计算机网络安全技术

- 课程代号：*40240572*
- 课程对象：本科生
- 授课教师：尹　霞
- 开课单位：计算机系网络所

互联网安全协议

IPsec：IP+安全

- 概述
- 体系结构
- 认证头AH
- 封装安全载荷ESP
- 安全关联组合

IKE管理密钥

- 报文格式、体系结构
- 工作模式、工作过程

网络层安全协议

- **IPsec**：IP+安全
- **IKE**：IPsec管理密钥

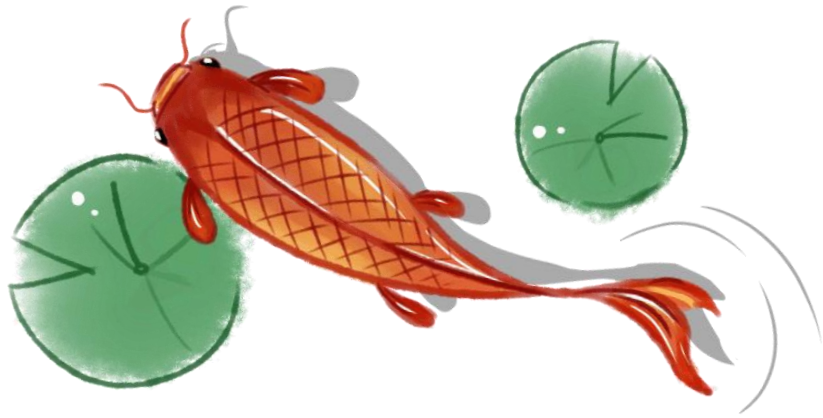
传输层安全协议

- **SSL**：为应用层服务

应用层安全协议

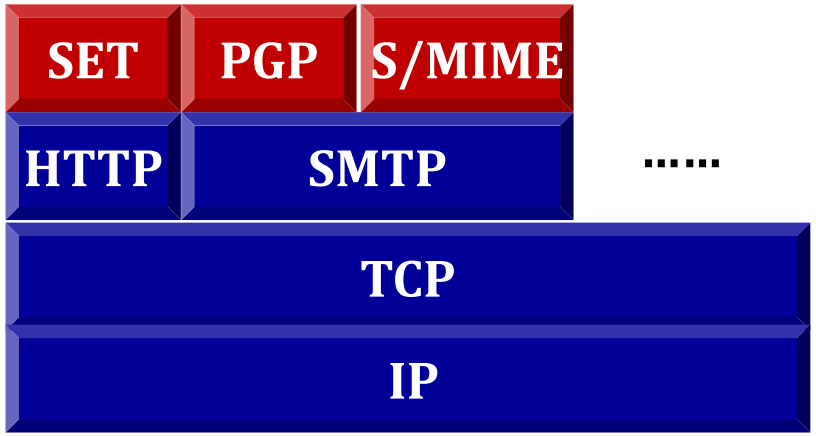
- **HTTPS**：HTTP+SSL
- **S/MIME**：安全电子邮件
- **SET**：安全电子交易

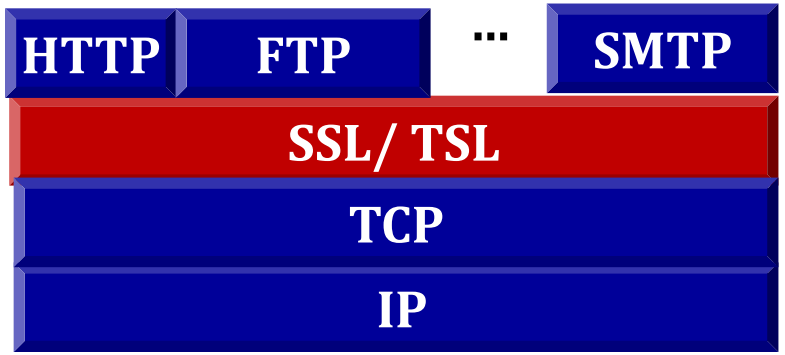
网络层安全协议：IPsec

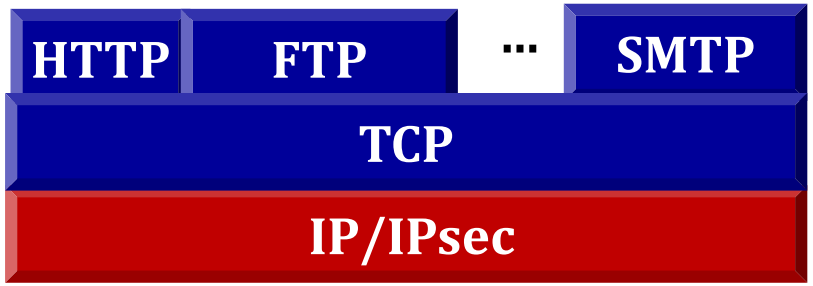


安全通信协议

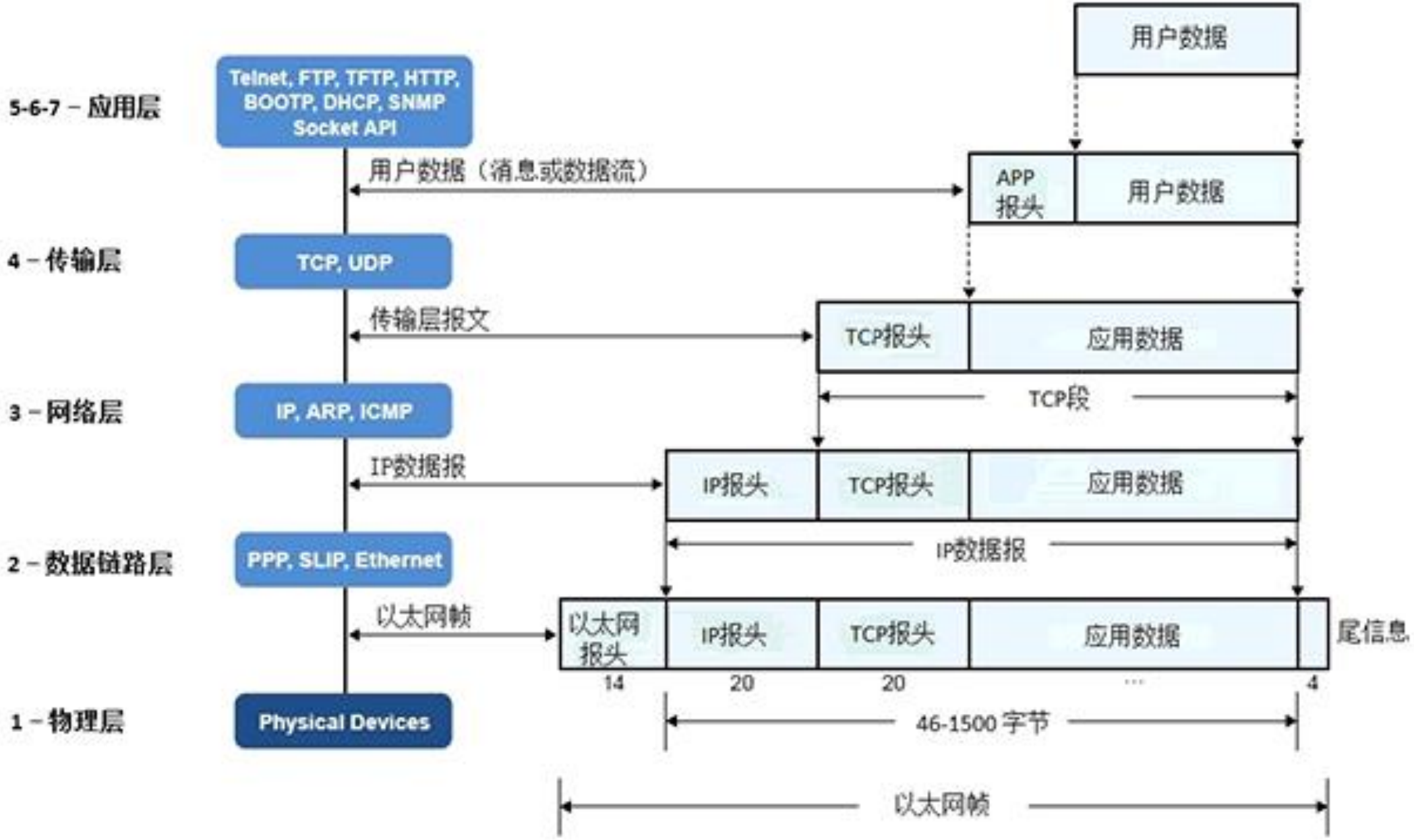
- 应用层
  - S/MIME
  - PGP
  - SET
- 传输层
  - SSL
  - TSL
- 网络层
  - IPSec







互联网的数据流


5-6-7 – 应用层
Telnet, FTP, TFTP, HTTP, BOOTP, DHCP, SNMP Socket API
用户数据
用户数据（消息或数据流）
APP 报头
用户数据
4 – 传输层
TCP, UDP
传输层报文
TCP报头
应用数据
TCP段
3 – 网络层
IP, ARP, ICMP
IP数据报
IP报头
TCP报头
应用数据
IP数据报
2 – 数据链路层
PPP, SLIP, Ethernet
以太网帧
以太网报头
IP报头
TCP报头
应用数据
尾信息
14
20
20
...
4
1 – 物理层
Physical Devices
46-1500 字节
以太网帧

IP级安全性

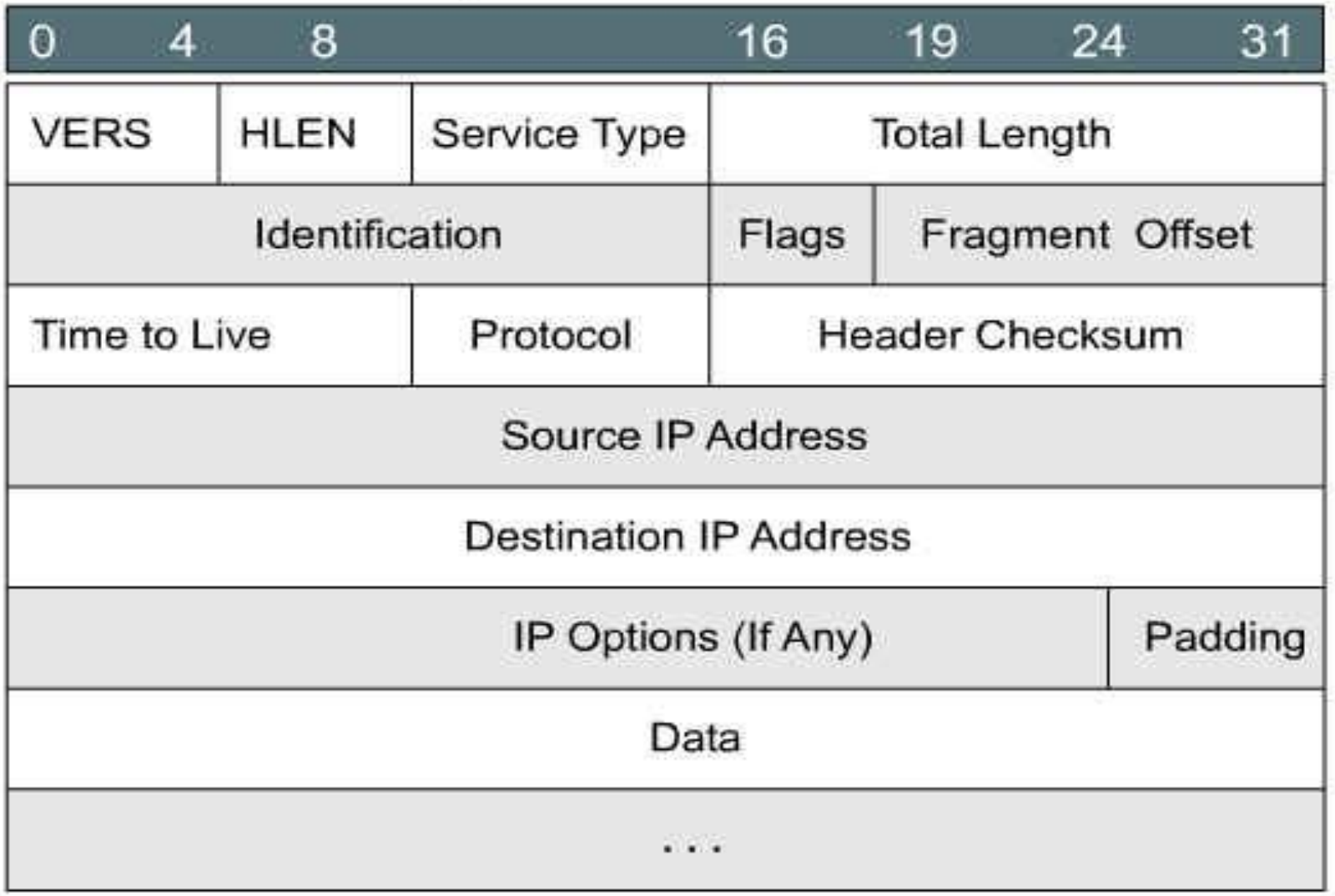
- IPsec保障了IP级的安全性，包括：
  - 认证：确保收到的包是从包头标识的源端发出的，而且该包在传输过程中未被篡改
  - 保密：将报文加密后传输，防止第三方窃听
  - 密钥管理：密钥管理机制与密钥的安全交换相关

现有IP协议的安全特性

- 无连接，不保证顺序到达；存在着重复包、丢失包；设备简单、无状态
- 所提供的安全服务
  - 认证：无
  - 完整性：无
  - 保密：无
  - 访问控制：基于IP地址，但是不完备
- 所面临的威胁
  - 窃听、伪造IP地址、篡改、重发

IP Packet

- IP 协议是无状态、无连接的
- IP数据报由20个字节的报头和来自传输层的数据构成



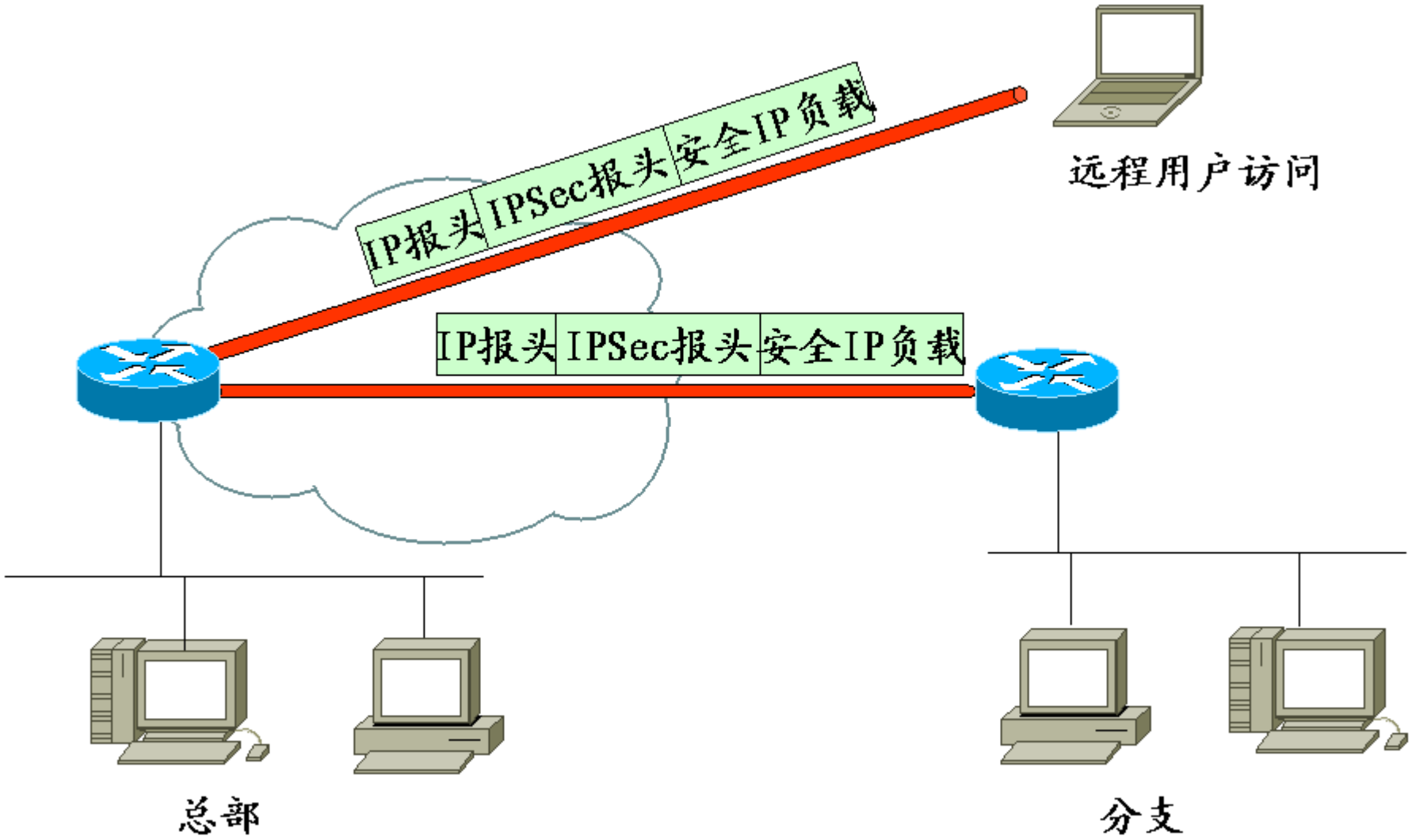
IPSec的历史

- 1994年，互联网体系结构委员会IAB 发布了RFC1636---“Internet 体系结构中的安全性”，明确指出大多数人认为互联网需要更多更好的安全性
- IAB认为应该在网络层实现端到端的安全性
  - 数据源认证机制
  - 数据加密机制
  - 密钥管理
- **IPSec的原理在于可以在IP层加密和/或认证所有流量**
  - 这些安全能力在IPv4和IPv6中都适用

IPSec 的应用

- IPSec提供了在局域网、广域网和互联网中安全通信的能力，其用途包括：
  - 分支机构通过互联网安全互联
    - 一个公司可以在公网上建立安全的虚拟专用网，减少了对专用网络的需求，节省了开销和网络管理费用
  - 远程安全访问互联网
    - 使用了IPsec的终端用户可以通过互联网获得对公司网络的安全访问，减少了雇员上班和远程通信的费用
  - 与合作者建立外联网和内联网联系
    - IPSec为不同组织之间提供安全通信，确保认证、保密和密钥交换
  - 加强电子商务安全性

IPSec 的应用：虚拟专用网VPN

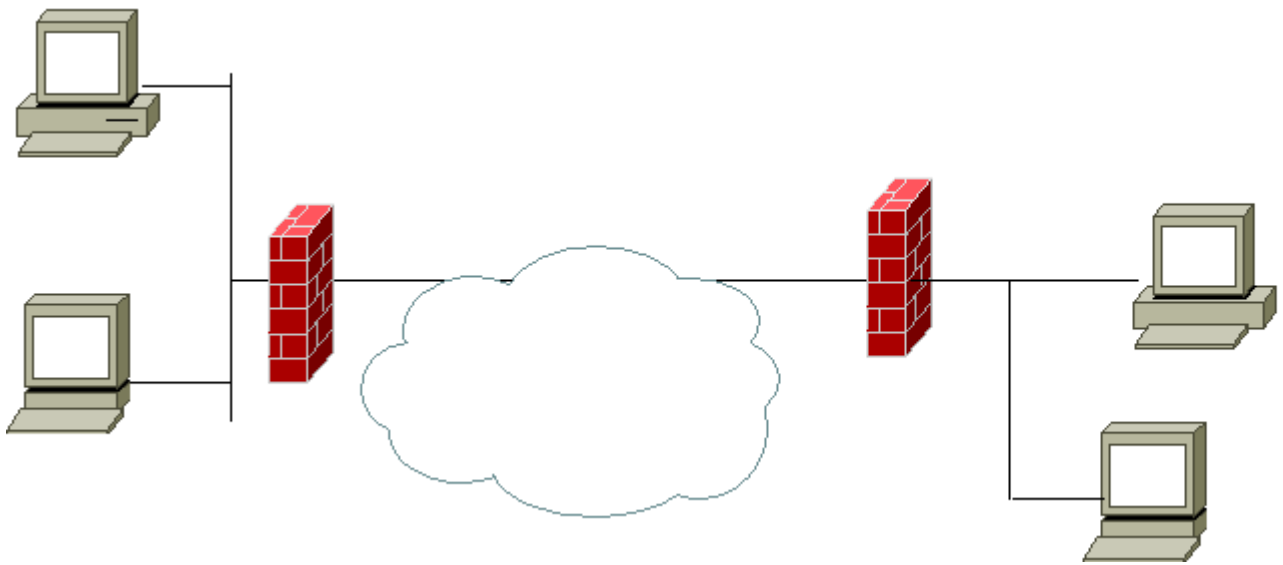


IPSec的实施：主机

- 在主机上实现（与操作系统集成）
  - 保障端到端的安全
  - 能够针对用户的每个会话提供安全保障
  - 对应用透明，不必修改用户或服务器系统的软件
  - IPSec可以对最终用户透明

