Let’s stop using DNS

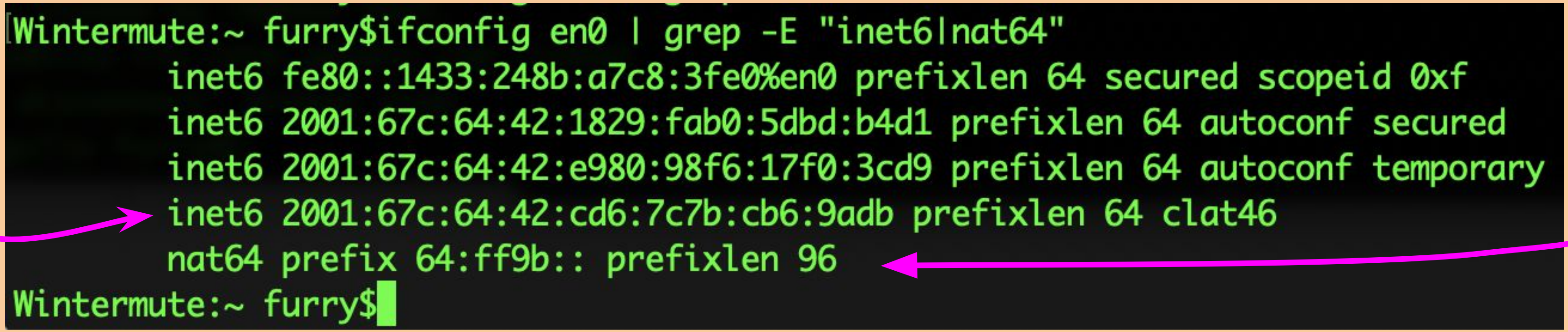
Let's stop using DNS64

for NAT64 prefix discovery

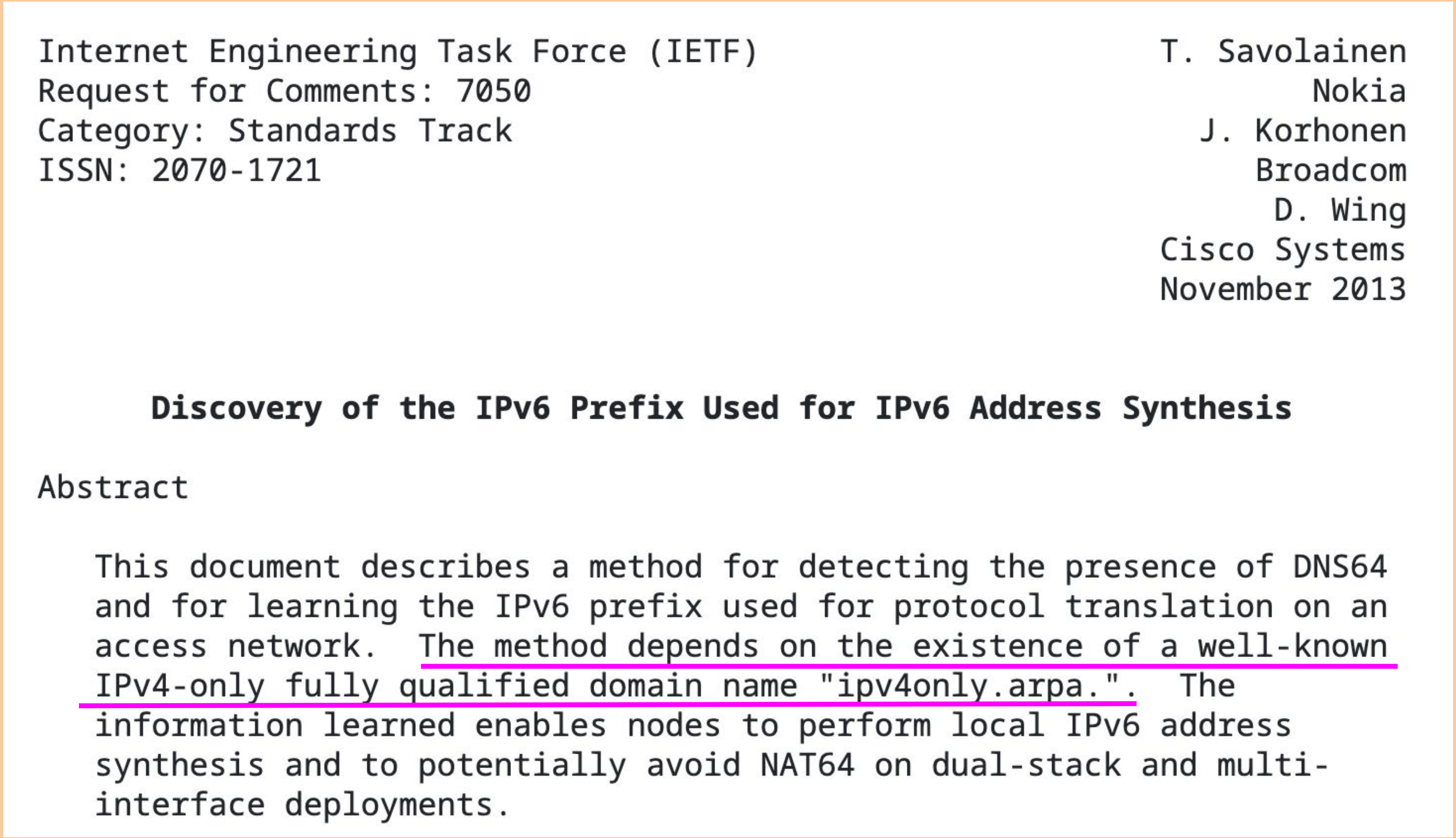
Jen Linkova, furry13@gmail.com, RIPE89

If you run IPv6-only network...

- Endpoints run <u>CLAT</u> (to provide IPv4-only applications with IPv4)
- To run CLAT, the client needs to know the NAT64 prefix



```
Wintermute:~ furry$ifconfig en0 | grep -E "inet6|nat64"
        inet6 fe80::1433:248b:a7c8:3fe0%en0 prefixlen 64 secured scopeid 0xf
