高级网络安全研究与应用——

安全需求与安全应用

北京邮电大学

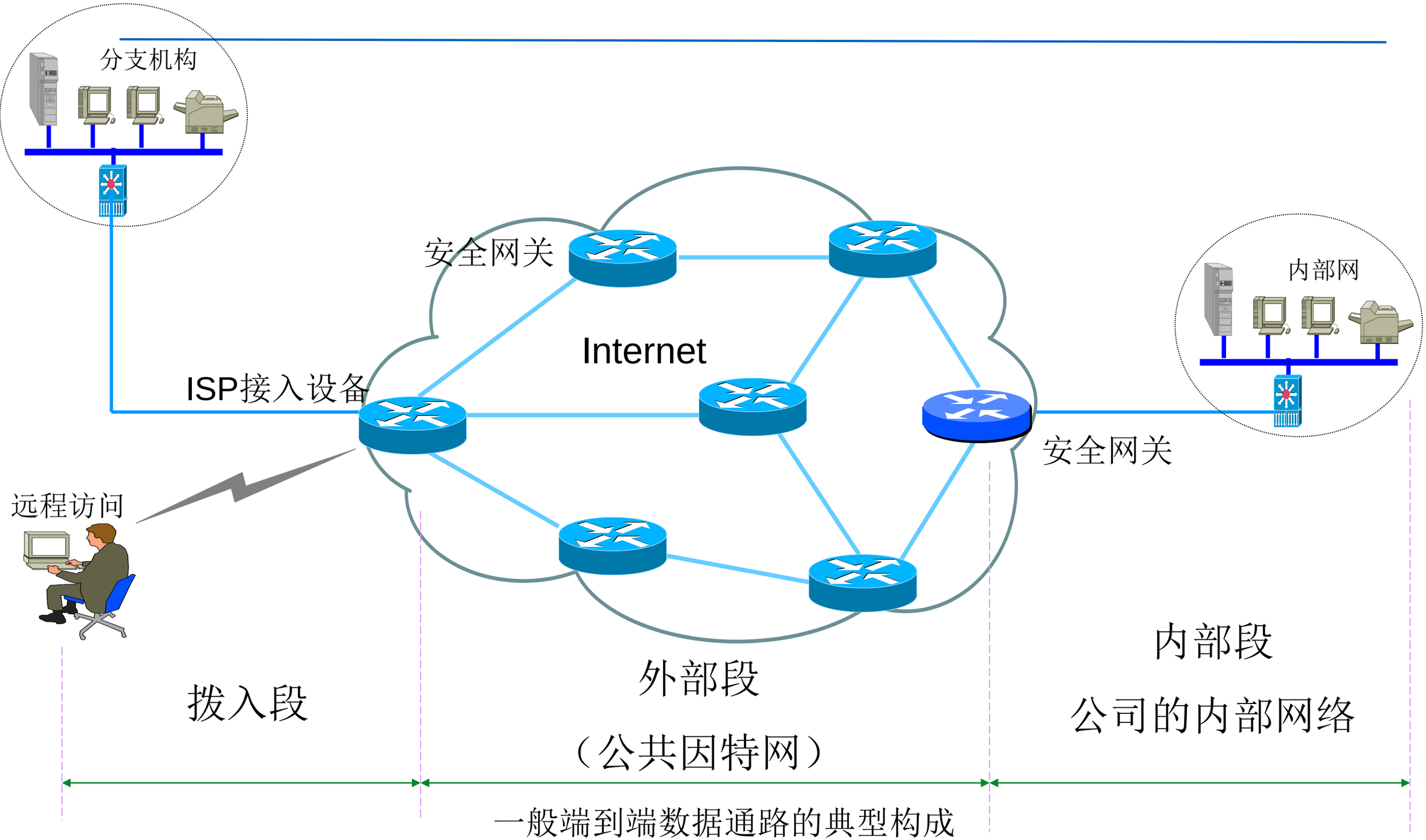
郑康锋 zkfbupt@163.com

伍淳华 wuchunhua@bupt.edu.cn

安全需求与安全应用——

一、虚拟专用网

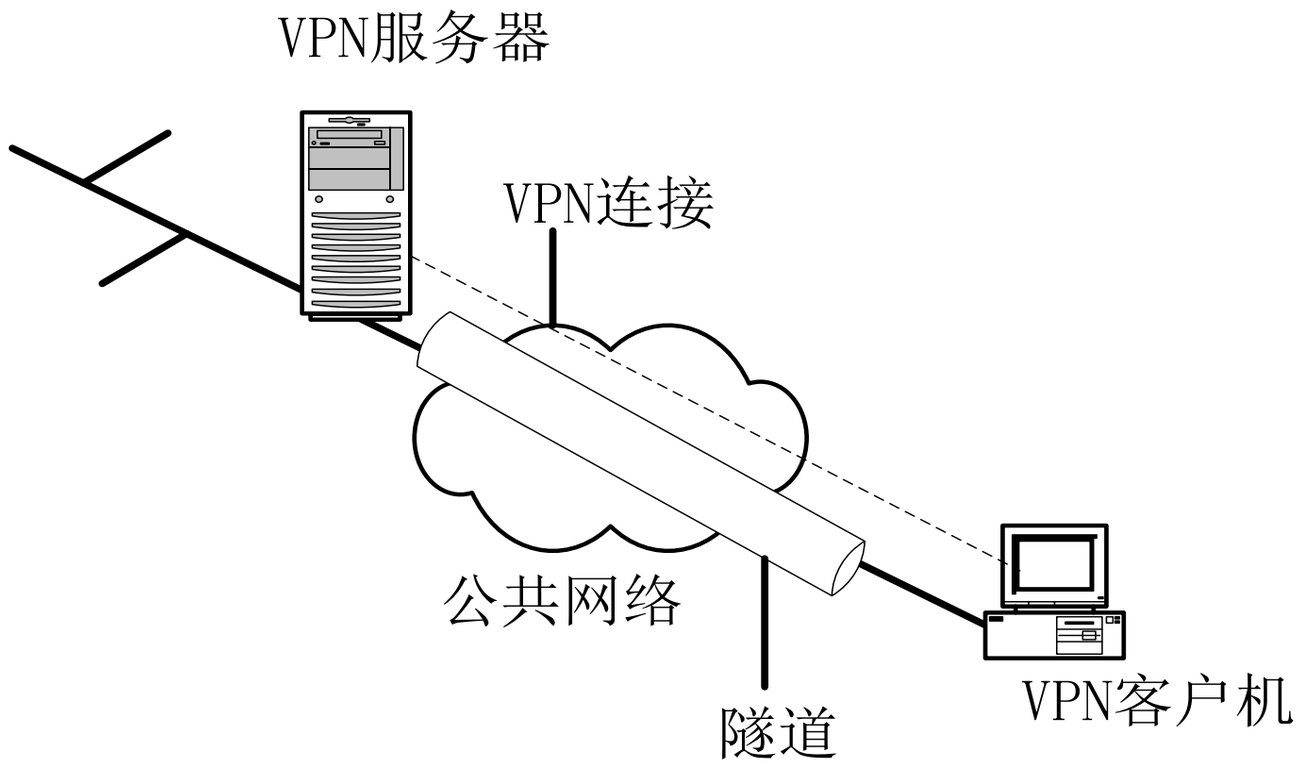
VPN提出-----端到端数据安全性



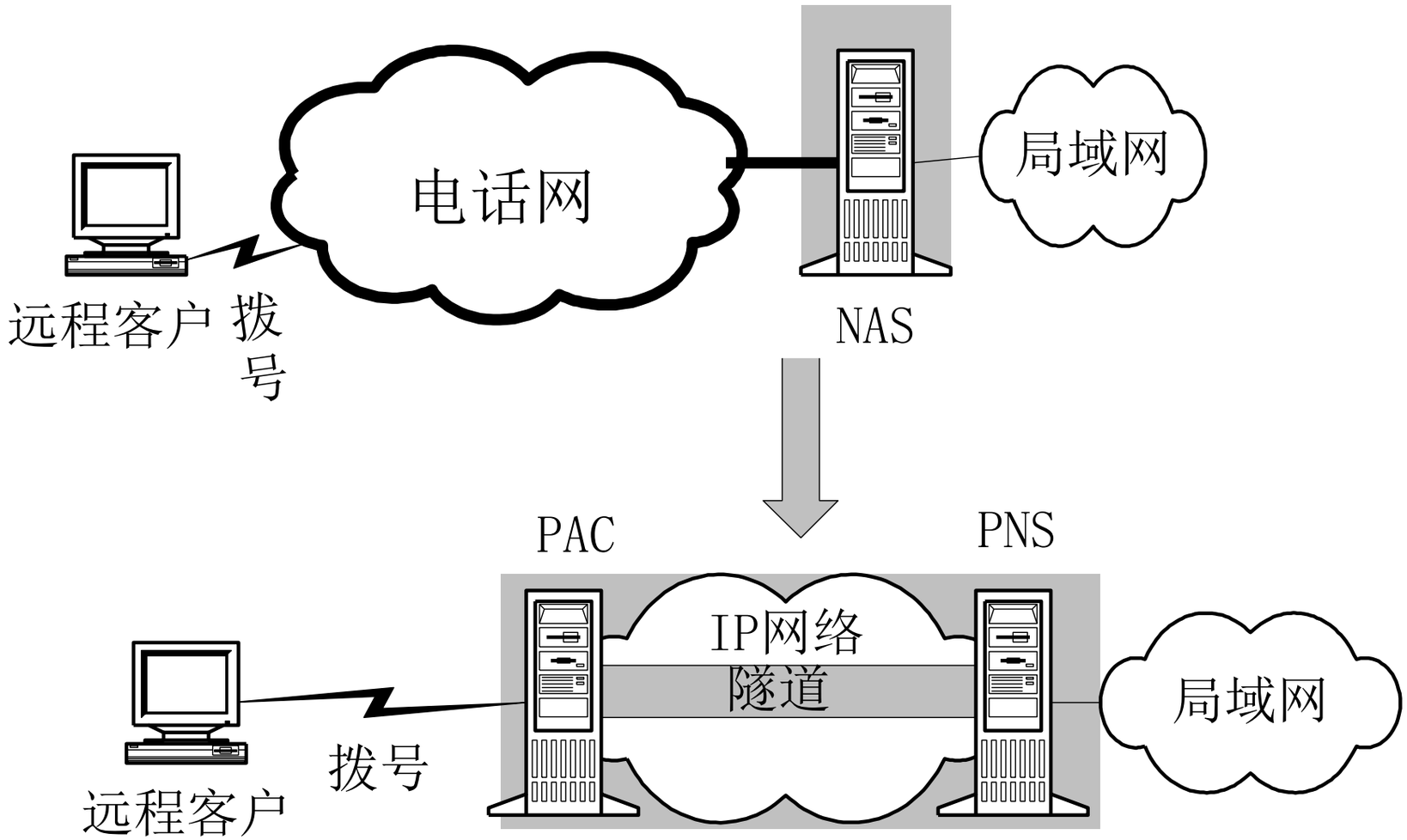
一般端到端数据通路的典型构成

VPN

- VPN：virtual private network，虚拟专用网
- VPN的定义：是指依靠ISP或其他NSP在公用网络基础设施之上构建的专用的数据通信网络，这里所指的公用网络有多种，包括IP网络、帧中继网络和ATM网络。
- IETF对基于IP的VPN定义：使用IP机制仿真出一个私有的广域网



