

RouterOS Assistant — Bedienungsanleitung

Diese Anleitung beschreibt ausschließlich Funktionen, die **live gegen echte MikroTik-Hardware getestet und bestätigt** sind (Meilensteine mit  in `README.md`). Funktionen, die noch nicht vollständig verifiziert sind (z.B. Teile der WLAN-Einrichtung, der neue wifiwave2-Treiber), sind hier als solche markiert oder stehen in `HANDOFF.md`.

Hinweis zu den Abbildungen: Diese Anleitung wird von einem KI-Assistenten gepflegt, der keinen Zugriff auf Bildschirm-/UI-Automatisierung für native macOS-Apps hat — echte Screenshots der App können deshalb nicht erzeugt werden. Zur Visualisierung dienen stattdessen Mermaid-Diagramme (als vorgerenderte Bilder in `Manual-assets/` eingebettet, aus derselben Quelldatei auch direkt als Mermaid-Code lesbar). Wer echte Screenshots ergänzen möchte: Bilder unter `Manual-assets/` ablegen und per `! [Beschreibung] (Manual-assets/dateiname.png)` einbinden.

Alle Feldnamen, Hilfetexte und Warnhinweise in Kapitel 5 (Experte) sind **wörtlich aus dem App-Quellcode übernommen** (`RouterOSSchemaCatalog.swift`, automatisiert extrahiert) — nicht paraphrasiert, damit sie exakt dem entsprechen, was in der App tatsächlich angezeigt wird.

Inhaltsverzeichnis

0. [Überblick & Architektur](#)
 1. [Verbinden](#)
 2. [Einrichten \(Wizard\)](#)
 3. [Übersicht](#)
 4. [LAN-Scanner](#)
 5. [Experte](#)
 6. [Sicherungen](#)
 7. [English summary](#)
-

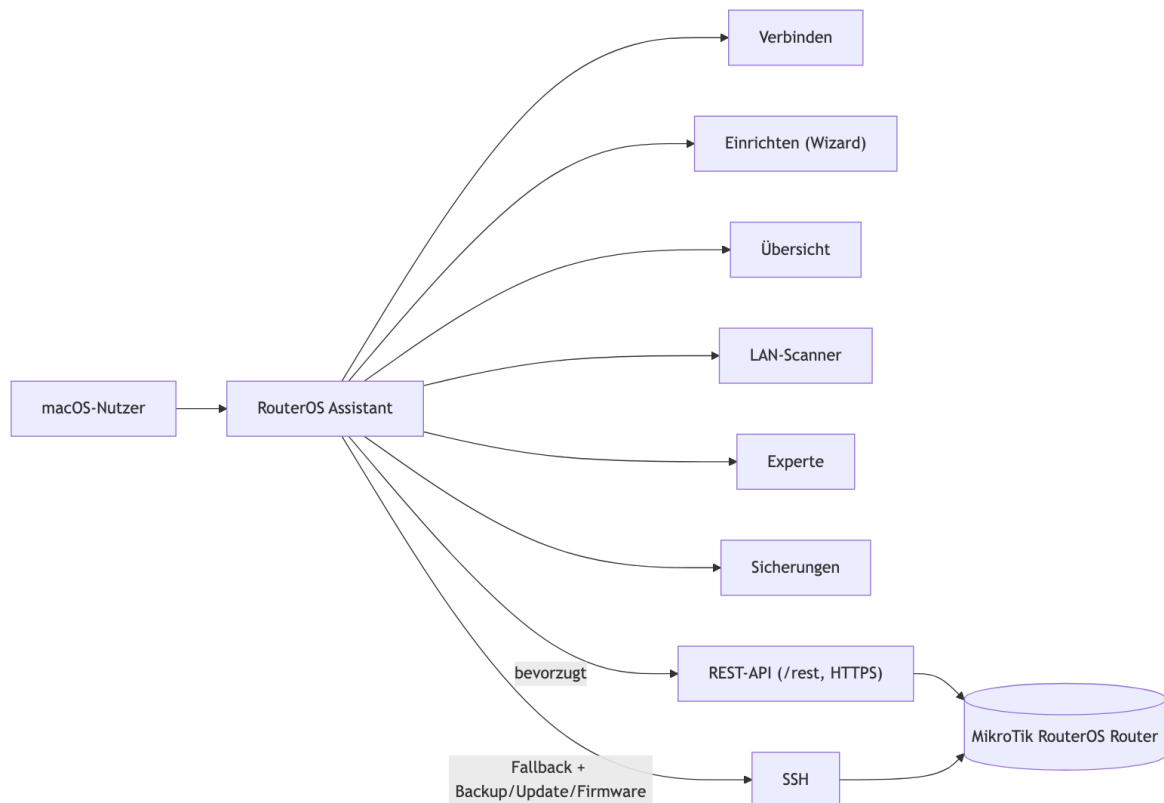
0. Überblick & Architektur

RouterOS Assistant ist eine native macOS-App (SwiftUI), die MikroTik-RouterOS-Router per geführtem Wizard einrichtet und über sechs Tabs verwaltet: **Verbinden**, **Einrichten**, **Übersicht**, **LAN-Scanner**, **Experte**, **Sicherungen**.

Die App spricht mit dem Router über zwei Transportwege:

- **REST-API** (`/rest/...`, HTTPS) — bevorzugt, seit RouterOS 7.1.
- **SSH** — Fallback, sowie zwingend für Funktionen, die es nur über die Kommandozeile gibt (automatisches Backup vor Änderungen, Firmware-Update, Software-Update-Check).

Welcher Weg genutzt wird, entscheidet die App automatisch — ohne Konfiguration.



Ein DE/EN-Umschalt-Button (Landesflagge) in der Toolbar wechselt die Sprache der App (persistiert über Neustarts). Alle sechs Tabs sind vollständig übersetzt (statische UI-Texte, Buttons, Tooltips). Werte, die direkt vom Router kommen (Fehlermeldungen, CLI-Befehlszeilen, Live-Log), bleiben unübersetzt.

1. Verbinden

Verbindungsaufbau

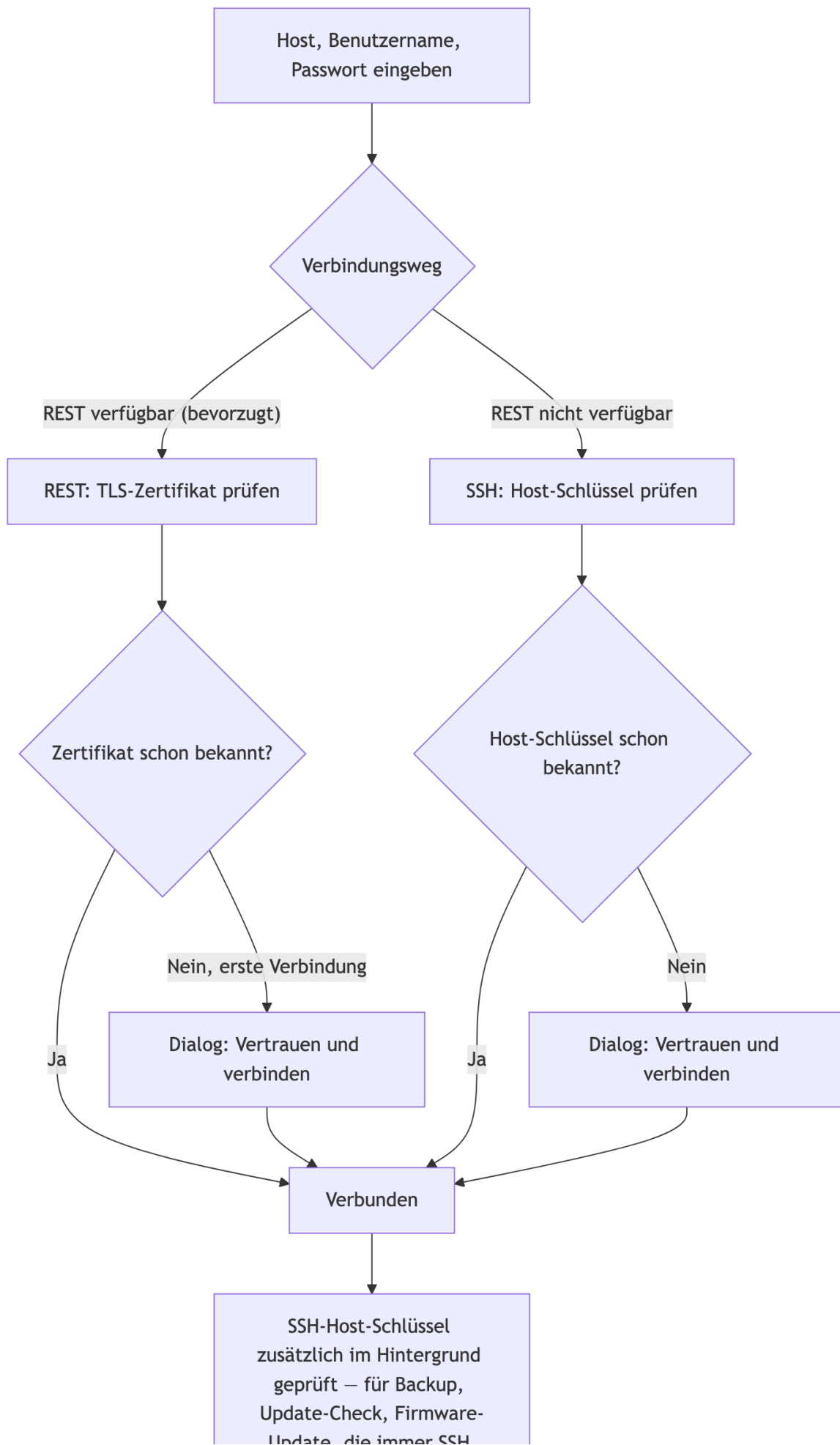
Feld	Hilfetext (wörtlich aus der App)
Host	„Die Adresse deines Routers im Netzwerk. Werkseinstellung bei Mikrotik ist meist 192.168.88.1.“
Benutzername	„Der Admin-Benutzername deines Routers. Werkseinstellung ist meist ‚admin‘.“
Passwort	„Das Passwort für diesen Benutzer. Bei unverändertem Werkszustand oft leer.“
Passwort merken	„Speichert das Passwort verschlüsselt in der macOS-Schlüsselbundverwaltung, damit du es nicht jedes Mal neu eingeben musst.“

Ein Augen-Symbol neben dem Passwortfeld deckt die Eingabe zur Kontrolle auf.

Vertrauensprüfung (Trust-on-First-Use)

Beim ersten Verbinden zu einem Router zeigt die App einen Dialog „Der Router hat sich mit einem unbekannten Zertifikat gemeldet“ (REST) bzw. „...mit einem unbekannten SSH-Schlüssel gemeldet“ (SSH) — einmalig zu bestätigen über „Vertrauen und verbinden“ (oder „Abbrechen“). Das schützt vor einem ausgetauschten/gefälschten Gerät unter derselben IP-Adresse.

Bei einer REST-Verbindung können **beide** Dialoge nacheinander erscheinen: den SSH-Host-Schlüssel prüft die App auch dann einmalig im Hintergrund, weil Backup, Update-Check und Firmware-Update immer SSH brauchen — unabhängig vom für die eigentliche Konfiguration genutzten Verbindungsweg.



