la creazione della richiesta di certificato. Alla fine della procedura comparirà un "KR" a fianco della definizione del certificato. Di seguito un esempio.



14. Utilizzo di SNMP

RouterOS supporta il protocollo SNMP nelle versioni V1 e V2.

Configurazione SNMP in lettura

Dal terminale:

```
/snmp print
           enabled: yes
           contact: "rtmtc"
          location: "rtmtc"
         engine-id: ""
      engine-boots: 4
       time-window: 15
         trap-sink: 192.168.1.34
    trap-community: public
      trap-version: 1
  trap-generators: start-trap,interfaces
```

Per abilitare l'SNMP in lettura è necessario settare i parametri essenziali come di seguito illustrato.

```
/ snmp community
set public name="public" address=0.0.0.0/0 read-access=yes
```

Per abilitare il servizio

```
/ snmp set enabled=yes
```

Abilitazione di SNMP Trap
RouterOS supporta le trap in due modalità:
Automatica da sistema
Manuale da riga di comando

Per abilitare SNMP Trap si devono settare i seguenti parametri:
trap-generator
E' la sorgente della trap e può essere interfaces o start-trap
trap-sink
E' l'ip della macchina che riceverà il pacchetto Trap.

```
/ set trap-generators=interfaces trap-sink=192.168.1.34
```

15. Puntamento e sistemi di ottimizzazione

Una delle operazioni più delicate è rappresentata dal puntamento e l'ottimizzazione dei ponti radio. Il puntamento comprende una serie di operazione e richiede delle conoscenze essenziali della teoria delle onde radio.

Gli esempi che seguono sono concentrati sull'allineamento di due apparati Punto-Punto 108-20-BR.

La prima operazione da eseguire è quella di effettuare un'analisi dello spettro per capire quali canali sono liberi e cosa è già occupato. Per fare ciò è fondamentale utilizzare il tool denominato "Snooper" che è un vero e proprio analizzatore di spettro integrato negli apparati.
E' consigliabile effettuare questa operazione da un apparato Slave così da rilevare tutti gli apparati master che occupano la banda.
Una volta eseguita la scansione si avrà una dettagliata panoramica su tutti i canali e si potrà selezionare quello meno disturbato.

Selezionato un canale sull'apparato master procedere all'allinemanto cercando di fare agganciare l'apparato slave. Per questa operazione è importante conoscere bene l'orografia del territorio per puntare nella giusta direzione. Una bussola può essere particolarmente utile per allineare la direzione verso il punto giusto. Una volta agganciati il valore principale di riferimento è rappresentato dal "Signal Streight". Più tale valore è basso (tendente a 0) e meglio è. Una volta orientate le antenne ottenendo il valore massimo si deve procedere ad analizzare altri parametri come di seguito riportato.
Valori da considerare:
CCQ: E' la qualità della costellazione. Deve tendere al 100%
SNR: E' il rapporto segnale rumore. Deve essere il più alto possibile
Noise Level: E' il livello di rumore rilevato. Deve tendere al basso quindi un valore di -100 è migliore rispetto ad un valore di -80.
Un altro parametro da considerare è il livello di modulazione ottenuto. La modulazione massima è 54Mbs. Fare attenzione che il valore di modulazione in tx può assumere valori bassi anche in condizioni ideali per effetto del TPC che utilizza la potenza minima per ottenere il massimo risultato.

Finite le prove di allineamento si può procedere ad eseguire delle prove di trasfert rate. Tale prova può essere effettuata direttamente dagli apparati utilizzata il tool bandwidth test oppure esternamente con l'utility iperf allegata al cd fornito con gli apparati.
Si consideri che il badwidth test integrato negli apparati riporta dei valori leggermente inferiori (circa il 20%) a quelli reali per effetto del carico sulla cpu. Valori più reali si possono ottenere con iperf.

16. Utilizzo di Bandwidth Test

Applicabile a: Tutti gli apparati

L'utility Bandwidth Test è già abilitata su tutti gli apparati.
Aprire la maschera Tools->Bandwidth Test

L'esempio riporta un test di trasmissione con il protocollo tcp. Notare che è richiesta la user name e la password dell'apparato che riceverà il flusso.
La prova può essere effettuata sia in trasmissione che in ricezione o in modalità full duplex.

