SICHERHEIT BEI IPv6

MEHR, WENIGER ODER NUR ANDERS?

Uwe Kaiser, 24. November 2014

Fraunhofer FOKUS

GOVERNMENTS ENABLED WITH IPv6 GEN6

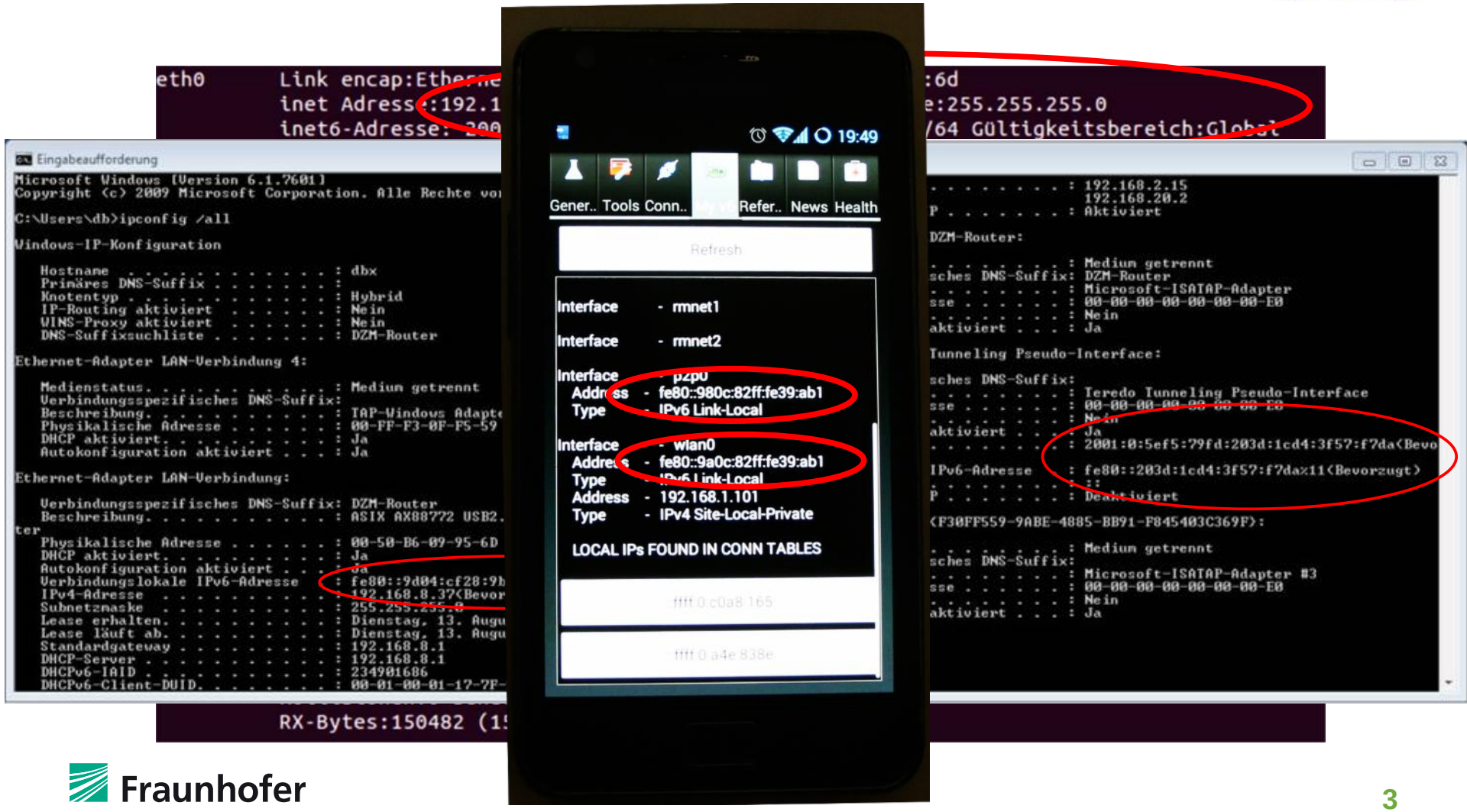
European Commission
This project has received funding from the European Union´s

