IPv6
Names & Numbers

Namensauflösung in IPv6 Netzwerken

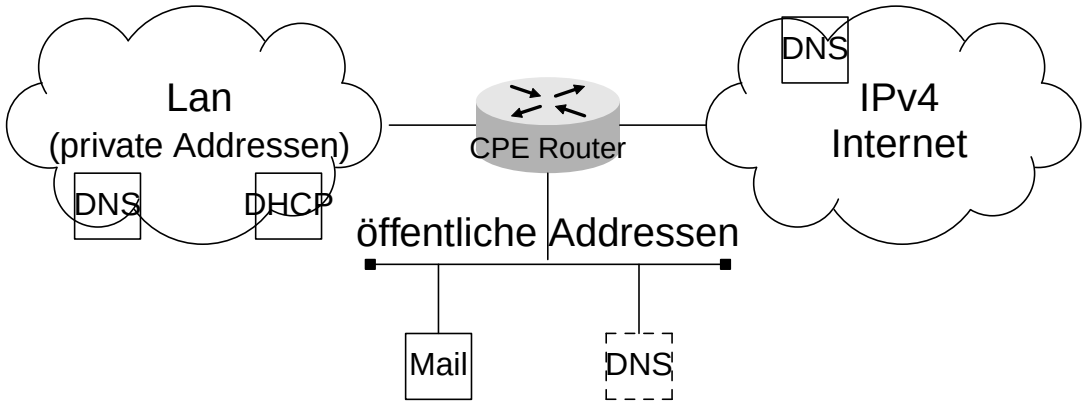
iX, DE-CIX IPv6 Kongress
28.–29. Mai 2009
Frankfurt

Holger.Zuleger@hznet.de

Agenda

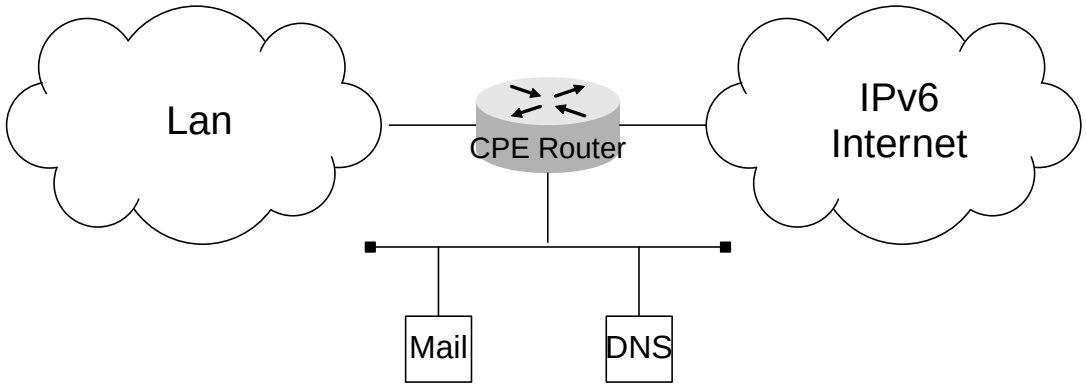
- Einführung
  - Unterschiede IPv4 und IPv6 Netzwerke
- DNS Provisionierung
  - Statisch / Skriptgesteuert
  - Dynamic DNS
    - Authentisierung / Updateverfahren
    - DDNS und IPv6
- DNS Resolver config
  - IPv4 / IPv6 Transport
  - IPv6 only Netze
- IPv6 Address Renumbering
  - Gründe
  - Renumbering und DNS
  - Empfehlungen
- Referenzen

IPv4 Netzwerk



- Private Adressen im LAN (NAT/PAT auf CPE Router)
- Adresszuordnung im LAN über DHCP (dynamisch oder fix)
- DNS im Lan für lokale (private) Systeme
  Provisionierung statisch oder dynamisch
- Kleines öffentliches Netz für public Services (DMZ)
  Statische IP Konfiguration
- DNS für public Services oft bei ISP gehostet

