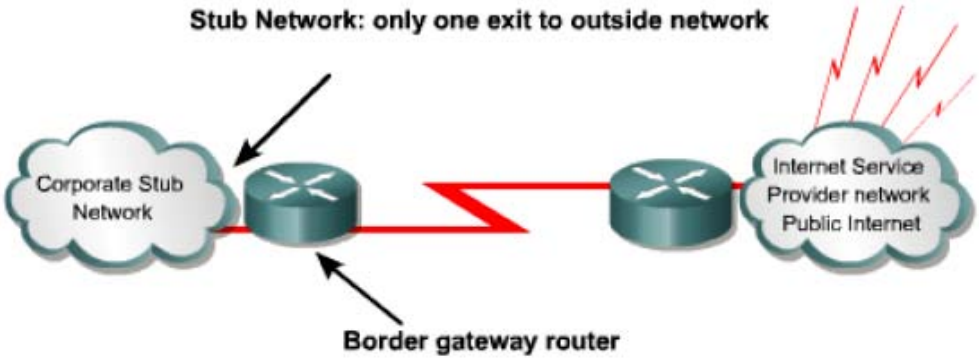
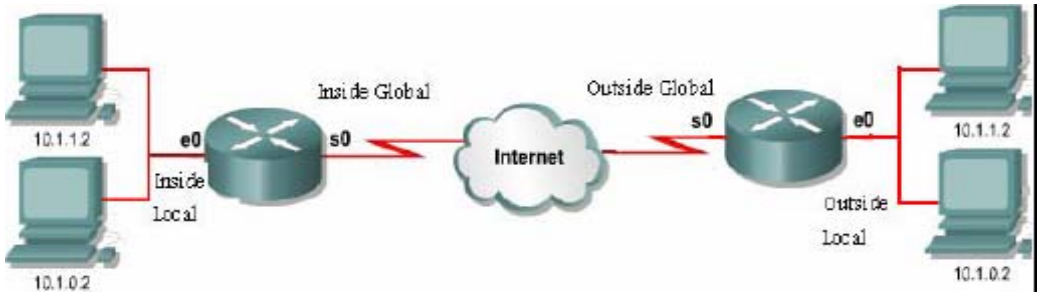
Eng. Mohammed Alani
http://www.certificationist.com

NAT (Network Address Translation) & PAT (Port Address Translation)



First let's define NAT terms:

- **Inside local address** – The IP address assigned to a host on the inside network. The address is usually not an IP address assigned by the Internet Network Information Center (InterNIC) or service provider. This address is likely to be an RFC 1918 private address.
- **Inside global address** – A legitimate IP address assigned by the InterNIC or service provider that represents one or more inside local IP addresses to the outside world.
- **Outside local address** – The IP address of an outside host as it is known to the hosts on the inside network.
- **Outside global address** – The IP address assigned to a host on the outside network. The owner of the host assigns this address.



Now let's remember the ranges of private addresses:

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 and PAT main features:

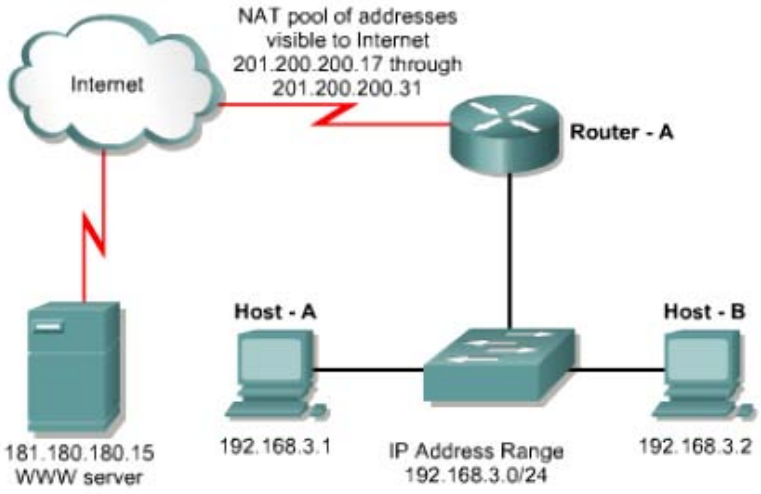
NAT translations can be used for a variety of purposes and can be either dynamically or statically assigned. Static NAT is designed to allow one-to-one mapping of local and global addresses. This is particularly useful for hosts which must have a consistent address that is accessible from the Internet. These internal hosts may be enterprise servers or networking devices.

