
**Faculty of Engineering and Technology**

**Department of Electrical and Computer Engineering ENCS 413**

# Experiment 7 and 8 ROS and SVI

**Student Name :Aseel Khalaf**

**Student Number : 1160689**

Instructor:
Dr.MuhammadHussein
Assistant: Eng.Eman karaja

# Abstract

The report will be talking about switches and how they work and the main concept of VLANs.
It aims to get familiar with switches, implementing VLANs with different ways we implement ROS and SVI.
To implement our experiments, we used layer 3 Switch which is a special kind of switches, we configure our network based on Router-on-a-stick concepts. We Used Cisco Packet Tracer to implement networks that used Router on a stick (ROS), Switch Virtual Interface (SVI) and layer 3 switches

I

# Table Of Content

**II**

# Theory

Switching is a core subject in computer networks. It discusses the different operations that a switch does in parallel to other kinds of concepts such as VLANs, multilayer switching, trunks, layering model of switches, a bundle of cables… etc.

- **Switch**

A switch, in the context of networking, is a high-speed device that receives incoming data packets and redirects them to their destination on a local area network (LAN). A LAN switch operates at the data link layer (Layer 2) or the network layer of the OSI Model and, as such, it can support all types of packet protocols.
Essentially, switches are the traffic cops of a simple local area network.

A switch in an Ethernet-based LAN reads incoming TCP/IP data packets/frames containing destination information as they pass into one or more input ports. The destination information in the packets is used to determine which output ports will be used to send the data on to its intended destination.
Switches are similar to hubs, only smarter. A hub simply connects all the nodes on the network -- communication is essentially in a haphazard manner with any device trying to communicate at any time, resulting in many collisions. A switch, on the other hand, creates an electronic tunnel between source and destination ports for a split second that no other traffic can enter. This results in communication without collisions.
Switches are similar to routers as well, but a router has the additional ability to forward packets between different networks, whereas a switch is limited to node-to-node communication on the same network.

- **How does a switch work?**

A network switch is a small hardware device that filters and forwards packets between LAN segments. Different models of network switch support various numbers of connected devices. The consumer-grade network switch provides either four or eight connection for Ethernet devices, while corporate network switch typically supports between 32 and 128 connections. Moreover, network switches can be additionally connected to each other that is regarded as a daisy-chaining method to add an increasingly larger number of devices to a LAN.

- Unmanaged and Managed Network Switch Unmanaged switch, a type of plug and play Ethernet network switch, is typically designed for basic connectivity. Since unmanaged switch requires no configuration at all, it is often used in home networks or wherever a few ports are needed.

## III

Compared with unmanaged switch, the managed network switch can be configured and properly managed to offer a more tailored experience. It will usually bear the weight of the most comprehensive functions for a network. Since their rich features such as VLAN, CLI, SNMP, IP routing, QoS and etc., a managed network switch is commonly applied in the core layer in a network, especially in large and complex data centers.

- PoE Network Switch A gigabit PoE switch is a network switch and also a power sourcing equipment (PSE) that has Power over Ethernet setting built-in to provide the concentrated function of data transmission and power supply for network terminals over one single cable simultaneously.
- Network Switch vs Hub A network switch resembles a network hub in appearance. However, network switches are capable of inspecting incoming messages when received, determining the source and destination of each packet and then forwarding data only to the specific devices. While the hub transmits the packets to every port except the one which is received the traffic. In general, there is a limit to the amount of bandwidth that users can share on a hub-based network. The more devices are added to the network, the longer it takes data to reach its destination. A network switch can avoid these and other limitations of hub networks.
- Network Switch vs Router Network switches create a network while routers connect networks. In other words, network switches allow different devices on a network to communicate, but routers allow different networks to communicate. In a nutshell, a network switch is typically a Layer-2 device of the OSI model while a router is a Layer-3 device. A switch only deals with MAC addresses and has no knowledge of higher-layer protocols. A router acts as a dispatcher, choosing the best path for information to travel. It can handle IP addresses and route between different network subnets.

All in all, a network switch, hub, and router are all devices that allow you to connect one or more computers to other computers, networked devices or even other networks. A hub glues together an Ethernet network segment; a switch connects multiple Ethernet segments more efficiently and a router can do those functions plus route TCP/IP (Transmission Control Protocol/Internet Protocol) packets between multiple LANs and/or WANs.

- VLAN

A virtual LAN (Local Area Network) is a logical subnetwork that can group together a collection of devices from different physical LANs. Larger business computer networks often set up VLANs to re-partition their network for improved traffic management.
Several different kinds of physical networks support virtual LANs, including both Ethernet and Wi-Fi.

- What Are VLANs Helpful With?

When setting up correctly, virtual LANs can improve the overall performance of busy networks. VLANs are intended to group together client devices that communicate with each other most frequently. The traffic between devices split across two or more physical networks ordinarily needs to be handled by a network's core routers, but with a VLAN that traffic can be handled more efficiently by network switches instead.

## IV

VLANs also bring additional security benefits on larger networks by allowing greater control over which devices have local access to each other. Wi-Fi guest networks are often implemented using wireless access points that support VLANs.

- Static and Dynamic VLANs

Network administrators often refer to static VLANs as “port-based VLANs.” A static VLAN requires an administrator to assign individual ports on the network switch to a virtual network. No matter what device plugs into that port, it becomes a member of that same preassigned virtual network.
Dynamic VLAN configuration allows an administrator to define network membership according to characteristics of the devices themselves rather than their switch port location. For example, a dynamic VLAN can be defined with a list of physical addresses (MAC addresses) or network account names.

- Trunk A trunk is a communications line or link designed to carry multiple signals simultaneously to provide network access between two points. Trunks typically connect switching centers in a communications system. The signals can convey any type of communications data. A trunk can consist of multiple wires, cables or fiber optic strands bundled together to maximize the available bandwidth in a single physical cable, or it can consist of a single high-capacity link over which many signals are multiplexed.[5]

A trunk can also consist of a cluster of broadcast frequencies, as in a trunked radio system that enables the sharing of a few radio frequency channels among a large group of users.[5]
In telephony, trunks interconnect switching nodes, such as private branch exchanges (PBX) and central offices. In enterprise telephony, the transition from traditional time-division multiplexing (TDM) trunks to SIP trunks began around 2009 to use Voice over IP (VoIP) to connect a PBX to the internet.
Data networks use two types of trunks. First, trunks can carry data from multiple local area networks (LANs) or virtual LANs (VLANs) across a single interconnect between switches or routers, called a trunk port. Second, trunks can bond or aggregate multiple physical links to create a single, higher-capacity, more reliable logical link, which is called port trunking.

A trunk port marks frames with special identifying tags -- defined by IEEE standard 802.1Q for VLAN tags for Ethernet frames -- as they pass between switches, so each frame can be routed to its intended VLAN at the other end of the trunked link. Using port trunking to aggregate links is defined by IEEE standard 802.1aq and by the 802.1AX standard for LANs and metropolitan area networks, as well by various vendor-proprietary methods.

- subinterface  The interface is the point of communication between two devices. Imagine a scenario where we have a router with a single interface and the same interface has to connect to two different IP networks.

Instead of having another router or additional interface cards, it is very easy to divide the physical interface into two parts logically.

**V**

A subinterface is the logical division of the physical interface. A physical interface can be divided into multiple subinterfaces.

Subinterfaces are used when Virtual Local Area Network (VLAN) is created in the network and inter-VLAN routing is enabled using a router on a stick method. The configuration of a subinterface is the same as that of configuring physical interface. Before configuring a sub interface, the physical interface that is going to be divided must be turned active or on.

- Switch Virtual Interface Traditionally, switches send traffic only to hosts within the same broadcast domain (Single VLAN) and routers handled traffic between different broadcast domains (Different VLANs). This meant that network devices in different broadcast domains could not communicate without a router.

With SVIs the switch will use virtual Layer 3 interface to route traffic to other Layer 3 interface thus eliminating the need for a physical router. VLANs reduce the load on a network by dividing a LAN into smaller segments and keeping local traffic within a VLAN. However, because each VLAN has its own domain, a mechanism is needed for VLANs to pass data to other VLANs without passing the data through a router.

The solution is to use a switched virtual interface – SVI. An SVI is normally found on switches (Layer 3 and Layer 2). With SVIs the switch recognizes the packet destinations that are local to the sending VLAN and switches those packets and packets destined for different VLANs are routed.

There is a one-to-one mapping between a VLAN and SVI, thus only a single SVI can be mapped to a VLAN. In the default setting, an SVI is created for the default VLAN (VLAN1) to permit remote switch administration.

In most typical designs we have the default gateway for the hosts pointing to the switches SVI, then the switch will route the packets to rest of the Layer 3 domain .

- A layer 3 switch

A layer 3 switch combines the functionality of a switch and a router. It acts as a switch to connect devices that are on the same subnet or virtual LAN at lightning speeds and has IP routing intelligence built into it to double up as a router. It can support routing protocols, inspect incoming packets, and can even make routing decisions based on the source and destination addresses. This is how a layer 3 switch acts as both a switch and a router. Often referred to as a multilayer switch, a layer 3 switch adds a ton of flexibility to a network.

