Enhanced ESP
IETF 121

draft-klassert-ipsecme-eesp

Steffen Klassert, Antony Antony, Chris Hopps

Why a new security protocol?

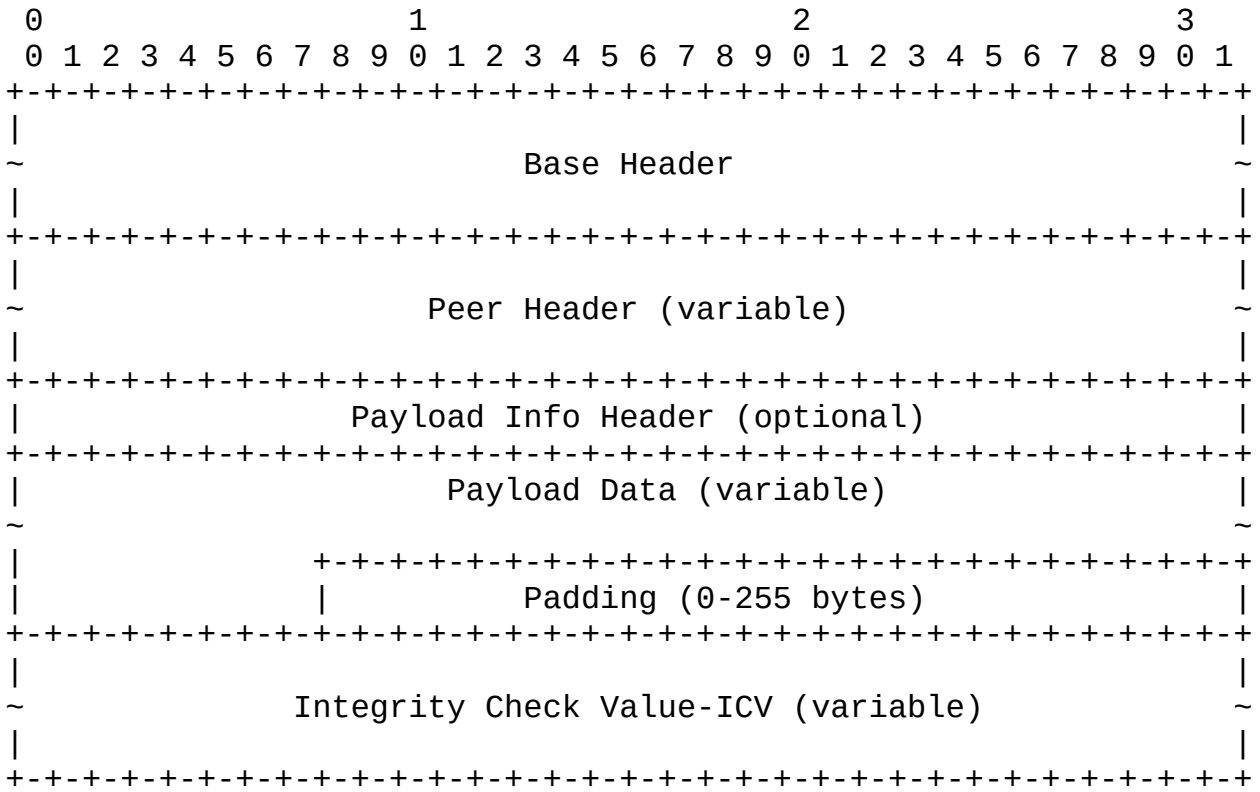
- ESP lacks flexibility and extensibility for modern needs
  - No version number in packet
  - New features must be negotiated
  - Not transparent to the network
- Lot of proposals to extend ESP
  - Suffer from ESP limitations
- Need to be HW offload friendly: Google PSP (for Data Center traffic)
  - Similar to ESP but more flexible
  - No standard!