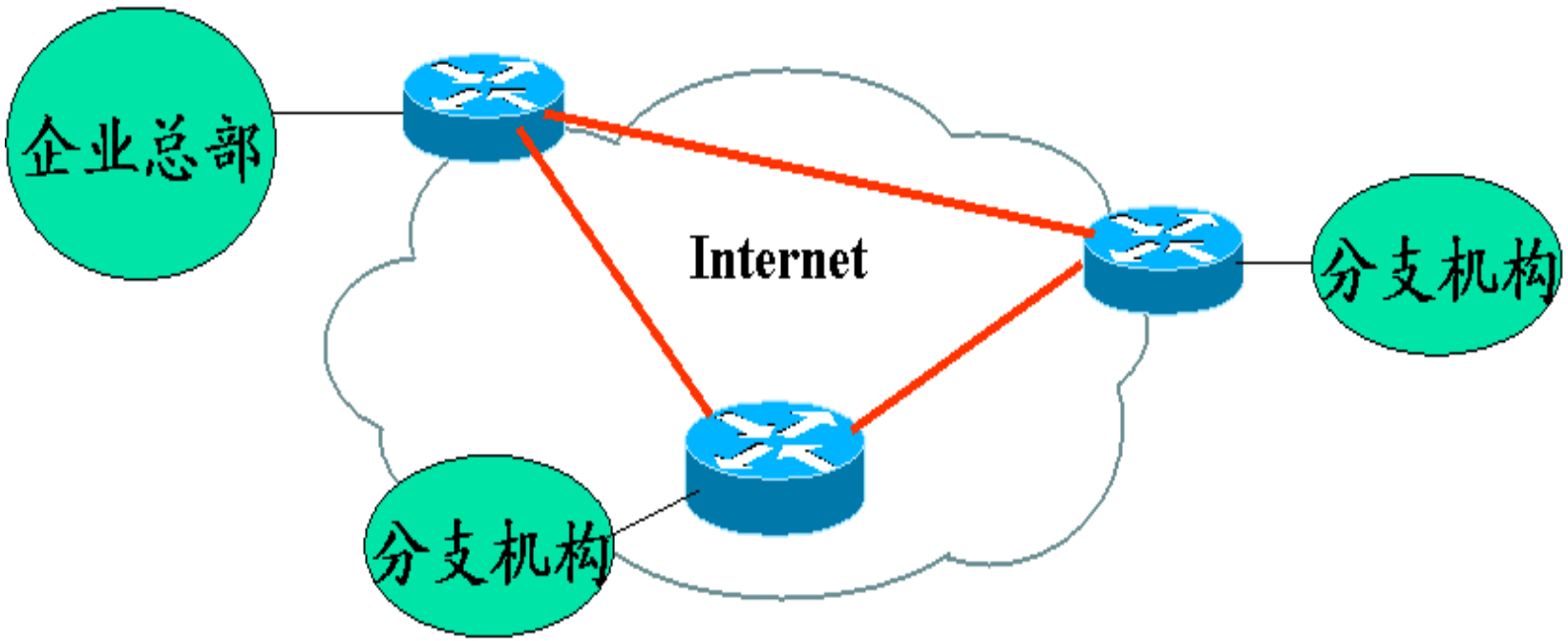
IPSec的实施：防火墙

- 在防火墙上实施
  - 无须改变操作系统
  - 为内部所有的应用提供安全服务



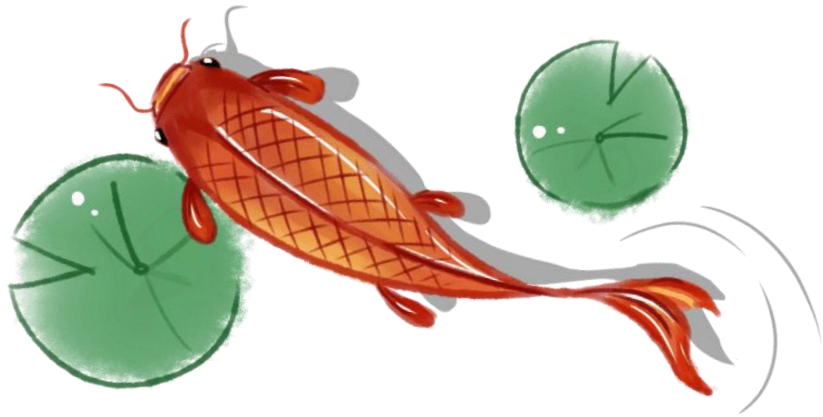
IPSec的实施：路由器

- 在路由器上实施，虚拟专用网(Virtual Private Network， VPN)：可以对通过公用网络在两个子网之间流动的数据提供安全保护

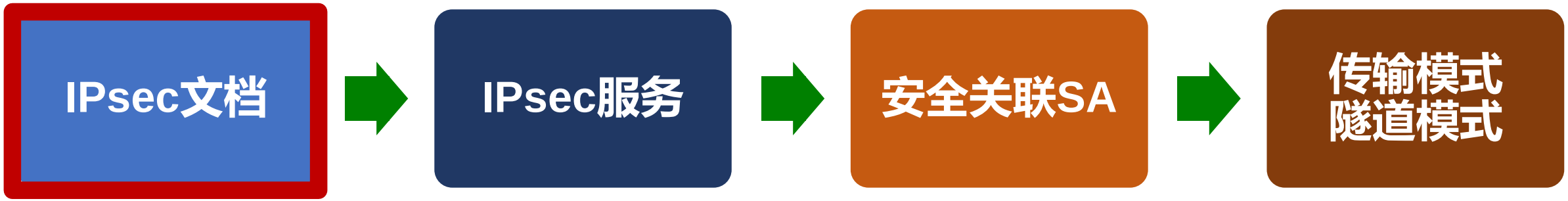


IPSec：体系结构

- 文档、服务、安全关联、传输模式和隧道模式



IPSec 体系结构

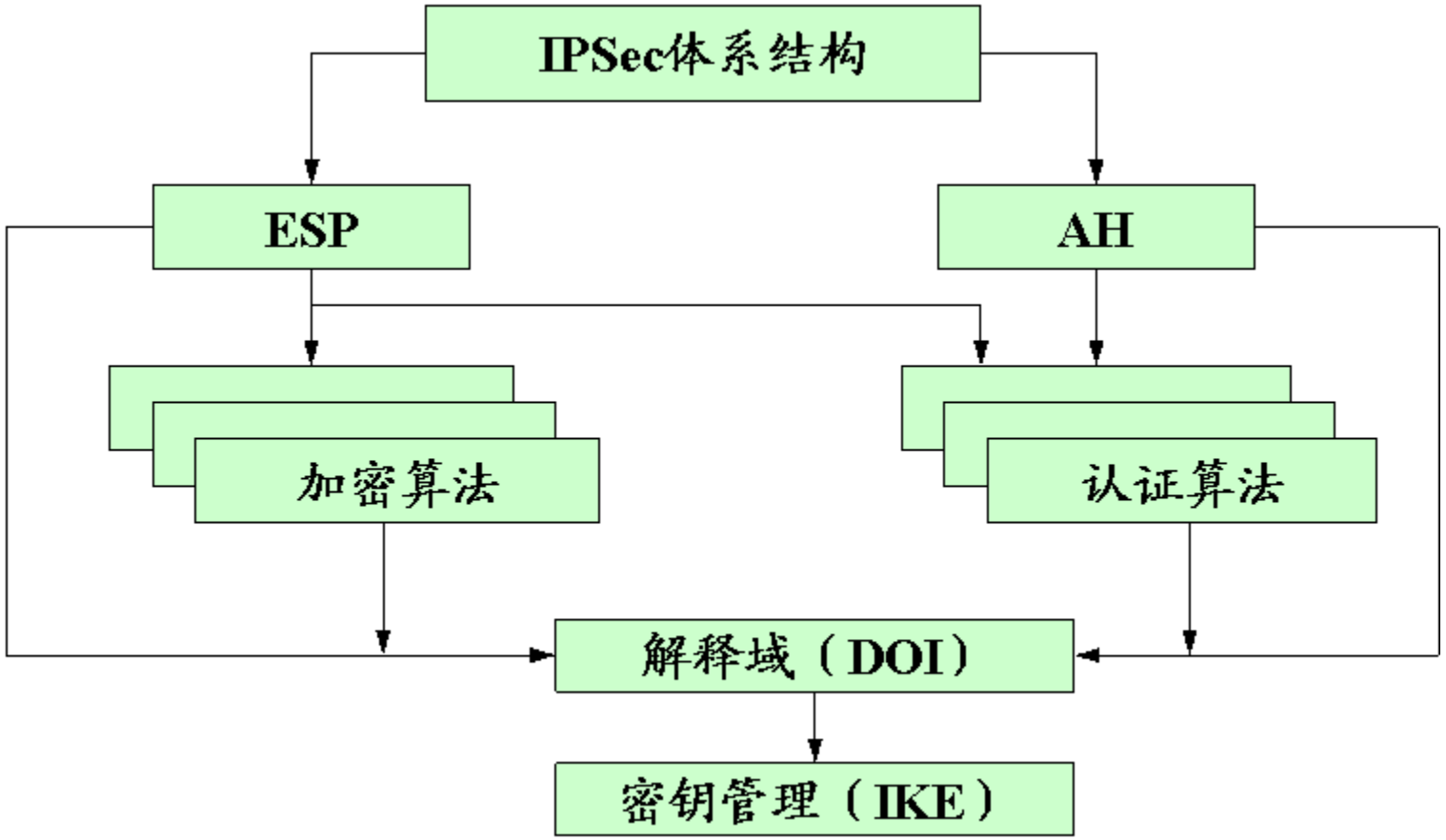


IPSec文档

- IPSec有很多文档，重要的有1998年发布的RFC 2401/2402/2406/2408
  - RFC 2401：安全结构概述
  - RFC 2402：IP扩展的包认证描述（IPv4和IPv6）
  - RFC 2406：IP扩展的包加密描述（IPv4和IPv6）
  - RFC 2408：特定加密机制
- IPv6必须支持这些特性，IPv4可选；包认证和包加密都是在主IP报头中使用了扩展报头实现安全特性
  - 包认证的扩展报头称为认证头AH（Authentication Header）
  - 包加密的扩展报头称为封装安全载荷ESP（Encapsulating Security Payload）

IPSec文档

- 除了上述四个文档，IETF下设的IP安全协议工作组又做了大量的工作，整个IPSec 文档被分成七个部分



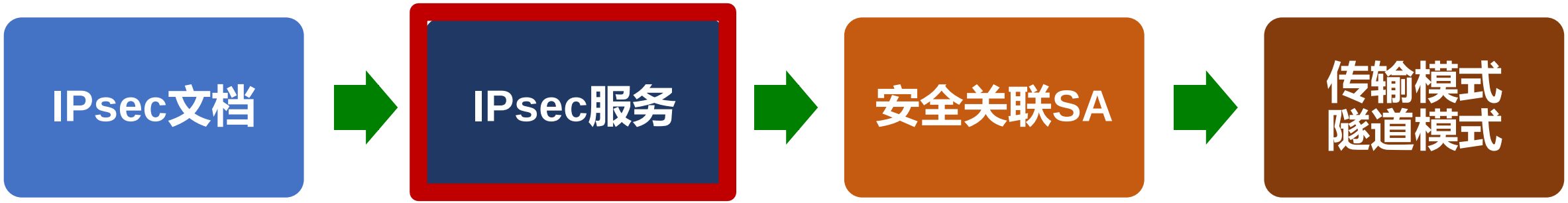
IPSec文档

- 整个IPSec 文档被分成七个部分：
  - 体系结构：
    - 定义IPSec技术的一般性概念、需求和机制
  - 认证头AH：
    - IP 数据包中的一个扩展域，用于提供数据的源发认证和完整性保护
  - 封装安全载荷ESP ：
    - IP 数据包中的一个扩展域，用于提供数据保密、源发认证和完整性保护
  - 加密算法
    - 一系列描述ESP中使用的各种加密算法的文档
    - RFC2405, The ESP DES-CBC Cipher Algorithm With Explicit IV

IPSec文档

- 整个IPSec 文档被分成七个部分：
  - 认证算法
    - 一系列描述AH中使用的各种认证算法和ESP认证选项的文档
    - RFC2403，The Use of HMAC-MD5-96 within ESP and AH
      RFC2404，The Use of HMAC-SHA-1-96 within ESP and AH
  - 密钥管理
    - 描述密钥管理模式的文档
  - 解释域（DOI）
    - 其他文档需要的为了彼此间互相联系的一些值，包括经过检验的加密和认证算法的标识以及操作参数，比如密钥的生存期

IPSec 体系结构



IPSec提供的服务

- IPSec在IP层提供安全服务，系统可以选择所需要的安全协议，确定该服务所用的算法，并提供安全服务所需加密密钥

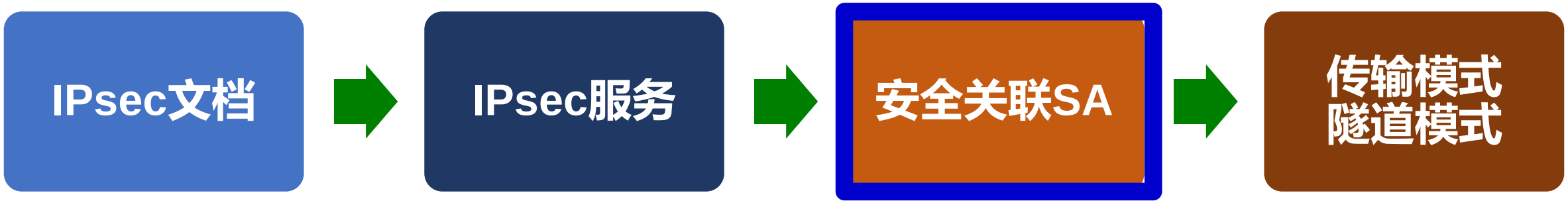
- 使用AH协议报头的认证协议和为数据包设计的加密/认证协议ESP，提供安全性
  - ESP可以分成支持和不支持认证两种
  - AH和ESP均支持基于分布密钥的访问控制，而流量管理则与加密协议相关

IPSec提供的服务

- 它们提供的安全服务包括：
  - 访问控制
  - 无连接完整性
  - 数据源发认证
  - 拒绝重放数据包
  - 保密性（加密）
  - 有限的信息流保密性

	AH	ESP(只加密)	ESP(加密并认证)
访问控制	✓	✓	✓
无连接的完整性	✓		✓
数据源发认证	✓		✓
检测重放攻击	✓	✓	✓
机密性		✓	✓
有限的通信流保密		✓	✓

IPSec 体系结构



安全关联

- IP认证和保密机制中的一个核心概念是安全关联SA（Security Association）
- 安全关联SA是IPsec通信双方之间对某些要素的一种协商，一组安全信息参数集合，包括：
  - 协议、操作模式、密码算法、认证算法、密钥、密钥生存期等
- 关联是发送方和接收方之间的单向关系，该关联为双方的通信提供了安全服务
  - 如果需要双方安全交换，则建立两个安全关联
  - 安全服务可由AH或者ESP提供，但不能两者都提供

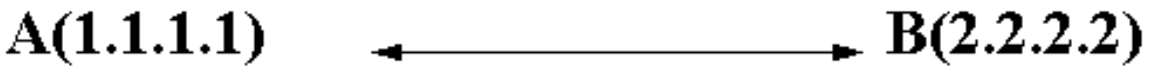
安全关联

- 一个安全关联SA由三个参数唯一确定：
  - 安全参数索引SPI(Security Parameters Index)
    - SPI是一个和SA相关的位串，仅在本地有意义
    - SPI由AH和ESP携带，使得接收方能够选择合适的SA处理接收包
  - IP 目的地址IPDA
    - 只允许使用单一地址，表示SA的目的地址，

      可以是用户末端系统、防火墙或者路由器
  - 安全协议标识
    - 标识该关联是一个AH安全关联或ESP安全关联

安全关联

- 在任何IPSec实现中，都有一个安全关联数据库SADB，它定义了与每个SA相关联的参数



source	dst	protocol	spi	SA记录
1.1.1.1	2.2.2.2	AH	11	MD5, K1
2.2.2.2	1.1.1.1	ESP	12	DES, K2
2.2.2.2	1.1.1.1	AH	13	SHA, K3

A的 SADB

安全关联数据库SADB

- 安全关联数据库SADB中包含现行所有SA条目，每个SA由包含【SPI，IPDA，AH/ESP】三元组索引
- SAD中的安全关联参数包括：
  - Sequence Number Counter
  - Sequence Counter Overflow
  - Anti-Replay Window
  - AH Authentication algorithm, keys, etc
  - ESP Encryption algorithm, keys, IV mode, IV, etc
  - ESP authentication algorithm, keys, etc
  - Lifetime of this Security Association
  - IPsec protocol mode
  - Path MTU

SA的参数（1）

- 序列号计数器（必须实现）
  - 一个32位整数，刚开始通常为0，用于生成AH或ESP头中的序列号域
  - 每次用SA保护一个包时增1；在溢出之后，SA会重新进行协商
- 序列号溢出标志（必须实现）
  - 表明序列号计数器是否溢出，
  - 序列号计数器的溢出时，该值为1时，产生审查事件并阻止该SA继续下发数据包
- 反重放窗口（必须实现）
  - 用于决定输入AH或ESP报文是否是重放的32位计数器
- AH信息组（AH必须实现）
  - 认证算法，密钥，密钥生存期和AH的相关参数

SA的参数（2）

- ESP信息组（ESP必须实现）
  - 加密和认证算法，密钥，初始值，密钥生存期和ESP的相关参数
- SA的生存期
  - 一个时间间隔或字节计数
  - 生存期结束时，SA必须终止，或用一个新的SA替换
- IPSec协议模式（必须实现）
  - 隧道模式或者传输模式
- Path MTU（必须实现）
  - 任何遵从的最大传送单位路径和迟滞变量

安全关联数据库SADB的工作过程

- 在IP数据包中，安全管理SA由IPv4或IPv6报头中的目的地址唯一标识，SPI被封装在AH或者ESP扩展头中
- 任何IPSec实现中都必须实现安全关联数据库SADB；对于收到的数据包，解析出三元组【SPI、目的地址、AH /ESP】，并据此查找SADB：
  - 如果查找到一个匹配的SA条目，则将该SA的参数与AH或ESP头中相关域进行比较：参数相一致，就处理该数据包；参数不一致，就丢弃该数据包
  - 如果没有查找到匹配的SA条目：如果数据包是输入包，丢弃：如数据包是输出包，将创建一个新的SA，并将其存入SADB中

SA选择子

- IPSec提供了多种方式在IP通信中实现IPSec服务，用户可根据自己的意愿进行配置
- IPSec对需要IPSec保护的流量和不需要IPSec保护的流量进行了大粒度区分
- IP流量与特定SA相关是通过安全策略数据库SPDB定义的
  - SPDB至少应该包括定义IP流量子集的入口、指向该流量SA的指针
- 更复杂的情况是：
  - 多个入口可以与一个SA相连
  - 多个SA与一个SPDB入口相连

SA选择子

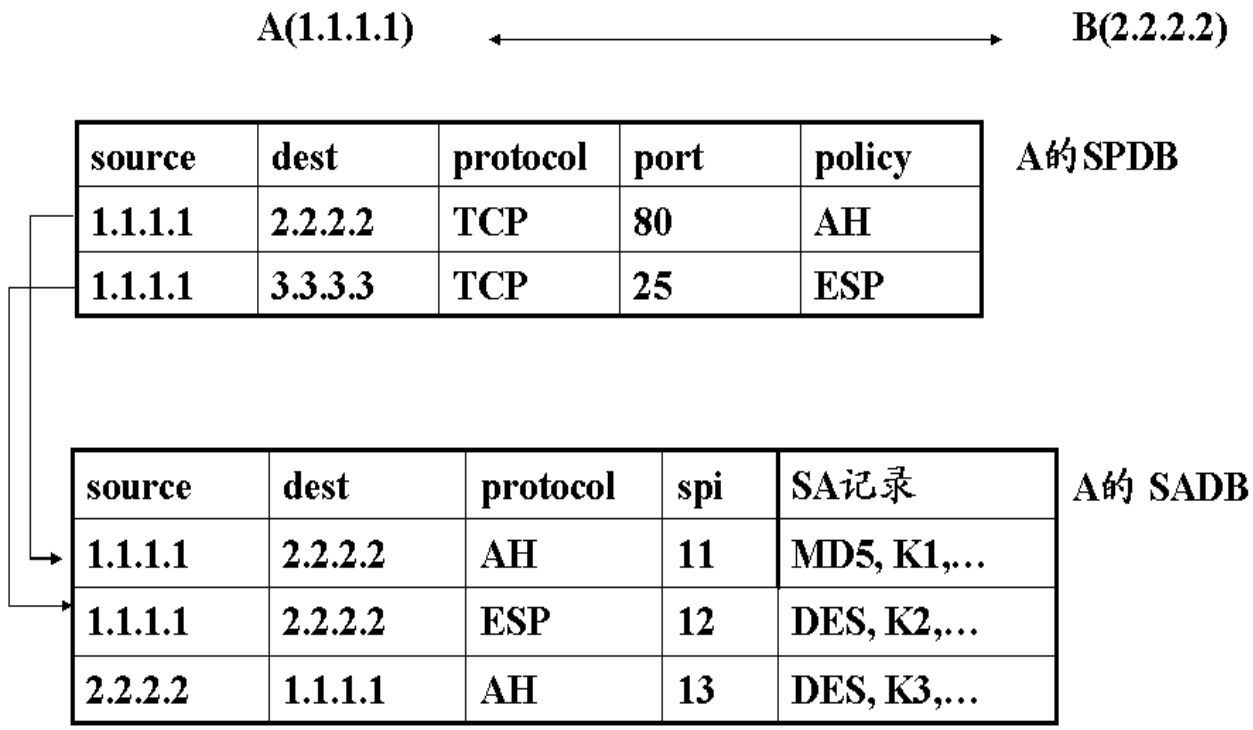
- 每个SPDB入口由一个IP集合和上层协议定义，称为选择子(SA selector)
  - 选择子用于过滤输出流量，并将它们映射到某个特定的SA
- 每个IP包的输出过程如下：
  - 在SPDB中比较相应域的值，寻找匹配的入口，可能是零或多个
  - 如果存在SA，则选定SA和其关联的SPI执行所需的IPSec处理（AH或ESP）
- SPDB入口由下列选择子确定
  - 目的IP地址、源IP地址
  - 用户标识
  - 数据敏感性级别
  - 传输层协议
  - IPSec协议
  - 源端口和目的端口
  - IPv6报类
  - IPv6报流标签
  - IPv6报服务类型

安全策略数据库SPBD

- 在IPSec中，安全策略通过SPDB来定义、标识、管理和维护
- SPDB中的每个元组都定义了要保护的数据包以及如何保护
- 对于数据包的操作策略包括：
  - Discard：不让这个包进入或外发
  - bypass IPsec：不对进入或外发的数据包进行安全服务
  - apply IPsec：对外发的数据包提供安全服务，同时认为接收的数据包已经进行过安全服务

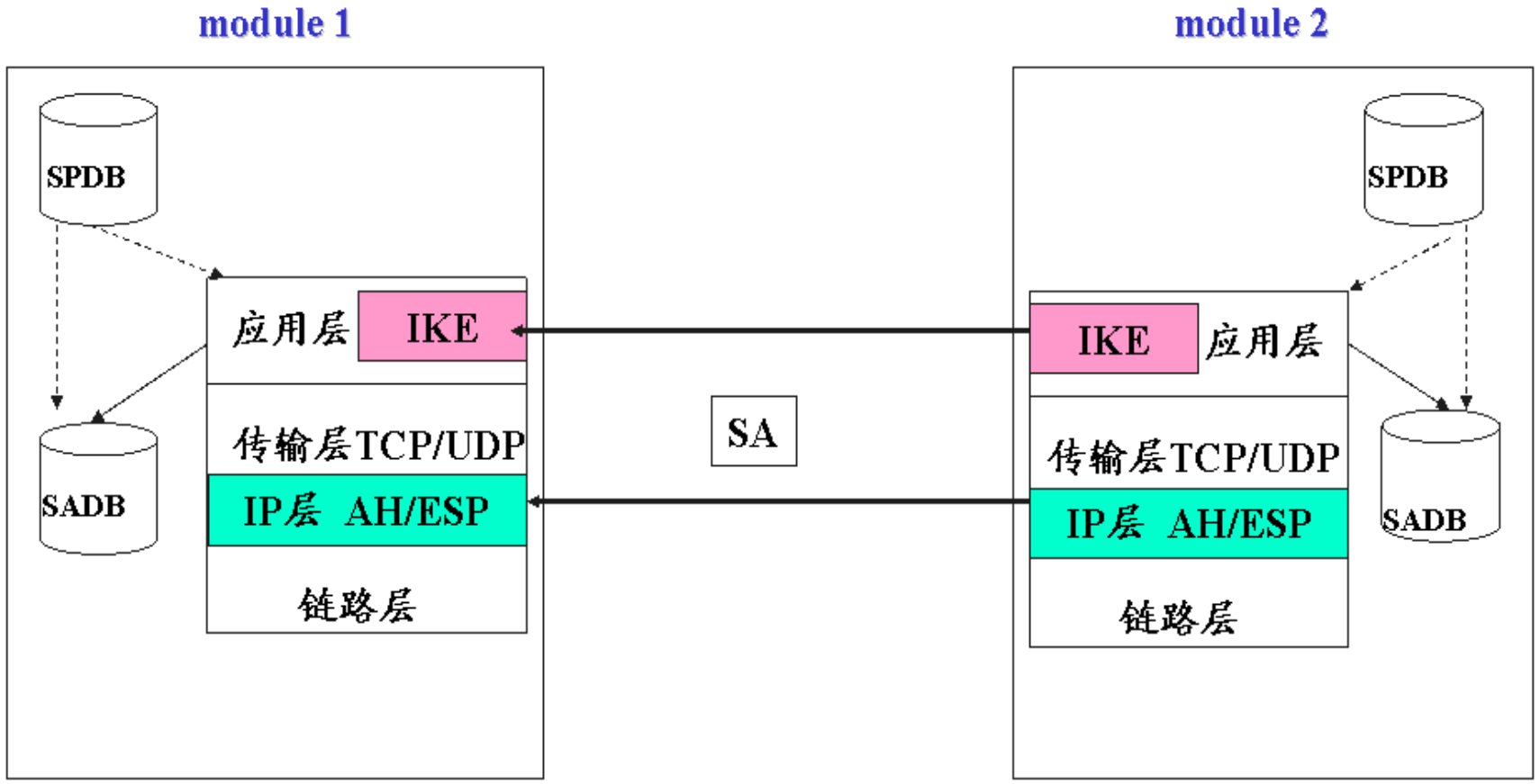
与SA相关的两个数据库

- IPSec的安全通信之前必须建立安全关联SA
- 安全关联数据库(SADB)：
  SA存储在本地的安全关联数据库(SADB)中，定义了与每个SA相关联的参数，决定了进行何种安全操作
- 安全策略数据库(SPBD)：
  SPDB是把IP信息流与SA联系起来的手段，决定了对流入和流出的哪些数据包进行安全操作(认证或加密/解密)

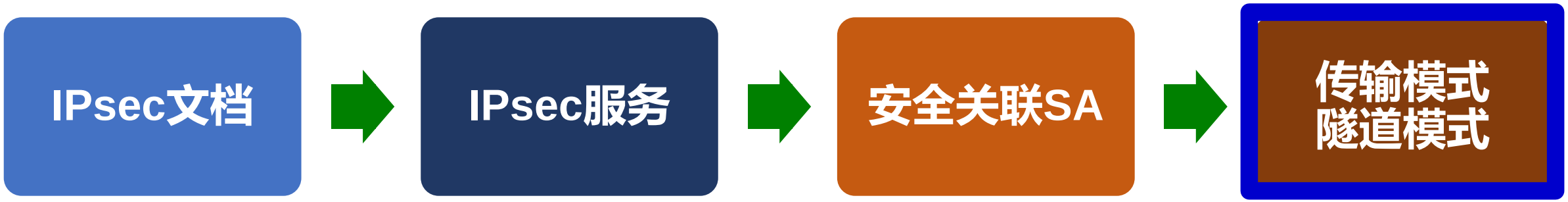


与SA相关的两个数据库

- 安全关联数据库(SADB)：定义SA
- 安全策略数据库(SPBD)：使用SA



IPSec 体系结构

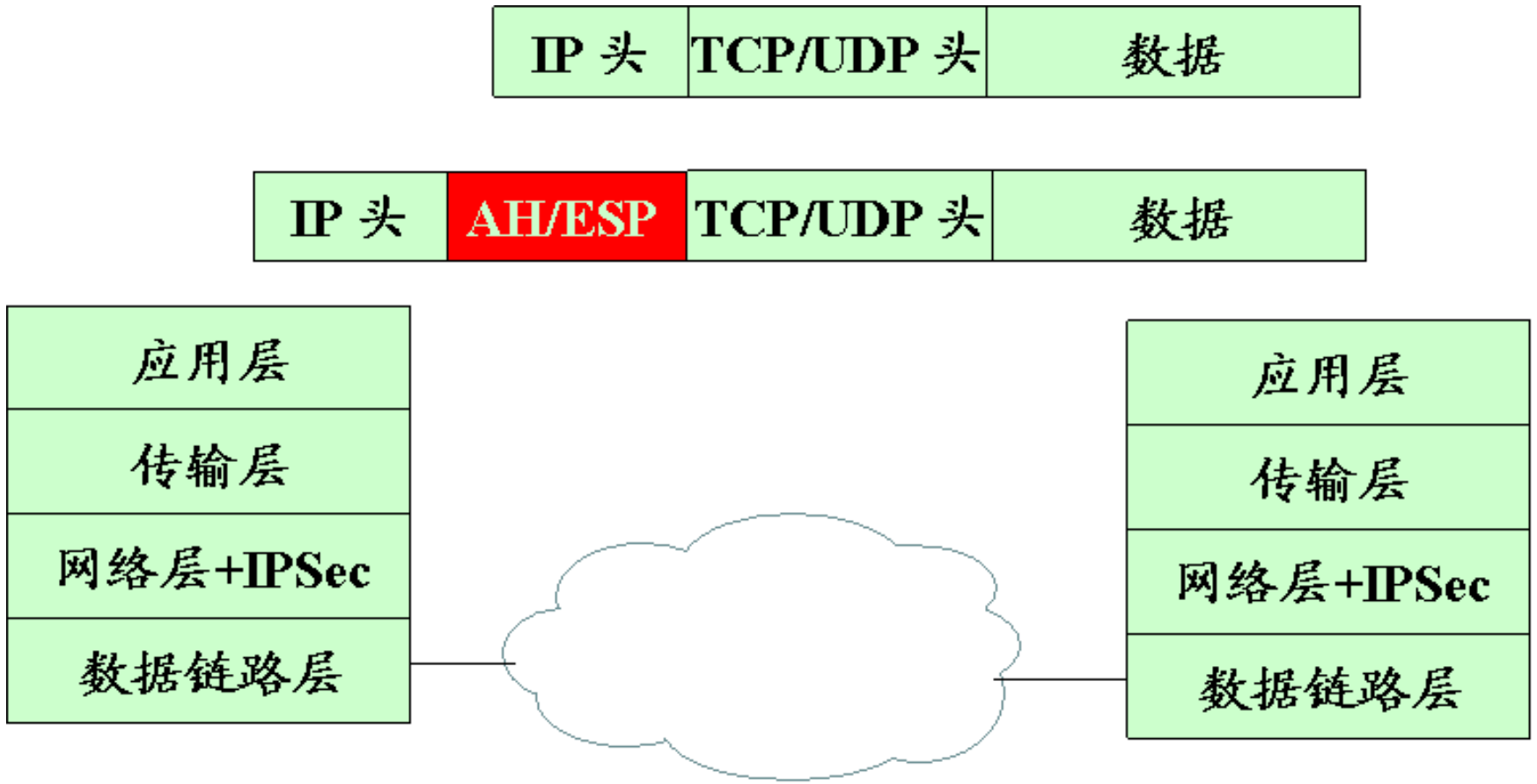


传输模式和隧道模式

- AH和ESP均支持两种模式：传输模式和隧道模式

- 传输模式(Transport Mode)主要为上层协议提供保护，同时增加了IP包载荷的保护
  - 典型的传输模式用于两台主机之间进行的端到端通信
  - 传输模式的ESP加密和认证（可选）IP载荷，不包括报头
  - 传输模式的AH认证IP载荷和报头的选中部分