Dynamic NAT is designed to map a private IP address to a public address. Any IP address from a pool of public IP addresses is assigned to a network host. Overloading, or Port Address Translation (PAT), maps multiple private IP addresses to a single public IP address. Multiple addresses can be mapped to a single address because each private address is tracked by a port number.

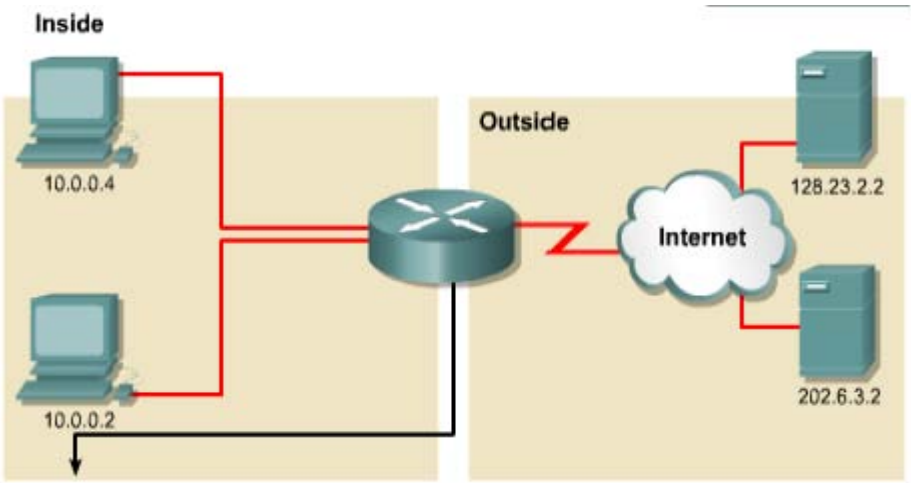
PAT uses unique source port numbers on the inside global IP address to distinguish between translations. The port number is encoded in 16 bits. The total number of internal addresses that can be translated to one external address could theoretically be as high as 65,536 per IP address. Realistically, the number of ports that can be assigned a single IP address is around 4000. PAT will attempt to preserve the original source port. If this source port is already used, PAT will assign the first available port number starting from the beginning of the appropriate port group 0-511, 512-1023, or 1024-65535. When there are no more ports available and there is more than one external IP address configured, PAT moves to the next IP address to try to allocate the original source port again. This process continues until it runs out of available ports and external IP addresses.

Note: Cisco IOS NAT does NOT support the following traffic types:

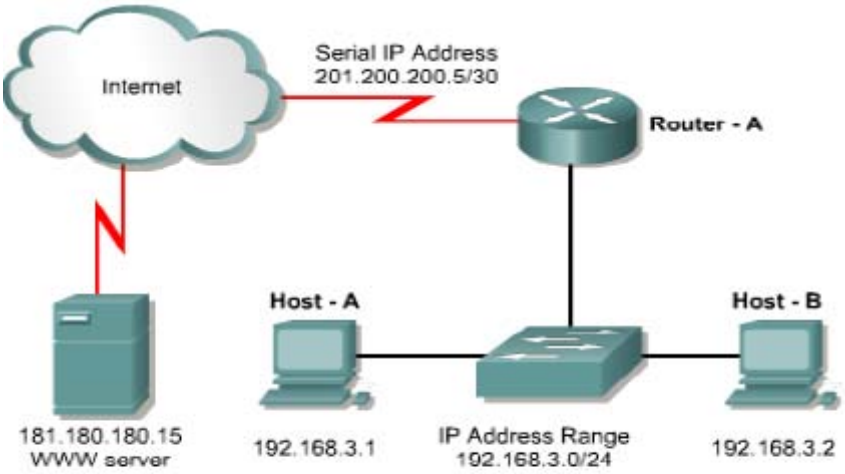
Routing table updates, DNS zone transfers, BOOTP, Talk and ntalk protocols, and SNMP.



