# 第一章：网络安全综述

## 概念、定义、名词

常见的**不安全因素**：

- 物理因素：物理设备的不安全，电磁波泄漏等
- 系统因素：系统软、硬件漏洞，病毒感染，入侵
- **网络因素**：网络协议漏洞，会话劫持、数据篡改，网络拥塞，拒绝服务
- 管理因素：管理员安全意识淡漠，误操作

不安全的**原因**：

- **自身的缺陷**：系统软硬件缺陷、网络协议的缺陷
- **开放性**
  - **系统开放：**计算机及计算机通信系统是根据行业标准规定的接口建立起来的。
  - **标准开放：**网络运行的各层协议是开放的，并且标准的制定也是开放的。
  - **业务开放：**用户可以根据需要开发新的业务
- **黑客攻击**

**网络安全的特征**：

- **机密性**：信息不泄漏给非授权的用户、实体或者过程的特性。
- **完整性**：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏的特性。
- **可用性**：可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息。
- **（可控性）**：对网络信息的传播及内容具有控制能力

**常见攻击**：社会工程、口令破解、地址欺骗、连接盗用、网络窃听、数据篡改、恶意扫描、基础设施破坏、拒绝服务、数据驱动攻击。总的来说有：

- 中断：可用性
- 窃听：机密性
- 修改：完整性
- 伪造：**可认证性**

## 安全模型、安全体系结构

**网络参考模型**：ISO - OSI模型，TCP/IP模型

### 安全体系结构

在X.800中定义为**安全攻击、安全机制、安全服务**三个层面。用一种或多种**安全机制**来实现**安全服务**，**安全服务**致力于抵御**安全攻击。**

**安全攻击**：

- 主动攻击：篡改、伪装、重放、拒绝服务
- 被动攻击：窃听、流量分析
- 区别在于会不会主动改变数据流

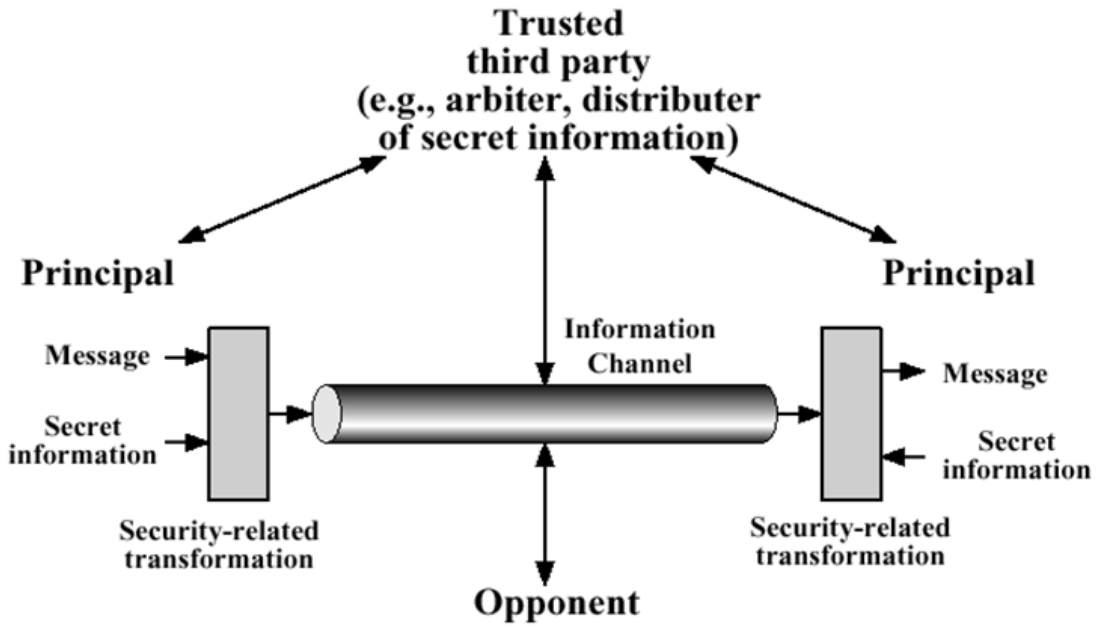
**安全机制**：加密、数字签名、访问控制、数据完整性、认证交换、流量填充、路由控制、公证

**安全服务**：X.800定义了5类14种安全服务

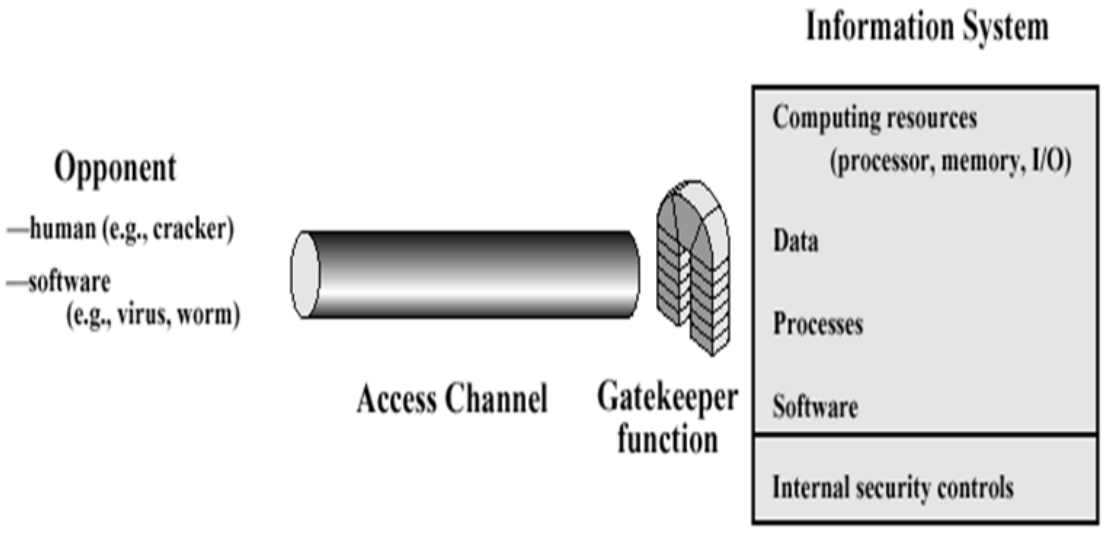
- **认证**：对等实体认证、数据源认证
- **访问控制**
- **数据机密性**：连接保密性、无连接保密性、选择域保密性、流量保密性
- **数据完整性**：具有恢复功能的连接完整性、无恢复功能的连接完整性、选择与连接完整性、无连接完整性、选择域无连接完整性
- **不可否认性**：源点的不可否认性、信宿的不可否认性

### 安全模型

- **网络安全模型**：实现端到端的安全通信。安全通道等




- **网络访问安全模型**：保护信息系统免遭恶意访问。防火墙等




# 第二章：公钥基础设施PKI

## PKI基本概念

**是什么**：

- 公钥基础设施

- 用非对称密码算法原理和技术来实现并提供安全服务的具有通用性的**安全基础设施。**是一种遵循标准的利用公钥加密技术为电子商务的开展提供安全基础平台的**技术和规范。**能够为所有网络应用提供采用加密和数字签名等密码服务所需要的**密钥和证书管理。**

**为什么要PKI**：

- 电子政务、电子商务对信息传输的安全需求，**统一标准**
- 对可信第三方的需要（CA）
- 在收发双方建立信任关系，提供身份认证、数字签名、加密等安全服务
- 收发双方不需要事先共享密钥，通过公钥加密传输会话密钥（**数字信封**）

**提供的服务**：

- **认证**：实体认证，数据源认证
- **完整性**：哈希+数字签名技术,消息认证码(数字信封传输对称密钥)
- **机密性**：数字信封传递会话密钥
- **不可否认性**：数字签名、时间戳
- **公证**：CA充当可信第三方

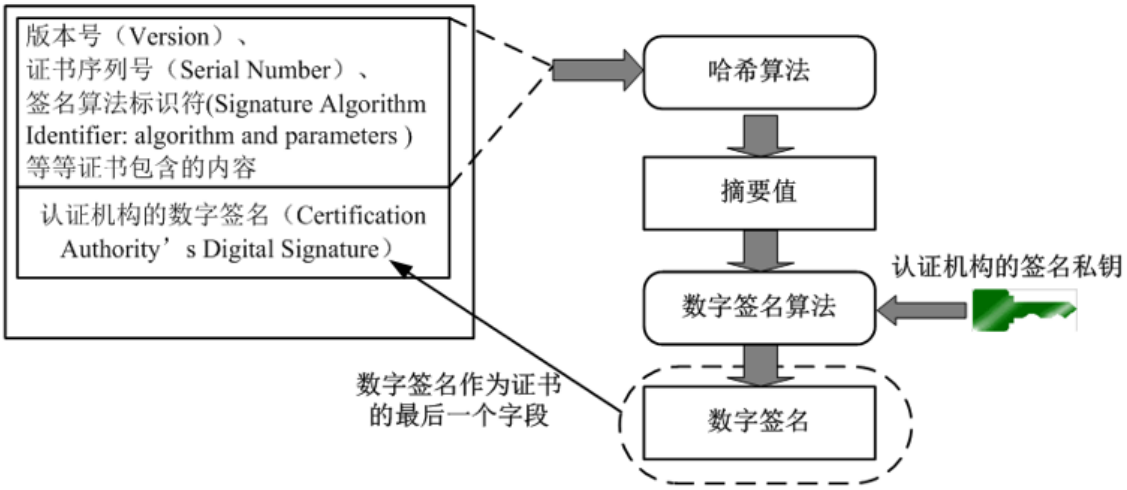
# PKI的组成

- **认证中心CA**：证书的签发机构，它是PKI的**核心构件**，是PKI应用中权威的、可信任的、公正的第三方机构。
- **注册机构RA**：按照特定的政策和管理规范对用户的资格进行审查，并执行是否同意给该申请人发放证书。撤销证书等操作，应注意的是RA**不容许直接颁发证书或CRL。**
- **证书库**：CA颁发证书和证书撤销列表CRL的集中存放地，提供公众查询，常用目录服务器提供服务
- **密钥备份及恢复系统**：
  - **签名密钥对：**签名私钥相当于日常生活中的印章效力，为保证其唯一性、抗否认性，**签名私钥不作备份。**签名密钥的生命期较长。
  - **加密密钥对：**加密密钥通常用于分发会话密钥，为防止密钥丢失时无法解密数据，**解密密钥应进行备份。**这种密钥应频繁更换。
- **证书作废处理系统**：证书由于某种原因需要作废，终止使用，这将通过证书作废列表（CRL）记录
- **自动密钥更新**：无需用户干预，当证书失效日期到来时，启动更新过程，生成新的证书
- **密钥历史档案**：由于密钥更新，每个用户都会拥有多个旧证书和至少一个当前证书，这一系列证书及相应私钥（除签名私钥）组成密钥历史档案。

# 证书的生命周期

初始化 -> 使用 -> 撤销

**证书创建**：




**证书使用**：

- 证书获取：找发送者or发布机构要
- 证书验证：验证CA签名以及验证是否在CRL中，证书链、序列号、有效期是否有效等
- 密钥恢复：**加密密钥**丢了可以找CA或信任第三方恢复
- 密钥更新：合法密钥快过期时，自动产生新的密钥并颁发证书

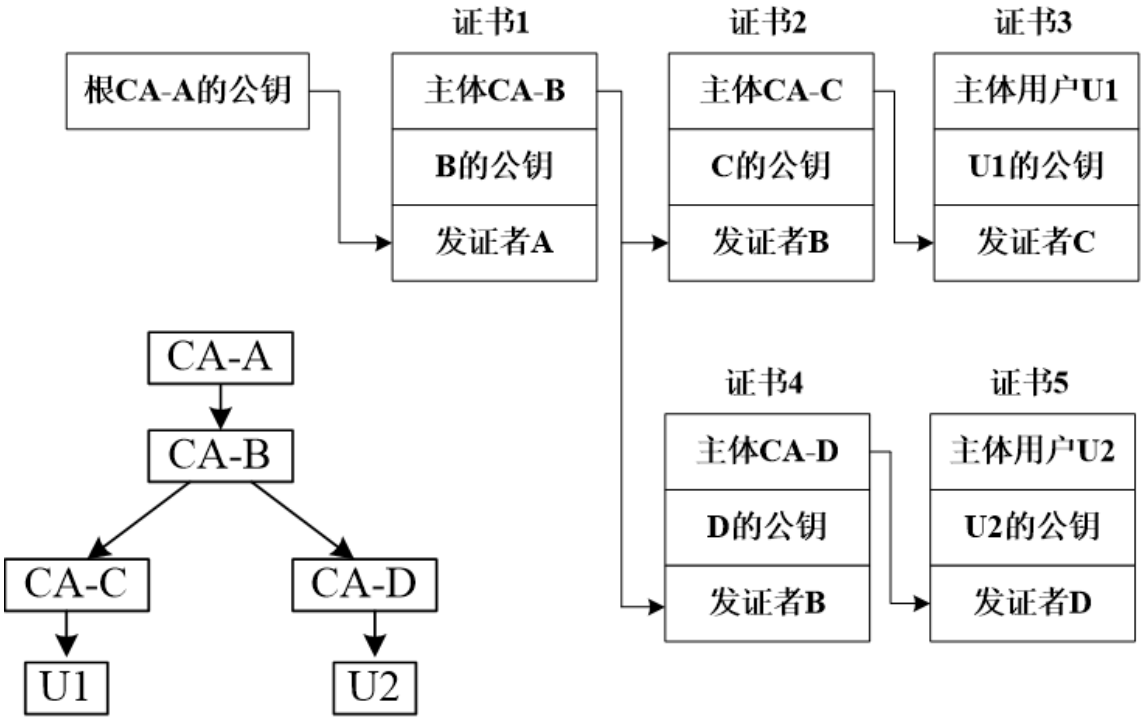
**撤销**

- 证书过期：证书生命周期的自然结束
- 证书撤销：证书在过期之前被撤销。比如私钥泄露、关系终止、CA签名私钥泄露或者变更等
- 存档：维持一个历史证书记录，以便解密之前的信息
- 审计信息

