IPv6 Business Conference

Organized by SWISS IPv6 COUNCIL

2016 June, 16

ERNW providing security.

IPv6 from a Developers' Perspective

Some Notes

Enno Rey
erey@ernw.de / @Enno_Insinuator

ERNW providing security.

Who Am I

- Old-school network security guy with background in provider operations.
- Involved with LIR administration in some enterprise LIRs
  - Including the one with probably the coolest org handle: ORG-HACK1-RIPE.
- IPv6 since 1999 and regularly blogging about it at `www.insinuator.net/tag/ipv6`.

ERNW providing security.

Agenda

- IPv6 Fundamentals & Basic Properties
- Implications of a dual-stack world
- Various bits from a security point of view

Preliminary Notes

- This talk assembles a loose collection of points which can be relevant for developers.
  - Some might be helpful when doing troubleshooting, too.
  - I'm not a developer myself. So my assumptions may be plain wrong at times.
- The talk assumes
  - that you're a developer (hence the title ...)
  - that you don't know much about IPv6.
  - Both may be dubious assumptions for the audience at this event ;-)
- I won't cover any coding relating aspects.
  - Sofia in the next slot (other room) can do this much better.

IPv6 Addresses

Format / Text Representation

- IPv6 addresses look very different from IPv4 ones:
  - Different length (128 bit vs. 32 bit)
    → different number of “blocks” (eight “quartets” vs. four “octets” in v4)
  - Different delimiter (“:” instead of “.”).
  - Different notation (hex vs. decimal).
  - All types of “shortened representations” are permitted (see RFC 4291 sect. 2).
    - And there's even a “recommended representation” (RFC 5952). We'll get back to this.
- Whenever you do any parsing of IP(v6) addresses, you may keep the above in mind.

ERNW providing security.

Some Notes on the ":" Delimiter

- Config files
- URLs
- Do you accept ":" in a form/field where an IP address is entered?
  - Do you accept it as a delimiter?
  - Same question for square brackets.
- Interesting read:
  - The IPv6 Numeric IP Format is a Serious Usability Problem https://www.zerotier.com/blog/?p=724

More on the Delimiter & Address Shortening

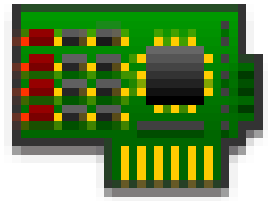
- Do not use “text boxes“ for individual quartets of address
  - Inhibits entering shortened addresses
  - Might inhibit copy+paste, which in turn is much more important now (IPv6).

ERNW providing security.

Parsing & Validating Addresses

- Input validation approaches/ routines for IP addresses entered by user must allow additional characters
  - Letters a-f in lower/upper case
  - ":"
  - "[" and "]" in some cases.

Number of IP Addresses on an Interface



- Pretty much always an interface has several IP addresses:
  - The so-called “link local” one (fe80:: sth).
    - This one can not be used for any “remote communication”…
  - Usually at least one so-called “global” one, with very high probability starting with a “2” (as of 2016).
    - On “client” systems this one is often accompanied by another one from the same prefix (“network”).
    - Once the latter one exists, it is used by default for any outbound connections from this system / interface.

ERNW providing security.

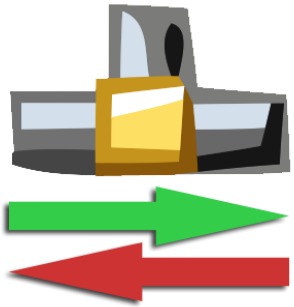
Multiple IP Addresses on an Interface

Implications

- Whenever you perform a call to determine “the IP address of the local endpoint”, be very careful
  - You might not expect multiple addresses as a response and hence might not be prepared to parse response (“array”) properly.
  - You might not get the info you're interested in when (only) looking at the first address (fair chance this is the so-called link local one).
  - You might not be able to determine the one that is actually used in a connection your app initiates/performs.

ERNW providing security.

A Note on Link-Local Addresses

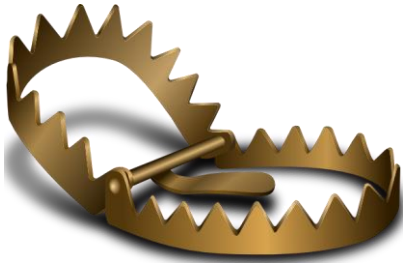


- They can only be used in the local network.
- → Good, from a security perspective, for everything happening only there
  - Local synchronization traffic, e.g. cluster sync
- → Bad if there might be a chance that communication with "outside" network might be needed at some point.

