

IPv6 Support Required for All IP-Capable Nodes (RFC 6540)

Das Protokoll und der passende Packetfilter

Bernd Kohler

UMIC Research Centre
RWTH Aachen

12. Juni 2012

Inhaltsverzeichnis

- 1 Begriffe und Infos
- 2 IPv6 Header
- 3 IPv6 Adressen
- 4 ICMP6
- 5 Erfahrungsbericht
- 6 Linux IPv6 Kommandos
- 7 Packetfilter - iptables/netfilter
- 8 Sicherheit/Privatsphäre
- 9 Referenzen

Inhaltsverzeichnis

- 1 Begriffe und Infos
- 2 IPv6 Header
- 3 IPv6 Adressen
- 4 ICMP6
- 5 Erfahrungsbericht
- 6 Linux IPv6 Kommandos
- 7 Packetfilter - iptables/netfilter
- 8 Sicherheit/Privatsphäre
- 9 Referenzen

Inhaltsverzeichnis

- 1 Begriffe und Infos
- 2 IPv6 Header
- 3 IPv6 Adressen
- 4 ICMP6
- 5 Erfahrungsbericht
- 6 Linux IPv6 Kommandos
- 7 Packetfilter - iptables/netfilter
- 8 Sicherheit/Privatsphäre
- 9 Referenzen

Inhaltsverzeichnis

- 1 Begriffe und Infos
- 2 IPv6 Header
- 3 IPv6 Adressen
- 4 ICMP6
- 5 Erfahrungsbericht
- 6 Linux IPv6 Kommandos
- 7 Packetfilter - iptables/netfilter
- 8 Sicherheit/Privatsphäre
- 9 Referenzen

Inhaltsverzeichnis

- 1 Begriffe und Infos
- 2 IPv6 Header
- 3 IPv6 Adressen
- 4 ICMP6
- 5 Erfahrungsbericht
- 6 Linux IPv6 Kommandos
- 7 Packetfilter - iptables/netfilter
- 8 Sicherheit/Privatsphäre
- 9 Referenzen

Inhaltsverzeichnis

- 1 Begriffe und Infos
- 2 IPv6 Header
- 3 IPv6 Adressen
- 4 ICMP6
- 5 Erfahrungsbericht
- 6 Linux IPv6 Kommandos
- 7 Packetfilter - iptables/netfilter
- 8 Sicherheit/Privatsphäre
- 9 Referenzen

Inhaltsverzeichnis

- 1 Begriffe und Infos
- 2 IPv6 Header
- 3 IPv6 Adressen
- 4 ICMP6
- 5 Erfahrungsbericht
- 6 Linux IPv6 Kommandos
- 7 Packetfilter - iptables/netfilter
- 8 Sicherheit/Privatsphäre
- 9 Referenzen

Inhaltsverzeichnis

- 1 Begriffe und Infos
- 2 IPv6 Header
- 3 IPv6 Adressen
- 4 ICMP6
- 5 Erfahrungsbericht
- 6 Linux IPv6 Kommandos
- 7 Packetfilter - iptables/netfilter
- 8 Sicherheit/Privatsphäre
- 9 Referenzen

Inhaltsverzeichnis

- 1 Begriffe und Infos
- 2 IPv6 Header
- 3 IPv6 Adressen
- 4 ICMP6
- 5 Erfahrungsbericht
- 6 Linux IPv6 Kommandos
- 7 Packetfilter - iptables/netfilter
- 8 Sicherheit/Privatsphäre
- 9 Referenzen

Begriffe

- node
- link
- scope
 - local
 - global
 - organisation
- unicast, multicast und anycast
- SLAAC (StateLess Address AutoConfiguration)
EUI-64 (Extended Unique Identifier)
- mobile IPv6
- MTU

Begriffe

- node
link
- scope
local
global
organisation
- unicast, multicast und anycast
- SLAAC (StateLess Address AutoConfiguration)
EUI-64 (Extended Unique Identifier)
- mobile IPv6
- MTU

