NAT traversal w sieciach p2p

—

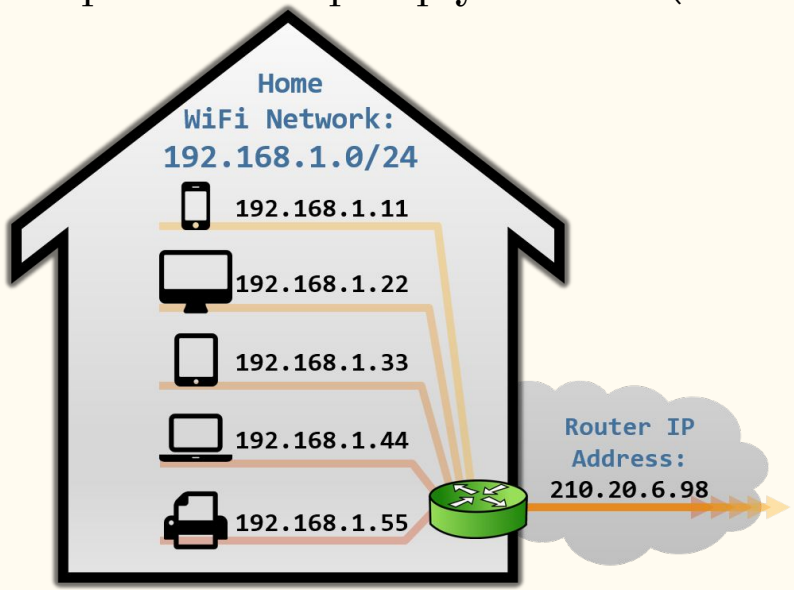
Stanisław Barański
https://stan.bar

20.10.2018

Czym jest NAT ?

Network Address Translation

Metoda przesyłania ruchu sieciowego poprzez router, która wiąże się ze zmianą źródłowych lub docelowych adresów IP. Zwykle również numerów portów TCP/UDP pakietów IP podczas ich przepływu PAT (Port Address Translation).



Sesja NAT

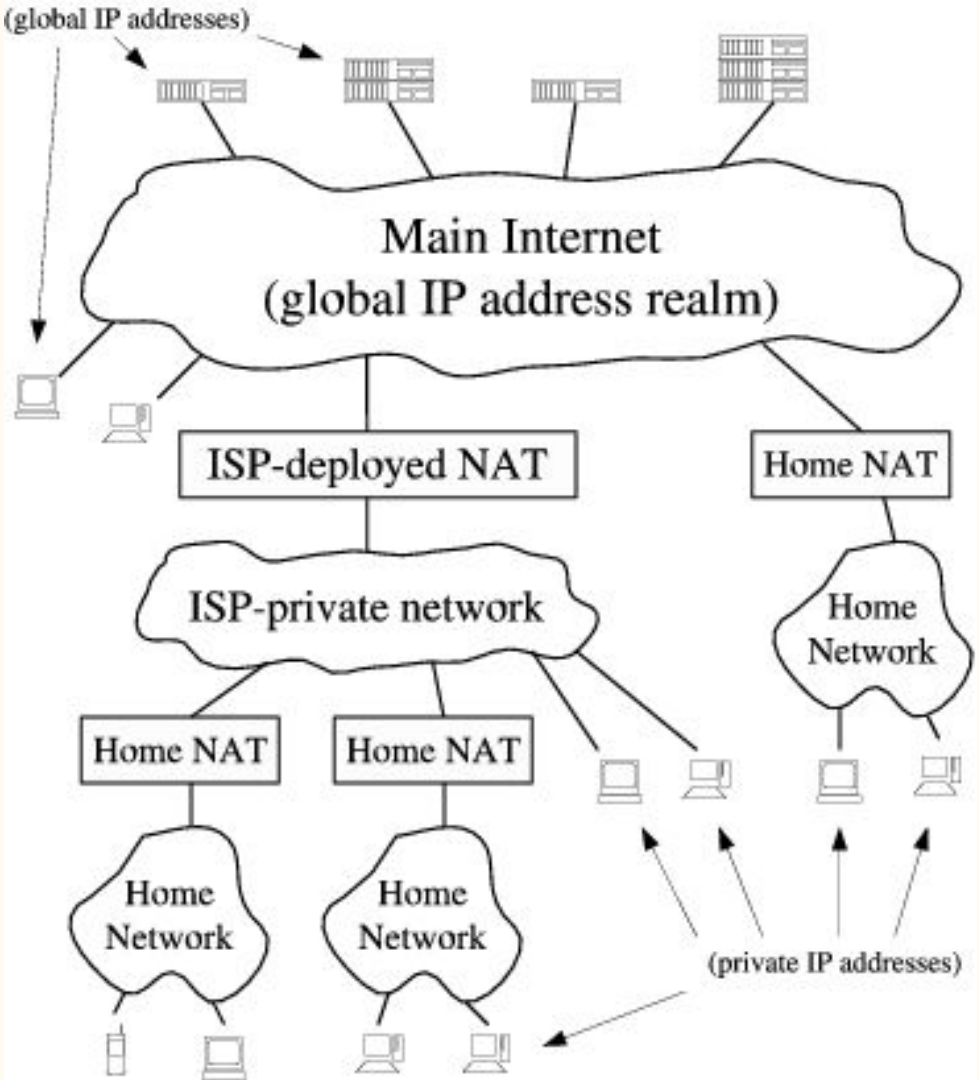
Sesja to dwie pary (Adres Lokalny:Port Lokalny, Adres Publiczny:Port Publiczny)

Kierunek sesji jest określany przez pierwszy pakiet który otwiera sesję SYN dla TCP, lub pierwszy pakiet dla UDP

Najpopularniejszym NATem jest outbound NAT, który jest asymetrycznym mostem pomiędzy prywatną siecią a publiczną siecią.

Outbound NAT pozwala tylko na inicjowanie połączeń ze strony sieci prywatnej, połączenia przychodzące dla których nie ma sesji NAT zostają odrzucone.

Adres Lokalny	Port Lokalny	Adres Publiczny	Port Publiczny
192.168.1.100	80	212.45.19.17	10000
192.168.1.200	80	212.45.19.17	10001


(global IP addresses)
Main Internet
(global IP address realm)
ISP-deployed NAT
Home NAT
ISP-private network
Home
Network
Home NAT
Home NAT
Home
Network
Home
Network
(private IP addresses)

Dlaczego potrzebny jest NAT?

Brak konieczności re-adresacji hostów podczas przenoszenia sieci.

Wyczerpanie publicznych adresów IPv4

Jaki wpływ na działanie sieci p2p ma NAT ?

Konflikt w sieciach p2p

Kiedy klient sieci p2p będący za NATem chce nawiązać połączenie z drugim klientem będącym za NATem powstaje konflikt, ponieważ połączenia inicjujące zostają odrzucane przez NAT drugiej strony.

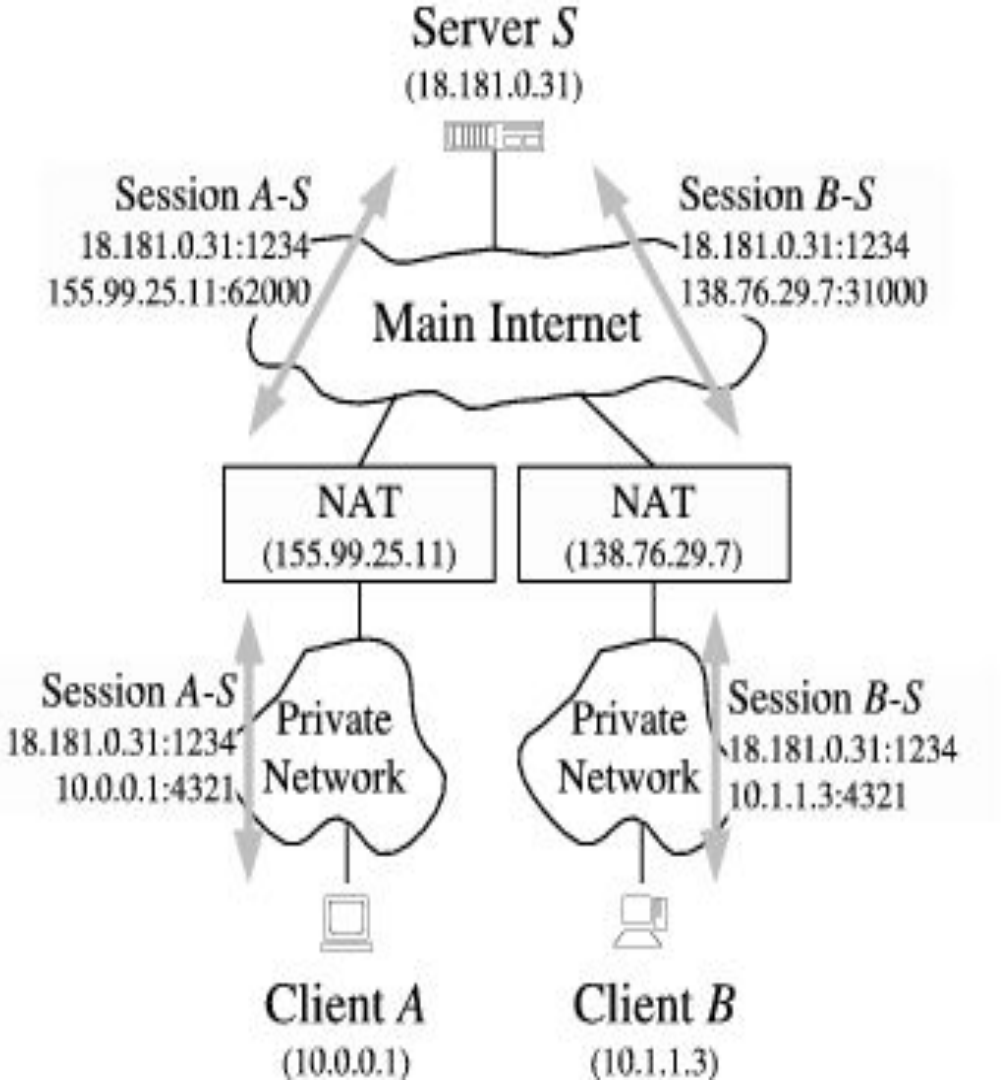
NAT pociąga za sobą konieczność budowania sesji p2p w taki sposób, aby dla każdej strony wyglądały na sesje wychodzące z sieci prywatnej.

Jak radzić sobie z problemem NATów w sieciach p2p

Relaying

TURN - Traversal Using Relays around NAT

1. Najbardziej niezawodne i najmniej wydajne rozwiązanie - zamienić p2p na klient-serwer
2. Serwer jako pośrednik wiadomości od Alice do Boba
3. Wady: Single point of failure, opóźnienia, koszty zasobów i łącza

