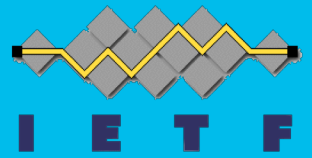
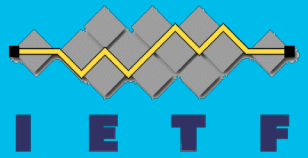


WHAT ARE THE IPV6 NEWS FROM THE IETF ?

Eric Vyncke, evyncke@cisco.com, @evyncke
Distinguished Engineer, Paris Innovation & Research Lab
March 2019



IPv6-related Working Groups

Source https://datatracker.ietf.org/meeting/103/materials/slides-103-edu-sessm-internet-area-overview-00
By Suresh Krishnan and Pascal Thubert

6MAN: IPv6 Maintenance

- Defines / controls the Evolution of IPv6
  - And prepare for IPv4 sunset
- It is the design authority for extensions and modifications to the IPv6 protocol
- Sociological dimension
  - Address Privacy
  - Freedom to form an address
- Political dimension
  - Conservationists care for a stable protocol to encourage deployments
  - Progressists want the protocol to evolve, else it dies (e.g., SR, BBR)

6lo and LPWAN

- Low Power Link layer crowds
  - BLE, BACNet, NFC, PowerLine, ZWave, 802.15.4, LoRaWAN, NB IOT, SIGFOX…
- IOT: new Internet use cases
  - Metering and Automation, Industrial Internet
- Redefining some classical operation
  - IPv6 ND
- Providing new solutions to
  - Fragmentation for small MTUs
  - Header Compression

6tisch: IPv6 over the TSCH mode of IEEE 802.15.4e

- OK, do not panic ☺
- TSCH is Time Slotted Channel Hopping
  - See https://en.wikipedia.org/wiki/Time_Slotted_Channel_Hopping
  - low-rate wireless personal area networks (LR-WPANs)
- The 6tisch working group works on defining IPv6 over TSCH in order to enable the further adoption of IPv6 in industrial standards
- Interaction with open source
  - WG tracks open source implementations and supports plugtests
  - F-interop

IPWAVE: IP Wireless Access in Vehicular Environments

- V2V and V2I use-cases where IP is well-suited as a networking technology
  - develop **an IPv6-based solution** to establish direct and secure connectivity between a vehicle and other vehicles or stationary systems.
- Specify the mechanisms for transmission of **IPv6 datagrams** over IEEE 802.11-OCB mode.

V6OPS: IPv6 Operations

- Operation crowd practicing the technology
- Feeds back on the protocol in the real world
- Produces Best Practice

- When real world experience meets academics ☺
- Really worth reading/learning from...

Homenet

- This working group focuses on the evolving networking technology within and among relatively small residential networks
  - Designed to work on residential networks involving multiple routers and subnets
  - Mainly focused on IPv6-based operations
- Job is now mostly done

Softwires

- Focuses on the specification of IPv4-IPv6 transition and co-existence mechanisms that are based on encapsulation (i.e. tunneling)
  - Discovery, control and encapsulation methods for connecting IPv4 networks across IPv6 networks and vice versa
  - Implementation considerations for handling selection and use of one of these transition/co-existence solutions

- Job is mostly done

DMM Distributed Mobility Management

- Distributed Mobility Management solutions for IP networks so that traffic between mobile and correspondent nodes can take an optimal route
- It is also chartered to work on maintenance and bug fixes of the specifications in the **Mobile IPv6** protocol family

LWIG Light-Weight Implementation Guidance

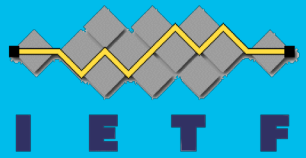
- The LWIG working group focuses on collecting and documenting experiences from implementers of IP stacks in constrained devices
- implementation techniques for reducing complexity, memory footprint, or power usage

- IPv6 can be chatty…

GIT GitHub Integration and Tooling

- Many IETF working groups use external code repository services, primarily GitHub, in managing their work
- It is about HOW to use github-like tools for RFC, ...
- It is NOT about github protocols

- Interesting when GitHub is IPv4-only ☹ ☹



Recent IPv6 RFC

Finally, IPv6 is a Standard

Internet Engineering Task Force (IETF) — S. Deering
Request for Comments: 8200 — Retired
STD: 86 — R. Hinden
Obsoletes: 2460 — Check Point Software
Category: Standards Track — July 2017
ISSN: 2070-1721

Internet Protocol, Version 6 (IPv6) Specification

Abstract

This document specifies version 6 of the Internet Protocol (IPv6). **It obsoletes RFC 2460**.

Internet Engineering Task Force (IETF)
Request for Comments: 8219
Category: Informational
ISSN: 2070-1721

M. Georgescu
L. Pislaru
RCS&RDS
G. Lencse
Szechenyi Istvan University

August 2017

BMWG ☺

Benchmarking Methodology for IPv6 Transition Technologies

Abstract

Benchmarking methodologies that address the performance of network interconnect devices that are IPv4- or IPv6-capable exist, but the IPv6 transition technologies are outside of their scope. This document provides complementary guidelines for evaluating the performance of IPv6 transition technologies. More specifically, this document **targets IPv6 transition technologies that employ encapsulation or translation mechanisms**, as dual-stack nodes can be tested using the recommendations of RFCs 2544 and 5180. The methodology also includes a metric for benchmarking load scalability.

