AN INTERNSHIP PROJECT ON

CAMPUS AREA NETWORK USING VLAN

SUBMITTED BY

DLN PRANITHA

REG ID: RTTCHYDINTS52549

SUBMITTED TO

HEAD, RTTC HYD

PROJECT COMPLETED UNDER THE GUIDANCE OF

BSNL

RTTC

INDEX

LIST OF FIGURES

ABSTRACT

A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.

In essence, a VLAN is a collection of devices or network nodes that communicate with one another as if they made up a single LAN, when in reality they exist in one or several LAN segments. In a technical sense, a segment is separated from the rest of the LAN by a bridge, router, or switch, and is typically used for a particular department. This means that when a workstation broadcasts packets, they reach all other workstations on the VLAN but none outside it.

VLANs are cost-effective, because workstations on VLANs communicate with one another through VLAN switches and don’t require routers unless they are sending data outside the VLAN.

VLANs offer more flexibility than nonvirtual networking solutions. VLANs can be configured and assigned based on port, protocol, or subnet criteria, making it possible to alter VLANs and change network design when necessary.

VLANs decrease the amount of administrative oversight required by network overseers like managed services providers (MSPs). VLANs allow network administrators to

automatically limit access to a specified group of users by dividing workstations into different isolated LAN segments.

PROJECT 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.

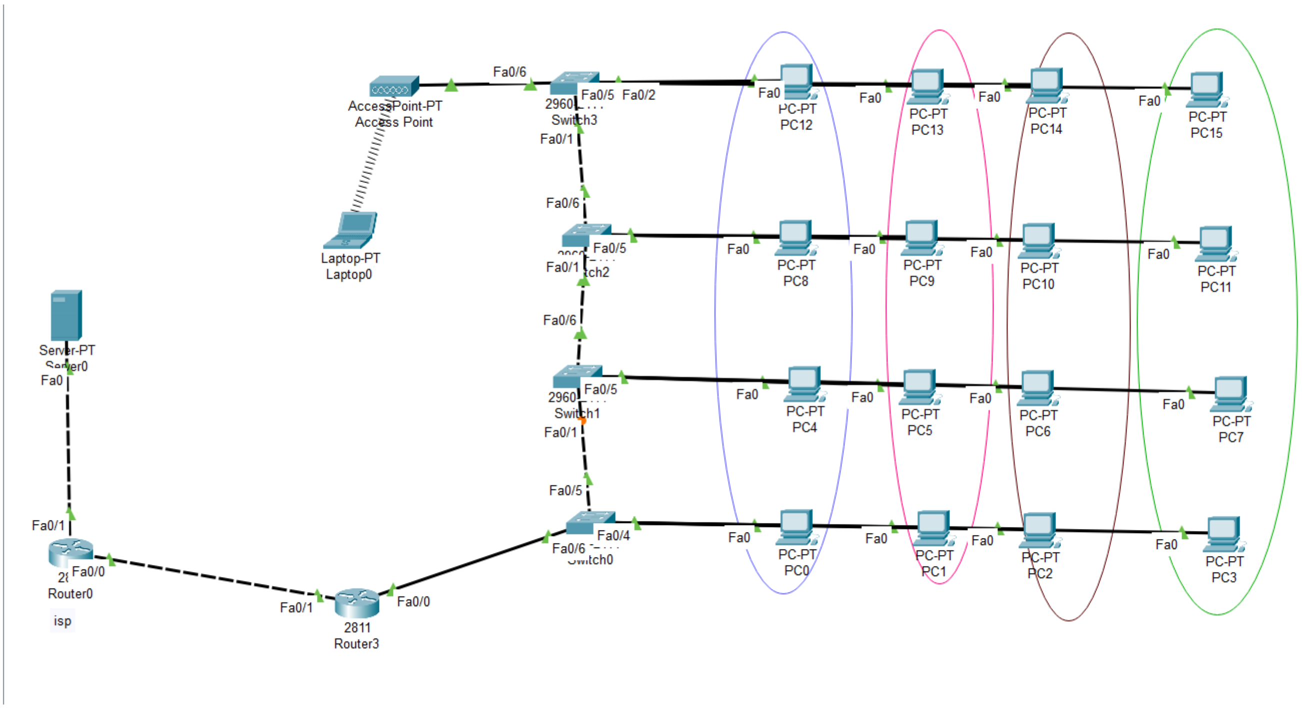
8. Administrator has been asked to make sure that if anyone connect a PC in the vacant ports of switch in any floor they should not be connected to Network.
9. Administrator has been asked to allocate 40 Mbps bandwidth to CSC department, 30 Mbps bandwidth to IT department, 20 Mbps bandwidth for ECE department & 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 by ISP 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)
13. DHCP Protocol and Configuration of DHCP on CISCO Router for automatic assignment of IP addresses.

