Introducing the Path Aware Networking (PAN) proposed RG

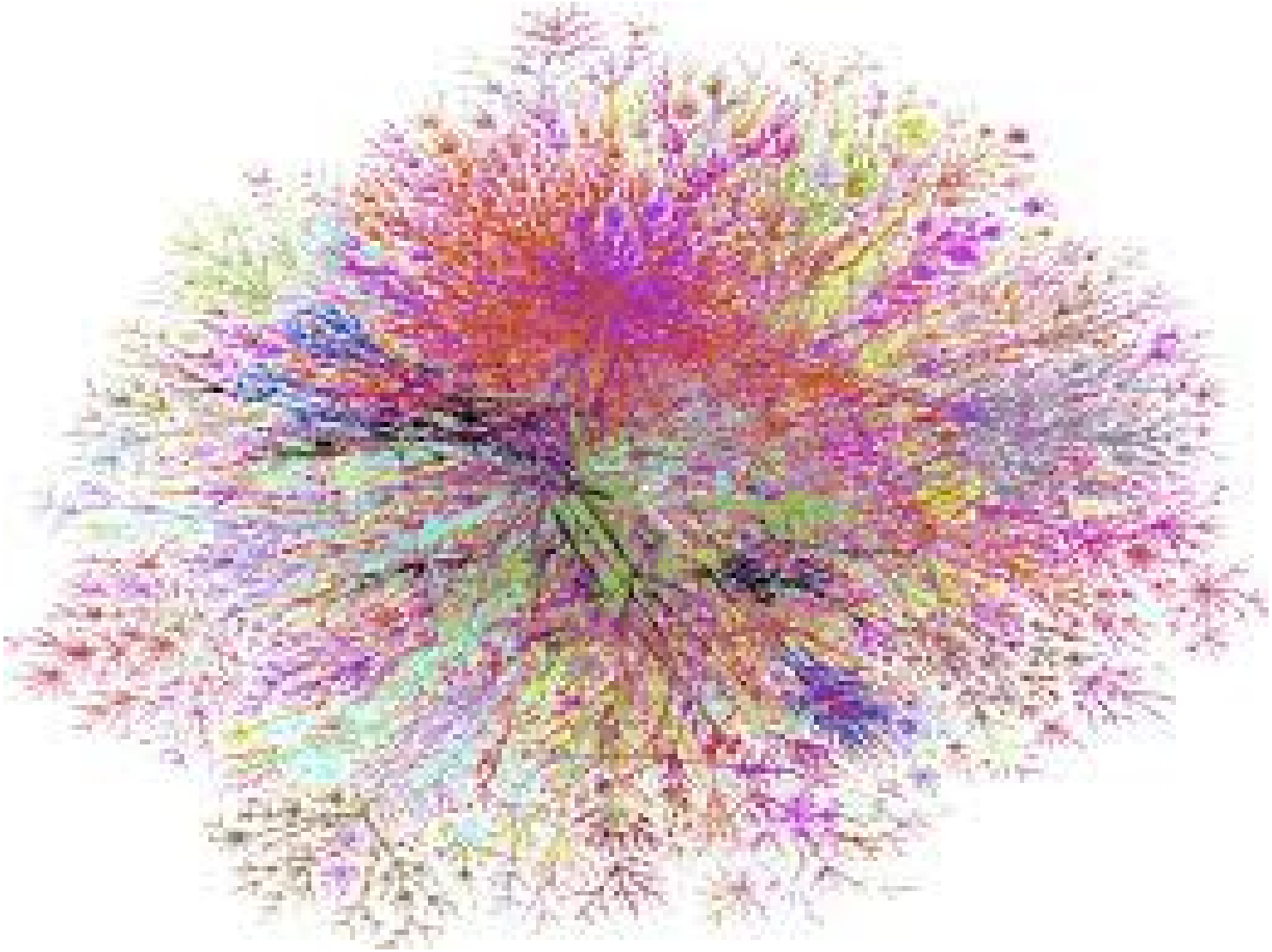
Jen Linkova

based on PANRG presentation by
Olivier Bonaventure

UCLouvain, Belgium

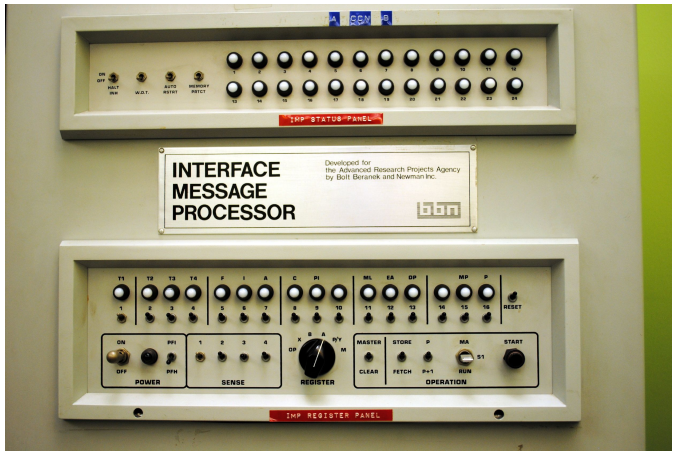
http://inl.info.ucl.ac.be

What could path awareness mean ?



Our starting points

Lucky endhosts have one network interface



Routers have several network interfaces

Today's environment

Routers and endhosts have several network interfaces

The host/network interface

- What does an endhost know about the network ?
  - Embarrassingly, nothing…

Network paths : dumb host and intelligent routers

- Routers manage network paths and need to be informed about their availability and characteristics
  - Intradomain versus interdomain paths
  - Scalability
- Endhosts only need connectivity and thus they should not bother with the network paths

Reliability
Intelligent hosts and dumb routers

- Endhosts require reliable data transfer for some applications and thus need to deal with losses/retransmissions/…
  - Transport protocols
  - Congestion control

- Routers should only forward packets without caring about their content
