SWINBURNE
UNIVERSITY OF
TECHNOLOGY

TNE20002 / TNE70003

Topic 7 NAT V1.1

NAT

Network

Address

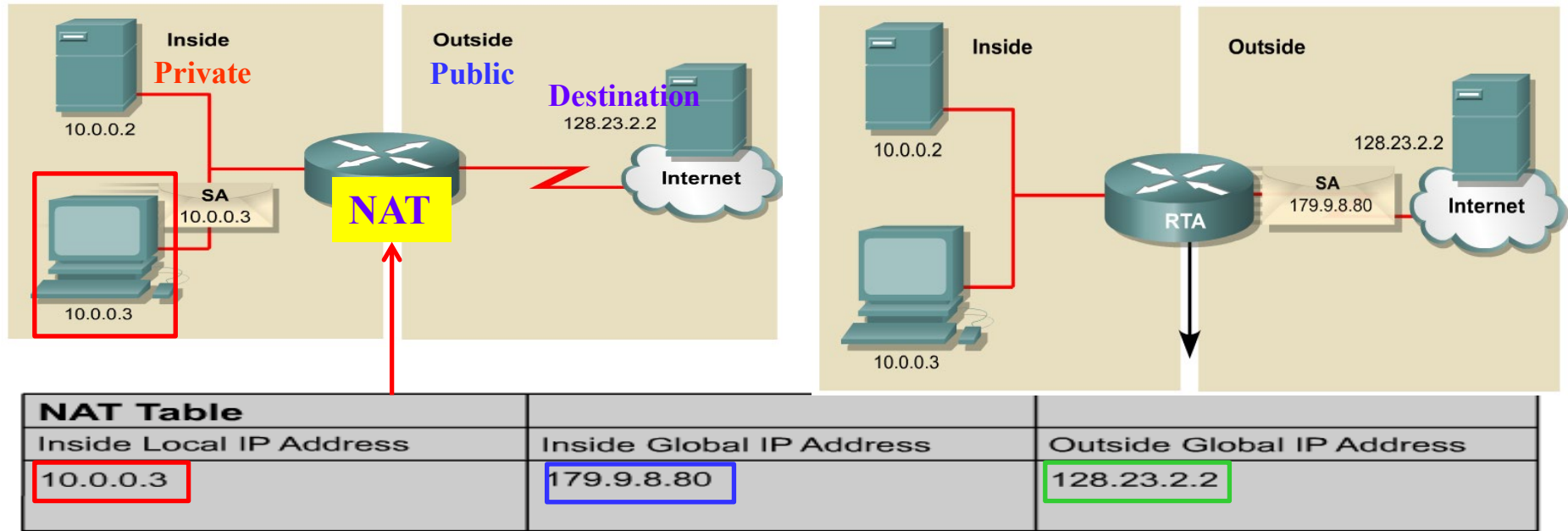Translation

Network Address Translation

- NAT (defined by RFC 1631) is designed to **conserve** IP addresses and enable networks to use **private** IP addresses in **internal** networks.

- These private IP addresses are **translated** to routable public IP addresses for accessing the Internet.

- NAT translations can occur dynamically or statically.

- **NAT (PAT)** **port address translation** allows multiple private ip addresses to map to the same public ip address.

Private addressing – Internal Networks

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 Example

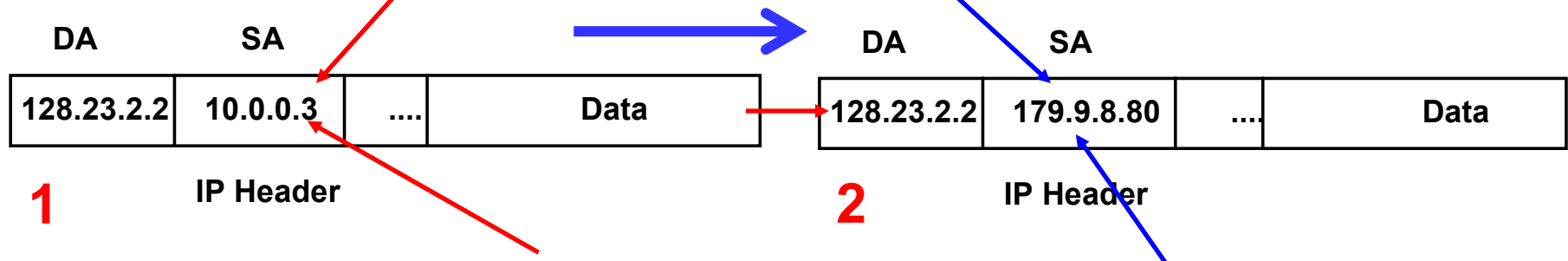| NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.3	179.9.8.80	128.23.2.2

