### **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 <u>https://mt.lv/winbox64</u>

Componenti necessari:

- 1. Un Router Mikrotik <u>RB952Ui-5ac2nD</u>
- 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:

Ses	sion Settings Dashb	noard Contract Contra
5	Cafe Mode	Session: B8:69:F4:67:93:AA
	💉 Quick Set	
	Interfaces	
	Q Wireless	
	👯 Bridge	
	tan and a set the set of the set	
	🙄 Switch	
	° 🕻 Mesh	
	🏥 IP 🗈 🗅	
	MPLS N	
	Conting N	
	System 🗅	
	Sequences	
	Files	
	Log	
	Tasla	
	New Terminal	
	Partition	
	Make Supout.rif	
	New WinBox	
	K Exit	
4		
Q		
in i		
$\geq$		
S		
5		
lter		
õ		
щ		

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.

Sess	ion Settings Dashb	ard
5	Cafe Mode	Session: 88:69:F4:67:93:AA
	🖋 Quick Set	
	CAPSMAN	
	Interfaces	
	Wireless	
	Bridge	
	PPP	
	T Switch	
	1. Mesh	
	IP D	
	MPLS D	
	Routing	
	System	
	Queues	
	Files	
	Log	Reset Configuration
		Keen User Configuration Reset Configuration
	Now Terminal	
	MetaROUTER	
	Partition	Do Not Backup
	Make Supout.rif	Run After Reset:
	New WinBox	
	K Exit	
	🛄 Windows 🗈 🗈	
×		
B		
in		
$\geq$		
SC		
Li li		
ute		
Ro		

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.

<b>é wine64-preloader</b> Edit Window	🔼 💷 💽 🏵 🧰 Q 岩 💿 Sab 10 dic 13:52
• • •	admin@B8:69:F4:67:93:AA (Router-ufficio) - WinBox (64bit) v6.48.6 on hAP ac lite (mipsbe)
🖉 🖉 Quick Set	
CAPSMAN	
m Interfaces	
📿 Wireless	
💢 Bridge	
The second secon	
The switch	
"  <sup>®</sup> Mesh	
IP	
O MPLS	
<b>Routing</b>	
System P	
Files	
Tools	
2 New Terminal	Identity: Router-ufficio OK
I Dot1X	Cancel
MetaROUTER	Apply
🤔 Partition	- · · · · · · · · · · · · · · · · · · ·
Make Supout.rif	
S New WinBox	
Exit	
Windows	
X	
<u>ě</u>	
S S S S S S S S S S S S S S S S S S S	
Q	
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@blo.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.

	sion Settings Dashboard									
Oddawi         Sorka	Cafe Mode Session: B	38:69:F4:67:93:AB								
	🖉 Quick Set									
	CAPSMAN									
	Interfaces									
	🗘 Wireless									
	Bridge									
	PPP									
Image: Image	🙄 Switch									
p       text is       i </td <td>Mesh</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Mesh									
MPCS       P       Graups       SS91tays       SS91tays <td>IP D</td> <td>User List</td> <td></td> <td></td> <td>IP Service List</td> <td></td> <td></td> <td></td> <td>[</td> <td></td>	IP D	User List			IP Service List				[	
Buckang         P         Contract         Find           Contract         Image: Contract Contract         Image: Contract Contract Contract         Image: Contract Cont	MPLS D	Users Groups SSH Keys SSH Private Keys Act	ive Users						Find	
System         Image: System </td <td>Routing</td> <td></td> <td></td> <td>Circl</td> <td></td> <td>( D-1</td> <td>a shirt man</td> <td>C. If a</td> <td>TICH</td> <td></td>	Routing			Circl		( D-1	a shirt man	C. If a	TICH	
Question       If Meme       If Graup       Address       Last Logged In       If Meme       If Graup       If Meme       If Graup	System		1	Find	X @ api	8728	Available From	Certificate	TLS Ver	• •
Image         Image <td< td=""><td>P Queues</td><td>Name Group Allowed Address</td><td>Last Logged In</td><td></td><td>X 🛛 api-ssl</td><td>8729</td><td></td><td>none</td><td>any</td><td></td></td<>	P Queues	Name Group Allowed Address	Last Logged In		X 🛛 api-ssl	8729		none	any	
Log RADUS Tools P Wertmind Sext Wndow P L Ren L Ren	Files				X @ ftp	21	192,168,120,0/24			
New Tennial         • who          631 192.166.120.0/24         •           New Tennial         • who          631 192.166.120.0/24         •           Meds Suppl.f.ff         • who          631 192.166.120.0/24         •           New Webbo         Exit         •         •         •           New Webbo         Item         •         •         •					X @ telnet	23				
New Teminal         Dokt         Pation         Mare Support.rf         New Wrebox         Exit         Windows         1 item					winbox	8291	192.168.120.0/24			
DottX   MetaGUUER   Partion   Mete Suport If   State     It em     It em     It em     It em	New Terminal				X @ www-ssl	443	192.108.120.0/24	none	any	
MetaROUTER   Pattion   New WrBox   It     Windows     Item     Item     Item	Dot1X									
Patition Male Suport. If Exk I Rem I Rem	MetaROUTER									
Make Support.rf   New Wridows     Windows     I item     B Rems     B Rems	Partition									
	Make Supout.rif									
	S New WinBox									
	🛃 Exit									
					8 items					_
	Windows	1 ikana				_		_	_	
		I icem								
F minimum manage in discussions and the										
E unining many in signature parton										
F minimum manage in cianneges and the	_									
5 minimum manage in discussions and the										
F minimum manage in diamage anter										
5 minimum mana in signature sector										
	5 minima m	an in dialanger and								

# **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 etherl. (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.