- Features of a layer 3 switch The features of a layer 3 switch are: • Comes with 24 Ethernet ports, but no WAN interface. • Acts as a switch to connect devices within the same subnet. • Switching algorithm is simple and is the same for most routed protocols. • Performs on two OSI layers — layer 2 and layer 3.

**VI**

- Purpose of a layer 3 switch There is a ton of confusion about the use of a layer 3 switch because, in a traditional setup, routers operate at layer 3 of the OSI model while switches operate at layer 2. So, how does this layer 3 switches fit into this model? Also, the name “layer 3 switch” causes confusion because switches typically operate from layer 2. Originally, layer 3 switches were conceived to improve routing performance on large networks, especially corporate intranets. To understand the purpose, let’s step back a bit in time to see how these switches evolved.

Layer 2 switches work well when there is low to medium traffic in VLANs. But these switches would hang when traffic increased. So, it became necessary to augment layer 2’s functionality.

One option was to use a router instead of a switch, but then routers are slower than switches, so this could lead to slower performance. To overcome this downside, researchers thought about implementing a router within a switch. Though technically feasible, it was not the ideal option because layer 2 switches operate only on the Ethernet MAC frame while layer 3 handles multiple routing protocols.

Researchers felt this was too complicated, so they came up with the idea of a layer 3 switches that acted as routers with fast-forwarding done through the underlying hardware. This is why the main difference between layer 3 switches and routers lies in the hardware. If you were to take a peek into a layer 3 switch’s hardware, you’ll see a mix of traditional switches and routers, except that the routers’ software logic is replaced with integrated circuit hardware to improve performance.

- Benefits of a layer 3 switch

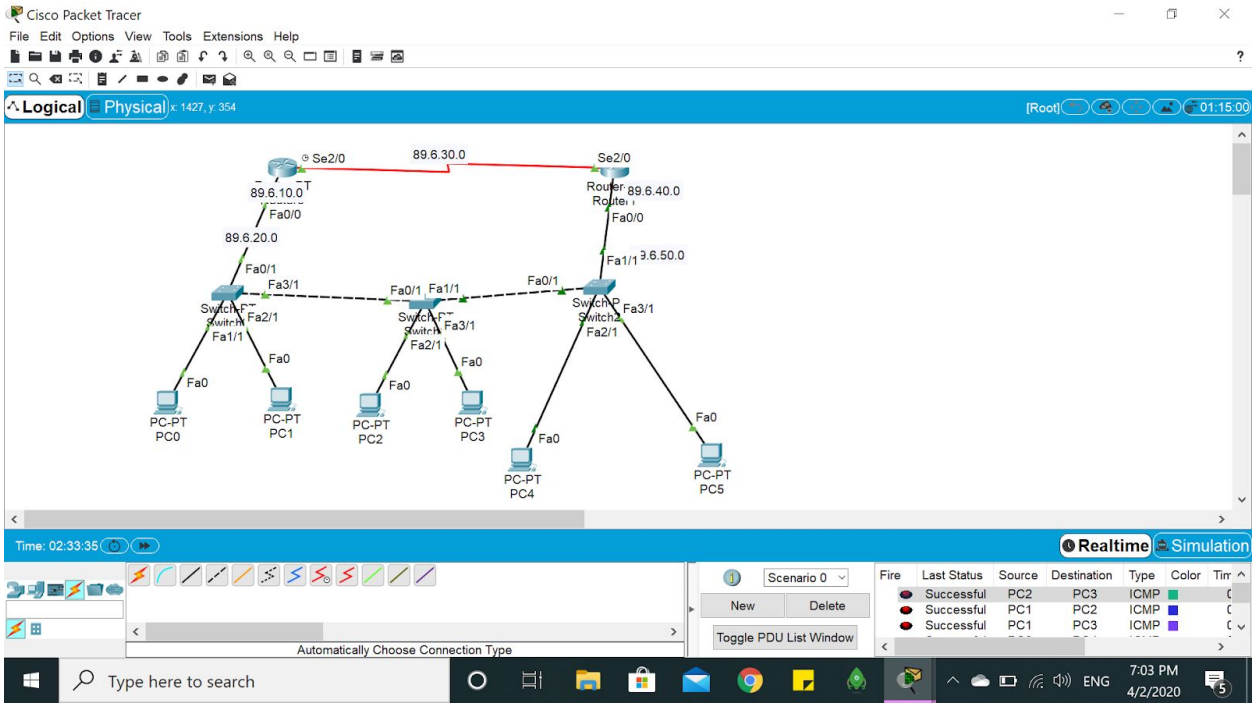
• Support routing between virtual LANs. • Improve fault isolation.
• Simplify security management.
• Reduce broadcast traffic volumes.
• Ease the configuration process for VLANs, as a separate router isn’t required between each VLAN.
• Separate routing tables, and as a result, segregate traffic better.
• Simplify troubleshooting as, fixing problems in the L2 layer is tedious and time-consuming.
• Support flow accounting and high-speed scalability.
• Lower network latency as a packet doesn’t have to make extra hops to go through a router

