What can only be done with IPv6…

Eric Vyncke, evyncke@cisco.com, @evyncke
Distinguished Engineer, Cisco Paris Innovation & Research Lab
May 2018

This session is about technologies being drafted at the IETF and still under development...

Comments will be welcome ☺

6CN

Content Networking with IPv6, http://6cn.io

Eric Vyncke
Distinguished Engineer, evyncke@cisco.com

6CN: Coding Content Description – Example of ipv6 address template

IPV6	Routing prefix + subnet id	Interface identifier
Bits	48 + 16	64

Fields	Stream Type	Service ID	Content Descriptor	Chunk Descriptor		
Bits	2	12	26	24		
				4	4	16
Comments	= 4 types 00 = linear 01 = non-linear 10 = UGC 11 = corp.	= 4096 services per type	= 70+ millions per service	= 16 profiles To combining appropriated AV formats (DASH/HLS most significant bit) and ABR qualities =0 reserved value	= duration From 1 to 15s =0 can be reserved for none, so a single (big) chunk/file	= chunk sequence number Allows by iteration to (pre)-fetch/cache over the network Combined with Duration, it references from 6 hours to 4 days per service/content. It also gives direct time stamps for trick modes =0 can be reserved for the DASH/HLS manifest

Example of recommendation

Fields	Show/Serie ID	Episode ID
Bits	16	10
Comment	= 65000+ per service	= 1000+ per show
Fields	Source ID	Movie ID
Bits	12	14
Comment	= 4000+ per service	= 16000+ per source
Fields	#Day	#Clock
Bits	15	11
Comment	*year/month/day*	*minute in the day*

6CN: IPv6-Centric to Cache, Analyze and Route Videos

http://6cn.io *Sunnyvale, California (origin server)*

Home | Introduction to 6CN | Video catalog | Video via DASH | Video via HLS | Analytics | CDN

Streaming video

Video streaming is usually done by two incompatible systems (DASH and HLS described in other tabs) but share the concept of splitting a long movie in small video sequences. The duration of each sequence is usually small (1 to 5 seconds) in order to allow quick start (once a couple of chunks are preloaded) as well as sliding quickly through the video. As there are usually multiple representation of one movie (language, resolution, required bandwidth, ...), there will be multiple video chunks for the same video segment.

Introduction to 6CN

In the usual system, the video chunks are in the same file and the browser accesses them by fetching a specific byte range or by using URI with some parameters.

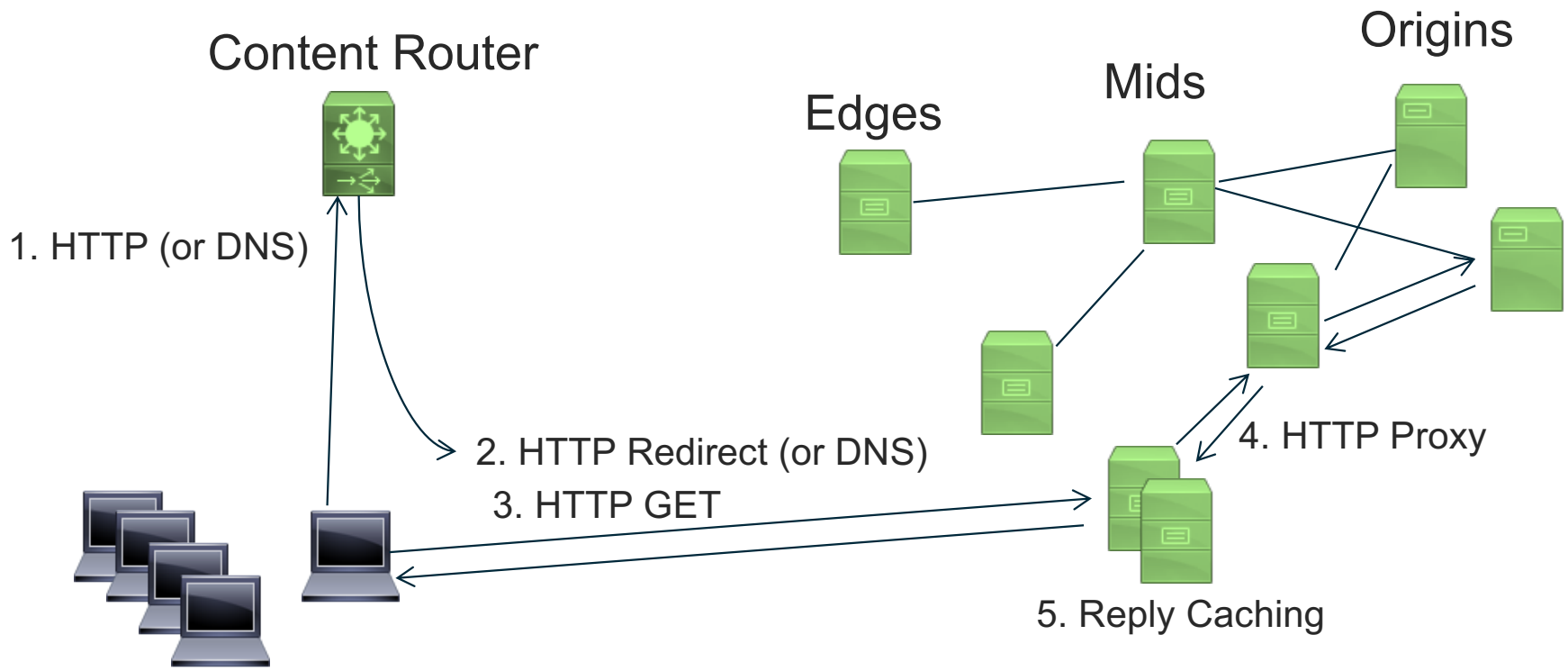
In the 6CN (Content Networking for Delivery and Caching), each video chunk has its own IPv6 address (which can vary based on the cache the chunk is located).

All IPv6 addresses are generated in a special way, you can try to decode, or encode them ;-). The encoding scheme is described in a specific format and there is a tool to edit this format.

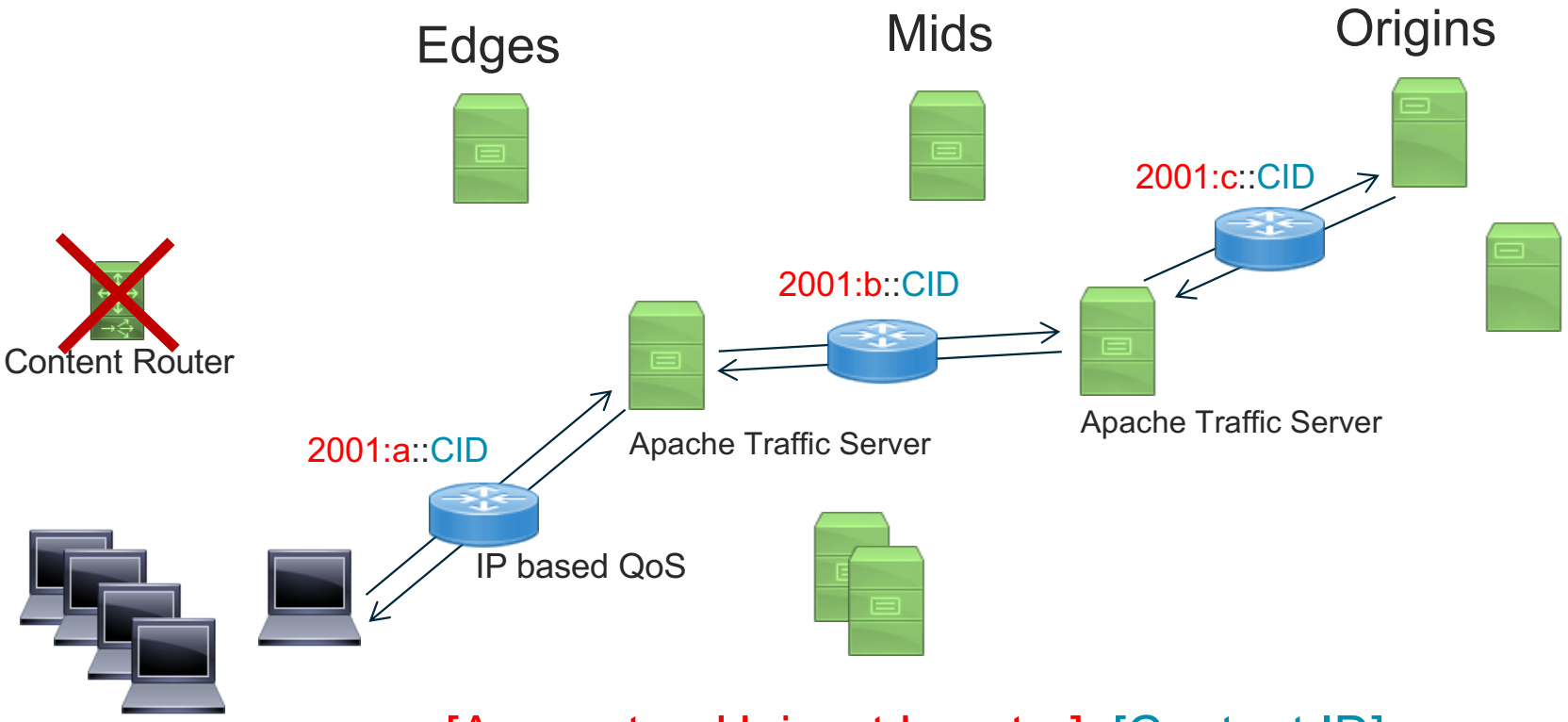
Putting semantics in IPv6 addresses also opens the door for NetFlow-based analytics by the provider even when chunks are encrypted. The addressing scheme used by this demo is described below (and look at the impressive number of videos which can be encoded in a single /64):