PPTP



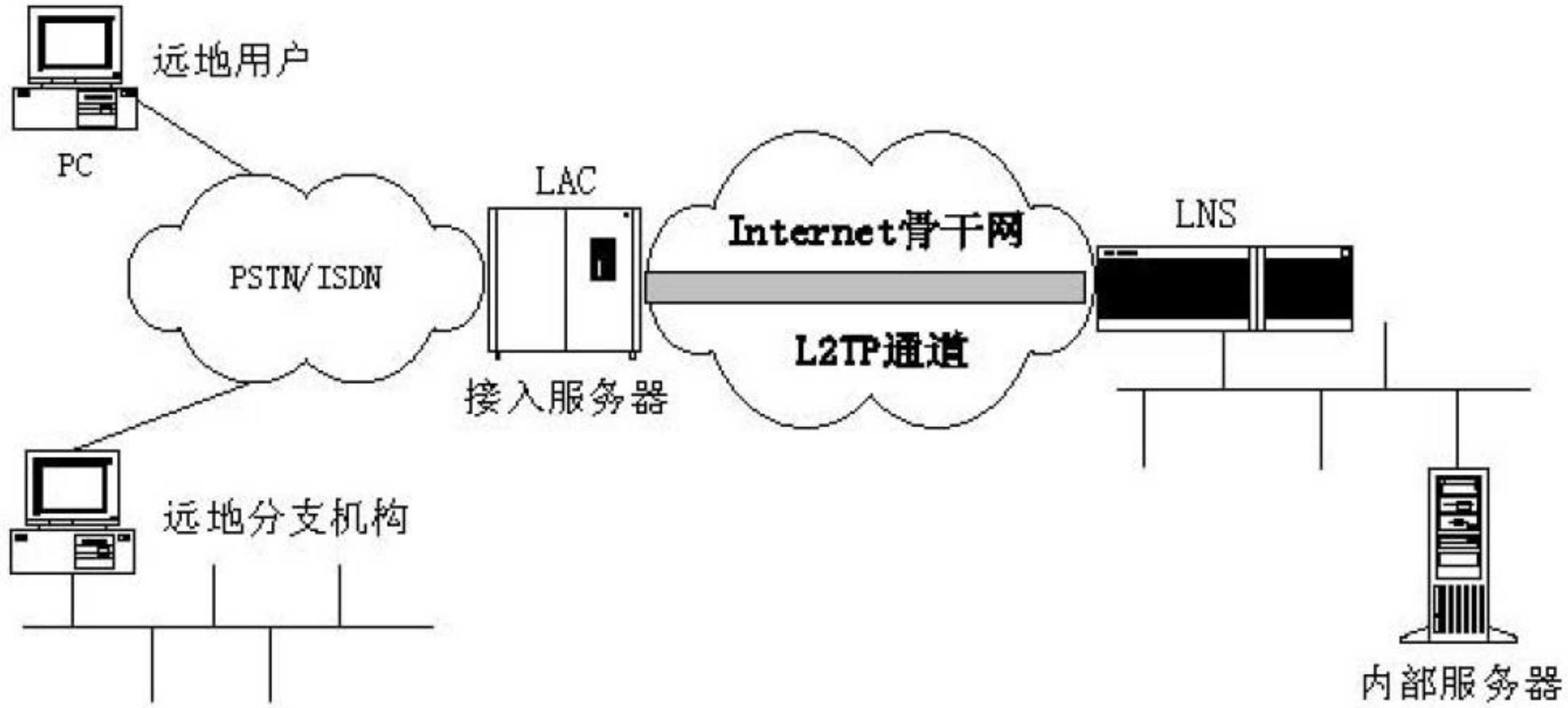
PPTP（Point-to-Point Tunneling Protocol，点到点隧道协议）是由美国微软公司设计，将PPP分组通过IP网络封装传输。

L2F

Bits 0-12													13-15	16-23	24-31
F	K	P	S	0	0	0	0	0	0	0	0	C	Ver	Protocol	Sequence (opt)
Multiplex ID														Client ID	
Length														Payload offset (opt)	
Packet key (optional)															
Payload															
														L2F Checksum (opt)	

L2F（Layer 2 Forwarding，二层转发协议），由Cisco公司提出的可以在多种介质如ATM、帧中继、IP 网上建立多协议的安全虚拟专用网（VPN）的通信方式。

L2TP



L2TP（Layer 2 Tunneling Protocol，二层通道协议），L2TP 结合了L2F 和PPTP 的优点， 可以让用户从客户端或访问服务器端发起VPN连接。L2TP 是把链路层PPP 帧封装在公共网络设施如IP、ATM、帧中继中进行隧道传输的封装协议。

L2TP

- PPTP和L2TP都使用PPP协议对数据进行封装，然后添加附加包头用于数据在互联网络上的传输。尽管两个协议非常相似，但是仍存在以下几方面的不同：

  - PPTP要求互联网络为IP网络。L2TP只要求隧道媒介提供面向数据包的点对点的连接。L2TP可以在IP（使用UDP），桢中继永久虚拟电路（PVCs),X.25虚拟电路（VCs）或ATM VCs网络上使用。

  - PPTP只能在两端点间建立单一隧道。L2TP支持在两端点间使用多隧道。使用L2TP，用户可以针对不同的服务质量创建不同的隧道。

  - L2TP可以提供包头压缩。当压缩包头时，系统开销（overhead）占用4个字节，而PPTP协议下要占用6个字节。

  - L2TP可以提供隧道验证，而PPTP则不支持隧道验证。但是当L2TP或PPTP与IPSEC共同使用时，可以由IPSEC提供隧道验证，不需要在第2层协议上验证隧道

IPSec体系结构

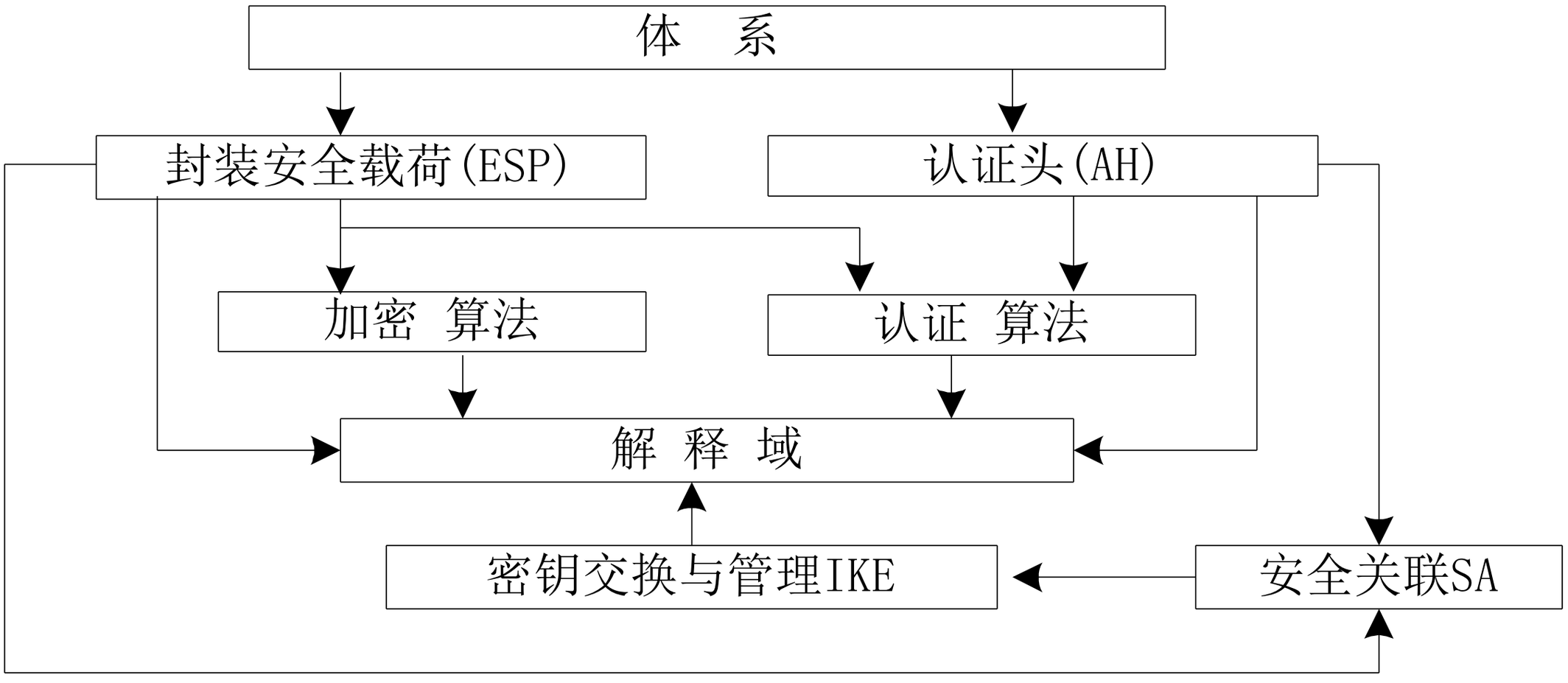
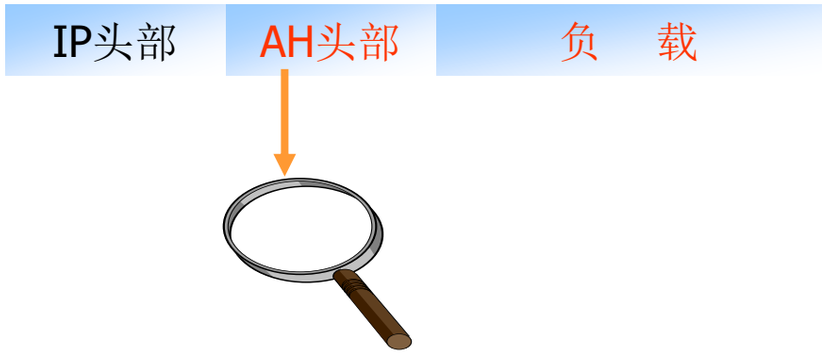


