Is 2019 finally the Year for Linux on the Desktop? Or for v6-only Networks?

Enno Rey
erey@ernw.de | @enno_insinuator

Christopher Werny
cwerny@ernw.de | @bcp38_

ERNW
providing security.

#whoarewe

- Old-school networking guys, with a special focus on security (www.ernw.de)
- Doing quite some stuff in the IPv6 space
  - https://insinuator.net/2019/01/ipv6-talks-publications
- Operating a (medium-size) conference network with v6-only+NAT64 in the default SSID since 2016

ERNW
providing security.

Background of This Talk

- An increasing number of organizations currently consider implementing IPv6 in a specific mode often called “v6-only + NAT64”.
- Some conferences already implement this in their WiFi networks:
  - Troopers ;-)
  - FOSDEM
  - Cisco Live (but somewhat “experimental”)

https://insinuator.net/2019/02/some-notes-on-the-ipv6-properties-of-the-wireless-network-cisco-live-europe/

ERNW
providing security.

This Raises a Crucial Question

- What breaks? ;-)
- Let's be more precise
  - Which stuff that we (or they = customers) actually need breaks?
  - Do (should) we care?
  - Technical alternatives / solutions?

Faust and Gretchen in the garden
(painting by James Tissot, 1861)

ERNW
providing security.

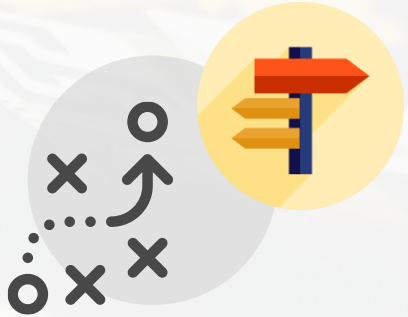
Case Study

- $COMPANY plans to enable IPv6 in up to 3K Wi-Fi hotspots in supermarkets in Western Europe
  - Dual-stack or v6-only?
- Free offering → no SLAs
- But still they'd like to avoid "discussions which could affect their brand".

ERNW
providing security.

Strategy / Decisions

- Dual-Stack vs. v6-only (+NAT64)
  - From “IPv6 perspective” the most important one
- Lots of misinformation floating, in different circles
- Thoroughly consider users, platforms, applications and expectations.
- Timeline might play a role, too.



ERNW
providing security.

The Lab Infrastructure – Overview

- Pretty small and basic setup:
  - Cisco ISR 4321 as NAT64 GW
  - Unbound as DNS64
  - WLC + AP for Wifi Connectivity

ERNW
providing security.

Testbed

- Windows 10 – Build 1809 / Windows 7
- macOS 10.14 – Mojave
- Apple iOS – 12.1.4
- Arch Linux – Kernel 4.19
- Android 9 Pie (API 28)

ERNW
providing security.

The Lab – Methodology

- Group applications in categories.
  - e.g. Social Media, Communication etc.
- Define first set of (potential) relevant applications to be tested.
- Define test cases for each app
- Perform the tests
- (Try) to evaluate root cause for failed test cases

Stuff Tested (I)

- Social Media
  - Signal
  - Instagram
  - Snapchat
  - Tik Tok
  - Twitter
  - WhatsApp
  - Tinder
  - Threema

- Streaming
  - Spotify
  - Twitch
  - Amazon Music
  - Amazon Prime Video
  - Netflix
  - Apple Music

ERNW
providing security.

Stuff Tested (II)

- Communication
  - Microsoft Teams
  - Discord
  - Skype
  - Slack
  - Facetime
  - Skype for Business
  - Cisco WebEx

- Games
  - Fortnite
  - PUBG
  - Pokemon Go
  - Steam

ERNW
providing security.

Display of Sample Categories / Test cases

Social	*Test*	Windows 10	Windows 7 or lower	Linux	MacOS	Android	iOS
Signal							
	Send a message						
	Receive a message						
Instagram							
	Test if login works						
	Follow someone						
	Comment a picture						
	Watch a story						
	Receive a private message						
	Send a private message						
Snapchat							
	Send a message						
	Send a picture						
	Test if Login works						
	Receive a picture						
	Create a story						
	Receive a message						

ERNW
providing security.