Update, die immer sein
brauchen

Nach dem Verbinden

- Detailseite mit vollständigen Routerboard-Infos (Modell, Revision, Seriennummer, Firmware-Typ/-Version).
- **Software-Update-Check:** „Prüft bei MikroTik, ob eine neuere RouterOS-Version verfügbar ist. Braucht Internetzugang auf dem Router.“ Buttons „Jetzt prüfen“ / „Update installieren“.
- **Firmware-Update:** aktualisiert die Routerboard-Bootloader-Firmware separat. „Nötig, damit die neu geschriebene Firmware aktiv wird — passiert nicht automatisch“ → Button „Jetzt neu starten“.
- Quick-Backup-Button direkt im Tab: „Sichert die aktuelle Router-Konfiguration — sinnvoll direkt nach dem Verbinden, bevor du im Einrichten-Tab etwas änderst.“
- „Trennen“: „Beendet die Verbindung zum Router. Zugangsdaten bleiben erhalten (falls gemerkt).“

Bekannte Router

Nach jeder erfolgreichen Verbindung merkt sich die App Host, Benutzername und (falls vom Router gemeldet) Seriennummer. Zwei unterschiedliche Router mit identischem Host+Benutzername (z.B. beide auf MikroTiks Werks-Adresse 192.168.88.1 / admin) bleiben dadurch getrennte Einträge, erkennbar an der „SN: ...“-Zeile; das gemerkte Passwort wird pro Gerät getrennt im macOS-Schlüsselbund gespeichert. Der Anzeigename wird beim ersten Mal automatisch auf die Hardware-Bezeichnung gesetzt (z.B. „hEX“), lässt sich aber jederzeit über „Bearbeiten“ ändern — dort auch ein freies Standort-Feld (z.B. „Keller, Serverschrank“) zur besseren Unterscheidung mehrerer Router. Klick auf einen Eintrag füllt Host/Benutzername/Passwort ins Formular, ohne sofort zu verbinden. Ab ca. 4 Einträgen scrollt die Liste in sich selbst.

Live-Traffic-Anzeige

Der Punkt vor jedem Interface in der Geräte-Übersicht ist grau (kein Link), grün (Link, aber kein Datenverkehr) oder pulsierend grün (überträgt gerade tatsächlich Daten).

2. Einrichten (Wizard)

Geführter Schritt-für-Schritt-Assistent für die Grundkonfiguration. Ein Modus-Schalter zu Beginn wählt zwischen:

- **Einfach:** „Grundeinrichtung: Internetverbindung (WAN), ein Heimnetzwerk (LAN) mit DHCP, WLAN und ein fest aktivierter Firewall-Grundschutz. Kein VLAN, keine mehreren getrennten Netzwerke, keine Netzwerk-Isolation — für später jederzeit über den Expertenmodus nachrüstbar.“
- **Experte:** „Voller Zugriff: mehrere LAN-Interfaces mit je eigenem DHCP-Server, VLANs, Netzwerk-Isolation zwischen Netzwerken, und alle Firewall-Optionen.“



WAN (Internetanschluss)

Feld	Hilfetext
Port	„Der Netzwerkport, über den dein Router mit dem Internet verbunden ist (z.B. das Kabel zu deinem Modem oder deiner Anschlussdose).“
Verbindungsart	„Wie sich der Router beim Internetanbieter anmeldet. ‚Automatisch (DHCP)‘ passt für die meisten Kabel-/Glasfaseranschlüsse.“
Automatisch (DHCP)	„Der Router bezieht seine Internetadresse automatisch von deinem Anbieter. Für die meisten Kabel-/Glasfaser-Anschlüsse die richtige Wahl.“
Feste IP-Adresse	„Die feste IP-Adresse, die dir dein Anbieter zugewiesen hat, inklusive Netzmaske (die Zahl nach dem /, z.B. /24).“
Gateway	„Die Adresse des nächsten Geräts Richtung Internet — steht meist in den Unterlagen deines Anbieters.“
PPPoE-Benutzername	„Zugangsdaten von deinem Internetanbieter für die Einwahl (z.B. bei DSL-Anschlüssen).“
PPPoE-Passwort	„Das zum Benutzernamen gehörende Passwort von deinem Internetanbieter.“

LAN (ein oder mehrere Netzwerke)

Feld	Hilfetext
Port	„Der interne Netzwerk-Anschluss, an dem deine Geräte hängen (dein lokales Netzwerk, LAN).“
Router-Adresse	„Die Adresse, unter der der Router selbst in diesem Netzwerk erreichbar ist.“
Netzbereich	„Der komplette Adressbereich dieses Netzwerks (z.B. /24 erlaubt bis zu 254 Geräte).“
DHCP von	„Ab welcher Adresse der Router automatisch Adressen an Geräte in diesem Netzwerk vergibt.“
DHCP bis	„Bis zu welcher Adresse der Router automatisch Adressen an Geräte in diesem Netzwerk vergibt.“
Lease-Zeit	„Wie lange ein Gerät seine zugewiesene Adresse behält, bevor sie erneuert werden muss.“
DNS-Server	„Welcher Server Geräten in diesem Netzwerk Internetadressen in Namen übersetzt (z.B. www.google.de). Meist der Router selbst.“
Netzwerk-Isolation	„Verhindert Datenverkehr zwischen diesem und allen anderen konfigurierten LAN-/VLAN-Netzwerken. Der Internetzugriff bleibt erhalten. Wird im Firewall-Schritt umgesetzt.“

Im Experte-Modus lassen sich mehrere physische Ports/Interfaces als getrennte Netzwerke einrichten (Button „Weiteres LAN-Netzwerk hinzufügen“), jeweils mit eigenem Adressbereich und optionaler Netzwerk-Isolation. Adressfelder starten leer — das Feld selbst zeigt ein Beispielformat, das beim Tippen verschwindet.

Port-Konflikt-Prüfung: wählt der Nutzer einen Port, der bereits anders konfiguriert ist, erscheint eine Warnung mit dem Grund und der Option „Port jetzt freimachen...“ — „Wähle oben einen anderen, freien Port — oder mache diesen jetzt frei. Die bestehende Konfiguration wird dabei entfernt.“ Tatsächlich ausgeführt wird das erst mit „Jetzt anwenden“ am Ende des Assistenten — bis dahin lässt es sich rückgängig machen, indem oben ein anderer Port gewählt wird.

VLAN (optional)

„Ein VLAN ist ein zusätzliches Netzwerk mit eigenem Adressbereich — z.B. für Gäste oder smarte Geräte. Ob es vom Hauptnetzwerk abgeschottet ist, legst du unten pro Netzwerk über ‚Von anderen Netzwerken isolieren‘ fest. Wenn du unsicher bist, ob du das brauchst, überspring diesen Schritt einfach.“

Feld	Hilfetext
Name	„Ein Name zur Wiedererkennung, z.B. ‚Gäste‘ oder ‚Smart Home‘.“
VLAN-ID	„Eine eindeutige Nummer zur technischen Unterscheidung dieses Netzwerks. Muss nur innerhalb deines Routers einmalig sein.“
Basis-Port	„Der physische Anschluss, auf dem dieses zusätzliche Netzwerk aufbaut.“
Router-Adresse	„Die Adresse des Routers innerhalb dieses zusätzlichen Netzwerks.“
Netzbereich	„Der komplette Adressbereich dieses zusätzlichen Netzwerks.“
DHCP von/bis	„Ab/Bis zu welcher Adresse Geräte in diesem Netzwerk automatisch eine Adresse bekommen.“

WLAN (nur falls erkannt)

„An diesem Gerät wurde kein WLAN erkannt. Dieser Schritt wird übersprungen.“ — sonst: „Schaltet WLAN auf diesem Funkmodul ein und vergibt Netzwerkname und Passwort.“

Feld	Hilfetext
Netzwerkname (SSID)	„Der Name, den Geräte in ihrer WLAN-Liste sehen und mit dem sie sich verbinden.“
Passwort	„Das WLAN-Passwort (WPA2). Muss mindestens 8 Zeichen lang sein.“

Firewall-Grundschutz

„Schützt deinen Router und deine Geräte vor unaufgeforderten Zugriffen aus dem Internet und ermöglicht deinen Geräten den Internetzugriff (NAT).“ Im einfachen Modus immer aktiv; im Experte-Modus wählbar: „Richtet einen Standard-Schutz ein: Internetfreigabe (NAT) für dein Heimnetz, und blockiert unaufgeforderte Zugriffe aus dem Internet auf deinen Router und deine Geräte. Bestehende, selbst eingerichtete Regeln bleiben erhalten — die neuen Regeln werden vorangestellt.“

Hat der Router bereits eigene Firewall-Regeln, warnt die App zusätzlich: „Dein Router hat bereits eigene Firewall-Regeln. Die neuen Regeln werden vorangestellt, bestehende bleiben erhalten — prüfe nach dem Anwenden trotzdem die Reihenfolge, z.B. über Winbox oder ‚ip firewall filter print‘.“

Review / Apply

„Vor dem Anwenden wird automatisch eine Sicherung der aktuellen Konfiguration erstellt (Tab ‚Sicherungen‘). Ein garantiertes automatisches Zurückrollen bei Verbindungsabbruch gibt es nicht — bei Problemen die Sicherung im Tab ‚Sicherungen‘ verwenden oder den Router lokal (Ethernet/Konsole) wiederherstellen.“ Jeder einzelne Befehl wird vor der Ausführung angezeigt.

Der Wizard lässt sich auf einem bereits eingerichteten Router erneut ausführen (z.B. um ein weiteres Netzwerk hinzuzufügen) — bereits bestehende Einstellungen werden dabei nicht doppelt angelegt oder

beschädigt. „Abbrechen“ ist jederzeit über den Button oben rechts verfügbar (Einfach- wie Experte-Modus): „Alle in diesem Assistenten eingegebenen Werte gehen verloren“ — Bestätigungsdialog, setzt den Assistenten auf den ersten Schritt zurück.

3. Übersicht

Grafisches Diagramm des kompletten aktuellen Router-Zustands (IST-Zustand) — fünf Spalten, mit echten Verbindungslinien (keine Vermutungen, abgeleitet aus den tatsächlichen RouterOS-Referenzfeldern):

Spalte	RouterOS-Bereich
Interfaces	Physische Ports, Bridges, VLANs, WireGuard, ...
IP-Adressen	Zuweisungen aus <code>/ip address</code>
Pools & DHCP	Adress-Pools, DHCP-Server/-Netzwerke/-Clients
Routen	<code>/ip route</code>
Firewall & NAT	Filter-/NAT-Regeln, Adress-Listen

Nicht im Diagramm (aber über den Experte-Tab erreichbar): VPN: PPP-Benutzer/-Profile, WLAN-Sicherheitsprofile, Queues/Bandbreiten-Steuerung, System (Name/Uhrzeit/Scheduler/Skripte/Benutzerkonten), Werkzeuge (Netwatch/E-Mail), Firewall: Mangle- und Raw-Regeln.