        inet6 2001:67c:64:42:1829:fab0:5dbd:b4d1 prefixlen 64 autoconf secured
        inet6 2001:67c:64:42:e980:98f6:17f0:3cd9 prefixlen 64 autoconf temporary
        inet6 2001:67c:64:42:cd6:7c7b:cb6:9adb prefixlen 64 clat46
        nat64 prefix 64:ff9b:: prefixlen 96
Wintermute:~ furry$
```



Internet Engineering Task Force (IETF)
Request for Comments: 7050
Category: Standards Track
ISSN: 2070-1721

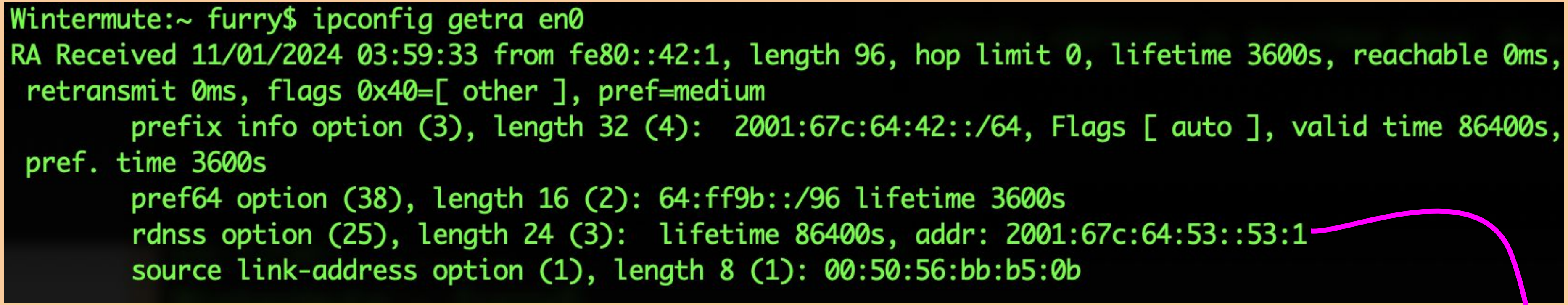
T. Savolainen
Nokia
J. Korhonen
Broadcom
D. Wing
Cisco Systems