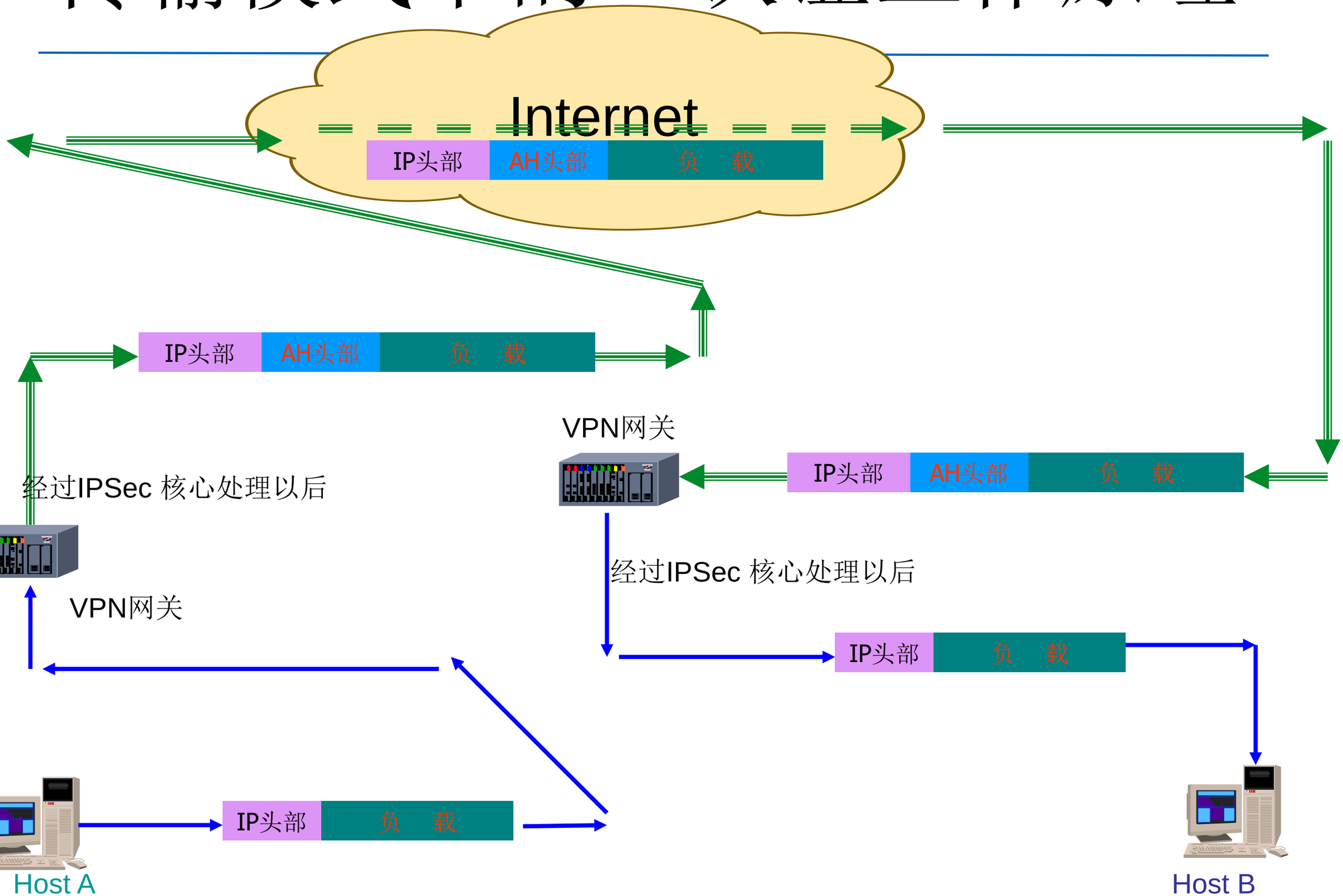
图 IPSec安全体系结构

认证头部(AH)

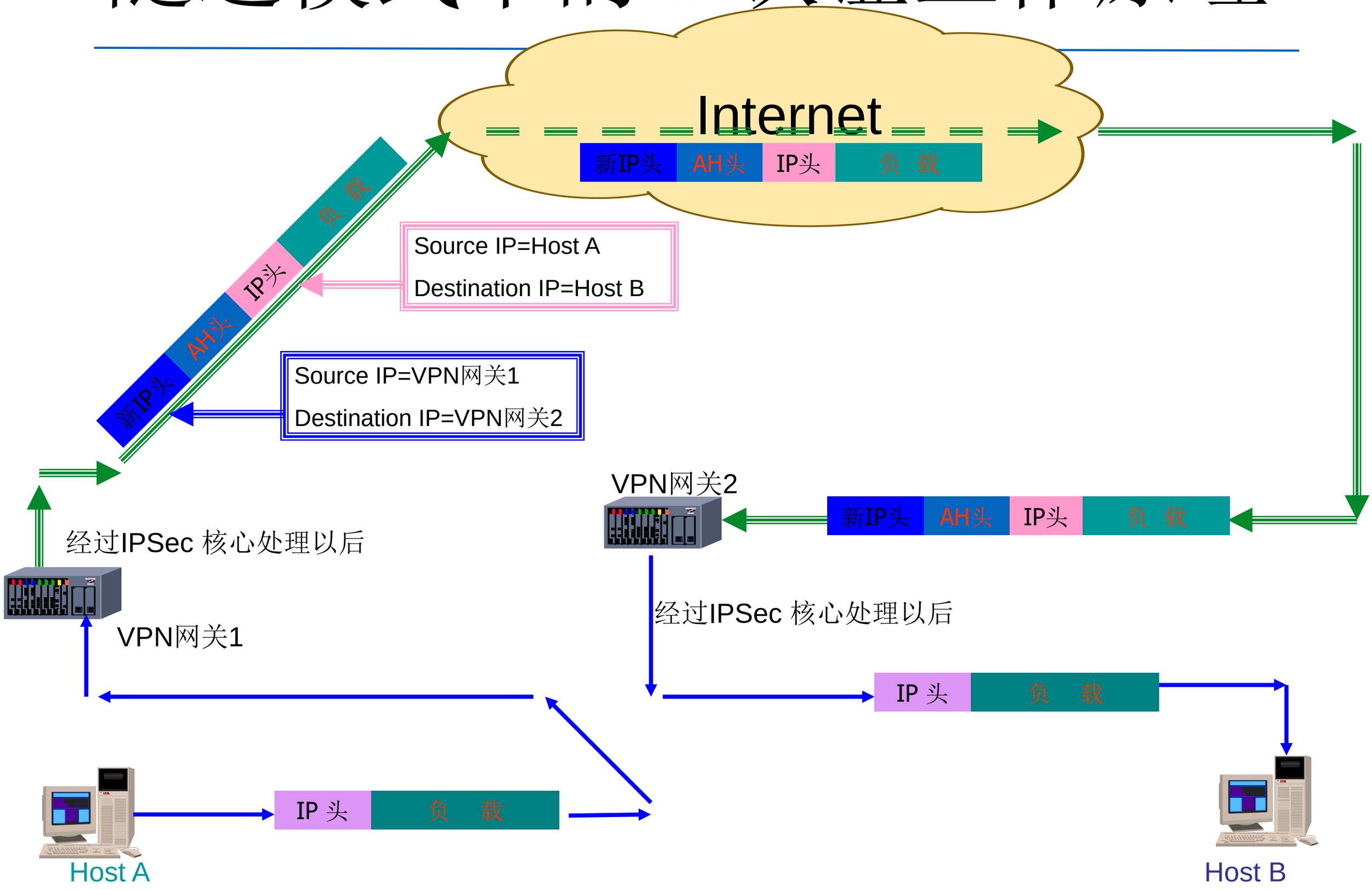


- ❖认证数据：一个变长字段，也叫Integrity Check Value，由SA初始化时指定的算法来计算。长度=整数倍32位比特
- ❖序列号：32比特，一个单项递增的计数器，用于防止重放攻击，SA建立之初初始化为0，序列号不允许重复
- ❖SPI：32比特，用于标识有相同IP地址和相同安全协议的不同SA。由SA的创建者定义，只有逻辑意义
- ❖ 下一头部：8比特，标识认证头后面的下一个负载类型
- ❖保留字段：16比特，保留将来使用，Default=0
- ❖ 负载长度：8比特，表示以32比特为单位的AH头部长度减2，Default=4

