## CYBER DEFENSE CONFIGURATION

This section focuses on configuring RouterOS for defensive cybersecurity purposes. Proper use of firewall rules, connection tracking, logging, and service hardening protects the router and internal network from attacks. Students should understand how to enforce a least-privilege policy, monitor for anomalies, and detect scanning or suspicious behavior at the edge.

### FIREWALL

#### Command Examples

- /ip firewall filter add chain=input connection-state=established,related action=accept
  Permit return traffic from legitimate sessions (stateful firewall).
- /ip firewall filter add chain=input connection-state=invalid action=drop
  Drop malformed or suspicious packets to reduce attack surface.
- /ip firewall filter add chain=input protocol=tcp dst-port=22 action=accept
  Allow SSH management from approved hosts only.
- /ip firewall filter add chain=input src-address-list=blocked action=drop
  Block known malicious IPs.
- /ip firewall address-list add list=blocked address=203.0.113.5
  Add IP to blocklist (dynamic or manual).
- /ip firewall filter add chain=forward protocol=tcp tcp-flags=syn action=log log-prefix="SYN Scan:"
  Log suspicious SYN-only packets, indicative of port scanning.
- /system logging add topics=firewall action=memory
  Enable real-time logging of firewall events for analysis.
- /ip service set winbox disabled=yes
  Disable unnecessary services to reduce attack vectors.
- /ip service set telnet disabled=yes
  Disable Telnet to enforce encrypted management channels.

#### Interpretation

- Stateful firewall rules allow legitimate session return traffic while preventing unsolicited connections.
- Dropping invalid packets mitigates malformed packet attacks and avoids router resource exhaustion.
- Restricting services (SSH, Winbox, Telnet) enforces the principle of least privilege and reduces exposure.
- Maintaining dynamic or manual IP blocklists allows rapid response to observed malicious activity.
- Logging suspicious traffic (e.g., SYN scans) enables early detection of reconnaissance or attempted exploitation.
- Regular monitoring of firewall logs and connection tracking is critical for incident response and threat hunting.
- Cyber defense configurations should be tested in lab environments before deployment to ensure critical services remain reachable.
- Integration with VLANs and bridges ensures segmentation and prevents lateral movement in the network.

## CYBER PENETRATION TESTING

This section focuses on controlled penetration testing using RouterOS diagnostic and monitoring tools. These exercises help students understand potential vulnerabilities, traffic reconnaissance, and network behavior under simulated attack scenarios. Commands shown here should only be used in lab or authorized test environments.

### RECONNAISSANCE & TRAFFIC ANALYSIS

**Command Examples**

- /tool torch interface=LAN
  Monitor live traffic to detect scanning, unusual protocols, or suspicious flows.
- /tool sniffer start interface=LAN filter-ip-address=192.168.1.100
  Capture packets from a target host for analysis.
- /tool sniffer stop
  Stop packet capture.
- /tool sniffer export-file=test-capture.pcap
  Export captured packets for Wireshark analysis.
- /ping 192.168.1.0/24 count=1 interface=LAN
  Perform host discovery on a subnet (ICMP sweep).
- /tool bandwidth-test address=192.168.1.101 duration=10s direction=both
  Test link capacity between router and host, can be used to simulate DoS conditions in lab safely.
- /ip firewall filter add chain=forward src-address=192.168.1.150 action=log log-prefix="PenTest:"
  Log simulated attack traffic for lab exercises.
- /tool traceroute 8.8.8.8 protocol=icmp
  Map network paths to simulate reconnaissance techniques.
- /ip firewall connection print where src-address=192.168.1.150
  Verify connection tracking of simulated penetration traffic.