Inside Local IP ADDRESS	Inside Global IP ADDRESS	Outside Global IP ADDRESS
192.168.3.1	201.200.200.17	181.180.180.15
192.168.3.2	201.200.200.18	181.180.180.15



NAT Table with Overload			
Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global Address
10.0.0.2:1331 10.0.0.4:1555	179.9.8.80:1331 179.9.8.80:1555	202.6.3.2:80 128.23.2.2:80	202.6.3.2:80 128.23.2.2:80



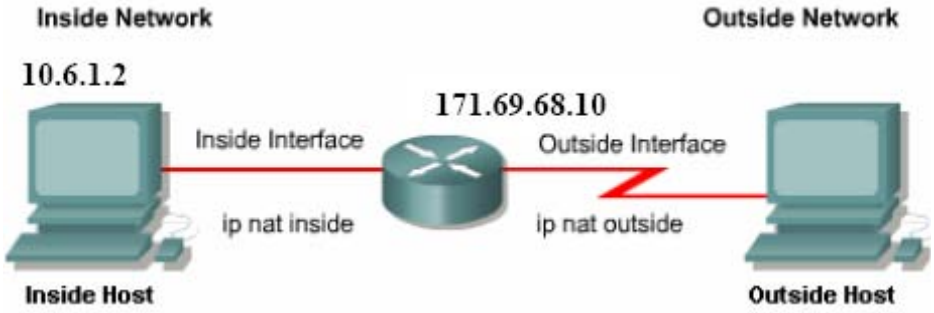
Inside Local IP ADDRESS:Port	Inside Global IP ADDRESS:Port	Outside Global IP ADDRESS:Port
192.168.3.1:1125	201.200.200.5:1125	181.180.180.15:80
192.168.3.2:1126	201.200.200.5:1126	181.180.180.15:80

Configuring NAT and PAT

Static Translation: configure a static NAT between the private IP 10.6.1.2 & the public 171.69.68.10
Configuration steps:
1. Establish static translation between an inside local add. & an inside global add.
Router(config)#ip nat inside source static <inside local add.> < inside global add.>
2. Specify the inside interface.

Router(config)#int <type & no.>
Router(config-if)#ip nat inside
3. Specify the outside interface
Router(config)#int <type & no.>
Router(config-if)#ip nat outside

An example is the following:



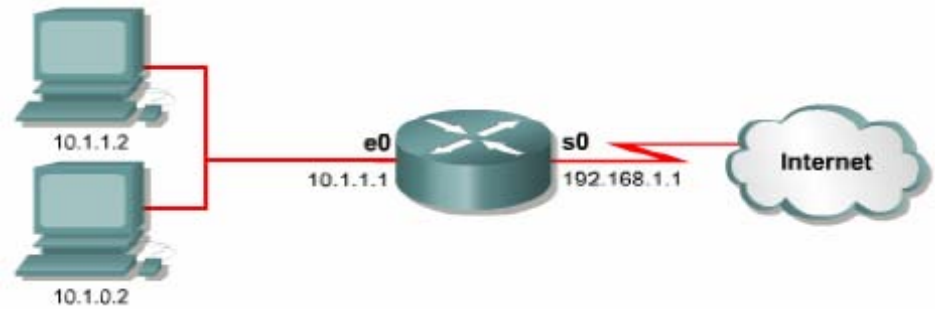
Router(config)#ip nat inside source static 10.6.1.2 171.69.68.10
Router(config)#int e0
Router(config-if)#ip nat inside
Router(config-if)#int s0
Router(config-if)#ip nat outside

Dynamic Translation:

To configure dynamic inside source address translation an access list must permit only those addresses that are to be translated. Remember that there is an implicit "deny all" at the end of each access list. An access list that is too permissive can lead to unpredictable results. Cisco advises against configuring access lists referenced by NAT commands with the **permit any** command. Using **permit any** can result in NAT consuming too many router resources, which can cause network problems.

