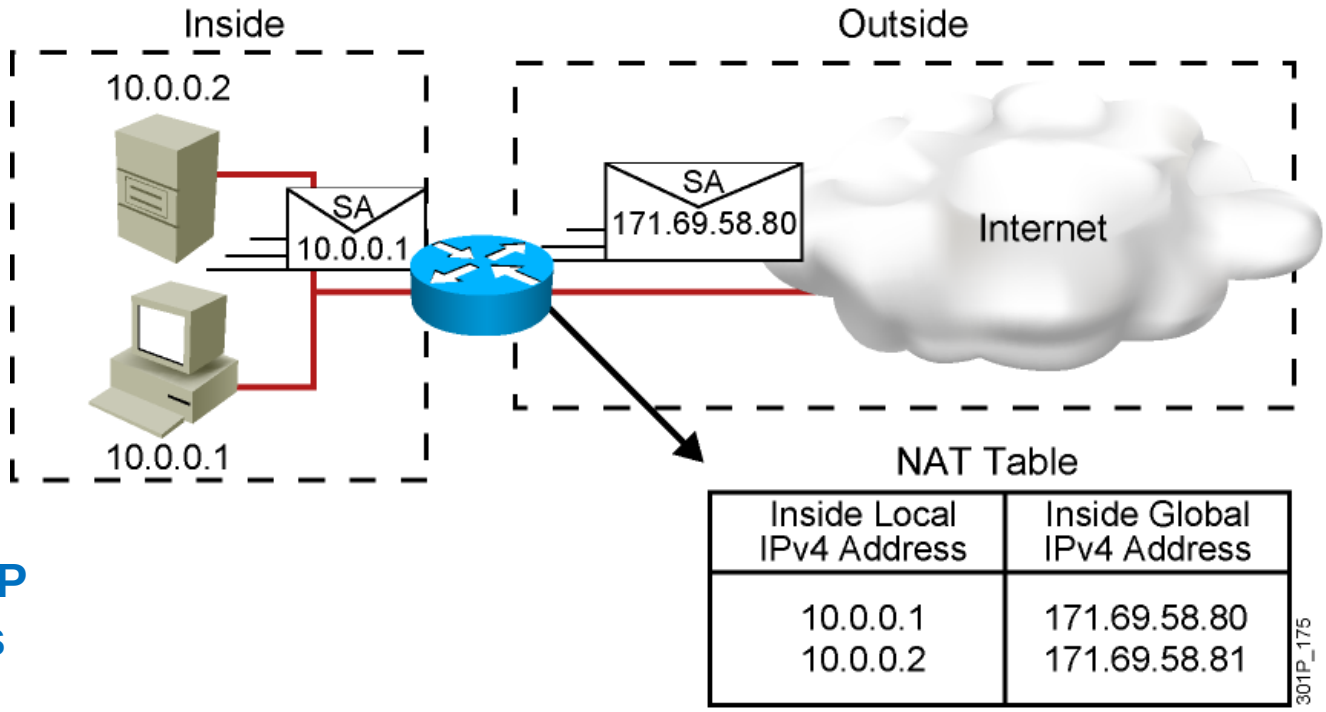
Address Space Management

Scaling the Network with NAT and PAT

Network Address Translation

- **Network location:**
  - **Inside**
  - **Outside**
- **Type of IP address:**
  - **Local**
  - **Global**

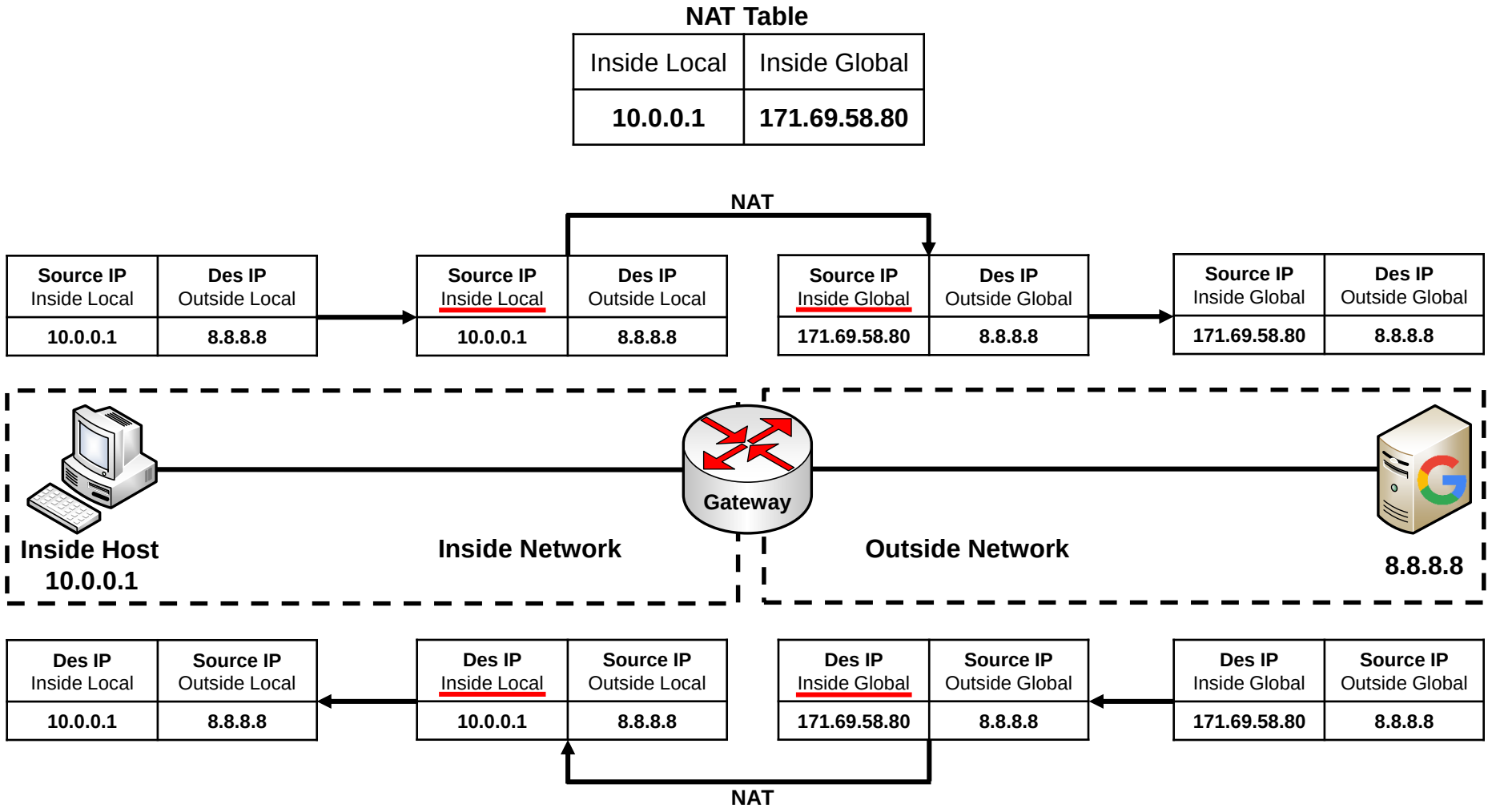


- **NAT Terms:**

Host location **Type of IP address**

- **Inside Local address:** the Local IP address of an Inside host.
- **Inside Global address:** the Global IP address that represents the Inside host.
- **Outside Local address:** the IP address of an Ouside host as it appears to the Inside network.
- **Outside Global address:** the IP address of an Outside host as it appears to the Outside network.

