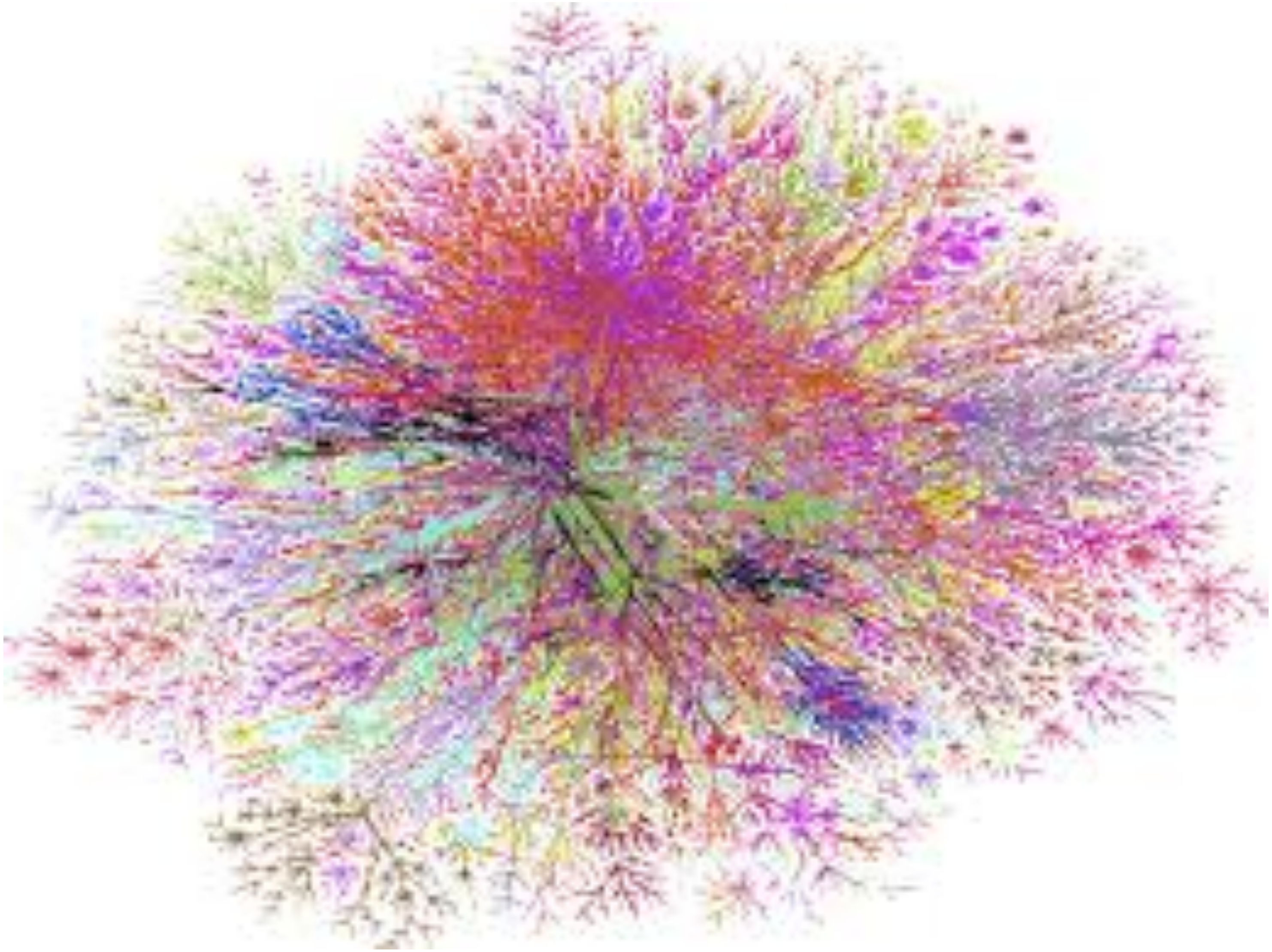
A Decade of Path Awareness

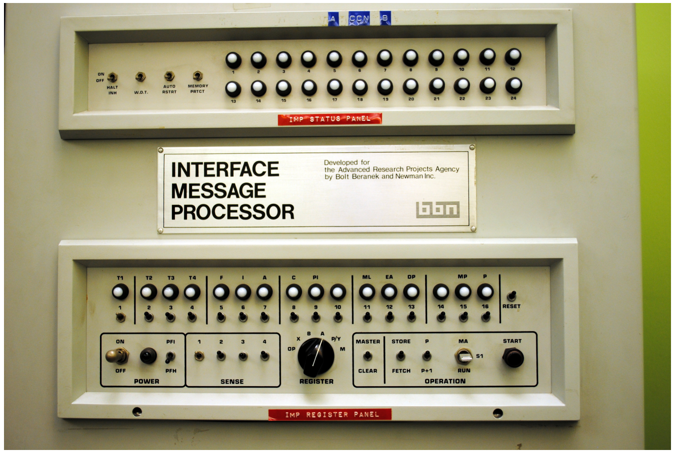
Olivier Bonaventure
UCLouvain, Belgium
http://inl.info.ucl.ac.be

What could path awareness means ?



Our starting points

Lucky endhosts
have one network
interface


IMP STATUS PANEL
INTERFACE MESSAGE PROCESSOR
Developed for the Advanced Research Projects Agency by Bolt Beranek and Newman Inc.
bbn
POWER
SENSE
REGISTER
OPERATION
IMP REGISTER PANEL

