IPv6 Address Management – The First Five Years

Enno Rey, erey@ernw.de
@enno_insinuator

ERNW
providing security.

#whoami

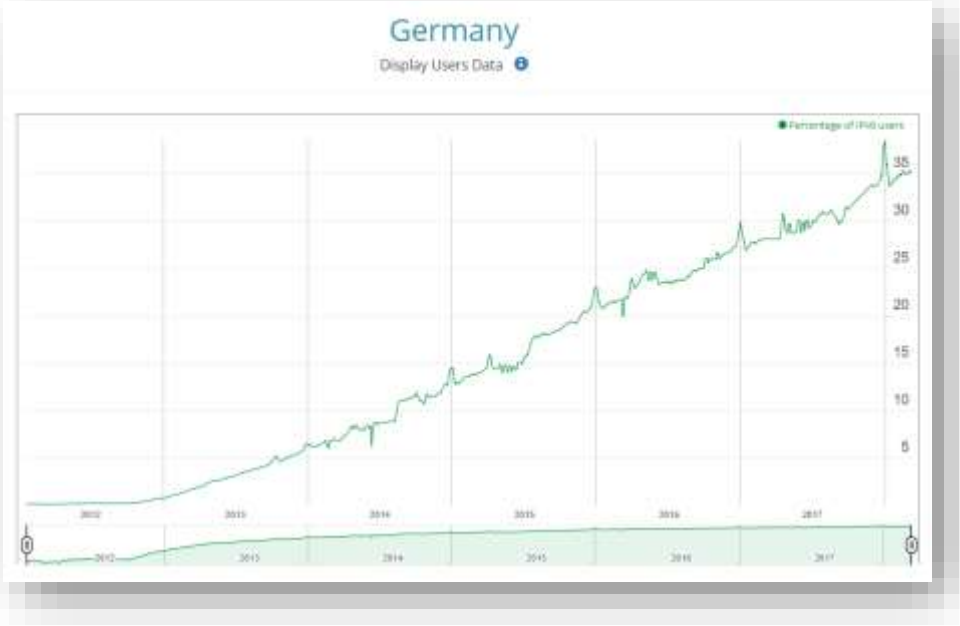
- Some background in large scale networking, doing security as a full-time profession since '97.
- Founded (in 2001) a company specialized in highly technical security assessments and consulting
  - `www.ernw.de`
- Blogging about IPv6 & other pieces at `https://insinuator.net/tag/ipv6/`
- Responsible for administrative tasks in a number of LIRs, incl. ORG-HACK1-RIPE ;-)

ERNW
providing security.

Agenda

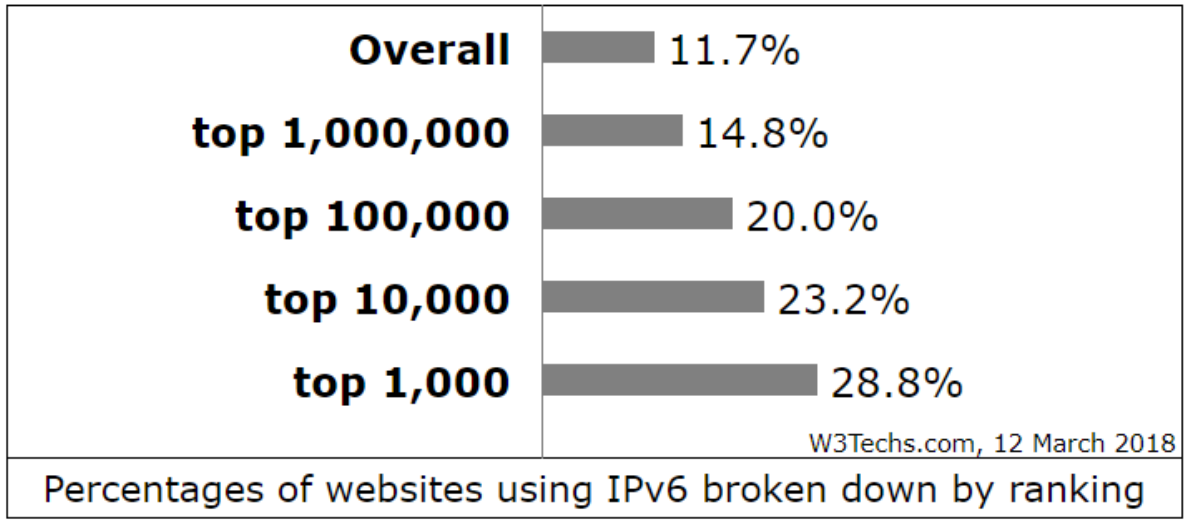
- Approaches to get addresses for an organization (Review)
- Approaches to distribute addresses within an organization
- Approaches how to actually manage addresses

