Security and Privacy for Multi-Prefix and Provisioning Domains in IPv6

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

March 2018

Agenda

- Problem statement: what are we trying to solve?
- Introduction to the technologies
  - Provisioning the host with provisioning domains
  - Routing to the multi-home exit with Source Address Dependent Routing
- Potential attacks on PvD and SADR
- Other topics about IPv6 and security

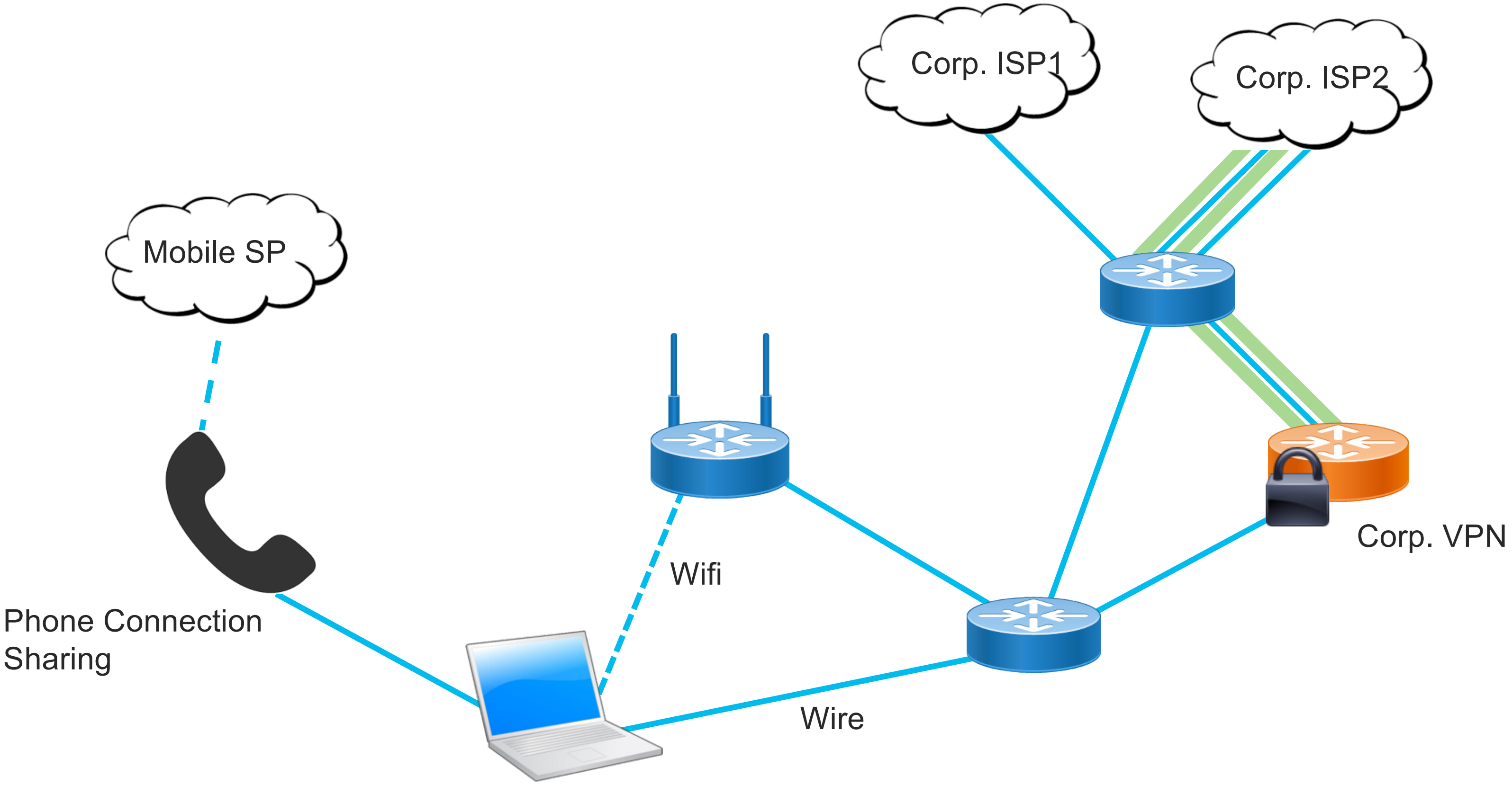
This session is about technologies being drafted at the IETF and still under development…

