Why IPv6 Security Is So Hard – Structural Deficits of IPv6 & Their Implications

Enno Rey, erey@ernw.de, @enno_insinuator

#whoami

- Some background in large scale networking, doing security as a full-time profession since ’97.
- Founded (in 2001) a company specialized in high level security assessments and consulting
  - www.ernw.de
- Blogging about IPv6 & other pieces at https://insinuator.net/tag/ipv6/
- This talk is an shortened (and slightly updated) version of
  - https://ripe74.ripe.net/archives/video/58/

Agenda

- Some objectives, from a security perspective
- Properties of IPv6, and their implications
- Conclusions

Some Objectives
When It Comes to Network Security

Taking an Infosec Practitioner's View

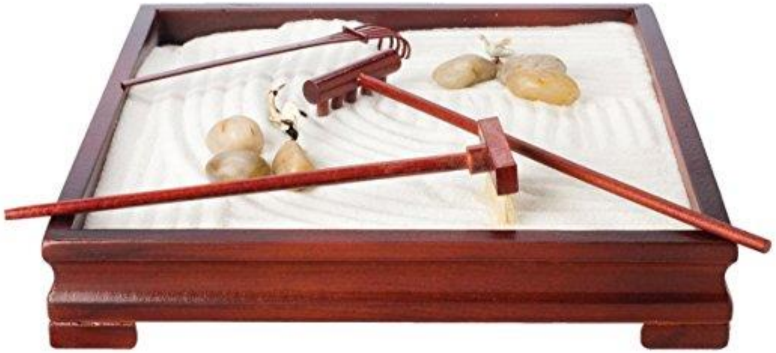
- Predictability (<=> Trustworthiness)
  - "trust: the extent to which someone who relies on a system can have confidence that the system meets its specifications, i.e., that the system does what it claims to do and does not perform unwanted functions" (RFC 2828).
- Identification
  - Be able to identify actors being part of connections
    - Usually the basis for filtering
    - Helpful in the context of accountability, too.
- Ability to restrict / filter
  - To enforce security policy.

A bit more Abstract Objectives

- Keep things simple
- Avoid complexity
- Minimize state

Keep It Simple & Small

- There might be a direct relationship between (number of) lines of code and amount of vulnerabilities…
- Parsing needs CPU cycles
  - Often: more parsing → higher susceptibility to DoS
- The more protocols one uses the more attack surface might be exposed.



William of Ockham

Entia non sunt multiplicanda praeter necessitatem.

This translates roughly as:

More things should not be used than are necessary.

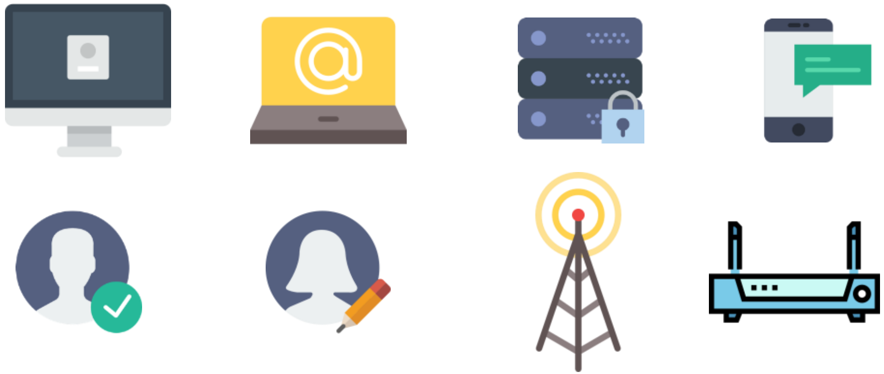
Occam‘s Razor
Phrased by a Networking Guy

- RFC 1925:

  (12) In protocol design, perfection has been reached not when there is nothing left to add, but when there is nothing left to take away.

