Der
ipv6calc
Werkzeugkasten

Dr. Peter Bieringer
Deep Space 6
peter@deepspace6.net
http://www.deepspace6.net/

IPv6-Kongress
Frankfurt/Main, Deutschland
22. - 23. Mai 2014
http://www.ipv6-kongress.de/

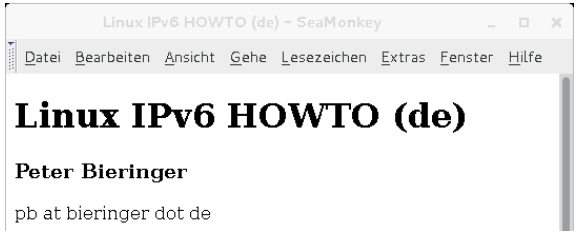
Über mich

- **Wohnhaft in München (Deutschland)**
- **Beschäftigt als *Senior IT Architect* bei *Giesecke & Devrient 3S GmbH***

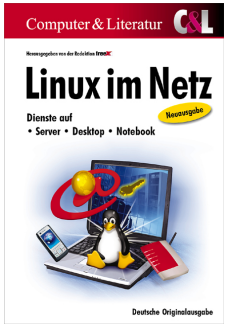
Giesecke & Devrient
Creating Confidence.

- **Mitbegründer und Kernmitglied von *Deep Space 6***

- **Autor des "Linux IPv6 HowTo"**



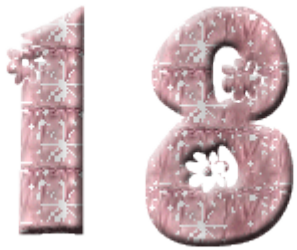
- **Mitautor des Buches "Linux im Netz" (2006)**
  - Grundlagen von TCP/IP incl. IPv6, DNS, DHCP



Meine Internet- & IPv6-Historie

- **1993: Erster Kontakt mit dem Internet (Univ., SunOS)**
- **1996: Erste Erfahrungen mit IPv6 und Linux**
- **1997: *IPv6 & Linux - HowTo*, *initscripts-ipv6***
- **1999: *IPv6 & Linux - Current Status***
- **2001: *Linux IPv6 HOWTO*, *ipv6calc***
- **2002: Mitbegründer von *Deep Space 6***

inzwischen 18 Jahre IPv6-Erfahrung!



Inhalt

Der ipv6calc Werkzeugkasten

- **Übersicht**
- **Interner Aufbau**
  - Features
- **Werkzeuge**
  - ipv6calc
  - ipv6loganon
  - ipv6logconv
  - ipv6logstats
- **Wrapper**
  - ipv6calcweb.cgi
- **Ausblick**

Übersicht

Übersicht (1)

- **Der ipv6calc Werkzeugkasten ist**
  - programmiert in C
    - Ausnahme: ipv6calcweb.cgi (Perl)
  - kompilierbar unter Linux & Unix
  - verfügbar in diversen Distributionen, z.B.
    - RPM:
      - Fedora 20 — 0.94.1-3.fc20
      - Red Hat Enterprise Linux 5 — 0.61-1
      - Red Hat Enterprise Linux 6+7 — n/a (Maintainer für EPEL fehlt momentan)
      - openSuSE — n/a
    - DPKG:
      - Ubuntu 14.04 — 0.95.0
    - Gentoo/Funtoo:
      - Funtoo — 0.96.0
  - nutzbar auf Kommandozeile
    - Ausnahme: ipv6calcweb.cgi (CGI für Webserver)

Lizenz:
GNU GPL version 2

Übersicht (2)

- **Der ipv6calc Werkzeugkasten bietet**
  - Informationen über IPv4/IPv6, MAC-Adressen
    - "ipv6calc -i ..."
  - Möglichkeiten zur Format-Umwandlung
    - z.B. für PTR-Einträge in DNS-Zonen
  - Aktionen
    - Anonymisieren
    - Filtern (Pipe-Modus)
    - ....
  - statistische Auswertungen
    - ipv6logstats, ipv6logconv
- **Homepage: http://www.deepspace6.net/projects/ipv6calc.html**
- **Quell-Code: tar.gz (Releases), CVS (aktuelle Entwicklung)**

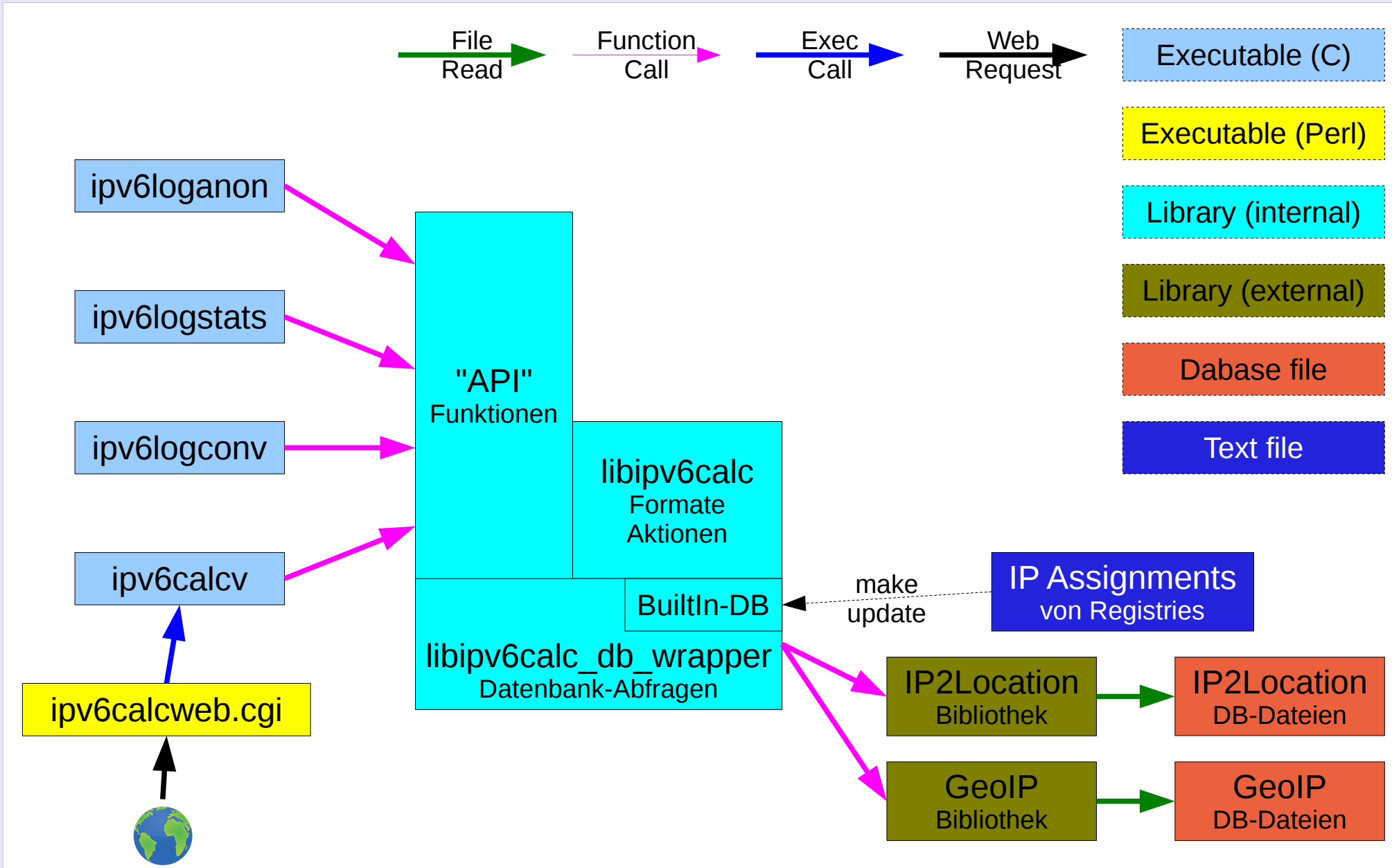
Historie

- **2001: ipv6calc**
- **2002: ipv6logconv, ipv6calcweb.cgi**
- **2003: ipv6logstats**
- **2007: ipv6loganon**
- **2013 / 0.94: Unterstützung für OUI-36**
- **2013 / 0.95:**
  - Restrukturierung GeoIP/IP2Location incl. Dynamic Load
  - vollständige IPv4/IPv6-Adress-Anonymisierung
- **2014 / 0.96: Shared Library Build-Option**
- **2014 / 0.97: Bugfix-Release** 

Aktuell:
0.97.2
(2014-05-23)

Aufbau / Funktionsweise

Interner Aufbau



Interne Datenbanken

- **Datenbank-Typ: "Built-In"**
  - Abfragen
    - IPv4, IPv6 -> Registry
      - ARIN, RIPE NCC, LACNIC, APNIC, AFRINIC
    - MAC, EUI-64 -> Hersteller
      - IAB, OUI, OUI-36 (IEEE)
  - Aktualisierung
    - Vor jedem Release ("make update") durch Download und Aggregierung
      - IANA Adress Space
      - IP-Assignments der Registries
      - IAB, OUI, OUI-36 (IEEE)

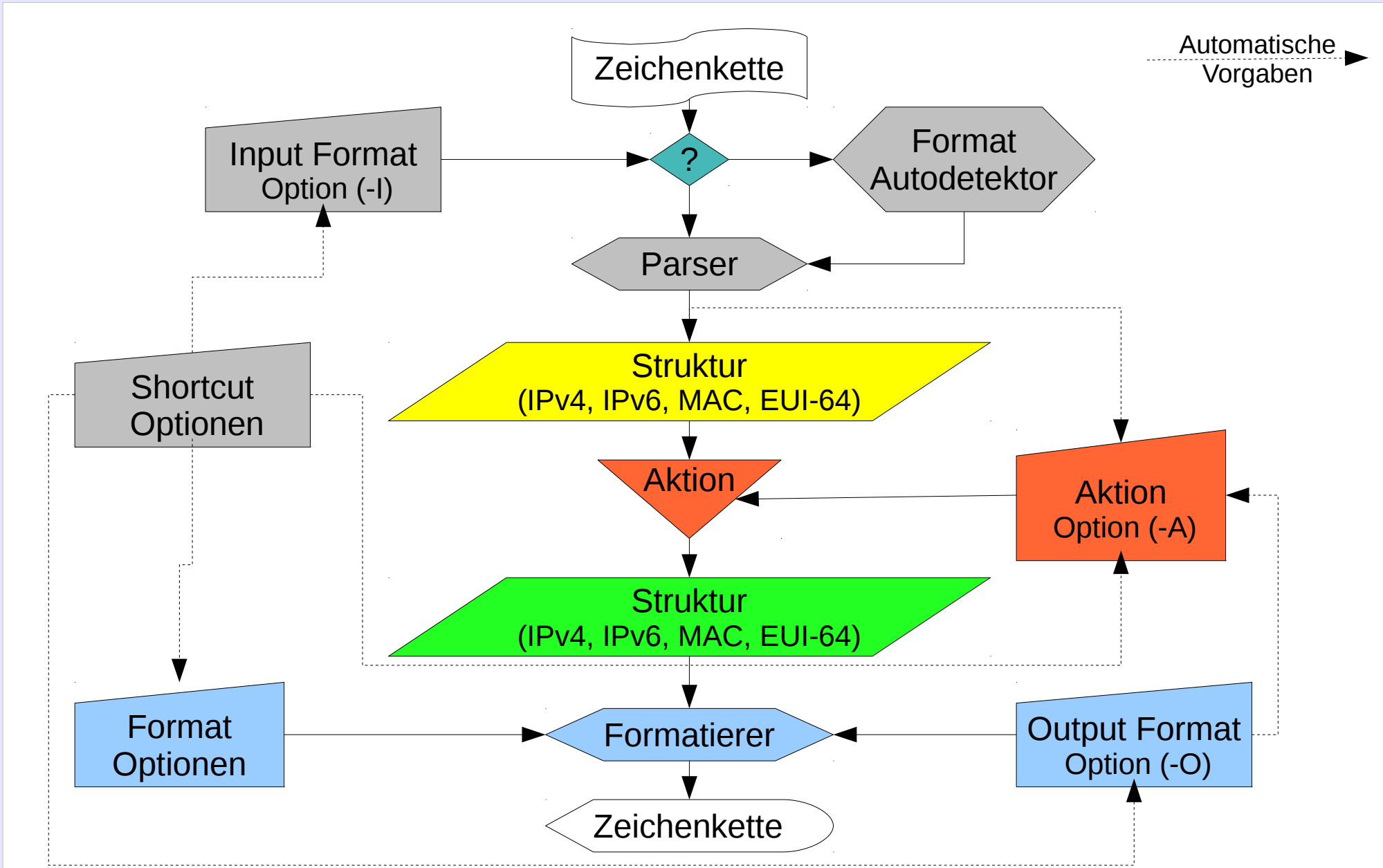
Externe Datenbank-Abfragen

- **Unterstützte Datenbanken**
  - Anbieter
    - GeoIP
    - IP2Location
  - Abfragen
    - IPv4, IPv6 -> Informationen
      - AS Nummer (nur GeoIP)
      - Land (Country Code)
      - ...(siehe ipv6calc -m -i ... bzw. ipv6calcweb.cgi)
  - Aktualisierung
    - extern, systemabhängig (cron, manueller Download)
  - Kompilieroptionen
    - Dynamisch gelinkt
    - Dynamisch gelinkt mit Laden bei Verfügbarkeit (dynamic load)
      - Deaktivieren von Features, wenn "runtime" externe Bibliothek fehlt

ipv6calc

Schweizer Messer
für verschiedene Adresstypen
IPv4, IPv6, MAC, EUI-64

ipv6calc / Funktionsweise



ipv6calc / Features

- **Anzeige der einkompilierten Features**
  - Einfache Version (ohne externe Datenbanken)

```
$ ipv6calc -v
ipv6calc: version 0.97.1 DB_AS DB_IPV4 DB_IPV6 DB_CC_REG DB_IEEE ANON_ZEROISE
ANON_ANONYMIZE
```

  - Incl. allen unterstützten externen Datenbanken
    - Abhängige Features werden automatisch freigeschaltet

```
$ ipv6calc -v
ipv6calc: version 0.97.1 IP2Location GeoIP GeoIPv6 DB_AS DB_IPV4 DB_IPV6 DB_IPV4_AS
DB_IPV6_AS DB_IPV4_CC DB_IPV6_CC DB_CC_REG DB_IEEE ANON_ZEROISE ANON_ANONYMIZE ANON_KEEP-
TYPE-ASN-CC
```

- **Arbeitsweise**
  - "single-shot" : nur eine Adresse
  - "pipe-mode" : Benutzung als Pipe-Filter

ipv6calc / Optionen

- **Allgemein**
  - -I <INPUT-FORMAT>
    - Vorgabe: Auto-Erkennung
  - -O <OUTPUT-FORMAT>
    - Vorgabe: abhängig vom <INPUT-FORMAT>
  - -A <ACTION> (optional)
    - Vorgabe: tw. von <INPUT-FORMAT> und <OUTPUT-FORMAT>
- **Abkürzungen**
  - -a = -I ipv6addr -O revnibbles.arpa
  - … (siehe Online-Hilfe: -h)
- **Speziell**
  - -i [-m] Informations-Modus [-m = machine-readable]

ipv6calc / Input-Format

- **Unterstütze Input-Formate (-I <FORMAT>)**
  - revnibbles.arpa : Reverse DNS mit ip6.arpa am Ende
  - ipv6addr : IPv6 Adresse
  - ipv4addr : IPv4 Adresse
  - mac : MAC Adresse (48 bit)
  - eui64 : EUI-64 (64 bit)
  - asn : Autonomous System Number
  - … (siehe Online-Hilfe: -I -h)

fast alle Formate werden auch automatisch erkannt !

