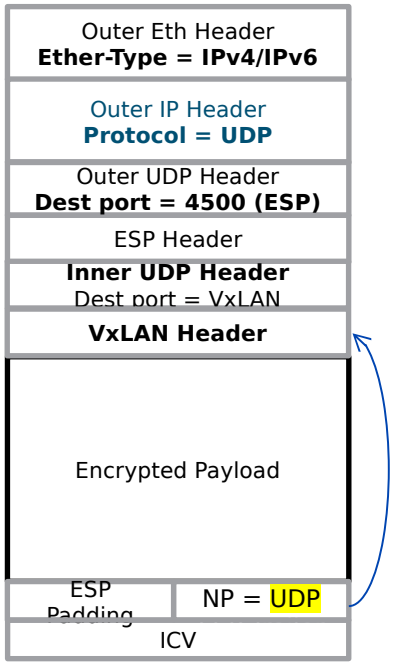
Cut-Through mode for draft-ietf-bess-secure-evpn.txt

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

IETF 121, November 2024

Dublin, Ireland

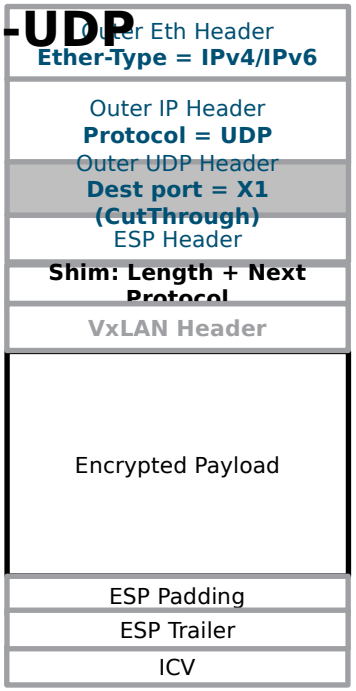
Issue



- **When a PE operates in cut-through mode, it needs to decrypt one part of the packet at a time as it receives the packet bitstream.**
- **Therefore, the PE cannot wait till it receives the entire packet to look at the ESP trailer for packet type and length**

Proposal:
Introduce a new Encap for Cut-Through mode

VxLAN-in-ESP-in-UDP



- **Introduce a new UDP port to indicate a header that consists of an ESP header + 8-byte shim header**
- **Shim header is not encrypted**
- **There is still a 2-byte ESP trailer for backward compatibility**
- **1st nible of shim header should be set to 0100 as default**

8-byte shim header

4-bit field=0x4	**Reserved = 0**	**16-bit Length**
16-bit Encap Type		**reserved = 0xFFFF**

Encap for Cut-Through – Cont.

- For BGP signaling, the Tunnel Type of Tunnel Encapsulation TLV is set to ESP-Cut-Through and the Tunnel Type of Encapsulation Extended Community is set to NVO encap type (e.g., VxLAN)
- This implies that the host packets are first encapsulated using NVO encapsulation type and then it is further encrypted and encapsulated using ESP-Cut-Through with Transport mode.
- Encrypted packet format will use new UDP dest port ID to indicate ESP + shim header
- The reserved fields are defined in the figure for backward compatibility with existing PHY

Next Step

- Solicit further input from WG