Home Office Network Setup Guide

Below is a MikroTik configuration tailored to your requirements.

This configuration includes:

- **4 VLANs**: Home (VLAN 10), Office (VLAN 20), Guest (VLAN 30), and IoT (VLAN 40).
- **Subnetting**: Each VLAN uses the `10.x.x.x/24` subnet, with the subnet identifier matching the VLAN ID.
- **Firewall Rules**: Home and Office VLANs can access the IoT VLAN; IoT and Guest VLANs are isolated from other VLANs.
- **Security Enhancements**: Hardened router security with essential services only and restricted management access.

1. Bridge and VLAN Setup

Create a Bridge Interface with VLAN Filtering

```
/interface bridge
add name=bridge1 vlan-filtering=yes
```

Add Physical Ports to the Bridge

Assuming `ether2` to `ether5` are your LAN ports:

```
/interface bridge port
add bridge=bridge1 interface=ether2 pvid=10
add bridge=bridge1 interface=ether3 pvid=20
add bridge=bridge1 interface=ether4 pvid=30
add bridge=bridge1 interface=ether5 pvid=40
```

Define VLANs on the Bridge

```
/interface bridge vlan
add bridge=bridge1 tagged=bridge1 untagged=ether2 vlan-ids=10
add bridge=bridge1 tagged=bridge1 untagged=ether3 vlan-ids=20
add bridge=bridge1 tagged=bridge1 untagged=ether4 vlan-ids=30
add bridge=bridge1 tagged=bridge1 untagged=ether5 vlan-ids=40
```

Create VLAN Interfaces

```
/interface vlan
add interface=bridge1 name=VLAN10 vlan-id=10
add interface=bridge1 name=VLAN20 vlan-id=20
add interface=bridge1 name=VLAN30 vlan-id=30
add interface=bridge1 name=VLAN40 vlan-id=40
```

---

2. IP Addressing

Assign IP addresses to each VLAN interface, matching the subnet with the VLAN ID:

```
/ip address
add address=10.10.10.1/24 interface=VLAN10 network=10.10.10.0
add address=10.10.20.1/24 interface=VLAN20 network=10.10.20.0
add address=10.10.30.1/24 interface=VLAN30 network=10.10.30.0
add address=10.10.40.1/24 interface=VLAN40 network=10.10.40.0
```

---

3. DHCP Server Configuration

Create IP Pools for Each VLAN

```
/ip pool
add name=dhcp_pool_vlan10 ranges=10.10.10.10-10.10.10.254
add name=dhcp_pool_vlan20 ranges=10.10.20.10-10.10.20.254
add name=dhcp_pool_vlan30 ranges=10.10.30.10-10.10.30.254
add name=dhcp_pool_vlan40 ranges=10.10.40.10-10.10.40.254
```

Set Up DHCP Servers

```
/ip dhcp-server
add address-pool=dhcp_pool_vlan10 interface=VLAN10 lease-time=12h name=dhcp_vlan10
add address-pool=dhcp_pool_vlan20 interface=VLAN20 lease-time=12h name=dhcp_vlan20
add address-pool=dhcp_pool_vlan30 interface=VLAN30 lease-time=12h name=dhcp_vlan30
add address-pool=dhcp_pool_vlan40 interface=VLAN40 lease-time=12h name=dhcp_vlan40
```

Define DHCP Networks

```
/ip dhcp-server network
add address=10.10.10.0/24 dns-server=8.8.8.8,8.8.4.4 gateway=10.10.10.1
```

```
add address=10.10.20.0/24 dns-server=8.8.8.8,8.8.4.4 gateway=10.10.20.1
add address=10.10.30.0/24 dns-server=8.8.8.8,8.8.4.4 gateway=10.10.30.1
add address=10.10.40.0/24 dns-server=8.8.8.8,8.8.4.4 gateway=10.10.40.1
```