**Interpretation**

- Torch and sniffer provide real-time visibility into network traffic and potential scanning behavior.
- Packet capture enables detailed forensic review, detection of unauthorized protocols, and payload inspection.
- ICMP sweeps and traceroutes illustrate common network discovery methods used by attackers.
- Bandwidth tests simulate stress on network links without impacting production traffic in a controlled lab.
- Logging simulated penetration traffic allows students to correlate network activity with firewall and connection tracking events.
- Reviewing connection tracking and firewall logs teaches how stateful inspection can detect reconnaissance and exploitation attempts.
- Safe lab penetration testing helps students understand attack surfaces without compromising live systems.
- Combining VLAN segmentation, bridge monitoring, and firewall rules reinforces the importance of layered defenses.

## SYSTEM INTERFACE MANAGEMENT

This section focuses on foundational RouterOS system configuration and physical interface management. Proper identity configuration, interface labeling, time synchronization, and administrative controls establish the baseline for secure deployment and structured network design. Analysts and engineers must ensure device naming, port roles, hardware status, and management access are clearly defined before implementing Layer 2 switching, VLAN segmentation, routing policies, or firewall controls. Failure to properly define system-level parameters often leads to misconfiguration, routing ambiguity, or security exposure later in deployment.

### SYSTEM CONTROL & DEVICE MANAGEMENT

**Command Examples**

- /system identity set name=R1
  Set router hostname for identification in logs, monitoring systems, and multi-device labs.
- /system identity print
  Verify current configured hostname.
- /user print
  Display configured administrative users and privilege levels.
- /user add name=admin2 group=full password=StrongPass123
  Create additional administrative account.
- /system clock print
  Verify system date and time.
- /system clock set time-zone-name=America/New_York
  Set correct time zone for accurate logging and forensics.
- /system backup save name=backup1
  Create binary configuration backup for disaster recovery.
- /export file=config-export
  Export human-readable configuration file.
- /system resource print
  Display CPU, memory, and uptime statistics.
- /system reboot
  Reboot RouterOS safely.
- /interface print
  List all physical and logical interfaces.
- /interface ethernet print
  Display detailed Ethernet port information including speed and link status.
- /interface set ether1 name=WAN
  Rename interface for clarity and role identification.
- /interface set ether2 comment="LAN Port 1"
  Add descriptive comment to interface.
- /interface disable ether2
  Disable interface administratively.
- /interface enable ether2
  Re-enable disabled interface.

**Interpretation**

- Proper device naming prevents confusion in multi-router labs and improves centralized monitoring clarity.
- Maintaining unique administrative accounts improves accountability and audit traceability.
- Time synchronization is critical for correlating logs, identifying beacon intervals, and reconstructing incident timelines.
- Binary backups allow full configuration restoration after hardware failure or misconfiguration.
- Exported configurations support documentation, version control, and peer review.
- Resource monitoring assists in detecting overload conditions, denial-of-service behavior, or hardware constraints.
- Interface visibility confirms hardware detection, negotiated speed, duplex state, and operational status.
- Renaming interfaces clarifies WAN vs LAN role separation and simplifies firewall rule creation.
- Interface comments improve documentation discipline in complex lab or enterprise deployments.
- Administrative shutdown is a controlled method for isolating suspected compromised segments or performing maintenance.
- System-level configuration should always precede Layer 2 and Layer 3 deployment to ensure structural integrity.

## LAYER 2 – BRIDGING VLAN CONFIGURATION

This section addresses Layer 2 switching behavior within RouterOS. Bridges combine multiple interfaces into a single broadcast domain, while VLAN interfaces enable logical segmentation. Correct implementation ensures proper MAC learning, broadcast containment, and traffic separation prior to routing.
Here is your expanded BRIDGE VLAN CONFIGURATION section, written in the same formal technical style and structured for your LaTeX pocket reference format.
You can paste this directly into your document.

