MIKROTIK – CONFIGURIAMO UN ROUTER

In questa pratica guida vedremo come configurare un Router Mikrotik da zero passo per passo

Ipotizziamo di avere un router hAP ac lite (RB952Ui-5ac2nD) e due PC di cui uno in IP statico e uno in DHCP client come indicato nel seguente diagramma.

Potrebbe interessarti anche questa guida: Configurare un Router Cisco partendo da zero.

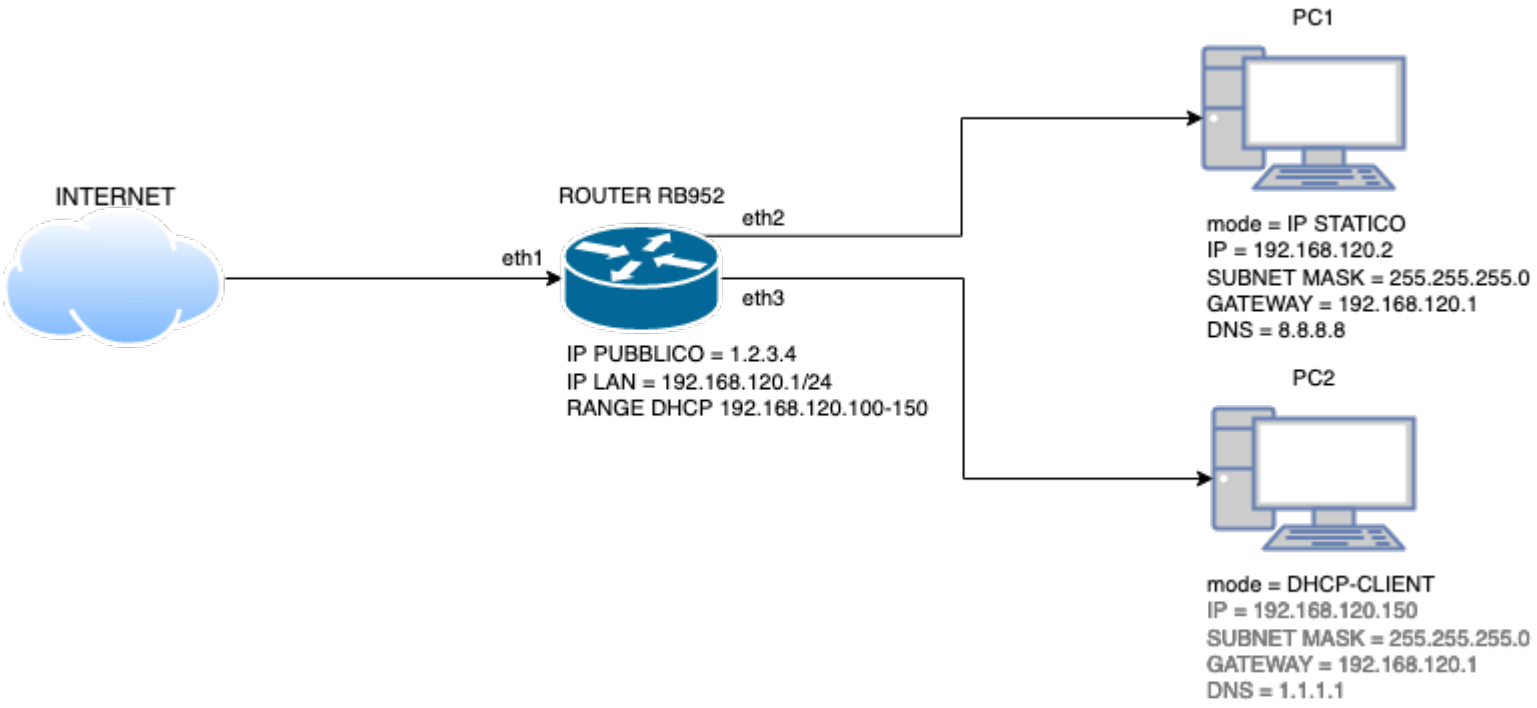


fig.1 – Diagramma

configurazione di base
.Scarichiamo il software Winbox dal sito Mikrotik https://mt.lv/winbox64

Componenti necessari:

1. Un Router Mikrotik RB952Ui-5ac2nD
2. Due cavi LAN.
3. Una connessione internet funzionante.
4. Almeno un PC

Obbiettivo 1: Eseguire la connessione al Router e accedere al pannello di configurazione.

1. Collegare il vostro PC alla porta ethernet 2 del router.
2. Aprire il software **Winbox** appena scaricato e installato.
3. Cliccare nel tab **Neighbors.**
4. Attendere che appaia nell'elenco il proprio router.
5. Inserire nome username **admin** e password (vuota).
6. Cliccare sul MAC address del router e poi sul tasto Connect.

Dovresti trovarti in una schermata simile a questa:

fig.2 – Primo accesso a Winbox

Obbiettivo 2: Eseguire il reset alle impostazioni di fabbrica.

1. Clicca sul tab **System, Reset Configuration.**
2. Apparirà una schermata come quella visualizzata di seguito.
3. Inserire il flag sulla voce **No Default Configuration**.
4. Cliccare sul tab **Reset Configuration**.
5. Il Router si riavvierà e resetterà completamente senza caricare la configurazione di default.

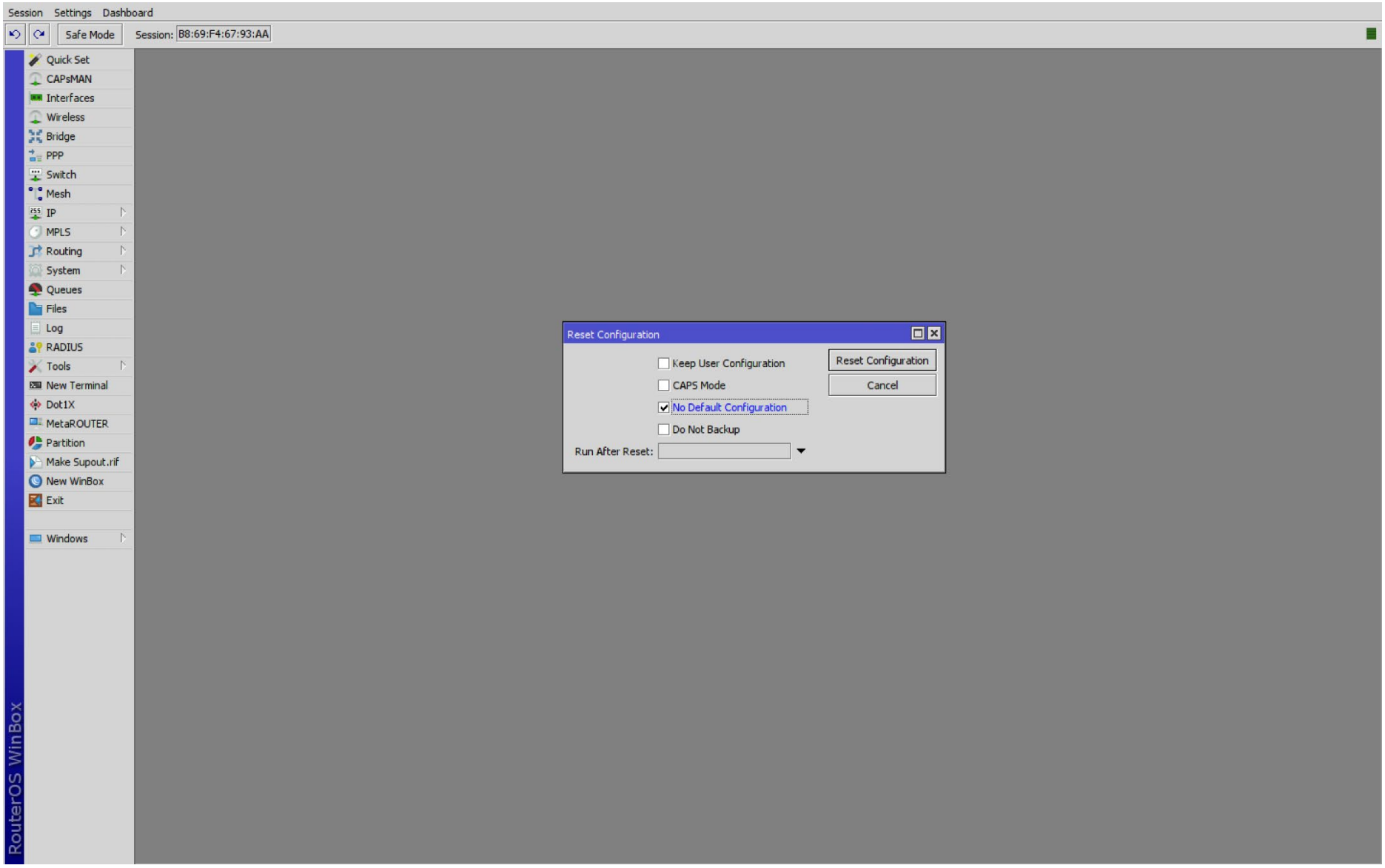


fig.3 – Reset del Router

Obbiettivo 3: Rinominare il Router e proteggerlo.

A seguito del reset, al primo accesso ci occupiamo di dare un nome al Router.

1. Cliccare sul tab **System, Identity.**
2. Digitare il nome che si vuole dare al router; (esempio: ***Router-ufficio***)
3. Cliccare su **OK**.
4. Il Router verrà rinominato come potrete vedere nella barra del titolo.

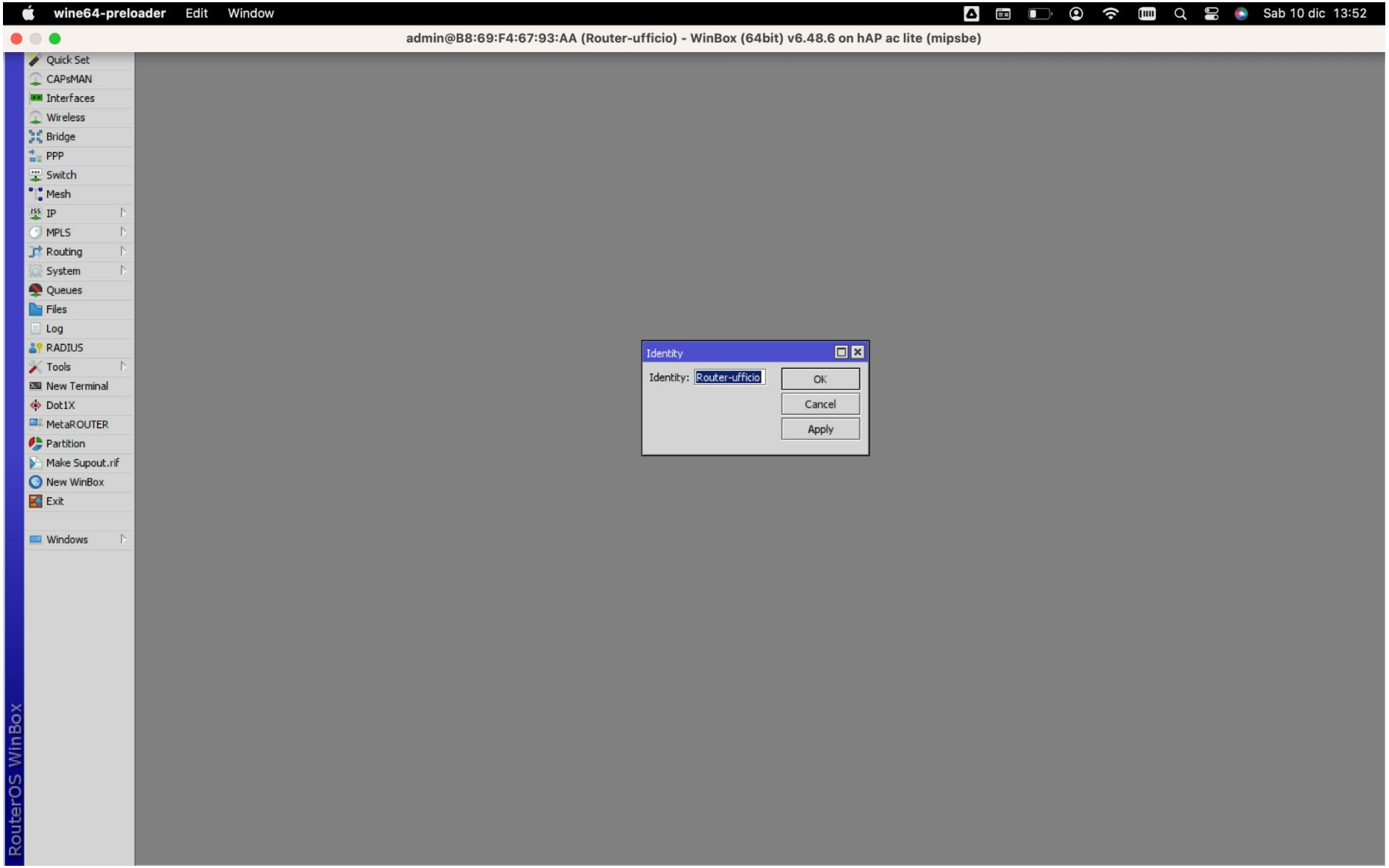


fig.4 – Rinominare il router

Ora vediamo come proteggere con un minimo di sicurezza il nostro Router.

1. Cliccare sul Tab **System**, **Users** e sul tasto **+** .
2. Inserire nel campo name, un nome utente diverso da admin (es. ***Fabio28***).

3. Selezionare dal menu a tendina del campo **Group**, ***full*** .
4. Nel campo password inserire una password complessa che abbia lettere minuscole, maiuscole, numeri e caratteri speciali (es. ***F@b1o.Parigi35***)
5. Confermare la medesima password nel campo Confirm Password.
6. Cliccare su **OK**.
7. Sarebbe bene uscire da Winbox è provare ad accedere con le credenziali appena create.
8. Se le credenziali funzionano, proviamo ad eseguire modifiche sul router, in modo da essere sicuri che l'utente creato, abbia privilegi di scrittura. Se riusciamo ad inserire i punti 9 e 10 senza errori, l'utente funziona.
9. Cliccare nel tab **IP**, **Services.**
10. Cliccare su **api** e successivamente sulla **X** nella barra del titolo della medesima finestra. La voce api diventerà grigia e verrà disabilitata.
11. Ripeti il punto 10, anche sulle voci: **api-ssl**, **ftp** e **telnet.**
12. Ora cliccare due volte sulla voce **ssh**, apparirà una piccola finestra.
13. Nel campo Available From inserisci ***192.168.120.0/24*** e clicca su **OK*.***
14. Ripeti il punto 13, anche sulle voci: **winbox** e **www**.
15. Cliccare sul tab **System**, **Users** e fare un clic sull'utente **admin**.
16. Una volta selezionato l'utente admin, clicca sul tasto **–** nella barra degli indirizzi per rimuovere il medesimo utente.

Dovresti trovarti delle finestre come quelle in figura 5.

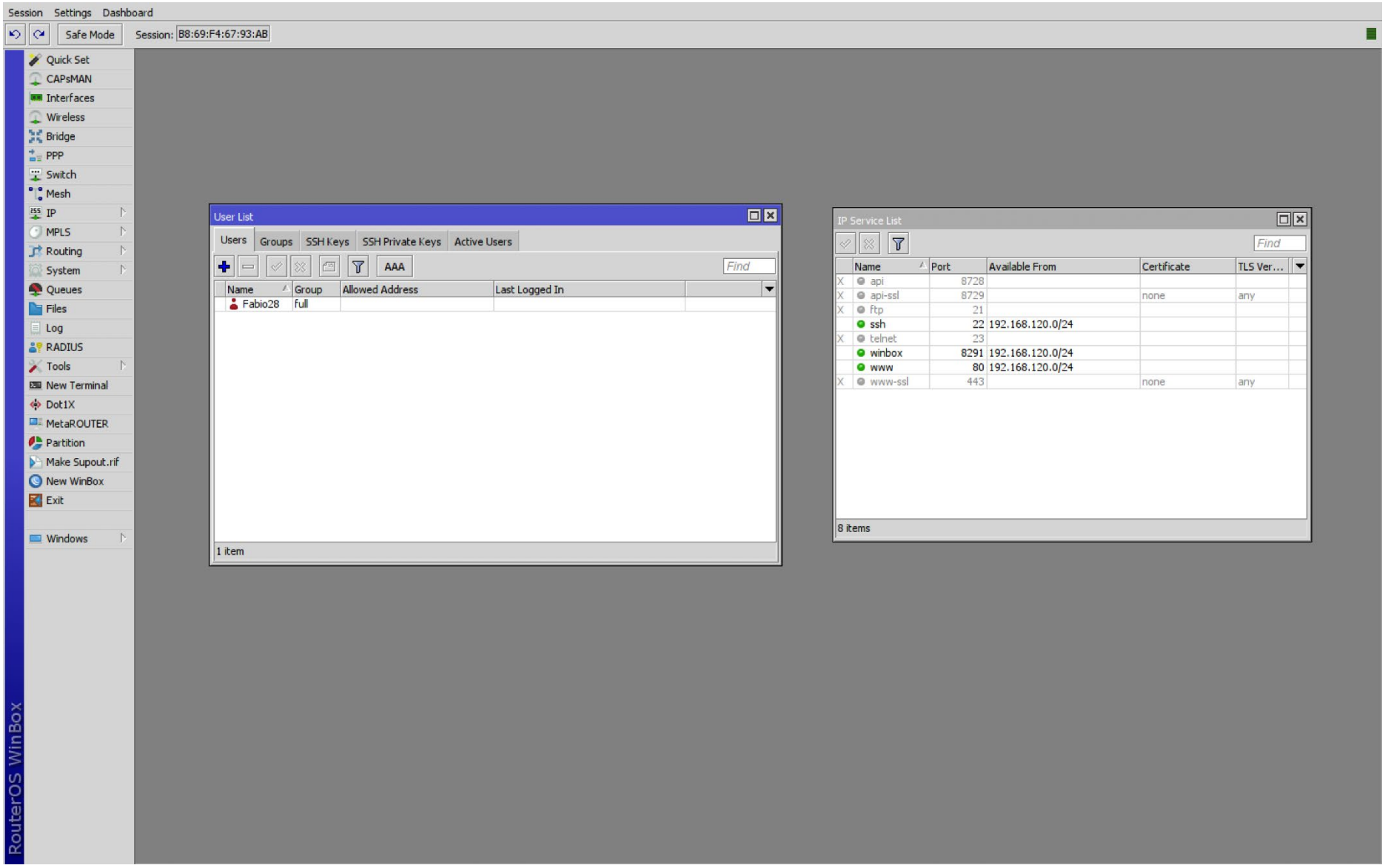


fig.5 – minima messa in sicurezza router

Obbiettivo 4: Descrivere le interfacce.

1. Cliccare sul Tab **Interface.**
2. Cliccare su **ether1** per selezionare l'interfaccia.
3. Cliccare sul **simbolo giallo** posto sopra l'elenco interfacce come indicato nella figura 6.
4. Digita il commento dell'interfaccia ether1. (es. ***Interfaccia_pubblica***) e clicca su **OK**.
5. Esegui la stessa procedura con ether2. (es.***———————LAN———————***).
6. Dovrebbero ora apparire le interfacce commentate come in figura 7.

