# 464XLAT Trial in einem IPv6-only Mobilfunknetz

Vodafone Innovation Park

**Johannes Spanier**
**IPv6 Kongress 2014**

Want to play along? → SSID 464XLAT

- tethered IPv6-only Mobilfunkverbindung
- CLAT auf dem Hot-Spot
- leider sehr schlechter Empfang im Saal

# Standortbestimmung

## Wo stehen wir aktuell mit IPv6 in Mobilfunk-Netzen?

| | |
|---|---|
| Mobile Packet Data Access Network | Alle Transportnetz Elemente im Mobilfunknetz für IPv6 abgenommen.<br>BGP Peerings etbliert.<br>Noch angepasste Mechanismen für Redundanz benötigt. |
| Endgeräte | Aktuelle Gerätegeneration mit LTE grundsätzlich durchgängig IPv6 fähig. |
| Dual-Stack | Roll-out Projekt läuft. Abschluss dieses Geschäftsjahr zunächst für ein spezifisches Mobilfunkprodukt erwartet. |
| DHCPv6 Prefix Delegation | Funktionalität erfolgreich getestet. Wird zum Start von Dual-Stack zur Verfügung stehen. |
| Backendsysteme / Middleboxen | Viele sind noch anzupassen. Im angepeilten Produkt nicht relevant für die Einführung |

