哈爾濱工業大學

毕业设计（论文）的外文文献翻译

原始资料的题目/来源：

Rfc4303-IP Encapsulating Security Payload (ESP)

翻译后的中文题目：

Rfc4303-IP 封装安全有效载荷(ESP)

专　　业　信息安全

学　　生　殷 悦

学　　号　**150120526**

班　　号　**1504201**

指导教师　刘　扬

翻译日期　**2019 年 6 月 4 日**

外文文献的中文翻译

1. 介绍

封装安全有效载荷头在 IPv4 和 IPv6 中提供一种混合的安全服务。ESP 可以单独应用，与 IP 验证头(AH)结合使用，或者采用嵌套形式，例如，隧道模式的应用(参看"SecurityArchitecturefortheInternetProtocol"[KA97a]，下面使用“安全架构文档”代替)。安全服务可以在一对通信主机之间，一对通信的安全网关之间，或者一个安全网关和一台主机之间实现。在各种网络环境中如何使用 ESP 和 AH 的详细细节，参看安全架构文档。

ESP 头可以插在 IP 头之后、上层协议头之前(传送模式)，或者在封装的 IP 头之前(隧道模式)。下面将详细介绍这些模式。

ESP 提供机密性、数据源验证、无连接的完整性、抗重播服务(一种部分序列完整性的形式)和有限信息流机密性。提供的这组服务由 SA 建立时选择的选项和实现的位置来决定，机密性的选择与所有其他服务相独立。但是，确保机密性而不保证完整性/验证(在 ESP 或者单独在 AH 中)可能使信息易受到某种活动的、破坏机密性服务的攻击(参看[Bel96])。数据源验证和无连接的完整性(下面统一称作“验证”引用它们)是相互关联的服务，它们作为一个选项与机密性(可选择的)结合提供给用户。只有选择数据源验证时才可以选择抗重播服务，由接收方单独决定抗重播服务的选择。（尽管默认要求发送方增加抗重播服务使用的序列号，但只有当接收方检查序列号，服务才是有效的。）信息流机密性要求选择隧道模式，如果在安全网关上实现信息流机密性是最有效的，这里信息聚集能够掩饰真正的源-目的模式。注意尽管机密性和验证是可选的，但它们中必须至少选择一个。

假定读者熟悉安全架构文档中描述的术语和概念。特别是，读者应该熟悉 ESP 和 AH 提供的安全服务的定义，SA 定义，ESP 可以和验证（AH）头结合使用的方式，以及 ESP 和 AH 使用的不同密钥管理选项。（至于最后一项，ESP 和 AH 要求的当前密钥管理选项是通过 IKE 进行的手工建立密钥和自动建立密钥[HC98]。）

2. 封装安全有效载荷分组格式

ESP 头紧紧跟在协议头（IPv4，IPv6，或者扩展）之后，协议头的协议字段（IPv4）将是 50，或者协议的下一个头(IPv6，扩展)字段[STD-2]值是 50。下面小节定义了头格式中的字段。“可选项”意味着如果没有选择它，该字段被忽略。即它既

不被包含在传送的分组中，也不会在完整性校验值(ICV，参看 2.7)计算中出现。建立 SA 时决定是否选择某个选项，因此 ESP 分组的格式对于给定的 SA 是确定的，

整个 SA 存活期间也是确定的。相对而言，“强制性”字段总是出现在 ESP 分组格式中，对所有 SA 均如此。

2.1 安全参数索引 SPI

SPI 是一个任意的 32 位值，它与目的 IP 地址和安全协议（ESP）结合，唯一地标识这个数据报的 SA。从 1 至 255 的这组 SPI 值是由 InternetAssignedNumbersAuthority(IANA)保留给将来使用的；除了分配的 SPI 值的使用由 RFC 指定，否则，一般 IANA 不会分配保留的 SPI 值。通常在建立 SA 时目的系统选择 SPI（详细内容请参看安全架构文档）。SPI 字段是强制性的。

SPI 的值为 0 是保留给本地、特定实现使用的，不允许在线路上发送。例如，密钥管理实现可以使用 SPI 的 0 值表示当 IPsec 实现要求它的密钥管理实体建立新 SA，但 SA 仍然没有建立时，“没有 SA 存在”。

