IPv6-Mostly Networks Deployment and Operations Considerations

draft-link-v6ops-6mops

Jen Linkova, RIPE88

Motivation

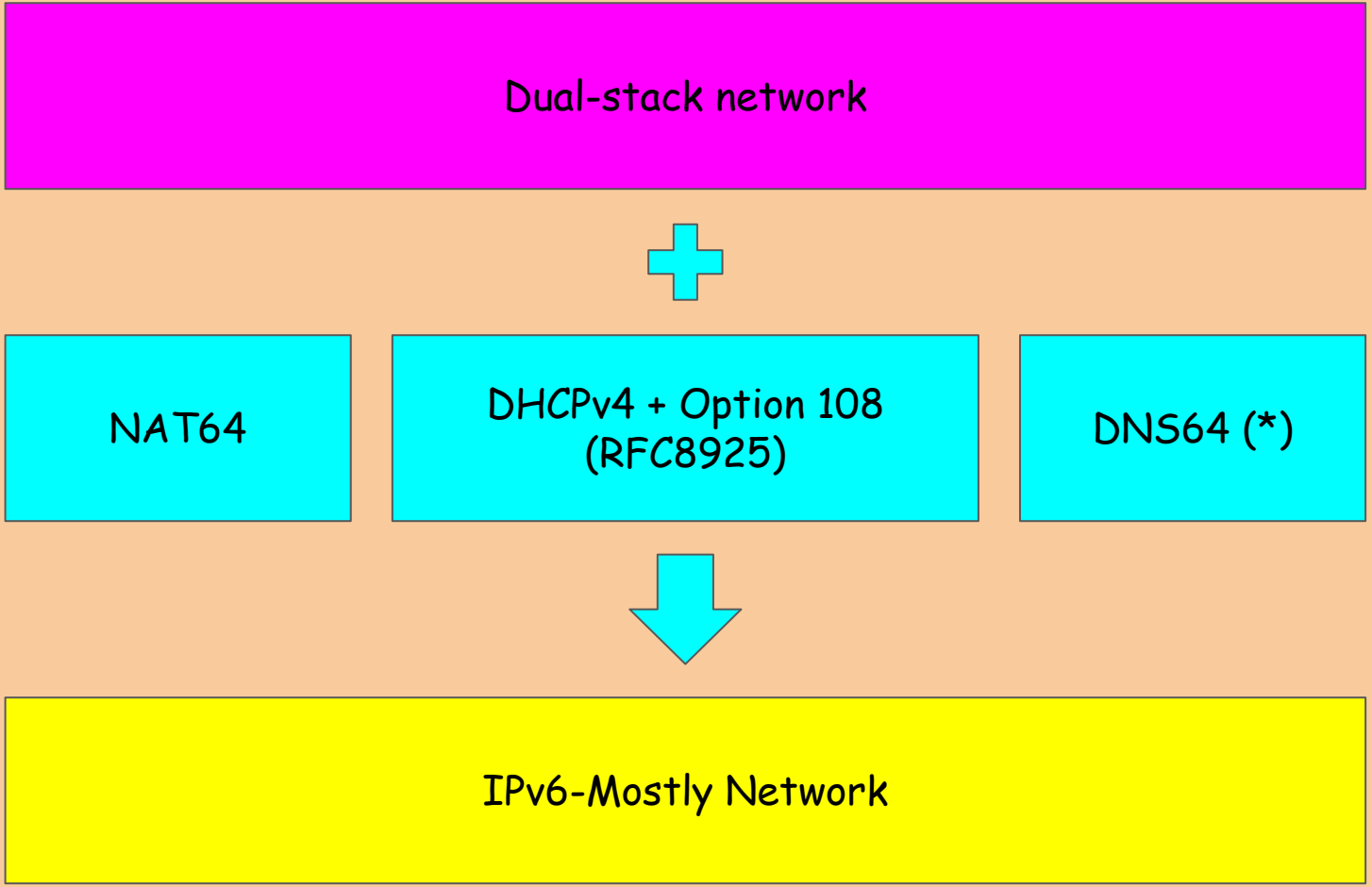
Follow-up on "Mission Possible" RIPE87 presentation

Documenting successful IPv6-Mostly deployments.

