**Laboratory Manual  
for**

**Computer Science and Engineering**

**Network and System security**

**Paper Code:** **PC- CSEP602CS**

**Credit: 3**

**No. of Periods / Week for a Group: 4**

**Computer Science and Engineering**

**List of Experiments**

|  |  |
| --- | --- |
| Experiment No. | Name of the Experiments |
| 1 | Introduction to CISCO packet tracer and associated tool box handling |
| 2 | Implementation of the Local Area Networks (LAN) using multiple HUB and SWITCH under different collision and broadcast domain approach. |
| 3 | Implementation of IEEE 802.11 Wireless LAN using Access point and networking devices along with wireless PDA. Verification of ARP and ICMP request from source to destination end. |
| 4 | Creation and validation of VLAN in segmented network environment. Verification of packet forwarding is restricted segment. |
| 5 | Verification of Routing Information Protocol – Delta Connection and Mesh Connection |
| 6 | Port security and MAC address filtering in LAN |
| 7 | Implementation of full secure hybrid VLAN with multiple IEEE 802.3 & IEEE 802.11network for data communication with RIP protocol at network layer and port security interface with layer 2 switch. |
| 8 | Introduction to access list and cisco firewall and configuring adaptive security appliance basic setting and firewall using CLI toplogy |

**Overall Safety for the Lab:**

This is a partial list of basic safety precautions to use when working on a computer:

* Remove your watch and jewelry and secure loose clothing.
* Turn off the power and unplug equipment before performing service.
* Cover sharp edges inside the computer case with tape.
* Never open a power supply unit (PSU) because a PSU has capacitors in it that have a large enough stored charge to seriously harm you. .
* Do not touch areas in printers that are hot or that use high voltage.
* Know where the fire extinguisher is located and how to use it.
* Keep food and drinks out of your workspace.
* Keep your workspace clean and free of clutter.

**Electrical devices have certain power requirements. For example, AC adapters are manufactured for specific laptops. Exchanging power cords with a different type of laptop or device may cause damage to both the AC adapter and the laptop.**

**Work Instruction**

**EXPERIMENT NO: CSEP602CS/1**

**NAME OF EXPERIMENT:** **Introduction to CISCO packet tracer and associated tool box handling**

**OBJECTIVE:To know the details of packet tracer simulator in OSI model and formation of network, connectivity, device handling, step by step simulation, inbound, out bound PDU verification etc.**

**TEORITICAL BACKGROUND:-**

The main purpose of Cisco Packet Tracer is to help students learn the principles of networking with hands-on experience as well as develop Cisco technology specific skills. Since the protocols are implemented in software only method, this tool cannot replace the hardware Routers or Switches. Interestingly, this tool does not only include Cisco products but also many more networking devices.Workspace :

1. Logical –  
   Logical workspace shows the logical network topology of the network the user has built. It represents the placing, connecting and clustering virtual network devices.
2. Physical –  
   Physical workspace shows the graphical physical dimension of the logical network. It depicts the scale and placement in how network devices such as routers, switches and hosts would look in a real environment. It also provides geographical representation of networks, including multiple buildings, cities and wiring closets.

**PRINCIPLE:-**

Using cisco packet tracer toolbox different networking devices are connected to form a network .Source terminal (Transmitter) sends ARP/ICMP packet to the network depends upon their protocol to all the devices (broadcasting). The device with correct IP address accepts the packet and all the other devices reject it. When multiple devices try to transmit packet together, It is observed that the packets are dropped during collision.

**TOOLS/APPARATUS REQUIRED:-**

1. Windows computer
2. CISCO packet tracer Software

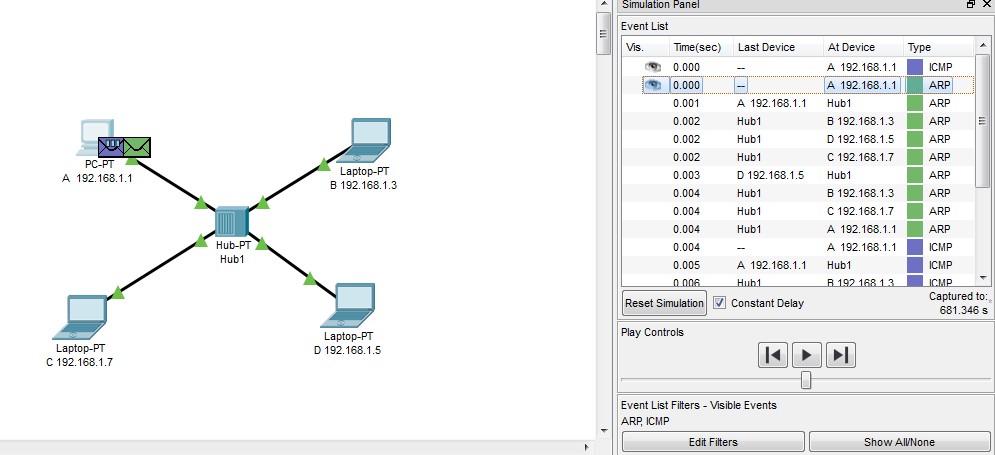
**PROCEDURE:**

1. Select hub and four end devices (laptop, pc etc) in CISCO packet tracer.

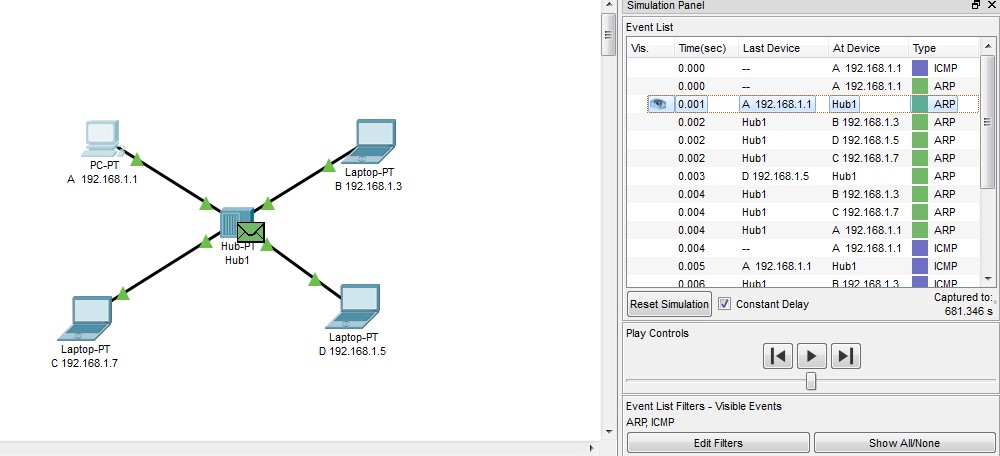
from cisco device toolbox

1. Rename the devices A, B, C, and D for our own understanding.
2. Connect end devices to the hub (Ethernet 0) with straight through cable.
3. Configure the IP addresses of the end devices.
4. Save the file and start simulation.
5. Edit filters to only ICMP and ARP.
6. Sent a simple PDU from device A to device D.
7. Observe the output.
8. Note down the inbound and outbound pdu and pdu information of the ICMP packets.
9. Observe the output.

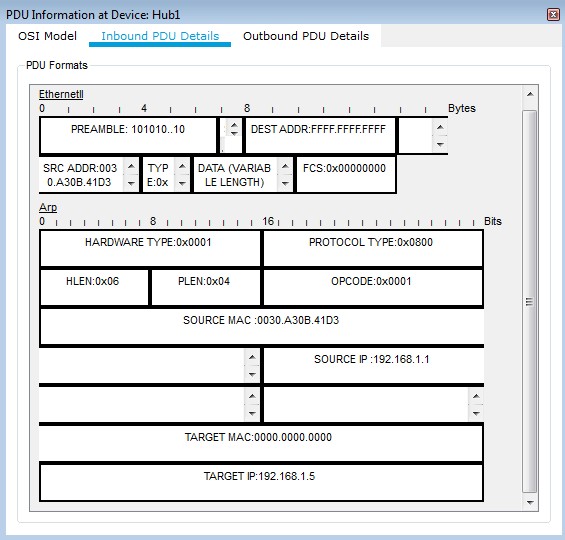
* **Result:** SPDU sending from A to D



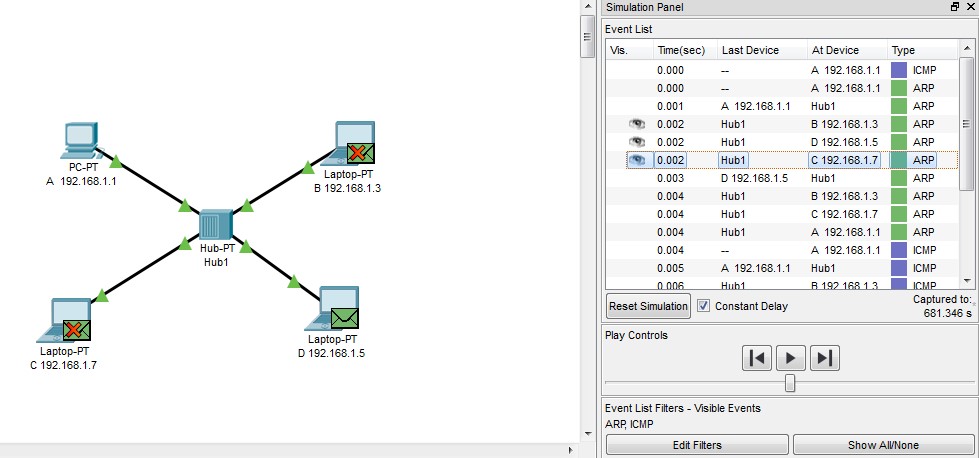
* ARP request sent from A to Hub.



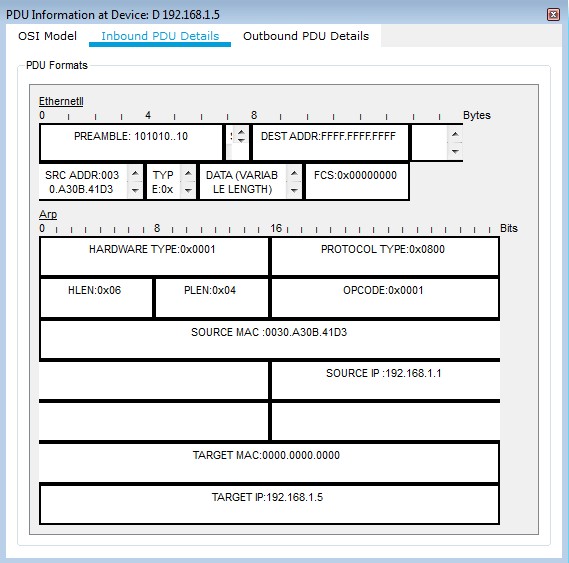
Pdu information at Hub



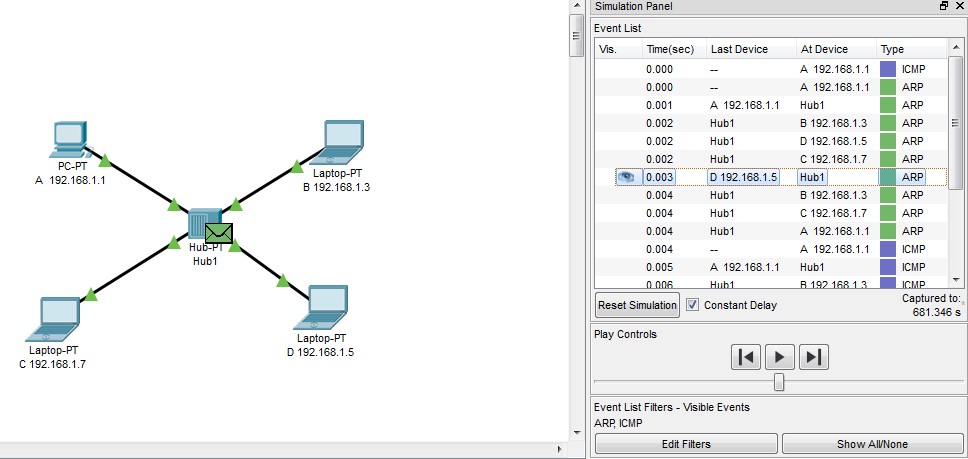
* ARP request is sent from Hub to all devices.



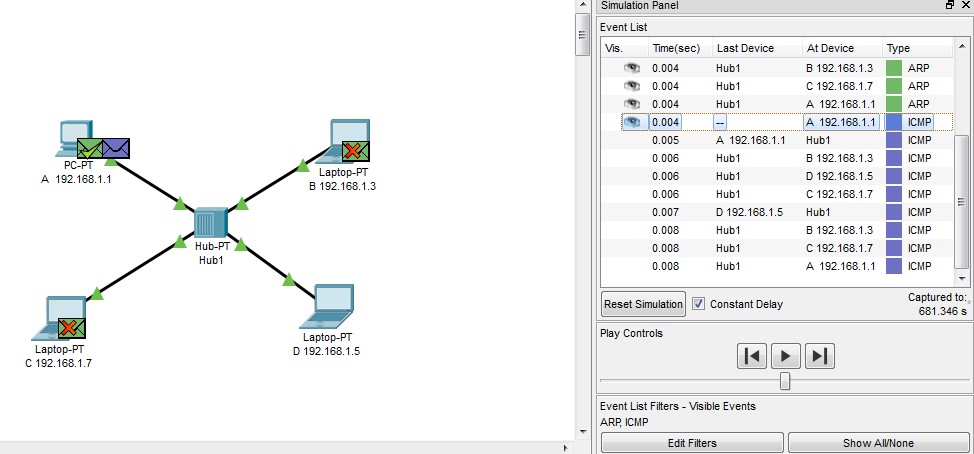
Inbound PDU information at D. Here, source is A, and destination is D.



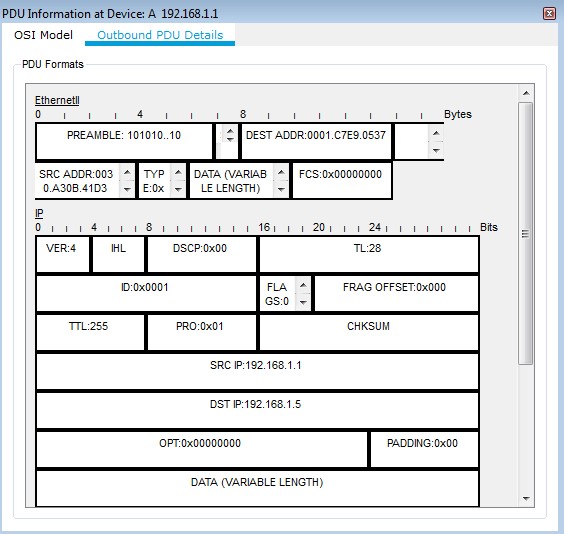
* D sends response back to Hub



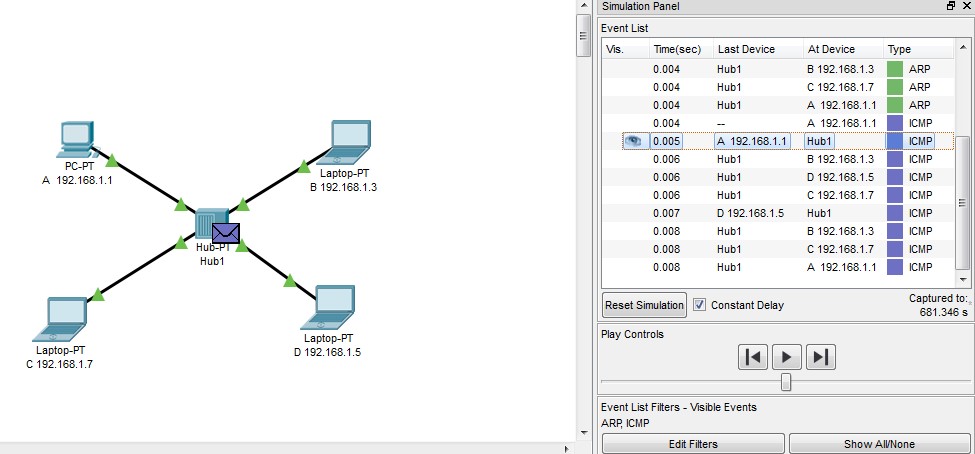
Hub send the ICMP packet to A



* Outbound pdu information at A



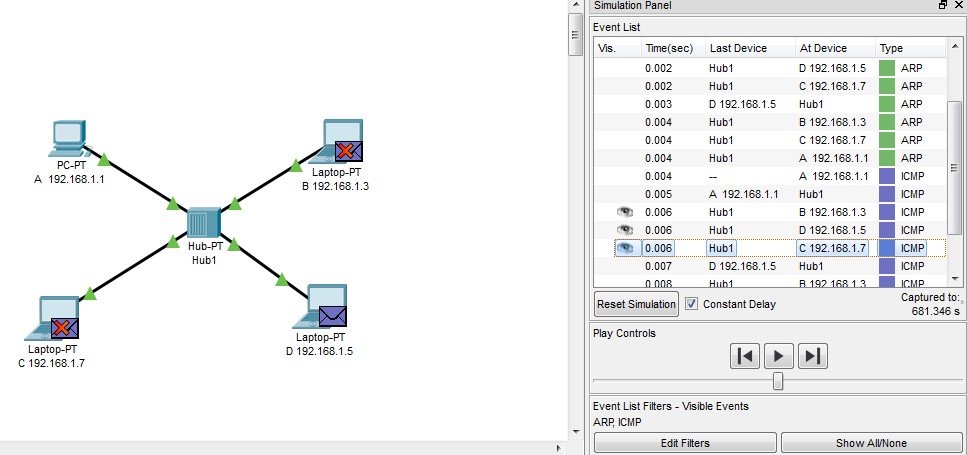
ICMP packet sent from A to Hub



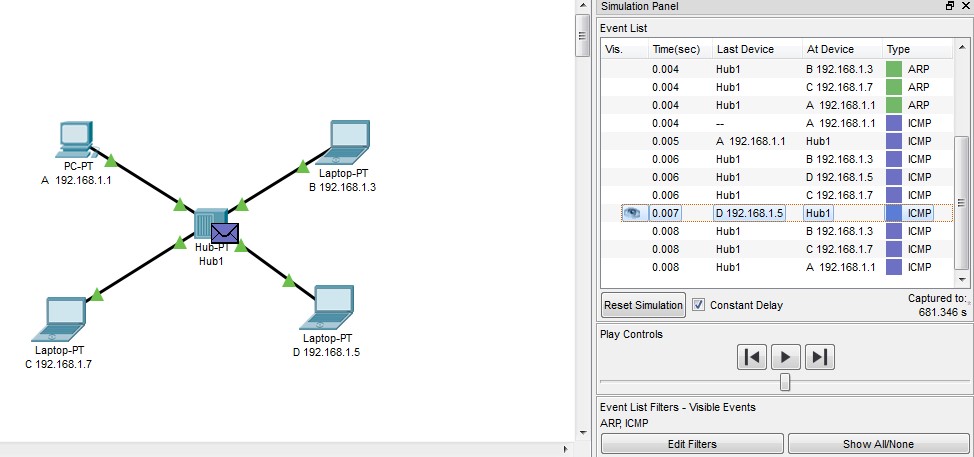
* PDU information at A.



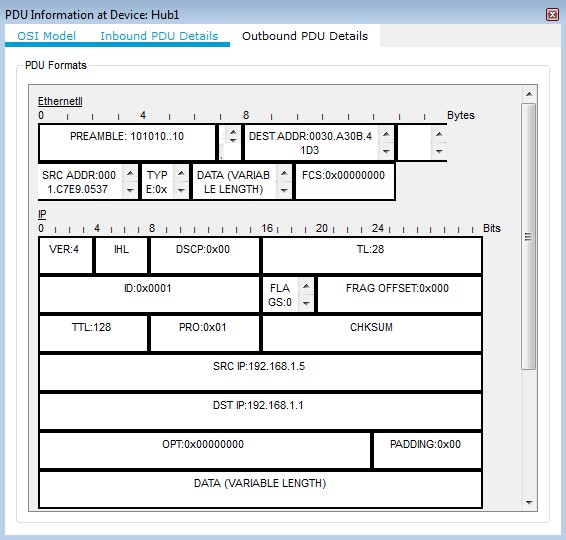
ICMP packet sent from hub to all devices.



