Chapter 09

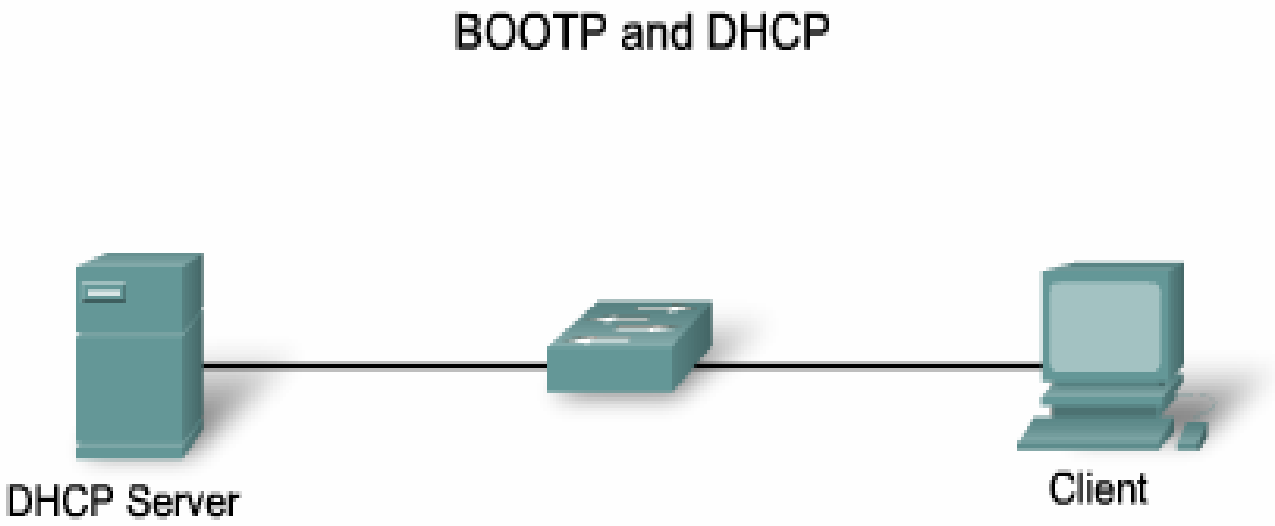
IP Services and Management

Outlines

- Dynamic Host Configuration Protocol (DHCP)
- Access Control Lists (ACL)
- Network Address Translation (NAT)
- Routers Password recovery

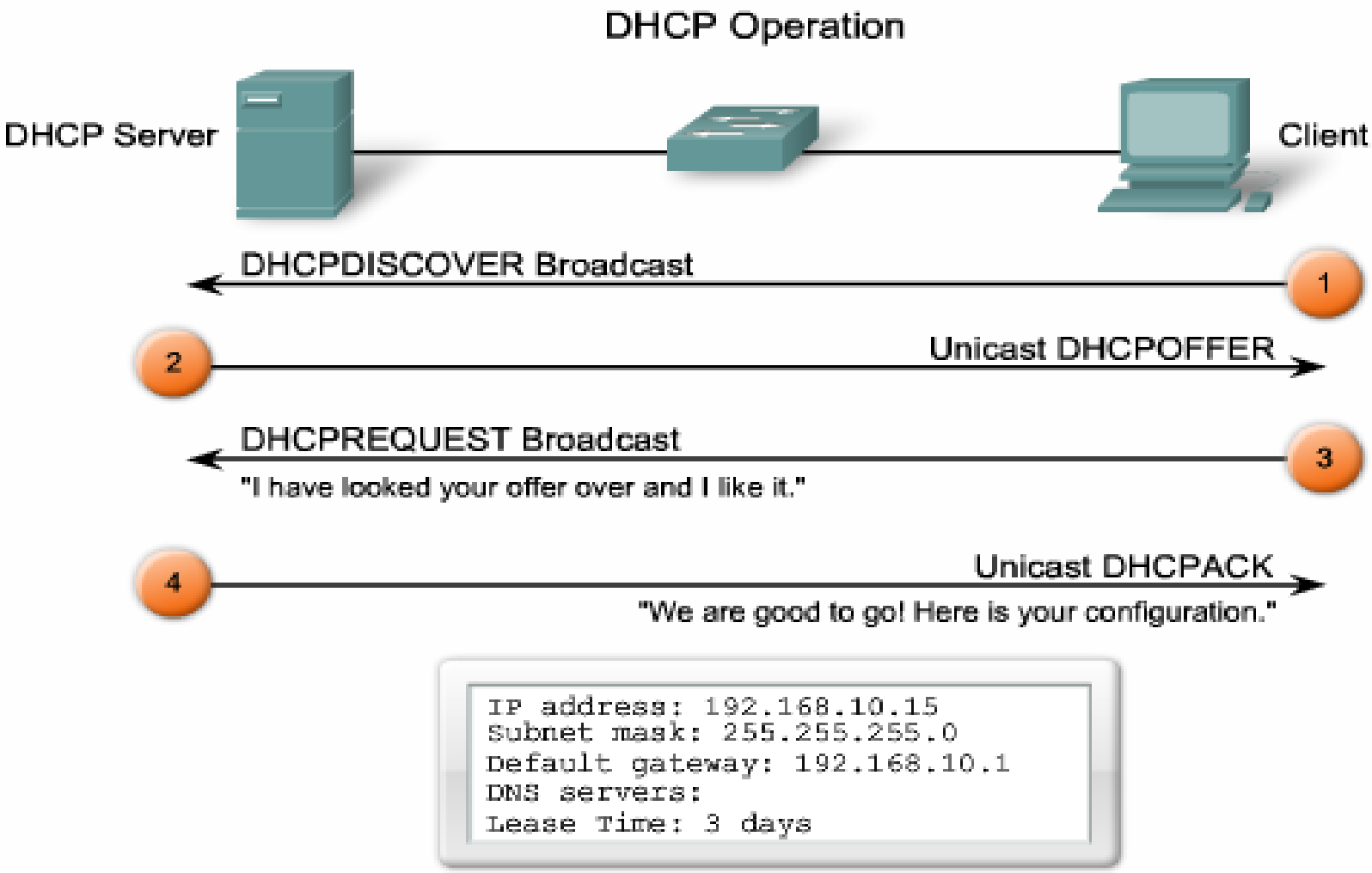
Dynamic Host Configuration Protocol (DHCP)

BOOTP vs DHCP

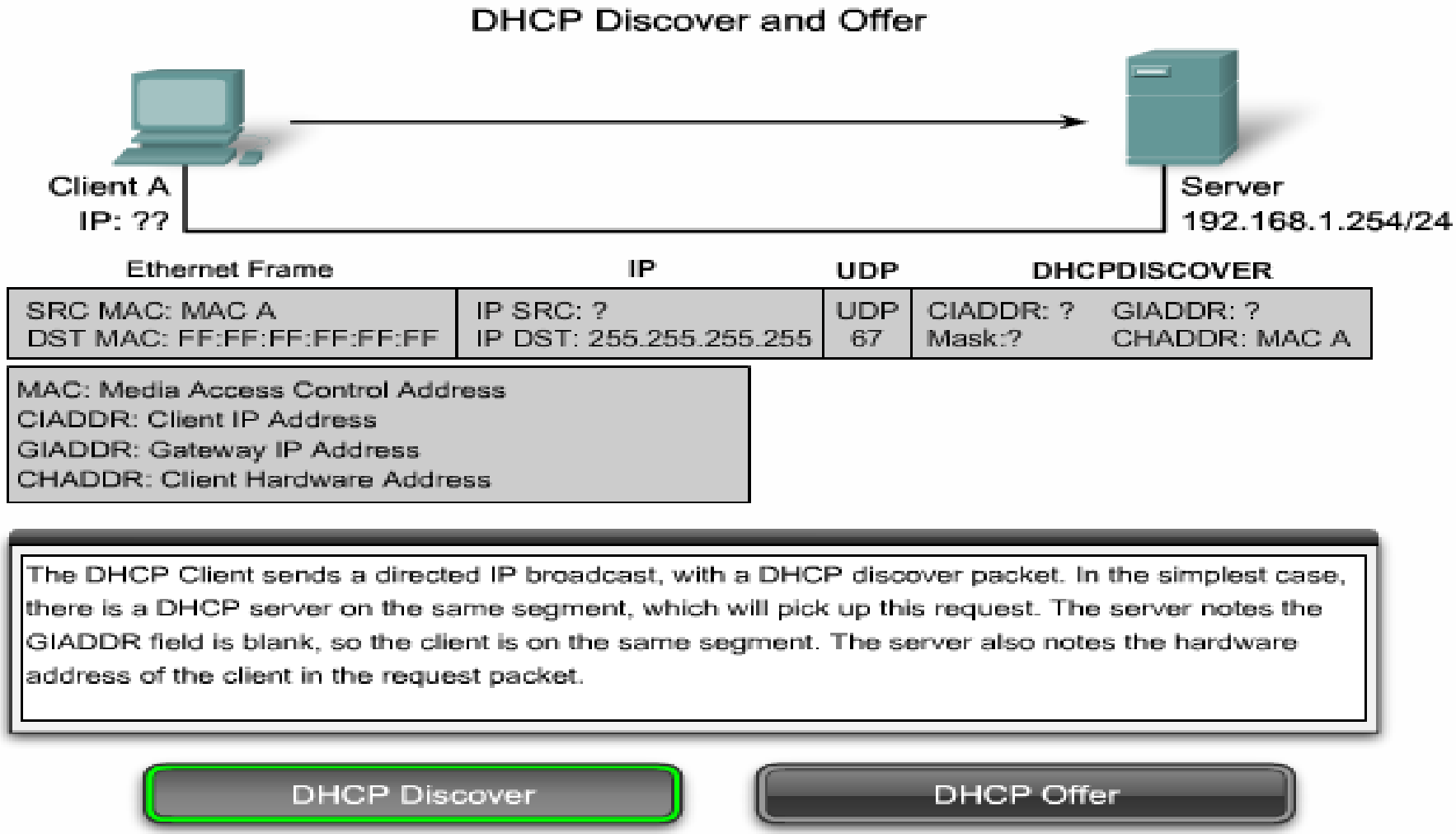


BOOTP	DHCP
Static mappings	Dynamic mappings
Permanent assignment	Lease
Only supports four configuration parameters	Supports over 20 configuration parameters