Session Settings Dash	hboard												
い 🖓 Safe Mode	Session: B8:69:F4:67:9	93:AB											
2 Quick Set													
CAPSMAN													
C Windows	-												
wireless													
Bridge													
T PPP	-												
Twitch													
° ° Mesh													
P D													
MPLS D													
📑 Routing													
System													
🐥 Queues	Interface List												
Files	Interface Interface	EList Ethernet EoIP Tunnel	IP Tunnel	GRE Tunnel VLA	N VRRP Bondina LT	E							
Log													First
<b>AP RADIUS</b>	+ - <b>*</b> ×	Detect Interne	t										Fina
🔀 Tools 🛛 🗎	Name	<sup>▲</sup> Comment	Actual MTU	L2 MTU Tx	Rx		Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	F	P Tx Packet (p/s)	P Rx Packet (p/s)
🖾 New Terminal	ether1	Ethernet	1500	1598	0 bps	0 bps		)	0	0 bps	0 bps	0	0
do Dot1X	ether3	Ethernet	1500	1598	0 bps	0 bps		)	0	0 bps	0 bps	0	0
MetaROLITER	🚸 ether4	Ethernet	1500	1598	0 bps	0 bps	(	0	0	0 bps	0 bps	0	0
Partition	🚸 ether5	Ethernet	1500	1598	0 bps	0 bps	(	)	0	0 bps	0 bps	0	0
Mala Curath uit	X BB wlan1	Wireless (Atheros AR	1500	1600	0 bps	0 bps	(	)	0	0 bps	0 bps	0	0
Make Supput.ni	- Winner	WILCIESS (ACTOLOS ARCT.)	1500	1000	0 bps	0 bps		/	0	0 005	0 003	0	0
Exit													
Windows													
	7 items (1 selected)												
	1												
X													
ě													
Vir													
>													
00													
U U													
lt.													
2													

Fig.6 – Commentare le interfacce

#### Session Settings Dashboard

Safe Mode Session: B8:69:F4:67:93:AB

🖉 Quick Set									
CAPSMAN									
Interfaces									
🔔 Wireless									
3 Bridge	Interface Lis	st							
= PPP	Interface	Interface Li	ist Etherne	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN VRRF	Bonding	LTE
T Switch				Data da Tata mai					Tind
°L° Mesh				Detect Internet	•				Filla
855 TP	Nam	ie Andre andre believe	Туре		Actual MTU	L2 MTU Tx	(	Rx	
MPLS N	;;; interr	accia_pubblic ether1	.a Ethernet		1500	1598		0 bps	
Routing	;;;		LAN						
Suctam	R 🔅 e	ether2	Ethernet		1500	1598	77.	3 kbps	37.1
Overver	(*) e	ether3	Ethernet		1500	1598		0 bps	
T Queues	() (i) (i) (i) (i) (i) (i) (i) (i) (i) (	ether5	Ethernet		1500	1598		0 bps	
Files	X 60 v	vlan1	Wireless	Atheros AR	1500	1600		0 bps	
Log	X \$9 v	vlan2	Wireless	Atheros AR	1500	1600		0 bps	
ADIUS									
🗡 Tools 🔹 🗅									
New Terminal									
Dot1X									
MetaROUTER									
🥵 Partition	•								•
Make Supout.rif	7 items (1 s	elected)							
🕓 New WinBox	1								
🔣 Exit									
💻 Windows 🗈									
5									
5									

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 <u>Hardware Offloading</u> 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, selezioniare 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.

#### Session Settings Dashboard

♥ ♥ Safe Mode Session: B8:69:F4:67:93:AB

💉 Quick Set		
CAPSMAN	1915-c.	
Interfaces	Bridge	
Q Wireless	Bridge Ports Port Extensions VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB	
👫 Bridge		Find
Termination PPP	The second	
🙄 Switch	Interface proge profizen intusted priority ( Path Cost Role	N T
° 🕻 Mesh		
😳 IP 🛛 🗅		
O MPLS		
📑 Routing 🛛 🗅		
🔯 System 🗅		
🙅 Queues		
Files		
📃 Log		
RADIUS		
🔀 Tools 🛛 🗅		
💵 New Terminal		
🚸 Dot1X		
MetaROUTER	0 items	¥
🥵 Partition		•
Nake Supout.rif	8 items	
🕓 New WinBox		
🔣 Exit		
Windows		
<u>í</u>		
5		
0		
2		

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.

sion Settings	Dashboa	ard						
Safe M	lode S	ession: B8	3:69:F4:67:93:	AB				
🖉 🏏 Quick Set								
CAPSMAN								
Interfaces	1	Bridge						
🔔 Wireless		Bridge	Ports Port E	xtensions VLANs MS	TIs Port MST Over	rides Filters NA	T Hosts MDB	
🕃 Bridge	[	+ -						Find
TE PPP	[	#	Interface	Bridge	Horizon Trusted	Priority ( Path	Cost Role	R 🕶
Switch		0 H	a ether2	bridge_LAN	no	80	10 designated po	rt
255 TD	N	1 IH 2 IH	ether3	bridge_LAN	no	80	10 disabled port	
MPLS		3 IH	a ether5	bridge_LAN	no	80	10 disabled port	
TR Routing		4 I	& wlan1	bridge_LAN	no	80	10 disabled port	
System		51	widii2	Dridge_LAN	no	00	10 disabled port	
Queues			Add	ress List				
Files			+	- / * =	7	Find		
📃 Log					Network Ir	terface 💌		
2 RADIUS				+ 1.2.3.4	1.2.3.4 e	ther1		
🔀 Tools	$\triangleright$			+ 192.168.120.1/24	192.168.120.0 b	idge_LAN		
🖾 New Termin	nal							
Oot1X		•				-		•
	ER	6 items						
Partition		•						•
Make Supor		8 items				l.		
S New Winbo	DX							
	_							
Windows	Þ							
			2 ite	ems				
			<u>,</u>					
õ								
nB								
N								
S								
5								
lite								
Sol								

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.

Session Settings Dashb	oard		
Safe Mode	Session: B8:69:F4:67:93:AB		
🚀 Quick Set			
CAPsMAN			
Interfaces			
💭 Wireless	Takaufana List		
Contraction Bridge		DHC/Server	
E PPP	Interface Interface List Ethernet EoIP Tunnel IP Tunnel GRE Tunnel V	A V DHCP Networks Leases Options Option Sets Vendor Classes Alerts	
Switch	+ ▼ ─	Find	
255 TD	IP Pool	Address 🛆 Gateway DNS Servers Domain WINS Servers Next Ser	-
	Pools Used Addresses	192.168.120.0/24 192.168.120.1 1.1.1.1 WORKGRO	
Routing			
System D		nd DHCP Server <dhcp-server></dhcp-server>	
Queues	Name Addresses Next Pool	Generic Queues Script OK	
Files	192.100.120.100-192.100.120.130 None	Name: dhcp-server Cancel	
Log		Interface: bridge LAN	
29 RADIUS		Npphy         DHCP Network <192.168.120.0/24>           Relay:	
🗡 Tools 🗈 🗅	1 item	Lease Time: 12:00:00 Disable Address: 192.168.120.0/24 OK	
New Terminal		Booto Lease Time: Forever	
Dot1X     MohaDOUITED		Address Paol: Ipool.dhrp	
Partition			
Make Supout.rif	Ritems	DNS Servers: 1.1.1.1  Comment	_
New WinBox		Src. Address: Domain: WORKGROUP A Copy	
K Exit		Delay Threshold:	
		Authoritative: ves 🔍 🔍	
💻 Windows 🛛 🗅		Bootn Support: Static CAPS Managers:	
		Client MAC Limit	
		Lice PADTUS: no	
		Always Broadcast	
		Add ARP For Leases	
		✓ Use Framed As Classless	
		Conflict Detection	
Xo		enabled	
an D			
M			
ຽ			
nte			
9			

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.