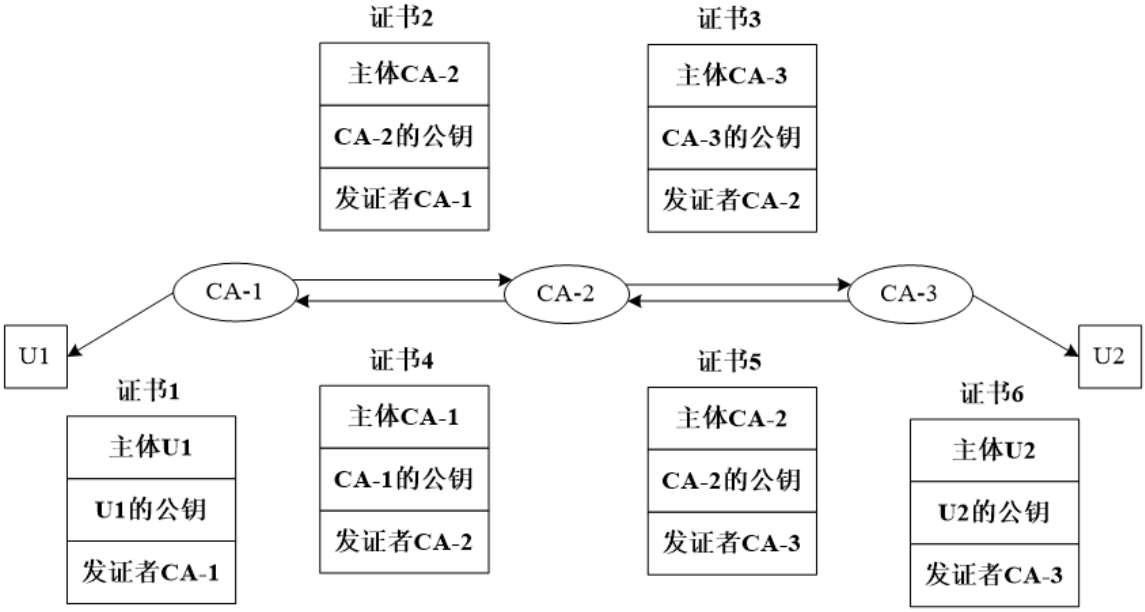
## PKI体系的互通性与标准化

**证书链**：由不同CA创建的证书序列构成，每个连续的证书都是由CA颁发的证明下一个CA公钥可信任的证书。

**严格的层次模型**：易于控制，但是根一旦被破坏整个体系都会受影响。**证书链**如下图




**分布式信任结构模型**：鲁棒性好，可拓展性好，CA间通过交叉认证在不同的CA之间建立信任。但是证书链不确定，可能会很长。更有可能出现**环路**。证书链如下图




**桥式结构**：首先要建立一个桥CA，桥CA在不同的PKI体系之间起**信任桥梁**的作用，**它不直接向用户签发证书，也不作为体系中用户的一个信任点，**只用来建立一个端到端的信任关系。

**混合结构**

## X.509标准

目前使用最多的为V3版本，V4版本还在标准化当中，PKI是在X.509基础上发展起来的

X.509标准的目的：

- 定义了一个使用X.500目录向用户提供认证服务的框架
- 每个证书包含了用户公钥，并由受信任证书颁发机构私钥签名。

# 第三章：IPSec-AH和ESP

**IPSec优点**：

- 对上层应用透明
- 可以构建可靠的虚拟专用网
- 对边界所有流量强制实现安全性，内部网络无需关注开销

## 安全关联SA、SAD/SPD

**SA**：为使通信双方的认证/加密算法及其参数、密钥的一致，相互间建立的联系被称为**安全组合或安全关联**

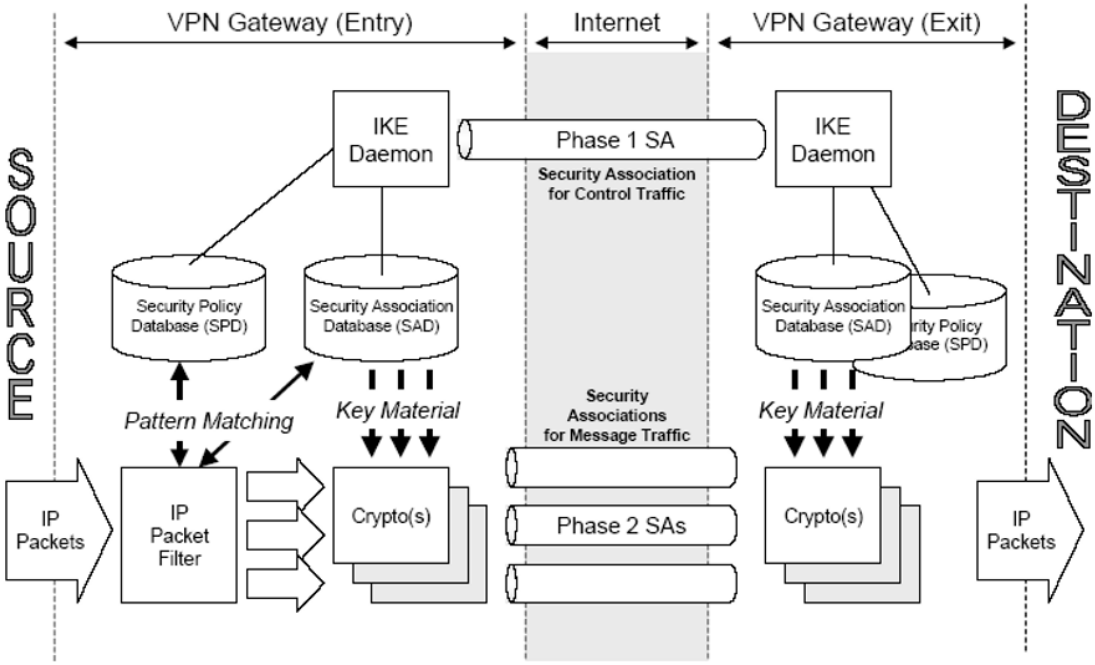
- 不同方向可能存在不同的策略，因此**SA是单向的**，在**双向通信时要建立两个SA。**对于某一主机来说，某个会话的输出数据和输入数据流处理需要两个独立的SA。
- SA是通过**密钥管理协议（如IKE）**在通信双方之间进行协商，协商完毕后，双方都在它们的**安全关联数据库（SAD）**中存储该SA参数。
- SA由一个三元组唯一地标识，该三元组为**安全参数索引SPI**、一个用于输出处理的**目的IP地址**和**协议（如AH或ESP）**。
    - SPI是为了唯一标识SA而生成的一个32位整数，包含在AH/ESP头标中。SPI为同一个源与目的之间建立多个SA提供可能

**安全策略数据库（SPD）**：SPD中包含一个策略条目的有序表，通过使用一个或多个选择符来确定每一个条目。选择符可以是**五元组（目的/源地址，协议，目的/源端口号）**，或其中几个，理论上可以根据数据包的任何一个域来确定。条目中包含：

- 策略（是否需要IPSec处理）：丢弃，绕过不使用IPSec，加载IPSec
- SA规范
- IPSec协议（AH/ESP）
- 算法
- 操作模式
- 对外出处理，**应在SPD中查找指向SAD中SA的指针**

**安全关联数据库（SAD）**：包含现行的SA条目，每个SA由三元组索引，一个SAD条目包含下面域：

- 序列号计数器：32位整数，用于生成AH或ESP头中的序列号
- 序列号溢出：是一个标志，标识是否对序列号计数器的溢出进行审核。
- 抗重放窗口：使用一个32位计数器和位图确定一个输入的AH或ESP数据包是否是重放包
- AH/ESP所需的认证算法和密钥
- ESP加密算法和IV
- IPSec操作模式
- SA生存期
- 路径最大传输单元（PMTU）




# AH/ESP头标

## 认证头标AH

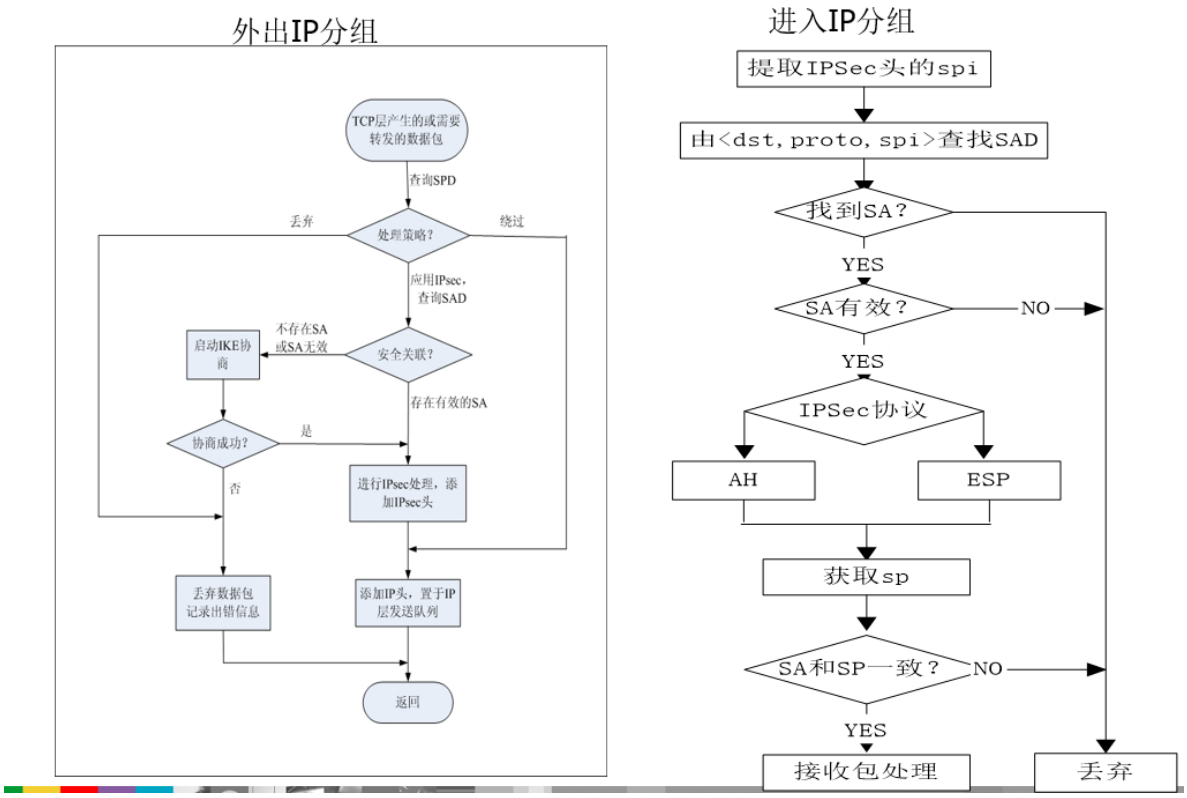
AH协议提供**无连接的完整性（覆盖IP头标除可变域的部分）**、**数据源认证**和**抗重放保护**服务。不提供保密性服务。AH使用**消息认证码（MAC）**对IP进行认证。

## 封装安全载荷头标ESP

ESP提供**数据保密（对称密码）**、**无连接完整性**（可选，不**覆盖IP头标**）、**抗重放攻击**服务，用对称密码体制提供保密性。使用**消息认证码（MAC）**对IP进行认证和完整性保护。

