Lab Session 2: VLANs

Objective: Configure VLANs on Cisco switches, establish trunk links, and verify intra-VLAN connectivity. Extend the setup with a router-on-a-stick to enable inter-VLAN communication, and apply basic Layer 2 security mechanisms.

0. Wrap-Up Report

- During the lab, write in a short report:
  - The answers to the lab questions.
  - Copy paste the `show running-config` output from both your switch and router at the end of the lab before the clean up.

1. Setup

- Recall: *!?2+en+dur?!* (Host and VM)
- Open **VirtualBox**.
- Import either the Windows or Linux VM from `/VM-Source/`.
- While it load, connect to the switch (Catalyst 2960) with the console cable (blue cable).
  - connect to it using the `minicom` command line tool.
  - perform the clean up from the Cisco cheatsheet.
  - perform the start up section.

2. VLAN Setup

WARNING: At some point in the lab, you will work with the group at your side. Be sure to name your VLAN the same way, and to not use the exact same IP addresses (XX and YY).

- Connect to the switch.
- Create the VLAN 10, 20, 99.
- Give them names.
- Connect one of your ethernet interface to the switch and assign VLAN 10 to it in access mode.
- Connect another one in access with VLAN 20.

- In your VM, change the network adaptater to the VLAN 10 interface.
- Give IP addresses to your interfaces both on your host and VM:
  - VM (VLAN 10): 10.10.10.XX/24
  - Host (VLAN 20): 10.10.20.YY/24
  - **Pro tips:** look at the MAC addresses on your adapters behind your screen.
- Try to ping one interface with the other.
- **What do you observe and can you explain what happened?**

- ***Helpful commands:***
  - `ip a`
  - `ip addr add`
  - `ping -I`

3. Interface Security

- As a good practice, move all non used ports to a specific VLAN (not VLAN 1!!) in access mode, and shutdown the interfaces. **Pro tips:** you can configure multiple interfaces at once.
- For interfaces in use, look at the command `Switch(conf-if)# switchport port-security ?`
  - **What could you define to avoid a CAM overflow (MAC flooding)?**
- Look at the `spanning-tree ?` command.
  - **What could you define to block STP messages from non switch devices? Why would you do that?**

4. VLAN Trunking and IntraVLAN

WARNING: This step is to be done with the group at your side. Recheck that your IPs are not conflicted and that VLANs are the same.

- Connect a cable from your switch to the one of the other group.
- Configure this new interface to be a trunk mode.
- Set the native VLAN to 99 on this trunk.
- Only allow VLAN 10, 20 and 99.
- Make the port non negotiate for DTP.

If everything is the same on both end, try to ping the other group's VLAN 10 PC with yours. Also try VLAN 20 - VLAN 20.

- **Checkpoint: Call your lab supervisor.**

5. InterVLAN: Router on Stick

- Now disconnect your trunk from your neighbour's switch.
- Turn on the Router (Cisco 1941) and connect to it with `minicom`.
  - Don't forget to do the cheatsheet clean up on the router to be sure everything is new.
- Connect your trunk to the G0/0 interface.
- Configure the subinterfaces 10 and 20 (for VLAN 10 and 20 respectively) to be used as gateway.
- For both, do the following:
  - enable the dot1Q encapsulation for the right VLAN.
  - define the ip address of this gateway. (*Select one in the right network depending on the VLAN.*)
- Now, change the default gateway on the host and the VM according to the right VLAN.
- Try to ping the host from the VM.
- **Checkpoint: Call your lab supervisor.**

- ***Helpful commands:***
  - `encapsulation ?`
  - `ip ?`

6. Clean up

- Quit and remove the imported VM from **VirtualBox** (erase without file!).
- Perform the clean up section using minicom for **BOTH** the router and the switch.
- Turn off the cisco equipments.