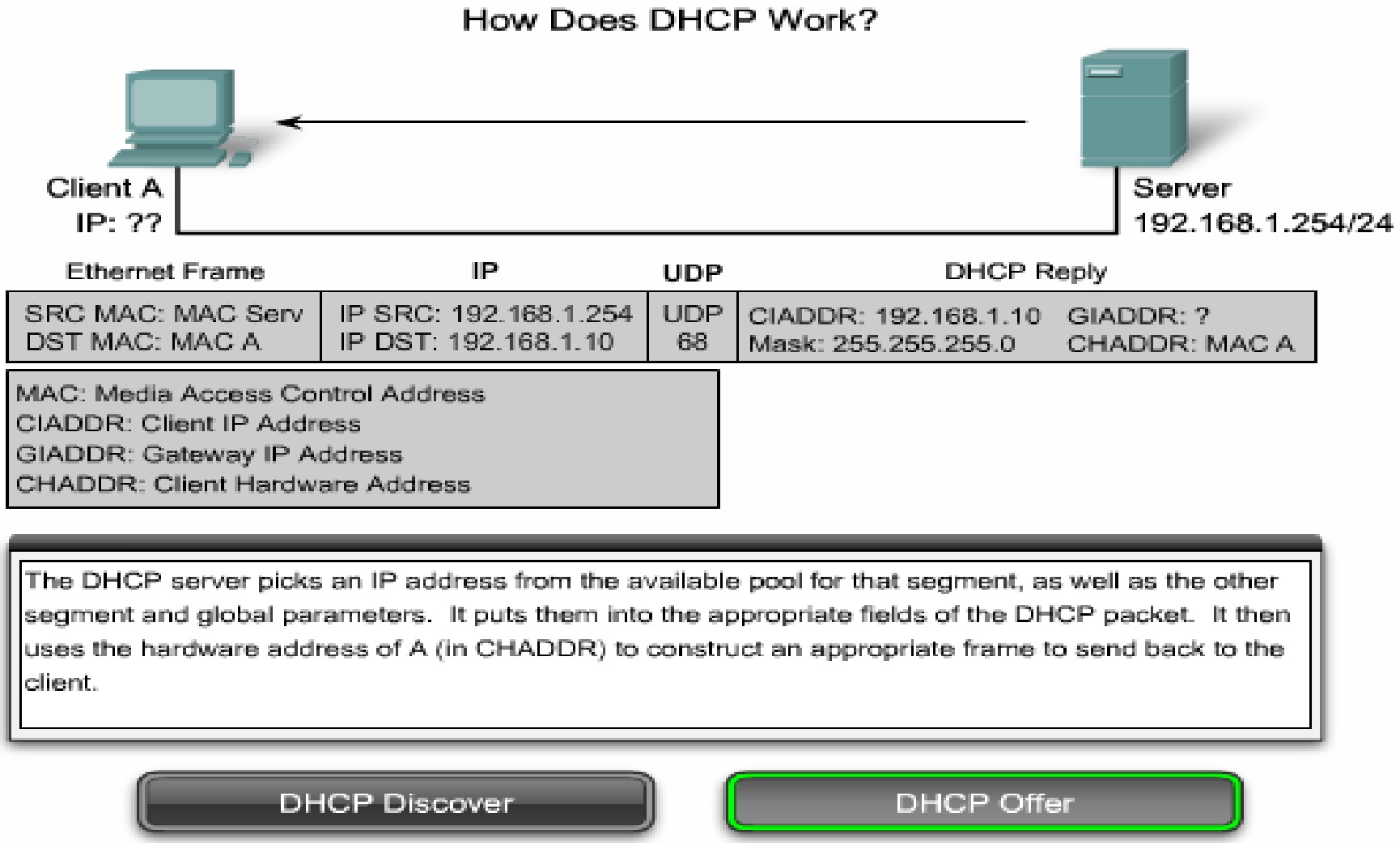
DHCP operation



DHCP operation



DHCP operation



DHCP configuration

Configuring DHCP Step 1: Excluding IP Addresses

```
R1(config)#ip dhcp excluded-address low-address [high-address]
```

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)#ip dhcp excluded-address 192.168.10.254
```

Excluded Addresses | DCHP Pool | DHCP Tasks | DHCP Example

DHCP configuration

Configuring DHCP Step 2: Configuring a DHCP Pool

```
R1(config)#ip dhcp pool pool-name
```

```
R1(config)#ip dhcp pool LAN-POOL-1
R1(dhcp-config)#
```

Excluded Addresses | DCHP Pool | DHCP Tasks | DHCP Example

DHCP configuration

Configuring DHCP Step 3: Specific Tasks

Required Tasks	Command
Define the address pool	`network network-number [mask | /prefix-length]`
Define the default router or gateway	`default-router address [address2...address8]`

Optional Tasks	Command
Define a DNS server.	`dns-server address [address2...address8]`
Define the domain name	`domain-name domain`
Define the duration of the DHCP lease	`lease {days [hours] [minutes] | infinite}`
Define the NetBIOS WINS server	`netbios-name-server address [address2...address8]`

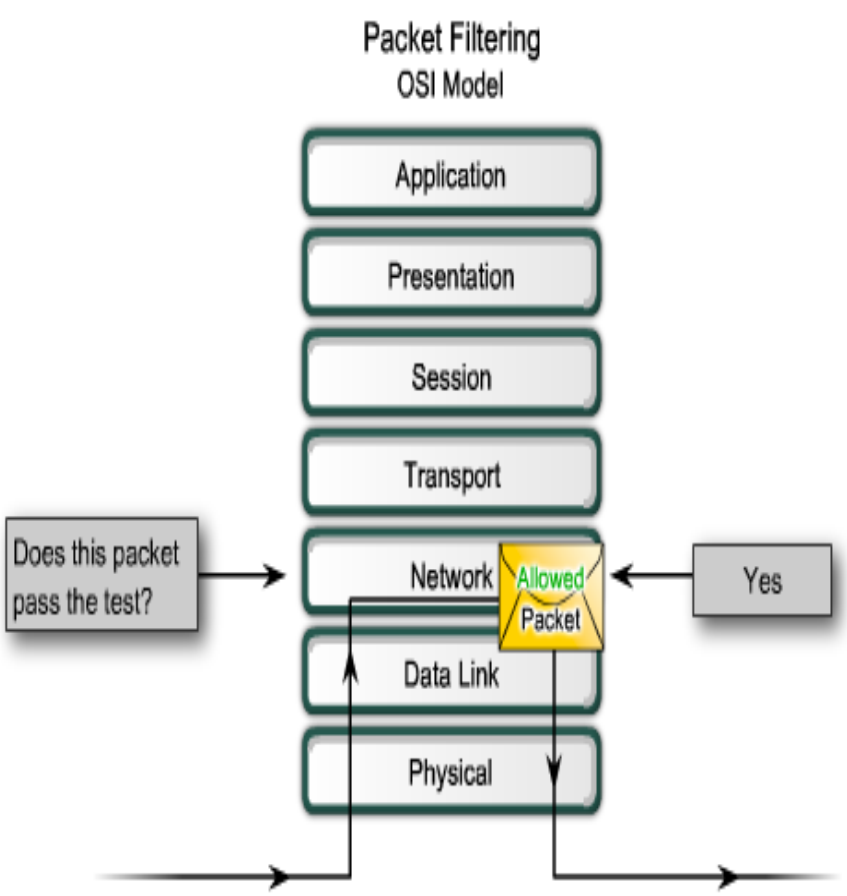
DHCP configuration

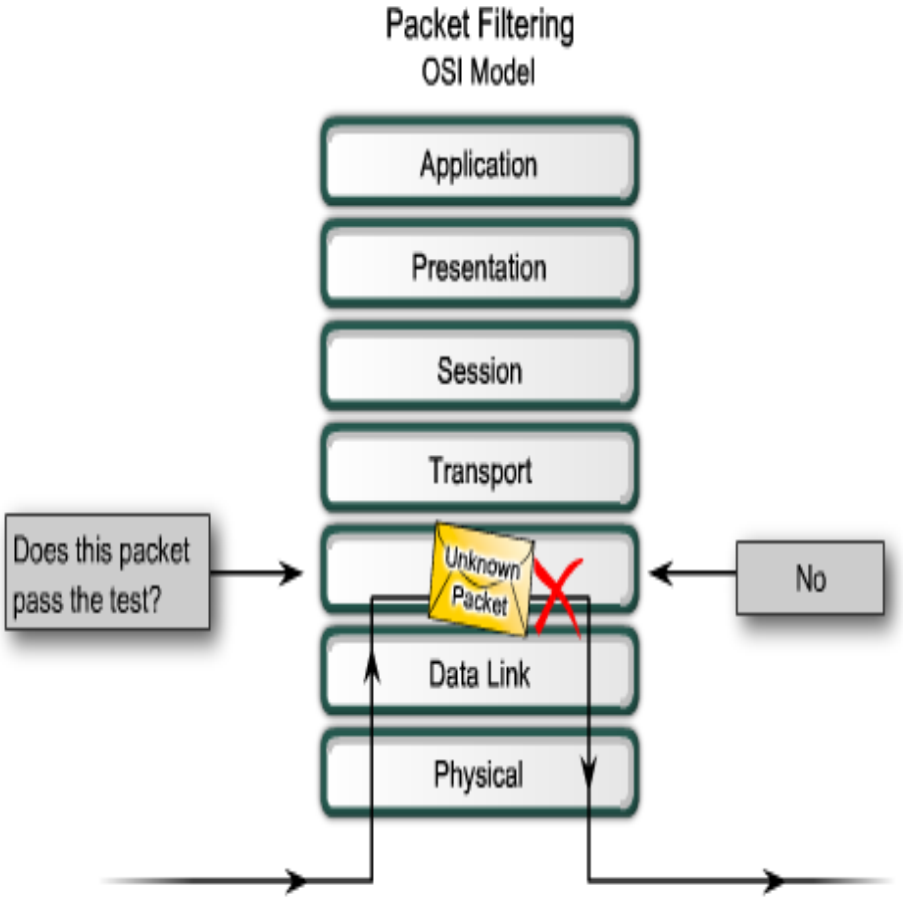
DHCP Configuration Example

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# domain-name span.com
R1(dhcp-config)# end
```

