Step 1: Configure the PC interfaces.

a. Configure the IP address, subnet mask, and default gateway settings on PC-A.

b. Configure the IP address, subnet mask, and default gateway settings on PC-B.

Step 2: Configure the router.

a. Console into the router and enable privileged EXEC mode.

```
Router> enable
Router#
```

b. Enter into global configuration mode.

```
Router# config terminal
Router(config)#
```

c. Assign a device name to the router.

```
Router(config)# hostname R1
```

d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.

```
R1(config)# no ip domain-lookup
```

e. Require that a minimum of 10 characters be used for all passwords.

```
R1(config)# security passwords min-length 10
```

Besides setting a minimum length, list other ways to strengthen passwords.

f. Assign cisco12345 as the privileged EXEC encrypted password.

```
R1(config)# enable secret cisco12345
```

g. Assign ciscoconpass as the console password, establish a timeout, enable login, and add the logging synchronous command. The logging synchronous command synchronizes debug and Cisco IOS
software output and prevents these messages from interrupting your keyboard input.

```
R1(config)# line con 0
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
R1(config-line)# exit
R1(config)#
```

For the exec-timeout command, what do the 5 and 0 represent?

h. Assign ciscovtypass as the vty password, establish a timeout, enable login, and add the logging synchronous command.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
```

```
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
R1(config-line)# exit
R1(config)#
```

i. Encrypt the clear text passwords.

```
R1(config)# service password-encryption
```

j. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

```
R1(config)# banner motd #Unauthorized access prohibited!#
```

k. Configure an IP address and interface description. Activate both interfaces on the router.

```
R1(config)# int g0/0
R1(config-if)# description Connection to PC-B
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# int g0/1
R1(config-if)# description Connection to S1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
R1#
```

l. Set the clock on the router; for example:

```
R1# clock set 17:00:00 18 Feb 2013
```

m. Save the running configuration to the startup configuration file.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Step 4: Configure the router for SSH access.

a. Enable SSH connections and create a user in the local database of the router.

```
R1# configure terminal
R1(config)# ip domain-name CCNA-lab.com
R1(config)# username admin privilege 15 secret adminpass1
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
R1(config-line)# exit
```

R1(config)# crypto key generate rsa modulus 1024
R1(config)# exit
b. Remotely access R1 from PC-A using the Tera Term SSH client

a. Assign an IPv6 global unicast address to interface G0/0, assign the link-local address in addition to the unicast address on the interface, and enable IPv6 routing.

R1# configure terminal
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ipv6 unicast-routing
R1(config)# exit

Part 2: Configure Basic Network Device Settings

Step 1: Configure basic switch settings.

no ip domain-lookup
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
Exit

S1# configure terminal
S1(config)# vlan 99
S1(config-vlan)# exit
S1(config)# interface vlan99
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit

S1(config)#
S1(config)# interface range f0/1 – 24,g0/1 - 2
S1(config-if-range)# switchport access vlan 99

```
S1(config-if-range)# exit
S1(config)#
S1(config)# ip default-gateway 192.168.1.1
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# logging synchronous
S1(config-line)# exit

S1(config)#
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
S1# show mac address-table
S1# show mac address-table dynamic
```