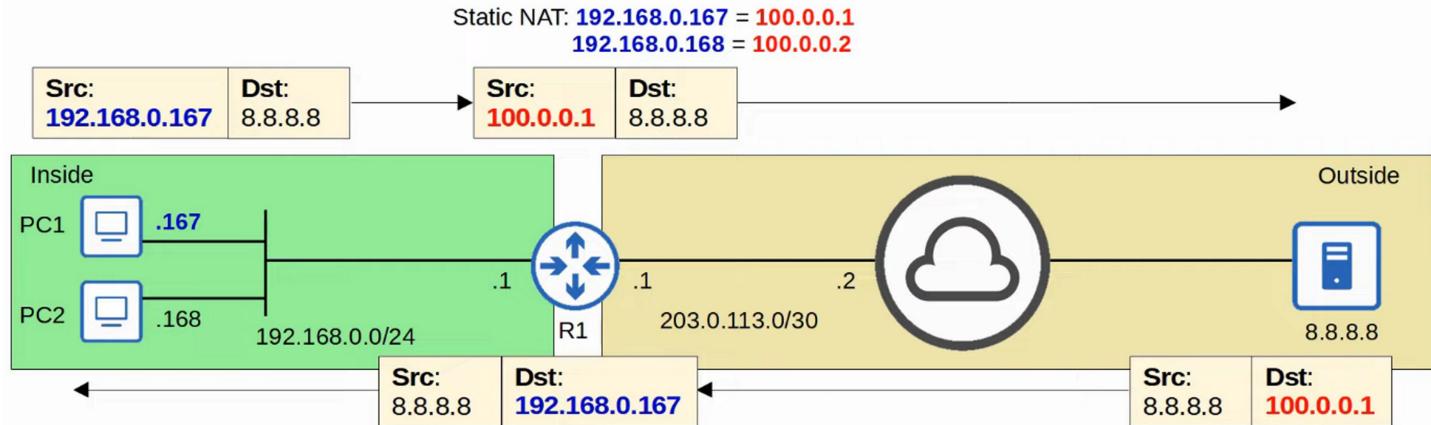


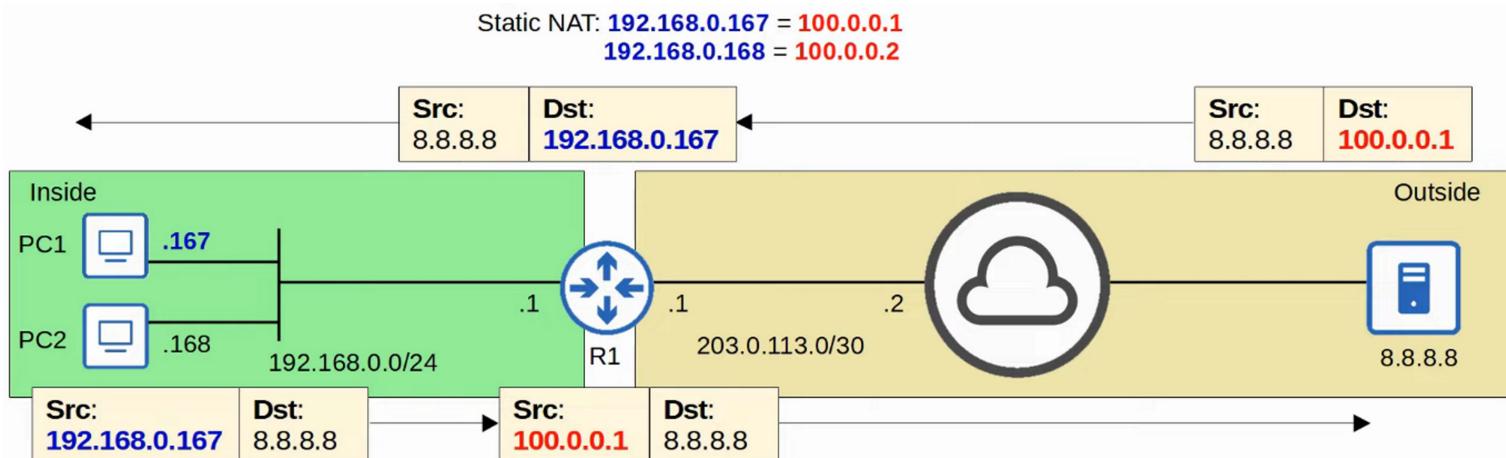
NAT (DYNAMIC): PART 2

MORE ABOUT STATIC NAT

- STATIC NAT involves statically configuring one-to-one mappings of PRIVATE IP ADDRESSES to PUBLIC IP ADDRESSES
- When traffic from the INTERNAL HOST is sent to the OUTSIDE NETWORK, the ROUTER will translate the SOURCE ADDRESS



