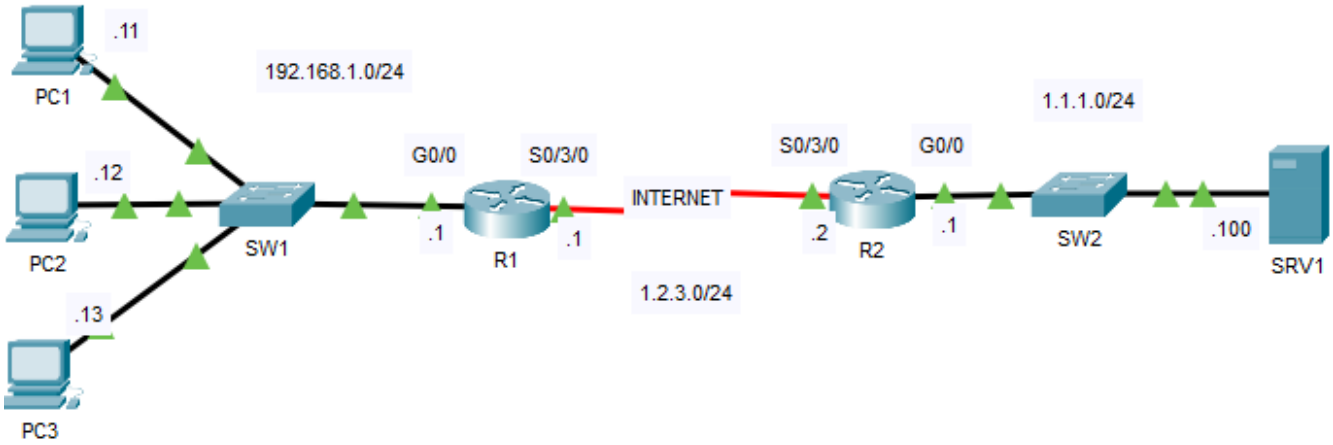
ACTIVITY 37: Static NAT



1. RIP has been configured so that R1 and R2 can reach their inside networks. Why can't PC1, PC2, and PC3 successfully ping SRV1? (Hint: The serial connection between R1 and R2 is simulating the Internet with ACLs)

Let's see the ACL to see if the connection from/to 192.168.1.0/24 is permitted.

```
R1#show ip access-list
Extended IP access list 100
    10 deny ip any 10.0.0.0 0.255.255.255
    20 deny ip any 172.16.0.0 0.15.255.255
    30 deny ip any 192.168.0.0 0.0.255.255
    40 permit ip any any
```

As we can see, any network is denied to access it. That's why the PCs can't access SRV1.

2. Configure static NAT on R1 to translate the address of PC1, PC2, and PC3 to 1.2.3.11, 1.2.3.12, and 1.2.3.13, respectively.

```
R1(config)#interface g0/0
R1(config-if)#ip nat inside
R1(config-if)#interface s0/3/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#ip nat inside source static 192.168.1.11 1.2.3.11
R1(config)#ip nat inside source static 192.168.1.12 1.2.3.12
R1(config)#ip nat inside source static 192.168.1.13 1.2.3.13
```

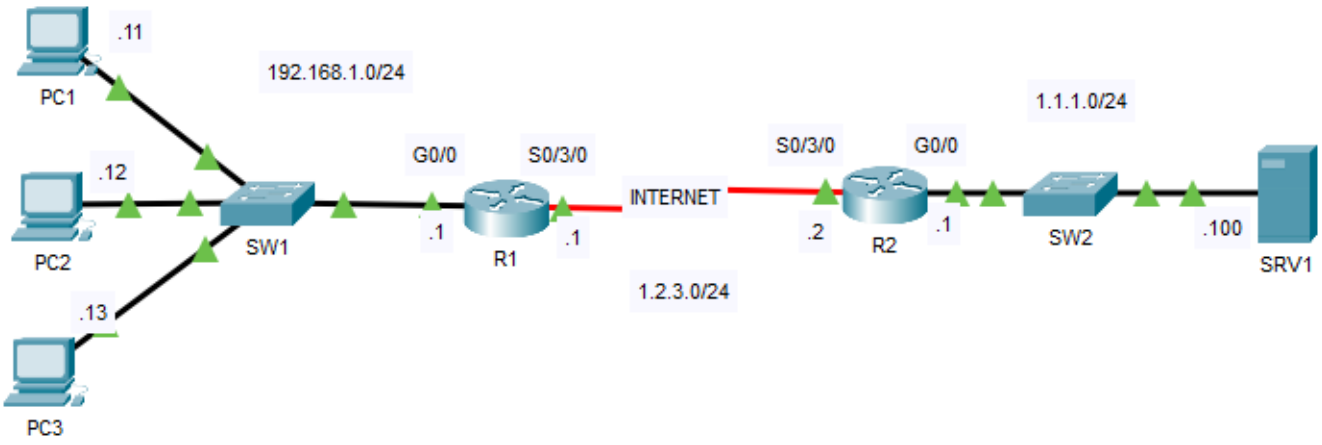
3. Attempt to ping SRV1 from each PC again. Do the pings succeed?

```
C:\>ping 1.1.1.100

Pinging 1.1.1.100 with 32 bytes of data:

Request timed out.
Reply from 1.1.1.100: bytes=32 time=1ms TTL=126
Reply from 1.1.1.100: bytes=32 time=1ms TTL=126
Reply from 1.1.1.100: bytes=32 time=1ms TTL=126
```