Wir machen Städte schlau

IPV6 – ZEITLEISTE

1990	**Adressproblem erkannt**
1992	Classless Inter-Domain Routing (CIDR)
1993	Beginn der IPv6 Standardisierung
1993	Dynamic Host Configuration Protocol (DHCP)
1994	Network Address Translation (NAT)

LINUX ANDROID WINDOWS



NICHTS – ETWAS - UMFASSEND

Das Bild kann nicht angezeigt werden. Dieser Computer verfügt möglicherweise über zu wenig Arbeitsspeicher, um das Bild zu öffnen, oder das Bild ist beschädigt. Starten Sie den Computer neu, und öffnen Sie dann erneut die Datei. Wenn weiterhin das rote x angezeigt wird, müssen Sie das Bild möglicherweise löschen und dann erneut einfügen.

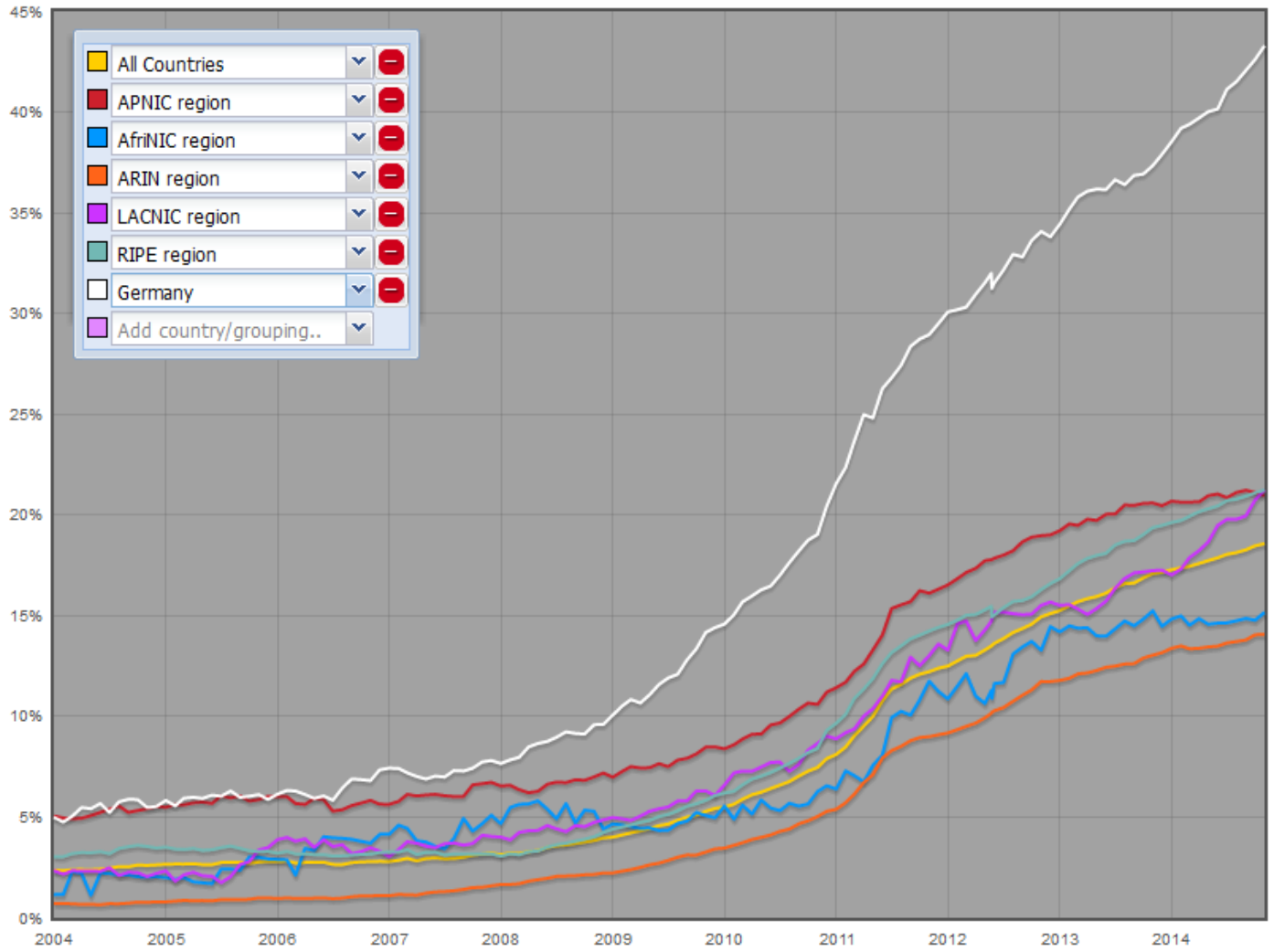
IPv6 Kongress

IPv6 Security Summit

IPv6 Hackers

Fraunhofer FOKUS

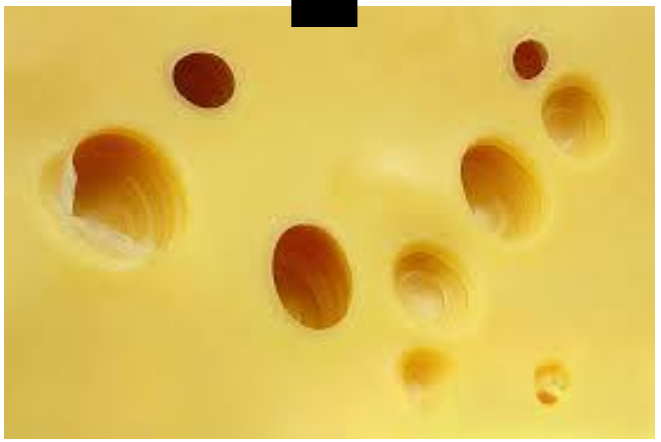
ANNO 2004 - 2014



DIE FRAGE

IPv6

?

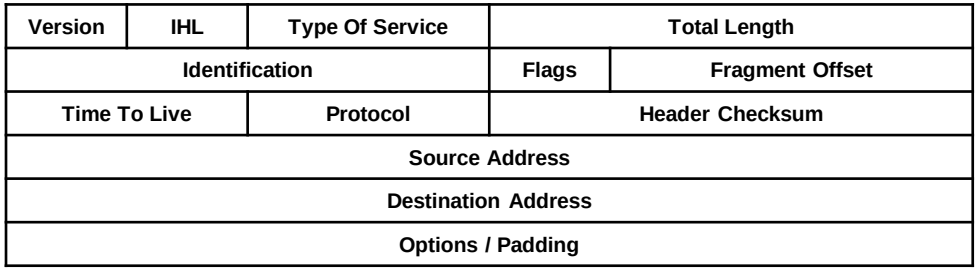


Fraunhofer FOKUS

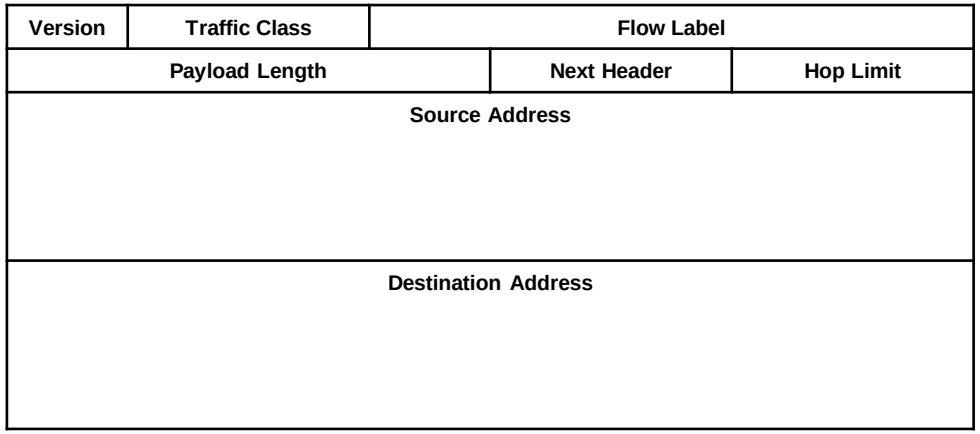
WARUM IST ES MIT DER EINFÜHRUNG NICHT GETAN?

