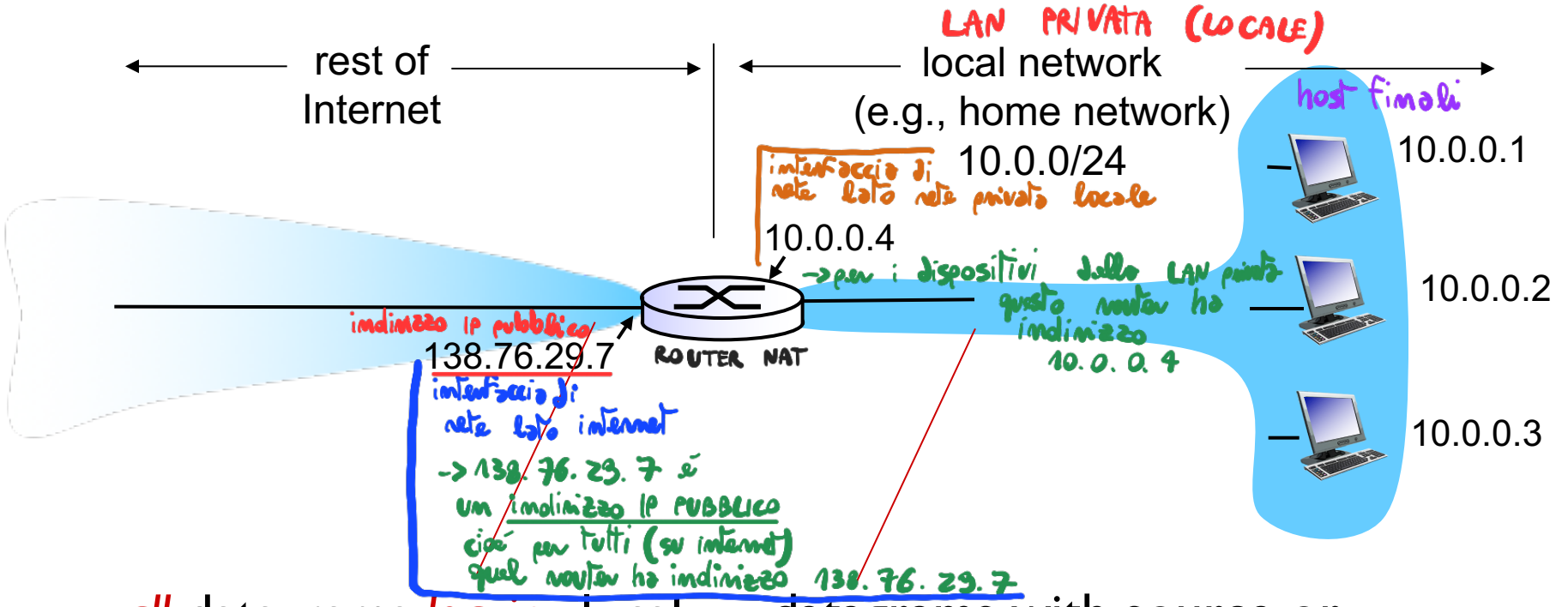
NAT: network address translation

protocollo NAT → viola lo standard ISO/OSI → stiamo mescolando livello rete e trasporto



all datagrams *leaving* local network have *same* single source NAT IP address: 138.76.29.7,different source port numbers

datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)

NAT: network address translation

motivation: local network uses just one IP address as far as outside world is concerned:

- range of addresses not needed from ISP: just one IP address for all devices
- can change addresses of devices in local network without notifying outside world
- can change ISP without changing addresses of devices in local network
- devices inside local net not explicitly addressable, visible by outside world (a security plus)

NAT: network address translation

implementation: NAT router must:

- *outgoing datagrams: replace* (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)

  . . . remote clients/servers will respond using (NAT IP address, new port #) as destination addr

- *remember (in NAT translation table)* every (source IP address, port #) to (NAT IP address, new port #) translation pair

- *incoming datagrams: replace* (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table

N.B. Se io ho un nome di dominio di una macchina in una LAN PRIVATA, es. 10.0.0.1 NON è un'indirizzo IP pubblico → SERVE IL PORT MAPPING (che fa la NAT TRANSLATION TABLE)

