

5.1 Übersicht

5.2 Adressen

5.3 Lokale Netze: Bridges und Switches

5.4 Intra-Domain Routing

5.5 Inter-Domain Routing

5.6 Internet Protocol (IPv4)

5.7 Network Address Translation (NAT)

5.8 IPv6

5.9 Mobilitätsunterstützung

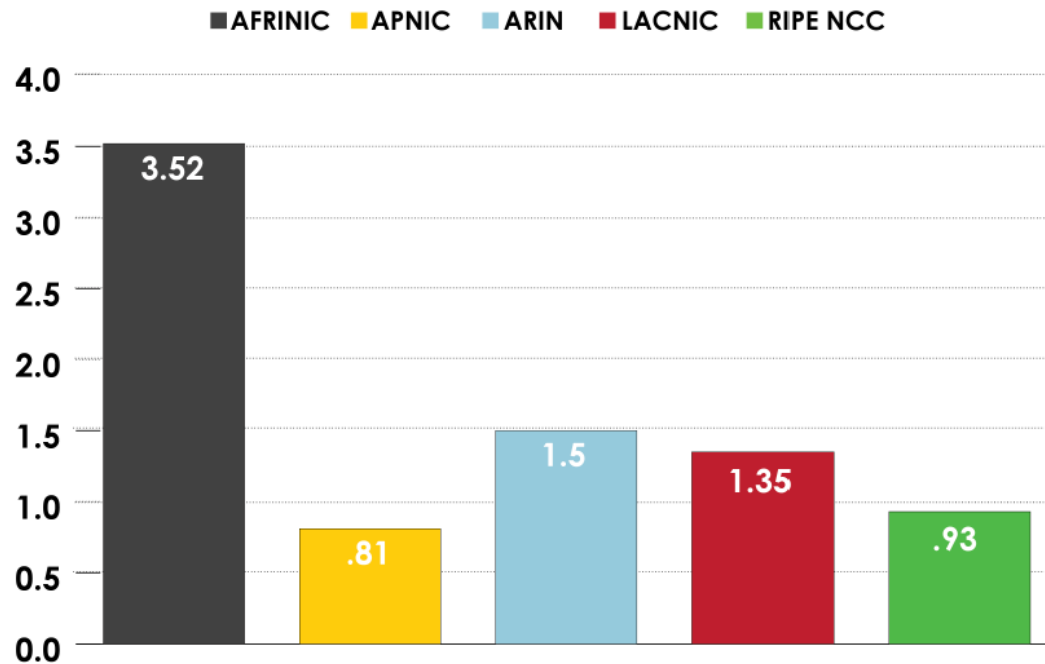
5.10 Zusammenfassung

IPv4 Adresszuteilung

- IPv4 Adressraum ist zu klein
 - 2^{32} also ungefähr 4.3 Milliarden Adressen
 - weniger als eine Adresse pro Person
- Teile der Welt haben den zugeteilten Adressraum vollständig ausgeschöpft

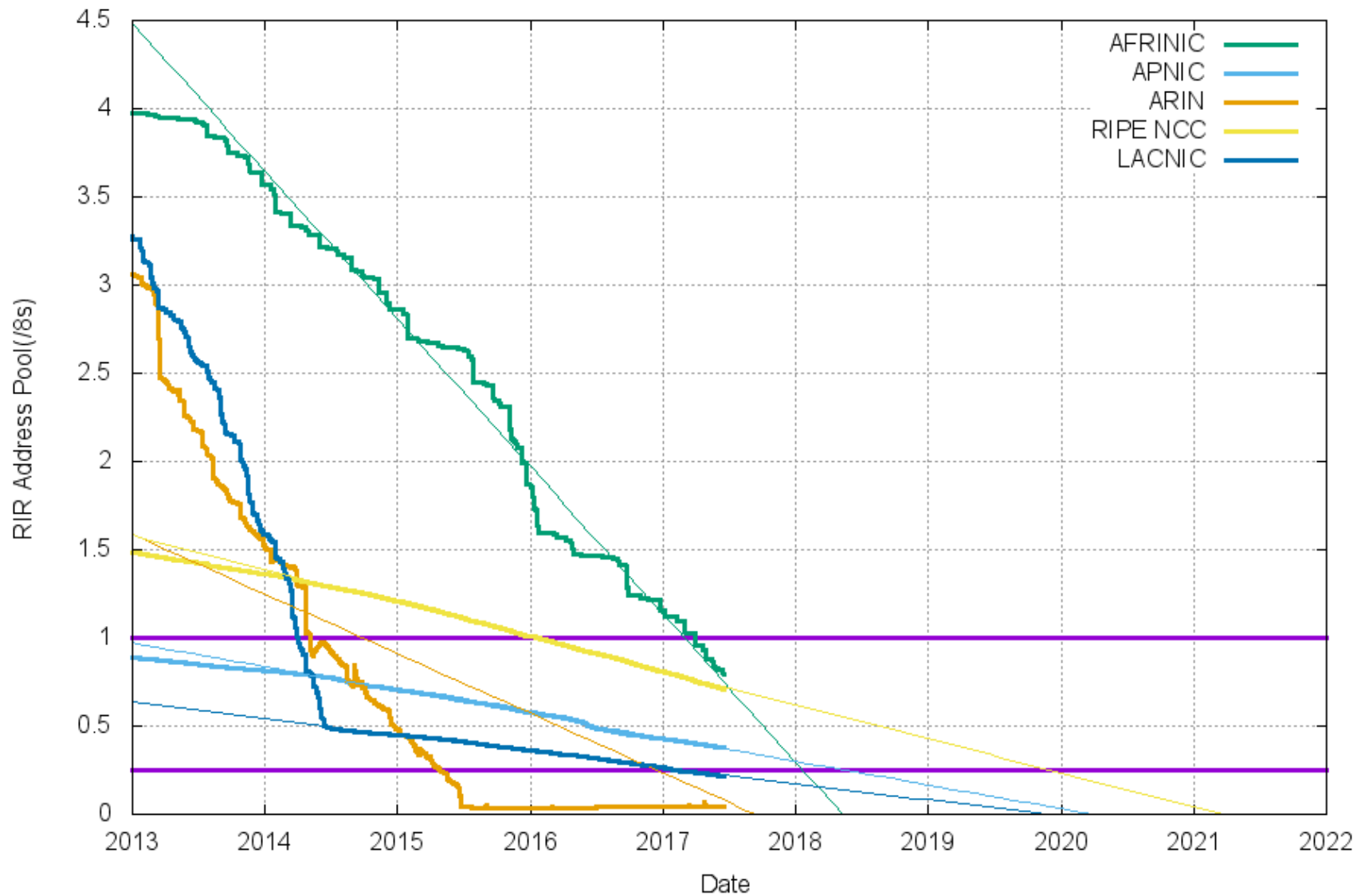
verbleibende IPv4
Adressen
(Anzahl /8s)

/8=16777216 Adressen



IPv4 Verbrauch

RIR IPv4 Address Run-Down Model

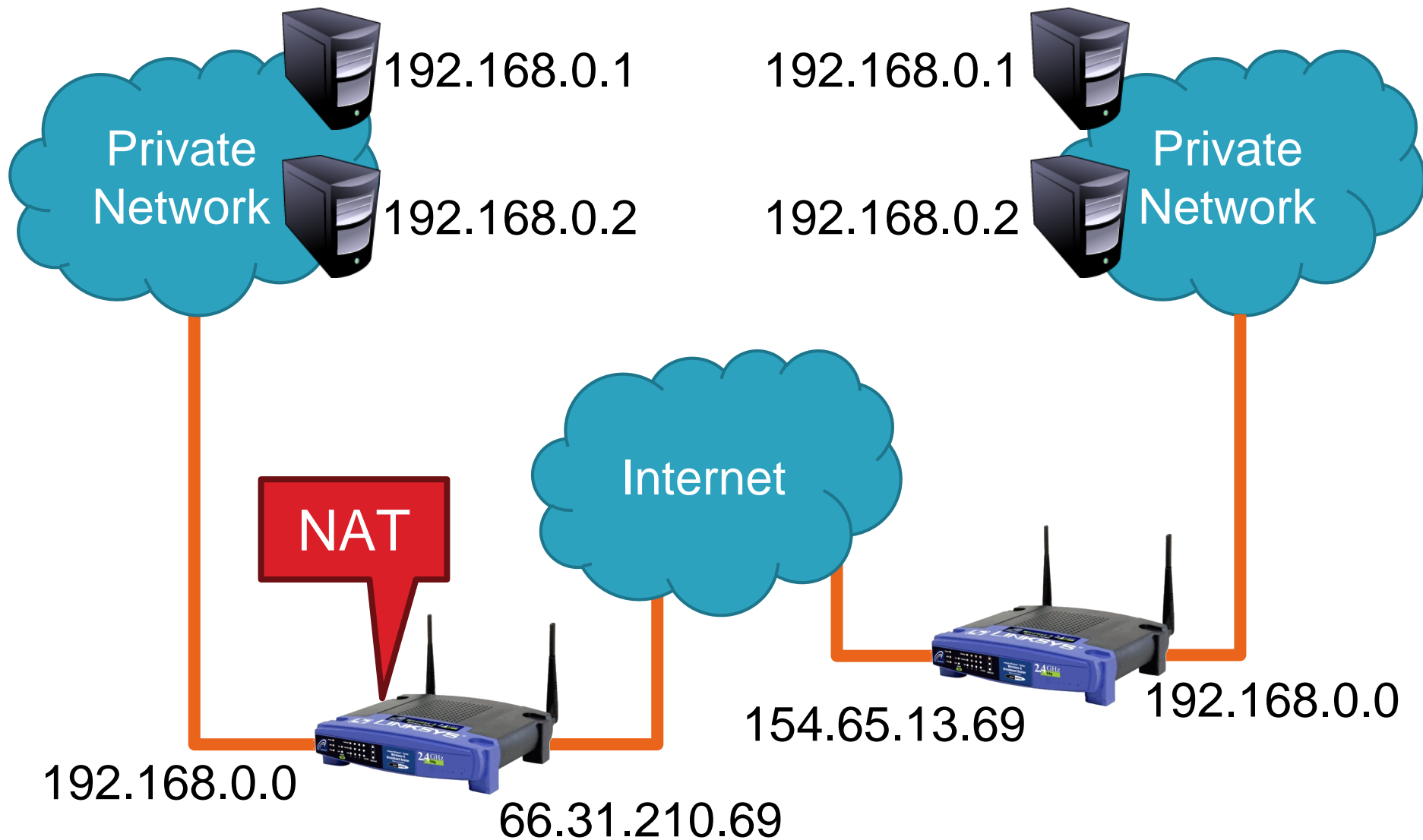


Mangel an IPv4 Adressen

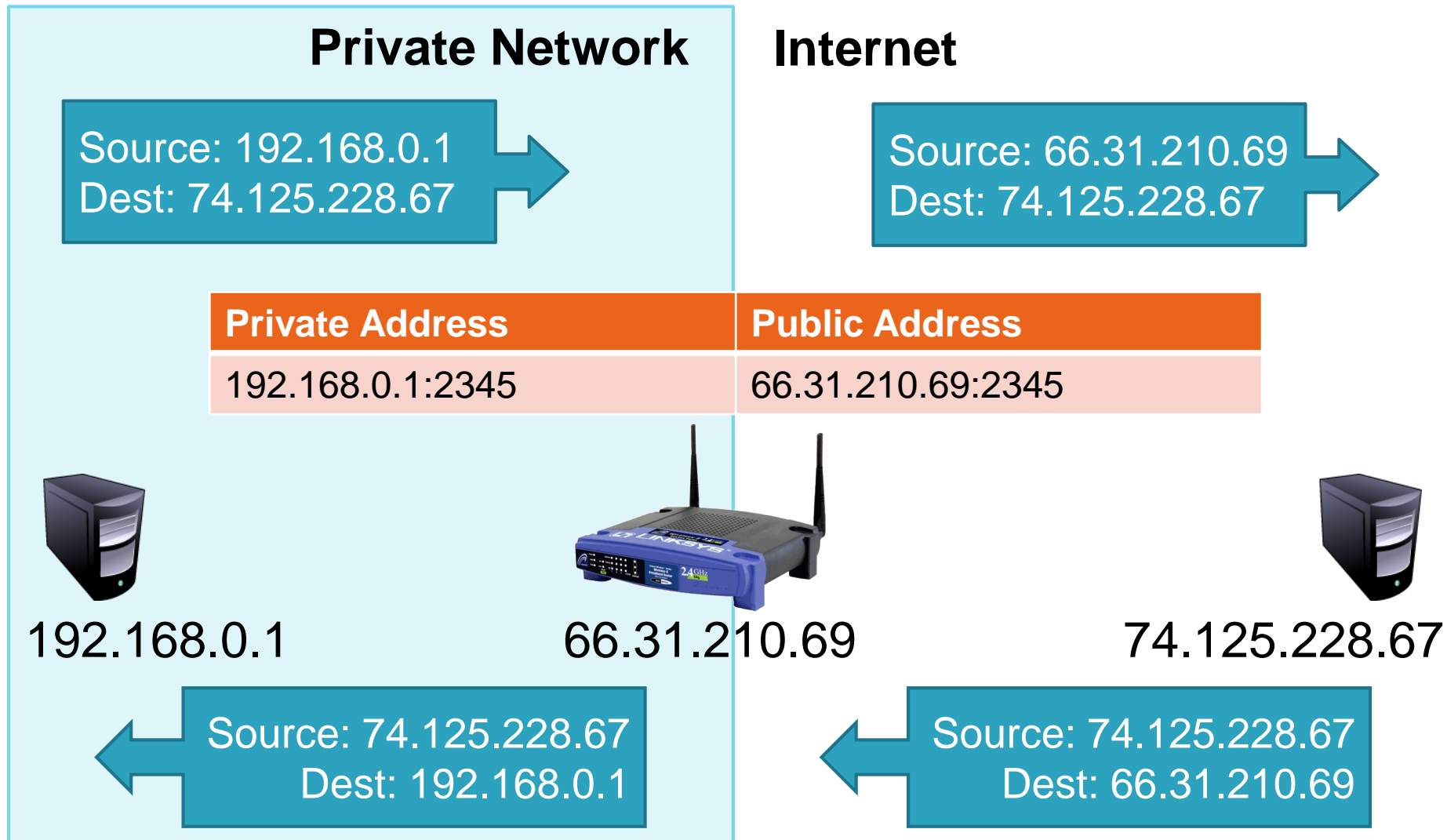
- Problem: Internet-Provider vergeben nur eine IPv4-Adresse pro Haushalt
 - zusätzliche IPs kosten extra
 - keine zusätzlichen IPs vorhanden
 - Anzahl von Geräten mit IP Adresse im Haushalt wächst stetig, Explosion in den letzten Jahren
 - Laptops, Desktops, TV, Blu-Ray-Player, Spiel-Konsole, Tablets, Smartphones, eReaders, Kameras, etc.
 - Faktor 10-100 durch IoT erwartet
 - Wie gehen alle Devices online?
- Problem gilt generell
 - Internet Provider haben mehr Kunden als IP Adressen
 - Firmen benötigen mehr IP Adressen als sie vom ISP bekommen
- Zusätzlich: Privacy
 - feste öffentliche IP macht Identifikation einfach