ipv6calc / Output-Format

- **Unterstützte Output-Formate (-O <FORMAT>)**
  - revnibbles.arpa : Reverse DNS mit ip6.arpa am Ende
  - ipv6addr : IPv6 Adresse
  - ipv4addr : IPv4 Adresse
  - mac : MAC Adresse (48 bits)
  - eui64 : EUI-64 (64 bits)
  - iid : Interface identifier
  - addrtype : Adress-Typ
  - ouitype : OUI (IEEE) Typ
  - ipv6addrtype : IPv6 Adress-Typ
  - revipv4 : Reverse DNS mit in-addr.arpa am Ende
  - … (siehe Online-Hilfe: -O -h)

ipv6calc / Aktionen

- **Mögliche Aktionen (-A <ACTION>)**
  - geneui64 : MAC => EUI-64
  - conv6to4 : IPv4 <-> 6to4 IPv6
  - prefixmac2ipv6 : Präfix + MAC => IPv6
  - anonymize : Anonymisierung
  - filter : Adress-Filterung (Pipe-Modus)
  - … (siehe Online-Hilfe: -A -h)

  - Beispiele via Online-Hilfe: -A <ACTION> -h

Aktionen werden teilweise auch
durch INPUT und OUTPUT-Format festgelegt

ipv6calc / Adress-Information

- **"Human Readable"**

```
$ ipv6calc -q -i 2001:a60:0000:0001:489c:1212:34fd:130f
Address type: unicast, global-unicast, productive, iid-random, iid, iid-local
Address type has SLA: 0001
Registry for address: RIPENCC
Country Code: DE
ASN for address: 8767
Interface identifier: 489c:1212:34fd:130f
Interface identifier is probably generated by privacy extension
IP2Location country name and code: GERMANY (DE)
 IP2Location not machinereadable output currently only limited supported
GeoIP country name and code: Germany (DE)
 GeoIP not machinereadable output currently only limited supported
```

ipv6calc / Adress-Information

Maschinen-Lesbar

```
$ ipv6calc -q -i -m 2001:a60:0000:0001:489c:1212:34fd:130f

IPV6=2001:0a60:1168:0001:489c:1212:34fd:130f
IPV6_ANON=a909:16fa:9092:23ff:a909:4941:0000:0007
IPV6_TYPE=unicast,global-unicast,productive,iid-random,iid,iid-local
SLA=0001
IPV6_REGISTRY=RIPENCC
IPV6_COUNTRYCODE=DE
IPV6_AS_NUM=8767
IID=489c:1212:34fd:130f
EUI64_SCOPE=local-random
IP2LOCATION_COUNTRY_SHORT=DE
IP2LOCATION_COUNTRY_LONG=GERMANY
GEOIP_AS_TEXT=AS8767 M-net Telekommunikations GmbH, Germany
GEOIP_COUNTRY_SHORT=DE
GEOIP_COUNTRY_LONG=Germany
GEOIP_LATITUDE=51.000000
GEOIP_LONGITUDE=9.000000
IP2LOCATION_DATABASE_INFO=IP2L-DB1 20130307 Copyright (c) 2013 IP2Location All Rights Reserved
GEOIP_DATABASE_INFO=GEO-106FREE 20140304 Build 1 Copyright (c) 2014 MaxMind Inc All Rights Reserved / GEO-117 20130306 Build 1
Copyright (c) 2013 MaxMind Inc All Rights Reserved / GEO-536LITE 20140305 Build 1 Copyright (c) 2014 MaxMind Inc All Rights
Reserved
IPV6CALC_NAME=ipv6calc
IPV6CALC_VERSION=0.96.1.rc.1
IPV6CALC_COPYRIGHT="(P) & (C) 2001-2014 by Peter Bieringer <pb (at) bieringer.de>"
IPV6CALC_OUTPUT_VERSION=7
IPV6CALC_SETTINGS_ANON="set=keep-type-asn-cc,mask-ipv6=56,mask-ipv4=24,mask-eui64=40,mask-mac=24,method=keep-type-asn-cc"
IPV6CALC_FEATURES="IP2Location(dyn-load) GeoIP(dyn-load) GeoIPv6 ANON_ZEROISE ANON_ANONYMIZE ANON_KEEP-TYPE-ASN-CC DB_AS
DB_IPV4 DB_IPV6 DB_IPV4_AS DB_IPV6_AS DB_IPV4_CC DB_IPV6_CC DB_CC_REG DB_IEEE"
```

ipv6calc / Format-Änderungen

- **Für Reverse DNS-Zonen (PTR)**

```
$ ipv6calc -a -q 2001:a60:0000:0001:489c:1212:34fd:130f
f.0.3.1.d.f.4.3.2.1.2.1.c.9.8.4.1.0.0.0.8.6.1.1.0.6.a.0.1.0.0.2.ip6.arpa.

$ ipv6calc -a -q 2001:a60:0000:0001:489c:1212:34fd:130f/64 --printprefix
1.0.0.0.8.6.1.1.0.6.a.0.1.0.0.2.ip6.arpa.
```

  - bis < 0.8.0 und ab 0.9.7 wieder funktionsfähig

```
$ ipv6calc -a -q 2001:a60:0000:0001:489c:1212:34fd:130f/64 --printsuffix
f.0.3.1.d.f.4.3.2.1.2.1.c.9.8.4
$ ipv6calc -a -q 2001:a60:0000:0001:489c:1212:34fd:130f --printstart 49 --printend 64
1.0.0.0
```

-a
Abkürzung für
-I ipv6addr -O revnibbles.arpa

ipv6calc / Filter-Modus

- **Filter nach Typ einer Adresse**
  - Typ einer Adresse

```
$ ipv6calc -q -m -i 2001:db8::1 | grep ^IPV6_TYPE
IPV6_TYPE=unicast,global-unicast,productive,iid,iid-local
```

    - Filterung (positiv)

```
$ echo "2001:db8::1" | ipv6calc -E iid-local
2001:db8::1
```

    - Filterung (negiert)

```
$ echo "2001:db8::1" | ipv6calc -E ^iid-local
(keine Ausgabe)
```

  - Verfügbare Filter-Tokens (Auswahl)

Aktuelle Token-Liste:
-A filter -h

    - IPv6 Adresse

ipv6 unknown unicast multicast anycast loopback link-local site-local compat-v4 mapped reserved unique-local-unicast anonymized-iid anonymized-prefix 6to4 6bone global-unicast unspecified solicited-node productive 6to4-microsoft teredo orchid link-local-teredo nat64 iid-random iid iid-local iid-global iid-teredo iid-eui48 iid-eui64 iid-isatap iid-includes-ipv4

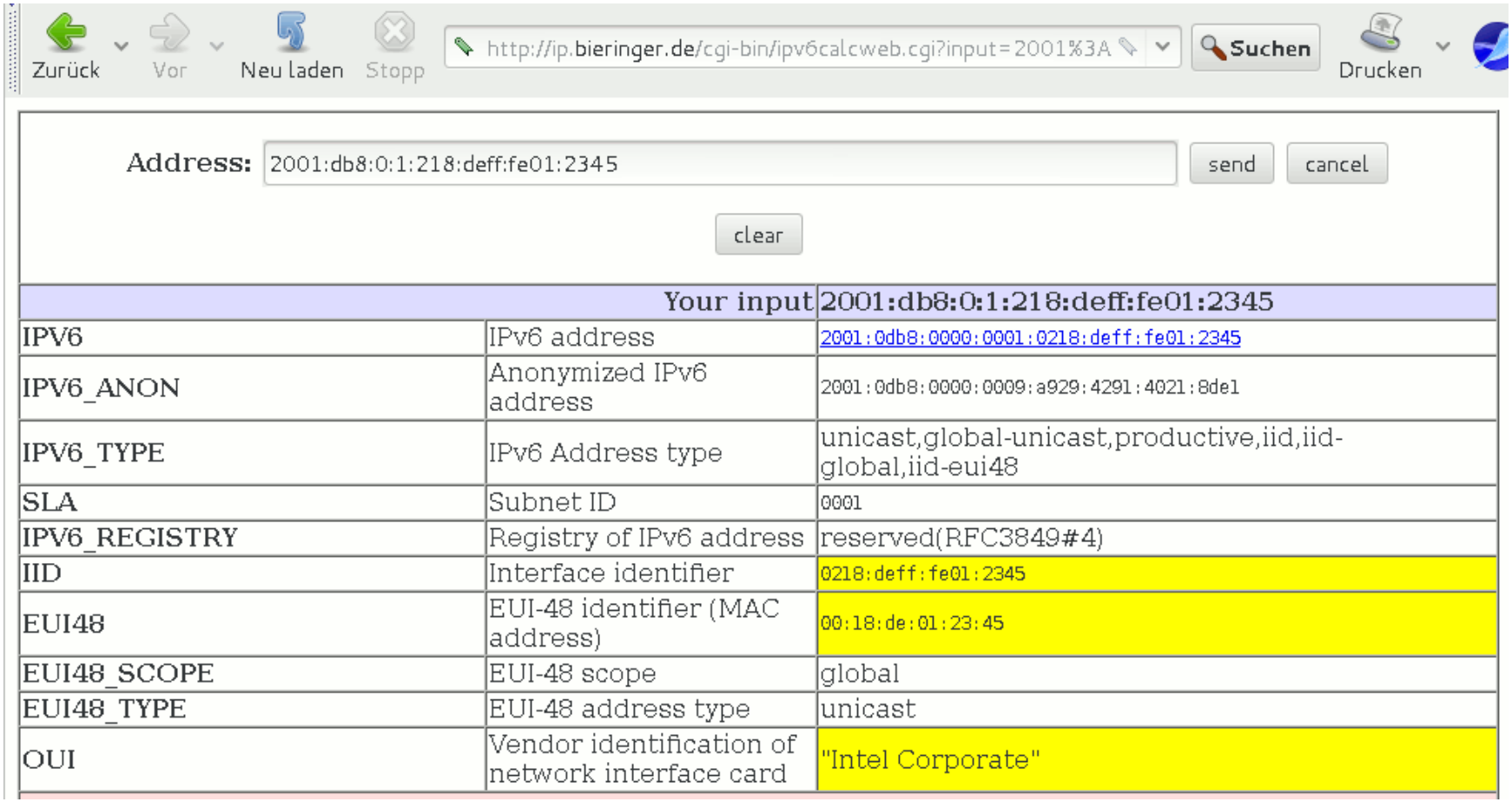
    - IPv4 Adresse

ipv4 any unicast multicast anycast broadcast loopback unspecified unknown reserved zeroconf site-local anonymized global 6to4relay

Online-Werkzeug

ipv6calc Online Tool

- **URL: http://ip.bieringer.de/cgi-bin/ipv6calcweb.cgi**
  - Betrieb von ipv6calcweb.cgi im “Form”-Modus
  - Information über MAC, IPv4 & IPv6-Adressen

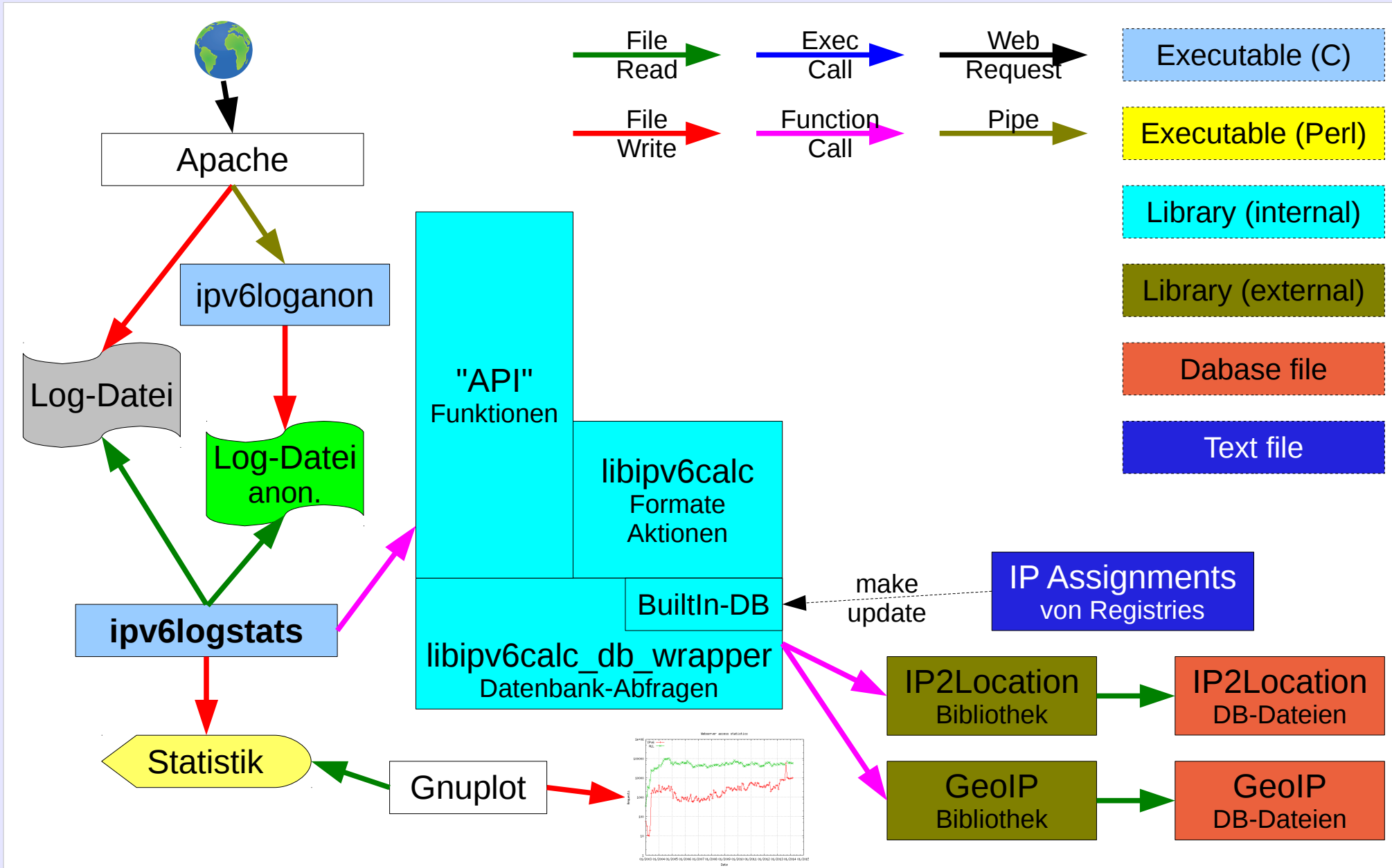


Your input	2001:db8:0:1:218:deff:fe01:2345
IPV6	IPv6 address	2001:0db8:0000:0001:0218:deff:fe01:2345
IPV6_ANON	Anonymized IPv6 address	2001:0db8:0000:0009:a929:4291:4021:8de1
IPV6_TYPE	IPv6 Address type	unicast,global-unicast,productive,iid,iid-global,iid-eui48
SLA	Subnet ID	0001
IPV6_REGISTRY	Registry of IPv6 address	reserved(RFC3849#4)
IID	Interface identifier	0218:deff:fe01:2345
EUI48	EUI-48 identifier (MAC address)	00:18:de:01:23:45
EUI48_SCOPE	EUI-48 scope	global
EUI48_TYPE	EUI-48 address type	unicast
OUI	Vendor identification of network interface card	"Intel Corporate"

ipv6logstats

Statistische Auswertungen von IP-Adressen in Apache-Logfiles

ipv6logstats / Aufbau



ipv6logstats / Konfiguration

- **Ausgabe-Optionen**
  - column => Spalten-Modus (für z.B. GnuPlot)
- **Erweiterte Statistik im Zeilenmodus (nur mit GeoIP)**
  - Country Code => Protokoll-Version
  - Protokoll-Version => Country Code
  - AS-Nummer => Protokoll
  - Protokoll => AS-Nummer

ipv6logstats / Benutzung

- **Offline (Batch)**
  - Statistik in Zeilen zur späteren Auswertung

```
$ cat /path/to/http_log | ipv6logstats <OPTIONS> >/path/to/stats.data
```

