NAT (Network Address Translation)

Private addressing

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

- 172.16.0.0 – 172.31.255.255: 172.16.0.0/12
  - ¿De donde viene /12

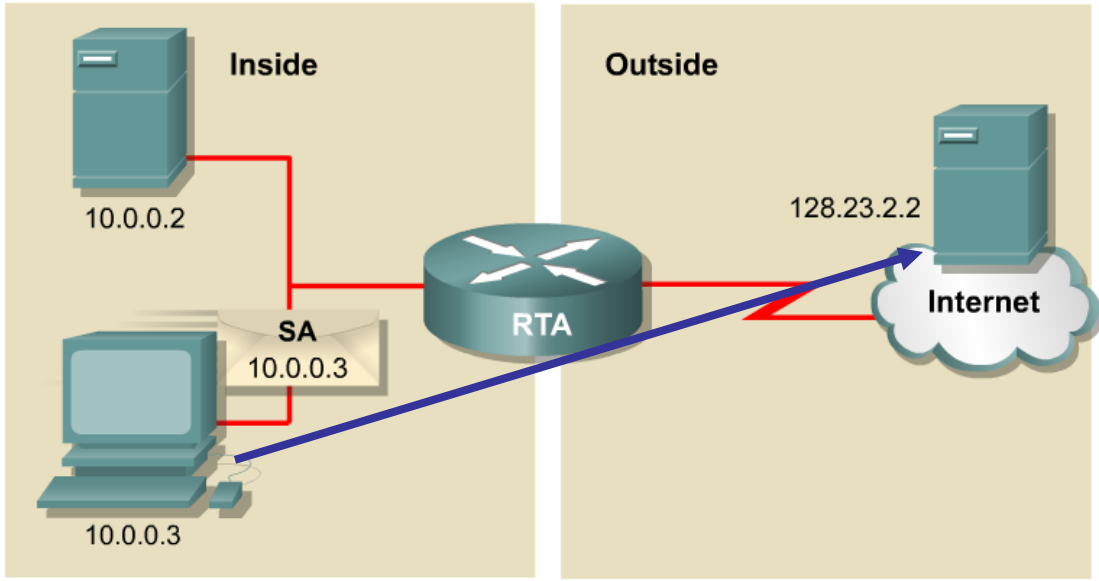
12 bits in common

10101100 . 0001 0000 . 00000000 . 00000000 – 172.16.0.0

10101100 . 0001 1111 . 11111111 . 11111111 – 172.16.255.255

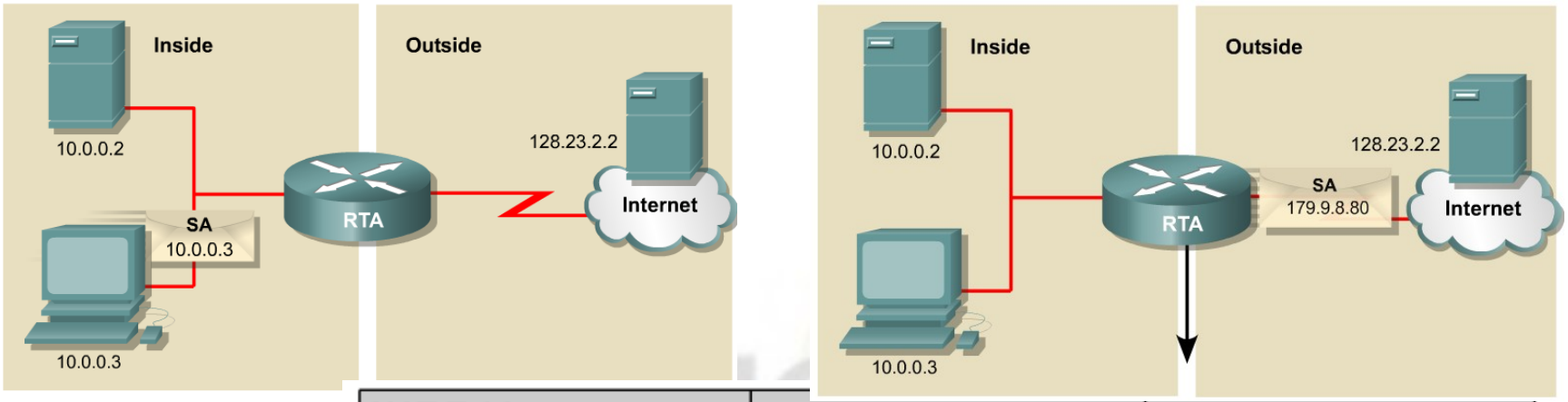
10101100 . 0001 0000 . 00000000 . 00000000 – 172.16.0.0/12

Introducing NAT and PAT



- NAT se diseño para conservar las direcciones IP y habilitar a las redes a usar direcciones privadas en las redes internas.
- Esas direcciones privadas internas, son traducidas a direcciones publicas ruteables.
- **NAT**,como lo define el RFC 1631, es el proceso de reemplazo de una direccion IP por otra en la cabecera IP.
- En la practica, NAT es usado para permitir a los hosts que son identificadas privadamente acceder a Internet.
- La traduccion NAT puede ocurrir estaticamente o dinamicamente.
- La caracteristica mas resaltante de los ruteadores NAT es su capacidad de usar port address translation (PAT), el cual permite a multiples direcciones internas mapear a las mismas direcciones globales.
- Esto es algunas veces NAT muchos a uno.