- Idee: Definieren einen privaten IP-Adressbereich, der vom Rest des Netzes getrennt und nicht sichtbar ist
 - Private IP Adressen werden für internes Routing (im Haushalt) und vor allem auf dem lokalen Rechner (zur Identifikation in Sockets) verwendet
 - Spezieller Router als Schnittstelle zwischen LAN und WAN, der die internen Adressen von außen erreichbar macht
 - NAT: Network Address Translation
- Eigenschaften von privaten IPs
 - nicht weltweit eindeutig, können mehrfach wiederverwendet werden
 - DSL Kunden eines Providers haben tendenziell das gleiche private Netz
 - normalerweise aus dem Bereich der nicht-routebaren Adressen
- Typische private IP Adressen:
 - 10.0.0.0 – 10.255.255.255
 - 172.16.0.0 – 172.31.255.255
 - 192.168.0.0 – 192.168.255.255

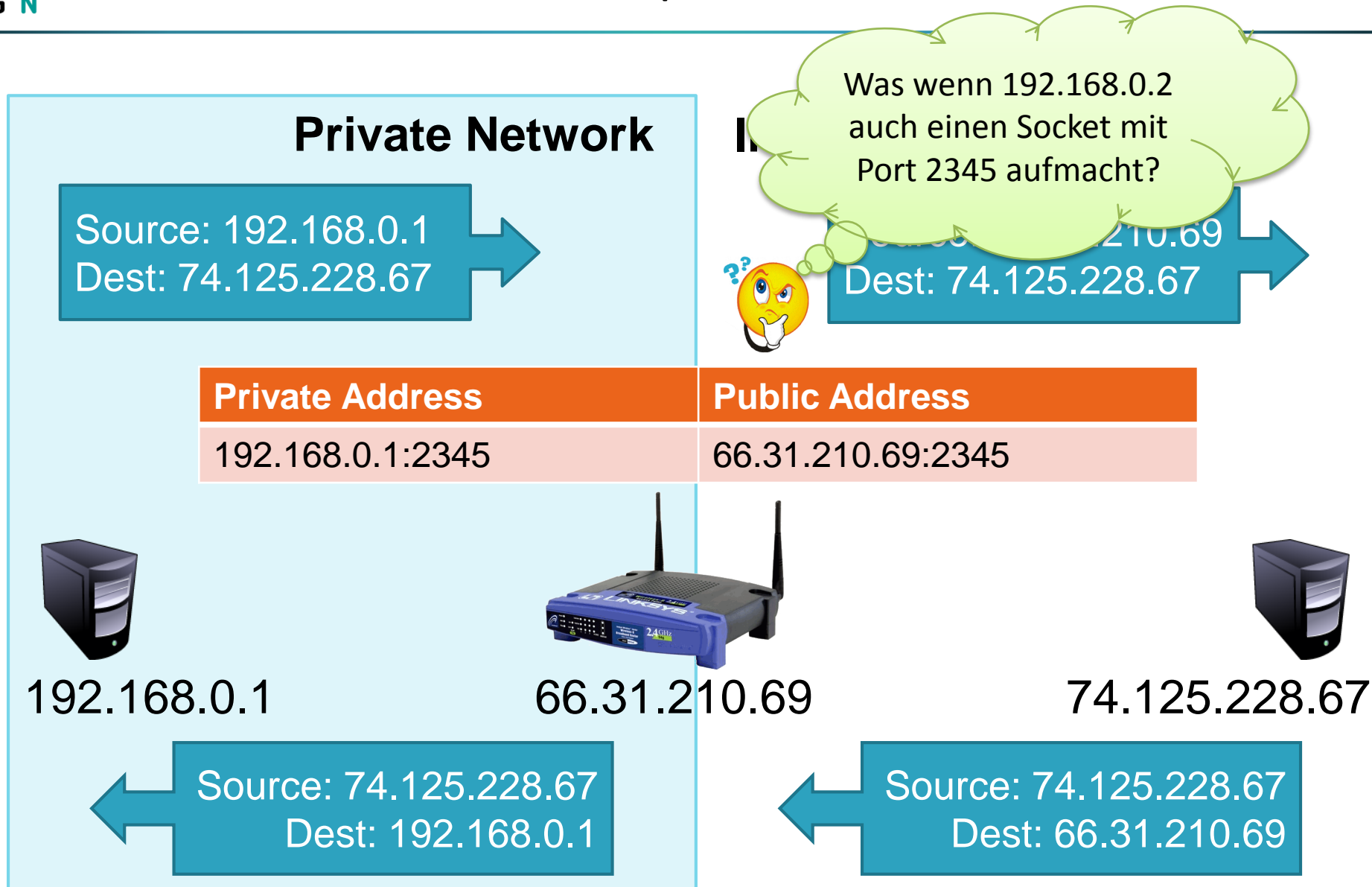
NAT – Network Address Translation



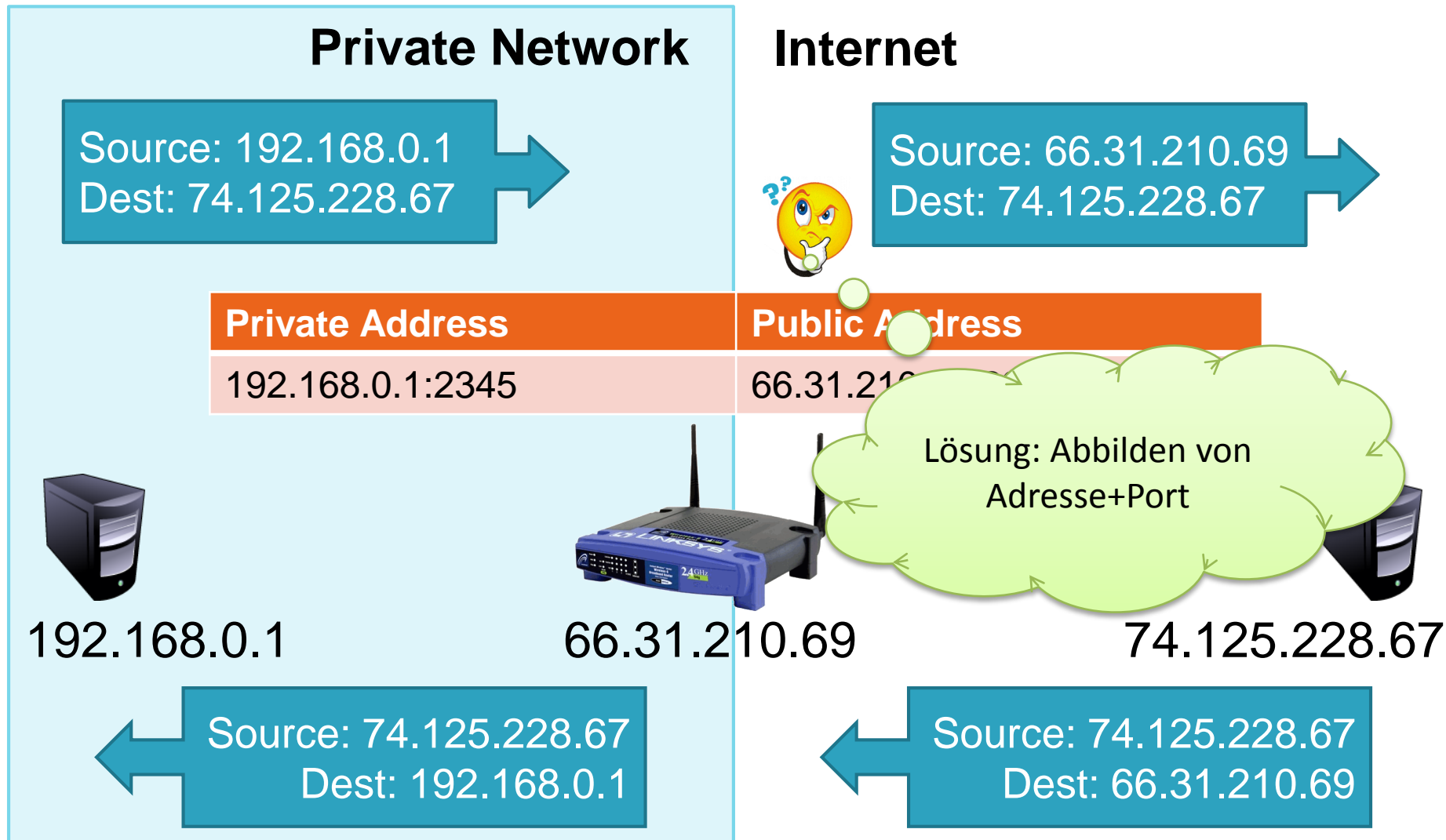
Prinzip von NAT



Prinzip von NAT



Prinzip von NAT



NAT und NAT

- NAT: Network Address Translation
 - Abbildung von privater auf öffentliche Adresse
- NAT: Network and Port Address Translation
 - Abbildung von private IP Adresse+Port auf öffentliche Adresse + Port



66.31.210.69

192.168.0.1



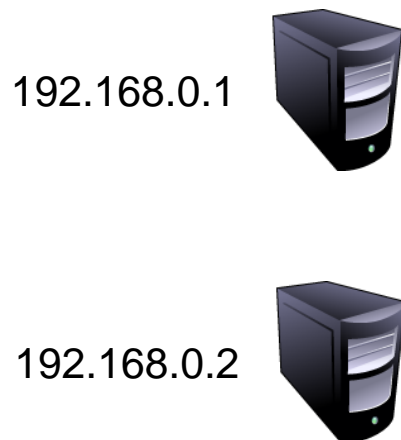

192.168.0.2



Private Address	Public Address
192.168.0.1:2345	66.31.210.69:50000
192.168.0.1:3001	66.31.210.69:50001
192.168.0.2:2345	66.31.210.69:60000
192.168.0.2:7023	66.31.210.69:60001

NAT und NATP


- NAT: Network Address Translation
 - Abbildung von privater auf öffentliche Adresse
- NATP: Network and Port Address Translation
 - Abbildung von privatem Adresse+Port-Paar auf öffentliches Adresse+Port-Paar

Private Address	
192.168.0.1:2345	
192.168.0.1:3001	
192.168.0.1:80	
192.168.0.2:2345	66.31.210.69:60000
192.168.0.2:7023	66.31.210.69:60001

66.31.210.69

Web-Server hinter NAT?