Sess	sion Settings Dashb	oard											
Ю	Cafe Mode	Session: B8:69:F4:67:93:AB											
	🖋 Quick Set												
	CAPsMAN												
	Interfaces												
	Wireless												
	💥 Bridge												
	= PPP												
	T Switch												
	° 🖁 Mesh	DNS Settings			DNS	Static							
	255 IP	Servers:	1.1.1.1	OK							Find		
	MPLS N		208 67 222 220					-					
	📌 Routing 💦 👌		200.07.222.220	Cancel	#	Name	Regexp router.lan	A	1 d 00:00	Address 0:00 192,168,120	IPve V		
	🔯 System 🗈	Dynamic Servers:		Apply									
	🗣 Queues	Use DoH Server:	▼	Chabie									
	Files		Verify DoH Certificate	Static									
	Log			Cache									
	RADIUS		Allow Remote Requests										
	🔀 Tools 🛛 🗅	Max UDP Packet Size:	4096										
	🖾 New Terminal	Query Server Timeout	2.000										
	🚸 Dot1X	Query Server Timeouch	10,000										
	MetaROUTER	Query Total Timeout:	s										
	🦺 Partition	Max. Concurrent Queries:	100										
	Make Supout.rif	Max. Concurrent TCP Sessions:	20										
	New WinBox				•						•		
	🛃 Exit	Cache Size:	2048 KiB		1 ite	m (1 selected)							
		Cache Max TTL:	7d 00:00:00										
	Windows	Cache Used:	29 KiB										
				_	J								
×													
R													
in i													
$\geq$													
S													
2													
lt.													
ğ													
ĽĽ.													
~	10 0 0												

fig.12 – Configurazione DNS

### Obbiettivo 9: Impostare il Gateway del Router

Nel paragrafo 6 – punto 2, abbiamo assegnato all'interfaccia etherì 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.

Sessi	on Settings Das	hboard								
Ю	Cafe Mode	Sessio	ion: B8:69:F4:67:93:AB							
	🖉 Quick Set									
	CAPSMAN									
	Interfaces									
	Wireless									
	Bridge									
	= PPP									
	T Switch									
•	Mesh									
	IP	<b>N</b>								
	MPLS	$\triangleright$								
	Routing	Þ								
	System	Þ						ล		
	P Queues		Route <0.0.0.0/0>	>				1		
	Files		General Attribu	ites			OK			
	Log		Dst. Address:	0.0.0/0			Cancel			
	RADIUS		Gateway:	10.246.159.50	▼ reachable ether1	\$	Apply			
	🖌 Tools	$\triangleright$					, app.y			
	New Terminal		Check Gateway:			<b>~</b>	Disable			
	Dot1X		Туре:	unicast		Ŧ	· · · · ·			
	MetaROUTER	_	Distance:	1	Route List					
	🖢 Partition		Econor	20	Routes Nexthops Rules VRF					
	Make Supout.rif		Scope:	50	+ - / * 2 7				Find all 🔻	
	New WinBox	- 11	Target Scope:	10	Dst. Address A Gateway		Dis	tance Routing Mark	Pref. Source	
	Kata Exit	- 11	Routing Mark:		AS 0.0.0.0/0 10.246.15	9.50 reachable ether1	Die	1	There boared	
			Pref. Source:		DAC 10.246.159.50 ether1 rea	chable		0	1.2.3.4	
	Windows				DAC   192.168.120 bridge_LAP	N reachable		0	192.168.120.1	
			enabled							
			<u>.</u>	1						
×										
B										
in'										
$\leq$					3 icems					
SO										
E L										
Ę										
8										

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.

🗯 wine64-prel	<b>bader</b> Edit Window				🙂 🗢 🛄 Q	음 💿 Sab 10 dic 17:28
		abio28@B8:69:F4:67:93:AB (Router-ufficio)	- WinBox (64bit) v6.48.6 on hAP ac lite (n	nipsbe)		
Session Settings Dash	poard					
Safe Mode	Session: B8:69:F4:67:93:AB					
V Quick Set	Terminal <1>					🗉 ×
CAPSMAN						•
Interfaces	-					
Q Wireless						
3 Bridge						
tan PPP						
🙄 Switch						
°[ູ່ Mesh						
III IP						
MPLS D						
📑 Routing						
System						
Queues		<u>. 1 _ 1 1 1 - 1 1</u>				
Files						
Log		II\_/II				
APRADIUS	TEL. 3495329899 consulenza@fo	sfabio.it _ _ / \ _ _				
Now Terminal	MINIOCIN NOUCCIOS 0.40.0 (C) 1955-202					
	[?] Gives the list of avail	able commands				
MetaROLITER	command [?] Gives help on the comma	a and list of arguments				
Partition	[Tab] Completes the command/w	ord. If the input is ambiguous,				
Make Supout.rif	a second [Tab] gives po	ssible options				
New WinBox	/ Move up to base level					
Exit	Move up one level	level				
	[Fabio28@Router-ufficio] > ping 1.1.1.1	IEVEL				
💻 Windows 🗅	SEQ HOST	SIZE TTL TIME STATUS				
		56 58 45ms 56 58 45ms				
	2 1.1.1.1	56 58 46ms				
ŏ	3 1.1.1.1	56 58 46ms				
28	sent=5 received=5 packet-loss=0% mi:	1-rtt=44ms avg-rtt=45ms max-rtt=46ms				
N.						
S	SEO HOST	SIZE TTL TIME STATUS				
5	0 142.250.180.131	56 117 45ms				
<u>a</u>	1 142.250.180.131	56 117 48ms 56 117 45ms				
õ	3 142.250.180.131	56 117 46ms				
Er.						•
		10 = <u>*tv</u>		9 🥑 🗧		
	SEQ HOST 0 1.1.1.1 1 1.1.1.1 2 1.1.1.1 3 1.1.1.1 4 1.1.1.1 sent=5 received=5 packet-loss=0% min [Fabio28@Router-ufficio] > ping google. SEQ HOST 0 142.250.180.131 1 142.250.180.131 2 142.250.180.131 3 142.250.180.131 3 142.250.180.131 3 142.250.180.131	SIZE TTL TIME STATUS 56 58 45ms 56 58 46ms 56 58 46ms 56 58 46ms 56 58 44ms 100 STATUS 56 117 45ms 56 117 45ms 57 10 10 10 10 10 10 10 10 10 10 10 10 10				