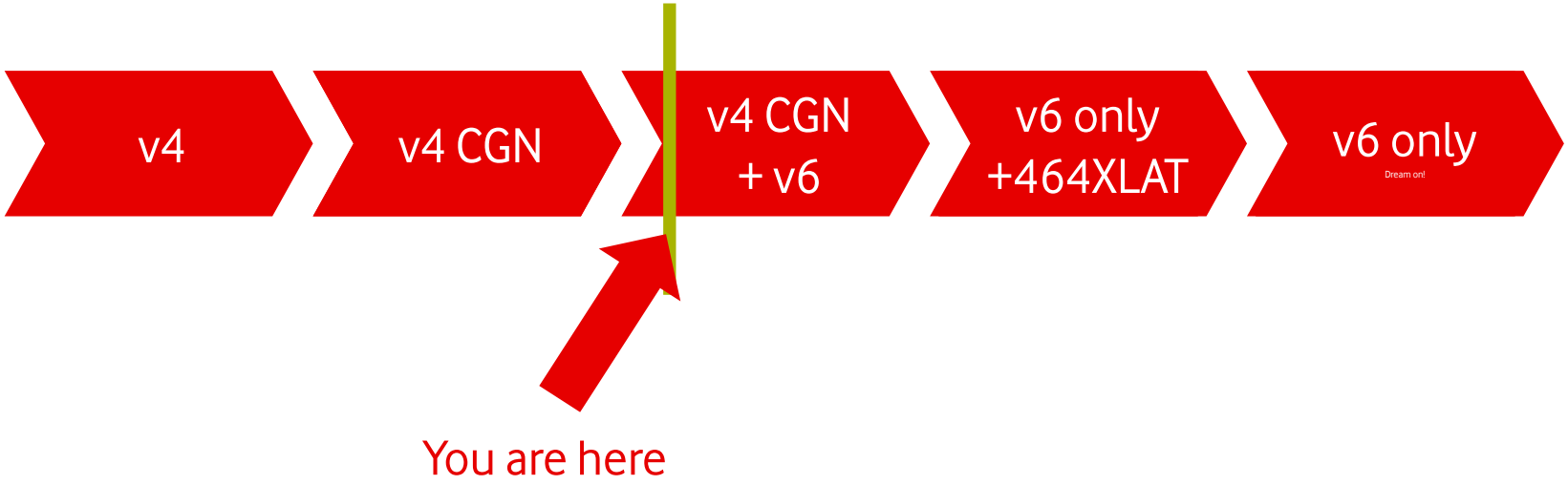




SSID: 464XLAT

Vodafone Innovation Park

# Wie geht´s weiter?





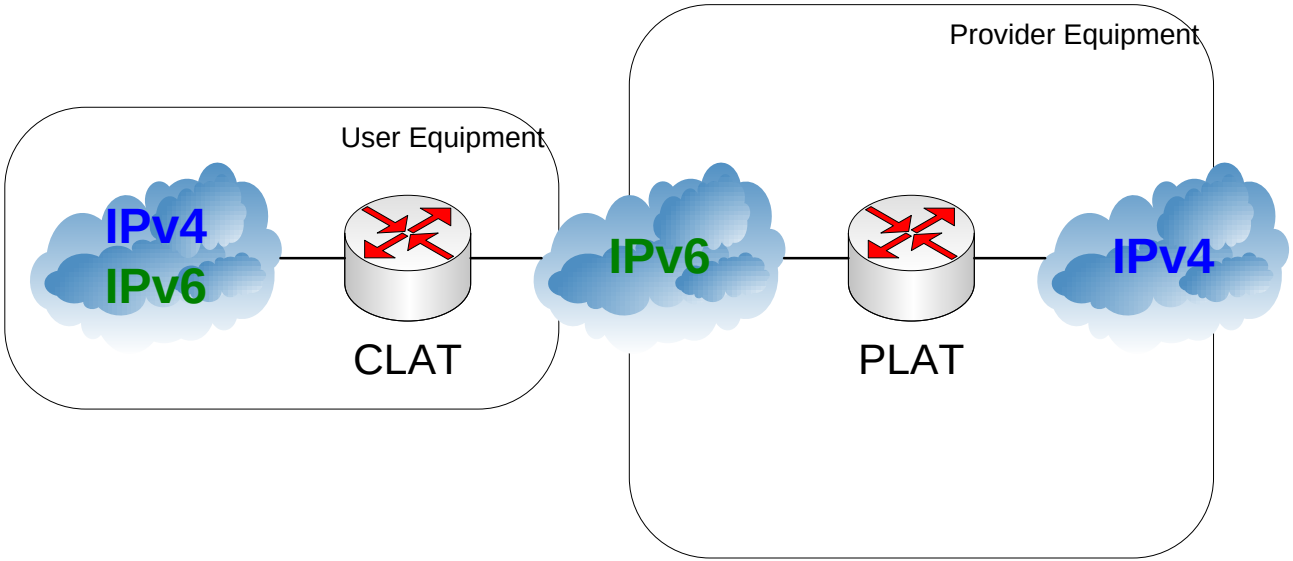



SSID: 464XLAT

Vodafone Innovation Park

# 464XLAT

# 464XLAT Architektur



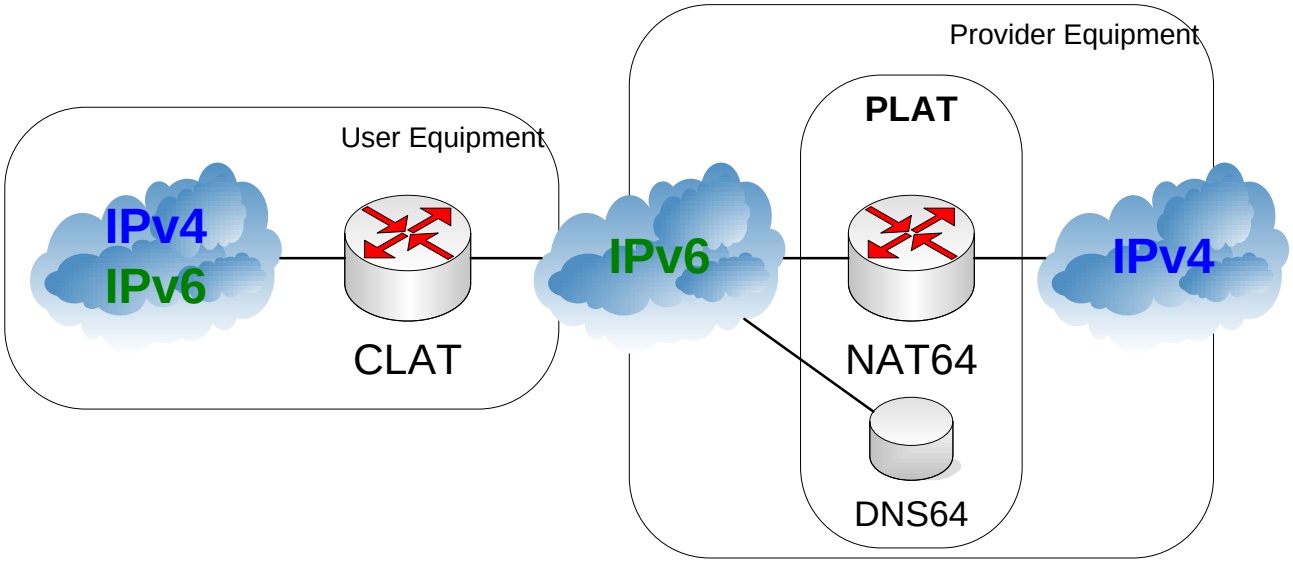





SSID: 464XLAT

Vodafone Innovation Park

# 464XLAT Architektur



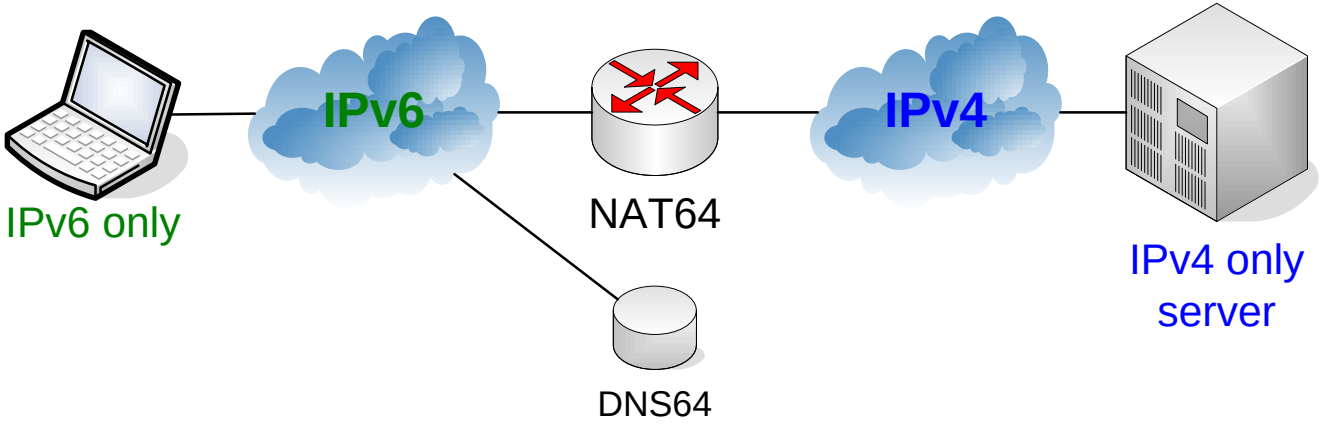





SSID: 464XLAT

Vodafone Innovation Park

# NAT64 Architektur



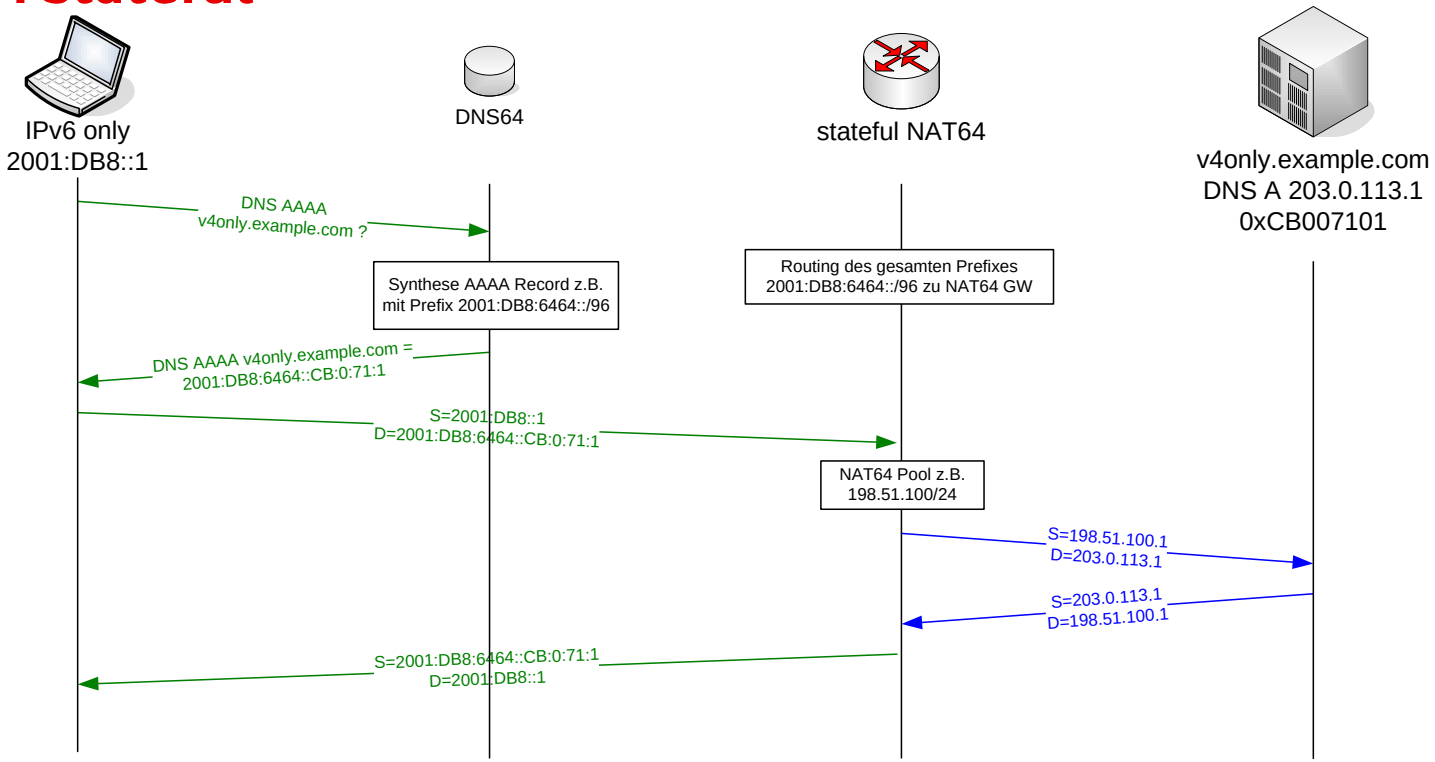





SSID: 464XLAT

Vodafone Innovation Park

# NAT64 stateful



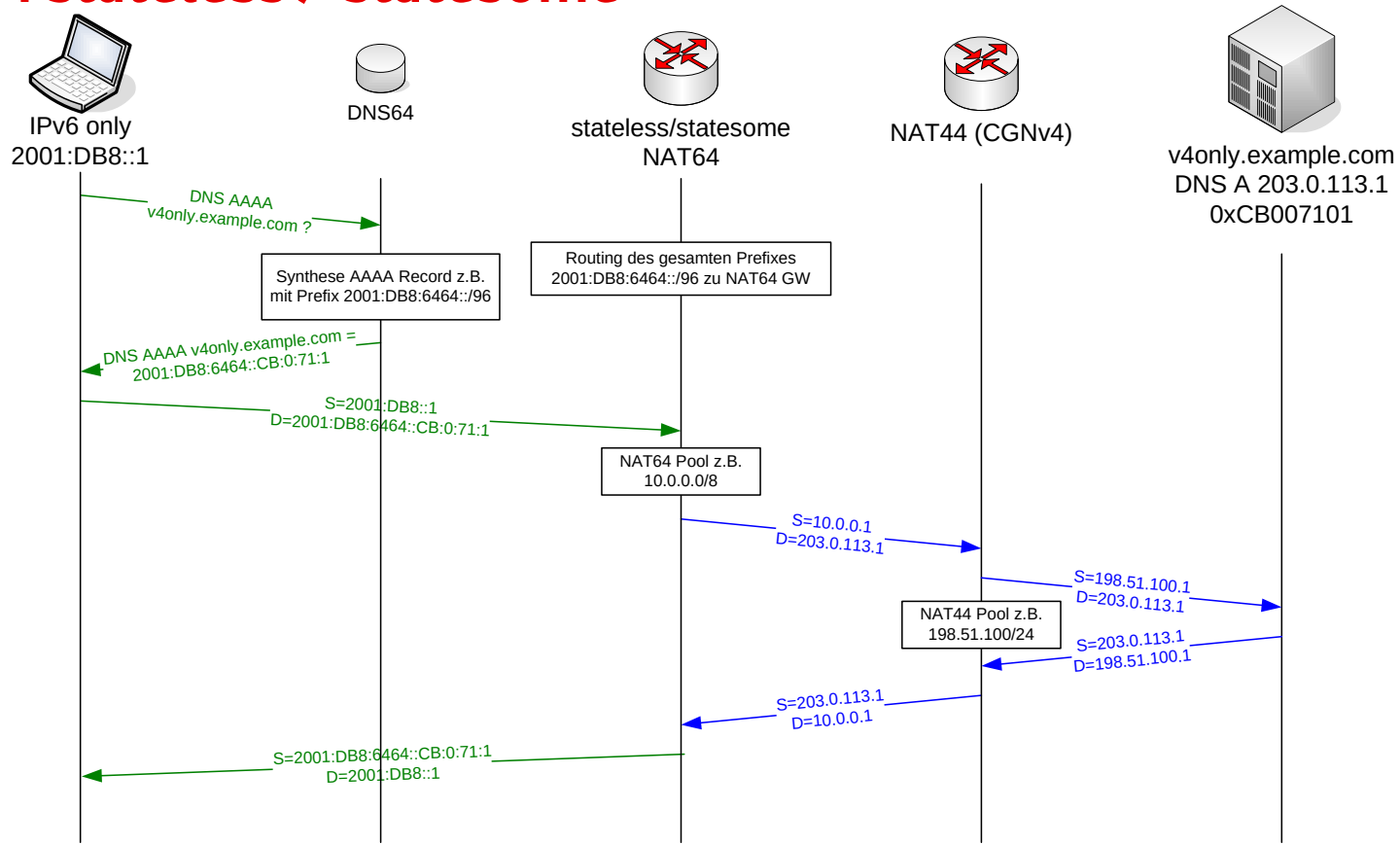





SSID: 464XLAT

Vodafone Innovation Park

# NAT64 stateless / statesome








SSID: 464XLAT

Vodafone Innovation Park

# NAT64 Varianten

| NAT64 Variante | stateless | statesome | stateful | statesome + CGNv4 |
|---|---|---|---|---|
