An Investigation Into Teredo and 6to4 Transition Mechanisms: Traffic Analysis

M. Elich, P. Velan, T. Jirsík, P. Čeleda

{elich|jirsik|celeda}@mail.muni.cz, petr.velan@cesnet.cz

The 7th IEEE Workshop on Network Measurements, Sydney, October 21-24, 2013

Part I

Introduction

Motivation and R&D Goals

What are the characteristics of IPv6 transition mechanisms?

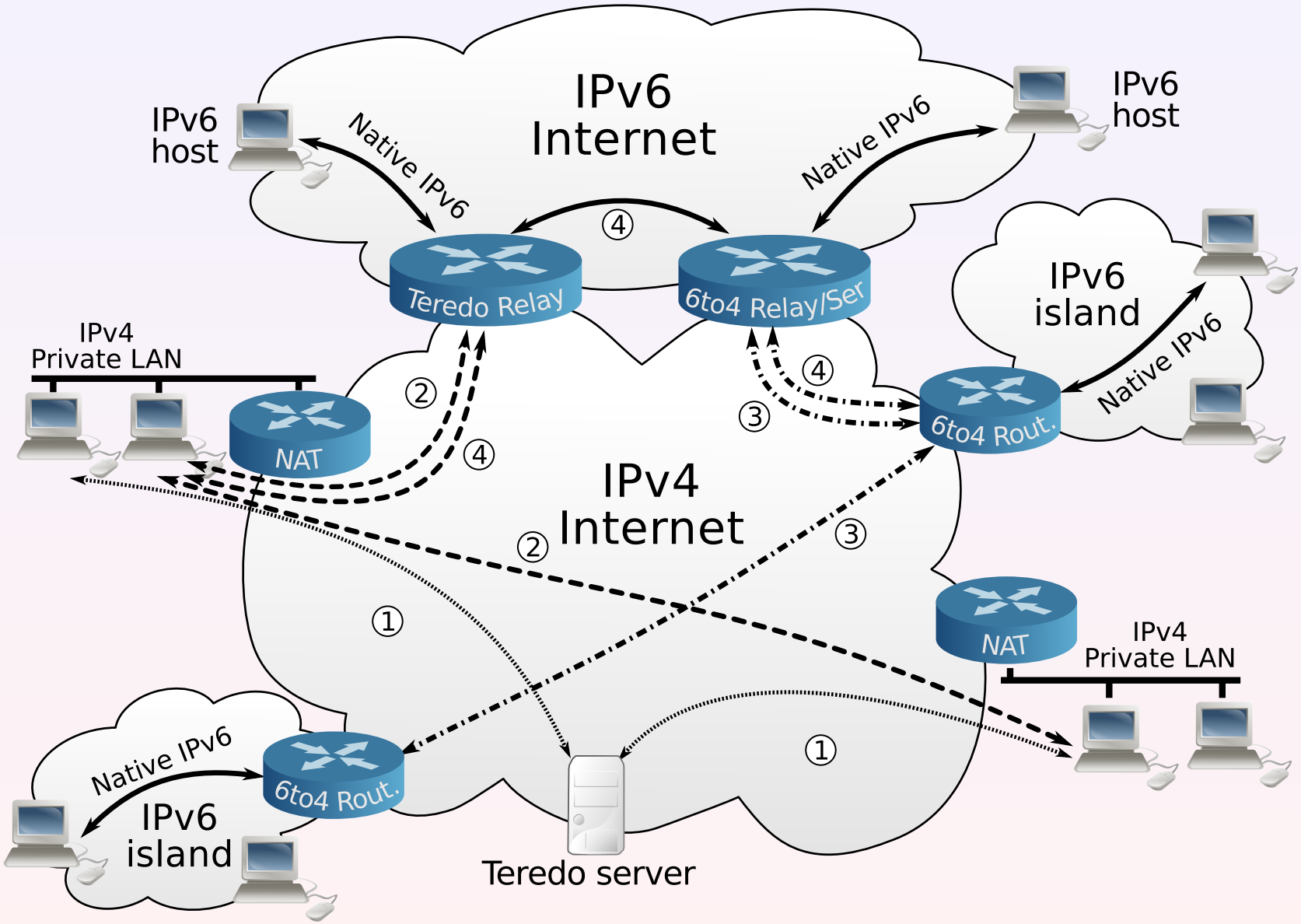
What traffic is tranported using IPv6 transition mechanisms?