2.2 序列号 SequenceNumber

这个无符号的、32 位字段包含一个单调递增的计数器值（序列号）。它是强制性的，即使接收方没有选择激活一个特定 SA 的抗重播服务，它也总是存在。序列号字段由接收方处理，即发送方必须总是传输这个字段，但接收方不需要对其操作（参看下面“入站分组处理”中序列号确认的讨论）。

发送方的计数器和接收方的计数器在一个 SA 建立时被初始化为 0。（使用给定 SA 发送的第一个分组的序列号 1；序列号如何产生的细节参看 3.3.3 节）如果激活抗重播服务（默认地），传送的序列号必须决不允许循环。因此，在 SA 上传送第 2 的 32 次方个分组之前，发送方计数器和接收方计数器必须重新置位（通过建立新 SA 和获取新密钥）

2.3 有效载荷数据 PayloadData

有效载荷数据是变长字段，它包含下一个头字段描述的数据。有效载荷数据字段是强制性的，它的长度是字节的整数倍。如果加密有效载荷的算法要求加密同步数据，例如初始化向量（IV），那么这个数据可以明确地装载在有效载荷字段。任何要求这样明确的、每分组同步数据的加密算法必须指出同步数据的长度、结构和位置，这是指定 ESP 中算法如何使用的某个 RFC 的一部分。如果这种同步数据是隐式的，派生数据的算法必须是 RFC 的一部分。

注意关于确保 IV 存在时（实际）密文对齐：对于一些基于 IV 模式的操作，接收

方把 IV 作为密文的开始，直接把 IV 传给算法。这些模式中，（实际）密文是否开始对齐对于接收方并不重要。某些情况下，接收方从密文中单独读入 IV。此时，算法规范必须解决（实际）密文对齐如何实现。

2.4 填充(供加密使用)

几种因素要求或者激活填充字段的使用。

如果采用的加密算法要求明文是某个数量字节的倍数，例如块密码（blockcipher）的块大小，使用填充字段填充明文（包含有效载荷数据、填充长度和下一个头字段，以及填充）以达到算法要求的长度。

不管加密算法要求如何，也可以要求填充字段来确保结果密文以 4 字节边界终止。特别是，填充长度字段和下一个头字段必须在 4 字节字内右对齐，如上图所示的 ESP 分组格式，从而确保验证数据字段（如果存在）以 4 字节边界对齐。

除了算法要求或者上面提及的对齐原因之外，填充字段可以用于隐藏有效载荷实际长度，支持（部分）信息流机密性。但是，包含这种额外的填充字段占据一定的带宽，因而小心使用。

发送方可以增加 0 至 255 个字节的填充。ESP 分组的填充字段是可选的，但是所有实现必须支持填充字段的产生和消耗。

a.为了确保加密位是算法块大小（上面第一个加重号）的倍数，填充计算应用于除 IV 之外的有效载荷数据、填充长度和下一个头字段。

b.为了确保验证数据以 4 字节边界对齐（上面第二个加重号），填充计算应用于包含 IV 的有效载荷数据、填充长度和下一个头字段。

如果需要填充字节，但是加密算法没有指定填充内容，则必须采用下列默认处理。填充字节使用一系列（无符号、1 字节）整数值初始化。附加在明文之后的第一个填充字节为 1，后面的填充字节按单调递增：1,2,3,…。当采用这种填充方案时，接收方应该检查填充字段。（选择这种方案是由于它相对简单，硬件实现容易。在没有其他完整性措施实施情况下，如果接收方检查解密的填充值，这种方案粉碎了某种形式的“剪切和粘贴”攻击，提供有限的保护。）

任何要求填充字段但不同于上述默认方法的加密算法，必须在一个指定 ESP 中算法如何使用的 RFC 中定义填充字段内容（例如，0 或者随机数）和所有要求接收方对这些填充字节的处理。这种情况下，填充字段的内容将由相应算法 RFC 中定义和选择的加密算法和模式决定。相关的算法 RFC 可以指定接收方必须检查填充字段或者接收方必须通知发送方接收方如何处理填充字段。

2.5 填充长度 PadLength

填充长度字段指明紧接其前的填充字节的个数。有效值范围是 0 至 255，0 表明没有填充字节。填充长度字段是强制性的。

2.6 下一个头

下一个头是一个 8 位字段，它标识有效载荷字段中包含的数据类型，例如，IPv6 中的扩展头或者上层协议标识符。该字段值从 InternetAssignedNumbersAuthority(IANA)最新“AssignedNumbers”[STD-2]RFC 定义的 IP 协议号集当中选择。下一个头字段是强制性的。

