NAT Types

- Static NAT – permanent one-to-one mapping usually between a public and private IP address. Used for servers which must accept incoming connections.
- Dynamic NAT – uses a pool of public addresses which are given out on an as needed first come first served basis. Usually used for internal hosts which need to connect to the Internet but do not accept incoming connections.
- **PAT (Port Address Translation)– allows the same IP address to be reused.**

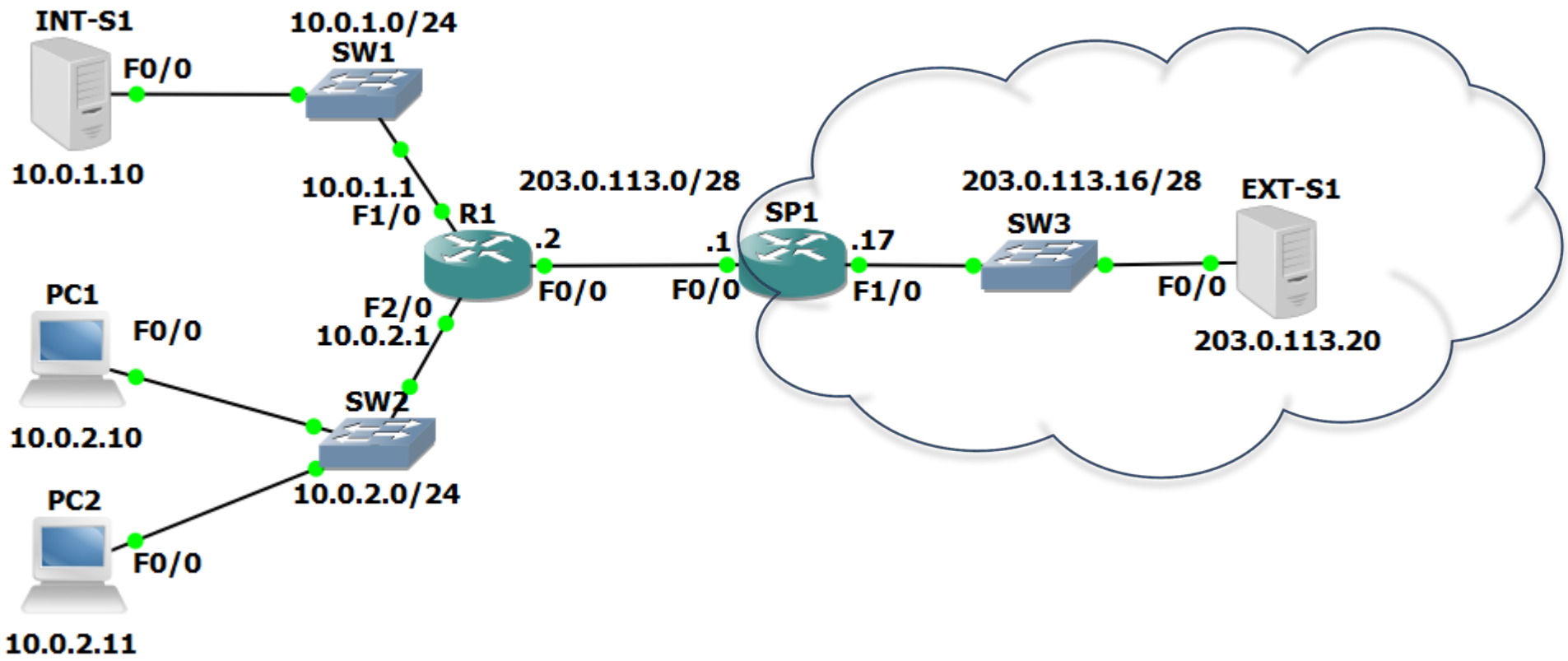
Dynamic NAT Address Exhaustion

- With standard dynamic NAT the inside hosts are translated to public IP addresses on a first come first served basis when they send traffic out
- This requires a public IP address for every inside host which communicates with the outside network
- When all the addresses in the pool have been used, new outbound connections from other inside hosts will fail because there will be no addresses left to translate them to

PAT Port Address Translation

- Port Address Translation (PAT) is an extension to NAT that permits multiple devices to be mapped to a single public IP address
- With PAT you do not need a public IP address for every inside host
- The router tracks translations by IP address and Layer 4 port number
- Because different inside hosts are assigned different port numbers, the router knows which host to send return traffic to, even when the public IP address is the same

