

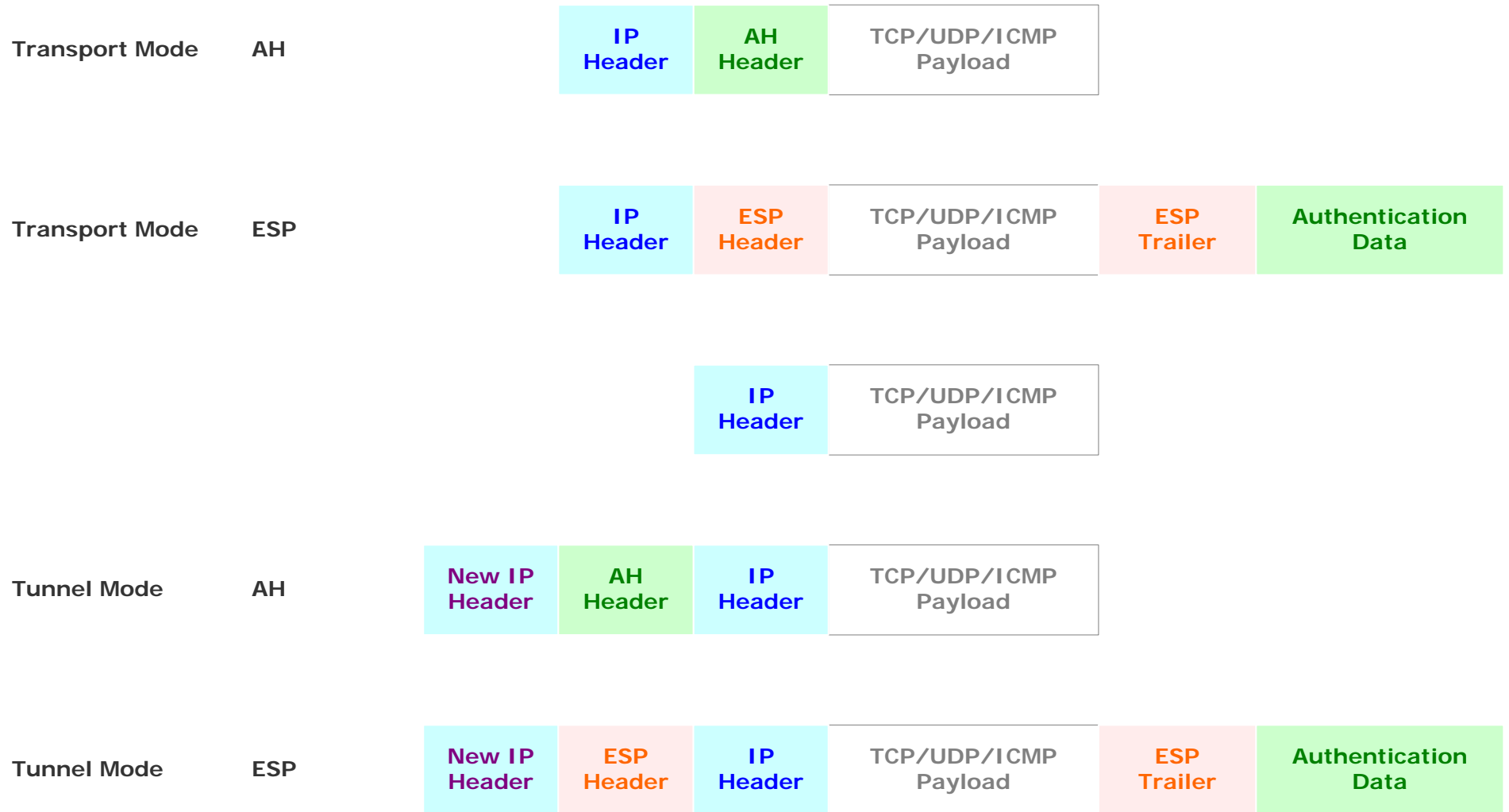
IPSec Guide

IPSec Modes & Protocols

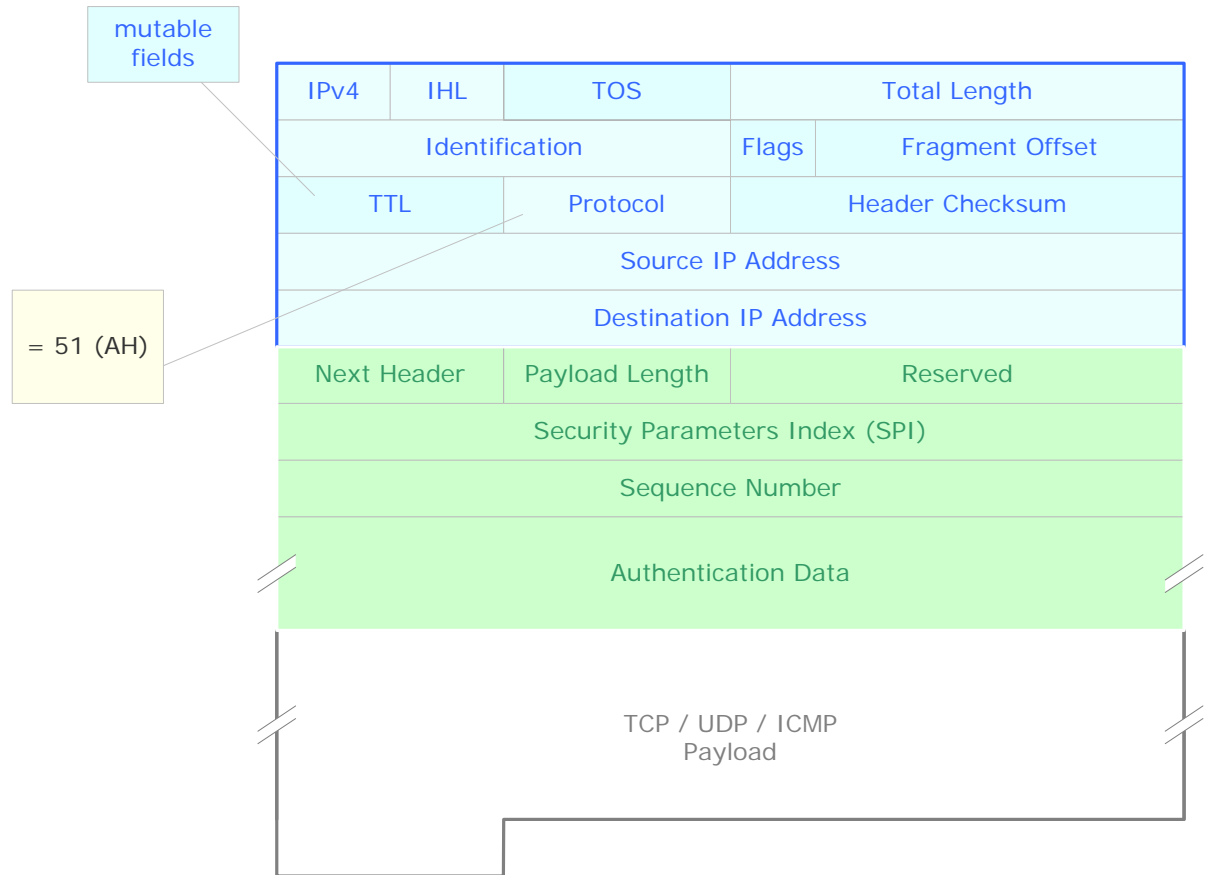
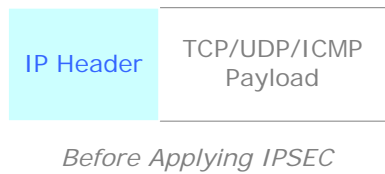
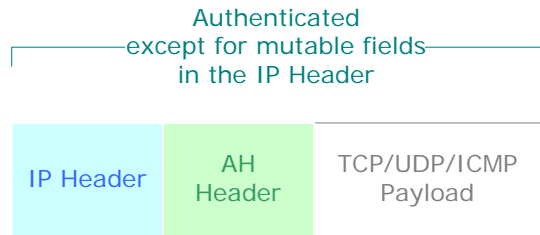
V1.1 – October 12, 2006

This document illustrates, as a synopsis, the IPSec encapsulation of secured IP packets according to IPSec protocol (AH or ESP) and mode (Transport or Tunnel).

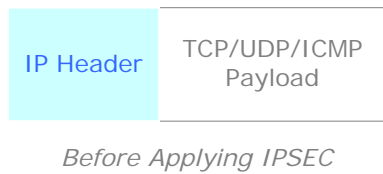
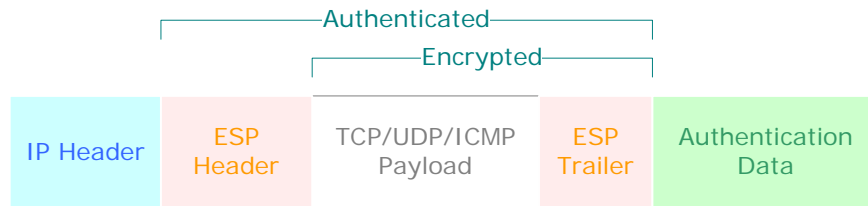
IPSec – Modes & Protocols – Synoptic View