Begriffe

- node
link
- scope
local
global
organisation
- unicast, multicast und anycast
- SLAAC (StateLess Address AutoConfiguration)
EUI-64 (Extended Unique Identifier)
- mobile IPv6
- MTU

Begriffe

- node
link
- scope
local
global
organisation
- unicast, multicast und anycast
- SLAAC (StateLess Address AutoConfiguration)
EUI-64 (Extended Unique Identifier)
- mobile IPv6
- MTU

Begriffe

- node
link
- scope
local
global
organisation
- unicast, multicast und anycast
- SLAAC (StateLess Address AutoConfiguration)
EUI-64 (Extended Unique Identifier)
- mobile IPv6
- MTU

Begriffe

- node
link
- scope
local
global
organisation
- unicast, multicast und anycast
- SLAAC (StateLess Address AutoConfiguration)
EUI-64 (Extended Unique Identifier)
- mobile IPv6
- MTU

Infos

- kleinere Routingtabellen, kein CIDR/VLSM, **64 Bit Netmask**
- Verzicht auf Broadcast (stattdessen **Multicast**, Anycast)
- Mobilitätsunterstützung (Mobile IPv6)
- native IPsec Unterstützung
- **Autokonfiguration (SLAAC)**
- grösserer Adressraum (128 Bit IPv6, 32 Bit IPv4)
- **IP-Header fester Grösse** (dafür **Extension Header**)
- **mehrere IPs je Link möglich**
- Ersatz von ARP durch ICMPv6 NDP
- **Reichweite von IP-Paketen (scope)**
- Einführung von privaten aber (global) einzigartigen IP-Adressen
- Verzicht von NAT
- Multihoming - Shim6 (siehe RFC 5533)

IPv6 Header

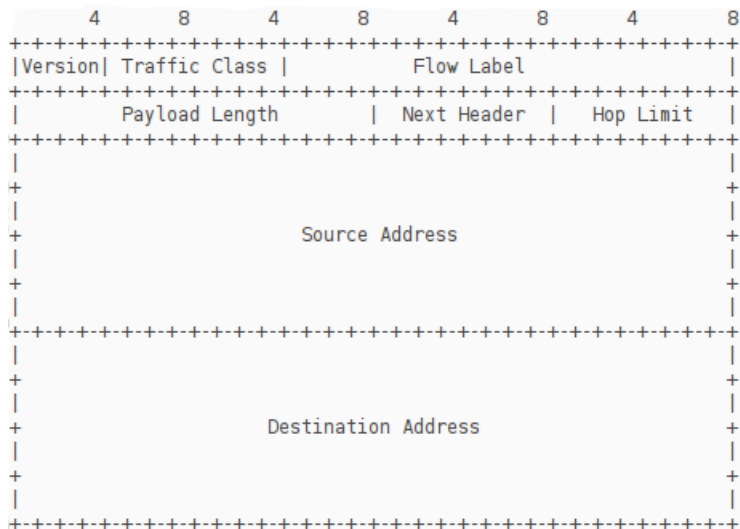


Abbildung: IPv6 Header

IPv6 Header - empfohlene Reihenfolge d. Extension Header

- 6 IPv6 Extension Header (siehe RFC 2460):
- empfohlene Reihenfolge nach RFC 2460:
 1. IPv6-Header
 2. Hop-by-Hop
 3. Destination Options (processed by first hop)
 4. Routing
 5. Fragment
 6. Authentication Header (AH)
 7. Encrypted Security Payload (ESP)
 8. Destination Options (processed by final destination)
 9. Upper-Layer