NAT Lab


INT-S1
F0/0
10.0.1.10
10.0.1.0/24
SW1
10.0.1.1
F1/0
R1
203.0.113.0/28
.2
F0/0
.1
F0/0
SP1
.17
F1/0
203.0.113.16/28
SW3
F0/0
EXT-S1
203.0.113.20
PC1
F0/0
10.0.2.10
F2/0
10.0.2.1
SW2
10.0.2.0/24
PC2
F0/0
10.0.2.11

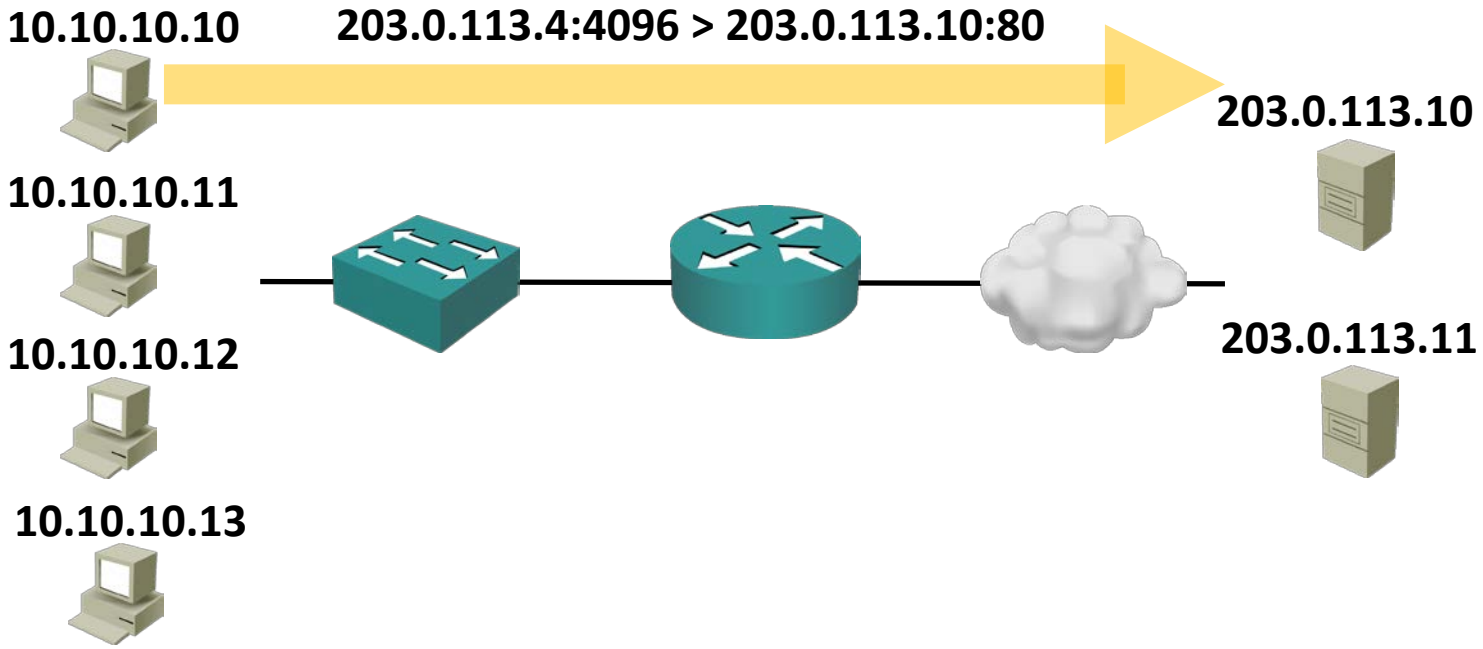
Dynamic NAT with Overload

- Dynamic NAT with Overload uses PAT to allow more clients to be translated than IP addresses are available in the NAT pool
- If the NAT pool is 203.0.113.4 to 203.0.113.6 for example, the first 2 hosts which initiate outbound connections will be translated to 203.0.113.4 and 203.0.113.5