2.7 验证数据

验证数据是可变长字段，它包含一个完整性校验值（ICV），ESP 分组中该值的计算不包含验证数据本身。字段长度由选择的验证函数指定。验证数据字段是可选的，只有 SA 选择验证服务，才包含验证数据字段。验证算法规范必须指定 ICV 长度、验证的比较规则和处理步骤。

3. 封装安全协议处理

3.1ESP 头定位

类似于 AH，ESP 有两种使用方式：传送模式或者隧道模式。前者仅在主机中实现，提供对上层协议的保护，不提供对 IP 头的保护。（传送模式中，注意安全架构文档中定义的“堆栈中的块”或者“线路中的块”实现，入站和出站 IP 分片可能要求 IPsec 实现执行额外的 IP 重组/分片，以便遵照这个规范，提供透明 IPsec 支持。当存在多个接口时，在这些实现内部执行这些操作要特别小心。）

传送模式中，ESP 插在 IP 头之后，上层协议之前，例如 TCP，UCP，ICMP 等，或者在任何已经插入的 IPsec 头之前。IPv4 中，意指把 ESP 放在 IP 头（和它包含的任何其他选项）之后,但是在上层协议之前。（注意术语“传输”模式不应该曲解为把它的应用限制在 TCP 和 UDP 中。例如 ICMP 报文可能使用“传输”模式或者“隧道”模式发送。）下面数据报图示了典型 IPv4 分组中 ESP 传送模式位置，以“表示出外形上尖锐对照”为基础。(“ESP 尾部”包含所有填充，加填充长度和下一个头字段。)

IPv6 中，ESP 被看作端到端的有效载荷，因而应该出现在逐跳，路由和分片扩展头之后。目的选项扩展头既可以在 ESP 头之前，也可以在 ESP 头之后，这由期望的语义决定。但是，因为 ESP 仅保护 ESP 之后的字段，通常它可能愿意把目的选项头放在 ESP 头之后。下面数据报图示了典型 IPv6 分组中 ESP 传送模式位置。如果存在，

应该在 ESP 之前，ESP 之后，或者 ESP 和 AH 头以各种模式组合。IPsec 架构文档描述了必须支持的 SA 组合。隧道模式 ESP 可以在主机或者安全网关上实现。ESP 在安全网关（保护用户传输流量）实现时必须采用隧道模式。隧道模式中，“内部”IP 头装载最终的源和目的地址，而“外部”IP 头可能包含不同的 IP 地址，例如安全网关地址。ESP 保护整个内部 IP 分组，其中包括整个内部 IP 头。相对于外部 IP 头，隧道模式的 ESP 位置与传送模式中 ESP 位置相同。下面数据报图示了典型 IPv4 和 IPv6 分组中 ESP 隧道模式的位置。

3.2 算法

强制实现算法在第 5 节描述，“一致性要求”。但也可以支持其他算法。注意尽管机密性和验证是可选的，但是至少要从这两种服务中选择其一，因此相应的两种算法不允许同时为 NULL。

3.2.1 加密算法

采用的加密算法由 SA 指定。ESP 使用对称加密算法。因为到达的 IP 分组可能失序，每个分组必须携带所有要求的数据，以便允许接收方为解密建立加密同步。这个数据可能明确地装载在有效载荷字段，例如作为 IV（上面描述的），或者数据可以从分组头推导出来。因为 ESP 准备了明文填充，ESP 采用的加密算法可以显示块或者流模式特性。注意因为加密（机密性）是可选的，这个算法可以为“NULL”。

3.2.2 验证算法

ICV 计算使用的验证算法由 SA 指定。点对点通信时，合适的验证算法包括基于对称加密算法（例如 DES）的或者基于单向散列函数（例如 MD5 或 SHA-1）的键控消息鉴别码（MAC）。对于多点传送通信，单向散列算法与不对称数字签名算法结合使用比较合适，虽然目前性能和空间的考虑阻止了这种算法的使用。注意验证是可选的，这个算法可以是“NULL”。

3.3 出站分组处理

传送模式中，发送方把上层协议信息封装在 ESP 头/尾中，保留了指定的 IP 头（和 IPv6 中所有 IP 扩展头）。隧道模式中，外部和内部 IP 头/扩展头以各种方式相关。封装处理期间外部 IP 头/扩展头的构建在安全架构文档中描述。如果安全策略要求不止一个 IPsec 头扩展，安全头应用的顺序必须由安全策略定义。

