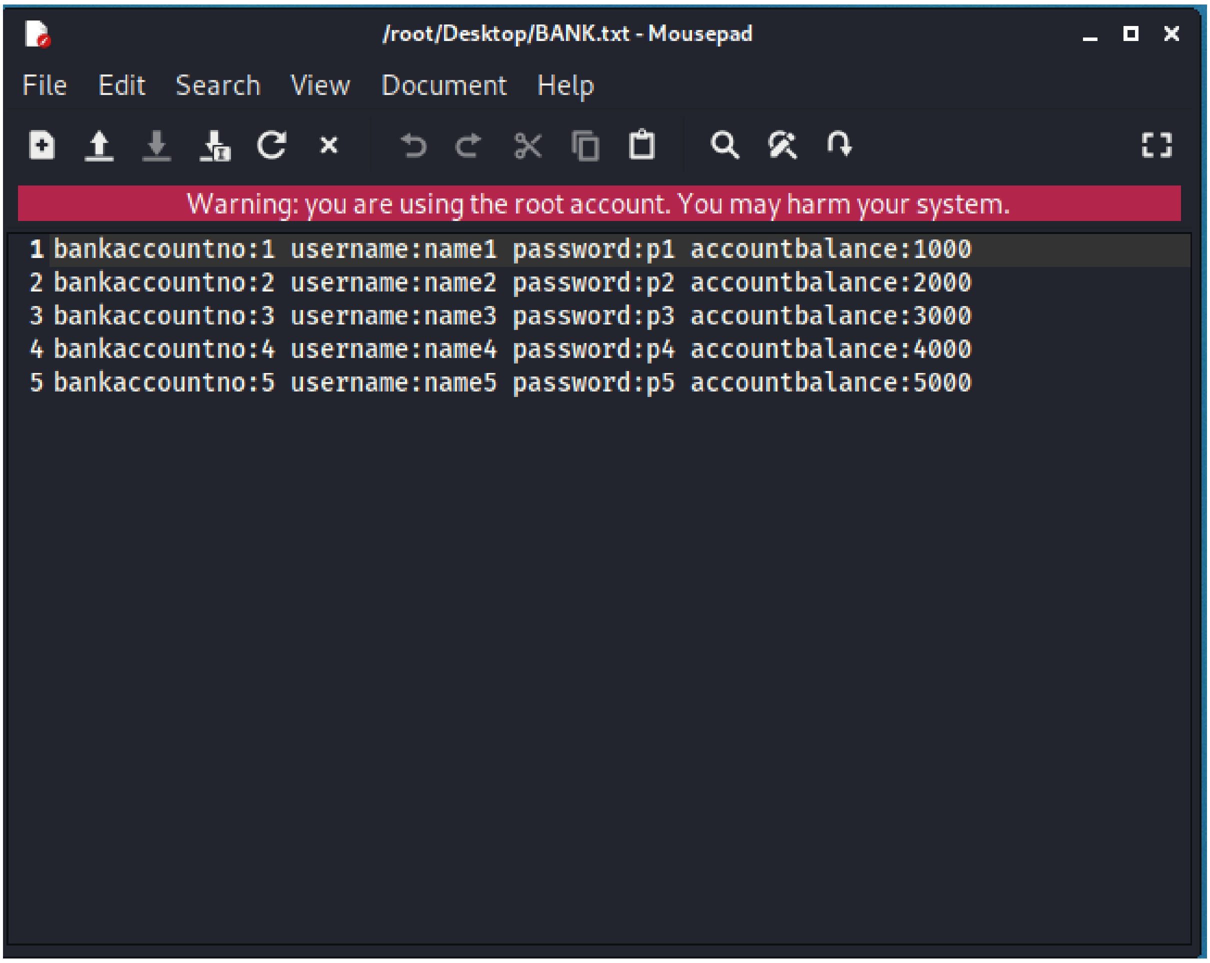
Aryaman Mishra

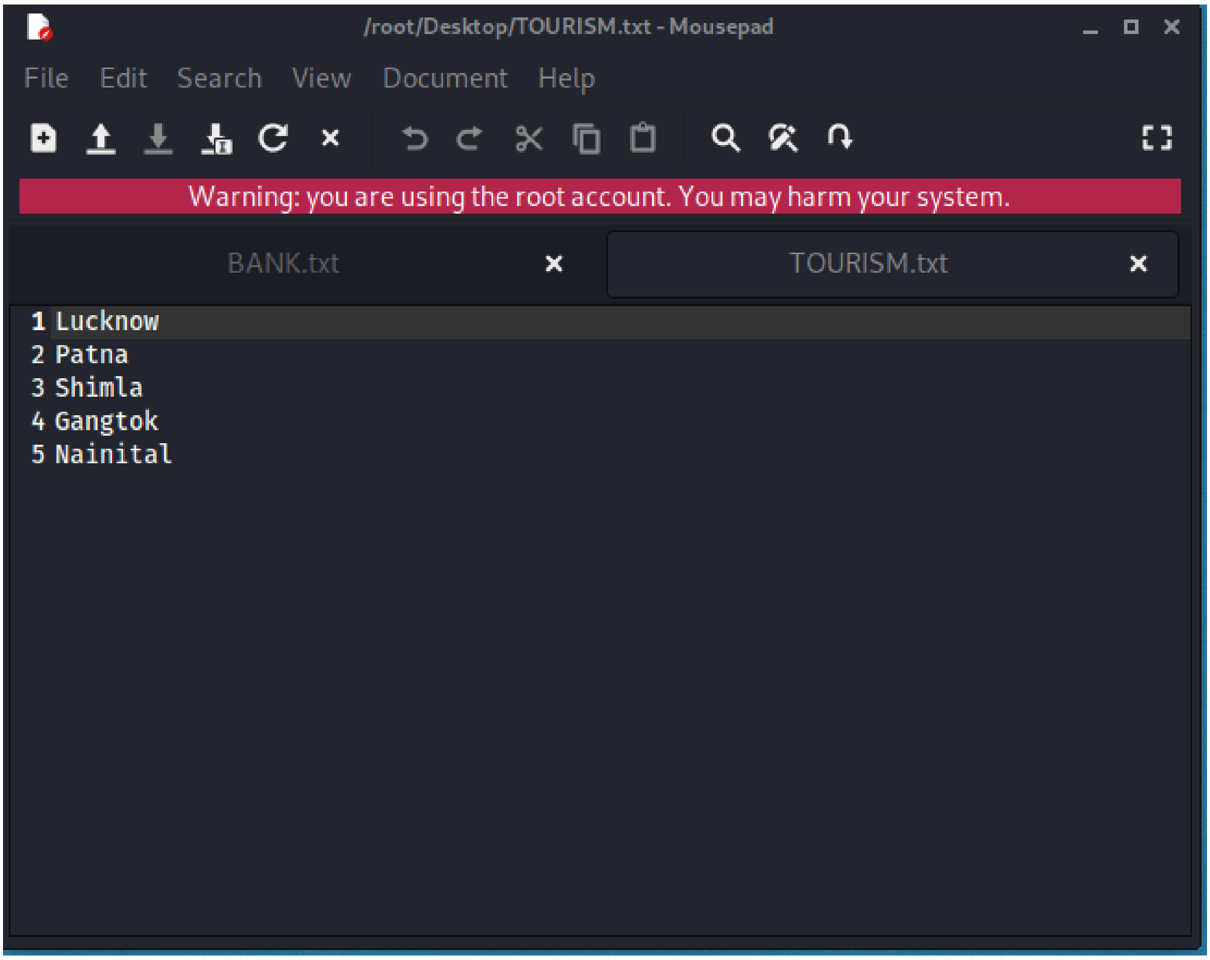
19BCE1027

You have a text file with sensitive information that contains the bank account number, username, and their respective account balance of five customers with their passwords. Demonstrate how you can hide and retrieve this sensitive text file in another text file which is containing the tourism destinations in the North India. Encrypt the file before hiding. {Note that the name of the sensitive text file is: BANK and another text file is: TOURISM}



Warning: you are using the root account. You may harm your system.

```
bankaccountno:1 username:name1 password:p1 accountbalance:1000
bankaccountno:2 username:name2 password:p2 accountbalance:2000
bankaccountno:3 username:name3 password:p3 accountbalance:3000
bankaccountno:4 username:name4 password:p4 accountbalance:4000
bankaccountno:5 username:name5 password:p5 accountbalance:5000
```



Warning: you are using the root account. You may harm your system.

```
Lucknow
Patna
Shimla
Gangtok
Nainital
```