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.

Ses	sion Settings Dashbo	shboard	
Ю	Cafe Mode	Session: B8:69:F4:67:93:AB	
	🚀 Quick Set		
	CAPsMAN		
	Interfaces		
	💭 Wireless		
	Stidge		
	tana ang tang tang tang tang tang tang t		
	🙄 Switch	Firewall	
	° 🕻 Mesh	Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols	
	∰ IP ▷		
	MPLS D		
	Routing	Action Chain Src. Address Dst. Address Prot Src. Port Dst. Port In. Int Out. I In. Int Out. I Src. A Dst. A Bytes Packets	
	System	1 \$\$ drop input 0 0 0 0	
	Queues		
	Files		
	Log		
	and RADIUS		
	X Tools		
	A Debty		
	Metakoutek		
	Make Superit rif		
	Now WinPox		
	EXIC	2 items	
	Windows		
ŏ			
Be			
Nit			
S			
õ			
ē			
no			
Ř			

Session Settings Dashboard	
Safe Mode Session: B	8:69:F4:67:93:AB
🖌 Quick Set	
CAPSMAN	
Interfaces	
T Wireless	
3 Bridge	
PPP	
🙄 Switch	Firewall
° Mesh	The Date NAT Mercle Date Constraints address to be constraints
IP D	Titlet Rules inn Mangle Raw Service Ports Connections Address Layer/ Protocols
MPLS D	+ - V 🛞 🖆 🍸 CReset Counters CReset Al Counters
📝 Routing	# Action 🛆 Chain 🗠 Src. Address Dst. Address Prot Src. Port Dst. Port In. Int Out. I Src. A Du Bytes 💌
System 🗅	0         \$ masquerade         srcnat         192.168.120.0/24         ether1         1056 B
🛖 Queues	
Files	
📃 Log	
ar RADIUS	
🔀 Tools 🗈	
🖾 New Terminal	
I Dot1X	
Partition	
Make Supout.rif	
S New WinBox	•
K Exit	1 item
The second secon	
Windows	
×	
8	
li)	
>	
S	
Ť	
8	
tig. 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 <u>vedi questa pagina</u>

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.

ession Settings Dashb	oard										
Safe Mode	Session: B8:69:F4:67:93:AB										
🚀 Quick Set											
CAPSMAN											
Interfaces											
💭 Wireless											
C Bridge		-			_						-
Te PPP		Interface <wian1></wian1>					Interface <wlan2></wlan2>				
Switch		General Wireless	Data Rates Advanced	HT HT MCS WD	s	OK	General Wireless	Data Rates Advanced HT H	IT MCS WDS	OK	
Iss TD		Mode	: ap bridge		<b>=</b>	Cancel	Mode	ap bridge	<b>•</b>	Cancel	
	Wireless Tables	Band	: 2GHz-B/G/N		₹	Apply	Band	5GHz-A/N/AC	₹	Apply	
Routing	WiFi Interfaces W60G Stati	Channel Width	: 20/40MHz Ce		∓		Channel Width:	20/40/80MHz Ceee	₹		
System	wood stat	Frequency	: 2412	Ŧ	MHz	Disable	Frequency:	5260	<b>▼</b> MHz	Disable	
🙅 Queues		SSID	GREENET			Comment	Secondary Channel:			Comment	Fina
Files	Name ∆Ty S #awlan1 W	Radio Name	: B869F46793B0			Simple Mode	SSID	GREENET	▲	Simple Mode	MAC Addres 88:69:E4:67:93
Log	S 😝 wlan2 W	Scan List	: default	1	₹ ♦	Torch	Radio Name:	B869F46793AF		Torch	88:69:F4:67:93
AP RADIUS		Skip DFS Channels	: disabled	, Tun	Ţ	W/DE Accopt	Scan List	default	<b>.</b>	WDC Assess	
Tools		Wireless Protocol	: 802.11		₹	WP5 Accept	Skip DES Channels:	disabled		WP5 Accept	
New Terminal		Security Profile	: default		₹	WPS Client	Wireless Protocol	802.11	Ţ	WPS Client	
MetaROUTER		Interworking Profile	: disabled		╶╤╶	Setup Repeater	Security Profile	default		Setup Repeater	
Partition		WPS Mode	: disabled			Scan	Interworking Profile	disabled	 	Scan	
Make Supout.rif						Freg, Usage	WPS Mode	disabled		Freq. Usage	
🚫 New WinBox		Frequency Mode	: regulatory-domain		Ŧ	Alian				Alt-	
🔣 Exit		Country	: italy		Ŧ	Align	Frequency Mode:	regulatory-domain	<b>.</b>	Align	
		Installation	: indoor		₹	Sniff	Country	italy	<b></b>	Sniff	
Windows D	•	WMM Support	: disabled		Ŧ	Snooper	Installation	indoor		Snooper	•
	2 items out of 8 (1 selected)	Bridge Mode	: enabled		<b>Ŧ</b>	Reset Configuration	WMM Support:	disabled	<b>▼</b> •	Reset Configuration	
		enabled	running	slave	running	ap	enabled	running	running ap		-
	l		L'anna 2	1-1-1-1	1	-r		i si n in sy	ranning ap		_
5											
2											
A 4											
Q											
0											
* · · · · · · · · · · · · · · · · · · ·											

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: <u>https://www.mio-ip.it/</u>
- 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=LANLANLAN
/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