Verbindungsarten (Linienfarben)

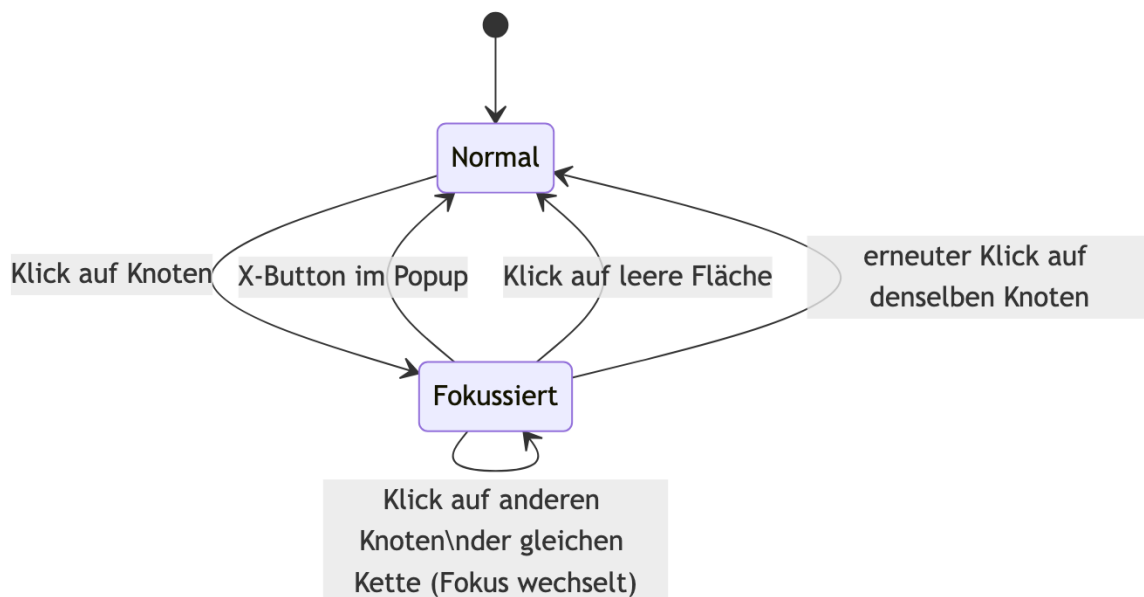
Art	Bedeutung (wörtlich aus der App)
VLAN → Basis-Interface	„Das VLAN-Interface baut auf dem Basis-Interface auf — es ist ein eigenes, per VLAN-Kennung getrenntes Netzwerk auf demselben physischen Anschluss.“
Bridge-Port	„Dieser physische Port ist Mitglied dieser Bridge — Geräte an diesem Port verhalten sich, als hängen sie am selben Kabel wie alle anderen Bridge-Ports.“
WireGuard-Peer	„Dieser WireGuard-VPN-Tunnel läuft über dieses Interface.“
Interface → IP-Adresse	„Diesem Interface ist diese IP-Adresse zugewiesen.“
DHCP / Pool	„Diese DHCP-Komponente (Server, Pool oder Netzwerk-Optionen) gehört zu diesem Interface bzw. dieser Adresse.“
Route → Interface	„Diese Route führt über dieses Interface bzw. dieses Gateway.“
Firewall/NAT → Interface	„Diese Firewall- oder NAT-Regel bezieht sich auf dieses Interface (als Eingang oder Ausgang).“
Adress-Liste → Regel	„Diese Regel prüft, ob eine Adresse in dieser Adress-Liste steht.“

Interaktion

- **Hover** über einen Knoten hebt seine Verbindungen hervor; **Klick** macht die Hervorhebung dauerhaft und öffnet gleichzeitig den **Fokus-Modus**.
- **Klick auf eine Verbindungslinie** zeigt rechts eine verständliche Erklärung, was diese Verbindung bedeutet, plus Sprung zu den beiden verbundenen Elementen.
- Zoom-Buttons (–/100%/+) für die Diagrammgröße; Kästchen lassen sich frei verschieben (Verbindungslinien folgen live mit), „Zurücksetzen“ in der Toolbar stellt die ursprüngliche Spalten-Anordnung wieder her.
- Verbindungslinien laufen animiert in Flussrichtung („von → nach“).
- Aktualisiert sich automatisch, sobald in den Tab gewechselt wird.

Fokus-Modus

Klick auf einen Knoten öffnet ein schwebendes Popup mit der **kompletten verbundenen Kette** (alle direkt und indirekt verbundenen Elemente, transitive Hülle) im selben Spalten-Layout wie oben, sauber neu angeordnet; alles andere im Hauptdiagramm wird abgedunkelt. Schließen über den X-Button oben im Popup, Klick auf die leere Fläche daneben, oder erneuten Klick auf denselben Knoten. Da es sich um ein nicht-modales Overlay handelt (kein System-Sheet), bleibt die rechte Seitenleiste währenddessen bedienbar — ein Knoten aus der Kette lässt sich also direkt aus dem Popup heraus über „Bearbeiten“ ändern. Die Popup-Größe passt sich automatisch dem Inhalt an, ohne Scrollbalken.



Direktes Bearbeiten

IP-Adressen, Pools, DHCP-Server/-Netzwerke/-Clients, Routen, Firewall-Filter-/NAT-Regeln, WireGuard-Peers und Interfaces (Ethernet, Bridge, WLAN, VLAN, WireGuard) lassen sich anklicken und über „Bearbeiten“ direkt ändern — schreibt sofort an den Router zurück. Adress-Listen-Knoten sind hier noch nicht direkt editierbar, nur über den Experte-Tab, da ein Knoten dort mehrere Einträge zusammenfasst. Dynamische/ automatisch angelegte Routen (z.B. die Verbindungsrouten eines Netzwerks) zeigen bewusst keinen Bearbeiten-Button, da RouterOS solche Einträge selbst verwaltet.

4. LAN-Scanner

Zeigt alle Geräte im Netzwerk (aus DHCP-Leases und ARP-Tabelle), gruppiert nach physischem Port. „Neu scannen“ fragt Leases/ARP/ Bridge-Host-Tabelle erneut ab. Jede Port-Überschrift zeigt zusätzlich den aktuellen Live-Durchsatz in MB/s (↓/↑, grünes Symbol bei aktivem Datenverkehr, graues im Leerlauf, Abfrage alle 0,1s) mit kleinem Liniendiagramm der letzten 30 Sekunden. Spalten: Name, IP-Adresse, MAC-Adresse, Status.

Alle Aktionen zu einem Gerät liegen im „Aktionen“-Button (⋯) hinter der jeweiligen Zeile:

- Bei dynamischer Adresse → **„Feste IP zuweisen“** (macht die aktuelle Adresse dauerhaft, RouterOS' „Make Static“). Rückweg: „Aktionen“ → „Feste Zuweisung entfernen“ — danach muss das Gerät kurz die Verbindung trennen/neu aufbauen, um automatisch wieder eine dynamische Adresse zu bekommen. Ohne DHCP-Lease ist die Option ausgegraut: „Kein DHCP-Lease — feste Zuweisung hier nicht möglich“.
- Bei fester Adresse → **„Feste Zuweisung entfernen“**.
- **Netzwerk-Tools** (im selben Menü):
 - **Ping / Traceroute** — „Ausgeführt vom Router aus (eigene SSH-Verbindung) — testet die Erreichbarkeit vom Router zu diesem Gerät, nicht von diesem Mac.“
 - **DNS-Auflösung (nslookup)** — nur verfügbar, wenn ein Hostname bekannt ist.
 - **Port-Scan** — „TCP-Verbindungsversuch auf gängige Ports, ausgeführt von diesem Mac aus (nicht vom Router) — rot = offen, grün = geschlossen (Gerät antwortet, aber nichts lauscht dort), grau = keine Antwort (Firewall, Gerät aus, oder Port gefiltert).“
 - **Rohdaten anzeigen** — „Alle Felder, die RouterOS für diesen Eintrag zurückgegeben hat — hilfreich, falls Status/Port hier falsch aussieht.“

Alle drei Ergebnis-Popups (Rohdaten, Netzwerk-Test, Port-Scan) teilen dasselbe Layout: fester Kopfbereich mit Titel + X-Button zum Schließen, darunter der scrollbare Inhalt — derselbe Aufbau wie beim Fokus-Popup der Übersicht und beim Experte-Bearbeiten-Formular (siehe Kapitel 3 und 5).

5. Experte

Direkter, kuratierter Zugriff auf die meisten RouterOS-Bereiche. Für jedes Feld gibt es einen Hilfetext mit Format-Beispiel. Kategorien sind einklappbar (Standard: zugeklappt) — Klick auf die größere, farblich hinterlegte Überschrift klappt sie auf/zu.

Eigener Menüpfad: jeder RouterOS-Menüpfad ist erreichbar, auch ohne kuratiertes Formular — Felder erscheinen dann generisch als Schlüssel/Wert-Paare. Auch bei kuratierten Menüs landet jedes von RouterOS zusätzlich gelieferte, nicht kuratierte Feld automatisch im Bereich „Weitere Parameter (frei)“ — nichts, was RouterOS unterstützt, ist dadurch unerreichbar, auch wenn es (noch) kein eigenes Formularfeld hat.

Vor jeder Änderung: Bestätigungsdiallog mit dem exakten Befehl, der ausgeführt wird. Automatisches Backup einmal pro Verbindungssitzung vor der ersten Änderung.

Das Bearbeiten-Formular selbst hat denselben festen Kopfbereich (Titel + X-Button, bleibt beim Scrollen sichtbar) wie das Fokus-Popup der Übersicht und die Ergebnis-Popups des LAN-Scanners — ein einheitliches Schließen-Verhalten in der ganzen App.

Die folgende Referenz ist **automatisiert aus RouterOSSchemaCatalog.swift extrahiert** — Feldname, RouterOS-Parametername, Feldtyp, Pflicht-Status, Vorbelegung und Hilfetext entsprechen exakt dem, was in der App angezeigt wird. „Verweis auf bestehenden Eintrag“ bedeutet: die App lädt beim Öffnen live die existierenden Namen aus dem referenzierten Menü und zeigt sie als Auswahlliste. „Auswahl aus Live-Interface-Liste“ lädt beim Öffnen die aktuell am Router vorhandenen Interfaces.

System

Router-Name (*Einstellungsmenü — genau ein Eintrag, kein Anlegen/Löschen*)

RouterOS-Menü: `/system identity` · REST-Pfad: `system/identity`

Der Name, unter dem sich der Router meldet (z.B. in Winbox/Terminal-Prompt).

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	<code>name</code>	Text	Ja	—	Frei wählbar, z.B. MeinRouter.

Uhrzeit/Zeitzone (*Einstellungsmenü — genau ein Eintrag, kein Anlegen/Löschen*)

RouterOS-Menü: `/system clock` · REST-Pfad: `system/clock`

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Zeitzone	<code>time-zone-name</code>	Text	Nein	—	Z.B. Europe/Berlin.

Zeitserver (NTP) (*Einstellungsmenü — genau ein Eintrag, kein Anlegen/Löschen*)

RouterOS-Menü: `/system ntp client` · REST-Pfad: `system/ntp/client`

Hält die Router-Uhr über einen Zeitserver synchron.

Die Server-Liste selbst liegt in einem eigenen Menü ("NTP-Zeitserver-Liste") — hier nur Ein/Aus und Modus.

