SLIIT

Discover Your Future

IT2050 - Computer Networks

Lecture 8

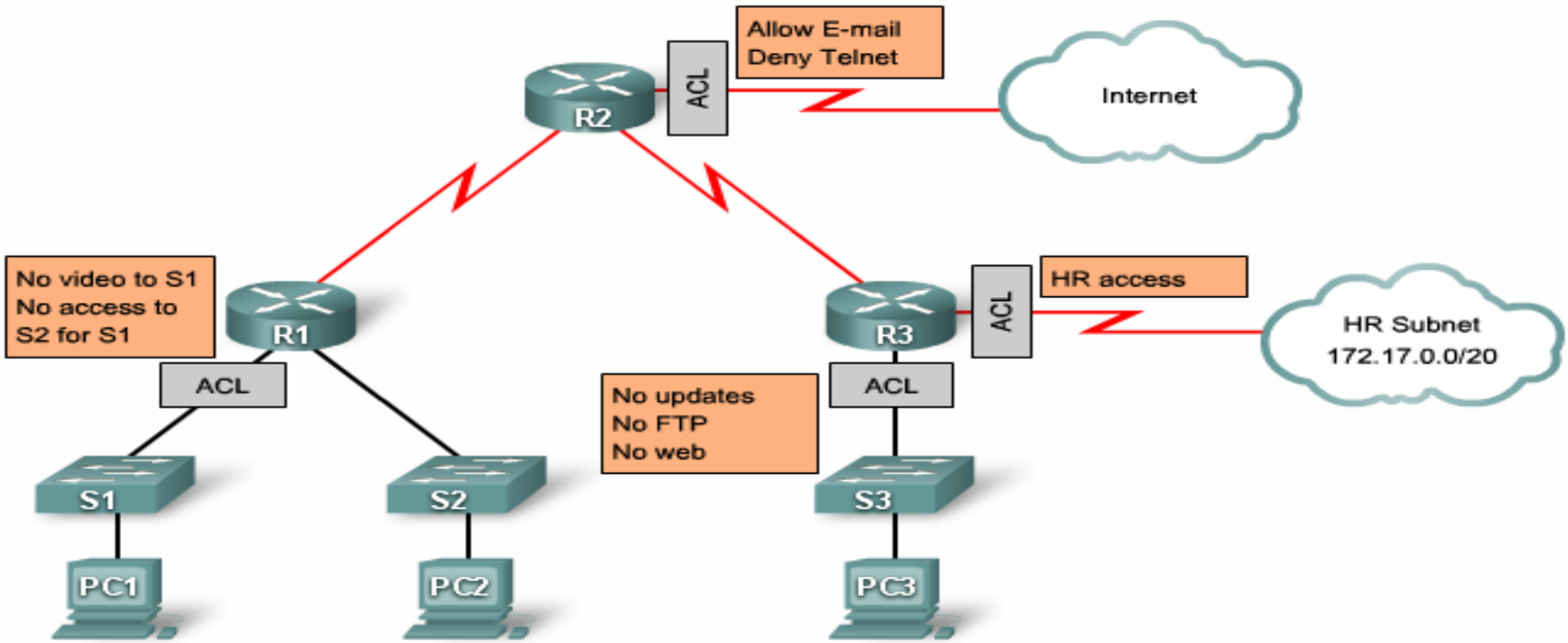
Access Control Lists (ACL)

Ms.Hansika Mahaadikara

Introduction

- ACLs are lists of conditions used to test network traffic that tries to travel across a router interface
- ACLs tell the router what types of packets to accept or deny
- Acceptance and denial can be based on specified conditions
- Conditions are based on source address, destination address, protocols, and upper-layer port numbers.

Introduction cont.



What are the things an ACL can do ?

- Prevent unwanted traffic in the network
- Prevent hackers from penetrating the network
- Prevent employees from using systems in unauthorized manner
- Filter routing updates
- Match packets for prioritization
- match packets for VPN tunneling
- Match packets for implementing quality of service features

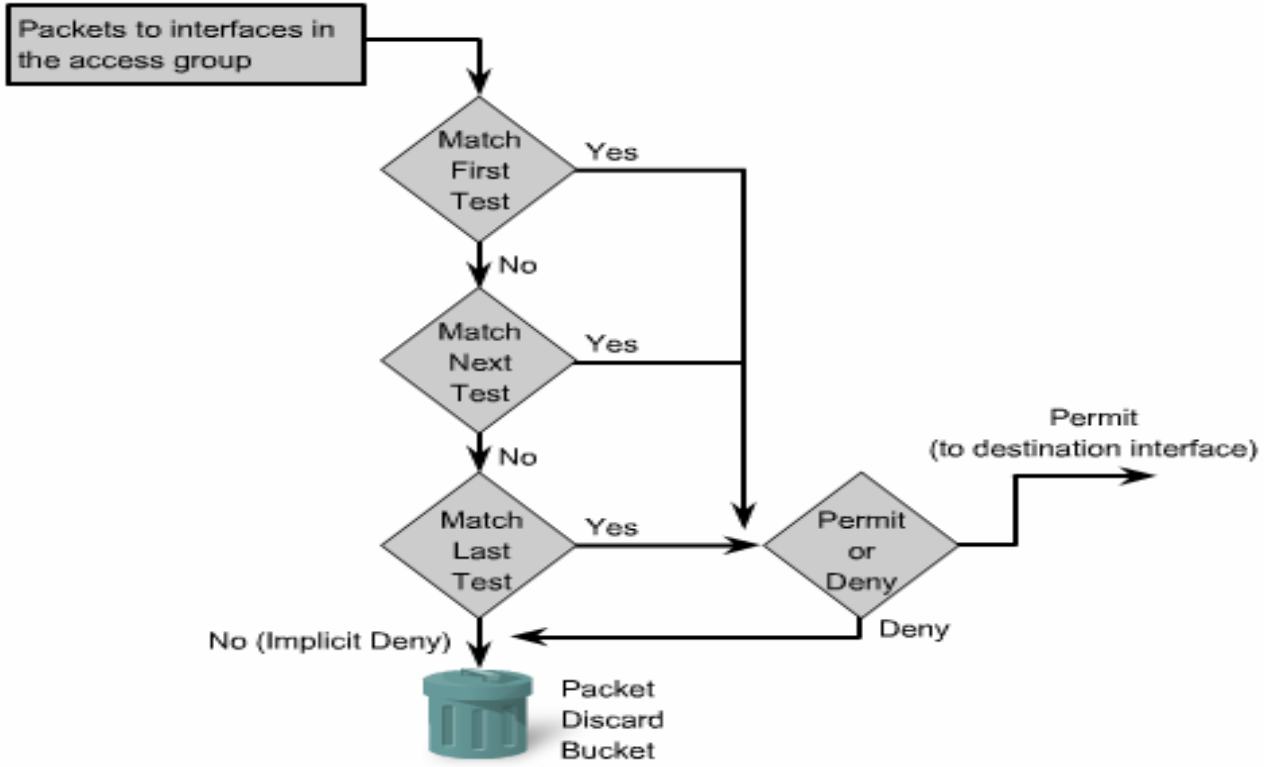
How ACL works ?