  - Statistik in Spalten mit Präfix ohne Kopfzeile

```
$ cat /path/to/http_log | ipv6logstats -n -q -c -p `date '+%Y%m'`
```

ipv6logstats / Ergebnis (1)

- **Statistik in Zeilen**

```
$ cat apache-log | ipv6logstats -q
```

```
*Version                4.0
*DateTime: 2014:04:26 13:43:12+0000 GMT
*UnixTime: 1398519792
*3*DB-Info: DB features: 0x0000133f
…
ALL                     48799
IPv4                    40336
IPv6                    8463
UNKNOWN                 0
IPv4/APNIC              3212
IPv4/ARIN               9307
IPv4/RIPE               25159
IPv4/LACNIC             1680
IPv4/AFRINIC            978
IPv4/UNKNOWN            0
IPv6/6bone              0
IPv6/IANA               0
IPv6/APNIC              1187
IPv6/ARIN               661
IPv6/RIPE               6383
IPv6/LACNIC             108
IPv6/AFRINIC            0
IPv6/RESERVED           0
IPv6/UNKNOWN            0
```

```
…
*3*CC-code-proto/DE/ALL   13667
*3*CC-code-proto/DE/IPv4  9937
*3*CC-code-proto/DE/IPv6  3730
*3*CC-code-proto-list/DE  13667 9937 3730
…
*3*CC-proto-code/ALL/DE   13667
*3*CC-proto-code/IPv4/DE  9937
*3*CC-proto-code/IPv6/DE  3730
…
*3*AS-num-proto/8767/ALL   210
*3*AS-num-proto/8767/IPv4  126
*3*AS-num-proto/8767/IPv6  84
*3*AS-num-proto-list/8767  210 126 84
…
*3*AS-proto-num/ALL/8767   210
*3*AS-proto-num/IPv4/8767  126
*3*AS-proto-num/IPv6/8767  84
…
```

ipv6logstats / Ergebnis (2)

- **Statistik in Spalten**

```
$ cat apache-log | ipv6logstats -q -c
```

```
ALL IPv4 IPv6 UNKNOWN IPv4/APNIC IPv4/ARIN IPv4/RIPE IPv4/LACNIC IPv4/AFRINIC
IPv4/UNKNOWN IPv6/6bone IPv6/IANA IPv6/APNIC IPv6/ARIN IPv6/RIPE IPv6/LACNIC
IPv6/AFRINIC IPv6/RESERVED IPv6/UNKNOWN IPv6/6to4/IANA IPv6/6to4/APNIC
IPv6/6to4/ARIN IPv6/6to4/RIPE IPv6/6to4/LACNIC IPv6/6to4/AFRINIC
IPv6/6to4/RESERVED IPv6/6to4/UNKNOWN IPv6/Teredo/IANA IPv6/Teredo/APNIC
IPv6/Teredo/ARIN IPv6/Teredo/RIPE IPv6/Teredo/LACNIC IPv6/Teredo/AFRINIC
IPv6/Teredo/RESERVED IPv6/Teredo/UNKNOWN IPv6/NAT64/IANA IPv6/NAT64/APNIC
IPv6/NAT64/ARIN IPv6/NAT64/RIPE IPv6/NAT64/LACNIC IPv6/NAT64/AFRINIC
IPv6/NAT64/RESERVED IPv6/NAT64/UNKNOWN IPv6/IID/Global IPv6/IID/Random
IPv6/IID/Manual IPv6/IID/ISATAP IPv6/IID/Unknown #Version(4.0)
```

```
48799 40336 8463 0 3212 9307 25159 1680 978 0 0 0 1187 661 6383 108 0 0 0 0 0
0 21 0 0 0 0 0 103 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1640 2083 4594 22 0 #4.0
```

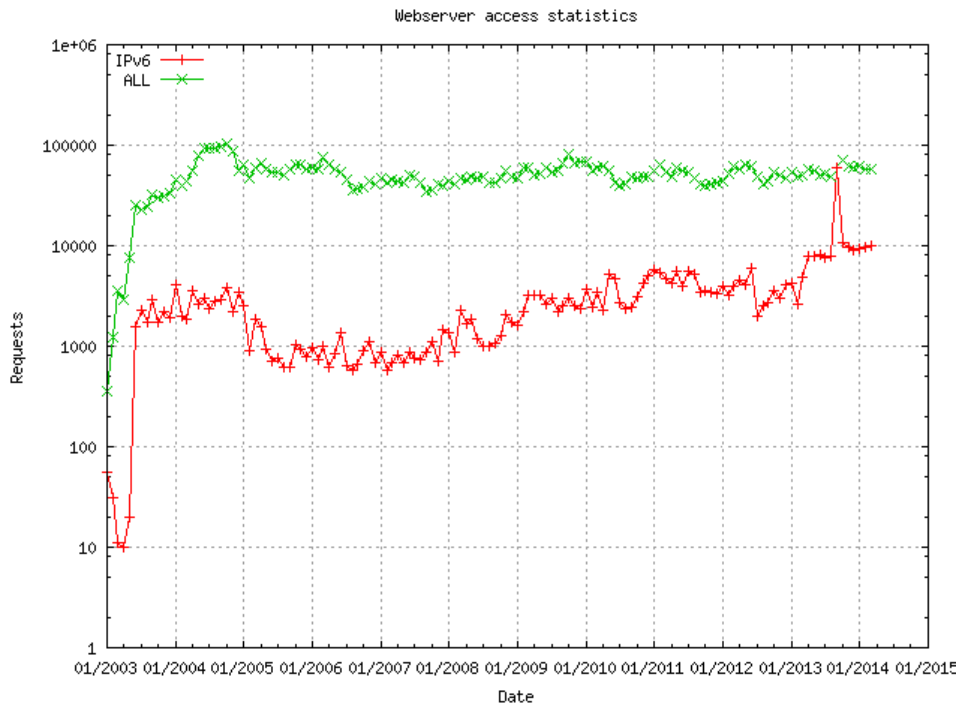
keine CountryCode / ASN Statistik in diesem Format !

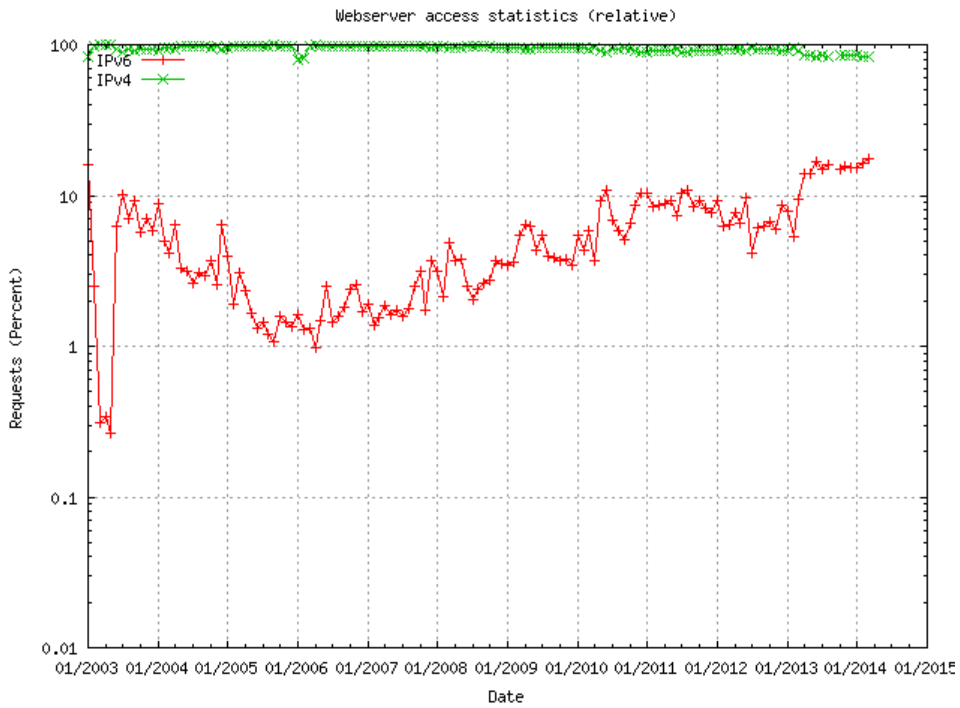
ipv6logstats / Ergebnis

- **Statistik in Spalten über Zeit (einfaches Shell-Script)**

```
$ cat data.ipv6logstats

200301 351 295 56 0 11 168 105 0 11 4 0 0 0 0 0 0 0 0 0 0 52 0 0 0
…
201403 57339 47227 10112 0 3816 12202 28448 1779 982 0 0 576 933 8572 23 0 0 0
0 0 8 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1370 2712 6009 13 0
```

- **Aufbereitung mit GnuPlot**

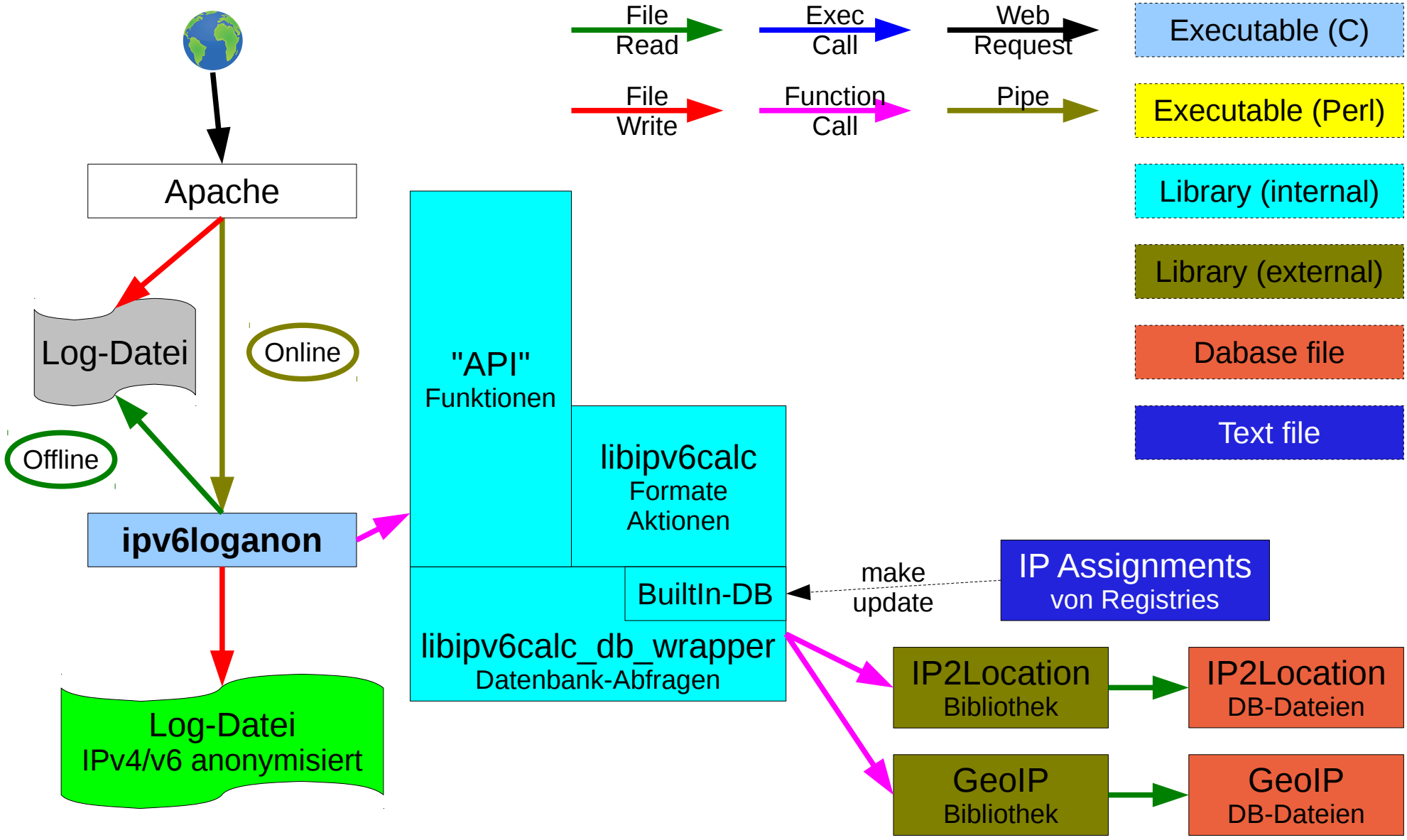




ipv6loganon

Anonymisierung von IP-Adressen
in Apache-Logfiles

ipv6loganon / Aufbau



ipv6loganon / Konfiguration

- **Anonymisierungs-Methoden**
  - anonymize => versucht, Typ und z.B. OUI zu erhalten
  - zeroize => einfaches maskieren
  - keep-type-asn-cc => kodiert Typ, ASN, CountryCode
- **Anonymisierungs-Optionen**
  - Manuell:

```
mask-ipv4  <bits>     : mask IPv4 address [0-32] (even if occurs in IPv6 address)
mask-ipv6  <bits>     : mask IPv6 prefix [0-64] (only applied to related address types)
mask-eui64 <bits>     : mask EUI-64 address or IPv6 interface identifier [0-64]
mask-mac   <bits>     : mask MAC address [0-48]
mask-autoadjust yes|no: autoadjust mask to keep type/vendor information regardless of less given mask
```

  - Voreingestellte Sets:

```
anonymize-standard, anonymize-careful, anonymize-paranoid
zeroize-standard, zeroize-careful, zeroize-paranoid
keep-type-asn-cc
```

ipv6loganon / keep-type-asn-cc

- **Vorgabe: möglichst wenig Informationsverlust**
  - Adresstyp (Präfix, IID), CountryCode, ASN
  - Nur das notwendigste anoymisieren

- **IPv6-Adresse** (siehe auch lib/libipv6addr.h)
  - Präfix: 0xa909 + CountryCode (10-bit) + ASN (32-bit)
  - IID: 0xa9f9 + kodierte IID (typabhängig)
    (beide mit 4-Bit Checksumme gesichert)
- **IPv4-Adresse** (siehe auch lib/libipv4addr.h)
  - Bit 0-3: 0xF (240-255)
  - Bit 4 Parity
  - Bit 5-14 Country Code (10-bit)
  - Bit 15 ASN Flag (0: 16-bit, 1: reduzierte 32-bit)
  - Bit 16-31 ASN (16-bit) bzw. reduzierte 32-bit

ipv6loganon / keep-type-asn-cc

::1 => ::1

::1.2.3.4 => ::246.24.59.65

::ffff:1.2.3.4 => ::ffff:246.24.59.65

46.244.223.233 => 242.222.34.63 (0xf2de223f, AS=8767, CC=DE)

2001:0a60:11e1:9501:e876:aee4:0721:e8ac
=> a909:16fa:9092:23ff:a909:4941::7
(iid-random, AS=8767, CC=DE)

2001:0db8:0000:0000:81c0:0f3f:c807:1455
=> 2001:db8::a909:4941:0:7
(iid-random, IPV6_REGISTRY=reserved)

3ffe:831f:ce49:7601:8000:efff:af4a:86bf
=> 3ffe:831f:ce49:7601:8000:ffff:a0b:f33a
(teredo, Server-IP bleibt erhalten)

64:ff9b::0102:0304 => 64:ff9b::f618:3b41
(nat64)

ipv6loganon / keep-type-asn-cc

IPv4

```
$ ipv6calc -m -i -q 1.2.3.4
IPV4_TYPE=unicast,global
IPV4_AS_NUM=15169
IPV4_COUNTRYCODE=AU
IPV4_REGISTRY=APNIC

$ ipv6calc -m -i -q 246.24.59.65
IPV4_TYPE=unicast,anonymized,global
IPV4_AS_NUM=15169
IPV4_COUNTRYCODE=AU
IPV4_REGISTRY=APNIC
```

Country Code, ASN und Registry bleiben trotz Anonymisierung für statistische Auswertungen erhalten!