November 2013

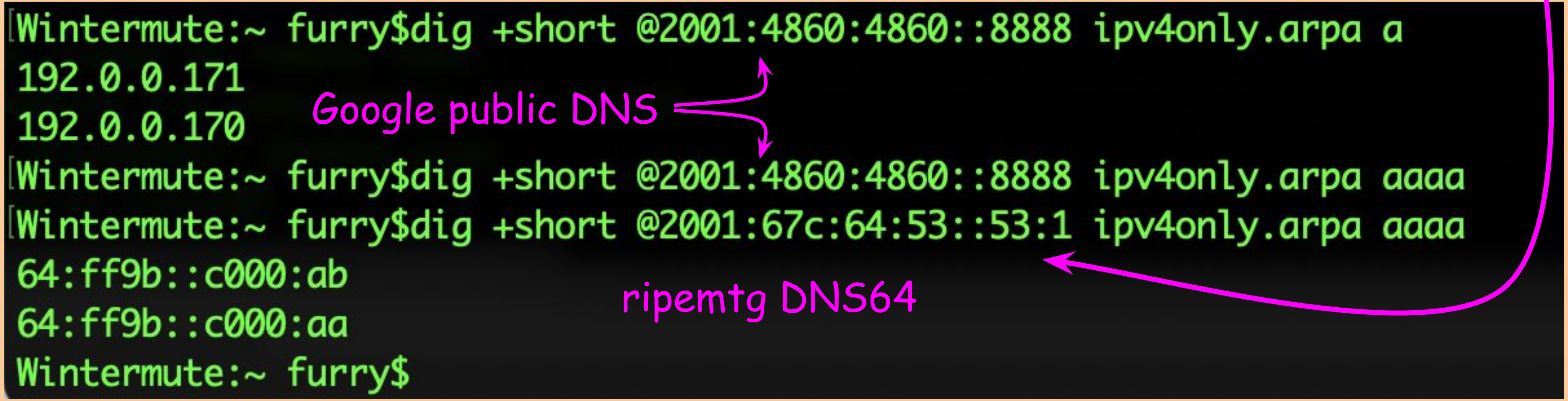
Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis

Abstract

This document describes a method for detecting the presence of DNS64 and for learning the IPv6 prefix used for protocol translation on an access network. The method depends on the existence of a well-known IPv4-only fully qualified domain name "ipv4only.arpa.". The information learned enables nodes to perform local IPv6 address synthesis and to potentially avoid NAT64 on dual-stack and multi-interface deployments.

