

IPv6 - Eine Einführung

Jens Link

jenslink@quux.de

Security Day Oranienburg, September 2009

- 1 Einführung
 - IPv6 Adressen
 - Protokolle
- 2 Konfiguration
 - IOS
 - Linux
 - Dienste
- 3 Netzplanung
- 4 IPv6@Home
- 5 Literatur / Kontakt

- Freiberuflicher Consultant
- Schwerpunkt: komplexe Netzwerke, Netzwerksecurity, Netzwerkmonitoring, Troubleshooting

Ich bin käuflich ;-)

Vom Plakat mit dem an der TU Berlin für diesen Vortrag geworben wurde:

Du willst 2001:4D88:FFFF:FFFF:D0:B723:863F:2 Lesen?
blog.fefe.de

Was ist eigentlich mit IPv5?

0-1	Reserved
2-3	Unassigned
4	Internet Protocol
5	ST Datagram Mode
6	Internet Protocol version 6
7	TP/IX: The Next Internet
8	The P Internet Protocol
9	TUBA
10-14	Unassigned
15	Reserved

Quelle: <http://www.iana.org/assignments/version-numbers>

- Viele, auch grosse Provider arbeiten an der Einführung von IPv6

Aus der Presse

... macht eine neue Servicequalität für Datenübertragungen in Echtzeit möglich, zum Beispiel für Internet-Telefonie und Internet-TV

<http://www.egovernment-computing.de/standards/articles/155074/index3.html>

- IPv6 ist viel sicherer, weil da IPSec mit drin ist!

- Wenn ich IPv6 einsetze kann ich kein IPv4 mehr nutzen
- Falsch! Irgendwann in ferner Zukunft mag das zutreffen, noch kann und **muss** man beide Protokolle einsetzen (DualStack).

- “Wir fangen in 14 Jahren damit an. Mein Kollege geht da in Rente.”
- “Da können wir uns ja nicht mehr mit NAT rausreden und müssen Firewallregeln bauen.”
- “Wann ist IPv6 so sicher wie IPv4?”

Heise: ICANN legt sich für rasche Migration zu IPv6 ins Zeug

Zwischen 2009 und 2011 wird die Internet Assigned Numbers Authority (IANA) die letzten IPv4-Nummernblöcke vergeben. Danach gibt es keine solchen Nummern nach Internet Protocol Version 4 mehr.

Quelle: <http://www.heise.de/newsticker/meldung/92004>, 30.06.2007

Wenn 10/8 zu klein ist

Comcast (größter amerikanischer Kabelmodemprovider) ist 10/8 zu klein.

- Je Kunde 2,5 Settop-Boxen
- je Box 2IPs.
- > 20Mio Kunden

http://www.ripe.net/ripe/meetings/ripe-54/presentations/IPv6_management.pdf

Warum IPv6? (IV)

IPv4 hat 255 mögliche /8 Netze davon sind einige Bereiche für spezielle Aufgaben reserviert:

0.0.0.0/8

10.0.0.0/8 Private Network RFC1918

127.0.0.0/8 Loopback

169.254.0.0/16 link local

172.16.0.0/12 Private Network RFC1918

192.0.2.0/24 Test und Dokumentation

192.168.0.0/16 Private Network RFC1918

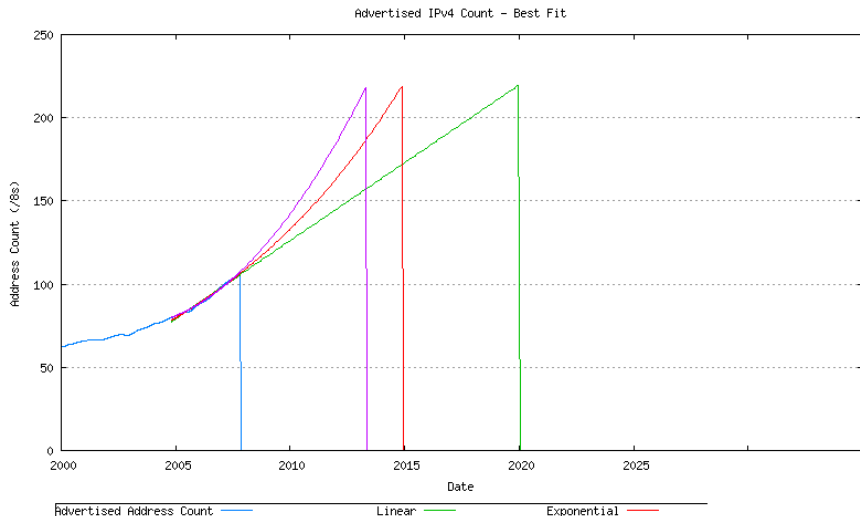
224.0.0.0/4 Multicast

240.0.0.0/4 Experimental

Quelle: <ftp://ftp.rfc-editor.org/in-notes/rfc3330.txt>

Warum IPv6? (V)

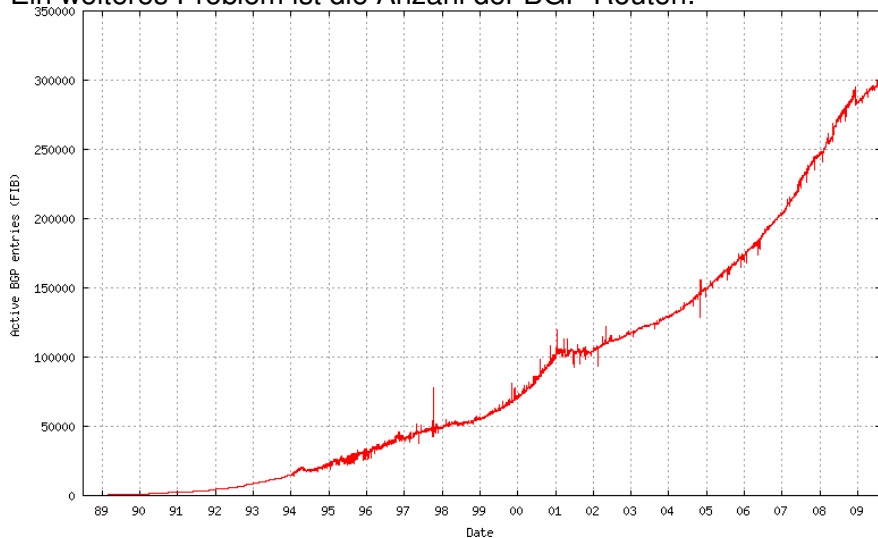
Die Zahl der vergebenen /8 Netze wächst ständig:



Quelle: <http://www.potaroo.net/tools/ipv4/index.html>

Warum IPv6? (VI)

Ein weiteres Problem ist die Anzahl der BGP Routen:



Quelle: <http://bgp.potaroo.net/as2.0/bgp-active.html>

Früher oder später wird IPv6 kommen, es ist besser sich in Ruhe in das Thema einzuarbeiten und jetzt schon passende Entscheidungen beim Netzdesign zu treffen.

Ersteinmal sind IPv4-Adressen noch nicht wirklich knapp. Sie werden nur teurer. Es wurden schon erste kleine ISPs aufgekauft um an zusätzliche Adressen zu kommen. Der Handel mit Adressen hat begonnen. Irgendwann wird es einfach günstiger sein IPv6 einzusetzen.