As we see, the ping from PC1 to SRV1 succeeded because the router translated the private address to a public one :

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 1.2.3.11:1        192.168.1.11:1     1.1.1.100:1        1.1.1.100:1
icmp 1.2.3.11:2        192.168.1.11:2     1.1.1.100:2        1.1.1.100:2
icmp 1.2.3.11:3        192.168.1.11:3     1.1.1.100:3        1.1.1.100:3
icmp 1.2.3.11:4        192.168.1.11:4     1.1.1.100:4        1.1.1.100:4
---  1.2.3.12          192.168.1.12       ---                ---
---  1.2.3.13          192.168.1.13       ---                ---
```

ACTIVITY 38: Dynamic NAT



1. RIP has been configured so that R1 and R2 can reach their inside networks. Why can't PC1, PC2, and PC3 successfully ping SRV1? (Hint: The serial connection between R1 and R2 is simulating the Internet with ACLs)

Let's see the ACL to see if the connection from/to 192.168.1.0/24 is permitted.

```
R1#show ip access-list
Extended IP access list 100
    10 deny ip any 10.0.0.0 0.255.255.255
    20 deny ip any 172.16.0.0 0.15.255.255
    30 deny ip any 192.168.0.0 0.0.255.255
    40 permit ip any any
```

As we can see, any network is denied to access it. That's why the PCs can't access SRV1.

2. Configure dynamic NAT on R1 to translate the 192.168.1.0/24 subnet to the address range 1.2.3.10 - 1.2.3.20

```
R1(config)#interface g0/0
R1(config-if)#ip nat inside
R1(config-if)#interface s0/3/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#ip nat pool POOL 1.2.3.10 1.2.3.20 netmask 255.255.255.0
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#ip nat inside source list 1 pool POOL
```

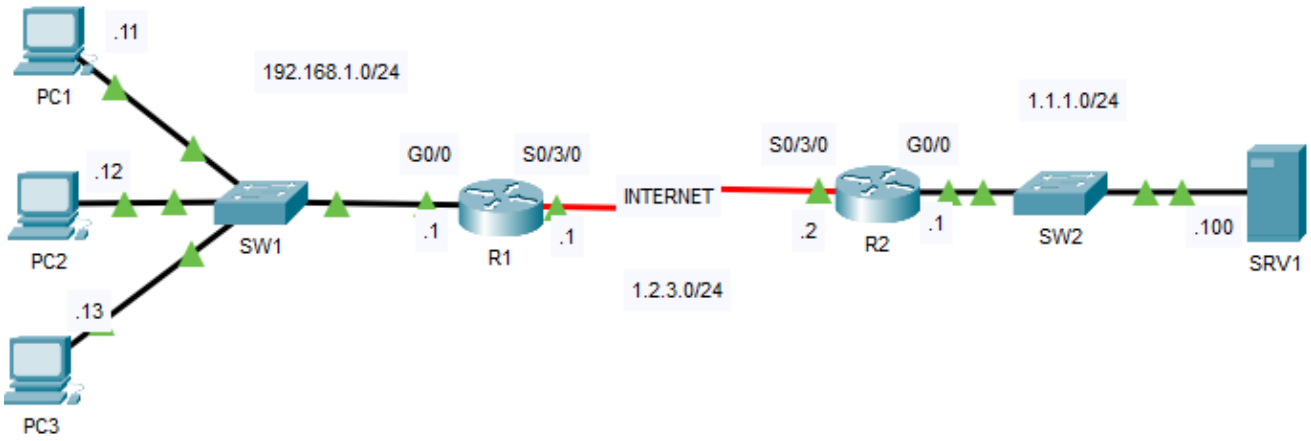
3. Ping from each PC to SRV1, then use a show command on R1 to check the translations.