Bandwidth Test

General	**Advanced**
Test To: 10.10.10.2	User: admin
Protocol: tcp	Password: rtm
Local UDP Tx Size: 1500	
Remote UDP Tx Size: 1500	
Direction: receive	

17. Gestione Licenze

RouterOS viene rilasciato con vari livelli di licenza.
Gli apparati Townet possono essere rilasciati con vari livelli di licenza in base al modello.

Per aggiornare una licenza ad un livello più alto si deve ottenere la chiave da Townet come l'esempio di seguito riportato:

```
-----BEGIN MIKROTIK SOFTWARE KEY------------
xBgJx5RA4V9q1UExSfrLlr3rpGdqZiYOZHGJ5VJZPJT0
Tht2QwZikkd8DYRn5Pk/fwYcJvPzeenhZEhDtZJdMA==
-----END MIKROTIK SOFTWARE KEY--------------
```

Selezionare la chiave e effettuare la "Copia".
Aprire WinBox al menù System -> License e premere il pulsante Paste Key

Aggiornamento Licenza 8 cifre
Il SoftwareID è passato dalla versione 3.25 a 8 cifre. Qualora si abbia un apparato con licenza a 8 cifre e si voglia eseguire un upgrade è necessario aggiornare la gestione di tale elemento.
Per aggiornare il SoftwareID alla nuova versione procedere come segue:

1. L'apparato deve poter collegarsi a internet e raggiungere il sito www.mikrotik.com
2. Andare nel menù System -> License e premere il pulsante Upgrade License Key.

Criteri di aggiornamento Software
Ogni apparato può essere aggiornato ad una versione software più recente in funzione del livello di licenza come di seguito riportato:

L3/4 = CurrentVersion + 1
L5/6 = CurrentVersion + 2

Ad esempio:
Versione 5.x L3 e L4 potrà essere aggiornata fino alla 6.x
Versione 5.x L5 e L6 potrà essere aggiornata fino alla 7.x

Comparazione Licenze
A questo link è possibile visionare le varie funzionalità utilizzabili con i vari livelli di licenza: http://wiki.mikrotik.com/wiki/Manual:License

18. Tavola di comparazione

dbm	Volt	Watt
30 dBm	7.07 V	1.00 W
29 dBm	6.30 V	794.33 mW
28 dBm	5.62 V	630.96 mW
27 dBm	5.01 V	501.19 mW
26 dBm	4.46 V	398.11 mW
25 dBm	3.98 V	316.23 mW
24 dBm	3.54 V	251.19 mW
23 dBm	3.16 V	199.53 mW
22 dBm	2.82 V	158.49 mW
21 dBm	2.51 V	125.89 mW
20 dBm	2.24 V	100.00 mW
19 dBm	1.99 V	79.43 mW
18 dBm	1.78 V	63.10 mW
17 dBm	1.58 V	50.12 mW
16 dBm	1.41 V	39.81 mW
15 dBm	1.26 V	31.62 mW
14 dBm	1.12 V	25.12 mW
13 dBm	1.00 V	19.95 mW
12 dBm	890.19 mV	15.85 mW
11 dBm	793.39 mV	12.59 mW
10 dBm	707.11 mV	10.00 mW
9 dBm	630.21 mV	7.94 mW
8 dBm	561.67 mV	6.31 mW
7 dBm	500.59 mV	5.01 mW
6 dBm	446.15 mV	3.98 mW
5 dBm	397.64 mV	3.16 mW
4 dBm	354.39 mV	2.51 mW
3 dBm	315.85 mV	2.00 mW
2 dBm	281.50 mV	1.58 mW
1 dBm	250.89 mV	1.26 mW
0 dBm	223.61 mV	1.00 mW

19. Indicazioni per la corretta installazione

Verifica cablaggio RF (solo se collegate antenne esterne)
Collegare il connettore N saldamente, assicurarsi che tutto sia asciutto e privo di umidità (non collegare cavi RF in giornate piovose o umide)
Nastrare con nastro "autoagglomerante o autovulcanizzante" fino a coprire anche il tubetto di termoretraibile che copre i connettori.
Nastrare con nastro isolante per proteggere la vulcanizzazione. Se possibile fornire un'immagine di questo isolamento.

