VLAN Lab Quick Implementation Plan - Group 1A-4

Objective

Implement IEEE 802.1Q VLANs to separate Host1/2 (VLAN 10) from Host3/RPi3 (VLAN 20) using tagged VLANs on Router 1.

Step 1: Router 1 Initial Setup

```
# Enable IPv6 on external interface
sudo sysctl -w net.ipv6.conf.all.forwarding=1
sudo ip link set enp1s0f1 up

# Load VLAN module
sudo modprobe 8021q
```

Step 2: Create VLAN Interfaces on Router 1

```
# Create and configure VLAN interfaces
sudo ip link add link enp1s0f0 name enp1s0f0.10 type vlan id 10
sudo ip link add link enp1s0f0 name enp1s0f0.20 type vlan id 20

# Bring up interfaces
sudo ip link set enp1s0f0 up
sudo ip link set enp1s0f0.10 up
sudo ip link set enp1s0f0.20 up

# Assign IPv6 addresses (using ULA for internal network)
sudo ip -6 addr add fd00:1:2:10::1/64 dev enp1s0f0.10
sudo ip -6 addr add fd00:1:2:20::1/64 dev enp1s0f0.20
```

Note: *Using ULA (fd00::/8) instead of link-local because we need routable addresses between VLANs. The fd00::/8 prefix is for locally-assigned addresses (fc00::/8 is reserved but unused).*

Step 3: Configure Managed Switch

Access web interface at `http://192.168.0.1` (admin/admin)

1. **Enable 802.1Q VLAN**
2. **Create VLANs**: Add VLAN 10 and VLAN 20
3. **Port Configuration**:
   - Router 1 port: Tagged for VLAN 10 & 20
   - Host 1/2 ports: Untagged VLAN 10 (PVID=10)
   - Host 3/RPi3 ports: Untagged VLAN 20 (PVID=20)

Step 4: Configure Hosts

Host 1 (VLAN 10):

```
sudo ip -6 addr add fd00:1:2:10::11/64 dev eth0
sudo ip -6 route add default via fd00:1:2:10::1
```

Host 2 (VLAN 10):

```
sudo ip -6 addr add fd00:1:2:10::12/64 dev eth0
sudo ip -6 route add default via fd00:1:2:10::1
```

Host 3 (VLAN 20):

```
sudo ip -6 addr add fd00:1:2:20::11/64 dev eth0
sudo ip -6 route add default via fd00:1:2:20::1
```

RPi3 (VLAN 20):

```
sudo ip -6 addr add fd00:1:2:20::12/64 dev eth0
sudo ip -6 route add default via fd00:1:2:20::1
```

Step 5: Testing & Verification

Start Wireshark on Router 1:

```
sudo wireshark -i enp1s0f0 &
# Filter: vlan
```

Test VLAN Separation:

From Host 1:

```
# Should work (same VLAN)
ping6 fd00:1:2:10::12  # to Host 2

# Should fail (different VLAN)
ping6 fd00:1:2:20::11  # to Host 3
```

Generate Test Traffic:

On Router 1:

```
# Test multicast on each VLAN
ping6 -I enp1s0f0.10 ff02::1
ping6 -I enp1s0f0.20 ff02::1
```

Key Demonstrations

(a) VLAN Functionality

- Wireshark should show 802.1Q headers with VLAN IDs
- Broadcast packets should stay within VLAN boundaries

(b) Network Separation

- Ping tests should prove isolation between VLANs
- Single physical infrastructure, multiple logical networks

(c) Security Benefit Demo

On Host 1:

```
# Generate broadcast storm (flood of broadcast packets that can overwhelm a
network)
# This simulates a malfunctioning device or attack
sudo hping3 --flood --rand-source -1 ff02::1 -I enp1s0f0
# Sends rapid broadcast packets to all-nodes IPv6 multicast address
```

On Host 3:

```
# Monitor - should see no storm packets
sudo tcpdump -i enp1s0f0 -n
# Shows: No packets from the broadcast storm reach VLAN 20
# Proves: VLANs contain network problems/attacks within their boundary
```

Quick Troubleshooting

- Verify 8021q module: `lsmod | grep 8021q`
- Check VLAN interfaces: `ip -d link show | grep vlan`
- Verify switch VLAN membership in web interface
- Ensure IPv6 forwarding is enabled on Router 1