- NAT (auch auf Seiten von Providern)
- Mehrfach NAT
- 240/4
- Viele andere obskure Idee, wer viel Zeit hat schaue in die Archive der NANOG, IETF, ... Mailinglisten

- IPv6 Adressen sind 128bit lang, es gibt also 2^{128} mögliche Adressen
- $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$
- Das entspricht 665 Milliarden Adressen pro mm^2 Erdoberfläche

IPv6 Adressen werden hexadezimal geschrieben, immer zwei Bytes werden durch einen ':' getrennt. Zum Beispiel:

- 2001:0DB:0000:0000:0000:6BFF:FE42:EC1F

Führende Nullen können weggelassen werden:

- 2001:DB8:0:0:0:6BFF:FE42:EC1F

Genau ein Block von Nullen kann durch zwei Doppelpunkte ersetzt werden:

- 2001:DB8::6BFF:FE42:EC1F
- 2001:DB8:0000:0000:1:0000:0000:1 läßt sich **nicht** zu 2001:DB8::1::1 zusammenfassen

Netzwerkadressen werden wie bei IPv4 als Prefix dargestellt

2001:DB8::/32	65.536 /48 Netze (Kleinste Größe für PI)
2001:DB8:1231::/48	65.536 /64 Netze (Kleinste Größe für PA)
2001:DB8:2241:123::/64	18.446.744.073.709.551.616 Hosts

Es gibt verschiedene Arten der Adressierung:

- Unicast
 - global
 - link-local
 - (site-local) Wird nicht mehr verwendet!
- Anycast
- Multicast

- Ein Interface hat immer eine link-local Unicast Adresse
- Ein Interface hat immer eine oder mehrere Multicast Adressen
- Ein Interface kann mehrere globale Adressen haben

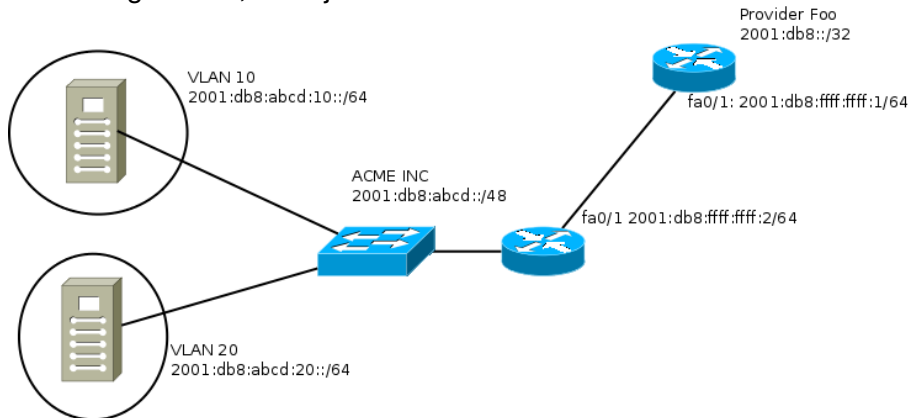
```
j1-home#sh ipv6 interface vlan1
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::219
                                          :30FF:FE11:D813
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:1F0B:8E::1, subnet is 2001:DB8:1F0B
                                          :8E::/64

Joined group address(es):
  FF02::1
  FF02::2
  ...
```

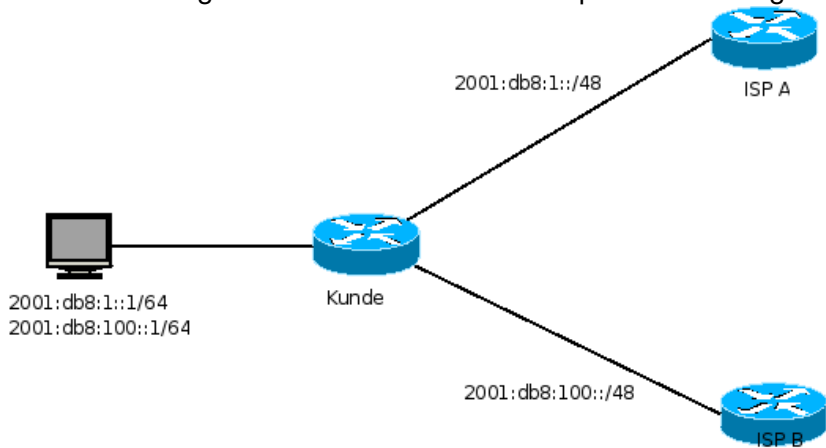
Spezielle Adressen und Adressbereiche

::	nicht spezifizierte Adresse
::1	loopback
FE80::/10	link-local
FF00::/8	multicast
FF01::1	multicast, "all hosts"
FF01::2	multicast, "all routers"
FC00::/8	Unique Local Adressen (zentral verwaltet)
FD00::/8	Unique Local Adressen
2000::/3	globale Unicast Adressen
2001:DB8::/32	Prefix für Dokumentation