- **Inside Local IP address** – The **IP private** address assigned to a host on the 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 Example – Private source to Public source
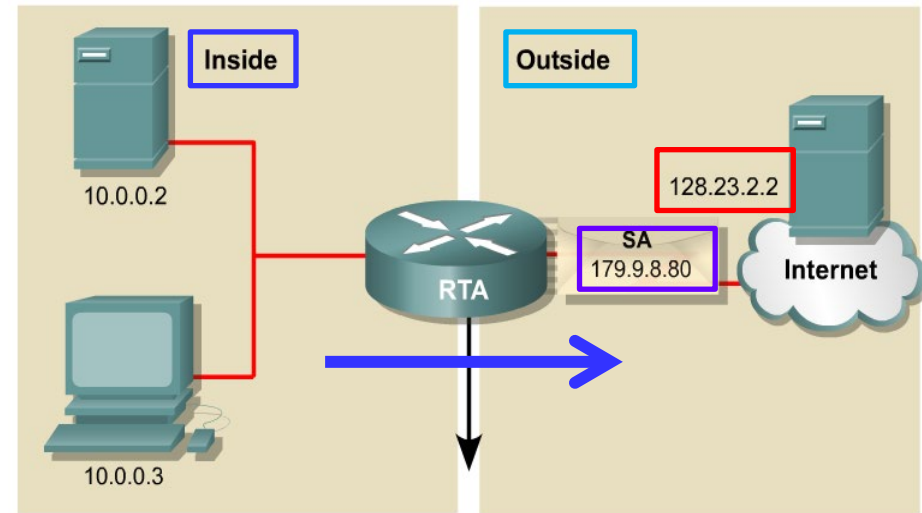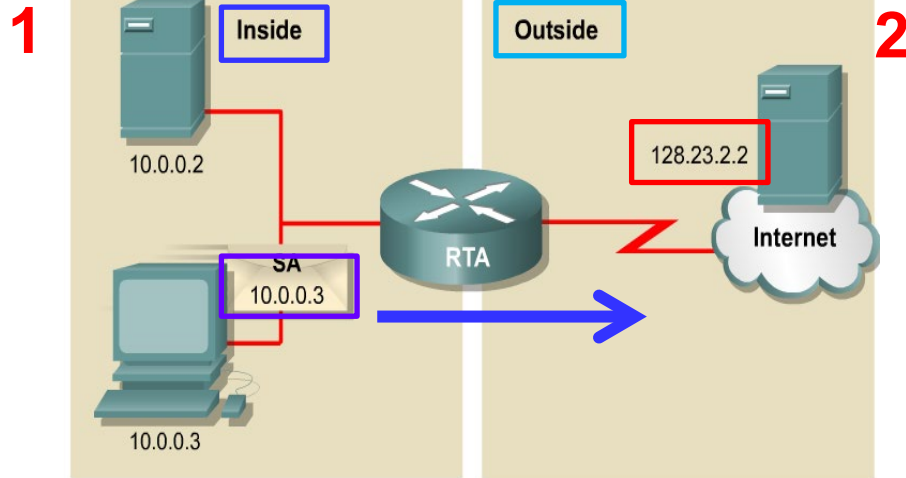
NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.3	179.9.8.80	128.23.2.2