More of this Network Stuff

- There is no concept of “broadcasting” (talk/yell to everybody) any longer.
  - Ask yourself: Does your application rely on something like that?
- There is special multicast group that resembles broadcast very much: all-nodes (ff02::1).

This MTU Thing



You may read also:
https://www.ietf.org/mail-archive/web/v6ops/current/msg22311.html

- You might have never heard of this.
- It's a complicated matter ;-)
- The main difference to [IP]v4 is:
  - In case there's a problem in this space, the network devices called routers can't help you anymore.
- Again, do not assume anything.

ERNW providing security.

Living (and Developing) in a Multi-Protocol World

Dual-Stack

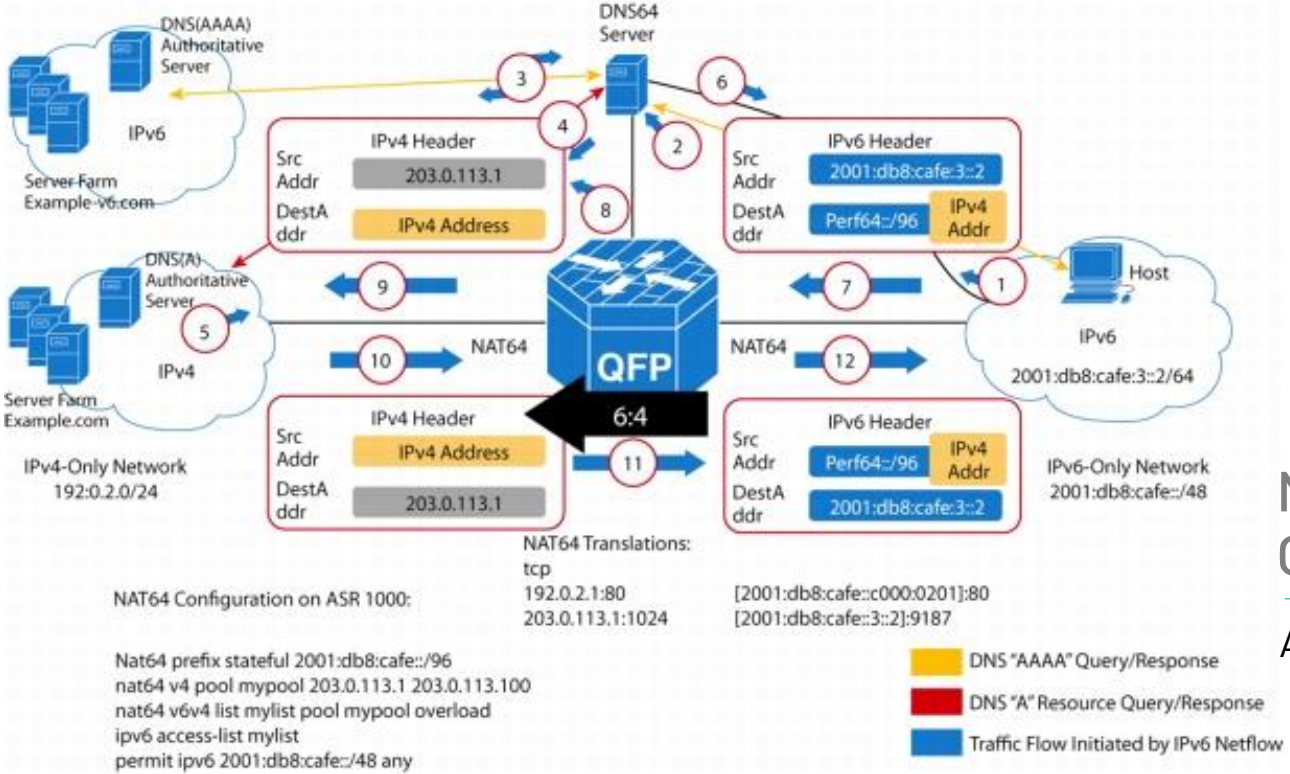
- Be aware that there's a fair chance that two “IP related” protocol stacks exist in parallel on a given system.
  - Depending on your age this might be unfamiliar for you ;-)
- How do you know which one is used for
  - anything your application does.
  - Anything your application relies on (e.g. DNS).
  - The way your server-side application keeps track/state of users?
- Never rely on “a helper protocol from $STACK working” means “$STACK works for everything”.
- When storing IP addresses (e.g. in a database), can you store (at least) two of them?
  - In a different format?

