IPv6 Prefix Alteration – An Opportunity to Improve Online Privacy

Dominik Herrmann, Christine Arndt and Hannes Federrath

University of Hamburg

9th October 2012

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

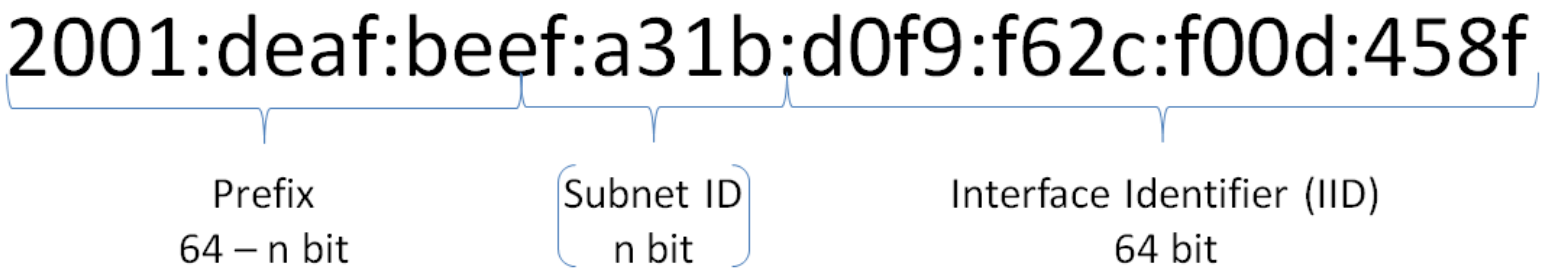
Content

IPv4 Address Exhaustion

~~192.168.1.2~~

fe80::db8:cafe:babe:8a4

New Address Format



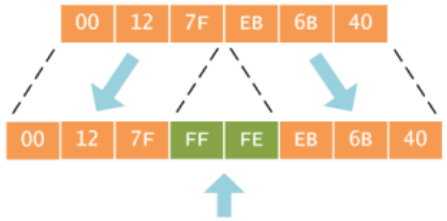
Prefix provided by ISP up to 64 bit
Interface Identifier (IID) derived from host's MAC address

- $3.4 \cdot 10^{38}$ IPv6 addresses
- Implementation of end-to-end principle with static IPv6 addresses

Source: [RFC4291]

Privacy Issues with IPv6

Interface Identifier based on MAC addresses



- Static identifier can be used to keep track of (mobile) nodes' communications and movements

Privacy Extensions

- Randomize IID with MD5 and change over time
- **RFC 3041:** Separate incoming and outgoing connections with stable and temporary addresses
- **RFC 4941:** Configure new IID and en-/disable privacy extentions per prefix
- Tracking due to static IPv6 Prefixes mostly neglected so far

Source: [RFC3041, RFC4941]

Related Work

Sakurai et al. Private communication of two nodes by switching through a list of previously negotiated Interface Identifiers

Dunlop et al. Dynamically obscure sender and receiver addresses

Lindqvist and Tapio Local translation daemon replacing identifiers on all communication layers at once

→ Focus on Interface Identifier only, infeasible for the context of an Internet connection

Raghavan et al. ISPs provide hidden and sticky addresses and NAT gateway to rewrite source and destination addresses