1

DA	SA		
128.23.2.2	10.0.0.3	....	Data

IP Header

2

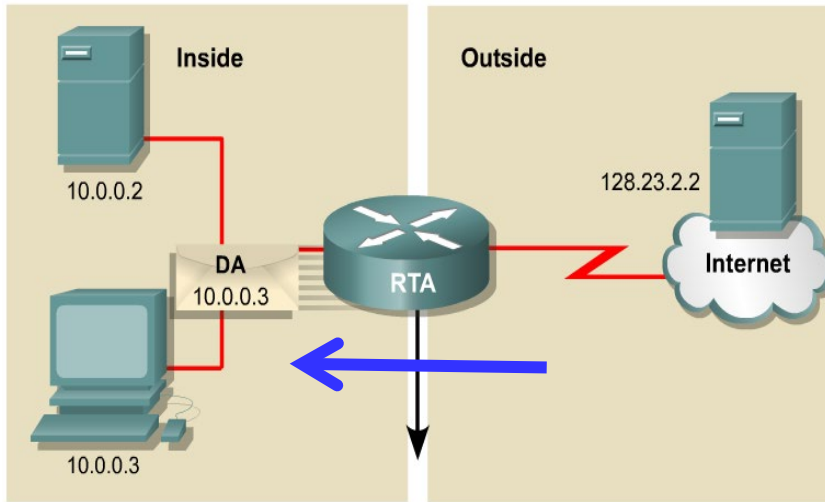| DA	SA		
128.23.2.2	179.9.8.80	....	Data

IP Header

The **translation** from **Private source** IP address to **Public source** IP address.
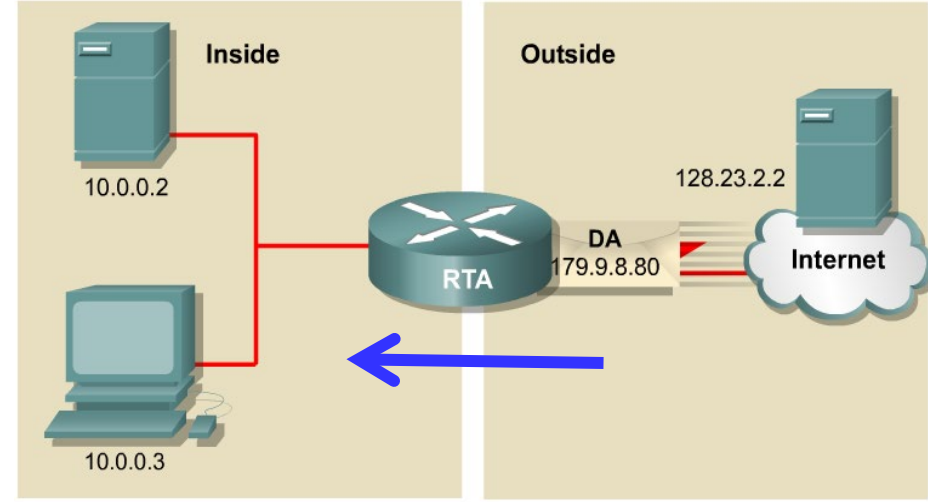
NAT Example - Public destination to Private destination

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

DA   **SA**

10.0.0.3	128.23.2.2	....	Data

4   **IP Header**

DA   **SA**

179.9.8.80	128.23.2.2	....	Data

3   **IP Header**

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

Port

Address

Translation

NAT - PAT

- Maps multiple private IP addresses to a single public IP address

- Your ISP assigns one public IP address to your home router

- Via PAT several of your friends can simultaneously share the this one public IP address, to surf the internet
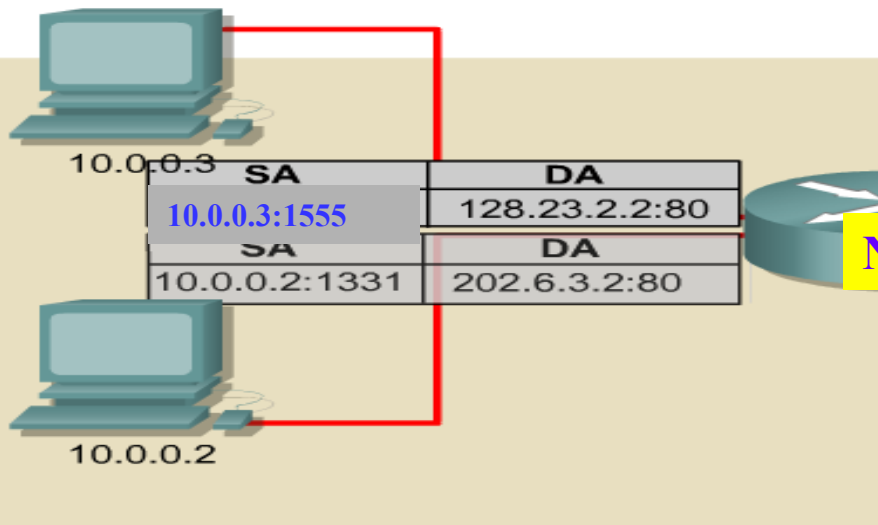
NAT - PAT