NAT als Firewall

Private Network

Internet

Private Address

Public Address



192.168.0.1



66.31.210.69



74.125.228.67

Source: 74.125.228.67
Dest: 66.31.210.69

Port Forwarding

Private Network

Internet

Private Address

192.168.0.1:80

Public Address

* * * * *



192.168.0.1



66.31.210.69



74.125.228.67

Source: 74.125.228.67:8679
Dest: 192.168.0.1:80

Source: 74.125.228.67:8679
Dest: 66.31.210.69:80

NAT Hole Punching

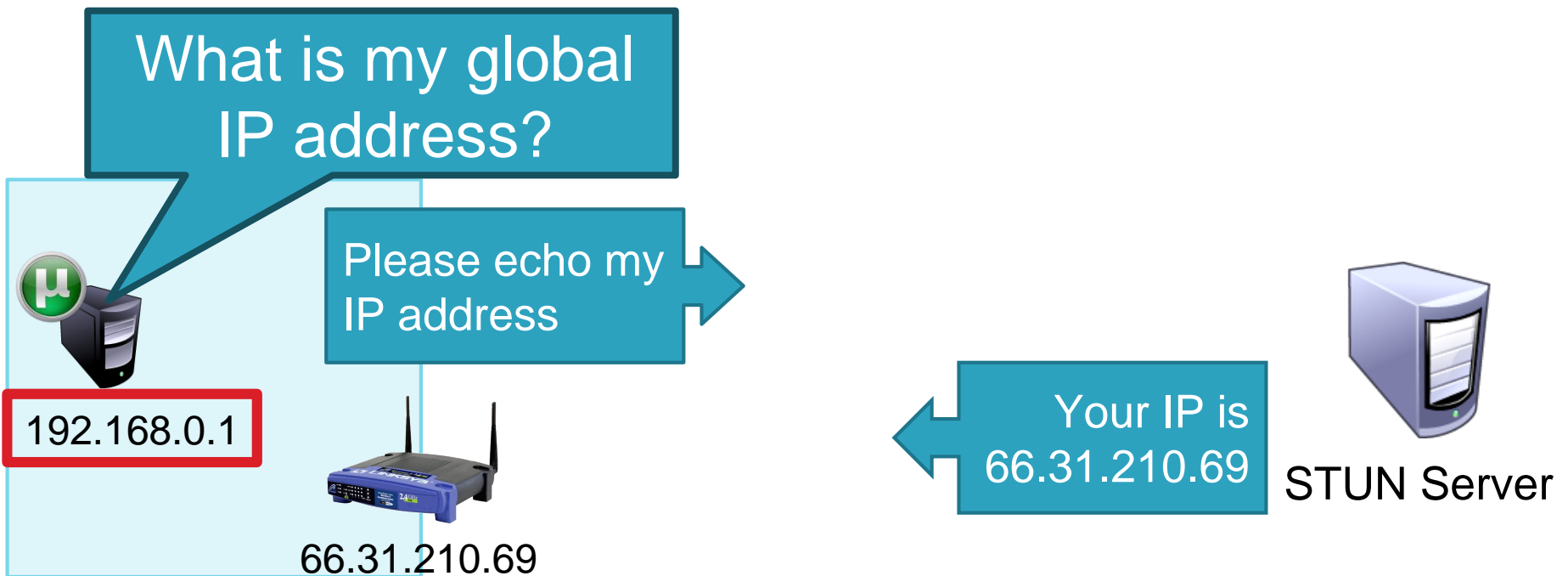
- Problem: Kommunikation von zwei Hosts (Sykpe-Anwendungen), die sich beide hinter NATs befinden und es ist kein „statisches“ Port Forwarding konfiguriert
- Hole Punching: NAT Einträge für die Kommunikation generieren



Lösungsansätze auf Anwendungsschicht:

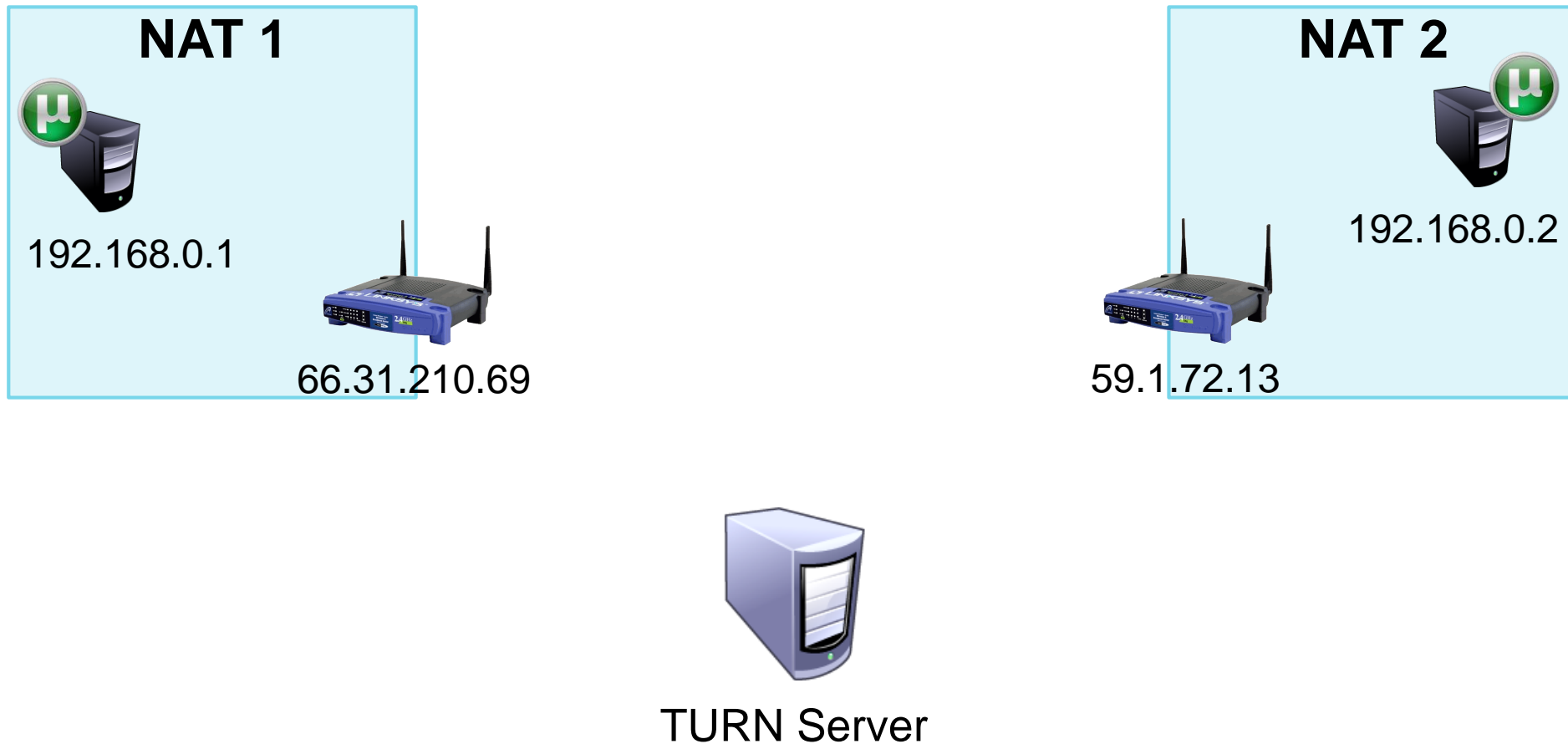
- STUN
- TURN

- STUN: Session Traversal Using NAT
- Prinzip: Rückgabe der globalen IP Adresse durch Anfrage an Server und Rückmeldung als Payload
 - dient zum Testen der Art von NAT
 - IP Adresse kann z.B. einem Server mitgeteilt werden



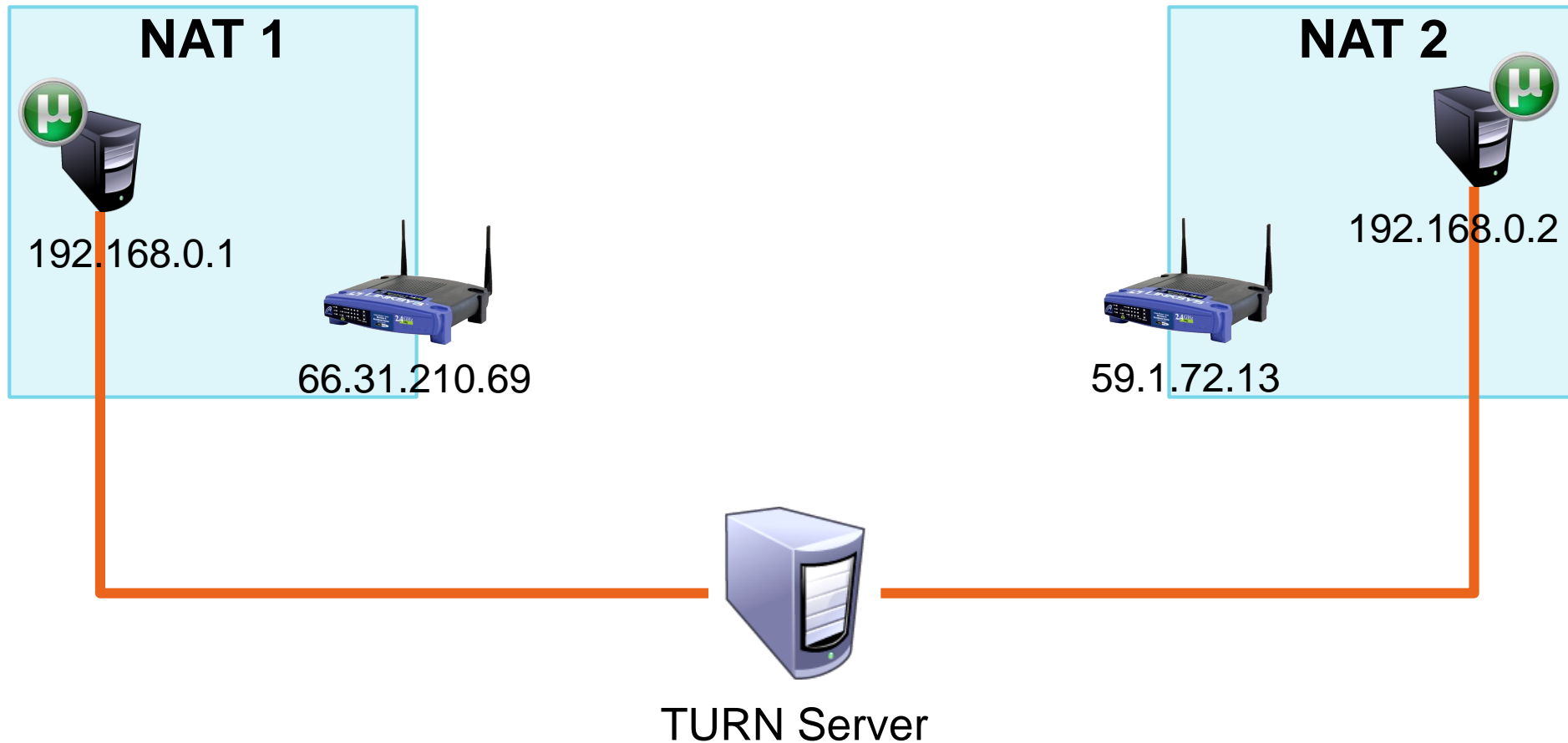
TURN

- TURN: Traversal Using Relays around NAT
- Prinzip: Öffnen eines NAT Ports und Mitteilung über TURN Server