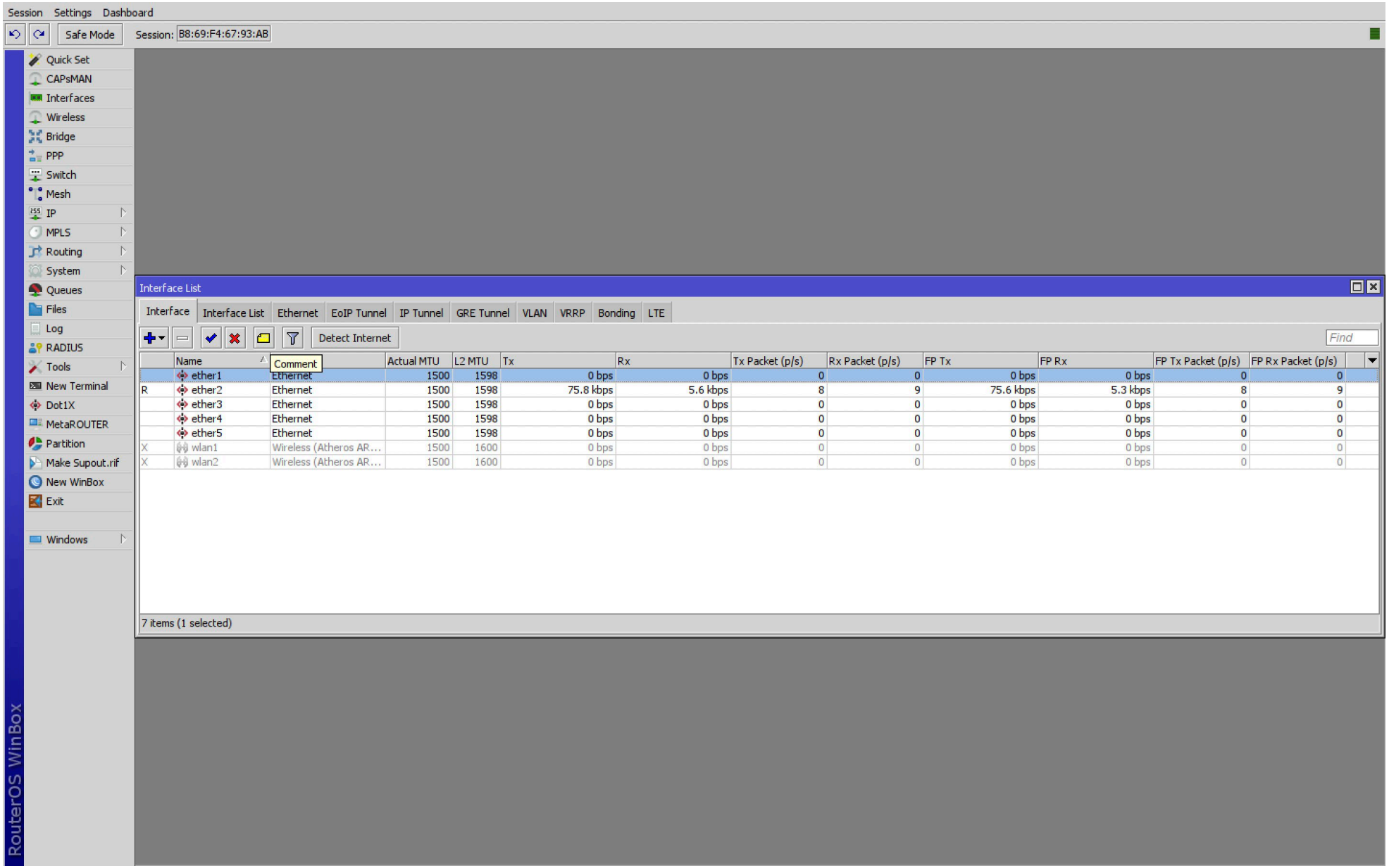


Fig.6 – Commentare le interfacce

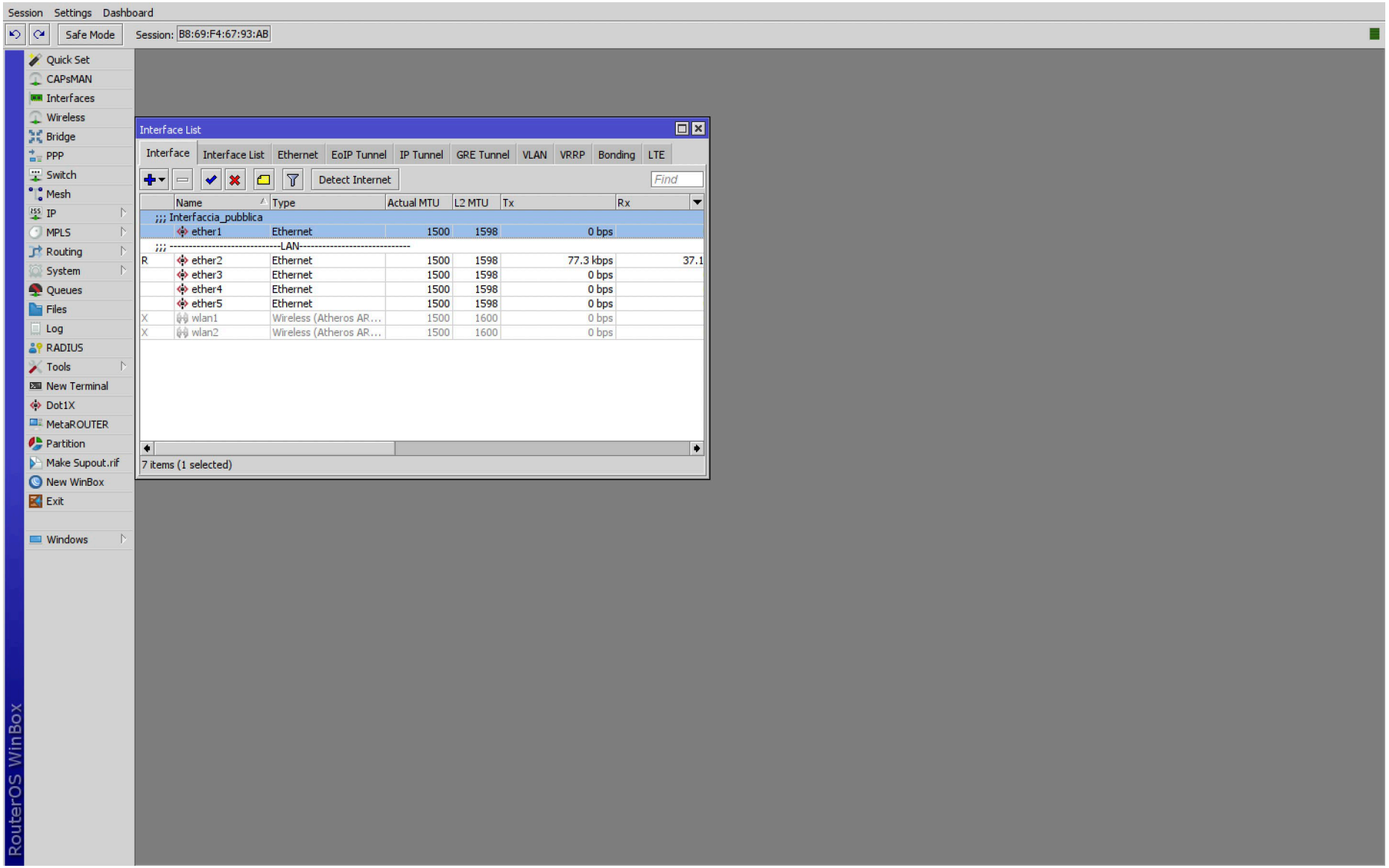


fig.7 – Interfacce con relativo commento

Obbiettivo 5: Creare un Bridge per definire le interfacce LAN

Prima di configurare un bridge, è importante tenere a mente quanto segue:

Nei Router Mikrotik, tutte le interfacce sono slegate a livello software. Ogni interfaccia può svuolgere un ruolo diverso.

Nell nostro caso, le interfacce ethernet 2 ed ethernet 3, hanno il medesimo ruolo. In previsione che questa rete si possa espendare, daremo anche alle interfacce ethernet 4, ethernet 5 e le interfacce Wi-Fi lo stesso ruolo.

Creando un bridge e inserendo le porte citate all'interno di esso, le interfacce diventeranno interfacce slave, dipendenti dal bridge e assumeranno tutte le impostazioni legate al bridge.

Nelle recenti versioni di RouterOS (since v6.41), è stata introdotto ***Hardware Offloading*** Questo permette in parecchi Router Mikrotik, di sfruttare l'hardware del chip Switch integrato per fare Switching senza far passare i pacchetti per la CPU del Router. Questo favorisce un throughput elevato e un minor carico della CPU.

Ora creiamo un Bridge e lo configuriamo.

1. Cliccare sul tab **Bridge** e sul tasto **+** in alto a sinistra.
2. Inseriamo il nome nel campo name (es. ***bridge_LAN***) e clicchiamo su **OK**.
3. Cliccare sul tab **Port** e sul tasto **+**
4. Apparirà una schermata come in figura 8.
5. Nella voce interface, selezionare dal menu a tendina l'interfaccia **ether2** e cliccare su **OK.**
6. Eseguire il punto 5 anche sulle interfacce ether3, ether4, ether5, wlan1 e wlan2.

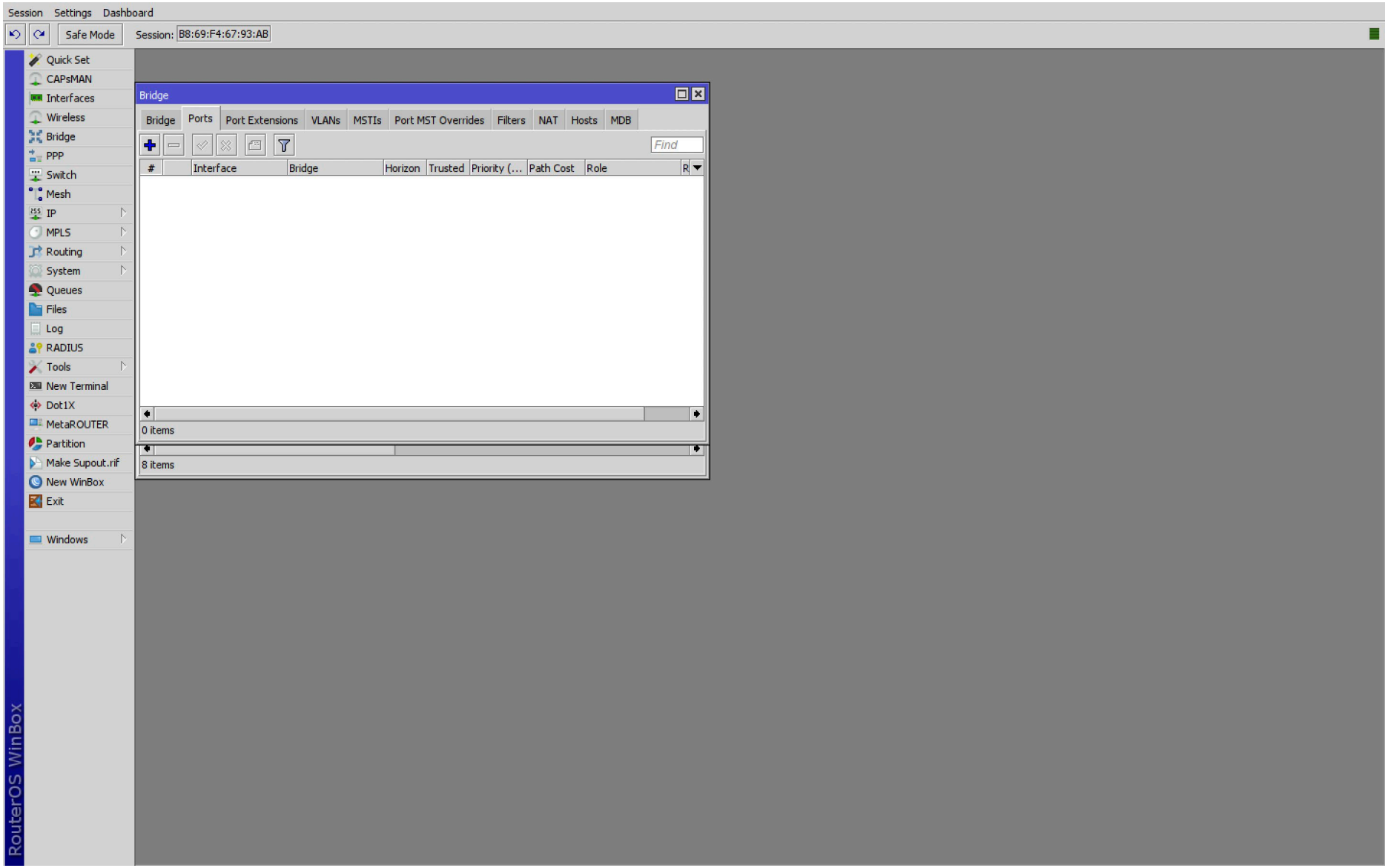


fig.8 – menu Bridge port

Per comodità, nel punto 5, anzichè usare il tasto OK a fine passaggio, può esser utilizzato il tasto Apply, questo applica la modifica ma non chiude la finestra. Questo permette dopo aver applicato la configurazione, di cliccare sul tasto Copy, in quest maniera viene aperta una nuova finestra clone di quella appena configurata, in cui basta semplicemente inserire l'interfaccia

ether3 e cliccare ancora su Apply per inserire anche essa agevolmente riducendo e semplificando i passaggi. Questo si puo sfruttare per tutte le interfacce da aggiungere.

Dopo aver inserito tutte le interfacce nel bridge, dovreste avere una schermata come in figura 9.

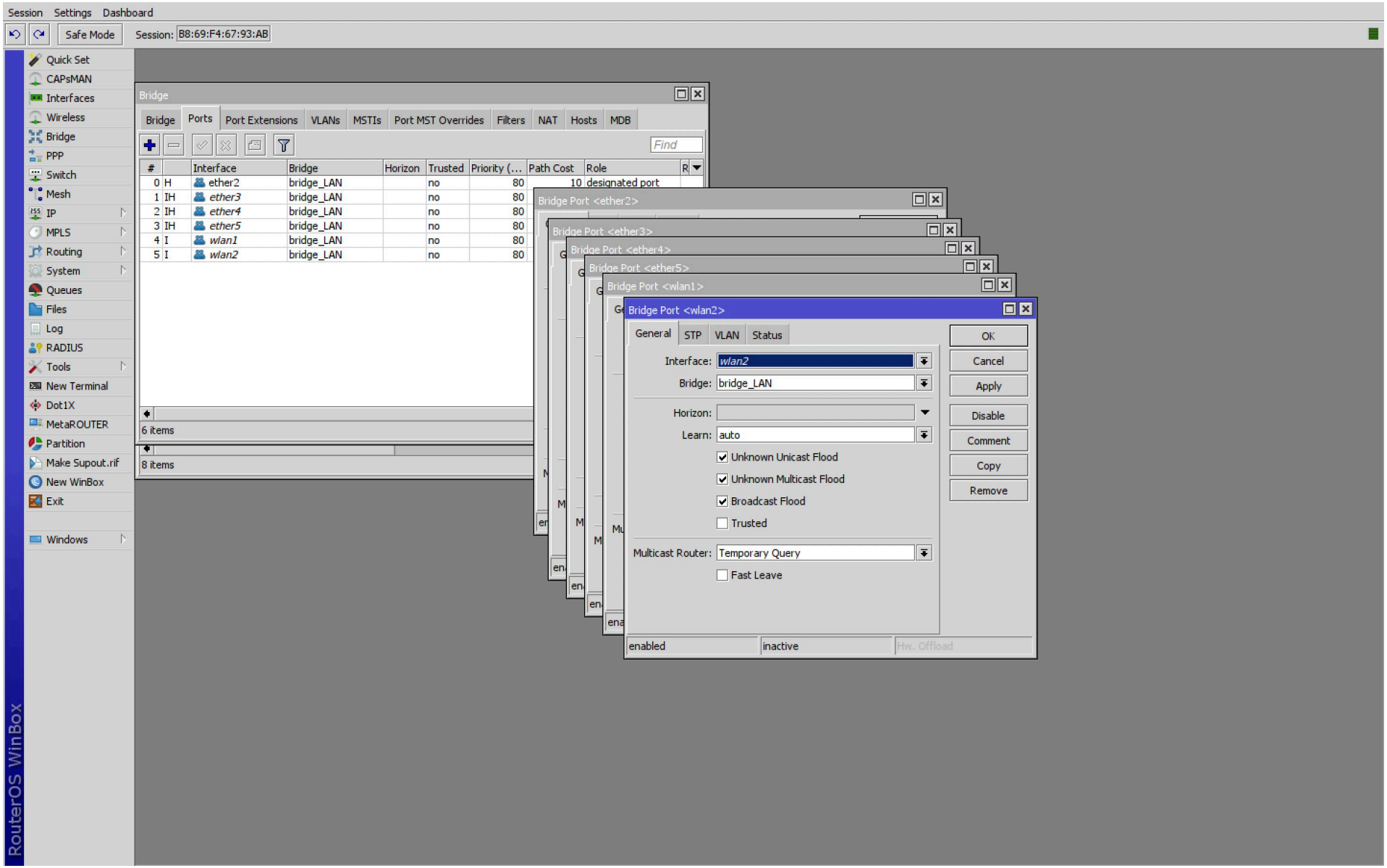


fig.9 – Interfacce aggiunte al bridge

Obbiettivo 6: Assegnare gli indirizzi IP alle interfacce

1. Cliccare sul tab **IP**, **Addresses** e sul tasto **+ .**
2. Assegnare nel campo Address, l'indirizzo IP pubblico indicato dal nostro Provider ***1.2.3.4/32*** , nel campo interface selezioniamo interface ***ether1*** e cliccare su **OK**, il campo network si compilerà automaticamente.
3. Ripetiamo il punto 1, però ora occupiamo di assegnare l'indirizzo alla LAN utilizzando quello del diagramma in figura 1.
4. Assegnare nel campo Address, l'indirizzo IP LAN ***192.168.120.1/24*** , nel campo interface selezioniamo dal menu l'interfaccia ***bridge_LAN*** e cliccare su **OK**.

Ci troveremo una schermata simile a quella in figura 10.

Volendo potremo commentare i due indirizzamenti, usando lo stesso metodo indicato nel paragrafo 4 – punto 3.