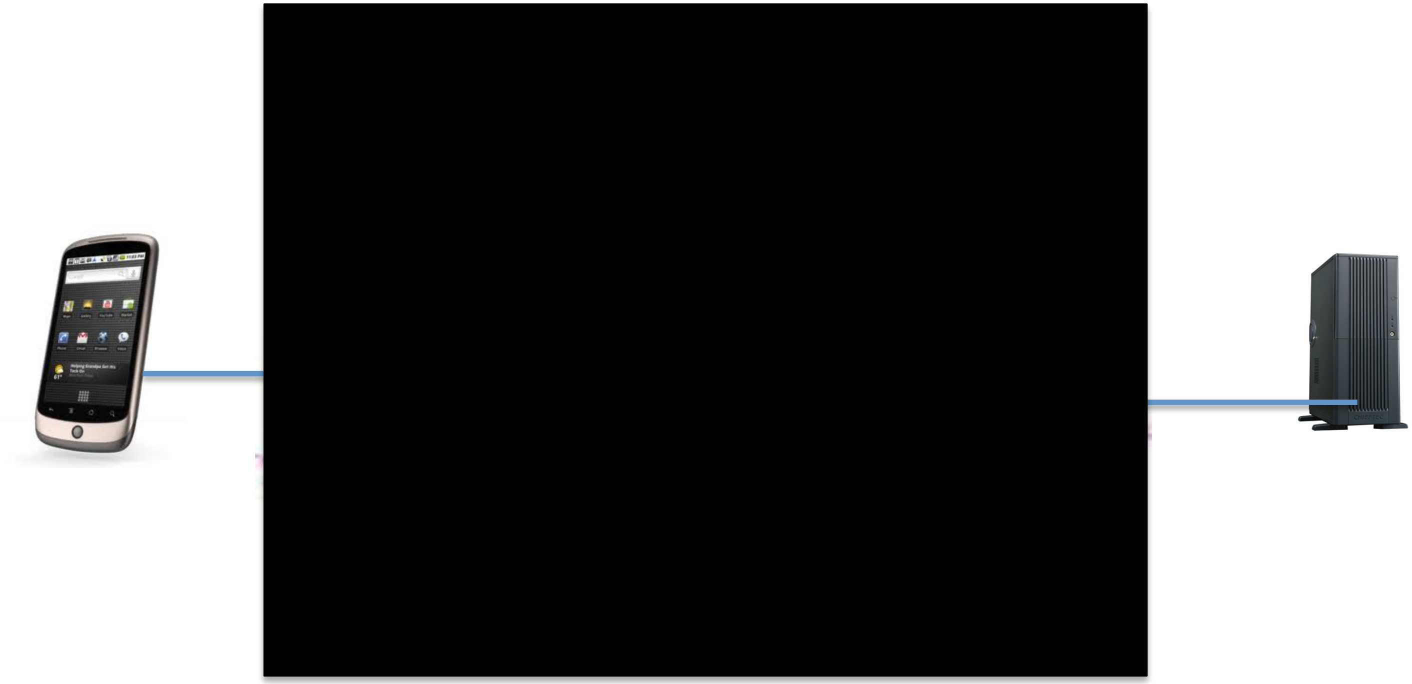
Routers have
several network
interfaces

Today's environment

Routers and enhosts have several network interfaces

The host/network interface

- What does an endhost know about the network ?
  - Embarassingly 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

Path awareness
The router's viewpoint

- First generation routing protocols
  - Connectivity is king, let's find one path to each prefix
  - If other paths are available, we'll use them to recover from link and node failures
