Netzwerk

MikroTik Router

- Einfache Konfiguration selbst ohne IP-Adressvergabe über MAC-Adresse per Winbox.
- in Default-Config ist Port-1 = WAN (kein Management)
- **SafeMode** (oben links): Konfiguration wird sofort aktiv, aber nicht zurück geschrieben bis man Safe-Mode beendet. Vorher reicht aus/ein für Urzustand.
- Konfiguration per Winbox, WEB-Gui oder SSH möglich.
- Werksreset: Reset-Taste (ca. 5 sek.) + Power-on oder SSH: /system reset-configuration oder GUI: System -> Reset Configuration

- Stromversorgung: meist 24V, Hohlstecker 5,5x2.1mm (Plus Innen), teilweise auch PoE oder Schraubklemme

RouterOS wird in Lizenzlevel 0 (Demo) bis 6 (Controller) angeboten.
Preise und Funktionen:
https://help.mikrotik.com/docs/display/ROS/RouterOS+license+keys
Alle **Lizenzen**:

- gelten zeitlich unbegrenzt
- beinhalten alle zukünftigen Updates
- können unbegrenzt Interfaces nutzen
- sind für ein Gerät

Default Config (Router Mode)**:**

- WAN Port geschützt durch Firewall, DHCP= on
- Eth.-Ports (außer WAN) sind Mitglied in "LAN Bridge"
- LAN-Bridge IP= 192.168.88.1/24, DHCP-Server und DNS = ON
- WAN Gateway = Ether-1, IP v4 Firewall= ON, NAT= ON, DHCP-Client= ON

Default-Konfig löschen im Terminal: system reset-configuration skip-backup=yes no-default=yes
oder GUI: System -> Reset Configuration -> Haken bei "No default Configuration"

Backup

- Backup per GUI: Files -> Backup (komplett incl. Zertifikate, geht aber nur

optimal auf gleicher Hardware + Firmware)
dann Konfiguration Download
- Backup Plaintext per Terminal: (reines Konfig-Backup ohne Zertifikate, aber Script einfach anpassbar, hardwareübergreifend)
  - /export show-sensitive file=backup.rsc (Scrip Export, dann File Download)
  - /system reset-configuration skip-backup=yes run-after-reset=backup.rsc (Löschen + Import)
  - import backup.rsc (Teil-Import als Ergänzung des Systems)

Einrichtung Best Practice:

- Passwort unter System / Users festlegen (Default: admin / ohne PW, bei manchen WLAN-Accesspoints vorkonf. auf dem Gehäuse)
- Gerätename GUI: System -> Identity oder Terminal: /system identity set name="UKRouter"
- IP unter IP -> Addresses (pro Interface oder Bridges) (IP:x.x.x.y/24, Network: x.x.x.0)
- alle Ports, die "das Gleiche" machen sollen, werden als Bridge zusammen gefasst (jeder Port kann nur zu einer Bridge gehören)
- Internetzugang kann auf beliebigen Port definiert werden
  - DHCP-Client einrichten, DNS, NTP
  - Default-Gateway aktivieren (Default-Route wird automat. erstellt unter IP -> Routes)
  - NAT einrichten (IP -> Firewall -> NAT): Chain: srcnat, Src.Address: [LAN\24], Out.Interface: Internet, Action: masquerade
  - DNS-Weiterleitung: IP -> DNS: Allow Remote Requests ->aktivieren
- Firmware Upgrade unter System / Packages (Channel: upgrade)
- Router auf HTTPS umstellen ([1])
  /certificate
  add name=LocalCA common-name=LocalCA days-valid=36500 key-usage=key-cert-sign,crl-sign
  sign LocalCA
  add name=Webfig common-name=192.168.88.1
  sign Webfig ca=LocalCA
  /ip service
  set www-ssl certificate=Webfig disabled=no
  disable www

- Firewall (IPTables) unter IP -> Firewall ist per Default aus!
- Firewall: Accept Input: DNS(56), HTTP/S, Stateful, PING(ICMP), SNMP(UDP-161/162), NTP(UDP-123) / DROP ALL (siehe Firewall)
- Firewall: Accept Forward: Stateful,
  pro Wireguard-Verbindung: Wireguard Client Src.Address, LAN-Ziel Dst.Address, In.Interface: WIREGUARD, Out.Interface: Lan-Bridge
- Internetzugang für LAN: unter IP -> Firewall -> NAT: Chain:dstnat,

Protocol:tcp, Dst.Port:80,443, In.Interface oder In.Interface List:festlegen(WAN), Action:dst-nat, To-Adresses:192.168.0.24/32

```
/ip firewall filter
add action=accept chain=input comment=HTTP/S dst-port=443 in-interface=all-ethernet protocol=tcp
add action=accept chain=input comment=Stateful connection-state=established,related
add action=accept chain=forward comment=Stateful connection-state=established,related
add action=accept chain=input comment=DNS dst-port=56 protocol=tcp
add action=accept chain=input comment=DNS dst-port=56 protocol=udp
add action=accept chain=input comment=NTP dst-port=123 protocol=udp
add action=accept chain=input comment=SNMP dst-port=161,162 protocol=udp
add action=accept chain=input comment=PING protocol=icmp
add action=accept chain=forward comment=PING protocol=icmp
add action=drop chain=forward comment="DROP ALL"
add action=drop chain=input comment="DROP All"
```