💓 Quick Set	Wirel	ess Tables							
CAPsMAN	WiFi	i Interfaces	W60G Station	Nstreme Dual A	Access List Reg	istration Conne	ct List Security Profi	iles Channels	
Interfaces									Find
Wireless			U			a			1 110
Bridge	Na Na	ame 🛆	Mode	Authentication	Unicast Ciphers	Group Ciphers	WPA Pre-Shared	WPA2 Pre-Shared	<b></b>
≟≣ PPP		iduit	none						
T Switch									
°T <mark>°</mark> Mesh									
P D									
🕐 MPLS 🛛 🗅									
茸 Routing 🛛 🗅									
🔯 System 🗈									
🙅 Queues									
Files									
🗒 Log									
2 RADIUS									
💥 Tools 🛛 🗅									
🔤 New Terminal	1 iten	n							
🚸 Dot1X									

New Security Profile		
General RADIUS EAP	Static Keys	ОК
Name:	[WPA2-PSK]	Cancel
Mode:	dynamic keys ∓	Apply
Authentication Types:	WPA PSK WPA2 PSK	Comment
	WPA EAP WPA2 EAP	Сору
Unicast Ciphers:	✓ aes ccm _ tkip	Remove
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 <b>T</b>	
Management Protection Key:		
	Disable PMKID	

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

💓 Quick Set	Wireless Tables			
CAPsMAN	WiFi Interfaces W60G Station	Nstreme Dual Access List Registration	n Connect List Security Profiles Chann	nels
M Interfaces		CAP WPS Client Setup Renea	er Scapper Freq Usage Alignm	ant Wireless Spiffer Wireless Spooper Find
💭 Wireless				
👫 Bridge	X Wan1 Wire	Actual MTU IX	Abas Obas	TX Packet (p/s) RX Packet (p/s) FP TX V
🛓 🛓 PPP	X H wlan2 Wire	less (IPQ4019) 1500	0 bps 0 bps	0 0
The Switch		× × , , , , , , , , , , , , , , , , , ,		
°L <mark>°</mark> Mesh				
📮 IP 📄				
🕐 MPLS 🗈 🗈				
📑 Routing				
🔯 System 🗅				
🐥 Queues				
Files				
🗒 Log				
RADIUS				
🗙 Tools 🛛 🗅				
New Terminal	2 items out of 8 (1 selected)			

nterface <w< th=""><th>lan1&gt;</th><th></th><th></th><th></th><th></th><th></th><th></th></w<>	lan1>						
General	Wireless	HT WDS	Nstreme	NV2	Advanced Status	<b>;</b>	ОК
	Mode	station				Ŧ	Cancel
	Band	: 2GHz-B/G				₹	Apply
Cha	nnel Width	: 20MHz				₹	Enable
F	Frequency	: 2412				<b>∓</b> MHz	Comment
	SSID	: MikroTik				-	Advanced Mode
Secu	urity Profile	: default					Torch
Freque	ency Mode	: regulatory	-domain				WPS Accept
	Country	: etsi					WPS Client
	Installation	any					Setup Repeater
		<ul> <li>Default</li> </ul>	Authenticat	e			Scan
							Freq Usage
							Alian
							Sniff
							Snooper
							Reset Configuration

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

🚀 Quick Set			Wireless	a Tables											'×
🔔 CAPsMAN			WiFi In	terfaces	W60G Station	Nstreme D	ial Access I	ist Registration	Connect List	Security Profile	s Channels	Interworking Pr	ofiles		
Interfaces												incontrolling 11			
🔉 Wireless			<b>+</b> -			CAP	WPS Client	Setup Repeater	Scanner	Freq. Usage	Alignment	Wireless Sniffer	Wireless Snoop	Find	
👯 Bridge				Name	— Туре	,	∇ Actual	MTU Tx		Rx	Tx Pa	acket (p/s) R	x Packet (p/s)	FP Tx	-
🏣 PPP			X	00 wlan1	Wire	less (IPQ401	9)	1500	0 bps		0 bps	0		)	
🕎 Switch		- <b>-</b> - ,	<u>(</u> ^	igg wianz	2 Vvire	iess (IPQ401	9)	1000	0 bps		Ubps	0		J	
°∐ <mark>°</mark> Mesh															
🐺 IP	$\land$														
MPLS	$\sim$														
3 Routing	$\square$														
🔯 System	Þ														
🙅 Queues															
📔 Files															
🚊 Log			•												•
RADIUS			2 items	out of 8											
V Tools	N														

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

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

June	arare an orrage					
	🚀 Quick Set	Bridge				IX
	CAPsMAN	Bridge Ports VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB				
	Interfaces					
	Wireless				Find	
	👯 Bridge	Name / Type L2 MTU Tx Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	-
	늘 PPP	New Interface				
	🙄 Switch	General STP VLAN Status Traffic	ОК			
	°T <mark>°</mark> Mesh					
	🍄 IP 🛛 🗅	Name: [nome_bridge]	Cancel			
	MPLS ▷	Type: Bridge	Apply			
	🔀 Routing	MTU:	Disable			
	🔯 System 🗅	Actual MTU:				
	🙅 Queues	L2 MTU:	Comment			
	📄 Files	MAC Address:	Сору			
	🗐 Log	ABP: enabled	Remove			
	RADIUS		T			
	🔀 Tools 🛛 🗅	ARP Timeout:	Torch			-
	New Terminal	Admin. MAC Address:				
	Dot1X	Ageing Time: 00:05:00			_	
	🥵 Partition					
	Nake Supout.rif	IGMP Snooping				
	New WinBox	DHCP Snooping				
	🛃 Exit					
	💻 Windows 🛛 🗅					
		enabled running slave				