Unterstützung in "ipv6logstats" eingebaut!

IPv6

```
$ ipv6calc -m -i -q 2001:0a60:11e1:9501:e876:aee4:0721:e8ac
IPV6_TYPE=unicast,global-unicast,productive,iid-random,iid,iid-local
IPV6_REGISTRY=RIPENCC
IPV6_COUNTRYCODE=DE
IPV6_AS_NUM=8767

$ ipv6calc -m -i -q a909:16fa:9092:23ff:a909:4941::7
IPV6_TYPE=unicast,anonymized-iid,anonymized-prefix,global-unicast,productive,iid-random,iid,iid-local
IPV6_COUNTRYCODE=DE
IPV6_REGISTRY=RIPENCC
IPV6_AS_NUM=8767
```

ipv6loganon / Benutzung

- **Offline (Batch)**

```
$ cat /path/to/http_log | ipv6loganon <OPTIONS> >/path/to/http_log_anonymized
```

- **Online (hier in Verbindung mit "cronolog")**
  - Apache version < 2.4:

```
CustomLog "|/usr/bin/ipv6loganon -f <OPTIONS> |/usr/sbin/cronolog
/var/log/httpd/access.log-%Y%m%d" combined
```

  - Apache version >= 2.4:

```
CustomLog "|$/usr/bin/ipv6loganon -f <OPTIONS> |/usr/sbin/cronolog
/var/log/httpd/access.log-%Y%m%d" combined
```

ipv6loganon / Ergebnis

- **Original**

```
$ tail -1 apache-log
2001:a60:149c:7c01:283e:882e:3fcf:90a8 - - [12/Apr/2014:07:20:35 +0200] "GET /
HTTP/1.1" 200 453 "" "Mozilla/5.0"
```

- **Anonymisierung**
  - "Keep Type, ASN, Country Code"

```
$ tail -1 apache-log | ipv6loganon --anonymize-preset keep-type-asn-cc
a909:16fa:9092:23ff:a909:4941::7 - - [12/Apr/2014:07:20:35 +0200] "GET /
HTTP/1.1" 200 453 "" "Mozilla/5.0"
```

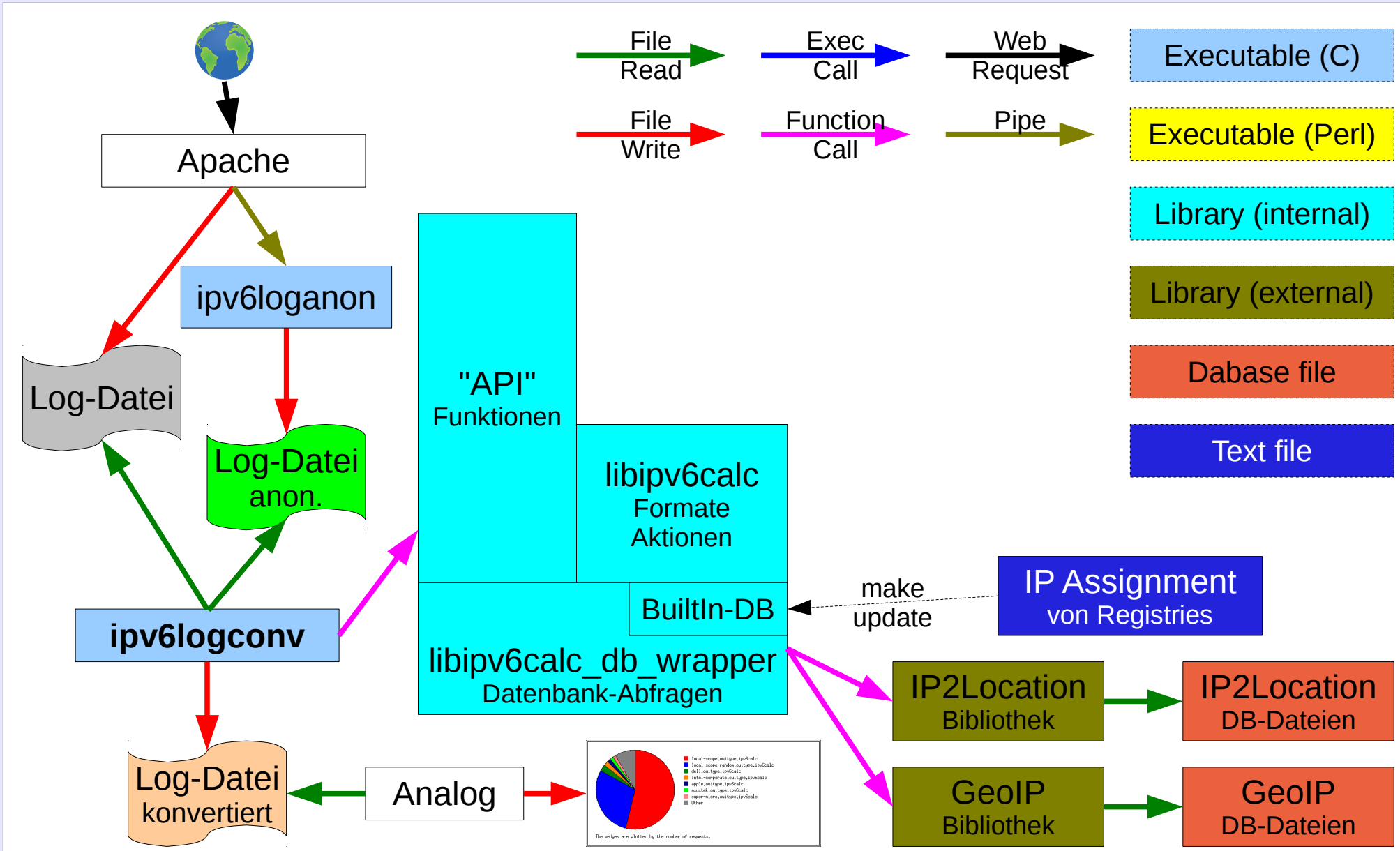
  - "Standard" (nur Interface-ID und SLA)

```
$ tail -1 apache-log | ipv6loganon --anonymize-preset anonymize-standard
2001:a60:149c:7c09:a929:4941::c - - [12/Apr/2014:07:20:35 +0200] "GET /
HTTP/1.1" 200 453 "" "Mozilla/5.0"
```

ipv6logconv

Spezielle Umwandung von IP-Adressen
in Apache-Logfiles
für statistische Aufbereitung

ipv6logconv / Aufbau



ipv6logconv / Konfiguration

- **Ausgabe-Typen**
  - addrtype => Adress-Typ (IPv4/IPv6)
  - ouitype => OUI
  - ipv6addrtype => IPv6-Address-Typ
  - any => Jeder Typ (kombiniert)

ipv6logconv / Benutzung

- **Offline (Batch)**

```
$ cat /path/to/http_log | ipv6logconv <OPTIONS> >/path/to/http_log_converted
```

ipv6logconv / Ergebnis

- **Original**

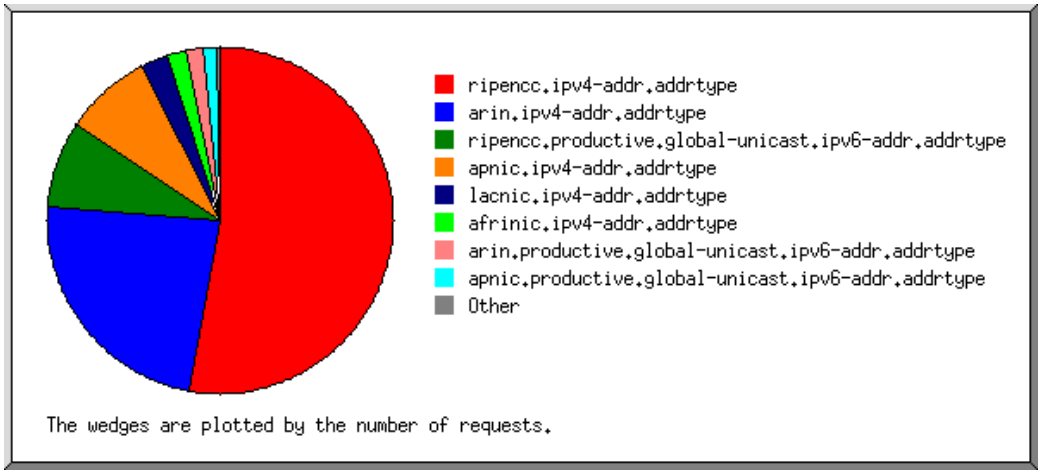
```
$ tail -1 apache-log
2001:a60:149c:7c01:283e:882e:3fcf:90a8 - - [12/Apr/2014:07:20:35 +0200] "GET / HTTP/1.1" 200 453 "" "Mozilla/5.0"
```

- **Konvertiert**

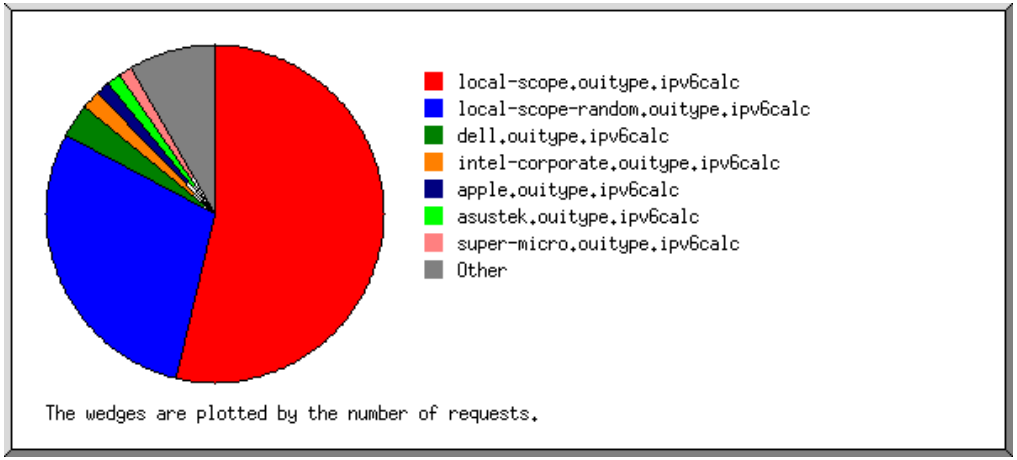
```
$ tail -1 apache-log | ipv6logconv -q --out any
RIPENCC.productive.global-unicast.ipv6-addr.addrtype.ipv6calc - local-scope-random.ouitype.ipv6calc [12/Apr/2014:07:20:35 +0200] "GET / HTTP/1.1" 200 453 "" "Mozilla/5.0"

$ tail -1 apache-log | ipv6logconv -q --out ouitype
local-scope-random.ouitype.ipv6calc - - [12/Apr/2014:07:20:35 +0200] "GET / HTTP/1.1" 200 453 "" "Mozilla/5.0"

$ tail -1 apache-log | ipv6logconv -q --out ipv6addrtype
productive-global.ipv6addrtype.ipv6calc - - [12/Apr/2014:07:20:35 +0200] "GET / HTTP/1.1" 200 453 "" "Mozilla/5.0"
```

ipv6logconv => Analog

- **Grafische Aufbereitung mit Analog**
  - Verteilung nach Registries



  - Verteilung nach IIDs



Siehe auch http://mirrors.bieringer.de/ → Access Statistics

Ausblick

- **Zukunftspläne**
  - Code Cleanup / Verbesserungen
  - Erweiterung Online Hilfe incl. Debug-Optionen
  - Aktualisieren der Manual-Pages
  - Shared-Library & Dynamic Load als Standard
    - Definition von 3rd-Party aufrufbarer API-Funktionen
  - Output-Selektor für maschinenlesbare Ausgabe (Info-Modus)
  - Aktualisierungsmechanismus für eingebaute Datenbanken
    - optionales Laden als externe DB-Dateien
  - Apache-Modul für Inline-Anonymisierung
  - Perl-Programm für universelles Anonymisieren
    - Regular Expressions in Perl
    - ipv6calc für Anonymisierung (Caching durch Hashes in Perl)
  - Internet-Draft für IPv4/IPv6-Anonymisierungsmethode Keep-Type-ASN-CC

Kontakt-Information

peter@deepspace6.net

http://www.deepspace6.net/

pb@bieringer.de

http://www.bieringer.de/pb/

http://www.bieringer.de/linux/IPv6/

http://mirrors.bieringer.de/

Vielen Dank für die Teilnahme!

Fragen & Antworten

Vortrag mit Notizen ist als PDF per E-Mail bzw. über Veranstalter erhältlich!

Dankeschön an

Jürgen Seeger, iX (Einladung)

Der
ipv6calc
Werkzeugkasten

Dr. Peter Bieringer
Deep Space 6
peter@deepspace6.net
http://www.deepspace6.net/

IPv6-Kongress
Frankfurt/Main, Deutschland
22. - 23. Mai 2014
http://www.ipv6-kongress.de/

Über mich

- **Wohnhaft in München (Deutschland)**
- **Beschäftigt als *Senior IT Architect* bei *Giesecke & Devrient 3S GmbH***

Giesecke & Devrient
Creating Confidence.

- **Mitbegründer und Kernmitglied von *Deep Space 6***

- **Autor des "Linux IPv6 HowTo"**

- **Mitautor des Buches "Linux im Netz" (2006)**
  - Grundlagen von TCP/IP incl. IPv6, DNS, DHCP

Meine Internet- & IPv6-Historie

- **1993: Erster Kontakt mit dem Internet (Univ., SunOS)**
- **1996: Erste Erfahrungen mit IPv6 und Linux**
- **1997: *IPv6 & Linux - HowTo*, *initscripts-ipv6***
- **1999: *IPv6 & Linux - Current Status***
- **2001: *Linux IPv6 HOWTO*, *ipv6calc***
- **2002: Mitbegründer von *Deep Space 6***

inzwischen 18 Jahre IPv6-Erfahrung!

