JEREMY'S IT LAB

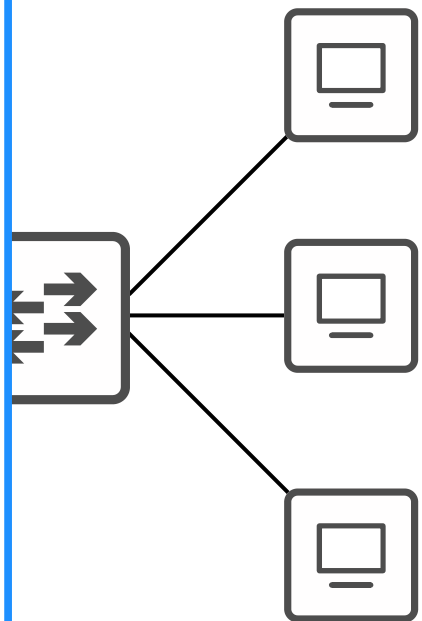
CCNA Day 45

Network Address Translation (Part 2)

1.0 Network Fundamentals	20%
2.0 Network Access	20%
3.0 IP Connectivity	25%
4.0 IP Services	10%

4.1 Configure and verify inside source NAT using static and pools
4.2 Configure and verify NTP operating in a client and server mode
4.3 Explain the role of DHCP and DNS within the network
4.4 Explain the function of SNMP in network operations
4.5 Describe the use of syslog features including facilities and levels
4.6 Configure and verify DHCP client and relay
4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
4.8 Configure network devices for remote access using SSH
4.9 Describe the capabilities and function of TFTP/FTP in the network