  - They queue and may drop (mark ?) packets when overloaded

Defining path awareness

- How can we define path awareness ?
  - Control plane viewpoint
    - How can an endhost learn the existence/availability/characteristics of different network paths ?
  - Data plane viewpoint
    - How can an endhost request the utilisation of a specific path to the network ?

Why a new RG?

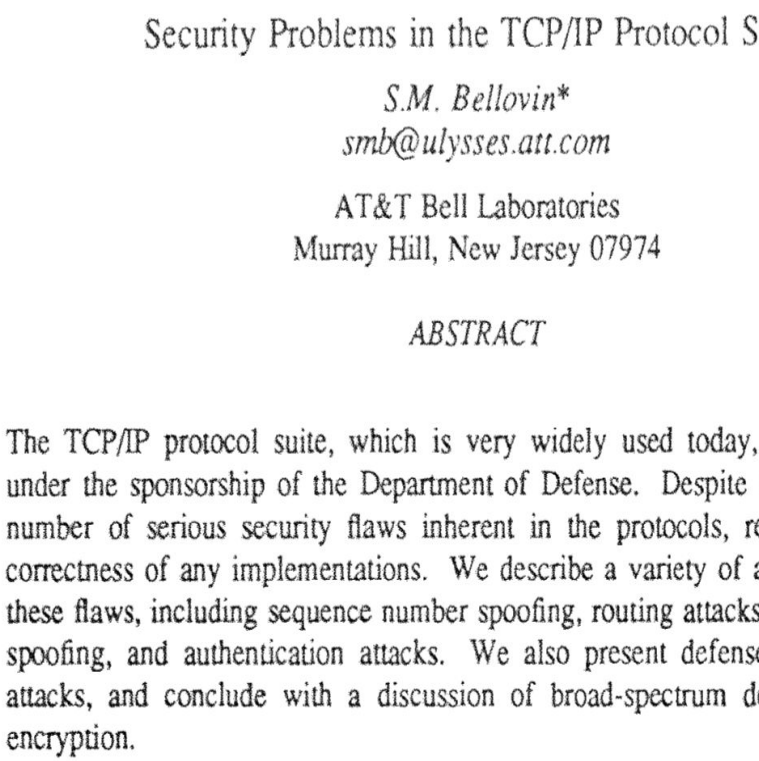
We identified a common theme* of *path awareness* in a lot of research on the edge of standardization in the IETF:

- multipath transport protocols (MPTCP, future QUIC)
- hybrid access approaches (BANANA BoF, MPTCP)
- emerging path control approaches (SFC, SPRING)
- dynamic interface/transport selection (MIF, TAPS)
- work on path signaling (IAB stackevo, PLUS, ALTO)

*please don’t feel bad if we missed your favorite path-aware WG

Failed opportunities for path awareness

- IPv4 Source routing
  - Token Ring networks used similar principles
  - Endhosts can encode strict or loose source route in their packets, but
    - IP header restricts route length
    - How do endhosts learn paths?



