

Any

0.0

# IPv4 Access Lists

Workbook

Version 2.0

permit

deny

access-group

access-list

Wildcard Mask

# Standard

Student Name:

Lim Jun Wei

### Standard ACL

- cover layer 3 only
- permit (allow) : permit <source ip>
- deny (block) : deny <source ip>

### Extended ACL

- extended to layer 3 & 4
- can filter by protocol
- involve source & destination address

## Access-List Numbers

IP Standard	1	to	99
IP Extended	100	to	199
Ethernet Type Code	200	to	299
Ethernet Address	700	to	799
DECnet and Extended DECnet	300	to	399
XNS	400	to	499
Extended XNS	500	to	599
Appletalk	600	to	699
48-bit MAC Addresses	700	to	799
IPX Standard	800	to	899
IPX Extended	900	to	999
IPX SAP (service advertisement protocol)	1000	to	1099
IPX SAP SPX	1000	to	1099
Extended 48-bit MAC Addresses	1100	to	1199
IPX NLSP	1200	to	1299
IP Standard, expanded range	1300	to	1999
IP Extended, expanded range	2000	to	2699
SS7 (voice)	2700	to	2999
Standard Vines	1	to	100
Extended Vines	101	to	200
Simple Vines	201	to	300
Transparent bridging (protocol type)	200	to	299
Transparent bridging (vendor type)	700	to	799
Extended Transparent bridging	1100	to	1199
Source-route bridging (protocol type)	200	to	299
Source-route bridging (vendor type)	700	to	799

Produced by: Robb Jones  
 Robert.Jones@fcps.org  
 Frederick County Career & Technology Center  
 Cisco Networking Academy  
 Frederick County Public Schools  
 Frederick, Maryland, USA

Special Thanks to Melvin Baker, Jim Dorsch, and Brent Sieling  
 for taking the time to check this workbook for errors, and making suggestions for improvements.

Instructors (and anyone else for that matter) please do not post the Instructors version on public websites.  
 When you do this you are giving everyone else worldwide the answers. Yes, students look for answers this way.  
 It also discourages others; myself included, from posting high quality materials.

## What are Access Control Lists?

ACLs...

...are a sequential list of instructions that tell a router which packets to permit or deny.

## General Access Lists Information

Access Lists...

...are read sequentially.

...are set up so that as soon as the packet matches a statement it stops comparing and permits or denies the packet.

...need to be written to take care of the most abundant traffic first.

...must be configured on your router before you can deny packets.

...can be written for all supported routed protocols; but each routed protocol must have a different ACL for each interface.

...must be applied to an interface to work.

## How routers use Access Lists

(Outbound Port - Default)

- ❑ The router checks to see if the packet is routable. If it is it looks up the route in its routing table.
- ❑ The router then checks for an ACL on that outbound interface.
- ❑ If there is no ACL the router switches the packet out that interface to its destination.
- ❑ If there is an ACL the router checks the packet against the access list statements sequentially. Then permits or denies each packet as it is matched.
- ❑ If the packet does not match any statement written in the ACL it is denied because there is an implicit “deny any” statement at the end of every ACL.

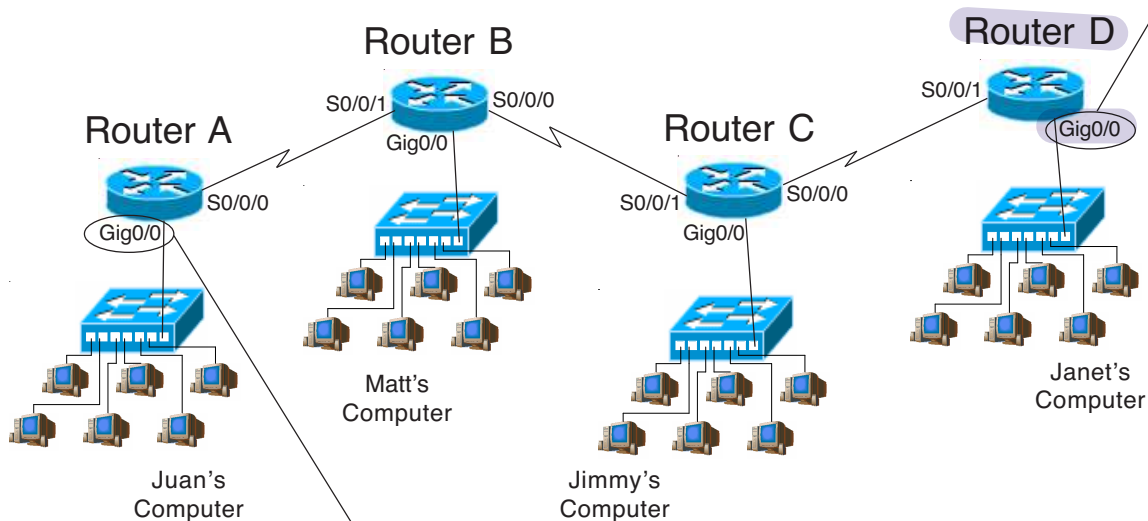
## Standard Access Lists

Standard Access Lists...

- ...are numbered from 1 to 99 or 1300 to 1999.
- ...filter (permit or deny) only source addresses.
- ...do not have any destination information so it must be placed as close to the destination as possible.
- ...work at layer 3 of the OSI model.

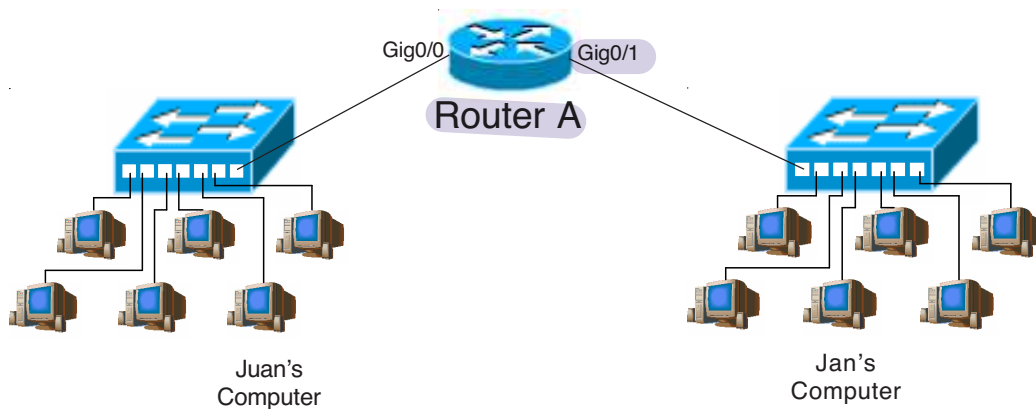
### Why standard ACLs are placed close to the destination.

If you want to block traffic from Juan's computer from reaching Janet's computer with a standard access list you would place the ACL **close to the destination** on Router D, interface Gig0/0. Since it's using only the source address to permit or deny packets the ACL here will not effect packets reaching Routers B, or C.

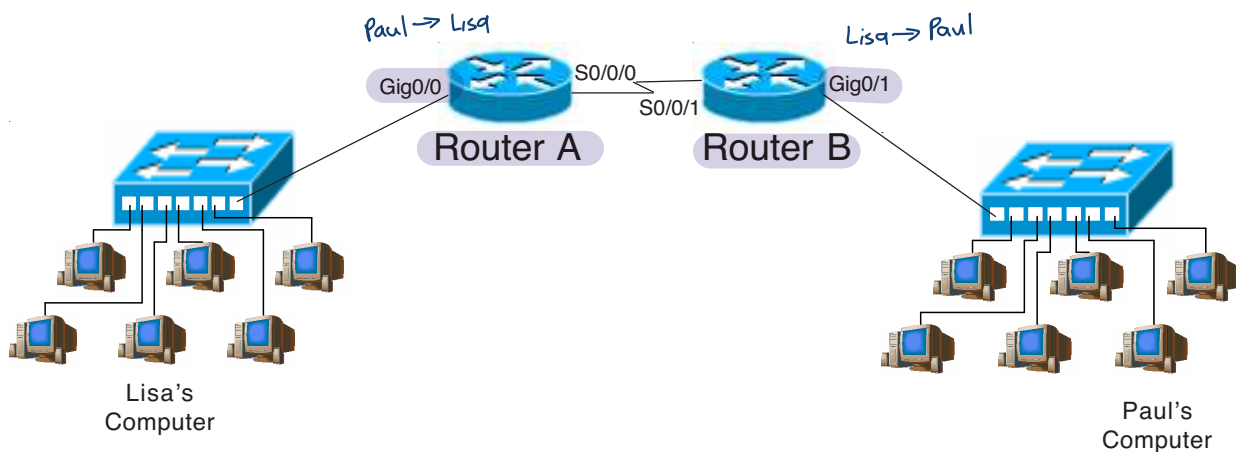


If you place the ACL on router A to block traffic to Router D it will also block all packets going to Routers B, and C; because all the packets will have the same source address.

## Standard Access List Placement Sample Problems



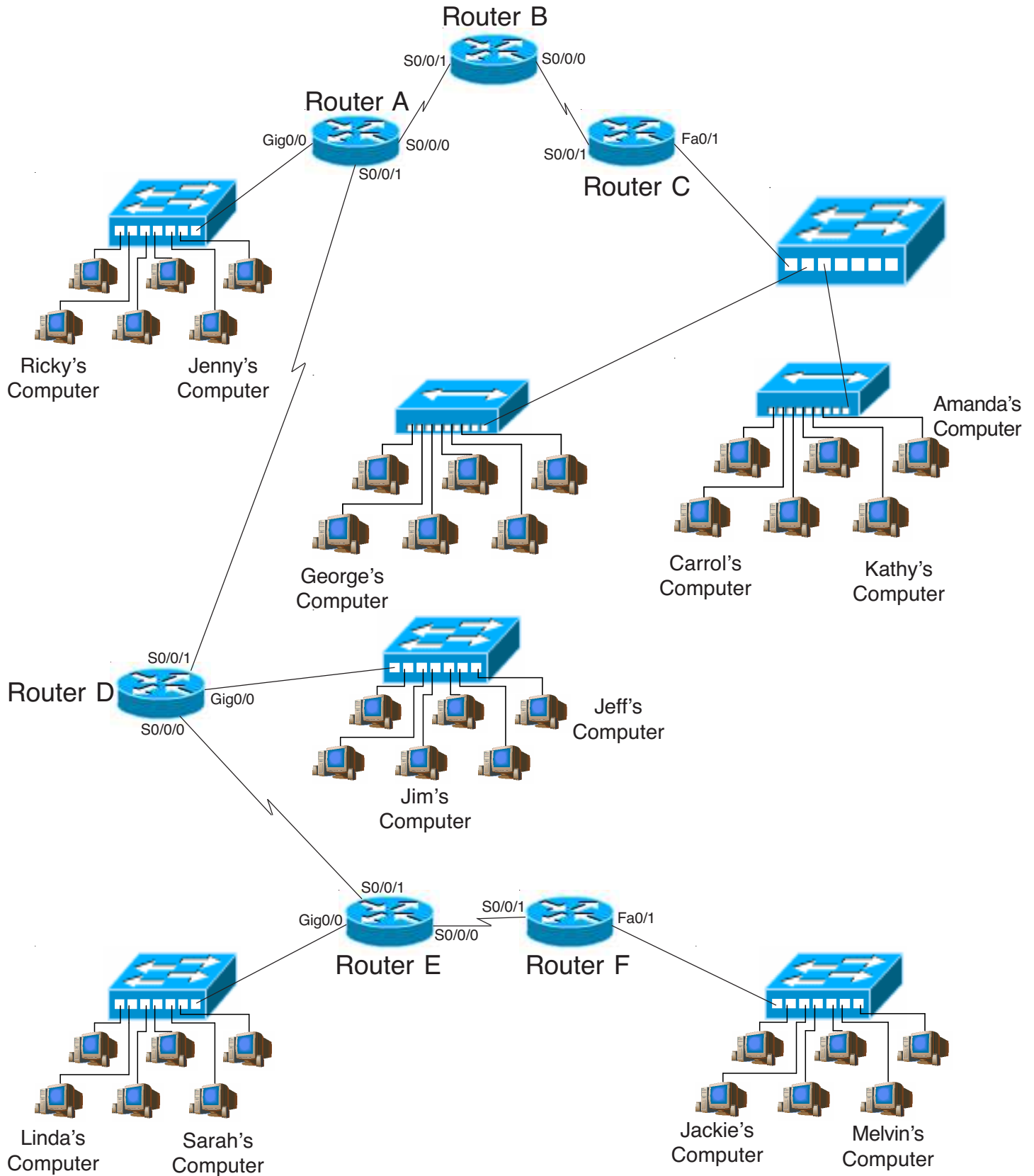
In order to permit packets from Juan's computer to arrive at Jan's computer you would place the standard access list at router interface Gig0/1.



Lisa has been sending unnecessary information to Paul. Where would you place the standard ACL to deny all traffic from Lisa to Paul?  
Router Name Router B Interface Gig0/1

Where would you place the standard ACL to deny traffic from Paul to Lisa?  
Router Name Router A Interface Gig0/0

# Standard Access List Placement



## 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 int g0/0  
Interface 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



## Extended Access Lists

Extended Access Lists...

...are numbered from 100 to 199 or 2000 to 2699.

...filter (permit or deny) based on the:

- source address
- destination address
- protocol
- application / port number

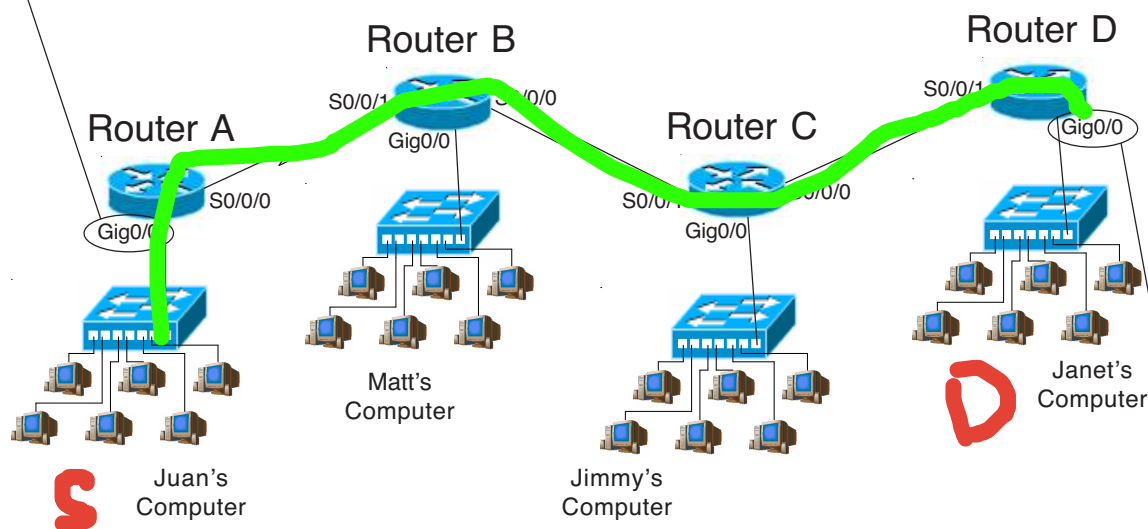
... are placed close to the source.

...work at both layer 3 and 4 of the OSI model.

TCP/UDP

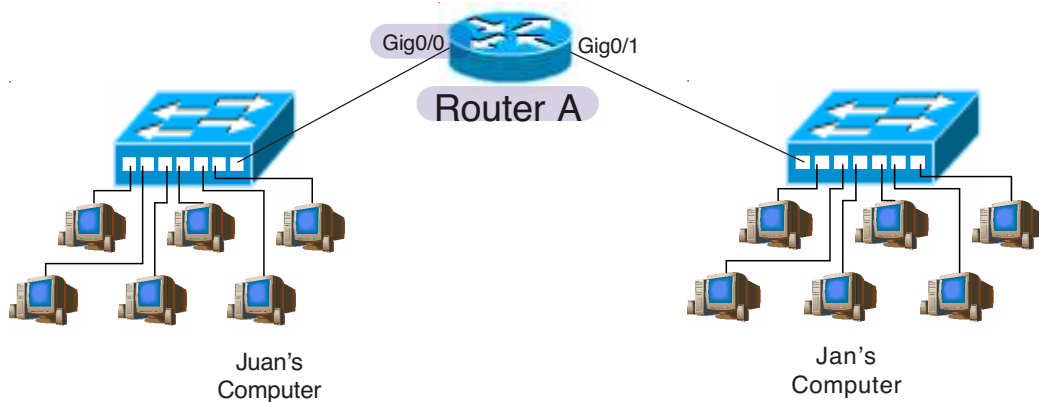
## Why extended ACLs are placed close to the source.