Inhalt

Der ipv6calc Werkzeugkasten

- **Übersicht**
- **Interner Aufbau**
  - Features
- **Werkzeuge**
  - ipv6calc
  - ipv6loganon
  - ipv6logconv
  - ipv6logstats
- **Wrapper**
  - ipv6calcweb.cgi
- **Ausblick**

Übersicht

Übersicht (1)

- **Der ipv6calc Werkzeugkasten ist**
  - programmiert in C
    - Ausnahme: ipv6calcweb.cgi (Perl)
  - kompilierbar unter Linux & Unix
  - verfügbar in diversen Distributionen, z.B.
    - RPM:
      - Fedora 20 — 0.94.1-3.fc20
      - Red Hat Enterprise Linux 5 — 0.61-1
      - Red Hat Enterprise Linux 6+7 — n/a (Maintainer für EPEL fehlt momentan)
      - openSuSE — n/a
    - DPKG:
      - Ubuntu 14.04 — 0.95.0
    - Gentoo/Funtoo:
      - Funtoo — 0.96.0
  - nutzbar auf Kommandozeile
    - Ausnahme: ipv6calcweb.cgi (CGI für Webserver)

Lizenz:
GNU GPL version 2

Übersicht (2)

- **Der ipv6calc Werkzeugkasten bietet**
  - Informationen über IPv4/IPv6, MAC-Adressen
    - "ipv6calc -i ..."
  - Möglichkeiten zur Format-Umwandlung
    - z.B. für PTR-Einträge in DNS-Zonen
  - Aktionen
    - Anonymisieren
    - Filtern (Pipe-Modus)
    - ....
  - statistische Auswertungen
    - ipv6logstats, ipv6logconv
- **Homepage: http://www.deepspace6.net/projects/ipv6calc.html**
- **Quell-Code: tar.gz (Releases), CVS (aktuelle Entwicklung)**

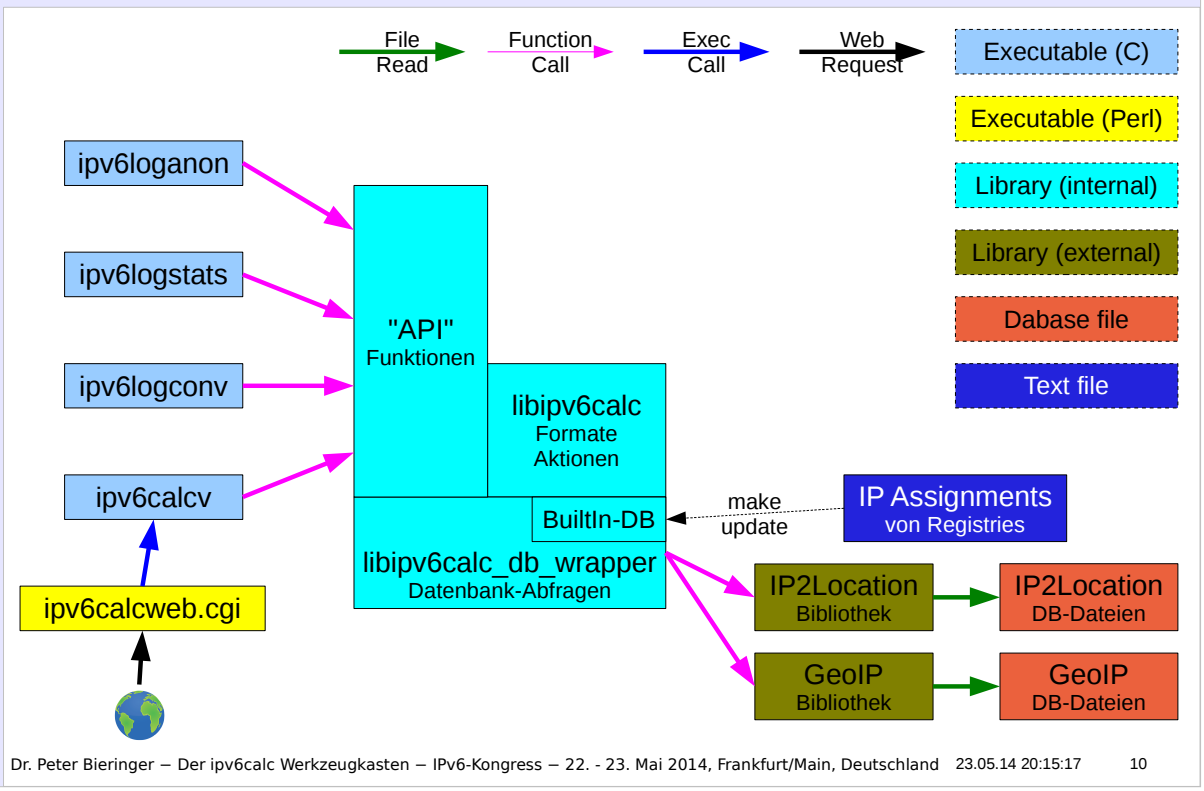
Historie

- **2001: ipv6calc**
- **2002: ipv6logconv, ipv6calcweb.cgi**
- **2003: ipv6logstats**
- **2007: ipv6loganon**
- **2013 / 0.94: Unterstützung für OUI-36**
- **2013 / 0.95:**
  - Restrukturierung GeoIP/IP2Location incl. Dynamic Load
  - vollständige IPv4/IPv6-Adress-Anonymisierung
- **2014 / 0.96: Shared Library Build-Option**
- **2014 / 0.97: Bugfix-Release** 

Aktuell:
0.97.2
(2014-05-23)

Aufbau / Funktionsweise

Interner Aufbau



Interne Datenbanken

- **Datenbank-Typ: "Built-In"**
  - Abfragen
    - IPv4, IPv6 -> Registry
      - ARIN, RIPE NCC, LACNIC, APNIC, AFRINIC
    - MAC, EUI-64 -> Hersteller
      - IAB, OUI, OUI-36 (IEEE)
  - Aktualisierung
    - Vor jedem Release ("make update") durch Download und Aggregierung
      - IANA Adress Space
      - IP-Assignments der Registries
      - IAB, OUI, OUI-36 (IEEE)

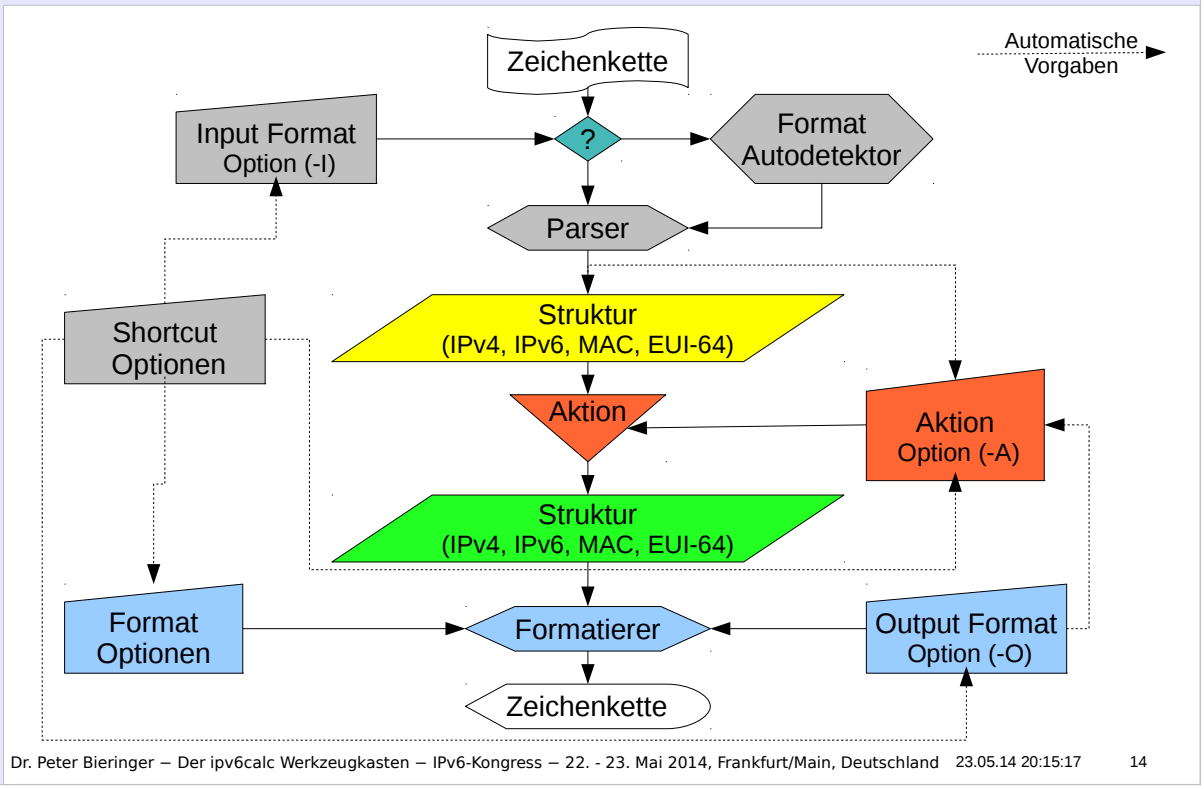
Externe Datenbank-Abfragen

- **Unterstützte Datenbanken**
  - Anbieter
    - GeoIP
    - IP2Location
  - Abfragen
    - IPv4, IPv6 -> Informationen
      - AS Nummer (nur GeoIP)
      - Land (Country Code)
      - ...(siehe ipv6calc -m -i ... bzw. ipv6calcweb.cgi)
  - Aktualisierung
    - extern, systemabhängig (cron, manueller Download)
  - Kompilieroptionen
    - Dynamisch gelinkt
    - Dynamisch gelinkt mit Laden bei Verfügbarkeit (dynamic load)
      - Deaktivieren von Features, wenn "runtime" externe Bibliothek fehlt

ipv6calc

Schweizer Messer
für verschiedene Adresstypen
IPv4, IPv6, MAC, EUI-64

ipv6calc / Funktionsweise



Dr. Peter Bieringer – Der ipv6calc Werkzeugkasten – IPv6-Kongress – 22. - 23. Mai 2014, Frankfurt/Main, Deutschland 23.05.14 20:15:17 14

ipv6calc / Features

- **Anzeige der einkompilierten Features**
  - Einfache Version (ohne externe Datenbanken)

```
$ ipv6calc -v
ipv6calc: version 0.97.1 DB_AS DB_IPV4 DB_IPV6 DB_CC_REG DB_IEEE ANON_ZEROISE
ANON_ANONYMIZE
```

  - Incl. allen unterstützten externen Datenbanken
    - Abhängige Features werden automatisch freigeschaltet

```
$ ipv6calc -v
ipv6calc: version 0.97.1 IP2Location GeoIP GeoIPv6 DB_AS DB_IPV4 DB_IPV6 DB_IPV4_AS
DB_IPV6_AS DB_IPV4_CC DB_IPV6_CC DB_CC_REG DB_IEEE ANON_ZEROISE ANON_ANONYMIZE ANON_KEEP-
TYPE-ASN-CC
```

- **Arbeitsweise**
  - "single-shot" : nur eine Adresse
  - "pipe-mode" : Benutzung als Pipe-Filter

Online Help (1/2):

```
$ ipv6calc -h
ipv6calc: version 0.97.0 DB_AS DB_IPV4 DB_IPV6 DB_CC_REG DB_IEEE ANON_ZEROISE
ANON_ANONYMIZE
(P) & (C) 2001-2014 by Peter Bieringer <pb (at) bieringer.de>

This program formats and calculates IPv6/IPv4/MAC addresses and can do many
more tricky things

  [-d|--debug <debug value>] : debug value (bitwise like)
                               can also be set by IPV6CALC_DEBUG environment
value
  [-v|--version [-v [-v]]]   : version information (2 optional verbose
levels)
  [-h|--help|-?]             : this online help

  [-q|--quiet]               : be more quiet (auto-enabled in pipe mode)
  [-f|--flush]               : flush each line in pipe mode

 Usage with new style options:
  [--in|-I <input type>]   : specify input  type
                             (default: autodetect)
  [--out|-O <output type>] : specify output type
                             (sometimes: autodetect)
  [--action|-A <action>]   : specify action
                             (default: format conversion, sometimes:
autodetect)
  [<format option> ...] : specify format options
  <input data> [...]    : input data

  Available input  types:  [-m] -I|--in     -?|-h|--help
  Available output types:  [-m] -O|--out    -?|-h|--help
  Available action types:  [-m] -A|--action -?|-h|--help
```

ipv6calc / Optionen

- **Allgemein**
  - -I <INPUT-FORMAT>
    - Vorgabe: Auto-Erkennung
  - -O <OUTPUT-FORMAT>
    - Vorgabe: abhängig vom <INPUT-FORMAT>
  - -A <ACTION> (optional)
    - Vorgabe: tw. von <INPUT-FORMAT> und <OUTPUT-FORMAT>
- **Abkürzungen**
  - -a = -I ipv6addr -O revnibbles.arpa
  - … (siehe Online-Hilfe: -h)
- **Speziell**
  - -i [-m] Informations-Modus [-m = machine-readable]

Online Help (2/2):

```
 Other usage:
  --showinfo|-i [--machine_readable|-m] : show information about input data
  --showinfo|-i --show_types            : show available types on '-m'

 Usage with shortcut options: <shortcut option> [<format option> ...] <input
data>
  for more information and available format options use: <shortcut option>
-?|-h|--help

  -r|--addr2ip6_int (-O revnibbles.int)
  -r|--addr_to_ip6int (-O revnibbles.int)
  -a|--addr2ip6_arpa (-O revnibbles.arpa)
  -a|--addr_to_ip6arpa (-O revnibbles.arpa)
  -b|--addr_to_bitstring (-O bitstring)
     --addr2compaddr (--printcompressed)
     --addr_to_compressed (--printcompressed)
     --addr2uncompaddr (--printuncompressed)
     --addr_to_uncompressed (--printuncompressed)
     --addr_to_base85 (-I ipv6addr -O base85)
     --base85_to_addr (-I base85 -O ipv6addr)
     --mac_to_eui64 (-I mac -O eui64)
     --addr2fulluncompaddr (--printfulluncompressed)
     --addr_to_fulluncompressed (--printfulluncompressed)
     --addr2if_inet6 (-I ipv6addr -O ifinet6)
     --addr_to_ifinet6 (-I ipv6addr -O ifinet6)
     --if_inet62addr (-I ifinet6 -O ipv6addr --printcompressed)
     --ifinet6_to_compressed (-I ifinet6 -O ipv6addr --printcompressed)
     --eui64_to_privacy (-I iid_token -O iid_token -A genprivacyiid)
     --ipv4_to_6to4addr (-I ipv4 -O ipv6addr -A conv6to4)
```

ipv6calc / Input-Format

- **Unterstütze Input-Formate (-I <FORMAT>)**
  - revnibbles.arpa : Reverse DNS mit ip6.arpa am Ende
  - ipv6addr : IPv6 Adresse
  - ipv4addr : IPv4 Adresse
  - mac : MAC Adresse (48 bit)
  - eui64 : EUI-64 (64 bit)
  - asn : Autonomous System Number
  - … (siehe Online-Hilfe: -I -h)

fast alle Formate werden auch automatisch erkannt !