14 .Configuration of DNS entries for browsing using URL.

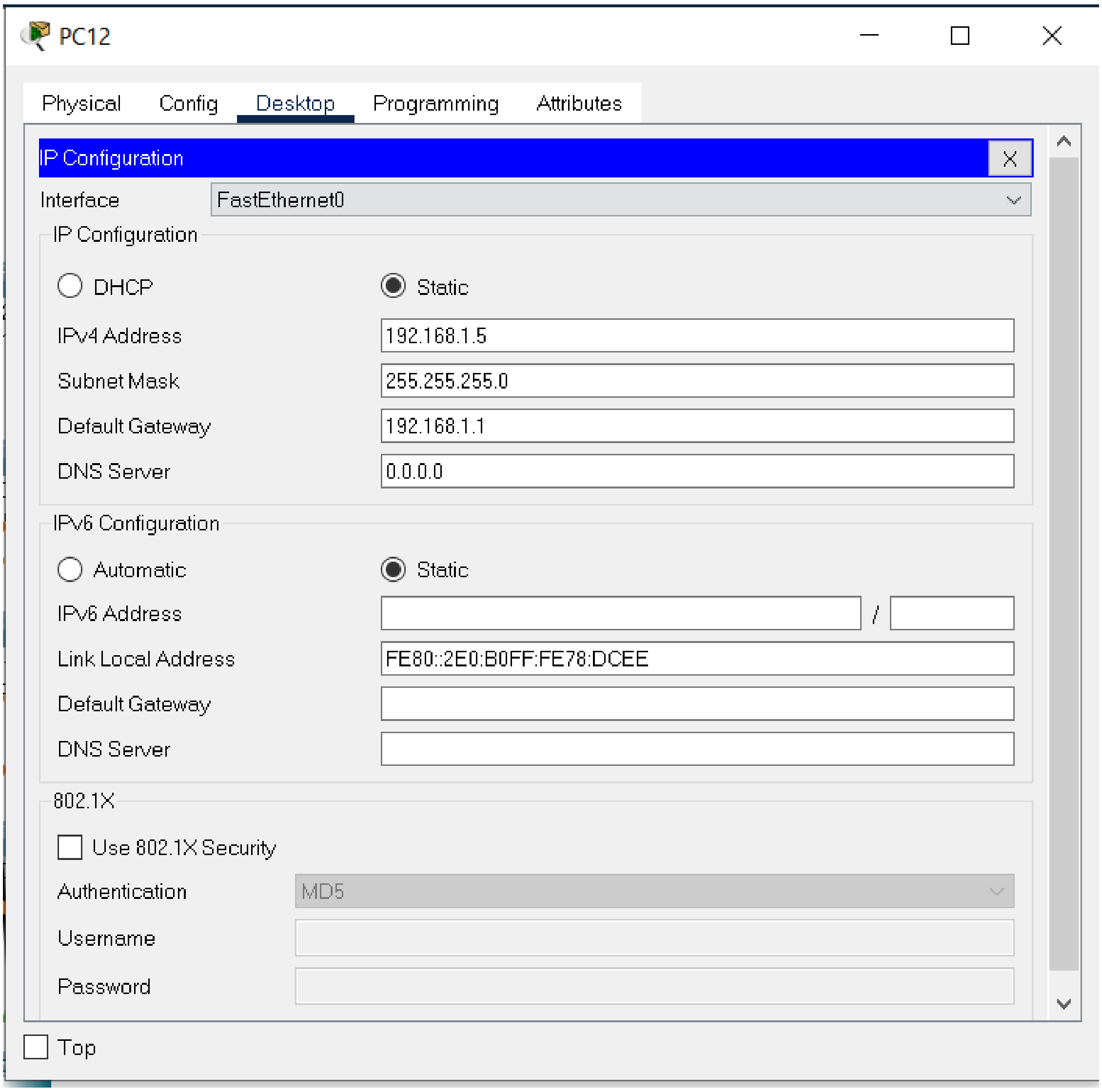
SIMULATION

CONSTRUCTING THE NETWORK



The network is to be constructed in the above manner. It contains 5 floors, the ground being given for the college router and ISP router and the other floors given for respective years. All the end devices in in same department must be configured in same VLAN. It can be done in the following manner.