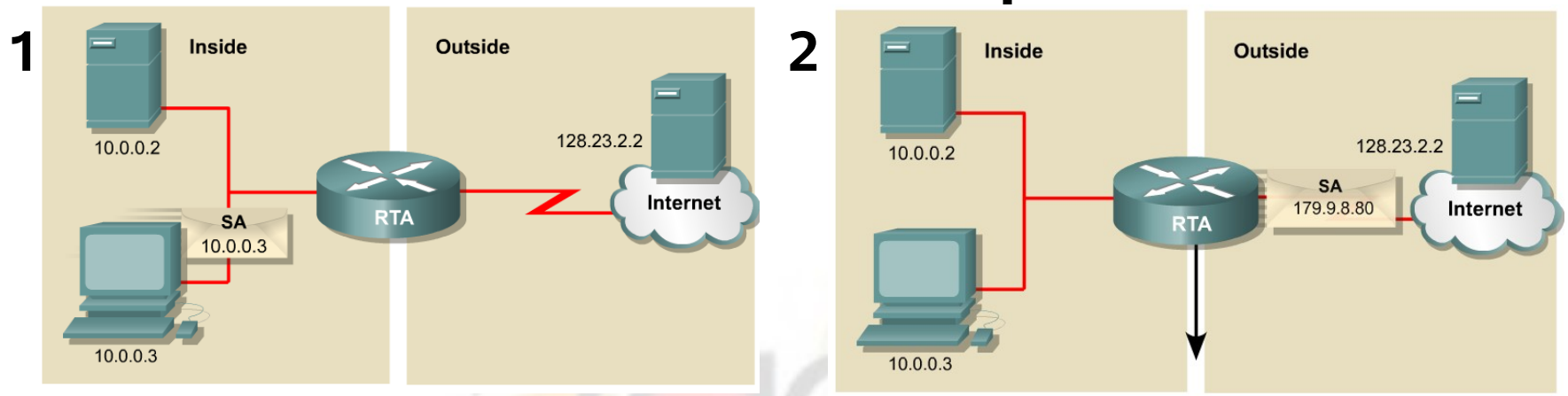
NAT Example



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 address** – La direccion IP asignada a un host en la red interna. Esta direccion es una direccion segun el RFC 1918 (direcciones privadas).
- **Inside global address** – Una direccion IP legitima (ruteable en internet o publica)direcciones IP asignadas por el ISP que representan a una o mas direcciones IP locales internas ante el mundo externo.
- **Outside local address** – La direccion IP de un host externo como este es conocido por los host en la red interna.

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

1

DA	SA		
128.23.2.2	10.0.0.3	....	Data

IP Header

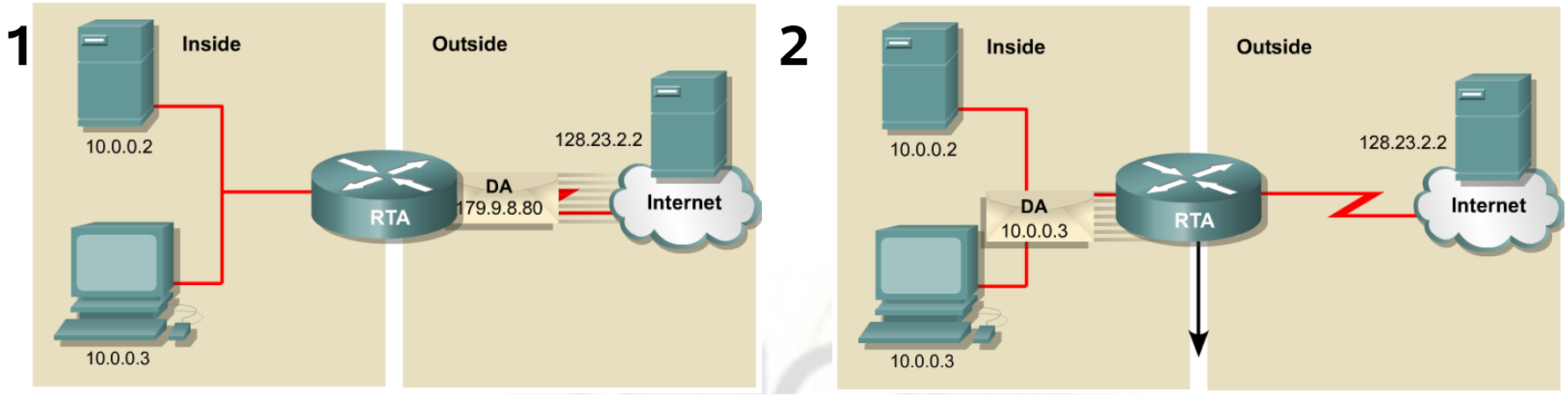
2

DA	SA		
128.23.2.2	179.9.8.80	....	Data

IP Header

- La traduccion de direcciones IP privadas a direcciones IP publicas.