If you want to deny traffic from Juan's computer from reaching Janet's computer with an extended access list you would place the ACL close to the source on Router A, interface Gig0/0. Since it can permit or deny based on the destination address it can reduce backbone overhead and not affect traffic to Routers B or C.

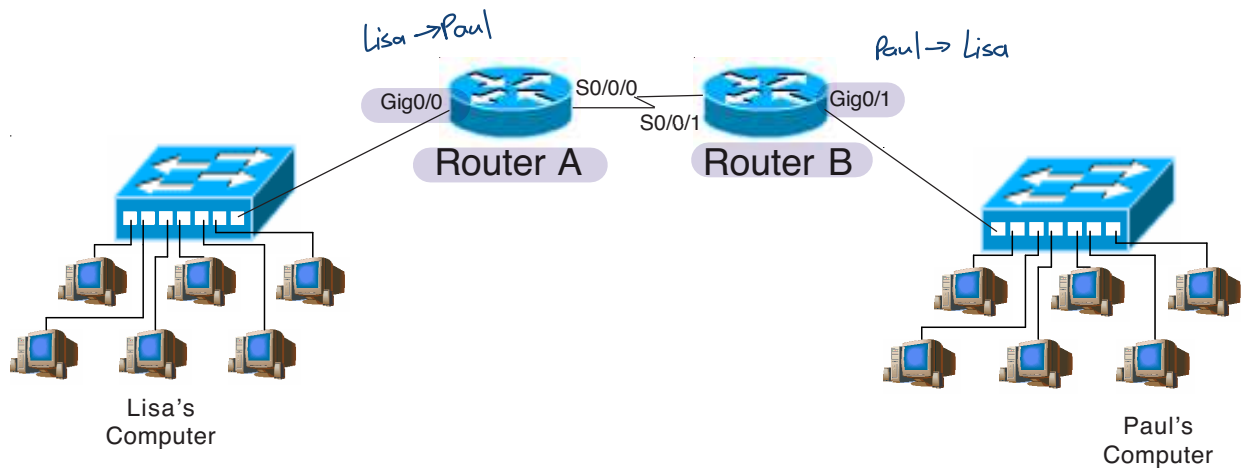


If you place the ACL on Router D to block traffic from Router A, it will work. However, Routers B and C will have to route the packet before it is finally blocked at Router D. This increases the volume of useless network traffic.

## Extended Access List Placement Sample Problems



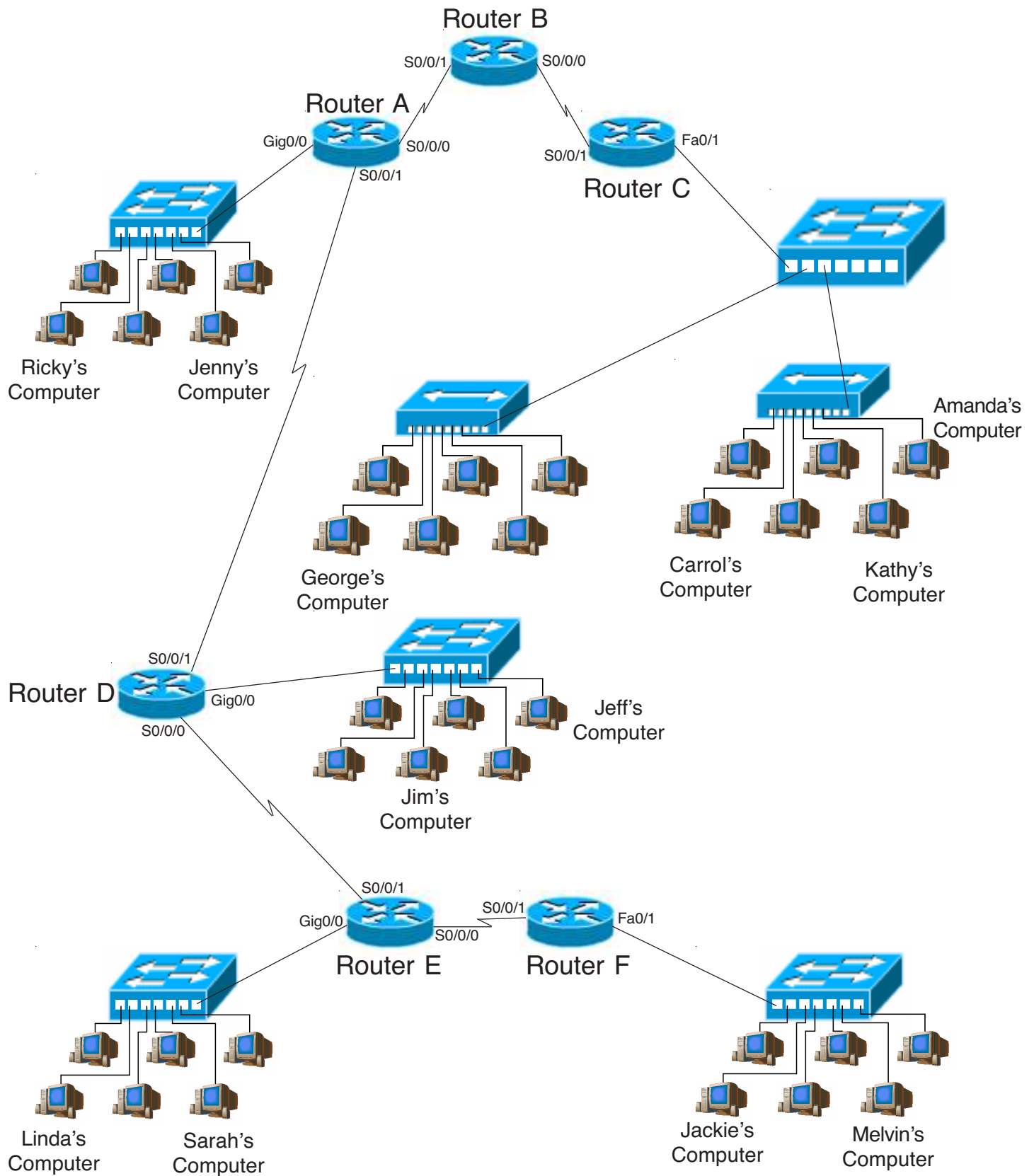
In order to permit packets from Juan's computer to arrive at Jan's computer you would place the extended access list at router interface Gig0/0.



Lisa has been sending unnecessary information to Paul. Where would you place the extended ACL to deny all traffic from Lisa to Paul?  
Router Name Router A Interface Gig0/0

Where would you place the extended ACL to deny traffic from Paul to Lisa?  
Router Name Router B Interface Gig0/1

## 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 Router A  
Interface g0/0 (in) 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 Router F  
Interface f0/1 fa0/1 (in)

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~~ Router C  
Interface ~~g0/0~~ fa0/1 (in)

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 (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

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)  
Router C  
fa0/1 (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 D  
Interface g0/0 (in)

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

Router Name Router E  
Interface g0/0 (in)

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

Router Name Router E  
Interface g0/0 (in)

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 C  
Interface fa0/1 (in)

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

Router Name Router E  
Interface g0/0 (in)

## Choosing to Filter Incoming or Outgoing Packets

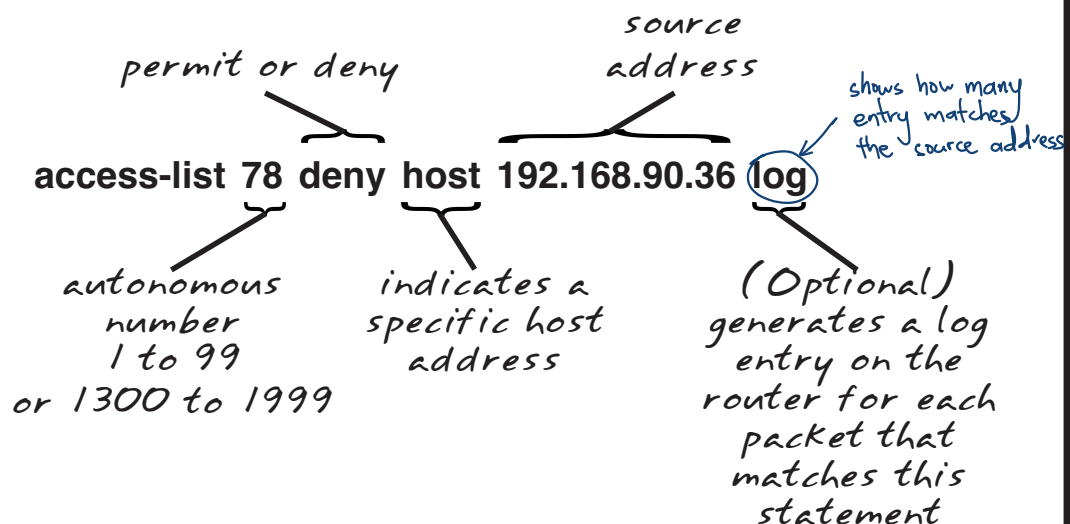
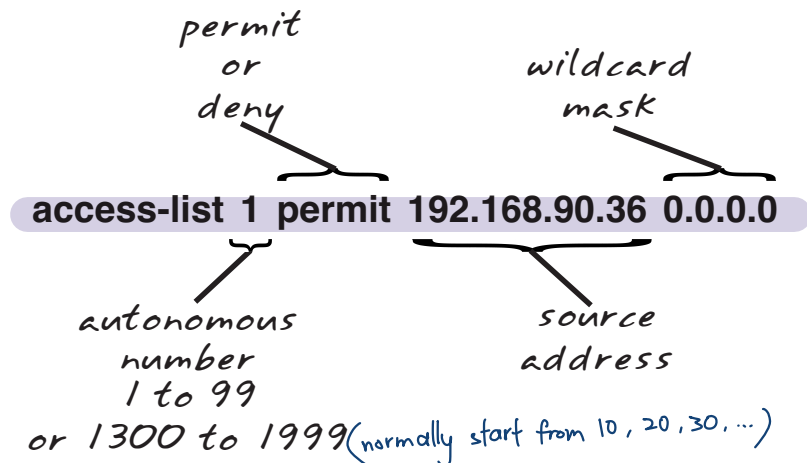
Access Lists on your incoming port...

- ...requires less CPU processing.
- ...filters and denies packets before the router has to make a routing decision.

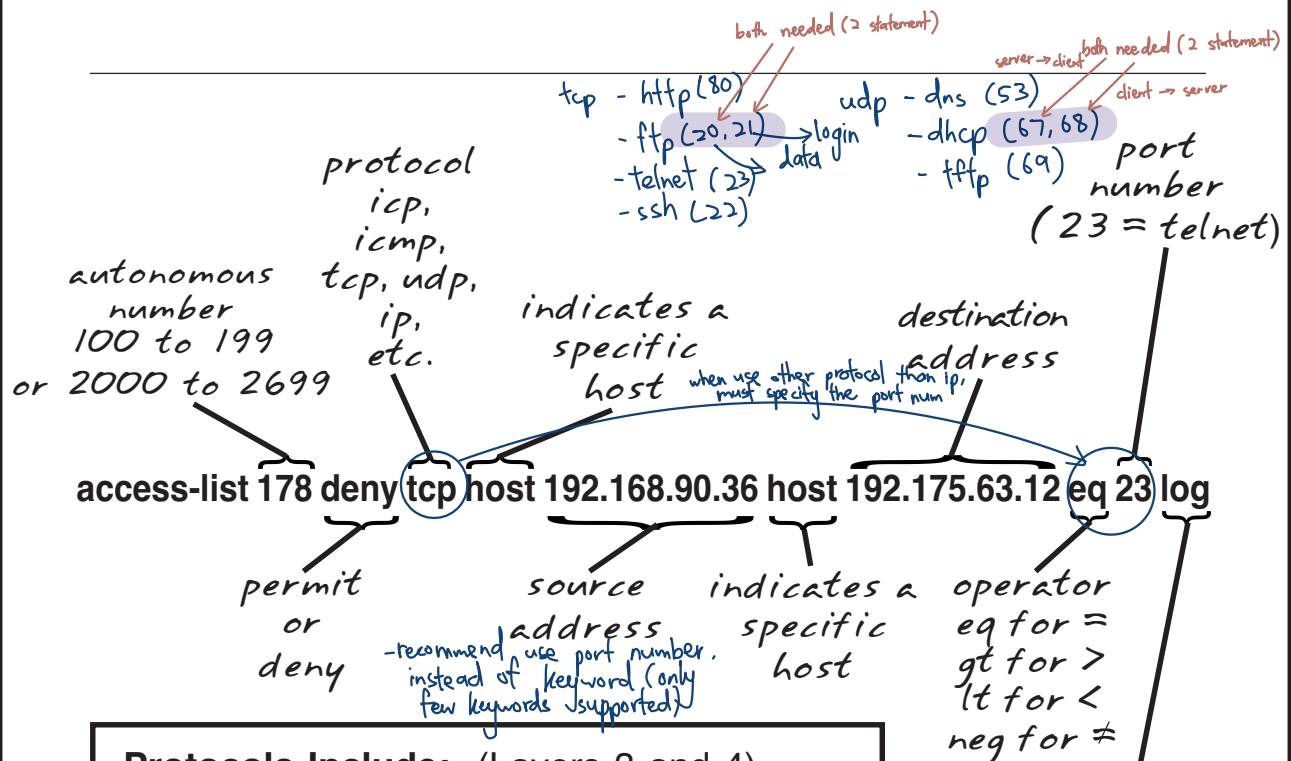
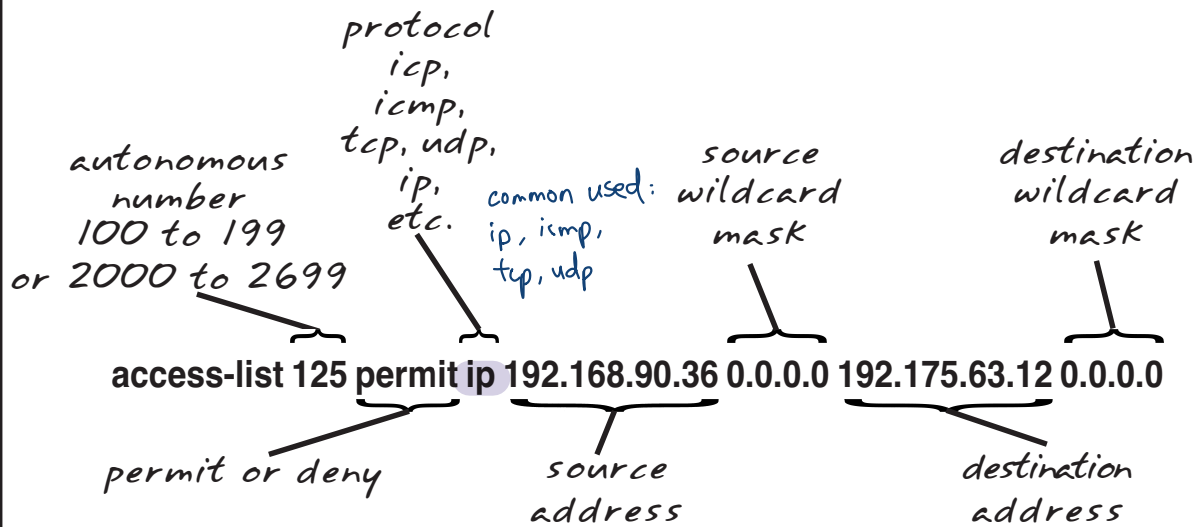
Access Lists on your outgoing port...

- ...are outbound by default unless otherwise specified.
- ...increases the CPU processing time because the routing decision is made and the packet switched to the correct outgoing port before it is tested against the ACL.

## Breakdown of a Standard ACL Statement



## Breakdown of an Extended ACL Statement



### Protocols Include: (Layers 3 and 4)

IP	IGMP	IPINIP
TCP	GRE	OSPF
UDP	IGRP	NOS
ICMP	EIGRP	Integer 0-255

To match any internet protocol use IP.

## What are Named Access Control Lists?

Named ACLs...

...are standard or extended ACLs which have an alphanumeric name instead of a number. (ie. 1-99 or 100-199)

## Named Access Lists Information

Named Access Lists...

- ...identify ACLs with an intuitive name instead of a number.
- ...eliminate the limits imposed by using numbered ACLs.  
(798 for standard and 799 for extended)
- ...names should be typed in all CAPS to make it easier to see.
- ...provide the ability to modify your ACLs without deleting and reloading the revised access list. It will only allow you to add statements to the end of the existing statements.
- ...are not compatible with any IOS prior to Release 11.2.
- ...can not repeat the same name on multiple ACLs.

## Applying a Standard Named Access List called "GEORGE"

Write a named standard access list called "GEORGE" on Router A, interface E1 to block Melvin's computer from sending information to Kathy's computer; but will allow all other traffic.