- In the ACL you can have several statements
- ACL statements operate in sequential, logical order
- If statement 1 is matched, router has to carry out the action defined in that statement
- If it isn't matched, router has to examine the next statement
- If it matches, router has to carry out the action it defines

How ACL works ? cont.

- Router has to continue looping through the list until a statement is matched or until the last statement in the list is not matched
- If none of the statements is matched, it will be passed to the final implied statement (DENY ANY)
- It results in a deny and the packet is discarded.
- Instead of proceeding in or out an interface, all these remaining packets are dropped.

How ACL works ? cont.



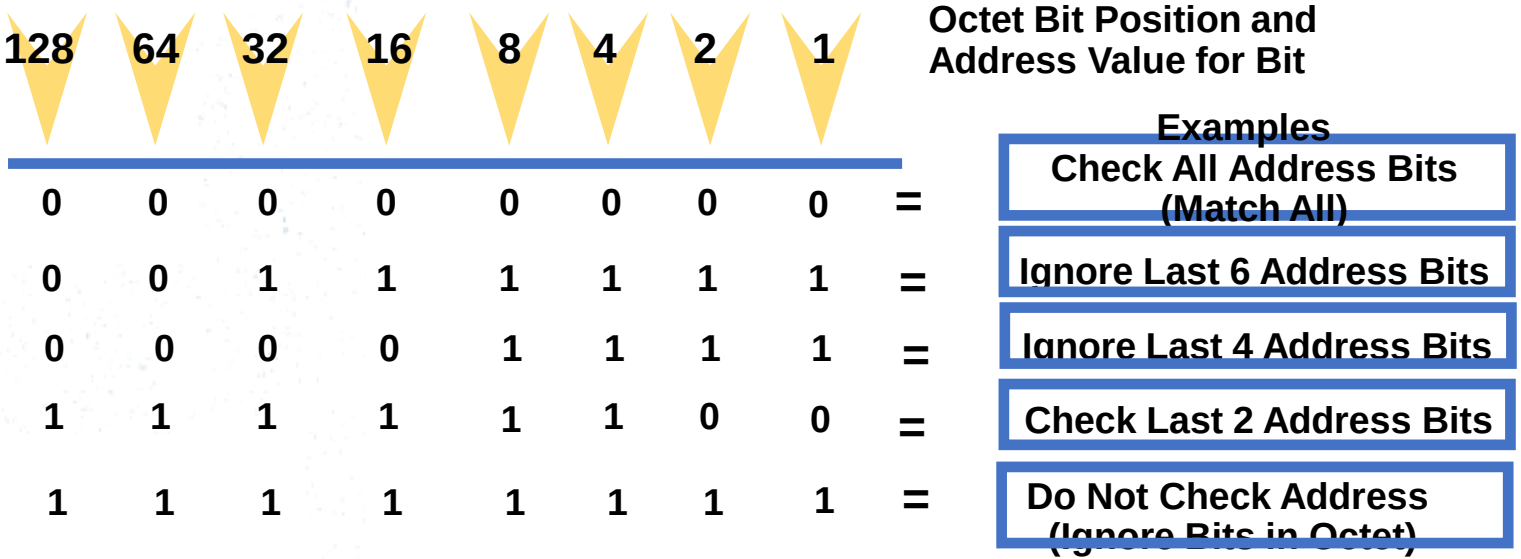
Wildcard Mask

- ACLs use wildcard masking
- Wildcard Masking for IP address bits uses the number 1 and the number 0 to identify how to treat the corresponding IP address bits.
  - A wildcard mask bit 0 means

    “check the corresponding bit value”
  - A wildcard mask bit 1 means

    “do not check (ignore) that corresponding bit value”

Wildcard Bits: How to Check the Corresponding Address Bits



- 0 means check value of corresponding address bit.
- 1 means ignore value of corresponding address bit.

Wildcard Bits to Match a Specific IP Host Address

- **Check all the address bits (match all).**
  - **Verify an IP host address, for example:**

172.30.16.29

Wildcard Mask: 0.0.0.0
(Checks All Bits)

- For example, 172.30.16.29 0.0.0.0 checks all the address bits.
- Abbreviate this wildcard mask using the IP address preceded by the keyword host (host 172.30.16.29).

Wildcard Bits to Match Any IP Address

- **Test conditions: Ignore all the address bits (match any).**
  - **An IP host address, for example:**

198.10.0.1

Wildcard Mask: 255.255.255.255

(Ignore All)

