

iliad

CONFIGURAZIONE MIKROTIK - GUI



iliad.it

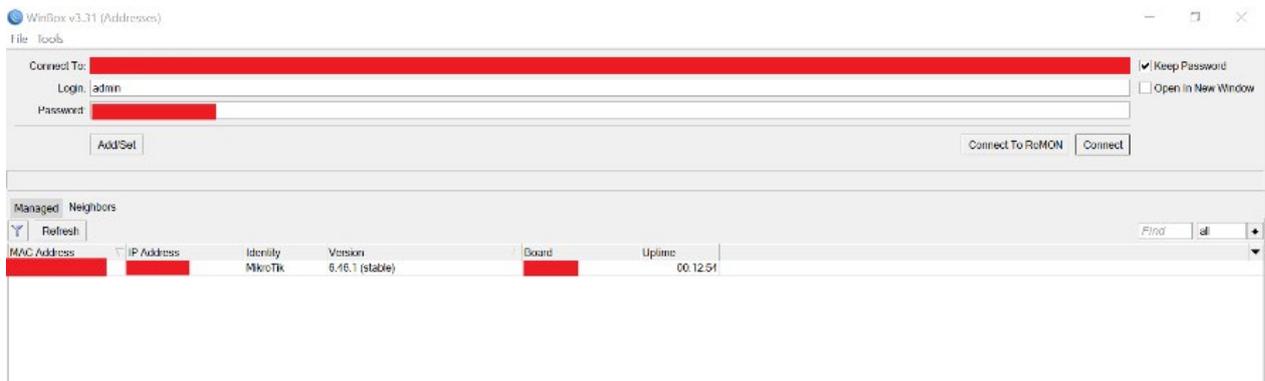
CONFIGURAZIONE MIKROTIK - GUI

CONNESSIONE ALL'APPARATO

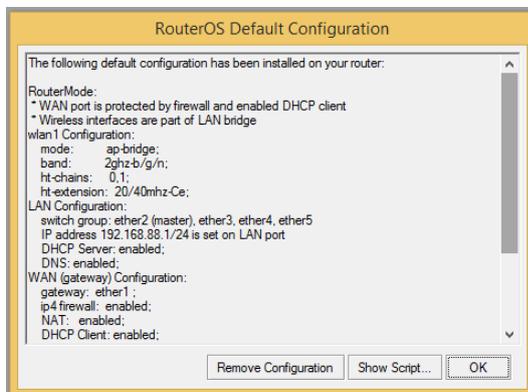
Effettuare il download di Winbox dal seguente link: <https://mikrotik.com/download>

Note: Verificare compatibilità con sistema operativo utilizzato. Se compatibile, procedere con gli step seguenti.

1. Collegare il router Mikrotik e il proprio PC tramite cavo RJ-45. Di default, tutte le porte del router sono attive.
2. Aprire Winbox sul device utilizzato per effettuare la configurazione e verificare che nella sezione neighbors venga rilevato il router Mikrotik
3. Effettuare il login con i parametri di default – Login: admin (no password)



4. Rimuovere la “default config” che si presenta al primo avvio come da esempio che segue e attendere il reboot. Al termine del riavvio, effettuare nuovamente il login seguendo i punti 2 e 3.



5. La schermata di winbox dovrà presentarsi come segue:



CONFIGURAZIONE INTERFACCE FISICHE/VIRTUALI E WIRELESS

6. Partendo dal punto 5:
 - Selezionare System → Packages → Selezionare ipv6 → Enable
 - Selezionare System → Reboot: Yes

7. Partendo dal punto 5:
 - Selezionare Interfaces → + → Bridge → Name : WAN → OK
 - Selezionare Interfaces → + → Bridge → Name : LAN → OK
 - Selezionare Interfaces → + → Bridge → Name : LAN-VOIP → OK
 - Selezionare Interfaces → + → VLAN → Name: WAN:836 → VLAN ID: 836 → Interface: WAN
 - Selezionare Interfaces → + → IPIPv6 Tunnel → Name: ipv6-tunnel1 → Local Address: **Dato disponibile in area personale** → Remote Address: **Dato disponibile in area personale** → OK
 - Selezionare Interfaces → wlan1 o wlan2 → Wireless → Mode: AP bridge

Note: Avendo la possibilità di modificare i parametri in base alle proprie esigenze, un esempio di configurazione potrebbe essere come segue:

The screenshot shows the configuration page for Interface <wlan1> in WinBox. The 'Wireless' tab is active, and several settings are highlighted with yellow boxes:

- Mode: ap bridge
- Band: 5GHz-A/N/AC
- Channel Width: 20/40/80MHz Ceee
- Frequency: 5180
- SSID: Home
- Country: italy
- Installation: indoor
- WMM Support: disabled
- Bridge Mode: enabled
- VLAN Mode: no tag
- VLAN ID: 1
- Default AP Tx Limit: (empty)
- Default Client Tx Limit: (empty)
- Default Authenticate:
- Default Forward:
- Hide SSID:
- Multicast Helper: default
- Multicast Buffering:
- Keepalive Frames:

8. Partendo dal punto 5:
 - Selezionare Wireless → doppio click su default → Mode: dynamic keys → Authentication Types: WPA PSK, WPA2 PSK → Unicast Ciphers: aes ccm,tkip → Group Ciphers: aes ccm,tkip

Note: Nelle sezioni successive "WPA Pre-Shared Key" e "WPA2 Pre-Shared Key" configurare la password del WIFI associata all'SSID scelto nel punto 6

CONFIGURAZIONE BRIDGE

9. Partendo dal punto 5:

- Selezionare Bridge → Ports → + → Interface: sfp-sfplus1 → Bridge: WAN → OK
- Selezionare Bridge → Ports → + → Interface: ether1 → Bridge: LAN → OK
- Selezionare Bridge → Ports → + → Interface: ether2 → Bridge: LAN → OK
- Selezionare Bridge → Ports → + → Interface: ether3 → Bridge: LAN → OK
- [...] fino alla porta ether9
- Selezionare Bridge → Ports → + → Interface: wlan1 → Bridge: LAN → OK
- Selezionare Bridge → Ports → + → Interface: wlan2 → Bridge: LAN → OK
- Selezionare Bridge → Ports → + → Interface: ether10 → Bridge: LAN-VOIP → OK

CONFIGURAZIONE IPv4 ADDRESSING

10. Partendo dal punto 5:

- Selezionare IP → Addresses → + → Address: **Dato disponibile in area personale** → Interface: ipipv6-tunnel1 → OK
- Selezionare IP → Addresses → + → Address: 192.168.1.1/24 → Interface: LAN → OK
Note: L'IP utilizzato è d'esempio, è possibile utilizzare qualsiasi altra classe IP privata riportata nella documentazione RFC 1597 e 1918
- Selezionare IP → Addresses → + → Address: 192.168.2.1/24 → Interface: LAN-VOIP → OK
- Selezionare IP → Pool → + → Name: DHCP-LAN → Addresses: 192.168.1.2-192.168.1.254 → OK
Note: Gli IP utilizzati sono d'esempio, è possibile utilizzare qualsiasi altra classe IP riportata nella documentazione RFC 1597 e 1918.
- Selezionare IP → DHCP Server → + → Name: DHCP-LAN → Interface: LAN → Address Pool: DHCP-LAN → OK
- Selezionare IP → DHCP Server → Networks → + → Address: 192.168.1.0/24 → Gateway: 192.168.1.1 → DNS Server: 8.8.8.8,8.8.4.4 → OK
Note: Verificare che nella sezione Leases il dispositivo/dispositivi collegati abbiano ricevuto un IP dal DHCP server (in questo caso la Mikrotik)
- Selezionare IP → Pool → + → Name: DHCP-VOIP-LAN → Addresses: 192.168.2.2-192.168.2.254 → OK
Note: Gli IP utilizzati sono d'esempio, è possibile utilizzare qualsiasi altra classe IP riportata nella documentazione RFC 1597 e 1918. In questa sezione è fondamentale configurare un range di IP disponibili.
- Selezionare IP → DHCP Server → + → Name: DHCP-VOIP-LAN → Interface: LAN-VOIP → Address Pool: DHCP-VOIP-LAN → OK
- Selezionare IP → DHCP Server → Networks → + → Address: 192.168.2.0/24 → Gateway: 192.168.2.1 → DNS Server: 8.8.8.8,8.8.4.4 → OK
Note: Verificare che nella sezione Leases il dispositivo/dispositivi collegati abbiano ricevuto un IP dal DHCP server (in questo caso la Mikrotik)
- Selezionare IP → Firewall → NAT → + → Chain: srcnat → Src. Address: 192.168.1.0/24 → Action → Action: masquerade → OK
- Selezionare IP → Routes → + → Dst. Address: 0.0.0.0/0 → Gateway: ipipv6-tunnel1 → OK