IP HEADER

IPv4 Header



IPv6 Base Header



- Keine Prüfsumme
  ~~Header Checksum~~
- Feste Header Größe
  ~~Internet Header Length~~
- Keine Fragmentierung
  ~~Identification~~
  ~~Flags~~
  ~~Fragment Offset~~
- Erweiterungen in separaten Headern
  ~~Options~~

Fraunhofer FOKUS

EXTENSION HEADER

Extra Header für alles was nicht immer gebraucht wird:

- Authentication
- Encapsulation
- Fragmentation
- Source Routing
- Destination Options
- Hop-by-hop Options
- Mobility

IST IPv6 AUSGEREIFT?

Fraunhofer FOKUS

IN DER FEINABSTIMMUNG

- 332 RFCs mit „IPv6“ im Titel
- (Vermutlich mehr mit IPv6-bezug)

- Viele Erweiterungen

- Änderungen älterer RFCs

- → Hersteller kommen nur bedingt nach
- → Ältere Produkte unterstützen neuen Standards nicht

EINIGE PRODUKTE NOCH NICHT AUSGEREIFT

- Kaum eine Vergleichbarkeit von Eigenschaften
- Schlechtere Performance im Vergleich zu IPv4

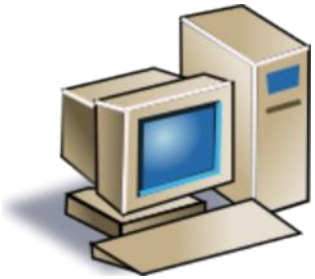
  (wenn als Software-Stack realisiert)
- Fehlende Konfigurationshilfen
- Kein Management über IPv6
- Unzureichende Unterstützung von Extension Headern
- Fragmente werden unterschiedlich zusammengesetzt
- . . .

ANGRIFFE UND (UN-)SICHERHEITEN

IPsec

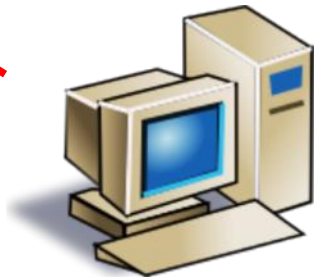
- Spezifiziert für IPv6
- Für IPv4 „rückportiert“
- Seit 2011 nicht mehr verpflichtend