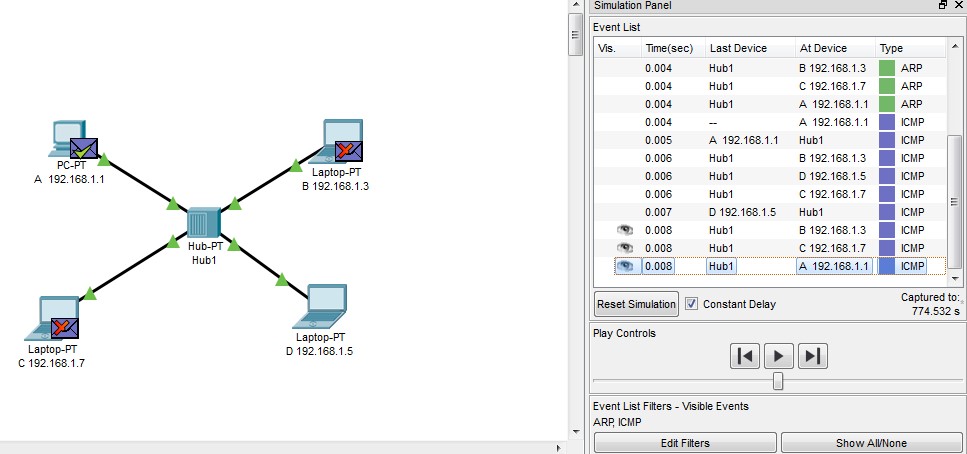
* D sends acknowledgement to A via Hub



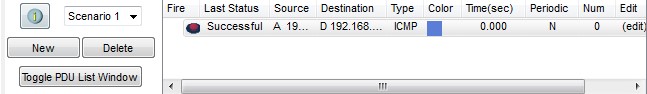
Inbound pdu details at Hub



* Finally, A accepts the acknowledgement.



* Transmission from A to D is successful.

**DISCUSSION:**

During simulation each interfaces can be verified by inbound and out bound PDU transfer and thereby ensures efficient packet delivery. It may observed some times buffer full during simulation.

**EXPERIMENT NO: CSEP602CS/2**

**NAME OF EXPERIMENT:**  Implementation of the Local Area Networks (LAN) using multiple HUB and SWITCH under different collision and broadcast domain approach.

**OBJECTIVE:**

To interconnect multiple LAN using Cisco hub and 2960 switch to verify that

1. Hub works on a single collision and broadcast domain
2. Therefore most of the packet will be dropped during simultaneous packet transmission
3. Switch works on multiple collision domain and single broadcast domain
4. Therefore network collision can effectively controlled by suitable network architecture.

**TEORITICAL BACKGROUND:-**

Collision Domain –

A Collision Domain is a scenario in which when a device sends out a message to the network, all other devices which are included in its collision domain have to pay attention to it, no matter if it was destined for them or not. This causes a problem because, in a situation where two devices send out their messages simultaneously, a collision will occur leading them to wait and re-transmit their respective messages, one at a time. Remember, it happens only in the case of a half-duplex mode.

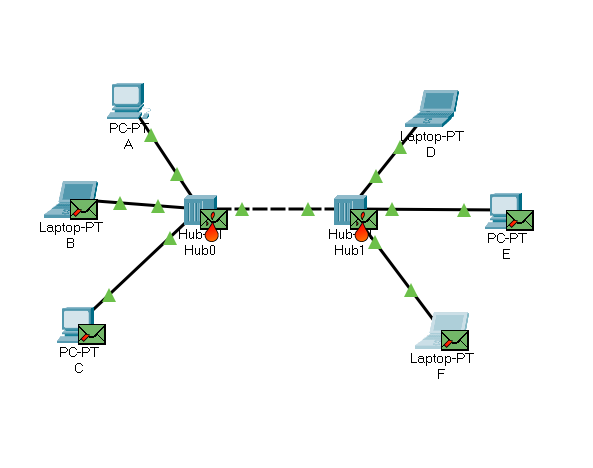
Broadcast Domain –

A Broadcast Domain is a scenario in which when a device sends out a broadcast message, all the devices present in its broadcast domain have to pay attention to it. This creates a lot of congestion in the network, commonly called LAN congestion, which affects the bandwidth of the users present in that network.

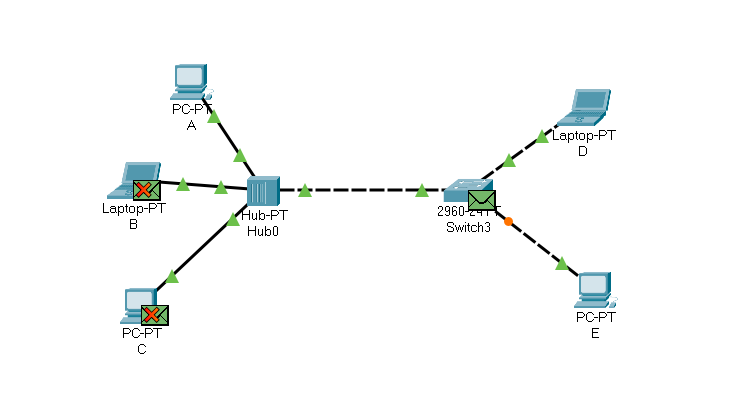
From this, we can realize that the more the number of collision domains and the more the number of broadcast domains, the more efficient is the network providing better bandwidth to all its users.

**Results**

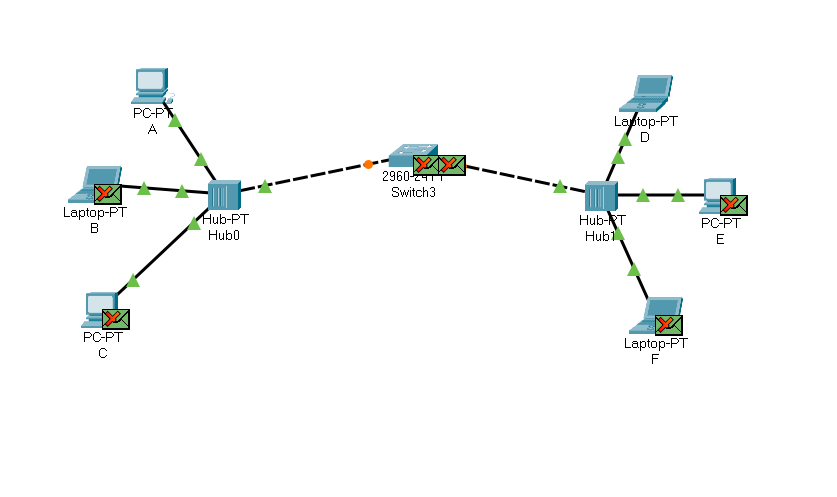
**Senario: 1**



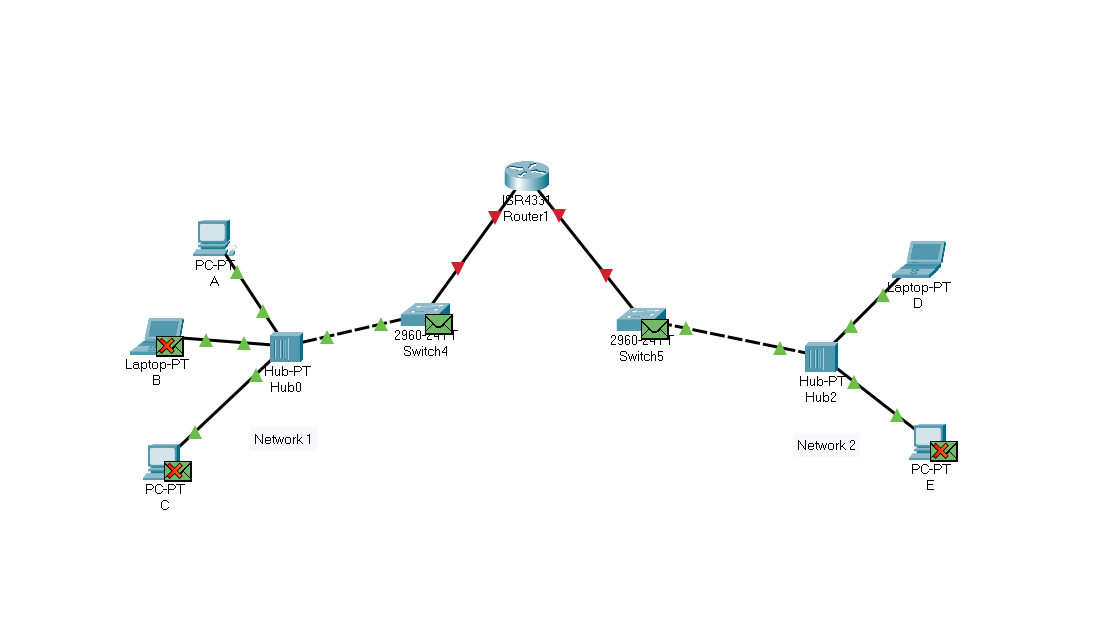
**Senario: 2**



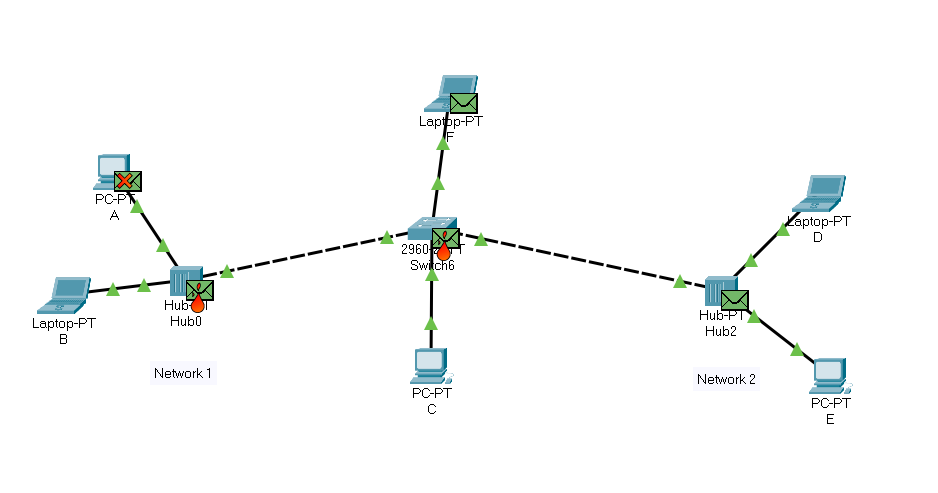
**Senario: 3**



**Senario: 4**



**Senario: 5**



**Discussion:**

In case of packet transmission using hub, we have seen that multiple packets from multiple source to multiple destination cannot be transmitted due to hub’s single collision domain i.e. packets will be lost. But switch has multiple collision domains, so it can transmit multiple packets from multiple sources to multiple destinations using time sharing technique i.e. there will always be some delay between two transmissions.

**EXPERIMENT NO: CSEP602CS/3**

**NAME OF EXPERIMENT:-** Implementation of IEEE 802.11 Wireless LAN using Access point and networking devices along with wireless PDA. Verification of ARP and ICMP request from source to destination end.

**OBJECTIVE:-**

1. Setting up a wireless Lan using Access point and number of n devices (wired and wireless).
2. Interconnection of IEEE802.11 and IEEE802.3 through CISCO2960 switch.

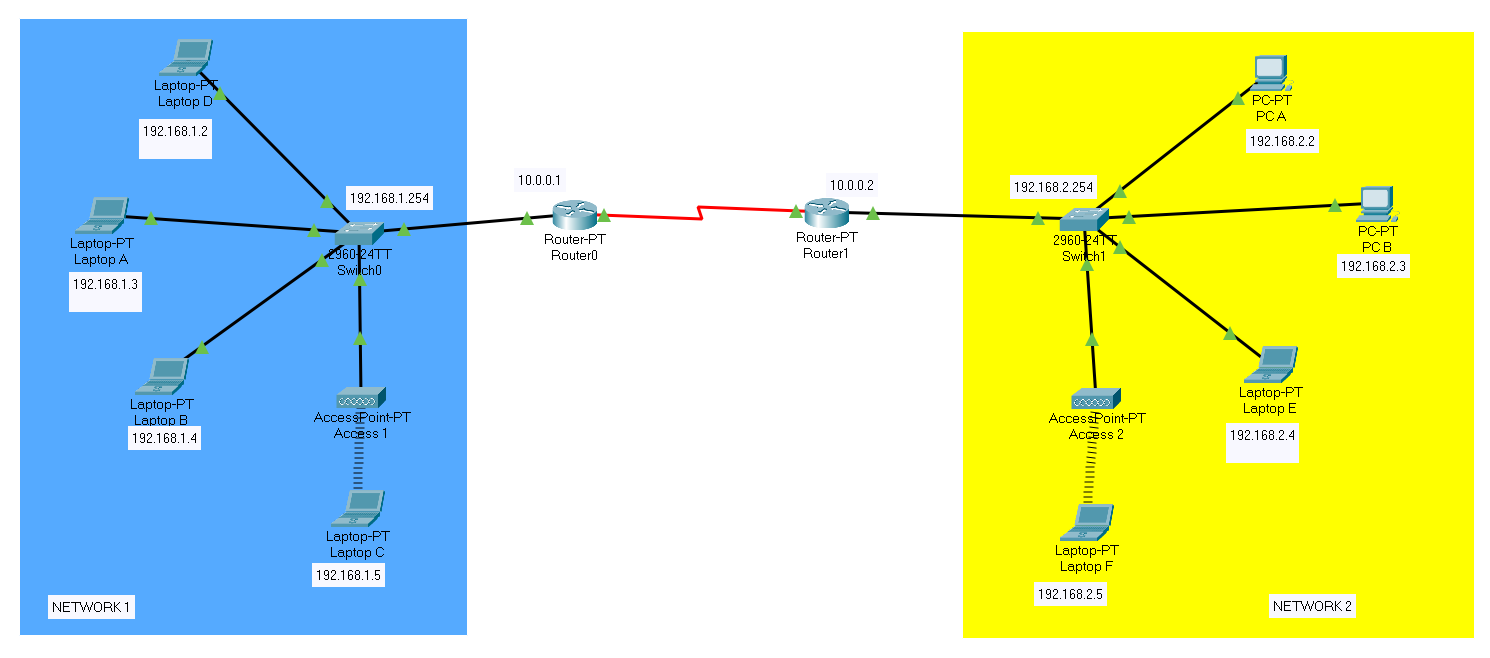
Interworking between two wired and wireless networks via CISCO router using RIP protocol.

**TEORITICAL BACKGROUND:-**

Wireless LAN stands for Wireless Local Area Network. It is also called LAWN (Local Area Wireless Network). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.The IEEE 802.11 group of standards defines the technologies for wireless LANs. For path sharing, 802.11 standard uses the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance). It also uses an encryption method i.e. wired equivalent privacy algorithm.Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.

**RESULT:-**

**Scenario:1**



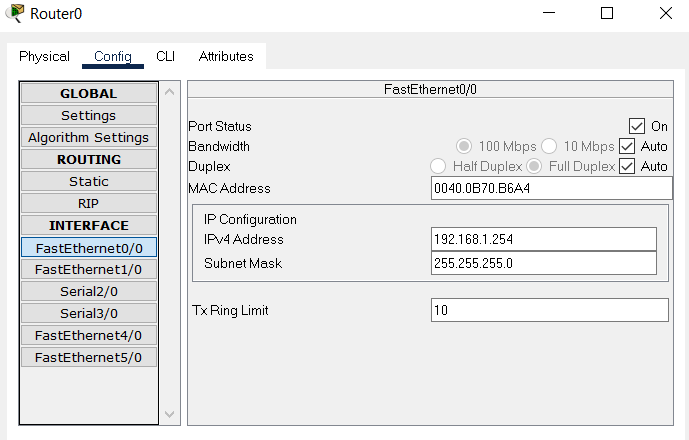
**Steps:**

1. After connecting all devices and giving their respective IP and gateway addresses

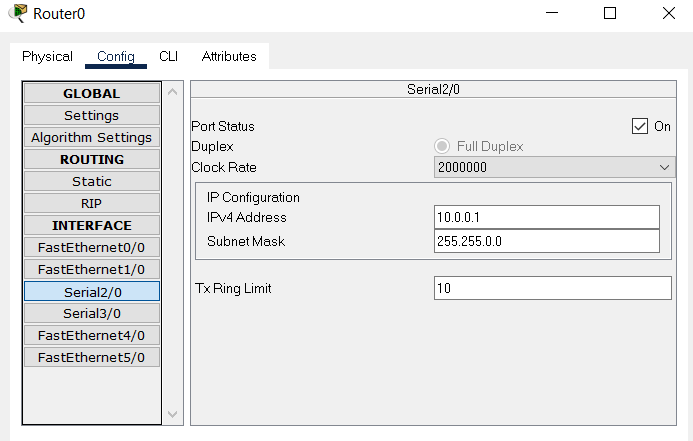
follow these steps.

