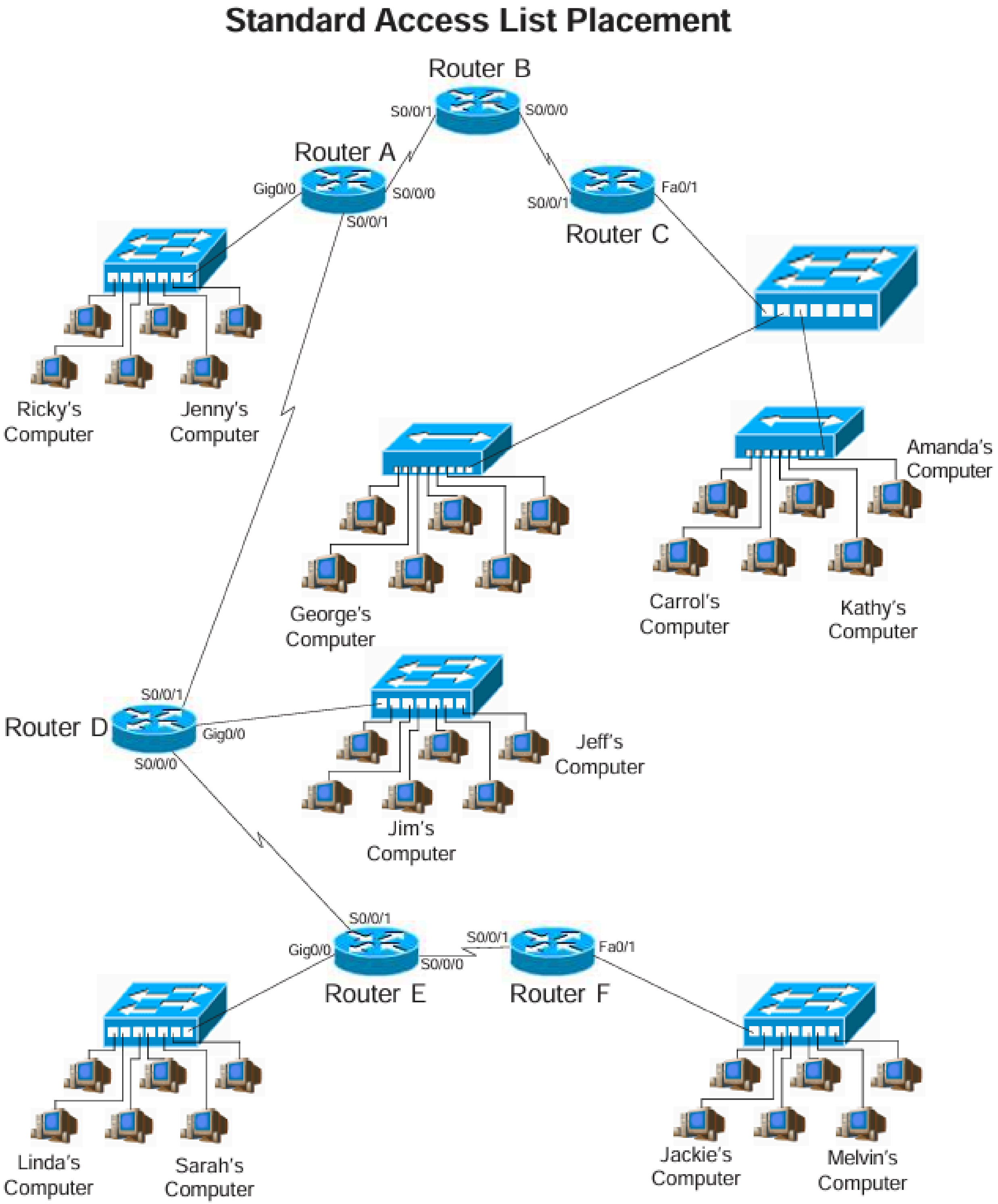
Q1

a) Page 5



Standard Access List Placement
Router B
S0/0/1
S0/0/0
Router A
Gig0/0
S0/0/0
S0/0/1
S0/0/1
Fa0/1
Router C
Ricky's Computer
Jenny's Computer
Amanda's Computer
George's Computer
Carrol's Computer
Kathy's Computer
S0/0/1
Router D
Gig0/0
S0/0/0
Jeff's Computer
Jim's Computer
S0/0/1
Gig0/0
S0/0/0
S0/0/1
Fa0/1
Router E
Router F
Linda's Computer
Sarah's Computer
Jackie's Computer
Melvin's Computer

Standard Access List Placement

1. Where would you place a standard access list to permit traffic from Ricky's computer to reach Jeff's computer?

Router Name Router D
Interface Gig0/0

2. Where would you place a standard access list to deny traffic from Melvin's computer from reaching Jenny's computer?

Router Name Router A
Interface Gig0/0

3. Where would you place a standard access list to deny traffic to Carrol's computer from Sarah's computer?

Router Name Router C
Interface fa0/1

4. Where would you place a standard access list to permit traffic to Ricky's computer from Jeff's computer?

Router Name Router A
Interface g0/0

```
int g0/0
ip access-group 88 out
```

5. Where would you place a standard access list to deny traffic from Amanda's computer from reaching Jeff and Jim's computer?

Router Name Router D
Interface g0/0

6. Where would you place a standard access list to permit traffic from Jackie's computer to reach Linda's computer?

Router Name Router E
Interface g0/0

7. Where would you place a standard access list to permit traffic from Ricky's computer to reach Carrol and Amanda's computer?

Router Name Router C
Interface fa0/1

8. Where would you place a standard access list to deny traffic to Jenny's computer from Jackie's computer?

Router Name Router A
Interface g0/0

9. Where would you place a standard access list to permit traffic from George's computer to reach Linda and Sarah's computer?

Router Name Router E
Interface g0/0

10. Where would you place an ACL to deny traffic from Jeff's computer from reaching George's computer?

Router Name Router C
Interface fa0/1

11. Where would you place a standard access list to deny traffic to Sarah's computer from Ricky's computer?

Router Name Router E
Interface g0/0

12. Where would you place an ACL to deny traffic from Linda's computer from reaching Jackie's computer?

Router Name Router F
Interface fa0/1

b) Page 17

Wildcard Mask Problems

1. Create a wildcard mask to match this exact address.
IP Address: 192.168.25.70
Subnet Mask: 255.255.255.0
0 . 0 . 0 . 0 0.0.0.255

2. Create a wildcard mask to match this range.
IP Address: 210.150.10.0
Subnet Mask: 255.255.255.0
0 . 0 . 0 . 255

3. Create a wildcard mask to match this host.
IP Address: 195.190.10.35
Subnet Mask: 255.255.255.0
0.0.0.255

4. Create a wildcard mask to match this range.
IP Address: 172.16.0.0
Subnet Mask: 255.255.0.0
0.0.255.255

5. Create a wildcard mask to match this range.
IP Address: 10.0.0.0
Subnet Mask: 255.0.0.0
0.255.255.255

6. Create a wildcard mask to match this exact address.
IP Address: 165.100.0.130
Subnet Mask: 255.255.255.192
0.0.0.63

7. Create a wildcard mask to match this range.
IP Address: 192.10.10.16
Subnet Mask: 255.255.255.224
0.0.0.31

8. Create a wildcard mask to match this range.
IP Address: 171.50.75.128
Subnet Mask: 255.255.255.192
0.0.0.63

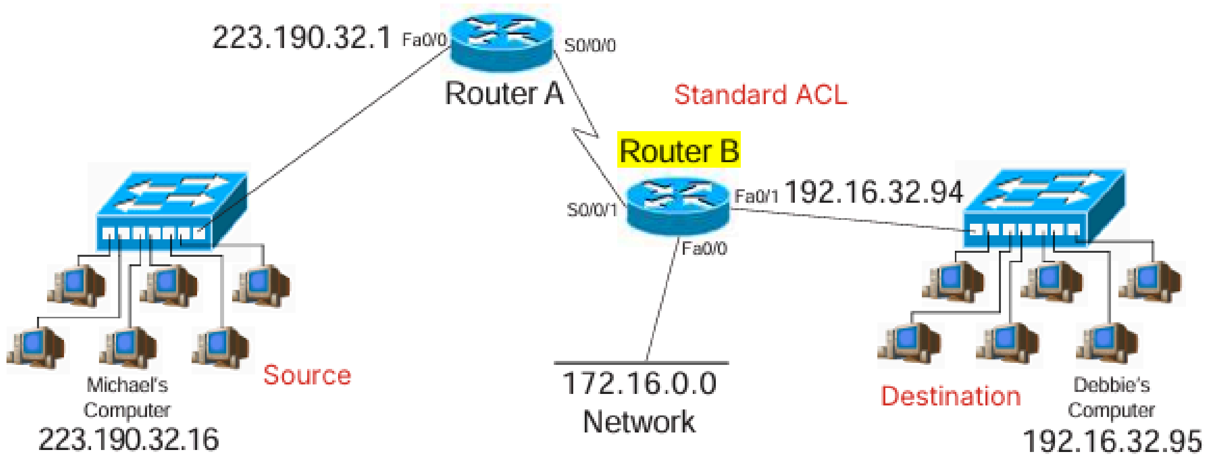
9. Create a wildcard mask to match this host.
IP Address: 10.250.30.2
Subnet Mask: 255.0.0.0
0.255.255.255