ND DAD DENIAL OF SERVICE



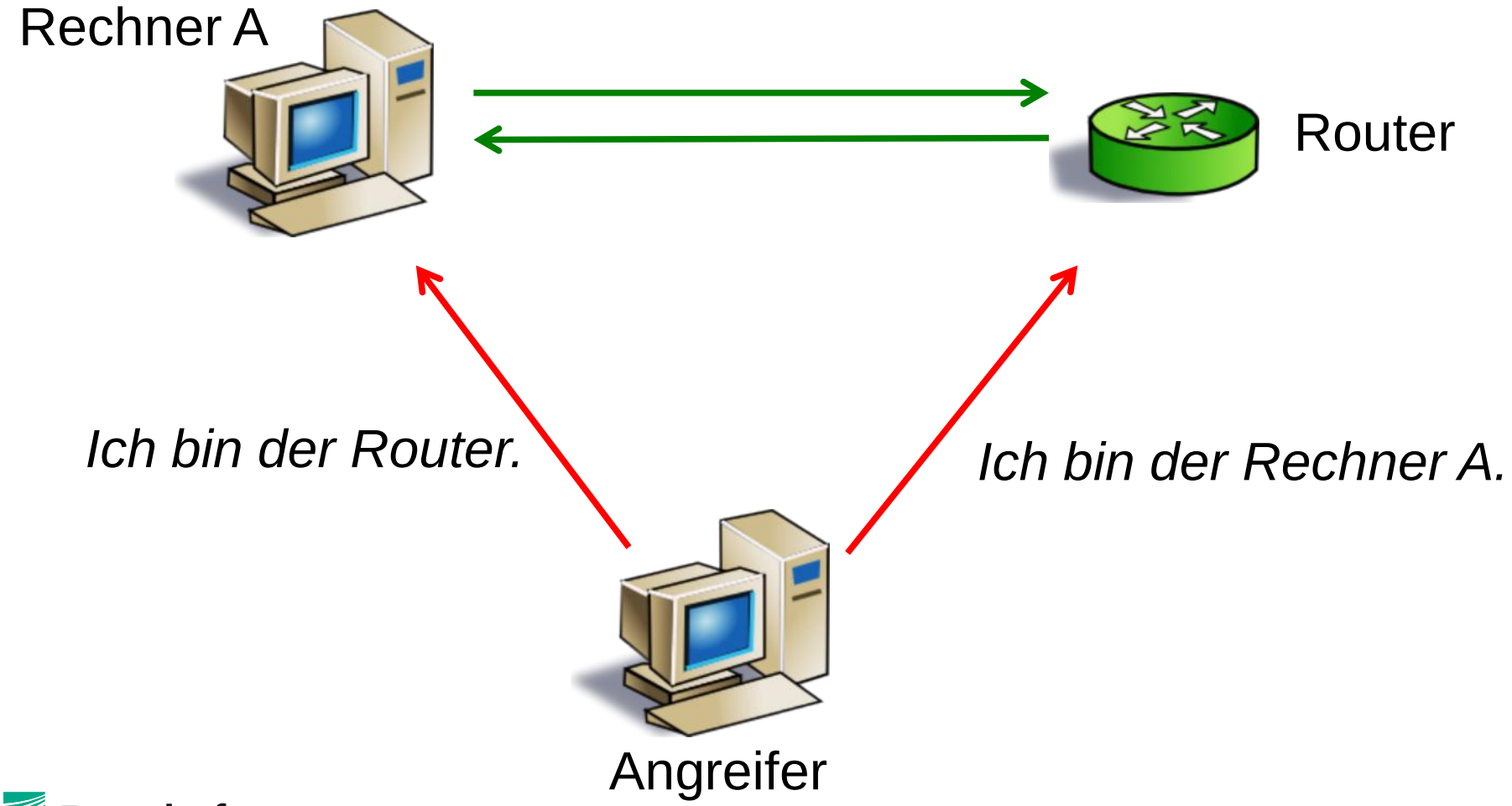
*Ist die IP **x** frei?*
*Ist die IP **y** frei?*
*Ist die IP **z** frei?*

*Adresse **x** besitze ich bereits.*
*Adresse **y** besitze ich bereits.*
*Adresse **z** besitze ich bereits.*