What is the impact on native IPv4 and IPv6?

Goals

- **Improve existing framework accuracy/data gathering**
- **Analyze collected flow data to find the answers**

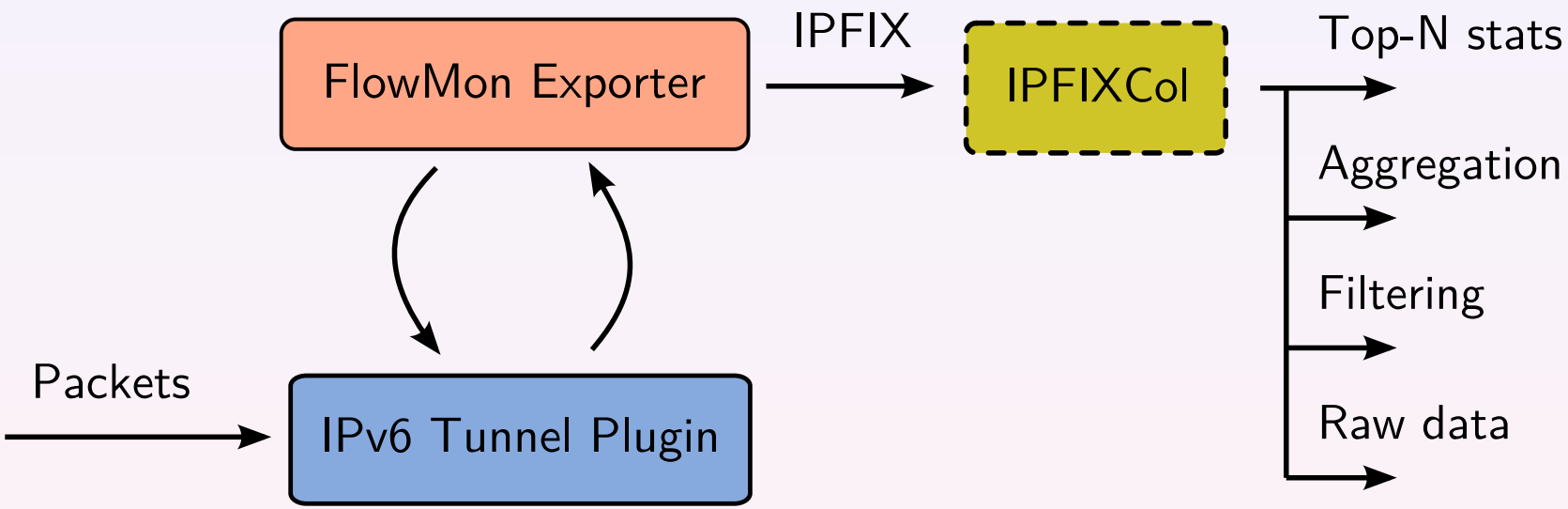
IPv6 Tunnels



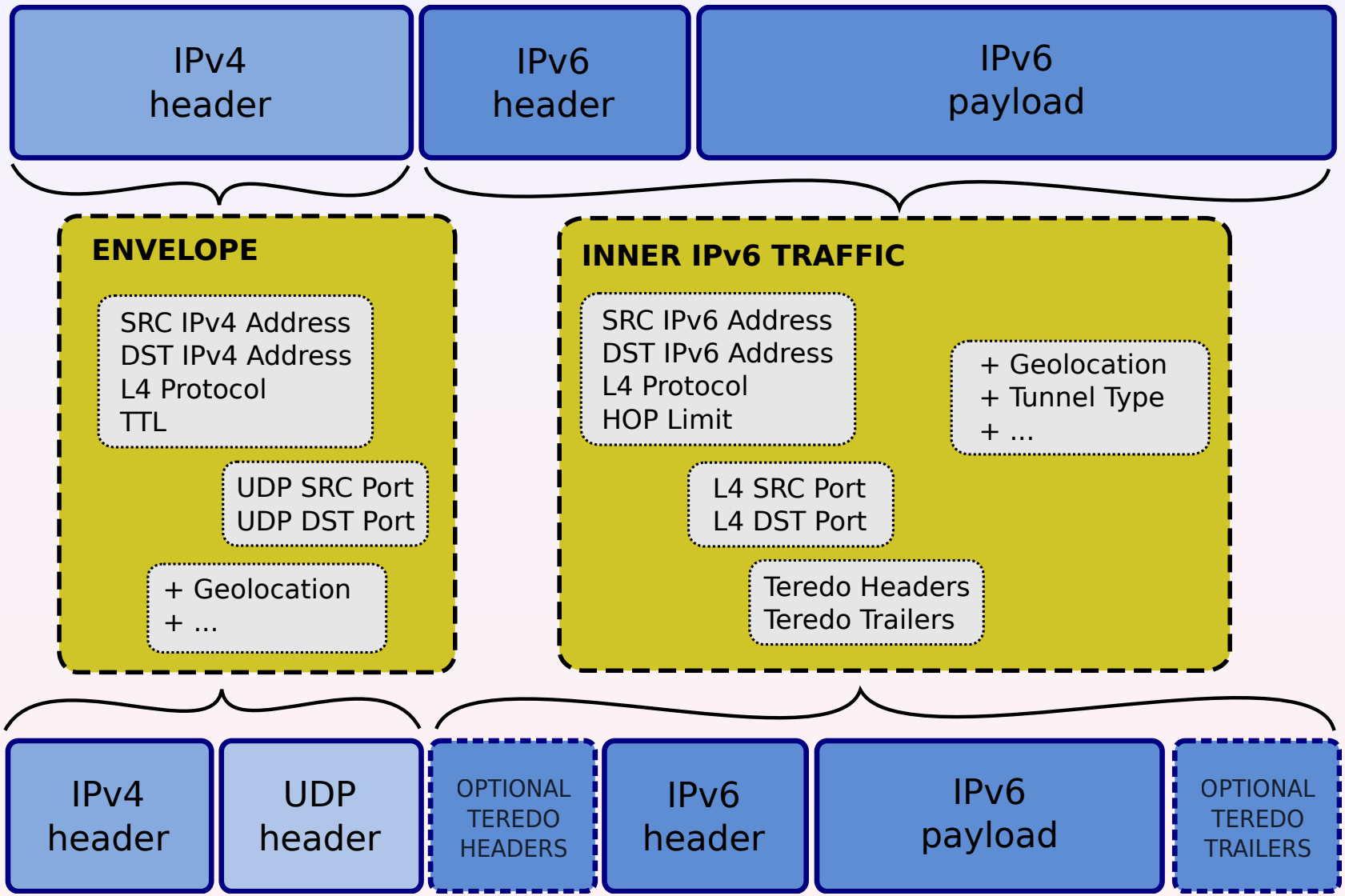
Part II

Monitoring Setup

Monitoring Setup