IPv6 Adressen

- RWTH-Adressen: 2001:638:410: x^1 x^2 x^3 x^4 :interface ID/64
(bspw. 2001:638:410:1230:224:8cff:fe33:e443/64)
- x^1 : 0x0 - 0xD Fachbereich (0=ZHV, 1=Informatik ...) Ausnahmen sind 0xE = Servernetze und 0xF = Infrastruktur (z.B. Transportnetz)
- x^2 : 0x0 - 0xD Einrichtungscode
- x^3 : 0x0 - 0xD Einrichtungscode Fortsetzung zu x^2 (daher 256 Möglichkeiten Einrichtungscode je Fachbereich)
- x^4 : 0x0 - 0xD Netztyp (z.B. Server, Labor, Desktop-PC, Notebook, PC-Pool ...)
- 64 Bit interface ID in modified EUI-64 Format (RFC 4291, RFC 4941) das 7. Bit (2. Bit des 2. Byte) invertiert (1→0 et versus) aus 0000 0000 (0x00) wird bspw. 0000 0010 (0x02) ff:fe padding

IPv6 Adressen

- RWTH-Adressen: 2001:638:410: x^1 x^2 x^3 x^4 :interface ID/64
(bspw. 2001:638:410:1230:224:8cff:fe33:e443/64)
- x^1 : 0x0 - 0xD Fachbereich (0=ZHV, 1=Informatik ...) Ausnahmen sind 0xE = Servernetze und 0xF = Infrastruktur (z.B. Transportnetz)
- x^2 : 0x0 - 0xD Einrichtungscode
- x^3 : 0x0 - 0xD Einrichtungscode Fortsetzung zu x^2 (daher 256 Möglichkeiten Einrichtungscode je Fachbereich)
- x^4 : 0x0 - 0xD Netztyp (z.B. Server, Labor, Desktop-PC, Notebook, PC-Pool ...)
- 64 Bit interface ID in modified EUI-64 Format (RFC 4291, RFC 4941) das 7. Bit (2. Bit des 2. Byte) invertiert (1→0 et versus) aus 0000 0000 (0x00) wird bspw. 0000 0010 (0x02) ff:fe padding

IPv6 Adressen

- RWTH-Adressen: 2001:638:410: x^1 x^2 x^3 x^4 :interface ID/64
(bspw. 2001:638:410:1230:224:8cff:fe33:e443/64)
- x^1 : 0x0 - 0xD Fachbereich (0=ZHV, 1=Informatik ...) Ausnahmen sind 0xE = Servernetze und 0xF = Infrastruktur (z.B. Transportnetz)
- x^2 : 0x0 - 0xD Einrichtungscode
- x^3 : 0x0 - 0xD Einrichtungscode Fortsetzung zu x^2 (daher 256 Möglichkeiten Einrichtungscode je Fachbereich)
- x^4 : 0x0 - 0xD Netztyp (z.B. Server, Labor, Desktop-PC, Notebook, PC-Pool ...)
- 64 Bit interface ID in modified EUI-64 Format (RFC 4291, RFC 4941) das 7. Bit (2. Bit des 2. Byte) invertiert (1→0 et versus) aus 0000 0000 (0x00) wird bspw. 0000 0010 (0x02) ff:fe padding

IPv6 Adressen

- RWTH-Adressen: 2001:638:410: x^1 x^2 x^3 x^4 :interface ID/64
(bspw. 2001:638:410:1230:224:8cff:fe33:e443/64)
- x^1 : 0x0 - 0xD Fachbereich (0=ZHV, 1=Informatik ...) Ausnahmen sind 0xE = Servernetze und 0xF = Infrastruktur (z.B. Transportnetz)
- x^2 : 0x0 - 0xD Einrichtungscode
- x^3 : 0x0 - 0xD Einrichtungscode Fortsetzung zu x^2 (daher 256 Möglichkeiten Einrichtungscode je Fachbereich)
- x^4 : 0x0 - 0xD Netztyp (z.B. Server, Labor, Desktop-PC, Notebook, PC-Pool ...)
- 64 Bit interface ID in modified EUI-64 Format (RFC 4291, RFC 4941) das 7. Bit (2. Bit des 2. Byte) invertiert (1→0 et versus) aus 0000 0000 (0x00) wird bspw. 0000 0010 (0x02) ff:fe padding

