Computer Networks *(Redes de Computadores - RCOMP)* – 2025/2026

Laboratory Class 03 (PL03 – 2.5 hours)

Command Line Interface (CLI) management of network devices. A VLAN based layer two platform. VLAN Trunking Protocol (VTP). Spanning Tree Protocol (STP). Packet Tracer activities.

1. Command Line Interface management of network devices

The basic tool to manage a network device is the command line interface (CLI), other available tools like a WEB interface or SNMP (Simple Network Management Protocol) only provide a small subset of features available at the command line. Also, management tools operating through the network are not available when the device is not yet configured.

The access to the command line interface can be achieved either through the network (when device network settings are already in place) or through the **console connection** (Figure 1), the latter is the only option for a fresh new device.

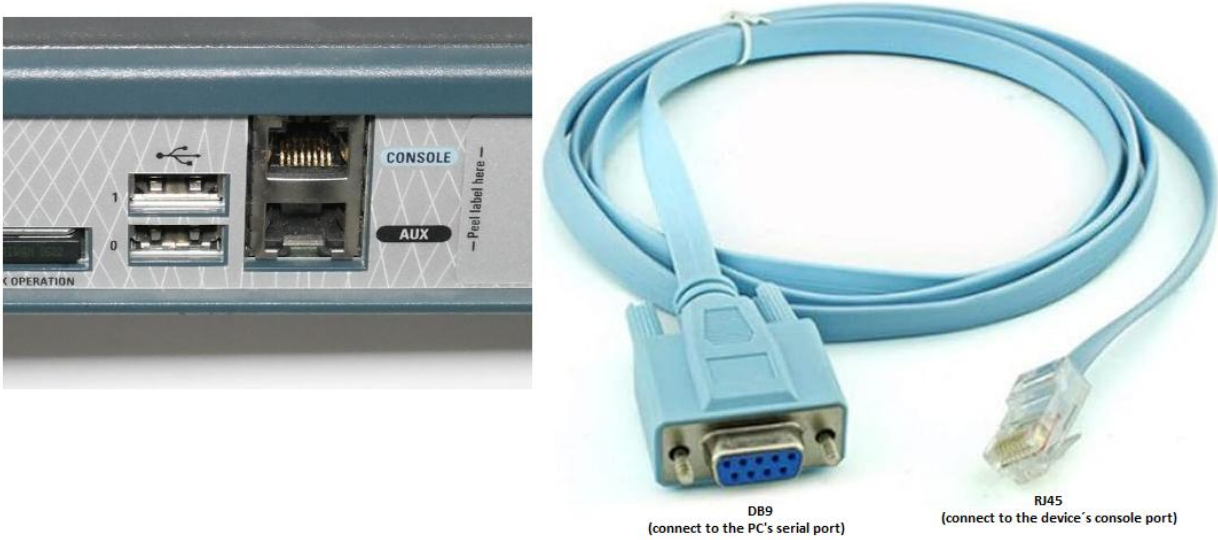

Figure 1 – The console port in a 2811 Cisco router and a roll-over cable

In most network devices, a console connection can be accomplished by a serial line cable known as roll-over, connecting the RJ-45 console port to an RS-232 port with a DB9 or DB25 connector. A hardware text terminal device can be used for command line interaction, but also a terminal emulator (e.g., Putty) running on a standard PC or laptop. If no RS-232 interface is available at the laptop, then a special cable with a USB adapter will be required.

After initial settings at the console, including network basic configuration and remote access services, the command line interface will then be reachable through the network itself by using the TELNET protocol (insecure) or the SSH (Secure Shell) protocol. Most terminal emulators support both these protocols in addition to the direct serial line connection.

Cisco Packet Tracer allows beginners to configure devices through friendly form windows and thus avoid the CLI. However, the ultimate goal is to gradually start using the command line interface (on real devices there are no forms available). On Cisco Packet Tracer, for each management action performed using the form, the command line equivalent is presented on a window at the bottom of the form (Equivalent IOS Commands).