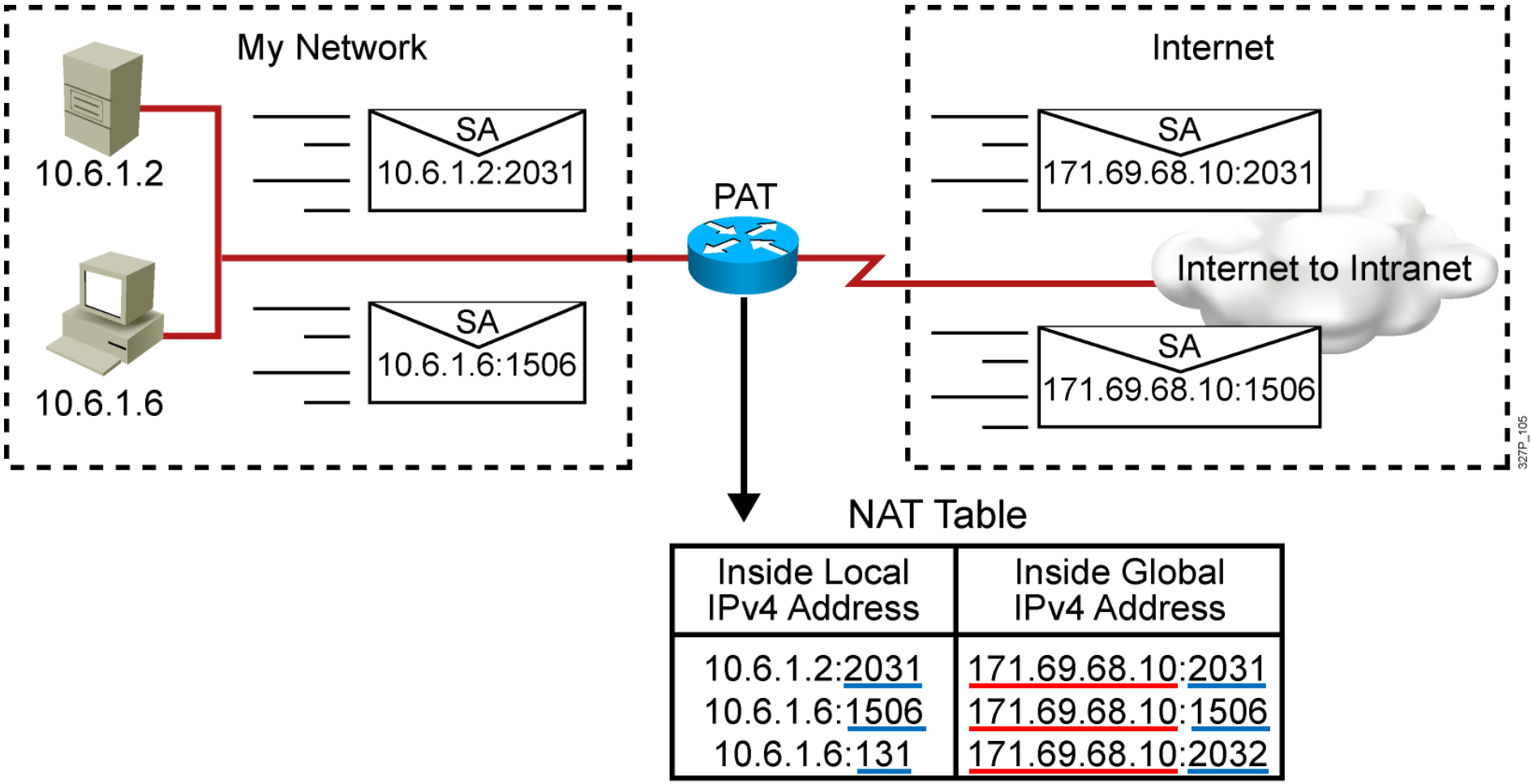
Network Address Translation



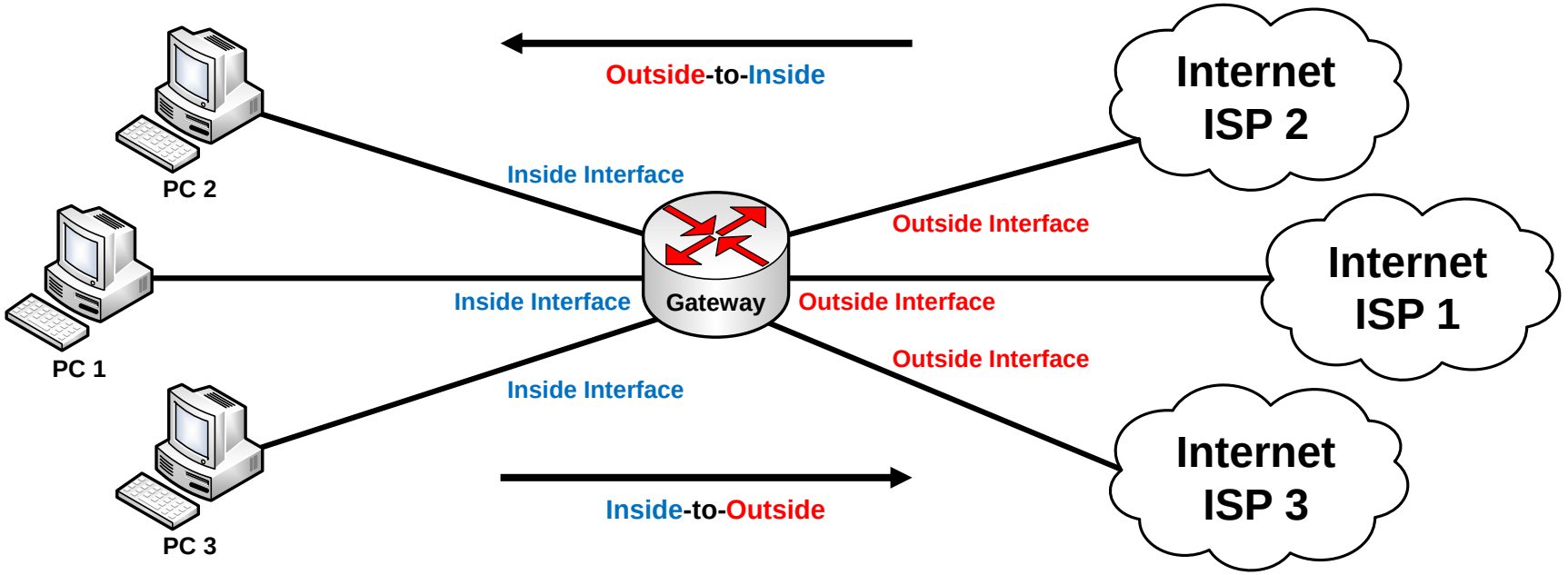
Different types of NAT

- **Static NAT:** One-to-One mapping
  - 1 Private IP address → 1 Public IP address
  - Useful when a network device inside a private network needs to be accessible from internet.
- **Dynamic NAT:** Many-to-Many mapping
  - Many Private IP addresses → Many Public IP addresses (NAT pool)
  - Establishes a one-to-one mapping between a private IP address to a public IP address. The public IP address is taken from the NAT pool.
- **NAT Overloading** or **PAT (Port Address Translation):** Many-to-One mapping
  - Many Private IP addresses → 1 Public IP address
  - Permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

NAT Overloading
Port Address Translation (PAT)



NAT Order of Operation



NAT Order of Operation	
Inside-to-Outside	**Outside-to-Inside**
▪ check input access list ▪ routing ▪ **NAT inside to outside (local to global translation)** ▪ check output access list	▪ check input access list ▪ **NAT outside to inside (global to local translation)** ▪ routing ▪ check output access list

Configuring and Verifying Static Translation

```
RouterX(config)# ip nat inside source static local-IP global-IP
```

- Establishes static translation between an inside local address and an inside global address

```
RouterX(config-if)# ip nat inside
```