CONFIGURAZIONE IPv6 ADDRESSING

11. Partendo dal punto 5:

- Selezionare IPv6 → Addresses → + → Addresses: **Dato disponibile in area personale** → Interface: ipipv6-tunnel1 → OK
- Selezionare IPv6 → DHCP Client → + → DHCP → Interface: WAN:836 → Request: Selezionare address,prefix → Pool Name: ipv6-pool → Selezionare "Use Peer DNS, Rapid Commit, Add default Route → OK → Click sulla voce "Release"
- Selezionare IPv6 → Addresses → + → Addresses: ::192:168:1:1/64 → From Pool: : ipv6-pool → Interface: LAN → Selezionare Advertise → OK
- Selezionare IPv6 → Addresses → + → Addresses: ::192:168:2:1/64 → From Pool: : ipv6-pool → Interface: LAN-VOIP → Selezionare Advertise → OK
- Selezionare IPv6 → Routes → + → Dst. Address: **Dato disponibile in area personale** → Gateway: WAN → OK

PERSONALIZZARE CREDENZIALI DI ACCESSO ALL'APPARATO

Come best practices una volta effettuate le configurazioni, si consiglia dalla schermata di winbox (punto 5):

- New Terminal → copiare e incollare
/user add name=myname password=mypassword group=full
/user remove admin

Note: "Myname" e "mypassword" sono valori di default che devono essere cambiati con le credenziali che si vogliono utilizzare per collegarsi all'apparato.

- New Terminal → copiare e incollare
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set api disabled=yes
set api-ssl disabled=yes

Per maggiori dettagli

- https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router

- https://wiki.mikrotik.com/wiki/Main_Page

CONFIGURAZIONE VOIP – ESEMPIO CON GRANDSTREAM H813

Di seguito i dati necessari per la configurazione del dispositivo e le relative schermate.

- **SIP USERNAME:** Dato disponibile in area personale
- **SIP PASSWORD:** Dato disponibile in area personale
- **SIP DOMAIN:** voip.iliad.it
- **SIP OUTBOUND PROXY:** Dato disponibile in area personale
- **SIP PORT:** 5060
- **SIP PROTOCOL:** UDP

https://www.grandstream.com/hubfs/Product_Documentation/HT813_User_Guide.pdf

Internet Protocol: IPv4 Only IPv6 Only Both, prefer IPv4 Both, prefer IPv6

Disable SIP NOTIFY Authentication: No Yes (Device will not challenge NOTIFY with 401 when set to Yes)

Authenticate Conf File: No Yes (cfg file would be authenticated before acceptance if set to Yes)

Validate Server Certificates: No Yes (validate server certificates with our trusted list of TLS connections)

Account Active: No Yes

Primary SIP Server: (e.g., sip.mycompany.com, or IP address)

Failover SIP Server: (Optional, used when primary server no response)

Prefer Primary SIP Server: No Yes (yes - will register to Primary Server if Failover registration expires)

Outbound Proxy: (e.g., proxy.myprovider.com, or IP address, if any)

Backup Outbound Proxy: (e.g., proxy.myprovider.com, or IP address, if any)

Prefer Primary Outbound Proxy: No Yes (yes - will reregister via Primary Outbound Proxy if registration expires)

Allow DHCP Option 120 (override SIP server): No Yes

SIP Transport: UDP TCP TLS (default is UDP)

SIP URI Scheme When Using TLS: sip sips

Use Actual Ephemeral Port in Contact with TCP/TLS: No Yes

NAT Traversal: No Keep-Alive STUN UPnP

SIP User ID: (the user part of an SIP address)

Authenticate ID: (can be identical to or different from SIP User ID)

Authenticate Password: (purposely not displayed for security protection)

Name: (optional, e.g., John Doe)

DNS Mode: A Record SRV NAPTR/SRV

DNS SRV use Registered IP: No Yes

Tel URI: Disabled

SIP Registration: No Yes

Unregister On Reboot: No Yes

Outgoing Call without Registration: No Yes

Register Expiration: 60 (in minutes, default 1 hour, max 45 days)

Reregister before Expiration: 0 (0-64800, Default 0 second)

SIP Registration Failure Retry Wait Time: 20 (in seconds, Between 1-3600, default is 20)

SIP Registration Failure Retry Wait Time upon 403 Forbidden: 1200 (in seconds, Between 0-3600, default is 1200, 0 means stop retry registration upon 403 response.)