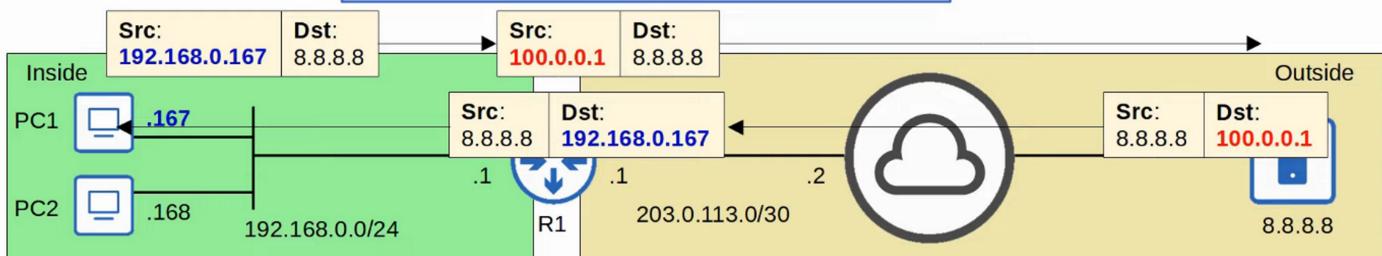
- HOWEVER, this one-to-one mapping also allows EXTERNAL HOSTS to access the INTERNAL HOST via INSIDE GLOBAL ADDRESS



DYNAMIC NAT

- In DYNAMIC NAT, the ROUTER dynamically maps INSIDE LOCAL ADDRESSES to INSIDE GLOBAL ADDRESSES, as needed
- An ACL is used to identify WHICH traffic should be translated
 - If the SOURCE IP is PERMITTED; the SOURCE IP will be translated
 - If the SOURCE IP is DENIED; the SOURCE IP will NOT be translated
 - 💡 However, Packet Traffic will NOT be dropped
- A NAT POOL is used to define the available INSIDE GLOBAL ADDRESS

On R1:
ACL 1: permit 192.168.0.0/24
 deny any
POOL1: 100.0.0.1 to 100.0.0.10
 If a packet with a source IP permitted by **ACL 1** arrives,
 translate the source IP to an address from **POOL1**.



- Although they are dynamically assigned, the mappings are still one-to-one (one INSIDE LOCAL IP ADDRESS per INSIDE GLOBAL IP ADDRESS)
 - If there are NOT enough INSIDE GLOBAL IP ADDRESSES available (=ALL are being used), it is called 'NAT POOL EXHAUSTION'
 - If a PACKET from another INSIDE HOST arrives and needs NAT but there are no AVAILABLE ADDRESSES, the ROUTER will drop the PACKET
 - The HOST will be unable to access OUTSIDE NETWORKS until one of the INSIDE GLOBAL IP ADDRESSES becomes available
 - DYNAMIC NAT entries will time out automatically if not used, or you can clear them manually
- NAT POOL EXHAUSTION

NAT Pool Exhaustion	
Source IP	Translated Source IP
192.168.0.167	100.0.0.1
192.168.0.168	100.0.0.2
192.168.0.100	100.0.0.3
192.168.0.12	100.0.0.4
192.168.0.28	100.0.0.5
192.168.0.56	100.0.0.6
192.168.0.202	100.0.0.7
192.168.0.221	100.0.0.8
192.168.0.116	100.0.0.9
192.168.0.188	100.0.0.10
192.168.0.98	No address available! Router will drop the packet