- Marks the interface as connected to the inside network

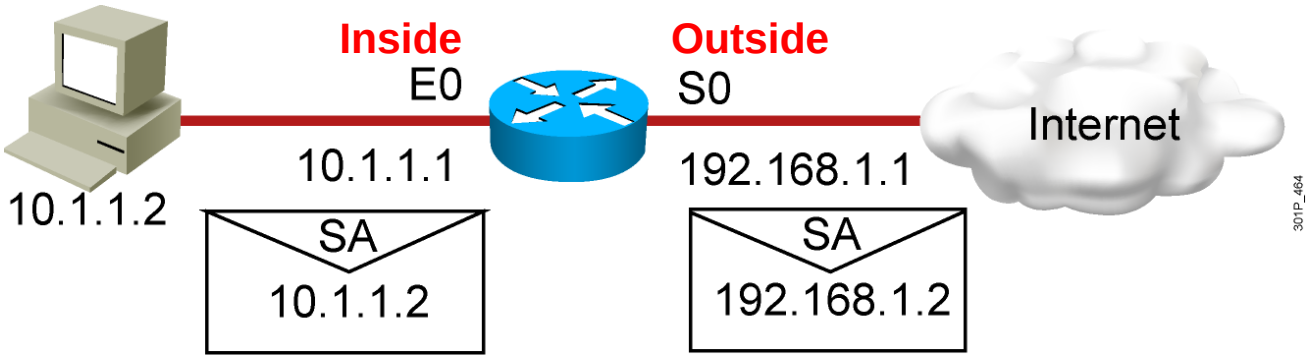
```
RouterX(config-if)# ip nat outside
```

- Marks the interface as connected to the outside network

```
RouterX# show ip nat translations
```

- Displays active translations

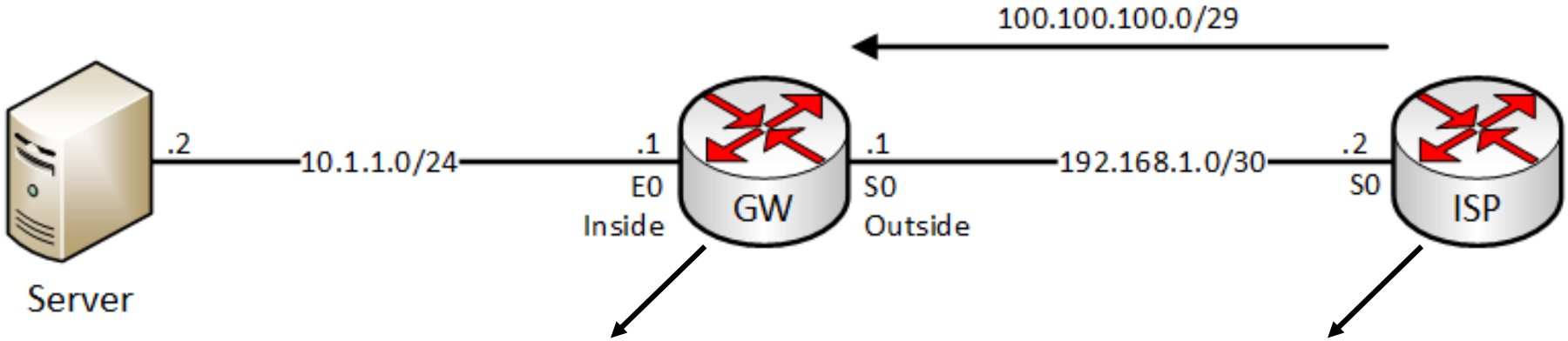
Enabling Static NAT Address Mapping Example




```
interface s0
 ip address 192.168.1.1 255.255.255.0
 ip nat outside
!
interface e0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
!
ip nat inside source static  10.1.1.2  192.168.1.2
!
ip route  0.0.0.0  0.0.0.0  s0
```

```
RouterX# show ip nat translations
    Pro     Inside global     Inside local      Outside local      Outside global
    ---     192.168.1.2       10.1.1.2          ---                ---
    icmp    192.168.1.2:21    10.1.1.2:21       192.168.1.10:21    192.168.1.10:21
```

Enabling Static NAT Address Mapping Example (cont.)




```
interface s0
 ip address 192.168.1.1 255.255.255.252
 ip nat outside
!
interface e0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
!
ip nat inside source static 10.1.1.2  100.100.100.1
!
ip route  0.0.0.0  0.0.0.0  192.168.1.2
```

```
interface s0
 ip address 192.168.1.2 255.255.255.252
!
ip route 100.100.100.0 255.255.255.248 192.168.1.1
```

```
GW# show ip nat translations
    Pro  Inside global   Inside local   Outside local   Outside global
    ---  100.100.100.1   10.1.1.2       ---             ---
```

