MikroTik RouterOS 7.x Cheat Sheet

CLI Navigation & Basics

Navigation Commands

Command	Description
`/`	Move to root menu
`..`	Move up one menu level
`/menu/submenu`	Navigate to specific menu
`?`	Display available commands and arguments
`Tab`	Auto-complete commands
`Ctrl+X`	Enable safe mode
`Ctrl+C`	Cancel current operation
`Ctrl+D`	Logout

Universal Commands

Command	Description
`print`	Display items from current menu
`print detail`	Display detailed information
`print where <condition>`	Filter output by condition
`add`	Create new item
`set <id>`	Modify existing item
`remove <id>`	Delete item
`find`	Locate items matching criteria
`edit <id>`	Open text editor for item
`move <id>`	Reorder items in list
`enable <id>`	Enable item
`disable <id>`	Disable item
`comment <id>`	Add comment to item

IP Addressing

IPv4 Address Configuration

```
 # Add IPv4 address
/ip address add address=192.168.88.1/24 interface=ether1

# View all addresses
/ip address print

# View detailed address information
/ip address print detail

# Remove address
/ip address remove [find where address="192.168.88.1/24"]

# Disable address
/ip address disable [find where address="192.168.88.1/24"]
```

IPv6 Address Configuration

```
# Add IPv6 address
/ipv6 address add address=2001:DB8::1/64 interface=ether1 advertise=no

# Add with EUI-64 auto-generation
/ipv6 address add address=2001:DB8::1/64 interface=ether1 eui-64=yes

# View IPv6 addresses
/ipv6 address print
```

Routing

Static Routes

```
# Add static route
/ip route add dst-address=192.168.2.0/24 gateway=172.16.1.2

# Add default route (gateway to internet)
/ip route add gateway=172.16.1.1
/ip route add dst-address=0.0.0.0/0 gateway=172.16.1.1

# View routes
/ip route print

# View only static routes
/ip route print where static

# View routing table (read-only)
/routing route print

# Remove route
/ip route remove [find where dst-address="192.168.2.0/24"]

# Disable hardware offloading for routes
/ip route set [find where static] suppress-hw-offload=yes
```

Interface Configuration

Basic Interface Management

```
# View all interfaces
/interface print

# Enable/disable interface
/interface enable ether1
/interface disable ether1

# Set interface comment
/interface set ether1 comment="WAN Interface"

# Monitor interface traffic
/interface monitor-traffic ether1
```

Bridge Configuration

```
# Create bridge
/interface bridge add name=bridge1

# Add ports to bridge
/interface bridge port add interface=ether2 bridge=bridge1
/interface bridge port add interface=ether3 bridge=bridge1

# View bridge configuration
/interface bridge print
/interface bridge port print

# Enable VLAN filtering on bridge
/interface bridge set bridge1 vlan-filtering=yes
```

VLAN Configuration

```
# Add VLAN interface
/interface vlan add name=vlan10 vlan-id=10 interface=ether1

# Configure bridge VLAN (tagged)
/interface bridge vlan add bridge=bridge1 tagged=ether1 vlan-ids=20

# Configure bridge VLAN (untagged)
/interface bridge vlan add bridge=bridge1 untagged=ether2 vlan-ids=10

# Admit only VLAN-tagged frames
/interface bridge port set [find interface=ether1] frame-types=admit-only-vlan-tagged
```

DHCP

DHCP Server

```
# DHCP server setup wizard
/ip dhcp-server setup

# Manual DHCP server configuration
/ip pool add name=dhcp-pool ranges=192.168.88.10-192.168.88.254
/ip dhcp-server add name=dhcp1 interface=bridge1 address-pool=dhcp-pool disabled=no
/ip dhcp-server network add address=192.168.88.0/24 gateway=192.168.88.1 dns-server=8.8.8.8,8.8.4.4

# View DHCP leases
/ip dhcp-server lease print

# Make lease static
/ip dhcp-server lease make-static [find where address="192.168.88.50"]

# Add static lease
/ip dhcp-server lease add address=192.168.88.100 mac-address=00:11:22:33:44:55 server=dhcp1
```

DHCP Client

```
# Add DHCP client on WAN interface
/ip dhcp-client add disabled=no interface=ether1

# View DHCP client status
/ip dhcp-client print detail

# Release and renew DHCP lease
/ip dhcp-client release [find interface=ether1]
/ip dhcp-client renew [find interface=ether1]
```