Configuration steps:

1. Define a pool of global addresses to be allocated as needed
   Router(config)#ip nat pool <name> <start-IP> <end-IP> netmask <netmask>
2. Define the Access list
   Router(config)#access-list <number> permit <IPs> <wildcard>
3. Establish dynamic source translation, specifying the access list defined in the prior step.
   Router(config)#ip nat inside sourse list <ACL number> pool <name>
4. Specify the inside interface.
   Router(config)#int <type & no.>
   Router(config-if)#ip nat inside
5. Specify the outside interface
   Router(config)#int <type & no.>
   Router(config-if)#ip nat outside



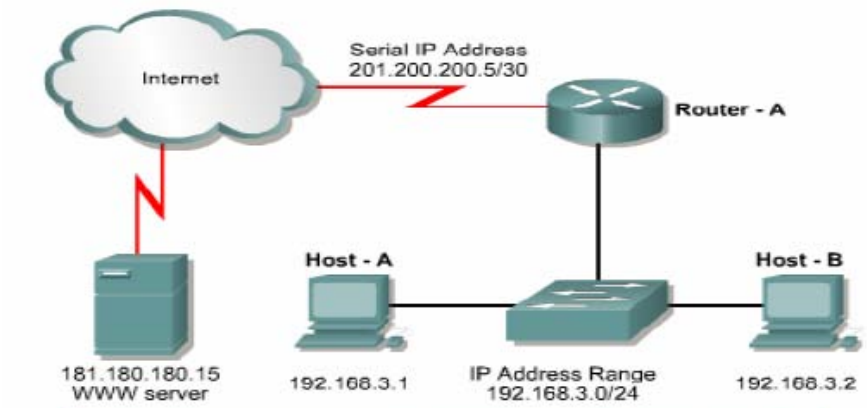
Note: NAT will not translate any host that is not permitted for translation by the access list.

Overloading:

Overloading is configured in two ways depending on how many public IP addresses have been allocated. An ISP can allocate a network only one public IP address, and this is typically assigned to the outside interface which connects to the ISP.

Configuration steps:

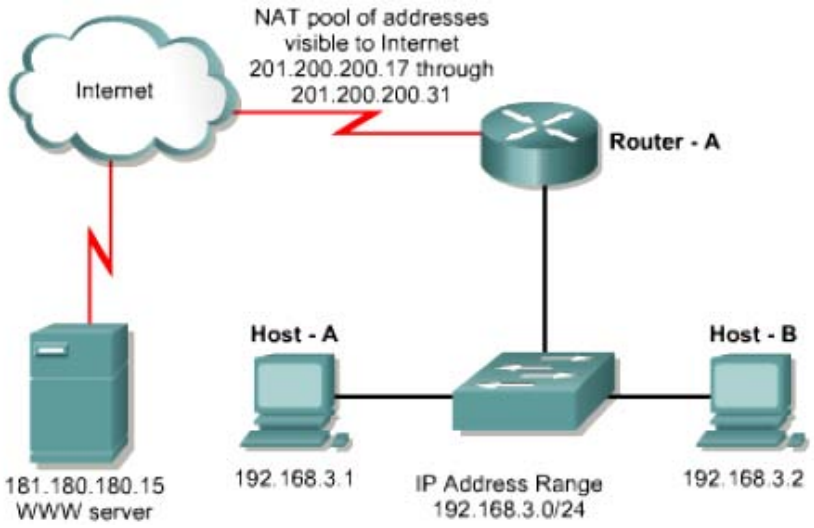
1. Define a standard Access list
   Router(config)#access-list <number> permit <IPs> <wildcard>
2. Establish dynamic source translation, specifying the access list defined in the prior step.
   Router(config)#ip nat inside sourse list <ACL number> interface <type & no> overload
3. Specify the inside interface.
   Router(config)#int <type & no.>
   Router(config-if)#ip nat inside
4. Specify the outside interface
   Router(config)#int <type & no.>
   Router(config-if)#ip nat outside



Inside Local IP ADDRESS:Port	Inside Global IP ADDRESS:Port	Outside Global IP ADDRESS:Port
192.168.3.1:1125	201.200.200.5:1125	181.180.180.15:80
192.168.3.2:1126	201.200.200.5:1126	181.180.180.15:80