Configuring and Verifying Dynamic Translation

```
RouterX(config)# ip nat pool name start-ip end-ip
{netmask netmask | prefix-length prefix-length}
```

- Defines a pool of global addresses to be allocated as needed

```
RouterX(config)# access-list access-list-number permit
source-IP [source-wildcard]
```

- Defines a standard IP ACL permitting those inside local addresses that are to be translated

```
RouterX(config)# ip nat inside source list access-list-number
pool name
```

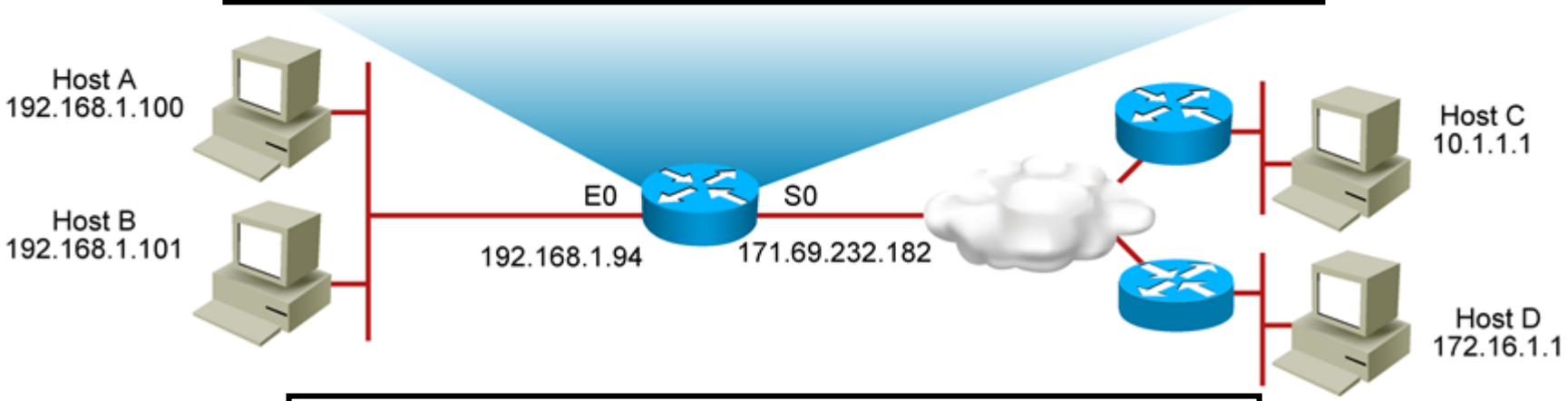
- Establishes dynamic source translation, specifying the ACL that was defined in the previous step

```
RouterX# show ip nat translations
```

- Displays active translations

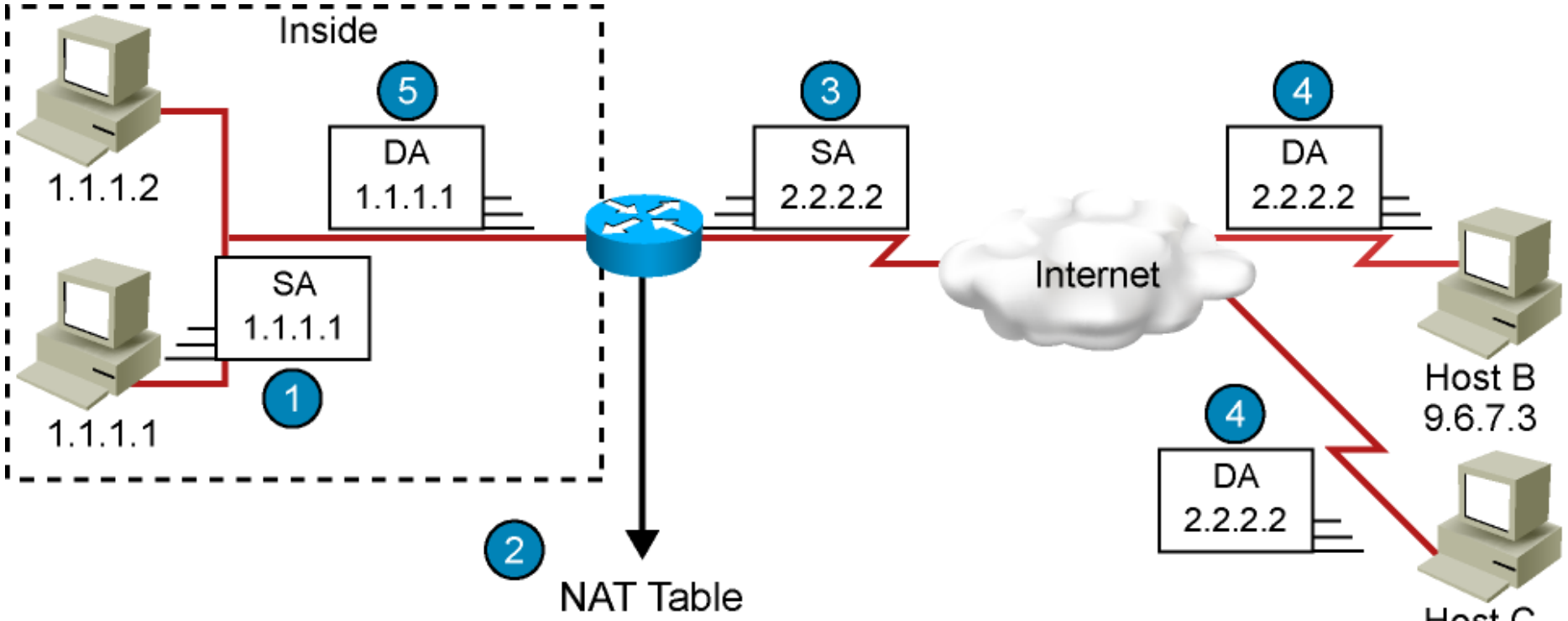
Dynamic Address Translation Example

```
ip nat pool net-208  171.69.233.209  171.69.233.222  netmask  255.255.255.240
access-list  1  permit  192.168.1.0  0.0.0.255
ip nat inside source list  1  pool  net-208
!
ip route  0.0.0.0  0.0.0.0  s0
!
interface serial 0
 ip address  171.69.232.182  255.255.255.240
 ip nat outside
!
interface ethernet 0
 ip address  192.168.1.94  255.255.255.0
 ip nat inside
```




```
RouterX# show ip nat translations
  Pro   Inside global     Inside local       Outside local      Outside global
  ---   171.69.233.209    192.168.1.100      ---                ---
  ---   171.69.233.210    192.168.1.101      ---                ---
```

Overloading an Inside Global Address



Protocol	Inside Local IPv4 Address:Port	Inside Global IPv4 Address:Port	Outside Global IPv4 Address:Port
TCP	1.1.1.2:1723	2.2.2.2:1723	6.5.4.7:23
TCP	1.1.1.1:1024	2.2.2.2:1024	9.6.7.3:23