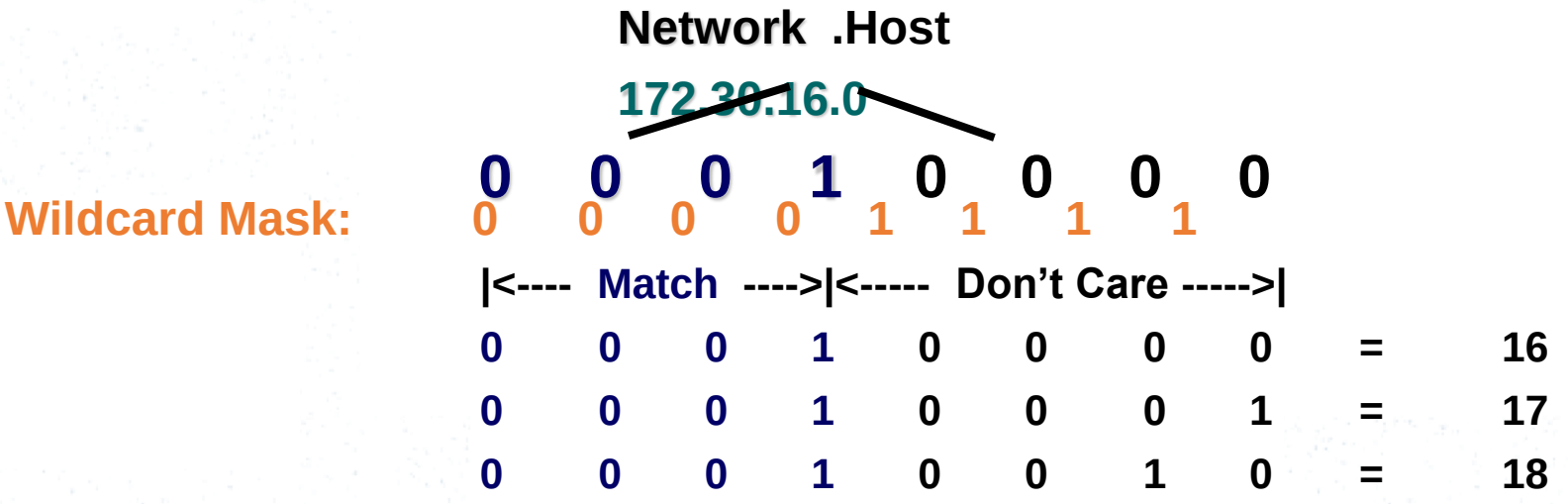
- Accept any address: 198.10.0.1 255.255.255.255.
- Abbreviate the expression using the keyword any.

Wildcard Bits to Match IP Subnets

- **Check for IP subnets 172.30.16.0/24 to 172.30.31.0/24.**

Address and wildcard mask:

172.30.16.0 0.0.15.255



Wildcard Mask cont.

Wildcard Mask	Binary Version of the Mask	Description
0.0.0.0	00000000.00000000.00000000.00000000	The entire IP address must match.
0.0.0.255	00000000.00000000.00000000.11111111	Just the first 24 bits must match.
0.0.255.255	00000000.00000000.11111111.11111111	Just the first 16 bits must match.
0.255.255.255	00000000.11111111.11111111.11111111	Just the first 8 bits must match.
255.255.255.255	11111111.11111111.11111111.11111111	Don't even bother to compare; it's automatically considered to match (0 bits need to match).

Wildcard Mask cont.

Wildcard Mask	Binary Version of the Mask	Description
0.0.15.255	00000000.00000000.00001111.11111111	Just the first 20 bits must match.
0.0.3.255	00000000.00000000.00000011.11111111	Just the first 22 bits must match.
32.48.0.255	00100000.00110000.00000000.11111111	All bits except the 3rd, 11th, 12th, and last 8 must match.

ACL Configurations

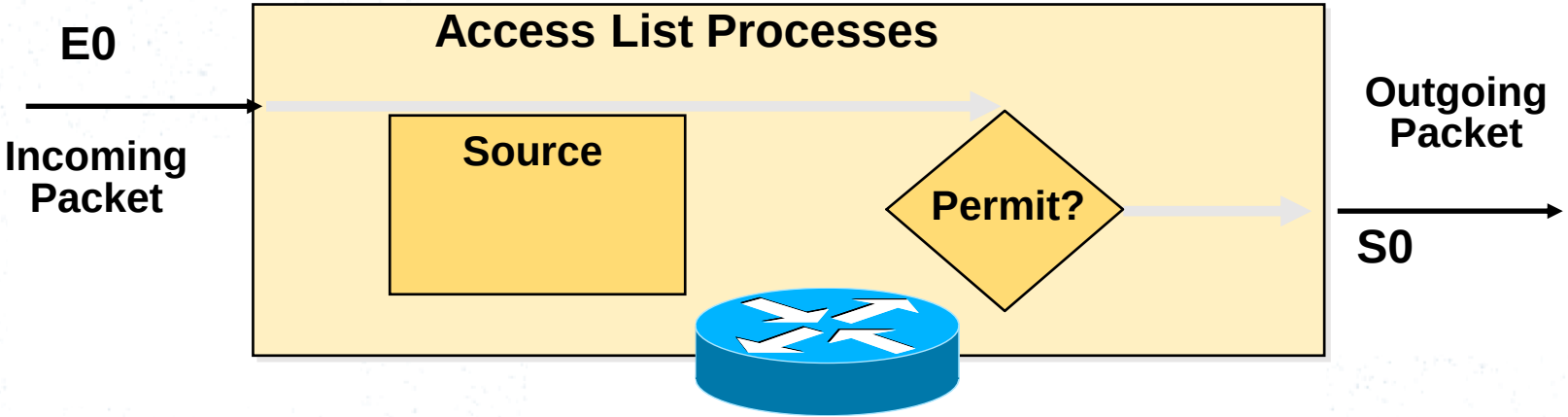
- Create ACL
- Apply ACL to an interface

Create ACL cont.

- There are two types of ACLs
  - Standard ACLs
  - Extended ACLs

Standard ACLs

- ACL number is in between 1-99
- Checks source address
- Generally permits or denies entire protocol suite



Standard ACLs cont.