Whenever the student feels ready, he can start switching to CLI by selecting the CLI tab on the device´s form window.

Be aware that management actions available at Packet Tracer forms are only a small subset of all actions Packet Tracer indeed supports for that device in CLI mode. Also be aware, features supported by Packet Tracer devices don´t include all features available on the same real device.

In Figure 2 the Packet Tracer form for configuring a router's network interface is shown, there we can see that this action corresponds to two CLI commands below, one for selecting the interface to be configured and another to set the IPv4 address and network mask for that interface.

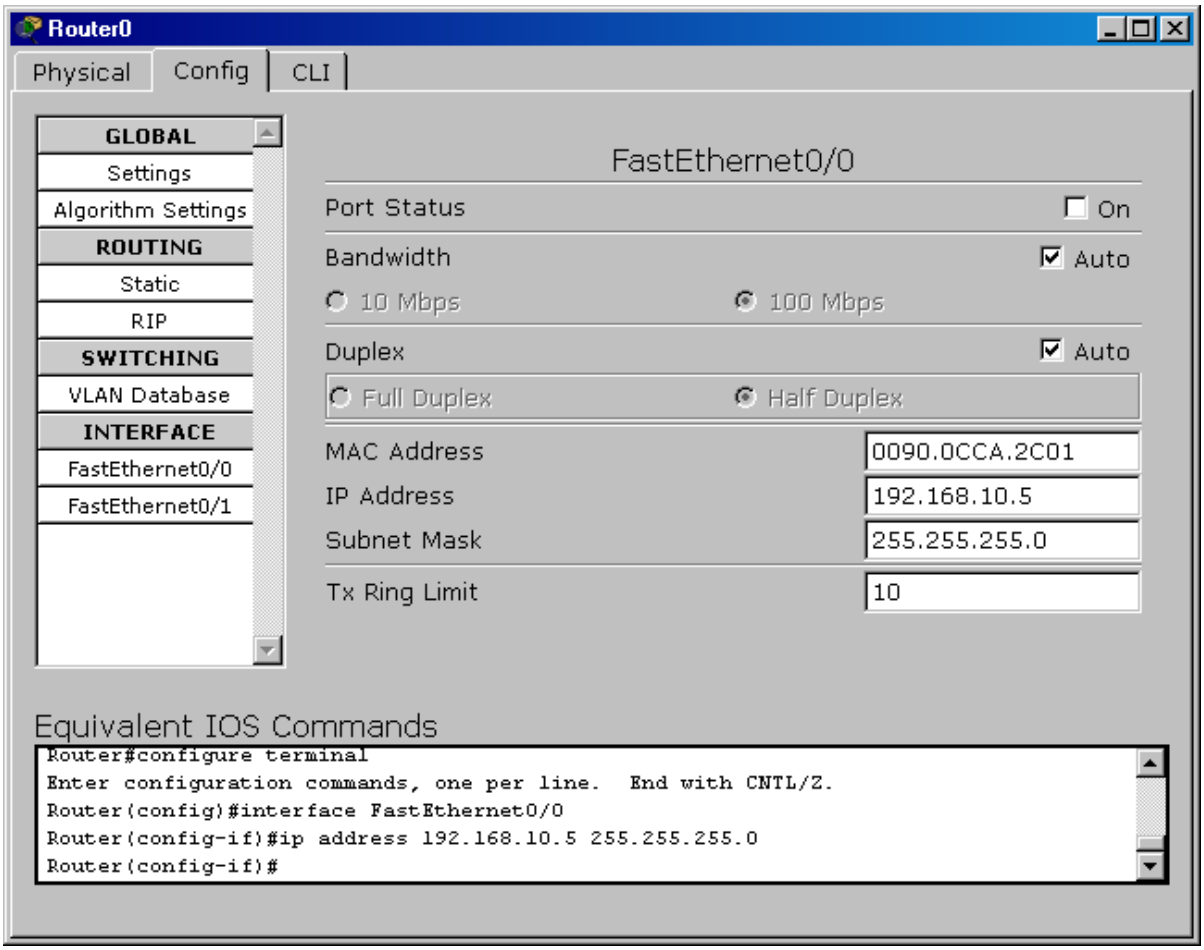

Figure 2 - Cisco Packet Tracer configuration form for a router

1.1. CLI command modes

The CLI is privilege-level or command-mode oriented, there are several command modes, for each, a different set of commands are available, the terminal prompt shows the current mode.

