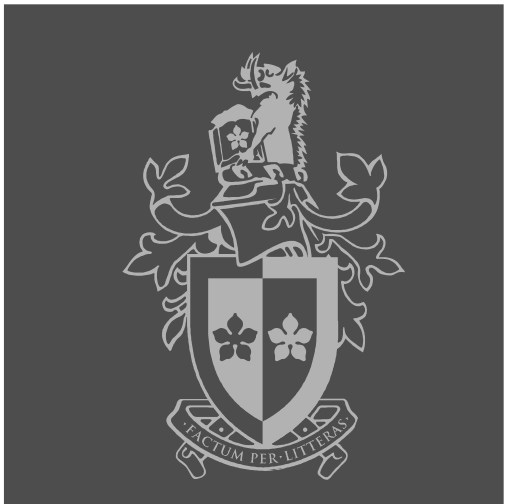
SWINBURNE UNIVERSITY OF TECHNOLOGY

TNE20002 / TNE70003

Topic 8. NAT



Rev. 1.3

Outline

8.1 Introducing NAT

- NAT Characteristics
- NAT Terminology
- NAT Translation

8.2 Types of NAT

- Static NAT
- Dynamic NAT

8.3 NAT Overload

- Port Address Translation PAT
- PAT Example

8.4 Configure PAT

- PAT Overload on Pool
- PAT Overload on Interface
- Verifying NAT

NAT Characteristics

Private IP addresses are not registered & can be used within any internal network.

Routers do not advertise Private IP addresses on the Internet.

Private IP address packets will be dropped before reaching Internet

Private Internet Addresses are Defined in RFC 1918

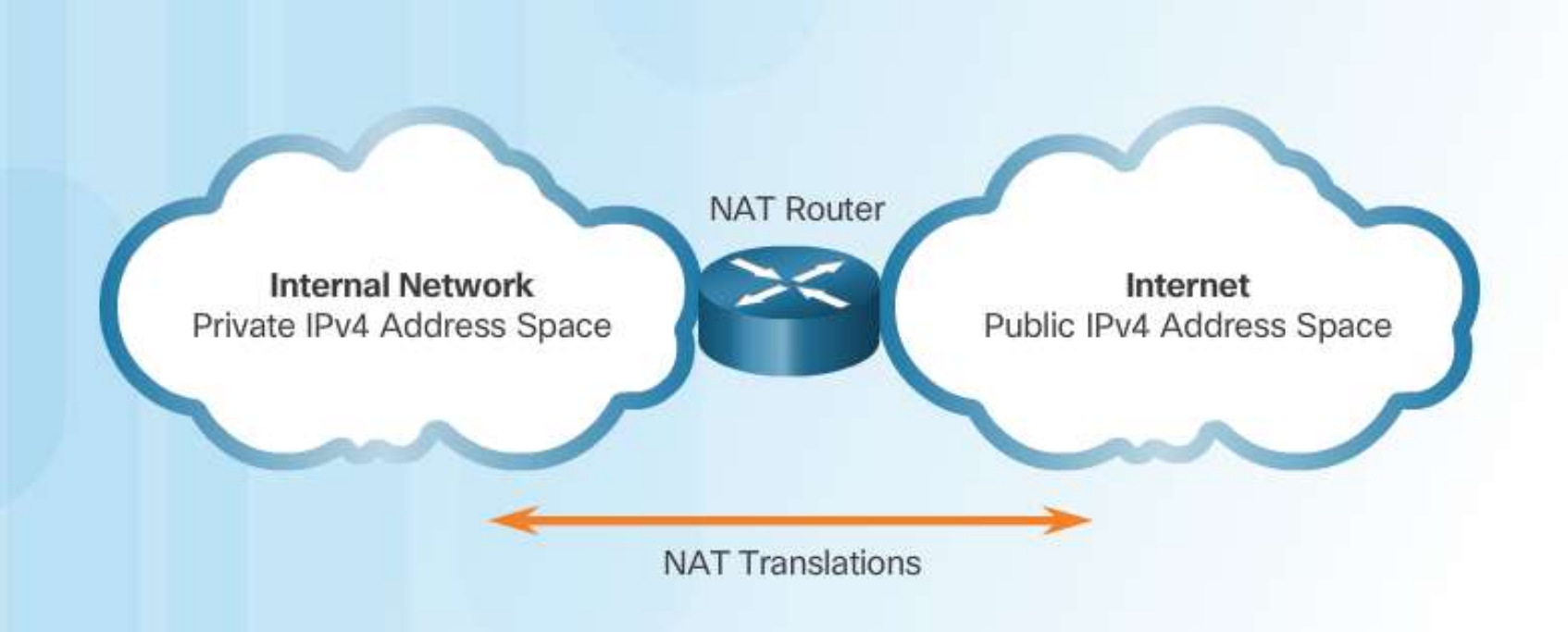
Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

NAT Characteristics

* Private IP addresses cannot be routed over the Internet

* Network Address Translation is used to translate private IP addresses to public addresses that can be routed over the Internet.

* One public IPv4 address can be used for thousands of devices that have private IP addresses



Network Address Translation

NAT Characteristics

* NAT (defined by RFC 1631) is designed to conserve IP addresses and enable networks to use private IP addresses in internal networks.
* NAT hides internal private IPv4 addresses from outside networks
* These private IP addresses are translated to routable public IP addresses for accessing the Internet.

Types of NAT (Static or Dynamic)

Static NAT

assigns one public IP address to one private IP address.