Dynamic NAT with Overload

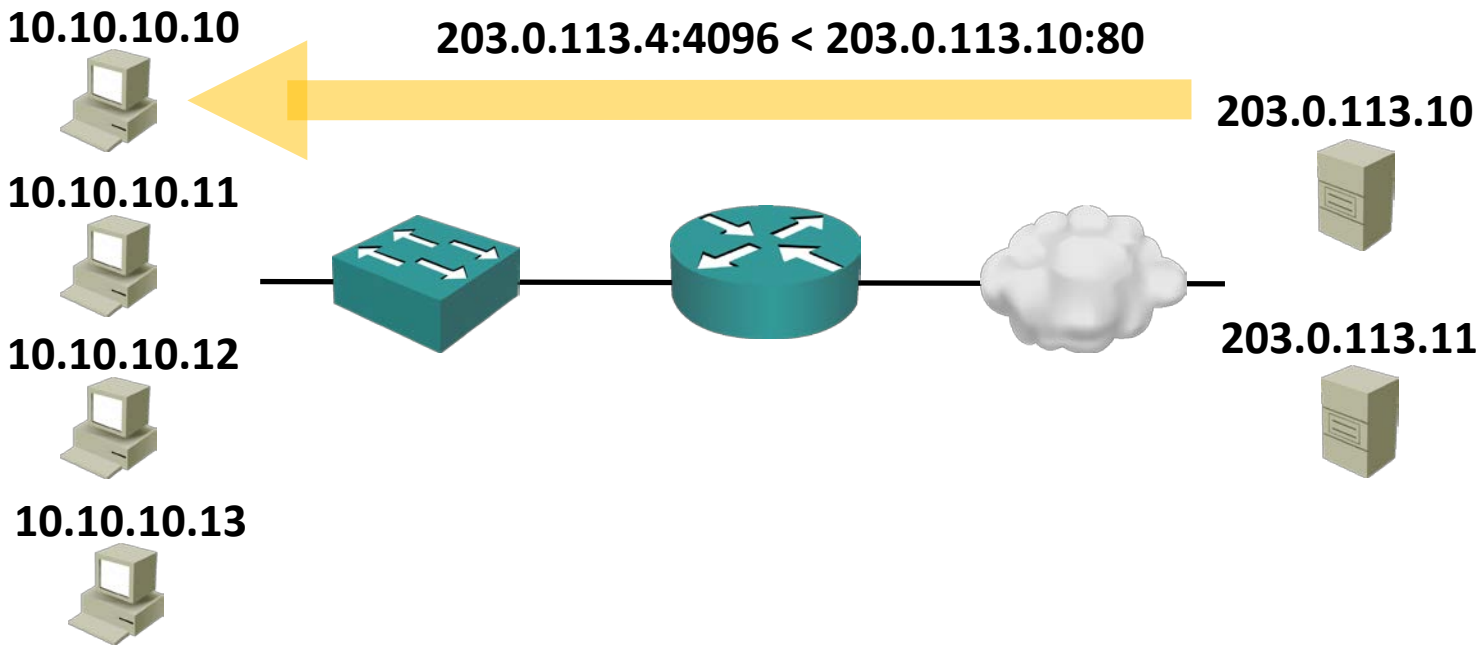
- The 3rd host will be translated to 203.0.113.6 and the router will track which source port number was used in the translation table
- The 4th and 5th etc. hosts will also be translated to 203.0.113.6 but with different source port numbers
- When the return traffic is sent back the router checks the destination port number to see which host to forward it to