---

4. Firewall Configuration

Basic Firewall Rules

- Accept established and related connections.
- Drop invalid packets.

```
/ip firewall filter
add chain=forward connection-state=established,related action=accept
add chain=forward connection-state=invalid action=drop
```

Inter-VLAN Communication Rules

- **Allow** Home and Office VLANs to access the IoT VLAN.

```
add chain=forward src-address=10.10.10.0/24 dst-address=10.10.40.0/24 action=accept
add chain=forward src-address=10.10.20.0/24 dst-address=10.10.40.0/24 action=accept
```

- **Allow** Home and Office VLANs to access the internet.

```
add chain=forward src-address=10.10.10.0/24 action=accept out-interface-list=WAN
add chain=forward src-address=10.10.20.0/24 action=accept out-interface-list=WAN
```

Restrict IoT and Guest VLANs

- **Drop** traffic from IoT VLAN to other VLANs.

```
add chain=forward src-address=10.10.40.0/24 dst-address=10.10.10.0/24 action=drop
add chain=forward src-address=10.10.40.0/24 dst-address=10.10.20.0/24 action=drop
add chain=forward src-address=10.10.40.0/24 dst-address=10.10.30.0/24 action=drop
```

- **Drop** traffic from Guest VLAN to other VLANs.

```
add chain=forward src-address=10.10.30.0/24 dst-address=10.10.10.0/24 action=drop
add chain=forward src-address=10.10.30.0/24 dst-address=10.10.20.0/24 action=drop
add chain=forward src-address=10.10.30.0/24 dst-address=10.10.40.0/24 action=drop
```

- **Allow** IoT and Guest VLANs to access the internet.

```
add chain=forward src-address=10.10.40.0/24 action=accept out-interface-list=WAN
add chain=forward src-address=10.10.30.0/24 action=accept out-interface-list=WAN
```

Drop All Other Traffic

```
add chain=forward action=drop
```

---

5. NAT Configuration

Ensure that all VLANs can access the internet:

```
/ip firewall nat
add chain=srcnat out-interface-list=WAN action=masquerade
```

---

6. Security Hardening

Restrict Router Access

- Allow management access only from Home and Office VLANs.

```
/ip firewall filter
add chain=input connection-state=established,related action=accept
add chain=input connection-state=invalid action=drop
add chain=input src-address=10.10.10.0/24 action=accept
add chain=input src-address=10.10.20.0/24 action=accept
add chain=input action=drop
```

Disable Unnecessary Services

```
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set ssh disabled=yes
set api disabled=yes
set api-ssl disabled=yes
set winbox address=10.10.10.0/24,10.10.20.0/24
```

> **Note:** Only Winbox is enabled for management, and access is restricted to Home and Office VLANs.

Set Strong Passwords

Ensure the router's admin password is strong:

```
/user set 0 name=admin password=YourStrongPassword
```

Replace `YourStrongPassword` with a strong, unique password.

Additional Security Measures

- **System Updates**: Regularly update your router's firmware to the latest stable version.
- **Backup Configuration**: Keep backups of your configuration in a secure location.
- **Logging**: Enable system logging for monitoring.

---

7. Final Notes

- **Adjust Interface Names**: Replace `ether2`, `ether3`, etc., with your actual interface names if they differ.
- **WAN Interface**: Ensure your WAN interface is added to the `WAN` interface list.

```
/interface list
add name=WAN
/interface list member
add interface=ether1 list=WAN
```

Assuming `ether1` is your WAN interface.

- **DNS Servers**: You can replace `8.8.8.8,8.8.4.4` with your preferred DNS servers.
- **Safe Mode**: When applying configurations, use Safe Mode in Winbox or CLI to prevent lockouts.

By implementing this configuration, you'll have a secure and segmented network that meets your home office needs.

Revision #4
Created 13 September 2024 05:11:53 by Jarryd
Updated 26 October 2024 08:53:09 by Jarryd