IPv6 Netzwerk



- Großer öffentlicher Adressbereich (/48 oder /56)
  Öffentliche Adressen im LAN und in der DMZ (65536 bzw. 256 Subnetze)
- IPv6 Adresszuordnung immer über SLAAC (RFC2462)
  Stateless Address Autoconfiguration: Kein DHCP Server erforderlich
- Nutzung von DHCPv6 (RFC3315) nur für Information Request
- Eigener öffentlicher Nameserver
  Forward und Reverse Zone
- DNS Provisionierung ?
  Statisch oder dynamisch aber ohne DHCP Server

- Einführung
  - Unterschiede IPv4 und IPv6 Netzwerke
- DNS Provisionierung
  - Statisch / Skriptgesteuert
  - Dynamic DNS
    - Authentisierung / Updateverfahren
    - DDNS und IPv6
- DNS Resolver config
  - IPv4 / IPv6 Transport
  - IPv6 only Netze
- IPv6 Address Renumbering
  - Gründe
  - Renumbering und DNS
  - Empfehlungen
- Referenzen

DNS Provisionierung (Statisch)

- Statische Konfiguration meist „Datenbank“ gesteuert
  (Rechnername, IPv4-Adresse, evtl. Macadresse, ...)
- Automatische Generierung von Zonefile, DHCP Config, usw.
- IPv6 Tool gen6dns
  - Inputfile (hosts.txt: name macaddresse subnet_oder_host_ip)

```
horst   00:17:53:85:80:3b       0:0:0:10::/64
dns1                            0:0:0:d::53/128
        00:13:35:a2:91:f4       0:0:0:10::/64
```

  - Forward DNS Einträge

```
$ gen6dns -f -o example.de -p 2001:db8:affa::/48 hosts.txt
horst            IN AAAA 2001:db8:affa:10:217:53ff:fe85:803b
dns1             IN AAAA 2001:db8:affa:d::53
host001335a291f4 IN AAAA 2001:db8:affa:10:213:35ff:fea2:91f4
```

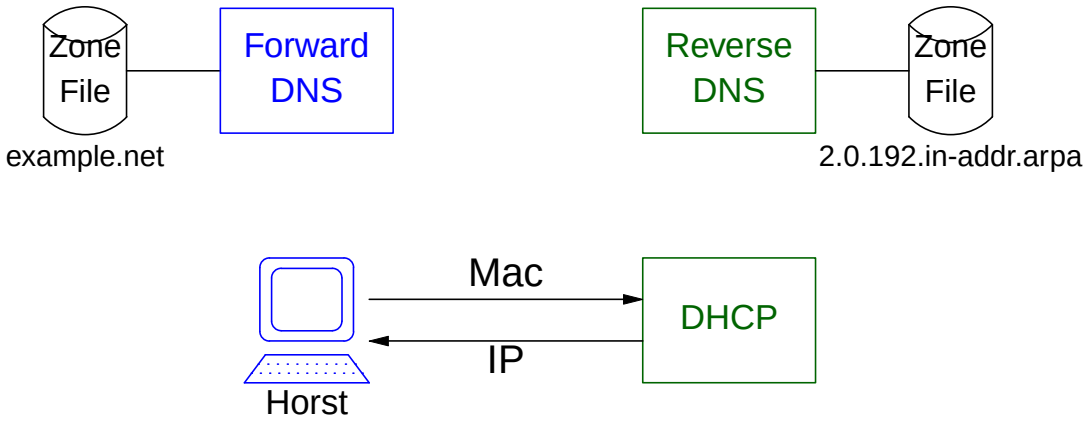
  - Reverse DNS Einträge

```
$ gen6dns -r 64 -o example.de -p 2001:db8:affa::/48 hosts.txt
b.3.0.8.5.8.e.f.f.f.3.5.7.1.2.0 IN PTR horst.example.de ; 0010
5.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR dns1.example.de  ; 000d
4.f.1.9.2.a.e.f.f.f.5.3.3.1.2.0 IN PTR host001335a291f4.example.de  ;
```