3.3.1SA 查找

只有当 IPsec 实现确定与某个调用 ESP 处理的 SA 相关联时，ESP 才应用于一个出站分组。确定对出站分组采取哪些 IPsec 处理的过程在安全架构文档中描述。

3.3.2 分组加密

在本节中，由于格式化的含意，我们依据经常采用的加密算法来讲述。需要理解采用 NULL 加密算法提供的“没有机密性”。因此发送方：

1.封装（到 ESP 有效载荷字段）：

-传送模式－只有原始上层协议信息。

-隧道模式－整个原始 IP 数据报。

2.增加所有需要的填充。

3.使用 SA 指明的密钥，加密算法，算法模式和加密同步数据（如果需要）加密结果。

-如果指出显式加密同步数据，例如 IV，它经由算法规范输入到加密算法中，并放在有

效载荷字段中。

-如果指出隐式加密同步数据，例如 IV，它被创建并经由算法规范输入加密算法。

构建外部 IP 头的确切步骤依赖于模式（传输或者隧道），并在安全架构文档中描述。

如果选择验证，验证之前首先执行加密，而加密并不包含验证数据字段。这种处理顺序易于

在分组解密之前，接收方迅速检测和拒绝分组重播或伪造分组，因而潜在地降低拒绝服务攻击的

影响。同时它也考虑了接收方并行分组处理的可能性，即加密可以与验证并发执行。注意因为验

证数据不受加密保护，必须采用一种键控的验证算法计算 ICV。

3.3.3 序列号产生

当 SA 建立时，发送方的计数器初始化为 0。发送方为这个 SA 增加序列号，把新值插入到序列号字段中。采用给定 SA 发送的第一个分组具有序列号 1。如果激活抗重播服务（默认），发送方核查确保在序列号字段插入新值之前计数器没有循环。换言之，发送方不允许在一个 SA 上发送一个引起序列号循环的分组。传输一个可能导致序列号溢出的分组的尝试是可审核事件。（注意这种序列号管理方式不需要使用模

运算）发送方假定抗重播服务是一种默认支持，除非接收方另外通告（参看 3.4.3）。因此，如果计数器已经循环，发送方将建立新 SA 和密钥（除非 SA 被配置为手工密钥管理）。如果抗重播服务被禁止，发送方不需要监视或者把计数器置位，例如，手工密钥管理情况下（参看第 5 节）。但是，发送方仍然增加计数器的值，当它达到最大值时，计数器返回 0 开始。

3.3.4 完整性校验值计算

如果 SA 选择验证，发送方在 ESP 分组上计算 ICV 但不包含验证数据。因此 SPI、序列号、有效载荷数据、填充（如果存在）、填充长度和下一个头字段都包含在 ICV 计算中。注意因为加密比验证先执行，最后 4 个字段将是密文形式。一些验证算法中，ICV 计算实现所使用的字节串必须是算法指定的块大小的倍数。如果这个字节串长度与算法要求的块大小不匹配，必须在 ESP 分组末端添加隐含填充，（下一个头字段之后）在 ICV 计算之前添加。填充八位组必须是 0 值。算法规范指定块大小（和因此的填充长度）。这个填充不随分组传输。注意 MD5 和 SHA-1 内部填充协定，它们被看作有 1 字节的块大小。

3.3.5 分片

如果需要，IPsec 实现内部 ESP 处理之后执行分片。因此传送模式 ESP 应用于整个 IP 数据报（而不是 IP 片段）。ESP 处理过的分组本身可以在途中由路由器分片，这样的片段接收方必须在 ESP 处理之前重组。隧道模式时，ESP 应用于一个 IP 分组，它的有效载荷可能是一个已分片的 IP 分组。例如，安全网关或者“堆栈中的块”或者“线路上的块”IPsec 实现（安全架构文档中定义）可以把隧道模式 ESP 应用到这样的片段中。

注意：传送模式—3.1 节开始提及的，堆栈中的块和线路上的块实现可以由本地 IP 层首先重组已分片的分组，接着应用 IPsec，再把结果分组分片。

注意：对于 IPv6 - 堆栈中的块和线路上的块实现，有必要查看所有扩展头来确定是否有一个分片的头，从而决定分组是否需要在 IPsec 处理之前重组。

外文文献的原稿

1. Introduction

The Encapsulating Security Payload (ESP) header is designed to provide a mix of security services in IPv4 and IPv6. ESP may be applied alone, in combination with the IP Authentication Header (AH) [KA97b], or in a nested fashion, e.g., through the use of tunnel mode (see "Security Architecture for the Internet Protocol" [KA97a], hereafter referred to as the Security Architecture document). Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. For more details on how to use ESP and AH in various network environments, see the Security Architecture document [KA97a].