ESP使用时要填充，目的：

- 32位对齐
- 分组密码要求长度是某个长度的整数倍
- 抗流量分析

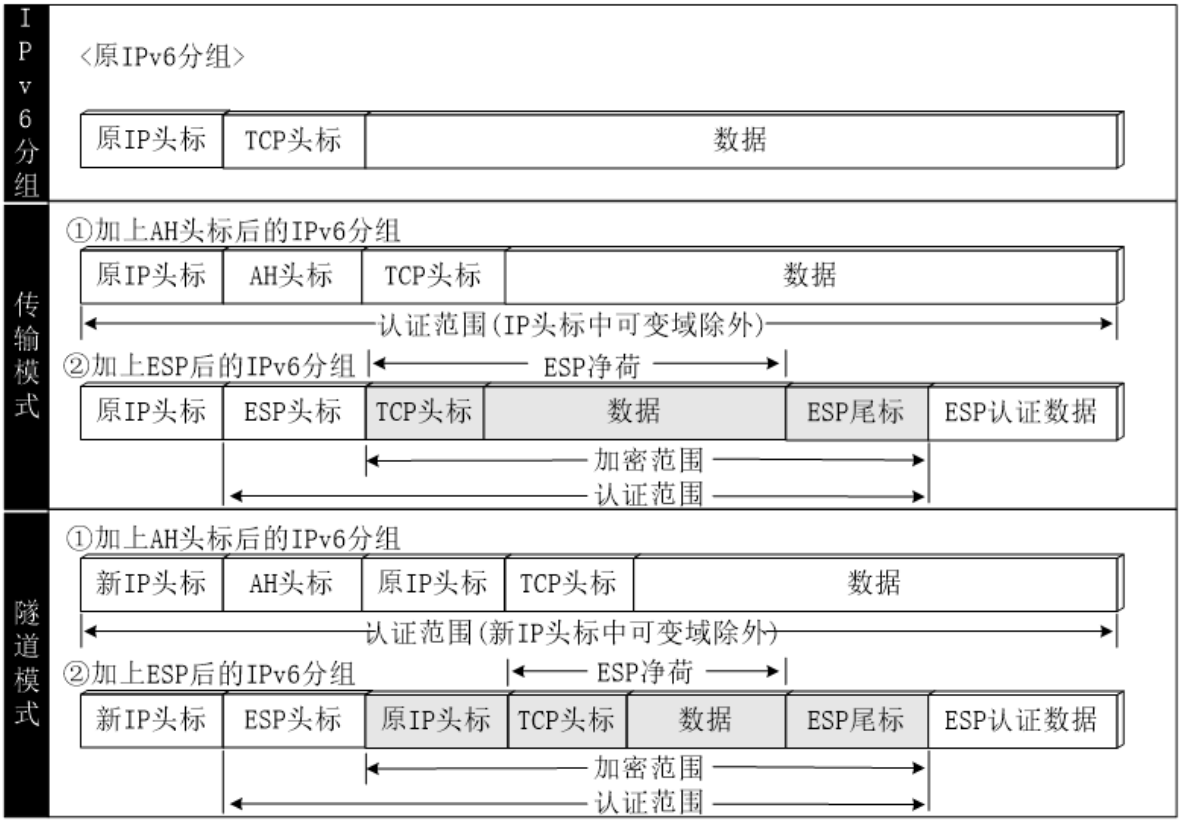



**保护范围差异**：

- AH的认证范围是整个IP分组（除了头标中的可变域）
- ESP的认证范围不包括头标，加密范围包括除了IP头标和ESP头标的部分

## 传输模式和隧道模式

- **传输模式**：AH和ESP头标被插在IP头标及其他选项（或扩展头标）之后，但在传输层协议之前。它保护净荷的完整性和机密性。
- **隧道模式**：AH或ESP头标插在IP头标之前，另外生成一个**新的IP头**放在前面，隧道的起点和终点的网关地址就是新IP头的源/目的IP地址，保护整个IP分组

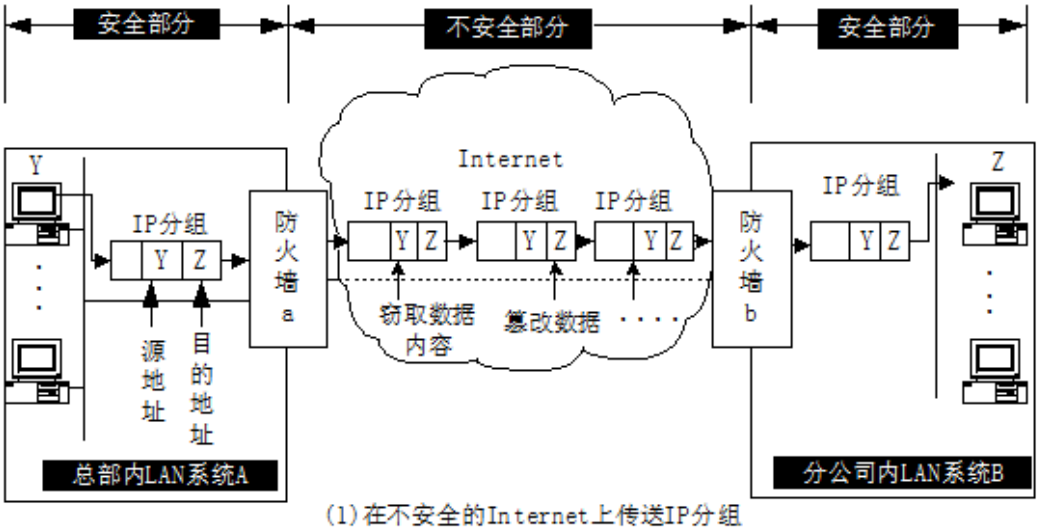



## IPSec与NAT

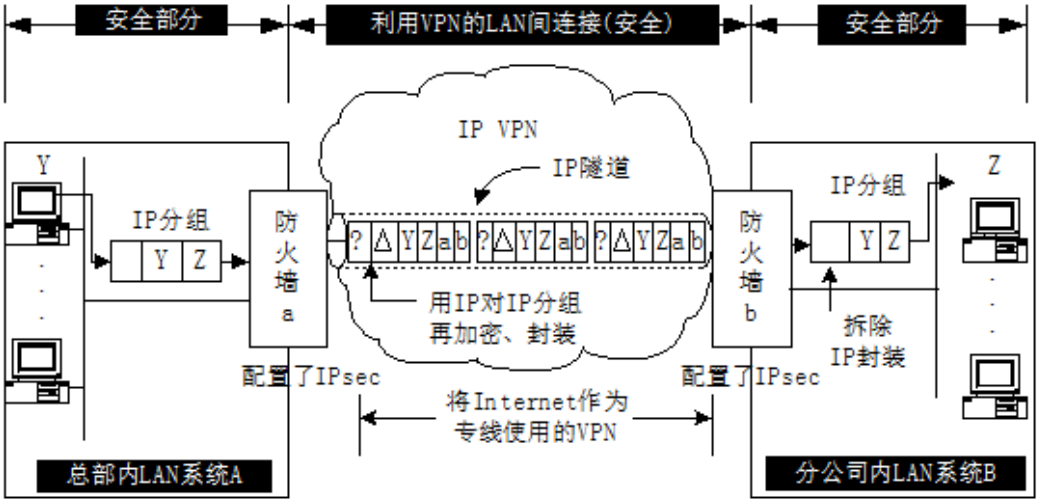
NATPT通常在防火墙或网关上实现，对过往的IP地址、端口号进行转换。具有AH头标或ESP头标的的IP分组不能穿越NAT和NATPT。原因：

- 地址的修改使得接收端的AH认证失败
- 上层端口号信息的ESP加密，使得端口无法被得知，无法进行NAT-PT
- 上层TCP/UDP中校验和计算涉及伪头标，包括IP地址和端口，通过ESP认证，校验和字段不能被修改，上层会校验验证失败
- 针对ESP问题，IETF的解决方案：在ESP头标前插入一个UDP头标

## IPSec VPN




(1)在不安全的Internet上传送IP分组




(2)分组的封装与加密

# 第四章：IPSec-IKE

IKE：因特网密钥交换协议，是一个以**受保护的方式动态协商IPsec SA**的协议。功能：使用某种**长期密钥（共享秘密密钥、只用于签名的密钥、用于加密的密钥）**进行双向认证并建立会话密钥。

## IKEv1

使用了**ISAKMP**框架，希望独立于具体的密钥协商算法，部分使用了Oakley协议和SKEME协议

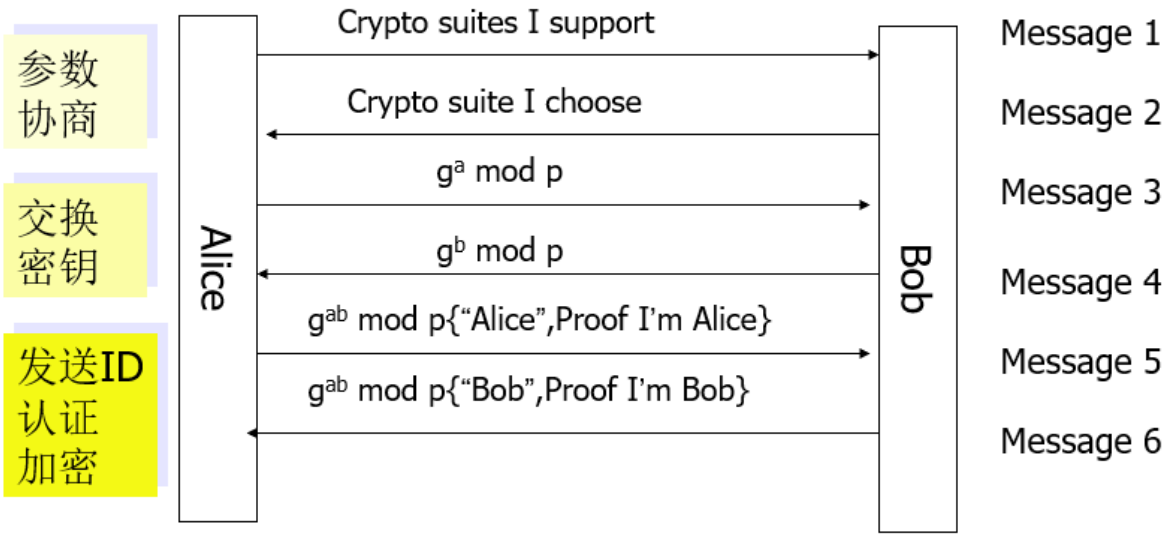
两个阶段：

- **第一阶段**，为建立IKE本身使用的安全信道而相互交换SA（采用ISAKMP）——**ISAKMP SA**（双向）
  - 步骤（交换3/6个报文）：
    - 安全参数协商
    - DH密钥交换
    - 实体认证
  - 交换模式：
    - 主模式
    - 野蛮模式
  - 认证方式：
    - 预先共享密钥
    - 数字签名
    - 公钥加密（加/解密四次）

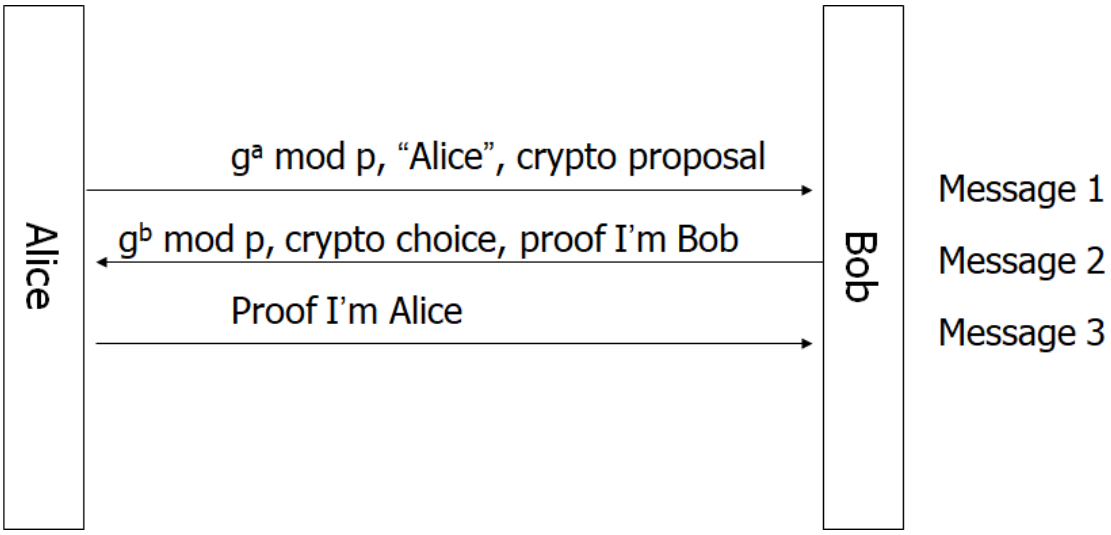
        - 修订的公钥加密
- **第二阶段**，利用第一阶段建立的安全信道交换IPSec通信中使用的SA——**IPSec SA**（单向）
    - 步骤（交换3个报文）
        - 安全参数协商
        - 可选的DH密钥交换
        - 可选的实体认证

