PROJECT REPORT

- **Vemu Lakshmi Ananya**

Design of campus area network using Virtual Local Area Network (VLAN) with Physical Network Security Implementation and connectivity of Internet with wired and wireless access.

ABSTRACT:

A LAN includes all the user devices, servers, switches, routers, cables, and wireless access points in one location. It includes all devices in the same broadcast domain. A broadcast domain includes the set of all LAN-connected devices, so that when any of the devices sends a broadcast frame, all the other devices get a copy of the frame. So, from one perspective, a LAN and a broadcast domain as being basically the same thing. Without VLANs, a switch considers all its interfaces to be in the same broadcast domain. That is, forgone switch, when a broadcast frame entered one switch port, the switch forwarded that broadcast frame out all other ports. With that logic, to create two different LAN broadcast domains, needs two different Ethernet LAN switches.

With support for VLANs, a single switch can accomplish the same goals of the design to create two broadcast domains—with a single switch. With VLANs, a switch can configure some interfaces into one broadcast domain and some into another, creating multiple broadcast domains. These individual broadcast domains created by the switch are called virtual LANs (VLAN).

Designing campus LANs to use more VLANs, each with a smaller number of devices, often helps improve the LAN in many ways. For example, a broadcast sent by one host in a VLAN will be received and processed by all the other hosts in the VLAN—but not by hosts in a different VLAN. Limiting the number of hosts that receive a single broadcast frame reduces the number of hosts that waste effort processing unneeded broadcasts. It also reduces security risks, because fewer hosts see frames sent by any one host.

The following list summarizes the most common reasons for choosing to create smaller broadcast domains (VLANs):

- To reduce CPU overhead on each device by reducing the number of devices that receive each broadcast frame.
- To reduce security risks by reducing the number of hosts that receive copies of frames that the switches flood (broadcasts, multicasts, and unknown unicasts)
- To improve security for hosts that send sensitive data by keeping those hosts on a separate VLAN
- To create more flexible designs that group users by department, or by groups that work together, instead of by physical location
- To solve problems more quickly, because the failure domain for many problems is the same set of devices as those in the same broadcast domain

DESCRIPTION:

In this Project trainee should design a college campus area Network with VLANs with different Hosts and Departments as per the following requirement.

1. College campus is a (Ground + 4) 5 Floor building.
2. Ground Floor have 100Mbps connectivity to ISP for Internet with a CISCO 2811 Router with a single LAN port .
3. First, second, Third and Fourth floors have Hosts belongs to CSC/IT//ECE/EEE departments related to I year, II year, III Year and Final year students class rooms. Each Floor has a switch connecting these hosts.
4. Switch from the top floor is connected directly to its next floor switch and finally from the First floor switch, a cable is extended to ground floor to the LAN port of CISCO Router 2811.
5. Administrator has been asked to configure the departments in different VLAN domains and also instructed that the communication between the departments is also required.
6. Administrator has been asked to place an Access point for wireless connectivity with security password from the Fourth Floor on need basis
7. Administrator has been asked to create security credentials for login to the Router and Switches such that authorized person only logs in.
8. Administrator has been asked to make sure that if anyone connect a host in the vacant ports of switch in any floor they should not work.
9. Administrator has been asked to allocate 40 Mbps bandwidth to CSC department, 30 Mbps bandwidth to IT department, 20 Mbps bandwidth for ECE department & 10 Mbps bandwidth to EEE department for Internet access.
10. ISP has given 10.10.10.0/30 subnet to college and asked the administrator to configure the WAN link IP 10.10.10.1 at College side WAN interface on Router. The Internet IP pool given to college is 117.117.117.0/29.
11. Administrator has been instructed to make sure that all computers available in the campus should be connected with Internet (except 192.168.2.3).
12. Administrator has been asked put college website IP as 117.117.117.3 and this website has to be accessed from Internet.

(Please Take any Class C, IP Pool s for the LAN networks connectivity)

SIMULATOR:

In order to design campus network, I used cisco packet tracer. Cisco Packet Tracer is a networking simulator used for teaching and learning program by offering a unique combination of realistic comparison between physical devices and simulator software.

Benefits of Packet Tracer are:

- Offers a realistic simulation and visualization
- Permits users to design, build, configure, and troubleshoot complex networks
- Allows students to explore concepts, conduct experiments.

Things and Components available in Packet Tracer 7.3.0:

It includes more support for wireless and wide-area network (WAN) technologies. and featuring

two new devices, can simulate the Cisco 4331 Integrated Services Router (ISR) with integrated WAN ports and the Cisco 3504 Wireless Controller (WLC), including centralized control, management, and troubleshooting for next-generation wireless networks. Packet Tracer v7.3.0 also offers enhancements for accessibility and usability, support for new CLI commands.

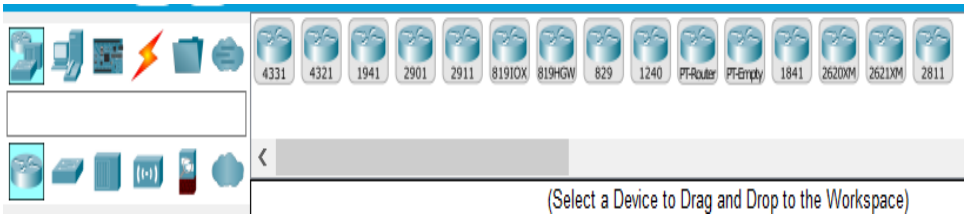
Packet Tracer Modes: Cisco Packet Tracer provides two operating modes to visualize the behavior of a network real-time mode and simulation mode. In real-time mode the network behaves as real devices do, with immediate real-time response for all network activities. The real-time mode gives students a viable alternative to real equipment and allows them to gain configuration practice before working with real equipment. In simulation mode the user can see and control time intervals, the inner workings of data transfer, and the propagation of data across a network. This helps students understand the fundamental concepts behind network operations. A solid understanding of network fundamentals can help accelerate learning about related concepts.

Protocols: Cisco Packet Tracer supports the following protocols.

LAYER	Cisco Packet Tracer Supported Protocols
APPLICATION	FTP, SMTP, POP3, HTTP, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, ISR VOIP, SCCP config and calls ISR command support Call Manager Express
TRANSPORT	TCP and UDP. TCP Nagle Algorithm & IP Fragmentation, RTP
NETWORK	BGP, IPV4, ICMP, ARP, IPv6, ICMPv6, IPsec, RIPv1/V2/NG, Multi-Area OSPF, EIGRP, Static Routing, Route redistribution, Multilayer switching, L3 QoS, NAT, CBAL, Zone-based policy firewall and intrusion Protection System on the ISR, GRE VPN, IPsec VPN
NETWORK ACCESS/ INTERFACE	Ethernet (802.3), 80211. HDLC, Frame Relay. PPP, PPPoE, STP, RSTP, VTP, DTP, CDP, 802.1q, PAgp, L2 QoS, SLARP, Simple EP, WPA, EAP.

CONNECTIONS:

To implement the campus area network, different networking devices are used. Those devices are like Cisco 2811 Router, 2950-24 Switch, Access Point AP-PT, Server and some devices like Laptop (laptop-PT), computer (PC-PT) and used the wire connections in connecting all those devices.

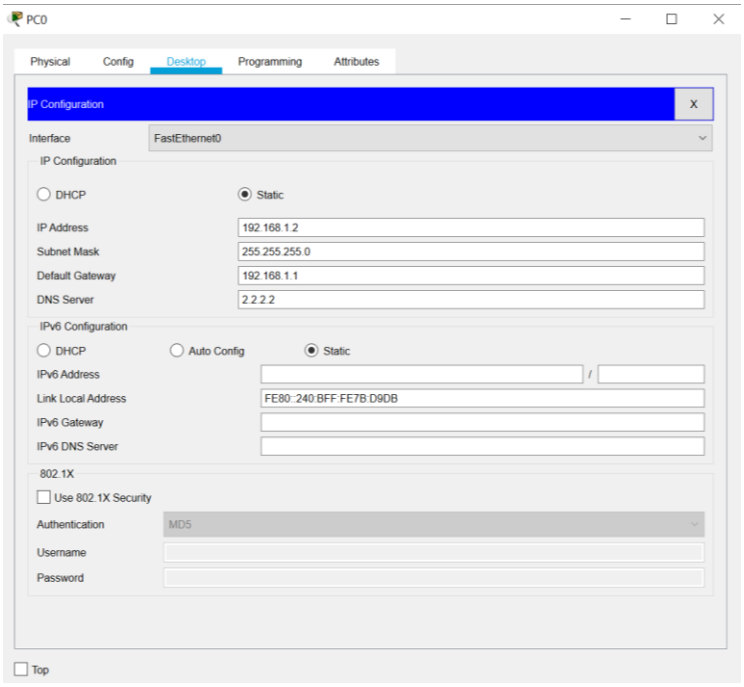


To implement the campus network design on cisco packer tracer, I used class C IP address that is 117.117.117.0/29 subnet and this subnet divided into eight subnets from these eight subnets, I used one of them and the rest are reserved for future scalability.

