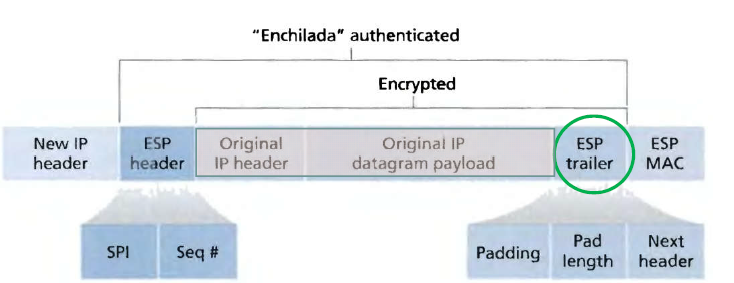
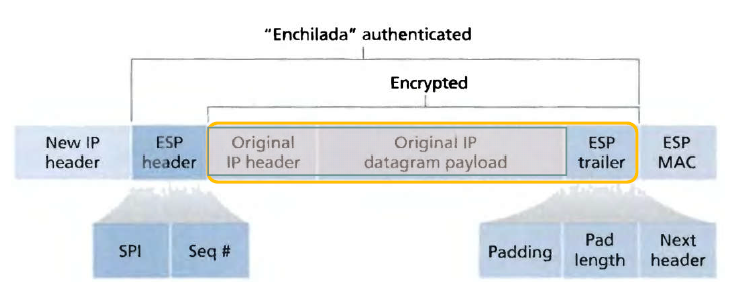
**IPSec 传输模式下ESP 报文的装包与拆包过程**

1. **装包过程**
2. 在原IP报文末尾添加ESP trailer(尾部/挂载)信息，如下图所示：

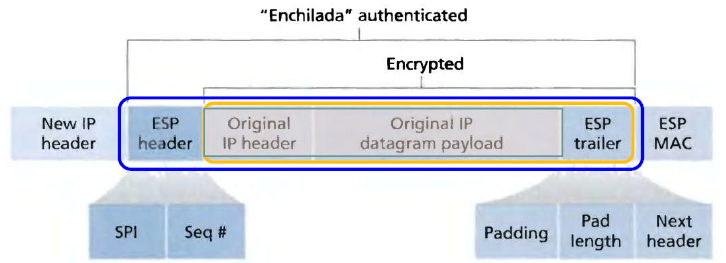


ESP trailer包含三部分。由于所选加密算法可能是块加密，当最后一块长度不足时就需要填充(padding)，附上填充长度(Pad length) 方便解包时顺利找出用来填充的那一段数据。Next header 用来标明被封装的原报文的协议类型，例如4=IP。

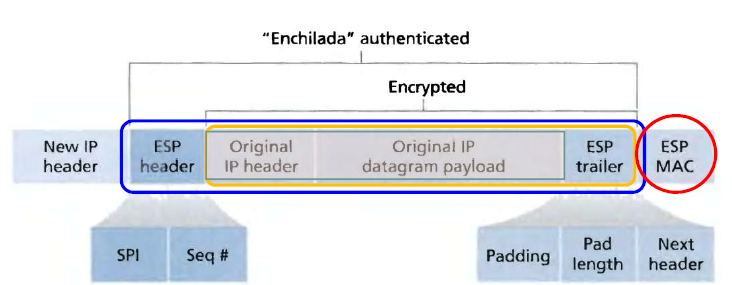
1. 将原IP 报文以及第1步得到的ESP trailer 作为一个整体进行加密封装。具体的加密算法与密钥由SA 给出。

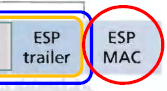


(3) 为第2步得到的加密数据添加ESP header。ESP header由SPI 和Seq# 两部分组成。加密数据与ESP header 合称为“Enchilada”，构成认证部分。注意到被封装的原报文的协议类型受到保护，由加密的ESP trailer 的Next header 声明，而不出现在未加密的ESP header 中。

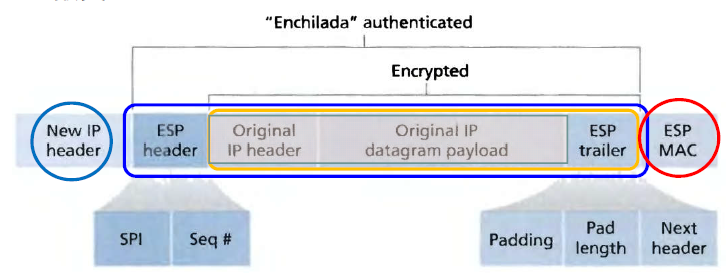


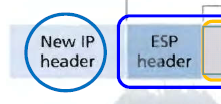
(4) 附加完整性度量结果(ICV，Integrity check value)。对第3步得到的“enchilada” 部分做认证，得到一个32位整数倍的完整性度量值(MAC)，并附在ESP 报文的尾部。完整性度量算法包括需要的认证密钥由SA 给出。





(5) 加上新的IP header 构成IPsec 报文。新构造的IP header 附在ESP 报文的前面组成一个新的IP 报文。注意这个新的IP header的IP 地址由路由器和安全网关解释，可以和原报文(由主机创建的IP 地址) 不同。协议类型为50，说明它封装的是一个ESP报文。





1. **拆包过程**

(1) 接收方收到IP 报文后，发现协议类型是50，表明这是一个ESP包。首先查看ESP header，通过SPI 决定数据报文所对应的SA，获得对应的模式(tunnel/transport mode) 以及安全规范。

(2) 计算“enchilada” 部分的摘要，与附在末尾的ICV 做对比，验证数据完整性。

(3) 检查Seq# 里的顺序号，保证数据是“新鲜”的。

(4) 根据SA 所提供的加密算法和密钥，解密被加密过的数据，得到原IP 报文与ESP trailer。

(5) 根据ESP trailer 的填充长度信息，找出填充字段的长度，删去后得到原来的IP 报文。

(6) 最后根据得到的原IP 报文的目的地址进行转发。