Troopers’ comments will be welcome ☺

Problem statement

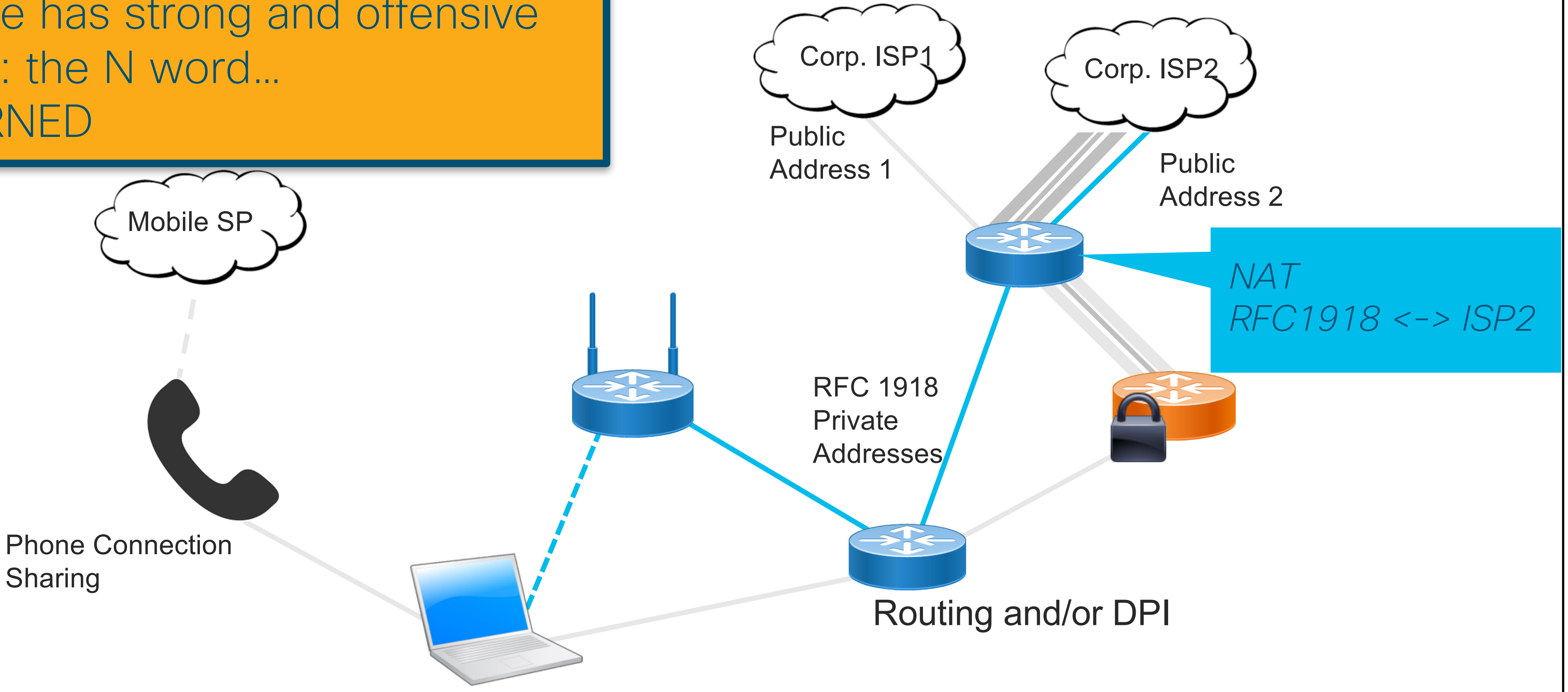
Hosts and networks are multi-homed

Just a few examples…



Multi-Homing, the legacy way…

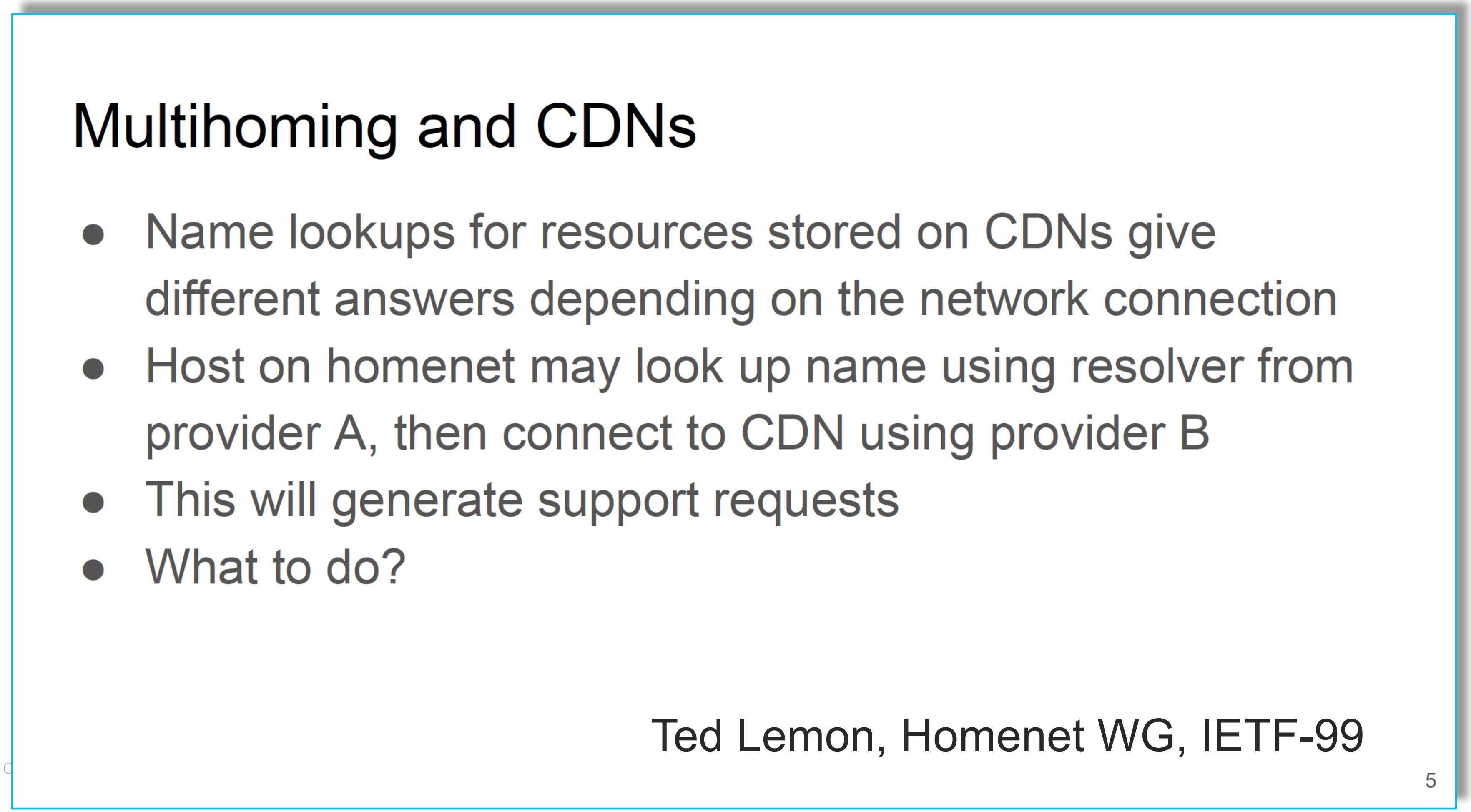
WARNING
This slide has strong and offensive wording: the N word…
BE WARNED



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.