The lowest privilege-level is zero (user EXEC mode) and the prompt will be the greater-than symbol, **>**. The most significant command at this level is **enable**, the **enable** command enters a higher privilege-level, the default is privilege-level 15 (privileged EXEC mode), at this level the prompt is a hash symbol: **#**.

In **privileged EXEC mode**, all the device configuration and status can be queried, also, from this level we can enter **configuration mode** by using the **configure** command, the prompt will then be (config)#. If the configuration is to be performed from the terminal the full command should be **configure terminal**.

Although the **privileged EXEC mode** allows querying about any device's feature status, it doesn't allow configuration changes, for that purpose, entering the **configuration mode** is required. There are also several configuration sub-modes, for instance at the previous image we can see the **interface** command was used in the **configuration mode** to enter the **interface configuration sub-mode**, represented by the (config-if)# prompt.

At any configuration mode, the **end** command can be used to leave back to the **privileged EXEC mode**. The **exit** command can be used in any mode to go back to the previous mode.

Most configuration commands can be reverted by repeating the exact same command line preceded by the word **no**. For instance, in interface configuration sub-mode, **shutdown** to disable the interface and **no shutdown** to enable the interface.

1.2. CLI command typing

For command typing at CLI, several useful features are available. The TAB key may be used for complete: a partially written command or command argument can be completed by the system by pressing this key. As far as they are not ambiguous, commands and arguments may be abbreviated, for instance, **en** instead of **enable**, or **conf t** instead of **configure terminal**.

Before entering a command or a command argument the question mark may be used to get assistance, the system will provide a list of available valid commands or arguments on that context.

