draft-ietf-bess-secure-00.txt

A. Sajassi (Cisco), A. Banerjee (Cisco), S. Thoria (Cisco), D. Carrel (Cisco), B. Weis (Cisco)

IETF 103, November 2018

Bangkok

Problem Statement

- EVPN has become prevalent solution in DC, SP, and Enterprise networks
- For DC and Enterprise applications, specially for DC Interconnect (DCI) and Enterprise connectivity over WAN, customers want secure connectivity with EVPN

Requirements

1. Protection of Tenant's Layer-2 and Layer-3 data & control traffic by IPsec
2. Protection of Tenant's unicast and multicast data traffic by IPsec
3. Using of BGP P2MP signaling for setting up P2P IPsec SAs – reducing # of message exchanges from O(N^2) to O(N)
4. Supporting following levels of granularity for IPsec SAs
5. Supporting single policy and DH group as well as multiple policies and DH groups

Requirements (2)

6. Supporting following levels of granularity of IPsec SAs
   a) Per PE: A single IPsec tunnel between a pair of PEs to be used for all tenants' traffic supported by the pair of PEs.
   b) Per tenant: A single IPsec tunnel per tenant per pair of PEs.
   c) Per subnet: A single IPsec tunnel per subnet (e.g., per VLAN) of a tenant on a pair of PEs.
   d) Per IP address: A single IPsec tunnel per pair of IP addresses of a tenant on a pair of PEs.
   e) Per MAC address: A single IPsec tunnel per pair of MAC addresses of a tenant on a pair of PEs

Solution Overview

- Secure control channel between each PE and the RR (e.g., using existing scheme such as IKv2)
  - Setup BGP session over this secure tunnel
- Use this secured BGP channel for P2MP signaling to establish P2P IPsec SAs
  - No need for P2P signaling to establish P2P SA
  - Reducing # of msg exchanges from O(N^2) to O(N)
  - Each PE advertises to other PEs the info needed for establishing P2P SAs

Solution Overview (2)

- When a PE device first comes up and wants to setup an IPsec SA between itself and each of the interested remote PEs, it generates a DH pair for each of its intended IPsec SA using an algorithm defined in the IKEv2 Diffie-Hellman Group Transform IDs [IKEv2-IANA].
- The originating PE distributes DH public value along with a nonce (using IPsec Tunnel TLV in Tunnel Encapsulation Attribute) to other remote PEs via the RR.
- Each receiving PE uses this DH public number and the corresponding nonce in creation of IPsec SA pair to the originating PE

Encapsulations

- Two types of IPSec encapsulations for our applications
  1. IPsec encap in transport mode without outer UDP header
  2. IPsec encap in transport mode with outer UDP header per [RFC3948]
     - Needed to NAT traversal or per flow LB using UDP header

