



# SICHERHEIT BEI IPv6

## MEHR, WENIGER ODER NUR ANDERS?

Uwe Kaiser, 24. November 2014



This project has received funding from the European Union's



# 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



```
eth0 Link encap:Ethernet  
inet Address::192.1  
inet6-Adresse: 200
```

```
:6d  
e:255.255.255.0  
/64 Gültigkeitsbereich:Global
```

```
Eingabeaufforderung  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.  
C:\Users\ndb>ipconfig /all  
  
Windows-IP-Konfiguration  
  
Hostname . . . . . : dbx  
Primäres DNS-Suffix . . . . . :  
Knotentyp . . . . . : Hybrid  
IP-Routing aktiviert . . . . . : Nein  
WINS-Proxy aktiviert . . . . . : Nein  
DNS-Suffixsuchliste . . . . . : DZM-Router  
  
Ethernet-Adapter LAN-Verbindung 4:  
  
Medienstatus. . . . . : Medium getrennt  
Verbindungsspezifisches DNS-Suffix:  
Beschreibung. . . . . : IAP-Windows Adapter  
Physikalische Adresse . . . . . : 00-FE-F3-0F-F5-59  
DHCP aktiviert. . . . . : Ja  
Autokonfiguration aktiviert . . . . . : Ja  
  
Ethernet-Adapter LAN-Verbindung:  
  
Verbindungsspezifisches DNS-Suffix: DZM-Router  
Beschreibung. . . . . : ASIX AX88772 USB2.0  
Physikalische Adresse . . . . . : 00-50-B6-09-95-6D  
DHCP aktiviert. . . . . : Ja  
Autokonfiguration aktiviert . . . . . : Ja  
Verbindungslokale IPv6-Adresse . . . . . : fe80::9d84:cf28:9b  
IPv4-Adresse . . . . . : 192.168.8.37<Bevorz  
Subnetzmaske . . . . . : 255.255.255.0  
Lease erhalten. . . . . : Dienstag, 13. Augu  
Lease läuft ab. . . . . : Dienstag, 13. Augu  
Standardgateway . . . . . : 192.168.8.1  
DHCP-Server . . . . . : 192.168.8.1  
DHCPv6-IAID . . . . . : 234901686  
DHCPv6-Client-DUID. . . . . : 00-01-00-01-17-7F-
```

Refresh

|           |                            |
|-----------|----------------------------|
| Interface | - wlan1                    |
| Address   | - fe80::980c:82ff:fe39:ab1 |
| Type      | - IPv6 Link-Local          |

|           |                            |
|-----------|----------------------------|
| Interface | - wlan0                    |
| Address   | - fe80::9a0c:82ff:fe39:ab1 |
| Type      | - IPv6 Link-Local          |

|           |                           |
|-----------|---------------------------|
| Interface | - wlan0                   |
| Address   | - 192.168.1.101           |
| Type      | - IPv4 Site-Local-Private |