Takeaways from IETF 120 WESPv2 presentation

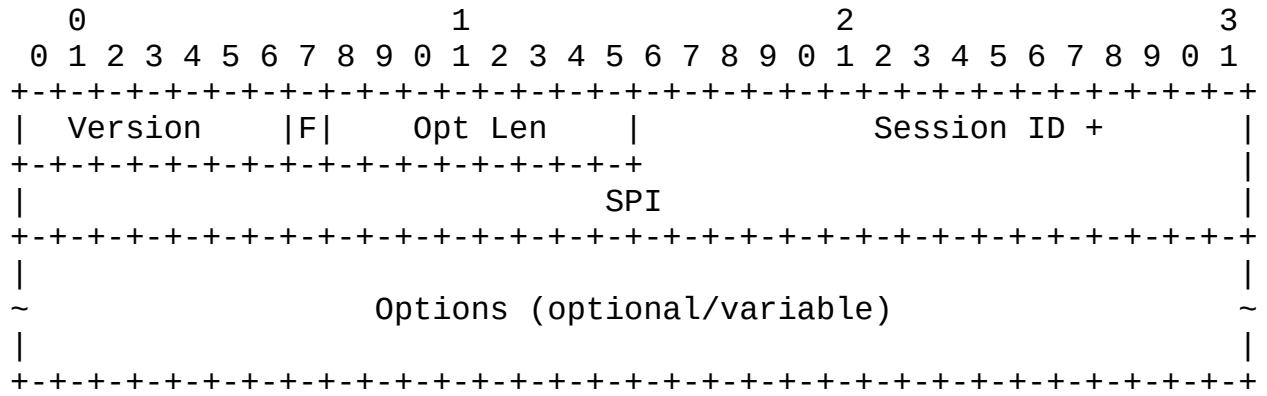
- Go big, define a new ESP (new IANA protocol number)!
- WESPv2 is just because we don’t want to go for a new protocol number
- New ESP can fix all existing problems with one document
- New ESP is the most flexible solution
- On new ESP, CryptOffset is not in the base header (compared to WESPv2)

EESP Packet Format

Toplevel Packet Format

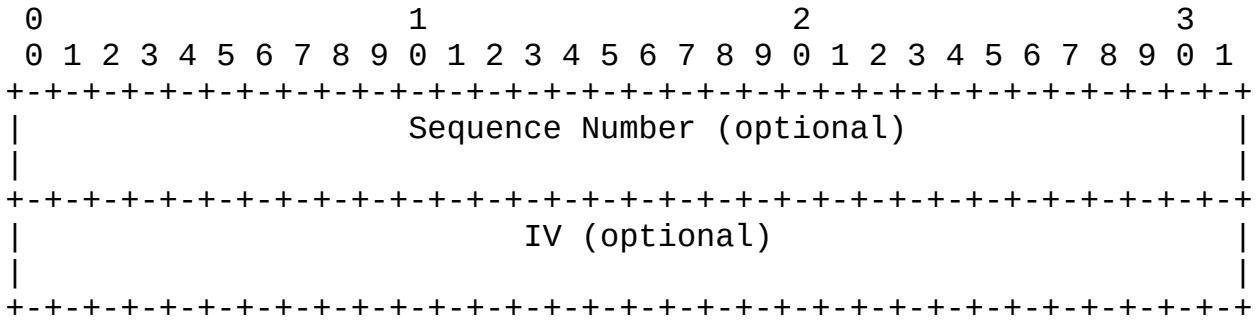


EESP Base Header with Options



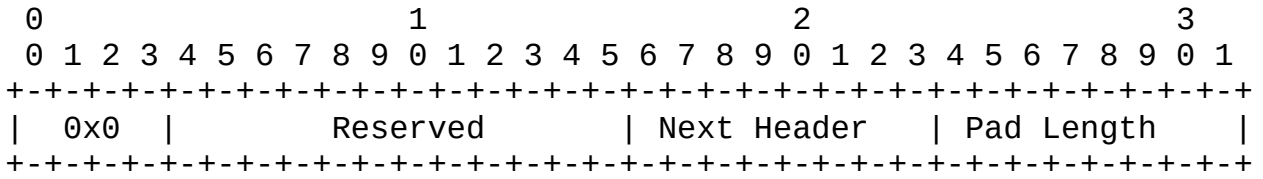
- Version (7 bits)
- F: Packet Format
  - 0 – Full Format
  - 1 – Optimized Format
- Opt Len: Overall Options length
- Session ID (16 bits)
- SPI: same as in ESP
- Options: TLV encoded

EESP Peer Header



- Sequence Number: 64 bit, if present
- IV: Depends on algorithm type.
    - AEAD may use SN as IV.