传输模式

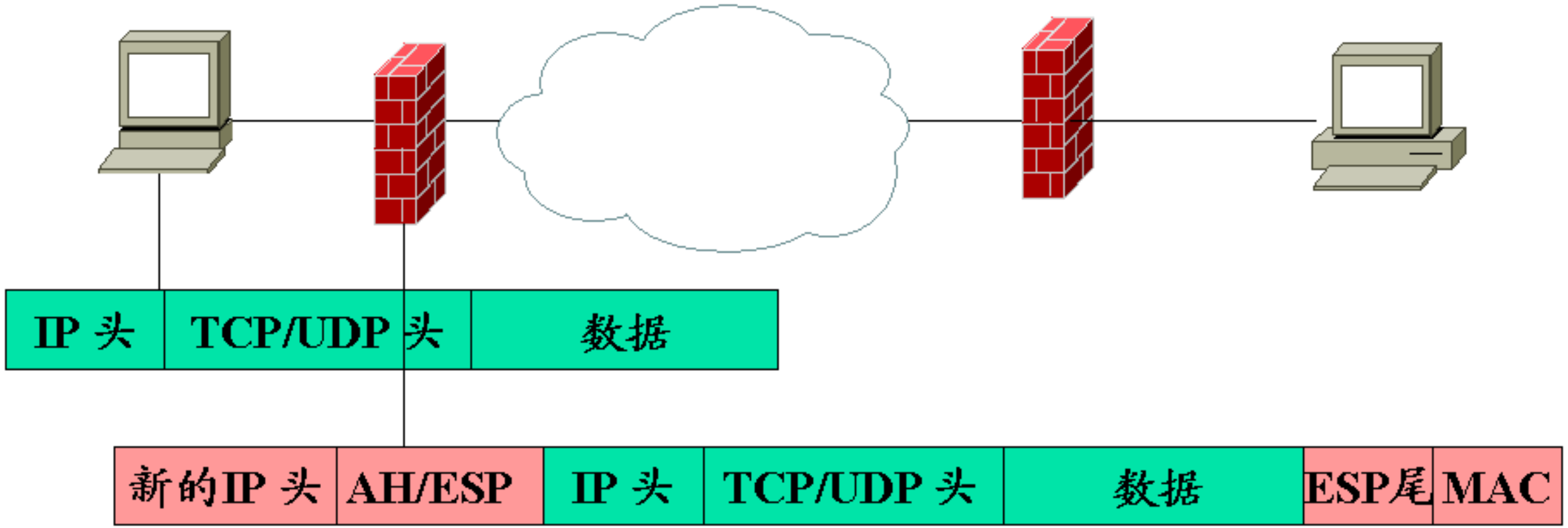

IP 头
TCP/UDP 头
数据
IP 头
AH/ESP
TCP/UDP 头
数据
应用层
传输层
网络层+IPSec
数据链路层
应用层
传输层
网络层+IPSec
数据链路层

隧道模式

- 隧道模式(Tunnel Mode)对整个IP包提供保护
  - 当IP包加上AH/ESP域后，整个数据包和安全域被当作一个新的IP载荷，并拥有一个新的外部IP报头
  - 新的IP数据包利用隧道在网络中传输，途中的路由器不能检查内部IP报头
  - ESP在隧道模式中加密和认证（可选）整个内部IP包，包括内部IP报头
  - AH在隧道模式中认证整个内部IP包和外部IP报头的选中部分

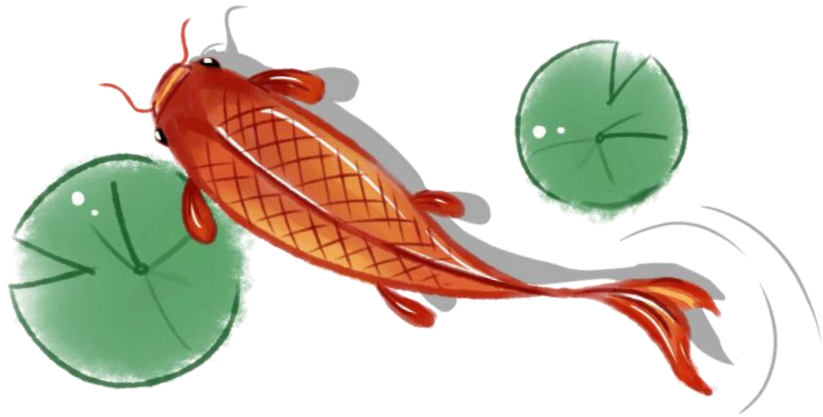
隧道模式

- 隧道模式（Tunnel Mode）
  - Firewall or Router



IPsec：认证头AH

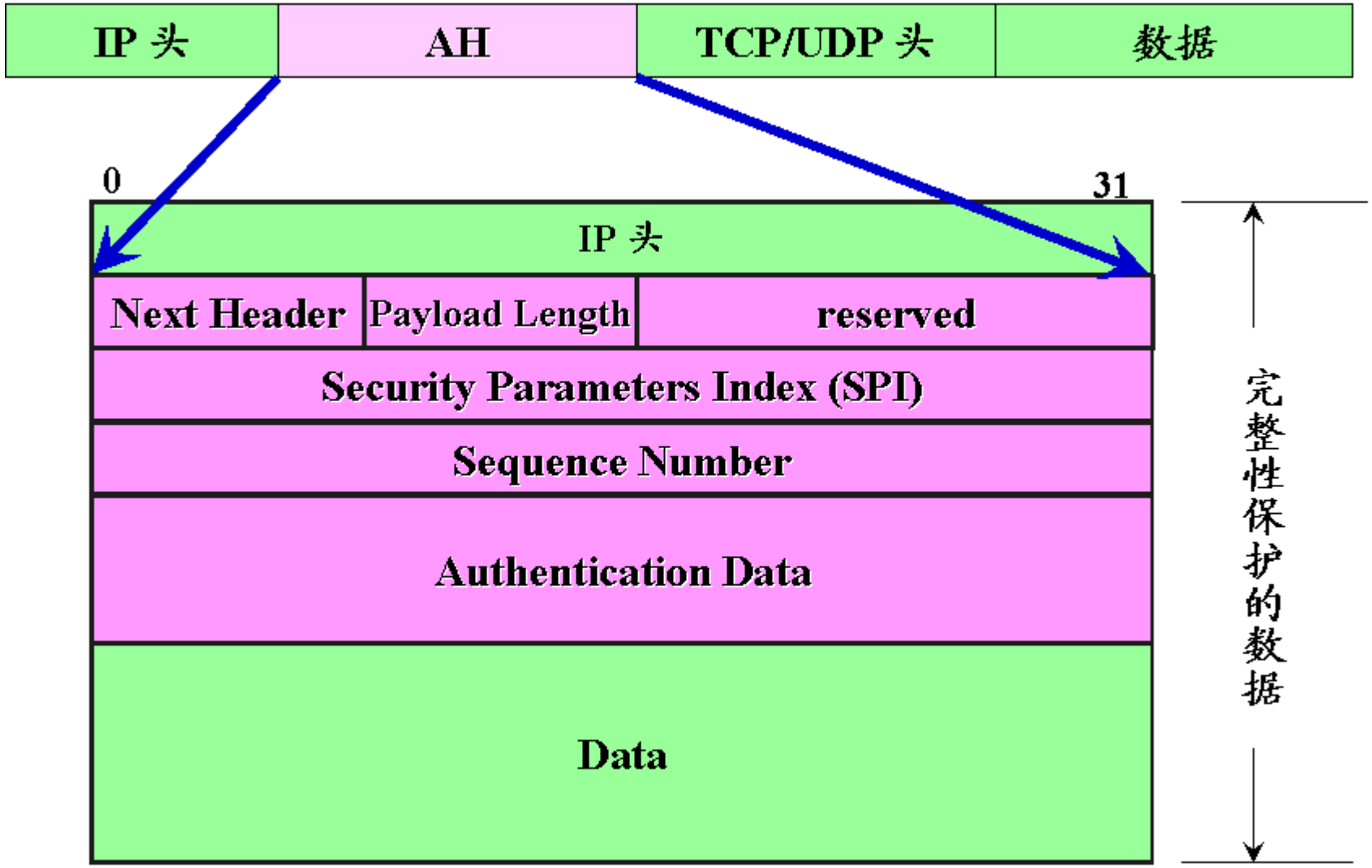
- *Authentication Header*



认证头Authentication Header

- 认证头AH支持数据完整性和IP包的认证
- 数据完整性确保在包的传输过程中内容不可更改
- 认证确保末端系统或者网络设备对用户或者应用程序进行认证，并提供相应的流量过滤功能，同时还能防止地址欺诈攻击和重放攻击
- 认证基于消息认证码MAC，双方必须共享一个公钥

认证头的组成


IP 头
AH
TCP/UDP 头
数据
0
31
IP 头
Next Header
Payload Length
reserved
Security Parameters Index (SPI)
Sequence Number
Authentication Data
Data
完整性保护的数据

认证头的组成（1）

- Next header(邻接头)
  - 8 bits，标识数据载荷中的封装方式或协议
  - 例如：TCP/UDP/ICMP、AH、ESP
- Payload length(有效载荷长度)
  - 8 bits，以 32 位字为单位的认证数据字段长度
- Reserved(保留字)
  - 16 bits，保留以供将来使用
  - 发送时必需设置为全零
    - 这个值包含在认证数据计算中，否则被接收方忽略

认证头的组成（2）

- Security Parameters Index (安全参数索引)
  - SPI为数据报识别安全联合的 32 位伪随机值，SPI=0被保留，表明“没有安全关联存在”
- Sequence Number(序列号)
  - 32bits，单调递增计数器，用于防范重放类型攻击
- Authentication Data(认证数据AD)
  - 变长域，必须是32 bits的整数倍
  - 包含完整性校验值ICV或者包的MAC

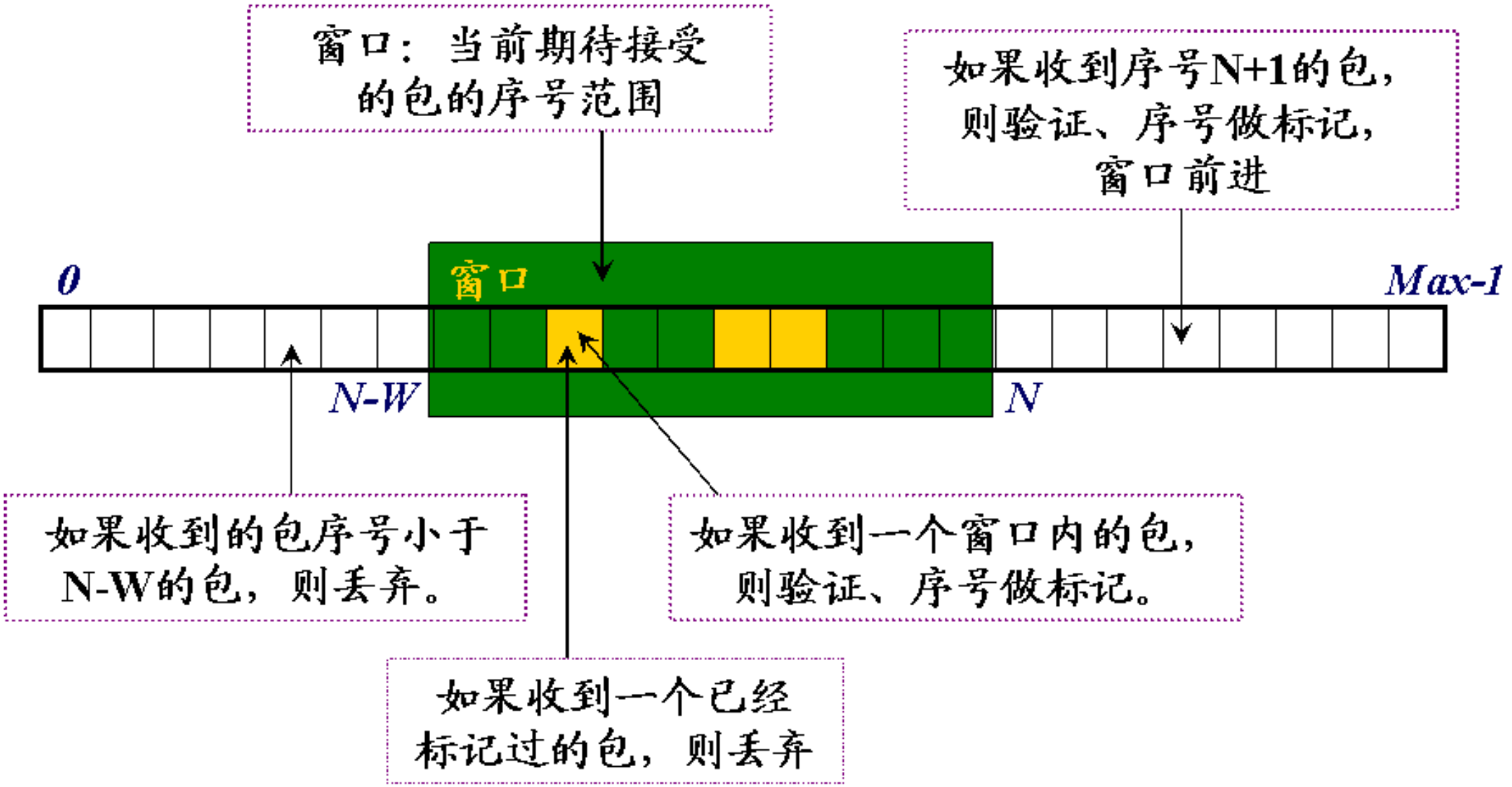
反重放攻击

- 重放攻击是指攻击者在得到一个经过认证的包后，又将其传送到目的站点的行为
- 重复接收经过认证的IP包可能会以某种方式中断服务或者产生不可预料的后果，序列号域就可以防止重放攻击
- 当建立了一个新的SA时，发送方将序列号初值设为0，每次在SA上发送一个包，则计数器加1并将值放入序列号域，则使用的第一个值就是1
- 发送方不允许循环计数，否则，同一个序列号就可以产生多个合法的包；如果该序列号到达$2^{32}-1$，则SA必须中止，用新的密钥协商声称新的SA

反重放攻击

- IP是无连接的，即不能保证包按照顺序传输，也不能保证所有的包均被传输；IPsec认证文档中声明，接收方应该实现一个大小为W的窗口（W的默认值为64）
- 窗口的右边界代表最大的序号N，记录目前收到的合法包的最大序列号，任何序列号在N-W+1到N之间的包均可以被正确接收，并标记窗口的正确位置
- 包到达之后：
  - 如果接收包在窗口中且是新包，则验证MAC；验证通过，则在窗口中标记位置
  - 如果接收的包超过窗口右边界而且是新包，则验证MAC；验证通过，则以这个序列号为窗口的右边界并在窗口中标记相应的位置
  - 如果接收包超过窗口的左边界或未通过验证，则丢弃此包，并生成审核事件

反重放攻击

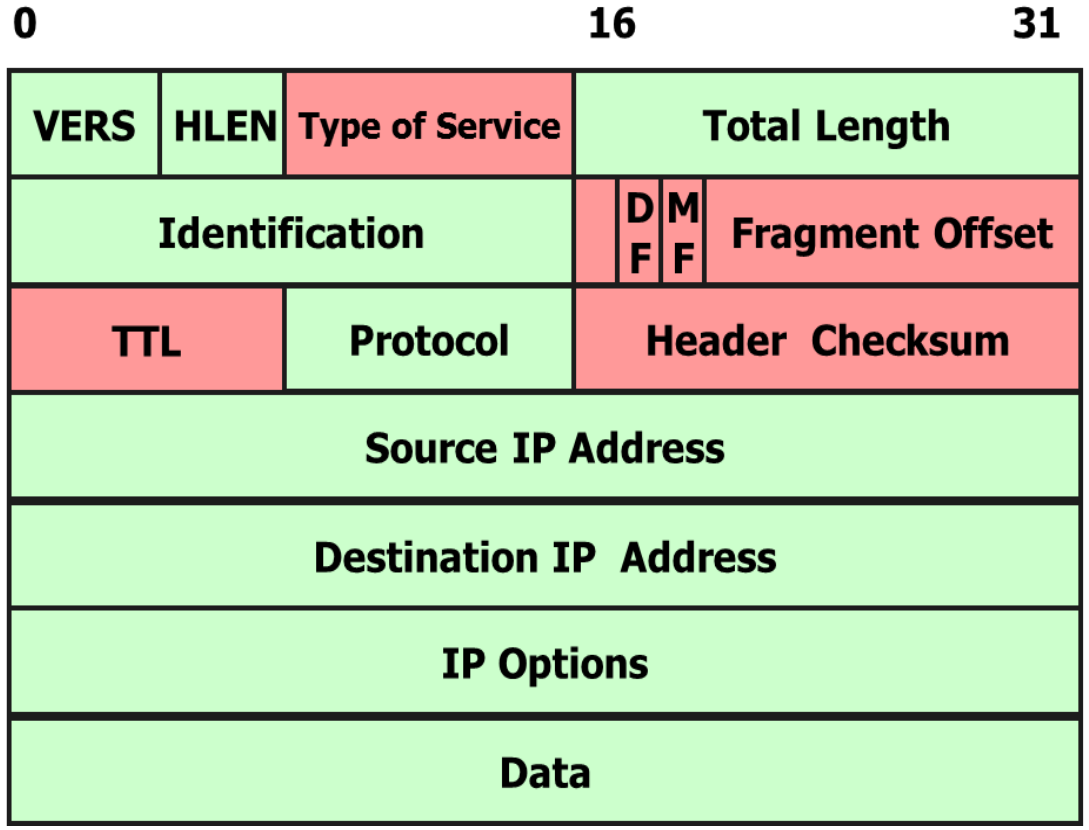

窗口：当前期待接受的包的序号范围
如果收到序号N+1的包，则验证、序号做标记，窗口前进
窗口
0
Max-1
N-W
N
如果收到的包序号小于N-W的包，则丢弃。
如果收到一个窗口内的包，则验证、序号做标记。
如果收到一个已经标记过的包，则丢弃

完整性校验值

- 认证数据AD域包含完整性校验值ICV，ICV是一种报文认证编码MAC或者MAC算法生成的截断代码
- 下面两种规范描述了ICV的生成：
  先计算全部的HMAC值，然后截取计算结果的前96bits
  - HMAC-MD5-96
  - HMAC-SHA-1-96

完整性校验值

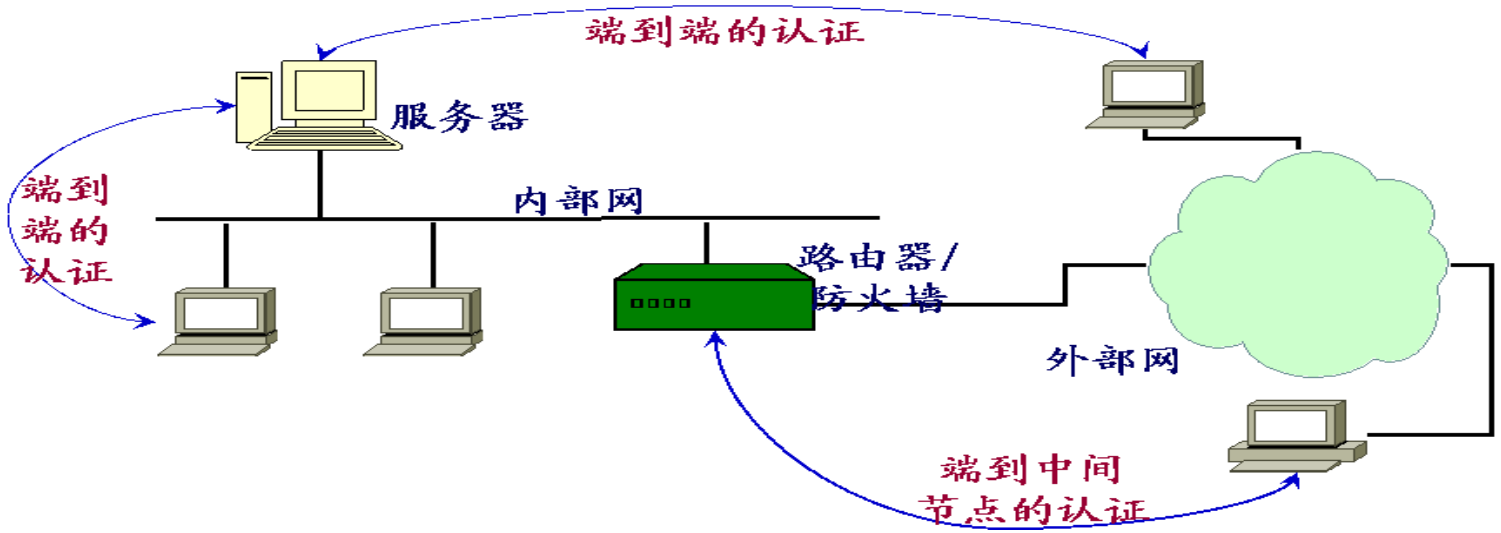
- 在以下字段计算MAC值：
  - IP报头：传输过程中不变的部分和AH SA终点可以预测的部分参与计算MAC
    对于可变部分和不可预测的部分全部置0，便于在源端和目的端计算
  - AH报头中不计算认证数据域；认证数据域被置成0，便于在源端和目的端计算
  - 整个上层协议数据，如TCP/UDP数据，假设在传输过程中不变



IPv4 Header 中的可变部分

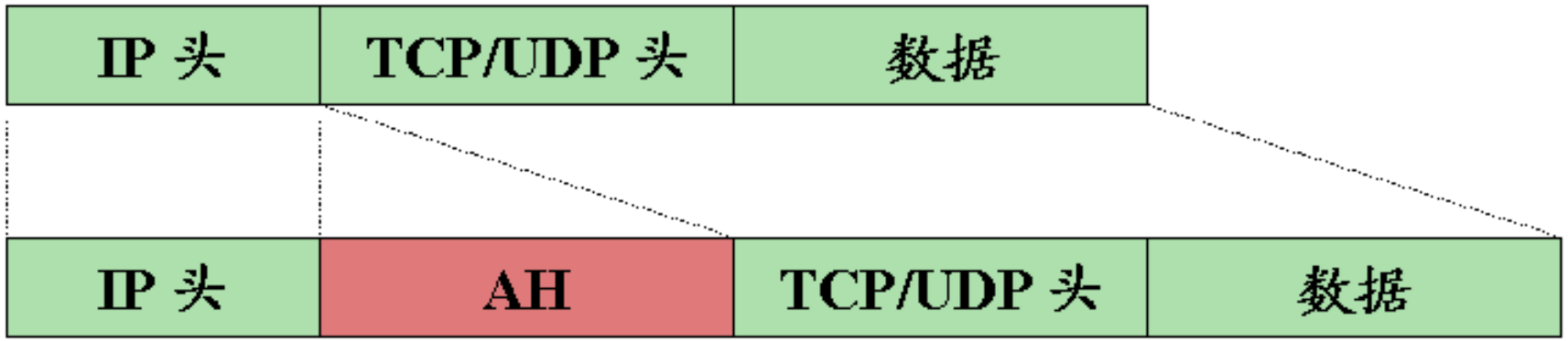
传输模式和隧道模式

- 有两种途径使用IPSec认证服务
  - 途径1：直接在服务器和客户工作站之间提供传输模式的认证
    - 客户工作站可以与服务器在同一个网络中，也可以在外部网络中
    - 只要客户工作站和服务器共享一个受保护的密钥，认证就是安全的
  - 途径2：在服务器不支持认证的情况下，远程工作站向防火墙证明自己身份，以便访问整个内部网络的时候，使用隧道模式SA