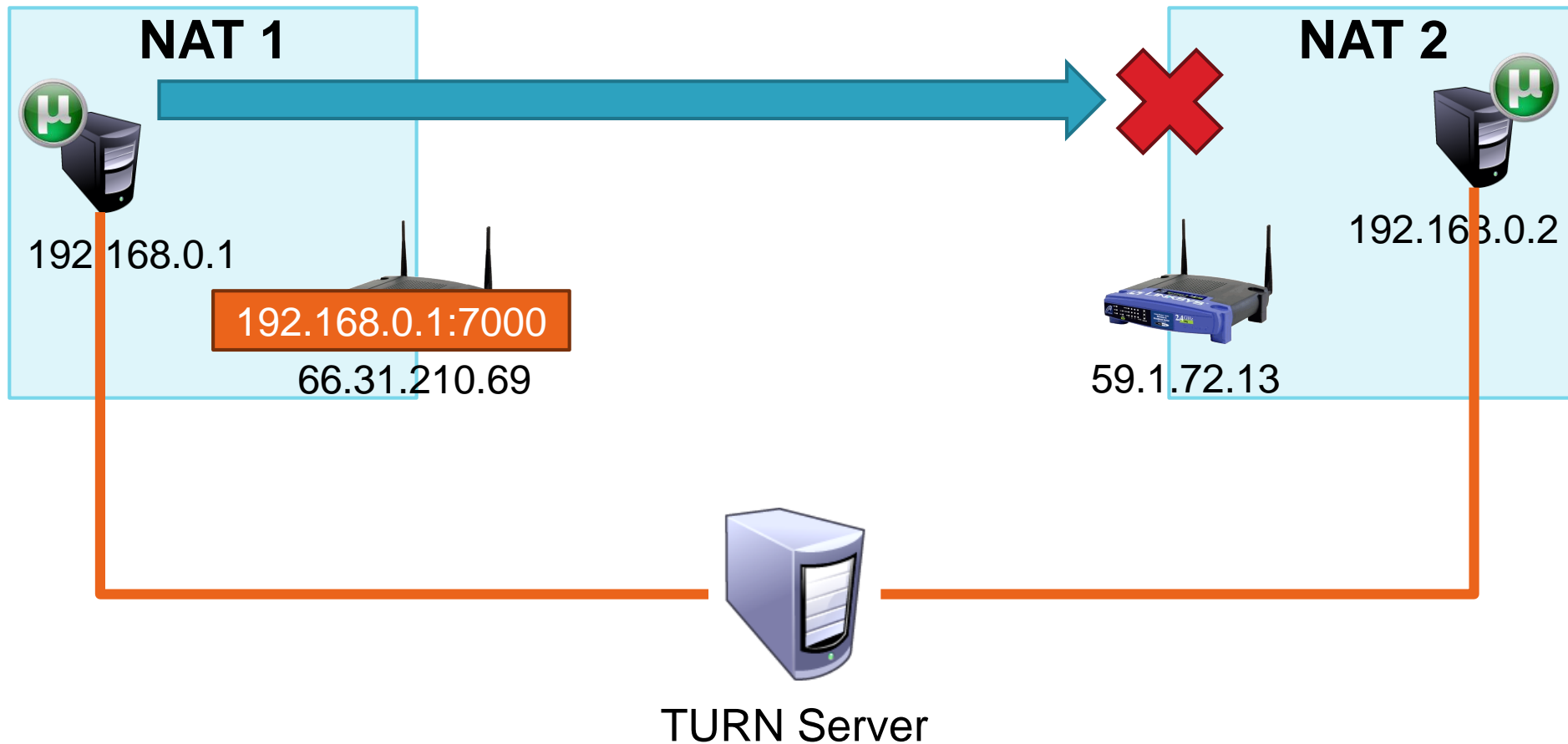


TURN

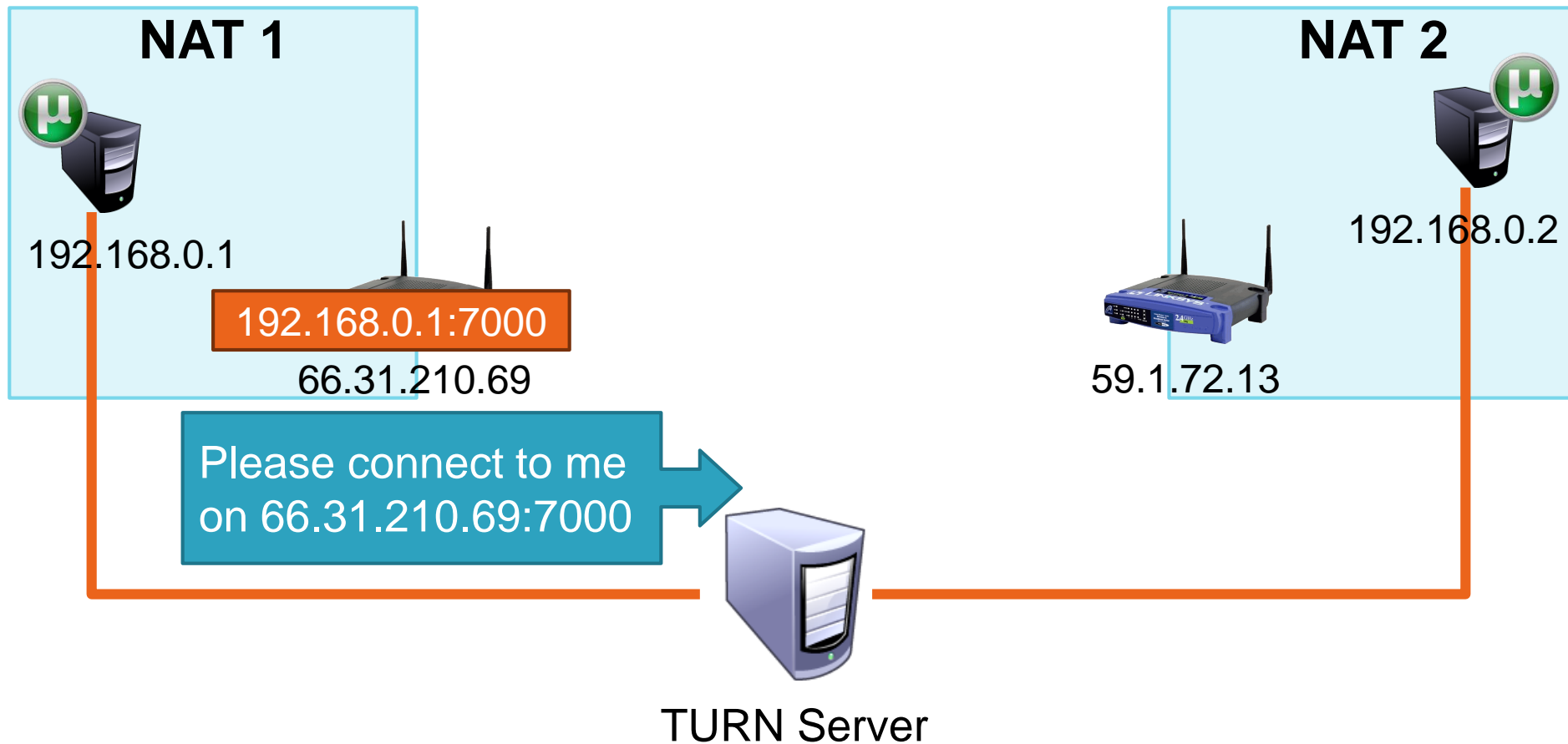
(1) Knoten nehmen Verbindung mit TURN Server auf, um IP-Adresse des NAT Gateways des Kommunikationspartners zu erfahren sowie einen Ziel-Port zu vereinbaren.



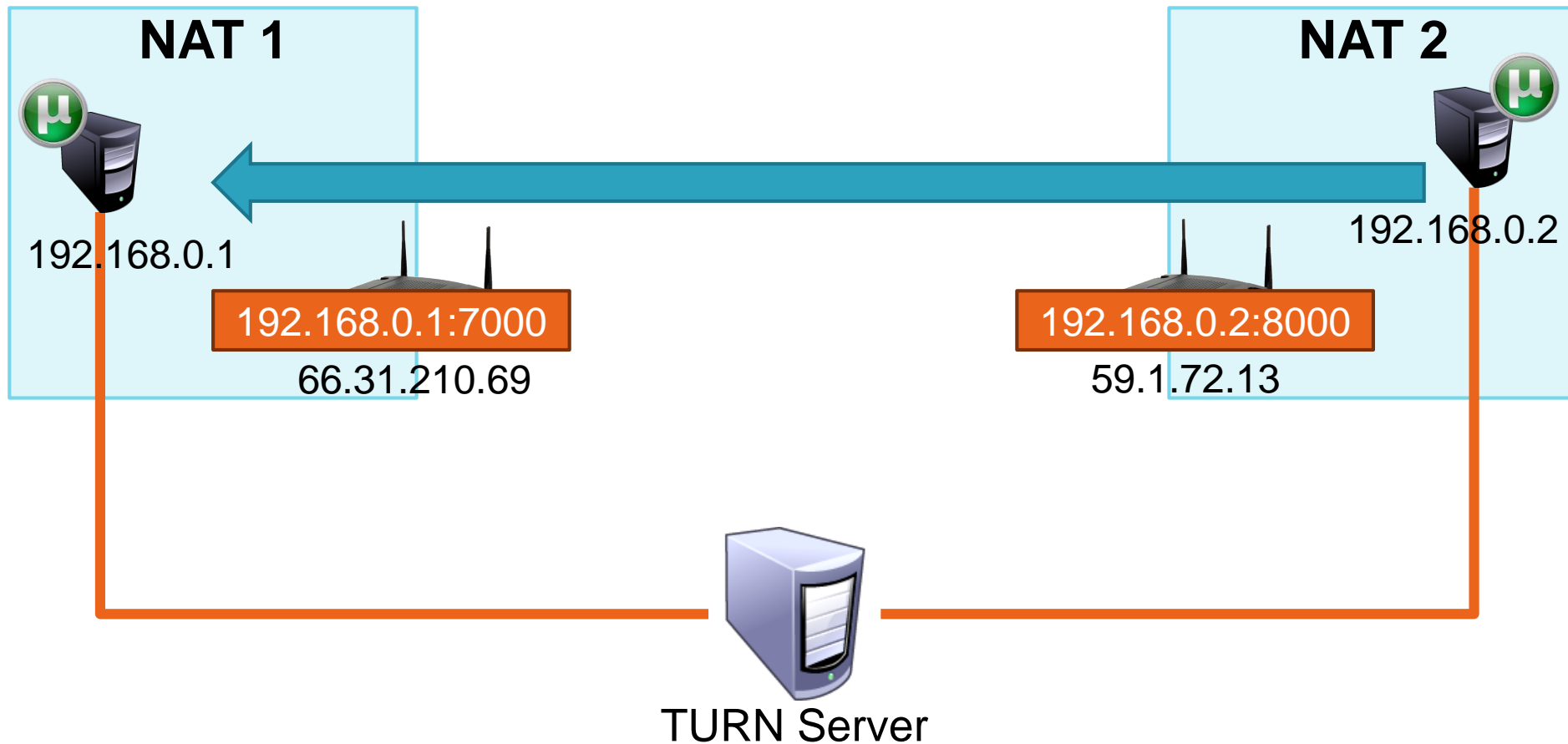
(2) Kommunikation mit Ziel-NAT-Gateway bewirkt Eintrag in NAT Table. Kommunikation wird von Ziel-NAT geblockt.



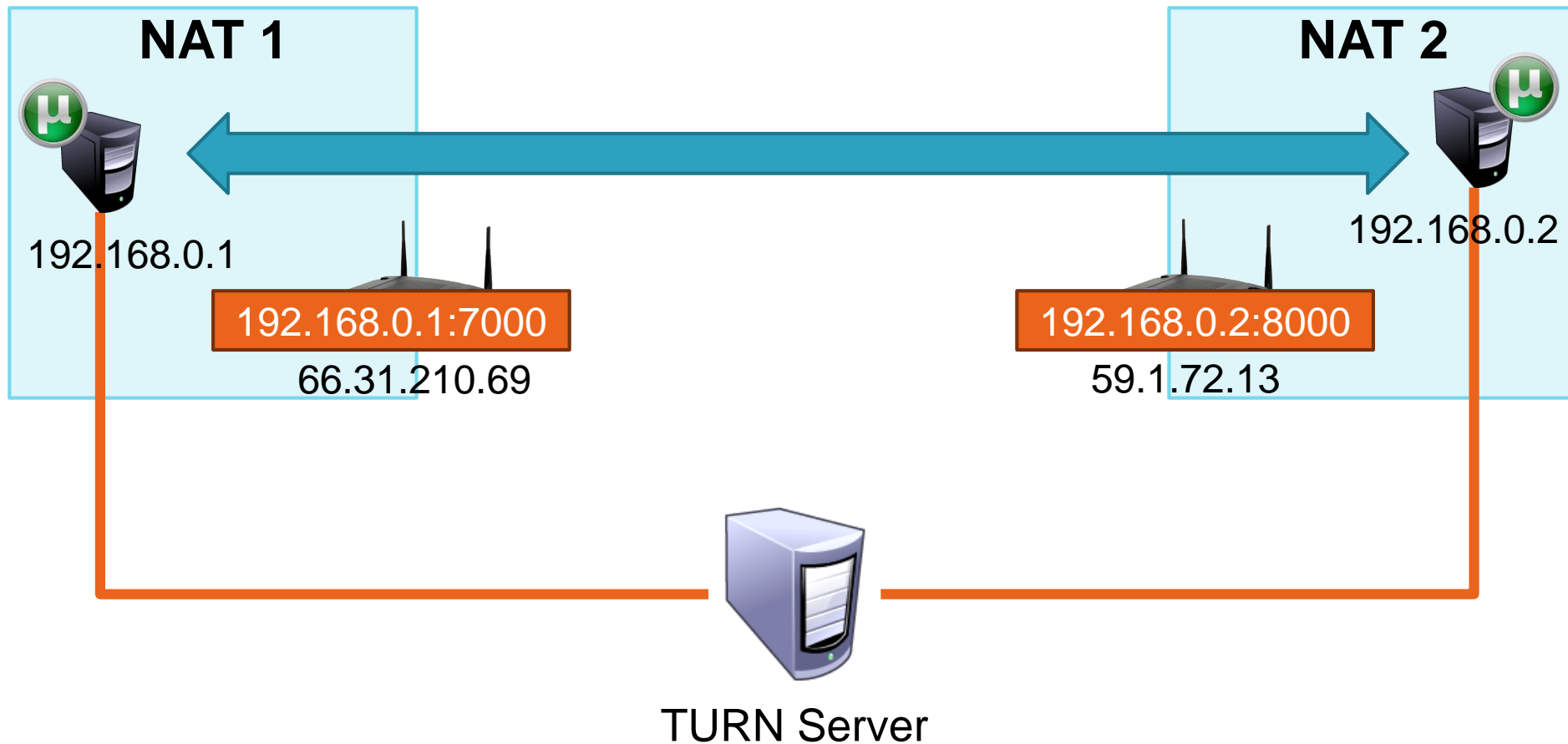
(3) Aufforderung an gegenüber, Nachricht auf offenen Port zu schicken.



(4) Nachricht auf „offenem“ NAT-Port.



(5) Verbindung ist aufgebaut und bi-direktionale Kommunikation ist möglich.



- Full Cone NAT:
 - Konsistentes Mapping von internem Adress+Port-Paar zu öffentlichem Adress+Port-Paar.
 - Weiterleitung von Paketen erfolgt ohne Überprüfung des Remote-Hosts
- Restricted Cone NAT:
 - wie Full Cone NAT, aber Pakete von externem Host werden nur weitergeleitet, wenn der interne Host bereits Pakete an diesen gesendet hat
- Port Restricted Cone NAT:
 - wie Restricted Cone NAT aber Pakete werden hier nur weitergeleitet, wenn der interne Host vorher Pakete an das Adress+Port-Paar des Remote Hosts gesendet hat.

