ENSA (Version 7.00) Final PT Skills Assessment Exam (PTSA) Answers

itexamanswers.net/ensa-version-7-00-final-pt-skills-assessment-exam-ptsa-answers.html

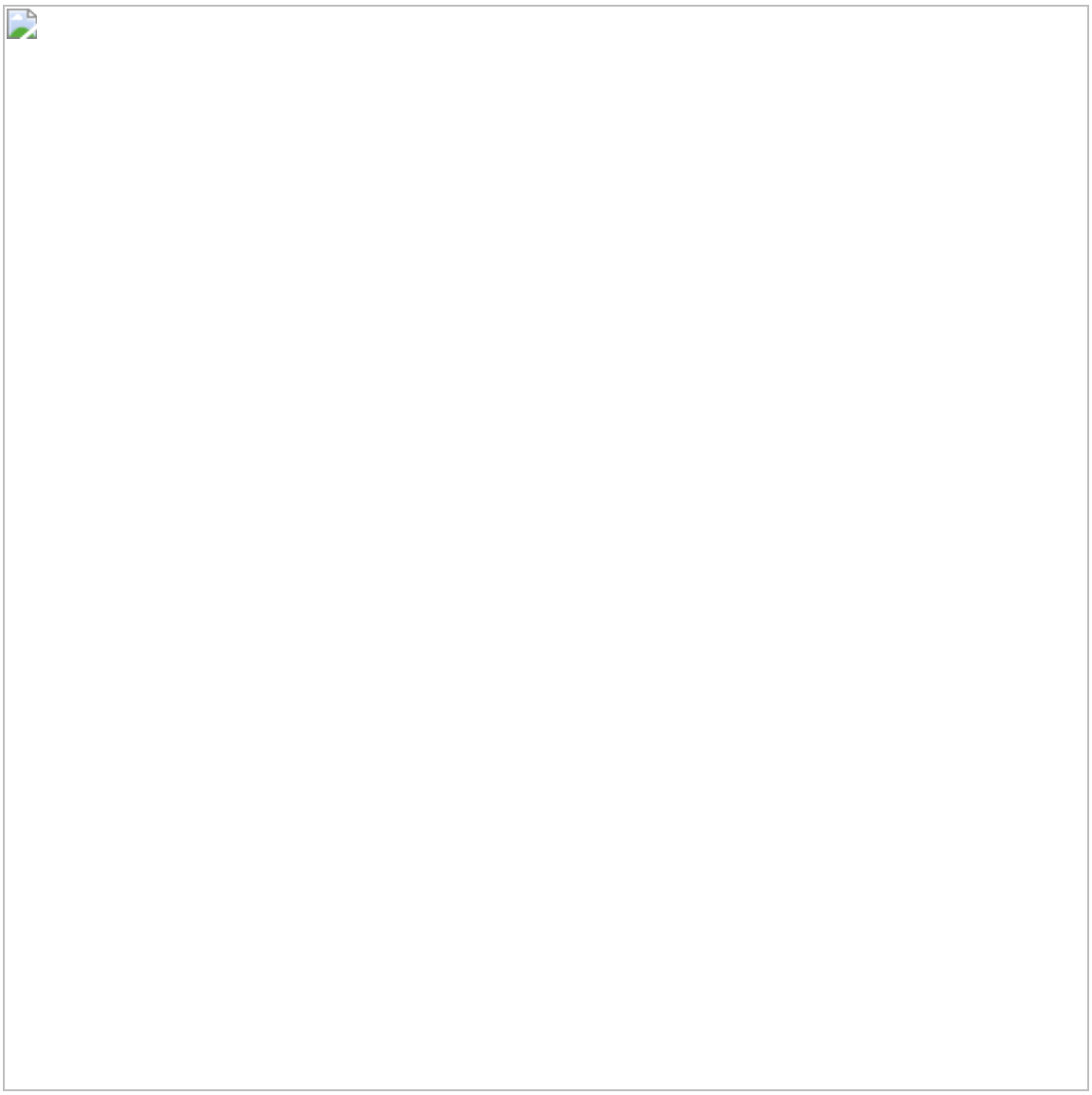
December 22, 2019

Enterprise Networking, Security, and Automation (Version 7.00) – ENSA Final PT Skills Assessment (PTSA)

A few things to keep in mind while completing this activity:

1. Do not use the browser Back button or close or reload any exam windows during the exam.
2. Do not close Packet Tracer when you are done. It will close automatically.
3. Click the Submit Assessment button in the browser window to submit your work.

Topology



Addressing Table

Device Name	G0/0/0	IP Address	Default Gateway
R1	G0/0/0	198.51.100.1/30	N/A
	G0/0/1	192.168.1.1/24	N/A
	G0/0/2	64.100.1.1/29	N/A
R2	G0/0/0	198.51.100.2/30	N/A
	G0/0/1	172.16.2.1/24	N/A
	G0/0/2	209.165.202.129/27	N/A
S1	VLAN1	64.100.1.2/29	64.100.1.1
S2	VLAN1	192.168.1.2/24	192.168.1.1

Device Name	G0/0/0	IP Address	Default Gateway
S3	VLAN1	209.165.202.130/27	209.165.202.129
S4	VLAN1	172.16.2.2/24	172.16.2.1
DNS/WebServer	NIC	209.165.202.131/27	209.165.202.129
PC-A	NIC	64.100.1.5/29	64.100.1.1
PC-B	NIC	192.168.1.5/24	192.168.1.1
PC-C	NIC	172.16.2.5/24	172.16.2.1

Scenario

In this Packet Tracer Skills Assessment, you will configure the devices in a small network. You will complete all tasks in PT Physical Mode. You will not have access to the logical topology.