5.0 Security Fundamentals	15%
6.0 Automation and Programmability	10%

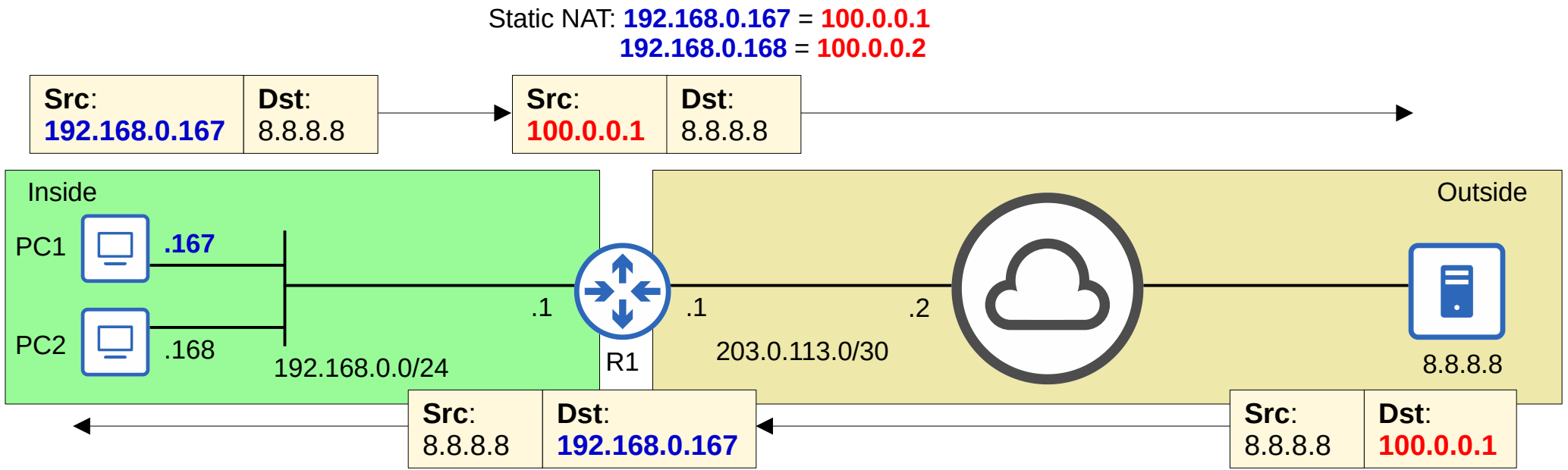


Things we'll cover

- More about static NAT
- Dynamic NAT
- Dynamic PAT

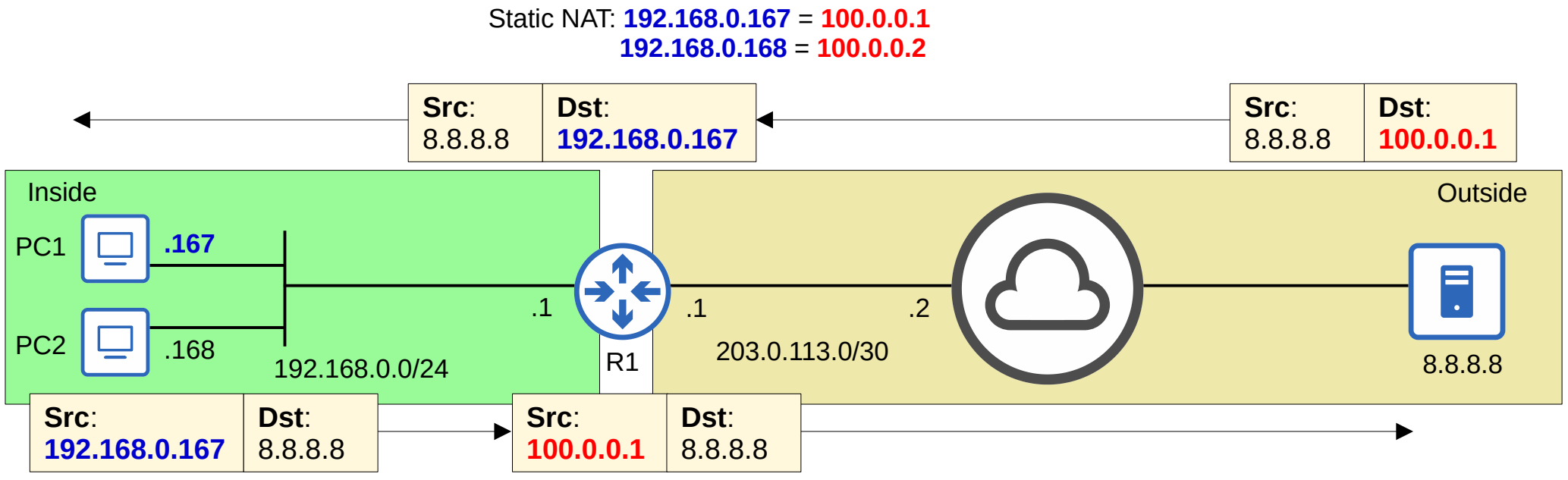
Static NAT

- **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.



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 the inside global address.



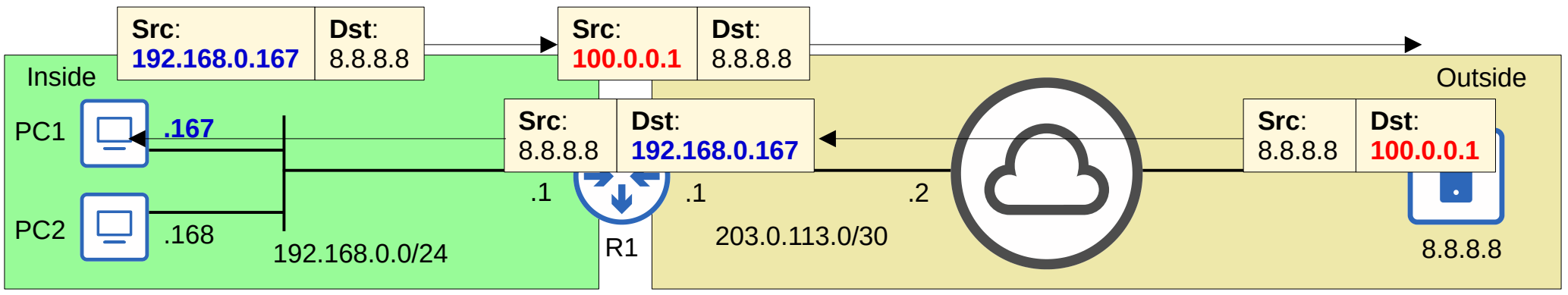
Dynamic NAT

- 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** by the ACL, the source IP will be translated.
  → If the source IP is **denied** by the ACL, the source IP will NOT be translated. *the traffic will NOT be dropped!

