One Day Skill Development Workshop for MAHE Support Staff

On

"Learning Network Configuration using Cisco Packet Tracer"

9th December 2019

MANIPAL SCHOOL OF INFORMATION SCIENCES,

LOWER GROUND 02, ACADEMIC BLOCK 05,
MANIPAL INSTITUTE OF TECHNOLOGY CAMPUS, MANIPAL – 576014. KARNATAKA.

0820 – 2925032 | office.sois@manipal.edu
www.manipal.edu/sois

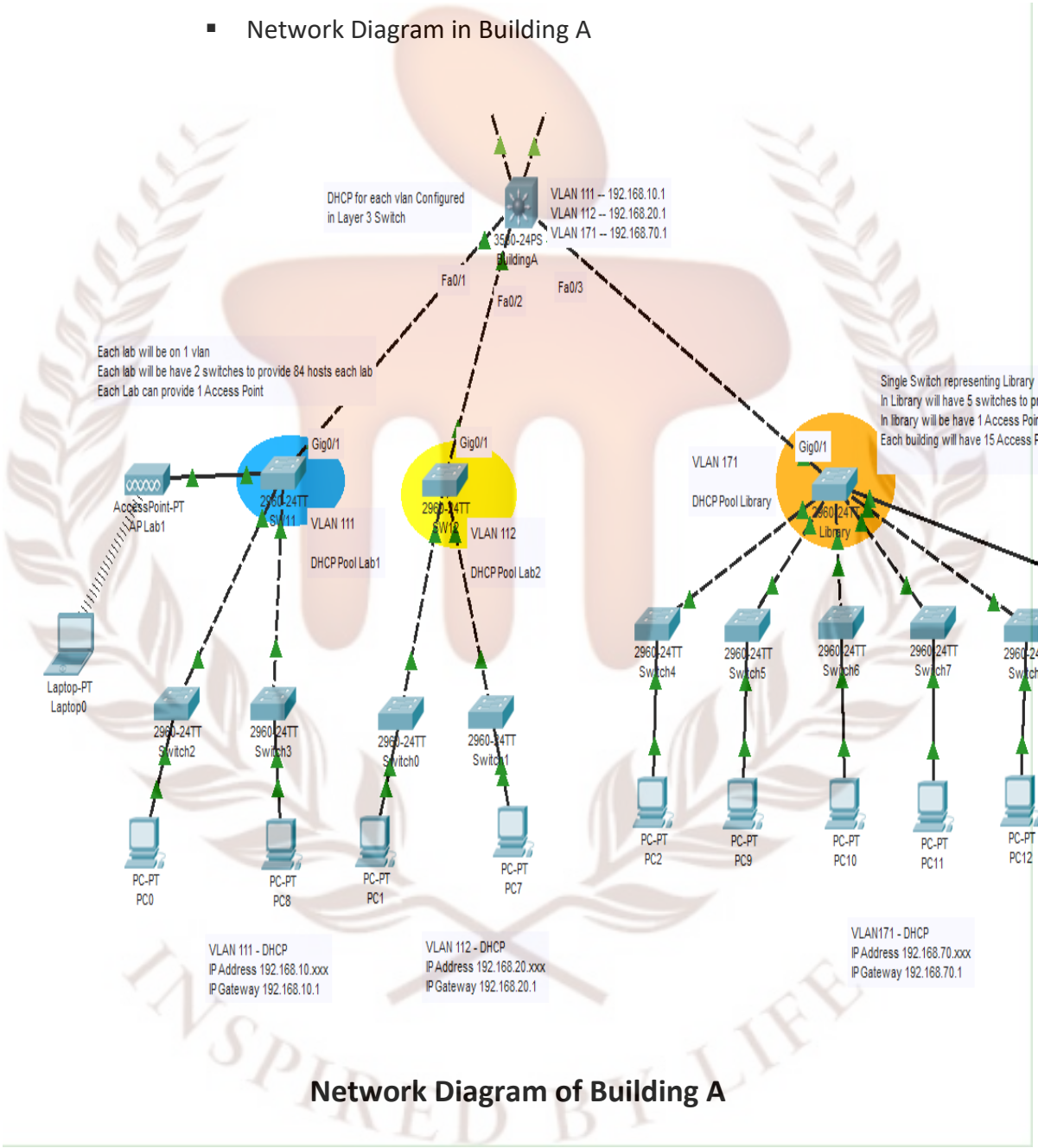
Computer Networks

- A computer network is a set of connected computers.
- Computers on a network are called nodes.
- The connection between computers can be done via cabling, most commonly the Ethernet cable, or wirelessly through radio waves.
- Connected computers can share resources, like access to the Internet, printers, file servers, and others.
- A network is a multipurpose connection, which allows a single computer to do more.

A typical university network scenario

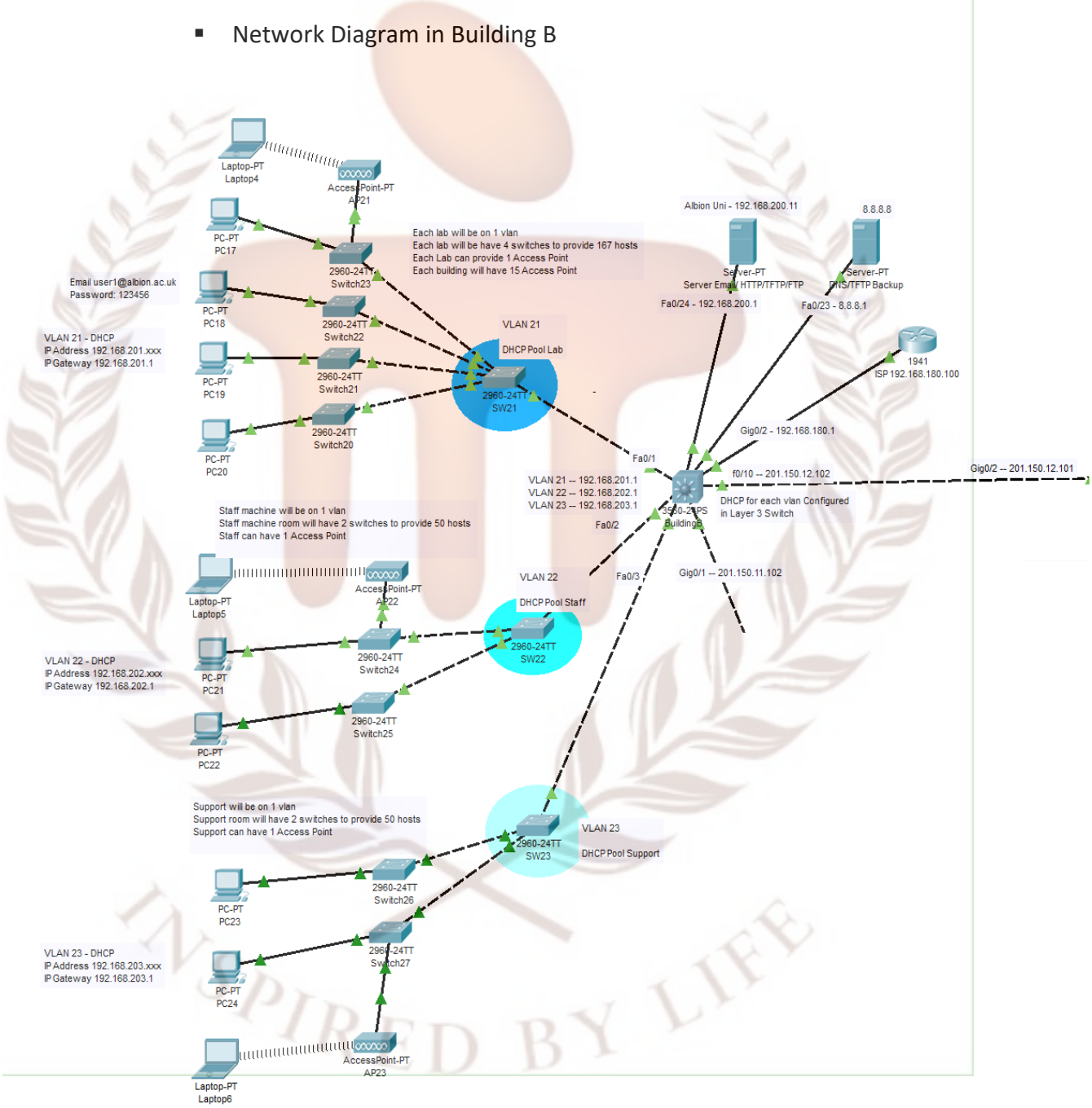
- Consider a university consisting of few institutions. Each institution will have few departments. The university would **like to upgrade** the network technology to provide better e-learning, web Services, email services, corporate information systems, voice, video communication, multimedia and other developments.
- The university campus has three buildings: Building A, B and C. The university server room, IT staff and university support staff offices are in Building B. The laboratories are in Building A and C.
- Assume that the **current network technology** is based on **10BaseT cabling** and **10Base-T Hubs**. Remote access into the university network is provided through an ADSL Internet link terminating in a building B.
- The university has about 20,000 students in **three facilities distributed over the campuses**; these are the faculties of Engineering/Computing, Health Sciences, Business, and Art/Design. Every member of staff in the University has a PC and a Laptop.
- **Requirements of new network technology:**
    1. Each student will be offered 2GB of storage. Total storage space required for 20,000 students is 40.96 TB
    2. Each staff member will be offered 5GB of storage. Total storage space required for 450 staff members is 2.304 TB.
    3. Wireless LAN access within all buildings.
    4. IP based video and voice communication.
    5. Remote access to university network.
    6. Provisions for backups, disaster recovery and redundancy.

- **Facility Requirements in Each Building:**
  - **Building A:**
    - Total number of workstations are 700.
    - 500 workstations in 6 separate laboratories with 84 workstations in each lab.
    - 200 workstations in the library.
    - Network Diagram in Building A



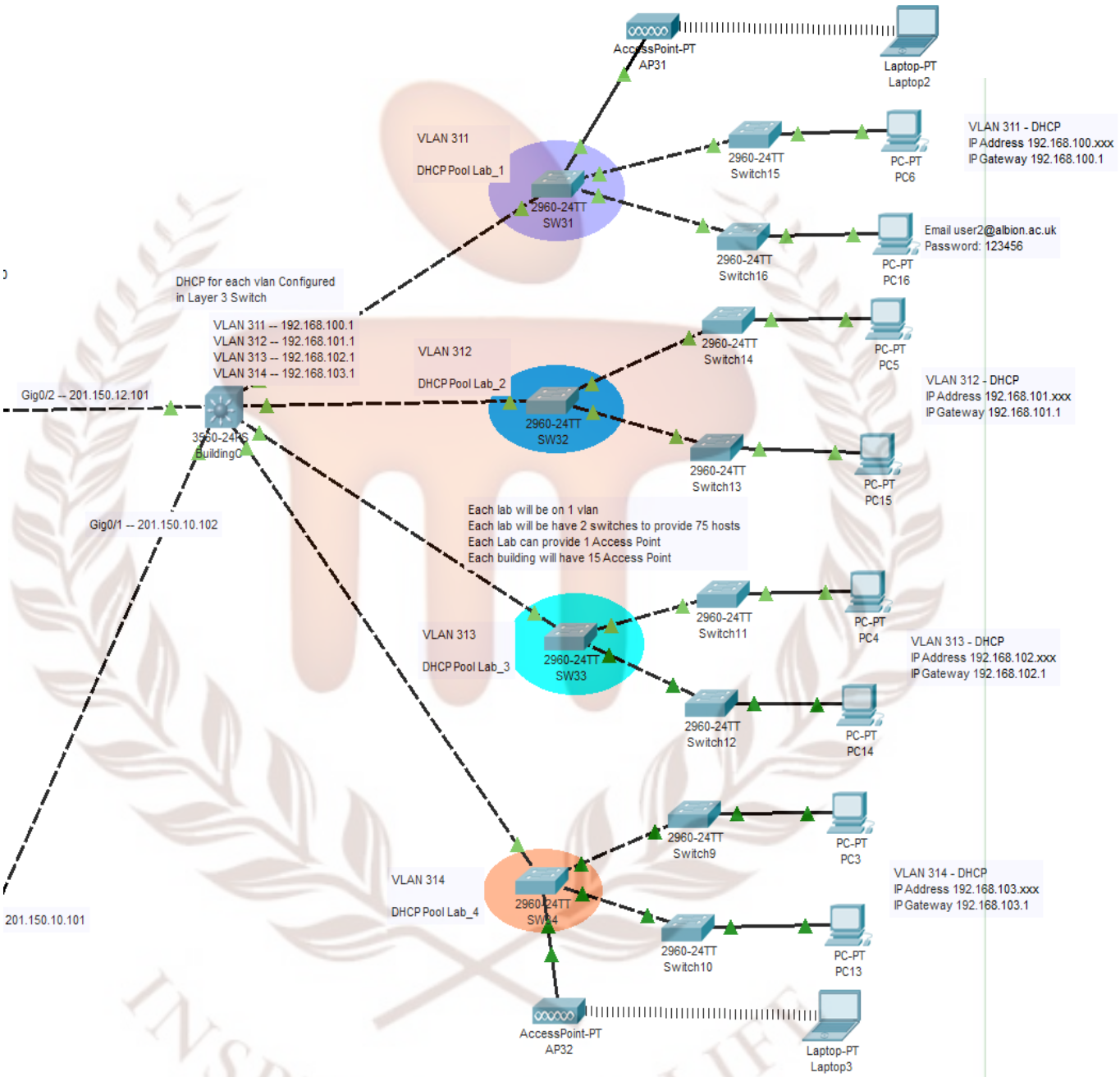
Network Diagram of Building A

- **Building B:**
  - Total number of workstations are 600.
  - 500 workstations in 3 labs. 167 workstations in each lab.
  - 50 workstations for IT staff machines.
  - 50 workstations for university support services staff.
  - Servers: DNS Server, HTTP server, SMTP server, FTP server, TFTP Server
  - Network Diagram in Building B