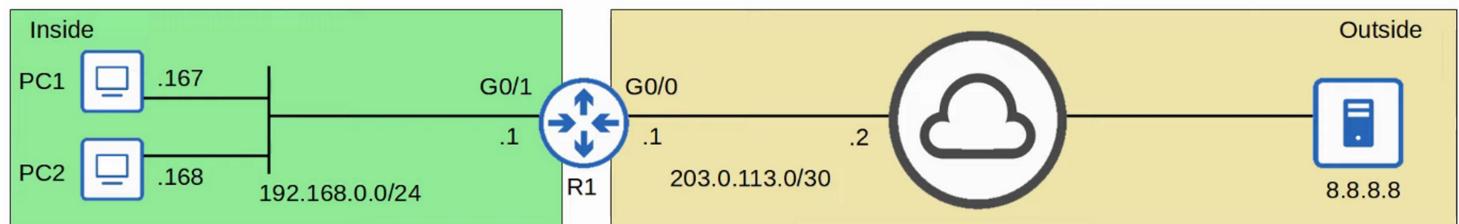
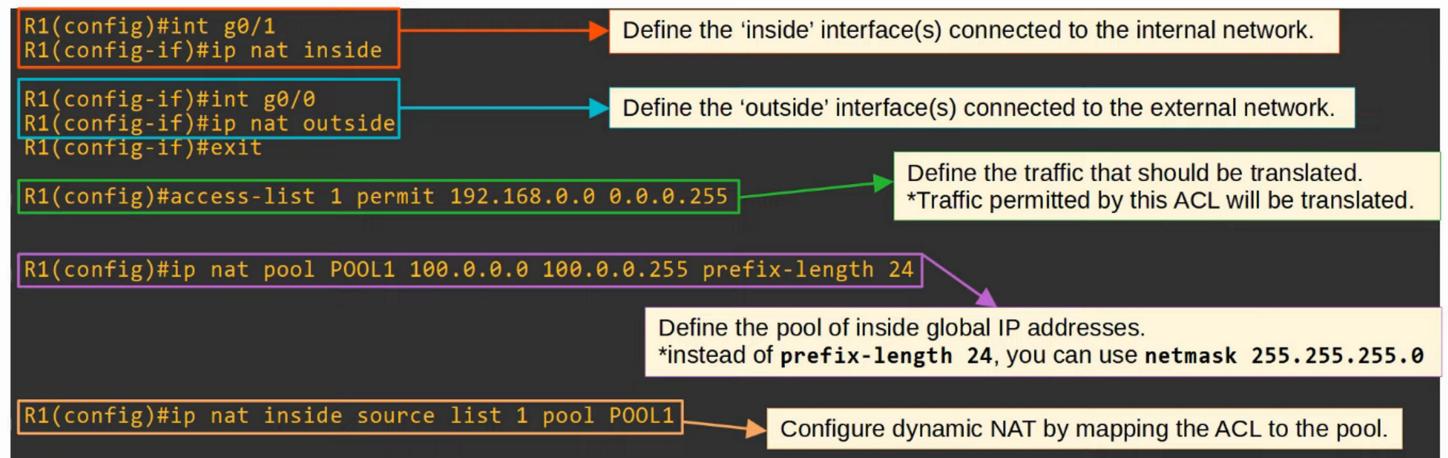
192.168.0.167 TIMES OUT and 192.168.0.98 is assigned it's TRANSLATED SOURCE IP

NAT Pool Exhaustion	
Source IP	Translated Source IP
192.168.0.168	100.0.0.2
192.168.0.100	100.0.0.3
192.168.0.12	100.0.0.4
192.168.0.28	100.0.0.5
192.168.0.56	100.0.0.6
192.168.0.202	100.0.0.7
192.168.0.221	100.0.0.8
192.168.0.116	100.0.0.9
192.168.0.188	100.0.0.10
192.168.0.98	100.0.0.1