⚠ Achtung: Falsche Systemzeit kann Zertifikatsprüfungen (HTTPS/REST) und Log-Zeitstempel durcheinanderbringen.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Aktiviert	<code>enabled</code>	Ja/Nein	Nein	<code>yes</code>	Zeitsynchronisation ein-/ausschalten.
Modus	<code>mode</code>	Auswahl (fest): <code>unicast</code> , <code>broadcast</code> , <code>multicast</code> , <code>manycast</code>	Nein	<code>unicast</code>	Fast immer "unicast" (direkte Anfrage an feste Server).

NTP-Zeitserver-Liste

RouterOS-Menü: `/system ntp client servers` · REST-Pfad: `system/ntp/client/servers`

Die Zeitserver, die der Client abfragt.

"servers" ist bei RouterOS 7.x kein Feld am NTP-Client selbst, sondern eine eigene Liste — jeder Server ist ein eigener Eintrag hier (statt kommagetrennt in einem Textfeld).

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Adresse	<code>address</code>	Text	Ja	—	Hostname oder IP eines Zeitservers, z.B. pool.ntp.org .
Deaktiviert	<code>disabled</code>	Ja/Nein	Nein	<code>no</code>	Diesen Server deaktivieren, ohne ihn zu löschen.
Kommentar	<code>comment</code>	Text	Nein	—	Nur zur eigenen Wiedererkennung.

Zeitplaner

RouterOS-Menü: `/system scheduler` · REST-Pfad: `system/scheduler`

Führt ein hinterlegtes Skript zu festen Zeiten/Intervallen aus.

⚠ Achtung: Ein fehlerhaftes geplantes Skript kann unbeaufsichtigt wiederholt Änderungen vornehmen — vor dem Einplanen einmal manuell testen.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	<code>name</code>	Text	Ja	—	Frei wählbar, z.B. taeglicher-neustart.
Startzeit	<code>start-time</code>	Text	Nein	—	Z.B. 00:00:00 oder "startup".
Intervall	<code>interval</code>	Zeitdauer (Tage/Std/Min/Sek, per Stepper)	Nein	—	Wie oft wiederholt wird. Alles auf 0 lassen = nur einmal zur Startzeit.
Auszuführendes Skript	<code>on-event</code>	Verweis auf bestehenden Eintrag unter <code>/system script</code>	Nein	—	Name eines zuvor unter "Skripte" angelegten Skripts.
Deaktiviert	<code>disabled</code>	Ja/Nein	Nein	<code>no</code>	Zeitplan inaktiv schalten, ohne ihn zu löschen.

Skripte

RouterOS-Menü: `/system script` · REST-Pfad: `system/script`

Gespeicherte RouterOS-Befehlsfolgen, die manuell oder per Scheduler ausgeführt werden.

⚠ Achtung: Skripte laufen mit den Rechten des Routers selbst — kein Unterschied zu manuell eingegebenen Befehlen.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	name	Text	Ja	—	Frei wählbar, z.B. backup-taeglich.
Skript-Inhalt	source	Text	Nein	—	RouterOS-Befehle, z.B. ":log info "Test"".

Benutzerkonten

RouterOS-Menü: `/user` · REST-Pfad: `user`

Zugangskonten für den Router (Winbox/SSH/REST/Terminal).

⚠ Achtung: Das zum Verbinden genutzte eigene Konto hier nicht versehentlich löschen oder herabstufen.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Benutzername	name	Text	Ja	—	Frei wählbar, z.B. admin2.
Passwort	password	Text	Nein	—	Ausreichend lang und zufällig wählen.
Rechte-Gruppe	group	Auswahl (fest): full, write, read	Nein	full	full = Vollzugriff, write = ohne Benutzerverwaltung, read = nur lesen.
Deaktiviert	disabled	Ja/Nein	Nein	no	Konto inaktiv schalten, ohne es zu löschen.

Protokollierung

RouterOS-Menü: `/system logging` · REST-Pfad: `system/logging`

Was der Router mitschreibt und wohin (Speicher, Datei, Remote-Syslog, E-Mail).

Besteht aus "rules" (was protokolliert wird) und "actions" (wohin) — hier generischer Zugriff, verwandte Teile über "Eigener Menüpfad" (z.B. `/system logging action`).

Noch kein kuratiertes Formular — alle Felder erscheinen als freie Schlüssel/Wert-Paare (siehe „Eigener Menüpfad“).

Interfaces (Bridge, VLAN, VPN-Tunnel...)

Alle Interfaces (generisch)

RouterOS-Menü: `/interface` · REST-Pfad: `interface`

Gemeinsame Felder, die für jedes Interface gelten, unabhängig vom Typ (Ethernet, Bridge, WLAN, WireGuard, VLAN, ...).

RouterOS listet hier alle Interfaces zusammen. Typ-spezifische Felder (z.B. die VLAN-ID eines VLAN-Interfaces) liegen in den jeweils eigenen Menüs (z.B. "VLAN-Interfaces") — hier nur das, was für jeden Interface-Typ gleich funktioniert.

⚠ Achtung: RouterOS liefert hier zusätzlich einen "default-name" (Werksname des Ports) mit — der erscheint unten bei "Weitere Parameter", ist aber nicht änderbar ("bad parameter default-name", live bestätigt). Zum Umbenennen nur das Feld "Name" oben verwenden.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	name	Text	Ja	—	Der aktuelle Name dieses Interfaces, z.B. ether5 oder vlan20 — nicht zu verwechseln mit "default-name" (Werksname, weiter unten bei "Weitere Parameter", nicht änderbar).
Kommentar	comment	Text	Nein	—	Nur zur eigenen Wiedererkennung, ohne technische Wirkung.
Deaktiviert	disabled	Ja/Nein	Nein	no	Interface inaktiv schalten, ohne es zu löschen.

Bridge

RouterOS-Menü: `/interface bridge` · REST-Pfad: `interface/bridge`

Fasst mehrere physische Ports zu einem gemeinsamen Layer-2-Netzwerk zusammen.

Geräte an gebrückten Ports verhalten sich, als hingen sie am selben Netzwerk-Kabel. Eine IP-Adresse wird meist auf die Bridge selbst gelegt, nicht auf die einzelnen Ports.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	name	Text	Ja	—	Frei wählbar, z.B. bridge-lan.
VLAN-Filterung (802.1Q)	vlan-filtering	Ja/Nein	Nein	no	Aktiviert echte VLAN-Trennung über diese Bridge — nötig, wenn mehrere VLANs über dieselben Bridge-Ports laufen sollen.
Deaktiviert	disabled	Ja/Nein	Nein	no	Bridge inaktiv schalten, ohne sie zu löschen.

Bridge-Ports

RouterOS-Menü: `/interface bridge port` · REST-Pfad: `interface/bridge/port`

Ordnet einen physischen Port einer Bridge zu.

Erst danach ist der Port Teil des Bridge-Netzwerks.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Bridge	bridge	Text	Ja	—	Name der Bridge, z.B. bridge-lan.
Physischer Port	interface	Auswahl aus Live-Interface-Liste des Routers	Ja	—	Der Port, der der Bridge hinzugefügt wird, z.B. ether2.
Port-VLAN-ID (PVID)	pvid	Zahl	Nein	—	Nur mit aktivierter VLAN-Filterung relevant: VLAN, dem untagged ankommender Verkehr an diesem Port zugeordnet wird, z.B. 20.

VLAN-Interfaces

RouterOS-Menü: `/interface vlan` · REST-Pfad: `interface/vlan`

Virtuelle, getaggte Sub-Interfaces auf einem physischen Port oder einer Bridge.

Ein eigenes logisches Netzwerk auf demselben Kabel, unterschieden durch eine VLAN-Kennung im Ethernet-Rahmen.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	name	Text	Ja	—	Frei wählbar, z.B. vlan20-gaeste.
VLAN-ID	vlan-id	Zahl	Ja	—	Eindeutige Kennung, 2–4094, z.B. 20.
Basis-Interface	interface	Auswahl aus Live-Interface-Liste des Routers	Ja	—	Physischer Port oder Bridge, auf dem dieses VLAN aufsetzt, z.B. bridge.
Deaktiviert	disabled	Ja/Nein	Nein	no	VLAN-Interface inaktiv schalten, ohne es zu löschen.

WireGuard-Interfaces

RouterOS-Menü: `/interface wireguard` · REST-Pfad: `interface/wireguard`

Moderner, schlanker VPN-Tunnel-Typ.

Ein WireGuard-Interface allein stellt noch keine Verbindung her — dazu gehören Gegenstellen (siehe "WireGuard-Peers") mit öffentlichem Schlüssel und erlaubten Adressen.

⚠ Achtung: Erst hier das Interface anlegen (mit Listen-Port), danach unter WireGuard-Peers die Gegenstellen eintragen. Der private Schlüssel wird beim Anlegen automatisch erzeugt, falls nicht angegeben.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	name	Text	Ja	—	Frei wählbar, z.B. wg-heim.
Listen-Port (UDP)	listen-port	Zahl	Nein	51820	Port, auf dem dieser Tunnel auf eingehende Verbindungen lauscht, z.B. 51820.
Privater Schlüssel	private-key	Text	Nein	—	Geheim halten. Leer lassen, damit RouterOS automatisch einen erzeugt.
Deaktiviert	disabled	Ja/Nein	Nein	no	Interface inaktiv schalten, ohne es zu löschen.

WireGuard-Peers

RouterOS-Menü: `/interface wireguard peers` · REST-Pfad: `interface/wireguard/peers`

Gegenstellen (Clients/andere Router) eines WireGuard-Tunnels.

Jede Gegenstelle braucht ihren eigenen öffentlichen Schlüssel und eine Angabe, welche Adressen über sie geroutet werden.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
WireGuard-Interface	interface	Verweis auf bestehenden Eintrag unter <code>/interface wireguard</code>	Ja	—	Name des zuvor angelegten WireGuard-Interfaces.
Öffentlicher Schlüssel der Gegenstelle	public-key	Text	Ja	—	Vom Gerät der Gegenstelle kopieren (z.B. per "wg show public-key").
Erlaubte Adressen	allowed-address	Text	Nein	—	Welche IP-Adressen/Netze über diesen Peer laufen dürfen, mit Präfix, z.B. 10.10.10.2/32.
Feste Adresse der Gegenstelle	endpoint-address	Text	Nein	—	Nur nötig, wenn diese Gegenstelle selbst erreichbar sein muss (Site-to-Site), z.B. eine feste öffentliche IP oder ein DNS-Name. Bei Roadwarrior-Clients, die sich selbst melden, leer lassen.
Port der Gegenstelle	endpoint-port	Text	Nein	—	Meist derselbe Port wie der Listen-Port der Gegenstelle, z.B. 51820.
Keepalive	persistent-keepalive	Zeitdauer (Tage/Std/Min/Sek, per Stepper)	Nein	—	Hält die Verbindung durch NAT/Firewalls am Leben. Wichtig bei Clients hinter NAT.

PPPoE-Client

RouterOS-Menü: `/interface pppoe-client` · REST-Pfad: `interface/pppoe-client`

DSL-Einwahl-Client, meist auf dem WAN-Port.