### BRIDGE & VLAN CONFIGURATION

**Command Examples**

- /interface bridge add name=LAN
  Create a software switch (bridge) that forms a single Layer 2 broadcast domain.
- /interface bridge set LAN protocol-mode=rstp
  Enable Rapid Spanning Tree Protocol to prevent Layer 2 loops.
- /interface bridge port add bridge=LAN interface=ether2
  Add physical port to the bridge.
- /interface bridge port add bridge=LAN interface=ether3
  Add additional LAN port to same broadcast domain.
- /interface bridge port print
  Display bridge membership and port states.
- /interface bridge host print
  View dynamically learned MAC addresses.
- /interface bridge vlan add bridge=LAN vlan-ids=10 tagged=LAN untagged=ether2
  Define VLAN membership on bridge (RouterOS v7 VLAN filtering model).
- /interface bridge set LAN vlan-filtering=yes
  Enable VLAN filtering on bridge (required for production VLAN enforcement).
- /interface vlan add name=vlan10 vlan-id=10 interface=LAN
  Create Layer 3 VLAN interface associated with bridge.
- /ip address add address=192.168.10.1/24 interface=vlan10
  Assign IP address to VLAN interface for gateway functionality.
- /interface vlan print
  Verify VLAN interface configuration.

**Interpretation**

- A bridge functions as a software-based Layer 2 switch within RouterOS.
- All ports assigned to the same bridge share a common broadcast domain unless segmented by VLAN.
- MAC address learning occurs dynamically and can be inspected for traffic analysis or anomaly detection.
- RSTP reduces the risk of broadcast storms caused by accidental switching loops.
- VLAN filtering enforces tagged and untagged membership rules at the bridge level.
- Untagged ports typically represent access ports for endpoints.
- Tagged interfaces represent trunk ports carrying multiple VLANs.
- VLAN interfaces create logical Layer 3 gateways for segmented networks.
- Each VLAN should receive its own IP subnet to maintain routing separation.
- Without VLAN filtering enabled, VLAN configuration does not enforce traffic isolation.
- Proper VLAN segmentation improves security posture, limits broadcast propagation, and supports structured network design.
- Layer 2 segmentation must be validated before implementing firewall or routing policies to avoid traffic leakage between zones.

## LAYER 3 – IP ADDRESSING DHCP SERVICES

This section covers IP assignment, DHCP provisioning, and gateway configuration. Layer 3 configuration enables inter-network communication and dynamic client addressing. Proper IP structure ensures predictable routing behavior and scalable deployment.

### IP ADDRESSING & DHCP CONFIGURATION

**Command Examples**

- /ip address add address=192.168.1.1/24 interface=LAN
  Assign a Layer 3 address to the LAN interface. The /24 mask (255.255.255.0) defines the broadcast domain and determines usable host range (.1–.254). This IP typically functions as the default gateway for client devices.
- /ip address print
  Display all configured interface IP addresses. Useful for verifying subnet masks, interface bindings, and identifying overlapping networks or misconfigurations.
- /ip pool add name=pool1 ranges=192.168.1.100-192.168.1.200
  Create a dynamic allocation pool for DHCP clients. The defined range establishes the allowable lease boundaries and should exclude static infrastructure devices (servers, printers, management IPs).
- /ip dhcp-server add name=dhcp1 interface=LAN address-pool=pool1
  Instantiate a DHCP service bound to the LAN interface using the defined address pool. The server will listen for broadcast DHCPDISCOVER messages on this interface only.
- /ip dhcp-server network add address=192.168.1.0/24 gateway=192.168.1.1
  Define network parameters distributed to clients, including default gateway. Additional parameters such as DNS servers and domain names can also be defined here.
- /ip dhcp-server lease print
  Display active and expired leases. Provides visibility into assigned IP addresses, MAC addresses, lease durations, and client hostnames for asset tracking.

