IPv6 in Wi-Fi Hotspots

Enno Rey @enno_insinuator
Christopher Werny @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

Agenda

- Strategy / Decisions
- IPv6 in Wireless Networks / Technical Considerations
- Supporting Infrastructure & Stuff

- Summary / Conclusions

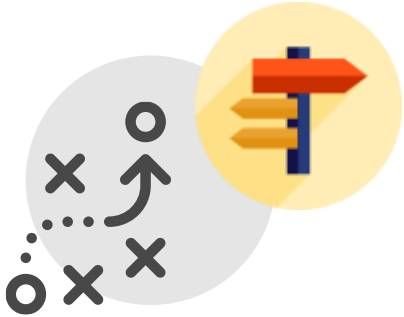
ERNW
providing security.

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".

Strategy / Decisions

- Dual-Stack vs. v6-only (+NAT64)
  - From “IPv6 perspective” the most important one
- Lots of misinformation floating, in different circles
  - Which is why we built the lab discussed on Monday
  - https://ripe78.ripe.net/wp-content/uploads/presentations/42-ERNW_RIPE78_LightningTalk_2019_WiFi_v6only.pdf
- One must thoroughly consider users, platforms, applications and expectations.



- Timeline might play a role, too.

Strategy / Decisions

- Audience
  - Expectations (⇔ communication)
  - Types of devices (platforms, OSs, versions!)
  - Types of applications (e.g. gaming vs. VPN clients)

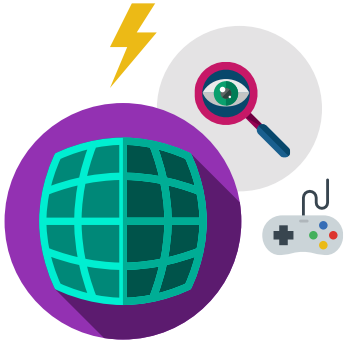
- Requires
  - Definition
  - Testing
  - Communication & mgmt/sponsor approval

ERNW
providing security.

Stuff That *Might* Have Issues

- As of 05/2019 (→ issues might be gone 06/2019...)
  - Gaming (namely multiplayer)
  - VPN clients
    - But a lot of things (progress) seem to happen in this space right now.

- Please note: it is crucial that you perform your own testing if needed. This exact slide should *not* be used to spread FUD in future discussions ;-)



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

From FOSDEM:
IPsec VPN Clients & v6-only

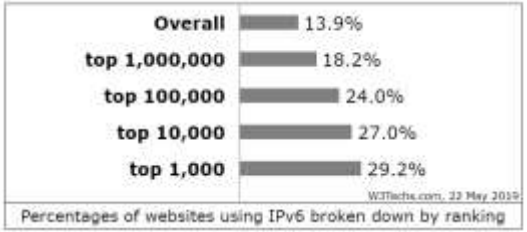
- This means that at least about 2–3% of all traffic was on an IPSEC VPN. And this excludes the TCP VPN traffic on ports 443/TCP and 22/TCP. On the IPv6 network we do not see a similar amount of ESP traffic.

- 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

Rationale re: Trends

- IPv6-enabled connection endpoints (e.g. websites/servers) increase over time.



- Client-side apps (on mobile) nearly fully support IPv6, not least due to Apple's respective requirements (2016).

- Overall IPv6 support of client OSs and "exotic applications" continuously gets better.