- Einführung
  - Unterschiede IPv4 und IPv6 Netzwerke
- DNS Provisionierung
  - Statisch / Skriptgesteuert
  - Dynamic DNS
    - Authentisierung / Updateverfahren
    - DDNS und IPv6
- DNS Resolver config
  - IPv4 / IPv6 Transport
  - IPv6 only Netze
- IPv6 Address Renumbering
  - Gründe
  - Renumbering und DNS
  - Empfehlungen
- Referenzen

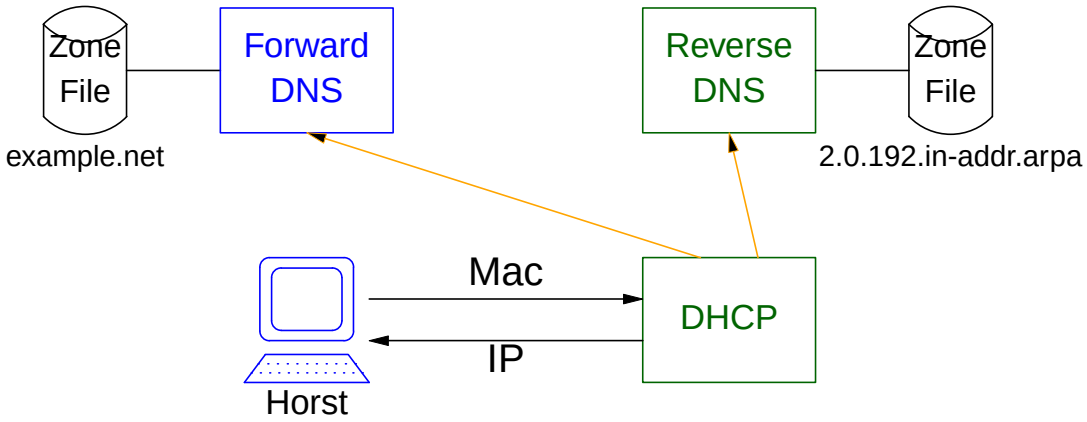
Dynamic DNS

- Modifikation der Zone über DNS Protokollerweiterung (RFC2136)
- Updates müssen authentisiert sein (RFC3007)
  - IP Access Liste (schwach)
  - Shared Secret (symmetrischer Key) (TSIG-MD5)
  - Asymetrischer Key (SIG0)
  - Third Party (GSS-TSIG aka Kerberos)
  - TCP Authentisierung (schwach)
- Wer führt Update aus ?



Dynamic DNS Update (DHCP Server)

- Durch DHCP Server

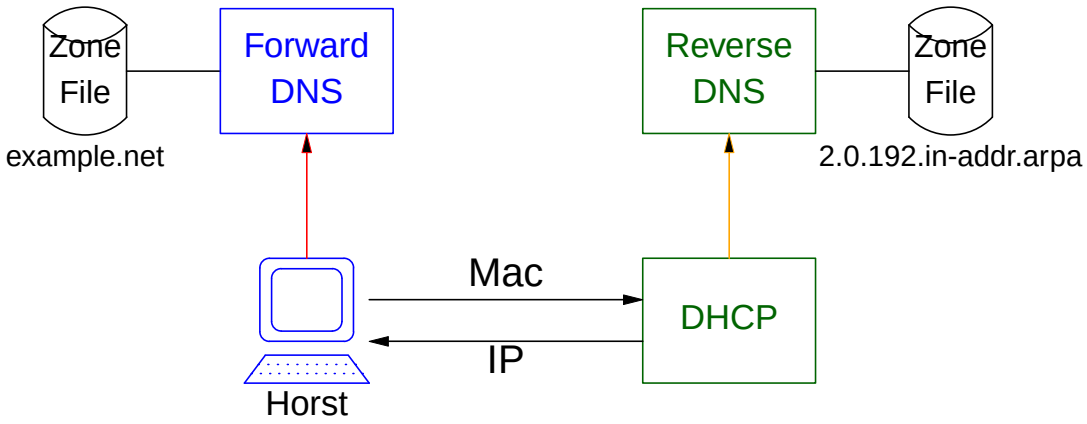


- Authentisierung durch
  - IP-Adresse (Nicht empfohlen)
  - Shared Secret

```
key "dhcp-key" {
        algorithm hmac-md5;
        secret "Qi...Z5MAFTUIKOf0kfcQCAcDL3ZAtZjvbqXg==";
};
zone "2.0.192.in-addr.arpa" {
     type master;   file "db.192.0.2";
     allow-update { dhcp-key; };
};
```