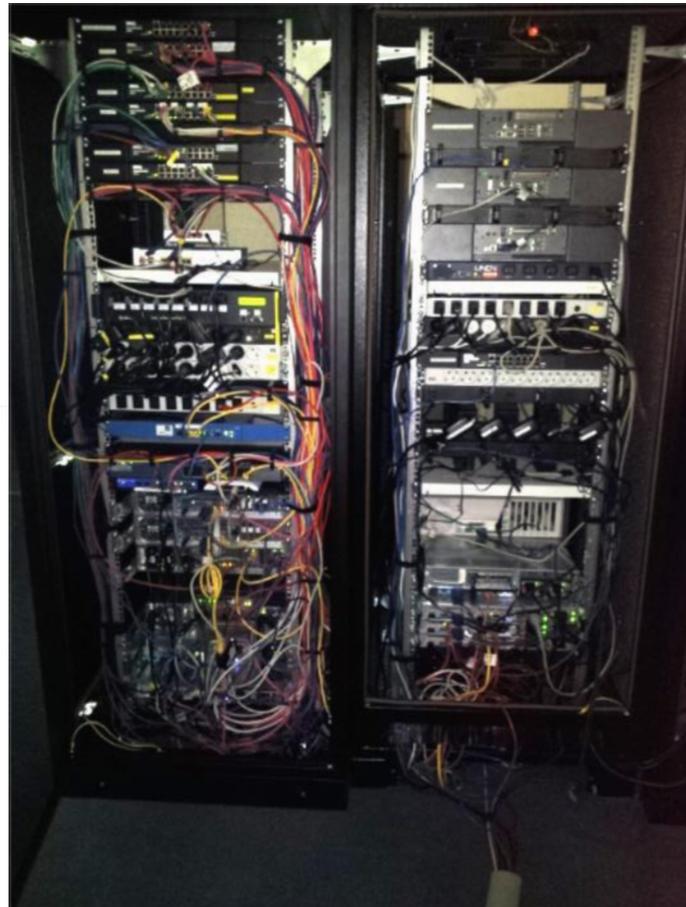
LOCAL IPs FOUND IN CONN TABLES

|              |
|--------------|
| ffff0c0a8165 |
| ffff0a4e838e |

```
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.  
C:\Users\ndb>ipconfig /all  
  
Windows-IP-Konfiguration  
  
Hostname . . . . . : dbx  
Primäres DNS-Suffix . . . . . :  
Knotentyp . . . . . : Hybrid  
IP-Routing aktiviert . . . . . : Nein  
WINS-Proxy aktiviert . . . . . : Nein  
DNS-Suffixsuchliste . . . . . : DZM-Router  
  
Ethernet-Adapter LAN-Verbindung 4:  
  
Medienstatus. . . . . : Medium getrennt  
Verbindungsspezifisches DNS-Suffix:  
Beschreibung. . . . . : IAP-Windows Adapter  
Physikalische Adresse . . . . . : 00-FE-F3-0F-F5-59  
DHCP aktiviert. . . . . : Ja  
Autokonfiguration aktiviert . . . . . : Ja  
  
Ethernet-Adapter LAN-Verbindung:  
  
Verbindungsspezifisches DNS-Suffix: DZM-Router  
Beschreibung. . . . . : ASIX AX88772 USB2.0  
Physikalische Adresse . . . . . : 00-50-B6-09-95-6D  
DHCP aktiviert. . . . . : Ja  
Autokonfiguration aktiviert . . . . . : Ja  
Verbindungslokale IPv6-Adresse . . . . . : fe80::9d84:cf28:9b  
IPv4-Adresse . . . . . : 192.168.8.37<Bevorz  
Subnetzmaske . . . . . : 255.255.255.0  
Lease erhalten. . . . . : Dienstag, 13. Augu  
Lease läuft ab. . . . . : Dienstag, 13. Augu  
Standardgateway . . . . . : 192.168.8.1  
DHCP-Server . . . . . : 192.168.8.1  
DHCPv6-IAID . . . . . : 234901686  
DHCPv6-Client-DUID. . . . . : 00-01-00-01-17-7F-
```

RX-Bytes:150482 (150482)