1. **PC**: PCs are provided for the students to access. You will find these PCs in the END DEVICES. You just need to drag and drop them in an order. IP configuration is done to all the PC's according to the department we have considered. In my project this is how I configured the IPs to the PCs,

SWITCH 3	PC 12 (192.168.1.5)	PC 13 (192.168.2.5)	PC 14 (192.168.3.5)	PC 15 (192.168.4.5)	4th Floor
SWITCH 2	PC 8 (192.168.1.4)	PC 9 (192.168.2.4)	PC 10 (192.168.3.4)	PC 11 (192.168.4.4)	3rd Floor
SWITCH 1	PC 4 (192.168.1.3)	PC 5 (192.168.2.3)	PC 6 (192.168.3.3)	PC 7 (192.168.4.3)	2nd Floor
SWITCH 0	PC 0 (192.168.1.2)	PC 1 (192.168.2.2)	PC 2 (192.168.3.2)	PC 3 (192.168.4.2)	1st Floor
	CSE (192.168.1.1)	IT (192.168.2.1)	ECE (192.168.3.1)	EEE (192.168.4.1)	SUBNET MASK (255.255.255.0)/ DNS (2.2.2.2)

CLICK ON PC >> DESKTOP >> IP CONFIGURATION >> ENTER THE VALUES



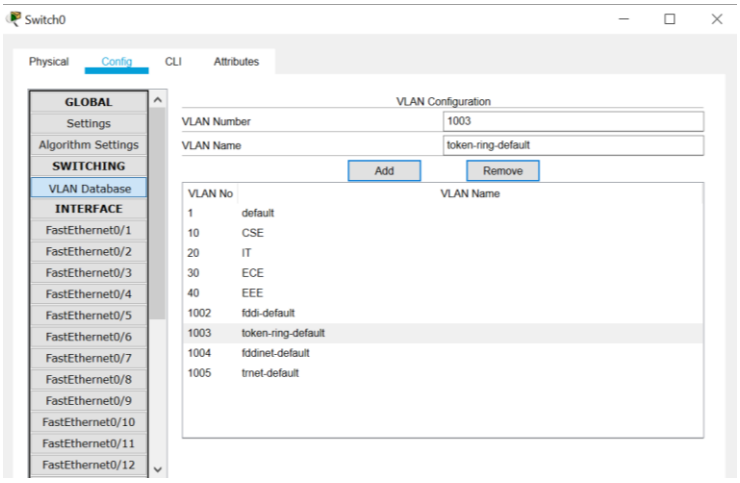
2. **SWITCH**: Allows to set IP address on interface level. IP address assigned on interface is used to manage that particular interface

The switch is password encrypted . There are 2 types of switch port modes: access and trunk. Access is used for connection between switch and PC, whereas Trunk is used for connection between 2 different switches or switch and router. There are 2 ways of configuring the switch : You can either use GUI mode or Code.

1. **GUI MODE (Graphic User Interface):**

   Step 1: Create a VLAN DATABASE. According to the question, there are 4 departments, so I created 4 VLAN's. CSE VLAN10, IT VLAN 20, ECE VLAN 30, EEE VLAN 40.

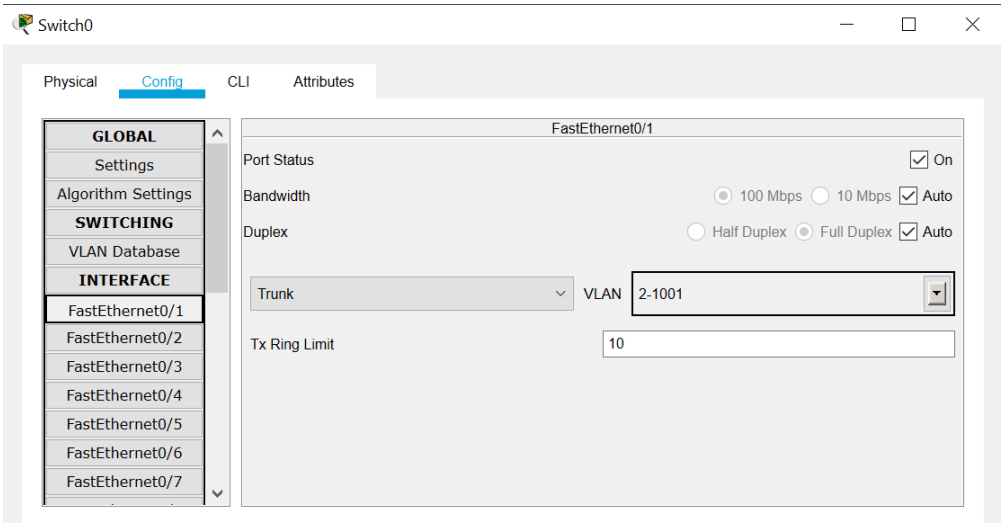
   SWITCH >>CONF>>VLAN DATABASE>>VLAN NAME,NUM>>ADD



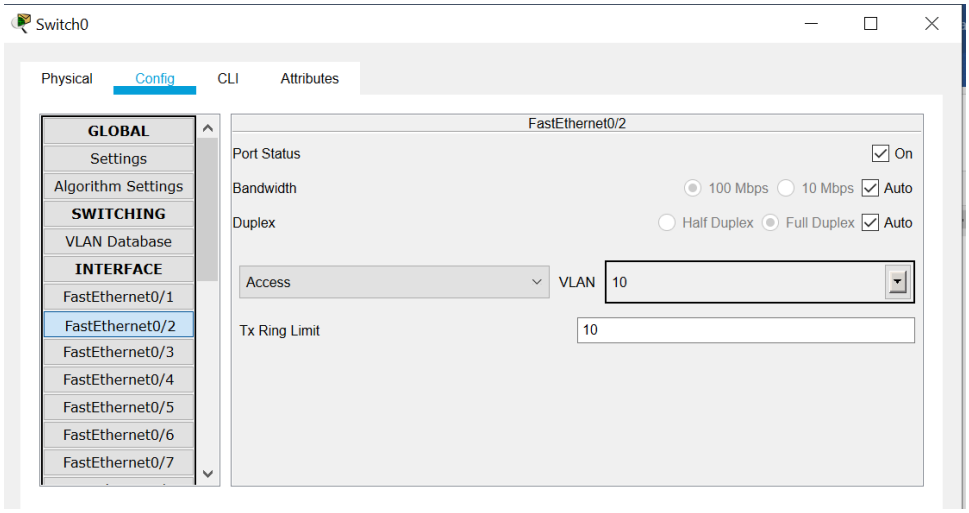
Step 2: Switch Modes must be assigned ie either Trunk or Access. In my project the Switches 0,1,2,3 are connected to the PC's FastEthernet 0/2 - 0/5 (0/2-VLAN 10, 0/3 VLAN 20, 0/4 VLAN 30, 0/5 VLAN 40). So FastEthernet 0/2- 0/5 is given Access mode. Similarly, the Switches are connected to other Switches in FastEthernet 0/1 ; 0/6 so they are given Trunk Mode. (Exception: Switch 0 FastEthernert 0/1 is connected to College Router. Still it must be given trunk mode).

SWITCH>>CONF>>FASTETHERNET 0/?>>TRUNK/ACCESS>>VLAN

NOTE: For Trunk Mode choose VLAN 10,20,30,40. For Access Mode choose VLAN as mentioned above (0/2-VLAN 10, 0/3 VLAN 20, 0/4 VLAN 30, 0/5 VLAN 40).