Configuring Overloading

```
RouterX(config)# access-list access-list-number permit
source-IP source-wildcard
```

- Defines a standard IP ACL that will permit the inside local addresses that are to be translated

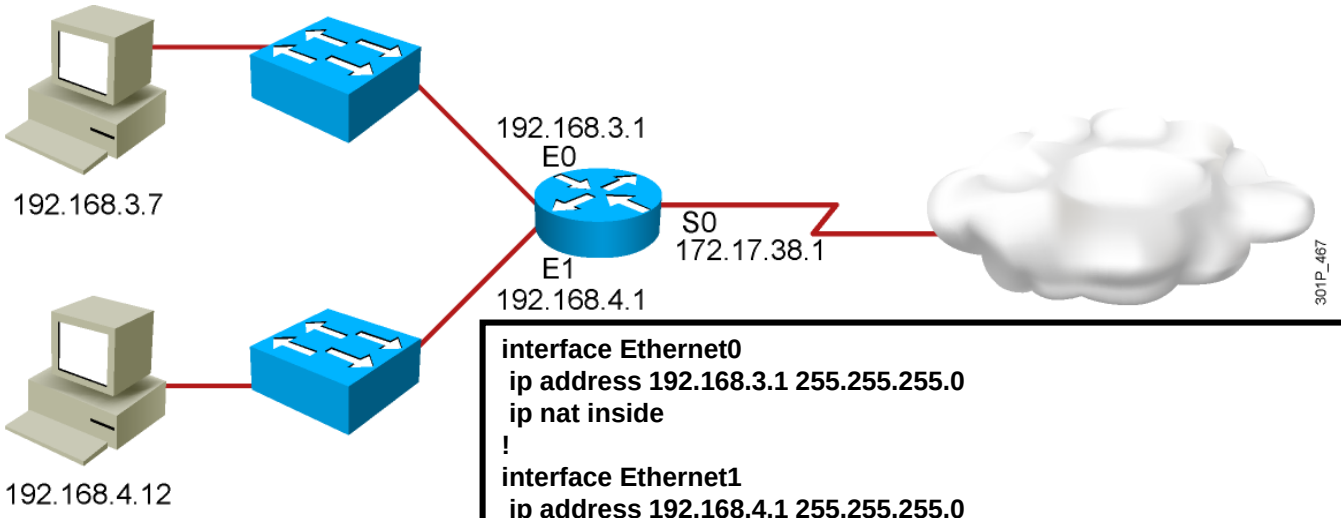
```
RouterX(config)# ip nat inside source list access-list-number
interface interface overload
```

- Establishes dynamic source translation, specifying the ACL that was defined in the previous step

```
RouterX# show ip nat translations
```

- Displays active translations

Overloading an Inside Global Address Example




```
interface Ethernet0
 ip address 192.168.3.1 255.255.255.0
 ip nat inside
!
interface Ethernet1
 ip address 192.168.4.1 255.255.255.0
 ip nat inside
!
interface Serial0
 description To ISP
 ip address 172.17.38.1 255.255.255.0
 ip nat outside
!
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.0.255
!
ip nat inside source list 1 interface Serial0 overload
!
ip route 0.0.0.0 0.0.0.0 Serial0
```

```
RouterX# show ip nat translations
    Pro Inside global     Inside local       Outside local      Outside global
    TCP 172.17.38.1:1050  192.168.3.7:1050   10.1.1.1:23        10.1.1.1:23
    TCP 172.17.38.1:1776  192.168.4.12:1776  10.2.2.2:25        10.2.2.2:25
```

Clearing the NAT Translation Table

```
RouterX# clear ip nat translation *
```

- **Clears all dynamic address translation entries**

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

- Clears a simple dynamic translation entry that contains an inside translation or both an inside and outside translation

```
RouterX# clear ip nat translation outside
local-ip global-ip
```

- Clears a simple dynamic translation entry that contains an outside translation

```
RouterX# 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 (PAT entry)

Translation Not Occurring: Translation Not Installed in the Table

Verify that:

- **There are no inbound ACLs that are denying the packets entry to the NAT router**
- **The ACL referenced by the NAT command is permitting all necessary networks**
- **There are enough addresses in the NAT pool**
- **The router interfaces are appropriately defined as NAT inside or NAT outside**

Displaying Information with show and debug Commands

