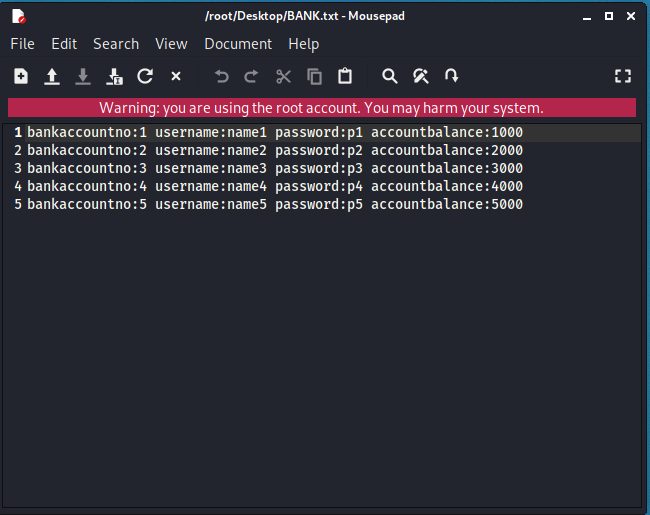
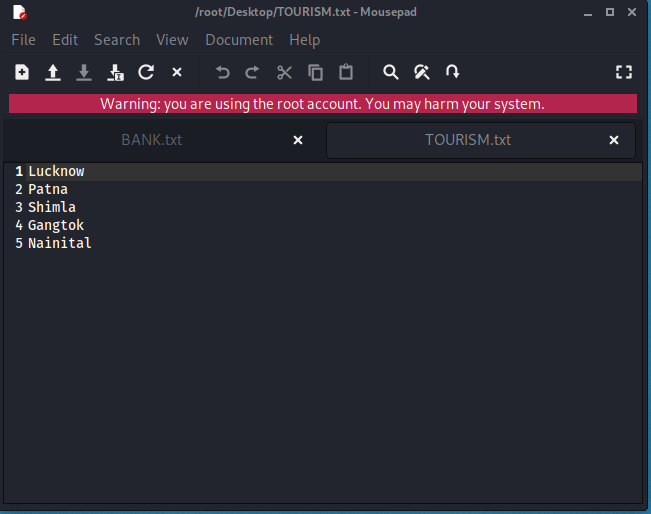
Aryaman Mishra

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}





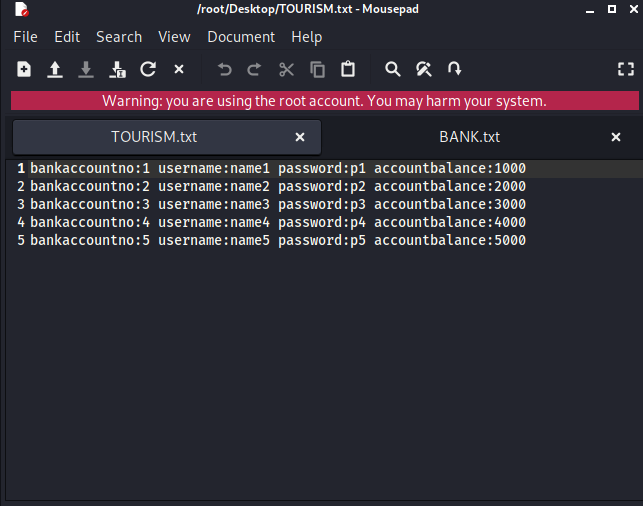
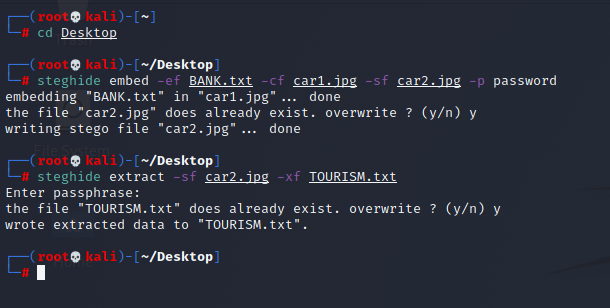
Embedding data in the image: We hide the data in the image using the Steghide so that only the person who accepts it can read it. Therefore, we created a text file named “TOURISM.txt”, in which we wrote our confidential data and images. JPEG is the file in which we are embedding our data.

