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.

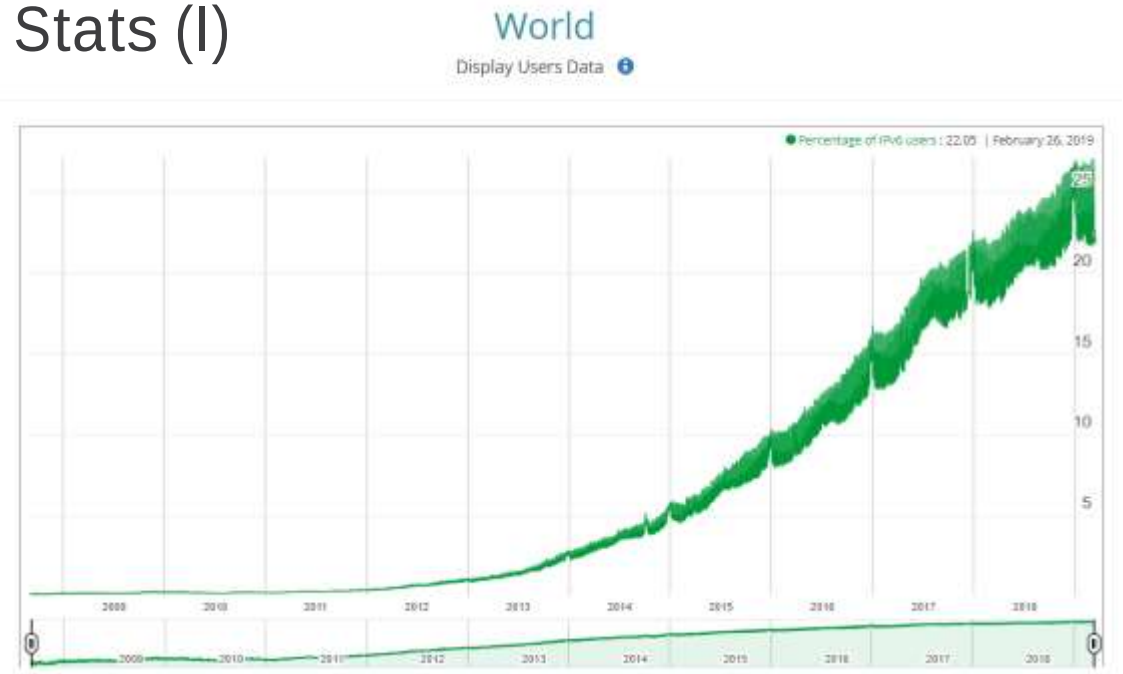
Agenda

- Technologies & Approaches
- Case Study & Initial Thoughts
- Results from the Lab

Current Stats

- Germany
- World
- Websites

Stats (I)

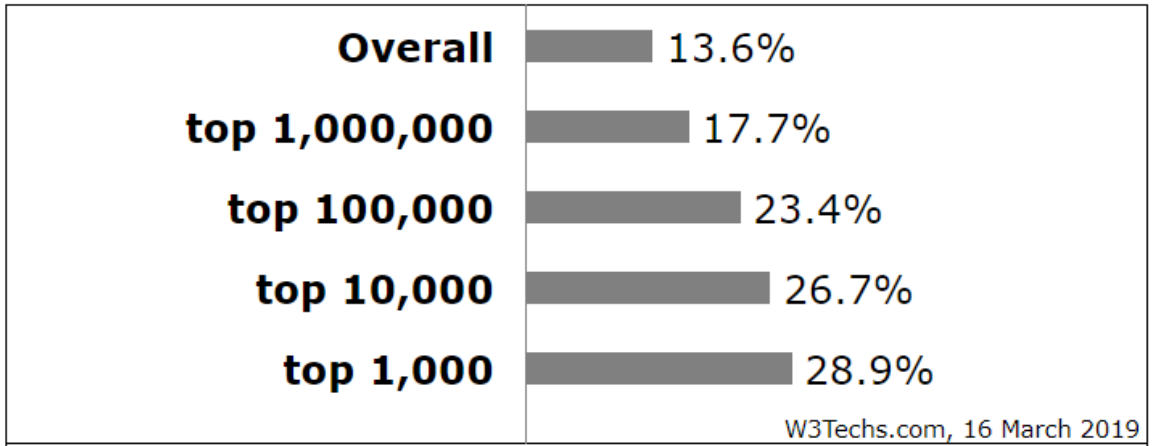

World
Display Users Data
Percentage of IPv6 users : 22.05 | February 26, 2019
20
15
10
5
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018

Stats (II)

Src: http://6lab.cisco.com/stats/cible.php?country=DE&option=users

ERNW
providing security.

Stats (III)



Percentages of websites using IPv6 broken down by ranking

Src: https://w3techs.com/technologies/breakdown/ce-ipv6/ranking

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.

