Experience 1 – Switching

Practice with switch configuration, security and VLANs..

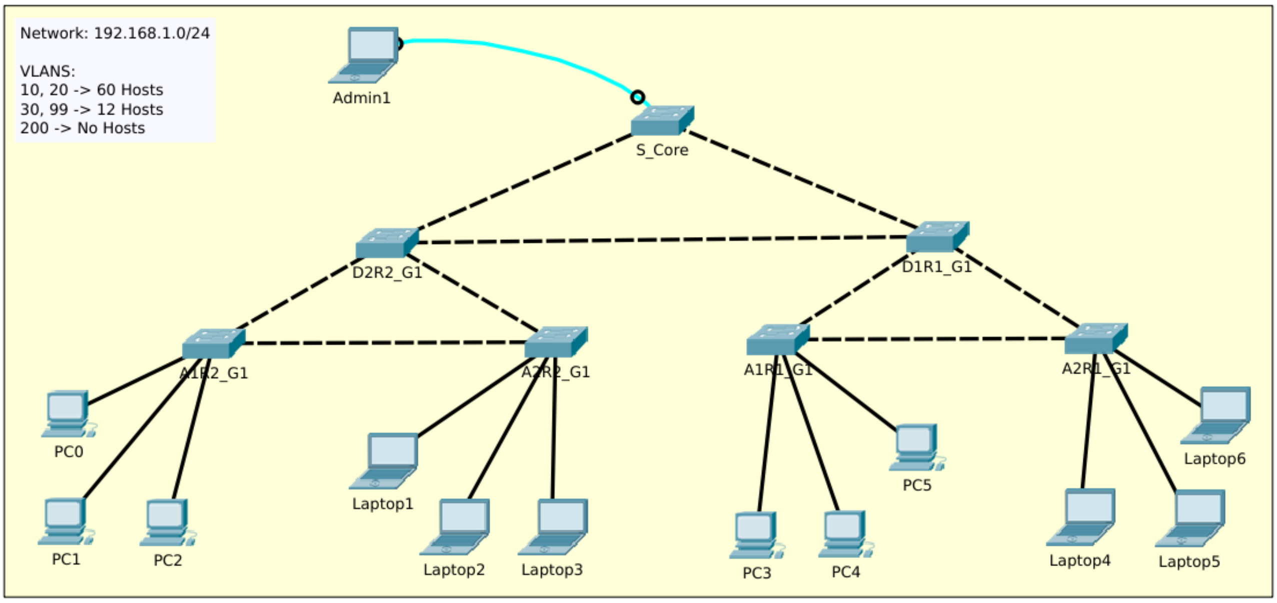

Figure 1: Topology Experience1

Part 1 - Cabling and basic configurations

Perform the **cabling** of the devices according to the previous shown topology:

- use the first FastEthernet ports for the hosts,
- use the last FastEthernet ports for the switch-to-switch connections,
- save the Gigabit ports for future usage.

Perform the **basic configuration** on the switches (hostname, banner, enable pwd and VTY pwd):

- connect via console to the devices from the Admin1 PC,
- use the same hostnames in the topology,
- enable the telnet protocol,
- configure the management access on the VLAN1 with IP Addresses on the network 192.168.1.0/24,
- configure the IP addresses also on the hosts.

Create a the **topology map** in a table form; the table should report the relevant information on the devices. You can use the following as an example (report the information available at this stage):

Name	Management	Interface	Connets to	Mode	VLANs	Port Security (Y/N)
SW1	**SVI Number:** 1 **IP Address:** 192.168.1.1/24 **Def. GW:** - **Telnet/SSH:** SSHv2	Fa0/0	SW3	Access	77	Y
		G0/1	CoreA	Trunk	1-1005	N
		Fa0/10	...	Dynamic Desirable	10-100, 200	N
		...	...	...	...	...
		...	...	...	...	...

Verify the connectivity. Use the `ping`, `traceroute` and `telnet` tools to check that:

- every host should be able to reach all the other hosts and every switch should be able to reach all the other switches,
- the host and the switches should be able to reach each other,
- the host and the switches should be able to access with `telnet` to the other switches.

Report the tests done and its results creating a dedicated table in the document.

Part 2 – SSH and Port Security

Configure remote secure access (**SSHv2**) on the switches:

- use labtlc.com as domain name and generate a 1024 bit keys;
- allow only the SSH protocol on VTYs;
- verify the ability to connect with SSH and Telnet from the PCs.

Report the tests done and its results creating a dedicated table in the document.

Practice with **port security**:

- enable the port security with the default configuration and use the show commands to look for the device behavior (on the host ports only);
- change the MAC address learning mode and practice with both the static and the sticky. Experience also with the maximum MAC addresses;
- finally practice with the different violation modes.

Report the tests done and its results creating a dedicated table in the document.

Part 3 - VLANs

Modify the configurations and the topology to support the VLANs:

- on the access switches reserve 6 ports for VLAN 10, 6 ports for VLAN 20, 4 ports for VLAN 30 and 2 ports for VLAN 99 and shutdown the others,
- define 4 VLANs, the number 10 (Student), the 20 (Faculty), the 30 (Guest) and the 99 (Mgmt),
- perform the variable length subnetting for the 192.168.1.0/24 to obtain 60 hosts on the VLANs 10 and 20; on VLANs 30 and 99, 12 hosts are enough,
- in every VLAN, start from the first IP address for the hosts (Admin1 should be in VLAN 99 when connected with the ethernet cable on the access switches).

- On the access switches, don’t use the dynamic negotiation of trunks; on distribution and core switches test all the three modes: `dynamic auto`, `dynamic desirabl`e and `trunk` mode. Use the VLAN number 200 as native and allow only the 10, 20, 30 and 99 on trunks.
- Move the management address from the VLAN 1 to the VLAN 99 and use the last available addresses on the switches.

Create a new updated **topology map** to add also the VLAN informations and the new IP usages.

Report the tests done and its results creating a dedicated table in the document.