Es ist vorgesehen, dass jede Site ein /48 bekommt



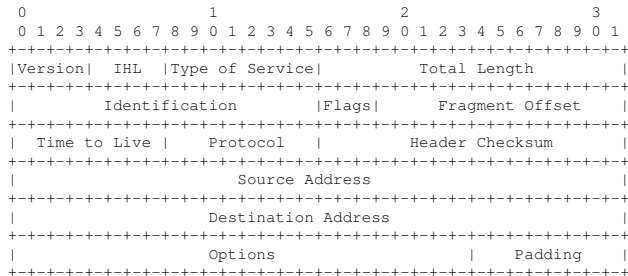
Eine Anbindung über mehr als einen ISP ist problemlos möglich



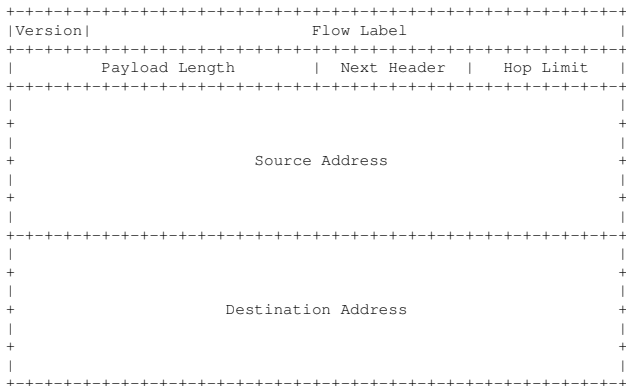
- Eigener Ethernettype: 86DD
- kleinste MTU: 1280 Byte
- Path MTU Discovery (PMTUD)

IPv4 Header

- Die Länge des Headers ist variabel
- Die minimale Länge beträgt 20Byte



Der IPv6 Header:



Version	4 Bit	IP Version (==6)
Flowlabel	28 Bit	Zusatzinformationen für Router, z.B. für QOS
Payload Length	16 Bit	Länge des Paketes nach dem Header
Next Header	8 Bit	Welcher Header kommt danach?
Hop Limit	8 Bit	vgl. TTL bei IPv4
Source Address	128 Bit	
Destination Address	128 Bit	

IPv6 bietet die Möglichkeit zusätzliche Header an den normalen Header anzuhängen.

- Hop-by-Hop Option Header
- Routing Header
- Fragment Header
- Authentication Header
- Privacy Header

IPv6 (V)

```
+-----+-----+
| IPv6 header | TCP header + data
|             |
| Next Header = |
|     TCP     |
+-----+-----+
```

```
+-----+-----+-----+-----+
| IPv6 header | Routing header | Fragment header | fragment of TCP
|             |             |             | header + data
| Next Header = | Next Header = | Next Header = |
|   Routing    |   Fragment    |   TCP         |
+-----+-----+-----+-----+
```


- 1 Destination Unreachable
- 2 Packet Too Big
- 3 Time Exceeded
- 4 Parameter Problem
- 128 Echo Request
- 129 Echo Reply
- 130 Group Membership Query
- 131 Group Membership Report
- 132 Group Membership Reduction
- 133 Router Solicitation
- 134 Router Advertisement
- 135 Neighbor Solicitation
- 136 Neighbor Advertisement
- 137 Redirect
- 138 Router Renumbering