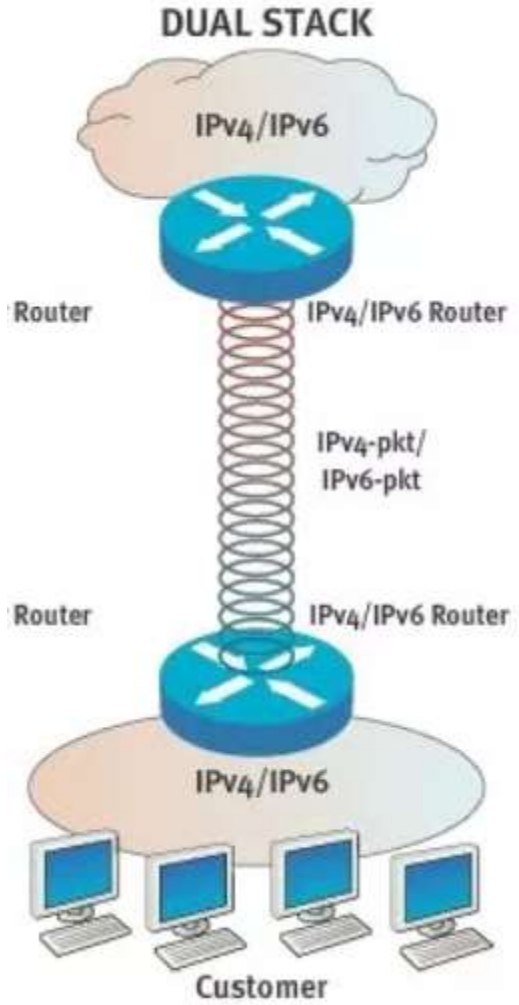
Potential Reasons for such an Approach

- Avoid disadvantages of “dual-stack” approach (see below)
- Keep it simple (?)
- Organizations running out of IP(v4) address space incl. RFC 1918 space and/or their own public/12s

ERNW
providing security.

Dual-Stack

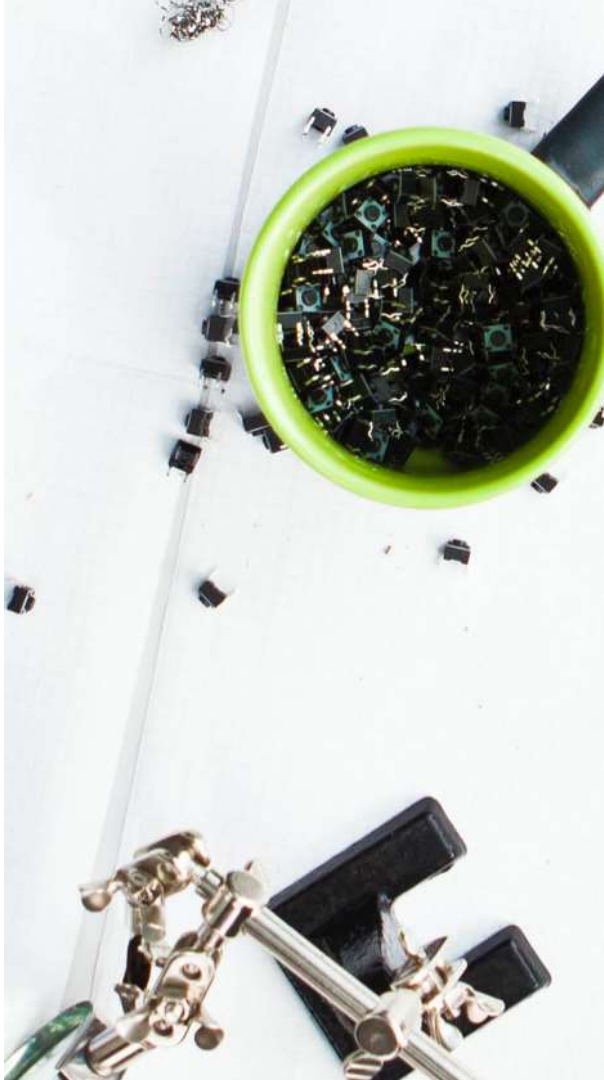
- Every/most node(s) on the network will be configured with IPv6 and IPv4 addresses.
- Each address family needs dedicated routing protocols (e.g. OSPFv2 and OSPFv3).
- Clients receive full IPv4 and IPv6 interface configuration and choose the preferred protocol based on the service and/or some local (OS-specific) selection mechanism.



ERNW
providing security.