Verifica cablaggio Ethernet
Usare sempre plug schermati cat.5e, idonei ad accettare cavi 26AWG (attenzione che alcune marche di plug non entrano nei cavi Townet e Belden)
Assicurarsi di aver inserito il gruppo pressa cavo spiralato prima di crimpare il cavo. Crimpare la calza del cavo schermato saldamente ai plug Ethernet FTP.
Assicurarsi di aver inserito l'o-ring di tenuta prima di avvitare la base del pressa cavo.
Avvitare la terminazione spiralata del pressa cavo esclusivamente a mano.

Verifica alimentazione
Assicurarsi che gli apparati siano alimentati alla giusta tensione, 9-28V DC con una potenza disponibile di almeno 15W ad apparato.
Usare l'injector fornito, oppure il PoE attivo fornito da Townet (quello con i 3 led ed il caricabatterie).

Verificare Indirizzamento
Impostare sulla ether1 l'indirizzo di collaudo come da schema di configurazione
Una volta finito il collaudo, assicurarsi di aver impostato gli indirizzi coerenti con lo schema generale di configurazione

Verifica link ethernet
Collegare un PC direttamente alla ethernet dell'apparato, assicurarsi che avvenga una negoziazione 100Mbps full duplex (gli apparati sono tutti auto MDI/MDX).
Assicurarsi di poter pingare l'apparato con pacchetti da 64.000 bytes per almeno 1 minuito senza alcun pacchetto perso. La stringa da usare è:
ping [IP address] –l 64000 –t

Verifica aggancio link radio
Impostare i parametri corretti di collegamento, ovvero: SSID, NStreme, Criptazione ecc, come da documento di configurazione. Quando gli apparati sono collegati, compare una "R" davanti all'interfaccia "WLAN1"

Verifica puntamento
Controllare i parametri di segnale e procedere al puntamento fine. I parametri sono sull'apparato SLAVE sotto "status". Nella macchina MASTER è possibile vedere questi dati sotto "registration table" cliccando 2 volte sulla stazione agganciata.
I parametri di segnale sono Tx/Rx Signal Strenght, che devono ovviamente essere similari e il più possibile prossimi al valore di -60.
Valori più alti (es -50,-40) possono creare saturazione, aumentare quindi il valore del guadagno d'antenna fino ad ottenere valori compresi tra -60 e -70.

Verifica qualità del LINK
Il segnale ricevuto, di per se, non è un parametro indicativo sulla qualità di un link.

Per analizzare con precisione la qualità si usa il parametro percentuale "CCQ” Control connection quality. Questo parametro scaturisce dall’analisi della corretta demodulazione di ogni singola trama OFDM. Il valore, sia in Tx che in Rx, deve essere prossimo al valore di 100/100%, questa è la situazione ideale.
Per poter avere dati significativi di CCQ, il link deve fare traffico, possibilmente in entrambe le direzioni, per fare traffico si usa il tool interno agli apparati "bandwidth test”, deve essere eseguito per almeno 2 minuti, al fine di stabilizzare le tarature interne alla radio. I valori di questo test non sono indicativi circa la capacità del link, per avere la reale capacità del link usare 2 pc con il tool IPerf. Per correggere il CCQ, si può provare a cambiare canale, cambiare polarizzazione, cambiare posizione ecc ecc.
Valori ideali: 95-100%
Valori accettabili: 85-95%
Valori inaccettabili: 0-85%