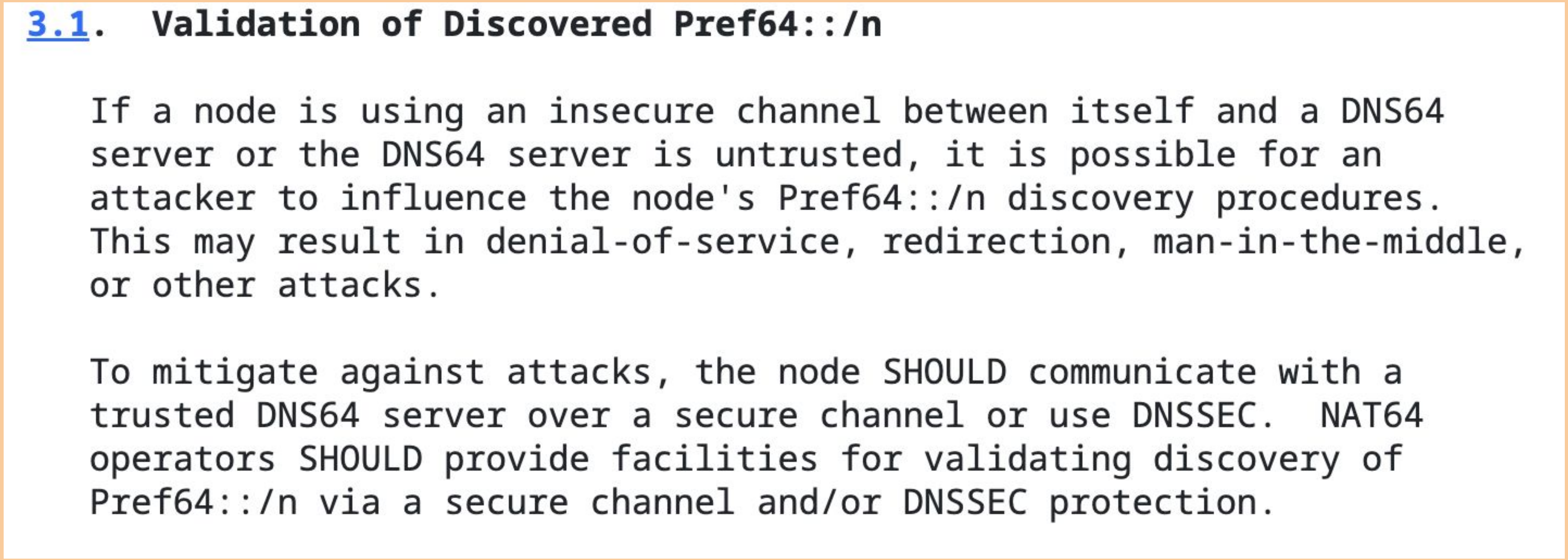


```
Wintermute:~ furry$ ipconfig getra en0
RA Received 11/01/2024 03:59:33 from fe80::42:1, length 96, hop limit 0, lifetime 3600s, reachable 0ms,
 retransmit 0ms, flags 0x40=[ other ], pref=medium
        prefix info option (3), length 32 (4):  2001:67c:64:42::/64, Flags [ auto ], valid time 86400s,
 pref. time 3600s
        pref64 option (38), length 16 (2): 64:ff9b::/96 lifetime 3600s
        rdnss option (25), length 24 (3):  lifetime 86400s, addr: 2001:67c:64:53::53:1
        source link-address option (1), length 8 (1): 00:50:56:bb:b5:0b
```



```
Wintermute:~ furry$dig +short @2001:4860:4860::8888 ipv4only.arpa a
192.0.0.171
192.0.0.170
Wintermute:~ furry$dig +short @2001:4860:4860::8888 ipv4only.arpa aaaa
Wintermute:~ furry$dig +short @2001:67c:64:53::53:1 ipv4only.arpa aaaa
64:ff9b::c000:ab
64:ff9b::c000:aa
Wintermute:~ furry$
```

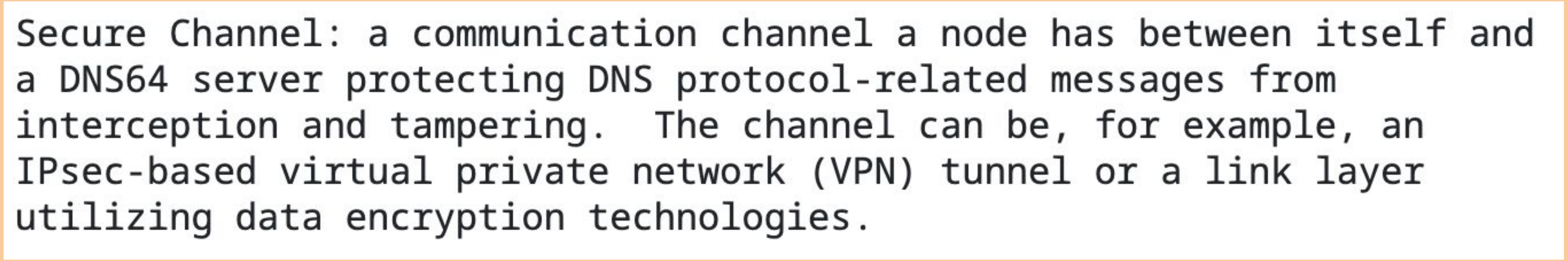
RFC7050: What Could Possibly Go Wrong?