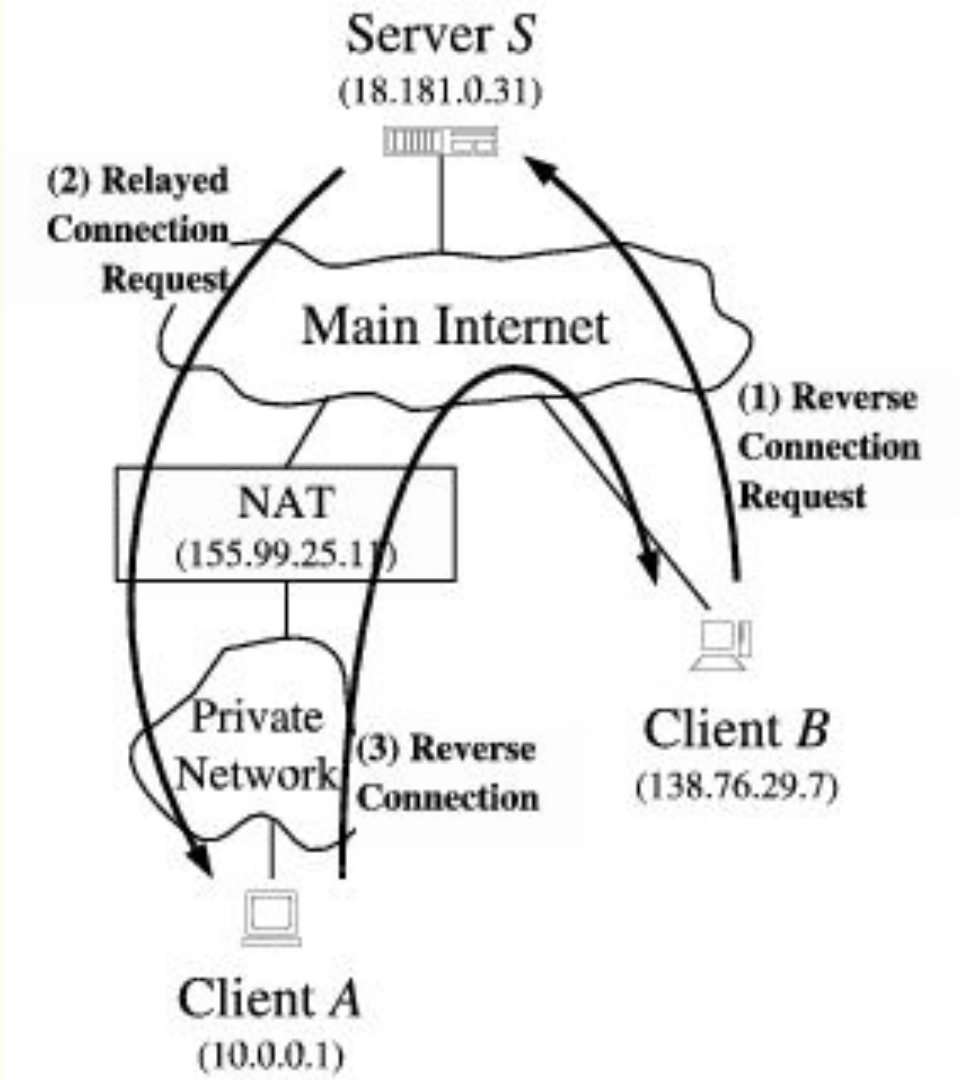


Connection Reversal

1. Technika wymagająca, aby jedna ze stron miała publiczny adres IP.

2. Serwer rendezvous pośredniczy tylko w ustanowieniu połączenia pomiędzy Alice i Bobem.

3. Jeśli Bob chce ustanowić połączenie z Alice, prosi serwer rendezvous, aby ten poinformował Alice, aby to ona zainicjowała połączenie, tym samym otworzyła sesję w NAT'cie.

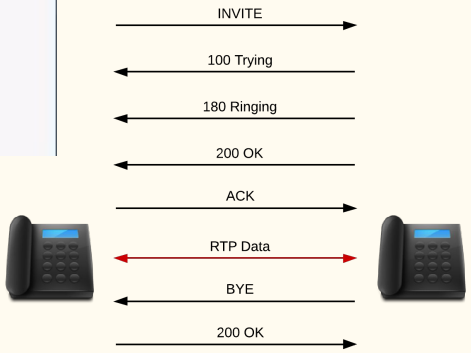


UDP Hole Punching

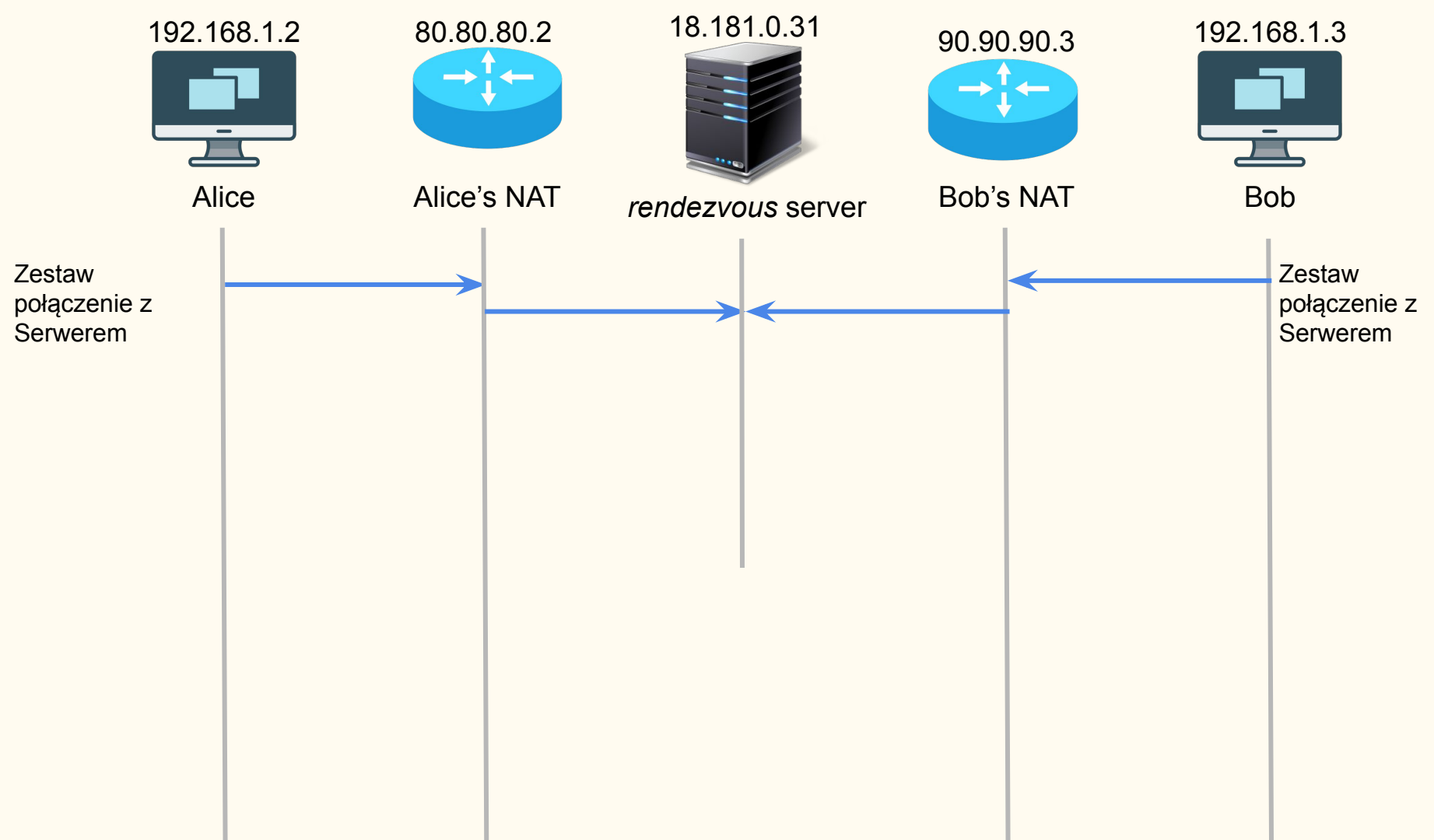
- Działa we wszystkich konfiguracjach NATa, (Jeden host za NATem, Oba hosty za NATem oraz maskarady).
- Wymaga, aby oba hosty miały zestawioną sesję ze znanym serwerem *rendezvous*.

