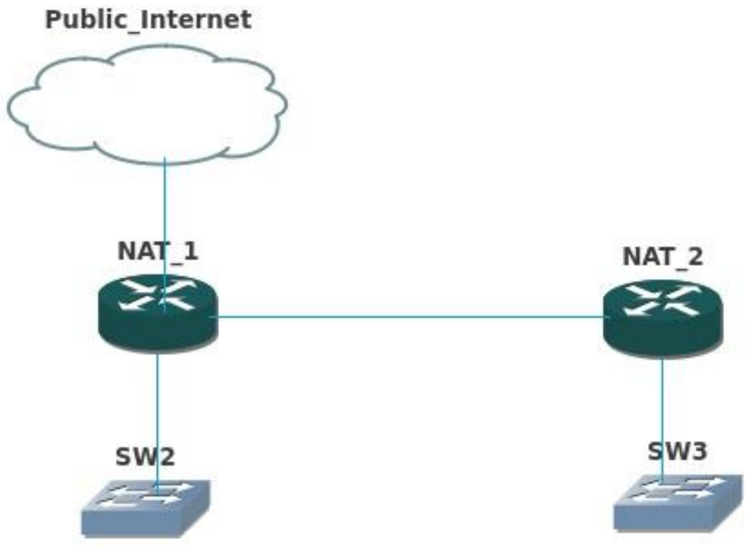
Double Network Address Translation (NAT)

Sean McGrath

UCSC CMPE151 Spring 2015

What is Double NAT?

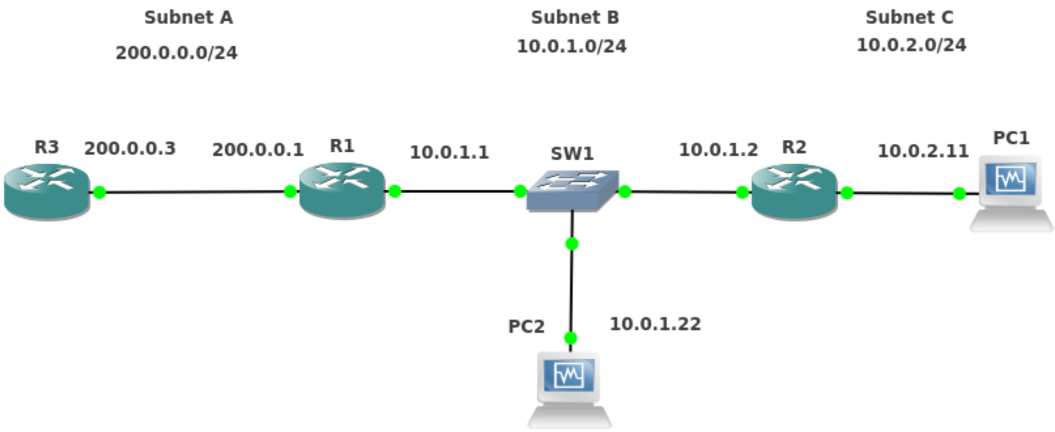
- When a router running network address translation is itself behind another NAT router.
- Normally implemented unknowingly in home or small business
- Example: connecting a wireless router to a modem provided by your ISP



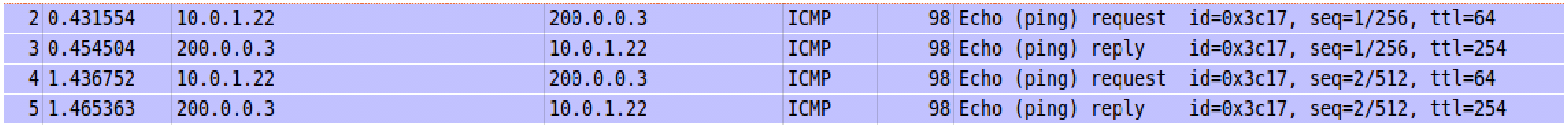
Goals of the Lab

- Successfully configure a double NAT topology
- Understand the address translation process while communicating between each subnet
- Determine if topology limits performance
- Discover how addressing problems can arise within the private network(s).