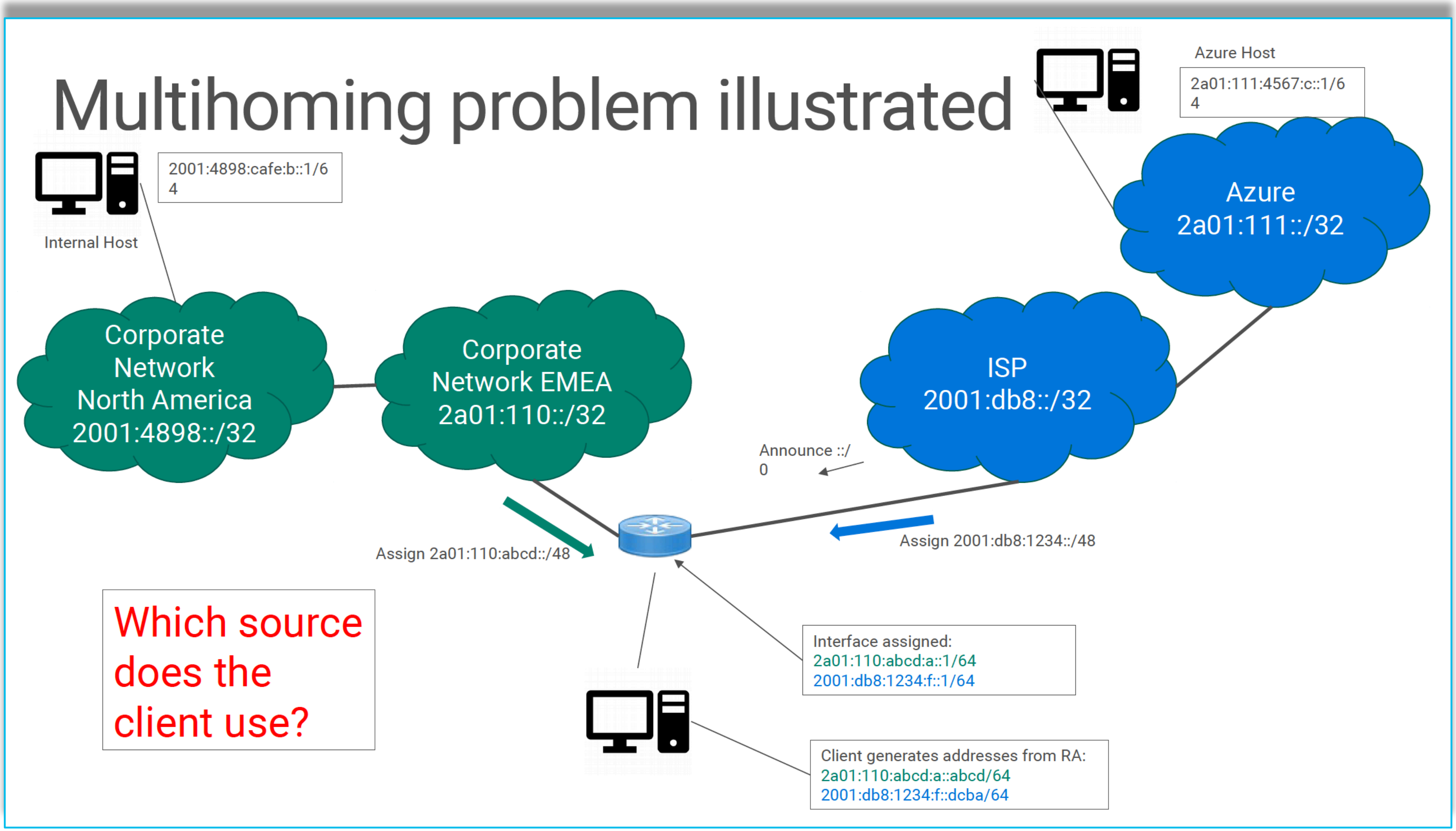
Bundling IP address & DNS resolver



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



Multihoming problem illustrated

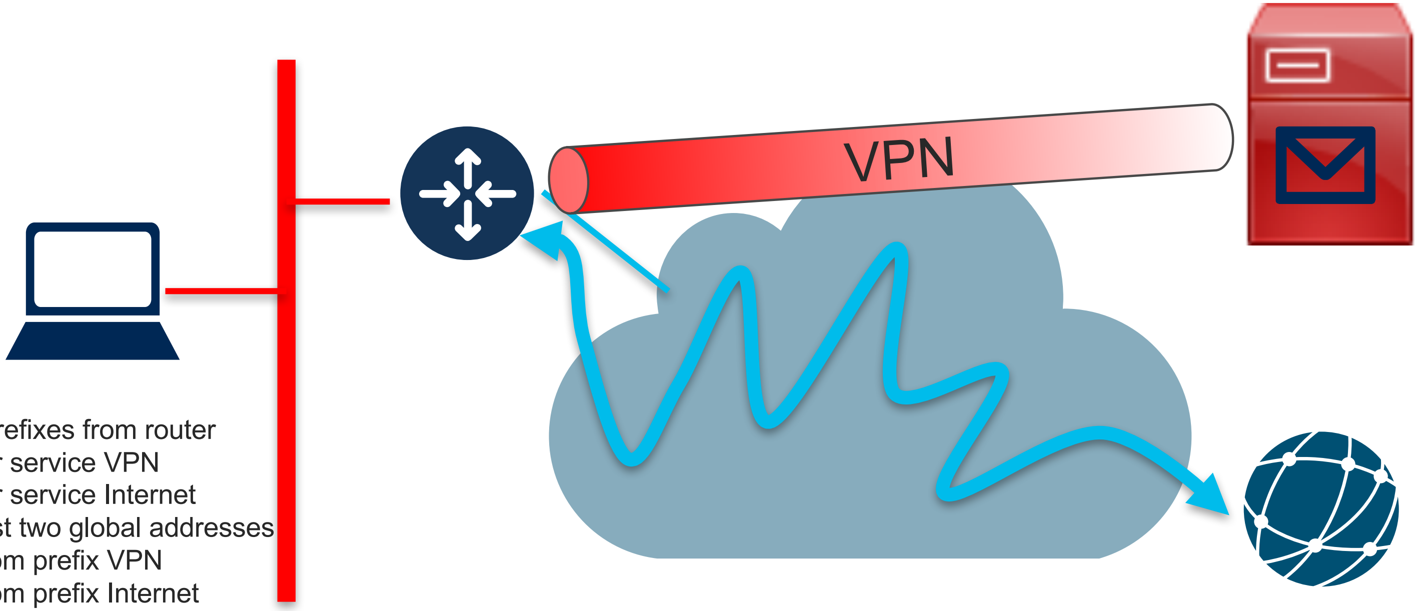
Interface assigned:
2a01:110:abcd:a::1/64
2001:db8:1234:f::1/64

Client generates addresses from RA:
2a01:110:abcd:a::abcd/64
2001:db8:1234:f::dcba/64

Which source does the client use?

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

Selecting the Service by Source Address



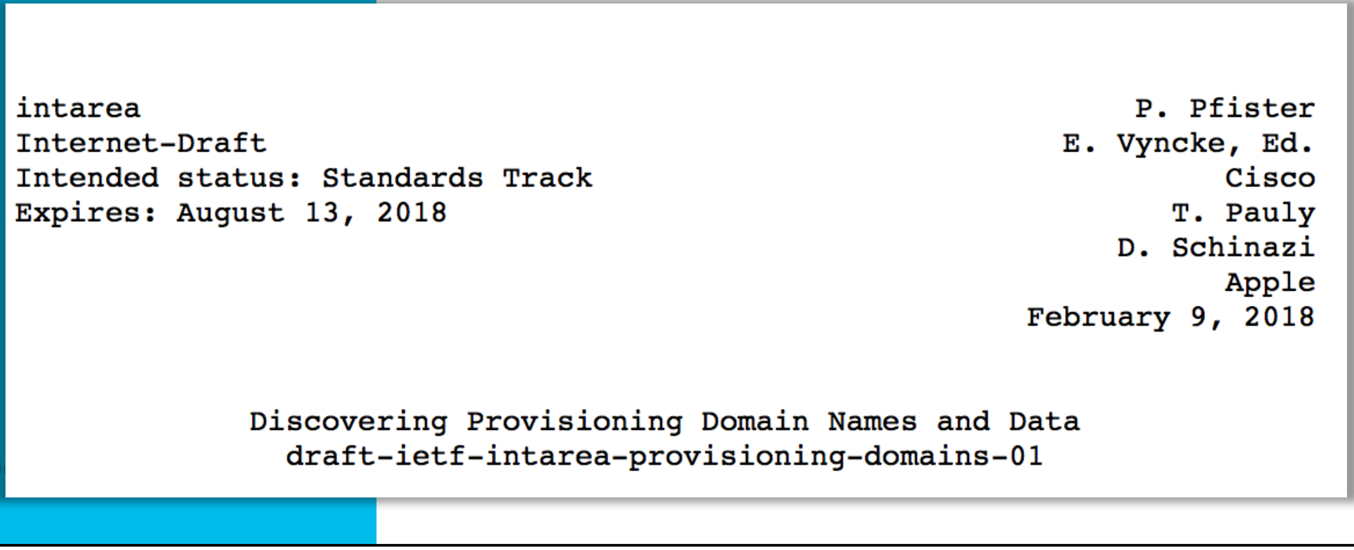
Two prefixes from router
1. For service VPN
2. For service Internet

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                                                       P. Pfister
Internet-Draft                                            E. Vyncke, Ed.
Intended status: Standards Track                                   Cisco
Expires: August 13, 2018                                        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.*

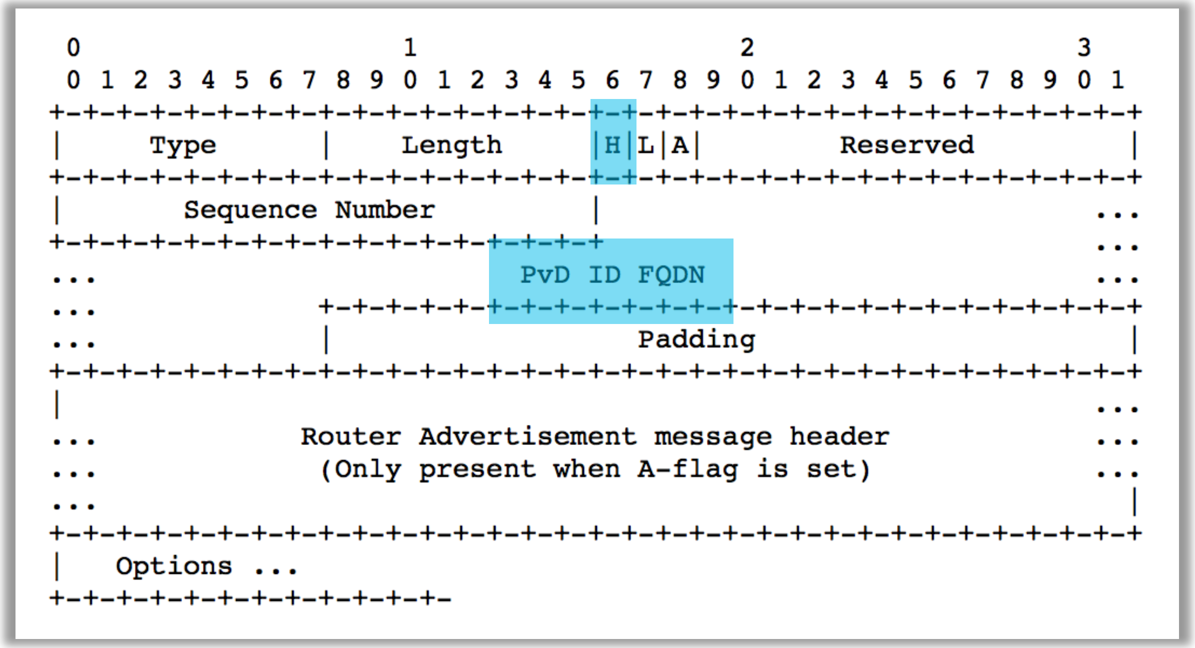
Differentiate provisioning domains by using FQDN identifiers.