3.1. Validation of Discovered Pref64::/n

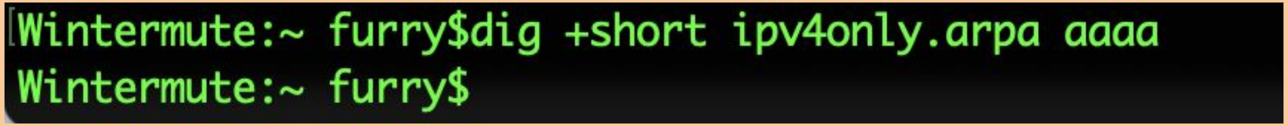
If a node is using an insecure channel between itself and a DNS64 server or the DNS64 server is untrusted, it is possible for an attacker to influence the node's Pref64::/n discovery procedures. This may result in denial-of-service, redirection, man-in-the-middle, or other attacks.

To mitigate against attacks, the node SHOULD communicate with a trusted DNS64 server over a secure channel or use DNSSEC. NAT64 operators SHOULD provide facilities for validating discovery of Pref64::/n via a secure channel and/or DNSSEC protection.

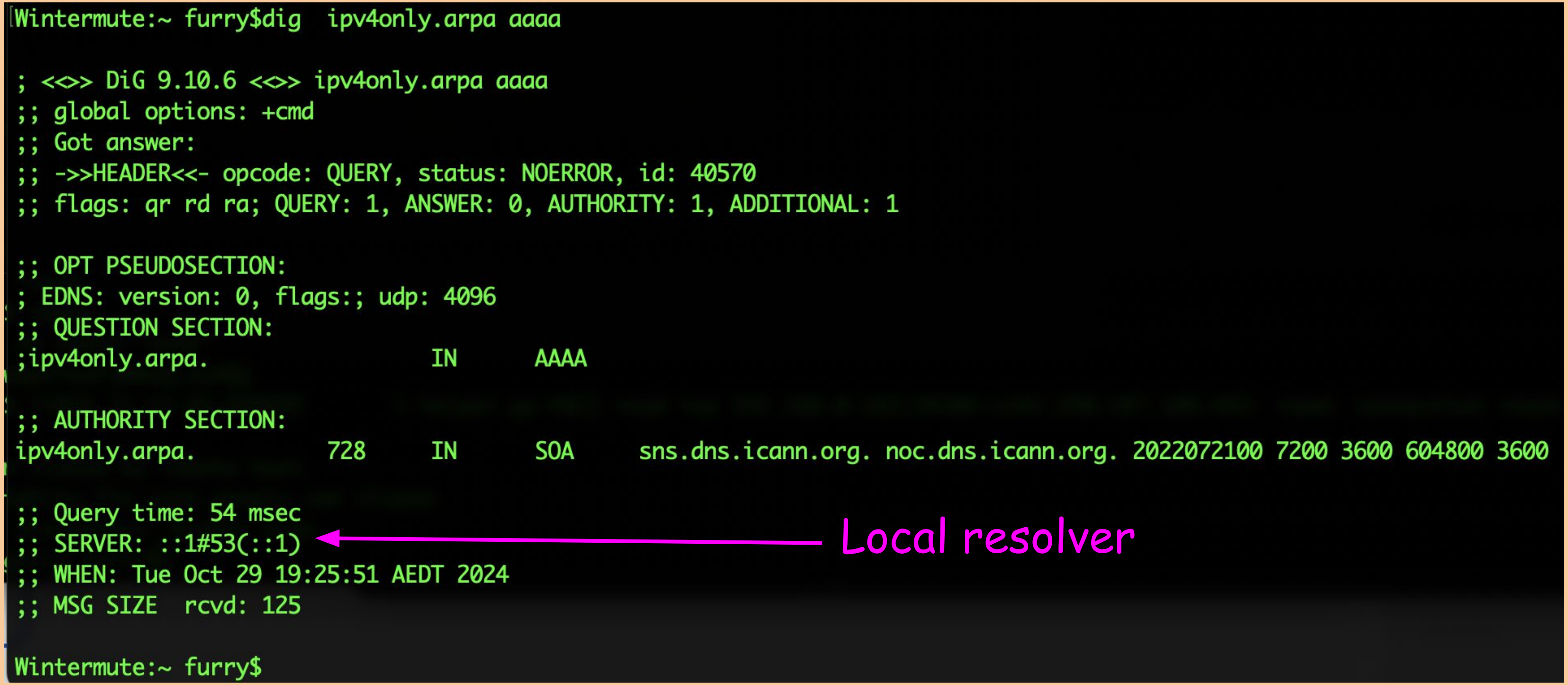


Secure Channel: a communication channel a node has between itself and a DNS64 server protecting DNS protocol-related messages from interception and tampering. The channel can be, for example, an IPsec-based virtual private network (VPN) tunnel or a link layer utilizing data encryption technologies.