Firewallregeln
"Action: log" nutzen zur Fehlersuche
Regeln können deaktiviert werden (D/E), ohne sie zu löschen.
In den einzelnen Regeln wird der Traffic für jede Regel angezeigt, d.h. man sieht ob die Regel greift.

- **INPUT Regeln** zum Router
- Erlaube alle Antworten zur Verbindung (statefull): Chain: input, Connection State: established+related, Action: accept
- Management-Interface erlauben: Chain: input, In.Interface: festlegen oder Bridge-LAN, Action: accept
- DNS-Server des Routers erlauben: Chain: input, Dst.Address: [LAN-IP des Routers], Protocol: UDP+TCP, Dst.Port: 56(DNS), Action: accept
- ggf. PING vom LAN erlauben: Chain: input, Protocol: icmp, In.Interface: Bridge-LAN, Action: accept

- INPUT DROP REGEL
  Drop All: Chain: input, Action: drop
  Achtung! Dann ist alles zu! Ggf. erst Action: log oder "Safe Mode". Zugang lokal immer über WinBox möglich.

- **FORWARD Regeln** (Traffic durch den Router)
- Erlaube alle Antworten zur Verbindung (statefull): Chain: forward, Connection State: established+related, Action: accept
- Erlaube lokale PCs über HTTP/S zu Internet: Chain: forward, Dest.Address:

NICHT! 192.168.1.0/24 (LAN), Protocol: TCP, Dst.Port: 80,443, In.Interface: LAN-Ports/Bridge, Action: accept
- Bsp: Erlaube PING LAN ins Gäste-LAN: Chain: forward, Protocol: ICMP, In.Interface: Bridge-LAN, Out.Interface: bridge-gast, Action: accept
- Bsp: Erlaube WebServer im Gäste-LAN aus LAN: Chain: forward, Protocol: TCP, Dst.Port:80.443, In.Interface: Bridge-LAN, Out.Interface: bridge-gast, Action: accept (genauso in Gegenrichtung)

- FORWARD DROP REGELn
- Drop All: Chain: forward, Action: drop

- Bsp: Trenne 2 Netze: Chain: forward, Src.Address: 192.168.10.0/24, Dst.Address: 192.168.20.0/24, Action: Accept, dann DROP ALL

Bedienung per Terminal

- Aktuelle Firmware und mögliche Updates ermitteln /system routerboard print
- Update Stable Version: /system package update set channel=current
- Update-Check online: /system package update check-for-updates
- 1.Schritt: RouterOS Update: /system package update download
- 2.Wichtig: Reboot!: /system reboot
- 3.Schritt: Bootlader aktualisieren: /system routerboard upgrade
- 4.Wieder Reboot: /system reboot
- SSH Hostkey neu erstellen: /ip ssh regenerate-host-key
- System-Name setzen: /system identity set name="UKRouter"
- Benutzer Admin neu einrichten:/user set admin name="maxmuster"
- Benutzer Passwort setzen: /passwort

- Routing Table: /ip route print
- Ping: ping <ip>
- komplette Konfig ausgeben: /export verbose
- nur von Default abweichende Konfiguration ausgeben: /export compact

- Export (compact) in Datei: /export file=configuration.rsc (Datei kann dann unter "Files-Download" übertragen werden

- Import Konfigurationsdatei von "Files": /import file=configuration.rsc

DHCP-Server

- IP -> Addresses: feste IP für gewünschtes Interface einrichten (DHCP-Server, Bsp. 192.168.100.1/24)
- IP -> DHCP-Server -> DHCP: DHCP-Server auf o.g. Interface anlegen (geht auch über Assistent: DHCP-Setup)
- IP -> DHCP-Server -> Networks: DHCP-LAN (/24), Gateway (IP aus Schritt 1), DNS, NTP
- IP -> DHCP-Server -> Leases: zeigt die zugewiesenen DHCP-Clients
- IP -> Pool: DHCP-Pool anlegen, Bereich aus dem DHCP-LAN (192.168.100.10-192.168.100.12), mehrere Bereiche möglich
- IP -> DHCP-Server -> DHCP: eben definierten Address Pool angeben

VPN IPSec:

- Verbindung mit Preshare oder Zertifikat
- Ausführliche Beschreibung: VPN IPSec zwischen Lancom und MikroTik Router

VPN Wireguard (ab FW 7):

- Verbindung mit öffentlichem und privatem Key
- Ausführliche Beschreibung: VPN Wireguard Verbindung von MikroTik Routern