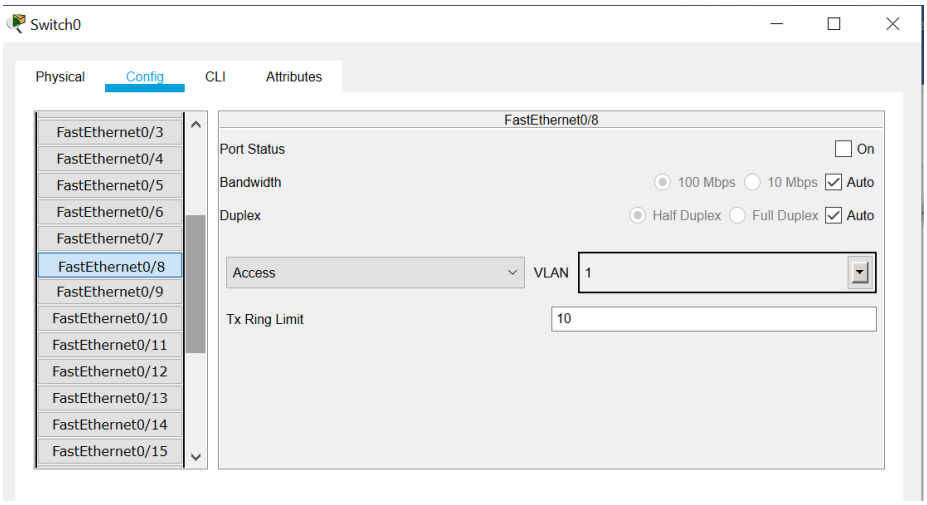
TRUNK MODE GIVEN TO CONNECTION BETWEEN SWITCH 0 AND ROUTER



ACCESS MODE GIVEN TO SWITCH WHICH CONNECTS TO PC

Also according to our question, access must not be given to switches which are not connected to PCs , ie from FastEthernet 0/7-0/24 The ports must not be on. (EXCEPTION: Switch 3 FastEthernet 0/7 is connected to college server, and its mode will be access mode).

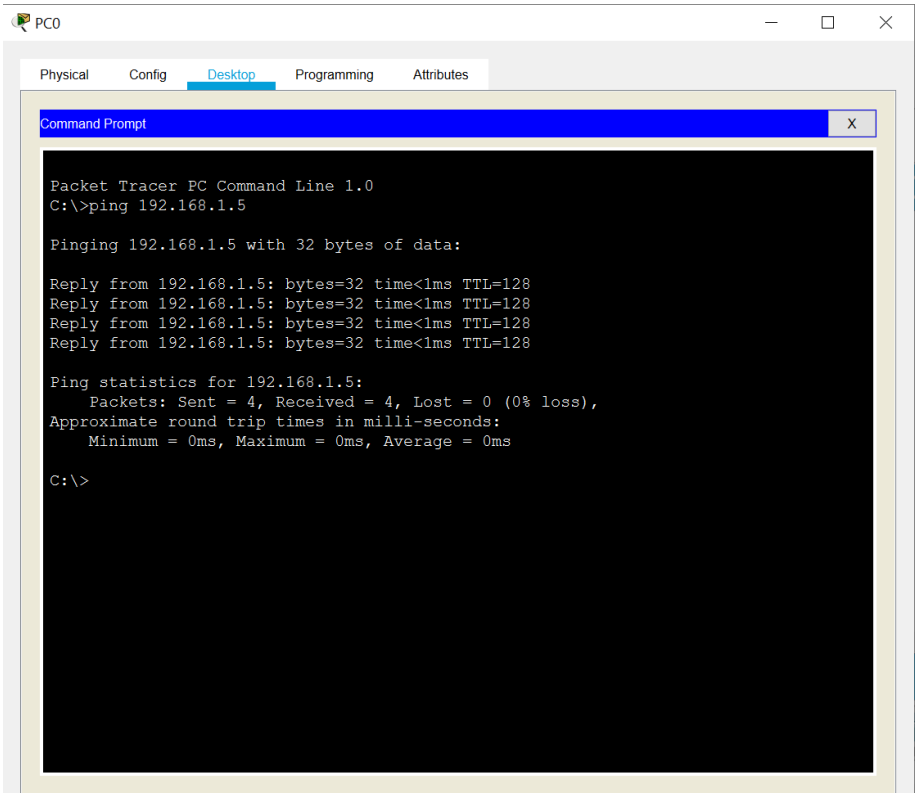
SWITCH>>CONF>>FASTETHERNET 0/?>>PORT>>REMOVE TICK



FastEthernet 0/8 Port Status is OFF

Step 3. To check if the computers of the same department are pinging, we are going to use the command prompt.

PC(192.168.1.2)>>DESKTOP>>COMMAND PROMPT



IP 192.168.1.2 PC is pinging 192.168.1.5 PC

So we have successfully completed the department communication using GUI Mode.

2. CLI MODE(Command Line Interface):

SWITCH>>CLI>>CODE

```
Password:

Switch>en
Password:
Switch#sh run
Building configuration...

Current configuration : 1634 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch
!
enable password 7 0820424F07000437405E
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 --More--
```

```
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport trunk allowed vlan 2-1001
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
!
interface FastEthernet0/3
 switchport access vlan 20
!
interface FastEthernet0/4
 switchport access vlan 30
!
interface FastEthernet0/5
 switchport access vlan 40
 switchport trunk allowed vlan 2-9,11-19,21-29,31-1001
 switchport mode access
!
interface FastEthernet0/6
 switchport trunk allowed vlan 2-1001
 switchport mode trunk
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 --More--
```

```
interface FastEthernet0/8
 shutdown
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 --More--
```

```
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface Vlan1
 ip address 10.10.10.1 255.255.255.0
 shutdown
!
!
!
!
 --More--
```

```
!
interface Vlan1
 ip address 10.10.10.1 255.255.255.0
 shutdown
!
!
!
!
line con 0
 password 7 0820424F07000437405E
 login
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end


Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
```

3. **COLLEGE ROUTER**: Used to connect campus network to the internet. Also it allows the computers to communicate between different VLANs. The code configuration of college router is done as follows-

   COLLEGE ROUTER>>CLI>>CODE

```
Password:

Router>en
Password:
Router#sh run
Building configuration...

Current configuration : 1501 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
!
!
enable password 7 0820424F07000437405E
!
!
!
ip dhcp pool VLAN10
!
!
!
ip cef
 --More-- |
```

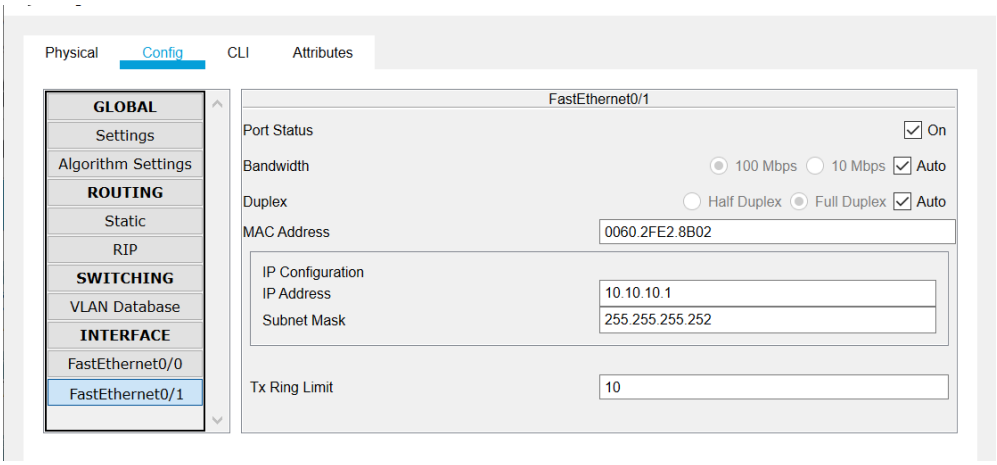
```
interface FastEthernet0/0
 no ip address
 ip access-group 1 in
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 bandwidth 40000
 encapsulation dot1Q 10
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
!
interface FastEthernet0/0.20
 bandwidth 30000
 encapsulation dot1Q 20
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
!
interface FastEthernet0/0.30
 bandwidth 20000
 encapsulation dot1Q 30
 ip address 192.168.3.1 255.255.255.0
 ip nat inside
!
interface FastEthernet0/0.40
 bandwidth 10000
 encapsulation dot1Q 40
 ip address 192.168.4.1 255.255.255.0
 --More--
```

```
interface FastEthernet0/1
 ip address 10.10.10.1 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip nat pool ananya 117.117.117.1 117.117.117.1 netmask 255.255.255.248
ip nat inside source list 1 pool ananya overload
ip nat inside source static 192.168.1.100 117.117.117.3
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.10.2
!
ip flow-export version 9
!
!
access-list 1 deny host 192.168.2.3
access-list 1 permit any
!
!
!
!
!
!
line con 0
 --More--
```