Results / Overview

- OS-wise iOS apps successfully completed all test cases
  - Maybe not a surprise given Apple's strategy
- Most categories worked quite nicely, e.g.
  - Social Media
  - Communication
- Issues were mostly identified in two areas
  - Games
  - Streaming

ERNW
providing security.

Applications with Issues / Overview

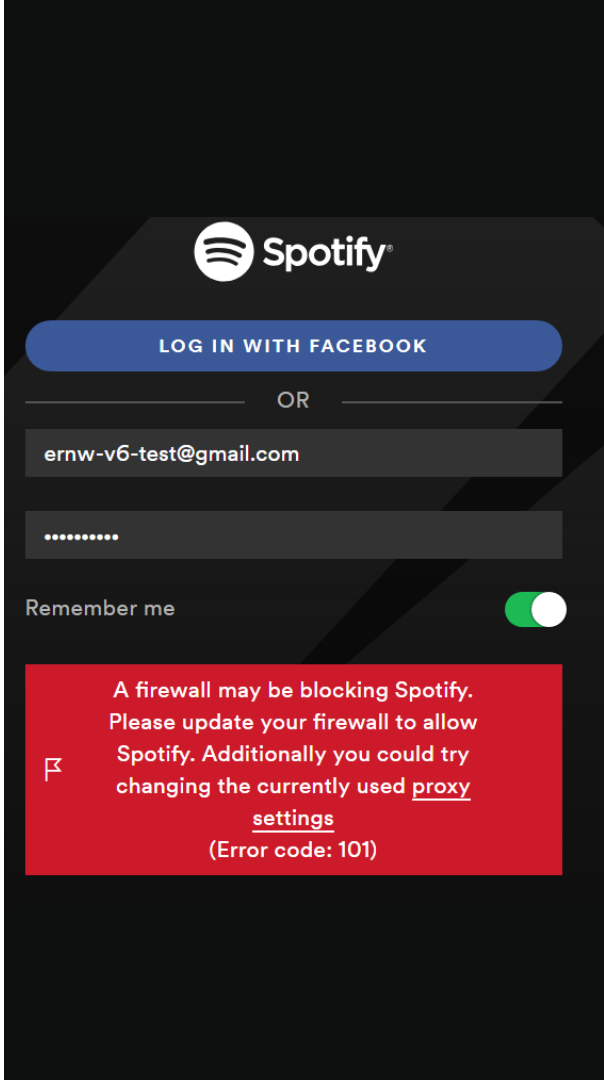
- In general, we could observe two failure scenarios:
  - Either the app just doesn't work at all without IPv4
  - In general the app works but some functionality is limited.

ERNW
providing security.

Streaming - Spotify

- Unfortunately, the Spotify app on Windows 10/7/macOS does not work.
  - The web client works as intended

- No network activity could be observed. We assume the client tries to open a IPv4 socket, which of course fails.



ERNW
providing security.

Games – Fortnite

- “Hottest“ Battle Royal game for a year or two.
- Based on the Unreal engine developed by Epic.
- To play Fortnite, one has to install the Epic Games Launcher.

ERNW
providing security.

Turns out...XMPP client only asks for an A record ☹

```
Queries
  xmpp-service-prod.ol.epicgames.com: type A, class IN
Answers
  xmpp-service-prod.ol.epicgames.com: type CNAME, class IN, cname xmpp-service-prod-weighted.ol.epicgames.com
  xmpp-service-prod-weighted.ol.epicgames.com: type A, class IN, addr 34.195.135.176
  xmpp-service-prod-weighted.ol.epicgames.com: type A, class IN, addr 34.202.107.122
  xmpp-service-prod-weighted.ol.epicgames.com: type A, class IN, addr 34.199.177.138
  xmpp-service-prod-weighted.ol.epicgames.com: type A, class IN, addr 34.200.66.169
  xmpp-service-prod-weighted.ol.epicgames.com: type A, class IN, addr 34.197.247.209
  xmpp-service-prod-weighted.ol.epicgames.com: type A, class IN, addr 34.196.225.72
  xmpp-service-prod-weighted.ol.epicgames.com: type A, class IN, addr 34.202.23.197
  xmpp-service-prod-weighted.ol.epicgames.com: type A, class IN, addr 34.192.117.58
```

ERNW
providing security.