The crux?

- Some transition mechanisms involve DNS64
  => need to take DNS into account
  => happy eye ball (see later)

Internet Engineering Task Force (IETF)
Request for Comments: 8250
Category: Standards Track
ISSN: 2070-1721

N. Elkins
Inside Products
R. Hamilton
Chemical Abstracts Service
M. Ackermann
BCBS Michigan

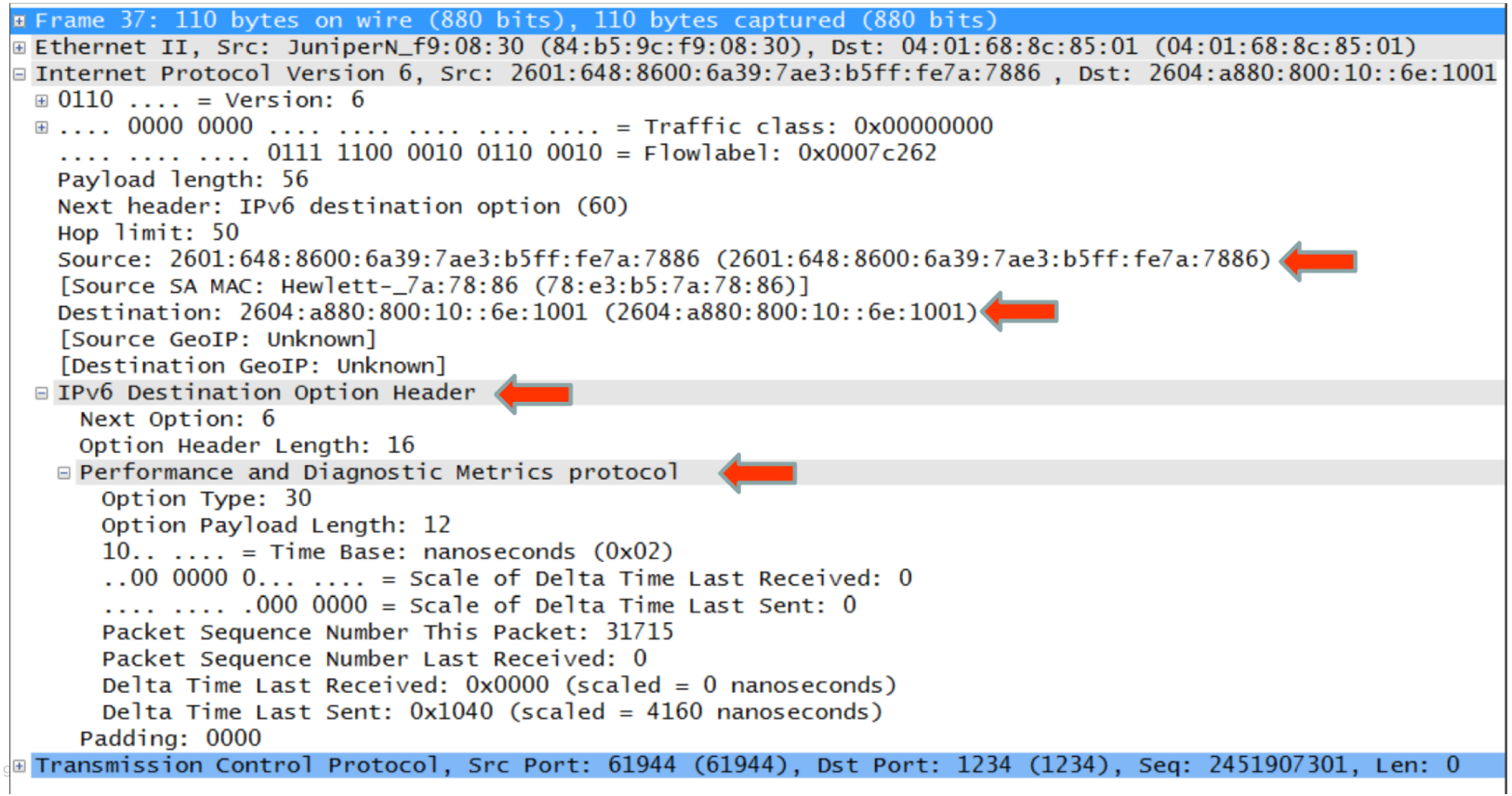
September 2017

IPv6 Performance and Diagnostic Metrics (PDM) Destination Option

Abstract

To assess performance problems, this document describes optional headers embedded in each packet that provide sequence numbers and timing information as a basis for measurements. Such measurements may be interpreted in real time or after the fact. This document specifies the Performance and Diagnostic Metrics (PDM) Destination Options header. The field limits, calculations, and usage in measurement of PDM are included in this document.