## 第一阶段

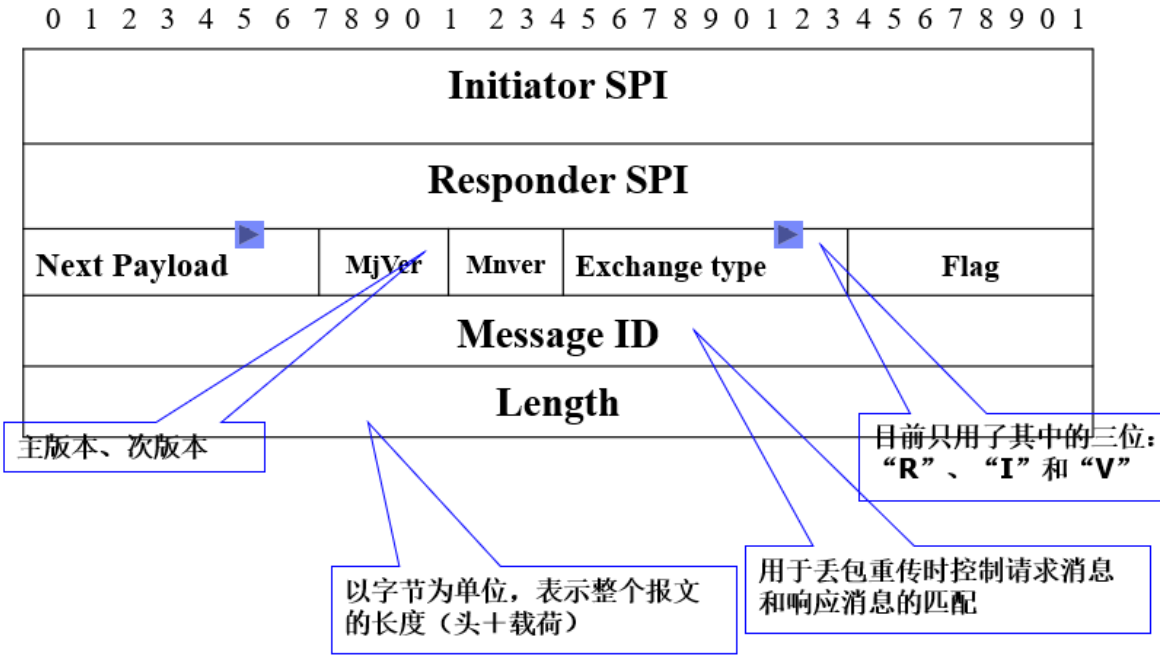
**主模式**：注意认证时要把前两步信息都用到，以**防止重放**




**野蛮模式**：




**IKE头标**




IKE载荷

- **通用头**：每一个IKE载荷的开始，它定义了载荷的边界，所以可以连接不同的载荷。
- **SA载荷**：用于协商SA所的相关属性，实际上是一个嵌套的层次结构。1个SA载荷包含1个或者多个P载荷，1个P载荷包含1个或者多个T载荷
  - **P载荷**：包括SA协商中需要的信息，协商的协议（AH/ESP）
  - **T载荷**：定义特定协议中使用的密码算法
- **密钥交换载荷**：用于传输DH密钥交换中的报文
- **标识载荷**：用于通信双方交换身份信息
- **认证载荷**：包含了用于认证的数据，目前定义的认证方式包括RSA数字签名、消息认证码、DSS数字签名。
- **现实载荷**：保证交换及时性的随机数据，用来阻止重复攻击。

**密钥推导:**

- **SKEYID**：一个衍生自仅有通信双方知道的秘密密钥信息的密钥串。
- **SKEYIDe**：ISAKMP用来保护它的消息保密性的密钥信息
- **SKEYIDa**：ISAKMP用来认证它的消息的密钥信息
- **SKEYIDd**：用来在第二阶段协商中为非ISAKMP SA生成密钥的密钥信息
- 后三个密钥都是通过SKEYID和其他信息（发起响应者的cookie等）利用随机数算法派生得到。

## IKEv2

出现原因：

- NAT穿越
- EAP中的legacy authentication（password）
- 移动场景的远程地址获取
- 进一步**简化旧的协议**
- 为减少计算负担，**避免使用大强度的密钥**和减少频繁协商的次数
- 节省通信资源，应该**减少和简化交互次数**，从而提供IKE的效率

**三个阶段**：

- **初始交换阶段**：建立IKE本身使用的安全信道而相互交换SA——IKE SA（双向）和最初的CHILD_SA，包含两对消息：IKE_SA_INIT、IKE_AUTH
- **CREATE_CHILD_SA阶段**：更新IKE SA，或者更新和创建一个新的CHILD_SA，一对消息
- **INFORMATIONAL交换阶段**：用于删除SA，发送错误通知，检查IKE_SA，一对消息的存活性等。

### 初始交换

- 第一对消息用于**IKE_SA_INIT**交换，用来协商加密算法、(可选地)指示信任的CA名字、交换现时值（Nonce）和实现Diffie-Hellman交换，该过程**建立IKE_SA。**
- 第二对消息用于**IKE_AUTH**交换，用来**认证先前的消息**，交换标识符和证书，并且**建立第一个CHILD_SA**用于AH或者ESP中的IPSec SA。

三种认证方式：

- 基于预共享密钥的MAC
- 数字签名，包括RSA和DSS
- EAP方法

**密钥生成**

- 作为密钥种子的SK_d（为新的CHILD_SA派生产生新的相关密钥）
- 作为完整性密钥的SK_ai和SK_ar（对构成交换的后续消息提供认证）
- 作为加密算法密钥的SK_ei和SK_er（对后续交换包含的消息进行加密）
- 在产生AUTH载荷时使用的SK_pi和SK_pr

### Create_Child_SA交换

用于创建新的Child_SA、或IKE_SA和Child_SA的密钥更新。由单一的请求/响应对构成，可在初始交换之后由IKE_SA的任何一端发起，因而这里的发起者指的是发送CREATE_CHILD_SA请求的端点。

### 改进的DH密钥交换

为了应对DoS攻击、中间人攻击、重放攻击，具体应对策略：

- **DoS**：
  - IKEv2的固定头标中包含各8字节的发起者SPI和响应者SPI。一段时间系统只处理一次相同SPI的包
  - 通过定义携带Cookie的辅助交换（Cookie包含在公告载荷中）来抵御DoS攻击
  - IKEv2中消息成对出现，在每对消息中，发起方负责重传事件，响应者不必对响应消息进行重传，除非受到重传请求。这样可以避免同时发生重传，造成资源的浪费，同时也可以防止攻击者截获消息后，伪装成发起者不断发起重传请求，耗费协商双方的资源
  - IKEv2只通过两种情况判断对方是否失效：一种是重复尝试联系对方，直到应答时间过期；另外一种是受到对方的不同的IKE_SA加密保护的INITIAL_CONTACT通知消息
- **重放攻击**：
  - 现时载荷被加到第3和第4个消息（也就是IKE_AUTH交换的两个消息）中，来保持信息的更新。
  - 消息ID也主要设计用于防止重放攻击。
- **中间人攻击**：三种认证方式

# 第五章：SSL/TLS基本协议

**SSL协议族**：一种在**TCP之上**为两个**端实体**之间提供安全通道的协议，包括SSLv2，SSLv3，TLS协议。在不提供IPSec安全保护的网络上，要实现安全的信息传输，只有依靠端到端的上层安全协议提供保护。

**SSL解决的问题**：

- **客户对服务器的认证**：SSL服务器允许客户的浏览器使用标准的公钥加密技术和一些**可靠的认证中心（CA）的证书**，来确认服务器的合法性。
- **服务器对客户的认证**：公钥+证书/用户名+口令
- **建立服务器与客户之间安全的数据通道**：SSL要求客户与服务器之间的所有发送的数据都被发送端**加密**、接收端解密，同时还检查**数据的完整性**

SSL提供的服务：

- 用户和服务器的**合法性认证**：X.509数字证书
- 传输数据**机密性**：DES, 3DES, RC2, RC4, IDEA...
- 传输数据**完整性**：MAC-MD5, MAC-SHA1...

## SSL的基本层次结构

SSL协议分为两层：

- 底层：记录协议
- 上层：握手协议、密码变更协议、警告协议、**用户数据**

**握手协议**：

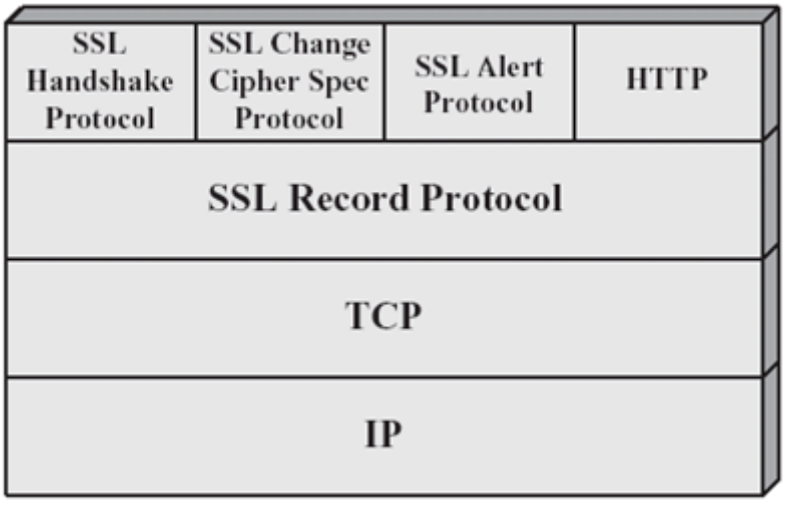
- 客户对服务器的认证，与服务器对客户的认证（**可选**）
- 协商加密算法和密钥
- 协商的密钥是安全的（中间人不知道），协商本身是可靠的

**记录协议**：

- 建立在TCP提供的可靠传输服务上
- 提供保密性（对称加密），和完整性（HMAC），身份认证
- 封装上层协议

**告警协议**：向对端指示其安全错误

**改变密码规格协议：**告知改变密码参数

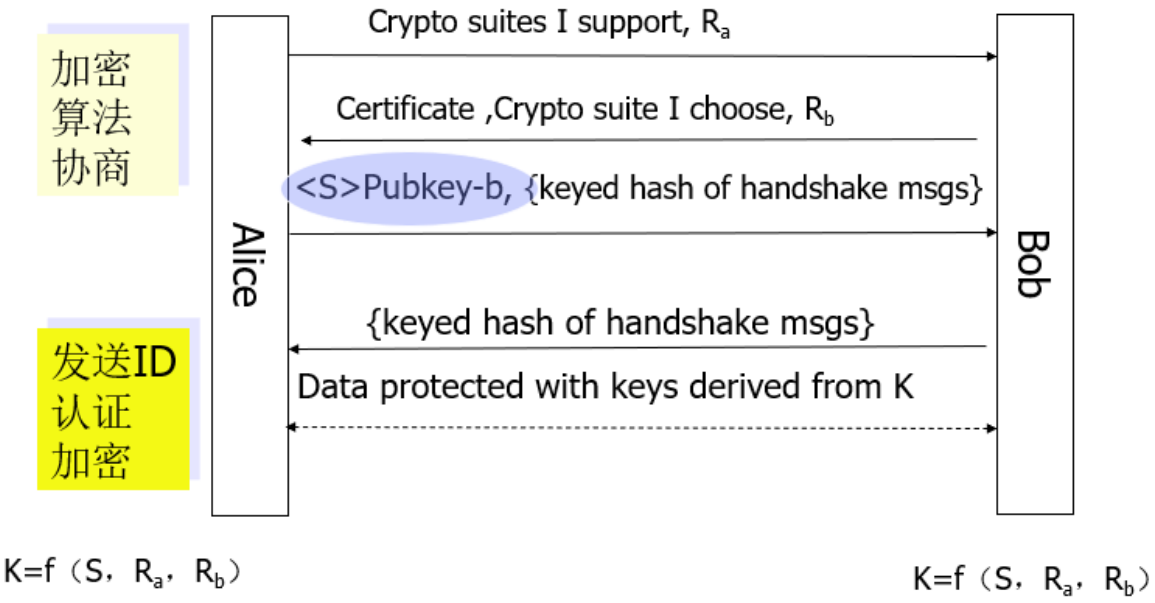



**SSL记录协议保护方式**：分段 -> 压缩 -> 添加MAC值（对压缩以后的数据完整性保护）-> 加密 -> 加记录协议头

**SSL 握手协议(RSA方式)**

下图中的<S>Pubkey-b是用Bob公钥加密的**pre-master key**。最终**主密钥**K = f(S, Ra, Rb)。对于每个连接，每个方向上各三个密钥，分别为**加密密钥**、**完整性保护密钥**、**IV**：gi（K，Ra，Rb），利用主密钥派生。

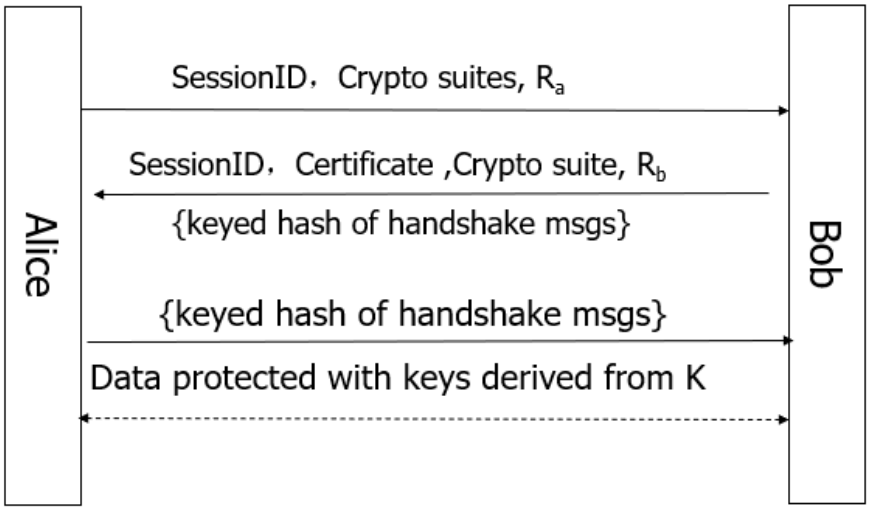
**master_secret**总是**48**字节长，而**pre_master_secret**长度不定，取决于密钥交换算法




**会话重用**：SSL/TLS认为会话通常是具有较长的生命期，在此之上需要在会话基础上容易派生出多个连接。这是因为协议被设计为能够与HTTP协议协同工作，而HTTP协议能够在相同客户和服务器之间打开大量的TCP连接。

- 会话：客户与服务器的关联，由握手协议创建。会话定义一组安全参数，可以在多个连接之间共享。避免每次连接都进行昂贵的参数协商
- 连接：提供适当类型服务的传输，连接是暂时的，每个连接都与一个会话相关联