| Übersetzung v6:v4 | 1:1 | 1:1 | N:1 | N:1 |
| IPv4 Pool Nutzung | statisch | dynamisch | dynamisch | dynamisch |
| Einsparung IPv4 | Nein | Nein | Ja | Ja |
| Ende-zu-Ende Transparenz IPv4 | Ja | Nein | Nein | Nein |
| nutzt vorhandene CGN Infrastruktur | Nein | Nein | Nein | Ja |





SSID: 464XLAT

# NAT64 - Was geht nicht?

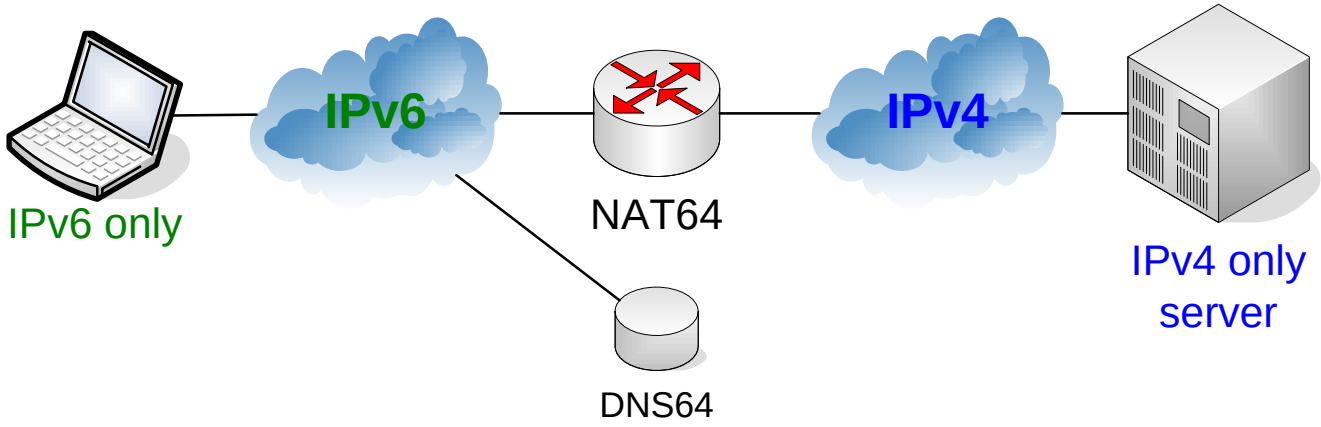
| | |
|---|---|
| IPv4 Literale | http://203.0.113.1/index.html<br>Keine DNS Anfrage → Synthetisierung von AAAA DNS Records nicht möglich |
| v4-only sockets | senden von IPv6 Paketen nicht möglich |
| DNSSec | Synthetisierung von AAAA DNS Records durch DNS64 Resolver<br>keine Prüfung der Antwort am Client möglich<br>OK wenn DNSSec dem DNS64 vertraut |
| v4 Internet zu v6 Server@User | nur bei statischem NAT64 möglich<br>Dynamische Pools und stateful NAT64 → Ende-zu-Ende Transparenz nicht vorhanden |