Full Packet Format - Payload Info Header



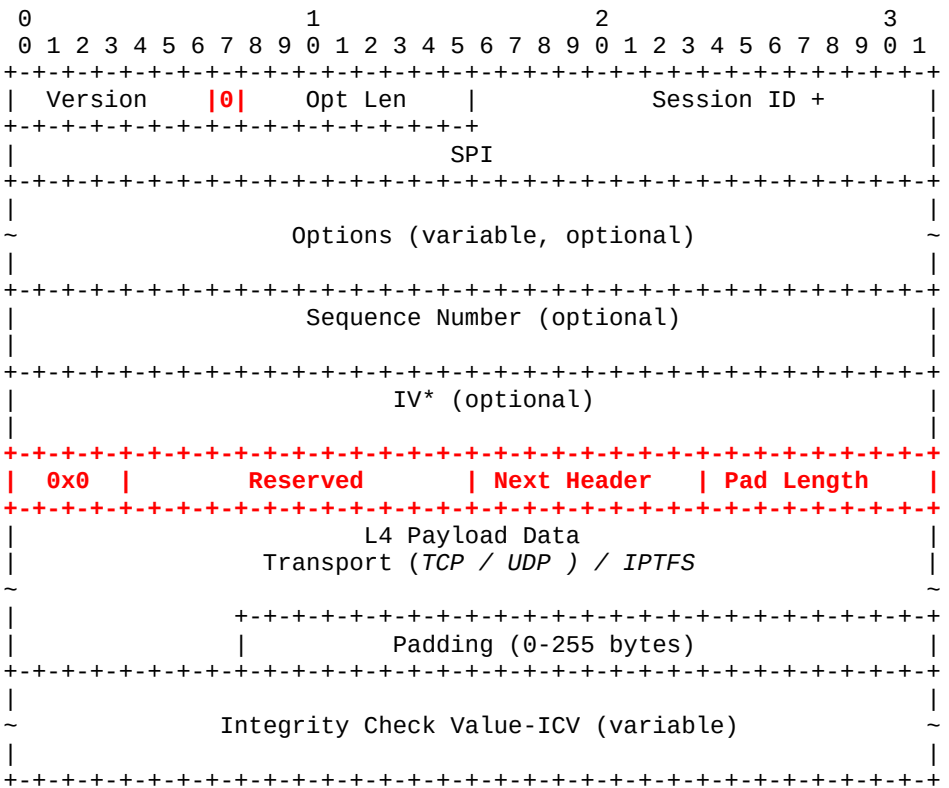
- **Required for Transport and IPTFS**
- Can’t derive “Next Header” from outer IP (set to ESP protocol)
- Can’t determine “Pad Length” from outer IP length
  - IP Length (Total) == IP+EESP+Payload+Pad+ICV

Optimized Packet Format

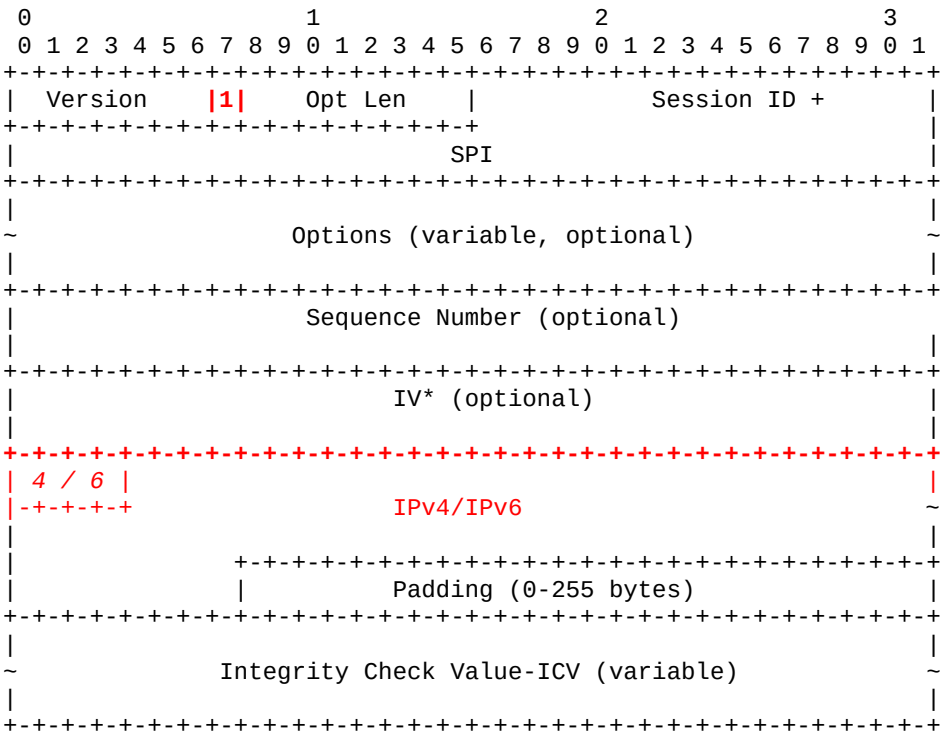
- **Payload Info Header Not Needed for IPv4/IPv6 Tunnel Mode**
- First Nibble defines payload (0x4 or 0x6 IP version value)
- “Pad Length” computed using outer length and inner length fields
- “Next Header” not needed in tunnel mode