- 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 a 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.
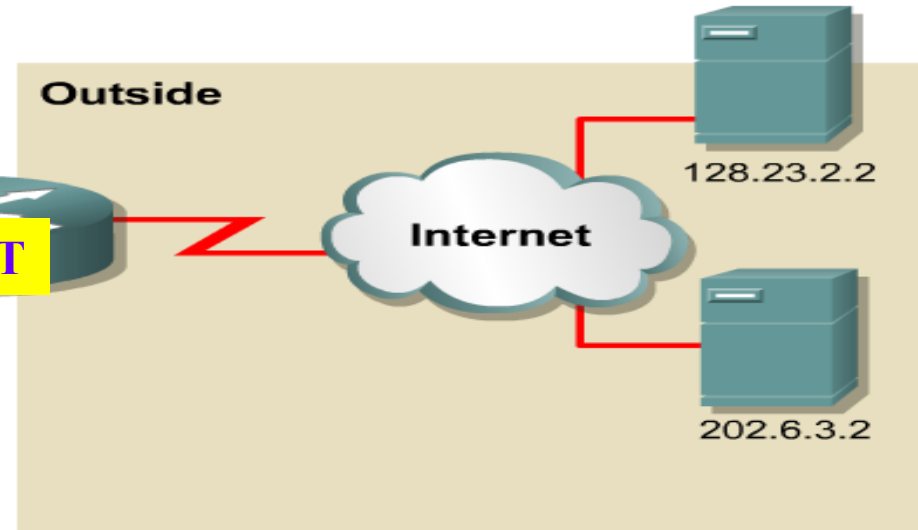
PAT – Port Address Translation

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

Inside

PC3
10.0.0.3

Web Browsing

PC2
10.0.0.2

NAT

Outside

Web Server
128.23.2.2

Internet

202.6.3.2

NAT/PAT table maintains translation of:

DA, SA, DP, SP

DA	SA	DP	SP	
128.23.2.2	10.0.0.3	80	1331	Data

IP Header   TCP/UDP Header

1

DA	SA	DP	SP	
128.23.2.2	10.0.0.2	80	1555	Data

IP Header   TCP/UDP Header

DA	SA	DP	SP	
128.23.2.2	179.9.8.80	80	1331	Data

IP Header   TCP/UDP Header

2

DA	SA	DP	SP	
128.23.2.2	179.9.8.80	80	1555	Data

IP Header   TCP/UDP Header

PAT Example   Two PCs using 179.9.8.80

Inside

PC3 10.0.0.3

PC2 10.0.0.2

Outside

Internet

128.23.2.2

202.6.3.2

NAT/PAT table maintains translation of:

SA (DA), DA (SA), DP (SP)

	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		

SWIN BUR NE
SWINBURNE UNIVERSITY OF TECHNOLOGY

Static

Address

Translation

Static NAT
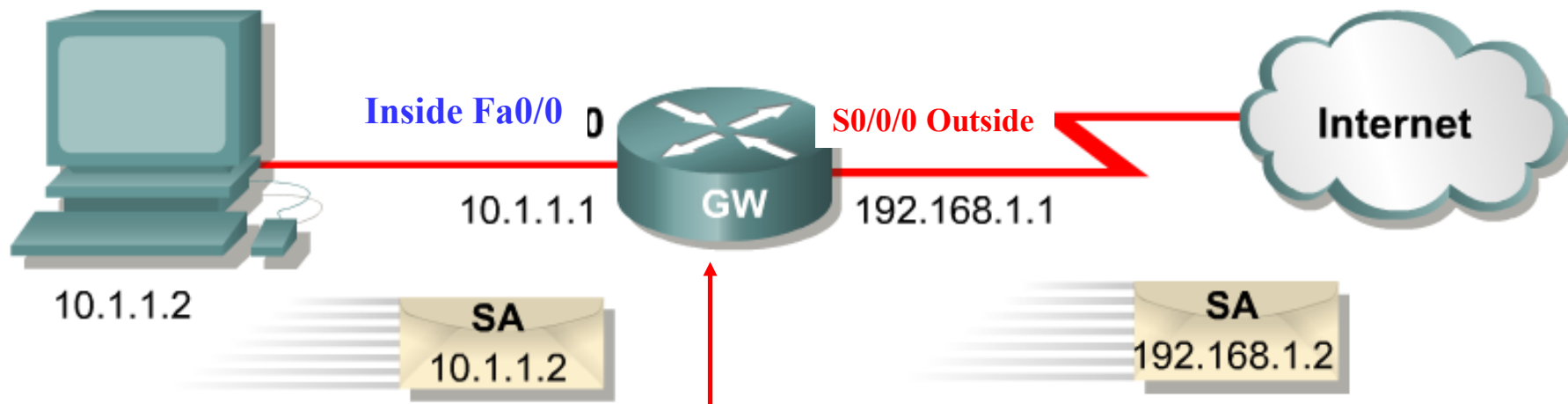
- Uses a one-to-one mapping of private and public addresses