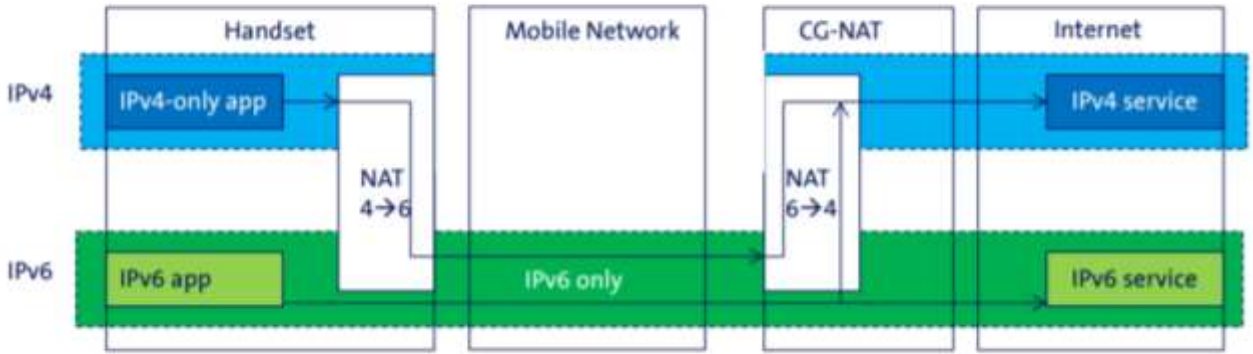
IPv6-only with NAT64/DNS64

- Control- & data plane will be deployed in an IPv6-only fashion.
- NAT64 deployed on e.g. ASR 1k performs (stateful) protocol translation IPv6 → IPv4.
- DNS64 synthesis AAAA Records for IPv4-only clients.
- See also
  - https://www.troopers.de/media/filer_public/5b/34/5b340a58-2c8e-46a0-9d96-834e5edd9154/tr16_ipv6_sec_summit_secure_reliable_guest_wlan_v15.pdf



ERNW
providing security.

464XLAT Might Come into Play



Src: http://www.ipv6conference.ch/wp-content/uploads/2015/06/B10-Swisscom-Status_Roadmap_and_Outlook_IPv6.pdf

ERNW
providing security.

What Apple Does

Supporting IPv6-only Networks

Starting June 1, 2016, all apps submitted to the App Store must support IPv6-only networking. A majority of apps will not require any changes as IPv6 is already supported by NSURLSession and CFNetwork APIs. However, if your app utilizes IPv4-specific APIs or hard-coded IP addresses, you will need to make changes. Be sure to test for IPv6 compatibility before submitting your app to the App Store for review.

For more information on supporting IPv6 networks, review Supporting IPv6 DNS64/NAT64 Networks.

Testing your app in an IPv6-only environment

You should test your app on an IPv6-only network. If you don't have one, you can set up a test network by following the instructions in Test for IPv6 DNS64/NAT64 Compatibility Regularly.

IMPORTANT: If you're testing with a WWAN-capable device, make sure to turn off WWAN before running your test. This will ensure your device is using the IPv6-only Wi-Fi.

Note: You can turn off WWAN using Settings > Cellular > Cellular Data (for English localizations outside of North America use Settings > Mobile > Mobile Data).

ERNW
providing security.

Case Study

- $COMPANY plans to enable IPv6 in up to 3K WiFi 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".

Types of Connections / Initial Assumptions

Will most certainly work.	+
Very likely to work, but individual apps might expose problems.	++
Unclear. Will heavily depend on specific circumstances.	?
Problems to be expected.	–

		Connection Endpoint					
		IPv6	IPv4				
Type of Client Device		All	Web	Fat Client/ App	VPN Client (SSL)	VPN Client (IPsec)	Other
Smartphones	iOS	++	++	+	++	–	+
	Android	++	++	++	++	–	+
	Other	++	++	+	++	–	+
Laptops	Windows, Pre–10	++	++	+	++	–	+
	Windows 10	++	++	++	++	–	+
	Other	++	++	?	++	–	+
Other	IoT Devices	++	++	?	++	–	+

ERNW
providing security.

From FOSDEM: IPsec VPN Clients & v6-only

- When we look into the legacy dual stack network, we notice that for the IPv4 traffic distribution we see outgoing
  - ~214M TCP packets and
  - ~6M ESP (VPN) packets while incoming was
  - ~394M TCP packets with
  - ~8M ESP packets

Src: https://blogs.cisco.com/getyourbuildon/fosdem-2019-a-new-view-from-the-noc

ERNW
providing security.

From FOSDEM: IPsec VPN Clients & v6-only

- This means that at least about 2-3% of all traffic was on an IPSEC VPN. And this excludes the TCP VPN traffic on ports 443/TCP and 22/TCP. On the IPv6 network we do not see a similar amount of ESP traffic.

- This strongly suggests that the people remaining on the dual stack network do so because their VPN solution does not work with an IPv6 only network.

Src: https://blogs.cisco.com/getyourbuildon/fosdem-2019-a-new-view-from-the-noc

Connections / Expected Trends

ERNW
providing security.

Situation/numbers will get better/increase over time

Numbers/problems will get less/decrease over time

		Connection Endpoint					
		IPv6	IPv4				
Type of Client Device		All	Web	Fat Client/ App	VPN Client (SSL)	VPN Client (IPsec)	Other
Smartphones	iOS	++	++	+	++	–	+
	Android	++	++	++	++	–	+
	Other	++	++	+	++	–	+
Laptops	Windows, Pre-10	++	++	+	++	–	+
	Windows 10	++	++	++	++	–	+
	Other	++	++	?	++	–	+
Other	IoT Devices	++	++	?	++	–	+

ERNW
providing security.

