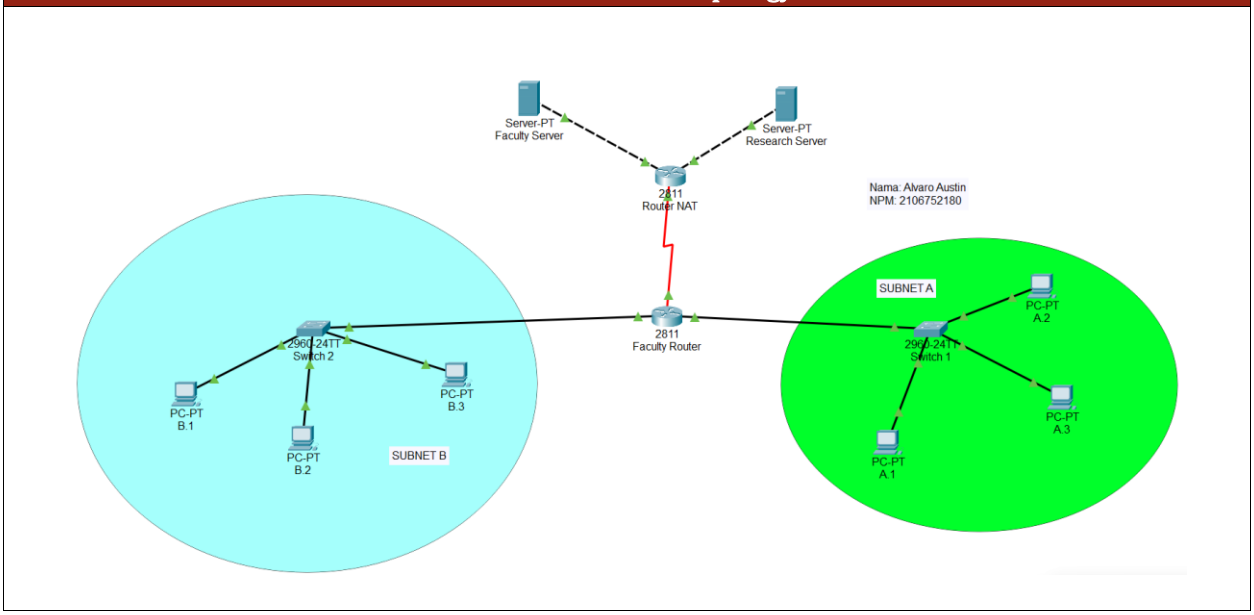
Answer Sheet
Hands On - H03

NAT and OSPF

Name : Alvaro Austin
Student ID : 2106752180

1. [10]Topology Screenshot

Screenshot of the Topology



2. [20]IP address Allocation

Subnetting Distribution using VLSM Method

Subnet	Network Address	Slash	Subnet Mask	First Device IP Address	Last Device IP Address	Default Gateway
A	192.168.0.0	/26	255.255.255.192	192.168.0.2	192.168.0.62	192.168.0.1
B	192.168.0.64	/27	255.255.255.224	192.168.0.66	192.168.0.94	192.168.0.65

IPv4 Address Distribution

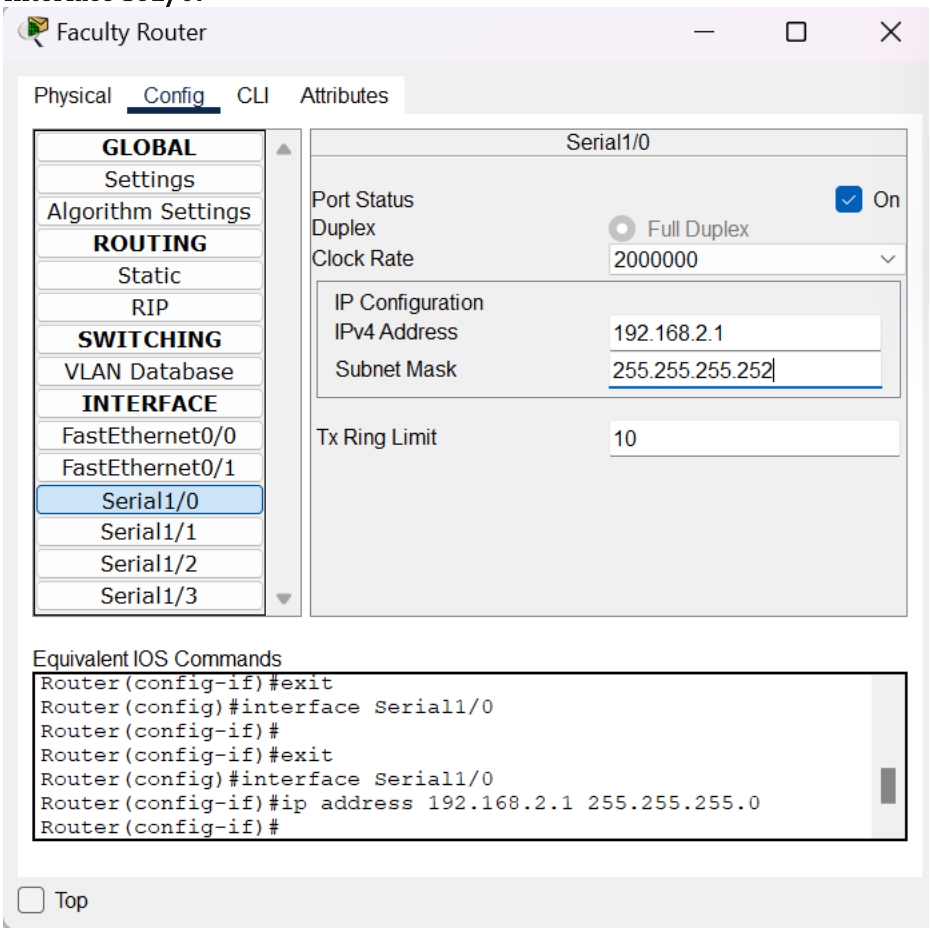
Device Name	IPv4 Address	Subnet Mask	Default Gateway
Research Server	34.16.12.33	255.255.224.0	34.16.0.1
Faculty Server	10.5.2.0	255.255.248.0	10.5.0.1
A.1	192.168.0.2	255.255.255.192	192.168.0.1
A.2	192.168.0.3	255.255.255.192	192.168.0.1
A.3	192.168.0.4	255.255.255.192	192.168.0.1
B.1	192.168.0.66	255.255.255.224	192.168.0.65

B.2	192.168.0.67	255.255.255.224	192.168.0.65
B.3	192.168.0.68	255.255.255.224	192.168.0.65

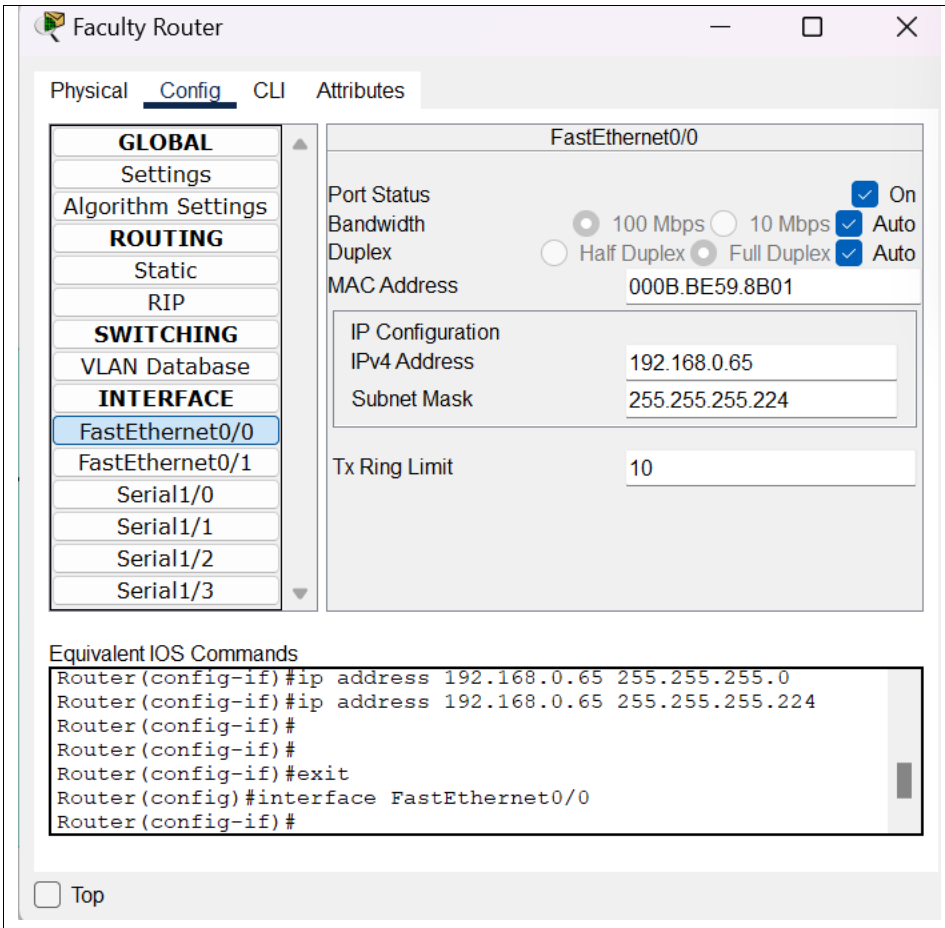
Screenshots of Configuration for each Device

