IPv6 & LISP

„The Intouchables“
or
„Ziemlich beste Freunde“?

Deutscher IPv6 Kongress 2014
May 23, 2014
Frankfurt / Germany

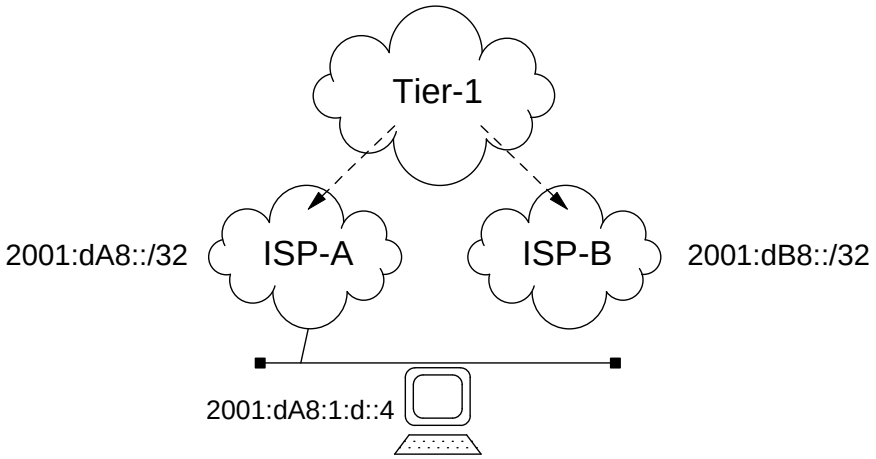
Holger.Zuleger@hnet.de

Locator / Identifier Problem

- The IP address is used as an Identifier **and** a Locator

Locator part

- Prefix aggregation on AS boundary
  Ideally just one IPv6 prefix per AS (DTAG: 2003::/19)
- All customers of an ISP use the same prefix

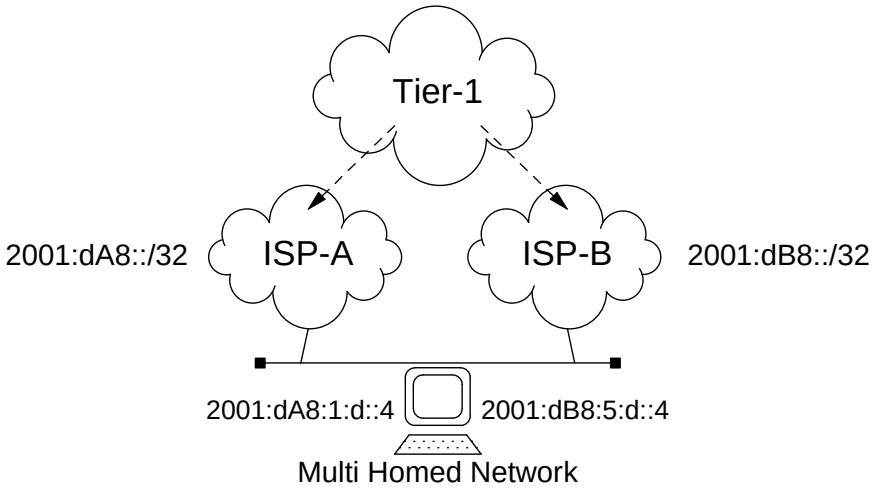


Locator / Identifier Problem

- The IP address is used as an Identifier **and** a Locator

Locator part

- Prefix aggregation on AS boundary
  Ideally just one IPv6 prefix per AS (DTAG: 2003::/19)
- All customers of an ISP use the same prefix



- Multihomed customers use two prefixes
  Or have to use PI address space

Locator / Identifier Problem

- The IP address is used as an Identifier **and** a Locator

Identifier part

- OS needs a way to bind incoming ip packet to application
- For tcp/udp peers 5-tuple used as identifier
  protocol, src-ip, dest-ip, src-port, dest-port

```
$ netstat -n -t
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 88.198.13.165:43162     74.125.39.125:5269      ESTABLISHED
tcp6       0  10920 2a01:4f8:130:1261::5222 2001:91fd:6426:1:2:7744 ESTABLISHED

# netstat -t -A inet6 -p
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp6       0      0 2a01:4f8:130:1261::5222 2001:91fd:6426:1:2:7744 ESTABLISHED 16602/c2s
```

- Session freeze if IP address or port changes
  That's only one reason why NAT is evil
- Even on multihomed networks active sessions via failure ISP go stale
  This is why we need LISP or a similar protocol