CONFIGURING THE DEVICES



PC12

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.5

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2E0:B0FF:FE78:DCEE

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:

□ Top

Every device in a network is given an IP address. This IP address can be filled in the Desktop tab of every device. The above is the example of the same.

UNDERSTANDING AND IMPLEMENTING VLAN

The following code is configured in each router to implement VLAN

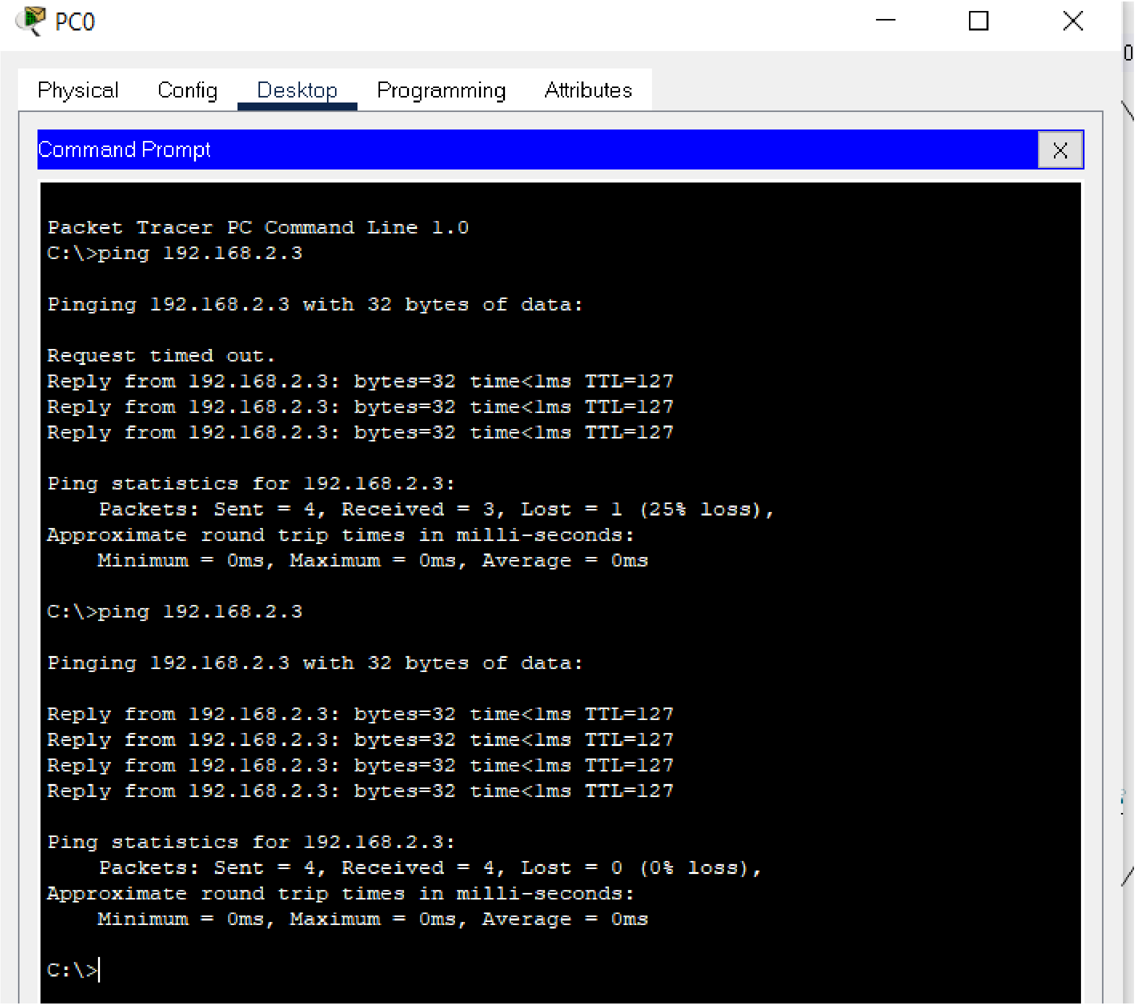
Configuring the Sub interfaces on the router

```
Router#config t
Router(config)#int fa0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#exit

Router(config)#int fa0/0.20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#exit

Router(config)#int fa0/0.30
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int fa0/0.40

Router(config-subif)#encapsulation dot1q 40

Router(config-subif)#ip address 192.168.4.1 255.255.255.0

Router(config-subif)#end


Router#wr
```

