PROJECT REPORT
BY V ANDAL
PRIYADHARSHINI

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. A LAN 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.

- College campus is a (Ground + 4)5 Floor building.
- Ground Floor have100Mbps connectivity to ISP for Internet with a CISCO 2811 Router with a single LAN port.
- 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.
- 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.
- Administrator has been asked to configure the departments in different VLAN domains and also instructed that the communication between the departments is also required.
- Administrator has been asked to place an Access point for wireless connectivity with security password from the Fourth Floor on need basis
- Administrator has been asked to create security credentials for login to the Router and Switches such that authorized person only logs in.
- 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.
- 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.
- ISP has given 10.10.10.0/30 subnet to college and asked the administrator to configure the WAN link IP 10.10.10.1at College side WAN interface on Router. The Internet IP pool given to college is 117.117.117.0/29.
- Administrator has been instructed to make sure that all computers available in the campus should be connected with Internet.
- 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, the cisco packet tracer is used. 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.

ROUTER: Used to connect campus network to the internet

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

COLLEGE SERVER: Used to connect cellular system to the router

SERVER (testing): To control smart thing registered on it and provide difference server functionalities

PC: Connect to access layer

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.

College Router: The code configuration of college router is done as follows-

```
Current configuration : 1468 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
!
!
enable password 7 08315E471018
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
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
 ip nat inside
!
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
!
router rip
!
ip nat pool priya 117.117.117.1 117.117.117.1 netmask 255.255.255.248
ip nat inside source list 1 pool priya 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
 password 7 08315E471018
 login
!
line aux 0
!
line vty 0 4
 password 7 08315E471018
!
ip flow-export version 9
!
!
access-list 1 deny host 192.168.2.3
access-list 1 permit any
!
!
!
!
!
!
line con 0
 password 7 08315E471018
 login
!
line aux 0
!
line vty 0 4
 password 7 08315E471018
 login
!
!
!
end
```

In ISP Router:

```
Current configuration : 623 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
!
!
!
!
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