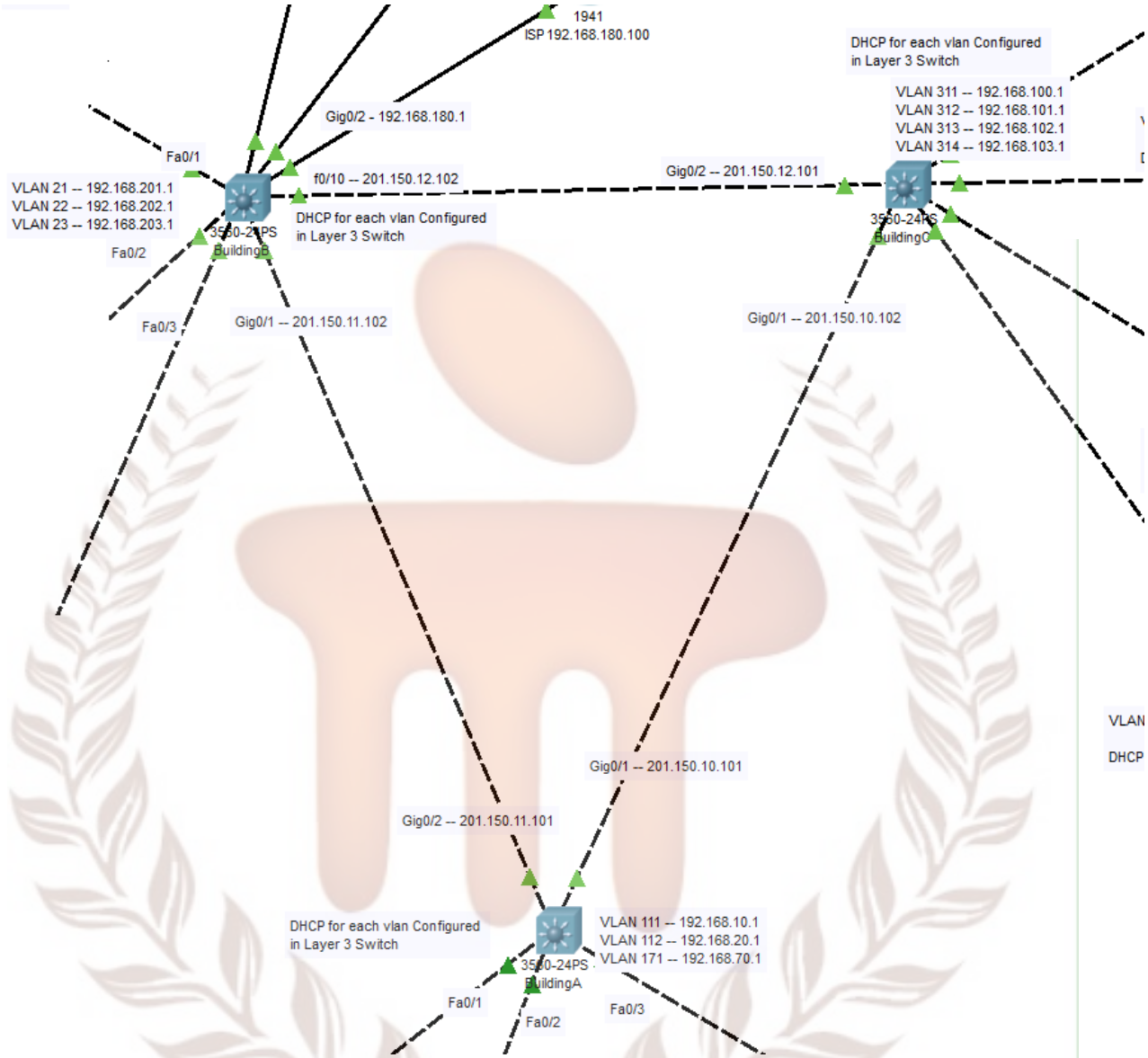
Network Diagram of Building B

- **Building C:**
  - Total number of workstations are 750
  - 750 workstations in 10 labs.



Network Diagram of Building C

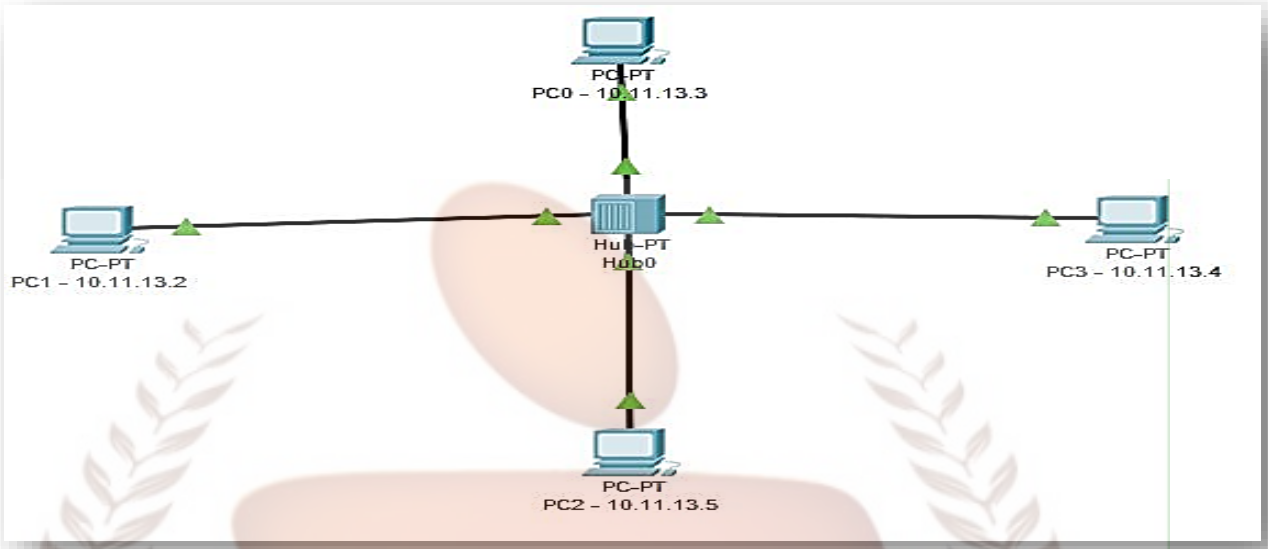
Network Topology between buildings



Reference:

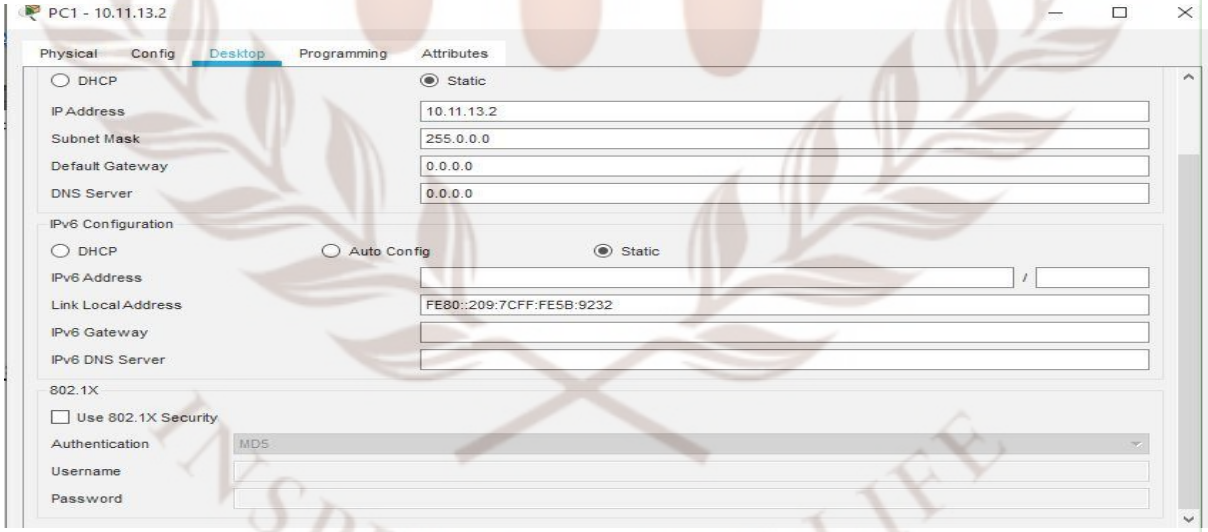
- **SEKTI WICAKSONO**, MSC COMPUTER SCIENCE, COCS71175 - IT INFRASTRUCTURE, Staffordshire University
- **GitHub:** https://github.com/sekti92/it_infrastructure

Scenario 1: Understanding the Configuration and Working of HUB



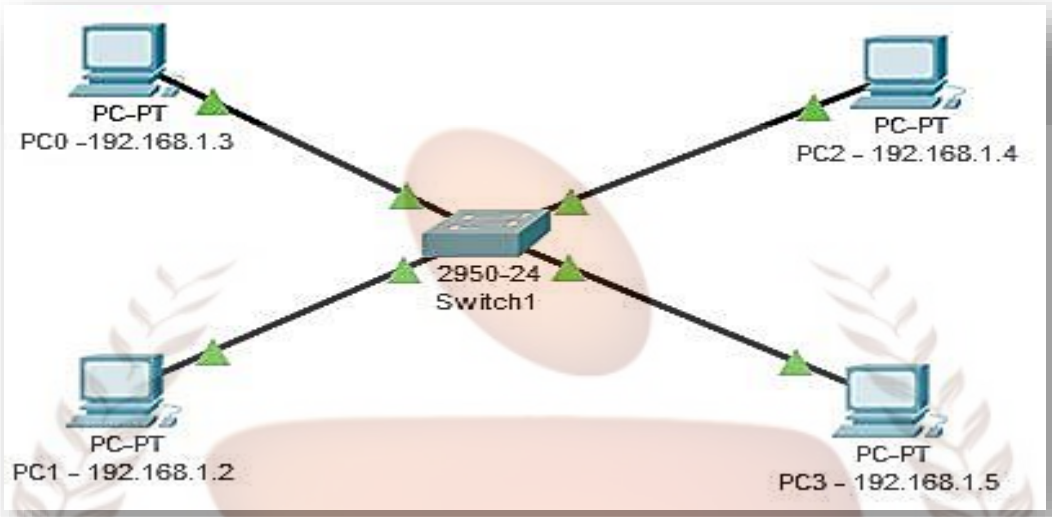
Assignment of IP Address:

- **PC1:**
  - Click on PC1 select IP Configuration, assign IP address as **10.11.13.2** and subnet mask as **255.0.0.0** as shown below



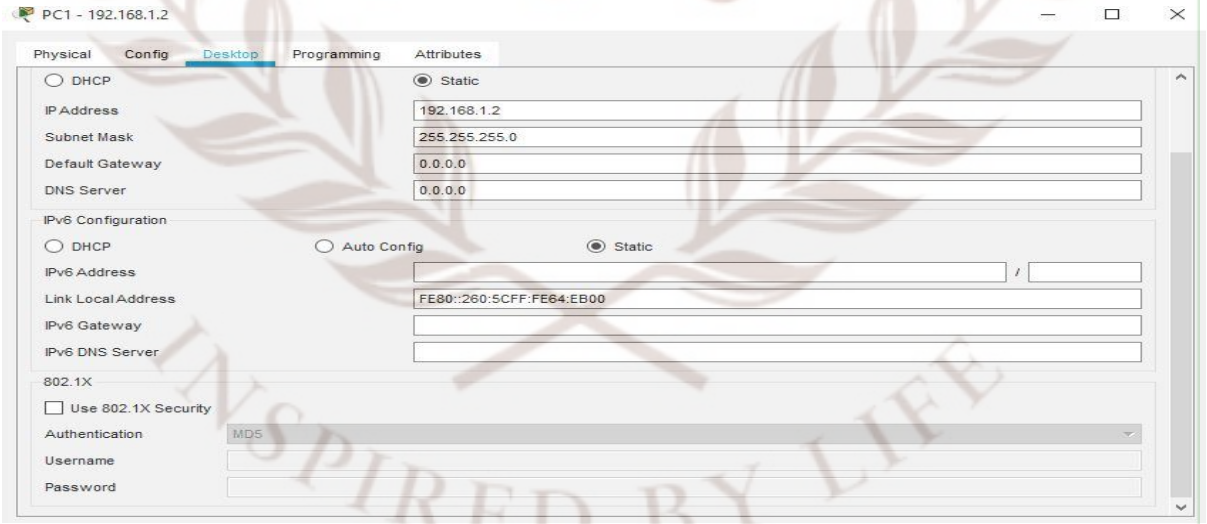
  - Repeat the for PC2, PC3, PC4 with IP's: **10.11.13.3, 10.11.13.4, 10.11.13.5** and subnet mask as **255.0.0.0**
  - Now press on Simulation Tab, send packet from PC1, to PC3.
  - Observe the movement of packet in the network topology using paly controls.