1. Configuring router 0 :

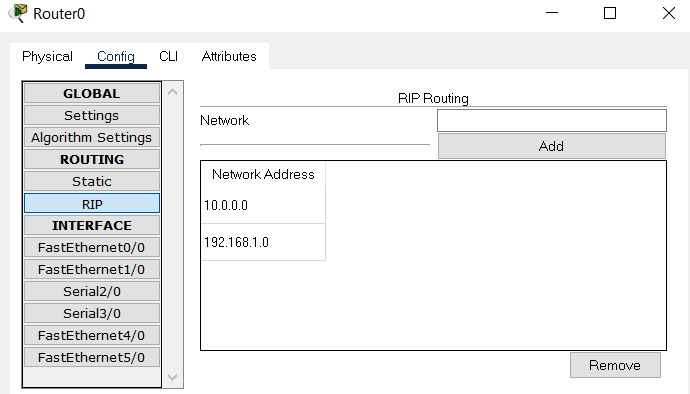
* For input port :



* For output port :

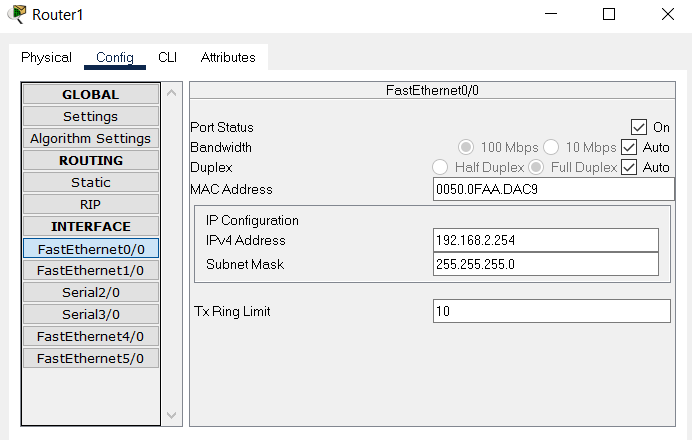


* Set RIP :

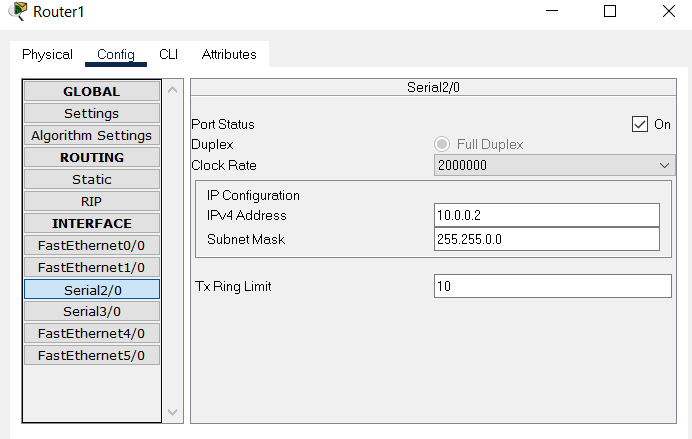


1. Similarly configuration of router 1:

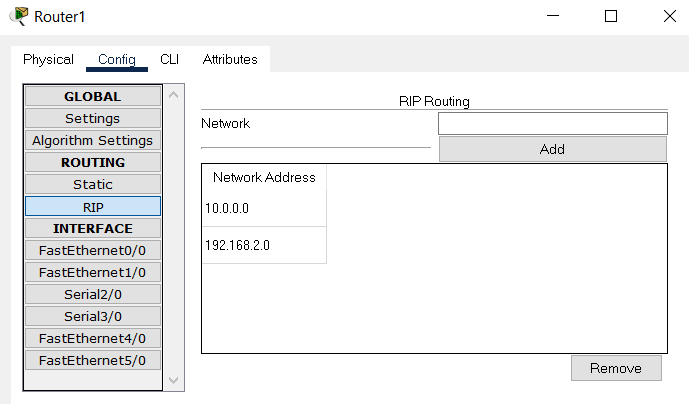
* For input port :

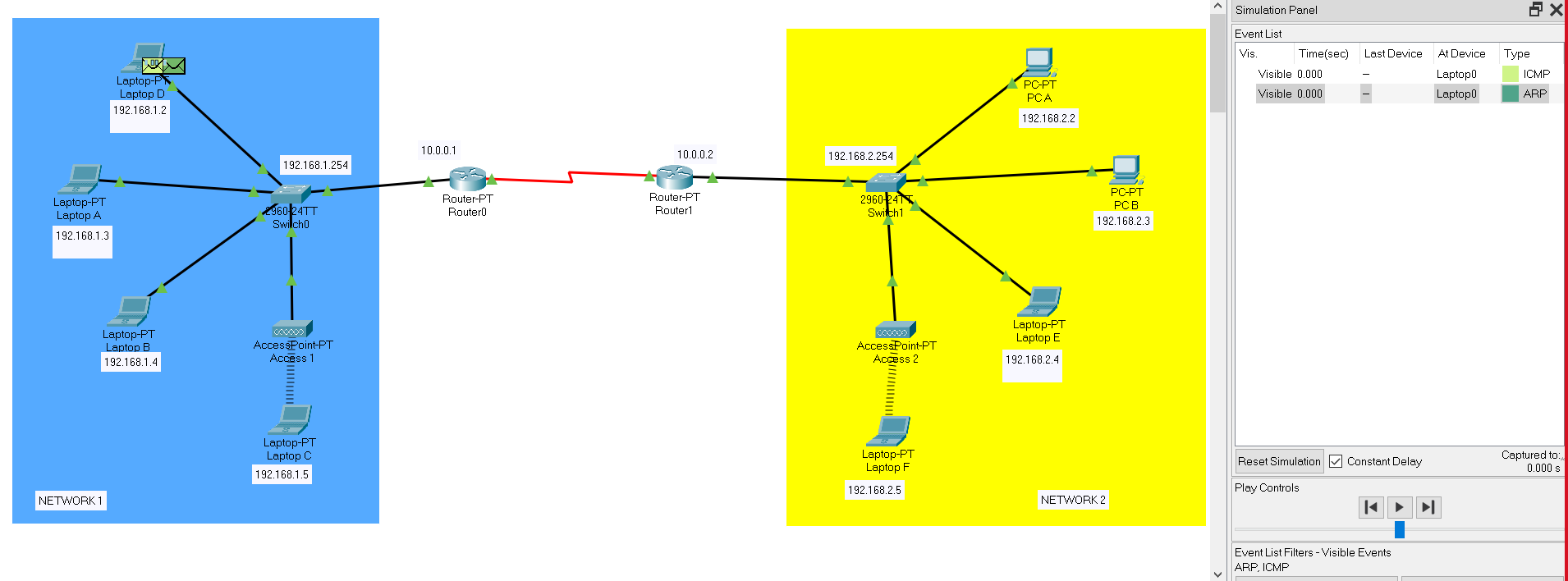


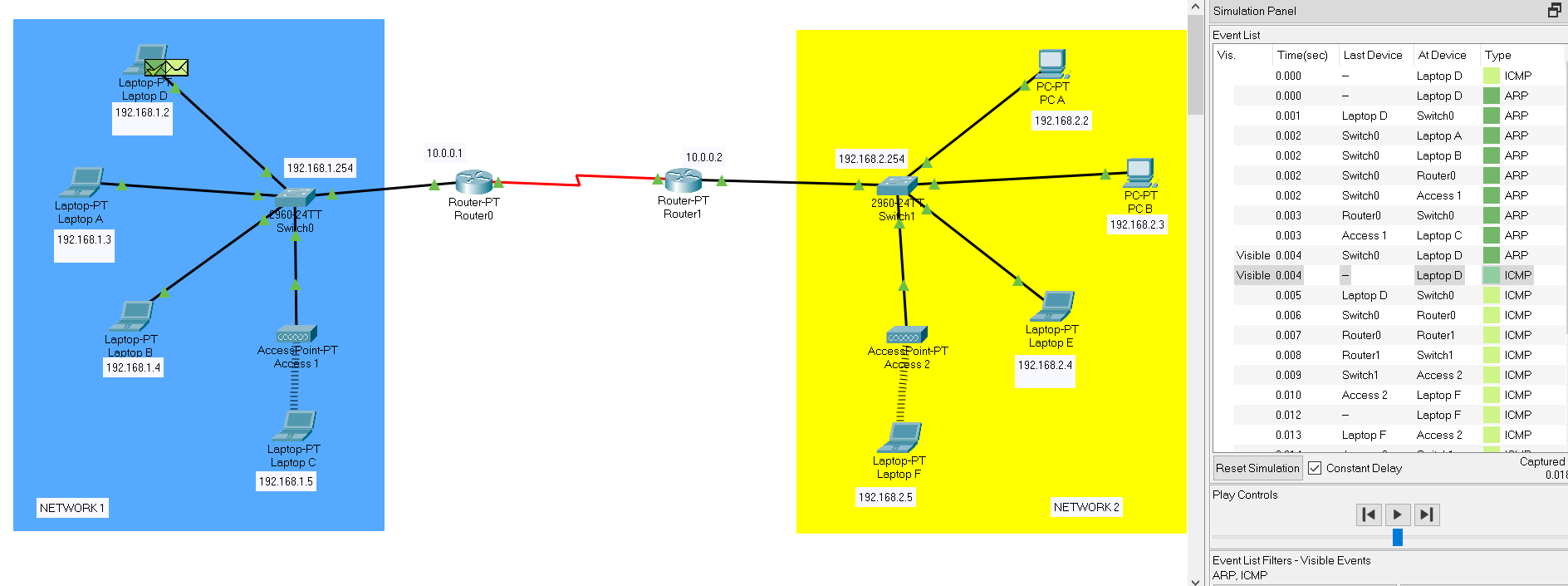
* For output port :



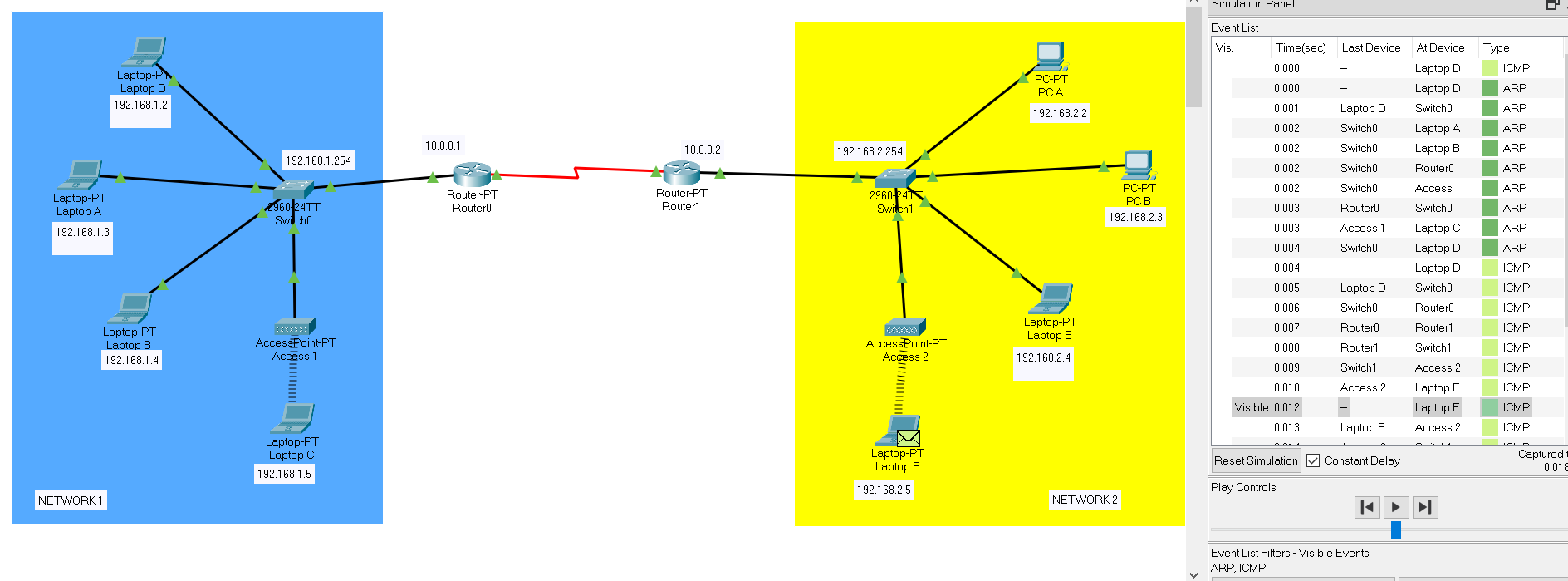
* Set RIP :

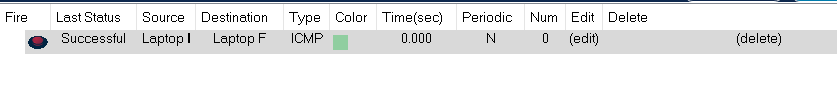


1. Start simulation (edit filters and select ARP, ICMP).
2. Now, send simple PDU from Laptop D of NETWORK 1 to Laptop F of NETWORK 2.
3. ARP response is received by Laptop D from Switch 0. Now Laptop D is ready to transmit ICMP.



1. ICMP is sent from router 0 to router 1.
2. ICMP is finally received by Laptop F from router 1 via Switch 1 and access point 2.



1. ICMP response is received by Laptop D from Laptop F via access point 2, Switch 1, router 1, router 0 and Switch 0.
2. Now the transmission is successfully completed.

**Discussion:**

In this experiment, as usual we have provided all the IPs and also configured both routers with RIP with net id of both networks, so that the RIP can work and data can be transmitted and also connected two access points in those two network. We were also able to interwork between two wired and wireless network. In this way we have successfully completed our experiment. Now, if we delete those two net ids from router RIP config, we will see the routers will constantly send RIPv1 to both networks to know the net id, and transmission will be failed.

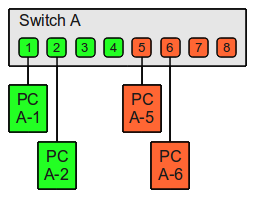
**EXPERIMENT NO: CSEP602CS/4**

NAME OF EXPERIMENT:- Creation and validation of VLAN in segmented network environment. Verification of packet forwarding is restricted segment.

OBJECTIVE:

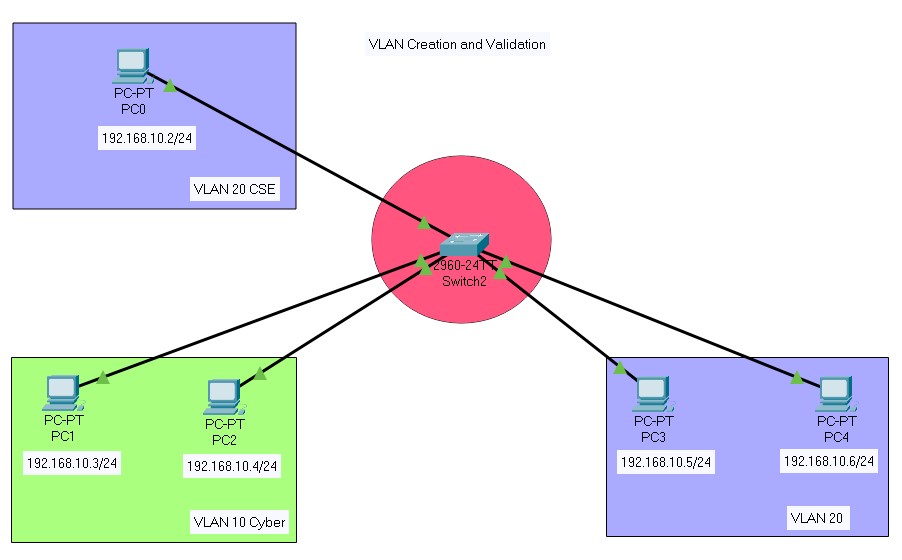
1. Creation of VLAN using CISCO 2960 Switch
2. Using Switch CLI configure VLAN 10 and VLAN 20
3. Verify packet forwarding is restricted in each VLAN

TEORITICAL BACKGROUND:- Virtual Local Area Networks (VLANs) divide a single existing physical network into multiple logical networks. Thereby, each VLAN forms its own broadcast domain. Communication between two different VLANs is only possible through a router that has been connected to both VLANs. VLANs behave as if they had been constructed using switches that are independent of each other.



Simulation Results:-

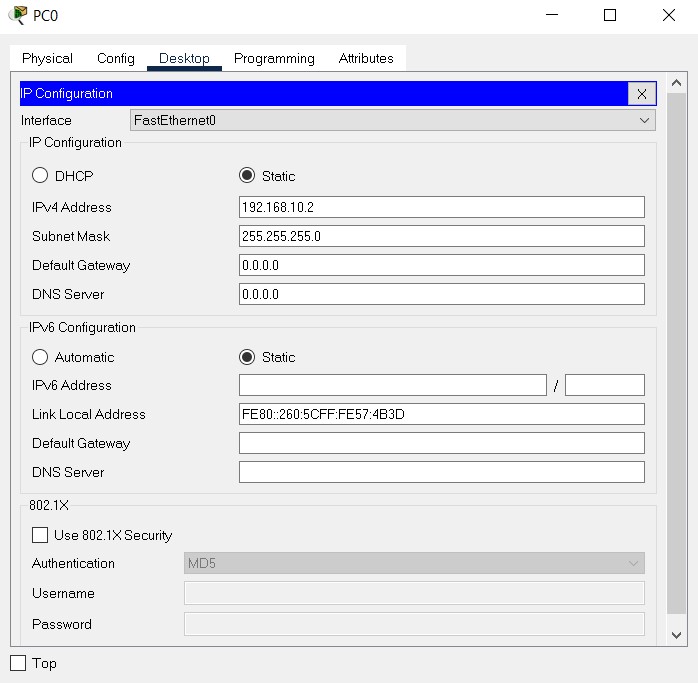
**Model:**

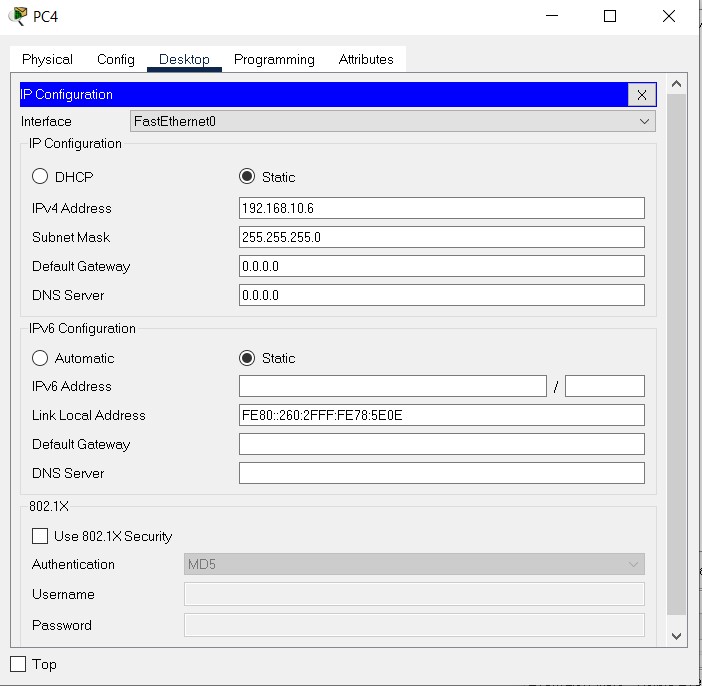
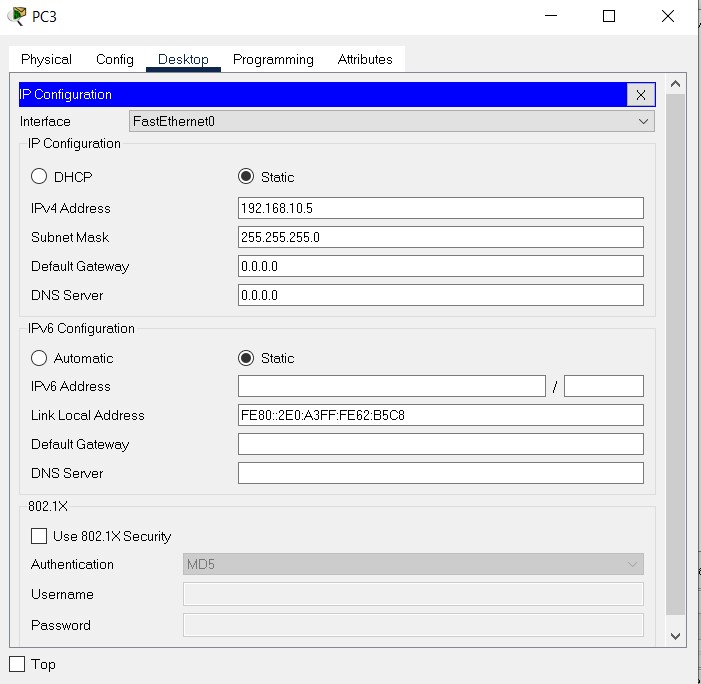
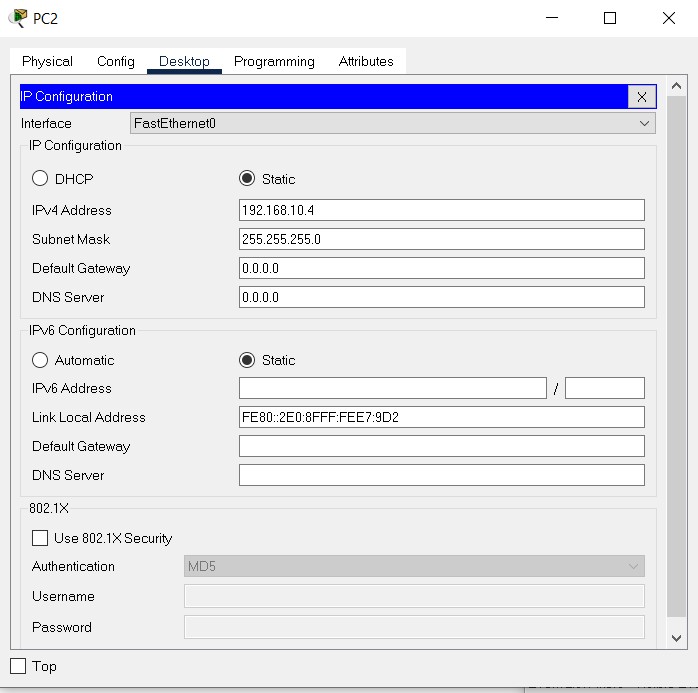
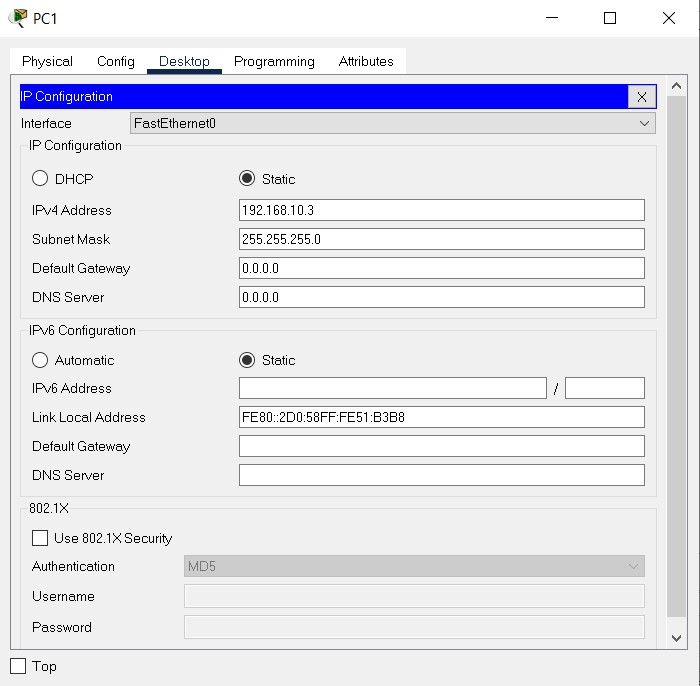


**Procedure:**

* 1. Connect the PCs to Switch 2960 using copper straight through cable and separate the PCs into 2 segments VLAN 10 and VLAN 20. Assign IP address to all devices.
  2. Open CLI of switch 2960 and run commands to configure VLANs.
  3. Next, we will simulate transmission within the VLANs as well as between the VLANs and check if we successful in restricting transmission between VLAN 10 and VLAN 20.