Dynamic DNS Update (Host und DHCP)

- Durch DHCP Server und Host



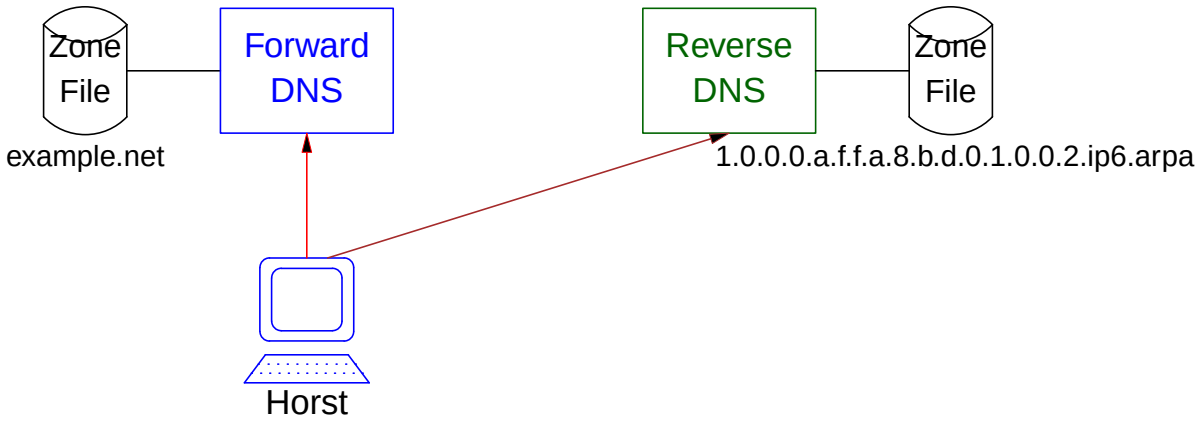
- Host Authentisierung durch
  - Asymetrische Keys (SIG0)

```
zone "example.net" {
     type master;   file "db.example.net";
     update-policy { grant * self * A AAAA; };
};
```

  - Kerberos (GSS-TSIG)
- DHCP Server Authentisierung durch Shared Secret

Dynamic DNS Update (IPv6)

- Nur durch Host (IPv6)



- Authentisierung gegenüber Forward DNS durch
  - Asymetrische Keys (SIG0)
  - Kerberos (GSS-TSIG)
- Authentisierung gegenüber Reverse DNS über TCP

```
zone "1.0.0.0.a.f.f.a.8.b.d.0.1.0.0.2.ip6.arpa" {
     type master;   file "db.0001";
     update-policy { grant * tcp-self * PTR; };
};
```

DDNS SIG0 Setup

- Generieren eines asymetrischen Keys (per Host)

```
$ dnssec-keygen -k -a rsasha1 -b 1024 -n HOST horst.example.net
Khorst.example.net.+005+33451
$ ls -l K*
-rw-r--r-- 1 dns admin 214 Apr 21 20:11 Khorst.example.net.+005+33451.key
-rw------- 1 dns admin 937 Apr 21 20:11 Khorst.example.net.+005+33451.private
```

- Öffentlicher Teil des Schlüssel als KEY Record in die Zone aufnehmen

```
$ cat Khorst.example.net.*.key
horst.example.net. IN KEY 512 3 5 AwEAMb+O+1unDje8eruaV15POh.....A7PF2/zT
```

