MikroTik Router Setup Guide with Multiple WAN Connections (SD-WAN) and VLAN Configuration

This guide will help you configure your MikroTik router with the following features:

- **Introduction to Multiple WAN Connections (SD-WAN)**
- **Three WAN Connections**: Fiber (Primary), 5G, and Starlink
- **Load Balancing and Failover**: Prioritize Fiber connection
- **Three VLANs**: Home, Guest, and IoT
- **Firewall Rules**: Optimized for streaming and gaming
- **Traffic Prioritization**: Using Quality of Service (QoS)

Prerequisites

- **MikroTik Router**: Ensure your device supports the necessary features (e.g., RB4011, CCR series).
- **Access to Router Management Interface**: Use Winbox or WebFig to configure the router.
- **WAN Connections**: Have your Fiber, 5G, and Starlink connections physically connected to the router.
- **Basic Network Knowledge**: Familiarity with network configurations and terms.

Step-by-Step Setup

Step 1: Access the MikroTik Router

1. **Connect to the Router**: Use an Ethernet cable to connect your computer to the router.
2. **Open Winbox**: Download from the MikroTik website if you haven't already.

3. **Login**:
   - **MAC Address**: Use the MAC address to connect if the IP is not set.
   - **Default Username**: `admin`
   - **Default Password**: *(Leave blank initially; change immediately for security)*

Step 2: Configure WAN Interfaces

Identify the interfaces connected to your WAN connections.

Assign Names to WAN Interfaces

1. **Fiber Connection (Primary)**
   - **Interface**: e.g., `ether1`
   - **Name**: `WAN_Fiber`
2. **5G Connection**
   - **Interface**: e.g., `ether2`
   - **Name**: `WAN_5G`
3. **Starlink Connection**
   - **Interface**: e.g., `ether3`
   - **Name**: `WAN_Starlink`

Configure IP Addresses for WAN Interfaces

1. **Go to**: `IP > DHCP Client`
2. **Add DHCP Client** for each WAN interface:
   - **Interface**: `WAN_Fiber`
   - **Use Peer DNS**: Yes
   - **Add Default Route**: No *(We'll set routes manually)*
   - Repeat for `WAN_5G` and `WAN_Starlink`

Step 3: Configure Load Balancing and Failover

We'll set up routing rules to prioritize the Fiber connection and use the 5G and Starlink as backups.

Set Default Routes with Different Distances

1. **Go to**: `IP > Routes`
2. **Add Route for Fiber Connection**
   - **Destination Address**: `0.0.0.0/0`
   - **Gateway**: Select the gateway provided by the DHCP client on `WAN_Fiber` (e.g., `WAN_Fiber` interface)
   - **Distance**: `1` *(Primary connection)*
3. **Add Route for 5G Connection**
   - **Destination Address**: `0.0.0.0/0`

- **Gateway**: Select the gateway from `WAN_5G`
- **Distance**: `2`

4. **Add Route for Starlink Connection**
   - **Destination Address**: `0.0.0.0/0`
   - **Gateway**: Select the gateway from `WAN_Starlink`
   - **Distance**: `3`

Set Up Check Gateway

1. **Edit Each Route**: Enable `Check Gateway` with `ping` to monitor the connection.
   - This allows the router to detect when a connection is down and automatically switch to the next available connection.

Step 4: Configure VLANs

Create VLAN Interfaces

1. **Go to**: `Interfaces`
2. **Click**: `+` (Add New Interface)
   - **Type**: `VLAN`

Home VLAN

- **Name**: `VLAN_Home`
- **VLAN ID**: `10`
- **Interface**: Physical interface connected to your switch (e.g., `ether5`)

Guest VLAN

- **Name**: `VLAN_Guest`
- **VLAN ID**: `20`
- **Interface**: `ether5`

IoT VLAN

- **Name**: `VLAN_IoT`
- **VLAN ID**: `30`
- **Interface**: `ether5`

Configure Bridge Interface

If using multiple VLANs on a single physical interface, it's good practice to use a bridge.

1. **Go to**: `Bridge`
2. **Add New Bridge**
   - **Name**: `BR_LAN`

3. **Add Ports to Bridge**
   - **Go to**: `Bridge > Ports`
   - **Add**: `ether5` to `BR_LAN`
   - **Add**: `VLAN_Home`, `VLAN_Guest`, `VLAN_IoT` to `BR_LAN`

Assign IP Addresses to VLAN Interfaces

1. **Go to**: `IP > Addresses`
2. **Add New Address**

Home VLAN

- **Address**: `192.168.10.1/24`
- **Interface**: `VLAN_Home`

Guest VLAN

- **Address**: `192.168.20.1/24`
- **Interface**: `VLAN_Guest`

IoT VLAN

- **Address**: `192.168.30.1/24`
- **Interface**: `VLAN_IoT`

Step 5: Configure DHCP Servers for Each VLAN

1. **Go to**: `IP > DHCP Server`
2. **Click**: `DHCP Setup`

Home VLAN DHCP

- **Interface**: `VLAN_Home`
- **Follow the prompts** to set:
  - **Address Pool**: `192.168.10.2-192.168.10.254`
  - **Gateway**: `192.168.10.1`
  - **DNS Servers**: Use your preferred DNS (e.g., `8.8.8.8`)

Guest VLAN DHCP

- **Interface**: `VLAN_Guest`
- **Address Pool**: `192.168.20.2-192.168.20.254`
- **Gateway**: `192.168.20.1`
- **DNS Servers**: `8.8.8.8`

IoT VLAN DHCP

- **Interface**: `VLAN_IoT`
- **Address Pool**: `192.168.30.2-192.168.30.254`
- **Gateway**: `192.168.30.1`
- **DNS Servers**: `8.8.8.8`

Step 6: Configure Firewall Rules

MikroTik uses a default firewall configuration; we'll modify it to suit our needs.