You will place devices in proper locations and power them on. You will configure routers, switches, and PCs to support IPv4 connectivity for hosts. The routers and switches must be managed securely. You will configure Single-Area OSPFv2, NAT, and access control lists. Further, you will backup up your working configurations to a TFTP server and upload a working configuration to another device.
Furthermore, different versions of the IOS image are used in switches. You will update a switch to use the latest IOS.

Instructions

Part 1: Place Devices in Proper Locations and Connect them with Proper Cables

Step 1: Place devices in proper Locations inside the main wiring closet

In the Physical Mode place network devices in the following locations:

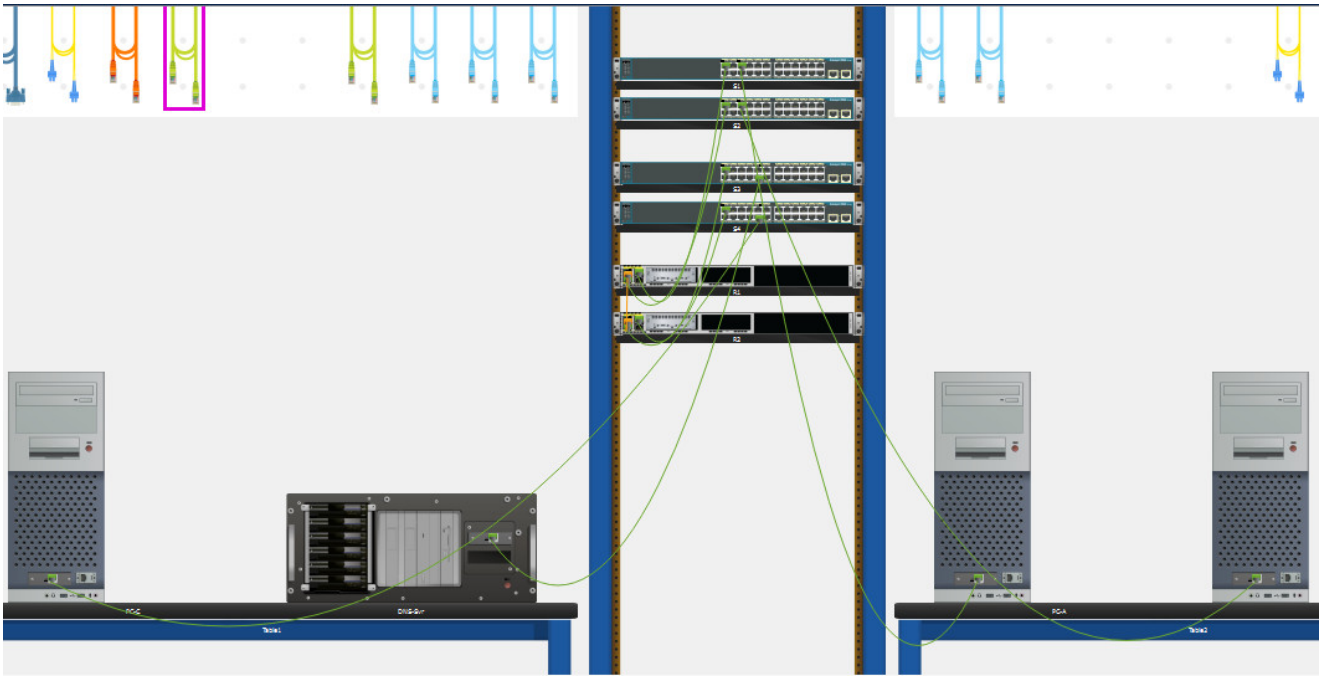
- Organize the rack for ease of configuration. Place R1, R2, S1, S2, S3, and S4 from top down, with some space between the devices.
- Drag two 4331 routers, R1 and R2, from the shelf to the rack.
- Drag four switches, S1, S2, S3, and S4, from the shelf to the rack.
- Move PC-C to Table1, on the left, and place it in the left-hand area of the tabletop
- Move the DNS server to Table1, on the left, and place it in the right-hand area of the tabletop.
- Move PC-A to Table2, on the right, and place it in the left-hand area of the tabletop.
- Move PC-B to Table2, on the right, and place it in the right-hand area of the tabletop.