**Assigning IP address to all PCs:**

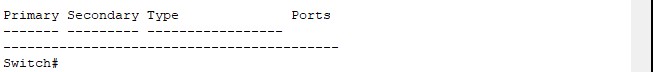
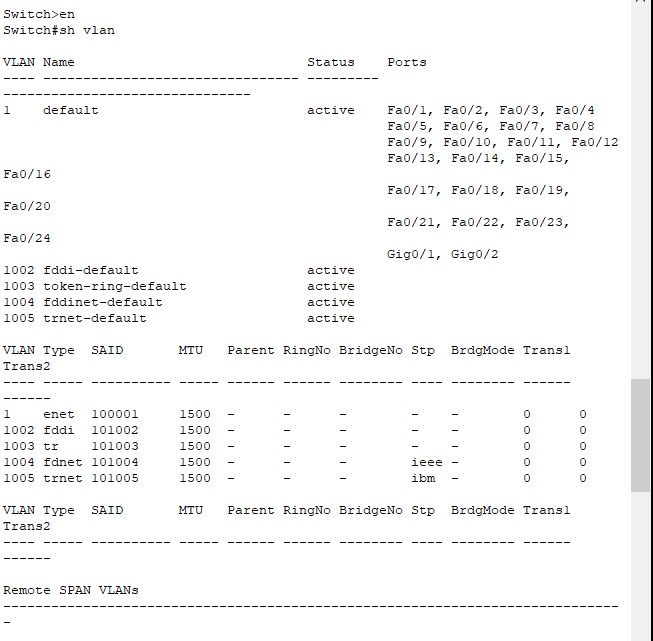




**Commands:** Open CLI of 2960 switch0

Switch>en

Switch#sh vlan



**Currently no VLAN has been created**

Command

Switch#config t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 10

Switch(config-vlan)#name Cyber

Switch(config-vlan)#exit

Switch(config)#vlan 20

Switch(config-vlan)#name CSE

Switch(config-vlan)#exit

Switch(config)#interface fa0/1

Switch(config-if)#switchport access vlan 20

Switch(config-if)#exit

Switch(config)#interface fa0/4

Switch(config-if)#switchport access vlan 20

Switch(config-if)#exit

Switch(config)#interface fa0/5

Switch(config-if)#switchport access vlan 20

Switch(config-if)#exit

Switch(config)#interface fa0/2

Switch(config-if)#switchport access vlan 10

Switch(config-if)#exit

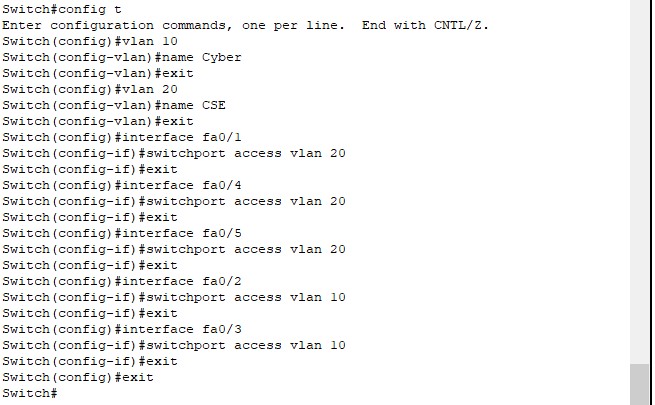
Switch(config)#interface fa0/3

Switch(config-if)#switchport access vlan 10

Switch(config-if)#exit

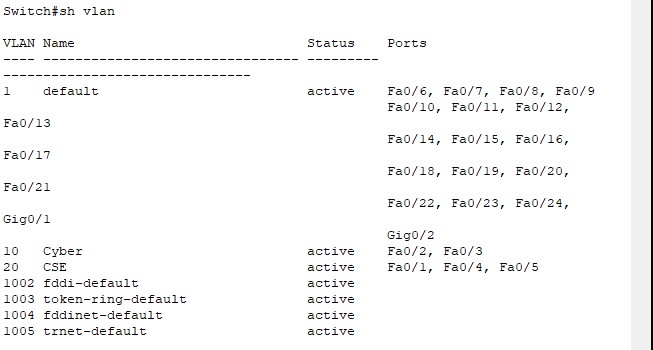
Switch(config)#exit

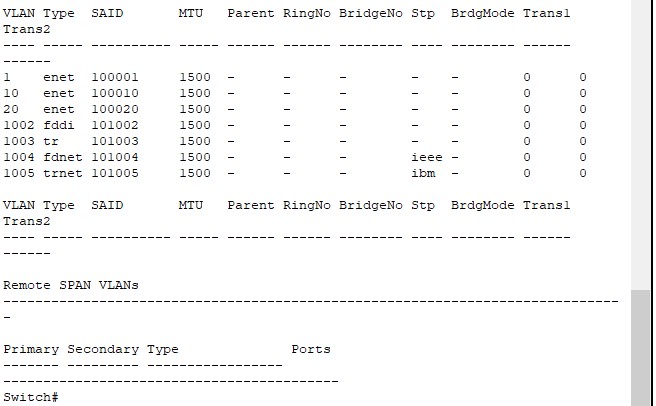
Switch#



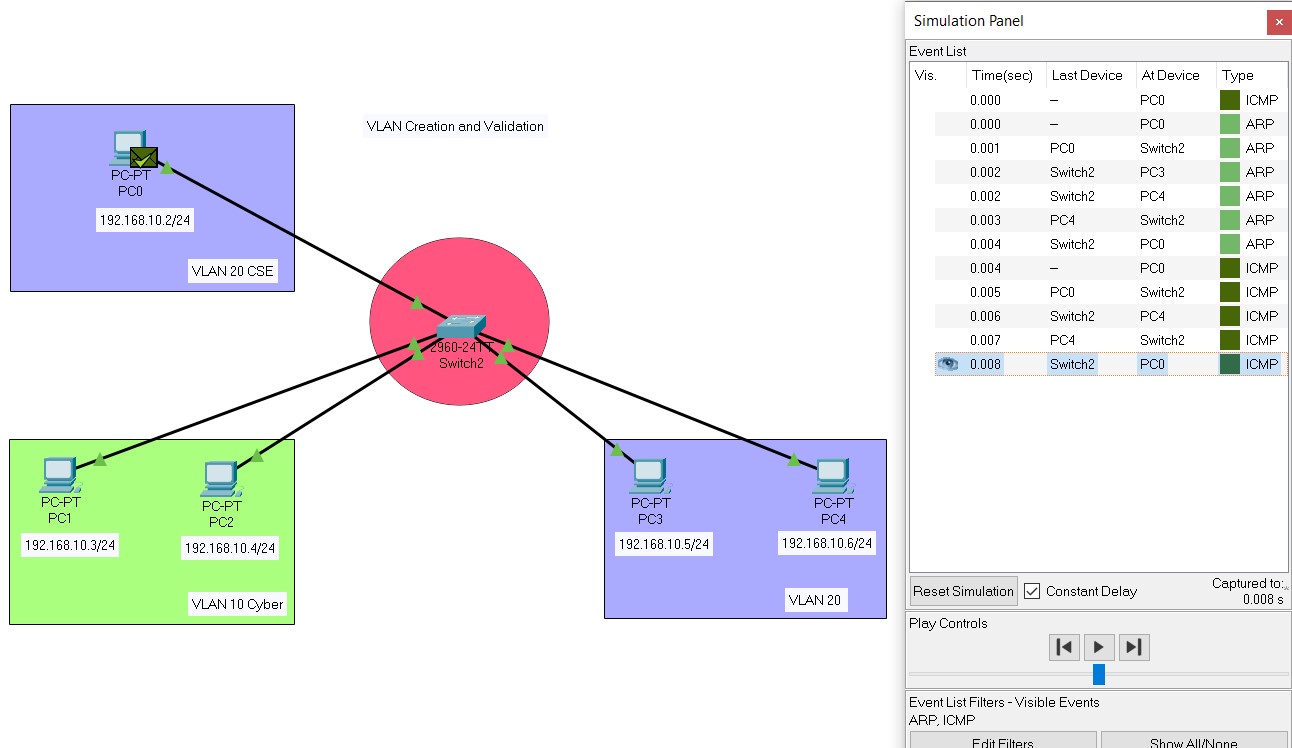
**VLAN has been created we will now check by following command:**

Switch#sh vlan

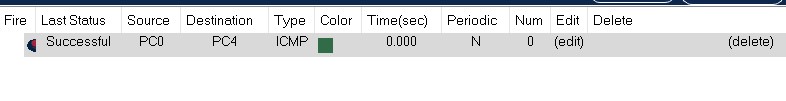




## I. Transmission within VLAN 20 from PC0 to PC4

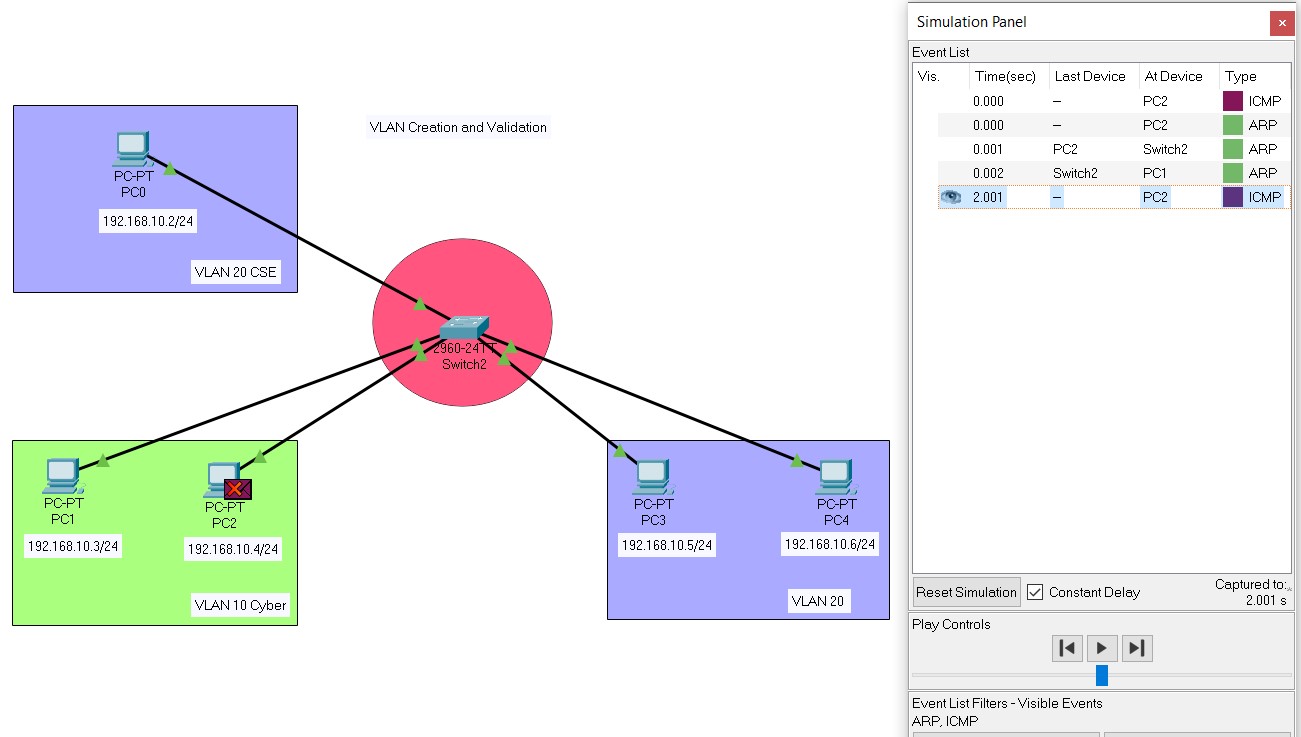


**Result:**

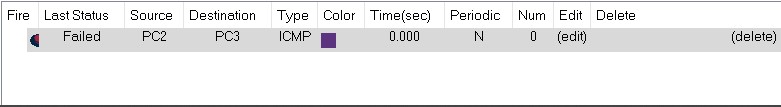


Transmission is successful

II. Transmission from VLAN 10 (PC2) to VLAN 20 (PC3)

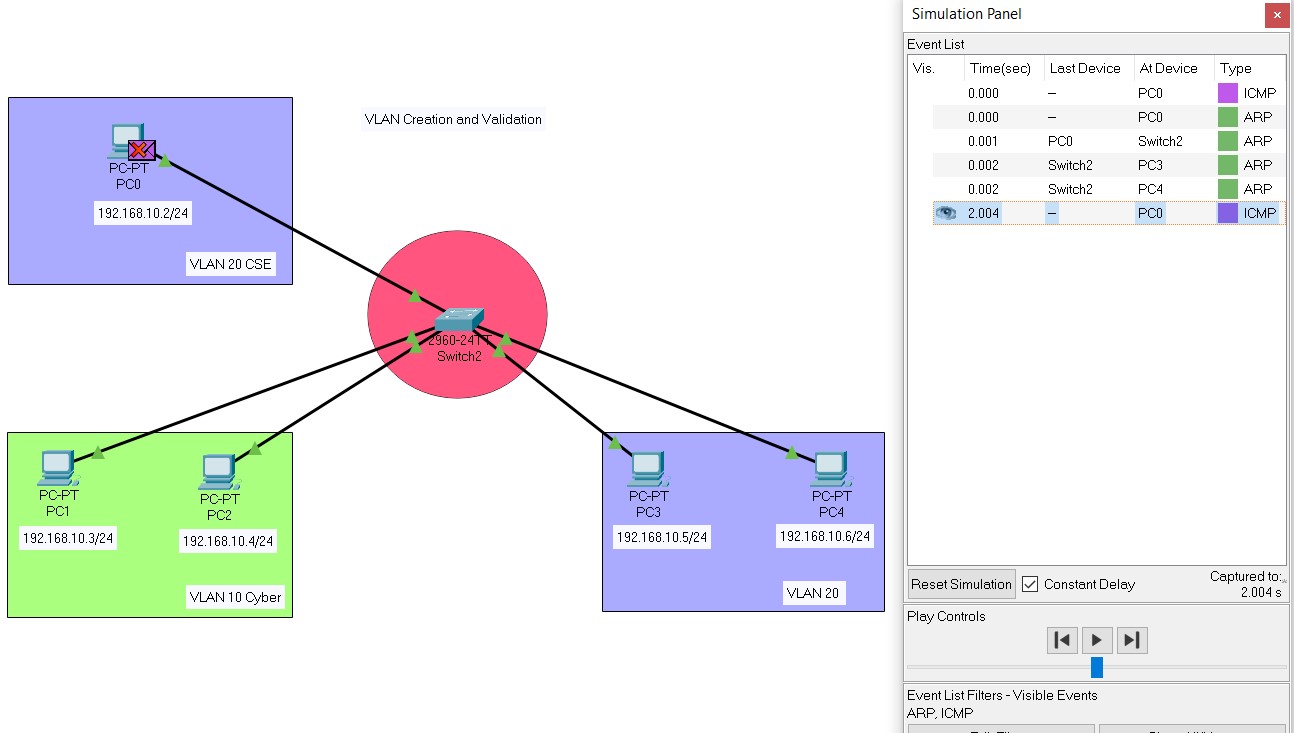


**Result:**

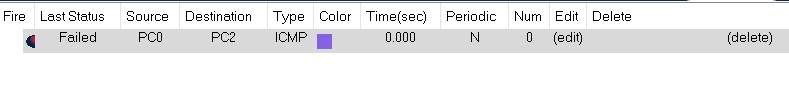


## Transmission failed We have successful restricted transmission between VLAN 10 and VLAN 20

III. Transmission from VLAN 20 (PC0) to VLAN 10 (PC2)



**Result:**



Transmission failed

We have successful restricted transmission between VLAN 10 and VLAN 20

**Discussion**

* Configuration of VLANs reduces network traffics.
* Adds more security while restricting other networks or data loses.

**EXPERIMENT NO: CSEP602CS/5**

NAME OF EXPERIMENT:- Verification of Routing Information Protocol (RIP) – Delta Connection and Mesh Connection.

1. OBJECTIVE: Validation of RIP protocol in delta network
2. Validation of RIP protocol in mesh network

TEORITICAL BACKGROUND:-

The Routing Information Protocol (RIP), which uses the hop count as a routing measure, is one of the oldest distance-vector routing technologies. RIP eliminates routing loops by restricting the number of hops permitted in a path from source to destination.RIP permits a maximum of 15 hops, which limits the size of networks that can be supported by the protocol.

**Open Shortest Path First (OSPF)**

OSPF is an Internet Interior Gateway Protocol (IGP) that distributes IP routing information in an IP network over a single Autonomous System (AS).OSPF is a link-state routing protocol, which means that routers exchange topological information with their closest neighbors.OSPF is one of the several Interior Gateway Protocols (IGPs) designated by the Internet Engineering Task Force (IETF), which are protocols aimed at the traffic moving around within a more extensive autonomous system network, such as a single enterprise's network, which may be made up of many separate local area networks linked through routers.The OSPF routing system has essentially replaced the older Routing Information Protocol (RIP) in business networks. When an OSPF router learns of a routing table modification or detects a change in the network, it multicasts the information to all other OSPF hosts in the network, ensuring that everyone gets the same routing table information.

