Konstantin Agouros

IPv6 Einführung im Rechenzentrum
SLAC 2011

2.12.2011

Übersicht

- Die Theorie
  - Adressformat
  - Adresszuweisung
  - Was ist anders
- Planung
  - Wer braucht wann v6
  - Mögliche Anschlussszenarien
- Security
- Wer kann v6?
  - Betriebssysteme / Applikationen/ Netzwerkkomponenten / Clients
- Administrative Aspekte
- Praxis

Theorie

Warum IPv6?

- “IPv4 ist alle”
- Large Scale Deployment (Sensoren, Mobilfunk,...)
- Konnektivität mit neuen Diensten
- Manche Dinge werden einfacher

Theorie

Adressformat

- 128bit statt 32bit
  - 232 = 4.294.967.296
  - 2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456
- Darstellung als 32stellige Hex Zahl in vierer Gruppen mit : getrennt
- Eine (oder mehrere) Gruppe aus nur 0 kann ausgelassen werden
- Führende nullen können weggelassen werden
- Beispiele:
  - 2001:0db8:0000:130F:0000:0000:087C:140B
  - 2001:db8:0:130F:0:0:87C:140B
  - 2001:db8:0:130F::87C:140B
- Darstellung Netz (wie bei IPv4 aber mit Weglassen):
  - 2001:db8::/32

Theorie

Adresstypen

- Unicast
  - Adresse ist einer Schnittstelle zugeordnet (Schnittstelle kann mehrere Adressen haben)
  - Für 1 zu 1 Verbindungen
- Multicast
  - Adresse einer Menge von Schnittstellen (logische Mengen)
  - Für 1 zu N Verbindungen
- Anycast
  - Adresse einer Menge von Schnittstellen (logische Mengen)
  - Für 1 zu 1 aus N (der eine ist der “nächste”)
- **Kein Broadcast**
  - Wenn alle Rechner erreicht werden müssen, per funktionaler Multicast Adresse z.B. DHCPv6

Theorie

Adressen

- Scope
  - Link Local (Prefix FE80) nur im angeschlossenen Segment ansprechbar, werden nicht gerouted
  - Global
- Ablaufdatum
  - Damit Umadressierungen automatisch passieren
- Anycast
  - Adresse einer Menge von Schnittstellen (logische Mengen)
  - Für 1 zu 1 aus N (der eine ist der “nächste”)