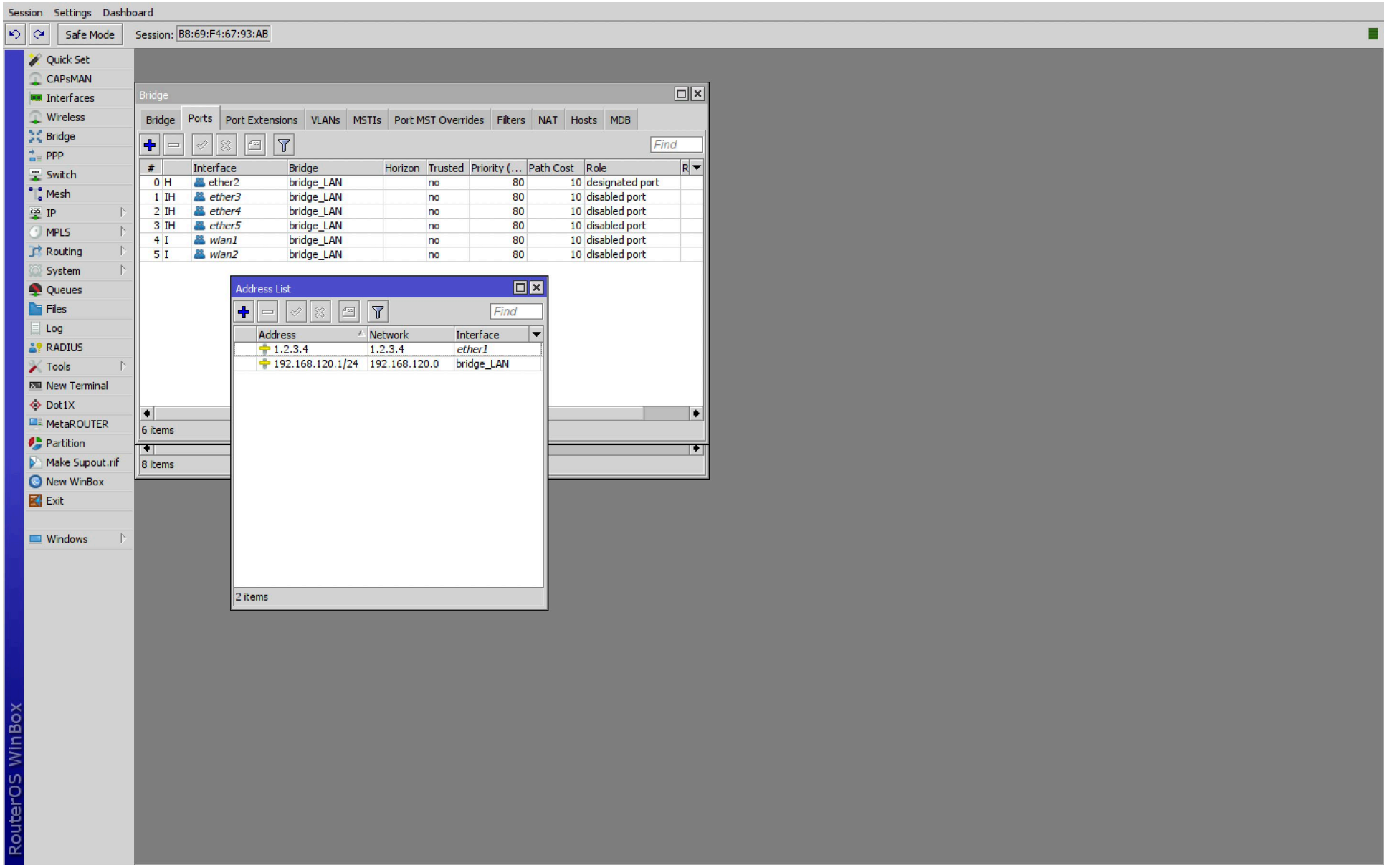


fig.10 – Assegnazione indirizzi IP

Obbiettivo 7: Impostare il DHCP-SERVER

1. Il primo passo è generare un POOL IP. Cliccare nel tab **IP**, **Pool** e sul tasto **+** .
2. Inserire nel campo name, il nome del pool (es. ***pool_dhcp***).
3. Inserire nel campo Addresses, il range di indirizzi come dal diagramma in figura 1, ***192.168.120.100-192.168.120.150*** e cliccare su **OK**.
4. Cliccare nel tab **IP**, **DHCP Server** e sul tasto **+** .
5. Inserire nel campo name, il nome del server dhcp (es. ***dhcp-server***).
6. Selezionare dal menu a tendina del campo interface, ***bridge_LAN .***
7. Impostare il campo Lease Time a ***12:00:00*** , in modo che gli indirizzi si rinnovino con tempo più lungo rispetto alle impostazioni di default.
8. Nel campo Address Pool, selezioniamo il pool ***pool_dhcp*** precedentemente creato.
9. Infine cliccare sul tasto **OK.**
10. Ora cliccare sul tab **IP**, **DHCP Server, Network**, infine sul tasto **+** .
11. Inserire nel campo Address, la Network mask della nostra LAN ***192.168.120.0/24*** .
12. Inserire nel campo Gateway, l'indirizzo del Router ***192.168.120.1*** .
13. Inserire nel campo Nemask, la maschera ***24***
14. Inserire nel campo DNS, l'indirizzo 1.1.1.1
15. Inserire nel campo Domain, ad esempio il dominio ***WORKGROUP*** utilizzato da Windows.
16. Infine cliccare su **OK.**

Dovreste trovarvi i menu configurati come in Figura 11.

N.B. che i router Mikrotik, assegnano gli indirizzi, partendo dall'ultimo indirizzo del pool disponibile.

Puoi verificare gli indirizzi assegnati dal router mikrotik nel Tab **IP**, **DHCP Server**, **Leases**.

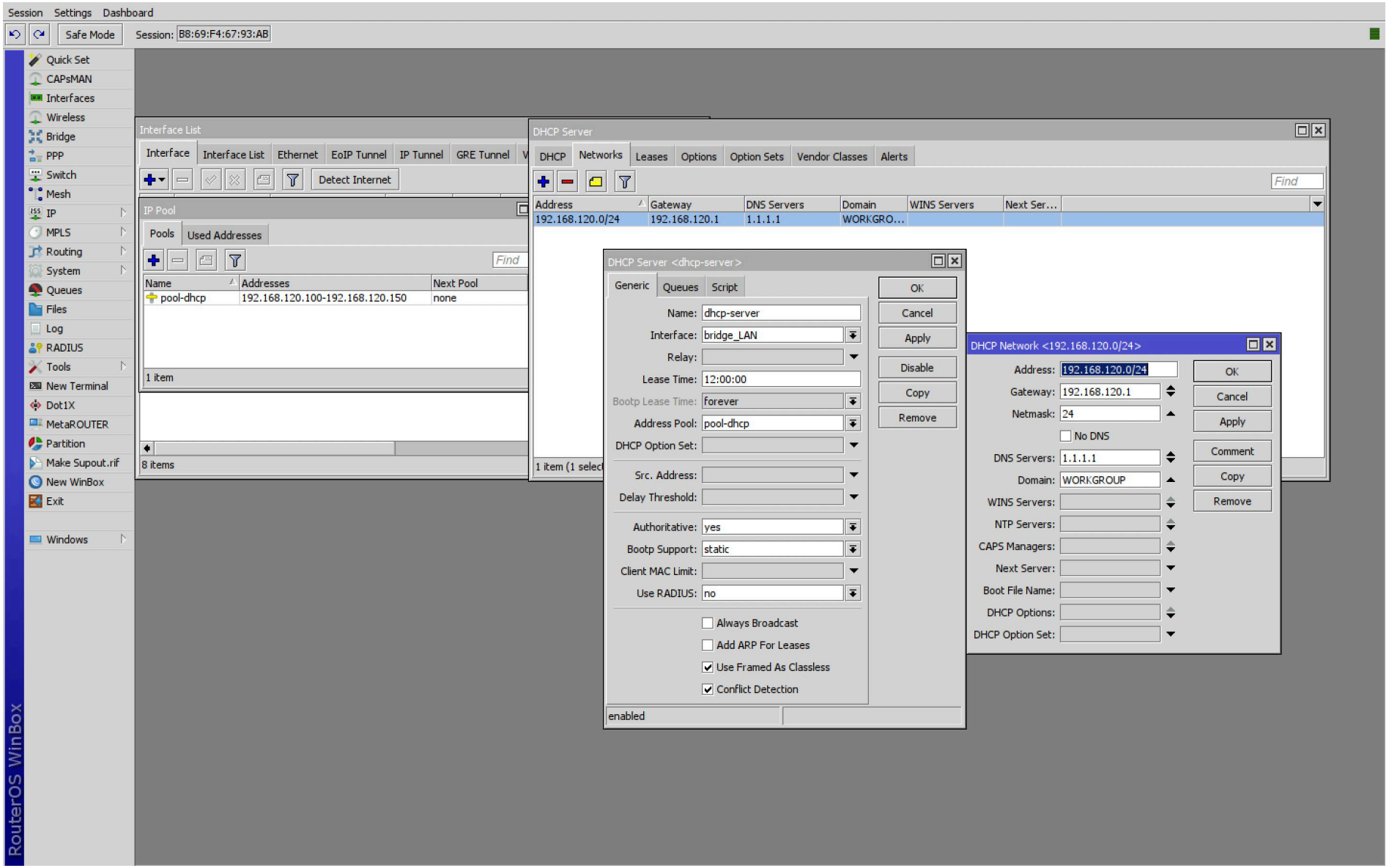


fig.11 – configurazione del DHCP server

Obbiettivo 8: Impostare i Server DNS

I Router Mikrotik, hanno la possibilità di svolgere la funzione di server DNS e DNS relay.

Infatti oltre a gestire direttamente le cache DNS e passarle ad un server DNS pubblico, possono appunto gestire delle query statiche raggiungibili dall'interno della rete locale.

Esempio, è possibile raggiungere il router stesso dalla lan chiamandolo con il DNS ***router.lan*** .

Vediamo come configurare la parte DNS.

1. Cliccare nel tab **IP**, **DNS**.
2. Nel campo Servers, indicare due server DNS pubblici es. ***1.1.1.1*** e ***208.67.222.220*** .
3. Inserire il flag su ***Allow Remote Requests***
4. Infine cliccare su **Apply**.
5. Cliccare sul tasto **Static** e sul tasto **+** .
6. Inserire nel campo Regexp, ***router.lan***
7. Inserire nel campo Address, ***192.168.120.1*** e clicca su **OK**.

In questo il router potrà raggiungere DNS pubblici.

I passaggi dei punti 5,6,7, servono appunto per poter gestire chiamate interne dalla lan verso roter.lan e reinderizzarle all'IP del router stesso.

Perchè questo possa avvenire, i PC devono utilizzare come server DNS predefinito, l'ip del router stesso. Quindi per beneficiare di questa funzione, nel paragrafo 7 – punto 14, andrebbe inserito l'IP 192.168.120.1 .

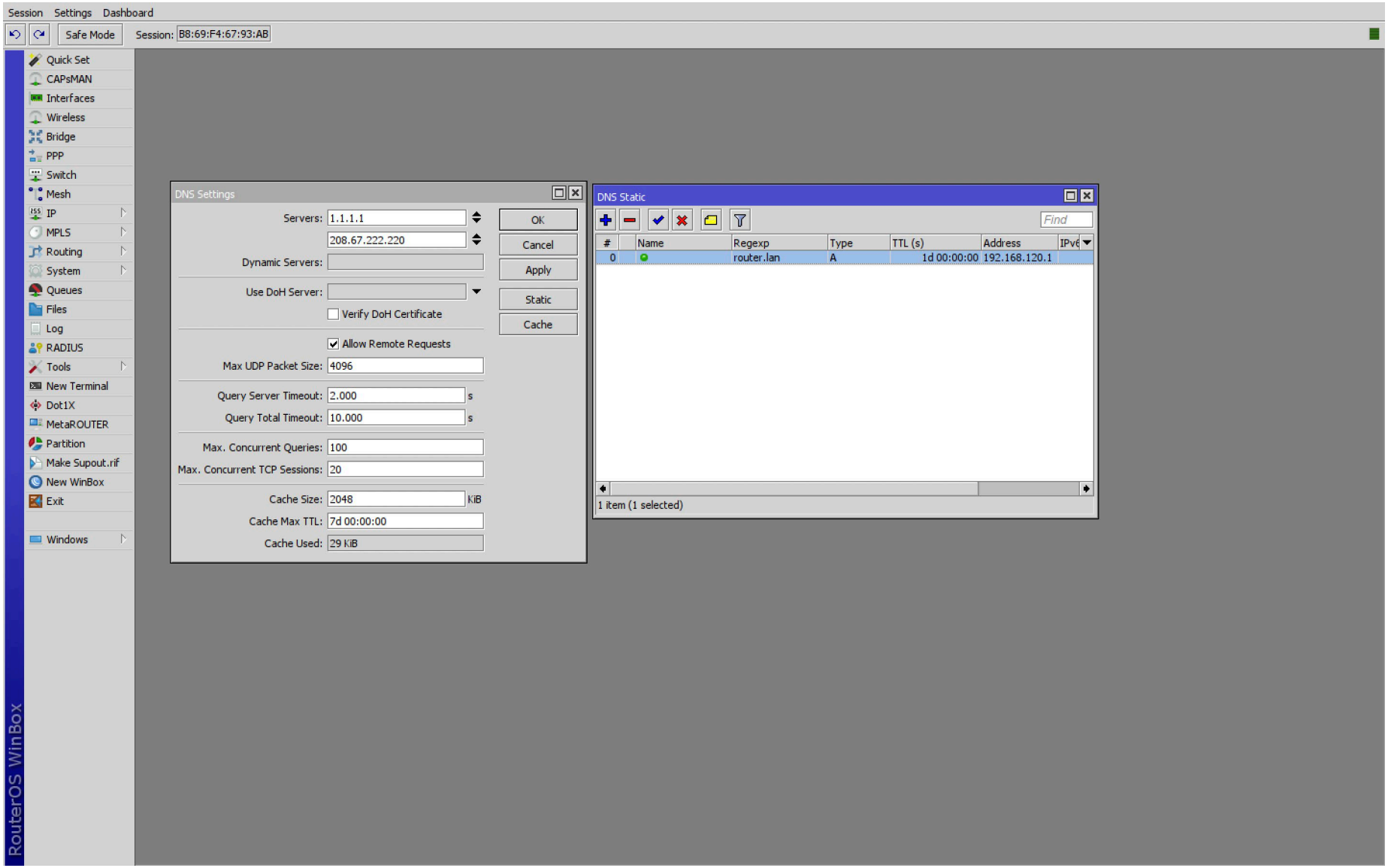


fig.12 – Configurazione DNS

Obbiettivo 9: Impostare il Gateway del Router

Nel paragrafo 6 – punto 2, abbiamo assegnato all'interfaccia ether1 l'ip pubblico statico rilasciato dal Provider.

Esso ci ha rilasciato anche il gateway statico da impostare nel nostro Router, che in questo caso è 10.246.159.50. Ora vediamo come impostarlo nel nostro router Mikrotik.

1. Cliccare sul tab **IP**, **Route** e sul tasto **+** .
2. Impostare nel campo gateway, ***10.246.159.50*** e cliccare su **OK** .

Il nostro router avendo ora, indirizzo IP pubblico, gateway e DNS impostati dovrebbe essere in grado di uscire attraverso internet.

Non rimane che collegare il modem o la cpe del nostro gestore alla porta ethernet 1 del nostro mikotik per accertarsi che tutto funzioni. Prima sarebbe fondamentale proteggere il router, in modo da evitare che qualcuno attraverso internet possa raggiungere il nostro mikrotik e far danni.

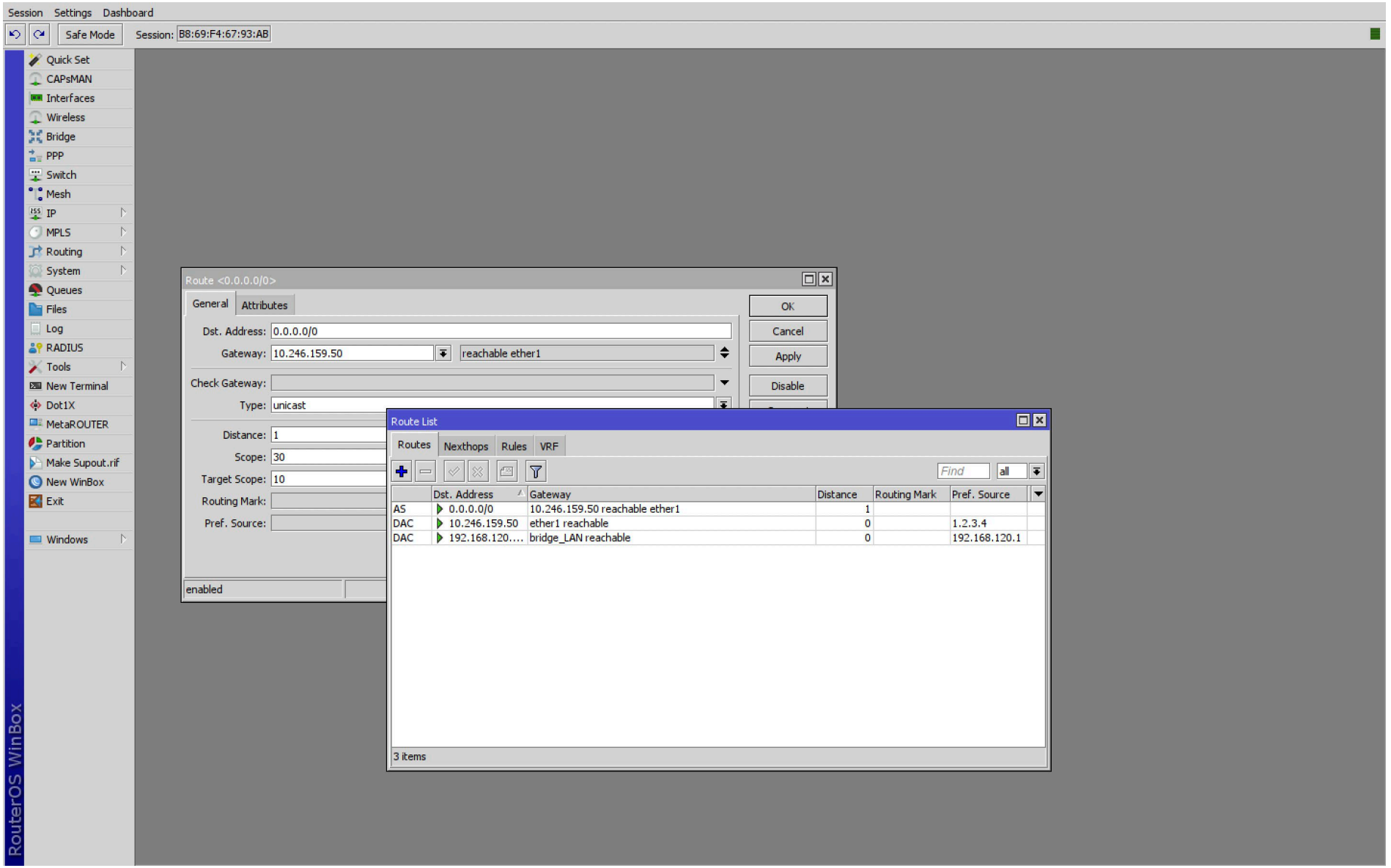


fig.13 – Impostare il gateway

Obbiettivo 11: Verificare che il router navighi in Internet

Per verificare che il router navighi in Internet, ci sono svariati modi.