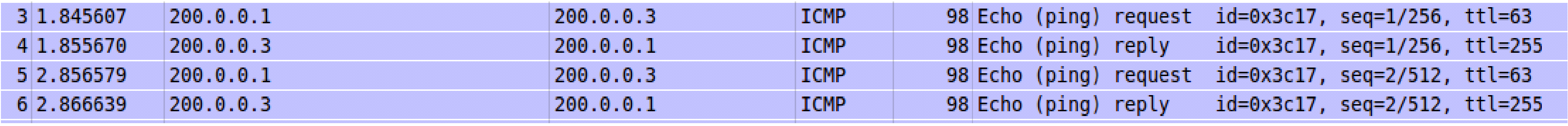
Topology 1



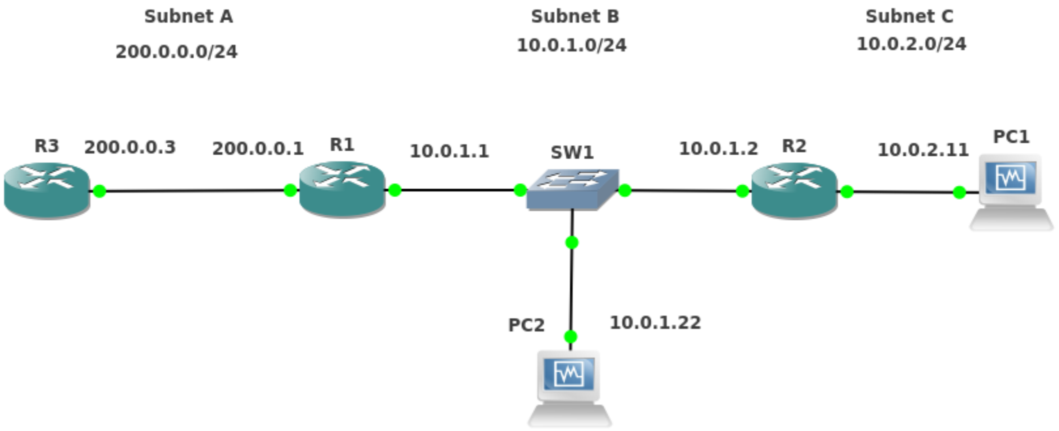
Pinging R3 from PC2



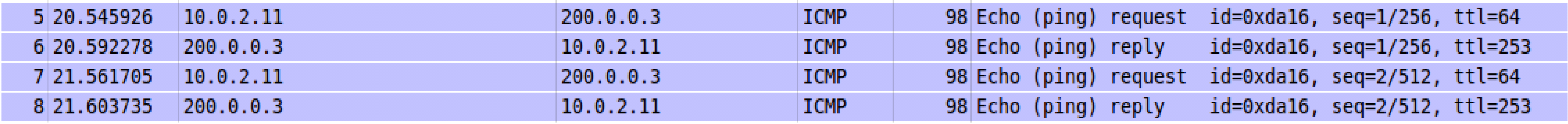
```
2 0.431554  10.0.1.22   200.0.0.3   ICMP   98 Echo (ping) request  id=0x3c17, seq=1/256, ttl=64
3 0.454504  200.0.0.3   10.0.1.22   ICMP   98 Echo (ping) reply    id=0x3c17, seq=1/256, ttl=254
4 1.436752  10.0.1.22   200.0.0.3   ICMP   98 Echo (ping) request  id=0x3c17, seq=2/512, ttl=64
5 1.465363  200.0.0.3   10.0.1.22   ICMP   98 Echo (ping) reply    id=0x3c17, seq=2/512, ttl=254
```



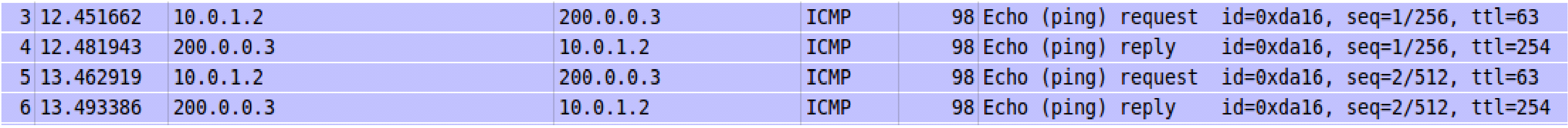
```
3 1.845607  200.0.0.1   200.0.0.3   ICMP   98 Echo (ping) request  id=0x3c17, seq=1/256, ttl=63
4 1.855670  200.0.0.3   200.0.0.1   ICMP   98 Echo (ping) reply    id=0x3c17, seq=1/256, ttl=255
5 2.856579  200.0.0.1   200.0.0.3   ICMP   98 Echo (ping) request  id=0x3c17, seq=2/512, ttl=63
6 2.866639  200.0.0.3   200.0.0.1   ICMP   98 Echo (ping) reply    id=0x3c17, seq=2/512, ttl=255
```