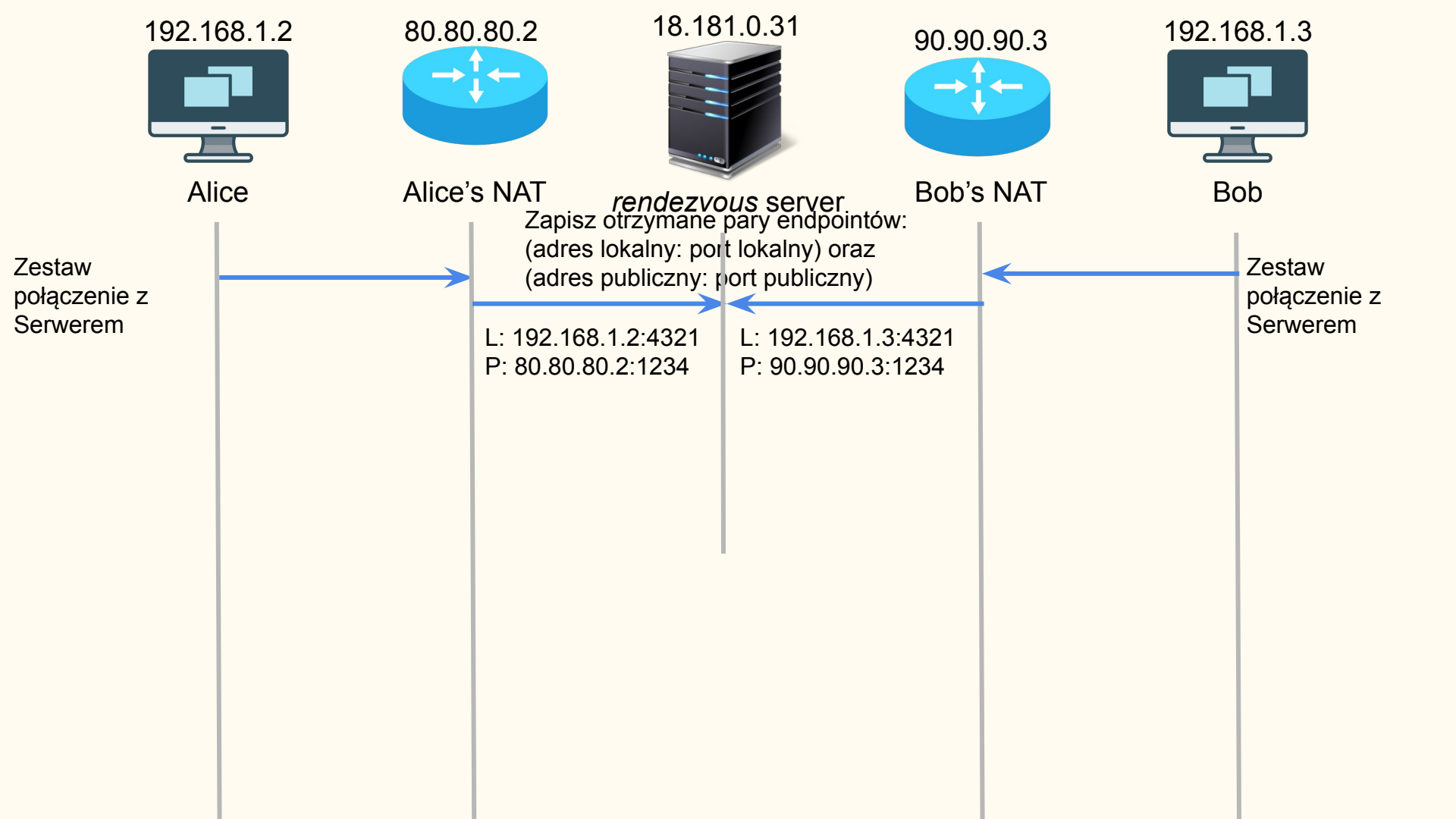
BitTorrent™

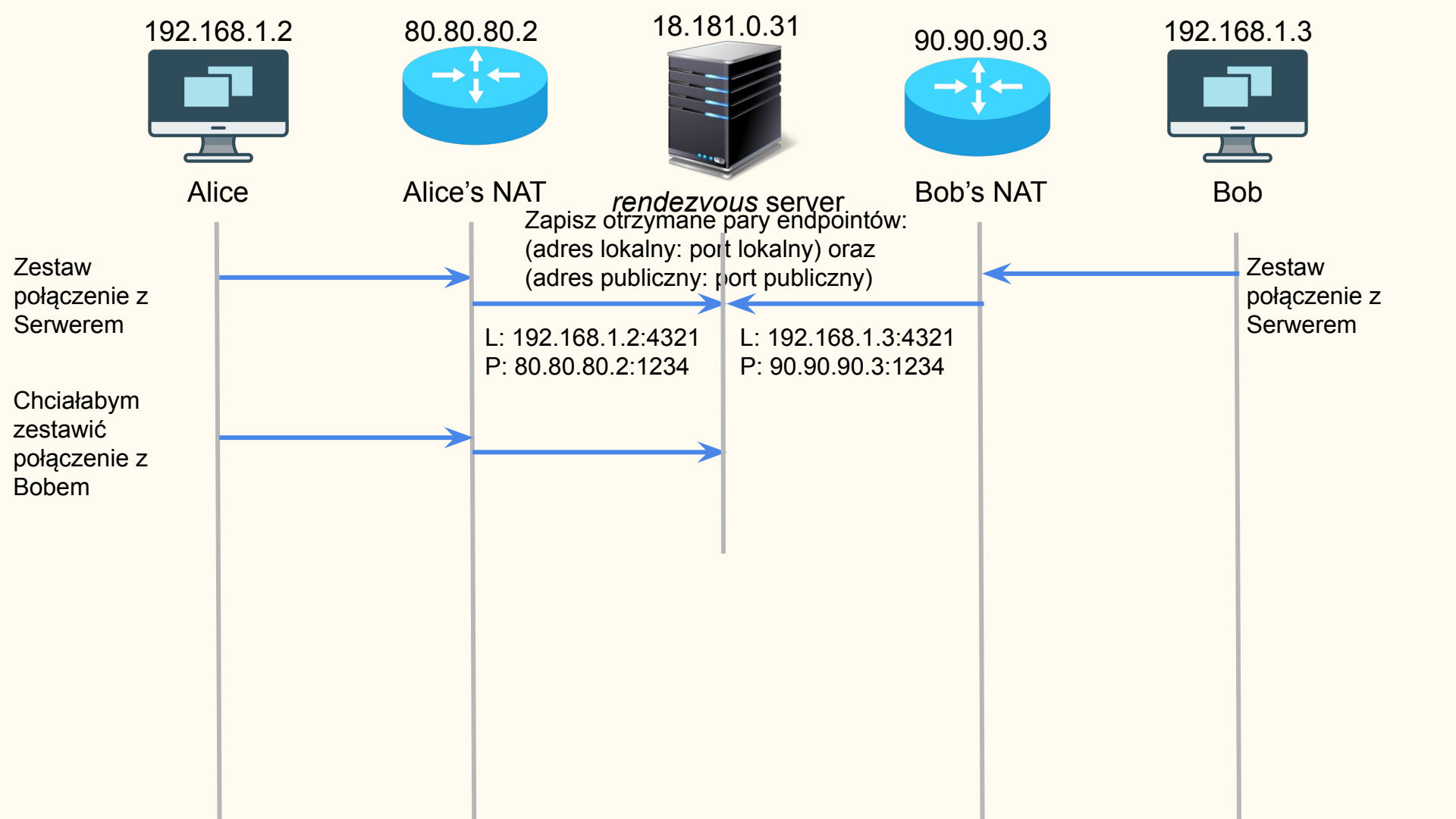
Gdzie stosowany

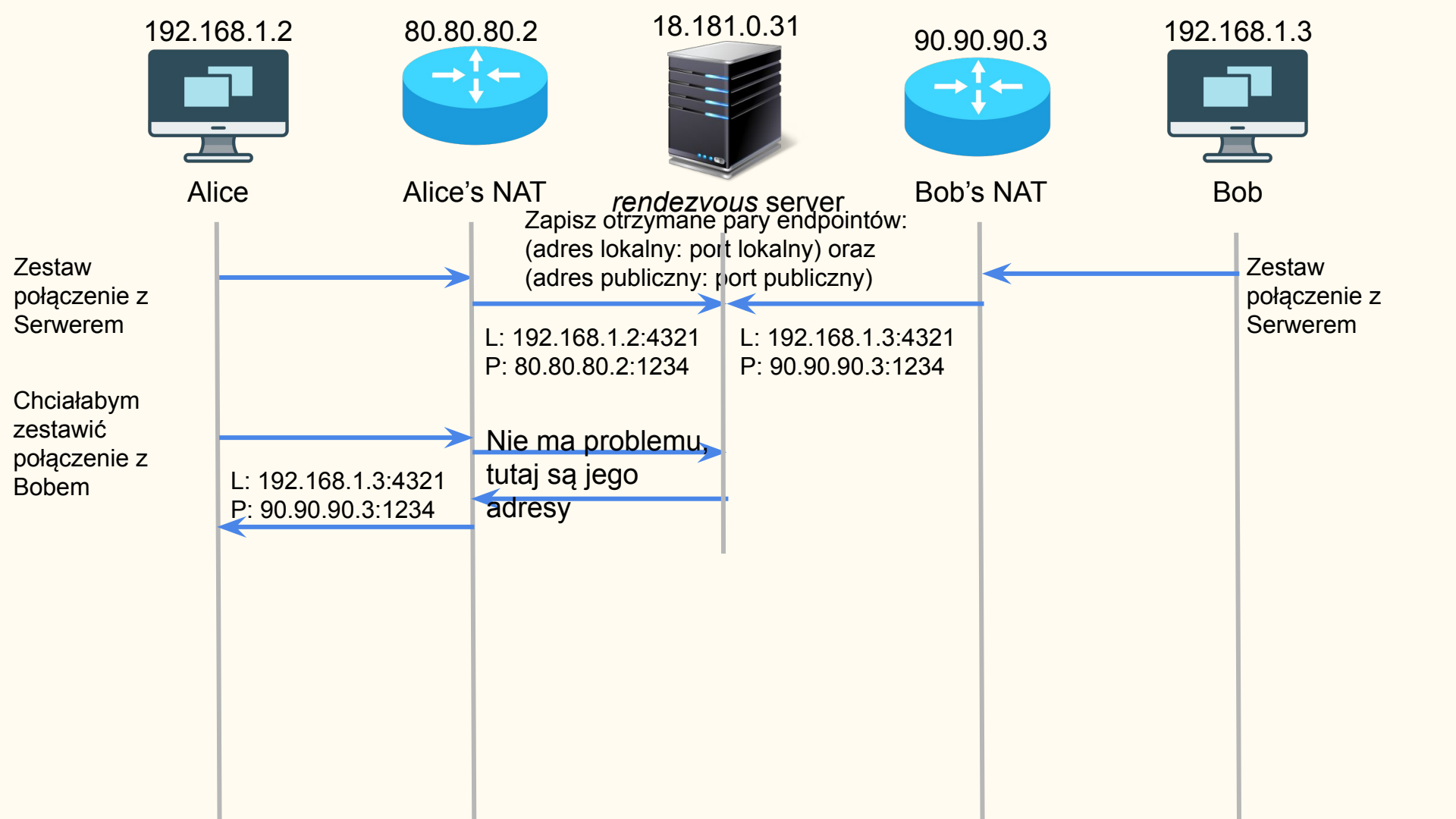


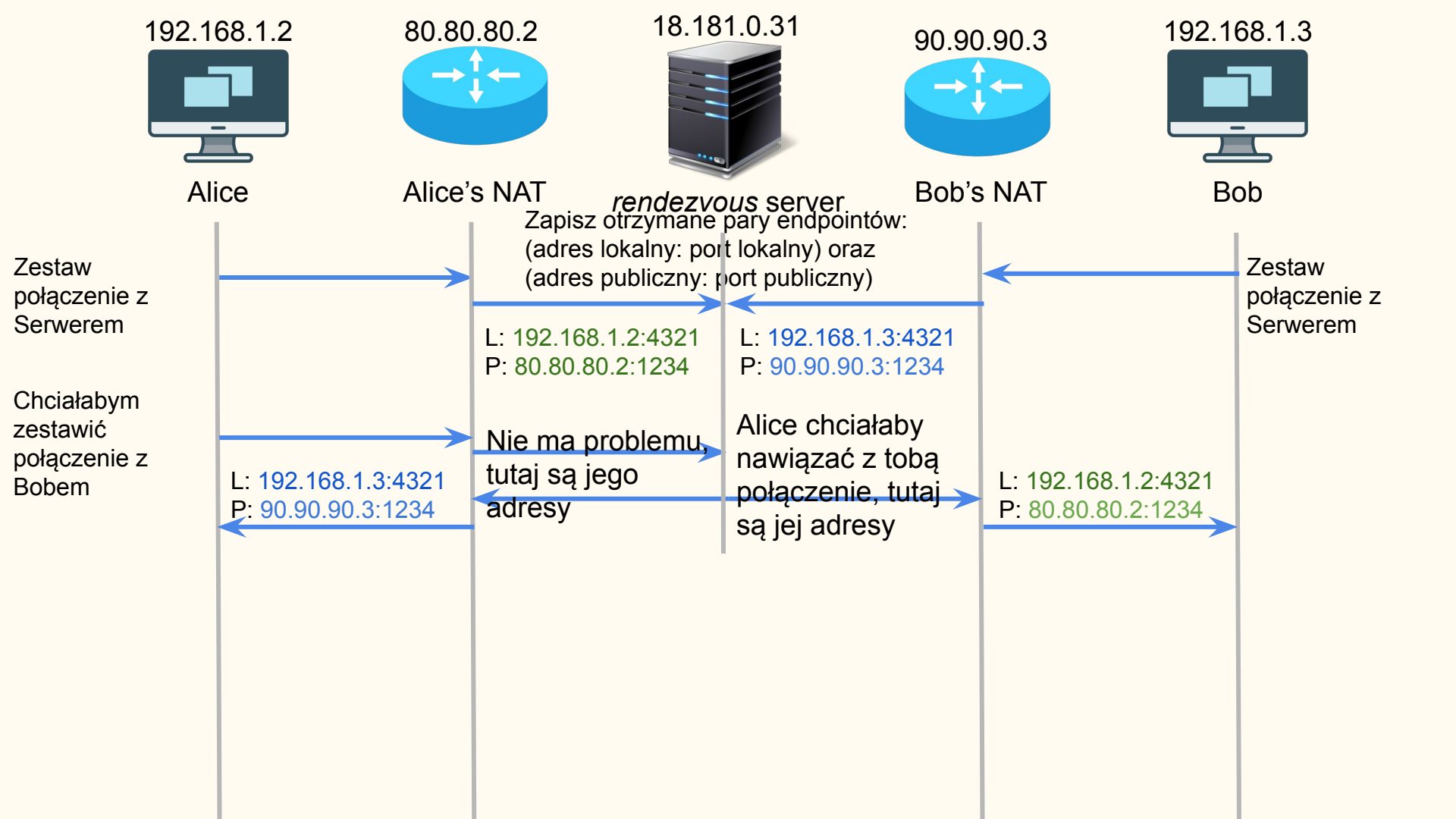
LogMeIn Hamachi

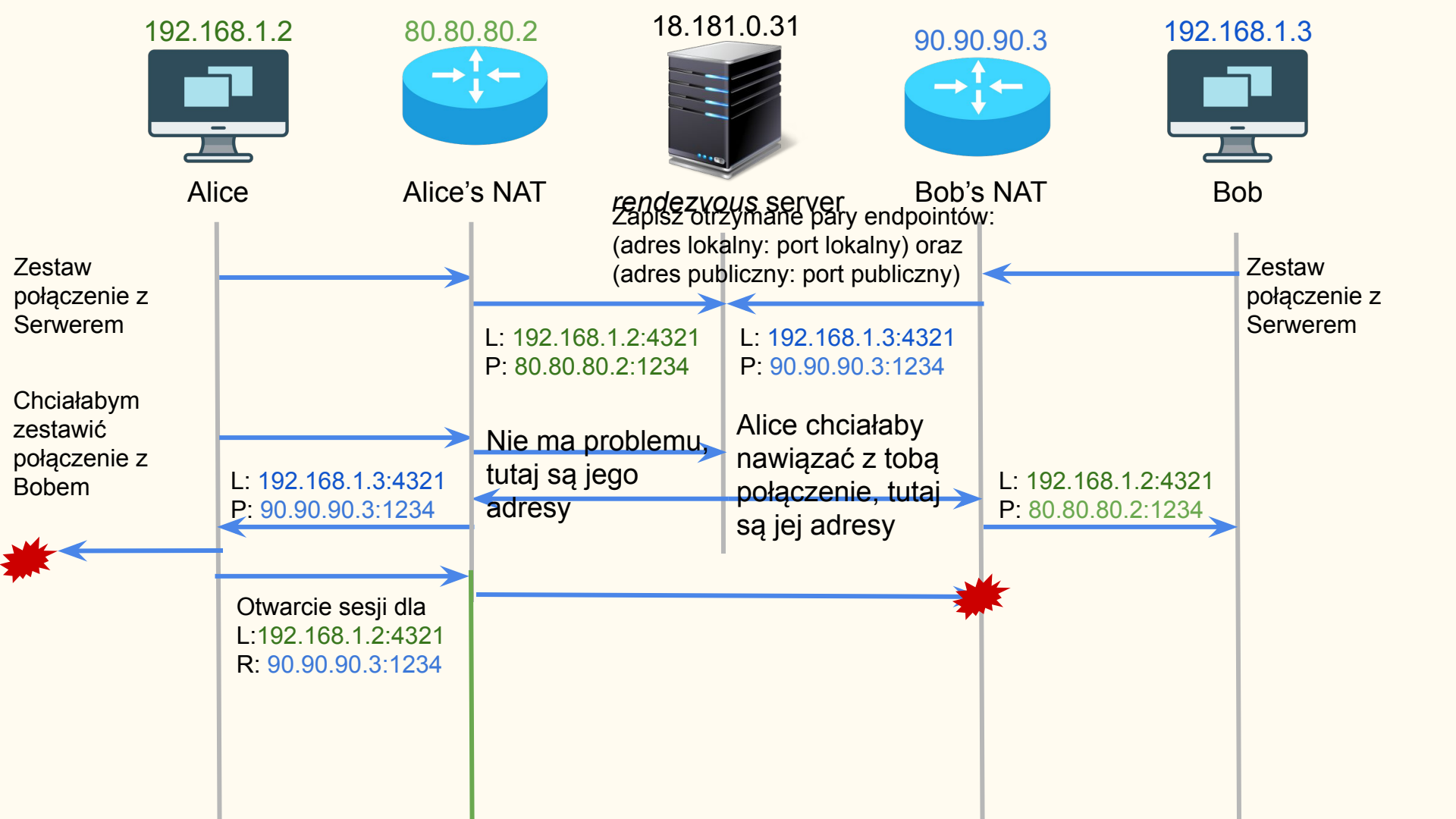

192.168.1.2
80.80.80.2
18.181.0.31
90.90.90.3
192.168.1.3
Alice
Alice's NAT
rendezvous server
Bob's NAT
Bob
Zestaw połączenie z Serwerem
Zestaw połączenie z Serwerem