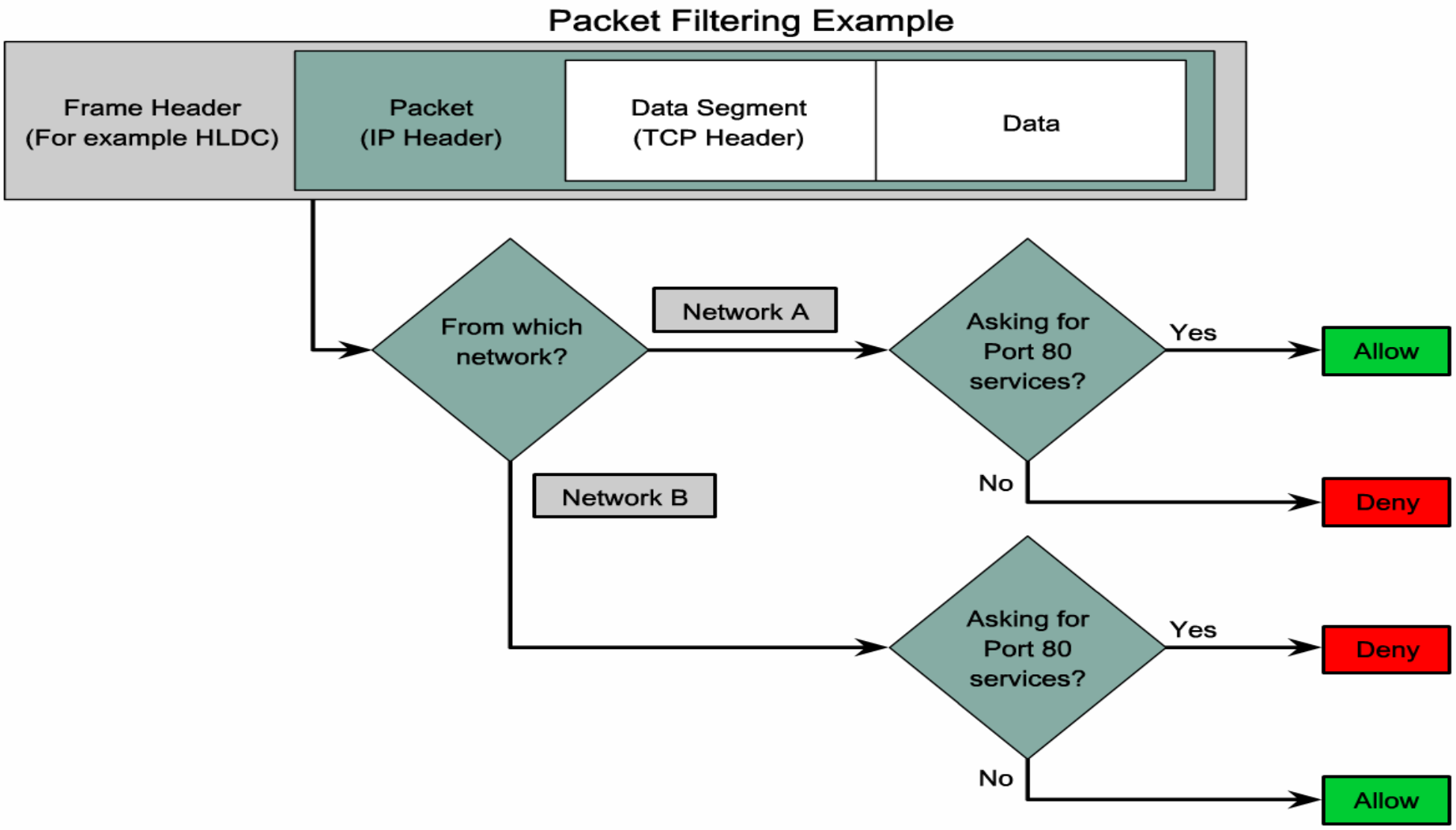
Access Control Lists (ACL)

What is the packet filter?

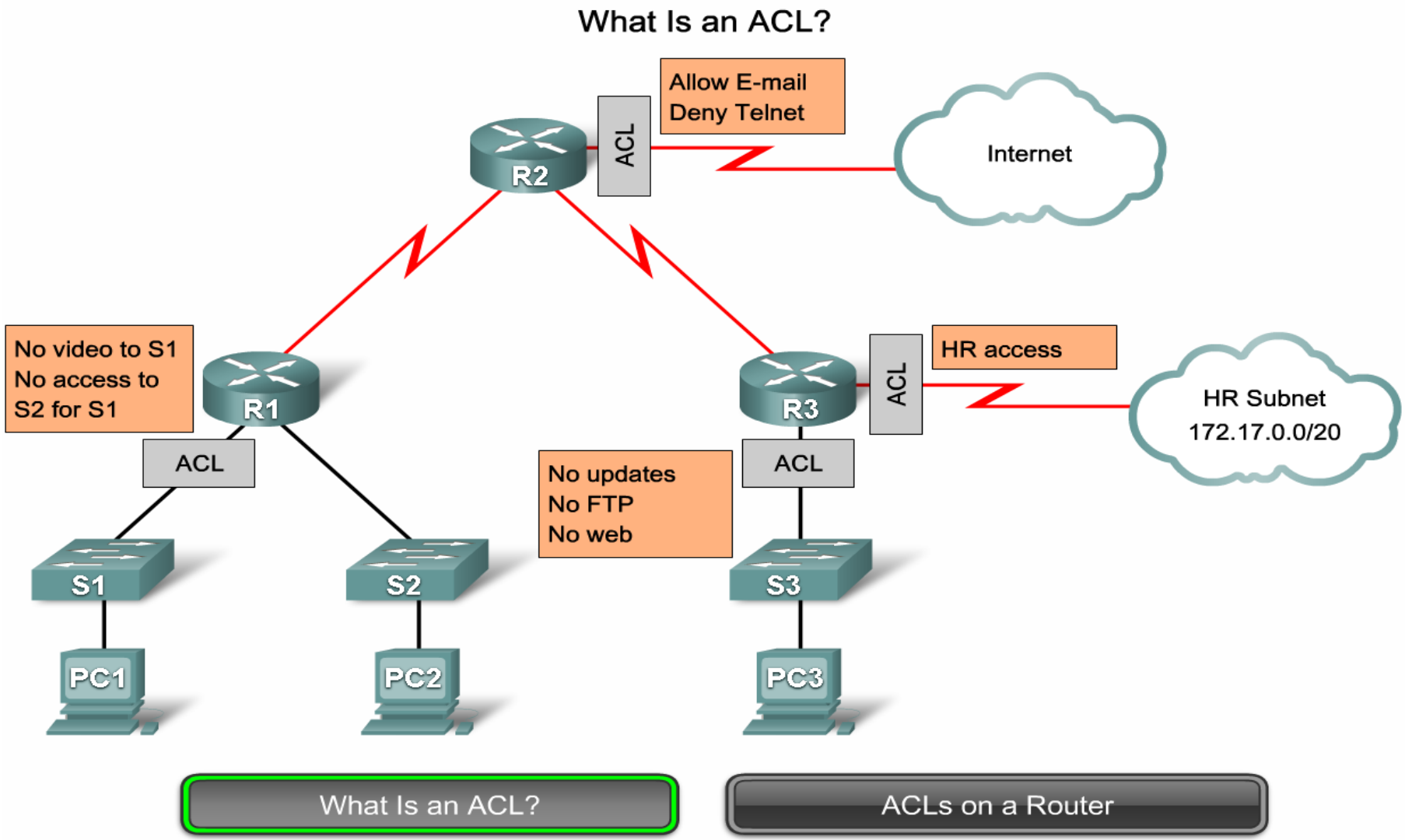




What is the packet filter?



What is an Access Control List (ACL)?



What is an Access Control List (ACL)?

ACL Traffic Filtering on a Router

One list per interface, per direction, and per protocol

With two interfaces and three protocols running, this router could have a total of 12 separate ACLs applied.