- Update
  - Keine Link local oder Multicast Adressen
  - Keine Unique Local Adressen (nicht im public DNS)
  - Keine temporären oder deprecated Addressen

```
$ nsupdate -k Khorst.example.net.+005+33451.private
> zone example.net
> update delete horst.example.net IN AAAA
> update add horst.example.net 7200 IN AAAA 2001:db8:affa:1:217:53ff:fe85:803b
> send
$ nsupdate -v
> zone 1.0.0.0.a.f.f.a.8.b.d.0.1.0.0.2.ip6.arpa.
> update delete b.3.0.8.5.8.e.f.f.f.3.5.7.1.2.0.1.0.0.0.a.f.f.a.8.b.d.0.1.0.0.2.ip6.arpa. IN PTR
> update add b.3.0.8.5.8.e.f.f.f.3.5.7.1.2.0.1.0.0.0.a.f.f.a.8.b.d.0.1.0.0.2.ip6.arpa. 7200 IN PTR horst.example.net.
> send
```

- Einführung
  - Unterschiede IPv4 und IPv6 Netzwerke
- DNS Provisionierung
  - Statisch / Skriptgesteuert
  - Dynamic DNS
    - Authentisierung / Updateverfahren
    - DDNS und IPv6
- DNS Resolver config
  - IPv4 / IPv6 Transport
  - IPv6 only Netze
- IPv6 Address Renumbering
  - Gründe
  - Renumbering und DNS
  - Empfehlungen
- Referenzen

DNS (Stub) Resolver Konfiguration

IPv4 Transport

- Typischerweise über DHCP
- Oder statisch in `/etc/resolv.conf`

```
nameserver 192.0.2.1
nameserver 192.0.2.5
```

IPv6 Transport

- Verschiedene Verfahren in Diskussion (RFC4339)
- Statisch in `/etc/resolv.conf` (Anycast adresse?!)

```
nameserver 2001:db8:affa:d::53
```

- RA „OtherConfig“ Flag + DHCPv6 Information Message
- Über Router Advertisement Option (RFC5006)
  Zur Zeit nicht weit verbreitet
- Über lokalen (validierender) Resolver
  DNSSEC Unterstützung hilfreich bei Renumbering

DNS Resolver Konfig (Empfehlung)

- IPv4 Transport zur Zeit unverzichtbar
  - Nicht alle Stub Resolver sind IPv6 fähig
  - IPv6 Netze noch nicht weit verbreitet
  - Parallele Konfiguration problematisch (Wer legt /etc/resolv.conf an)
- IPv6 Transport noch nicht notwendig
  Warten auf IPv6 Anycast oder RA Option
- Resolver Konfig für Hosts im LAN
  - Nur IPv4 Resolver über DHCP konfigurieren
- Für mobile Hosts
  - Auf dem mobile Host lokalen validierender Resolver aufsetzen
  - und statisch konfigurierte `/etc/resolv.conf`

```
nameserver 127.0.0.1
nameserver ::1
```

  - In manchen Netzen problematisch (z.B. Hotel WLAN)
    DNS Redirection für HTML Pushpage

DNS Resolver in IPv6 only Netzen

- Stub Resolver Konfig
  - RA + „Other Config“ Flag + DHCPv6 Information Message
  - In Zukunft hoffentlich über RA Option
- Resolver (Caching Nameserver) **muß** Dual Stack Server sein!

```
options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { any; };
        recursion yes;
}
```

- Oder er benötigt einen Dual Stack „Helper“ als Forwarder

```
options {
        listen-on-v6 port 53 { any; };
        recursion yes;
        dual-stack-servers {
                2001:db8:affa:d::53;
                2001:db8:affa:e::53;
        };

}
```

- Einführung
  - Unterschiede IPv4 und IPv6 Netzwerke
- DNS Provisionierung
  - Statisch / Skriptgesteuert
  - Dynamic DNS
    - Authentisierung / Updateverfahren
    - DDNS und IPv6
- DNS Resolver config
  - IPv4 / IPv6 Transport
  - IPv6 only Netze
- IPv6 Address Renumbering
  - Gründe
  - Renumbering und DNS
  - Empfehlungen
- Referenzen