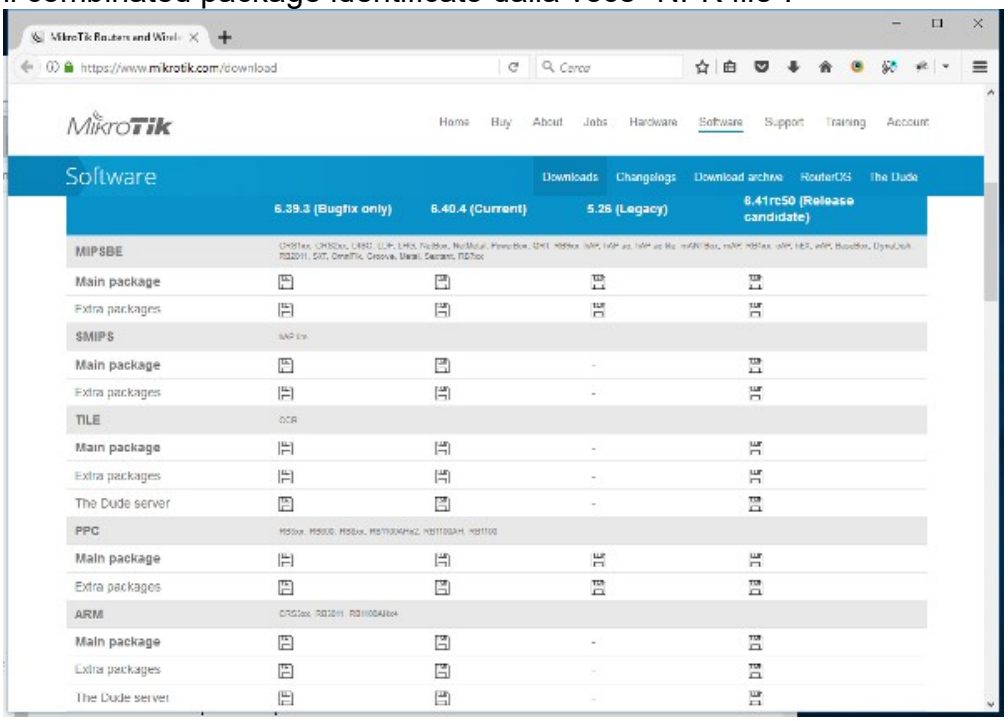
Collaudo througput
Collegare 2 PC ai lati del link ed eseguire i test indicati sulla procedura di test. Riportare qui i valori di TCP e UDP, sia mono che bidirezionale.

20. Aggiornamento firmware

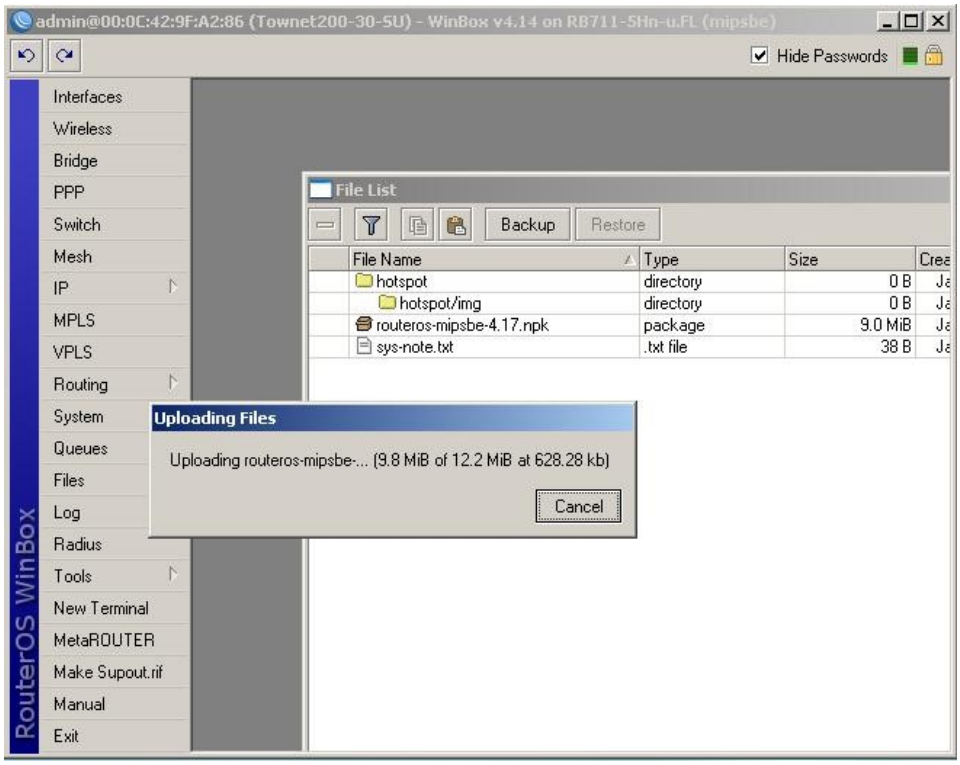
La procedura per aggiornare un apparato su base mikrotik è molto semplice.
Per prima cosa scaricare dal sito mikrotik il nuovo firmware:

`https://www.mikrotik.com/download`

Scegliere il "combined package" e scaricarlo sul proprio computer.
Nell'immagine seguente è stato scelto un firmware per la serie Rb400 a titolo di esempio, dopo aver scelto il tipo di software, nel nostro caso la versione "stable", si può procedere a scaricare il combinated package identificato dalla voce "NPK file".