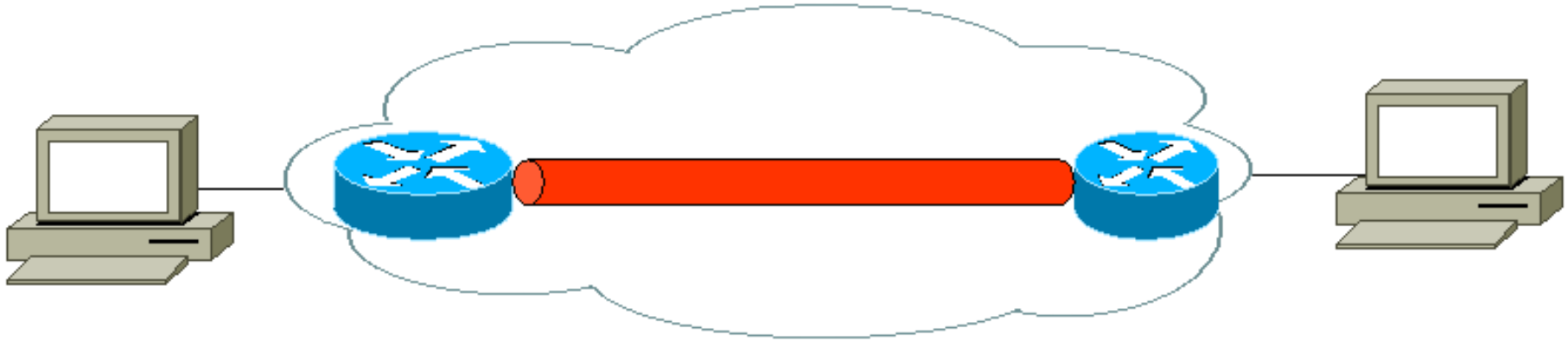
传输模式

- 传输模式
  - 通常以端到端方式实现（在主机上实现）
  - 不修改IP头，只添加AH头

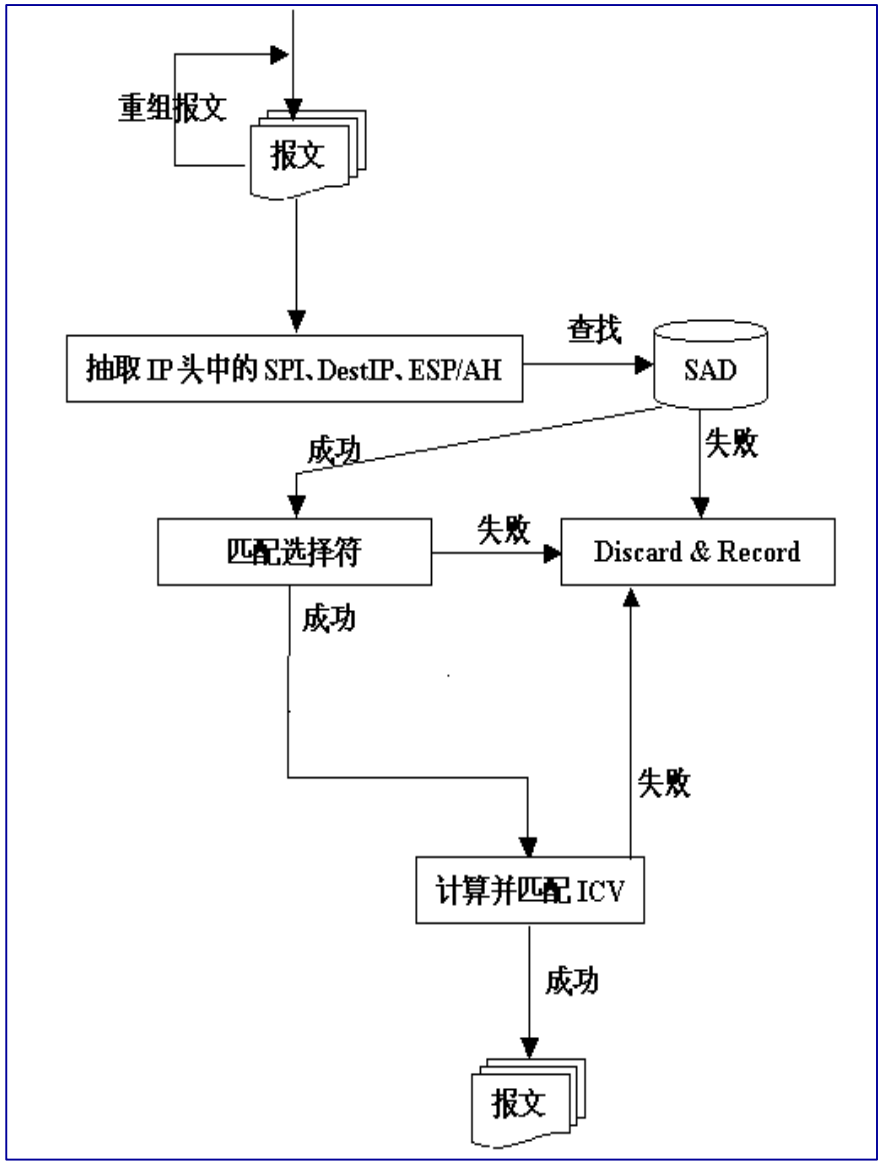


隧道模式

- 隧道模式
  - 通常在防火墙或路由器上实现
  - 把整个IP包作为数据，增加一个新的IP头、AH头



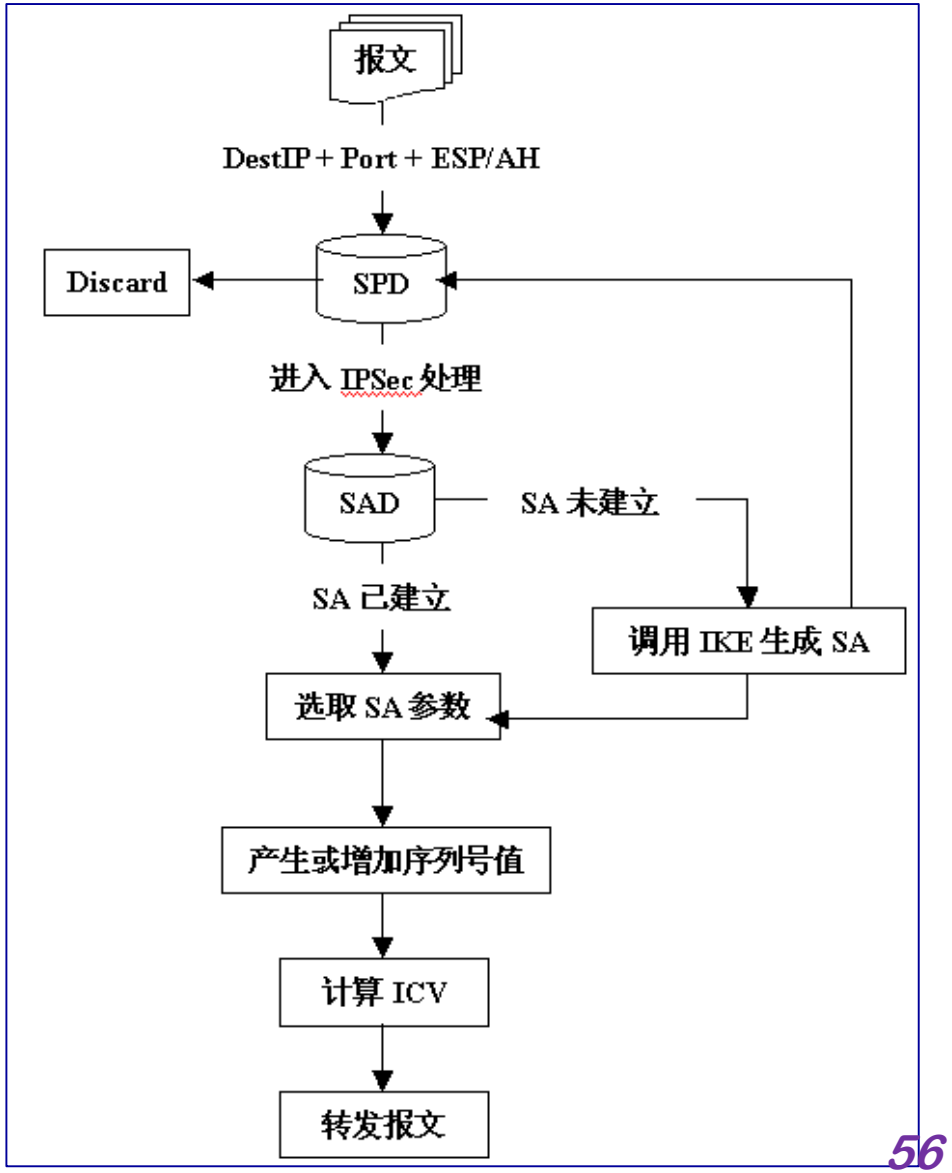
AH对接收数据包 (Inbound)的处理



- 从端口收到输入的数据包，解析出其SA三元组，查找SADB
  - 如查找到一个匹配的SA条目，将该SA参数与数据包相关域参数进行比较：参数一致，处理该数据包；参数不一致，丢弃该数据包
  - 如果没有找到匹配的SA条目，丢弃该数据包
- 检查序列号(可选，针对重放攻击)
  - 使用滑动窗口来检查序列号重放
- 计算数据包的ICV，将其和数据包中的值进行比较：
  - 相等，恢复数据包，转IP协议栈进行路由
  - 不相等，丢弃该数据包并审计事件

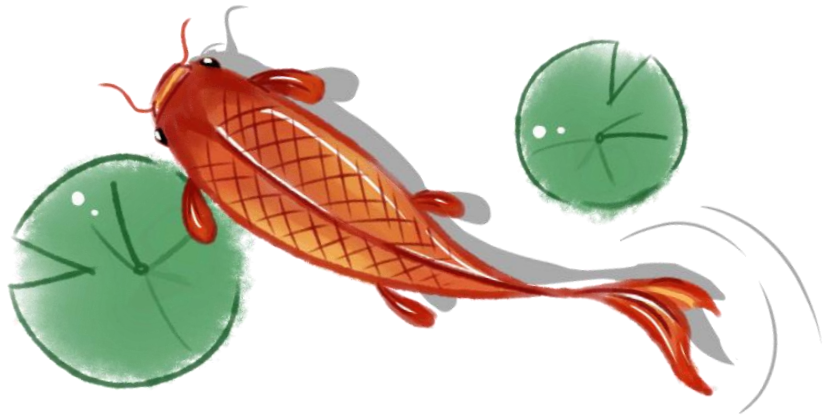
AH对输出数据包(Outbound)的处理过程

- 从IP协议栈中收到需要转发的数据包，使用相应的选择子查找安全策略数据库SPDB，获取对数据包的安全策略
- 如果确定对数据包实施IPsec处理，查找安全关联数据库SADB
  - 如果SA已经建立，选取参数，计算ICV，转发报文
  - 如果SA未建立，调用IKE协商新的SA；在选取参数，计算ICV，转发报文



IPsec：封装安全载荷ESP

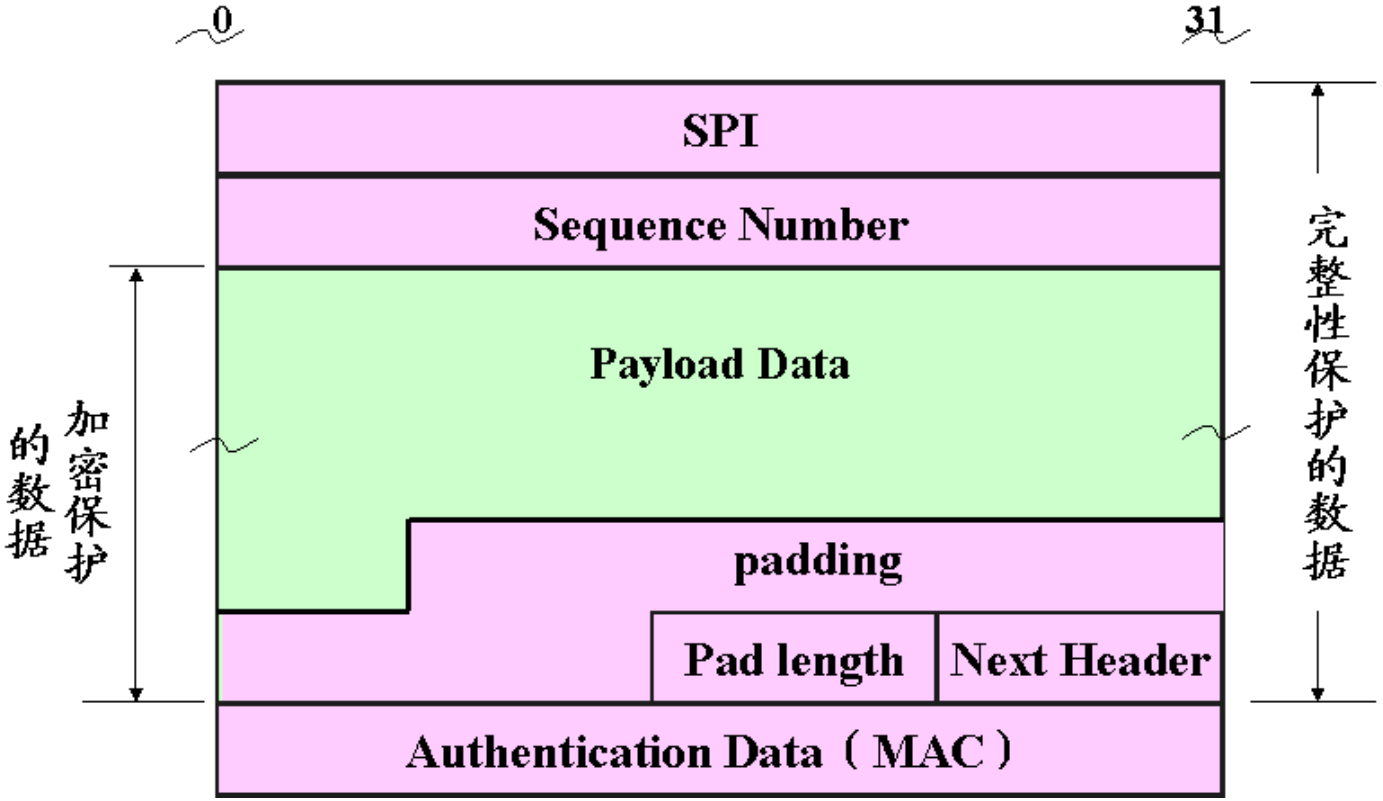
- *Encapsulating Security Payload*



封装安全载荷ESP的格式

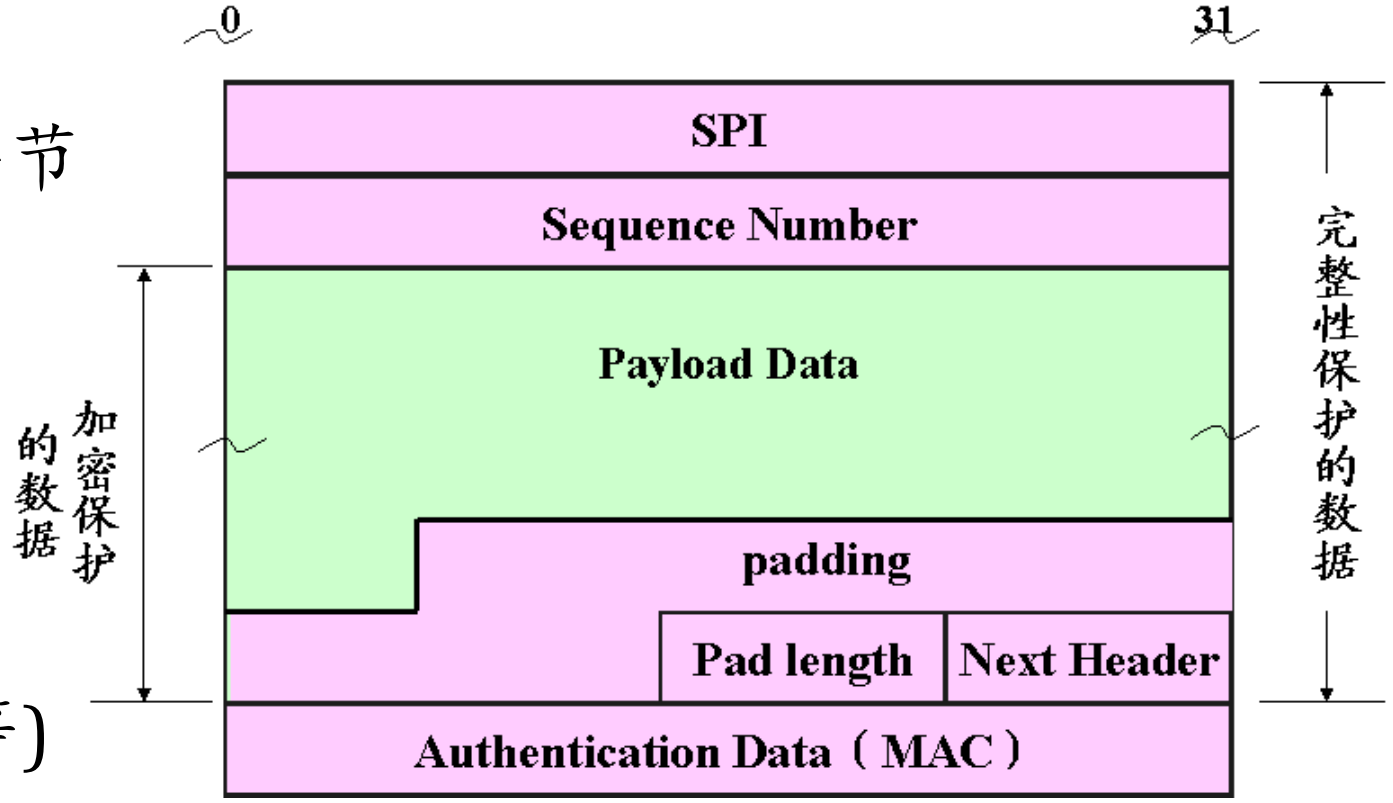
- 封装安全载荷ESP提供保密性服务包括报文内容保密和流量限制保密，ESP还可以提供和AH同样的认证服务

- Security Parameters Index (安全参数索引)
  - SPI为数据报识别安全联合的32 位伪随机值，
  - SPI=0被保留，表明“没有安全关联存在”
- Sequence Number (序列号)
  - 32bits，单调递增的计数器，用于防范重放类型的攻击



封装安全载荷ESP的格式

- Padding(填充域)
  - 可变长域，范围在0~255字节
- Pad Length(填充域长度)
- Next header(邻接头)
  - 8 bits，标识载荷中的封装方式或协议(TCP/UDP/ICMP/AH/ESP等)
- Authentication Data (认证数据AD)
  - 变长域，必须是32 bits的整数倍
  - 包含完整性校验值ICV或者包的MAC



ESP的加密算法、认证算法、填充域

- 载荷数据、填充数据、填充长度和邻接头域都在ESP中被加密。可用加密算法有：3DES、RC5、IDEA、CAST、Blowfish
- 与AH相同，ESP支持使用默认为96位的MAC，并且支持HMAC-MD5-96和HMAC-SHA-1-96
- 填充域的功能如下：
  - 如果加密算法需要明文是某个字节的倍数，则填充域可以用于扩展明文长度
  - 填充域用来保证ESP格式需要填充长度和邻接头域为右对齐的32位字
  - 增加额外的填充域可以隐藏载荷的实际长度，并提供部分流量保护

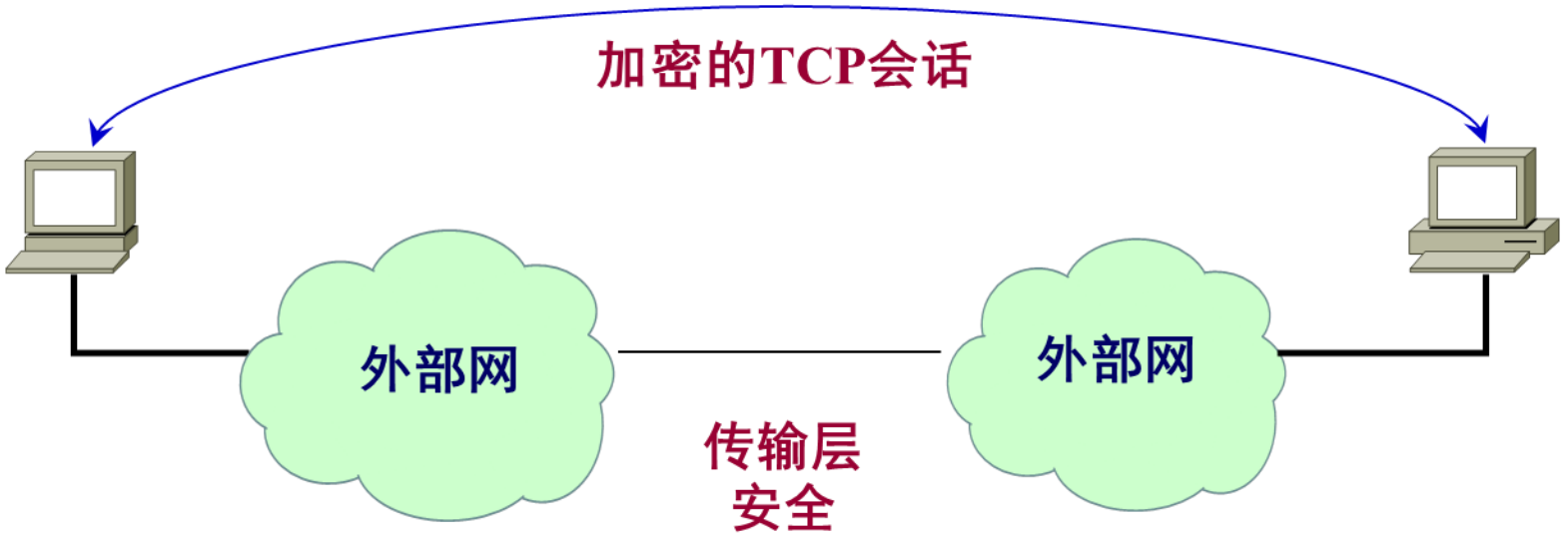
传输模式和隧道模式

- IPSec的ESP提供两种使用途径
  - 加密和认证（可选）直接由两个主机提供，采用传输模式
  - 隧道模式的ESP用于加密整个IP包，可以创建VPN
- 传输模式：加密和认证(可选)直接由两个主机提供
  - 在源端，包括ESP尾和整个传输层分段的数据块被加密，块中的明文被密文替代，形成要传输的IP包；如果选择了认证，则加上认证
  - 将包送往目的地：中间路由器需要检查和处理IP报头以及任何附加的IP扩展头，但不需要检查密文
  - 目的节点对IP报头和任何附加的IP扩展报头进行处理后，利用ESP报头中的SPI解密包的剩余部分，恢复传输层分段数据

传输模式


IP 头
TCP/UDP 头
数据


IP 头
ESP 头
TCP/UDP 头
数据
ESP尾
MAC

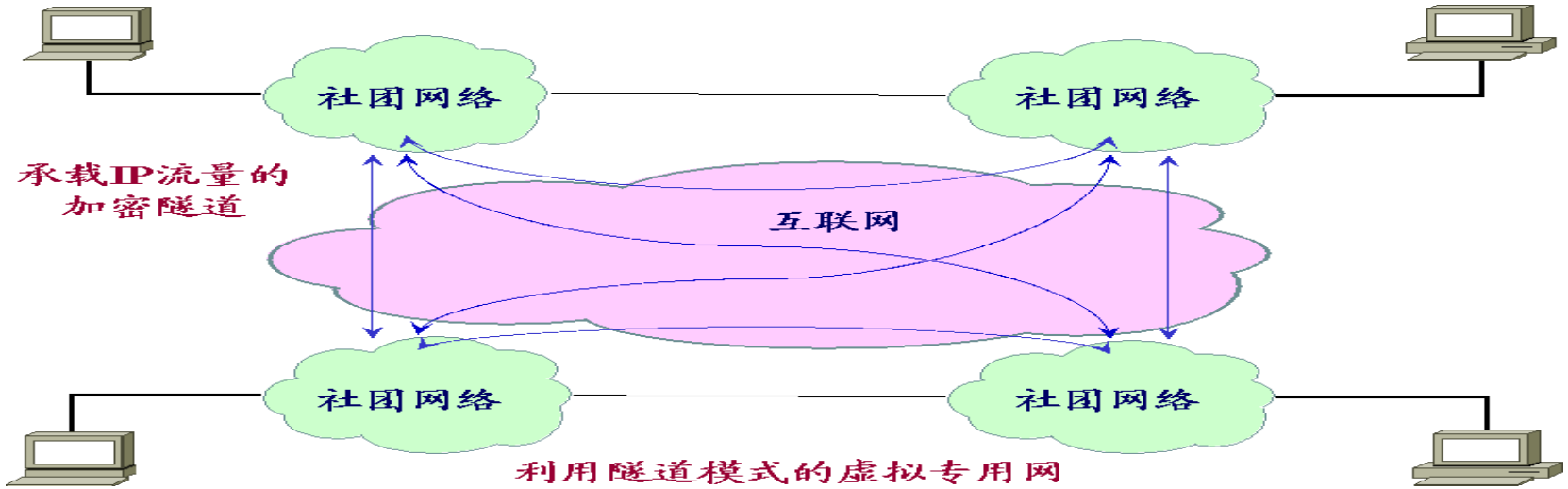

加密的TCP会话
外部网
外部网
传输层
安全

隧道模式

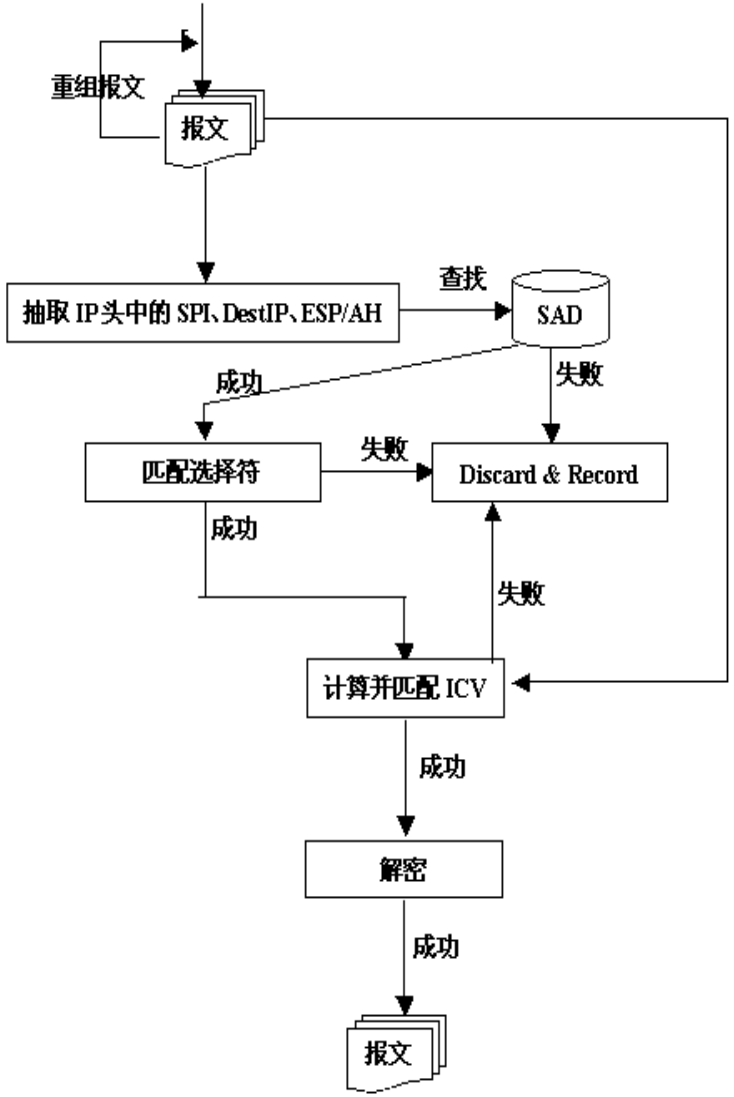
- 隧道模式的ESP用于加密整个IP包，可用于建设虚拟专用网
  - 将ESP头作为包的前缀，并在包后附加ESP尾，然后对其进行加密