Format Comparison

Full Packet Format

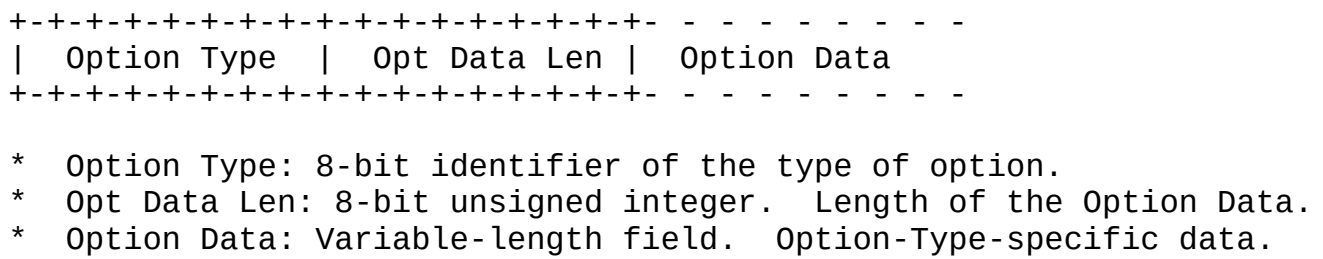


Optimized Packet Format



EESP Options

EESP Options

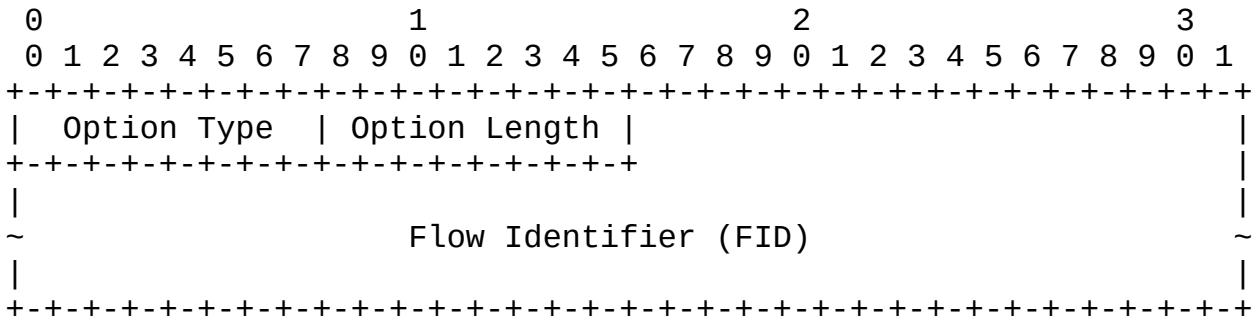


- Options are Type Length Values (TLV)
- Adapted from IPv6 Extension Header Options (RFC 8200 Section 4.2)
- Multiple Options can follow the header
- Future documents can define new Options
- Reserved space for private Options

Option Types

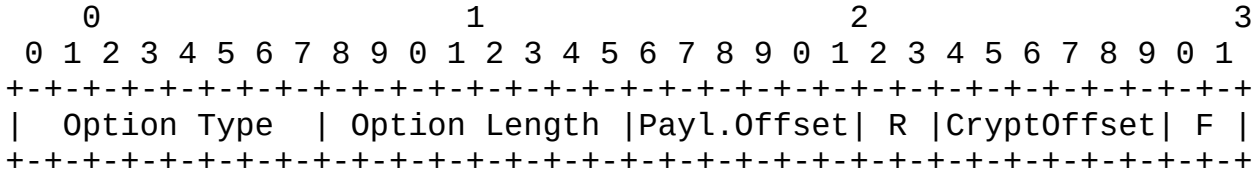
- Flow Identifiers
- Crypto Offset
- Padding
- Future documents can define new Option Types