Online Help:

```
$ ipv6calc -I -h
ipv6calc: version 0.97.0 DB_AS DB_IPV4 DB_IPV6 DB_CC_REG DB_IEEE ANON_ZEROISE
ANON_ANONYMIZE
(P) & (C) 2001-2014 by Peter Bieringer <pb (at) bieringer.de>

 Available input types:
  auto            : automatic detection
  revnibbles.int  : dot separated nibbles reverse, ending with ip6.int.
  revnibbles.arpa : dot separated nibbles reverse, ending with ip6.arpa.
  bitstring       : bitstring labes, ending with ip6.arpa.
  ipv6addr        : IPv6 address
  ipv6literal     : IPv6 address in literal
  ipv4addr        : IPv4 address
  ipv4hex         : IPv4 in hexdecimal format
  ipv4revhex      : IPv4 in byte-reversed hexdecimal format
  mac             : MAC address (48 bits)
  eui64           : EUI-64 identifier (64 bits)
  base85          : Base-85 string
  ifinet6         : Like line in /proc/net/if_inet6
  iid+token       : Interface identifier and token
  ipv6logconv     : ipv6logconv (currently not supported)
  prefix+mac      : IPv6 prefix and a MAC address
  asn             : Autonomous System Number
```

ipv6calc / Output-Format

- **Unterstützte Output-Formate (-O <FORMAT>)**
  - revnibbles.arpa : Reverse DNS mit ip6.arpa am Ende
  - ipv6addr : IPv6 Adresse
  - ipv4addr : IPv4 Adresse
  - mac : MAC Adresse (48 bits)
  - eui64 : EUI-64 (64 bits)
  - iid : Interface identifier
  - addrtype : Adress-Typ
  - ouitype : OUI (IEEE) Typ
  - ipv6addrtype : IPv6 Adress-Typ
  - revipv4 : Reverse DNS mit in-addr.arpa am Ende
  - … (siehe Online-Hilfe: -O -h)

Online Help:

```
$ ipv6calc -O -h
ipv6calc: version 0.97.0 DB_AS DB_IPV4 DB_IPV6 DB_CC_REG DB_IEEE ANON_ZEROISE
ANON_ANONYMIZE
(P) & (C) 2001-2014 by Peter Bieringer <pb (at) bieringer.de>

 Available output types:
  revnibbles.int  : dot separated nibbles reverse, ending with ip6.int.
  revnibbles.arpa : dot separated nibbles reverse, ending with ip6.arpa.
  bitstring       : bitstring labes, ending with ip6.arpa.
  ipv6addr        : IPv6 address
  ipv4addr        : IPv4 address
  mac             : MAC address (48 bits)
  eui64           : EUI-64 identifier (64 bits)
  base85          : Base-85 string
  ifinet6         : Like line in /proc/net/if_inet6
  iid             : Interface identifier
  iid+token       : Interface identifier and token
  addrtype        : Address type
  ouitype         : OUI (IEEE) type
  ipv6addrtype    : IPv6 address type
  any             : any type (currently not supported)
  revipv4         : reverse IPv4, ending with in-addr.arpa
  ipv4hex         : IPv4 in hexdecimal format
  hex             : IP address in hexadecimal format
  octal           : IP address in escaped octal format
  ipv6literal     : IPv6 address in literal

 For examples and available format options use:
    -O|--out <type> --examples
```

ipv6calc / Aktionen

- **Mögliche Aktionen (-A <ACTION>)**
  - geneui64 : MAC => EUI-64
  - conv6to4 : IPv4 <-> 6to4 IPv6
  - prefixmac2ipv6 : Präfix + MAC => IPv6
  - anonymize : Anonymisierung
  - filter : Adress-Filterung (Pipe-Modus)
  - … (siehe Online-Hilfe: -A -h)
  - Beispiele via Online-Hilfe: -A <ACTION> -h

Aktionen werden teilweise auch
durch INPUT und OUTPUT-Format festgelegt

Online Help:

```
$ ipv6calc -A -h
ipv6calc: version 0.97.0 DB_AS DB_IPV4 DB_IPV6 DB_CC_REG DB_IEEE ANON_ZEROISE
ANON_ANONYMIZE
(P) & (C) 2001-2014 by Peter Bieringer <pb (at) bieringer.de>

 Available action types:
  auto             : Automatic selection of action (default)
  geneui64         : Converts a MAC address to an EUI-64 address
  conv6to4         : Converts IPv4 address <-> 6to4 IPv6 address (prefix)
  genprivacyiid    : Generates a privacy interface ID out of a given one
(arg1) and a token (arg2)
  prefixmac2ipv6   : Generates an IPv6 address out of a prefix and a MAC
address
  anonymize        : Anonymize IPv4/IPv6 address without loosing much
information
  6rd_local_prefix : Calculate the 6rd prefix from given IPv6 prefix & relay
prefix and IPv4
                      Required options:
                       --6rd_prefix ...
                       --6rd_relay_prefix ...
  filter           : Filter addresses related to filter options
```

ipv6calc / Adress-Information

- **"Human Readable"**

```
$ ipv6calc -q -i 2001:a60:0000:0001:489c:1212:34fd:130f
Address type: unicast, global-unicast, productive, iid-random, iid, iid-local
Address type has SLA: 0001
Registry for address: RIPENCC
Country Code: DE
ASN for address: 8767
Interface identifier: 489c:1212:34fd:130f
Interface identifier is probably generated by privacy extension
IP2Location country name and code: GERMANY (DE)
 IP2Location not machinereadable output currently only limited supported
GeoIP country name and code: Germany (DE)
 GeoIP not machinereadable output currently only limited supported
```


ipv6calc / Adress-Information

Maschinen-Lesbar

```
$ ipv6calc -q -i -m 2001:a60:0000:0001:489c:1212:34fd:130f

IPV6=2001:0a60:1168:0001:489c:1212:34fd:130f
IPV6_ANON=a909:16fa:9092:23ff:a909:4941:0000:0007
IPV6_TYPE=unicast,global-unicast,productive,iid-random,iid,iid-local
SLA=0001
IPV6_REGISTRY=RIPENCC
IPV6_COUNTRYCODE=DE
IPV6_AS_NUM=8767
IID=489c:1212:34fd:130f
EUI64_SCOPE=local-random
IP2LOCATION_COUNTRY_SHORT=DE
IP2LOCATION_COUNTRY_LONG=GERMANY
GEOIP_AS_TEXT=AS8767 M-net Telekommunikations GmbH, Germany
GEOIP_COUNTRY_SHORT=DE
GEOIP_COUNTRY_LONG=Germany
GEOIP_LATITUDE=51.000000
GEOIP_LONGITUDE=9.000000
IP2LOCATION_DATABASE_INFO=IP2L-DB1 20130307 Copyright (c) 2013 IP2Location All Rights Reserved
GEOIP_DATABASE_INFO=GEO-106FREE 20140304 Build 1 Copyright (c) 2014 MaxMind Inc All Rights Reserved / GEO-117 20130306 Build 1
Copyright (c) 2013 MaxMind Inc All Rights Reserved / GEO-536LITE 20140305 Build 1 Copyright (c) 2014 MaxMind Inc All Rights
Reserved
IPV6CALC_NAME=ipv6calc
IPV6CALC_VERSION=0.96.1.rc.1
IPV6CALC_COPYRIGHT="(P) & (C) 2001-2014 by Peter Bieringer <pb (at) bieringer.de>"
IPV6CALC_OUTPUT_VERSION=7
IPV6CALC_SETTINGS_ANON="set=keep-type-asn-cc,mask-ipv6=56,mask-ipv4=24,mask-eui64=40,mask-mac=24,method=keep-type-asn-cc"
IPV6CALC_FEATURES="IP2Location(dyn-load) GeoIP(dyn-load) GeoIPv6 ANON_ZEROISE ANON_ANONYMIZE ANON_KEEP-TYPE-ASN-CC DB_AS
DB_IPV4 DB_IPV6 DB_IPV4_AS DB_IPV6_AS DB_IPV4_CC DB_IPV6_CC DB_CC_REG DB_IEEE"
```

ipv6calc / Format-Änderungen

Für Reverse DNS-Zonen (PTR)

```
$ ipv6calc -a -q 2001:a60:0000:0001:489c:1212:34fd:130f
f.0.3.1.d.f.4.3.2.1.2.1.c.9.8.4.1.0.0.0.8.6.1.1.0.6.a.0.1.0.0.2.ip6.arpa.

$ ipv6calc -a -q 2001:a60:0000:0001:489c:1212:34fd:130f/64 --printprefix
1.0.0.0.8.6.1.1.0.6.a.0.1.0.0.2.ip6.arpa.
```

- bis < 0.8.0 und ab 0.9.7 wieder funktionsfähig

```
$ ipv6calc -a -q 2001:a60:0000:0001:489c:1212:34fd:130f/64 --printsuffix
f.0.3.1.d.f.4.3.2.1.2.1.c.9.8.4
$ ipv6calc -a -q 2001:a60:0000:0001:489c:1212:34fd:130f --printstart 49 --printend 64
1.0.0.0
```

-a
Abkürzung für
-I ipv6addr -O revnibbles.arpa

ipv6calc / Filter-Modus

Filter nach Typ einer Adresse

Typ einer Adresse

```
$ ipv6calc -q -m -i 2001:db8::1 | grep ^IPV6_TYPE
IPV6_TYPE=unicast,global-unicast,productive,iid,iid-local
```

Filterung (positiv)

```
$ echo "2001:db8::1" | ipv6calc -E iid-local
2001:db8::1
```

Filterung (negiert)

```
$ echo "2001:db8::1" | ipv6calc -E ^iid-local
(keine Ausgabe)
```

Verfügbare Filter-Tokens (Auswahl)

Aktuelle Token-Liste:
-A filter -h

IPv6 Adresse

ipv6 unknown unicast multicast anycast loopback link-local site-local compat-v4 mapped reserved unique-local-unicast anonymized-iid anonymized-prefix 6to4 6bone global-unicast unspecified solicited-node productive 6to4-microsoft teredo orchid link-local-teredo nat64 iid-random iid iid-local iid-global iid-teredo iid-eui48 iid-eui64 iid-isatap iid-includes-ipv4

IPv4 Adresse

ipv4 any unicast multicast anycast broadcast loopback unspecified unknown reserved zeroconf site-local anonymized global 6to4relay

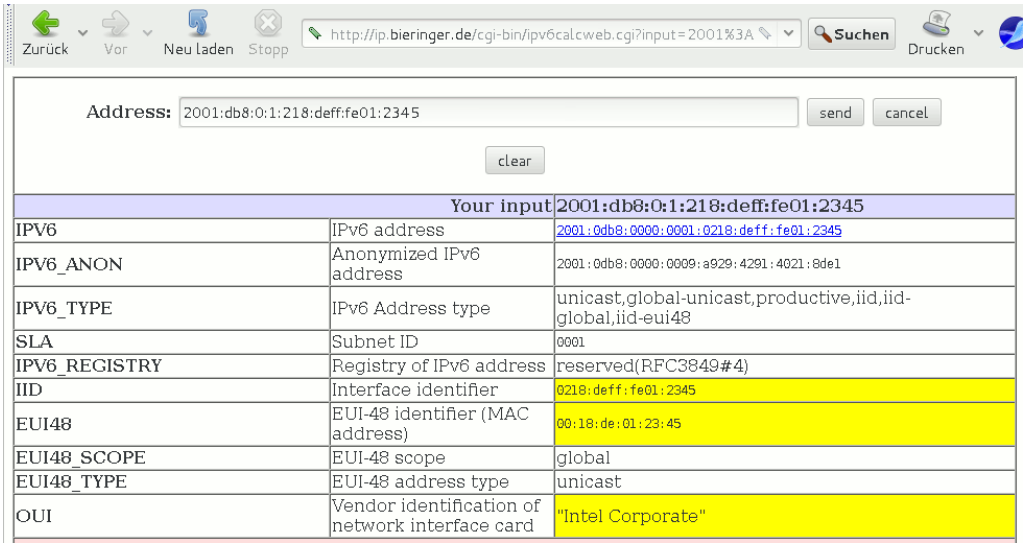
Online Help:

```
$ ipv6calc -A filter -h
ipv6calc: version 0.97.0 DB_AS DB_IPV4 DB_IPV6 DB_CC_REG DB_IEEE ANON_ZEROISE
ANON_ANONYMIZE

 Filter given addresses from stdout by filter expression, e.g.
  echo '2001:db8::1' | ipv6calc [-A filter] -E iid-local
  echo '2001:db8::1' | ipv6calc [-A filter] -E iid-local,global-unicast
  echo '2001:db8::1' | ipv6calc [-A filter] -E ^iid-randomy

 (note: since version 0.95.0 '-A filter' is autoselected if option '-E
<filter expression>' is given)

  IPv6 address filter tokens:
   ipv6  unknown unicast multicast anycast loopback link-local site-local
compat-v4 mapped reserved unique-local-unicast anonymized-iid anonymized-
prefix 6to4 6bone global-unicast unspecified solicited-node productive 6to4-
microsoft teredo orchid link-local-teredo nat64 iid-random iid iid-local iid-
global iid-teredo iid-eui48 iid-eui64 iid-isatap iid-includes-ipv4

  IPv4 address filter tokens:
   ipv4  any unicast multicast anycast broadcast loopback unspecified unknown
reserved zeroconf site-local anonymized global 6to4relay

  EUI-48/MAC address filter tokens:
    IMPLEMENTATION MISSING

  EUI-64 address filter tokens:
    IMPLEMENTATION MISSING
```

Online-Werkzeug

ipv6calc Online Tool

- **URL: http://ip.bieringer.de/cgi-bin/ipv6calcweb.cgi**
  - Betrieb von ipv6calcweb.cgi im “Form”-Modus
  - Information über MAC, IPv4 & IPv6-Adressen



Your input	2001:db8:0:1:218:deff:fe01:2345
IPV6	IPv6 address	2001:0db8:0000:0001:0218:deff:fe01:2345
IPV6_ANON	Anonymized IPv6 address	2001:0db8:0000:0009:a929:4291:4021:8de1
IPV6_TYPE	IPv6 Address type	unicast,global-unicast,productive,iid,iid-global,iid-eui48
SLA	Subnet ID	0001
IPV6_REGISTRY	Registry of IPv6 address	reserved(RFC3849#4)
IID	Interface identifier	0218:deff:fe01:2345
EUI48	EUI-48 identifier (MAC address)	00:18:de:01:23:45
EUI48_SCOPE	EUI-48 scope	global
EUI48_TYPE	EUI-48 address type	unicast
OUI	Vendor identification of network interface card	"Intel Corporate"