10. Create a wildcard mask to match this range.
IP Address: 210.150.28.16
Subnet Mask: 255.255.255.240
0.0.0.15

11. Create a wildcard mask to match this range.
IP Address: 172.18.0.0
Subnet Mask: 255.255.224.0
0.0.31.255

12. Create a wildcard mask to match this range.
IP Address: 135.35.230.32
Subnet Mask: 255.255.255.248
0.0.0.7

c) Page 26 (Problem 1)



Standard Access List Problem #1

Write a standard access list to block Debbie's computer from receiving information from Michael's computer; but will allow all other traffic. List all the command line options for this problem. Keep in mind that there may be multiple ways many of the individual statements in an ACL can be written.

Place the access list at:
Router Name: ___Router B___
Interface: ___Fa0/1___
Access-list #: _1_

[Writing and installing an ACL]

access-list (1-99) deny ______ 0.0.0.0
source add. source wildcard mask

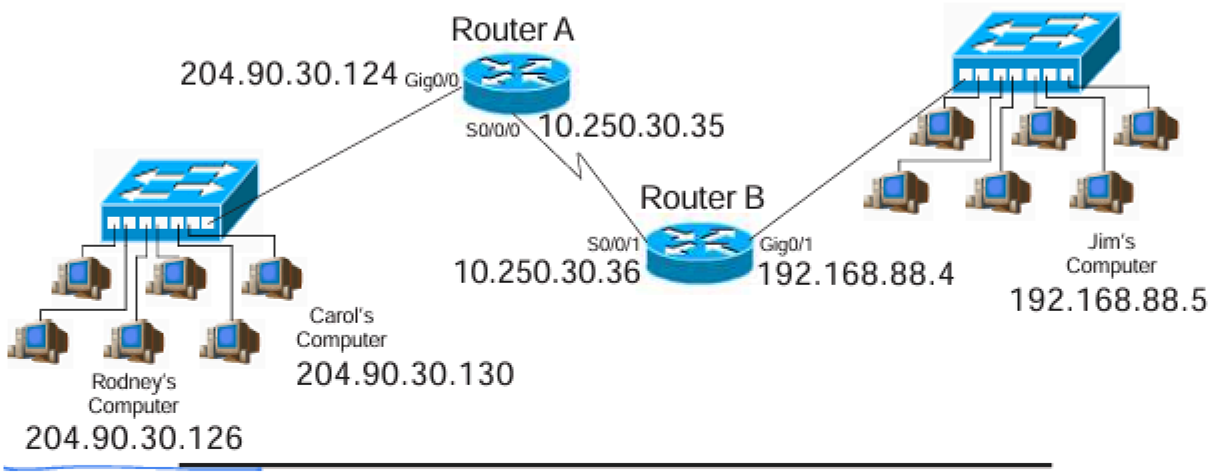
Router# *configure terminal (or config t)*
Router B
Router(config)# ___access-list 1 deny host 223.190.32.16___
or
___access-list 1 permit any___
or
______

Router(config)# ___int f0/1___
Router B
or
___ip access-group 1 out___

Router(config)# *interface* ________

Router(config-if)# *ip access-group* ________ *in or out* (circle one)
Router(config-if)# *exit*
Router(config)# *exit*

d) Page 28 (Problem 3)



Standard Access List Problem #3

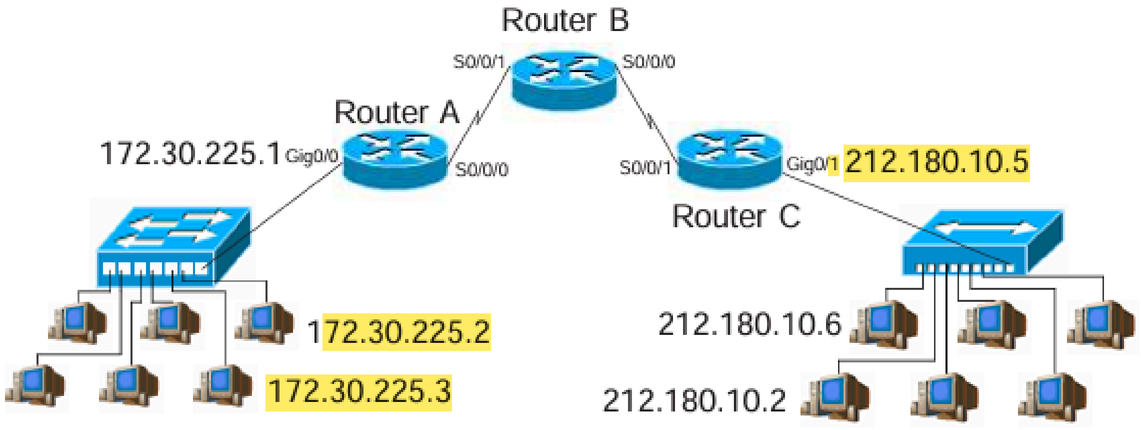
Write a standard access list to block Rodney and Carol's computer from sending information to Jim's computer; but will allow all other traffic from the 204.90.30.0 network. Block all other traffic. Keep in mind that there may be multiple ways many of the individual statements in an ACL can be written.

Place the access list at:
Router Name: ____Router B____
Interface: ____Gig0/1____
Access-list #: ____1____

[Writing and installing an ACL]

```
Router# configure terminal (or config t)

Router(config)# ____access-list 1 deny host 204.90.30.126____
                ____access-list 1 deny host 204.90.30.130____
                ____access-list 1 deny all any____
                ____access-list-1 permit 204.90.30.0 0.0.0.255____
                ________________________________
                ________________________________

Router(config)# interface __g0/1__

Router(config-if)# ip access-group __1__ [✓ in] or out (circle one)
Router(config-if)# exit
Router(config)# exit
```

e) Page 30 (Problem 5)



Standard Access List Problem #5

Write a standard access list to block 172.30.225.2 and 172.30.225.3 from sending information to the 212.180.10.0 network; but will allow all other traffic. Keep in mind that there may be multiple ways many of the individual statements in an ACL can be written.

Place the access list at:
Router Name: ________Router C________________
Interface: ___________g0/1________________
Access-list #: ________69________________

[Writing and installing an ACL]

