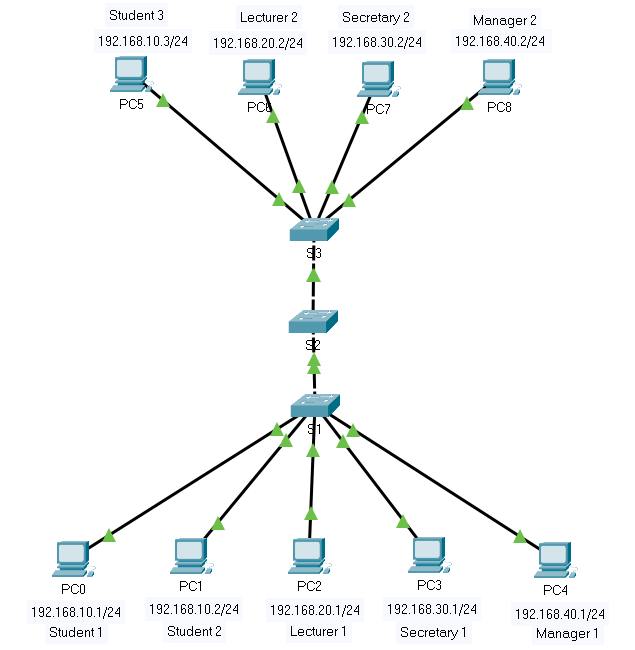
**LAB 27**

**VLANs**

1. Download the PKA file “Lab 27 – VLANs” from Leho. You will find the following setup:



1. This setup contains 9 PCs that are used by 4 types of users: students, lecturers, secretaries and managers. It was decided to use 4 different IP networks to support these different user groups. Write down below the network addresses (including prefix) of these user groups, together with the PCs which belong to that network.

**IP address network of the students:** 192.168.10.0/24

**IP address network of the lectors:** 192.168.20.0/24

**IP address network of the secretaries:** 192.168.30.0/24

**IP address network of the managers:** 192.168.40.0/24

We’ve already configured the IP addresses and subnet masks to each PC (no VLAN configuration is currently applied on the switches).

1. Because not all users of a particular user group are physically in the same location, not all their PCs are connected to the same switch.

For example, students 1 and 2 are connected to switch S1 and student 3 is connected to switch S3 because the latter student is physically located in a different location. However, it is possible to ping between student 1 (PC0) and student 3 (PC5) in this setup. Why is that so?

S1 is connected to S3 through S2 and the IP addresses are in the same network

Test this out!

1. Conversely, 2 users who are physically connected to the same switch but on a different IP network will not be able to communicate with each other.

For example, student 1's computer will not be able to ping with the computer of secretary 1. Why?

They are not in the same network

Test this out!

1. However, if Lecturer 1 is an evil lecturer 👺 (so not Mr. Pareit 😉), trying to pretend to be a student and communicate with the student network, he can change his IP address to be within the student IP network. Change its IP address e.g. to 192.168.10.100/24 and verify Lecturer 1 will be able to ping Student 1.

Therefore, in practice, such a set-up often involves working with a number of VLANs, each of which corresponds to the network of a user group which is equivalent to having 4 physically separated networks.

Before we start creating those VLANs on the switches, it is interesting to first check whether VLANs were not already defined on these switches.

Use an IOS command to get a list of the VLANs defined on S1 and paste below a screenshot of the output of your command (see lecture slides on ‘verifying VLAN configuration’).

Afbeelding met tekst

Automatisch gegenereerde beschrijving

You will find that 5 VLAN IDs (numbers) have already been defined by Cisco by default and which cannot be removed (see lecture slides). Which ones?

VLAN 1, 1001, 1002, 1003, 1004 and 1005

Only the VLAN with the name “default” is interesting here.

What ID (number) does this VLAN have?

1

Which switch ports belong to this VLAN by default?

All ports

1. On S1 create the following VLANs (see lecture slides):

* A VLAN with the name *students* and ID 10
* A VLAN named *lecturers* and ID 20
* A VLAN named *secretaries* and ID 30
* A VLAN named *managers* and ID 40

Note: use these exact same names (in lower case) and the exact same VLAN IDs (as we’ll check it that way).

Verify that the VLANs on S1 are correctly defined.

1. Create the same VLANs on S2 and S3 as on S1.
2. After the creation of the VLANs you also need to connect the correct switch ports to those VLANs.

Connect the correct ports to the appropriate VLANs on switch S1 (see lecture slides).

1. Also connect the right ports to the right VLANs on Switch 3.
2. Verify that our evil Lecturer 1 is now no longer to ping Student 1 although he had configured an IP address within the same IP network. This is because they are on different VLANs, which has a similar effect as if they would be on physically separated networks.
3. Verify that Student 1 (PC0) can still ping Student 2 (PC1).
4. However, although Student 1 (PC0) and Student 3 (PC5) belong to the same IP network and the same VLAN, they can no longer ping each other. You can test that.

This is because both PCs are connected via S2 and because the interfaces of the switches that provide that connection are not yet configured as so-called **trunk ports** to ‘connect the same VLANs with each other over different switches’. (See lecture slides).

Therefore, define the required trunk port on S1. Also define VLAN 99 as native VLAN on that trunk port.

1. On the other switches, also configure the required trunk ports and also connect them to native VLAN 99.
2. Check if you can ping between computers located in the same VLAN and connected to different switches. Ping for this, e.g. from PC0 and PC5.

By creating all VLANs and setting all access and trunk ports correctly, you can now imagine the 4 different networks as being equivalent to 4 physically separated networks which would all have their own dedicated switch.

1. Use a command to show information about the trunk interface on Switch1 (see lecture slides) and paste below a screenshot of the output of this command.

Afbeelding met tekst, zwart, scherm, schermafbeelding

Automatisch gegenereerde beschrijving

Which VLANs are allowed on the trunk according to the output of your command?

All VLANs

1. Suppose ‘Manager 2’ did something fishy with the company’s finance accounting (as managers sometimes tend to do) and the directory board now longer trust him/her. We don’t want any communication of Manager 1 to reach Manager 2 anymore. Therefore, make sure VLAN 40 is no longer passed to the trunk port fa0/1 of Switch1.

Hint: Use a switchport ***trunk allowed*** command with additional arguments (see lecture slides).

Then, again use the command to show information about the trunk interface on Switch1 to see if the restriction has been implemented. Paste below a screenshot of the output of your command.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Verify that vlan 40 is indeed no longer passed by pinging from PC4 to PC8. This should no longer be possible because both PCs are connected by a trunk on which the VLAN to which both PCs belong is not allowed.

1. To make your topology more secure, you should disable all switchports which are not in use, using the ***shutdown*** command for those interfaces.

Hint: To do this, use the command ***interface range*** (completed with a correct argument) to select a whole set of interfaces with a single command, instead of having to do this for each interface manually.

Note that it is not possible to communicate from a PC within one IP network to a PC in another IP network. Routing is Layer 3 functionality, thus to this end we would need to add a router to the network or replace a switch with a L3-switch. We’ll consider that in the next lab.

1. Save the running-config to the startup-config files (in the NVRAM memory) for each switch.
2. Save your PKA file and upload it via Leho.