Place the access list at:

Router Name: Router A

Interface: E1

Access-list Name: GEORGE

### [Writing and installing an ACL]

```
Router# configure terminal (or config t)
Router(config)# ip access-list standard GEORGE
Router(config-std-nacl)# deny host 72.16.70.35
Router(config-std-nacl)# permit any
Router(config-std-nacl)# interface gig0/1
Router(config-if)# ip access-group george out
Router(config-if)# exit
Router(config)# exit
```

## Applying an extended Named Access List called "GRACIE"

Write a named extended access list called "GRACIE" on Router A, Interface E0 called "Gracie" to deny HTTP traffic intended for web server 192.168.207.27, but will permit all other HTTP traffic to reach the only the 192.168.207.0 network. Deny all other IP 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: E0  
Access-list Name: GRACIE

### [Writing and installing an ACL]

```
Router# configure terminal (or config t)
Router(config)# ip access-list extended GRACIE
Router(config-ext-nacl)# deny tcp any host 192.168.207.27 eq www
Router(config-ext-nacl)# permit tcp any 192.168.207.0 0.0.0.255 eq www
Router(config-ext-nacl)# interface gig0/1
Router(config-if)# ip access-group gracie in
Router(config-if)# exit
Router(config)# exit
```



## Choices for Using Wildcard Masks

**Wildcard masks are usually set up to do one of four things:**

1. Match a specific host.
2. Match an entire subnet.
3. Match a specific range.
4. Match all addresses.

### 1. Matching a specific host.

**For standard access lists:**

Access-List 10 permit 192.168.150.50 0.0.0.0

or

Access-List 10 permit 192.168.150.50 (standard ACL's  
assume a 0.0.0.0 mask)

or

Access-List 10 permit host 192.168.150.50

↖ keyword

**For extended access lists:**

Access-list 110 deny ip 192.168.150.50 0.0.0.0 any

or

Access-list 110 deny ip host 192.168.150.50 any

### 2. Matching an entire subnet

**Example 1**

Address: 192.168.50.0 Subnet Mask: 255.255.255.0

Access-list 25 deny 192.168.50.0 0.0.0.255

**Example 2**

Address: 172.16.0.0 Subnet Mask: 255.255.0.0

Access-list 12 permit 172.16.0.0 0.0.255.255

**Example 3**

Address: 10.0.0.0 Subnet Mask: 255.0.0.0

Access-list 125 deny udp 10.0.0.0 0.255.255.255 any

### 3. Match a specific range

#### Example 1

wildcard : 0 → must match exactly  
1 → can ignore (wildcard)

Address: 10.250.50.112 Subnet Mask: 255.255.255.224

255.255.255.255

Custom Subnet mask: -255.255.255.224

Wildcard: 0. 0. 0. 31

Access-list 125 permit udp 10.250.50.112 0.0.0.31 any

#### Example 2

Address Range: 192.168.16.0 to 192.168.16.127

192.168.16.0  
⋮

192.168.16.127

-192.168.16. 0

Wildcard: 0. 0. 0.127

0. 0. 0. 127 → wildcard  
↓ ↓ ↓  
must match

Access-list 125 deny ip 192.168.16.0 0.0.0.127 any  
(This ACL would block the lower half of the subnet.)

#### Example 3

Address: 172.250.16.32 to 172.250.31.63

172.250.16.32  
⋮

0001 0000 . 0010 0000

172.250.31. 63

-172.250.16. 32

172.250.31.63

0001 1111 . 0011 1111

Wildcard: 0. 0.15. 31

0. 0. 15. 31

0000 1111 . 0001 1111

15 . 31

Access-list 125 permit ip 172.250.16.32 0.0.15.31 any

### 4. Match everyone.

#### For standard access lists:

Access-List 15 permit any

or

Access-List 15 deny 0.0.0.0 255.255.255.255

#### For extended access lists:

Access-List 175 permit ip any any

or

Access-List 175 deny tcp 0.0.0.0 255.255.255.255 any

## Creating Wildcard Masks

- ❑ Just like a subnet mask the wildcard mask tells the router what part of the address to check or ignore. Zero (0) must match exactly, one (1) will be ignored.
- ❑ The source address can be a single address, a range of addresses, or an entire subnet.
- ❑ As a rule of thumb the wildcard mask is the inverse of the subnet mask.

Example #1:

IP Address and subnet mask: 204.100.100.0 255.255.255.0

IP Address and wildcard mask: 204.100.100.0 0.0.0.255

- ❑ All zero's (or 0.0.0.0) means the address must match exactly.

Example #2:

10.10.150.95 0.0.0.0 (This address must match exactly.)

- ❑ One's will be ignored.

Example #3:

10.10.150.95 0.0.0.255 (Any 10.10.150.0 subnet address will match.  
10.10.150.0 to 10.10.150.255)

- ❑ This also works with subnets.

Example #4:

IP Address and subnet mask: 192.170.25.30 255.255.255.224

IP Address and wildcard mask: 192.170.25.30 0.0.0.31  
(Subtract the subnet mask from  
255.255.255.255 to create the wildcard)

Do the math...  $255 - 255 = 0$  (This is the inverse of the subnet mask.)  
 $255 - 224 = 31$

Example #5:

IP Address and subnet mask: 172.24.128.0 255.255.128.0

IP Address and wildcard mask: 172.24.128.0 0.0.127.255

Do the math...  $255 - 255 = 0$  (This is the inverse of the subnet mask.)  
 $255 - 128 = 127$   
 $255 - 0 = 255$

# 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
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  

0.0.0.0    0.0.0.0
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    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    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  

0.0.0.0    0.0.0.0
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    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    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  

0.0.0.0    0.0.0.0
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    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    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    0.0.0.7

## Basic Wildcard Mask Problems

Based on the given information list the range of **source addresses** for each ACE statement.

1. access-list 10 permit **192.168.150.50 0.0.0.0**

Answer: 192.168.150.50

2. access-list 5 permit **any**

Answer: Any address

3. access-list 125 deny tcp **195.223.50.0 0.0.0.63** host 172.168.10.1 fragments

Answer: 195.223.50.0 to 195.223.50.63

4. access-list 11 deny **210.10.10.0 0.0.0.255**

Answer: 210.10.10.0 - 210.10.10.255 210.10.10.0 - 210.10.10.255

5. access-list 108 deny ip **192.220.10.0 0.0.0.15** 172.32.4.0 0.0.0.255

Answer: 192.220.10.0 - 192.220.10.15 192.220.10.0 - 192.220.10.15

6. access-list 171 deny any host 175.18.24.10 fragments

Answer: Any address Any address

7. access-list 105 permit 192.168.15.0 0.0.0.255 any

Answer: 192.168.15.0 - 192.168.15.255

8. access-list 109 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq 80

Answer: 172.16.10.0 - 172.16.10.255

9. access-list 111 permit ip any any

Answer: Any address

10. access-list 195 permit udp 172.30.12.0 0.0.0.127 172.50.10.0 0.0.0.255

Answer: 172.30.12.0 - 172.30.12.127

11. **access-list 110 permit ip 192.168.15.0 0.0.0.3 192.168.30.10 0.0.0.0**

Answer: 192.168.15.0 - 192.168.15.3

12. **access-list 120 permit ip 192.168.15.0 0.0.0.7 192.168.30.10 0.0.0.0**

Answer: 192.168.15.0 - 192.168.15.7

13. **access-list 130 permit ip 192.168.15.0 0.0.0.15 192.168.30.10 0.0.0.0**

Answer: 192.168.15.0 - 192.168.15.15

14. **access-list 140 permit ip 192.168.15.0 0.0.0.31 192.168.30.10 0.0.0.0**

Answer: 192.168.15.0 - 192.168.15.31

15. **access-list 150 permit ip 192.168.15.0 0.0.0.63 192.168.30.10 0.0.0.0**

Answer: 192.168.15.0 - 192.168.15.63

16. **access-list 101 Permit ip 192.168.15.0 0.0.0.127 192.168.30.10 0.0.0.0**

Answer: 192.168.15.0 - 192.168.15.127

17. **access-list 185 permit ip 192.168.15.0 0.0.0.255 192.168.30.0 0.0.0.255**

Answer: 192.168.15.0 - 192.168.15.255

18. **access-list 160 deny udp 172.16.0.0 0.0.1.255 172.18.10.18 0.0.0.0 gt 22**

Answer: 172.16.0.0 - 172.16.1.255

19. **access-list 195 permit icmp 172.85.0.0 0.0.15.255 172.50.10.0 0.0.0.255**

Answer: 172.85.0.0 - 172.85.15.255

20. **access-list 10 permit 175.15.120.0 0.0.0.255**

Answer: 175.15.120.0 - 175.15.120.255

21. **access-list 190 permit tcp 192.15.10.0 0.0.0.31 any**

Answer: 192.15.10.0 - 192.15.10.31

22. **access-list 100 permit ip 10.0.0.0 0.255.255.255 172.50.10.0 0.0.0.255**

Answer: 10.0.0.0 - 10.255.255.255

## (Slightly More) **Advanced Wildcard Mask Problems**

Not every address range ends with a zero making it simple to determine the address range. Using basic subnetting you can adjust the host portion of the IP address with the wildcard mask to indicate specific ranges.

IP Address: 192 . 100 . 10 . 0  
Custom Subnet Mask: 255.255.255.240

Address Ranges: 192.100.10.0 to 192.100.10.15  
192.100.10.16 to 192.100.10.31  
192.100.10.32 to 192.100.10.47 (Range in the sample below)  
192.100.10.48 to 192.100.10.63  
192.100.10.64 to 192.100.10.79  
192.100.10.80 to 192.100.10.95  
192.100.10.96 to 192.100.10.111  
192.100.10.112 to 192.100.10.127  
192.100.10.128 to 192.100.10.143  
192.100.10.144 to 192.100.10.159  
192.100.10.160 to 192.100.10.175  
192.100.10.176 to 192.100.10.191  
192.100.10.192 to 192.100.10.207  
192.100.10.208 to 192.100.10.223  
192.100.10.224 to 192.100.10.239  
192.100.10.240 to 192.100.10.255

Based on this sample to deny or permit the third subnet we would create the correct wildcard mask by inverting the subnet mask from 255.255.255.240 to 0.0.0.15. The third address range would be 192.100.10.32 to 192.100.10.47 .

A standard ACE statement would be written as:

**access-list 10 permit 192.100.10.32 0.0.0.15**

The wildcard mask indicates that address range 0 to 15 will be permitted. If the source address was 192.100.10.**0** it would indicate the first 16 addresses (0 to 15). Since the source address is 192.100.10.**32**, it indicates that the address range will be from 192.100.10.**32** to 192.100.10.**47** (32 to 47). The IP address indicates the starting point for the wildcard mask to begin counting up from.

This technique gives you greater control with the addresses you want to permit or deny. It is a **Best Practice** to stay within standard address ranges.

Based on the given information list the range of source addresses for each ACE statement.

1. access-list 10 permit 192.100.10.64 0.0.0.15

Answer: 192.100.10.64 to 192.100.10.79

2. access-list 5 permit 172.16.128.0 0.0.63.255

Answer: 172.16.128.0 to 172.16.191.255

3. access-list 125 deny tcp 192.100.10.208 0.0.0.15 host 192.168.10.1 log

Answer: 192.100.10.208 to 192.100.10.223

4. access-list 11 deny 210.48.72.192 0.0.0.31

Answer: 210.48.72.192 to 210.48.72.223

5. access-list 108 deny ip 192.168.5.184 0.0.0.7 192.64.4.0 0.0.0.255

Answer: 192.168.5.184 to 192.168.5.191

6. access-list 171 deny 172.32.128.0 0.0.15.255 any

Answer: 172.32.128.0 to 172.32.143.255

7. access-list 105 permit 165.50.196.0 0.0.3.255 any

Answer: 165.50.196.0 to 165.50.199.255

8. access-list 109 permit tcp 172.16.128.0 0.0.127.255 host 172.16.20.1

Answer: 172.16.128.0 to 172.16.255.255

9. access-list 111 permit ip 192.168.1.236 0.0.0.3 any

Answer: 192.168.1.236 to 192.168.1.239

10. access-list 195 permit udp 172.32.160.0 0.0.31.255 172.100.10.0 0.0.0.255

Answer: 172.32.160.0 to 172.32.191.255

11. access-list 110 permit ip 10.64.0.0 0.63.255.255 172.168.40.10 0.0.0.0

Answer: 10.64.0.0 to 10.127.255.255



## Wildcard Mask Problems

Based on the given information list the range of destination addresses for each ACE statement.

1. **access-list 125 deny tcp 195.223.50.0 0.0.0.63 host 172.168.10.1 fragments**

Answer: 172.168.10.1

2. **access-list 115 permit any any**

Answer: Any address

3. **access-list 150 permit ip 192.168.30.10 0.0.0.0 192.168.15.0 0.0.0.63**

Answer: 192.168.15.0 to 192.168.15.63

4. **access-list 120 deny tcp 172.32.4.0 0.0.0.255 192.220.10.0 0.0.0.15**

Answer: 192.220.10.0 to 192.220.10.15

5. **access-list 108 deny ip 192.220.10.0 0.0.0.15 172.32.4.0 0.0.0.255**

Answer: 172.32.4.0 to 172.32.4.255

6. **access-list 101 deny ip 140.130.110.100 0.0.0.0 0.0.0.0 255.255.255.255**

Answer: Any address

7. **access-list 105 permit any 192.168.15.0 0.0.0.255**

Answer: 192.168.15.0 to 192.168.15.255

8. **access-list 120 permit ip 192.168.15.10 0.0.0.0 172.16.40.0 0.0.3.255**

Answer: 172.16.40.0 to 172.16.43.255

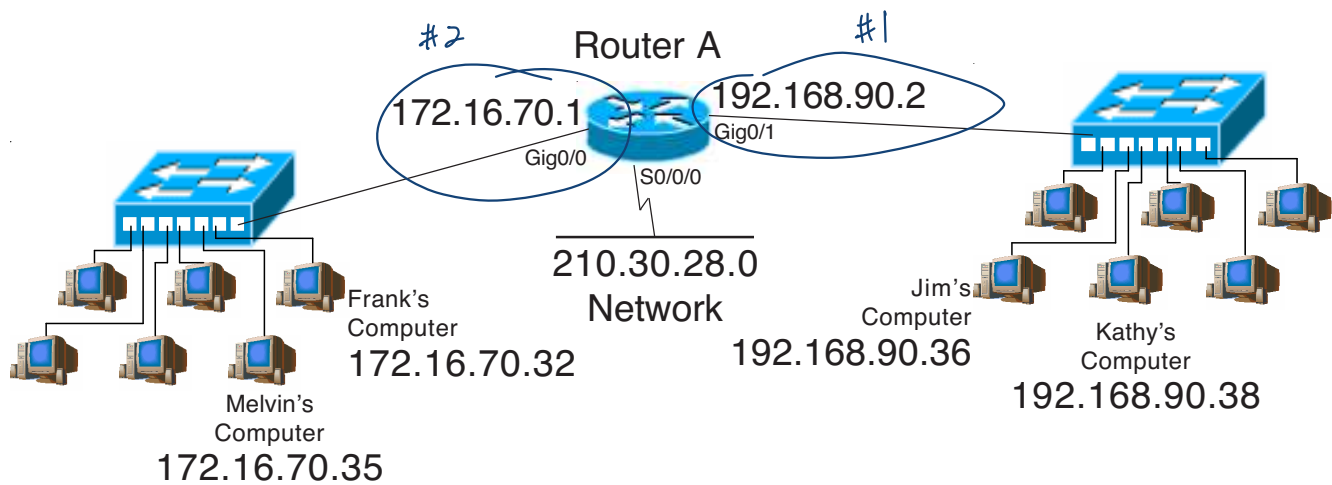
9. **access-list 160 deny udp 172.16.0.0 0.0.1.255 172.18.104.0 0.0.7.255 eq 21**

Answer: 172.18.104.0 to 172.18.110.255

10. **access-list 150 permit ip 192.168.30.0 0.0.0.63 192.168.15.96 0.0.0.31**

Answer: 192.168.15.96 to 192.168.15.127

# **Writing Standard Access Lists...**



## Standard Access List Sample #1

Write a standard access list to block Melvin's computer from sending information to Kathy's computer; 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 A  
 Interface: Gig0/1  
 Access-list #: 10

### Note:

A standard access list blocks only the source address. Melvin will also be blocked from sending information to Jim or anyone else on the 192.168.90.0 network.

### [Writing and installing an ACL]

```
Router# configure terminal (or config t)
Router(config)# access-list 10 deny 172.16.70.35
                        or
                        access-list 10 deny 172.16.70.35 0.0.0.0
                        or
                        access-list 10 deny host 172.16.70.35
Router(config)# access-list 10 permit 0.0.0.0 255.255.255.255
                        or
                        access-list 10 permit any
Router(config)# interface gig0/1
Router(config-if)# ip access-group 10 out ← nearest interface going out
Router(config-if)# exit
Router(config)# exit
```

\* If only deny Melvin and didn't mention permit others, the router will consider denying all traffics. Must permit the rest after denying the specific hosts.