Rationale re: Trends

- IPv6-enabled connection endpoints (e.g. websites/servers) increase over time.
- Client-side apps increasingly support IPv6, not least due to Apple's respective requirements (2016).
- Overall IPv6 support of client OSs and "exotic applications" continuously gets better.

ERNW
providing security.

Initial Proposal

- Due to the operational overhead induced by Dual Stack, we recommend to go with a IPv6-only approach with NAT64/DNS64.

- While some things (in the lower one digit %) might not fully work currently, it is expected (as can be seen on the tables before) that this number will decrease over time.

ERNW
providing security.

The Lab

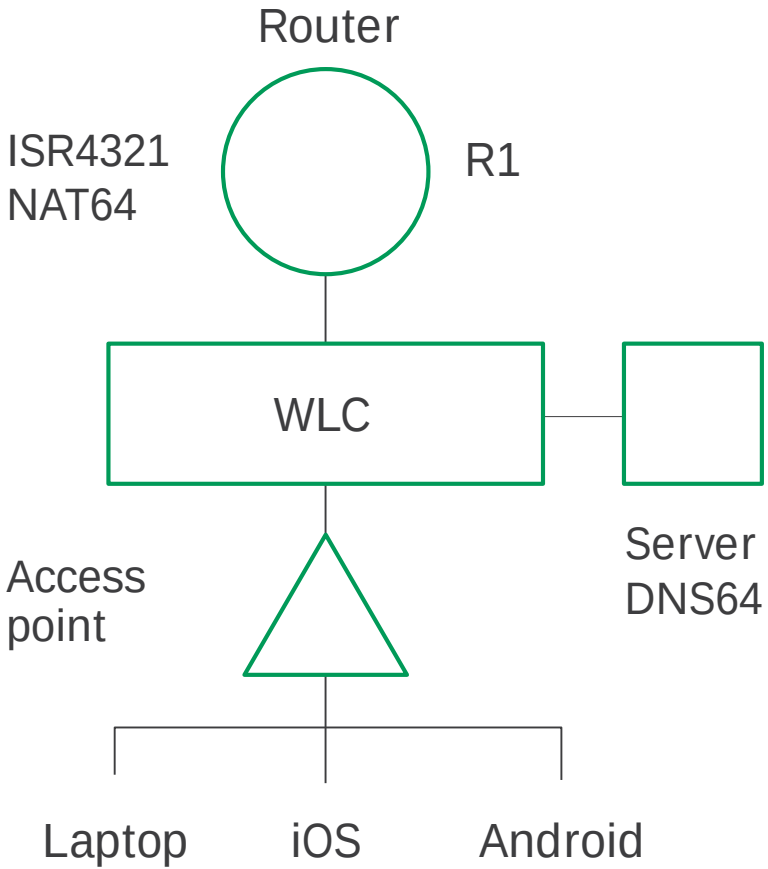
Flickr: shando.

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.

The Lab – Overview



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

ERNW
providing security.

Categories

- Social Media
- Streaming
- Communication
- Games
- Informational
- Other

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						

Results

- Kudos to Marius for performing the majority of test cases!

ERNW
providing security.

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.

Spotify – in 2015

"Enabling IPv6 for a client application is not technically a big deal.....

....Unfortunately our client code had its own IP-address type which didn't support IPv6, and it also assumed that an IP-address would fit in 4 bytes in numerous places...."

Src: https://labs.spotify.com/2015/11/05/oh-ipv6-where-art-thou/

Spotify Labs

Oh IPv6, Where Art Thou

Posted on November 5, 2015 by Per Knytt

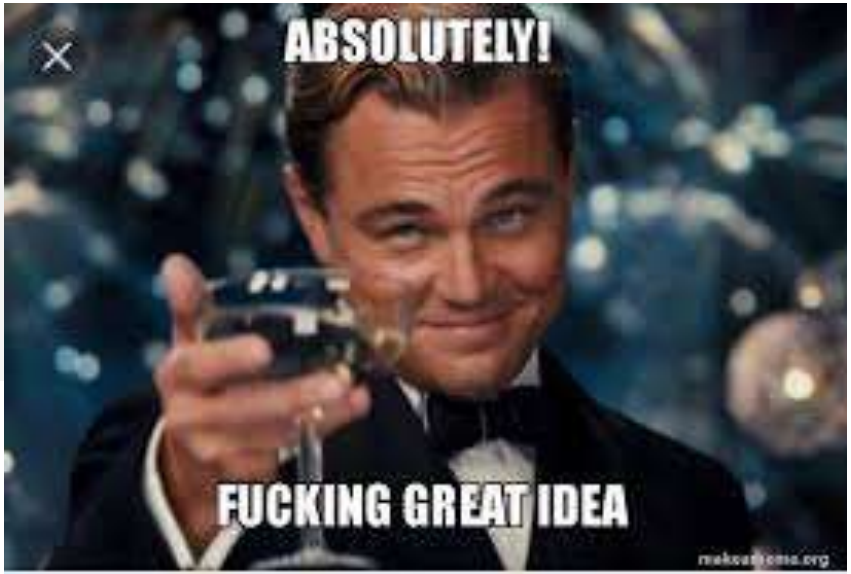
Spotify – in 2019

https://community.spotify.com/t5/Live-Ideas/Other-IPv6-Support/idi-p/4469460

[Other] IPv6 Support

Submitted by sdstrowes on 2018-04-30 08:16 PM

When we will be able to use Spotify without IPv4?