DYNAMIC NAT CONFIGURATION



Dynamic NAT Configuration

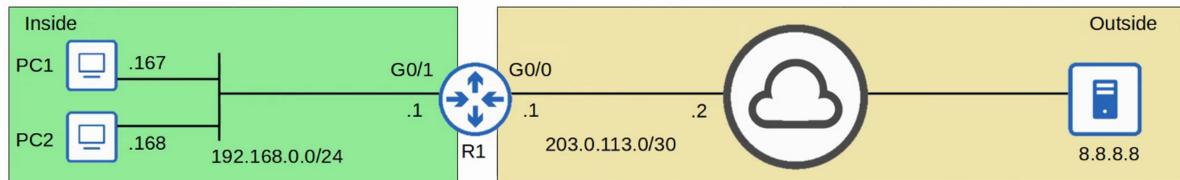


`show ip nat translations`



Dynamic NAT Configuration

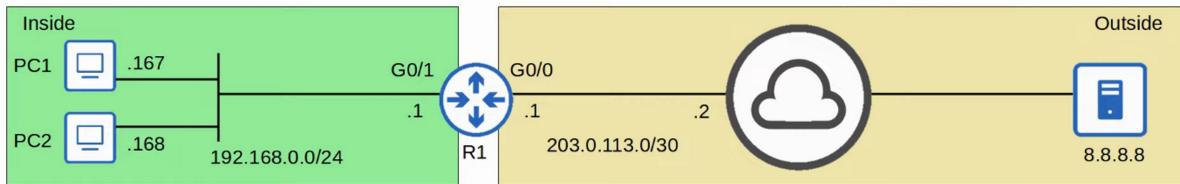
```
R1#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 100.0.0.1:3      192.168.0.167:3  8.8.8.8:3        8.8.8.8:3
udp 100.0.0.1:58685   192.168.0.167:58685 8.8.8.8:53      8.8.8.8:53
--- 100.0.0.1         192.168.0.167       ---           ---
icmp 100.0.0.2:3      192.168.0.168:3    8.8.8.8:3        8.8.8.8:3
udp 100.0.0.2:49536   192.168.0.168:49536 8.8.8.8:53      8.8.8.8:53
--- 100.0.0.2         192.168.0.168       ---           ---
```





Dynamic NAT Configuration

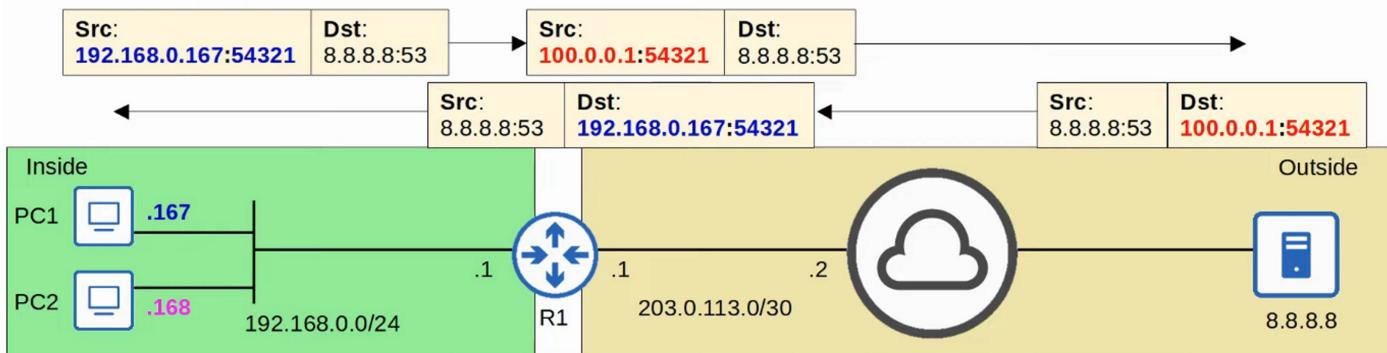
```
R1#show ip nat statistics
Total active translations: 6 (0 static, 6 dynamic; 4 extended)
Peak translations: 6, occurred 00:00:30 ago
Outside interfaces:
  GigabitEthernet0/0
Inside interfaces:
  GigabitEthernet0/1
Hits: 32 Misses: 0
CEF Translated packets: 20, CEF Punted packets: 12
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool POOL1 refcount 6
  pool POOL1: netmask 255.255.255.0
    start 100.0.0.0 end 100.0.0.255
    type generic, total addresses 256, allocated 2 (0%), misses 0
[output omitted]
```