# Assigning default gateway

# 

Assigning routers with IP

# 

# 

# 

# Configuring RIP

# 

# 

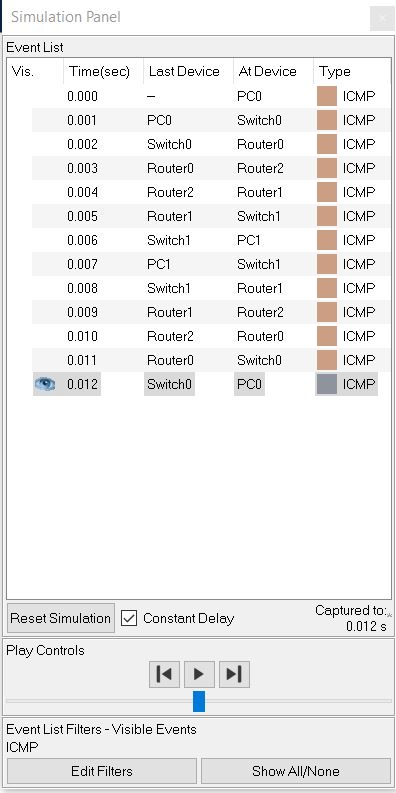
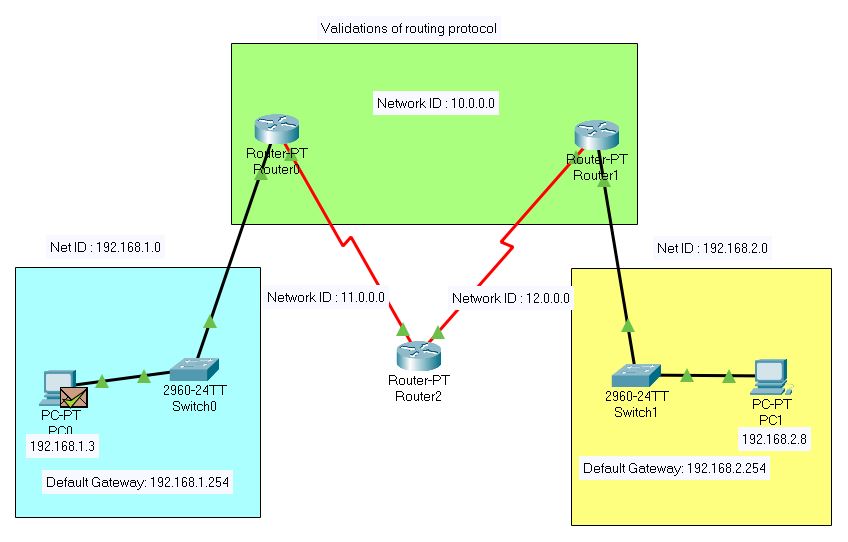
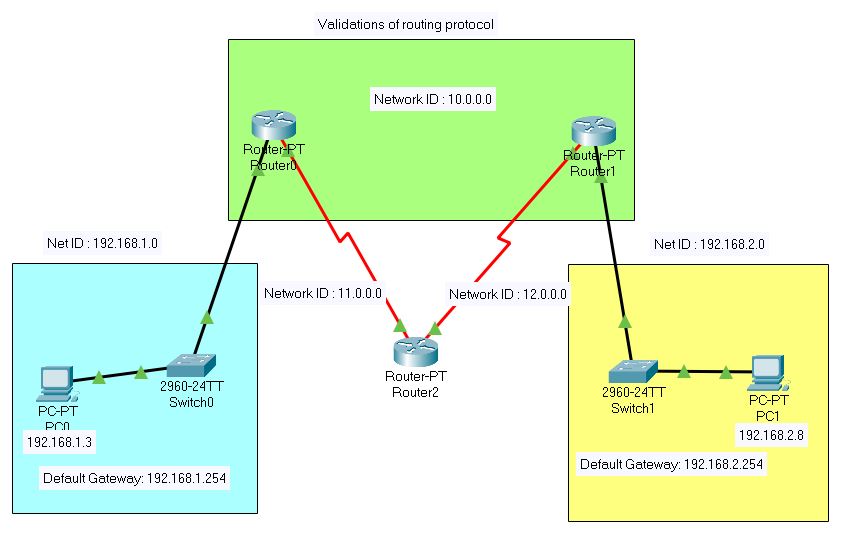
# **Simulation :**Delta Network

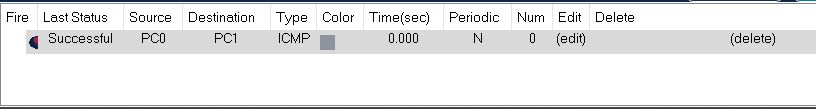
# CASE 1:-

# 

# 

CASE 2 – when the previous connection fails

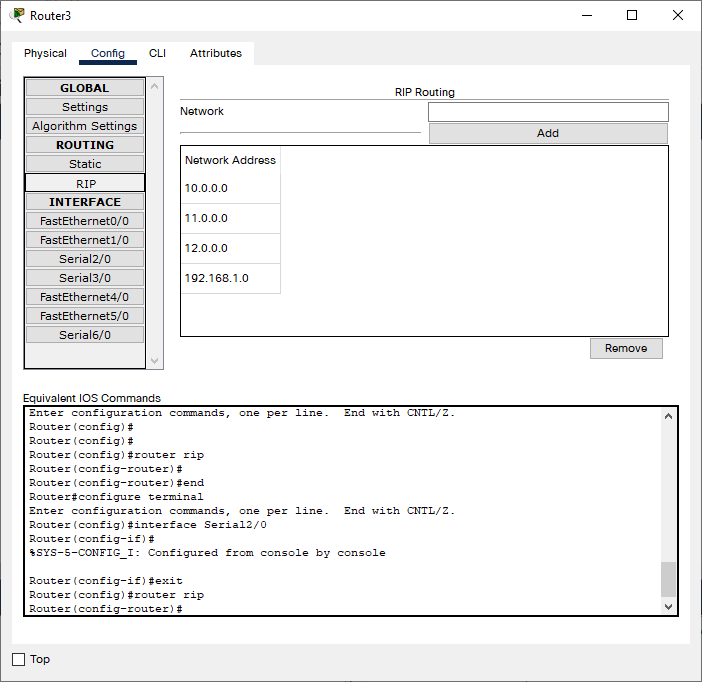




Successful. Hence the network is working properly

# **Mesh Network**

# **Configuration of RIP**

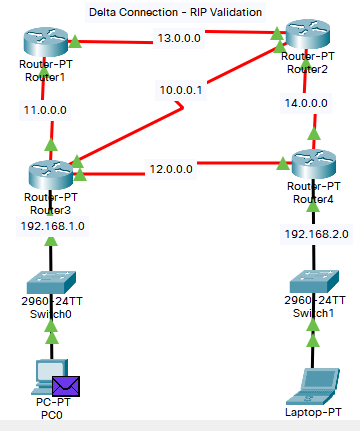


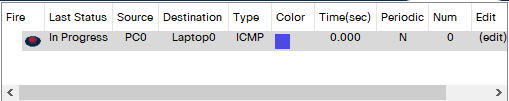
# 

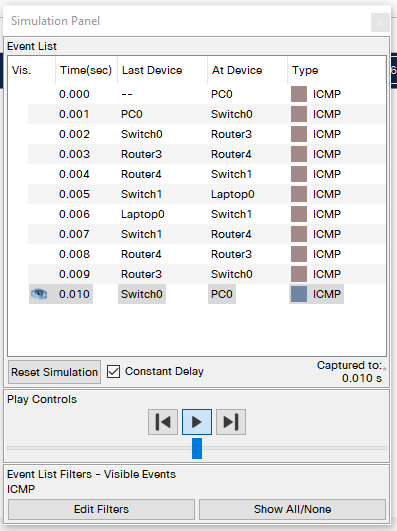
# 

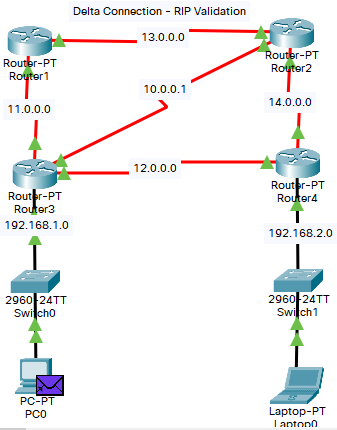
**Simulation Result :-**

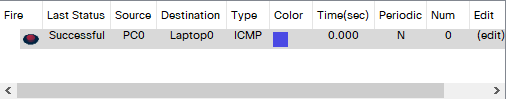
Case 1: R3 to R4 normal mode



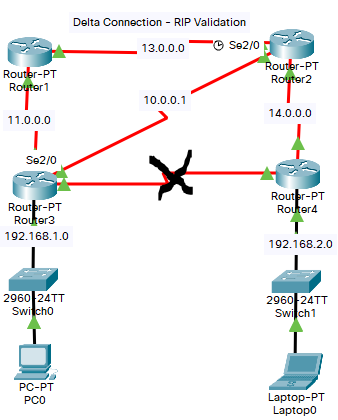




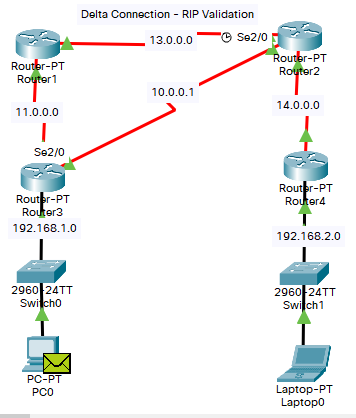


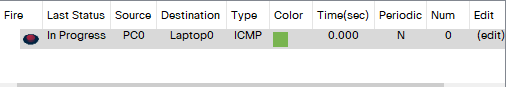


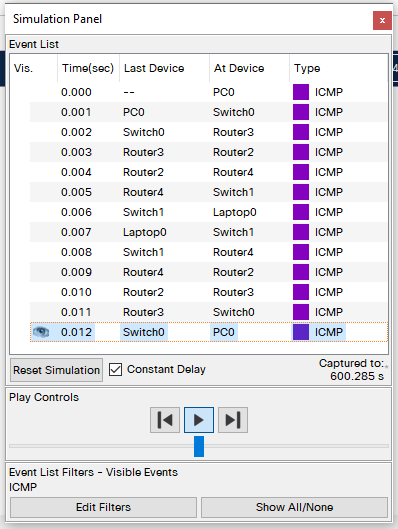
Case 2 : R3 , R2 , R4 , when case 1 is failed to connect

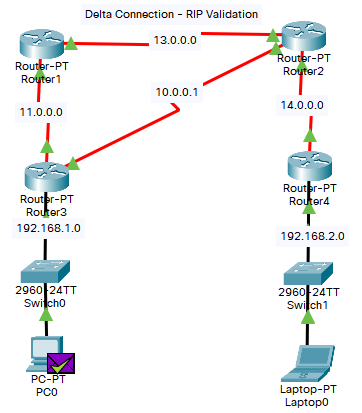


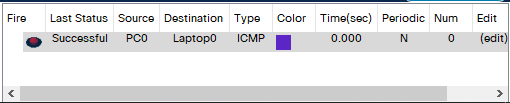
When there is a problem between the connection of Router3 and Router4











Discussion

1. RIP configuration must be done correctly to make it work properly.
2. Routing Information Protocol results in increased network traffic due to the checks and updates it performs on neighboring routers every 30 seconds.
3. RIP only updates neighboring routers

**EXPERIMENT NO: CSEP602CS/06**

**NAME OF EXPERIMENT**:- Port security and MAC address filtering in LAN

OBJECTIVE:

1.To know the CLI interface of Cisco switch with variety of command

2. To connect the multiple end device to switch port with sticky MAC address security

3. Verification of secure connection with third party end device connection

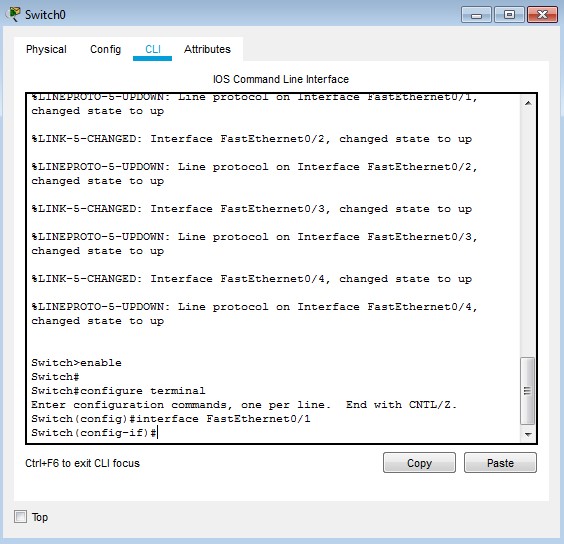
4. Switch port up for authorized MAC for an assigned end device.

TEORITICAL BACKGROUND:- Port security with sticky MAC addresses provides many of the same benefits as port security with static MAC addresses, but sticky MAC addresses can be learned dynamically. Port security with sticky MAC addresses retains dynamically learned MAC addresses during a link-down condition.

If you enter a write memory or copy running-config startup-config command, then port security with sticky MAC addresses saves dynamically learned MAC addresses in the startup-config file and the port does not have to learn addresses from ingress traffic after bootup or a restart.

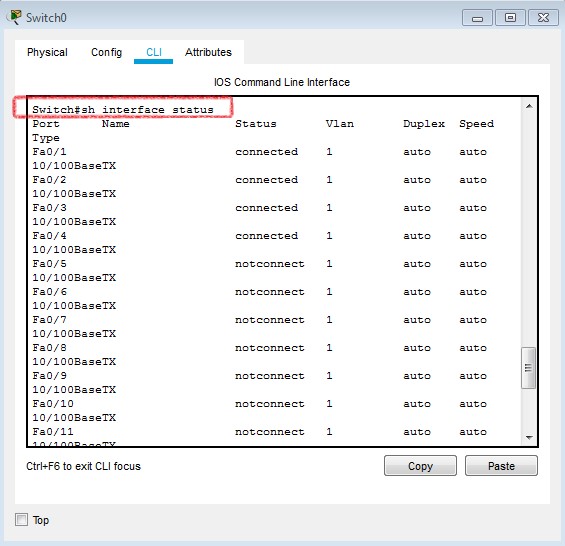
**Simulation result:**

1. **Enable mode in switch’s command-line interface (CLI):**



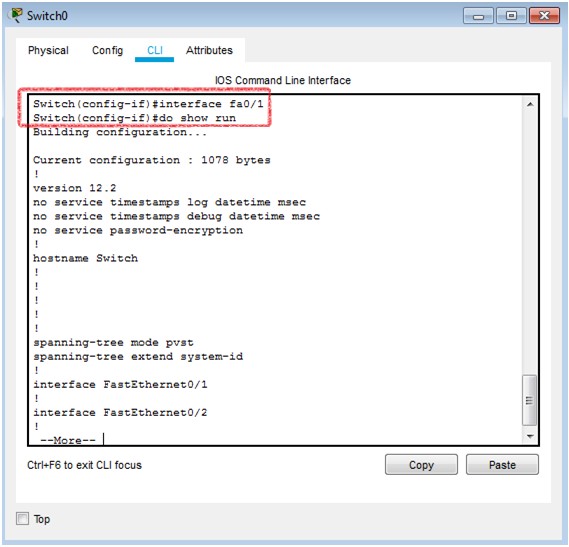
To know the detail interface status

**2. Switch #sh interface status :**



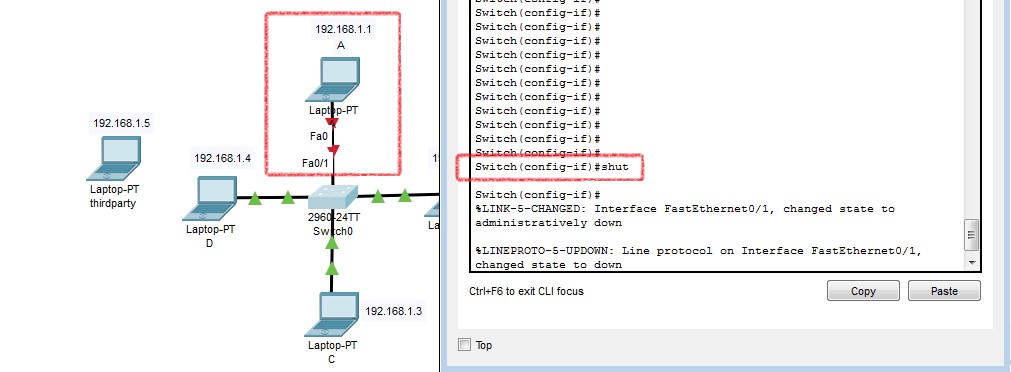
status of Fa0/1 along with other port

**3. Switch(config)#interface fa0/1 :**

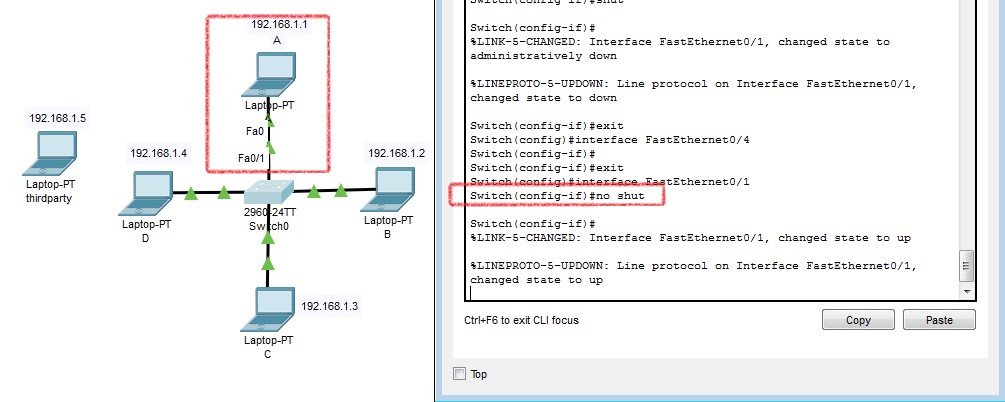


**4.** **To shut down the switch port Fa 0/1 :**

**4.1. Switch(config‐if)#shut**

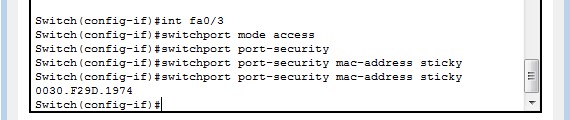


**4.2. Switch(config‐if)#no shut**

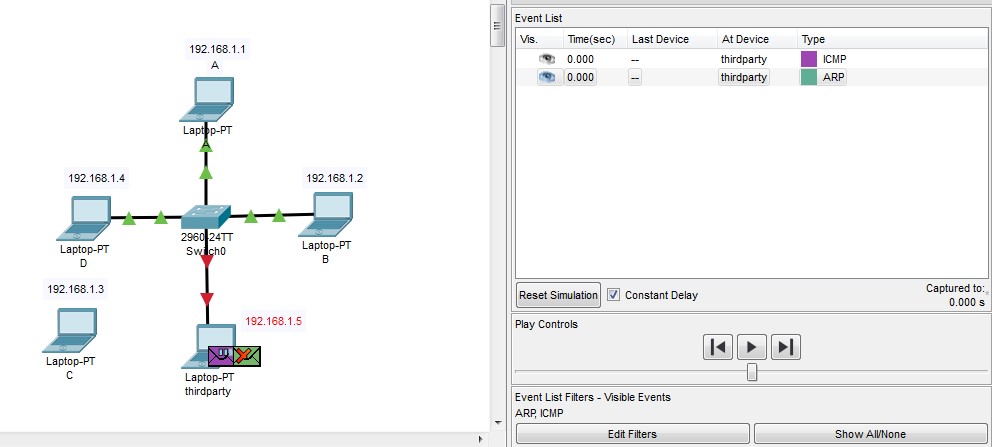


**5. Port security:**

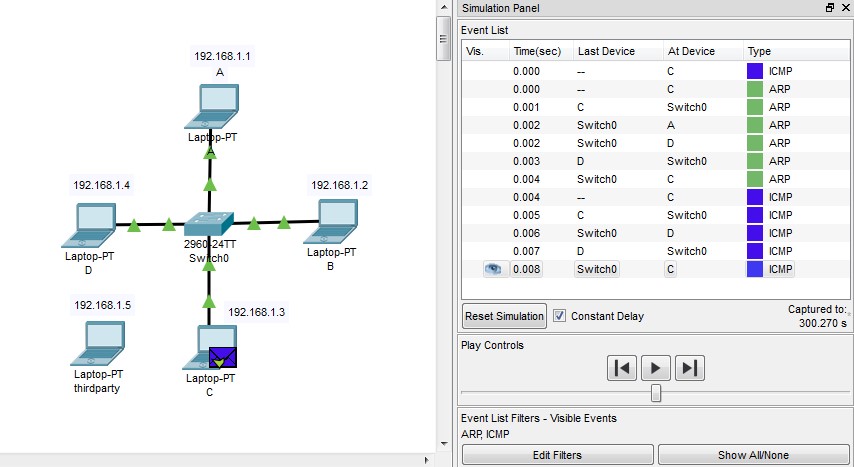
We have provided MAC address of switch’s fa0/3 connection. Now, no third party can access that particular port.