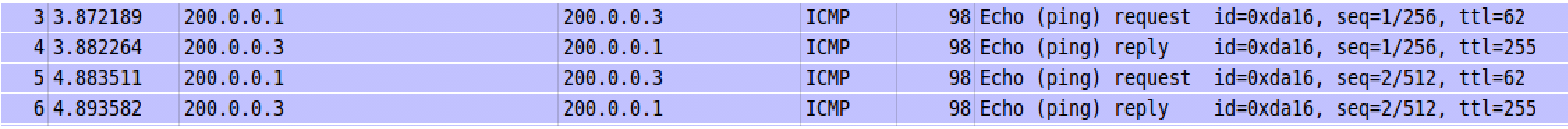
Issue a *ping* from PC1 to R3



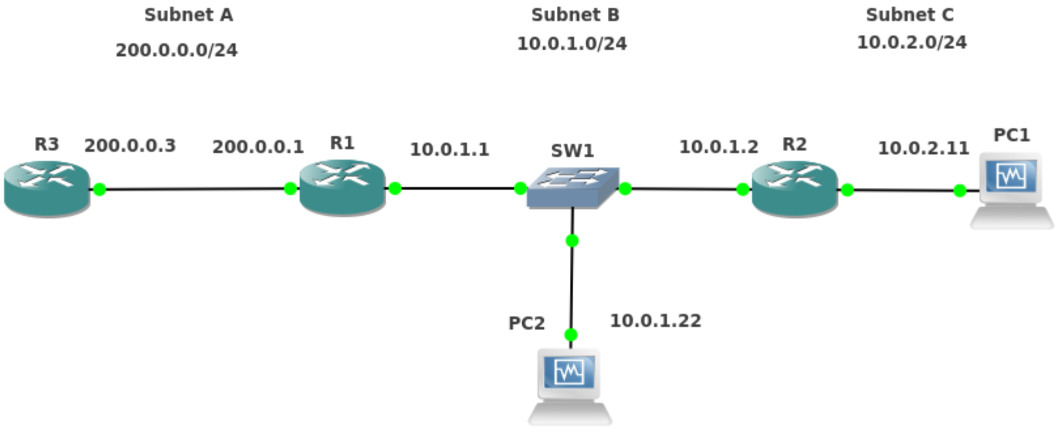
```
5 20.545926  10.0.2.11   200.0.0.3   ICMP   98 Echo (ping) request  id=0xda16, seq=1/256, ttl=64
6 20.592278  200.0.0.3   10.0.2.11   ICMP   98 Echo (ping) reply    id=0xda16, seq=1/256, ttl=253
7 21.561705  10.0.2.11   200.0.0.3   ICMP   98 Echo (ping) request  id=0xda16, seq=2/512, ttl=64
8 21.603735  200.0.0.3   10.0.2.11   ICMP   98 Echo (ping) reply    id=0xda16, seq=2/512, ttl=253
```



```
3 12.451662  10.0.1.2    200.0.0.3   ICMP   98 Echo (ping) request  id=0xda16, seq=1/256, ttl=63
4 12.481943  200.0.0.3   10.0.1.2    ICMP   98 Echo (ping) reply    id=0xda16, seq=1/256, ttl=254
5 13.462919  10.0.1.2    200.0.0.3   ICMP   98 Echo (ping) request  id=0xda16, seq=2/512, ttl=63
6 13.493386  200.0.0.3   10.0.1.2    ICMP   98 Echo (ping) reply    id=0xda16, seq=2/512, ttl=254
```



```
3 3.872189   200.0.0.1   200.0.0.3   ICMP   98 Echo (ping) request  id=0xda16, seq=1/256, ttl=62
4 3.882264   200.0.0.3   200.0.0.1   ICMP   98 Echo (ping) reply    id=0xda16, seq=1/256, ttl=255
5 4.883511   200.0.0.1   200.0.0.3   ICMP   98 Echo (ping) request  id=0xda16, seq=2/512, ttl=62
6 4.893582   200.0.0.3   200.0.0.1   ICMP   98 Echo (ping) reply    id=0xda16, seq=2/512, ttl=255
```