Dynamic NAT with Overload



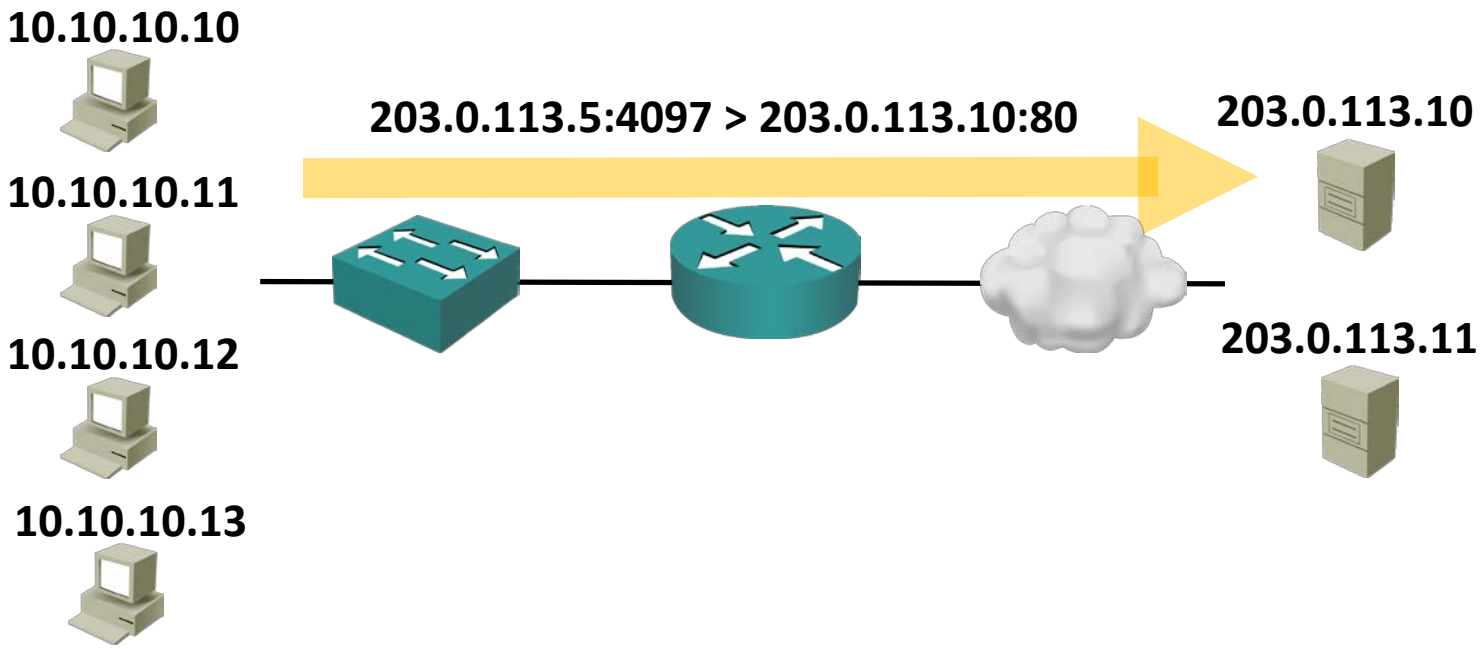
Inside Local Source	Inside Global Source	Outside Local Destination	Outside Global Destination
10.10.10.10:49165	203.0.113.4:4096	203.0.113.10:80	203.0.113.10:80

Dynamic NAT with Overload



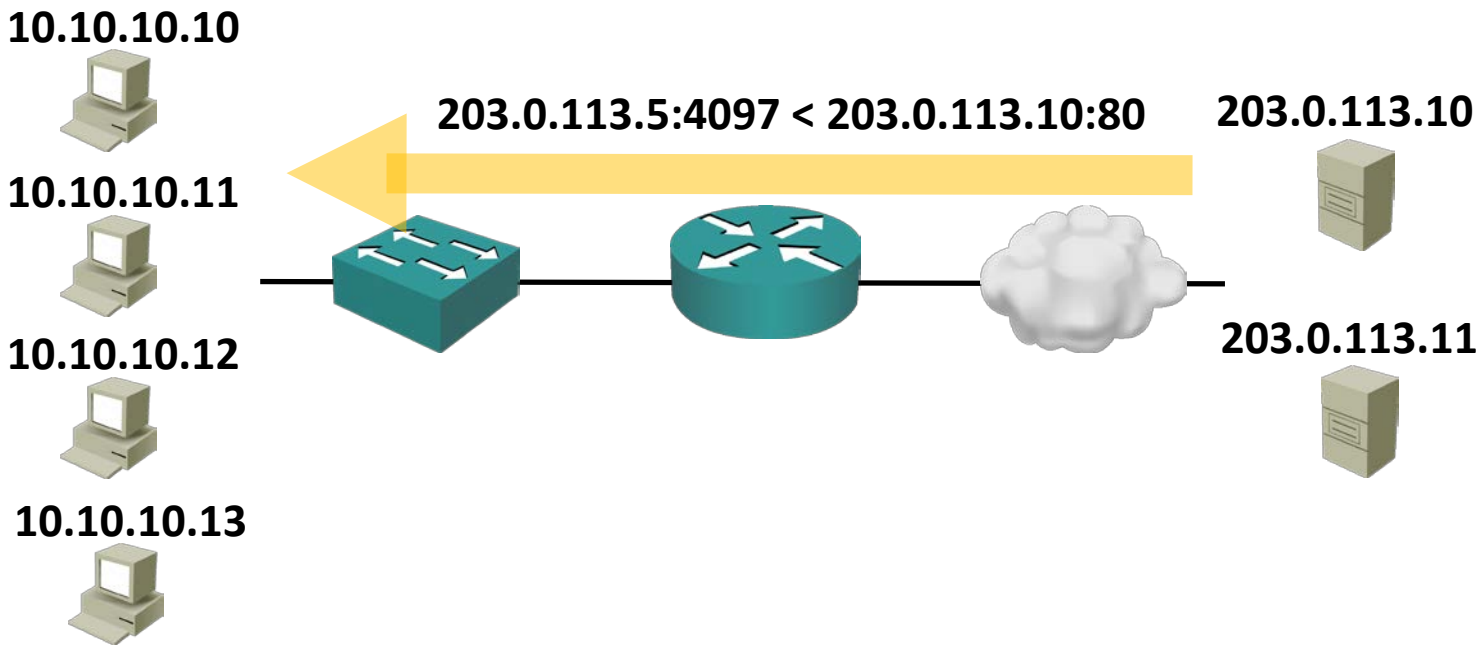
Inside Local Source	Inside Global Source	Outside Local Destination	Outside Global Destination
10.10.10.10:49165	203.0.113.4:4096	203.0.113.10:80	203.0.113.10:80