**VII**

# Procedure and Discussion

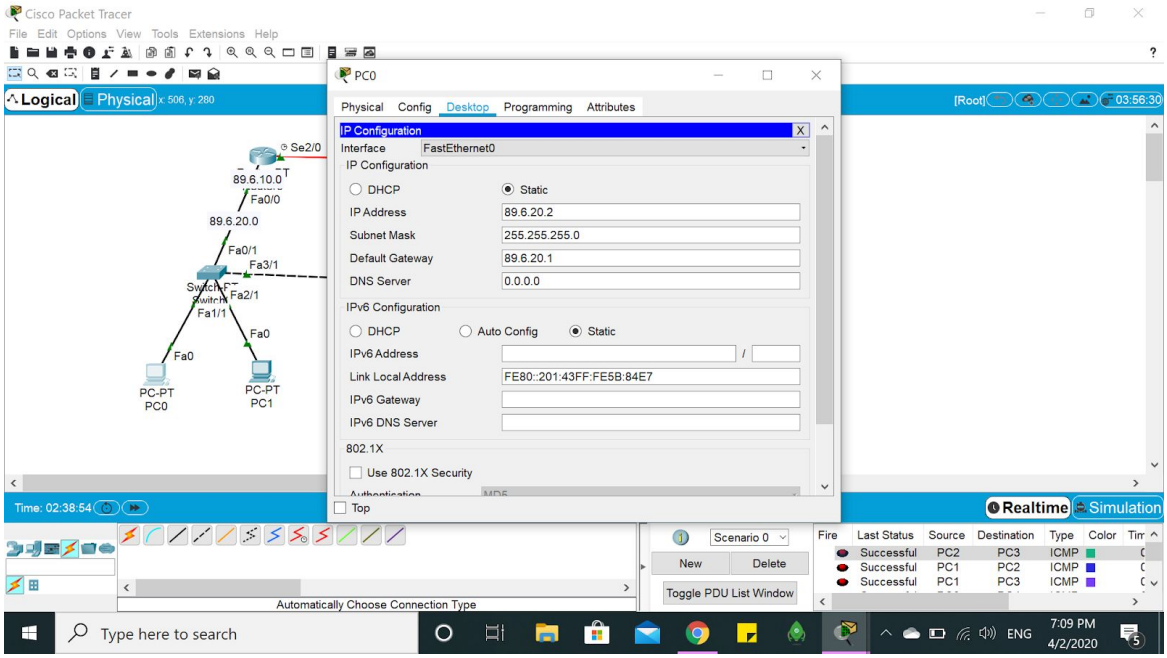
ROS Procedure

Topology



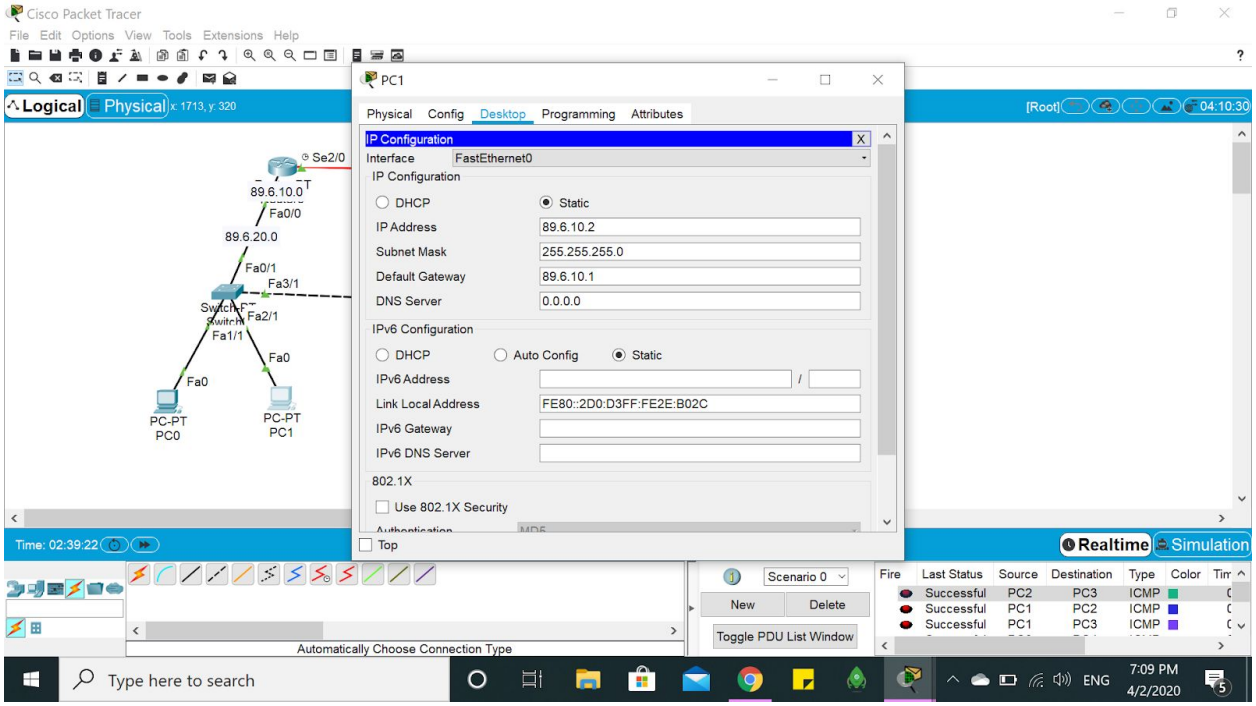

**IPS**

Pc0

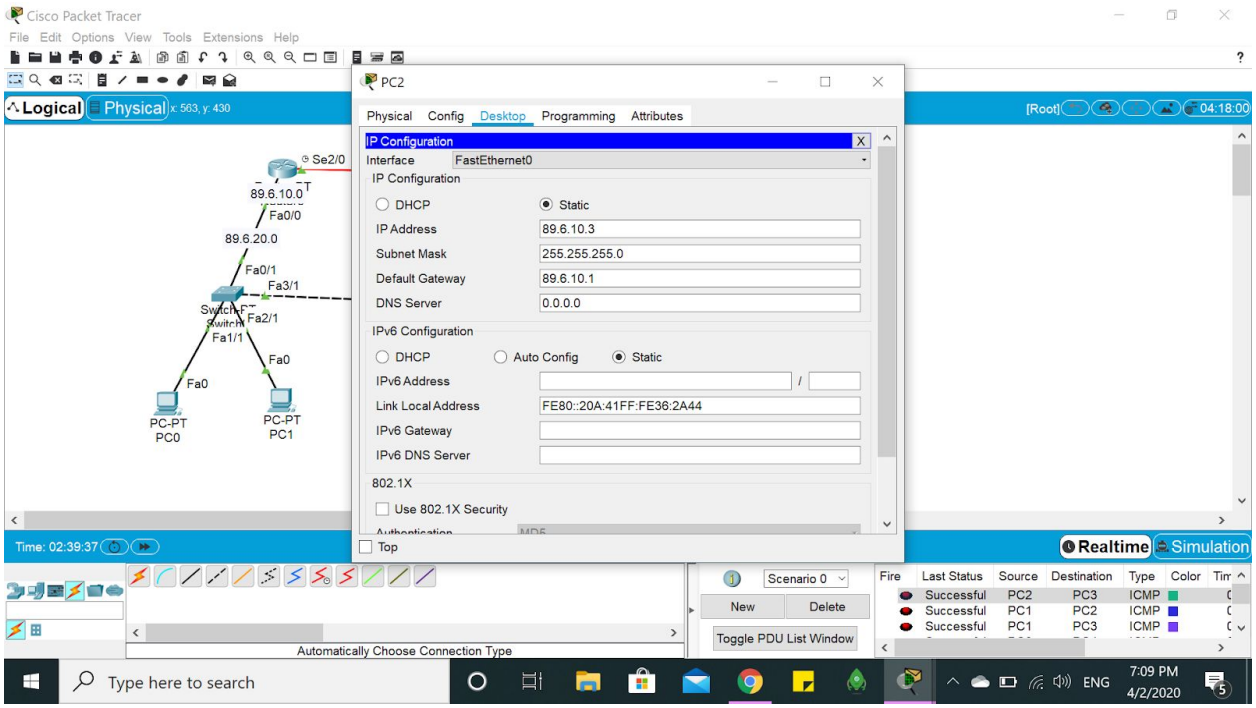

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical Physical x: 506, y: 280
[Root] 03:56:30
PC0
Physical Config Desktop Programming Attributes
IP Configuration
Interface FastEthernet0
IP Configuration
DHCP Static
IP Address 89.6.20.2
Subnet Mask 255.255.255.0
Default Gateway 89.6.20.1
DNS Server 0.0.0.0
IPv6 Configuration
DHCP Auto Config Static
IPv6 Address
Link Local Address FE80::201:43FF:FE5B:84E7
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top
Se2/0
89.6.10.0
Fa0/0
89.6.20.0
Fa0/1
Fa3/1
Switch-PT
Fa2/1
Fa1/1
Fa0
Fa0
PC-PT PC0
PC-PT PC1
Time: 02:38:54
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color
Successful PC2 PC3 ICMP
Successful PC1 PC2 ICMP
Successful PC1 PC3 ICMP
Automatically Choose Connection Type
Type here to search
ENG 7:09 PM 4/2/2020

**8**

Pc1

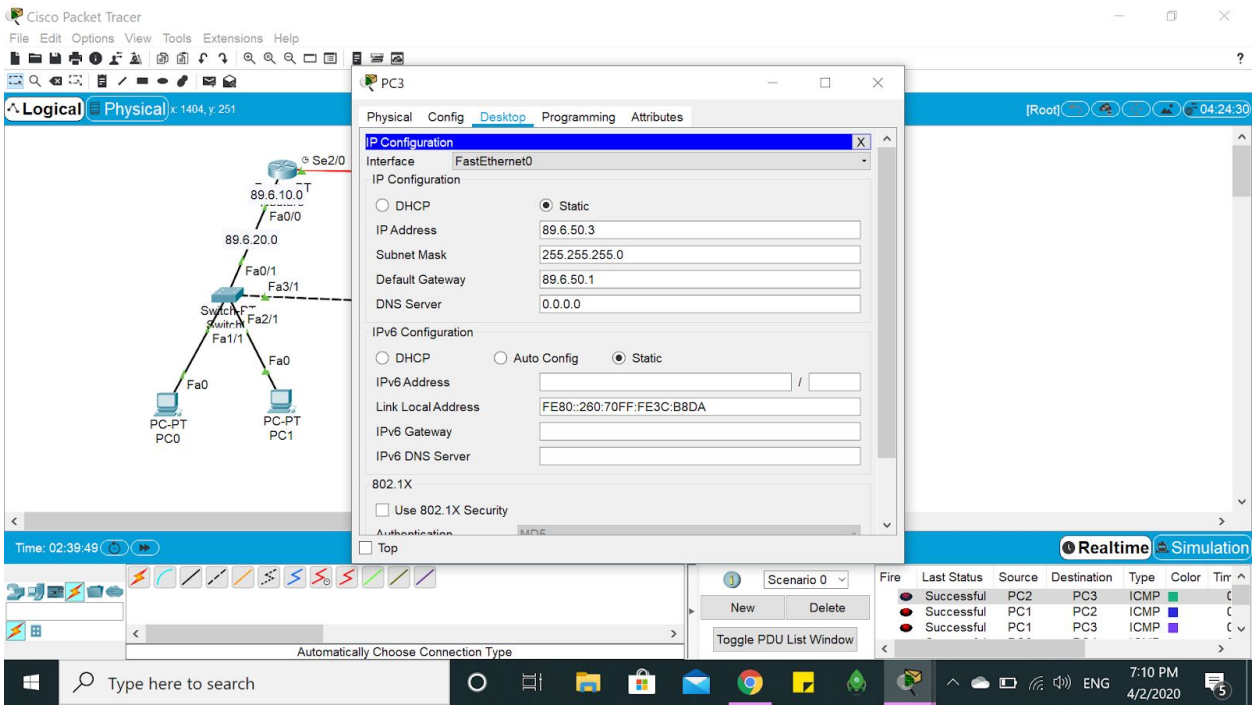

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical Physical x: 1713, y: 320
[Root] 04:10:30
PC1
Physical Config Desktop Programming Attributes
IP Configuration
Interface FastEthernet0
IP Configuration
DHCP Static
IP Address 89.6.10.2
Subnet Mask 255.255.255.0
Default Gateway 89.6.10.1
DNS Server 0.0.0.0
IPv6 Configuration
DHCP Auto Config Static
IPv6 Address
Link Local Address FE80::2D0:D3FF:FE2E:B02C
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top
Se2/0
89.6.10.0
Fa0/0
89.6.20.0
Fa0/1
Fa3/1
Switch-PT
Fa2/1
Fa1/1
Fa0
Fa0
PC-PT PC0
PC-PT PC1
Time: 02:39:22
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color
Successful PC2 PC3 ICMP
Successful PC1 PC2 ICMP
Successful PC1 PC3 ICMP
Automatically Choose Connection Type
Type here to search
ENG 7:09 PM 4/2/2020