VxLAN Encap with ESP

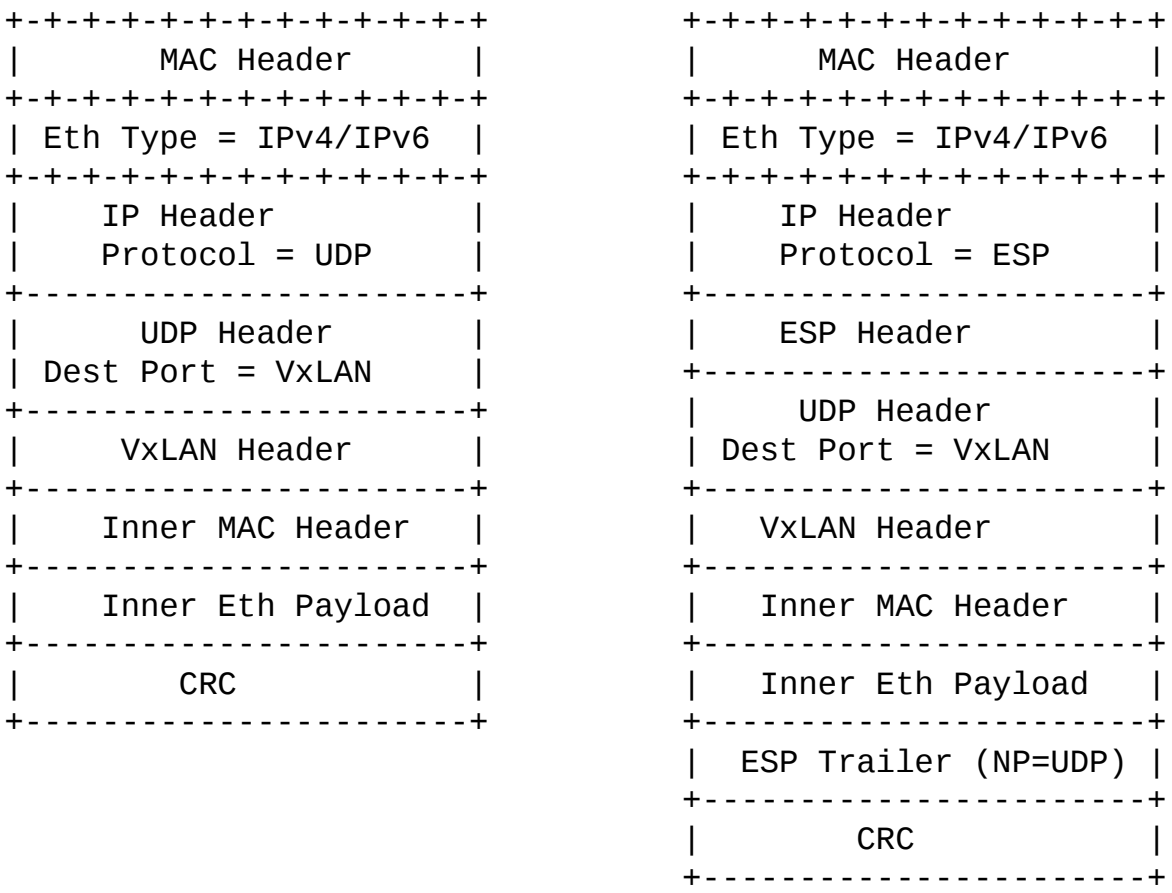

Figure 3: VxLAN Encapsulation within ESP

VxLAN Encap with ESP within UDP

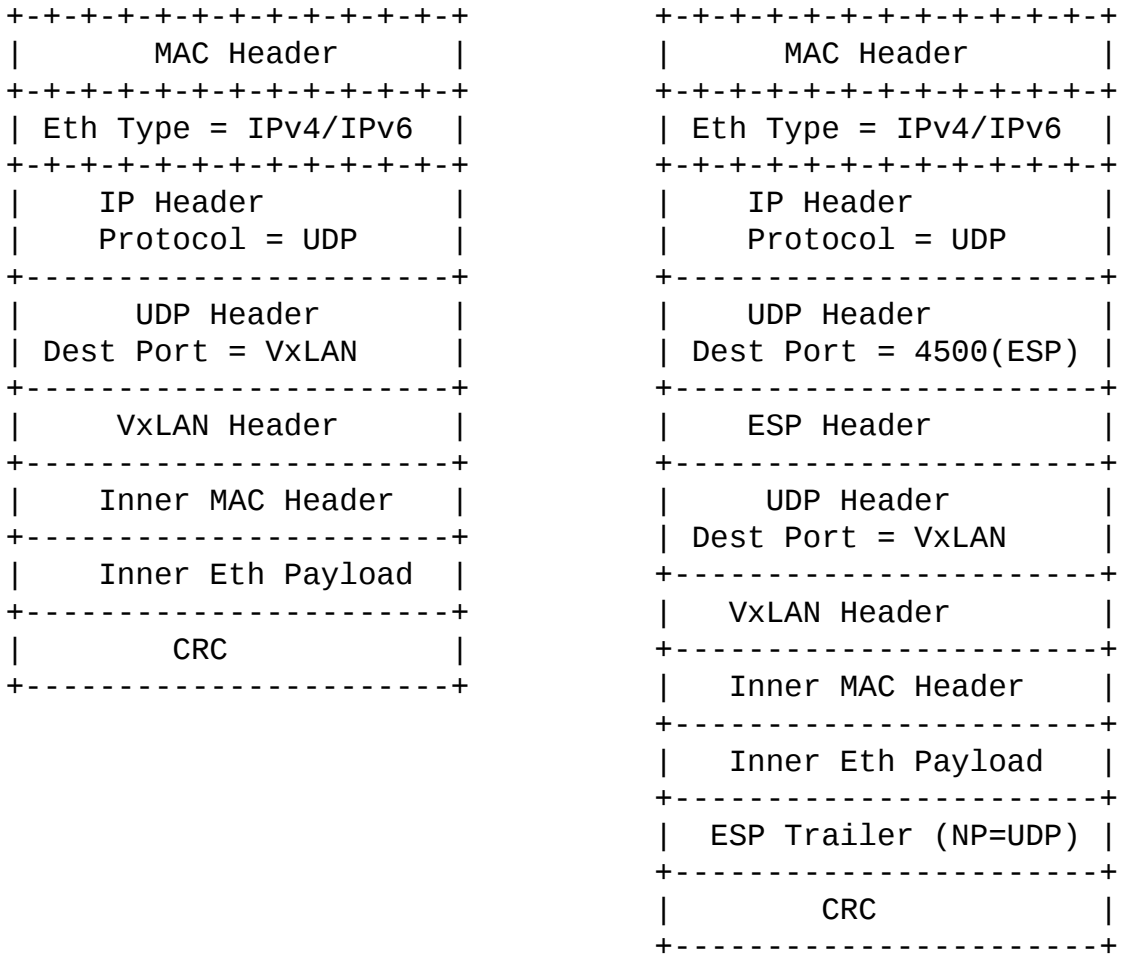

Figure 4: VxLAN Encapsulation within ESP Within UDP

Functionality	EVPN	IP-VPN	MVPN	VPLS
per PE	IPv4/v6 route	IPv4/v6 route	IPv4/v6 rte	IPv4/v6
per tenant	IMET (or new)	lpbk (or new)	I-PMSI	N/A
per subnet	IMET	N/A	N/A	VPLS AD
per IP	EVPN RT2/RT5	VPN IP rt	*,G or S,G	N/A
per MAC	EVPN RT2	N/A	N/A	N/A

Min set

Minimum Set

```
ID, [N(INITIAL_CONTACT),] KE, Ni; where

     ID payload is defined in section 3.5 of [RFC7296]
     N (Notify) Payload in section 3.10 of [RFC7296]
     KE (Key Exchange) payload in section 3.4 of [RFC7296]
     Ni (Nonce) payload in section 3.9 of [RFC7296]

KE payload contains the DH public number and also identifies which DH
```

Single Policy

```
ID, [N(INITIAL_CONTACT),SA, KE, Ni

     SA (Security Association) payload in section 3.3 of [RFC7296]
```

Policy List and DH group List

```
ID, [N(INITIAL_CONTACT), [SA], [KE], [Ni]

     [SA] list of IPsec policies (i.e., list of SA payloads)
     [KE] list of KE payloads
```