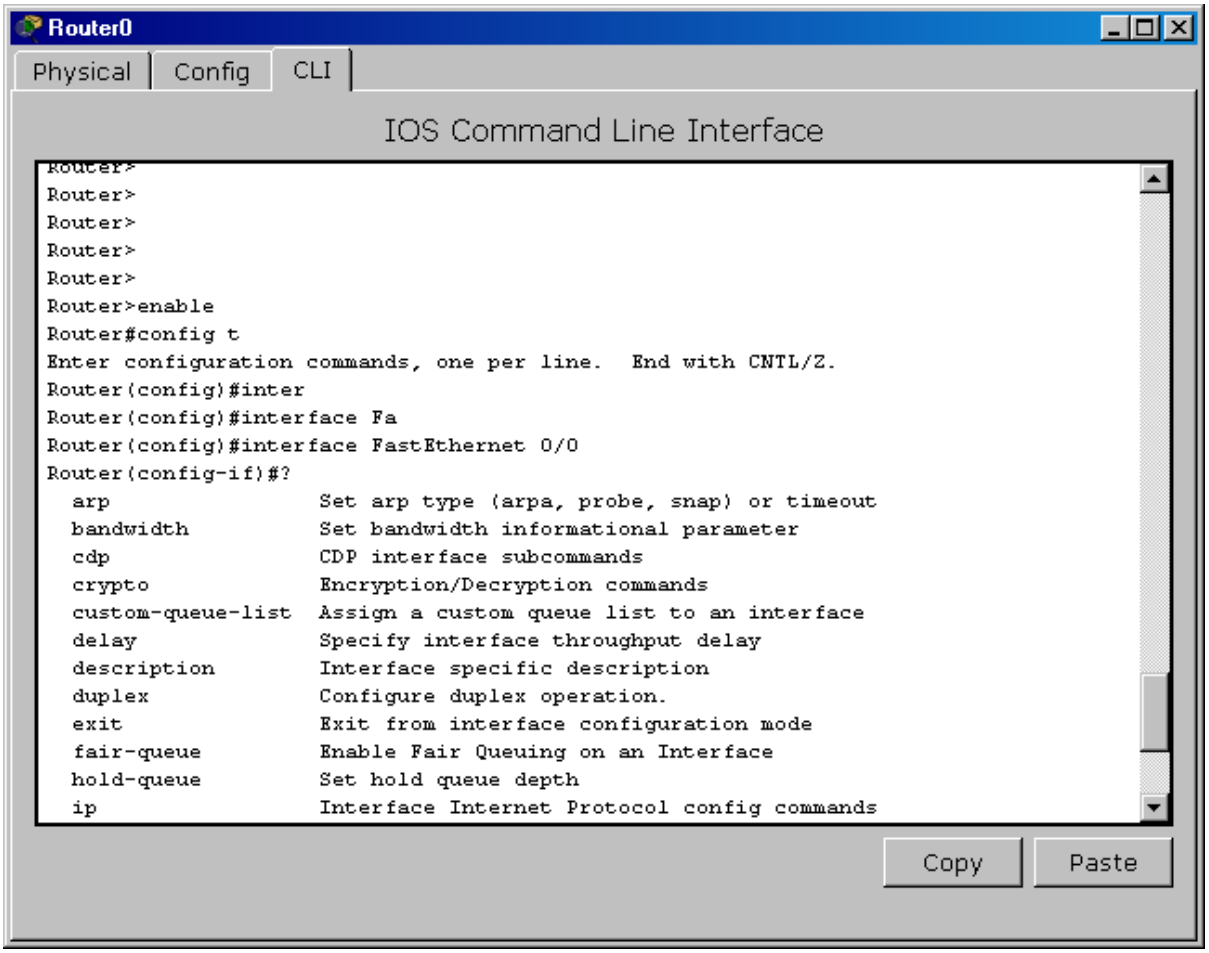

Figure 3 - Examples of CLI interactions

As an example, Figure 3 presents a session that starts in **user EXEC mode**. Then the **enable** command was used to enter **privileged EXEC mode**, and then **configuration mode** by using the **config t** (t is terminal abbreviated) command line.

In configuration mode, TAB was used to complete first the **interface** command and then the command's argument. At last, in interface configuration sub-mode, the question mark was used to display the list of available commands at that stage.

2. VLAN Trunking Protocol (VTP).

A layer two infrastructure is made of a set on interconnected layer two switches, in order to provide the maximum administrative flexibility, such an infrastructure must be continuous, meaning there's layer two connectivity between all switches. This will allow the administrator to establish independent networks through VLANs encompassing whatever nodes it's necessary.

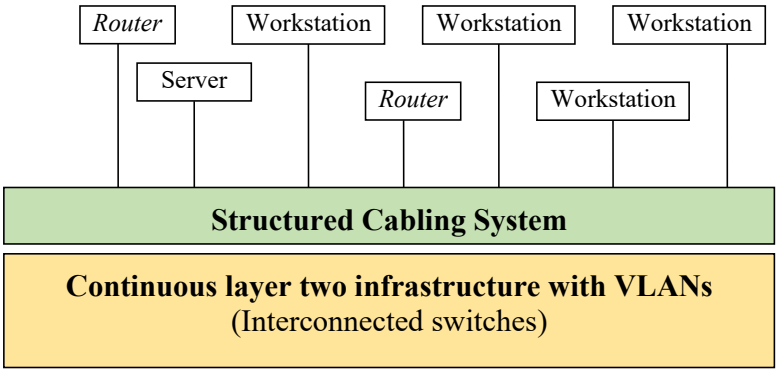

Figure 4 - Continuous layer two infrastructure

A continuous layer two guarantees the maximum flexibility because any point within the infrastructure can be assigned to any VLAN. In other words, VLANs can be drawn freely over the entire infrastructure.