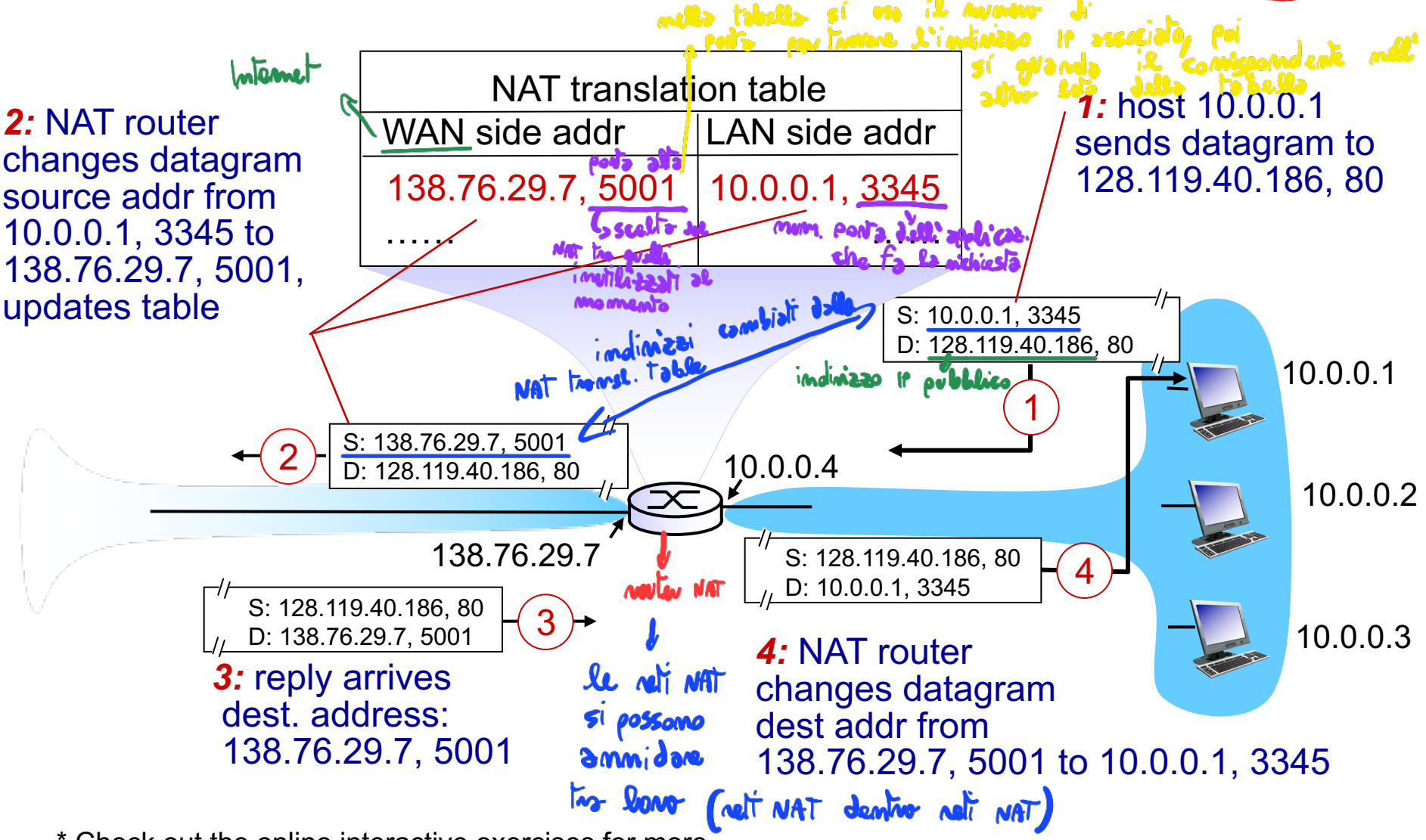
Il PORT MAPPING sfrutta il fatto di mappare gli indirizzi IP grazie alle porte e permette di raggiungere le macchine locali di interesse.

Nell'esempio di prima voglio 10.0.0.1
devo usare il PORT MAPPING così da sapere che l'indirizzo pubblico che mi permette di raggiungere quella macchina 136.76.29.7

- Attacco PORT SCANNING: l'attaccante, non avendo fatto richiesta, non sa l'indirizzo privato associato alla macchina da attaccare, l'unico modo è tentare di beccare la porta giusta (→ tanti tentativi) per attraversare il NAT ed entrare nella rete, anche se non sai chi stai contattando e quali servizi. Magari hai aperto la connessione e devi cercare di indovinare la porta giusta per il servizio che fa quella specifica macchina
  → Porta ad insospettirsi
  → se ci sono più NAT diventa lungo il port scanning e facilmente sgamabile

La NAT translation table usa la tecnica del "MASQUERADE": vuol dire cambiare un indirizzo IP

NAT: network address translation



* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

NAT: network address translation

- 16-bit port-number field:
  - 60,000 simultaneous connections with a single LAN-side address!
- NAT is controversial:
  - routers should only process up to layer 3
  - address shortage should be solved by IPv6
  - violates end-to-end argument
    - NAT possibility must be taken into account by app designers, e.g., P2P applications
  - NAT traversal: what if client wants to connect to server behind NAT?