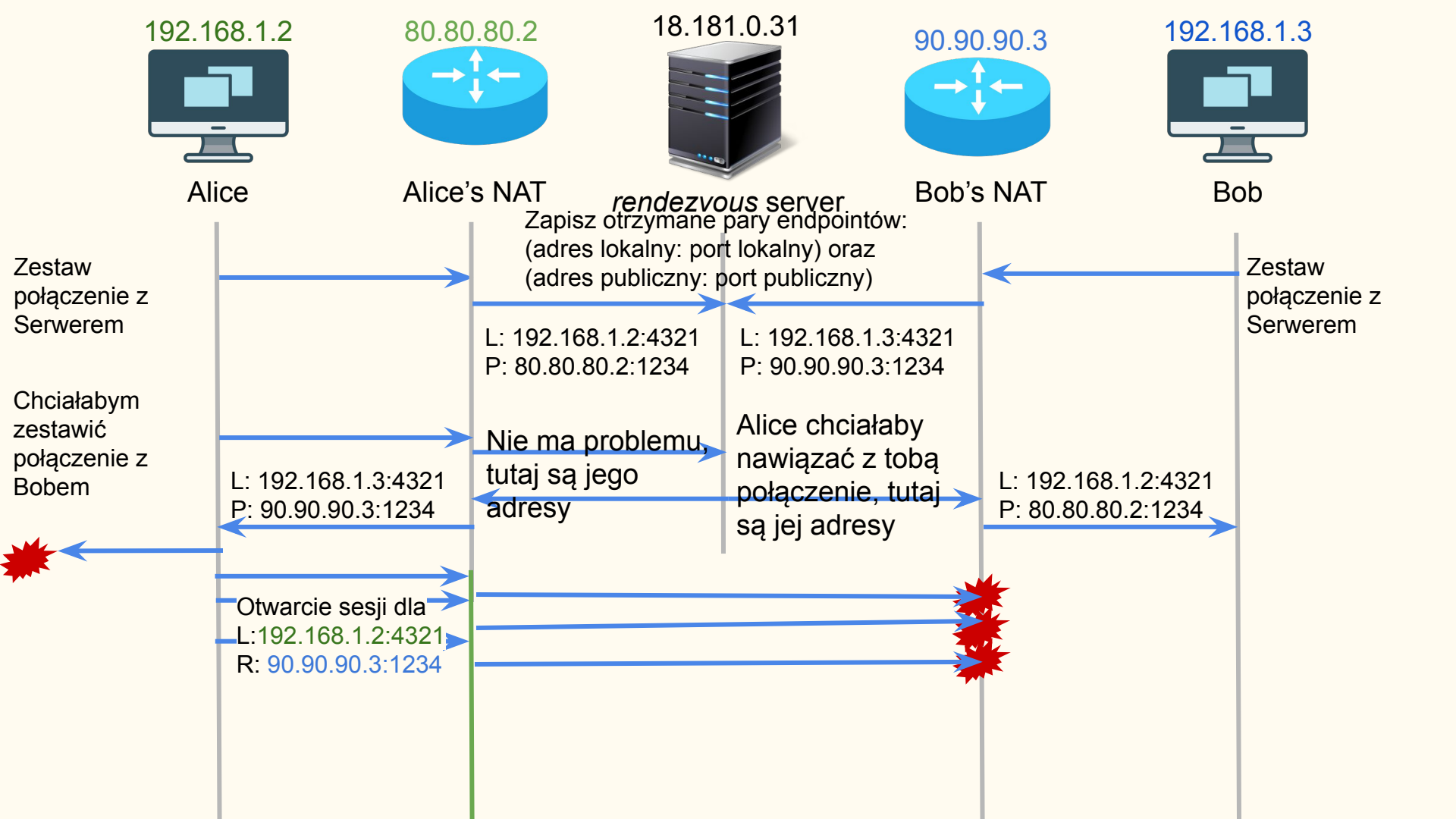

192.168.1.2
80.80.80.2
18.181.0.31
90.90.90.3
192.168.1.3
Alice
Alice's NAT
rendezvous server
Bob's NAT
Bob
Zapisz otrzymane pary endpointów:
(adres lokalny: port lokalny) oraz
(adres publiczny: port publiczny)
Zestaw połączenie z Serwerem
Zestaw połączenie z Serwerem
L: 192.168.1.2:4321
P: 80.80.80.2:1234
L: 192.168.1.3:4321
P: 90.90.90.3:1234

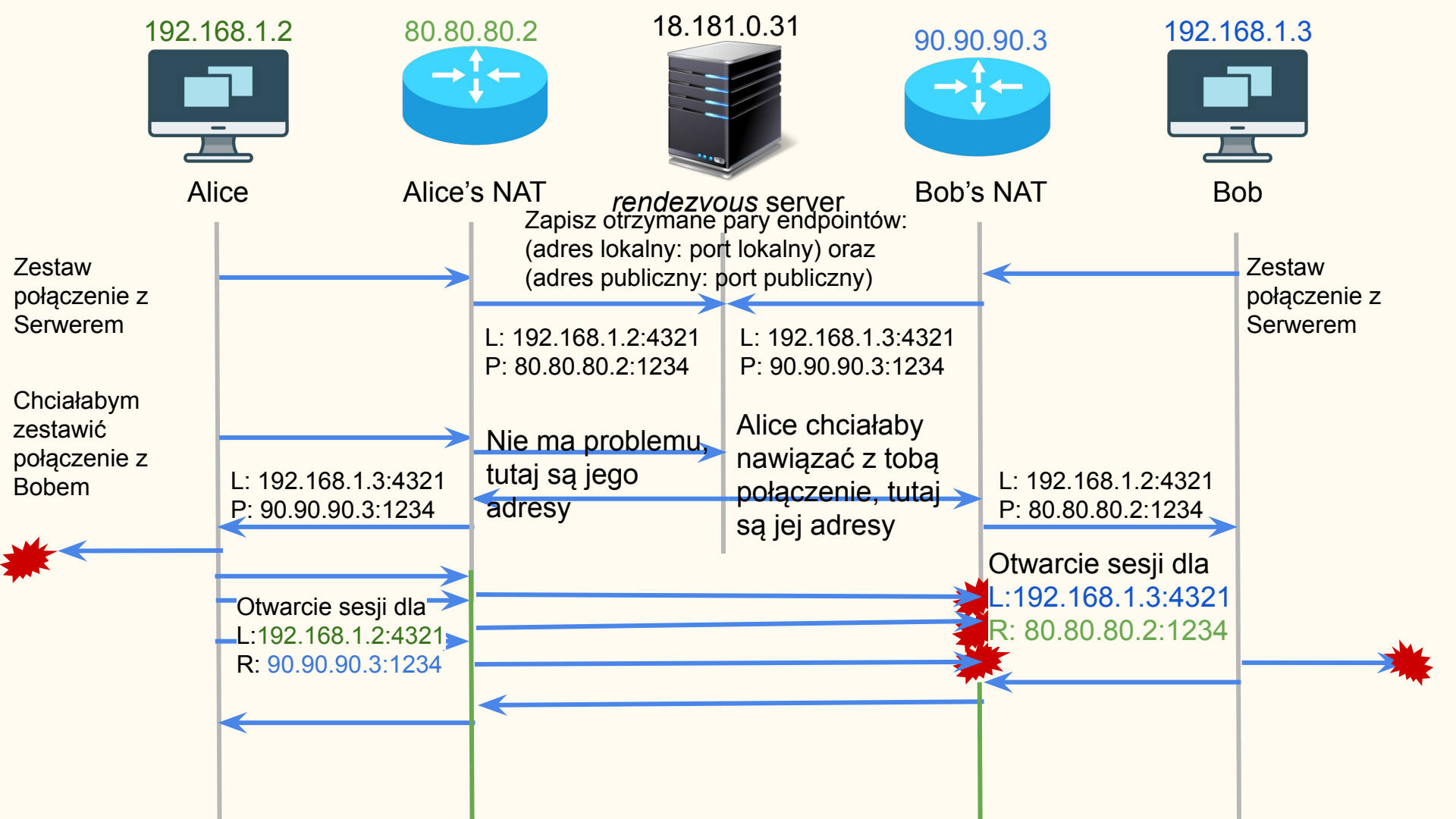

192.168.1.2
80.80.80.2
18.181.0.31
90.90.90.3
192.168.1.3
Alice
Alice's NAT
rendezvous server
Bob's NAT
Bob
Zapisz otrzymane pary endpointów:
(adres lokalny: port lokalny) oraz
(adres publiczny: port publiczny)
Zestaw połączenie z Serwerem
Zestaw połączenie z Serwerem
L: 192.168.1.2:4321
P: 80.80.80.2:1234
L: 192.168.1.3:4321
P: 90.90.90.3:1234
Chciałabym zestawić połączenie z Bobem

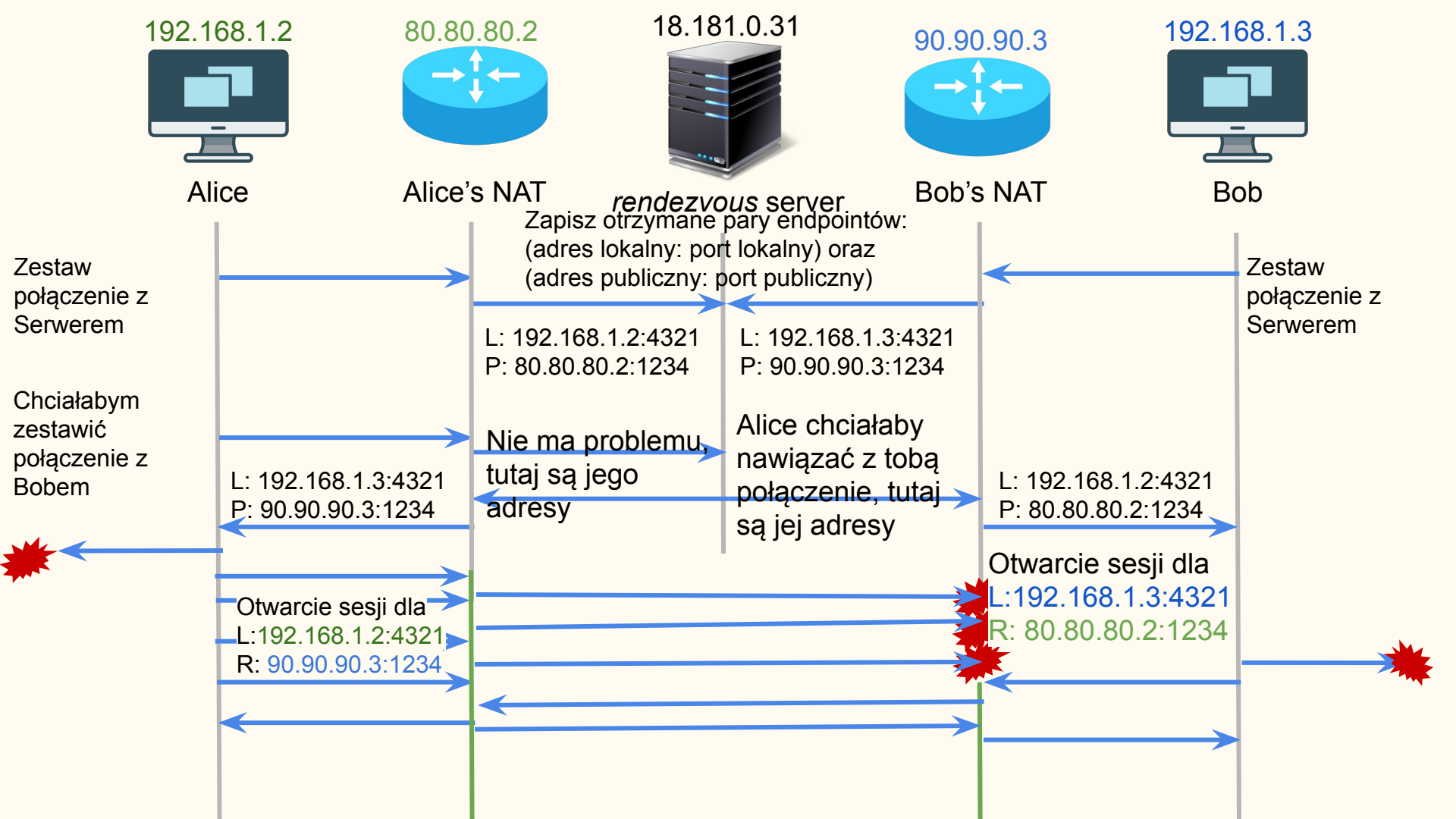

192.168.1.2
80.80.80.2
18.181.0.31
90.90.90.3
192.168.1.3
Alice
Alice's NAT
rendezvous server
Bob's NAT
Bob
Zapisz otrzymane pary endpointów:
(adres lokalny: port lokalny) oraz
(adres publiczny: port publiczny)
Zestaw połączenie z Serwerem
Zestaw połączenie z Serwerem
L: 192.168.1.2:4321
P: 80.80.80.2:1234
L: 192.168.1.3:4321
P: 90.90.90.3:1234
Chciałabym zestawić połączenie z Bobem
Nie ma problemu, tutaj są jego adresy
L: 192.168.1.3:4321
P: 90.90.90.3:1234