IPv6 Adressen

- RWTH-Adressen: 2001:638:410: x^1 x^2 x^3 x^4 :interface ID/64
(bspw. 2001:638:410:1230:224:8cff:fe33:e443/64)
- x^1 : 0x0 - 0xD Fachbereich (0=ZHV, 1=Informatik ...) Ausnahmen sind 0xE = Servernetze und 0xF = Infrastruktur (z.B. Transportnetz)
- x^2 : 0x0 - 0xD Einrichtungscode
- x^3 : 0x0 - 0xD Einrichtungscode Fortsetzung zu x^2 (daher 256 Möglichkeiten Einrichtungscode je Fachbereich)
- x^4 : 0x0 - 0xD Netztyp (z.B. Server, Labor, Desktop-PC, Notebook, PC-Pool ...)
- 64 Bit interface ID in modified EUI-64 Format (RFC 4291, RFC 4941) das 7. Bit (2. Bit des 2. Byte) invertiert (1→0 et versus) aus 0000 0000 (0x00) wird bspw. 0000 0010 (0x02)
ff:fe padding

IPv6 Adressen

- RWTH-Adressen: 2001:638:410: x^1 x^2 x^3 x^4 :interface ID/64
(bspw. 2001:638:410:1230:224:8cff:fe33:e443/64)
- x^1 : 0x0 - 0xD Fachbereich (0=ZHV, 1=Informatik ...) Ausnahmen sind 0xE = Servernetze und 0xF = Infrastruktur (z.B. Transportnetz)
- x^2 : 0x0 - 0xD Einrichtungscode
- x^3 : 0x0 - 0xD Einrichtungscode Fortsetzung zu x^2 (daher 256 Möglichkeiten Einrichtungscode je Fachbereich)
- x^4 : 0x0 - 0xD Netztyp (z.B. Server, Labor, Desktop-PC, Notebook, PC-Pool ...)
- 64 Bit interface ID in modified EUI-64 Format (RFC 4291, RFC 4941) das 7. Bit (2. Bit des 2. Byte) invertiert (1→ 0 et versus) aus 0000 0000 (0x00) wird bspw. 0000 0010 (0x02) ff:fe padding

IPv6 Adressen

- hexadezimal Blöcke zu je zwei Bytes
- führende Nullen in einzelnen Blöcken müssen weggelassen werden
- max Anzahl aufeinander folgender Null-Blöcke durch "::" ersetzen
- Abkürzung "::" nicht für einzelnes Feld, hier: "0"
Notation für 2001:db8:0000:0056:0000:abcd:ef12:1234/64 nicht 2001:db8::56/64 sondern 2001:db8:0:56::/64
- sämtliche Buchstaben als Kleinbuchstaben
- Scope neben Hop-Limit (IPv4: TTL)
- Eintrag bei div. Diensten (bspw. apache2): [IPv6]:\$PORT
- Adress Typen:
 - Unicast: node ↔ node
 - Multicast: node → node-group (eigener Adressbereich)
 - Anycast: node → node-group (Teil des Unicast Adressbereiches, bsp. alle Router)

IPv6 Adressen

- global unicast: 2000::- link local: fe80 - febf (fe80::- unique local: fc00 - fdf (fc00::- multicast: ff00::- \$x = 0-/R-/P-/T-Flag (RFC 3956/RFC 3306/RFC 4291)
- \$y = scope, man unterscheidet hier:
 - global scope
 - \$y = e - im gesamten IPv6 Internet (aka Internet6) gültig
 - local scope
 - \$y = 1 - interface local (nur auf Interface)
 - \$y = 2 - link local (nur im VLAN)
 - \$y = 4 - admin local (Grenzen auf Router definiert)
 - \$y = 5 - site local (nur noch Multicast, administrativ auf Router)
 - \$y = 8 - organisation local (nur Multicast)