```
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 2.2.2.1 255.0.0.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 117.117.117.0 255.255.255.248 10.10.10.1
!
ip flow-export version 9
!
```

IN Switch:

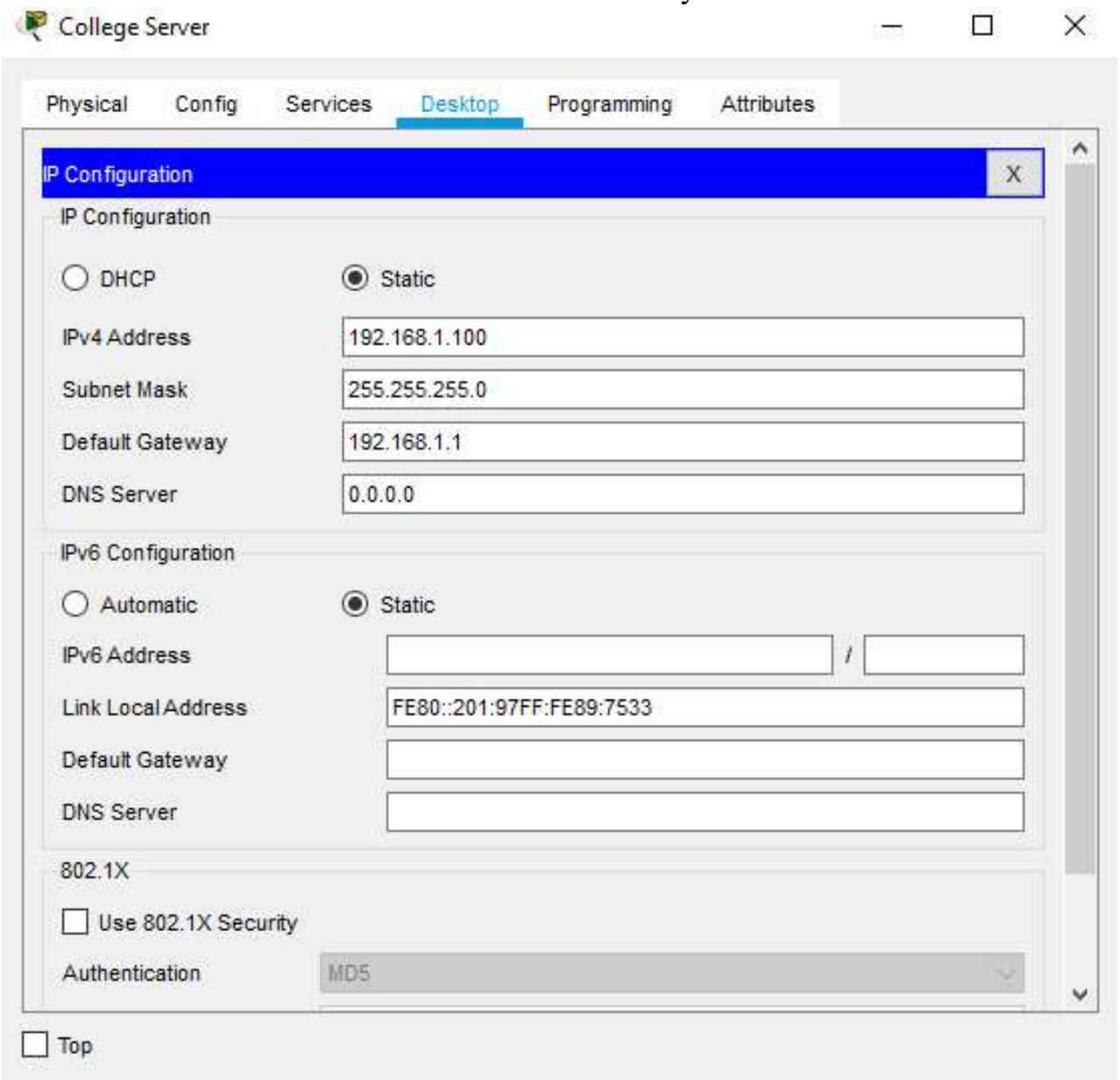
```
Current configuration : 1490 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch
!
enable password 7 08701E1D5D4C
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
!
interface FastEthernet0/2
 switchport access vlan 20
!interface FastEthernet0/3
  switchport access vlan 30
 !
 interface FastEthernet0/4
  switchport access vlan 40
 !
 interface FastEthernet0/5
  switchport trunk allowed vlan 2-1001
  switchport mode trunk
 !
 interface FastEthernet0/6
  switchport trunk allowed vlan 2-1001
  switchport mode trunk
 !
 interface FastEthernet0/7
  shutdown
 !
 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
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
 password 7 08701E1D5D4C
 login
!
```

```
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

In all the 4 switches the same type of configuration is done.

I have created 4 Vlans I.e., vlan 10, 20, 30, 40 for CSE, IT, ECE, EEE departments respectively. In all the computers assigned all the IP Address, Subnet Mask Value, Default ip GATEWAY. For CSE department IP 192.168.1.(2,3,4,5) are used for computers with gateway as 192.168.1.1, like way 192.168.2.(2, 3, 4, 5) in IT, gateway as 192.168.2.1. 192.168.3.(2, 3, 4, 5) in ECE, gateway as 192.168.3.1, 192.168.4.(2, 3, 4, 5) in EEE, gateway as 192.168.4.1. Coming to the Access point I have configured the ports 0, 1 with respective measures like assigning SSID, etc. In College Server I have assigned 192.168.1.100 as IP address and 255.255.255.0 as subnet mask and 192.168.1.1 as Default Gateway.



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-

For the IP Address allocation, I have configured 192.168.1.0, 255.255.255.0 as subnet mask, 192.168.1.1 as default gateway.

