SOP-NET-002_MikroTik_Config_v1.0.0

SOP-NET-002_MikroTik_Config_v1.0.0

Standard Operating Procedure: Network Configuration

Document ID:	SOP-NET-002
Title:	MikroTik Router Configuration
Version:	1.1
Status:	Final
Author:	System Administrator
Approved By:	Director of Technology
Effective Date:	2025-12-02

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to provide a standardized, step-by-step guide for the basic configuration of MikroTik routers. Adhering to this procedure ensures that all routers are set up with consistent, secure, and reliable settings.

2.0 Scope

This SOP applies to all IT personnel and network engineers responsible for deploying and managing MikroTik routers within the organization's infrastructure. This document covers the initial setup and essential configuration components. Advanced or client-specific configurations are outside the scope of this document.

3.0 Responsibilities

- **Network Engineers / IT Technicians:** Responsible for executing the procedures outlined in this document.

- **Director of Technology:** Responsible for reviewing and approving this SOP and any subsequent revisions.

4.0 Prerequisites

- Physical or remote access to the MikroTik router.
- Access to the MikroTik WinBox utility (download from mikrotik.com).
- Knowledge of the client's network requirements, including WAN IP information, and internal IP schema.
- Default credentials: username `admin`, password is blank (empty) on new devices.

5.0 Procedure

This procedure outlines the key configuration steps to be performed in the MikroTik router's interface, typically using WinBox.

5.1 Initial Security Configuration (CRITICAL)

> **IMPORTANT:** Complete these steps FIRST on any new or factory-reset device before proceeding with network configuration.

5.1.1 Change Admin Password

1. Navigate to **System > Users**.
2. Double-click the `admin` user.
3. Click **Password** and set a strong password (minimum 12 characters, mixed case, numbers, symbols).
4. Click **OK** to save.

CLI alternative:

```
/user set admin password="YourSecurePassword123!"
```

5.1.2 Set System Identity

1. Navigate to **System > Identity**.
2. Set the `Identity` field to a descriptive name related to the client or location (e.g., `ClientName-Router`).

5.1.3 Configure Time and NTP

1. Navigate to **System > Clock**.
2. Set the correct **Time Zone**.
3. Navigate to **System > NTP Client**.
4. Enable the NTP Client.
5. Set NTP Servers: `time.google.com` and `pool.ntp.org`.

CLI alternative:

```
/system clock set time-zone-name=America/Chicago
/system ntp client set enabled=yes servers=time.google.com,pool.ntp.org
```

5.2 Interfaces

Review and manage the physical and virtual interfaces.

1. Navigate to **Interfaces**.
2. Disable any unused physical ports.
3. If required, create VLANs by clicking the **Add (+)** button and selecting **VLAN**. Assign a `Name`, `VLAN ID`, and associate it with a physical `Interface`.

5.3 Bridge

Create a bridge to logically group multiple interfaces (e.g., for a single LAN segment).

1. Navigate to **Bridge**.
2. On the **Bridge** tab, click **Add (+)** to create a new bridge.
3. On the **Ports** tab, click **Add (+)** to assign interfaces (physical ports or VLANs) to the newly created bridge.

5.4 IP: Addresses

Assign IP addresses to the router's interfaces.

1. Navigate to **IP > Addresses**.
2. Click **Add (+)** to assign an IP address.
3. Specify the `Address` with its subnet (e.g., `192.168.1.1/24`).
4. Assign it to the correct `Interface` (e.g., the WAN port, a LAN bridge, or a VLAN).
5. Repeat for all necessary interfaces (WAN, LAN, etc.).

5.5 IP: DHCP Client

Configure the WAN interface to receive an IP address automatically if a static IP is not provided by the ISP.

1. Navigate to **IP > DHCP Client**.
2. Click **Add (+)**.
3. Set the `Interface` to the primary WAN port (e.g., `ether1`).
4. Ensure this is only used if the WAN IP is dynamic.

5.6 IP: Pool

Define the range of IP addresses to be distributed by the DHCP server.

1. Navigate to **IP > Pool**.
2. Click **Add (+)**.

3. Assign a `Name` to the pool (e.g., `lan-pool`).
4. Define the `Addresses` range. Format: `192.168.1.20-192.168.1.200`.