Dynamic NAT with Overload



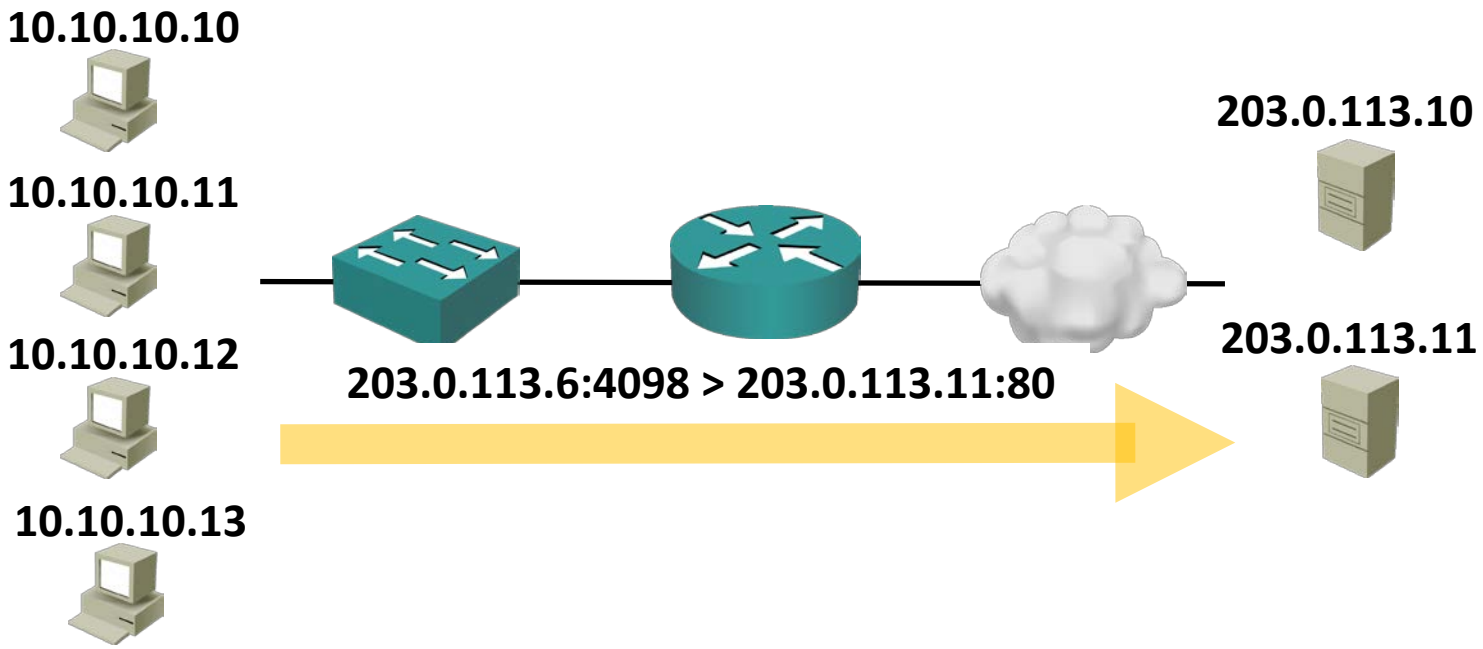
Inside Local Source	Inside Global Source	Outside Local Destination	Outside Global Destination
10.10.10.11:49158	203.0.113.5:4097	203.0.113.10:80	203.0.113.10:80