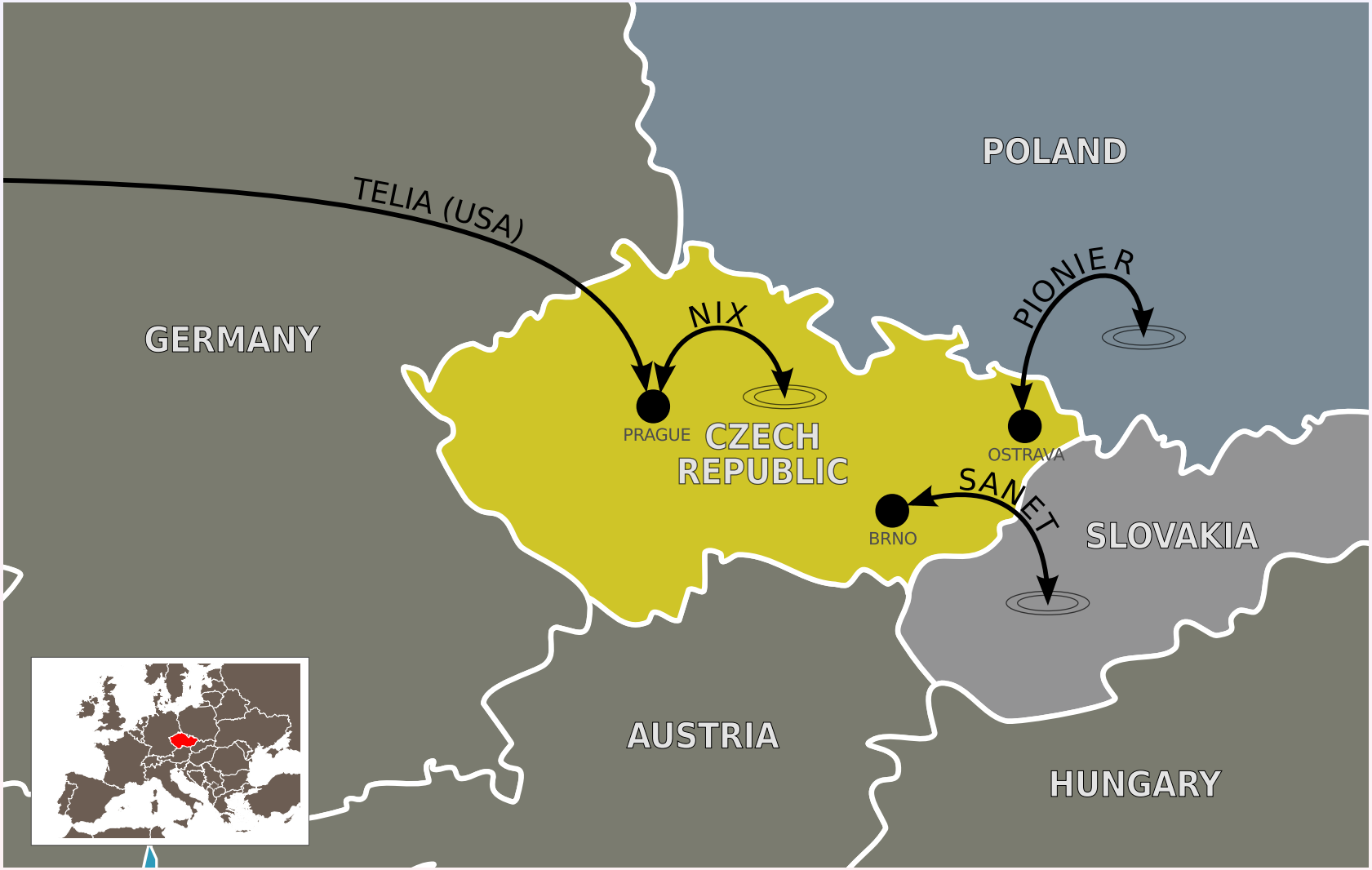
Packet Processing



Part III

Traffic Analysis

Monitored Links



Dataset

IPFIX Flow Data

- Collected over 7 days in January 2013
- No sampling
- Size of 2.45 TB $\sim$ 34 billion flows

Per Flow Information

- Regular flow information
- Encapsulated flow information (as IPFIX Enterprise elements)

Analysis

We analysed following characteristics

- Location of IPv4, IPv6 and tunnel endpoints
- CCDF of flow duration, packets per flow, packet size
- TTL distribution of IPv4 and IPv4 tunnel traffic
- HOP distribution of IPv6 and encapsulated IPv6 traffic
- 6to4 and Teredo frequency
- Port number frequency
- Teredo Servers