Pc2

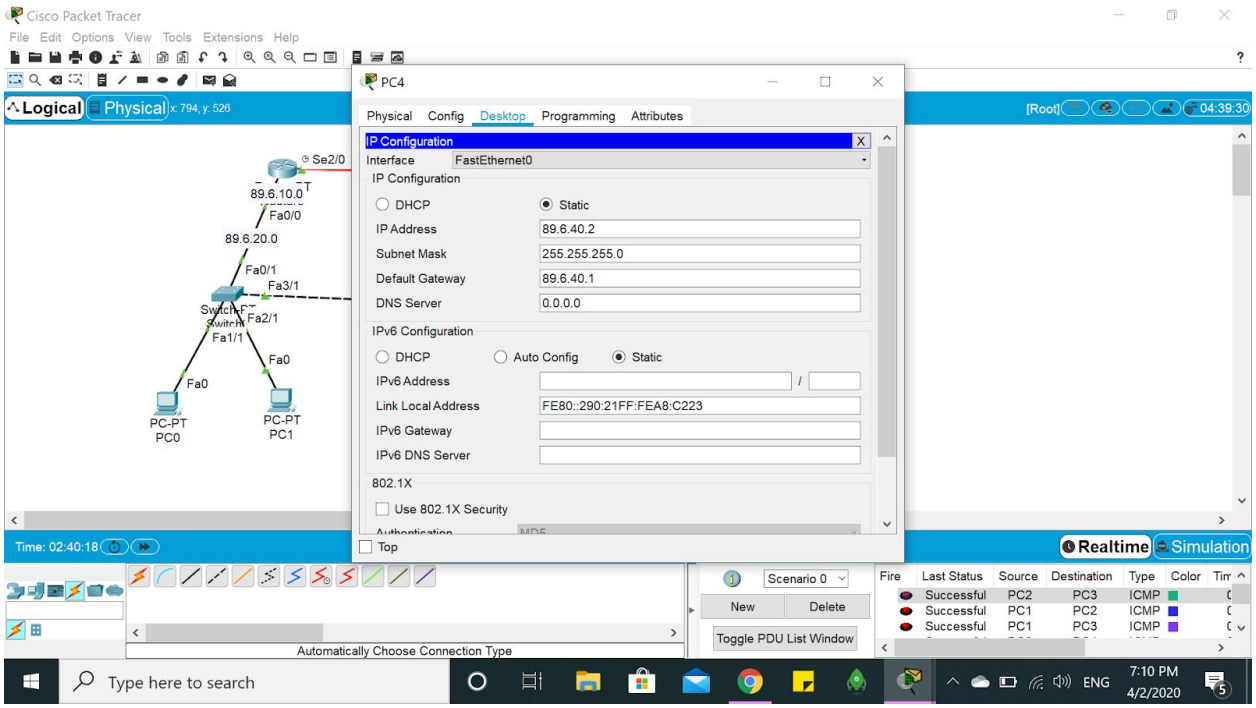

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical Physical x: 563, y: 430
[Root] 04:18:00
PC2
Physical Config Desktop Programming Attributes
IP Configuration
Interface FastEthernet0
IP Configuration
DHCP Static
IP Address 89.6.10.3
Subnet Mask 255.255.255.0
Default Gateway 89.6.10.1
DNS Server 0.0.0.0
IPv6 Configuration
DHCP Auto Config Static
IPv6 Address
Link Local Address FE80::20A:41FF:FE36:2A44
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top
Se2/0
89.6.10.0
Fa0/0
89.6.20.0
Fa0/1
Fa3/1
Fa2/1
Fa1/1
Fa0
Fa0
PC-PT PC0
PC-PT PC1
Time: 02:39:37
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color
Successful PC2 PC3 ICMP
Successful PC1 PC2 ICMP
Successful PC1 PC3 ICMP
Automatically Choose Connection Type
Type here to search
ENG
7:09 PM
4/2/2020

**9**

Pc3

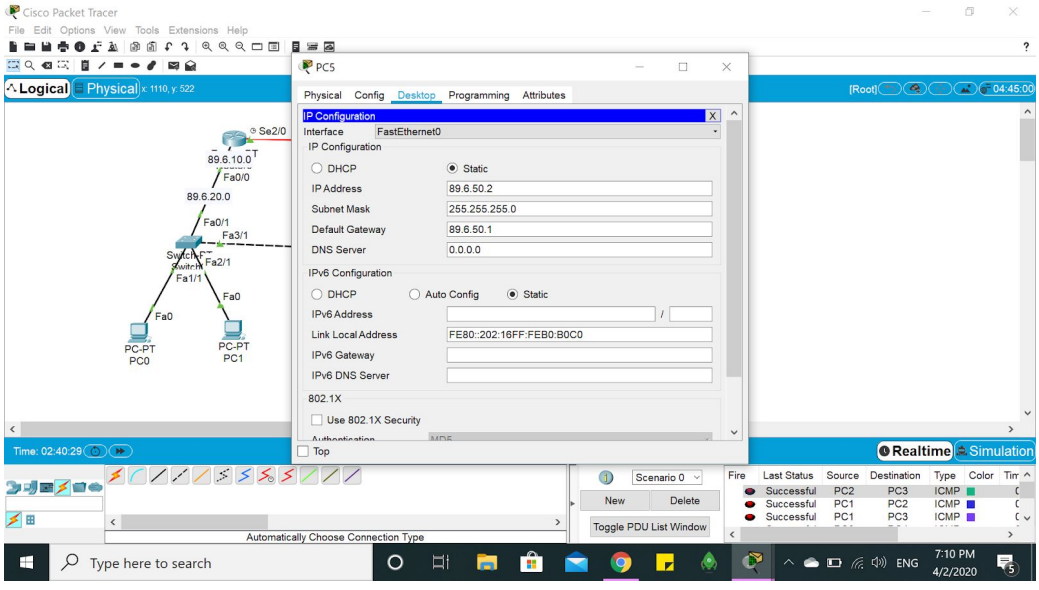

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical Physical x: 1404, y: 251
[Root] 04:24:30
PC3
Physical Config Desktop Programming Attributes
IP Configuration
Interface FastEthernet0
IP Configuration
DHCP Static
IP Address 89.6.50.3
Subnet Mask 255.255.255.0
Default Gateway 89.6.50.1
DNS Server 0.0.0.0
IPv6 Configuration
DHCP Auto Config Static
IPv6 Address
Link Local Address FE80::260:70FF:FE3C:B8DA
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top
Se2/0
89.6.10.0
Fa0/0
89.6.20.0
Fa0/1
Fa3/1
Fa2/1
Fa1/1
Fa0
Fa0
PC-PT PC0
PC-PT PC1
Time: 02:39:49
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color
Successful PC2 PC3 ICMP
Successful PC1 PC2 ICMP
Successful PC1 PC3 ICMP
Automatically Choose Connection Type
Type here to search
ENG
7:10 PM
4/2/2020

Pc4



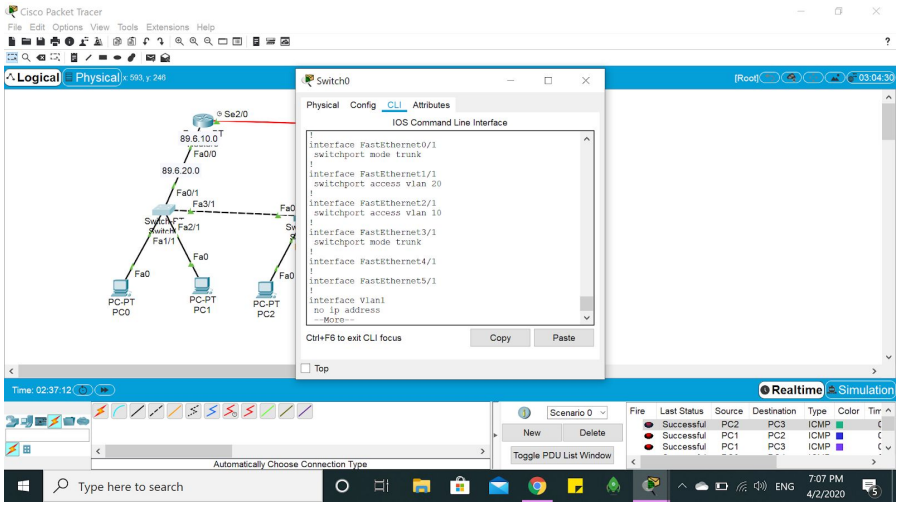

**10**

Pc5

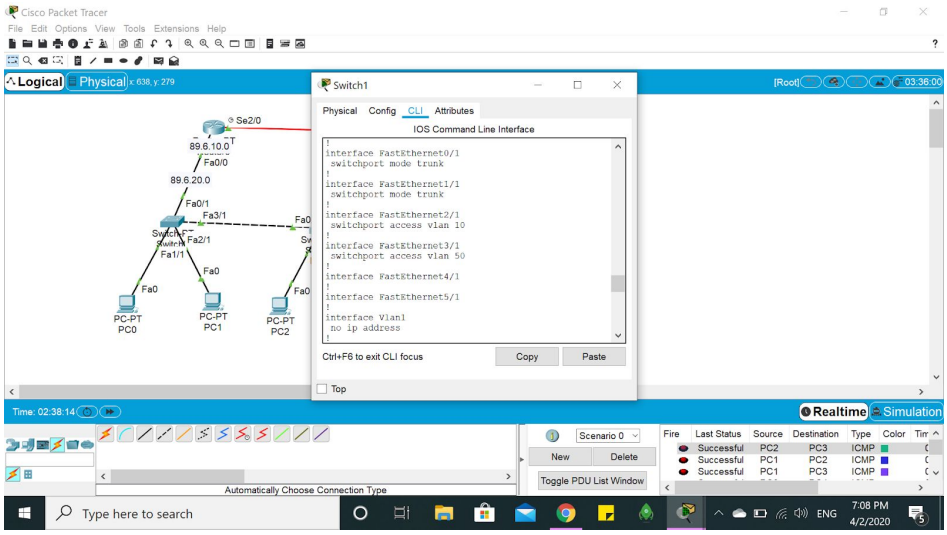



Switches configuration:

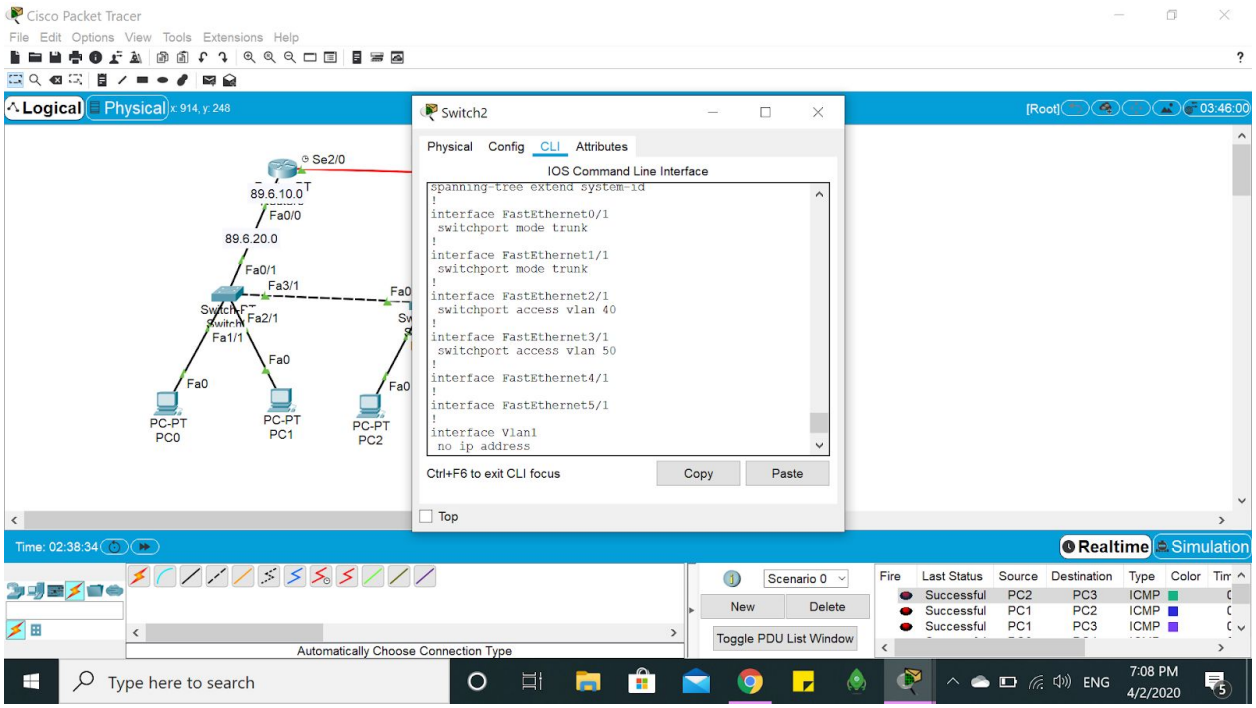
Step 1: Creating a VLAN You can create a specific vlan on a switch using the following command
Switch(config)# VLAN 10
Step 2: Assigning an interface to an existing VLAN
Switch(conf-if)# switchport access VLAN 10
Step 3 : we have to configure many trunk cables based on the following:
1- Each “Switch to Router” cabling should be configured as a TRUNK.
2- Each “Switch to Switch” cabling should be configured as a TRUNK.
Swit
ch(conf-if)# switchport mode trunk
Switch 0




**11**
Switch 1




Switch 2




**12**

Router configuration:

Step 1: Sub interface

When we use the concept of Router on Stick in configuring VLANs, we have to do a sub interface for

each VLAN configured on the switch. A Sub interface acts as default gateway for a specific VLAN.

Initializing a sub interface is done as follows:

Router# conf t

Router(conf)# interface FastEthernet X.X // the first X stands for the interface Name and the second X

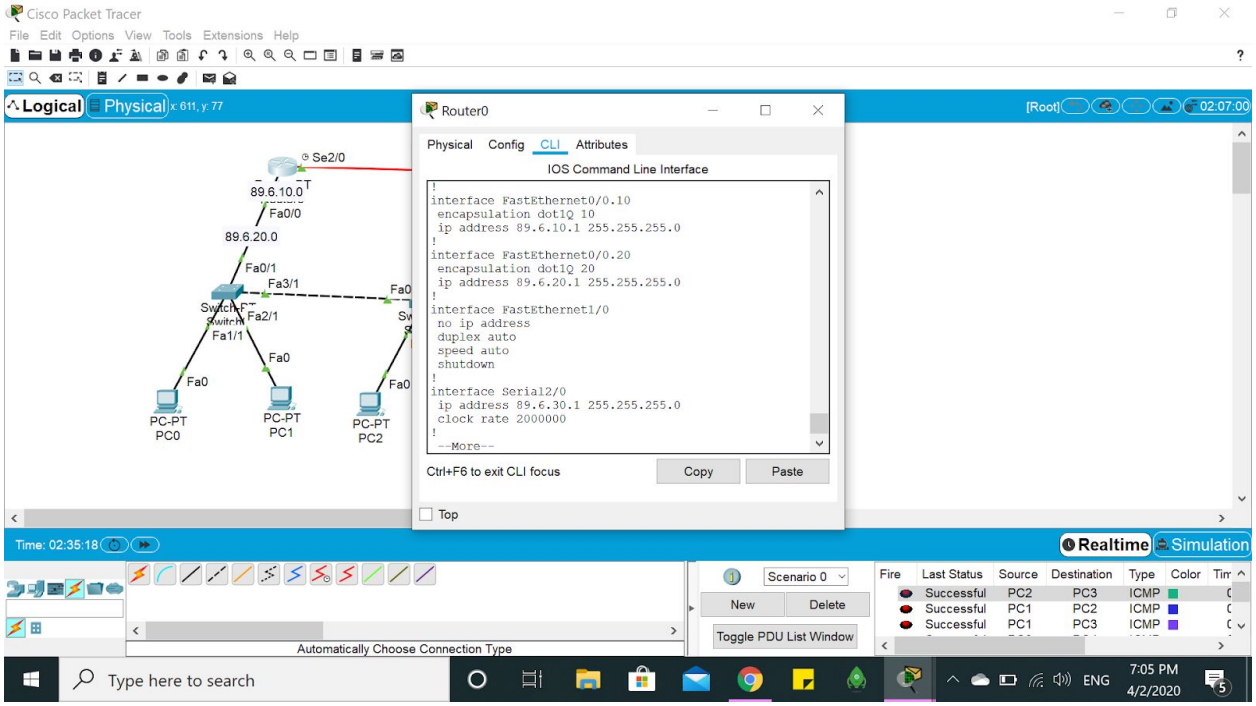
stands for the Sub interface number --- Example: fastethernet 0/0.10

Router(conf-if)# ip address X.X.X.X X.X.X.X

Router(conf-if)# encapsulation dotQ X // this command is used to mark (tag) the traffic for this subinterface