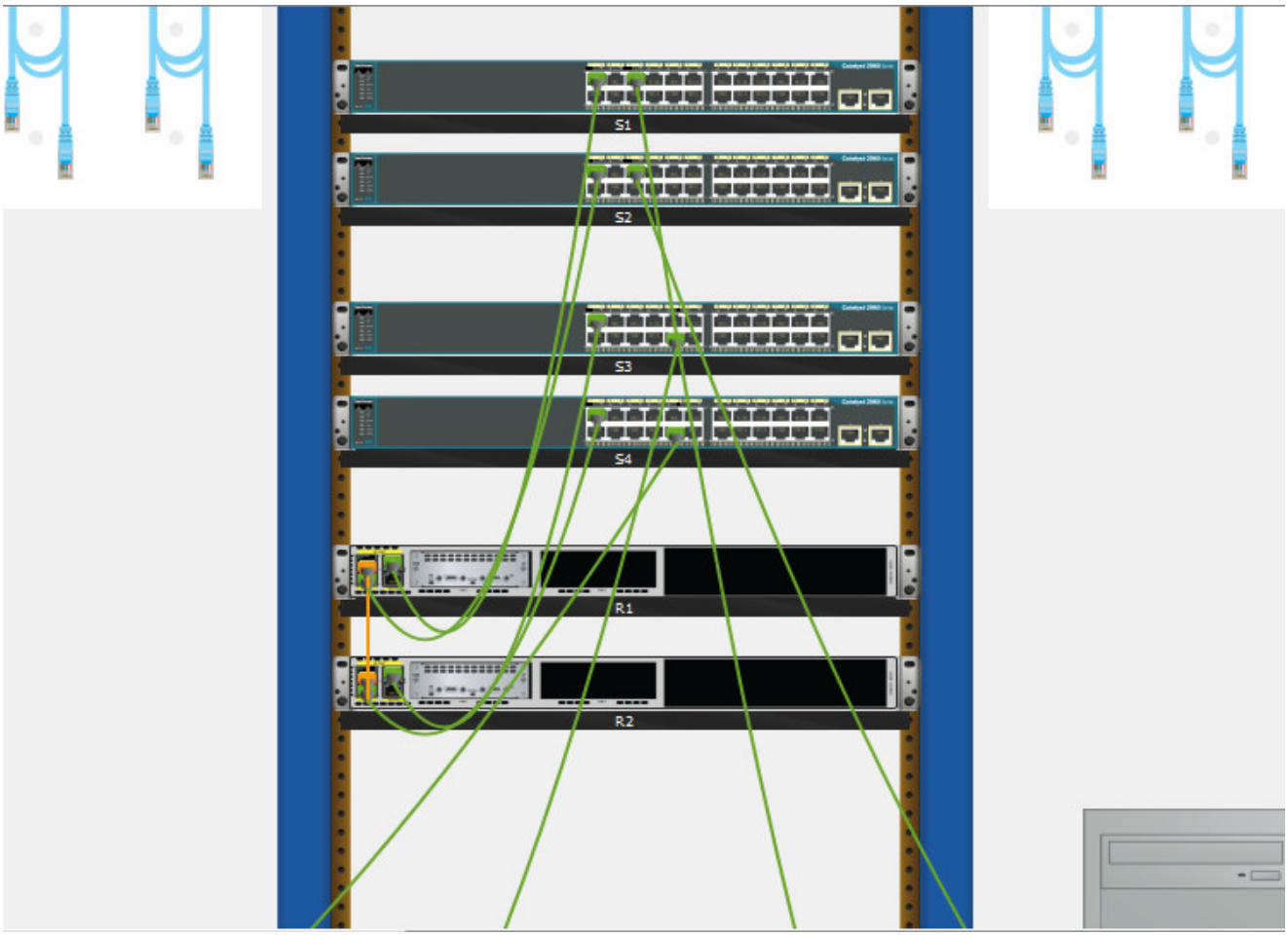
Step 2: Make sure all devices are powered on.

Power on all devices.

Step 3: Connect devices according to the network topology.

Use the logical topology diagram to connect the devices to the correct ports with correct cables.





Part 2: Configure Basic Devices Settings

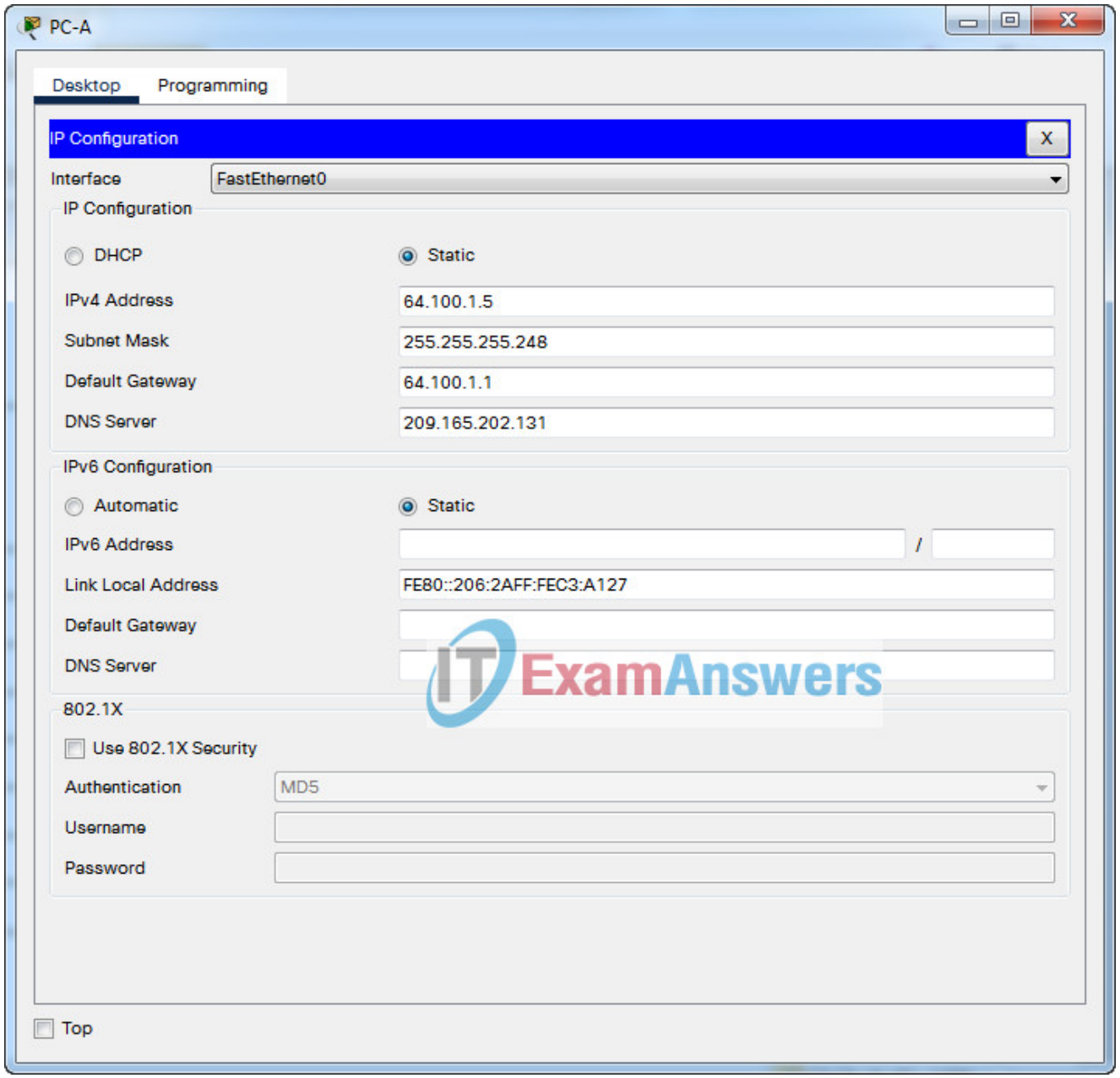
All configurations are made through a direct console connection.