A Word on DNS

- Just because the lookup of an IPv6 hostname worked, doesn‘t mean that IPv6 (communication to a remote endpoint) works as a whole, or the resolved address is indeed reachable over IPv6.
  - In DNS the IP transport of a query and the information queried are “de-coupled“.

NAT64

- There‘s a mechanism that translates IPv6 into IPv4 (or vice versa) at network boundaries.
- This changes the properties of a network packet.
  - Does your application‘s behavior rely on any of the affected ones?



NAT64 Is a Complicated Thing

As so many in the IPv6 world ;-(

Happy Eyeballs

That's what you want, right? ;-)

- From RFC 6555:

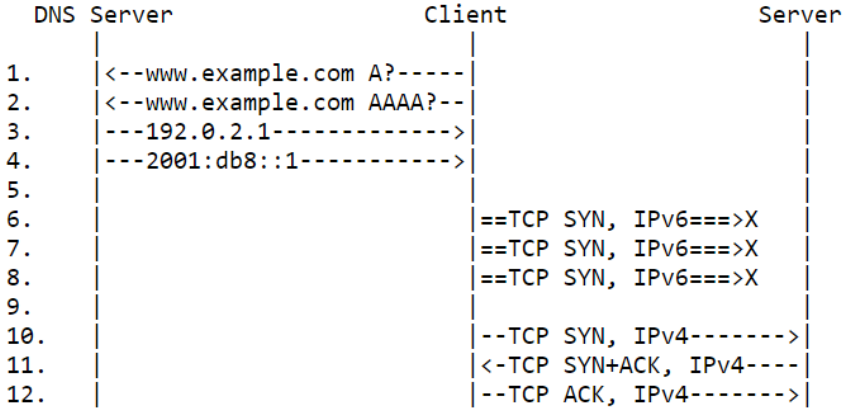


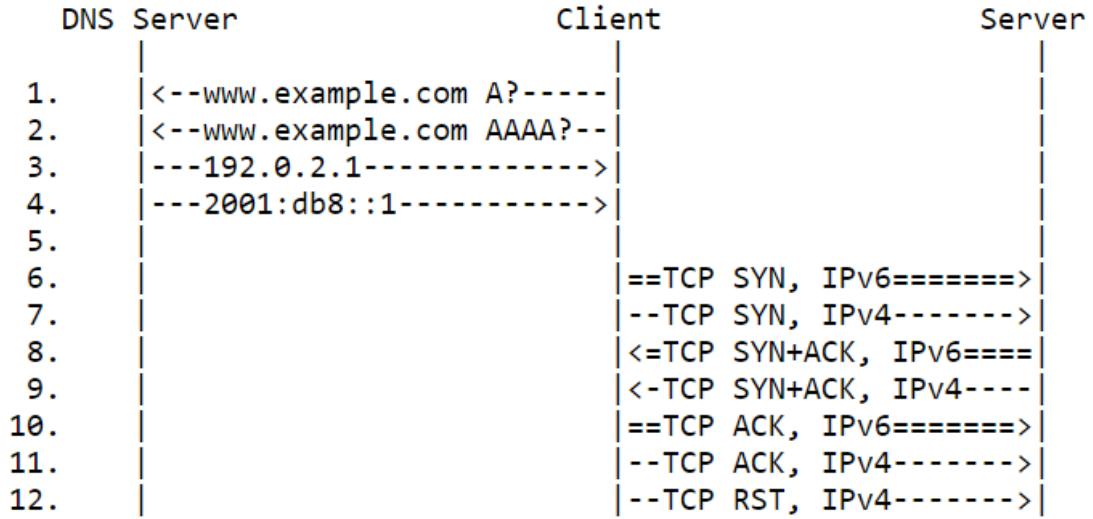
Figure 1: Existing Behavior Message Flow

Mission / Solution

- Happy Eyeballs algorithm has two main goals.
- Fast connectivity for users by connecting to a given destination using IPv6 and IPv4 in parallel.
- While still avoiding trashing the network.

Connection Setup with HE

Again from RFC 6555



Things to Consider

- How do you know
  - If HE comes into play.
  - If so, with which exact properties/ behavior.
  - How to control this on $PLATFORM.
- HE might be the source of interesting problems itself.