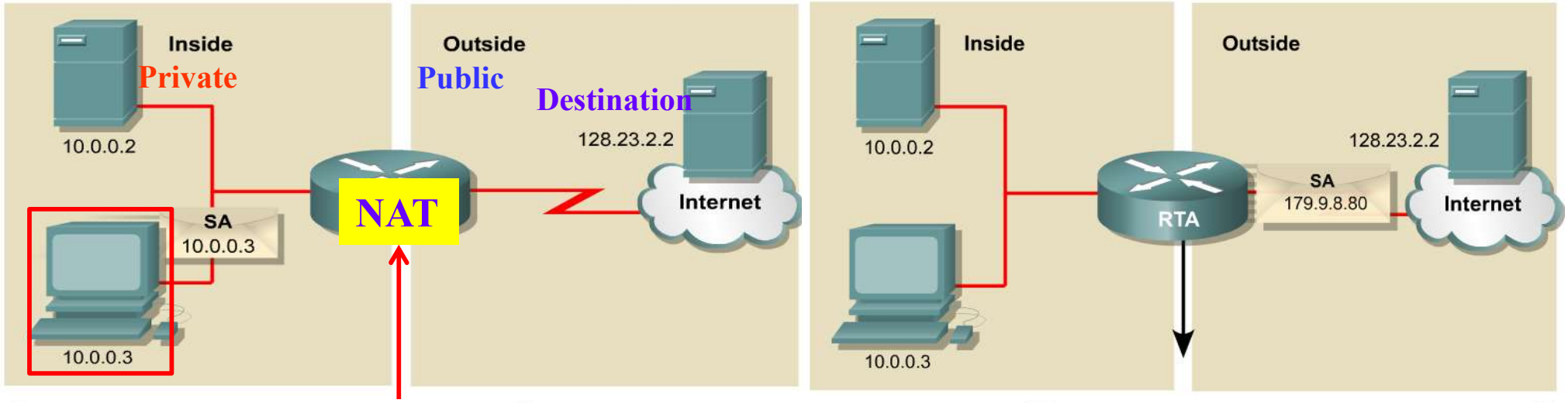
Dynamic NAT

assigns public IP address (from pool of addresses)to each private IP address

Port Address Translation PAT (or NAT Overload)

(PAT) port address translation allows multiple private IP addresses to map to one public ip address.

NAT Characteristics



NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.3	179.9.8.80	128.23.2.2

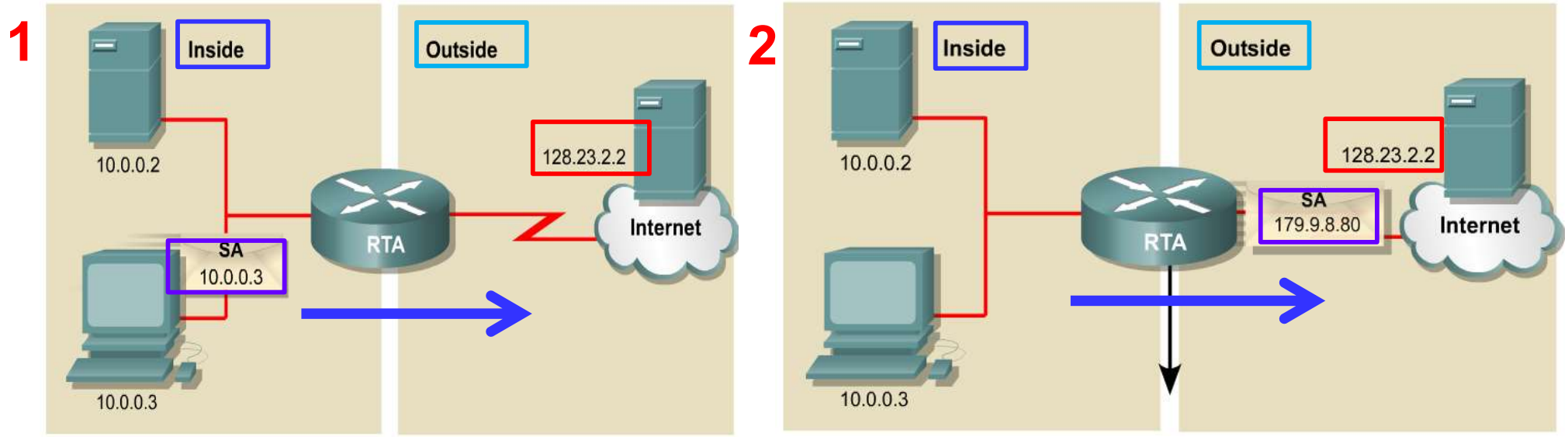
NAT Terminology

Inside Local IP address – A **private IP** address assigned to host on inside network.

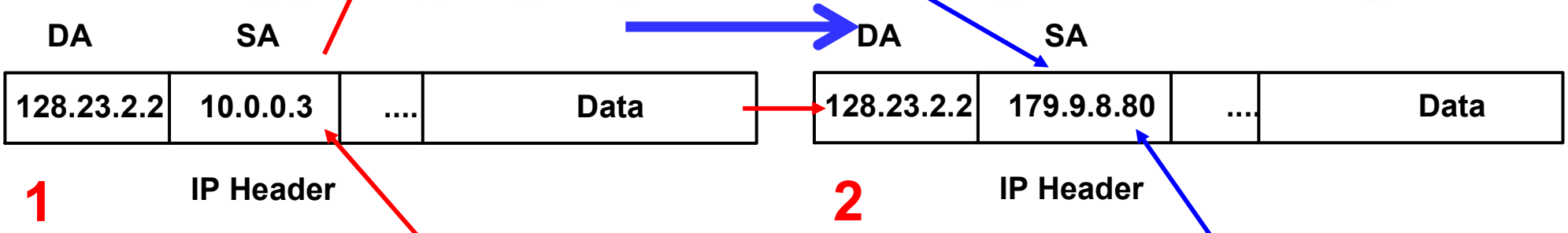
Inside Global IP address - A **public IP** address that represents one or more inside local IP addresses to the outside world.

Outside Global IP address – The **public IP** address assigned to a destination host on the outside network.

