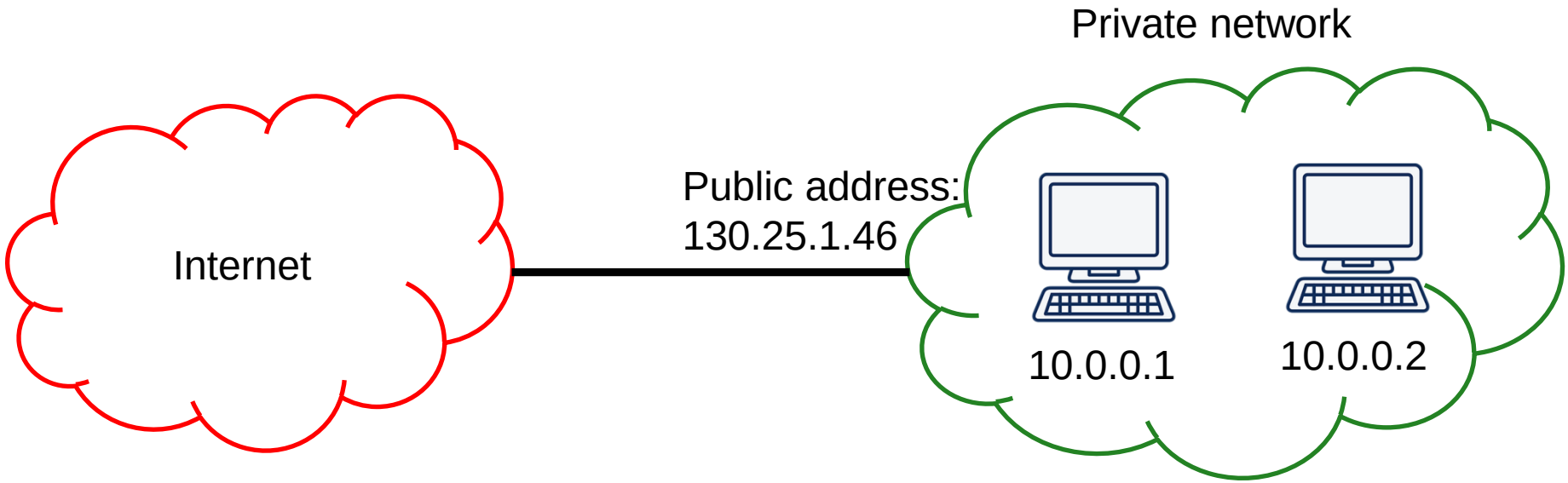
Network Address Translation

Ramin Sadre

Scenario

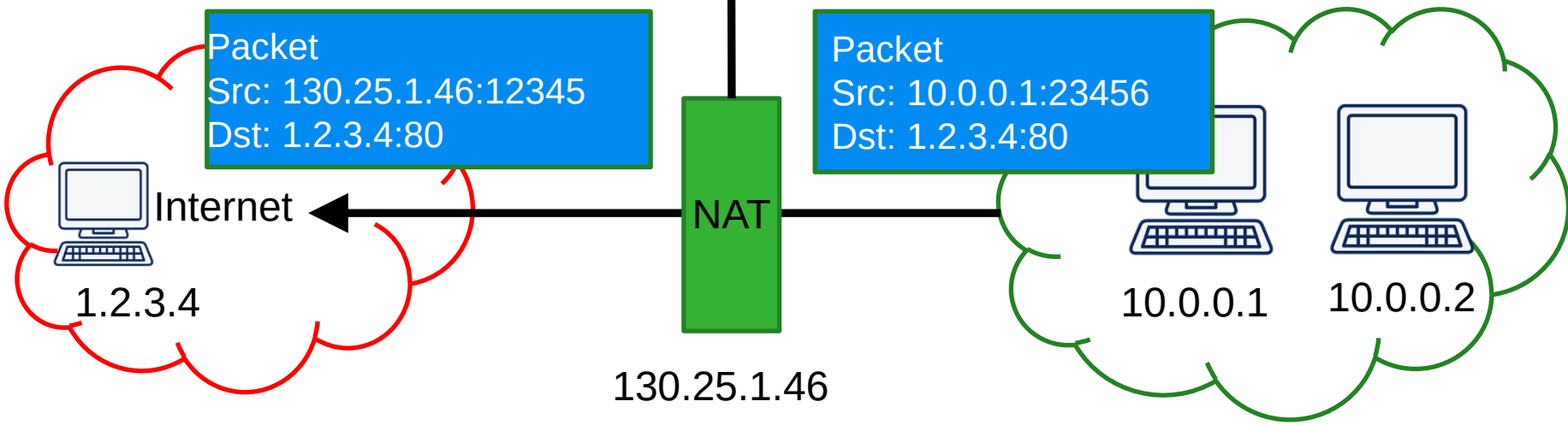
- Imagine your network at home
  - Your ISP gives you only one IP address for your home
  - Inside your home network, all hosts have private (non-routable) IP addresses



How NATs work on outgoing packets

- NAT manipulates packets on network and transport layer
- The NAT replaces
  - the source IP address of an outgoing packet by the public address
  - the source port by an arbitrary unused port

Protocol	Local address and port	Peer address and port	Local port replaced by
…	…	…	…
TCP	10.0.0.1:23456	1.2.3.4:80	12345
…	…	…	…



How it works: Outgoing packets (2)

