

Send/CGA for OMNI Links

IETF 122 6MAN Session – March 21, 2025

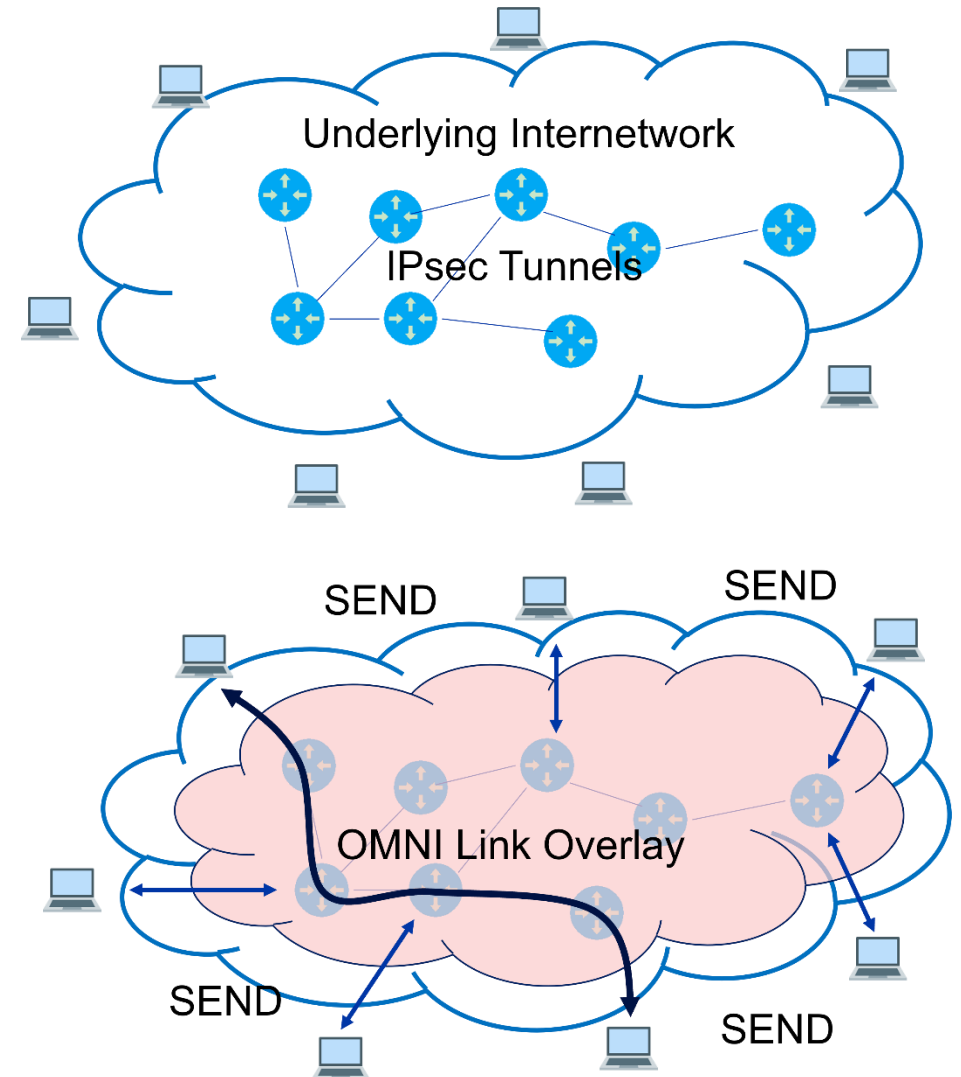
<https://datatracker.ietf.org/doc/draft-templin-6man-omni3>

<https://datatracker.ietf.org/doc/draft-templin-6man-aero3>

Fred L. Templin
(fltemplin@acm.org)

Problem Statement and Solution Summary

- Gateways and Proxy/Servers form interior topology joined by IPsec tunnels over underlying Internetworks
- OMNI link as adaptation layer overlay configured over interior topology
- IPv6 Neighbor Discovery (ND) messages transit OMNI link in a single hop, but may traverse many underlay segments
- Clients and Proxy/Servers need way to authenticate IPv6 ND messages at edges: SEcure Neighbor Discovery (SEND)



Next Steps

- **SEND (RFC3971) options useful for IPv6 ND message authentication**
 - Authentication, Certificate, Timestamp, Nonce, etc.
- **SEND cites SHA1 as authentication default, but SHA1 vulnerable**
 - Alternatives: SHA-224, SHA-256, SHA-384, SHA-512, TBD
- **SEND cites Cryptographically Generated Addresses (CGA – RFC3972) as addressing default, but CGAs incompatible with remote attestation**
 - SEND permits use of IPv6 address types other than CGAs
 - Alternative certifiable IPv6 address type with cryptographic elements needed
 - New or existing candidate address types (e.g., RFC9374, etc.) considered
- **SEND defines mechanisms; not operational practices. Issues such as PKI are operational concerns; not protocol concerns**
- **Request to working group: Reinstate SEND in IPv6 Node Requirements (draft-ietf-6man-rfc8504-bis)**