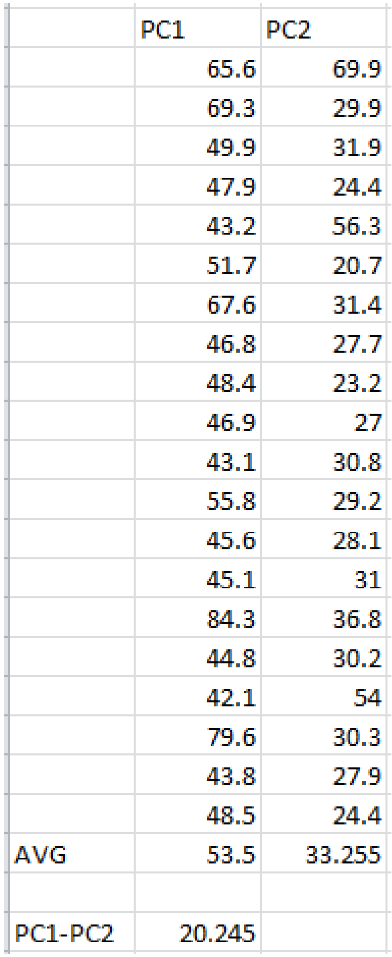


Subnet B and C are able to communicate since their IPv4 prefixes are necessarily different—R2 cannot have two interfaces with same IP prefix.

Examining Added Delay by 2nd NAT Router

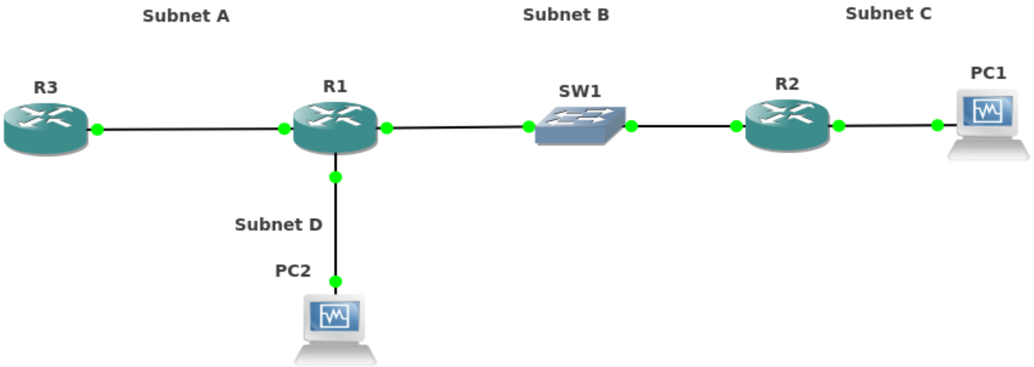
- Simultaneously *pinged* R3 from PC1 and PC2

- Took average delay in milliseconds over 20 ICMP messages for each host
- Average delay for PC1 was about 20.25 ms more than PC2
- Suggests double NAT topology will slightly impact performance of streaming applications



	PC1	PC2
	65.6	69.9
	69.3	29.9
	49.9	31.9
	47.9	24.4
	43.2	56.3
	51.7	20.7
	67.6	31.4
	46.8	27.7
	48.4	23.2
	46.9	27
	43.1	30.8
	55.8	29.2
	45.6	28.1
	45.1	31
	84.3	36.8
	44.8	30.2
	42.1	54
	79.6	30.3
	43.8	27.9
	48.5	24.4
AVG	53.5	33.255
PC1-PC2	20.245	