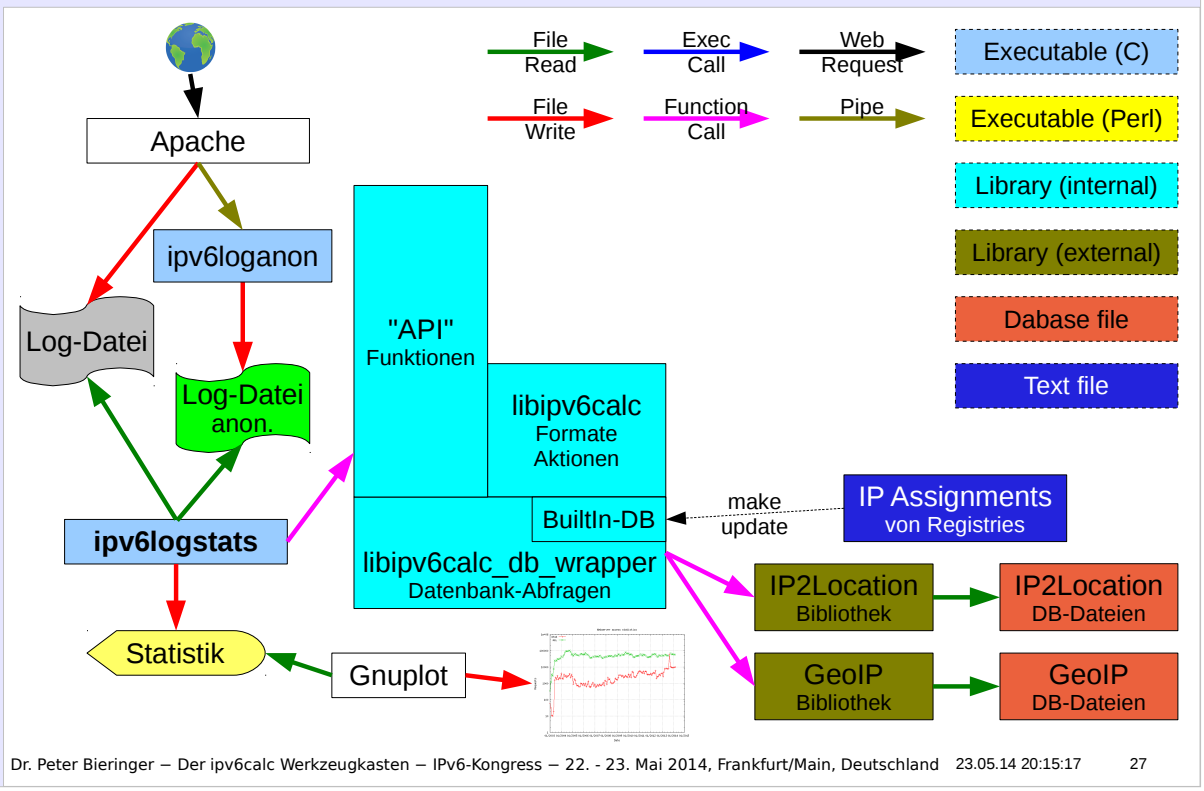
Dr. Peter Bieringer – Der ipv6calc Werkzeugkasten – IPv6-Kongress – 22. - 23. Mai 2014, Frankfurt/Main, Deutschland 23.05.14 20:15:17 25

„Form“-Modus ist neues Feature in „ipv6calcweb.cgi“ seit Version 0.93

ipv6logstats

Statistische Auswertungen von IP-Adressen in Apache-Logfiles

ipv6logstats / Aufbau



ipv6logstats / Konfiguration

- **Ausgabe-Optionen**
  - column => Spalten-Modus (für z.B. GnuPlot)
- **Erweiterte Statistik im Zeilenmodus (nur mit GeoIP)**
  - Country Code => Protokoll-Version
  - Protokoll-Version => Country Code
  - AS-Nummer => Protokoll
  - Protokoll => AS-Nummer

Online Help:

```
$ ipv6logstats -h
ipv6logstats: version 0.97.0 STAT_REG
(P) & (C) 2003-2014 by Peter Bieringer <pb (at) bieringer.de>

 Takes web server log data (or any other data which has IPv4/v6 address in
first column)
   from stdin and print statistics table/list (depending on option) to stdout

  [-d|--debug <debug value>] : debug value (bitwise like)
                                can also be set by IPV6CALC_DEBUG environment
value
  [-v|--version [-v [-v]]]   : version information (2 optional verbose
levels)
  [-h|--help|-?]             : this online help

  [-u|--unknown]             : print unknown IP addresses to stderr
  [-c|--columns]             : print statistics in columns (1)
  [-n|--noheader]            : don't print header in columns mode (1)
  [-o|--onlyheader]          : print only header in columns mode (1)
  [-p|--prefix <token>]      : print token as prefix (1)
  [-q|--quiet]               : be more quiet
  [-s|--simple]              : disable extended statistic (CountryCode/ASN)

 (1) unsupported for CountryCode & ASN statistics
```

ipv6logstats / Benutzung

- **Offline (Batch)**
  - Statistik in Zeilen zur späteren Auswertung

```
$ cat /path/to/http_log | ipv6logstats <OPTIONS> >/path/to/stats.data
```

  - Statistik in Spalten mit Präfix ohne Kopfzeile

```
$ cat /path/to/http_log | ipv6logstats -n -q -c -p `date '+%Y%m'`
```


ipv6logstats / Ergebnis (1)

Statistik in Zeilen

```
$ cat apache-log | ipv6logstats -q
```

```
*Version              4.0
*DateTime: 2014:04:26 13:43:12+0000 GMT
*UnixTime: 1398519792
*3*DB-Info: DB features: 0x0000133f
…
ALL                   48799
IPv4                  40336
IPv6                  8463
UNKNOWN               0
IPv4/APNIC            3212
IPv4/ARIN             9307
IPv4/RIPE             25159
IPv4/LACNIC           1680
IPv4/AFRINIC          978
IPv4/UNKNOWN          0
IPv6/6bone            0
IPv6/IANA             0
IPv6/APNIC            1187
IPv6/ARIN             661
IPv6/RIPE             6383
IPv6/LACNIC           108
IPv6/AFRINIC          0
IPv6/RESERVED         0
IPv6/UNKNOWN          0
```

```
…
*3*CC-code-proto/DE/ALL    13667
*3*CC-code-proto/DE/IPv4   9937
*3*CC-code-proto/DE/IPv6   3730
*3*CC-code-proto-list/DE   13667 9937 3730
…
*3*CC-proto-code/ALL/DE    13667
*3*CC-proto-code/IPv4/DE   9937
*3*CC-proto-code/IPv6/DE   3730
…
*3*AS-num-proto/8767/ALL    210
*3*AS-num-proto/8767/IPv4   126
*3*AS-num-proto/8767/IPv6   84
*3*AS-num-proto-list/8767   210 126 84
…
*3*AS-proto-num/ALL/8767    210
*3*AS-proto-num/IPv4/8767   126
*3*AS-proto-num/IPv6/8767   84
…
```


ipv6logstats / Ergebnis (2)

Statistik in Spalten

```
$ cat apache-log | ipv6logstats -q -c
```

```
ALL IPv4 IPv6 UNKNOWN IPv4/APNIC IPv4/ARIN IPv4/RIPE IPv4/LACNIC IPv4/AFRINIC
IPv4/UNKNOWN IPv6/6bone IPv6/IANA IPv6/APNIC IPv6/ARIN IPv6/RIPE IPv6/LACNIC
IPv6/AFRINIC IPv6/RESERVED IPv6/UNKNOWN IPv6/6to4/IANA IPv6/6to4/APNIC
IPv6/6to4/ARIN IPv6/6to4/RIPE IPv6/6to4/LACNIC IPv6/6to4/AFRINIC
IPv6/6to4/RESERVED IPv6/6to4/UNKNOWN IPv6/Teredo/IANA IPv6/Teredo/APNIC
IPv6/Teredo/ARIN IPv6/Teredo/RIPE IPv6/Teredo/LACNIC IPv6/Teredo/AFRINIC
IPv6/Teredo/RESERVED IPv6/Teredo/UNKNOWN IPv6/NAT64/IANA IPv6/NAT64/APNIC
IPv6/NAT64/ARIN IPv6/NAT64/RIPE IPv6/NAT64/LACNIC IPv6/NAT64/AFRINIC
IPv6/NAT64/RESERVED IPv6/NAT64/UNKNOWN IPv6/IID/Global IPv6/IID/Random
IPv6/IID/Manual IPv6/IID/ISATAP IPv6/IID/Unknown #Version(4.0)
```

```
48799 40336 8463 0 3212 9307 25159 1680 978 0 0 0 1187 661 6383 108 0 0 0 0 0
0 21 0 0 0 0 0 103 0 0 0 0 0 0 0 0 0 0 0 0 0 1640 2083 4594 22 0 #4.0
```

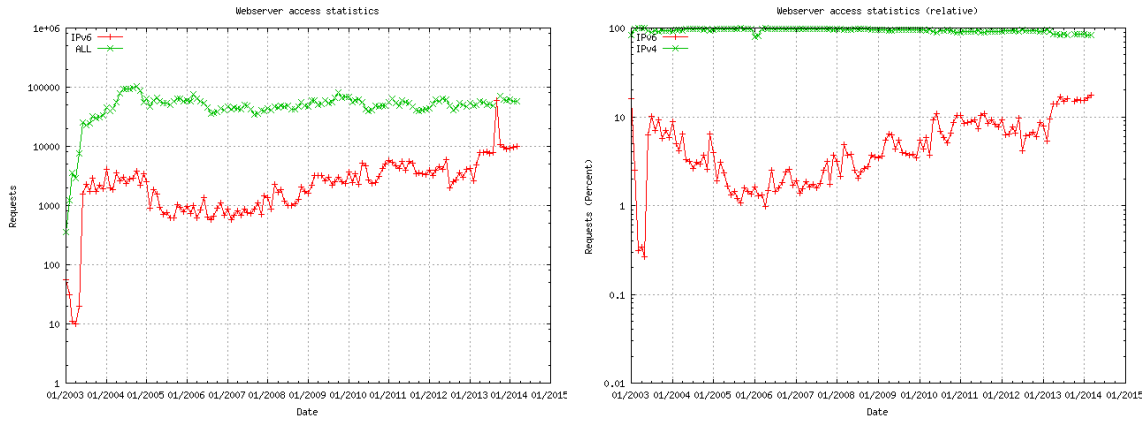
keine CountryCode / ASN Statistik in diesem Format !

ipv6logstats / Ergebnis

- **Statistik in Spalten über Zeit (einfaches Shell-Script)**

```
$ cat data.ipv6logstats
200301 351 295 56 0 11 168 105 0 11 4 0 0 0 0 0 0 0 0 0 52 0 0 0
…
201403 57339 47227 10112 0 3816 12202 28448 1779 982 0 0 576 933 8572 23 0 0 0
0 0 8 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1370 2712 6009 13 0
```

- **Aufbereitung mit GnuPlot**



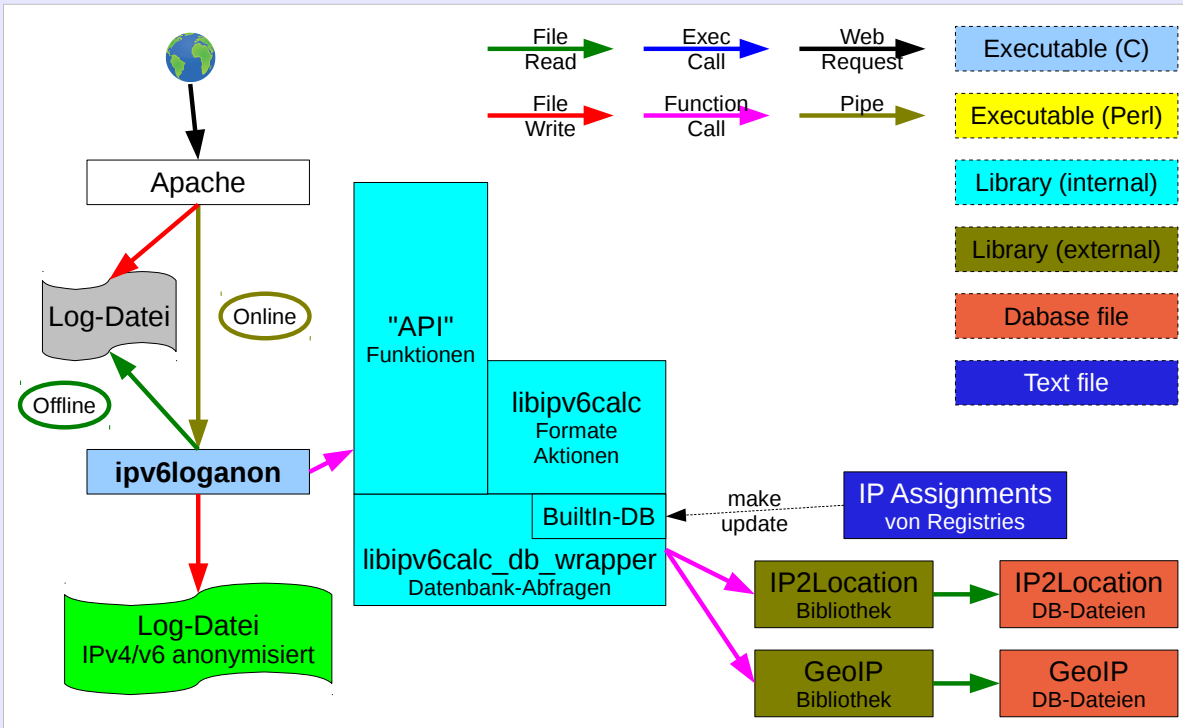
Dr. Peter Bieringer – Der ipv6calc Werkzeugkasten – IPv6-Kongress – 22. - 23. Mai 2014, Frankfurt/Main, Deutschland 23.05.14 20:15:17 32

Konfigurationsbeispiele und Scripts sind im ipv6calc-Paket zu finden

ipv6loganon

Anonymisierung von IP-Adressen in Apache-Logfiles

ipv6loganon / Aufbau



ipv6loganon / Konfiguration

- **Anonymisierungs-Methoden**
  - anonymize => versucht, Typ und z.B. OUI zu erhalten
  - zeroize => einfaches maskieren
  - keep-type-asn-cc => kodiert Typ, ASN, CountryCode
- **Anonymisierungs-Optionen**
  - Manuell:

```
mask-ipv4  <bits>     : mask IPv4 address [0-32] (even if occurs in IPv6 address)
mask-ipv6  <bits>     : mask IPv6 prefix [0-64] (only applied to related address types)
mask-eui64 <bits>     : mask EUI-64 address or IPv6 interface identifier [0-64]
mask-mac   <bits>     : mask MAC address [0-48]
mask-autoadjust yes|no: autoadjust mask to keep type/vendor information regardless of less given mask
```

  - Voreingestellte Sets:

```
anonymize-standard, anonymize-careful, anonymize-paranoid
zeroize-standard, zeroize-careful, zeroize-paranoid
keep-type-asn-cc
```