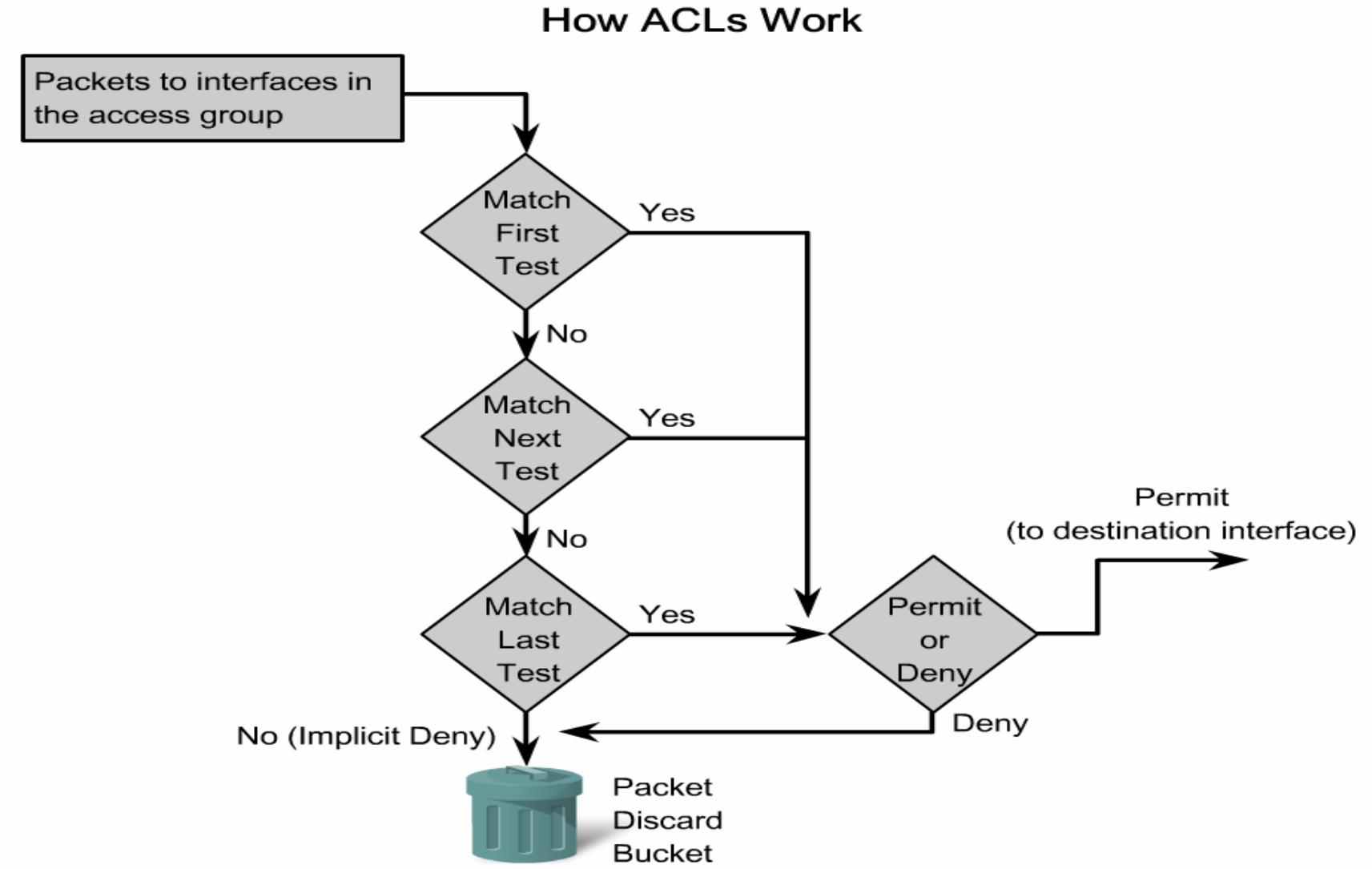
The three Ps for using ACLs

You can only have one ACL per protocol, per interface, and per direction:

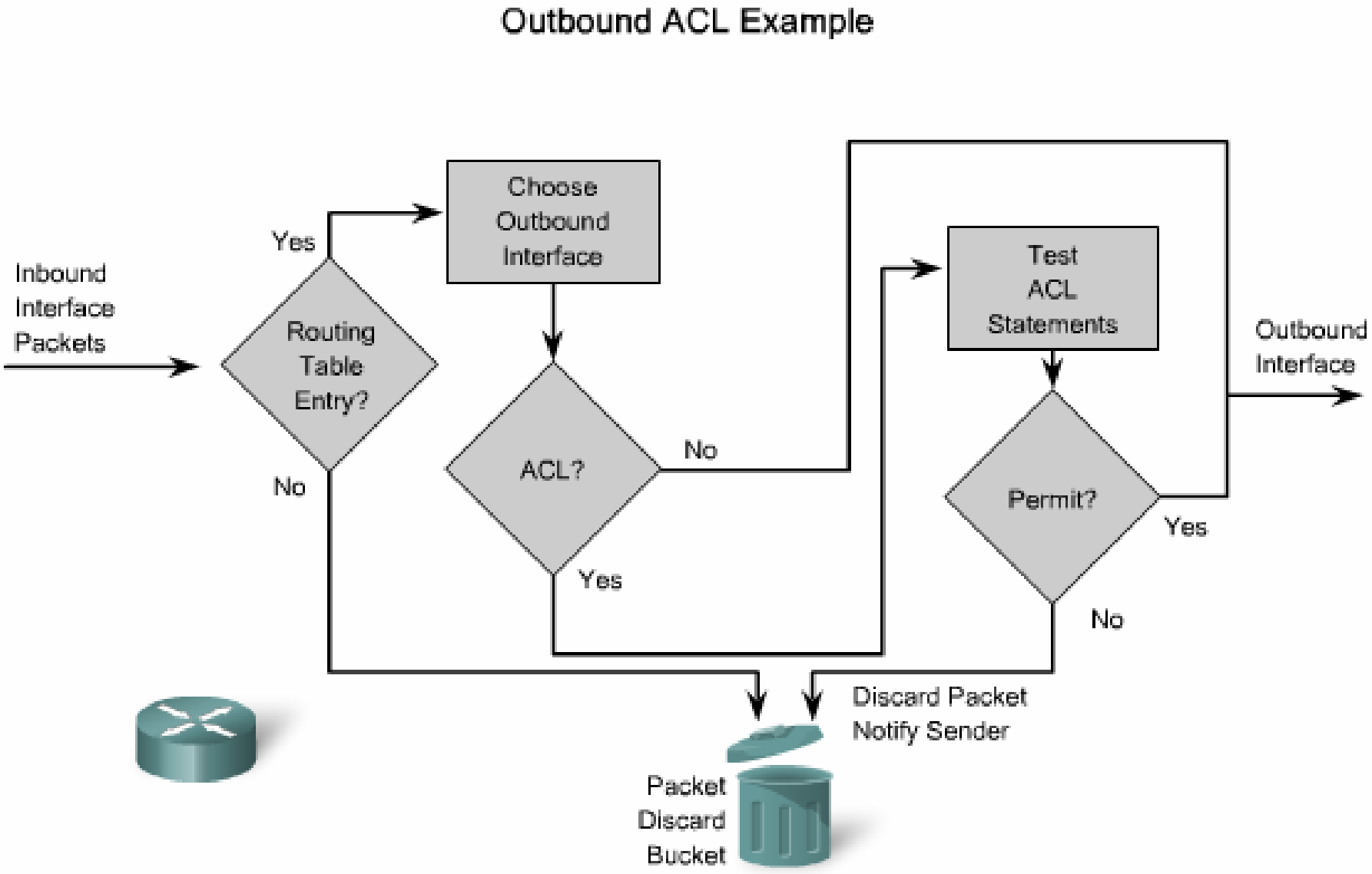
- One ACL per protocol (e.g., IP or IPX)
- One ACL per interface (e.g., FastEthernet0/0)
- One ACL per direction (i.e., IN or OUT)

What is an Access Control List (ACL)?

- Inbound ACL flow chart



What is an Access Control List (ACL)?



Wild Card Mask (WCM)

Wildcard Mask Example

	Decimal Address	Binary Address
IP address to be processed	192.168.10.0	11000000.10101000.00001010.00000000
Wildcard mask	0.0.255.255	00000000.00000000.11111111.11111111
Resulting IP address	192.168.0.0	11000000.10101000.00000000.00000000

Wildcard Mask Calculation - 1

255.255.255.255
- 255.255.255.000
000.000.000.255

Wildcard Mask Calculation - 2

255.255.255.255
- 255.255.255.240
000.000.000.015

Types of the Access Control List (ACL)

Types of Cisco ACLs

Standard ACLs filter IP packets based on the source address only.

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Extended ACLs filter IP packets based on several attributes, including the following:

- Source and destination IP addresses
- Source and destination TCP and UDP ports
- Protocol type (IP, ICMP, UDP, TCP, or protocol number)

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

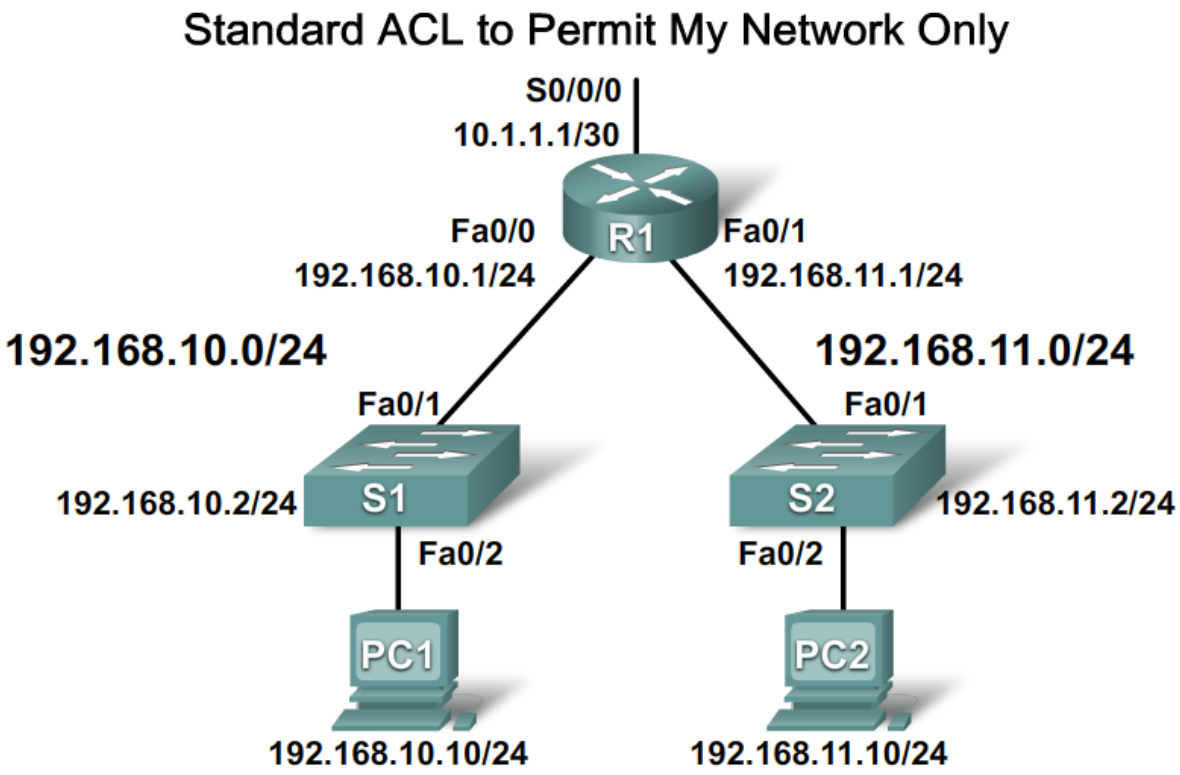
Where to place ACL ?