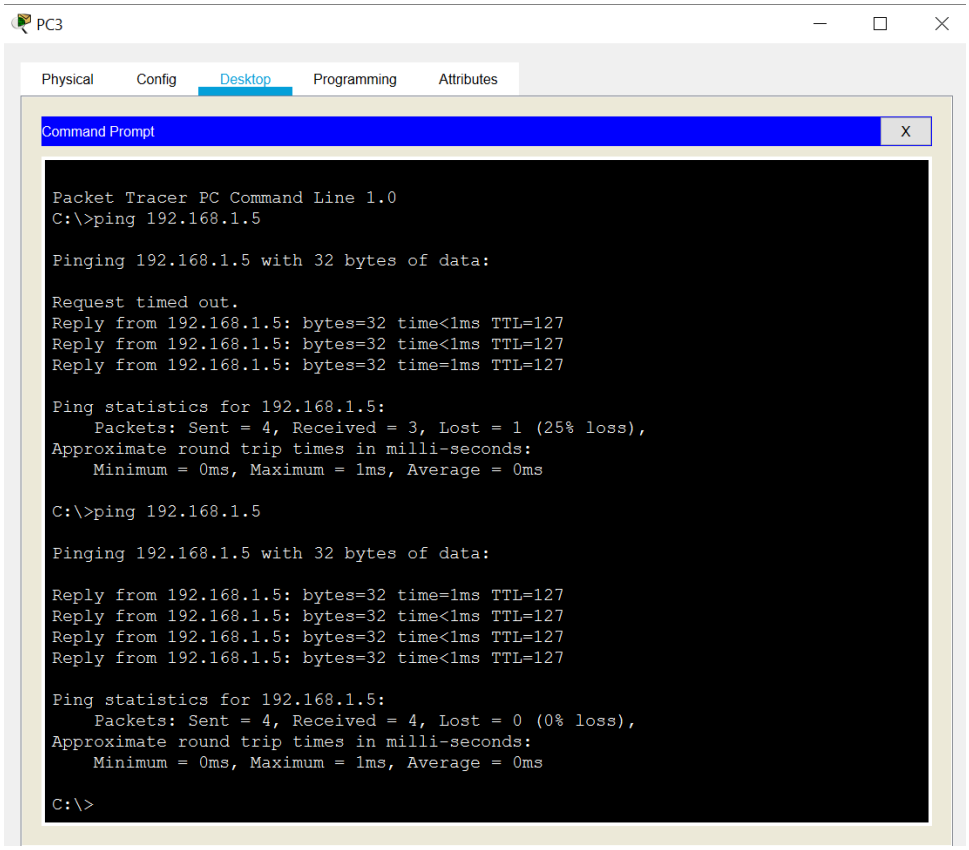
```
ip flow-export version 9
!
!
access-list 1 deny host 192.168.2.3
access-list 1 permit any
!
!
!
!
!
!
line con 0
 password 7 0820424F07000437405E
 login
!
line aux 0
!
line vty 0 4
 password 7 0820424F07000437405E
 login
!
!
!
end


Router#
Router#
Router#
```

COLLEGE ROUTER>>CONFIGURATION>>FastEthernet 0/1



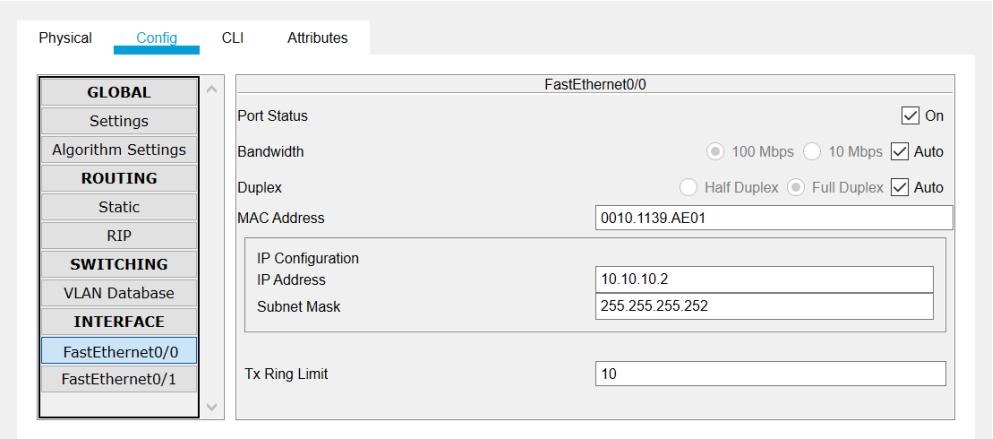
COLLEGE ROUTER IP ADDRESS



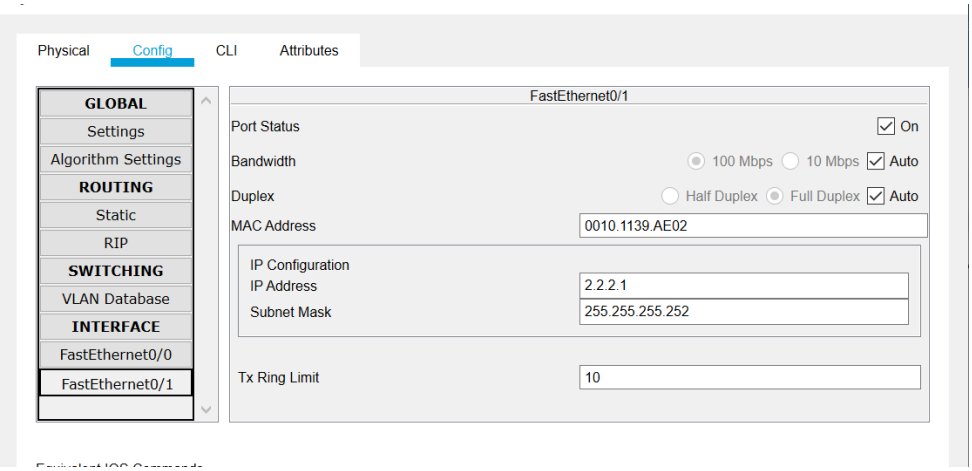
IP 192.168.4.2 PC is pinging 192.168.1.5 PC

4. **ISP ROUTER:** Connection between ISP Server and College Router.

ISP ROUTER>>CONFIG>>FAST ETHERNET 0/?>>IP ADDRESS>>SUBNET MASK



ISP ROUTER FAST ETHERNET 0/0 CONNECTED TO COLLEGE ROUTER



ISP ROUTER FAST ETHERNET 0/1 CONNECTED TO TEST SERVER

CODING IN CLI MODE:

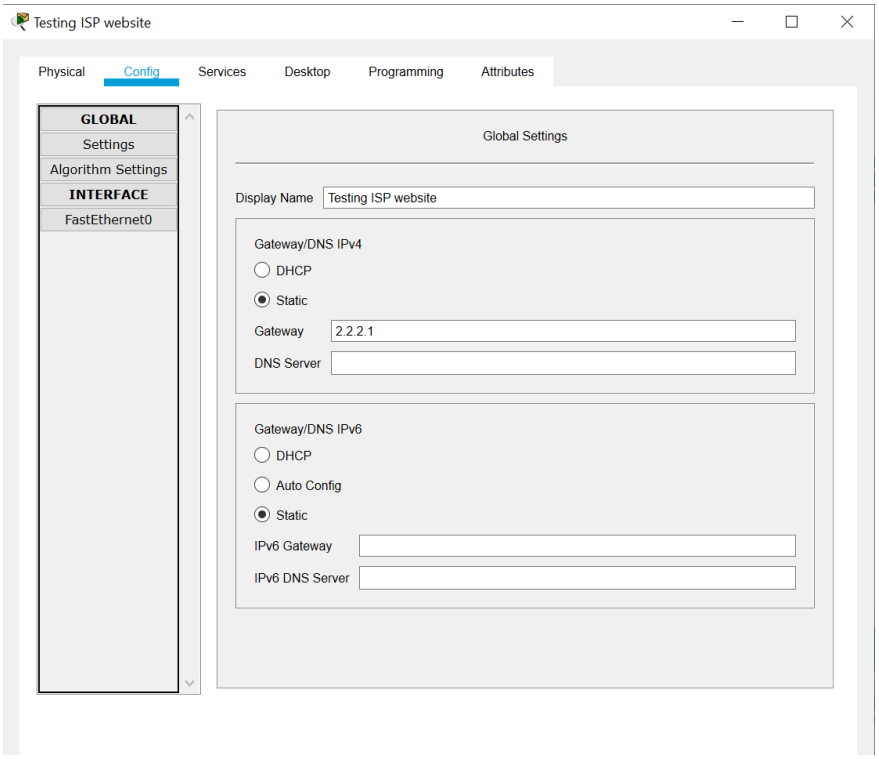
```
Router>en
Router#sh run
Building configuration...

Current configuration : 627 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
 --More--
```