CCDF – Highlights

Generally

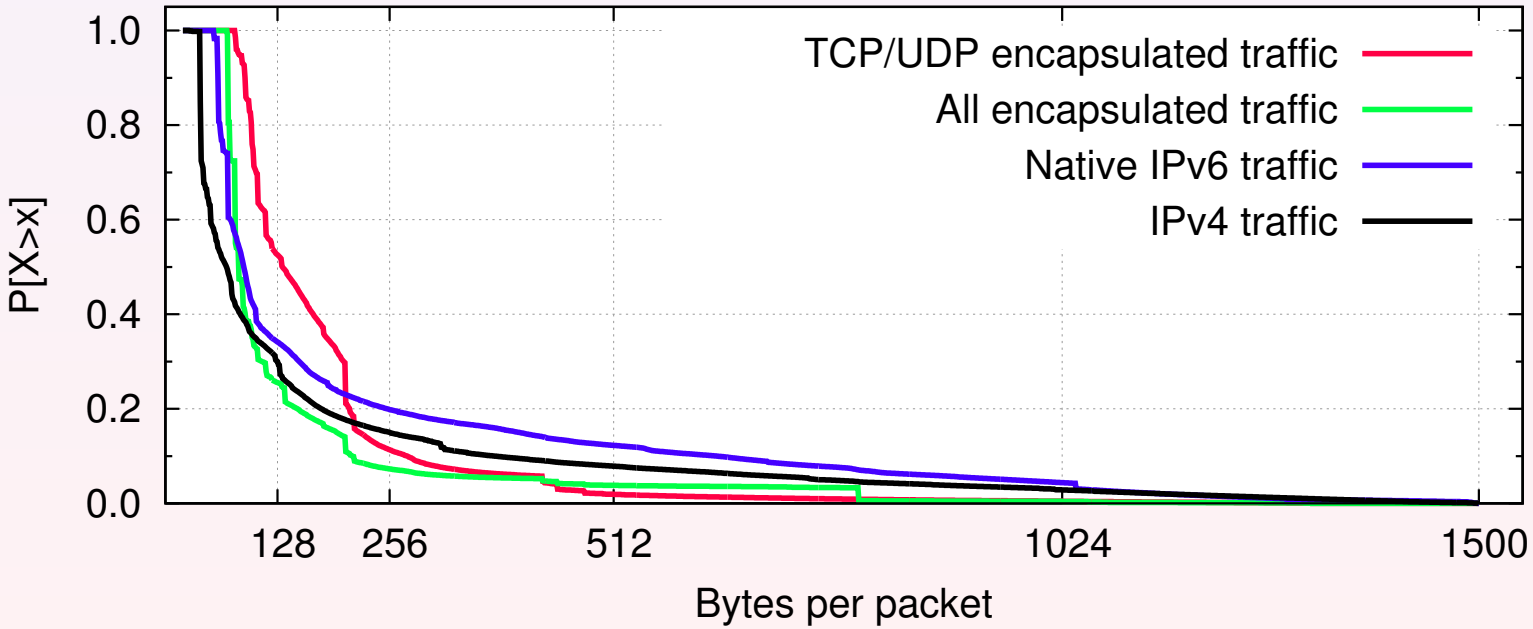
- Most flows are shorter then 10 seconds