Scenario 2: Understanding the Configuration and Working of Bridge/Link Layer Switch in the Same Network



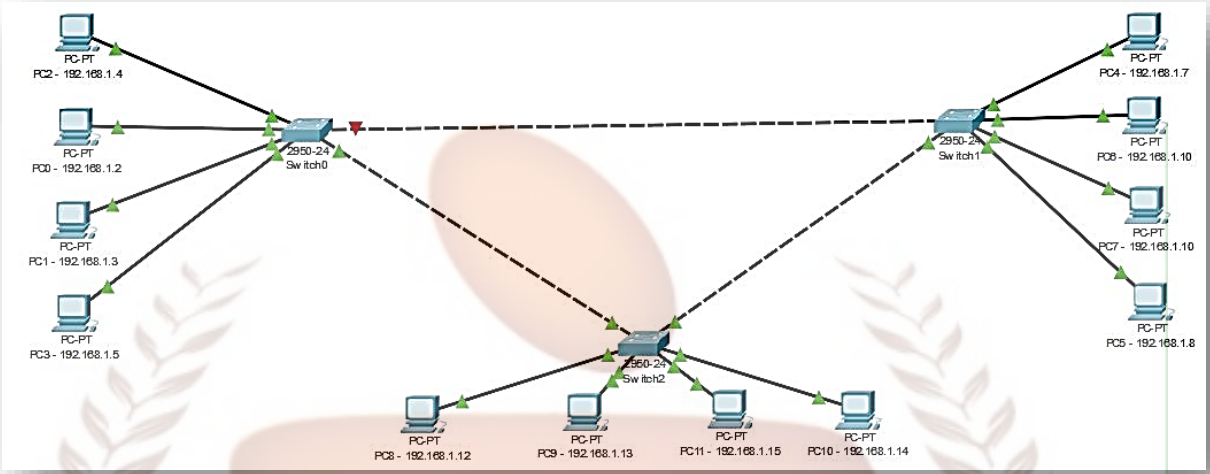
Assignment of IP Address:

- **PC1:**
  - Click on PC1 select IP Configuration, assign IP address as **192.168.1.2** and subnet mask as **255.255.255.0** as shown below



  - Repeat the for PC0, PC2, PC3 with IP's: **192.168.1.3, 192.168.1.4, 192.168.1.5** and subnet mask as **255.255.255.0**
  - Now press on Simulation Tab, send packet from PC1, to PC3.
  - Observe the movement of packet in the network topology using paly controls.

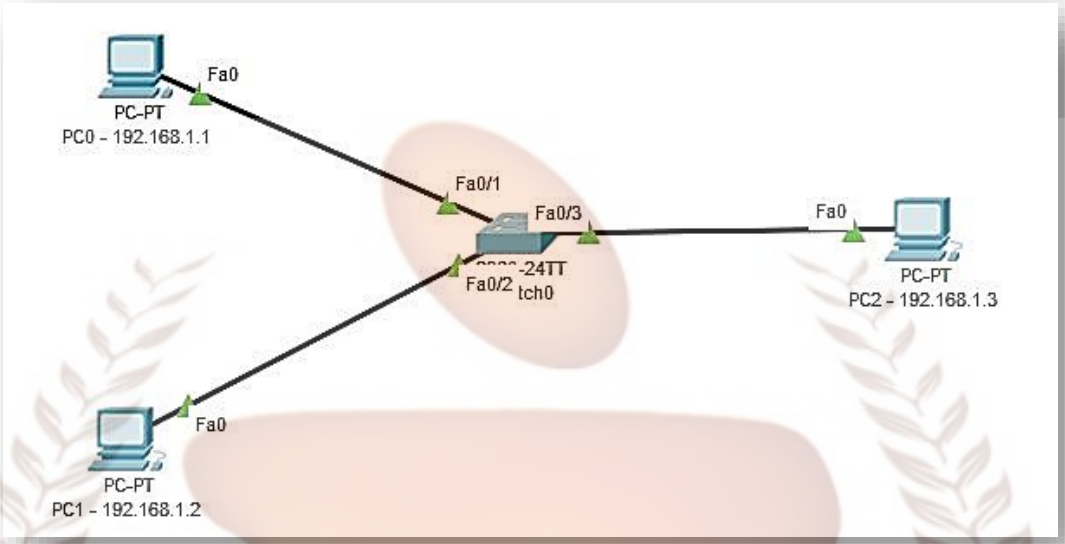
Scenario 3: Understanding the Configuration and Working of Bridge/Link Layer Switch connecting multiple Network (Across many LAB)



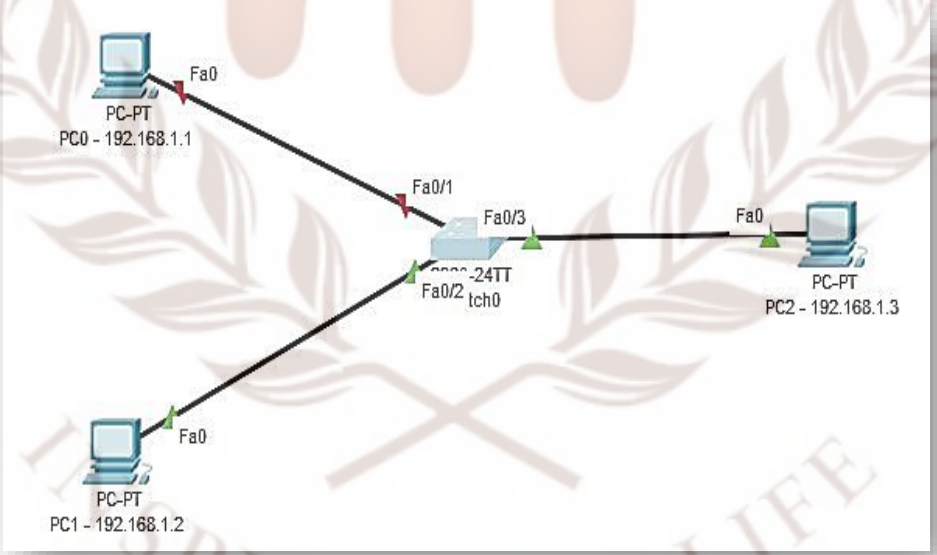
- Assign IP Address and Subnet Mask as shown in the figure.
- Send Simple PDU within the Network and Across the Network.

Scenario 4: To illustrate how to enable and disable ports on link layer switch

- Create a topology as shown in figure below

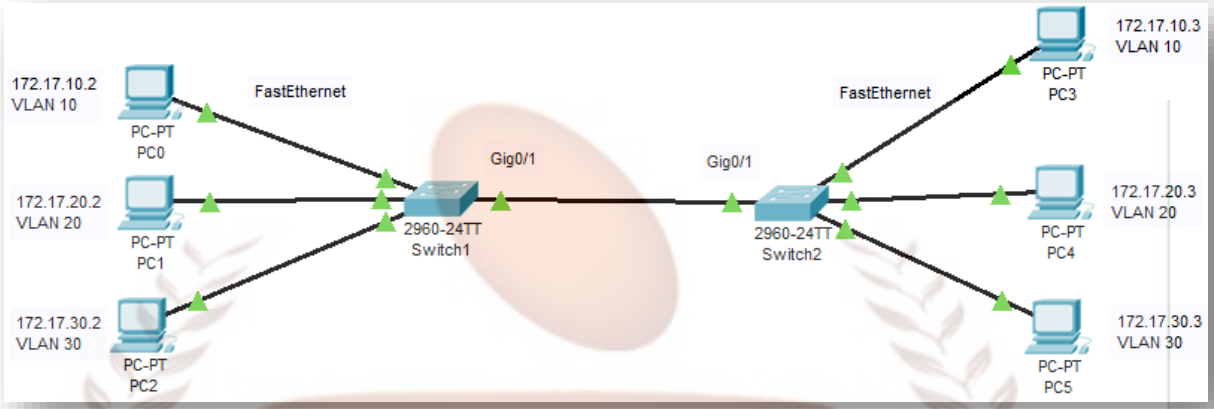


- Assign IP to PC as shown in the figure above
- Send simple PDU packet between PC's and transmission will be successful.
- Now go to switch config tab uncheck the port status on Interface FastEthernet0/1



- Now, Send simple PDU packet between PC0 and PC1 the transmission will not be successful.

Scenario 5: A physical network having two LAN where each of them having three computers. The Two LANs are interconnected by a switch. We need to configure three VLANs having a computer from each physical LAN.



VLAN Switch Configuration

- Assign IP address to the PC as shown in the Topology Diagram

Note:

- Try to send simple packet between two machines within switch and across the switch.
- Before configuring VLAN type on each switch go to CLI and type ***show vlan*** see the default port configuration

On switch 1:

- **we are creating three VLAN 10, 20, 30 and assigning then a name.**

en
conf t

Entering Switch configuration Mode

```
vlan 10
name imageinglab
exit

vlan 20
name datasciencelab
exit

vlan 30
name iotcloudlab
exit
exit

show vlan
```

- **we are assigning interfaces of switch1 to created VLAN 10, 20, 30.**

```
conf t
interface f0/1
switchport access vlan 10
exit

interface f0/2
switchport access vlan 20
exit

interface f0/3
switchport access vlan 30
exit
exit
```

Note: After configuring VLAN type ***show vlan*** see the assigned port configuration

On switch 2:

Note: before configuring VLAN type ***show vlan*** see the default port configuration

- **we are creating three VLAN 10, 20, 30 and assigning then a name.**

```
en
conf t
vlan 10
name imageinglab
exit

vlan 20
name datasciencelab
exit

vlan 30
name iotcloudlab
exit
exit

show vlan
```

- **we are assigning interfaces of switch1 to created VLAN 10, 20, 30.**

```
conf t
interface f0/1
switchport access vlan 10
exit

interface f0/2
```

```
switchport access vlan 20
exit

interface f0/3
switchport access vlan 30
exit
exit
```

Note: After configuring VLAN type ***show vlan*** see the assigned port configuration

Below steps are performed for trunking purpose:

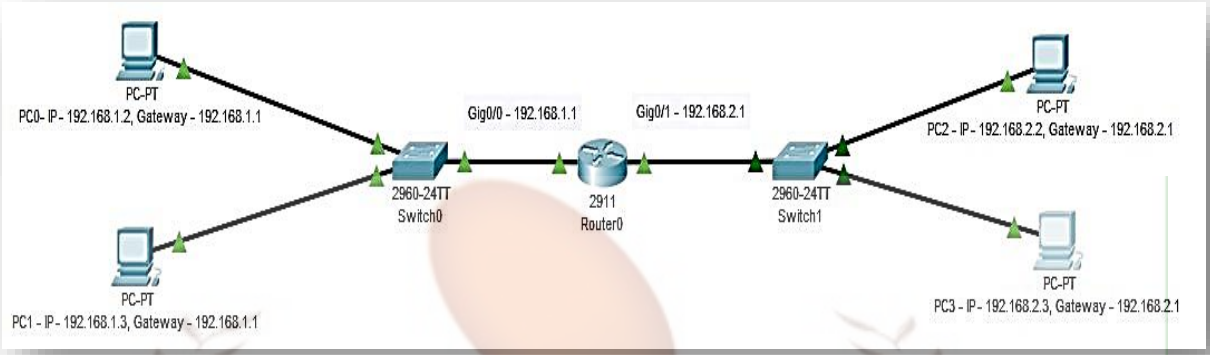
- **On switch 1:**

```
en
conf t
interface g0/1
switchport mode trunk
switchport trunk allowed vlan 1-99
end

show interface ?
 you should See trun in the list

show interface trunk

show vlan
```

- **On switch 2:**

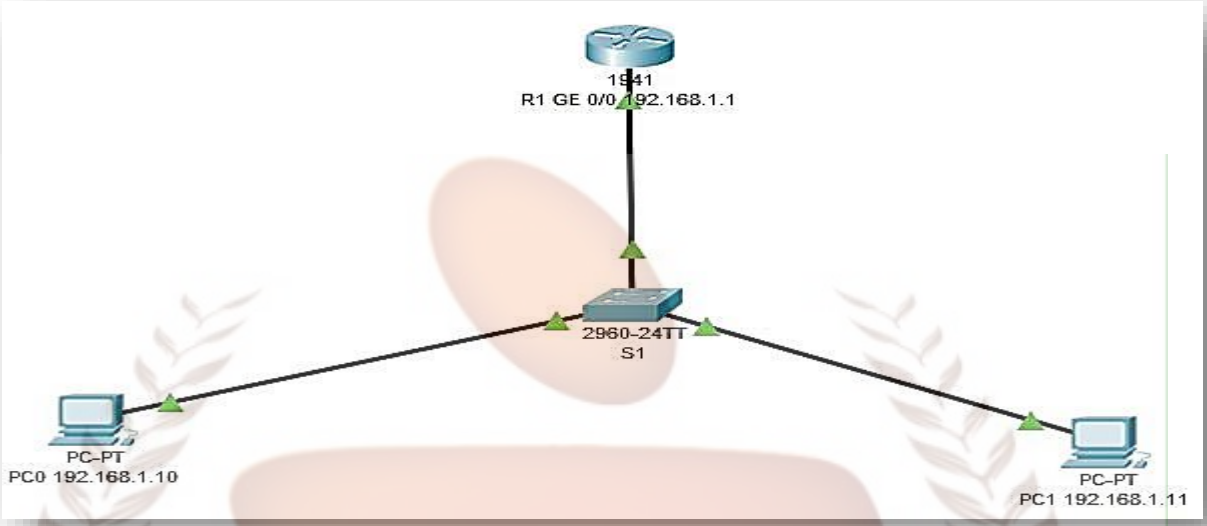
```
en
conf t
interface g0/1
switchport mode trunk
switchport trunk allowed vlan 1-99
end

show interface ?
show interface trunk
show vlan
```

Scenario 6: Need of router, communication between two networks



- Create the topology, assign the IP's and default gateway to device as show in the figure above.
- Try to send simple PDU packets with in the network and across the network.