Enable NAT for Internet Access

1. **Go to**: `IP > Firewall > NAT`
2. **Add New NAT Rule**
   - **Chain**: `srcnat`
   - **Out Interface List**: `WAN` *(We'll create an interface list for WAN interfaces)*
   - **Action**: `masquerade`

Create Interface List for WAN

1. **Go to**: `Interfaces > Interface List`
2. **Add New List**
   - **Name**: `WAN`
   - **Add Interfaces**: `WAN_Fiber`, `WAN_5G`, `WAN_Starlink`

Allow Traffic from VLANs to WAN

1. **Go to**: `IP > Firewall > Filter Rules`
2. **Add New Rule**
   - **Chain**: `forward`
   - **Src. Address**: `192.168.10.0/24`, `192.168.20.0/24`, `192.168.30.0/24`
   - **Out Interface List**: `WAN`
   - **Action**: `accept`

Drop Inter-VLAN Traffic

1. **Add New Rule**
   - **Chain**: `forward`
   - **Src. Address List**: Create an address list for your VLAN subnets.
     - **Name**: `VLAN_Networks`
     - **Addresses**: `192.168.10.0/24`, `192.168.20.0/24`, `192.168.30.0/24`
   - **Dst. Address List**: `VLAN_Networks`
   - **Action**: `drop`
   - **Place this rule before the rule that accepts established/related traffic.**

Allow Established and Related Traffic

1. **Ensure you have a rule to accept established and related connections**
   - **Chain**: `forward`
   - **Connection State**: `established, related`
   - **Action**: `accept`

Drop Invalid Traffic

1. **Add Rule**
   - **Chain**: `forward`
   - **Connection State**: `invalid`
   - **Action**: `drop`

Step 7: Configure Traffic Prioritization (QoS)

We'll use **Simple Queues** to prioritize gaming and streaming traffic.

Identify Gaming and Streaming Traffic

1. **Go to**: `IP > Firewall > Mangle`
2. **Add New Rule for Gaming Traffic**
   - **Chain**: `forward`
   - **Protocol**: Select protocols used by games (e.g., TCP/UDP ports)
   - **Dst. Port**: Add known gaming ports
   - **Action**: `mark-packet`
   - **New Packet Mark**: `Gaming_Traffic`
   - **Passthrough**: `yes`
3. **Add New Rule for Streaming Traffic**
   - **Chain**: `forward`
   - **Dst. Address List**: Create an address list for streaming services (e.g., Netflix IP ranges)
   - **Action**: `mark-packet`
   - **New Packet Mark**: `Streaming_Traffic`
   - **Passthrough**: `yes`

Create Simple Queues

1. **Go to**: `Queues > Simple Queues`

Gaming Traffic Queue

- **Name**: `Priority_Gaming`
- **Target**: `192.168.10.0/24` *(Assuming gaming devices are on the Home VLAN)*
- **Max Limit**: Set according to your bandwidth
- **Limit At**: Set minimum guaranteed bandwidth
- **Priority**: `1` *(Highest priority)*
- **Advanced Tab**:

- **Packet Marks**: `Gaming_Traffic`

Streaming Traffic Queue

- **Name**: `Priority_Streaming`
- **Target**: `192.168.10.0/24`
- **Max Limit**: Set according to your bandwidth
- **Limit At**: Set minimum guaranteed bandwidth
- **Priority**: `2`
- **Advanced Tab**:
  - **Packet Marks**: `Streaming_Traffic`

Step 8: Secure the Router

Change the Default Admin Password

1. **Go to**: `System > Users`
2. **Edit**: `admin`
3. **Set a strong password**

Disable Unnecessary Services

1. **Go to**: `IP > Services`
2. **Disable** services you don't use (e.g., FTP, Telnet)
3. **Ensure Winbox and SSH are secured**

Enable HTTPS for WebFig

1. **Go to**: `IP > Services`
2. **Enable**: `www-ssl`
3. **Disable**: `www` (HTTP)

Step 9: Test the Configuration

- **VLAN Connectivity**: Connect devices to each VLAN and ensure they receive the correct IP addresses.
- **Internet Access**: Verify that devices can access the internet.
- **Failover**: Disconnect the Fiber connection to test if traffic fails over to 5G or Starlink.
- **Load Balancing**: Monitor traffic using `Tools > Torch` to see if load balancing works as expected.
- **QoS Effectiveness**: Use bandwidth-intensive applications to test if gaming and streaming traffic are prioritized.

Additional Tips

- **Regular Backups**: Go to `Files`, select your configuration file, and download it to your computer.
- **Firmware Updates**: Check `System > Packages` for updates and upgrade to the latest stable version.
- **Monitor Traffic**: Use `Tools > Graphing` or `Queues > Queue Tree` to monitor bandwidth usage.
- **Logs**: Check `Log` for any errors or unusual activity.

By following this guide, you should have a MikroTik router configured with multiple WAN connections, VLAN segmentation, firewall rules, and QoS prioritization. The Fiber connection is set as the primary WAN, with 5G and Starlink serving as backup connections to ensure uninterrupted internet access.

Note: MikroTik routers are highly versatile but can be complex. Always make sure to back up your configuration before making significant changes, and consult the MikroTik Wiki or Forums if you encounter issues.

Revision #1
Created 11 October 2024 05:12:04 by Jarryd
Updated 11 October 2024 05:13:25 by Jarryd