LISP

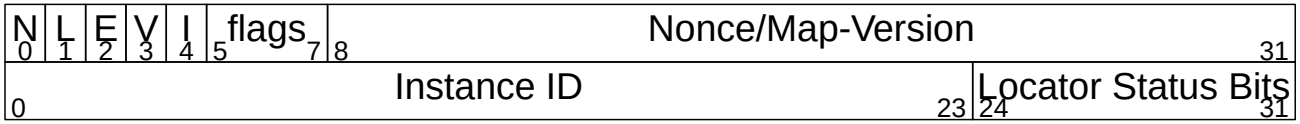
- The Locator/Identifier Separation Protocol (RFC 6830)
  - Solves the Locator Identifier Problem
  - Many other ideas how to solve this around
  - ILNP, IPNL, GSE/8+8, SCTP, Shim6, HIP, MIPv6, TCP Multipath
- LISP is a network based approach
  - No wonder, it's developed by Cisco
  - Others are host based (like HIP, MIPv6, Shim6, SCTP, TCP Multipath)
- Map-n-Encap mechanism
  - Encapsulation (data plane) means tunneling
  - Mapping (control plane) is used to learn the tunnel endpoint
- Several Mapping-Systems developed over the years
  - ALT (BGP + GRE)
  - DDT (Delegated Database Tree)
  - No mapping protocol neccessary for what we doing here

LISP Basics

- LISP uses two IP addresses
  - The other one is used as Routing Locator (RLOC)
  - One is used as Endpoint Identifier (EID)
- Map-n-Encap
  - Encapsulation is data plane (Ingress- and Egress Tunnel Router)
  - Mapping mechanism is control plane (Map Server & Map Resolver)
- Encapsulation means tunneling via LISP UDP packets
  Overhead: OuterIP(20/40) + UDP(8) + LISP Header(8)

IPv4/v6 RLOC	UDP Port 4341	LISP Header	IPv4/v6 EID	Payload

- LISP Header
  Instance ID can be used for EID virtualization (like Vlan ID or VPN label)

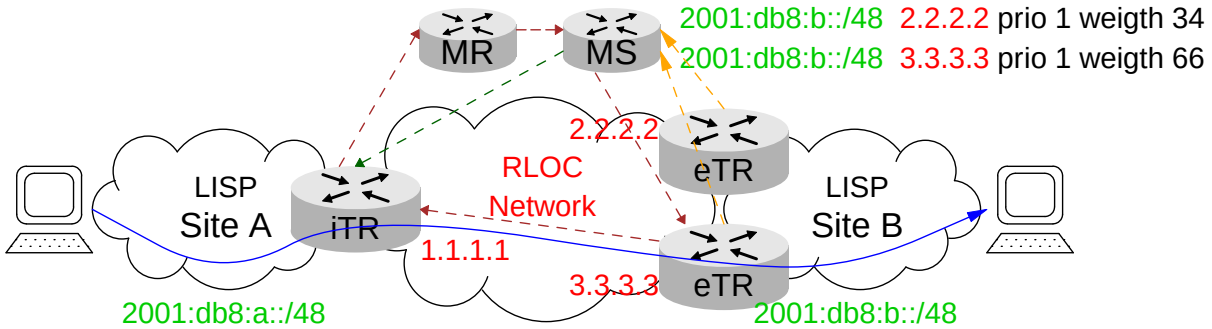


Nonce-present; **L**ocator-Status-Bits; **E**cho-nonce-request; map-**V**ersion; **I**nstance-id

LISP Details

LISP data plane

- Ingress Tunnel Router (iTR) encapsulate LISP packets
  Mapping of EID to RLOC via map cache (LISP forwarding table)
- Egress Tunnel Router (eTR) decapsulate LISP packets