2. Extend PvD with additional information

For the applications: name, captive portal, etc…

Step 1: Identify PvDs

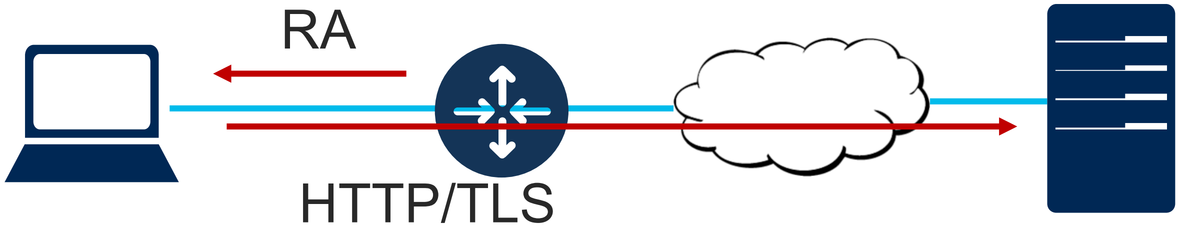
With the PvD ID Router Advertisement Option



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |H|L|A|       Reserved          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Sequence Number         |                             ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                             ...
...                         PvD ID FQDN                       ...
...             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
...             |                 Padding                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                             ...
...            Router Advertisement message header            ...
...             (Only present when A-flag is set)             ...
...                                                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Options ...
+-+-+-+-+-+-+-+-+-+-+-+-
```

- 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 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

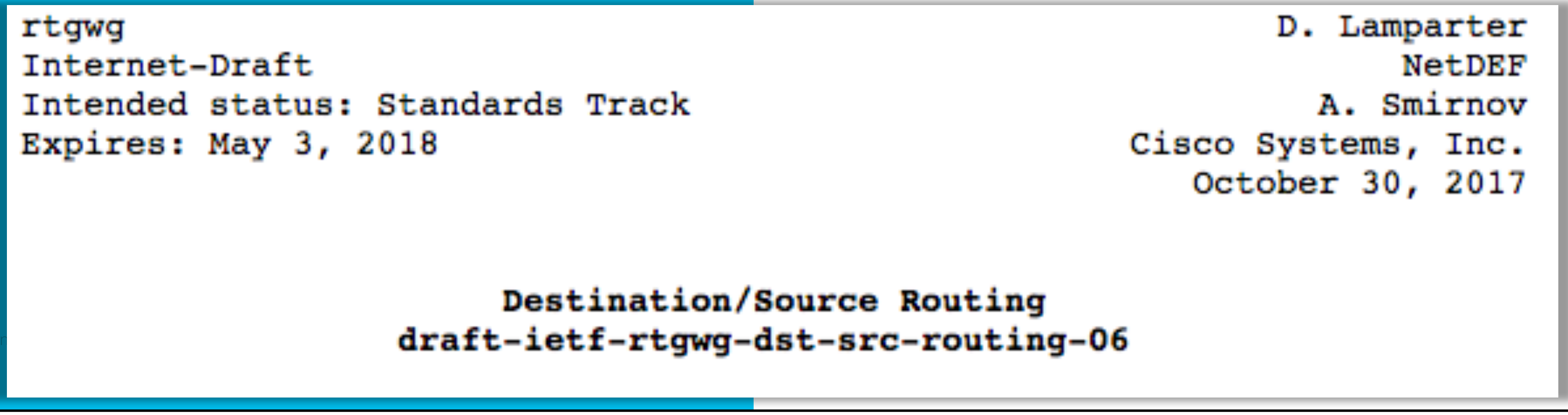
Linux - https://github.com/IPv6-mPvD

- **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                                                D. Lamparter
Internet-Draft                                            NetDEF