IPSec – Transport Mode & AH Protocol

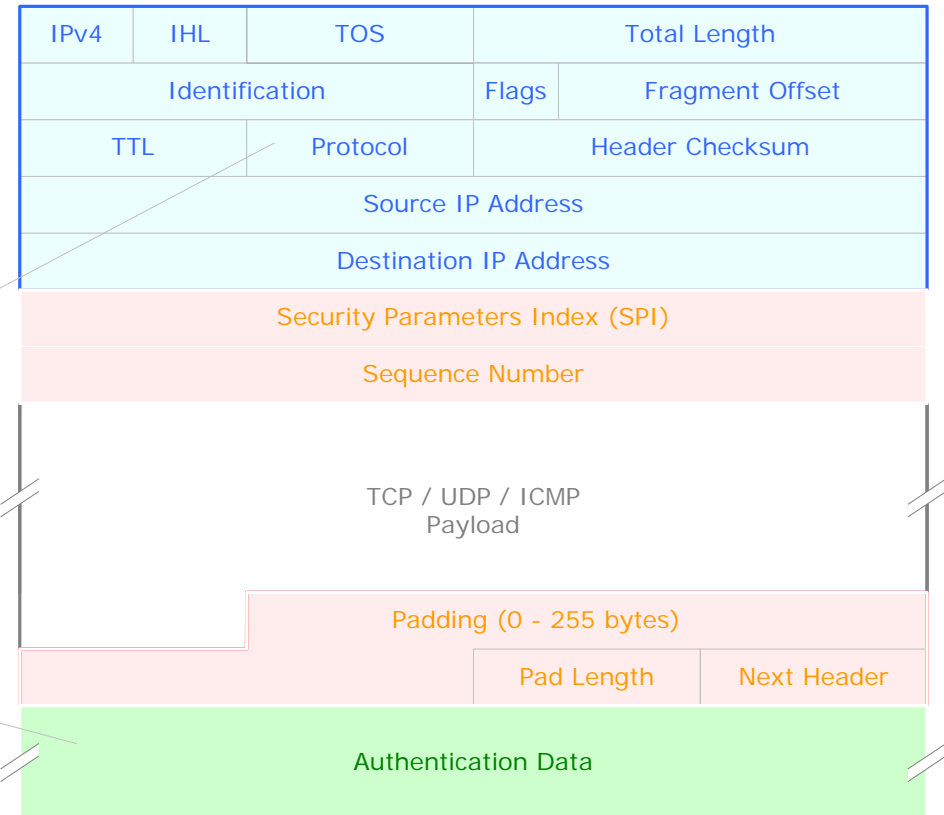


IPSec – Transport Mode & ESP Protocol

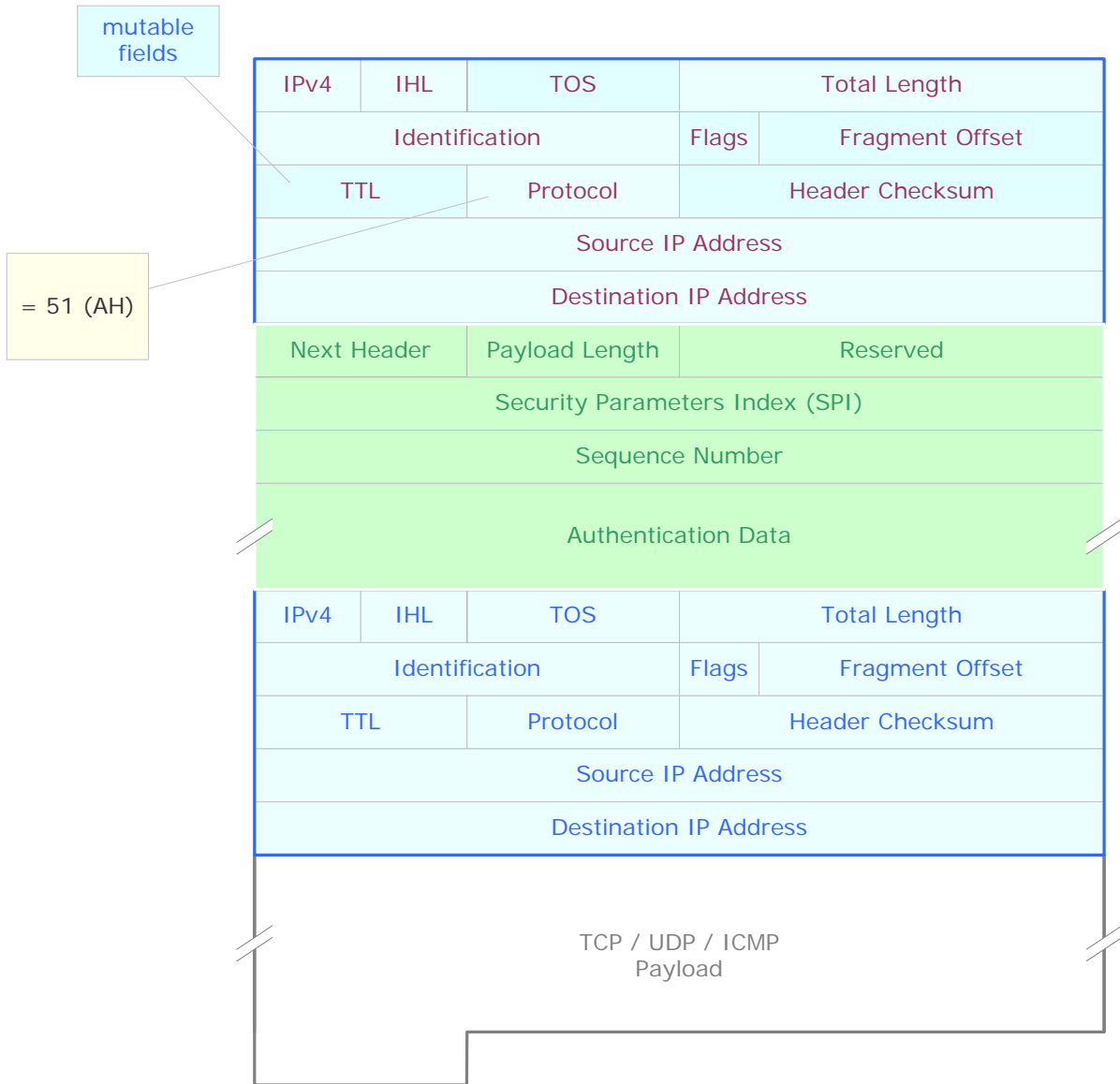
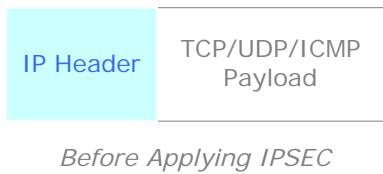
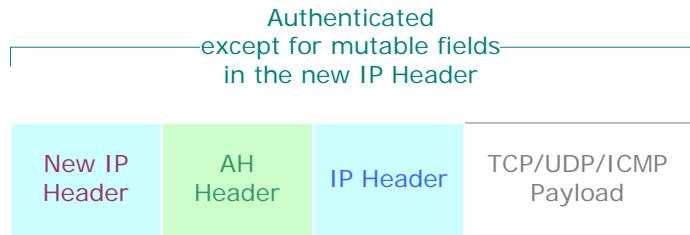


= 50 (ESP)

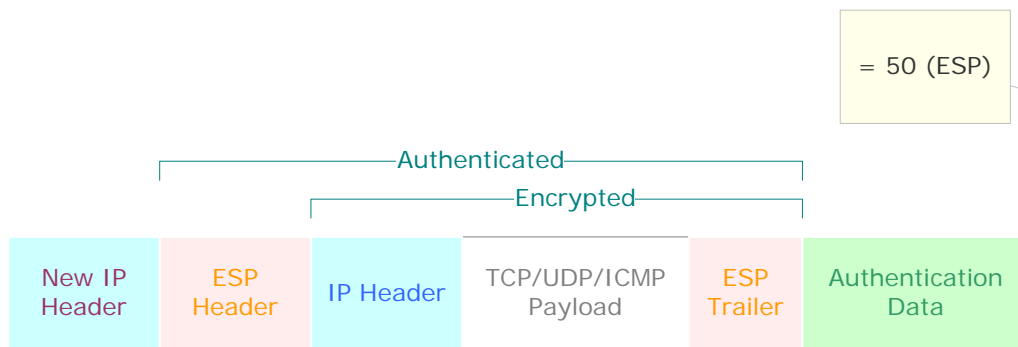
Contains an Integrity Check Value (ICV) computed over the ESP packet minus the Authentication Data. This field is optional, and is included only if the authentication service has been selected for the SA, i.e. if the "Authentication Algorithm" attribute was included in the Transform. The length of this field is 12 bytes (96 bits) for HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404).



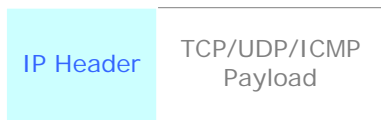
IPSec – Tunnel Mode & AH Protocol



IPSec – Tunnel Mode & ESP Protocol



= 50 (ESP)



Before Applying IPSEC

Contains an Integrity Check Value (ICV) computed over the ESP packet minus the Authentication Data. This field is optional, and is included only if the authentication service has been selected for the SA, i.e. if the "Authentication Algorithm" attribute was included in the Transform. The length of this field is 12 bytes (96 bits) for HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404).