Just to Make this Clear

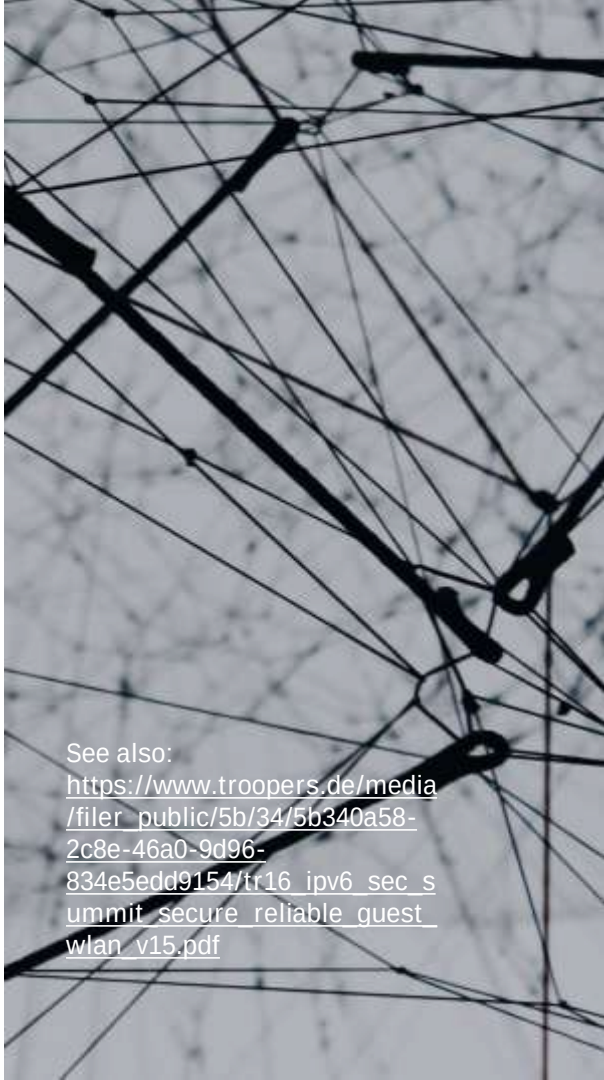
- Based on our testing we think that going with v6-only (+ NAT64) is a reasonable approach now
  - Only very few issues (stuff not working) to expect
  - Namely on platforms or types of app which might not even be relevant for your deployment scenario
  - At the same time this can save a lot of operational 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/RDNSS **and** stateless DHCPv6 to be strongly considered.

IPv6 in Wi-Fi Networks / Technical Considerations

IPv6 in Wi-Fi Networks

- WLANs are shared media
  - Ftr: yes, even with 802.11ax ;-)
- IPv6 communication on the *local link* involves a lot of multicast. How does that translate to/affect traffic
  - On air
  - Between APs serving "[the same] IP subnets"
- Some ongoing discussion, e.g.
  - IETF I-D *IPv6 Neighbor Discovery on Wireless Networks. draft-thubert-6man-ipv6-over-wireless*



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

In Practice

- Some tuning is needed
  - (WLAN) Controller level
    - Which (of the above) to proxy/throttle/block
    - Inter-AP communication
  - L3 infrastructure
    - Properties of RAs
    - Properties of ND
    - Other (e.g. MLD[?])

Neighbor Binding Table on Cisco WLC

```
summary        Display the IPv6 Neighbor Binding Table

(Cisco Controller) >show ipv6 neighbor-binding SUMmary
Binding Table has 173 entries, 173 dynamic (limit 11000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    IPv6 address                            MAC Address       Port  VLAN Type     prlvl age  state     Time left
-- ----------------------------------------- ----------------- ----- ---- -------- ----- ---- --------- ----------
ND  fe80::fedb:b3ff:                        fc:db:b3:           AP   10 wireless  0005    5 STALE      87917
ND  fe80::dafc:93ff:                        d8:fc:93:           AP   10 wireless  0005   36 STALE      88191
ND  fe80::bef5:acff:                        bc:f5:ac:           AP   30 wireless  0005    7 STALE      88784
ND  fe80::aebc:32ff:                        ac:bc:32:           AP   10 wireless  0005   11 STALE      89981
ND  fe80::ad24:85f3:                        18:5e:0f:           AP   10 wireless  0005    5 STALE      90461
ND  fe80::aa66:7fff:                        a8:66:7f:           AP   10 wireless  0005    3 REACHABLE  122
ND  fe80::a6e4:b8ff:                        a4:e4:b8:           AP   10 wireless  0005   30 STALE      86388
ND  fe80::a65e:60ff:                        a4:5e:60:           AP   10 wireless  0005   11 STALE      87166
ND  fe80::9ad6:f7ff:                        98:d6:f7:           AP   30 wireless  0005   11 STALE      88756
ND  fe80::8938:cac5:                        5c:51:4f:           AP   40 wireless  0005    3 REACHABLE  118
ND  fe80::868e:dfff:                        84:8e:df:           AP   10 wireless  0005   38 STALE      88401
ND  fe80::80ec:8805:                        dc:f1:10:           AP   10 wireless  0005   21 STALE      88366
ND  fe80::7ed1:c3ff:                        7c:d1:c3:           AP   30 wireless  0005    2 REACHABLE  178

--More-- or (q)uit
```