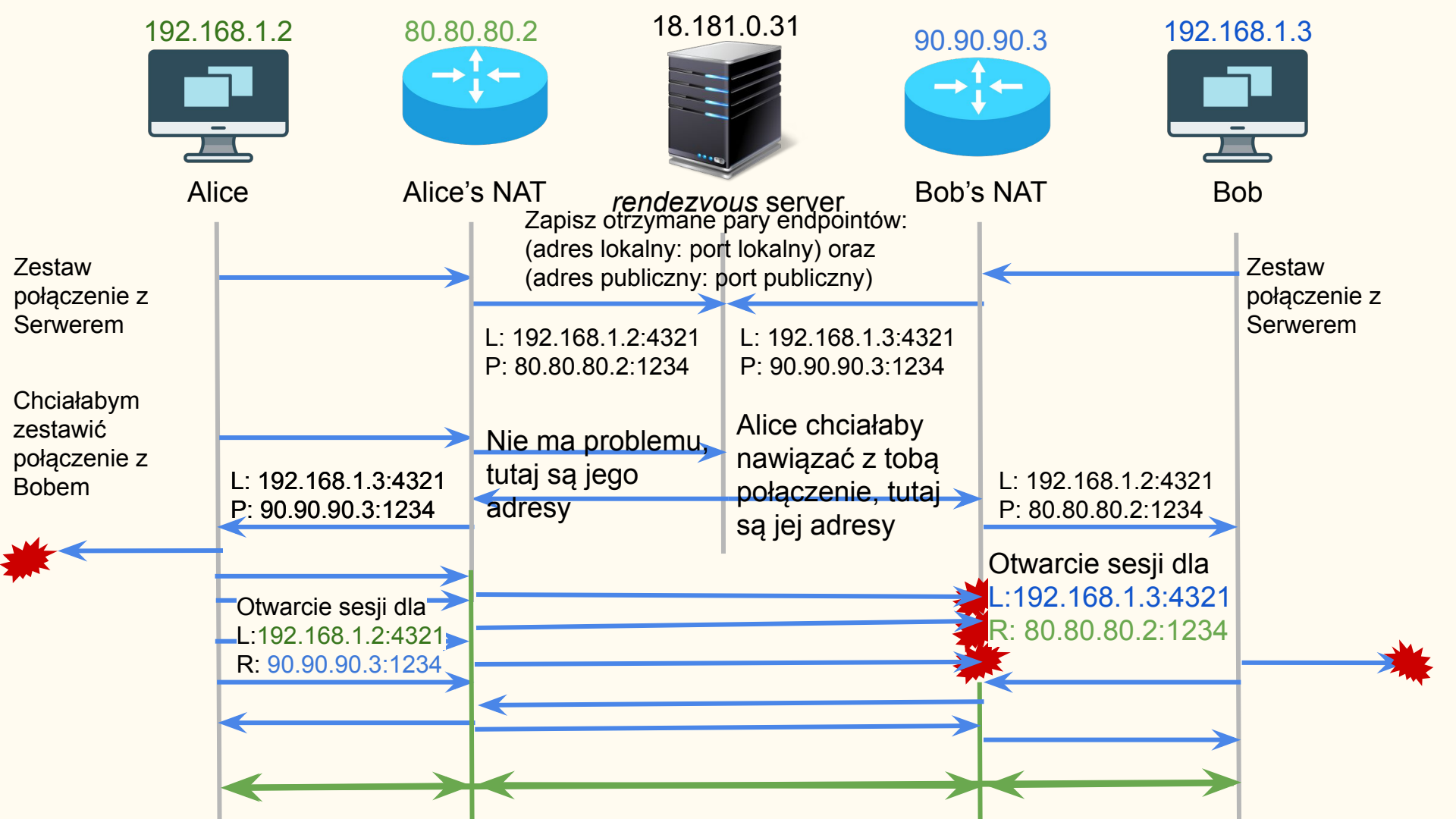

192.168.1.2
80.80.80.2
18.181.0.31
90.90.90.3
192.168.1.3
Alice
Alice's NAT
rendezvous server
Bob's NAT
Bob
Zapisz otrzymane pary endpointów:
(adres lokalny: port lokalny) oraz
(adres publiczny: port publiczny)
Zestaw połączenie z Serwerem
Zestaw połączenie z Serwerem
L: 192.168.1.2:4321
P: 80.80.80.2:1234
L: 192.168.1.3:4321
P: 90.90.90.3:1234
Chciałabym zestawić połączenie z Bobem
Nie ma problemu, tutaj są jego adresy
Alice chciałaby nawiązać z tobą połączenie, tutaj są jej adresy
L: 192.168.1.3:4321
P: 90.90.90.3:1234
L: 192.168.1.2:4321
P: 80.80.80.2:1234


192.168.1.2
80.80.80.2
18.181.0.31
90.90.90.3
192.168.1.3
Alice
Alice's NAT
rendezvous server
Bob's NAT
Bob
Zapisz otrzymane pary endpointów:
(adres lokalny: port lokalny) oraz
(adres publiczny: port publiczny)
Zestaw połączenie z Serwerem
Zestaw połączenie z Serwerem
L: 192.168.1.2:4321
P: 80.80.80.2:1234
L: 192.168.1.3:4321
P: 90.90.90.3:1234
Chciałabym zestawić połączenie z Bobem
Nie ma problemu, tutaj są jego adresy
Alice chciałaby nawiązać z tobą połączenie, tutaj są jej adresy
L: 192.168.1.3:4321
P: 90.90.90.3:1234
L: 192.168.1.2:4321
P: 80.80.80.2:1234
Otwarcie sesji dla
L:192.168.1.2:4321
R: 90.90.90.3:1234

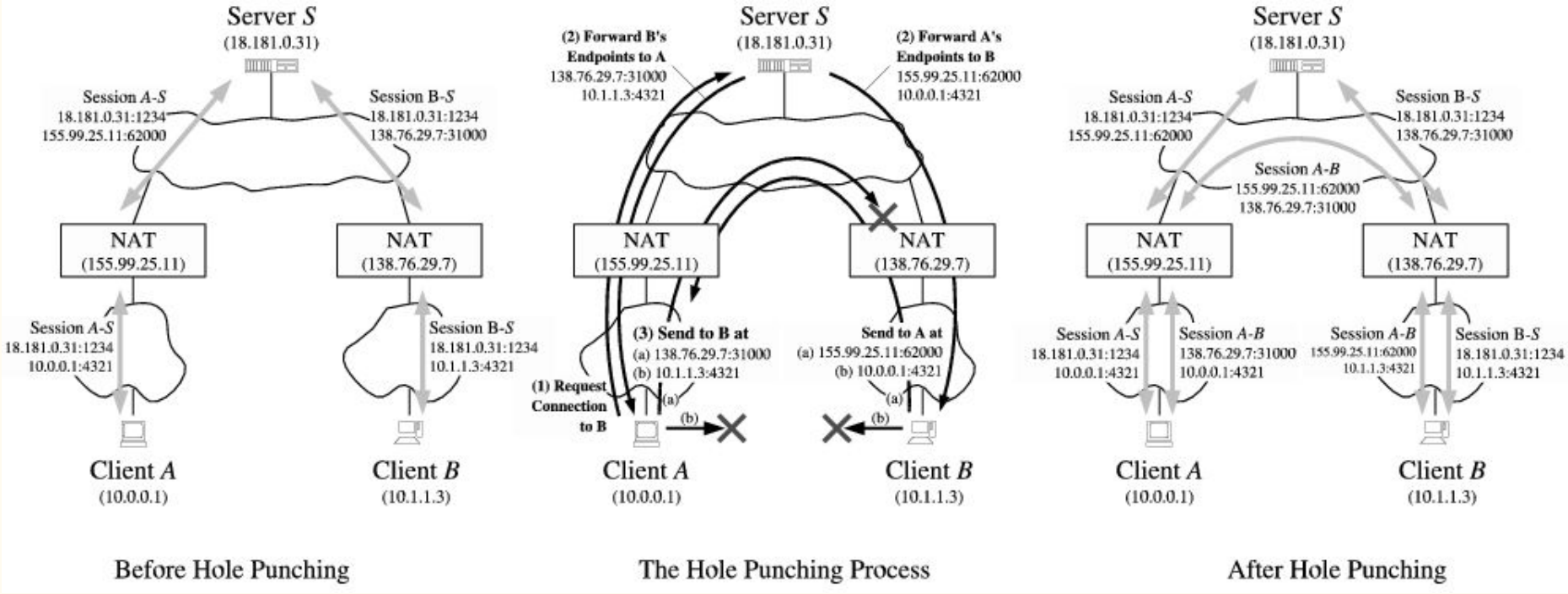

192.168.1.2
80.80.80.2
18.181.0.31
90.90.90.3
192.168.1.3
Alice
Alice's NAT
rendezvous server
Bob's NAT
Bob
Zapisz otrzymane pary endpointów:
(adres lokalny: port lokalny) oraz
(adres publiczny: port publiczny)
Zestaw połączenie z Serwerem
Zestaw połączenie z Serwerem
L: 192.168.1.2:4321
P: 80.80.80.2:1234
L: 192.168.1.3:4321
P: 90.90.90.3:1234
Chciałabym zestawić połączenie z Bobem
Nie ma problemu, tutaj są jego adresy
Alice chciałaby nawiązać z tobą połączenie, tutaj są jej adresy
L: 192.168.1.3:4321
P: 90.90.90.3:1234
L: 192.168.1.2:4321
P: 80.80.80.2:1234
Otwarcie sesji dla
L:192.168.1.2:4321
R: 90.90.90.3:1234


192.168.1.2
80.80.80.2
18.181.0.31
90.90.90.3
192.168.1.3
Alice
Alice's NAT
rendezvous server
Bob's NAT
Bob
Zapisz otrzymane pary endpointów:
(adres lokalny: port lokalny) oraz
(adres publiczny: port publiczny)
Zestaw połączenie z Serwerem
Zestaw połączenie z Serwerem
L: 192.168.1.2:4321
P: 80.80.80.2:1234
L: 192.168.1.3:4321
P: 90.90.90.3:1234
Chciałabym zestawić połączenie z Bobem
Nie ma problemu, tutaj są jego adresy
Alice chciałaby nawiązać z tobą połączenie, tutaj są jej adresy
L: 192.168.1.3:4321
P: 90.90.90.3:1234
L: 192.168.1.2:4321
P: 80.80.80.2:1234
Otwarcie sesji dla
L:192.168.1.2:4321
R: 90.90.90.3:1234
Otwarcie sesji dla
L:192.168.1.3:4321
R: 80.80.80.2:1234