```
RouterX# 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 [23312]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23313]
```

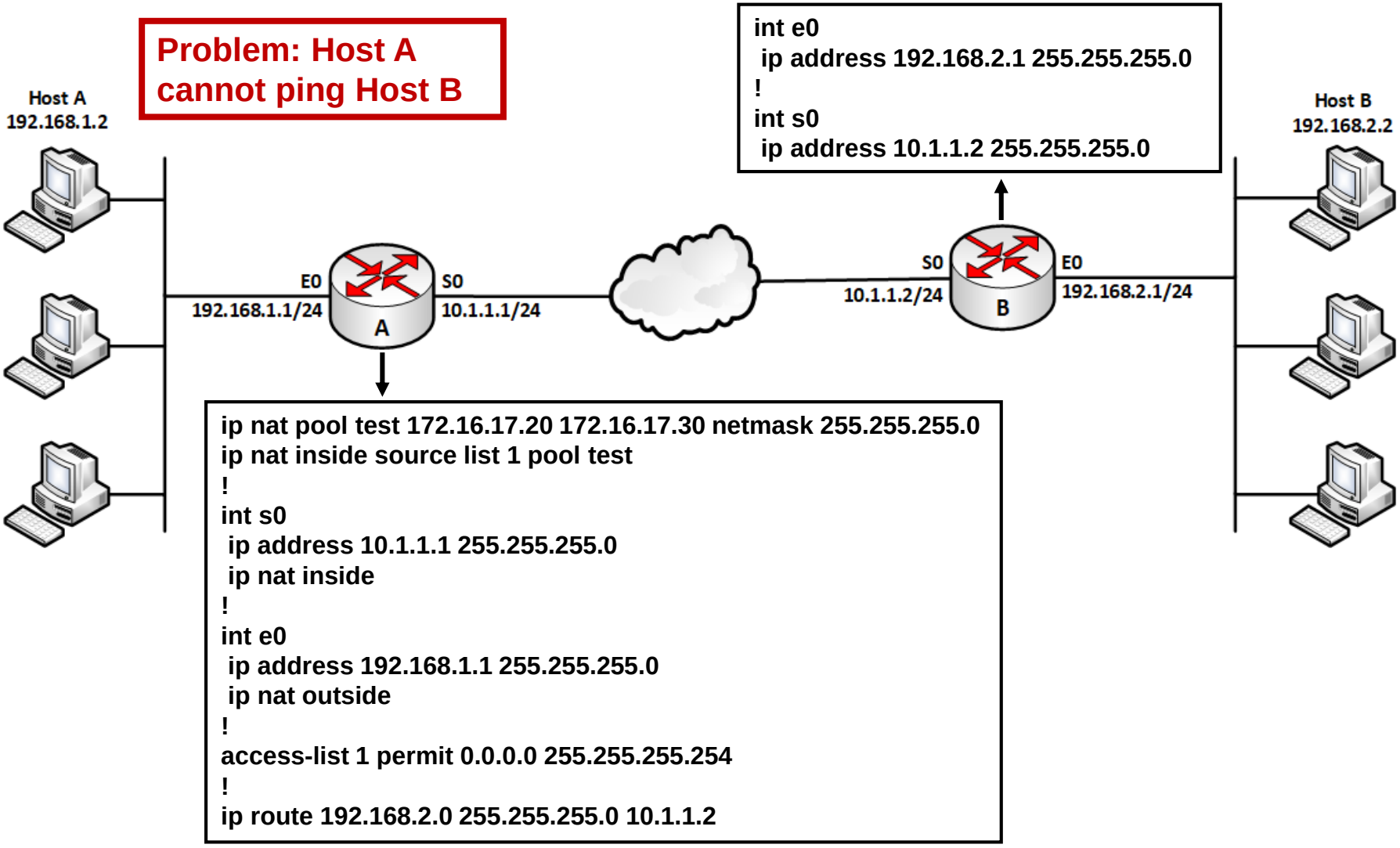
```
RouterX# show ip nat statistics
    Total active translations: 1 (1 static, 0 dynamic; 0 extended)
    Outside interfaces:
    Ethernet0, Serial2
    Inside interfaces:
    Ethernet1
    Hits: 5  Misses: 0
    …
```

Translation Occurring: Installed Translation Entry Not Being Used

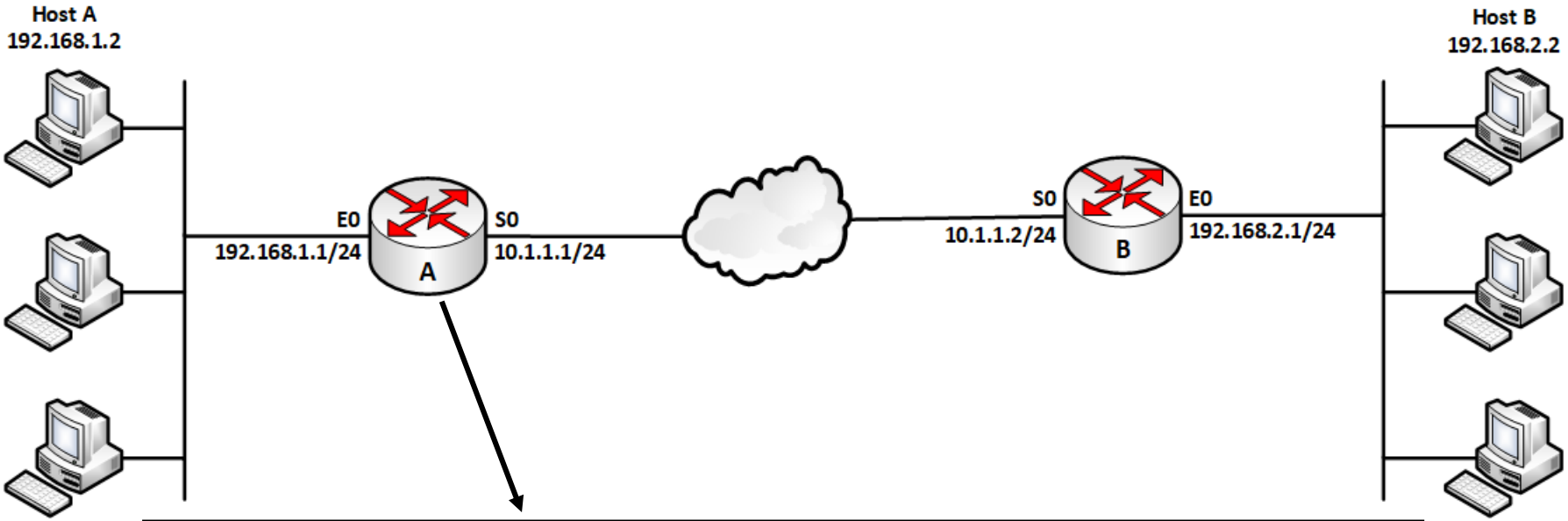
Verify:

- What the NAT configuration is supposed to accomplish
- That the NAT entry exists in the translation table and that it is accurate
- That the translation is actually taking place by monitoring the NAT process or statistics
- That the NAT router has the appropriate route in the routing table if the packet is going from inside to outside
- That all necessary routers have a return route back to the translated address

Sample Problem: Cannot Ping Remote Host



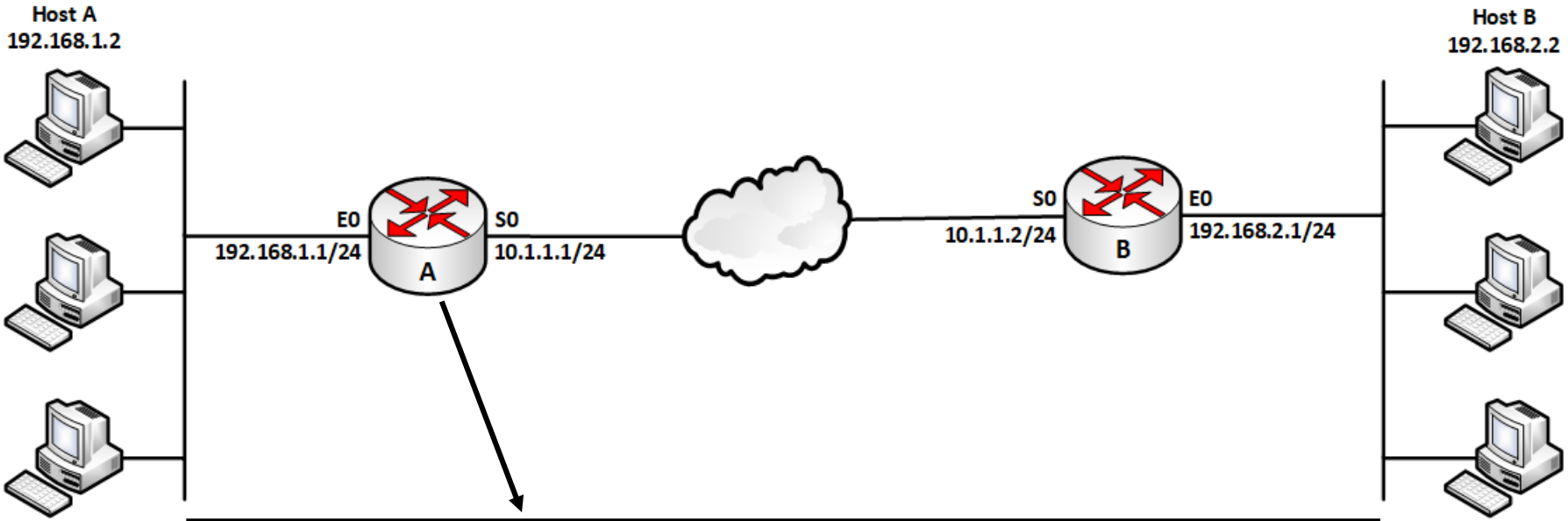
Sample Problem: Cannot Ping Remote Host (Cont.)