Step 1: Configure PCs with IPv4 addresses

Use the addressing table to manually configure the PCs with full IP addressing.

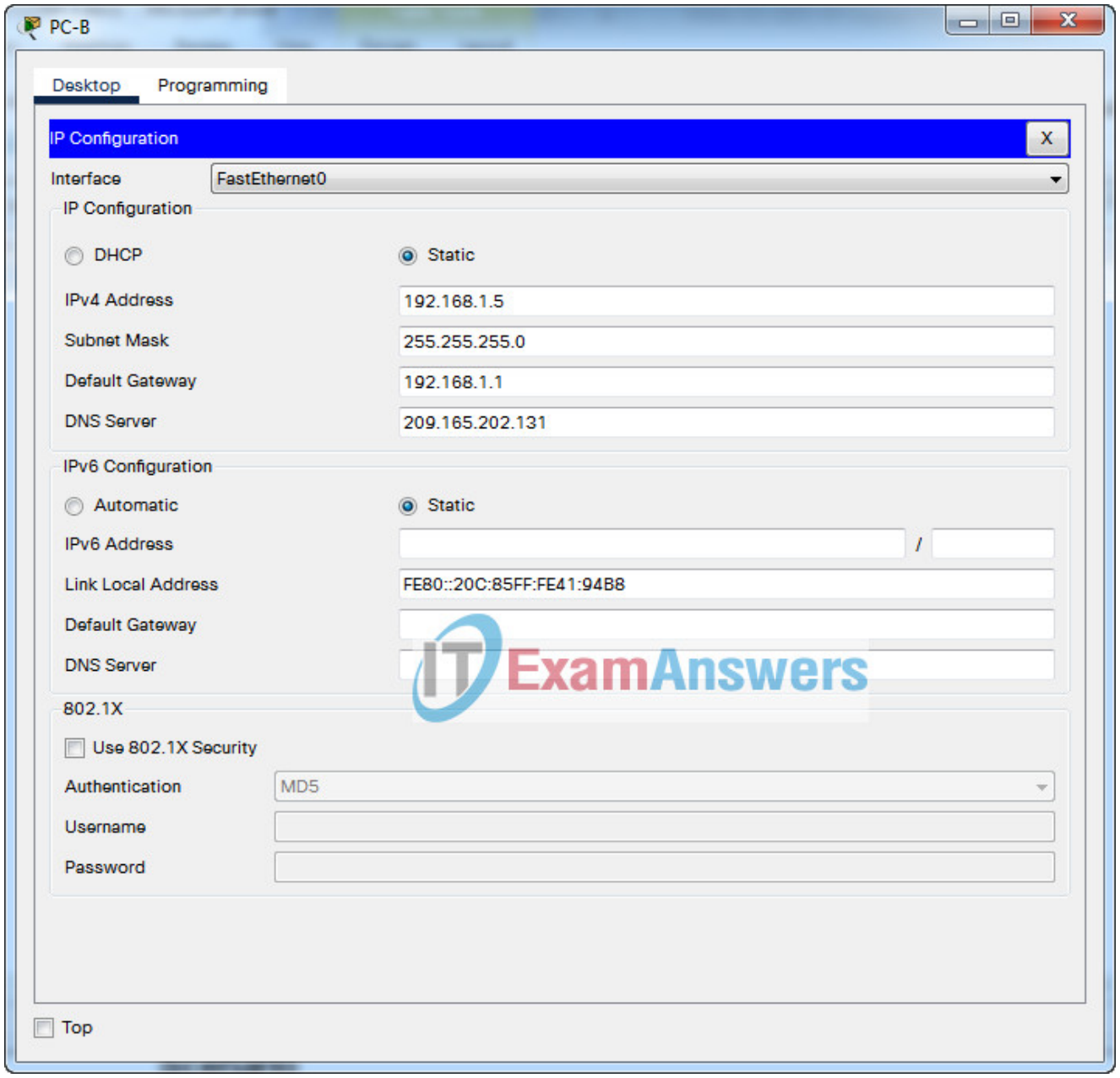
- PC-A
- PC-B
- PC-C

PC-A IPv4 addresses:
IP Address: **64.100.1.5**
Subnet Mask: **255.255.255.248**
Default Gateway: **64.100.1.1**
DNS Server: **209.165.202.131**