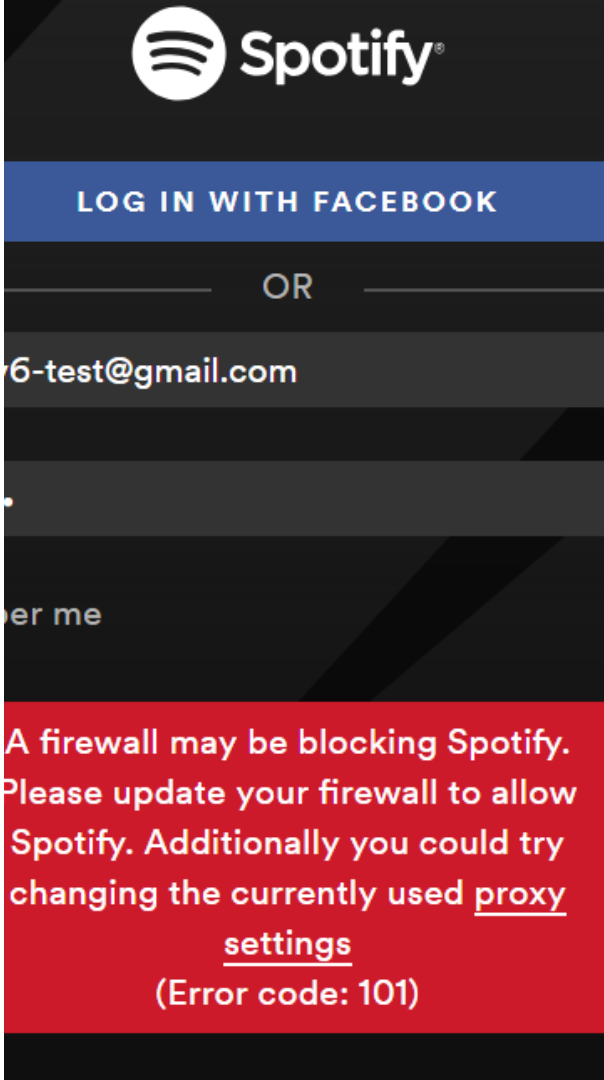


ERNW
providing security.

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.

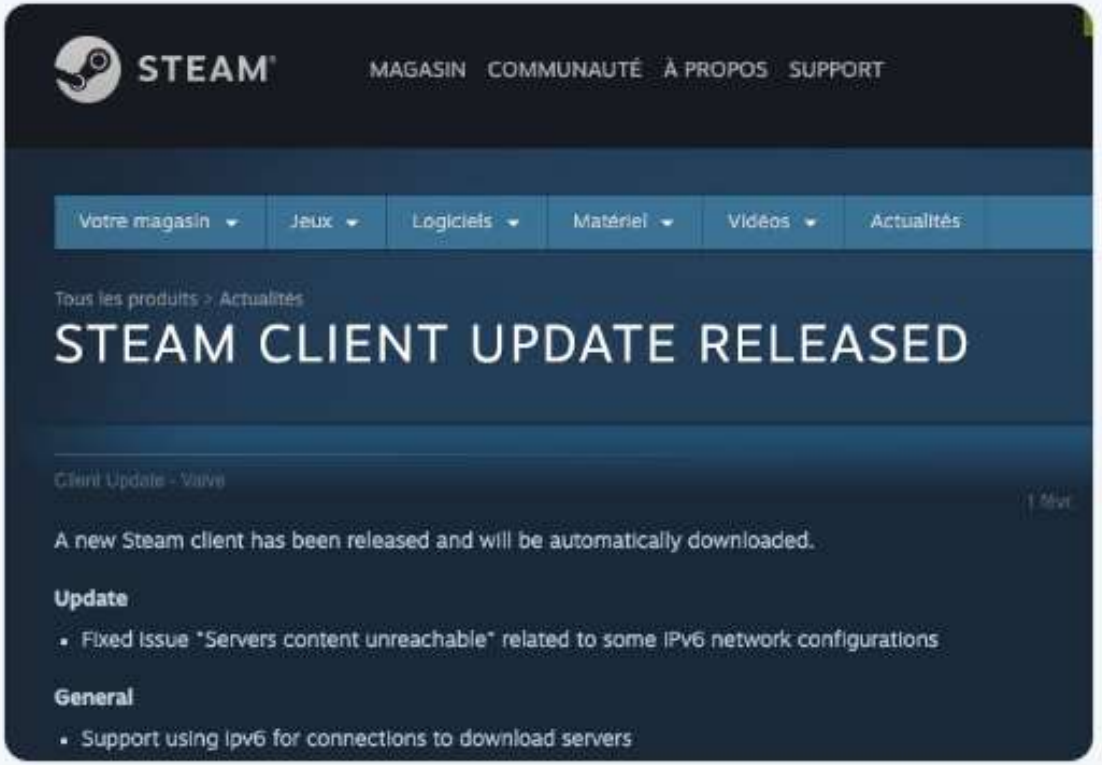


ERNW
providing security.