Firewall

Firewall Filter Rules

```
# Accept established and related connections
/ip firewall filter add chain=input connection-state=established,related action=accept

# Drop invalid connections
/ip firewall filter add chain=input connection-state=invalid action=drop

# Accept ICMP (ping)
/ip firewall filter add chain=input protocol=icmp action=accept

# Accept from LAN
/ip firewall filter add chain=input in-interface=bridge1 action=accept

# Drop all other input
/ip firewall filter add chain=input action=drop

# Forward established/related
/ip firewall filter add chain=forward connection-state=established,related action=accept

# Drop invalid forward
/ip firewall filter add chain=forward connection-state=invalid action=drop

# View firewall rules
/ip firewall filter print

# Remove rule
/ip firewall filter remove [find where comment="my rule"]

# Disable rule
/ip firewall filter disable [find where comment="my rule"]
```

NAT (Network Address Translation)

```
# Masquerade (source NAT for internet sharing)
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade

# Port forwarding (destination NAT)
/ip firewall nat add chain=dstnat dst-port=80 protocol=tcp in-interface=ether1 action=dst-nat to-
addresses=192.168.88.10 to-ports=80

# View NAT rules
/ip firewall nat print
```

Firewall Mangle

```
# Mark connections
/ip firewall mangle add chain=prerouting src-address=192.168.88.0/24 action=mark-connection new-connection-
mark=lan-conn

# Mark packets
/ip firewall mangle add chain=prerouting connection-mark=lan-conn action=mark-packet new-packet-mark=lan-packet

# View mangle rules
/ip firewall mangle print
```

Address Lists

```
# Add to address list
/ip firewall address-list add list=blacklist address=10.0.0.5

# Add with timeout
/ip firewall address-list add list=whitelist address=192.168.1.100 timeout=1h

# View address lists
/ip firewall address-list print

# Use in firewall rule
/ip firewall filter add chain=input src-address-list=blacklist action=drop
```

Wireless Configuration

Basic Wireless Setup

```
# Create security profile
/interface wireless security-profiles add name=myProfile authentication-types=wpa2-psk mode=dynamic-keys wpa2-pre-shared-key=YourPassword123

# Enable wireless interface
/interface wireless enable wlan1

# Configure as Access Point
/interface wireless set wlan1 mode=ap-bridge ssid="MyNetwork" security-profile=myProfile frequency=2437 band=2ghz-b/g/n channel-width=20/40mhz-XX

# Configure as Station (client)
/interface wireless set wlan1 mode=station ssid="ExistingNetwork" security-profile=myProfile

# Add wireless to bridge
/interface bridge port add interface=wlan1 bridge=bridge1

# View wireless status
/interface wireless print
/interface wireless monitor wlan1

# Registration table (connected clients)
/interface wireless registration-table print
```

DNS

DNS Configuration

```
# Set DNS servers
/ip dns set servers=8.8.8.8,8.8.4.4

# Enable DNS cache
/ip dns set allow-remote-requests=yes

# View DNS cache
/ip dns cache print

# Flush DNS cache
/ip dns cache flush

# Add static DNS entry
/ip dns static add name=router.local address=192.168.88.1

# View DNS settings
/ip dns print
```

PPPoE

PPPoE Client

```
# Add PPPoE client for internet connection
/interface pppoe-client add name=pppoe-out1 interface=ether1 user=username password=password add-default-route=yes use-peer-dns=yes

# View PPPoE status
/interface pppoe-client print detail
/interface pppoe-client monitor pppoe-out1
```

PPPoE Server

```
# Create IP pool for PPPoE clients
/ip pool add name=pppoe-pool ranges=192.168.100.2-192.168.100.254

# Configure PPPoE server
/interface pppoe-server server add service-name=myPPPoE interface=ether2 default-profile=default-encryption

# Add PPPoE user
/ppp secret add name=user1 password=pass1 service=pppoe local-address=192.168.100.1 remote-address=pppoe-pool

# View active PPPoE sessions
/ppp active print
```

User Management

User Accounts

```
# View users
/user print

# Add new user
/user add name=newuser password=SecurePass123 group=full

# Set password for existing user
/user set admin password=NewPassword123

# Change password (interactive)
/password

# Disable default admin account
/user disable admin

# Set user group
/user set newuser group=read

# View user groups
/user group print

# Remove user
/user remove [find name=olduser]
```

System Administration

System Information

```
# View system resources
/system resource print

# View system identity
/system identity print

# Set system identity
/system identity set name=MyRouter

# View RouterBoard info
/system routerboard print

# View system clock
/system clock print

# Set time zone
/system clock set time-zone-name=America/New_York

# View system license
/system license print

# View installed packages
/system package print

# Update packages
/system package update check-for-updates
/system package update download
/system package update install
```

System Logs

```
# View logs
/log print

# View logs with filter
/log print where topics~"firewall"

# Configure logging
/system logging action print
/system logging print

# Add custom log rule
/system logging add topics=firewall action=memory
```

NTP Client

```
# Enable NTP client
/system ntp client set enabled=yes

# Set NTP servers
/system ntp client servers add address=time.google.com
/system ntp client servers add address=pool.ntp.org

# View NTP status
/system ntp client print
```