Wireshark Capture from IPPM at IETF-93



Difference with draft-ietf-ippm-ioam-data

- iOAM can use IPv6 extension headers but also NSH, Segment Routing, ...
- Requires support on each router on the path
- It is also about proving the path with signatures

Internet Engineering Task Force (IETF)
Request for Comments: 8273
Category: Informational
ISSN: 2070-1721

J. Brzozowski
Comcast Cable
G. Van de Velde
Nokia

December 2017

Unique IPv6 Prefix per Host

Abstract

This document outlines an approach utilizing existing IPv6 protocols to allow hosts to be assigned a unique IPv6 prefix (instead of a unique IPv6 address from a shared IPv6 prefix). Benefits of using a unique IPv6 prefix over a unique service-provider IPv6 address include improved host isolation and enhanced subscriber management on shared network segments.

Could we even go to a /64 per host ????

- Do not panic, we have enough IPv6 addresses !
- Remove all layer-[23] threats: rogue RA & co
- This I-D is for a /64 per host but host is now aware, but, what of ?
  - For containers, the /64 can contain
    - The timestamp of instantiation
    - Father process ID
    - Image ID
    - In short, a fingerprint for audit

Request for Comments: 8305
Obsoletes: 6555
Category: Standards Track
ISSN: 2070-1721

T. Pauly
Apple Inc.

December 2017

Happy Eyeballs Version 2: Better Connectivity Using Concurrency

Abstract

Many communication protocols operating over the modern Internet use hostnames. These often resolve to multiple IP addresses, each of which may have different performance and connectivity characteristics. Since specific addresses or address families (IPv4 or IPv6) may be blocked, broken, or sub-optimal on a network, clients that attempt multiple connections in parallel have a chance of establishing a connection more quickly. This document specifies requirements for algorithms that reduce this user-visible delay and provides an example algorithm, referred to as "Happy Eyeballs". This document obsoletes the original algorithm description in RFC 6555.

New Happy Eyeball ?

- Mainly clarifications about
  - Multiple DNS servers
  - Multiple addresses are returned
  - 50 msec preference for IPv6

- Simple new implementation is compatible with ‘old’ version

Independent Submission
Request for Comments: 8367
Category: Informational
ISSN: 2070-1721

Wrongful Termination of Internet Protocol (IP) Packets

Abstract

Routers and middleboxes terminate packets for various reasons. In some cases, these packets are wrongfully terminated. This memo describes some of the most common scenarios of wrongful termination of Internet Protocol (IP) packets and presents recommendations for mitigating them.

April Fools' Day RFC

- Packet can be terminated based on
  - Color : DSCP
  - Age: Hop Limit
  - Origin: source address
  - ...

Internet Engineering Task Force (IETF)
Request for Comments: 8415
Obsoletes: 3315, 3633, 3736, 4242, 7083,
7283, 7550
Category: Standards Track
ISSN: 2070-1721

T. Mrugalski
M. Siodelski
ISC
B. Volz
A. Yourtchenko
Cisco
M. Richardson
SSW
S. Jiang
Huawei
T. Lemon
Nibbhaya Consulting
T. Winters
UNH-IOL

November 2018

Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

Huw? New DHCPv6 ???

- No… unique DUID is unchanged
- No… DHCPv6 still leases address(es) to DUID and not to client-HW-address
  - Sorry, security guy / controlling freaks
- It is about clarifications mainly
  - And removing client hints

Internet Engineering Task Force (IETF)
Request for Comments: 8475
Category: Informational
ISSN: 2070-1721