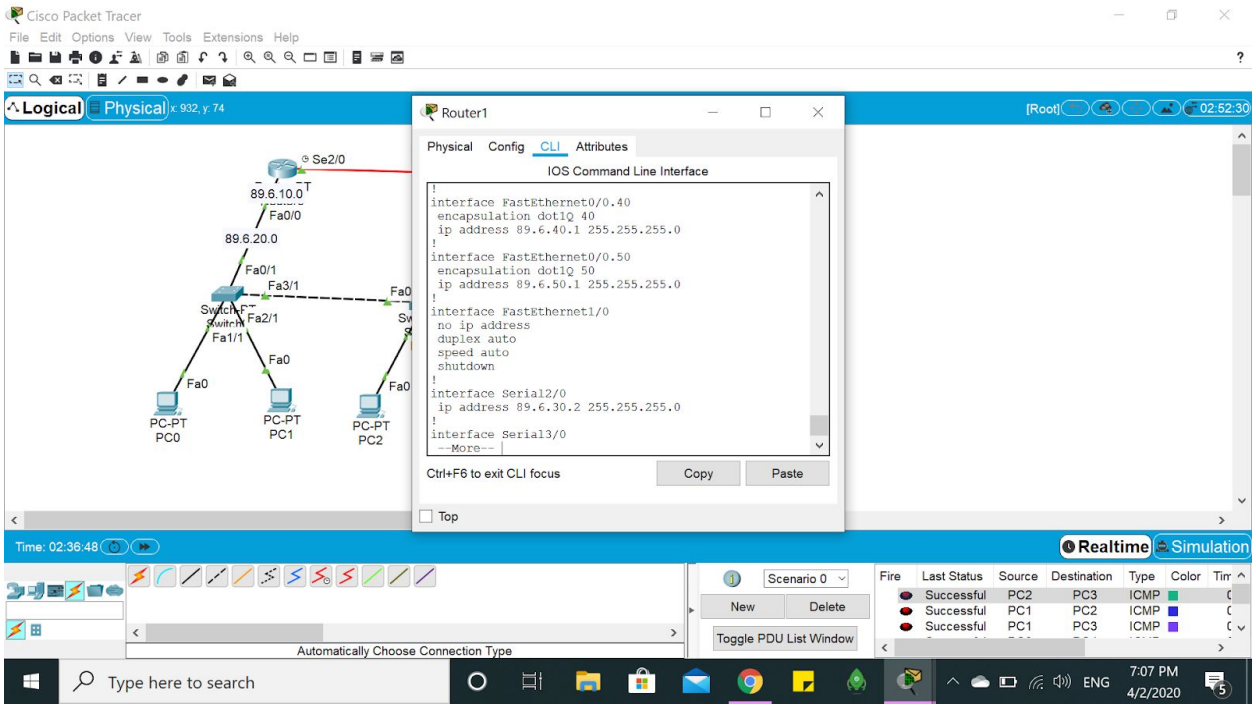
Obviously, there is no need to insert an interface address on the main Ethernet interface. Fast Ethernet 0/0 DOES not have an IP address.

Router 0

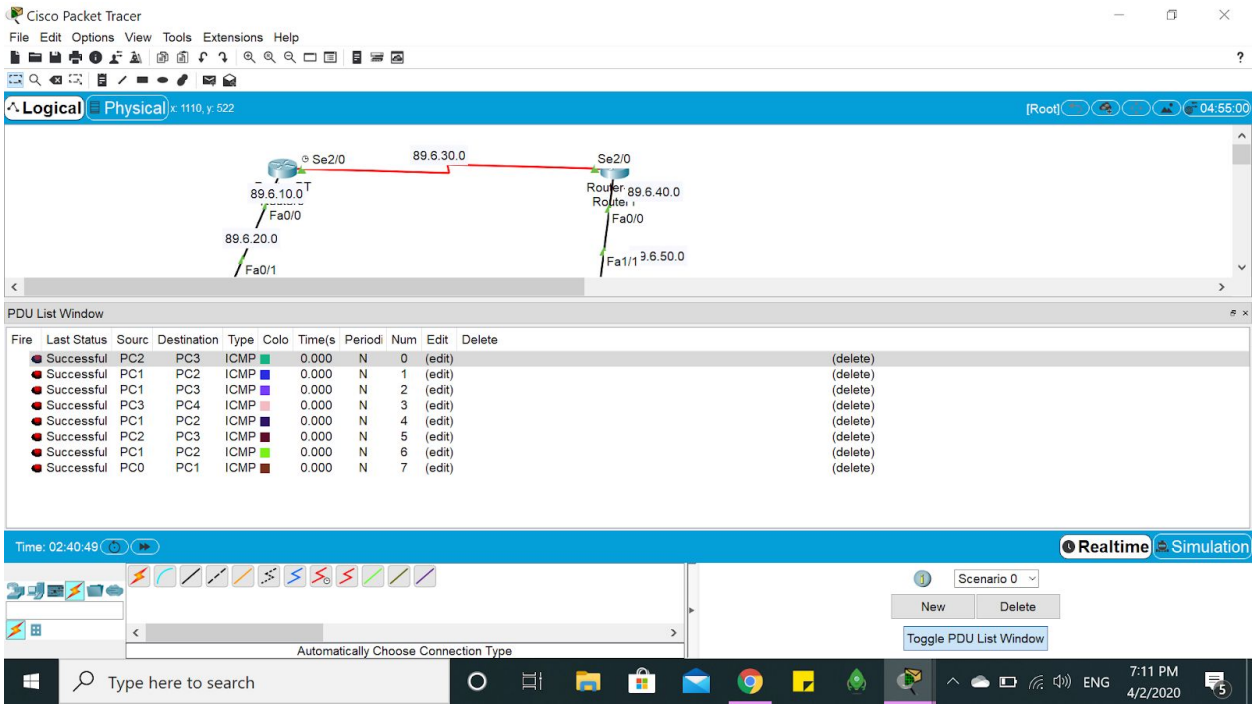



**13**

Router 1




- Result When testing the result of sending packets between PCs :



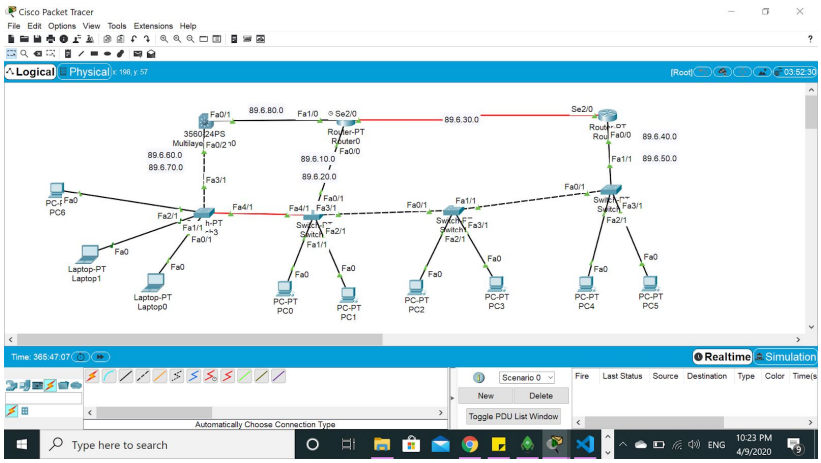
- Discussion

  When we use the concept of Router on Stick in configuring VLANs, we have to do a subinterface for each VLAN configured on the switch.

First, we configure PCs then we configure VLANs in switches and configure trunk between switches.
Use switchport accesses VLAN X to configure VLANs in switches interface
Second, we configure sub-interface and add IPs.
Use the encapsulation dot1q to mark (tag) the traffic for a particular sub-interface.

- **SVI**

  Topology




Switches configuration:
Step 1: Adding the needed hardware to our topology
1- Layer 3 switch: it would act as a router when connected with Router 1 (serial cable) and as a switch when connected with Switch 4 (trunk). This device would configure a Switch Virtual Interface SVI, for all the VLANs that it would act as a gateway for.
2- Normal switch: this device would act as the normal switches we used last experiment.
3-PCs
Step 2: 3rd layer switch Configuration
1- Switch to Router link: we need to connect this switch to router 1 via straight through cable, but in order for a 3rd layer switch port to work as a router port, we have to use the following command: Switch(conf-if)#no switchport
2- Enable routing on the switch: for this kind of switch, we need to enable its ability to route packets as its default configuration would not do that. This can be done using the following command: Switch(config)# ip routing
3- Create the needed VLANs: we need to create our new VLANs on this switch as on a normal one, and then assign some ports for these VLANs
Switch#VLAN 60
Switch(conf-if)#switchport access vlan 60
Switch#VLAN 70
Switch(conf-if)#switchport access vlan 60

**15**

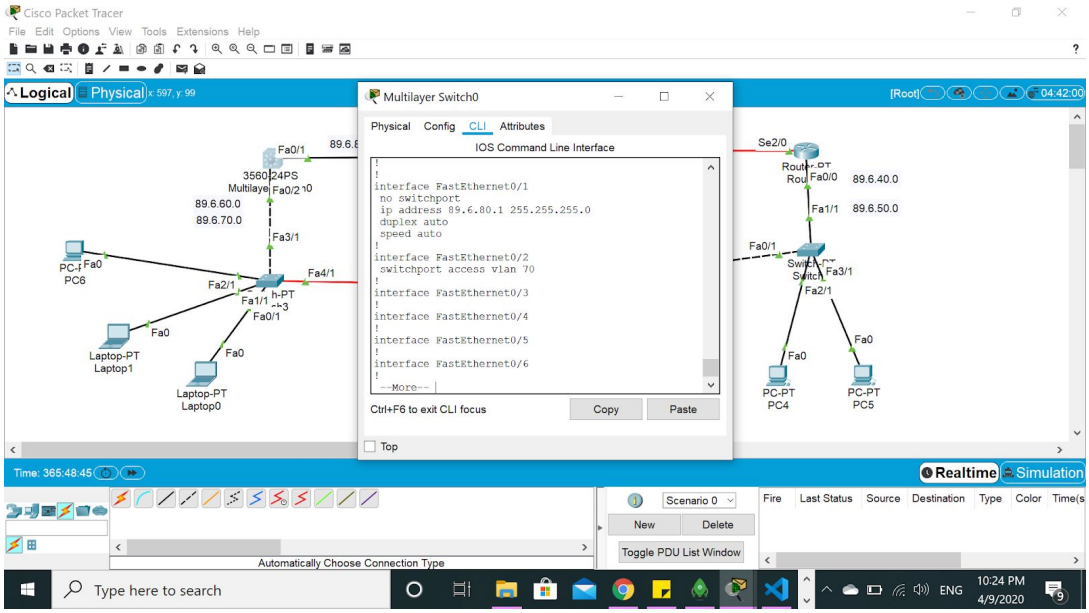
4- Switch Virtual Interfaces: we need to configure two SVIs on this switch to act as default gateways for the new VLANs. This can be done as follows:

Switch(conf)#interface vlan60

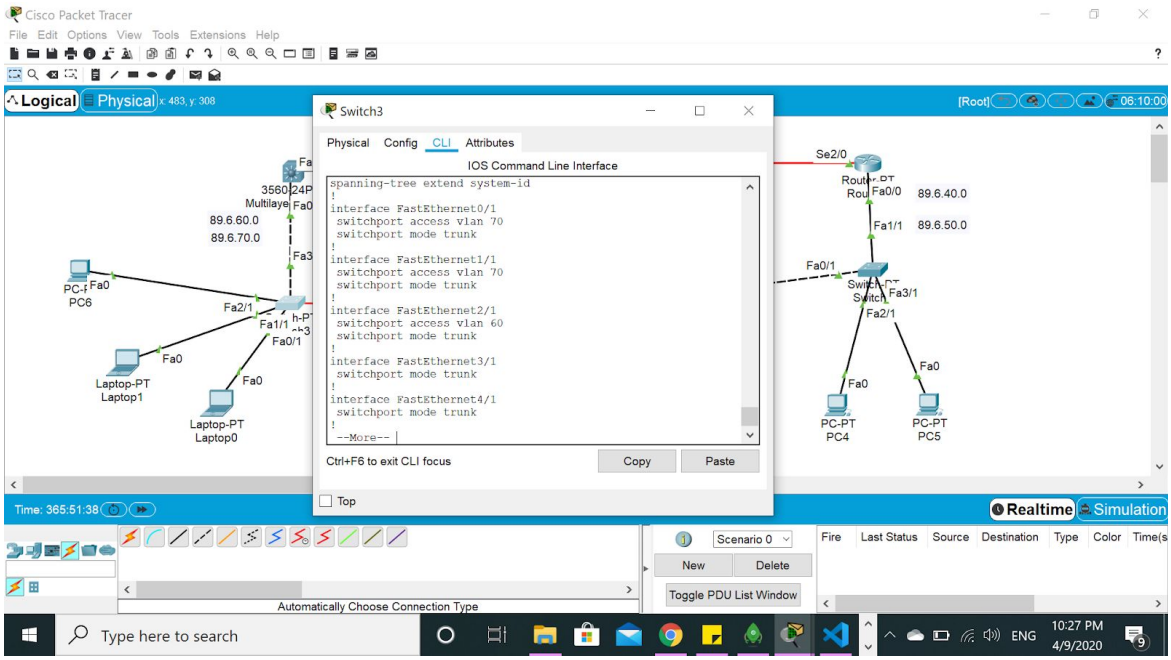
Switch(conf-if)#ip address 192.168.60.1 255.255.255.0

Step 3 : Router ospf configuration , just like previous experiment .

**Switch 0**

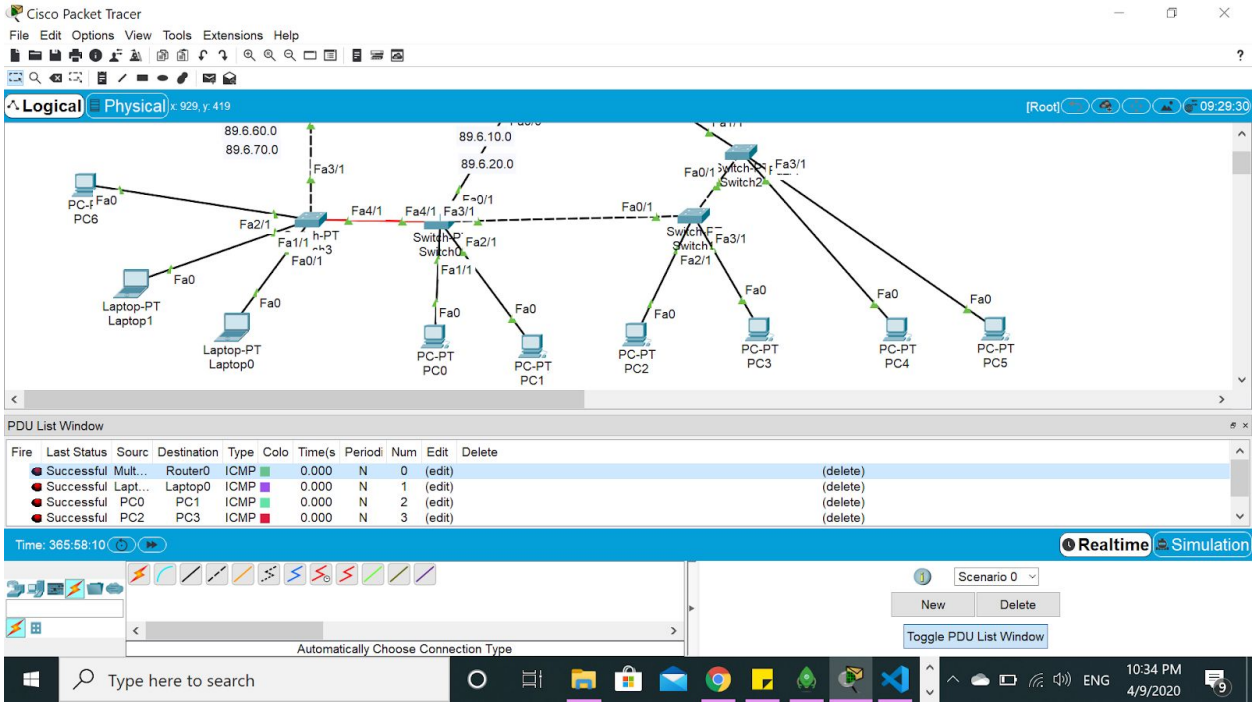



**Switch 3**



**16**

- Result When testing the result of sending packets between PCs :