NAT Translation – Private source to Public source

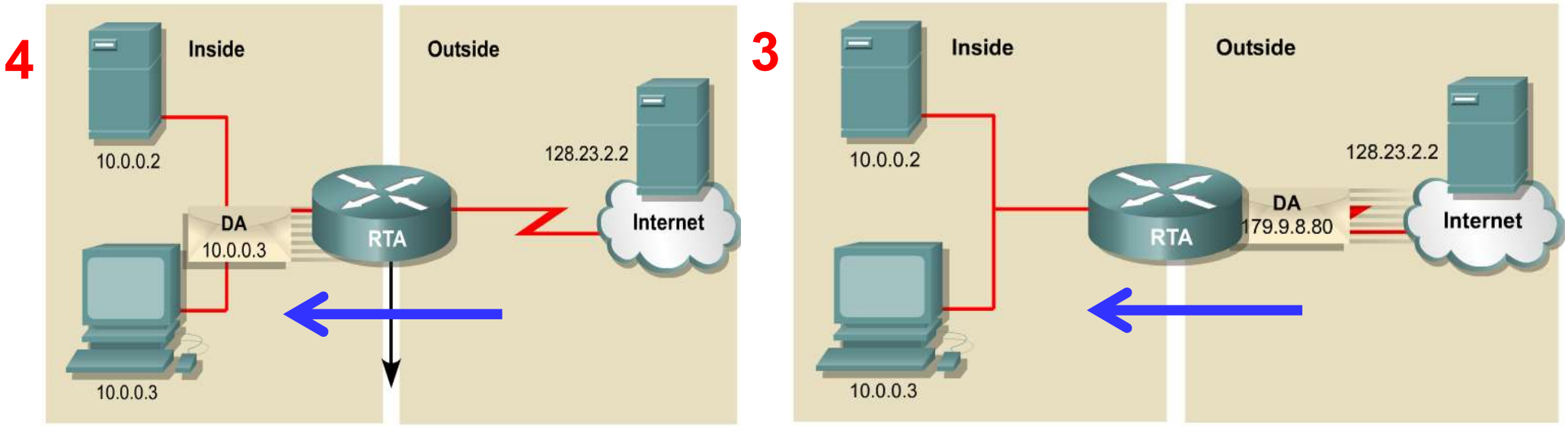


NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.3	179.9.8.80	128.23.2.2

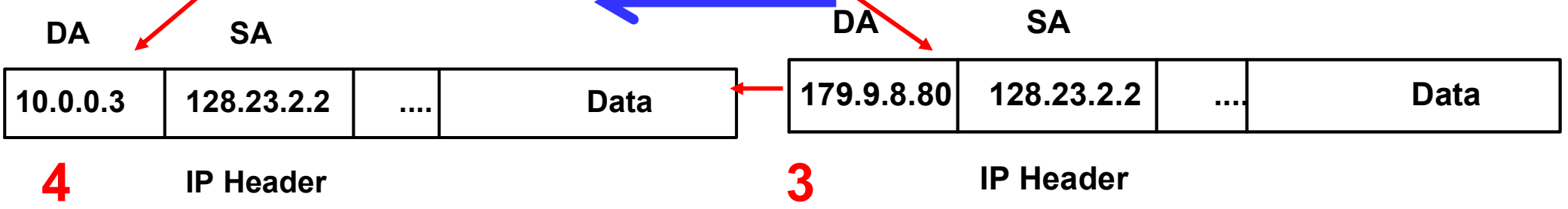


The **translation** from **Private source** IP address to **Public source** IP address.

NAT Translation - Public destination to Private destination



NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.2	179.9.8.79	128.23.2.2
10.0.0.3	179.9.8.80	128.23.2.2



Translation back, from **Public destination** IP address to **Private destination** IP address.

8.2 Types of NAT

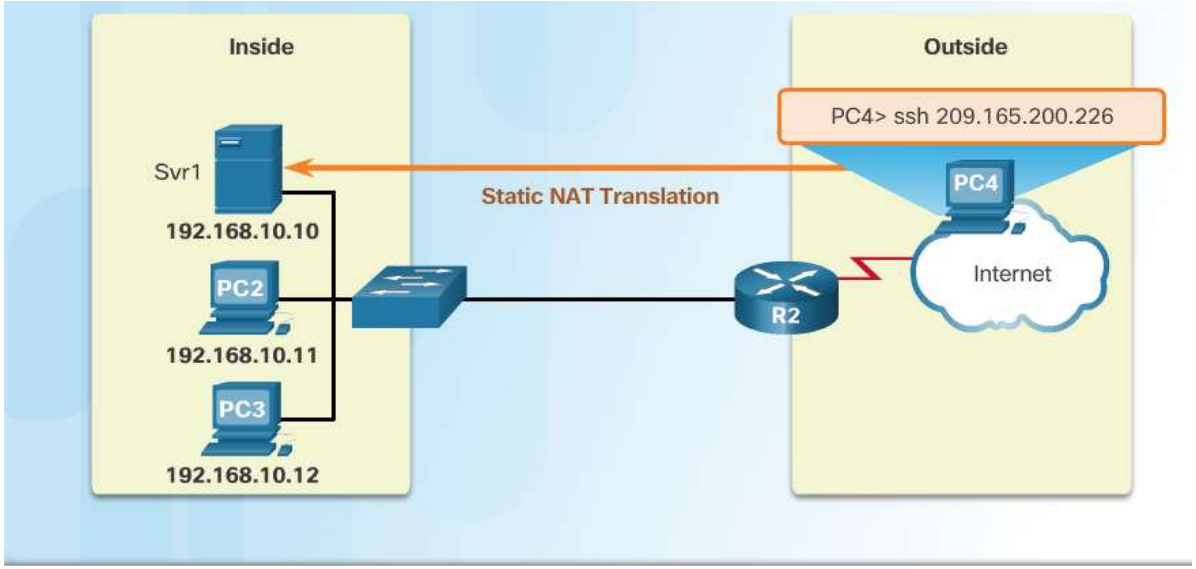
- Static NAT
- Dynamic NAT

Types of NAT - Static NAT

Static NAT

* Static address translation (Static NAT) assigns one public IP address to one private IP address. (Uses a one-to-one mapping of private and public addresses) Mappings remain constant.

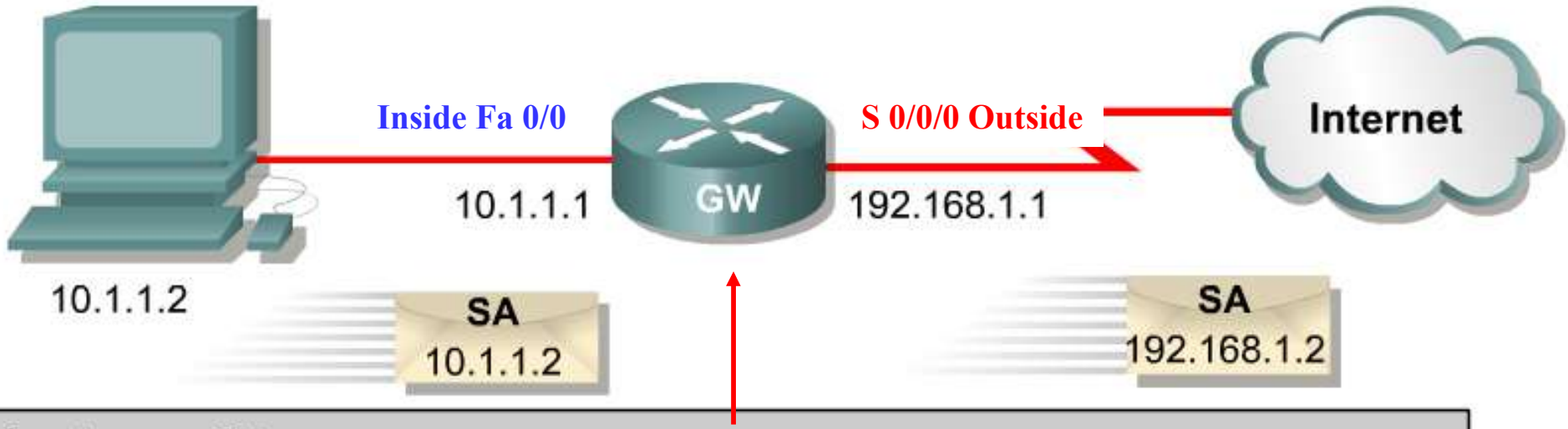
* Commonly used for web servers that need to be accessed by external devices or for devices that must be accessible by authorized personnel when offsite.
* One-to-one address mapping between local and global addresses