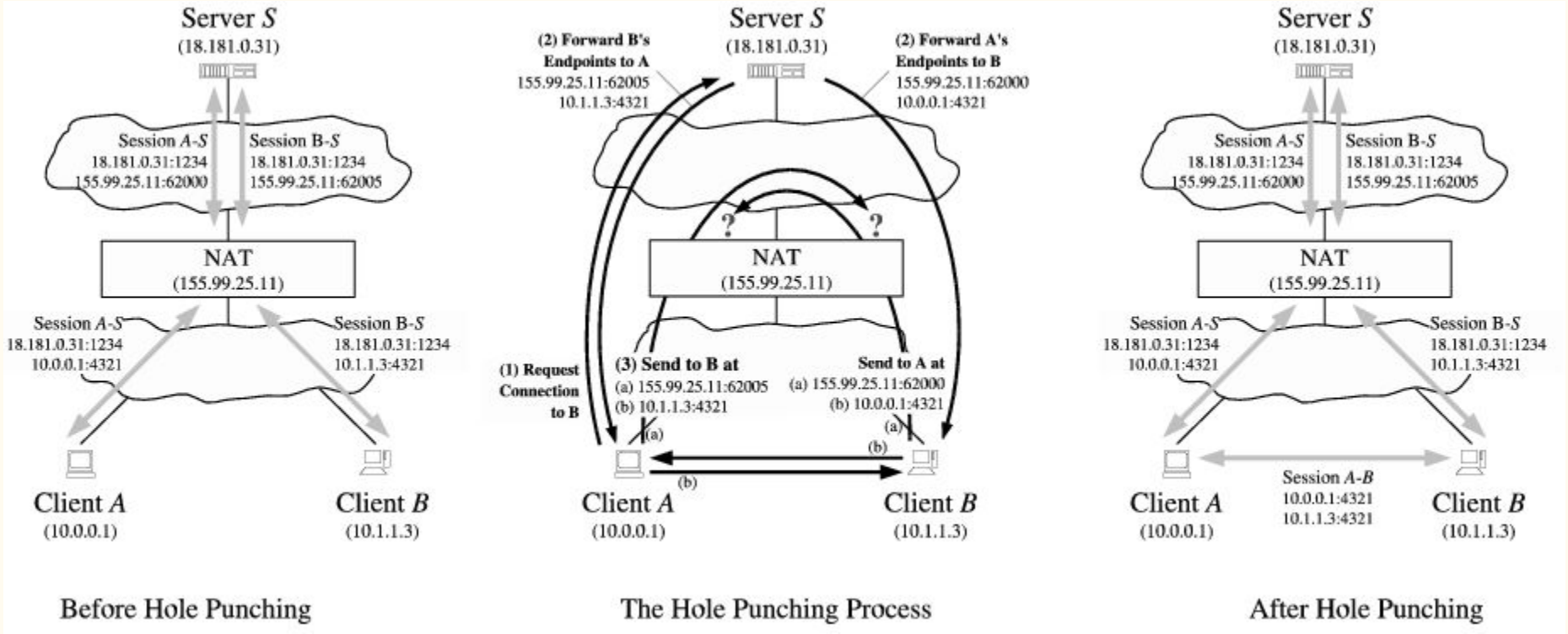

192.168.1.2
80.80.80.2
18.181.0.31
90.90.90.3
192.168.1.3
Alice
Alice's NAT
rendezvous server
Bob's NAT
Bob
Zapisz otrzymane pary endpointów:
(adres lokalny: port lokalny) oraz
(adres publiczny: port publiczny)
Zestaw połączenie z Serwerem
Zestaw połączenie z Serwerem
L: 192.168.1.2:4321
P: 80.80.80.2:1234
L: 192.168.1.3:4321
P: 90.90.90.3:1234
Chciałabym zestawić połączenie z Bobem
Nie ma problemu, tutaj są jego adresy
Alice chciałaby nawiązać z tobą połączenie, tutaj są jej adresy
L: 192.168.1.3:4321
P: 90.90.90.3:1234
L: 192.168.1.2:4321
P: 80.80.80.2:1234
Otwarcie sesji dla
L:192.168.1.2:4321
R: 90.90.90.3:1234
Otwarcie sesji dla
L:192.168.1.3:4321
R: 80.80.80.2:1234


192.168.1.2
80.80.80.2
18.181.0.31
90.90.90.3
192.168.1.3
Alice
Alice's NAT
rendezvous server
Bob's NAT
Bob
Zapisz otrzymane pary endpointów:
(adres lokalny: port lokalny) oraz
(adres publiczny: port publiczny)
Zestaw połączenie z Serwerem
Zestaw połączenie z Serwerem
L: 192.168.1.2:4321
P: 80.80.80.2:1234
L: 192.168.1.3:4321
P: 90.90.90.3:1234
Chciałabym zestawić połączenie z Bobem
Nie ma problemu, tutaj są jego adresy
Alice chciałaby nawiązać z tobą połączenie, tutaj są jej adresy
L: 192.168.1.3:4321
P: 90.90.90.3:1234
L: 192.168.1.2:4321
P: 80.80.80.2:1234
Otwarcie sesji dla
L:192.168.1.2:4321
R: 90.90.90.3:1234
Otwarcie sesji dla
L:192.168.1.3:4321
R: 80.80.80.2:1234

Different NAT

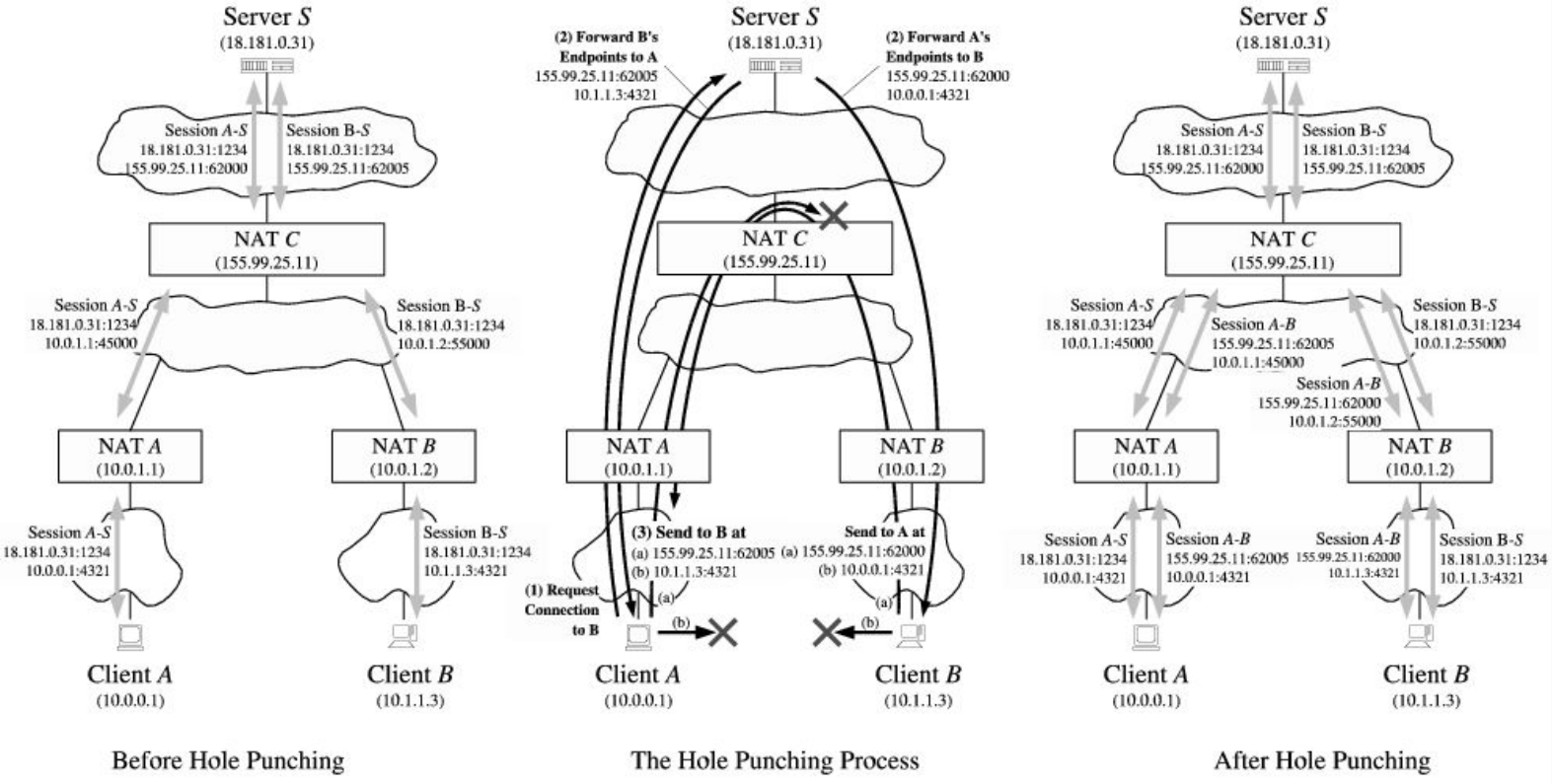


Common NAT



Sytuacja podobna do poprzedniej z tą różnicą, że odpowiada nam adres prywatny hosta docelowego

Multilevel NAT



Sytuacja w większości domów. NAT A i NAT B są naszymi domowymi routerami, NAT C jest routerem ISP. Optymalnym rozwiązaniem dla Alice było by wysyłanie datagramów na adres routera Boba, tak aby router naszego ISP nie musiał pośredniczyć w tej komunikacji. Nie jest to niestety możliwe ponieważ, rendezvous Serwer widzi tylko adresy końcowe (nasz lokalny i publiczny od ISP).

Hairpin - NAT loopback

Dostęp do urządzenia w tej samej sieci LAN przez adres zewnętrzny.

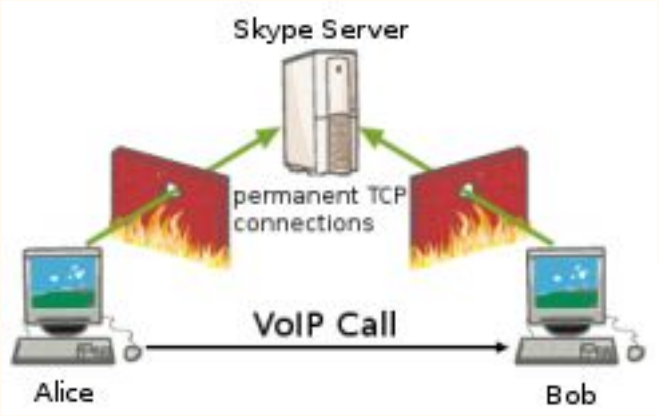
Nie wspierane przez wszystkie NATy

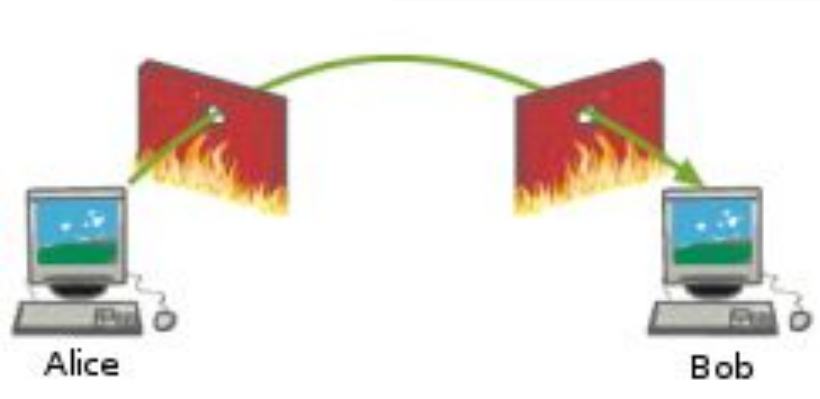
Zrastanie się dziury, czyli UDP Idle Timeouts

Większość NATów posiada timeout na sesję UDP której czas nie jest ustandaryzowany, czasami jest to zaledwie 20 sek. Jeśli aplikacja chce utrzymać sesję, musi wysyłać okresowo datagramy keep-alive, lub ponawiać procedurę *hole punching*

TCP Hole Punching

- Bardziej skomplikowane
- Wspierane przez mniejszą ilość NATów
- Tak samo szybkie i rzetelne jak UDP hole punching