6CN: Coding Content Description – Example of ipv6 address template

Traditional Traffic Control CDN

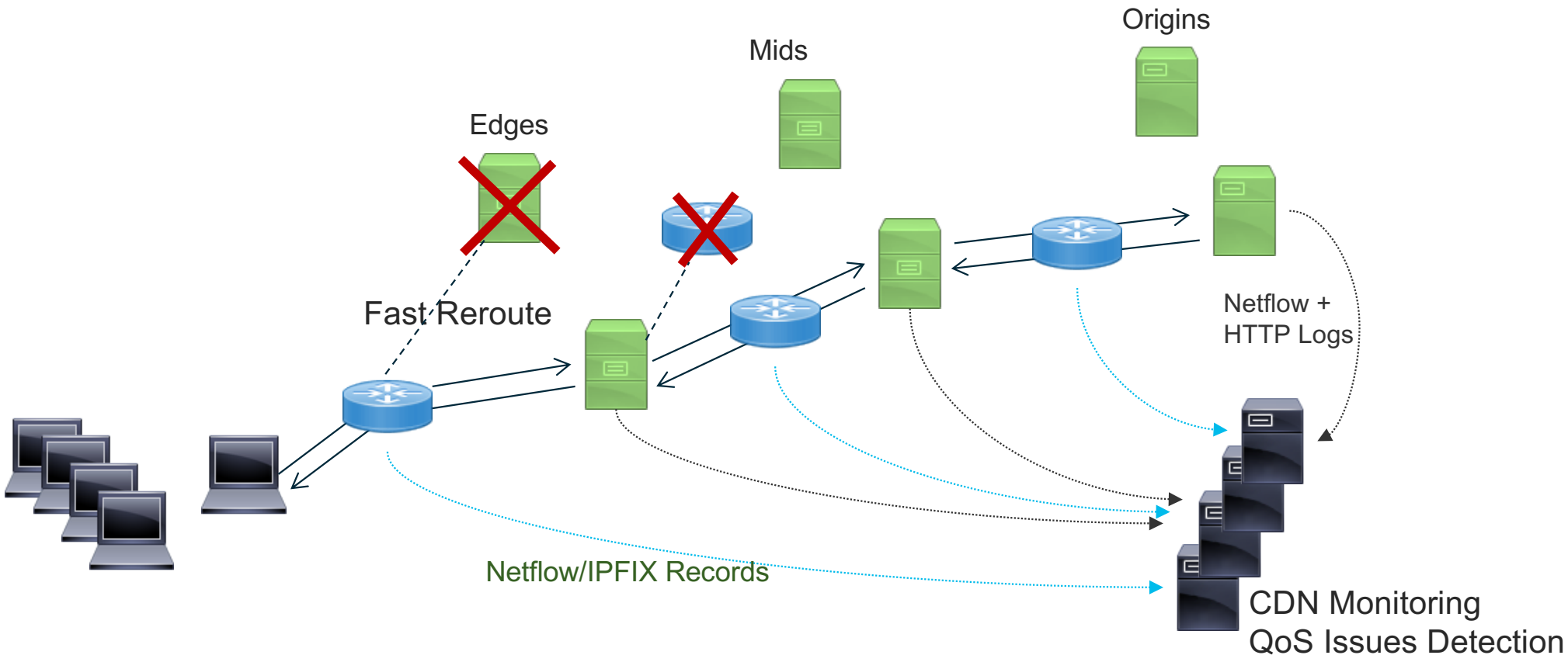


Adding 6CN to Traffic Control



[Anycast or Unicast Locator]::[Content ID]

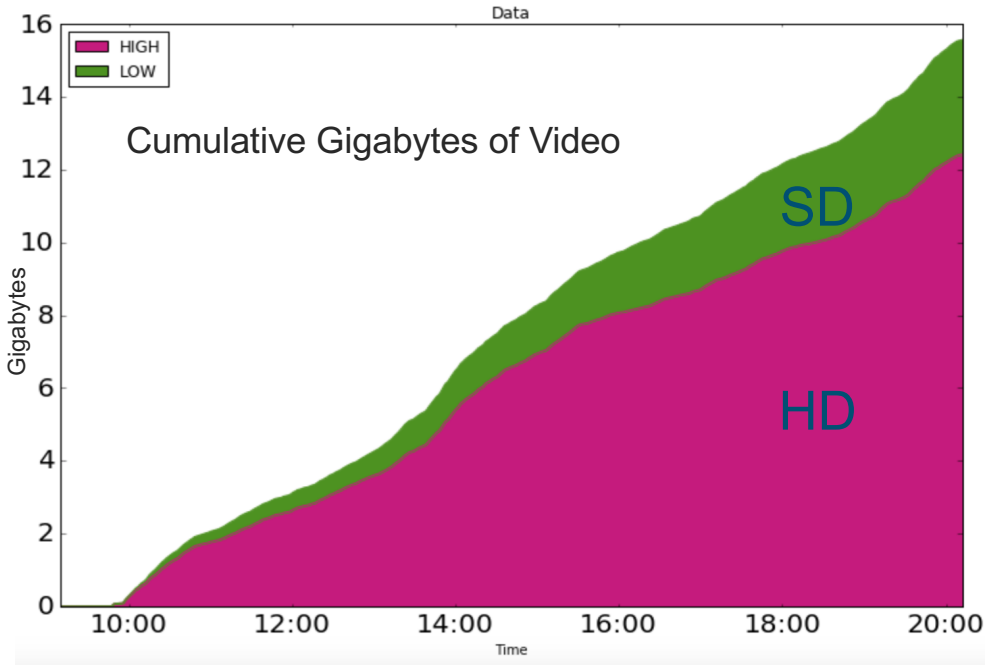
6CN Advantages – High Availability, Monitoring