For future reference

New: Improved IPv6 Support

Support for IPv4 and IPv6 has been merged into a single socket subsystem, where previously support for each protocol was isolated to a specific subsystem. This allows platforms that used one of the BSD subsystems to support both IPv4 and IPv6 at the same time, and do it transparently to the calling code.

https://www.unrealengine.com/en-US/blog/unreal-engine-4-21-released Nov 2018

ERNW
providing security.

Interim Conclusion (i)

- We tested around 35 different applications with a total of 120 test cases
  - On (if available) six different operating systems.
- Only three applications didn't work at all on non-mobile operating systems.
- Two applications had some feature limitations
  - E.g. not able to join a voice channel @Discord

Conclusions

- We see an increasing interest in deploying v6-only + NAT64 networks.
  - For reasons…
- Testing creates #transparency ;-) & hence well-informed decision making…
- Overall less issues than expected
  - Apple's strategy seems to work.
  - Communication strategy will be crucial, with management, users & vendors.

Just to Make this Clear

- Based on our testing we think that going with v6-only (+ NAT64) is a reasonable approach now
  - Only very few issues (stuff not working) to expect
  - Namely on platforms or types of app which might not even be relevant for your deployment scenario
  - At the same time this can save a lot of operational effort.
  - Telemetry data & lab results are always a good idea ;-)
  - Proper supporting communication can be helpful.

- Note: for most scenarios distributing DNS resolvers via RAs/RDNNS **and** stateless DHCPv6 to be strongly considered.

ERNW
providing security.

Lab / Next Steps

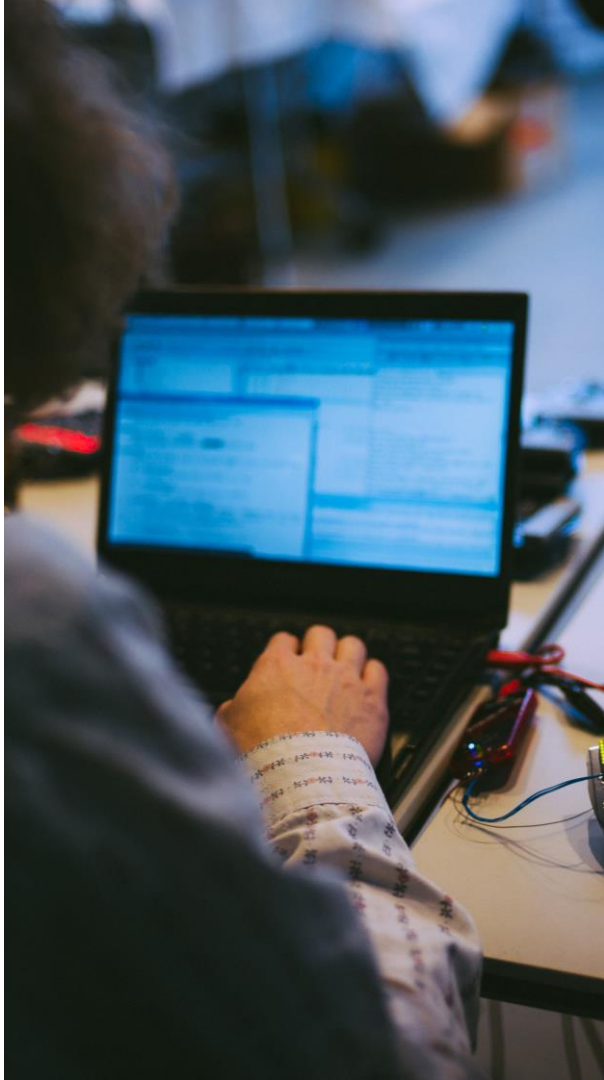
- Validate / further investigate failure cases
- Vendor communication!
- Probably even easier when the vendor is the only failing one in a group of similar apps ;-)
- In parallel / very soon we will release the full results (incl. sanitized pcaps)

ERNW
providing security.

Next Steps (II)

- Test more/other categories
  - Corporate applications besides HTTP[S]-based north-south traffic
  - VPN clients

- We see this evaluation as a permanent ongoing activity and are happy about suggestions.



ERNW
providing security.

Thank you for your Attention!


erey@ernw.de


cwerny@ernw.de


www.ernw.de


www.insinuator.net

ERNW
providing security.

Sources

As indicated on slides.

Image Sources

Icons made by Freepik
from www.flaticon.com
https://unsplash.com
https://www.pexels.com/