Static NAT Table

Inside Local Address	Inside Global Address - Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

Types of NAT - Static NAT




```
hostname GW
!
ip nat inside source static 10.1.1.2 192.168.1.2
!
interface Fa 0/0
  ip address 10.1.1.1 255.255.255.0
  ip nat inside
!
interface S 0/0/0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
```

Types of NAT - Dynamic NAT

Dynamic NAT

Dynamic address translation (Dynamic NAT) assigns a public IP address from a pool of addresses to each packet from a device that has a private IP address when that packet is destined to a network outside the company.

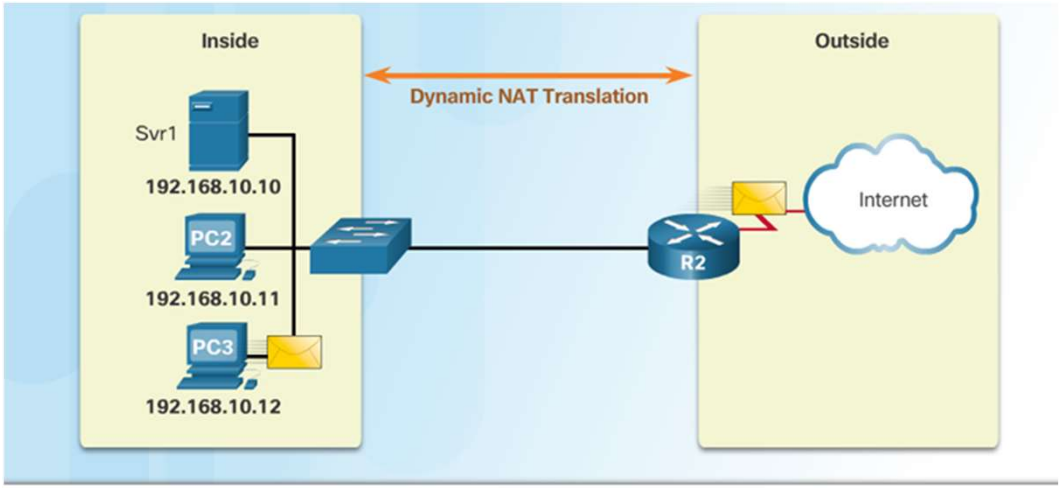
* The number of internal devices that can transmit outside the company is limited to the number of public IP addresses in the pool.
* Addresses are assigned on a first-come, first serve basis

Dynamic NAT parameters

NAT Pool,
range of ip addresses available

ACL,
that permits access to NAT Pool

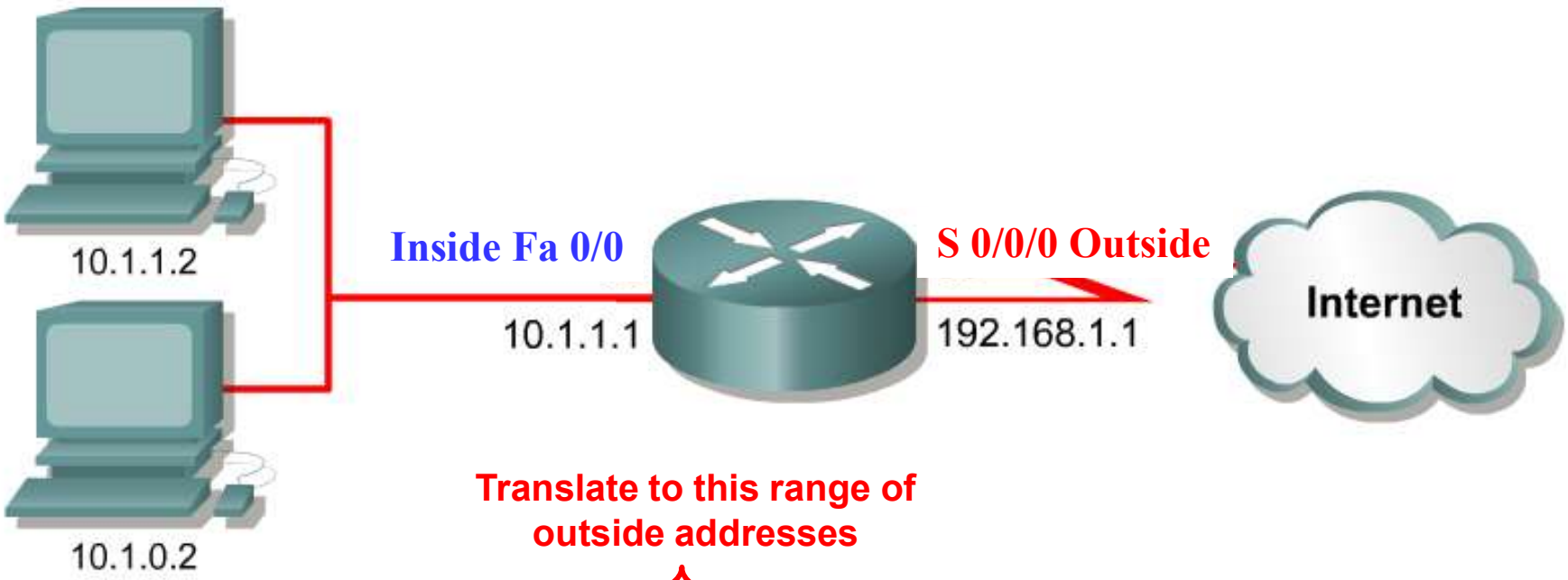
Binding Statement
binding ACL to the NAT Pool