Flow Identifier Options



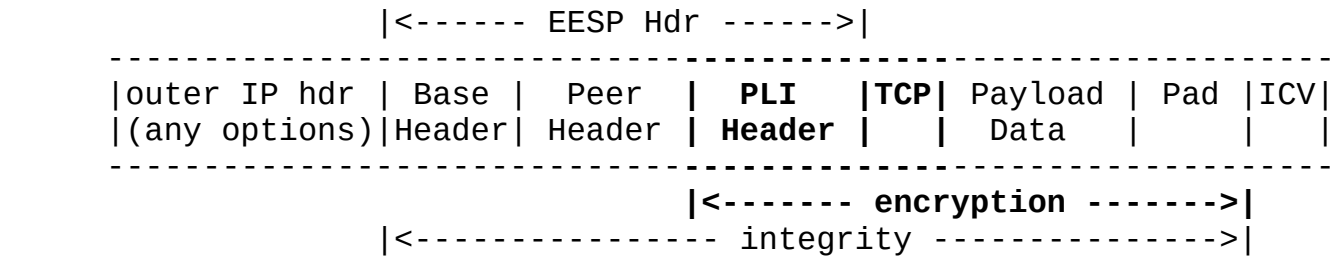
- Carries characteristic information of the inner flow
- Simple Flow Identifier specified in EESP
- Further Flow Identifiers may be specified by future documents
- Can be used by intermediate devices
  - ECMP
  - RSS

Crypto Offset Option

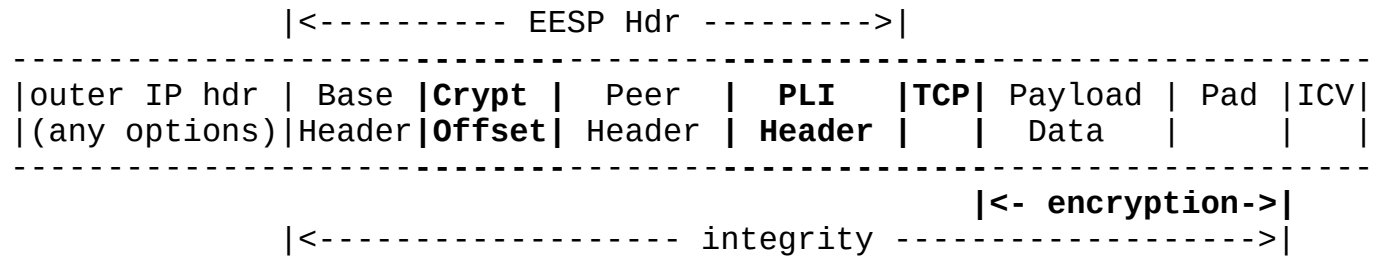


- Payload Offset – Start of the inner packet
- R – Reserved
- CryptOffset – Offset left unencrypted at beginning of the inner packet
- F – Flags (e.g. for PSP usecase)

Crypto Offset (Full Packet Format)



NO CryptOffset Option (Full Packet Format)



CryptOffset Option present (Full Packet Format)

Padding Options

- Pad1, PadN adapted from RFC 8200
- Used to align following header (4 byte IPv4, 8 byte IPv6)
- Future usecase: Ciphertext alignment (for SIMD, AVX)

Major changes to ESP

- Adds Version Number (no need for new IP protocol numbers)
- 8 byte base header
- Session ID
- Variable Header-Options possible
- Transmit 64 bit SeqNo (always use ESN)
- Make SeqNo optional
- Two packet formats (full/optimized)
- Remove implicit header parts
- Remove the trailer
- Remove TFC padding, use IPTFS instead

Open Questions (engineering)

- Optimized Packet Format?
  - Saves 4 bytes per packet on Tunnel Mode
- Header TLV use OK?