- Symmetric NAT:
 - kein konsistentes Mapping von internem Adress+Port-Paar zu öffentlichem Adress+Port-Paar sondern socket-spezifisches Mapping
 - ein internes Adress+Port-Paar wird für verschiedene Ziel-Adress+Port-Paare auf unterschiedliche öffentliche Adress+Port-Paare abgebildet
 - gilt auch für UDP
 - Aufbau einer Verbindung zwischen zwei Hosts ist nicht möglich, wenn sich beide hinter Symmetric NATs befinden
 - Einziger Ausweg: Relaying aller Pakete z.B. über TURN Server
 - beispielsweise bei Skype (aber nicht über TURN Server)

Full Cone NAT

(1) S: 192.168.0.1:50000, D: 1.1.1.4:100 → S: 66.31.210.69:6000, D: 1.1.1.4:100

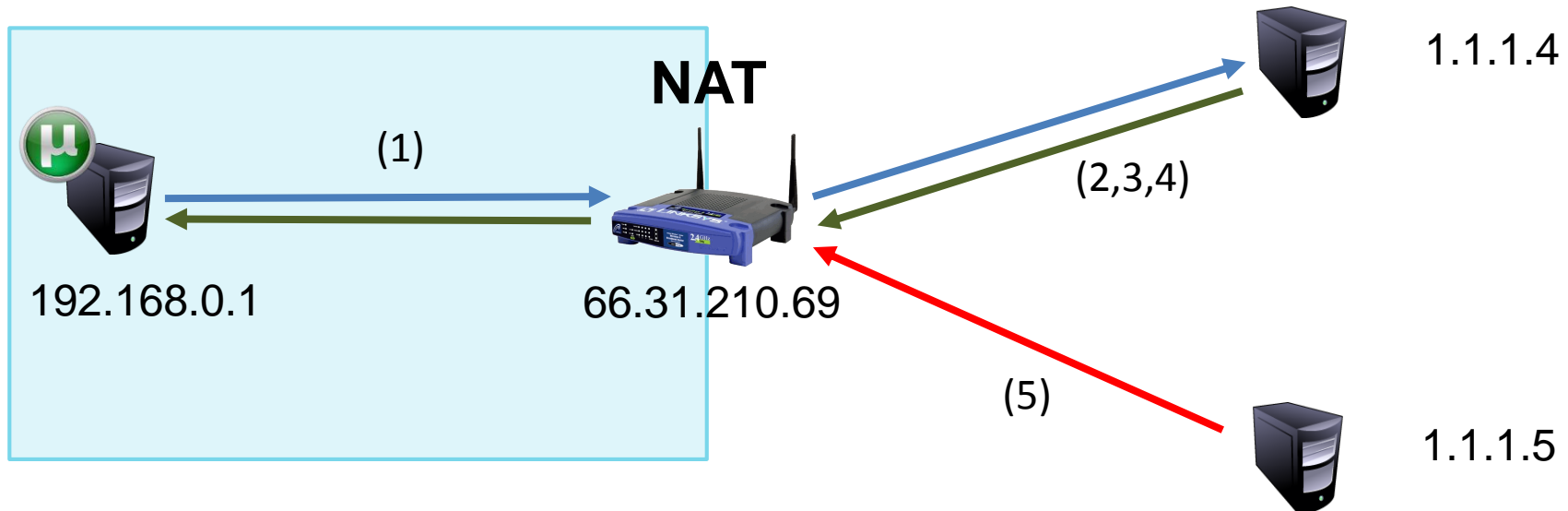
- NAT Table Entry 1

(2) S: 1.1.1.4:100, D: 66.31.210.69:6000 → S: 1.1.1.4:100, D: 192.168.0.1:50000

(3) S: 1.1.1.4:200, D: 66.31.210.69:6000 → S: 1.1.1.4:200, D: 192.168.0.1:50000

(4) S: 1.1.1.4:100, D: 66.31.210.69:5000 → blocked

(5) S: 1.1.1.5:200, D: 66.31.210.69:6000 → S: 1.1.1.5:200, D: 192.168.0.1:50000



NAT Table

1. 192.168.0.1:50000 ⇔ 66.31.210.69:6000 (allow ALL to 66.31.210.69:6000)

Restricted Cone NAT

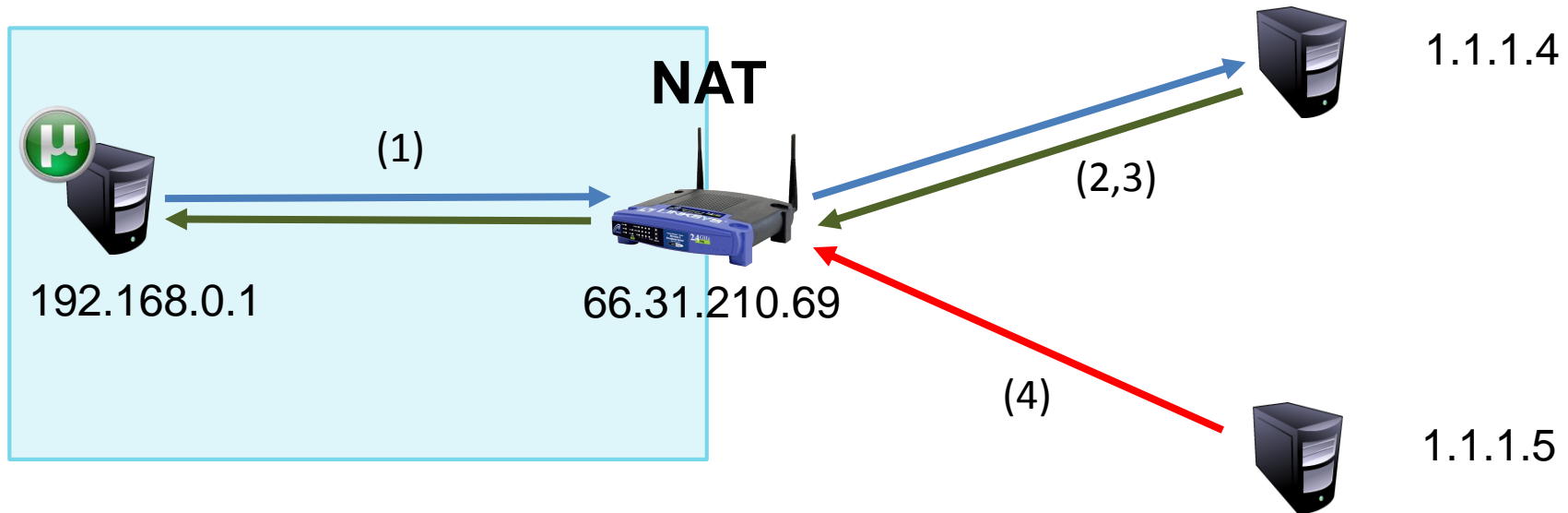
(1) S: 192.168.0.1:50000, D: 1.1.1.4:100 → S: 66.31.210.69:6000, D: 1.1.1.4:100

- NAT Table Entry 1

(2) S: 1.1.1.4:100, D: 66.31.210.69:6000 → S: 1.1.1.4:100, D: 192.168.0.1:50000

(3) S: 1.1.1.4:200, D: 66.31.210.69:6000 → S: 1.1.1.4:200, D: 192.168.0.1:50000

(4) S: 1.1.1.5:100, D: 66.31.210.69:6000 → blocked

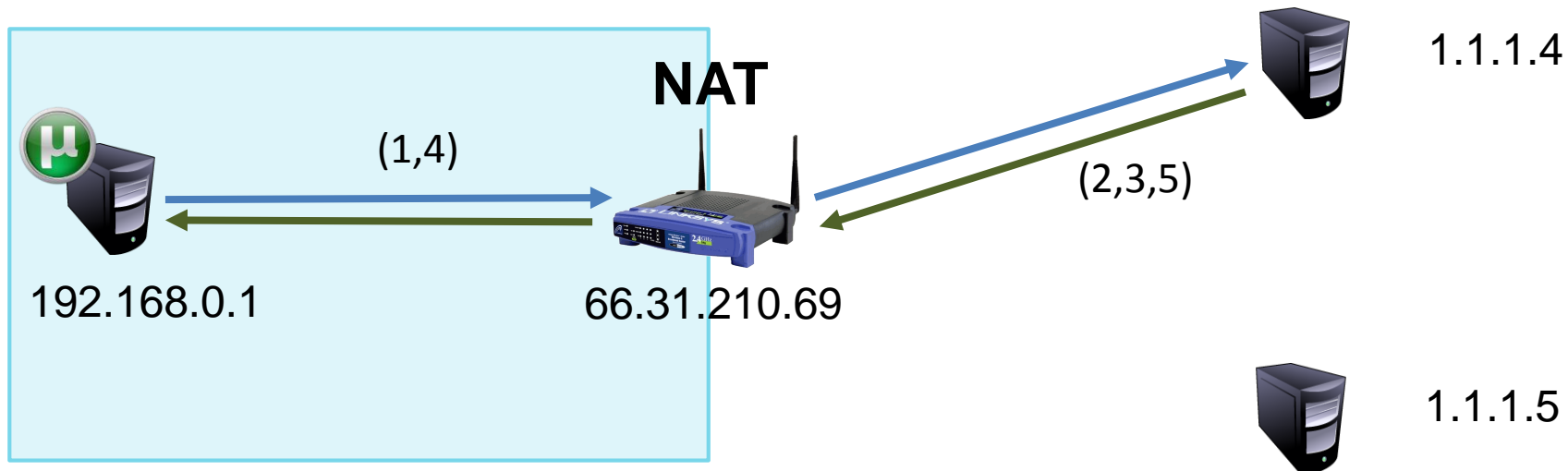


NAT Table

1. 192.168.0.1:50000 ⇔ 66.31.210.69:6000 (allow 1.1.1.4:* to 66.31.210.69:6000)

Port Restricted Cone NAT

- (1) S: 192.168.0.1:50000, D: 1.1.1.4:100 → S: 66.31.210.69:6000, D: 1.1.1.4:100
 - NAT Table Entry 1
- (2) S: 1.1.1.4:100, D: 66.31.210.69:6000 → S: 1.1.1.4:100, D: 192.168.0.1:50000
- (3) S: 1.1.1.4:200, D: 66.31.210.69:6000 → blocked
- (4) S: 192.168.0.1:50000, D: 1.1.1.4:200 → S: 66.31.210.69:6000, D: 1.1.1.4:200
 - NAT Table Entry 2
- (5) S: 1.1.1.4:200, D: 66.31.210.69:6000 → S: 1.1.1.4:200, D: 192.168.0.1:50000

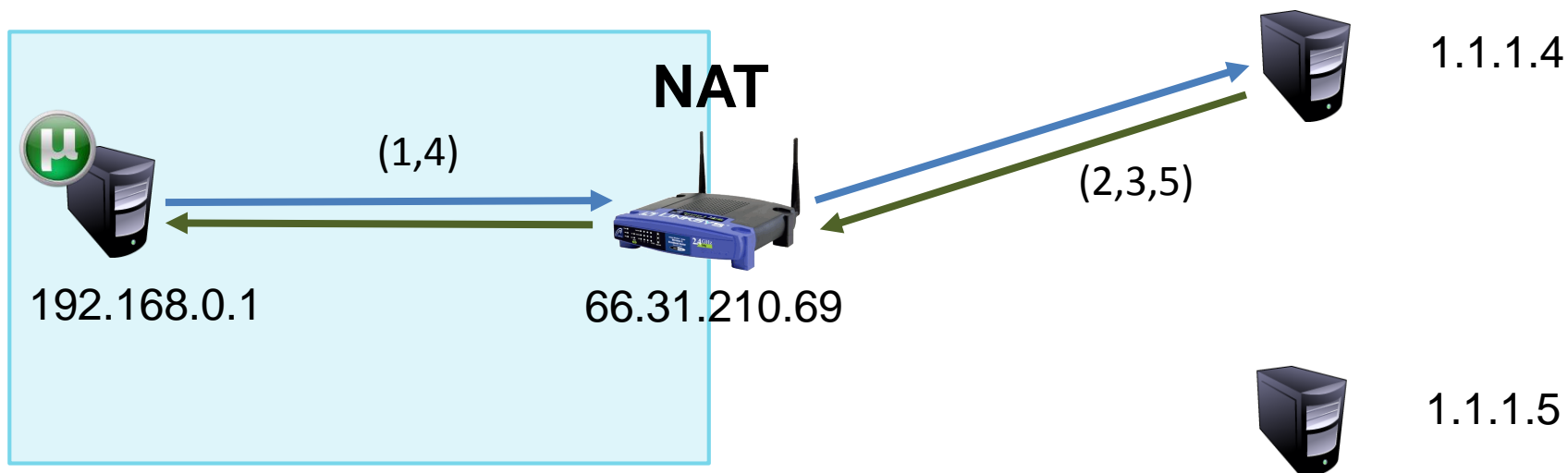


NAT Table

1. 192.168.0.1:50000 ⇔ 66.31.210.69:6000 (allow 1.1.1.4:100 to 66.31.210.69:6000)
2. 192.168.0.1:50000 ⇔ 66.31.210.69:6000 (allow 1.1.1.4:200 to 66.31.210.69:6000)

