

Sicherheitsaspekte bei der Einführung von IPv6



André Beck
IBH IT-Service GmbH
Gostritzer Str. 67a
01217 Dresden
<http://www.ibh.de/>
support@ibh.de

www.ibh.de

Inhalt

- ◆ IPv6 Primer
- ◆ 2011: Das Jahr von IPv6?
- ◆ Sicherheitsaspekte

Geschichte

◆ Classful IPv4 skaliert nicht

- Bereits Mitte der 1980er wurde die Problematik klar
- Vergeudung von IPv4-Adressen reduzieren
 - 1985: Subnetting (RFC950)
 - 1987: VLSM (Variable Length Subnet Masks)
 - 1993: CIDR (Classless InterDomain Routing)
- Address Space Conservation
 - Zunehmend striktere Regeln seit Mitte der 1990er
 - Ende der Adressvergabe trotzdem absehbar
 - 2011-02-03: IANA IPv4 Adressraum erschöpft
 - 2011-04-15: APNIC IPv4 Adressraum erschöpft
 - Generelles Ende bei allen RIRs noch 2011 erwartet

Was tun?

◆ Ein neues Protokoll muss her

- Entwicklung seit den frühen 1990ern
 - 1992: Erste Vorschläge, IETF Call for White Papers
 - 1993: IETF ad-hoc IPng Area
 - 1994: IETF IPng Working Group
 - 1996: Erste RFCs (RFC1883 etc)
- Designziele
 - Praktisch unerschöpflicher Adressraum
 - Optimiertes Paketformat (effizientes Routing)
 - Rückerobern des End-to-End-Prinzips (statt NAT)
 - Beseitigen diverser Designfehler von IPv4

IPv6 Primer

Paketformat

◆ Konservative Änderung an IPv4

● Vereinfachungen

- Header fester Größe
- Extension Header bei Bedarf (behandelt wie Payload)
 - ◆ Weniger wichtige Felder nur in Extension Headers
- TTL ist reiner Zähler (Hop Limit)
- Keine Header-Checksumme
- Keine Fragmentierung durch Router
 - ◆ Nur beim Absender mittels PMTUD

● Erweiterungen

- Neues Adressformat mit 128 Bit Länge
- Flow Label
- IPsec-Unterstützung vorgeschrieben (über Extension Header)

IPv6 Primer

Adressen 1

- ◆ Vierfache Länge gegenüber IPv4
 - Adressraum von 2^{128} entspricht ca. 3.4×10^{38} Adressen
 - Geeignete Schreibweise nötig
 - 8 Gruppen zu 16 Bit Hexadezimal
 - Trennung der Gruppen durch Doppelpunkt
 - ◆ 2001:0db8:0000:0000:0000:0000:dead:beef
 - Clevere Abkürzungsregeln (kanonisches Format)
 - ◆ Führende Nullen in einer Gruppe eliminieren
→ 2001:db8:0:0:0:0:dead:beef
 - ◆ Längste (bzw. erste gleichlange) Kette von Null-Gruppen durch :: ersetzen
→ 2001:db8::dead:beef
 - Netze immer in CIDR-Notation, z.B. 2001:db8::/32
 - Enorme Größe primär aus Strukturgründen
 - Spezielle Adressklassen
 - Hierarchische Aggregation

IPv6 Primer

Adressen 2

◆ Adressklassen

- Unicast

- Individuelle Adresse eines Interface

- Multicast

- Gruppen von Interfaces
- IPv6 kennt kein Broadcast (aber all-nodes Link Local Multicast)

- Anycast

- Gleiche Unicast-Adresse an mehreren Interfaces (und Nodes)

◆ Scopes

- Klares Design des Scopings (gegenüber IPv4)

- Interface Local, Link Local
- Admin Local, Site Local, Organization Local
- Global

IPv6 Primer

Adressformate 1

◆ Unicast

● Global Unicast & Anycast

■ 64 Bit Network Prefix

◆ Beliebig weiter strukturierbar (CIDR)

◆ Kanonisch ≥ 48 Bit Routing Prefix und ≤ 16 Bit Subnet ID

■ 64 Bit Interface Identifier

◆ Nicht strukturierbar (kein weiteres Subnetting!)