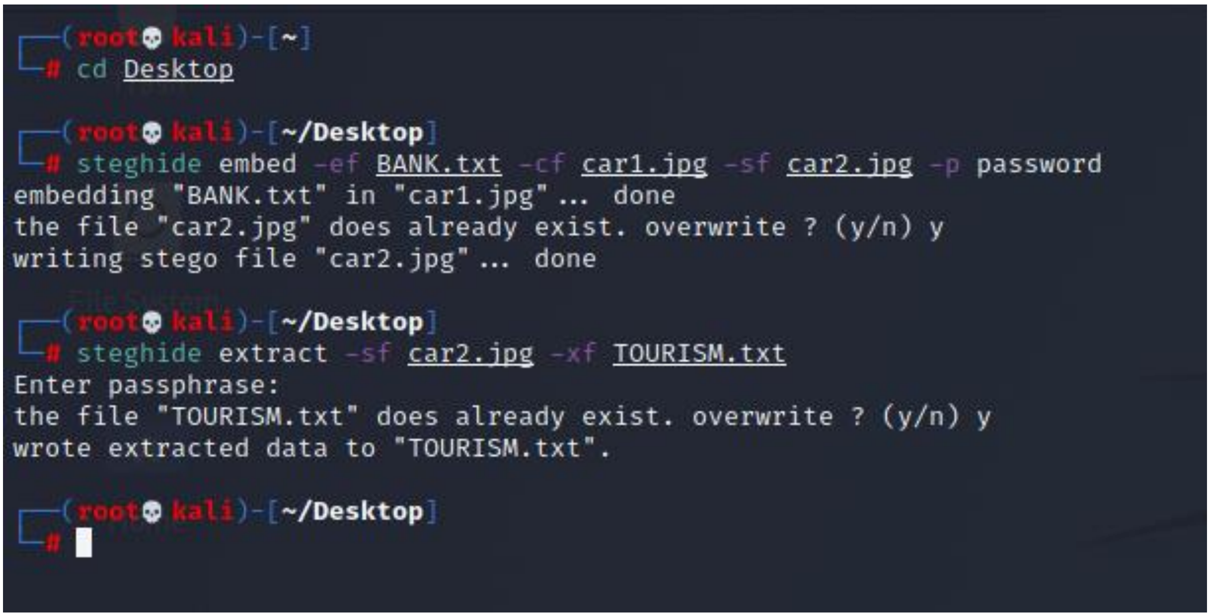
Embedding data in the image: We hide the data in the image using the Steghide so that only the person who accepts it can read it. Therefore, we created a text file named “TOURISM.txt”, in which we wrote our confidential data and images. JPEG is the file in which we are embedding our data.

Here, ef and cf are termed as embedded files and cover files, respectively. Let’s see what this command is doing: Steghide – Program Name Embed – this is the command -cf – This flag is for the cover file (the file used to embed the data) filename – this is the name of the cover file -ef – This flag is for the embed file (the file that will be embedded) Filename – This is the name of the embedded file Extraction of Data From Image Via Steghide: Using Steghide adds an extra layer of security by allowing us to use a password for it. As long as you know the passphrase, it is quite easy to extract data from the image.

Password Protect Files: Now, we can also extract files using the following command. This command is different in that it specifies a password in the command itself, therefore, we do not need to specify it separately.

Retrieve Information of Embedded File: If we have an image in which the data is suspected to be hidden and if so, what algorithm is used to encrypt the data in the file

Commands:

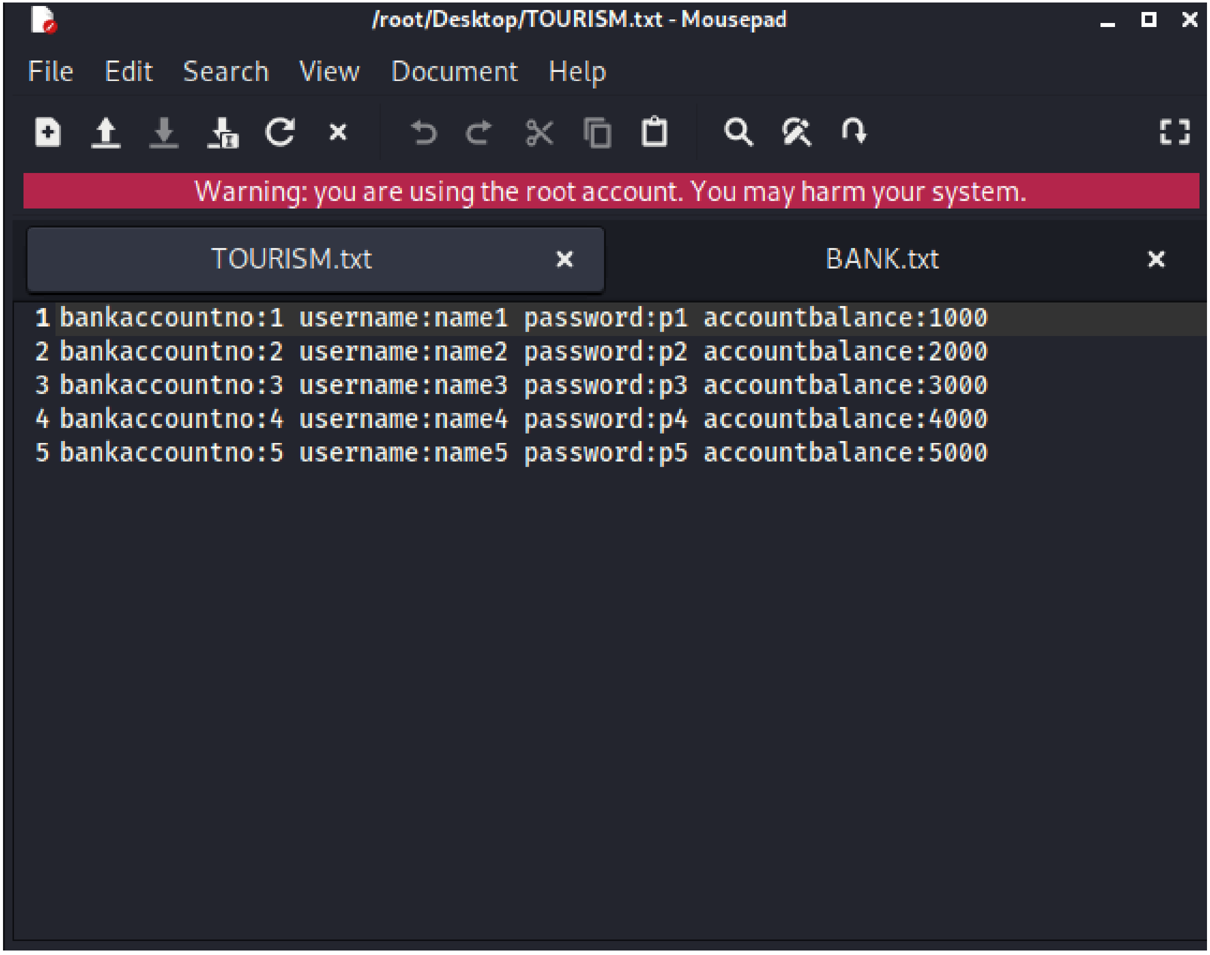


```
┌──(root💀kali)-[~]
└─# cd Desktop

┌──(root💀kali)-[~/Desktop]
└─# steghide embed -ef BANK.txt -cf car1.jpg -sf car2.jpg -p password
embedding "BANK.txt" in "car1.jpg"... done
the file "car2.jpg" does already exist. overwrite ? (y/n) y
writing stego file "car2.jpg"... done

┌──(root💀kali)-[~/Desktop]
└─# steghide extract -sf car2.jpg -xf TOURISM.txt
Enter passphrase:
the file "TOURISM.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "TOURISM.txt".

┌──(root💀kali)-[~/Desktop]
└─# 
```



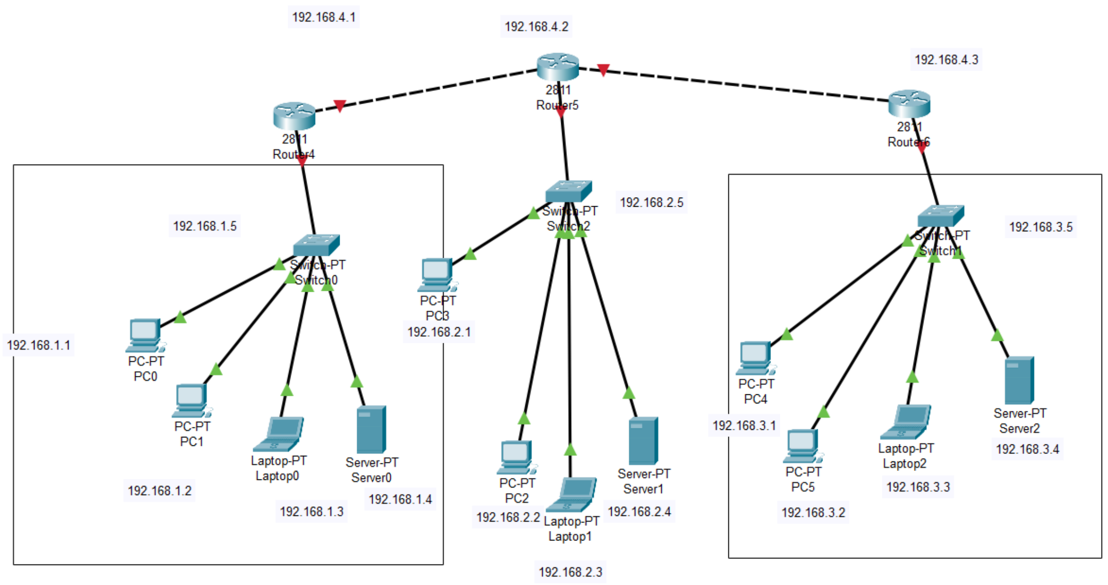
Warning: you are using the root account. You may harm your system.