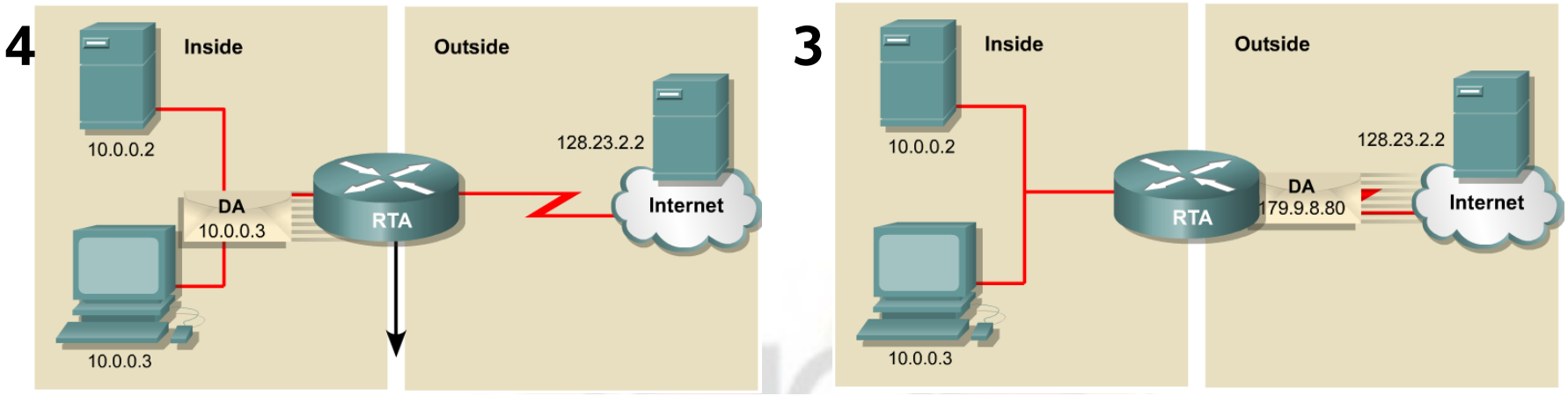
NAT Example



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

- **Inside local address** – La direccion IP asignada a un host en la red interna.
- **Inside global address** – Una direccion IP legitima asignada por el proveedor del servicio.
- **Outside global address** – La direccion IP asignada a un host en la red externa. Los propietarios del host asignan esta direccion.

NAT Example



NAT Table

Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.2	179.9.8.80	128.23.2.2
10.0.0.3	179.9.8.80	128.23.2.2

4

DA	SA		
10.0.0.3	128 .23.2.2	....	Data

IP Header

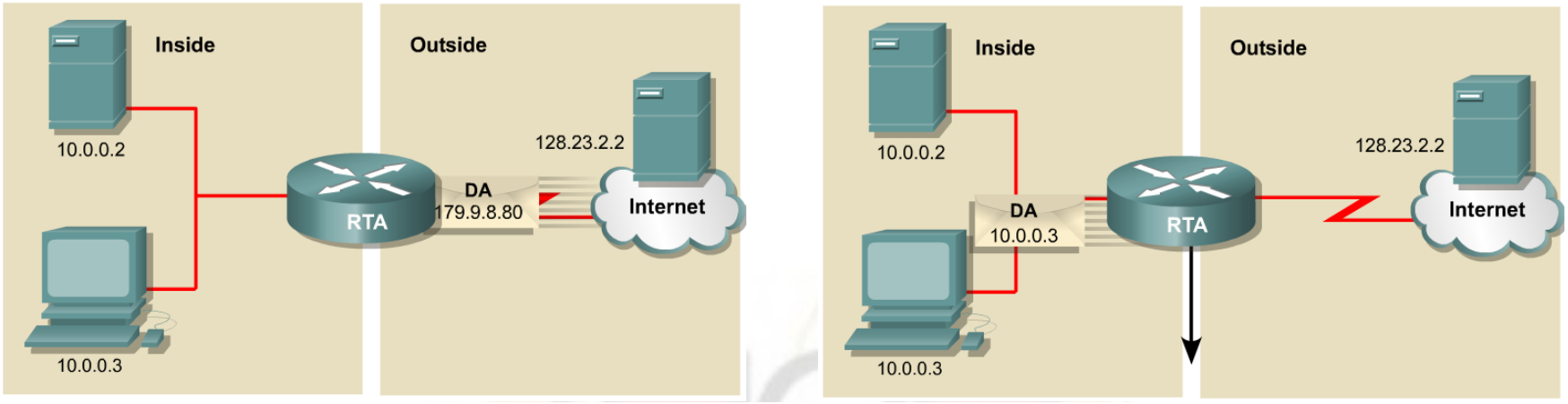
3

DA	SA		
179.9.8.80	128.23.2.2	....	Data

IP Header

- Traduccion de retorno, de la direccion IP publica a la direccion IP privada.