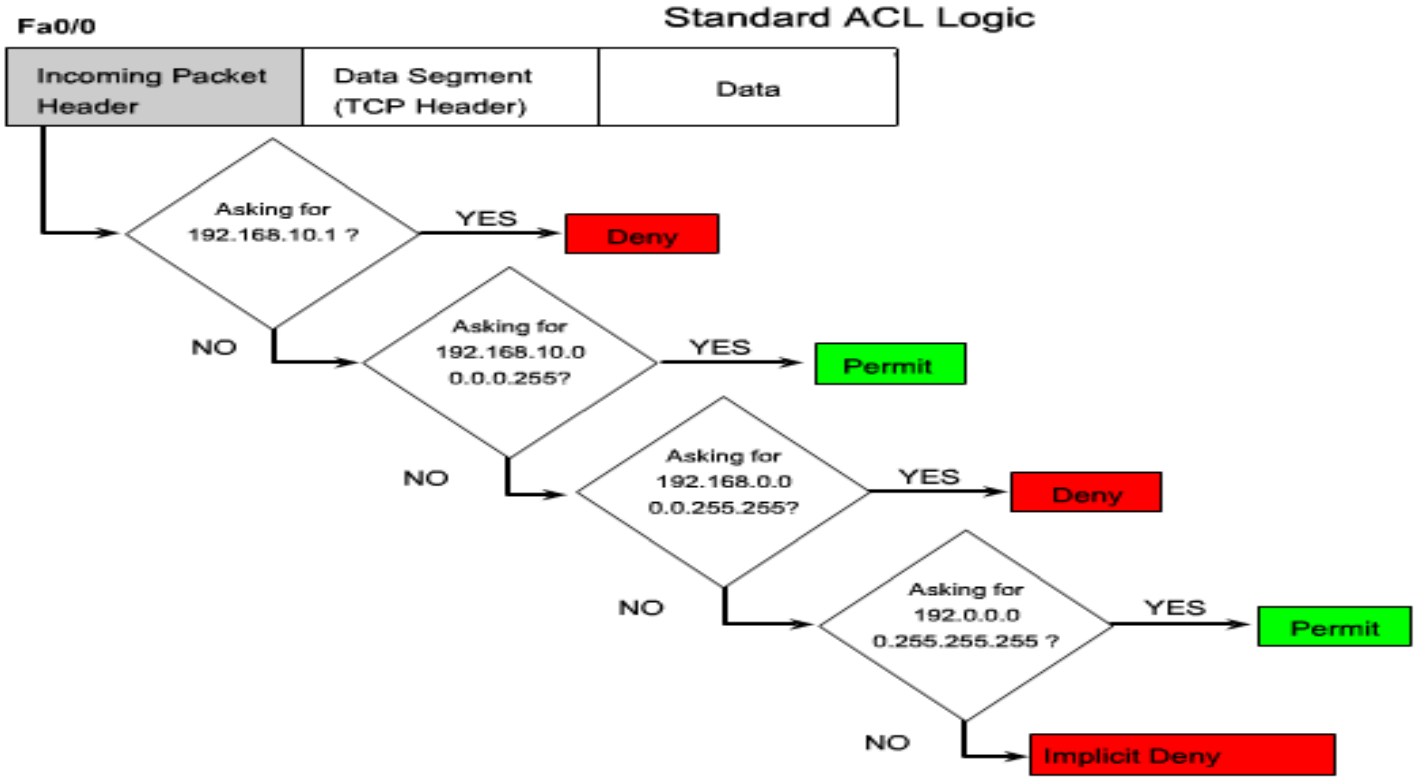
```
Router(config)# access-list access-list-number
                {permit | deny} {Source address}
                                {wildcard mask}
```

- R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255

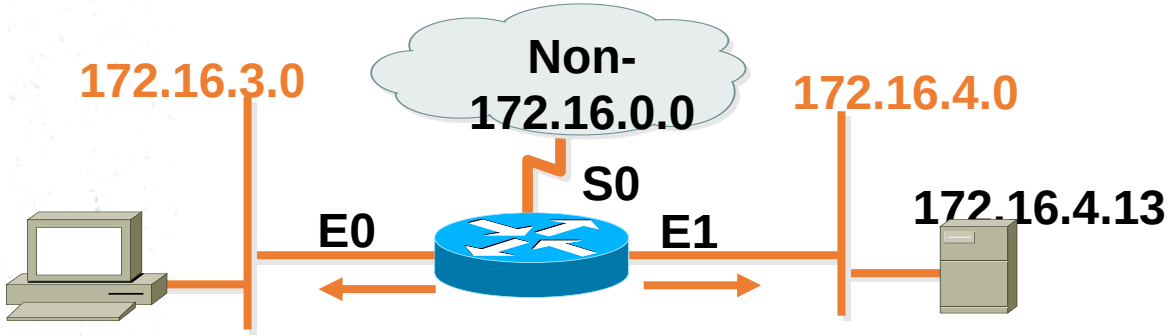
Standard ACLs cont.

- access-list 2 deny host 192.168.10.1
- access-list 2 permit 192.168.10.0 0.0.0.255
- access-list 2 deny 192.168.0.0 0.0.255.255
- access-list 2 permit 192.0.0.0 0.255.255.255

Standard ACLs cont.



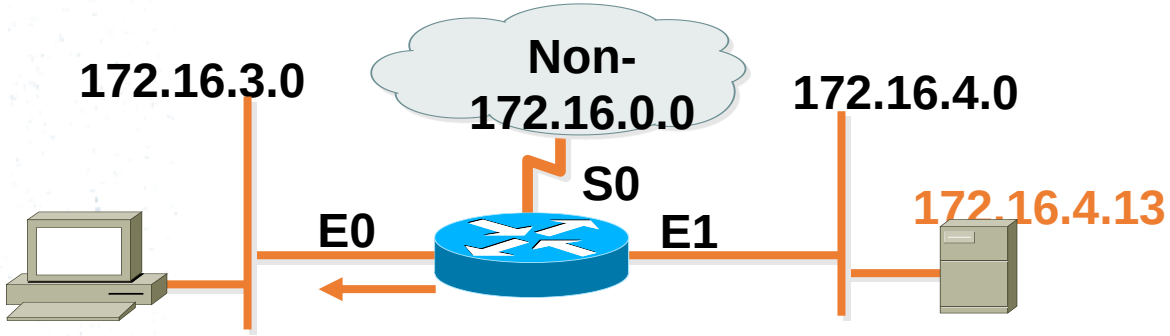
Standard ACL cont.




```
access-list 1 permit 172.16.0.0  0.0.255.255
(implicit deny all - not visible in the list)
(access-list 1 deny 0.0.0.0   255.255.255.255)
```

- **Permit my network only.**

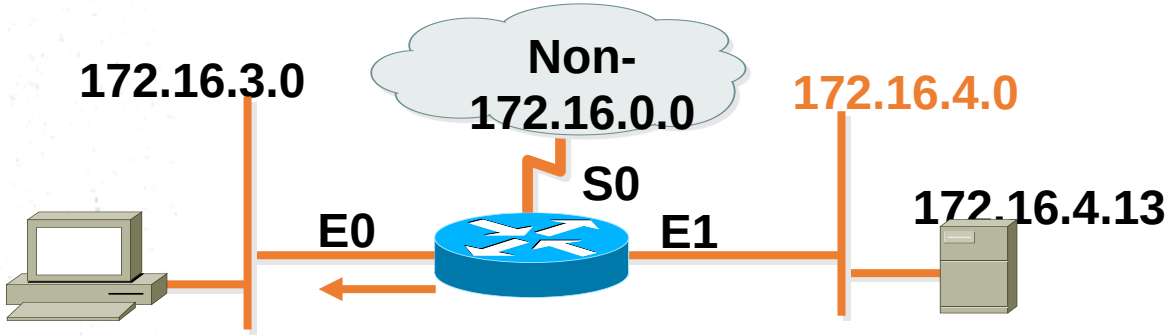
Standard ACL cont.




```
access-list 1 deny 172.16.4.13 0.0.0.0
access-list 1 permit 0.0.0.0  255.255.255.255
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)
```

- **Deny a specific host.**

Standard ACL cont.