IPv6 Adressen

- global unicast: 2000::- link local: fe80 - febf (fe80::- unique local: fc00 - fdf (fc00::- multicast: ff00::- \$x = 0-/R-/P-/T-Flag (RFC 3956/RFC 3306/RFC 4291)
- \$y = scope, man unterscheidet hier:
 - global scope
 - \$y = e - im gesamten IPv6 Internet (aka Internet6) gültig
 - local scope
 - \$y = 1 - interface local (nur auf Interface)
 - \$y = 2 - link local (nur im VLAN)
 - \$y = 4 - admin local (Grenzen auf Router definiert)
 - \$y = 5 - site local (nur noch Multicast, administrativ auf Router)
 - \$y = 8 - organisation local (nur Multicast)

IPv6 Adressen

- global unicast: 2000::- link local: fe80 - febf (fe80::- unique local: fc00 - fdf (fc00::- multicast: ff00::- \$x = 0-/R-/P-/T-Flag (RFC 3956/RFC 3306/RFC 4291)
- \$y = scope, man unterscheidet hier:
 - global scope
 - \$y = e - im gesamten IPv6 Internet (aka Internet6) gültig
 - local scope
 - \$y = 1 - interface local (nur auf Interface)
 - \$y = 2 - link local (nur im VLAN)
 - \$y = 4 - admin local (Grenzen auf Router definiert)
 - \$y = 5 - site local (nur noch Multicast, administrativ auf Router)
 - \$y = 8 - organisation local (nur Multicast)

IPv6 Adressen

"well known" Multicast Adressen siehe auch

<http://www.iana.org/assignments/ipv6-multicast-addresses>

- scope: interface local
 - ff01::1 all-nodes
 - ff01::2 all-routers
- scope: link-local
 - ff02::1 all-nodes
 - ff02::2 all-routers
 - ff02::b all-mobile-agents
- scope: site local
 - ff05::2 all-routers
 - ff05::1:3 all-dhcp-server

IPv6 Adressen

"well known" Multicast Adressen siehe auch

<http://www.iana.org/assignments/ipv6-multicast-addresses>

- scope: interface local
 - ff01::1 all-nodes
 - ff01::2 all-routers
- scope: link-local
 - ff02::1 all-nodes
 - ff02::2 all-routers
 - ff02::b all-mobile-agents
- scope: site local
 - ff05::2 all-routers
 - ff05::1:3 all-dhcp-server

IPv6 Adressen

”well known” Multicast Adressen siehe auch

<http://www.iana.org/assignments/ipv6-multicast-addresses>

- scope: interface local
 - ff01::1 all-nodes
 - ff01::2 all-routers
- scope: link-local
 - ff02::1 all-nodes
 - ff02::2 all-routers
 - ff02::b all-mobile-agents
- scope: site local
 - ff05::2 all-routers
 - ff05::1:3 all-dhcp-server

IPv6 Adressen

- ff0?::fb alle Multicast-DNS-Server (? muss durch scope ersetzt werden)
ff0?::101 alle NTP-Server (? muss durch scope ersetzt werden)
- solicited-node multicast (SNM)
jede node tritt dieser Gruppe bei, u.a. verwendet bei NDP (RFC 4291)
ff02:0:0:0:0:1:ff00::/104 + host ID der MAC, z.B.
MAC Adr: 00:02:B3:1E:83:29
SNM: ff02::1:ff1e:8329
LL Adr: ff80::2002:b3ff:fe1e:8329

IPv6 Adressen

- ff0?::fb alle Multicast-DNS-Server (? muss durch scope ersetzt werden)
ff0?::101 alle NTP-Server (? muss durch scope ersetzt werden)
- solicited-node multicast (SNM)
jede node tritt dieser Gruppe bei, u.a. verwendet bei NDP (RFC 4291)
ff02:0:0:0:0:1:ff00::/104 + host ID der MAC, z.B.
MAC Adr: 00:02:B3:1E:83:29
SNM: ff02::1:ff1e:8329
LL Adr: ff80::2002:b3ff:fe1e:8329