**Interpretation**

- The interface IP address serves as the default gateway, enabling inter-subnet routing and external connectivity.
- Subnet mask selection defines broadcast scope and directly impacts network scalability and traffic containment.
- DHCP automates endpoint configuration, reducing administrative overhead and minimizing manual addressing errors.
- Address pools must be carefully scoped to avoid conflicts with statically assigned infrastructure devices.
- Lease tables provide valuable operational intelligence for identifying unauthorized devices, tracking endpoint behavior, and assisting with incident response.
- Proper DHCP configuration supports centralized control of DNS distribution, gateway enforcement, and network policy consistency.
- Monitoring lease churn rates can help detect abnormal activity such as rogue devices or automated scanning behavior.
- Segregating DHCP services by VLAN enhances security and limits broadcast domain exposure.
- Poor subnet design can create overlapping routes, asymmetric routing, and broadcast storms that degrade network performance.

## ROUTING

This section focuses on packet forwarding decisions, default route configuration, and traffic filtering. RouterOS evaluates packets through routing tables and firewall chains before transmission. Proper NAT and filter configuration enables secure internet access and internal traffic control.

### ROUTING

#### Command Examples

- /ip route add dst-address=0.0.0.0/0 gateway=ISP-Gateway-IP
  Add default route directing all unknown traffic toward upstream gateway.
- /ip route add dst-address=10.10.10.0/24 gateway=192.168.1.2
  Add static route to remote network via next-hop router.
- /ip route print detail
  Display routing table with administrative distance and route status.
- /ip route print where active
  Display only active routes currently used for forwarding decisions.
- /ip firewall nat add chain=srcnat out-interface=WAN action=masquerade
  Enable dynamic source NAT for outbound internet access.
- /ip firewall nat add chain=dstnat protocol=tcp dst-port=80 action=dst-nat to-addresses=192.168.1.100
  Forward inbound TCP port 80 traffic to internal server.
- /ip firewall filter add chain=input connection-state=established,related action=accept
  Permit return traffic for existing sessions.
- /ip firewall filter add chain=input connection-state=invalid action=drop
  Drop malformed or out-of-state packets.
- /ip firewall filter add chain=input protocol=tcp dst-port=22 action=accept
  Allow SSH management access.
- /ip firewall filter add chain=input action=drop
  Drop all other inbound traffic (default deny).
- /ip dns set servers=8.8.8.8 allow-remote-requests=yes
  Enable DNS forwarding for internal clients.
- /ip firewall connection print
  View active connection tracking table.

#### Interpretation

- The routing table determines packet forwarding decisions based on longest-prefix match.
- The default route (0.0.0.0/0) handles all traffic not explicitly defined by more specific routes.
- Administrative distance influences route preference when multiple routes to the same destination exist.
- Static routes provide predictable path control in lab and enterprise environments.
- Source NAT (masquerade) dynamically translates private addresses to the public WAN IP.
- Destination NAT enables port forwarding and internal service exposure.
- Connection tracking maintains state awareness for TCP, UDP, and ICMP sessions.
- Established/related rules are essential for stateful firewall behavior.
- Invalid packet drops reduce attack surface and prevent malformed packet exploitation.
- A default drop rule enforces a least-privilege security posture.
- The input chain protects the router itself.
- The forward chain protects internal network traffic traversing the router.
- DNS forwarding allows internal hosts to resolve external domain names without direct exposure.
- Firewall processing order follows RouterOS packet flow: RAW → MANGLE → DST-NAT → ROUTING → FILTER → SRC-NAT.
- Misordered firewall rules may unintentionally permit or block traffic.
- Proper routing and firewall configuration should always be validated using ping, traceroute, and connection tracking inspection.

## TROUBLESHOOTING & TRAFFIC ANALYSIS

This section provides diagnostic commands used for connectivity verification and live traffic inspection. Effective troubleshooting requires validation of routing decisions, packet flow direction, and interface activity.