5.7 IP: DHCP Server

Configure the DHCP server to assign IP addresses to client devices on the LAN.

1. Navigate to **IP > DHCP Server**.
2. On the **DHCP** tab, click **Add (+)**.
3. Configure the server instance:
   - **Name:** A descriptive name for the server.
   - **Interface:** The LAN bridge or interface the server will listen on.
   - **Address Pool:** Select the pool created in step 5.6.
4. Navigate to the **Networks** tab and click **Add (+)**.
5. Define the network details:
   - **Address:** The network address and subnet (e.g., `192.168.1.0/24`).
   - **Gateway:** The router's LAN IP address (e.g., `192.168.1.1`).
   - **DNS Servers:** The DNS servers to be provided to clients.
6. Navigate to the **Leases** tab to view active leases. Static leases can be created here by assigning an IP to a specific MAC address.

5.8 IP: DNS

Configure the DNS servers that the router itself will use for resolution.

1. Navigate to **IP > DNS**.
2. In the `Servers` field, enter the IP addresses of the primary and secondary DNS servers.

5.9 IP: Routes

Ensure a default route exists for outbound internet traffic. This is often added automatically but should be verified.

1. Navigate to **IP > Routes**.
2. Check for a route where `Dst. Address` is `0.0.0.0/0`.
3. If it does not exist, click **Add (+)** and create it:
   - **Dst. Address:** `0.0.0.0/0`
   - **Gateway:** The ISP's gateway IP address (the WAN gateway).

5.10 IP: Firewall - NAT

Configure Network Address Translation (NAT) to allow devices on the internal network to access the internet.

1. Navigate to **IP > Firewall > NAT**.
2. Click **Add (+)** to create a new rule.
3. In the **General** tab:
   - **Chain:** `srcnat`

- **Out. Interface:** Set to the primary WAN port (e.g., `ether1`).

4. In the **Action** tab:
   - **Action:** `masquerade`

5.11 IP: Firewall - Filter Rules (CRITICAL)

> **IMPORTANT:** Proper firewall rules are essential for security. Rules are processed in order - connection tracking rules MUST come first.

Navigate to **IP > Firewall > Filter Rules** and create the following rules in this exact order:

5.11.1 Input Chain (Traffic TO the Router)

#	Chain	Connection State	In Interface	Action	Comment
1	input	established,related	-	accept	Allow established connections
2	input	invalid	-	drop	Drop invalid packets
3	input	-	ether1 (WAN)	drop	Drop all other WAN input

5.11.2 Forward Chain (Traffic THROUGH the Router)

#	Chain	Connection State	In Interface	Action	Comment
4	forward	established,related	-	accept	Allow established connections
5	forward	invalid	-	drop	Drop invalid packets
6	forward	new	ether1 (WAN)	drop	Drop new connections from WAN

5.11.3 CLI Commands (Recommended)

```
/ip firewall filter

# Input chain - traffic to the router
add chain=input connection-state=established,related action=accept comment="Accept establish
add chain=input connection-state=invalid action=drop comment="Drop invalid"
add chain=input in-interface=ether1 action=drop comment="Drop all other WAN input"

# Forward chain - traffic through the router
add chain=forward connection-state=established,related action=accept comment="Accept establi
add chain=forward connection-state=invalid action=drop comment="Drop invalid"
add chain=forward connection-state=new in-interface=ether1 action=drop comment="Drop new fro
```

5.11.4 Optional: Allow Specific Management Access If remote management is needed from specific IPs, add BEFORE the drop rules:

```
/ip firewall filter
add chain=input src-address=YOUR.MANAGEMENT.IP.HERE dst-port=8899 protocol=tcp action=accept
```

5.12 IP: Services (Security Hardening)

Disable non-essential services and restrict management access.