LISP control plane

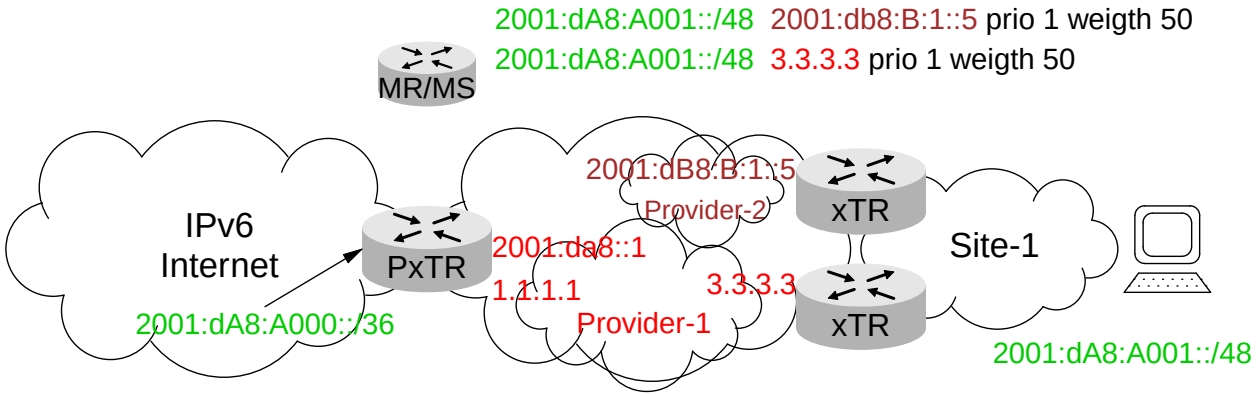
- eTR must register EID with current RLOC
  priority and weigth can be set for active/standby or loadsharing configuration
- Communication eTR → Map Server (MS) is authenticated (PSK)
  Map Server is authoritative only for configured prefixes
- Map Resolver (MR) is used by iTR to request mapping EID → RLOC
  MS can forward the request to an eTR or answer itself (ProxyMode)

LISP Details (Control plane)

- LISP Control Plane packets using UDP port 4342
  - Map-Request / Map-Reply
  - Map-Register / Map-Notify
- Different protocols for MR ⇔ MS communication available
  Only two are deployed: LISP + ALT and LISP DDT
- ALT: Alternative Logical Topology (RFC 6836)
  - Hierachical, 3 Tier BGP network for EID prefixes
  - GRE Tunnel between BGP speakers
  - MR/MS are part of the ALT network
  - EID→RLOC request is forwarded through ALT network
  - Formaly used by the LISP beta network
- DDT: Delegated Database Tree (draft-ietf-lisp-ddt)
  - A (reverse) DNS like approach
  - Root DDT servers needed for MS delegation
  - Actually used by the LISP beta network (since May 2012)

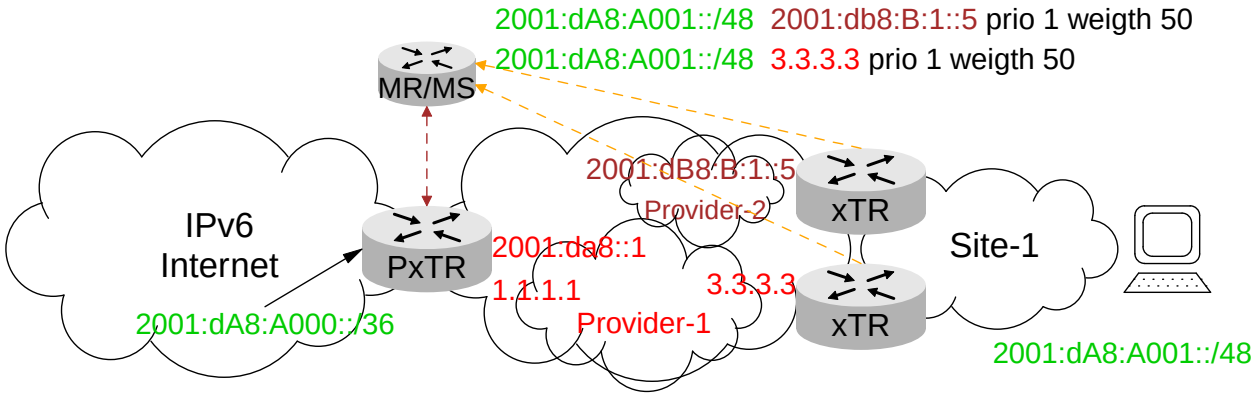
LISP for Internet connectivity (LISP Provider)

- Assume one LISP site is „The Internet“
  xTR is replaced by Proxy-xTR (PeTR + PiTR) (RFC 6832)
- LISP provider runs Map Server/Resolver and the Proxy-xTR
  PiTR announces aggregate for all EID sites
- Customer gets a prefix and a key to register it at the Map-Server
  Like DynDNS in todays IPv4 world, but now for an entire (IPv4/IPv6) prefix



LISP for Internet connectivity (LISP Provider)

- Assume one LISP site is „The Internet“
  xTR is replaced by Proxy-xTR (PeTR + PiTR) (RFC 6832)
- LISP provider runs Map Server/Resolver and the Proxy-xTR
  PiTR announces aggregate for all EID sites
- Customer gets a prefix and a key to register it at the Map-Server
  Like DynDNS in todays IPv4 world, but now for an entire (IPv4/IPv6) prefix