Ersetzt eine feste/DHCP-WAN-Adresse durch eine PPPoE-Einwahl beim Provider.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	name	Text	Ja	—	Frei wählbar, z.B. pppoe-wan.
Physischer Port	interface	Auswahl aus Live-Interface-Liste des Routers	Ja	—	Der Port, über den die Einwahl läuft, meist der WAN-Port, z.B. ether1.
Benutzername	user	Text	Ja	—	Zugangsdaten des Providers.
Passwort	password	Text	Ja	—	Zugangsdaten des Providers.
Deaktiviert	disabled	Ja/Nein	Nein	no	Einwahl inaktiv schalten, ohne sie zu löschen.

Bonding

RouterOS-Menü: `/interface bonding` · REST-Pfad: `interface/bonding`

Bündelt mehrere physische Ports zu einer logischen, ausfalltoleranten/schnelleren Verbindung.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	name	Text	Ja	—	Frei wählbar, z.B. bond1.
Gebündelte Ports	slaves	Text	Nein	—	Kommagetrennte Liste physischer Ports, z.B. ether2,ether3.
Modus	mode	Auswahl (fest): 802.3ad , active-backup , balance-rr , balance-xor , broadcast	Nein	—	802.3ad (LACP) braucht einen kompatiblen, entsprechend konfigurierten Switch.

IP-Adressierung & Dienste

IP-Adressen

RouterOS-Menü: `/ip address` · REST-Pfad: `ip/address`

Weist Interfaces IP-Adressen zu.

Jede IP-Adresse hängt an genau einem Interface (physischer Port, Bridge oder VLAN).

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Adresse	address	Text	Ja	—	IP-Adresse mit Netzmaske als Präfix (Router-Adresse in diesem Netz), z.B. 192.168.88.1/24 oder 10.10.10.1/24. Das /24 legt fest, wie viele Geräte in dieses Netz passen (/24 = bis zu 254).

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Interface	<code>interface</code>	Auswahl aus Live-Interface-Liste des Routers	Ja	—	Interface, dem diese Adresse zugewiesen wird, z.B. bridge oder ether4.
Deaktiviert	<code>disabled</code>	Ja/Nein	Nein	<code>no</code>	Adresse inaktiv schalten, ohne sie zu löschen.

Adress-Pools

RouterOS-Menü: `/ip pool` · REST-Pfad: `ip/pool`

Adressbereiche, aus denen DHCP-Server oder PPP-Profil Adressen vergeben.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	<code>name</code>	Text	Ja	—	Frei wählbar, z.B. dhcp_pool_lan.
Bereich(e)	<code>ranges</code>	Text	Ja	—	Von-bis-Adresse ohne Präfix, z.B. 192.168.88.10-192.168.88.254. Mehrere Bereiche kommasetrennt.

DHCP-Server

RouterOS-Menü: `/ip dhcp-server` · REST-Pfad: `ip/dhcp-server`

Vergibt automatisch IP-Adressen an Geräte in einem Netzwerk.

Für die üblichen Fälle deckt das bereits der Einrichten-Assistent (LAN-/VLAN-Schritt) ab — hier direkter Zugriff für Sonderfälle.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	<code>name</code>	Text	Ja	—	Frei wählbar, z.B. dhcp_lan.
Interface	<code>interface</code>	Auswahl aus Live-Interface-Liste des Routers	Ja	—	Netzwerk, in dem dieser Server Adressen vergibt, z.B. bridge.
Adress-Pool	<code>address-pool</code>	Verweis auf bestehenden Eintrag unter <code>/ip pool</code>	Ja	—	Name eines zuvor angelegten Adress-Pools.
Lease-Zeit	<code>lease-time</code>	Zeitdauer (Tage/Std/Min/Sek, per Stepper)	Nein	—	Wie lange ein Gerät seine Adresse behält, bevor sie erneuert werden muss, z.B. 1d oder 12h.
Deaktiviert	<code>disabled</code>	Ja/Nein	Nein	<code>no</code>	DHCP-Server inaktiv schalten, ohne ihn zu löschen.

DHCP-Netzwerke

RouterOS-Menü: `/ip dhcp-server network` · REST-Pfad: `ip/dhcp-server/network`

Gateway/DNS/Optionen, die ein DHCP-Server an seine Klienten verteilt.

Getrennt vom DHCP-Server selbst, weil dieselben Netzwerk-Optionen für mehrere DHCP-Server gelten können.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Netz	address	Text	Ja	—	Für dieses Netz gelten die folgenden Optionen — die Netzadresse mit Präfix, z.B. 192.168.88.0/24.
Gateway	gateway	Text	Ja	—	In der Regel die Router-Adresse in diesem Netz, ohne Präfix, z.B. 192.168.88.1.
DNS-Server	dns-server	Text	Nein	—	Meist der Router selbst, z.B. 192.168.88.1. Mehrere Server kommagetrennt möglich.

DHCP-Client (WAN)

RouterOS-Menü: `/ip dhcp-client` · REST-Pfad: `ip/dhcp-client`

Bezieht automatisch eine IP-Adresse vom Internetanbieter.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Interface	interface	Auswahl aus Live-Interface-Liste des Routers	Ja	—	Meist der WAN-Port, z.B. ether1.
Standardroute übernehmen	add-default-route	Ja/Nein	Nein	yes	Übernimmt die vom Provider mitgeteilte Standardroute ins Internet.
DNS-Server übernehmen	use-peer-dns	Ja/Nein	Nein	yes	Übernimmt die vom Provider mitgeteilten DNS-Server.
Deaktiviert	disabled	Ja/Nein	Nein	no	DHCP-Client inaktiv schalten, ohne ihn zu löschen.

DNS-Einstellungen (*Einstellungsmenü — genau ein Eintrag, kein Anlegen/Löschen*)

RouterOS-Menü: `/ip dns` · REST-Pfad: `ip/dns`

Namensauflösung des Routers selbst (und optional als DNS-Server fürs LAN).

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
DNS-Server	servers	Text	Nein	—	Ein oder mehrere Server, kommagetrennt, z.B. 1.1.1.1,8.8.8.8.
Als DNS-Server fürs LAN erlauben	allow-remote-requests	Ja/Nein	Nein	no	Lässt Geräte im LAN den Router selbst als DNS-Server nutzen. Ohne das schlagen DNS-Anfragen von Geräten an den Router fehl, selbst wenn sie ihn als DNS-Server eingetragen haben.

Verwaltungsdienste

RouterOS-Menü: `/ip service` · REST-Pfad: `ip/service`

Schaltet Zugriffswege auf den Router (Winbox, API, SSH, WWW/REST, Telnet, FTP) an/aus und ändert deren Port.

Jeder aktive Dienst ist ein potenzieller Angriffspunkt aus dem jeweils erreichbaren Netz — nicht benötigte Dienste deaktivieren.

⚠ Achtung: Den gerade genutzten Zugriffsweg hier abzuschalten oder umzuportieren kann die eigene Verbindung sofort kappen — Vorsicht bei `www-ssl` (REST-API dieser App) und `ssh`.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Dienst	<code>name</code>	Auswahl (fest): <code>www</code> , <code>www-ssl</code> , <code>ssh</code> , <code>api</code> , <code>api-ssl</code> , <code>winbox</code> , <code>ftp</code> , <code>telnet</code>	Ja	—	Welcher Verwaltungsdienst geändert wird.
Port	<code>port</code>	Zahl	Nein	—	Auf welchem Port der Dienst lauscht, z.B. 22 für <code>ssh</code> .
Erlaubt von	<code>available-from</code>	Text	Nein	—	Optional: nur von dieser Adresse/diesem Netz aus erreichbar, mit Präfix, z.B. 192.168.88.0/24.
Deaktiviert	<code>disabled</code>	Ja/Nein	Nein	<code>no</code>	Dienst inaktiv schalten, ohne den Eintrag zu löschen.

Hotspot

RouterOS-Menü: `/ip hotspot` · REST-Pfad: `ip/hotspot`

Login-Portal für Gäste-WLAN/-LAN mit Umleitung auf eine Anmeldeseite.

Besteht aus mehreren zusammenhängenden Teilen (Server, Server-Profil, Benutzer-Profil, Benutzer) — hier generischer Zugriff auf `/ip hotspot` selbst, verwandte Teile über "Eigener Menüpfad" (z.B. `/ip hotspot user`).

Noch kein kuratiertes Formular — alle Felder erscheinen als freie Schlüssel/Wert-Paare (siehe „Eigener Menüpfad“).

Routing

Statische Routen

RouterOS-Menü: `/ip route` · REST-Pfad: `ip/route`

Feste, manuell eingetragene Wegewahl zu Netzen, die nicht direkt angeschlossen sind.

Für alles außer "Standard-Internet über eine WAN-Schnittstelle" (das übernimmt bereits die DHCP-Client-/PPPoE-Route automatisch).

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Zielnetz	<code>dst-address</code>	Text	Ja	—	Netz mit Präfix, z.B. 10.0.0.0/24, oder 0.0.0.0/0 für eine Standardroute.
Gateway	<code>gateway</code>	Text	Ja	—	Nächster Hop — IP-Adresse ohne Präfix (z.B. 192.168.88.254) oder Name eines Interfaces (z.B. ether1).
Distanz	<code>distance</code>	Zahl	Nein	—	Priorität bei mehreren passenden Routen zum selben Ziel — kleinere Zahl wird bevorzugt, z.B. 1.
Kommentar	<code>comment</code>	Text	Nein	—	Nur zur eigenen Wiedererkennung.
Deaktiviert	<code>disabled</code>	Ja/Nein	Nein	<code>no</code>	Route inaktiv schalten, ohne sie zu löschen.

OSPF-Instanzen

RouterOS-Menü: `/routing ospf instance` · REST-Pfad: `routing/ospf/instance`

Dynamisches Innennetz-Routing-Protokoll — tauscht Routen automatisch mit anderen OSPF-Routern aus.

Nur relevant, wenn mehrere Router im selben Netz eigenständig Routen lernen sollen.

⚠ Achtung: Fehlkonfiguriertes OSPF kann Routen zu bestehenden Netzen überschreiben. Nur mit Netzwerkplan einsetzen.

Noch kein kuratiertes Formular — alle Felder erscheinen als freie Schlüssel/Wert-Paare (siehe „Eigener Menüpfad“).

BGP-Verbindungen

RouterOS-Menü: `/routing bgp connection` · REST-Pfad: `routing/bgp/connection`

Routing-Protokoll für Verbindungen zwischen unabhängigen Netzen/Providern.

Für Privat-/Kleinnetz i.d.R. nicht nötig — relevant bei eigenem Provider-unabhängigem Adressraum (Multihoming).

Noch kein kuratiertes Formular — alle Felder erscheinen als freie Schlüssel/Wert-Paare (siehe „Eigener Menüpfad“).

VPN-Server/Clients

PPP-Benutzer

RouterOS-Menü: `/ppp secret` · REST-Pfad: `ppp/secret`

Zugangsdaten für PPPoE-/L2TP-/PPTP-/OpenVPN-Einwahl in den Router.