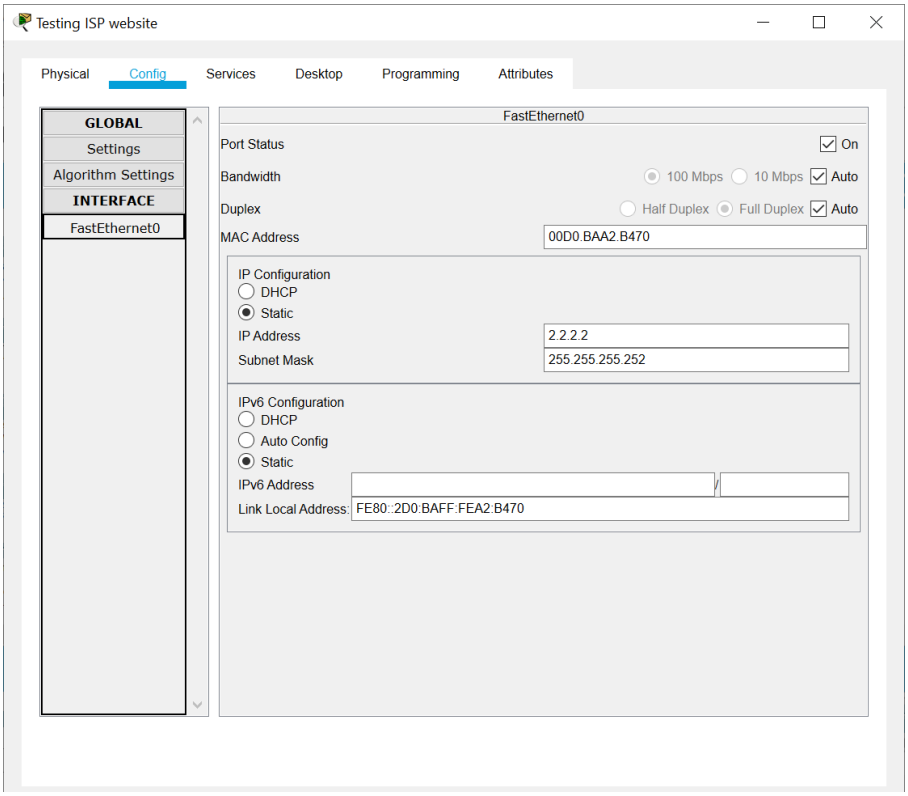
```
interface FastEthernet0/0
 ip address 10.10.10.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 2.2.2.1 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 117.117.117.0 255.255.255.0 10.10.10.1
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
!
 --More--
```