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

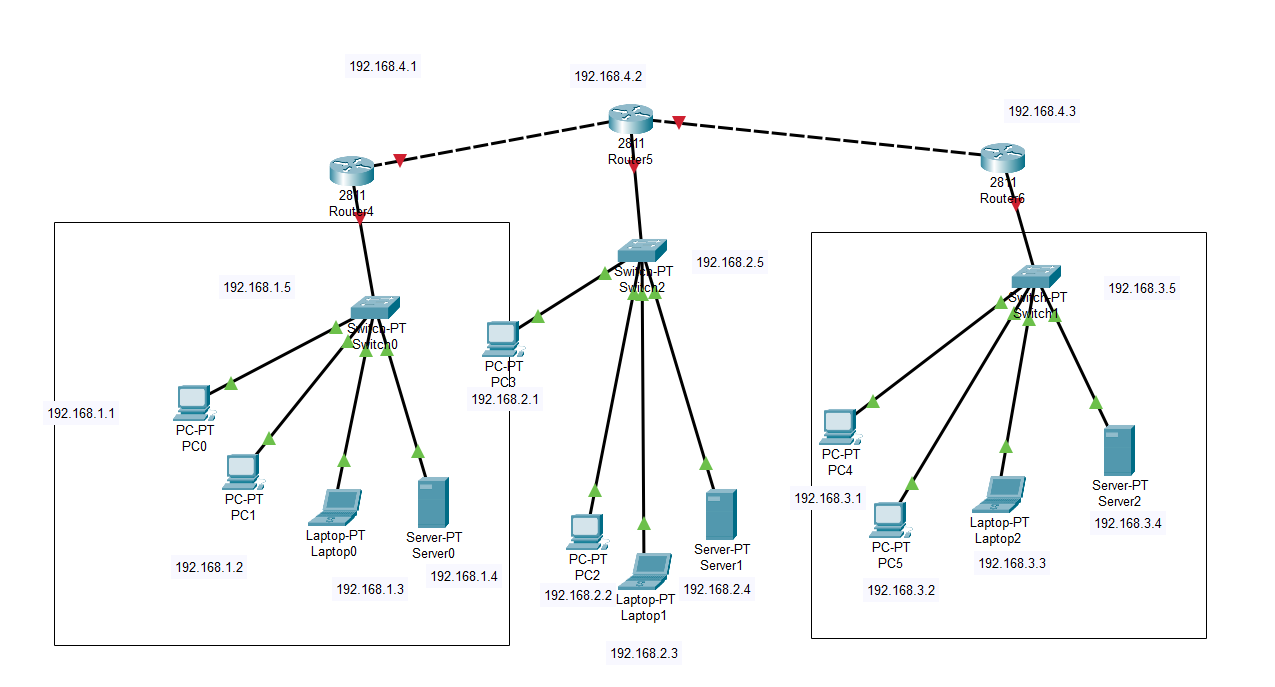
Commands:

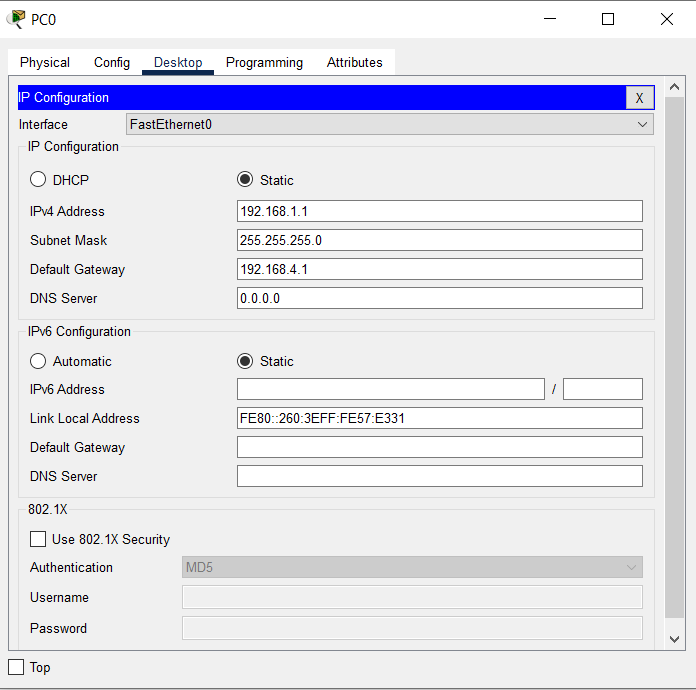