Game(s) Client

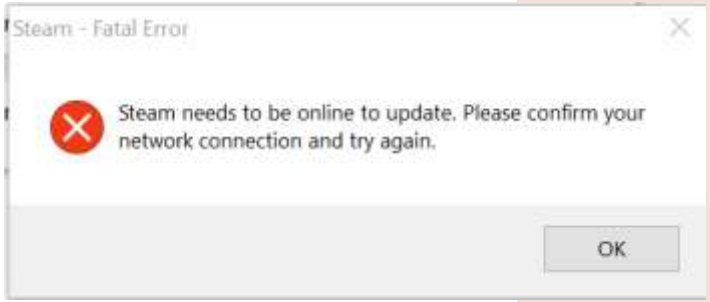
Eric Vyncke @evyncke · Feb 4

Wow #Steam Downloads are now over #IPv6 ! Expecting more **IPv6** traffic in the access store.steampowered.com/news/48091/



15 25

ERNW
providing security.



Games - Steam

- Downloading and installing worked without a problem.
- Unfortunately, the updater (that is run on every start) fails with a “connection problem”.
- As with Spotify, no network activity could be observed -> potentially tries to open IPv4 socket.

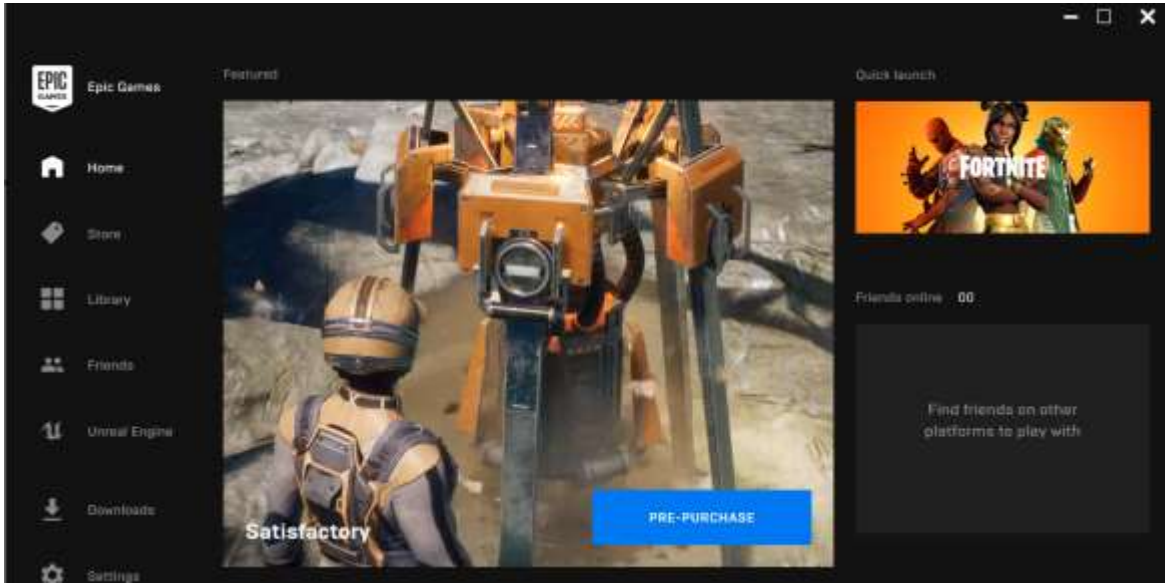
ERNW
providing security.

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.

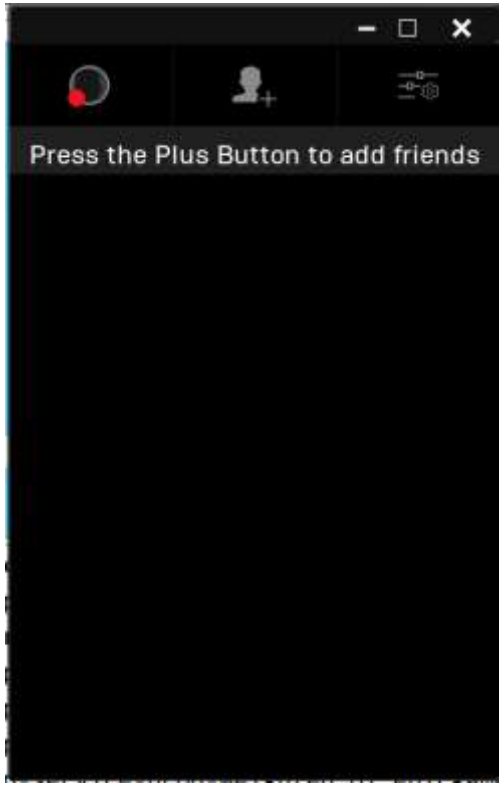
Epic Games Launcher – Looks good from IPv6 PoV



ERNW
providing security.