IP 头	TCP/UDP 头	数据

新的IP 头	ESP 头	IP 头	TCP/UDP 头	数据	ESP尾	MAC



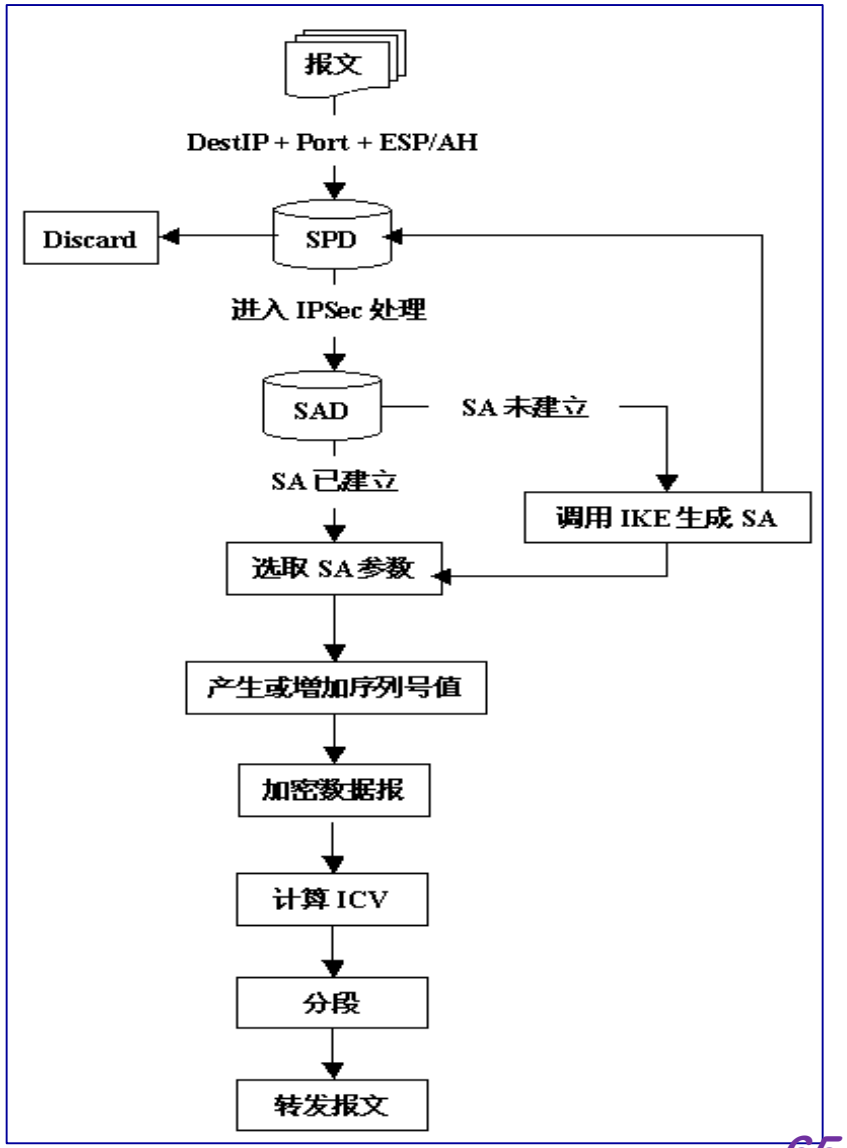
ESP对接收数据包 (Inbound)的处理



- 从端口收到输入的数据包，解析出其SA三元组，查找SADB
  - 如查找到一个匹配的SA条目，将该SA参数与数据包相关域参数进行比较：一致，处理该数据包；不一致，丢弃该数据包
  - 如果没有找到匹配的SA条目，丢弃该数据包
- 检查序列号(可选，针对重放攻击)
  - 使用滑动窗口来检查序列号重放
- 计算数据包的ICV，将其和数据包中的值进行比较：
  - 相等，恢复数据包，转IP协议栈进行路由
  - 不相等，丢弃该数据包并审计事件
- 解密
  - 根据SA中指定的算法/密钥/参数，对被加密部分的数据进行解密
  - 去掉padding，重构原始的IP包，准备路由

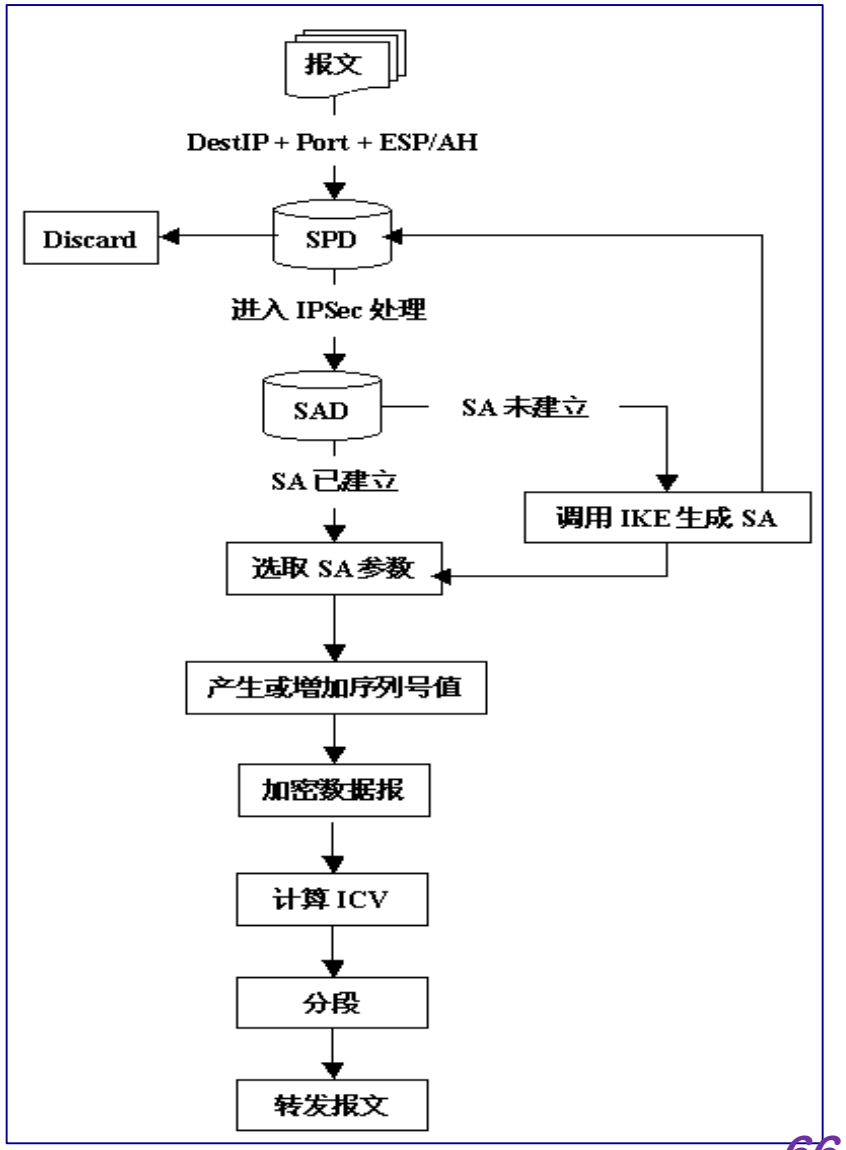
ESP对输出数据包(Outbound)的处理过程[1]

- 从IP协议栈中收到需要转发的数据包，使用相应的选择子查找安全策略数据库SPDB，获取对数据包的安全策略
- 如果确定对数据包实施IPsec处理，查找安全关联数据库SADB
  - 如果SA已经建立，选取参数，计算ICV，转发报文
  - 如果SA未建立，调用IKE协商新的SA；在选取参数，计算ICV，转发报文
- 产生序列号：防止重放攻击

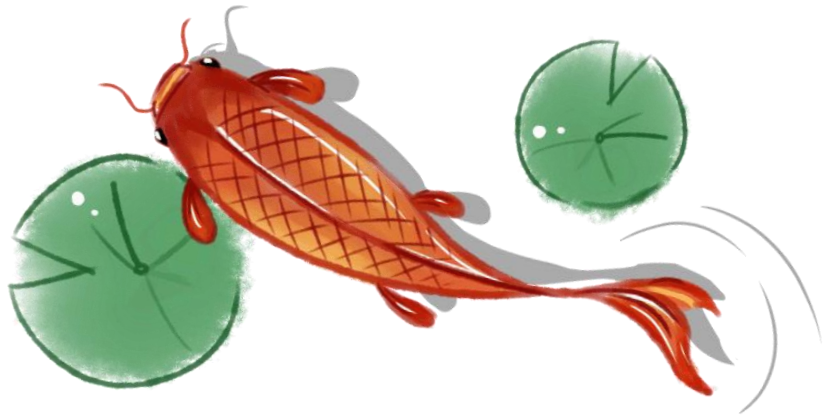


ESP对输出数据包(Outbound)的处理过程[2]

- 加密
  - 封装必要的数据，放到payload data域中
    - 不同的模式，封装数据的范围不同
  - 增加必要的padding数据
  - 加密操作
- 计算ICV
  - 针对加密后的数据计算ICV
- 分片
  - 根据最大传输单元MTU，将数据包分成适当大小的包发往目的节点



IPsec：安全关联组合



安全关联组合

- 单个SA可以实现AH或者ESP，但是不能两者都实现
- 有时，特定流量需要在主机间提供IPSec服务，并在安全网关间（如防火墙）为相同流量提供分离的服务
- 安全关联组合（安全关联束）是指提供特定的IPSec服务集所需的一个SA序列，SA可通过两种方式组合成束：
  - 传输邻接：在不使用隧道的情况下，对一个IP包使用多个安全协议；组合AH和ESP的方法仅允许一级组合
  - 隧道迭代：指通过IP隧道应用多层安全协议；由于每个隧道可以在路径上的不同IPSec节点起始和结束，因此该方法允许多层嵌套

AH和ESP的典型组合

Transport	Tunnel
1. [IP1][AH][upper]]	4. [IP2][AH][IP1][upper]
2. [IP1][ESP][upper]	5. [IP2][ESP][IP1][upper]
3. [IP1][AH][ESP][upper]	

- 这里upper指上层协议数据
- IP1指原来的IP头
- IP2指封装之后的IP头

互联网安全协议

IPsec：IP+安全

- 概述
- 体系结构
- 认证头AH
- 封装安全载荷ESP
- 安全关联组合

IKE管理密钥

- 报文格式、体系结构
- 工作模式、工作过程

网络层安全协议

- **IPsec**：IP+安全
- **IKE**：IPsec管理密钥

传输层安全协议

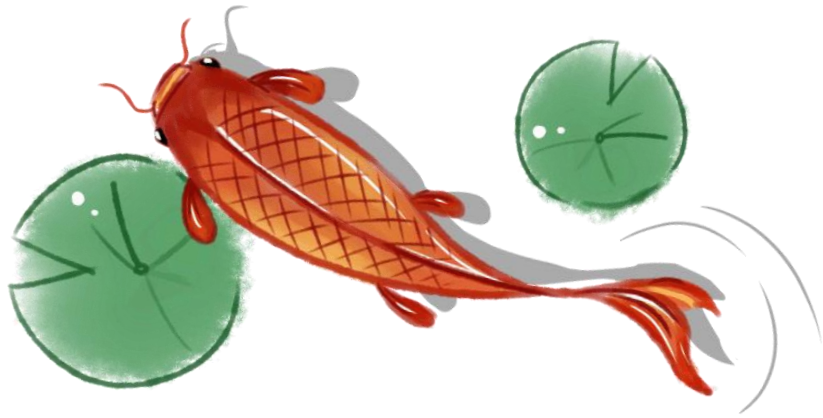
- **SSL**：为应用层服务

应用层安全协议

- **HTTPS**：HTTP+SSL
- **S/MIME**：安全电子邮件
- **SET**：安全电子交易

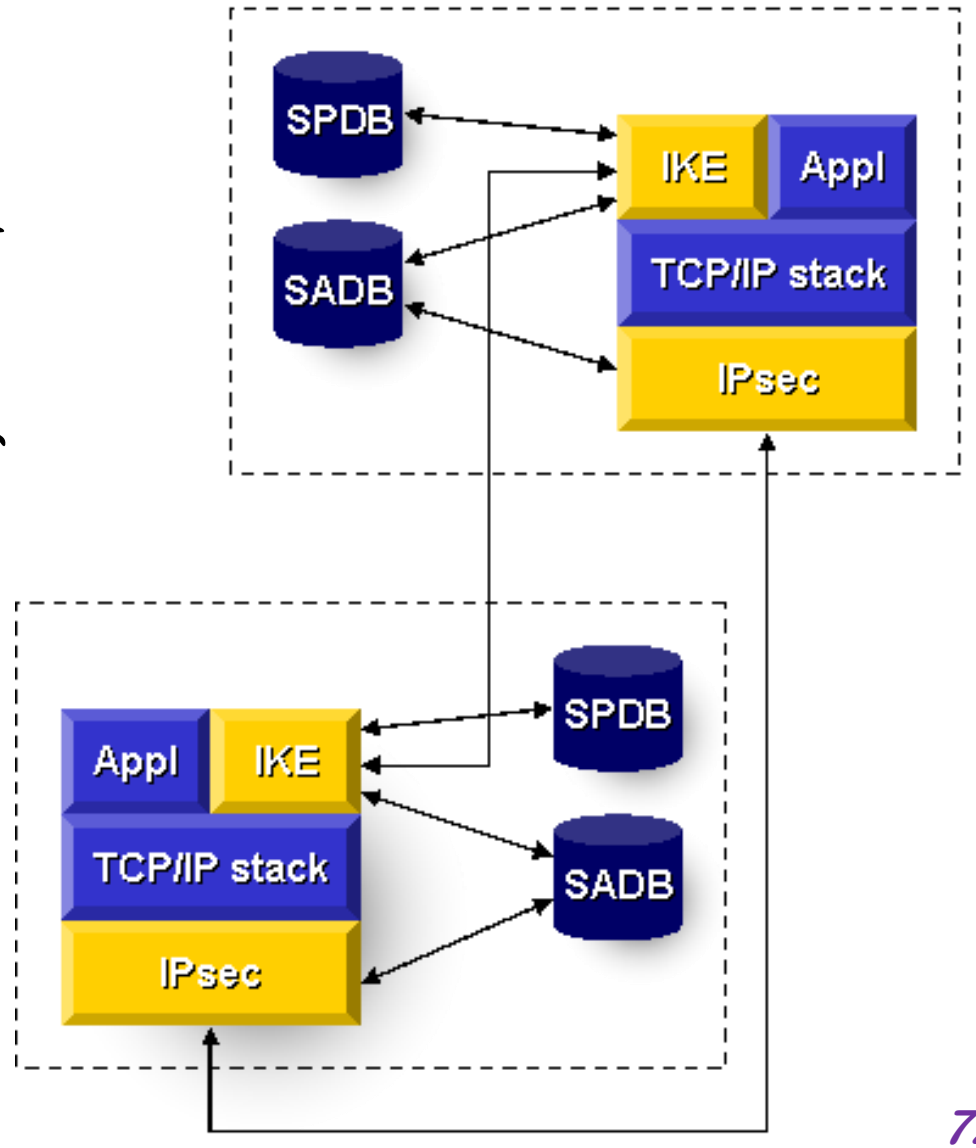
IKE：为IPsec管理密钥

- *Internet Key Exchange*



密钥管理

- IPSec体系结构支持两种密钥管理类型
  - 手工的：系统管理员手动为每个系统配置所需各类密钥，SA永远存在，应用于小规模、结构简单的网络
  - 自动的：在大型分布系统中，SA通过协商方式产生，SA过期后可以重新协商，适用于较复杂拓扑和较高安性的网络
- IKE(Internet Key Exchange)协议为IPSec提供了自动协商交换密钥、建立安全关联SA的服务，简化了IPSec的使用和管理



互联网密钥交换协议—IKE

- 作为互联网的密钥交换协议，IKE协议解决了在不安全的网络环境中安全地建立或更新共享密钥的问题
- IKE是非常通用的协议，不仅可为IPsec协商安全关联，而且可以为SNMPv3、RIPv2、OSPFv2等要求保密的协议协商安全参数
- 目前IKE协议只在IPsec协议中得到了应用
  - Cisco路由器、Windows操作系统、FreeBSD操作系统中都实现和部署了IKE

IKE和IPsec

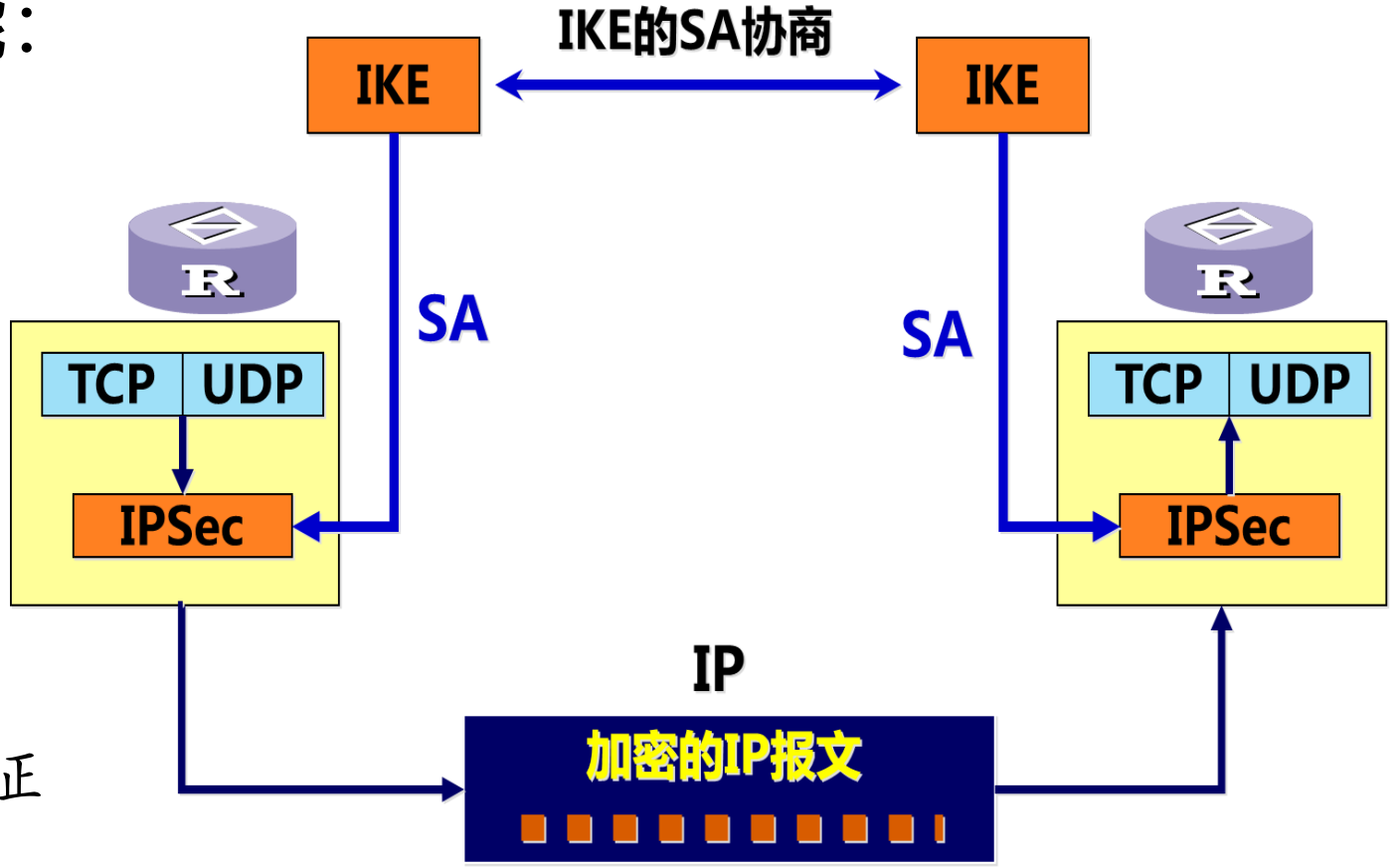
- IKE为IPSec提供了自动协商交换密钥、建立安全联盟的服务，简化IPSec的使用和管理
- IKE的精髓在于：永远不在不安全的网络上直接传送密钥，而是通过一系列的数据交换，通信双方最终计算出共享密钥
- 即使黑客截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥，其核心技术就是DH秘钥交换算法，使得IKE具备了完善的前向安全性
  - 完善的前向安全性PFS(Perfect Forward Secrecy) 是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，这些密钥间没有派生关系

IKE和IPsec

- 在IPsec协议应用中，当应用环境的规模较小时，可以用手工配置安全关联SA
- 当应用环境规模较大、参与节点位置不固定时，必须有一种能够自动协商安全关联SA(各种安全参数组合，如加密算法、认证算法、传输协议、工作模式、生存时间等等）的密钥交换协议。
- IKE 协议就充当了这个角色：IKE不但可自动地为参与通信的实体协商安全关联SA，还可以维护安全关联数据库SADB

IKE和IPsec

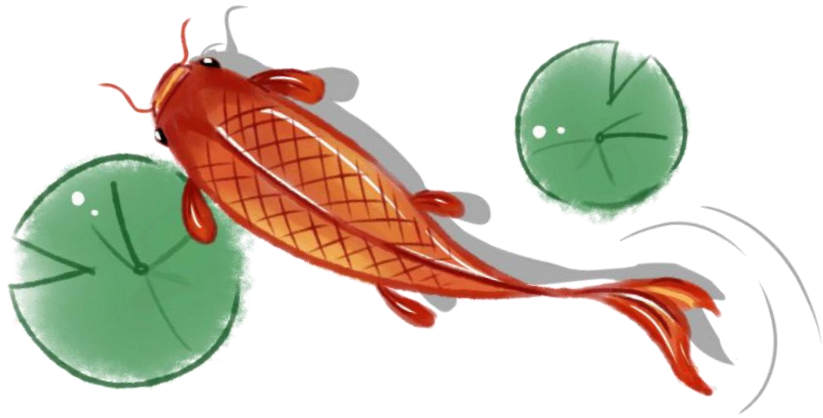
- IKE为IPsec提供了如下功能：
  - 降低手工配置复杂度
  - 安全关联SA定时更新
  - 密钥定时更新
  - 允许IPSec提供反重放服务
  - 允许在端与端之间动态认证