VPN L2TP:

- L2TP ohne Zertifikate: https://administrator.de/forum/mikrotik-router-als-vpn-client-1721997934.html#comment-1736463492

VPN OpenVPN:

- OpenVPN mit Zertifikaten: https://blog.effenberger.org/2019/04/21/openvpn-server-unter-mikrotik-routeros-einrichten/

Port based VLAN:

- VLAN erstellen: Interfaces -> VLAN -> VLAN anlegen (VLANs 10 .. 30, Interface=Uplink Port, Trunk-Port)
- Router-IP im VLAN erstellen: IP -> Adresses -> IP-Adresse/24, Netzwerkmaske und Interface auf das entsprechende VLAN Interface einstellen
- ggf. DHCP im VLAN: IP -> Pool -> Bereich definieren (192.168.3.10-192.168.3.20)
- IP -> DHCP-Server: Interface= (vlan-Interface), Adress-Pool: Pool von oben

wählen

VLAN (FW 7.17)
Allgemeines

- Routing Port ether1 (PoE) darf (in den meisten Setups) nicht Mitglied der VLAN-Bridge sein
- Interface "VLAN-Bridge" darf keine direkte IP-Adresse besitzen

Einrichtung

- Bridge -> Bridge -> neue "vlan-bridge" erstellen (VLAN Filterung erstmal AUS)
- Interfaces -> VLAN -> neus VLAN: Name, VLAN-ID, vlan-bridge eintragen (mehrfach für alle VLANs)
- IP -> Addresses -> IP-Adresse für jedes VLAN festlegen (192.168.60.1/32, Network: 192.168.60.0)
- Bridge -> Ports -> NEW:
  - Bridge: vlan-bridge (von oben)
  - VLAN-ID(s) eintragen
  - alle gewünschten VLAN-Ports der VLAN-Bridge zuweisen
    - Untagged Ports: "Admit only untagged and..", PVID entsprechend VLAN
    - Trunk Ports: "Admit All"
- Bridge -> VLANs: Bridge=vlan-bridge, Tagged=vlan-bridge, alle gewünschten VLAN-IDs
- Bridge -> Bridge: VLAN-Filterung für vlan-bridge = EIN

siehe auch:

- VLAN - RouterOS - MikroTik Documentation
- https://administrator.de/tutorial/mikrotik-vlan-konfiguration-ab-routeros-version-6-41-367186.html

WLAN

- CAP - Controlled Access Point (einzelner AP)
  (MikroTik Router mit WLAN-Hardware)
- CAPsMAN - Controlled Access Points Manager
  (kann jeder MikroTik Router, ist nur 1x erforderlich, geht aber auch mehrfach)
- Grundkonfiguration CAP Einzelgerät Wireless:
  - WiFi-Interface: WLAN1 +2: Mode= "ap bridge", Country, Frequenz (auto), SSID, (Indoor), WPA aus
  - Security Profiles: Verschlüsselung und Passwort
- Konfig. als Accesspoint mit DHCP-IP vom LAN:

- Bridge anlegen, LAN + WLAN-Interfaces aufnehmen
- IP -> DHCP-Client auf Bridge konf.

- Konfig. als Accesspoint mit eigenem DHCP-Server:
- Bridges getrennt für LAN und WLAN anlegen
- Einrichtung DHCP auf WLAN-Interface siehe DHCP-Server
- Reset-Button hat 3 Funktionen:
- Hold this button during boot time until LED light starts flashing, release the button to reset RouterOS configuration (total 5 seconds).
- Keep holding for 5 more seconds, LED turns solid, release now to turn on CAP mode. The device will now look for a CAPsMAN server (total 10 seconds).
- Keep holding the button for 5 more seconds until LED turns off, then release it to make the RouterBOARD look for Netinstall servers (total 15 seconds).

CAPsMAN:

- ist als Funktion und Lizenz in (jedem) Routerboard enthalten (Pocket Geräte haben teils kein CAPsMAN)
- zentralisiert die Konfiguration aller APs (Provisioning)
- optional wird auch der Datenverkehr zentral am CAPsMAN per VLAN angebunden (WLAN Control)
- CAPsMAN -> CAP-Interface -> Manager -> CAPsManager =ENABLED, CA+Certificate= auto
- Wireless -> WiFi-Interface -> CAP= ENABLED, Interface= WLANs, Certificate= Request, Discovery Interface festlegen
  Danach ist das WiFI-Interface nur noch vom CAPsMAN zu steuern.

siehe auch

- MikroTik Geräte (Hardware)
- Wireguard mit MikroTik
- ([1]) https://wiki.mikrotik.com/wiki/Manual:Webfig
  https://wiki.mikrotik.com/wiki/Manual:Create_Certificates

Eindeutige ID: #1424
Verfasser: Uwe Kernchen
Letzte Änderung: 2025-02-14 21:56