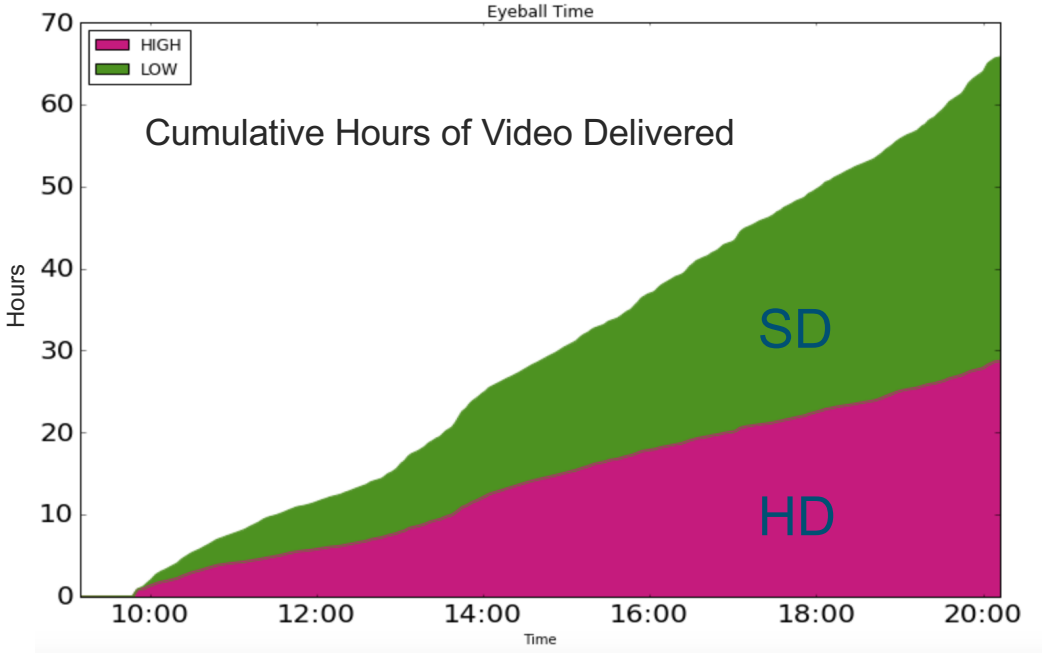


Leverage decades of IP layer optimizations

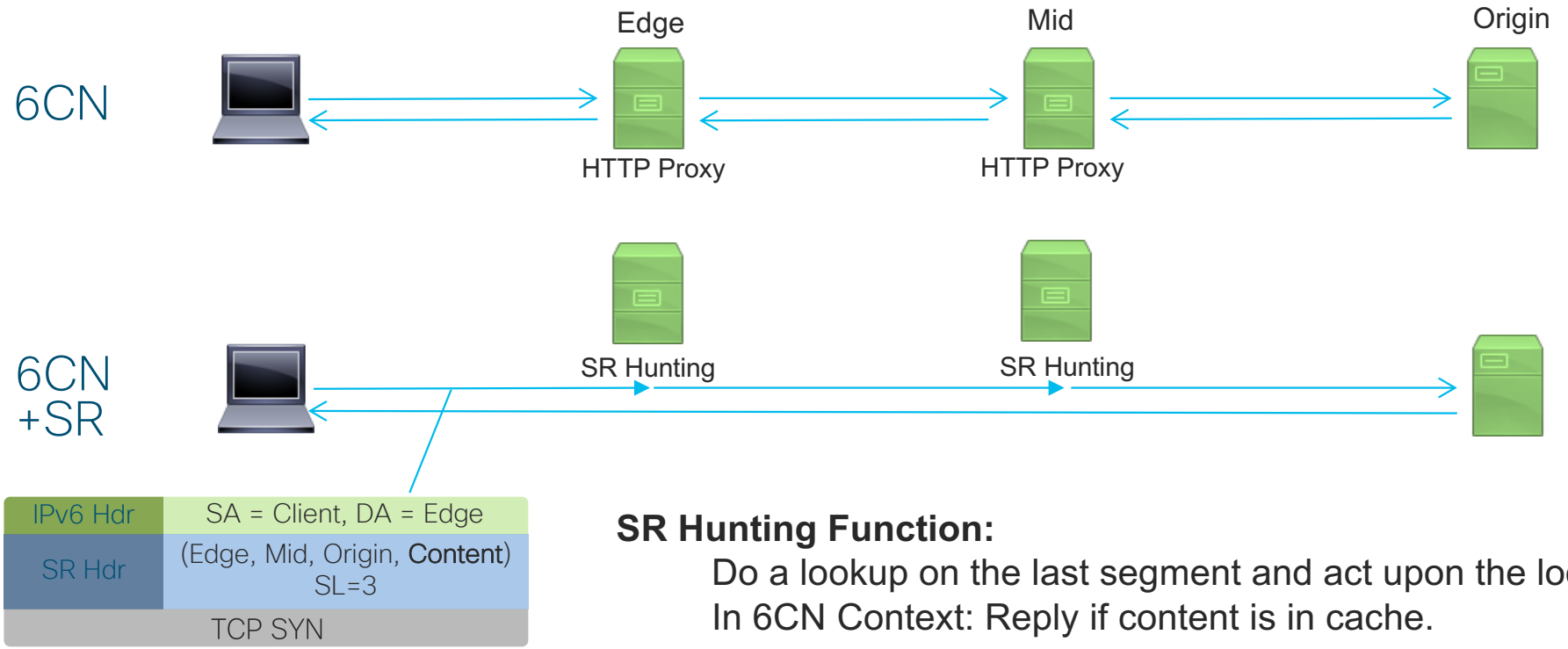
Bytes vs. Hours for a given video (in HD or SD)

14 hour test period, using IPFIX records sent to PNDA (logstash & Kafka)





Work In Progress: Segment Routing Content Hunting

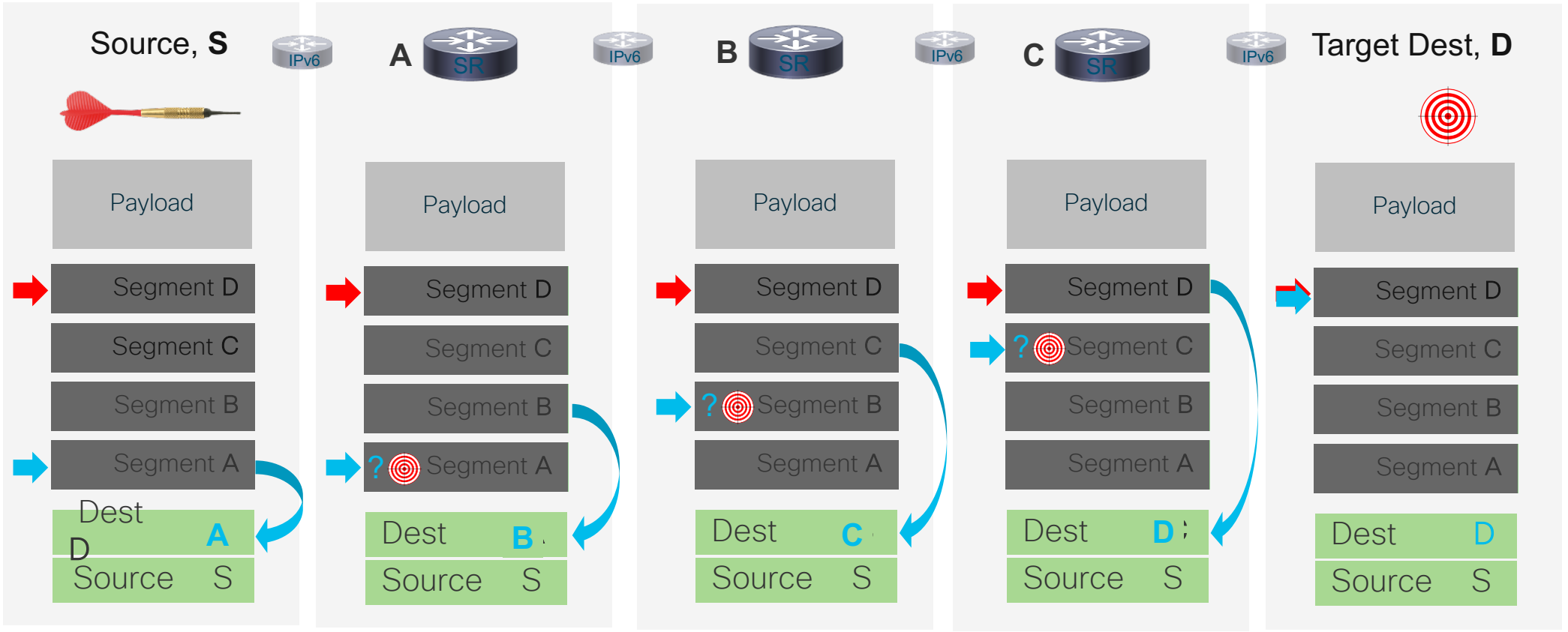


SR Hunting Function:

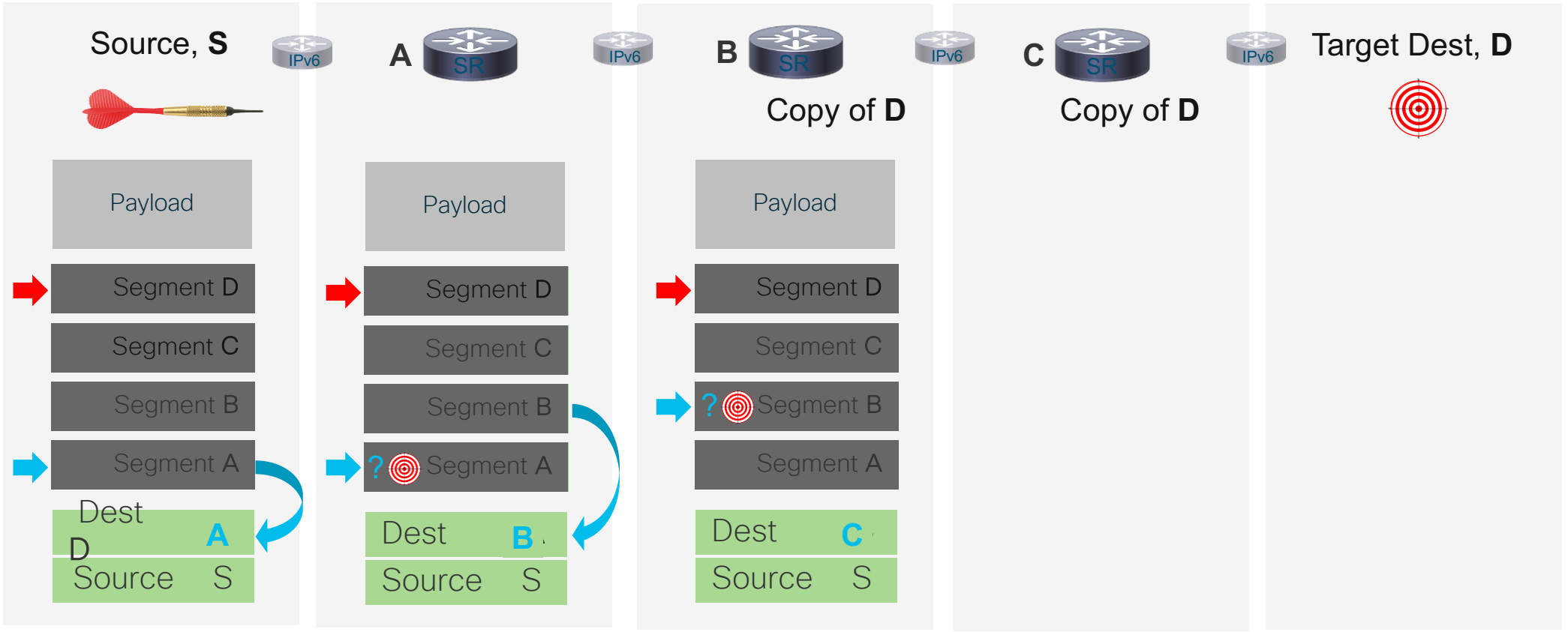
Do a lookup on the last segment and act upon the lookup result.
In 6CN Context: Reply if content is in cache.

No HTTP Proxying

6CN Content Hunting



6CN Content Hunting



Upload your own 6CN Video

http://6cn.io/users/

Home | Introduction to 6CN | Video catalog | Video via DASH | Video via HLS | Analytics | CDN

Users videos

CISCO

6CN community videos

Mark Townsley uses 6CN Videos.

Welcome back Mark Townsley

On this page you can find a couple of videos uploaded by the 6CN community.

You can also upload your own videos.