IPv4 NAT Pool

Inside Local Address	Inside Global Address Pool - Addresses reachable via R2
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230

Types of NAT - Dynamic NAT




```
ip nat pool nat-pool1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool1
!
interface ethernet
  ip address 10.1.1.1 255.255.0.0
  ip nat inside
!
interface serial
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
access-list 1 permit
```

Fa 0/0

Binding NAT pool to ACL

S 0/0/0

10.1.0.0 0.0.255.255

8.3 NAT Overload

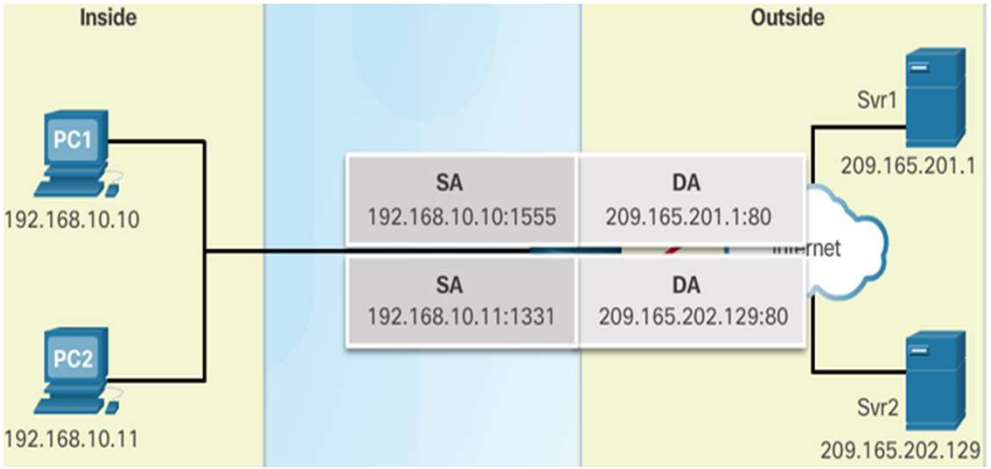
- Port Address Translation PAT
- PAT Example

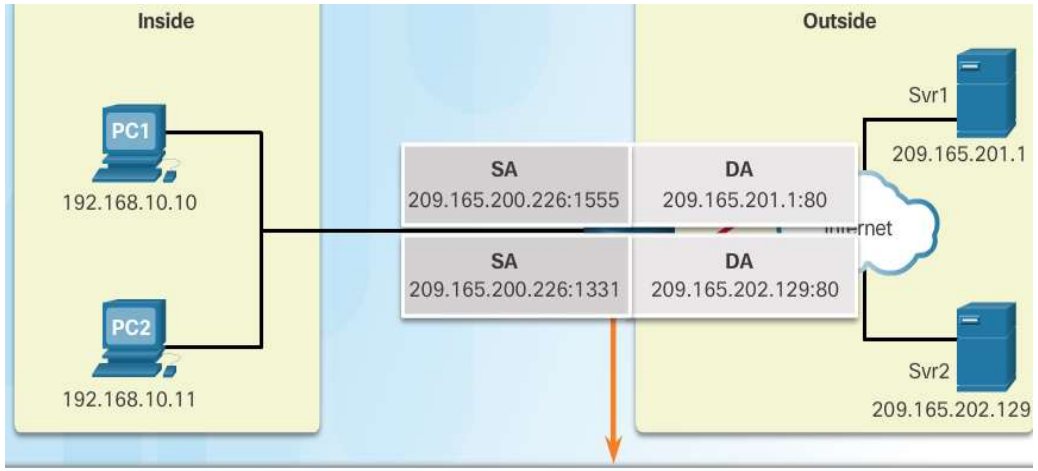
Port Address Translation PAT

Port Address Translation PAT

* PAT (otherwise known as NAT overload) can use one public IPv4 address to allow many private IPv4 addresses to communicate with outside network devices.
* Uses port numbers to track the session

* Maps multiple private IP address to a single public IP address or
* Many-to-One address mapping between local and global addresses





NAT Table with Overload

Inside Global IP Address	Inside Local IP Address	Outside Local IP Address	Outside Global IP Address
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.11:1331	209.165.202.129:80	209.165.202.129:80

Port Address Translation PAT

When a client opens a TCP/IP session, NAT maps a PORT number to client's source IP address.

When a response comes back from an external server, the source port number becomes the destination port number on the return trip.

This port number determines to which client application, the packet is forwarded.

Preserving Port Numbers

PAT tries to preserve the original source port number.

