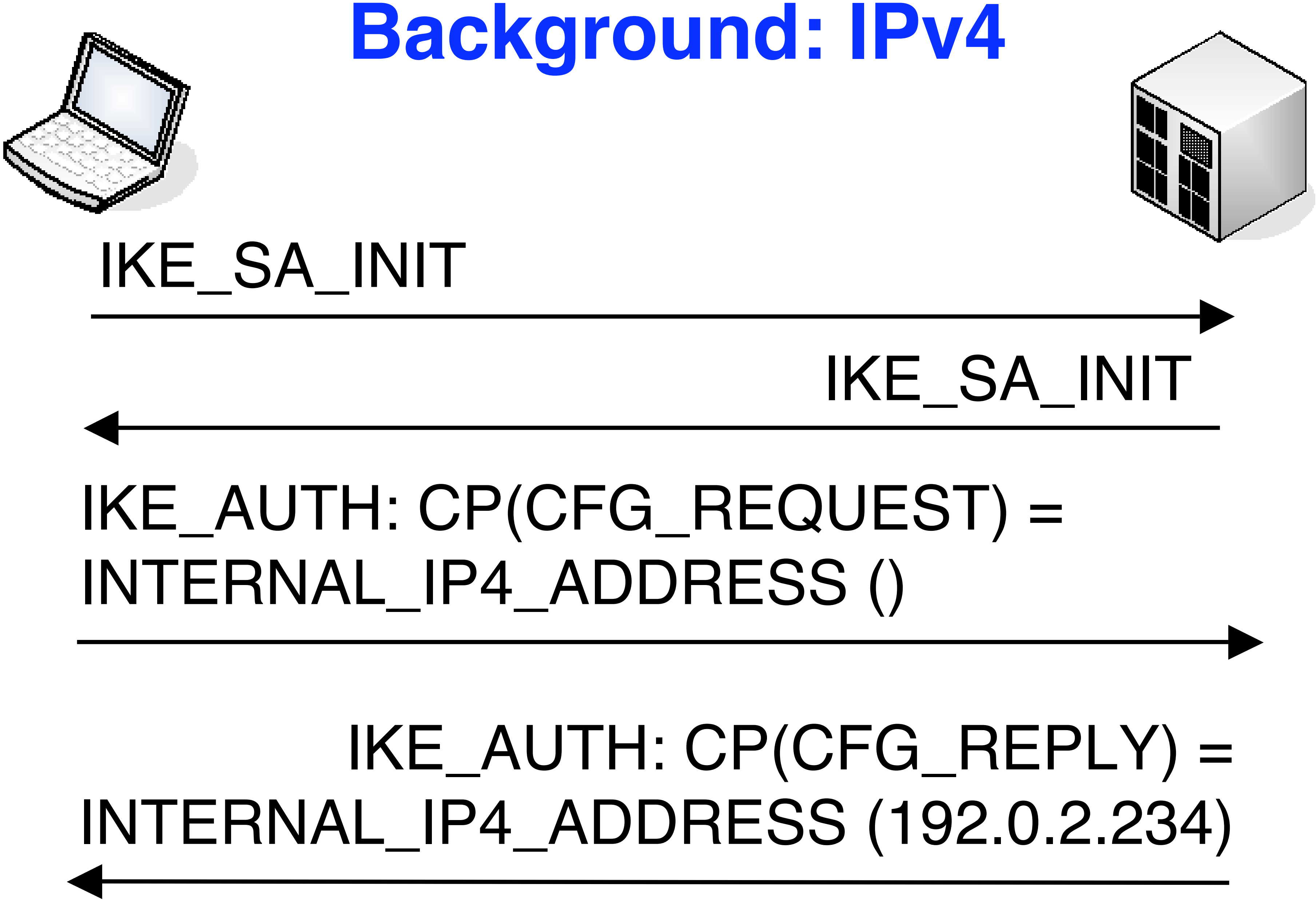
IPv6 Configuration in IKEv2

draft-eronen-ipsec-ikev2-ipv6-config-01

pasi.eronen@nokia.com

Background: IPv4



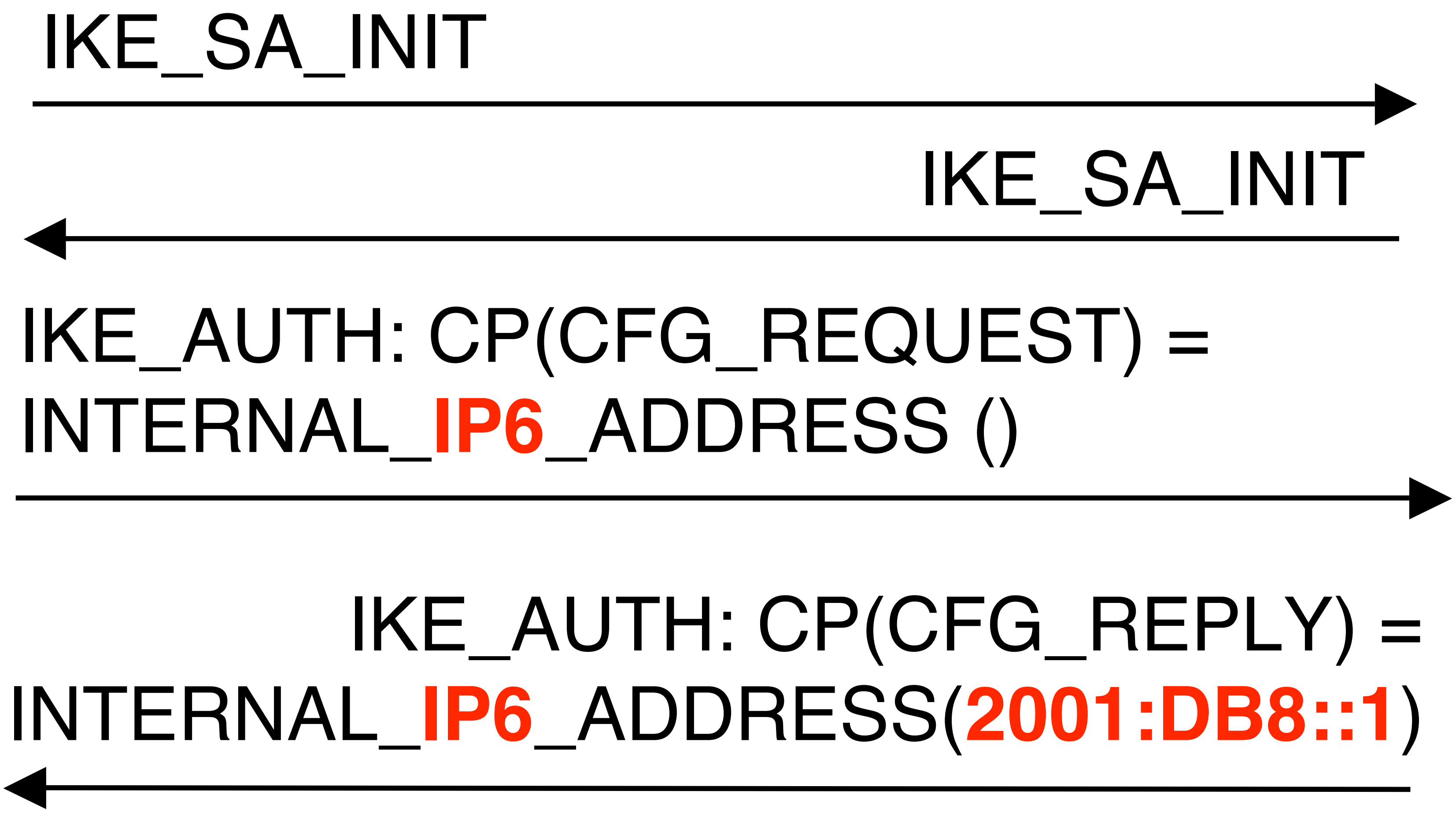
IKE_SA_INIT

IKE_SA_INIT

IKE_AUTH: CP(CFG_REQUEST) =
INTERNAL_IP4_ADDRESS ()

IKE_AUTH: CP(CFG_REPLY) =
INTERNAL_IP4_ADDRESS (192.0.2.234)

IPv6 version



IKE_SA_INIT

IKE_SA_INIT

IKE_AUTH: CP(CFG_REQUEST) =
INTERNAL_**IP6**_ADDRESS ()

IKE_AUTH: CP(CFG_REPLY) =
INTERNAL_**IP6**_ADDRESS(**2001:DB8::1**)

Problems 1/2

- No multiple prefixes (renumbering, host-based site multihoming, …)
- No link-local addresses (violates MUST in RFC 4291)
- Additional references:
  - Why this was bad idea for 3GPP: RFC 3314
  - Why multilink subnets are complex: RFC 4903

Problems 2/2

- Interface ID selection (CGAs, HBAs)
  - Possible, but gets very complicated (see draft for details)
- Sharing VPN access to other devices
  - (without NAT!)

Proposal

- Point-to-point link model
- Allocate whole /64 prefix(es)
  - Client can use any interface ID

How to configure addresses?

- Draft version –00: RS/RA
  - + “Just a virtual interface for IPv6”
  - – Doesn’t follow IPsec way of doing access control (SPD traffic selectors)
  - – May not work with existing stacks nicely (100,000 virtual interfaces on gateway?)
  - – Totally different from IPv4 case

How to configure addresses?

- Draft version –01: IKEv2 Cfg Payloads
  - + More compatible with IPsec access control
  - + Address knowledge in IKE (which does RADIUS/etc. backend interaction anyway)
  - + IPv4 and IPv6 done in similar way
  - – IPsec specific (note: recommends DHCPv6 Information-Request/Reply for everything else than address)

How to configure addresses?

- “RFC 3456” like: first create SA for RS/RA or DHCPv6, then do RS/RA or DHCPv6, then create real SAs and delete old ones
  - More roundtrips
  - Not necessarily simple to implement
  - RFC 3456 not successful
- Something else?

Next steps

- Please read and comment the draft