The ESP header is inserted after the IP header and before the upper layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode). These modes are described in more detail below.

ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality. The set of services provided depends on options selected at the time of Security Association establishment and on the placement of the implementation. Confidentiality may be selected independent of all other services. However, use of confidentiality without integrity/authentication (either in ESP or separately in AH) may subject traffic to certain forms of active attacks that could undermine the confidentiality service (see [Bel96]). Data origin authentication and connectionless integrity are joint services (hereafter referred to jointly as "authentication) and are offered as an option in conjunction with (optional) confidentiality. The anti- replay service may be selected only if data origin authentication is selected, and its election is solely at the discretion of the receiver. (Although the default calls for the sender to increment the Sequence Number used for anti-replay, the service is effective only if the receiver checks the Sequence Number.) Traffic flow confidentiality requires selection of tunnel mode, and is most effective if implemented at a security gateway, where traffic aggregation may be able to mask true source-destination patterns. Note that although both confidentiality and authentication are optional, at least one of them MUST be selected.

It is assumed that the reader is familiar with the terms and concepts described in the Security Architecture document. In particular, the reader should be familiar with the definitions of security services offered by ESP and AH, the concept of Security

Associations, the ways in which ESP can be used in conjunction with the Authentication Header (AH), and the different key management options available for ESP and AH. (With regard to the last topic, the current key management options required for both AH and ESP are manual keying and automated keying via IKE [HC98].)

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD,SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in RFC 2119 [Bra97].

2. Encapsulating Security Payload Packet Format

The protocol header (IPv4, IPv6, or Extension) immediately preceding the ESP header will contain the value 50 in its Protocol (IPv4) or Next Header (IPv6, Extension) field [STD-2].

The following subsections define the fields in the header format. "Optional" means that the field is omitted if the option is not selected, i.e., it is present in neither the packet as transmitted nor as formatted for computation of an Integrity Check Value (ICV, see Section 2.7). Whether or not an option is selected is defined as part of Security Association (SA) establishment. Thus the format of ESP packets for a given SA is fixed, for the duration of the SA. In contrast, "mandatory" fields are always present in the ESP packet format, for all SAs.

2.1 Security Parameters Index

The SPI is an arbitrary 32-bit value that, in combination with the destination IP address and security protocol (ESP), uniquely identifies the Security Association for this datagram. The set of SPI values in the range 1 through 255 are reserved by the Internet Assigned Numbers Authority (IANA) for future use; a reserved SPI value will not normally be assigned by IANA unless the use of the assigned SPI value is specified in an RFC. It is ordinarily selected by the destination system upon establishment of an SA (see the Security Architecture document for more details). The SPI field is mandatory.

The SPI value of zero (0) is reserved for local, implementation- specific use and MUST NOT be sent on the wire. For example, a key management implementation MAY use the zero SPI value to mean "No Security Association Exists" during the period when the IPsec implementation has requested that its key management entity establish a new SA, but the SA has not yet been established.

2.2 Sequence Number

This unsigned 32-bit field contains a monotonically increasing counter value (sequence number). It is mandatory and is always present even if the receiver does not elect to enable the anti-replay service for a specific SA. Processing of the Sequence Number field is at the discretion of the receiver, i.e., the sender MUST always transmit this field, but the receiver need not act upon it (see the discussion of Sequence Number Verification in the "Inbound Packet Processing" section below).

The sender's counter and the receiver's counter are initialized to 0 when an SA is established. (The first packet sent using a given SA will have a Sequence Number of 1; see Section 3.3.3 for more details on how the Sequence Number is generated.) If anti-replay is enabled(the default), the transmitted Sequence Number must never be allowed to cycle. Thus, the sender's counter and the receiver's counter MUST be reset (by establishing a new SA and thus a new key) prior to the transmission of the 2^32nd packet on an SA.