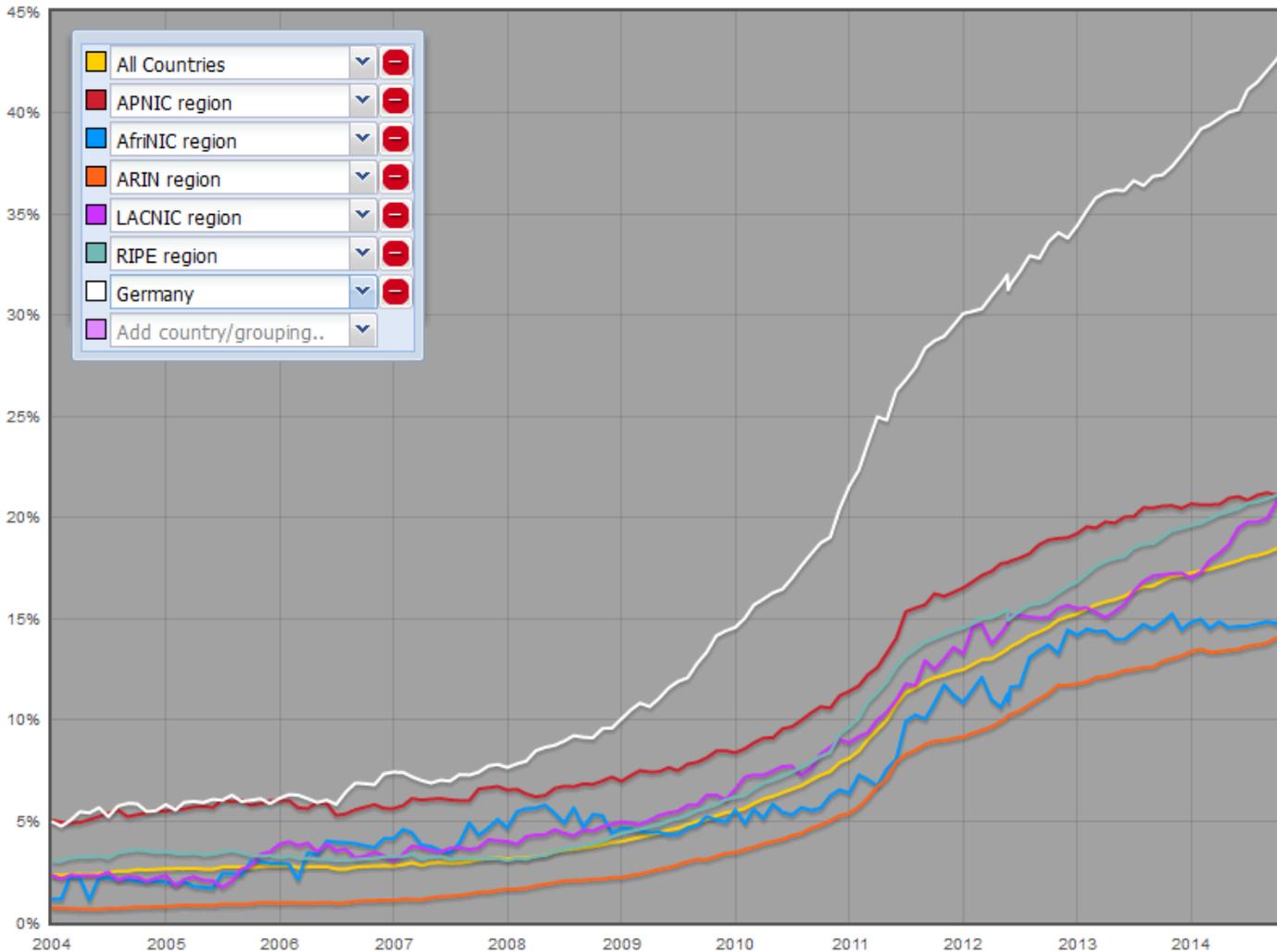
# NICHTS – ETWAS - UMFASSEND



**IPv6 Security Summit**

**IPv6 Hackers**

# ANNO 2004 - 2014



# DIE FRAGE



# WARUM IST ES MIT DER EINFÜHRUNG NICHT GETAN?



# IP HEADER



## IPv4 Header

|                     |          |                 |              |                 |
|---------------------|----------|-----------------|--------------|-----------------|
| Version             | IHL      | Type Of Service | Total Length |                 |
| Identification      |          |                 | Flags        | Fragment Offset |
| Time To Live        | Protocol | Header Checksum |              |                 |
| Source Address      |          |                 |              |                 |
| Destination Address |          |                 |              |                 |
| Options / Padding   |          |                 |              |                 |

## IPv6 Base Header

|                     |               |             |           |  |
|---------------------|---------------|-------------|-----------|--|
| Version             | Traffic Class | Flow Label  |           |  |
| Payload Length      |               | Next Header | Hop Limit |  |
| Source Address      |               |             |           |  |
| Destination Address |               |             |           |  |

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

# 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?



## 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
- ◆ . . .

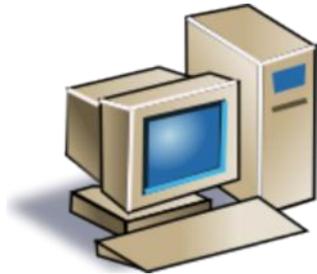
# ANGRIFFE UND (UN-)SICHERHEITEN



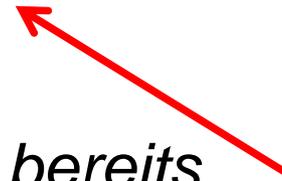
- ◆ Spezifiziert für IPv6
- ◆ Für IPv4 „rückportiert“
- ◆ Seit 2011 nicht mehr verpflichtend