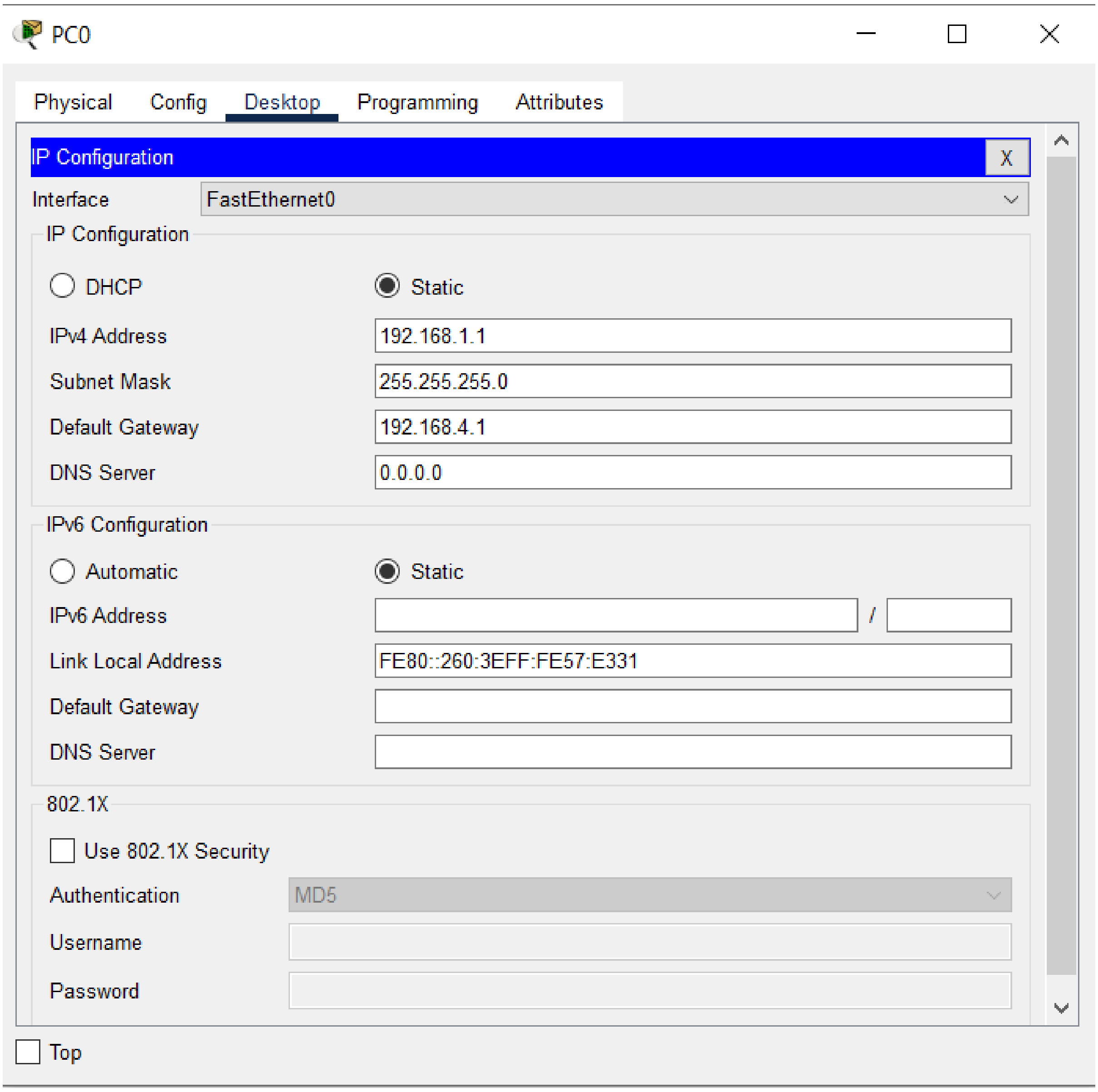
```
bankaccountno:1 username:name1 password:p1 accountbalance:1000
bankaccountno:2 username:name2 password:p2 accountbalance:2000
bankaccountno:3 username:name3 password:p3 accountbalance:3000
bankaccountno:4 username:name4 password:p4 accountbalance:4000
bankaccountno:5 username:name5 password:p5 accountbalance:5000
```

Create a network topology consisting of three subnets in which each subnet consists of two PCs, one Laptop and two servers.

i. Complete the basic routing procedure to establish a proper communication among each end devices

ii. Establish a VPN for any two subnets that you have developed.





Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.4.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::260:3EFF:FE57:E331

Default Gateway:

DNS Server:

802.1X

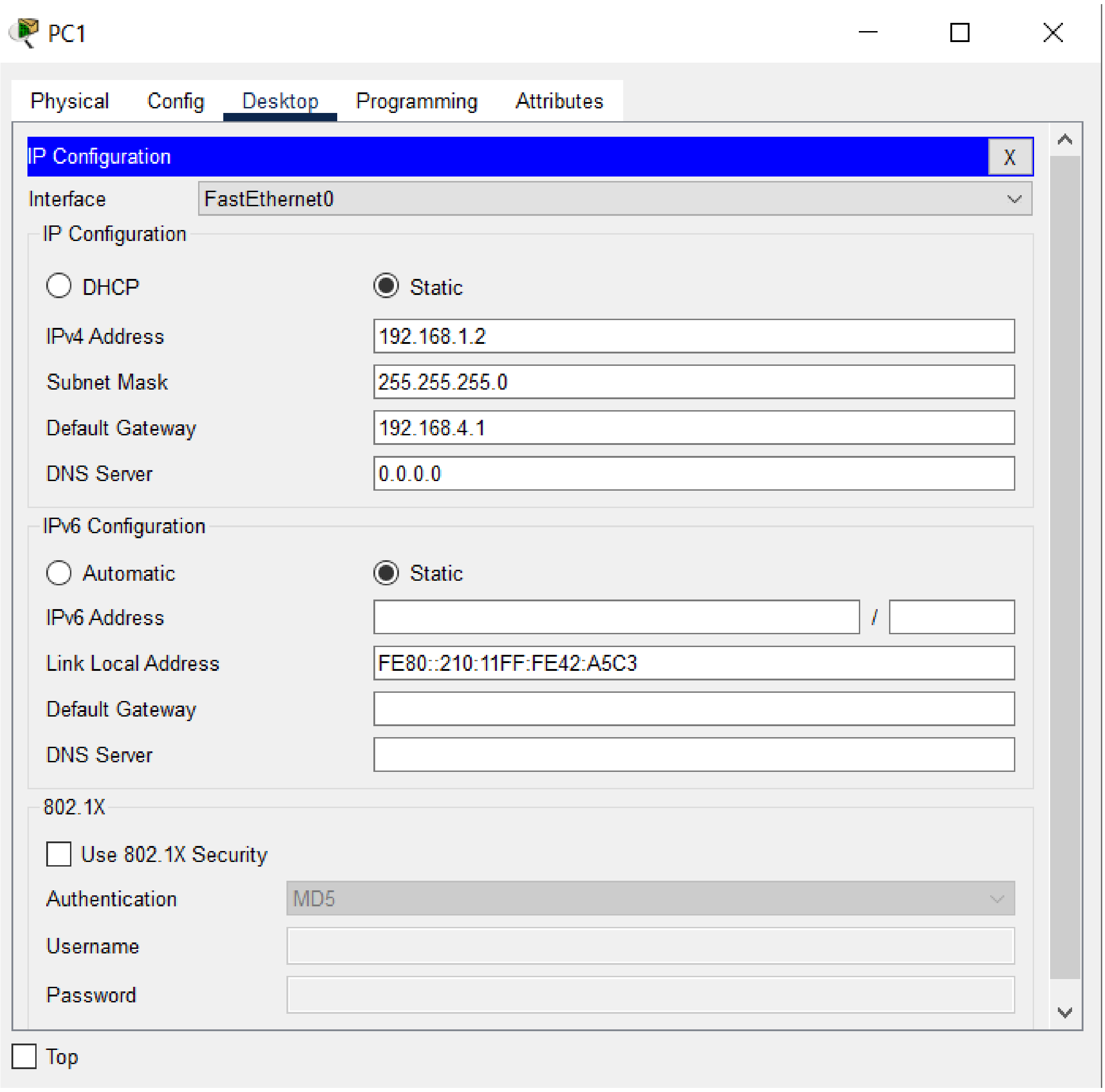
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

□ Top



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.4.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::210:11FF:FE42:A5C3

Default Gateway:

DNS Server:

802.1X

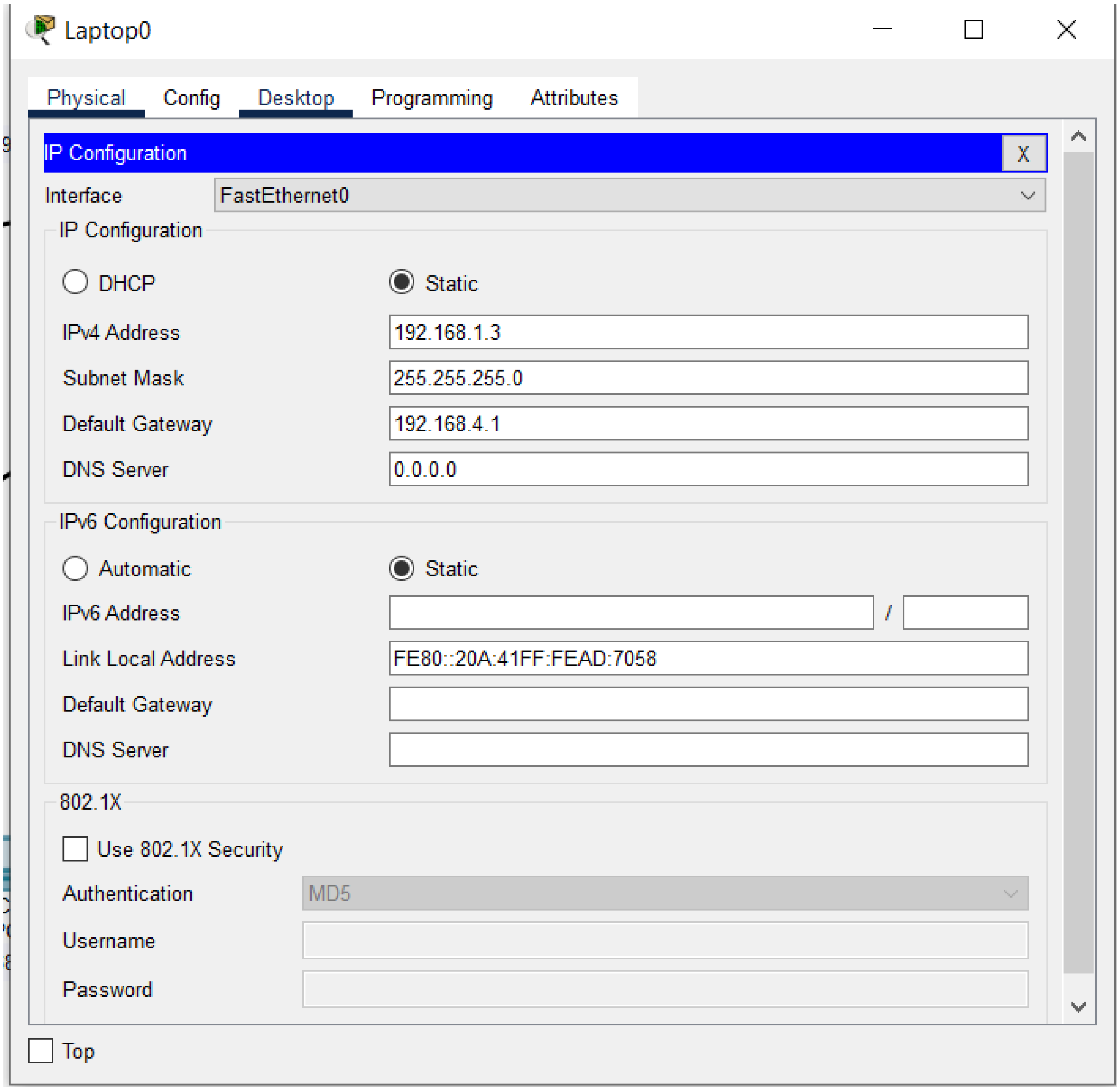
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

□ Top



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.4.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::20A:41FF:FEAD:7058

Default Gateway:

DNS Server:

802.1X

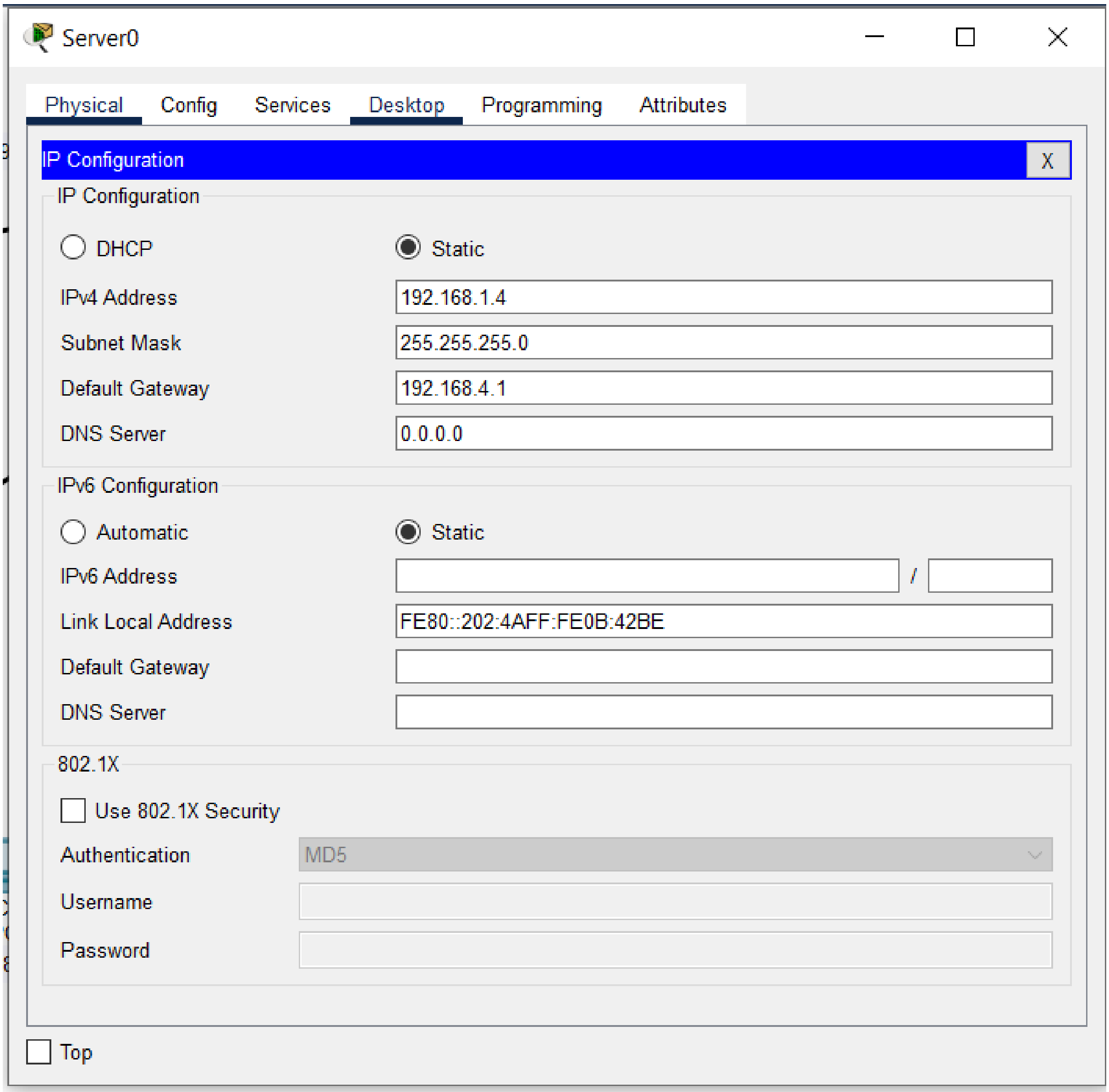
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

□ Top



IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.4

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.4.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::202:4AFF:FE0B:42BE

Default Gateway:

DNS Server:

802.1X

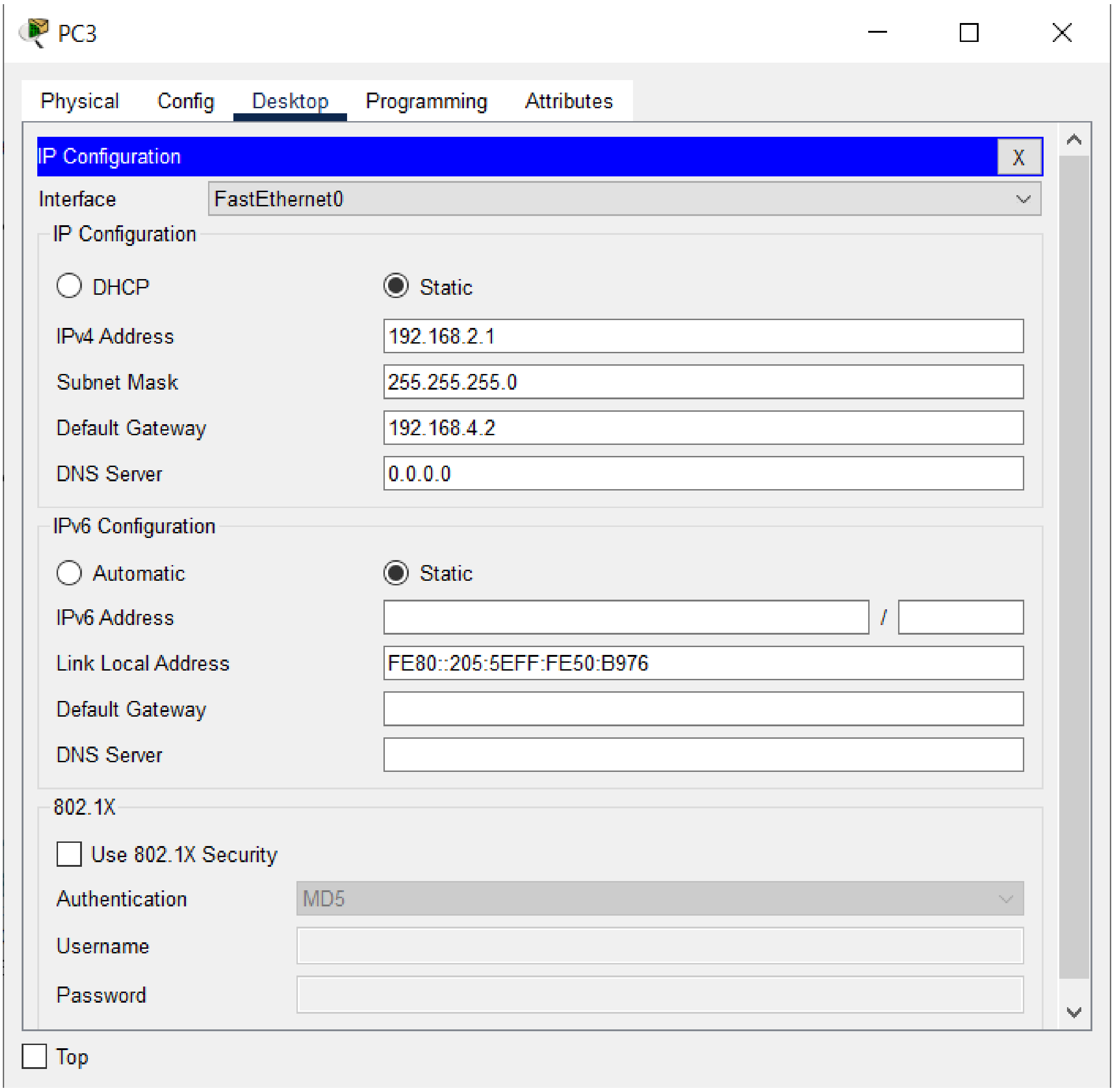
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