◆ Belegung folgt Modified EUI-64

■ Momentan „nur“ 2000:: $/3$ alloziert

● Link Local Unicast

■ Präfix fe80:: $/10$ und 64 Bit Interface Identifier (s.o.)

■ Nicht routbar, ähnlich IPv4 APIPA (169.254.0.0/16)

IPv6 Primer

Adressformate 2

◆ Multicast

● General Multicast Address Format

- Präfix ff00::/8
- 4 Bit Flags
- 4 Bit Scope
- 112 Bit Group ID

● Spezielle Multicast Adressformate

- Solicited-Node Multicast Address
 - ◆ 24 Bit der Unicast-Adresse eines Node in die Multicast-Adresse kopiert
 - ◆ Optimierung zur Vermeidung von Quasi-Broadcasts z.B. in ICMPv6
- Unicast-Prefix based Multicast Address
- Link-scoped Multicast Address
 - ◆ Für serverfreie automatische Discovery-Protokolle etc.

IPv6 Primer

Spezielle Adressen und Allokationen

- ◆ `::/128` Unspecified Address
- ◆ `::/0` Default Route
- ◆ `::1/128` Loopback
- ◆ `::ffff:0:0/96` IPv4-mapped IPv6 (Socket API)
- ◆ `::ffff:0:0:0/96` IPv4-translated IPv6 (SIIT)
- ◆ `64:ff9b::/96` IPv4-embedded IPv6 (Well known prefix)
- ◆ `2000::/3` Global Unicast Allocation
 - `2001::/32` Teredo Tunneling
 - `2001:2::/48` Benchmarking
 - `2001:10::/28` ORCHID (Kryptografische Hashes)
 - `2001:db8::/32` Documentation
 - `2002::/16` 6to4 Tunneling
- ◆ `fc00::/7` Unique Local (ähnlich RFC1918)
- ◆ `fe80::/10` Link Local
- ◆ `ff00::/8` Multicast
 - `ff02::1` Link Local All-Nodes Multicast