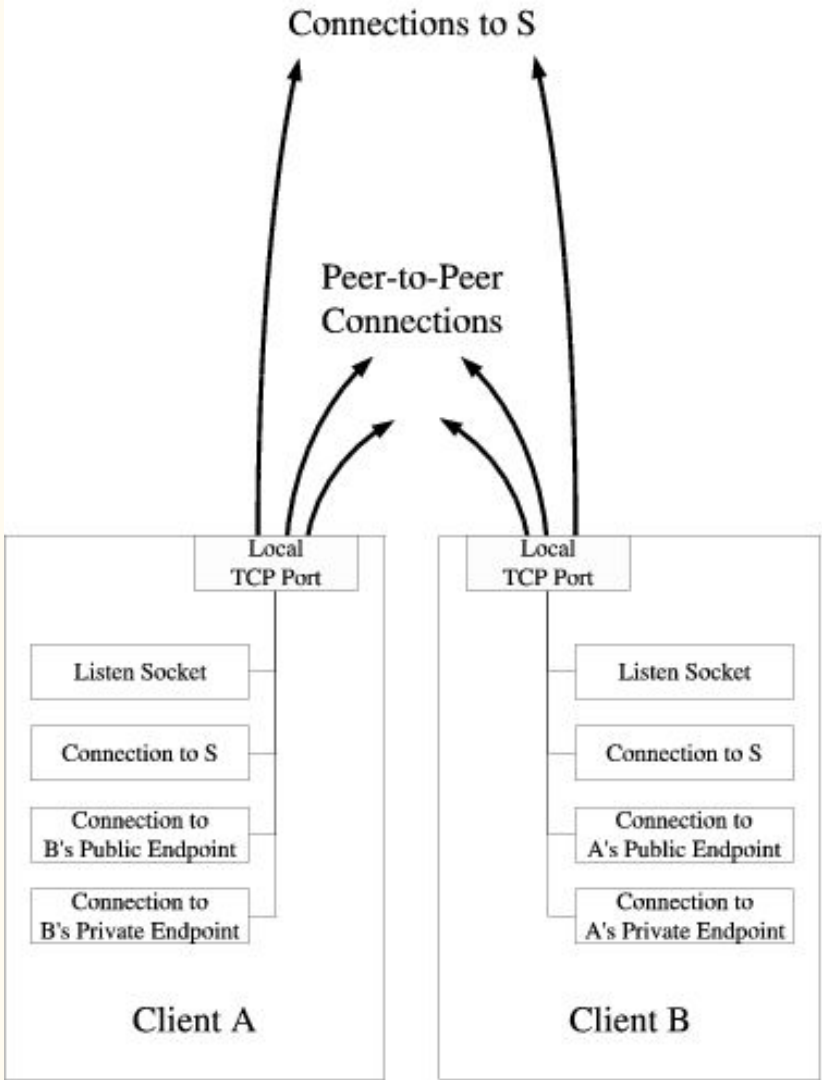
The hole trick - How Skype & Co. get round firewalls (2006)

Opening Peer-to-Peer TCP Streams

TCP, unlike UDP, needs to manage several sockets bounded to single TCP port.

Each client needs a

- Stream socket representing its connection to Server.
- Listen socket to accept incoming connections from peers
- At least two additional stream sockets to initialize outgoing connections to the other peers.



Session Traversal Utilities for NAT (STUN) [RFC 5389]

Obsoletes *Simple Traversal of User Datagram Protocol* [RFC 3489]

STUN

Is a TOOL used by other protocols dealing with NAT traversal, such as

- Interactive Connectivity Establishment (ICE).
- Session Initiation Protocol (SIP).
- WebRTC.

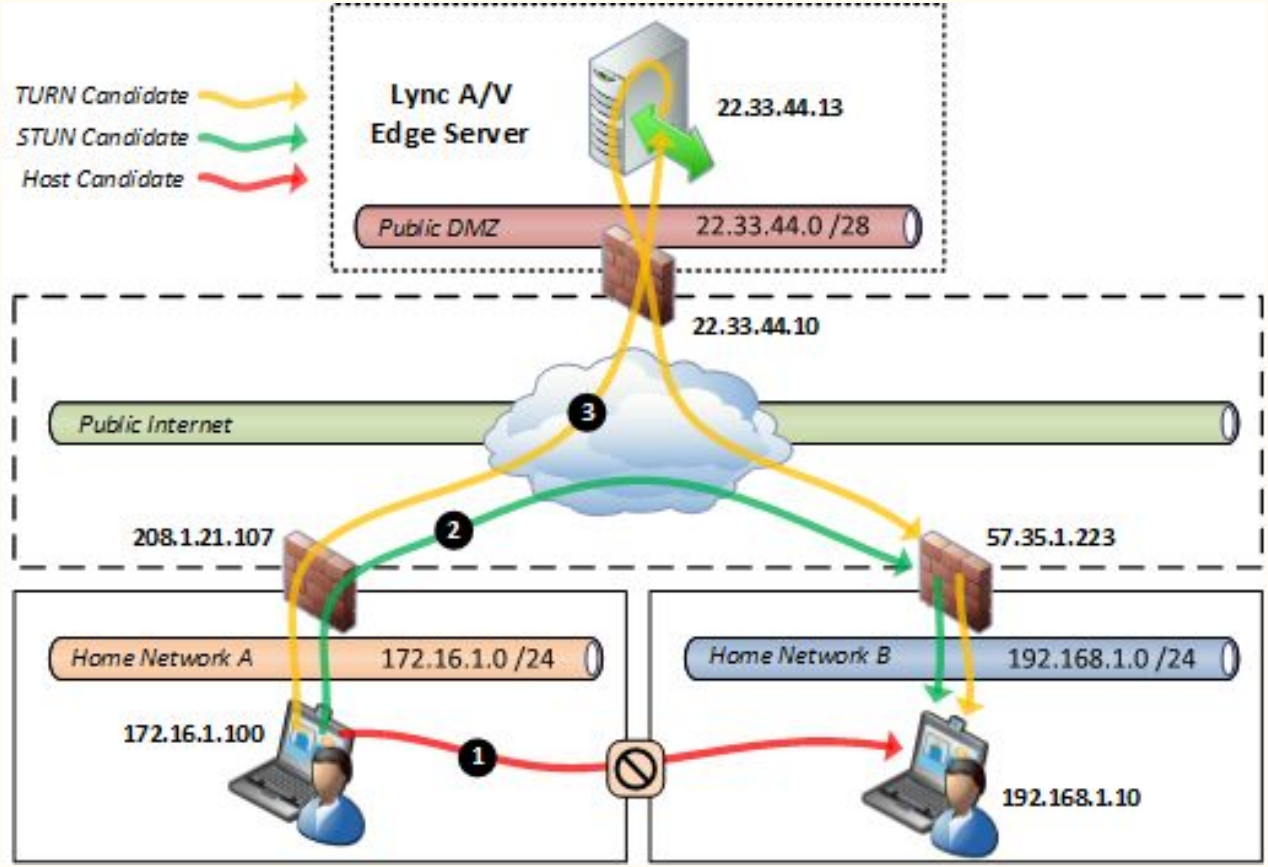
It can be used by an endpoint to

- determine IP address and port allocated to it by a NAT, that corresponds to its private IP address and port
- check connectivity between two endpoints.
- keep-alive protocol to maintain NAT bindings.
- relay packets between two endpoints

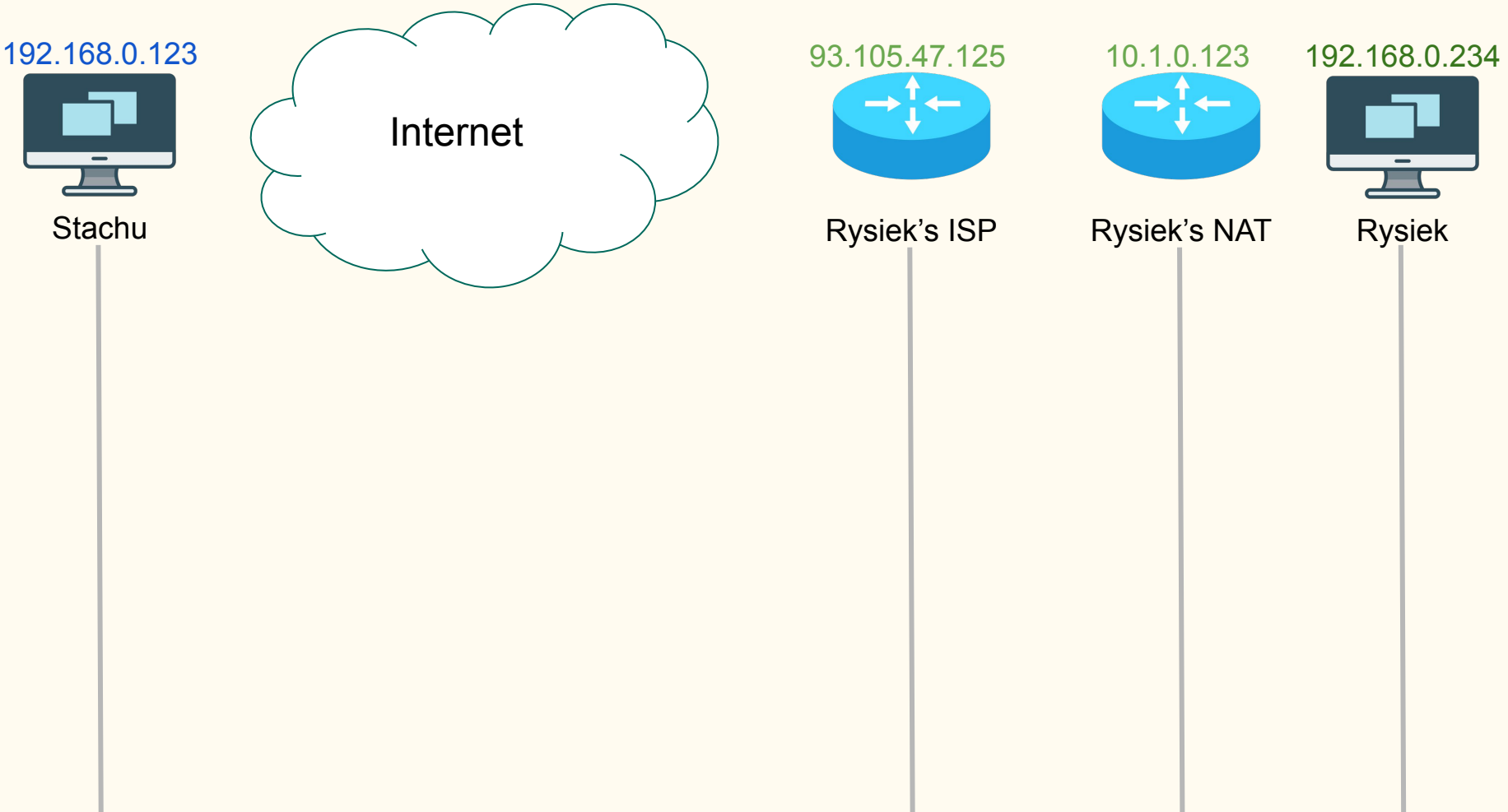
Interactive Connectivity Establishment (ICE)

—

ICE makes use of the Session Traversal Utilities for NAT (STUN) protocol and its extension, Traversal Using Relay NAT (TURN).