- *What*
- *Why*
- *How*
- *What we wish we knew*

IPv6-mostly network

A network that provides NAT64 (possibly with DNS64) service as well as IPv4 connectivity and allows the coexistence of IPv6-only, dual-stack, and IPv4-only hosts on the same segment. (RFC8925)


Dual-stack network
NAT64
DHCPv4 + Option 108
(RFC8925)
DNS64 (*)
IPv6-Mostly Network

Endpoint:

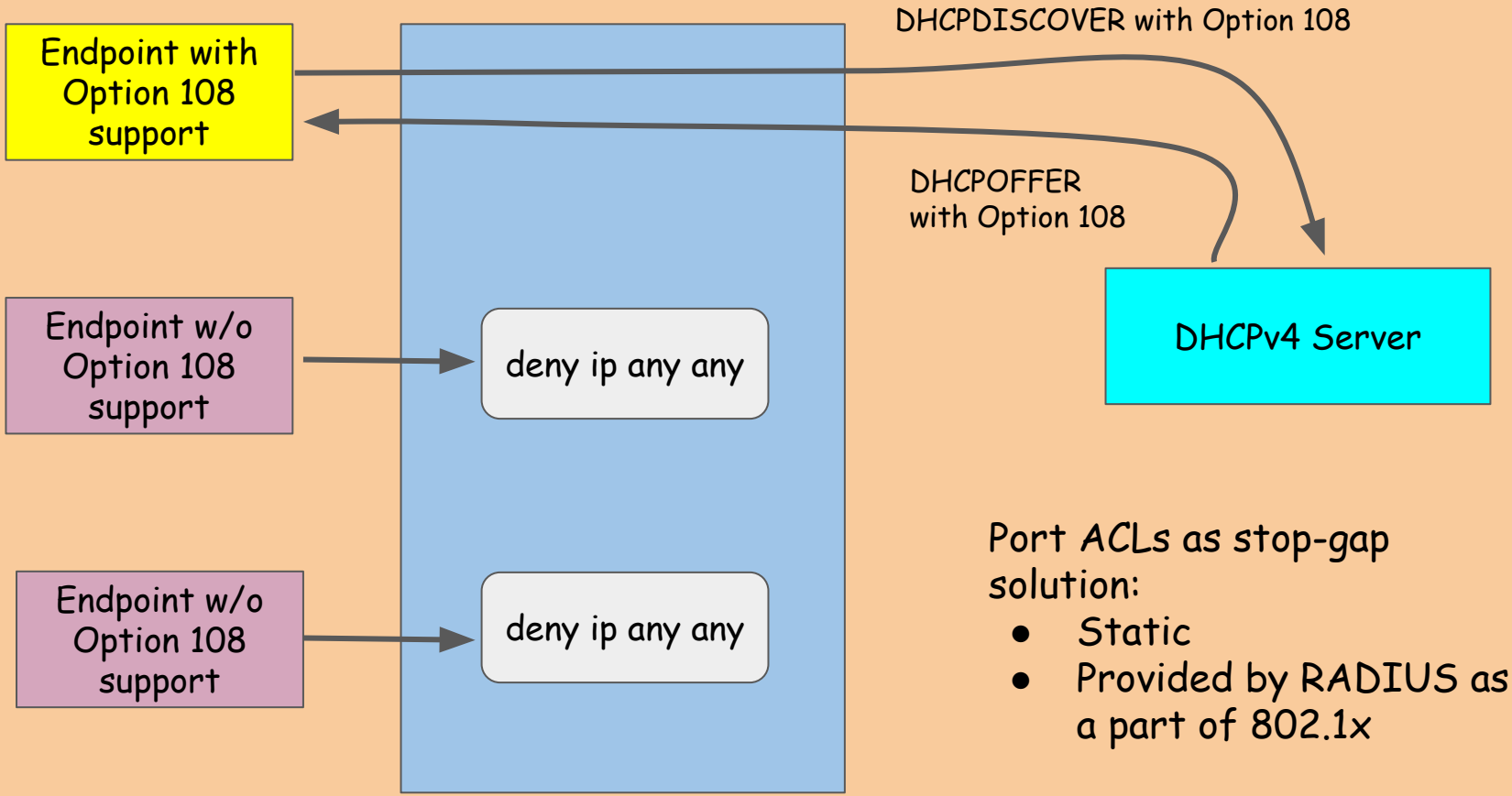
A device connected to a network and considered a host from the operator's perspective.