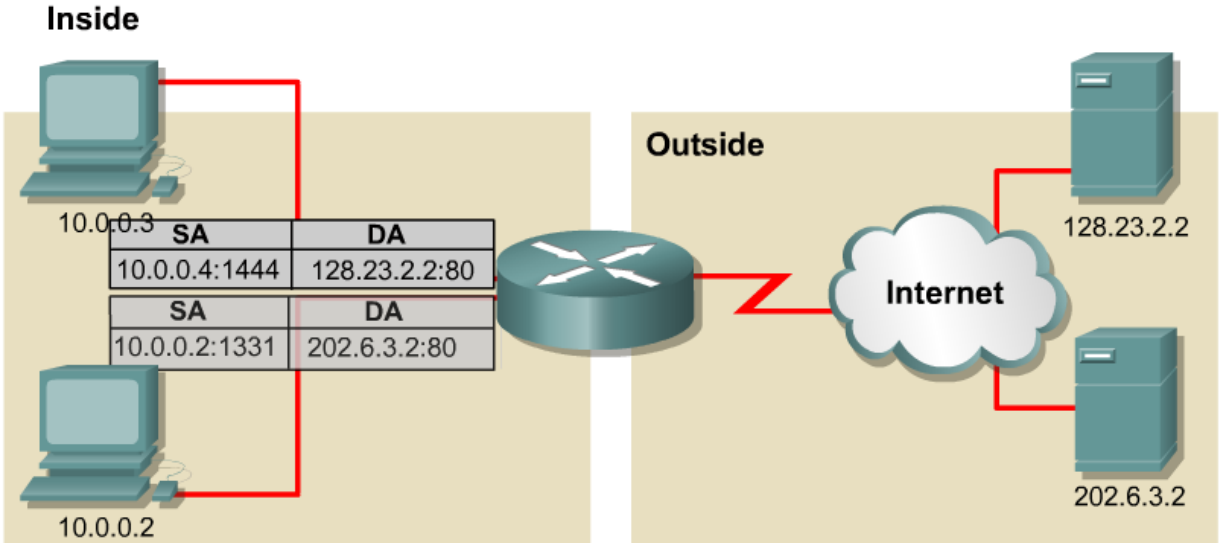
NAT Example



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

- NAT permite tener mas direcciones IP que las asignadas, mediante el RFC 1918.
- Sin embargo, debido a que tiene que usar direcciones IP publicas para la internet, NAT limita el numero de host que puede tener acceso a Internet a uno a la vez (dependiendo el numero de host en su mascara de red publica).

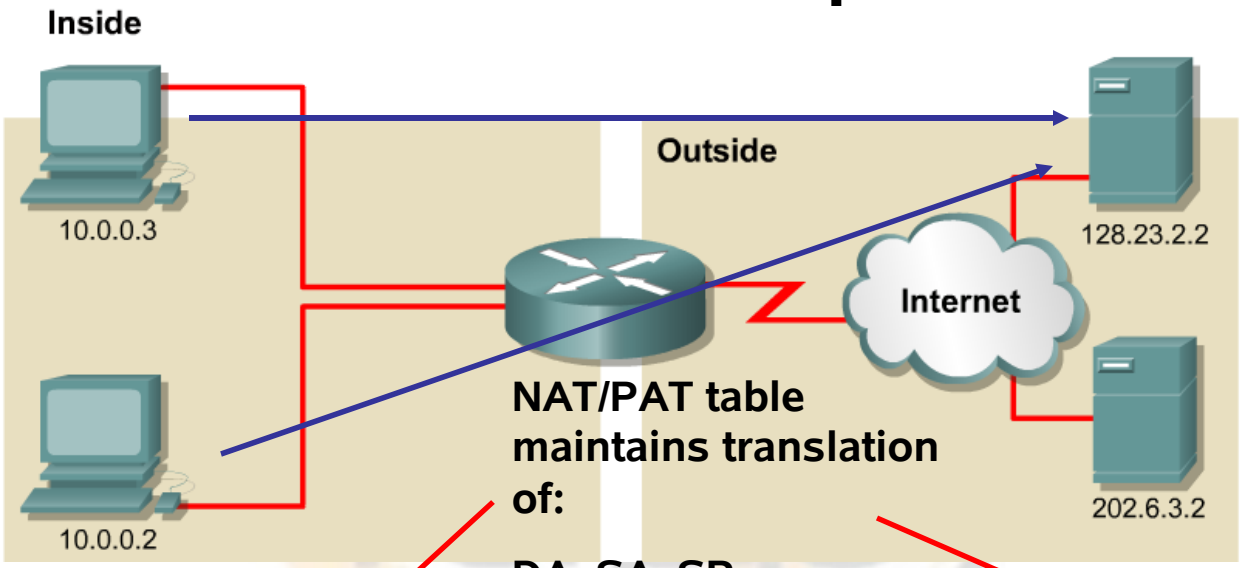
PAT – Port Address Translation



NAT Table			
Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global Address
10.0.0.2:1331 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

- PAT (Port Address Translation)permite usar una unica direccion publica y asignar hasta 65536 hosts internos (4000 es mas realista).
- PAT modifica el puerto origen TCP/UDP para el seguimiento de la direccion de host interna.
- El seguimiento y traduccion SA, DA y SP (los cuales identifican de manera unica cada conexion) para cada flujo de datos.