ICMP6

- **echo request** (Typ 128) / **echo response** (Typ 129)
Erreichbarkeit von node
- **router solicitation** (Typ 133)
node kann Router-Infos anfordern
- **router advertisement** (Typ 134)
router publiziert Existenz sowie verschiedene Parameter (auf router solicitation oder in regelm. Abständen)
- **neighbor solicitation** (Typ 135)
Anfrage nach Link-Layer Adresse des Nachbarn, oder Duplicate Address Detection
- **neighbor advertisement** (Typ 136)
bzw. **unsolicited neighbor advertisement**
node publiziert Anwesenheit auf Anfrage oder selbständig
- Parameter des Übertragungsweges
Path MTU Discovery

ICMP6

- Neighbor Discovery Options (laut RFC 2461)
 - Typ 01 = source link-layer address
 - Typ 02 = target link-layer address
 - Typ 03 = prefix information
 - Typ 04 = redirect header
 - Typ 05 = MTU
- Inverse Neighbor Discovery (IND)
 - Erweiterung von NDP, definiert in RFC 3122
 - IND solicitation - und IND advertisement Nachrichten
 - ähnlich wie RARP
 - Optionen wie NDP zzgl.
 - Typ 09 = source address list
 - Typ 10 = target address list
- Multicast Listener Discovery, Multicast Router Discovery

<https://www.iana.org/assignments/icmpv6-parameters>

ICMP6

- Neighbor Discovery Options (laut RFC 2461)
 - Typ 01 = source link-layer address
 - Typ 02 = target link-layer address
 - Typ 03 = prefix information
 - Typ 04 = redirect header
 - Typ 05 = MTU
- Inverse Neighbor Discovery (IND)
 - Erweiterung von NDP, definiert in RFC 3122
 - IND solicitation - und IND advertisement Nachrichten
 - ähnlich wie RARP
 - Optionen wie NDP zzgl.
 - Typ 09 = source address list
 - Typ 10 = target address list
- Multicast Listener Discovery, Multicast Router Discovery

<https://www.iana.org/assignments/icmpv6-parameters>

ICMP6

- Neighbor Discovery Options (laut RFC 2461)
 - Typ 01 = source link-layer address
 - Typ 02 = target link-layer address
 - Typ 03 = prefix information
 - Typ 04 = redirect header
 - Typ 05 = MTU
- Inverse Neighbor Discovery (IND)
 - Erweiterung von NDP, definiert in RFC 3122
 - IND solicitation - und IND advertisement Nachrichten
 - ähnlich wie RARP
 - Optionen wie NDP zzgl.
 - Typ 09 = source address list
 - Typ 10 = target address list
- Multicast Listener Discovery, Multicast Router Discovery

<https://www.iana.org/assignments/icmpv6-parameters>

IPv6-Netz

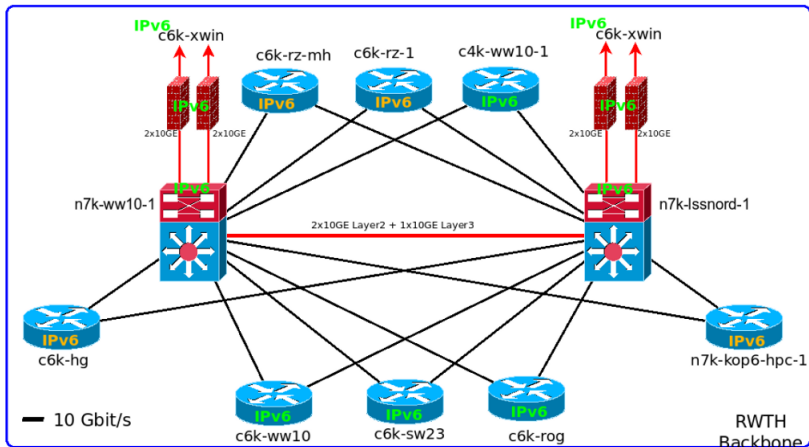


Abbildung: RWTH IPv6 Backbone

Erfahrungsbericht

- ndpmon: <http://ndpmon.sourceforge.net/>
- ndpmon - webinterface:
http://ndpmon.sourceforge.net/web_interface.html
- NDPWatch: <http://ndpwatch.sourceforge.net/>
- Nield: <http://nield.sourceforge.net/index.html>