1. Navigate to **IP > Services**.
2. Disable the following services by selecting and clicking the **X** (disable) button:
   - `telnet` (port 23) - insecure, use SSH instead
   - `ftp` (port 21) - insecure
   - `www` (port 80) - use www-ssl instead if web access needed
   - `api` (port 8728) - disable unless specifically required
   - `api-ssl` (port 8729) - disable unless specifically required
3. Configure `winbox`:
   - Double-click `winbox`
   - Change **Port** to `8899` (non-standard port)
   - Set **Available From** to restrict access to trusted networks (e.g., `10.0.0.0/8` or specific management IPs)
4. If SSH access is needed:
   - Keep `ssh` enabled
   - Change port from default 22 to non-standard (e.g., `2222`)
   - Set **Available From** to trusted networks only

CLI commands:

```
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set api disabled=yes
set api-ssl disabled=yes
set winbox port=8899 address=10.0.0.0/8
set ssh port=2222 address=10.0.0.0/8
```

5.13 Configuration Backup

Always export configuration after completing setup.

1. Navigate to **Files**.
2. Click **Backup** to create a binary backup (.backup file).
3. For human-readable export, open **Terminal** and run: `/export file=router-config`
4. Download backup files via WinBox drag-and-drop or FTP.

Backup types: - `.backup` - Binary, includes passwords, restore to same hardware only - `.rsc` (export) - Plain text script, portable, passwords excluded by default

CLI backup commands:

```
# Binary backup (includes passwords)
/system backup save name=ClientName-backup

# Text export (portable, excludes sensitive data)
/export file=ClientName-export

# Text export with sensitive data
/export file=ClientName-export-full hide-sensitive=no
```

5.14 RouterOS Upgrade

Check and upgrade RouterOS firmware regularly.

1. Navigate to **System > Packages**.
2. Click **Check For Updates**.
3. If update available, review the changelog.
4. Click **Download & Install** (router will reboot).

CLI alternative:

```
/system package update check-for-updates
/system package update install
```

> **NOTE:** For major version upgrades (e.g., 6.x to 7.x), review migration guide at mikrotik.com first.

5.15 Troubleshooting

Issue	Cause	Resolution
Cannot connect via WinBox	Wrong IP, firewall blocking, or WinBox service disabled	Use MAC address connection in WinBox. Check IP > Services for WinBox status. Verify Available From restrictions.
Router not reachable after firewall changes	Firewall rules blocking management access	Use MAC-WinBox to connect. Check input chain rules. Add accept rule for WinBox port before drop rule.
No internet after NAT configuration	Masquerade not on correct interface or missing default route	Verify masquerade Out Interface = WAN. Check IP > Routes for 0.0.0.0/0 route to gateway.
DHCP clients not getting addresses	DHCP server not enabled or wrong interface	Check IP > DHCP Server. Verify server is on correct bridge/interface. Check address pool.
Slow performance	CPU overload, bad cables, or hardware issues	Check System > Resources for CPU usage. Check interface errors with `/interface print stats`.
Cannot SSH to router	SSH disabled or port changed	Check IP > Services. Verify SSH is enabled and note port number. Check Available From restrictions.
Password forgotten	N/A	Physical access required. Use Netinstall to reset (erases config).
WinBox connection drops	Idle timeout or network issues	Check System > Identity (session timeout). Use keepalive or reconnect.
VLANs not working	Bridge VLAN filtering misconfigured	Verify `/interface bridge vlan print`. Check pvid on ports. Ensure VLAN filtering is enabled on bridge.
Firmware upgrade fails	Insufficient storage or incompatible package	Check System > Resources for free space. Download correct package for architecture (arm, mipsbe, etc.).

Diagnostic Commands:

```
# Check system resources
/system resource print

# View interface status and errors
/interface print stats
```

```
# Check active connections
/ip firewall connection print

# View logs
/log print

# Test connectivity
/tool ping 8.8.8.8
/tool traceroute 8.8.8.8

# Check CPU usage by process
/tool profile
```

6.0 Revision History

Version	Date	Author	Change Description
1.0	2025-12-02	System Administrator	Initial document creation.
1.1	2025-12-29	Jeremy Smith	SME Review: Added Section 5.1 (Initial Security - admin password, NTP). Rewrote Section 5.11 with proper connection tracking firewall rules. Enhanced Section 5.12 with service restriction by source IP. Added Section 5.13 (Backup) and 5.14 (RouterOS Upgrade). Added Section 5.15 (Troubleshooting) with common issues and diagnostic commands.