Intended status: Standards Track                      A. Smirnov
Expires: May 3, 2018                         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

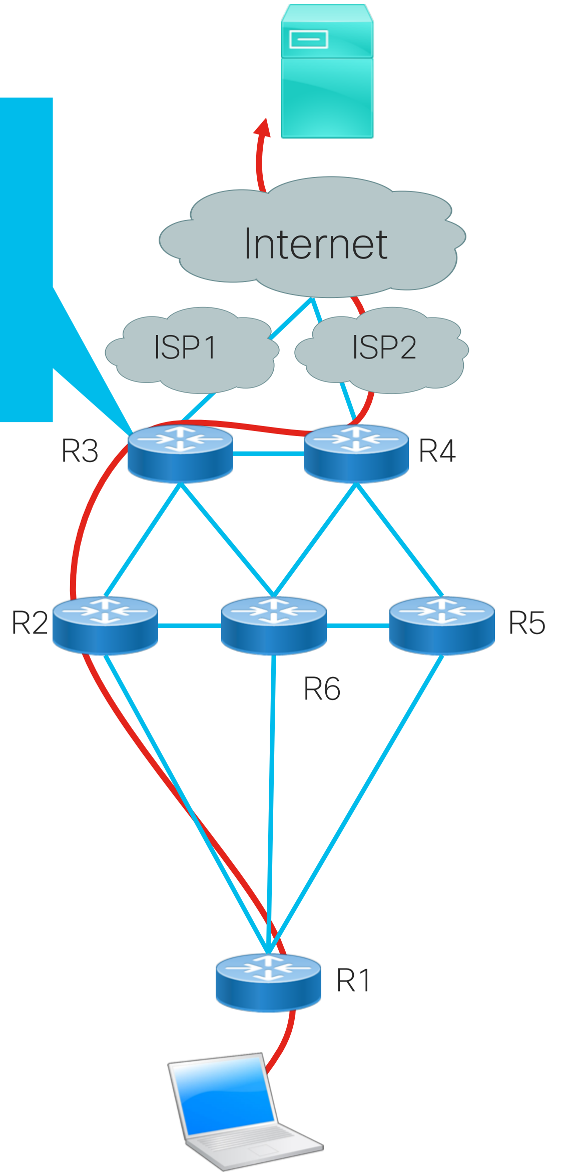
- SADR FIB

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



SADR
Src: prefix2
Dst: ::/0
Next-Hop:
R4

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

What about security ?

Rogue PvD?

- Can PvD ID be spoofed?
- Confidentiality of additional information ?

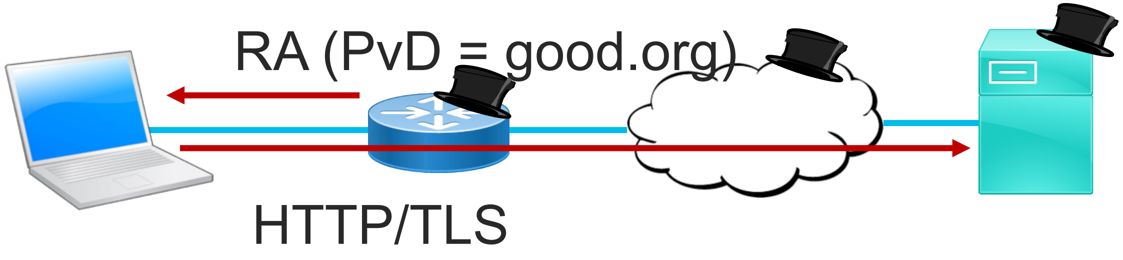
Confidentiality of PvD Additional Information

- The well-known URL https://pvd-name.example.org/.well-known/pvd could contain some sensitive data (bandwidth, recursive DNS servers, ...)
- This well-known URL is guessable ;-)
- How to provide confidentiality ?

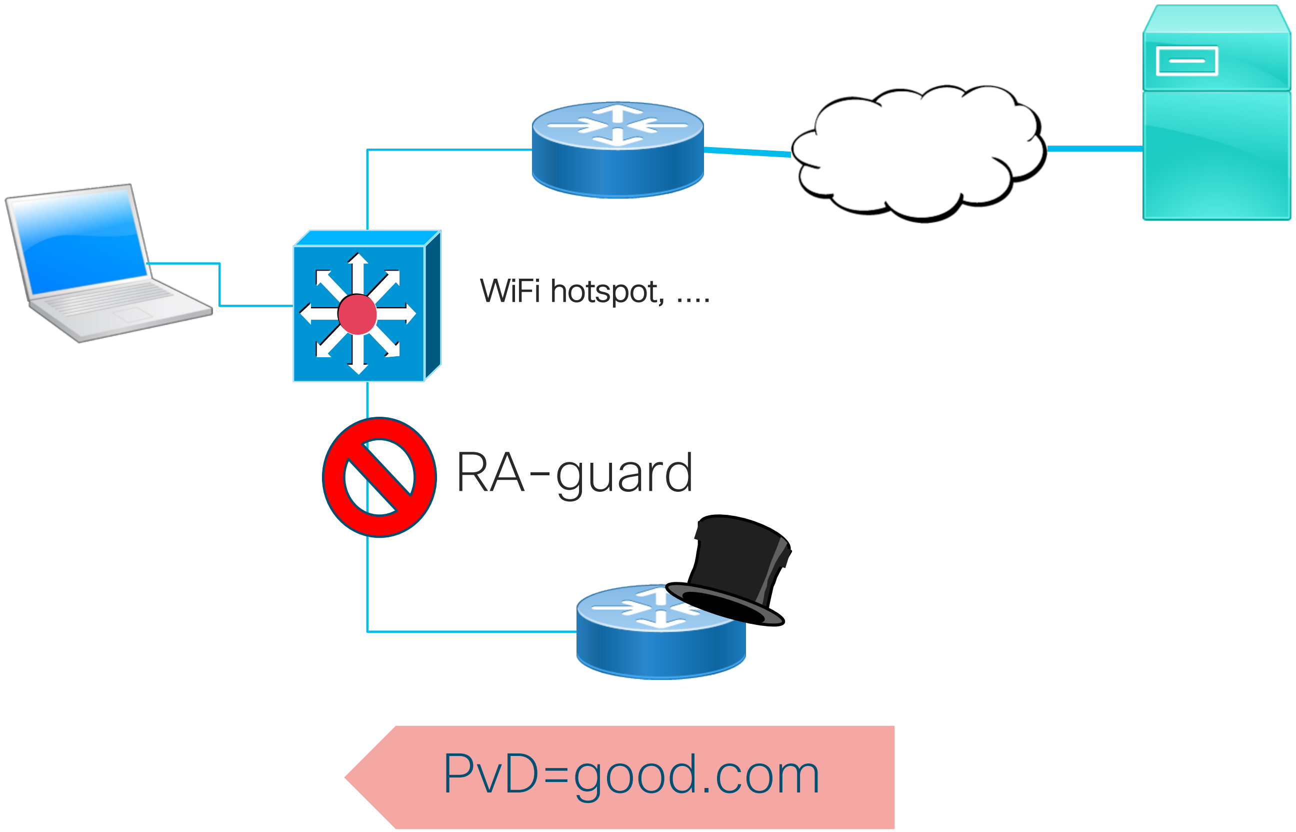
- 1) do not put anything which is really confidential
- 2) the HTTPS server should reject connections originated from prefixes not belonging to example.org

Spoofing the PvD ID

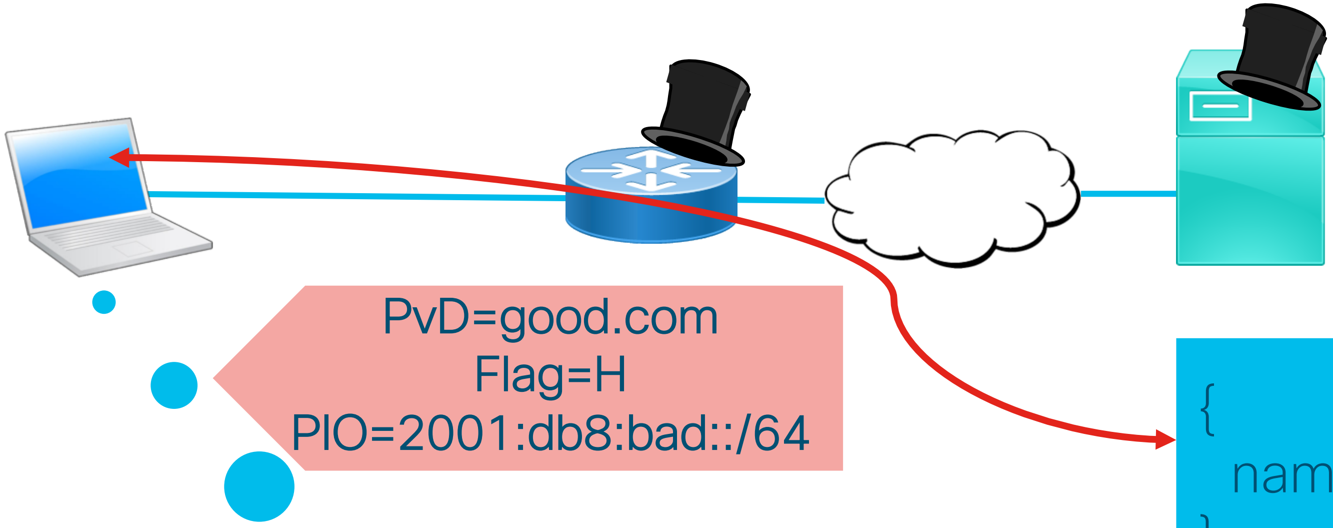
- Can an hostile party send rogue PvD, pretending to be example.org while they are hacker.org ?
- No signature in the RA option (SeND not used)



Layer-2 Adjacent Attacker



Attackers are First Hop Router and PvD "Server"

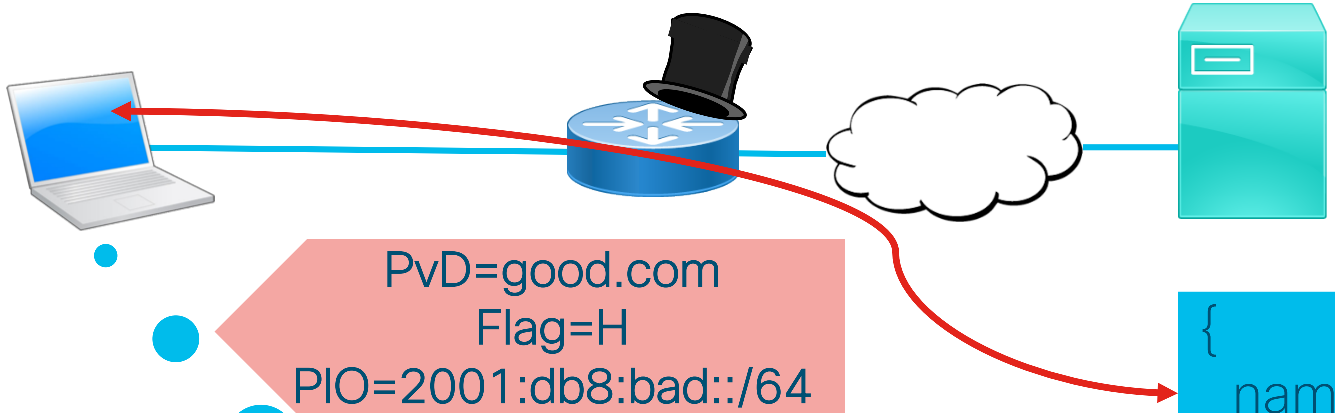


PvD=good.com
Flag=H
PIO=2001:db8:bad::/64