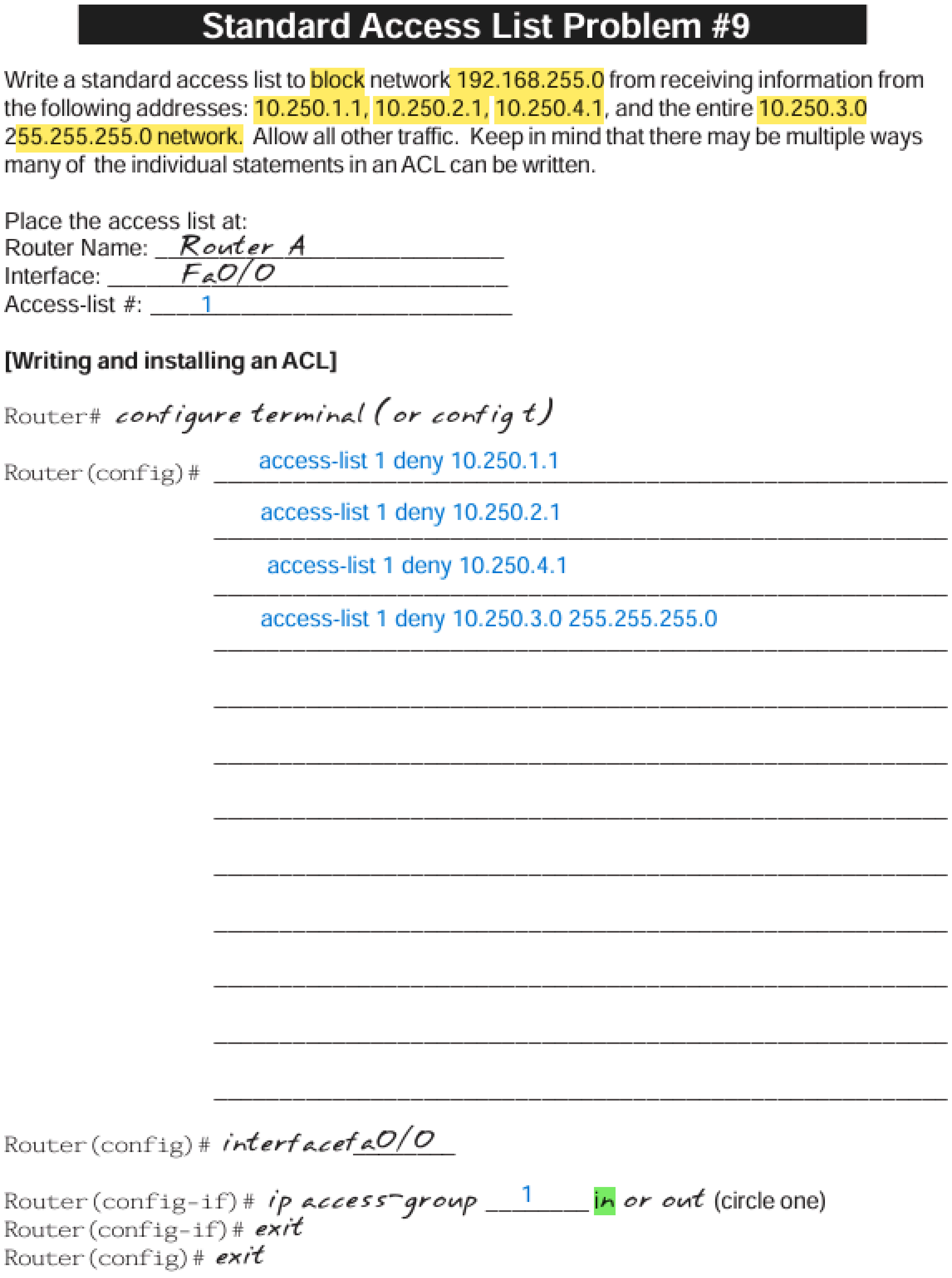
Router# *configure terminal (or config t)*

Router(config)# access-list 69 deny 172.30.225.2
access-list 69 deny 172.30.225.3
access-list 69 permit any
Router C
int g0/1
ip access-group 69 out

Router(config)# *interface* ___g0/1___

Router(config-if)# *ip access-group* ___69___ *in or* [✓ *out*] (circle one)
Router(config-if)# *exit*
Router(config)# *exit*

f) Page 34 (Problem 9)



Standard Access List Problem #9

Write a standard access list to block network 192.168.255.0 from receiving information from the following addresses: 10.250.1.1, 10.250.2.1, 10.250.4.1, and the entire 10.250.3.0 255.255.255.0 network. Allow all other traffic. Keep in mind that there may be multiple ways many of the individual statements in an ACL can be written.

Place the access list at:
Router Name: Router A
Interface: Fa0/0
Access-list #: 1

[Writing and installing an ACL]

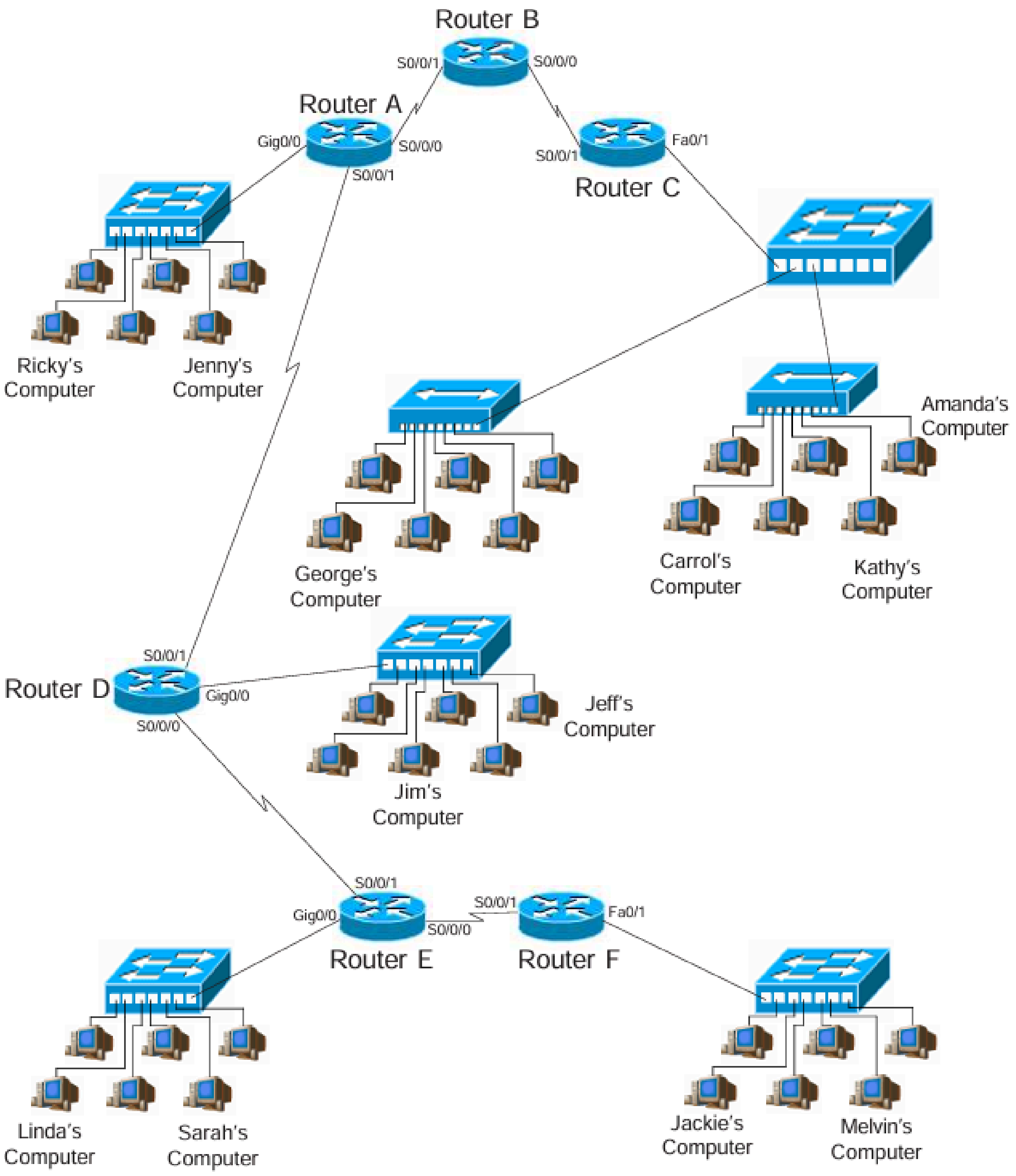
```
Router# configure terminal (or config t)
Router(config)# access-list 1 deny 10.250.1.1
                access-list 1 deny 10.250.2.1
                access-list 1 deny 10.250.4.1
                access-list 1 deny 10.250.3.0 255.255.255.0

Router(config)# interfacefa0/0
Router(config-if)# ip access-group 1 [✓ in] or out (circle one)
Router(config-if)# exit
Router(config)# exit
```

Q2

2. Extended ACL - Refer to T4 ACL Workbookv2:

a) Page 9

Extended Access List Placement



Extended Access List Placement

1. Where would you place an ACL to deny traffic from Jeff's computer from reaching George's computer?

Router Name Router D
Interface Gig0/0 (out)

2. Where would you place an extended access list to permit traffic from Jackie's computer to reach Linda's computer?

Router Name Router F
Interface FA0/1 (out)

3. Where would you place an extended access list to deny traffic to Carrol's computer from Ricky's computer?

Router Name Router A
Interface g0/0 (in)

4. Where would you place an extended access list to deny traffic to Sarah's computer from Jackie's computer?

Router Name Router F
Interface f0/1

5. Where would you place an extended access list to permit traffic from Carrol's computer to reach Jeff's computer?

Router Name Router A
Interface g0/0

6. Where would you place an extended access list to deny traffic from Melvin's computer from reaching Jeff and Jim's computer?

