# Create and configure VLANs in Cisco packet tracer

**In this Lab, you will learn to create VLANs and configure them in packet tracer. Use the commands shown below for assigning ports and naming the VLANs**

We will create VLAN 10 and VLAN 20 in this lab. It is always a good practice to give names to the VLANs as this makes it easier for the admins to manage the configured VLANs. The best way to give a name is according to their role in the network for e.g. if there is a VLAN that handles traffic for the voice of IP then we can give the name ‘voice’ to the VLAN and another way of assigning a name is according to the departments in the organization like Sales, marketing, etc.

In a case of a network outage or any issue with the VLANs, admins can easily identify the VLANs with names, which makes their work easier

We can use the following command to create VLAN 10 and 20 and give it a name.

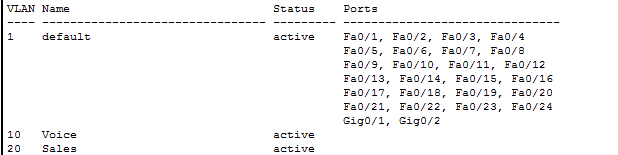
*Switch(config)#vlan 10*

*Switch(config-vlan)#name Voice*

*Switch(config)#vlan 20*

*Switch(config-vlan)#name Sales*

Once we are done creating the VLANs, we can check the created VLANs with the command ‘show VLAN’



**Assigning ports to VLANs**

You can see in the image above that although we have created the VLANs however to use those VLANs, we have to assign ports to VLAN. By default, all ports are assigned to VLAN 1

We will assign 1 port to VLAN 10 and 5 ports to VLAN 20

If we want to assign multiple ports to a single VLAN then we can use the interface range command and include the range of ports that we want to add to any VLAN

*Switch(config)#interface fastEthernet 0/1*

*Switch(config-if)#switchport mode access*

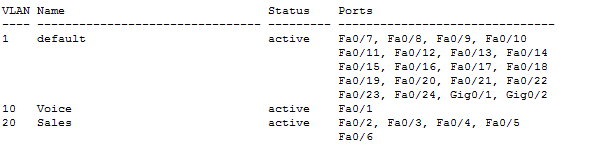
*Switch(config-if)#switchport access vlan 10*

*Switch(config)#interface range fastEthernet 0/2 – 6*

*Switch(config-if-range)#switchport mode access*

*Switch(config-if-range)#switchport access vlan 20*

Now, we can see in the image below that assigned ports are appearing in the front of VLAN 10 and 20



**Inter VLAN routing in packet tracer**

Each VLAN represents a separate network so to enable routing from one VLAN to another VLAN; we have to either use a layer 3 switch or router.

On a single router interface, we can create sub interfaces and configure those interfaces to accept traffic from specific VLANs so we can use only one interface that is connected to the switch for routing purposes.

After configuring the sub-interfaces, we have to assign a default gateway on the end device so the default gateway would be the IP address of the sub-interface specified for the same VLAN of the end device.

Now the traffic will travel within switch when communicating with the end device in the same VLAN and traffic will travel through the router when communicating with devices on other VLANs.

The next task is to properly configure inter VLAN routing.

# Router on a Stick Configuration

‘Router on a Stick’ allows routing between VLANs with only one interface. Each VLAN represents a different Subnet. In general, routers can take traffic from only one subnet and transfer it to another subnet. And we can assign only one IP Address to a router interface. ‘Router on a stick’ allows us to create sub-interfaces, and assign IP Addresses to those sub-interfaces. To make it work, we have to create a truck connection between the switch and a router so that traffic from multiple VLANs can be sent to the router.

If we create a route between VLANs without the ‘Router on a Stick’ method, then we have to waste interfaces on the switches and routers. And if we enable routing between multiple VLANs then it will become practically inefficient as the switches and the routers will use those multiple interfaces.

The image below is an alternative method for allowing routing between VLANs. As you can see, we are using two interfaces on both the router and a switch to allow routing between VLANs. We have not created a sub-interface in the below figure.

Diagram

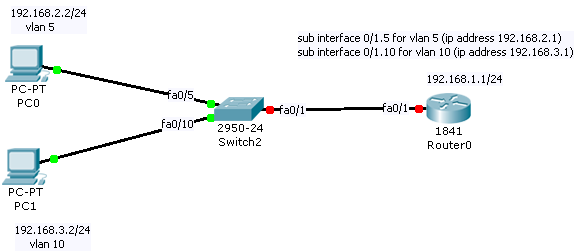
Description automatically generated

You can see that we have to use extra interfaces for each VLAN. So, it becomes practically non-efficient if we have multiple VLANs. Hence, ‘Router on a Stick’ is a perfect solution for routing between VLANs with just one router interface.