互联网密钥交换协议—IKE

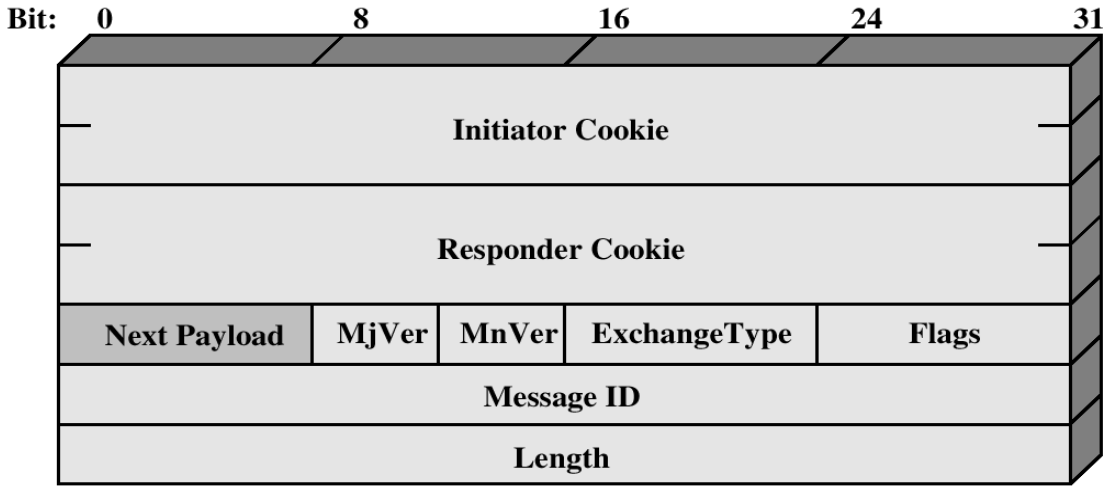
- IKEv1的标准包括 RFC 2407, RFC 2408和RFC 2409
- IKEv2的标准是，摘自RFC4306 附录 A：
  - To define the entire IKE protocol in a single document, replacing RFCs 2407, 2408, and 2409 and incorporating subsequent changes to support NAT Traversal, Extensible Authentication, and Remote Address acquisition
- IKE是一个混合协议，IKE == “ISAKMP格式 + Oakley模式 + SKEME密钥交换”
  - 借鉴了ISAKMP协议的格式和“阶段”概念，实现了部分子集
  - 借鉴了Oakley协议“模式”概念，实现了部分子集
  - 只使用了SKEME协议中用于验证公钥加密的方法，定义了两种密钥交换方式

IKE的报文格式



IKE的报文格式

- IKE的报文格式继承自ISAKMP，所以也称为ISAKMP报文
- ISAKMP可以在任何传输层协议(UDP、TCP)或IP层上实现，利用UDP协议的端口500进行传输
- ISAKMP双方交换的信息以“报文头+载荷”的形式传输，每个ISAKMP报文由一个定长的报文头和不定数量的载荷组成

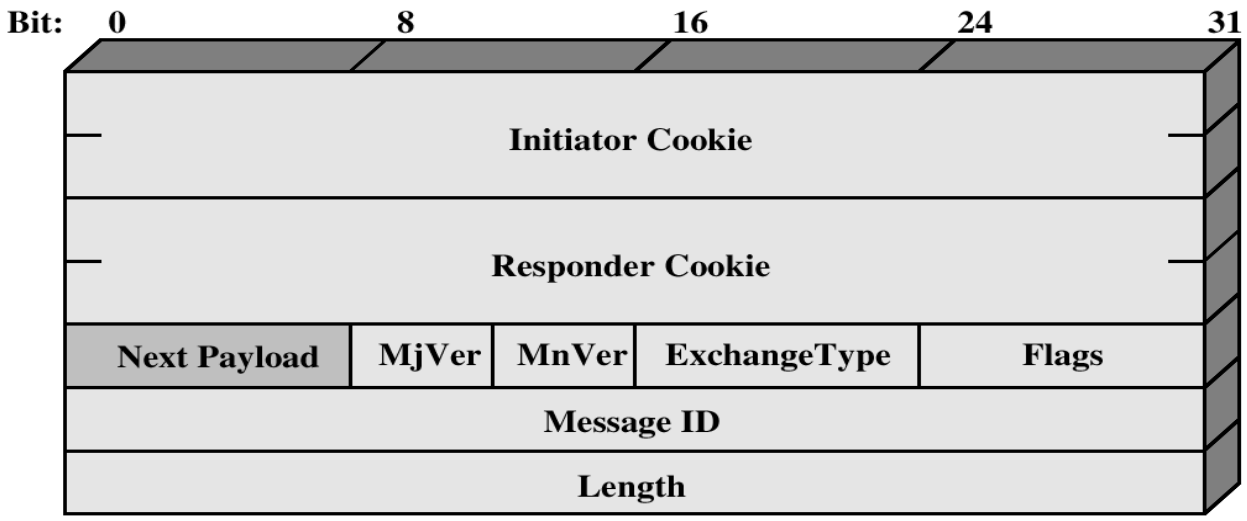


(a) ISAKMP Header

(b) Generic Payload Header

ISAKMP报文头

- Initiator Cookie (32 bits)：发起者Cookie
  - Cookie是一个随机数，发起者和应答者的Cookie一起可以唯一标识一个密钥交换会话和该会话生成的IKE SA
- Responder Cookie (32 bits)：应答者的Cookie
- Next Payload (8 bits)：ISAKMP报文的第一个载荷类型
- MjVer (4 bits)：主版本号
- MnVer (4 bits)：次版本号
- Exchange Type (8 bits)：密钥交换的类型

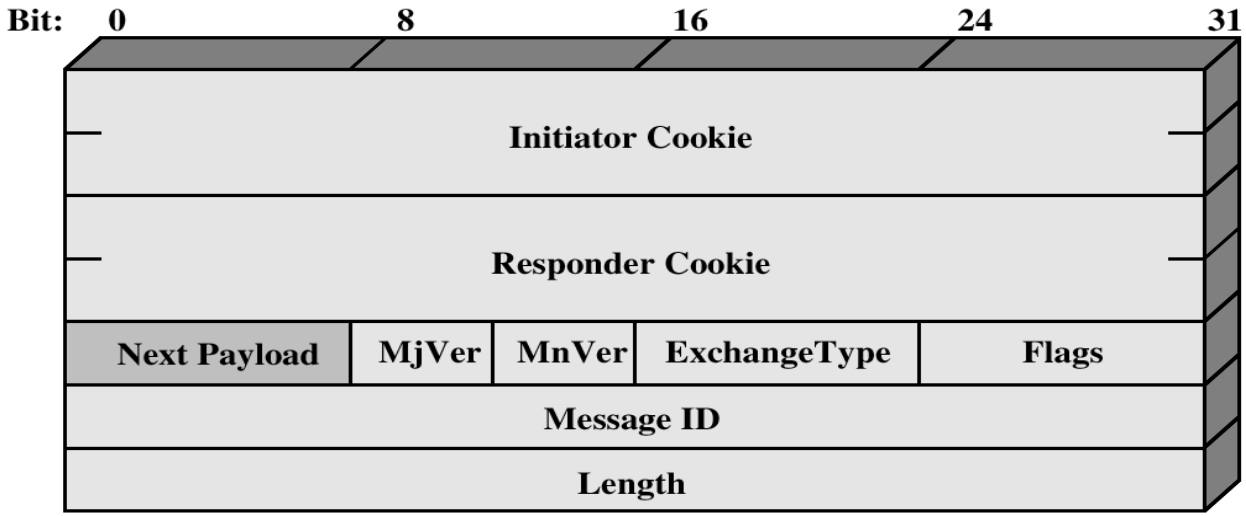


(a) ISAKMP Header

ISAKMP报文头

- Flags (8 bits)： 每个标志位都代表密钥交换的一个特定属性，目前只定义了最低三位，其余位必须被置0
  - 第1位是加密位(Encryption Bit)
    - 置1表明ISAKMP消息头后面的载荷是被加密的
    - 置0则表明是明文传输
  - 第2位是约束位(Commit Bit) 用来同步密钥交换
    - 如果密钥协商的一方A生成的ISAKMP报文将该位置1，那么对方B在安全关联建立起来后，仍要等待A发送一个安全关联建立成功的通知，才可以利用该安全关联进行保密的数据通信
  - 第3位是认证位(Authentication Only Bit)
    - 置1表明该ISAKMP消息头后面的载荷是有认证的
    - 置0表明该ISAKMP报文没有做加密处理，只是做了认证处理

ISAKMP报文头



(a) ISAKMP Header

- Message ID (32 bits)：由第二阶段密钥协商的发起者生成的随机数，用来标志一个第二阶段密钥协商会话
- Total Message Length (32 bits)：ISAKMP报文的总长度，即报文头和所有载荷的总长度，加密可能会导致报文长度增大

ISAKMP的13种载荷

- ISAKMP定义了13种载荷，具有相同格式的载荷头
  - Next Payload (8 bits):
    该载荷的后继载荷类型；如果当前载荷最后一个，则该域被置为0
  - Reserved (8 bits):
    保留字节，置0
  - Payload Length:
    载荷长度（以字节为单位），该长度包括载荷头的长度。

(b) Generic Payload Header

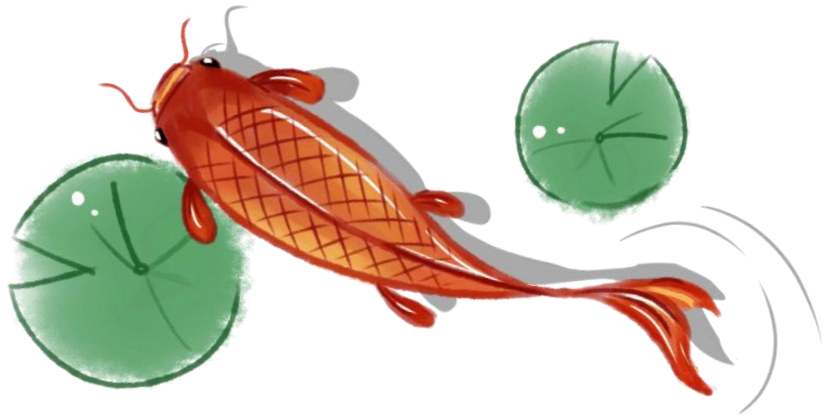
ISAKMP的13种载荷

- 编号1：SA载荷，用来协商安全属性，指明解释域和状态
- 编号2：Proposal载荷，包含在SA载荷中
- 编号3：Transform载荷，总是包含在Proposal载荷内
- 编号4：Key Exchange载荷，传送密钥的各类信息，可为Oakley/DH等所用
- 编号5：Identification身份认证载荷，传送身份信息
- 编号6：Certificate证书认证载荷，传送证书和相关信息
- 编号7：Certificate Request证书请求载荷，向对方要求证书和相关信息
  - 收到含有Certificate Request载荷的ISAKMP报文的接收方，要用Certificate载荷（编号6）发送它的证书

ISAKMP的13种载荷

- 编号8：Hash载荷，传送Hash函数的结果
- 编号9：Signature签名载荷，传送数字签名信息
  - 可以用来对数据完整性进行检查，或者提供不可抵赖服务
- 编号10：Nonce载荷，传送大随机数，可以防止重放攻击
- 编号11：Notification通知载荷
  - 通知对方某些信息，比如报文格式出错，SA生成等
- 编号12：Delete删除载荷，通知对方删除某个或多个SA
- 编号13：Vendor ID供应商载荷，提供了一种扩展手段
  - 密钥交换双方可通过对方的Vendor ID来判断是否可以采用某种扩展

IKE的体系结构



IKE的两个阶段

- IKE使用了两个阶段的ISAKMP框架
- 第一阶段，协商创建一个通信信道（IKE SA），并对该信道进行验证，为双方进一步的IKE通信提供机密性、消息完整性以及消息源验证服务
  - 主模式：6个消息交互
  - 积极模式：3个消息交互
- 第二阶段，使用已建立的IKE SA建立IPsec SA
  - 快速模式：3个消息交互

IKE的两个阶段

第一阶段：
协商 IKE SA

主模式

快速模式

第二阶段：
协商 IPsec SA

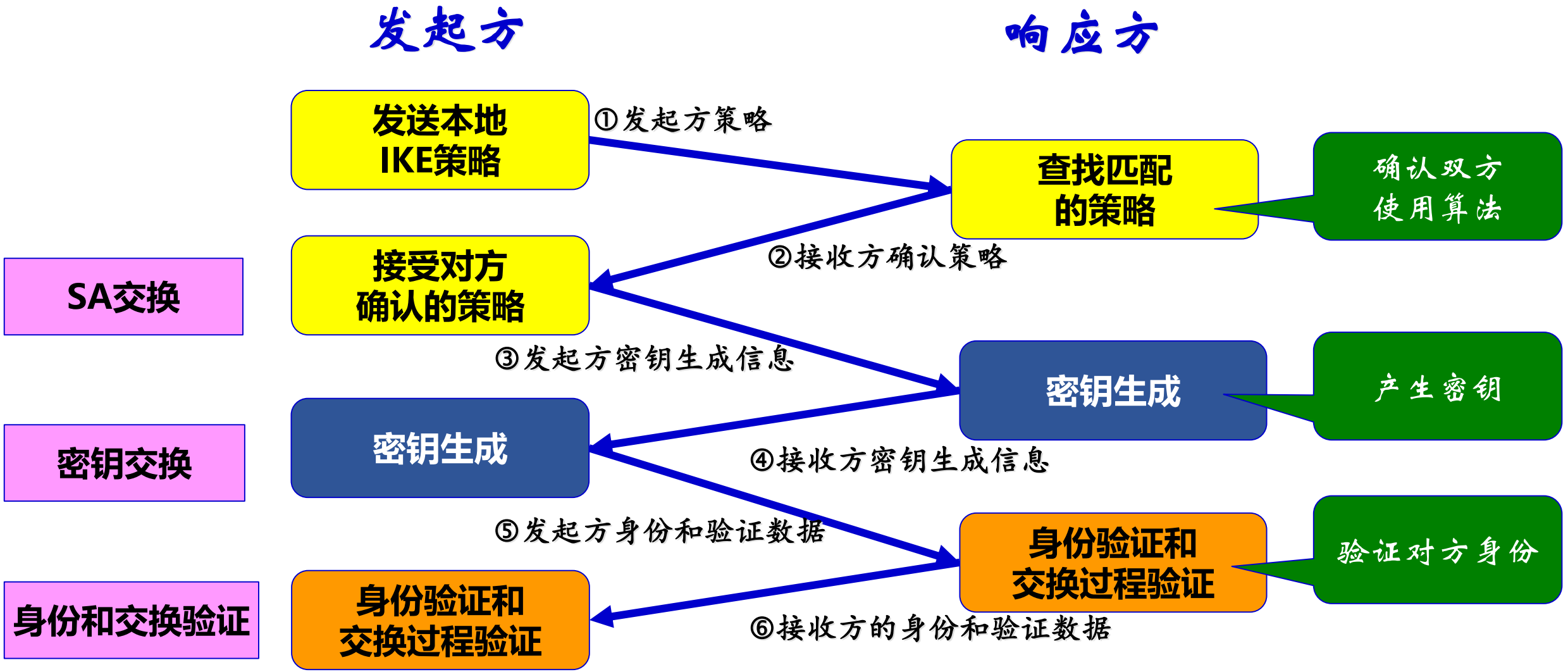
快速模式

IKE的第一阶段：协商IKE SA

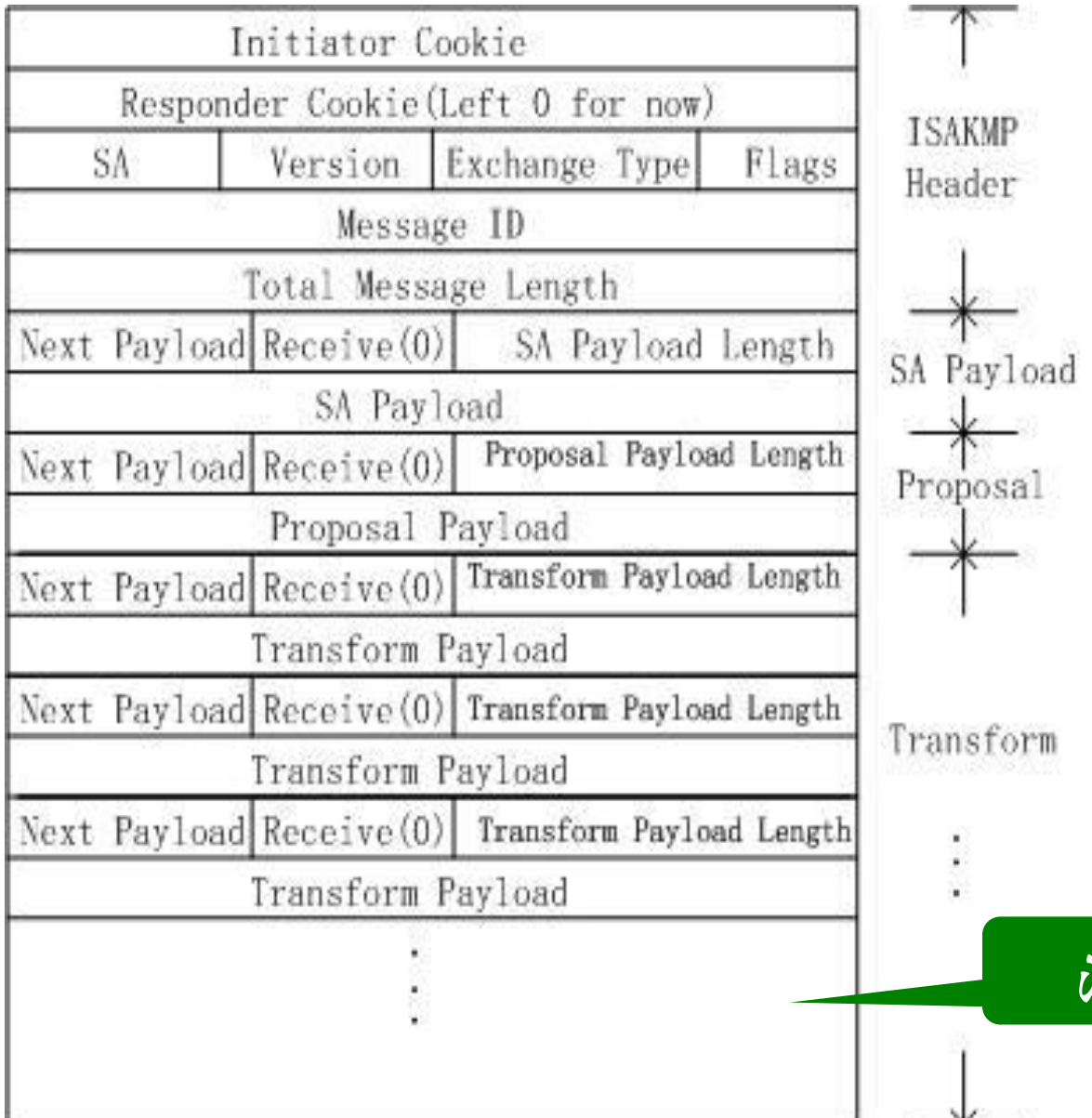
- IKE在第一阶段中要协商建立IKE SA，建立一个经过验证的安全通道，为后续的协商提供机密性和完整性保护
  - 必须协商的内容包括：加密算法、哈希算法、认证(验证)方法、进行DH操作所使用组的有关信息等

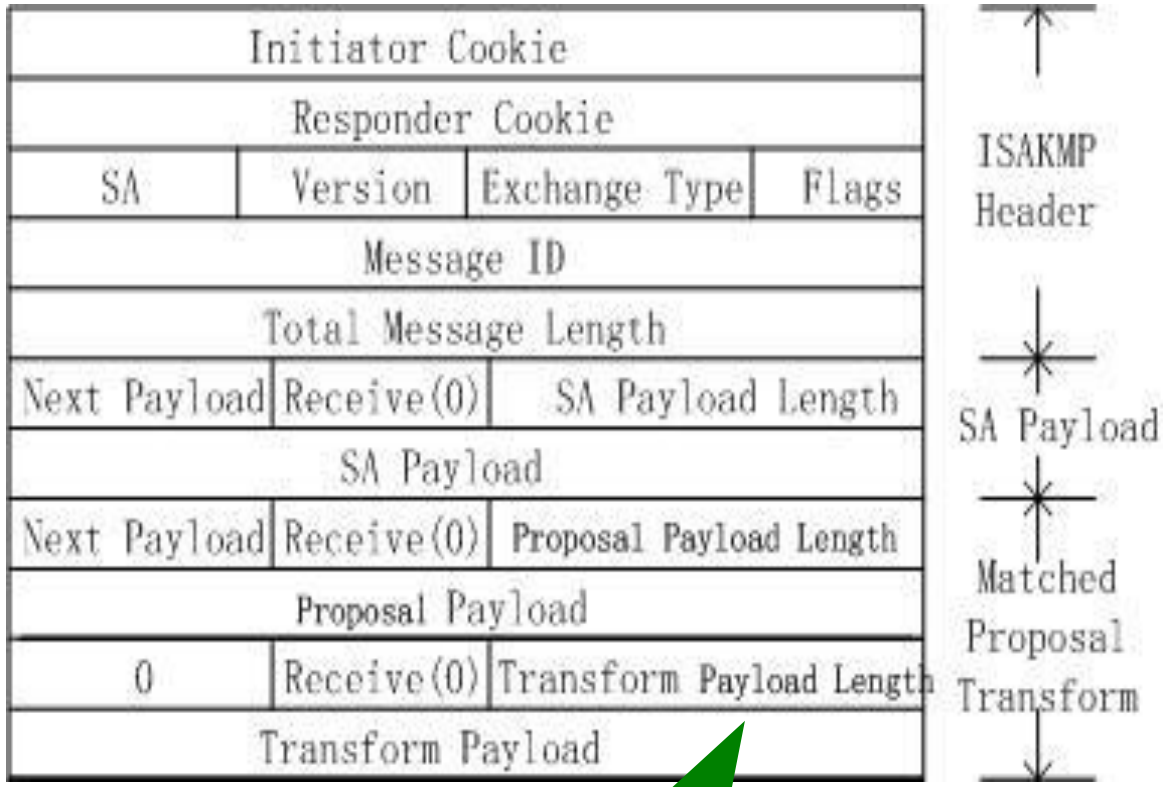
- IKE第一阶段中可以使用主模式和积极模式，这两种模式只能在第一阶段中使用
  - 主模式提供了对通信双方的身份保护
  - 当身份保护不必要时，可以使用积极模式以减少信息传输的数量，提高协商效率

IKE的第一阶段：主模式



SA交换：消息①和②





消息①

消息②

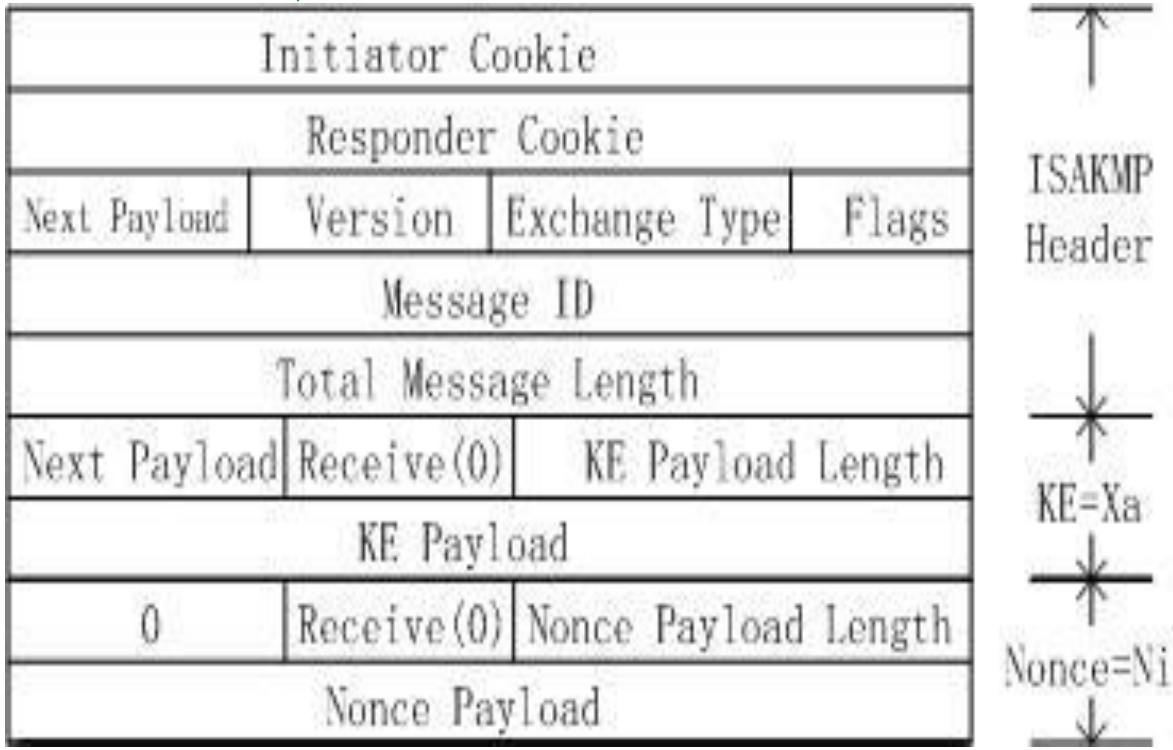
SA交换：消息①和②

- 在协商之前，发起者和响应者必须计算产生cookie，用于唯一的标识每个单独的协商交换过程
  - cookie使用源/目的IP地址、随机数字、日期和时间等信息进行MD5计算，其结果写入ISAKMP报文头的“cookie”域中