- Mappings remain constant

- Useful for web servers or hosts that must have a constant address that is accessible from the internet

Configuring **Static** NAT

Inside Fa0/0 0 **S0/0/0 Outside** Internet

10.1.1.1 GW 192.168.1.1

10.1.1.2

SA
10.1.1.2

SA
192.168.1.2

```
hostname GW
!
ip nat inside source static 10.1.1.2 192.168.1.2
!
interface Fa0/0
  ip address 10.1.1.1 255.255.255.0
  ip nat inside
!
interface S0/0/0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
```

Dynamic NAT

- Uses a pool of public addresses and assigns them on a first-come, first-served basis

- When a host with a Private IP address requests access to the Internet, an ip address from the pool is allocated

- The NAT Pool, the range of ip addresses available

- The ACL, that permits access to the NAT pool

- The Binding Statement, binding the ACL to the NAT Pool

Configuring **Dynamic** NAT

Inside Fa0/0

10.1.1.1

S0/0/0 Outside

192.168.1.1

Internet

10.1.1.2

10.1.0.2
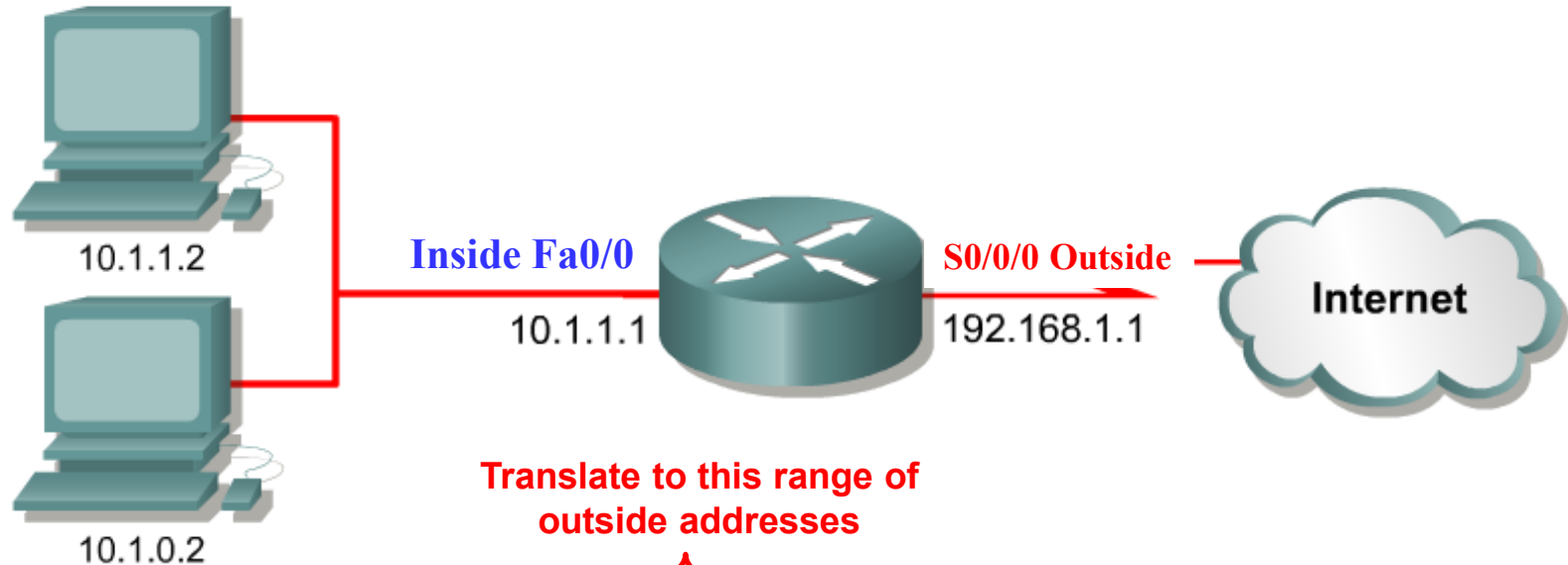
Translate to this range of outside addresses

```
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 10.1.0.0 0.0.255.255
```
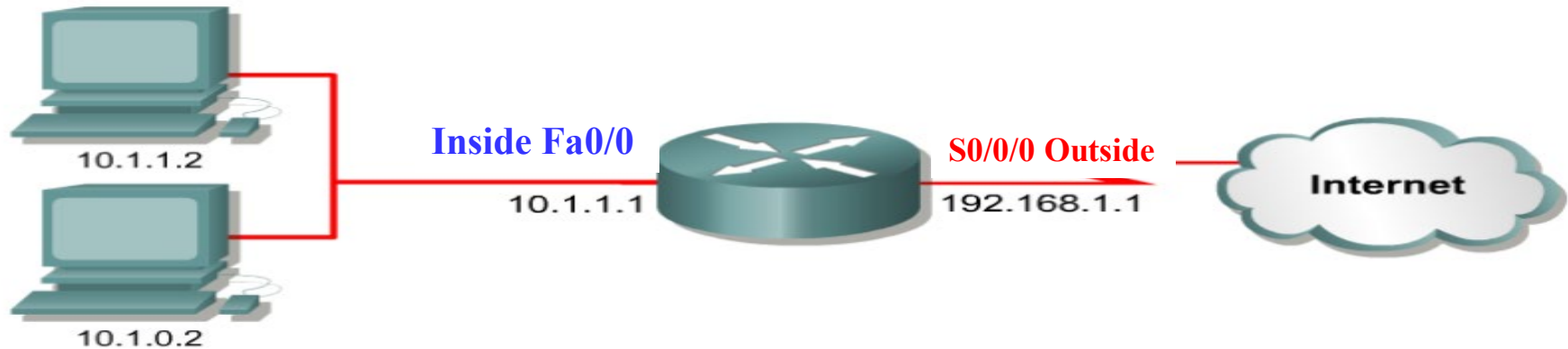
Fa0/0