## 会话重用（进行重用的情况）




这样不用每次建立连接都算一个新的密钥。

**密钥计算**

- 秘密值S：预备主密钥（Pre-mastersecret），由客户端生成
- 主密钥（Master secret）K：K = f（S，Ra，Rb）
- 对于每个连接，每个方向上各三个密钥，分别为**加密密钥**、**完整性保护密钥**、**IV**：gi（K，Ra，Rb）

## SSL协议的安全性分析

SSL协议采用的加密和认证算法

- 加密算法与会话密钥：算法有RC4，RC2，IDEA和DES；密钥由消息散列函数MD5、SHA-1产生
- 认证算法：采用X.509证书

安全**优势**：

- 监听和中间人攻击（√）
- 流量数据分析攻击（x）**TLS可以抵抗此类攻击**
- 截拼攻击（√）
- 重发攻击（√）
- 密码回滚攻击CipherSuiteRollback attack （√）:SSL3.0中新加的功能，可以防止对密码学算法协商过程的更改

**问题**：

- 密钥管理问题：许多实现，服务器的证书**不是基于可信的CA颁发**
- 加密强度问题：低比特位数的加密算法(**出口限制**)
- 数字签名问题：没有数字签名，不能抗抵赖

# 第六章：防火墙和NAT

**防火墙**：是位于两个(或多个)网络间，实施网间访问控制的一组组件的集合（软件+硬件+控制策略），它满足以下条件：

- 内部和外部之间的所有网络数据流必须经过防火墙；
- 只有符合安全政策的数据流才能通过防火墙；
- 防火墙自身能抗攻击；

## 包过滤防火墙

通常在路由器的**网络层**实现，实际上是一种网络层的访问控制机制

工作原理：

- 过滤的规则以五元组，即IP和传输层的头中的域(字段)为基础，包括源和目标IP地址、IP协议域、源和目标端口号。区分出入
- 过滤器往往建立**一组规则**，IP包**自上而下**进行匹配，根据IP包是否匹配规则中指定的条件来作出决定。
    - 如果匹配到一条规则，则根据此规则决定转发或者丢弃
    - 如果所有规则都不匹配，则根据**缺省策略**（放行or丢弃）

优点：

- 实现简单
- 对用户透明
- 效率高

缺点：

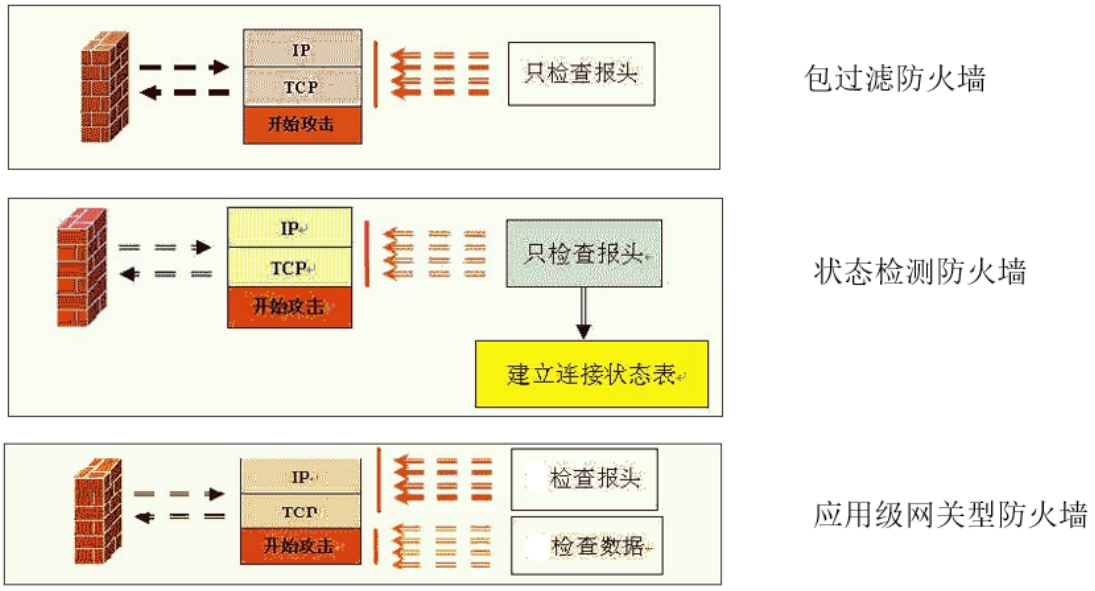
- 正确制定完全符合安全特性的规则并不容易
- 不可能引入认证机制
- 并没有考虑连接状态信息
- 不能对应用层数据进行处理
- 纯粹的包过滤防火墙比较适合于单连接的服务(比如smtp, pop3)，不适合于多连接的服务(比如ftp)

## 状态检测防火墙

通过建立一个出网的TCP连接目录而加强TCP数据流的检测规则(**连接记录**)。即状态检测防火墙 = 包过滤防火墙 + 连接记录。报文过滤机制只允许那些和目录中某个连接匹配的数据流通过防火墙

## 应用级网关型防火墙

在**应用层**上建立**协议过滤**和**转发**功能。即包过滤 + 应用层协议信息。因此可以实现**基于内容的安全**




## 代理服务器防火墙

**代理服务**(Proxy Service)也称**电路级网关**或**TCP通道**。其特点是**将所有跨越防火墙的网络通信分为两段**。防火墙内外计算机系统间应用层的"链接"，由两个终止代理服务器上的 "链接"来实现，外部计算机的网络链路只能到达代理服务器，从而起到了隔离防火墙内外计算机系统的作用。


优点：

- 允许用户"直接"访问Internet
- 易于记录日志

缺点：

- 新的服务不能及时地被代理
- 每个被代理的服务都要求专门的代理软件
- 客户软件需要修改，重新编译或者配置
- 有些服务要求建立直接连接（如聊天服务），无法使用代理
- 不能避免协议本身缺陷

## 复合型防火墙

- 屏蔽路由型结构
- 屏蔽主机结构

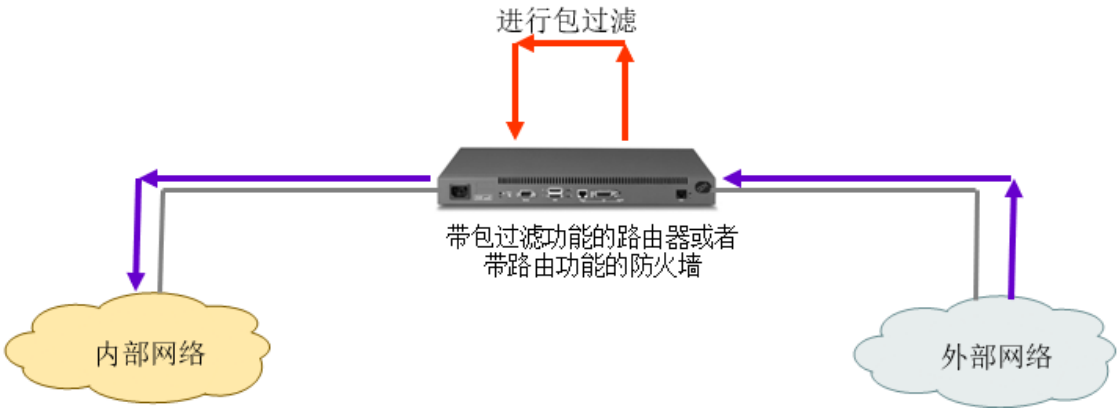
    - 单宿主主机
    - 双宿主主机
- 屏蔽子网结构
- 双热设备

### 屏蔽路由型结构

屏蔽路由器：

- 简单的包过滤功能
- 投资小，配置简单
- 但是在ACL众多时影响性能

适合内部主机安全性好，对性能、可靠性要求比较高的环境




### 屏蔽主机结构（单宿主主机）

包过滤路由器和**堡垒主机**一起构成安全系统，堡垒主机暴露在外网攻击下，只允许堡垒主机与外部直接通信，内部其他主机与外部通信必须经过堡垒主机。

适用于只对外提供较少的服务，外部的来的连接比较少，以及内部主机安全性配置较好的环境

**缺点**：

- 堡垒主机与其他主机在同一个子网
- 一旦包过滤路由器被攻破或被越过，整个内网和 堡垒主机之间就再也没有任何阻挡。

## NAT

### 屏蔽主机结构（双宿主主机）

双宿主主机：

- 有两块网卡
- 可以是包过滤软件/硬件、应用层代理
- 增加了单一故障点，影响网络吞吐量
- 只有同时攻破堡垒主机和路由器内部才是不安全的

使用环境：去往Internet流量小，可靠性要求不高，不对外提供服务

难点：如何保证双宿主主机安全

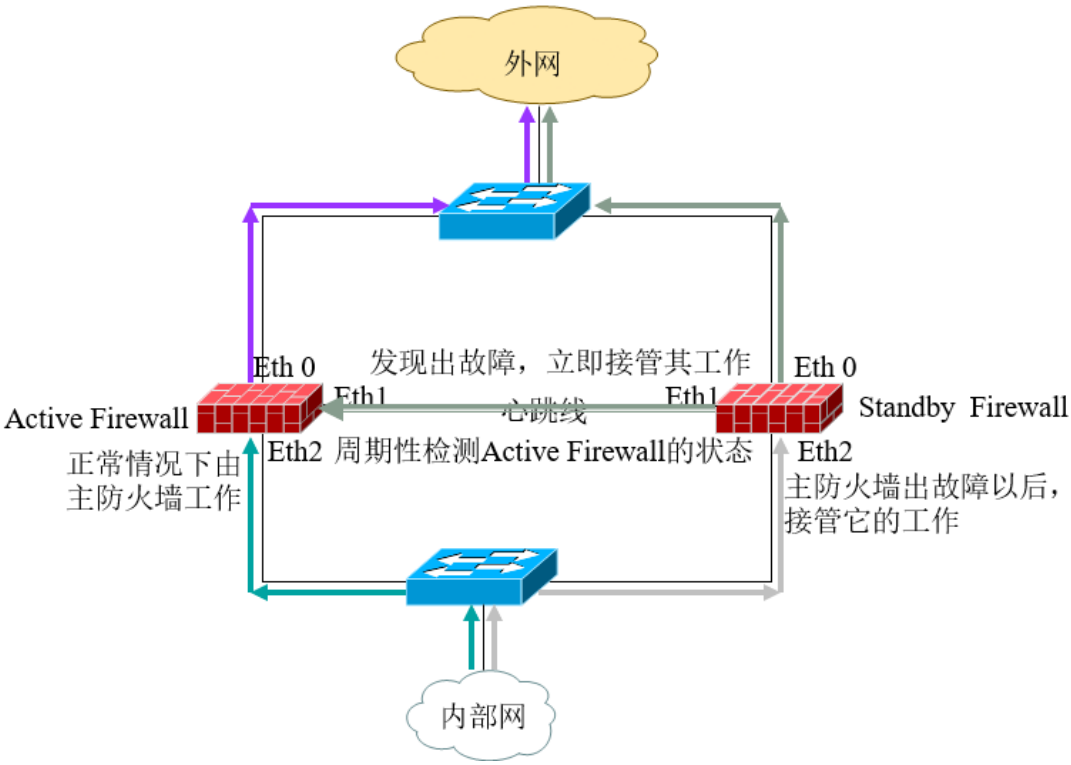
### 屏蔽子网结构

**DMZ**（Demilitarized Zone），非军事区或者停火区：

- 包含**两个包过滤路由器**
  - 外部路由器：只允许对DMZ的访问，拒绝所有以内部网络地址为目的地址的包进入内部网络。
  - 内部路由器：保护内部网络，防止来自Internet或DMZ的非法访问，拒绝外部发起的一切连接，**只允许内部对外的访问**，在特定需要前提下，可以允许从堡垒主机来的访问，从内部往外的访问也可以限制为必须通过堡垒主机。
- 在内部网络和外部网络之间创建了一个新的子网，可能只包含**堡垒主机**，也可能还包含一个或者多个**信息服务器**（所有对外服务在DMZ完成）
- 内外网通信必须经过堡垒主机