PAT Example



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	179.9.8.80	80	3333	Data

IP Header | TCP/UDP Header

2

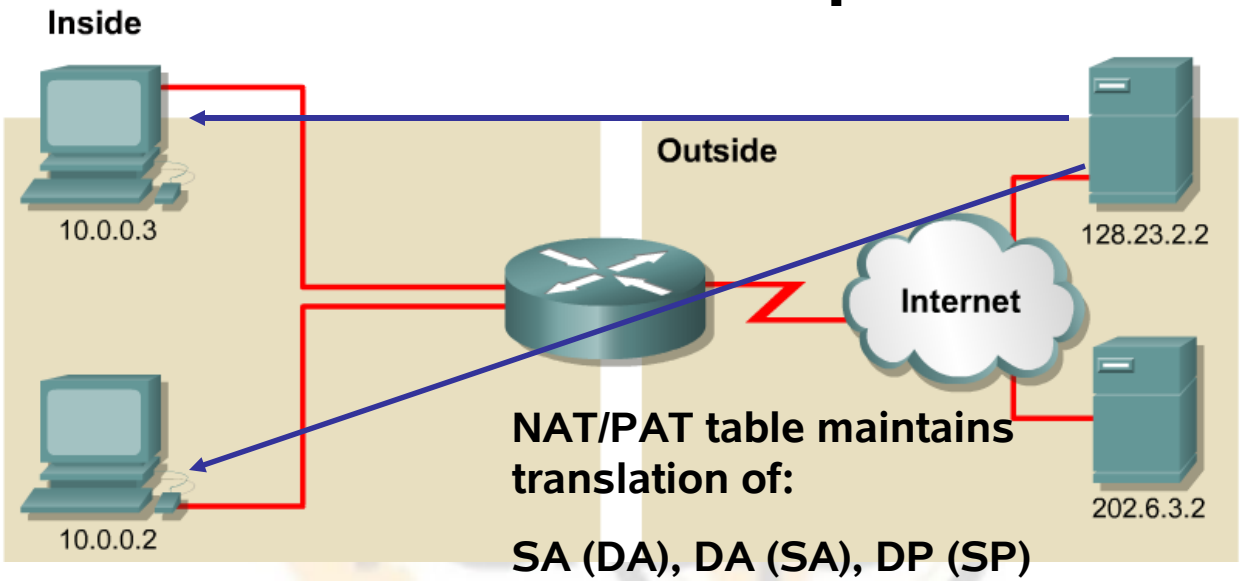
DA	SA	DP	SP	
128.23.2.2	10.0.0.2	80	1555	Data

IP Header | TCP/UDP Header

DA	SA	DP	SP	
128.23.2.2	179.9.8.80	80	2222	Data

IP Header | TCP/UDP Header

PAT Example



DA	SA	DP	SP	
10.0.0.3	128.23.2.2	1331	80	Data

IP Header | TCP/UDP Header

4

DA	SA	DP	SP	
179.9.8.80	128.23.2.2	3333	80	Data

IP Header | TCP/UDP Header

3

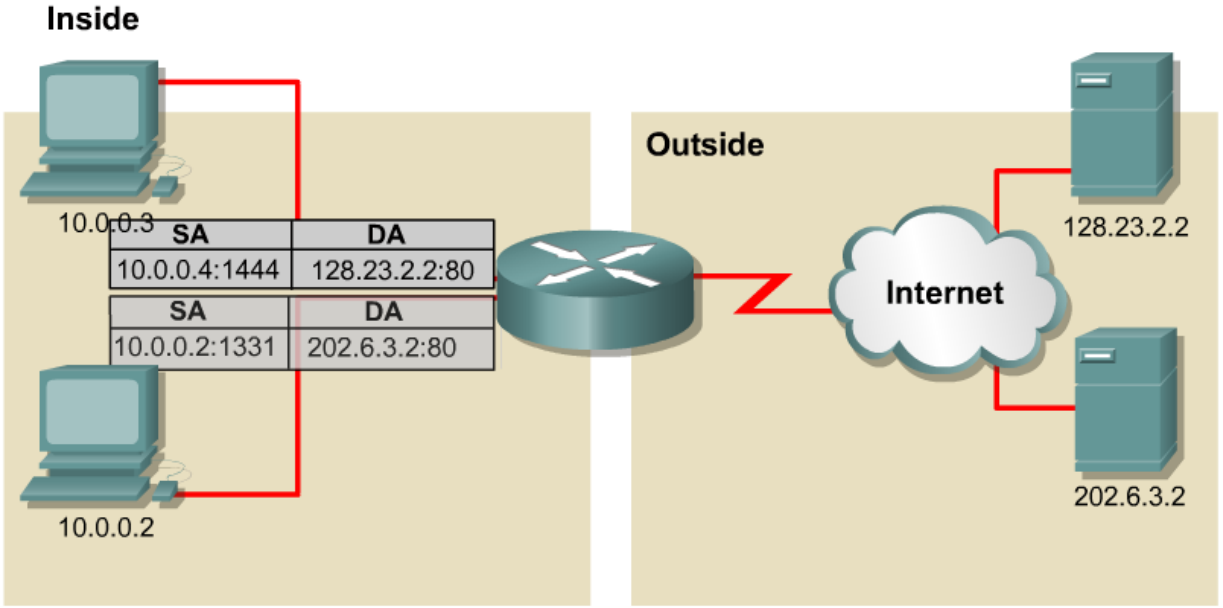
DA	SA	DP	SP	
10.0.0.2	128.23.2.2	1555	80	Data