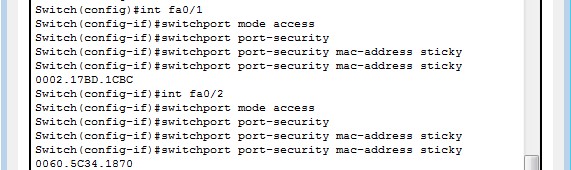
Third party cannot access port fa0/3

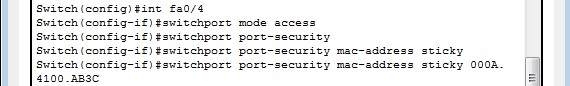


If we reconnect C, it will work normally as before.



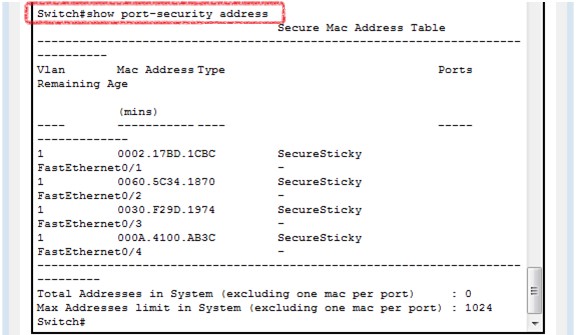
Do the same for the rest of the ports.



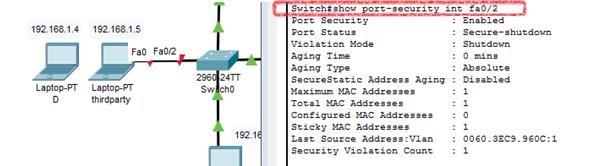


**6. Now, all the ports are secure.**

**Check: Secure Mac Address Table**



**7. If third-party wants to access port, connection will be automatically shut down. We can see the details as follow:**



**Discussion:**

In this experiment we have seen how we can configure switch, so that no third party end device can access the ports of the switch. We have gave some commands in Command Line Interface(CLI) of switch, like, Switch()#switchport port-security mac-address sticky, so when third party devices want to access any port, the connection will automatically will be cut off. We also can give commands like Switch#show port-security address to see the security of ports.

**EXPERIMENT NO: CSEP602CS/07**

**NAME OF EXPERIMENT:-** Setup a full secure hybrid VLAN with multiple IEEE 802.3 & IEEE 802.11network for data communication with RIP protocol at network layer and port security interface with layer 2 switch.

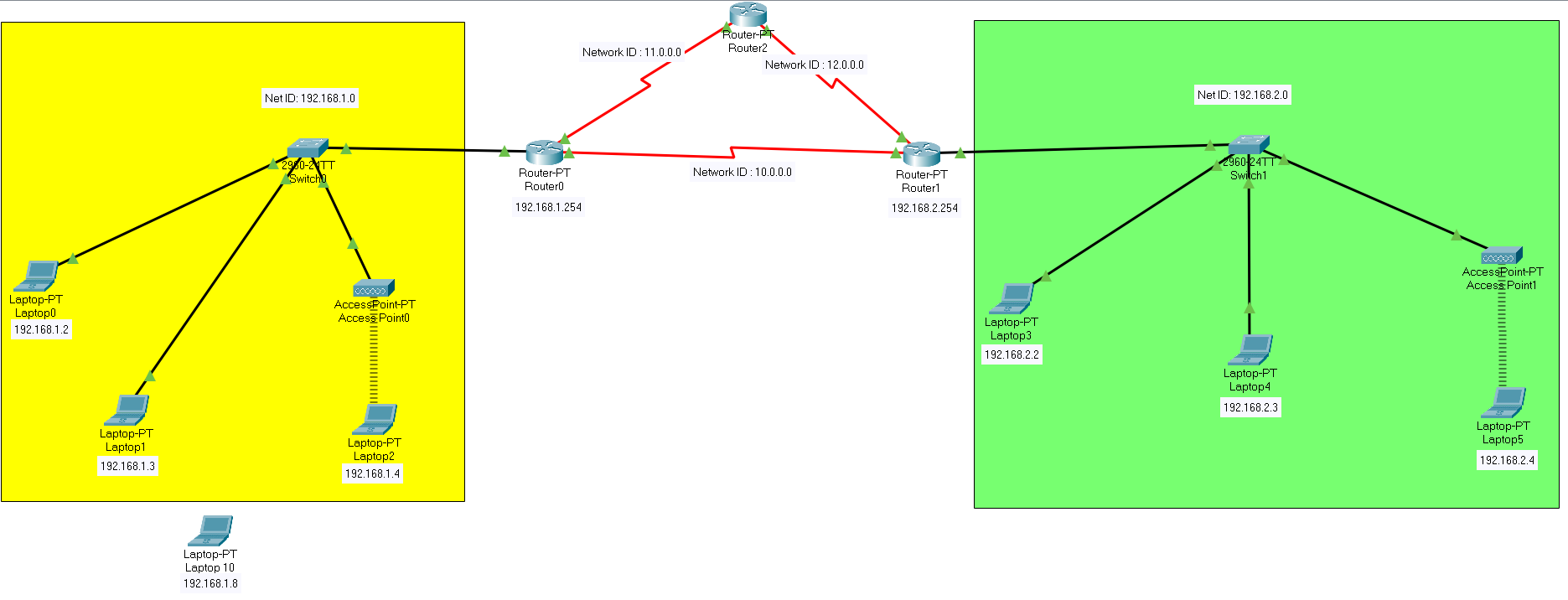
**OBJECTIVE:-** .

1. VLAN data transfer between IEEE 802.11 and IEEE 802.3 network

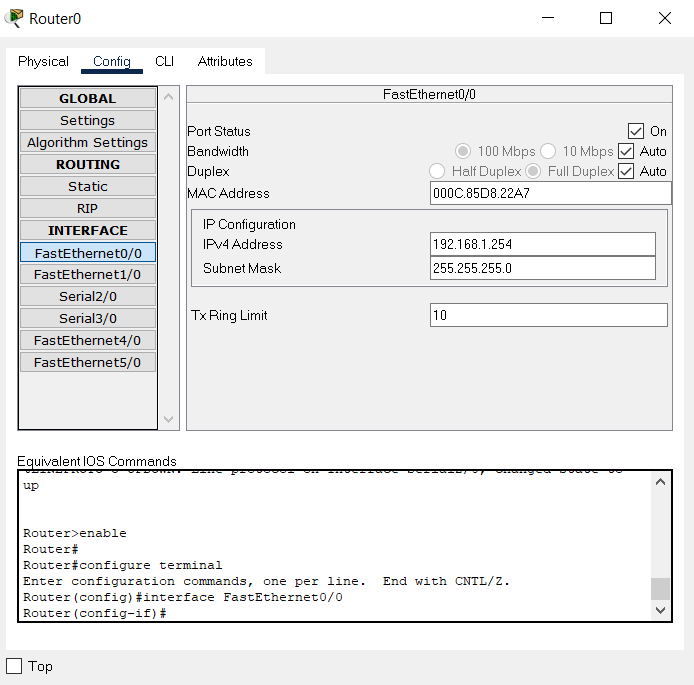
2. Delta connected routing interface with RIP protocol.

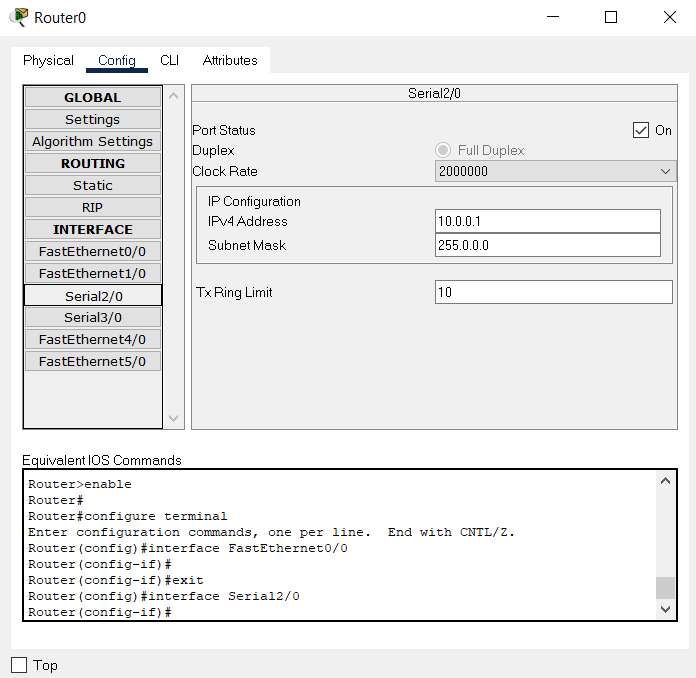
3. Sticky mac validation and port security with switch no shut / shut command, with interface