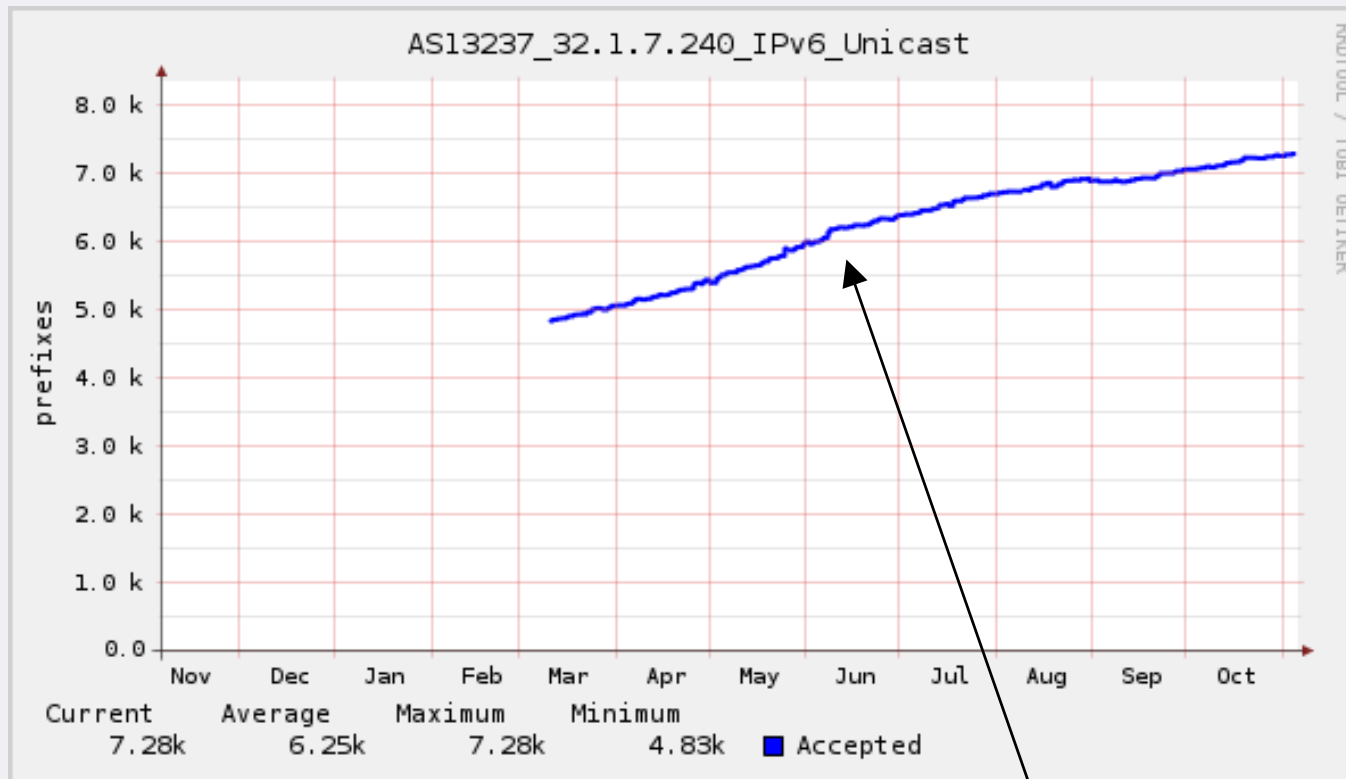
Aktueller Stand 2011

Das Jahr von IPv6?

- ◆ IPv4 Adressraum erschöpft
 - 2011-02-03: IANA vergibt letzte fünf /8 an RIRs
 - 2011-04-15: APNIC vergibt letzte Adressen an LIRs
 - Generelles Ende bei allen RIRs noch 2011 erwartet
- ◆ 2011-06-08: World IPv6 Day
 - Zahlreiche Betreiber testen IPv6 Dual-Stack (z.B. Google)
 - Erfolg: Manche Teilnehmer lassen es aktiv
- ◆ 15 Jahre IPv6
 - Protokollfamilie stabilisiert sich zunehmend
 - IBH beantragt LIR Allocation zum 15. Geburtstag ;-)
 - Seitdem Präfixanzahl in der DFZ um 50% gestiegen
 - Traffic bescheiden (Promille von IPv4, kein klarer Zuwachs)
 - Kundeninteresse noch verhalten
 - Große Endkunden-ISPs (z.B. T-Online) planen Pilot noch 2011

Aktueller Stand 2011

IPv6-Präfixzuwachs in der DFZ



World IPv6 Day

Sicherheitsaspekte

Grobe Klassifizierung von Sicherheit

◆ Security

- Direkte Bedrohung sicherheitsrelevanter Daten/Systeme
- Datensicherheit
- z.B. Root Compromise, Remote Code Execution

◆ Privacy

- Verletzung von Privatsphäre und Vertraulichkeit
- Datenschutz
- z.B. Informationsleck bei Dienstanbieter

◆ Safety

- Störung der Betriebssicherheit und Verfügbarkeit
- z.B. Auswirkung des Anschluss eines fehlerkonfigurierten Endgeräts
- Jedes derartige Problem ist eine schlummernde DoS-Attacke!