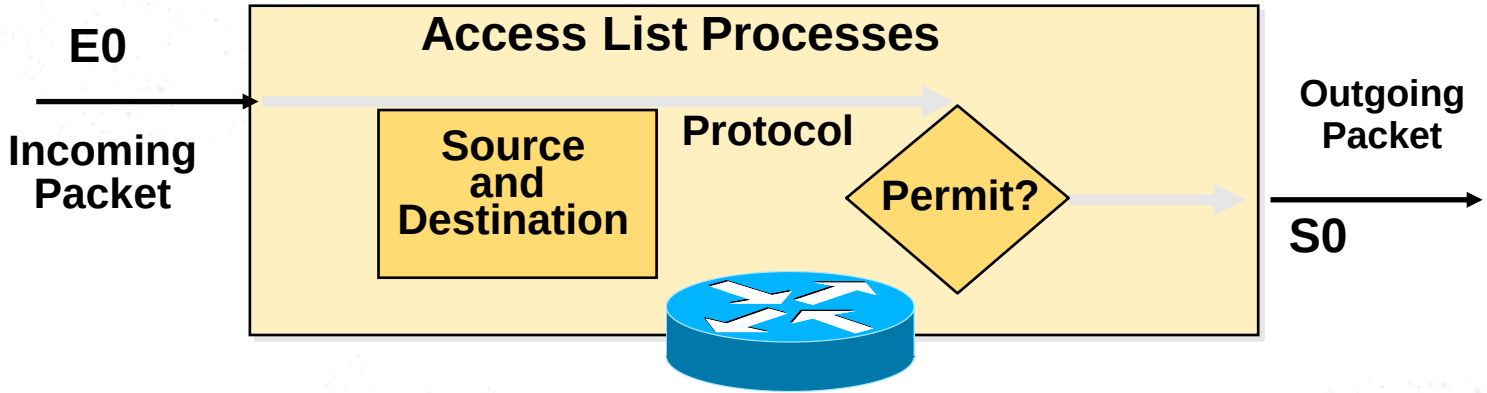



```
access-list 1 deny 172.16.4.0  0.0.0.255
access-list 1 permit any
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)
```

- **Deny a specific subnet.**

Extended ACLs

- ACL number is in between 100-199
- Checks source and destination address
- Generally permits or denies specific protocols



Extended ACLs cont.

```
Router(config)# access-list access-list-number
                {permit | deny} {protocol}
                {Source address} {wildcard mask}
           {destination address} {wildcard mask}
                   {eq | lt | gt} {port number}
```

Extended ACLs cont.

Using port numbers

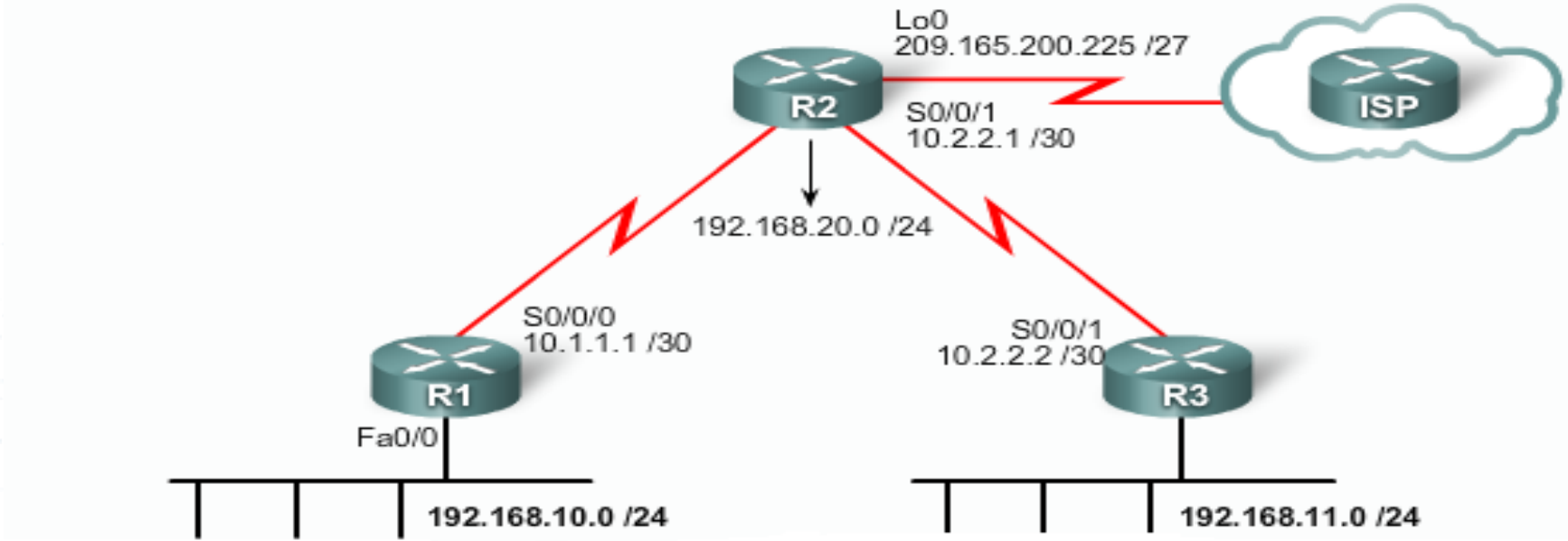
```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 22
```