Scenario 7: A network having two PC's, a switch and a router. We will enable SSH protocol on router and switch such that PC can access them remotely.



- Assign the IP's to device as shown in the figure above
- **Configuring Router**:

```
en
conf t
hostname r1
enable secret class
line console 0
password msois
login
exit

interface gigabitEthernet 0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
show running-config
```

- **Configuring Switch**:

```
en
conf t
hostname s1
enable secret class
line console 0
password msois
login
exit

interface vlan 1
ip address 192.168.1.2 255.255.255.0
no shutdown
exit
```

```
ip default-gateway 192.168.1.1
exit
show running-config
```

- **Configuring PC 0**:

```
ip address: 192.168.1.10
gateway: 192.168.1.1
```

- **Configuring PC 1**:

```
ip address: 192.168.1.11
gateway: 192.168.1.1
```

- **Configuring SSH on Switch for key Generation**:

```
Go to cli
Password: msois
en
PW: class
conf t
ip domain-name msois.com
crypto key generate rsa
Size: 1024
```

- **Configuring SSH on Router for key Generation**:

```
Go to cli
Password: sois@123
En
PW: class
Conf t
ip domain-name msois.com
crypto key generate rsa
Size: 1024
```

- **Configuring SSH on Switch for adding User and only giving ssh to access**:

```
User
username admin secret msois
line vty 0 15
login local
transport input ssh
```

- **Configuring SSH on router for adding User and only giving ssh to access**:

```
user
username admin secret msois
line vty 0 15
login local
transport input ssh
###copy running-config stratup-config
```

- **On PC1 Command prompt:**

  telnet 192.168.1.1 (you will get connect closed by foreign host)

- **Getting access to router from command line:**

  ssh -l admin 192.168.1.1
  password: msois

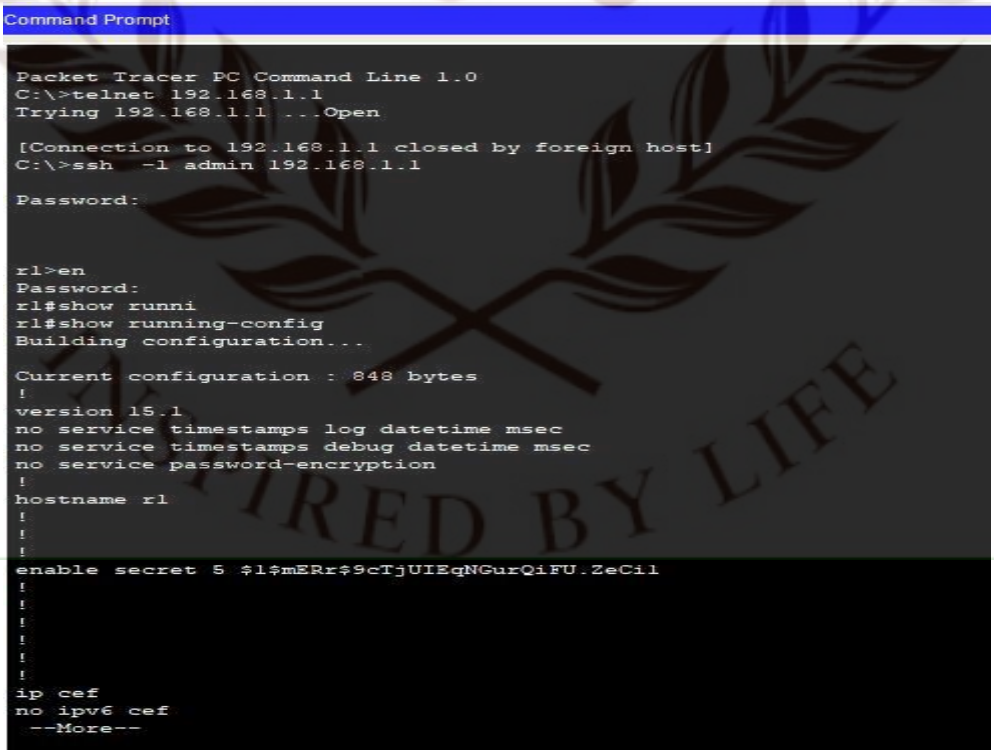
  After this you will be SSHed to router (prompt change)
  r1>
  r1> en
  password class
  r1# show running-config

- **Getting access to switch from command line:**

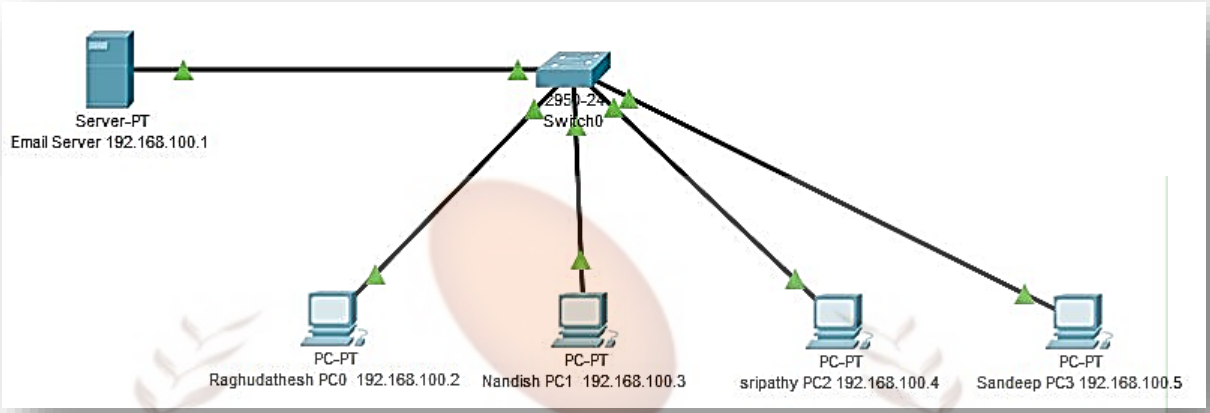
  ssh -l admin 192.168.1.2
  password: msois

- After this you will be SSHed to router (prompt change)

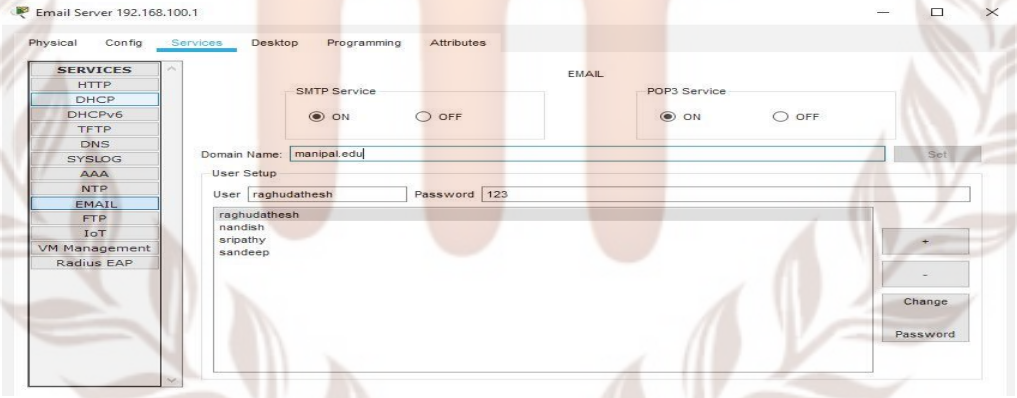
  s1>
  s1> en
  password class
  s1# show running-config



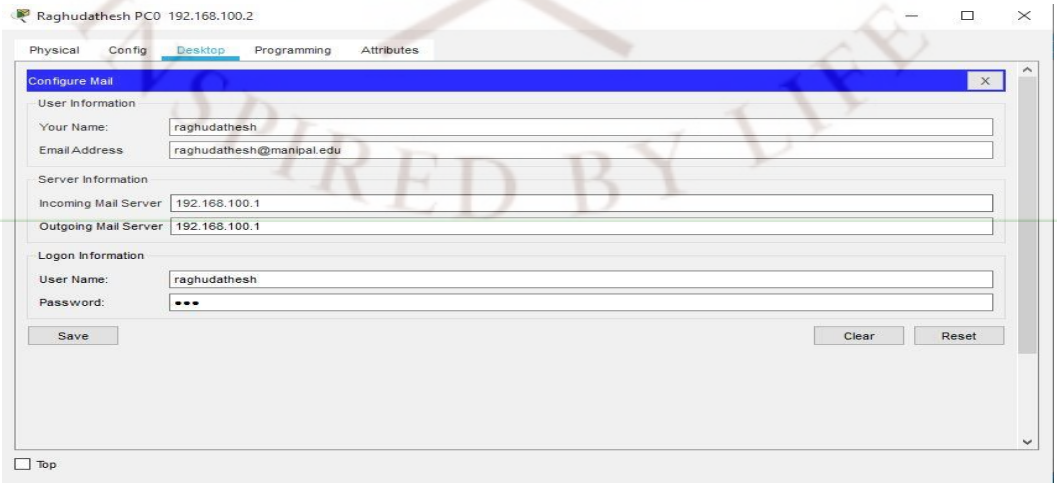
Scenario 8: Creation of E-mail ID's with specific domain names and usage of E-mail services



- Create the topology, assign the IP and subnet to devices as show in the figure above.
- On Email server go to services tab → select email service
- In email service tab create 4 email with domain names as shown in figure below

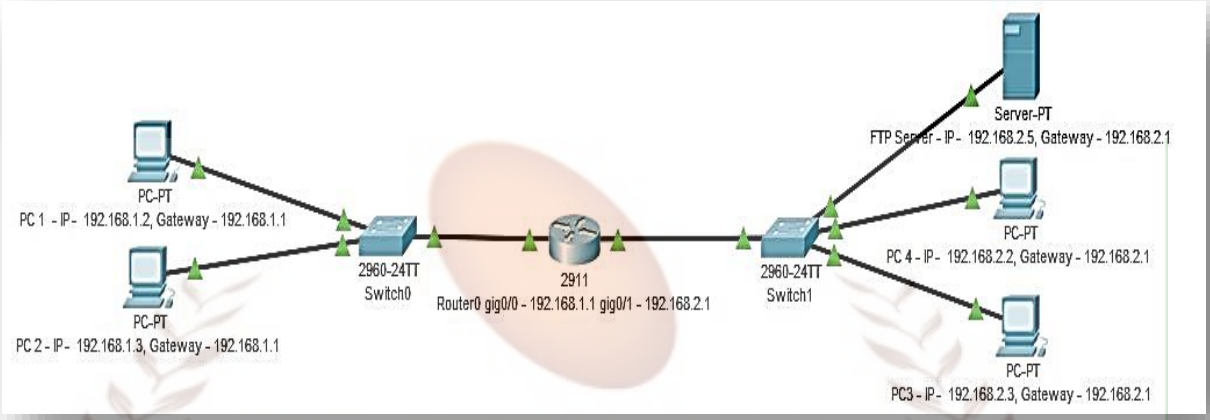


- On PC0 in desktop select email API ➔ Configure email application ➔ Enter the information as shown in figure below



- Perform the above step for all other PC's
- Compose a mail to any of the user on the other PC's using email application and send the email.
- On the destination PC select email API, you can read the email and replay to the email.

Scenario 9: Imagine a situation where you need to share a file across various departments and networks using FTP Service.



On PC 1, 2, 4, 3:

- Assign IP address as 192.168.1.2, 192.168.1.3, 192.168.2.2, 192.168.2.3.
- For PC 1 and 2 assign gateway as 192.168.1.1.
- For PC 3 and 4 assign gateway as 192.168.2.1.

On Router:

- Set the gigabit ethernet interface as
- Gig0/0: 192.168.1.1
- Gig0/1: 192.168.2.1

Add a Server:

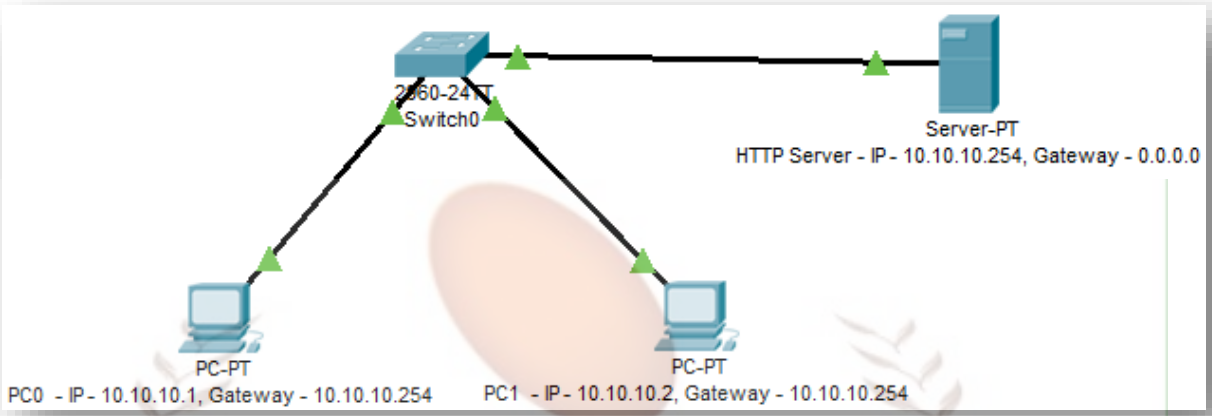
- Assign IP address as 192.168.2.5 and gateway as 192.168.2.1
- Go to services and enable ftp service as on.
- Assign Username: **msois** and password: **sois@123**
- **Select all permission**: read, wright, delete, list.