J. Linkova
Google
M. Stucchi
RIPE NCC

October 2018

Using Conditional Router Advertisements for Enterprise Multihoming

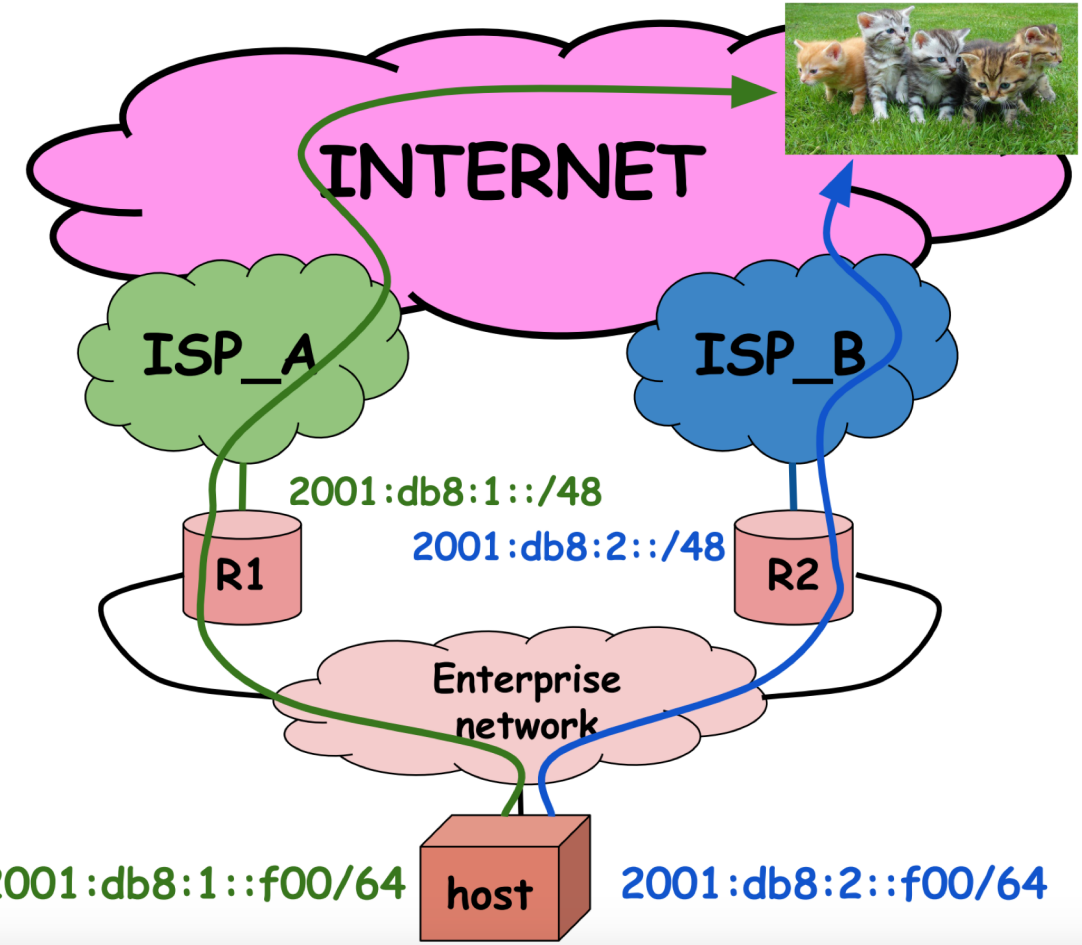
Abstract

This document discusses the most common scenarios of connecting an enterprise network to multiple ISPs using an address space assigned by an ISP and how the approach proposed in "Enterprise Multihoming using Provider-Assigned Addresses without Network Prefix Translation: Requirements and Solution" could be applied in those scenarios. The problem of enterprise multihoming without address translation of any form has not been solved yet as it requires both the network to select the correct egress ISP based on the packet source address and hosts to select the correct source address based ...

Selecting the Uplink

- Two uplinks used for Internet access (primary/backup or active/active)
- Simple network topology
- Each ISP allocates a prefix
- Packets SHOULD NOT be sent to the uplink if
  - It's backup uplink and the primary one is up
  - The packet source address does not belong to that ISP

Source: https://datatracker.ietf.org/meeting/99/materials/slides-99-v6ops-sessa-conditional-router-advertisements/



Source: https://datatracker.ietf.org/meeting/99/materials/slides-99-v6ops-sessa-conditional-router-advertisements/

Influencing the Source Address Selection

If the primary uplink is operational

Address from the backup prefix SHOULD NOT be used

If the ISP uplink fails

Addresses from that ISP prefix SHOULD NOT be used

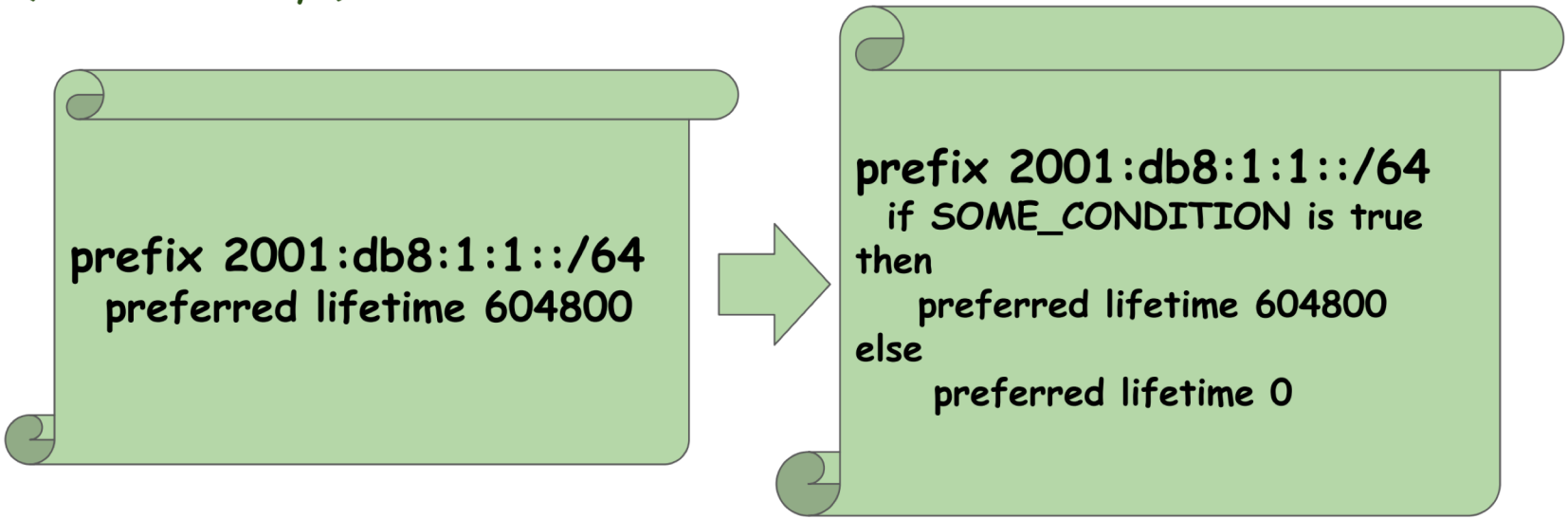
deprecate the address

Source: https://datatracker.ietf.org/meeting/99/materials/slides-99-v6ops-sessa-conditional-router-advertisements/