### 双热设备

**目的**：保证稳定性，一个防火墙完蛋了另一个马上顶上



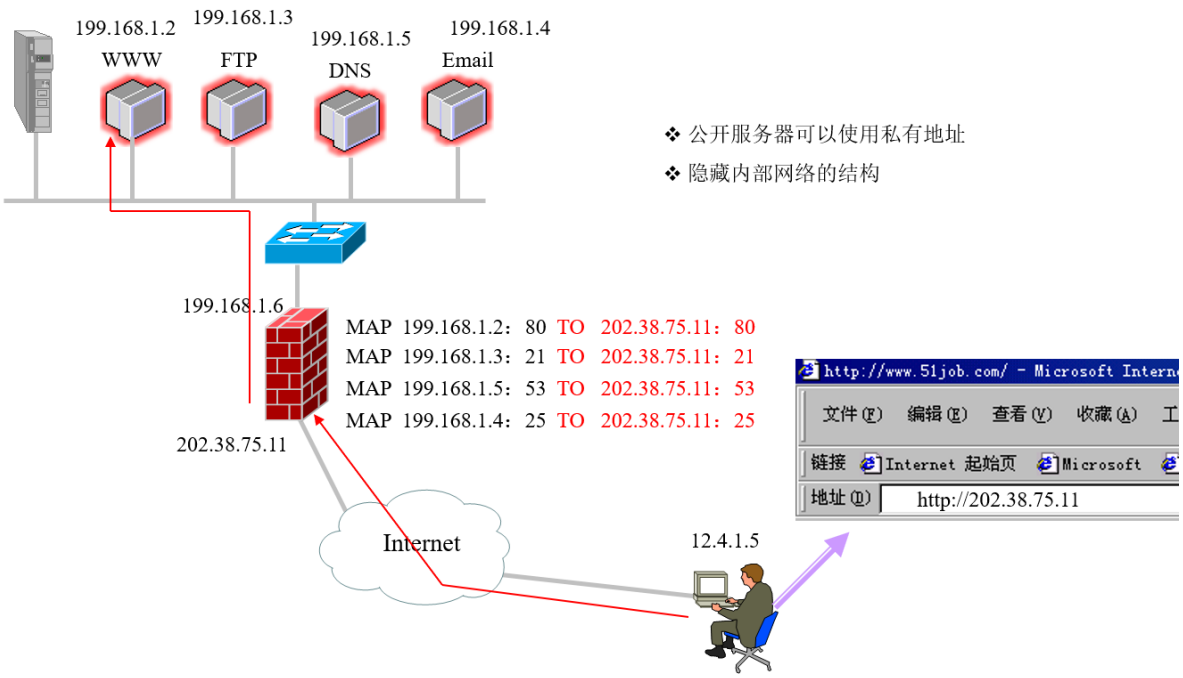

## NAT

NAT（网络地址转换）可以划分为以下两种类型（从发起者的报文）：

- 源网络地址转换(**SNAT**，即IP伪装)：复用内部的全局地址，解缓IP地址不足的压力。同时可以向外部**隐藏内部IP**
  - 对于传出数据包，源IP地址(专用地址)被映射到ISP分配的地址(公用地址)，并且TCP/UDP端口号也会被映射到不同的TCP/UDP端口号，建立**映射表信息**。
  - 对于传入数据包，根据**映射表**信息，目标IP地址(公用地址)被映射到源Internet地址(**专用地址**)，并且TCP/UDP端口号被重新映射回源TCP/UDP端口号。
- 目的网络地址转换(**DNAT**)：在实现SNAT的环境下进行有效的服务访问，以及流量均衡

实现方式：

- NAT
  - 静态NAT（static NAT）：内部网络地址与NAT地址和端口号一一对应
  - 动态NAT（Dynamic NAT）：多对多
- NAT-PT：过载：一对多


# 第七章：虚拟专用网VPN

**是什么**：

- 可以实现不同网络的组件和资源之间的相互连接。虚拟专用网络能够利用Internet或其它公共互联网络的基础设施为用户创建**隧道**，并提供与专用网络一样的**安全和功能保障**。
- 并没有传统专网所需的端到端的物理链路，而是利用某种公众网的资源动态组成的。
- 是通过**隧道技术**在公共数据网络上**虚拟**出一条点到点的专线技术。

用来保证安全的**技术**：

- **隧道技术**
- 加解密技术

- 密钥管理技术
- 认证技术
- 访问控制

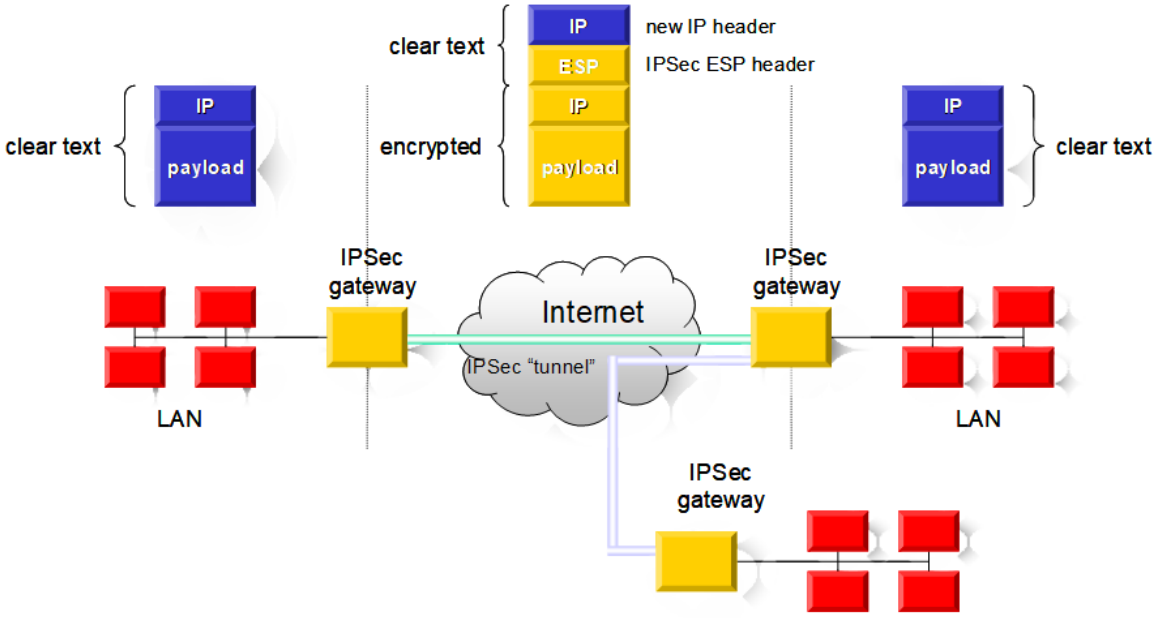
VPN**分类**：

- 按照隧道协议分类：
  - 基于第二层隧道技术的VPN：L2F，PPTP，L2TP
  - IPSec VPN
  - SSL VPN
  - MPLS VPN
  - GRE VPN
- 按照应用类型分类：
  - 远程访问型
  - LAN间互连

## IPSec VPN

主要适用于**LAN间VPN**（隧道模式）。实现方式：

- VPN专用设备
- IPSec嵌入防火墙/路由器设备
- 动态IP地址的IPSec VPN

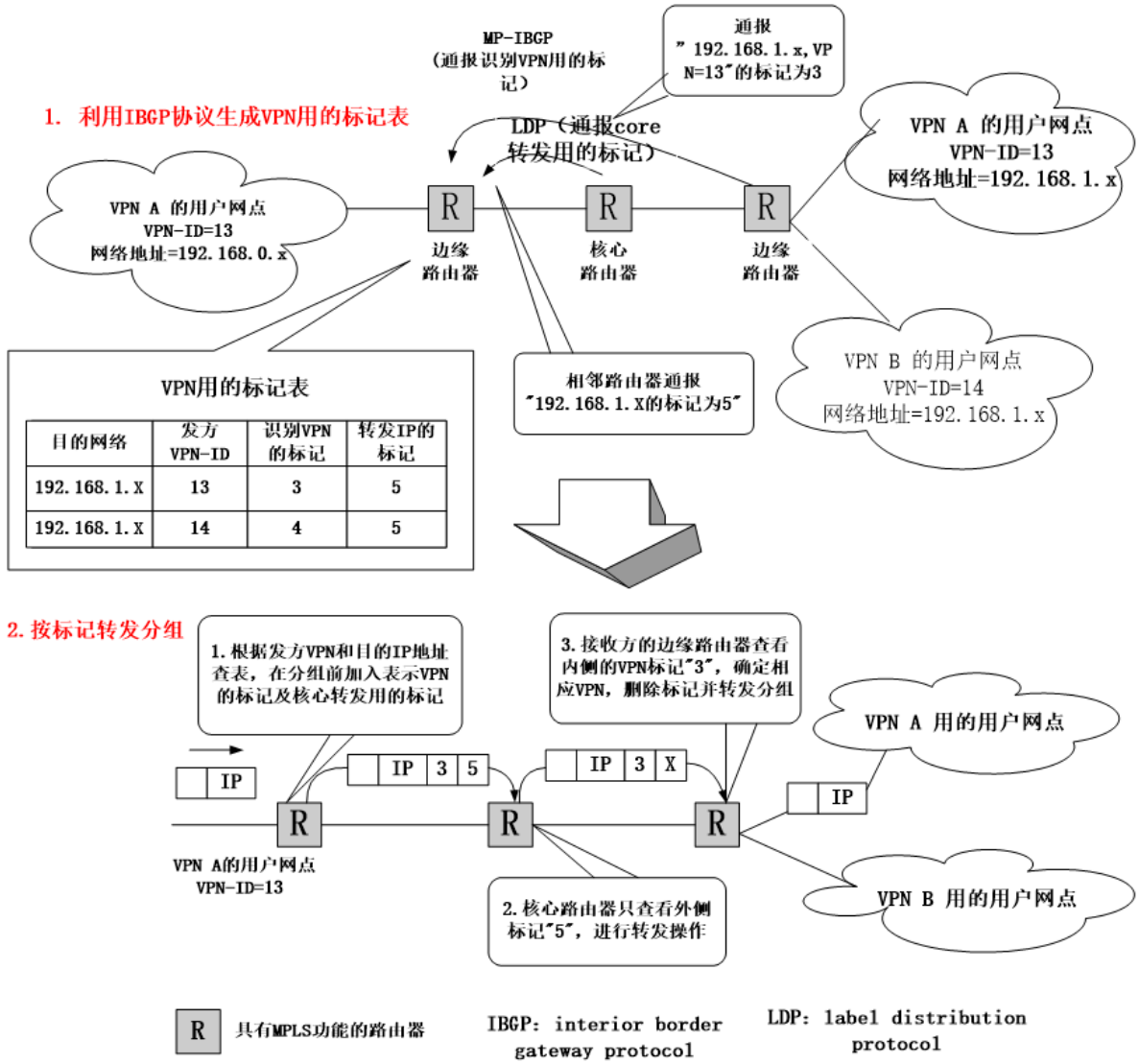



## MPLS VPN

MPLS（MultiProtocol Label Switching）：**多协议标记（标签）交换。**与传统路由的区别在于转发时不是根据IP地址，而是**根据标记转发**

- 利用MPLS构建VPN时，只需对不同的企业集团分配不同的**标记通道**，企业网使用的内部地址也仍可以原封不动使用（即企业网网关可以不用NAT）。
- 利用**标记堆叠**来实现VPN，在一个IP分组上**叠加两个MPLS标记头标**进行转发，外侧标记用于**转发**，内侧标记用于VPN**接入**（FEC标识+VPN标识）

**工作步骤**


1. 利用IBGP协议生成VPN用的标记表
MP-IBGP
（通报识别VPN用的标记）
通报
”192.168.1.x,VPN=13″的标记为3
LDP（通报core转发用的标记）
VPN A 的用户网点
VPN-ID=13
网络地址=192.168.1.x
VPN A 的用户网点
VPN-ID=13
网络地址=192.168.0.x
R
边缘路由器
R
核心路由器
R
边缘路由器
VPN B 的用户网点
VPN-ID=14
网络地址=192.168.1.x
相邻路由器通报
″192.168.1.X的标记为5″
VPN用的标记表
目的网络 | 发方VPN-ID | 识别VPN的标记 | 转发IP的标记
192.168.1.X | 13 | 3 | 5
192.168.1.X | 14 | 4 | 5
2. 按标记转发分组
1. 根据发方VPN和目的IP地址查表，在分组前加入表示VPN的标记及核心转发用的标记
3. 接收方的边缘路由器查看内侧的VPN标记″3″，确定相应VPN，删除标记并转发分组
IP
IP 3 5
IP 3 X
IP
VPN A 用的用户网点
VPN B 用的用户网点
VPN A的用户网点
VPN-ID=13
2. 核心路由器只查看外侧标记″5″，进行转发操作
R 具有MPLS功能的路由器
IBGP: interior border gateway protocol
LDP: label distribution protocol

