IPv6-Only

Sites

Now?

Deutscher IPv6 Kongress 2013

June 6/7, 2013
Frankfurt / Germany

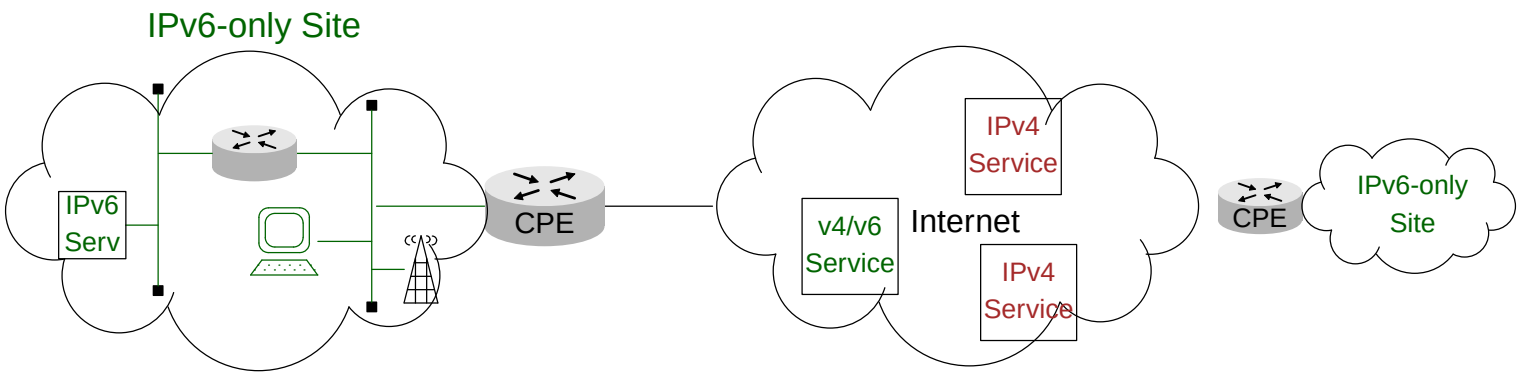
Holger.Zuleger@hznet.de

IPv6 Transition: Dual Stack or IPv6-only

- Many people are asking for IPv6-only deployments
  - Again, just one stack to operate
  - Only one kind of access list / routing process / address management
  - Dual stack sounds like „double trouble“
- But „The Internet“ is still (at most) IPv4-only
- Translation between IPv6 (client) and IPv4 (server) needed
  - Proxy (Layer 4 and above) based
  - Stateful NAT64 + DNS64 (Layer 3 based)
    In the meantime, available from different vendors
- Remember: The recommended migration path to IPv6 is dual stack!
  IPv6-only is the big exception
- See also
  - Tore Anderson „The case for IPv6-only Data Centers“ (RIPE#64, 4/2012)
  - RFC 6586: „Experiences from an IPv6-Only Network“ (April 2012)
  - Andrew Yourtchenko „IPv6-only clients experience“ (RIPE#66, 5/2013)