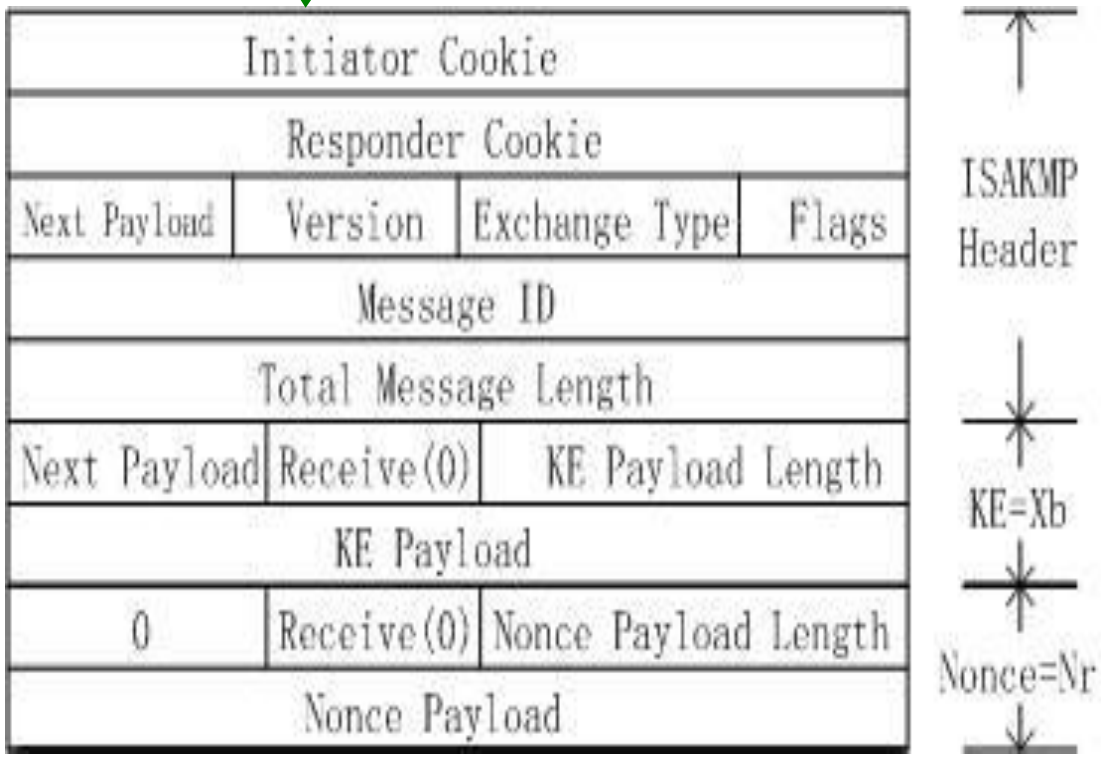
- 发起者发送消息①，接受者响应消息②；
双方就散列函数、加密算法、认证方法、IKE SA协商的时间限制等进行了协商

密钥交换：消息③和④

消息③

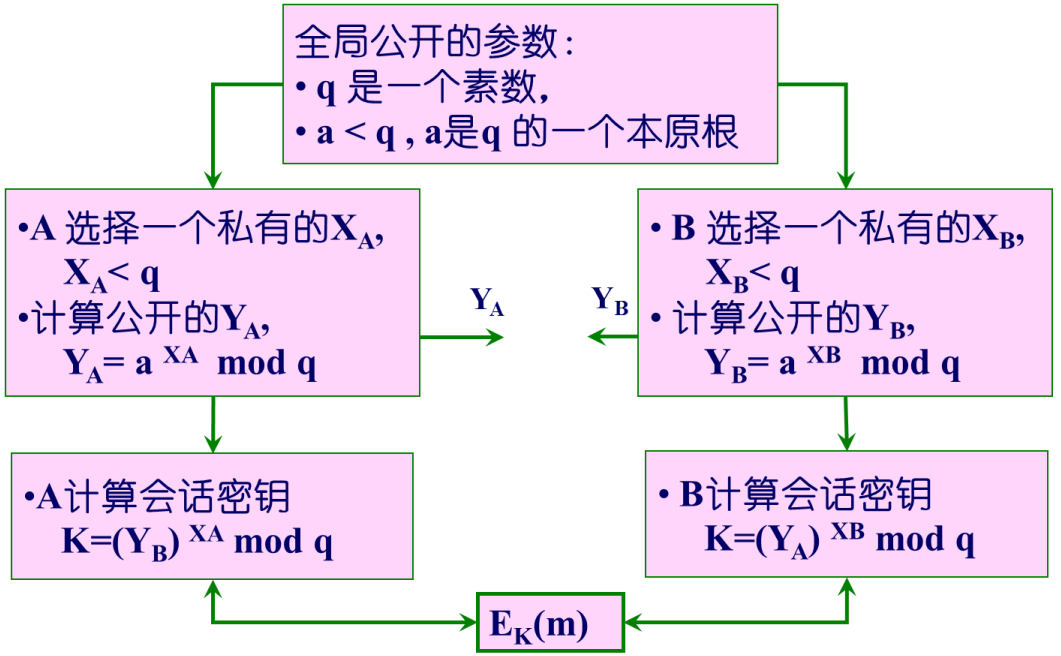


消息④



密钥交换：消息③和④

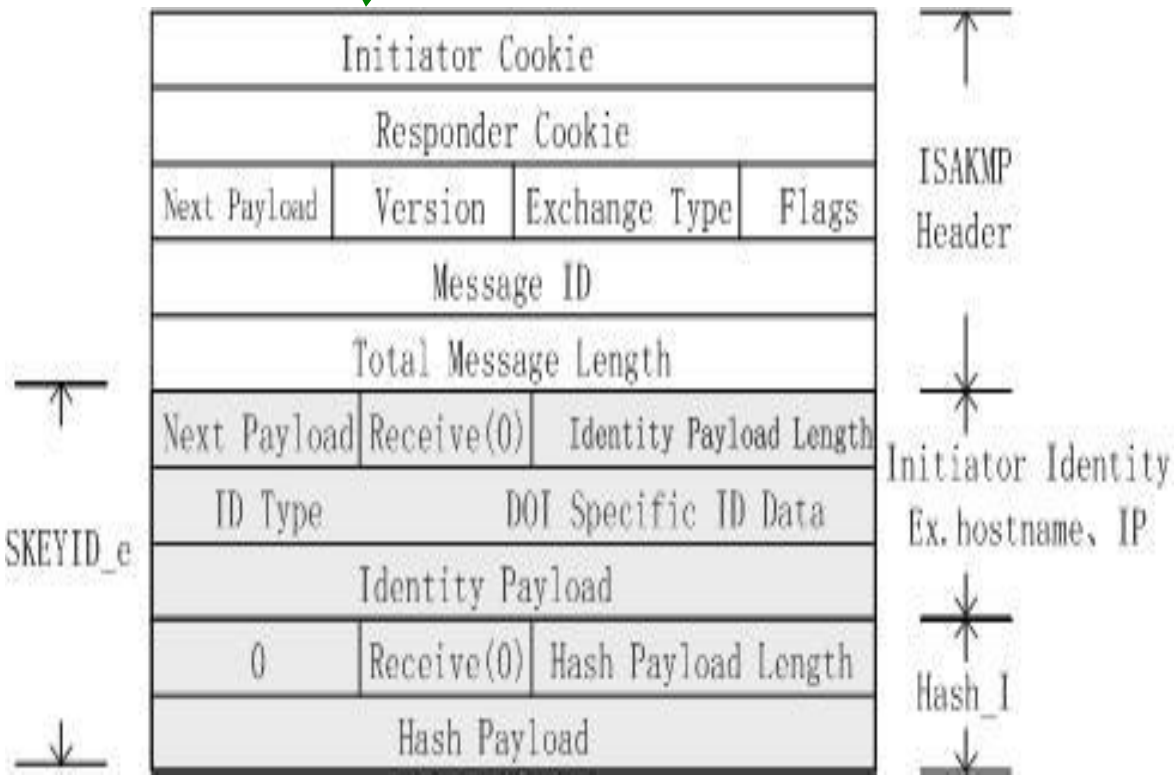
- 发起方和响应方采用Diffie-Hellman密钥交换算法计算共享密钥



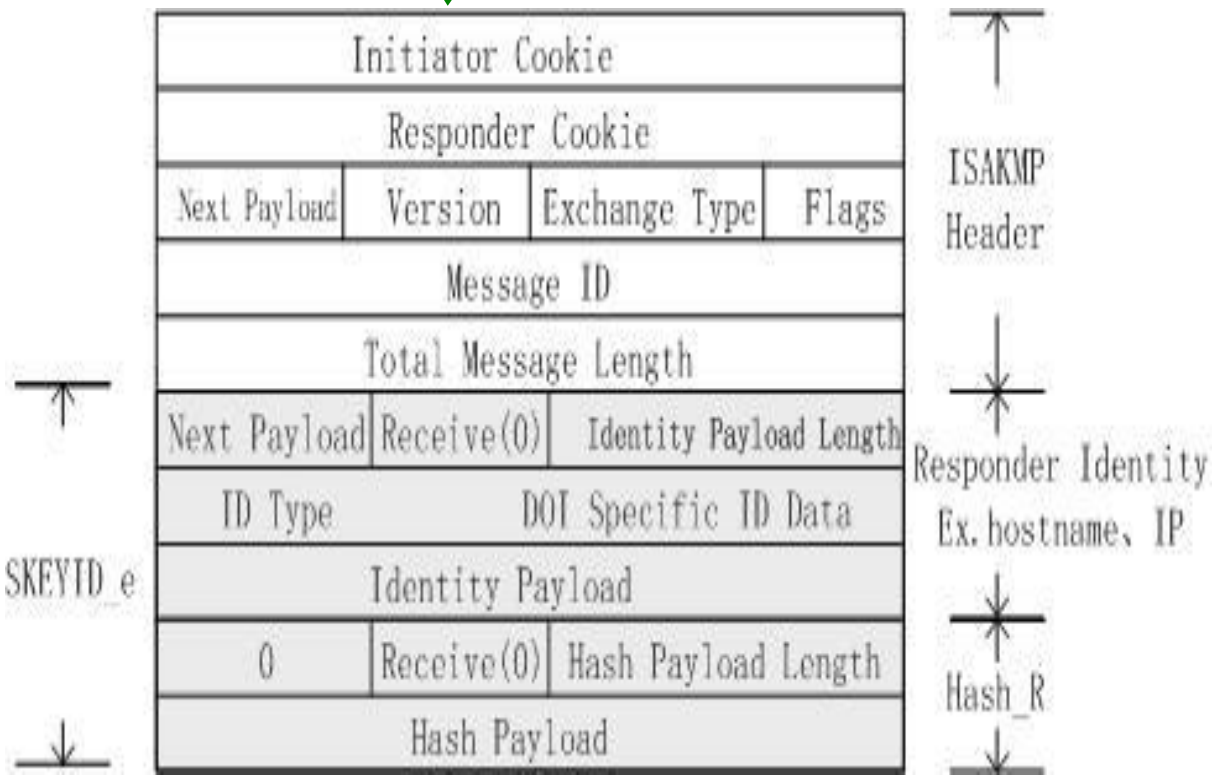
- 发起方发送消息③，响应方发送消息④：
  - 消息③ ④的ISAKMP报文头和消息①和②相同，但载荷不同
  - 消息③ 包含了Key Exchange载荷和Nonce载荷
    - 消息类型4 和 消息类型10

身份和交换验证：消息⑤和⑥

消息⑤



消息⑥



身份和交换验证：消息⑤和⑥

- 发起方发送消息⑤，ISAKMP头还是和前面的一样，但是载荷不同，消息⑤中的载荷包含标识载荷和散列载荷，并且加密传输
  - 身份认证载荷（消息类型5）包含了发起者的标识信息，IP地址或者主机名；散列载荷（消息类型8）包含对上一过程中产生的三组密钥进行Hash运算得出的值
  - 这两个载荷加密传输
- 消息⑥是响应方发送的，包含了响应者相应的信息
- 如果双方在消息⑤和消息⑥中的散列载荷中的hash值相同，那么双方的认证成功→→→ IKE第一阶段协商顺利完成

IKE的两个阶段

第一阶段：
协商 IKE SA

主模式

快速模式

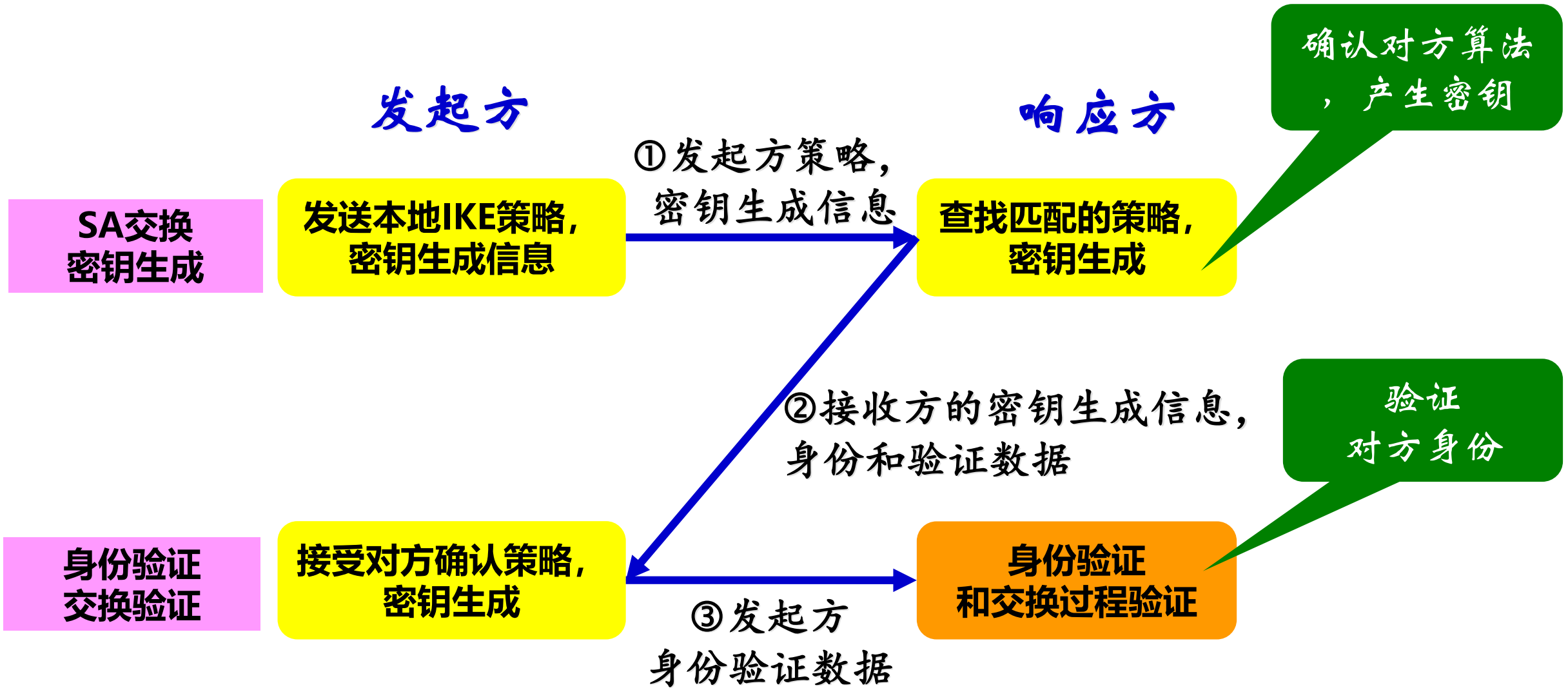
第二阶段：
协商 IPsec SA

快速模式

IKE的第一阶段：快速模式

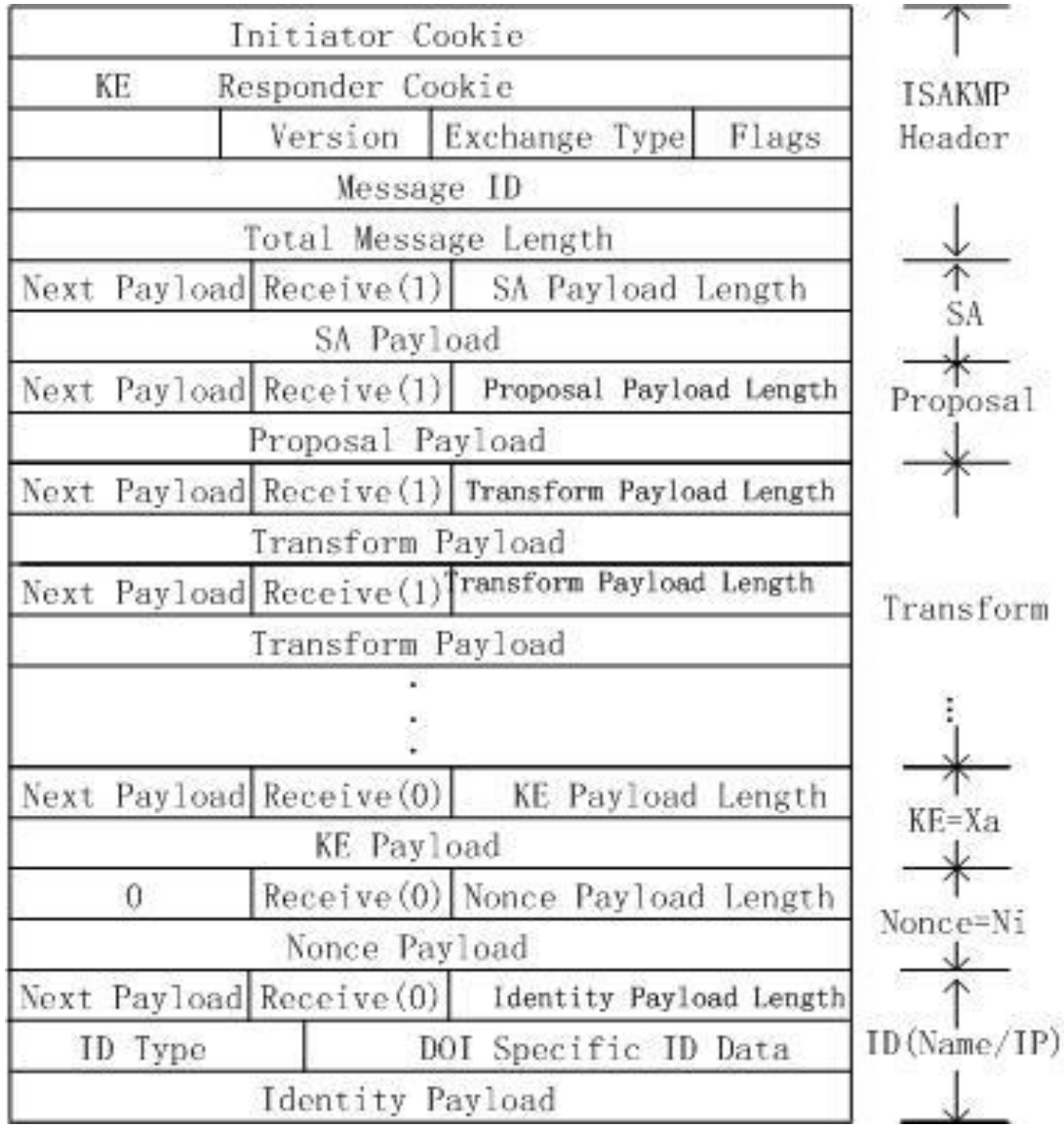
- IKE为什么需要快速模式：
- 适用于一方地址为动态的情况
  - 主模式只能采用IP地址作为ID进行协商，不能够应用于IP地址变化的情况
  - 快速模式可以采用Name方式进行验证，可以应对IKE协商双方中有一方为动态地址的情况；但是，快速模式不能用于两端地址都变化的情况
- 快速模式传输的消息更少，效率更高
  - 主模式需要交换6个消息，快速模式只需要交换3个消息

IKE的第一阶段：快速模式



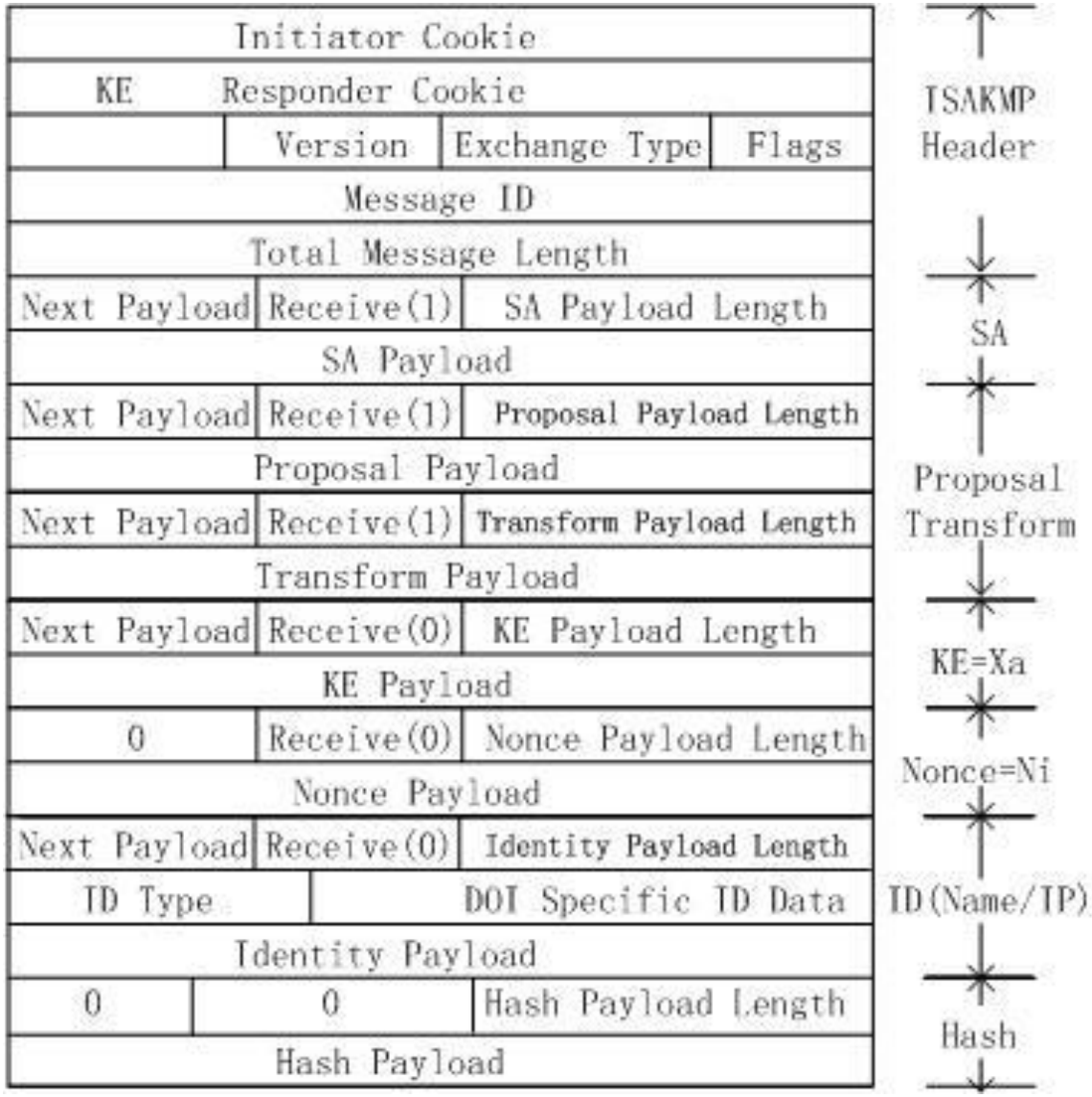
快速模式：消息①

- 在协商之前，发起者发送前计算好cookie
- 消息①交换SA、KEY、Nonce和ID等载荷
- 消息②在响应消息①内容的同时，增加了Hash认证
- 消息③是响应方对发起方的认证



快速模式：消息②

- 消息②在交换消息①内容的同时，增加了Hash认证
- 与主模式中的消息⑤⑥的准备工作一样，响应方计算好几个密钥，然后使用这些密钥以及其他信息计算hash值
- 消息②回答了消息①的相应内容，还包括了计算好的hash值



快速模式：消息③

- 发送方根据消息②传来的密钥，计算Hash值；
  如果这个Hash值和消息②中的Hash值一致，则发送方验证响应方成功；然后，再计算一个新的Hash值，加载在消息③ 中，发送给响应方
- 响应方收到了消息③后，
  计算自己的Hash值，
  与消息③的Hash值进行比对，
  如果一致，认证成功
- 快速模式顺利完成

IKE的两个阶段

第一阶段：
协商 IKE SA

主模式

快速模式

第二阶段：
协商 IPsec SA

快速模式

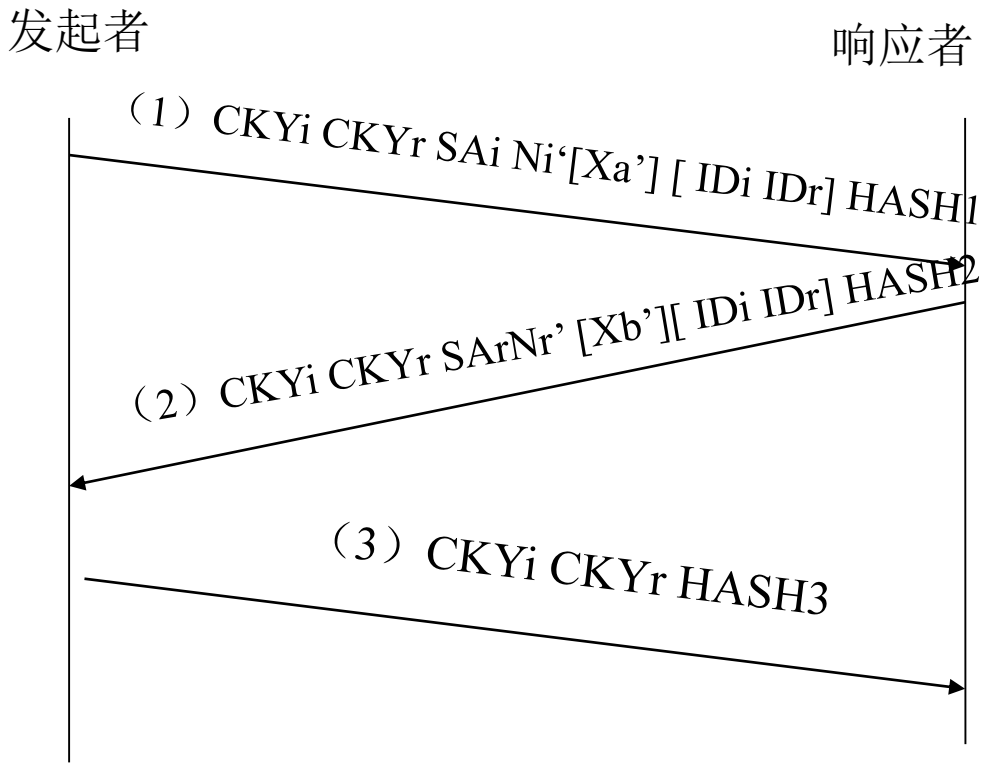
IKE的第二阶段：建立IPsec SA

- 一个IKE SA协商（第一阶段）可为多个IPsec SA协商（第二阶段）提供服务
- 第二阶段为IPsec AH 和 / 或 IPsec ESP协商安全参数，还可以实现密钥数据的交换
- 第二阶段协商的内容与所协商的安全协议等相关
  - 例如：IPsec AH 协议需要协商认证算法，IPsec ESP 协议需要协商认证和加密算法
- 第二阶段中使用快速模式进行信息交换，一个第二阶段协商可以建立多个安全关联
  - 例如：用于两个通信实体的双方向的共8个安全关联：每个通信实体都包含一个出AH SA、一个入AH SA、一个出ESP SA、一个入ESP SA