There are 9 videos in our 6CN video store. Feel free to click on any randomly selected video below to play it with some IPv6 information being displayed.

Happy 2017 !
2017-01-23 (7 view(s))
101 IPv6 addresses
Uploaded by: Eric Vyncke

Drone Racing in Alsace
2017-02-17 (7 view(s))
231 IPv6 addresses
Uploaded by: Pierre Pfister

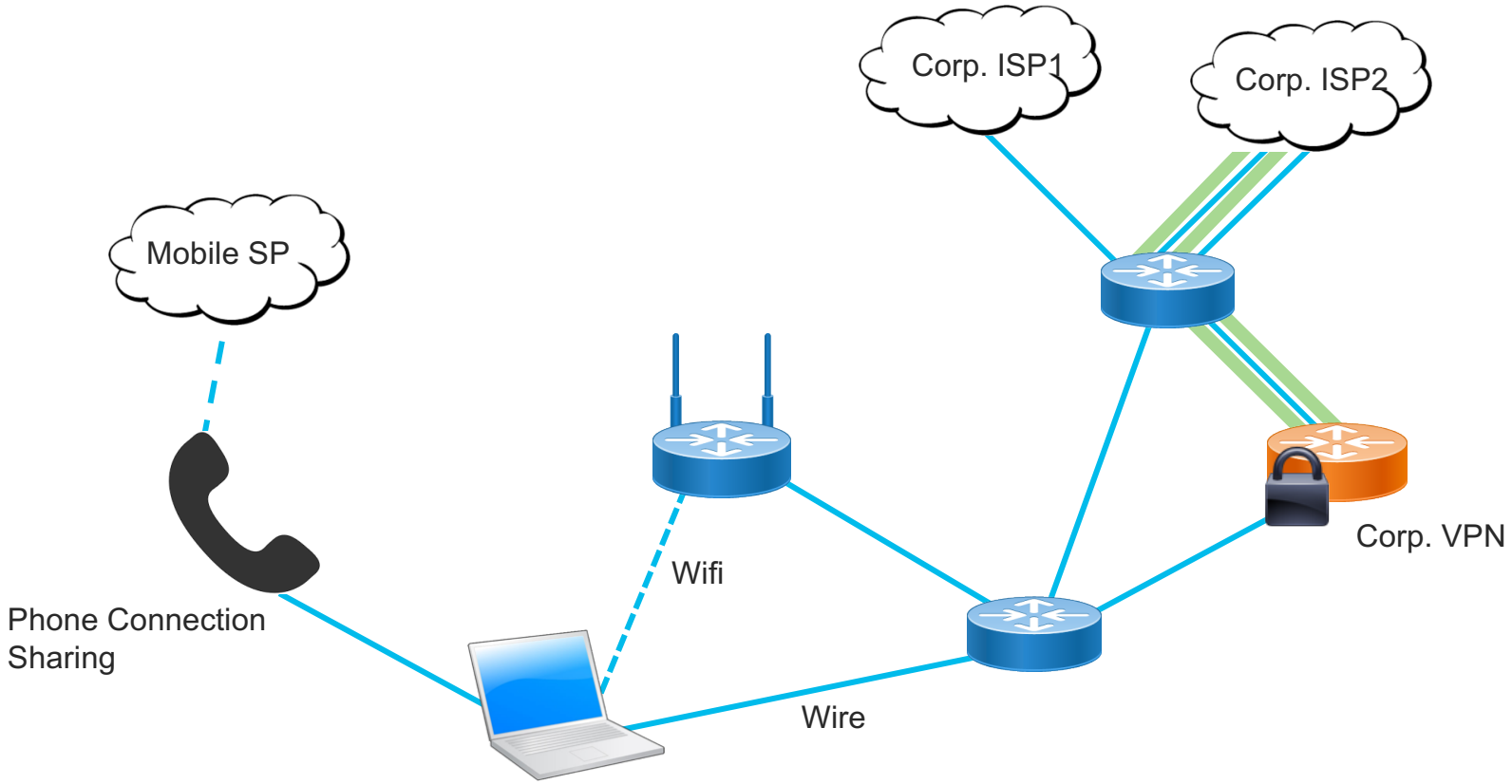
Freeride in the Alps
2017-02-20 (5 view(s))
601 IPv6 addresses
Uploaded by: Pierre Pfister

Flying over the San Francisco Bay (fast forward)
2017-01-23 (14 view(s))
85 IPv6 addresses
Uploaded by: Eric Vyncke