Step to use FTP Services:

- **Go to PC 3** and open text editor add the content and save the file as msois-ftp.txt.
- Open command prompt:
  - Connect to FTP server using following command: ftp 192.168.2.5
  - enter username: "**msois**" and password: "**sois@123**"
  - To upload the file to FTP Server use the following command:
  - dir (it list the file in the ftp server)
  - To upload file from PC3 to Server: **put msois-ftp.txt**
  - dir (msois-ftp.txt should be reflected)

- **Go to PC 1** and download the uploaded file from FTP Server:
- Open command prompt:
  - Connect to FTP server using following command: ftp 192.168.2.5
  - Enter username: "***msois***" and password: "***sois@123***"
  - To download the file to FTP Server use the following command:
  - dir (it list the file in the ftp server)
  - To download file from Server to PC1: ***get msois-ftp.txt***
  - dir (msois-ftp.txt should be reflected)

Scenario 10: Creation and usage of webservice services

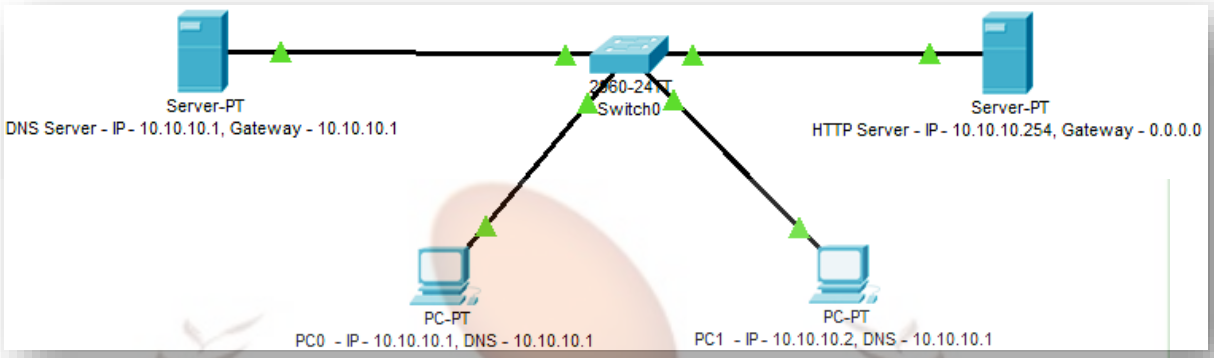


- Create the topology, assign the IP, subnet and gateway to devices as show in the figure above.
- On HTTP server go to services tab → select HTTP service → enable HTTP protocol
- Click on new file and copy the HTML code below:

```
<div class="bgimg">
<div class="topleft">
<p>MAHE, Manipal</p>
</div>
<div class="middle">
<h1>Welcome to Networking Workshop</h1>
<hr>
<p>09 December 2019</p>
</div>
<div class="bottomleft">
<p>Greetings From MSOIS</p>
</div>
</div>
```

- save it as "***index.html***"
- From PC0 or 1 → Desktop → web browser → access website on HTTP service put entering 10.10.10.254→ you will be presented with a web page.

Scenario 11: Creation and usage of webservice services

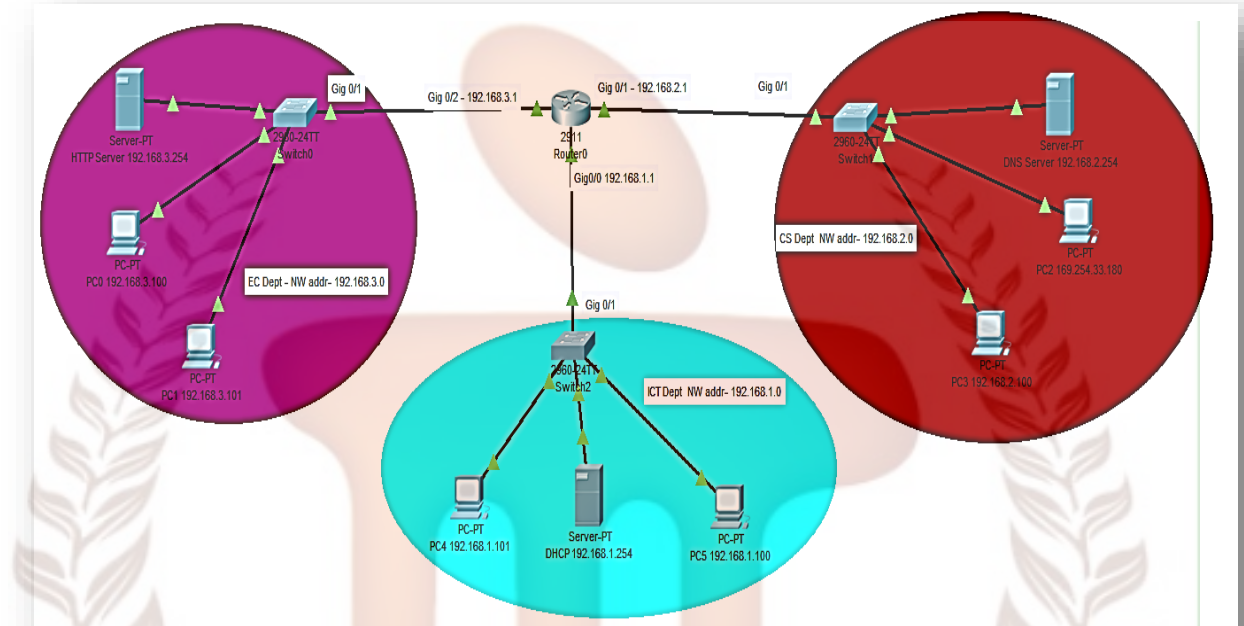


- Create the topology, assign the IP, subnet and gateway to devices as show in the figure above.
- On HTTP server go to services tab → select HTTP service → enable HTTP protocol
- Click on new file and copy the HTML code below:

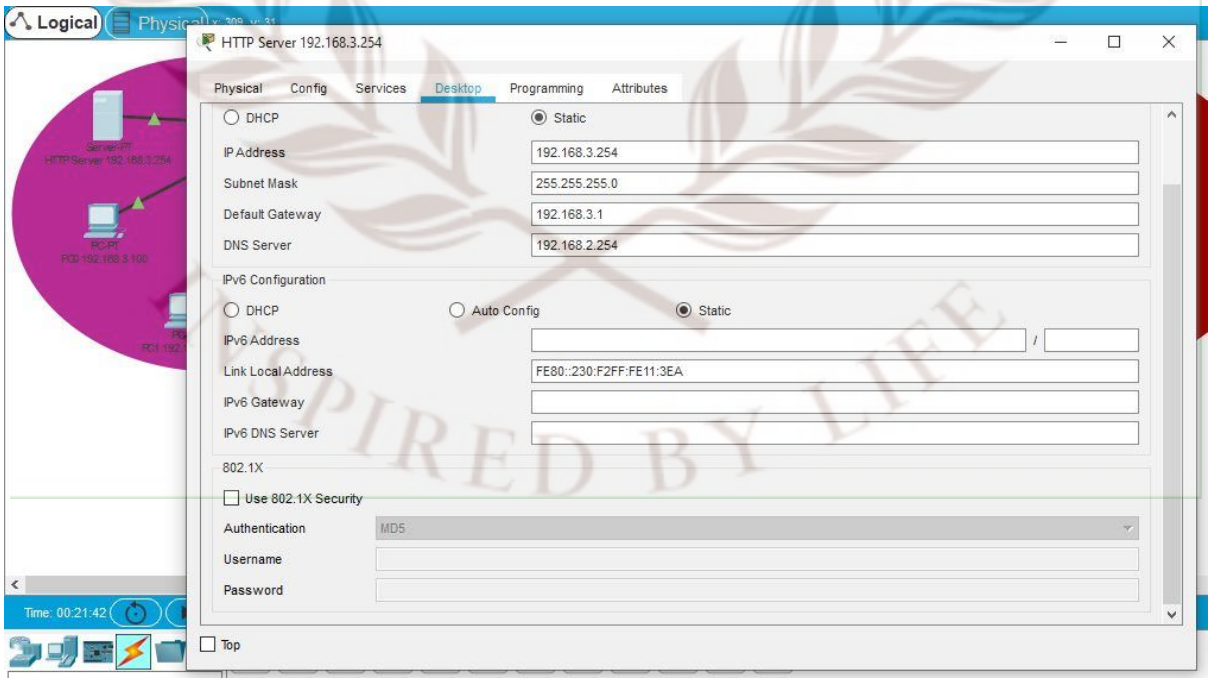
```
<div class="bgimg">
<div class="topleft">
<p>MAHE, Manipal</p>
</div>
<div class="middle">
<h1>Welcome to Networking Workshop</h1>
<hr>
<p>09 December 2019</p>
</div>
<div class="bottomleft">
<p>Greetings From MSOIS</p>
</div>
</div>
```

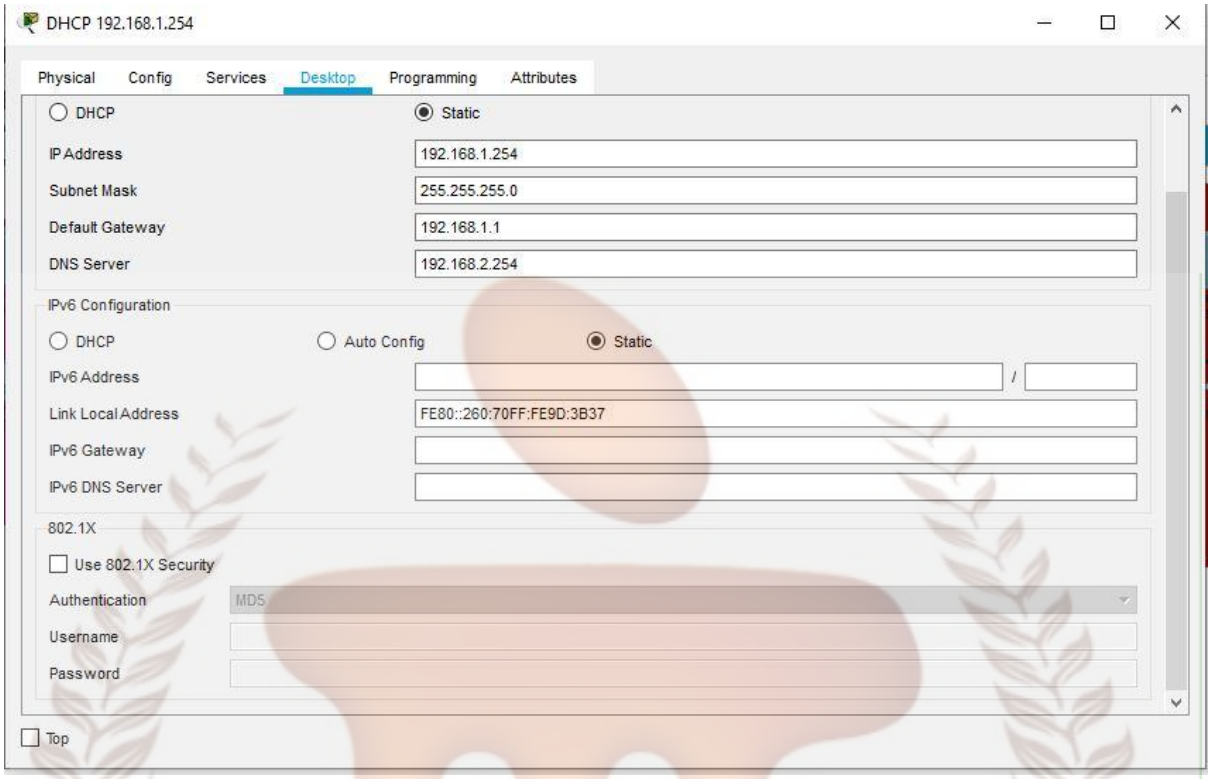
- save it as "***index.html***"
- On DNS server go to services tab → select DNS service → enable DNS service
- Name = msois.com, address = 10.10.10.254 and click save.
- From PC0 or 1 → Desktop → web browser → access website by entering url as ***msois.com*** → you will be presented with a web page.