2.3 Payload Data

Payload Data is a variable-length field containing data described by the Next Header field. The Payload Data field is mandatory and is an integral number of bytes in length. If the algorithm used to encrypt the payload requires cryptographic synchronization data, e.g., an Initialization Vector (IV), then this data MAY be carried explicitly in the Payload field. Any encryption algorithm that requires such explicit, per-packet synchronization data MUST indicate the length, any structure for such data, and the location of this data as part of an RFC specifying how the algorithm is used with ESP. If such synchronization data is implicit, the algorithm for deriving the data MUST be part of the RFC.

Note that with regard to ensuring the alignment of the (real) ciphertext in the presence of an IV:

For some IV-based modes of operation, the receiver treats the IV as the start of the ciphertext, feeding it into the algorithm directly. In these modes, alignment of the start of the (real) ciphertext is not an issue at the receiver.

In some cases, the receiver reads the IV in separately from the ciphertext. In these cases, the algorithm specification MUST address how alignment of the (real) ciphertext is to be achieved.

2.4 Padding (for Encryption)

Several factors require or motivate use of the Padding field.

If an encryption algorithm is employed that requires the plaintext to be a multiple of some number of bytes, e.g., the block size of a block cipher, the Padding field is used to fill the plaintext (consisting of the Payload Data, Pad Length and Next Header fields, as well as the Padding) to the size required by the algorithm.

Padding also may be required, irrespective of encryption algorithm requirements, to ensure that the resulting ciphertext terminates on a 4-byte boundary. Specifically,the Pad Length and Next Header fields must be right aligned within a 4-byte word, as illustrated in the ESP packet format figure above, to ensure that the Authentication Data field (if present) is aligned on a 4-byte boundary.

Padding beyond that required for the algorithm or alignment reasons cited above, may be used to conceal the actual length of the payload, in support of (partial) traffic flow confidentiality. However, inclusion of such additional padding has adverse bandwidth implications and thus its use should be undertaken with care.

The sender MAY add 0-255 bytes of padding. Inclusion of the Padding field in an ESP packet is optional, but all implementations MUST support generation and consumption of padding.

a. For the purpose of ensuring that the bits to be encrypted are a multiple of the algorithm's blocksize (first bullet above), the padding computation applies to the Payload Data exclusive of the IV, the Pad Length, and Next Header fields.

b. For the purposes of ensuring that the Authentication Data is aligned on a 4-byte boundary (second bullet above), the padding computation applies to the Payload Data inclusive of the IV, the Pad Length, and Next Header fields.If Padding bytes are needed but the encryption algorithm does not specify the padding contents, then the following default processing MUST be used. The Padding bytes are initialized with a series of (unsigned, 1-byte) integer values. The first padding byte appended to the plaintext is numbered 1, with subsequent padding bytes making up a monotonically increasing sequence: 1, 2, 3, ... When this padding scheme is employed, the receiver SHOULD inspect the Padding field. (This scheme was selected because of its relative simplicity, ease of implementation in hardware, and because it offers limited protection against certain forms of "cut and paste" attacks in the absence of other integrity measures, if the receiver checks the padding values upon decryption.)

Any encryption algorithm that requires Padding other than the default described above, MUST define the Padding contents (e.g., zeros or random data) and any required receiver processing of these Padding bytes in an RFC specifying how the algorithm is used with ESP.

In such circumstances, the content of the Padding field will be determined by the encryption algorithm and mode selected and defined in the corresponding algorithm RFC. The relevant algorithm RFC MAY specify that a receiver MUST inspect the Padding field or that a receiver MUST inform senders of how the receiver will handle the Padding field.

2.5 Pad Length

The Pad Length field indicates the number of pad bytes immediately preceding it. The range of valid values is 0-255, where a value of zero indicates that no Padding bytes are present. The Pad Length field is mandatory.

2.6 Next Header

The Next Header is an 8-bit field that identifies the type of data contained in the Payload Data field, e.g., an extension header in IPv6 or an upper layer protocol identifier. The value of this field is chosen from the set of IP Protocol Numbers defined in the most recent "Assigned Numbers" [STD-2] RFC from the Internet Assigned Numbers Authority (IANA). The Next Header field is mandatory.

2.7 Authentication Data

The Authentication Data is a variable-length field containing an Integrity Check Value (ICV) computed over the ESP packet minus the Authentication Data. The length of the field is specified by the authentication function selected. The Authentication Data field is optional, and is included only if the authentication service has been selected for the SA in question. The authentication algorithm specification MUST specify the length of the ICV and the comparison rules and processing steps for validation.