Router Name Router F
Interface fa0/1

7. Where would you place an extended access list to permit traffic from George's computer to reach Jeff's computer?

Router Name Router D
Interface g0/0 (in

```
access-list 199 deny icmp host
10.10.10.10(source) host
192.168.1.5(destination)
access-list 188 permit ip any any
Router D
int g0/0
ip access-group 188 in
```

8. Where would you place an extended access list to permit traffic from Jim's computer to reach Carrol and Amanda's computer?

Router Name Router C
Interface fa0/1

9. Where would you place an ACL to deny traffic from Linda's computer from reaching Kathy's computer?

Router Name Router C
Interface g0/0

10. Where would you place an extended access list to deny traffic to Jenny's computer from Sarah's computer?

Router Name Router A
Interface g0/0

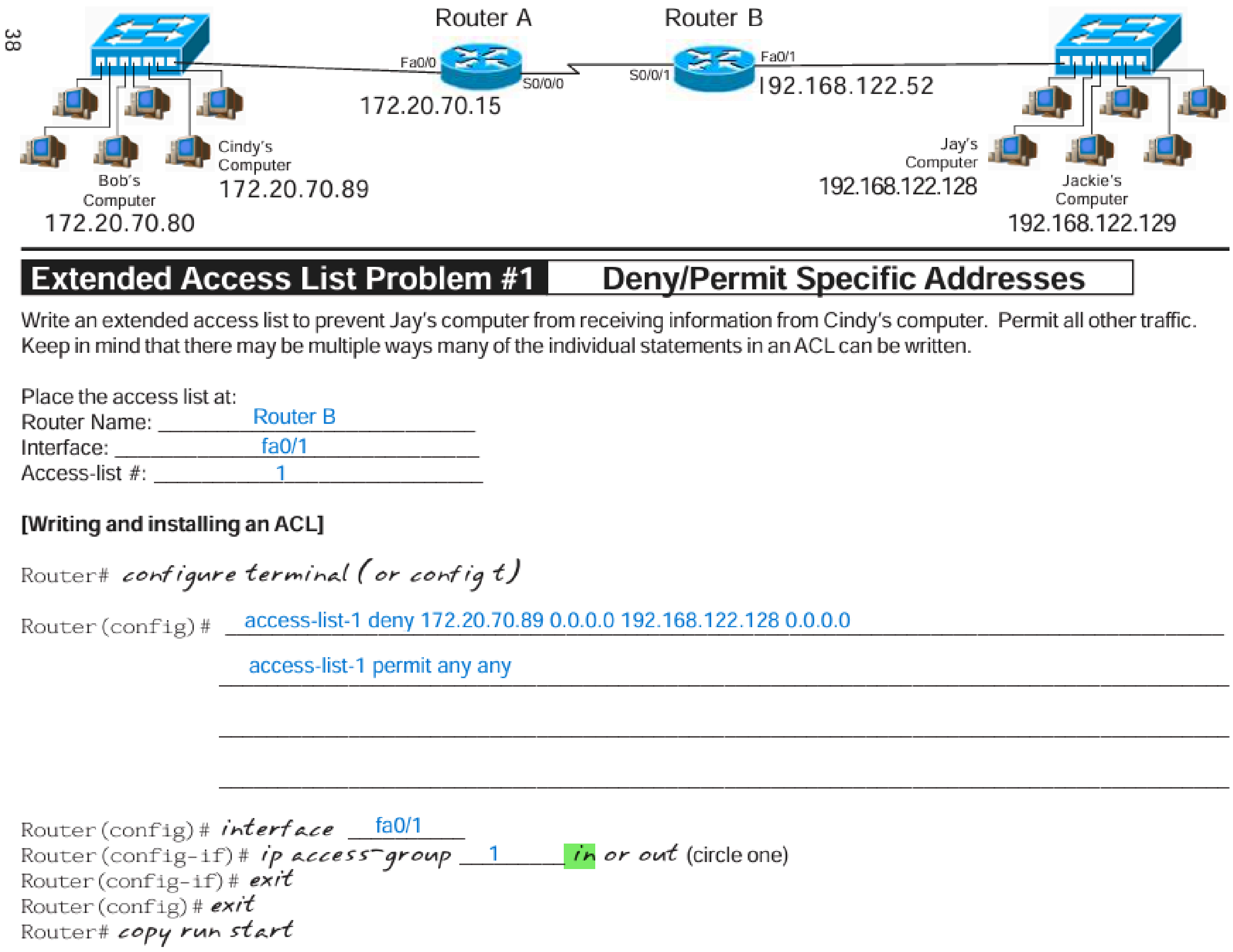
11. Where would you place an extended access list to permit traffic from George's computer to reach Linda and Sarah's computer?

Router Name Router E
Interface g0/0

12. Where would you place an extended access list to deny traffic from Linda's computer from reaching Jenny's computer?

Router Name Router A
Interface g0/0

b) Page 38 (Problem 1)



Router A
Router B
Fa0/0
S0/0/0
S0/0/1
Fa0/1
172.20.70.15
192.168.122.52
Cindy's Computer
172.20.70.89
Bob's Computer
172.20.70.80
Jay's Computer
192.168.122.128
Jackie's Computer
192.168.122.129

Extended Access List Problem #1 | Deny/Permit Specific Addresses

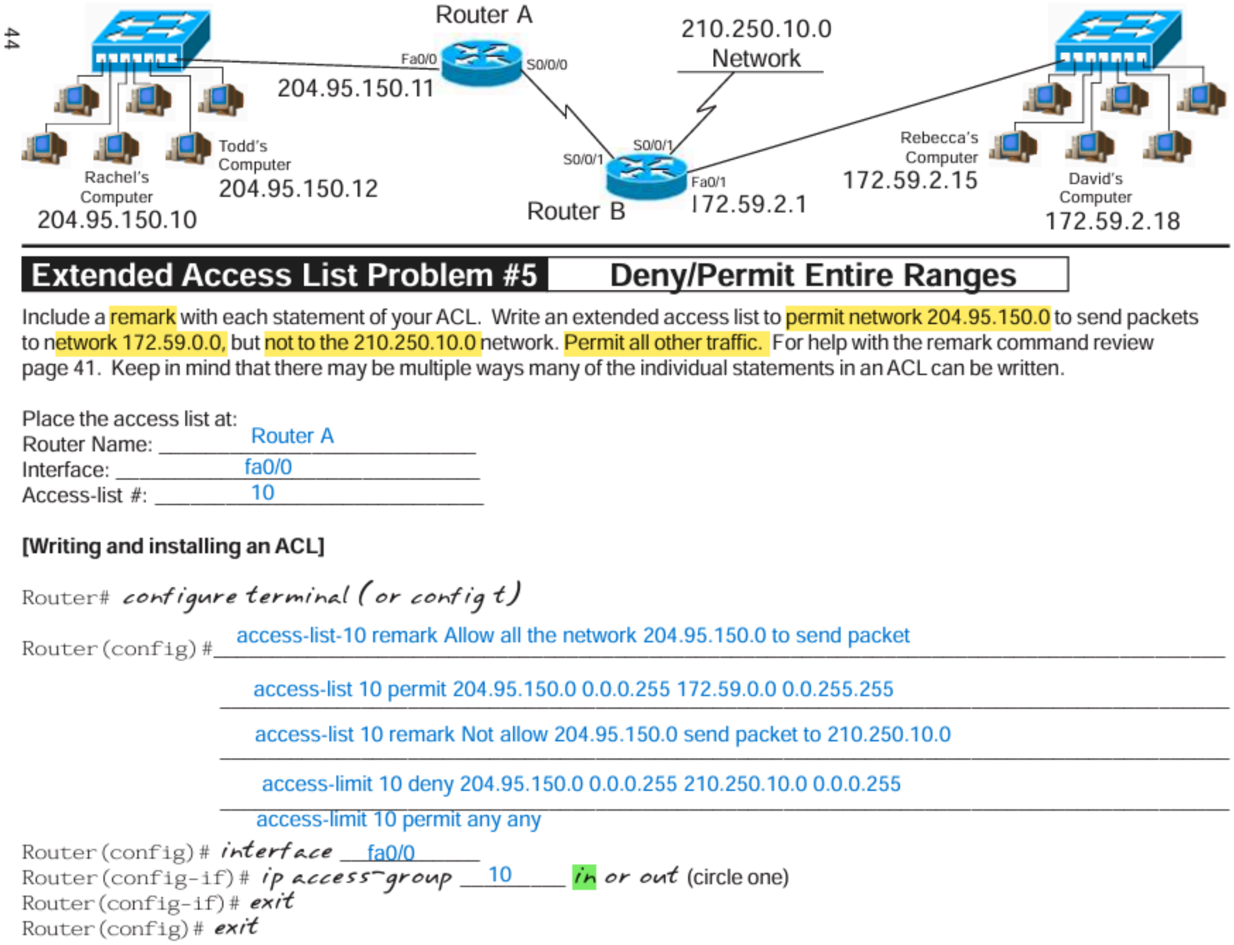
Write an extended access list to prevent Jay's computer from receiving information from Cindy's computer. Permit all other traffic. Keep in mind that there may be multiple ways many of the individual statements in an ACL can be written.