Tunneled Traffic

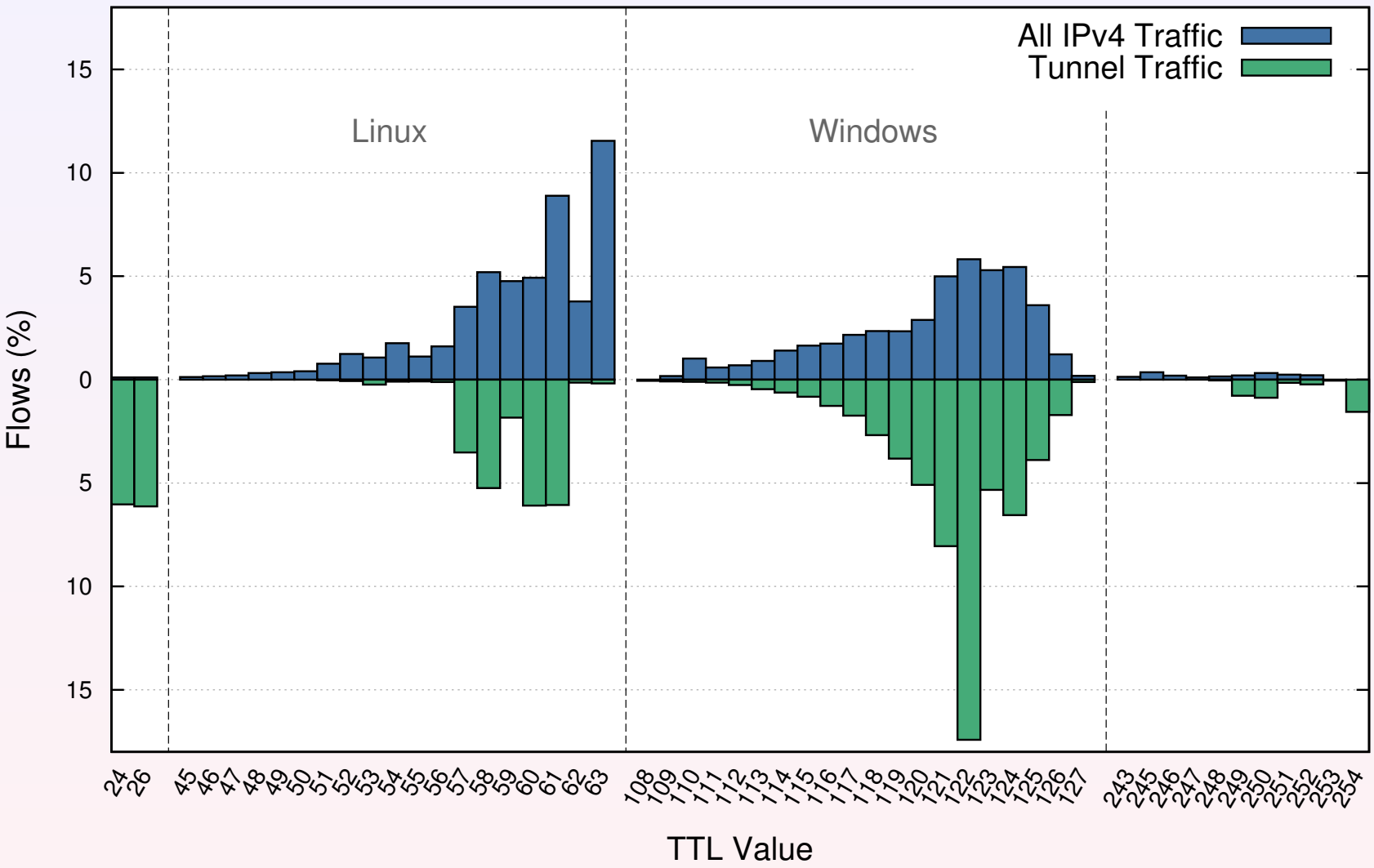
- Fewer short duration flows than IPv4 or IPv6 traffic