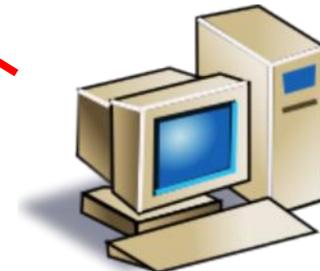
# ND DAD DENIAL OF SERVICE



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



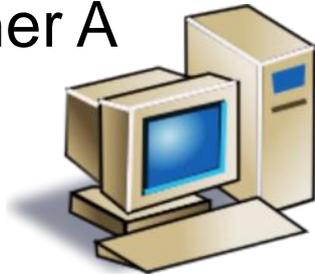
*Adresse **x** besitze ich bereits.  
Adresse **y** besitze ich bereits.  
Adresse **z** besitze ich bereits.*



Angreifer

# MAN IN THE MIDDLE

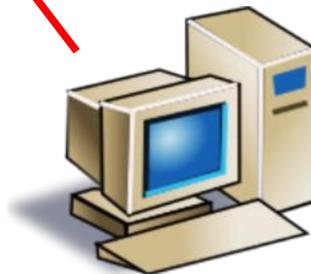
Rechner A



Router

*Ich bin der Router.*

*Ich bin der Rechner A.*

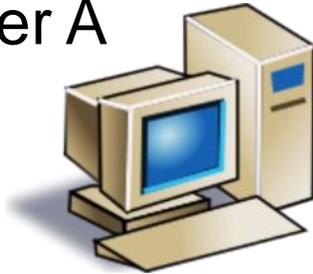


Angreifer

# ROGUE ROUTER

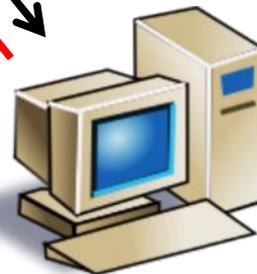
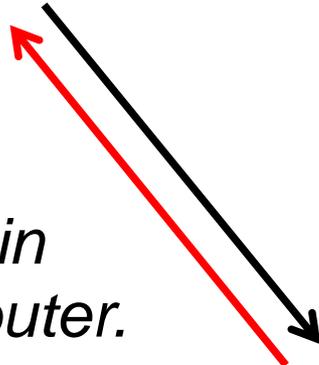


Rechner A



IPv4  
Router

*Ich bin ein  
IPv6- Router.*



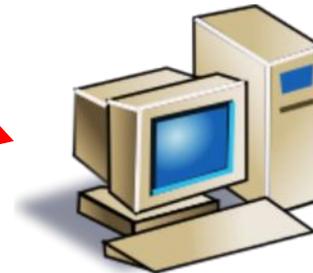
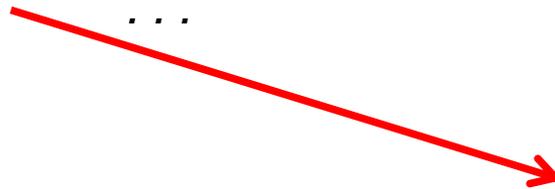
Angreifer

# RA FLOODING



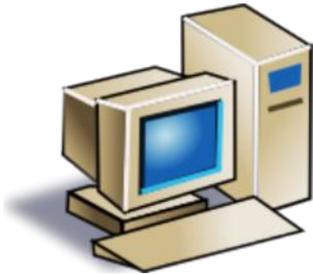
Angreifer

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



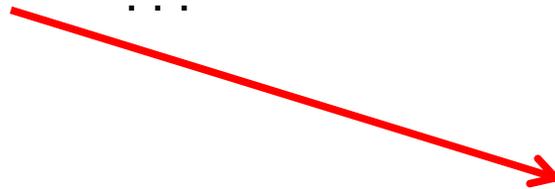
2001:db8:1::bad:f00d  
2001:db8:2::bad:f00d  
2001:db8:3::bad:f00d  
2001:db8:4::bad:f00d  
...