- Second generation routing protocols
  - Leverage network path diversity to better spread traffic without any interaction with the endhosts
    - Equal Cost Multipath, MPLS

Defining path awareness

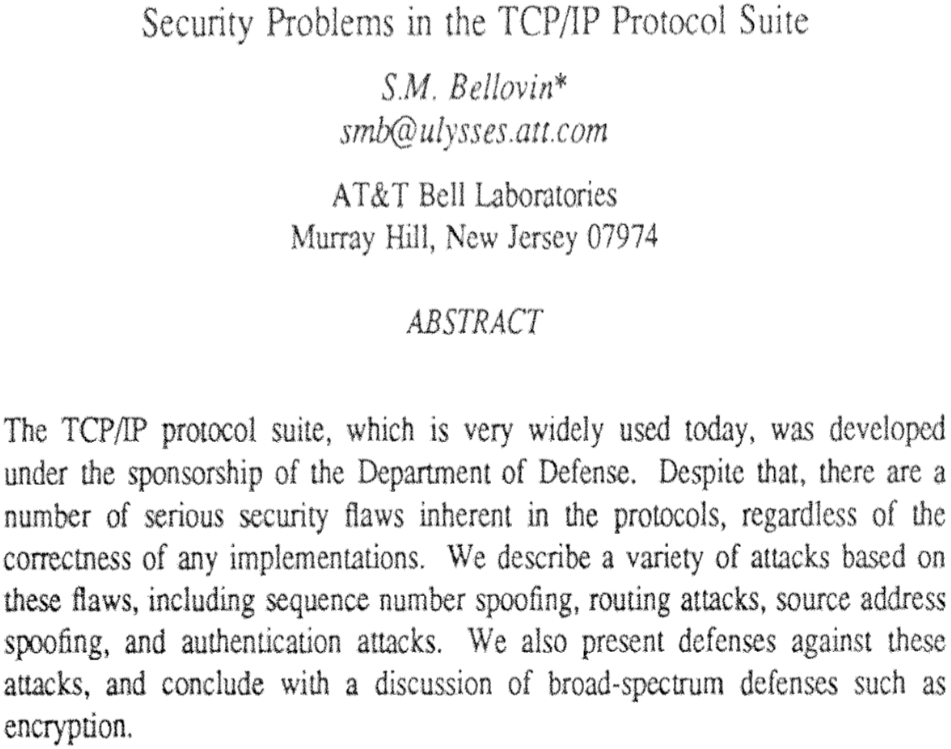
- How can we define path awareness ?
  - – Control plane viewpoint
    - How can an endhost learn the existence/availability/characteristics of different network paths ?
  - – Data plane viewpoint
    - How can an endhost request the utilisation of a specific path to the network ?