Place the access list at:
Router Name: Router B
Interface: fa0/1
Access-list #: 1

[Writing and installing an ACL]

```
Router# configure terminal (or config t)

Router(config)# access-list-1 deny 172.20.70.89 0.0.0.0 192.168.122.128 0.0.0.0

                access-list-1 permit any any

Router(config)# interface fa0/1
Router(config-if)# ip access-group 1 [✓ in] or out (circle one)
Router(config-if)# exit
Router(config)# exit
Router# copy run start
```

c) Page 44 (Problem 5)



Extended Access List Problem #5 Deny/Permit Entire Ranges

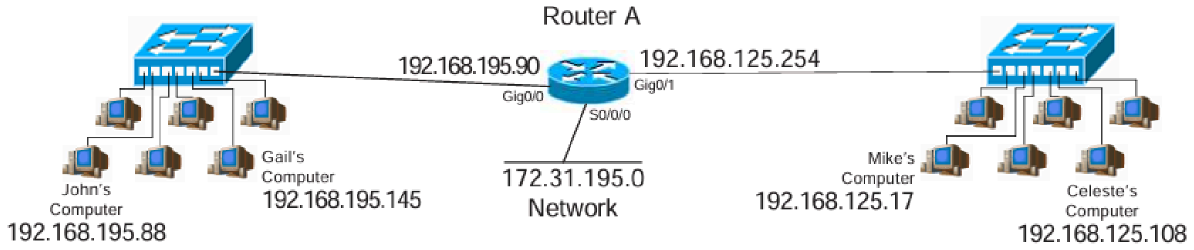
Include a remark with each statement of your ACL. Write an extended access list to permit network 204.95.150.0 to send packets to network 172.59.0.0, but not to the 210.250.10.0 network. Permit all other traffic. For help with the remark command review page 41. Keep in mind that there may be multiple ways many of the individual statements in an ACL can be written.

Place the access list at:
Router Name: Router A
Interface: fa0/0
Access-list #: 10

[Writing and installing an ACL]

Router# *configure terminal (or config t)*
Router(config)# access-list-10 remark Allow all the network 204.95.150.0 to send packet
access-list 10 permit 204.95.150.0 0.0.0.255 172.59.0.0 0.0.255.255
access-list 10 remark Not allow 204.95.150.0 send packet to 210.250.10.0
access-limit 10 deny 204.95.150.0 0.0.0.255 210.250.10.0 0.0.0.255
access-limit 10 permit any any
Router(config)# *interface* fa0/0
Router(config-if)# *ip access-group* 10 [✓ *in*] or *out* (circle one)
Router(config-if)# *exit*
Router(config)# *exit*

d) Page 50 (Problem 9)



Extended Access List Problem #9 Deny/Permit a Range of Addresses

Write an extended access list to prevent the first 31 usable addresses in the 192.168.125.0 network from reaching the 192.168.195.0 network. Permit all other traffic. Keep in mind that there may be multiple ways many of the individual statements in an ACL can be written.

Place the access list at:
Router Name: Router A
Interface: g0/1
Access-list #: 10

[Writing and installing an ACL]

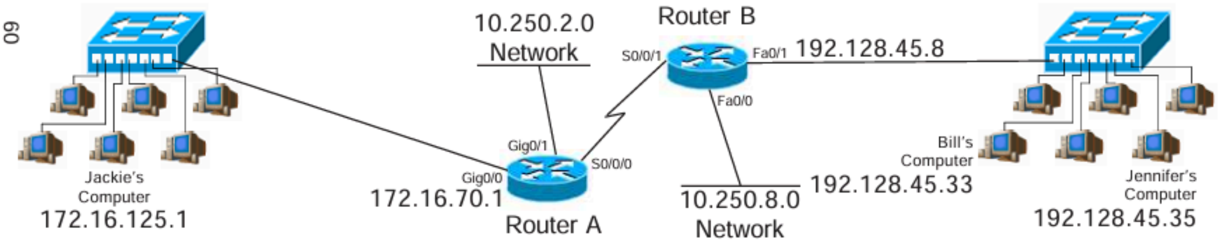
Router# *configure terminal (or config t)*

Router(config)# access-list 10 deny 192.168.125.0 0.0.0.32 192.168.195 0.0.0.0

access-list 10 permit any any

Router(config)# *interface* g0/0
Router(config-if)# *ip access-group* 10 [✓ *in*] or *out* (circle one)
Router(config-if)# *exit*

e) Page 60 (Problem 15)



Extended Access List Problem #15 Deny/Permit a Port Numbers

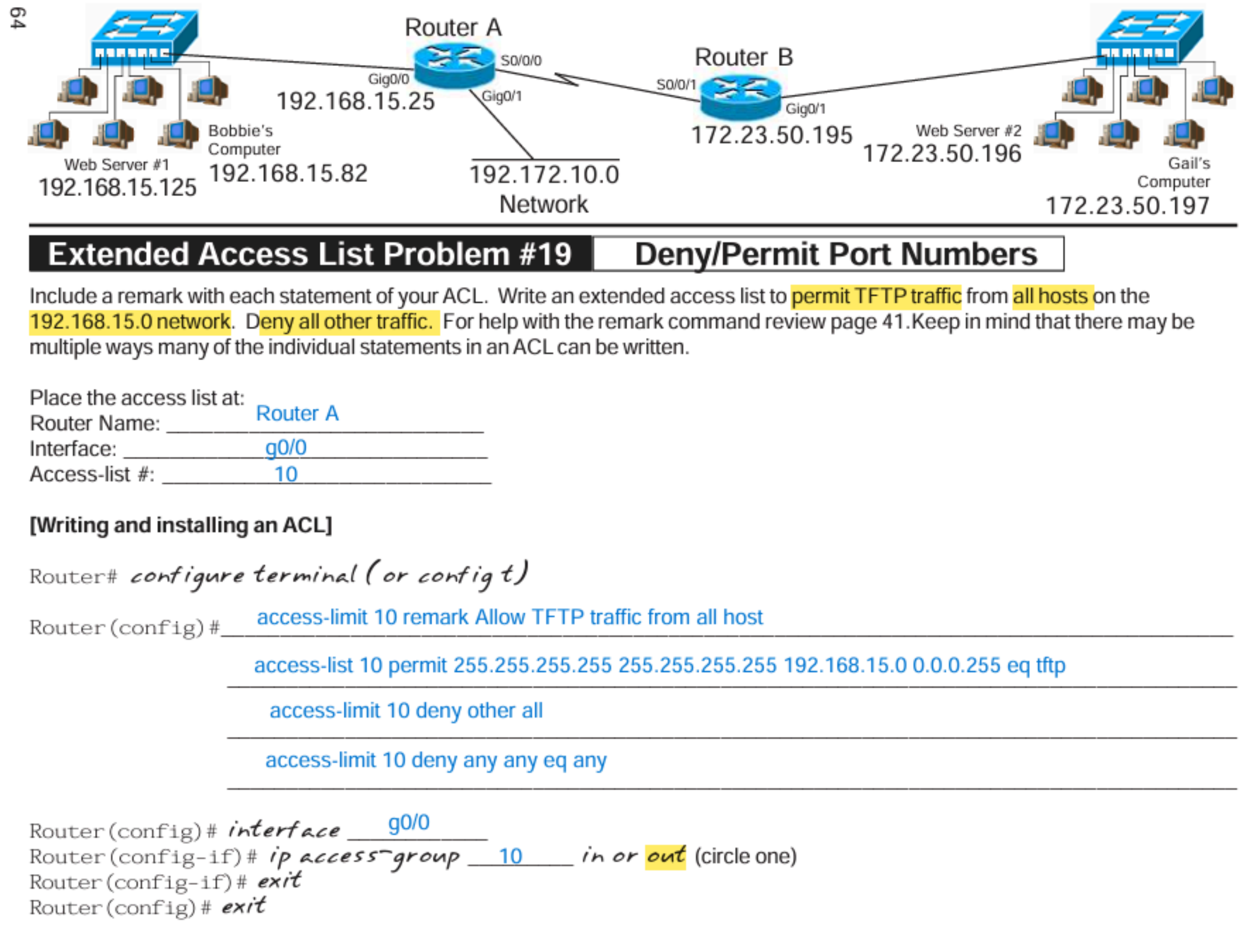
Write an extended access list to permit ICMP traffic from the 192.128.45.0 network to reach the 172.16.125.0 255.255.255.0 and 10.250.2.0 255.255.255.0 networks. Deny all other traffic. Keep in mind that there may be multiple ways many of the individual statements in an ACL can be written.