Very Quick Stats (1)



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

Very Quick Stats (2)



Percentages of websites using IPv6 broken down by ranking

Source:
http://w3techs.com/technologies/breakdown/ce-ipv6/ranking

Very Quick Stats (3)

CC	Country	IPv6 Capable
BE	Belgium, Western Europe, Europe	59.09%
IN	India, Southern Asia, Asia	58.32%
UY	Uruguay, South America, Americas	44.28%
US	United States of America, Northern America, Americas	43.74%
DE	Germany, Western Europe, Europe	41.85%
GR	Greece, Southern Europe, Europe	38.98%
LU	Luxembourg, Western Europe, Europe	30.60%
CH	Switzerland, Western Europe, Europe	30.46%
JP	Japan, Eastern Asia, Asia	27.83%
GB	United Kingdom of Great Britain and Northern Ireland, Northern Europe, Europe	25.88%

Source:
http://stats.labs.apnic.net/ipv6/

Very Quick Stats (4)

ERNW
providing security.

Very Quick Recap:
Ways of Getting IPv6 Addresses for $ORG

- Act as *Local Internet Registry* (LIR) / Become member of RIR (e.g. RIPE)
- Apply for *provider independent* (PI) address space/assignment, thru *sponsoring LIR*
- Get (provider dependent) *assignment* out of ISP's (provider aggregatable) *allocation*
- Other (e.g. via tunnel broker)

- Pretty much all large enterprise organizations we know have opted for the 1st ("LIR") approach.

Reasons to Act as LIR / Become RIPE Member

See also:
https://insinuator.net/2017/10/position-paper-on-an-enterprise-organizations-ipv6-address-strategy/

http://www.ipv6conference.ch/wp-content/uploads/2015/06/B09-Rey_IPv6_Business_Conference_Address_Space_Approaches.pdf

Enterprise LIR / Things to Keep an Eye On

- Strict Filtering
  - Haven't seen issues in a while (provided proper `route6` objects were created).
  - See also:
    - https://www.troopers.de/media/filer_public/8a/6c/8a6c1e42-f486-46d7-8161-9cfef4101ecc/tr15_ipv6secsummit_langner_rey_schaetzle_slash48_considered_harmful_update.pdf
- Out-of-region announcements
  - Some of our customers do this ("RIPE space" getting announced in Americas, APAC, LATAM)
    - So far we've not observed issues.
  - On the other hand some organizations have opted to explicitly choose another path, namely for reasons in the space of geolocation.

How to Distribute Address Space Within $ORG

Address Management

- "Address Management" can serve different functions & objectives
  - *Prescriptive*
    (Try to) control how addresses are granted (and assigned to individual systems), usually on the basis of rules.
    - Requires governance ;-)
  - *Descriptive*
    Document/perform inventory of the current use of addresses

See also:
https://insinuator.net/2016/02/ipv6-address-planning-in-2016-observations/

ERNW
providing security.