Under this perspective, the structured cabling system role is connecting switches to layer three devices like routers and end-nodes. Bun in fact, each layer three device connection is managed at layer two by using VLANs, thus, no physical handling of patch cords is required. Changing the VLAN to which a layer three device is connected to just a matter of changing the VLAN assigned to a switch port.

If the layer two implementation is split into two or more areas with no layer two connection between them, then a VLAN defined in one area can never be propagated to the other area. This introduces a restriction to the desired flexibility in VLANs design over the infrastructure.

For this scenario, every VLAN that exists must be known and available on every switch of the infrastructure, meaning all switches interconnections must be in trunk-mode with all VLANs.

This also requires every switch's VLAN database to be the same, establishing the same VLAN database, by hand, on every switch, is overwhelming, and here is where we can use some specific VLAN configuration protocols like VTP.

VTP is a Cisco proprietary protocol using the server-client model. VTP works by sending special layer two frames **through trunk-mode links** between switches, these frames transport a domain name (**VTP domain name**) and are accepted only if the domain name matches the locally set VTP domain name.

The main goal of VTP is establishing a VLAN database in switches taking the VTP server role (vtp mode server) and replicate that VLAN database to all switches within the same VTP domain.

By default, Cisco switches are in VTP server mode with no VTP domain defined, so to achieve our goal of establishing the VLAN database on a central switch and having it copied to every switch, the following conditions must be met:

- All switches' interconnections must be in trunk-mode.
- All switches must have the same VTP domain name.
- At least one switch must be in VTP server mode, the VLAN database must be manually defined on those switches.

Cisco switches also provide some automatic configuration features for VTP, namely:

- When a Cisco switch's previously unused port is connected to another Cisco switch's port that is already in trunk-mode, the first switch's port is automatically changed to trunk-mode as well.

- When the above scenario happens with a fresh Cisco switch with the default VTP configuration (no VTP domain), then the new switch automatically changes its VTP domain to the one announced.

2.1. Practical VTP exercise with Packet Tracer

Create the network layout shown in Figure 5 and set the IP addresses of the four PCs as represented, **or download it**, it's available at Moodle (**pl03.pkt**) with the IP addresses already settled.

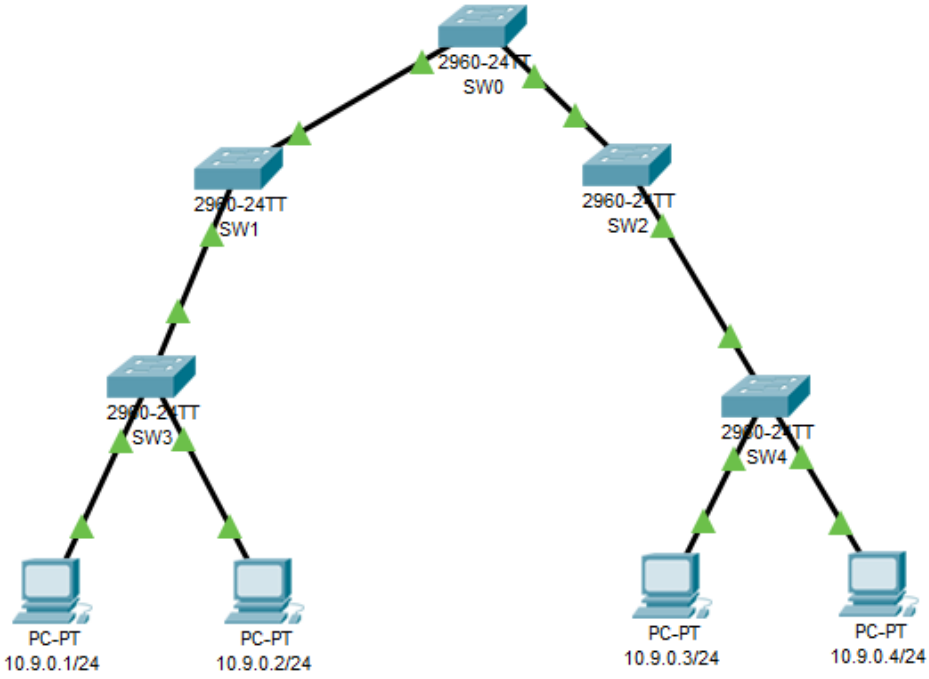

Figure 5 - Network layout to test VTP

By default, all switches' ports are in access-mode and assigned to the default VLAN (VLANID=1).

a) Switch SW0 is going to be the central switch from where the VLAN database is propagated to other switches.