Place the access list at:
Router Name: Router B
Interface: fa0/1
Access-list #: 1

[Writing and installing an ACL]

```
Router# configure terminal (or config t)
Router(config)# access-list 1 permit 192.128.45.0 0.0.0.255 172.16.125.0 0.0.0.255 eq icmp
                access-list 1 deny any any



Router(config)# interface fa0/1
Router(config-if)# ip access-group 1 [✓ in] or out (circle one)
Router(config-if)# exit
```

f) Page 64 (Problem 64)


64
Router A
S0/0/0
Gig0/0
192.168.15.25
Gig0/1
Router B
S0/0/1
Gig0/1
172.23.50.195
Web Server #2
172.23.50.196
Gail's Computer
172.23.50.197
Bobbie's Computer
192.168.15.82
Web Server #1
192.168.15.125
192.172.10.0 Network

Extended Access List Problem #19 | Deny/Permit Port Numbers

Include a remark with each statement of your ACL. Write an extended access list to permit TFTP traffic from all hosts on the 192.168.15.0 network. Deny all other traffic. For help with the remark command review page 41.Keep in mind that there may be multiple ways many of the individual statements in an ACL can be written.

Place the access list at:
Router Name: Router A
Interface: g0/0
Access-list #: 10

[Writing and installing an ACL]

```
Router# configure terminal (or config t)

Router(config)# access-limit 10 remark Allow TFTP traffic from all host
                access-list 10 permit 255.255.255.255 255.255.255.255 192.168.15.0 0.0.0.255 eq tftp
                access-limit 10 deny other all
                access-limit 10 deny any any eq any

Router(config)# interface g0/0
Router(config-if)# ip access-group 10 in or [✓ out] (circle one)
Router(config-if)# exit
Router(config)# exit
```

Q3

3. a) Based on Figure 1-1, write an extended access list named **LOWER_NET** to allow first half of LAN_1 to ping hosts with odd numbered IP addresses in LAN_2. Deny all other traffic which must be explicitly written in your ACL. Use suitable keyword(s) in the ACL. Indicate the router, interface, and direction to apply the ACL.

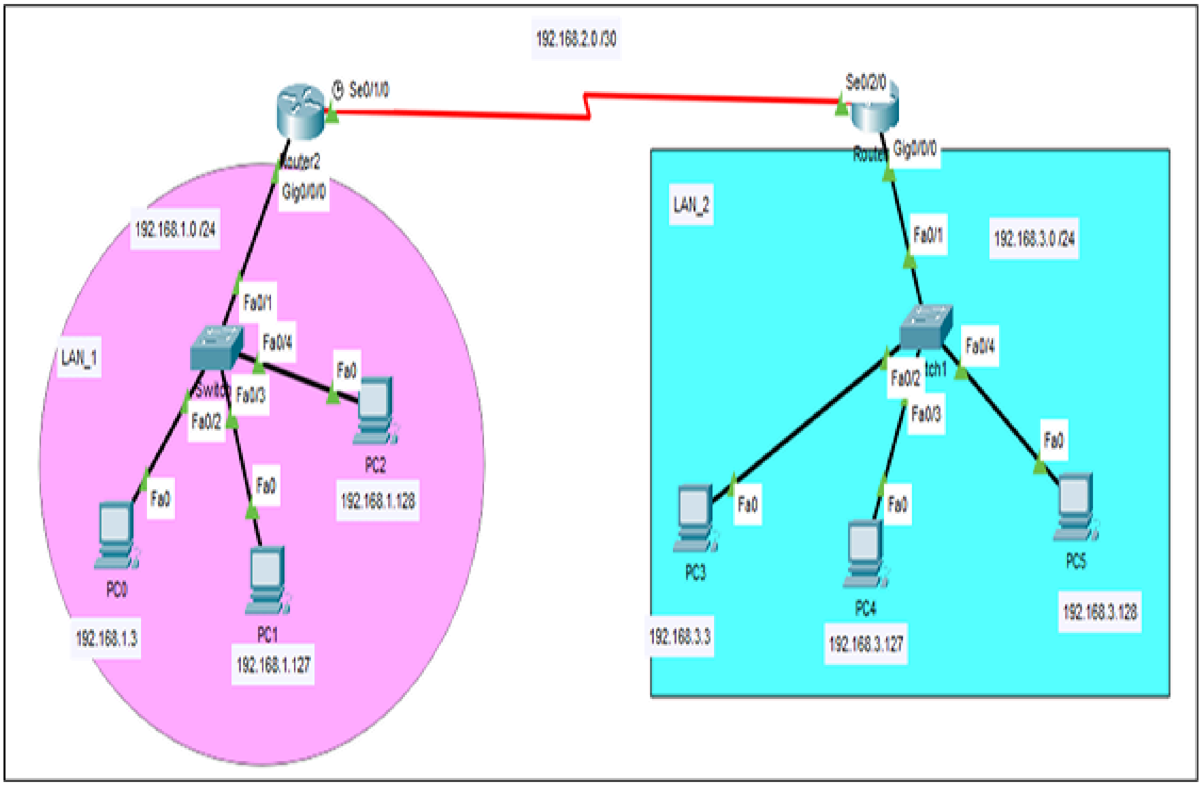


Figure 1-1: A network topology

Router: Router 2
Interface: g0/0/0
Access-list number: 100

```
ip access-list  extended LOWER_NET

permit ip 192.168.1.0 0.0.0.127 host 192.168.3.3
permit ip 192.168.1.0 0.0.0.127 host 192.168.3.127
deny ip any any
exit

interface g0/0/0
```

```
ip access-group LOWER_NET in
exit
exit
```

b) Based on Figure 1-2, write an extended access list named **UPPER_NET** to allow second half of LAN_4 to ping hosts with even numbered IP addresses in LAN_3. Deny all other traffic which must be explicitly written in your ACL. Use suitable keyword(s) in the ACL. Indicate the router, interface, and direction to apply the ACL.