Avoid Complexity

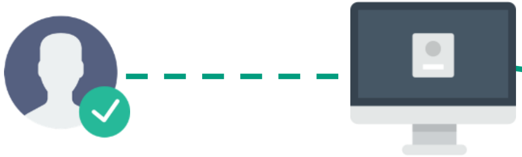
Complexity (I)

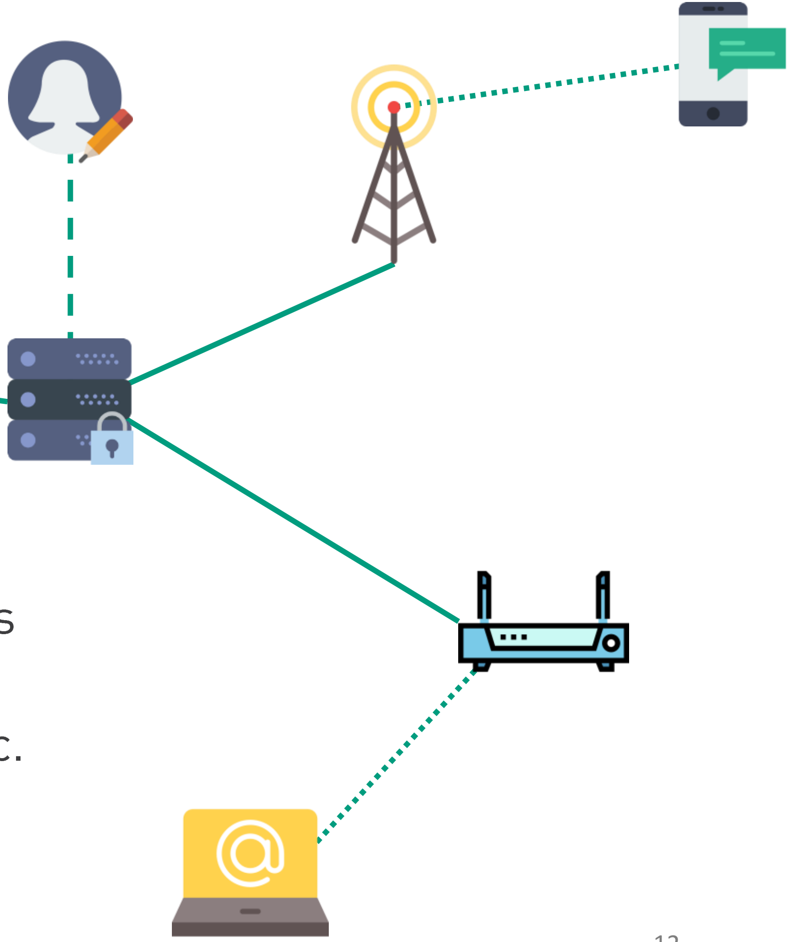


- Composed of many interconnected parts

See also: https://insinuator.net/2015/05/ipv6-complexity/

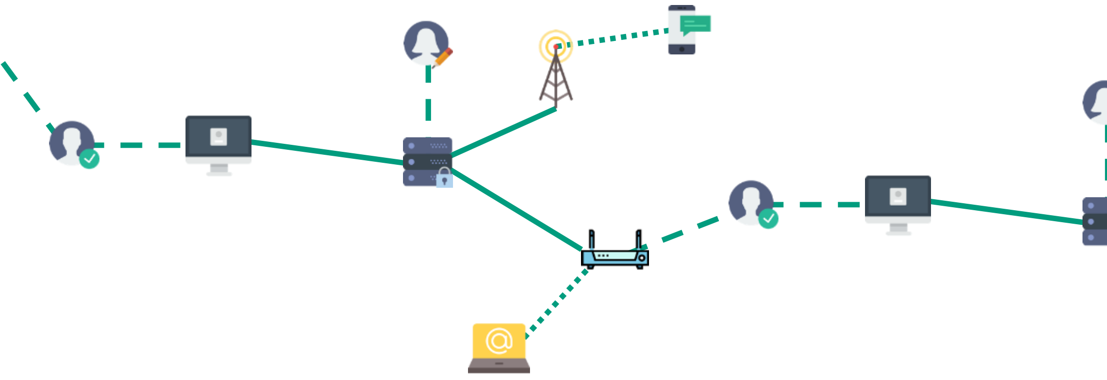
Complexity (II)