Proposed Approach

RA fields values are set based on the present network state

("conditionally")



Source: https://datatracker.ietf.org/meeting/99/materials/slides-99-v6ops-sessa-conditional-router-advertisements/

Internet Engineering Task Force (IETF)
Request for Comments: 8501
Category: Informational
ISSN: 2070-1721

L. Howard
Retevia

November 2018

Reverse DNS in IPv6 for Internet Service Providers

Abstract

In IPv4, Internet Service Providers (ISPs) commonly provide IN-ADDR.ARPA information for their customers by prepopulating the zone with one PTR record for every available address. This practice **does not scale in IPv6**. This document analyzes different approaches and considerations for ISPs in managing the IP6.ARPA zone.

How to make reverse DNS scale ?

- Such as
  - `a.9.8.7.6.5.e.f.f.f.4.3.2.1.0.0.0.0.0.0.0.0.f.0.8.b.d.0.1.0.0.2 .IP6.ARPA.`
- Proposals
  - Negative response NXDOMAIN
  - Wildcard match
  - Dynamic DNS update (but not so scalable)
    - By residential gateway (managed or not)
    - By individual nodes
  - DNS delegation
  - Populate from DHCP/RADIUS server ?

Internet Engineering Task Force (IETF)
Request for Comments: 8504
BCP: 220
Obsoletes: 6434
Category: Best Current Practice
ISSN: 2070-1721

T. Chown
Jisc
J. Loughney
Intel
T. Winters
UNH-IOL

January 2019

IPv6 Node Requirements

Abstract

This document defines requirements for IPv6 nodes. *It is expected that IPv6 will be deployed in a wide range of devices and situations*. Specifying the requirements for IPv6 nodes allows IPv6 to function well and interoperate in a large number of situations and deployments.

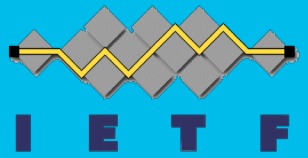
This document obsoletes RFC 6434, and in turn RFC 4294.

Meta-RFC 8504 roadmap to all RFC and recommendations

- Not all RFC need to be implemented all the time ;-)
- Beware of fragmentation (done by the source, ICMP required, extension header, ...)
- Source address selection
- Mandatory SLAAC, optional DHCP
- ...

Changes in RFC 8504

- DNS over RA is mandatory
- Adding RESTCONF, NETCONF for management
- And new features such as ECN, mDNS, unique prefix per host, ...
- Stable address creation RFC 8064
- Removed IPv6 over ATM ;-)



Recent IPv6 Internet Drafts

More than 300 active I-D have IPv6 references

Network Working Group
Internet-Draft
Updates: 4861, 5175 (if approved)
Intended status: Standards Track
Expires: September 8, 2019

R. Hinden
Check Point Software
B. Carpenter
Univ. of Auckland
B. Zeeb
March 7, 2019

IPv6 Router Advertisement IPv6-Only Flag

draft-ietf-6man-ipv6only-flag-05

Abstract

This document specifies a Router Advertisement Flag to indicate to hosts that the administrator has configured the router to advertise that the link is IPv6-Only. This document updates RFC4861 and RFC5175.

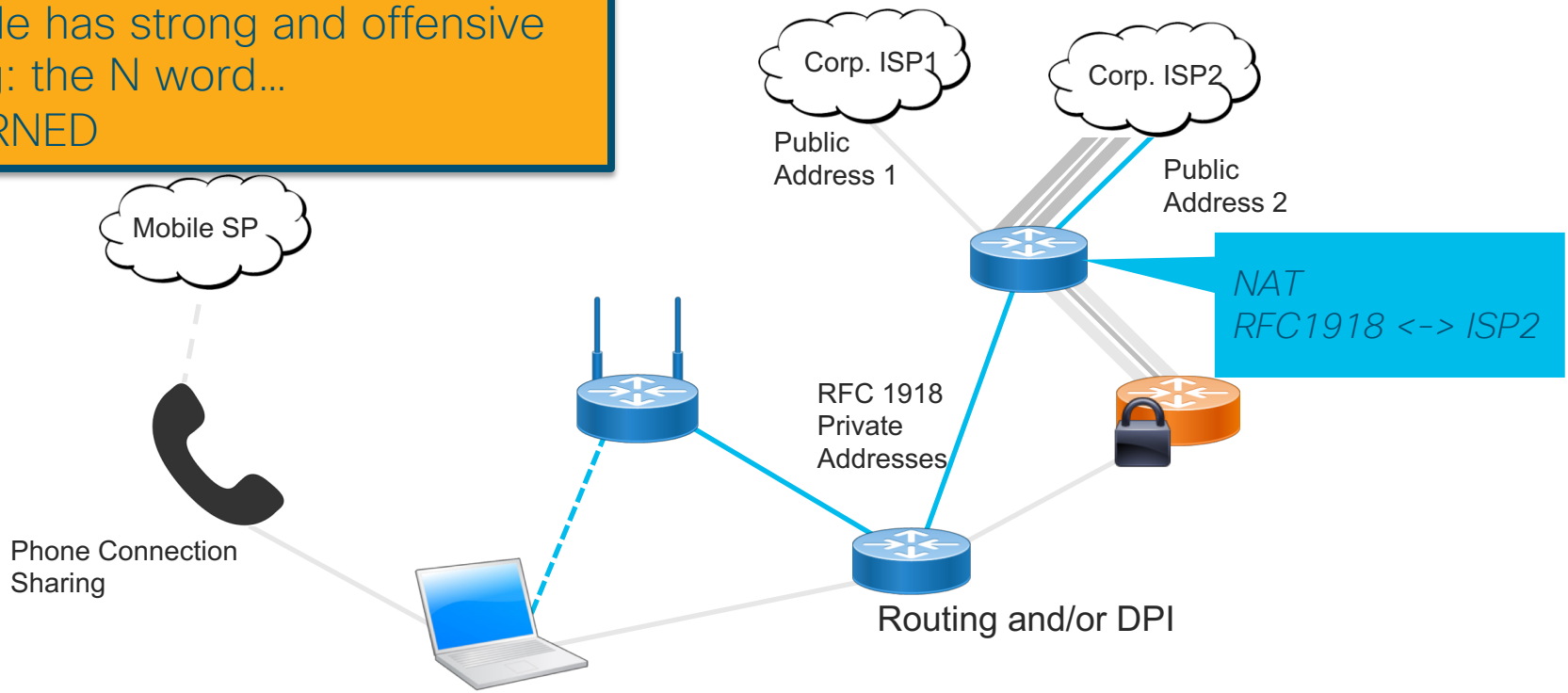
Why ?