5. TEST SERVER:

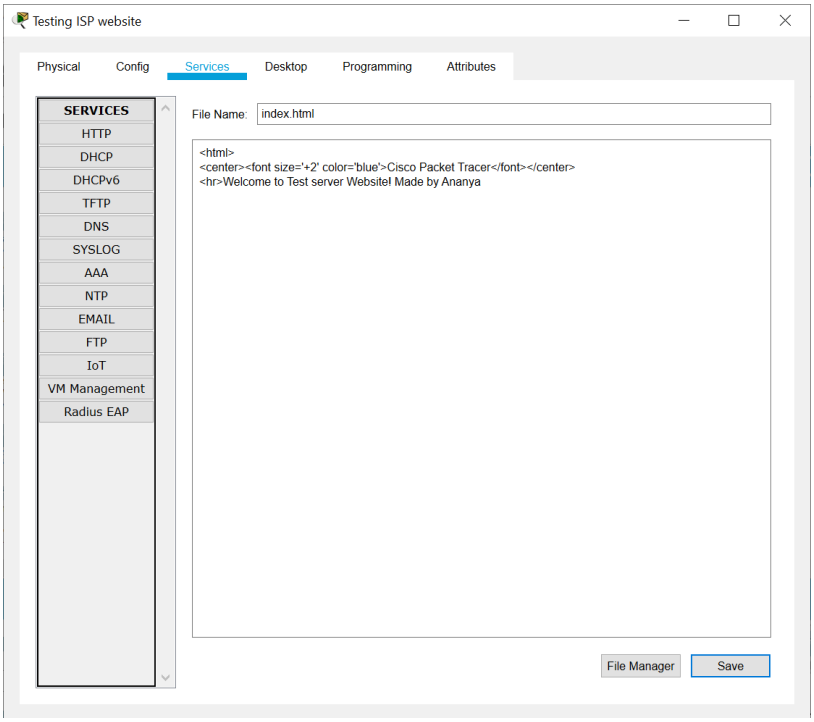
TEST SERVER>>CONFIG>>GATEWAY



TEST SERVER>>CONF>>FAST ETHERNET 0>>IP ADDRESS>> SUBNET MASK



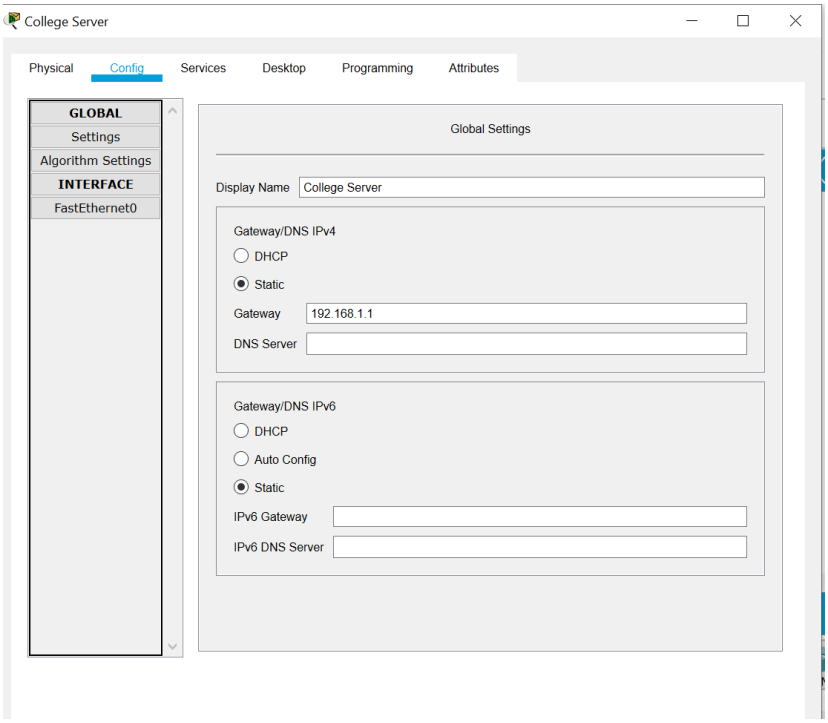
TEST SERVER>>SERVICES>>INDEX.HTML>>EDIT>>SAVE



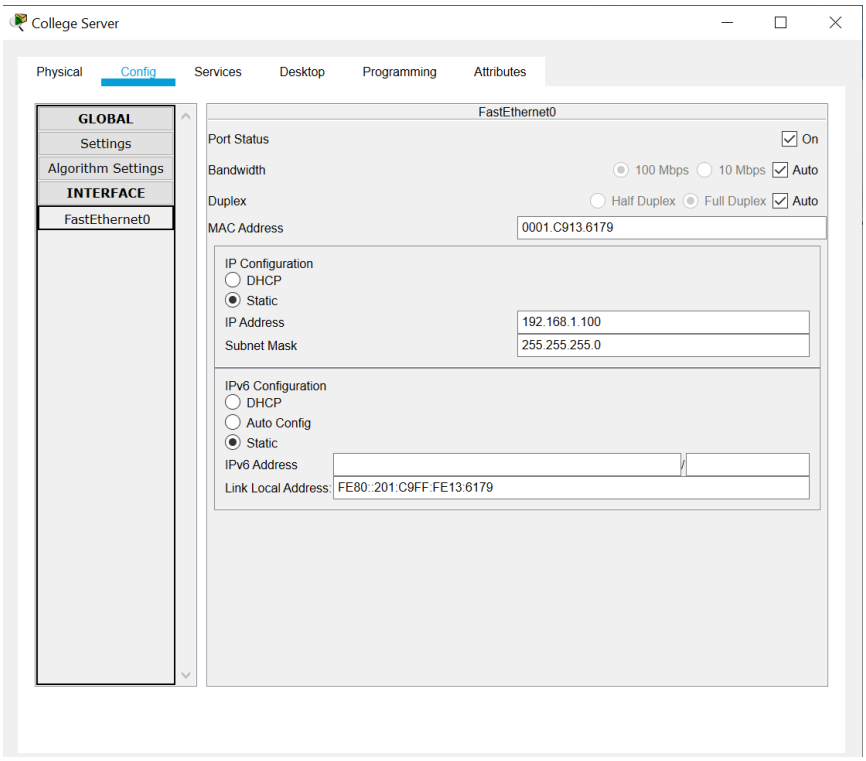
2.2.2.2 OR w.w.w.isp.com

6. COLLEGE SERVER:

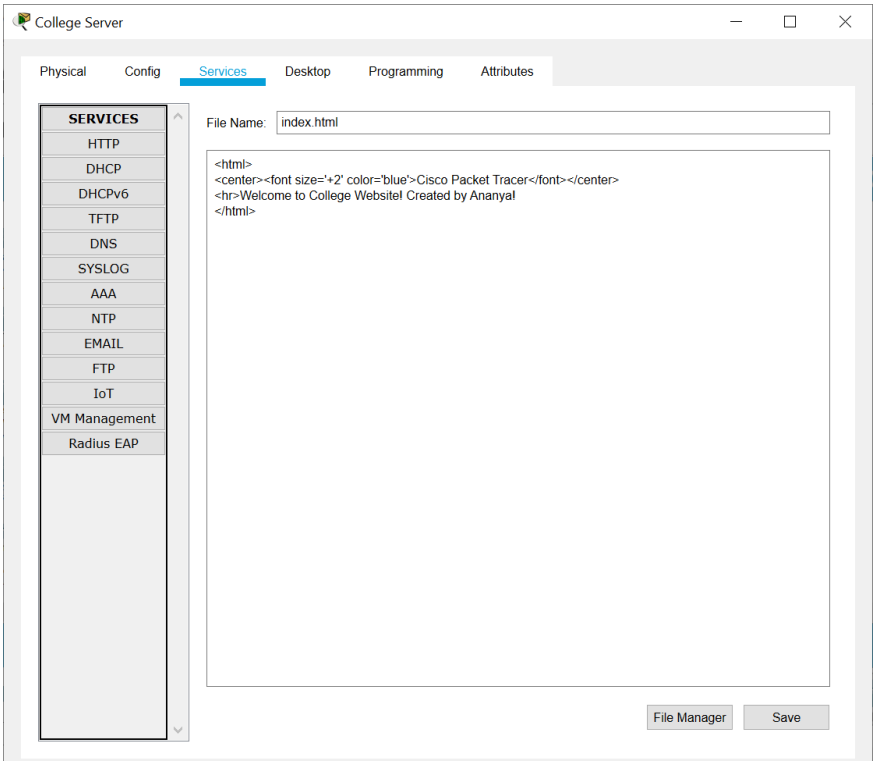
COLLEGE SERVER>>CONFIG>>GATEWAY



COLLEGE SERVER>>CONF>>FAST ETHERNET 0>>IP ADDRESS>> SUBNET MASK

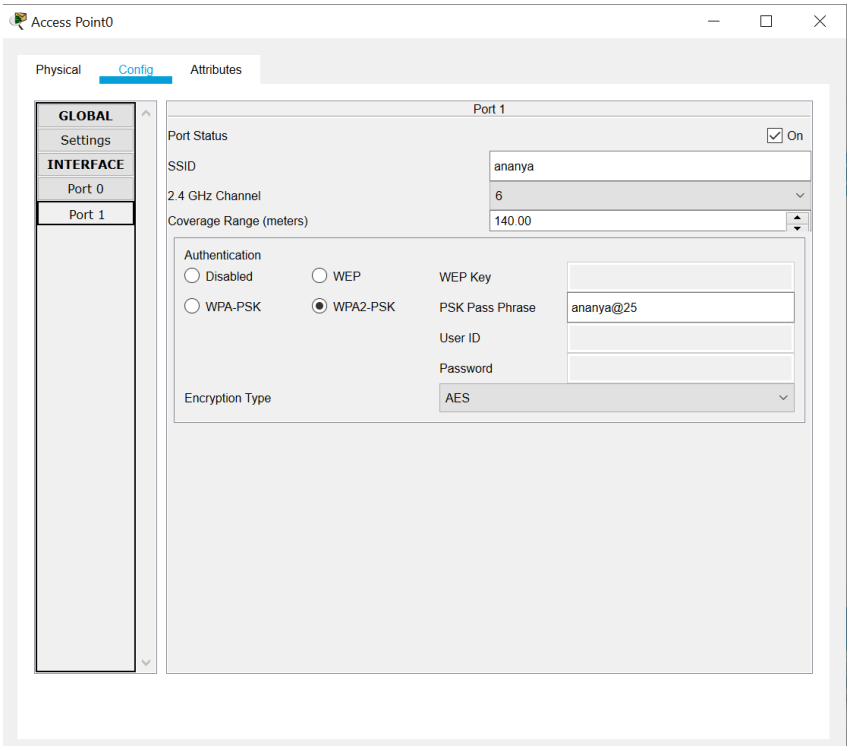


COLLEGE SERVER>>SERVICES>>INDEX.HTML>>EDIT>>SAVE



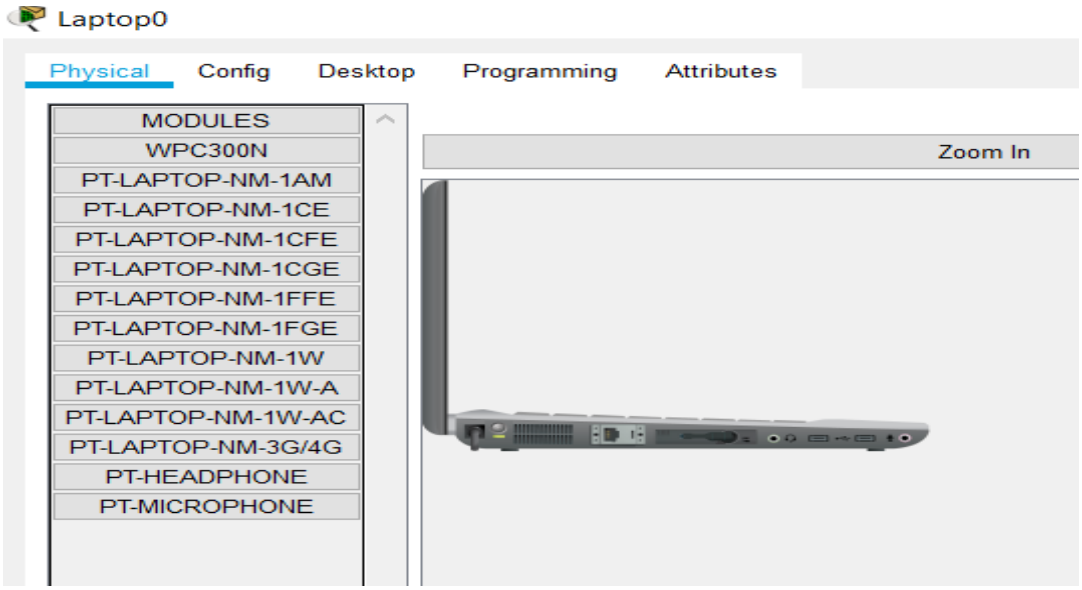
192.168.1.100 OR w.w.w.college.com

7. ACCESS POINT:

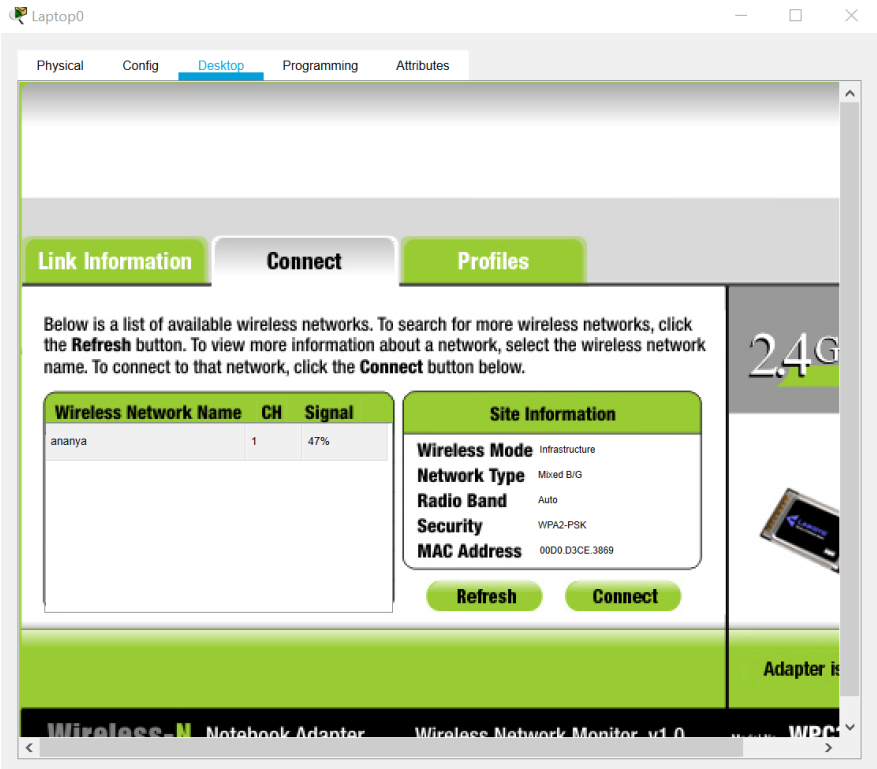


8. LAPTOP:

Coming to the configuration of laptop, firstly I have changed the wired connectivity of laptop to a wireless connection one using WPC300N Module as follows-



LAPTOP>>DESKTOP>>PC WIRELESS>>CONNECT



Using all these methodologies I have placed the components at correct places and connected them by means of wire and assigned all the above-mentioned configurations to all the components and finally designed a CAMPUS AREA NETWORK.

SOME IMPORTANT CODES:

ISP ROUTER

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#ip route 117.117.117.0 255.255.255.248 10.10.10.1
Router(config)#end
Router#wr
```

COLLEGE ROUTER

1) Configure the Access control-list ACL 1-99 EXTENDED ACL - SPECIFIC

```
Router#conf t
```

Router(config)#access-list 1 deny 192.168.2.3
Router(config)#access-list 1 permit any

2) Configure the default Routing towards ISP

Router(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2