## 工作原理

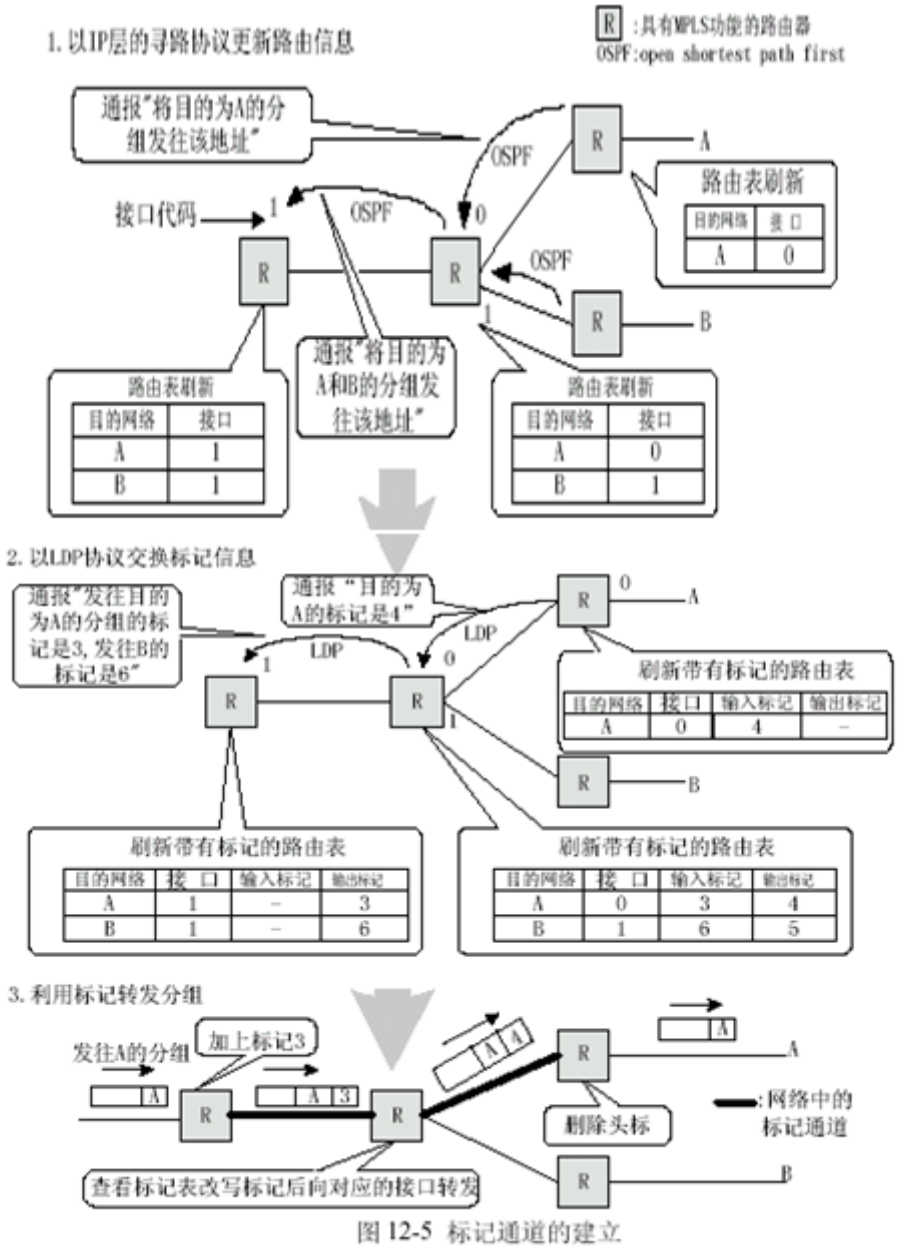


图 12-5 标记通道的建立

**转发等价类FEC**：所有在MPLS网络中需要做相同转发处理、相同路由处理的分组。

**与IPSec VPN的关系**：

- MPLS VPN的安全性与帧中继、ATM类似，即租用了一条虚连接（局部）。
- MPLS VPN不涉及认证、加密功能。而IPSec VPN提供认证、加密功能，能保证数据的机密性、完整性
- 对安全需求强的业务可以将IPSec和MPLS VPN结合使用

# 第八章 应用层安全协议

## 电子邮件安全协议（PGP、S/MIME）

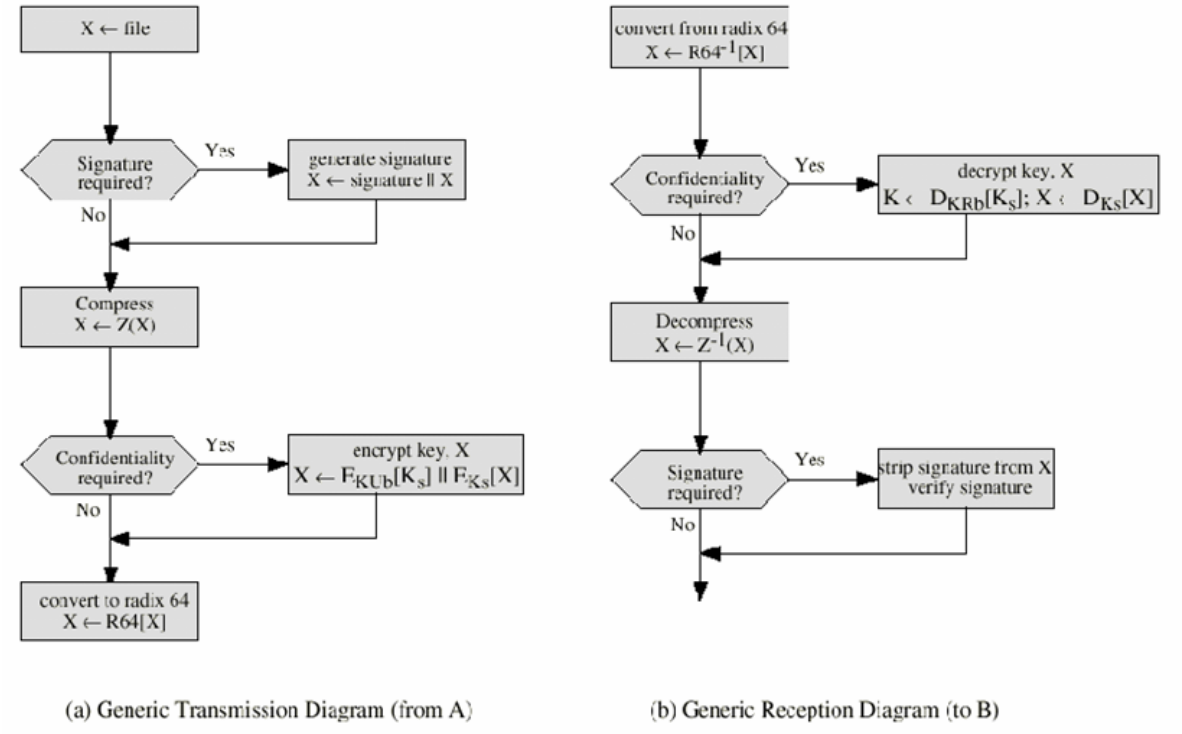
电子邮件安全需求：

- **机密性**：报文的加密：关键是密钥的分发（**数字信封**）
- **认证**：私钥签名或者基于共享密钥的MAC
- **完整性**：可以和认证一起进行
- **抗否认性**：私钥签名

### PGP（Pretty Good Privacy）

提供的安全业务：

- **加密**：**发信人产生一次性会话密钥**，以IDEA、3-DES或CAST-128算法加密报文，采用RSA算法用**收信人的公钥加密会话密钥**，并和消息一起送出。
- **认证**：用SHA-1对报文杂凑，并以**发信人的私钥签字**，签名算法采用RSA或DSS 。
- **压缩**：ZIP，用于消息的传送或存储。**在压缩前签名，压缩后加密。**原因：之所以在压缩前签名是因为不同时刻压缩结果可能不同，若在压缩后签名可能导致认证失效。之所以在签名后加密是因为接收端保留明文和签名，而不会保存会话密钥，这么操作有利于接收方随时验证签名。
- **兼容性**：由于历史原因，Email只被允许传送ASCII字符。采用**Radix-64**可将加密的报文转换成ASCII字符，**将原报文扩展了33%.**
- **数据分段**：PGP具有分段和组装功能，适应最大消息长度限制




(a) Generic Transmission Diagram (from A)　　(b) Generic Reception Diagram (to B)

**加密密钥和密钥环**：PGP使用四种类型的密钥：一次性会话对称密钥，公钥，私钥，基于对称密钥的口令，需求：

- 需要生成不可预测的会话密钥（随机算法）
- 需要某种手段来**标识具体的密钥**（一个用户可拥有多个公钥/私钥对，以便随时更换且让对方知道来自哪个密钥对）
  - 将公钥与消息一起传送
  - 将一个**标识符（KeyID = KUa mod 2^64）**与一个公钥关联，对一个用户来说做到一一对应
- 每个PGP实体需要维护一个**保存其公钥/私钥对**的文件和一个**保存通信对方公钥**的文件
  - 存储该节点拥有的公钥/私钥对私钥环（**口令保护密钥**）
  - 存储本节点知道的其他用户的公钥环

**公钥管理**：PGP虽然采用公钥密码体系，但不是证书。如何保证公钥是合法的？

- 直接索取，其他方式确认
- 从可信任证书机构获得B的公钥
- 采用信任关系保护（从可信第三方）公钥

## S/MIME

**S/MIME** 旨在成为商业和机构使用的工业标准，**PGP** 为个人e-mail 提供安全 。S/MIME强化了证书的规范，使用X.509证书方案。

## SSH

体系框架：

- SSH**传输层(**Transport Layer)协议：提供服务器主机认证，提供数据加密，提供数据完整性支持
- SSH**认证**(Authentication)协议：为服务器提供用户的身份认证
- SSH**连接**（Connection）协议：将加密的信息隧道复用成若干个逻辑通道，提供给高层的应用协议使用。

## HTTPS（http over SSL）

- 由http和SSL结合来实现浏览器和服务器之间的安全通信
- https的功能被嵌入到所有当前的主流浏览器当中，但依赖于服务器端是否支持https通信
- https的周知端口为443，http为80
- 当使用HTTPS时以下内容被加密：请求文件的URL、文件内容、浏览器表单内容、cookie、http头标内容
- **连接建立**：TLS握手，然后是标准的http过程。一个会话有多个连接
- **连接关闭**：先关http再关SSL，TCP

## 安全电子交易协议-SET

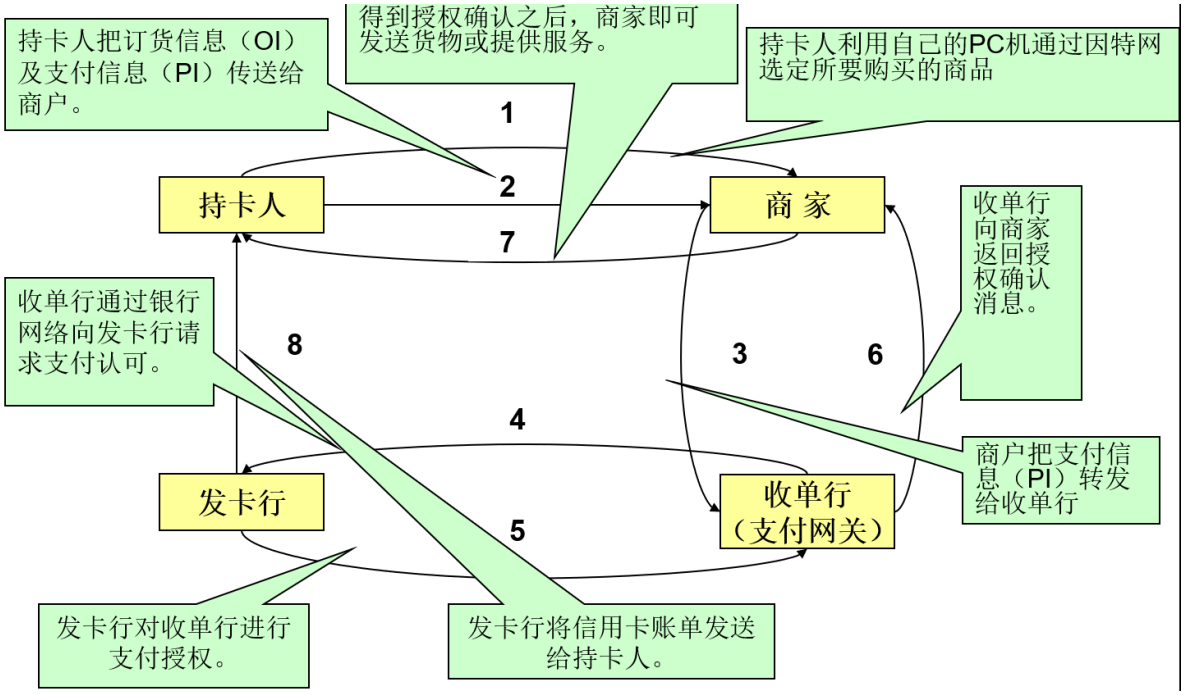
SET提供了**消费者、商家和银行**之间的认证，确保了网上交易数据的**保密性**，数据的**完整性**以及交易的**不可抵赖性。**特别是能**保证不将消费者银行卡号暴露给商家，不将消费者的购物信息暴露给银行**等优点，因此它成为目前公认的信用卡/借记卡网上交易安全标准。采用公钥密码体制，遵循X.509数字证书标准。