Path awareness
The router's viewpoint

- Multiprotocol Label Switching
  - Initial motivation : hardware forwarding on routers
  - Evolution
    - (one) shortest path with LDP
    - (ECMP) shortest paths with LDP
    - RSVP-TE for traffic engineering purposes coupled with OSPF-TE/ISIS-TE
      - PCE for path computation
    - Segment Routing
      - Closer coupling between MPLS and IGP, control plane simplified by removing both LDP and RSVP-TE
  - Endhost viewpoint : invisible
    - Researchers detect MPLS with `traceroute`

Failed opportunities for path awareness

- IPv4 Source routing
  - Token Ring networks used similar principles
  - Endhosts can enc source route in tl
    - IP header restric
    - How do endhost



Security Problems in the TCP/IP Protocol Suite

*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, was developed under the sponsorship of the Department of Defense. Despite that, there are a number of serious security flaws inherent in the protocols, regardless of the correctness of any implementations. We describe a variety of attacks based on these flaws, including sequence number spoofing, routing attacks, source address spoofing, and authentication attacks. We also present defenses against these attacks, and conclude with a discussion of broad-spectrum defenses such as encryption.

Failed opportunities for path awareness

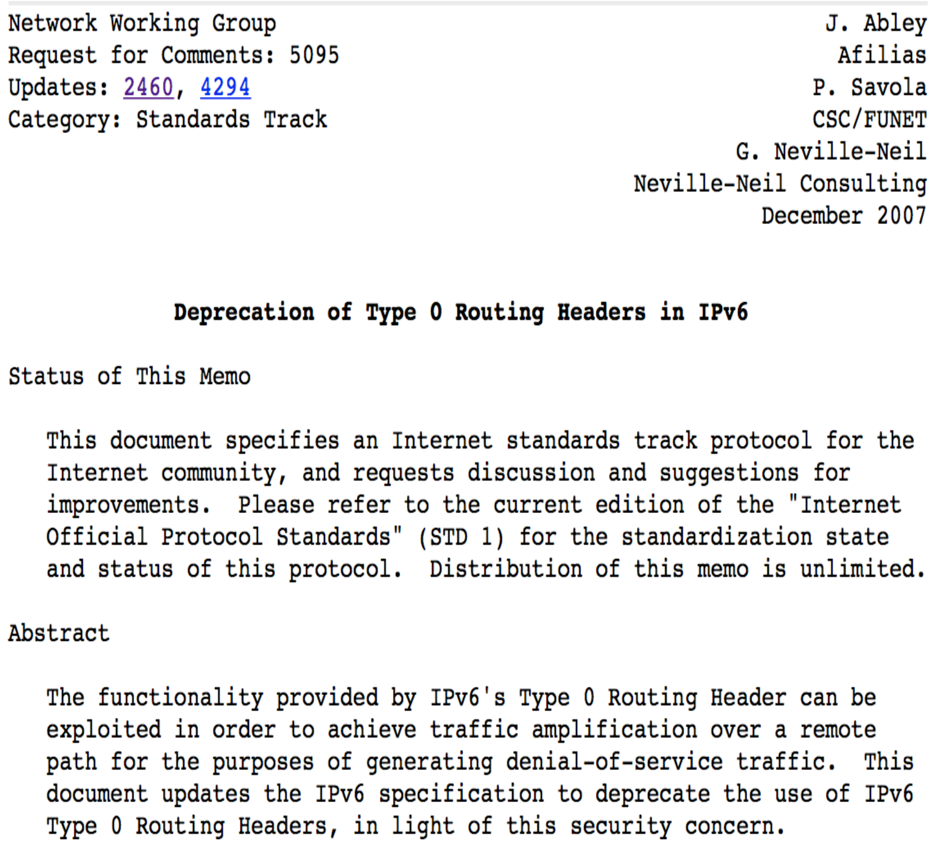
- Integrated services
  - Researcher's viewpoint
    - Endhost signals path requirements using signalling protocol
    - Network finds path most appropriate path using QoS routing
  - Solution adopted by IETF
    - Endhost signals path requirement with RSVP
    - RSVP messages are forwarded along shortest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

Failed opportunities for path awareness

- Differentiated services and ToS routing
  - Researchers's 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 thei
    - How do endhosts le



```
Network Working Group                                          J. Abley
Request for Comments: 5095                                      Afilias
Updates: 2460, 4294                                           P. Savola
Category: Standards Track                                      CSC/FUNET
                                                         G. Neville-Neil
                                                Neville-Neil Consulting
                                                           December 2007
```