传输模式下的AH认证工作原理



隧道模式下的AH认证工作原理



ESP协议

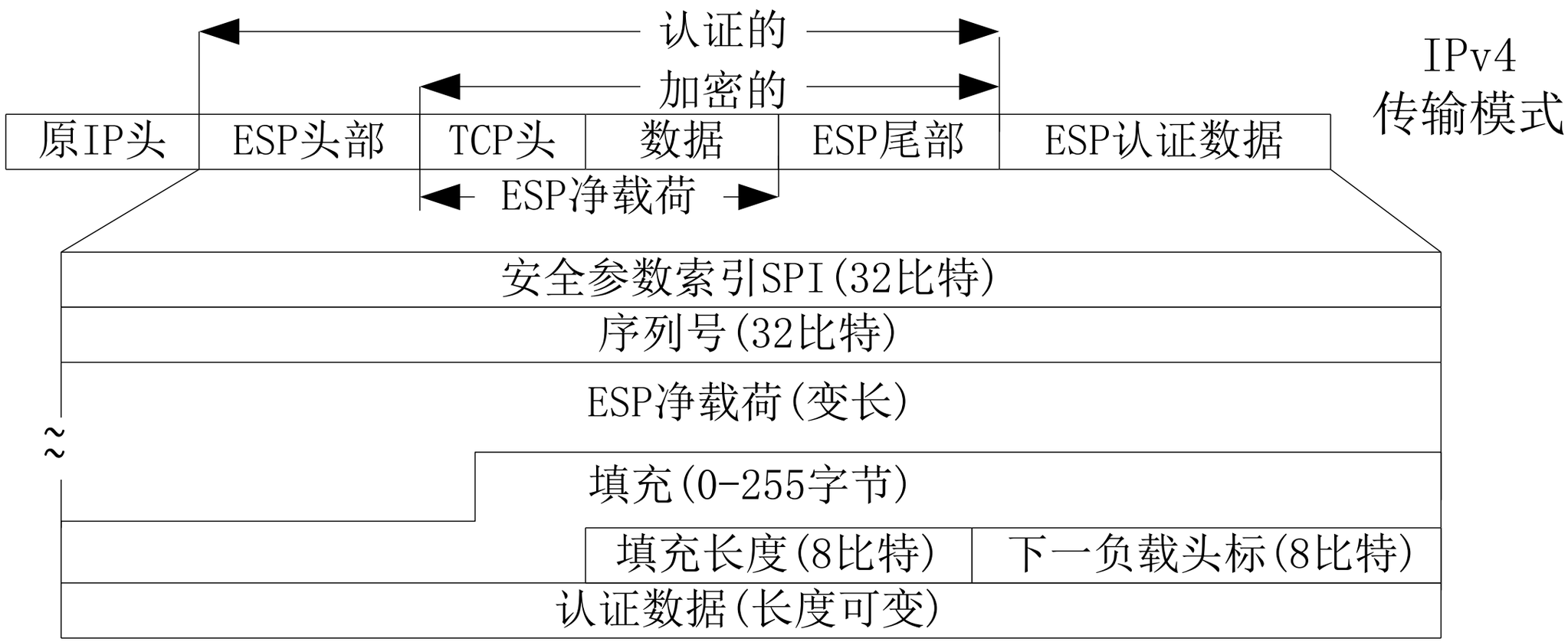
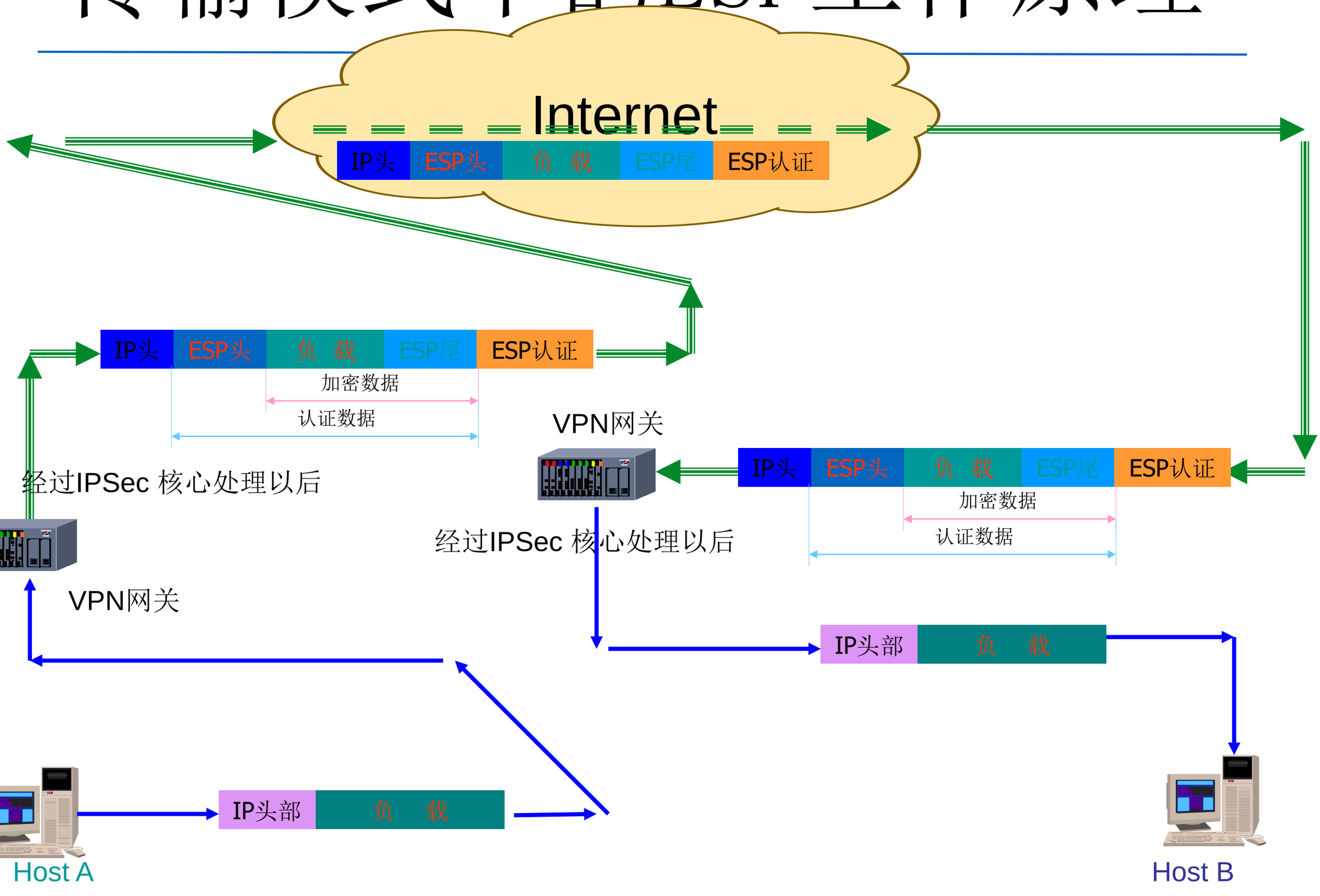


图 ESP格式

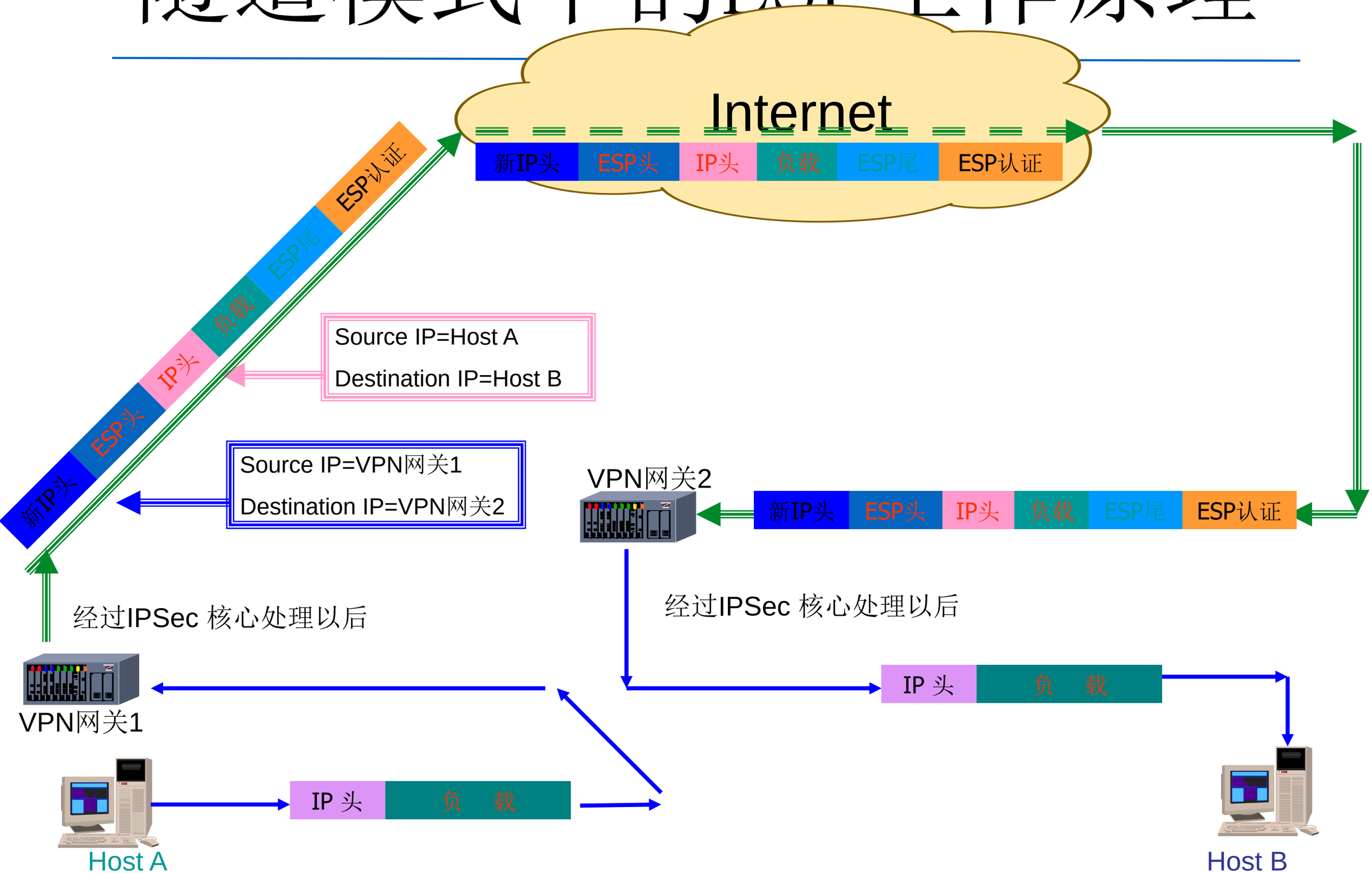
负载安全封装(ESP)