- IPbv6-only network is doable (with caveats)
- But, hosts still want to try IPv4 (DHCPv4, IPv 4 LLA, ...)
- Flag in RA can signal IPv6-only => avoiding IPv4 startup
- Obviously cannot be done over DHCPv4
  - Assuming IPv6-only host stack

- Yet another RA flags though... Exhaustion is coming !

Multi-Homing, the legacy way…

WARNING
This slide has strong and offensive wording: the N word…
BE WARNED



rtgwg
Internet-Draft
Intended status: Standards Track
Expires: September 11, 2019

D. Lamparter
NetDEF
A. Smirnov
Cisco Systems, Inc.

March 10, 2019

Destination/Source Routing

draft-ietf-rtgwg-dst-src-routing-07

Abstract

This note specifies using packets' source addresses in route lookups as additional qualifier to be used in hop-by-hop routing decisions. **This applies to IPv6** [RFC2460] in general with specific considerations for routing protocol left for separate documents. *There is nothing precluding similar operation in IPv4, but this is not in scope of this document*.

Note that destination/source routing, source/destination routing, SADR, source-specific routing, source-sensitive routing, S/D routing and D/S routing are all used synonymously.

SADR in a nutshell

- All FIB entries are associated with a source prefix
  - ::/0 for entries without a source prefix
- draft-ietf-rtgwg-dst-src-routing
- Find route matching both source and destination prefixes while preferring longest destination prefix match and breaking ties with longest source prefix match
- Not optimal SADR algorithm
  1. `PotentialRoutes :=Longest match(es) on destination prefix`
  2. `SourceRoute := longest match on the packet source in the PotentialRoutes`
  3. `If not found, then back to 1) with a shorter match`
- Other implementations are possible

Trivial SADR Example

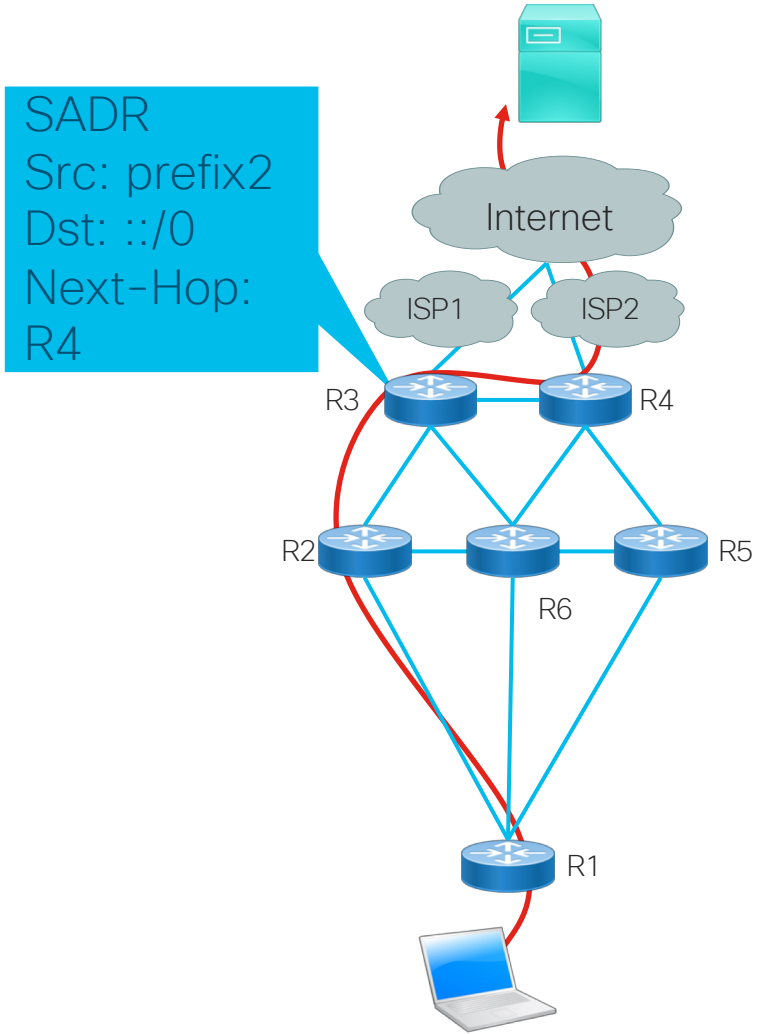
- SADR FIB

Source	Destination	Next - Hop
::/0	::/0	R3
2001:db8::/32	::/0	R3
2001:db8:2::/64	::/0	R4