Enable SIP OPTIONS Keep Alive: No Yes

SIP OPTIONS Keep Alive Interval: 30 (in seconds, Between 1-64800, default is 30)

SIP OPTIONS Keep Alive Max Lost: 3 (Number of max lost packets for SIP OPTIONS Keep Alive before re-registration. Between 3-10, default is 3)

Layer 3 QoS: 26 SIP DSCP (Diff-Serv value in decimal, 0-63, default 26)

46 RTP DSCP (Diff-Serv value in decimal, 0-63, default 46)

SIP Registration Failure Retry Wait Time: (in seconds. Between 1-3600, default is 20)

SIP Registration Failure Retry Wait Time upon 403 Forbidden: (in seconds. Between 0-3600, default is 1200. 0 means stop retry registration upon 403 response.)

Enable SIP OPTIONS Keep Alive: No Yes

SIP OPTIONS Keep Alive Interval: (in seconds. Between 1-64800, default is 30)

SIP OPTIONS Keep Alive Max Lost: (Number of max lost packets for SIP OPTIONS Keep Alive before re-registration. Between 3-10, default is 3)

Layer 3 QoS: SIP DSCP (Diff-Serv value in decimal, 0-63, default 26)
 RTP DSCP (Diff-Serv value in decimal, 0-63, default 46)

Local SIP Port: (default is 5060 for UDP; 5061 for TLS)

Local RTP Port: (even number between 1024-65535, default 5004)

Use Random SIP Port: No Yes

Use Random RTP Port: No Yes

Enable RTCP: No Yes

Hold Target Before Refer: No Yes

Refer-To Use Target Contact: No Yes

Transfer on Conference Hangup: No Yes

Disable Bellcore Style 3-Way Conference: No Yes (Using star code *23 for 3-way conference)

Remove OBP from Route Header: No Yes

Support SIP Instance ID: No Yes

Validate Incoming SIP Message: No Yes

Check SIP User ID for incoming INVITE: No Yes (no direct IP calling if Yes)

Authenticate incoming INVITE: No Yes

Authenticate server certificate domain: No Yes

Authenticate server certificate chain: No Yes

SIP Registration Failure Retry Wait Time: (in seconds. Between 1-3600, default is 20)

SIP Registration Failure Retry Wait Time upon 403 Forbidden: (in seconds. Between 0-3600, default is 1200. 0 means stop retry registration upon 403 response.)

Enable SIP OPTIONS Keep Alive: No Yes

SIP OPTIONS Keep Alive Interval: (in seconds. Between 1-64800, default is 30)

SIP OPTIONS Keep Alive Max Lost: (Number of max lost packets for SIP OPTIONS Keep Alive before re-registration. Between 3-10, default is 3)

Layer 3 QoS: SIP DSCP (Diff-Serv value in decimal, 0-63, default 26)
 RTP DSCP (Diff-Serv value in decimal, 0-63, default 46)

Local SIP Port: (default is 5060 for UDP; 5061 for TLS)

Local RTP Port: (even number between 1024-65535, default 5004)

Use Random SIP Port: No Yes

Use Random RTP Port: No Yes

Enable RTCP: No Yes

Hold Target Before Refer: No Yes

Refer-To Use Target Contact: No Yes

Transfer on Conference Hangup: No Yes

Disable Bellcore Style 3-Way Conference: No Yes (Using star code *23 for 3-way conference)

Remove OBP from Route Header: No Yes

Support SIP Instance ID: No Yes

Validate Incoming SIP Message: No Yes

Check SIP User ID for incoming INVITE: No Yes (no direct IP calling if Yes)

Authenticate incoming INVITE: No Yes

Authenticate server certificate domain: No Yes

Authenticate server certificate chain: No Yes

SIP User-Agent:

SIP User-Agent Postfix:

Disable Call-Waiting: No Yes

Disable Call-Waiting Caller ID: No Yes

Disable Call-Waiting Tone: No Yes

Disable Connected Line ID: No Yes

Disable Receiver Offhook Tone: No Yes (ROH tone will not be played after offhook for 60 seconds)

Disable Reminder Ring for On-Hold Call: No Yes

Disable Visual MWI: No Yes

Do Not Escape '#' as %23 in SIP URI: No Yes

Disable Multiple m line in SDP: No Yes

Ring Timeout: (0-300, default is 60 seconds, 0 means no timeout)

Delayed Call Forward Wait Time: (Allowed range 1-120, in seconds.)