- ❖认证数据：一个变长字段，也叫Integrity Check Value，由SA初始化时指定的算法来计算。长度=整数倍32位比特
- ❖ 填充长度：8比特，给出前面填充字段的长度，置0时表示没有填充
- ❖ 填充字段：8比特，大多数加密加密算法要求输入数据包含整数各分组，因此需要填充
- ❖负载数据：包含由下一头部字段给出的变长数据
- ❖序列号：32比特，一个单项递增的计数器，用于防止重放攻击，SA建立之初初始化为0，序列号不允许重复
- ❖SPI：32比特，用于标识有相同IP地址和相同安全协议的不同SA。由SA的创建者定义，只有逻辑意义
- ❖ 下一头部：8比特，标识认证头后面的下一个负载类型

传输模式下的ESP工作原理



隧道模式下的ESP工作原理



IPSec传输模式

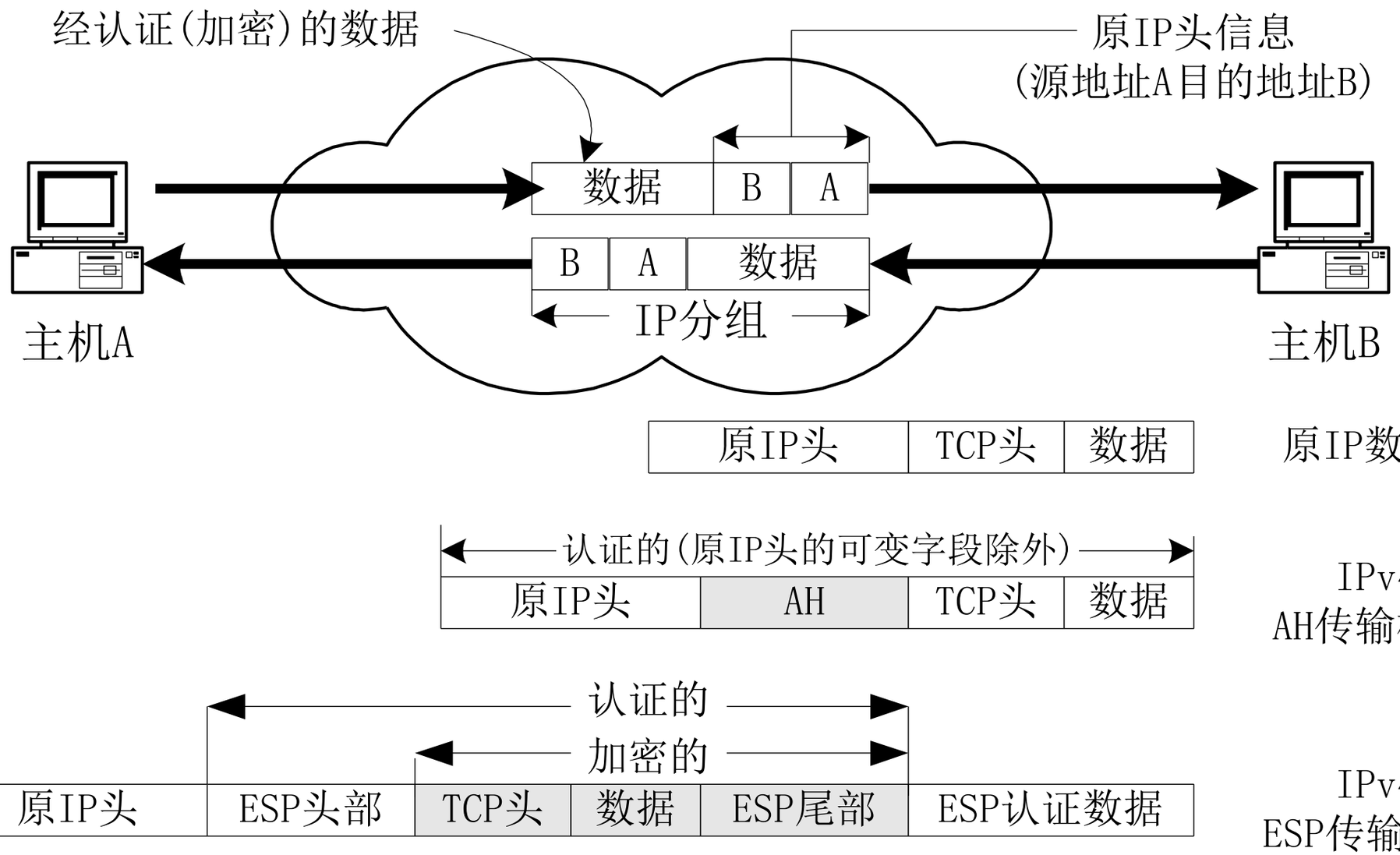
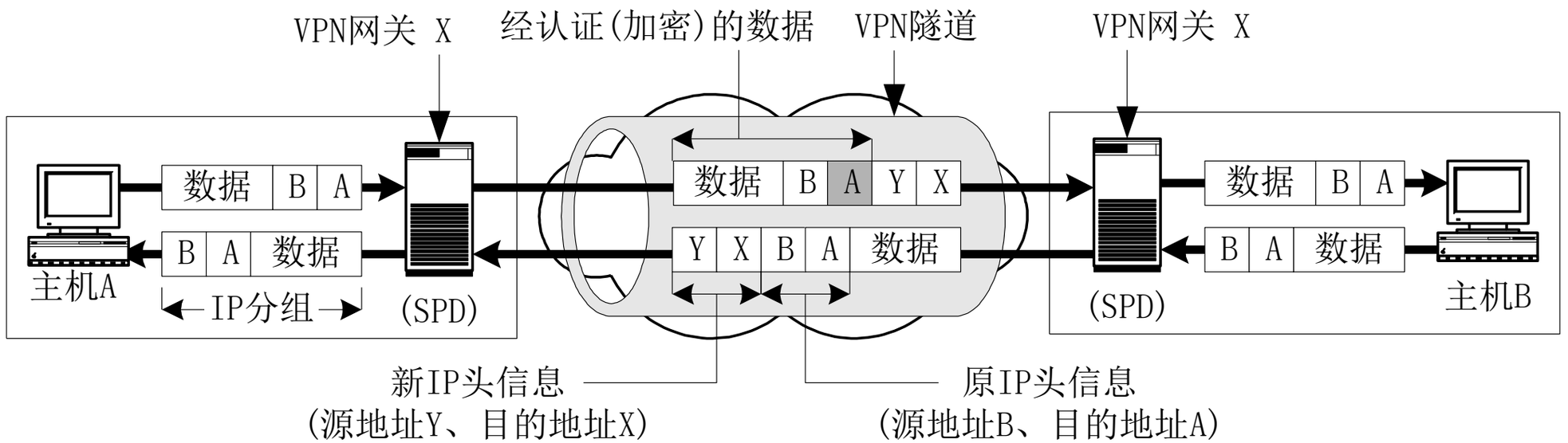


