draft-maino-gpe-vpn

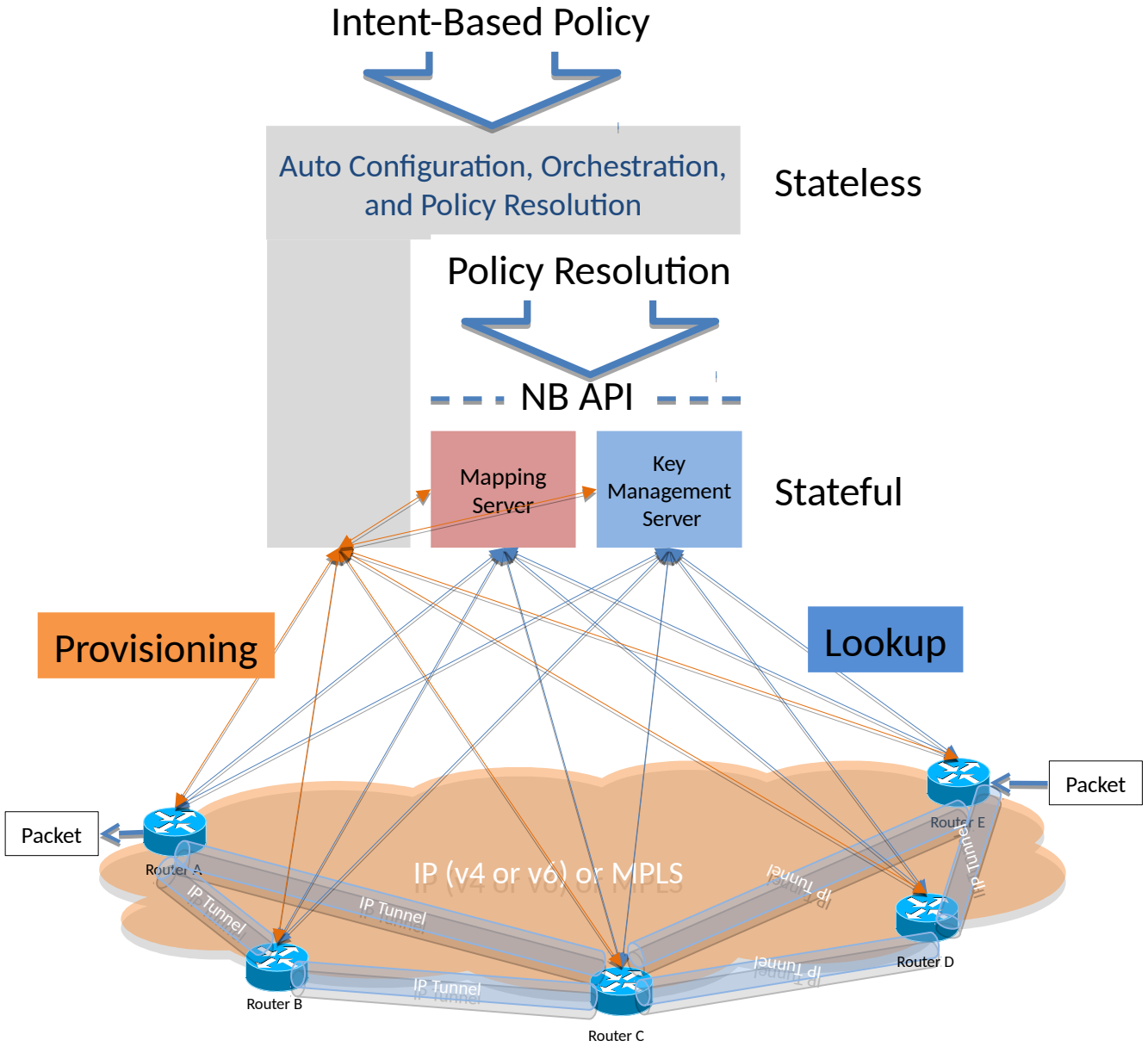
F. Maino, V. Ermagan, J. Evans, H. Miclea