- Packet SRC = 2001:db8:1::1 to DST = 2001:db8:cafe::babe via R3
- Packet SRC = 2001:db8:2::1 to DST = 2001:db8:cafe::babe via R4

Incremental Deployment

- SADR only on edge routers
- Best effort forwarding:
  - R3 can have a SADR route to R4 for ISP2 source prefix
- SADR on R1 / R6 would only improve
- If R3 and R4 are not adjacent, then SRv6 (or a tunnel) can be used



draft-ietf-intarea-provisioning-domains

1. Identify Provisioning Domains (PvDs)

[RFC7556] *Provisioning Domains (PvDs) are consistent sets of network properties that can be implicit, or advertised explicitly.*

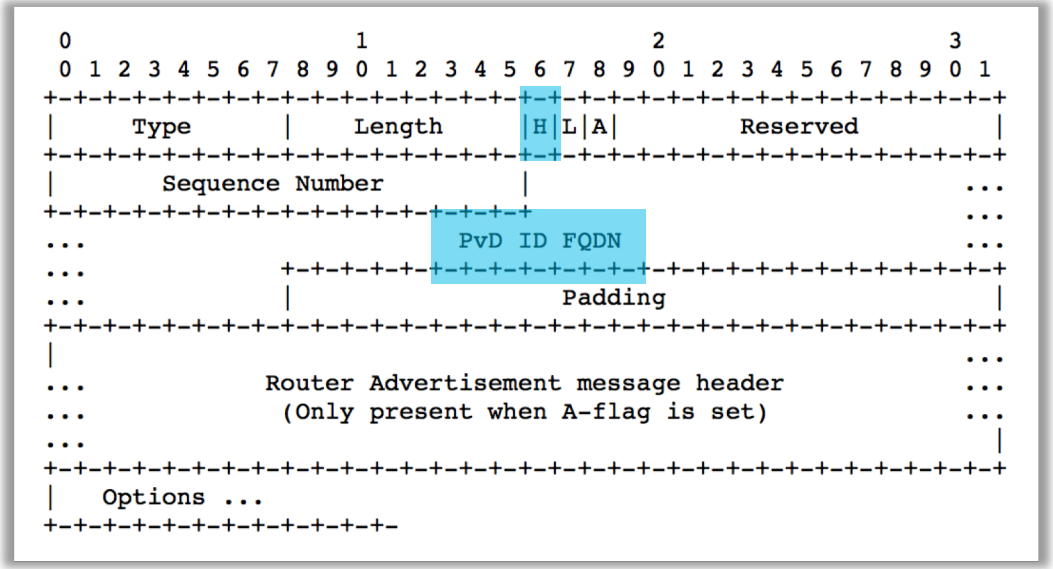
Differentiate provisioning domains by using FQDN identifiers.

2. Extend PvD with additional information

For the applications: name, captive portal, etc…

Identify PvDs

With the PvD ID Router Advertisement Option



- At most **one occurrence in each RA**.
- **PvD ID is an FQDN** associated with options included in the PvD option**.**
- **H bit** to indicate **Additional Information is available with HTTPS**.
- **L bit** to indicate the **PvD has legacy DHCP on the link**.
- **A bit** to indicate that another RA header is included in the container
- Seq. number used for **push-based refresh**.

Network Working Group
Internet-Draft
Intended status: Experimental
Expires: July 1, 2019

O. Troan
Cisco Systems

December 28, 2018

The Universal IPv6 Router Advertisement Option (experiment)

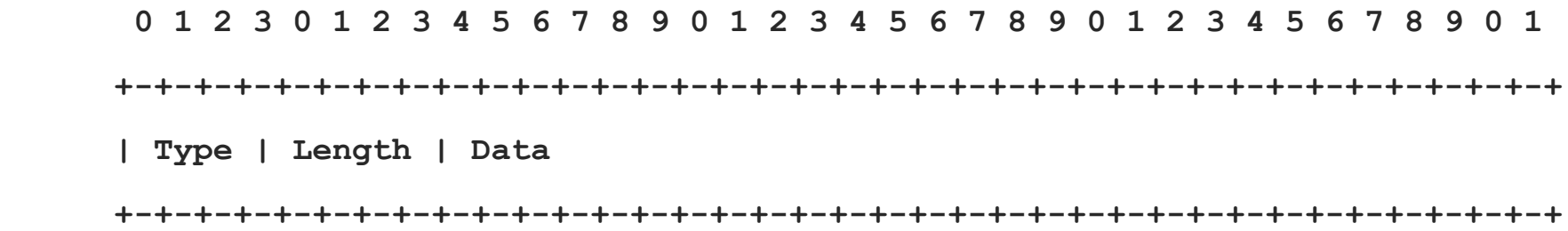
draft-troan-6man-universal-ra-option-01

Abstract

One of the original intentions for the IPv6 host configuration, was to configure the network-layer parameters only with IPv6 ND, and use service discovery for other configuration information. Unfortunately that hasn't panned out quite as planned, and we are in a situation where all kinds of configuration options are added to RAs and DHCP. This document proposes a new universal RA option in a self-describing data format, with the list of elements maintained in an IANA registry, with greatly relaxed rules for registration.