Theorie

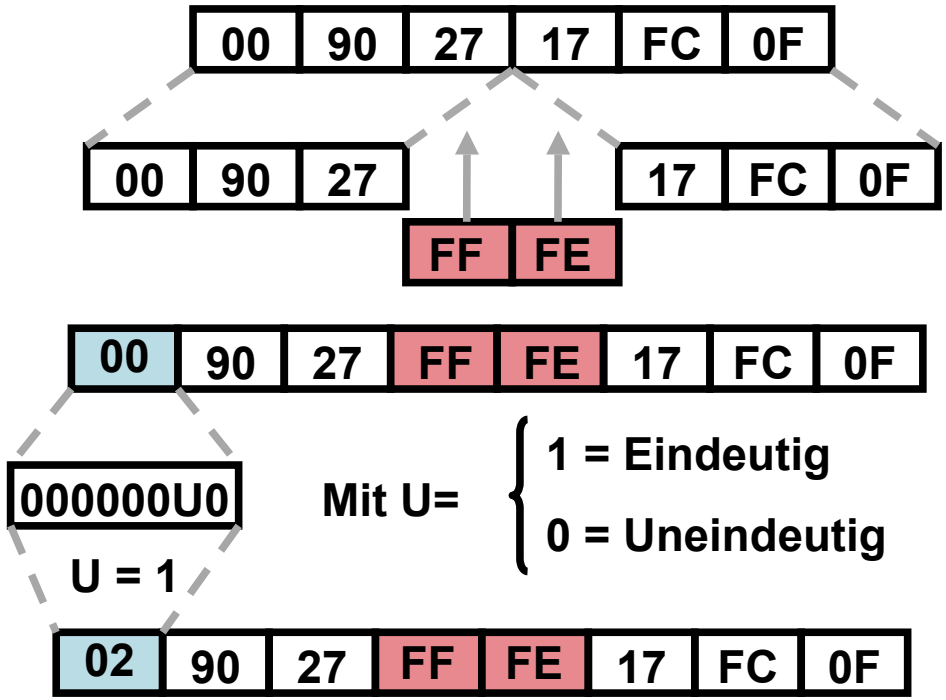
Adressen

- Aufteilung meistens die ersten 64bit für das Netz und die letzten 64 für die Schnittstelle
  - Andere Varianten z.B. für Transfernetze bei manueller Adressierung möglich

Theorie

EUI64 Adresskonfiguration

- 48bit Mac wird in der Mitte geteilt
- FFFE wird eingefügt
- Das erste Byte wird mit einem Indikator für Eindeutigkeit geodert
- Prefix davor
- Oder zufällig generiert (temporary address)



Theorie

Automatische Adresszuweisung

- Stateless vs. Stateful
- Stateless
  - Router Advertisments beinhalten den Prefix für das Lansegment
  - Außerdem beinhalten sie:
    - Flags für das LAN
    - Routen die über den sendenden Router erreichbar sind
    - Per Erweiterung Nameserver
  - Aus Prefix und generierter Adresse wird die zugewiesene Adresse
- Stateful
  - Wenn im RA Autokonfiguration aus und Managed an ist, soll der Client DHCPv6 verwenden
  - Autokonfiguration an + Managed an, IP wie stateless, aber weitere Informationen per DHCP

Neighbor Discovery

- IPv6 hat kein ARP
- Statt dessen ND via ICMPv6 an Multicast

```
▷ Ethernet II, Src: Apple_03:de:fc (10:93:e9:03:de:fc), Dst: IPv6mcast_ff:2e:26:a6 (33:33:ff:2e:26:a6)
▷ Internet Protocol Version 6, Src: 2a01:198:2cc:3:1293:e9ff:fe03:defc (2a01:198:2cc:3:1293:e9ff:fe03:defc), Dst: ff02::1:ff2e:26a6 (ff02::1:ff2e:26a6)
▽ Internet Control Message Protocol v6
    Type: Neighbor Solicitation (135)
    Code: 0
    Checksum: 0xe1cd [correct]
    Reserved: 00000000
    Target Address: 2a01:198:2cc:3:da30:62ff:fe2e:26a6 (2a01:198:2cc:3:da30:62ff:fe2e:26a6)
  ▽ ICMPv6 Option (Source link-layer address : 10:93:e9:03:de:fc)
      Type: Source link-layer address (1)
      Length: 1 (8 bytes)
      Link-layer address: Apple_03:de:fc (10:93:e9:03:de:fc)
```

Theorie

Routing

- Router Discovery
  - Solicitation - Advertisment
  - Client findet damit selber den Weg, wenn ein Router im Netz den Weg kennt und verteilt
- Routing Protokolle
  - OSPFv6
  - BGPv6

Theorie

Unterschiede

- Größere Header
  - MTU für Nutzdaten kleiner
- Größere Pakete möglich
- IP-Extension Headers
- Anycast
- ICMPv6 absolut notwendig

Theorie

Tunnel

- Mehrere Technologien zum Übergang
  - 6in4 - wie 4in4 einfachster Ansatz benötigt zwei entsprechende Endpunkte mit Dualstack, die sich via v4 erreichen (RFC 2893)
  - v6 über GRE (RFC 2473)
  - 6to4 (RFC 3056)
  - ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) (RFC 4214)
  - Teredo über UDP mit Autokonfiguration -> NAT möglich (RFC 4380)
  - MPLS Varianten
- Vorsicht mit der MTU!!!!