参加SET协议支付系统的实体主要有：

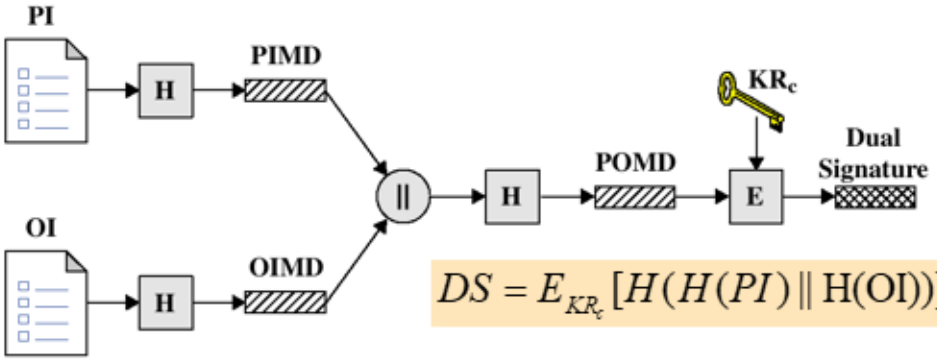
- 持卡人
- 商家
- 支付网关

SET协议信息结构包括：

- 持卡人/商家注册流程
- 购买请求过程
- 支付授权流程
- 支付执行过程
- 持卡人查询过程

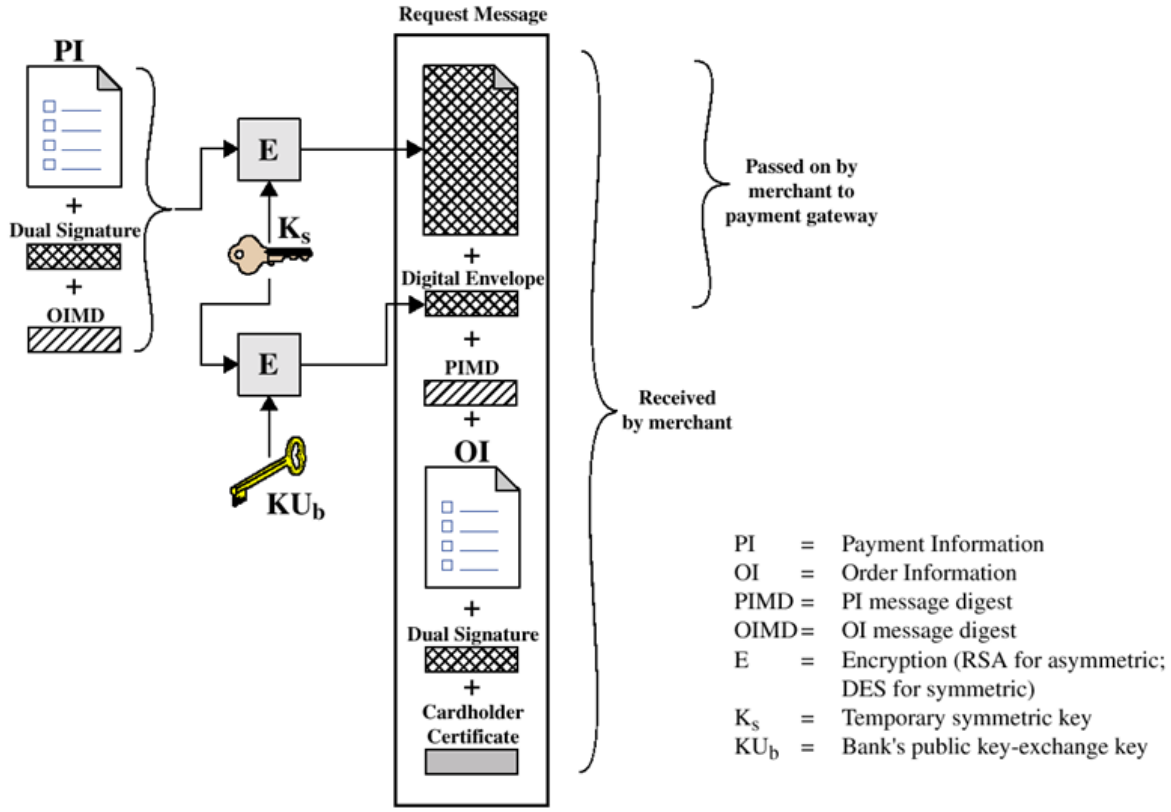



**双重数字签名**：发送者寄出**两个相关信息**给接收者，对这两组相关信息，接收者**只能解读其中一组**，另一组只能转送给第三方接收者，不能打开看其内容。这时发送者就需分别加密两组密文，做两组数字签名，故称**双重数字签名。**

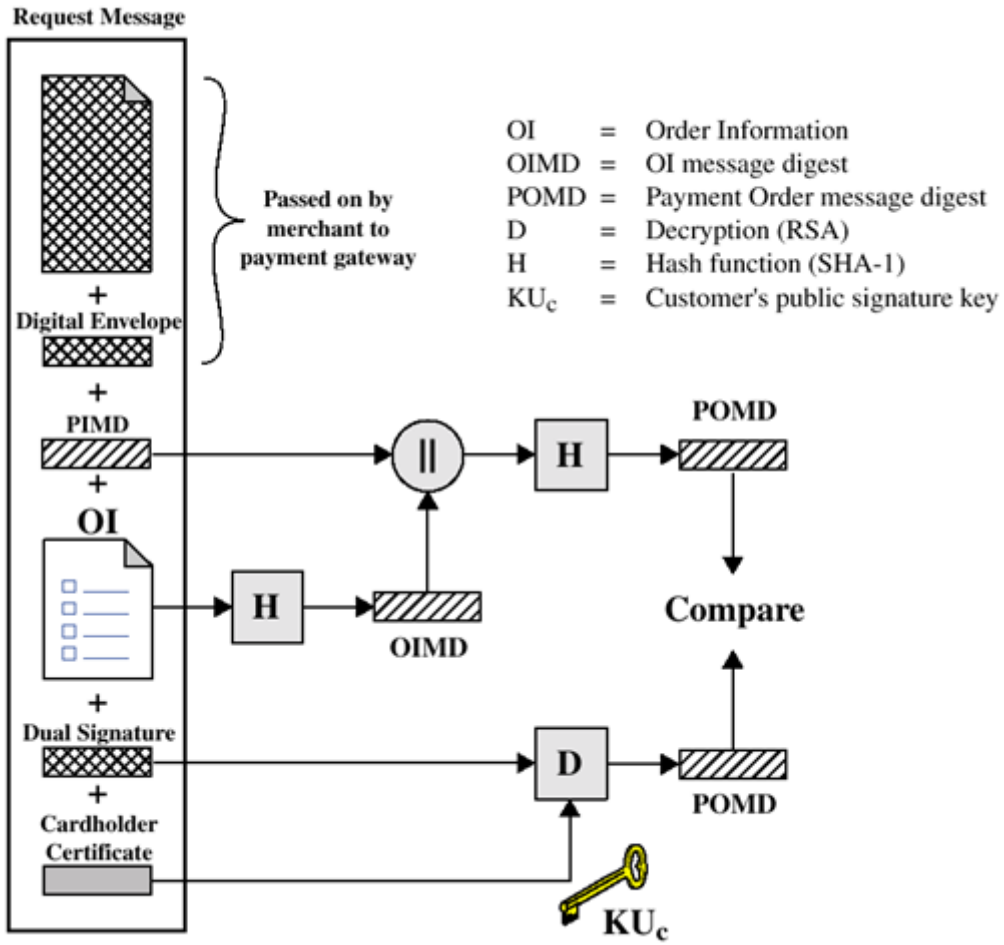



1. 商家收到PIMD、 OI、 DS，计算H(PIMD||H(OI))和$D_{KUc}$(DS)
2. 银行收到OIMD、 PI 、DS，计算H(H(PI)||OIMD)和$D_{KUc}$(DS)
3. 顾客将PI OI链在一起起到签名作用。

**持卡人发送购买请求**：




**商家验证过程**:




# 第九章：WLAN安全

WLAN标准：802.11系列

建立方式：

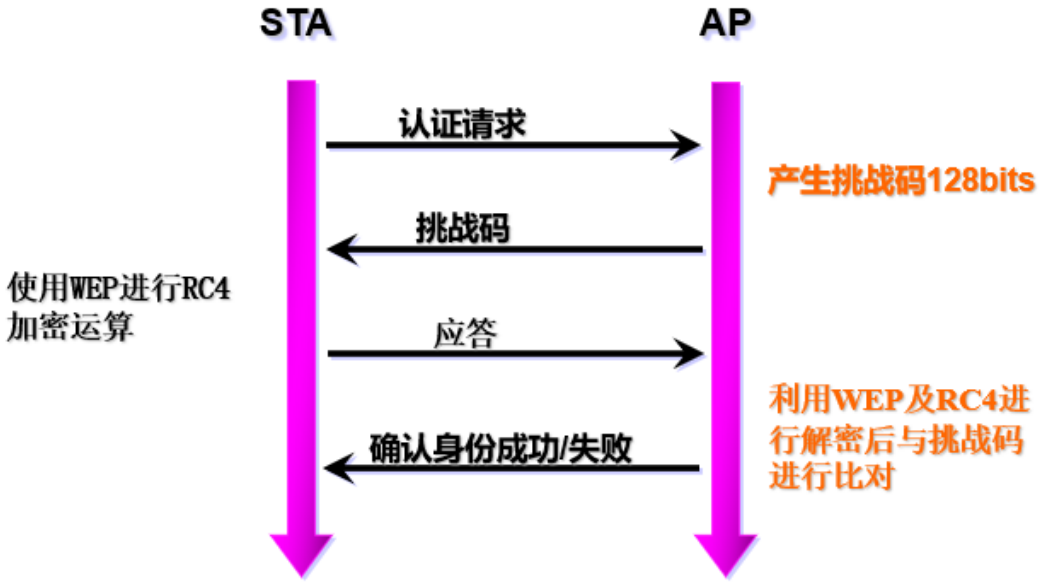
- Ad-hoc：一群使用无线网卡的Station，直接相互连接，资源共享，无需通过接入点（AP）
- Infrastructure Mode：所有Station通过接入点连接成网络实现资源共享

## WLAN的安全需求

无线网络安全缺陷：物理链路开放，窃听、通信阻断、注入攻击、中间人攻击、客户端/AP伪造

802.11的**安全机制**

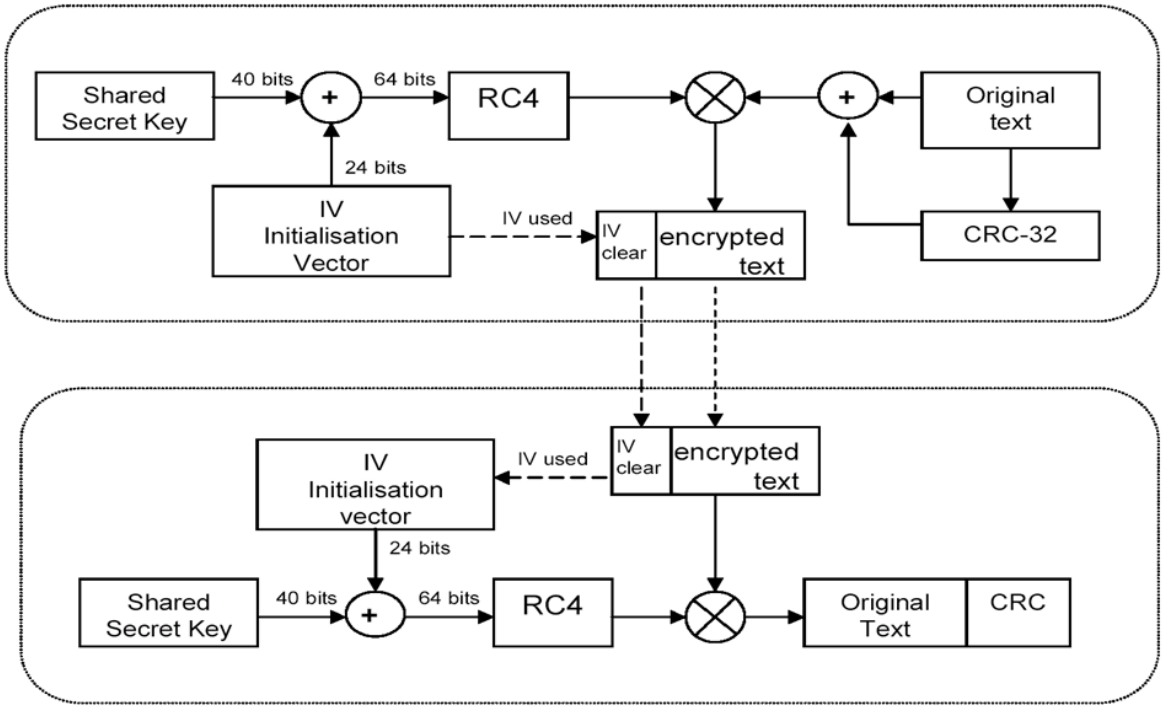
- 身份认证
  - 开放式系统：公开SSID，是802.11的缺省设置，不认证
  - 封闭式系统：不公开SSID
  - 共享密钥认证：使用共享密钥和挑战-相应机制完成AP对接入点的认证




- 数据机密性：WEP（使用一个40/104bit 密钥，RC4流加密算法，一个24bit 的初始向量IV ）
- 数据完整性：CRC32

## WEP协议

提供**访问控制**和**数据保密性**




**协议弱点**

- IV：24bit太短，明文传输，设计不合理（从0开始，数据包加一则IV+1）
- CRC-32进行差错判断，被放入数据进行加密，无法预先进行数据完整性判断（先完整性再加密），且CRC有线性性。
- 没有提供源和目的地址的完整性校验信息，并且缺少**重放攻击**的对策

**安全增强**

- **使用104-bit WEP 密钥**. 这个已经被广泛应用，40bit的密钥安全性很差 ->WPA（Wi-Fi Protected Access ）
- **标准的密钥交换和分发。**802.11的共享密钥机制很不安全，可以用一系列协议来完成，例如RADIUS, Kerberos, SSL/TLS和IPSec.
- 使用带有密钥的**MAC算法**进行数据完整性校验（CRC太菜了）
- **双向认证**. **抵抗中间人**窃取数据或者**会话劫持**
- 采用其他安全协议（WPA, WPA2, 802.1X, WAP1）

**802.11i操作的5个阶段**

- **发现**：AP使用信标和探测响应信息发布802.11i安全策略。站点（STA）则通过这些来希望确认希望进行通信的AP身份。STA访问接入点，当信标和探测响应提供选择时，选择加密套件和认证机制。
- **认证**：STA和认证服务器各自互相证明各自身份。接入点组织STA和认证服务器直到认证成功前尚未被认证的数据。AP不参与认证，而是转发他们的认证数据
- **密钥生成和分发**：接入点和STA几种操作后产生加密密钥，并配送到接入点和STA。数据帧只在AP和STA之间交换。
- **保密数据传输**：数据帧在STA和终端站点之间通过AP交换。安全数据传输只发生在AP和STA之间（STA和终端站点之间的安全性不保证）
- **连接终止**：AP和STA交换数据帧，安全连接解除