Universal RA option ?

- Opaque carrier for self-describing configuration options
- Allow for communication network -> host applications

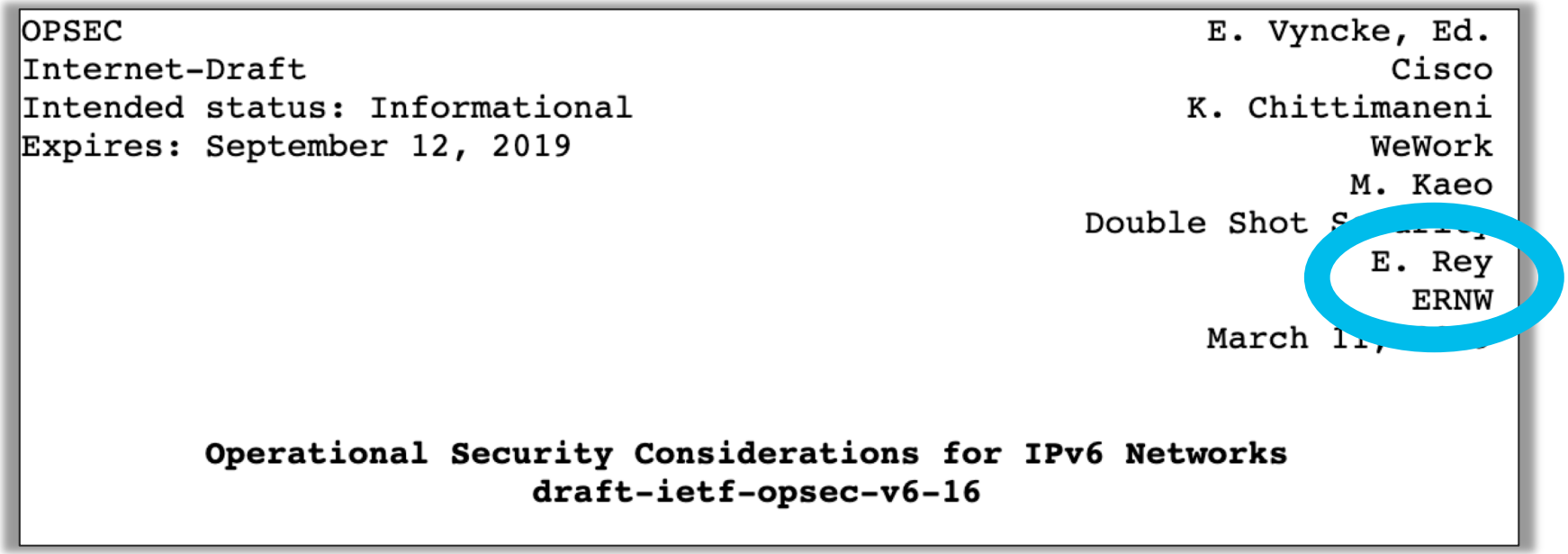


- Encoding as JSON

Example of Universal RA Option

```
{ "ietf": {
      "dns": {
            "dnssl": [ "example.com" ],
            "rdnss": [ "2001:db8::1",
                  "2001:db8::2" ]
      },
      "nat64": {
            "prefix": "64:ff9b::/96"
      }
}
```

And as we are at Troopers



OPSEC
Internet-Draft
Intended status: Informational
Expires: September 12, 2019

E. Vyncke, Ed.
Cisco
K. Chittimaneni
WeWork
M. Kaeo
Double Shot S[illegible]
E. Rey
ERNW
March 11, [illegible]

Operational Security Considerations for IPv6 Networks
draft-ietf-opsec-v6-16

https://tools.ietf.org/html/draft-ietf-opsec-v6-16

OPSECv6

- A long long time ago, it all started
- Focus on enterprise, SP and residential
  - A touch of 3GPP
  - Nothing about IoT
- Topics: addressing, extension headers, NDP, ...
- Just “considerations” to be easier at the IETF
  - Still very hot about ULA...

See also

- IP Fragmentation Considered Fragile: draft-ietf-intarea-frag-fragile-09
- IKEv2 Notification Status Types for IPv4/IPv6 Coexistence: draft-ietf-ipsecme-ipv6-ipv4-codes-02
- Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers: draft-ietf-opsec-ipv6-eh-filtering-06
- ...

Thank you

- For listening
- But also to ACT

- IETF is not about superpower of Gods
- It is about engineering mainly (and vendor politics sometime)
- Decisions are made on MAILING LIST
  - Free
  - You are an individual and not an employee/student
  - No NEED to be in physical meetings