```
RouterA# show ip nat translations
    Pro Inside global     Inside local       Outside local      Outside global
    ---                   ---                ---
    ---                   ---                ---
```

There are no translations in the table.

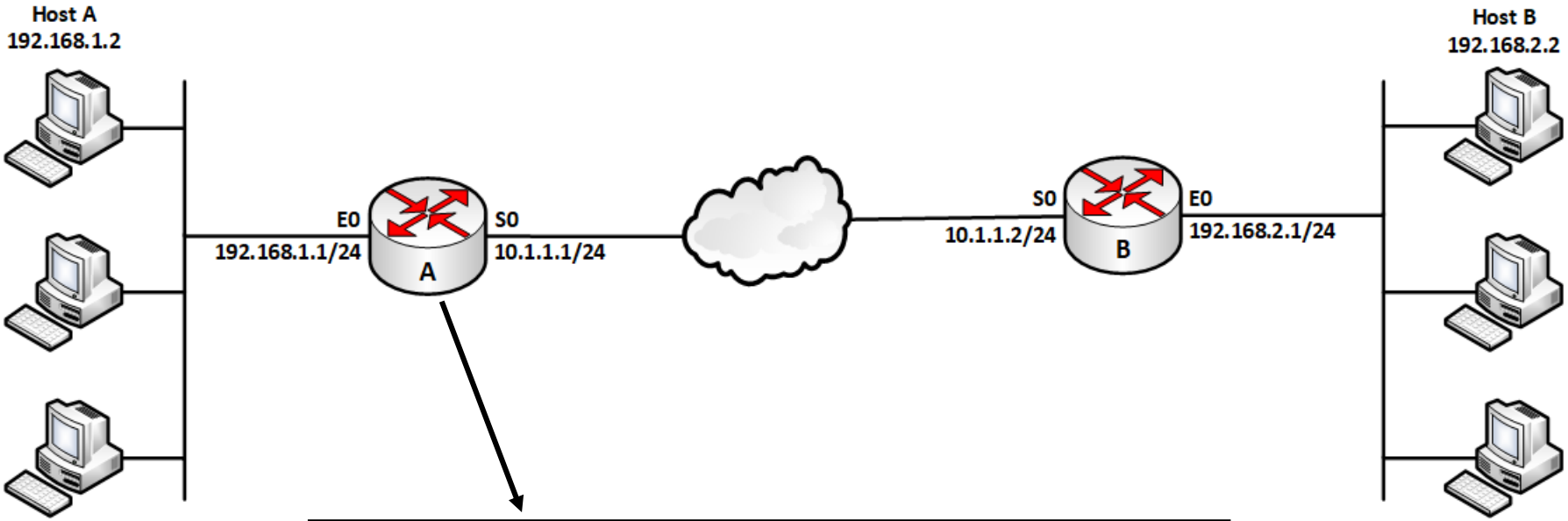
Sample Problem: Cannot Ping Remote Host (Cont.)




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

The router interfaces are inappropriately defined as NAT inside and NAT outside.

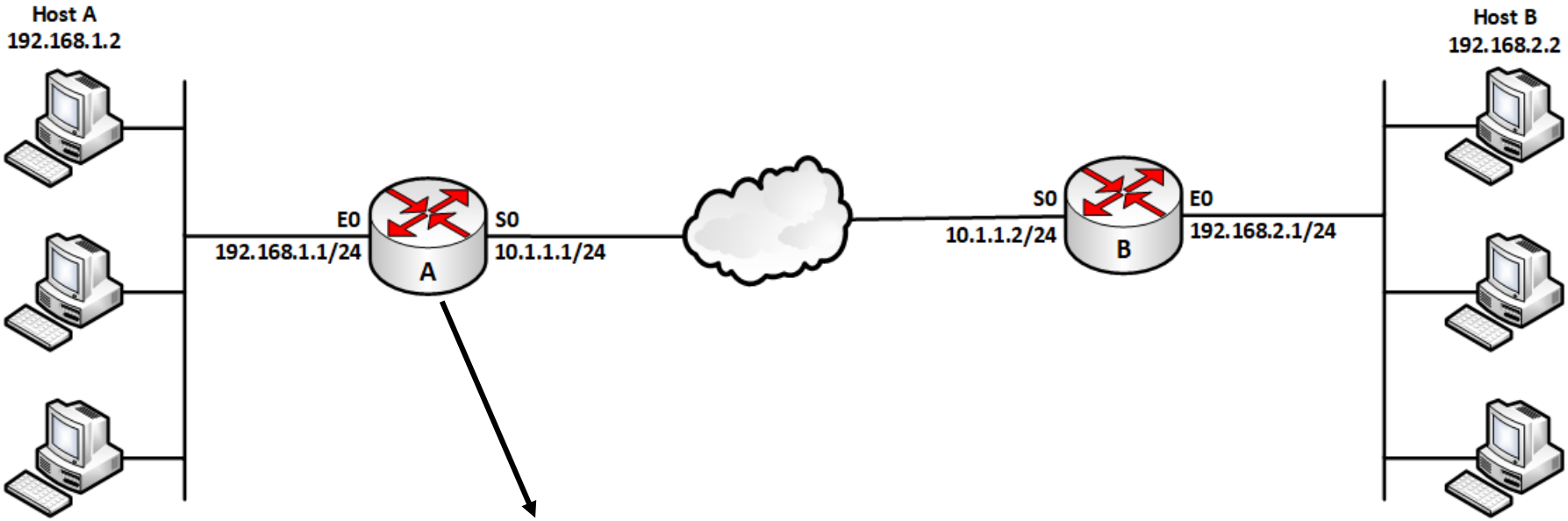
Sample Problem: Cannot Ping Remote Host (Cont.)