Password is also been created in order to maintain secrecy. The configuration for password setting is as follows:

1) Console:

Router> user mode

Router>enable

Router# priviliged mode

Router#confgiure terminal

Router(config)#

Router(config)#line con 0

Router(config-line)#password priya

Router(config-line)#login

Router(config-line)#end

Router#write

2) enable password

Router(config)#

Router(config)#enable password priya

Router(config)#end

Router#wr

3) Telnet password

Router(config)#line vty 0 4

Router(config-line)#password dharshini

Router(config-line)#login

Router(config-line)#end

Router#

Router#write

4) secure the password

Router#configure terminal

Router(config)#

Router(config)#service password-encryption

Router(config)#end

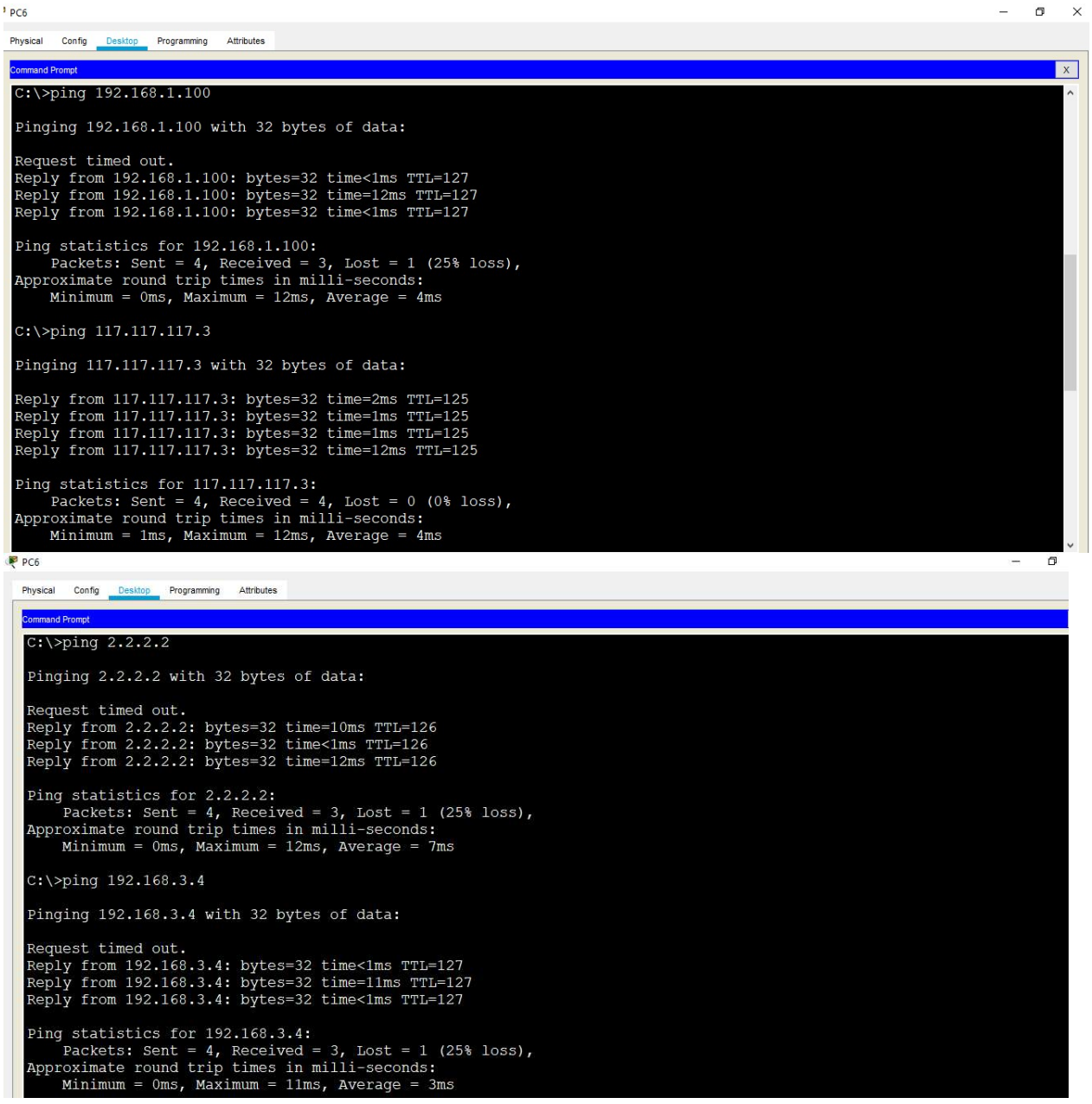
Router#

Router#write

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.