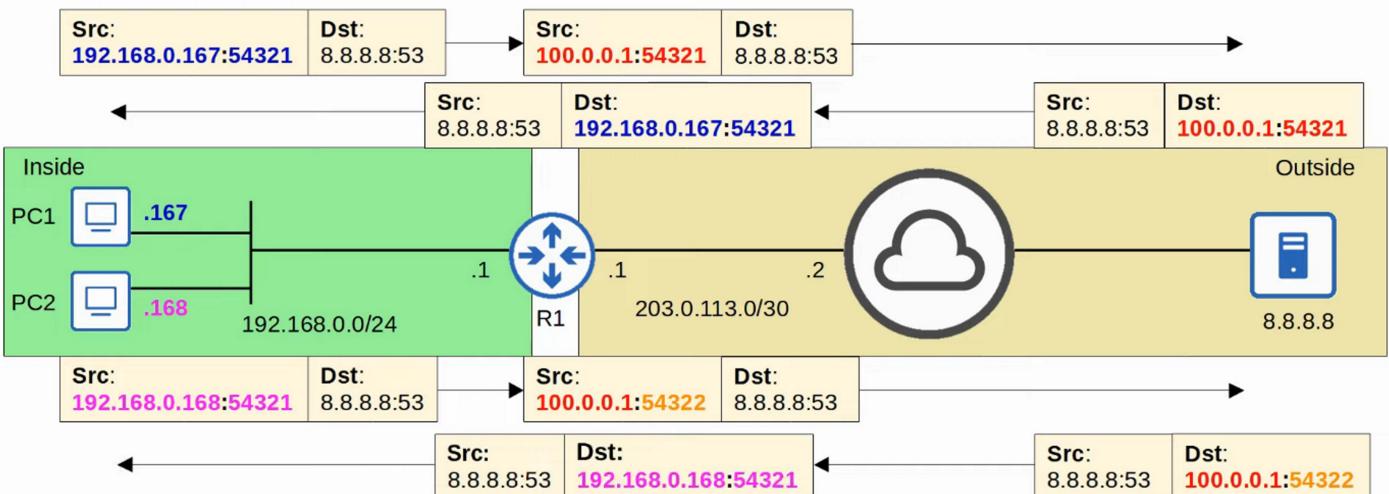


```
R1#show ip nat statistics
Total active translations: 6 (0 static, 6 dynamic; 4 extended)
Peak translations: 6, occurred 00:00:30 ago
Outside interfaces:
  GigabitEthernet0/0
Inside interfaces:
  GigabitEthernet0/1
Hits: 32 Misses: 0
CEF Translated packets: 20, CEF Punted packets: 12
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool POOL1 refcount 6
  pool POOL1: netmask 255.255.255.0
    start 100.0.0.0 end 100.0.0.255
    type generic, total addresses 256, allocated 2 (0%), misses 0
[output omitted]
```

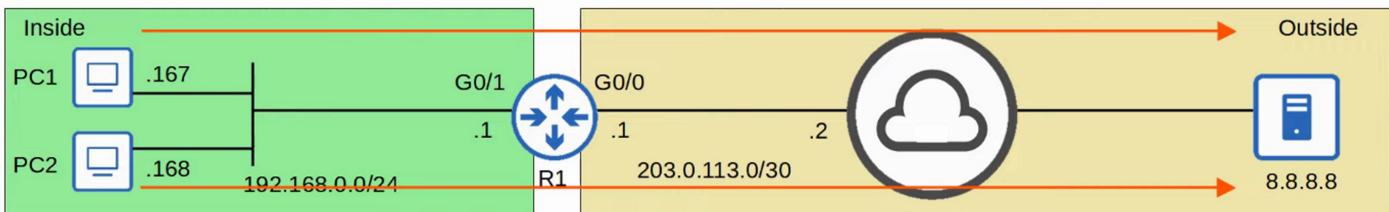
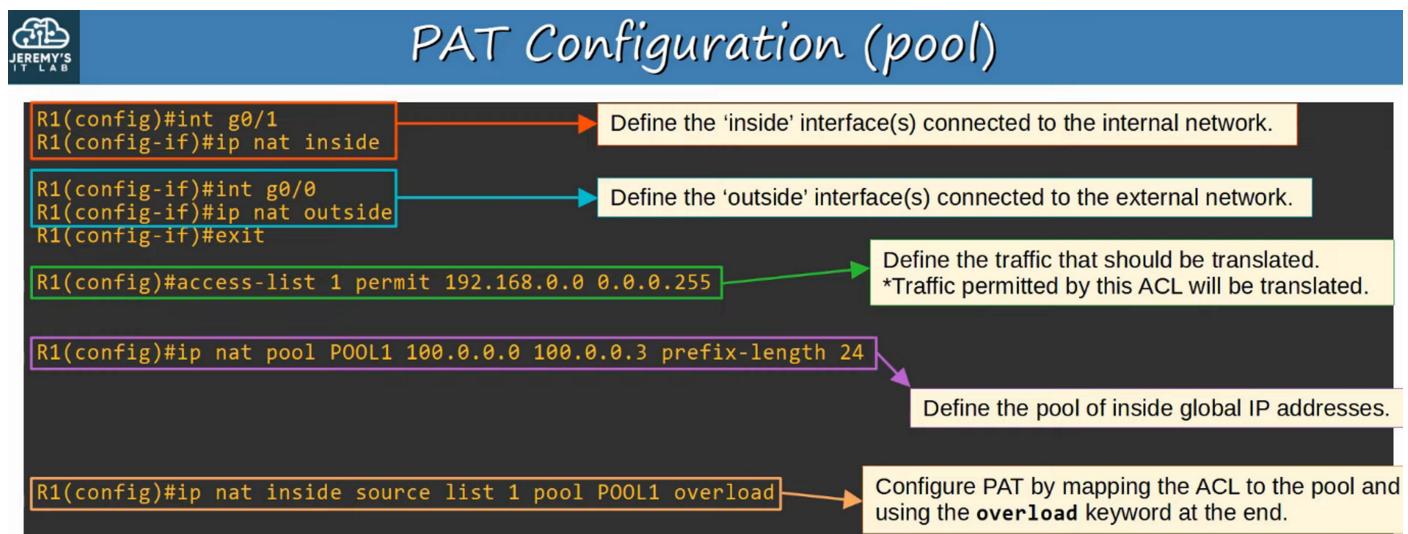
DYNAMIC PAT (NAT OVERLOAD)