- Site-1 probably must `use-petr` to encap non-LISP destination traffic
  Otherwise traffic could be blocked by access provider (BCP48 filtering)

LISP Applications

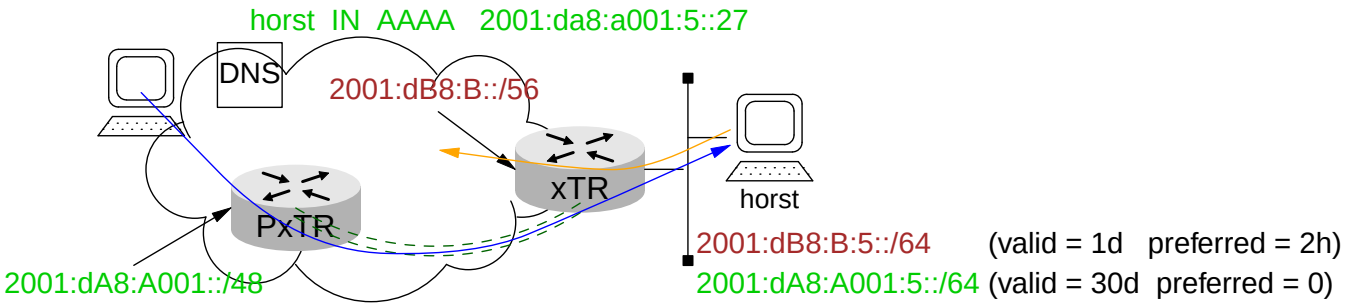
- Provide stable IPv6 Prefix (/48 or /56)
  - to IPv4-only sites (w/ or w/o static IPv4 address)
  - to sites with dynamic IPv6 prefix (LISP can handle dynamic RLOCs)
  - to sites with only one subnet (/64)
  - Can also provide a stable IPv4 prefix (But who cares about IPv4?)
- Simple and efficient Multi-Homing
  - Multihoming via different service provider networks
  - Different access technologies (DSL/Cable/LTE)
  - Active/Standby or load sharing possible (Ingress traffic engineering)
  - Locator Satus Bits (LSB) used for failure signalisation
  - Minimal traffic disruption on active flows

LISP Applications II

- Concurrent use of dynamic & stable IPv6 prefix
  - Stable prefix for remote inititated (incoming) traffic (services)
  - Dynamic prefix for local initiated (outgoing) traffic (privacy)
  - Advertise stable (LISP) prefix with preferred lifetime of 0

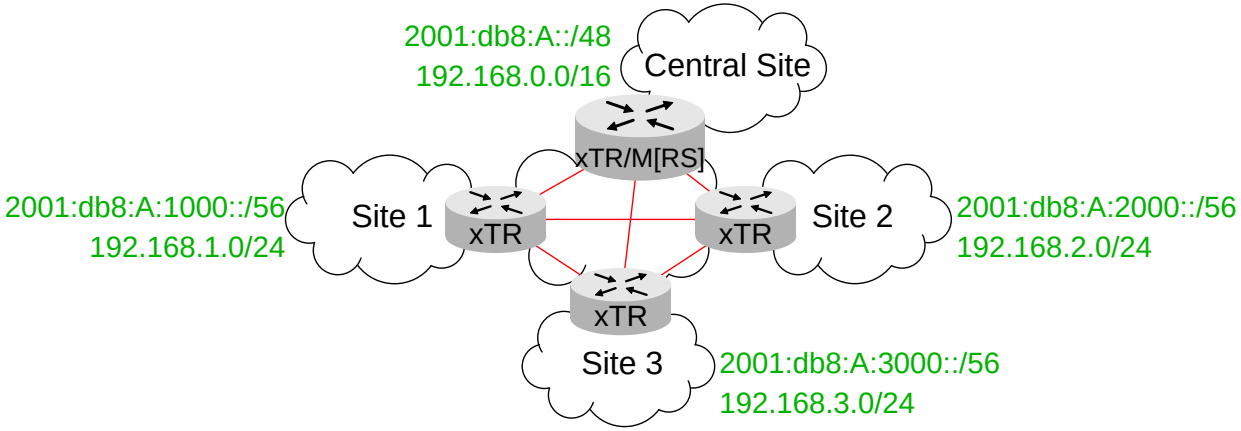
```
int fa0/1
  description LAN interface services&privacy
  ipv6 address DHCPv6-Prfx ::5:0:0:0:1/64
  ipv6 address 2001:dA8:A001:5:0:0:0:1/64
  ipv6 nd prefix default 86400 7200     ; valid=1d, pref=2h
  ipv6 nd prefix 2001:dA8:A001:5::/64 2592000 0   ; valid=30d, pref=0
```