Sicherheitsaspekte

Die Erwartungshaltung

◆ Vorbelastung

- Mehr als 20 Jahre Erfahrung mit IPv4
 - Jahrzehnte an Tuning von Paradigmen und Implementationen
 - Evolutionäres Modell mit Millionen Individuen
 - Hoher, ständig wachsender Selektionsdruck
 - Gefestigte Bedrohungsmodelle und Gegenmaßnahmen
 - Trotzdem immer wieder „böse Überraschungen“
- Nutzer, Administratoren und Betreiber betroffen

◆ Erwartungen

- „IPv6 ist die neue Version von IPv4“
 - Funktionale Parität
 - Vergleichbare Sicherheit und Wartbarkeit

Die Realität

◆ Designparadigmen

- Zero Configuration
 - Automatismen zur Adresskonfiguration
 - Automatismen zum Auffinden von Nachbarn
 - Automatismen zum Auffinden geeigneter Router
- End to End
 - NAT ist hässlich
 - NAT diene nur der IPv4 Address Space Conservation
 - IPv6 hat mehr als genug Adressen für Alles und Jeden
- Vereinfachung und Optimierung
- IPsec als Allzweckwaffe in Sicherheitsfragen

◆ Lernbedarf

- Auch wir stehen noch am Anfang –
20 Jahre Praxis sind durch nichts zu ersetzen
- A Work in Progress – das Folgende ist noch etwas unstrukturiert

Sicherheitsaspekte

Typische Trust Models

◆ All Nodes Trusted

- Stringent zentral administriertes Intranet
- z.B. Enterprise LAN
- Greift aus heutiger Sicht kaum noch
 - Physikalische Zugangssicherheit
 - Gesicherter Link Layer (802.1X, 802.11i)

◆ Trusted Router

- Übergabenetz eines Betreibers (Internet, Intranet)
- Alle Teilnehmer außer dem Router sind suspekt

◆ Trust No One

- Ad-hoc IPv6 Network

Sicherheitsaspekte

Neighbor Discovery (ND)

- ◆ Zentraler Automatismus in IPv6
 - Basiert vollständig auf ICMPv6 (kein Zusatzprotokoll wie ARP)
 - Nutzt ausgiebig Multicasts und Link Local Addressing
- ◆ Dient mehreren Zwecken
 - Neighbor Address Resolution (ersetzt ARP)
 - Neighbor Unreachability Detection (NUD)
 - Router Discovery (RD)
 - Auffinden von On-Link Prefixes und Default Routern
 - Redirect
 - Optimierung bei mehreren On-Link Prefixes
 - Stateless Address Auto Configuration (SLAAC)
 - DHCPv6 ist optional und kann über ND vermittelt werden
 - Duplicate Address Detection (DAD)

Sicherheitsaspekte

ND Threats (RFC3751)

- Neighbor Solicitation/Advertisement Spoofing
 - Redirect/DoS, ähnlich IPv4 ARP-Spoofing
- Neighbor Unreachability Detection (NUD) DoS
- Duplicate Address Detection DoS
- Malicious Last Hop Router
 - Redirect/DoS, Angreifer sendet plausible RAs
- Default Router Kill DoS
 - Kein Default Router → All Destinations On-Link! (RFC2461 5.2)
 - Indirektes Redirect, Angreifer stört Default Router um RD zu gewinnen
- Router Compromise (Redirect/DoS)
- Spoofed Redirect Message (Redirect/DoS)
- Bogus On-Link Prefix (Redirect/DoS)
 - Angreifer erklärt einen Prefix mit RA als On-Link
- Bogus Address Configuration Prefix
 - Angreifer erlaubt Prefix mit RA für SLAAC, Endsysteme konfigurieren ihn (DNS!)
- Parameter Spoofing DoS
- Replay attacks
- Neighbor Discovery DoS