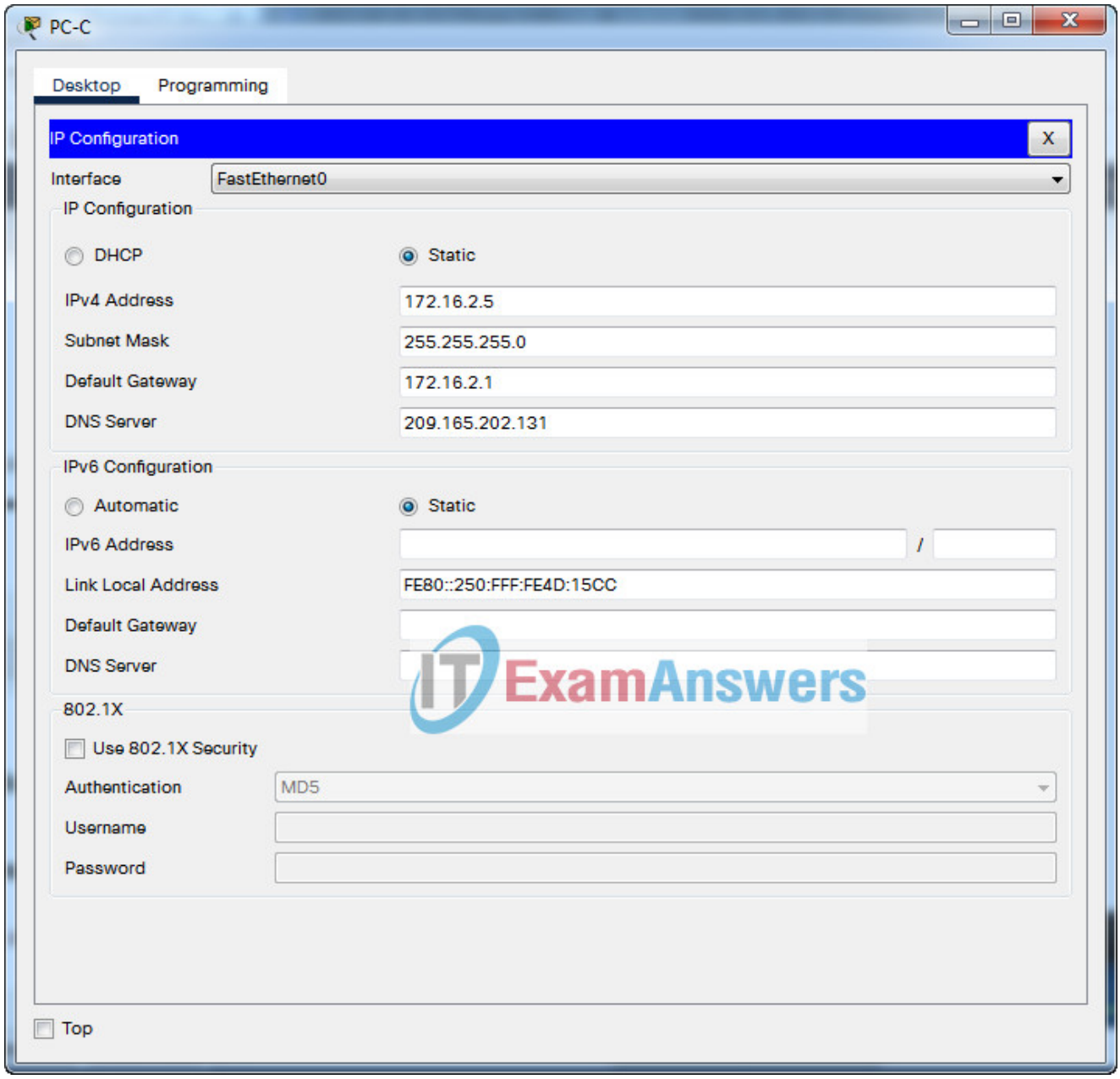
Configure PC-A with IPv4 addresses

PC-B IPv4 addresses:
IP Address: **192.168.1.5**
Subnet Mask: **255.255.255.0**
Default Gateway: **192.168.1.1**
DNS Server: **209.165.202.131**



Configure PC-B with IPv4 addresses

PC-C IPv4 addresses:
IP Address: **172.16.2.5**
Subnet Mask: **255.255.255.0**
Default Gateway: **172.16.2.1**
DNS Server: **209.165.202.131**



Configure PC-C with IPv4 addresses

Step 2: Configure router R1 and R2

a. Configure R1 and R2 with the following:

1. Prevent the router from attempting to resolve incorrectly entered commands as domain names.
2. Router name: **R1** or **R2**.
3. Encrypted privileged EXEC secret password: **ciscoenpass**.
4. Console access password: **ciscoconpass**.
5. Set the minimum password length to **10** characters.
6. Encrypt the clear text passwords.
7. Configure an appropriate MOTD Banner.

Answer:

- Router R1
- Router R2

```
Router(config)#no ip domain lookup
Router(config)#hostname R1
R1(config)#enable secret ciscoenpass

R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit

R1(config)#security passwords min-length 10
R1(config)#service password-encryption
R1(config)#banner motd #Unauthorized Acess is Prohibited#

Router(config)#no ip domain lookup
Router(config)#hostname R2
R2(config)#enable secret ciscoenpass

R2(config)#line console 0
R2(config-line)#password ciscoconpass
R2(config-line)#login
R2(config-line)#exit

R2(config)#security passwords min-length 10
R2(config)#service password-encryption
R2(config)#banner motd #Unauthorized Acess is Prohibited#
```

b. Configure the interfaces of routers **R1** and **R2** as follows.