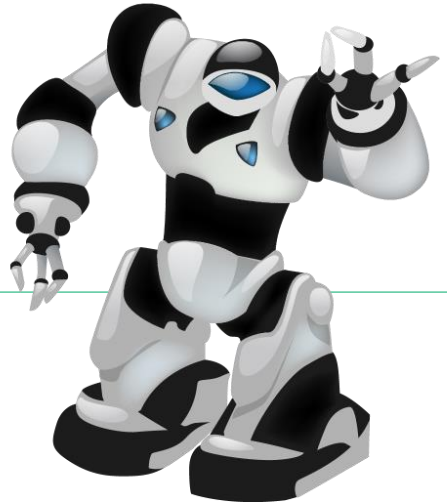
Client of $YOUR_APP Might Use HE, Too.

Source:
http://lists.cluenet.de/pipermail/ipv6-ops/2016-April/010851.html

```
dear ipv6-ops list members,

one of our users is unable to login to webmail, because the ip address is
changing during session. this problem isnt that unusual, but after a check
in the logfiles i realized its switching from ipv4 to ipv6 and so on, (see below).

is this phenomenon known?
is it us or the deutsche telekom who is causing the problem?

thanks in advance,
re - noc.mur.at

#####

Apr 29 09:54:34  dovecot: imap-login: Login: user=<>, method=PLAIN,
rip=217.233.160.66

Apr 29 09:57:54  dovecot: imap-login: Login: user=<>, method=PLAIN,
rip=2003:88:6c55:4707:b538:efe9:d4fb:bdf7

Apr 29 10:05:17  dovecot: imap-login: Login: user=<>, method=PLAIN,
rip=217.233.160.66

Apr 29 10:05:19  dovecot: imap-login: Login: user=<>, method=PLAIN,
rip=2003:88:6c55:4707:b538:efe9:d4fb:bdf7

Apr 29 11:29:03  dovecot: imap-login: Login: user=<>, method=PLAIN,
rip=217.233.160.66

Apr 29 11:45:09  dovecot: imap-login: Login: user=<>, method=PLAIN,
rip=2003:88:6c55:4707:b538:efe9:d4fb:bdf7
```

Miscellaneous / Backup Slides

with a Particular Focus on Security



ERNW providing security.

Let‘s Go Back to IPv6 Network Stuff for a Second

- Don‘t assume that binding a service to “::1“ means that it‘s only reachable from the local system.

- See also:
  - https://www.insinuator.net/2015/01/should-ipv6-packets-with-source-address-1-be-processed-when-received-on-an-external-interface/

Conclusions

- A lot of things have changed between IPv4 and IPv6.
- Those, and the multiprotocol world that we'll see for a long (?) time, can have a heavy impact on the actual behavior of applications.
- It might not hurt to expose developers in your organization to this stuff at some point.

ERNW providing security.

There's never enough time...

THANK YOU...

...for yours!

@Enno_Insinuator

erey@ernw.de

Slides & further information:
https://www.troopers.de
https://www.insinuator.net
(..soon)

Questions?

References

- Apple on “Avoiding Common Networking Mistakes“
  - https://developer.apple.com/library/mac/documentation/NetworkingInternetWeb/Conceptual/NetworkingOverview/CommonPitfalls/CommonPitfalls.html
- Apple on transition:
  - https://developer.apple.com/library/ios/documentation/NetworkingInternetWeb/Conceptual/NetworkingOverview/UnderstandingandPreparingfortheIPv6Transition/UnderstandingandPreparingfortheIPv6Transition.html

More References

- RFC 4038 Application Aspects of IPv6 Transition
  - https://tools.ietf.org/rfc/rfc4038.txt
- ARIN Guide "Preparing Applications for IPv6“
  - https://www.arin.net/knowledge/preparing_apps_for_v6.pdf

ERNW providing security.

Thanks to All Sponsors of the Event

Infoblox CONTROL YOUR NETWORK

f5

SWITCH

DIGICOMP

eb-Qual

itrain THE ESSENCE OF IT

Sunny Connection

BLUECAT

asecus securing your business

flowdays achieving more together

ERNW providing security.

Image Credits

- Icons made by Freepik from www.flaticon.com are licensed by CC 3.0 BY

<sergej.peters@everyware.ch

- Icons made by Nas Ztudio from www.flaticon.com are licensed by CC 3.0 BY.