3. Encapsulating Security Protocol Processing

3.1 ESP Header Location

Like AH, ESP may be employed in two ways: transport mode or tunnel mode. The former mode is applicable only to host implementations and provides protection for upper layer protocols, but not the IP header. (In this mode, note that for "bump-in-the-stack" or "bump-in-the- wire" implementations, as defined in the Security Architecture document, inbound and outbound IP fragments may require an IPsec implementation to perform extra

IP reassembly/fragmentation in order to both conform to this specification and provide transparent IPsec support. Special care is required to perform such operations within these implementations when multiple interfaces are in use.)

In transport mode, ESP is inserted after the IP header and before an upper layer protocol, e.g., TCP, UDP, ICMP, etc. or before any other IPsec headers that have already been inserted. In the context of IPv4, this translates to placing ESP after the IP header (and any options that it contains), but before the upper layer protocol. (Note that the term "transport" mode should not be misconstrued as restricting its use to TCP and UDP. For example, an ICMP message MAY be sent using either "transport" mode or "tunnel" mode.) The following diagram illustrates ESP transport mode positioning for a typical IPv4 packet, on a "before and after" basis. (The "ESP trailer" encompasses any Padding, plus the Pad Length, and Next Header fields.)

In the IPv6 context, ESP is viewed as an end-to-end payload, and thus should appear after hop-by-hop, routing, and fragmentation extension headers. The destination options extension header(s) could appear either before or after the ESP header depending on the semantics desired. However, since ESP protects only fields after the ESP header, it generally may be desirable to place the destination options header(s) after the ESP header. The following diagram illustrates ESP transport mode positioning for a typical IPv6 packet.
ESP and AH headers can be combined in a variety of modes. The IPsec Architecture document describes the combinations of security associations that must be supported.
Tunnel mode ESP may be employed in either hosts or security gateways. When ESP is implemented in a security gateway (to protect subscriber transit traffic), tunnel mode must be used. In tunnel mode, the "inner" IP header carries the ultimate source and destination addresses, while an "outer" IP header may contain distinct IP addresses, e.g., addresses of security gateways. In tunnel mode, ESP protects the entire inner IP packet, including the entire inner IP header. The position of ESP in tunnel mode, relative to the outer IP header, is the same as for ESP in transport mode. The following diagram illustrates ESP tunnel mode positioning for typical IPv4 and IPv6 packets.

3.2 Algorithms

The mandatory-to-implement algorithms are described in Section 5, "Conformance Requirements". Other algorithms MAY be supported. Note that although both confidentiality and authentication are optional, at least one of these services MUST be selected hence both algorithms MUST NOT be simultaneously NULL.

3.2.1 Encryption Algorithms

The encryption algorithm employed is specified by the SA. ESP is designed for use with symmetric encryption algorithms. Because IP packets may arrive out of order, each packet must carry any data required to allow the receiver to establish cryptographic synchronization for decryption. This data may be carried explicitly in the payload field, e.g., as an IV (as described above), or the data may be derived from the packet header. Since ESP makes provision for padding of the plaintext, encryption algorithms employed with ESP may exhibit either block or stream mode characteristics. Note that since encryption (confidentiality) is optional, this algorithm may be "NULL".

3.2.2 Authentication Algorithms

The authentication algorithm employed for the ICV computation is specified by the SA. For point-to-point communication, suitable authentication algorithms include keyed Message Authentication Codes (MACs) based on symmetric encryption algorithms (e.g., DES) or on one-way hash functions (e.g., MD5 or SHA-1). For multicast communication, one-way hash algorithms combined with asymmetric signature algorithms are appropriate, though performance and space considerations currently preclude use of such algorithms. Note that since authentication is optional, this algorithm may be "NULL".

3.3 Outbound Packet Processing

In transport mode, the sender encapsulates the upper layer protocol information in the ESP header/trailer, and retains the specified IP header (and any IP extension headers in the IPv6 context). In tunnel mode, the outer and inner IP header/extensions can be inter-related in a variety of ways. The construction of the outer IP header/extensions during the encapsulation process is described in the Security Architecture document. If there is more than one IPsec header/extension required by security policy, the order of the application of the security headers MUST be defined by security policy.

3.3.1 Security Association Lookup

ESP is applied to an outbound packet only after an IPsec implementation determines that the packet is associated with an SA that calls for ESP processing. The process of determining what, if any, IPsec processing is applied to outbound traffic is described in the Security Architecture document.

