Network Address Translation (NAT)

- By default, a private IP network is completely isolated from the Internet.
- **NAT is a technique allowing hosts within a private network to communicate with the outside.**
- The combination of NAT and private networks is a particularly popular technique in IPv4 networks because the pool of available public IPv4 addresses is exhausted.

- Main principles:
  - A specific kind of router (often called “NAT gateway”) connects a private network N_{priv} to a public network N_{pub}
  - For each packet, this router performs two steps: (1) packet modification + (2) traditional routing
  - From the “outside”, the packets sent by hosts within N_{priv} seem to originate from the NAT router. In other words, the NAT router “hides” the hosts of the private network.

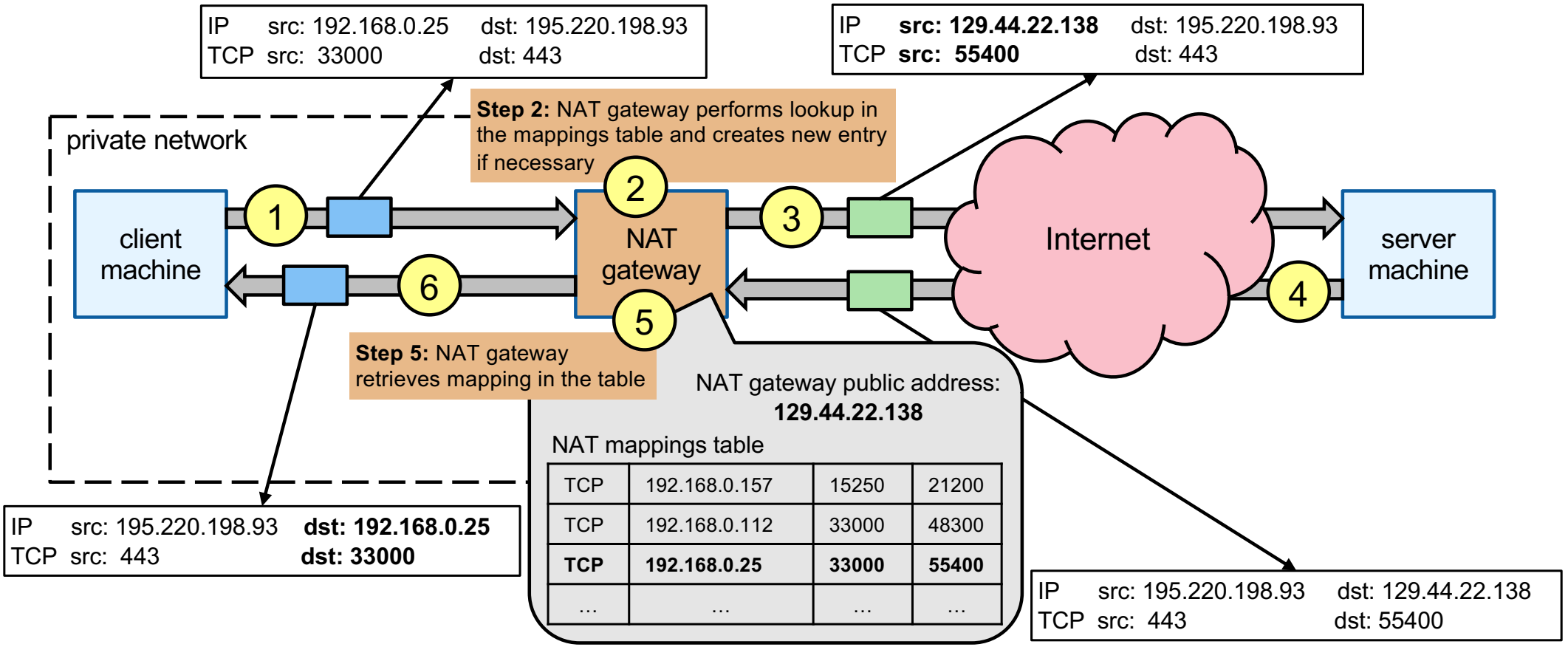
NAT – Details (1/3)

- **Packet modifications – IP addresses:**
  - **For outgoing packets:** When the router receives an IP packet from a host A in N_{priv}, the router modifies the "sender IP" in the packet (replacing A's address with its own address).
  - **For incoming packets:** When the router receives an IP packet from N_{pub}, the router modifies the "destination IP" in the packet (replacing the router's public address with the private address of the recipient in N_{priv}).

- **Packet modifications – Port numbers:**
  - In fact, **simply modifying the IP addresses is not sufficient**. The port numbers (in the TCP/UDP headers) must also be modified, because several hosts in N_{priv} can use the same (client or server) port numbers.
  - Therefore, in order to avoid ambiguity, the NAT router must remap the port numbers used by the client and server applications running on the hosts of N_{priv}.

NAT – Details (2/3)

- **Example scenario 1: TCP client on N_{priv} and TCP server on public network**



NAT – Details (3/3)

- **Example scenario 2: TCP client on public network and TCP server on N_{priv}**