Planung

Grundsätzliches

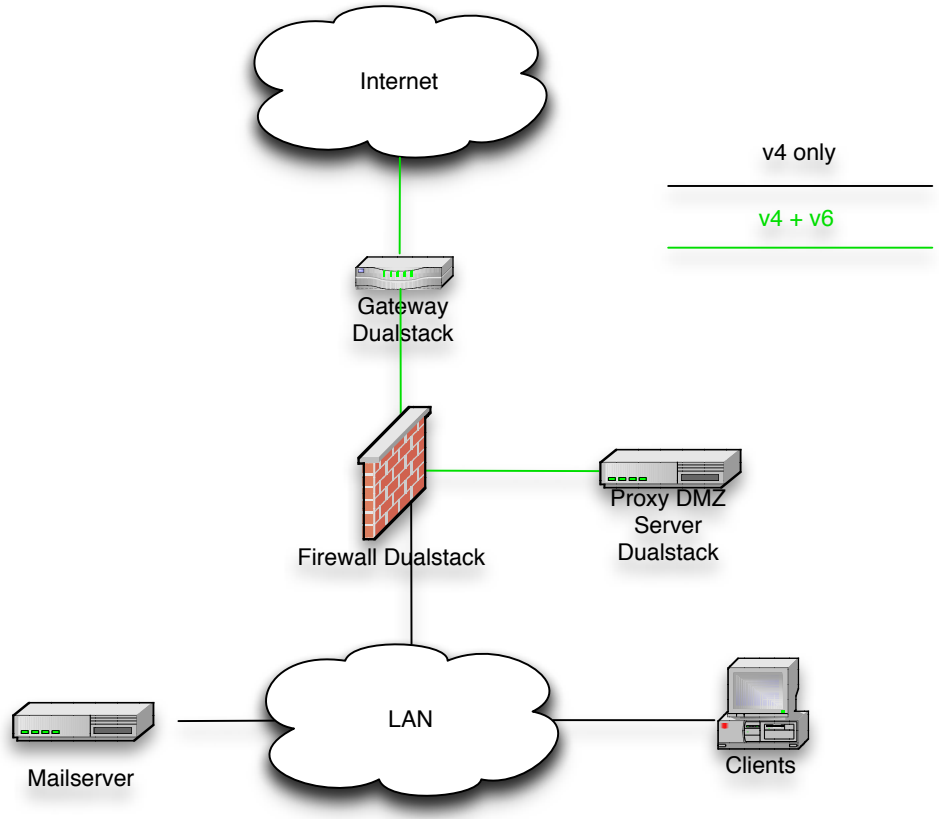
- Wer benötigt v6 (Server / Clients / Dienste)
- Inventur:
  - Betriebssystemversionen
  - Dienste
  - Netzinfrastruktur
    - Router
    - Switche
    - Firewalls
    - VPNs
- Adressplanung
- DNS

Planung

Anschlussszenarien

- v6 Dienste im Internet nutzen
- Notwendig:
  - v6-Anschluss
  - v6 Firewall
  - Dual Stack v6 Server in DMZ mit
    - Mail Server
    - Proxy
    - Webserver
  - DNS Records für Mail und DNS