```
{
  name : "good.com" ;
}
```

H-flag is required
X.509 certificate is wrong
=> Do not trust

Attacker is the First Hop Router

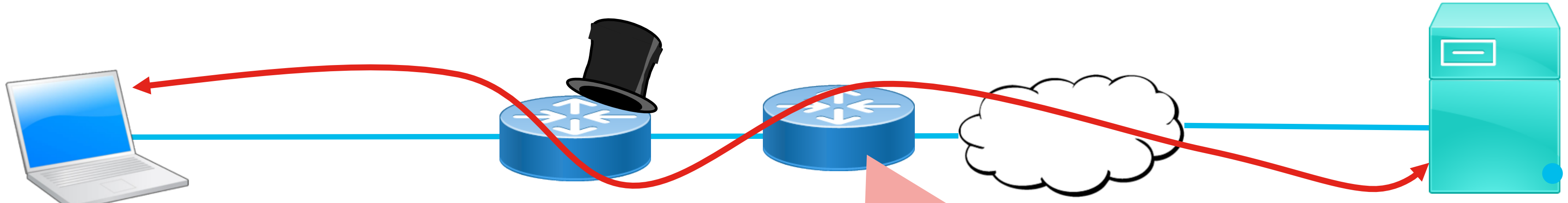


PvD=good.com
Flag=H
PIO=2001:db8:bad::/64

```
{
  name : “good.com” ;
  prefixes: [”2001:db8:beef::”];
}
```

H-flag is required
PIO not covered by
”Prefixes”
=> Do not trust

Attacker is the First Hop Router with NPTv6



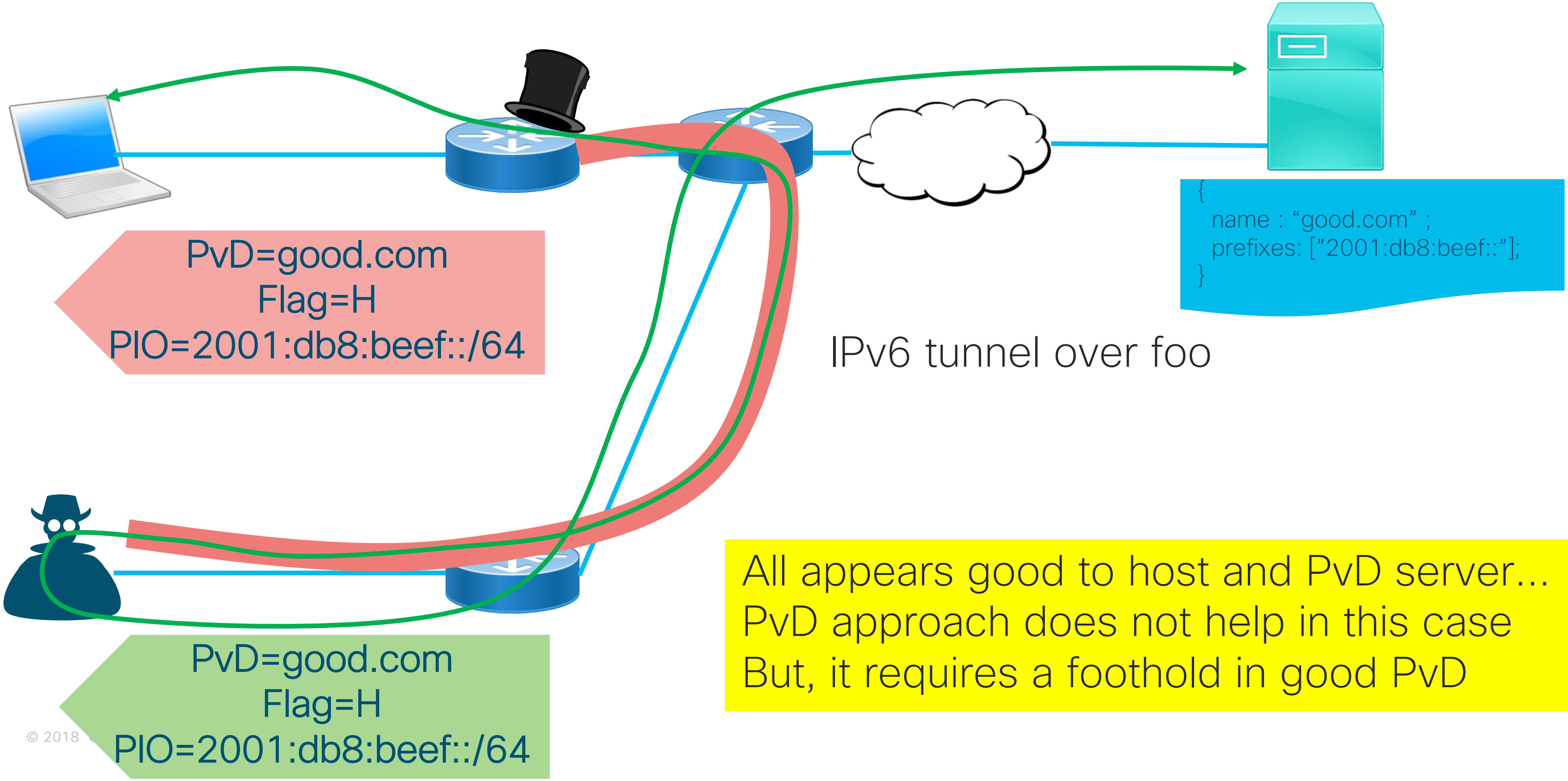
PvD=good.com
Flag=H
PIO=2001:db8:beef::/64

NTP
2001:db9:beef::
⇔
2001:db8:bad::

H-flag is required
But cannot connect to
the PvD server
=> Do not trust

My PvD are in
2001:db8:beef:: but this
TLS client is in
2001:db8:bad::
=> Drop HTTPS request

Attacker Has a Foothold in ”Good” PvD



PvD=good.com
Flag=H
PIO=2001:db8:beef::/64