IP Header | TCP/UDP Header

DA	SA	DP	SP	
179.9.8.80	128.23.2.2	2222	80	Data

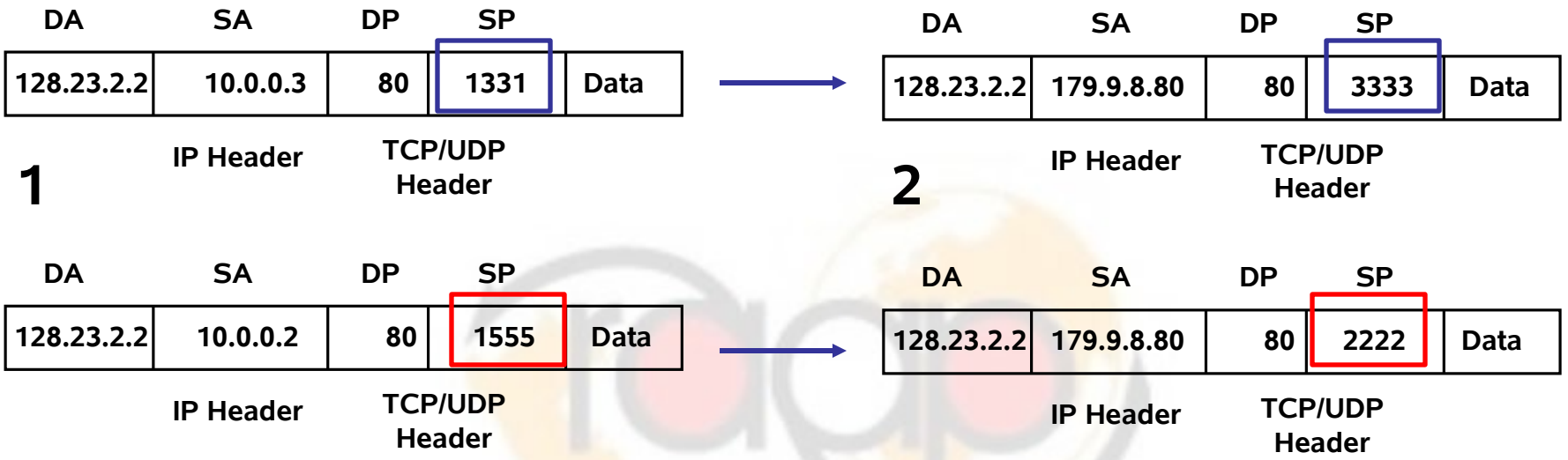
IP Header | TCP/UDP Header

PAT – Port Address Translation

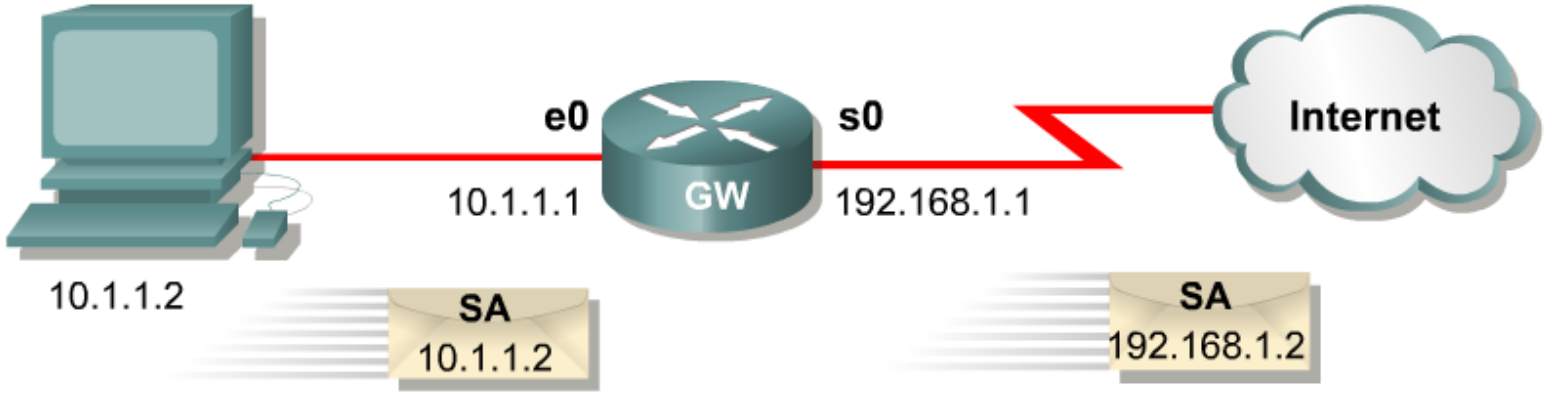


- Con PAT multiples direcciones IP privadas pueden ser traducidas a una unica direccion publica (many-to-one translation).
- Esto resuelve la limitacion de NAT, el cual hace una traduccion uno a uno.