Security Problems in the TCP/IP Protocol S

*S.M. Bellovin**
smb@ulysses.att.com

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

ABSTRACT

The TCP/IP protocol suite, which is very widely used today, under the sponsorship of the Department of Defense. Despite number of serious security flaws inherent in the protocols, re correctness of any implementations. We describe a variety of a these flaws, including sequence number spoofing, routing attacks spoofing, and authentication attacks. We also present defens attacks, and conclude with a discussion of broad-spectrum d encryption.

Failed opportunities for path awareness

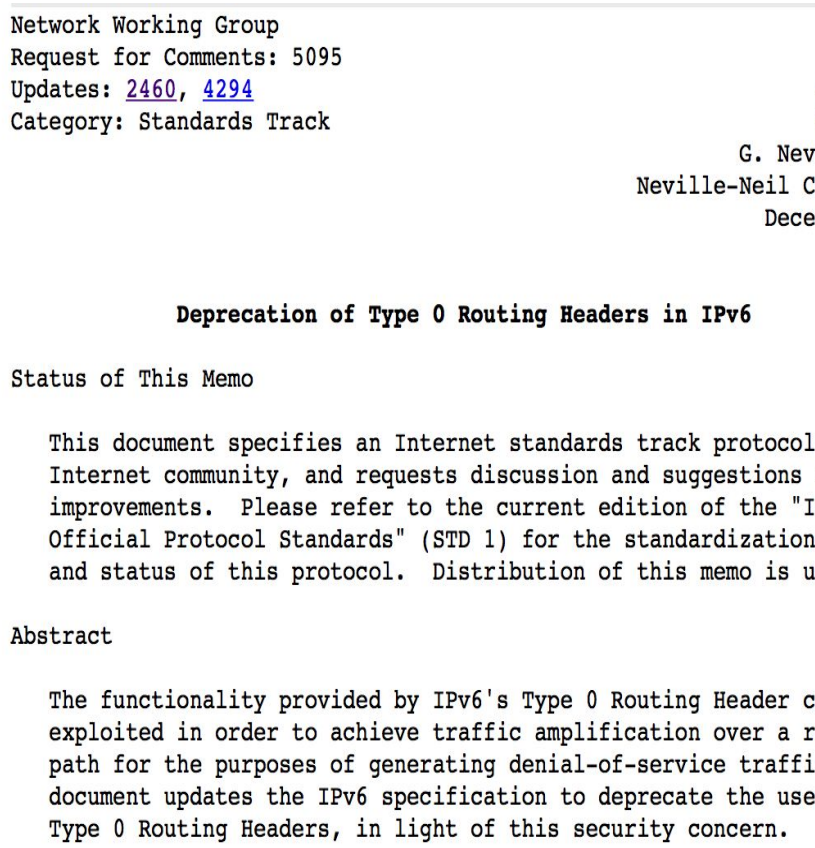
- Integrated services
  - Researcher's viewpoint
    - Endhost signals path requirements using signalling protocol
    - Network finds path most appropriate path using QoS routing
  - Solution adopted by IETF
    - Endhost signals path requirement with RSVP
    - RSVP messages are forwarded along shortest path selected by IGP and reserve resources on this path

Failed opportunities for path awareness

- Differentiated services and ToS routing
  - Researchers' viewpoint
    - Endhosts mark packet with different DSCP values
    - Routers queue/delay/drop packets based on their DSCP
    - Packets are forwarded on paths meeting their requirements
  - Deployed solutions
    - Marking is mainly done by routers
    - Routers queue/delay/drop packets based on their DSCP
    - Some networks use ToS routing or MPLS tunnels to forward packets based on DSCP, but this is opaque for endhost

Failed opportunities for path awareness

- IPv6 Source routing
  - Endhosts can encode strict or loose source route in their packets, but...
    - How do endhosts learn paths ?



Network Working Group
Request for Comments: 5095
Updates: 2460, 4294
Category: Standards Track

G. Nev
Neville-Neil C
Dece

Deprecation of Type 0 Routing Headers in IPv6

Status of This Memo

This document specifies an Internet standards track protocol
Internet community, and requests discussion and suggestions
improvements. Please refer to the current edition of the "I
Official Protocol Standards" (STD 1) for the standardization
and status of this protocol. Distribution of this memo is u

Abstract

The functionality provided by IPv6's Type 0 Routing Header c
exploited in order to achieve traffic amplification over a r
path for the purposes of generating denial-of-service traffi
document updates the IPv6 specification to deprecate the use
Type 0 Routing Headers, in light of this security concern.