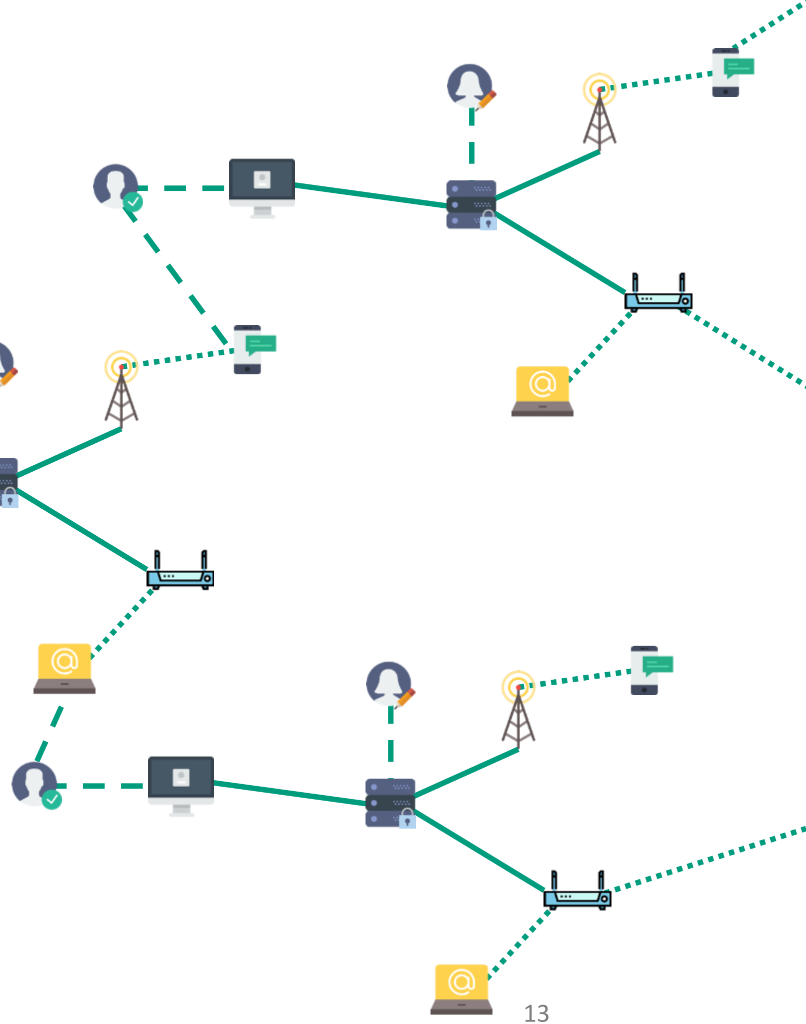




- Composed of many interconnected parts
- Characterized by a very complicated or involved arrangement of parts, units, etc.

Complexity (III)





- Composed of many interconnected parts
- Characterized by a very complicated or involved arrangement of parts, units, etc.
- So complicated or intricate as to be hard to understand or deal with

Why the "Understanding" Part is Crucial

- Understanding allows to
  - Develop mental model of inputs & their associated outputs
  - Predict output

- Mental model allows you to recognize when system isn't working correctly
  - Troubleshooting & fixing
  - Detection of security violations

ERNW providing security.

IPv6 – Interactions

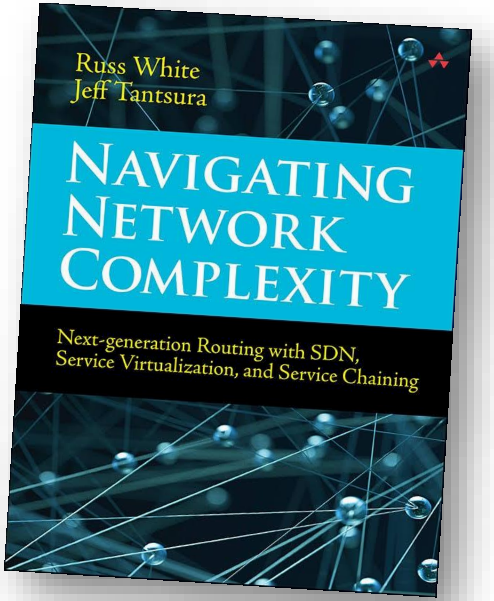
- Various types of relationships between SLAAC and DHCPv6
  - Unclear specs & several generations of them
  - Major vendors deviate, and still get it wrong
  - IETF WGs not aligned
    (e.g. RDNNS related momentum in v6ops vs. RFC 8106, sect. 5.3.1)

- Relationship between ND and MLD
- Relationship between RA flags, routing tables and address selection mechanisms
- Relationship between IP and other layers
  - All those lovely MTU issues come to mind.