Sicherheitsaspekte

ND Mitigations

- ◆ Angreifbarer Automatismus
 - Check auf HopLimit=255 verhindert immerhin Remote-Angriffe
 - Standardmäßig nicht authentisiert
 - RFC2461 schlägt IPsec (AH) vor
 - Geht nicht ins Detail
 - Key Management ungeklärt (manuell, für 2^{24} Multicastgruppen!)
 - Passt nur ins All Nodes Trusted Model – Abschalten?
- ◆ SEcure Neighbor Discovery (SEND, RFC3971)
 - Skalierbare kryptografische Sicherung von ND
 - Momentan noch kaum verbreitet
- ◆ First Hop Security
 - Gegenmaßnahmen auf dem Access Switch
 - Analog IPv4 DAI + DHCP Snooping + IP Source Guard
 - ND Inspection + IPv6 Source Guard? Kaum Hardware!
 - Mindestens RAs und DHCPv6 vom Access Layer per ACL filtern
 - ipv6 nd rguard

Sicherheitsaspekte

SLAAC

◆ Ziele

- Ad-Hoc-Netze ohne jegliche manuelle Konfiguration
- DHCPv6 auch in großen Netzen nicht zwingend
- Graceful Renumbering zu einem neuen Präfix

◆ Ablauf

- Interface erzeugt und aktiviert Link Local Address (nach DAD)
- Interface tritt Multicast-Gruppen bei (All Nodes und Solicited Node)
- Interface wartet auf RA oder sendet Router Solicitation
- RA enthält Global Prefix mit geeigneten Flags/Timern
- Host erzeugt Adresse aus Prefix und Interface Identifier
 - Interface Identifier basiert auf Modified EUI-64
- Host fügt die neue Adresse dem Interface hinzu (nach DAD)
- Host entfernt Adressen nach Ablauf ihrer Timer

◆ Fundamental anders als IPv4

- Mehrere IP-Netze auf eine Broadcastdomain, Kurzschlüsse...

Sicherheitsaspekte

Modified EUI-64

◆ Ziele

- Unique Interface ID aus MAC-Adresse des Interface
- Optional manuelle Konfiguration statt MAC möglich
- Kompakte Schreibweise bei manueller Vergabe

◆ Vorgehensweise

- Ausgangspunkt 48 Bit MAC, z.B. 00:23:14:57:9c:8c
- Einfügen ff:fe in der Mitte → 00:23:14:ff:fe:57:9c:8c
- Invertieren des Universal/Local Bits → 02:23:14:ff:fe:57:9c:8c
- Beispiel Link Local Address: fe80::223:14ff:fe57:9c8c

◆ Warum „Modified“ (Invertieren des U/L-Bits)?

- Manuelle Vergabe bedeutet Local, d.h. in EUI-64 U/L=1
- Durch die Invertierung bedeutet Local U/L=0
→ 2001:db8::1 statt 2001:db8::200:0:0:1 (Manuelle Vergabe)

Sicherheitsaspekte

Modified EUI-64 vs. Privacy

◆ End to End Principle

- Status Quo ist dynamische temporäre Adressvergabe
- User Tracking erfordert derzeit beträchtlichen Aufwand
- End to End + Modified EUI-64 unterläuft den Status Quo komplett
- Starker Gegenwind (33. Internationale Datenschutzkonferenz)

◆ Bedingt hilfreich: RFC4941

- Privacy Extensions for SLAAC in IPv6
- Randomisierte Interface IDs
- Standard unter Windows seit Vista
- Linux, BSDs, MacOS: `sysctl use_tempaddr`

◆ Stabiler Präfix?

- Verfügbarer Adressraum erlaubt wieder statische Konfiguration
- Nutzer an seinem /56 erkennbar → Dynamische Präfixe?