This code is configured in a switch

```
Switch>
Switch>en
Switch#conf t
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10

Switch>
Switch>en
Switch#conf t
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20

Switch>
Switch>en
Switch#conf t
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
```

```
Switch>
Switch>en
Switch#conf t
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
```



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

The output when the above code gets implemented.

ASSIGNING BANDWIDTH

It is required to assign different bandwidth and hence the speeds to different departments, this can be done using the following commands

```
Router(config)#int fa0/1
Router(config-subif)#bandwidth ?
Router(config-subif)#bandwidth 40000
Router(config-subif)#end
Router(config)#int fa0/1
Router(config-subif)#bandwidth ?
Router(config-subif)#bandwidth 30000
Router(config-subif)#end
Router(config)#int fa0/1
Router(config-subif)#bandwidth ?
Router(config-subif)#bandwidth 20000
Router(config-subif)#end
Router(config)#int fa0/1
Router(config-subif)#bandwidth ?
Router(config-subif)#bandwidth 10000
Router(config-subif)#end
```

CONFIGURATION OF DHCP ON ROUTER

The following commands are used:

```
Router#config t
Router(config)#ip dhcp pool VLAN10
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 2.2.2.2
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
Router(config)#end
Router#wr
Building configuration...
[OK]
Router#
```

ROUTER SECURITY

It is important to secure the router with password so that no changes can be made without consent of the administrator. The router is secured using the following commands:

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
```

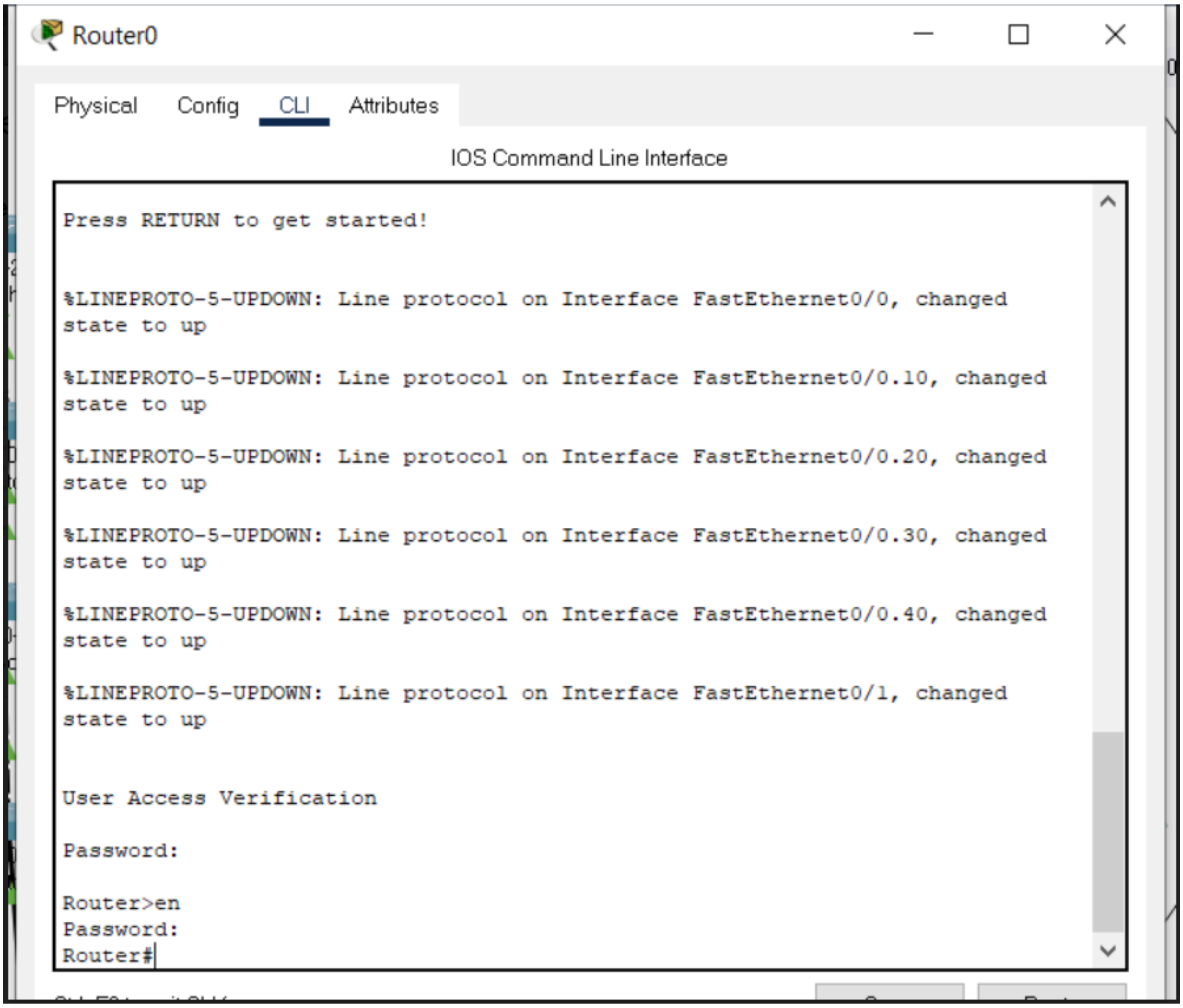
3) Telnet password