What Else Could Possibly Go Wrong?



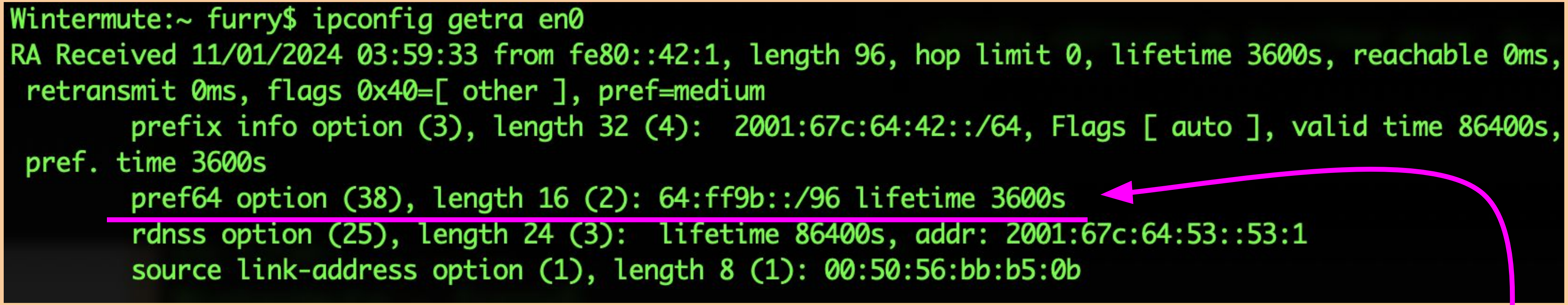
```
Wintermute:~ furry$dig +short ipv4only.arpa aaaa
Wintermute:~ furry$
```



```
Wintermute:~ furry$dig  ipv4only.arpa aaaa

; <<>> DiG 9.10.6 <<>> ipv4only.arpa aaaa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40570
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ipv4only.arpa.                 IN      AAAA

;; AUTHORITY SECTION:
ipv4only.arpa.          728     IN      SOA     sns.dns.icann.org. noc.dns.icann.org. 2022072100 7200 3600 604800 3600

;; Query time: 54 msec
;; SERVER: ::1#53(::1)
;; WHEN: Tue Oct 29 19:25:51 AEDT 2024
;; MSG SIZE  rcvd: 125

Wintermute:~ furry$
```

