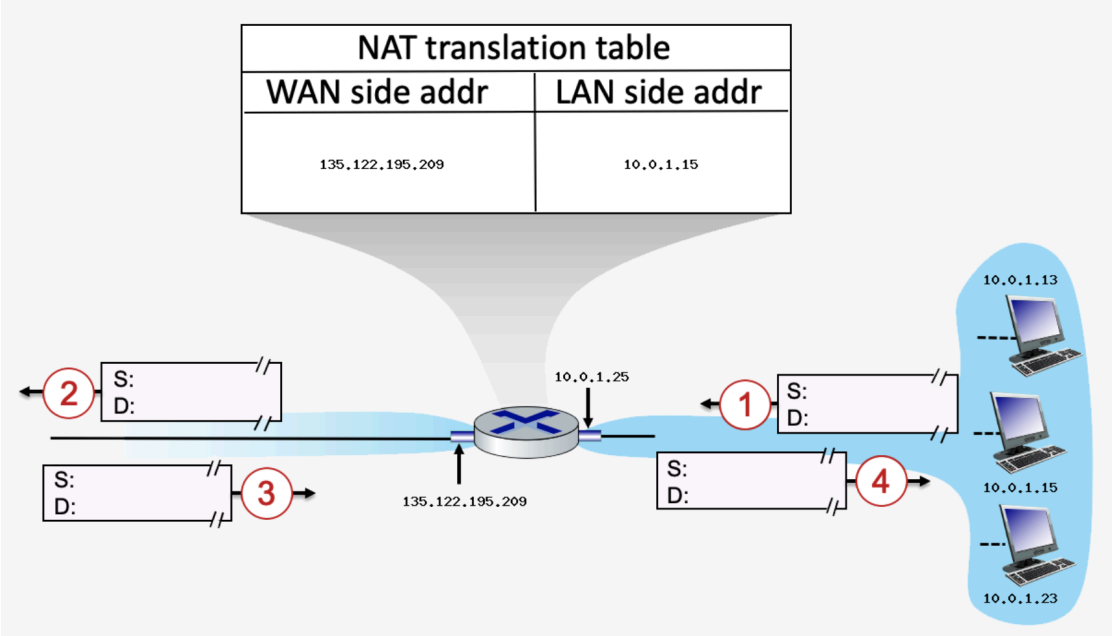
Worksheet Class-17: IPv6, NATs, DHCP

Q1.NAT: Consider the scenario below in which three hosts, with private IP addresses 10.0.1.13, 10.0.1.15, 10.0.1.23 are in a local network behind a NAT'd router that sits between these three hosts and the larger Internet.

IP datagrams being sent from, or destined to, these three hosts must pass through this NAT router. The router's interface on the LAN side has IP address 10.0.1.25, while the router's address on the Internet side has IP address 135.122.195.209

Suppose that the host with IP address 10.0.1.13 sends an IP datagram destined to host 128.119.169.188. The source port is 3327, and the destination port is 80.



Specify the source and destination addresses of packets 1 - 4.

1: Source: 10.0.1.13, 3327 Destination: 128.119.169.188, 80

2: Source:135.122.195.209, 5000 Destination:128.119.169.188, 80

3: Source:128.119.169.188, 80 Destination:135.122.195.209, 5000

4: Source:128.119.169.188, 80 Destination:10.0.1.13, 3327

Q2. When we use NATs, devices inside the local network are not explicitly addressable or visible to the outside world.

A) This is an advantage.
B) This is a disadvantage.

Q3. How do we feel about NATs?

A) NAT is great! It conserves IP addresses and makes it harder to reach non-public machines.
B) NAT is mostly good, but has a few negative features. No big deal.
C) NAT is mostly bad, but in some cases, it's a necessary evil.
D) NAT is an abomination that violates the end to end principle, and we should not use it!

Q4. How can we use IP fragmentation for evil?

A) Send fragments that overlap.
B) Send many tiny fragments, none of which have offset 0.
C) Send fragments that, when assembled, are bigger than the maximum IP datagram.
D) More than one of the above.
E) Nah, networks (and operating systems) are too robust for this to cause problems.