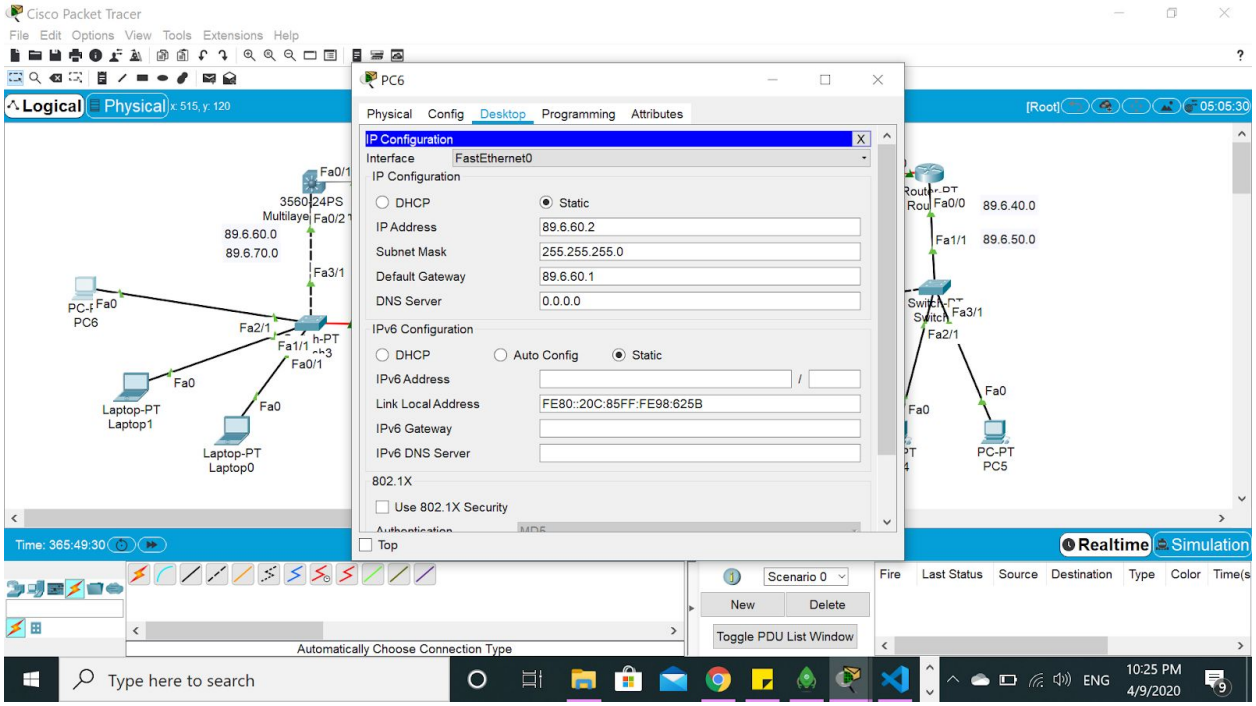



**Discussion**

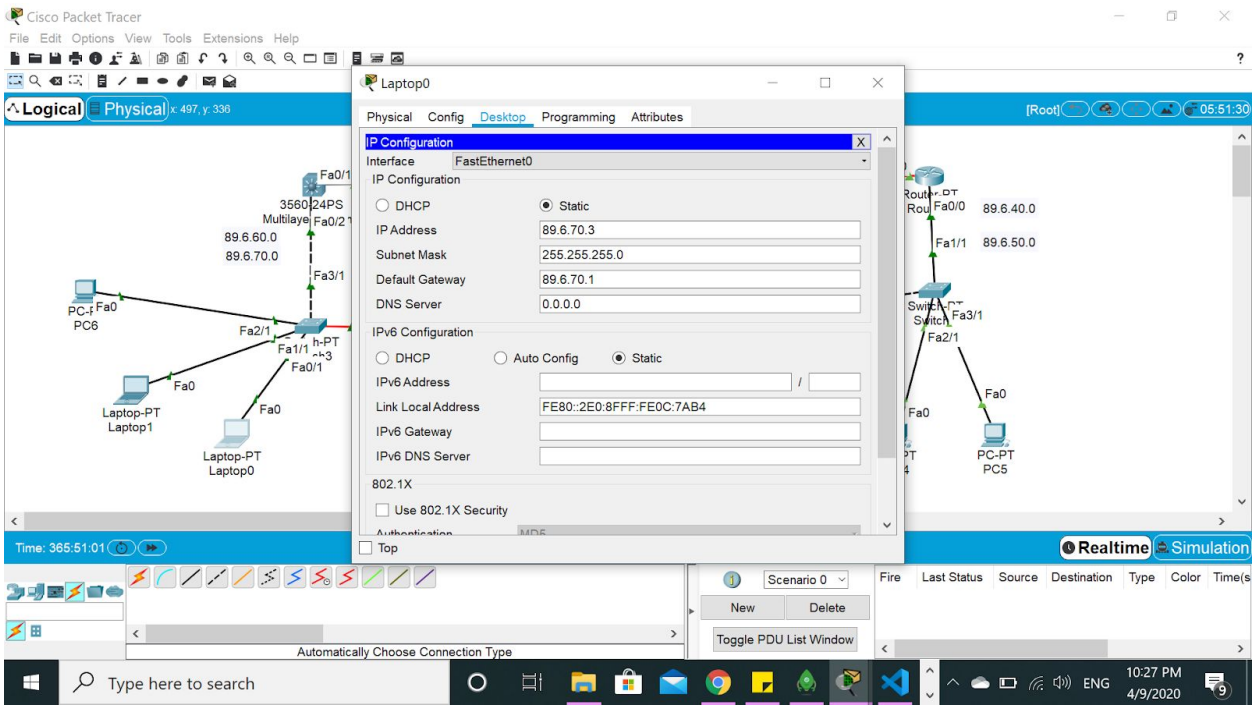
When we use the concept of Router on Stick in configuring VLANs and SVI, we have to do a sub-interface for each VLAN configured on the switch.
Configuration of PCs then configuration of VLANs in switches and configuration of trunk between switches.
Switch port accesses VLAN X to configuration VLANs in switches interface
We configure sub-interface and add IPs.
Use the encapsulation dot1q to mark (tag) the traffic for a particular sub interface.
We configure router RIP and configure networks.
In at layer 3 switch we enable the interface to use it as router using
No switch port.

- Then enable VLANs interface and add their  IPs.

**17**
**IPS**
**pc6**

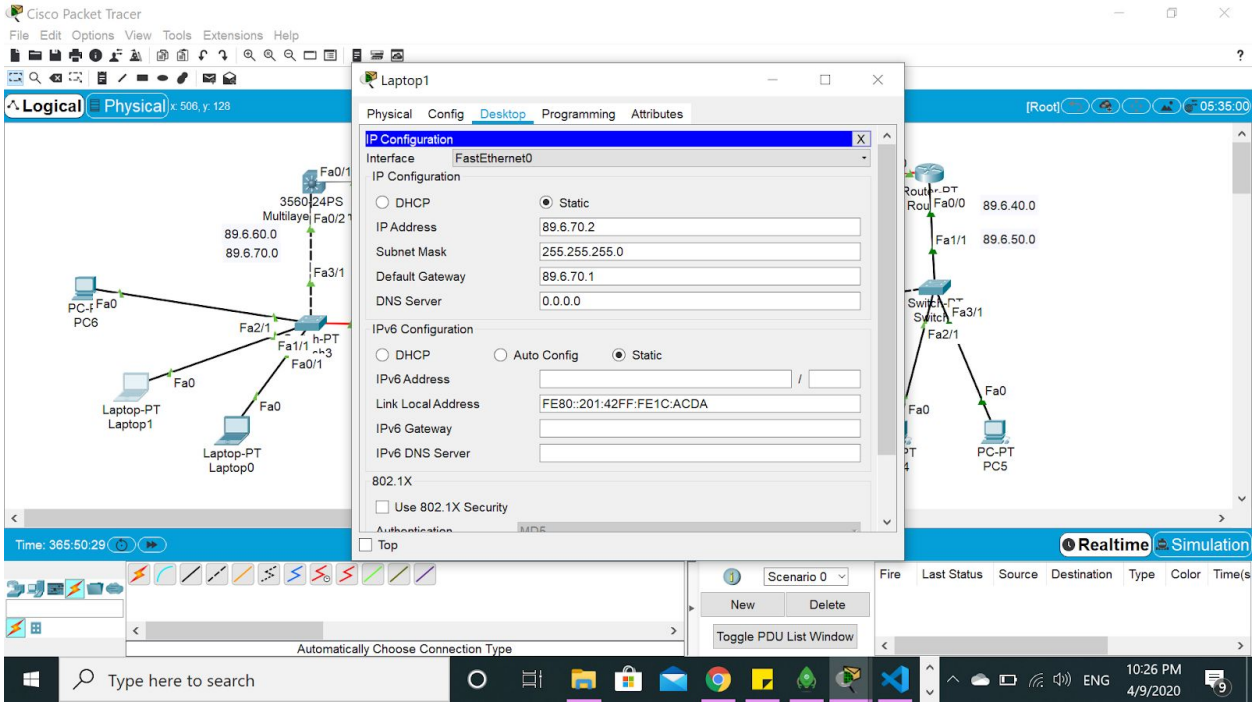



Laptop 0



**18**

Laptop 1




**19**

# Conclusion

In the experiments we used cisco packet tracer to implement different topologies .we have learned about Switches and how they connect devices together on a computer network by using packet switching how it reduces the traffic less than hubs, then we to talk about Router on Stick and VLANs and how it creates a network of devices.

We learned that VLANs enable logical grouping of end-stations that are physically dispersed and reduce the need to have routers and how to create a sub interface in routers and used then in a creative way.

We implemented it on the first topology and used the trunk port to transmit packets from different VLANs.

We learned about Layer 3 Switches how it can work as a router or as a switch, it advantages over a router in the way routing decisions performed. Then we learned about a Switch Virtual Interfaces which is a virtual interface created by dividing one physical interface into multiple logical interfaces.

We implanted 3 layer switches with sub-interfaces and show that it can reduce the amount of broadcast traffic and Simplified security management.

# References


**[1] “What is a Switch? - Definition from Techopedia,” Techopedia.com. [Online]. Available: http://www.techopedia.com/definition/2306/switch-networking. [Accessed: 22-april-2020].**

**[2] Admin, “How Does a Network Switch Work,” Fiber Optic Network Products, Accessed: 22-april-2020]. .**

**[3] orbitco, “What is Router-on-a-stick Inter-VLAN Routing ?,” orbit-computer-solutions.com,[Accessed: 22-april-2020].**

**[4] B. M. A. M. graduate who brings years of technical experience to articles on SEO, computers, and W. Networking, “What a VLAN Can Do for You and Your Business Computer Network,” Lifewire. [Online]. Available: https://www.lifewire.com/virtual-local-area-network-817357. [Accessed: 22-april-2020].**

**[5] “What is trunk? - Definition from WhatIs.com,” SearchNetworking. [Online]. Available: https://searchnetworking.techtarget.com/definition/trunk. [Accessed: 22-april-2020].**

**[6] “What is Subinterface? How to Configure Subinterface on Cisco Router.” .**

**[7] “Understanding Switch Virtual Interface – SVI - 62241 - The Cisco Learning Network.” [Online]. Available: https://learningnetwork.cisco.com/thread/62241. [Accessed: 22-april-2020].**

**[8] “What is a layer 3 switch and why would your network need it?,” TechGenix, 05-Oct-2018. [Online]. Available: http://techgenix.com/layer-3-switch/. [Accessed: 22-april-2020].**