Ora vediamo come eseguire la verifica più pratica e veloce.

1. Cliccare sul tab **New terminal** .
2. Digitare il comando ***ping 1.1.1.1***
3. Se il server risponde, vedrete nel campo time la latenza in mS, diversamente apparirà timeout o no route to host.
4. Se 1.1.1.1 risponde, premete ctrl + C per interrompere i ping.
5. Ora digitate il comando ***ping google.it***
6. Se anche questo server risponde, il router raggiunge internet e risolve i nomi DNS, quindi possiamo passare all'obbiettivo 12.

Se tutto funziona ti troverai una schermata simile a quella in figura 14.

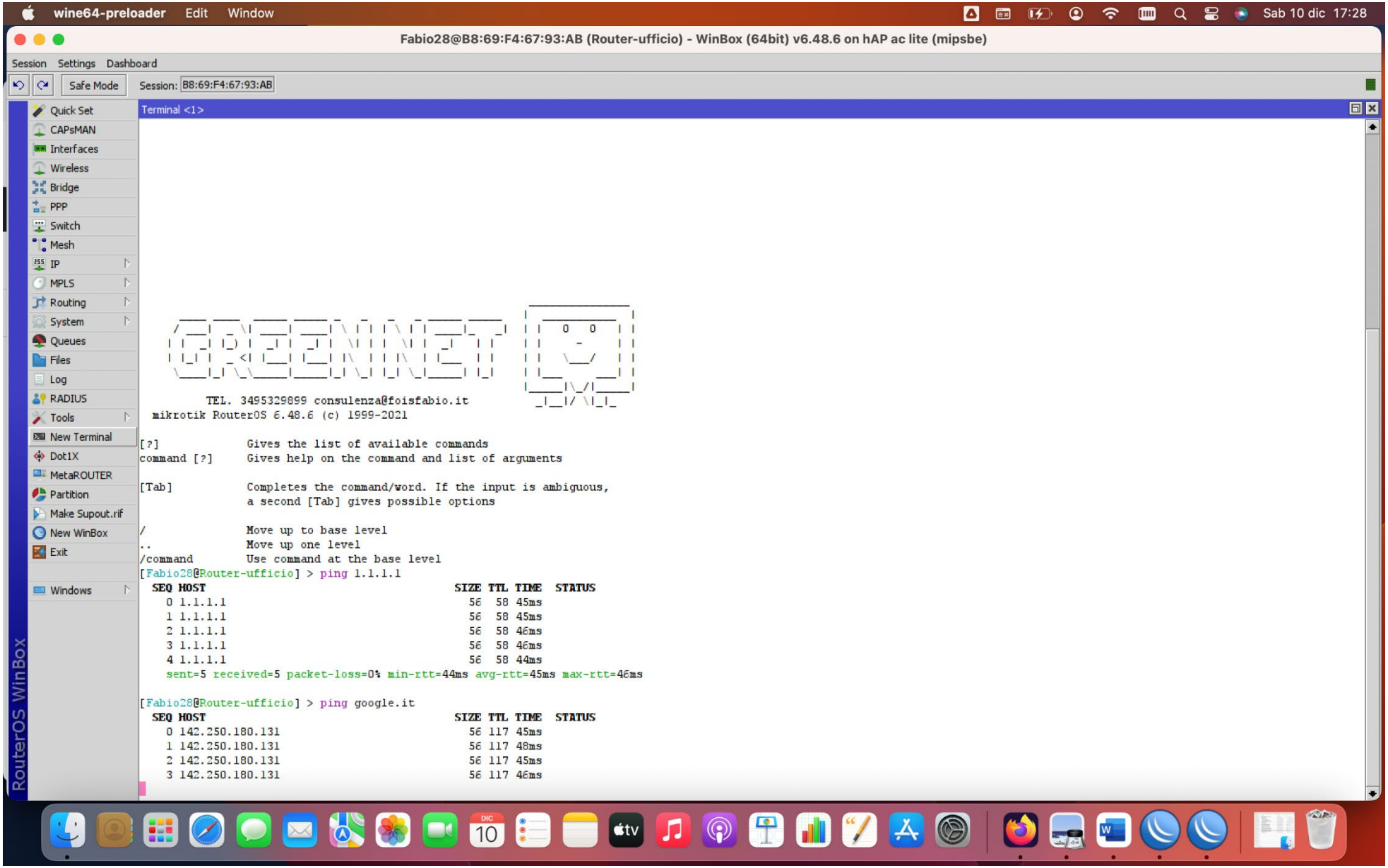


fig.14 – ping da terminale

Obbiettivo 12: Configurare il firewall e il NAT

Come avrete notato, anche se il vostro router naviga, il vostro PC non naviga. Questo perchè manca il NAT. Nei prossimi passi vedremo come configurarlo, e aggiungiamo un firewall minimo che permetterà di scartare i pacchetti invalidi.

12.1 Impostiamo il Firewall

1. Cliccare su **IP**, **Firewall, Filter rules** e sul tasto **+** .
2. Selezionare la **chain** di ***input*** .
3. Nel campo **Connection State**, inserisci il flag su ***estabilished***, ***related***, ***untracked*** .
4. Clicca sul tab **Action** nella barra del titolo.
5. Nel campo **Action**, seleziona la voce ***accept*** e clicca su **OK**.
6. Ripeti il punto 1 e il punto 2.
7. Nel campo **Connection State**, inserisci il flag su ***invalid*** .
8. Clicca sul tab **Action** nella barra del titolo.
9. Nel campo **Action**, seleziona la voce ***drop*** e clicca su **OK**.

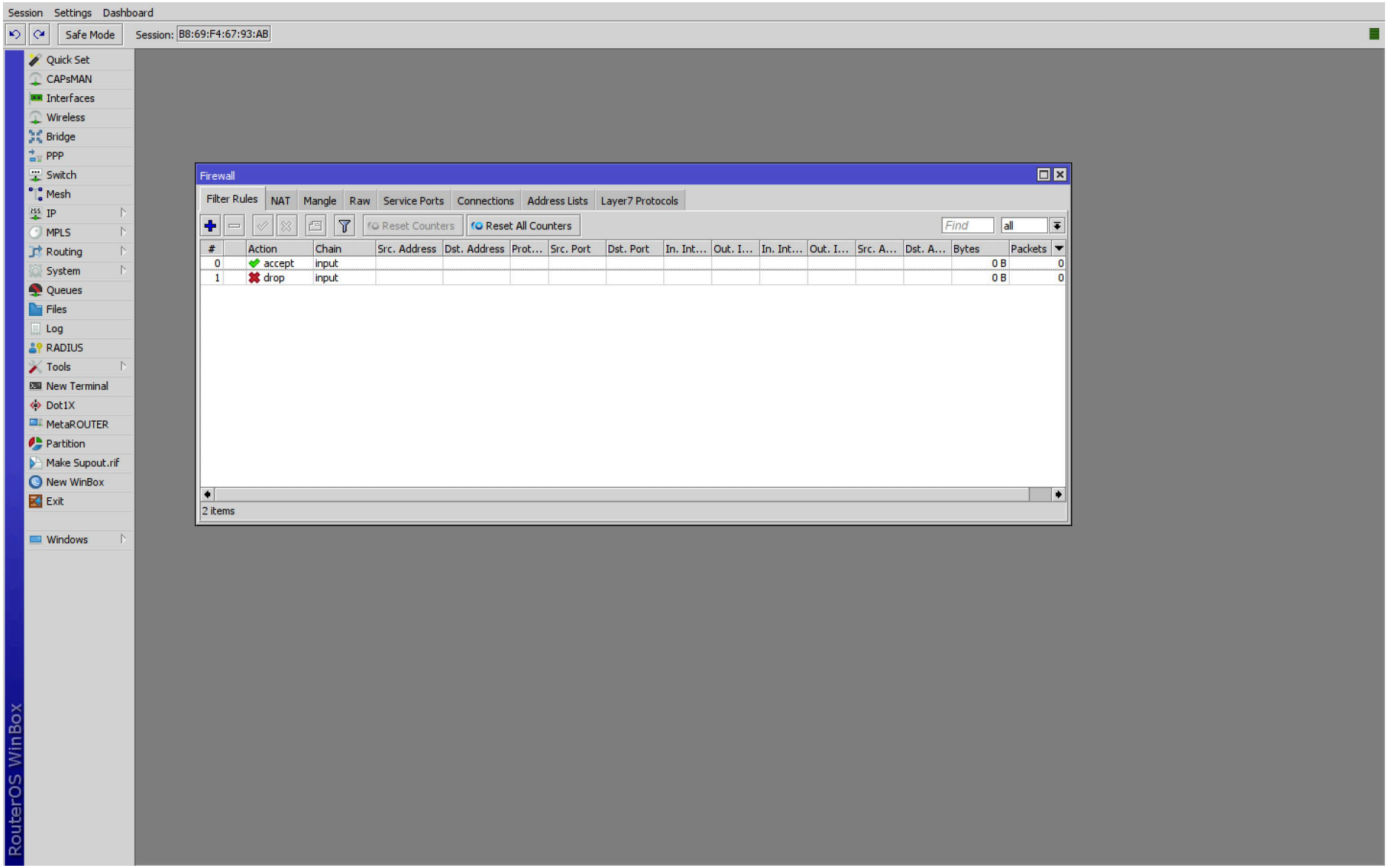
Dovresti trovarti una schermata come quella in figura 15.

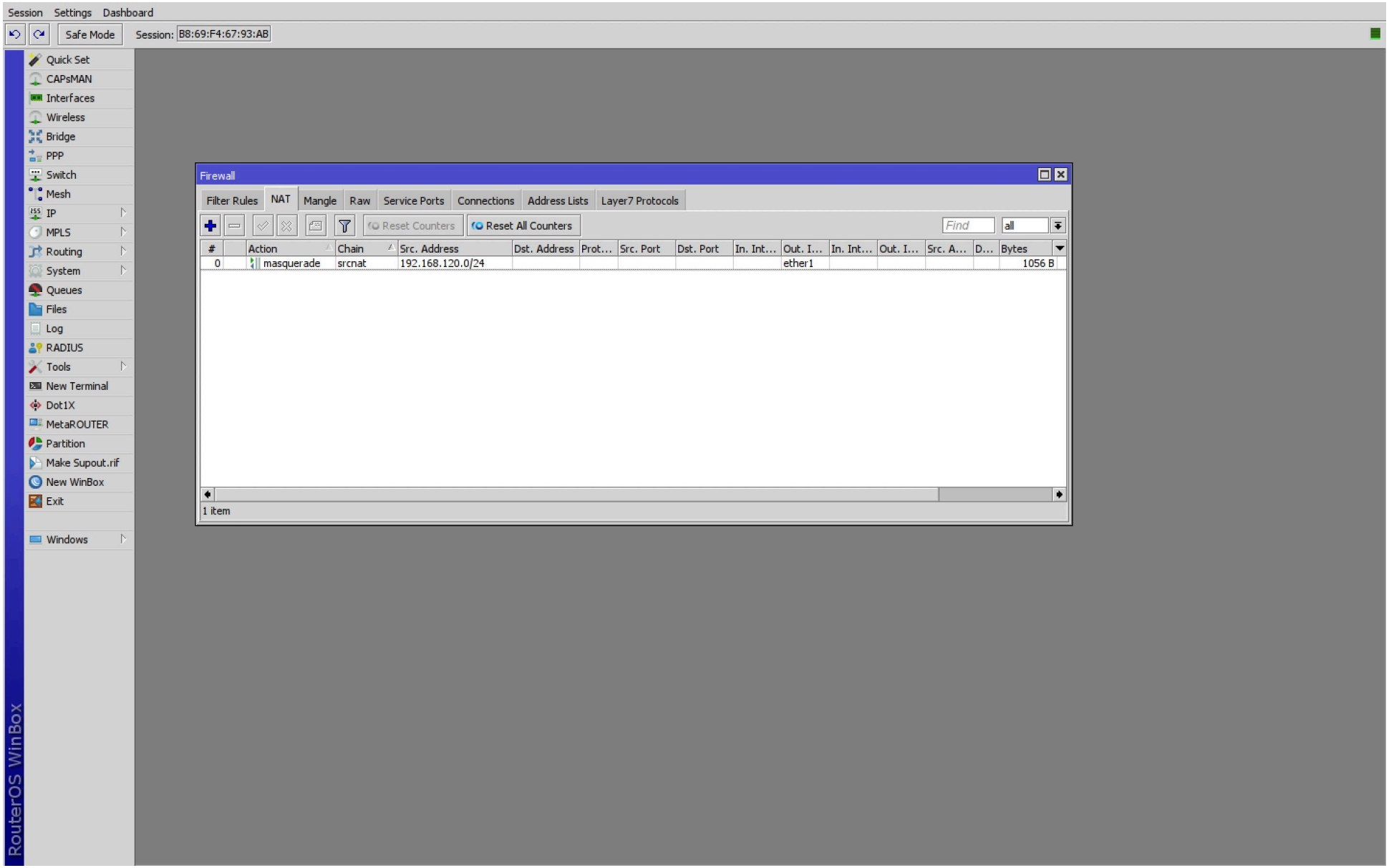
12.2 Impostiamo il NAT in modo che il tuo PC possa navigare.

1. Cliccare su **IP**, **Firewall, NAT** e sul tasto **+** .
2. Nel campo **chain**, selezionare ***srcnat***.
3. Nel campo **src-address** inserire, ***192.168.120.0/24*** .
4. Nel campo **out-interface** selezionare ***ether1*** .
5. Clicca sul tab **Action** nella barra del titolo.
6. Nel campo **Action**, seleziona la voce ***masquerade*** e clicca su **OK**.

Ora il tuo PC dovrebbe navigare. Puoi provare sia in dhcp client che in maniera statica come indicato nel diagramma in figura 1.

Dovresti trovarti una schermata come quella in figura 16.




Session Settings Dashboard
Safe Mode
Session: B8:69:F4:67:93:AB
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
MetaROUTER
Partition
Make Supout.rif
New WinBox
Exit
Windows
RouterOS WinBox
Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
Find
all
Action Chain Src. Address Dst. Address Prot... Src. Port Dst. Port In. Int... Out. I... In. Int... Out. I... Src. A... D... Bytes
0 masquerade srcnat 192.168.120.0/24 ether1 1056 B
1 item
fig. 16 – NAT

Obbiettivo 13: Configuriamo la parte Wireless modalità Access Point.

Come avreste notato, il vostro router ha un interfaccia wireless 2,4Ghz e una 5Ghz che sono attualmente disabilitate. Vediamo come configurarle e attivarle.

1. Cliccare sul tab **Wireless** e cliccare due volte sull'interfaccia **wlan1**.
2. Cliccare sul tab **Wireless** della finestra.
3. Cliccare sul tab **Advanced Mode**, sul lato destro della finestra.
4. Nel campo **Mode**, seleziona ***ap bridge*** .
5. Nel campo **Band**, seleziona ***2Ghz-B/G/N*** .
6. Nel campo **Channel Width**, seleziona ***20/40Mhz*** Ce .
7. Nel campo **Frequency**, imposta una frequenza standard (***2412***, ***2437*** o ***2462***).
8. Nel campo **SSID**, digita il nome che vuoi dare alla tua rete (es. ***GREENET***)
9. Nel campo **Wireless Protocol**, seleziona ***802.11*** .
10. Nel campo **WPS mode**, seleziona ***disabled*** .
11. Nel campo **Frequency Mode**, seleziona ***regolautory-domain.***
12. Nel campo **Country**, seleziona ***Italy*** .
13. Nel campo **Installation**, seleziona ***indoor***.
14. Accertati nella parte bassa della finestra sia flaggato il **Multicast Buffering**.
15. Cliccare su **Apply** e successivamente su **Enable**.
16. Cliccare sul tab **Security Profile** della finestra Wireless Tables.
17. Cliccare due volte sulla voce **default**.
18. Nel campo **Mode**, selezionare ***dynamic key*** .
19. Nel campo **Authentication Types**, inserisci il flag su **WPA2 PSK** .
20. Nel campo **Unicast Ciphers** e **Group Ciphers**, inserisci il flag su **aes ccm**.
21. Nel campo **WPA2 Pre-Shared key**, digita la password del tuo Wi-Fi (es. ***green2805***).
22. Infine clicca su OK.
23. Ora configuriamo allo stesso modo l'interfaccia wlan2.
24. Cliccare sul tab **Wireless** e cliccare due volte sull'interfaccia **wlan2**.

25. Ripeti i punti: 2,4,8,9,10,11,12,13,14
26. Nel campo **Band**, seleziona ***5Ghz-A/N/AC*** .
27. Nel campo **Channel Width**, seleziona ***20/40/80Mhz*** Ceee
28. Nel campo ***Frequency***, imposta una frequenza standard (es.***5260***) se vuoi approfondire vedi questa pagina

Ora dovresti riuscire a collegarti anche alle interfacce wi-fi con la medesima password. Dovreste avere le due interfacce configurate come in figura 17.

Se vuoi utilizzare password differenti per il Wi-Fi 2,4Ghz e 5Ghz, puoi creare un nuovo Profilo dal menu Security Profile e richiamarlo nella configurazione dell'interfaccia Wireless.