图 IPSec传输模式下的AH、ESP数据封装格式

IPSec隧道模式



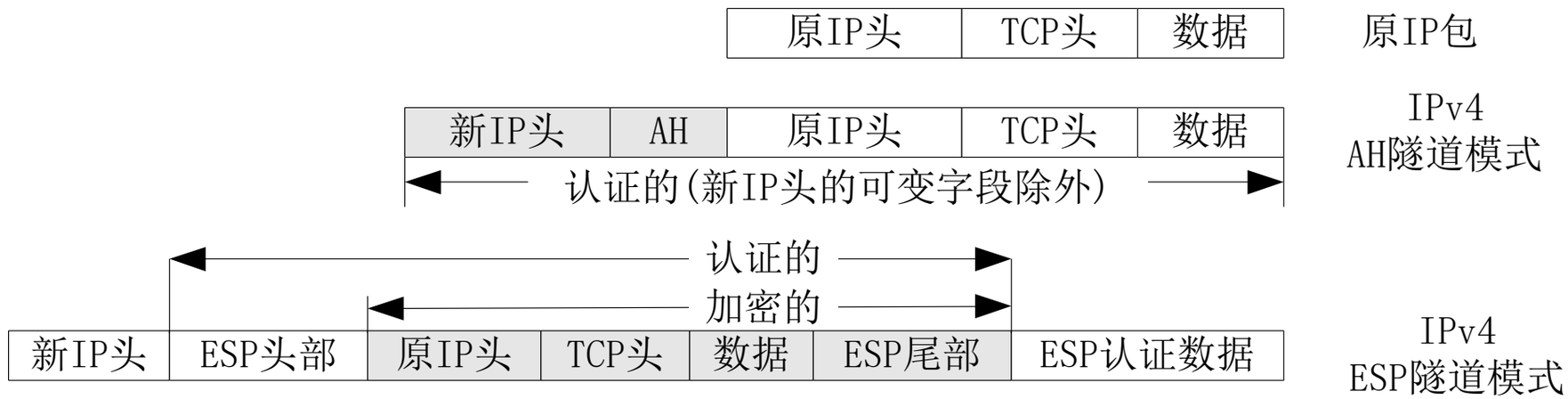


图 IPSec隧道模式下的AH、ESP的数据封装格式

IKE基本情况

IKE： Internet Key Exchange，互联网密钥交换

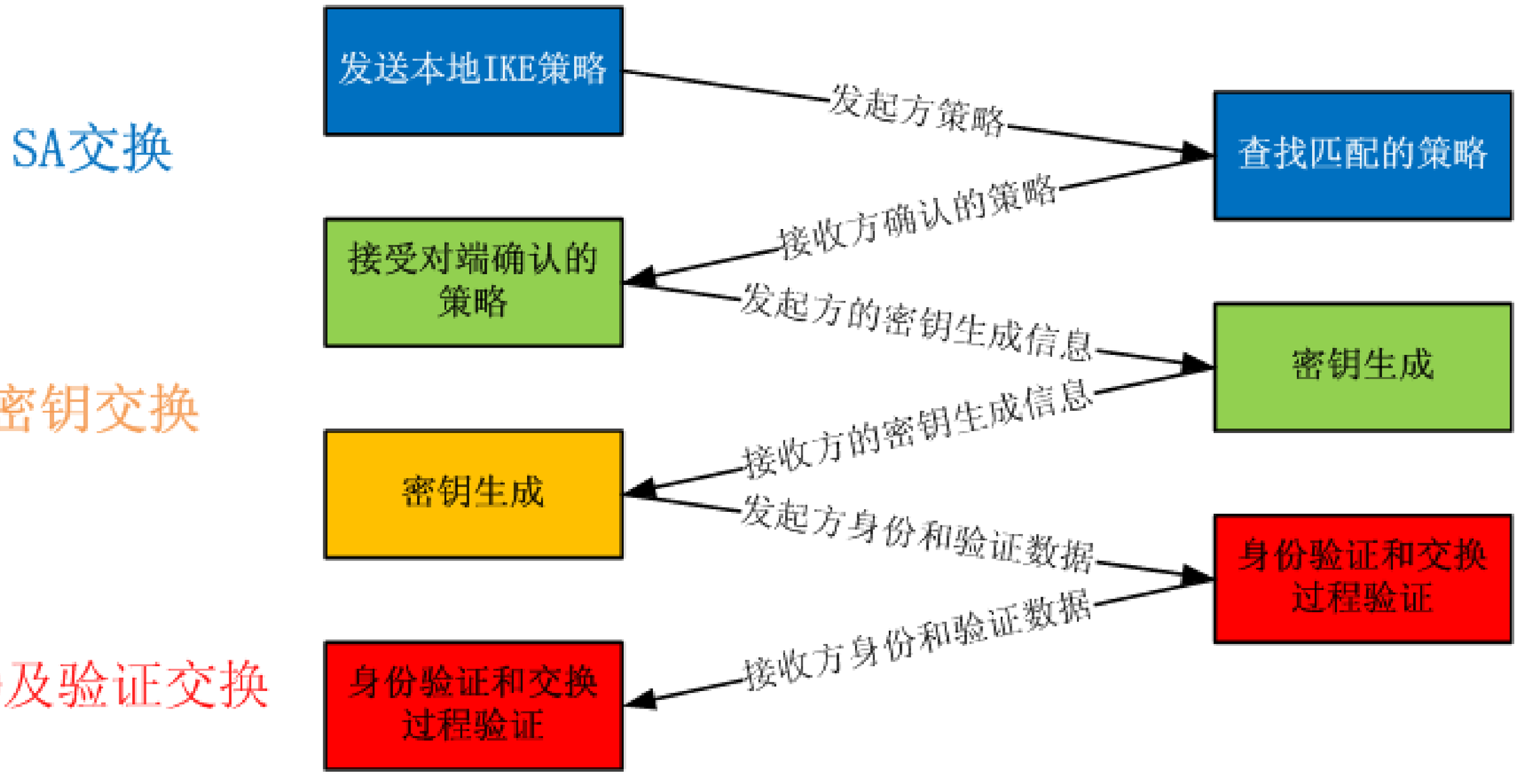
- 功能
  - 用IPSec保护数据包，必须首先建立一个IPSec的安全联盟，这个安全联盟可以手工建立，也可以动态由特定进程来创建。这个特定的进程就是Internet Key Exchange,即IKE。IKE的用途就是在IPSec通信双方之间通过协商建立起共享安全参数及验证过的密钥，也就是建立安全联盟。
  - IKE协议是Oakley和SKEME协议的混合，在由ISAKMP规定的一个框架内运作，可以为多种需要安全服务的协议进行策略磋商和密钥建立，比如SNMPv3,OSPFv2,IPSec等。

密钥交换的两个阶段

- **阶段一交换**(phase1 exchange)：在“阶段一”周期里，两个IKE实体建立一个安全的，经验证的信道进行后续通信，要建立这样的安全信道，双方会建立一对ISAKMP安全联盟。阶段一交换可以用**身份保护模式(也叫主模式)或野蛮模式**来实现，而这两种模式也仅用于阶段一中。

- **阶段二交换**(phase2 exchange)：“阶段二”周期里，IKE实体会在阶段一建立起来的安全信道中，为某种进程协商和产生需要的密钥材料和安全参数，在VPN实现中，就是**建立IPSec安全联盟**。快速模式交换可用来实现阶段二交换并且仅用于此阶段中。

IKE阶段一协商流程简图



交换流程（2）阶段一说明

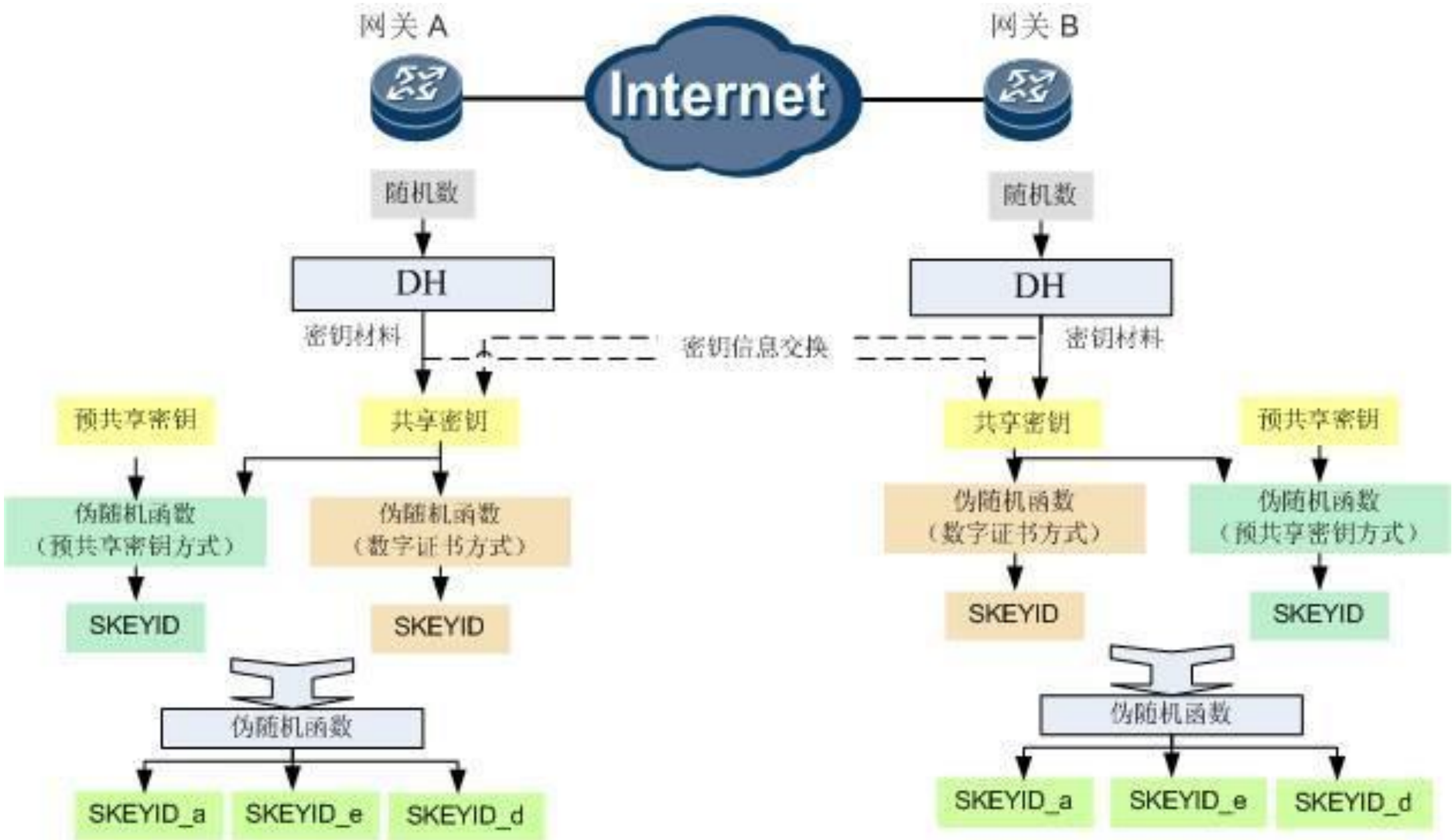
- 在消息(1)中，发起者生成他认为适当的安全提案列表，提交给响应方。消息(2)中，响应者与本地策略进行匹配和选择之后，将最终决定的安全联盟内容同样用相应载荷回送发起者。

- 在消息(3)、(4)中，发起者和响应者交换DH公开值，和随机信息串nonce，在第四步完成时，双方已经可以经计算得出共享的DH公共值，以及各自计算出SKEYID和相关衍生密钥。

- 消息(5)和消息(6)中，双方使用前两步得出的加密、验证算法和密钥保护传输的数据。

- 当采用数字签名的身份验证方法时，消息(5)和(6)可以包含证书载荷，将自己的公钥证书发给对方，验证数据AUTH DATA就是数字签名的运算结果，在这里数字证书也可以是从有效的远程有效的认证中心通过LDAP、DNSSEC等协议获得。

交换流程（2）阶段一说明



DH交换及密钥生成

Diffie-Hellman密钥交换

D-H交换的安全性源于在有限域上计算离散对数比计算指数更为困难。

DH交换的原理简述如下。

通信双方为 Alice和Bob,双方约定好一个参数组，其中指定了运算中使用的质数 p和底数 g,Alice和Bob分别选择一个随机的私人数字a和b,然后两人分别计算：