IPv6 Address Plan / Objectives

Goal	Weighting (Sample)
Persistence	High
Applicability	High
Scalability	High
Support for routing based security	Medium
Ability to aggregate	Medium
Ability to delegate	Medium
Legibility	Low

See also:
https://insinuator.net/2015/12/developing-an-enterprise-ipv6-security-strategy-part-2-network-isolation-on-the-routing-layer/

Observations

- For many years many organizations & people have tried to come up with well-structured (and –meant ;-) plans, centered around sites & services, see for example
  - https://labs.ripe.net/Members/steffann/preparing-an-ipv6-addressing-plan
  - http://shop.oreilly.com/product/0636920033622.do
  - http://blog.ipspace.net/2015/04/how-do-i-start-my-ipv6-addressing-plan.html
  - https://insinuator.net/2014/05/ipv6-address-plan-considerations-part-3-the-plan/
- From what we see this just doesn't work in practice…
  - VUCA type of organizations
  - "Agile"/MVP-driven projects
  - Slow start of IPv6 + disperse efforts here+there

This is Why…

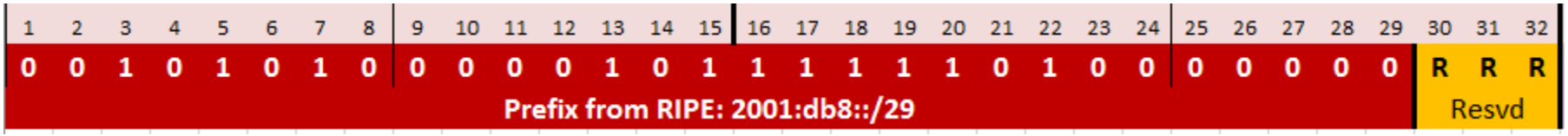
- We usually recommend a bit different approach
  - Not too prescriptive
  - Flexible
  - Allows for “delegation to projects”…

- We already see some organizations working on this basis. It’s laid out on the following slides.

Address Plan

General Approach

- Overall *prescriptive* approach, but given many uncertainties only loose prescriptions will be made.



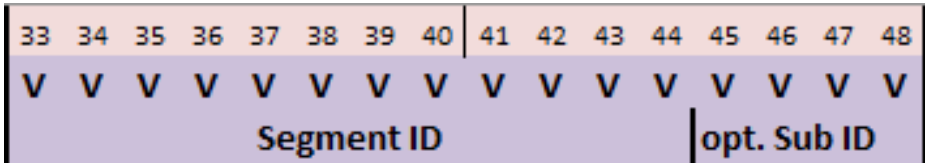
- Starting point is the first /32
  - From allocation 2001:db8::/29.
  - All other (seven) /32s will be used as a reserve, for the moment.
- Overall three hierarchy levels planned
  - Allows for high degree of future flexibility.

Address Concept

Hierarchy levels

- “Segment ID“ (/44)
- “Sub ID“ (/48)
- “Network ID“ (/64)

Segment ID



- Generic high level identifier for various types of segments/networks
  - 4096 possible entities (or 256 when grouped)
  - Examples: “Corp Site Berlin“, “Ireland Subsidiary“, “Cloud XY“

- Represented by first three letters in third quartet of address.

Segment ID

Number Range & Representation

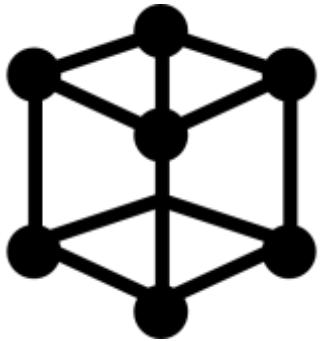
- 2001:db8:XXXY, where XXX = ID

2001:db8:2000::/44
2001:db8:2980::/44
2001:db8:4480::/44
2001:db8:8800::/44
2001:db8:aa80::/44
2001:db8:f100::/44

Segment ID

Mode of allocation

- Within first /32, and following initial grouping, Segment IDs will be allocated in a sequential manner.
- Segment IDs are administered in group of eight IDs so that a requesting party can get several consecutive Segment IDs, even with temporal delay.
  - Grouping allows for delegation of address management to specific organizational entities or 3rd parties.
- Still, consistent address management, with proper roles & tools will be crucial!
  - See discussion below.