Jeder Benutzer kann optional einem Profil zugeordnet werden, das IP-Pool/DNS/Verschlüsselung vorgibt.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Benutzername	name	Text	Ja	—	Frei wählbar, z.B. gast1.
Passwort	password	Text	Ja	—	Ausreichend lang und zufällig wählen.
Dienst	service	Auswahl (fest): any , pppoe , l2tp , pptp , ovpn , sstp	Nein	any	Für welche Einwahl-Art dieser Benutzer gilt.
Profil	profile	Verweis auf bestehenden Eintrag unter /ppp profile	Nein	—	Name eines zuvor angelegten PPP-Profiles.
Lokale Adresse	local-address	Text	Nein	—	IP-Adresse des Routers innerhalb dieser Verbindung, ohne Präfix, z.B. 10.10.10.1.
Adresse für den Client	remote-address	Text	Nein	—	Feste IP für diesen Benutzer (z.B. 10.10.10.2), oder Name eines Adress-Pools.
Deaktiviert	disabled	Ja/Nein	Nein	no	Benutzer inaktiv schalten, ohne ihn zu löschen.

PPP-Profile

RouterOS-Menü: /ppp profile · REST-Pfad: ppp/profile

Vorlagen (IP-Pool, DNS, Verschlüsselung) für PPP-Benutzer.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	name	Text	Ja	—	Frei wählbar, z.B. vpn-clients.
Lokale Adresse	local-address	Text	Nein	—	IP-Adresse des Routers, ohne Präfix, z.B. 10.10.10.1.
Adress-Pool für Clients	remote-address	Text	Nein	—	Name eines zuvor angelegten Adress-Pools.
DNS-Server für Clients	dns-server	Text	Nein	—	Ein oder mehrere Server, kommasetrennt, z.B. 1.1.1.1,8.8.8.8.

L2TP-VPN-Server

RouterOS-Menü: /interface l2tp-server server · REST-Pfad: interface/l2tp-server/server

Nimmt eingehende L2TP-VPN-Einwahlen entgegen.

Ein einzelnes Server-weites An/Aus mit gemeinsamen Verschlüsselungs-Einstellungen — Benutzer selbst kommen von "PPP-Benutzer".

Noch kein kuratiertes Formular — alle Felder erscheinen als freie Schlüssel/Wert-Paare (siehe „Eigener Menüpfad“).

OpenVPN-Server

RouterOS-Menü: `/interface ovpn-server server` · REST-Pfad: `interface/ovpn-server/server`

Nimmt eingehende OpenVPN-Einwahlen entgegen.

Braucht zusätzlich ein Zertifikat ("/certificate") — Benutzer selbst kommen von "PPP-Benutzer".

Noch kein kuratiertes Formular — alle Felder erscheinen als freie Schlüssel/Wert-Paare (siehe „Eigener Menüpfad“).

WLAN / CAPsMAN

WLAN (Legacy-Treiber)

RouterOS-Menü: `/interface wireless` · REST-Pfad: `interface/wireless`

WLAN-Interfaces auf älteren/Standard-Wireless-Chips.

Diese Interfaces existieren bereits ab Werk (ein WLAN-Chip = ein Interface) — hier werden sie nur konfiguriert, nicht neu angelegt. Ein Sicherheitsprofil (siehe "WLAN-Sicherheitsprofile") muss vorher angelegt sein.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Netzwerkname (SSID)	<code>ssid</code>	Text	Ja	—	Der Name, den WLAN-Geräte in der Netzwerkliste sehen, z.B. MeinWLAN.
Sicherheitsprofil	<code>security-profile</code>	Text	Nein	—	Name eines zuvor unter "WLAN-Sicherheitsprofile" angelegten Profils.
Modus	<code>mode</code>	Auswahl (fest): <code>ap-bridge</code> , <code>station</code> , <code>bridge</code>	Nein	<code>ap-bridge</code>	<code>ap-bridge</code> = Access Point (Normalfall), <code>station</code> = als Client mit einem anderen AP verbinden.
Deaktiviert	<code>disabled</code>	Ja/Nein	Nein	<code>no</code>	WLAN-Interface inaktiv schalten, ohne es zu löschen.

WLAN-Sicherheitsprofile

RouterOS-Menü: `/interface wireless security-profiles` · REST-Pfad: `interface/wireless/security-profiles`

Verschlüsselung/Passwort-Vorlagen für WLAN-Interfaces (Legacy-Treiber).

Ein Profil wird angelegt und dann bei einem WLAN-Interface als "security-profile" eingetragen.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	name	Text	Ja	—	Frei wählbar, z.B. heimnetz-wpa2.
Modus	mode	Auswahl (fest): none , static-keys-required , dynamic-keys	Nein	dynamic-keys	dynamic-keys ist der übliche WPA/WPA2-Modus.
Authentifizierung	authentication-types	Auswahl (fest): wpa-psk , wpa2-psk , wpa-psk , wpa2-psk , wpa-eap , wpa2-eap	Nein	—	wpa2-psk = WPA2 mit gemeinsamem Passwort (Heimnetz-Standard).
WPA2-Passwort	wpa2-pre-shared-key	Text	Nein	—	Mindestens 8 Zeichen.

WLAN (neuer wifiwave2/802.11ax-Treiber)

RouterOS-Menü: `/interface wifi` · REST-Pfad: `interface/wifi`

WLAN-Interfaces auf neueren Wireless-Chips.

Anderes, verschachteltes Konfigurationsschema als der Legacy-Treiber (Punkt-Notation wie "security.passphrase") — nicht mit "/interface wireless" mischen. Nur auf Geräten mit entsprechend neuem WLAN-Chip vorhanden.

⚠ Achtung: Diese App hat den .set-Pfad für den neuen Treiber noch nie gegen echte Hardware getestet (siehe [HANDOFF.md](#)) — nach dem Anwenden unbedingt prüfen.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Netzwerkname (SSID)	ssid	Text	Ja	—	Der Name, den WLAN-Geräte in der Netzwerkliste sehen, z.B. MeinWLAN.
Authentifizierung	security.authentication-types	Auswahl (fest): wpa2-psk , wpa3-psk , wpa2-psk , wpa3-psk	Nein	—	wpa2-psk, wpa3-psk deckt sowohl ältere als auch neuere Geräte ab.
Passwort	security.passphrase	Text	Nein	—	Mindestens 8 Zeichen.
Ziel-Bridge	datapath.bridge	Text	Nein	—	Name der Bridge, der dieses WLAN-Netz zugeordnet wird (üblicherweise dieselbe wie das kabelgebundene LAN), z.B. bridge.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Deaktiviert	<code>disabled</code>	Ja/Nein	Nein	<code>no</code>	WLAN-Interface inaktiv schalten, ohne es zu löschen.

CAPsMAN-Zentrale

RouterOS-Menü: `/caps-man manager` · REST-Pfad: `caps-man/manager`

Zentrale Verwaltung mehrerer WLAN-Access-Points von einem Router aus.

Nur relevant mit mehreren WLAN-Access-Points, die zentral verwaltet werden sollen — eigenes, umfangreiches Konfigurationsschema (Konfigurationen/Kanäle/Datapaths).

Noch kein kuratiertes Formular — alle Felder erscheinen als freie Schlüssel/Wert-Paare (siehe „Eigener Menüpfad“).

Firewall: Filter-Regeln

Filter-Regeln

RouterOS-Menü: `/ip firewall filter` · REST-Pfad: `ip/firewall/filter`

Entscheidet, ob Pakete durchgelassen (accept), verworfen (drop/reject) oder weiter geprüft werden.

input = Zugriffe auf den Router selbst, forward = Verkehr, der durch den Router hindurchgeht (z.B. LAN↔Internet oder zwischen zwei Netzen), output = vom Router ausgehender Verkehr. Regeln werden von oben nach unten geprüft; die erste passende Regel entscheidet.

⚠ Achtung: Reihenfolge zählt. Neue Regeln landen am Ende der Liste — eine bereits vorhandene, weiter oben stehende Regel kann eine neue Regel unerreichbar machen. Position danach mit `/ip firewall filter print` kontrollieren, notfalls mit `move` verschieben.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Chain	<code>chain</code>	Text	Ja	<code>forward</code>	input = an den Router, forward = durch den Router, output = vom Router aus. Eigene Chains (Sprungziele über "jump") sind ebenfalls möglich. Beispiel: forward

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Aktion	<code>action</code>	Auswahl (fest): <code>accept</code> , <code>drop</code> , <code>reject</code> , <code>log</code> , <code>jump</code> , <code>return</code> , <code>add-src-to-address-list</code> , <code>add-dst-to-address-list</code> , <code>fasttrack-connection</code> , <code>passthrough</code>	Ja	<code>accept</code>	Was mit passenden Paketen geschieht. <code>reject</code> schickt zusätzlich eine Fehlermeldung zurück, <code>drop</code> verwirft stillschweigend.
Quell-Adresse	<code>src-address</code>	Text	Nein	—	Einzel-IP oder Netz mit Präfix, z.B. 192.168.88.5 oder 192.168.88.0/24. Leer = beliebig.
Ziel-Adresse	<code>dst-address</code>	Text	Nein	—	Einzel-IP oder Netz mit Präfix, z.B. 192.168.88.5 oder 192.168.88.0/24. Leer = beliebig.
Quelle in Adress-Liste	<code>src-address-list</code>	Verweis auf bestehenden Eintrag unter <code>/ip firewall address-list</code>	Nein	—	Nur Pakete, deren Absender in dieser zuvor angelegten Adress-Liste steht.
Ziel in Adress-Liste	<code>dst-address-list</code>	Verweis auf bestehenden Eintrag unter <code>/ip firewall address-list</code>	Nein	—	Nur Pakete, deren Ziel in dieser zuvor angelegten Adress-Liste steht.
Eingangs-Interface	<code>in-interface</code>	Auswahl aus Live-Interface-Liste des Routers	Nein	—	Nur Pakete, die über dieses Interface hereinkommen, z.B. ether1 oder bridge.
Ausgangs-Interface	<code>out-interface</code>	Auswahl aus Live-Interface-Liste des Routers	Nein	—	Nur Pakete, die über dieses Interface hinausgehen, z.B. ether1 oder bridge.
Protokoll	<code>protocol</code>	Auswahl (fest): <code>tcp</code> , <code>udp</code> , <code>icmp</code> , <code>gre</code> , <code>ipsec-esp</code> , <code>ipsec-ah</code>	Nein	—	IP-Protokoll. Leer = alle.
Ziel-Port(s)	<code>dst-port</code>	Text	Nein	—	Nur bei tcp/udp sinnvoll. Einzelner Port (z.B. 80) oder Bereich (z.B. 8000-8100).
Verbindungsstatus	<code>connection-state</code>	Auswahl (fest): <code>new</code> , <code>established</code> , <code>related</code> , <code>invalid</code> , <code>untracked</code>	Nein	—	Status laut Connection-Tracking. "established,related" ist die übliche "schon erlaubte Verbindung"-Regel.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Layer7-Protokoll	layer7-protocol	Text	Nein	—	Name eines vorher unter "/ip firewall layer7-protocol" angelegten Musters (z.B. Erkennung bestimmter Apps). Kostet spürbar CPU, mit Bedacht einsetzen.
Kommentar	comment	Text	Nein	—	Nur zur eigenen Wiedererkennung, ohne technische Wirkung.
Deaktiviert	disabled	Ja/Nein	Nein	no	Regel inaktiv schalten, ohne sie zu löschen.

Firewall: NAT (Portweiterleitung etc.)