TURN Candidate
STUN Candidate
Host Candidate
Lync A/V
Edge Server
22.33.44.13
Public DMZ
22.33.44.0 /28
22.33.44.10
Public Internet
3
2
208.1.21.107
57.35.1.223
Home Network A
172.16.1.0 /24
Home Network B
192.168.1.0 /24
172.16.1.100
1
192.168.1.10

Demo


192.168.0.123
Stachu
Internet
93.105.47.125
Rysiek's ISP
10.1.0.123
Rysiek's NAT
192.168.0.234
Rysiek

192.168.0.234

Rysiek

```
▸1  22:35   ~ $  nc -u -l -p 14141 -v
Listening on [0.0.0.0] (family 0, port 14141)
```

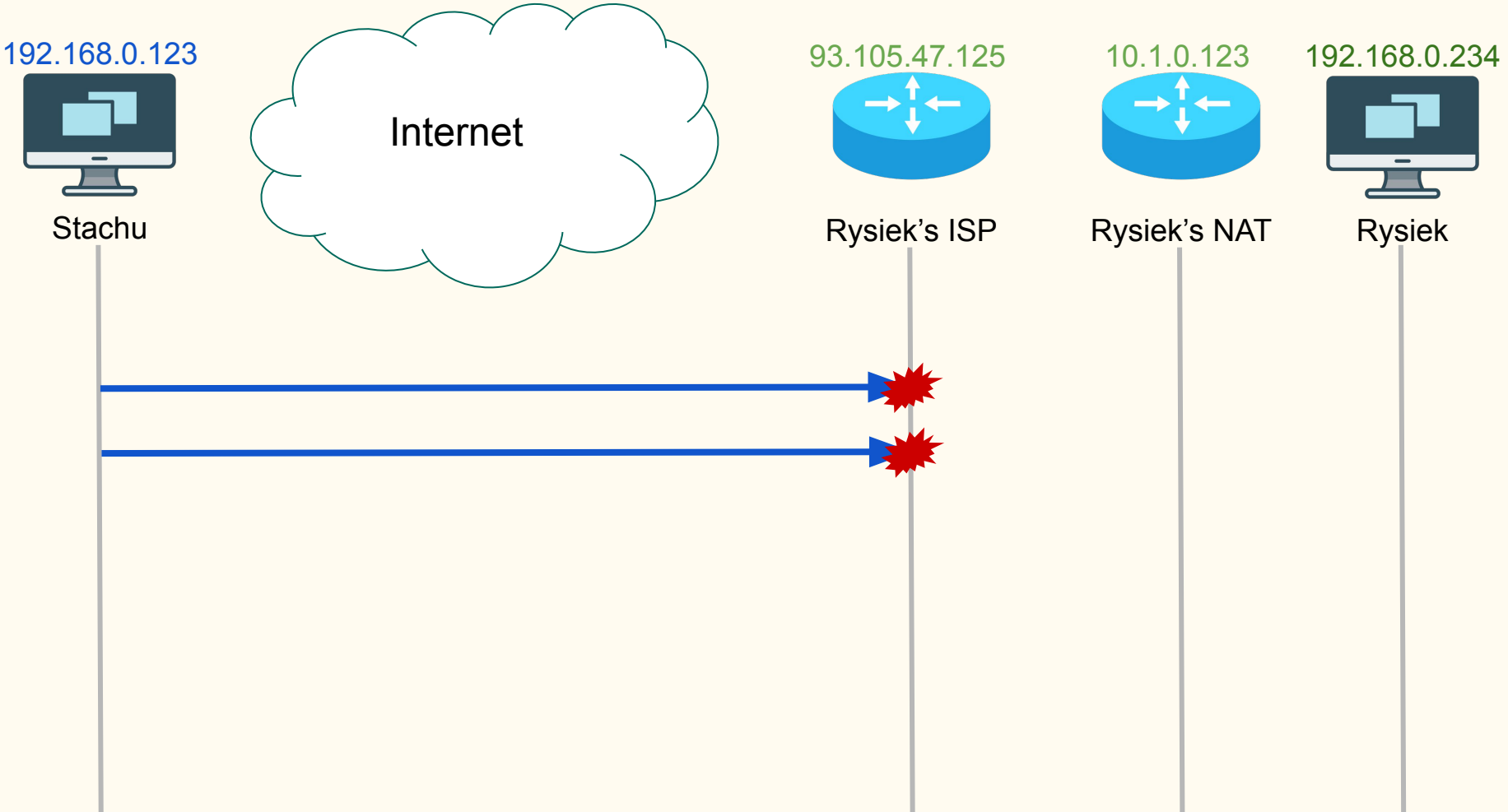
192.168.0.123

Stachu

```
[~ » echo "Siema, co tam ?" | nc -p 53 -u dragonic.duckdns.org 14141
```

```
[/usr/local/Cellar/hping » nslookup dragonic.duckdns.org
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   dragonic.duckdns.org
Address: 93.105.47.125
```


192.168.0.123
Internet
93.105.47.125
10.1.0.123
192.168.0.234
Stachu
Rysiek's ISP
Rysiek's NAT
Rysiek

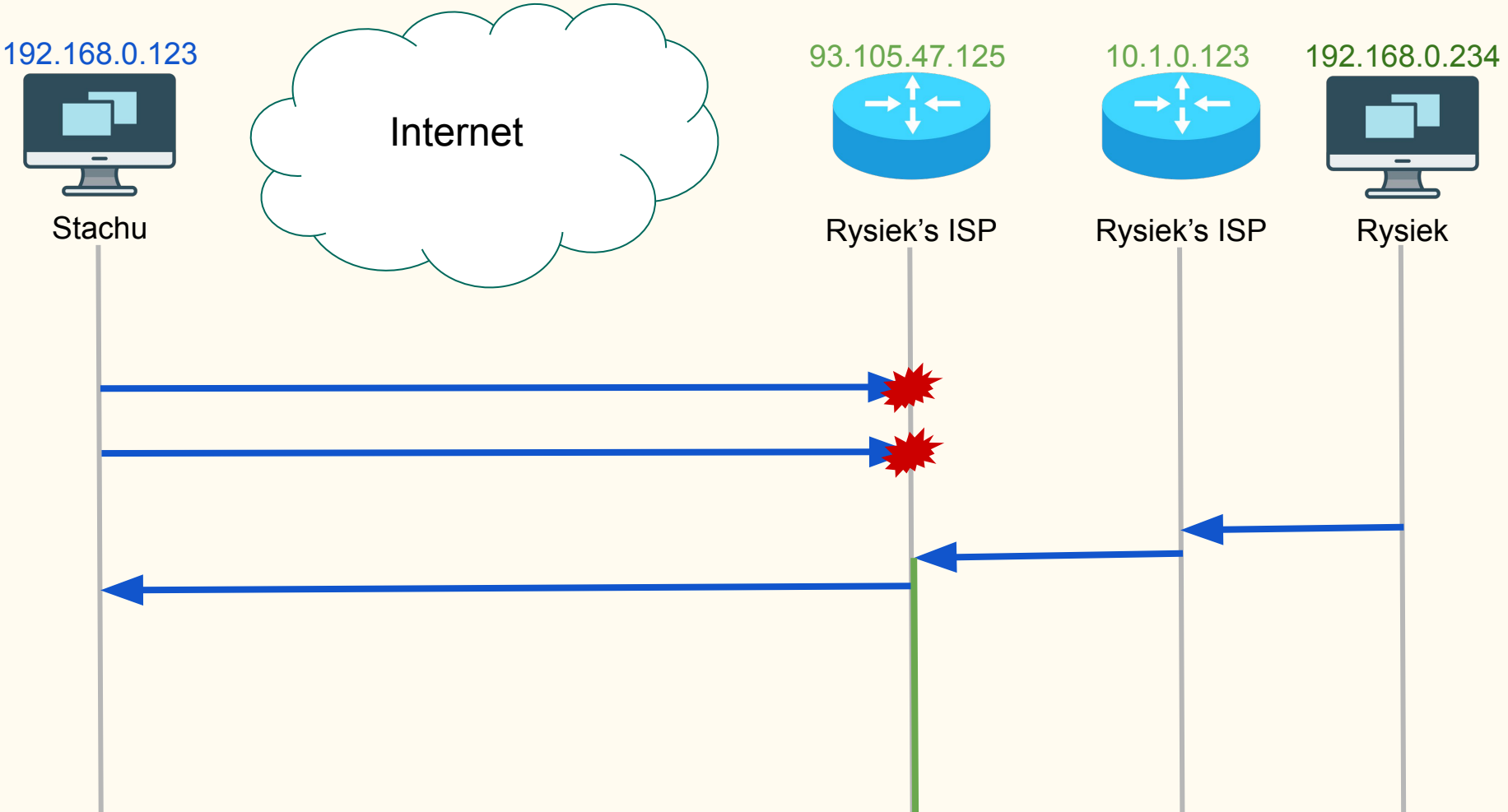
192.168.0.234

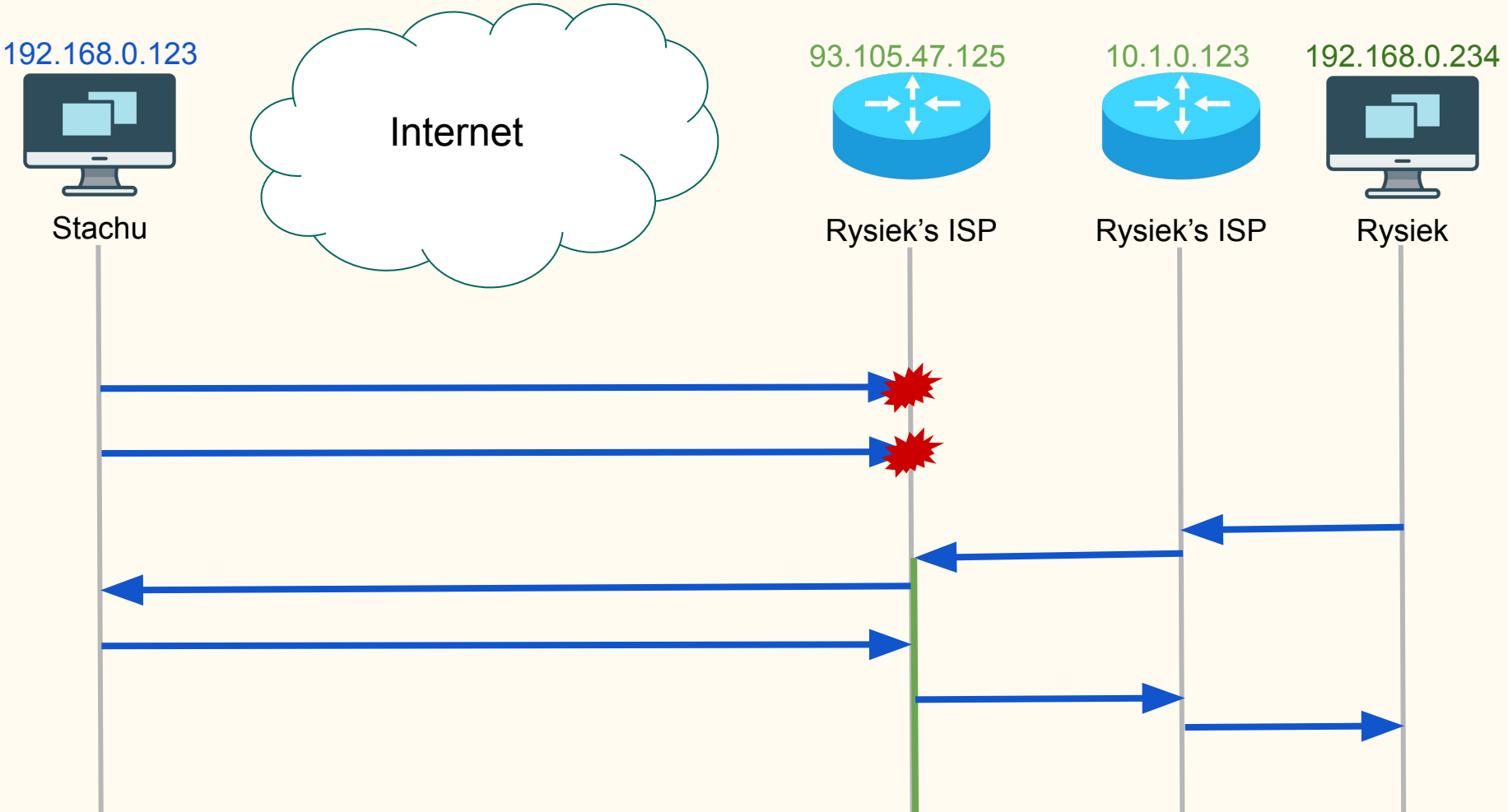
Rysiek

count UDP Source port Destination port

```
▶1  22:35  ~ $  sudo hping2 -c 1 -2 -s 14141 -p 53 80.238.125.248
HPING 80.238.125.248 (bridge0 80.238.125.248): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=80.238.125.248 name=host-80-238-125-248.jmdi.pl

--- 80.238.125.248 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```


192.168.0.123
Stachu
Internet
93.105.47.125
Rysiek's ISP
10.1.0.123
Rysiek's ISP
192.168.0.234
Rysiek


192.168.0.123
Stachu
Internet
93.105.47.125
Rysiek's ISP
10.1.0.123
Rysiek's ISP
192.168.0.234
Rysiek

192.168.0.234

Rysiek

```
▶1  22:35  ~ $  nc -u -l -p 14141 -v
Listening on [0.0.0.0] (family 0, port 14141)
Connection from host-80-238-125-248.jmdi.pl 53 received!
Siema, co tam ?
```

192.168.0.123

Stachu

```
~ » echo "Siema, co tam ?" | nc -p 53 -u dragonic.duckdns.org 14141
exit
```

Bibliografia

Peer-to-Peer Communication Across Network Address Translators

Session Traversal Utilities for NAT (STUN) [RFC 5389]

Traversal Using Relay NAT (TURN)

NAT_traversal

How Skype & Co. get round firewalls

How Your ISP Plans to "Help" You, and Break the Internet

Large Scale Symmetric NAT Traversal with Two Stage Hole Punching