IPv6-Only Capable Endpoint:

An endpoint which does not require an IPv4 address and can operate on IPv6-only networks. E.g.

- *A device with 464xlat enabled*
- *A device verified in IPv6-only environment*

IPv6-Only Endpoints



Port ACLs as stop-gap solution:

- Static
- Provided by RADIUS as a part of 802.1x

Access to IPv4-only Destination: NAT64

Do not use Well-Known Prefix (64:ff9b::/96) if access to RFC1918 destinations is needed. Use Network-Specific Prefix.

Access to IPv4-only Destination: CLAT

CLAT is RECOMMENDED for IPv6-only hosts.

Do not enable Option 108 w/o CLAT….

….unless you have a reason to…

Discovering NAT64 Prefix

RECOMMENDED: include PREF64 into RAs

Faster (CLAT available immediately)

More secure (RA Guard is enabled, right?)

Works with custom resolvers

DNS vs DNS64

DNS64 is needed for:

- 464XLAT prefix discovery (RCF7050)
  - PREF64 in RAs should be used instead
- IPv6-only devices w/o CLAT (or applications which do not use CLAT)
  - Fundamentally insecure
  - Breaks DNSSEC
  - Might not work if hosts/applications use custom resolvers
    - RFC8880 updates RFC7050 but….
  - Some applications do not work anyway

DNS vs DNS64: Recommendations

- PREF64 in RAs is widely supported
- Long-term goal: avoid DNS64
- Is it feasible now? Let's find out!

Try ripemtg WiFi right now!

Benefits Compared to Dual-Stack

- *Reduced IPv4 Consumption*
- *Simplified Operations*
- *Reduced Dependency on DHCPv4*

Benefits Compared to IPv6-Only (+fallback)

- *Scalability*
- *Simplicity*
- *Optimized IPv4 Consumption*
- *Problem Visibility*
- *Incremental Migration*

Incremental Rollout Recommendations

- *Per-Device and Per-Subnet Incremental Rollout*
  - *Devices sending 108 unconditionally: per-subnet*
  - *If option 108 can be turned on/off: per-device*
- *Rollback speed: controlled by Option 108 value*
  - *Start with minimal (300 secs), increase later*
- *Keep a "secret" dual-stack network as a fallback*

Address Assignment Policy

- All existing CLAT implementation require SLAAC

Security Policies

- Permit Extension Headers
  - Fragment Header
    - DNS, RADIUS, NTP
  - ESP Header
    - VPN
    - WiFi Calling

“What to Expect”/Typical Issues Section

- Not about implementation bugs!

All IPv6 Issues Become Highly Visible

- Brace yourself!