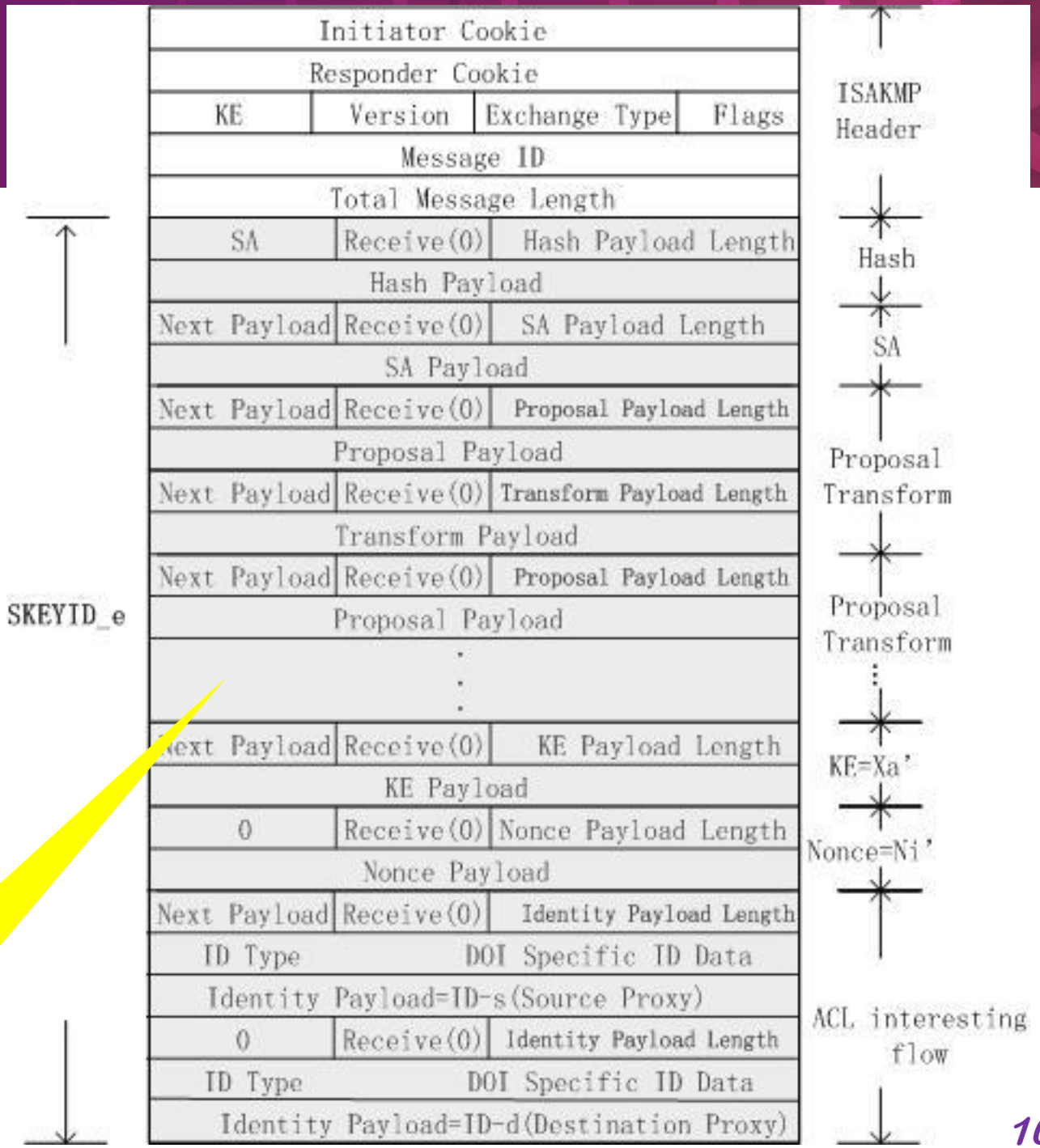
IKE的第二阶段：需要协商的参数

- 加密算法：包括DES、IDEA、Blowfish、3DES、CAST等
- 哈希算法：包括MD5、SHA、Tiger等
- 验证方法：包括共享密钥、RSA签名、DSS签名、RSA加密、 RSA加密等
- DH组
- 存活周期类型及长度：包括秒、千字节等
- 密钥长度
- 等等

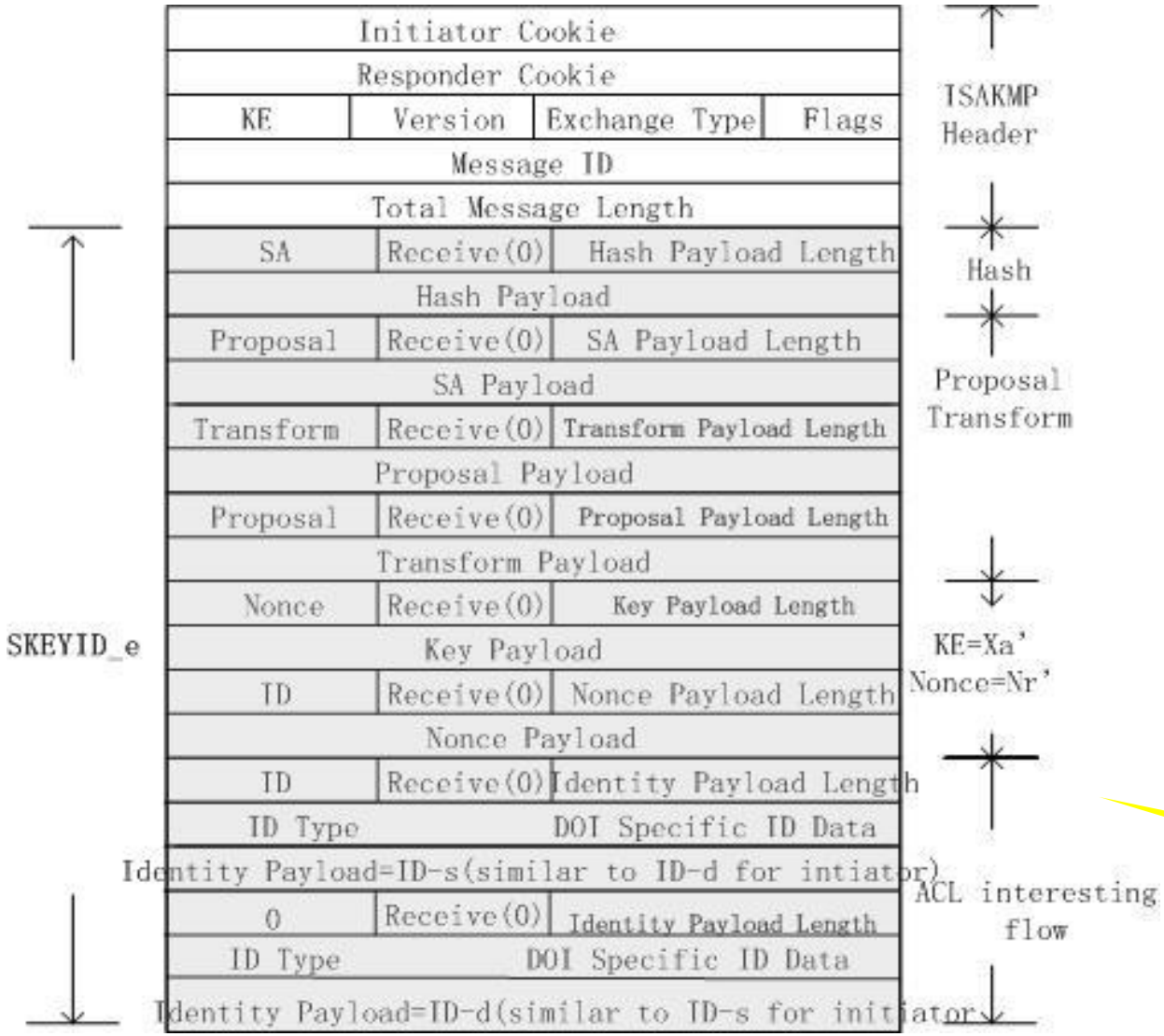
IKE的第二阶段消息交互举例

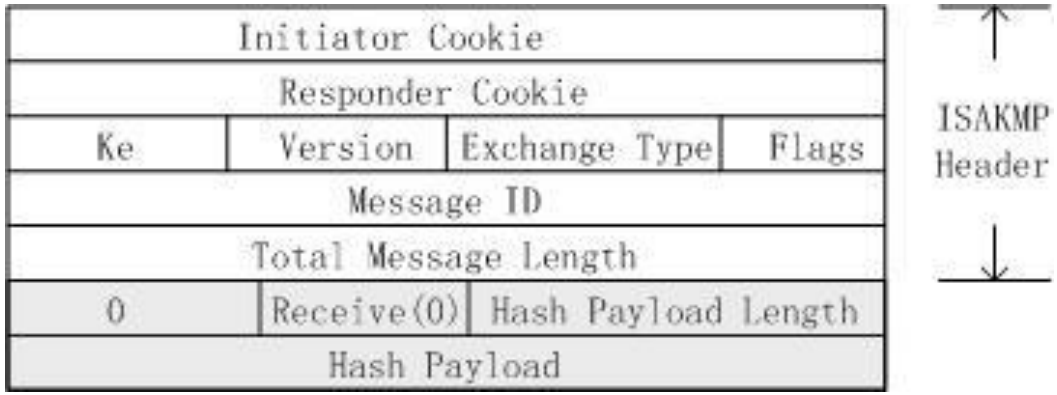


消息①



IKE的第二阶段：消息交互举例

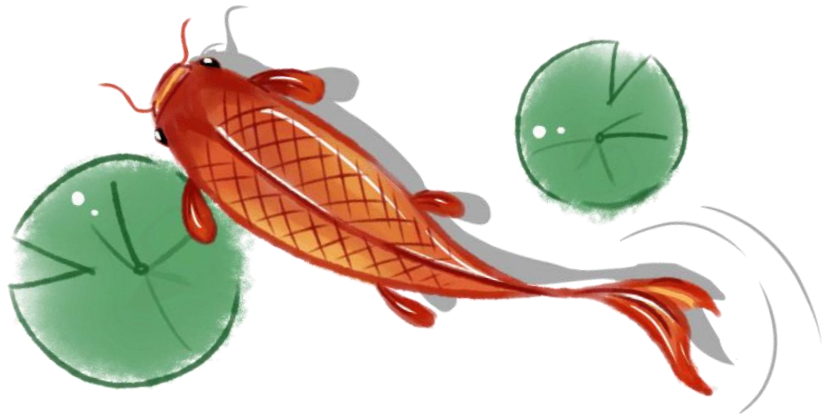




消息③

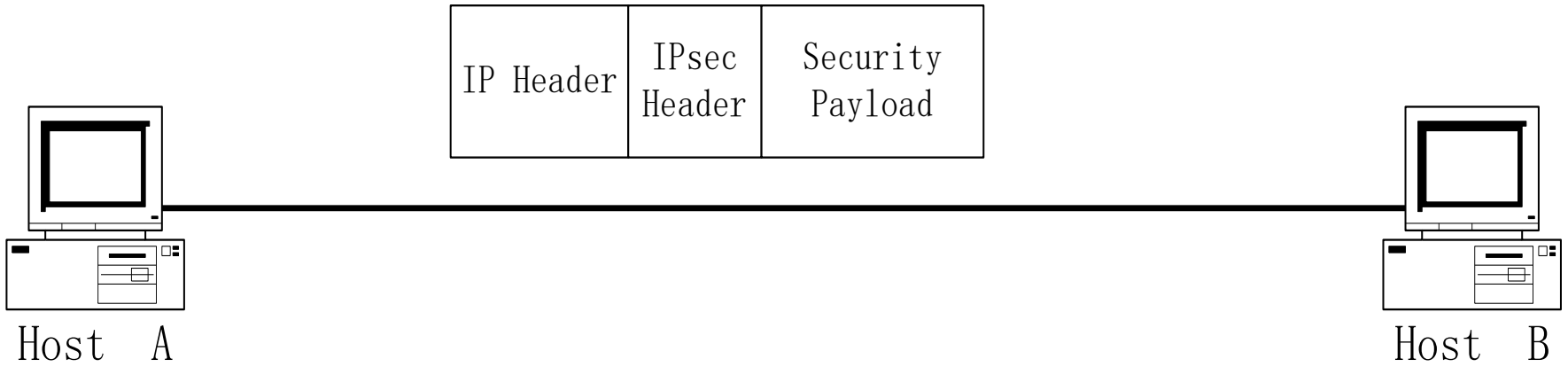
消息②

IKE的工作模式



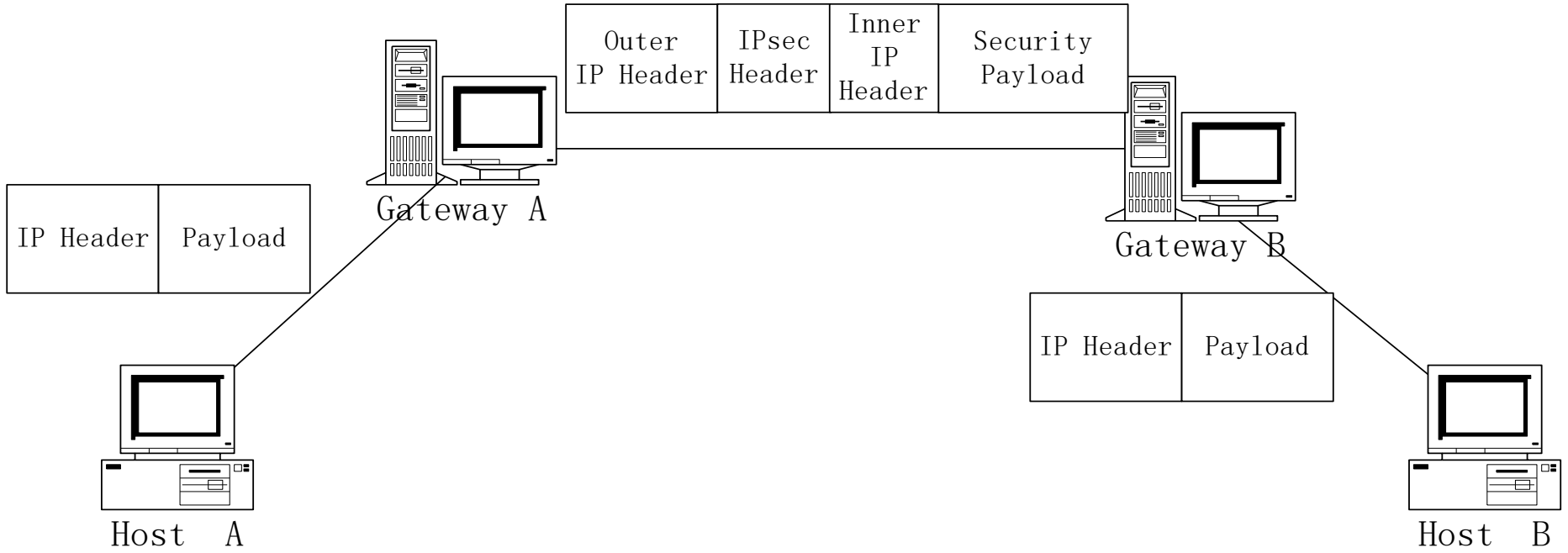
IKE的工作模式

- 端节点到端节点：采用传输模式
  - 两个端节点均实现IPsec，通常使用传输模式
  - IP头与数据间插入IPsec头，用来保护数据载荷



IKE的工作模式

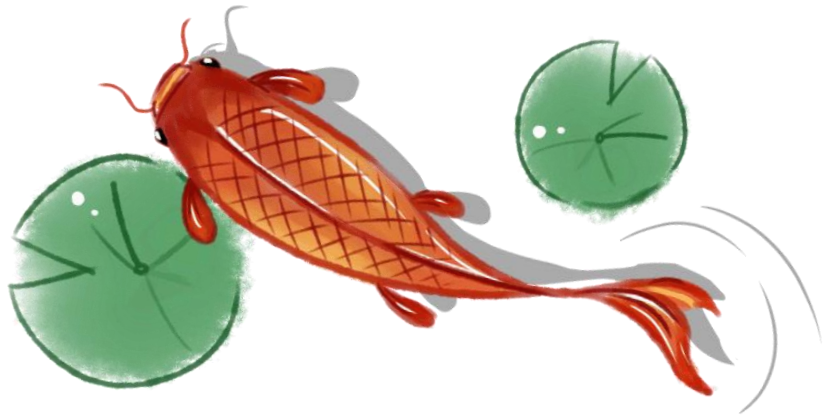
- 安全网关到安全网关：采用隧道模式
  - 端系统均不需要实现IPsec，由网络节点完成保护功能
  - 通常采用隧道模式发送，内部IP头包含实际端节点的IP地址



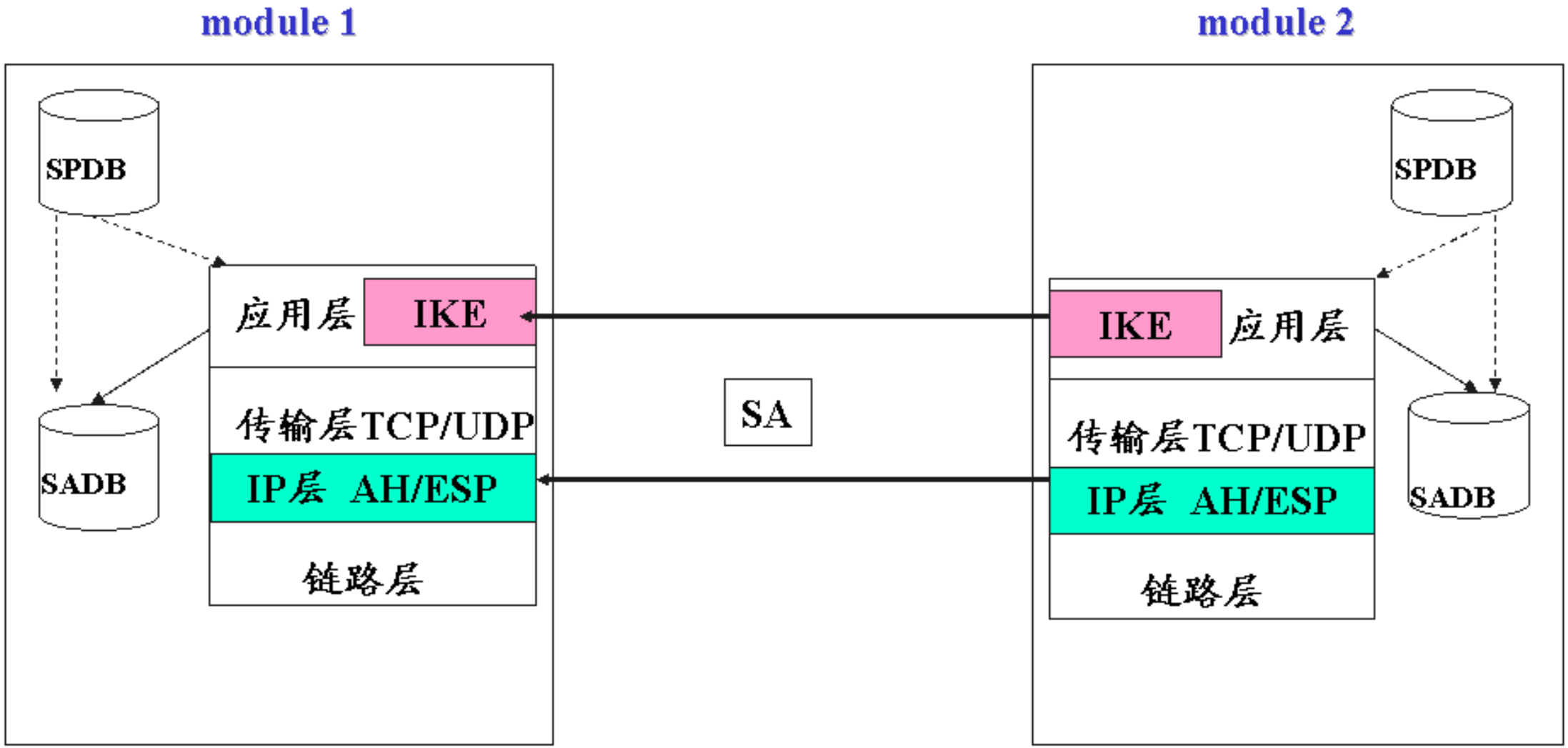
IKE的工作模式

- 常见的上面两种模式的嵌套组合
- 例如：端节点到安全网关模式
  - 假设一个便携漫游用户通过IPsec 保护的隧道连接回自己的协作网络，在这种情况中，数据包将使用隧道模式
  - 从便携漫游用户节点出来的数据包的外部IP 头将包含和其当前位置相关的IP 地址，而内部IP 头将包含由安全网关赋予的源IP 地址
  - 外部目的地址总是安全网关的地址，而内部目的地址会是数据包的最终地址

IKE的工作过程



IKE的工作过程


module 1
module 2
SPDB
SADB
应用层
IKE
传输层TCP/UDP
IP层 AH/ESP
链路层
SA
SPDB
SADB
IKE
应用层
传输层TCP/UDP
IP层 AH/ESP
链路层

IKE的工作过程

- IKE在协议实现上，是以守护进程的方式在后台运行
- 可以通过两种方式来启动IKE服务：
  - 由内核提交创建IKE SA请求
  - 同级IKE守护进程提交协商SA请求
- 两个守护进程通过UDP协议（端口500）来传递消息
- IKE协议使用两个数据库：
  安全关联数据库SADB和安全策略数据库SPDB，
  这两个数据库都保存在操作系统内核

IKE的工作过程

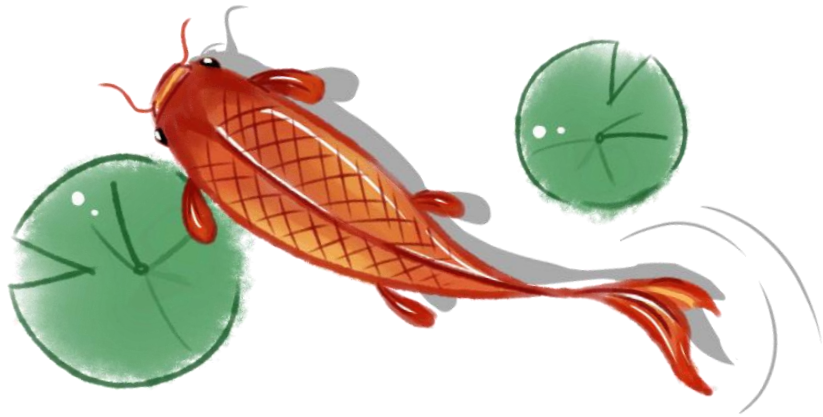
- SPDB在每个条目中隐藏有指针：
  无论对于外出IP包还是进入IP包，首先都要对SPDB表进行查询，以决定是否丢弃、绕过或应用IPsec
  - IPsec查询SADB，检查是否拥有合适的SA
  - 如果有，则进行相应的IPsec处理
  - 如果没有，就会向IKE守护进程发出创建SA请求

- IKE守护进程接收到内核发来的请求后，查询SPDB，得到所有协商参数；然后向远程IKE进程发出协商请求；IKE进程开始协商

IKE工作过程

- 如果协商成功，把新协商的SA增加到SADB中
  - 如果因为SPDB参数问题，协商未成功，IKE进程给策略及SA管理模块提示，由管理员来配置SPDB参数
- 当管理员指示IKE守护进程不再使用某个SA时， IKE守护进程会从SADB中删除掉相应的记录SA，同时会向远地的IKE守护进程发送删除信息，表示本地已经不再使用此SA了
- 远地IKE进程收到此信息后，根据实际的要求作不同的处理：
  - 可以选择删除相应的SA
  - 也可以选择忽略此信息，继续保留相应的SA，但是不允许使用此SA继续通信

IKE协议总结



IKE协议的不足

- IKE是一组复杂混合协议集合，虽然发展成为Internet标准，但是主要用途局限于为IPsec通信双方建立安全关联SA
- 标准定义的复杂性（需要参考3个RFC）容易导致理解上的困难和实现上的混乱，最终会导致不同实现间的互操作困难
- 完成协商的消息往返次数过多，这样会消耗较多的计算以及网络带宽资源
- 容易受到各种攻击，由于设计缺陷，协议实现容易受到拒绝服务攻击、中间人攻击、重放攻击等多种攻击行为的威胁


Thanks a lot !

Activity is the only road to knowledge!

Computer Network Security @ 2022Fall