Using keywords

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

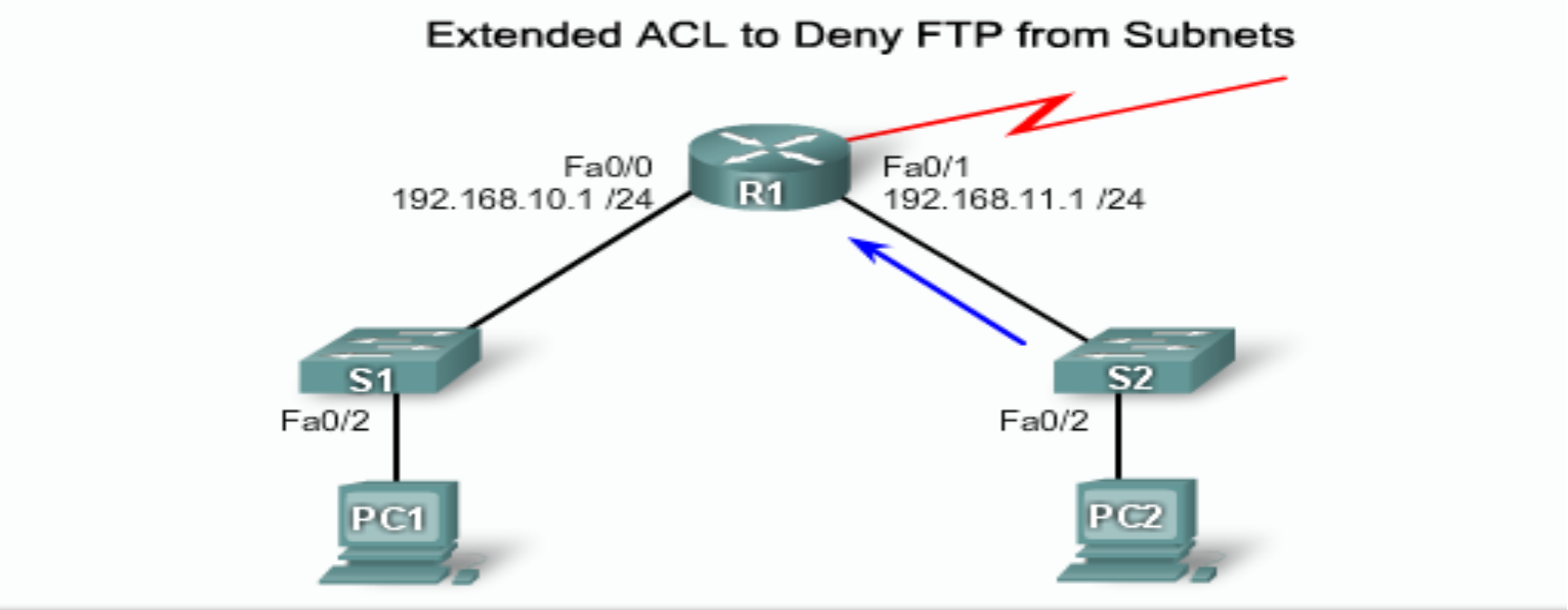
Extended ACLs cont.

- Network administrator needs to restrict Internet access of 192.168.10.0 to allow only website browsing



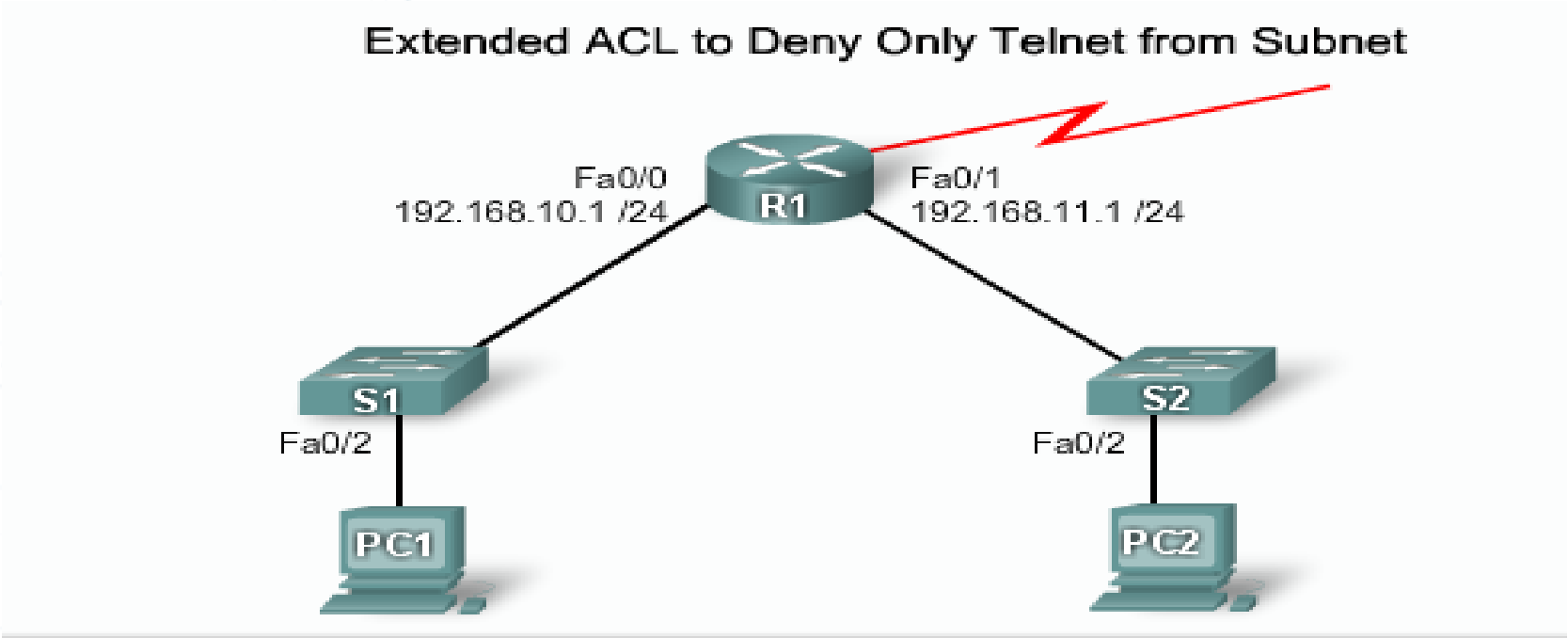

```
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
```

Extended ACLs cont.




```
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0
0.0.0.255 eq 21
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0
0.0.0.255 eq 20
R1(config)# access-list 101 permit ip any any
```

Extended ACLs cont.




```
R1(config)#access-list 101 deny tcp 192.168.11.0 0.0.0.255  any eq 23
R1(config)#access-list 101 permit ip any any
```

Access List Configuration Guidelines

- Access list numbers indicate which protocol is filtered.
- One access list per interface, per protocol, per direction is allowed.
- The order of access list statements controls testing.
- The most restrictive statements should be at the top of list.