3.3.2 Packet Encryption

In this section, we speak in terms of encryption always being applied because of the formatting implications. This is done with the understanding that "no confidentiality" is offered by using the NULL encryption algorithm. Accordingly, the sender:

1. encapsulates (into the ESP Payload field):
 - for transport mode -- just the original upper layerprotocol information.
 - for tunnel mode -- the entire original IP datagram.
2. adds any necessary padding.
3. encrypts the result (Payload Data, Padding, Pad Length, and Next Header) using the key, encryption algorithm, algorithm mode indicated by the SA and cryptographic synchronization data (if any).
 - If explicit cryptographic synchronization data, e.g.,an IV, is indicated, it is input to the encryption algorithm per the algorithm specification and placed in the Payload field.
 - If implicit cryptographic synchronication data, e.g., an IV, is indicated, it is constructed and input to the encryption algorithm as per the algorithm specification.

The exact steps for constructing the outer IP header depend on the mode (transport or tunnel) and are described in the Security Architecture document.

If authentication is selected, encryption is performed first, before the authentication, and the encryption does not encompass the Authentication Data field. This order of processing facilitates rapid detection and rejection of replayed or bogus packets by the receiver, prior to decrypting the packet, hence potentially reducing the impact of denial of service attacks. It also allows for the possibility of parallel processing of packets at the receiver, i.e., decryption can take place in parallel with authentication. Note that since the Authentication Data is not protected by encryption, a keyed authentication algorithm must be employed to compute the ICV.

3.3.3 Sequence Number Generation

The sender's counter is initialized to 0 when an SA is established.The sender increments the Sequence Number for this SA and inserts the new value into the Sequence Number field. Thus the first packet sent using a given SA will have a Sequence Number of 1.

If anti-replay is enabled (the default), the sender checks to ensure that the counter has not cycled before inserting the new value in the Sequence Number field. In other words, the sender MUST NOT send a packet on an SA if doing so would cause the Sequence Number to cycle. An attempt to transmit a packet that would result in Sequence Number overflow is an auditable event. (Note that this approach to Sequence Number management does not require use of modular arithmetic.)

The sender assumes anti-replay is enabled as a default, unless otherwise notified by the receiver (see 3.4.3). Thus, if the counter has cycled, the sender will set up a new SA and

key (unless the SA was configured with manual key management).
If anti-replay is disabled, the sender does not need to monitor or reset the counter, e.g., in the case of manual key management (see Section 5). However, the sender still increments the counter and when it reaches the maximum value, the counter rolls over back to zero.

3.3.4 Integrity Check Value Calculation

If authentication is selected for the SA, the sender computes the ICV over the ESP packet minus the Authentication Data. Thus the SPI, Sequence Number, Payload Data, Padding (if present), Pad Length, and Next Header are all encompassed by the ICV computation. Note that the last 4 fields will be in ciphertext form, since encryption is performed prior to authentication.

For some authentication algorithms, the byte string over which the ICV computation is performed must be a multiple of a blocksize specified by the algorithm. If the length of this byte string does not match the blocksize requirements for the algorithm, implicit padding MUST be appended to the end of the ESP packet, (after the Next Header field) prior to ICV computation. The padding octets MUST have a value of zero. The blocksize (and hence the length of the padding) is specified by the algorithm specification. This padding is not transmitted with the packet. Note that MD5 and SHA-1 are viewed as having a 1-byte blocksize because of their internal padding conventions.

3.3.5 Fragmentation

If necessary, fragmentation is performed after ESP processing within an IPsec implementation. Thus, transport mode ESP is applied only to whole IP datagrams (not to IP fragments). An IP packet to which ESP has been applied may itself be fragmented by routers en route, and such fragments must be reassembled prior to ESP processing at a receiver. In tunnel mode, ESP is applied to an IP packet, the payload of which may be a fragmented IP packet. For example, a security gateway or a "bump-in-the-stack" or "bump-in-the-wire" IPsec implementation (as defined in the Security Architecture document) may apply tunnel mode ESP to such fragments.
NOTE: For transport mode -- As mentioned at the beginning of Section
3.1, bump-in-the-stack and bump-in-the-wire implementations may haveto first reassemble a packet fragmented by the local IP layer, thenapply IPsec, and then fragment the resulting packet.
NOTE: For IPv6 -- For bump-in-the-stack and bump-in-the-wire implementations, it will be necessary to walk through all the extension headers to determine if there is a fragmentation header and hence that the packet needs reassembling prior to IPsec processing.