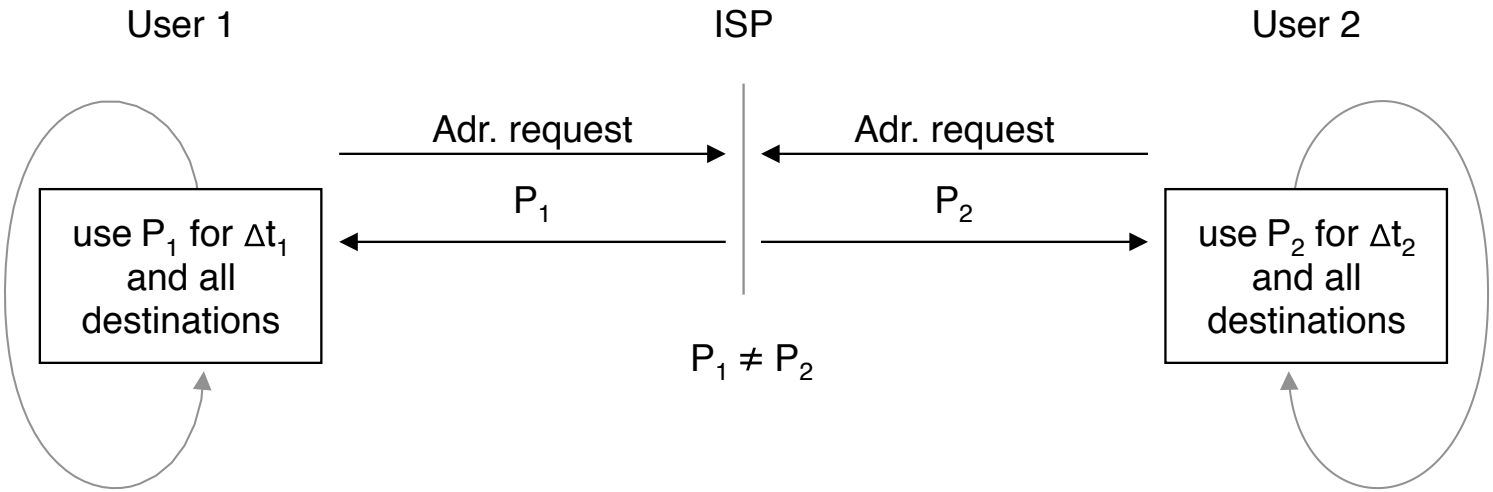
→ Approach resembles our 2^{nd} Prefix Alteration Scheme

Prefix Alteration Schemes

1. Prefix Hopping
2. Prefix Bouquets
3. Prefix Sharing

- Implementation Considerations

Prefix Hopping

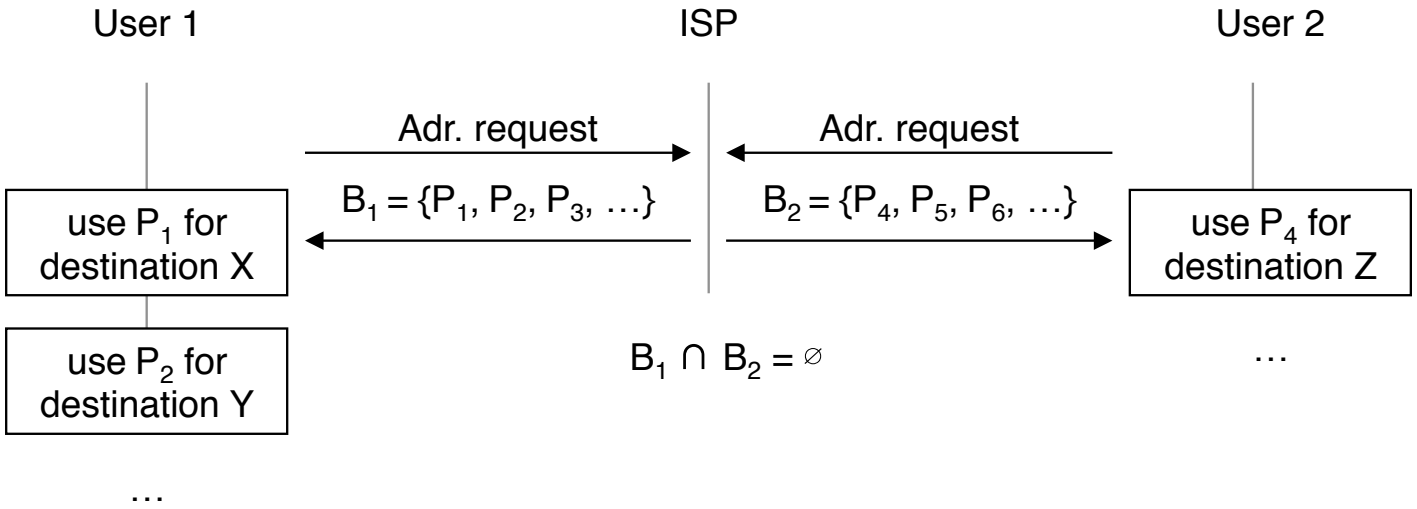


Idea: Changing Prefixes frequently (Δt)