- PAT (NAT OVERLOAD) translates BOTH the IP ADDRESS and the PORT NUMBER (if necessary)
- By using a unique PORT NUMBER for each communication flow, a single PUBLIC IP ADDRESS can be used by many different INTERNAL HOSTS
 - PORT NUMBERS are 16 bits = over 65,000 available port numbers
- The ROUTER will keep track of which INSIDE LOCAL ADDRESS is using which INSIDE GLOBAL ADDRESS and PORT





PAT CONFIGURATION (POOL)



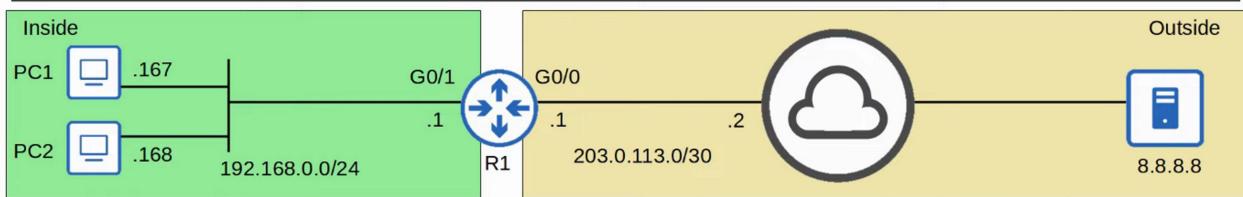
show ip nat translations



PAT Configuration (pool)

```
R1#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
  udp [100.0.0.1:63925] 192.168.0.167:63925 [8.8.8.8:53] 8.8.8.8:53
  udp [100.0.0.1:59549] 192.168.0.168:59549 [8.8.8.8:53] 8.8.8.8:53

R1#show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:00:03 ago
Outside interfaces:
  GigabitEthernet0/0
Inside interfaces:
  GigabitEthernet0/1
Hits: 4 Misses: 0
CEF Translated packets: 0, CEF Punted packets: 4
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool POOL1 refcount 2
  pool POOL1: netmask 255.255.255.0
    start 100.0.0.0 end 100.0.0.3
    type generic, total addresses 4, allocated 1 (25%), misses 0
```



PAT CONFIGURATION (INTERFACE)



PAT Configuration (interface)