- Standard ACL is placed as close the destination as possible.
- Extended ACL is placed as close the source as possible.

Access Control List configuration

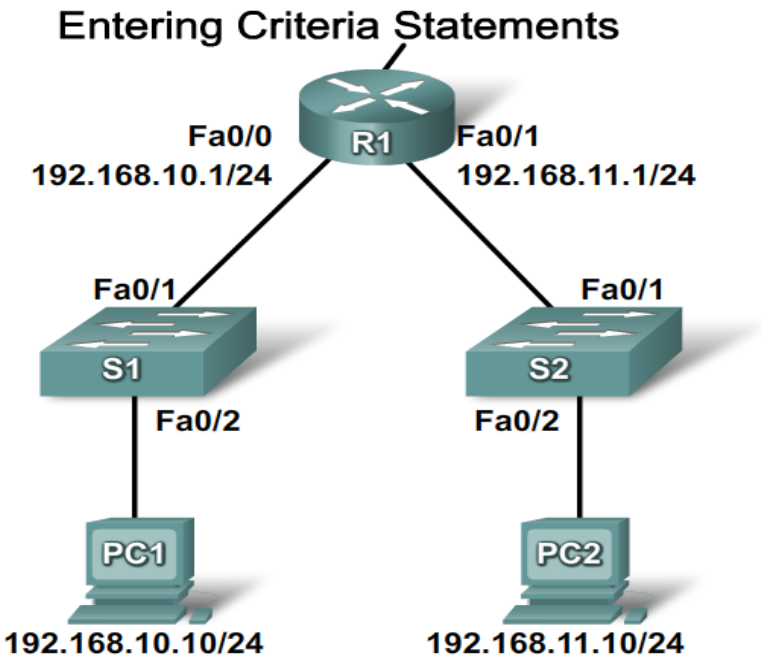
- Firstly : from global configuration mode write you ACL sentences
- Secondly : apply the ACL under the interface in the appropriate direction

Configure Standard ACLs




```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface S0/0/0
R1(config-if)# ip access-group 1 out
```

Configure Extended ACLs



ACL 101

```
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
```

ACL 102

```
access-list 102 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 102 deny ip any any
```

Extended ACL example

Extended ACL Examples

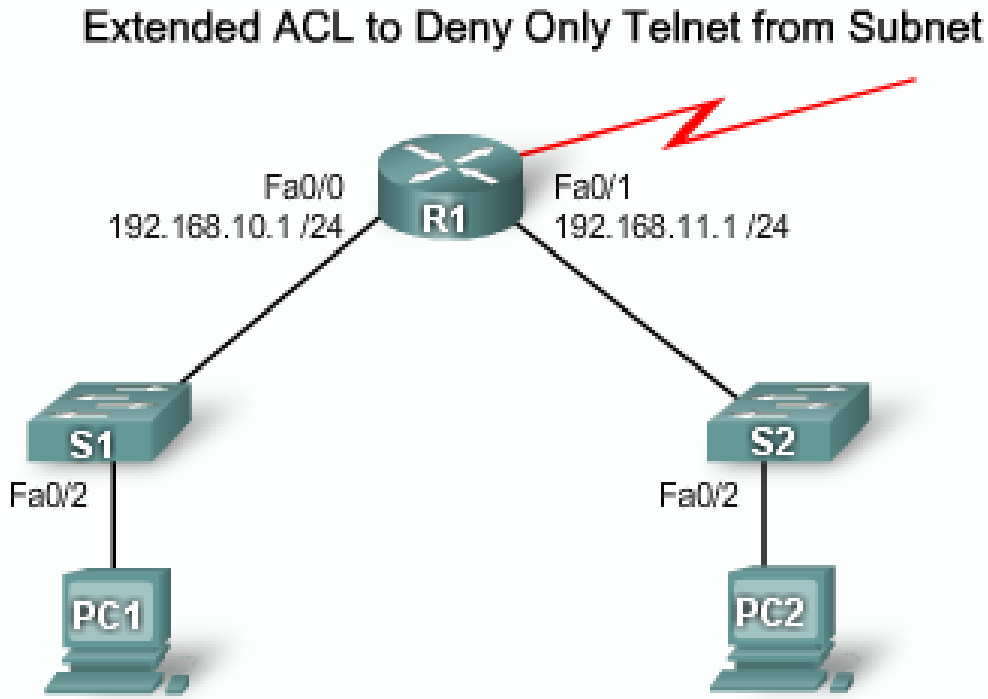
Using port numbers

```
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
```

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
```

Extended ACL example



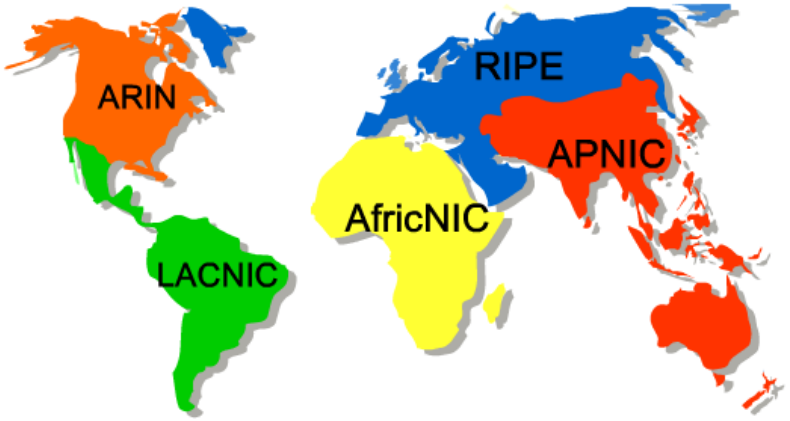

```
R1(config)#access-list 101 deny tcp 192.168.11.0 0.0.0.255  any eq 23
R1(config)#access-list 101 permit ip any any