Beispiel: RFC 4941 und Debian GNU/Linux

```
/etc/network/interfaces:  
[...]  
iface wlan0 inet manual  
        up sysctl -w net.ipv6.conf.${IFACE}.use_tempaddr=2  
[...]
```

```
# ip -6 addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qlen 1000  
    inet6 2a01:7700:0:4001:29f4:b979:52b5:cada/64 scope global temporary dynamic  
        valid_lft 85765sec preferred_lft 13765sec  
    inet6 2a01:7700:0:4001:8544:8f22:a67d:35e7/64 scope global temporary deprecated dynamic  
        valid_lft 71691sec preferred_lft 0sec  
    inet6 2a01:7700:0:4001:34d8:df4a:a71:318f/64 scope global temporary deprecated dynamic  
        valid_lft 57485sec preferred_lft 0sec  
    inet6 2a01:7700:0:4001:ble4:c4dd:1c07:51a8/64 scope global temporary deprecated dynamic  
        valid_lft 43294sec preferred_lft 0sec  
    inet6 2a01:7700:0:4001:bc0b:d7a1:dd1e:8acb/64 scope global temporary deprecated dynamic  
        valid_lft 28957sec preferred_lft 0sec  
    inet6 2a01:7700:0:4001:223:14ff:fe57:9c8c/64 scope global dynamic  
        valid_lft 86315sec preferred_lft 14315sec  
    inet6 fe80::223:14ff:fe57:9c8c/64 scope link  
        valid_lft forever preferred_lft forever
```

IPv4 to IPv6 Transition Issues

◆ Voraussichtlich langer Dual Stack Betrieb

● Übergangsphase wird (weitere) Jahrzehnte dauern

- Hosts bekommen nach und nach zusätzlich IPv6
- IPv4 und IPv6 funktionieren parallel
- Immer mehr IPv6-Only Dienste und Endsysteme tauchen auf
- IPv4 wird bedeutungslos und verschwindet langsam

● Dual Stack Issues

- Unerwartete Priorisierung von IPv6 wenn vorhanden
- DNS AAAA hat Vorrang vor A – das World IPv6 Day Problem
- DNS Reverse → Double Reverse → Bevorzugter Dienst IPv6!
- Security: Eine (IPv4-)Firewall ist nicht implizit eine IPv6-Firewall
- SLAAC + RD + kein IPv6-Filter → man ist schnell exponiert
- RIPE: Grundrauschen im IPv6 z.Z. minimal (aber wie lange?)

Sicherheitsaspekte

Unexpected Tunneling

◆ Transitionsmechanismen

- 6to4 Tunneling (IETF)
 - IPv6 in IPv4 (Protocol 41)
- Teredo (Microsoft)
 - Aka Shipworm (*Teredo navalis*)
 - Durchbohrt NAT (mit 3544/udp)
- ISATAP (Boeing/Cisco/Microsoft)

◆ Durchbrechen Sicherheitsannahmen von IPv4

- Speziell Teredo: Hosts hinter NAT sind exponiert

◆ Windows ab Vista

- Teredo ist standardmäßig aktiv
- Nur für reine IPv6-Ziele (AAAA only, weitere Limits)
- Test: ping -6 www.six.heise.de

Vermischtes 1

◆ Syntaktisches

- IPv6-Adressen haben mehr Zeichen
- IPv6-Adressen enthalten Doppelpunkte
 - Zwischenzeitlich in URLs für Portangaben benutzt
 - IPv6-Adressen in URLs in [] einschließen
 - `http://[2001:db8:815:4711::1]:8080/`
- Link Local Zone Identifiers
 - Link Local Adressen mehrdeutig auf Multihomed Hosts
 - Zone Identifier (systemabhängig) mit % angehängt
 - `fe80::1%eth0`
- Zahlreiche Probleme zu erwarten
 - Sonderzeichen, Logfiles, Datenbankfelder...