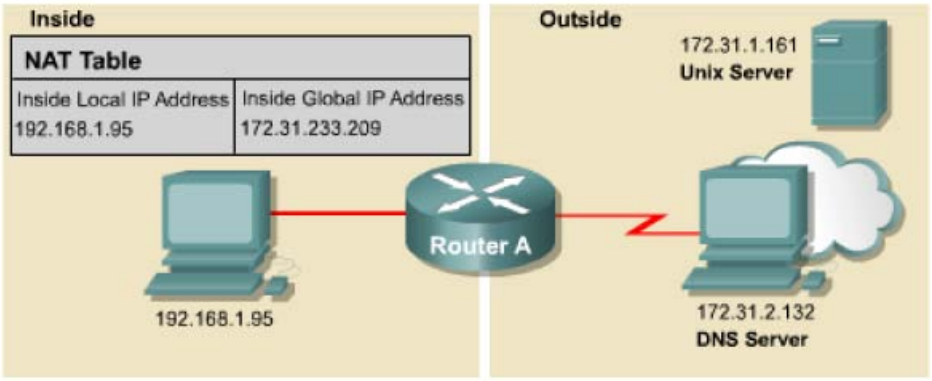
Another way of configuring overload is if the ISP has given one or more public IP addresses for use as a NAT pool. This pool can be overloaded.

1. Define a standard Access list
   Router(config)#access-list <number> permit <IPs> <wildcard>
2. Spacify the global address as a pool to be used for overloading.
   Router(config)#ip nat pool <name> <start-IP> <end-IP> netmask <netmask>
3. Establish overload translation.
   Router(config)#ip nat inside sourse list <ACL number> pool <name> overload
4. Specify the inside interface.
   Router(config)#int <type & no.>
   Router(config-if)#ip nat inside
5. Specify the outside interface
   Router(config)#int <type & no.>
   Router(config-if)#ip nat outside



Troubleshooting NAT and PAT configuration:

- **Router#**show ip nat translation
- **Router#**show ip nat statistics
- **Router#**show run
- **Router#**debug ip nat
- **Router#**debug ip nat detailed




```
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]
```

How to Change the Dynamic NAT Configuration:

Sometimes you receive these messages when you change the Network Address Translation (NAT) configuration:

- Dynamic mapping in use, cannot remove
- %Pool out pool in use, cannot destroy

The following will demonstrate how to change the NAT configuration if you receive these messages on the console.

Dynamic NAT creates active translation entries in a table when a packet crosses from an IP NAT inside interface to an IP NAT outside interface, or vice versa. This dynamic NAT entry can be seen using the **show ip nat translation** command. Cisco IOS® software checks for any existing active NAT translations in the translations table when either of the following existing dynamic NAT configurations is removed:

- no ip nat pool name
- no ip nat {inside | outside}source {list {access−list−number | name} pool name [overload] | static local−ip global−ip}

If a translation entry matches, then the %Dynamic Mapping in Use, Cannot remove message or the %Pool out pool in use, cannot destroy message are respectively echoed on the console.

The reason you receive these error messages is because you are trying to change part of a NAT configuration that is responsible for creating dynamic translations that still exist in the translation table. In order to change the NAT configuration in this situation, you need to clear the table of translations that are being used before the change is accepted.

Sometimes this is not easy because the router configured with NAT may be continuously receiving packets that create translations in the table; this can happen so quickly that you don't have time to change the configuration.

Using the clear ip nat translation Command:

This solution involves clearing the IP NAT translations using the **clear ip nat translation** command, and then replacing the NAT configuration quickly, before any new NAT entries are populated into the translation table due to active NAT traffic. To do this, create a script with the configuration commands written in a text format. For example:

Router#clear ip nat translation *
Router(config)#config terminal
Router(config)#no ip nat pool old pool name
Router(config)#ip nat pool new pool …….

Once you have the script, cut and paste the script into the router enable mode (Router#).

Note: This may take more than one try since it is still possible that the router will create a translation after the translation has been cleared.