### [Viewing information about existing ACL's]

Router# show configuration

(This will show which access groups are associated with particular interfaces)

Router# show access list 10

(This will show detailed information about this ACL)

## Standard Access List Sample #2

Include a remark with each statement of your ACL. Write a standard access list to block Jim's computer from sending information to Frank's computer; but will allow all other traffic from the 192.168.90.0 network. Permit all traffic from the 210.30.28.0 network to reach the 172.16.70.0 network. 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 A  
Interface: Gig0/0  
Access-list #: 28

### [Writing and installing an ACL]

```
Router# configure terminal
Router(config)# access-list 28 remark Block Jim from reaching Frank
Router(config)# access-list 28 deny 192.168.90.36
                        or
                    access-list 28 deny 192.168.90.36 0.0.0.0
                        or
                    access-list 28 deny host 192.168.90.36
Router(config)# access-list 28 remark Allow all other traffic
Router(config)# access-list 28 permit 192.168.90.0 0.0.0.255
Router(config)# access-list 28 remark Allow all traffic
Router(config)# access-list 28 permit 210.30.28.0 0.0.0.255
Router(config)# interface Gig0/0
Router(config-if)# ip access-group 28 out
Router(config-if)# exit
Router(config)# exit
Router# copy run start
```

*access-list 28 deny any (optional for this case)*

#### [Remark Command]

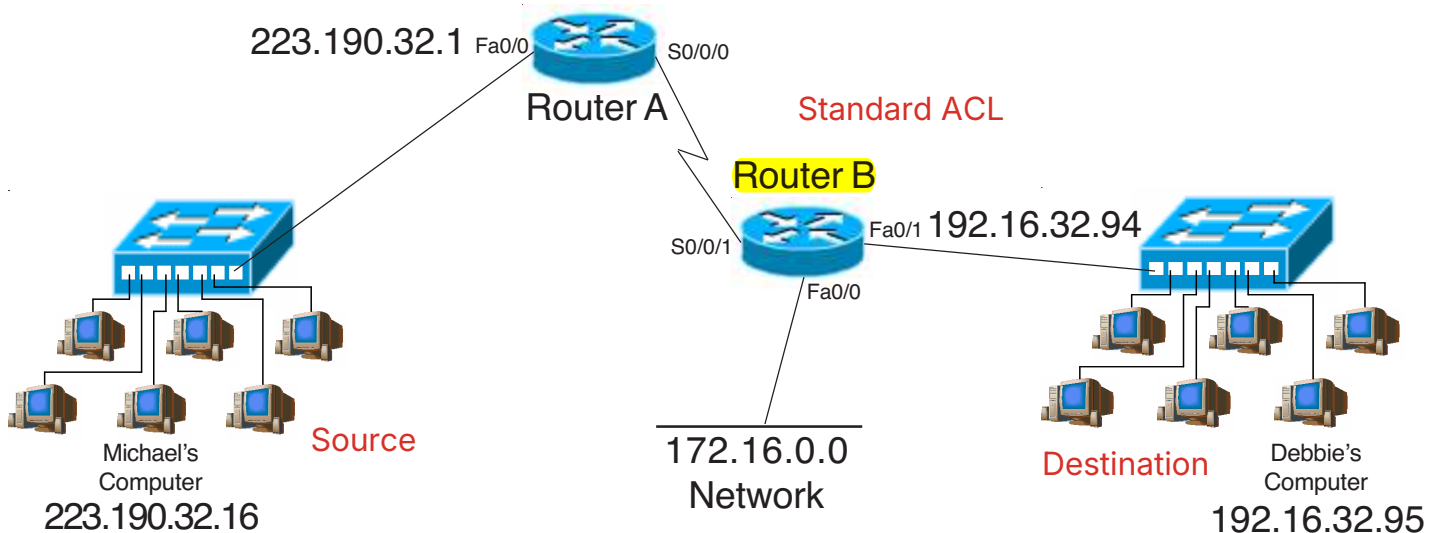
The remark command allows you to place text within the ACL so it can be viewed after it is inserted on the router. It can be viewed using the show run or any command that lists the ACL.

#### [Disabling ACL's]

```
Router# configure terminal
Router(config)# interface gig0/0
Router(config-if)# no ip access-group 28 out
Router(config-if)# exit
Router(config)# exit
```

#### [Removing an ACL]

```
Router# configure terminal
Router(config)# interface gig0/0
Router(config-if)# no ip access-group 28 out
Router(config-if)# exit
Router(config)# no access-list 28
Router(config)# exit
```



## 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]

Router# *configure terminal (or config t)*

Router B

Router(config)# access-list 1 deny host 223.190.32.16

*access-list (1-99) deny*  
access-list 1 permit any

*or*

Router(config)# int f0/1

Router B

*0.0.0.0 source wildcard mask*  
ip access-group 1 out

Router(config)# *interface f0/1*

Router(config-if)# *ip access-group 1 in or out (circle one)*

Router(config-if)# *exit*

Router(config)# *exit*

## Standard Access List Problem #2

Write a standard access list to permit Debbie's computer to receive information from Michael's computer; but will deny all other traffic from the 223.190.32.0 network. Block all traffic from the 172.16.0.0 network. Permit 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 #: 20

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# access-list 20 permit 223.190.32.16 0.0.0.0

access-list 20 permit host 223.190.32.16

access-list 20 permit 223.190.32.16

Router(config)# access-list 20 deny 223.190.32.0 0.0.0.255

Router(config)# access-list 20 deny 172.16.0.0 0.0.255.255

Router(config)# access-list 20 permit 0.0.0.0 255.255.255.255

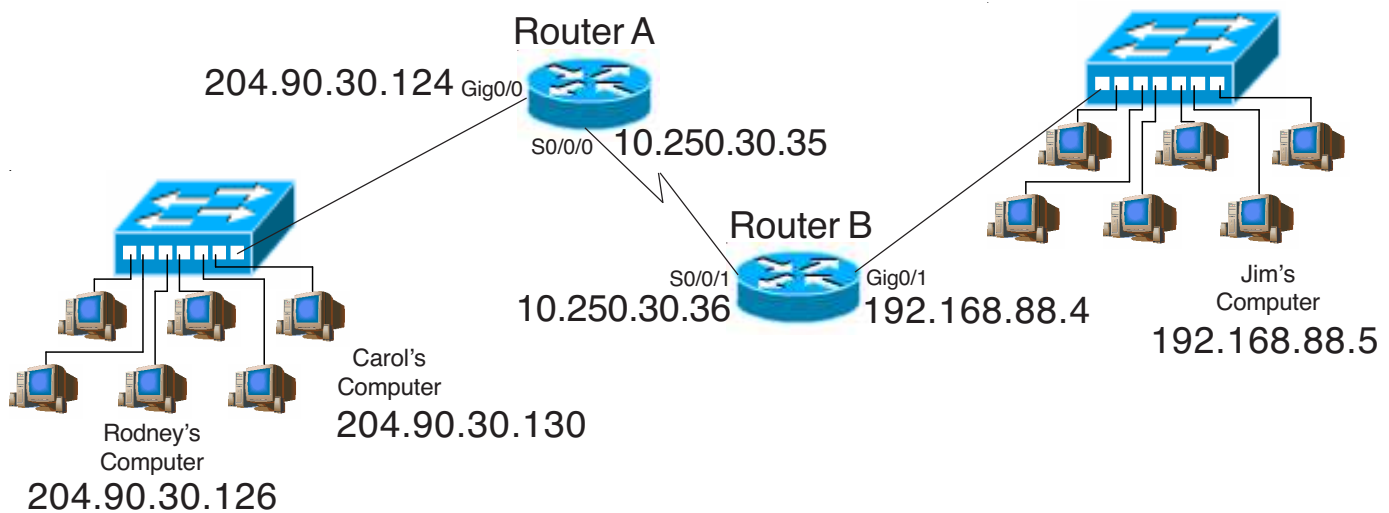
access-list 20 permit any

Router(config)# *interface* fa0/1

Router(config-if)# *ip access-group* 20 in or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*



### 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 #: 30

#### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# access-list 30 deny host 204.90.30.126  
access-list 30 deny host 204.90.30.130  
access-list 30 permit 204.90.30.0 0.0.0.255  
access-list 30 deny 0.0.0.0 255.255.255.255  
 or  
access-list 30 deny any

Router(config)# *interface* Gig0/1

Router(config-if)# *ip access-group* 30 *in or* out (circle one)  
 Router(config-if)# *exit*  
 Router(config)# *exit*

## Standard Access List Problem #4

Include a remark with each statement of your ACL. Using a minimum number of commands write a standard access list named "Ralph" to block Carol's computer from sending information to Jim's computer; but will permit Jim to receive data from Rodney. Block the upper half of the 204.90.30.0 range from reaching Jim's computer while permitting the lower half of the range. Block all other traffic. For help with blocking the upper half of the range review page 13 or the wildcard mask problems on pages 16 and 17. For help with named ACLs review pages 12 and 13. For help with the remark command review page 23.

Place the access list at:

Router Name: Router B

Interface: Gig0/1

Access-list Name: Ralph

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# ip access-list standard Ralph

Router(config-std-nacl)# remark block Carol sending info to Jim

deny host 204.90.30.130

remark permit Jim receiving data from Rodney

permit host 204.90.30.126

remark block upper half of 204.90.30.0 network

deny 204.90.30.128 0.0 0.127

remark permit lower half of 204.90.30.0 network

permit 204.90.30.0 0.0.0.127

remark block all other traffic

deny any

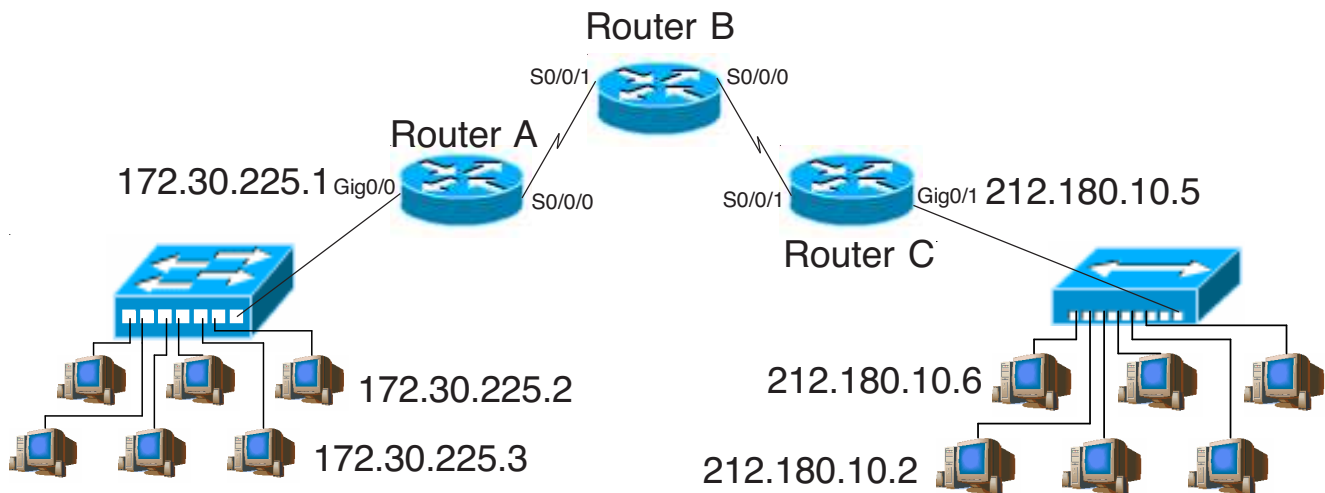
Router(config-std-nacl)# interface Gig0/1

Router(config-if)# ip access-group Ralph in or out (circle one)

Router(config-if)# exit

Router(config)# exit





## 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: Gig0/1

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
```

*Handwritten notes: A bracket groups the three deleted lines with the word "or". A handwritten note "access-list 69 deny 172.30.225.2 0.0.0.1" has an arrow pointing to the "out" direction in the final command.*

Router(config)# *interface Gig0/1*

Router(config-if)# *ip access-group 69 in or out (circle one)*

Router(config-if)# *exit*

Router(config)# *exit*

## Standard Access List Problem #6

Add a remark to each statement explaining its purpose. Write a standard access list to block and log 212.180.10.2 from sending information to the 172.30.225.0 network. Permit and log 212.180.10.6 to send data to the 172.30.225.0 network. Deny all other traffic. Keep in mind that there may be multiple ways many of the individual statements in an ACL can be written. Check the example on page 10 for help with the logging option. For help with the remark command review page 23.

Place the access list at:

Router Name: Router A

Interface: Gig0/0

Access-list #: 60

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# access-list 60 remark block and log 212.180.10.2 traffic to 172.30.225.0 network

access-list 60 deny 212.180.10.2 log

access-list 60 remark permit and log 212.180.10.6 traffic to 172.30.225.0 network

access-list 60 permit 212.180.10.6 log

access-list 60 remark deny all other traffic

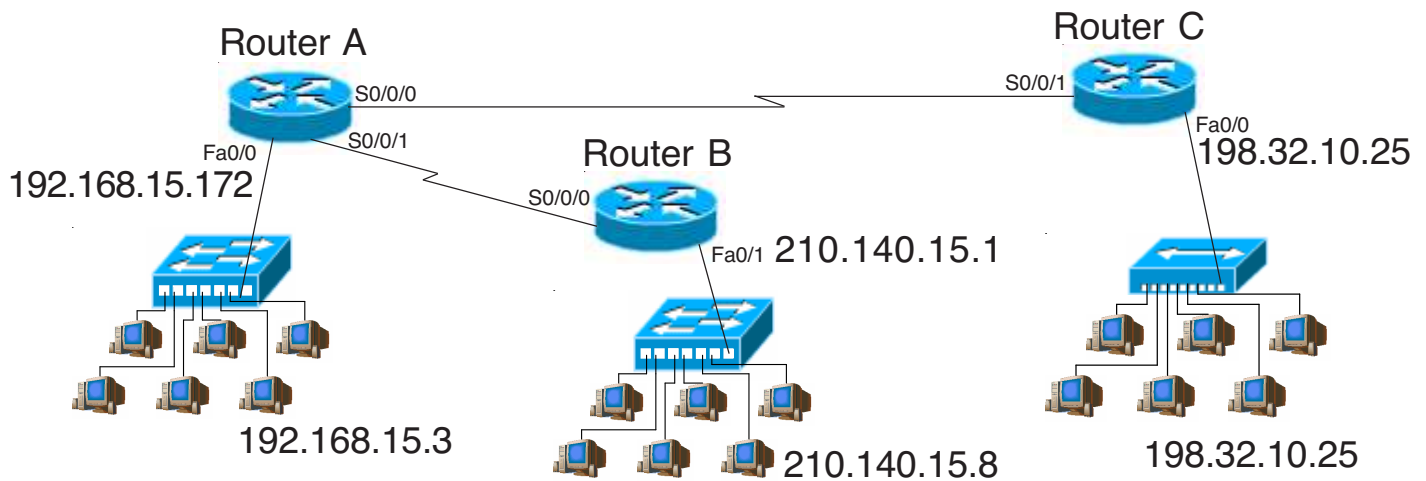
access-list 60 deny any

Router(config)# *interface* Gig0/0

Router(config-if)# *ip access-group* 60 in or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*



## Standard Access List Problem #7

Write a standard access list to block the addresses 192.168.15.1 to 192.168.15.31 from sending information to the 210.140.15.0 network. Do not permit any traffic from 198.32.10.25 to reach the 210.140.15.0 network. Permit all other traffic. For help with this problem review page 13 or the wildcard mask problems on pages 16 and 17.

Place the access list at:

Router Name: Router B

Interface: Fa0/1

Access-list #: 70

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# *access-list 70 remark block addresses 192.168.15.1 to 192.168.15.31 sending info to 210.140.15.0 network*

*access-list 70 deny 192.168.15.1 0.0.0.30*

*access-list 70 remark block 198.32.10.25 traffic to reach 210.140.15.0 network*

*access-list 70 deny host 198.32.10.25*

*access-list 70 permit all other traffic*

*access-list 70 permit any*

Router(config)# *interface Fa0/1*

Router(config-if)# *ip access-group 70 in or out (circle one)*

Router(config-if)# *exit*

Router(config)# *exit*

## Standard Access List Problem #8

Write a standard named access list called "CISCO\_LAB\_A" to permit traffic from the lower half of the 198.32.10.0 network to reach 192.168.15.0 network; block the upper half of the addresses.

Allow host 198.32.10.192 to reach network 192.168.15.0. Permit all other traffic. For help with this problem review page 13 or the wildcard masks problems on pages 16 and 17. For assistance with named ACLs review pages 12 and 13.

Place the access list at:

Router Name: Router A

Interface: Fa0/0

Access-list Name: CISCO-LAB-A

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# *ip access-list standard CISCO-LAB-A*

Router(config-std-nacl)# *permit 198.32.10.0 0.0.0.127*

*deny 198.32.10.128 0.0.0.127*

*permit host 198.32.10.192*

*permit any*

Router(config-std-nacl)# *interface Fa0/0*

Router(config-if)# *ip access-group CISCO-LAB-A* in or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*

## 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 #: 90

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