IPv6 Address Renumbering

- Address Renumbering aus verschiedenen Gründen notwendig
  - Provider Wechsel
    In IPv6 gibt's nur Provider Aggregated Address Space
  - PI Address Space nur für Multihoming
    RIPE-466 „IPv6 Address Allocation and Assignment Policy“ (Paragraph 8)
  - Wechsel der Access Technolgie
    Tunnel, SDLS, Metro Ethernet
  - Wechsel der Topologie innerhalb einer Site
    Identische Subnetgröße in IPv6
- Renumbering auch in IPv4 Netzen notwendig, aber:
  - Privater Addressraum im LAN
  - Adressanpassung durch NAT Device
  - Vorteil von NAT?
- IPv6 unterstützt den Prozess des Renumbering
  Renumbering w/o a flag day (RFC4192)

IPv6 Renumbering und DNS

- Gleichzeitige Nutzung mehrerer Adresspräfixe im Migrationsfenster
- Umschaltung DNS basierend
  - Vorab die TTL Zeiten reduzieren
  - kurzlebige Verbindungen (HTTP)
    unproblematisch
  - mittellange Verbindungen (ssh)
    evtl. Server reload notwendig / interaktive Anwendungen unproblematisch
  - langlebige Verbindungen (NTP, NFS)
    Evtl. auch Client reload notwendig
  - Forward- und Reverse-Zone signieren (DNSSEC)
- Herausforderungen
  - Applikation die TTL Zeiten nicht oder nicht richtig auswerten
  - Applikationen die IP-Adressen verwenden (Stub Resolver, NTP)
  - Applikationen die nur beim Start ein DNS Lookup durchführen
  - Netzmonitoring, Statistiken

IPv6 Renumbering (Empfehlungen)

- Renumbering einplanen
- Ausschließlich dynamische Adressvergabe (SLAAC) verwenden
- Mögliche Aussnahmen
  - DNS Resolver (Caching Nameserver)
  - Routerinterfaces
  - Alle statischen Konfigurationen dokumentieren
    Host, Subnetz, IP, Standort, Administrator, usw.
- DNS Einträge entweder dynamisch (DDNS) oder über Skript erzeugen

```
$ gen6dns -f -r 64 --ttl 2h -p 2001:db8:beeb::/48 -o example.net hosts.txt
```

- Evtl. Unique Local Addresses (ULA) für Netzmonitoring verwenden
  http://www.hznet.de/tools/generate-rfc4193-addr
- Erstes und letztes Subnetz nicht verwenden
  2001:db8:affa:0000::/64 und 2001:db8:affa:ffff::/64
- Wenn es soweit ist: RFC4192 folgen

- Einführung
  - Unterschiede IPv4 und IPv6 Netzwerke
- DNS Provisionierung
  - Statisch / Skriptgesteuert
  - Dynamic DNS
    - Authentisierung / Updateverfahren
    - DDNS und IPv6
- DNS Resolver config
  - IPv4 / IPv6 Transport
  - IPv6 only Netze
- IPv6 Address Renumbering
  - Gründe
  - Renumbering und DNS
  - Empfehlungen
- Referenzen

Referenzen

RFCs
- 4192 Procedures for Renumbering an IPv6 Network without a Flag Day
- 5006 IPv6 Router Advertisement Option for DNS Configuration
- 2462 IPv6 Stateless Address Autoconfiguration
- 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- 2136 Dynamic Updates in the Domain Name System (DNS UPDATE)
- 4339 IPv6 Host Configuration of DNS Server Information Approaches
- 3007 Secure Domain Name System (DNS) Dynamic Update
- 4193 Unique Local IPv6 Unicast Addresses
- 4472 Operational Considerations and Issues with IPv6 DNS

RIPE
- 466 IPv6 Address Allocation and Assignment Policy

DNS
- Validierende Resolver
  http://unbound.net, http://www.isc.org/software/bind
- gen6dns Zur Zeit nicht öffentlich verfügbar; Bitte per Mail anfragen

DNSSEC

http://www.dnssec.net, http://www.hznet.de/dns/zkt

Fragen ?

DNSsec, VoIPsec, IPsec, XMPPsec, SMTPsec, WLANsec ...

... DKIM, Kerberos, IMAP, LDAP, ENUM, SIP, ...

... NTP, DNS, DHCP, IPv6, Routing, Switching

Holger.Zuleger@hznet.de

CONTENTS