Anschlussszenarien - v6 Dienste im Internet nutzen

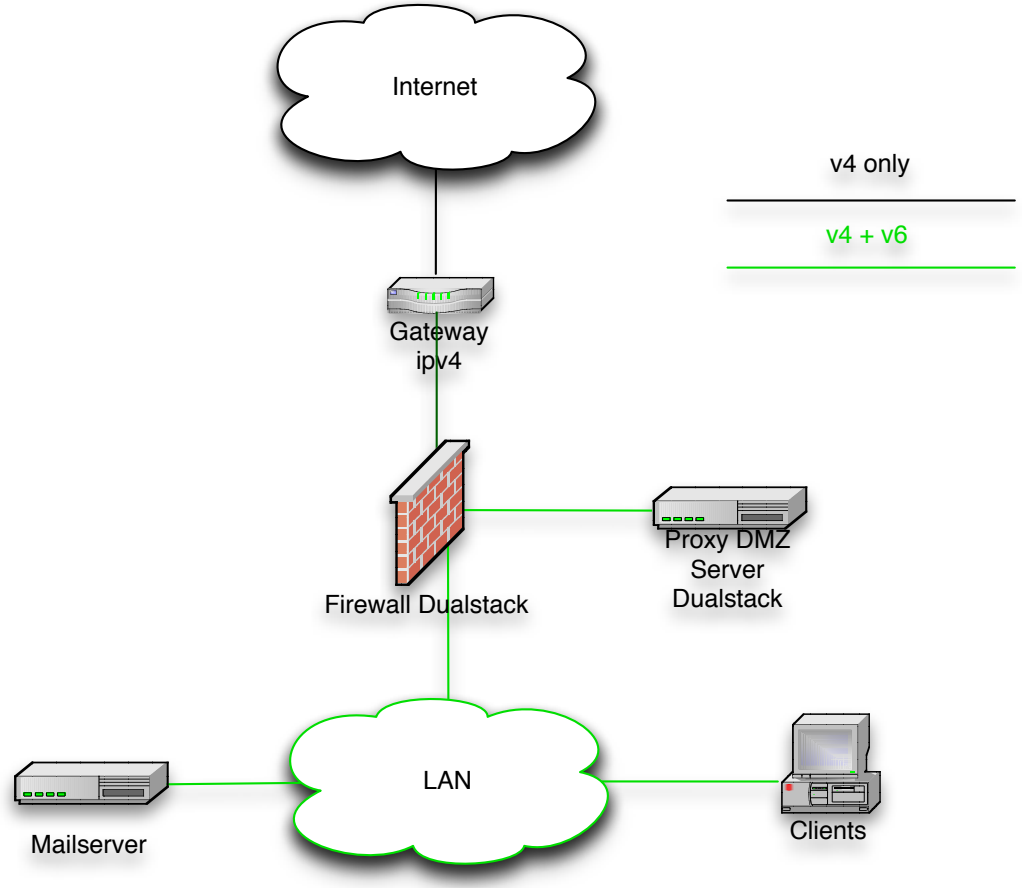


Planung

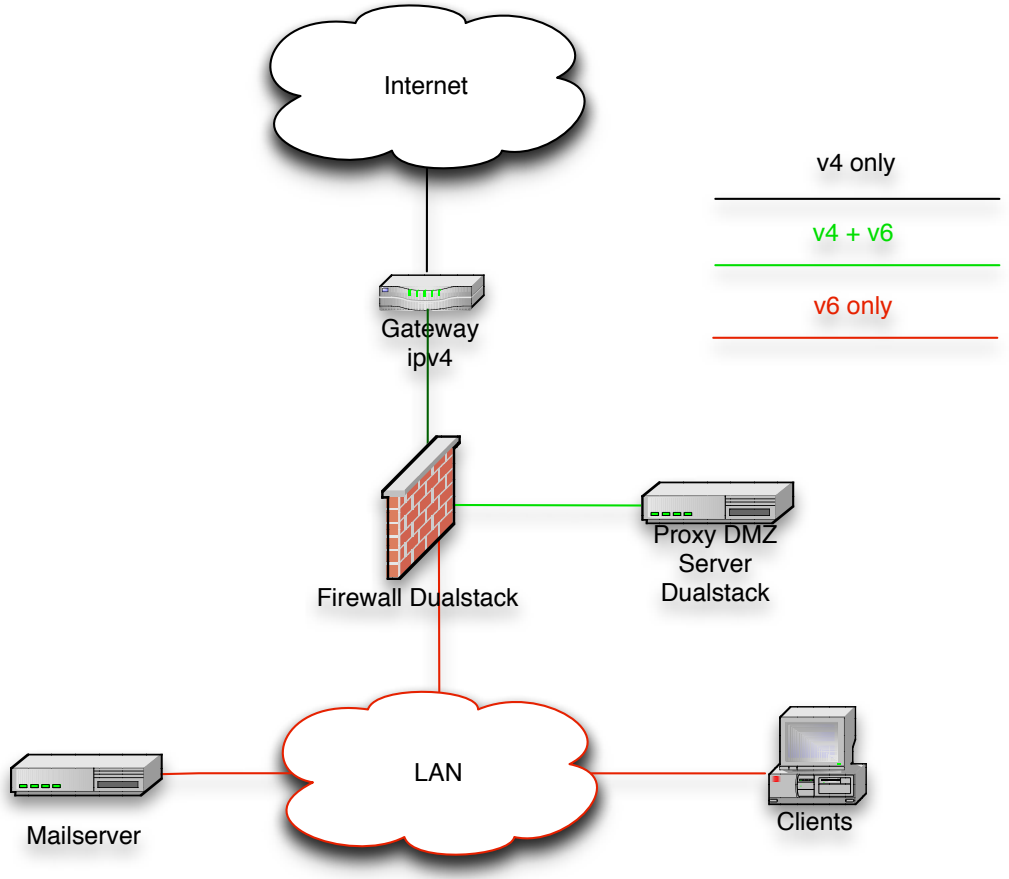
Anschlussszenarien

- v6 in LAN
- Notwendig:
  - v6 Firewall
  - Dual Stack v6 Server in DMZ mit
    - Mail Server
    - Proxy
    - Webserver
  - DNS Records für Mail und DNS
  - Dual Stack oder v6 only Server im LAN
  - Dual Stack oder v6 only Clients im LAN
  - Dienste zur v6 Konfiguration im LAN (RA, DHCPv6, DNSv6)