Faculty Router configuration for Interface Serial 1/0, FA 0/0, and FA 0/1

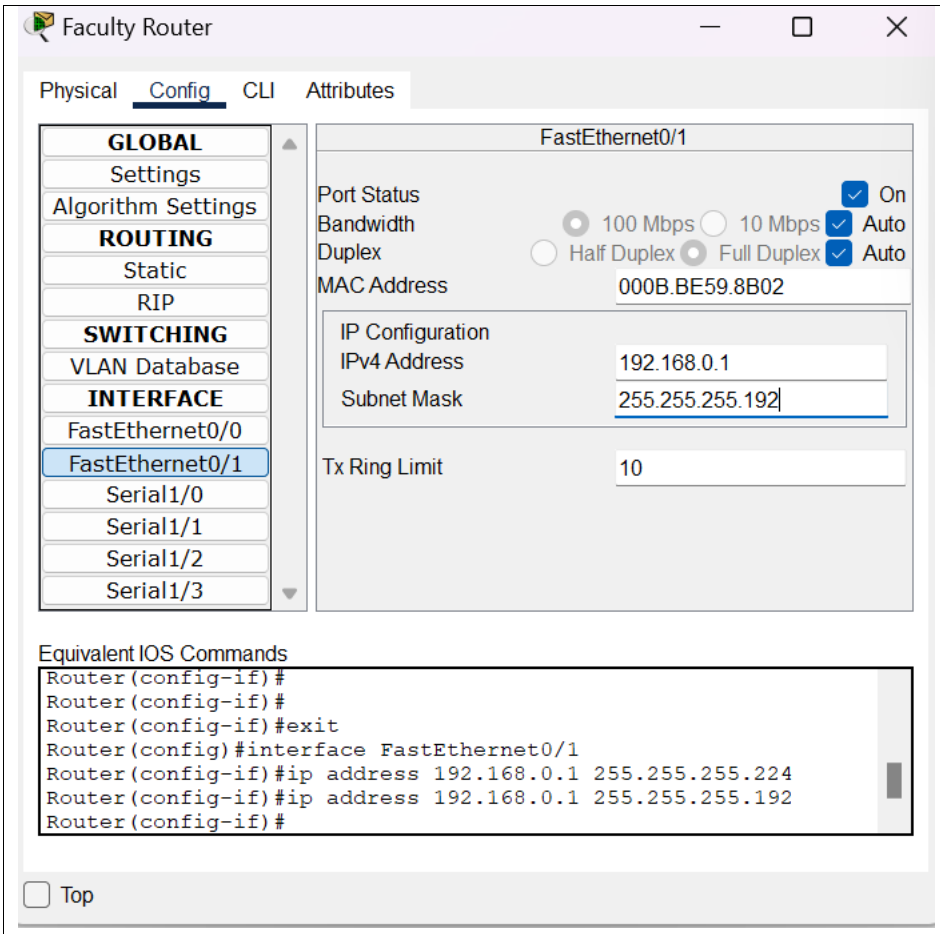
Interface Se1/0:



Interface Fa0/0:

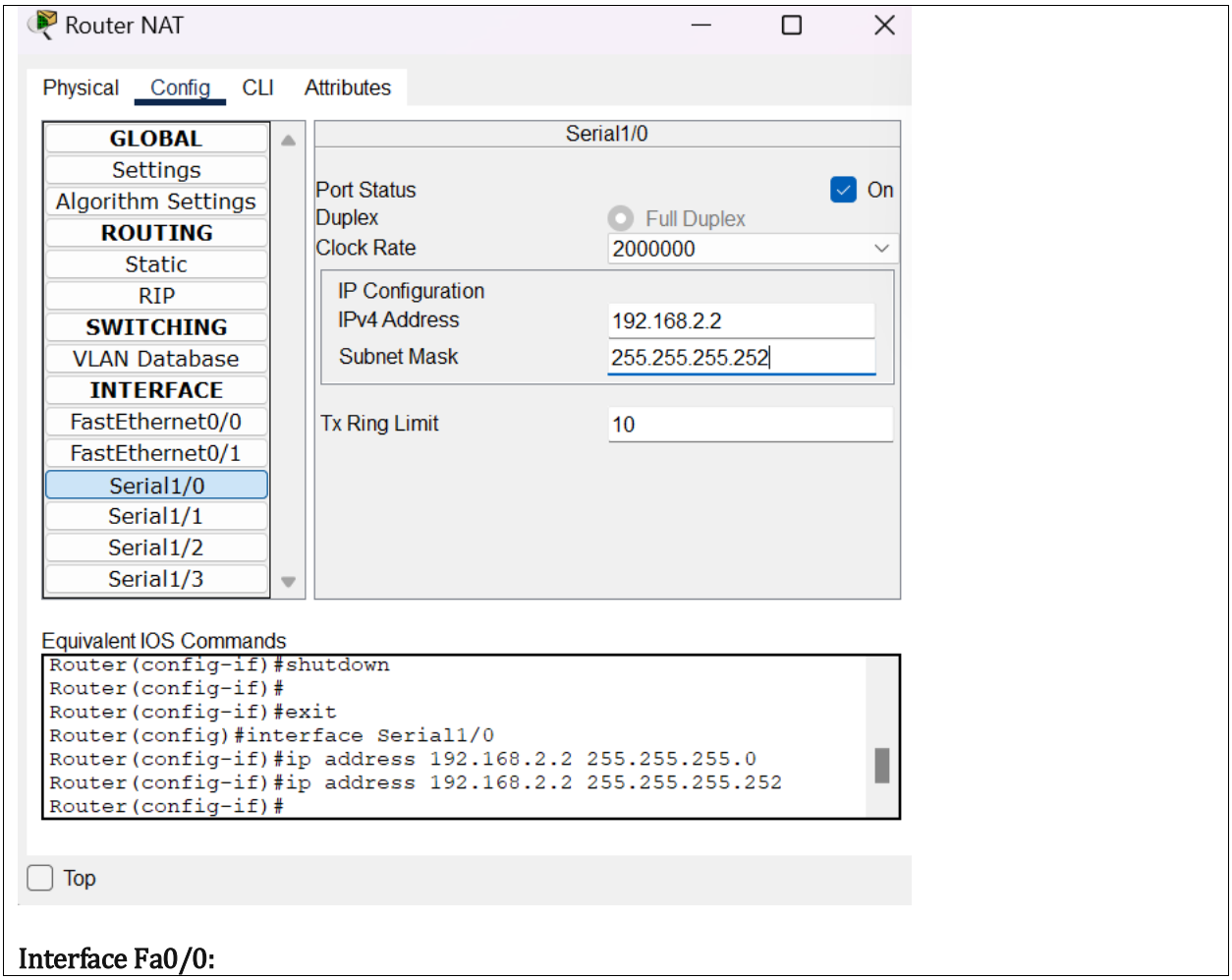


Interface Fa0/1:

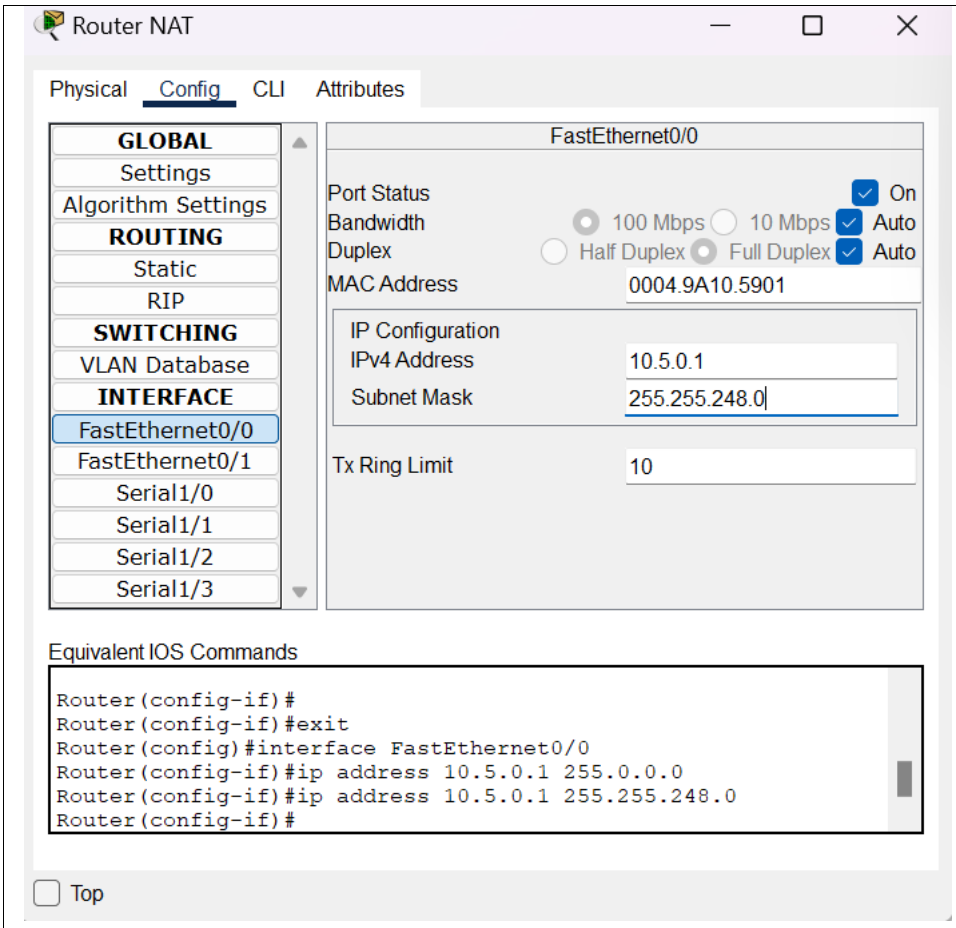


NAT Router configuration for Interface Serial 1/0, FA 0/0, and FA 0/1

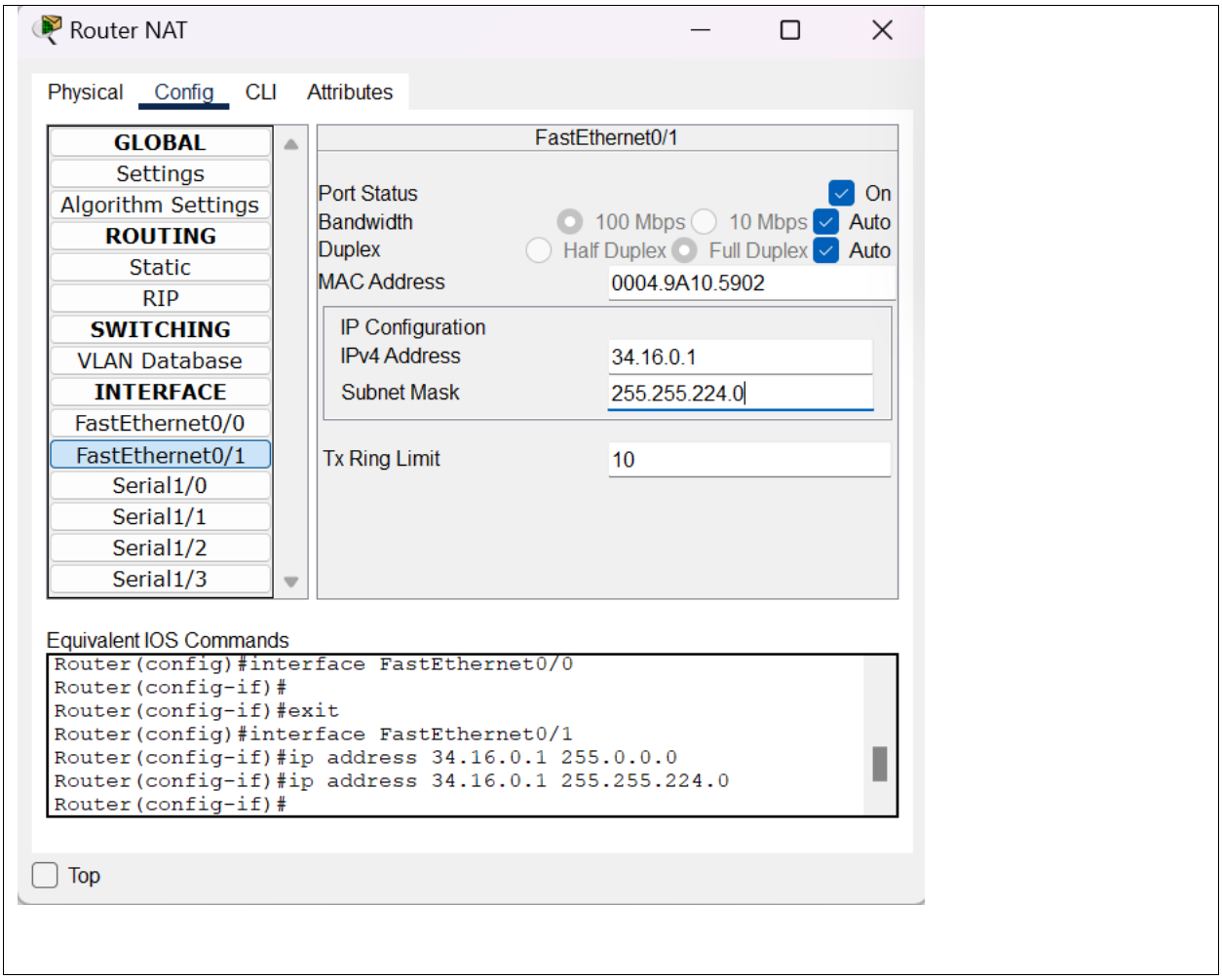
Interface Se1/0:



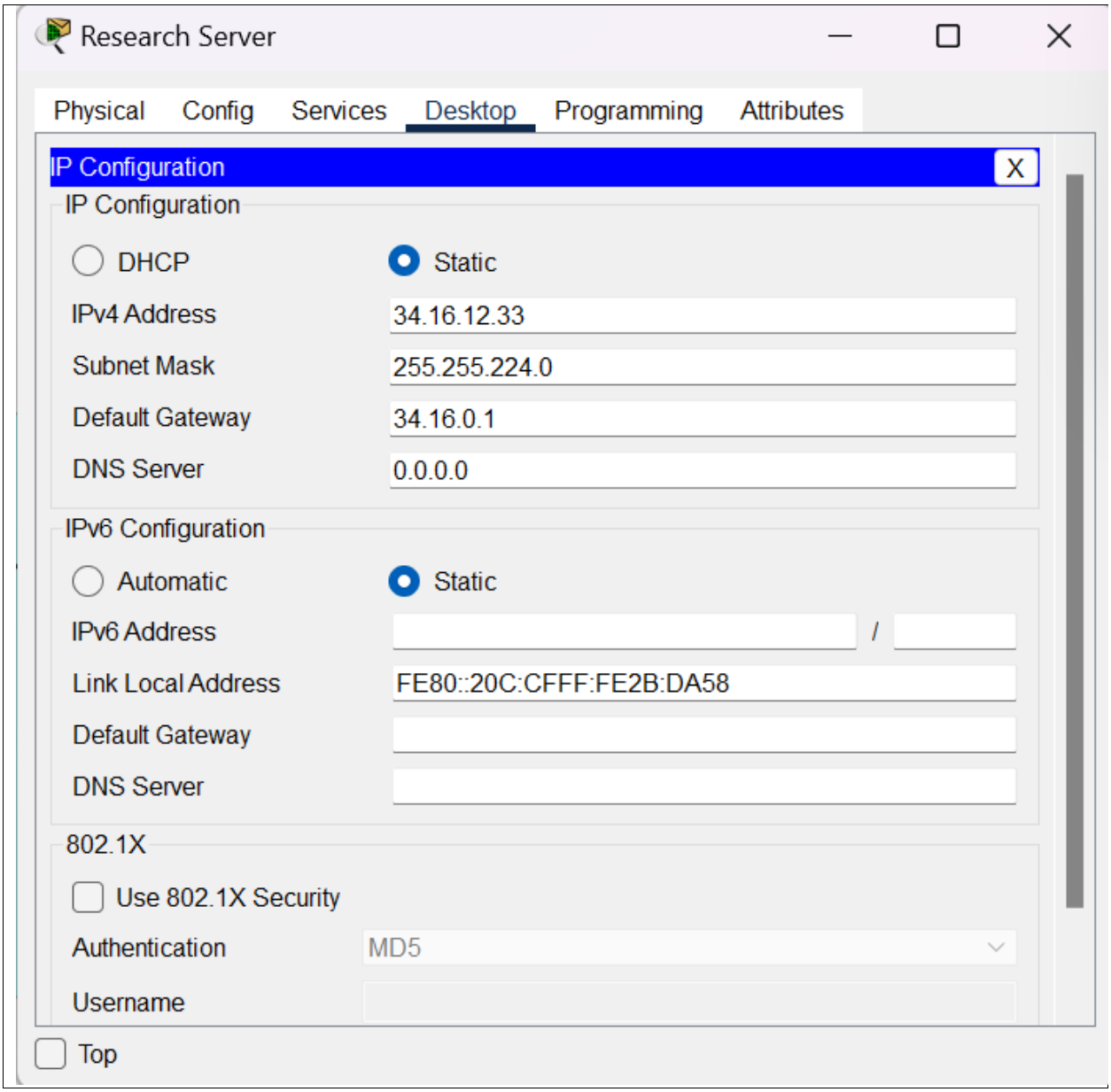
Interface Fa0/0:



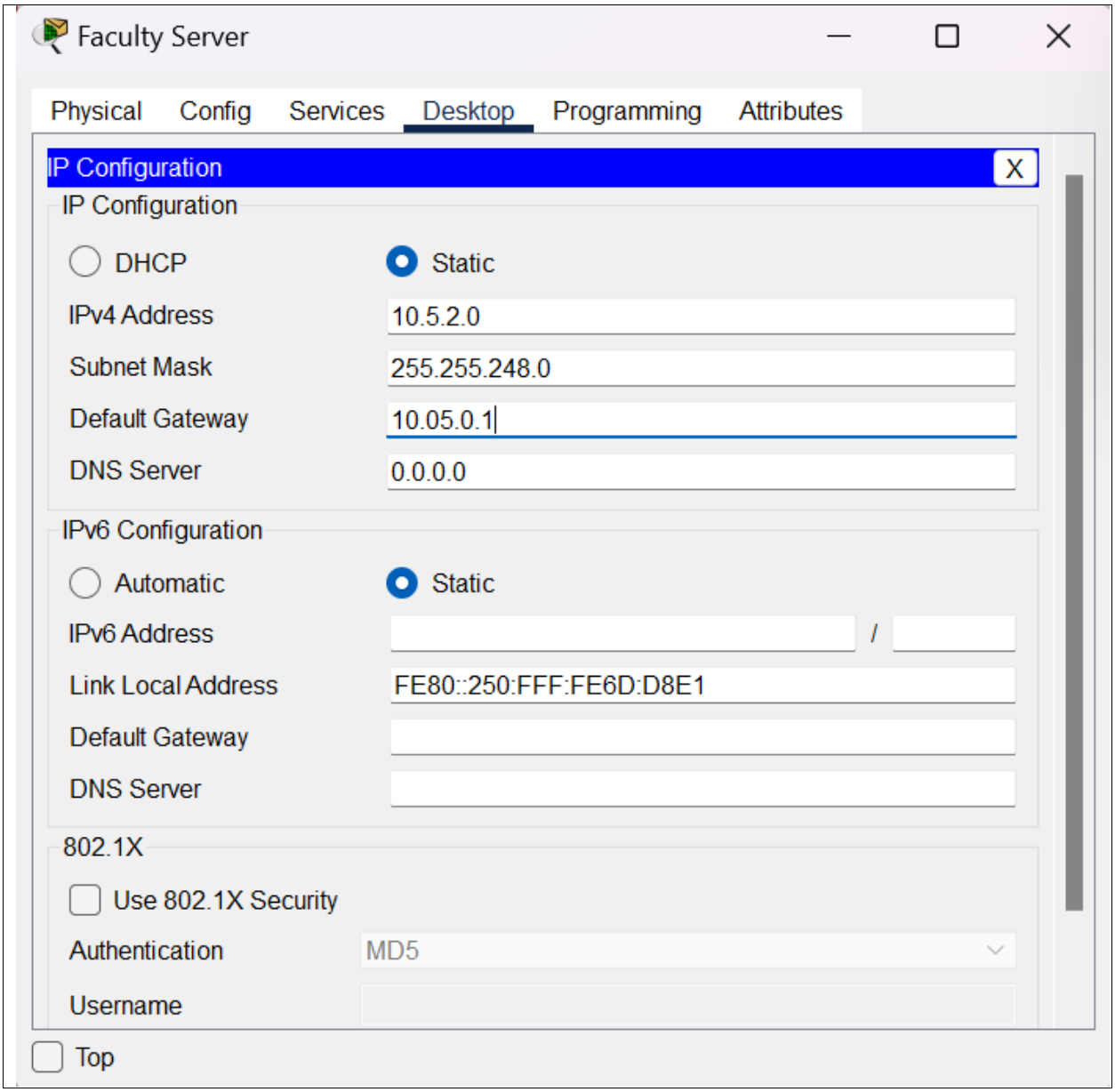
Interface Fa0/1:



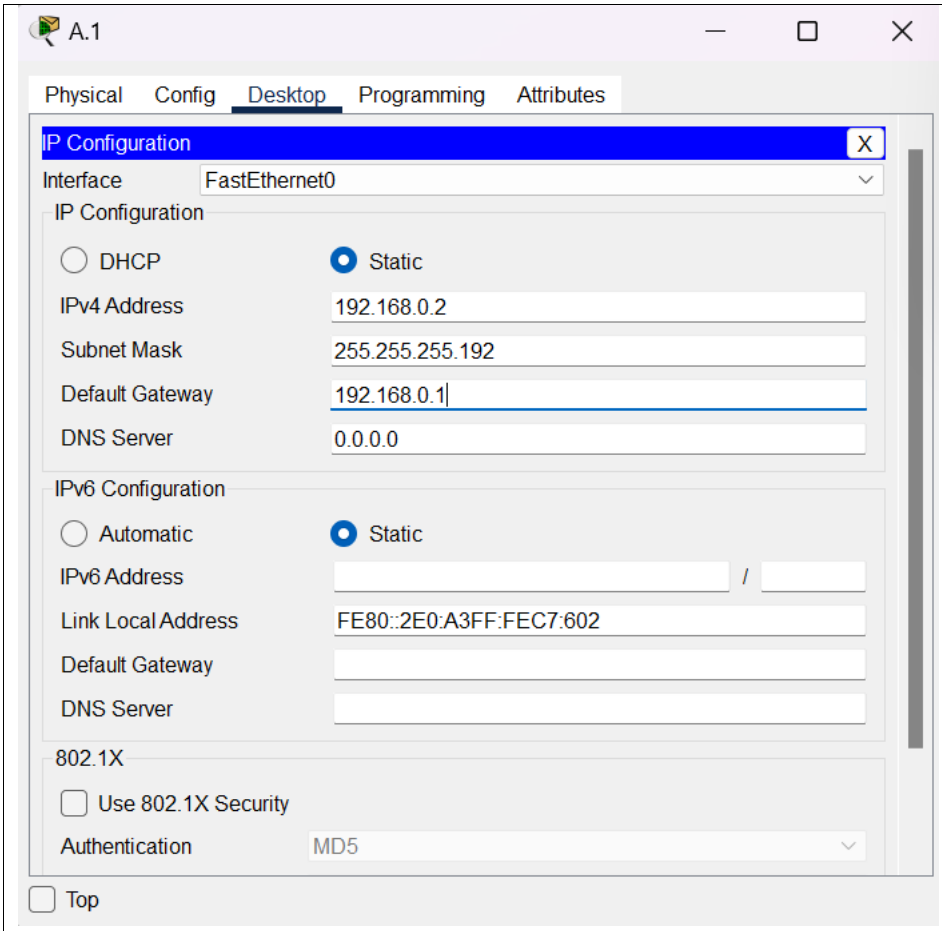
Research Server



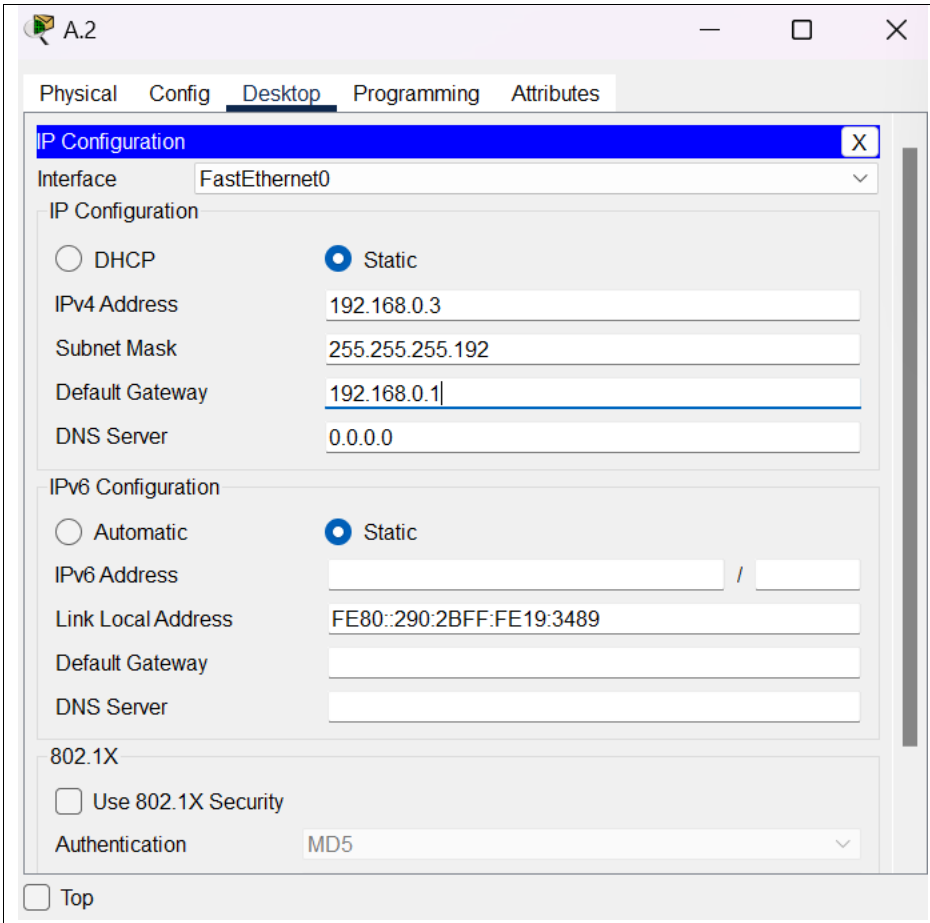
Faculty Server



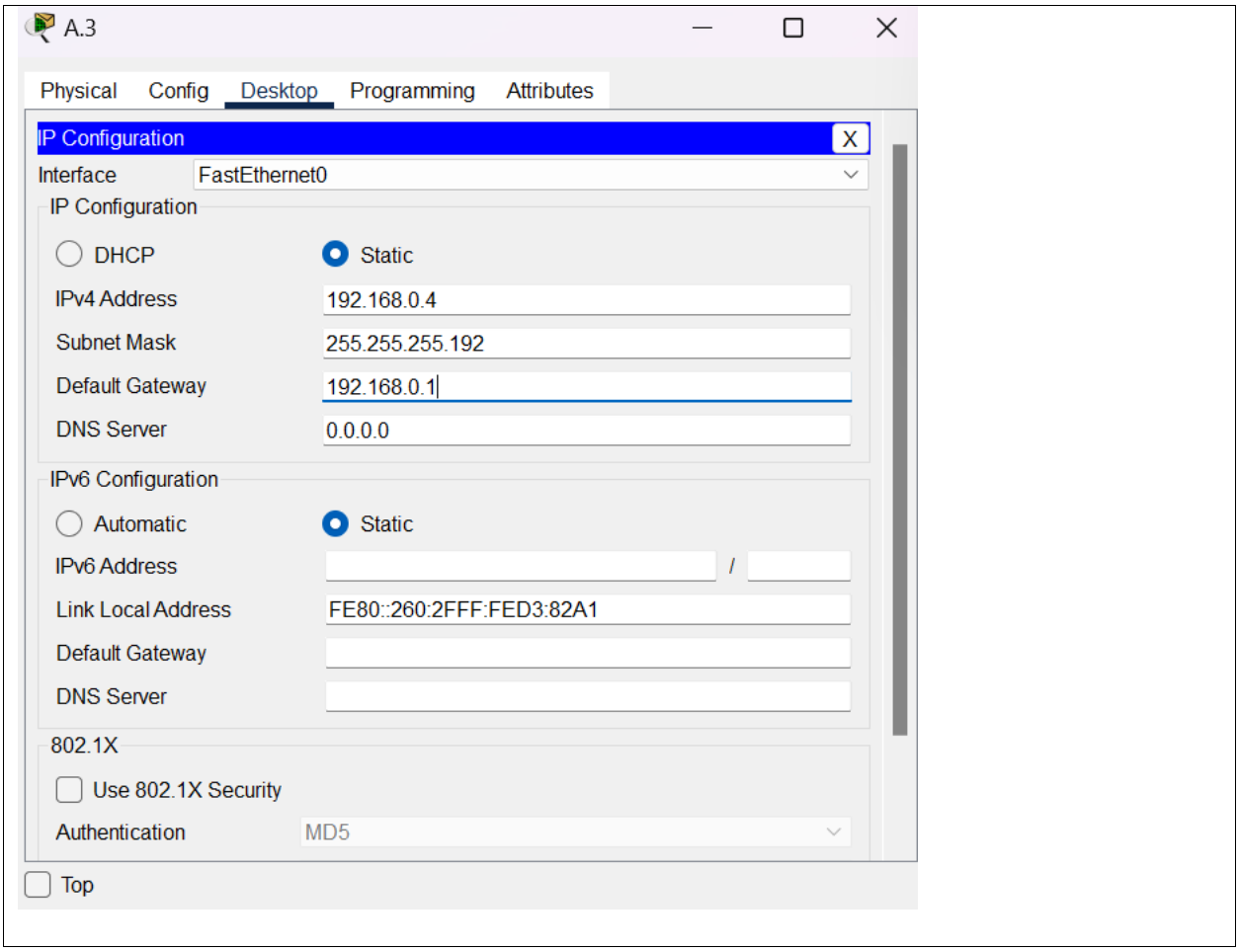
PC A.1, A.2, and A.3
PC A.1:


A.1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.0.2
Subnet Mask
255.255.255.192
Default Gateway
192.168.0.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2E0:A3FF:FEC7:602
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Top

PC A.2:

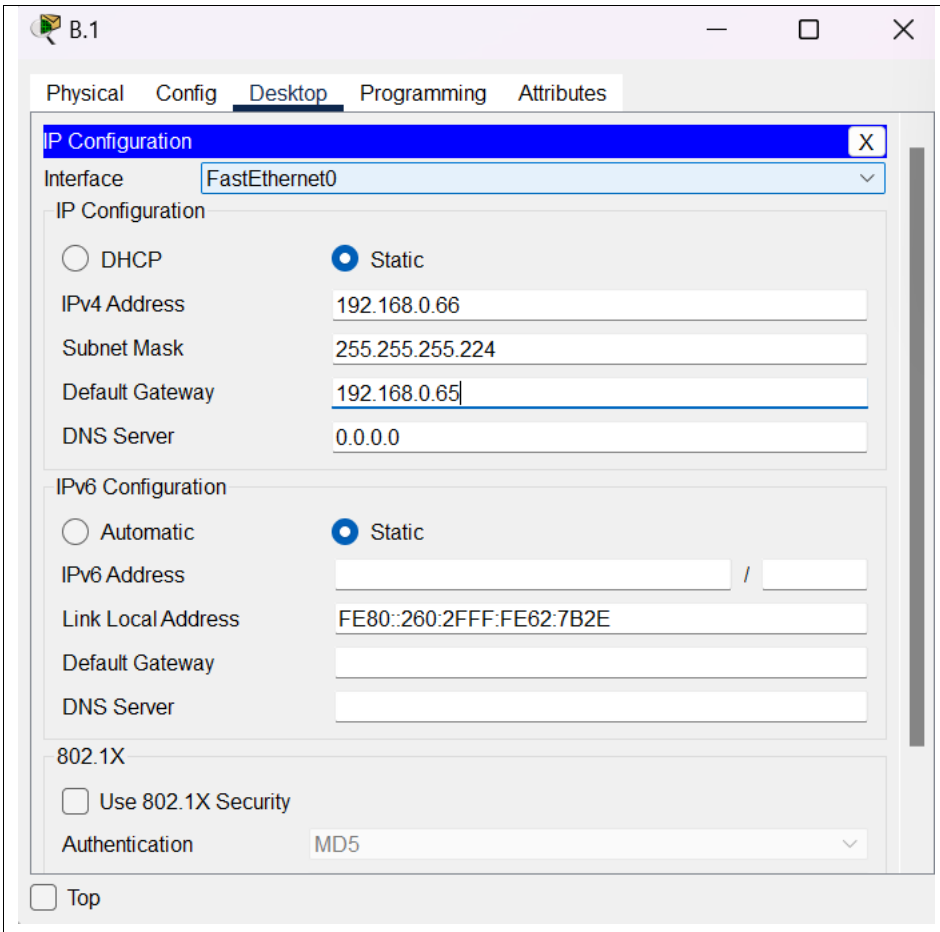

A.2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.0.3
Subnet Mask
255.255.255.192
Default Gateway
192.168.0.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::290:2BFF:FE19:3489
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Top

PC A.3:

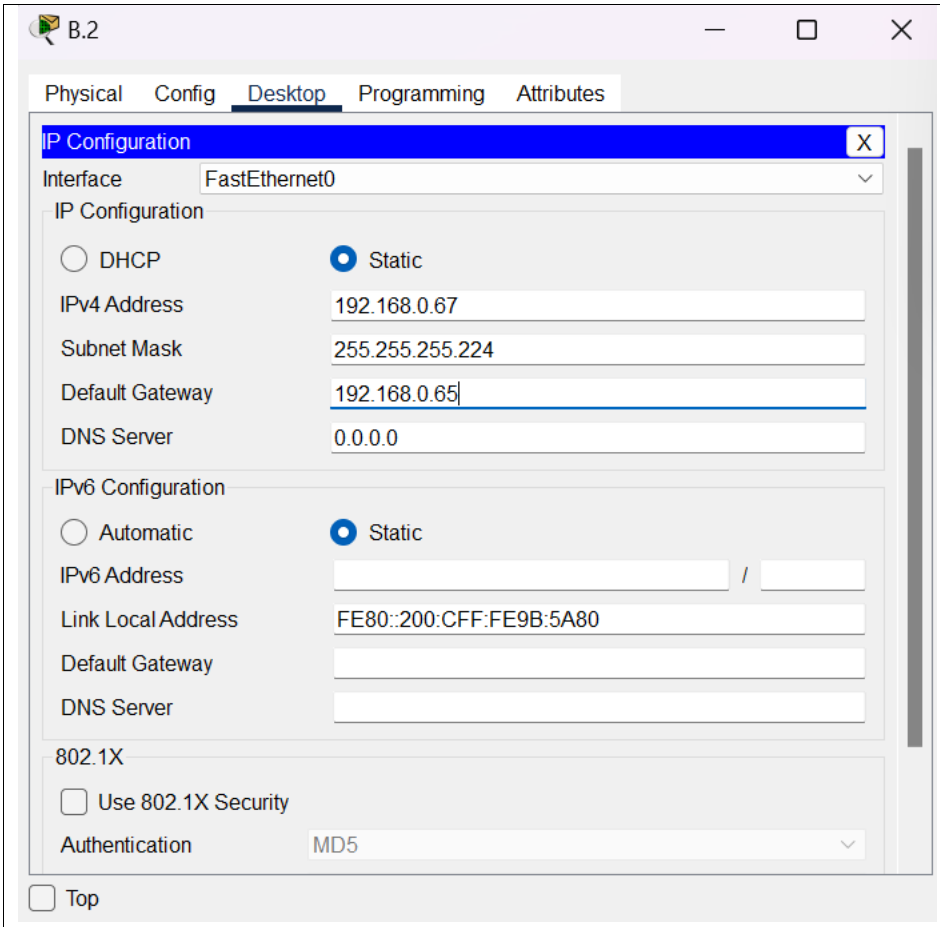


PC B.1, B.2, and B.3

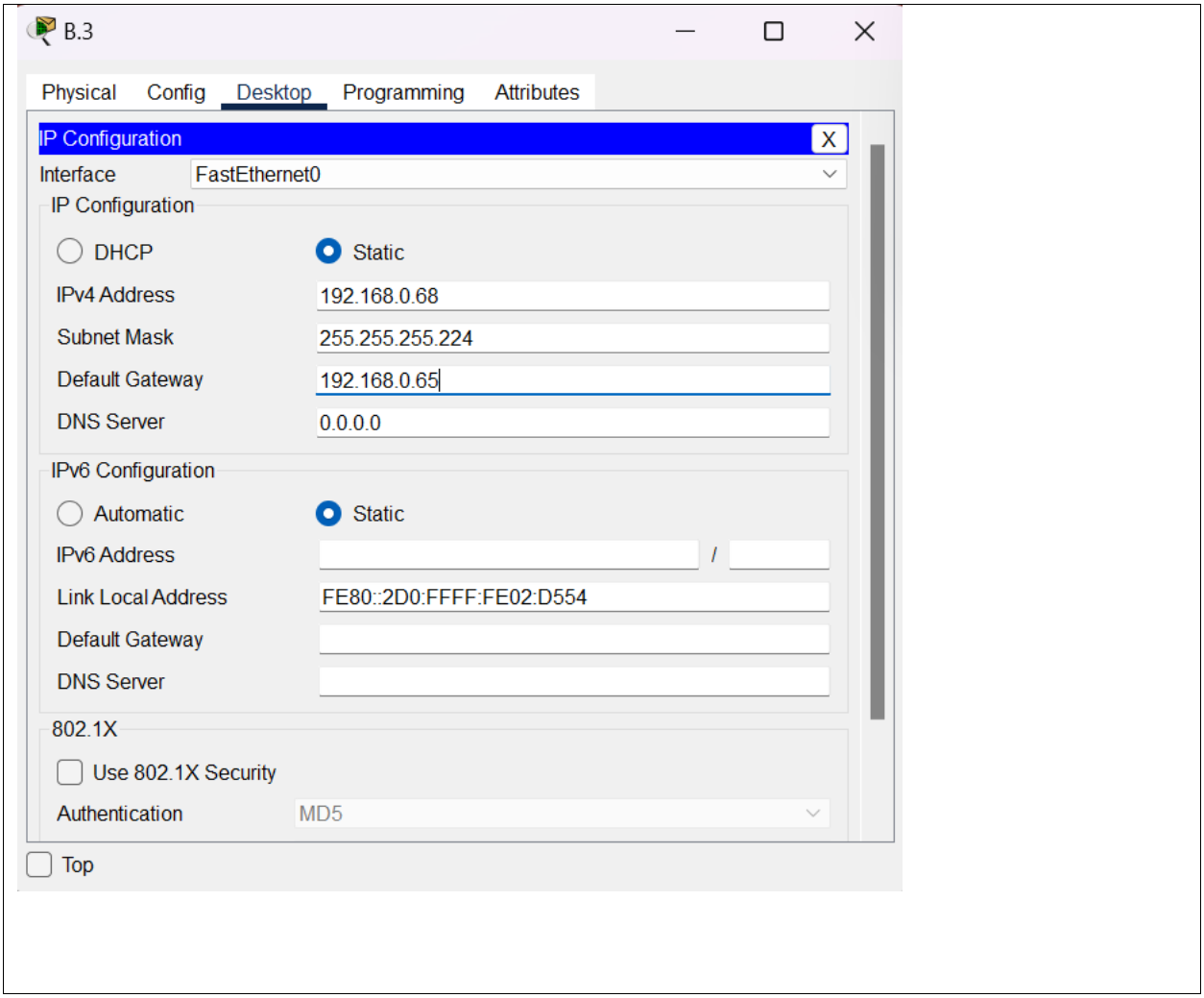
PC B.1:


B.1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.0.66
Subnet Mask
255.255.255.224
Default Gateway
192.168.0.65
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::260:2FFF:FE62:7B2E
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Top

PC B.2:

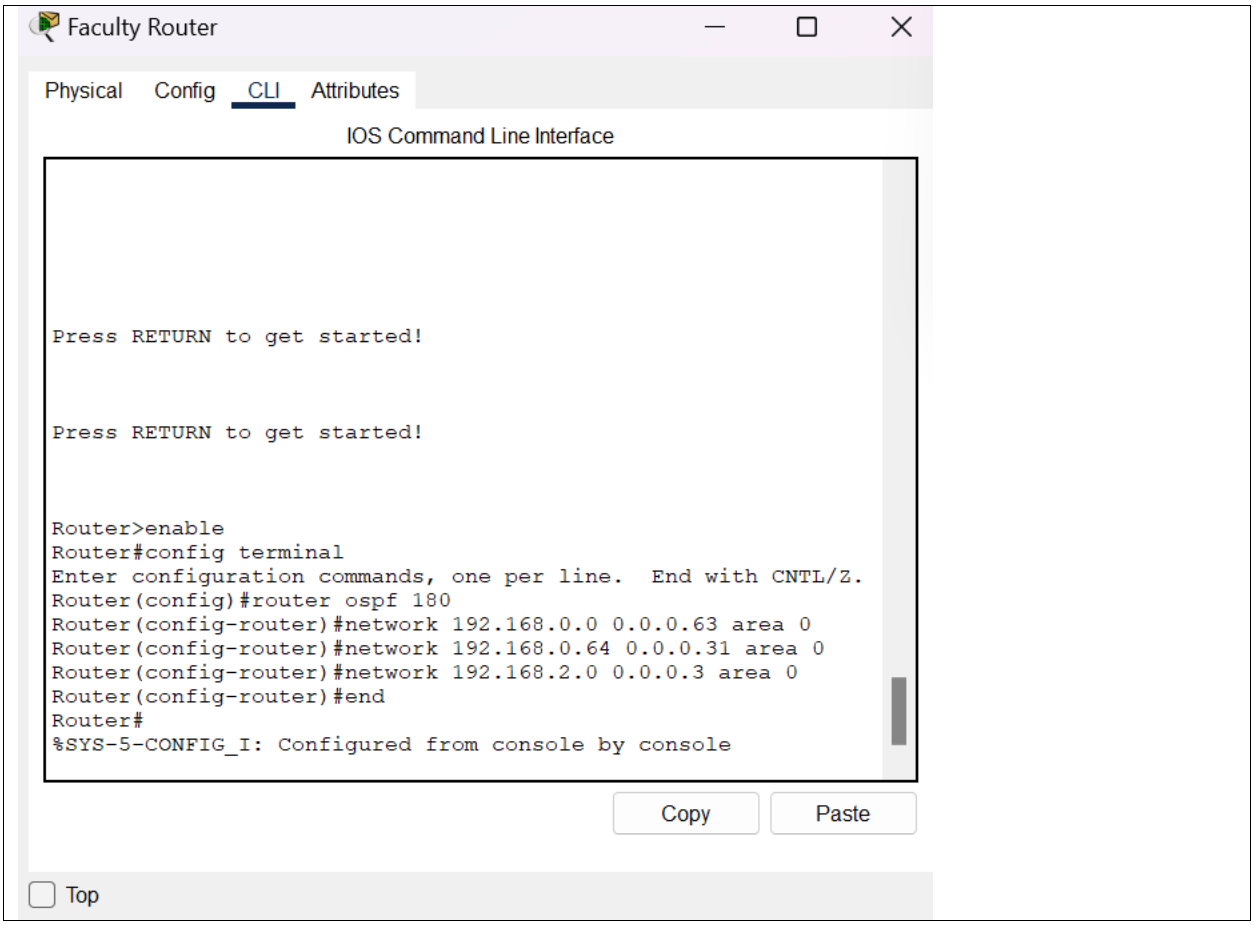

B.2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.0.67
Subnet Mask
255.255.255.224
Default Gateway
192.168.0.65
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::200:CFF:FE9B:5A80
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Top

PC B.3:

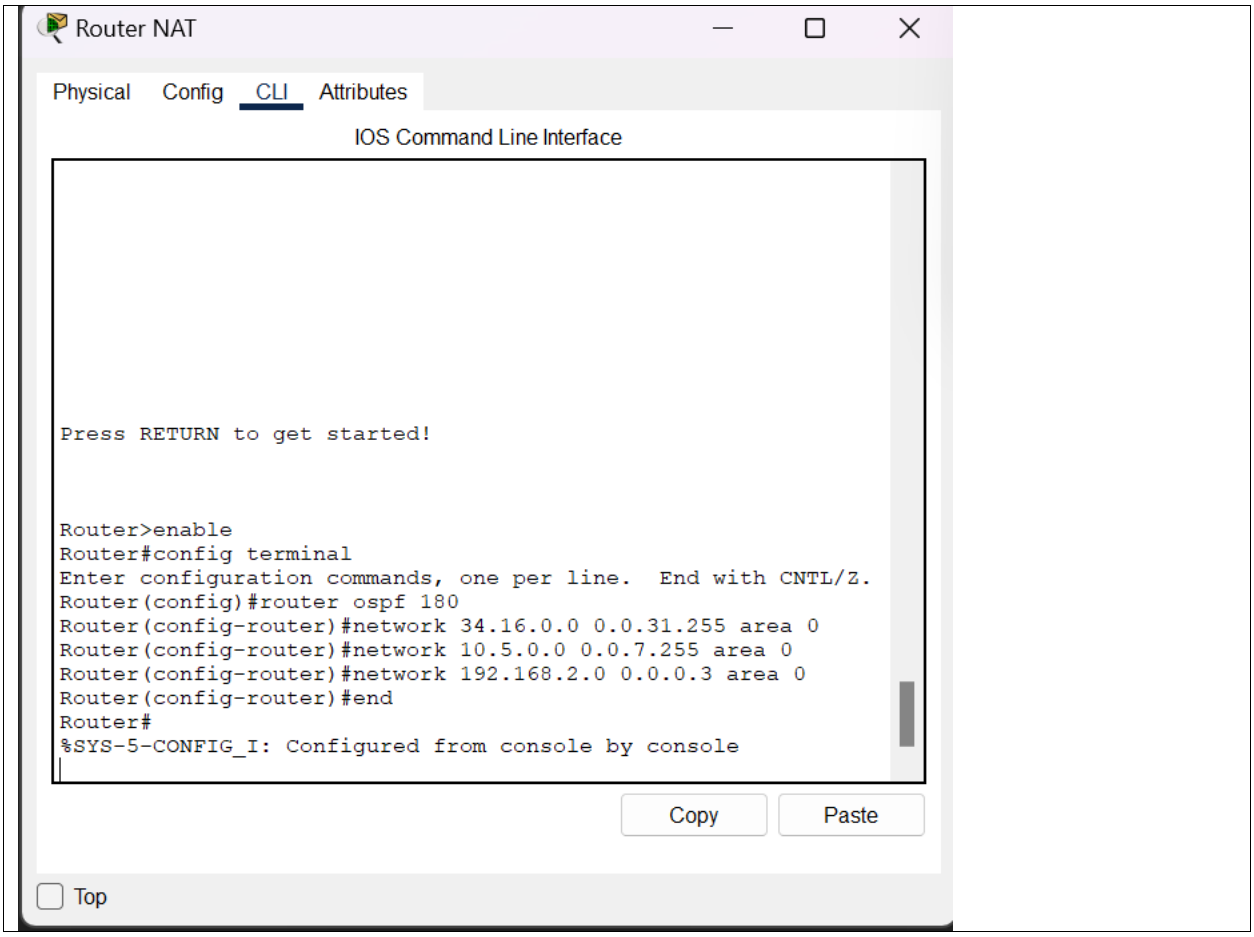


3. [30]OSPF Configuration

CLI for Faculty Router



CLI for NAT Router



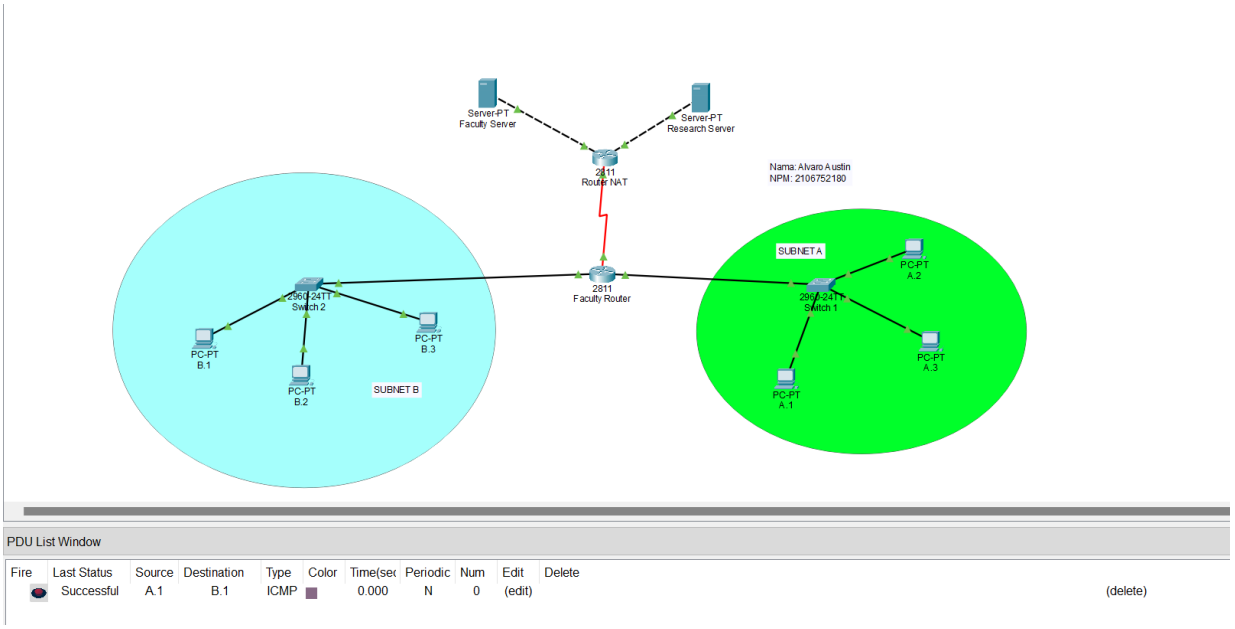
Connectivity Test

Answers:

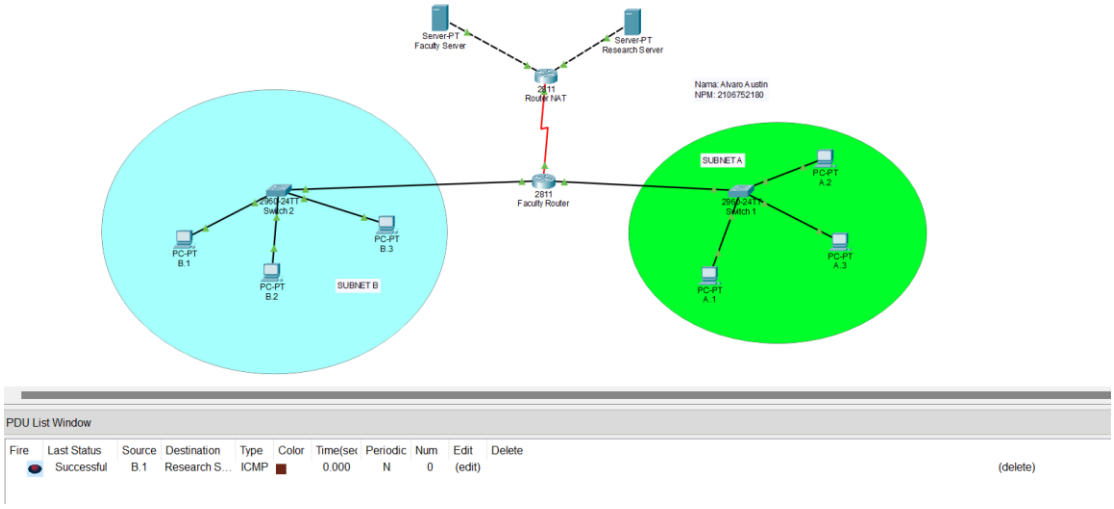
- A.1 to B.1 Test = **success**
- B.1 to Research Server = **success**

Proof:

- **A.1 to B.1 Test (First time failed but the rest successful)**

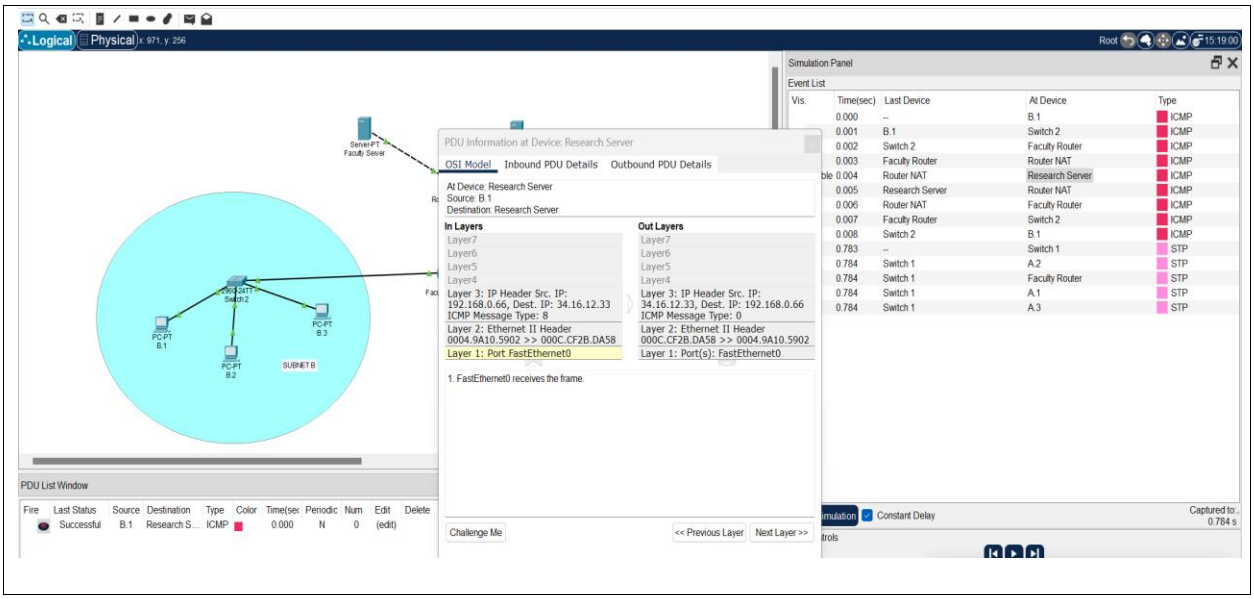


- **B.1 to Research Test (The same, first one failed, then the rest successful)**



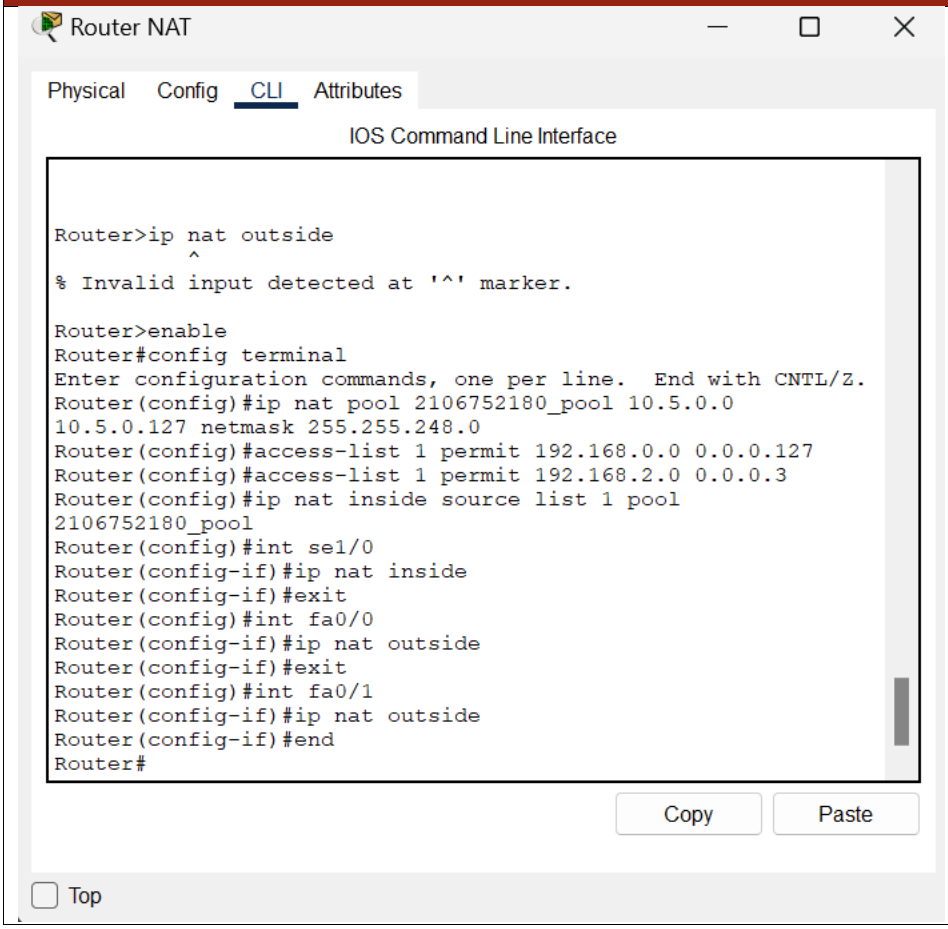
OSI Model

OSI Model at Device Research Server



4. [20]NAT Configuration

CLI for NAT Router



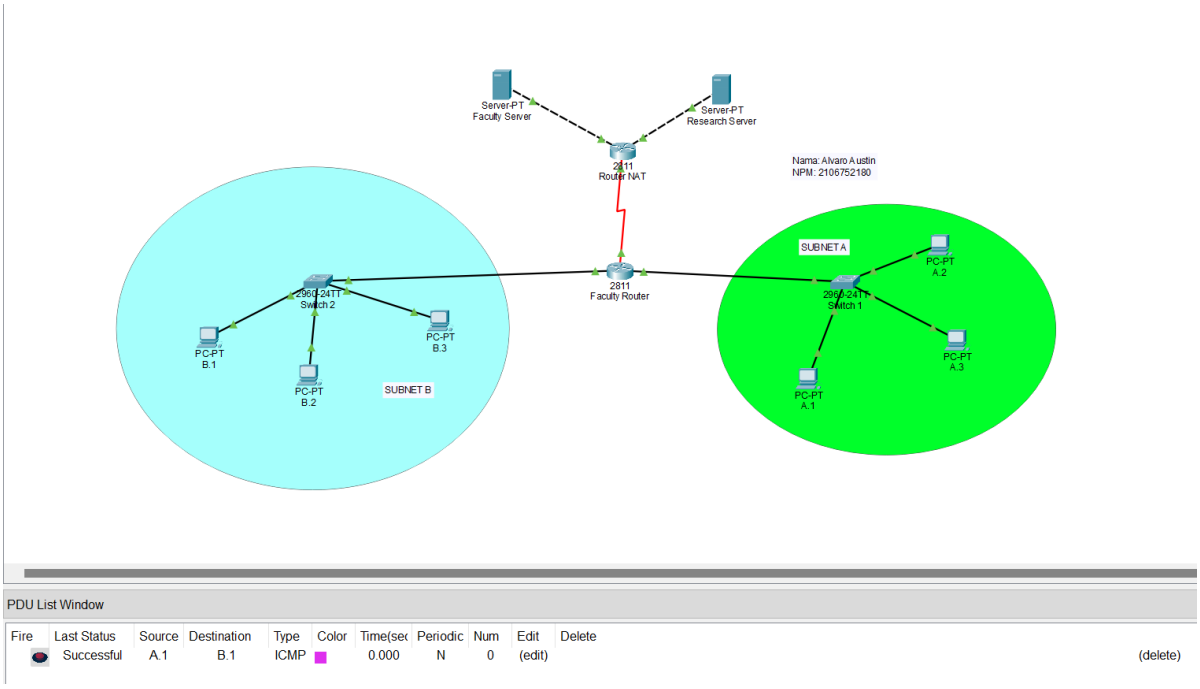
Connectivity Test

Answers:

- A.1 to B.1 Test = **success**
- B.1 to Research Server = **success**

Proof:

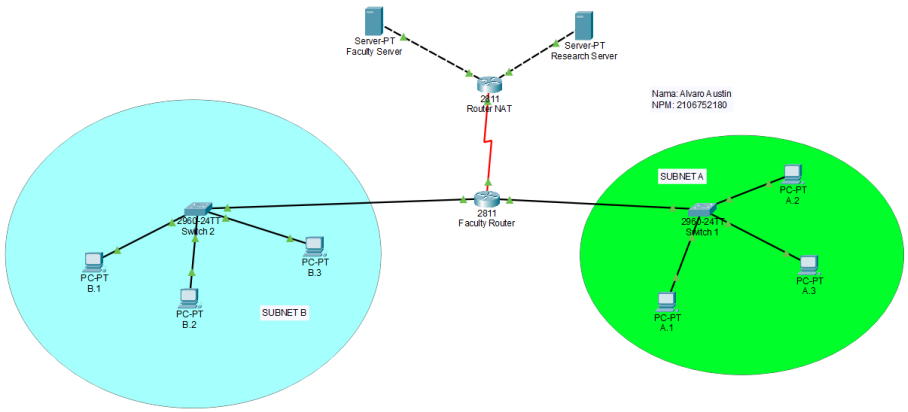
- **A.1 to B.1**



PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec	Periodic	Num	Edit	Delete
	Successful	A.1	B.1	ICMP		0.000	N	0	(edit)	(delete)

- **B.1 to Research Server**

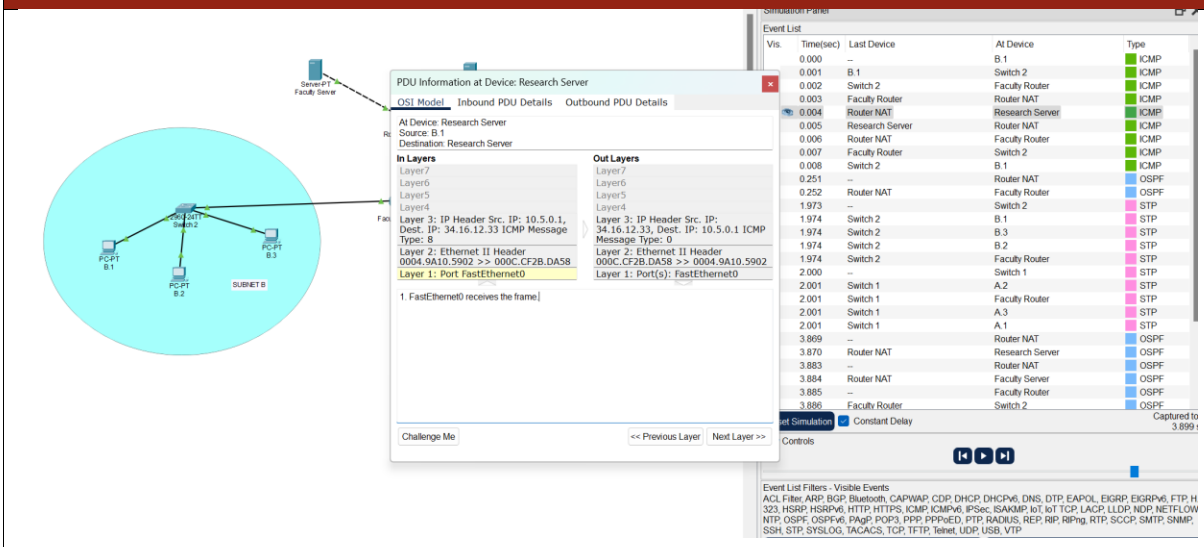


DU List Window

ire	Last Status	Source	Destination	Type	Color	Time(sec	Periodic	Num	Edit	Delete
	Successful	B.1	Research S...	ICMP		0.000	N	0	(edit)	(delete)

OSI Model

OSI Model at Device Research Server



5. [10]Connectivity Test

	A.1	A.2	A.3	B.1	B.2	B.3	Research	Faculty
A.1	✓	✓	✓	✓	✓	✓	✓	✓
A.2	✓	✓	✓	✓	✓	✓	✓	✓
A.3	✓	✓	✓	✓	✓	✓	✓	✓
B.1	✓	✓	✓	✓	✓	✓	✓	✓
B.2	✓	✓	✓	✓	✓	✓	✓	✓
B.3	✓	✓	✓	✓	✓	✓	✓	✓

Research	✓	✓	✓	✓	✓	✓	✓	✓
Faculty	✓	✓	✓	✓	✓	✓	✓	✓

Give ✓if connectivity test is successful **or** ✗if the connectivity test fails. **Or** you may give colors (example: green for success, red for fails).

Proof of Connectivity Test

From A.1 (Row 1):

Fire	Last Status	Source	Destination	Type
	Successful	A.1	A.1	ICMP
	Successful	A.1	A.2	ICMP
	Successful	A.1	A.3	ICMP
	Successful	A.1	B.1	ICMP
	Successful	A.1	B.2	ICMP
	Successful	A.1	B.3	ICMP
	Successful	A.1	Research Server	ICMP
	Successful	A.1	Faculty Server	ICMP

From A.2 (Row 2):

Fire	Last Status	Source	Destination	Type
	Successful	A.2	A.1	ICMP
	Successful	A.2	A.2	ICMP
	Successful	A.2	A.3	ICMP
	Successful	A.2	B.1	ICMP
	Successful	A.2	B.2	ICMP
	Successful	A.2	B.3	ICMP
	Successful	A.2	Research Server	ICMP
	Successful	A.2	Faculty Server	ICMP

From A.3 (Row 3):

Fire	Last Status	Source	Destination	Type
	Successful	A.3	A.1	ICMP
	Successful	A.3	A.2	ICMP
	Successful	A.3	A.3	ICMP
	Successful	A.3	B.1	ICMP
	Successful	A.3	B.2	ICMP
	Successful	A.3	B.3	ICMP
	Successful	A.3	Research Server	ICMP
	Successful	A.3	Faculty Server	ICMP

From B.1 (Row 4):

Fire	Last Status	Source	Destination	Type
	Successful	B.1	A.1	ICMP
	Successful	B.1	A.2	ICMP
	Successful	B.1	A.3	ICMP
	Successful	B.1	B.1	ICMP
	Successful	B.1	B.2	ICMP
	Successful	B.1	B.3	ICMP
	Successful	B.1	Research Server	ICMP
	Successful	B.1	Faculty Server	ICMP

From B.2 (Row 5):

Fire	Last Status	Source	Destination	Type
	Successful	B.2	A.1	ICMP
	Successful	B.2	A.2	ICMP
	Successful	B.2	A.3	ICMP
	Successful	B.2	B.1	ICMP
	Successful	B.2	B.2	ICMP
	Successful	B.2	B.3	ICMP
	Successful	B.2	Research Server	ICMP
	Successful	B.2	Faculty Server	ICMP

From B.3 (Row 6):

Fire	Last Status	Source	Destination	Type
	Successful	B.3	A.1	ICMP
	Successful	B.3	A.2	ICMP
	Successful	B.3	A.3	ICMP
	Successful	B.3	B.1	ICMP
	Successful	B.3	B.2	ICMP
	Successful	B.3	B.3	ICMP
	Successful	B.3	Research Server	ICMP
	Successful	B.3	Faculty Server	ICMP

From Research (Row 7):

Fire	Last Status	Source	Destination	Type
	Successful	Research Server	A.1	ICMP
	Successful	Research Server	A.2	ICMP
	Successful	Research Server	A.3	ICMP
	Successful	Research Server	B.1	ICMP
	Successful	Research Server	B.2	ICMP
	Successful	Research Server	B.3	ICMP
	Successful	Research Server	Research Server	ICMP
	Successful	Research Server	Faculty Server	ICMP

From Faculty (Row 8):

Fire	Last Status	Source	Destination	Type
	Successful	Faculty Server	A.1	ICMP
	Successful	Faculty Server	A.2	ICMP
	Successful	Faculty Server	A.3	ICMP
	Successful	Faculty Server	B.1	ICMP
	Successful	Faculty Server	B.2	ICMP
	Successful	Faculty Server	B.3	ICMP
	Successful	Faculty Server	Research Server	ICMP
	Successful	Faculty Server	Faculty Server	ICMP

6. [10]Analysis

- In the NAT configuration step, the Serial 1/0 is used for "ip nat inside", and not "ip nat outside". What is the reasoning behind the configuration? What will happen if we switch the "inside" and "outside" of the NAT configuration?

Answers:
The command of ip nat Inside and ip nat outside is used to connect an interface to private or public, where private means ip nat inside and public for ip nat outside. In this case, the reason Serial 1/0 interface uses ip nat inside is to convert to a public IP address before being sent to Internet. This is needed to be done because NAT Translation is needed for private IP to be translated to public IP for the sake of communication. In this case, Serial 1/0 is to connect the server with local pcs that uses private IP address. For the sake of it, we have to convert that private IP address to public IP address so it can be used to communicate.

If we switch inside and outside, it could cause communication failure between internal and external network. This happened because the process is reversed. At first we used ip nat inside to convert private IP address from local pcs , but if we change it to outside, then it can't communicate to the Internet.

- Pay attention to the OSI model on the 3rd and 4th part.
  - Are there any differences? Highlight the differences, if any.
  - Explain why there's any/no differences between both OSI models.

Answers:
Yes there are differences.
OSI Model on 3rd part:

OSI Model on 4th part:

1. In Layers:
- 3rd part:
  - ✓ Source IP: 192.168.0.66
  - ✓ Destination IP: 34.16.12.33
- 4th part:
  - ✓ Source IP: 10.5.0.1
  - ✓ Destination IP: 34.16.12.33

2. Out Layers:
- 3rd part:
  - ✓ Source IP: 34.16.12.33
  - ✓ Destination IP: 192.168.0.66
- 4th part:
  - ✓ Source IP: 34.16.12.33
  - ✓ Destination IP: 10.5.0.1

The difference between OSI models is on NAT that translate private IP address to public IP address. It translates the private IP addresses on 4th part source address to public IP address.