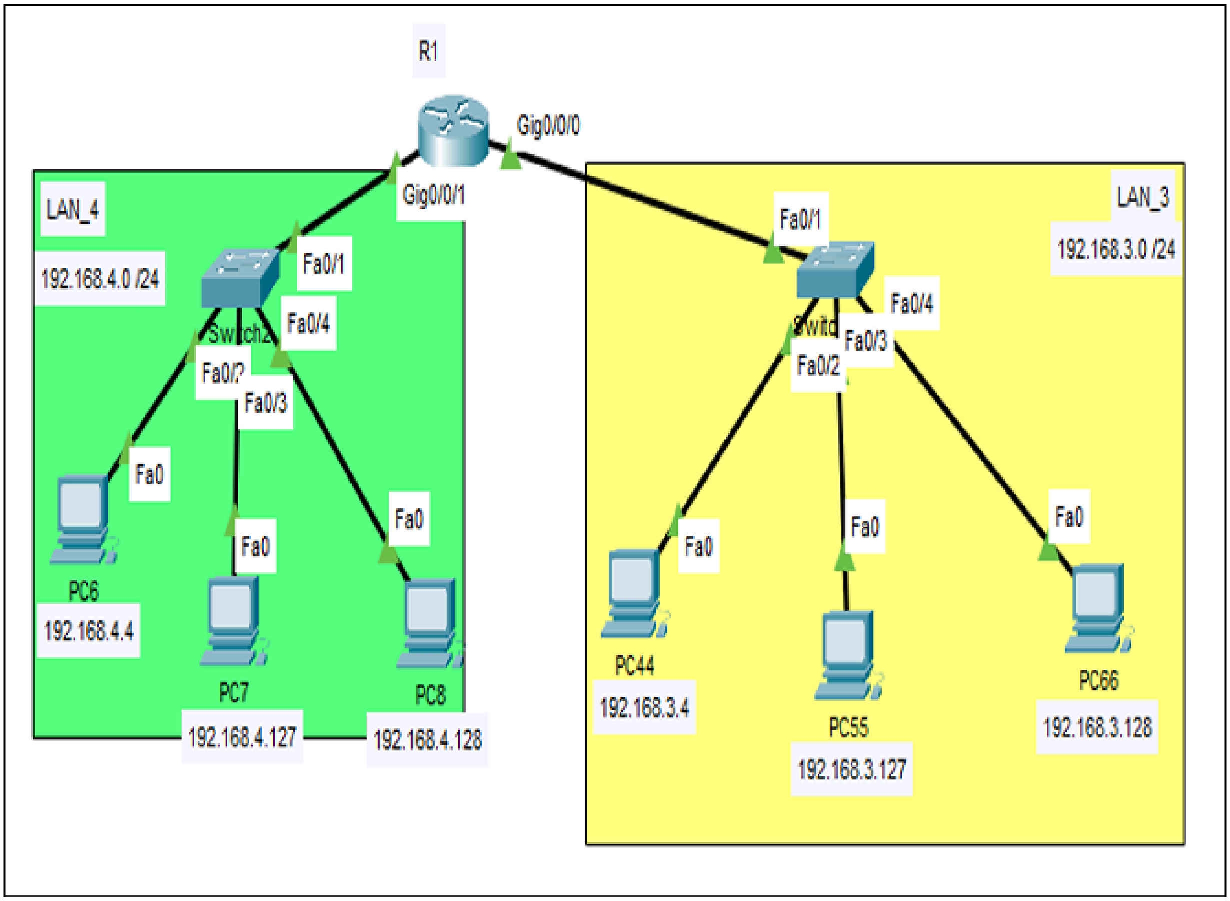


Figure 1-2: A network topology

Router: R1
Interface: g0/0/1
Access-list number: 100

```
ip access-list  extended UPPER_NET
```

```
permit ip 192.168.4.128 0.0.0.127 host 192.168.3.4
permit ip 192.168.4.128 0.0.0.127 host 192.168.3.128
deny ip any any
exit

interface g0/0/1
ip access-group UPPER_NET in
exit
exit
```

Q4

4. OSPF configurations were implemented in all routers and all PCs can communicate with each other in Figure 2-1 network topology. Answer the following questions.

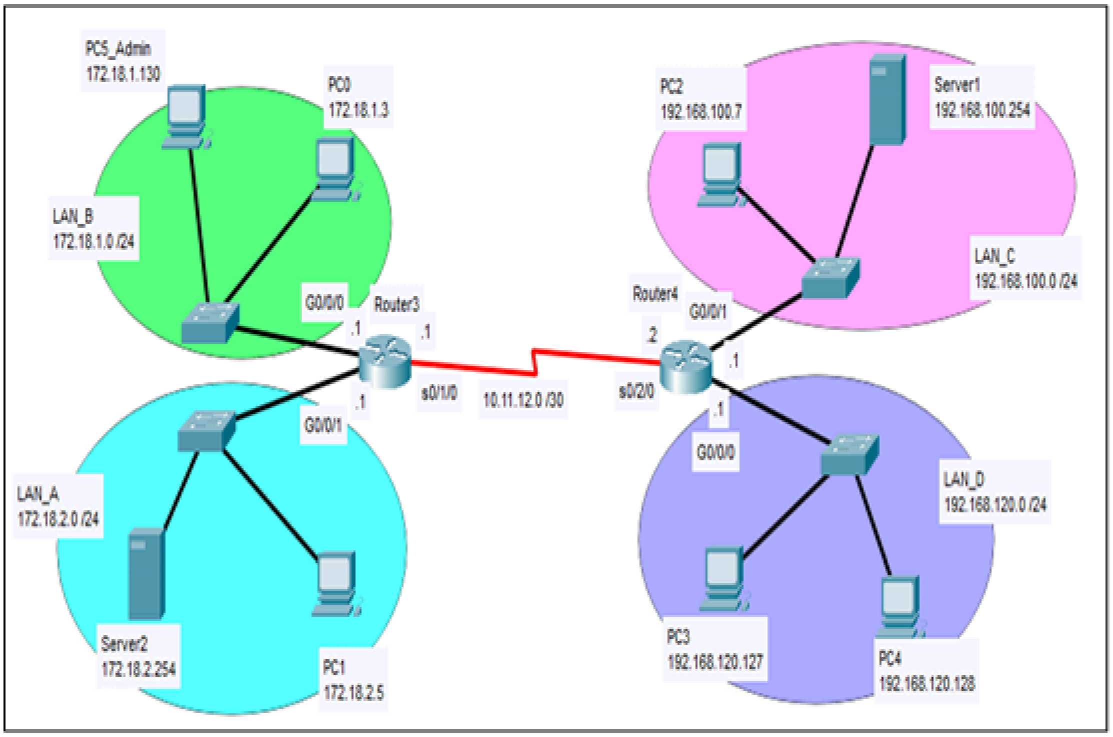
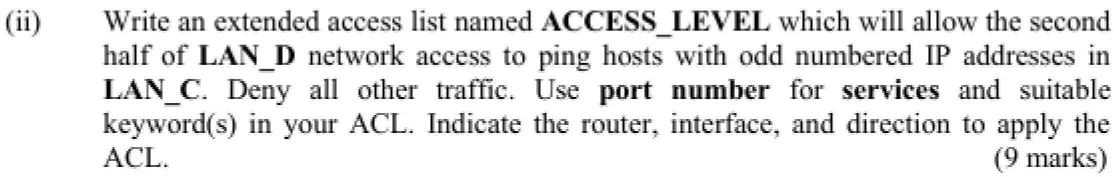


Figure 2-1: A network topology

(i) Write a standard access list numbered 13 to allow **PC5_Admin** to telnet into **Router3**. Deny all other traffic which must be explicitly written in your ACL. Use suitable keyword(s) in the ACL. Indicate the router, interface, and direction to apply the ACL. (6 marks)

Router: Router 3
interface: g0/0/0
access-list number: 13

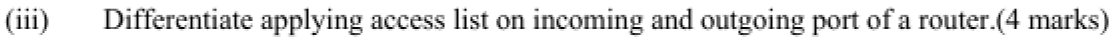
```
access-list 13 permit host 172.18.1.130
access-list 13 deny any any

interface g0/0/0
ip access-group 13 out
```



(ii) Write an extended access list named **ACCESS_LEVEL** which will allow the second half of **LAN_D** network access to ping hosts with odd numbered IP addresses in **LAN_C**. Deny all other traffic. Use **port number** for **services** and suitable keyword(s) in your ACL. Indicate the router, interface, and direction to apply the ACL. (9 marks)

Router: Router 4
interface: g0/0/0
access-list named: ACCESS_LEVEL

```
ip access-list extended ACCESS_LEVEL
permit ip 192.168.120.0 0.0.0.255 host 192.168.100.7
deny ip any any

interface g0/0/0
ip access-group ACCESS_LEVEL in
```



(iii) Differentiate applying access list on incoming and outgoing port of a router.(4 marks)

I guess

- *Apply on incoming port*
  - *filter all the packets that comes to the router*
  - *suitable when the port link which may receive the packet from only one network, as it will not affect the other network*
  - *For example, an extended access list can be applied on the incoming port of the router that as close as possible with the source to filter only the packets that send from a network.*
- *Apply on outcoming port*
  - *filter all the packets that leaving from the router*
  - *suitable when a router connects with two or more networks*
  - *The access-list will only filter the source IP when the packets leaving the router and going to the specific network.*

Q5

5. 202206 BMIT3094 pass year question

An enterprise will implement Access Control List (ACLs) to the router's interfaces to control and secure networks.