Anschlussszenarien - v6 Dienste im LAN



Anschlussszenarien - v6 Dienste im LAN

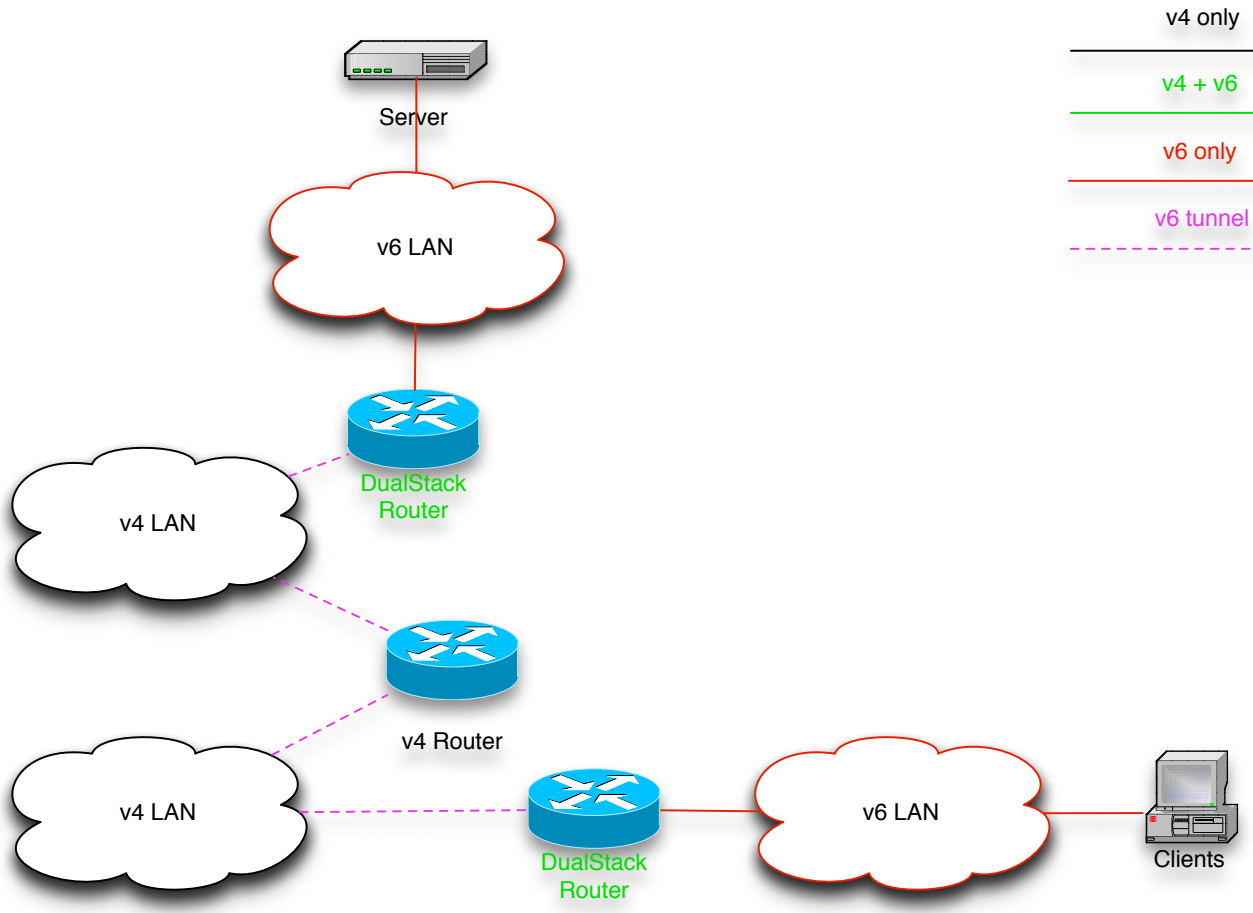


Planung

Anschlussszenarien

- Inseln
- Notwendig:
  - Dual Stack Router für jede Insel
  - v6 only Server im LAN
  - v6 only Clients im LAN
  - Dienste zur v6 Konfiguration im LAN (RA, DHCPv6, DNSv6)
  - Dual Stack Proxies wenn auch mit v4 Diensten kommuniziert werden soll

Anschlussszenarien - Inseln



Planung

Adressdesign

- Minimum Assignment /48 = 2^16 64Bit Netzblöcke
- Auch /32 üblich
- Empfehlung selbst für Transfernetze ein /64 verwenden
- Bei Verwendung von /64s einfaches Renumbering
- Trotz der Fülle von Adressen strukturiert vorgehen, sonst findet man nichts mehr wieder.

Risiken

Angriffe

- Gefälschte Router Advertisments
- Man in the middle bei Neighbor Discovery
- Gefälschtes DHCPv6 (nix neues)
- Win7 / W2k8 Umgebung ohne konfiguriertes v6 kann gestohlen werden
- Wenn Outgoing Traffic erlaubt ist, ist das Netz dank Teredo **offen!**

Firewalls

Check Point

- IPv6 seit R55
- Getrennte Netzwerkobjekte
- Andere Spalten im Log
- Regeln gemischt
- Vorsicht bei IPS (Smart Defense)
- Tunnel mit Handarbeit möglich (unsupported)
- Core XL funktionierte im Test nicht (kein Load Balancing)
- Kleine kosmetische Unschönheiten im GUI
- Momentan keine Virtualisierung
- Im Test kein VPN
- “Mit Gaia wird alles gut”

Security Produkte Firewalls

Juniper

- Netscreen bot IPv6 Support wurde aber abgekündigt
- SRX Plattform basiert auf den JunOS Routern daher:
  - Starker Support bei Routingprotokollen
  - Lange Erfahrung mit IPv6 auf Routing ebene
- JunOS 10 noch mit einigen Einschränkungen bzgl. z.B. IPS
- JunOS 11r2 behob das Gros der Einschränkungen lediglich Virtualisierung ist erst auf der Roadmap
- VPN funktioniert
- Bei High Performance Anforderungen für IPv6 ohne Virtualisierung momentan Produkt der Wahl

Firewalls

Fortinet

- Virtualisierung geht
- HA geht, aber ohne State Synchronisation (erst in der nächsten Release)
- Weiter keine Einschränkungen