(Minimize) State

- "State" usually encompasses several dimensions:
  - Amount of state (entries in $TABLE, RAM etc.)
  - Frequency/speed of state changes
  - Surface
    - Depth of interaction
    - Breadth of interaction

- **Simple rule:** the more state to be processed the higher the susceptibility to DoS.



IPv6 Properties

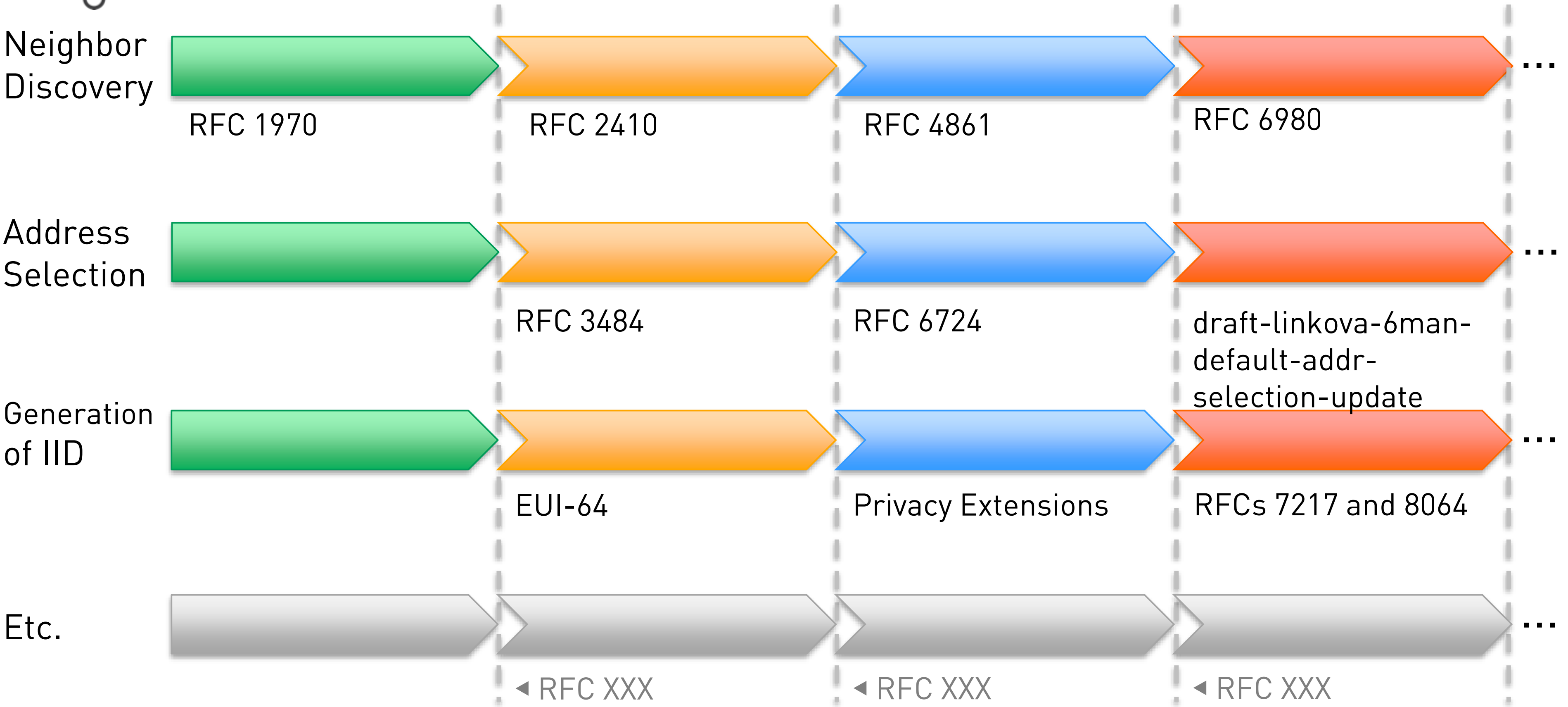
Now Let's Have a Look at IPv6's Technical Properties

- Oh, that's an easy one. Just look at the RFCs.

- "The nice thing about standards is that you have so many to choose from."