Dynamic NAT with Overload



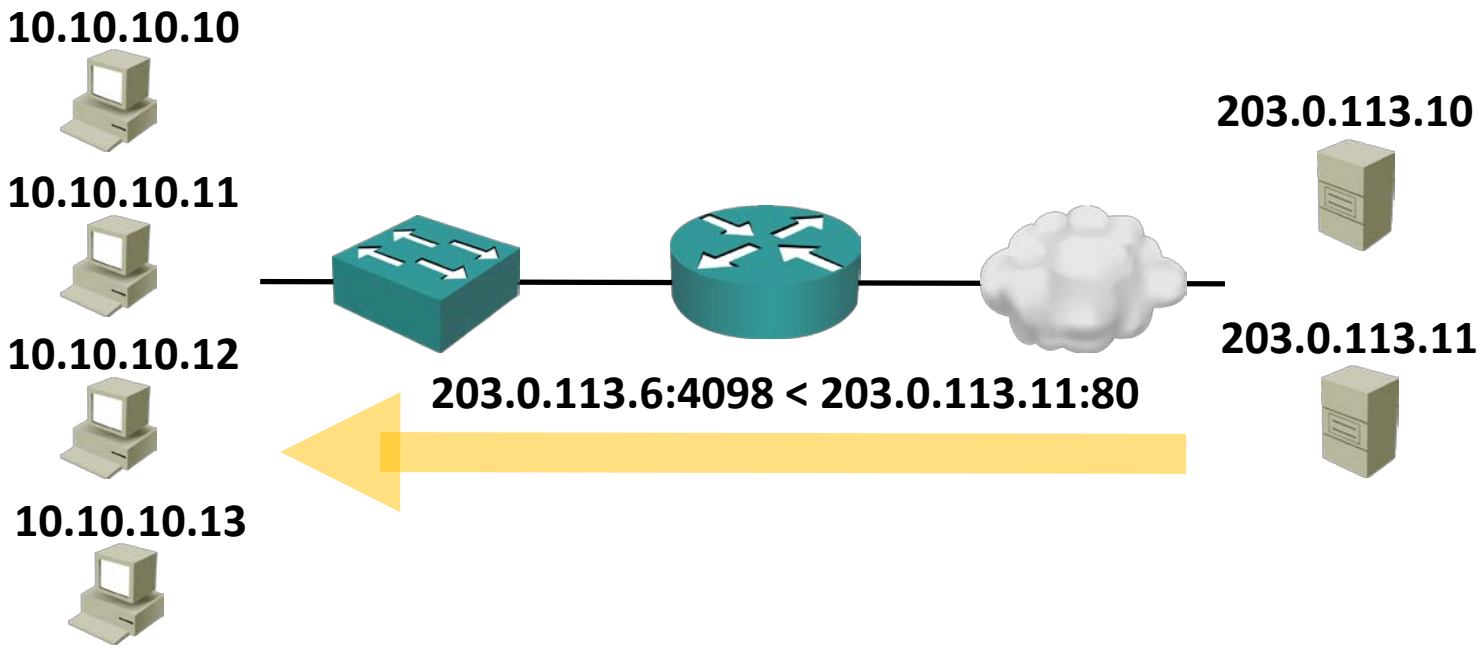
Inside Local Source	Inside Global Source	Outside Local Destination	Outside Global Destination
10.10.10.11:49158	203.0.113.5:4097	203.0.113.10:80	203.0.113.10:80