But.....

XMPP doesn't work.....



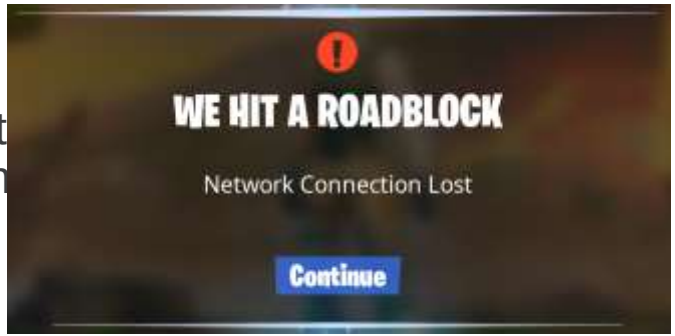
ERNW
providing security.

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
```

Joining the Game

- You can join the lobby, download content and contact the matchmaking server.
- Unfortunately, during the loading screen you get a network connectivity lost error and are back in the lobby.
- Wasn't able to verify what exactly causes the game to fail until now -> further research necessary.



The local log files weren’t helpful either

- [2019.03.15-14.20.00:564][561]LogOnlineGame: Warning: [AFortPlayerController::SubmitReturnToMenuError] Platform=WindowsClient Reason=Network Connection Lost

- [2019.03.18-14.20.00:564][561]LogOnlineGame: UFortMcpUtils::SubmitLogs - Flushing here to avoid slow log uploads blocking SubmitDone

ERNW
providing security.

[BUG] Dedicated server connection issues with IPv6 networks

1

Hi again, as you can already see (link text) we're working in an Android / IOS multiplayer project, and due the new apple policies (link text) we forced to make our app to be IPv6 capable, and here is when a new issue appears. Following the instructions provided by apple (link text) we setup a IPv6 network to perform our own tests.

DarielNS Aug 31 '17 at 5:38 PM

Hi Matthew, we deal with Apple to bypass the requisite for now, but the problem still there. We will aboard the issue again after finish our milestones. I appreciate your interest so much.

zompi2 Aug 31 '17 at 8:23 PM

Hi. If you could inform the programmers - the issue is that there is no structure to hold 128bit ip address anywhere. Adding specialized methods for setting and getting ipv6 should fix all problems.

```
{
    uint32 Addr;
    // Host name resolution just now succeeded.
    ResolveInfo->GetResolvedAddress().GetIp(Addr);
    RemoteAddr->SetIp(Addr);
    UE_LOG(LogNet, Log, TEXT("Host name resolution completed"));
    delete ResolveInfo;
    ResolveInfo = NULL;
}
```

https://answers.unrealengine.com/questions/583305/bug-dedicated-server-connection-issues-with-ipv6-n.html

ERNW
providing security.

For future reference

New: Improved IPv6 Support

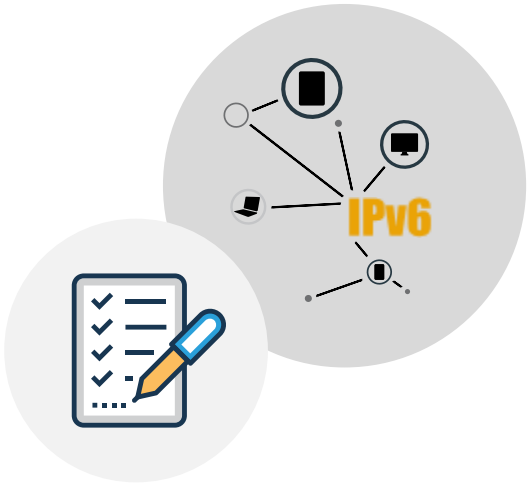
Support for IPv4 and IPv6 has been merged into a single socket subsystem, where previously support for each protocol was isolated to a specific subsystem. This allows platforms that used one of the BSD subsystems to support both IPv4 and IPv6 at the same time, and do it transparently to the calling code.

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

ERNW
providing security.

Interim Conclusion

- While we still see some (minor) breakage (that was to be expected) it is lower than we initially anticipated.
- Apps on mobile devices (Android/iOS) work just fine in an IPv6-only environment.
- Still, there is some work to do primarily for applications installed on your “typical” workstation.



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.

Additional Aspects

- Monitoring & Telemetry
- Measuring Progress
- General communication
  - With the users
  - With “management” (of $ORG)
- Incentivizing (the use of) v6-only
- Configuration
  - Provide DNS resolver to clients by both methods (stateless DHCPv6 and RA option 25/RDDNS).
    - Could be different servers/addresses if interested in telemetry.

Monitoring

- We wanted to get a feeling about the NAT64 translations that are active on our gateway during Troopers at any given time.

- But how do we get these data?
  - SNMP? Unfortunately there is no O.I.D we can query to get the active translations.

EEM to the Rescue

- One nice person on the c-nsp list send me a clever workaround
  - Thank you Nikolay!
- While he had initially created the EEM template for IPv4 NAT entries, we could adjust it easily to our needs

High Level Steps – EEM Template

- 1.) Perform the relevant "show commands"
  - Show nat64 translations in this case
- 2.) Parse the output with some Regex magic
- 3.) Store this value in a SNMP "Expression" MIB
- 4.) Query OID over SNMP to retrieve the value.
- 5.) Rinse and repeat every 30 seconds

ERNW
providing security.

Results – 18.03.2019

Complete EEM Template