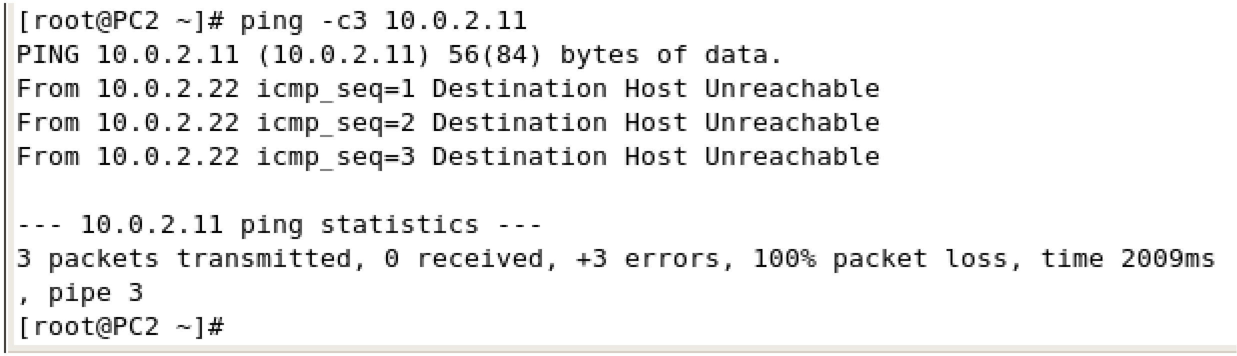
Topology 2



- PC2 is moved to a separate interface on R1, which is also NATed
- Configured Subnet D to have the *same* IP prefix as Subnet C

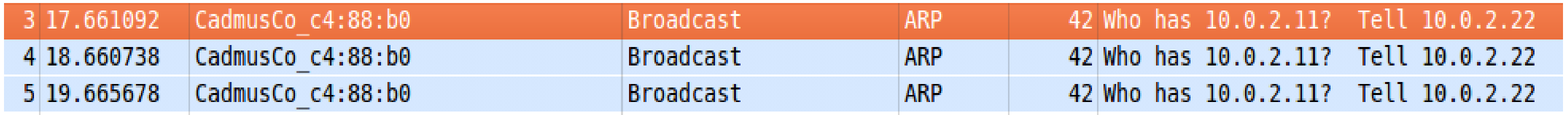
	Subnet A	Subnet B	Subnet C	Subnet D
IP prefix	200.0.0.0/24	10.0.1.0/24	10.0.2.0/24	10.0.2.0/24
R3	200.0.0.3			
R1	200.0.0.1	10.0.1.1		10.0.2.1
R2		10.0.1.2	10.0.2.2	
PC1			10.0.2.11	
PC2				10.0.2.22

Cannot communicate between Subnets C and D!



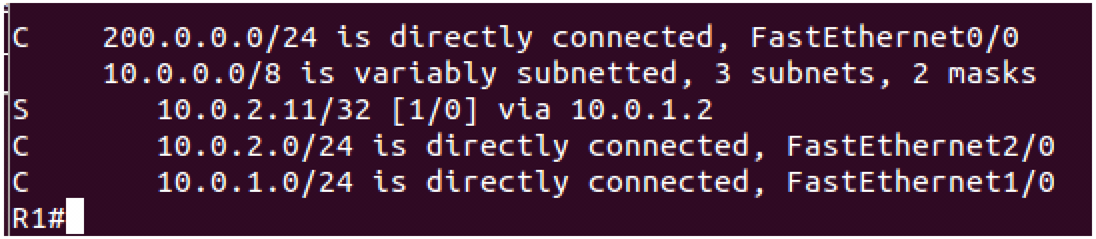
```
[root@PC2 ~]# ping -c3 10.0.2.11
PING 10.0.2.11 (10.0.2.11) 56(84) bytes of data.
From 10.0.2.22 icmp_seq=1 Destination Host Unreachable
From 10.0.2.22 icmp_seq=2 Destination Host Unreachable
From 10.0.2.22 icmp_seq=3 Destination Host Unreachable

--- 10.0.2.11 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2009ms
, pipe 3
[root@PC2 ~]#
```