- IPv4: A Record
- IPv6: AAAA Record, früher gab es auch noch einen A6 Record, dieser ist aber mittlerweile veraltet
- Reverse Lookups sind ekelig, die 4321:0:1:2:3:4:567:89ab wird als b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.1.2.3.4.ip6.arpa. geschrieben

Recht nützlich ist hier Peter Bieringers `ipv6calc`:

```
ipv6calc fe80::209:6bff:fe42:ec1f --out revnibbles.arpa
No input type specified, try autodetection found type: ipv6addr
f.1.c.e.2.4.e.f.f.f.b.6.9.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa.
```

ND ist der IPv6 Ersatz für ARP:

- Aus dem Prefix FF02::1:FF00:0/104 und den letzten 24Bit der Ziel IP wird eine Multicast Adresse gebaut
- An diese Adresse wird ein ICMP Paket vom Typ 135 geschickt
- Der Zielhost antwortet mit Layer2 Adresse in einem ICMP Paket vom Typ 136

DAD verhindert die mehrfache Vergabe von IP Adressen:

- Unicast, ICMP Typ 135, Absender ':::' an die Zieladresse
- Wenn die Adresse schon einmal vorhanden ist erfolgt eine Antwort an FF02:1

Autokonfiguration ist einer der Vorteile von IPv6. Ein Host

- wählt eine Interface ID, z.B. seine MAC Adresse
- erzeugt daraus seine link-local Adresse (Prefix: FE80::/64)
- prüft, via DAD ob die Adresse schon einmal vorhanden ist
- fragt via Multicast alle Router nach weiteren Prefixen
- fügt für jedes empfangene Prefix eine weitere Interface Adresse hinzu
- hört weiter auf Router Announcements und ändert ggf. die Adressen
- **Problem:** kein automatischer Eintrag ins DNS

Autokonfiguration löst zwar einige Probleme, welche man z.B. beim Aufbau von redundante DHCP-Server unter IPv4 hat, allerdings ist DHCP mit IPv6 nicht überflüssig geworden. “Optionale” Werte, wie z.B. DNS-Server werden immer noch via DHCP verteilt.

Achtung!

Eigener Client und Server, andere Ports

- Client 546/UDP
- Server/Relay 547/UDP

```
ipv6 unicast-routing
ipv6 cef
ipv6 dhcp pool ipv6-home
  dns-server 2001:DB8:110B::2
  domain-name example.com
  sntp address 2001:DB8:110B::2

!...
interface Vlan1
  ip address 192.168.73.1 255.255.255.0
  ipv6 address 2001:DB8:1F0B:8E::1/64
  ipv6 enable
  ipv6 nd prefix 2001:DB8:1F0B:8E::/64
```

```
interface Tunnel0
  no ip address
  ipv6 address 2001:DB8:1F0A:8E::2/64
  ipv6 enable
  tunnel source Dialer1
  tunnel destination 192.0.2.99
  tunnel mode ipv6ip

ipv6 route ::/0 Tunnel0
```

```
snmp-server community foobar RO ipv6 mgnt 1
!  
access-list 1 permit 192.0.2.0 0.0.0.255
!  
ipv6 access-list mgnt
    permit 2001:DB8:110B::/64  
  
line vty 0 4
    access-class 1 in
    ipv6 access-class mgnt in
!...
```

- ggf. Modul ipv6 laden
- Interface Konfiguration wie gehabt über ip/ifconfig oder automatisch
- eigener(!) Paketfilter: ip6tables
- Beim Einsatz von Linux als Router, den Router Advertising Daemon konfigurieren und starten

/etc/radvd.conf

```
interface eth0
{
  AdvSendAdvert on;
  prefix 2001:DB8:ABCD:EFEF::/64;
}
```

Alternative für radvd: Quagga

/etc/network/interfaces

```
...  
iface eth0 inet static  
    address 192.0.2.190  
    netmask 255.255.255.252  
    gateway 192.0.2.189  
  
iface eth0 inet6 static  
    address 2001:DB8:FFFF:FFFF:0002:B387:786F:2  
    netmask 112  
    gateway 2001:DB8:FFFF:FFFF:0002:B387:786F:1
```

Achtung!