```
> snmp mib expression owner NAT64 name NAT64TRANSLATIONS
>   description Total active translations
>   value type integer32
>   expression 0
> !
> event manager applet NAT64-Translations
>  event timer watchdog time 300 maxrun 60
>  action 010 cli command "enable"
>  action 030 cli command "configure terminal"
>  action 040 cli command "do-exec show nat64 translations"
>  action 050 regexp "^.+\s([0-9]+)" "$_cli_result" match
total_translations
>  action 100 cli command "snmp mib expression owner NAT64 name
NAT64TRANSLATIONS"
>  action 110 if $_regexp_result eq "1"
>  action 120  cli command "expression $total_translations"
>  action 130 else
>  action 140  cli command "expression 0"
>  action 150  cli command "exit"
>  action 160 end
```

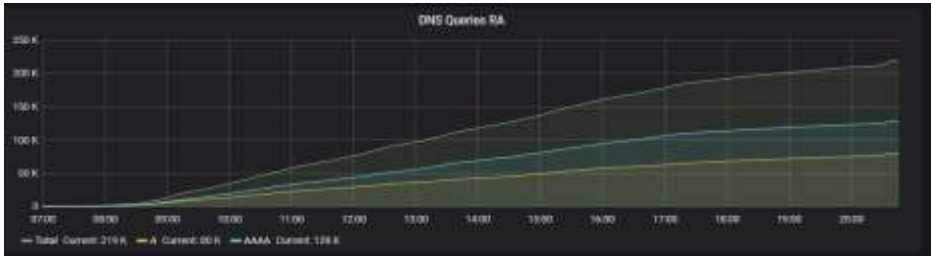
ERNW
providing security.

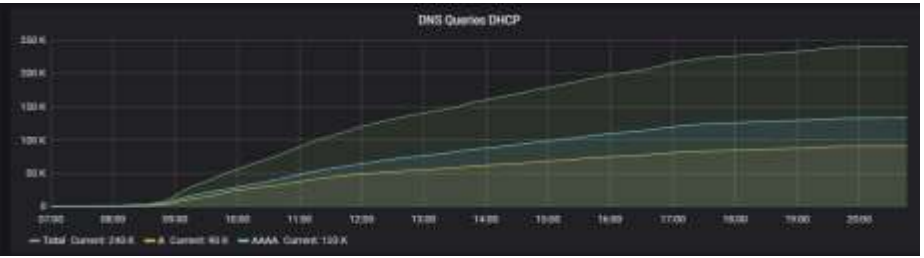
Telemetry for DNS Queries

- We also wanted to a get a feeling to which degree client systems use either the RA or (stateless) DHCPv6 provided DNS server.

- To achieve this, we (mainly Rafael) installed two instances of unbound, provided one each per RA and DHCPv6, and counted the total amount of DNS querries it receives
  - Just to be clear, we do not log what is actually requested.
  - These two DNS servers are only used within the Troopers SSID.

Total Amount of Queries – 18.03.2019





ERNW
providing security.

Implementation Guidance

- Ensure high availability of DNS64/NAT64 components.
- Implement monitoring capabilities during the early phases of the roll out to collect data in regards to non functioning applications.
- Be transparent with user base!

ERNW
providing security.

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.

Thank you for your Attention!


erey@ernw.de


cwerny@ernw.de


www.ernw.de


www.insinuator.net

ERNW
providing security.

References

- FOSDEM 2019
  - https://blogs.cisco.com/getyourbuildon/fosdem-2019-a-new-view-from-the-noc

- MSFT “Solving the IP address predicament with IPv6”
  - https://www.microsoft.com/itshowcase/blog/solving-the-ip-address-predicament-with-ipv6/

Appendix – Tested Applications 1/2

- Social Media
  - Signal
  - Instagram
  - Snapchat
  - Tik Tok
  - Twitter
  - WhatsApp
  - Tinder
  - Threema
- Streaming
  - Spotify
  - Twitch
  - Amazon Music
  - Amazone Prime Video
  - Netflix
  - Apple Music

Appendix – Tested Applications 2/2

- Communication
  - Microsoft Teams
  - Discord
  - Skype
  - Slack
  - Facetime
  - Skype for Business
  - Cisco WebEx
- Games
  - Fortnite
  - PUBG
  - Pokemon Go
  - Steam