ESP Notify Sub-TLV

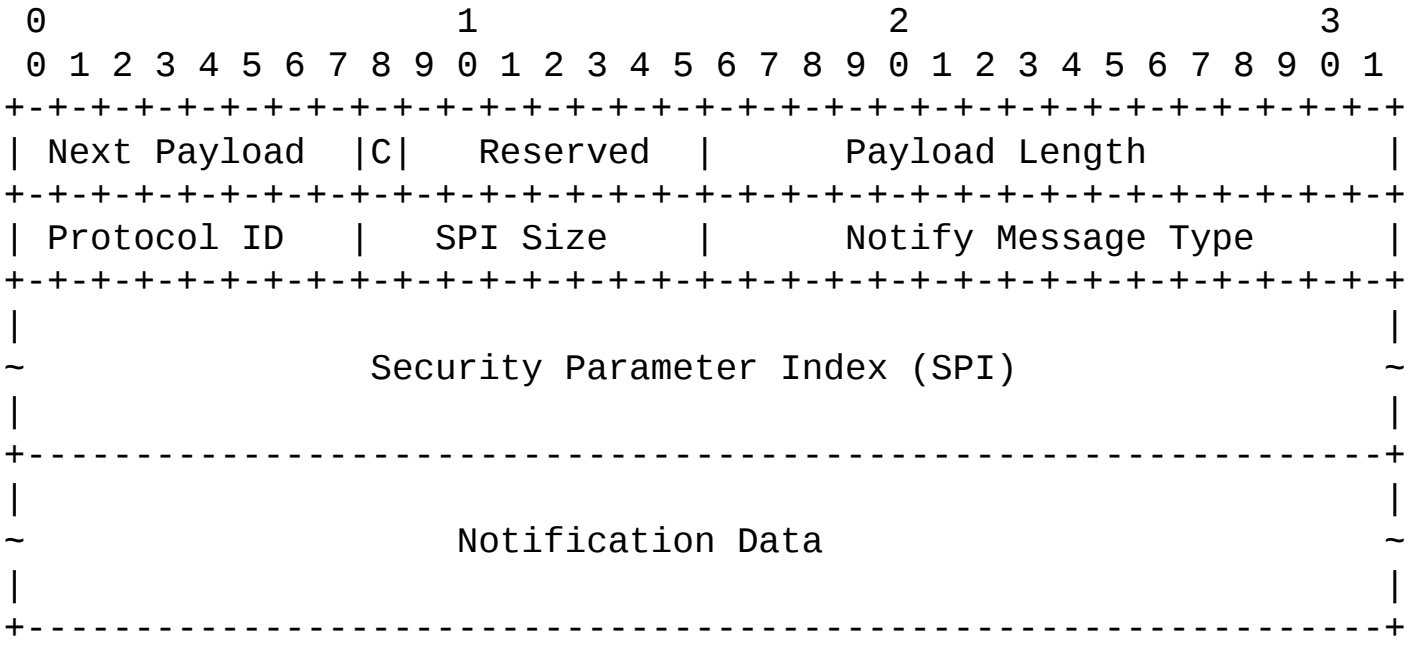

Figure 5: Notify Payload Format

ESP Key Exchange Sub-TLV

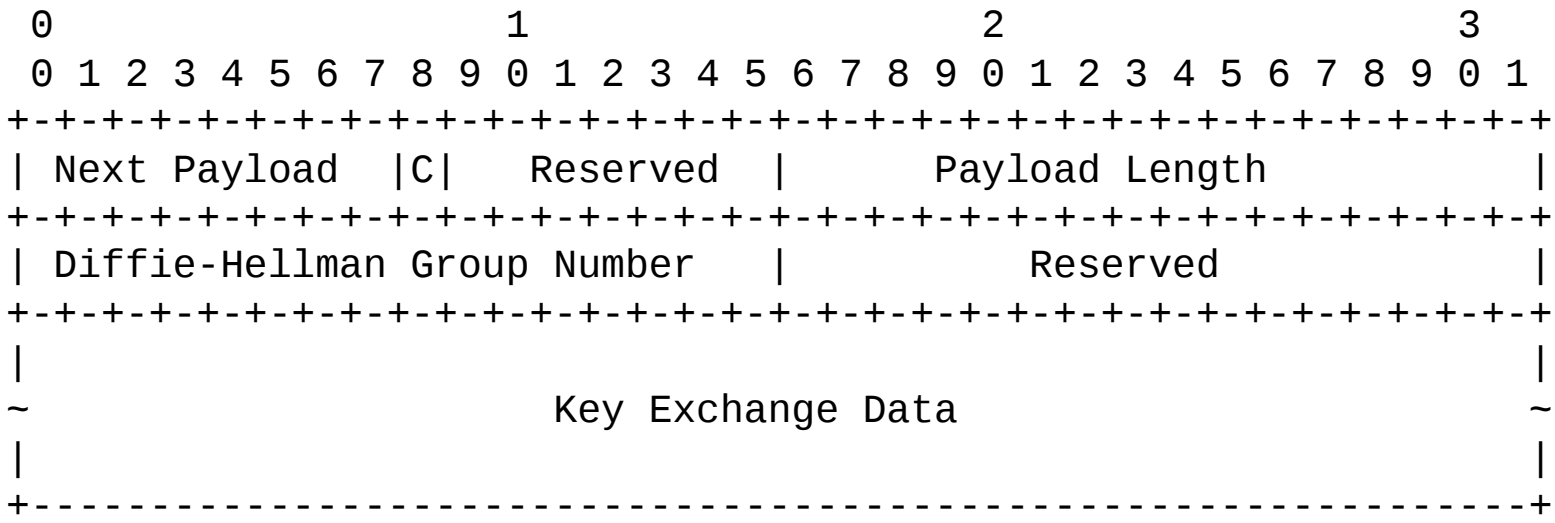

Figure 6: Key Exchange Payload Format