R1(config)# interface Fa0/0
R1(config-if)#ip access-group 101 out
```

Network Address Translation (NAT)

Network Address Translation

Public and Private Internet Addresses



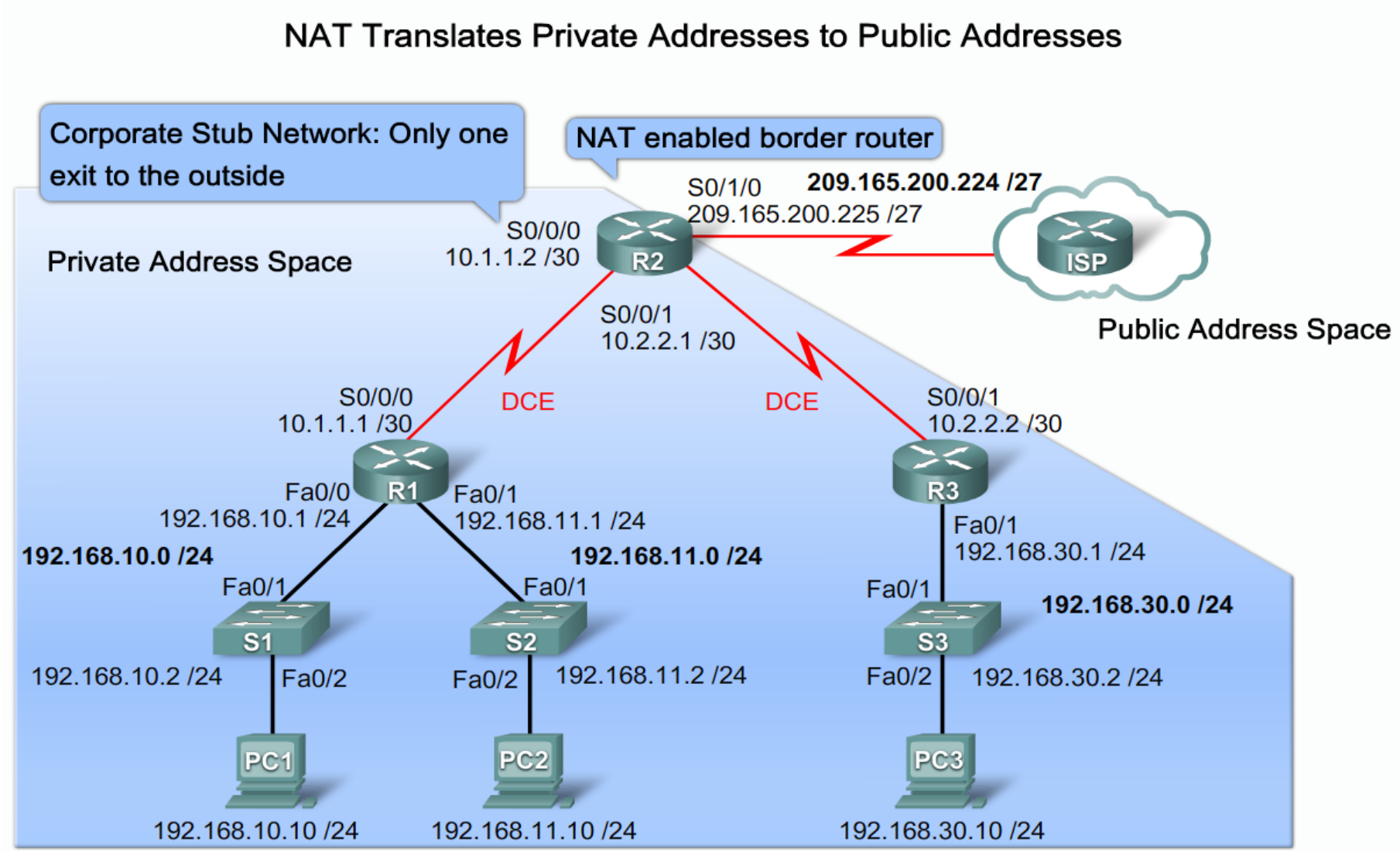
Public Internet addresses are regulated by five Regional Internet Registries (RIRs):

- ARIN
- RIPE
- APNIC
- LACNIC
- AfriNIC

Private Internet addresses are defined in RFC 1918:

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

Network Address Translation



NAT benefits & drawbacks

NAT Benefits and Drawbacks

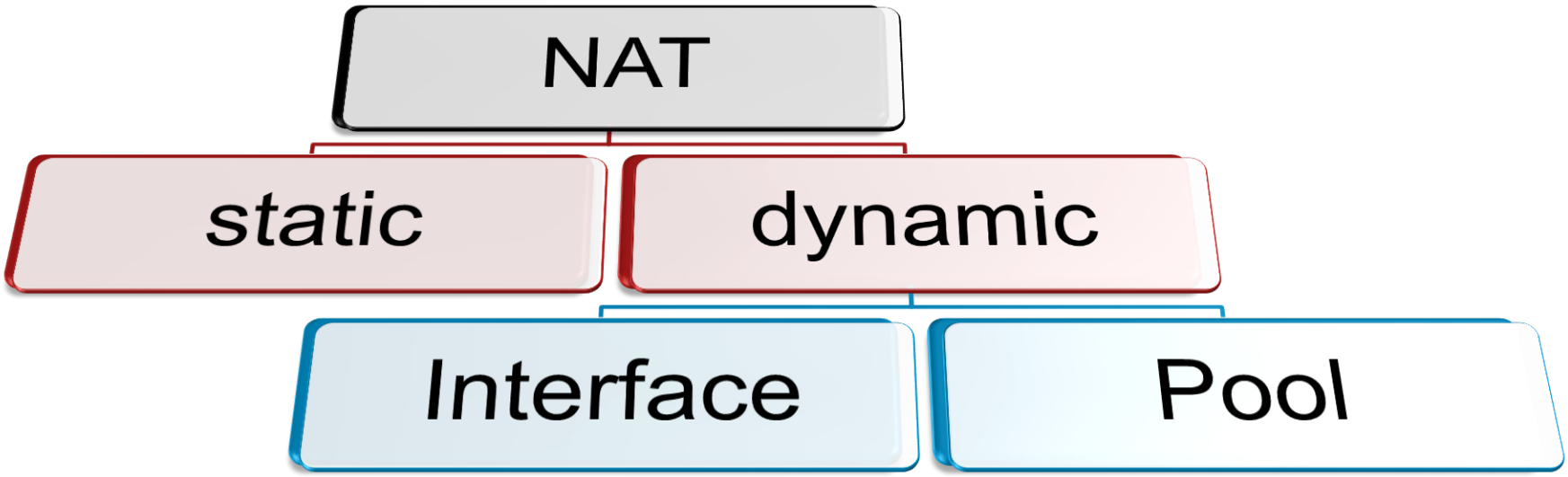
NAT Benefits

- Conserves the legally registered addressing scheme
- Increases the flexibility of connections to the public network
- Provides consistency for internal network addressing schemes.
- Provides network security

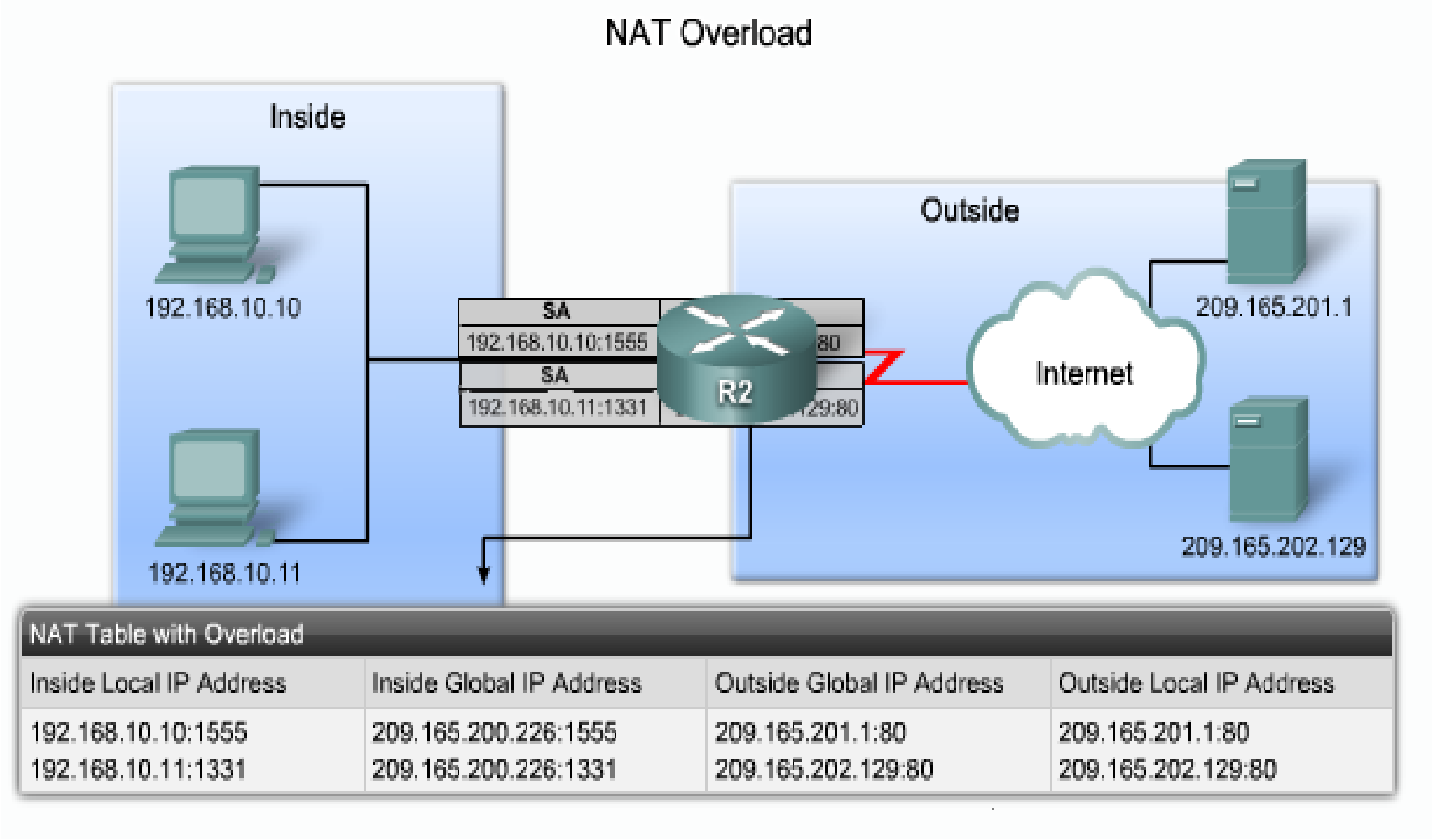
NAT Drawbacks

- Performance is degraded