- A NAT pool is used to define the available *inside global* addresses.

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**.



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** by the ACL, the source IP will be translated.
  → If the source IP is **denied** by the ACL, the source IP will NOT be translated. *the traffic will NOT be dropped!

- A NAT pool is used to define the available *inside global* addresses that can be used.

- Although they are dynamically assigned, the mappings are still one-to-one (one *inside local* IP address per *inside global* IP address).

- If there aren't enough *inside global* IP addresses available (=all are currently 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

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	100.0.0.11

No address available!
Router will drop the packet

Dynamic NAT Configuration

```
R1(config)#int g0/1
R1(config-if)#ip nat inside
```

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

```
R1(config-if)#int g0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
```

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

```
R1(config)#access-list 1 permit 192.168.0.0 0.0.0.255
```

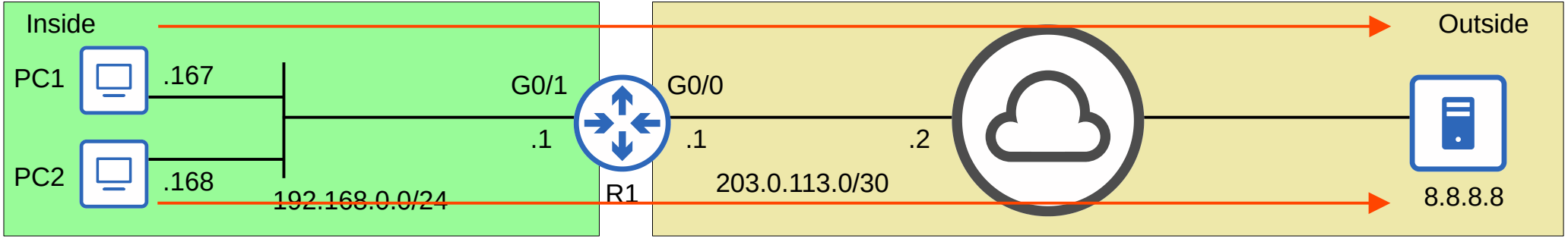
Define the traffic that should be translated.
*Traffic permitted by this ACL will be translated.

```
R1(config)#ip nat pool POOL1 100.0.0.0 100.0.0.255 prefix-length 24
```

Define the pool of inside global IP addresses.
*instead of **`prefix-length 24`**, you can use **`netmask 255.255.255.0`**

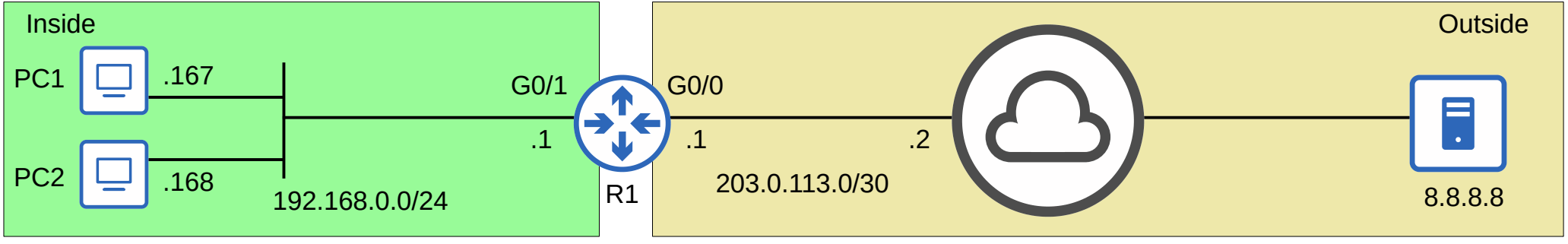
```
R1(config)#ip nat inside source list 1 pool POOL1
```

Configure dynamic NAT by mapping the ACL to the pool.