3) Configuration of NAT

Router(config)#ip nat pool RTTC 117.117.117.1 117.117.117.1 netmask 255.255.255.248
Router(config)#ip nat inside source static 192.168.1.100 117.117.117.3
Router(config)#ip nat inside source list 1 pool RTTC overload

4) Implementation of ACL

Router(config)#int fa0/0
Router(config-subif)#ip access-group 1 in
Router(config-subif)#exit

5) Implementation of NAT on LAN / WAN links

Router(config)#interface fa0/1 ----- wan
Router(config-if)#ip nat outside
Router(config-if)#exit

Router(config)#interface fa0/0.10   -- CSE
Router(config-if)#ip nat inside
Router(config-if)#exit

Router(config)#interface fa0/0.20   -- IT
Router(config-if)#ip nat inside
Router(config-if)#exit

Router(config)#interface fa0/0.30   -- ECE
Router(config-if)#ip nat inside
Router(config-if)#exit

Router(config)#interface fa0/0.40   -- EEE
Router(config-if)#ip nat inside
Router(config-if)#exit

Router#wr

Verification commands

Router#debug ip nat

Router#show ip nat translations

Give security to a Router

1) Console :

```
Router> user mode
Router>enable
Router# priviliged mode
Router#confgiure terminal
Router(config)#
Router(config)#line con 0
Router(config-line)#password rttc
Router(config-line)#login
Router(config-line)#end
Router#write
```

2) enable password

```
Router(config)#
Router(config)#enable password abcd
Router(config)#end
Router#wr
```

3) Telnet password

```
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#end
Router#
Router#write
```

4) secure the password

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#service password-encryption
Router(config)#end
Router#
Router#write
```