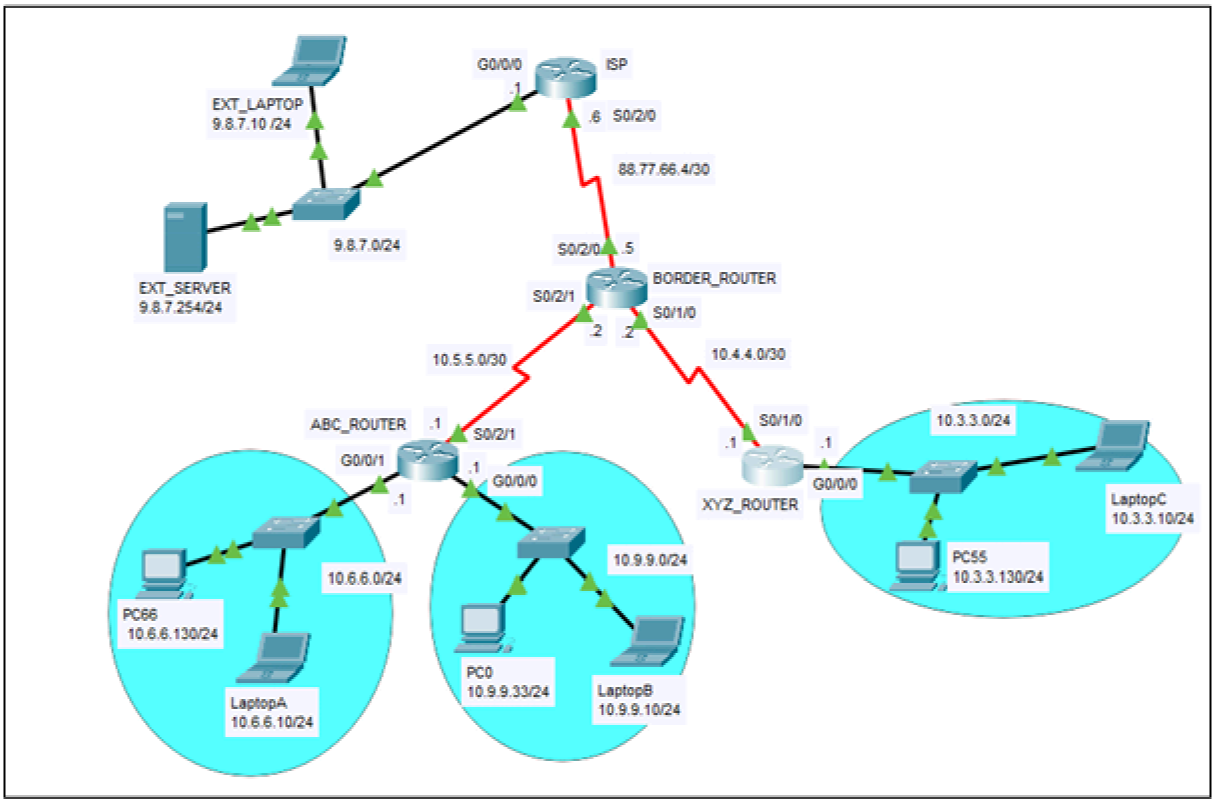


Figure 2-1: A network topology

Analyze Figure 2-1. The network topology has configured with OSPF configurations in all routers and all PCs can communicate with each other. Answer the following questions.

(i) Write an access list named **ACCESS_TELNET** to allow **LaptopC** to telnet into **XYZ_ROUTER**. Deny all other telnet traffics which must be explicitly written in your ACL. Use suitable keyword(s) in the ACL. Indicate the router, interface, and direction to apply the ACL. (6 marks)

Router: XYZ_Router
Interface: G0/0/0
Access list name: ACCESS_TELNET

```
ip access-list extended ACCESS_TELNET
permit tcp host 10.3.3.10 any eq 10
deny tcp ip any any eq 20
```

```
interface g0/0/0
ip access-group ACCESS_TELNET out
```

(ii) Write an extended access list numbered **148** to block **LaptopA** from accessing **EXT_SERVER** for **FTP (port 21)** services. Block the first 31 usable ip addresses in the 10.9.9.0 network to reach the **EXT_SERVER** for **HTTPS (port 443)** services. Permit all other traffics**.** Use **port number** for **services** and suitable keyword(s) in your ACL. Indicate the router, interface and direction to apply the ACL. (11 marks)

Router: ABC_Router
Interface: G0/0/1
Access list number: 148

```
access-list 148 deny tcp host 10.6.6.10 host 9.8.7.254 eq 21
access-list 148 deny tcp 10.9.9.0 0.0.0.31 host 9.8.7.254 eq 443
access-list 148 permit ip any any

interface g0/0/0
ip access-group 148 in
```

Q6

6. With reference to Figure 2-1, answer the following questions.

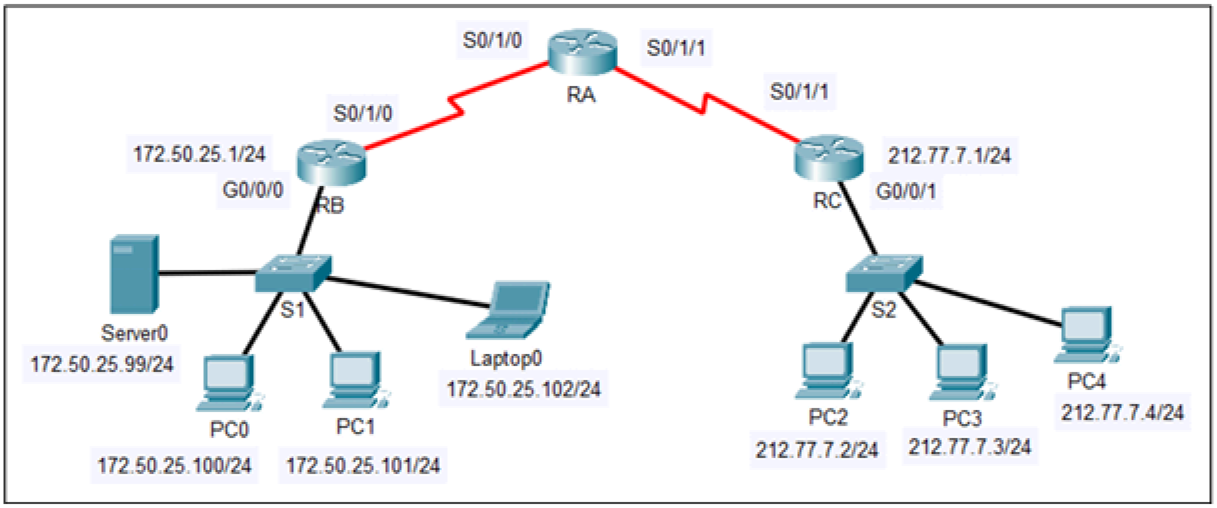


Figure 2-1: A network topology

(i) Write a standard numbered 55 access list to block 172.50.25.101 (PC1) and 172.50.25.102 (Laptop0) from sending information to the 212.77.7.0/24 network, but will allow all other traffic. Use **keyword** in your ACL. Indicate the router, interface and direction to apply the ACL

Router: RC
Interface: int g0/0/1
access list number: 55

```
access-limit 55 deny host 172.50.25.101 ip 212.77.7.0 0.0.0.255
access-limit 55 deny host 172.50.25.102 ip 212.77.7.0 0.0.0.255
access-limit 55 permit any any

interface g0/0/1
ip access-group 55 out
```

(ii) Write a standard named access list to permit traffic from the upper half of the 212.77.7.0/24 network to reach 172.50.25.0/24 network; block the lower half of the addresses. But allow only host 212.77.7.2 to reach network 172.50.25.0/24. Permit all other traffic.
The name of the standard ACL is **Permit_Upper.** Use **keyword** in your ACL. Indicate the router, interface and direction to apply the ACL

Router: RB
Interface: int g0/0/0
access list named: Permit_Upper

```
ip access-limit extended Permit_Upper
permit ip 212.77.7.0 0.0.0.127 ip 172.50.25.0 0.0.0.255
deny ip 212.77.7.128 0.0.0.127 ip 172.50.25.0 0.0.0.255
permit host 212.77.7.2 ip 172.50.25.0 0.0.0.255
permit ip any any

interface g0/0/1
ip access-group Permit_Upper out
```

(iii) Write an extended numbered 185 access list by using **keyword** to permit HTTP traffic from 212.77.7.0 network to web Server0 172.50.25.99 but deny first 15 usable addresses HTTP traffic in 212.77.7.0 network intended for web Server0 172.50.25.99. Deny all other traffic. Indicate the router, interface and direction to apply the ACL.

Router: RC
Interface: int g0/0/1
access list numbered: 185

```
access-list 185 deny tcp 212.77.7.1 0.0.0.15 host 172.50.25.99 eq www
access-list 185 permit tcp 212.77.7.0 0.0.0.255 host 172.50.25.99 eq www
access-list 185 deny any any

interface g0/0/1
ip access-group 185 in
```