Encapsulated Traffic

- Smaller number of packets larger than 400B



TTL distribution



TTL distribution

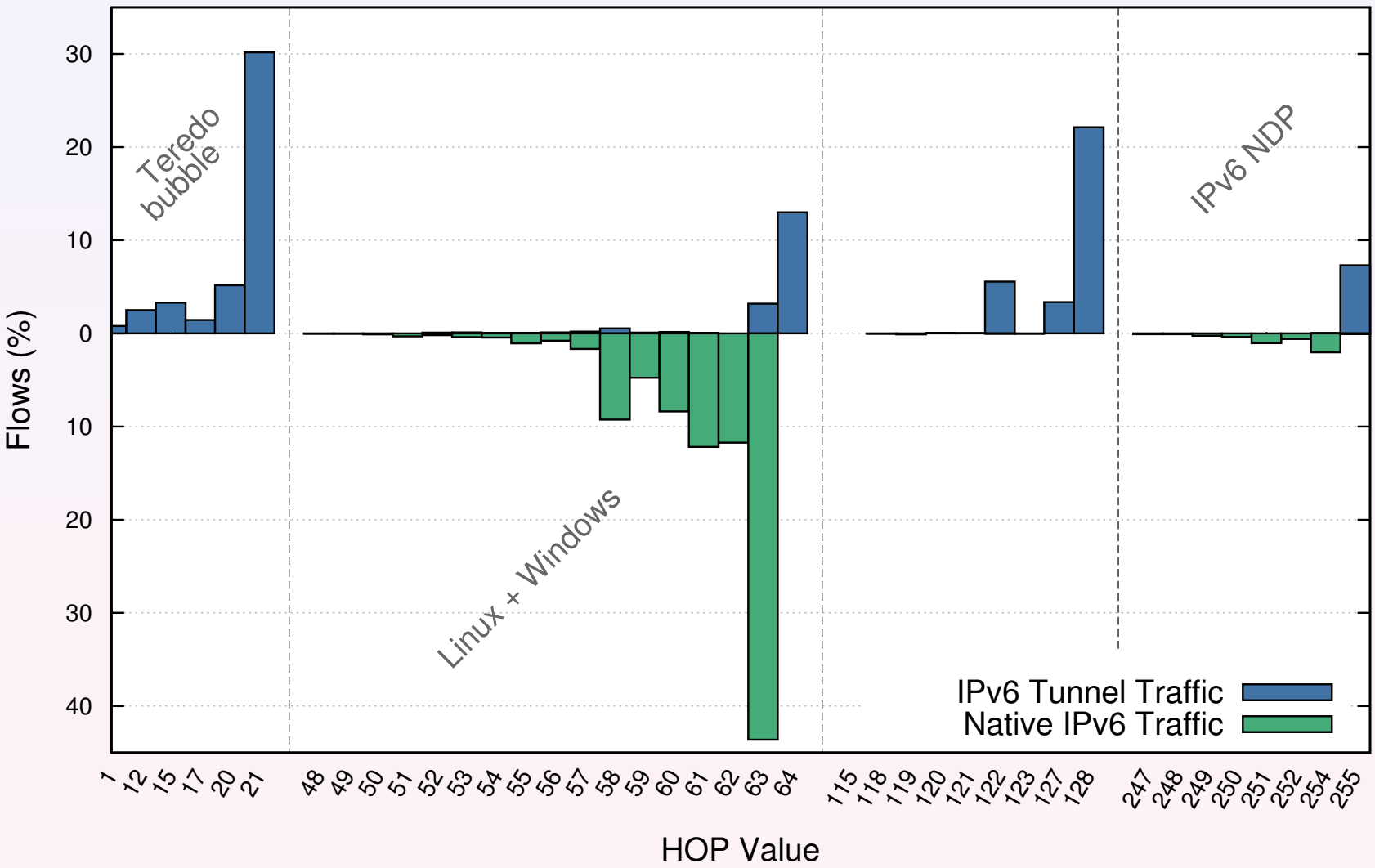
IPv4 traffic containing IPv6 payload

- Windows traffic is taking 60.3 % of the total traffic
- Linux machines is taking 23.8 %
- 6to4 traffic from anycast addresses (TTL 255) is taking 3.8 %
- TTL 1 – 32 makes 12.2 %

IPv4 Traffic

- Larger portion of Linux traffic
- TTL values of 32 and 255 are not as significant