SSID: 464XLAT

# NAT64



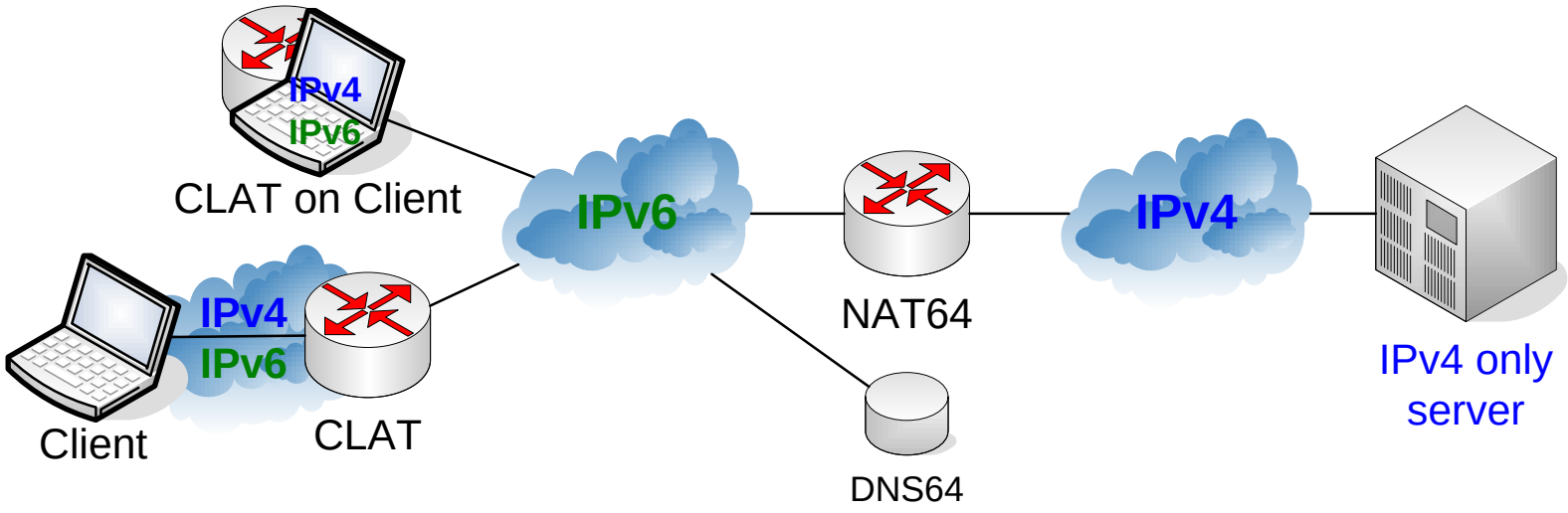





SSID: 464XLAT

Vodafone Innovation Park

# 464XLAT





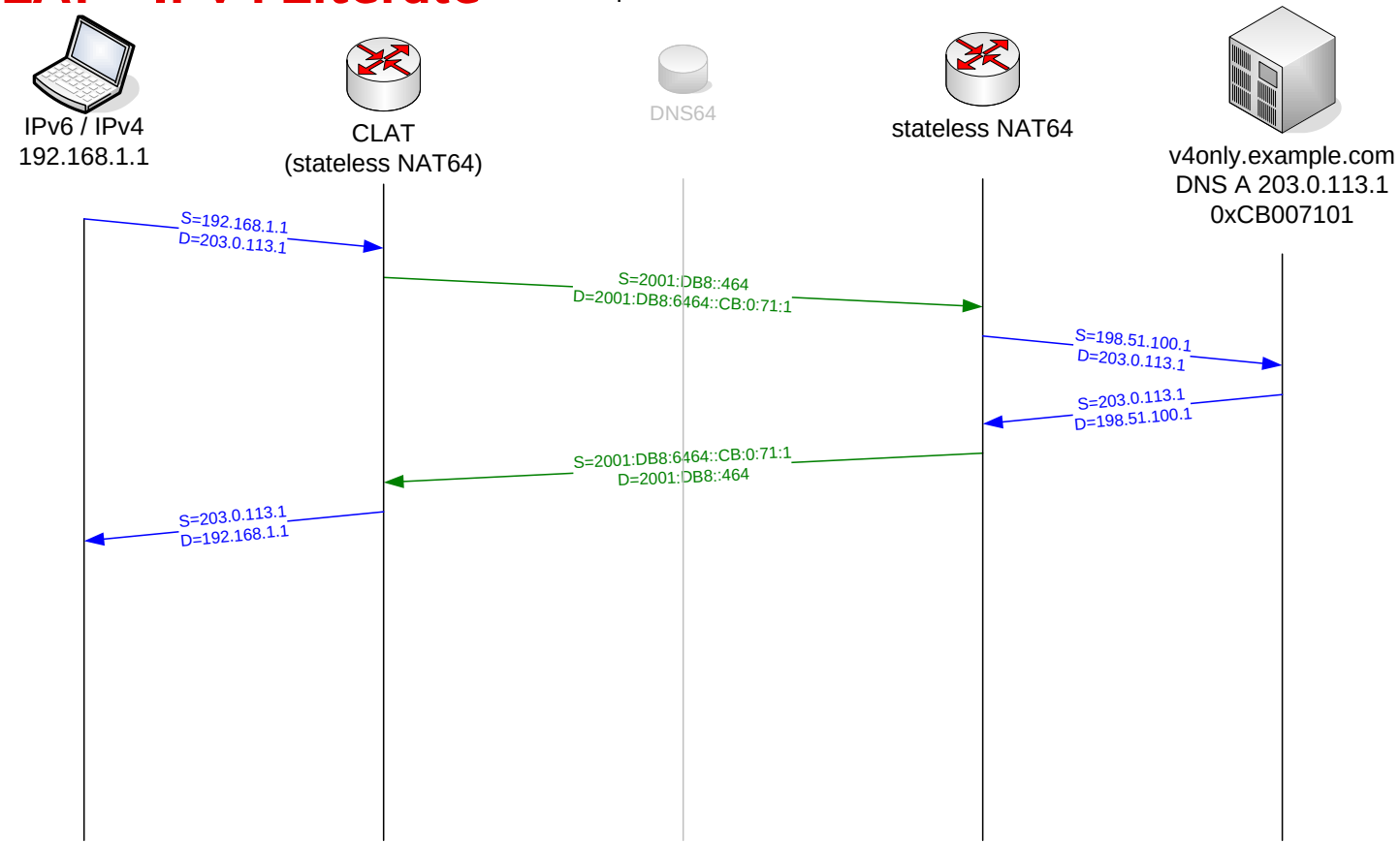



SSID: 464XLAT

Vodafone Innovation Park

# 464XLAT – IPv4 Literale

http://203.0.113.1/





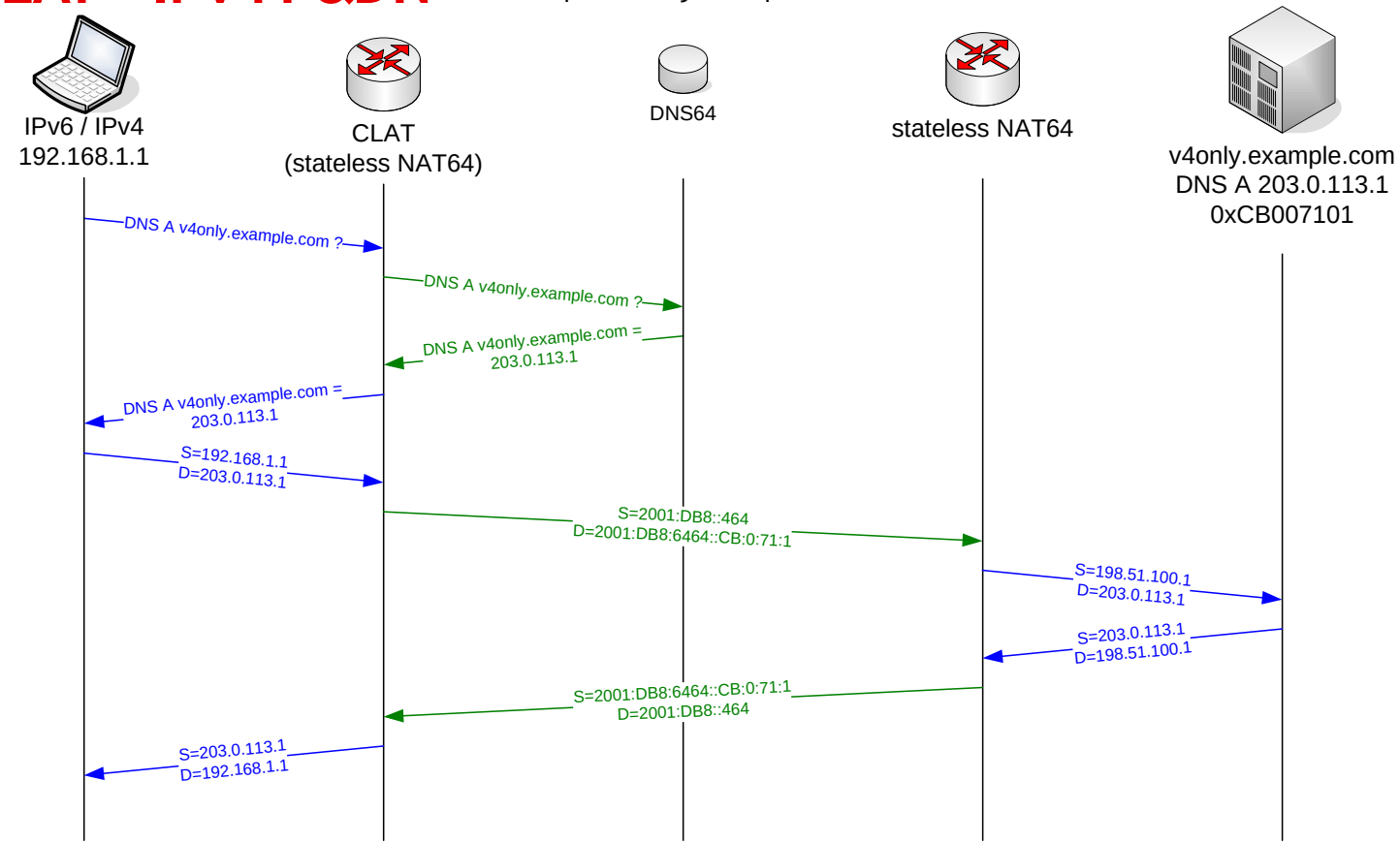



SSID: 464XLAT

Vodafone Innovation Park

# 464XLAT – IPv4 FQDN

http://v4only.example.com/



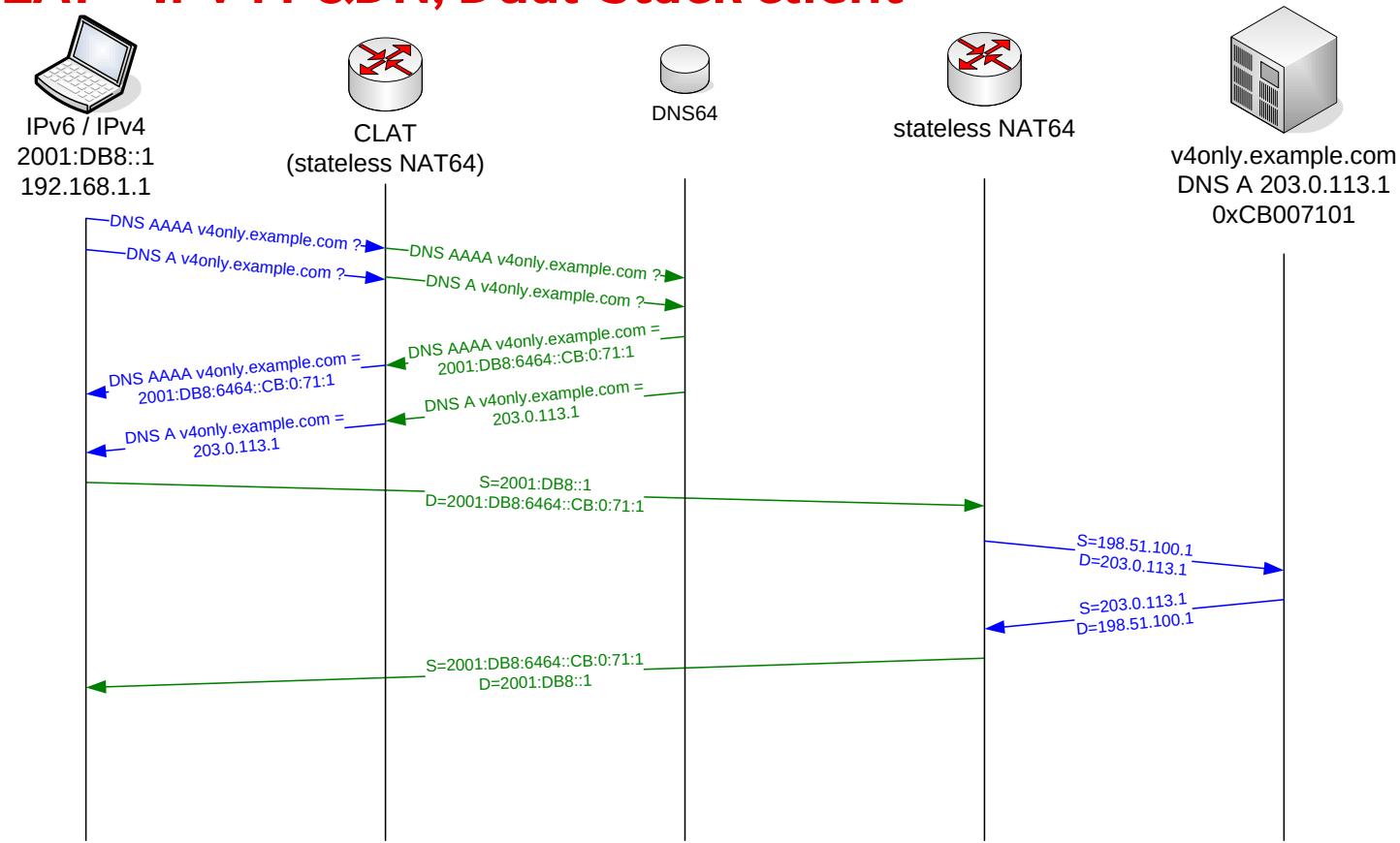





SSID: 464XLAT