Binding to ACL

S0/0/0

Source subnet IP address must match here

Configuring **PAT – Overload on Pool**

Inside Fa0/0
10.1.1.1

S0/0/0 Outside
192.168.1.1

10.1.1.2

10.1.0.2

Internet

```
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**
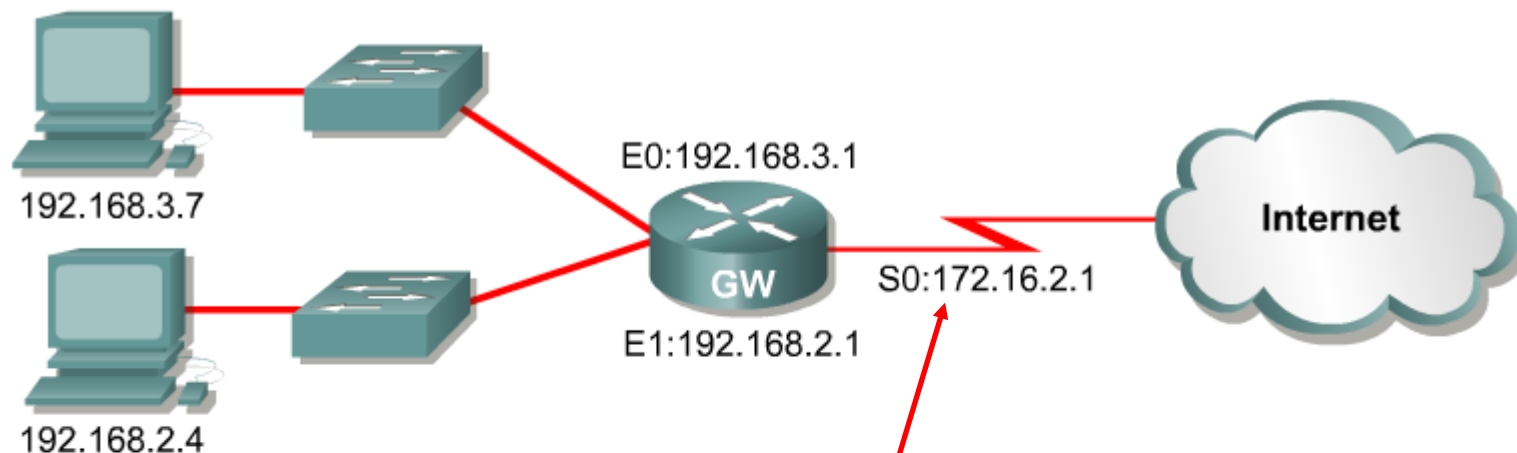