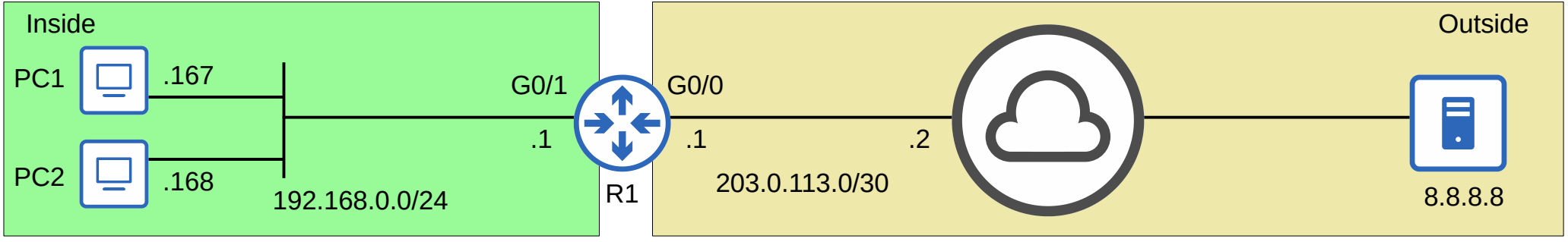
Dynamic NAT Configuration

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



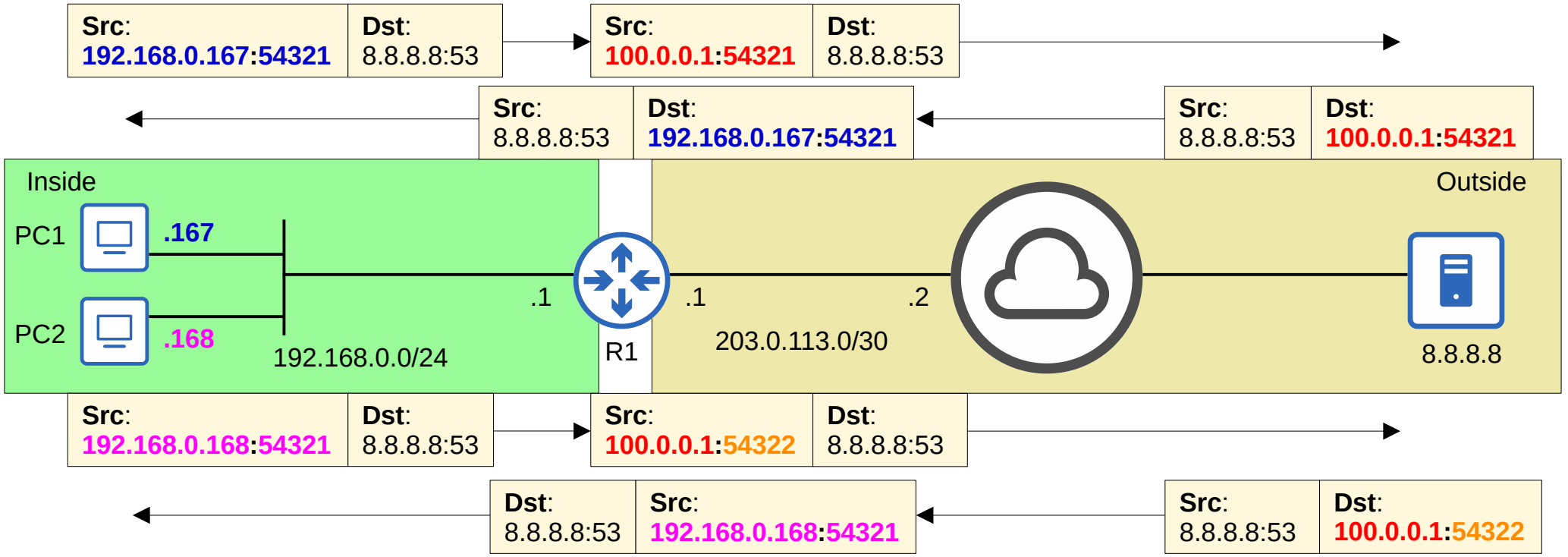
Dynamic NAT Configuration

```
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]
```



PAT (NAT Overload)

- **PAT** (aka **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 number 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.
- Because many inside hosts can share a single public IP, PAT is very useful for preserving public IP addresses, and it is used in networks all over the world.