```
Router(config)# access-list 90 deny host 10.250.1.1  
access-list 90 deny host 10.250.2.1  
access-list 90 deny host 10.250.4.1  
access-list 90 deny 10.250.3.0 0.0.0.255  
access-list 90 permit any  
  
  
  
  
  
  
  
  
  

```

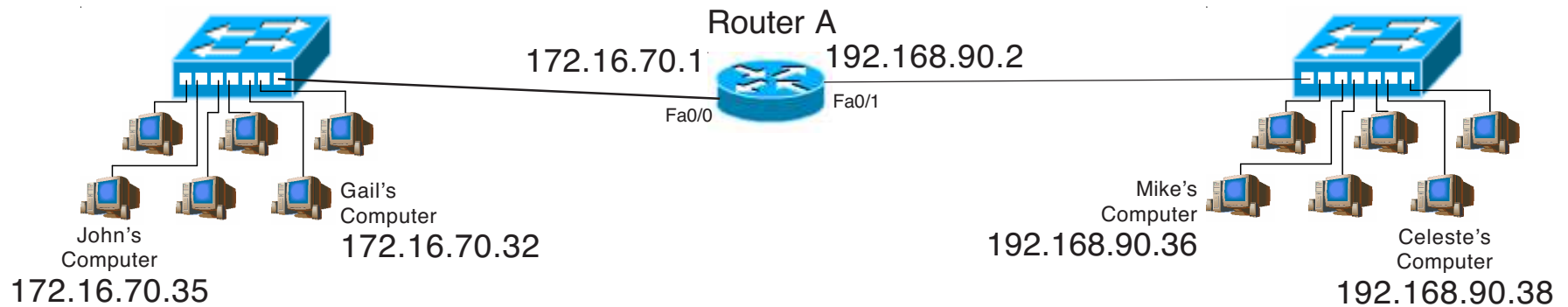
Router(config)# *interface fa0/0*

Router(config-if)# *ip access-group* 90 *in or* out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*

# **Writing Extended Access Lists...**



## Extended Access List Sample #1 Deny/Permit Specific Addresses



Write an extended access list to prevent John's computer from sending information to Mike's computer; 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 A  
 Interface: FA0/0  
 Access-list #: 110

### [Writing and installing an ACL]

```
Router# configure terminal (or config t)
Router(config)# access-list 110 deny ip 172.16.70.35 0.0.0.0 192.168.90.36 0.0.0.0
or
access-list 110 deny ip host 172.16.70.35 host 192.168.90.36
Router(config)# access-list 110 permit ip any any
or
access-list 110 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
Router(config)# interface fa0/0
Router(config-if)# ip access-group 110 in
Router(config-if)# exit
Router(config)# exit
```

### [Viewing information about existing ACL's]

Router# show configuration	(This will show which access groups are associated with particular interfaces)
Router# show access list 110	(This will show detailed information about this ACL)

## Extended Access List Sample #2

## Deny/Permit Specific Addresses

Write an extended access list to block the 172.16.70.0 network from receiving information from Mike's computer at 192.168.90.36. Block the lower half of the ip addresses from 192.168.90.0 network from reaching Gail's computer at 172.16.70.32. 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: FA0/1  
Access-list #: 135

### [Writing and installing an ACL]

```
Router# configure terminal
Router(config)# access-list 135 deny ip 192.168.90.36 0.0.0.0 172.16.70.0 0.0.0.255
                        or
                        access-list 135 deny ip host 192.168.90.36 172.16.70.0 0.0.0.255
Router(config)# access-list 135 deny ip 192.168.90.0 0.0.0.127 172.16.70.32 0.0.0.0
                        or
                        access-list 135 deny ip 192.168.90.0 0.0.0.127 host 172.16.70.32
Router(config)# access-list 135 permit ip any any
                        or
                        access-list 135 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
Router(config)# interface fa0/1
Router(config-if)# ip access-group 135 in
Router(config-if)# exit
Router(config)# exit
Router# copy run start
```

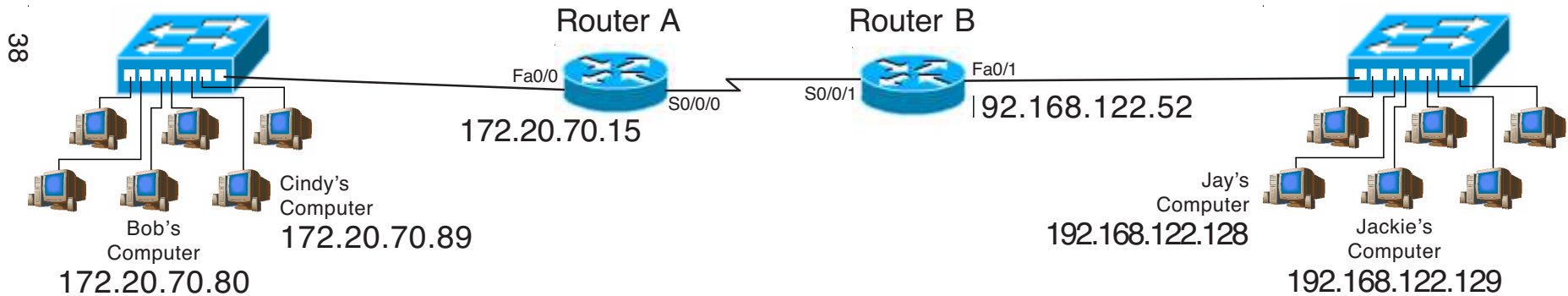
### [Disabling ACL's]

```
Router# configure terminal
Router(config)# interface fa0/1
Router(config-if)# no ip access-group 135 out
Router(config-if)# exit
Router(config)# exit
```

### [Removing an ACL]

```
Router# configure terminal
Router(config)# interface fa0/1
Router(config-if)# no ip access-group 135 out
Router(config-if)# exit
Router(config)# no access-list 135
Router(config)# exit
```





## 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 A

Interface: Fa0/0

Access-list #: 110

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# access-list 110 deny ip 172.20.70.89 0.0.0.0 192.168.122.128 0.0.0.0

access-list 110 permit ip any any

Router(config)# interface Fa0/0

Router(config-if)# ip access-group 110 in or out (circle one)

Router(config-if)# exit

Router(config)# exit

Router# copy run start

## Extended Access List Problem #2

## Deny/Permit Specific Addresses

Write an extended access list to block the 172.20.70.0 255.255.255.0 network from receiving information from Jackie's computer at 192.168.122.129. Block the lower half of the ip addresses from 192.168.122.0 network from reaching Cindy's computer at 172.20.70.89. 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 #: 120

### [Writing and installing an ACL]

Router# *configure terminal*

Router(config)# *access-list 120 deny ip 192.168.122.129 0.0.0.0 172.20.70.0 0.0.0.255*

*access-list 120 deny ip 192.168.122.0 0.0.0.127 172.20.70.89 0.0.0.0*

*access-list 120 permit ip any any*

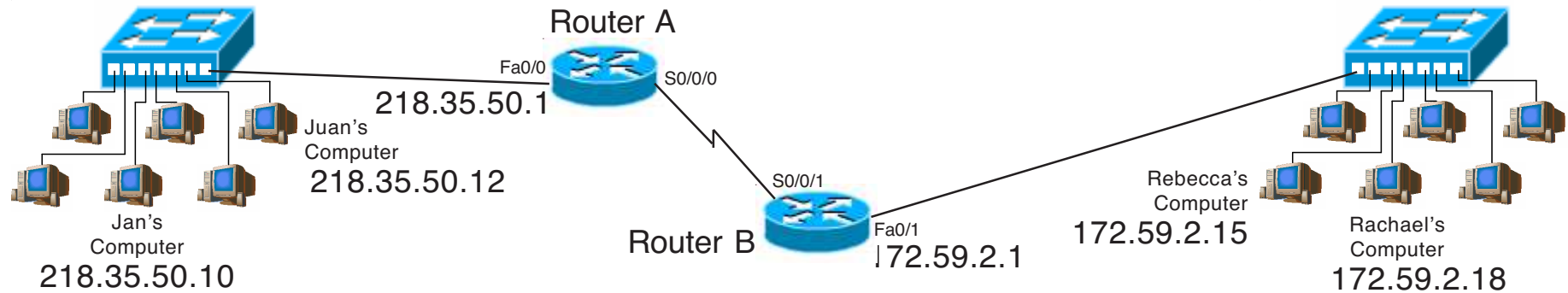
Router(config)# *interface fa0/1*

Router(config-if)# *ip access-group* 120 in or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*

Router# *copy run start*



## Extended Access List Problem #3

## Deny/Permit Specific Addresses

Write a named extended access list called "LAB\_166" to permit Jan's computer at 218.35.50.10 to receive packets from Rachael's computer at 172.59.2.18; but not Rebecca's computer at 172.59.2.15. Deny all other packets. 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 Name: LAB\_166

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# *ip access-list extended LAB\_166*

Router(config-ext-nacl)# *permit ip 172.59.2.18 0.0.0.0 218.35.50.10 0.0.0.0*

*deny ip 172.59.2.15 0.0.0.0 218.35.50.10 0.0.0.0*

*deny ip any any*

Router(config-ext-nacl)# *interface fa0/1*

Router(config-if)# *ip access-group LAB\_166* in or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*

## Extended Access List Problem #4

## Deny/Permit Specific Addresses

Write an extended access list to allow Juan's computer at 218.35.50.12 to send information to Rebecca's computer at 172.59.2.15; but not Rachael's computer at 172.59.2.18. 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: fa0/0

Access-list #: 140

### [Writing and installing an ACL]

Router# *configure terminal*

Router(config)# access-list 140 permit ip 218.35.50.12 0.0.0.0 172.59.2.15 0.0.0.0

access-list 140 deny ip 172.59.2.18 0.0.0.0 172.59.2.15 0.0.0.0

access-list 140 permit ip any any

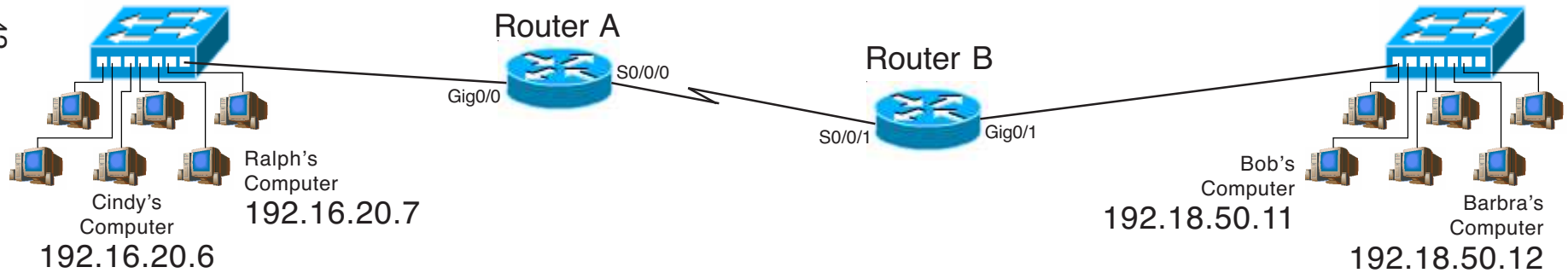
Router(config)# *interface* fa0/0

Router(config-if)# *ip access-group* 140 in or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*

Router# *copy run start*



## Extended Access List Sample #3

## Deny/Permit Entire Ranges

Write an extended access list to permit the 192.16.20.0 network to receive packets from the 192.18.50.0 network. 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: Gig0/1  
 Access-list #: 111

### [Writing and installing an ACL]

```
Router# configure terminal (or config t)
Router(config)# access-list 111 permit ip 192.18.50.0 0.0.0.255 192.16.20.0 0.0.0.255
Router(config)# access-list 111 deny ip any any
or
Router(config)# access-list 111 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
Router(config)# interface gig0/1
Router(config-if)# ip access-group 111 in
Router(config-if)# exit
Router(config)# exit
```

### [Viewing information about existing ACL's]

Router# *show configuration* (This will show which access groups are associated with particular interfaces)

Router# *show access list 111* (This will show detailed information about this ACL)

## Extended Access List Sample #4

## Deny/Permit Entire Ranges

Add a remark to each statement. Write an extended access list to block the 192.18.50.0 network from receiving information from the 192.16.20.0 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: Gig0/0  
Access-list #: 188

### [Remark Command]

The remark command allows you to place text within the ACL so it can be viewed after it is inserted on the router. It can be viewed using the show run or any command that lists the ACEs.

### [Writing and installing an ACL]

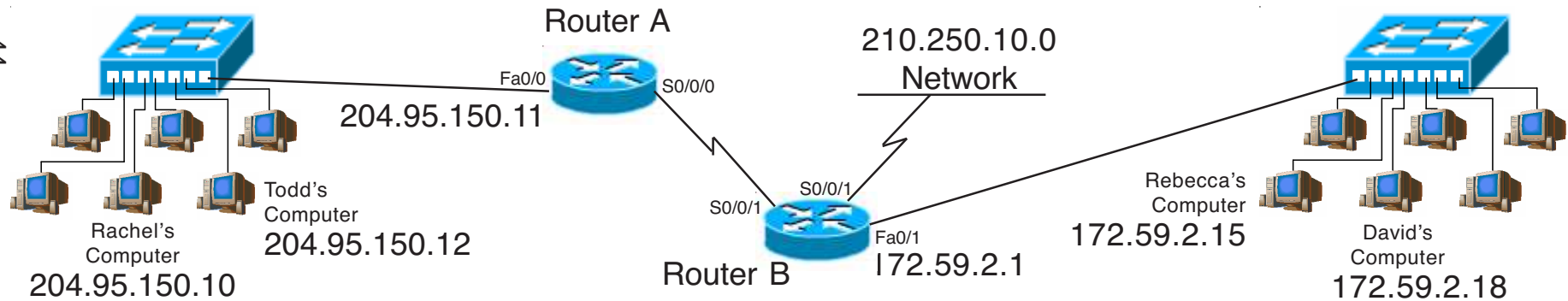
```
Router# configure terminal
Router(config)# access-list 188 remark block all traffic from the Science lab
Router(config)# access-list 188 deny ip 192.16.20.0 0.0.0.255 192.18.50.0 0.0.0.255
Router(config)# access-list 188 remark allow everyone else unrestricted access
Router(config)# access-list 188 permit ip any any
                        or
                        access-list 188 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
Router(config)# interface gig0/0
Router(config-if)# ip access-group 188 in
Router(config-if)# exit
Router(config)# exit
Router# copy run start
```

### [Disabling ACL's]

```
Router# configure terminal
Router(config)# interface gig0/0
Router(config-if)# no ip access-group 188 out
Router(config-if)# exit
Router(config)# exit
```

### [Removing an ACL]