Dynamic NAT with Overload



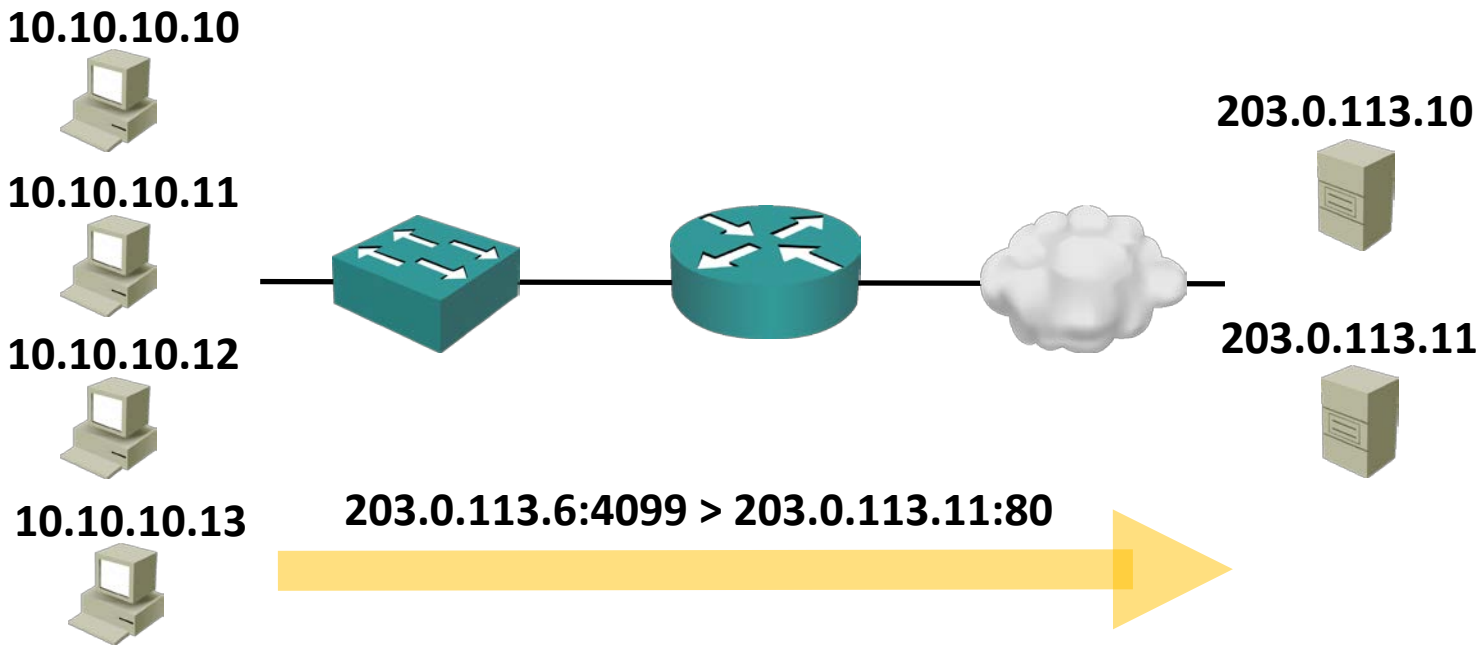
Inside Local Source	Inside Global Source	Outside Local Destination	Outside Global Destination
10.10.10.12:49152	203.0.113.6:4098	203.0.113.11:80	203.0.113.11:80

Dynamic NAT with Overload



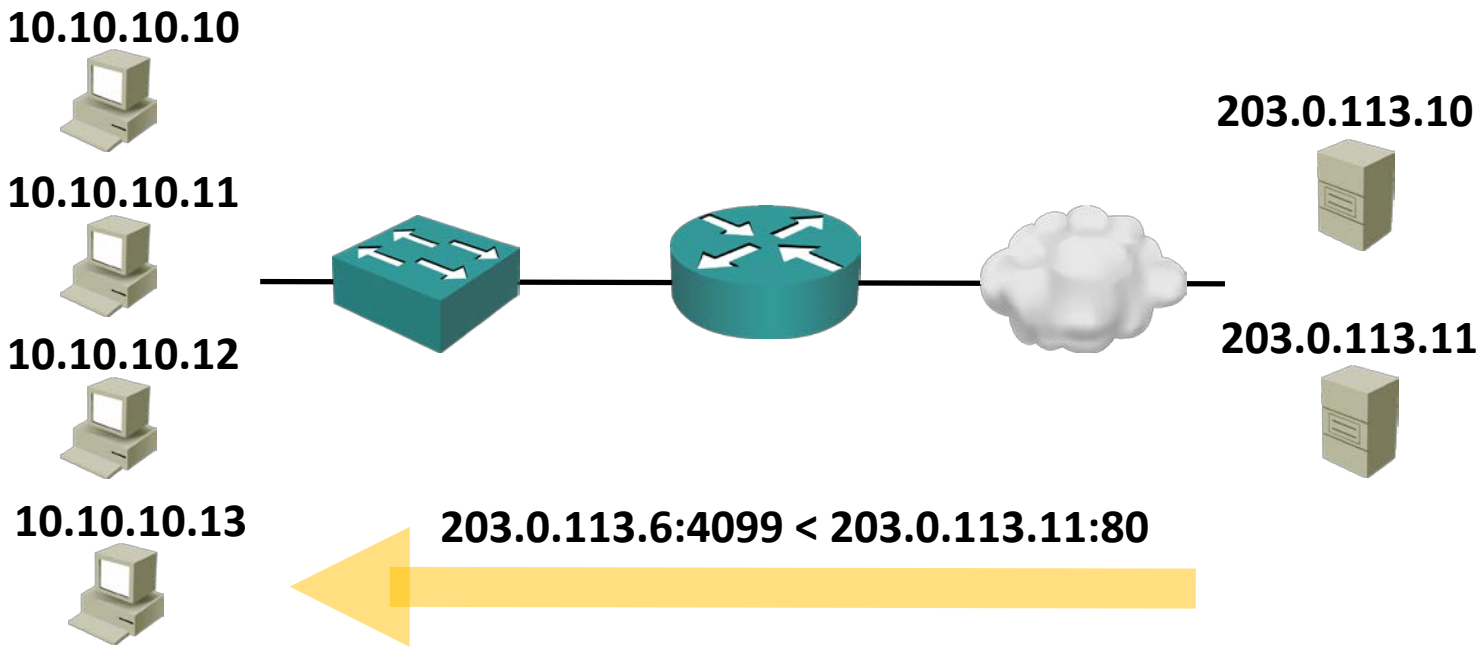
Inside Local Source	Inside Global Source	Outside Local Destination	Outside Global Destination
10.10.10.12:49152	203.0.113.6:4098	203.0.113.11:80	203.0.113.11:80