Configuration Management

Backup & Restore

```
# Create backup (binary)
/system backup save name=backup-2025-11-29

# Create encrypted backup
/system backup save name=backup-secure password=StrongPass encryption=aes-sha256

# Load backup
/system backup load name=backup-2025-11-29 password=StrongPass

# View backup files
/file print where type="backup"
```

Export & Import

```
# Export entire configuration (text)
/export file=config-backup

# Export with verbose (all settings)
/export verbose file=config-full

# Export without sensitive data
/export file=config-safe

# Export specific section
/ip firewall filter export file=firewall-rules

# Import configuration
/import file=config-backup.rsc

# Import with verbose (debugging)
/import file=config-backup.rsc verbose=yes

# Dry-run import (test without applying)
/import file=config-backup.rsc verbose=yes dry-run=yes
```

Reset Configuration

```
# Reset to factory defaults
/system reset-configuration

# Reset but keep users
/system reset-configuration keep-users=yes

# Reset without defaults (blank config)
/system reset-configuration no-defaults=yes

# Reset without creating backup
/system reset-configuration skip-backup=yes
```

Troubleshooting & Diagnostics

Ping

```
# Basic ping
/ping 8.8.8.8

# Ping with count
/ping 8.8.8.8 count=10

# Ping with interval
/ping 8.8.8.8 count=5 interval=50ms

# Ping with size
/ping 8.8.8.8 size=1000

# Ping from specific interface
/ping 8.8.8.8 interface=ether1

# Ping with source address
/ping 8.8.8.8 src-address=192.168.88.1

# MAC address ping
/ping 00:0C:42:72:A1:B0

# Ping specific interface by MAC
/ping 00:11:22:33:44:55%ether1
```

Traceroute

```
# Basic traceroute
/tool traceroute 8.8.8.8

# Traceroute with count
/tool traceroute 8.8.8.8 count=3

# Traceroute from source
/tool traceroute 8.8.8.8 src-address=192.168.88.1
```

Torch (Real-time Traffic Monitor)

```
# Monitor traffic on interface
/tool torch interface=ether1

# Monitor specific protocol
/tool torch interface=ether1 protocol=tcp

# Monitor specific port
/tool torch interface=ether1 port=80

# Monitor with source/destination filter
/tool torch interface=ether1 src-address=192.168.88.0/24
```

Bandwidth Test

```
# Test bandwidth between two MikroTik routers
# On server side:
/tool bandwidth-server set enabled=yes

# On client side:
/tool bandwidth-test 192.168.88.1 duration=30s protocol=tcp

# Test with specific direction
/tool bandwidth-test 192.168.88.1 direction=transmit
/tool bandwidth-test 192.168.88.1 direction=receive
```

Packet Sniffer

```
# Start packet sniffer
/tool sniffer set filter-interface=ether1 streaming-enabled=yes
/tool sniffer start

# Stop sniffer
/tool sniffer stop

# Save capture to file
/tool sniffer set file-name=capture.pcap
```

Connection Tracking

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

# View connections by protocol
/ip firewall connection print where protocol=tcp

# View connections to specific IP
/ip firewall connection print where dst-address~"192.168.88.10"

# Remove connection
/ip firewall connection remove [find where dst-address~"192.168.88.10"]
```

Interface Monitoring

```
# Monitor interface statistics
/interface monitor-traffic ether1

# View interface statistics
/interface print stats

# Reset interface statistics
/interface reset-counters ether1
```

File Management

File Operations

```
# List files
/file print

# View file contents
/file print file=filename.txt

# Remove file
/file remove [find name="oldfile.txt"]

# Rename file (set new name)
/file set [find name="old.txt"] name="new.txt"

# View file size and date
/file print detail
```

Services

Remote Access Services

```
 # View all services
/ip service print

# Disable insecure services
/ip service disable telnet,ftp,www,api

# Enable secure services
/ip service enable ssh,winbox,api-ssl

# Change service port
/ip service set ssh port=2222
/ip service set winbox port=8291

# Restrict access to specific IPs
/ip service set ssh address=192.168.88.0/24
/ip service set winbox address=192.168.88.0/24
```

MAC Server

```
 # Configure MAC server (WinBox/MAC telnet access)
/tool mac-server set allowed-interface-list=LAN

# Configure MAC WinBox server
/tool mac-server mac-winbox set allowed-interface-list=LAN

# Disable MAC discovery on WAN
/tool mac-server set allowed-interface-list=none

# View MAC server settings
/tool mac-server print
```

Neighbor Discovery

```
 # View discovered neighbors
/ip neighbor print

# Disable neighbor discovery on interface
/ip neighbor discovery-settings set discover-interface-list=none
```

Queue & QoS

Simple Queues

```
 # Add simple queue (bandwidth limit)
/queue simple add name=client1 target=192.168.88.10/32 max-limit=10M/10M