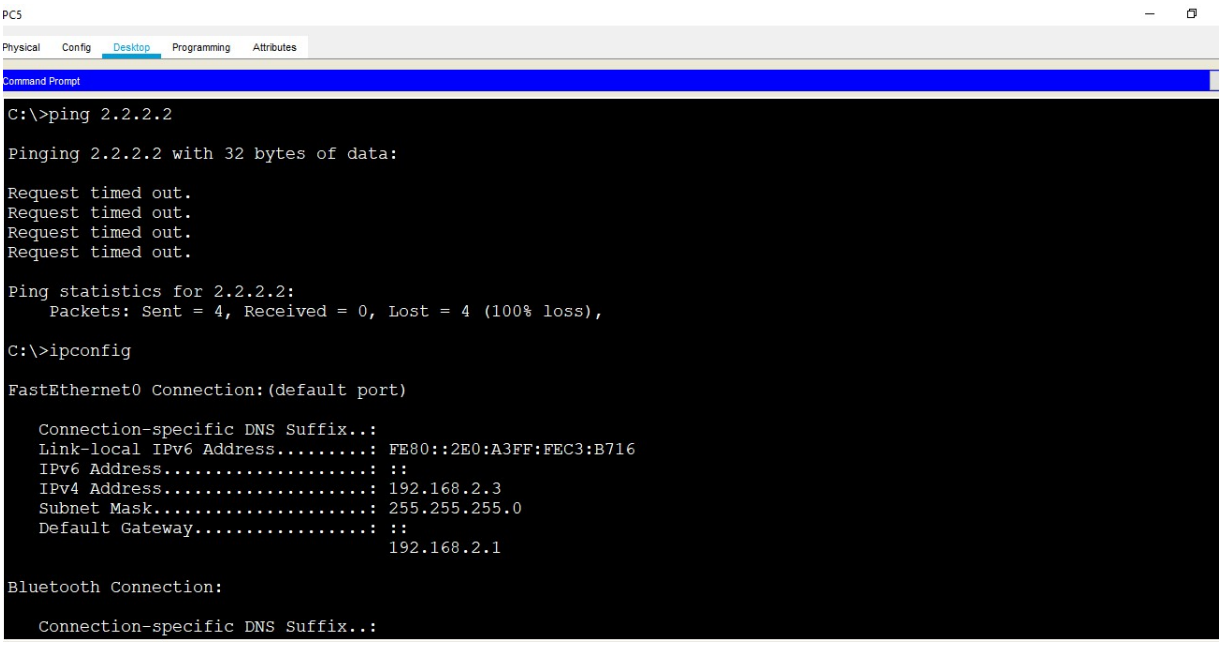
RESULTS:

1.First point in this results criterion is communication in same vlan. It is tested by PINGING from a computer to a computer of same vlan as follows-



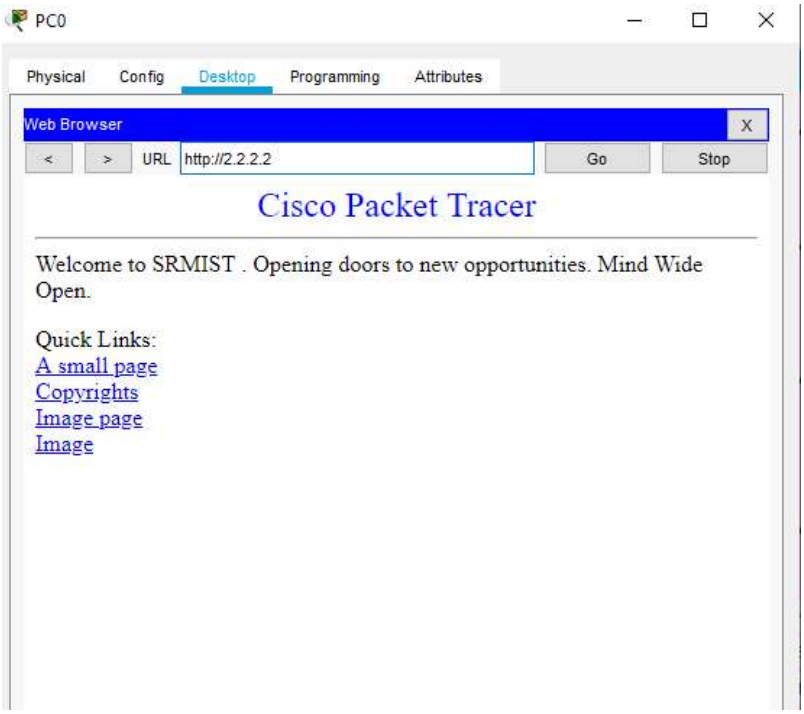
As shown in the figure I started pinging from 2.4 PC to 3.4 and the server and got reply from every PC which proves my PINGING of same vlan communication.