The more simple way to do routing between VLANs is by using a Layer 3 Switch. We just have to create virtual interfaces for each VLAN and assign them IP Addresses from the same network. A Layer 3 Switch will then enable routing between VLANs as it has routing capabilities as well. However, Layer 3 Switch is quite expensive so it might not be an affordable option for small office networks.

In the below lab, we will configure ‘Router on a Stick’ that would allow routing between the VLANs. Some of the important concepts in this lab are – to create sub-interfaces, use encapsulation dot1Q command to encapsulate the traffic, and mentioning the VLAN number to ascertain that for which VLAN the sub-interface should respond.

## **Router on a stick configuration in packet tracer.**

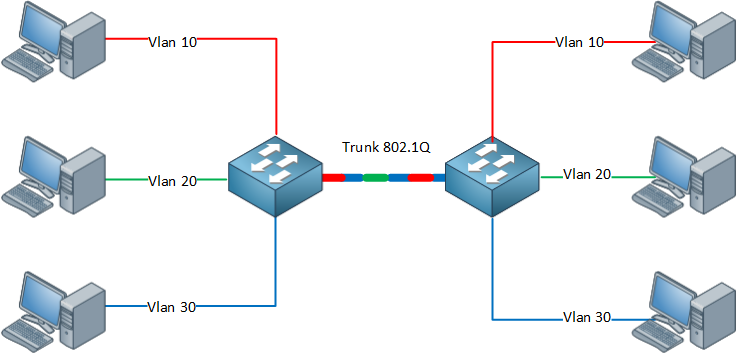


Lab Tasks

1. Assign IP address and default gateway to the PC  
2. Create Vlans and assign ports to the Vlans  
3. Configure trunk connection between router and a switch  
4. Create sub-interface and allow routing between the Vlans

A **trunk** is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.

If you want to VLAN traffic between switches we have to use a trunk. A trunk connection is simply said nothing more but a normal link but it is able to pass traffic from different VLANs and has a method to separate traffic between VLANs. Here’s an example:



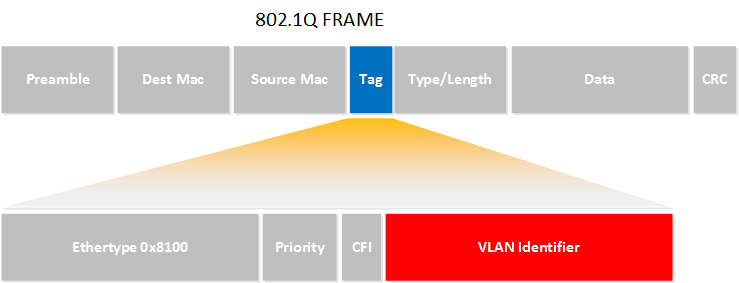
As you can see we have computers on both sides and they are in different VLANs, by using trunks we can make sure all VLAN traffic can be sent between the switches. Because our regular Ethernet frames don’t have anything to show to which VLAN they belong we will need another protocol.

There are two trunking protocols:

**802.1Q:** This is the most common trunking protocol. It’s a standard and supported by many vendors.

**ISL:** This is the Cisco trunking protocol. Not all switches support it.

Let’s take a look at 802.1Q:



Here’s an example of an 802.1Q Ethernet frame. As you can see it’s the same as a normal Ethernet frame but we have added a tag in the middle (that’s the blue field). In our tag you will find a “VLAN identifier” which is the VLAN to which this Ethernet frame belongs. This is how switches know to which VLAN our traffic belongs.

There’s also a field called “Priority” which is how we can give a different priority to the different types of traffic. This is useful when you have one VLAN for voice over IP traffic and another VLAN for data traffic, you probably want to give the VoIP traffic priority or your call quality might suffer.

Lab Configuration

*Task 1*

*Click on pc0 > click on desktop tab > click on IP configuration > set IP address and default gateway*