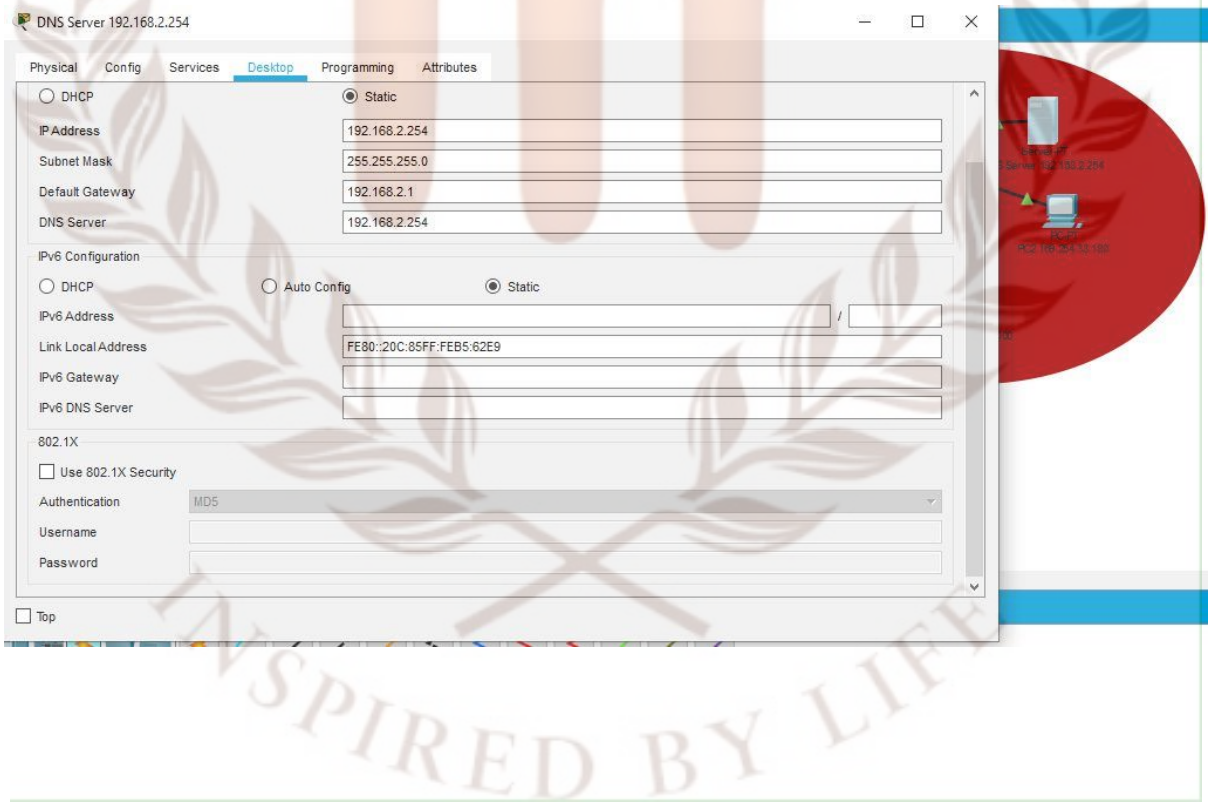
Scenario 12: A collage comprises of three branches (EC, CS, ICT) having their own local Area Network connected by a router. EC Department having a Web Server hosting the college website, CS Department is having a DNS Server used to resolve the URL to IP address and ICT Department is having a DHCP Server perform automatic IP address assignment from the configured pool of IP address.



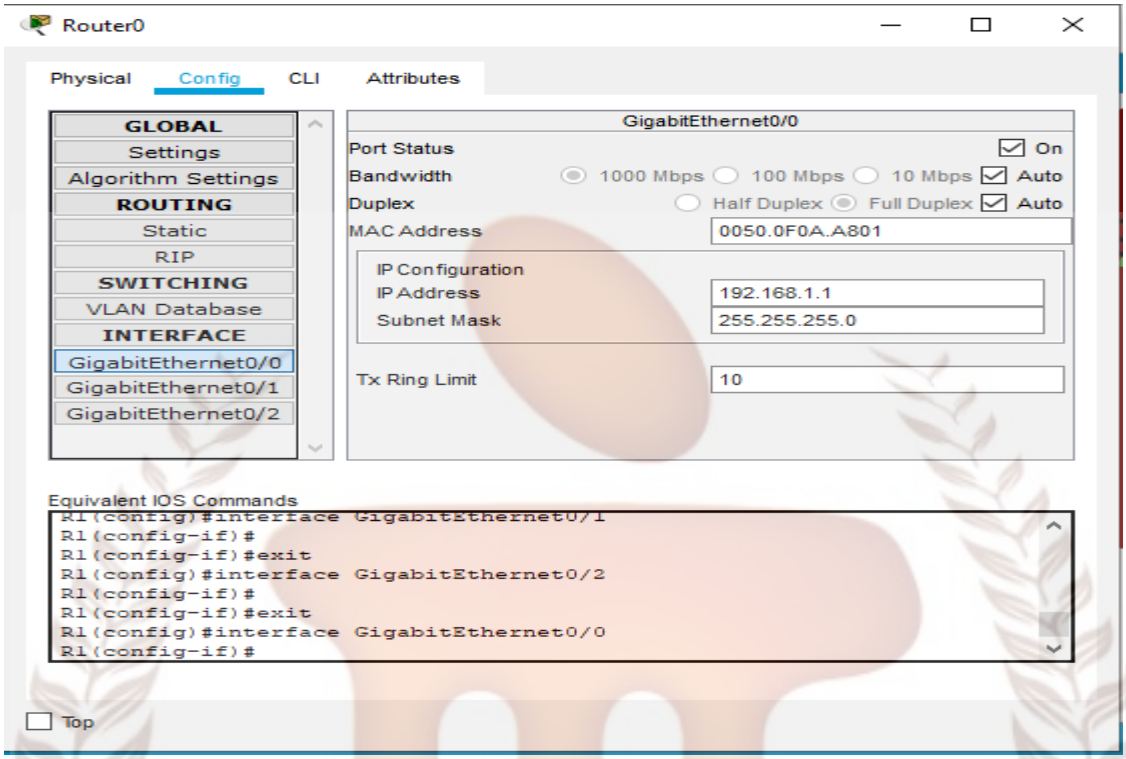
- Note: Allocate the specified IP addresses to DHCP, DNS, Web serves as shown in the diagram below



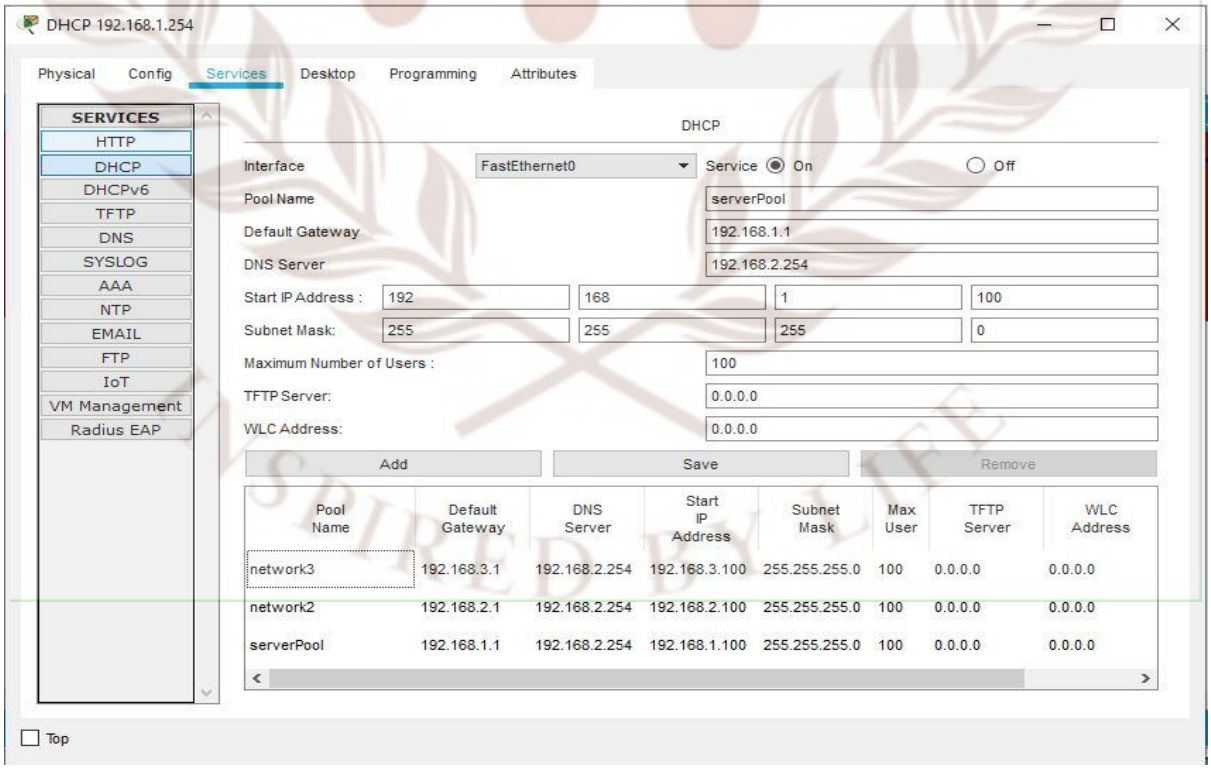

DHCP 192.168.1.254
Physical
Config
Services
Desktop
Programming
Attributes
DHCP
Static
IP Address
192.168.1.254
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
192.168.2.254
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::260:70FF:FE9D:3B37
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


DNS Server 192.168.2.254
Physical
Config
Services
Desktop
Programming
Attributes
DHCP
Static
IP Address
192.168.2.254
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
192.168.2.254
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::20C:85FF:FEB5:62E9
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

- Do the following configuration on router.



- Enabling DHCP Service on DHCP server to allocate IP address to systems on different network for an organization

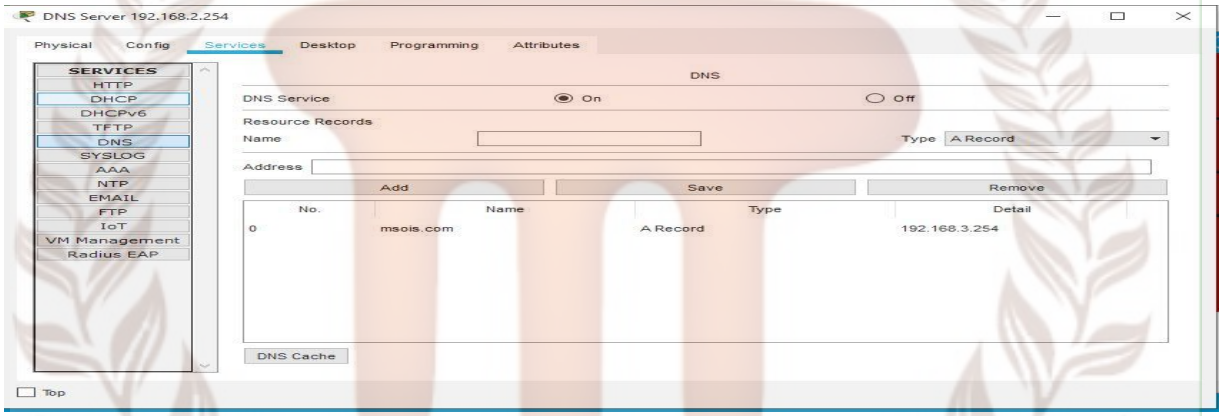


Go to Router CLI and do the Following:

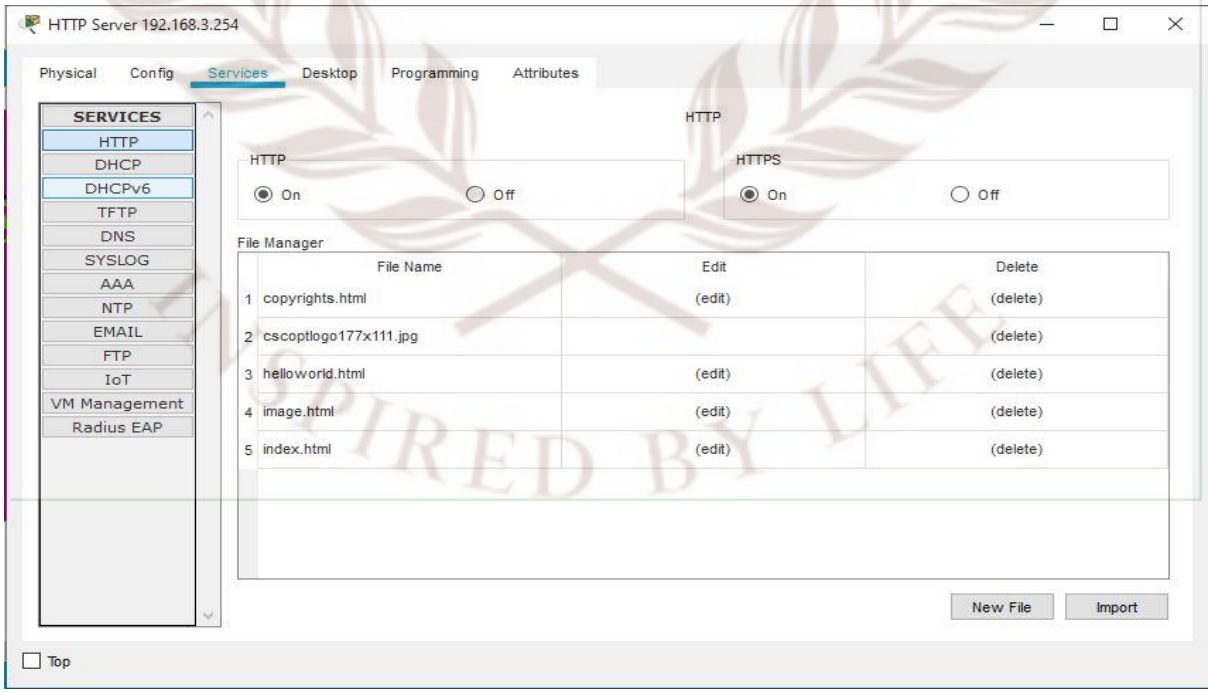
- Router DHCP port forwarding (helper)

```
en
conf t
interface gigabitEthernet 0/1
ip helper-address 192.168.1.254
exit

interface gigabitEthernet 0/2
ip helper-address 192.168.1.254
exit
```