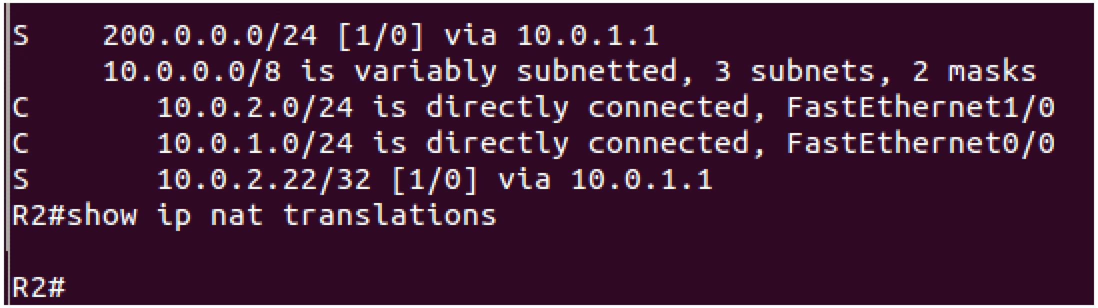


3	17.661092	CadmusCo_c4:88:b0	Broadcast	ARP	42	Who has 10.0.2.11? Tell 10.0.2.22
4	18.660738	CadmusCo_c4:88:b0	Broadcast	ARP	42	Who has 10.0.2.11? Tell 10.0.2.22
5	19.665678	CadmusCo_c4:88:b0	Broadcast	ARP	42	Who has 10.0.2.11? Tell 10.0.2.22

Solution: Static route to each host



```
C    200.0.0.0/24 is directly connected, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
S       10.0.2.11/32 [1/0] via 10.0.1.2
C       10.0.2.0/24 is directly connected, FastEthernet2/0
C       10.0.1.0/24 is directly connected, FastEthernet1/0
R1#
```

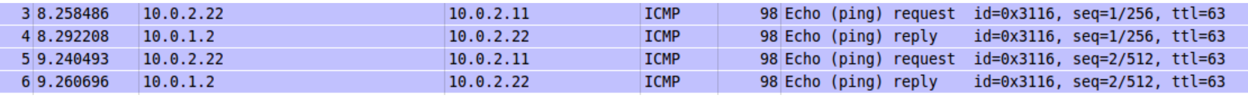


```
S    200.0.0.0/24 [1/0] via 10.0.1.1
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.0.2.0/24 is directly connected, FastEthernet1/0
C       10.0.1.0/24 is directly connected, FastEthernet0/0
S       10.0.2.22/32 [1/0] via 10.0.1.1
R2#show ip nat translations

R2#
```

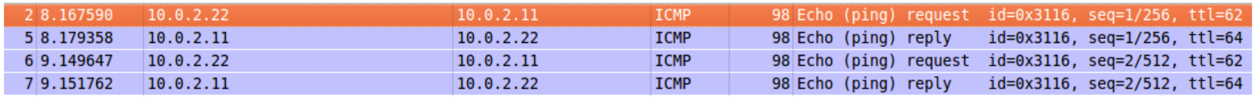
Connectivity is restored!

Packet capture on R2’s Subnet B interface



```
3 8.258486  10.0.2.22   10.0.2.11   ICMP   98 Echo (ping) request  id=0x3116, seq=1/256, ttl=63
4 8.292208  10.0.1.2    10.0.2.22   ICMP   98 Echo (ping) reply    id=0x3116, seq=1/256, ttl=63
5 9.240493  10.0.2.22   10.0.2.11   ICMP   98 Echo (ping) request  id=0x3116, seq=2/512, ttl=63
6 9.260696  10.0.1.2    10.0.2.22   ICMP   98 Echo (ping) reply    id=0x3116, seq=2/512, ttl=63
```