PAT – Port Address Translation

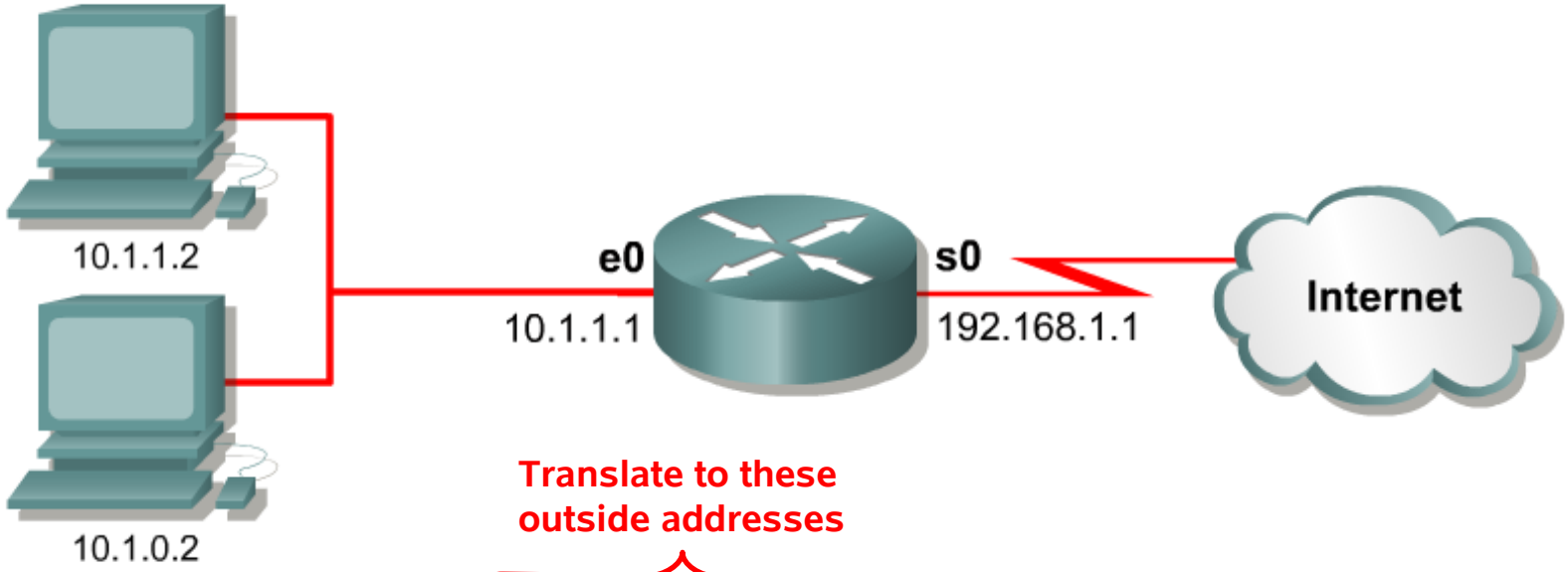


Configuring Static NAT




```
hostname GW
!
ip nat inside source static 10.1.1.2 192.168.1.2
!
interface ethernet 0
  ip address 10.1.1.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
```

Configuring Dynamic NAT



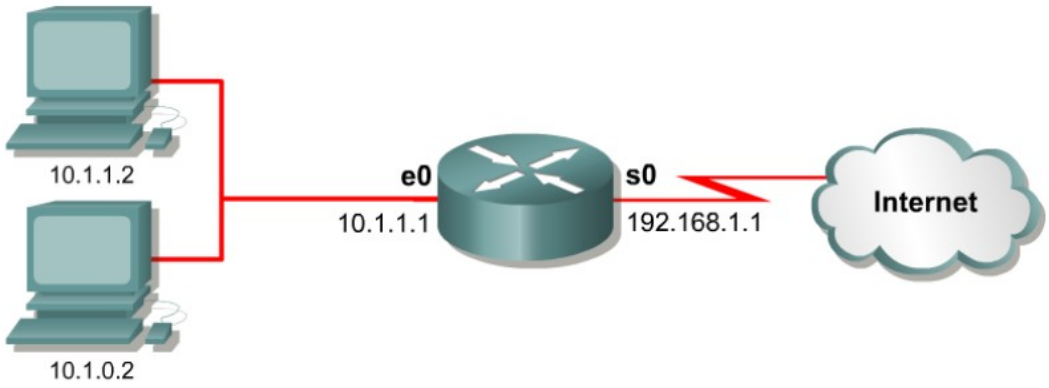
Translate to these outside addresses

Start here

```
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 0
  ip address 10.1.1.1 255.255.0.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
access-list 1 permit 10.1.0.0 0.0.0.255
```

Source IP address must match here

Configure PAT – Overload



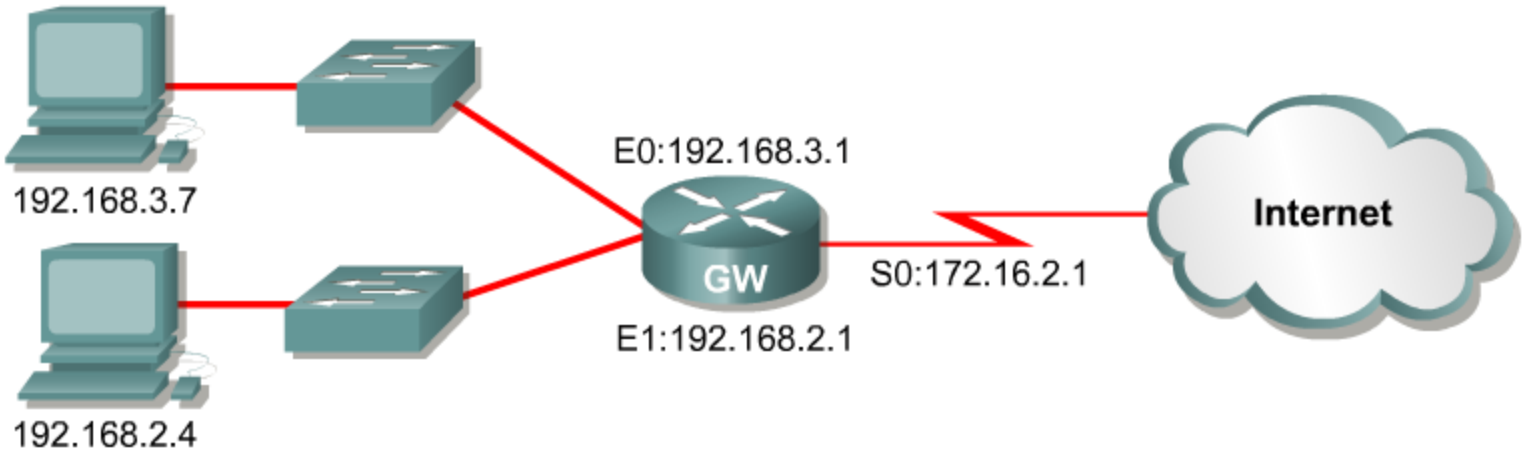

```
Router(config)#access-list 1 permit 10.0.0.0 0.0.255.255

Router(config)#ip nat pool nat-pool2 179.9.8.20 netmask
255.255.255.240

Router(config)#ip nat inside source list 1 pool nat-pool2
overload
```