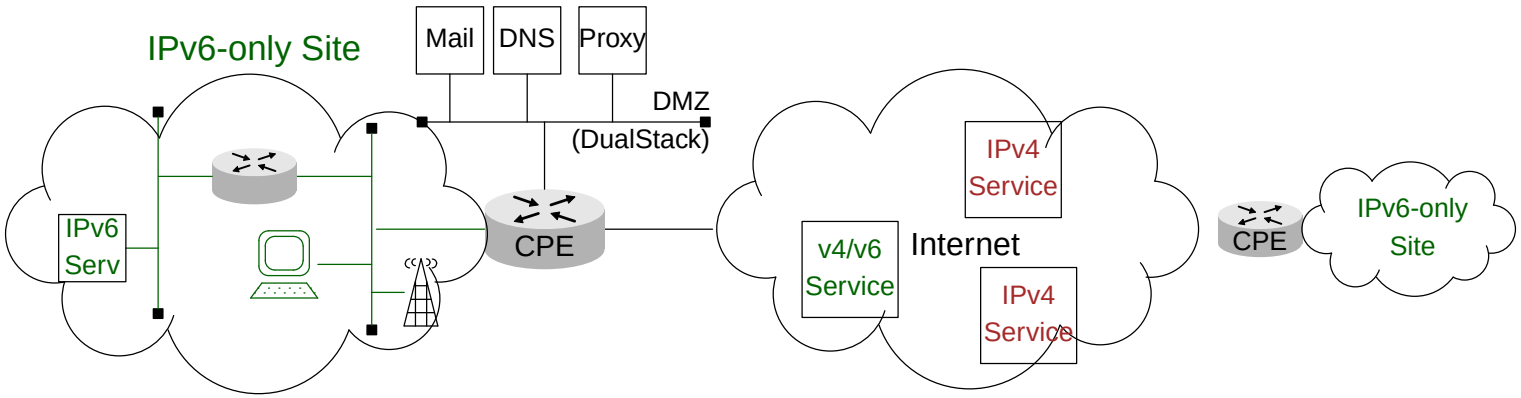
IPv6-only Example Network

1. Internet, still dominated by IPv4-only services
2. IPv6-only site with routers, access points, clients and servers
3. IPv6-only branch site
   IPv6-only site-to-site VPN



IPv6-only Example Network

1. Internet, still dominated by IPv4-only services
2. IPv6-only site with routers, access points, clients and servers
3. IPv6-only branch site
   IPv6-only site-to-site VPN



- Surprisingly, the access link must be dual stack
  At least at one of the IPv6-only sites
- The public services must be dual stack
  Until the entire Internet is dual stack

Network Elements

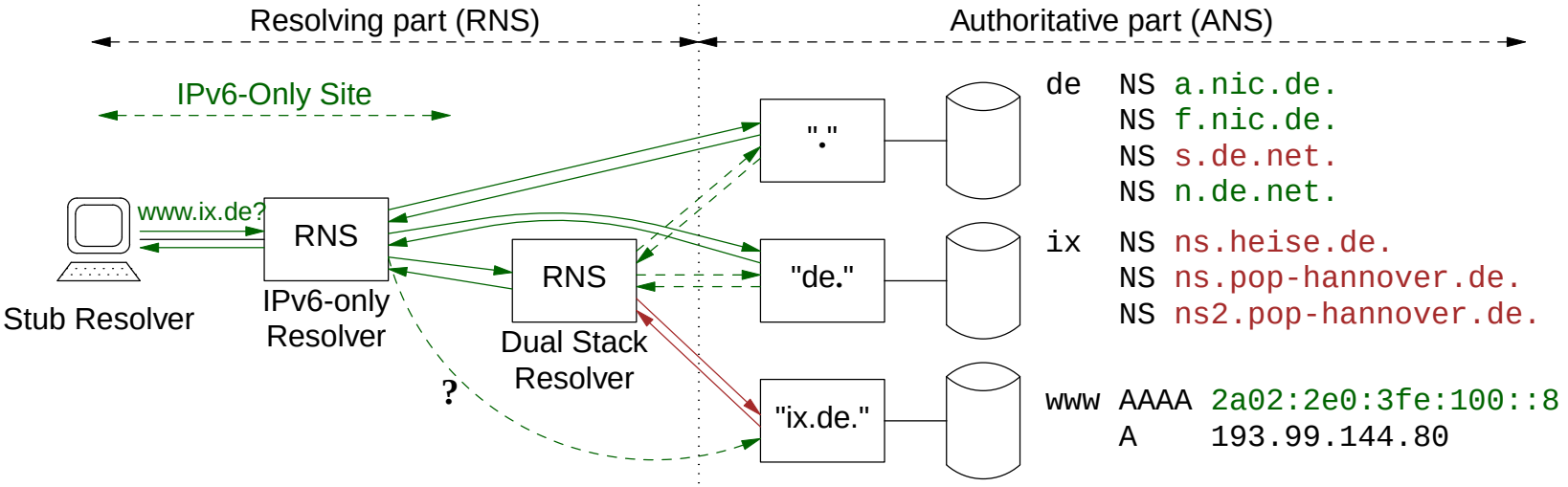
- Layer 3 devices (routers)
  - All dual stack routers should work also in IPv6-only environments
    (But now you must configure the OSPFv3/BGP router-id manually)
  - Look at management protocols (telnet/ssh/http/SNMP)
  - Have a close look at other, less familiar protocols
    Radius/Diameter, Tacacs+, Netflow, Syslog, ftp/tftp
- Layer 2 devices (switches, access points)
  - „Transparent“ for IPv6
  - But same mangement issues as layer 3 devices
  - 802.1x authenticator or any other kind of „network authentication“
- Terminal- or (ISDN) Dial-In Server
  - Unix-based terminal servers should be ok
  - Dial-In server must support PPP/IP6CP
- Others
  - UPS Management/Signaling
  - Remote Power Switches