  - Outgoing traffic with source of EID must be send to PeTR
  - Put EID addresses into DNS



LISP Applications III

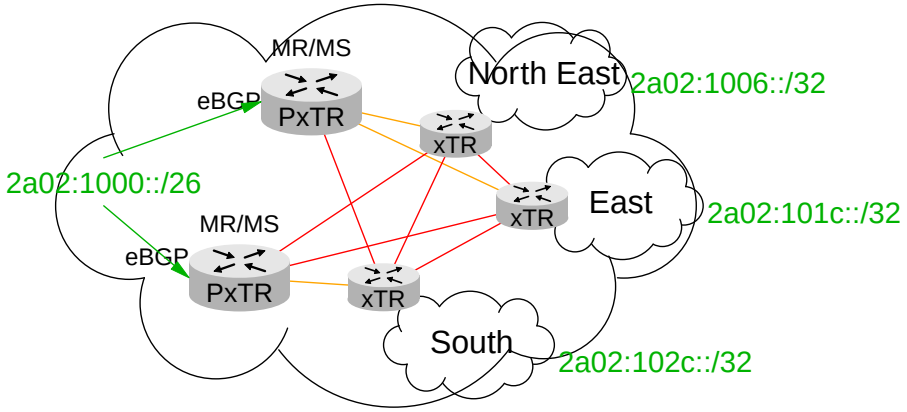
- Provider independent virtual (private) network (PIVN)
  - LISP is an overlay network
  - Any-to-any site interconnection (IPv6/IPv4) with your own prefix
  - Interconnecting public or private EID space



  - Multi VPN site (Different Instance ID (24bit) for traffic separation)
  - Local mapping of instance ID to VRF
  - Privacy: LISP + GETVPN (rloc enc) / GETVPN + LISP (eid enc)
  - LISP + Data Plane encryption (draft-farinacci-lisp-crypto)

LISP Applications IV

- Virtual AS
  - „The Internet“ is build by many autonomous systems (AS)
    Each AS has it’s own physical network and it’s own address space
  - ASes are interconnected via dedicated or shared links
    Address space is announced (routed) via eBGP to other ASes
  - What if you have a large address space (e.g. a /26) ...
    ... but no physical network?
  - Use LISP to build a virtual overlay network
    .. and connect it to the rest of the internet with Proxy-xTR



  - Use DDT to distribute EID prefixes between different MS
    and between other LISP sites / LISP Provider

Summary

- LISP is a routing architecture developed by Cisco
- Network based solution of the Locator/Identifier Problem
- Can be used to solve several problems
  - IPv6 deployment
  - Multihoming
  - Network virtualization
- Can be used independent or interconnected with other LISP sites
  - Use the Delegated Database Tree to „announce“ your LISP prefix
  - With this, LISP can help to decrease the size of the global routing table
- References
  - IETF `http://tools.ietf.org/wg/lisp/`
  - IRTF Routing Research Group `http://trac.tools.ietf.org/group/irtf/trac/wiki/RoutingResearchGroup`
  - LISP Beta Network `http://www.lisp[46].net`

Questions ?

DNSSEC, IPsec, DANE, XMPP, 802.1x, ...

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

... IPv6, LISP, IS-IS, BGP, OpenFlow, Segment Routing

Holger.Zuleger@hznet.de

CONTENTS

Backup Slides

LISP Example Configuration

- iTR

```
router lisp
 ipv6 itr                                              ; use similar commands additional for ipv4
 ipv6 itr map-resolver 4.4.4.4               ; a second (ipv6) map-resolver could be configured
```

- eTR

```
router lisp
 ipv6 etr
 ipv6 etr map-server 4.4.4.4 key xxxx        ; a second map-server is allowed for redundancy
 eid-table default instance-id 0
   database-mapping 2001:db8:2:b00::/56 2.2.2.2 priority 1 weight 50
   database-mapping 2001:db8:2:b00::/56 3.3.3.3 priority 1 weight 50
    or
   database-mapping 2001:db8:2:b00::/56 ipv4 interface Ser0/0 priority 1 weight 50
   database-mapping 2001:db8:2:b00::/56 auto-discover-rlocs
 exit
```

- Map Resolver / Map Server

```
router lisp
 ipv6 map-resolver
 ipv6 map-server
 site Left-Site
  eid-prefix instance-id 0 2001:db8:2:a00::/56
  authentication-key yyyy
 site Right-Site
  eid-prefix instance-id 0 2001:db8:2:b00::/56 accept-more-specifics
  authentication-key xxxx
 exit
```