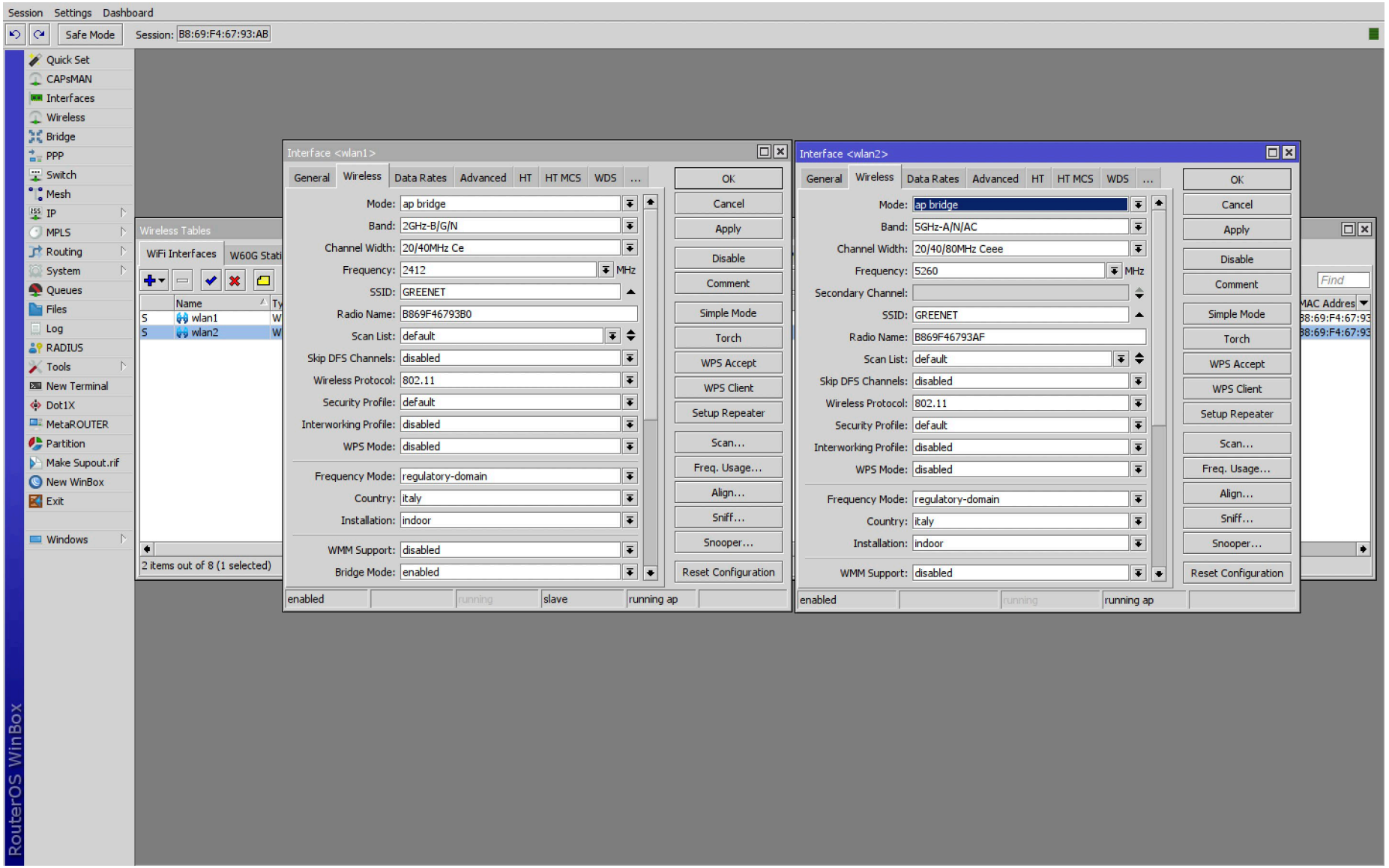


fig.17 – Configurare le Interfacce wireless

Obbiettivo 14: Salvare la configurazione e il backup

In RouterOS, si può salvare la configurazione in due modalità differenti: script o backup. Cosa cambia?

Il backup si utilizza per ricaricarlo sul medesimo Router, esso esporta anche gli utenti del router stesso oltre che la configurazione, e si porta dietro perfino i MAC address del router. Quindi va utilizzato esclusivamente sullo stesso router, o al massimo se il nostro router si rompesse, si porebbe caricare su un router dello stesso identico modello. (Questo, solo se il router da cui è stato salvato il backup è diventato inutilizzabile). Se no ci ritroveremo MAC address duplicati nella rete, creando dei conflitti.

Lo script.rsc si può leggere, editare e caricare su qualsiasi router, esso esporta la configurazione stessa senza utenti e password di accesso, può venir editata in file testo, dal blocco note di Windows o da Wordpad. Importa anche gli utenti vpn.

Come si esporta un backup?

Digitare sul terminale il seguente comando: ***system backup save name=backup_base***

Come si esporta uno script editabile.rsc?

Digitare sul terminale il seguente comando: export file=script_base

Entrambi i Files, si potranno trovare nel tab **Files** di Winbox.

Obbiettivo 15: Testare il funzionamento dei due percorsi.

1. Collega un PC sulla porta ether3.
2. Imposta un indirizzo statico, nella scheda di rete del pc. Se preferisci puoi impostarlo in Dhcp-client.
3. Accertati che il PC vada su internet.

4. Vai sul sito: https://www.mio-ip.it/
5. Accertati che l'indirizzo IP pubblico corrisponda a quello della linea FTTH.
6. Collega un PC sulla porta ether4.
7. Ripeti gli stessi passi già eseguiti con la precedente connessione, e accertati che la connessione sulla ether4 usi la connessione ADSL

Sei già abbastanza esperto con RouterOS e vuoi configurare la tua Routerboard da terminale??

Ecco qui di seguito lo script:

---

script_base.rsc

```
/interface bridge
add name=bridge_LAN
/interface ethernet
set [ find default-name=ether1 ] comment=Interfaccia_pubblica
set [ find default-name=ether2 ] comment=------------------------------LAN------------------------------
/interface wireless
set [ find default-name=wlan1 ] band=2ghz-b/g/n channel-width=20/40mhz-Ce country=italy disabled=no installation=indoor mode=ap-bridge ssid=GREENET wireless-protocol=802.11 \
    wps-mode=disabled
set [ find default-name=wlan2 ] band=5ghz-a/n/ac channel-width=20/40/80mhz-Ceee country=italy disabled=no frequency=5260 installation=indoor mode=ap-bridge ssid=GREENET \
    wireless-protocol=802.11 wps-mode=disabled
```

```
/interface lte apn
set [ find default=yes ] ip-type=ipv4-ipv6
/interface wireless security-profiles
set [ find default=yes ] authentication-types=wpa2-psk eap-methods="" mode=dynamic-keys supplicant-identity=MikroTik wpa2-pre-shared-key=green2805
/ip pool
add name=pool-dhcp ranges=192.168.120.100-192.168.120.150
/ip dhcp-server
add address-pool=pool-dhcp disabled=no interface=bridge_LAN lease-time=12h name=dhcp-server
/interface bridge port
add bridge=bridge_LAN interface=ether2
add bridge=bridge_LAN interface=ether3
add bridge=bridge_LAN interface=ether4
add bridge=bridge_LAN interface=ether5
add bridge=bridge_LAN interface=wlan1
add bridge=bridge_LAN interface=wlan2
/ip settings
set max-neighbor-entries=2048
/interface ovpn-server server
set auth=sha1,md5
/ip address
add address=1.2.3.4 interface=ether1 network=10.246.159.50
add address=192.168.120.1/24 interface=bridge_LAN network=192.168.120.0
/ip dhcp-server network
add address=192.168.120.0/24 dns-server=192.168.120.1 domain=WORKGROUP gateway=192.168.120.1 netmask=24
/ip dns
set allow-remote-requests=yes servers=1.1.1.1,208.67.222.220
/ip dns static
add address=192.168.120.1 regexp=router.lan
```

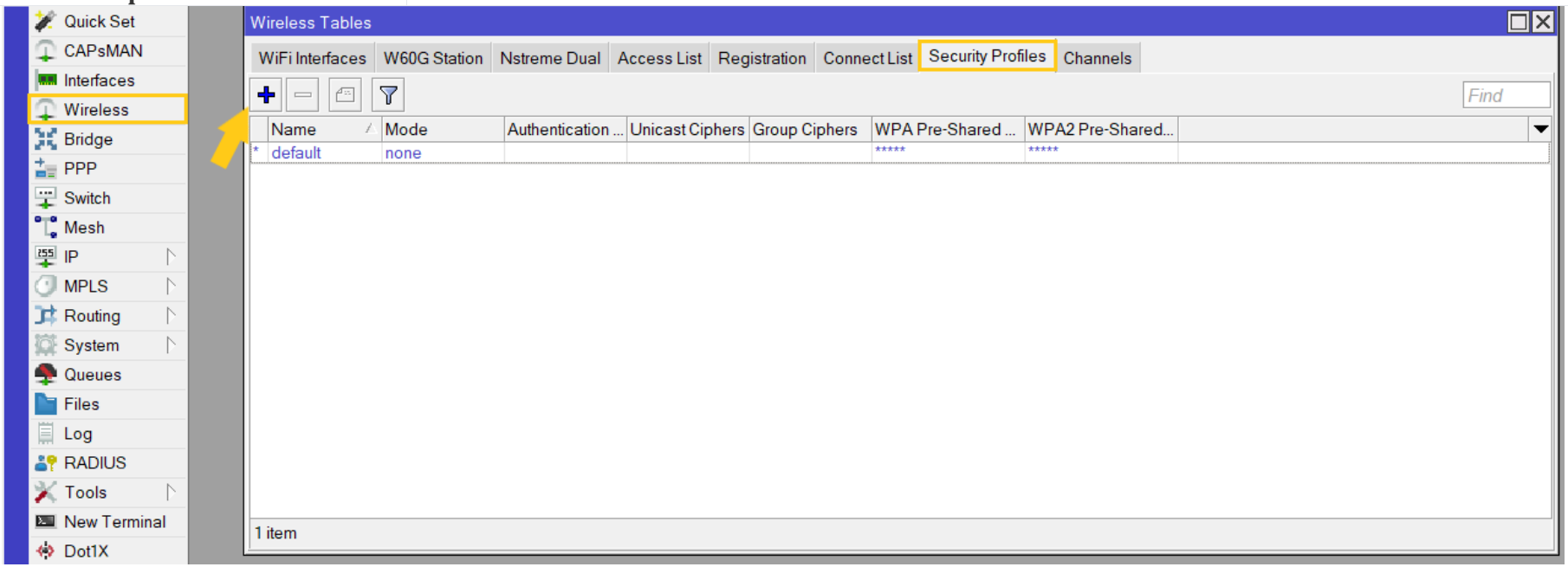
```
/ip firewall filter
add action=accept chain=input connection-state=established,related,untracked
add action=drop chain=input connection-state=invalid
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1 src-address=192.168.120.0/24
/ip route
add distance=1 gateway=10.246.159.50
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www address=192.168.120.0/24
set ssh address=192.168.120.0/24
set api disabled=yes
set winbox address=192.168.120.0/24
set api-ssl disabled=yes
/system clock
set time-zone-name=Europe/Rome
/system identity
set name=Router-ufficio
```

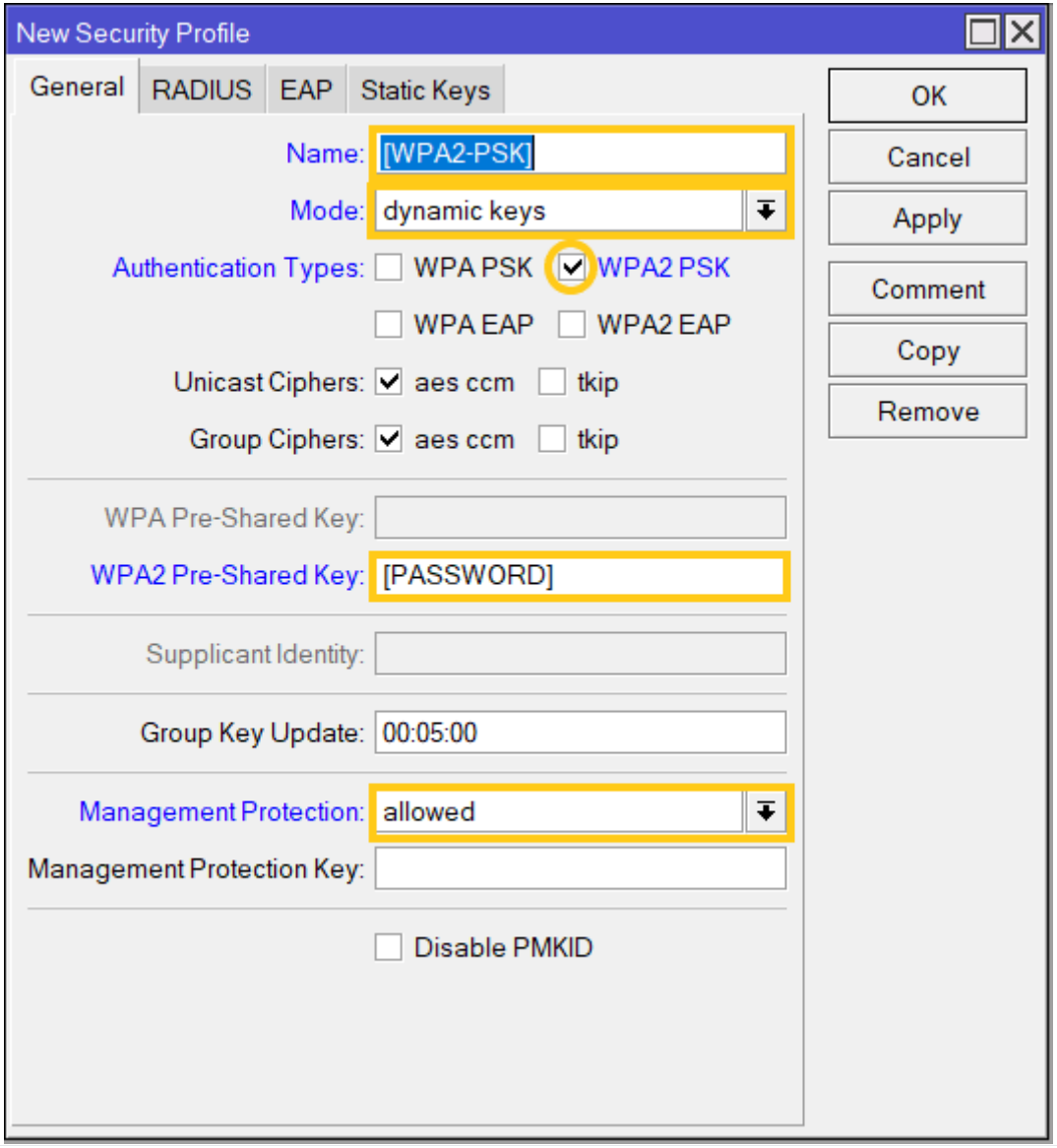
Come configurare una rete WiFi MikroTik?

Come sempre, MikroTik ci permette di effettuare la configurazione della nostra routerboard sia utilizzando l'interfaccia grafica di **Winbox**, scaricabile sul sito Mikrotik, sia **da terminale connettendosi al dispositivo via telnet o ssh.**
Per configurare una rete WiFi base avremo bisogno di:

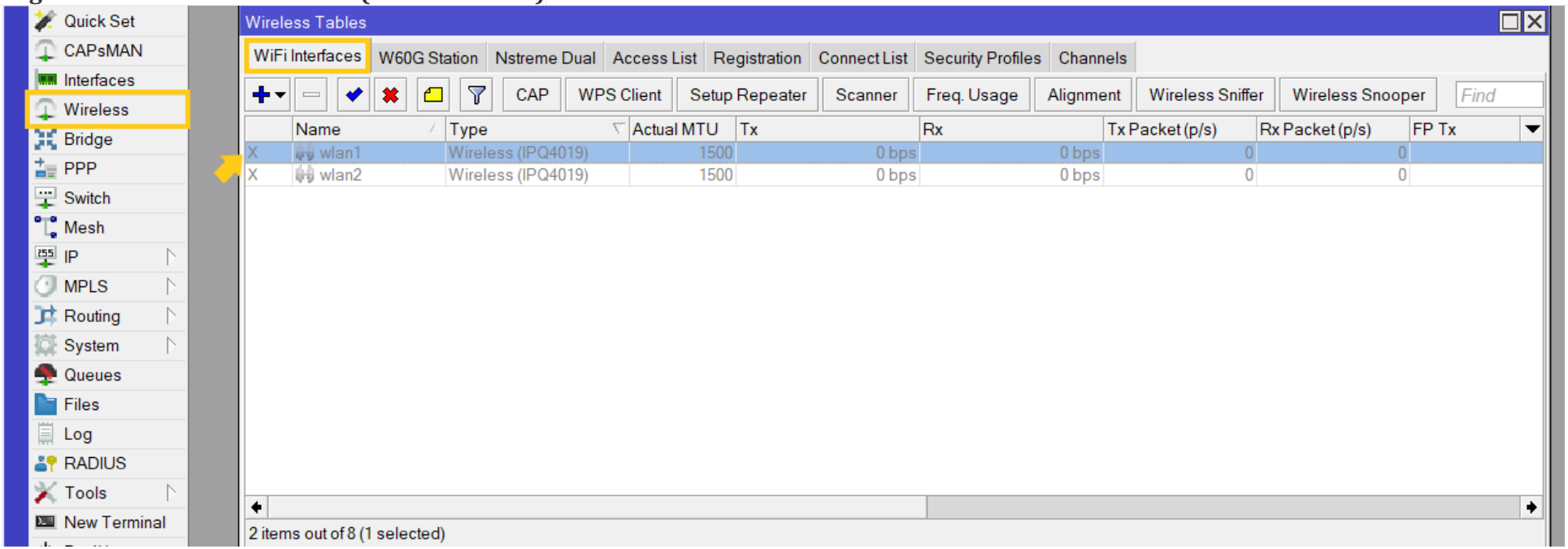
- Configurare le impostazioni di sicurezza
- Configurare l'interfaccia Wireless
- Configurare un bridge in cui includere le interfacce LAN e WiFi
- Attribuire una subnet privata all'interfaccia bridge
- Configurare un DHCP server per rilasciare gli IP privati ai dispositivi che si connetteranno in WiFi
- Creare una regola di NAT per permettere agli apparati connessi di navigare
- Attivare i moduli WiFi del router

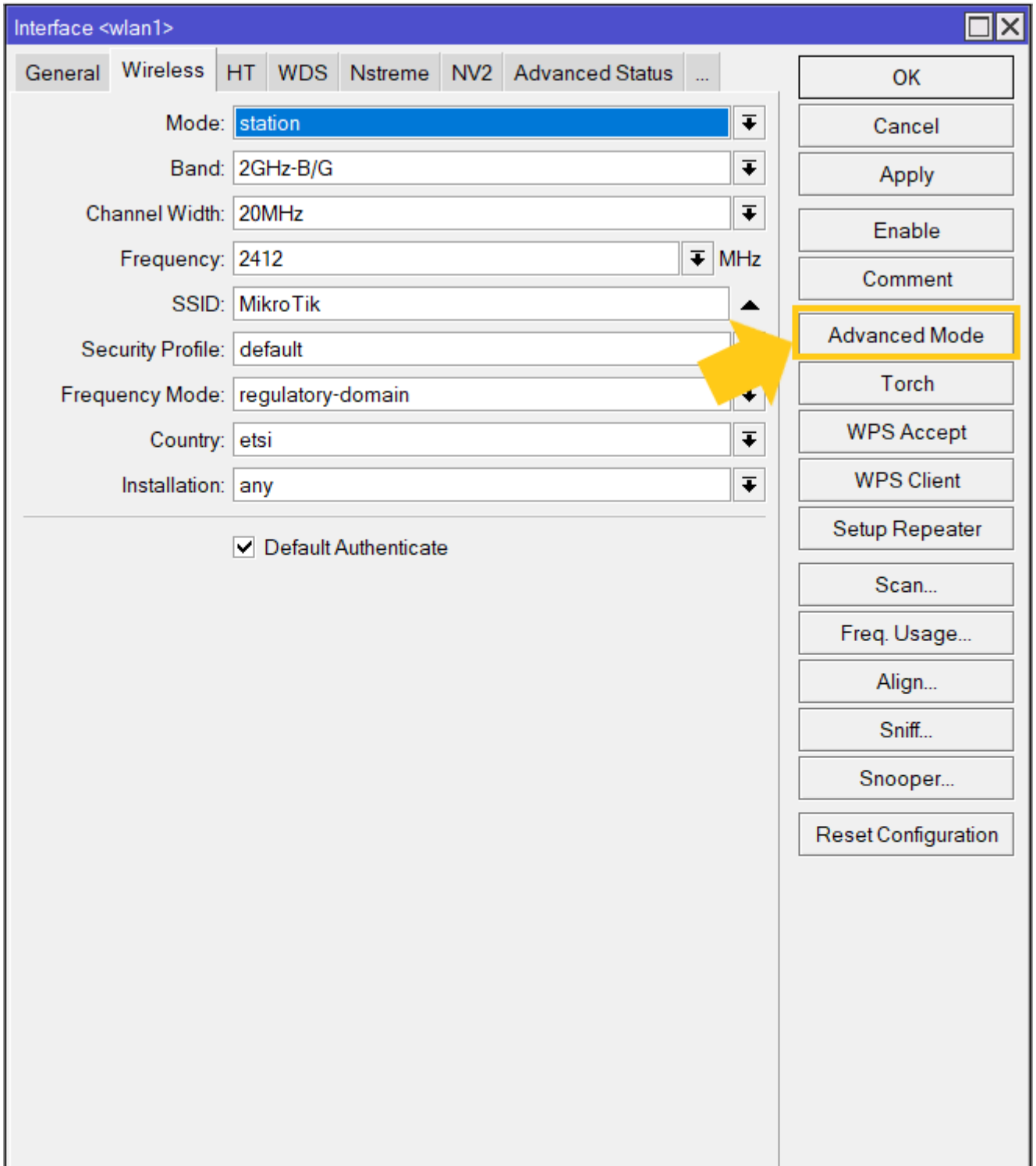
1.Configurare le impostazioni di sicurezza