No Key Entry Timeout: (1-15, default is 4 seconds)

Early Dial: No Yes (use "Yes" only if proxy supports 484 response)

Dial Plan Prefix: (this prefix string is added to each dialed number)

Use # as Dial Key: No Yes (if set to Yes, "#" will function as the "(Re-)Dial" key)

Dial Plan:

SUBSCRIBE for MWI: No, do not send SUBSCRIBE for Message Waiting Indication
 Yes, send periodical SUBSCRIBE for Message Waiting Indication

Send Anonymous: No Yes (caller ID will be blocked if set to Yes)

Anonymous Call Rejection: No Yes

Special Feature:

Enable Session Timer: No Yes

Session Expiration: (90-64800, default 180 seconds)

Min-SE: (90-64800, default 90 seconds)

Caller Request Timer: No Yes (Request for timer when making outbound calls)

Callee Request Timer: No Yes (When caller supports timer but did not request one)

Force Timer: No Yes (Use timer even when remote party does not support)

UAC Specify Refresher: UAC UAS Omit (Recommended)

UAS Specify Refresher: UAC UAS (When UAC did not specify refresher tag)

Force INVITE: No Yes (Always refresh with INVITE instead of UPDATE)

Enable 100rel: No Yes

Add Auth Header On Initial REGISTER: No Yes

Conference URI:

Use First Matching Vocoder in 200OK SDP: No Yes

Preferred Vocoder (in listed order):
 choice 1:
 choice 2:
 choice 3:
 choice 4:
 choice 5:
 choice 6:
 choice 7:

Voice Frames per TX:

G723 Rate: 6.3kbps encoding rate 5.3kbps encoding rate

iLBC Frame Size: 20ms 30ms

Disable OPUS Stereo in SDP: No Yes (removes "/2" from offer)

iLBC Payload Type: (between 96 and 127, default is 97)

OPUS Payload Type: (between 96 and 127, default is 123)

VAD: No Yes

Symmetric RTP: No Yes

Fax Mode: T.38 Pass-Through

Re-INVITE After Fax Tone Detected: Enabled Disabled

Jitter Buffer Type: Fixed Adaptive

Jitter Buffer Length: Low Medium High

SRTP Mode: Disabled Enabled but not forced Enabled and forced

Crypto Life Time: Disabled Enabled

SLIC Setting:

Caller ID Scheme:

DTMF Caller ID:

Polarity Reversal: No Yes (reverse polarity upon call establishment and termination)

Loop Current Disconnect: No Yes (loop current disconnect upon call termination)

Play busy/reorder tone before Loop Current Disconnect: No Yes (play busy/reorder tone before loop current disconnect upon call fail)

Loop Current Disconnect Duration: (100 - 10000 milliseconds. Default 200 milliseconds)

Enable Pulse Dialing: No Yes

Pulse Dialing Standard:

Enable Hook Flash: No Yes

Enable Hook Flash: No Yes

Hook Flash Timing: In 40-2000 milliseconds range, minimum: maximum:

On Hook Timing: (In 40-2000 milliseconds range, default is 400)

Gain: TX RX

Disable Line Echo Canceller (LEC): No Yes

Disable Network Echo Suppressor: No Yes

Outgoing Call Duration Limit: (0-180 minutes, default is 0 (No Limit))

Enable High Ring Power: No Yes

RFC2833 Events Count: (between 2 and 10, default is 8)

RFC2833 End Events Count: (between 2 and 10, default is 3)

Distinctive Ring Tone: used if incoming caller ID is
 used if incoming caller ID is
 used if incoming caller ID is

Ring Tones (Syntax: c=on1/off1-on2/off2-on3/off3;)

Ring Tone 1:

Ring Tone 2:

Ring Tone 3:

Ring Tone 4:

Ring Tone 5:

Ring Tone 6:

Ring Tone 7:

Ring Tone 8:

Ring Tone 9:

Ring Tone 10:

iliad