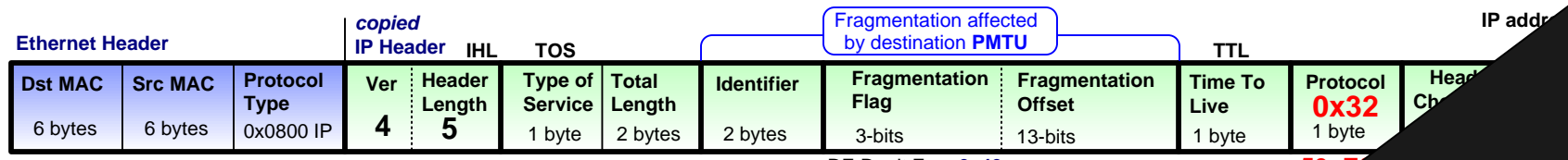


IPv4 IPsec - ESP*** protocol, Tunnel mode

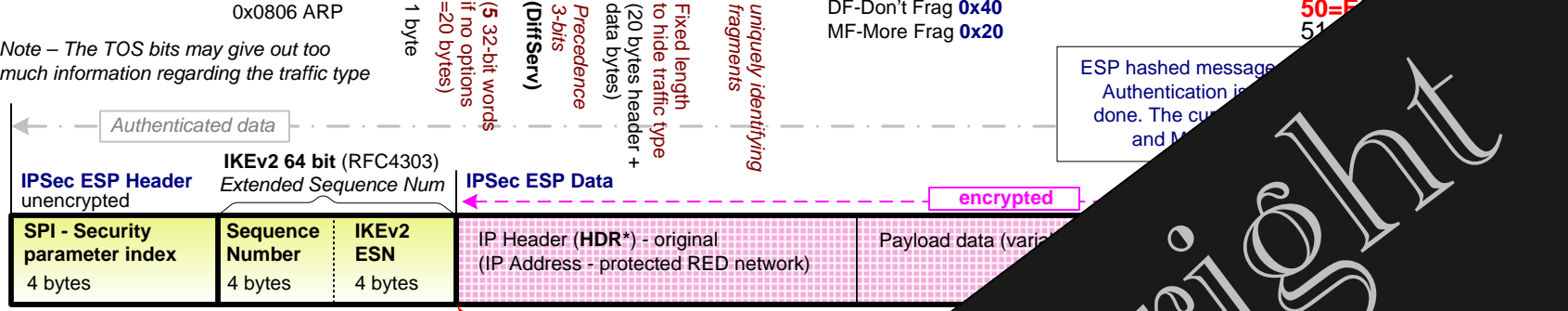
IPsec is a collection of protocols that provide low-level network security

(Encapsulating Security Payload - ESP, protocol 50, with tunnel mode the entire IP packet is encapsulated in another IP datagram and an IPsec is inserted)

Outbound: **Encryption**
Inbound: **Authentication**



Note - The TOS bits may give out too much information regarding the traffic type



Specifies an index to the SA database
Number, used to prevent replay attacks. **Never allowed to cycle.** Sender increases by 1 every transmitted packet.

The first step in IPsec communications is the determination of "Interesting traffic".

Traffic is deemed interesting when the IPsec security policy configured in the IPsec peer starts the IKE process.

For Cisco routers - access lists are used to determine the traffic to encrypt.

The major components of the IPsec are divided into the following categories:
Encapsulating Security Payload (ESP) - provides confidentiality, integrity, and data authentication.
Authentication Header (AH) - provides integrity and authentication.
Internet Key Exchange (IKE) - negotiates and distributes cryptography keys for the system, authenticates the system.
Manual Keys - distributing keys manually.

*** per RFC4301, IPsec MUST support ESP protocol, AH has been downgraded to MAY.