RA Throttling on Cisco WLCs / Sample

RA Throttle Policy > Edit

Enable RA Throttle Policy	☑	
Throttle Period (10-86400 seconds)	600	
Max Through (0-256)	5	No Limit ☐
Interval Option	Throttle ▼	
Allow At-least (0-32)	1	
Allow At-most (0-256)	1	No Limit ☐

FHS on WLC Controller

FHS Feature	Default	Configurable?
RA Guard	Enabled	Yes (only on APs)
DHCPv6 Guard	Enabled	No
IPv6 Source Guard	Enabled	Yes
IPv6 ACLs	Disabled	Yes

Gateway Configuration

- To reduce the multicast traffic the following parameters adjusted in Troopers network:
- Router lifetime to 9000 seconds
- Reachable lifetime to 900 seconds
- Unicast solicited RAs
- The above are some "best practice" values, initially inspired by Andrew Yourtchenko from the *Cisco Live* Wi-Fi implementation.

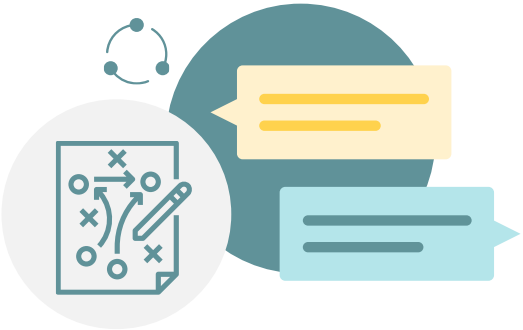
Config Snippet (incl. NAT64)

```
interface GigabitEthernet0/0/0.30
 <output omitted>
 description ====TRP-NAT64===
 encapsulation dot1Q 30
 ipv6 address FE80::1 link-local
 ipv6 address 2A02:8071:F00:64::1/64
 ipv6 enable
 ipv6 mtu 1280
 ipv6 nd reachable-time 900000
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
 ipv6 nd ra solicited unicast
 ipv6 nd ra lifetime 9000
 ipv6 nd ra interval 4
 ipv6 nd ra dns server 2A02:8071:F00:64::251
 ipv6 dhcp server DHCP-TRP-NAT64-v6-POOL
 nat64 enable
```

Supporting Infrastructure

Supporting Infrastructure & Processes

- Infrastructure
  - Captive Portal (usually 3rd party provider) ⇔ IPv6? ;-)
  - Management & WLC/AP-communication ⇔ IPv6? ;-)
  - Telemetry
- Processes
- Communication
  - Users
    - Feedback loop re: stuff not working
  - Management / Sponsor
  - Vendors (of apps that don't work)



Monitoring / Case Study

- 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 OID we can query to get the active translations.

EEM to the Rescue

- One nice person on the c-nsp list sent us 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

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
```

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 resolvers.

- To achieve this, we installed two instances of unbound, provided those per RA and DHCPv6 respectively, and counted the total amount of DNS queries each of them received.
  - Just to be clear, we didn't log what was actually requested.
  - In general you should be very cautious re: telemetry (not only DNS-related) in Wi-Fi hotspot type of networks.
    - Evidently some data points might be privacy-invasive.
    - Regulations might kick in, even conflicting ones.

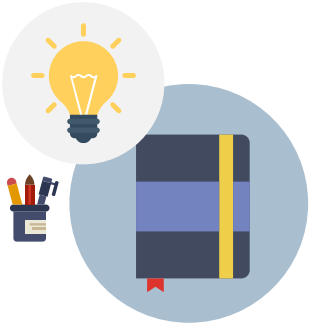
Communication et al.

- How to incentivize users to use the v6-only SSID if there's a "legacy" (usually: dual-stacked) in parallel?

- How to provide feedback loop for stuff not working?
  - "Go to vendor" [+ "here's a template"] vs.
  - Common generic customer support channels

Summary / Conclusions

- Deploying IPv6-enabled Wi-Fi hotspots requires specific considerations and tech. adjustments
  - Define strategy re: v6-only ✅
  - Perform specific configuration on devices ✅
  - Monitoring & telemetry ⚠️
  - Communication with users, vendors, mgmt.



Thank you for your Attention!

www.ernw.de
www.insinuator.net

Enno Rey, @enno_insinuator
Christopher Werny, @bcp38_

ERNW
providing security.

Image Sources

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