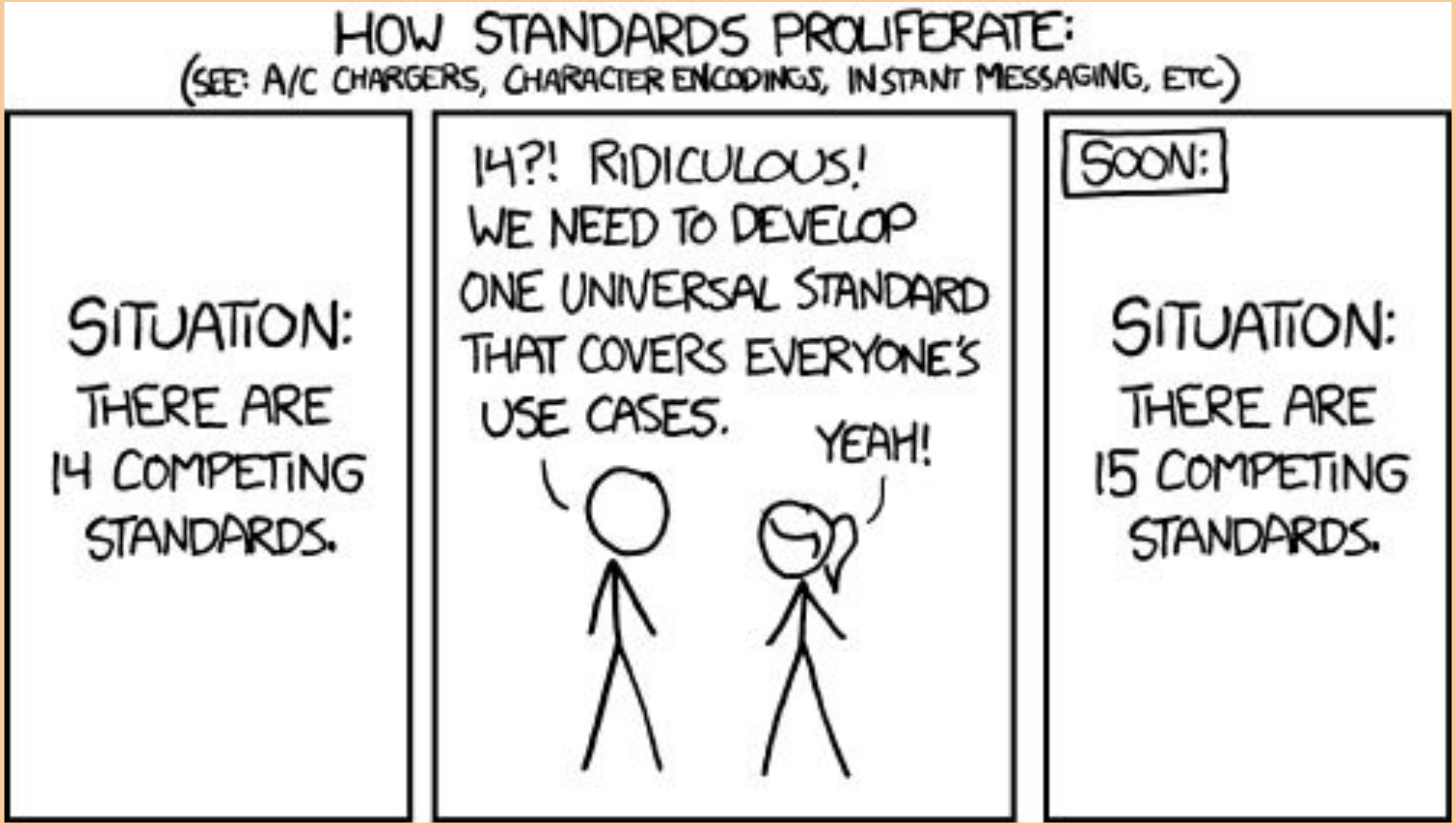
Local resolver

Another way to discover the NAT64 prefix



```
Wintermute:~ furry$ ipconfig getra en0
RA Received 11/01/2024 03:59:33 from fe80::42:1, length 96, hop limit 0, lifetime 3600s, reachable 0ms,
 retransmit 0ms, flags 0x40=[ other ], pref=medium
        prefix info option (3), length 32 (4):  2001:67c:64:42::/64, Flags [ auto ], valid time 86400s,
 pref. time 3600s
        pref64 option (38), length 16 (2): 64:ff9b::/96 lifetime 3600s
        rdnss option (25), length 24 (3):  lifetime 86400s, addr: 2001:67c:64:53::53:1
        source link-address option (1), length 8 (1): 00:50:56:bb:b5:0b
```