If that port number is already used,

PAT will assign the first available port number for the appropriate port group

0 - 511

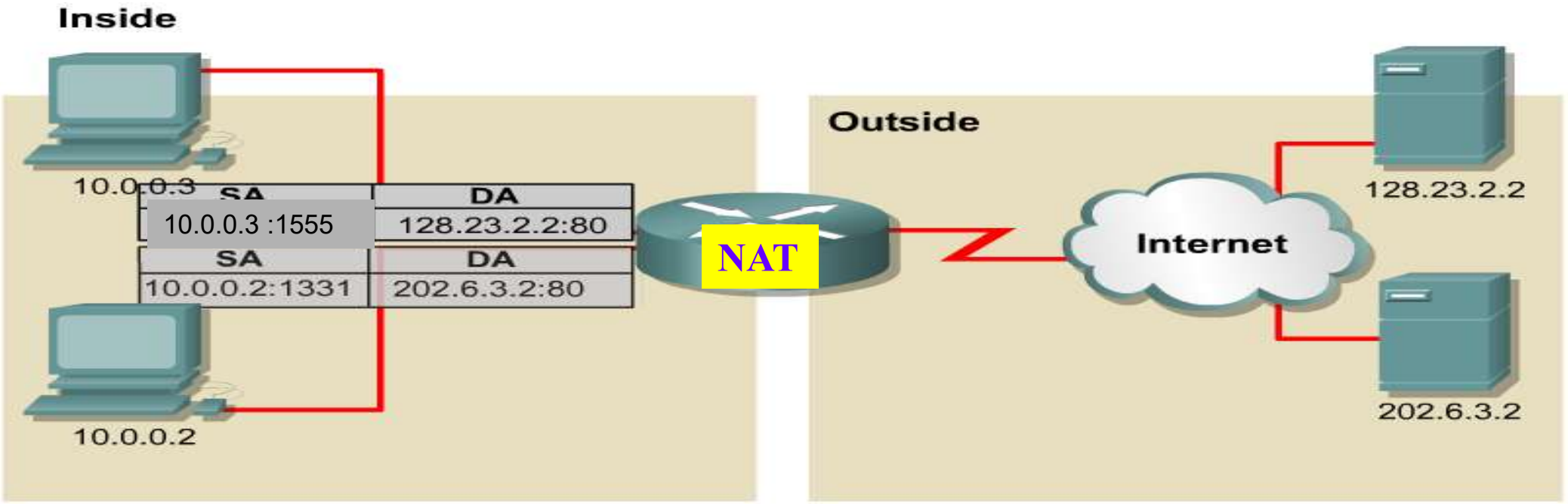
512 - 1023

1024 - 65,535

When there are no more port numbers available,

PAT moves to the next public IP address in the pool if there is one

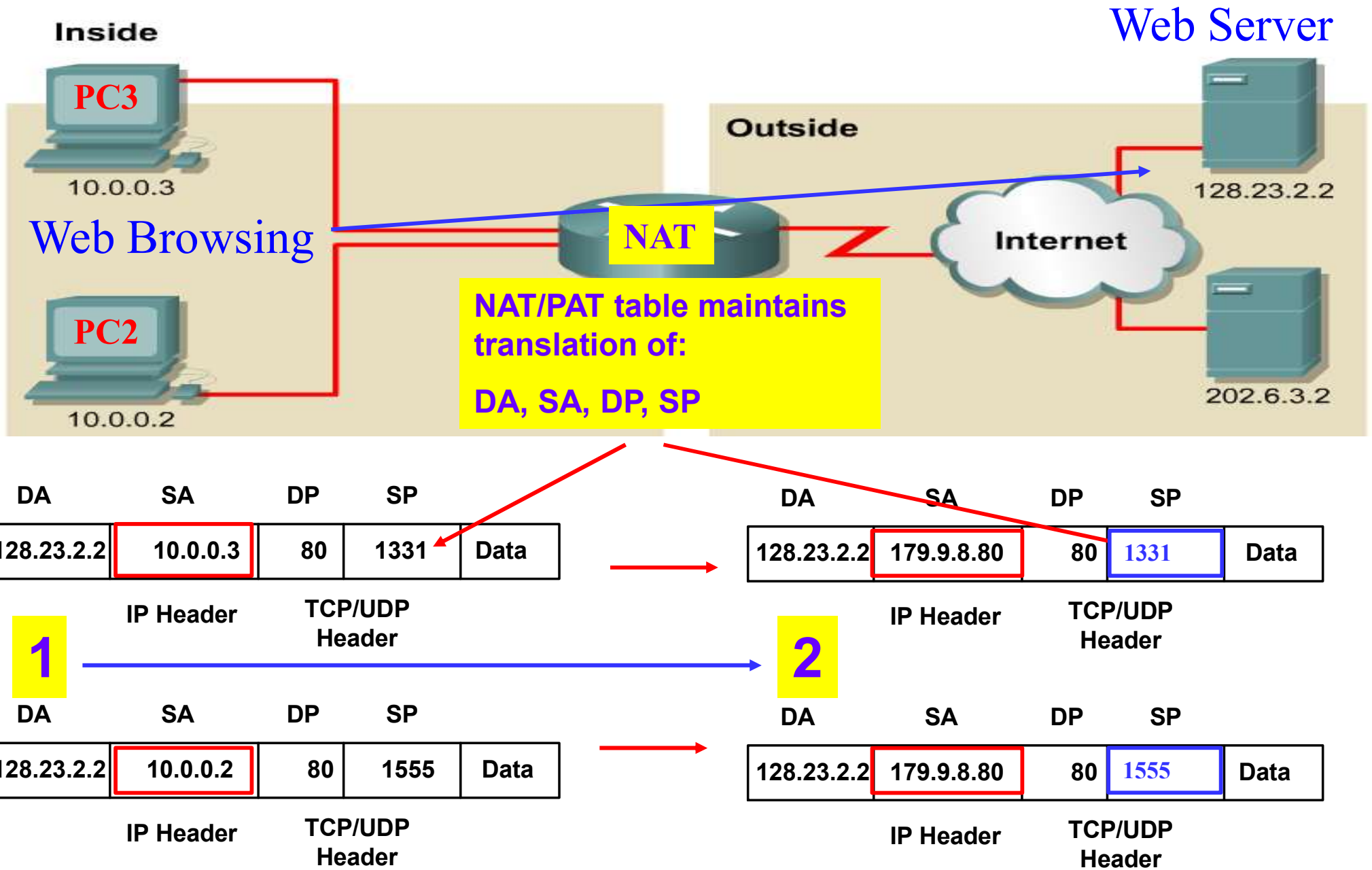
Port Address Translation PAT



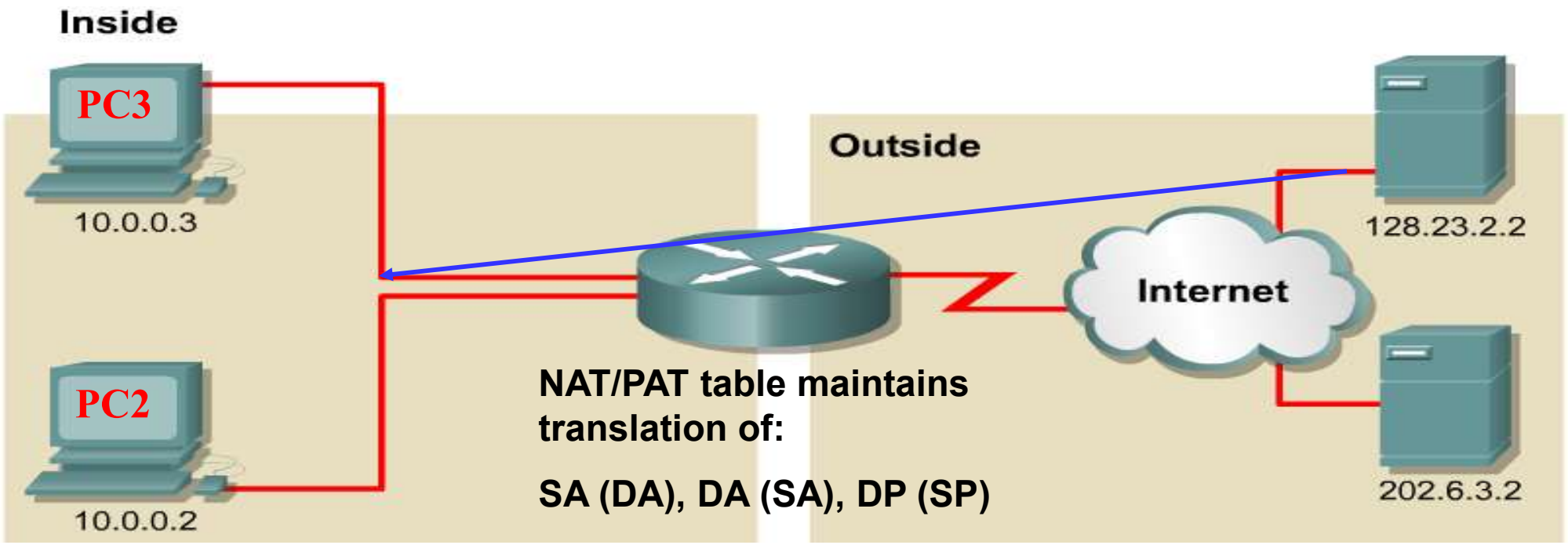
NAT Table			
Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global Address
10.0.0.2:1331 10.0.0.3:1555	179.9.8.20:1331 179.9.8.20:1555	202.6.3.2:80 128.23.2.2:80	202.6.3.2:80 128.23.2.2:80