Dopo aver aperto l'interfaccia di configurazione tramite il programma winbox cliccare su "file" dalla colonnina a sinistra.
Si aprirà una nuova finestra contenente tutti i file degli apparati.
Prendere il file scaricato in precedenda e trascinarlo dentro la schermata "file".



Attendere il completamento del trasferimento e poi riavviare la macchina.
Terminato il riavvio, rientrare nell'apparato e verificare la nuova versione di firmware istallata.

E' anche possibile aggiornare l'apparato tramite ftp.
Aprire un client ftp e collegarsi tramite questo protocollo alla macchina da aggiornare inserendo nome utente e psw per autenticarsi.
Una volta eseguito l'accesso caricare il file e poi riavviare la macchina.
ATTENZIONE accertarsi che sul menù IP->SERVICES la voce ftp sia abilitata.

21. Reset ai parametri di default

Procedura di reset ai parametri di default di RouterOS

Dal terminale
```
/system reset-configuration
y
```

l'apparato riparte e potrebbe avere l'ip settato a 0.0.0.0 oppure 192.168.881/24.
Nel primo caso l'apparato è ripartito senza alcuna configurazione e senza nessun ip assegnato.
Nel secondo caso l'apparato è ripartito con la configurazione base di RouterOS. E' consigliabile al primo accesso in terminale o winbox rimuovere tale configurazione come richiesto dall'interfaccia.

Ripristino configurazione Townet

Una volta resettato sarà possibile caricare la configurazione di default fornita con l'apparato utilizzando il file [nome_apparato].rsc o default.rsc.

Dal terminale
```
/import
file-name: [nome_file].rsc
```

 L'accesso alla configurazione per apparati senza ip (condizione 0.0.0.0) è possibile solo via mac. Fare riferimento al capitolo per maggiori dettagli

22. Convenzioni grafiche

Ogni paragrafo riporta la dicitura “Appllicabile a:” che indica all’utente quali apparati rispondono a questi parametri di configurazione.

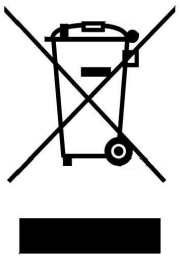
 Indica all’operatore di fare attenzione ad una particolare situazione per evitare spiacevoli inconvenienti.

 Indica un particolare comando o scorciatoia da utilizzare in alcune situazioni

Questo riquadro indica operazioni eseguite con WinBox

Questo riquadro indica operazioni eseguite al terminale

23. Trattamento in caso di cessato funzionamento



Questo apparecchio è contrassegnato dal simbolo della raccolta differenziata relativa allo smaltimento di materiale elettrico ed elettronico. La raccolta differenziata, della presente apparaecchiatura giunta a fine vita, è organizzata e gestita dal produttore. L'utente, che vorrà o dovrà disfarsi della presente apparecchiatura, dovrà quindi contattare il produttore e seguire il sistema che questo ha adottato per consentire una corretta ed efficace raccolta separata dell'apparecchiatura.

L’adeguata raccolta differenziata dell’apparecchiatura dismessa, per l’avvio successivo, al riciclaggio, al trattamento e allo smaltimento, ambientalmente compatibile, contribuisce ad evitare possibili effetti negativi sull’ambiente e sulla salute umana e favorisce il reimpiego e/o il riciclo dei materiali di cui è composta l’apparecchiatura.

Lo smaltimento abusivo del prodotto da parte del detentore comporta l'applicazione delle sanzioni amministrative previste dalla normativa vigente.

Si prega di contattare Townet srl al numero 0721 797396 per ricevere istruzioni sul corretto smaltimento.