NAT-Regeln

RouterOS-Menü: `/ip firewall nat` · REST-Pfad: `ip/firewall/nat`

Übersetzt Adressen — Internetfreigabe (srcnat/masquerade) und Portweiterleitung (dstnat).

srcnat ändert die Absenderadresse ausgehender Pakete (z.B. private LAN-IP → öffentliche WAN-IP).
dstnat ändert die Zieladresse eingehender Pakete (z.B. Anfrage an die WAN-IP auf Port 80 → internen Server auf 192.168.88.10:80 umleiten).

⚠ Achtung: Eine dstnat-Regel (Portweiterleitung) macht ein internes Gerät direkt aus dem Internet erreichbar — nur für Dienste einrichten, die das wirklich sein sollen, und danach den entsprechenden Port in der Filter-Tabelle nicht blockieren.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Chain	chain	Auswahl (fest): srcnat , dstnat	Ja	srcnat	srcnat = Absenderadresse ändern (Internetfreigabe). dstnat = Zieladresse ändern (Portweiterleitung).
Aktion	action	Auswahl (fest): masquerade , src-nat , dst-nat , netmap , redirect , same	Ja	masquerade	masquerade = automatisches NAT über die aktuelle WAN-IP (empfohlen bei wechselnder IP). src-nat = feste NAT-Adresse. dst-nat = Ziel umschreiben (Portweiterleitung). redirect = auf den Router selbst umlenken.
Quell-Adresse	src-address	Text	Nein	—	Einzel-IP oder Netz mit Präfix, z.B. 192.168.88.0/24. Leer = beliebig.
Ziel-Adresse	dst-address	Text	Nein	—	Einzel-IP oder Netz mit Präfix, z.B. 192.168.88.0/24. Leer = beliebig.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Eingangs-Interface	<code>in-interface</code>	Auswahl aus Live-Interface-Liste des Routers	Nein	—	Bei dstnat meist der WAN-Port (woher die Anfrage aus dem Internet kommt), z.B. ether1.
Ausgangs-Interface	<code>out-interface</code>	Auswahl aus Live-Interface-Liste des Routers	Nein	—	Bei srcnat/masquerade meist der WAN-Port, z.B. ether1.
Protokoll	<code>protocol</code>	Auswahl (fest): <code>tcp</code> , <code>udp</code> , <code>icmp</code>	Nein	—	Nötig, damit Ports geprüft werden können.
Ziel-Port der Anfrage	<code>dst-port</code>	Text	Nein	—	Der Port, auf den die Anfrage von außen ankommt, z.B. 8080.
Weiterleiten an (interne IP)	<code>to-addresses</code>	Text	Nein	—	Nur bei dst-nat: die interne IP-Adresse, an die weitergeleitet wird, z.B. 192.168.88.10.
Weiterleiten an (interner Port)	<code>to-ports</code>	Text	Nein	—	Nur bei dst-nat: interner Port, falls abweichend vom Ziel-Port (z.B. extern 8080 → intern 80).
Kommentar	<code>comment</code>	Text	Nein	—	Nur zur Wiedererkennung.
Deaktiviert	<code>disabled</code>	Ja/Nein	Nein	<code>no</code>	Regel inaktiv schalten, ohne sie zu löschen.

Firewall: Mangle (Markierung/QoS-Vorbereitung)

Mangle-Regeln

RouterOS-Menü: `/ip firewall mangle` · REST-Pfad: `ip/firewall/mangle`

Markiert Verbindungen/Pakete zur späteren Weiterverarbeitung (z.B. durch Queues).

Mangle selbst verändert nicht, wie ein Paket behandelt wird — es klebt nur eine Markierung darauf. Erst eine andere Regel (typischerweise eine Queue oder eine Routing-Regel), die genau diese Markierung als Bedingung abfragt, wird dadurch wirksam.

⚠ Achtung: Eine Markierung ohne etwas, das sie auswertet (z.B. keine passende Queue), hat keinerlei sichtbaren Effekt — das ist der häufigste Verwirrungspunkt bei Mangle.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Chain	<code>chain</code>	Auswahl (fest): <code>prerouting</code> , <code>input</code> , <code>forward</code> , <code>output</code> , <code>postrouting</code>	Ja	<code>forward</code>	Verarbeitungspunkt im Router-internen Paketfluss.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Aktion	<code>action</code>	Auswahl (fest): <code>mark-connection</code> , <code>mark-packet</code> , <code>mark-routing</code> , <code>change-mss</code> , <code>change-ttl</code> , <code>set-priority</code> , <code>accept</code> , <code>passthrough</code>	Ja	<code>mark-connection</code>	<code>mark-connection</code> markiert die ganze Verbindung (wirkt auf alle ihre Pakete), <code>mark-packet</code> nur einzelne Pakete.
Name der Verbindungsmarkierung	<code>new-connection-mark</code>	Text	Nein	—	Frei wählbarer Name, den z.B. eine Queue später wiedererkennt.
Name der Paketmarkierung	<code>new-packet-mark</code>	Text	Nein	—	Frei wählbarer Name für die Paketmarkierung.
Weitere Mangle-Regeln noch prüfen	<code>passthrough</code>	Ja/Nein	Nein	<code>yes</code>	Ja (Standard) lässt nachfolgende Mangle-Regeln diese Verbindung noch zusätzlich prüfen.
Quell-Adresse	<code>src-address</code>	Text	Nein	—	Einzel-IP oder Netz mit Präfix, z.B. 192.168.88.0/24. Leer = beliebig.
Ziel-Adresse	<code>dst-address</code>	Text	Nein	—	Einzel-IP oder Netz mit Präfix, z.B. 192.168.88.0/24. Leer = beliebig.
Eingangs-Interface	<code>in-interface</code>	Auswahl aus Live-Interface-Liste des Routers	Nein	—	Nur Pakete, die über dieses Interface hereinkommen, z.B. ether1 oder bridge.
Ausgangs-Interface	<code>out-interface</code>	Auswahl aus Live-Interface-Liste des Routers	Nein	—	Nur Pakete, die über dieses Interface hinausgehen, z.B. ether1 oder bridge.
Protokoll	<code>protocol</code>	Auswahl (fest): <code>tcp</code> , <code>udp</code> , <code>icmp</code>	Nein	—	IP-Protokoll. Leer = alle.
Ziel-Port(s)	<code>dst-port</code>	Text	Nein	—	Nur bei tcp/udp sinnvoll. Einzelner Port (z.B. 80) oder Bereich (z.B. 8000-8100).
Kommentar	<code>comment</code>	Text	Nein	—	Nur zur Wiedererkennung.
Deaktiviert	<code>disabled</code>	Ja/Nein	Nein	<code>no</code>	Regel inaktiv schalten, ohne sie zu löschen.

Firewall: Raw (vor Connection-Tracking)

Raw-Regeln

RouterOS-Menü: `/ip firewall raw` · REST-Pfad: `ip/firewall/raw`

Läuft vor jeder Connection-Tracking-Verarbeitung — meist zur Entlastung oder für DDoS-Grobfilter.

Regeln hier greifen, bevor RouterOS eine Verbindung überhaupt "kennt" (Connection-Tracking). Damit lässt sich z.B. bekannt uninteressanter Verkehr sehr günstig verwerfen, oder gezielt vom Tracking ausnehmen (notrack).

⚠ Achtung: notrack nimmt den betroffenen Verkehr aus dem Connection-Tracking heraus — danach greifen dafür keine Filter-/NAT-Regeln mehr, die sich auf connection-state oder NAT verlassen. Nur gezielt einsetzen.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Chain	<code>chain</code>	Auswahl (fest): <code>prerouting</code> , <code>output</code>	Ja	<code>prerouting</code>	prerouting = eingehende Pakete, bevor der Router sie verarbeitet. output = vom Router selbst erzeugte Pakete.
Aktion	<code>action</code>	Auswahl (fest): <code>accept</code> , <code>drop</code> , <code>notrack</code>	Ja	<code>accept</code>	notrack = von der Connection-Tracking-Verfolgung ausnehmen (siehe Warnhinweis oben).
Quell-Adresse	<code>src-address</code>	Text	Nein	—	Einzel-IP oder Netz mit Präfix, z.B. 192.168.88.0/24. Leer = beliebig.
Ziel-Adresse	<code>dst-address</code>	Text	Nein	—	Einzel-IP oder Netz mit Präfix, z.B. 192.168.88.0/24. Leer = beliebig.
Eingangs-Interface	<code>in-interface</code>	Auswahl aus Live-Interface-Liste des Routers	Nein	—	Nur Pakete, die über dieses Interface hereinkommen, z.B. ether1.
Protokoll	<code>protocol</code>	Auswahl (fest): <code>tcp</code> , <code>udp</code> , <code>icmp</code>	Nein	—	IP-Protokoll. Leer = alle.
Ziel-Port(s)	<code>dst-port</code>	Text	Nein	—	Nur bei tcp/udp sinnvoll. Einzelner Port (z.B. 80) oder Bereich (z.B. 8000-8100).
Kommentar	<code>comment</code>	Text	Nein	—	Nur zur eigenen Wiedererkennung.
Deaktiviert	<code>disabled</code>	Ja/Nein	Nein	<code>no</code>	Regel inaktiv schalten, ohne sie zu löschen.

Firewall: Adress-Listen

Adress-Listen

RouterOS-Menü: `/ip firewall address-list` · REST-Pfad: `ip/firewall/address-list`

Benannte Gruppen von IP-Adressen/Netzen, die Filter/NAT/Mangle-Regeln als Bedingung referenzieren können.

Statt in jeder Regel einzelne IPs aufzuzählen, legst du hier eine benannte Liste an (z.B. "gesperrt" oder "vertraut") und verweist in Filter-/NAT-/Mangle-Regeln per "src-address-list"/"dst-address-list" darauf. Einträge können dauerhaft oder mit Ablaufzeit (timeout) sein.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Listen-Name	list	Text	Ja	—	Frei wählbarer Name, wird in anderen Regeln referenziert, z.B. gesperrt.
Adresse	address	Text	Ja	—	Einzel-IP oder Netz mit Präfix, z.B. 192.168.88.5 oder 10.0.0.0/24.
Ablaufzeit	timeout	Zeitdauer (Tage/Std/Min/Sek, per Stepper)	Nein	—	Optional. Nach dieser Zeit wird der Eintrag automatisch entfernt. Alles auf 0 lassen = bleibt dauerhaft, bis manuell entfernt.
Kommentar	comment	Text	Nein	—	Nur zur eigenen Wiedererkennung.

Queues / Bandbreiten-Steuerung

Einfache Bandbreiten-Begrenzung

RouterOS-Menü: `/queue simple` · REST-Pfad: `queue/simple`

Begrenzt Up-/Download einer IP-Adresse oder eines Netzes.

Reicht für die meisten Heim-/Kleinnetz-Fälle ohne Mangle-Markierungen aus.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	name	Text	Ja	—	Frei wählbar, z.B. limit-gast.
Ziel	target	Text	Ja	—	IP-Adresse oder Netz, das begrenzt wird, mit Präfix, z.B. 192.168.88.50/32.
Max. Bandbreite (Upload/Download)	max-limit	Text	Ja	—	Zwei Werte getrennt durch "/", z.B. 10M/50M (Upload/Download).
Burst-Bandbreite	burst-limit	Text	Nein	—	Optional: kurzzeitig erlaubte höhere Bandbreite, z.B. 15M/60M.
Deaktiviert	disabled	Ja/Nein	Nein	no	Begrenzung inaktiv schalten, ohne sie zu löschen.