Devices with Disabled/Dysfunctional IPv6

- Audit and fix managed devices
- Clear message for BYOD

Endpoints Performing Network Extension

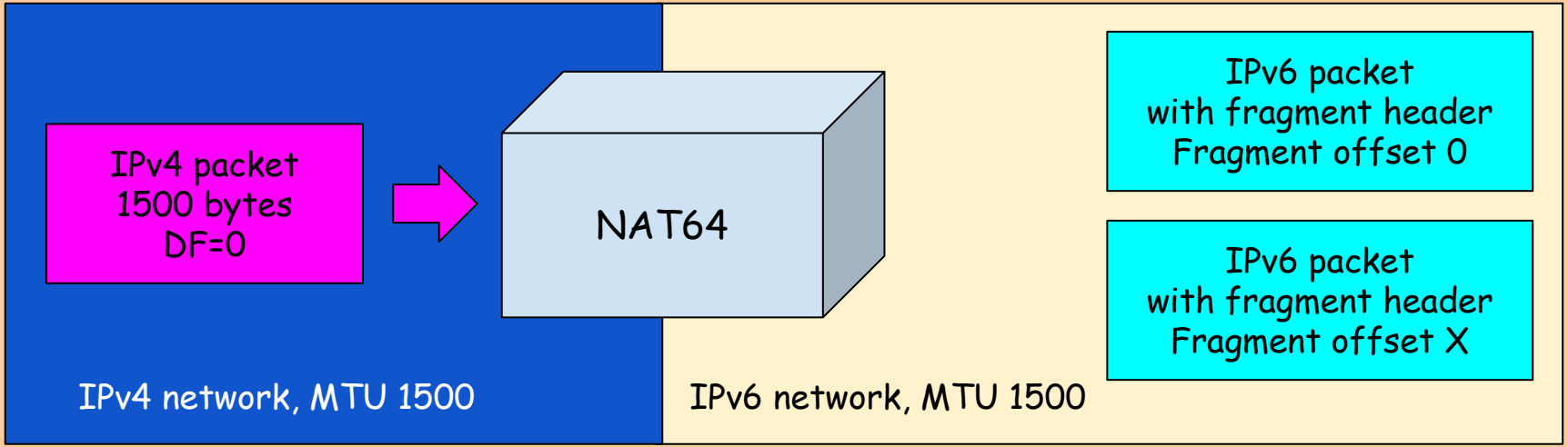
- IPv4: NAT44
- IPv6:
  - Delegate prefix per device
  - CLAT on endpoint
  - ND proxy (scalability issues!)

Multiple Addresses per Device

- Ensure APs and switches allows sufficient number of addresses per device

Custom/Manual DNS Config on Endpoints

- Scenarios:
  - Users configure resolvers manually
  - Local recursive resolver on the endpoint
  - Application-specific resolvers
- Advertize PREF64 in RA
- Request RFC8880 support from endpoints

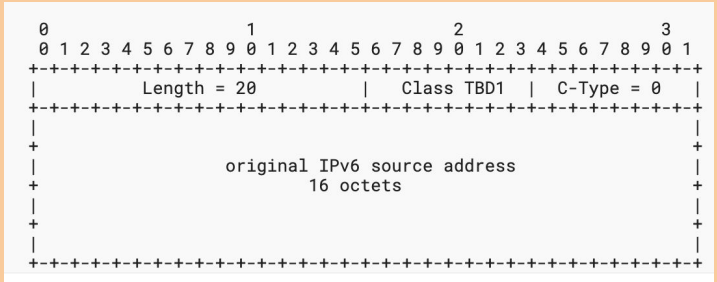


Fragmentation

- Maximize MTU on IPv6-only side
- Configure NAT64 correctly
- If using anycast (RADIUS) and ECMP: use flow labels for balancing

CLAT Not Representing IPv6 Addresses

- *ICMPv6 Errors (traceroute, PMTU)*
  - *how to represent IPv6 addresses?*
  - *Ignore?*
  - *Use reserved addresses +TTL*
- *Proposed solution:*
  - *If ICMPv6 src is not from NAT64 prefix: add IPv6 Original Source Extension*
  - *draft-equinox-intarea-icmpext-xlat-source*



Next Steps

- Solicit feedback
  - Providing specific recommendations
  - …while still covering various use cases
- More experience on deploying w/o DNS64
- Publish!