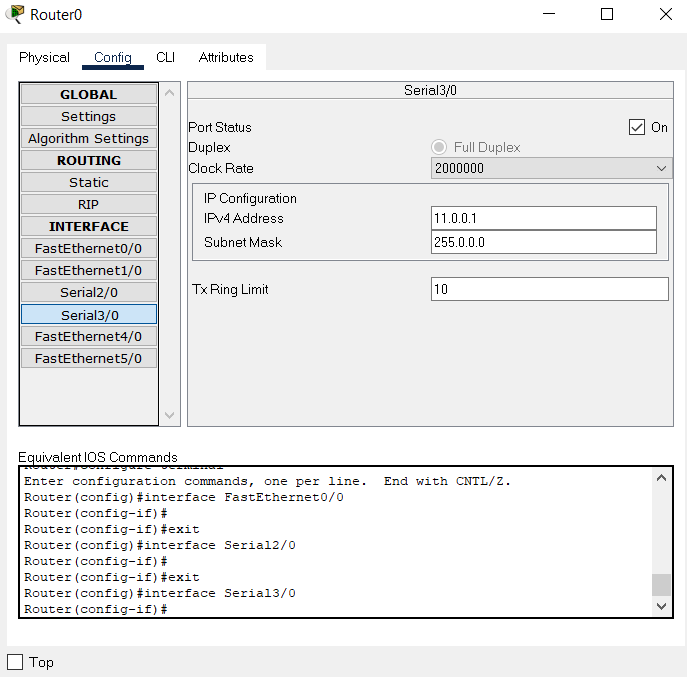
**Result:**

**Scenario:**

**Setup of Router0:**



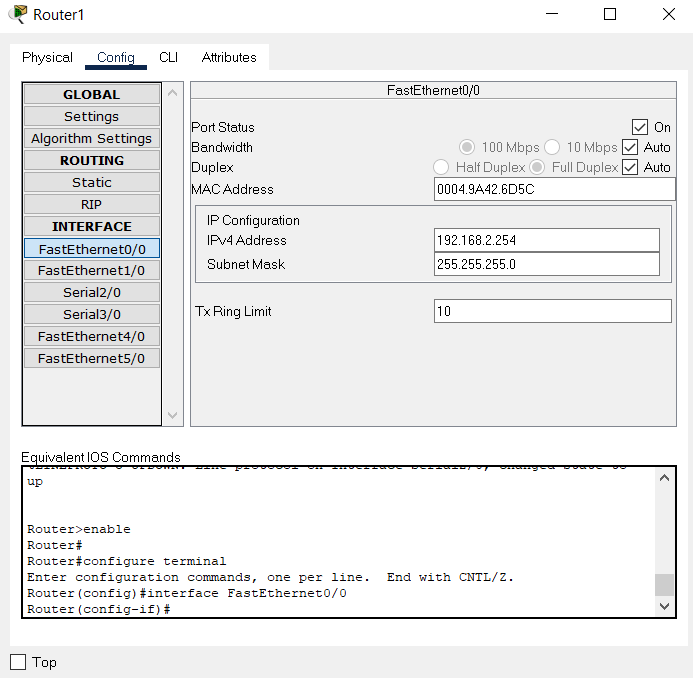


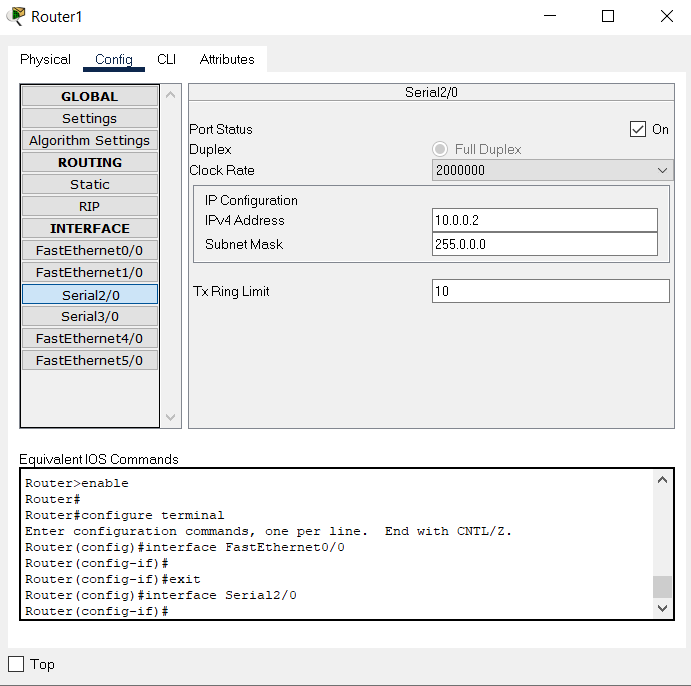


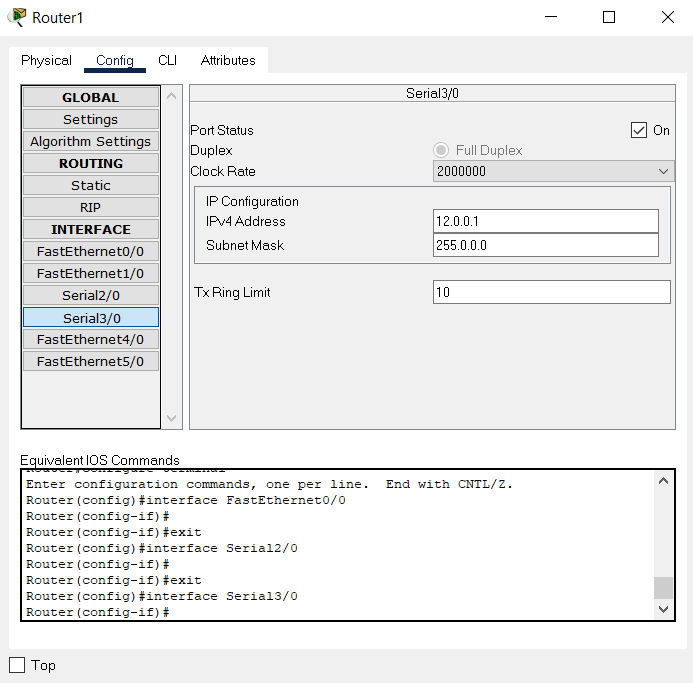
**Setup RIP:**



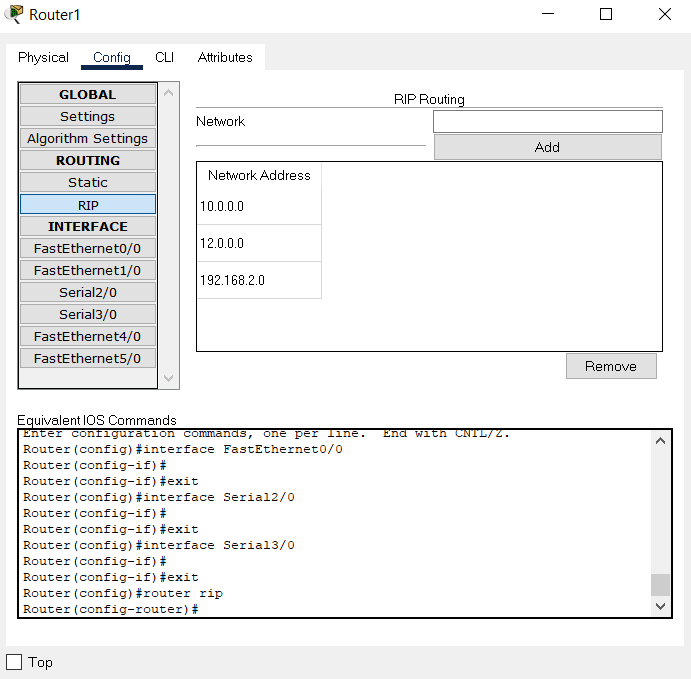
**Setup of Router1 :**



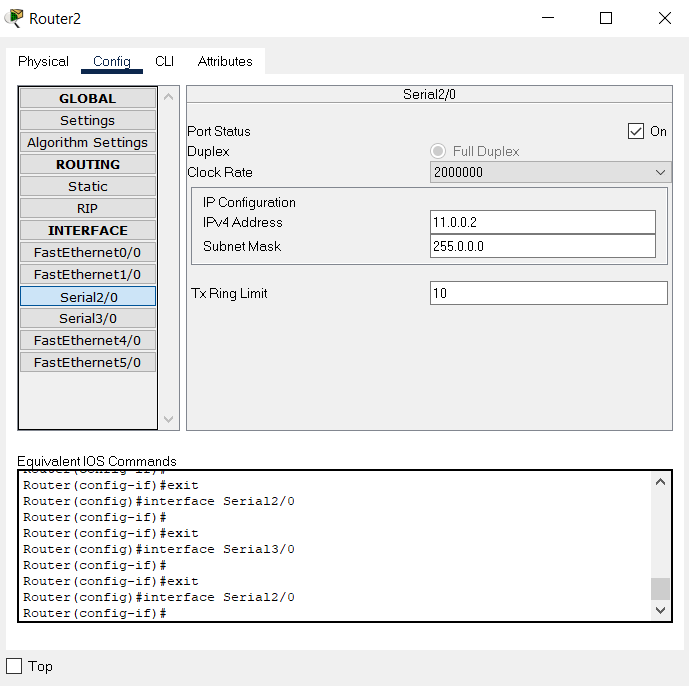


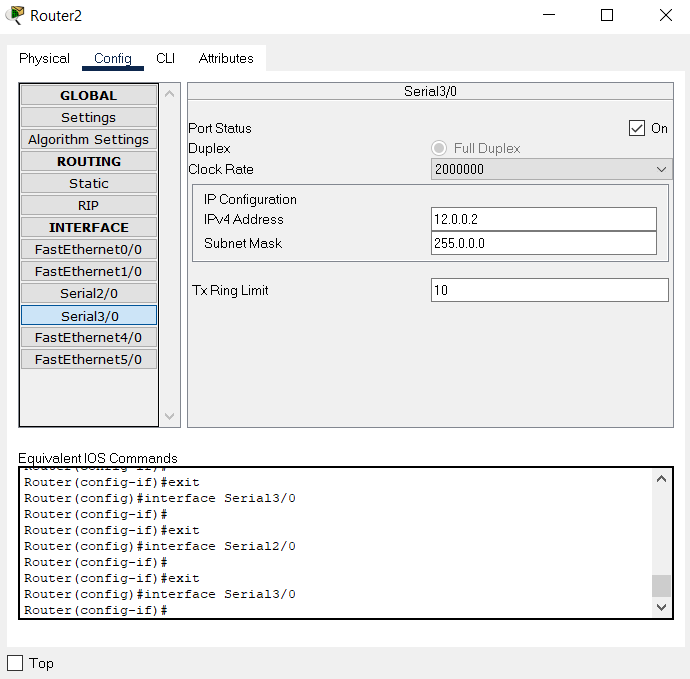


**Setup RIP:**

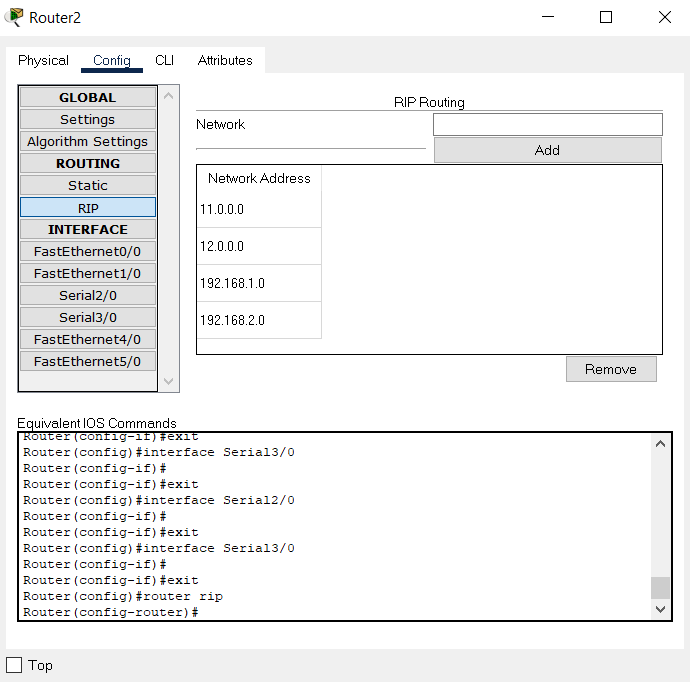


**Setup of Router2 :**



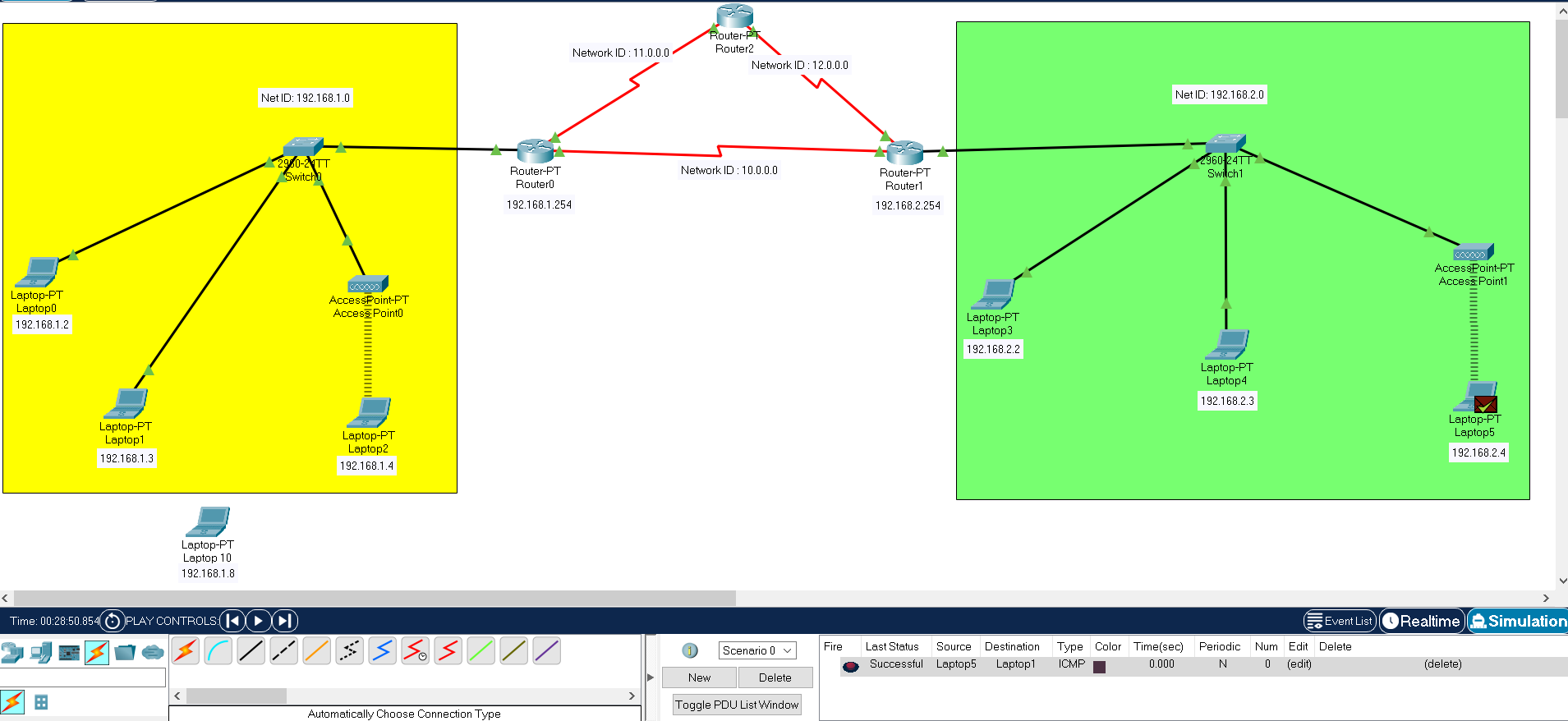


**Setup RIP:**

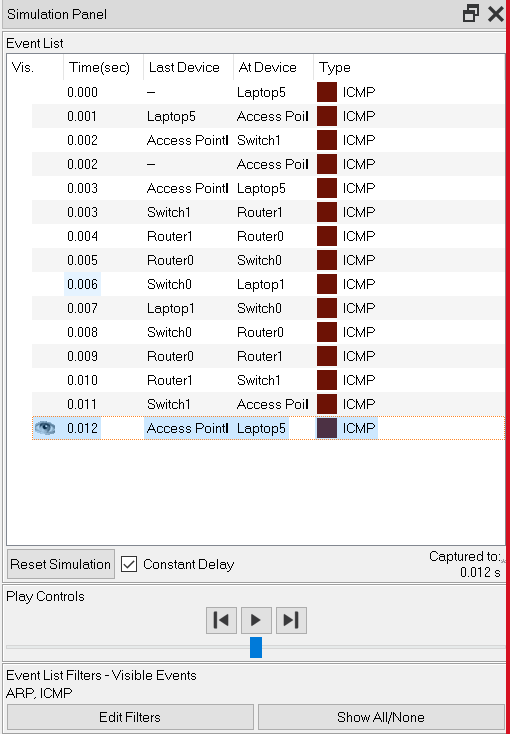


1. **VLAN data transfer between IEEE 802.11 and IEEE 802.3 network in delta network.**

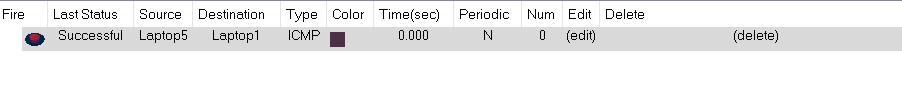
* Here we send a ICMP packet from Laptop5 to Laptop1



**Simulation Panel Image:**

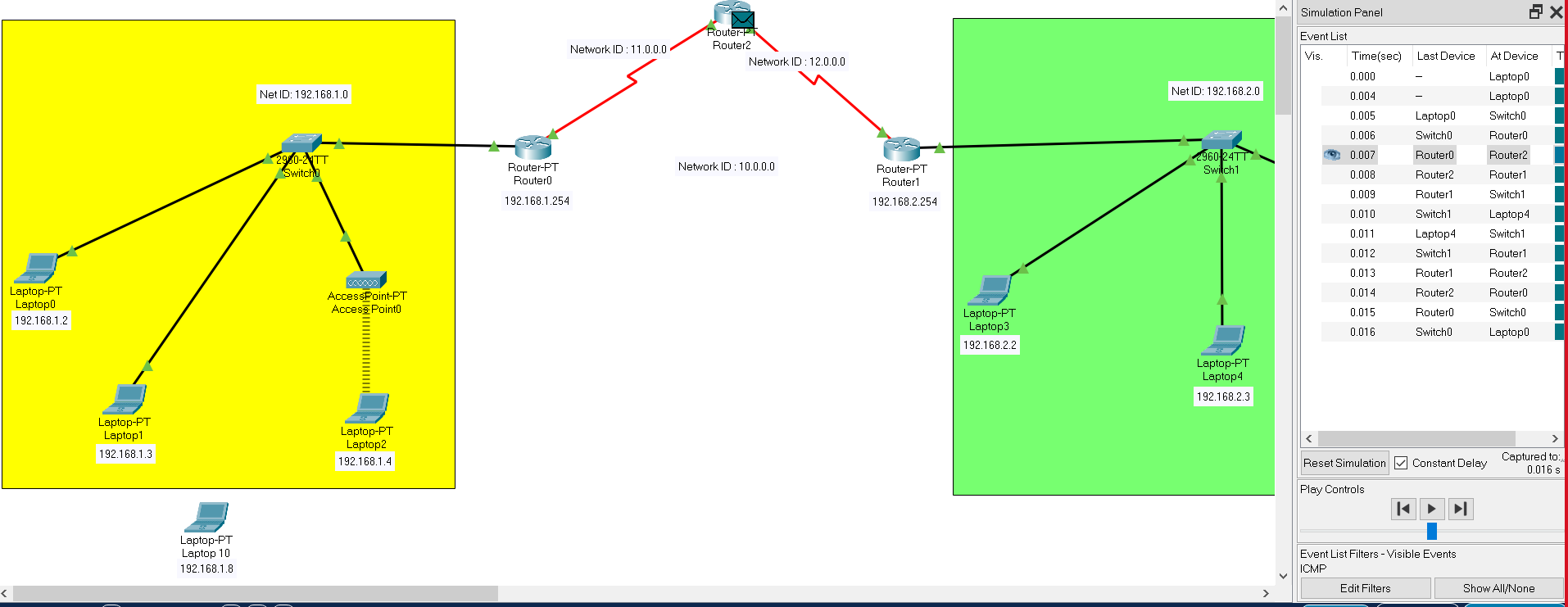


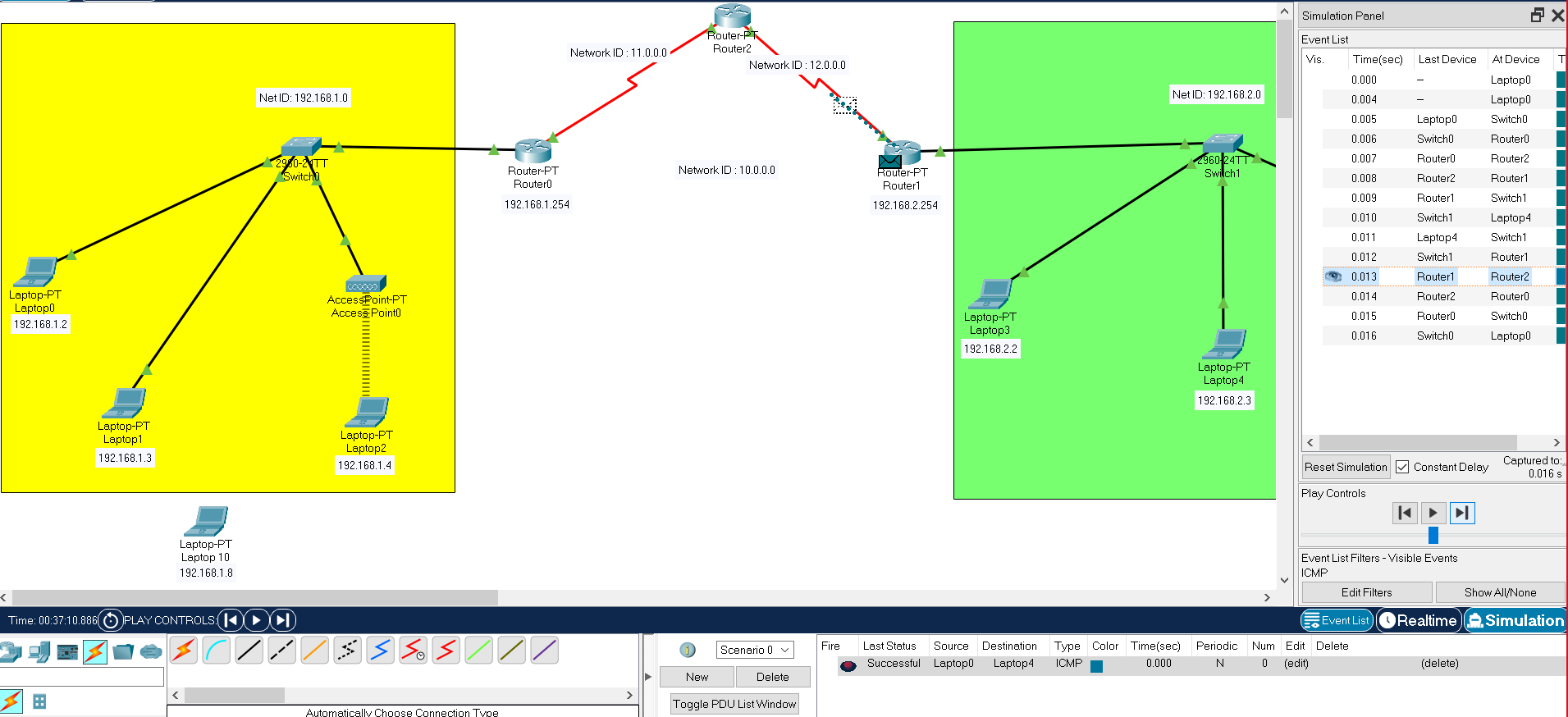
**Final Simulation Result:**



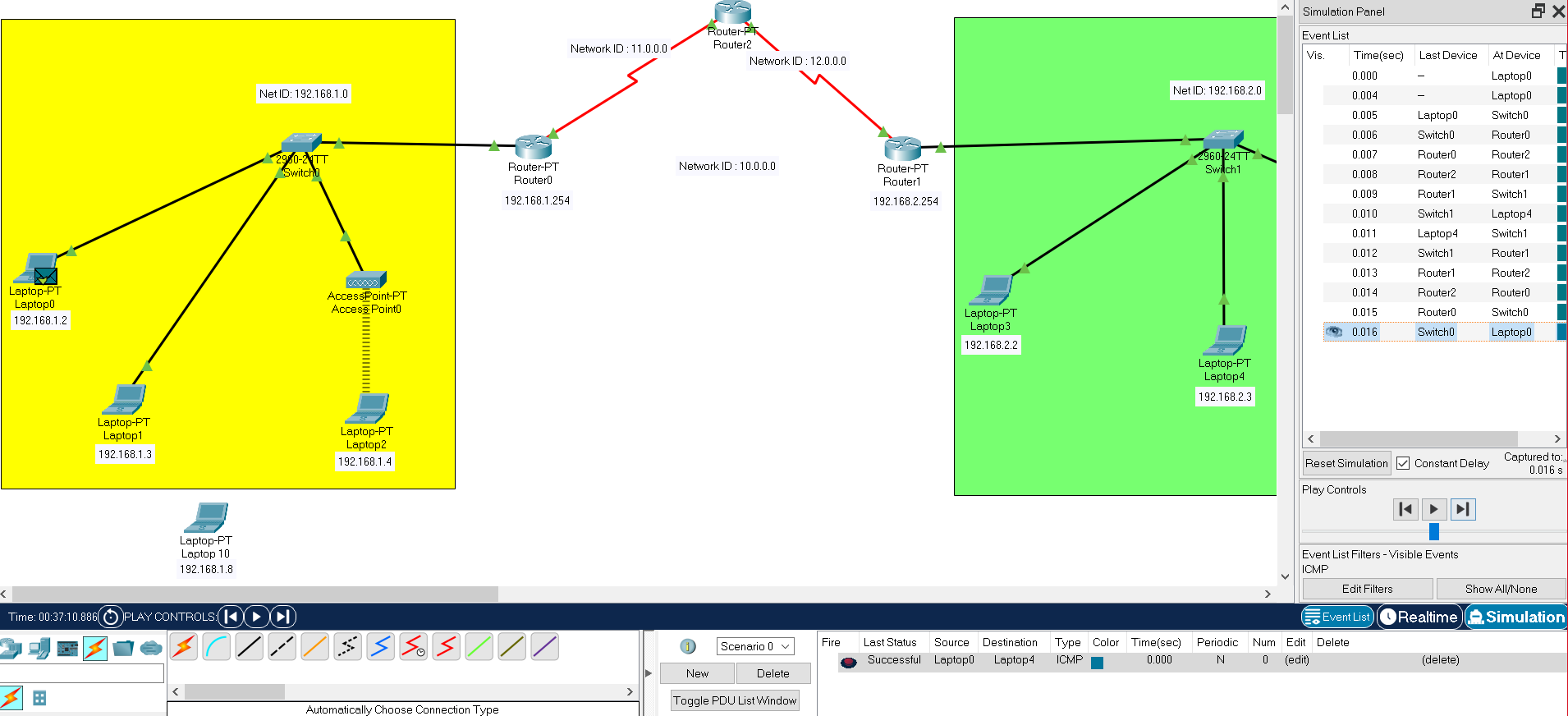
1. **If the connection between Router0 and Router1 become fail :**

* Here we send a ICMP packet from Laptop0 to Laptop4

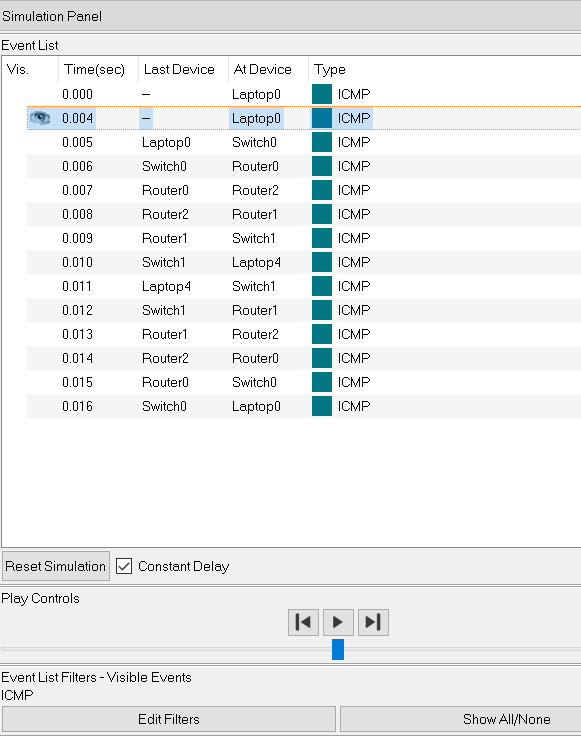
**Image1:**

**Image2**:

**Image3:**



**Simulation Panel Image:**

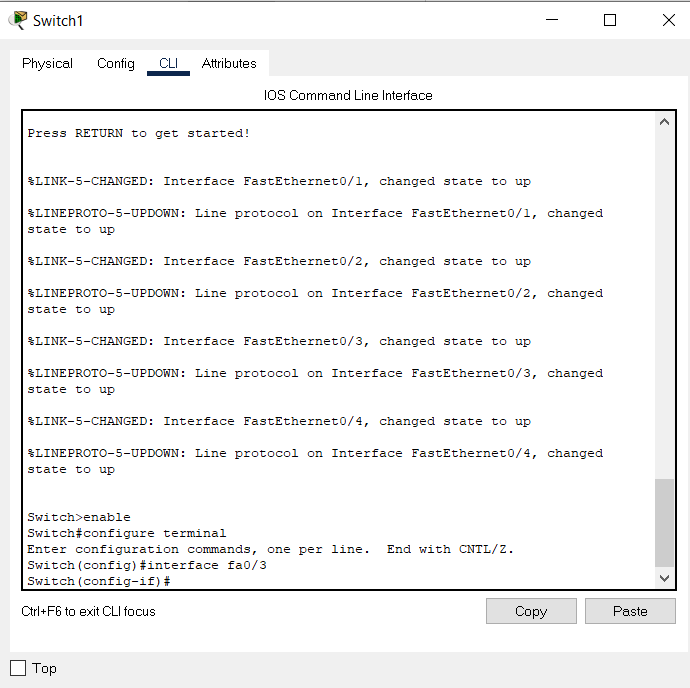


**Final Simulation Result:**



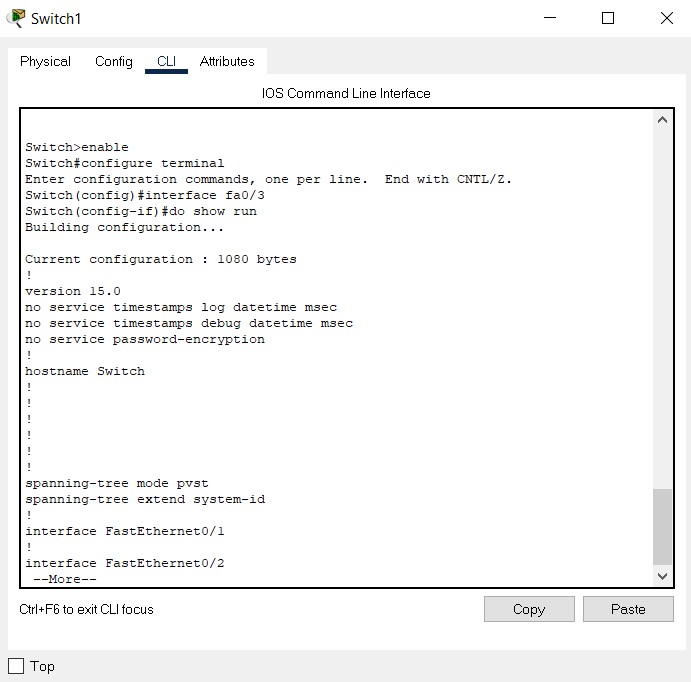
**3. Sticky mac validation and port security with switch no shut / shut command, with interface:**