```
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

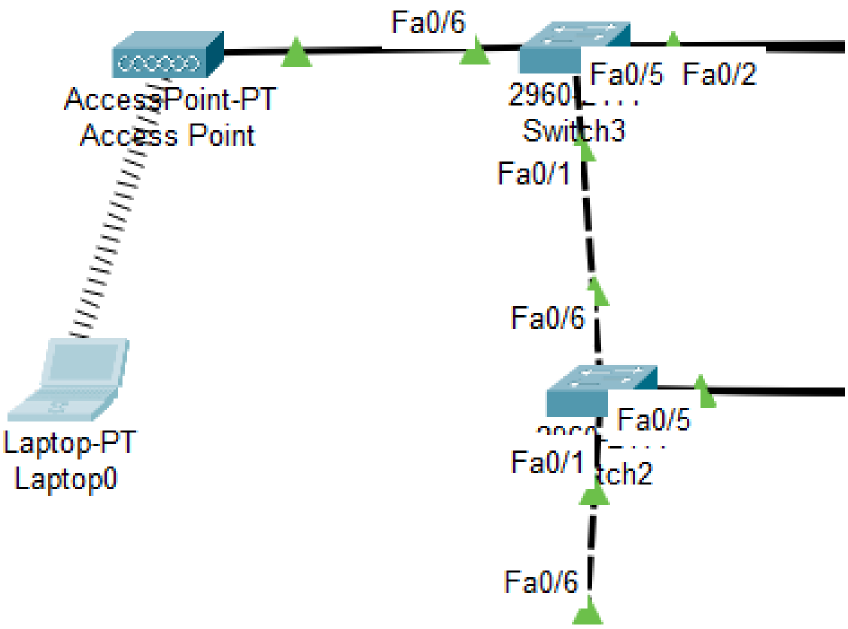
```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#service password-encryption
Router(config)#end
Router#
Router#write
```