```
{
  name : “good.com” ;
  prefixes: [”2001:db8:beef::”];
}
```

IPv6 tunnel over foo

PvD=good.com
Flag=H
PIO=2001:db8:beef::/64

All appears good to host and PvD server…
PvD approach does not help in this case
But, it requires a foothold in good PvD

Host Privacy with Additional Information

- Each host will fetch the additional information on connection
- The HTTPS server will know the IP address of all clients and that the client is connecting...
  - Some privacy issues esp. if using EUI-64 or stable address

- Host can change to another IP address after fetching the file
- HTTPS belongs to the network operator (same as RADIUS, DHCP, ...)
- Anyway, it has more privacy than http://captive.example.com/hotspot-detect.html which belongs to another global operator

So, PvD with additional information are not THAT bad

But we all know that nothing is never 100% secure !

And, in current standards/deployments hosts have to trust the first level of access (switch, WiFi AP, router)

Attack on SADR ?

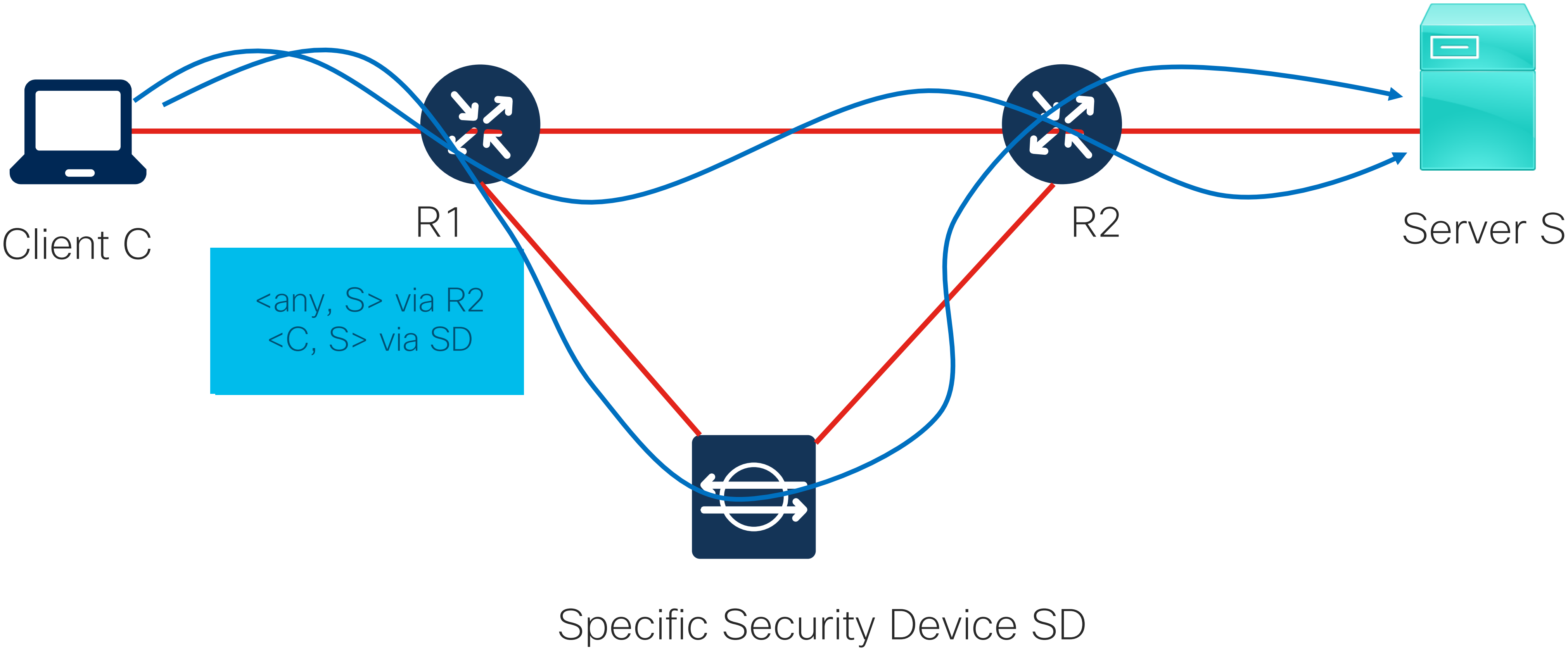
- New forwarding mechanism…
- New attacks?

DoS on Slower SADR Routers

- Based on the implementation, doing SADR forwarding may be slower than plain destination forwarding
  - Up to 256 times slower for very dumb implementations
  - Just 5% performance loss on smart ones ;-)

- Packets could be injected with specific <src, dst> to cause a performance drop on dumb implementations
  - Mitigation: use only good routers

Intercepting Traffic with Specific SADR



<any, S> via R2
<C, S> via SD

Injecting Very Specific SADR

- Injecting a /128 SADR route
- Can steer packets from one source via a specific path
  - Interception and MiTM attacks
  - DoS

- *Routing Protocol should be configured with security*

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

Troopers’ comments are welcome ☺

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."