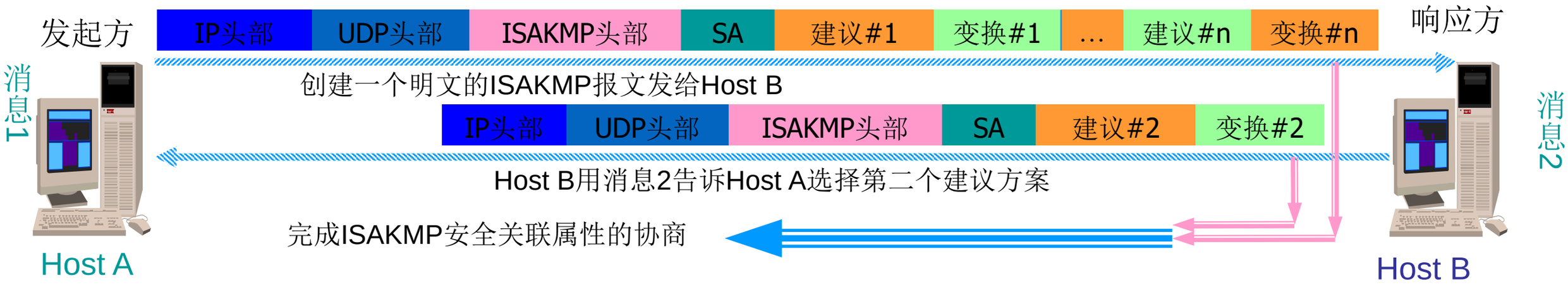
Alice: $A = g^a \bmod p$ Bob: $B = g^b \bmod p$

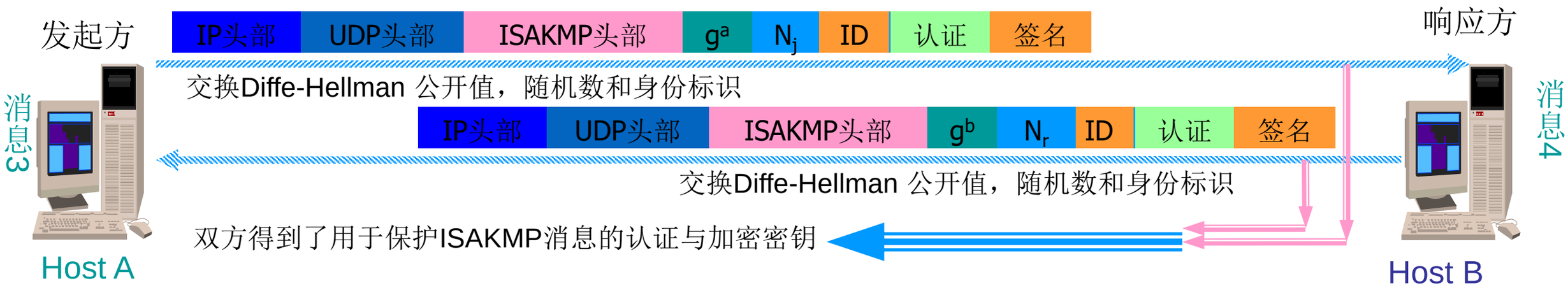
通过开放信道，两人交换 A和B,然后再次进行乘幂运算，使用收到的数字作底数，生成共享的一个公共值：

$$B^a \bmod p = g^{ab} \bmod p = A^b \bmod p$$

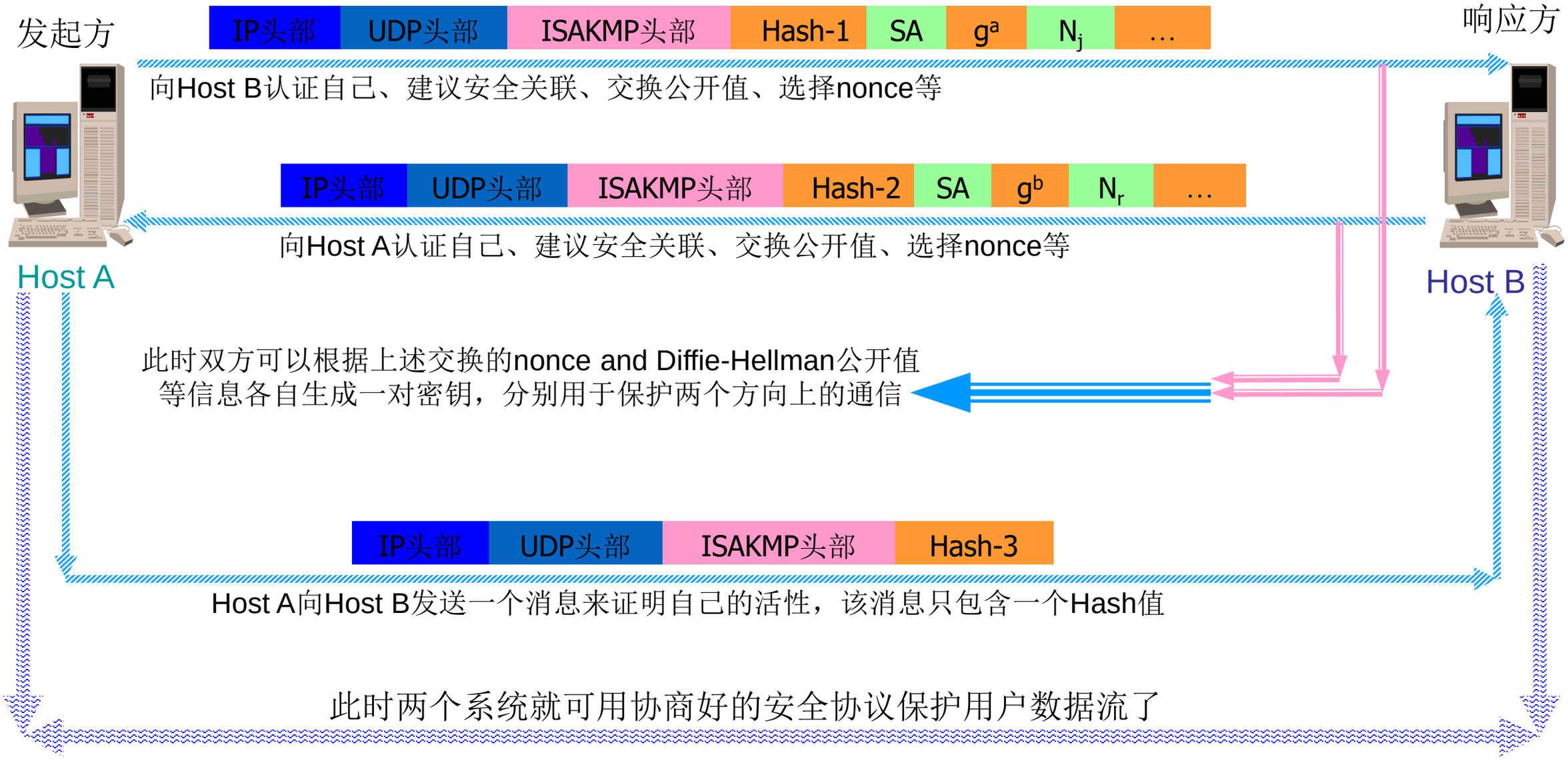
在交换运算过程中，只有私人数字a和b需要保密，其他数字 A, B, g, p都不必保密。交换双方生成共享密钥后，就可以用之来保护后续的通信，这样，原来不安全的信道就变得安全了。