PAT Configuration (pool)

```
R1(config)#int g0/1
R1(config-if)#ip nat inside
```

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

```
R1(config-if)#int g0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
```

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

```
R1(config)#access-list 1 permit 192.168.0.0 0.0.0.255
```

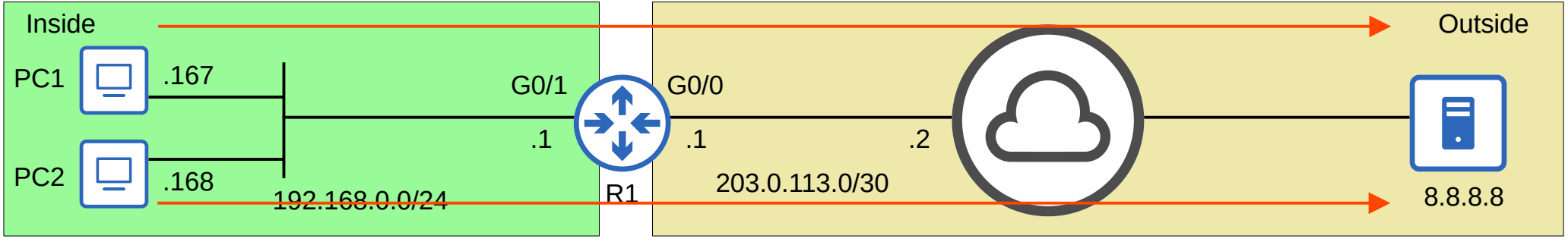
Define the traffic that should be translated.
*Traffic permitted by this ACL will be translated.

```
R1(config)#ip nat pool POOL1 100.0.0.0 100.0.0.3 prefix-length 24
```

Define the pool of inside global IP addresses.

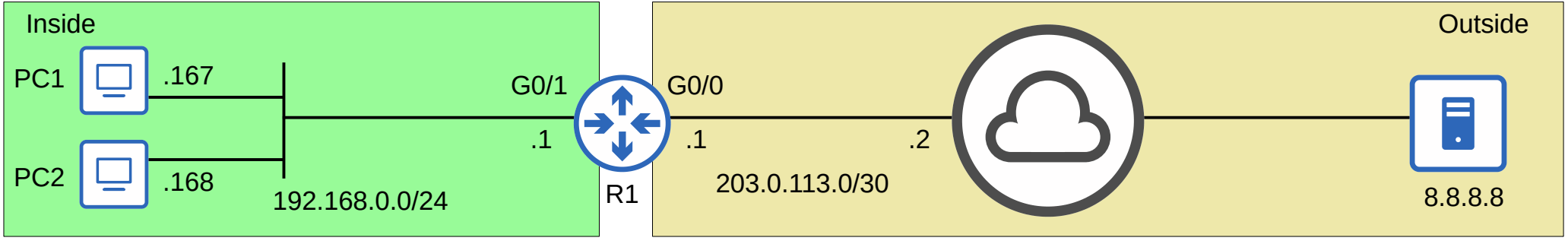
```
R1(config)#ip nat inside source list 1 pool POOL1 overload
```

Configure PAT by mapping the ACL to the pool and using the **`overload`** keyword at the end.



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
```



PAT Configuration (interface)

```
R1(config)#int g0/1
R1(config-if)#ip nat inside
```

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

```
R1(config-if)#int g0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
```

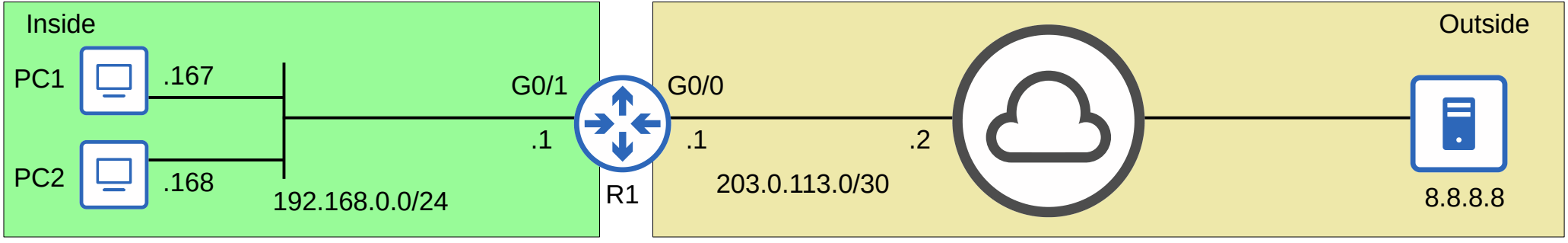
Define the 'outside' interface(s) connected to the external network.