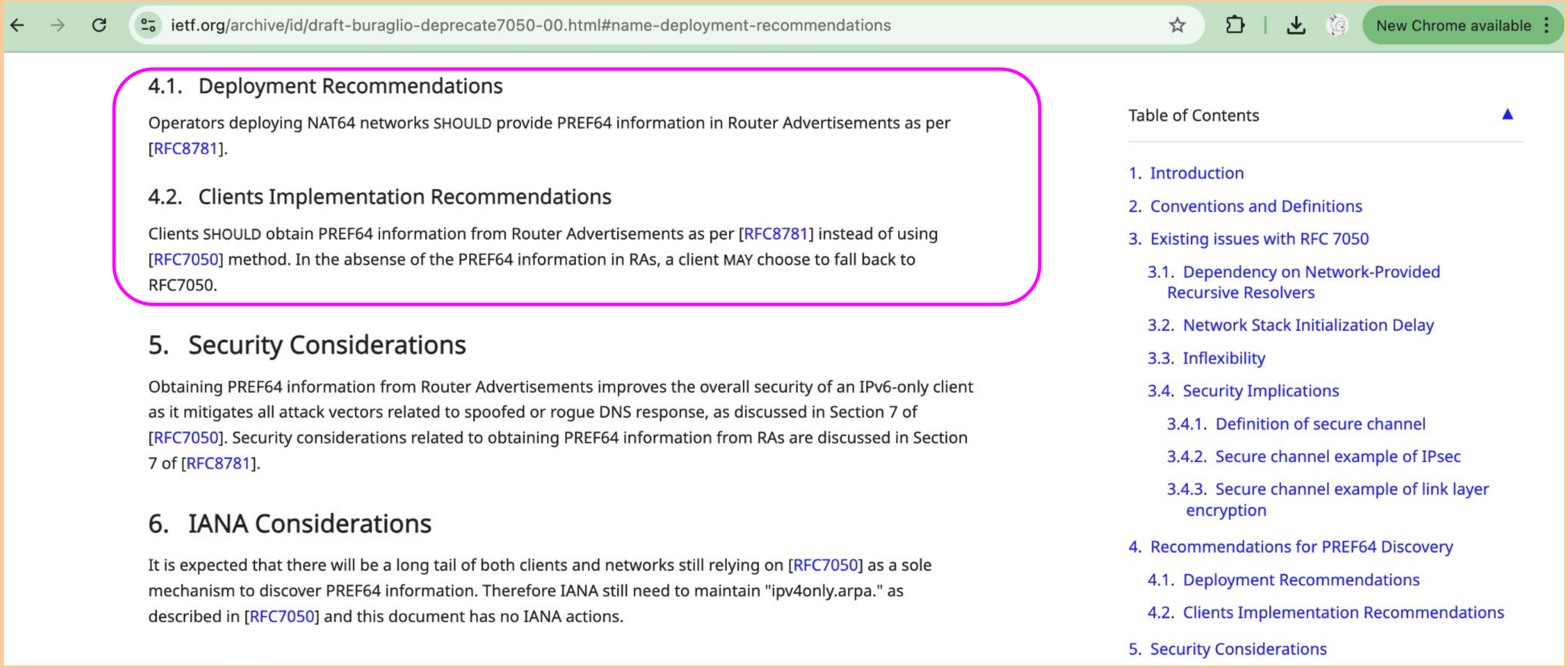
Include PREF64 into Router Advertisements, RFC8781 (April 2020)


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

HTTPS://XKCD.COM/927/

Deprecation of DNS64 for Discovery of NAT64 Prefix

draft-buraglio-deprecate7050



ietf.org/archive/id/draft-buraglio-deprecate7050-00.html#name-deployment-recommendations

New Chrome available

4.1. Deployment Recommendations

Operators deploying NAT64 networks SHOULD provide PREF64 information in Router Advertisements as per [RFC8781].

4.2. Clients Implementation Recommendations

Clients SHOULD obtain PREF64 information from Router Advertisements as per [RFC8781] instead of using [RFC7050] method. In the absense of the PREF64 information in RAs, a client MAY choose to fall back to RFC7050.

5. Security Considerations

Obtaining PREF64 information from Router Advertisements improves the overall security of an IPv6-only client as it mitigates all attack vectors related to spoofed or rogue DNS response, as discussed in Section 7 of [RFC7050]. Security considerations related to obtaining PREF64 information from RAs are discussed in Section 7 of [RFC8781].

6. IANA Considerations

It is expected that there will be a long tail of both clients and networks still relying on [RFC7050] as a sole mechanism to discover PREF64 information. Therefore IANA still need to maintain "ipv4only.arpa." as described in [RFC7050] and this document has no IANA actions.

Table of Contents

https://datatracker.ietf.org/doc/draft-buraglio-deprecate7050/

QUESTIONS?
COMMENTS?