Multiple IPv6 Addresses
Problem statement

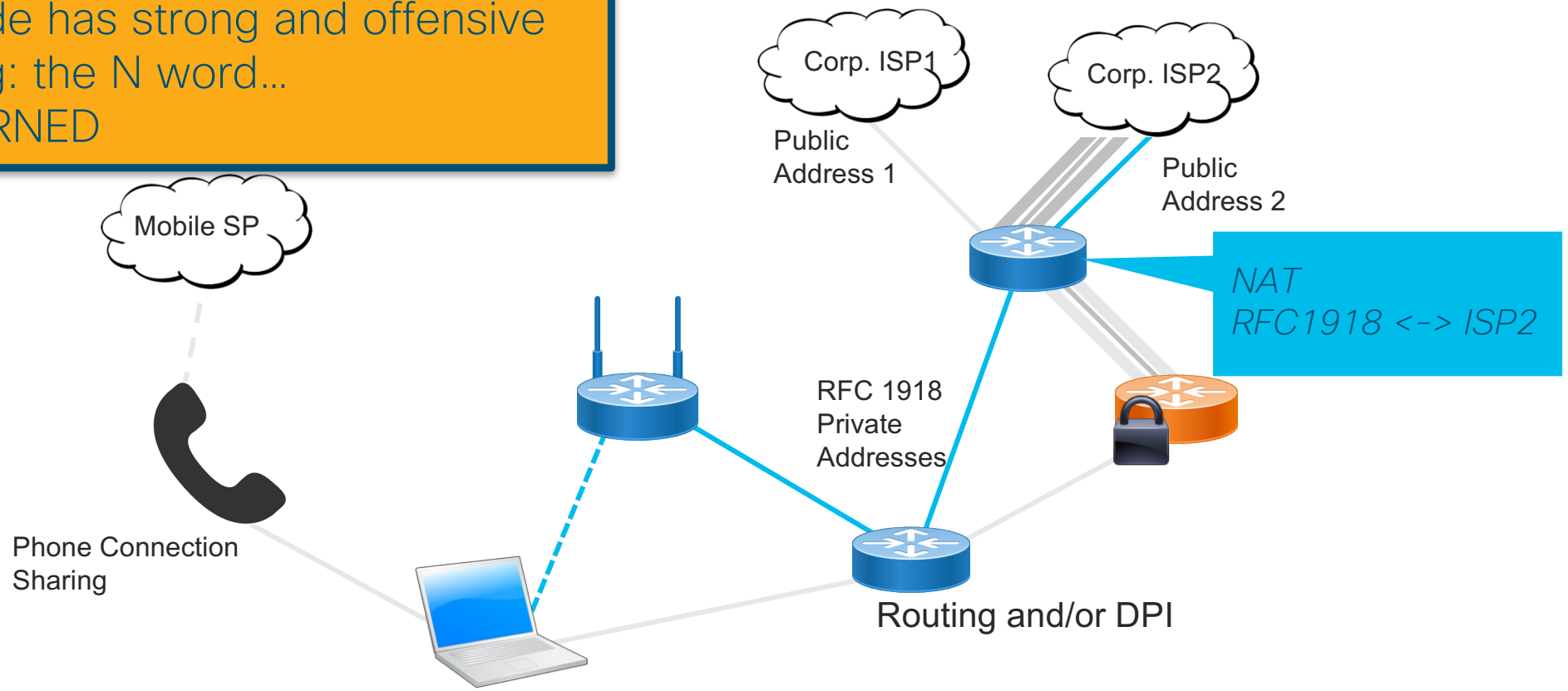
Hosts and networks are multi-homed

Just a few examples…



Multi-Homing, the legacy way…

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



Addressing in Multi-Homed Networks in IPv6

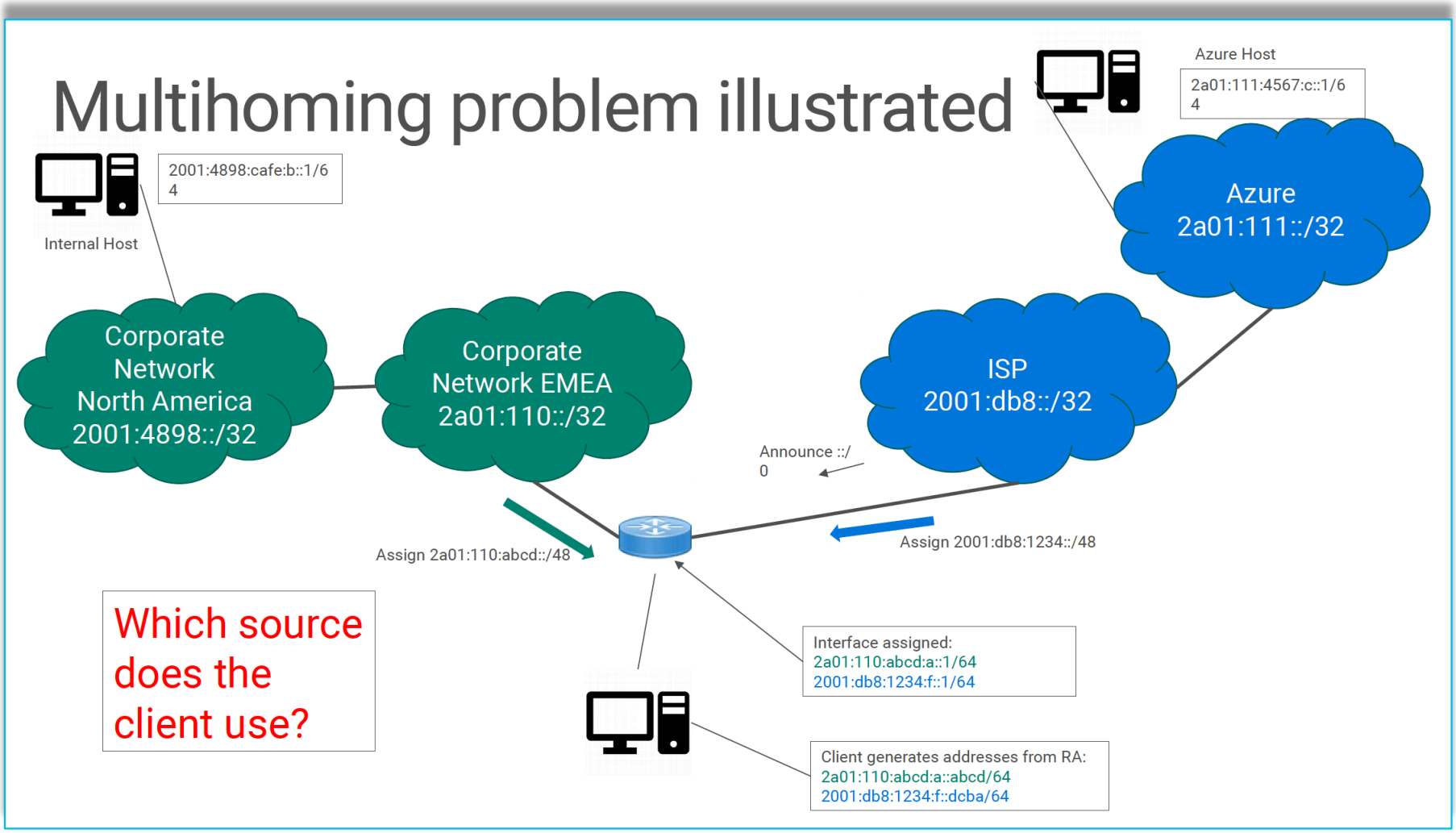
- Assign Provider Assigned (PA) addresses to hosts.
  - Native to IPv6 hosts (RFC4861, ...)
  - HNCP for home networks (RFC7788)
  - draft-ietf-rtgwg-enterprise-pa-multihoming for corporate networks.
- Teach the hosts to pick and use multiple addresses.
  - IPv6 source address selection (RFC6724)
  - Multi-Path TCP (RFC6824), SCTP, QUIC, ...
- Give the host meaningful information about the addresses.

Bundling IP address & DNS resolver

Multihoming and CDNs

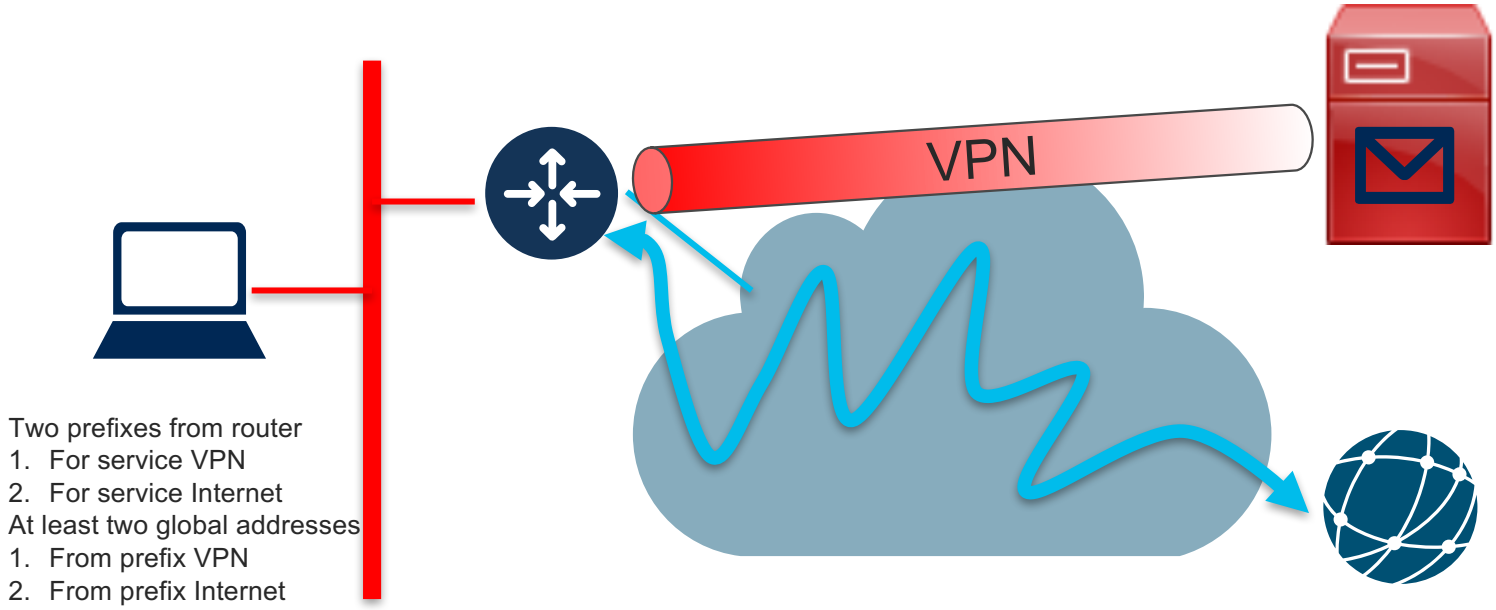
- Name lookups for resources stored on CDNs give different answers depending on the network connection
- Host on homenet may look up name using resolver from provider A, then connect to CDN using provider B
- This will generate support requests
- What to do?

Ted Lemon, Homenet WG, IETF-99



From Marcus Kean, Microsoft IT, at V6OPS IETF-99

Selecting the Service by Source Address



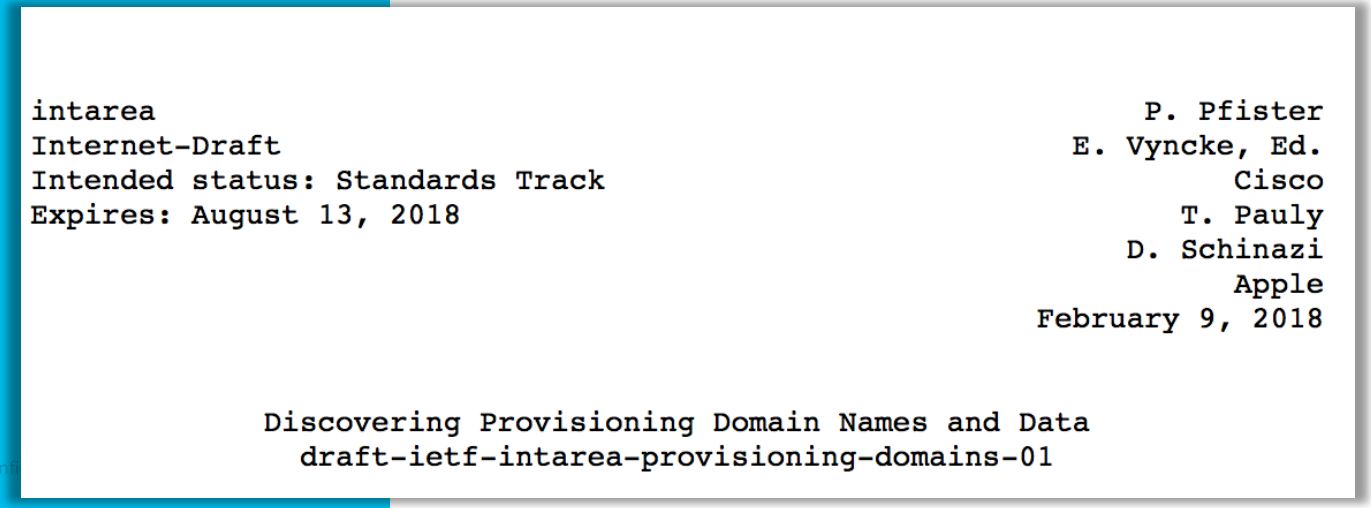
Two prefixes from router
1. For service VPN
2. For service Internet

At least two global addresses
1. From prefix VPN
2. From prefix Internet

Traffic engineering
Different QoS

Provisioning the host

- How can the host discover all network prefixes and services?
- At the network and application layers



intarea
Internet-Draft
Intended status: Standards Track
Expires: August 13, 2018

P. Pfister
E. Vyncke, Ed.
Cisco
T. Pauly
D. Schinazi
Apple
February 9, 2018

Discovering Provisioning Domain Names and Data
draft-ietf-intarea-provisioning-domains-01