*Task 2*

*Switch(config)#interface fa0/5*

*Switch(config-if)#switchport access vlan 5*

*Switch(config-if)#in fa0/10*

*Switch(config-if)#switchport access vlan 10*

*Task 3*

*Switch(config)#in fastethernet 0/1*

*Switch(config-if)#switchport mode trunk*

*Task 4*

*Router(config)#in fa 0/1*

*Router(config-if)#no shutdown*

*Router(config)#interface fastethernet 0/1.5*

*Router(config-subif)#encapsulation dot1Q 5*

*Router(config-subif)#ip address 192.168.2.1 255.255.255.0*

*Router(config-subif)#in fastethernet 0/1.10*

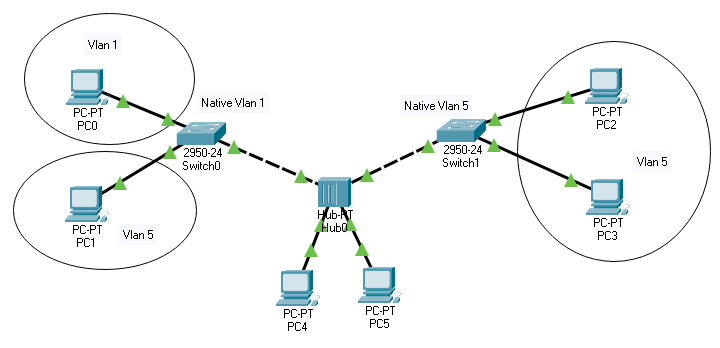
*Router(config-subif)#encapsulation dot1Q 10*

*Router(config-subif)#ip add 192.168.3.1 255.255.255.0*

# Configure native VLAN and fix native VLAN mismatch in packet tracer

**In this lab, you will learn to Configure native VLAN in Cisco packet tracer and Fix native VLAN mismatch.**

**Native VLAN** – Native VLAN allows untagged traffic to be part of one particular VLAN. Native VLAN functionality is used when untagged traffic is received on the trunk connection of the switch.



In the above image, you can see that the hub is connected with the switch. VLAN and tagging are switching technology and as Hub is unable to tag the traffic then what will happen if PC 4 and PC 5 which are connected to the Hub send the traffic? In that case, we have to specify native VLAN on both of the switches interfaces that are connected to Hub and that will help when the switch will receive the untagged traffic on those interfaces then it will be the part of the specified VLAN which we have configured as Native VLAN.

Although Hubs are not in use now a day’s however in a small organization where the budget is low and organizations cannot afford to spend money on new network equipment and they want to use the old network devices then network admin may have to work with such topologies.

In small networks, speed is not the priority for the company so using the device as a hub does not harm the network.

Another network scenario, in which native VLAN is used commonly, is shown below. IP phones are used commonly in the companies these days, they allow daisy-chaining of end devices like PC which saves the interfaces and saves the extra cost of the telecom.

**Daisy chain:** In electrical and electronic engineering, a daisy chain is a wiring scheme in which multiple devices are wired together in sequence or in a ring, similar to a garland of daisy flowers. Daisy chains may be used for power, analog signals, digital data, or a combination thereof

Diagram

Description automatically generated

Daisy-chaining the PC is an efficient solution as an organization does not have to buy extra switches to implement IP phones.

PC 6 cannot tag the traffic so we have to configure Native VLAN to route the traffic generated by the PC on the desired VLAN however, Cisco IP phone can tag the traffic so native VLAN will only be used by the PC.

By default, native VLAN is configured as 1 on all the interfaces however, in case we want to route traffic to another VLAN then we have to change the native VLAN accordingly.

To check the native VLAN that is configured, we can use the command ‘show interfaces trunk’

Text

Description automatically generated

To configure the native VLAN or to change the default native VLAN, we have to use the following command.

Switch(config)#interface fastEthernet 0/24  
Switch(config-if)#switchport trunk native vlan 5

We have to enter into interface configuration mode and then use the command shown above; we have to specify the VLAN number where we want to redirect untagged traffic. In the above example, traffic will be routed to the VLAN 5.

**Native VLAN mismatch**

Native VLAN mismatch happens when interfaces of the switch are configured with different native VLAN and in that case traffic generated by PC will be routed to both VLAN which will cause issues in the network.

The good thing about the switch is that it detects the native VLAN itself and the following message is displayed on the Command-line interface of the device.

— %CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/24 (5), with Switch FastEthernet0/24 (1) —

To fix the Native VLAN mismatch, we have to configure the same native VLAN on all interfaces that are connected to the hub so the traffic generated will only be redirected to the one VLAN.

# VTP configuration in Cisco packet tracer

**In this lab, we will set up Cisco VTP modes and configure them in packet tracer.**

VTP (Virtual trunking protocol) replicates the VLAN information from one switch to other switches in the network.

VTP protocol is enabled by default in every switch however it only works or replicates the data if the domain name and password will match.

VTP modes also play a role when VTP replicates the data. VTP mode defines how a switch will act when the VTP update will be received.

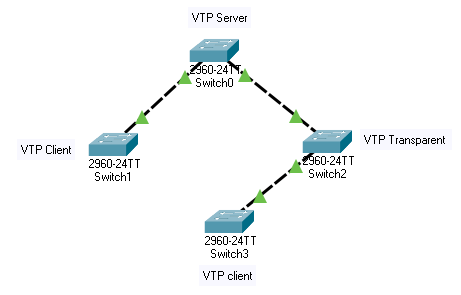
**Three types of VTP modes**

**VTP server**: VTP server switch can create VLANs and it can send and receive VTP updates within the network.

**VTP client**: VTP client switch cannot create VLANs however it receives the VTP updates and it updates its VLAN database according to the update.