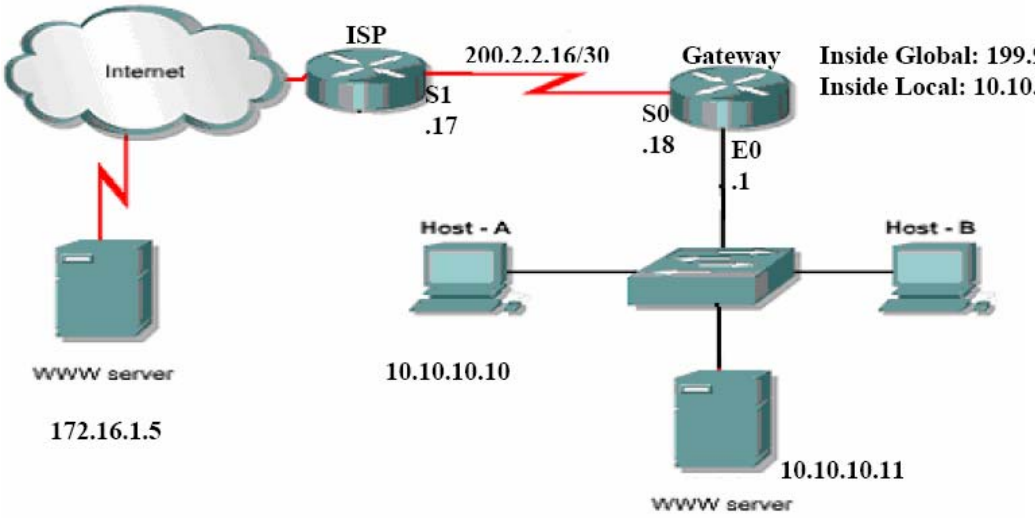
Disabling NAT on the Router:

This solution involves disabling NAT on the router so that it cannot create any more NAT translations. Do this by removing the **ip nat inside** or **ip nat outside** commands on the interfaces. Then clear the translation table and change the configuration.

Follow these steps to use this solution:

- Use the **no ip nat {inside | outside}** command to disable future translations from taking place.
- Use the **clear ip nat translation** command to clear IP NAT translations.
- Change the NAT configuration.
- Restore the NAT {inside | outside} arguments with the ip nat {inside | outside} configuration command.

An Example



The ISP will give the company the public IP range (199.99.9.33…..39/27) for static allocation. & the range (199.99.9.40……62/27) for dynamic allocation.

*Configure each router with basic configuration.

ISP(config)# ip route 199.99.9.32 255.255.255.224 200.2.2.18
ISP(config)#int loopback 1
ISP(config-if)#ip address 172.16.1.5 255.255.255.255
Gateway(config)# ip route 0.0.0.0 0.0.0.0 200.2.2.17
Gateway(config)#ip nat pool *public_access* 199.99.9.40 199.99.9.62 netmask 255.255.255.224 **S.M. could be 255.255.255.255 just as taken from ISP*
Gateway(config)#access-list 1 permit 10.10.10.0 0.0.0.255
Gateway(config)#ip nat inside source list 1 pool *public_access* **overload** [PAT]
Gateway(config)#int e0
Gateway(config-if)#ip nat inside
Gateway(config)#int s0
Gateway(config-if)#ip nat outside

From host A: ping 172.16.1.5 Reply
From host B: ping 172.16.1.5 Reply

Gateway#sh ip nat translation
Gateway#sh ip nat statistic
Gateway#sh run
Gateway#debug ip nat

For static NAT: **Gateway(config)#**ip nat inside source static 10.10.10.11 199.99.9.33

From ISP: ping 10.10.10.11 Request timed out
From ISP: ping 199.99.9.33 Reply
From ISP: ping 199.99.9.40 Request timed out

Notes:

1. Suppose you have only 1 public IP which is the address of interface S0:

Gateway(config)#access-list 1 permit 10.10.10.0 0.0.0.255
Gateway(config)#ip nat inside source list 1 interface s0 overload
Gateway(config)#int e0
Gateway(config-if)#ip nat inside
Gateway(config)#int s0
Gateway(config-if)#ip nat outside

2. Suppose that you have 1 registered IP (199.99.9.33) & you need to configure it with PAT:

Gateway(config)#ip nat pool *public_access* 199.99.9.33 199.99.9.33 netmask 255.255.255.252
**S.M. could be 255.255.255.255 just as taken from ISP*
Gateway(config)#access-list 1 permit 10.10.10.0 0.0.0.255
Gateway(config)#ip nat inside source list 1 pool *public_access* overload
Gateway(config)#int e0
Gateway(config-if)#ip nat inside
Gateway(config)#int s0
Gateway(config-if)#ip nat outside