- Allows you to use a **single Public IP address** and assign it to many inside hosts
- Multiple private IP addresses can be translated by a single public address (**many-to-one translation**).
- Tracks and translates SA, DA, **SP** and **DP** (which uniquely identifies each connection) for each stream of traffic.

PAT Example two PCs using 179.9.8.80



PAT Example two PCs using 179.9.8.80



	DA	SA	DP	SP	
PC3	10.0.0.3	128.23.2.2	1331	80	Data

IP Header | TCP/UDP Header

	DA	SA	DP	SP	
	179.9.8.80	128.23.2.2	1331	80	Data

IP Header | TCP/UDP Header

4 **3**

	DA	SA	DP	SP	
PC2	10.0.0.2	128.23.2.2	1555	80	Data

IP Header | TCP/UDP Header

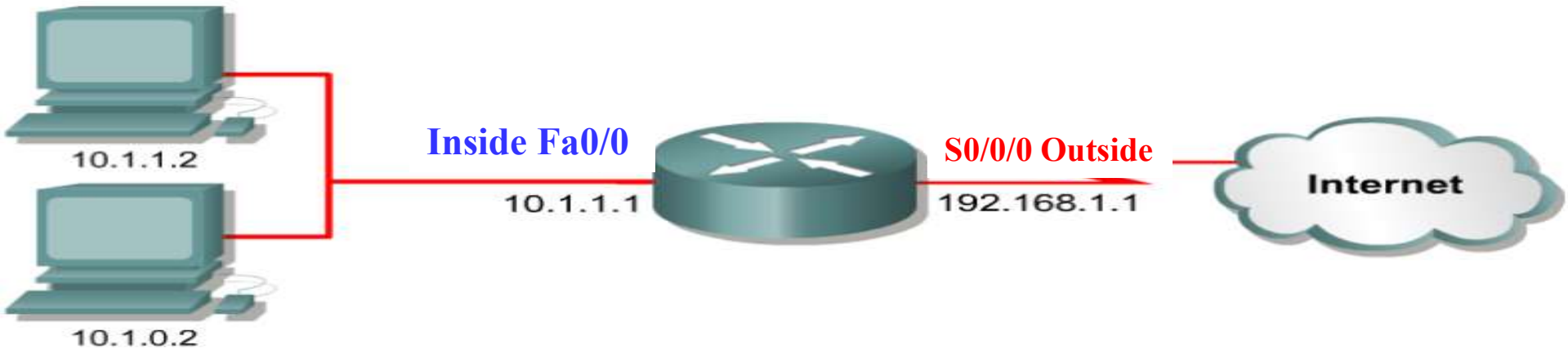
	DA	SA	DP	SP	
	179.9.8.80	128.23.2.2	1555	80	Data

IP Header | TCP/UDP Header

8.4 Configure PAT

- PAT Overload on Pool
- PAT Overload on Interface
- Verifying NAT

Configuring PAT – Overload on Pool

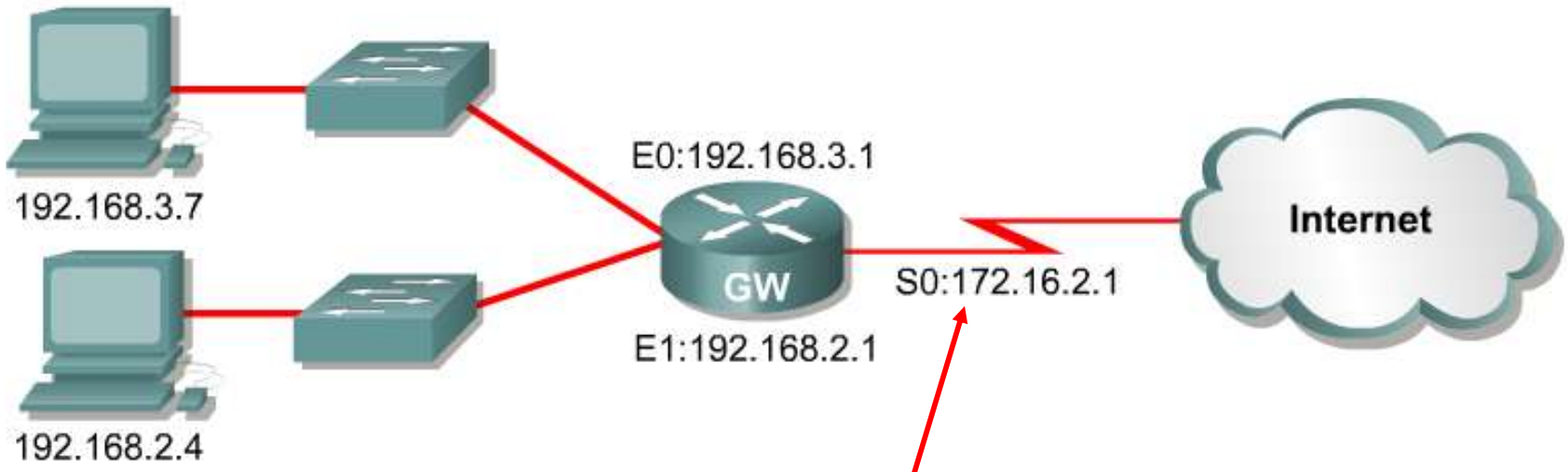



```
Router(config)#access-list 1 permit 10.1.0.0 0.0.255.255

Router(config)# ip nat pool nat-pool1 170.9.8.80 179.9.8.95
 netmask 255.255.255.0

Router(config) ip nat inside source list 1 pool nat-pool1 overload
```

- Establishes overload translation and specifies the IP address to be overloaded as that designated in the pool.