Sub ID (Optional)

- /48
  - Four bits only, max. 16 entities
- 4th letter of third quartet
  - 2001:db8:XXXY::/48
- Allows for additional “tagging“ of segments for handling
  - In firewall rules
  - For QoS purposes/marking (ideally with “wildcard rules“)
  - Routing based security
- Use with caution!
  - All parties involved have to understand implications, namely on operations.

ERNW
providing security.

Sub ID

Potential Approach

- “0“: default ID
- [...]
- “D“: data center networks (?)
- “E“: “Priority Queue“
- “F“: “Internal“ / “Secure“
  - → Special treatment on border gateways, firewalls etc.

Network ID / “Net ID“

- /64 (default IPv6 prefix length/size for subnets)

49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Net ID															

- To be used for individual VLANs, in a flexible manner. This means
  - No additional encoding of information (prescribed).
  - Can be assigned in a sequential manner within segment (ID).

Network ID

- Full fourth quartet (→ max 4096 entities)
  - 2001:db8:XXXY:NNNN::/64 e.g.
  - 2001:db8:1230:1234::/64
  - 2001:db8:1230:90ab::/64
  - 2001:db8:1230:aaaa::/64
  - 2001:db8:1230:cafe::/64
- Note: Network ID “0000“/“0“ not to be used (to avoid lack of clarity in context of RFC 5952)

Processes

IP Addresses

- Constitute the identity of an entity which communicates in an IP-based network, like the Internet ;-)

- Identity can be used for
  - Communication
  - Ex-post identification of an entity which performed a communication act (log/incident analysis et al.)

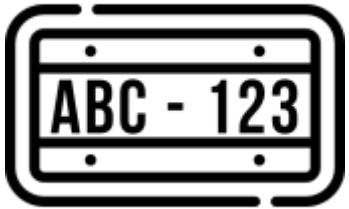
The Memento Mori of IP Networking

Dance of Death
(15th century fresco)

Note:
- There is a strong operations perspective in the above statement.

Reasons (Triggers) to Renumber

- Assigned addresses are not unique within $ENVIRONMENT
  - There‘s a clutch for this. It‘s called NAT.
    - It either sucks (IPv4) or it is not available (IPv6)
  - Any clear idea what $ENVIRONMENT looks like in, say, five years? See…



- Assigned addresses might turn out to be “unfit for purpose“ at some later point
  - This is a clear risk in the age of agile and MVP driven projects.
  - See also:
    - https://insinuator.net/2017/11/why-it-might-make-sense-to-use-ipv6-in-enterprise-infrastructure-projects/

ERNW
providing security.

General Differences Between “Private”/RFC 1918 (IPv4) Address Space & Public/Global Addresses

- RFC 1918 don’t have an “owner”
  - IPv6 GUAs do.
  - With power comes responsibility.
    - Handling of abuse.

- RFC 1918 can’t (shouldn’t) be routed outside own AS.
- GUAs can (be routed)…
  - → route leaks, becoming transit etc.

Challenges Induced by IPv6 (as LIR)

- In most cases only global IPv6 addresses (GUAs) will be used within $ORG
  - Those are kind-of “public resources“.
    This means handling them needs some extra scrutiny (in comparison with IPv4)
    - Route leaks, address abuse etc.
- Annual payment of RIPE fees needs to happen
  - Else resources (incl. IPv4 [PI] addresses) can be lost

Processes in Context of RIPE Membership / LIR

- Point of contact to RIPE NCC
- Payment (recurring per year)
- Database maintenance
  - Creation of objects
    (primarily `inetnum6/route6/domain` objects)
- Attend RIPE meetings ;-)

Changes (II)

- Assigning addresses to a site with a local Internet breakout might mean it has to be “routed independently“
  - Creation of proper `route6` objects required then.
  - Assignment itself to be accompanied by creation of `inet6num` object.