Path awareness and host multihoming

- With two or more interfaces, path awareness becomes more critical since can select path without requiring a specific marking in the dataplane

Multihomed host

- Early experience with a multihomed host

Subnet 1

Subnet 2

  - How can it select the best interface ?
    - `routed`

Shim6/HIP

- Basic idea
  - Endhosts have one stable identifier and several locators (one per interface)
  - Transport protocols rely on the identifiers and network layer transparently maps the packets to different locators (and thus paths)
- Status
  - HIP : research prototype
  - Shim6: RFCs and one prototype but no deployment
- Path awareness ?
  - No communication channel between endhost and network

LISP

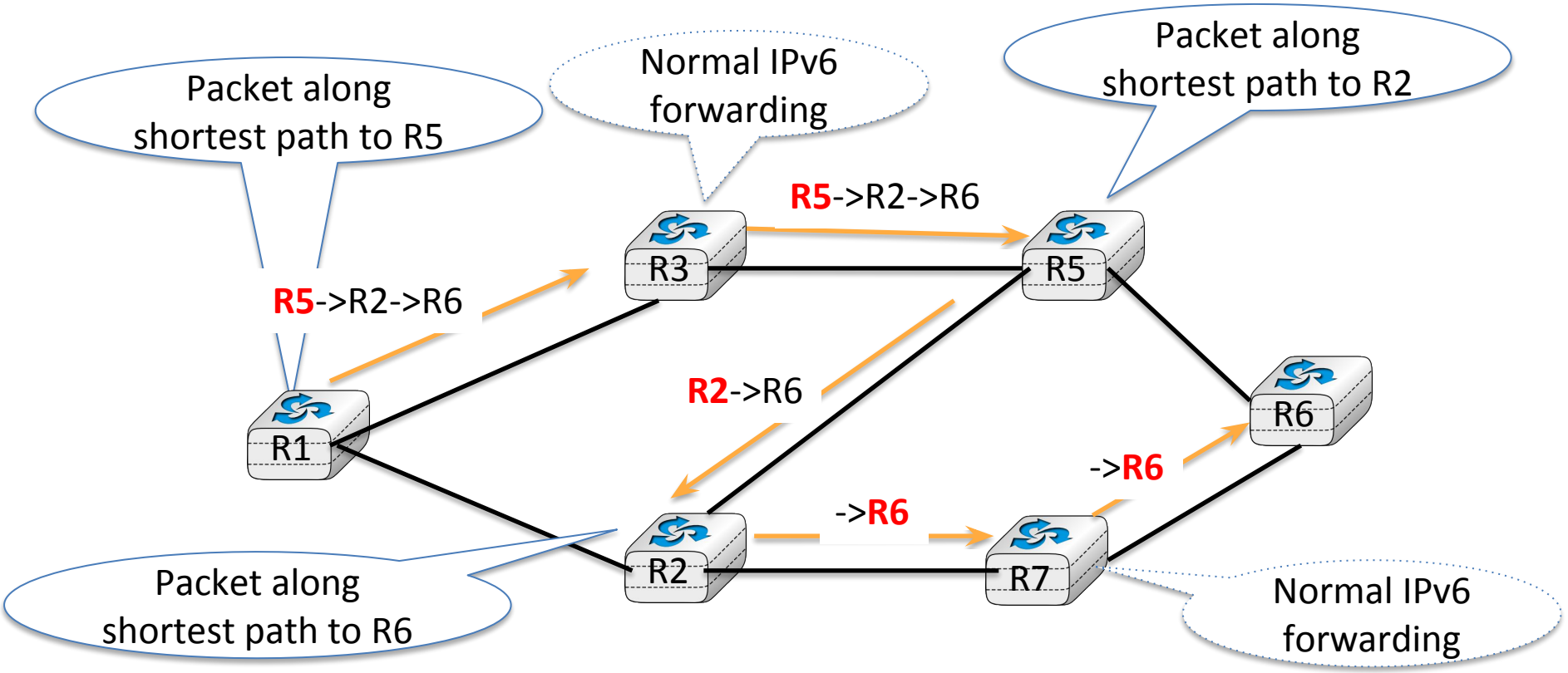
- Endhosts have identifiers that are not injected in the BGP Default Free Zone
  - Helps to scale routing tables
- Locators are attached to border routers
- Border routers map host identifiers onto locators and tunnel packets to reach remote border routers
- Path awareness ?
  - Routers are in control, endhosts are blind