```
R1(config)#access-list 1 permit 192.168.0.0 0.0.0.255
```

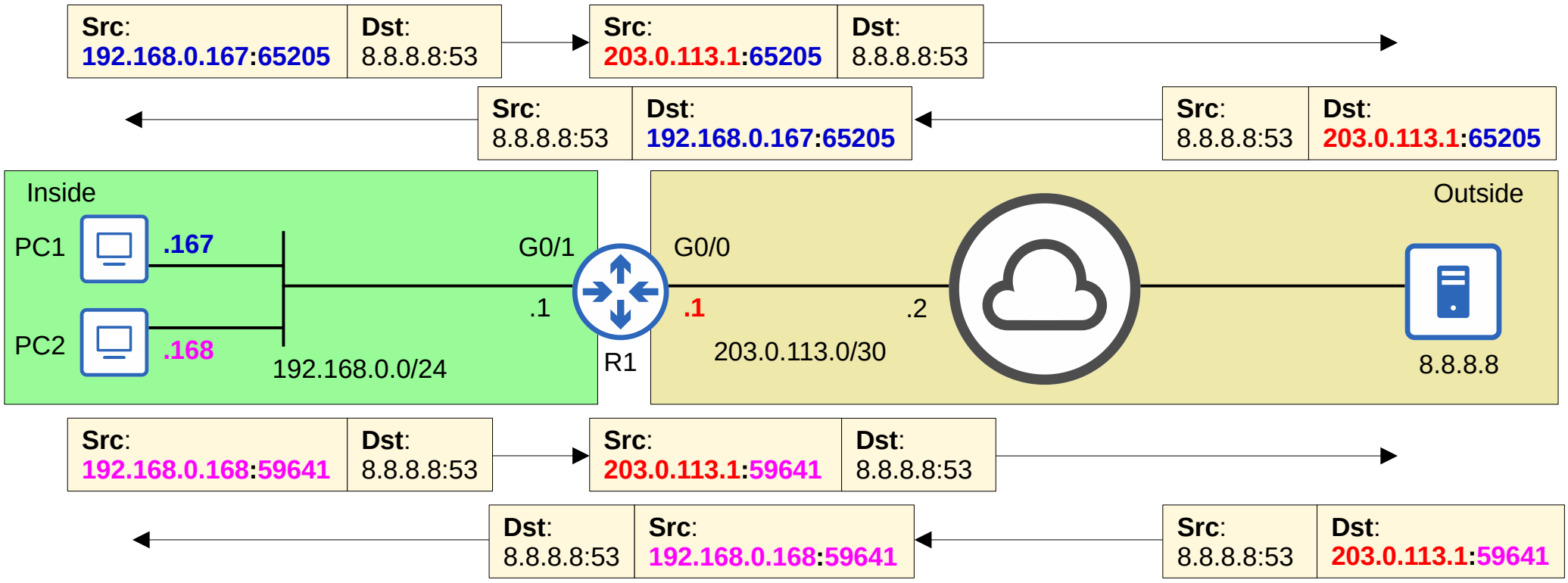
Define the traffic that should be translated.
*Traffic permitted by this ACL will be translated.