HOP distribution



HOP distribution

Native and Tunneled IPv6 Traffic

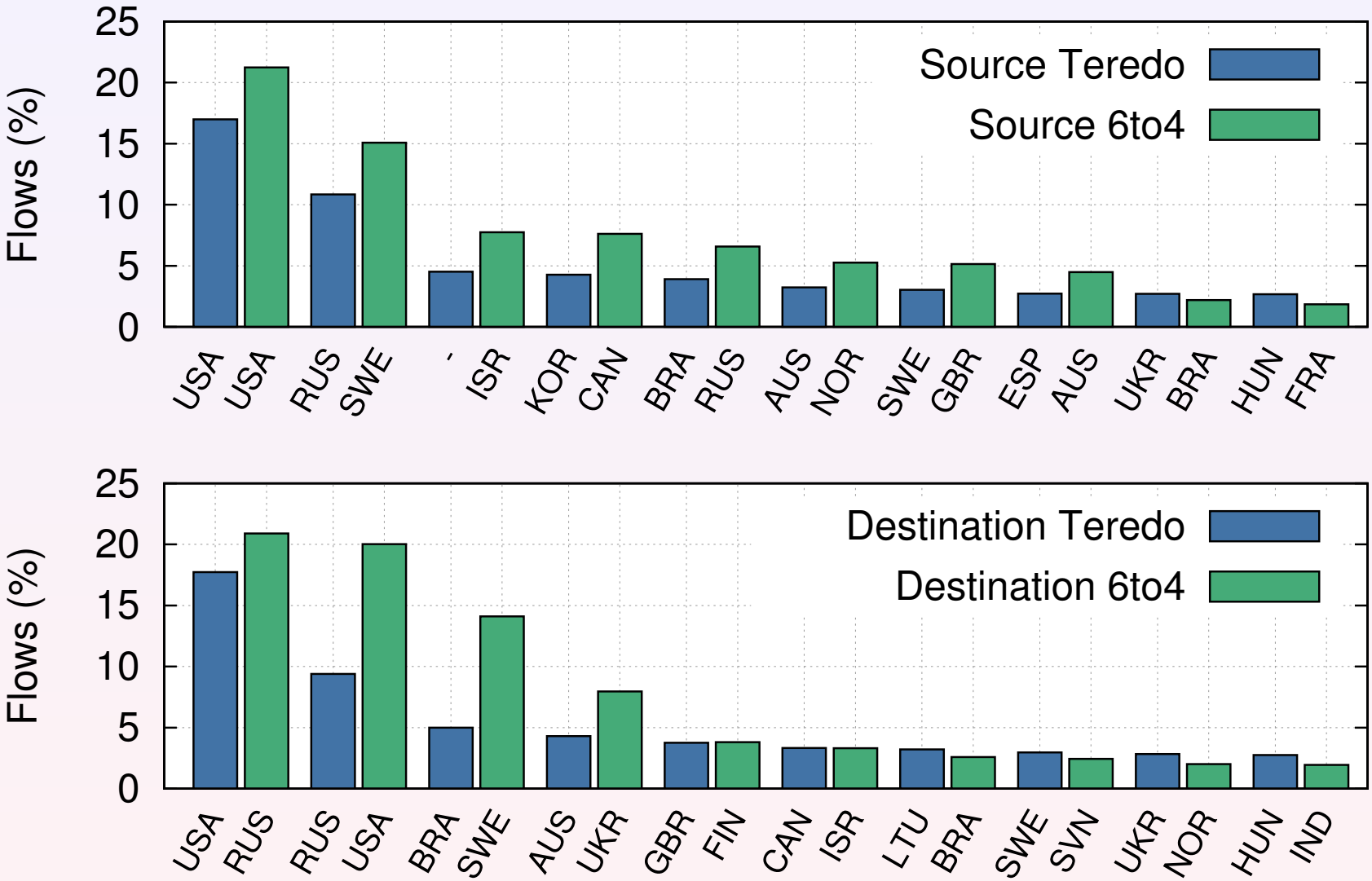
- HOP limit of 51 – 64 is most frequent.

Tunneled traffic

- Values are distributed with much less entropy
- Limits 21, 64, 128 and 255 are the most frequent
  - Value 21 is used for Teredo bubbles by Windows
  - Value 255 is used for IPv6 neighbor discovery messages
- Traffic never traversed the IPv6 network

  $\Rightarrow$ HOP limit untouched

Location of Tunnel Endpoints



Historical Comparison

Historical Traffic

- We measured tunneled IPv6 traffic in 2010
- CESNET links to SANET, PIONIER and NIX

Comparison

	2010		2013	
	flows	**bytes**	**flows**	**bytes**
Tunneled IPv6	1.5 %	0.66 %	1.5 %	1.28 %
Native IPv6	0.1 %	0.21 %	3.4 %	4.42 %
HTTP(s), DNS	1.0 %	-	5.5 %	- %

Part IV

Conclusion

Conclusion

Summary

- Tool for investigating IPv6 tunneled traffic
- Teredo and 6to4 traffic behavior
- Understanding of encapsulated IPv6 traffic

Future Work

- Security analysis of tunneled IPv6 traffic
- Detection methods development

Thank You For Your Attention!

An Investigation Into Teredo and 6to4 Transition Mechanisms: Traffic Analysis

P. Velan

petr.velan@cesnet.cz

M. Elich, T. Jirsík, P. Čeleda

{elich|jirsik|celeda}@mail.muni.cz

IPv6 Tunnel Monitoring Plugin

http://www.muni.cz/ics/920232/web/ipv6-tunnel-plugin