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.*

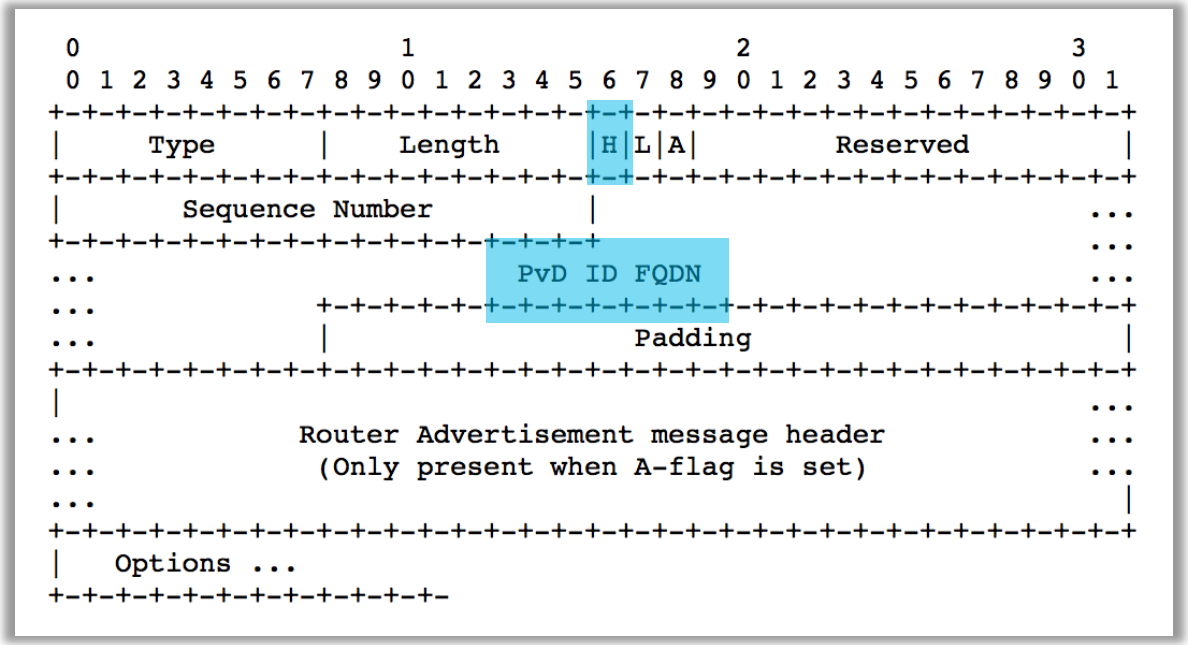
Differentiate provisioning domains by using FQDN identifiers.

2. Extend PvD with additional information

For the applications: name, captive portal, etc…

Step 1: Identify PvDs

With the PvD ID Router Advertisement Option

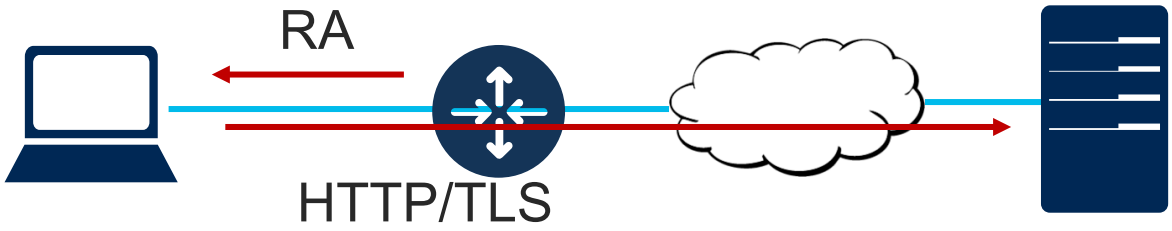


- At most **one occurrence in each RA**.
- **PvD ID is an FQDN** associated with options included in the PvD option**.**
- **H bit** to indicate **Additional Information is available with HTTPS**.
- **L bit** to indicate the **PvD has legacy DHCP on the link**.
- **A bit** to indicate that another RA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

Step 1b: Identifying PvD (Cont.)

- Information in an RA without PvD ID is linked to an implicit PvD (identified by interface & link-local address of router)
- Previously received options in RA can change of PvD when they are received in a RA with a different PvD ID
- DHCPv6 information MUST be associated to a PvD ID received on the same interface from the same link-local address

Step 2: Get the PvD Additional Application Data



When the H bit is set:

GET https://<pvd-id>/.well-known/pvd

Using network configuration (source address, default route, DNS, etc…) **associated with the received PvD**.

Step 2: Get the PvD Additional Data

```
{
  "name": "Foo Wireless",
  "expires": "2018-07-26T06:00:00Z",
  "prefixes" : ["2001:db8:1::/48", "2001:db8:4::/48"],
  "dnsZones": ["example.com","sub.example.com"];
}
```

Some other examples (see also https://smart.mpvd.io/.well-known/pvd) :

```
noInternet : true,
metered : true,
captivePortalURL : "https://captive.org/foo.html”
```

Captive Portals...

- Current working: HTTP(S) redirection
  - Not working with HSTS and normal browser
  - Or rely on OS detection via http://captive.example.com/hotspot-detect.html
  - Not easy for users when having multiple providers on a single portal (Boingo, Ipass, ...)
- PvD
  - One PvD per provider
  - Each PvD additional data has the provider name, optionally walled garden information and the **URL for the captive portal (working with HSTS)**

Implementation status

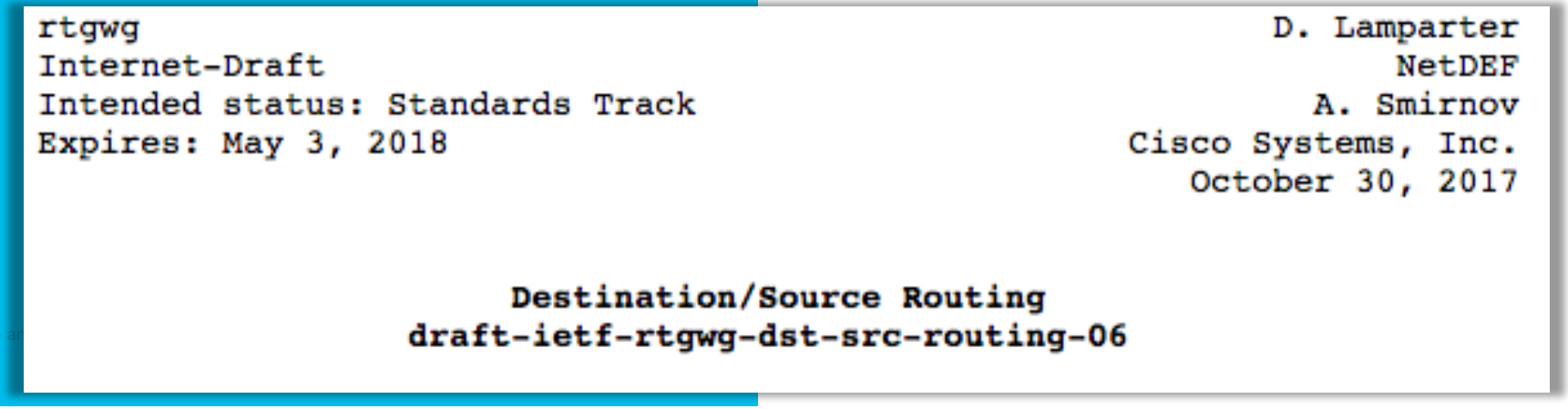
Linux - https://github.com/IPv6-mPvD

- **pvdd**: user-space daemon managing PvD IDs and additional data
- **Linux Kernel** patch for RA processing
- **iproute** tool patch to display PvD IDs
- **Wireshark** dissector
- **RADVD** and **ODHCPD** sending PvD ID

Implemented in one commercial vendor router

Source Address Dependent Routing (SADR)

- Forwarding based on the SOURCE rather than the destination as usual
- Based on source scoped Forwarding Information Base (FIB) entried