ESP Nonce Sub-TLV

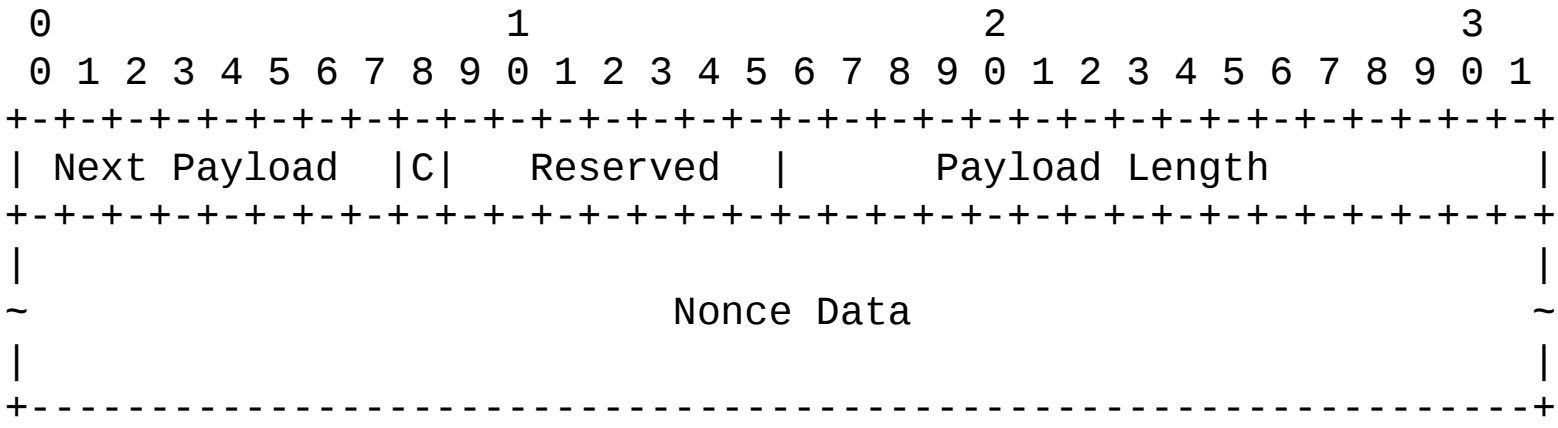

Figure 7: Nonce Payload Format

ESP Proposal Sub-TLV

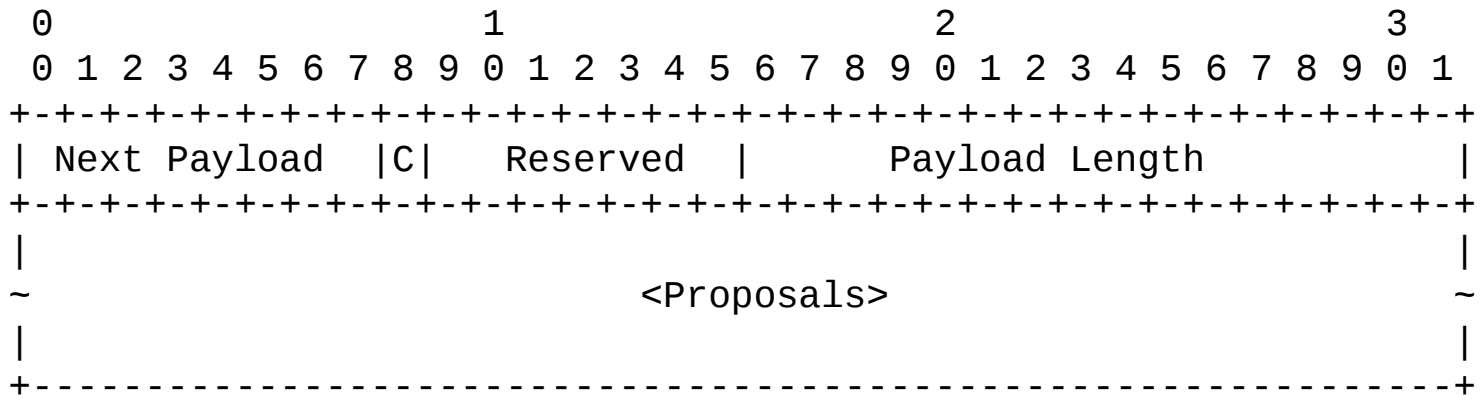

Figure 8: Security Association Payload