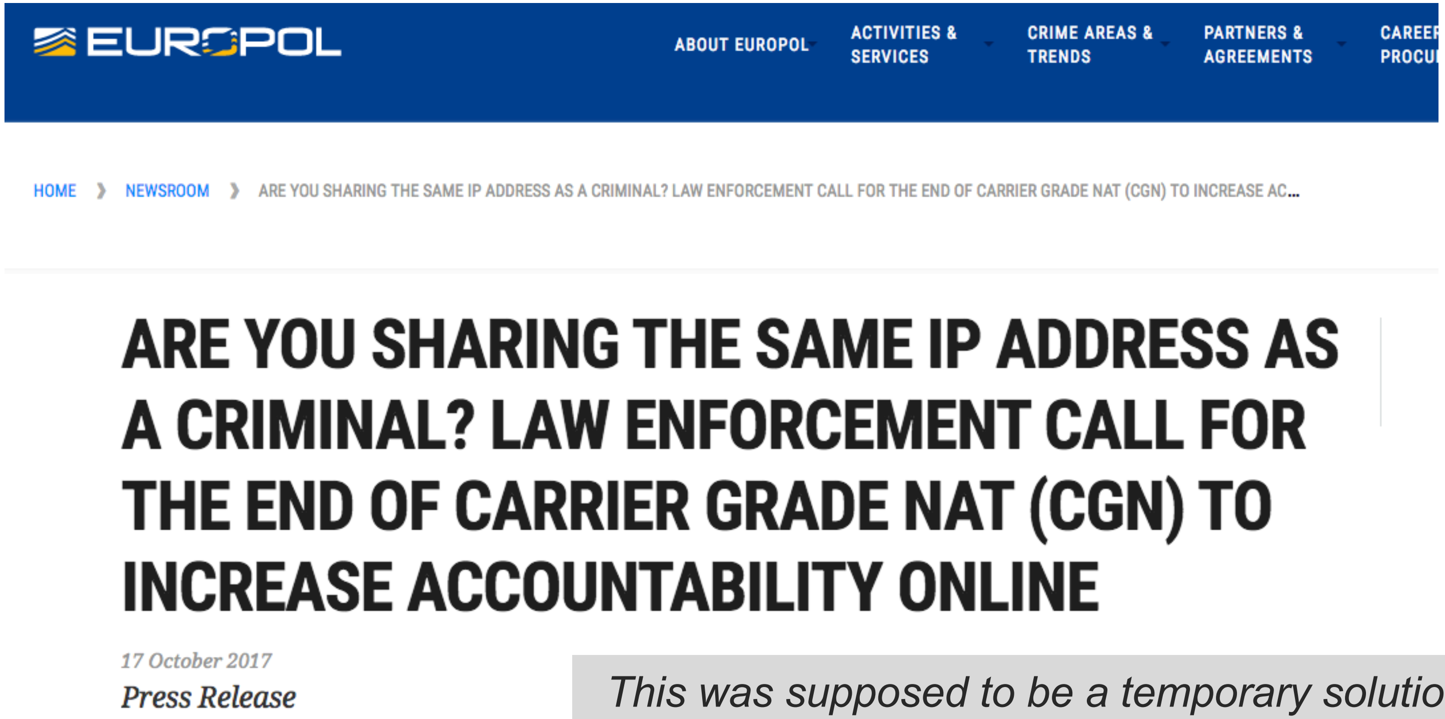
Glen Barney, IT Director, IETF Secretariat, 4 August 2017

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

Europol LEA: CGN Are Painful, IPv6 is THE solution



HOME ❯ NEWSROOM ❯ ARE YOU SHARING THE SAME IP ADDRESS AS A CRIMINAL? LAW ENFORCEMENT CALL FOR THE END OF CARRIER GRADE NAT (CGN) TO INCREASE AC...

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

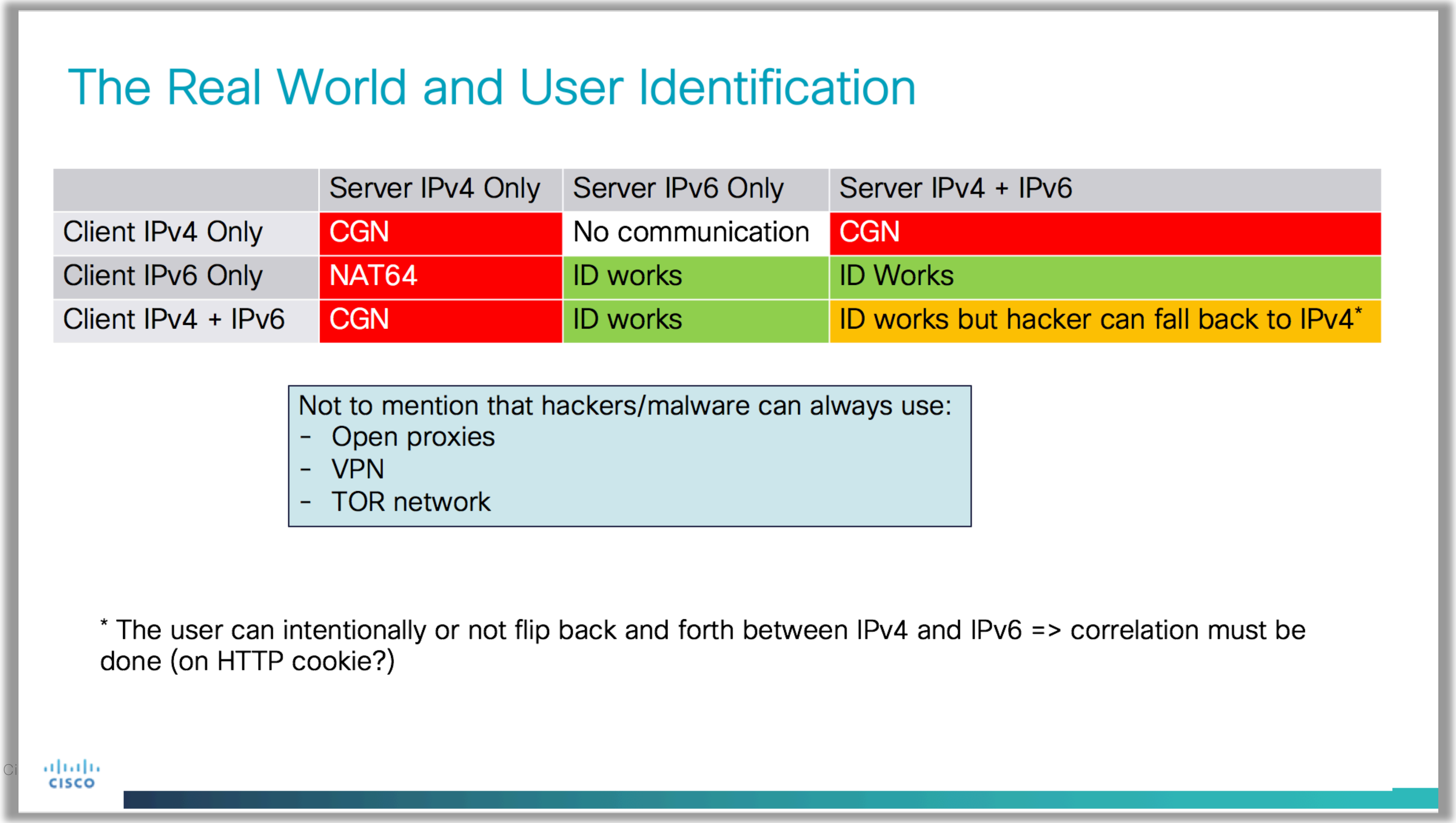
Press Release

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

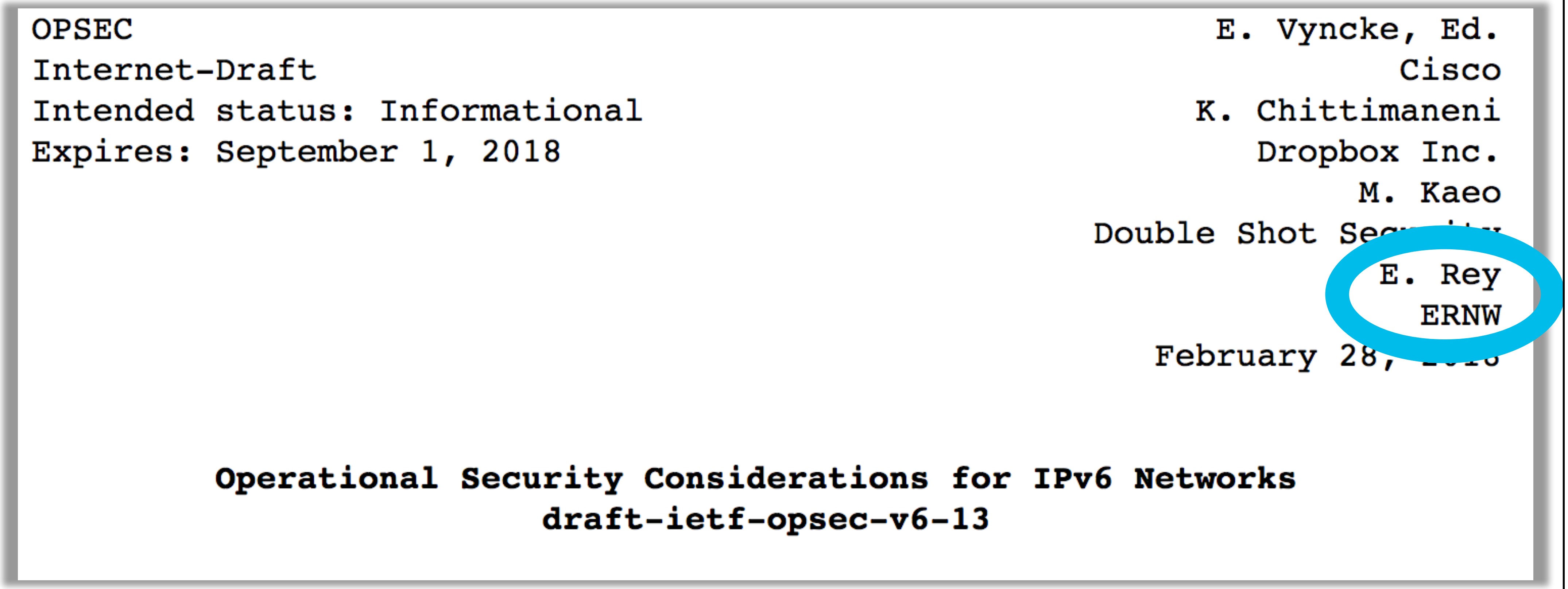
	Server IPv4 Only	Server IPv6 Only	Server IPv4 + IPv6
Client IPv4 Only	CGN	No communication	CGN
Client IPv6 Only	NAT64	ID works	ID Works
Client IPv4 + IPv6	CGN	ID works	ID works but hacker can fall back to IPv4*

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?)

And as we are at Troopers



```
OPSEC                                                   E. Vyncke, Ed.
Internet-Draft                                                   Cisco
Intended status: Informational                           K. Chittimaneni
Expires: September 1, 2018                                  Dropbox Inc.
                                                                 M. Kaeo
                                                    Double Shot Security
                                                                  E. Rey
                                                                    ERNW
                                                       February 28, 2018
```

Operational Security Considerations for IPv6 Networks
draft-ietf-opsec-v6-13

https://tools.ietf.org/html/draft-ietf-opsec-v6-13

Conclusions

- Vast amount of IPv6 addresses and absence of NAT for multihoming
- => PvD and SADR are innovative
- More IPv6-related innovations will come
- Let’s work together to make them secure !

cisco