rtgwg
Internet-Draft
Intended status: Standards Track
Expires: May 3, 2018

D. Lamparter
NetDEF
A. Smirnov
Cisco Systems, Inc.
October 30, 2017

Destination/Source Routing
draft-ietf-rtgwg-dst-src-routing-06

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

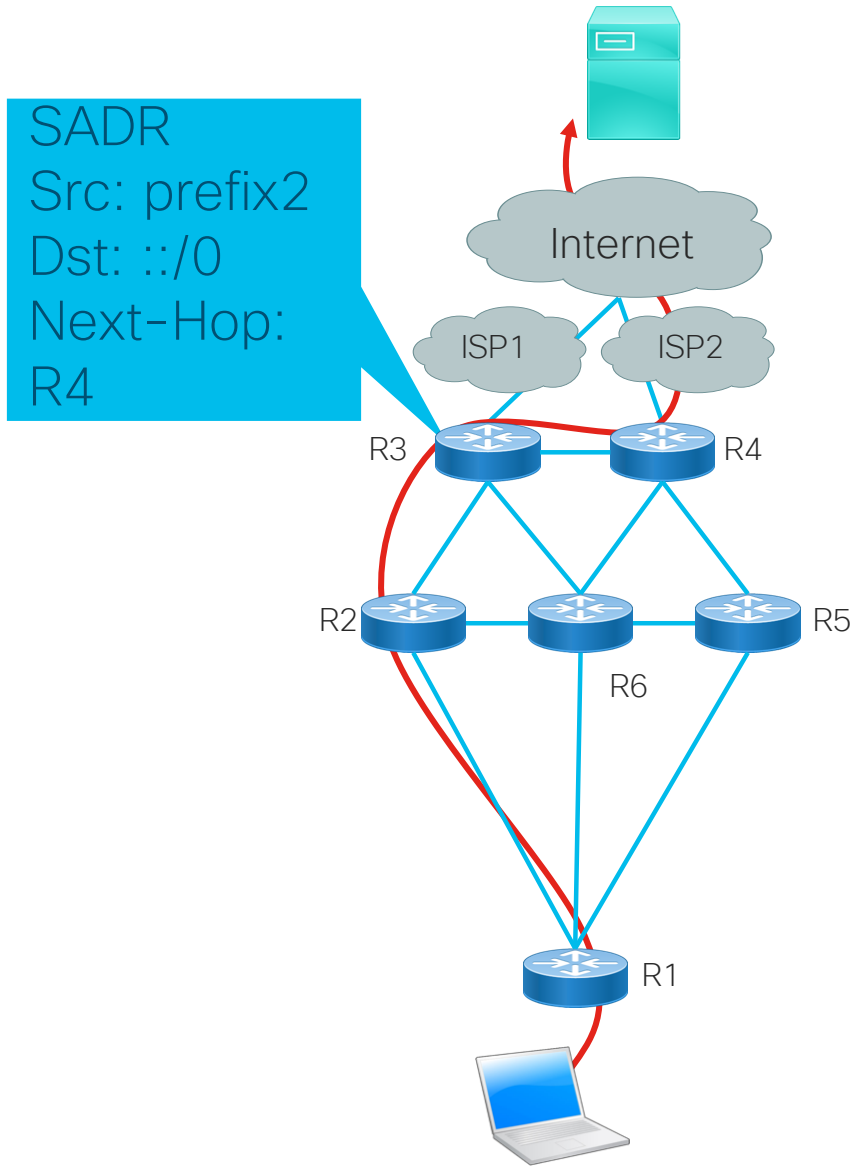
- SADR FIB

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



Summary of SADR for multi-homing

- SADR allows network to send packets to the “right” egress point
- SADR can be deployed incrementally
  - MUST be enabled on the edge
  - SRv6 or tunnels may be used until complete deployments
- Routing protocols can be extended to SADR`
  - draft-baker-ipv6-isis-dst-src-routing

Summary

- Multi-homing in IPv6 is vastly different than in IPv4
- Several addresses per interface
- Several interfaces per host in 2018
- Host must select the right bundle of DNS, address, next hop
- Network must route according to the host-selected address

This session was about technologies being drafted at the IETF and still under development...

Troopers' comments are welcome ☺

A bunch of non-related topics but worth mentioning

IETF Mail Servers under Spam Attack

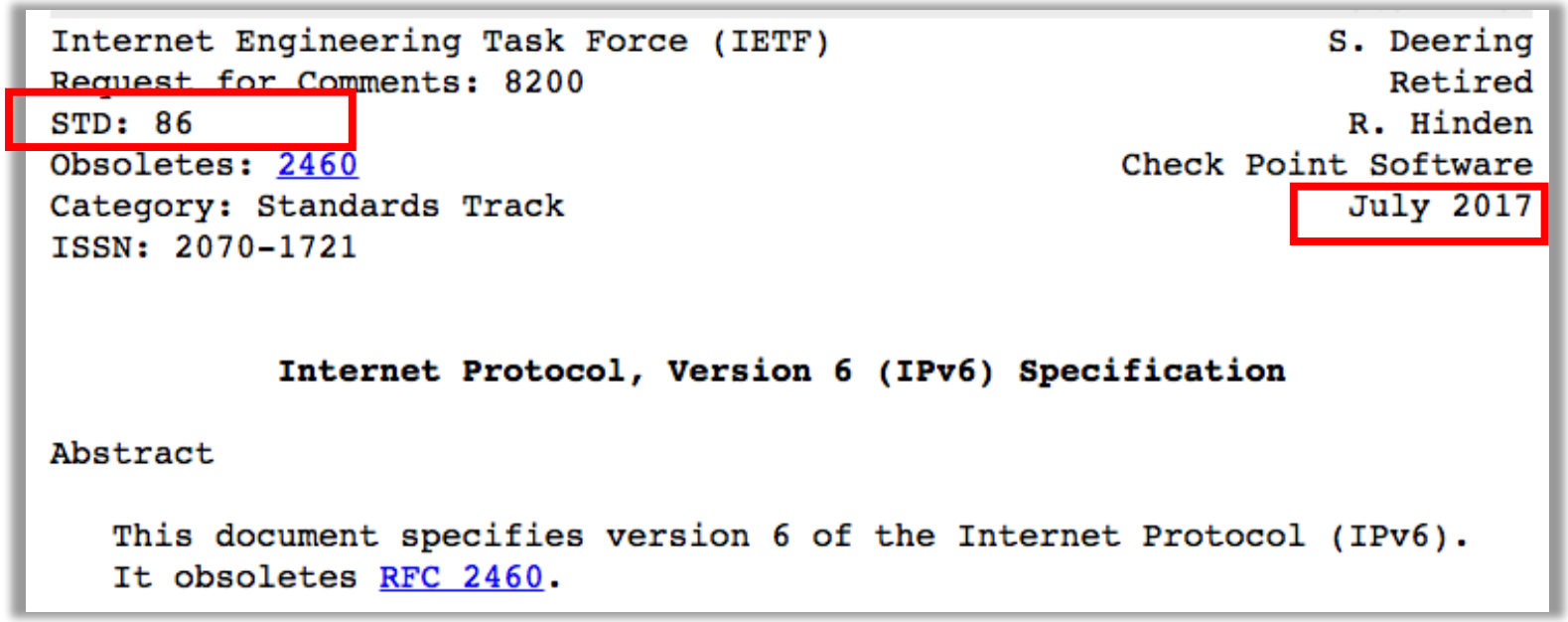
"A rather widespread spam attack is currently underway, and the IETF server is amongst its targets.

...

On a positive note, the IETF will at least be pleased to know that more than 10,000 of those 26,000 hosts are using IPV6. Hooray for our side."

Glen Barney, IT Director, IETF Secretariat, 4 August 2017

Getting More Mature



Internet Engineering Task Force (IETF) — S. Deering, Retired
Request for Comments: 8200 — R. Hinden, Check Point Software
STD: 86
Obsoletes: 2460
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.

Moving to IPv6-only

Network Working Group — R. Hinden
Internet-Draft — Check Point Software
Updates: 5175 (if approved) — B. Carpenter
Intended status: Standards Track — Univ. of Auckland
Expires: November 25, 2018 — May 24, 2018

IPv6 Router Advertisement IPv6-Only Flag
draft-ietf-6man-ipv6only-flag-00

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 RFC5175.

A More Specific Way for Multi-Homing

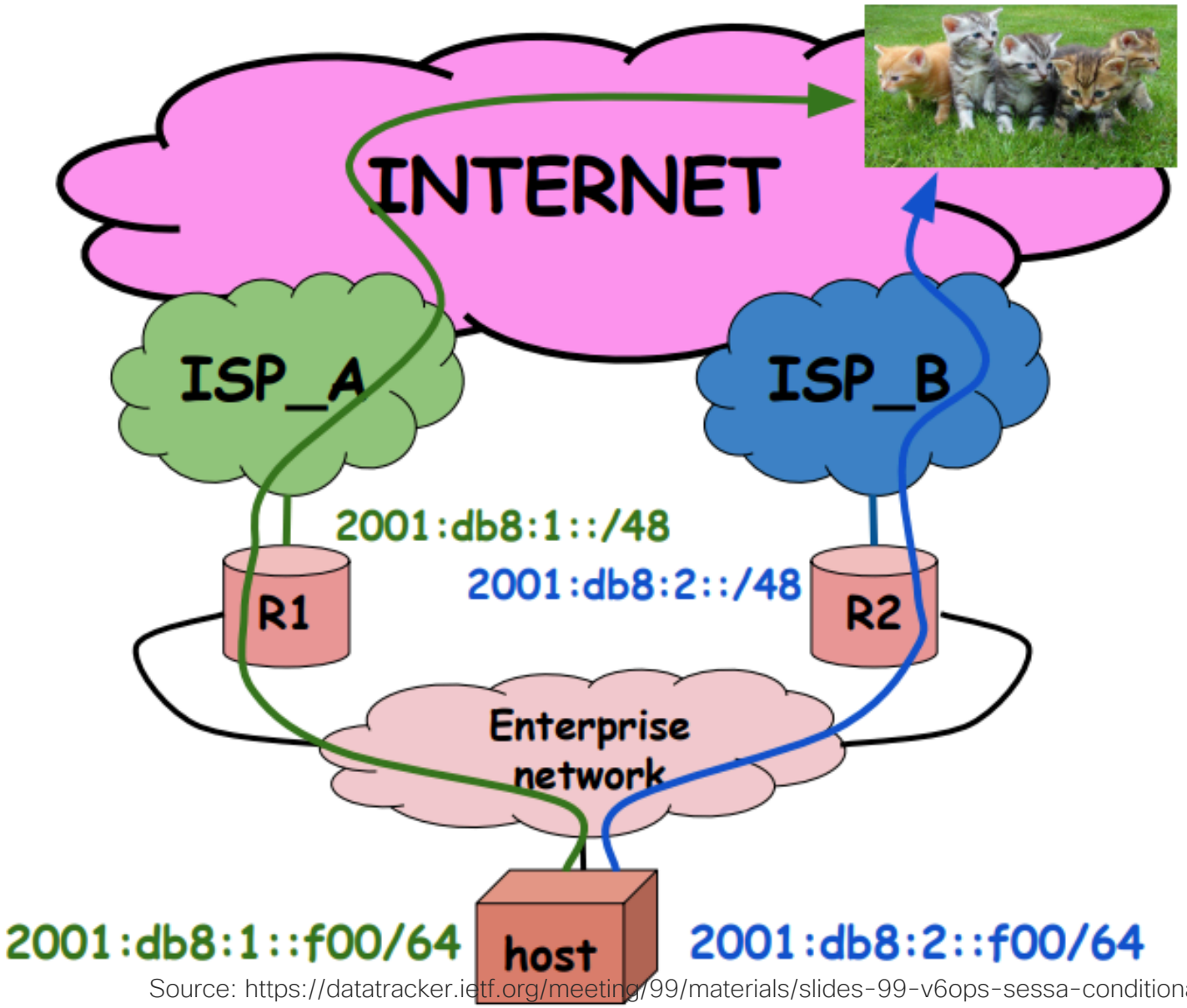
IPv6 Operations
Internet-Draft
Intended status: Informational
Expires: November 5, 2018