Benefit: Simple implementation, without adjusting existing protocols

Open Issues: Duration of Δt – long-living TCP connections

Prefix Bouquets



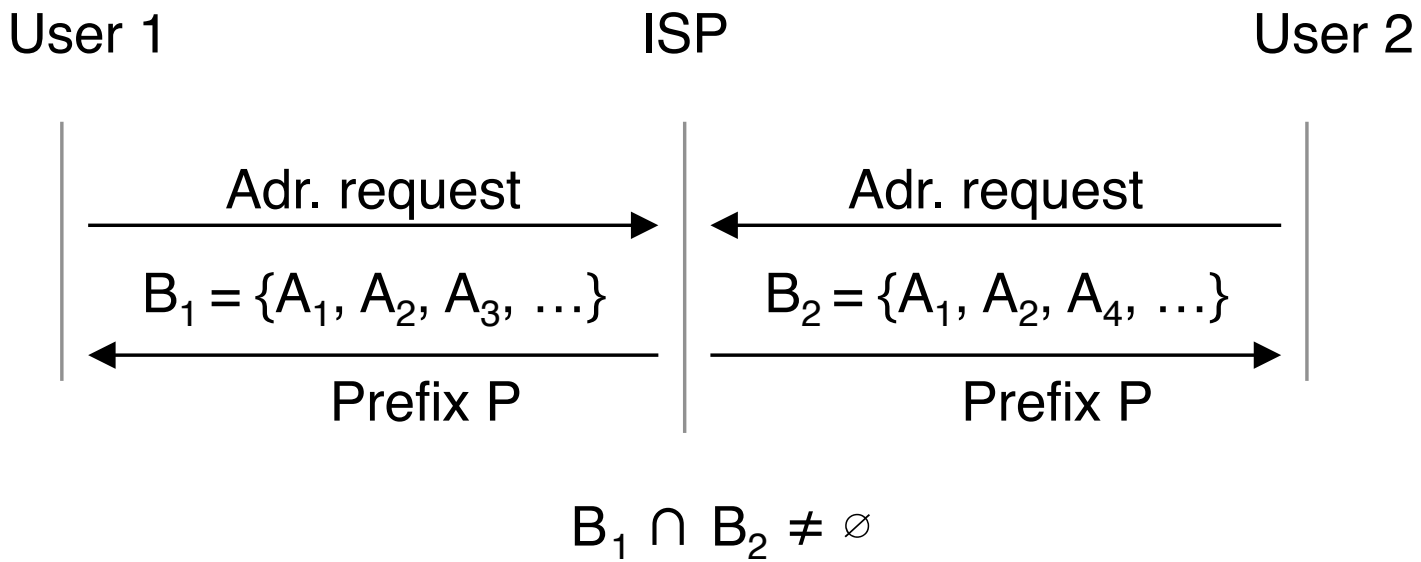
Idea: Split outbound traffic across different Prefixes by

- Destination
- TCP connection
- IP packet

Benefit: Unlinkability on transactional level

Open Issue: May break Cookie-based sessions on some websites

Prefix Sharing



Idea: Multiple customers share the same, common prefix

Benefit: Users form an anonymity group

Open Issue: Address collision

Limitations

- Unlinkability offered only in conjunction with Privacy Extensions
- Prefix Alteration tackles tracking on IP layer only

Open Issues

- Technical implementation
- Who is in control of Prefix alteration: ISP or consunmer's router?
- Increased consumption of IPv6 Prefixes – is it affordable at all?
- Even if one of the schemes proves technically feasible: How to convince ISPs and vendors to put it into practice?

Résumé

- Privacy Extensions solve privacy issue with static Interface Identifiers
- Static IPv6 Prefixes allow third parties to link user actions (communications and movement tracking)
- **Proposed alteration schemes**
  - Prefix Hopping
  - Prefix Bouquets
  - Prefix Sharing
- Open issues and technical implementation have to be considered for realisation

Upcoming introduction of IPv6:
Seldom opportunity to improve privacy

Thank you very much for your attention!