```
Router# configure terminal
Router(config)# interface gig0/0
Router(config-if)# no ip access-group 188 out
Router(config-if)# exit
Router(config)# no access-list 188
Router(config)# exit
```



## 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 #: 115

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# access-list 115 permit ip 204.95.150.0 0.0.0.255 172.59.0.0 0.0.255.255

access-list 115 deny ip 210.250.10.0 0.0.0.255 172.59.0.0 0.0.255.255

access-list 115 permit ip any any

Router(config)# *interface* Fa0/0

Router(config-if)# *ip access-group* 115 in or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*

## Extended Access List Problem #6

## Deny/Permit Entire Ranges

Write an extended access list to allow Rachel's computer at 204.95.150.10 to receive information from the 172.59.2.0 255.255.255.0 network. Deny all other hosts on the 204.95.150.0 network access from the 172.59.2.0 255.255.255.0 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 B

Interface: fa0/1

Access-list #: 160

### [Writing and installing an ACL]

Router# *configure terminal*

Router(config)# *access-list 160 permit ip 172.59.2.0 0.0.0.255 204.95.150.10 0.0.0.0*

*access-list 160 deny ip 172.59.2.0 0.0.0.255 204.95.150.0 0.0.0.255*

*access-list 160 permit ip any any*

Router(config)# *interface fa0/1*

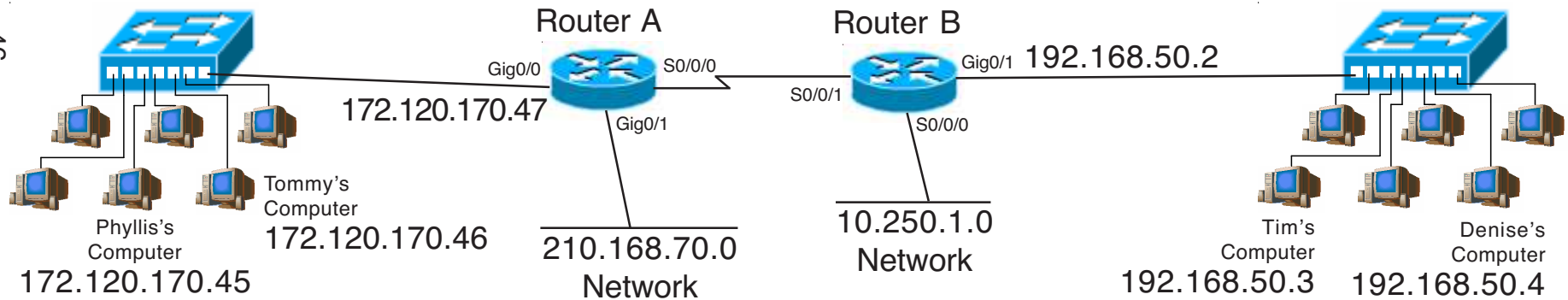
Router(config-if)# *ip access-group 160* in or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*

Router# *copy run start*





## Extended Access List Problem #7 Deny/Permit Entire Ranges

Write a named extended access list called "Godzilla" to prevent the 172.120.0.0 network from sending information to the 210.168.70.0, and 10.250.1.0 255.255.255.0 networks; but will permit traffic to the 192.168.50.0 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: g0/0

Access-list Name: Godzilla

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# ip access-list extended Godzilla

Router(config-ext-nacl)# deny ip 172.120.0.0 0.0.255.255 210.168.70.0 0.0.0.255

deny ip 172.120.0.0 0.0.255.255 10.250.1.0 0.0.0.255

permit ip 172.120.0.0 0.0.255.255 192.168.50.0 0.0.0.255

permit ip any any

Router(config-ext-nacl)# interface g0/0

Router(config-if)# ip access-group Godzilla in or out (circle one)

Router(config-if)# exit

Router(config)# exit

## Extended Access List Problem #8

## Deny/Permit Entire Ranges

Assuming default subnet masks write an extended access list to permit Tim at 192.168.50.3 to receive data from the 172.120.0.0 network. Allow the 192.168.50.0 network to receive information from Phyllis's computer at 172.120.170.45. 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 A

Interface: g0/0

Access-list #: 180

### [Writing and installing an ACL]

Router# *configure terminal*

Router(config)# *access-list 180 permit ip 172.20.0.0 0.0.255.255 192.168.50.3 0.0.0.0*

*access-list 180 permit ip 172.120.170.45 0.0.0.0 192.168.50.0 0.0.0.255*

*access-list 180 deny ip any any*

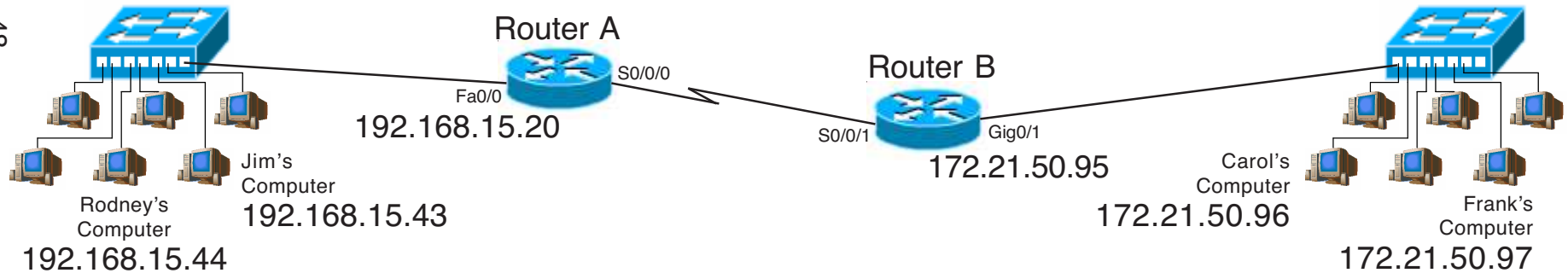
Router(config)# *interface g0/0*

Router(config-if)# *ip access-group 180* *in* or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*

Router# *copy run start*



## Extended Access List Sample #5

## Deny/Permit a Range of Addresses

Write an extended access list to deny the first 15 usable addresses of the 192.168.15.0 network from reaching the 172.21.0.0 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: Fa0/0  
 Access-list #: 185

### [Writing and installing an ACL]

```
Router# configure terminal (or config t)
Router(config)# access-list 185 deny ip 192.168.15.0 0.0.0.15 172.21.50.0 0.0.255.255
Router(config)# access-list 185 permit ip any any
or
Router(config)# access-list 185 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
Router(config)# interface fa0/0
Router(config-if)# ip access-group 185 in
Router(config-if)# exit
Router(config)# exit
```

### [Viewing information about existing ACL's]

Router# show configuration (This will show which access groups are associated with particular interfaces)

Router# show access list 185 (This will show detailed information about this ACL)

## Extended Access List Sample #6

## Deny/Permit a Range of Addresses

Write an extended access list which will allow the lower half of 192.168.15.0 network access to the 172.21.50.0 network. 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 A  
Interface: Fa0/0  
Access-list #: 121

### [Writing and installing an ACL]

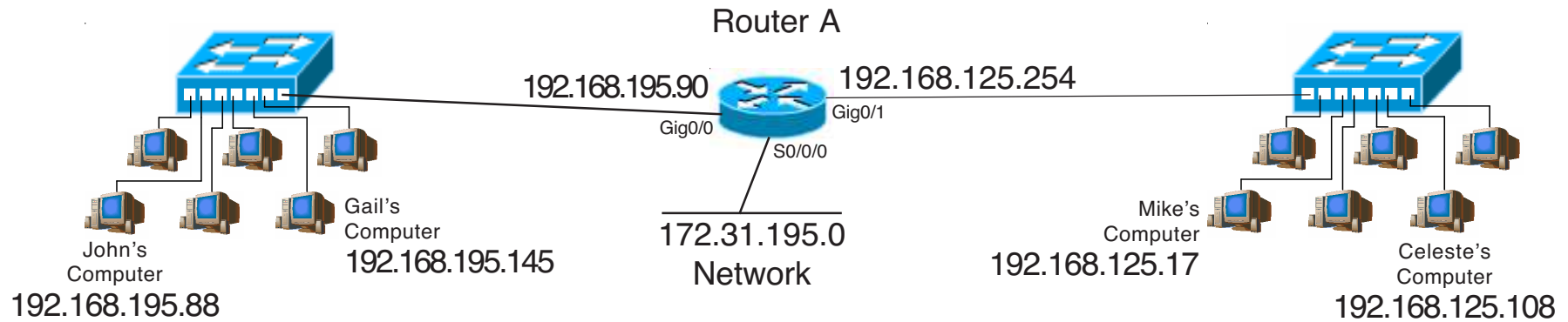
```
Router# configure terminal
Router(config)# access-list 121 permit ip 192.168.15.0 0.0.0.127 172.21.50.0 0.0.0.255
Router(config)# access-list 121 deny ip any any
                        or
                        access-list 121 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
Router(config)# interface fa0/0
Router(config-if)# ip access-group 121 in
Router(config-if)# exit
Router(config)# exit
Router# copy run start
```

### [Disabling ACL's]

```
Router# configure terminal
Router(config)# interface fa0/0
Router(config-if)# no ip access-group 121 in
Router(config-if)# exit
Router(config)# exit
```

### [Removing an ACL]

```
Router# configure terminal
Router(config)# interface fa0/0
Router(config-if)# no ip access-group 121 in
Router(config-if)# exit
Router(config)# no access-list 121
Router(config)# exit
```



## 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: Gig0/1  
 Access-list #: 110

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# *access-list 110 deny ip 192.168.125.0 0.0.0.31 192.168.195.0 0.0.0.255*  
*access-list 110 permit ip any any*

Router(config)# *interface Gig0/1*  
 Router(config-if)# *ip access-group 110 in or out (circle one)*  
 Router(config-if)# *exit*

## Extended Access List Problem #10 Deny/Permit a Range of Addresses

Include a remark with each statement of your ACL. Write a named extended access list called "Media\_Center" to permit the range of addresses from 172.31.195.1 through 172.31.195.7 to send data to the 192.168.125.0 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: so/0/0

Access-list Name: Media\_Center

### [Writing and installing an ACL]

Router# *configure terminal*

Router(config)# *ip access-list extended Media\_Center*

Router(config-ext-nacl)# *remark permit range of addresses from 172.31.195.1 through 172.31.195.7 sending data to 192.168.125.0 network*

*permit ip 172.31.195.0 0.0.0.7 192.168.125.0 0.0.0.255*

*deny ip 172.31.195.0 0.0.0.0 192.168.125.0 0.0.0.255*

*remark deny all other traffic*

*deny ip any any*

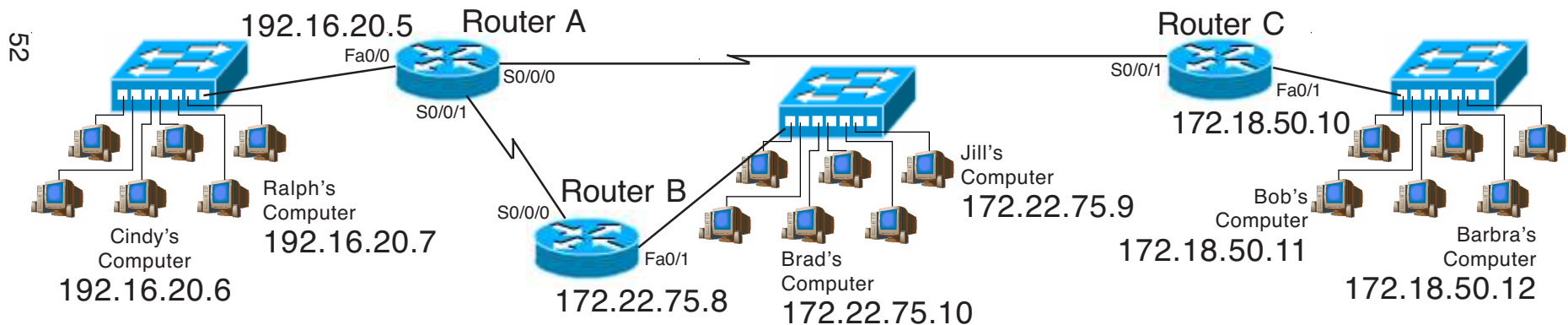
Router(config-ext-nacl)# *interface so/0/0*

Router(config-if)# *ip access-group Media\_Center* in or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*

Router# *copy run start*



## Extended Access List Problem #11 Deny/Permit a Range of Addresses

Write an extended access list to permit the first 3 usable addresses in the 192.16.20.0 network to reach the 172.22.75.0 network. Deny the addresses from 192.16.20.4 through 192.16.20.31 from reaching the 172.22.75.0 network. Permit all other traffic. Keep in mind that there are multiple ways this ACL can be written.

Place the access list at:

Router Name: Router A

Interface: fa0/0

Access-list #: 110

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# *access-list 110 permit ip 192.16.20.0 0.0.0.3 172.22.75.0 0.0.0.255*

*access-list 110 deny ip 192.16.20.4 0.0.0.27 172.22.75.0 0.0.0.255*

*access-list 110 permit ip any any*

Router(config)# *interface fa0/0*

Router(config-if)# *ip access-group 110 in* or out (circle one)

Router(config-if)# *exit*

## Extended Access List Problem #12 Deny/Permit a Range of Addresses

Write an extended access list to deny the addresses from 172.22.75.8 through 172.22.75.127 from sending data to the 172.18.50.0 network. Deny the first half of the addresses from the 172.22.75.0 network from reaching the 192.16.20.0 network. Permit all other traffic. Keep in mind that there are multiple ways this ACL can be written.

Place the access list at:

Router Name: Router B

Interface: fa0/1

Access-list #: 120

$$\begin{array}{r} .0 - .7 \quad 1000 \quad 0000 \\ \quad \quad 0000 \quad 0111 \\ \hline \quad \quad 0000 \quad 0111 \end{array}$$

.8 - .127

$$\begin{array}{r} .1 \quad 0000 \quad 0001 \\ .3 \quad 0000 \quad 0011 \\ .5 \quad 0000 \quad 0101 \\ .7 \quad 0000 \quad 0111 \\ \hline 111 \quad 1110 \end{array}$$

### [Writing and installing an ACL]

Router# *configure terminal*

Router(config)# access-list 120 permit ip 172.22.75.0 0.0.0.7 172.18.50.0 0.0.255.255

access-list 120 deny any any

access-list 120 deny ip 172.22.75.0 0.0.0.127 192.16.20.0 0.0.0.255

access-list 120 permit ip any any

Router(config)# *interface* fa0/1

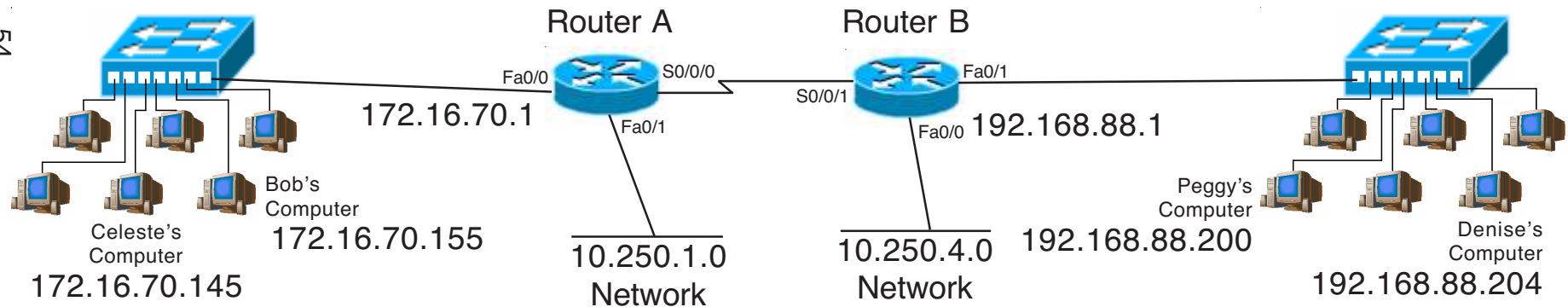
Router(config-if)# *ip access-group* 120 (in) or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*

Router# *copy run start*





## Extended Access List Problem #13 Deny/Permit a Range of Addresses

Include a remark with each statement of your ACL. Write an extended access list to permit the first 63 usable addresses in the 192.168.88.0 network to reach the lower half of the addresses in the 172.16.70.0 network; but not the upper half. 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 B  
 Interface: fa0/1  
 Access-list #: 130

0000 0000

0011 1111

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# *access-list 130 remark permit 192.168.88.0 to 192.168.88.63 to reach lower half of addresses in 172.16.70.0 network*

*access-list 130 permit ip 192.168.88.0 0.0.0.63 172.16.70.0 0.0.0.127*

*access-list 130 remark permit 192.168.88.0 to 192.168.88.63 to reach upper half of addresses in 172.16.70.0 network*

*access-list 130 permit ip 192.168.88.0 0.0.0.63 172.16.70.128 0.0.0.127*

*access-list 130 remark deny all other traffic*

*access-list 130 deny ip any any*

Router(config)# *interface fa0/1*

Router(config-if)# *ip access-group 130* in or out (circle one)

Router(config-if)# *exit*

## Extended Access List Problem #14 Deny/Permit a Range of Addresses

Write an extended access list to deny the addresses from 10.250.1.0 through 10.250.1.63 from sending data to Denise'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 A

Interface: fa0/1

Access-list #: 140

### [Writing and installing an ACL]

Router# *configure terminal*

Router(config)# *access-list 140 deny ip 10.250.1.0 0.0.0.63 192.168.88.204 0.0.0.0*

*access-list 140 permit ip any any*

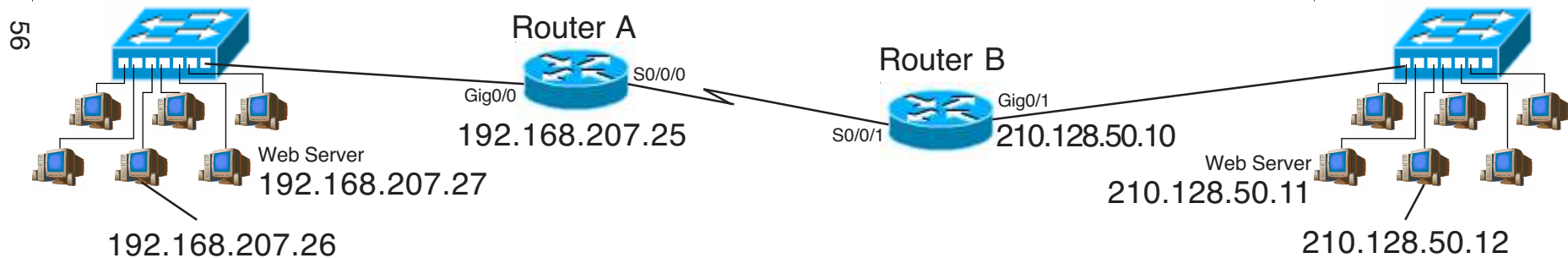
Router(config)# *interface fa0/1*

Router(config-if)# *ip access-group 140* in or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*

Router# *copy run start*



## Extended Access List Sample #7

## Deny/Permit Port Numbers

Write an extended access list to deny HTTP traffic intended for web server 192.168.207.27 from all other networks, but will permit all other HTTP traffic to reach the 192.168.207.0 network. Deny all other IP 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 #: 198

### [Writing and installing an ACL]