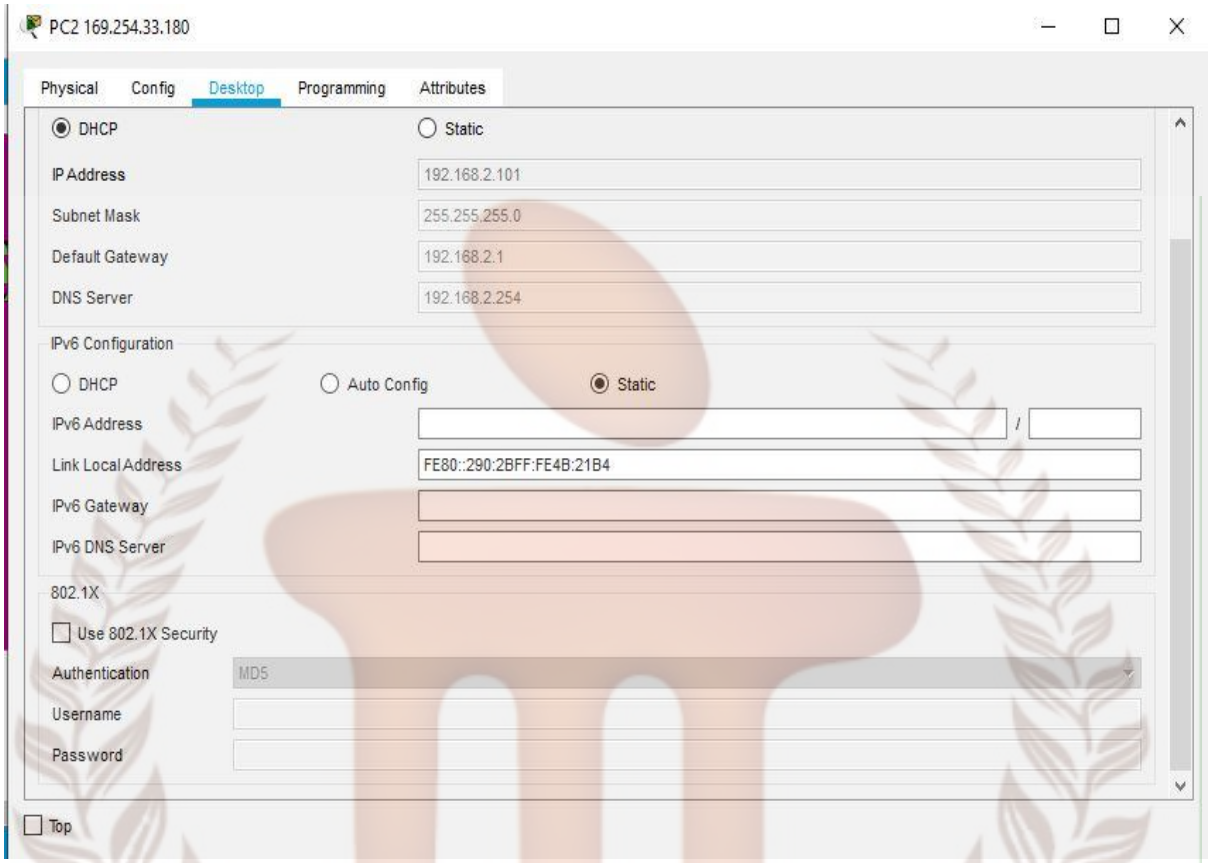
Enabling DNS Service on DNS server to resolve the domain name of web/HTTP server.



Enabling HTTP/HTTPS Service on Web server to deliver web pages to end user

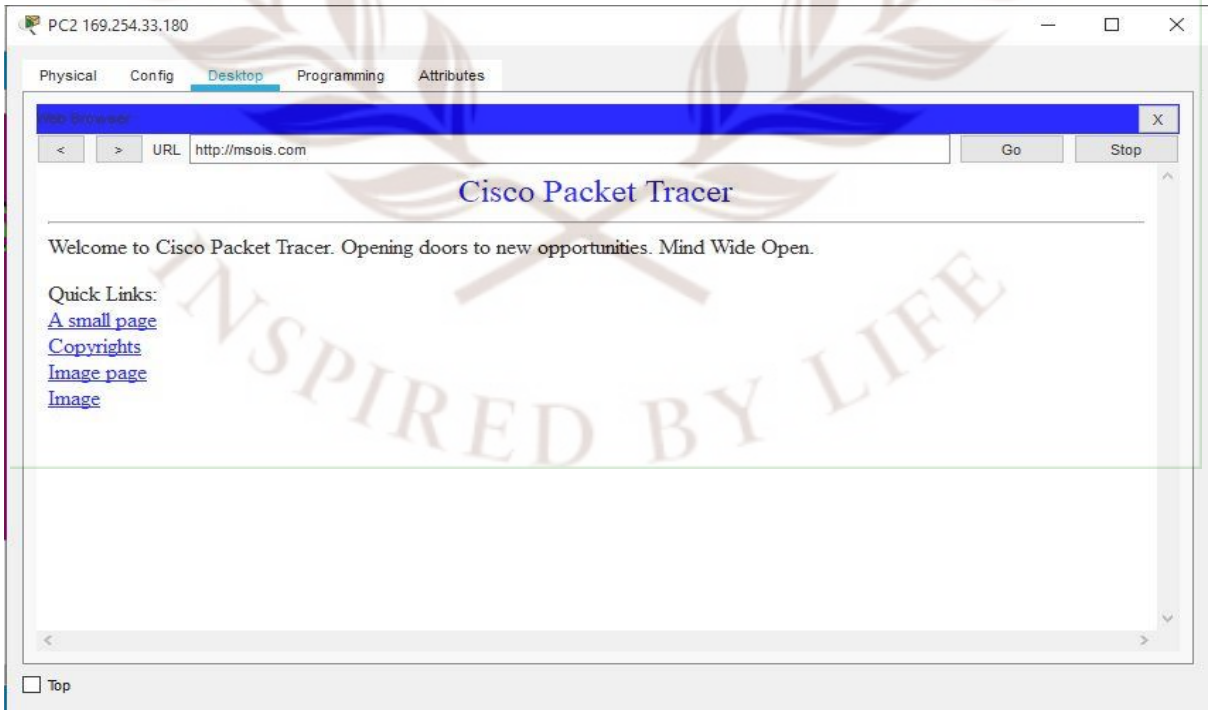


To illustrate working of DHCP server do the following on any PC:

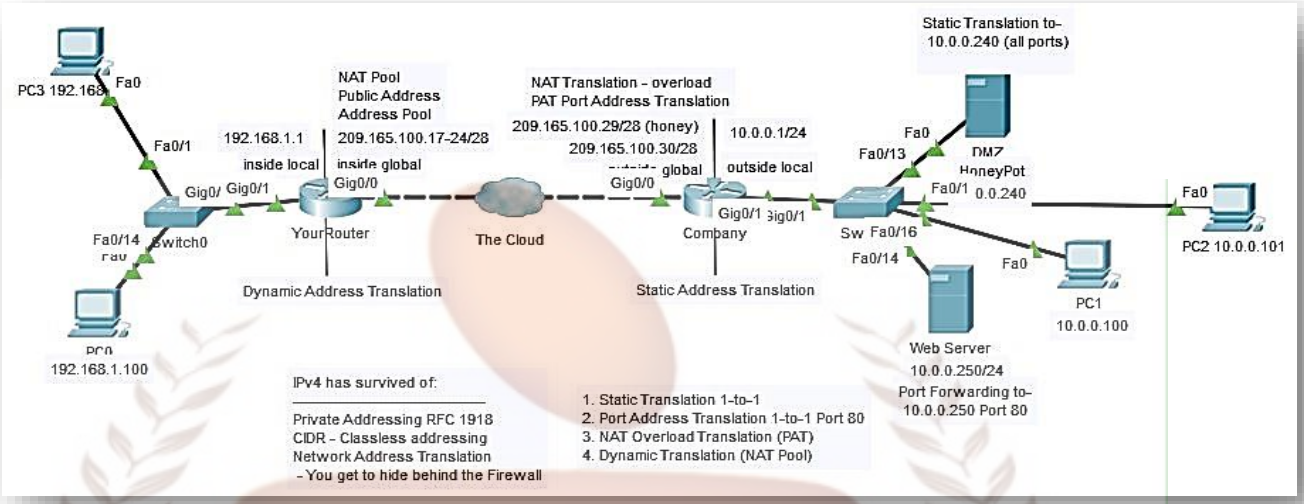


Now IP should be allocated with the configured IP Pool.

To illustrate working of DNS server do the following on any PC:



Scenario 12: Need of Network Address Translation (NAT) and Working



In Company Router go to CLI:

- Try to access DMZ server from PC0's web browser by using URL: http:// 209.165.100.29 then you should **not be able to access** the DMZ Server webpages.

```
Conf t
int g0/0
ip nat out
int g0/1
ip nat inside
```

- **Activity 1:** Static Translation from 1 public Ip to 1 private IP (Static 1-1 NAT)

```
ip nat inside source static 10.0.0.240 209.165.100.29
####exit (Config-if to config)
```

- Now try to access DMZ server from PC0's web browser by using URL: http:// 209.165.100.29 then you should be **able to access** the DMZ Server webpages.

- **Activity 2:** Static Translation from 1 public Ip with a specific port number (web server: port 80) to 1 private IP (Static 1-1 NAT with port mapping)

```
ip nat inside source static tcp 10.0.0.250  80 209.165.100.30 80
exit
```

```
company#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.100.29    10.0.0.240         ---                ---
tcp 209.165.100.29:80  10.0.0.240:80      192.168.1.100:1033 192.168.1.100:1033
tcp 209.165.100.29:80  10.0.0.240:80      192.168.1.100:1034 192.168.1.100:1034
tcp 209.165.100.30:80  10.0.0.250:80      ---                ---
tcp 209.165.100.30:80  10.0.0.250:80      192.168.1.100:1035 192.168.1.100:1035
```

- Now try to access Webserver from PC0's web browser by using URL: http:// 209.165.100.30:80 then you should be **able to access** the webpages in the webserver.

- **Activity 3:** To translate any private Ip address with in a network (say: 10.0.0.0) to a particular public IP Address over different pot number (PAT/NAT Overloaded Translation)

```
Conf t
access-list 10 permit 10.0.0.0 0.0.0.255 (wild card)
Ip nat inside source ?  displays (list static)
ip nat inside source list 10 interface g0/0 overload
Typ Ping command from PC1 to PC0
Exit or end
Company# show ip nat translation
```

```
company#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.100.30:2  10.0.0.100:2       192.168.1.100:2    192.168.1.100:2
icmp 209.165.100.30:3  10.0.0.100:3       192.168.1.100:3    192.168.1.100:3
icmp 209.165.100.30:4  10.0.0.100:4       192.168.1.100:4    192.168.1.100:4
---  209.165.100.29    10.0.0.240         ---                ---
tcp 209.165.100.29:80  10.0.0.240:80      192.168.1.100:1033 192.168.1.100:1033
tcp 209.165.100.29:80  10.0.0.240:80      192.168.1.100:1034 192.168.1.100:1034
tcp 209.165.100.30:80  10.0.0.250:80      ---                ---
tcp 209.165.100.30:80  10.0.0.250:80      192.168.1.100:1035 192.168.1.100:1035

company#
```

Add another PC to 10.0.0.0 network, assign Ip, gateway and Ping PC0

```
company#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.100.30:2  10.0.0.100:2       192.168.1.100:2    192.168.1.100:2
icmp 209.165.100.30:3  10.0.0.100:3       192.168.1.100:3    192.168.1.100:3
icmp 209.165.100.30:4  10.0.0.100:4       192.168.1.100:4    192.168.1.100:4
---  209.165.100.29    10.0.0.240         ---                ---
tcp 209.165.100.29:80  10.0.0.240:80      192.168.1.100:1033 192.168.1.100:1033
tcp 209.165.100.29:80  10.0.0.240:80      192.168.1.100:1034 192.168.1.100:1034
tcp 209.165.100.30:80  10.0.0.250:80      ---                ---
tcp 209.165.100.30:80  10.0.0.250:80      192.168.1.100:1035 192.168.1.100:1035

company#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.100.30:1  10.0.0.101:1       192.168.1.100:1    192.168.1.100:1
icmp 209.165.100.30:2  10.0.0.101:2       192.168.1.100:2    192.168.1.100:2
icmp 209.165.100.30:3  10.0.0.101:3       192.168.1.100:3    192.168.1.100:3
icmp 209.165.100.30:4  10.0.0.101:4       192.168.1.100:4    192.168.1.100:4
---  209.165.100.29    10.0.0.240         ---                ---
tcp 209.165.100.29:80  10.0.0.240:80      192.168.1.100:1033 192.168.1.100:1033
tcp 209.165.100.29:80  10.0.0.240:80      192.168.1.100:1034 192.168.1.100:1034
tcp 209.165.100.30:80  10.0.0.250:80      ---                ---
tcp 209.165.100.30:80  10.0.0.250:80      192.168.1.100:1035 192.168.1.100:1035

company#
```