ISAKMP/Oakley 阶段一工作原理





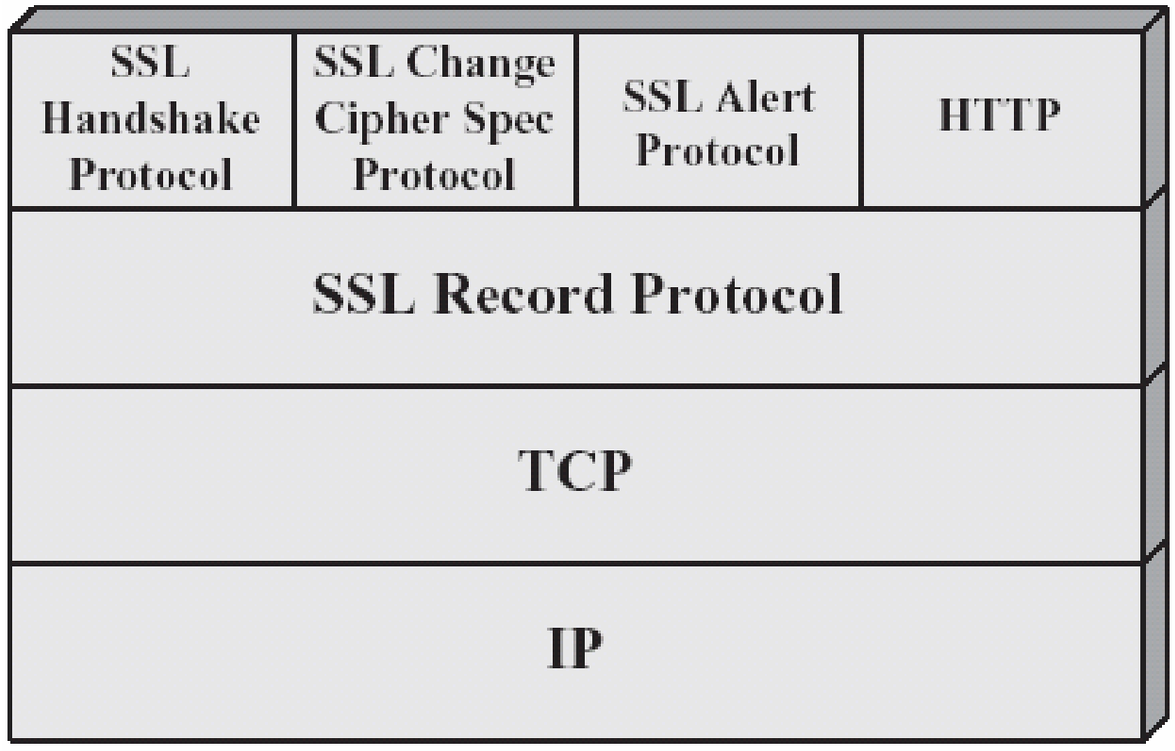
ISAKMP/Oakley 阶段二工作原理



SSL协议体系

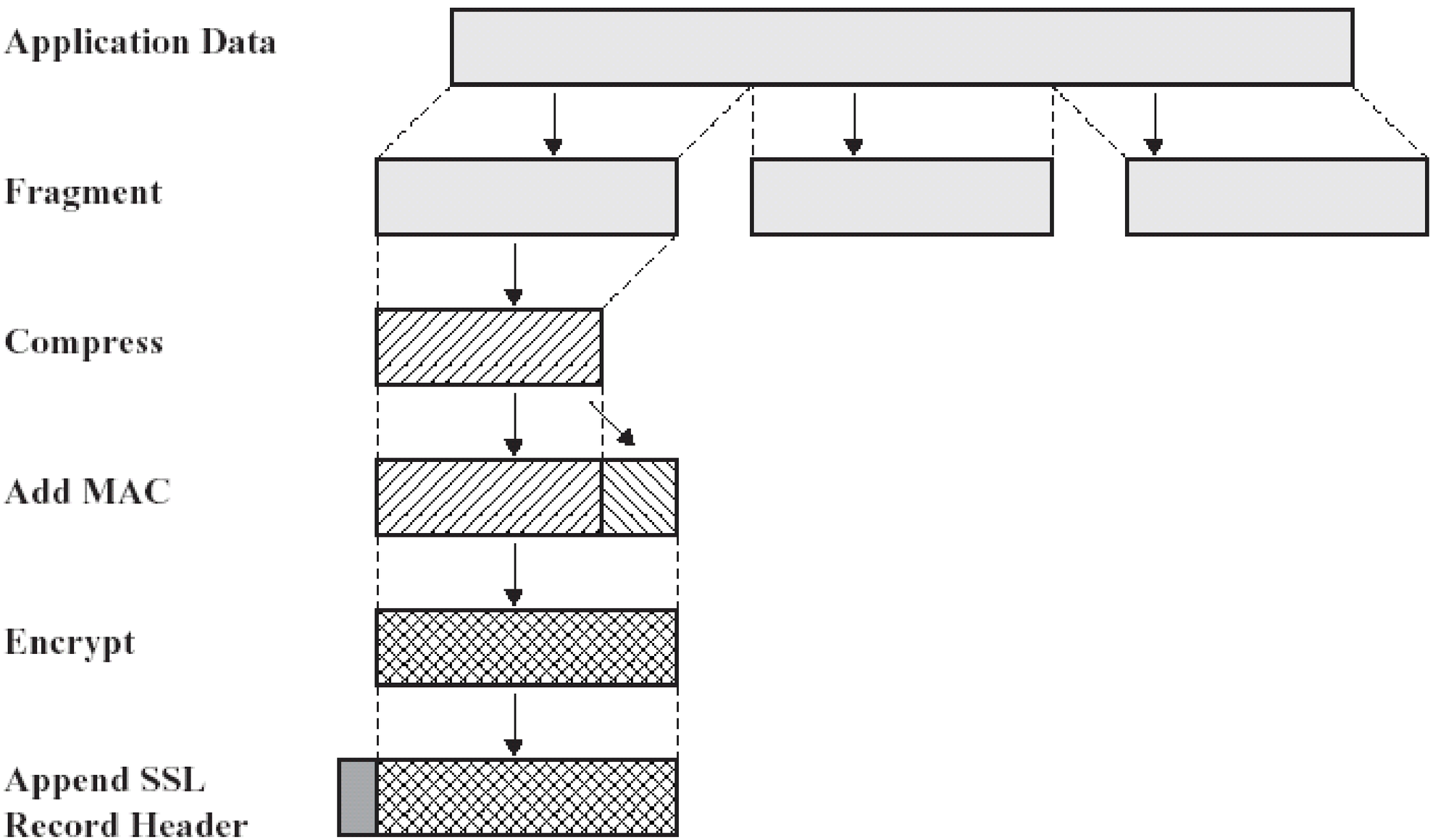
- SSL被设计用来使用TCP提供一个可靠的端到端安全服务。

- 协议分为两层
  - 底层：SSL记录协议
  - 上层：SSL握手协议、SSL密码变化协议、SSL警告协议



SSL记录层协议

- 记录层数据封装过程

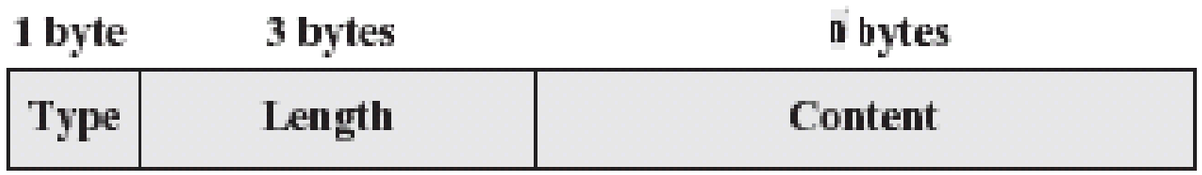


两个重要概念

- SSL连接（connection）
  - 一个连接是一个提供一种合适类型服务的传输（OSI分层的定义）
  - SSL的连接是点对点的关系
  - 连接是暂时的，每一个连接和一个会话关联
- SSL会话（session）
  - 一个SSL会话是在客户与服务器之间的一个关联。会话由Handshake Protocol创建。会话定义了一组可供多个连接共享的加密安全参数。
  - 会话用以避免为每一个连接提供新的安全参数所需昂贵的谈判代价。

SSL密钥交换——协议整体情况

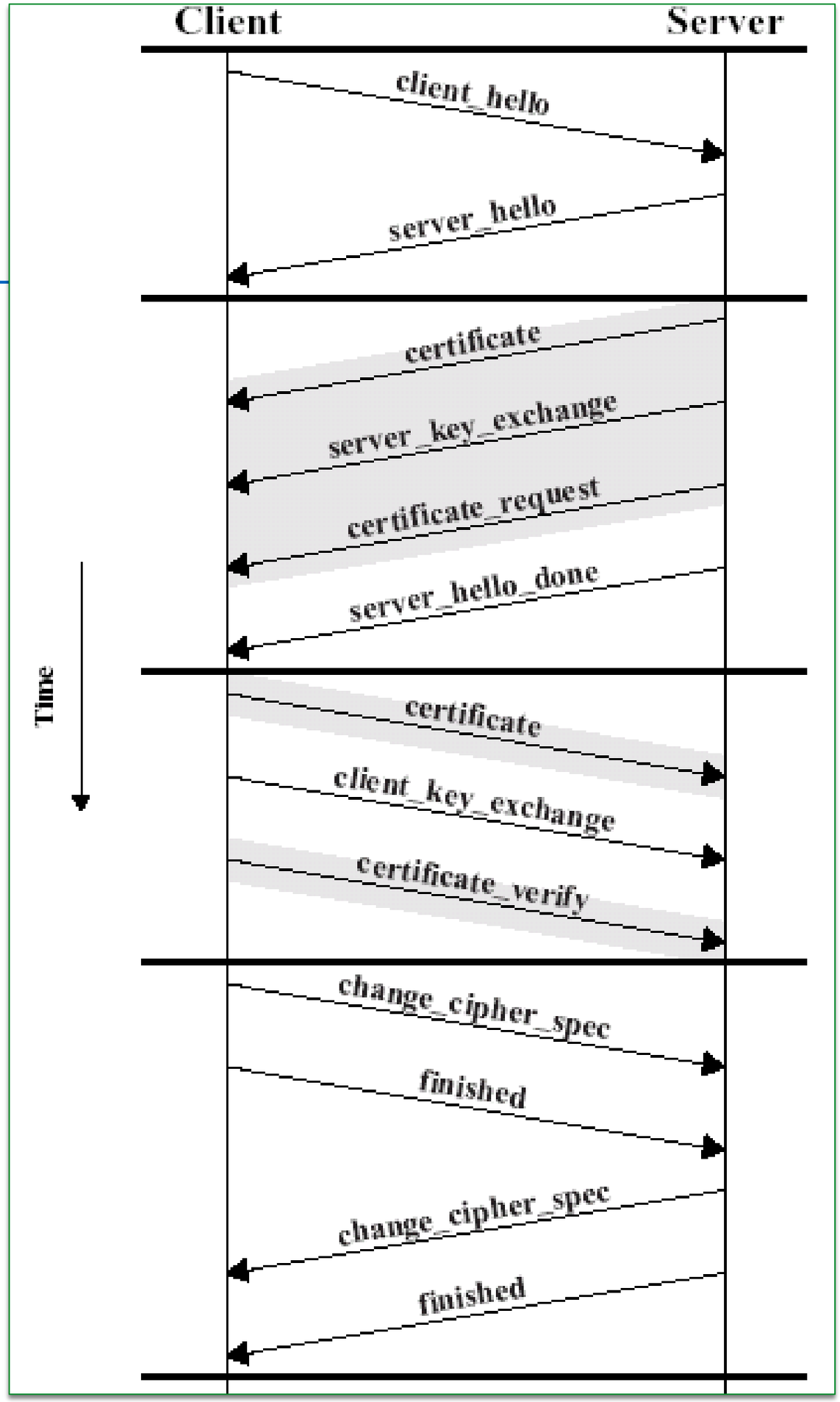
- 功能
  - 客户和服务器之间相互认证
  - 协商加密算法和密钥
  - 它提供连接安全性，有三个特点
    - 身份认证，至少对一方实现认证，也可以是双向认证
    - 协商得到的共享密钥是安全的，中间人不能够知道
    - 协商过程是可靠的
- 规范说明
  - 位于TLS记录协议之上，也用到了TLS记录协议的处理过程
  - ContentType = 22
  - 协议格式如图：



Handshake Protocol

整体流程

- (1)、交换Hello消息，对于算法、交换随机值等协商一致
- (2)、交换必要的密码参数，以便双方得到统一的premaster secret
- (3)、交换证书和相应的密码信息，以便进行身份认证
- (4)、产生master secret
- (5)、把安全参数提供给TLS记录层
- (6)、检验双方是否已经获得同样的安全参数



问题和讨论