Wer Dienste anbietet sollte sich genau überlegen was er tut:

- Unter IPv4 bietet NAT noch einen gewissen Schutz gegen versehentlich freigegebene Dienste
- IPv6 bietet Ende-zu-Ende Kommunikation, d.h. ein Dienst ist von überall erreichbar.
- Paketfilter Regeln auf dem Host bzw. Router gelten oft nur für IPv4!

- Linux - iptables
- *BSD - pf
- Check Point, Cisco (IOS + PixOS), NetScreen, . . .
- Vorsicht! Einige andere aber überhaupt nicht

- Zum Schutz vor ungewollt eingehenden Verbindungen, State prüfen, woher kommt die Verbindung?
- ICMP Filter gem. RFC 4890
- Sonstigen Voodoo “Deep Packet Inspection, ...”
- Dienste die man nur lokal braucht nur an Link-Local Adressen binden
- ...

Damit BIND über IPv6 arbeiten kann, muss die Option

```
listen-on-v6 {};
```

in der Konfiguration eingeschaltet sein.

Zonefile

```
...
      NS          ns1.example.com.
      NS          ns2.example.com.
      MX          10      mail.example.com.

localhost      A          127.0.0.1
ns1             A          192.0.2.254
ns1             AAAA       2001:DB8:1138::1
mail           A          192.0.2.254
mail           AAAA       2001:DB8:1138::1
...
```

SSH bindet sich automatisch auf alle Interfaces/Protokolle über

```
ListenAddress ::
```

bzw.

```
ListenAddress 0.0.0.0
```

lässt sich das ganze auf bestimmte Adressen und auf nur IPv4 oder nur IPv6 einschränken.

Apache ab der Version 2 unterstützt ebenfalls IPv6. Die Konfiguration ist recht simpel:

```
Listen [2001:DB8:ABCD::1]:80
<VirtualHost [2001:DB8:ABCD::1]:80>
    ServerName ipv6only.example.com
    # ...
</VirtualHost>
```

```
<VirtualHost ipv6.guug.de>  
ServerName ipv6.guug.de  
ProxyPass / http://www.guug.de/  
ProxyPassReverse / http://www.guug.de/  
</VirtualHost>
```

Auch Postfix unterstützt schon lange IPv6. In der `main.cf` muss die folgende Einstellung angepasst werden:

```
inet_protocols = ipv6|all|ipv4
```

/etc/dovecot.conf

```
# "[::]" listens in all IPv6 interfaces, but  
# may also listen in all IPv4 interfaces  
# depending on the operating system.
```

```
protocol pop3 {  
    listen = [::]:110  
}
```

- SQUID, vor Version 3.1
- Apache 1.3
- NFS unter Linux (portmapper)
- Standard Linux Syslogd
- Datenbanken (?)
- Selbstgeschriebene Software
- ...

- Unter http://www.deepspace6.net/docs/ipv6_status_page_apps.html findet man eine gute Übersicht vieler IPv6 fähiger (Linux) Applikationen.

- Für Tools wie ping und traceroute gibt es Ersatz, z.B. ping6 und traceroute6
- Bei einigen Tools läßt sich über -4 bzw. -6 steuern welches Protokoll gewählt wird
- Syntaxs für URLs: `http://[2001:DB8:DEAD:BEEF::1]:80`

Wer sein IPv6-Netz mal genauer testen will.

- <http://freeworld.thc.org/thc-ipv6/>

- Es gibt keinen grossen, roten Knopf mit dem zu Termin X von IPv4 auf IPv6 umgestellt wird
- Die Umstellung kann schrittweise erfolgen, System können (und müssen) erst einmal DualStacked fahren
- IPv6 Only User können z.B. über Proxy-Server auf IPv4 Ressourcen zugreifen
- Die meisten Applikationen unterstützen IPv6, auch (und vor allem) Windows ist in neueren Versionen kein Problem mehr

IPv6 ist nicht IPv4! Umdenken ist angesagt.