Packet capture on R2’s Subnet C interface

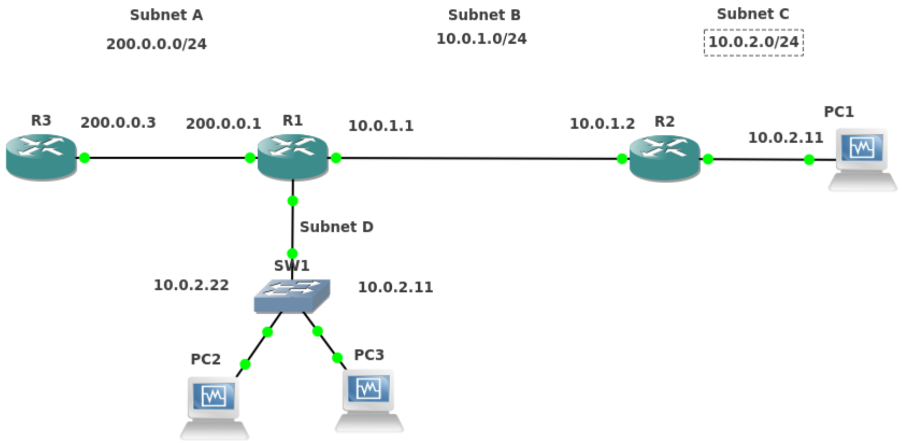


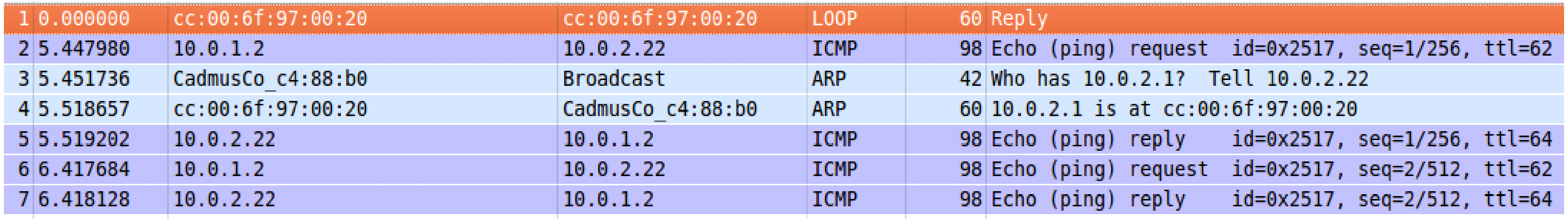
```
2 8.167590  10.0.2.22   10.0.2.11   ICMP   98 Echo (ping) request  id=0x3116, seq=1/256, ttl=62
5 8.179358  10.0.2.11   10.0.2.22   ICMP   98 Echo (ping) reply    id=0x3116, seq=1/256, ttl=64
6 9.149647  10.0.2.22   10.0.2.11   ICMP   98 Echo (ping) request  id=0x3116, seq=2/512, ttl=62
7 9.151762  10.0.2.11   10.0.2.22   ICMP   98 Echo (ping) reply    id=0x3116, seq=2/512, ttl=64
```

	Subnet A	Subnet B	Subnet C	Subnet D
IP prefix	200.0.0.0/24	10.0.1.0/24	10.0.2.0/24	10.0.2.0/24
R3	200.0.0.3			
R1	200.0.0.1	10.0.1.1		10.0.2.1
R2		10.0.1.2	10.0.2.2	
PC1			10.0.2.11	
PC2				10.0.2.22

A Subtle Potential for Problems…

- Add a second host onto Subnet D and give it the same IP address as the host on Subnet C
- Now PC2 cannot communicate directly with PC1, PC2 sends the message to PC3.
- However, communication can happen if PC1 initiates the message to PC2!





```
1 0.000000  cc:00:6f:97:00:20   cc:00:6f:97:00:20   LOOP   60 Reply
2 5.447980  10.0.1.2            10.0.2.22           ICMP   98 Echo (ping) request  id=0x2517, seq=1/256, ttl=62
3 5.451736  CadmusCo_c4:88:b0   Broadcast           ARP    42 Who has 10.0.2.1?  Tell 10.0.2.22
4 5.518657  cc:00:6f:97:00:20   CadmusCo_c4:88:b0   ARP    60 10.0.2.1 is at cc:00:6f:97:00:20
5 5.519202  10.0.2.22           10.0.1.2            ICMP   98 Echo (ping) reply    id=0x2517, seq=1/256, ttl=64
6 6.417684  10.0.1.2            10.0.2.22           ICMP   98 Echo (ping) request  id=0x2517, seq=2/512, ttl=62
7 6.418128  10.0.2.22           10.0.1.2            ICMP   98 Echo (ping) reply    id=0x2517, seq=2/512, ttl=64
```

Problems Encountered

- NAT overload (not in netref)
- This is equivalent to Port Address Translation—allows multiple internal addresses to be mapped to a single public address
- Simple solution

```
ip access-list standard NAT
permit 10.0.1.0 0.0.0.255
ip nat inside source list NAT interface fastEthernet 0/1 overload
```

Conclusions

- Double NAT isn’t “evil”, if it is configured well then it works, because NAT works!
- Performance impact is minimal
- Problem with topology is that people are usually unaware that it’s been implemented—makes troubleshooting a challenge
- Can be a simple way of segregating different parts of your network

NAT overload source

http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html

Questions?...