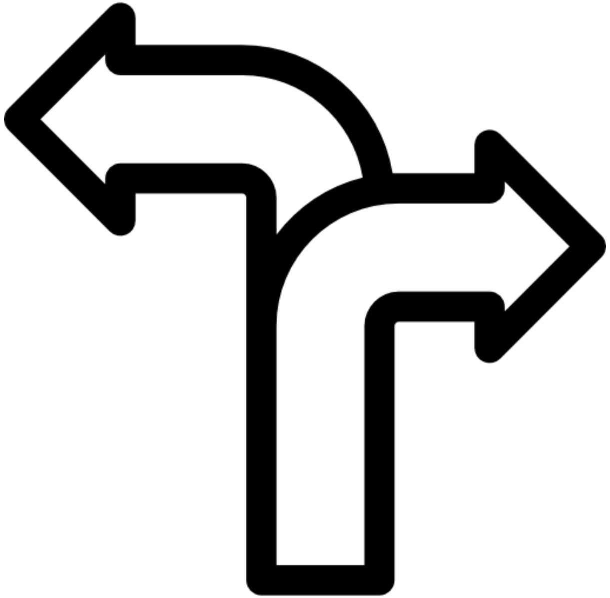
  Andrew Tanenbaum

Different Generations of IPv6 Stacks



Focus on Four of Them

- Multicast instead of broadcast
- Multiple address types & addresses
- Parameter provisioning
- Extension Headers



Multicast Instead of Broadcast

- Multicast based networking
  - Requires more state.
  - Usually (and in our case) requires more parsing
- One can probably write an implementation of ARP in max. 100 lines of Python code
  - Try this with ND ;-)
  - RFC 4861 has 94 pages. And has been updated by six (6) other RFCs…
- But, hey, you save some context changes/ interrupts on CPUs of local systems…

How (Multicast) State Can Kill a Network

"Our network switches have been observed using far more CPU than has historically been the case, we have had a variety of packet storms that appear to have been caused by forwarding loops despite the fact that we run a protocol designed to prevent such loops from taking place, and we have had a variety of unexplained switch crashes."

Massachusetts Institute of Technology

From: http://blog.bimajority.org/2014/09/05/the-network-nightmare-that-ate-my-week/

Multiple Address Types & Addresses

- IPv6 introduces the concept of a link-local address, as opposed to "global" addresses
  - Separating the two is not a new concept
  - Still it's mainly associated with Ethernet networks, and doesn't make much sense in other types of networks, e.g. mobile/telco.

- Separating the two introduces new problems...

LLA

GUA

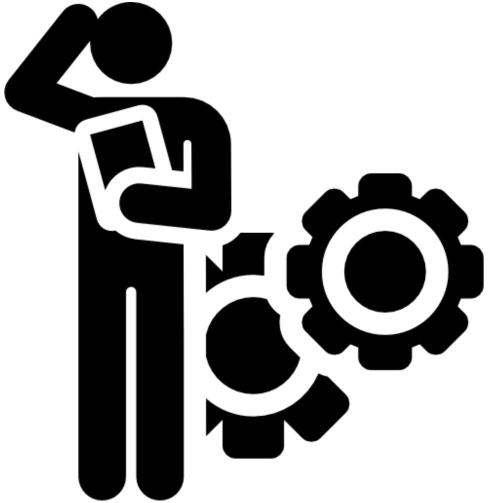
ULA

ERNW
providing security.