In this example a pool of Public IP addresses is used, using PAT, source ports, to differentiate between connection streams.

Configuring PAT – Overload on Interface




```
interface ethernet 0
  ip address 192.168.3.1 255.255.255.0
  ip nat inside
!
interface ethernet 1
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside
!
ip nat inside source list 1 interface serial 0 overload
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
```

This is a different example, using the the outside interface S0 instead of specifying a pool of IP addresses

NAT Clear Commands

```
Router#clear ip nat translation
```

- Clears all dynamic address translation entries

```
Router#clear ip nat translation inside global-ip local-ip [outside
local-ip global-ip]
```

- Clears a simple dynamic translation entry

```
Router#clear ip nat translation protocol inside global-ip global-port
local-ip local-port [outside local-ip local-port global-ip
global-port]
```

- Clears an extended dynamic translation entry

Command	Description
clear ip nat translation *	Clears all dynamic address translation entries from the NAT translation table
clear ip nat translation inside *global-ip local-ip* **[outside** *local-ip global-ip*]	Clears a simple dynamic translation entry containing an inside translation or both inside and outside translation
clear ip nat translation protocol inside *global-ip global-port local-ip local-port* **[outside** *local-ip local-port global-ip global-port*]	Clears a simple dynamic translation entry

Verifying NAT

```
Router#show ip nat translations [verbose]
```

- Displays active translation

```
Router#show ip nat translation
Pro Inside global     Inside local       Outside local      Outside global
172.16.131.1          10.10.10.1               ---                ---
```

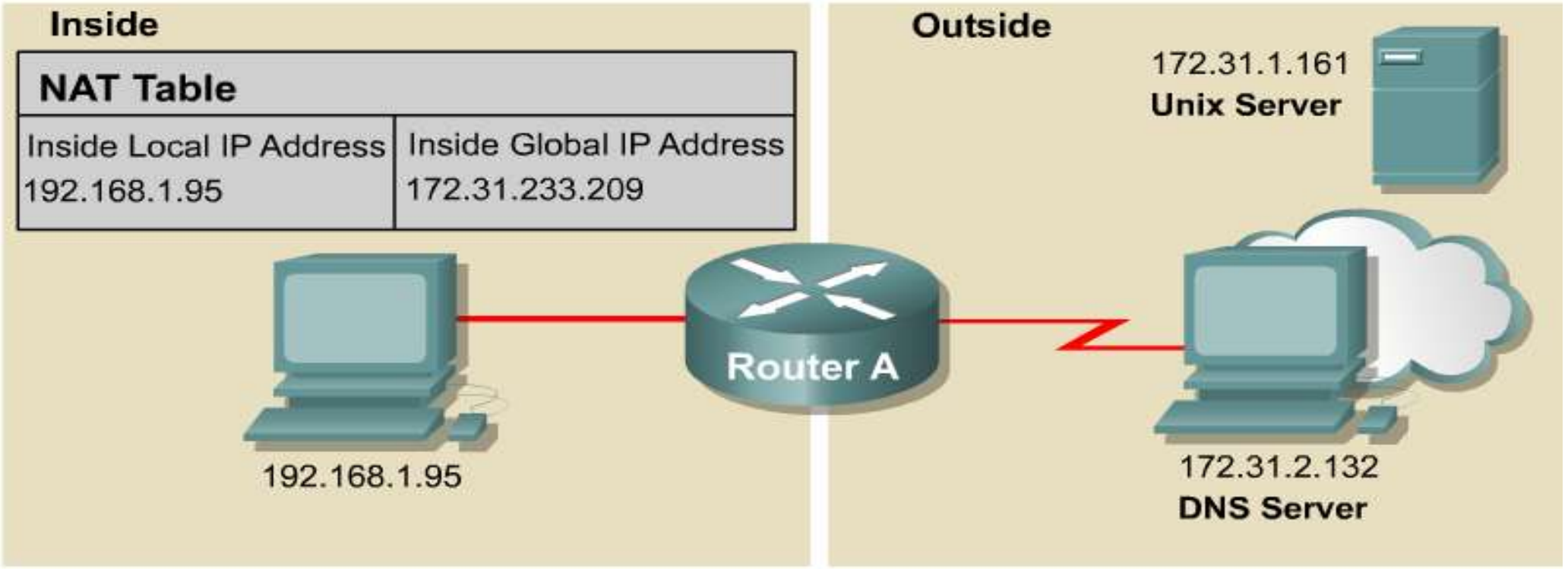
```
Router#show ip nat statistics
```

- Displays translation statistics

```
Router#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Serial0
Inside interfaces:
Ethernet0, Ethernet1
Hits: 5 Misses:0
```

Command	Description
`show ip nat translations`	Displays active translations
`show ip nat statistics`	Displays translation statistics

Troubleshooting NAT/PAT




```
RouterA#debug ip nat
NAT:   s= 192.168.1.95    → 172.31.233.209,      d=172.31.2.132 [6825]
NAT:   s= 172.31.2.132,     d=172.31.233.209,  → 192.168.1.95 [21852]
NAT:   s= 192.168.1.95    → 172.31.233.209,      d=172.31.1.161 [6826]
NAT*:  s= 172.31.1.161,     d=172.31.233.209,  → 192.168.1.95 [23311]
NAT*:  s= 192.168.1.95    → 172.31.233.209,      d=172.31.1.161 [6827]
NAT*:  s= 192.168.1.95    → 172.31.233.209,      d=172.31.1.161 [6828]
NAT*:  s= 172.31.1.161      d=172.31.233.209,  → 192.168.1.95 [23313]
NAT*:  s= 172.31.1.161,     d=172.31.233.209,  → 192.168.1.95 [23313]
```

Verify the NAT translations