□ Top



Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.4.2
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

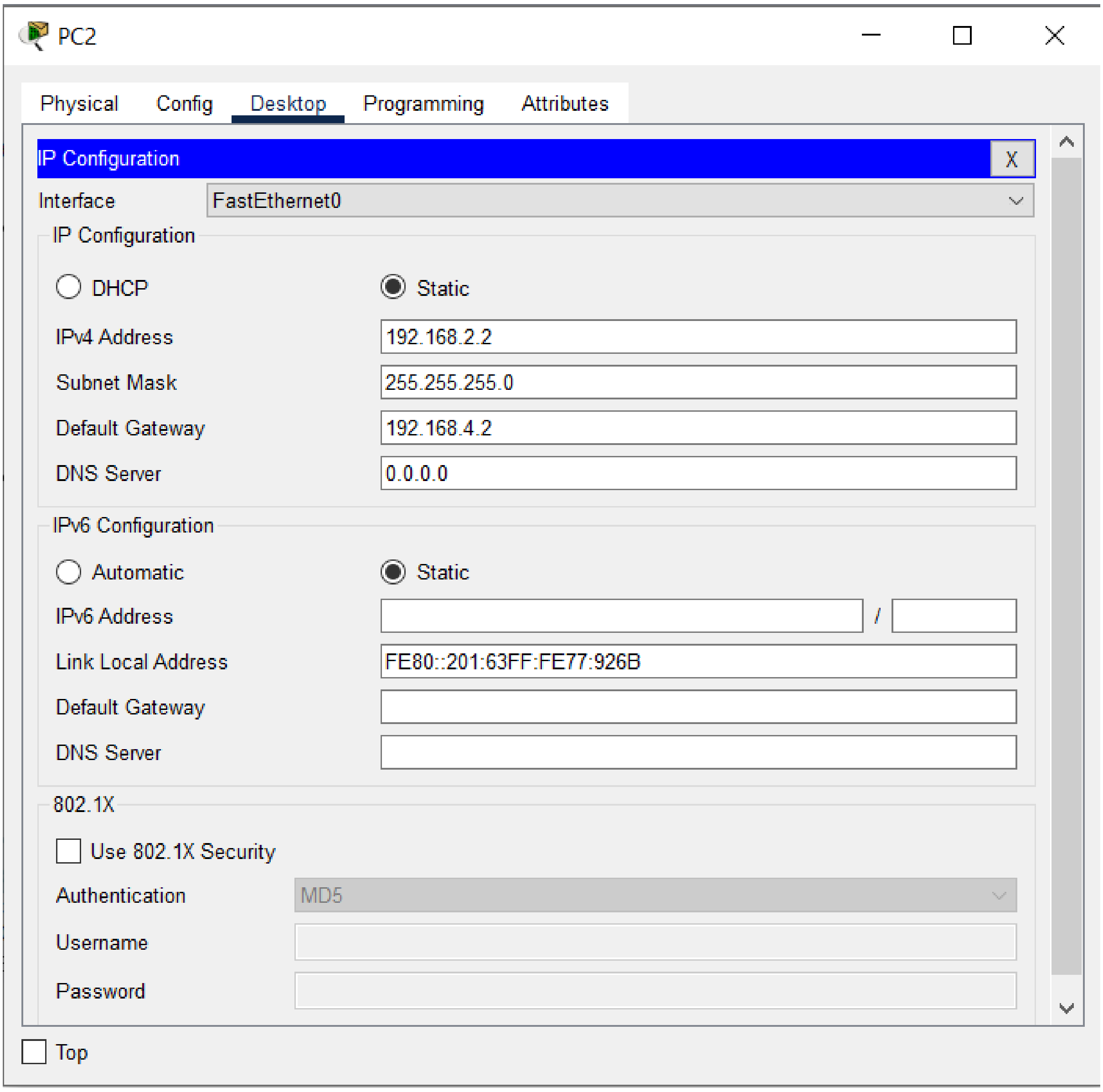
IPv6 Address	/
Link Local Address	FE80::205:5EFF:FE50:B976
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

□ Top



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.4.2

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::201:63FF:FE77:926B

Default Gateway:

DNS Server:

802.1X

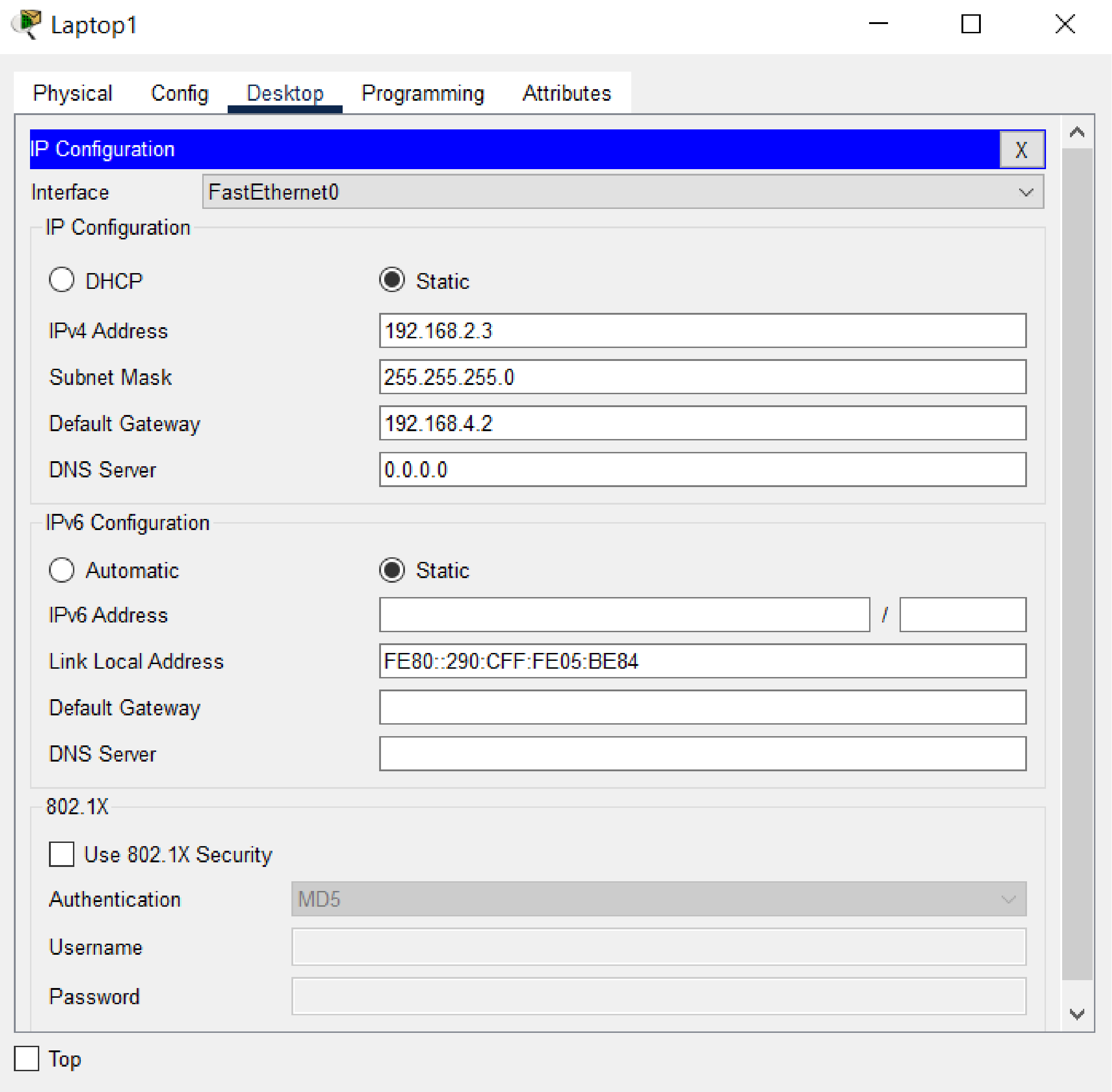
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

□ Top



Laptop1

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.2.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.4.2

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::290:CFF:FE05:BE84

Default Gateway:

DNS Server:

802.1X

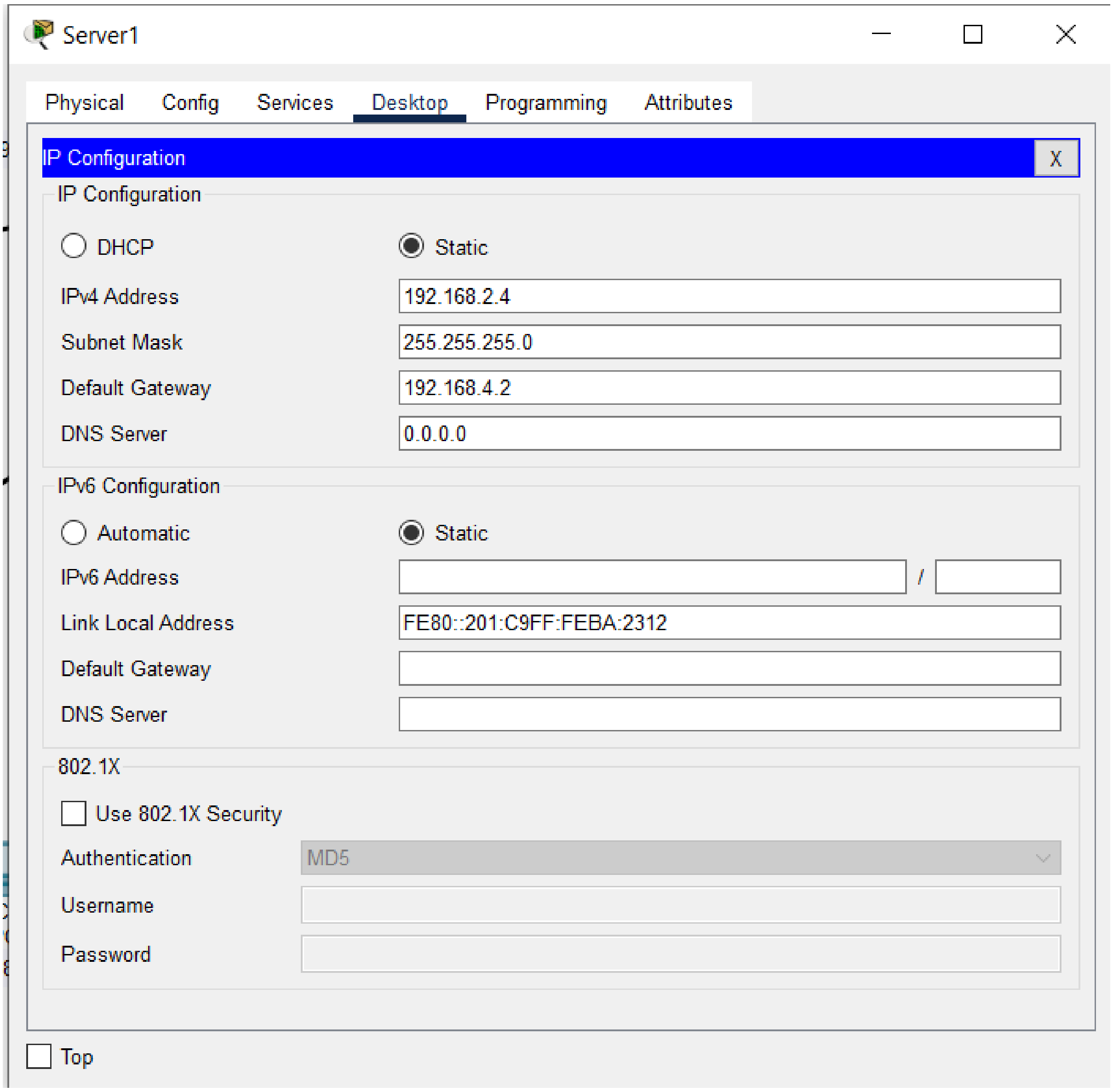
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

□ Top



IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.2.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.4.2
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

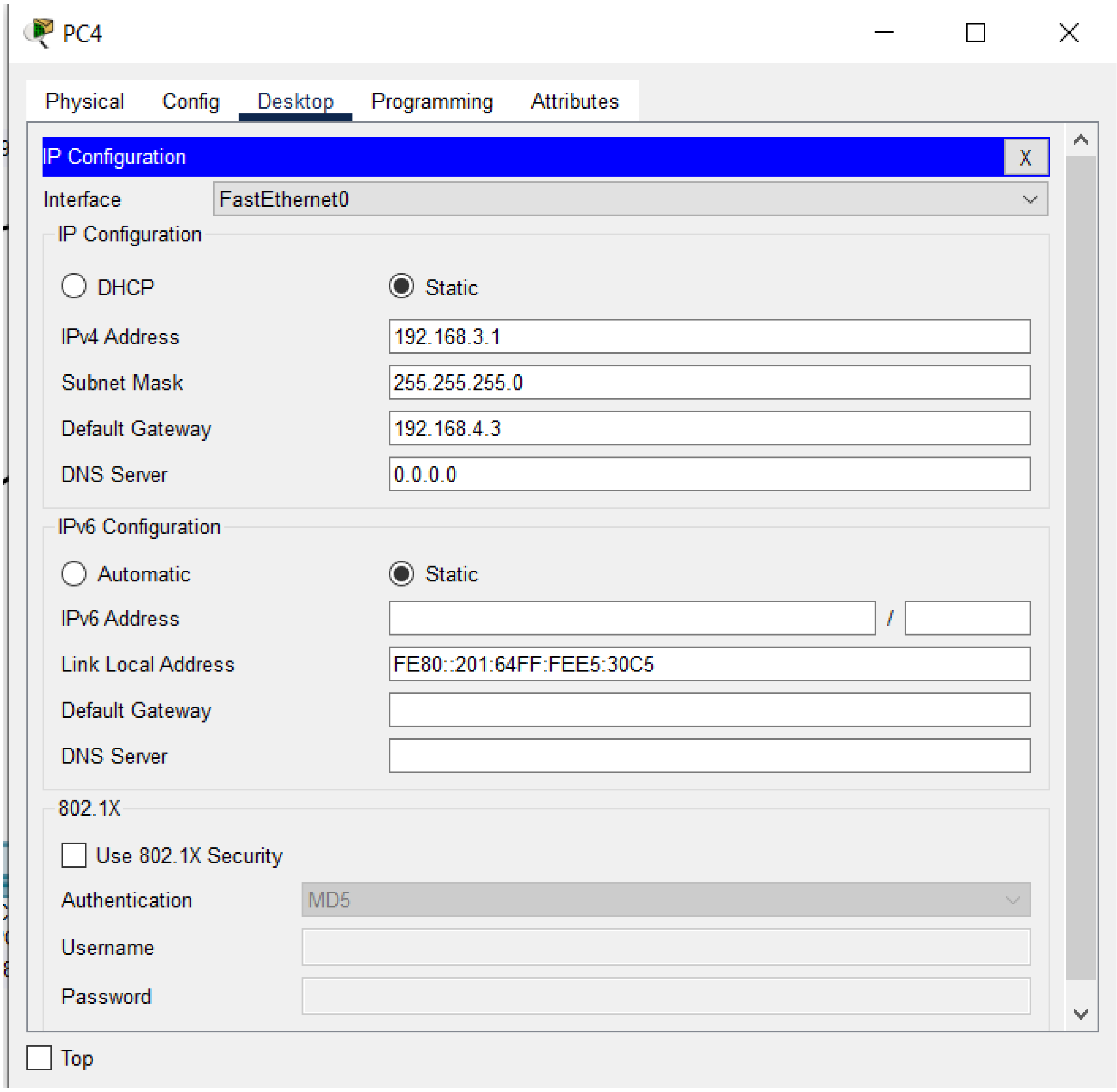
IPv6 Address	/
Link Local Address	FE80::201:C9FF:FEBA:2312
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

□ Top



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.3.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.4.3
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

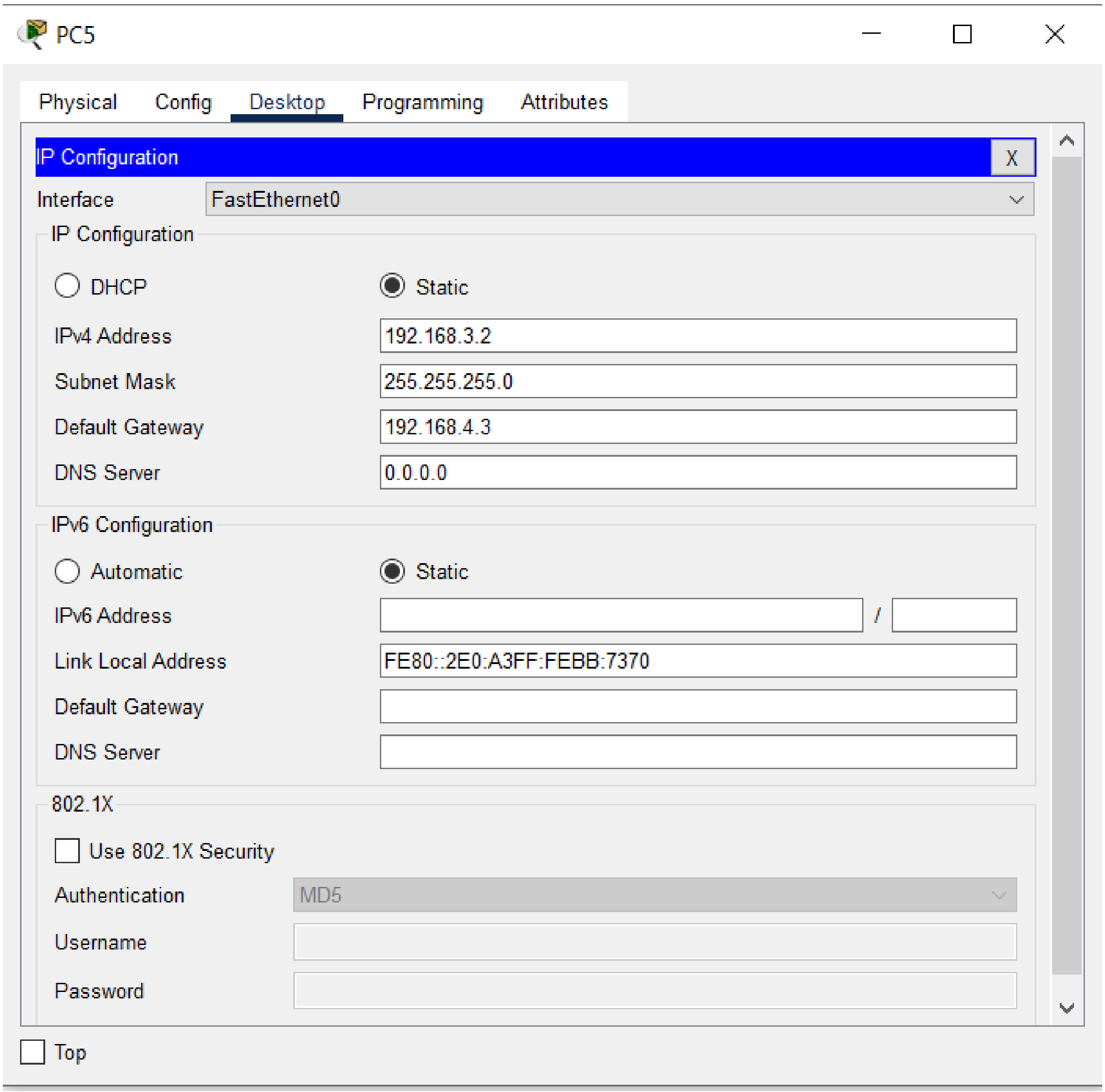
IPv6 Address	/
Link Local Address	FE80::201:64FF:FEE5:30C5
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