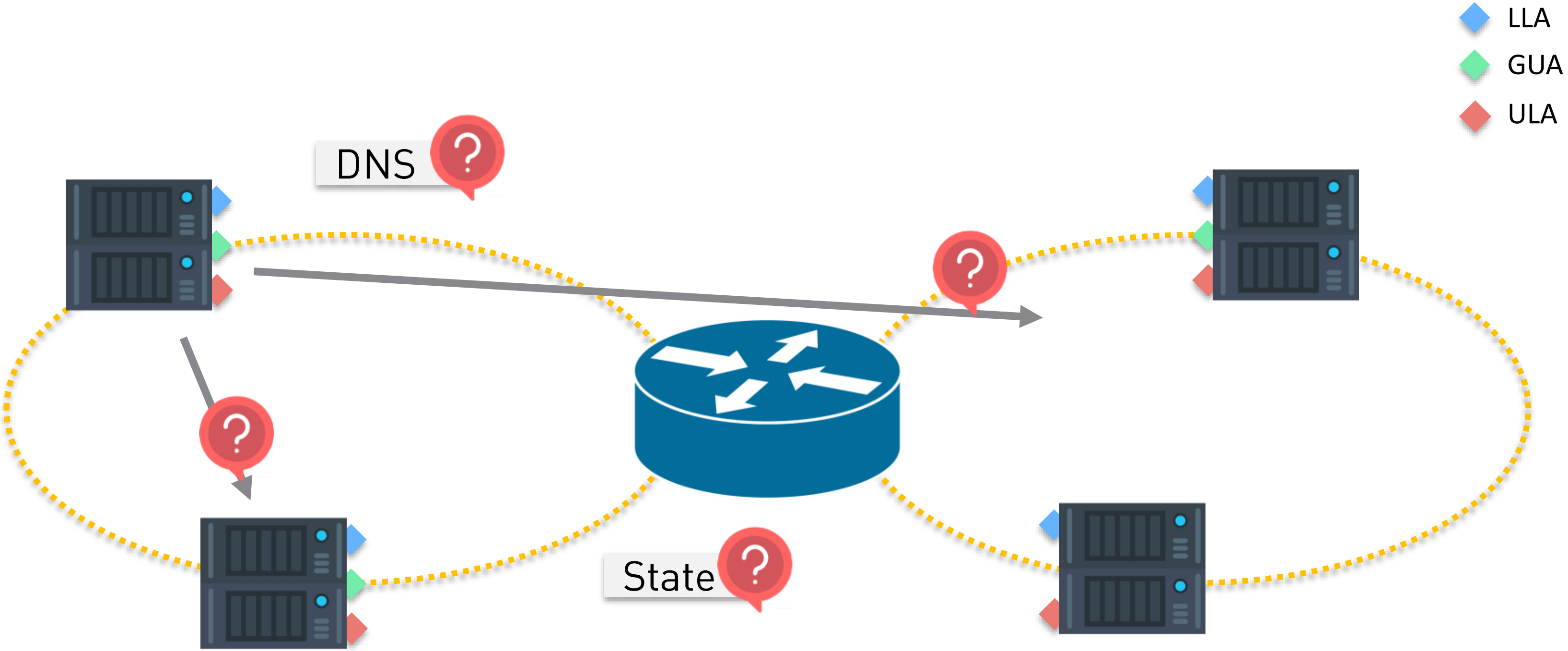
Multiple Address Types / Problems

- It increases (doubles?) the amount of state
  - Routing tables
  - Handling of addresses in kernel/IP stack etc.

- It creates a decision problem
  - Which address to choose for communication acts?
  - You´re probably aware that – surprise! – there‘s several IETF documents for this.



That Decision Problem

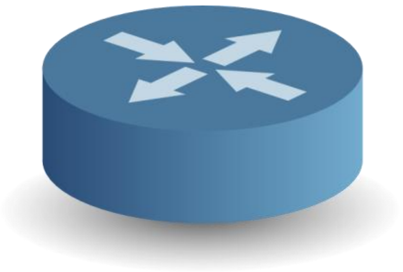


Parameter Provisioning

What’s a *Router*?

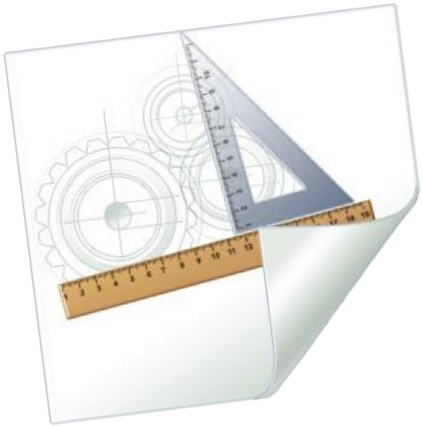
- Wikipedia:
  - router = “a **router** is a device that forwards *data packets* between *computer networks*”

- RFC 2460:
  - router: “router - a node that forwards IPv6 packets not explicitly addressed to itself.”



What's a *Router*, in IPv6?