Network Services

- Authentication Server
  Radius / Tacacs+
- All Unix-based network services shouldn't be much of a problem
  syslogd, ftpd, tfpd, ssh
- Network time protocol (NTP)
  - No dedicated IPv6 servers on pool.ntp.org available
    So
    ```
    server -6 0.de.pool.ntp.org
    server -6 1.de.pool.ntp.org
    server -6 2.de.pool.ntp.org
    server -6 3.de.pool.ntp.org
    ```
    will probably end up with just one working server
  - Configure IPv6 upstream NTP servers manually or use dual stack
- DNS resolver
  - The global DNS tree is actually not fully dual stack
  - Many zones have only IPv4 servers (e.g. `ix.de`) even 15% of all TLDs

DNS and IPv6 at a glance

- DNS Resolving



- IPv6-only clients must use IPv6 as transport protocol
  The query is always about an AAAA record
- The global DNS tree consists of dual stack and IPv4-only servers
  v6-only resolver needs the help of a DS resolver to query the entire DNS tree

```
# named.conf
dual-stack-servers {
     2001:db8:130:1261::53;
};
```

Operating Systems and Applications

Operating Systems

- Every modern OS supports IPv6! But IPv6-only?
  - — Windows XP can’t handle IPv6 name servers
  - — Rumors that some Linux network manager will not work w/o IPv4
- Currently no standard way for RDNS provisioning
  a. RA + Other config flag and a stateless DHCPv6 Server
  b. RDNS and domain is propagated by RA message (RFC 6106)
  c. „Well-known“ default DNS server addresses

  Which option will be supported by your hosts and routers?

Applications

- Check your own list of applications
- E.g. Skype is IPv4 only

More on RFC6586 and on Andrew’s presentation

Public Services

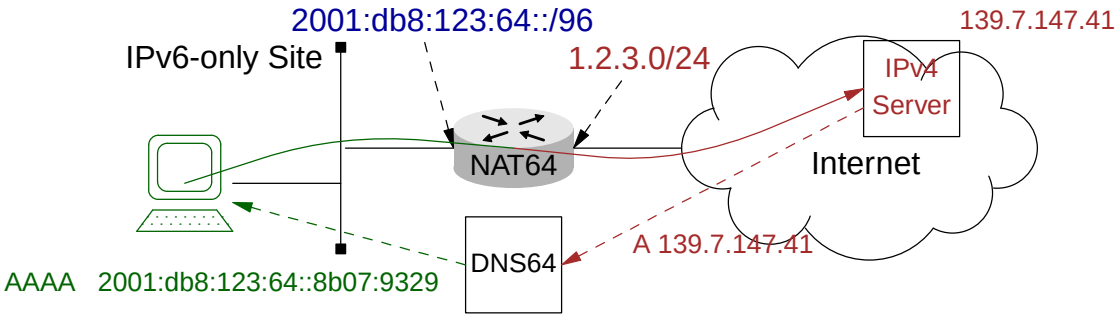
- All public services should be currently dual stack
  Because this is the overall migration strategy
- Put all your public servers in a dual stack DMZ
  Or have a deeper look at Tore Anderson's presentation
- Examples of dual stack public services
  - Mail (SMTP / IMAP)
  - DNS (recursive and authoritative servers)
  - Jabber (c2s, s2s)
  - SIP Registrar and Session Border Controller
  - Webserver / (reverse) Proxy
  - AD / LDAP / KDC
- More challenging
  - Remote access gateway: IPSEC / OpenVPN / SSL
    Inner protocol is IPv6, outer protocol is IPv4 or IPv6
  - Site-to-Site IPSEC VPN router
  - GETVPN is best for full-mesh IPSEC Site-to-Site IPv6-only VPN
    But it currently depends on IPv4 for control plane