```
Router# configure terminal (or config t)
Router(config)# access-list 198 deny tcp any 192.168.207.27 0.0.0.0 eq www
or
access-list 198 deny tcp any host 192.168.207.27 eq www
Router(config)# access-list 198 permit tcp any 192.168.207.0 0.0.0.255 eq www
Router(config)# interface gig0/1
Router(config-if)# ip access-group 198 in
Router(config-if)# exit
Router(config)# exit
```

### [Viewing information about existing ACL's]

```
Router# show configuration (This will show which access groups are associated
with particular interfaces)

Router# show access list 198 (This will show detailed information about this ACL)
```

## Extended Access List Sample #8

## Deny/Permit Port Numbers

Write an extended access list on Router B to deny pings between hosts on the 210.128.50.0 and the 192.168.207.0 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 B  
Interface: Gig0/1  
Access-list #: 134

### [Writing and installing an ACL]

```
Router# configure terminal
Router(config)# access-list 134 deny icmp 210.128.50.0 0.0.0.255 192.168.207.0 0.0.0.255
Router(config)# access-list 134 permit ip any any
Router(config)# interface gig0/1
Router(config-if)# ip access-group 134 in
Router(config-if)# exit
Router(config)# exit
Router# copy run start
```

#### Hint:

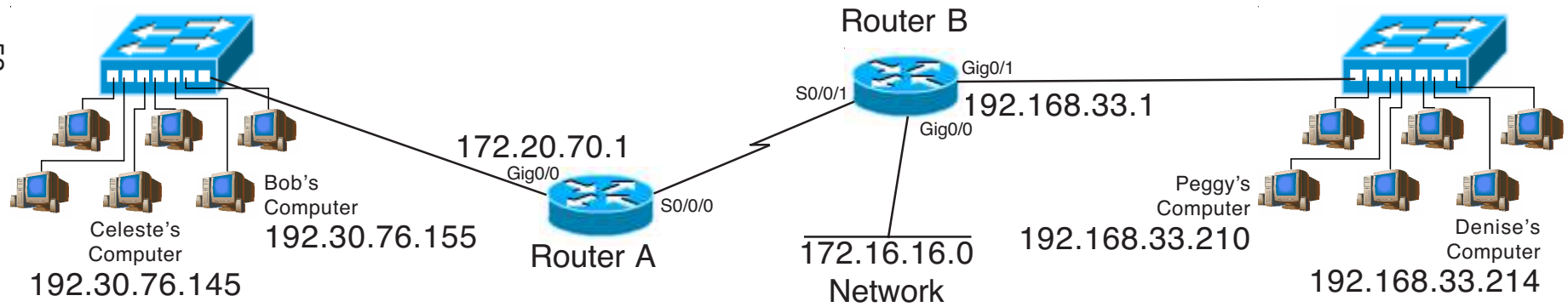
It's OK to use multiple protocols in the same ACL.

### [Disabling ACL's]

```
Router# configure terminal
Router(config)# interface Gig0/1
Router(config-if)# no ip access-group 134 out
Router(config-if)# exit
Router(config)# exit
```

### [Removing an ACL]

```
Router# configure terminal
Router(config)# interface Gig0/1
Router(config-if)# no ip access-group 134 out
Router(config-if)# exit
Router(config)# no access-list 134
Router(config)# exit
```



## Extended Access List Sample #9

## Deny/Permit Port Numbers

Write an Extended access list to permit Denise's computer to use TFTP with Bob's computer. Deny all other traffic from the 192.168.33.0 network to the 192.30.76.0 network. Keep in mind that there may be multiple ways many of the individual statements in an ACL can be written.

under udp

Place the access list at:

Router Name: Router B  
 Interface: Gig0/1  
 Access-list #: 145

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*  
 Router(config)# *access-list 145 permit udp 192.168.33.214 0.0.0.0 192.30.76.155 0.0.0.0 eq tftp*  
 or  
*access-list 145 permit udp host 192.168.33.214 host 192.30.76.155 eq tftp*  
 Router(config)# *interface Gig0/1*  
 Router(config-if)# *ip access-group 145 in*  
 Router(config-if)# *exit*  
 Router(config)# *exit*

(or 89)

### [Viewing information about existing ACL's]

Router# *show configuration* (This will show which access groups are associated with particular interfaces)

Router# *show access list 45* (This will show detailed information about this ACL)

## Extended Access List Sample #10

## Deny/Permit Port Numbers

Write an extended access list to deny **FTP** traffic from ip addresses 192.30.76.0 through 192.30.76.13 to any destination. 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: Gig0/0  
Access-list #: 155

### [Writing and installing an ACL]

Router# *configure terminal*  
Router(config)# *access-list 155 deny tcp 192.30.76.0 0.0.0.7 any eq ftp* (Blocks 0 to 7)  
Router(config)# *access-list 155 deny tcp 192.30.76.8 0.0.0.3 any eq ftp* (Blocks 8 to 11)  
Router(config)# *access-list 155 deny tcp 192.30.76.12 0.0.0.1 any eq ftp* (Blocks 12 to 13)  
Router(config)# *access-list 155 permit ip any any*  
*or*  
*access-list 155 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255*  
Router(config)# *interface gig0/0*  
Router(config-if)# *ip access-group 155 in*  
Router(config-if)# *exit*  
Router(config)# *exit*  
Router# *copy run start*

**Hint:**  
It's OK to use multiple protocols in the same ACL.

The first three TCP statements could be shortened to:

*access-list 155 permit tcp 192.30.76.14 0.0.0.1 any eq ftp* (Permits 14 and 15)  
*access-list 155 deny tcp 192.30.76.8 0.0.0.15 any eq ftp* (Blocks 0 to 15)

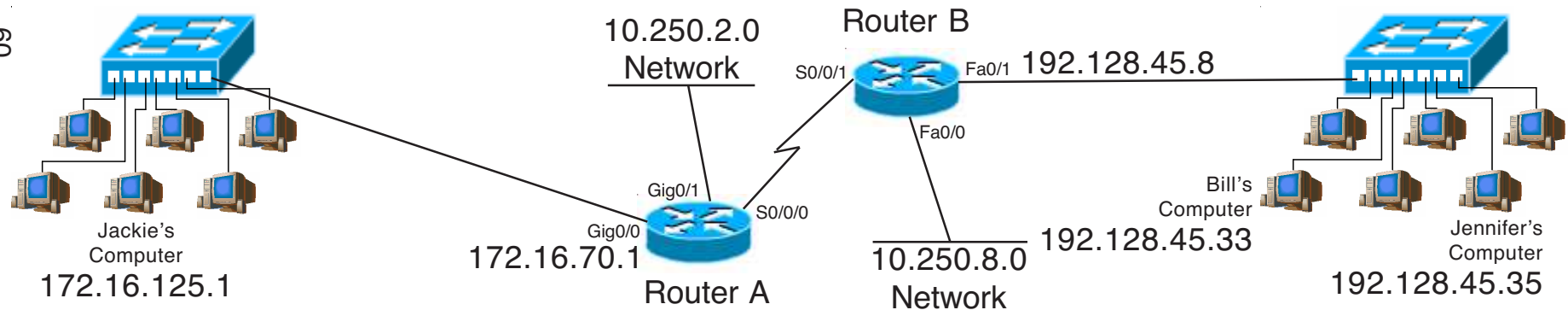
.0 - .13

0	0	0	0
0	0	0	1
0	0	1	0
0	0	1	1
0	1	0	0
0	1	0	1
0	1	1	0
0	1	1	1
1	0	0	0
1	0	0	1
1	0	1	0
1	0	1	1
1	1	0	0
1	1	0	1

3 digit combination x000 to x111  
(192.30.76.0 0.0.0.7)

2 digit combination xx00 to xx11  
(192.30.76.8 0.0.0.3)

1 digit combination xxx0 to xxx1  
(192.30.76.12 0.0.0.1)



## 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 #: 115

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# *access-list 115 permit icmp 192.128.45.0 0.0.0.255 172.16.125.0 0.0.0.255*

*access-list 115 permit icmp 192.128.45.0 0.0.0.255 10.250.2.0 0.0.0.255*

*access-list 115 deny ip any any*

Router(config)# *interface Fa0/1*

Router(config-if)# *ip access-group 115* in or out (circle one)

Router(config-if)# *exit*



## Extended Access List Problem #16 Deny/Permit a Port Numbers

Write a named extended access list called "PEGGYS\_LAB" to deny telnet from 10.250.8.0 through 10.250.8.127 from reaching the 192.128.45.0 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 B

Interface: fa0/0

Access-list Name: PEGGYS-LAB

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# ip access-list extended PEGGYS-LAB

Router(config-std-nacl)# deny tcp 10.250.8.0 0.0.0.127 192.128.45.0 0.0.0.255 eq 23

Router(config-std-nacl)# permit ip any any

---

---

---

---

---

Router(config-ext-nacl)# interface fa0/0

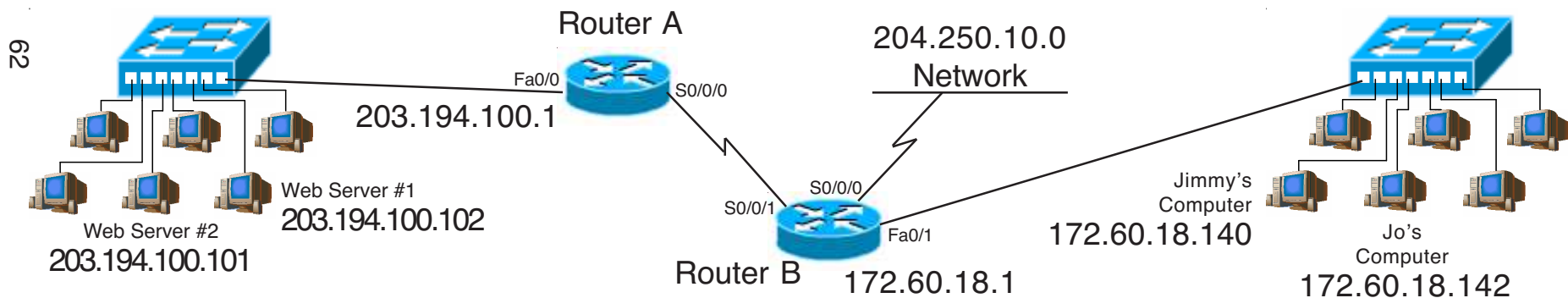
Router(config-if)# ip access-group PEGGYS-LAB in or out (circle one)

Router(config-if)# exit

Router(config)# exit

Router# copy run start

Router# copy run start



## Extended Access List Problem #17

## Deny/Permit Port Numbers

Write an access list to deny Jimmy's computer from sending ftp packets to Web Server 1, but permit ftp to Web Server #2. 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 #: 170

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# access-list 170 deny ftp 172.60.18.140 0.0.0.0 203.194.100.102 0.0.0.0 eq 21

access-list 170 permit ftp 172.60.18.140 0.0.0.0 203.194.100.101 0.0.0.0 eq 21

access-list 170 permit ip any any

Router(config)# *interface* Fa0/1

Router(config-if)# *ip access-group* 170 in or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*

## Extended Access List Problem #18

## Deny/Permit Port Numbers

Write an extended access list to deny all HTTP traffic intended for the web server at 203.194.100.102 from the 172.66.0.0 network. Permit all other HTTP traffic from the 204.250.10.0 and 172.60.0.0 networks to any other web servers. Deny all other IP traffic to the 203.194.100.0 network. 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 #: 180

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# *access-list 180 deny tcp 203.194.100.102 0.0.0.0 172.66.0.0 0.0.255.255 eq 80*

*access-list 180 permit tcp 204.250.10.0 0.0.0.255 any eq 80*

*access-list 180 permit tcp 172.60.0.0 0.0.255.255 any eq 80*

*access-list 180 deny ip any 203.194.100.0 0.0.0.255 eq 80*

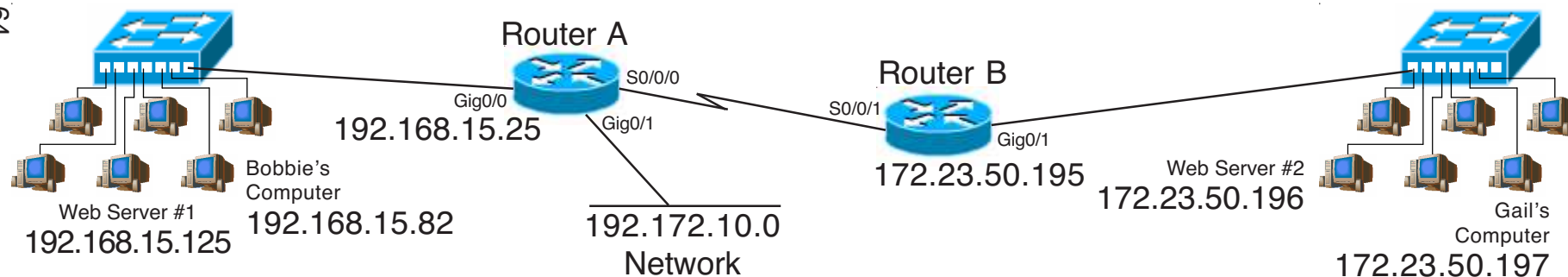
Router(config)# *interface fa0/0*

Router(config-if)# *ip access-group 180* in or out (circle one)

Router(config-if)# *exit*

Router(config)# *exit*

Router# *copy run start*



## 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: Gig 0/0

Access-list #: 119

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# *access-list 119 permit udp 192.168.15.0 0.0.0.255 any any eq 69*

*access-list 119 deny ip any any*

Router(config)# *interface Gig0/0*

Router(config-if)# *ip access-group 119 in or out (circle one)*

Router(config-if)# *exit*

Router(config)# *exit*

## Extended Access List Problem #20

## Deny/Permit Port Numbers

Write an extended access list that permits web traffic from web server #2 at 172.23.50.196 to reach everyone on the 192.168.15.0 network. Deny all other IP traffic going to the 192.172.10.0, and 192.168.15.0 networks from the 172.25.50.0 network. 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: g0/1

Access-list #: 120

### [Writing and installing an ACL]

Router# *configure terminal*

Router(config)# *access-list 120 permit tcp 172.23.50.196 0.0.0.0 192.168.15.0 0.0.0.255 eq 80*

*access-list 120 deny tcp 172.25.50.0 0.0.0.255 192.172.10.0 0.0.0.255 eq 80*

*access-list 120 deny tcp 172.25.50.0 0.0.0.255 192.168.15.0 0.0.0.255 eq 80*

Router(config)# *interface g0/1*

Router(config-if)# *ip access-group 120* in or out (circle one)

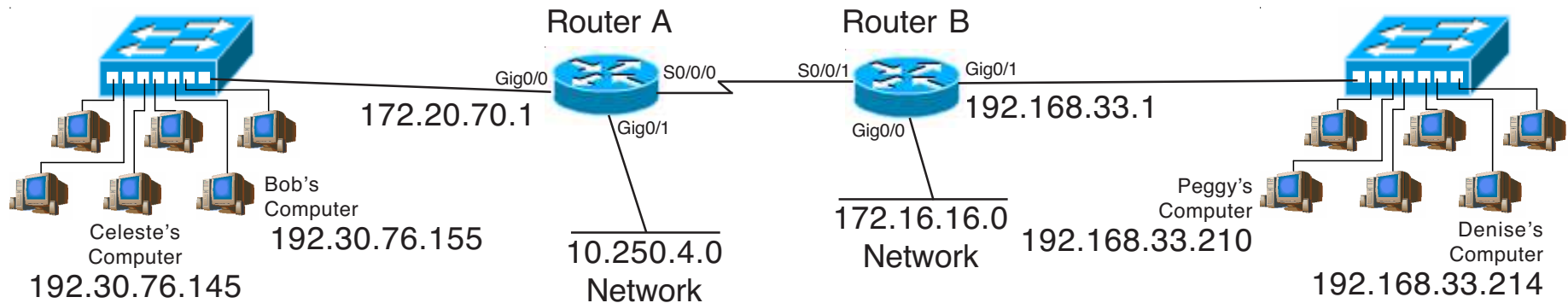
Router(config-if)# *exit*

Router(config)# *exit*

Router# *copy run start*

# Writing Access Lists to Restrict Telnet Access...

Restricting access to telnet can be a very usefull option. Telnet is considered a very insecure protocol because it sends passwords through the network in clear-text. By switching from the *access-group* command to the *access-class* command you can increase your security by allowing only those users through that you want to use telnet. The *access-class* command also allows you to apply this access list to the vty connections.



## Standard Access List Sample #11 Deny/Permit Telnet

Write a standard access list to permit Denise's and Bob's computers to telnet into Router B. Deny all other telnet 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: line VTY 0 4

Access-list #: 45

*(using line VTY 0 4 instead of an interface like E1 allows you to apply this access list to all VTY lines with one statement)*

### [Writing and installing an ACL]