IETF 95 – April 2016

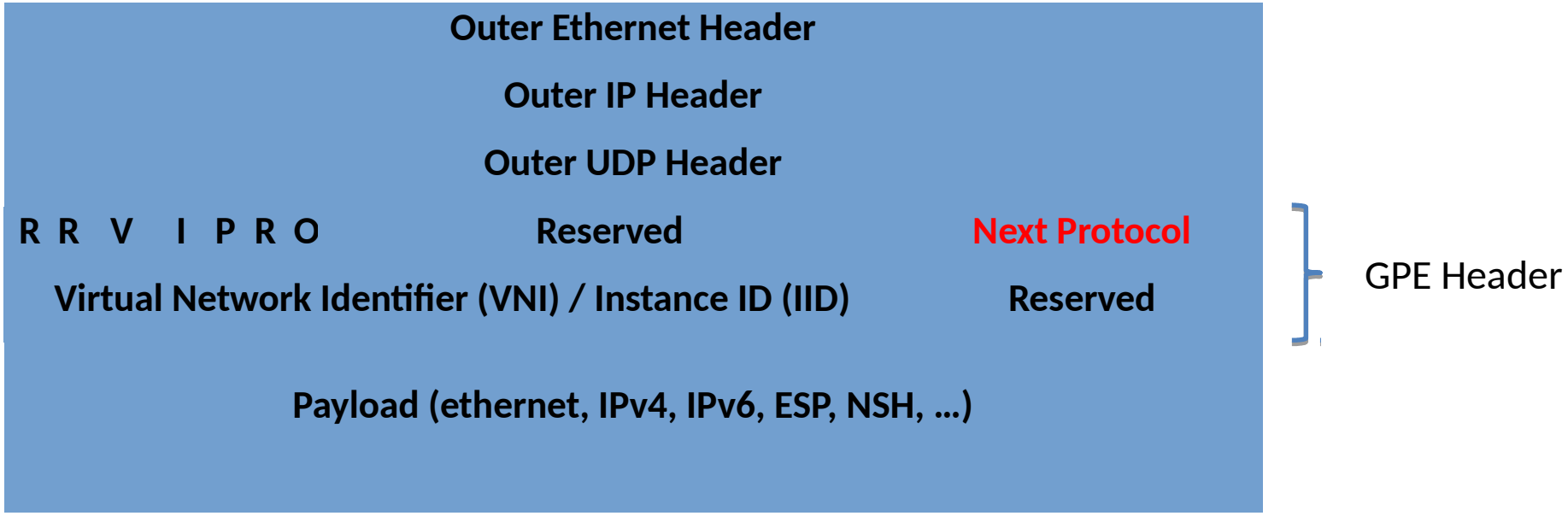
GPE-VPN

- LISP-based architecture for SD-WAN
  - programmable **LISP control plane**
  - **VXLAN-GPE data plane** with optional:
    - **ESP** encryption
    - **NSH**-based support for Service Function Chaining
- Mapping System is dynamically programmed via **NorthBound API**
  - **Policy rendering** via dynamic **mapping manipualtion**