Queue-Baum

RouterOS-Menü: `/queue tree` · REST-Pfad: `queue/tree`

Erweiterte, hierarchische Bandbreiten-Steuerung basierend auf Mangle-Markierungen.

Statt einer festen Adresse wirkt ein Queue-Baum-Eintrag auf Verkehr mit einer bestimmten Mangle-Markierung.

⚠ Achtung: Setzt eine passende Mangle-Regel voraus, die genau diese Markierung setzt (siehe Firewall: Mangle) — ohne die greift ein Queue-Baum-Eintrag ins Leere.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Name	name	Text	Ja	—	Frei wählbar, z.B. queue-gast.
Übergeordnet	parent	Text	Ja	—	Ein Interface (z.B. der WAN-Port, etwa ether1) oder der Name eines anderen Queue-Baum-Eintrags.
Paket-/Verbindungsmarkierung	packet-mark	Text	Nein	—	Name der Mangle-Markierung, auf die dieser Eintrag wirkt.
Max. Bandbreite	max-limit	Text	Nein	—	Einzelwert, z.B. 20M.
Deaktiviert	disabled	Ja/Nein	Nein	no	Begrenzung inaktiv schalten, ohne sie zu löschen.

Werkzeuge & Überwachung

Netwatch

RouterOS-Menü: `/tool netwatch` · REST-Pfad: `tool/netwatch`

Überwacht laufend, ob eine Adresse erreichbar ist, und kann bei Statuswechsel ein Skript auslösen.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Zu überwachende Adresse	host	Text	Ja	—	IP-Adresse oder Hostname, ohne Präfix, z.B. 192.168.88.1 oder 8.8.8.8.
Prüf-Intervall	interval	Zeitdauer (Tage/Std/Min/Sek, per Stepper)	Nein	10s	Wie oft die Erreichbarkeit geprüft wird.
Skript bei Erreichbarkeit	up-script	Text	Nein	—	Name eines Skripts unter "Skripte".
Skript bei Nichterreichbarkeit	down-script	Text	Nein	—	Name eines Skripts unter "Skripte".
Deaktiviert	disabled	Ja/Nein	Nein	no	Überwachung inaktiv schalten, ohne sie zu löschen.

E-Mail-Versand (*Einstellungsmenü — genau ein Eintrag, kein Anlegen/Löschen*)

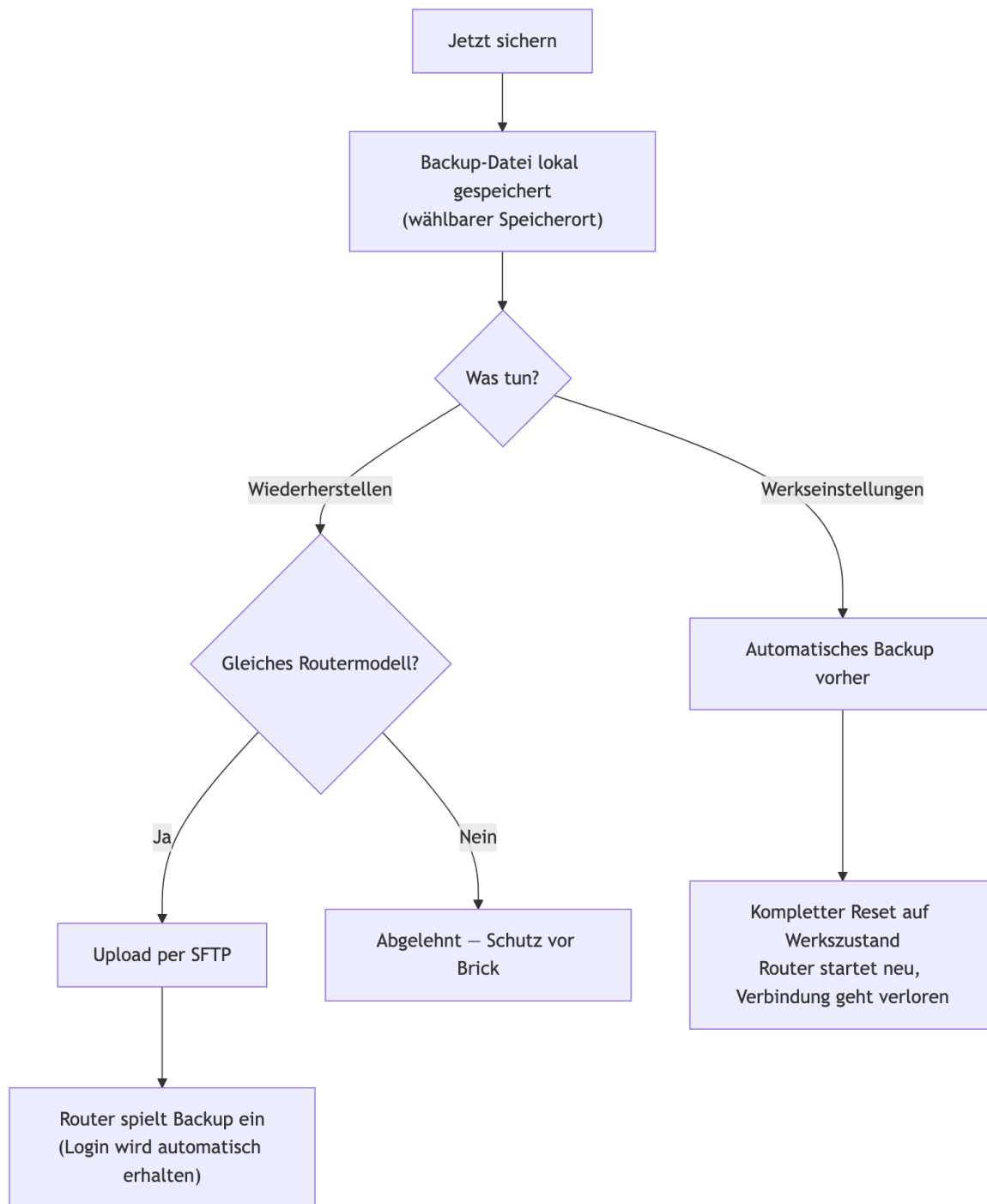
RouterOS-Menü: `/tool e-mail` · REST-Pfad: `tool/e-mail`

Postausgangs-Server, den Scheduler/Netwatch/Skripte für Benachrichtigungen nutzen.

Ein einzelner, geräteweiter Satz Einstellungen — kein Menü mit mehreren Einträgen.

Feld	RouterOS-Parameter	Typ	Pflicht	Standard	Hilfetext
Mailserver-Adresse	address	Text	Ja	—	Hostname oder IP-Adresse des Mailservers, z.B. smtp.gmail.com .
Port	port	Zahl	Nein	—	Meist 587 (STARTTLS) oder 465 (SSL).
Absenderadresse	from	Text	Nein	—	Z.B. router@example.com .
Benutzername	user	Text	Nein	—	Zugangsdaten des Mailservers.
Passwort	password	Text	Nein	—	Zugangsdaten des Mailservers.

6. Sicherungen



- **Jetzt sichern:** „Erstelle eine Sicherung, bevor du Änderungen am Router vornimmst.“ Exportiert die aktuelle Konfiguration.
- **Speicherort:** „Wähle einen eigenen Ordner für neue Sicherungen, z.B. auf einer externen Festplatte oder in iCloud Drive“ / „Standard verwenden“ — „Setzt den Speicherort zurück auf den App-eigenen Standardordner.“
- **Wiederherstellen:** „Diese Sicherung auf den verbundenen Router zurückspielen — nur für exakt dasselbe Routermodell.“ Lädt das Backup über SFTP hoch und spielt es zurück ein; prüft vorher, ob das Backup zum angeschlossenen Routermodell passt (Schutz vor einem „Brick“ durch falsches Modell), und erhält den aktuellen Login automatisch (Backups enthalten grundsätzlich keine Passwörter).
- **Gefahrenzone — Werkseinstellungen wiederherstellen:** „Setzt den Router komplett auf die vom Hersteller mitgelieferte Standardkonfiguration zurück — alle bisherigen Änderungen (Internet,

Heimnetz, VLANs, WLAN, Firewall) gehen verloren. Der Router startet danach neu.“ Vor dem endgültigen Zurücksetzen: „Dies löscht ALLE bisherigen Einstellungen ... Vorher wird zusätzlich automatisch eine Sicherung erstellt.“ Nur für den Notfall gedacht, falls etwas schiefgelaufen ist.

7. English summary

RouterOS Assistant is a native macOS app that sets up and manages MikroTik RouterOS routers through a guided wizard and six tabs: Connect, Setup, Topology, LAN Scanner, Expert, Backups. The app talks to the router over its REST API (preferred, RouterOS ≥ 7.1) or SSH (fallback, and mandatory for backup/update-check/firmware-update, which only exist as CLI commands) — chosen automatically, no configuration needed. A DE/EN toggle button (flag icon) in the toolbar switches the app's language and persists across restarts.

- **Connect:** enter host/username/password; first connection shows a trust-on-first-use dialog for an unknown TLS certificate (REST) or SSH host key (SSH) — for a REST connection, both can appear in sequence, since backup/update-check/firmware always need SSH regardless of the main connection path. "Known Routers" remembers host+username+serial number per device (so two routers sharing MikroTik's factory default don't collide), with a separate keychain entry per device and an editable display name/location field.
- **Setup Wizard:** Simple mode (WAN + one LAN + WLAN + a fixed basic firewall, no VLANs/isolation) or Expert mode (multiple LAN networks each with their own DHCP server, VLANs, network isolation, full firewall control). Every step's fields carry the exact same help text as the German version (see chapter 2) — this summary doesn't duplicate them. Review/Apply shows every command before running it and takes an automatic backup first.
- **Topology:** a live diagram of the router's complete current state — five columns (Interfaces → IP addresses → Pools & DHCP → Routes → Firewall & NAT) connected by real dependency lines. Clicking a node opens **Focus Mode:** a floating popup showing that node's complete connected chain (full transitive closure) neatly re-laid-out, with everything else in the main diagram dimmed — closable via its own X button, a click on empty space, or re-clicking the same node. The right-hand sidebar stays interactive while focused (it's a non-modal overlay, not a system sheet), so a chained node can be edited directly from the popup. Most node kinds are directly editable in place.
- **LAN Scanner:** every device from DHCP leases + ARP, grouped by physical port, with live per-port throughput. Per-device actions: assign/remove a static IP, and network tools (ping/traceroute/DNS lookup run from the router itself over SSH; a port scan runs from this Mac directly). All three result popups share the same fixed header-with-close-button layout as Topology's focus popup and the Expert tab's edit form.
- **Expert:** curated, tooltip-annotated direct access to most RouterOS areas (see chapter 5 for the full field-by-field German reference, extracted verbatim from the app's source), plus a free-form "custom menu path" for anything not yet curated. Every change shows a confirmation dialog with the exact command that will run first.
- **Backups:** create/restore backups over SFTP (model-checked before restoring, to avoid bricking the device with the wrong backup), configurable save location, and a danger-zone factory-reset switch (auto-backs-up first).