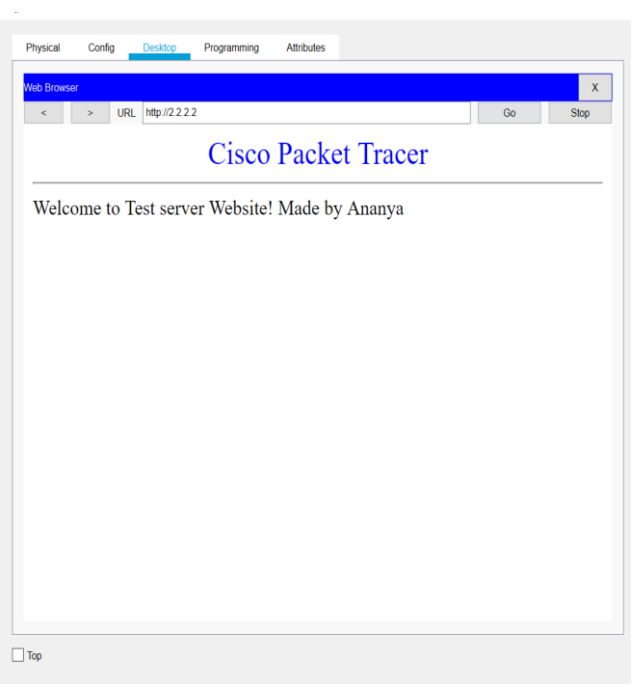
SWITCH:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range fa0/11-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#end
Switch#write
Building configuration...
[OK]
Switch#
```

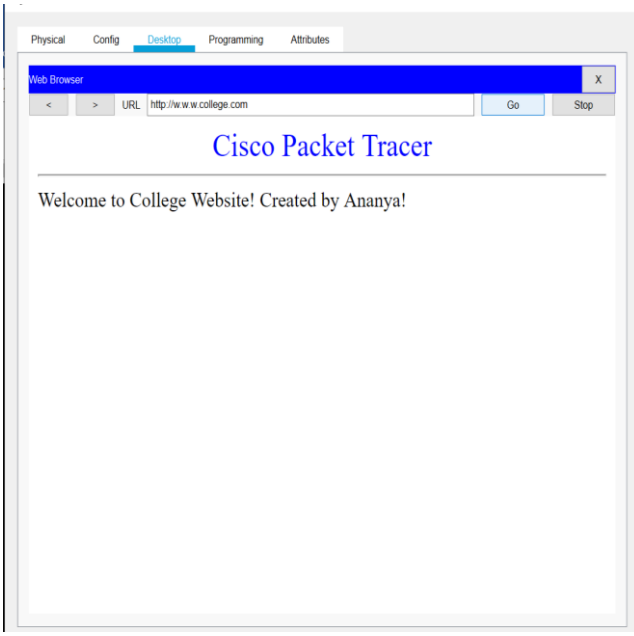
RESULTS:

As the college internet is accessed in each of computer on web browser it is checked as follows-

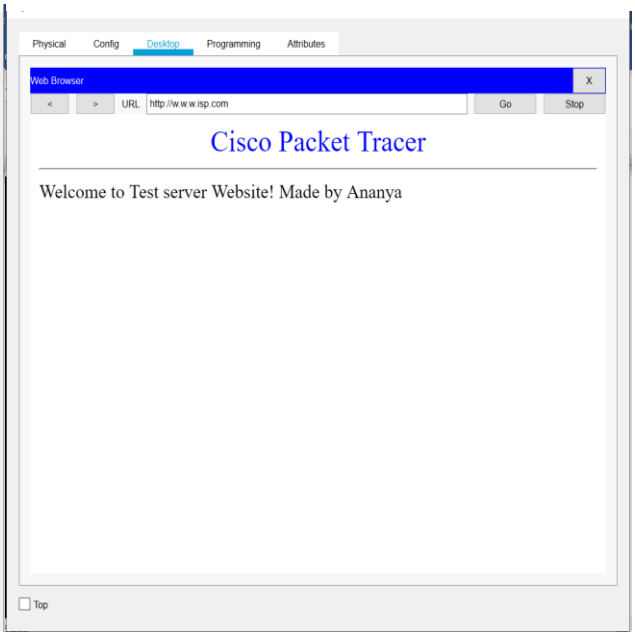
BROWSER 192.168.1.100



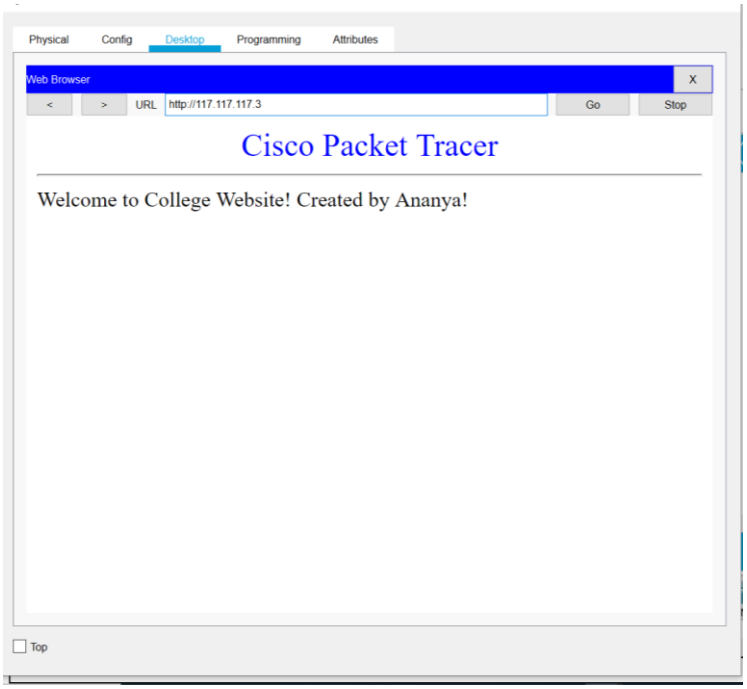
BROWSER 2.2.2.2



BROWSER w.w.w.college.com

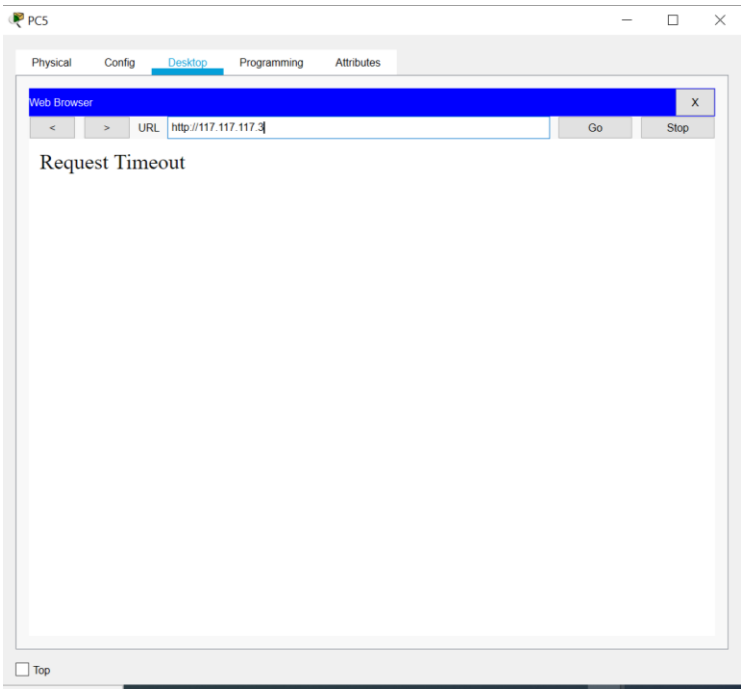


BROWSER w.w.w.isp.com



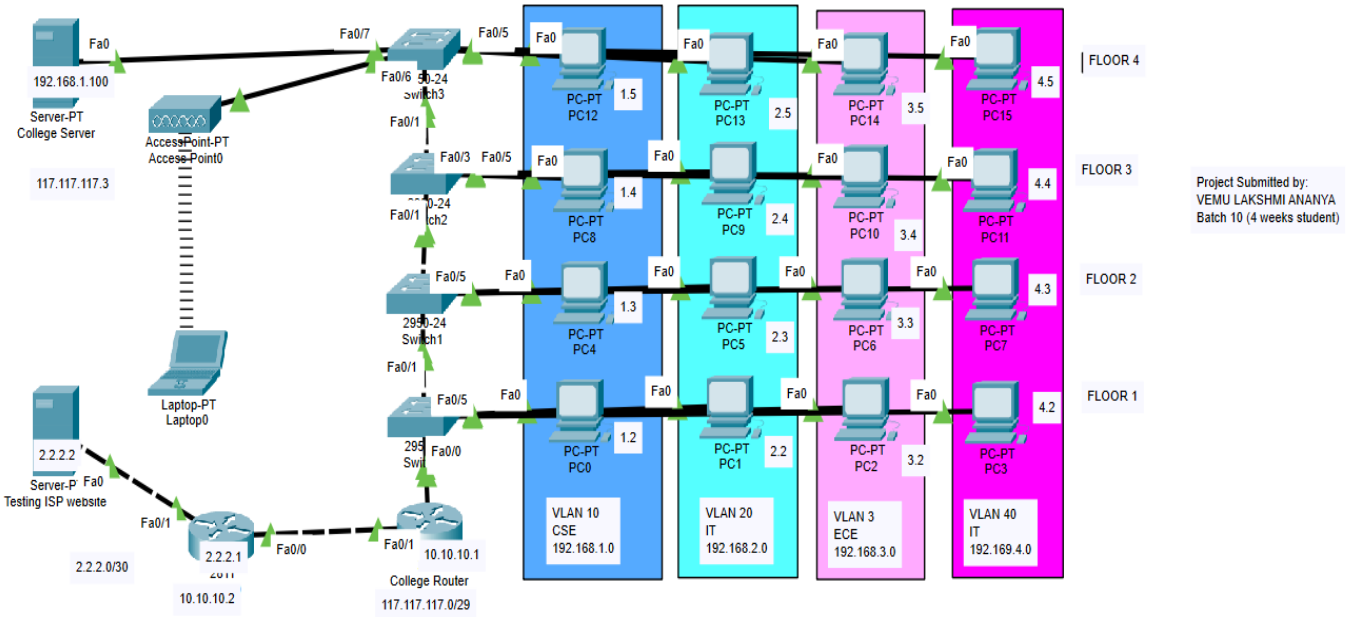
BROWSER 117.117.117.3

Through this I am able access the web browser.



INTERNET ACCESS DENIAL TO PC 5 - 192.168.2.3

FINAL NETWORK:



USES OF VLAN:

- VLANs enable logical grouping of end-stations that are physically dispersed on a network.
- When users on a VLAN move to a new physical location but continue to perform the same job function, the end-stations of those users do not need to be reconfigured. Similarly, if users change their job functions, they need not physically move: changing the VLAN membership of the end-stations to that of the new team makes the users' end-stations local to the resources of the new team.
- VLANs reduce the need to have routers deployed on a network to contain broadcast traffic.
- Flooding of a packet is limited to the switch ports that belong to a VLAN.
- Confinement of broadcast domains on a network significantly reduces traffic.
- By confining the broadcast domains, end-stations on a VLAN are prevented from listening to or receiving broadcasts not intended for them. Moreover, if a router is not connected between the VLANs, the end-stations of a VLAN cannot communicate with the end-stations of the other VLANs.

USES OF NAT:

- Reuse of Private IP addresses
- Enhancing security for private networks by keeping internal addressing private from the external network
- Connecting a large number of hosts to the global Internet using a smaller number of public (external) IP address, thereby conserving IP address space.

USES OF ACL:

- Improve network performance.
- Provides security as administrator can configure the access list according to the needs and deny the unwanted packets from entering the network.
- Provides control over the traffic as it can permit or deny according to the need of network.

FUTURE SCOPE OF PROJECT:

This project can be further used in many processes like increasing more and more algorithms and bringing in more simulation techniques.