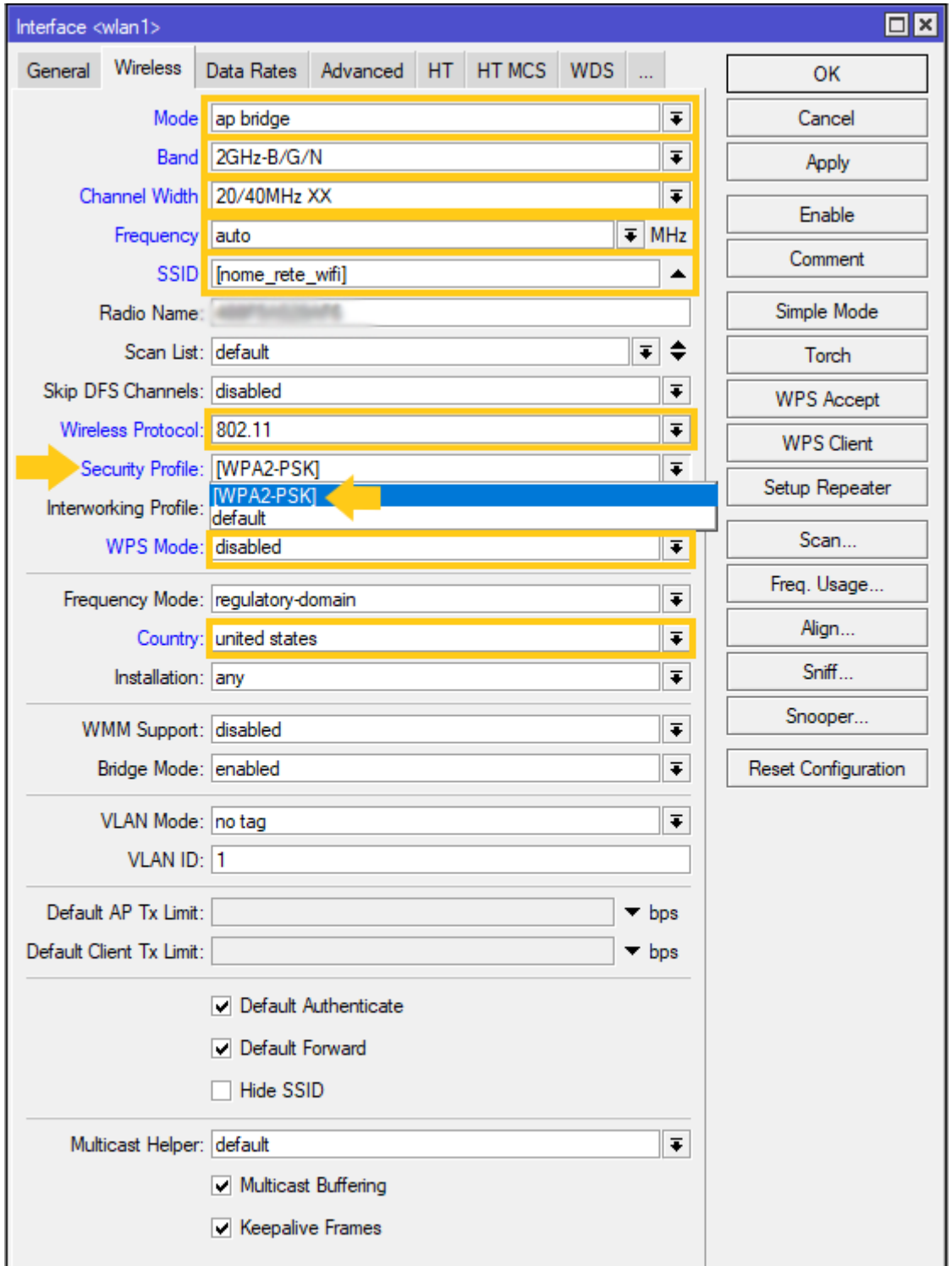


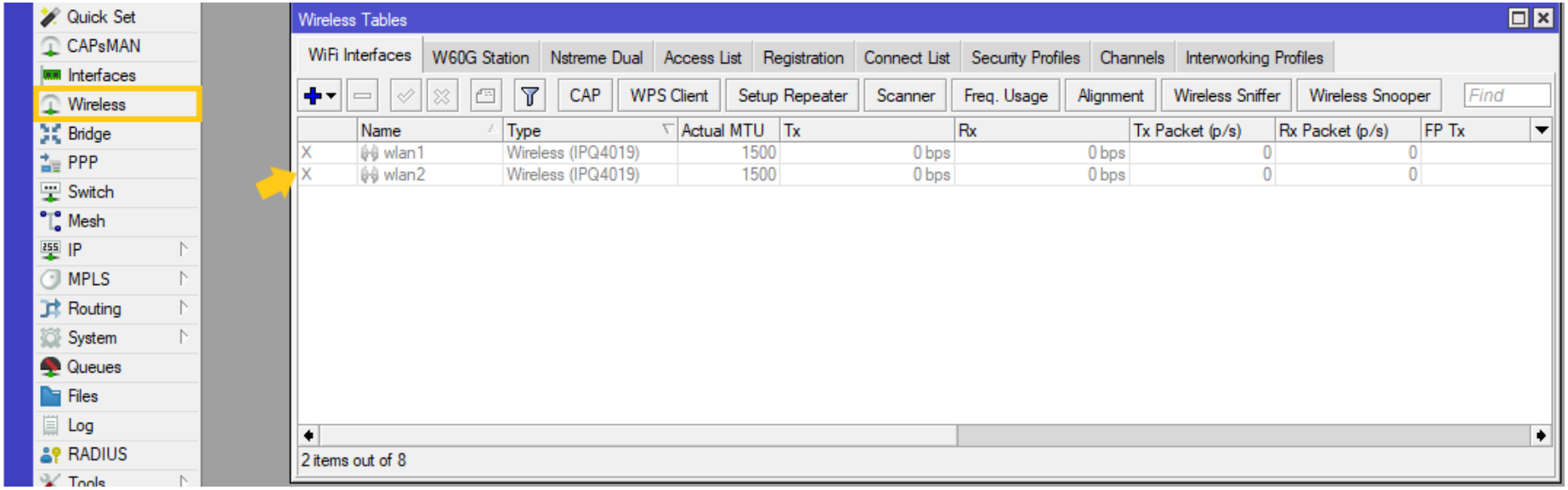

New Security Profile
General
RADIUS
EAP
Static Keys
OK
Cancel
Apply
Comment
Copy
Remove
Name: [WPA2-PSK]
Mode: dynamic keys
Authentication Types: WPA PSK WPA2 PSK
WPA EAP WPA2 EAP
Unicast Ciphers: aes ccm tkip
Group Ciphers: aes ccm tkip
WPA Pre-Shared Key:
WPA2 Pre-Shared Key: [PASSWORD]
Supplicant Identity:
Group Key Update: 00:05:00
Management Protection: allowed
Management Protection Key:
Disable PMKID

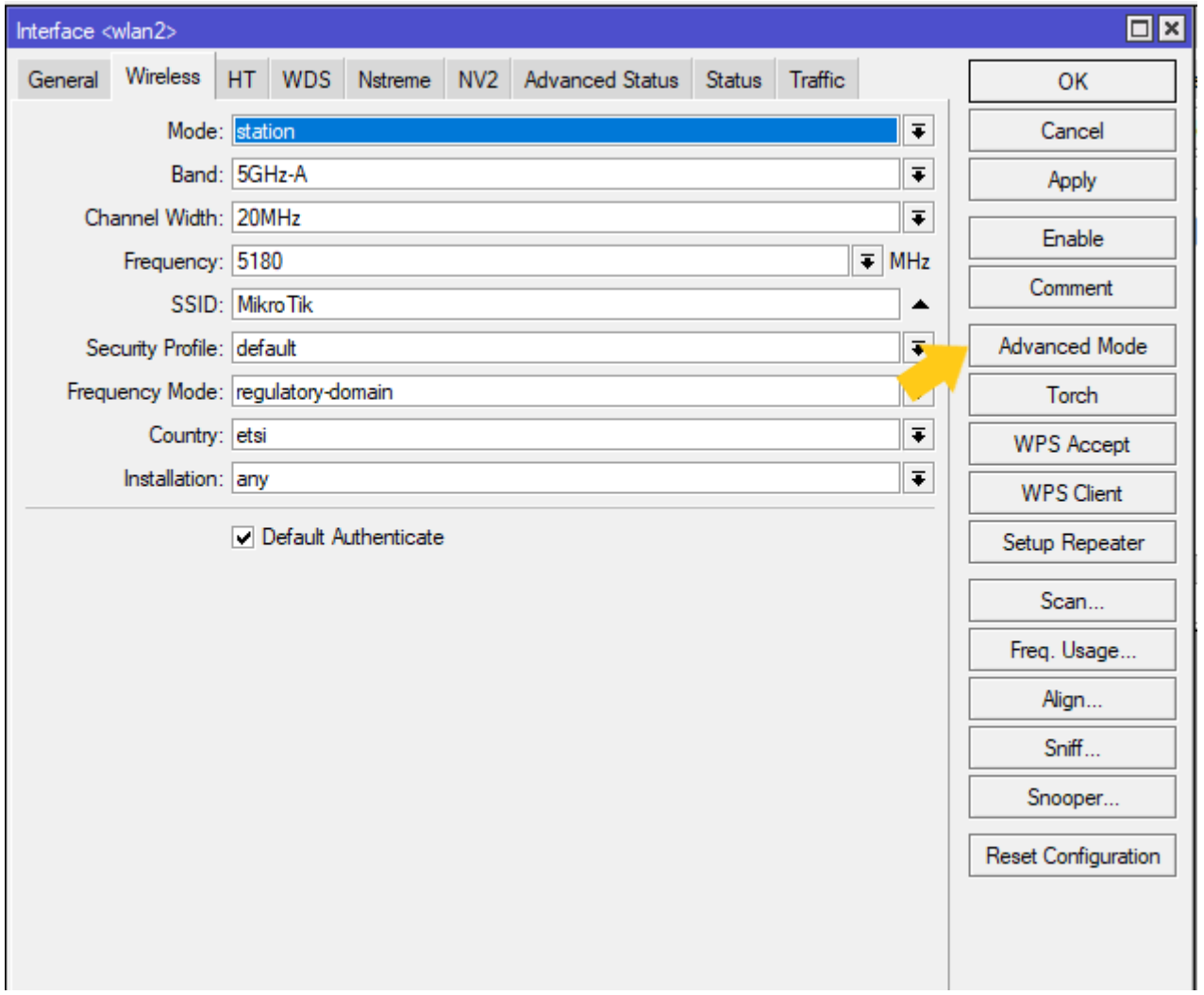
2.Configurare l'interfaccia Wireless (wlan1 – wlan2)

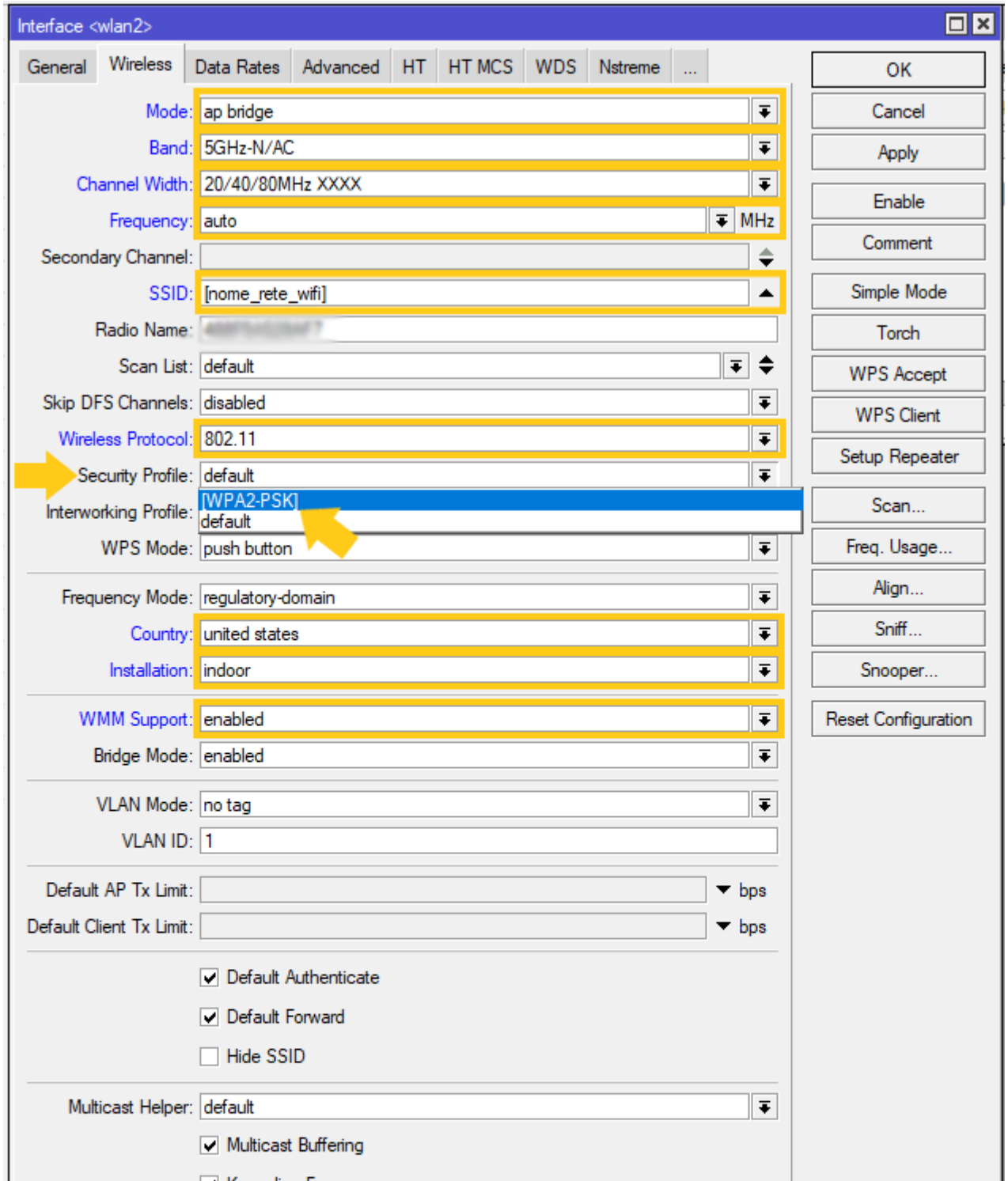



Interface <wlan1>
General
Wireless
HT
WDS
Nstreme
NV2
Advanced Status
...
Mode:
station
Band:
2GHz-B/G
Channel Width:
20MHz
Frequency:
2412
MHz
SSID:
MikroTik
Security Profile:
default
Frequency Mode:
regulatory-domain
Country:
etsi
Installation:
any
Default Authenticate
OK
Cancel
Apply
Enable
Comment
Advanced Mode
Torch
WPS Accept
WPS Client
Setup Repeater
Scan...
Freq. Usage...
Align...
Sniff...
Snooper...
Reset Configuration

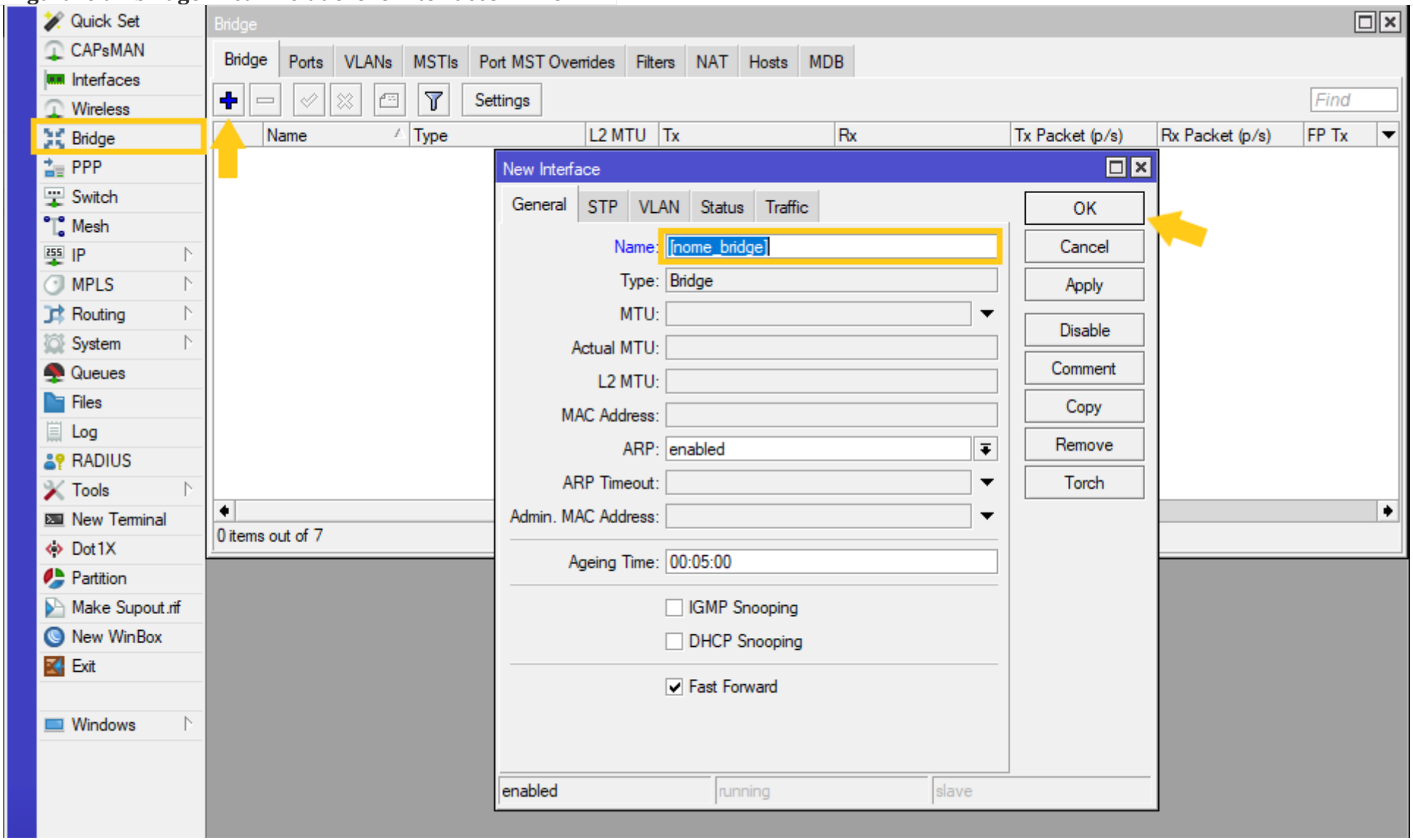

Interface <wlan1>
General
Wireless
Data Rates
Advanced
HT
HT MCS
WDS
...
Mode: ap bridge
Band: 2GHz-B/G/N
Channel Width: 20/40MHz XX
Frequency: auto MHz
SSID: [nome_rete_wifi]
Radio Name:
Scan List: default
Skip DFS Channels: disabled
Wireless Protocol: 802.11
Security Profile: [WPA2-PSK]
Interworking Profile:
[WPA2-PSK]
default
WPS Mode: disabled
Frequency Mode: regulatory-domain
Country: united states
Installation: any
WMM Support: disabled
Bridge Mode: enabled
VLAN Mode: no tag
VLAN ID: 1
Default AP Tx Limit: bps
Default Client Tx Limit: bps
Default Authenticate
Default Forward
Hide SSID
Multicast Helper: default
Multicast Buffering
Keepalive Frames
OK
Cancel
Apply
Enable
Comment
Simple Mode
Torch
WPS Accept
WPS Client
Setup Repeater
Scan...
Freq. Usage...
Align...
Sniff...
Snooper...
Reset Configuration