1. The pinging in 2.3 pc is shown where we have blocked the access to the website as shown: so the result says request timed out

2. 

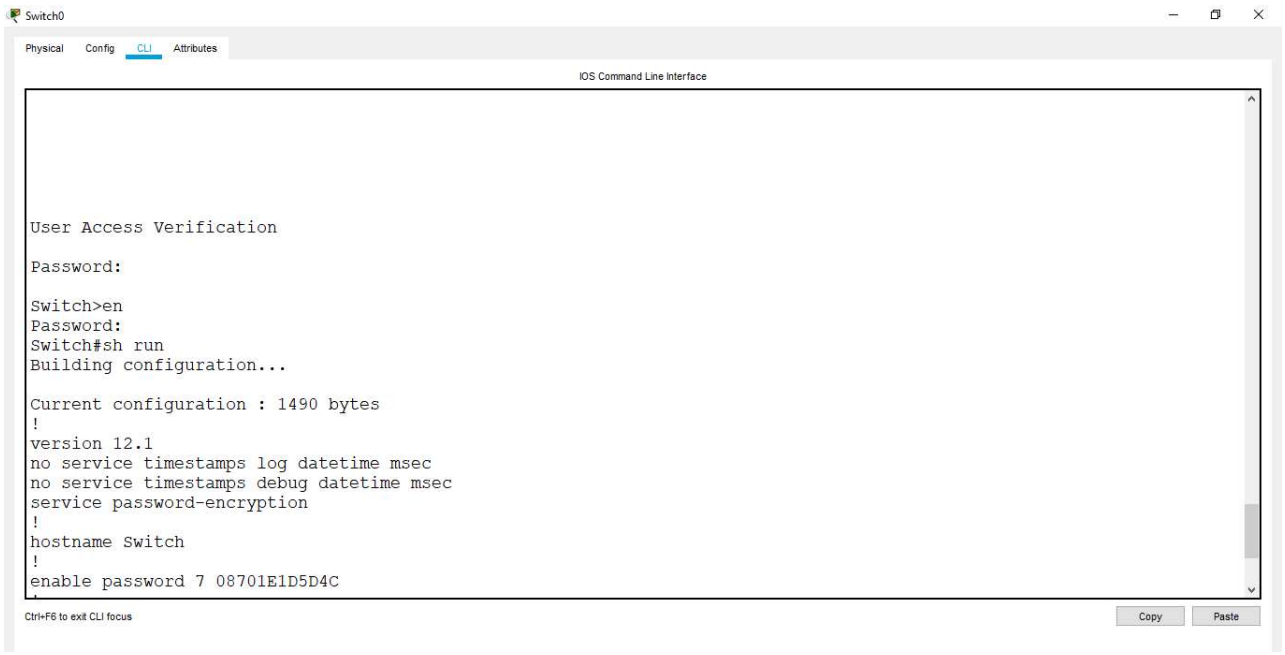
All these show the successful response of INTER VLAN communication.

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



Through this I am able access the web browser.

As a part of security for all the Routers and Switches I have set a password to them so that it can be accessed and used to change any configurations by authorized persons only. The password is also been encrypted.