□ Top



Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.3.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.4.3

DNS Server 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::2E0:A3FF:FEBB:7370

Default Gateway

DNS Server

802.1X

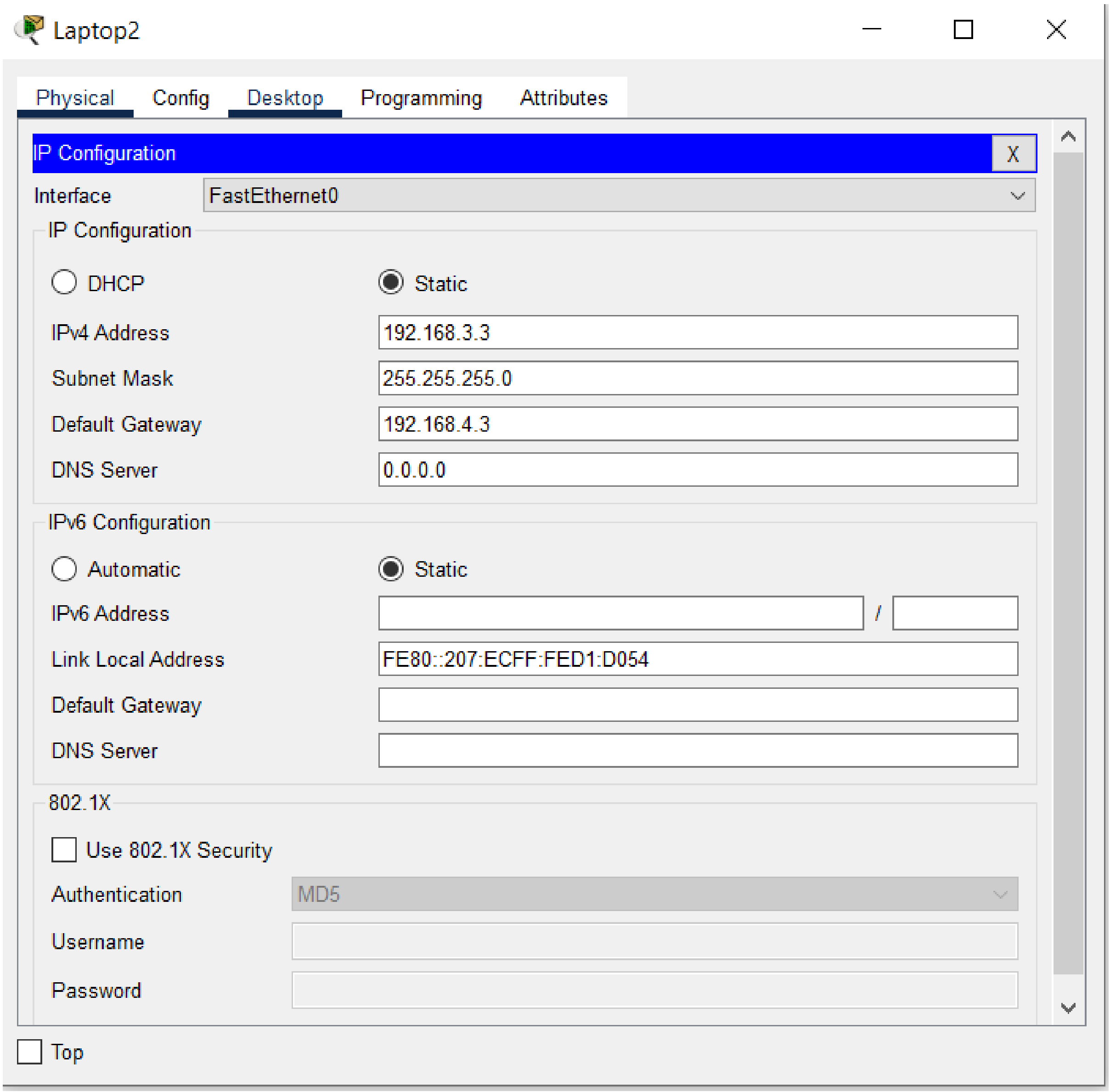
□ Use 802.1X Security

Authentication MD5

Username

Password

□ Top



Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.3.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.4.3
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

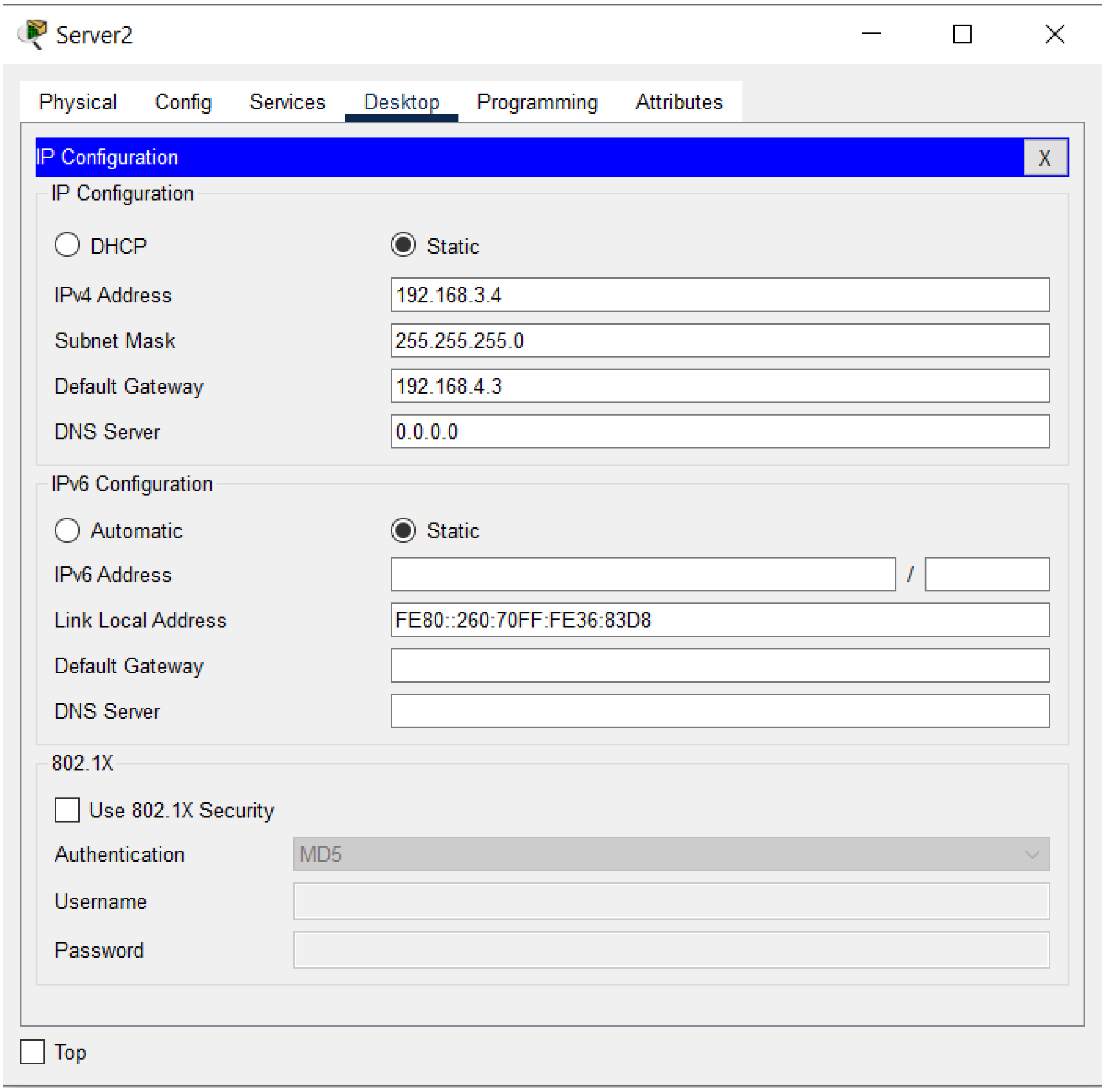
IPv6 Address	/
Link Local Address	FE80::207:ECFF:FED1:D054
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

□ Top



Server2

IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.3.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.4.3
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::260:70FF:FE36:83D8
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