1. **Enable mode in switch’s command-line interface (CLI):**



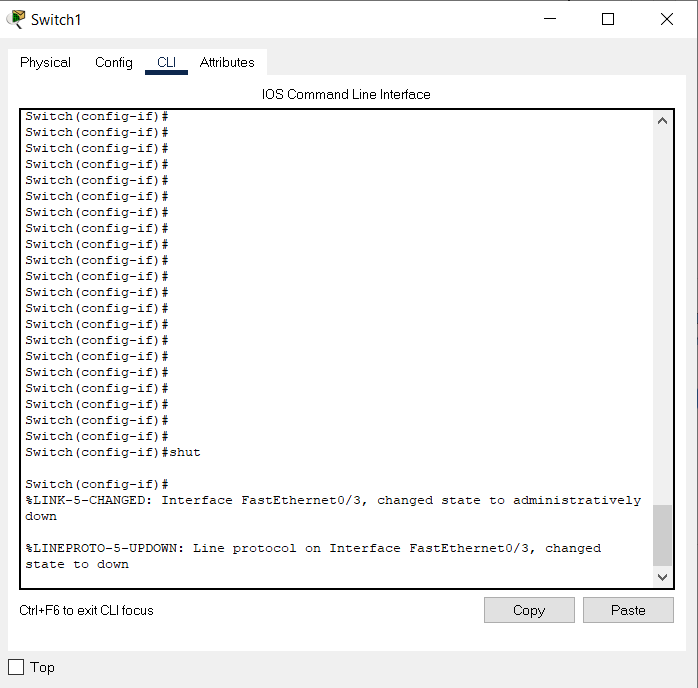
To know the detail interface status

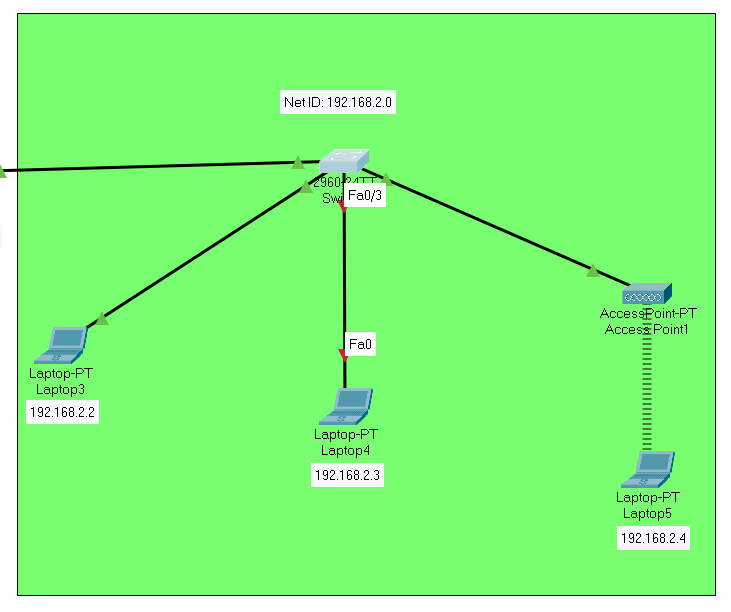
1. **Switch(config)#interface fa0/3 :**



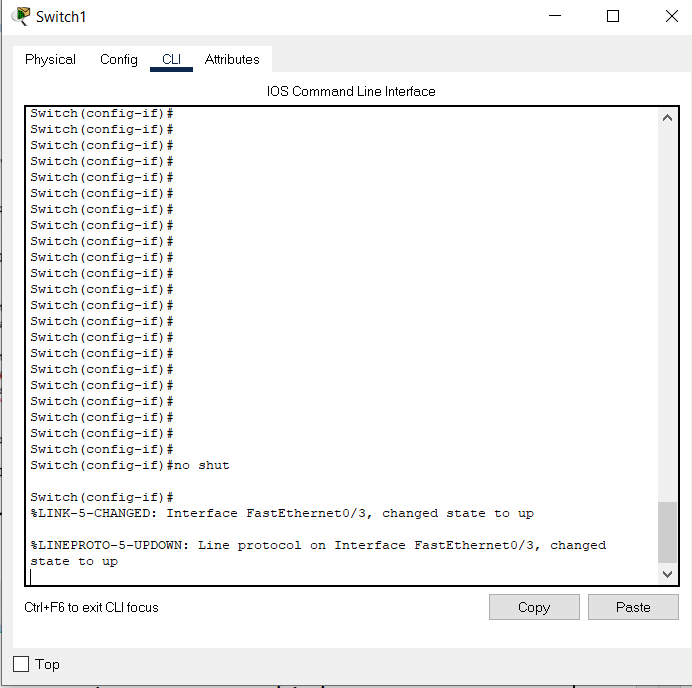
**3. To shut down the switch port Fa 0/3 :**

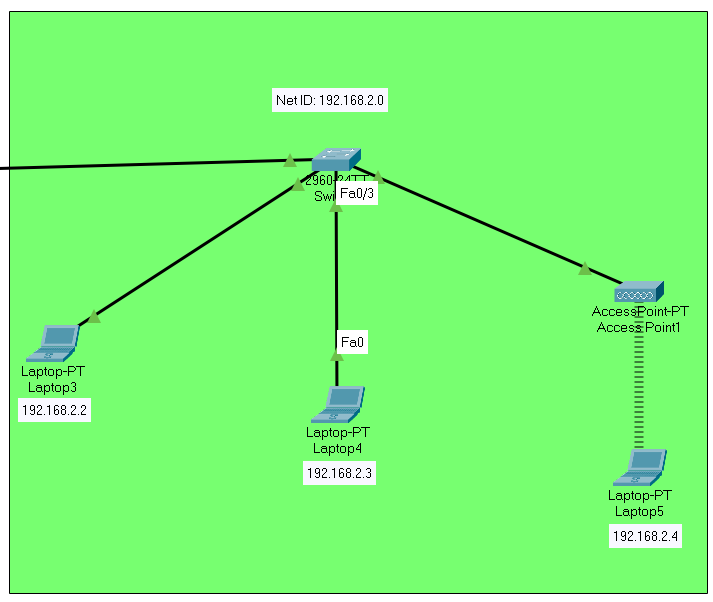
**3.1. Switch(config‐if)#shut**

****



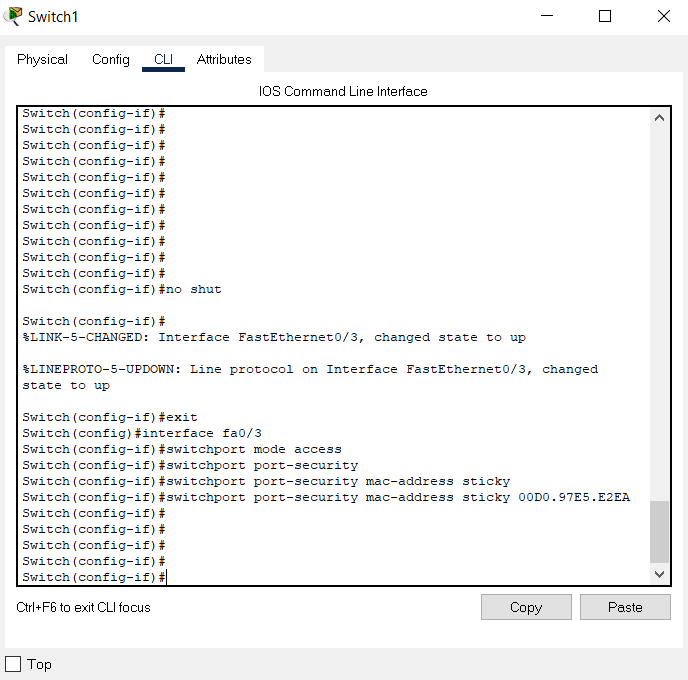
**3.2. Switch(config‐if)#no shut**

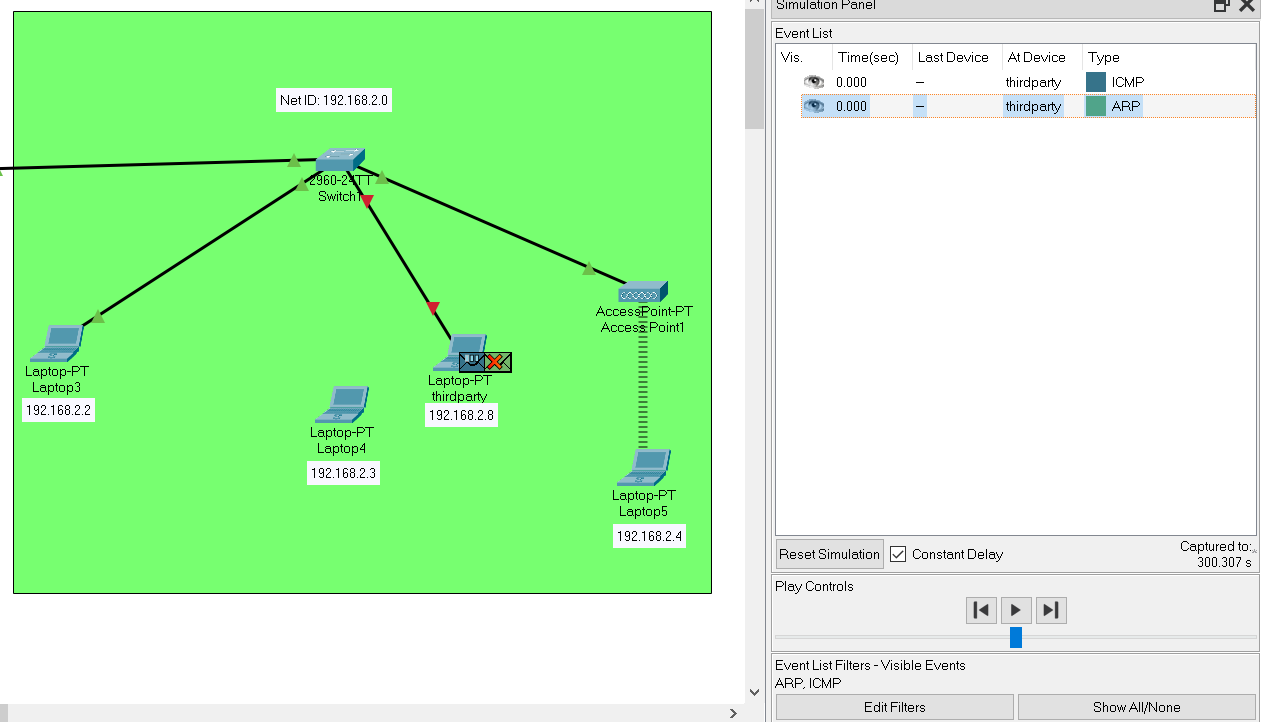
****

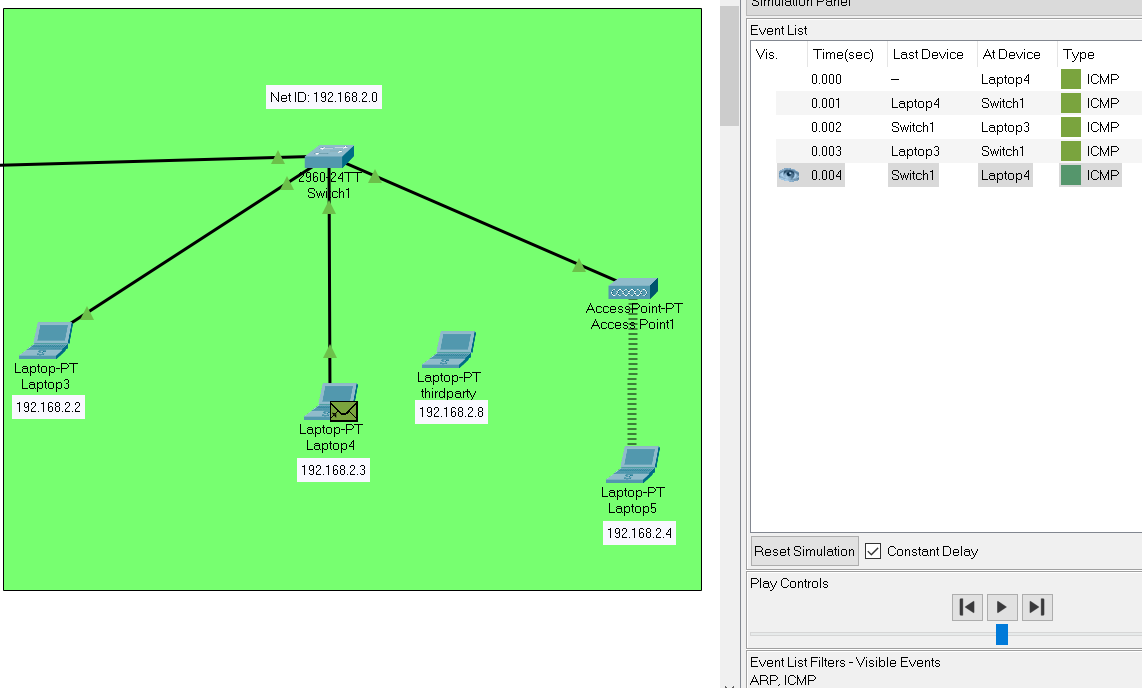
****

**4. Port security:**

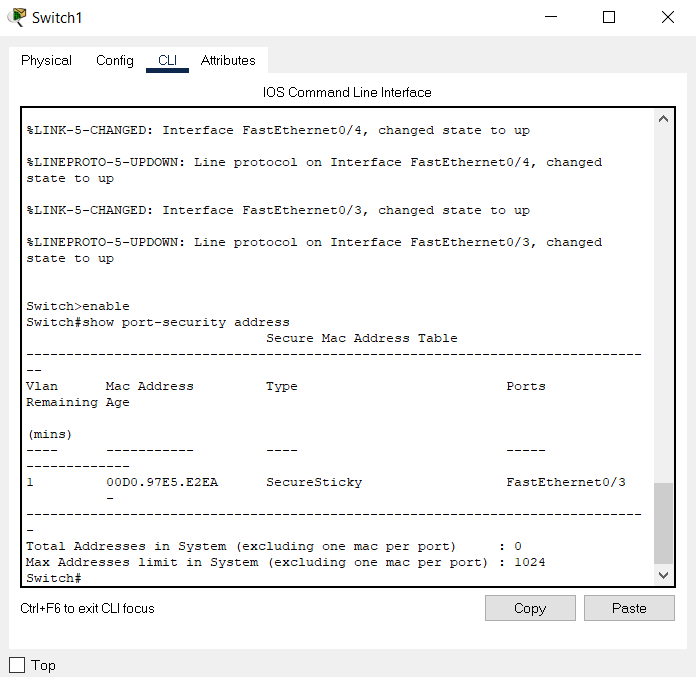
We have provided MAC address of switch’s fa0/3 connection. Now, no intruder can access that particular port.

****

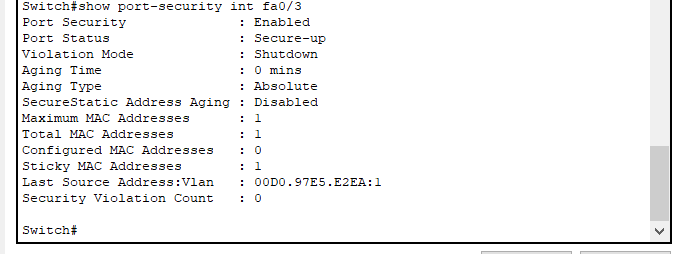
****\*\*Intruder cannot access port fa0/3

****\*\*If we reconnect Laptop4, it will work normally as before.

**5. Check: Secure Mac Address Table**

****

**6. If intruder wants to access port, connection will be automatically shut down. We can see the details as follow:**

****

**Discussion:**

In this experiment, as usual we have provided all the IPs and also configured both routers with RIP with net id of both networks, so that the RIP can work and data can be transmitted and also connected three access points in those two network. We were also able to interwork between two wired and wireless network. In this way we have successfully completed our experiment. Now, if we delete those two net ids from router RIP config, we will see the routers will constantly send RIPv1 to both networks to know the net id, and our transmission will be failed. If in 3 router, the shortest path connection is not possible then it transmit through Router no 3. Also we have seen how we can configure switch, so that no third party end device can access the ports of the switch. We have gave some commands in Command Line Interface(CLI) of switch, like, Switch()# switchport port-security mac-address sticky, so when third party devices want to access any port, the connection will automatically will be cut off. We also can give commands like Switch#show port-security address to see the security of ports.

**EXPERIMENT NO: CSEP602CS/08**

NAME OF EXPERIMENT**:-** Results Introduction to access list and cisco firewall and configuring adaptive security appliance basic setting and firewall using CLI toplogy

OBJECTIVE:

1. Creating IP Access Lists and applying It to an Interface

2. Creating a Standard Access List to Filter on Source Address

3. Creating a Named Extended Access List

TEORITICAL BACKGROUND:-

**Access lists** filter network traffic by controlling the forwarding or blocking of routed packets at the interface of a device. A device examines each packet to determine whether to forward or drop that packet, based on the criteria specified in access lists.

The criteria that can be specified in an access list include the source address of the traffic, the destination address of the traffic, and the upper-layer protocol. There are many reasons to configure access lists; for example, to restrict contents of routing updates or to provide traffic flow control. One of the most important reasons to configure access lists is to provide security for your network, which is the focus of this module.

Use access lists to provide a basic level of security for accessing your network. If you do not configure access lists on your device, all packets passing through the device are allowed access to all parts of your network.

Access lists can allow a host to access a part of your network and prevent another host from accessing the same area. In the figure below, Host A is allowed to access the Human Resources network, but Host B is prevented from accessing the Human Resources network.

Simulation Result :-

SUMMARY STEPS

1. enable

2. configure terminal

3. ip access-list standard name

4. remark remark

5. deny {source [source-wildcard] | any} [log]

6. remark remark

7. permit {source [source-wildcard] | any} [log]

8. Repeat some combination of Steps 4 through 7 until you have specified the sources on which you want to base your access list.

9. end

10. show ip access-list

Steps for Named Extended Access List

SUMMARY STEPS

1. enable

2. configure terminal

3. ip access-list extended name

4. remark remark

5. deny protocol source [source-wildcard] destination [destination-wildcard] [option option-name] [precedence precedence] [tos tos] [established] [log | log-input] [time-range time-range-name] [fragments]

6. remark remark

7. permit protocol source [source-wildcard] destination [destination-wildcard] [option option-name] [precedence precedence] [tos tos] [established] [log | log-input] [time-range time-range-name] [fragments]

8. Repeat some combination of Steps 4 through 7 until you have specified the fields and values on which you want to base your access list.

9. end

1. show ip access-list

Discussion:- Cisco ACLs are characterized by single or multiple permit/deny statements. The purpose is to filter inbound or outbound packets on a selected network interface. There are a variety of ACL types that are deployed based on requirements. Only two ACLs are permitted on a Cisco interface per protocol. That would include for instance a single IP ACL applied inbound and single IP ACL applied outbound.