1. Configure interface G0/0/0 with a description and IPv4 addressing.
2. Configure interface G0/0/1 with a description and IPv4 addressing.
3. Configure interface G0/0/2 with a description and IPv4 addressing.
4. All interfaces should be ready to send and receive traffic.

Answer:

- Router R1
- Router R2

```
R1(config)#interface GigabitEthernet0/0/0
R1(config-if)#description Connection to R2
R1(config-if)#ip address 198.51.100.1 255.255.255.252
R1(config-if)#no shutdown

R1(config-if)#interface GigabitEthernet0/0/1
R1(config-if)#description Connection to S2
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#interface GigabitEthernet0/0/2
R1(config-if)#description Connection to S1
R1(config-if)#ip address 64.100.1.1 255.255.255.248
R1(config-if)#no shutdown

R2(config)#interface GigabitEthernet0/0/0
R2(config-if)#description Connection to R1
R2(config-if)#ip address 198.51.100.2 255.255.255.252
R2(config-if)#no shutdown

R2(config-if)#interface GigabitEthernet0/0/1
R2(config-if)#description Connection to S4
R2(config-if)#ip address 172.16.2.1 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#interface GigabitEthernet0/0/2
R2(config-if)#description Connection to S3
R2(config-if)#ip address 209.165.202.129 255.255.255.224
R2(config-if)#no shutdown
```

c. Configure SSH.

1. Domain name: **ccna-lab.com**.
2. Create an administrative user in the local database:
    - Username: **admin**
    - Secret Password: **admin1pass**
3. Set login on VTY lines to use the local database
4. Set VTY lines to accept SSH connections only
5. Use an RSA crypto key with a **1024** bits modulus.
6. Enable SSH using **version 2**.

Answer:

- Router R1
- Router R2

```
R1(config)#ip domain name ccna-lab.com
R1(config)#username admin secret admin1pass

R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit

R1(config)#crypto key generate rsa
1024

R1(config)#ip ssh version 2

R2(config)#ip domain name ccna-lab.com
R2(config)#username admin secret admin1pass

R2(config)#line vty 0 15
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#exit

R2(config)#crypto key generate rsa
1024

R2(config)#ip ssh version 2
```

Step 3: Configure switches S1, S2, S3, and S4

a. Configure the hostname according to the Addressing Table.
b. Configure Management Interface (SVI) for VLAN 1: Set the IPv4 address and activate the interface.
c. Configure default gateway.

Answer:

- S1
- S2
- S3
- S4

```
Switch(config)#hostname S1
S1(config)#interface Vlan1
S1(config-if)#ip address 64.100.1.2 255.255.255.248
S1(config-if)#no shutdown

S1(config-if)#ip default-gateway 64.100.1.1
```

```
Switch(config)#hostname S2
S2(config)#interface Vlan1
S2(config-if)#ip address 192.168.1.2 255.255.255.0
S2(config-if)#no shutdown

S2(config-if)#ip default-gateway 192.168.1.1

Switch(config)#hostname S3
S3(config)#interface Vlan1
S3(config-if)#ip address 209.165.202.130 255.255.255.224
S3(config-if)#no shutdown

S3(config-if)#ip default-gateway 209.165.202.129

Switch(config)#hostname S4
S4(config)#interface Vlan1
S4(config-if)#ip address 172.16.2.2 255.255.255.0
S4(config-if)#no shutdown

S4(config-if)#ip default-gateway 172.16.2.1
```

Part 3: Configure Single Area OSPFv2

Step 1: Configure single-area OSPF routing

a. Configure the OSPF routing process: Use process id **1**.
b. Manually configure the router id: Use **0.0.0.1** for **R1** and **0.0.0.2** for **R2**
c. Configure network statements for the appropriate networks on **R1** and **R2**.
Note: For the purposes of this assessment, enter your network statements in the following order:
On R1:

- the G0/0/2 network
- the G0/0/0 network

On R2:

- the G0/0/2 network
- the G0/0/0 network

Answer:

- Router R1
- Router R2

```
R1(config)#router ospf 1
R1(config-router)#router-id 0.0.0.1
R1(config-router)#network 64.100.1.0 0.0.0.7 area 0
R1(config-router)#network 198.51.100.0 0.0.0.3 area 0
```

```
R2(config)#router ospf 1
R2(config-router)#router-id 0.0.0.2
R2(config-router)#network 209.165.202.128 0.0.0.31 area 0
R2(config-router)#network 198.51.100.0 0.0.0.3 area 0
```

Step 2: Adjust OSPF operation

a. Configure the appropriate interfaces to not forward OSPF updates where they are not required.
b. Configure the reference bandwidth: Adjust the reference bandwidth to 1 Gigabit.
c. Configure the OSPF network as a point-to-point network.
d. Configure the hello time for 30 seconds.
Answer:

- Router R1
- Router R2

```
R1(config)# router ospf 1
R1(config-router)# passive-interface GigabitEthernet0/0/1
R1(config-router)# passive-interface GigabitEthernet0/0/2
R1(config-router)# auto-cost reference-bandwidth 1000
R1(config-router)# exit

R1(config)# interface GigabitEthernet0/0/0
R1(config-if)# ip ospf network point-to-point
R1(config-if)# ip ospf hello-interval 30

R2(config)# router ospf 1
R2(config-router)# passive-interface GigabitEthernet0/0/1
R2(config-router)# passive-interface GigabitEthernet0/0/2
R2(config-router)# auto-cost reference-bandwidth 1000
R2(config-router)# exit

R2(config)# interface GigabitEthernet0/0/0
R2(config-if)# ip ospf network point-to-point
R2(config-if)# ip ospf hello-interval 30
```

Part 4: Configure Access Control and NAT

Step 1: Verify connectivity

- PC-B cannot visit the web server.
- PC-C cannot ping PC-A.