Firewalls

Cisco

- Ab Release 7
- Virtualisierung geht
- HA geht, aber ohne State Synchronisation (erst in der nächsten Release)
- Weiter keine Einschränkungen

Firewalls

OpenSource

- Linux seit Kernel 2.6
  - So “gut” wie stateful filtering in IPv4
- OpenBSD
  - Recht detailliert
- FreeBSD
  - Wie die IPv4 Firewall

IPS/IDS

- SNORT
  - versteht IPv6
  - hat eigene Patterns für IPv6 Spezifika
  - Frei erweiterbar
- IBM/ISS
  - Voll IPv6 fähig
  - Erkennt Tunnel
  - Auch über IPv6 managebar

VPN

- Cisco
  - Im Tunnel und zwischen Endpunkten
  - Cisco IPSEC Client ignoriert v6. Personal Firewall nutzt nichts, Hintertür in das Netzwerk einfach möglich
- Juniper
  - Im Tunnel und zwischen Endpunkten
- Windows
  - Im Tunnel und zwischen Endpunkten
- Linux
  - Im Tunnel und zwischen Endpunkten

Andere Komponenten

OS

- Windows
  - Ab Vista IPv6 default bei 2003/XP nachinstallierbar
  - Windows Firewall schlägt sich schon bei XP besser als andere Produkte
- Linux
  - Lange enthalten
  - Bei den meisten Distributionen angeschaltet und auf Autoconfig
  - Applikationen benutzen IPv6 bevorzugt, wenn ein AAAA Record funktioniert
- Apple
  - Seit OSX enthalten
  - In vollem Umfang erst seit Lion als Client
  - IPv6 wird bevorzugt verwendet, wenn ein AAAA Record vorhanden ist

Andere Komponenten

Mail / DNS / Proxies

- Mail
  - Exchange ab 2008
  - OpenSource Komponenten wie Postfix wenn das OS darunter und die Version aktuell genug sind
- DNS
  - Windows ab 2008 (2003 kann schon die records bereitstellen)
  - Bind ab Version 9.0 aber in vollem Umfang am besten ab 9.4
- Proxies
  - Squid ab Version 3

Clients

Autokonfiguration von Clients

- Win 7
  - Macht alles wie im RFC (je nach Patchstand komisch bei Dualstack)
- Linux
  - Kernel verarbeitet RAs wenn das aktiviert ist (net.ipv6.conf.all.accept_ra)
  - Kommunikation mit Userspace möglich, aber kaum genutzt
    - Ausnahme EDNS Dienst
  - DHCPv6 wird nur gestartet, wenn es reinkonfiguriert ist
- MAC
  - Erst ab Lion
  - Vorher werden RAs richtig verarbeitet, aber keine Dienst Konfiguration

Administrative Aspekte

Für den Admin

- DNS
  - Vorwärts nur AAAA Records hinzufügen
  - Rückwärts “Fummelei”
    - 4.3.2.1.c.e.e.f.f.f.d.5.f.f.a.1 IN PTR test.example.com.
- Schreibweisen
  - Bei Angabe von Server und Portnummer werden [ ] verwendet
    - [2001:db8:cafe::1]:80
- Autokonfiguration und mehrere Interfaces
  - Linux akzeptiert keine RAs wenn mehr als ein Interface vorhanden ist. Dies muss erst angeschaltet werden

Administrative Aspekte

Für den Admin

- Besondere Adressen
  - Kein ping 255.255.255.255 aber
    - ff02::1 All nodes (auf dem Link, Link local Adressen antworten)
    - ff02::2 All routers (auch hier antworten die Link local Adressen)
  - Das ganze mit ff01 für “Node Local”
  - Jede Menge weitere Adressen unter http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml
- Bei ping6 mit Link Local Adressen auf Multihomed Hosts immer das Interface von dem gepingt werden soll mit -I angeben

Ihr Kontakt

… Fragen? … offene Diskussion