ESP Proposal Variables

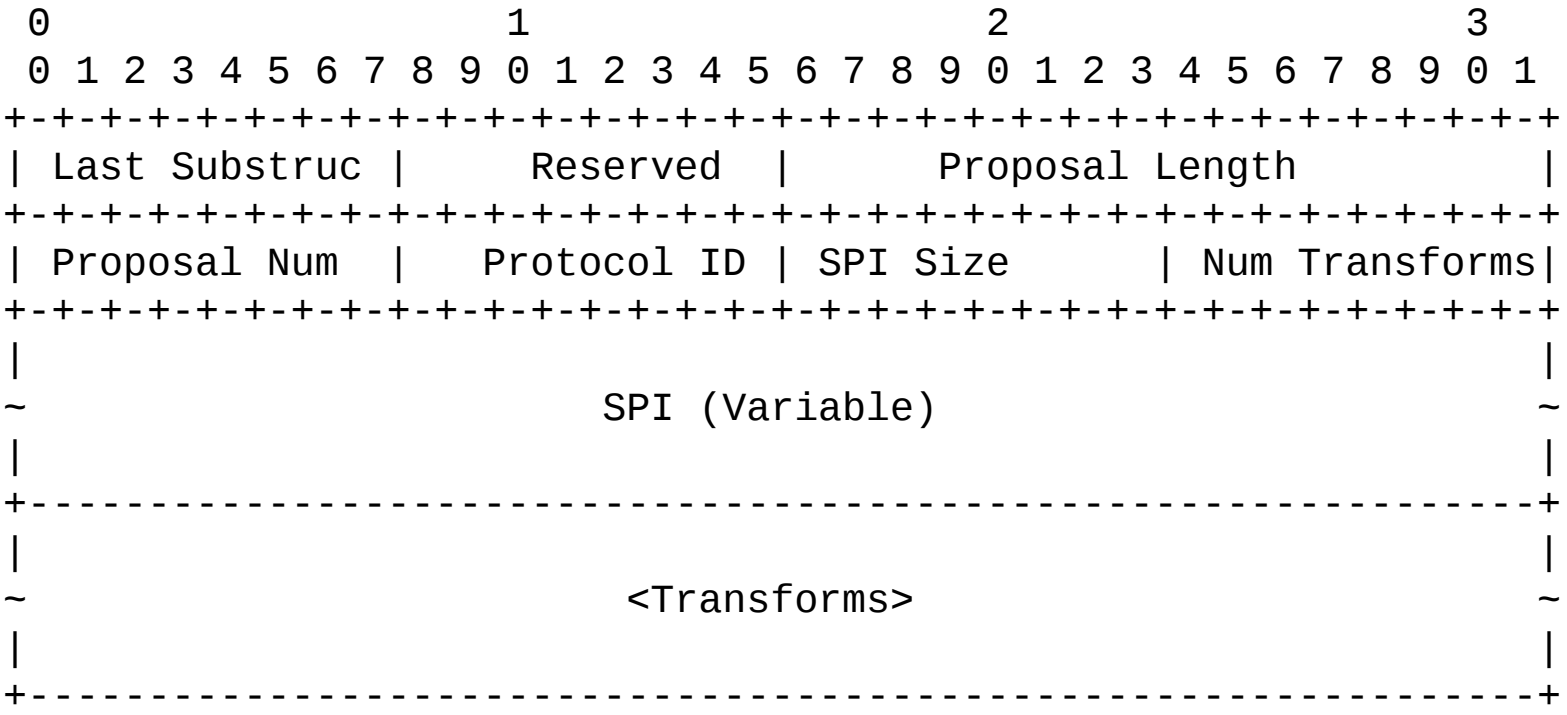

Figure 9: Proposal Substructure

Next Step

- Solicit input
- Request for WG adoption @ next IETF

THANK YOU!