Step 2: Configure NAT

a. Configure static NAT on router **R1** with a public IP address 64.100.1.7 to allow PC-B to access the web server.

```
R1(config)# ip nat inside source static 192.168.1.5 64.100.1.7

R1(config)# interface GigabitEthernet0/0/0
R1(config-if)# ip nat outside

R1(config-if)# interface GigabitEthernet0/0/1
R1(config-if)# ip nat inside
```

b. Configure PAT on router **R2** to enable some devices on the network attached to the G0/0/1 interface to access the internet

1. Create a NAT pool named IPNAT1 with IP address range of 209.165.202.140 to 209.165.202.150 with the subnet mask of 255.255.255.224.
2. Create a numbered ACL (ACL 1) to allow devices with IP address range of 172.16.2.1 through 172.16.2.15 to access the internet through NAT.
3. Use PAT to allow the range of the public IP addresses to be shared.

```
R2(config)# ip nat pool IPNAT1 209.165.202.140 209.165.202.150 netmask
255.255.255.224
R2(config)# ip nat inside source list 1 pool IPNAT1 overload
R2(config)# access-list 1 permit 172.16.2.0 0.0.0.15

R2(config)# interface GigabitEthernet0/0/1
R2(config-if)# ip nat inside
```

Step 3: Configure access control on R1

a. Create a standard ACL **R1-VTY-LIMIT** to allow only PC-B access to the R1 vty lines.
b. Apply the ACL.

```
R1(config)#ip access-list standard R1-VTY-LIMIT
R1(config-std-nacl)#permit host 192.168.1.5
R1(config-std-nacl)#
R1(config-std-nacl)#line vty 0 15
R1(config-line)#access-class R1-VTY-LIMIT in
```

Step 4: Configure access control on S1

a. Create a standard ACL **S1-VTY-LIMIT** to allow only PC-B access to the S1 vty lines.
b. Apply the ACL.

```
S1(config)#ip access-list standard S1-VTY-LIMIT
S1(config-std-nacl)#permit host 192.168.1.5
S1(config-std-nacl)#
S1(config-std-nacl)#line vty 0 15
S1(config-line)#access-class S1-VTY-LIMIT in
```

Step 5: Configure access control on R2

a. Create a standard ACL **R2-VTY-LIMIT** to allow only PC-C access to the R2 vty lines.

b. Create an extended ACL **R2-SECURITY** to restrict access from the internet

- Allow FTP connections from the PC-B public IP address to the web/DNS server
- Deny all other FTP connections from the internet to the R2 LANs
- Deny all SSH connections from the internet
- Allow all other types of connections from the internet

Your ACL should consist of **four** statements that correspond to the four requirements above.

c. Apply the ACLs

```
R2(config)#ip access-list standard R2-VTY-LIMIT
R2(config-std-nacl)#permit host 172.16.2.5
R2(config-std-nacl)#
R2(config-std-nacl)#line vty 0 15
R2(config-line)#access-class R2-VTY-LIMIT in
R2(config-line)#exit

R2(config)#ip access-list extended R2-SECURITY
R2(config-ext-nacl)#permit tcp host 64.100.1.7 host 209.165.202.131 eq ftp
R2(config-ext-nacl)#deny tcp any any eq ftp
R2(config-ext-nacl)#deny tcp any any eq 22
R2(config-ext-nacl)#permit ip any any

R2(config-ext-nacl)#interface GigabitEthernet0/0/0
R2(config-if)#ip access-group R2-SECURITY in
R2(config-if)#ip nat outside
```

Step 6: Configure access control on S3

a. Create a standard ACL **S3-VTY-LIMIT** to allow only PC-C access to the S3 vty lines.
b. Apply the ACL

```
S3(config)#ip access-list standard S3-VTY-LIMIT
S3(config-std-nacl)#permit host 172.16.2.5
S3(config-std-nacl)#
S3(config-std-nacl)#line vty 0 15
S3(config-line)#access-class S3-VTY-LIMIT in
S3(config-line)#login
```

Part 5: Perform Configuration Backup and IOS Update

Step 1: Use TFTP server to backup device configurations

a. Backup the running configurations of R1, S1, and S2 to the TFTP server on PC-B.
b. Name the configuration files as **R1-Run-Config**, **S1- Run-Config**, and **S2-Run-Config**.