- All these require proper roles & responsibilities
  - And ability to access RIPE web interface when needed.
    - → Accounts & passwords!

Current Process & Procedures as for (IPv6) Address Mgmt within $ORG

- this slide intentionally left blank

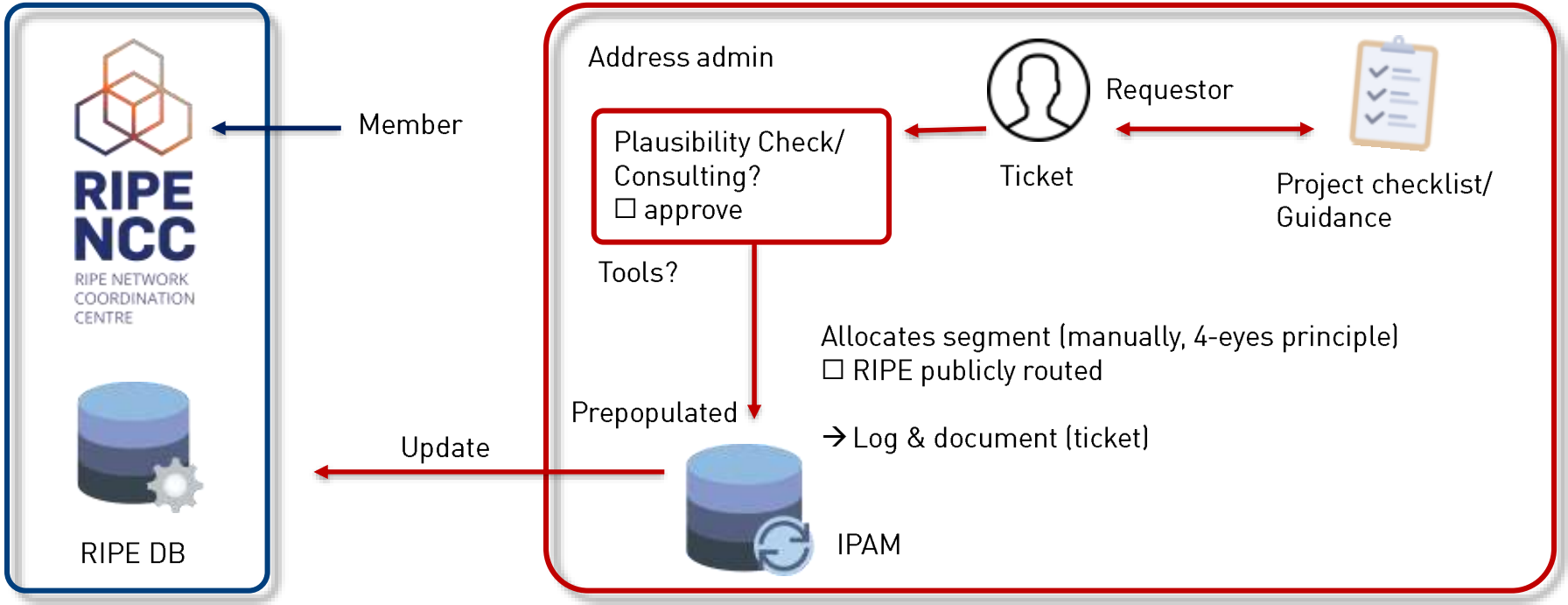
ERNW
providing security.

Processes / High-Level View

- LIR administration
- Ownership/maintenance/review of address concept
- Assignment of address ranges to $REQUESTORs

- Maintenance of “address [management] repository”
  - Usually an IPAM plays a role here…
- To be discussed: Where (within org)/who (sh|c)ould be owner of these processes?

Process / Overview



Processes / Details

- Requestor requests (IPv6) address block
  - Authentication / Authorization needed? [no]
    - Check will later be performed by address_admin
  - Web-Interface, Ticket, e-mail?[Ticket]
    - [Ticket], ideally w/ mandatory fields
  - Has to go through “project guidance/checklist” first.
    - Guidance tb made available in advance via address_admin (incl. governance/review/et al.)
    - Requestor has to confirm “have read & understood” ;-)
    - Guidance / checklist will be created by address_admin

Who is/can be $REQUESTOR?