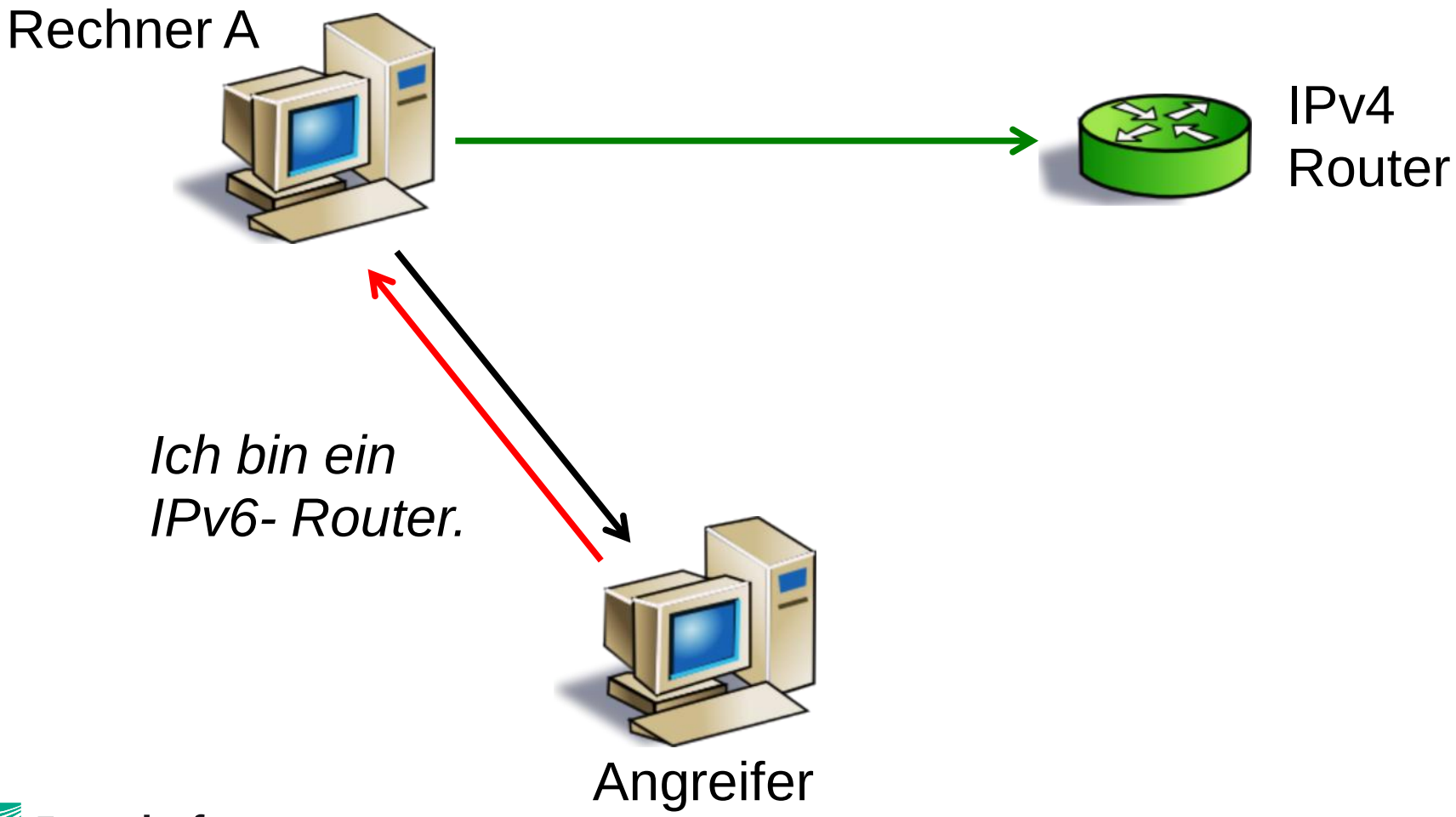


Angreifer

MAN IN THE MIDDLE



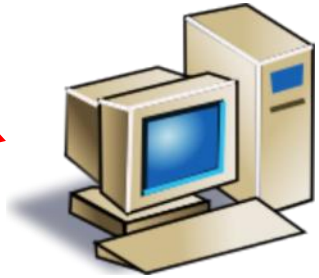
ROGUE ROUTER



RA FLOODING

Angreifer

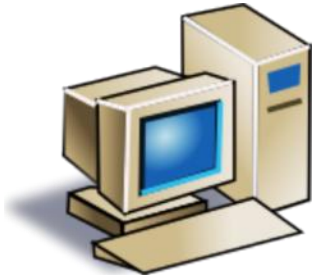
2001:db8:1::/64
2001:db8:2::/64
2001:db8:3::/64
2001:db8:4::/64
. . .



2001:db8:1::bad:f00d
2001:db8:2::bad:f00d
2001:db8:3::bad:f00d
2001:db8:4::bad:f00d
. . .

Fraunhofer FOKUS

ND CACHE EXHAUSTION



Angreifer

2001:db8:1::bad:f00d:1
2001:db8:1::bad:f00d:2
2001:db8:1::bad:f00d:3
2001:db8:1::bad:f00d:4
. . .