```
Router# configure terminal (or config t)
Router(config)# access-list 45 permit 192.168.33.214 0.0.0.0
```

or

```
access-list 45 permit host 192.168.33.214
Router(config)# access-list 45 permit 192.30.76.155 0.0.0.0
```

or

```
access-list 45 permit host 192.30.76.155
```

```
Router(config)# line vty 0 4
```

```
Router(config-line)# access-class 45 in
```

```
Router(config-line)# exit
```

```
Router(config)# exit
```

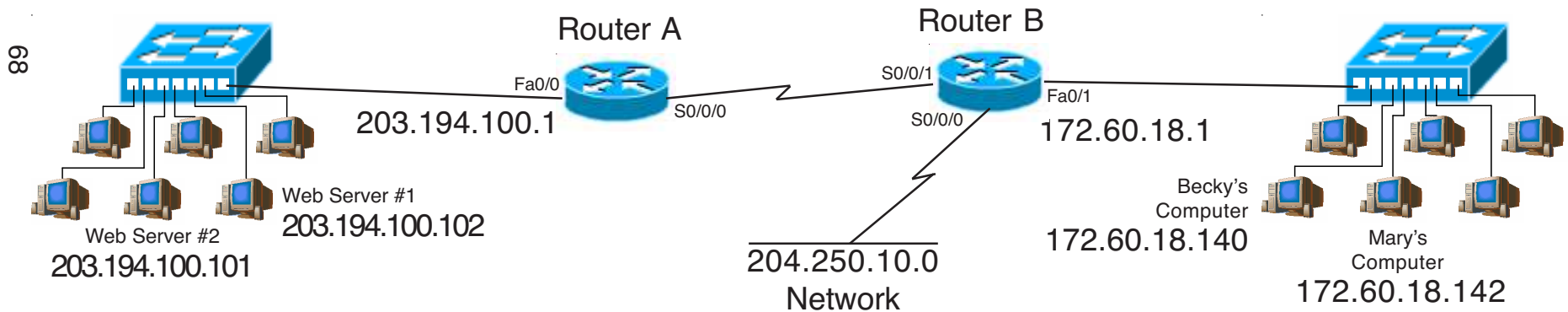
### [Viewing information about existing ACL's]

```
Router# show configuration
```

(This will show which access groups are associated with particular interfaces)

```
Router# show access list 45
```

(This will show detailed information about this ACL)



## Access List Problem #21 Deny/Permit Telnet

Write a standard access list to permit Becky and Mary's computer to telnet into Router B. 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 A  
 Interface: line vty 0 4  
 Access-list #: 130

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# access-list 130 permit host 172.60.18.140

access-list 130 permit host 172.60.18.142

access-list 130 deny any

Router(config)# line vty 0 4

Router(config-line)# access-class 130 (in) or out (circle one)

Router(config-line)# exit

Router(config)# exit



## Access List Problem #22

## Deny/Permit Telnet

Write a standard access list to permit which will permit Web Server #1 to telnet into Router A. Log the telnet attempts. Deny all other telnet access. 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: line vty 0 4  
Access-list #: 140

### [Writing and installing an ACL]

Router# *configure terminal (or config t)*

Router(config)# access-list 140 permit host 203.194.100.102 log  
access-list 140 deny any

Router(config)# line vty 0 4  
Router(config-line)# access-class 140 in or out (circle one)  
Router(config-line)# *exit*  
Router(config)# *exit*

## Deny/Permit Telnet

Place the access list at:

Interface: line vty 0 4

Access-list #: 170

Router# *configure terminal (or config t)*

```
Router(config)# access-list 170 deny host 192.60.18.61
```

access-list 170 deny host 192.60.18.62

```
access-list 170 permit 192.60.18.0 0.0.0.255
```

```
Router(config)# line vty 0 4
```

Router(config-line)# access-class 170 (in) or out (circle one)

```
Router(config-line)# exit
```

```
Router(config)# exit
```

# Reference

## Port Numbers

Port numbers are now assigned by the ICANN (Internet Corporation for Assigned Names and Numbers). Commonly used TCP and UDP applications are assigned a port number; such as: HTTP - 80, POP3 - 110, FTP - 20. When an application communicates with another application on another node on the internet, it specifies that application in each data transmission by using its port number. You can also type the name (ie. Telnet) instead of the port number (ie. 23). Port numbers range from 0 to 65536 and are divided into three ranges:

Well Known Ports	0 to 1,023
Registered Ports	1,024 to 49,151
Dynamic and/or Private Ports	49,152 to 65,535

Below is a short list of some commonly used ports. For a complete list of port numbers go to <http://www.iana.org/assignments/port-numbers>.

---

Some commonly used port numbers:

0	Reserved	
1	TCPMUX	(TCP Port Service Multiplexer)
5	RJE	(Remote Job Entry)
7	ECHO	
9	DISCARD	
11	SYSTAT	(Active users)
13	DAYTIME	
17	QUOTE	(Quote of the day)
18	MSP	(Message Send Protocol)
19	CHARGEN	(Character generator)
20	FTP-DATA	(File Transfer Protocol - Data)
21	FTP	(File Transfer Protocol - Control)
22	SSH	(Remote Login Protocol)
23	Telnet	(Terminal Connection)
25	SMTP	(Simple Mail Transfer Protocol)
29	MSG ICP	
37	TIME	
39	RLP	(Resource Location Protocol)
42	NAMESERV	(Host Name Server)

43	NICNAME	(Who Is)
49	LOGIN	(Login Host Protocol)
53	DNS	(Domain Name Server)
67	BOOTP	(Bootstrap Protocol Server)
68	BOOTPS	(Bootstrap Protocol Client)
69	TFTP	(Trivial File Transfer Protocol)
70	GOPHER	(Gopher Services )
75		(Any Private Dial-out Service)
79	FINGER	
80	HTTP	(Hypertext Transfer Protocol)
95	SUPDUP	(SUPDUP Protocol)
101	HOSTNAME	(NIC Host Name Server)
108	SNAGAS	(SNA Gateway Access Server)
109	POP2	(Post Office Protocol - Version 2)
110	POP3	(Post Office Protocol - Version 3)
113	AUTH	(Authentication Service)
115	SFTP	(Simple File Transfer Protocol)
117	UUCP-PATH	(UUCP Path Service)
118	SQLSERV	(SQL Services)
119	NNTP	(Newsgroup)
123	NTP	(Network Time Protocol)
137	NetBIOS-NS	(NetBIOS Name Service)
139	NetBIOS-SSN	(NetBIOS Session Service )
143	IMAP	(Interim Mail Access Protocol)
150	SQL-NET	(NetBIOS Session Service)
156	SQLSRV	(SQL Service)
161	SNMP	(Simple Network Management Protocol)
179	BGP	(Border Gateway Protocol)
190	GACP	(Gateway Access Control Protocol)
194	IRC	(Internet Relay Chat)
197	DLS	(Directory Location Service)
389	LDAP	(Lightweight Directory Access Protocol)
396	NETWARE-IP	(Novell Netware over IP )
443	HTTPS	(HTTP MCom)
444	SNPP	(Simple Network Paging Protocol)
445	Microsoft-DS	
458	Apple QuickTime	
546	DHCP Client	
547	DHCP Server	
563	SNEWS	
569	MSN	

# Class A Addresses

## VLSM Chart 8-15 Bits (2nd octet)

/8 255.0.0.0 16,777,216 Hosts	/9 255.128.0.0 8,388,608 Hosts	/10 255.192.0.0 4,194,304 Hosts	/11 255.224.0.0 2,097,152 Hosts	/12 255.240.0.0 1,048,576 Hosts	/13 255.248.0.0 524,288 Hosts	/14 255.252.0.0 262,144 Hosts	/15 255.254.0.0 131,072 Hosts
0 - 255	0-127	0-63	0-31	0-15	0-7	0-3	0-1
					8-15	4-7	2-3
				16-31	16-23	8-11	4-5
					24-31	12-15	6-7
						16-19	8-9
						20-23	10-11
		32-63	32-47	32-39	32-35	24-27	12-13
					36-39	28-31	14-15
				40-47	40-43	32-33	16-17
					44-47	34-35	18-19
					48-51	36-37	20-21
					52-55	38-39	22-23
			48-63	56-63	56-59	24-25	24-25
					60-63	26-27	26-27
				64-79	64-71	28-29	28-29
					72-79	30-31	30-31
					80-87	32-33	32-33
					88-95	34-35	34-35
		64-127	64-95	80-95	88-91	36-37	36-37
					92-95	38-39	38-39
				96-111	96-103	40-41	40-41
					104-111	42-43	42-43
					112-119	44-45	44-45
					120-127	46-47	46-47
			128-159	128-143	128-135	48-49	48-49
					136-143	50-51	50-51
				144-159	144-147	52-53	52-53
					148-151	54-55	54-55
					152-155	56-57	56-57
					156-159	58-59	58-59
		128-191	160-191	160-175	160-167	60-61	60-61
					168-175	62-63	62-63
				176-191	176-183	64-65	64-65
					184-187	66-67	66-67
					188-191	68-69	68-69
					192-199	70-71	70-71
		128-255	192-223	192-207	192-199	72-73	72-73
					200-207	74-75	74-75
				208-223	208-215	76-77	76-77
					216-219	78-79	78-79
					224-231	80-81	80-81
					232-239	82-83	82-83
		192-255	224-255	224-239	224-231	84-85	84-85
					232-239	86-87	86-87
				240-255	240-247	88-89	88-89
					248-251	90-91	90-91
					252-255	92-93	92-93
						94-95	94-95
			224-255	224-239	224-231	96-97	96-97
					232-239	98-99	98-99
				240-255	240-247	100-101	100-101
					248-251	102-103	102-103
					252-255	104-105	104-105
						106-107	106-107
						108-109	108-109
						110-111	110-111
						112-113	112-113
						114-115	114-115
						116-117	116-117
						118-119	118-119
						120-121	120-121
						122-123	122-123
						124-125	124-125
						126-127	126-127
						128-129	128-129
						130-131	130-131
						132-133	132-133
						134-135	134-135
						136-137	136-137
						138-139	138-139
						140-141	140-141
						142-143	142-143
						144-145	144-145
						146-147	146-147
						148-149	148-149
						150-151	150-151
						152-153	152-153
						154-155	154-155
						156-157	156-157
						158-159	158-159
						160-161	160-161
						162-163	162-163
						164-165	164-165
						166-167	166-167
						168-169	168-169
						170-171	170-171
						172-173	172-173
						174-175	174-175
						176-177	176-177
						178-179	178-179
						180-181	180-181
						182-183	182-183
						184-185	184-185
						186-187	186-187
						188-189	188-189
						190-191	190-191
						192-193	192-193
						194-195	194-195
						196-197	196-197
						198-199	198-199
						200-201	200-201
						202-203	202-203
						204-205	204-205
						206-207	206-207
						208-209	208-209
						210-211	210-211
						212-213	212-213
						214-215	214-215
						216-217	216-217
						218-219	218-219
						220-221	220-221
						222-223	222-223
						224-225	224-225
						226-227	226-227
						228-229	228-229
						230-231	230-231
						232-233	232-233
						234-235	234-235
						236-237	236-237
						238-239	238-239
						240-241	240-241
						242-243	242-243
						244-245	244-245
						246-247	246-247
						248-249	248-249
						250-251	250-251
						252-253	252-253
						254-255	254-255

# Class B Addresses

## VLSM Chart 16-23 Bits (3rd octet)

/16 255.255.0.0 65,536 Hosts	/17 255.255.128.0 32,768 Hosts	/18 255.255.192.0 16,384 Hosts	/19 255.255.224.0 8,192 Hosts	/20 255.255.240.0 4,096 Hosts	/21 255.255.248.0 2,048 Hosts	/22 255.255.252.0 1,024 Hosts	/23 255.255.254.0 512 Hosts
0 - 255	0-127	0-63	0-31	0-15	0-7	0-3	0-1
						4-7	2-3
					8-15	8-11	4-5
						12-15	6-7
						16-19	8-9
						20-23	10-11
						24-27	12-13
						28-31	14-15
							16-17
							18-19
							20-21
							22-23
							24-25
							26-27
							28-29
							30-31
			32-63	32-47	32-39	32-35	32-33
						36-39	34-35
					40-47	40-43	36-37
						44-47	38-39
						48-51	40-41
						52-55	42-43
						56-59	44-45
						60-63	46-47
				48-63			48-49
							50-51
							52-53
							54-55
							56-57
							58-59
							60-61
							62-63
		64-127	64-95	64-79	64-71	64-67	64-65
						68-71	66-67
					72-79	72-75	68-69
						76-79	70-71
							72-73
							74-75
							76-77
							78-79
							80-81
							82-83
							84-85
							86-87
							88-89
							90-91
							92-93
							94-95
							96-97
							98-99
							100-101
							102-103
							104-105
							106-107
							108-109
							110-111
							112-113
							114-115
							116-117
							118-119
							120-121
							122-123
							124-125
							126-127
							128-129
							130-131
							132-133
							134-135
							136-137
							138-139
							140-141
							142-143
							144-145
							146-147
							148-149
							150-151
							152-153
							154-155
							156-157
							158-159
		128-191	128-159	128-143	128-135	128-131	160-161
						132-135	162-163
					136-143	136-139	164-165
						140-143	166-167
							168-169
							170-171
							172-173
							174-175
							176-177
							178-179
							180-181
							182-183
							184-185
							186-187
							188-189
							190-191
							192-193
							194-195
							196-197
							198-199
							200-201
							202-203
							204-205
							206-207
							208-209
							210-211
							212-213
							214-215
							216-217
							218-219
							220-221
							222-223
							224-225
							226-227
							228-229
							230-231
							232-233
							234-235
							236-237
							238-239
							240-241
							242-243
							244-245
							246-247
							248-249
							250-251
							252-253
							254-255
	128-255	192-255	192-223	192-207	192-199	192-195	256-257
						196-199	258-259
					200-207	200-203	260-261
						204-207	262-263
					208-215	208-211	264-265
						212-215	266-267
					216-223	216-219	268-269
						220-223	270-271
			224-255	224-239	224-231	224-227	272-273
						228-231	274-275
					232-239	232-235	276-277
						236-239	278-279
					240-247	240-243	280-281
						244-247	282-283
					248-255	248-251	284-285
						252-255	286-287

# Class C Addresses

## VLSM Chart 24-30 Bits (4th octet)

/24	/25	/26	/27	/28	/29	/30
255.255.255.0 256 Hosts	255.255.255.128 128 Hosts	255.255.255.192 64 Hosts	255.255.255.224 32 Hosts	255.255.255.240 16 Hosts	255.255.255.248 8 Hosts	255.255.255.252 4 Hosts
0 - 255	0-127	0-63	0-31	0-15	0-7	0-3
						4-7
					8-15	8-11
						12-15
				16-31	16-23	16-19
						20-23
					24-31	24-27
						28-31
			32-63	32-47	32-39	32-35
						36-39
					40-47	40-43
						44-47
				48-63	48-55	48-51
						52-55
					56-63	56-59
						60-63
		64-127	64-95	64-79	64-71	64-67
						68-71
					72-79	72-75
						76-79
				80-95	80-87	80-83
						84-87
					88-95	88-91
						92-95
			96-127	96-111	96-103	96-99
						100-103
					104-111	104-107
						108-111
				112-127	112-119	112-115
						116-119
					120-127	120-123
						124-127
	128-255	128-191	128-159	128-143	128-135	128-131
						132-135
					136-143	136-139
						140-143
				144-159	144-151	144-147
						148-151
					152-159	152-155
						156-159
			160-191	160-175	160-167	160-163
						164-167
					168-175	168-171
						172-175
				176-191	176-183	176-179
						180-183
					184-191	184-187
						188-191
		192-255	192-223	192-207	192-199	192-195
						196-199
					200-207	200-203
						204-207
				208-223	208-215	208-211
						212-215
					216-223	216-219
						220-223
			224-255	224-239	224-231	224-227
						228-231
					232-239	232-235
						236-239
				240-255	240-247	240-243
						244-247
					248-255	248-251
						252-255