J. Linkova
Google
M. Stucchi
RIPE NCC
May 4, 2018

Using Conditional Router Advertisements for Enterprise Multihoming
draft-ietf-v6ops-conditional-ras-04

Abstract

This document discusses the most common scenarios of connecting an enterprise network to multiple ISPs using an address space assigned by an ISP. 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 on the desired egress ISP for that traffic. The "ietf-rtgwg-enterprise-pa-multihoming" document proposes a solution to this problem by introducing a new routing functionality (Source Address Dependent Routing) to solve the uplink selection issue and using Router Advertisements to influence the host source address selection.

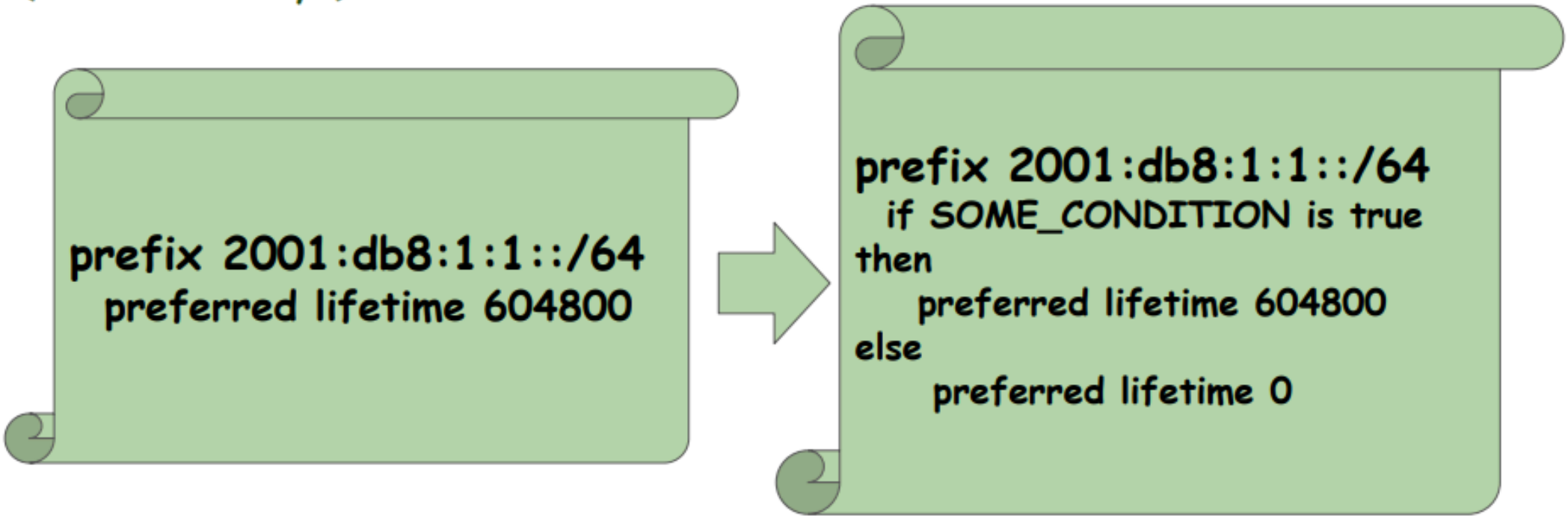


Source: https://datatracker.ietf.org/meeting/99/materials/slides-99-v6ops-sessa-conditional-router-advertisements/

Proposed Approach

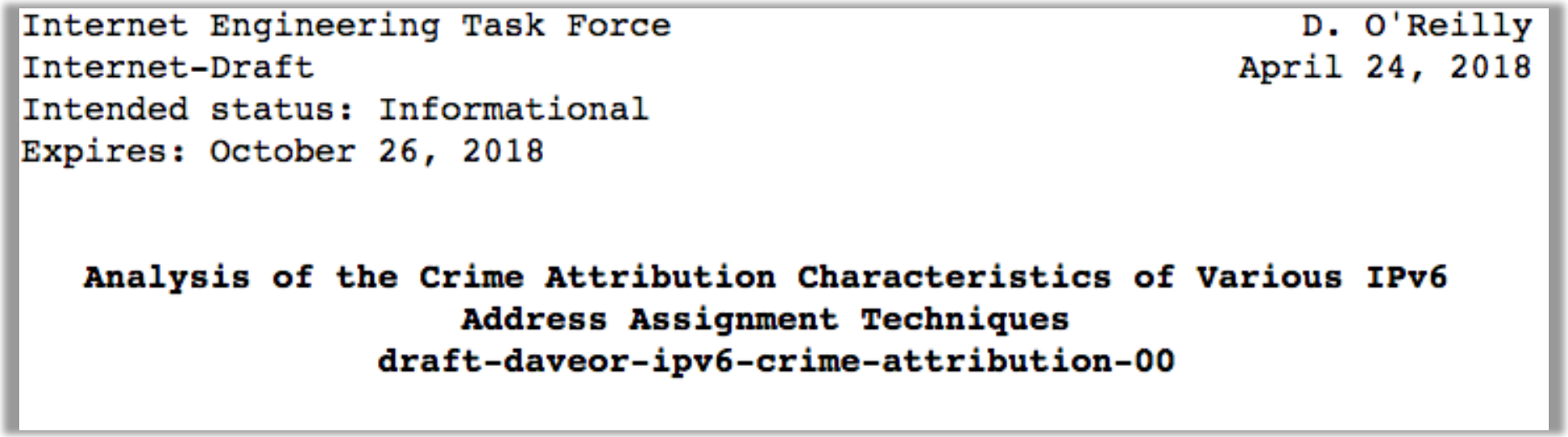
RA fields values are set based on the present network state

("conditionally")



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

CGN Are Bad



Internet Engineering Task Force — D. O'Reilly
Internet-Draft — April 24, 2018
Intended status: Informational
Expires: October 26, 2018

Analysis of the Crime Attribution Characteristics of Various IPv6 Address Assignment Techniques
draft-daveor-ipv6-crime-attribution-00

Europol LEA: CGN Are Painful, IPv6 is THE solution

ARE YOU SHARING THE SAME IP ADDRESS AS A CRIMINAL? LAW ENFORCEMENT CALL FOR THE END OF CARRIER GRADE NAT (CGN) TO INCREASE ACCOUNTABILITY ONLINE

17 October 2017

Press Release

This was supposed to be a temporary solution until the transition to IPv6 was completed but for some operators it has become a substitute for the IPv6 transition. Despite IPv6 being available for more than 5 years the internet access industry increasingly uses CGN technologies (90% for mobile internet and 50% for fixed line) instead of adopting the new standard.

Some Nuggets Heard at Europol

- About CGN sharing ratio
  - Some mobile providers has a sharing ratio of 1:30.000
  - Another ISP in Baltic countries shares 1 public to 100.000 subscribers!
  - Law Enforcement Agencies knows about the 5-tuple with client port and destination address
  - Big content providers do not log the source port / destination address (in case of CDN)
- Big ISP Infosec: IPv6 is more secure than IPv4 because IPsec is always used...

Europol: IPv6 does not solve everything

The Real World and User Identification

	Server IPv4 Only	Server IPv6 Only	Server IPv4 + IPv6
Client IPv4 Only	CGN	No communication	CGN
Client IPv6 Only	NAT64	ID works	ID Works
Client IPv4 + IPv6	CGN	ID works	ID works but hacker can fall back to IPv4*

Not to mention that hackers/malware can always use:
- Open proxies
- VPN
- TOR network

* The user can intentionally or not flip back and forth between IPv4 and IPv6 => correlation must be done (on HTTP cookie?)

NAT does not Protect IoT

"Early 2017, a multi-stage Windows Trojan containing code to scan for vulnerable IoT devices and inject them with Mirai bot code was discovered. The number of IoT devices which were previously safely hidden inside corporate perimeters, vastly exceeds those directly accessible from the Internet, allowing for the creation of botnets with unprecedented reach and scale."

"The call is coming from inside the house! Are you ready for the next evolution in DDoS attacks?"
Steinthor Bjanarson, Arbor Networks, DEFCON 25

Conclusions

- Vast amount of IPv6 addresses and absence of NAT for multihoming
- => PvD and SADR are innovative
- More IPv6-related innovations will come


CISCO