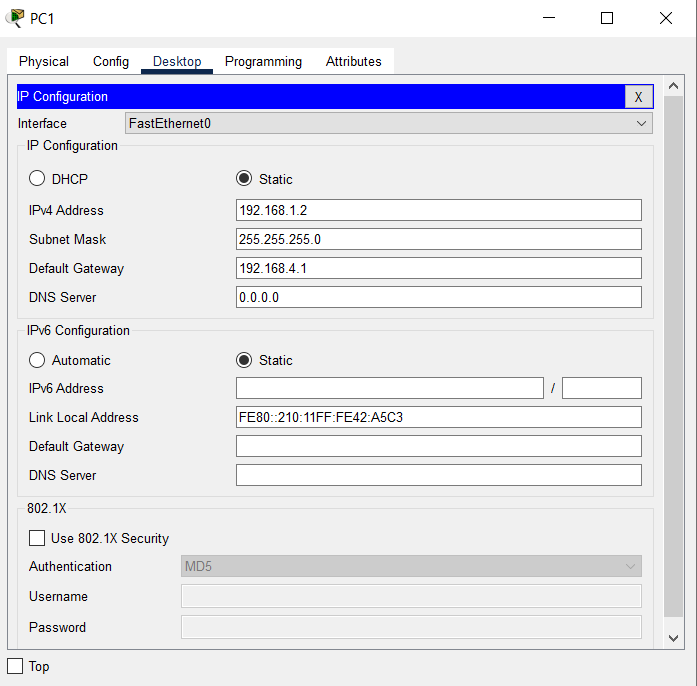
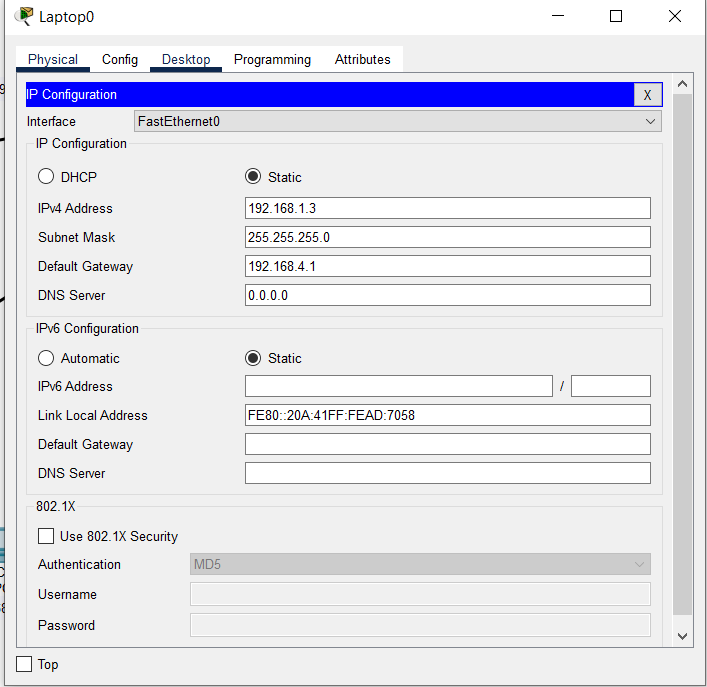
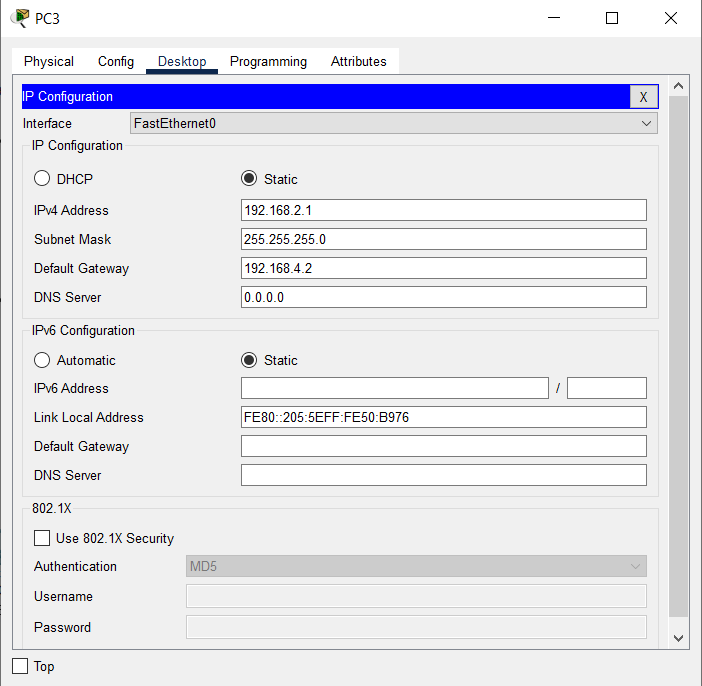
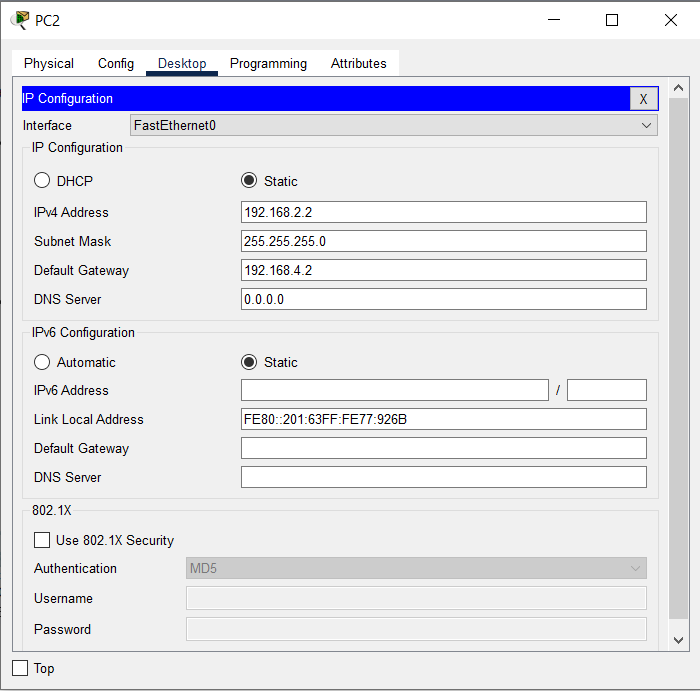