- The NAT keeps an internal translation table

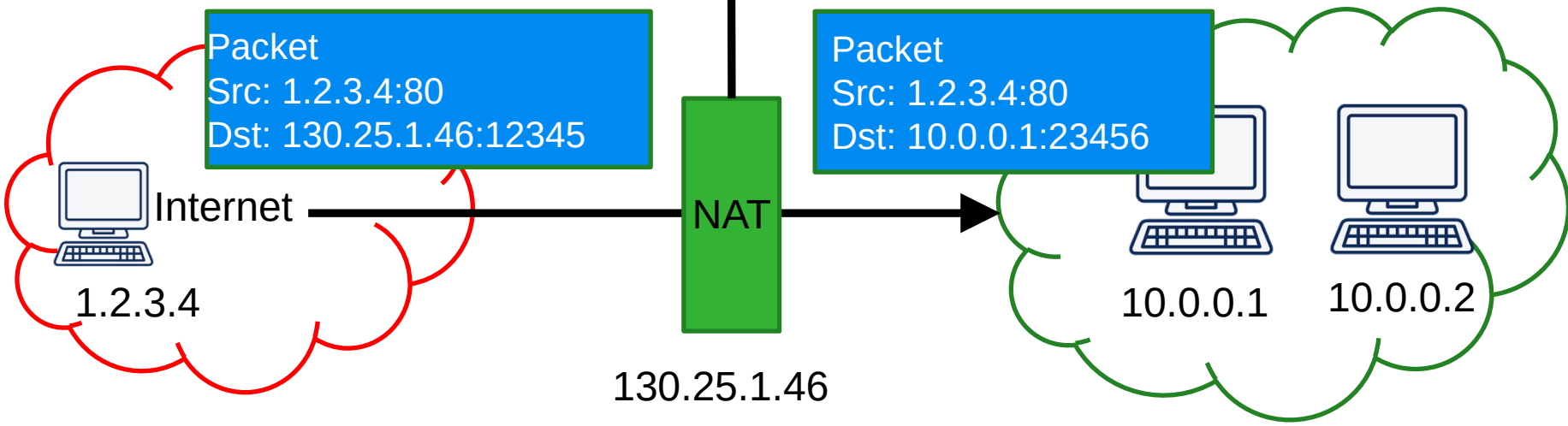
Protocol	Local address and port	Peer address and port	Local port replaced by
…	…	…	…
TCP	10.0.0.1:23456	1.2.3.4:80	12345
…	…	…	…

- Complete procedure for outgoing packets:
  1. Check whether there is already a matching entry in the table
  2. If no entry found, insert a new entry to the table
  3. Replace address and port number in the packet

How NATs work on incoming packets

- Incoming packets are translated back using the table
- Procedure:
  1. Check whether there is a matching entry in the table
  2. If no entry found, drop the packet!!! Else: replace destination address and port number in packet

Protocol	Local address and port	Peer address and port	Local port replaced by
…	…	…	…
TCP	10.0.0.1:23456	1.2.3.4:80	12345
…	…	…	…



Static table entries

- By default, outgoing connections will get a random port number assigned
- NAT also allows to add static entries to the translation table
- Example: Make a web server on port 8080 in the local network available to the outside world on port 80

Protocol	Local address and port	Peer address and port	Local port replaced by
TCP	10.0.0.1:8080	*	80

Advantages of NATs

- Entire private network only needs one public IP address
  - NAT was originally invented to delay the depletion of public IPv4 addresses
- Side effect: the hosts inside the private network are not anymore directly reachable from the Internet
  - Effect similar to firewall
  - NAT rejects all incoming connections
- But: NAT was not intended as a security solution
  - Every entry in the translation table “punches a hole” in your perimeter

Advantages (2)

- NAT can hide sequentially incrementing source port number

Local host's source port	Random source port used by NAT
10000	12345
10001	23456
10002	34567
…	…

This gives additional protection against spoofed packets that try to guess the source port (e.g. DNS cache poisoning)

Drawbacks

- NAT violates the separation of protocol layers
  - Often implemented on routers (= network layer)
  - NAT manipulates port numbers (= transport layer)
- NAT makes network debugging and forensic analysis of network traffic harder
  - Hosts behind a NAT are not individually visible in a packet trace
- An incorrectly implemented NAT might not choose port numbers randomly and makes them predictable for attacks

Drawbacks (2)

- Resource intensive
  - NAT has to recalculate checksums
  - Some application protocols, e.g. FTP, refer to the local port number **inside** the application message

    → NAT has to analyze the packet content

- NATs (similar to firewalls) break the *end-to-end* principle of the Internet
  - Two hosts between different NATs cannot communicate directly. Problem for P2P protocols.
  - The omni-presence of NATs in the Internet makes it very hard to deploy new protocols: Many NATs drop packets that they don't understand

Attacks against NATs

- Question: Can a NAT run out of available port numbers?
- Possible scenario:
  - Attacker inside the company network sends many SYN packets to different IP addresses
  - Result: NAT has used all its port numbers, no new outgoing connections possible for other hosts in the company network

Attacks against NATs (2)

1. Most NATs would probably already run out of memory after 10,000 or 20,000 connections

2. The TCP specification does actually not forbid to use the same source port for different connections as long as the destination address&port are unique!

   → If you have NAT port 12345 for connections to server 1.2.3.4, the NAT can still use that port for connections to other servers

Conclusion: Depends on implementation.