Vodafone Innovation Park

# 464XLAT – IPv4 FQDN, Dual-Stack client








SSID: 464XLAT

Vodafone Innovation Park

# Discovery Heuristic

- Woher kennt der CLAT das NAT64 Prefix?

- RFC 7050
  - Client: AAAA? ipv4only.arpa.
  - DNS64 : AAAA! <Prefix>:C000:AA
  - CLAT nutzt so gelerntes Prefix für 464XLAT

- manuelle, statische Konfiguration

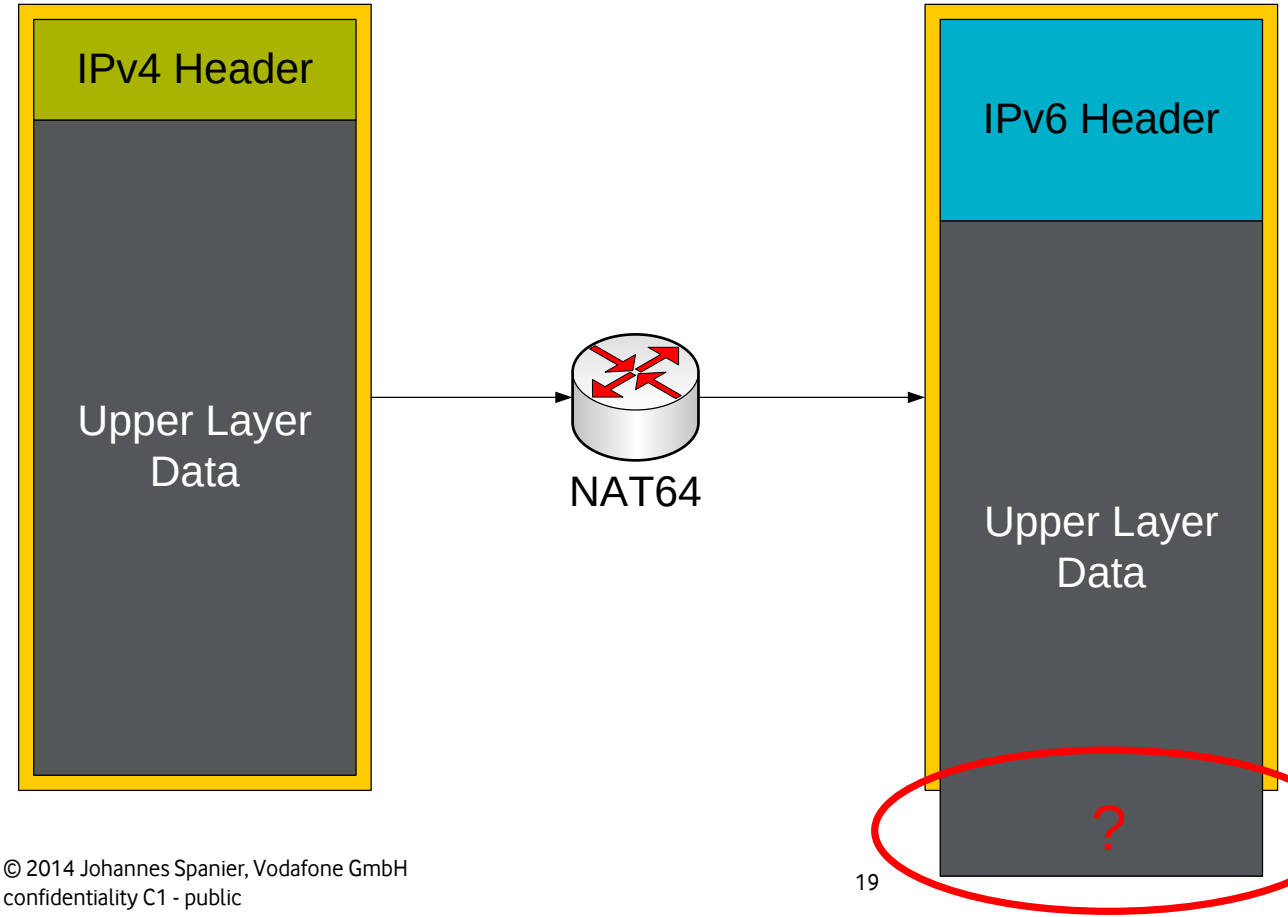




SSID: 464XLAT

# Hindernisse

# MTU Issue




**Lösungen**

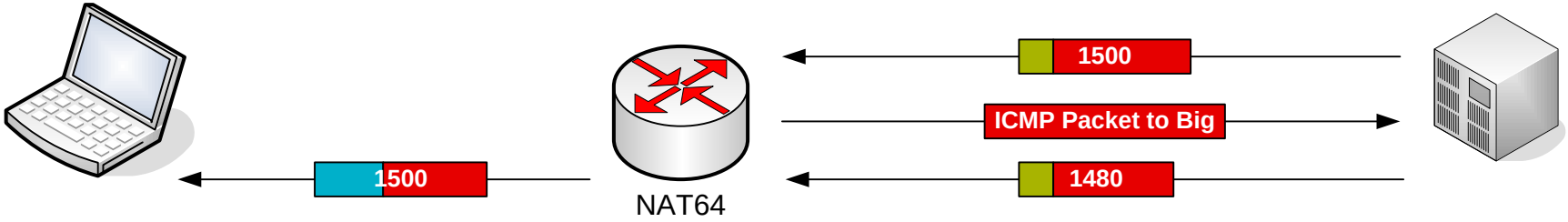
- PMTUD
- Fragmentierung
- MSS Clamping





SSID: 464XLAT

# Path MTU Discovery




- Verwendet wenn IPv4 Don't Fragement (DF) Bit == 1

- PMTUD vs. ICMP filtering → Blocking all ICMP is bad
- einige Sites haben DF=1 aber filtern ICMP
- funktioniert Ende-zu-Ende (auch über NAT64 hinweg)
- Es existieren pathologische Fälle, z.B. Loadbalancer die ICMP nicht stateful behandeln
- Auch bei IPv4 only ein Thema! (MTU bei PPPoE)