# Limit download/upload separately
/queue simple add name=client2 target=192.168.88.20/32 max-limit=5M/20M

# Queue for entire network
/queue simple add name=lan-limit target=192.168.88.0/24 max-limit=50M/50M

# View queues
/queue simple print

# Monitor queue
/queue simple monitor [find name=client1]
```

Scripts & Scheduler

Scripts

```
# Add script
/system script add name=backup-daily source={ /system backup save name=daily-backup }

# Run script
/system script run backup-daily

# View scripts
/system script print
```

Scheduler

```
# Schedule daily backup
/system scheduler add name=daily-backup interval=1d on-event=backup-daily start-time=02:00:00

# Schedule weekly task
/system scheduler add name=weekly-task interval=7d on-event=my-script start-date=2025-11-29

# View scheduled tasks
/system scheduler print
```

Security Hardening

Essential Security Commands

```
# Change default admin password
/user set admin password=VeryStrongPassword123!

# Create new admin and disable default
/user add name=myadmin password=SecurePass123! group=full
/user disable admin

# Restrict services to LAN only
/interface list add name=LAN
/interface list member add list=LAN interface=bridge1
/tool mac-server set allowed-interface-list=LAN
/tool mac-server mac-winbox set allowed-interface-list=LAN
/ip neighbor discovery-settings set discover-interface-list=LAN

# Disable unnecessary services
/ip service disable telnet,ftp,www,api
/ip service set ssh address=192.168.88.0/24
/ip service set winbox address=192.168.88.0/24

# Enable firewall rules (see Firewall section)
# Block brute force SSH attacks
/ip firewall filter add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_blacklist a
ction=drop
/ip firewall filter add chain=input protocol=tcp dst-port=22 connection-state=new add-src-to-address-
list=ssh_blacklist address-list-timeout=1d limit=3,5:packet action=accept

# Enable bandwidth server only on LAN
/tool bandwidth-server set enabled=yes authenticate=yes
```

Common Scenarios

Basic Router Setup (WAN + LAN)

```
 # Create bridge for LAN
/interface bridge add name=bridge1
/interface bridge port add interface=ether2 bridge=bridge1
/interface bridge port add interface=ether3 bridge=bridge1
/interface bridge port add interface=ether4 bridge=bridge1

# Configure LAN IP
/ip address add address=192.168.88.1/24 interface=bridge1

# Configure WAN (DHCP)
/ip dhcp-client add disabled=no interface=ether1

# Or configure WAN (Static)
/ip address add address=203.0.113.10/24 interface=ether1
/ip route add gateway=203.0.113.1
/ip dns set servers=8.8.8.8,8.8.4.4

# Setup DHCP server for LAN
/ip dhcp-server setup
# Follow wizard...

# NAT for internet sharing
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade

# Basic firewall
/ip firewall filter add chain=input connection-state=established,related action=accept
/ip firewall filter add chain=input connection-state=invalid action=drop
/ip firewall filter add chain=input in-interface=bridge1 action=accept
/ip firewall filter add chain=input action=drop
/ip firewall filter add chain=forward connection-state=established,related action=accept
/ip firewall filter add chain=forward connection-state=invalid action=drop
```

Reset & Factory Defaults

```
 # Soft reset (via command)
/system reset-configuration

# Hard reset (physical button)
# Hold reset button during boot until LED starts flashing
# Release button to reset configuration
```

Quick Reference

Common Keyboard Shortcuts

- `Tab` - Auto-complete
- `Ctrl+C` - Cancel operation
- `Ctrl+X` - Safe mode toggle
- `Ctrl+D` - Logout
- `?` - Show help
- `Up/Down Arrow` - Command history

Configuration Best Practices

1. Always set a strong admin password
2. Disable unused services
3. Restrict management access to LAN only
4. Create regular backups
5. Use firewall rules to protect the router
6. Keep RouterOS updated
7. Use strong wireless encryption (WPA2/WPA3)
8. Document your configuration changes

Helpful Tips

- Use `Tab` completion to avoid typing full commands
- Use `print` frequently to verify changes
- Test firewall rules in safe mode (`Ctrl+X`)
- Export configuration before major changes

- Use comments to document rules and settings
- Keep backups in multiple locations

Version Information

- **RouterOS Version:** 7.20.5
- **Document Version:** 1.0
- **Last Updated:** November 29, 2025

Resources & Documentation

- Official Documentation: https://help.mikrotik.com/docs/display/ROS/
- MikroTik Wiki: https://wiki.mikrotik.com/
- MikroTik Forum: https://forum.mikrotik.com/
- Command Line Interface: https://help.mikrotik.com/docs/display/ROS/Command+Line+Interface

---

Note: This cheat sheet covers the most commonly used RouterOS commands. For complete documentation and advanced features, refer to the official MikroTik documentation.