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

🚀 Quick Set	Bridge								
CAPsMAN	Bridge Ports VLANs	s MSTIs Po	rt MST Overri	des Filt	ers NAT	T Hosts	MDB		
Interfaces								<b></b>	
Wireless								<u> FII</u>	10
👯 Bridge	# Interface	Bridge		Horizon	Trusted	Priority (h	Path Cost	Role	-
🏣 PPP	0 IH La ether3	[nome_	bridge]		no	80	10	disabled port	
🙄 Switch	2 IH A ether5	[nome_ [nome	pnagej bridael		no	80	10	disabled port	
* Mesh	3 I 👗 wlan 1	[nome_	bridge]		no	80	10	disabled port	
₩ IP ト	A Ne	ew Bridge Port							
MPLS N	-	General CTD	VLAN St-	1.10					
Routing     ►	Aggiungere	acricital STF	VLAN JI	itus					
🔯 System 🗅	le interfacce	nterface: wlan2				•	- Ca	ancel	
Queues	al bridge	Bridge: [nome	_bridge]			1	A	pply	
📔 Files		Horizon							
🚊 Log								sable	
RADIUS		Leam: auto				•	Cor	mment	
🔀 Tools 🛛 🗅		Unl	known Unicas	st Flood				Copy	
💵 New Terminal	•	🗸 Uni	known Multica	ast Flood					•
Dot1X	4 items	✓ Bro	adcast Flood				Re	move	
🦺 Partition		Tru	sted						
Make Supout.rif									
S New WinBox									
🛃 Exit	en	abled	ina	active		Hw. (	Offload		
			1115		_				

4.Attribuire una subnet privata all'interfaccia bridge

CAPsMAN   Interfaces   Wreless   Bridge   PPP   Switch   Switch   Mesh   WIPLS   Accounting   Address   MPLS   Accounting   Address   Oucues   DHCP Client   DHCP Relay   DHCP Server   Prewall   Cog   DHCP Server   Partition   Kid Control   Make Supout.rf   Neighbors   Partition   Kid Control   Make Supout.rf   Neighbors   Sinther   Sinther   Sinther   Sinther   Windows   New Droxy	🚀 Quick Set		Address List		
Interfaces   Wreless   Wreless   PPP   Switch   Switch   Mesh   Provide   Mesh   Provide   Mesh   Provide   MPLS   Address   MPLS   Accounting   Address   System   Cloud   Oueues   DHCP Client   Disable   Comment   Copy   Files   DHCP Relay   DLOg   DHCP Server   Partition   Kid Control   Network   Network   Partition   Kid Control   Nake Supout.rif   Neighbors   SMB   SIMP   Services   Settings   Socks   TFTP   Traffic Row   UPnP   Web Proxy	CAPsMAN			[1]	E
Wireless       Interface:       Interface:       Interface:       Interface:       Interface:       Address         Year       Mesh       Addresses       Addresses       Addresse       Apply         Year       MPLS       Accounting       Interface:       Interface:       Interface:       Apply         Year       MPLS       Accounting       Disable       Cancel       Apply         Year       Okd       Cancel       Apply       Disable       Comment       Copy         Year       Okderses       DHCP Client       DHCP Server       Disable       Comment       Copy         Year       RADIUS       DNS       Firewall       Ditems       Ditems         Year       Nake Supout if       Neighbors       Packing       Ditems         Year       Pool       Routes       Soks       TFTP       Traffic Flow         Windows       Soks       TFTP       Traffic Flow       UPnP       Web Proxy	Interfaces		Address	/ Network	Interface
Bridge   PPP   Switch   Mesh   IP N   MPLS   Accounting   Addresses   System   Cloud   Cueues   DHCP Client   DHCP Client   DHCP Client   DHCP Server   Brites   DHCP Server   Patition   Kid Control   Make Supout If   New WinBox   Sorks   TFTP   Traffic Flow   UPnP   Web Proxy	Wireless		/ ddiess	Hermony	Intendee
Image: PPP       ARP         Image: Mesh       ARP         Image: Mesh       ARP         Image: Mesh       Addresses         Image: MPLS       Accounting         Image: MPLS       Addresses         Outling       DHCP Client         Image: Maxed Support iff       OK         Image: Maxed Support iff       Neighbors         Image: Parkiton       Kid Control         Image: Maxed Support iff       Packing         Sources       Settings         Socks       TFTP         Traffic Flow       UPnP         Web Proxy       Web Proxy	👯 Bridge		New Address		
Switch       Image: Switch       ARP         Mesh       ARP         MPLS       Accounting         Routing       Addresses         System       Cloud         Cloud       Disable         Courres       DHCP Client         Files       DHCP Relay         Log       DHCP Server         Prewall       Ottems         New Terminal       Hotspot         ♦ Dot1X       IPsec         Parking       Neighbors         Pool       Routes         Windows       SMB         SNMP       Services         Settings       Socks         TFTP       Traffic Flow         UPnP       Web Proxy	🛓 PPP		Address: 192.168	3.0.1/24	ОК
Mesh       Interface:       Interface:	🙄 Switch		Network: 192.168	3.0.0	Cancel
IP       ARP         MPLS       Accounting         Routing       Addresses         System       Cloud         Queues       DHCP Client         DGg       DHCP Relay         DHCP Server       Remove         RADIUS       DNS         Tools       Firewall         New Terminal       Hotspot         Nake Supout.nf       Neighbors         New WinBox       Packing         Exit       Pool         Routes       SNMP         Services       Settings         Socks       TFTP         Traffic Flow       UPnP         Web Proxy       Web Proxy	°T <mark>°</mark> Mesh		Interface: [nome t	oridae] 🛛 🔻	
MPLS Accounting   Routing Addresses   System Cloud   Queues DHCP Client   Files DHCP Relay   DACP Server Copy   RADIUS DNS   Tools Firewall   Make Supout If Neighbors   New WinBox Packing   New WinBox Packing   SNMP   Services   Settings   Socks   TFTP   Traffic Flow   UPnP   Web Proxy	∰ IP ト	ARP			Apply
Routing Addresses   System Cloud   Queues DHCP Client   Files DHCP Relay   DHCP Server   Pathion   New Terminal   Hotspot   Partition   Kid Control   Make Supout rif   Neighbors   New WinBox   Packing   Exit   Pool   Routes   SMB   SNMP   Services   Settings   Socks   TFTP   Traffic Flow   UPnP   Web Proxy	MPLS N	Accounting			Disable
System Cloud   Queues DHCP Client   Files DHCP Relay   DHCP Server   PRADIUS   Nos   Firewall   New Terminal   Hotspot   Hotspot   Partition   Kid Control   Make Supout.nff   Neighbors   New WinBox   Packing   Exit   Pool   Routes   SNMP   Services   Settings   Socks   TFTP   Traffic Flow   UPnP   Web Proxy	Routing ▷	Addresses			Commont
Cueues       DHCP Client       Copy         Files       DHCP Relay       Remove         I Log       DHCP Server       Ienabled         Y RADIUS       DNS       ienabled         Y Tools       Firewall       0 items         I New Terminal       Hotspot       ienabled         Y Partition       Kid Control         Y Make Supout.rff       Neighbors         Y New WinBox       Packing         Y Exit       Pool         Routes       SNMP         Services       Settings         Socks       TFTP         Traffic Rlow       UPnP         Web Proxy       Web Proxy	🔯 System 🗅	Cloud			Comment
Files DHCP Relay   Log DHCP Server   DNS DNS   Tools Firewall   New Teminal Hotspot   Ott1X IPsec   Patition Kid Control   Make Supout.rff Neighbors   New WinBox Packing   Exit Pool   Routes SNMP   Services Settings   Socks TFTP   Traffic Flow UPnP   Web Proxy Web Proxy	🙅 Queues	DHCP Client			Сору
Log DHCP Server   ♪ RADIUS DNS   ♪ Tools Firewall   ▶ New Terminal Hotspot   ♥ Dot1X IPsec   ♪ Partition Kid Control   ▶ Make Supout rff Neighbors   ♥ New WinBox Packing   ♥ Sol Routes   ♥ Windows SMB   SNMP Services   Settings Socks   TFTP Traffic Flow   UPnP Web Proxy	Files	DHCP Relay			Remove
Image: RADIUS DNS   Firewall Hotspot   Image: Rabies Firewall   Hotspot Hotspot   Image: Rabies Hotspot   Image: Rabies Hotspot   Image: Rabies Routes   Image: Rabies SMB   Simp Services   Services Settings   Socks TFTP   Traffic Flow UPnP   Web Proxy Web Proxy	🚊 Log	DHCP Server	apphlad		
Tools Firewall   Wew Terminal Hotspot   Hotspot IPsec   Partition Kid Control   Make Supout.rif Neighbors   New WinBox Packing   Pool Routes   Windows SMB   SNMP Services   Settings Socks   TFTP Traffic Flow   UPnP Web Proxy	RADIUS	DNS	enabled		
Image: Simple state	🔀 Tools 🛛 🗅	Firewall	0 items		
Dot1X    Partition   Kid Control   Make Supout.rif   Neighbors   New WinBox   Packing   Exit   Pool   Routes   Windows   SMB   SNMP   Services   Settings   Socks   TFTP   Traffic Flow   UPnP   Web Proxy	New Terminal	Hotspot			
Partition Kid Control   Make Supout.rif Neighbors   New WinBox Packing   Pool Routes   Routes SMB   SNMP Services   Settings Socks   Socks TFTP   Traffic Flow UPnP   Web Proxy Web Proxy	Dot1X	IPsec			
Make Supout.rifNeighborsNew WinBoxPackingPoolRoutesRoutesSMBSNMPServicesSettingsSocksTFTPTraffic FlowUPnPWeb Proxy	🦺 Partition	Kid Control			
New WinBox Packing   Pool Routes   Routes SMB   SMB SNMP   Services Services   Settings Socks   TFTP Traffic Flow   UPnP Web Proxy	Nake Supout.rif	Neighbors			
Exit Pool   Routes SMB   SNMP Services   Services Settings   Socks Socks   TFTP Traffic Flow   UPnP Web Proxy	New WinBox	Packing			
Routes   SMB   SNMP   Services   Settings   Socks   TFTP   Traffic Flow   UPnP   Web Proxy	🛃 Exit	Pool			
Windows SMB SNMP Services Settings Socks TFTP Traffic Flow UPnP Web Proxy		Routes			
SNMP Services Settings Socks TFTP Traffic Flow UPnP Web Proxy	Windows 🗅	SMB			
Services Settings Socks TFTP Traffic Flow UPnP Web Proxy		SNMP			
Settings Socks TFTP Traffic Flow UPnP Web Proxy		Services			
Socks TFTP Traffic Flow UPnP Web Proxy		Settings			
TFTP Traffic Flow UPnP Web Proxy		Socks			
Traffic Flow UPnP Web Proxy		TFTP			
UPnP Web Proxy		Traffic Flow			
Web Proxy		UPnP			
		Web Proxy			