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

Configure PAT – Overload




```
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 IP address of the outside interface instead specifying an IP address

NAT/PAT 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/PAT

```
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               ---                ---
```

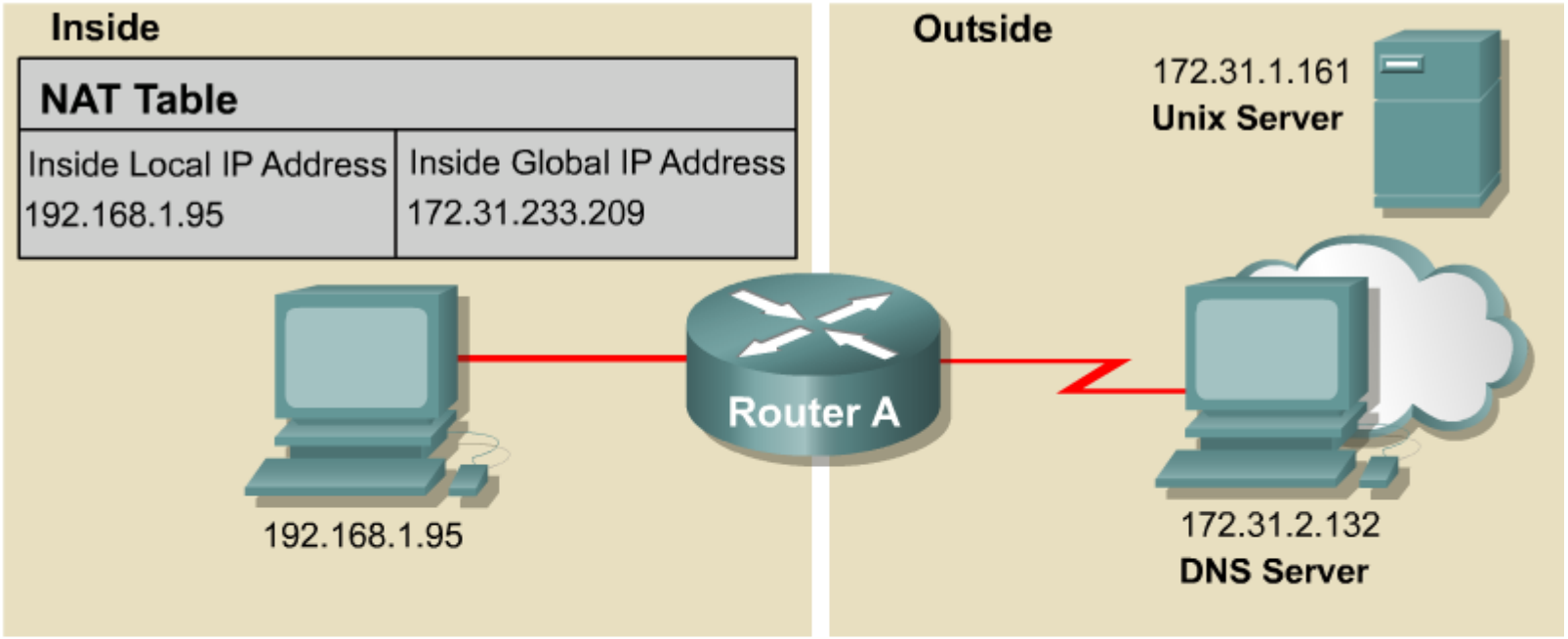
```
Router#show ip nat statistics
```

- 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]
```

Issues with NAT/PAT

NAT has several advantages, including the following:

- NAT conserves the legally registered addressing scheme by allowing the privatization of intranets.
- NAT allows the existing scheme to remain, and it still supports the new assigned addressing scheme outside the private network.

Cisco IOS NAT does support the following traffic types although they carry IP addresses in the application data stream:

- ICMP
- File Transfer Protocol (FTP), including PORT and PASV commands
- NetBIOS over TCP/IP, datagram, name, and session services
- Progressive Networks' RealAudio
- White Pines' CuSeeMe
- DNS "A" and "PTR" queries
- H.323/NetMeeting, versions 12.0(1)/12.0(1)T and later
- VDOLive, version 11.3(4)11.3(4)T and later
- Vxtreme, versions 11.3(4)11.3(4)T and later
- IP multicast, version 12.0(1)T, the source address translation only

Cisco IOS NAT does not support the following traffic types:

- Routing table updates
- DNS zone transfers
- BOOTP
- talk, ntalk
- Simple Network Management Protocol (SNMP)

PREGUNTAS