Linux IPv6 Kommandos

```
$ ip -6 addr show dev eth0
$ ip -6 addr show dev eth0 scope link
# ip -6 addr add 2001:638:410:1230:ID/64 dev eth0

$ ip -6 route show
$ route -A inet6 oder route -6

# ip route add to blackhole 2a02:2e0:3fe:100::6 \
  dev eth0
# ip route del 2a02:2e0:3fe:100::6
# ip -f inet6 route list

$ ip -6 neigh show

$ netstat -6tulpen
$ netstat -6 -g
```

Linux IPv6 Kommandos

```
$ ping6 -I eth0 ff02::1
```

```
$ ping6 ff02::1%eth0
```

```
$ tracepath6 six.heise.de          # mit MTU
```

```
$ traceroute6 six.heise.de
```

```
$ host -t AAAA six.heise.de 134.130.4.1
```

```
$ nslookup -type=AAAA six.heise.de 134.130.4.1
```

```
$ nslookup nslookup 2a02:2e0:3fe:100::6 134.130.4.1
```

```
$ ssh -6 ::1
```

```
$ nc -6 ::1 25
```

```
$ tcpdump -i eth0 -vv -n ip6 or proto ip6
```

```
$ nmap -6 ::1    # nmap 6.X full IPv6 Support
```

Packetfilter

- iptables/netfilter neue match extension:
 - `dst` Optionen im IPv6 Destination Header prüfen
 - `eui64` EUI64 Teil der IPv6 (SLAAC) Adresse prüfen
 - `frag` Optionen im IPv6 Fragmentation Header prüfen
 - `hbh` Optionen im IPv6 Hob-by-Hop Header prüfen
 - `hl` Option im IPv6 Hop-Limit Header prüfen
 - `ipv6header` Optionen im IPv6 Header prüfen (Next Header)
 - `mh` Optionen im IPv6 Mobility-Header prüfen
 - `rt` Optionen im IPv6 Routing Header prüfen
- Transient Addressing for Related Processes (TARP),
Zusammenfassung von Diensten anhand der "process group", mehrere IPv6 Adressen je link/host, Ziel: einfachere Filterregeln
<http://www.cs.columbia.edu/~smb/papers/tarp.pdf>

Sicherheit/Privatsphäre

- DNSSEC (RFC 4033, 4034 und 4035)
- SEND (RFC 3971)
<https://code.google.com/p/ipv6-send-cga/>
- IPsec (u.a. RFC 4301, 4302 und 4303)
- Cryptographically Generated Address (CGA, RFC 3972)
- IPv6 privacy extension

Referenzen

- Hagen, Silvia: IPv6 Essentials, 2nd Edition, Sebastopol CA 95472, 2006
[ISBN: 978-0-596-10058-2]
- Murphy, N.R. & Malone, D.: IPv6, Network Administration, Sebastopol CA 95472, 2005
[ISBN: 978-0-596-00934-2]
- Hogg, S. & Vyncke, E.: IPv6 Security, Indianapolis IN 46240, 2009
[ISBN: 978-1-58705-594-2]
- Bieringer, Peter: Linux IPv6 HOWTO, Version, 2011
[Online] Verfügbar unter
<http://mirrors.bieringer.de/Linux+IPv6-HOWTO-de/>