On switch SW0 add the VLANs shown in Table 1 to the switch's VLAN database.

Table 1 - The VLAN database for SW0

VLAN ID (Number)	VLAN Name
200	A
201	B
202	C

b) Change every connection between switches to trunk-mode.

Remember that, on Cisco switches, ports are by default in dynamic mode, thus, if one end of the connection is manually changed to trunk-mode, the other end will automatically also change to trunk-mode.

c) On switch SW0, change the VTP domain name to TEST123.

Unlike the previous activities that are supported by Packet Tracer forms, this must be performed on the command line. Enter configuration mode and use the following command:

```
vtp domain TEST123
```

Because SW0 is already in server mode (that's the default) the VTP domain name is going to be propagated to the remaining switches throughout trunk-mode connections.

d) Check the VTP status on every switch, to do that, again you must use the command line, in privileged EXEC mode use the following command:

```
show vtp status
```

Check that, although not instantly, the VTP domain name is propagated to all switches.

e) Change the VTP mode of every switch to client mode, except for SW0 that will be kept is server mode. Use the following command in configuration mode:

```
vtp mode client
```

Check that, every switch has now the same VLAN database.

f) Add one additional VLAN on switch SW0, using VLANID 300 and named D.

Check that the freshly added VLAN is also present on the other switches.

g) ICMP echo requests testing (ping). Check that every PC is able to ping any other PC.

This works because all PCs are connected to the same VLAN (the default VLAN).

h) Connect PC 10.9.0.1 and PC 10.9.0.3 to VLAN A and connect PC 10.9.0.2 and PC 10.9.0.4 to VLAN B.

This is accomplished by changing the VLAN assigned to the switch port in **access-mode**. For each PC check to which port it's connected, then enter the switch and change accordingly the VLAN assigned to that port in **access-mode**.

i) ICMP echo requests testing again. Check that now only PCs connected to the same VLAN can ping each other.

j) Connect PC 10.9.0.1 and PC 10.9.0.3 to VLAN B (change the assigned VLAN on corresponding switch ports).

Check that again every PC is able to ping any other PC, that's because now they are all connected to the same VLAN again.

With this configuration the administrator is able to remotely access the switch and connect a PC to any VLAN as required.

3. The Spanning Tree Protocol (STP)

One thing an Ethernet network should never have, is a loop, this is because Ethernet, and most layer two protocols, lack any feature that would avoid frames from start circulating indefinitely around such loop. If that happens, every sent packet is added to the loop and never eliminated, thus, ultimately the network becomes unusable due to excessive traffic.

Nevertheless, alternative paths in a network are desirable, they can provide **fault tolerance** and **load balancing**. Fault tolerance means if there is a fault, the system (in this case the network) will still work, this usually requires **redundancy**. Redundancy means there are alternative components (in this case alternative paths) to achieve the same task (in this case network connectivity).

To take advantage of redundant components, and provide fault tolerance, two approaches may be used, in the **failover** approach, only one alternative is used, and the remaining alternatives are meanwhile kept in standby. If there's a fault on the active alternative being used, then the failover mechanism provides its replacement by one of the alternatives previously in standby. The other approach is **load balancing** in which all available alternatives are used at the same time to improve performance.

For fault tolerance, STP can be used to disable existing loops. STP acts by detecting loops and temporarily disable some links to eliminate them, while STP is running, if a currently active link fails a previously disabled link is reactivated. This is, therefore, a failover mechanism, existing alternatives paths are not used at once, at each time there's only one active path.

STP does not provide load balancing, just failover. At layer two, load balancing over Ethernet networks can be achieved by using **Link Aggregation** (port trunking).