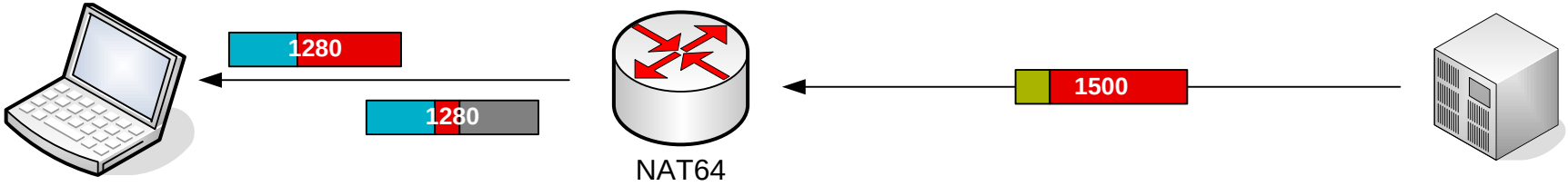




SSID: 464XLAT

Vodafone Innovation Park

# Fragmentierung




- Verwendet wenn IPv4 Don't Fragement (DF) Bit == 0

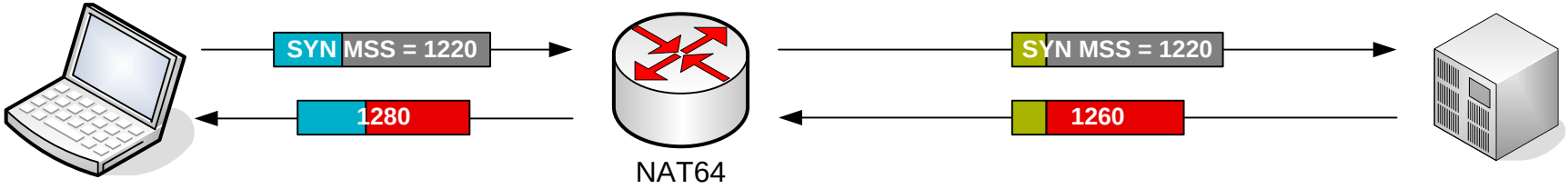
- Bei IPv6: nur Sender darf fragmentieren, DF-Bit existiert nicht, PMTUD verpflichtend
  → NAT64 Gateway fragmentiert
- Fragmentierung auf 1280 Byte MTU (minimum IPv6 MTU)
- ALLE Pakete sollten IPv6 Fragment Header bekommen
  (RFC6145 konform abschaltbar)
- Oft schlechtes (kein) Handling von IPv6 Fragmenten in Firewalls





SSID: 464XLAT

# MSS Clamping




- Vermeidung von ICMP Error Messages und Fragmentierung
- Nur bei TCP möglich
- Workaround für einen Fehler der eigentlich beim Server liegt
- But I can't fix all the Internets





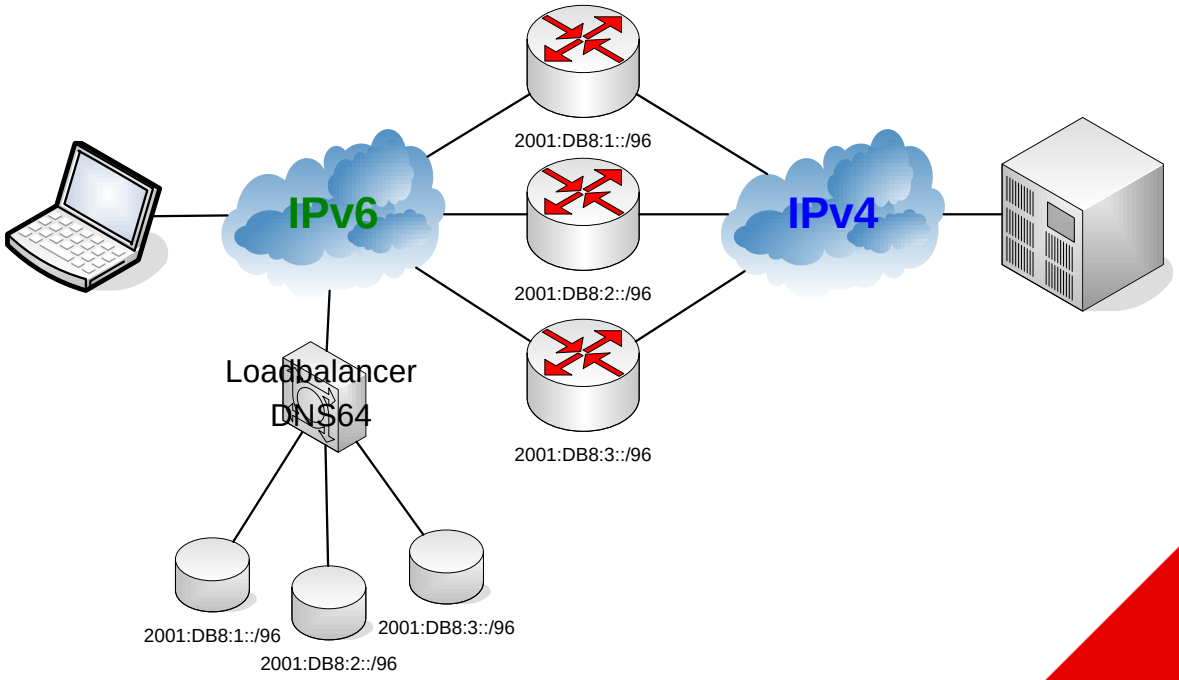
SSID: 464XLAT

Vodafone Innovation Park

# Skalierbarkeit

## Die 16 Mio. Frage

- stateless NAT64 + CGN
- größter Pool 10.0.0.0/8
  → max. 2^24 ≈ 16 Mio. User
- Skalierung nötig
- z.B. via DNS64
  Loadbalancing zu multiplen
  NAT64 GWs








SSID: 464XLAT

Vodafone Innovation Park

# Implementierungen

- NAT64
  - Tayga (Linux, Userspace, req. TUN/TAP)
  - pf (BSD > 5.1)
  - Ecdysis (Netfilter Module)
  - Jool (Netfilter Module + Userspace Tool)
  - Cisco IOS XE (> 3.2S)
  - Cisco ASA (> 9.0)
  - Juniper JunOS (> 10.2 on MX Series)
  - Fortinet FortiGate
  - F5