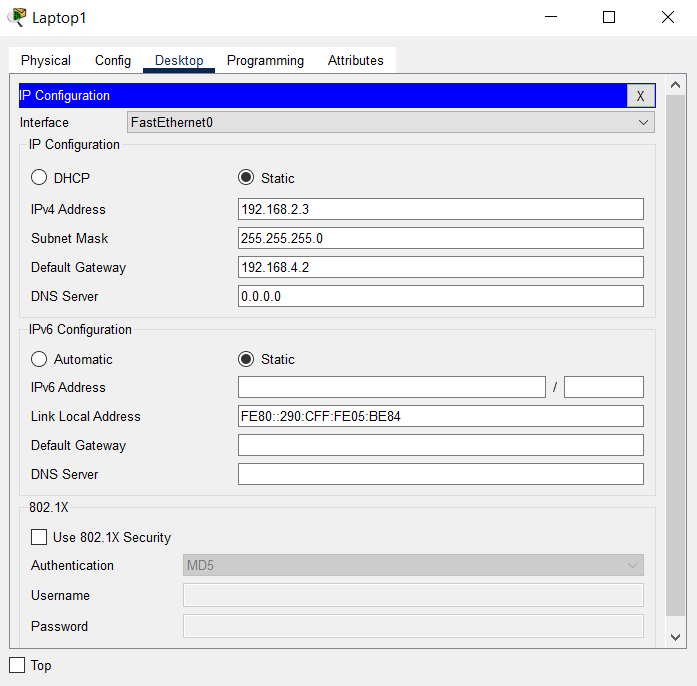
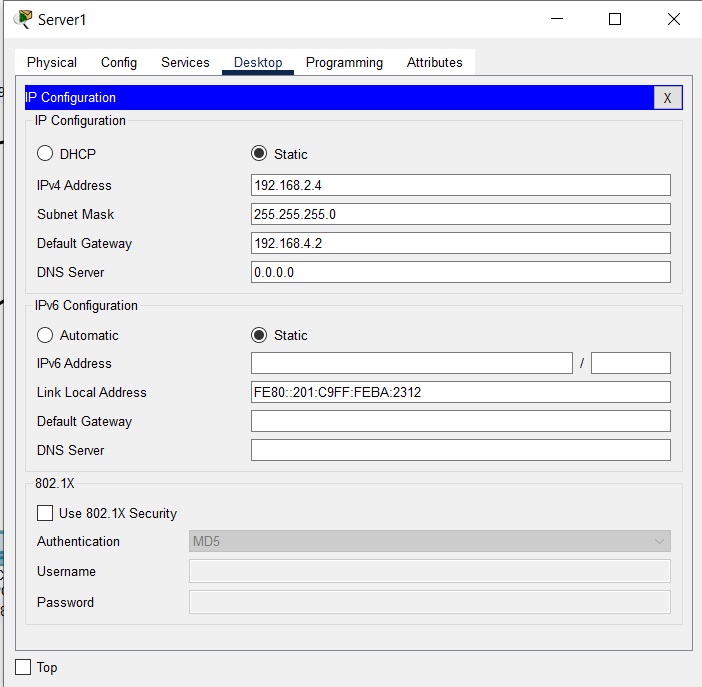
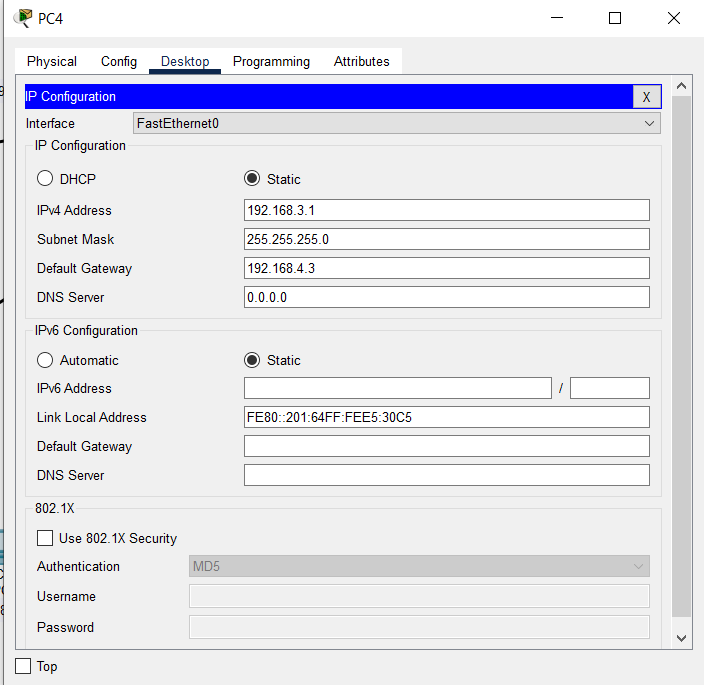