```
interface ethernet 0
  ip address 192.168.3.1 255.255.255.0
  ip nat inside
!
interface ethernet 1
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside
!
ip nat inside source list 1 interface serial 0 overload
!
access-list 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
```
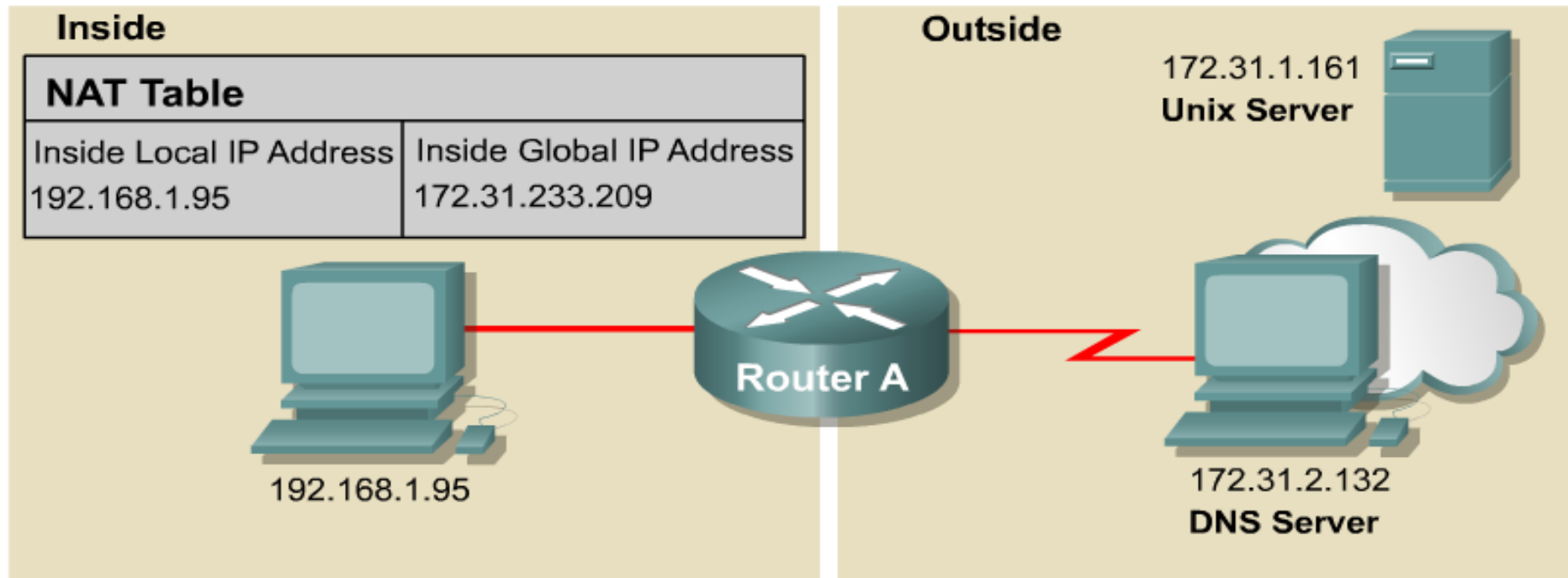
Command	Description
show ip nat translations	Displays active translations
show ip nat statistics	Displays translation statistics

Troubleshooting NAT/PAT

Inside

NAT Table

Inside Local IP Address	Inside Global IP Address
192.168.1.95	172.31.233.209

192.168.1.95

Router A

Outside

172.31.1.161
Unix Server

172.31.2.132
DNS Server

```
RouterA#debug ip nat                    Watch the NAT translations
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]
```

- [NAT Explained | Overload, Dynamic & Static - YouTube](#)

THE   END