```
RouterA# show access-list
Standard IP access list 1
    10 permit 0.0.0.0, wildcard bits 255.255.255.254
```

- Pings are still failing and there are still no translations in the table.
- There is an incorrect wildcard bit mask in the ACL that defines the addresses to be translated.

Sample Problem: Cannot Ping Remote Host (Cont.)

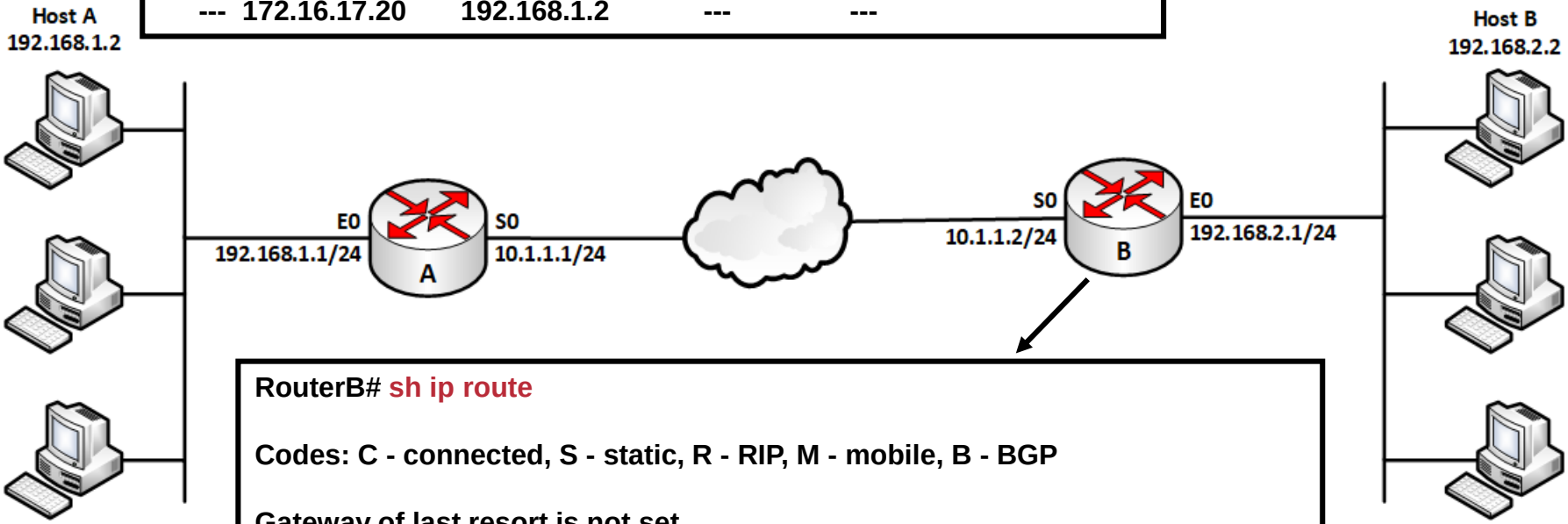



```
RouterA# show ip nat translations
    Pro Inside global     Inside local       Outside local      Outside global
    ---  172.16.17.20     192.168.1.2        ---                ---
```

- Translations are now occurring.
- Pings are still failing.

Sample Problem: Cannot Ping Remote Host (Cont.)

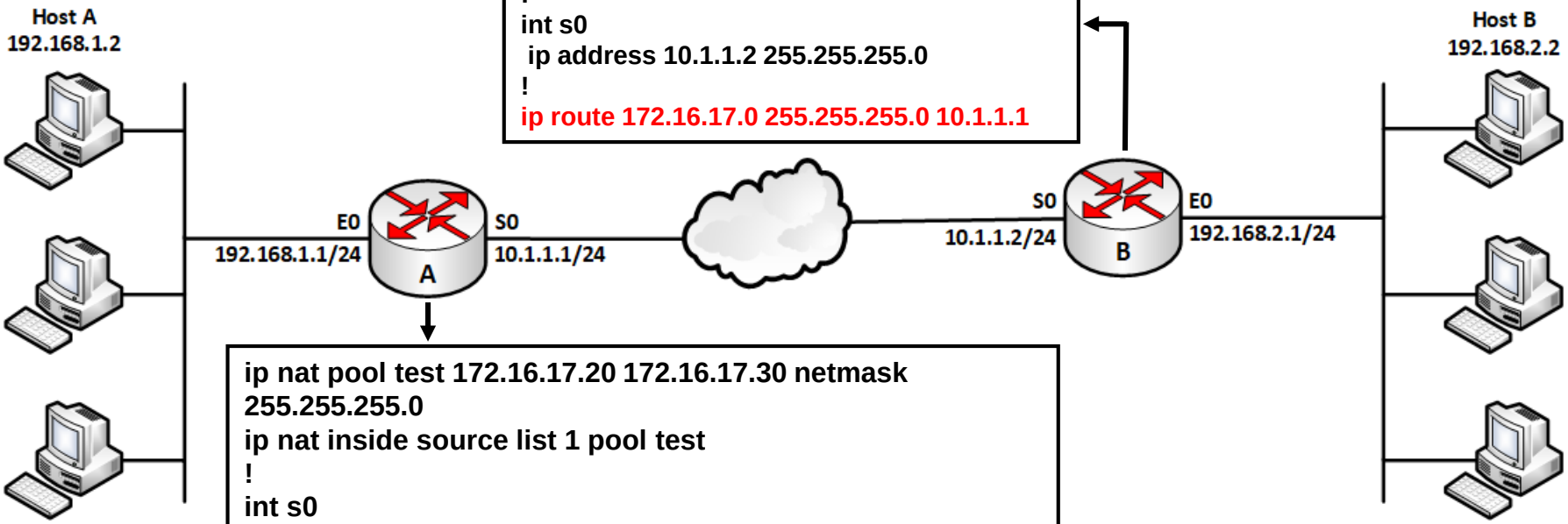
```
RouterA# show ip nat translations
    Pro Inside global     Inside local       Outside local      Outside global
    ---  172.16.17.20     192.168.1.2        ---                ---
```




```
RouterB# sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

Gateway of last resort is not set

    10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0/24 is directly connected, Serial0
   192.168.2.0/24 is subnetted, 1 subnets
C       192.168.2.0/24 is directly connected, Ethernet0
```

Router B has no route to the translated network address of 172.16.17.0/24

Solution: Corrected Configuration




```
int e0
 ip address 192.168.2.1 255.255.255.0
!
int s0
 ip address 10.1.1.2 255.255.255.0
!
ip route 172.16.17.0 255.255.255.0 10.1.1.1
```

```
ip nat pool test 172.16.17.20 172.16.17.30 netmask
255.255.255.0
ip nat inside source list 1 pool test
!
int s0
 ip address 10.1.1.1 255.255.255.0
 ip nat outside
!
int e0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
!
access-list 1 permit 0.0.0.0 255.255.255.255
!
ip route 192.168.2.0 255.255.255.0 10.1.1.2
```


CISCO