- Einige alternative Lösungen zu NAT werden in <http://www.ietf.org/rfc/rfc4864.txt> beschrieben
- Oberstes Ziel ist Aggregation. D.h. Routen zusammenfassen so gut es geht.
- /64 die kleinste Netzwerkgröße
- Verschwendung ist erlaubt. Es gibt genug Adressen. So wird für Point-2-Point-Links ein /64 verwendet
- Mit etwas Gehirnschmalz lassen sich auch Interface-Bezeichner, Routerbezeichnungen, etc. in den IPs unterbringen.
- RFC5375, IPv6 Unicast Address Assignment Considerations

Alle bekannten Routing-Protokollen gibt es auch in einer IPv6-Version bzw. mit IPv6 Unterstützung.

- RIPnG
- EIGRP
- OSPFv3
- ISIS
- BGP

Vorgehensweise bei der Einführung von IPv6

- In einer Testumgebung üben
- Feststellen ob die eingesetzte Hard- und Software auch IPv6 unterstützt
- Provider wegen IPv6 Prefix nerven
- Firewall und Router zum Internet
- internes Netz (Routing)
- DNS
- andere Dienste: SMTP, Web, ...

Provider	Zugang	URL
d-hosting.de	T-DSL u.a.	http://www.d-hosting.de/
RH-TEC	T-DSL u.a.	http://www.rh-tec.de/
Titan DSL	T-DSL	http://www.ipv6-dialin.de/
Tal.DE	T-DSL	http://www.tal.de/
Spacenet AG	T-DSL u.a.	http://www.space.net/
Speedpartner	T-DSL u.a.	http://www.speedpartner.de/
IN-Berlin	T-DSL	http://www.in-dsl.de/
IKS GmbH Jena	direkt	http://www.iks-jena.de/

(Q:Ignatios Souvatzis,

MsgID: <ipv6-providers.4@beverly.kleinbus.org>)

- Tunnel Broker, auch für Enduser
- Tunnel auch für dynamische Adressen (DSL), über spezielle Software
- kostenlos, aber Anmeldung erforderlich
- Punktesystem um Missbrauch vorzubeugen
- Tunnelendpunkte muessen 24/7 erreichbar sein, sonst gibt es keine Punkte
- <http://www.sixxs.net> bietet ausserdem noch zahlreiche Infos rund um IPv6
- Erfordert statische IP oder spez. Tunnelsoftware

- Tunnel Broker, auch für Enduser
- kostenlos, aber Anmeldung erforderlich
- <http://www.tunnelbroker.net/>

- Für einen Host hinter NAT
- Nutzt UDP 3544
- von Microsoft entwickelt
- unter Umständen aktiv
- Linux-Implementierung: Miredo

- 6to4
- GRE
- OpenVPN
- ...

Further Reading

- Benedikt Stockebrand
IPv6 in Practice
A Unixer's Guide to the Next Generation Internet
ISBN 978-3540245247
- Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete
Deploying IPv6 Networks
ISBN 1-58-705210-5
- Scott Hogg, Eric Vyncke
IPv6 Security
ISBN 1-58705-594-5
- UpTimes 03/2007 (Proceedings ECAI6 2007)
ISBN 978-3865412287
- Vorträge ECAI6, http://www.guug.de/veranstaltungen/ecai6-2007/further_readings.html
- DoD IPv6 Standard Profiles For IPv6 Capable Products
- Empfehlungen der NSA zum Thema IPv6 Firewalling

eMail	<code>jenslink@quux.de</code>
Jabber	<code>jenslink@guug.de</code>
PGP Fingerprint	D9FF E215 6686 6194 FFC8 A135 19CF A676 DB85 EF91
Blog	http://blog.quux.de

Coming soon...