□ Top

1. Starting configurations for R1, ISP, and R3. Paste to global config mode :

```
hostname R1
interface g0/1
ip address 192.168.1.1 255.255.255.0
no shut
interface g0/0
ip address 209.165.100.1 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 209.165.100.2
```

```
hostname ISP
interface g0/1
ip address 209.165.200.2 255.255.255.0
no shut
interface g0/0
ip address 209.165.100.2 255.255.255.0
no shut
exit

hostname R3
interface g0/1
ip address 192.168.3.1 255.255.255.0
no shut
interface g0/0
ip address 209.165.200.1 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 209.165.200.2
```

2. Make sure routers have the security license enabled:

```
show version
license boot module c1900 technology-package securityk9
copy run start
reload
```

3. Configure IPsec on the routers at each end of the tunnel (R1 and R3)

```
!R1
crypto isakmp policy 10
encryption aes 256
authentication pre-share
```

```
group 5
!
crypto isakmp key secretkey address 209.165.200.1
!
crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac
!
crypto map IPSEC-MAP 10 ipsec-isakmp
set peer 209.165.200.1
set pfs group5
set security-association lifetime seconds 86400
set transform-set R1-R3
match address 100
!
interface GigabitEthernet0/0
crypto map IPSEC-MAP
!
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

!R3
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
!
crypto isakmp key secretkey address 209.165.100.1
!
crypto ipsec transform-set R3-R1 esp-aes 256 esp-sha-hmac
!
crypto map IPSEC-MAP 10 ipsec-isakmp
set peer 209.165.100.1
set pfs group5
```

set security-association lifetime seconds 86400

set transform-set R3-R1

match address 100

!

interface GigabitEthernet0/0

crypto map IPSEC-MAP

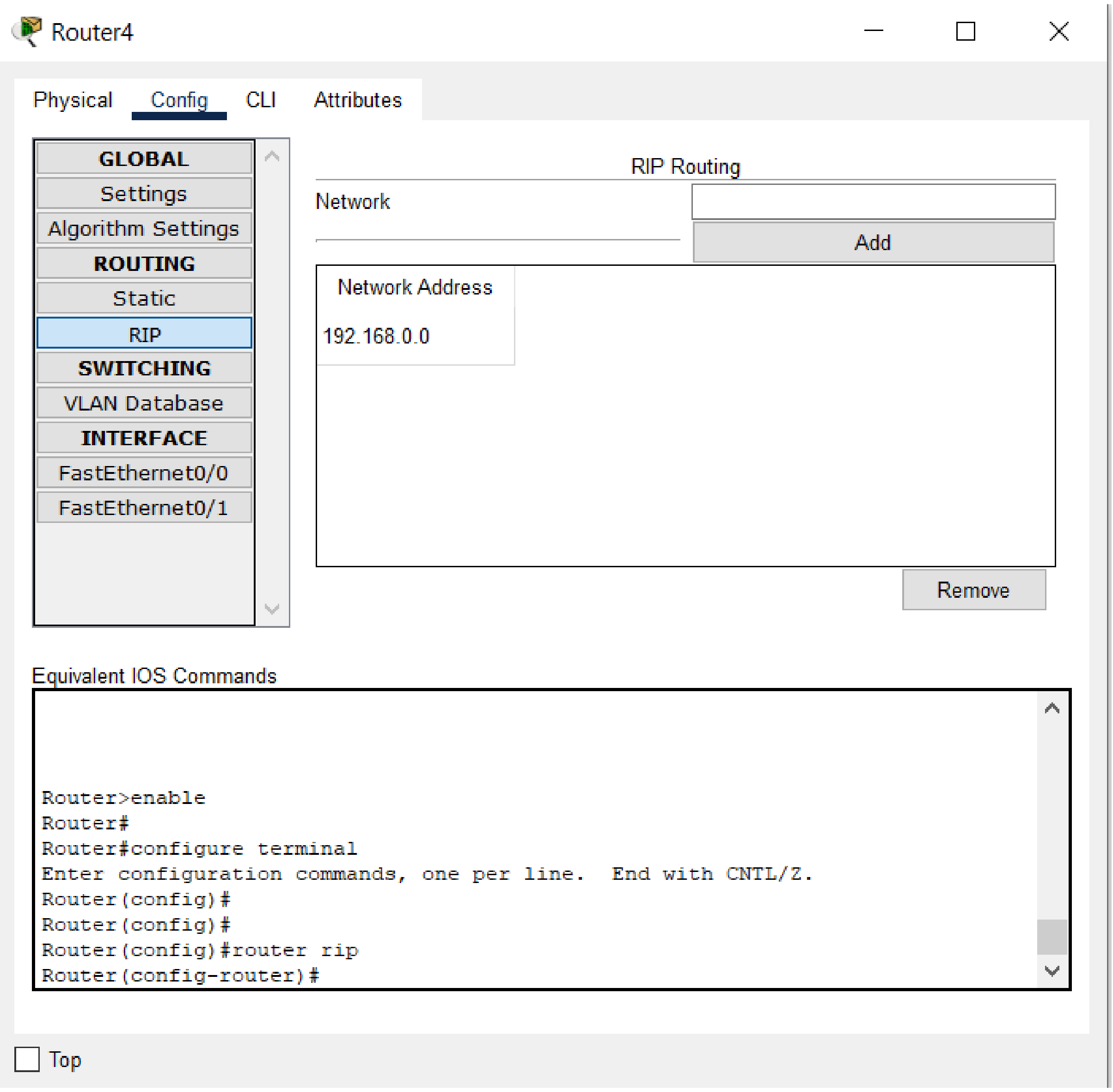
!

R3

access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

R1

access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255



RIP Routing

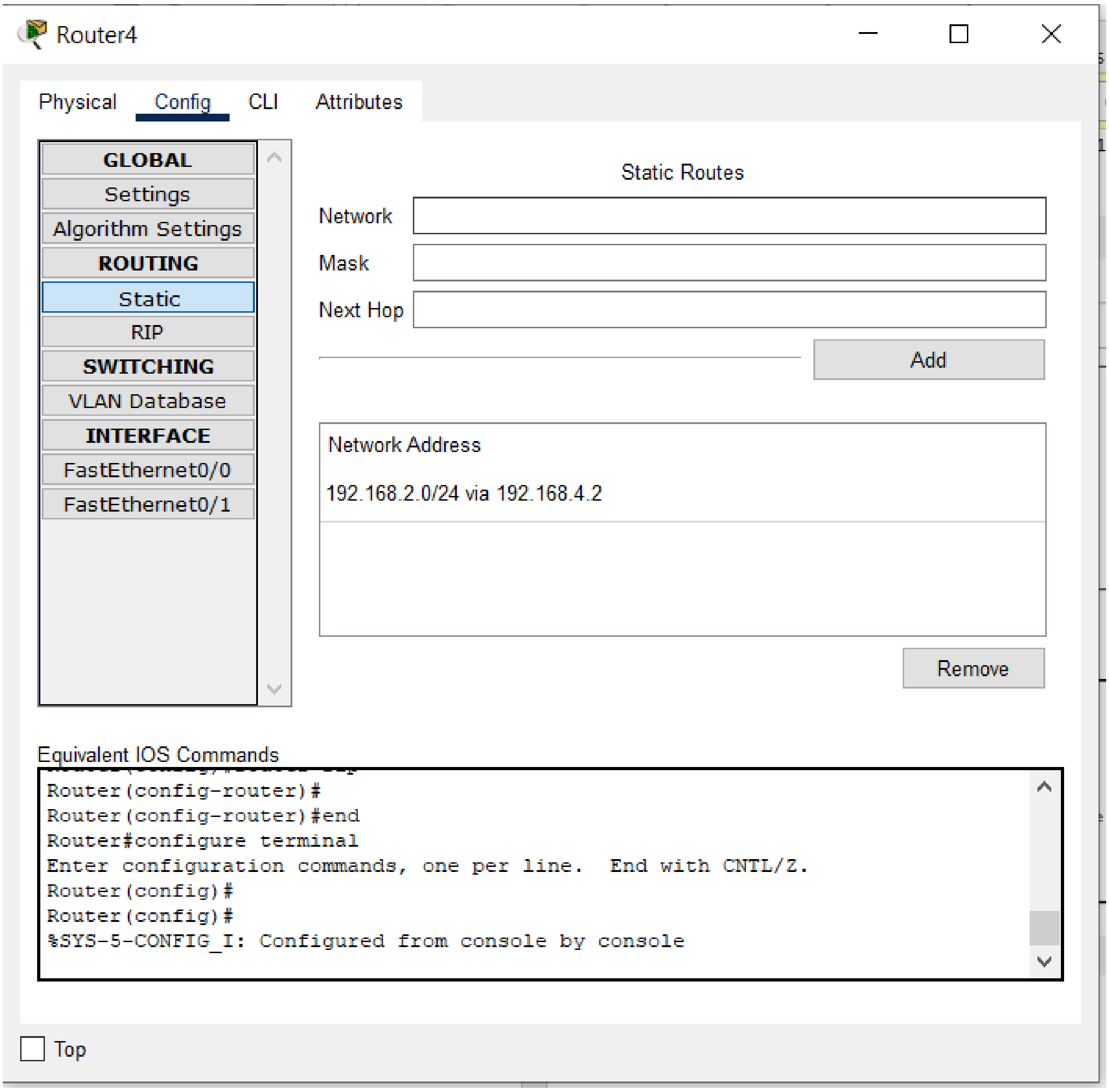
Network

Network Address

192.168.0.0

Equivalent IOS Commands

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#router rip
Router(config-router)#
```



Static Routes

Network

Mask

Next Hop

Network Address

192.168.2.0/24 via 192.168.4.2

Equivalent IOS Commands

```
Router(config)#router rip
Router(config-router)#
Router(config-router)#end
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
%SYS-5-CONFIG_I: Configured from console by console
```