Symmetric NAT

- (1) S: 192.168.0.1:50000, D: 1.1.1.4:100 → S: 66.31.210.69:6000, D: 1.1.1.4:100
 - NAT Table Entry 1
- (2) S: 1.1.1.4:100, D: 66.31.210.69:6000 → S: 1.1.1.4:100, D: 192.168.0.1:50000
- (3) S: 1.1.1.4:200, D: 66.31.210.69:6000 → blocked
- (4) S: 192.168.0.1:50000, D: 1.1.1.4:200 → S: 66.31.210.69:7000, D: 1.1.1.4:200
 - NAT Table Entry 2
- (5) S: 1.1.1.4:200, D: 66.31.210.69:6000 → blocked

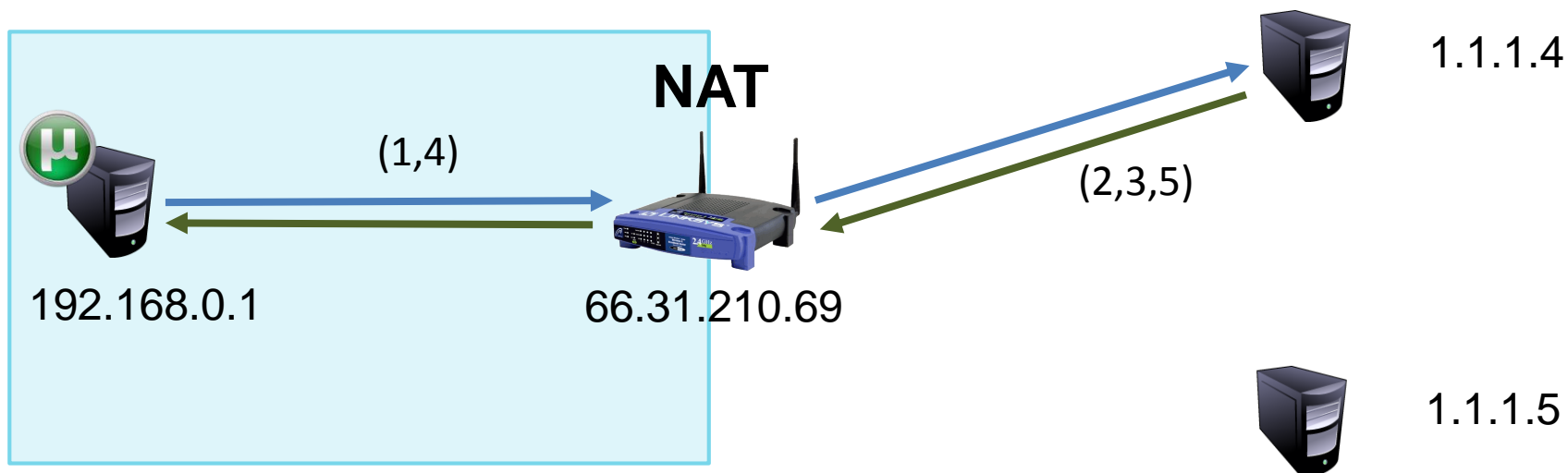


NAT Table

1. 192.168.0.1:50000 ⇔ 66.31.210.69:6000 (allow 1.1.1.4:100 to 66.31.210.69:6000)
2. 192.168.0.1:50000 ⇔ 66.31.210.69:7000 (allow 1.1.1.4:200 to 66.31.210.69:7000)

Symmetric NAT

- (1) S: 192.168.0.1:50000, D: 1.1.1.4:100 → S: 66.31.210.69:6000, D: 1.1.1.4:100
 - NAT Table Entry 1
- (2) S: 1.1.1.4:100, D: 66.31.210.69:6000 → S: 1.1.1.4:100, D: 192.168.0.1:50000
- (3) S: 1.1.1.4:200, D: 66.31.210.69:6000 → blocked
- (4) S: 192.168.0.1:50000, D: 1.1.1.4:200 → S: 66.31.210.69:7000, D: 1.1.1.4:200
 - NAT Table Entry 2
- (5) S: 1.1.1.4:200, D: 66.31.210.69:6000 → blocked

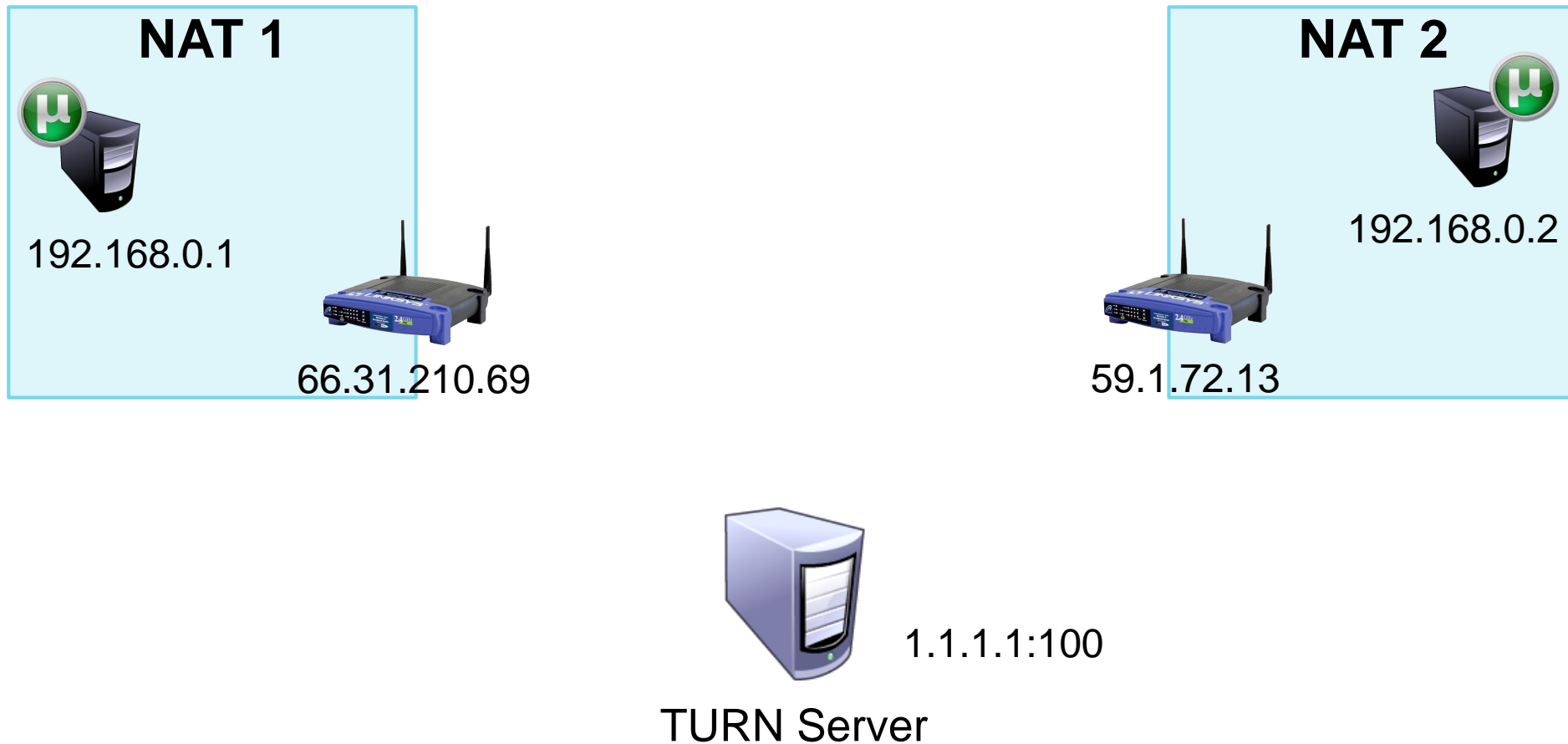


NAT Table

1. 192.168.0.1:50000 ⇔ 66.31.210.69:6000 (allow 1.1.1.4:100 to 66.31.210.69:6000)
2. 192.168.0.1:50000 ⇔ 66.31.210.69:7000 (allow 1.1.1.4:200 to 66.31.210.69:7000)

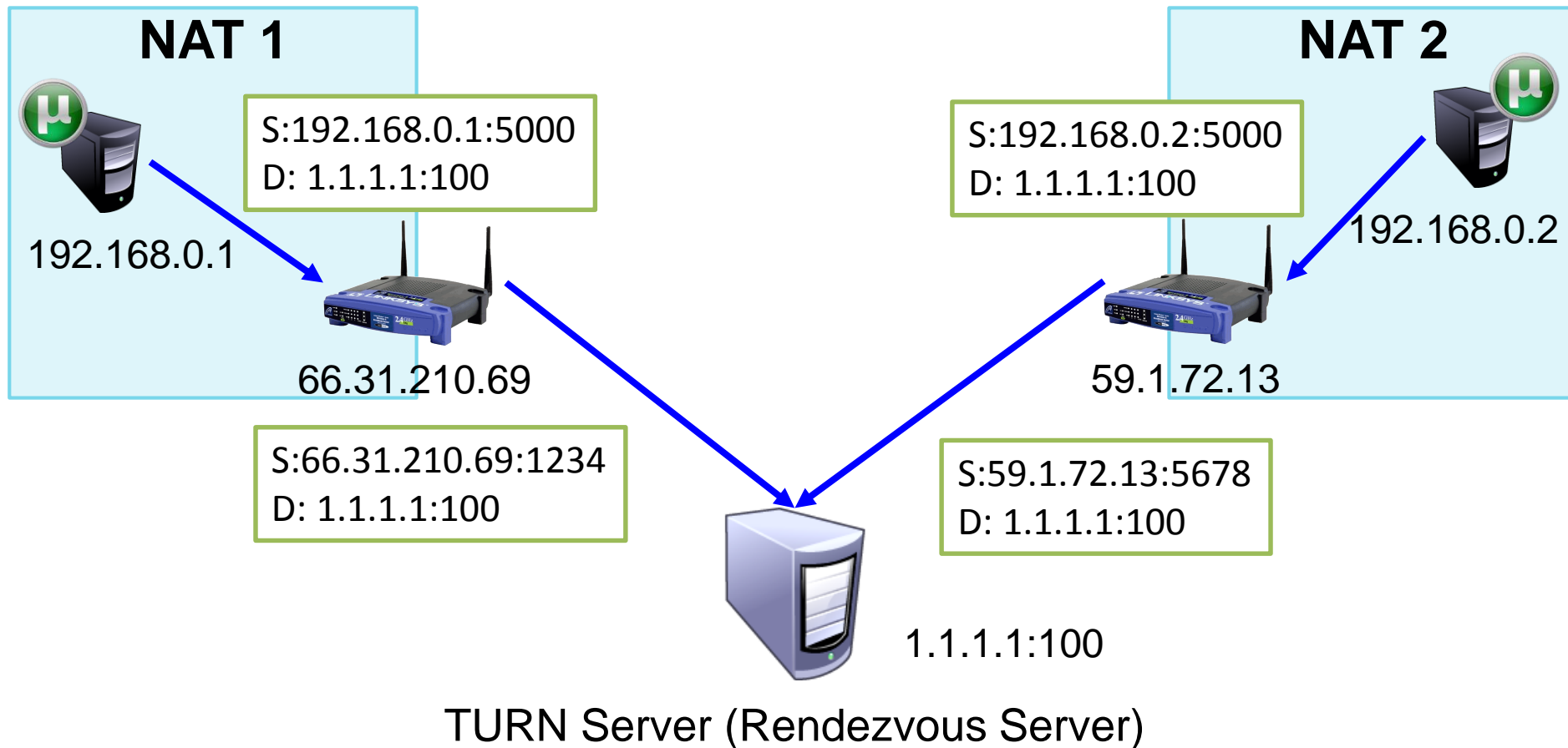
TURN with Port Restricted NAT

- Ziel: Kommunikation 192.168.0.1:5000 hinter NAT 1 mit 192.168.0.2:5000 hinter NAT 2 (Ports müssen nicht gleich sein)