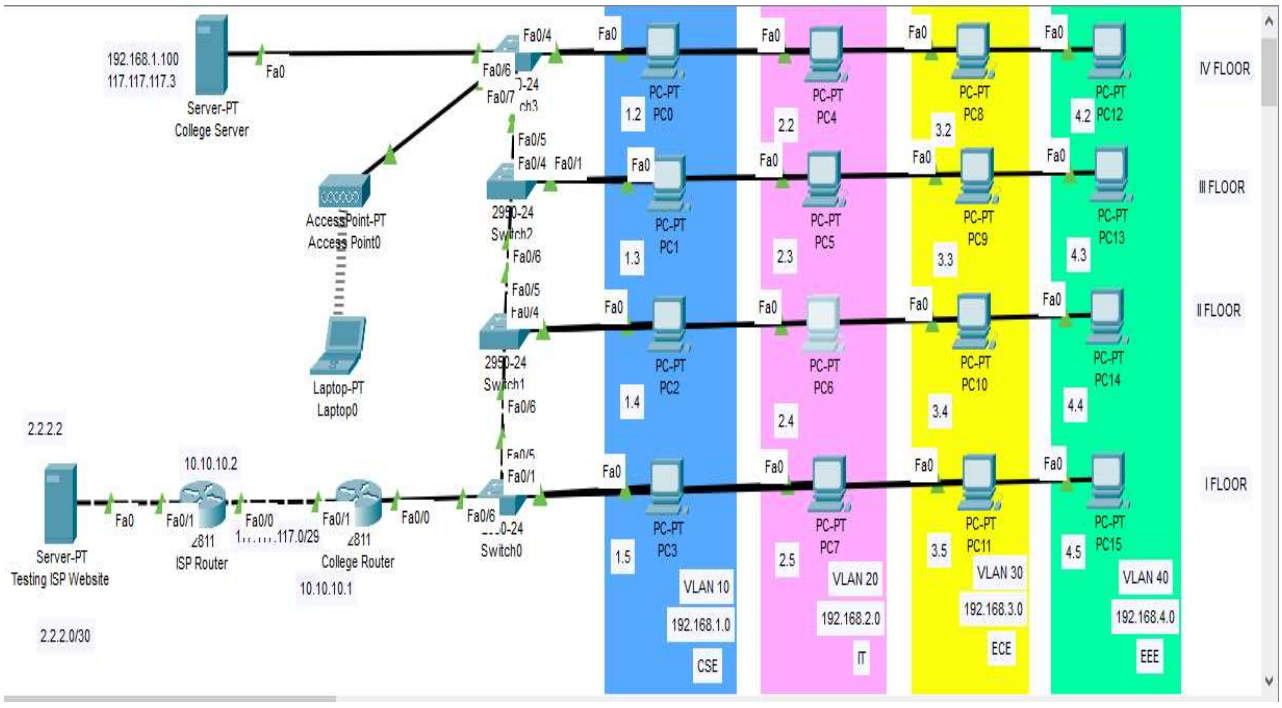
2. IP NAT Translation:

```
Pro  Inside global     Inside local       Outside local
Outside global
---  117.117.117.3     192.168.1.100      ---
---
tcp 117.117.117.1:1025 192.168.1.2:1025
117.117.117.3:80   117.117.117.3:80
tcp 117.117.117.3:80   192.168.1.100:80
117.117.117.1:1025 117.117.117.1:1025
```

3. Running configuration of college router:

```
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
 ip nat inside
!
interface FastEthernet0/1
 ip address 10.10.10.1 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
!
```

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.
- 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. The packet tracer is used to implement the network of the project and clarity the conception of the VLANs, DHCP, phone, website server and router configurations. Networking devices are expensive so the packet tracer is easy and best to implement structure of the network before implementing it on the real ground. Also in the paper, the VLANs provide the security, broadcast control and physical layer transparency while VTP reduce configuration and integrate VLAN management for any changing on VTP server then it will distributed to other switches in the same VTP domain therefore the time of configuration the same VLAN is reduce.

BY- V ANDAL PRIYADHARSHINI
(SRMIST)