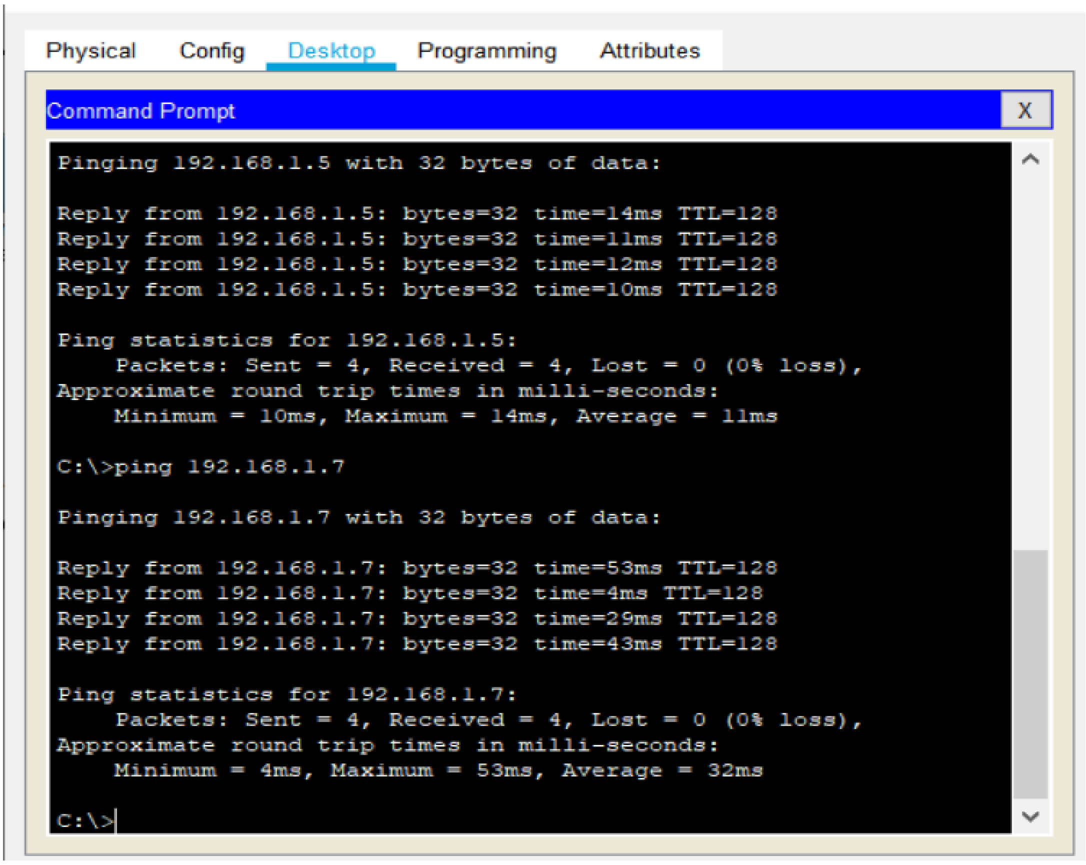
```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range fa0/7-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#end

Switch#write

Building configuration...

[OK]

Switch#
```



```
Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.40, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up


User Access Verification

Password:

Router>en
Password:
Router#
```

CONFIGURING ACCESS POINT AND WIRELESS CONNECTIVITY





```
Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=14ms TTL=128
Reply from 192.168.1.5: bytes=32 time=11ms TTL=128
Reply from 192.168.1.5: bytes=32 time=12ms TTL=128
Reply from 192.168.1.5: bytes=32 time=10ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 14ms, Average = 11ms

C:\>ping 192.168.1.7

Pinging 192.168.1.7 with 32 bytes of data:

Reply from 192.168.1.7: bytes=32 time=53ms TTL=128
Reply from 192.168.1.7: bytes=32 time=4ms TTL=128
Reply from 192.168.1.7: bytes=32 time=29ms TTL=128
Reply from 192.168.1.7: bytes=32 time=43ms TTL=128

Ping statistics for 192.168.1.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 53ms, Average = 32ms

C:\>
```

CONFIGURING IP POOL

It is done using the following code

For 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
```

For college router

```
Router#
```

1) Configure the default Routing towards ISP

```
Router(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

2) Configure the Access control-list 1) STANDARD ACL 1-99
2) EXTENDED ACL - SPECIFIC 100-199

```
Router#conf t
Router(config)#access-list 1 deny 192.168.2.3
Router(config)#access-list 1 deny 192.168.3.2
```