Deprecation of Type 0 Routing Headers in IPv6

Status of This Memo

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

Abstract

The functionality provided by IPv6's Type 0 Routing Header can be exploited in order to achieve traffic amplification over a remote path for the purposes of generating denial-of-service traffic. This document updates the IPv6 specification to deprecate the use of IPv6 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

- My first 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

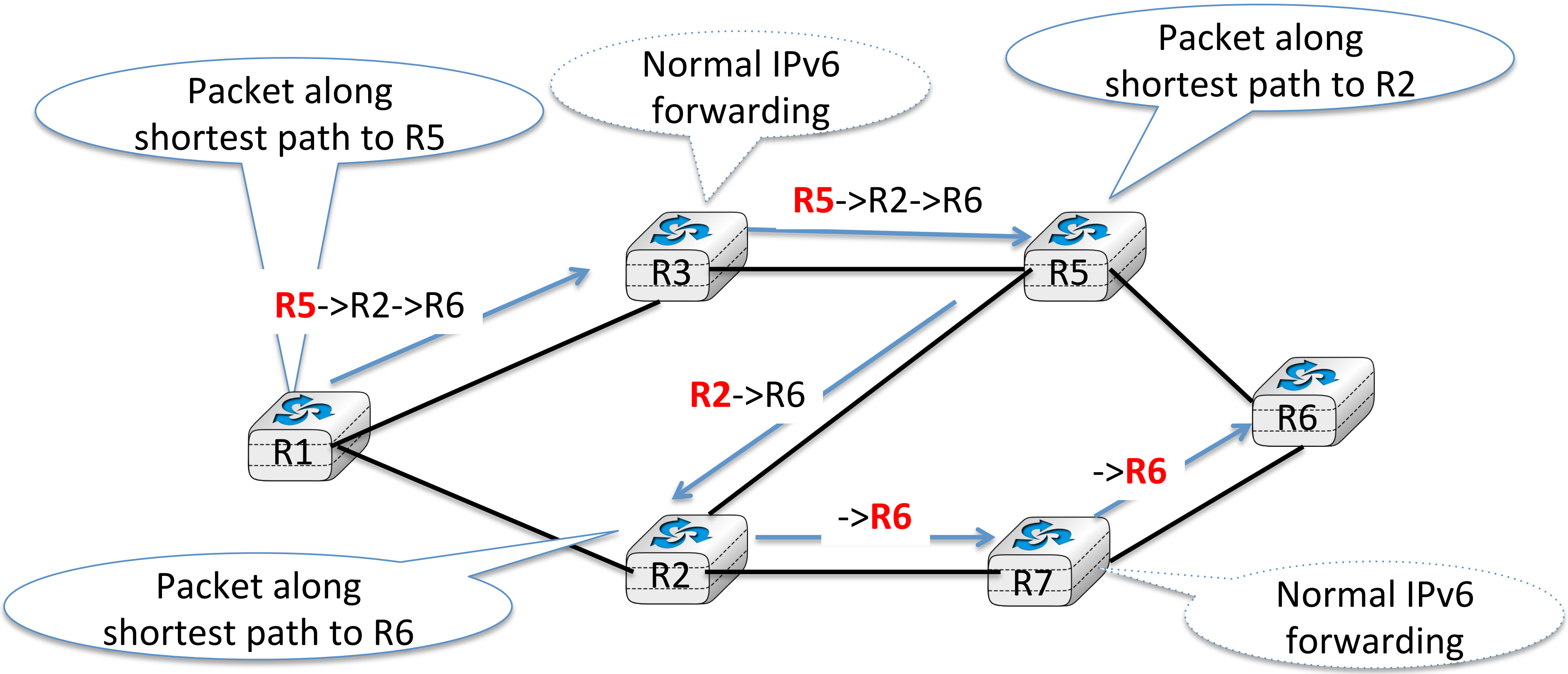
- Endhosts have identifiers that are not injected in the BGP Default Free Zone
  - Helps to scale routing tables
- Locators are attached to border routers
- Border routers map host identifiers onto locators and tunnel packets to reach remote border routers
- Path awareness ?
  - Routers are in control,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