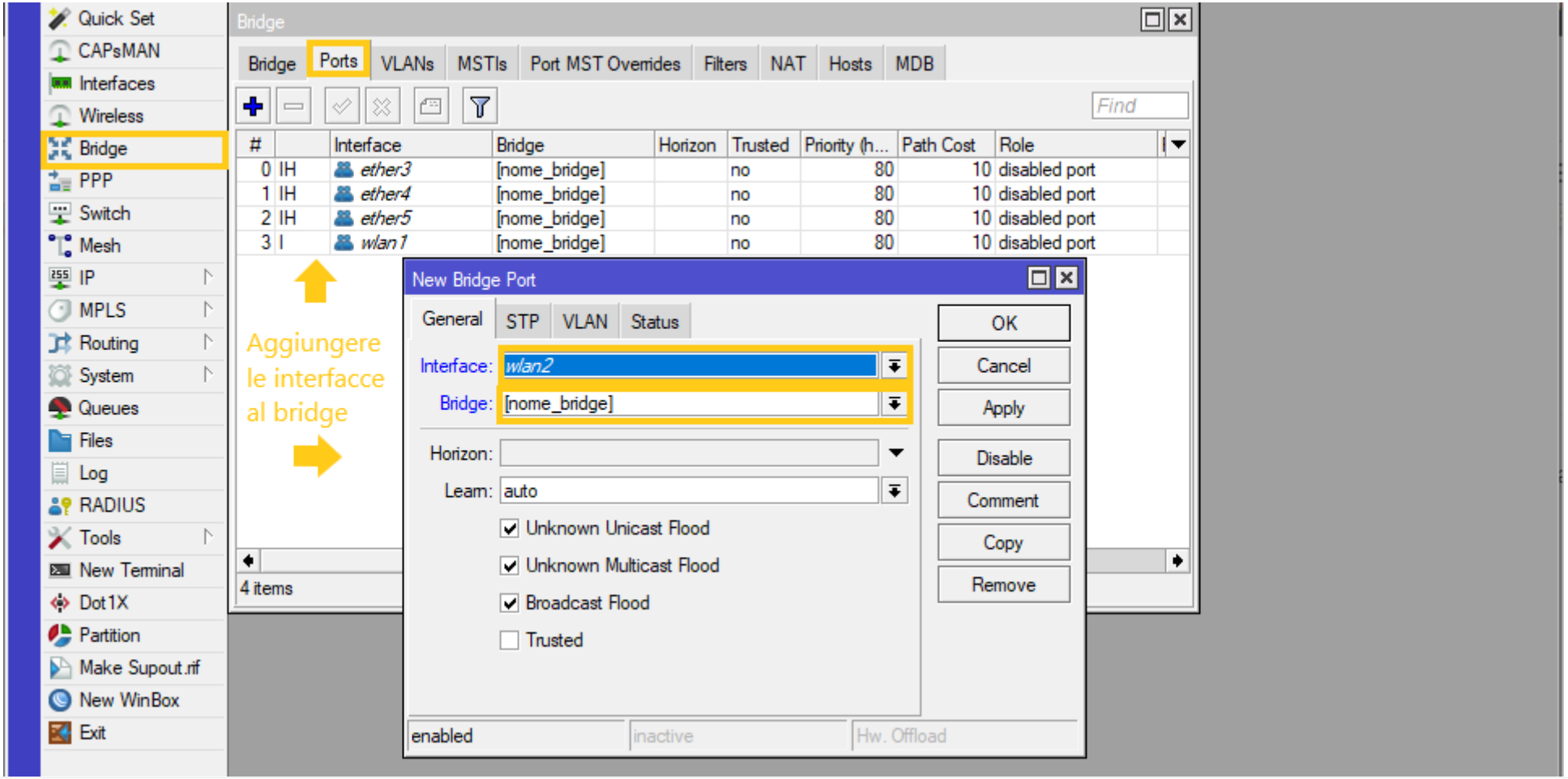

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
Wireless Tables
WiFi Interfaces
W60G Station
Nstreme Dual
Access List
Registration
Connect List
Security Profiles
Channels
Interworking Profiles
CAP
WPS Client
Setup Repeater
Scanner
Freq. Usage
Alignment
Wireless Sniffer
Wireless Snooper
Find
Name
Type
Actual MTU
Tx
Rx
Tx Packet (p/s)
Rx Packet (p/s)
FP Tx
X wlan1 Wireless (IPQ4019) 1500 0 bps 0 bps 0 0
X wlan2 Wireless (IPQ4019) 1500 0 bps 0 bps 0 0
2 items out of 8


Interface <wlan2>
General
Wireless
HT
WDS
Nstreme
NV2
Advanced Status
Status
Traffic
Mode: station
Band: 5GHz-A
Channel Width: 20MHz
Frequency: 5180 MHz
SSID: MikroTik
Security Profile: default
Frequency Mode: regulatory-domain
Country: etsi
Installation: any
Default Authenticate
OK
Cancel
Apply
Enable
Comment
Advanced Mode
Torch
WPS Accept
WPS Client
Setup Repeater
Scan...
Freq. Usage...
Align...
Sniff...
Snooper...
Reset Configuration

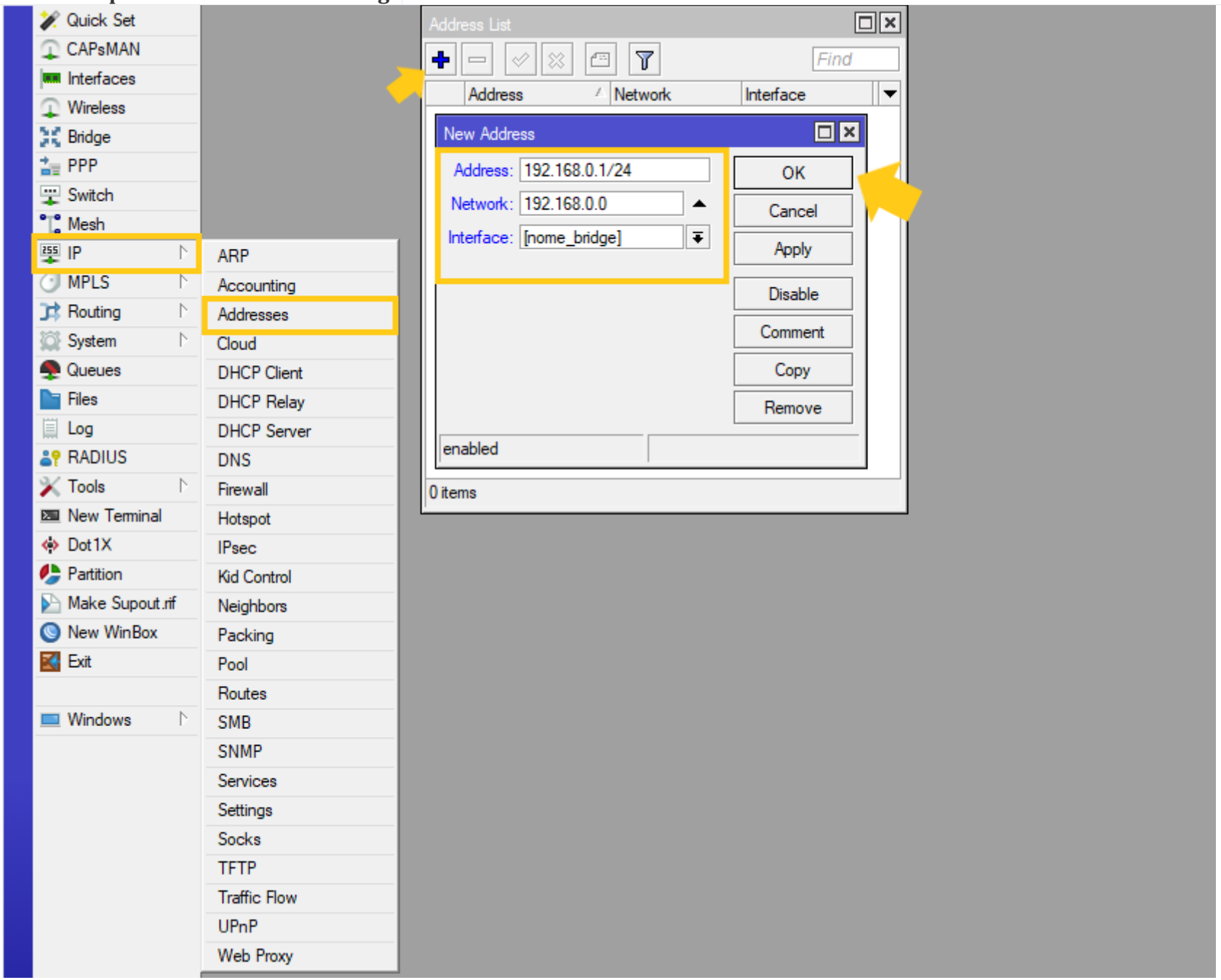

Interface <wlan2>
General
Wireless
Data Rates
Advanced
HT
HT MCS
WDS
Nstreme
...
Mode: ap bridge
Band: 5GHz-N/AC
Channel Width: 20/40/80MHz XXXX
Frequency: auto MHz
Secondary Channel:
SSID: [nome_rete_wifi]
Radio Name:
Scan List: default
Skip DFS Channels: disabled
Wireless Protocol: 802.11
Security Profile: default
Interworking Profile:
WPS Mode: push button
[WPA2-PSK]
default
Frequency Mode: regulatory-domain
Country: united states
Installation: indoor
WMM Support: enabled
Bridge Mode: enabled
VLAN Mode: no tag
VLAN ID: 1
Default AP Tx Limit: bps
Default Client Tx Limit: bps
Default Authenticate
Default Forward
Hide SSID
Multicast Helper: default
Multicast Buffering
OK
Cancel
Apply
Enable
Comment
Simple Mode
Torch
WPS Accept
WPS Client
Setup Repeater
Scan...
Freq. Usage...
Align...
Sniff...
Snooper...
Reset Configuration

3.Configurare un bridge in cui includere le interfacce LAN e WiFi

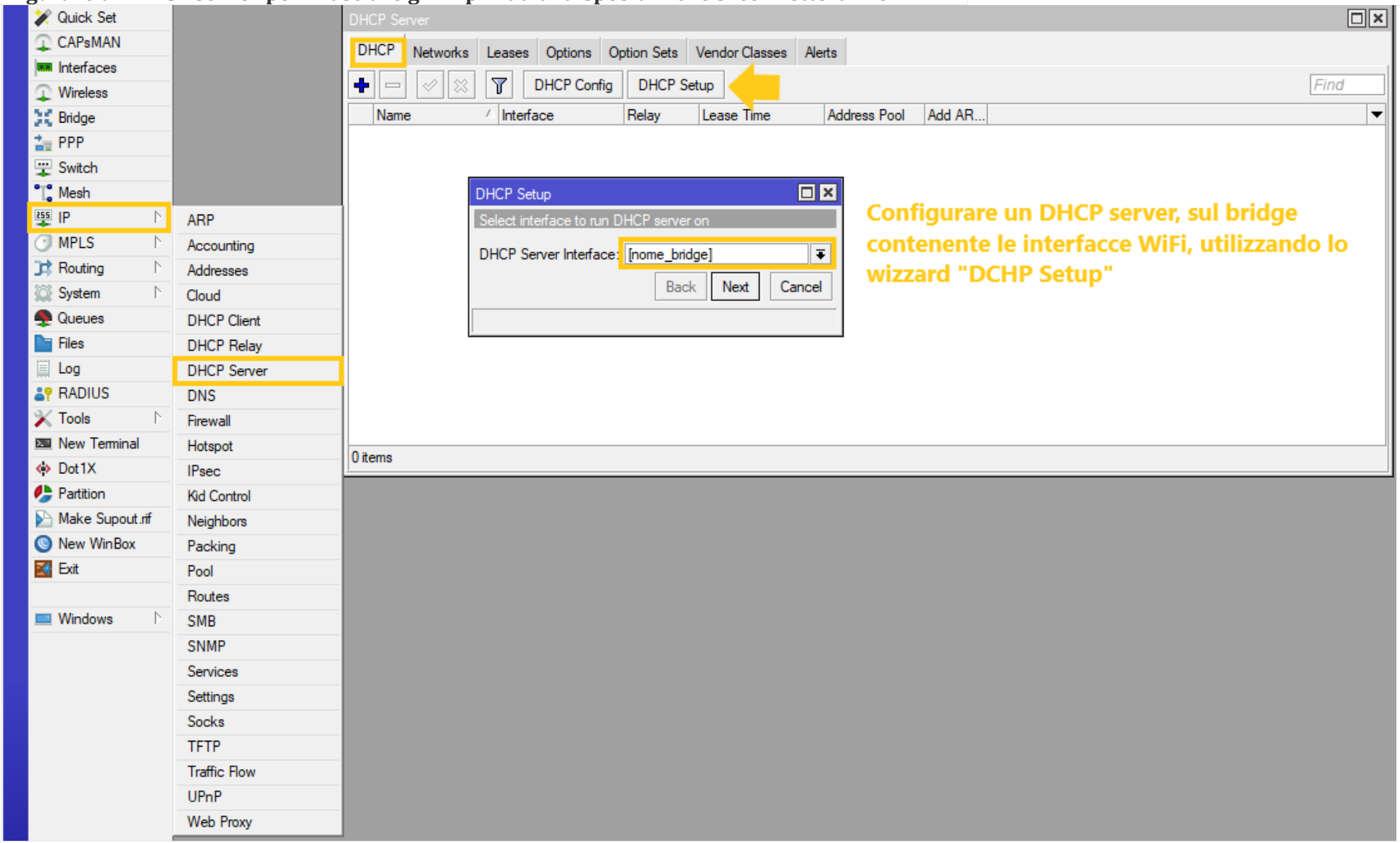



Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Partition
Make Supout.rif
New WinBox
Exit
Bridge
Bridge
Ports
VLANs
MSTIs
Port MST Overrides
Filters
NAT
Hosts
MDB
Find
Interface Bridge Horizon Trusted Priority (h... Path Cost Role
0 IH ether3 [nome_bridge] no 80 10 disabled port
1 IH ether4 [nome_bridge] no 80 10 disabled port
2 IH ether5 [nome_bridge] no 80 10 disabled port
3 I wlan1 [nome_bridge] no 80 10 disabled port
4 items
Aggiungere le interfacce al bridge
New Bridge Port
General
STP
VLAN
Status
Interface: wlan2
Bridge: [nome_bridge]
Horizon:
Learn: auto
Unknown Unicast Flood
Unknown Multicast Flood
Broadcast Flood
Trusted
OK
Cancel
Apply
Disable
Comment
Copy
Remove
enabled
inactive
Hw. Offload

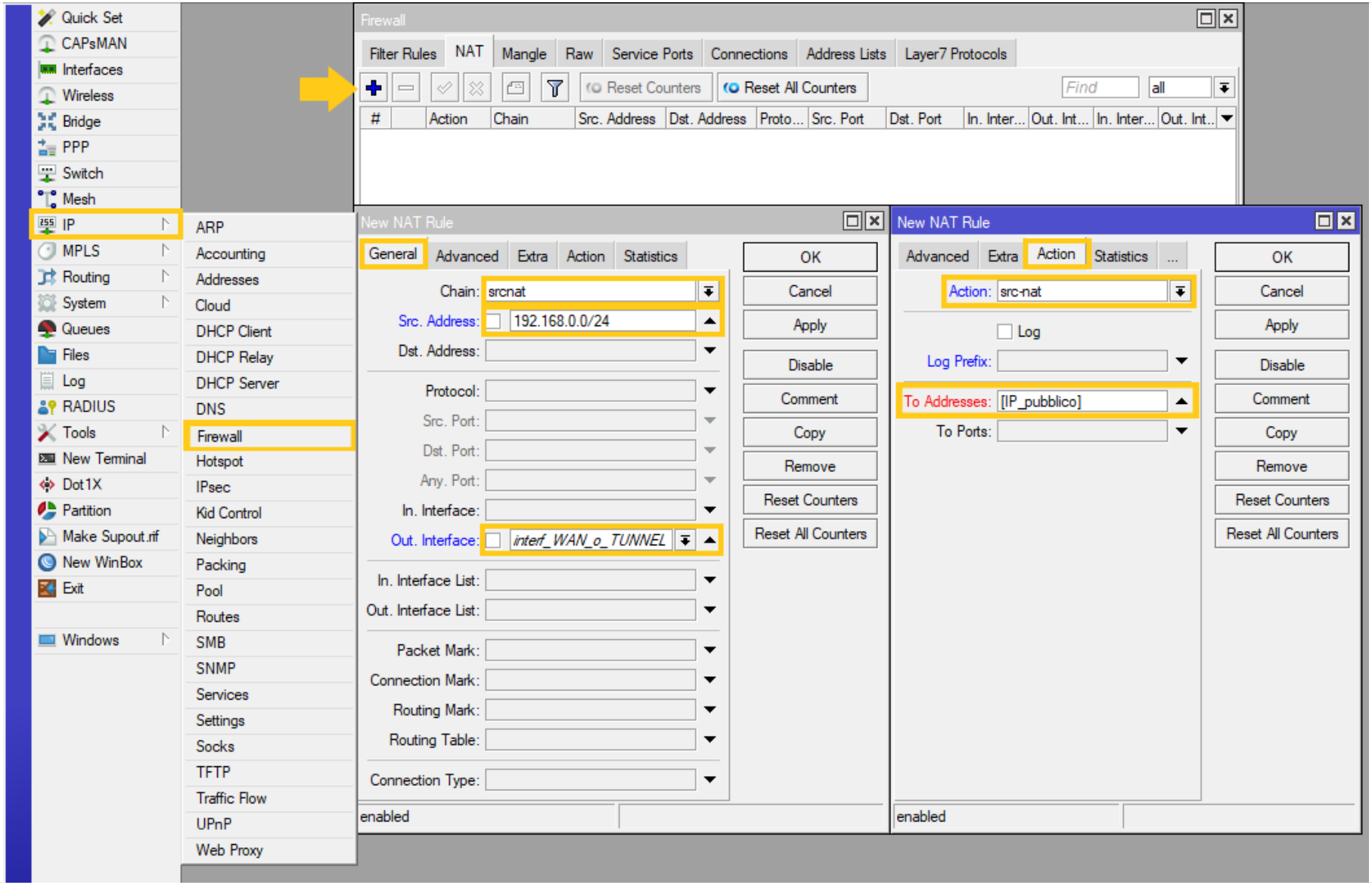
4.Attribuire una subnet privata all'interfaccia bridge