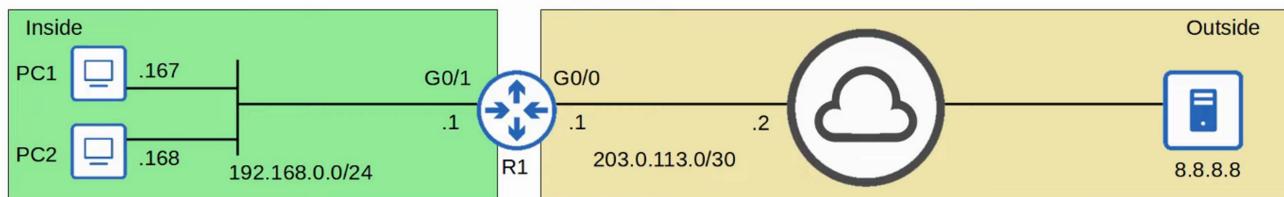
```
R1(config)#int g0/1
R1(config-if)#ip nat inside
R1(config-if)#int g0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#access-list 1 permit 192.168.0.0 0.0.0.255
R1(config)#ip nat inside source list 1 interface g0/0 overload
```

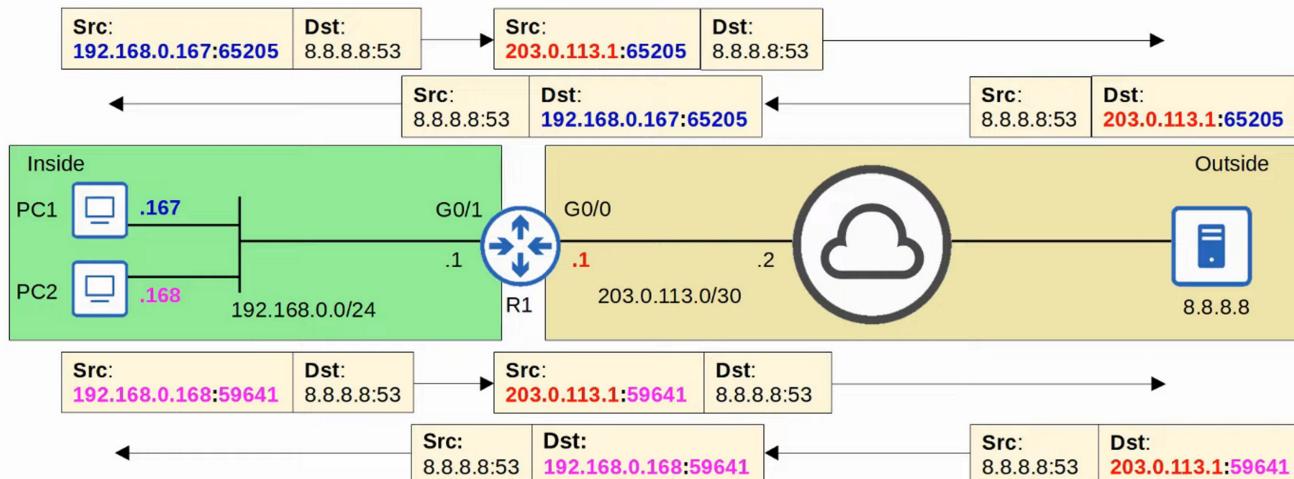
Define the 'inside' interface(s) connected to the internal network.

Define the 'outside' interface(s) connected to the external network.

Define the traffic that should be translated.
*Traffic permitted by this ACL will be translated.

Configure PAT by mapping the ACL to the interface and enabling **overload**.





```
R1#show ip nat translations
Pro Inside global           Inside local        Outside local      Outside global
  udp 203.0.113.1:65205   192.168.0.167:65205 8.8.8.8:53       8.8.8.8:53
  udp 203.0.113.1:59641   192.168.0.168:59641 8.8.8.8:53       8.8.8.8:53
R1#show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:36:30 ago
Outside interfaces:
  GigabitEthernet0/0
Inside interfaces:
  GigabitEthernet0/1
Hits: 12 Misses: 0
CEF Translated packets: 0, CEF Punted packets: 12
Expired translations: 4
Dynamic mappings:
-- Inside Source
[Id: 4] access-list 1 interface GigabitEthernet0/0 refcount 2
```

COMMAND REVIEW



Command Review

```
R1(config)# ip nat pool pool-name start-ip end-ip prefix-length prefix-length
R1(config)# ip nat pool pool-name start-ip end-ip netmask subnet-mask
R1(config)# ip nat inside source list access-list pool pool-name
R1(config)# ip nat inside source list access-list pool pool-name overload
R1(config)# ip nat inside source list access-list interface interface overload
```