# 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 versehentliche RAs
- ◆ Nicht gegen gezielte Angreifer
- ◆ NDPmon zum Beobachten
- ◆ Zugang zum Netz einschränken

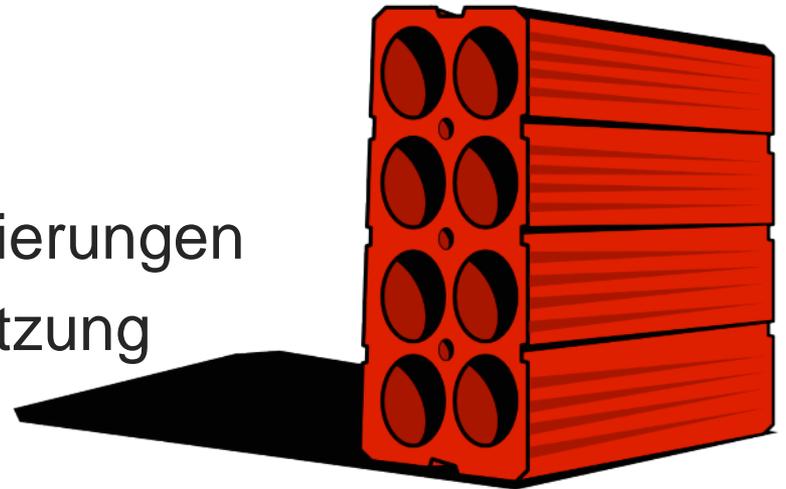


## Organisatorisch

- ◆ 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



## ◆ **Jetzt** Informieren

- ◆ Lesen
- ◆ Beobachten
- ◆ Testen

## ◆ **Jetzt** Vorsorgen

- ◆ Tunnel abschalten
- ◆ Geräte wie Firewall einrichten
- ◆ Bei Beschaffungen beachten

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



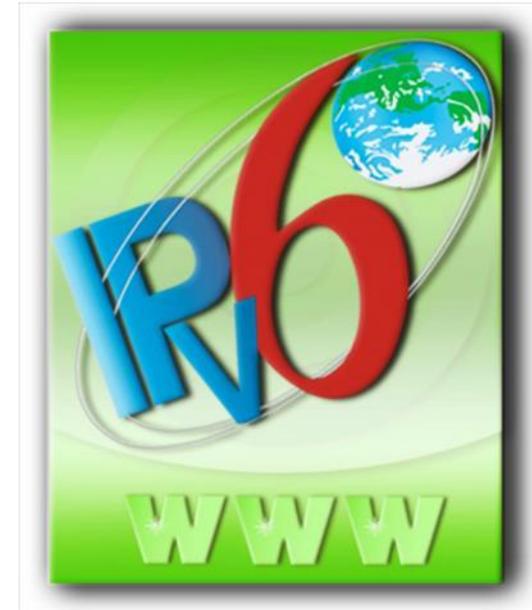
## 1. Testumgebung

- ◆ Regeln für die Firewall
- ◆ IPv6-Proxy
- ◆ Adressvergabe

## 2. Adressen besorgen

## 3. Web-Angebote v6-fähig machen

- ◆ Proxy
- ◆ Dual-Stack



Quelle: [ipv6ready.org](http://ipv6ready.org)

## DIE GUTEN SEITEN



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



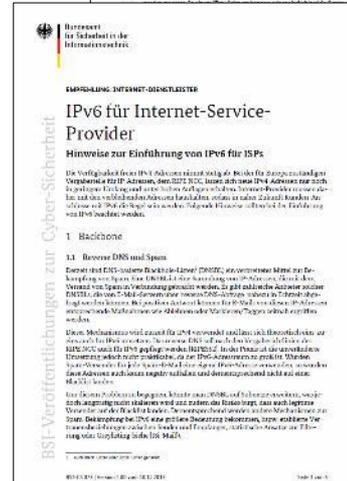
# INFORMATIONEN



# 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](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](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](http://www.fokus.fraunhofer.de)

Uwe Kaiser

[uwe.holzmann-kaiser@fokus.fraunhofer.de](mailto:uwe.holzmann-kaiser@fokus.fraunhofer.de)

Tel. +49 (0)30 3463-7217