- Can by anything/anybody
  - Project
  - Not project-related
  - “from the business line”
  - Originating from 3rd party
    - 3rd party performing operations

Processes

- Consulting if $REQUESTOR has questions
- Allocation of addresses (usually “Segment ID” level) to an administrative entity
  - In case of not publicly routable → fully automated
- Provisioning of parameters incl. IP addresses to individual systems.
  - Change of parameters etc.
  - → to be performed by $OPs of $REQUESTOR

Sub-Processes “Address Administration” (1)

- After request comes in
  - Plausibility check
    - → if needed, consulting (to $REQUESTOR)?
  - Approve [expected default] or deny
    - This decision has tb enforced by proper workflow.

Processes / Allocation of Addresses

- Address_Admin
  - Hands out 1st Segment_ID of group/container
  - In manual process (four-eyes principle)
    - Q: can/should this be automated?
  - Log/document allocation
    - How? Reference to ticket_no?

ERNW
providing security.

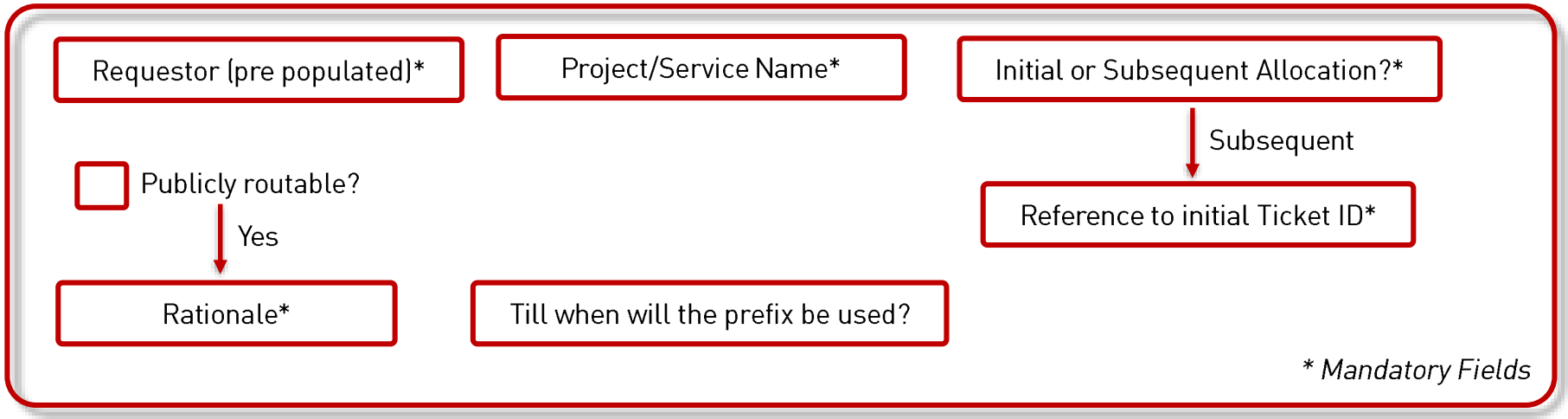
Approval Process

- Degree of automation depends on properties?
  - E.g. “Publicly routable” attribute?
    - Yes, *this* attribute.
    - Other fields/properties leading to involvement of human (address_admin)?
- Otherwise can happen in highly automated manner
  - This requires tickets with mandatory fields.