Packet along shortest path to R5
Normal IPv6 forwarding
Packet along shortest path to R2
R5->R2->R6
R5->R2->R6
R3
R5
R1
R2->R6
R6
->R6
->R6
R2
R7
Packet along shortest path to R6
Normal IPv6 forwarding

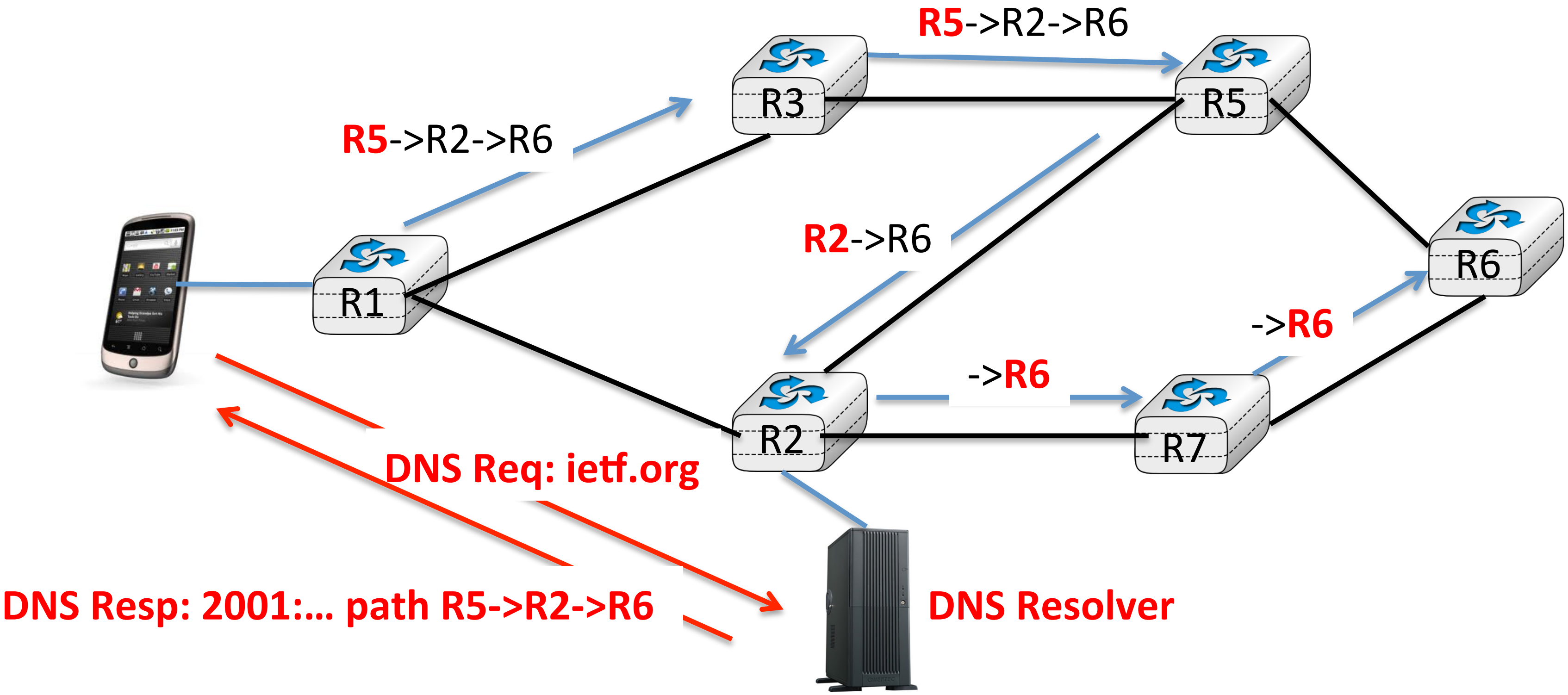
IPv6 Segment Routing

- 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

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 viewpoint
    - 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

What could path awareness means

- Scalability and business issues will prevent endhosts from having a full visibility of the network