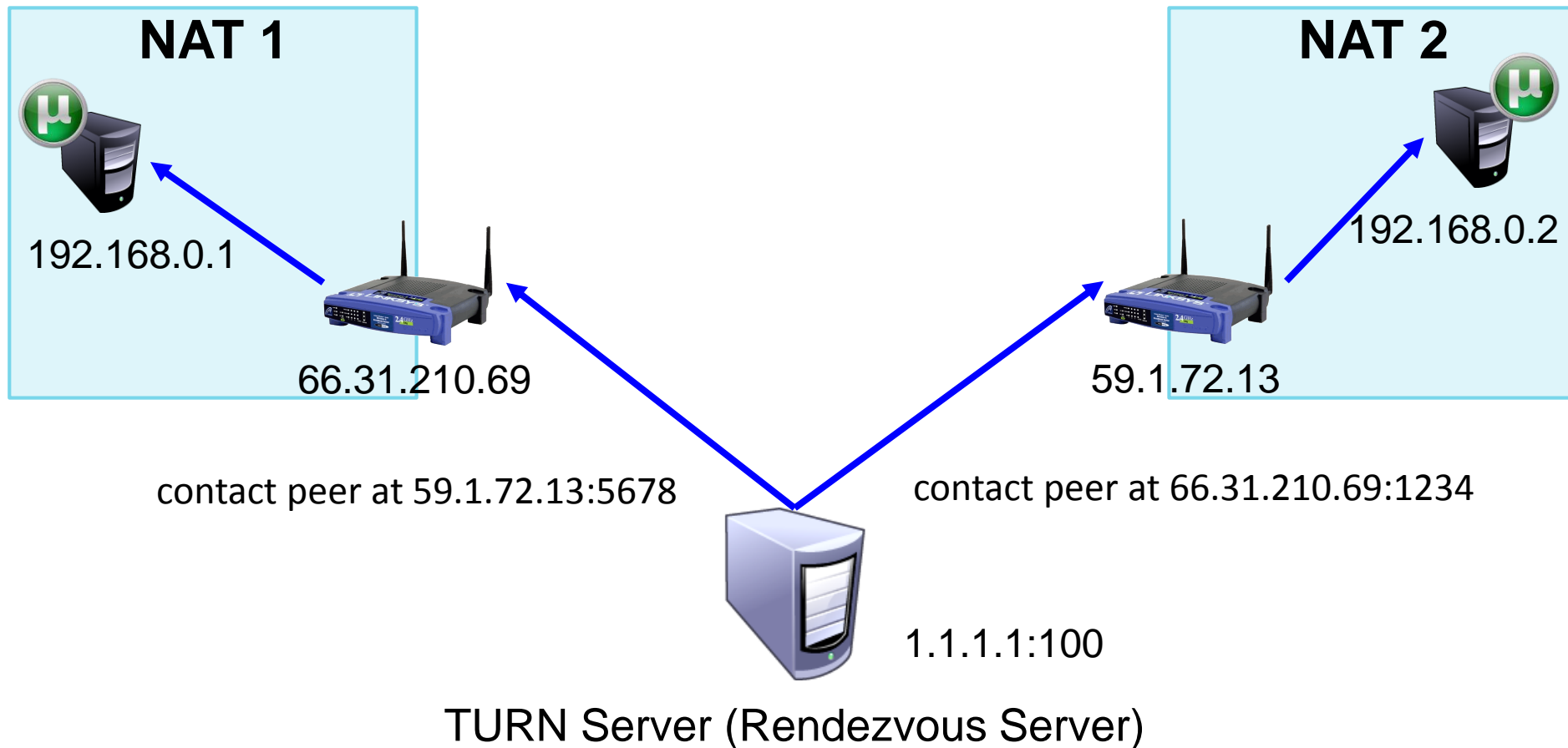
TURN with Port Restricted NAT

- Hosts hinter NAT kontaktieren Rendezvous (Turn) Server
- Rendezvous Server lernt offene Ports kennen, auf denen Verbindung stattfinden soll und weiß, dass
 - 192.168.0.1:5000 auf 66.31.210.69 gemappt wird



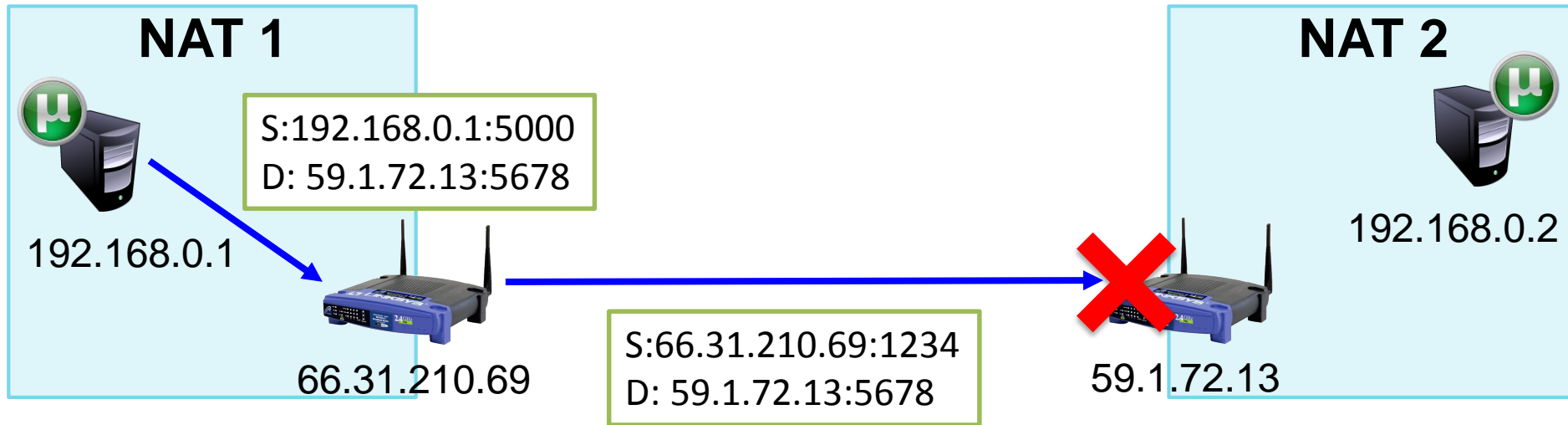
TURN with Port Restricted NAT

- Rendezvous Server mappt (wie auch immer) die Verbindungswünsche der beiden Hosts und teilt ihnen den offenen Port des jeweiligen Remote Hosts mit



TURN with Port Restricted NAT

- Host hinter NAT 1 schickt Paket an von TURN-Server erhaltenes Adress-Port-Paar
 - Paket wird von NAT 2 geblockt
 - Eintrag in NAT 1 wird erzeugt



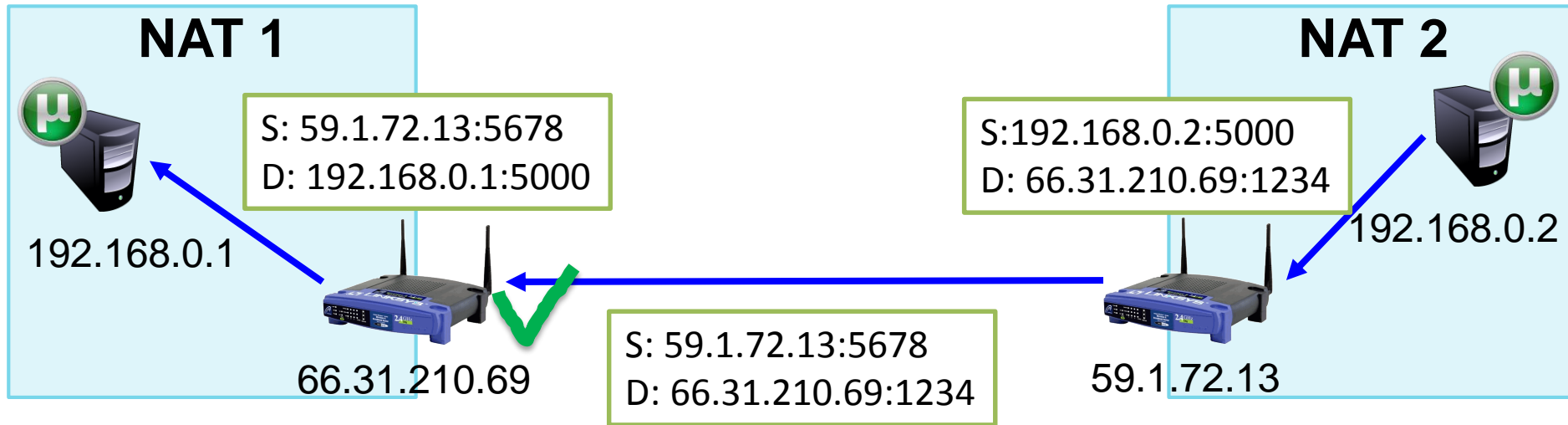
NAT 1 Table

192.168.0.1:5000 \leftrightarrow 66.31.210.69:1234

allow 59.1.72.13:5678 to 66.31.210.69:1234

TURN with Port Restricted NAT

- Host hinter NAT 2 schickt Paket an von TURN-Server erhaltenes Adress-Port-Paar
 - Paket wird von NAT 1 weitergeleitet
 - Eintrag in NAT 2 wird erzeugt



NAT 1 Table

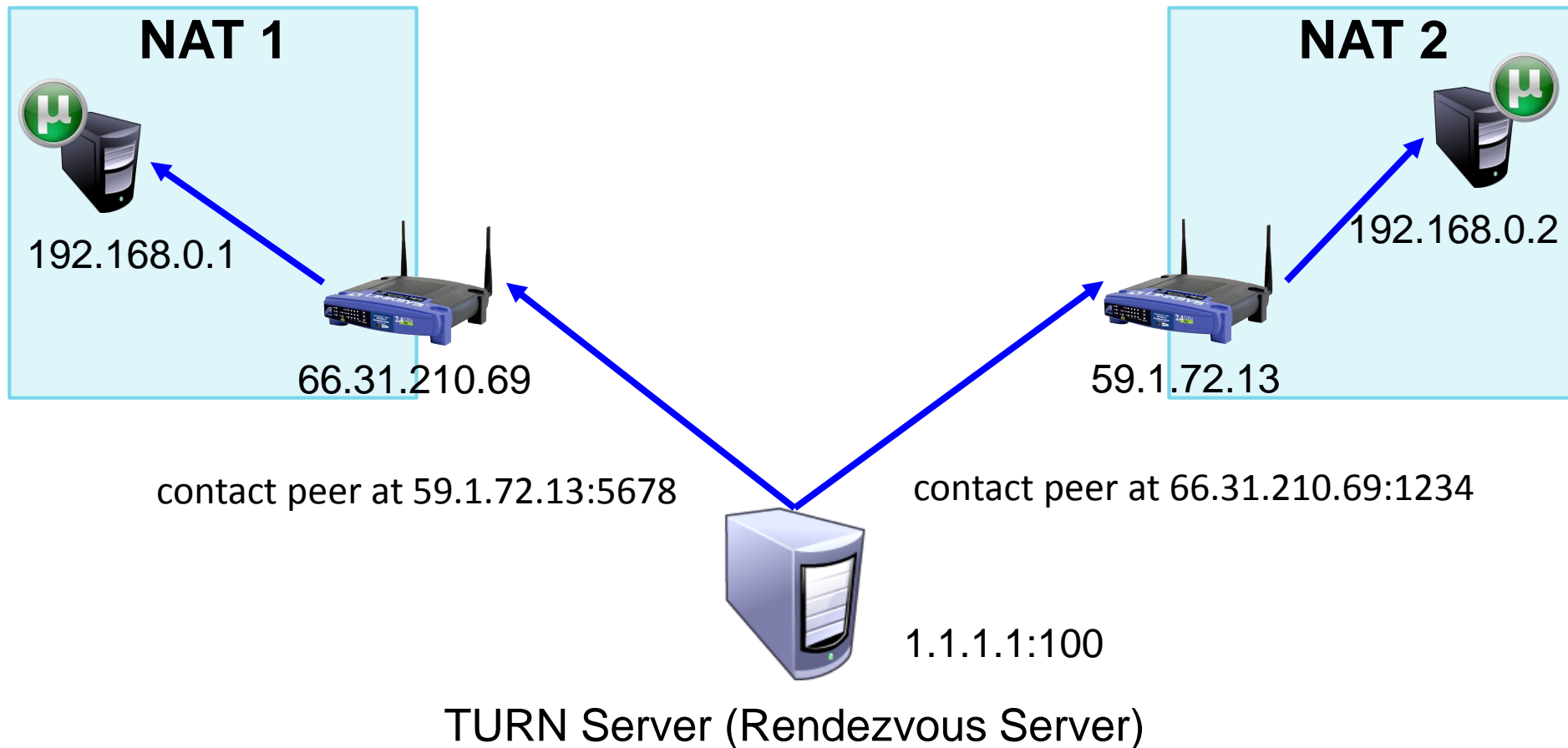
192.168.0.1:5000 ⇔ 66.31.210.69:1234
allow 59.1.72.13:5678 to 66.31.210.69:1234

NAT 2 Table

192.168.0.2:5000 ⇔ 59.1.72.13:5678
allow 66.31.210.69:1234 to 59.1.72.13:5678

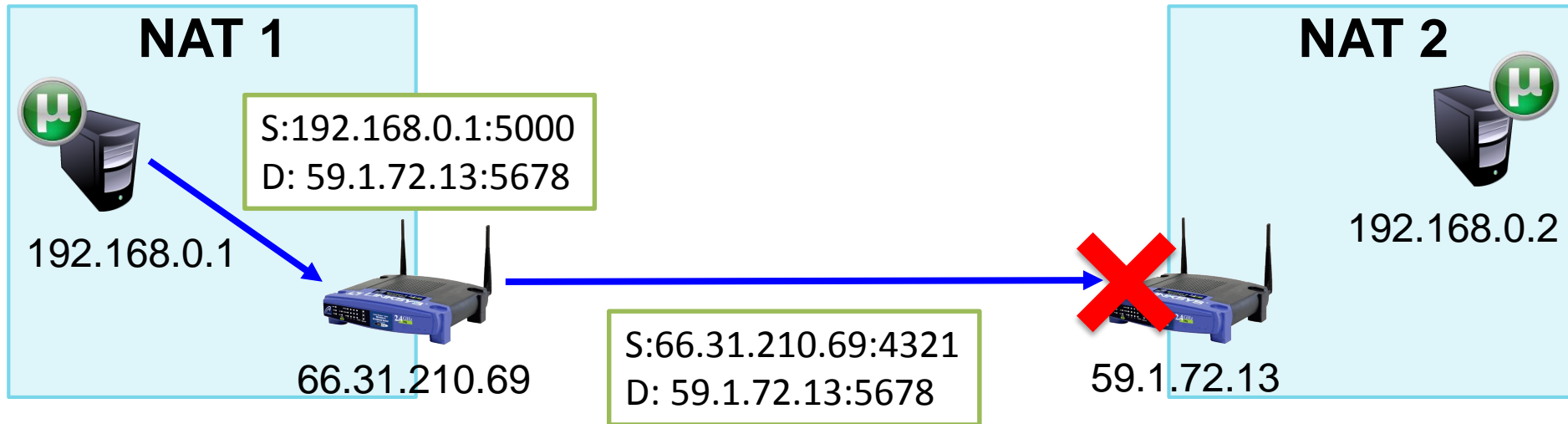
TURN with Symmetric NAT

- Rendezvous Server mappt (wie auch immer) die Verbindungswünsche der beiden Hosts und teilt ihnen den offenen Port des jeweiligen Remote Hosts mit