Dynamic NAT with Overload



Inside Local Source	Inside Global Source	Outside Local Destination	Outside Global Destination
10.10.10.13:49152	203.0.113.6:4099	203.0.113.11:80	203.0.113.11:80

Dynamic NAT with Overload



Inside Local Source	Inside Global Source	Outside Local Destination	Outside Global Destination
10.10.10.13:49152	203.0.113.6:4099	203.0.113.11:80	203.0.113.11:80

Standard Dynamic NAT Configuration

```
R1(config)#int f0/0
R1(config-if)#ip nat outside
R1(config)#int f2/0
R1(config-if)#ip nat inside
```

Configure the pool of global addresses.

```
R1(config)#ip nat pool Flackbox 203.0.113.4 203.0.113.6 netmask 255.255.255.240
```

Create an access list which references the internal IP addresses we want to translate.

```
R1(config)#access-list 1 permit 10.0.2.0 0.0.0.255
```

Associate the access list with the NAT pool to complete the configuration.

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

Dynamic NAT with Overload Configuration

```
R1(config)#int f0/0
R1(config-if)#ip nat outside
R1(config)#int f2/0
R1(config-if)#ip nat inside
```

Configure the pool of global addresses.

```
R1(config)#ip nat pool Flackbox 203.0.113.4 203.0.113.6 netmask 255.255.255.240
```

Create an access list which references the internal IP addresses we want to translate.

```
R1(config)#access-list 1 permit 10.0.2.0 0.0.0.255
```

Associate the access list with the NAT pool to complete the configuration.

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

PAT with Single IP Address

- The last NAT scenario to cover is a small office which has not purchased a range of public IP addresses
- In this case the outside interface will most likely get its IP address via DHCP from the service provider
- PAT can be used to allow multiple inside hosts to share the single outside public IP address

PAT with Single IP Address

- The configuration is very similar to Dynamic NAT with Overload but translates to the outside interface address rather than a pool of addresses
- You must translate to the outside interface rather than a specific IP address because a DHCP address can change

PAT with Single IP Address Configuration

```
R1(config)#int f0/0
R1(config-if)#ip address dhcp
R1(config-if)#ip nat outside

R1(config)#int f1/0
R1(config-if)#ip nat inside

R1(config)#access-list 1 permit 10.0.2.0 0.0.0.255

R1(config)#ip nat inside source list 1 interface f0/0 overload
```

NAT Verification – show ip nat translation

```
R1#sh ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
tcp 203.0.113.13:4096  10.0.2.10:54963    203.0.113.20:23    203.0.113.20:23
tcp 203.0.113.13:4097  10.0.2.11:52670    203.0.113.20:23    203.0.113.20:23
```

NAT Verification – debug ip nat

```
R1#debug ip nat
```

- Outbound

```
*Aug 21 23:52:55.739: NAT*: TCP s=52670->4097, d=23
*Aug 21 23:52:55.739: NAT*: s=10.0.2.11->203.0.113.13, d=203.0.113.20
[34332]
```

- Return Traffic

```
*Aug 21 23:52:55.763: NAT*: TCP s=23, d=4097->52670
*Aug 21 23:52:55.763: NAT*: s=203.0.113.20, d=203.0.113.13->10.0.2.11
[45975]
```