Referenzen

- Frankel S. et al.: NIST - Guidelines for the Secure Deployment of IPv6, 2010
[Online] Verfügbar unter http://www.nist.gov/itl/csd/ipv6_010511.cfm
- Ziring, Neal: Router Security Configuration Guide Supplement - Security for IPv6 Routers, 2006
[Online] Verfügbar unter http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/cisco_router_guides.shtml
- Anrath, W. et al.: IPv6 im lokalen Netz - Gefahren und Lösungen, 2011
[Online] Verfügbar unter <http://www2.fz-juelich.de/jsc/files/docs/ib/ib-11/ib-2011-07.pdf>

Referenzen

- Anrath, W. et al.: IPv6 Privacy Extensions - Alptraum im Enterprise LAN, 2011
[Online] Verfügbar unter <http://www2.fz-juelich.de/jsc/files/docs/ib/ib-11/ib-2011-08.pdf>
- McGann, Orla: IPv6 Packet Filtering. MSc Thesis, Hamilton Institute, NUI Maynooth, Ireland 2005
[Online] Verfügbar unter http://www.hamilton.ie/publications/orla_mcgann_thesis.pdf
- RFC 4864 - Van de Velde, G. et al.: Local Network Protection for IPv6
[Online] Verfügbar unter <https://tools.ietf.org/rfc/rfc4864.txt>
- RFC 4890 - Davies, E. & Mohacsi, J.: Recommendations for Filtering ICMPv6 Messages in Firewalls, 2007
[Online] Verfügbar unter <https://www.rfc-editor.org/rfc/rfc4890.txt>

Referenzen

- RFC 4942 - Davies, E. et al.: IPv6 Transition/Coexistence Security Considerations
[Online] Verfügbar unter <https://tools.ietf.org/rfc/rfc4942.txt>
- RFC 5157 - Chown, T.: IPv6 Implications for Network Scanning, 2008
[Online] Verfügbar unter <https://www.ietf.org/rfc/rfc5157.txt>
- RFC draft - Gont, F.: Host Scanning in IPv6 Networks, 2012
[Online] Verfügbar unter <https://tools.ietf.org/id/draft-gont-opsec-ipv6-host-scanning-00.txt>
- RFC draft - Gont, F.: Security Implications of IPv6 in IPv4 networks, 2012
[Online] Verfügbar unter <https://tools.ietf.org/id/draft-gont-opsec-ipv6-implications-on-ipv4-nets-00.txt>
- RFC draft - Gont, F.: Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)
[Online] Verfügbar unter <https://tools.ietf.org/id/draft-ietf-v6ops-ra-guard-implementation-04.txt>

Referenzen

- RFC draft - Gont, F.: Neighbor Discovery Shield (ND-Shield): Protecting against Neighbor Discovery Attacks
[Online] Verfügbar unter <https://tools.ietf.org/html/draft-gont-opsec-ipv6-nd-shield-00>
- RFC draft - Gont, F.: DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers
[Online] Verfügbar unter <https://tools.ietf.org/html/draft-gont-opsec-dhcpv6-shield-00>
- http://www.rfc-editor.org/cgi-bin/rfcsearch.pl?searchwords=ipv6&num=1500&filefmt=txt&opt=Keywords&sort_method=newer
- Leitlinien IPv6 und Datenschutz (2012), siehe http://www.ipv6council.de/documents/leitlinien_ipv6_und_datenschutz.html

Referenzen

- Internet Protocol Version 6 (IPv6) Basics cheat sheet:
http://www.roesen.org/files/ipv6_cheat_sheet.pdf
- IPv6:
<http://packetlife.net/media/library/8/IPv6.pdf>
- IPv6 Cheat Sheet:
<http://www.estoile.com/links/ipv6.pdf>
- shim6
IETF drafts <http://www.tm.uni-karlsruhe.de/doc/i-d/shim6/>
bzw. http://inl.info.ucl.ac.be/system/files/main_1.pdf
oder <http://www.sciencedirect.com/science/article/pii/S0140366411000995>,
<http://www.linux-ipv6.org/ml/usagi-users/msg03700.html>