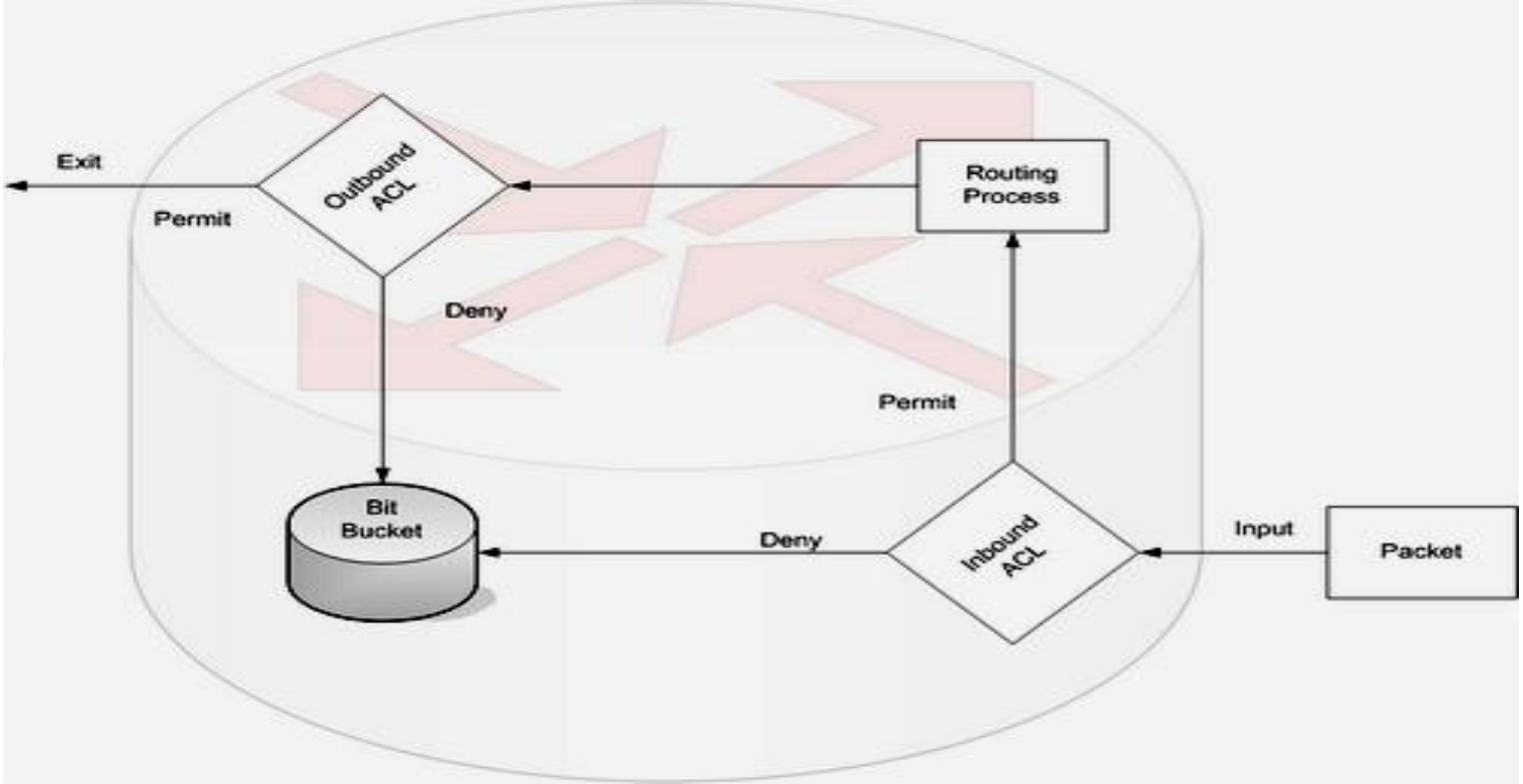
Access List Configuration Guidelines Contd….

- There is an implicit deny any as the last access list test—every list should have at least one permit statement.
- Access lists should be created before to interfaces being applied.
- Access lists filter traffic going through the router; they do not apply to traffic originated from the router.

Apply ACL to an interface

- ACLs are configured either to apply to inbound traffic or to apply to outbound traffic
- Inbound ACLs-Incoming packets are checked with the ACLs before taking the routing decisions
- An inbound ACL is efficient because it saves the overhead of routing lookups if the packet is discarded
- If the packet is permitted by the tests, it is then processed for routing
- Outbound ACLs-Incoming packets are first process for the routing decisions and then checked with the outbound ACL

Apply ACL to an interface cont.



Apply ACL to an interface cont.

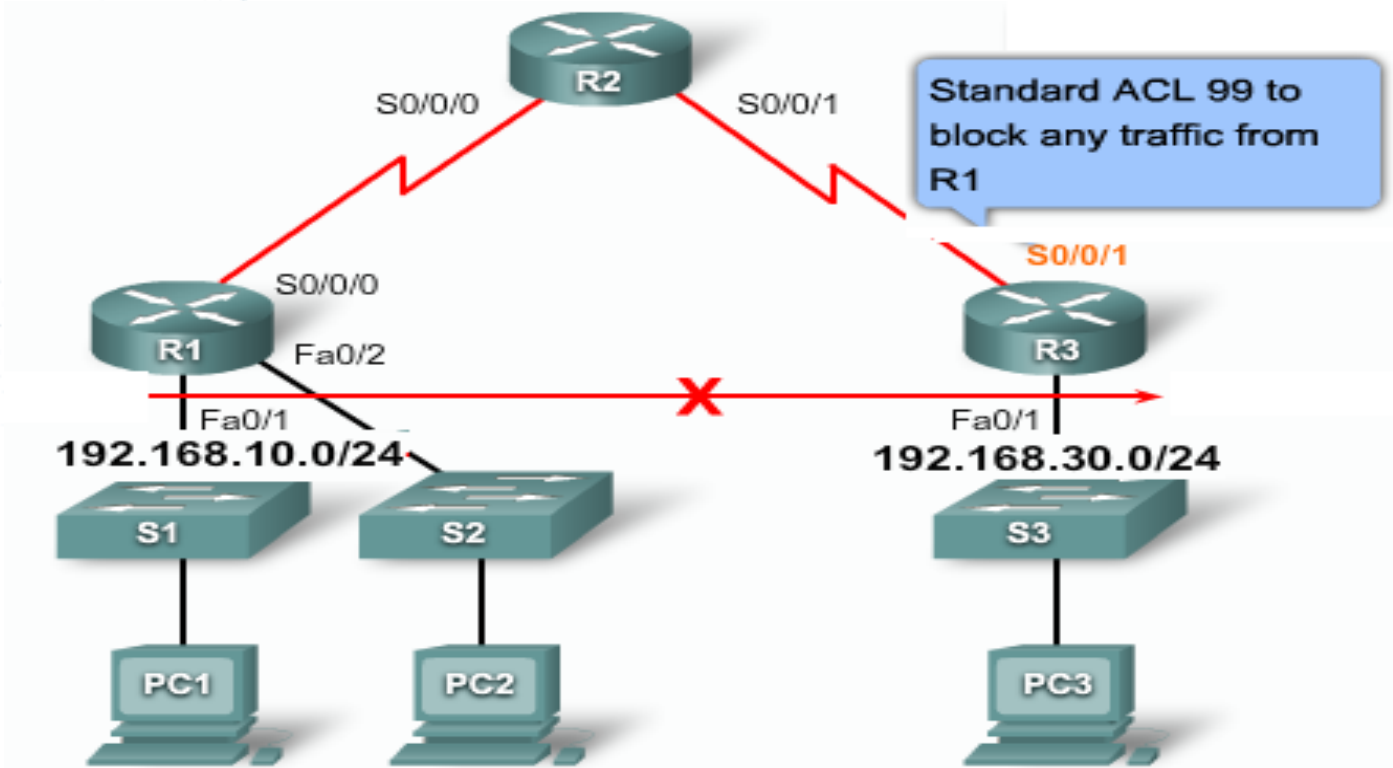
```
Router(config-if)# {protocol} access-group
                   access-list-number {in | out}
```

```
R1(config)# interface S0/0/0
R1(config-if)# ip access-group 103 out
R1(config-if)# ip access-group 104 in
```