- End-to-end functionality is degraded
- End-to-end IP traceability is lost
- Tunneling is more complicated
- Initiating TCP connections can be disrupted
- Architectures need to be rebuilt to accommodate changes

NAT configuration

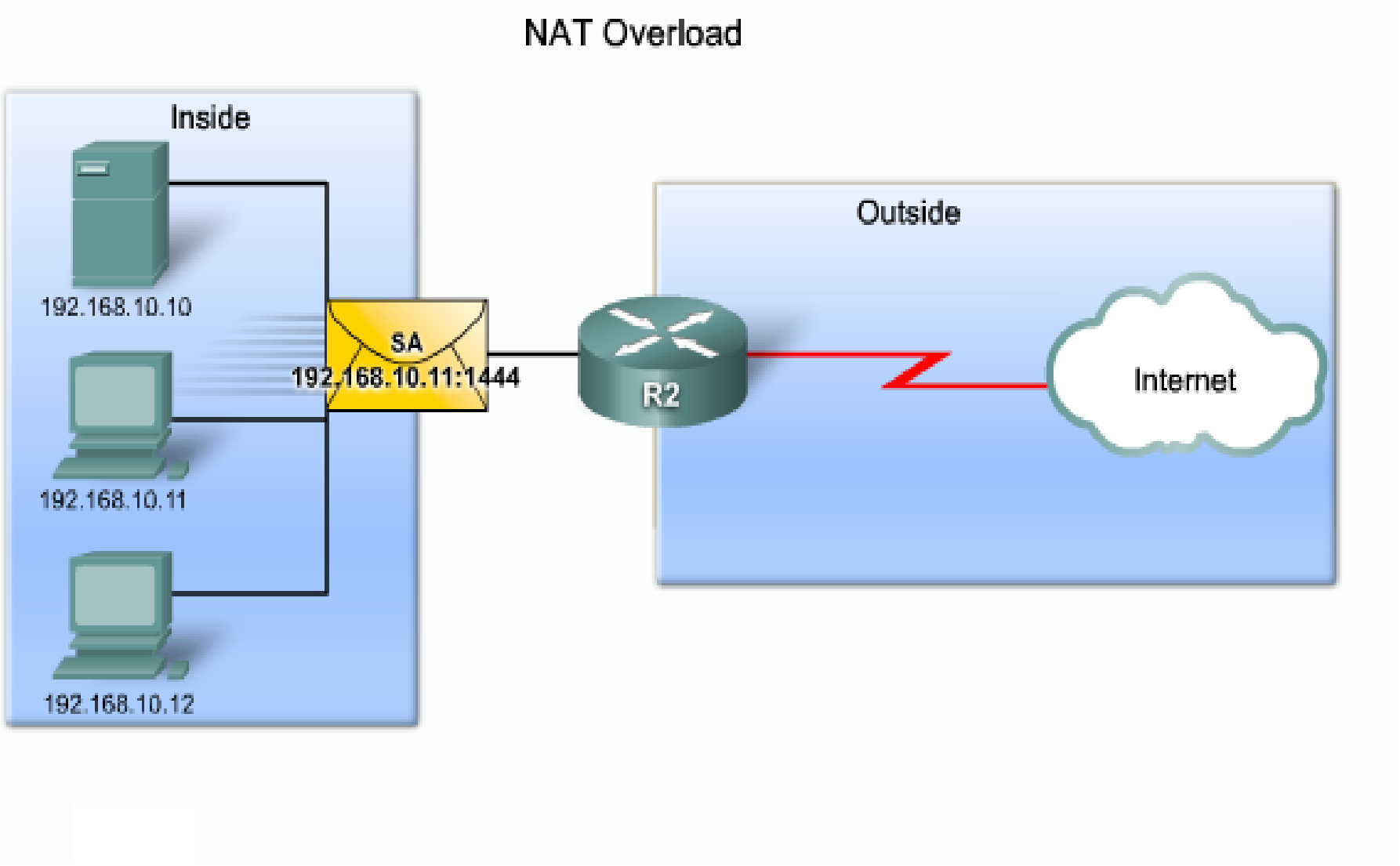


NAT overload

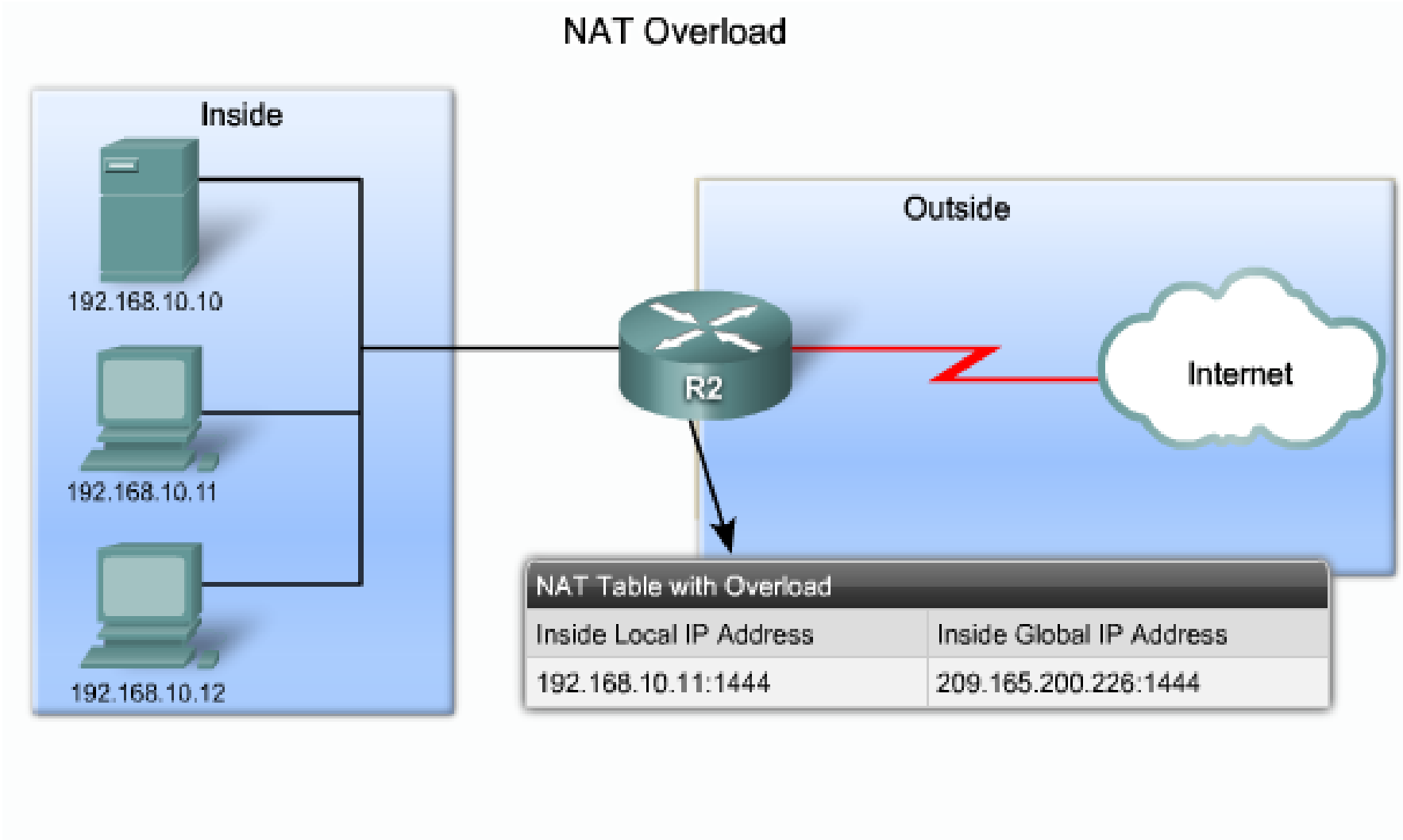


NAT Table with Overload			
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address	Outside Local IP Address
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

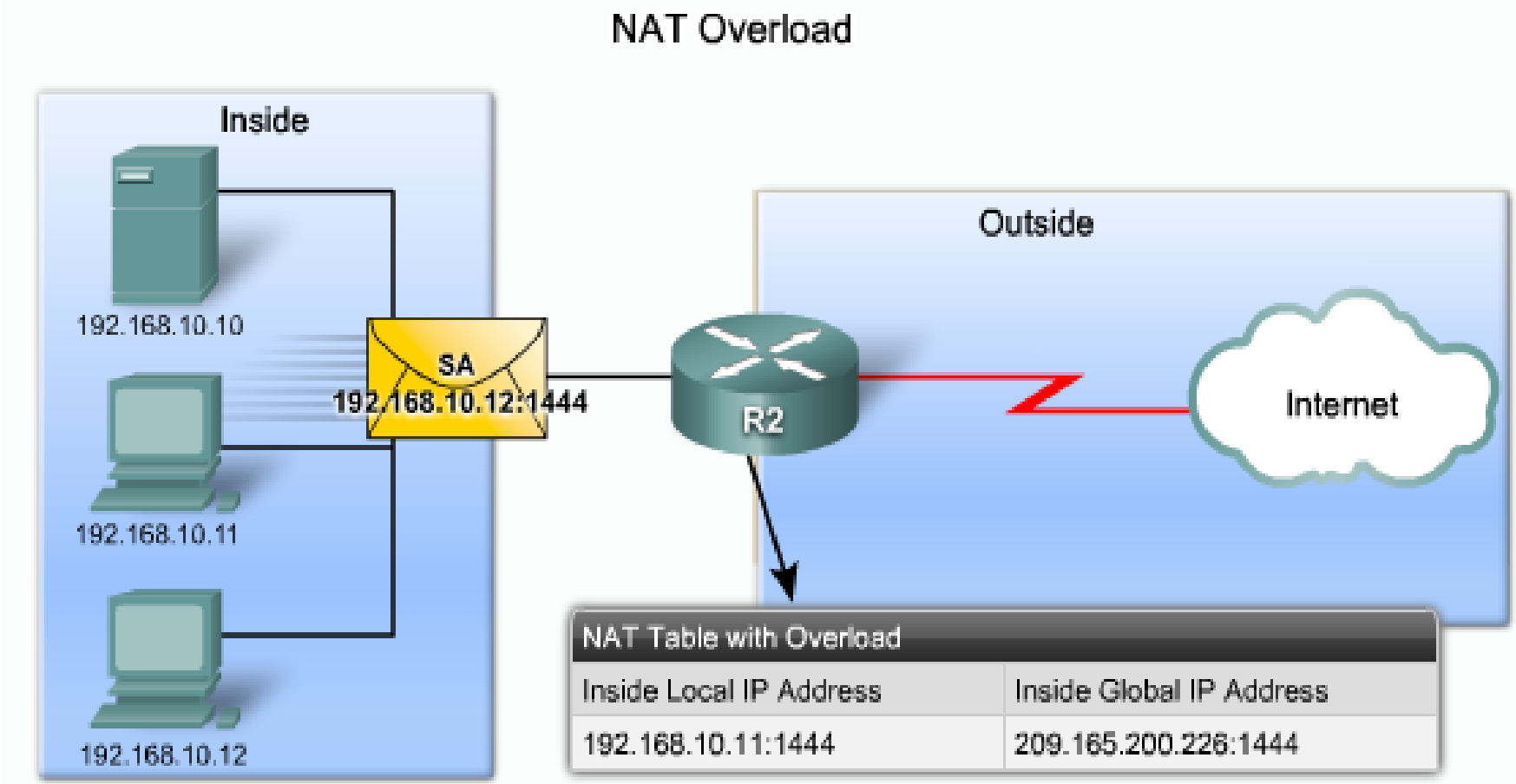
NAT overload



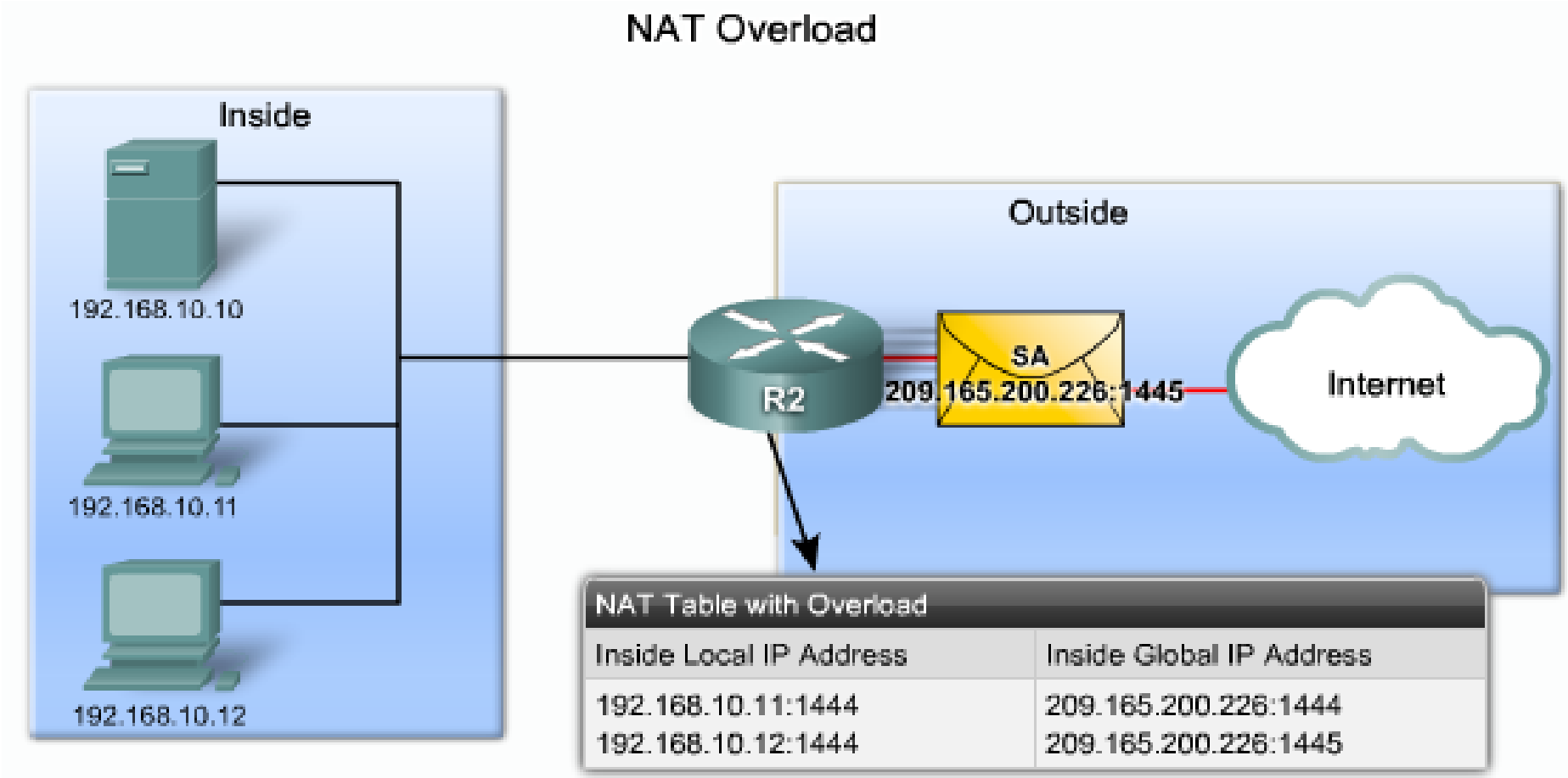
NAT overload



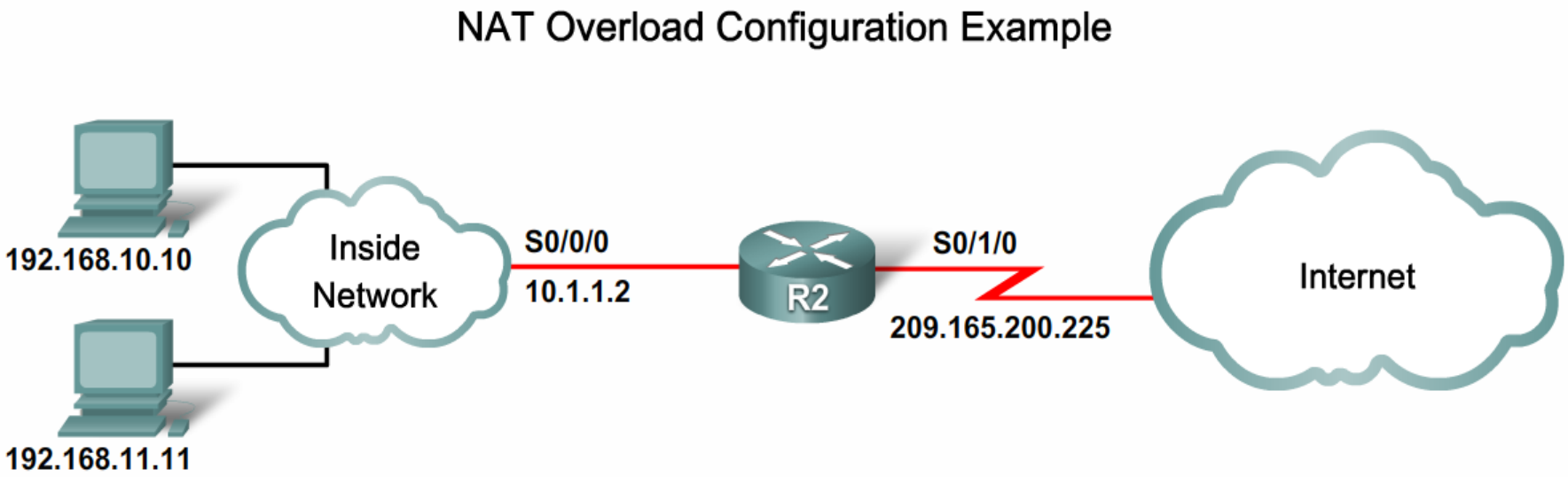
NAT overload



NAT overload



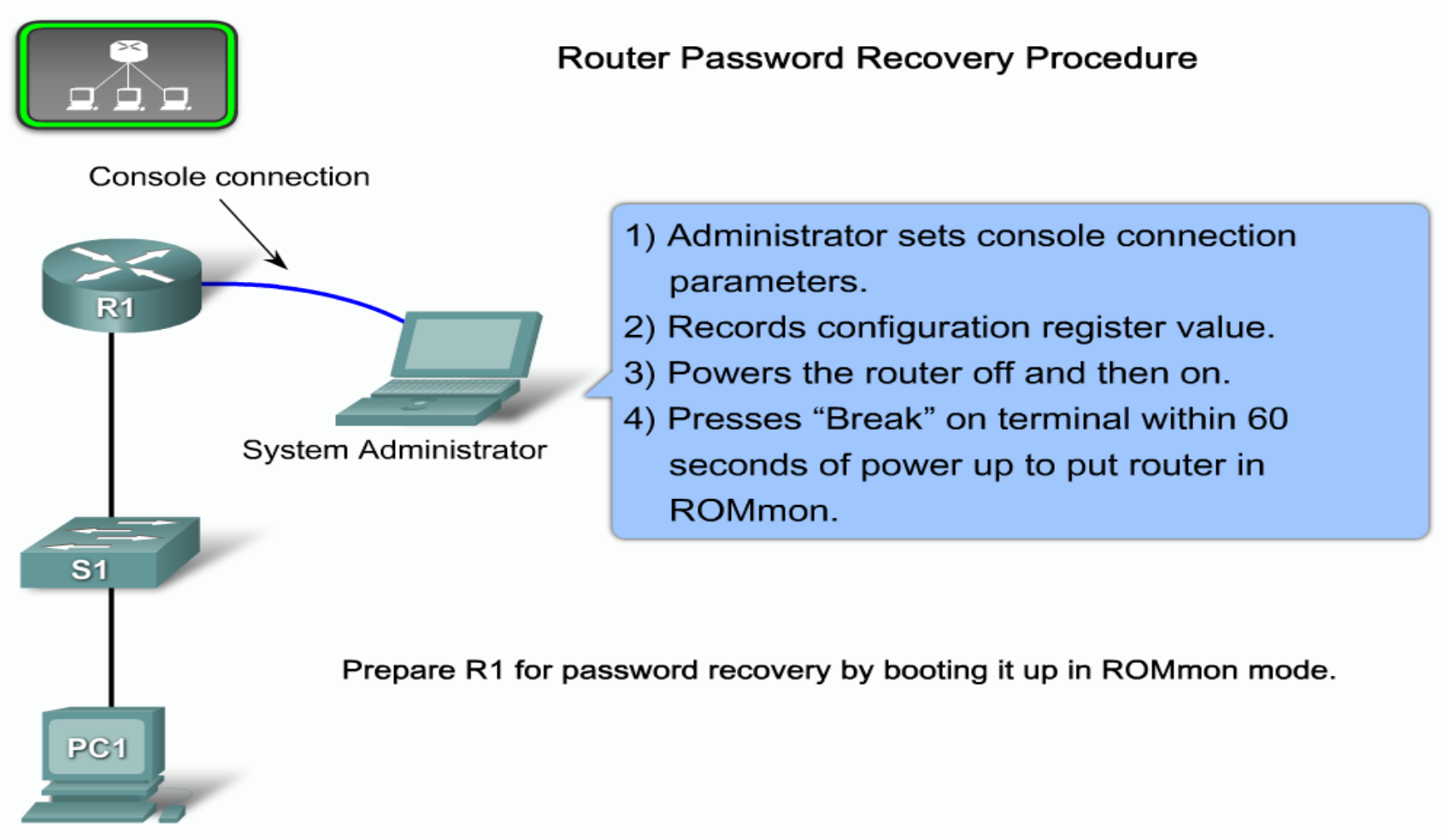
NAT overload




```
access-list 1 permit 192.168.0.0 0.0.255.255
ip nat inside source list 1 interface serial 0/1/0 overload
interface serial 0/0/0
  ip nat inside
interface serial 0/1/0
  ip nat outside
```

Routers Password recovery

Password recovery



Password recovery exact steps for routers

1. Connect your console to the router (password recovery can't be done using telnet, it must be done using console connection)
2. Turnoff the router then turn it on again
3. During 60 seconds of router startup → press "control + break" buttons
4. You will enter the rommon mode
5. Change the configuration register to 0x2142 using this command :
    1. Confreg 0x2142
    2. Reset
6. After the router startup again, you will find that there is no configuration on it and you can access it easily without any passwords.
7. From privilege mode copy the startup config to running config
    1. Router# copy start run
    2. Router# conf t
    3. Router(config)# configuration-register 0x2102
    4. Router(config)# enable secret new_pass
    5. Router(config)# Exit
    6. Router# Copy run start