TURN with Symmetric NAT

- Host hinter NAT 1 schickt Paket an von TURN-Server erhaltenes Adress-Port-Paar
 - Paket wird von NAT 2 geblockt
 - Eintrag in NAT 1 wird erzeugt, aber mit anderem öffentlichem Adress+Port-Paar



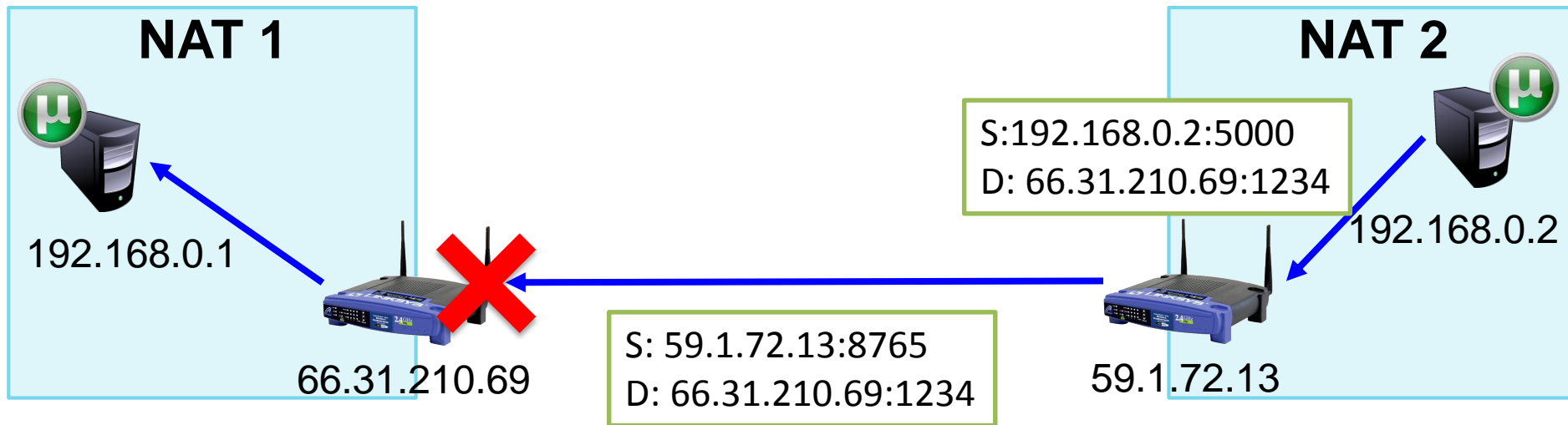
NAT 1 Table

192.168.0.1:5000 ⇔ 66.31.210.69:4321

allow 59.1.72.13:5678 to 66.31.210.69:4321

TURN with Symmetric NAT

- Host hinter NAT 2 schickt Paket an von TURN-Server erhaltenes Adress-Port-Paar
 - Paket wird von NAT 1 geblockt
 - Eintrag in NAT 2 wird erzeugt aber mit anderem Adress+Port-Paar
- Keine Kommunikation möglich



NAT 1 Table

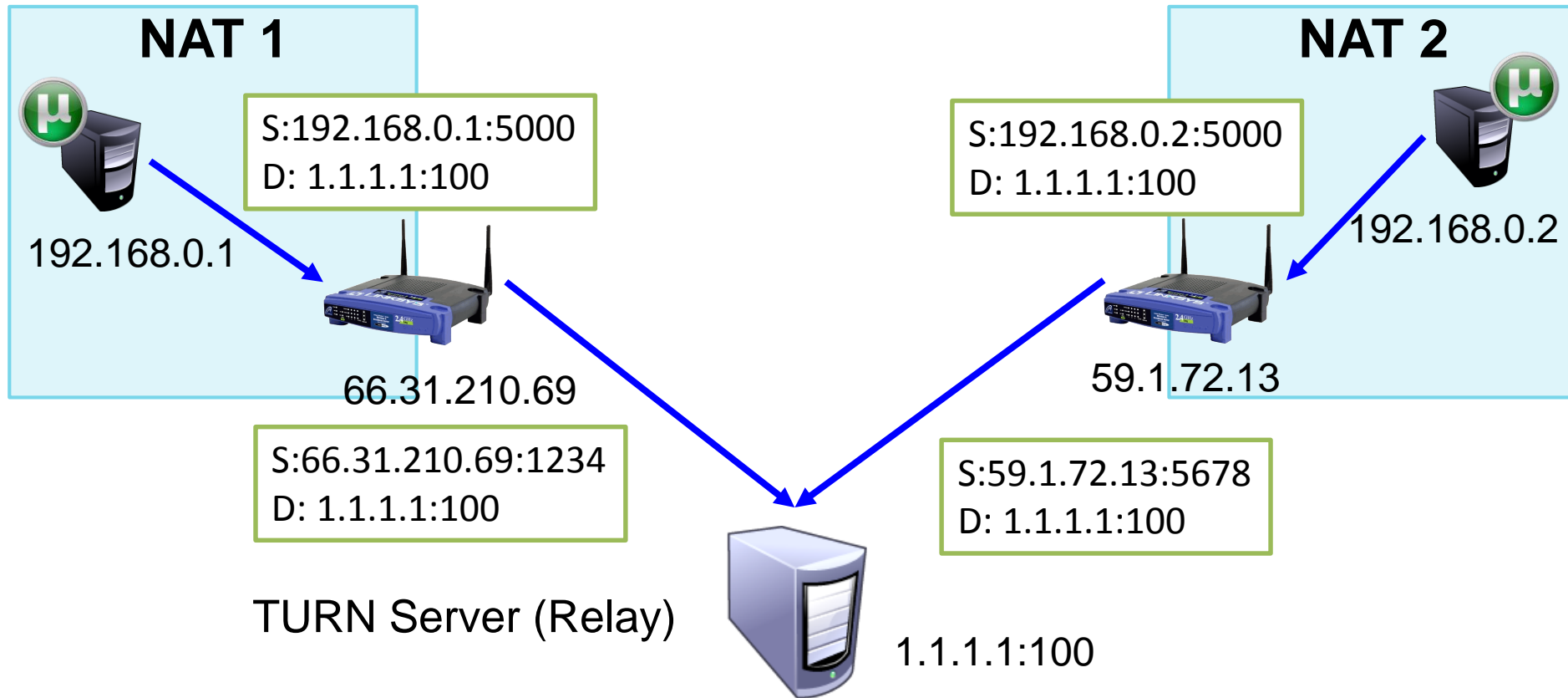
192.168.0.1:5000 ⇔ 66.31.210.69:4321
allow 59.1.72.13:5678 to 66.31.210.69:4321

NAT 2 Table

192.168.0.2:5000 ⇔ 59.1.72.13:8765
allow 66.31.210.69:1234 to 59.1.72.13:8765

TURN Lösung für Symmetric NAT

- Relaying aller Pakete über TURN Server



NAT 1 Table

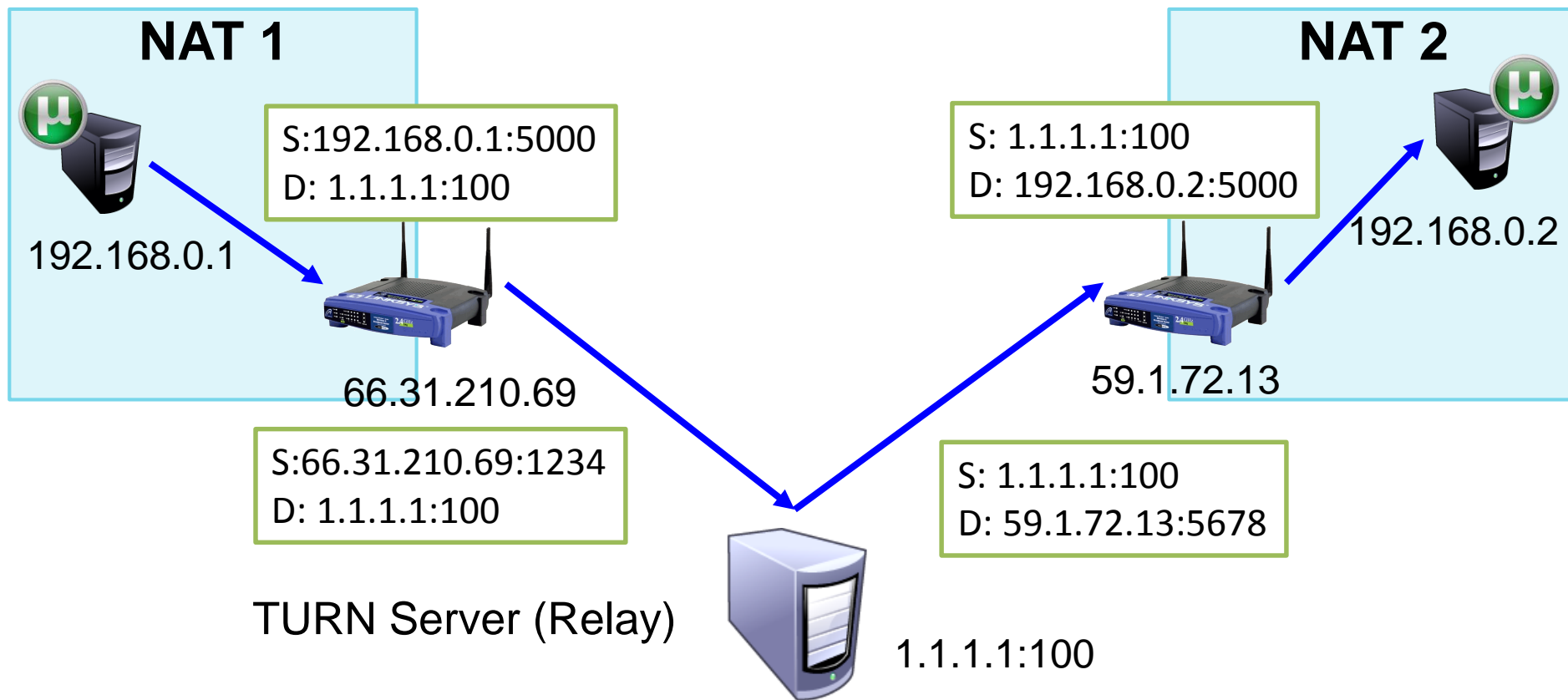
192.168.0.1:5000 ⇔ 66.31.210.69:1234
allow 1.1.1.1:100 to 66.31.210.69:1234

NAT 2 Table

192.168.0.2:5000 ⇔ 59.1.72.13:5678
allow 1.1.1.1:100 to 59.1.72.13:5678

TURN Lösung für Symmetric NAT

- Relaying aller Pakete über TURN Server, sehr teuer



NAT 1 Table

192.168.0.1:5000 \Leftrightarrow 66.31.210.69:1234
allow 1.1.1.1:100 to 66.31.210.69:1234

NAT 2 Table

192.168.0.2:5000 \Leftrightarrow 59.1.72.13:5678
allow 1.1.1.1:100 to 59.1.72.13:5678

- NA(P)T ermöglicht Kommunikation von privatem Netz mit dem Internet
- Abbildung von privater Adresse auf öffentliche Adresse
 - öffentliche/private ISP IP -> private Kunden IP
 - öffentliche ISP IP -> private ISP IP
 - auch zwischen IPv4 und IPv6
 - meist Abbildung zwischen Adress+Port-Paaren
- Eingeschränkte Kontaktaufnahme von außen:
 - Full Cone, Restrict Cone, Port-Restricted Cone NAT
 - Symmetric NAT
- Konkataufnahme möglich über
 - Konfiguration im NAT mit Port Forwarding
 - UDP Hole Punching (STUN, TURN)
 - Relaying: Kommunikation über einen Server, der nicht hinter einem NAT sitzt (Skype, P2P)

- Typisch: LSN und CPE NAT
 - Large Scale NAT (LSN): Public IPv4 auf Private IPv4 (ISP Ebene)
 - Customer Premises Equipment (CPE) NAT: Private IPV4 (ISP) auf private IPv4 (Home)

Mehr-stufiges NAT:
CPE (DSL Router) erhält vom ISP keine öffentliche sondern eine private IP Adresse. DSL Router nutzt wiederum NAT, um mit der einen „ISP-privaten“ Adresse ein privates Heimnetz zu betreiben.