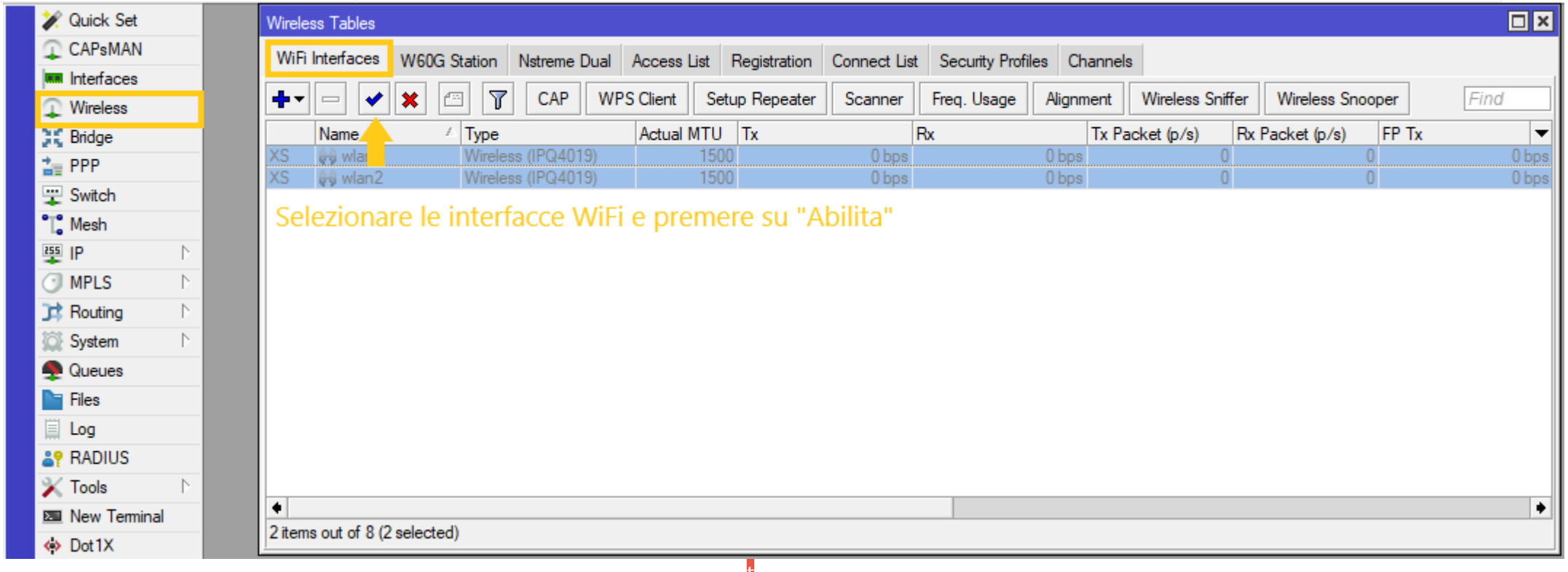
5.Configurare un DHCP server per rilasciare gli IP privati ai dispositivi che si connetteranno in WiFi



6.Creare una regola di NAT per permettere agli apparati connessi di navigare



7.Attivare i moduli WiFi del router



E se avessimo bisogno di eseguire la configurazione senza accedere all'interfaccia grafica?
Nessun problema, come di consueto, ecco di seguito uno script di configurazione ad hoc, sarà sufficiente modificare i caratteri tra le virgolette preceduti da ":global".
L'assegnazione dei valori delle global é riportata in ogni segmento dello script; ogni parte dello script può essere utilizzata in modo indipendente.

```
#Configurare le impostazioni di sicurezza
:global WPAPSK2 "nome del security profile. Es. WPAPSK2"
:global PASSWORD "Password rete WiFi"
/interface wireless security-profiles
add authentication-types=wpa2-psk eap-methods="" management-protection=allowed mode=dynamic-keys name=$WPAPSK2 supplicant-identity="" wpa2-pre-shared-key=$PASSWORD
#.Configurare l'interfaccia Wireless (wlan1 – wlan2)
:global SSID "nome della rete WiFi Es. Wifiufficio"
/interface wireless
set [ find default-name=wlan1 ] band=2ghz-b/g/n channel-width=20/40mhz-XX country="united states" disabled=no frequency=auto mode=ap-bridge
```

```
security-profile=$WPAPSK2 ssid=$SSID wireless-protocol=802.11 wps-mode=disabled
set [ find default-name=wlan2 ] band=5ghz-n/ac channel-width=20/40/80mhz-XXXX country=”united states” disabled=no frequency=auto mode=ap-bridge
security-profile=$WPAPSK2 ssid=$SSID wireless-protocol=802.11 wmm-support=enabled wps-mode=disabled
#.Configurare un bridge in cui includere le interfacce LAN e WiFi
:global nomebridge “nome bridge Es. brLAN35+WiFi”
/interface bridge
add name=$nomebridge
/interface bridge port
add bridge=$nomebridge interface=ether3
add bridge=$nomebridge interface=ether4
add bridge=$nomebridge interface=ether5
add bridge=$nomebridge interface=wlan1
add bridge=$nomebridge interface=wlan2
#.Attribuire una subnet privata all’interfaccia bridge
:global nomebridge “nome bridge Es. brLAN35+WiFi”
:global IPGW “IP GW da assegnare al router MK per rete privata Es. 192.168.0.1/24”
:global IPNW “IP di network della classe IP assegnata su rete privata Es. 192.168.0.0”
/ip address
add address=$IPGW interface=$nomebridge network=$IPNW
#.Configurare un DHCP server per rilasciare gli IP privati ai dispositivi che si connetteranno in WiFi
:global dhcpsrv “nome del server dhcp Es. dhcp_ufficio”
:global nomebridge “nome bridge Es. brLAN35+WiFi”
:global dhcppool “nome del dhcp pool Es. dhcppool_ufficio”
:global IPnetwork “IP network Es. 192.168.0.0/24”
:global serverdns “Server DNS Es. 8.8.8.8 o 1.1.1.1 o IP Gateway router se avete configurato IP->DNS”
:global IPGWdhcp “IP gateway router Es. 192.168.0.1”
:global rangeIPdhcp “Range di IP che il server DHCP distribuirà ai dhcp client Es. 192.168.0.100-192.168.0.200”
/ip pool
add name=$dhcppool ranges=$rangeIPdhcp
/ip dhcp-server
add address-pool=$dhcppool disabled=no interface=$nomebridge lease-time=1d name=$dhcpsrv
/ip dhcp-server network
add address=$IPnetwork dns-server=$serverdns gateway=$IPGWdhcp
#.Creare una regola di NAT per permettere agli apparati connessi di navigare
:global interfWANoTUNNEL “Interfaccia WAN o tunnel per navigazione Es. ether1 o pppoe_internet”
:global IPnetwork “IP network Es. 192.168.0.0/24”
:global IPpubblico “IP pubblico connettività”
```

```
/ip firewall nat
add action=src-nat chain=srcnat out-interface=$interfWANoTUNNEL src-address=$IPnetwork to-addresses=$IPpubblico
# In caso di connettività con IP dinamico possiamo creare una regola di masquerade al posto della src-nat, come riportato di seguito
/ip firewall nat
add action=masquerade chain=srcnat out-interface=$interfWANoTUNNEL src-address=$IPnetwork
#.Attivare i moduli WiFi del router
# Sarà sufficiente applicare lo script da terminale per attivare i moduli WiFi
```

NAT significato: dall'acronimo in poi

Partiamo dall'acronimo, NAT: **Network Address Translation.**
Impostare una regola di NAT **permette di modificare gli indirizzi IP contenuti negli header dei pacchetti dati**. Quelli che, ad esempio, girano per Internet portandosi dietro le informazioni.

Pensiamo per esempio a quando vogliamo raggiungere un motore di ricerca dal nostro PC.
Il nostro computer non può presentarsi a Google con l'IP che utilizza nella rete locale, non riceverebbe alcuna risposta.
Il PC si presenterà con il suo indirizzo IP privato al router che, **attraverso il NAT, andrà a "tradurre" l'IP contenuto nell'header del pacchetto con l'indirizzo IP pubblico**, così da navigare correttamente in internet.

A seconda di cosa vorrò raggiungere e della rete da cui mi presento avrò bisogno di una regola di Source NAT, Destination NAT o Masquerade.

Source NAT: permette di modificare l'IP sorgente del pacchetto (esempio da rete locale a internet)
Destination NAT: permette di modificare l'IP di destinazione del pacchetto (esempio da internet a rete locale)
Masquerade: permette di "tradurre" l'IP nel primo disponibile sull'interfaccia (esempio per navigare da una rete locale a internet in presenza d'IP pubblico dinamico)

Attraverso le regole di NAT possiamo riuscire poi a configurare quello che viene definito **Port Forwarding**.

Port Forwarding Mikrotik: a cosa serve

Per dirla in termini comprensibili ai più, configurare un Port Forwarding, Mikrotik o meno, **permette d'intercettare il traffico dati diretto a un indirizzo IP (a una o più porte) per un determinato protocollo; prenderlo e reindirizzarlo verso un altro IP o una porta differente.**

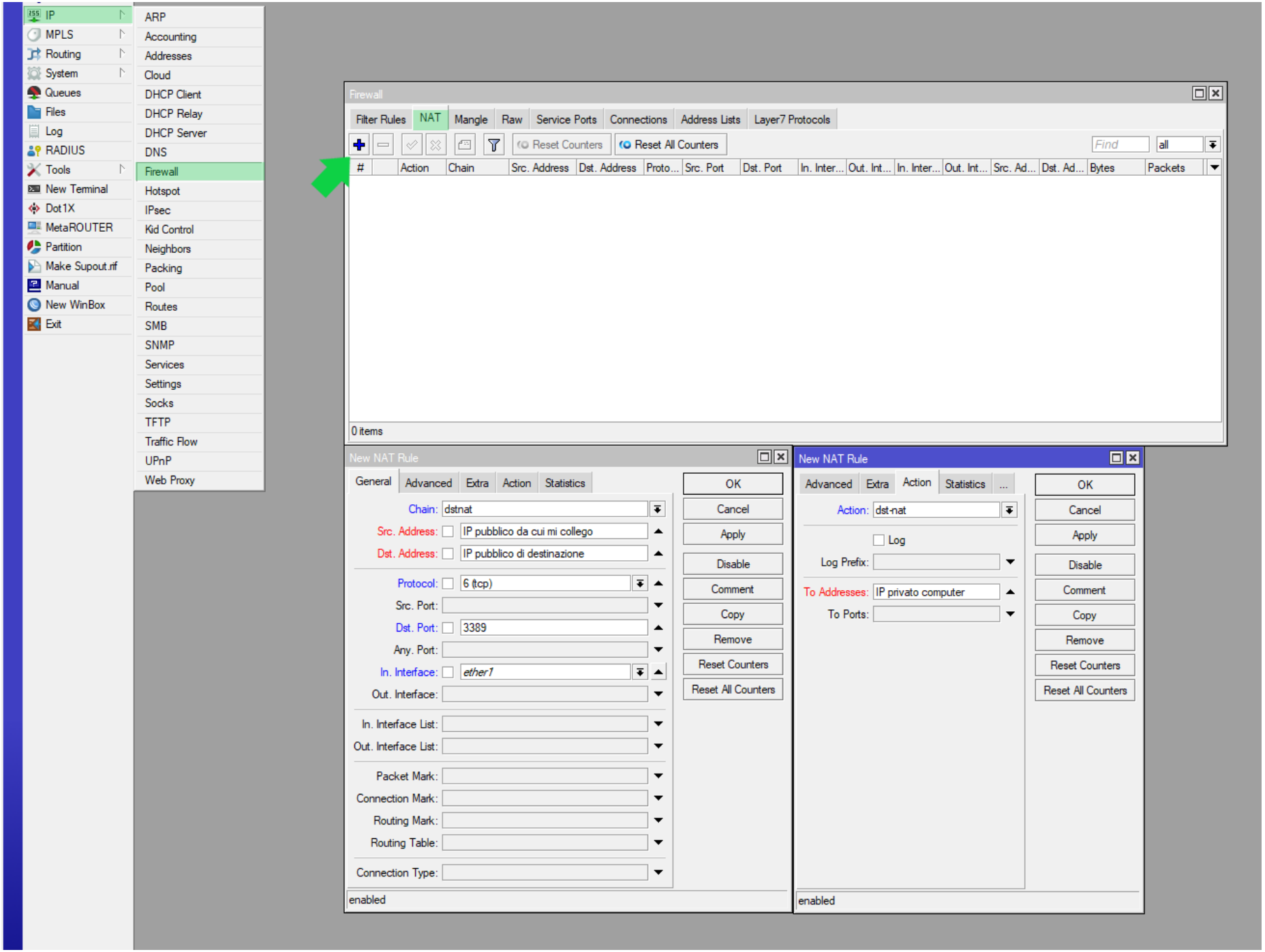
Esempio pratico, quand potrebbe servire il Port Forwarding

Potrei usare un Port Forarding se un mio Cliente mi chiede di configurare il suo Client di posta elettronica e io ho intenzione di farlo usando un desktop remoto.
Utilizzando un desktop remoto, di fatto, vado a collegarmi al suo PC attraverso la porta 3389, passando prima attraverso la rete Internet.

Per poter fare questa azione **devo prima di tutto creare una "regola di NAT" sul Mikrotik del Cliente**.

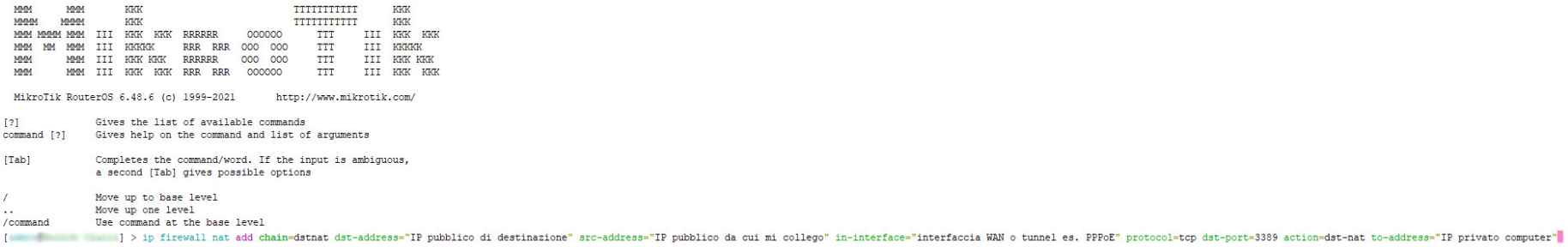
Port Forwarding MikroTik: Configurazione

Per creare un Port Forwarding su MikroTik possiamo utilizzare una regola di **dst-nat.**
Per farlo posso utilizzare sia l'interfaccia grafica via Winbox (scaricabile da sito MikroTik) nella sezione NAT, raggiungibile da IP > Firewall, sia usando i comandi da terminale.


IP
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit
ARP
Accounting
Addresses
Cloud
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Kid Control
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Settings
Socks
TFTP
Traffic Flow
UPnP
Web Proxy
Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
Find
all
Action Chain Src. Address Dst. Address Proto... Src. Port Dst. Port In. Inter... Out. Int... In. Inter... Out. Int... Src. Ad... Dst. Ad... Bytes Packets
0 items
New NAT Rule
General
Advanced
Extra
Action
Statistics
Chain: dstnat
Src. Address: IP pubblico da cui mi collego
Dst. Address: IP pubblico di destinazione
Protocol: 6 (tcp)
Src. Port:
Dst. Port: 3389
Any. Port:
In. Interface: ether1
Out. Interface:
In. Interface List:
Out. Interface List:
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:
enabled
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
New NAT Rule
Advanced
Extra
Action
Statistics
...
Action: dst-nat
Log
Log Prefix:
To Addresses: IP privato computer
To Ports:
enabled
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Un esempio di configurazione Port Forwarding da terminale

roterOS > ip firewall nat add chain=dstnat dst-address="IP pubblico di destinazione" src-address="IP pubblico da cui mi collego" in-interface="interfaccia WAN o tunnel es. PPPoE" protocol=tcp dst-port=3389 action=dst-nat to-addresses=IP privato computer



Rischi del port Forwarding

Realizzando un Port Forwarding **permettiamo di fatto che un dispositivo sia raggiungibile attraverso la rete internet, con la comodità e i rischi che questo comporta.** Ecco perché **è importante creare regole di Port Forwarding specificando l'IP sorgente a cui devono essere applicate (src-address) e creare delle regole di Firewall efficaci.**

NAT MikroTik: peculiarità e attenzioni

MikroTik è un hardware a uso professionale e le possibilità di configurazione, andando anche oltre il NAT MikroTik, sono estremamente elevate. Questo è un grande pro in termini di **flessibilità e sicurezza** ma dobbiamo fare attenzione ai margini di errore che questo comporta durante le configurazioni.

Su Hardware definibile come "consumer", è certo più difficile fare danni ma non si possono eseguire configurazioni complesse necessarie per reti business.

Per questi motivi **è fondamentale una considerazione:** per produrre una rete sicura, è necessario dotarsi di Hardware che permettano una libera configurazione e di professionisti esperti nel farla.

https://foisfabio.it/index.php/category/mikrotik/