```
C:\>ping 1.1.1.100

Pinging 1.1.1.100 with 32 bytes of data:

Request timed out.
Reply from 1.1.1.100: bytes=32 time=1ms TTL=126
Reply from 1.1.1.100: bytes=32 time=1ms TTL=126
Reply from 1.1.1.100: bytes=32 time=1ms TTL=126
```

It is successful from PC2 to SRV1, let's see the translations :

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 1.2.3.10:1        192.168.1.12:1     1.1.1.100:1        1.1.1.100:1
icmp 1.2.3.10:2        192.168.1.12:2     1.1.1.100:2        1.1.1.100:2
icmp 1.2.3.10:3        192.168.1.12:3     1.1.1.100:3        1.1.1.100:3
icmp 1.2.3.10:4        192.168.1.12:4     1.1.1.100:4        1.1.1.100:4
```

ACTIVITY 39: PAT



1. RIP has been configured so that R1 and R2 can reach their inside networks. Why can't PC1, PC2, and PC3 successfully ping SRV1? (Hint: The serial connection between R1 and R2 is simulating the Internet with ACLs)

Let's see the ACL to see if the connection from/to 192.168.1.0/24 is permitted.

```
R1#show ip access-list
Extended IP access list 100
    10 deny ip any 10.0.0.0 0.255.255.255
    20 deny ip any 172.16.0.0 0.15.255.255
    30 deny ip any 192.168.0.0 0.0.255.255
    40 permit ip any any
```

As we can see, any network is denied to access it. That's why the PCs can't access SRV1.

2. Configure PAT on R1 to translate addresses in the 192.168.1.0/24 network to R1's S0/3/0 interface. (make sure to 'overload' the interface!)

```
R1(config)#interface g0/0
R1(config-if)#ip nat inside
R1(config-if)#interface s0/3/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#ip nat inside source list 1 interface s0/3/0 overload
```

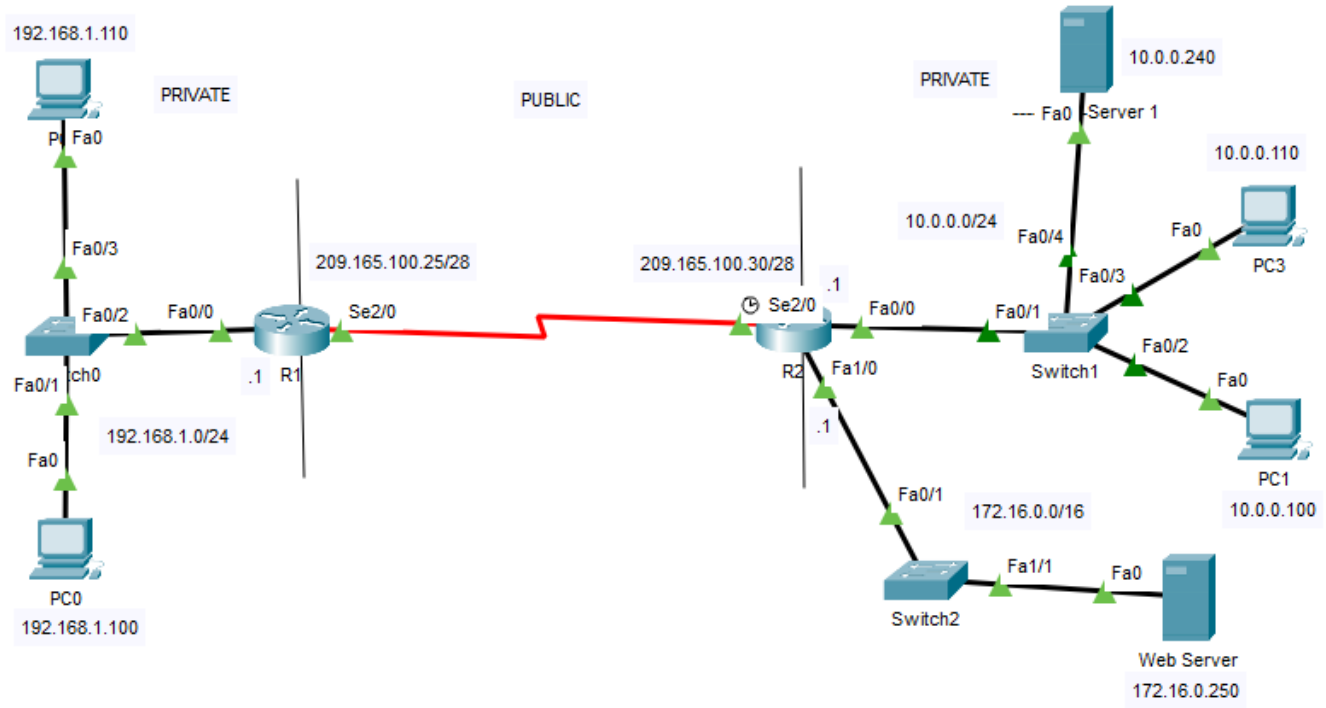
3. Ping from each PC to SRV1, then use a show command on R1 to check the translations.

```
C:\>ping 1.1.1.100

Pinging 1.1.1.100 with 32 bytes of data:

Request timed out.
Reply from 1.1.1.100: bytes=32 time=1ms TTL=126
Reply from 1.1.1.100: bytes=32 time=1ms TTL=126
Reply from 1.1.1.100: bytes=32 time=1ms TTL=126
```

