

# draft-sajassi-bess-secure-evpn-05.txt

A. Sajassi (Cisco), A. Banerjee (Cisco), S.  
Thoria (Cisco), D. Carrel (Cisco), B. Weis  
(Indep), J. Drake (Juniper)

IETF 112, Nov 2021

Online

# History

---

- Rev05 was published on Oct 2020
  - merged of draft-carrel-ipsecme-controller-ike-01 into this draft because of synergy between the two drafts
- Rev03 was published on July 2020
- Rev02 was published on July 2019
- Rev01 was published on March 2019 and presented at IETF 104 in Prague
- Rev00 was published on October 2018 and presented at IETF 103 in Bangkok

# Changes relative to rev03

## (Added the following sections)

---

- 4. SA and Key Management . . . . .
- 4.1. Generating Initial IPsec SAs . . . . .
- 4.2. Rekey of IPsec SAs . . . . .
- 4.2.1. Single IPsec Device Rekey . . . . .
- 4.2.2. Multiple IPsec Device Rekey . . . . .
- 5. IPsec Database Generation . . . . .
- 5.1. The Security Policy Database (SPD) . . . . .
- 5.2. Security Association Database (SAD) . . . . .
- 5.2.1. Generating Keying Material for IPsec SAs
- 5.2.1.1. g<sup>ir</sup> . . . . .
- 5.2.1.2. Nonces . . . . .
- 5.2.1.3. SPIs . . . . .
- 5.2.1.4. IPsec key generation . . . . .
- 5.3. Peer Authorization Database (PAD) . . . . .

# Changes relative to rev03 – Cont.

## (Corrected figure 5 by reverting the older version)

---

### VxLAN Encapsulation within ESP

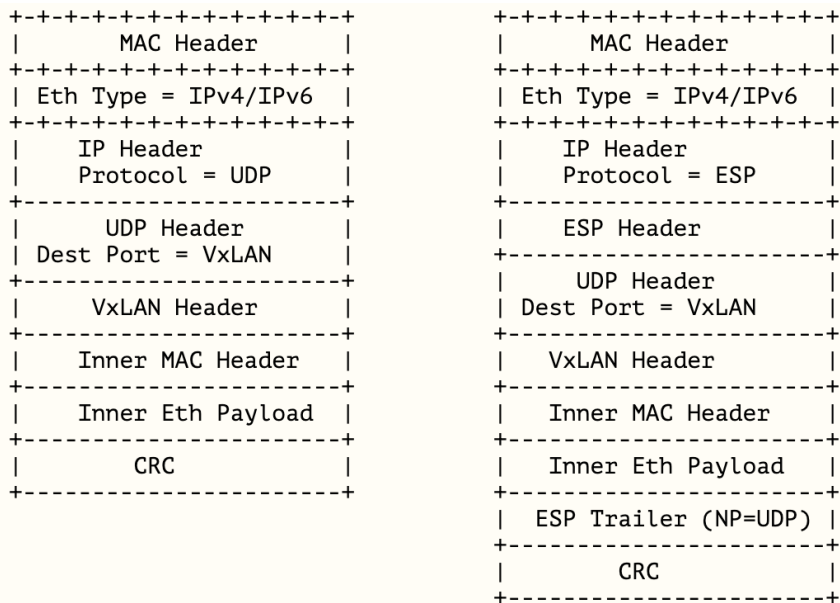


Figure 4

### VxLAN Encapsulation within ESP Within UDP

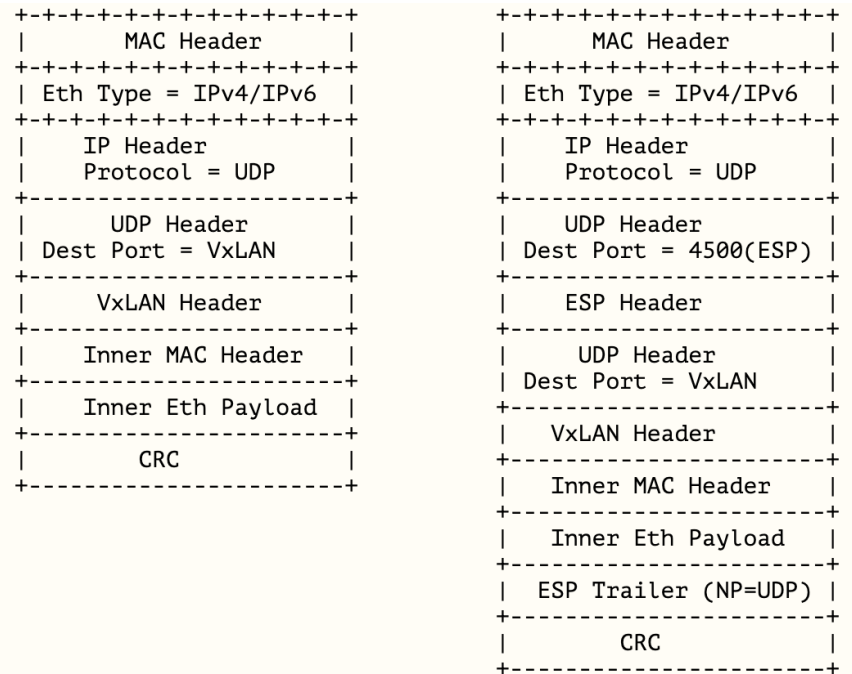


Figure 5

# Next Step

---

- This draft has been around for a few years, and it has been stable
- It is ready for WG adoption call

---

**THANK YOU!**