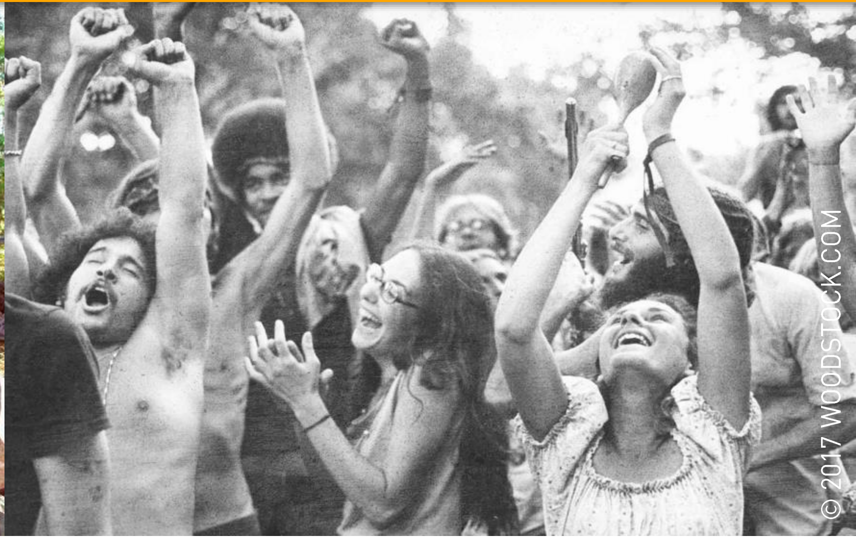
Looking Closer



- RFC 2461: "Routers advertise their presence together with various link and Internet parameters either periodically, or in response to a Router Solicitation message".
- In the end of the day, in IPv6 a router is not just a forwarding device but a provisioning system as well.

IPv6’s Trust Model

On the *local link* we’re all brothers.

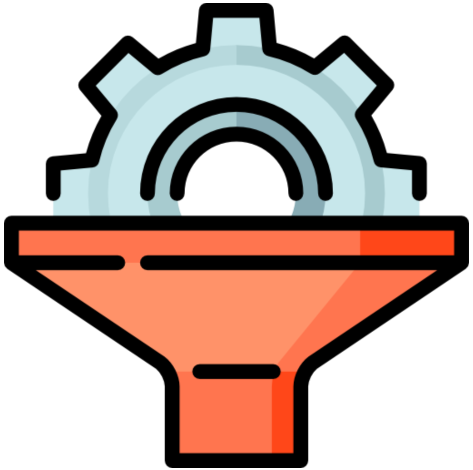


But Can't We just Filter the Bad Stuff?

There's RA Guard et al., right?

- Hmm... like most other *blacklist- based* security features RA Guard can be circumvented.
  - There's no (easy) cure for this. Choose two out of (function|speed|cost).

- Hey, we have RFC 6980 for this.
  - I for one consider this one of the most important IPv6 RFCs from the last years.
  - But it seems not easy to implement...
    - Which in turn might not be surprising...



From some Recent Testing

https://insinuator.net/2017/03/testing-rfc-6980-implementations-with-chiron/

Test Case No.	Description	Chiron Options Used (in addition to baseline cmd)	Impact on Target OS' IPv6 Config (without RA Guard)	What was observed in Wireshark on Target OS? (without RA Guard)	What still got through with RA Guard enabled?	Overall Result With RA Guard Enabled
13	Two fragments, with two DestOptions in fragmentable part	-lfE 60,60 -nf 2	Added 2nd default gw, created additional address	One fragment plus RA packet which contains two DestOptions EHs	1st fragment, but *not* the RA	No impact
14	Four fragments, with two DestOptions in fragmentable part	-lfE 60,60 -nf 4	Added 2nd default gw, created additional address	Three fragments plus RA packet which contains two DestOptions	Three fragments, plus RA containing two DestOptions EHs. Nothing logged on the switch.	Successful attack
15	Two fragments, with two RoutingHdr EHs in fragmentable part	-lfE 43,43 -nf 2	Added 2nd default gw, created additional address	One fragment plus RA packet which contains two RoutingHdr EHs	Two fragments, plus RA containing EHs. "traceback" on switch console when running 15.0(2)SE2	Successful attack when switch runs 15.0(2)SE2, no impact when switch runs 15.0(2)SE10a
16	Two fragments, with two RHs and two DestOptions, in mixed order	-lfE 60,43,60,43 -nf 2	Added 2nd default gw, created additional address	One fragment plus RA packet which contains the four EHs	1st fragment, but *not* RA	No impact
17	Same as 16 but four fragments	-lfE 60,43,60,43 -nf 4	none	1st three segments only, but not RA	1st three fragments, but not RA	No impact
18	Same as 16 but three fragments	-lfE 60,43,60,43 -nf 3	Added 2nd default gw, created additional address	Two fragments, then RA containing all EHs	1st two fragments plus RA	Successful attack