```
R1(config)#ip nat inside source list 1 interface g0/0 overload
```

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

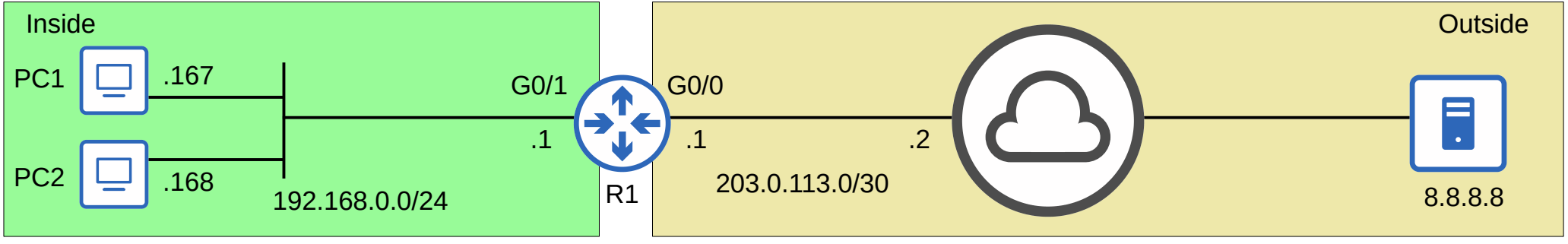


PAT Configuration (interface)



PAT Configuration (interface)

```
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
```



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
```

Things we covered

- More about static NAT
- Dynamic NAT
- Dynamic PAT

Quiz 1

Which of the following NAT types best fulfills the goal of preserving public IPv4 addresses?

a) Static NAT

b) Source NAT

c) Dynamic NAT

d) NAT Overload

Quiz 2

Which of the following dynamic NAT configurations will translate inside local addresses from 172.16.1.0/24 to addresses from the subnet 203.0.113.0/25?

a)

```
access-list 1 deny 172.16.1.0 0.0.0.255
ip nat pool POOL1 203.0.113.0 203.0.113.255 netmask 255.255.255.128
ip nat inside source list 1 pool POOL1
interface g0/0
ip nat inside
interface g0/1
ip nat outside
```

b)

```
access-list 1 permit 172.16.1.0 0.0.0.255
ip nat pool POOL1 203.0.113.0 203.0.113.127 netmask 255.255.255.128
ip nat inside source list 1 pool POOL1
interface g0/0
ip nat inside
interface g0/1
ip nat outside
```

c)

```
access-list 1 permit 172.16.1.0 255.255.255.0
ip nat pool POOL1 203.0.113.0 203.0.113.127 prefix-length 25
ip nat inside source list 1 pool POOL1
interface g0/0
ip nat inside
interface g0/1
ip nat outside
```

Quiz 3

Dynamic NAT is configured on R1 and a pool of 10 inside global addresses is specified. Currently, all 10 addresses are being used by inside hosts, but another inside host attempts to send a packet over the Internet. What does R1 do with this packet?

a) It uses PAT to translate the source IP address of the packet.

b) It discards the packet.

c) It holds the packet until an inside global address becomes available.

d) It translates the source IP to the statically mapped inside global address.

Quiz 4

Which of the following dynamic NAT configurations will translate inside local addresses from 10.0.1.0/27 to use the IP address of the router's G0/1 interface?

a)
```
access-list 1 permit 10.0.1.0 0.0.0.31
ip nat inside source list 1 interface gigabitethernet0/1 overload
interface g0/0
ip nat inside
interface g0/1
ip nat outside
```

b)
```
access-list 1 permit 172.16.1.0 0.0.0.31
ip nat inside source list 1 pool gigabitethernet0/1 overload
interface g0/0
ip nat inside
interface g0/1
ip nat outside
```

c)
```
access-list 1 permit 172.16.1.0 0.0.0.31
ip nat inside source list 1 interface gigabitethernet0/1 overload
interface g0/0
ip nat inside
interface g0/1
ip nat inside
```

d)
```
access-list 1 permit 172.16.1.0 0.0.0.224
ip nat inside source list 1 interface gigabitethernet0/1 overload
interface g0/0
ip nat inside
interface g0/1
ip nat outside
```

Quiz 5

After specifying the inside and outside NAT interfaces, you issue the following commands on R1. What will happen to hosts from the 192.168.1.0/24 subnet?

```
access-list 1 permit 10.0.1.0 0.0.0.255
access-list 1 deny 192.168.1.0 0.0.0.255
ip nat pool POOL1 203.0.113.0 203.0.113.255 prefix-length 24
ip nat inside source list 1 pool POOL1
```

a) The source IP of their packets will be translated to an address from 203.0.113.0/24.

b) The packets they send will be discarded by R1.

c) The packets they send will not be translated by R1.

d) The packets they send will be discarded until an inside global address is available.