- **Activity 4:** Configuration for Dynaic NAT on other router labelled your router

```
en
conf t
int g0/0
ip nat outside
int g0/1
ip nat inside
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat ?
ip nat pool OURSOIS 209.165.100.17 209.165.100.24 ?
ip nat pool OURSOIS 209.165.100.17 209.165.100.24 netmask
255.255.255.240
ip nat inside source list 1 pool OURSOIS overload
```

now from PC0 access DMZ server from browser

now router cli to see IP translation

exit or end or clt+C

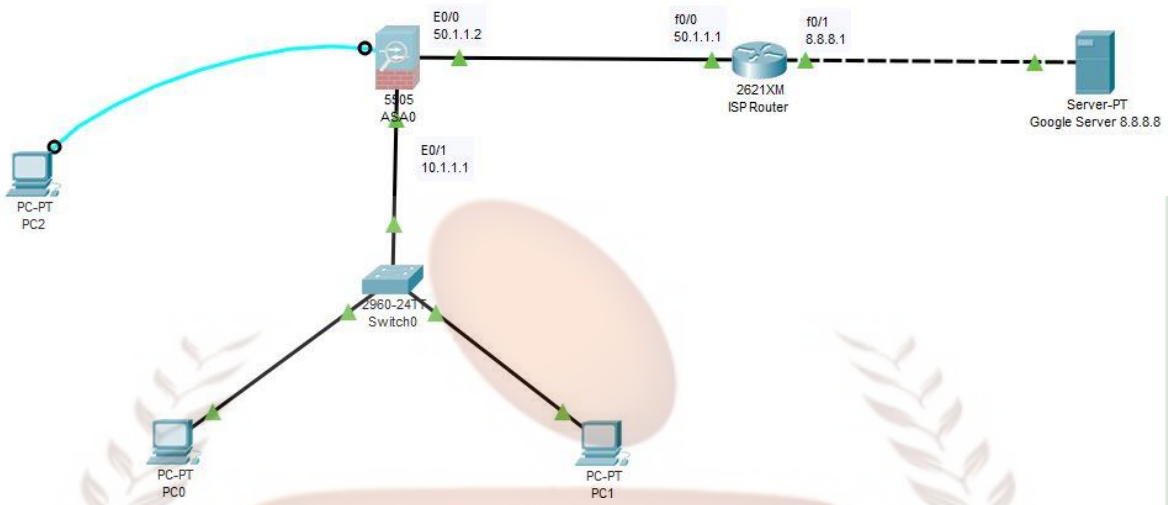
show ip nat translations

```
YourRouter#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
tcp 209.165.100.17:1036192.168.1.100:1036 209.165.100.29:80  209.165.100.29:80

YourRouter#
```

- Add another PC to 192.168.101 network, assign Ip, gateway and browse web server 209.165.100.30

```
YourRouter#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
tcp 209.165.100.17:1036192.168.1.100:1036 209.165.100.29:80  209.165.100.29:80

YourRouter#
YourRouter#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
tcp 209.165.100.17:1025192.168.1.101:1025 209.165.100.30:80  209.165.100.30:80
tcp 209.165.100.17:1036192.168.1.100:1036 209.165.100.29:80  209.165.100.29:80

YourRouter#
```

Scenario 13: Configuring Organisational Hardware Firewall



ASA Firewall Configurations:

- Go to the console of PC2 to access ASA Server using Terminal application.

```
en
show running-config
```

- By default DHCP is enabled we need to remove it

```
conf t
no dhcpd address 192.168.1.5-192.168.1.36 inside
exit
show running-config
```
(Now there is no dhcp configuration).

- Now we need to remove default VLAN IP address and set it to our environment

```
conf t
int vlan 1
ip add 10.1.1.1 255.0.0.0
no shut
nameif inside
security-level 100 (inside)
exit
int e0/1
switchport access vlan 1
no shut
exit
int vlan 2
```

```
ip add 50.1.1.2 255.0.0.0
no shut
nameif outside
security-level 0 (outside)
exit
int e0/0
switchport access vlan 2
exit
```

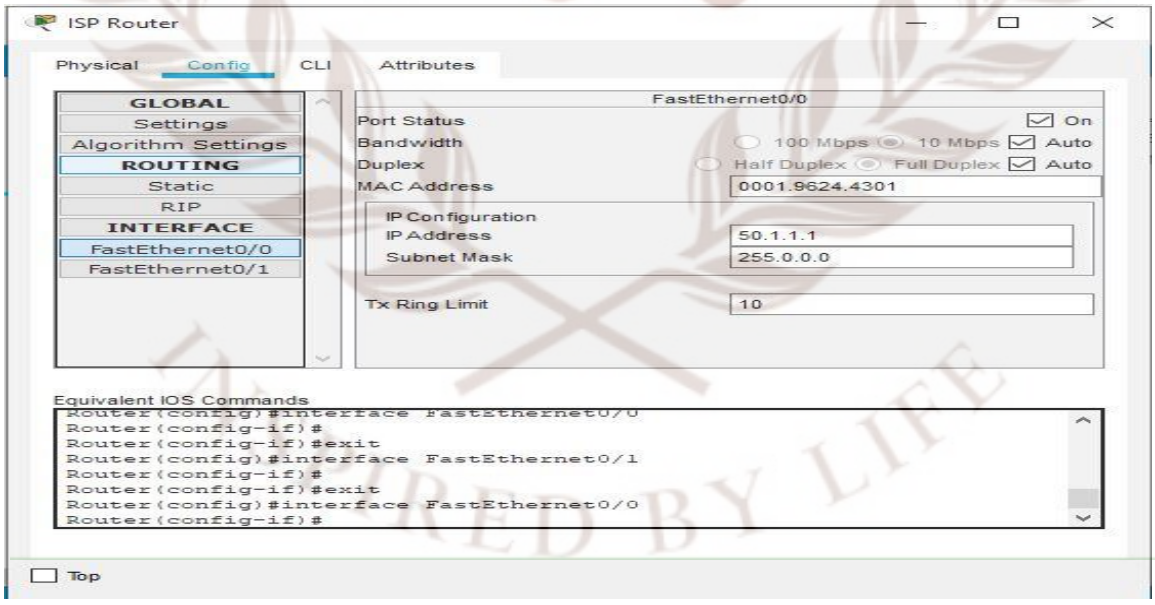
- Configuring DHCP and DNS ASA Server so that PC inside network go IP Adddress dynamically:
- Go to the console of PC2 to access ASA Server terminal using Terminal.

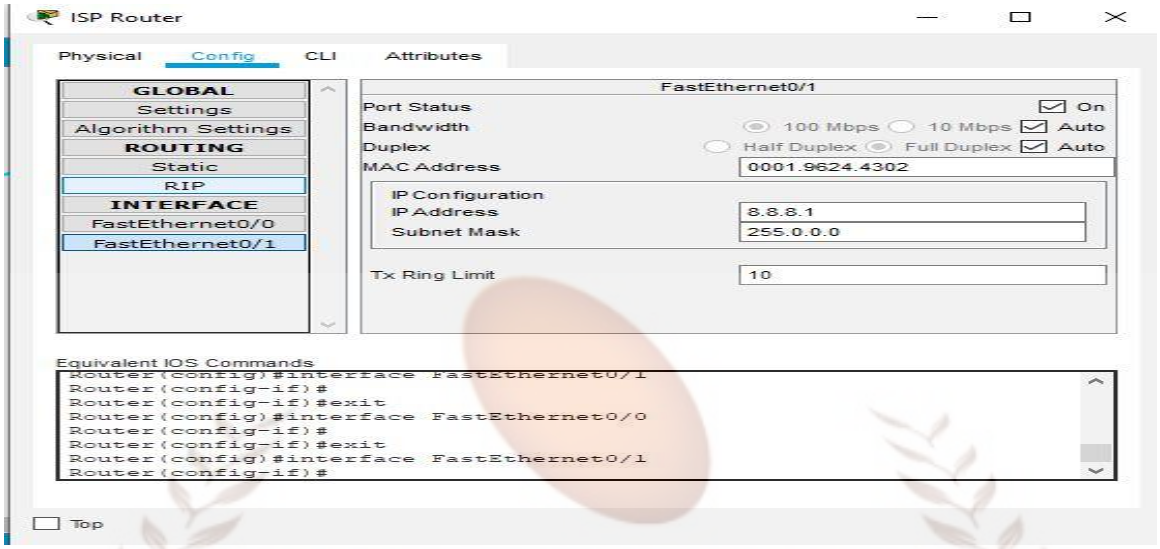
```
conf t
dhcpd address 10.1.1.10-10.1.1.30 inside
dhcpd dns 8.8.8.8 interface inside
```

- Configuring Default Route on ASA:

```
route outside 0.0.0.0  0.0.0.0 50.1.1.1
```

Router Configurations:

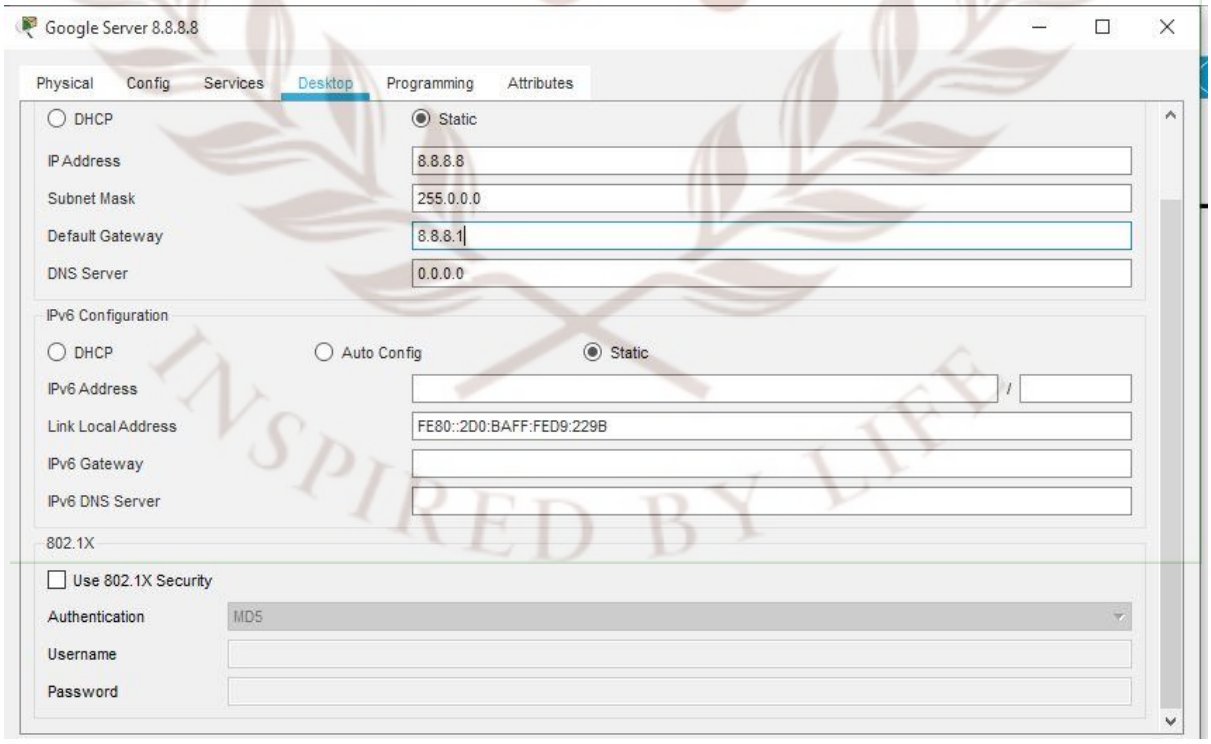




- Configuring OSPF Routeing Protocol:
- Go to CLI of router:

```
Conf t
router ospf 1
net 50.0.0.0 0.255.255.255 area 0
net 8.0.0.0 0.255.255.255 area 0
```

Google Server Configurations:



Assigning IP address to PC0 and PC1:

- Enable DHCP on PC1 and PC2

Create object Network & Enable NAT on ASA:

- Before do this pass a packet from PC0 to Google Server it should fail
- Go to the console of PC2 to access ASA Server using Terminal application.

```
object network ?
object network LAN (any Name)
subnet 10.0.0.0 255.0.0.0
nat ?
nat (inside, outside) dynamic interface
```

- Now pass a packet from PC0 to Google Server it should fail
- Open CLI of BOTh PCS and ping -t 8.8.8.8 it should fail and minimize

Create ACL on ASA:

- Go to the console of PC2 to access ASA Server using Terminal application.

```
Conf t
access-list maherules (general name) ?
access-list maherules (general name) extended permit tcp
any any
access-list maherules (general name) extended permit icmp
any any
access-group maherules ?
access-group maherules in interface outside
```

- (now check the CLI of both PCs we will see ping responses)

On ASA terminal:

```
show nat
show xlate
```

- You should be able to see the NAP/PAT translations