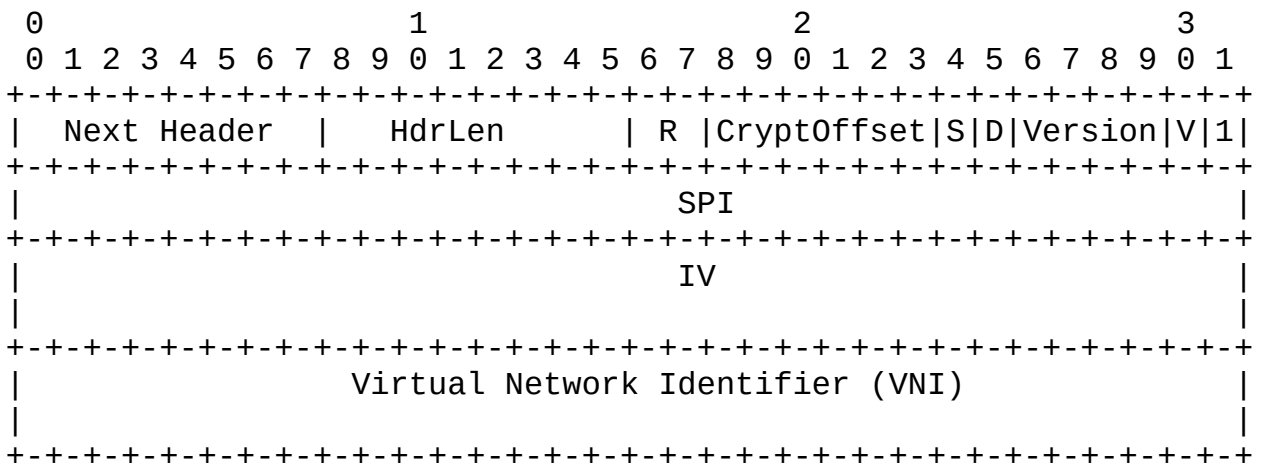
Open Questions (process)

- What should EESP Draft Look Like?
  - Add references to RFC 4303
  - Copy text from RFC 4303

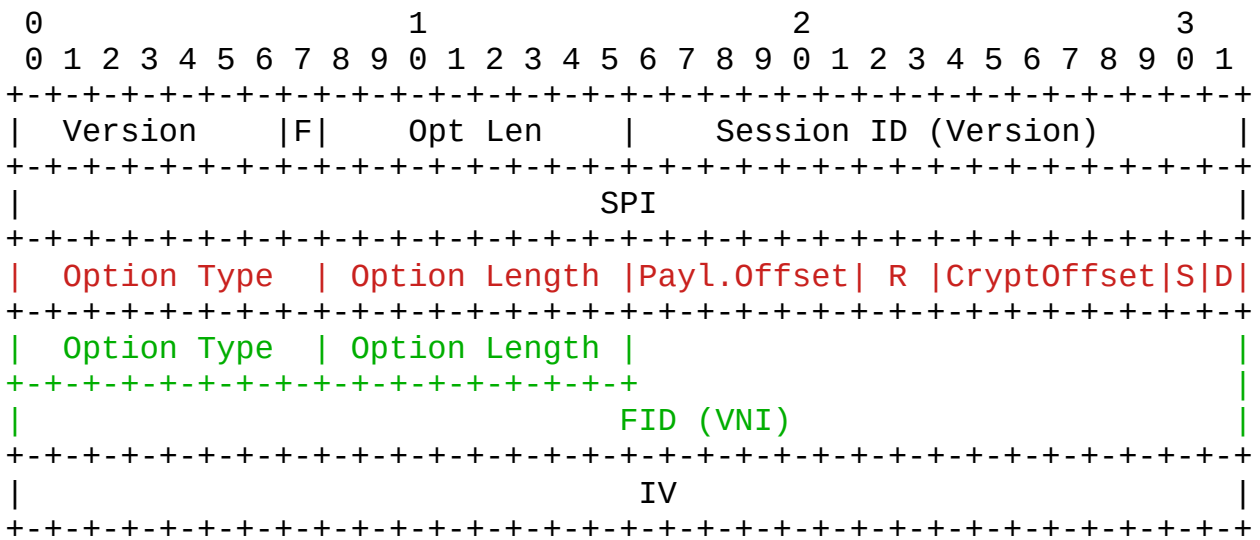
Questions?

Backup slides
Google PSP usecase with EESP

PSP


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Next Header
HdrLen
R
CryptOffset
S
D
Version
V
1
SPI
IV
Virtual Network Identifier (VNI)
orig IP hdr (any options)
PSP Hdr
TCP
Pyld Data
PSP ICV
<- encryption ->
<------- integrity ------->

EESP-PSP with CryptOffset and FID Option



EESP-PSP with combined CryptOffset and FID Option