Ŧ

Find

🎾 Quick Set		DHCP Server
CAPsMAN		DHCP Networks Leases Options Option Sets Vendor Classes Alerts
Interfaces		
Wireless		
🚉 Bridge		Name 🔨 Interface Relay Lease Time Address Pool Add AR
🛓 PPP		
🙄 Switch		
°∏ <mark>°</mark> Mesh		DHCP Setup
🐺 IP 🗈 🗅	ARP	Select interface to run DHCP server on Configurare un DHCP server, sul bridge
MPLS ▷	Accounting	DHCP Server Interface: [nome_bridge]
🔀 Routing 🛛 🗅	Addresses	wizzard "DCHP Setup"
🔯 System 🛛 🗅	Cloud	Back Next Cancel
🙅 Queues	DHCP Client	
📄 Files	DHCP Relay	
🚊 Log	DHCP Server	
RADIUS	DNS	
🔀 Tools 🛛 🗅	Firewall	
🔤 New Terminal	Hotspot	0 items
Dot1X	IPsec	
🤚 Partition	Kid Control	
📡 Make Supout.rif	Neighbors	
🔇 New WinBox	Packing	
🛃 Exit	Pool	
	Routes	
💻 Windows 🛛 🗅	SMB	
	SNMP	
	Services	
	Settings	
	Socks	
	TFTP	
	Traffic Flow	
	UPnP	
	Web Proxy	