Because loops have a major impact on ethernet networks, switches that support STP have it enabled by default.

3.1. Practical exercise with Packet Tracer

Create the following scenario:

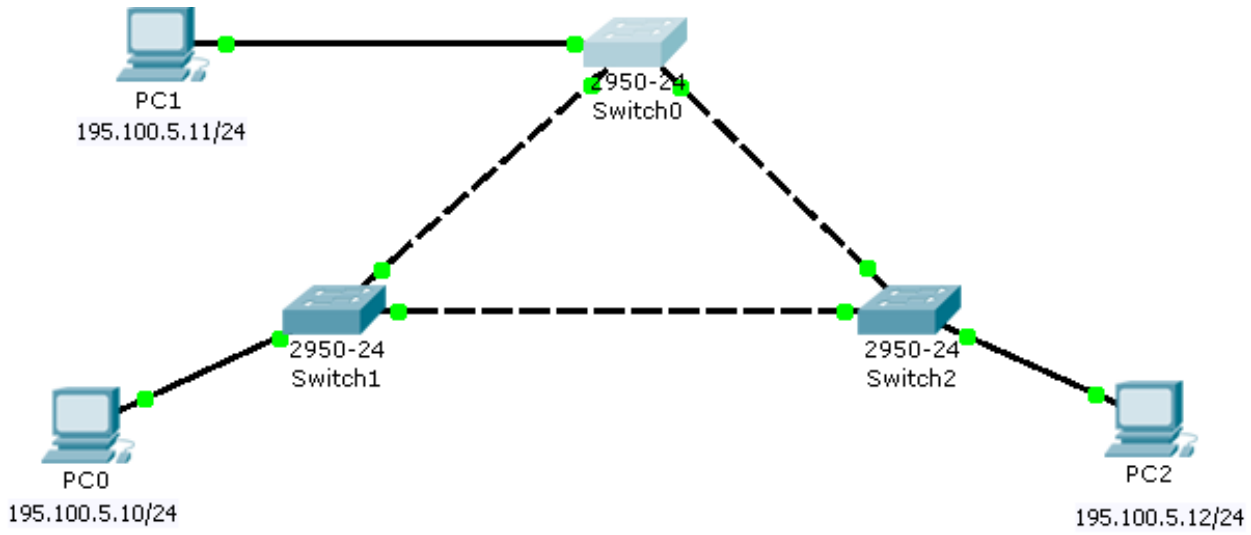

Figure 6 - Network layout for STP testing

As we can see there's a loop, however, thanks to STP (enabled by default on all switches) the loop is broken by temporarily disabling one switch interface.

Now, let's see what would happen if STP was not doing its job.

a) Disable STP on all three switches.

Use CLI at each switch and, in configuration mode, run the **no spanning-tree vlan 1** command. This will disable STP on the default VLAN (VLANID=1).

```
(config) no spanning-tree vlan 1
```

b) Set the end nodes IPv4 addresses as shown in the image.

c) Enter simulation mode and send an ICMP echo request between two end nodes.

Check that the network becomes unusable.

d) Enable STP on all three switches

Enter real mode and enable STP. Use CLI at each switch and, in configuration mode, run the **spanning-tree vlan 1** command.

```
(config) spanning-tree vlan 1
```

Wait until STP breaks the loop (one switch connection will be on standby/orange), this takes some time, called the **convergence time**. Convergence is the process by which when there's a physical change on the network, the system reaches a new operational stable working status.

e) Again, in simulation mode, send an ICMP echo request between two end nodes.

Now the network is working ok, there are no active loops.

f) Testing fault tolerance (failover).

Enter real mode again. To simulate a connection failure, disable one active connection between two switches (one with both ends green), simply disable one of the two ports.

Wait until STP converges (redefines active ports).

You will see the port previously deactivated by STP is now reactivated.

g) Again, in simulation mode, send an ICMP echo request between two end nodes.

Check that, again, the network can deliver packets between any pair of end nodes.