Multipath TCP / SCTP-CMT

- Transport level solution enabling endhosts to use multiple paths
  - Multipath TCP is aware of the utilisation of different paths and can act accordingly
    - Coupled congestion control
    - Retransmissions, reinjections
  - Use cases
    - Datacenters (leveraging ECMP)
    - Smartphones (combining cellular and WiFi)

IPv6 Segment Routing

- Marrying Segment Routing with IPv6

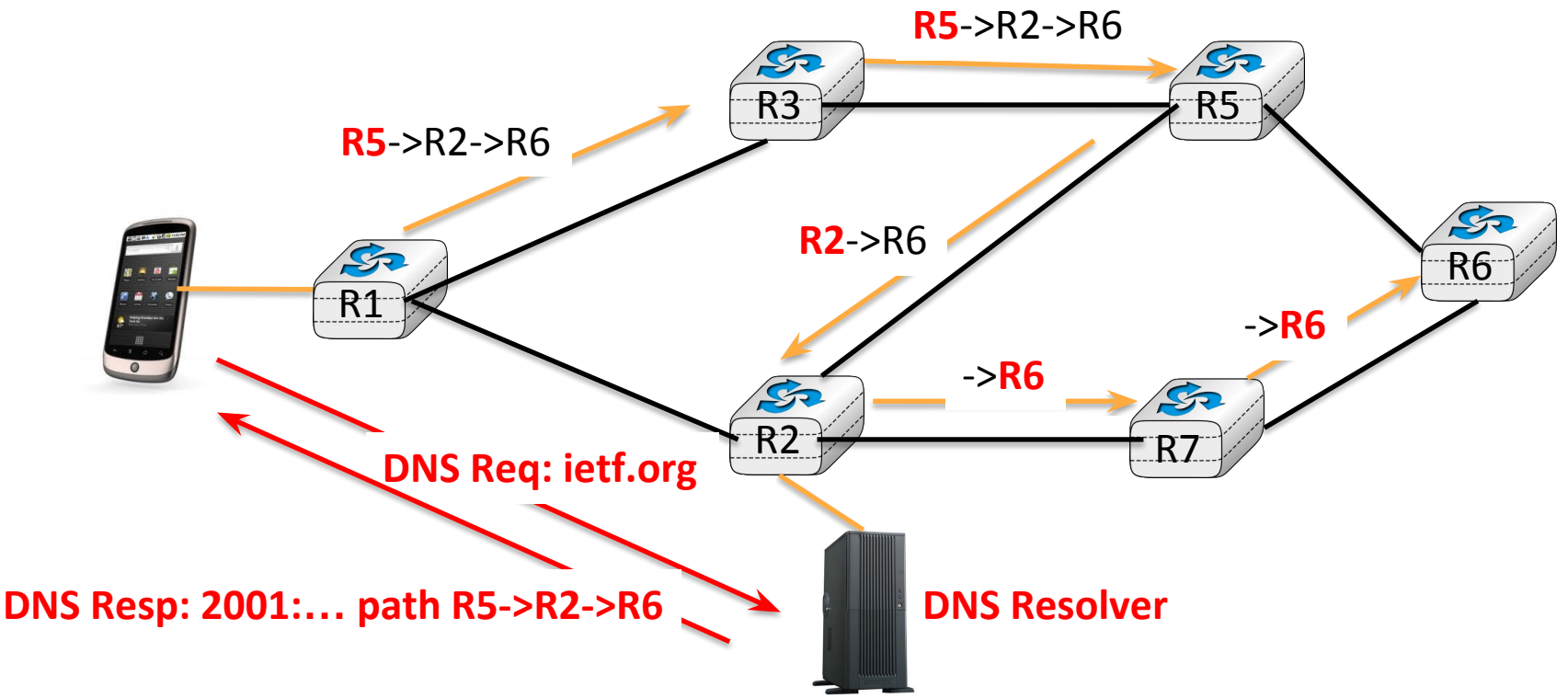


IPv6 Segment Routing

- What does it bring ?
  - A standardised way for endhosts to encode network paths (at least within an IPv6 domain)
- What is missing ?
  - A communication channel between the endhost and the network to enable it to learn the available network paths

The case for intelligent DSN resolvers

- How can endhosts learn the available paths ?