SSID: 464XLAT

# Implementierungen

- DNS64
  - Bind (> 9.8)
  - Totd
- CLAT
  - beleibiges stateless NAT64 (s.o.)
  - Included in Android (>4.3)



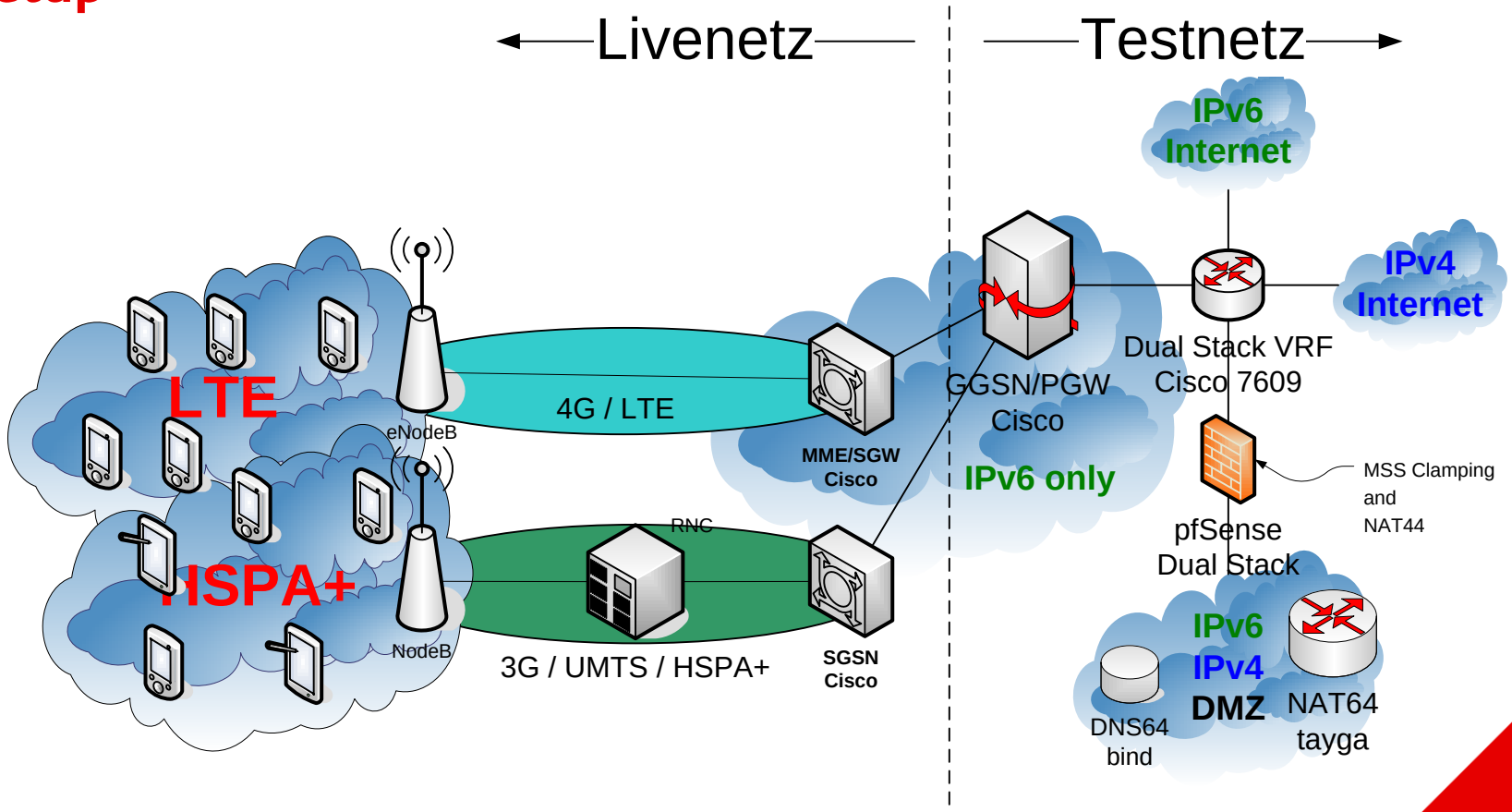


SSID: 464XLAT

Vodafone Innovation Park

# Trial

# Setup








SSID: 464XLAT

Vodafone Innovation Park

# Setup

- Mobilfunk
  - Vodafone Livenetz SGSNs (IPv6 enabled)
  - Vodafone Testnetz GGSNs (IPv6 enabled)
  - Cisco EPC (LTE / 4G Testnetz)
- NAT64 / DNS64
  - tayga
  - bind
  - pfSense (für IPv6 DMZ)
- Endgeräte
  - Samsung Galaxy S3 und S4
  - Sony XPERIA Z
  - LG G2





SSID: 464XLAT

# TOP 10 Android Apps die mit 464XLAT funktionieren*

| | |
|---|---|
| Hangouts | Viber |
| Lync | Watchever |
| Speedtest | Skype |
| Spotify | Shazam |
| Mail (Exchange) | Radio.de |

*) nicht in der Liste sind Apps die lediglich eine HTTP-API aufrufen, diese Funktionieren alle

Auch interessant: https://docs.google.com/spreadsheet/ccc?key=0AnVbRg3DotzFdGVwZWlWeG5wXzVMcG5qczZEZloxWGc





SSID: 464XLAT

Vodafone Innovation Park

# Android Apps aus der TOP 200 Liste, die trotz 464XLAT NICHT funktionieren*

- 
- 
- 

*) na gut sehr intensiv haben wohl noch nicht gesucht, Meldungen erwünscht





SSID: 464XLAT

Vodafone Innovation Park

# Android Apps aus der TOP 200 Liste, die trotz 464XLAT NICHT funktionieren*

**Gute Kandidaten:**

Apps die große UDP Pakete EMPFANGEN (MTU Problem IPv4→IPv6)





SSID: 464XLAT

Vodafone Innovation Park

# NAT64 / 464XLAT Trial

- **öffentlicher** IPv6 / NAT64 / 464XLAT Trial über Mobilfunknetz musste leider abgesagt werden
- **intern** wird weiter über Mobilfunk getestet

... aber...





SSID: 464XLAT

Vodafone Innovation Park

# NAT64 / 464XLAT Trial

- Interesse unser DNS64 / NAT64 Gateway für eigene Tests zu nutzen?
  - kurze Mail an johannes.spanier@vodafone.com
  - eigenes IPv6 Prefix nicht vergessen

- garantierte Untersuchung von „pathologischen“ Verbindungen
- Tracefiles vom NAT64 GW - IPv6 und IPv4 Seite
- Boni nur für „registrierte“ Nutzer
  - exklusiver Zugang zum internen IPv6/NAT64/464XLAT Bug Tracker der Innovation Park Labs
  - Wer bei unserem NAT64/DNS64 Setup eine Sicherheitslücke entdeckt und meldet, der bekommt eine Testnetz IPv6 SIM (HSPA+) für 1 Jahr inklusive unbegrenztem IPv6 Traffic gratis





SSID: 464XLAT

Vodafone Innovation Park