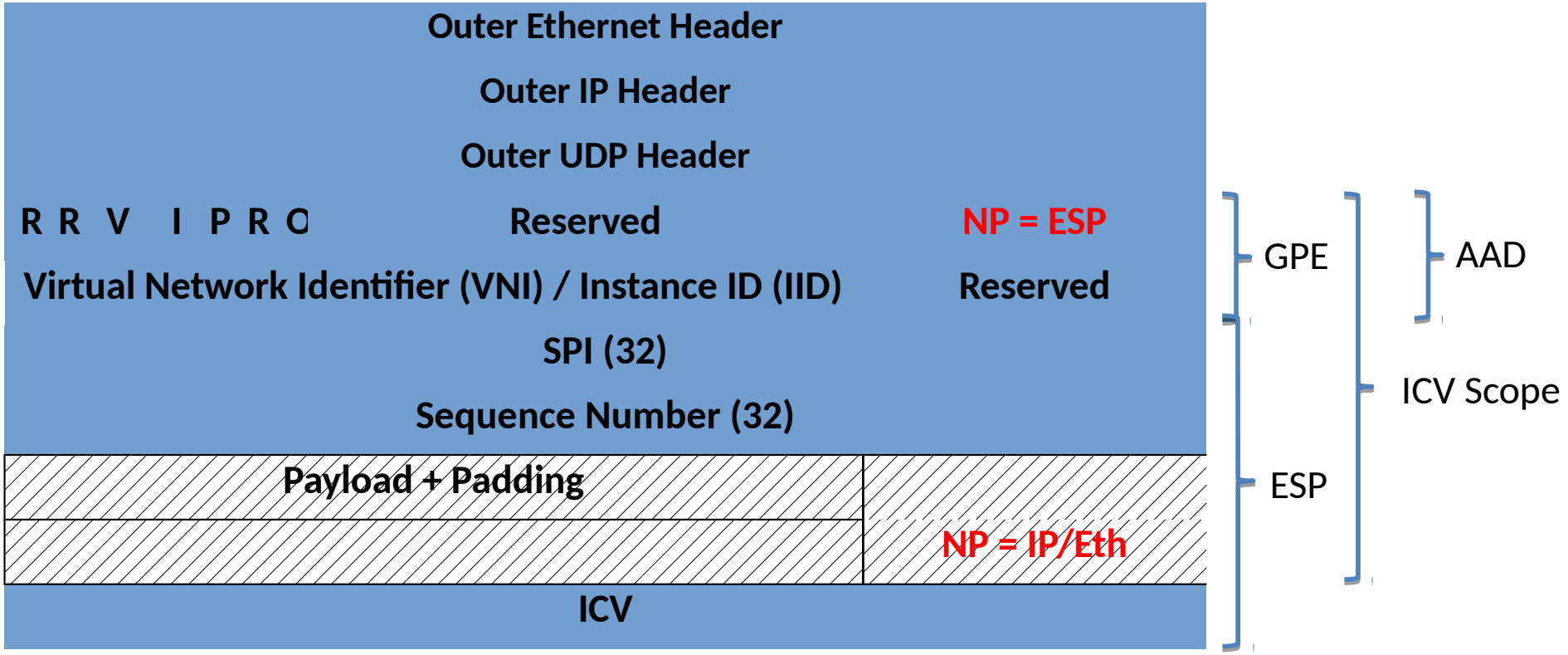
Overall Architecture



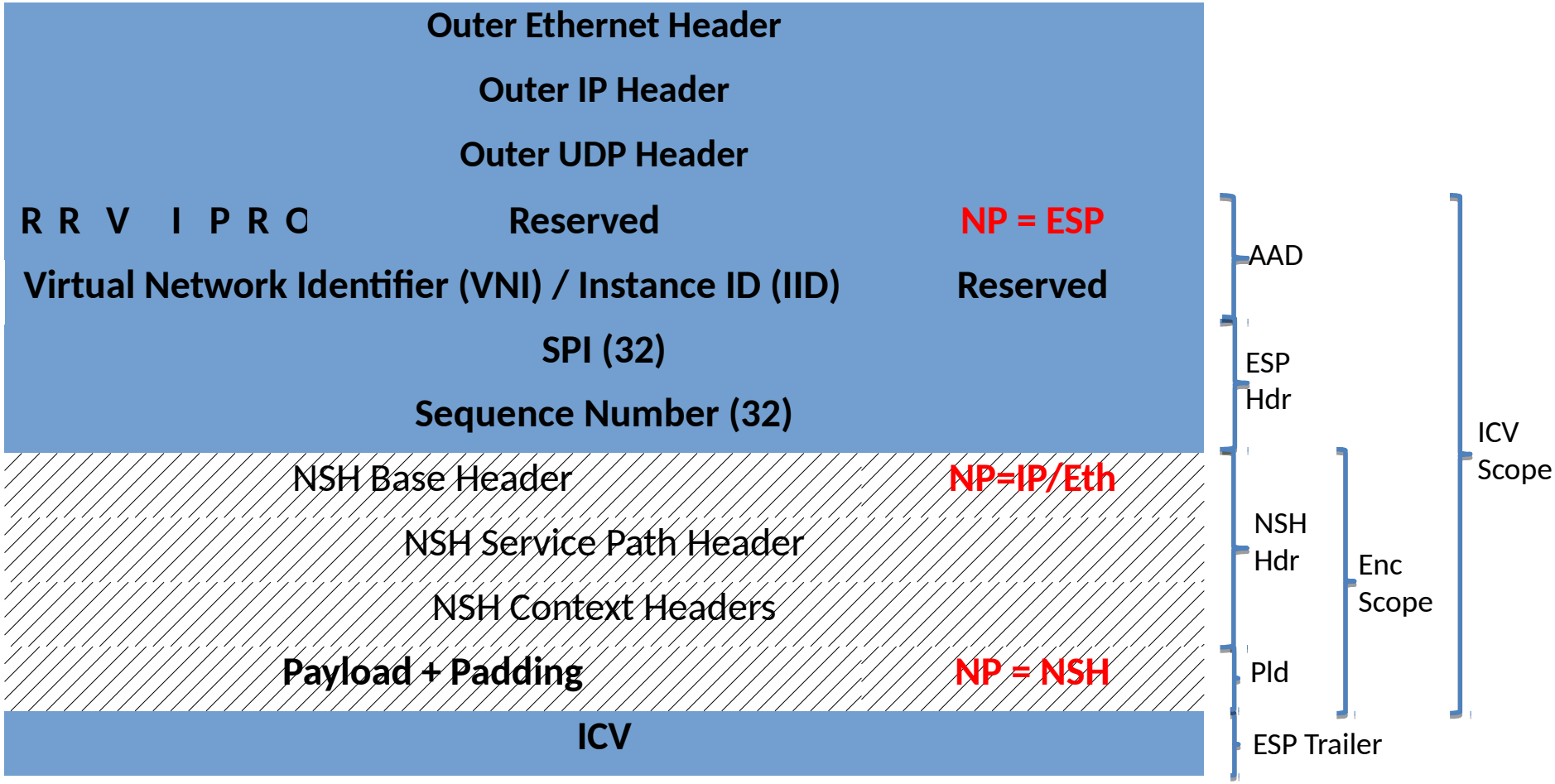
Data Plane: GPE Encapsulated Frame



Data Plane: GPE with AEAD (ESP-GCM)



Data Plane: GPE+NSH with ESP+GCM



Mapping Types

- GPE-VPN uses various mapping types to provide finer-grain policy control, and to support different policies
  - **Per-destination mapping**
    - EID -> RLOC
  - **FlowMapping**
    - <sEID, dEID, sPort, dPort, Protocol> -> RLOC
    - draft-rodrigueznatal-lisp-multi-tuple-eids
  - **Generic Mapping**
    - e.g. <NSH SPI, Index> -> RLOC
    - draft-ermagan-lisp-nsh
    - draft-rodrigueznatal-lisp-ms-smr

Dynamic Policy Rendering

- Dynamic mapping manipulation (via NB API) enables GPE-VPN generic policy rendering
  - **Forwarding and In-bound load balancing**
  - **Overlay Re-encapsulation** (via RTR)
    - Virtual topologies
    - Hierarchical VPNs
  - **Group-based Access Control**
  - **Support for Service Function Chaining**

Key Management Services

- SA provisioning is a **trade-off** between
  - **time** needed to set up the SA on demand
  - overall **security** afforded
- SA provisioning can be done with different mechanisms
  - Use **IKEv2** to negotiate pairwise SAs
  - Use Group Domain of Interpretation (GDOI) **for group key** management
  - Leverage **LISP map-request/reply** to accelerate on demand provisioning of SA
    - e.g. ietf-lisp-crypto

Q&A

Thanks!