### DIAGNOSTIC COMMANDS

**Command Examples**

- /ping 8.8.8.8
  Test Layer 3 reachability to a remote host. Useful for verifying default route, gateway connectivity, and basic ICMP response. Can also measure latency and packet loss.
- /ping 192.168.1.1 count=10 size=1400
  Perform targeted ping with custom packet size and count for MTU testing or connectivity troubleshooting.
- /tool traceroute 8.8.8.8
  Trace the network path from the router to the destination. Identifies each hop, potential bottlenecks, or misrouted traffic.
- /tool traceroute 8.8.8.8 protocol=icmp
  Force ICMP-based traceroute to bypass devices that may block UDP/TCP probes.
- /tool torch interface=WAN
  Monitor live traffic on a specific interface in real time. Shows source/destination IPs, ports, protocol, and bandwidth usage. Useful for detecting anomalies or verifying firewall/NAT rules.
- /tool torch interface=LAN port=80
  Filter torch output to a specific service or port to observe HTTP traffic in real time.
- /ip route print detail
  Verify routing table, next-hop addresses, administrative distances, and active status. Essential to ensure correct packet forwarding.
- /ip route print where active
  Display only active routes currently in use, helping identify route conflicts or redundant paths.
- /interface monitor-traffic ether1
  Check live traffic statistics per interface including Tx/Rx rate, packet errors, and drops.
- /ip firewall connection print
  Inspect the connection tracking table to verify stateful firewall behavior, NAT translations, and active sessions.

**Interpretation**

- Ping confirms network reachability and validates Layer 3 connectivity, including proper default gateway functionality.
- Traceroute allows identification of upstream devices and routing anomalies, useful for debugging multi-hop networks.
- Torch provides granular real-time insight into traffic patterns, helping detect unusual traffic, misrouted packets, or performance bottlenecks.
- Monitoring traffic per interface identifies errors, collisions, or bandwidth saturation impacting network performance.
- Connection tracking inspection confirms NAT translation behavior and firewall enforcement, useful in diagnosing asymmetric routing or blocked sessions.
- Using ping with packet size variations can reveal MTU issues causing fragmentation or dropped packets.
- Combining torch with port filters enables focused observation of critical services or suspicious activity.
- Routing table review ensures packets are being sent along intended paths and validates static or dynamic route configuration.
- Regular diagnostic checks are essential for both lab exercises and production troubleshooting to validate configuration changes and detect anomalies early.

## CONFIGURATION MANAGEMENT

This section focuses on viewing, saving, and restoring MikroTik RouterOS configurations. Unlike some other platforms, RouterOS applies configuration changes immediately (running config) and requires explicit saving for persistence across reboots. Understanding export, backup, and import mechanisms is essential for both lab exercises and production network administration.

### VIEWING

#### Command Examples

- /export
  Display all currently active configuration in a human-readable format. Useful for verification or quick documentation.
- /export file=config-current
  Save running configuration as a text file (‘config-current.rsc‘) that can be downloaded, version-controlled, or edited offline.
- /system backup save name=backup1
  Create a binary backup of the current configuration (‘backup1.backup‘) that includes passwords, user accounts, and system settings. This is recommended for full restore scenarios.
- /system backup print
  View all existing binary backups stored on the device.
- /import file-name=config-current.rsc
  Import a previously exported text configuration to restore settings. Useful for lab resets or replicating configurations across devices.
- /system backup load name=backup1.backup
  Restore a previously saved binary backup for full configuration recovery.

#### Interpretation

- RouterOS applies changes immediately (running config); unsaved changes are lost on reboot.
- Text-based exports (‘/export‘) are human-readable, editable, and ideal for documentation, training, and partial restores.
- Binary backups (‘/system backup save‘) preserve passwords, credentials, and proprietary settings not visible in text exports.
- Always export or backup after making significant configuration changes to ensure persistence and recovery capability.
- Restoring configurations allows for rapid lab resets, disaster recovery, or cloning a standard configuration to multiple routers.
- Differentiating between export and backup helps avoid accidental overwrites or missing sensitive information.
- Use descriptive filenames and maintain a repository of exports/backups to support change tracking and version control.