D. Lebrun et al. *Software Resolved Networks: Rethinking Enterprise Networks with IPv6 Segment Routing*, 2017, under submission

Multiple Provisioning Domain

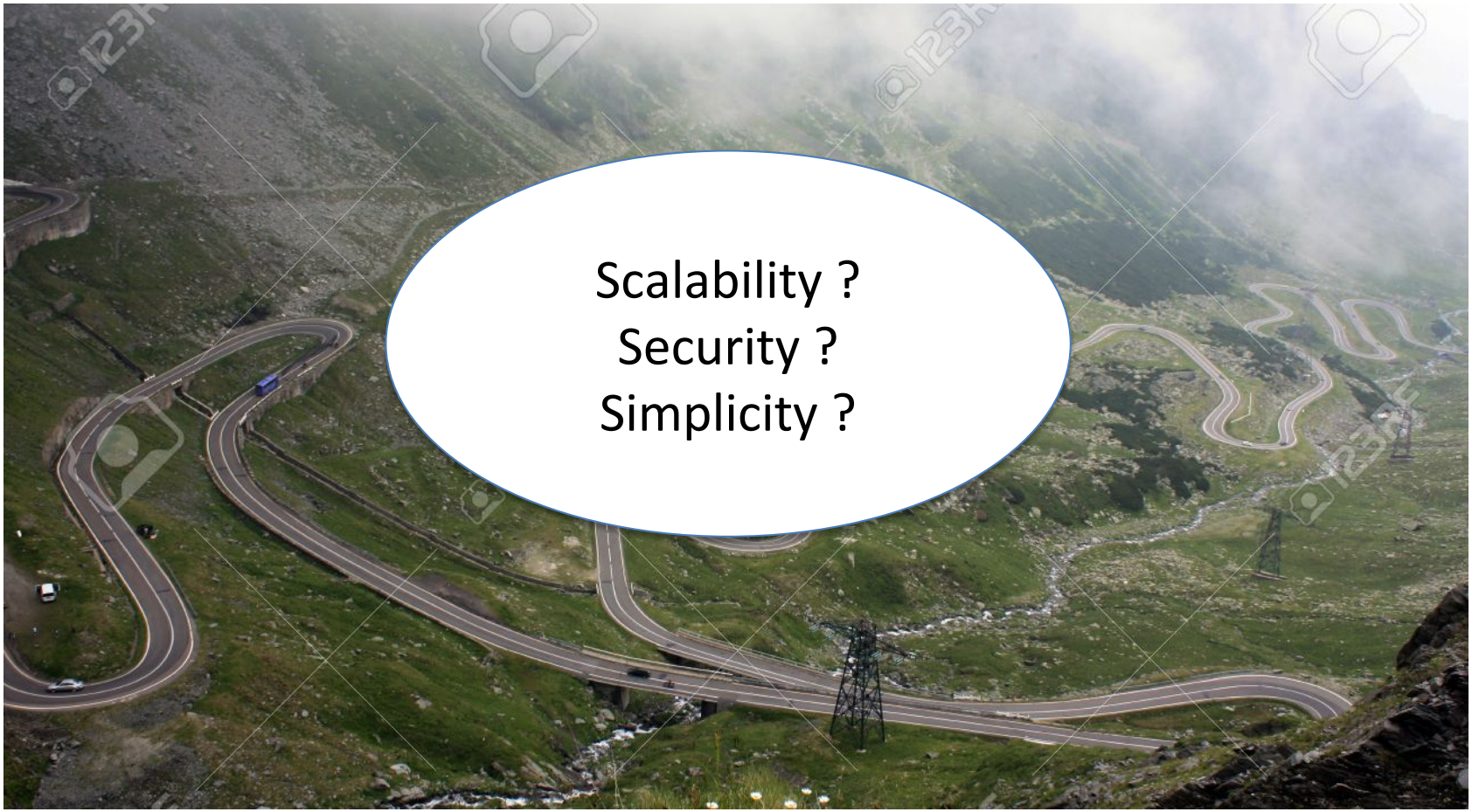
- Provisioning Domain (PvD):
  - A consistent set of network configuration information.
  - MPvD Architecture: RFC7556

- Discovering PvD
  - Via Router Advertisement option
  - draft-bruneau-intarea-provisioning-domains

The political layer of path awareness

- The network operator viewpoint
  - Post office model
    - I invest to build/operate the network and network paths are my sole responsibility. Users should not interfere
- The enduser viewpoint
  - Car driver model
    - I pay to use the network and should be able to autonomously select the best network path for my packets

The road to path awareness won't be easy but should be interesting



Getting Involved

Join the mailing list: panrg@irtf.org

Meeting in Singapore will have a better conflicts list; to propose topics/presentations, contact the chairs:

Jen Linkova <furry13@gmail.com>

Brian Trammell <ietf@trammell.ch>