#### 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

🚀 Quick Set		Firewall	
CAPsMAN		Filter Bulae NAT Mande Raw Service Porte Connections Address Lists Laver7 Protocols	
Interfaces			
Wireless		Image: Image	
💢 Bridge	· · · · · · · · · · · · · · · · · · ·	# Action Chain Src. Address Dst. Address Proto Src. Port Dst. Port In. Inter Out. Int In. Inter Out. Int ▼	
🛓 PPP			
🙄 Switch			
°T <mark>°</mark> Mesh			
彈 IP 🛛 🖻	ARP	New NAT Rule	IX
🕑 MPLS 🛛 🗅	Accounting	General Advanced Extra Action Statistics OK Advanced Extra Action Statistics OK	
🔀 Routing	Addresses		=
🔯 System 🗅	Cloud		=
🙅 Queues	DHCP Client	Src. Address: 192.168.0.0/24 Apply Log Apply	
📔 Files	DHCP Relay	Disable Log Prefix:	
🗒 Log	DHCP Server	Protocol:	$\exists$
RADIUS	DNS	Sre Port	
🗙 Tools 🛛 🗅	Firewall	Copy To Ports: Copy	
🔤 New Terminal	Hotspot	Dist. Port: Remove Remove	
Dot1X	IPsec	Any. Port:	
🥵 Partition	Kid Control	In. Interface:	<u>'</u>
Nake Supout.rif	Neighbors	Out. Interface: interf_WAN_o_TUNNEL  Reset All Counters Reset All Counters	rs
New WinBox	Packing		
🛃 Exit	Pool		
	Routes	Out. Interface List:	
Windows 🗅	SMB	Packet Mark:	
	SNMP	Connection Mark:	
	Services	Porting Mark	
	Settings		
	Socks	Kouting Table:	
	TFTP	Connection Type:	
	Traffic Flow		
	UPnP	enabled enabled	
	Web Proxy		

#### 7.Attivare i moduli WiFi del router

🚀 Quick Set	Wireless Tables	
CAPsMAN	WiFi Interfaces W60G Station Nstreme Dual Access List Registration Connect List Security Profiles Channels	
🛤 Interfaces		
🔉 Wireless	Find	
💢 Bridge	Name / Type Actual MTU Tx Rx Tx Packet (p/s) Rx Packet (p/s) FP Tx	-
🛓 PPP	XS         Wat         Wireless (IPQ4019)         1500         0 bps         0 bps         0         0           XS         Wireless (IPQ4019)         1500         0 bps         0 bps         0         0	0 bps
🙄 Switch		0 DPS
°T <mark>°</mark> Mesh	Selezionare le interfacce WiFi e premere su "Abilita"	
🐺 IP 🗈 🗈		
MPLS ▷		
🔀 Routing 🗈		
🔯 System 🗈		
🙅 Queues		
📄 Files		
🚊 Log		
2 RADIUS		
🗙 Tools 🛛 🗅		
🔤 New Terminal	A and a start of 9 (2 aslested)	•
Dot 1X		

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="" wpa2pre-shared-key=\$PASSWORD #.Configurare l'interfaccia Wireless (wlan1 – wlan2) :global SSID "nome della rete WiFi Es. Wifufficio" /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.

100 10	1													
	ARP													
MPLS N	Accounting													
Routing	Addresses													
System N	Cloud												_	
Se Queues	DHCP Client	Firew	vall											
Files	DHCP Relay	Filte	er Rules NAT	Mangle	Raw Service Ports (	Connections	Address Lists La	ayer7 Protocols						
📃 Log	DHCP Server				CO Reast Counter	(O React All	Countern					Find		
RADIUS	DNS	<b>_</b> _			To Reset Counters	to Reset All	Counters					Filla		
🔀 Tools 🛛 🗅	Firewall	#	Action	Chain	Src. Address Dst. Ad	dress Proto	Src. Port Dst.	Port In. Inte	er  Out. Int  In. Ir	ter Out. Int S	rc. Ad Dst. /	Ad Bytes	Packets	1
New Terminal	Hotspot													
Dot1X	IPsec													
MetaROUTER	Kid Control													
🤥 Partition	Neighbors													
Make Supout.rif	Packing													
🖳 Manual	Pool													
🔇 New WinBox	Routes													
🛃 Exit	SMB													
	SNMP													
	Services													
	Settings													
	Socks													
	TFTP	0.1	-											
	Traffic Flow	10 ite	ms											
	UPnP	New	NAT Rule				[	New N	IAT Rule				×	
	Web Proxy	Ge	neral Advance	ed Extra	Action Statistics		OK	Adva	nced Extra Act	ion Statistics		ОК	1	
			Chain	data =t			Connel		Antina data art			Connect		
			Chain:		b 1 0		Cancel	_	Action: dst-nat			Cancel		
			Src. Address:	IP pubb	lico da cui mi collego	<b></b>	Apply		Log			Apply		
			Dst. Address:	IP pubb	lico di destinazione	<b></b>	Disable	Lo	og Prefix:		•	Disable	]	
			Protocol	6 (tcp)		₹ ▲	Comment	To Ad	dresses; IP private	computer		Comment	i I	
			Src. Port:			•	Сору		To Ports:		•	Сору	i I	
			Dst. Port:	3389			Remove					Pemovo		
			Any. Port:			•	D					nemove		
			In. Interface:	ether1		₹ ▲	Reset Counter	s			Res	set Counters		
			Out. Interface:				Reset All Count	ers			Rese	at All Counters		
		In	. Interface List:			•								
		Out	. Interface List:			<b>•</b>								
		-	Packet Made											
		Co	nnection Mark			<b>_</b>								
		0	Routing Mark											
			Routing Table:											
		Co	nnection Type:											
			lad.						4				-	
		enab	ned					enable	a					

#### 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

MMM	MMM	KKK			TTTTTTTTTTT	KKK	
MMMM	MMMM	KKK			TTTTTTTTTTTT	KKK	
MMM MMMM	MMM II	KKK KKK	RRRRRR	000000	TTT	III KKK KKK	
MMM MM	MMM II	KKKKK	RRR RRR	000 000	TTT	III KKKKK	
MMM	MMM II	KKK KKK	RRRRRR	000 000	TTT	III KKK KKK	
MMM	MMM II	KKK KKK	RRR RRR	000000	TTT	III KKK KKK	
MikroTik	Router0	6.48.6 (c)	1999-2021	htt	p://www.mikr	otik.com/	
[?]	Gi	ves the list	of availa	ble comman	ds		
command [?	1 Gi	ves help on	the comman	d and list	of argument	5	
		-			-		
[Tab]	Cor	mpletes the	command/wo	rd. If the	input is am	biquous,	
	a	second [Tab	gives pos	sible opti	ons		
1	Mor	ve up to bas	e level				
	Mor	re up one le	vel				
/command	Use	e command at	the base	level			
1		1 > in fi	ewall nat	add chains	dstnat dst-a	ddress="TP pubbl	blico di destinazione" suc-addresse"TP pubblico da cui mi collego" in-interfaces "interfaceia MAN o tunnel es. PPPoF" protocolston dat-porta3389 actionadat-pat to-addresse"TP privato

#### **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/