**VTP transparent**: VTP transparent switch can create VLANs however it ignores the VTP updates but it passes the VTP updates to other switches in the network. This mode is useful when we want to disable VTP on some of the switches in the network but we want those switches to pass the information to other switches that have VTP enabled.

In this lab, we will configure four switches with different VTP modes.



Switch 0 will be the VTP server

Switch 1 and 3 will be the VTP client

Switch 2 will be configured with VTP transparent mode.

We will see that Switch 2 will not update its database with VTP updates however it will pass the information to Switch 3 so Switch 3 will have its database updated with the VLAN information received from the server.

We have to use the following commands to configure VTP on Cisco Switch. Please make sure that a trunk connection is established between all switches otherwise VTP will not work.

By default, all switches are configured with server mode however we will change that using the following commands.

**Command to change VTP mode**

Switch(config)#vtp mode client  
Setting device to VTP CLIENT mode.

**Command to assign VTP domain name**

Switch(config)#vtp domain Lab  
Changing VTP domain name from NULL to Lab

**Command to assign VTP password**

Switch(config)#vtp password Cisco  
Setting device VLAN database password to Cisco

To check the VTP configuration and which VTP mode is running on the switch, we can use the command.

**Show VTP status**

You can see the configuration of VTP in switch 1

Graphical user interface, text

Description automatically generated

The switch is running VTP version 2.  
The domain name is configured as Lab.  
VTP mode is the client.

VTP password configured is not visible using the status command so we have to use the following command to check the configured password.

Switch#show vtp password  
VTP Password: Cisco

We can see the configured password so this command is useful if we want to check the configured password or we are not sure if the password is configured or not.

Once configured, we can see that switch 1 and switch 3 received the update from switch 0 so VLAN information about VLAN 10 and 20 have been received and both switches have these two VLANs in their database while switch 2 has ignored the update and these two VLANs cannot be found in its database.

VTP should only be used if required otherwise it can be disabled on our network devices.

**Let’s discuss why VTP is not recommended and how to disable VTP on the Cisco switch.**

VTP replicates the VLANs created on one switch to other switches in the network so it appears to be a useful feature however, this feature does not fulfill any requirement. Moreover, VTP can cause a network outage.

We should not use VTP in our network for the following reasons.

**Cisco proprietary**

VTP is Cisco’s proprietary protocol so it only works with the Cisco switches. If we want to use VTP in our network then we have to use only Cisco switches for our topologies.

**Not so easy to configure**

Configuring VTP all over the network can be a demanding task because we have to assign VTP modes correctly to each switch as per our requirements and we also have to define the domain name and password for each switch. In case we want to use more than 1 VTP domain in the network then it makes configuring even harder.

**VTP can cause issues with the network**

VTP uses the revision number to send the VTP updates so whichever switch has the bigger number, its VLAN database will be replicated to other switches in the network. This working mechanism may lead to network downtime if anybody connected the other switch in the existing network that has a bigger revision number. When VTP will realize that the newly connected switch has the bigger revision number then it will wipe out the entire VLAN configuration of other switches and will replace it with the VLANs created on the new switch.

Although VTP updates will only be accepted by the other switches if the VTP domain name and password are same on the other switches. Sometimes, this can be possible when the staging network switch is used in the production network. Many times switches on the staging network are configured to mimic the production network so upon the requirement of more connections in the network, someone decides to use the old switch from the lab having the higher revision number then it will immediately cause the network outage as its VLANs will be replicated to other switches and all the ports assigned to VLANs will be unassigned if any particular VLAN will not exist.

**VTP is not much useful**

VTP only replicates the VLANs created on the switch however we still have to assign ports to those VLANs. Creating a VLAN only takes one command so using the VTP just to create VLANs on other switches does not make our work easier in any way as we have to configure everything else on our own.

**VTP pruning issue**

VTP pruning helps to reduce the unnecessary traffic in the network however it only works when all the switches are configured with the VTP server mode. This again increases the risk of jeopardizing the network as the VTP server has the ability to update the VLAN database and send the VTP updates so every switch in the network can update the VLAN database and in case someone messed up the VLAN configuration on any switch then it will jeopardize the whole network.

**Conclusion**

As discussed, VTP can cause more harm to the production network than doing any good hence it is the best practice to not use VTP in our network. To disable the VTP we can use the following command.

Switch(config)#vtp mode transparent  
Setting device to VTP TRANSPARENT mode.

Setting up VTP transparent mode on the switches will disable the VTP on the switch however switch can still pass the VTP updates to other switches to best practice is to enable transparent mode on all switches used in the network.