-------------etc

```
Router(config)#access-list 1 permit any
```

3) Implementation of ACL

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

4) Configuration of NAT

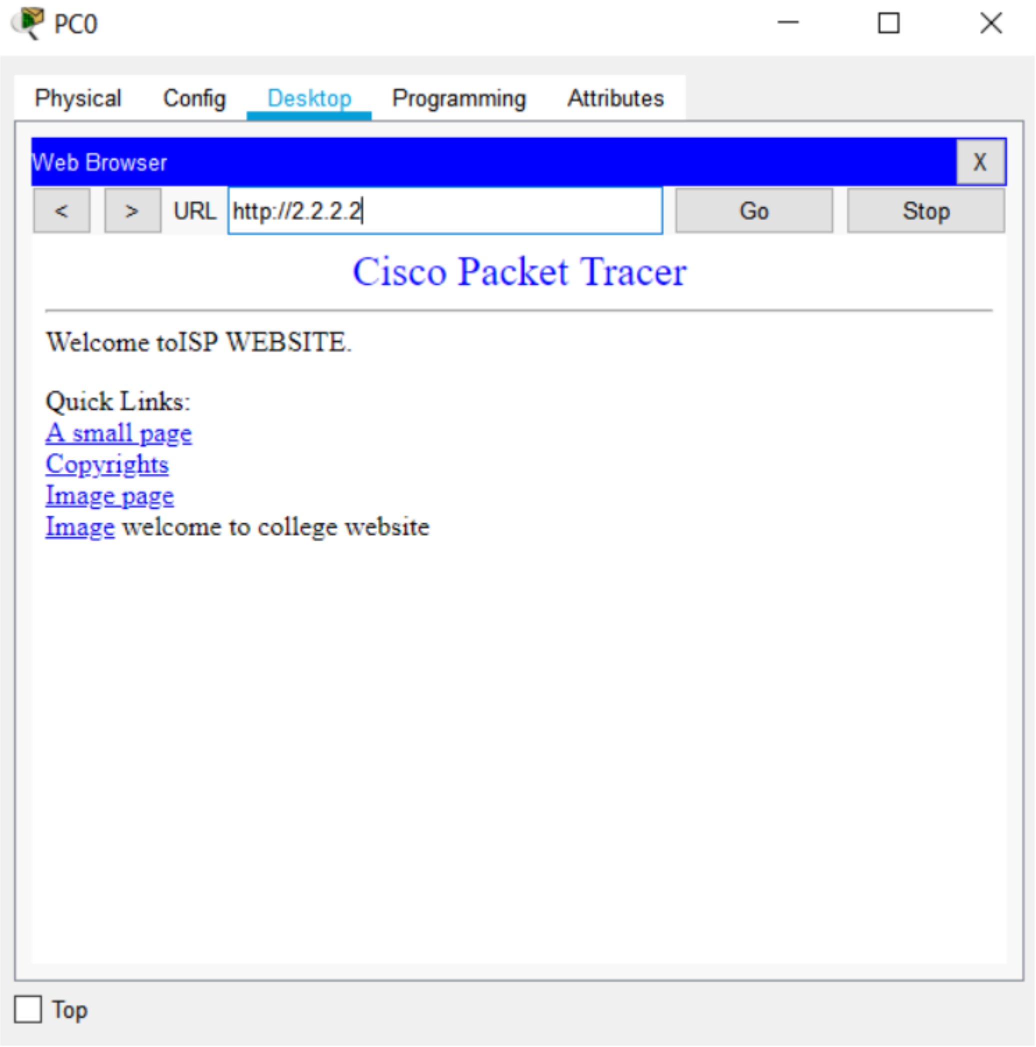
```
Router(config)#ip nat inside source static 192.168.1.100 117.117.117.3
Router(config)#ip nat pool RTTC 117.117.117.1 117.117.117.1 netmask 255.255.255.248

Router(config)#ip nat inside source list 1 pool RTTC overload
```

5) Implementation of NAT on LAN / WAN interfaces

```
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
```



http://2.2.2.2

Cisco Packet Tracer

Welcome toISP WEBSITE.

Quick Links:
A small page
Copyrights
Image page
Image welcome to college website

The output after the above code was implemented.

PROJECT THESIS

The project "CAMPUS AREA NETWORK USING VLAN" is all about to setup four different VLAN's and each VLAN consists of four PC's. There is a switch in each floor connecting to their interfaces respectively. In order to make VLAN's to communicate, we use router. Let us assume it as the COLLEGE ROUTER. Now we have taken a server and a router externally to verify the WIRED COMMUNICATION. Then we used an access point to make WIRELESS COMMUNICATION through laptop.

RESULT: After all the configurations, this setup is able to ping 2.2.2.2 and also able to browse the ISP website.

FUTURE SCOPE

Future work can be continued with refinement in the framework with inclusion on upcoming technologies like 802.11ac. More improved estimations for coverage area and placement of access points are possible with algorithms and simulation tools that can work for both indoor and outdoor simultaneously. Single integrated tool for performance measurement will definitely help network administrators to keep an eye on WLAN and delivery of content can be monitored.