As we can see the ping from PC3 to SRV1 succeeded. Let's check the translations :

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 1.2.3.1:2         192.168.1.13:2     1.1.1.100:2        1.1.1.100:2
icmp 1.2.3.1:3         192.168.1.13:3     1.1.1.100:3        1.1.1.100:3
icmp 1.2.3.1:4         192.168.1.13:4     1.1.1.100:4        1.1.1.100:4
```

OTHER ACTIVITY :



The networks are pre-configured with dynamic routing protocols

1- Does ping from private to private work?

```
C:\>ping 10.0.0.240

Pinging 10.0.0.240 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.240: bytes=32 time=1ms TTL=126
Reply from 10.0.0.240: bytes=32 time=1ms TTL=126
Reply from 10.0.0.240: bytes=32 time=1ms TTL=126
```

```
C:\>ping 172.16.0.250

Pinging 172.16.0.250 with 32 bytes of data:

Request timed out.
Reply from 172.16.0.250: bytes=32 time=12ms TTL=126
Reply from 172.16.0.250: bytes=32 time=1ms TTL=126
Reply from 172.16.0.250: bytes=32 time=1ms TTL=126
```

Yes the ping works from private to private.

2- Configure ACL to deny the traffic between private to private

```
R1(config)#access-list 100 deny ip any 192.168.1.0 0.0.0.255
R1(config)#access-list 100 permit ip any any
R1(config)#interface s2/0
R1(config-if)#ip access-group 100 in

R2(config)#access-list 100 deny ip any 10.0.0.0 0.0.0.255
R2(config)#access-list 100 deny ip any 172.16.0.0 0.0.255.255
R2(config)#access-list 100 permit ip any any
R2(config)#interface s2/0
R2(config-if)#ip access-group 100 in
```

Now the ping does not work:

```
C:\>ping 10.0.0.240

Pinging 10.0.0.240 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
C:\>ping 172.16.0.250

Pinging 172.16.0.250 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

3- Configure dynamic nat on 192.168.1.0/24 using pool 209.165.100.17-24/28

```
R1(config)#interface f0/0
R1(config-if)#ip nat inside
R1(config-if)#interface s2/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#ip nat pool POOL 209.165.100.17 209.165.100.24 netmask 255.255.255.240
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#ip nat inside source list 1 pool POOL
```

4- Configure static nat on Server 1 with 209.165.100.28

```
R2(config)#interface s2/0
R2(config-if)#ip nat outside
R2(config-if)#interface f0/0
R2(config-if)#ip nat inside
R2(config-if)#ip nat inside source static 10.0.0.240 209.165.100.28
```

5- Configure PAT on PC1 and PC3

```
R2(config)#access-list 1 permit 10.0.0.0 0.0.0.127
R2(config)#ip nat inside source list 1 interface s2/0 overload
```

6- Configure static port address translation on port 80 on the Web Server with address 209.165.100.29

```
R2(config)#interface f1/0
R2(config-if)#ip nat inside
R2(config-if)#ip nat inside source static tcp 172.16.0.250 80 209.165.100.29 80
```