IPAM / Prerequisites

- Segment_IDs prepopulated
  - Q: how is this done?
  - In groups of eight (8) segment IDs
    - “Containers” as of $SOME_IPAM?
  - Dedicated property “[Seg] In global routing”
    - If set → create `route6` object in RIPE DB
      - $SOME_IPAM supports this via API

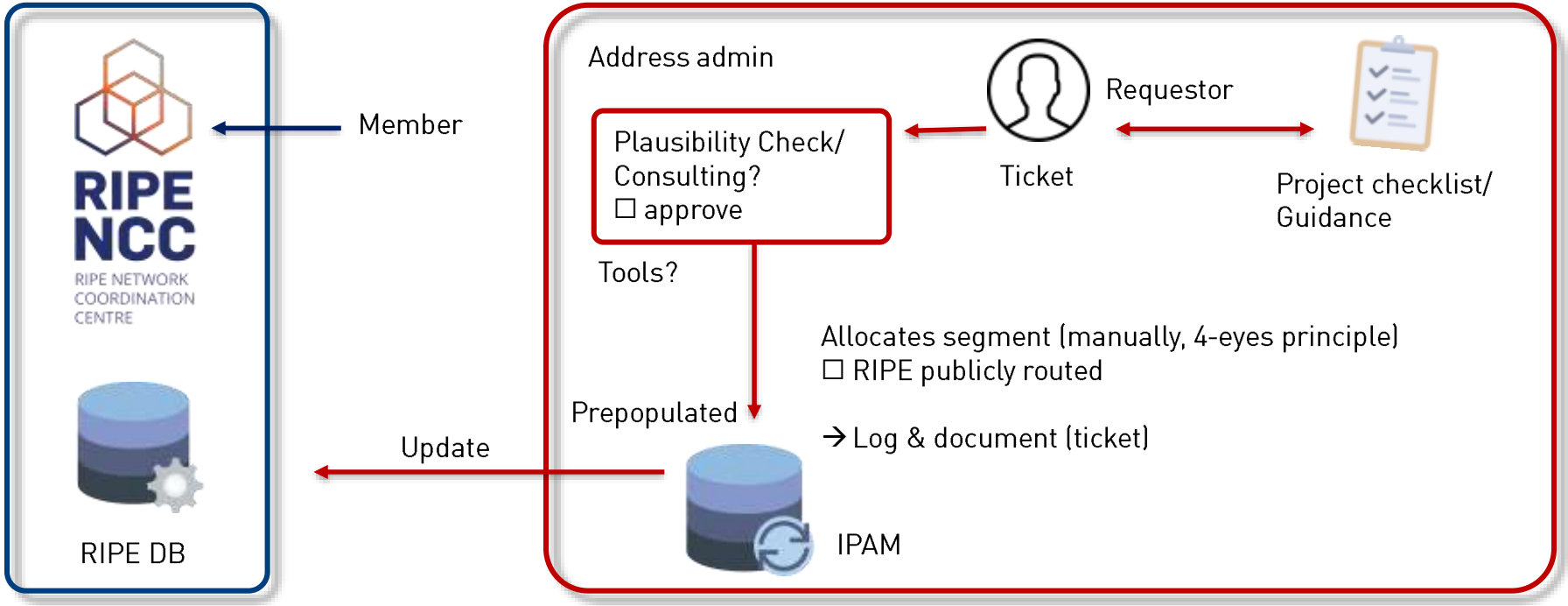
Fields of Ticket – Proposal



Workflow Open Items

- How to encourage / enforce documentation of prefix use?
  - First approach was to potentially tie it to a state gate within $PROJECT_FRAMEWORK
    - Not feasible → different approach needed
- Format of documentation?
  - How has $REQUESTOR documented the use?
    - Must be predefined for machine processing
- Technical feasibility of proposal to be discussed with $TICKET_SYSTEM_OPS

Process / Overview



ERNW
providing security.

Conclusions

- IPv6 is different from IPv4
  - Especially in reality ;-)

- Don't expect too much from an IPv6 address planning effort
  - Be liberal!

- Memento mori: renumbering hurts & costs!

- Take care of proper processes.
  - The earlier the better.

Thank You for Your Attention!

erey@ernw.de,
cwerny@ernw.de

@Enno_Insinuator
@bcp38_

www.ernw.de

www.insinuator.net

ERNW
providing security.

Image Sources

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