Go to R1:

```
R1>en
R1#copy running-config tftp
Address or name of remote host []? 192.168.1.5
Destination filename [R1-confg]? R1-Run-Config
```

Go to S1:

```
S1>en
S1#copy running-config tftp
Address or name of remote host []? 192.168.1.5
Destination filename [S1-confg]? S1-Run-Config
```

Go to S2:

```
S2>en
S2#copy running-config tftp
Address or name of remote host []? 192.168.1.5
Destination filename [S2-confg]? S2-Run-Config

Writing running-config....!!
[OK - 1122 bytes]

1122 bytes copied in 3.003 secs (373 bytes/sec)
```

Step 2: Use TFTP server to update/upgrade IOS software

a. Obtain a newer IOS image from the TFTP service on the web/DNS server.
b. The newer version of the switch IOS is c2960-lanbasek9-mz.150-2.SE4.bin.
c. Configure S3 to use this newer version IOS after reloading.

```
S3#copy tftp flash:
Address or name of remote host []? 209.165.202.131
Source filename []? c2960-lanbasek9-mz.150-2.SE4.bin
Destination filename [c2960-lanbasek9-mz.150-2.SE4.bin]?

Accessing tftp://209.165.202.131/c2960-lanbasek9-mz.150-2.SE4.bin....
Loading c2960-lanbasek9-mz.150-2.SE4.bin from 209.165.202.131:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

[OK - 4670455 bytes]

S3#configure terminal
S3(config)#boot system flash:c2960-lanbasek9-mz.150-2.SE4.bin
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S3#reload
Proceed with reload? [confirm]
```

Answer script

R1

```
enable
configure terminal

no ip domain lookup
hostname R1
enable secret ciscoenpass
line console 0
password ciscoconpass
login
exit

security passwords min-length 10
service password-encryption
banner motd #Unauthorized Acess is Prohibited#

interface GigabitEthernet0/0/0
description Connection to R2
ip address 198.51.100.1 255.255.255.252
no shutdown

interface GigabitEthernet0/0/1
description Connection to S2
ip address 192.168.1.1 255.255.255.0
no shutdown

interface GigabitEthernet0/0/2
description Connection to S1
ip address 64.100.1.1 255.255.255.248
no shutdown

ip domain name ccna-lab.com
username admin secret admin1pass

line vty 0 15
login local
transport input ssh
exit

crypto key generate rsa
1024

ip ssh version 2

router ospf 1
router-id 0.0.0.1
network 64.100.1.0 0.0.0.7 area 0
network 198.51.100.0 0.0.0.3 area 0
exit

router ospf 1
passive-interface GigabitEthernet0/0/1
passive-interface GigabitEthernet0/0/2
```

```
auto-cost reference-bandwidth 1000
exit

interface GigabitEthernet0/0/0
ip ospf network point-to-point
ip ospf hello-interval 30
exit

ip nat inside source static 192.168.1.5 64.100.1.7

interface GigabitEthernet0/0/0
ip nat outside
interface GigabitEthernet0/0/1
ip nat inside

ip access-list standard R1-VTY-LIMIT
permit host 192.168.1.5

line vty 0 15
access-class R1-VTY-LIMIT in
exit
```

R2

```
enable
configure terminal

no ip domain lookup
hostname R2
enable secret ciscoenpass
line console 0
password ciscoconpass
login
exit

security passwords min-length 10
service password-encryption
banner motd #Unauthorized Acess is Prohibited#

interface GigabitEthernet0/0/0
description Connection to R1
ip address 198.51.100.2 255.255.255.252
no shutdown

interface GigabitEthernet0/0/1
description Connection to S4
ip address 172.16.2.1 255.255.255.0
no shutdown

interface GigabitEthernet0/0/2
description Connection to S3
ip address 209.165.202.129 255.255.255.224
no shutdown

ip domain name ccna-lab.com
username admin secret admin1pass

line vty 0 15
login local
transport input ssh
exit

crypto key generate rsa
1024

ip ssh version 2

router ospf 1
router-id 0.0.0.2
network 209.165.202.128 0.0.0.31 area 0
network 198.51.100.0 0.0.0.3 area 0
exit

router ospf 1
passive-interface GigabitEthernet0/0/1
passive-interface GigabitEthernet0/0/2
```

```
auto-cost reference-bandwidth 1000
exit

interface GigabitEthernet0/0/0
ip ospf network point-to-point
ip ospf hello-interval 30
exit

ip nat pool IPNAT1 209.165.202.140 209.165.202.150 netmask 255.255.255.224
ip nat inside source list 1 pool IPNAT1 overload
access-list 1 permit 172.16.2.0 0.0.0.15

interface GigabitEthernet0/0/1
ip nat inside

ip access-list standard R2-VTY-LIMIT
permit host 172.16.2.5

line vty 0 15
access-class R2-VTY-LIMIT in
exit

ip access-list extended R2-SECURITY
permit tcp host 64.100.1.7 host 209.165.202.131 eq ftp
deny tcp any any eq ftp
deny tcp any any eq 22
permit ip any any

interface GigabitEthernet0/0/0
ip access-group R2-SECURITY in
ip nat outside
exit
```

S1

```
enable
configure ter
configure terminal

hostname S1
interface Vlan1
ip address 64.100.1.2 255.255.255.248
no shutdown

ip default-gateway 64.100.1.1

ip access-list standard S1-VTY-LIMIT
permit host 192.168.1.5

line vty 0 15
access-class S1-VTY-LIMIT in
exit
```

S2

```
enable
configure terminal

hostname S2
interface Vlan1
ip address 192.168.1.2 255.255.255.0
no shutdown

ip default-gateway 192.168.1.1
```

S3

```
enable
config ter

hostname S3
interface Vlan1
ip address 209.165.202.130 255.255.255.224
no shutdown

ip default-gateway 209.165.202.129

ip access-list standard S3-VTY-LIMIT
permit host 172.16.2.5

line vty 0 15
access-class S3-VTY-LIMIT in
```

S4

```
enable
config ter
hostname S4
interface Vlan1
ip address 172.16.2.2 255.255.255.0
no shutdown

ip default-gateway 172.16.2.1
```