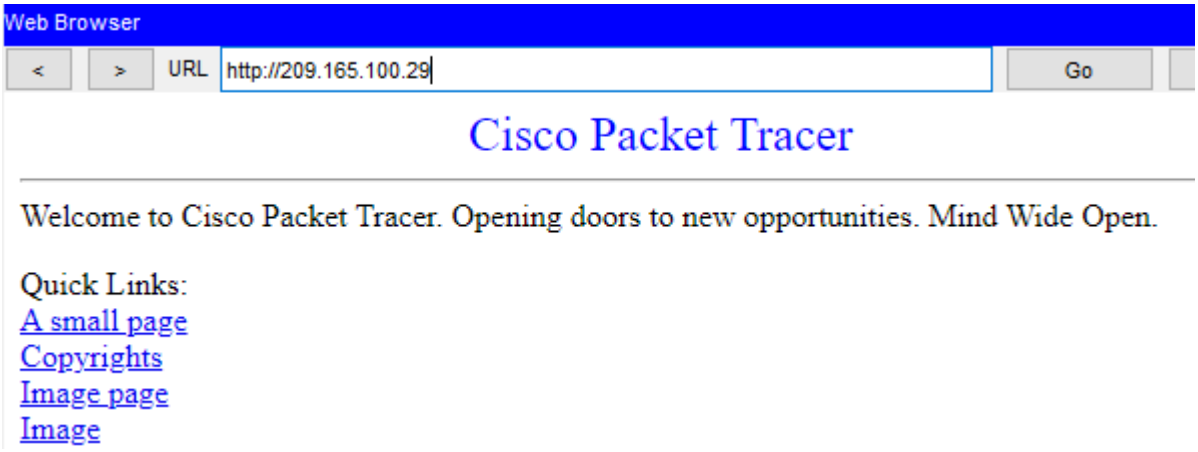
7- Ping from the PCs using public addresses and test the web server

```
C:\>ping 209.165.100.28

Pinging 209.165.100.28 with 32 bytes of data:

Reply from 209.165.100.28: bytes=32 time=13ms TTL=126
Reply from 209.165.100.28: bytes=32 time=1ms TTL=126
Reply from 209.165.100.28: bytes=32 time=1ms TTL=126
Reply from 209.165.100.28: bytes=32 time=1ms TTL=126
```

```
C:\>ping 209.165.100.30

Pinging 209.165.100.30 with 32 bytes of data:

Reply from 209.165.100.30: bytes=32 time=19ms TTL=254
Reply from 209.165.100.30: bytes=32 time=1ms TTL=254
Reply from 209.165.100.30: bytes=32 time=1ms TTL=254
Reply from 209.165.100.30: bytes=32 time=1ms TTL=254
```

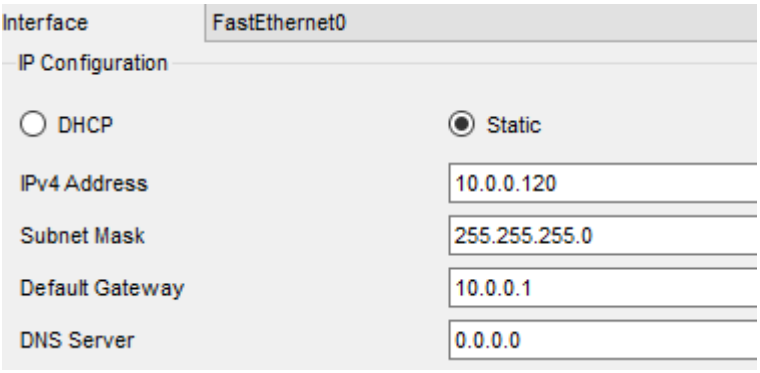
```
C:\>ping 209.165.100.29

Pinging 209.165.100.29 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

As we can see the ping works from PC0 to Server1 and PC3 or PC1 but does not work for the Web server. Let's check if we can access the web server:



Yes, the PC0 can access the Web server as it was configured only on port 80.

8- Change the address of PC1 to 10.0.0.120, does the ping still work?




```
C:\>ping 209.165.100.30

Pinging 209.165.100.30 with 32 bytes of data:

Reply from 209.165.100.30: bytes=32 time=14ms TTL=254
Reply from 209.165.100.30: bytes=32 time=1ms TTL=254
Reply from 209.165.100.30: bytes=32 time=1ms TTL=254
Reply from 209.165.100.30: bytes=32 time=1ms TTL=254
```

The ping still works because the address was overloaded on s2/0. So, all of the PCs within the range get this public IP address.