Sicherheitsaspekte

Vermischtes 2

◆ Sicherheitslücken

- CVEs, PSIRTs etc
- IPv6 Routing Header Vulnerability
 - cisco-sa-20070124-IOS-IPv6
 - Type 0 Routing Header (Source Routing)
 - RH0 ist ohnehin deprecated
 - Instant crash...
 - no ipv6 source-route (ab 12.2(15)T)
 - ACL hack
- Fünf IPv6 PSIRT Advisories 2011
 - cisco-sa-20110223-asa
 - cisco-sa-20110907-nexus
 - cisco-sa-20110928-ipv6
 - cisco-sa-20110928-ipv6mpls
 - cisco-sa-20111005-fwsm

Vermischtes 3

◆ Linux sysctl Race Conditions

- Auf mehreren Distributionen beobachtet
 - Systemstart: sysctl-Aufrufe vor Laden des ipv6-Moduls
 - Generell: Inkorrekte Wirkung von Änderungen
 - ◆ net.ipv6.conf.default/all wirken nicht auf Interfaces
 - ◆ Einstellungen lassen sich nicht ändern/werden zurückgesetzt
- Änderungen in die Interface-Konfiguration einbinden
 - sysctl.conf unzuverlässig
 - pre-up oder up Statements benutzen
 - Scripte in /etc/network/if-pre-up.d/ ablegen
 - Konkretes physisches Interface referenzieren (\$IFACE)
 - Details distributionsspezifisch (obiges für Debian)
 - Testen! Insbesondere Reboot!

Linux Server Best Practice

```
# This machine should not participate in SLAAC
sysctl -w net.ipv6.conf.${IFACE}.autoconf=0

# The evil RH0
sysctl -w net.ipv6.conf.${IFACE}.accept_source_route=0

# Not a v6 router, either
sysctl -w net.ipv6.conf.${IFACE}.forwarding=0

# Avoid MITM redirect attacks
sysctl -w net.ipv6.conf.${IFACE}.accept_redirects=0

# Static Address? Avoid DAD DoS (RFC violation)
sysctl -w net.ipv6.conf.${IFACE}.accept_dad=0

# Static Default Router? Disable RD (Caution!)
sysctl -w net.ipv6.conf.${IFACE}.accept_ra=0
sysctl -w net.ipv6.conf.${IFACE}.accept_ra_defrtr=0
```

IOS Feature Set Limitations

◆ IPv6: Mandatory IPsec

- IPsec wird vorausgesetzt
- Beispiel OSPFv3 Auth
 - OSPFv2 MD5 Digest Auth war in OSPF eingebaut
 - OSPFv3 benutzt stattdessen AH
- Ist ein IOS ohne IPsec wirklich IPv6-ready?
 - Upgrades notwendig
 - Planung, Lab-Test, Ticket, Rollout, Ausfall, Seiteneffekte...
 - Bewährte Feature Trains verlassen? (12.2S/SB)

Sicherheitsaspekte

Fazit: Ist 2011 das Jahr von IPv6?

◆ Sicherheitsexperten haben Zweifel

- Thread Model und Mitigation Design 15 Jahre alt
 - Es gab gewisse Änderungen/Erweiterungen
 - Fundamental ähnlich wie IPv4, aber noch komplexer
 - Evolutionärer Schmelztiegel winzig im Vergleich zu IPv4
 - Produkte kommen gerade erst oder fehlen noch
- Und nun?
 - Rollout im LAN abwarten, bis ernsthafte Driver auftauchen
 - Bei der externen Präsenz heute anfangen
 - ◆ z.B. dedizierter IPv6 WWW-Server hinter dedizierter Firewall
 - ◆ Noch nicht Mission Critical, aber Pilot zum Lernen

→ 2011 ist das Jahr zum *vorsichtigen Einstieg* in IPv6

Referenzen & Weiterführendes

Anfangen mit Lesen!

◆ Einstiegspunkte

- <http://en.wikipedia.org/wiki/IPv6>
- c't 16/2011: *Safer Six*

◆ Weiterführendes

- RFC4942:
IPv6 Transition/Coexistence Security Considerations

Vielen Dank!



professional IT-Service

**Fragen Sie!
Wir antworten.**

www.ibh.de