Internet Access

- Local IPv6 client to dual-stack Internet server is fine
- Local IPv6 client to IPv4-only Internet server is problematic
  The biggest part of the Internet is still IPv4-only
- Two kinds of Internet access
  A. Via Proxy or Application Level Gateway (ALG)
  B. Routed Internet access (Layer 3)
- For A. we are fine if the service is Proxy/ALG friendly
  — Inner proxy site is IPv6-only, outside is dual stack
  — Not all services are supported
- For B. we need a translation service between IPv6 and IPv4
  — This is what is called stateful NAT64
  — Stateful because of limited IPv4 address space
  — DNS64 is also required in this case

Stateful NAT64

- IPv6-only site wants to communicate with the IPv4 Internet
  Session is initiated on IPv6-only site



- IPv6-only site reserves a prefix (/96) for all IPv4-only devices
  Prefix (e.g. 2001:db8:123:64::/96) must be routed to the NAT box
- IPv4 address pool (at least one address) is needed on outside
- NAT box translate IPv6 header to IPv4 header
  - Dest v4 is taken out of the rightmost 32 bits of the v6 dest address
  - Src v4 is taken dynamically out of an IPv4 address pool on the NAT device
- Clients must use DNS64 as resolver
  Generates faked AAAA answers for hosts with A record only

DNS64 (RFC6147)

- A DNS64 Server is a recursive Name Server
  Can't be a DNSSEC validating server
- The server generates fake IPv6 address records if necessary
  The NAT64 prefix (2001:db8:123:64::/96) must be configured on the server
- An IPv6-only client sends an AAAA query to DNS64 server
  e.g. for `www.vodafone.de`
- The server must answer this
  1. DNS64 tries to get the real IPv6 address
  2. If this was successful, DNS64 responds with real IPv6 address
  3. If answer was empty, it tries to get the IPv4 address
     `www.vodafone.de IN A 139.7.147.41`
  4. Generate IPv6 address out of NAT64 prefix plus IPv4 address
     `www.vodafone.de IN AAAA 2001:db8:123:64::8b07:9329`
- BIND 9.9 can be configured as a DNS64 Server

```
dns64 2001:db8:123:64::/96 {
     clients { local-net-acl; };
     mapped { !rfc1918-acl; any; };
};
```

NAT64/DNS64 Issues

- NAT64 depends on domain names to work properly
  - No support for literal IPv4 addresses
  - E.g. `http://1.2.3.4:8080` is no longer working
  - Use `http://[2001:db8:1234:64::0102:0304]:8080` instead (if supported by the browser)
  - Websites sometimes uses IP based links instead of FQDN based ones
- DNS64 breaks DNSSEC
- Any protocol with embedded IP(v4) addresses will not work
  NAT64 GW could help with ALG (same as in NAT44)
- Skype will definitely not work through NAT64
  No IPv6 support / uses embedded addresses / content is encrypted
- The general experience with NAT64 seems similar to NAT44
  See RFC 6586
- Do not use a DNS64 resolver for dual stack clients!
  It will force unnecessary traffic load on the NAT64 GW

Summary

- Today a site can't live without IPv4 connectivity
  - At least 95% of the Internet is IPv4-only
  - Proxy works like a charm / NAT64/DNS64 has some issues
- All (public) sevices **must** be available by IPv4 **and** IPv6
  Mail, Web, DNS, IPsec GW, AD/DC, ...
- All private services could be IPv6-only
  Depends on local requirements (Applications/OS/Hardware)
- IPv6-only for network management is a bit challenging
  Too many network devices are IPv4-only
- IPv6-only sites are open for a new network design
  IPv6-only Site-to-Site VPN / Single DNS Namespace / End-to-End IPsec
- However:

  Start to roll out IPv6 now ...

  ... wether as dual stack or IPv6-only network

Questions ?

DNSSEC, IPsec, DANE, XMPP, ...

... Kerberos, Radius, NTP, DHCP, DNS, DKIM, ...

... IPv6, LISP, Routing, Switching, 802.1x

Holger.Zuleger@hznet.de

CONTENTS