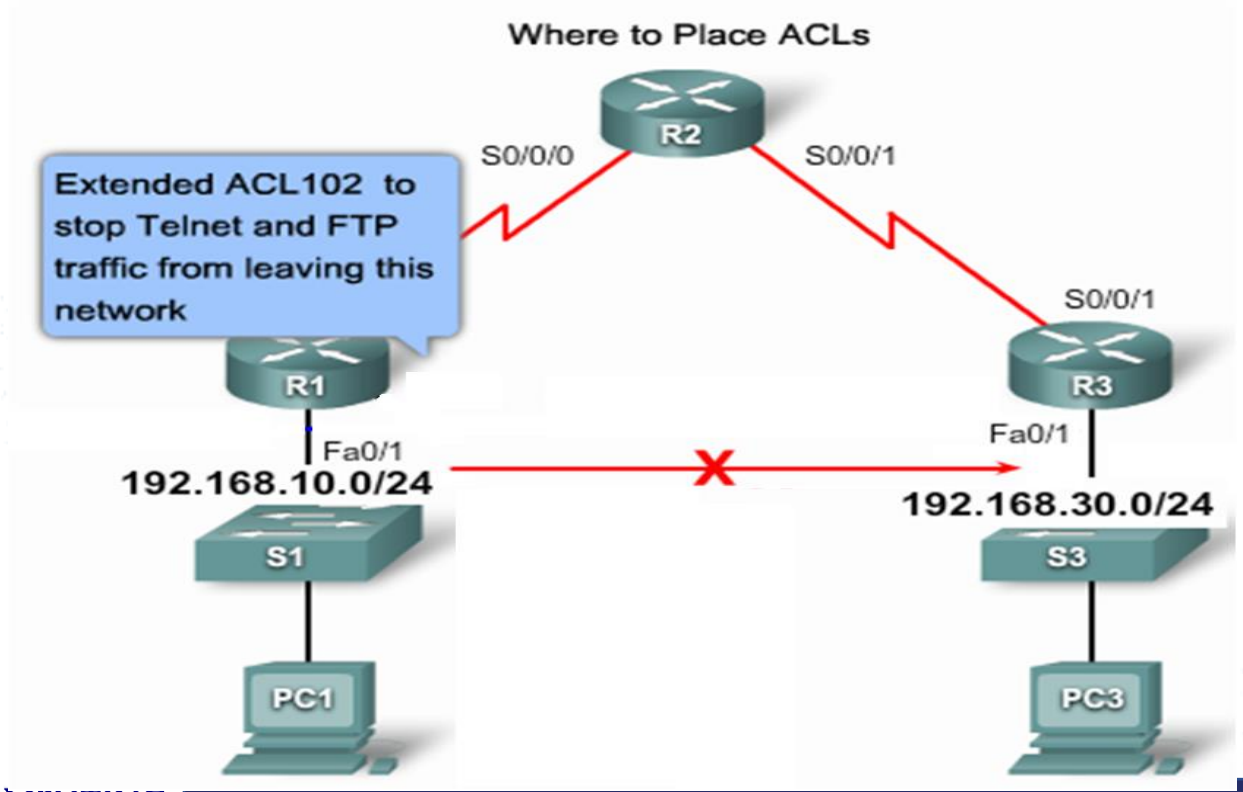
Placing ACLs

- Proper ACL placement will filter traffic and make the network more efficient
- The ACL should be placed where it has the greatest impact on efficiency.
- The general rule is to put the Extended ACLs as close as possible to the source of the traffic denied
- Standard ACLs should be placed as close to the destination as possible

Placing ACLs cont.



Placing ACLs cont.



Named ACLs

- Naming an ACL makes it easier to understand its function
- For example, an ACL to deny FTP could be called NO_FTP
- ACL names are alphanumeric

  and must be unique

  and must not begin with a number

Creating Named ACLs

```
Router(config)# ip access-list
      {standard | extended} {name}
```

```
Router(config-std-nacl)# {permit | deny}
      {source address} {wild card mask}
```

Creating Named ACLs cont.

```
R1(config)#ip access-list standard NO_ACCESS
R1(config-std-nacl)#deny host 192.168.11.10
R1(config-std-nacl)#permit 192.168.11.0 0.0.0.255
R1(config-std-nacl)#interface Fa0/0
R1(config-if)#ip access-group NO_ACCESS out
```

Advantages of Named ACLs

- it is easier to understand the function of ACL because you have used the function of ACL as its name
- It is easier to edit because Named ACLs allow you to delete individual entries in a specific ACL
- Can use sequence numbers to insert statements anywhere in the named ACL

Other types of ACLs

- Dynamic ACLs
- Time based ACLs
- Reflexive ACLs
- Turbo ACLs