Online Help (1/2):

```
$ ipv6loganon -h
ipv6loganon: version 0.97.0 ANON_ZEROISE ANON_ANONYMIZE
(P) & (C) 2007-2014 by Peter Bieringer <pb (at) bieringer.de>

This program anonymizes IPv4/IPv6 addresses in e.g. HTTP server log files

  [-d|--debug <debug value>] : debug value (bitwise like)
                               can also be set by IPV6CALC_DEBUG environment
value
  [-v|--version [-v [-v]]]   : version information (2 optional verbose
levels)
  [-h|--help|-?]             : this online help

  [-w|--write]               : write output to file instead of stdout
  [-a|--append]              : append output to file instead of stdout
  [-f|--flush]               : flush output after each line
  [-V|--verbose]             : be verbose
  [-n|--nocache]             : disable caching
  [-c|--cachelimit <value>]  : set cache limit
                               default: 20
                               maximum: 200

  Shortcut for anonymization presets:
   --anonymize-standard (default)
   --anonymize-careful
   --anonymize-paranoid

  Supported methods [--anonymize-method METHOD]:
   anonymize : reliable anonymization, keep as much type information as
possible
   zeroize   : simple zeroizing according to given masks, probably loose type
information
```

ipv6loganon / keep-type-asn-cc

- **Vorgabe: möglichst wenig Informationsverlust**
  - Adresstyp (Präfix, IID), CountryCode, ASN
  - Nur das notwendigste anoymisieren
- **IPv6-Adresse** (siehe auch lib/libipv6addr.h)
  - Präfix: 0xa909 + CountryCode (10-bit) + ASN (32-bit)
  - IID: 0xa9f9 + kodierte IID (typabhängig)
    (beide mit 4-Bit Checksumme gesichert)
- **IPv4-Adresse** (siehe auch lib/libipv4addr.h)
  - Bit 0-3: 0xF (240-255)
  - Bit 4 Parity
  - Bit 5-14 Country Code (10-bit)
  - Bit 15 ASN Flag (0: 16-bit, 1: reduzierte 32-bit)
  - Bit 16-31 ASN (16-bit) bzw. reduzierte 32-bit

Online Help (2/2):

```
   keep-type-asn-cc: special reliable anonymization, keep type & Autonomous
System Number and CountryCode

  Available presets (shortcut names) [--anonymize-preset PRESET-NAME]:
   anonymize-standard   (as): mask-ipv6= 56 mask-ipv4=24 mask-eui64=40 mask-
mac=24 mask-autoadjust=yes method=anonymize
   anonymize-careful    (ac): mask-ipv6= 48 mask-ipv4=20 mask-eui64=24 mask-
mac=24 mask-autoadjust=yes method=anonymize
   anonymize-paranoid   (ap): mask-ipv6= 40 mask-ipv4=16 mask-eui64= 0 mask-
mac=24 mask-autoadjust=no  method=anonymize
   zeroize-standard     (zs): mask-ipv6= 56 mask-ipv4=24 mask-eui64=40 mask-
mac=24 mask-autoadjust=yes method=zeroize
   zeroize-careful      (zc): mask-ipv6= 48 mask-ipv4=20 mask-eui64=24 mask-
mac=24 mask-autoadjust=yes method=zeroize
   zeroize-paranoid     (zp): mask-ipv6= 40 mask-ipv4=16 mask-eui64= 0 mask-
mac=24 mask-autoadjust=no  method=zeroize
   keep-type-asn-cc     (kp): mask-ipv6= 56 mask-ipv4=24 mask-eui64=40 mask-
mac=24 mask-autoadjust=yes method=keep-type-asn-cc

  Custom control:
  --mask-ipv4  <bits>     : mask IPv4 address [0-32] (even if occurs in IPv6
address)
  --mask-ipv6  <bits>     : mask IPv6 prefix [0-64] (only applied to related
address types)
  --mask-eui64 <bits>     : mask EUI-64 address or IPv6 interface identifier
[0-64]
  --mask-mac   <bits>     : mask MAC address [0-48]
  --mask-autoadjust yes|no: autoadjust mask to keep type/vendor information
regardless of less given mask

 Takes data from stdin, outputs the processed data to stdout (default)
```

ipv6loganon / keep-type-asn-cc

::1 => ::1

::1.2.3.4 => ::246.24.59.65

::ffff:1.2.3.4 => ::ffff:246.24.59.65

46.244.223.233 => 242.222.34.63 (0xf2de223f, AS=8767, CC=DE)

2001:0a60:11e1:9501:e876:aee4:0721:e8ac
=> a909:16fa:9092:23ff:a909:4941::7
(iid-random, AS=8767, CC=DE)

2001:0db8:0000:0000:81c0:0f3f:c807:1455
=> 2001:db8::a909:4941:0:7
(iid-random, IPV6_REGISTRY=reserved)

3ffe:831f:ce49:7601:8000:efff:af4a:86bf
=> 3ffe:831f:ce49:7601:8000:ffff:a0b:f33a
(teredo, Server-IP bleibt erhalten)

64:ff9b::0102:0304 => 64:ff9b::f618:3b41
(nat64)

ipv6loganon / keep-type-asn-cc

IPv4

```
$ ipv6calc -m -i -q 1.2.3.4
IPV4_TYPE=unicast,global
IPV4_AS_NUM=15169
IPV4_COUNTRYCODE=AU
IPV4_REGISTRY=APNIC
```

```
$ ipv6calc -m -i -q 246.24.59.65
IPV4_TYPE=unicast,anonymized,global
IPV4_AS_NUM=15169
IPV4_COUNTRYCODE=AU
IPV4_REGISTRY=APNIC
```

Country Code, ASN und Registry bleiben trotz Anonymisierung für statistische Auswertungen erhalten!

Unterstützung in "ipv6logstats" eingebaut!

IPv6

```
$ ipv6calc -m -i -q 2001:0a60:11e1:9501:e876:aee4:0721:e8ac
IPV6_TYPE=unicast,global-unicast,productive,iid-random,iid,iid-local
IPV6_REGISTRY=RIPENCC
IPV6_COUNTRYCODE=DE
IPV6_AS_NUM=8767
```

```
$ ipv6calc -m -i -q a909:16fa:9092:23ff:a909:4941::7
IPV6_TYPE=unicast,anonymized-iid,anonymized-prefix,global-unicast,productive,iid-random,iid,iid-local
IPV6_COUNTRYCODE=DE
IPV6_REGISTRY=RIPENCC
IPV6_AS_NUM=8767
```


Reduzierung der Ausgabe erfolgte mit

```
| egrep '^(IPV._TYPE|IPV._AS_NUM|IPV._COUNTRYCODE|IPV._REGISTRY)='
```

ipv6loganon / Benutzung

- **Offline (Batch)**

```
$ cat /path/to/http_log | ipv6loganon <OPTIONS> >/path/to/http_log_anonymized
```

- **Online (hier in Verbindung mit "cronolog")**
  - Apache version < 2.4:

```
CustomLog "|/usr/bin/ipv6loganon -f <OPTIONS> |/usr/sbin/cronolog
/var/log/httpd/access.log-%Y%m%d" combined
```

  - Apache version >= 2.4:

```
CustomLog "|$/usr/bin/ipv6loganon -f <OPTIONS> |/usr/sbin/cronolog
/var/log/httpd/access.log-%Y%m%d" combined
```


ipv6loganon / Ergebnis

- **Original**

```
$ tail -1 apache-log
2001:a60:149c:7c01:283e:882e:3fcf:90a8 - - [12/Apr/2014:07:20:35 +0200] "GET /
HTTP/1.1" 200 453 "" "Mozilla/5.0"
```

- **Anonymisierung**
  - "Keep Type, ASN, Country Code"

```
$ tail -1 apache-log | ipv6loganon --anonymize-preset keep-type-asn-cc
a909:16fa:9092:23ff:a909:4941::7 - - [12/Apr/2014:07:20:35 +0200] "GET /
HTTP/1.1" 200 453 "" "Mozilla/5.0"
```

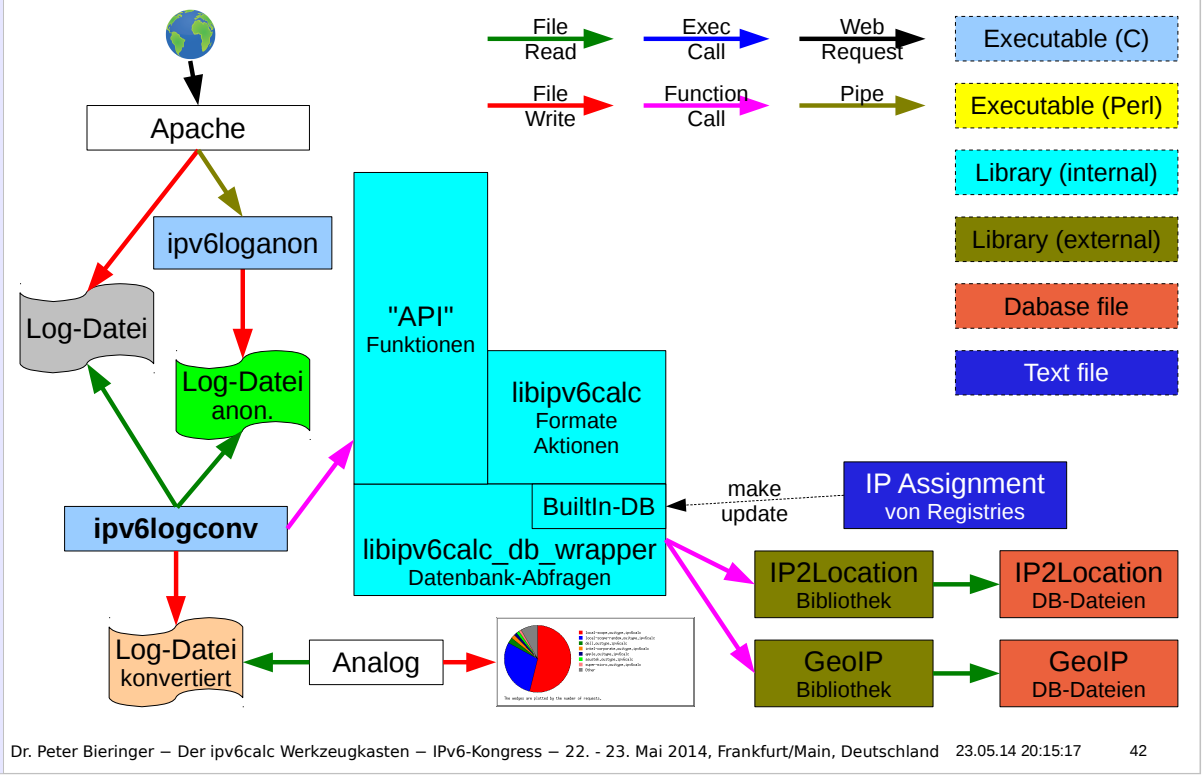
  - "Standard" (nur Interface-ID und SLA)

```
$ tail -1 apache-log | ipv6loganon --anonymize-preset anonymize-standard
2001:a60:149c:7c09:a929:4941::c - - [12/Apr/2014:07:20:35 +0200] "GET /
HTTP/1.1" 200 453 "" "Mozilla/5.0"
```


ipv6logconv

Spezielle Umwandung von IP-Adressen
in Apache-Logfiles
für statistische Aufbereitung

ipv6logconv / Aufbau



ipv6logconv / Konfiguration

- **Ausgabe-Typen**
  - addrtype => Adress-Typ (IPv4/IPv6)
  - ouitype => OUI
  - ipv6addrtype => IPv6-Address-Typ
  - any => Jeder Typ (kombiniert)

Online Help:

```
$ ipv6logconv -h
ipv6logconv: version 0.97.0 CONV_REG CONV_IEEE
(P) & (C) 2002-2014 by Peter Bieringer <pb (at) bieringer.de>

 General:
  [-d|--debug <debug value>] : debug value (bitwise like)
  [-q|--quiet] : be more quiet
  [-n|--nocache] : disable caching
  [-c|--cachelimit <value>] : set cache limit
                              default: 20
                              maximum: 200
 Output:
  [--out <output type>] : specify output type
   addrtype       : Address type
   ouitype        : OUI (IEEE) type
   ipv6addrtype   : IPv6 address type
   any            : any type

 Takes data from stdin, proceed it to stdout
```

ipv6logconv / Benutzung

- **Offline (Batch)**

```
$ cat /path/to/http_log | ipv6logconv <OPTIONS> >/path/to/http_log_converted
```


ipv6logconv / Ergebnis

Original

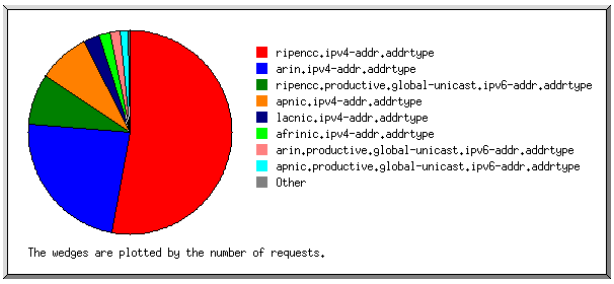
```
$ tail -1 apache-log
2001:a60:149c:7c01:283e:882e:3fcf:90a8 - - [12/Apr/2014:07:20:35 +0200] "GET / HTTP/1.1" 200 453 "" "Mozilla/5.0"
```

Konvertiert

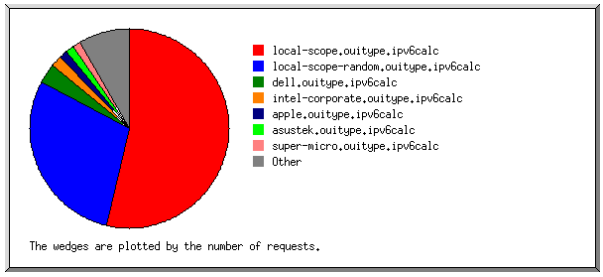
```
$ tail -1 apache-log | ipv6logconv -q --out any
RIPENCC.productive.global-unicast.ipv6-addr.addrtype.ipv6calc - local-scope-random.ouitype.ipv6calc [12/Apr/2014:07:20:35 +0200] "GET / HTTP/1.1" 200 453 "" "Mozilla/5.0"

$ tail -1 apache-log | ipv6logconv -q --out ouitype
local-scope-random.ouitype.ipv6calc - - [12/Apr/2014:07:20:35 +0200] "GET / HTTP/1.1" 200 453 "" "Mozilla/5.0"

$ tail -1 apache-log | ipv6logconv -q --out ipv6addrtype
productive-global.ipv6addrtype.ipv6calc - - [12/Apr/2014:07:20:35 +0200] "GET / HTTP/1.1" 200 453 "" "Mozilla/5.0"
```


ipv6logconv => Analog

- **Grafische Aufbereitung mit Analog**
  - Verteilung nach Registries



  - Verteilung nach IIDs



Siehe auch http://mirrors.bieringer.de/ → Access Statistics

Konfigurationsbeispiele und Scripts sind im ipv6calc-Paket zu finden unter "examples"

Ausblick

- **Zukunftspläne**
  - Code Cleanup / Verbesserungen
  - Erweiterung Online Hilfe incl. Debug-Optionen
  - Aktualisieren der Manual-Pages
  - Shared-Library & Dynamic Load als Standard
    - Definition von 3rd-Party aufrufbarer API-Funktionen
  - Output-Selektor für maschinenlesbare Ausgabe (Info-Modus)
  - Aktualisierungsmechanismus für eingebaute Datenbanken
    - optionales Laden als externe DB-Dateien
  - Apache-Modul für Inline-Anonymisierung
  - Perl-Programm für universelles Anonymisieren
    - Regular Expressions in Perl
    - ipv6calc für Anonymisierung (Caching durch Hashes in Perl)
  - Internet-Draft für IPv4/IPv6-Anonymisierungsmethode Keep-Type-ASN-CC

Kontakt-Information

peter@deepspace6.net

http://www.deepspace6.net/

pb@bieringer.de

http://www.bieringer.de/pb/

http://www.bieringer.de/linux/IPv6/

http://mirrors.bieringer.de/

Vielen Dank für die Teilnahme!

Fragen & Antworten

Vortrag mit Notizen ist als PDF per E-Mail bzw. über Veranstalter erhältlich!

Dankeschön an

Jürgen Seeger, iX (Einladung)