GEGENMAßNAHMEN

- SeND
- Implementierungen unvollständig, nicht verfügbar

- RA Guard
- Nur gegen versehendliche RAs
- Nicht gegen gezielte Angreifer

- NDPmon zum Beobachten

- Zugang zum Netz einschränken

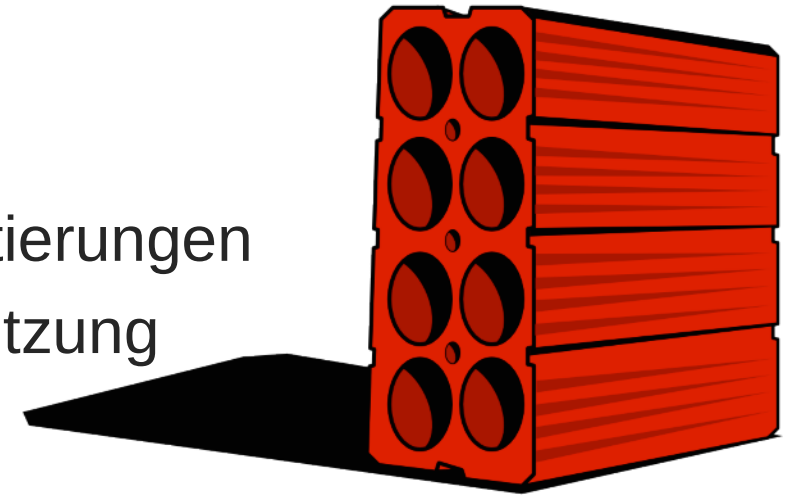
STOLPERSTEINE

Organisatorisch

- Wenig Erfahrung bei der Umsetzung -> Testumgebung
- Unwissenheit / fehlendes Verständnis
- Komplexität bei Dual-Stack

Technisch

- Noch nachreifende Implementierungen
- Teilweise mangelnde Unterstützung
- Automatische Tunnel
- Neue Angriffsmethoden



ZUSAMMENFASSUNG

NICHT ABWARTEN

- **Jetzt** Informieren
  - Lesen
  - Beobachten
  - Testen
- **Jetzt** Vorsorgen
  - Tunnel abschalten
  - Geräte wie Firewall einrichten
  - Bei Beschaffungen beachten

- **Jetzt** auf Clients (de)aktivieren, sofern es geht

VORBEREITET SEIN

1. Testumgebung
   - Regeln für die Firewall
   - IPv6-Proxy
   - Adressvergabe
2. Adressen besorgen
3. Web-Angebote v6-fähig machen
   - Proxy
   - Dual-Stack

Quelle: ipv6ready.org

DIE GUTEN SEITEN

- Es fallen einige Angriffe weg (IPv6-only)
- Bessere Netzwerkarchitektur möglich
- Externe Dienste (Web, Mail) sollten IPv6 fähig sein

INFORMATIONEN

EMPFEHLUNGEN ZUR CYBERSICHERHEIT

- Effekte von IPv6 auf IPv4 Netze
- VPN
- IPv6 Tunnel
- IPv6 Angriffe

- Zur Konzeption von IPv6 Netzen
- Netzarchitektur
- Adresswahl
- ICMPv6 Filterung

- IPv6 für ISPs

LINKS FÜR ALLE FÄLLE

- Sichere Anbindung lokaler Netze an das Internet v2.0 (ISi-LANA)https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_lana_studie_pdf.pdf
- Leitfaden für eine sichere IPv6-Netzwerkarchitektur
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_lana_leitfaden_IPv6_pdf.pdf
- Zur Konzeption von IPv6-Netzen (BSI-CS 057)
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-057.html
- Effekte von IPv6 auf reine IPv4-Netze (BSI-CS 058)
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-058.html
- IPv6 für Internet-Service-Provider (BSI-CS 073)
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-073.html

Fraunhofer FOKUS

Kaiserin-Augusta-Allee 31

10589 Berlin, Germany

www.fokus.fraunhofer.de

Uwe Kaiser

uwe.holzmann-kaiser@fokus.fraunhofer.de
Tel. +49 (0)30 3463-7217

Fraunhofer FOKUS