Extension Headers / Protocol Design

- Two main school of thoughts (re: protocol design)
  - Design a protocol that can handle many situations, and also support extensions that hadn´t been thought of initially.
  - Design a protocol that (only) supports initial requirements.
- Looking at RFC 2460 the decision taken at the time immediately becomes clear.
- I´m not judging this. But one must realize …

Implications of an Extensible Protocol

- Probably less predictability
- Almost certainly higher complexity
- More parsing (→ more code)
  - Also: https://youtu.be/Pru5BRrlmz0
- Most probably more state needed

What an IPv6 Datagrams Looks Like…

ERNW
providing security.

Problem

- Variable types
- Variable sizes
- Variable order
- Variable number of occurrences of each one.
- Variable fields

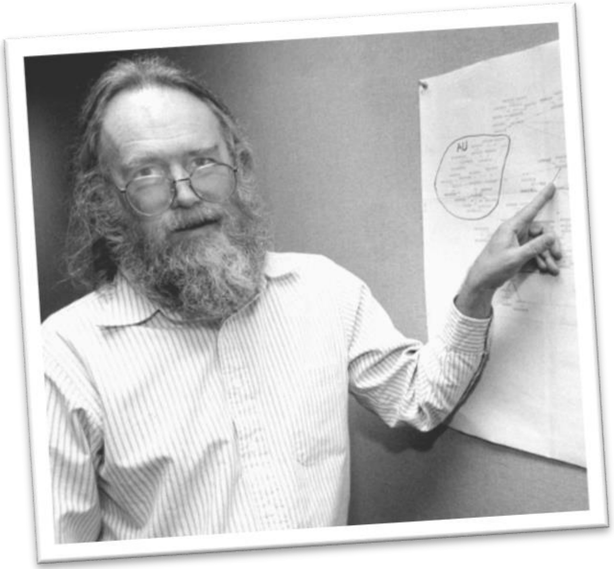
IPv6 = f(v,w,x,y,z)

ERNW
providing security.

Extensible Protocols Need This

"be conservative in what you do,
be liberal in what you accept from others"

RFC 761



Security Problems Due to EHs

- Heavily increased parsing complexity
- Evasion of blacklist-based security controls
  - IDPS systems.
  - First Hop Security (FHS) features
  - Insufficient ACL/filtering implementations.
- For the record
  - “EHs“ in the terminology of most sec ppl encompass: HBH, DestOptions, RH, FragHdr
  - AH &ESP have their (legitimate) role.
  - But nothing else…

https://www.ernw.de/download/eu-14-Atlasis-Rey-Schaefer-briefings-Evasion-of-HighEnd-IPS-Devices-wp.pdf

Conclusions (I)

- IPv6 is much more complex (than IPv4)
  - On the protocol level.
  - On the operations level.

- IPv6 requires much more state
  - On L2 devices (e.g. multicast groups)
  - On L3 devices (*neighbors*)
  - On security devices

ERNW
providing security.

Conclusions (II)

- Securing L2 communication (ND/RAs et al.) is a tough (impossible) task in IPv6 networks.
  - Consider all versions of RA Guard as evadable.
  - And it's not even available on most virtual switches
    - Maybe HV/NIC level filtering to the rescue in DC
      https://blog.apnic.net/2017/07/12/local-packet-filtering-ipv6/
  - Move to L3 instead?
    - See also "Unique IPv6 Prefix Per Host" approach
    - Note: this brings some trade-offs re: state.

What Now?

- Try to understand
  - IPv6 *interactions* in your network.
  - where state is maintained by/for IPv6.
  - vendor agendas & incentives, namely in context of IETF
- Minimize complexity where possible
  - Drop (the vast majority of) EHs at the border of your DCs.
  - Limit interactions and/or number of protocols.
  - Keep addressing simple…
- Minimize the amount of state where possible
  - Re-think filtering approach?
  - Perform an inventory which type of state is created on different types of devices. Understand trade-offs & device limitations when reducing state on $SOME_LAYER in exchange for an increase on $OTHER_LAYER.

THANK YOU... ...for yours!

@Enno_Insinuator

erey@ernw.de

ernw.de

insinuator.net

Slides available soon.

Sources

As indicated on slides.

Image Source:

- Icons made by Freepik from www.flaticon.com