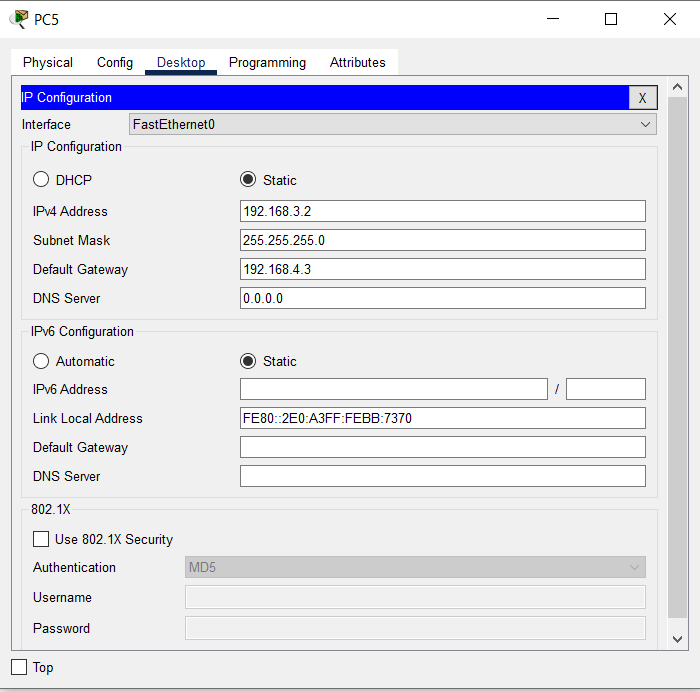
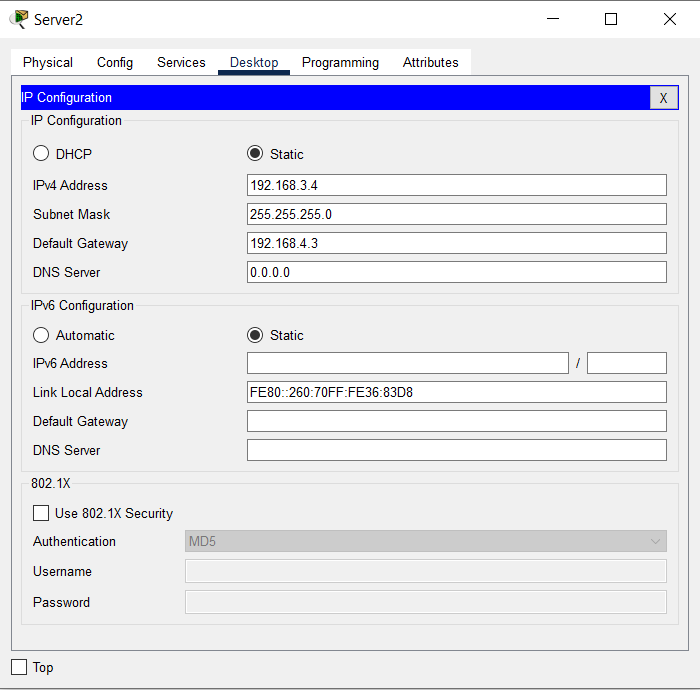


Create a network topology consisting of three subnets in which each subnet consists of two PCs, one Laptop and two servers.

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.



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

