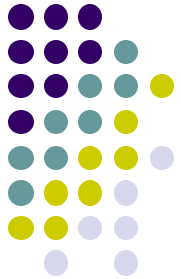
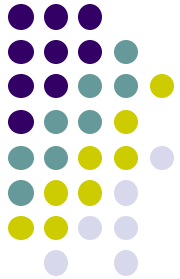


安全协议、隧道和VPN

1. 概述：主要安全协议



- 网络接口层
  - PAP（Password Authentication Protocol，密码认证协议）
  - CHAP（Challenge Handshake Authentication Protocol，挑战握手认证协议）
  - PPTP（Point-to-Point Tunneling Protocol，点对点隧道协议）
  - L2F（Level 2 Forwarding protocol，第二层转发协议）
  - L2TP（Layer 2 Tunneling Protocol，第二层隧道协议）
  - WEP（Wired Equivalent Privacy，有线等效保密）
  - WPA（Wi-Fi Protected Access，Wi-Fi网络保护访问）
  - 。。。

主要安全协议

- 网际层
  - IPSec（IP Security，IP层安全协议）
- 传输层
  - SSL（Secure Socket Layer，安全套接字层）/TLS（Transport Layer Security，安全传输层）

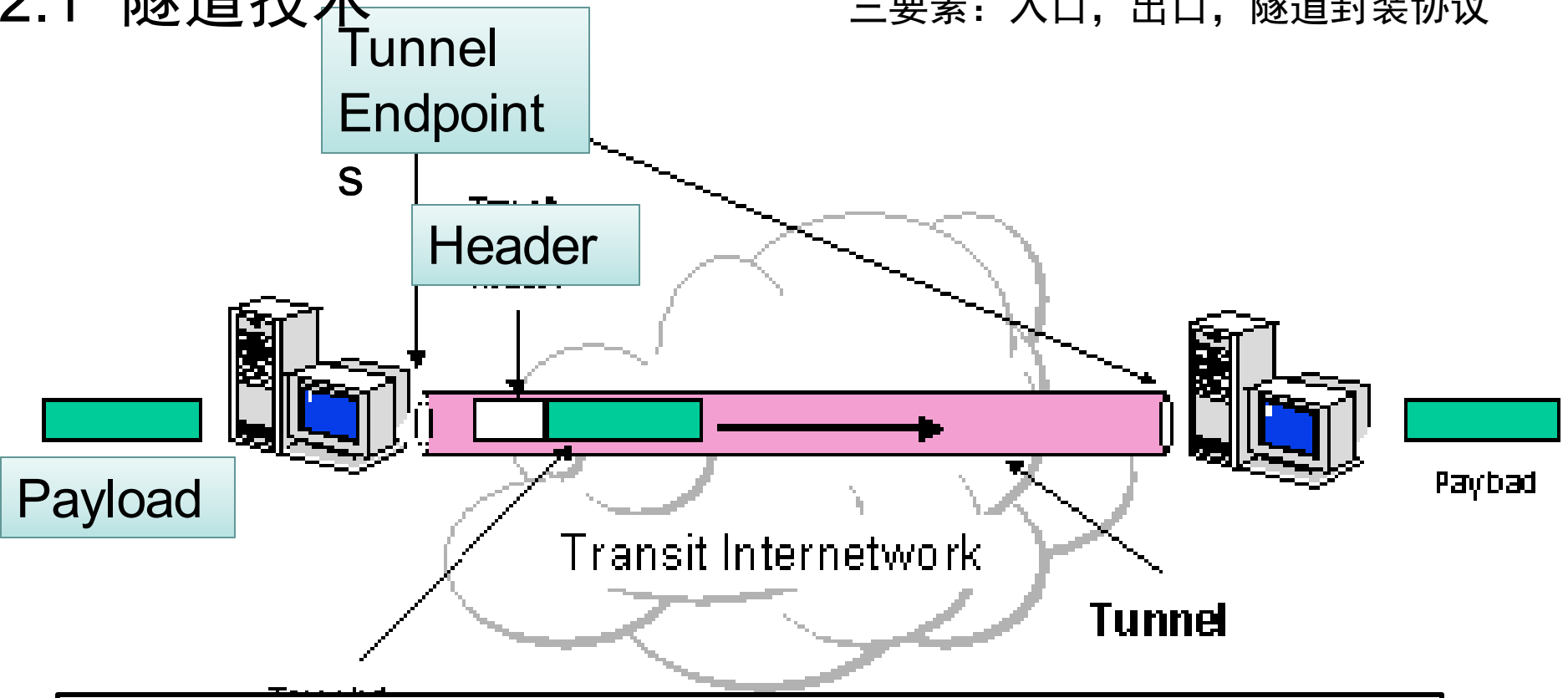
主要安全协议

- 应用层
  - SSH（Secure Shell Protocol，安全外壳协议）
  - Kerberos
  - PGP（Pretty Good Privacy）
  - S/MIME（Secure/Multipurpose Internet Mail Extensions，安全的多功能Internet电子邮件扩充）
  - S-HTTP（Secure Hyper Text Transfer Protocol，安全超文本传输协议）
  - SET（Secure Electronic Transaction，安全电子交易）
  - ……

2. 安全协议应用

2.1 隧道技术

三要素：入口，出口，隧道封装协议

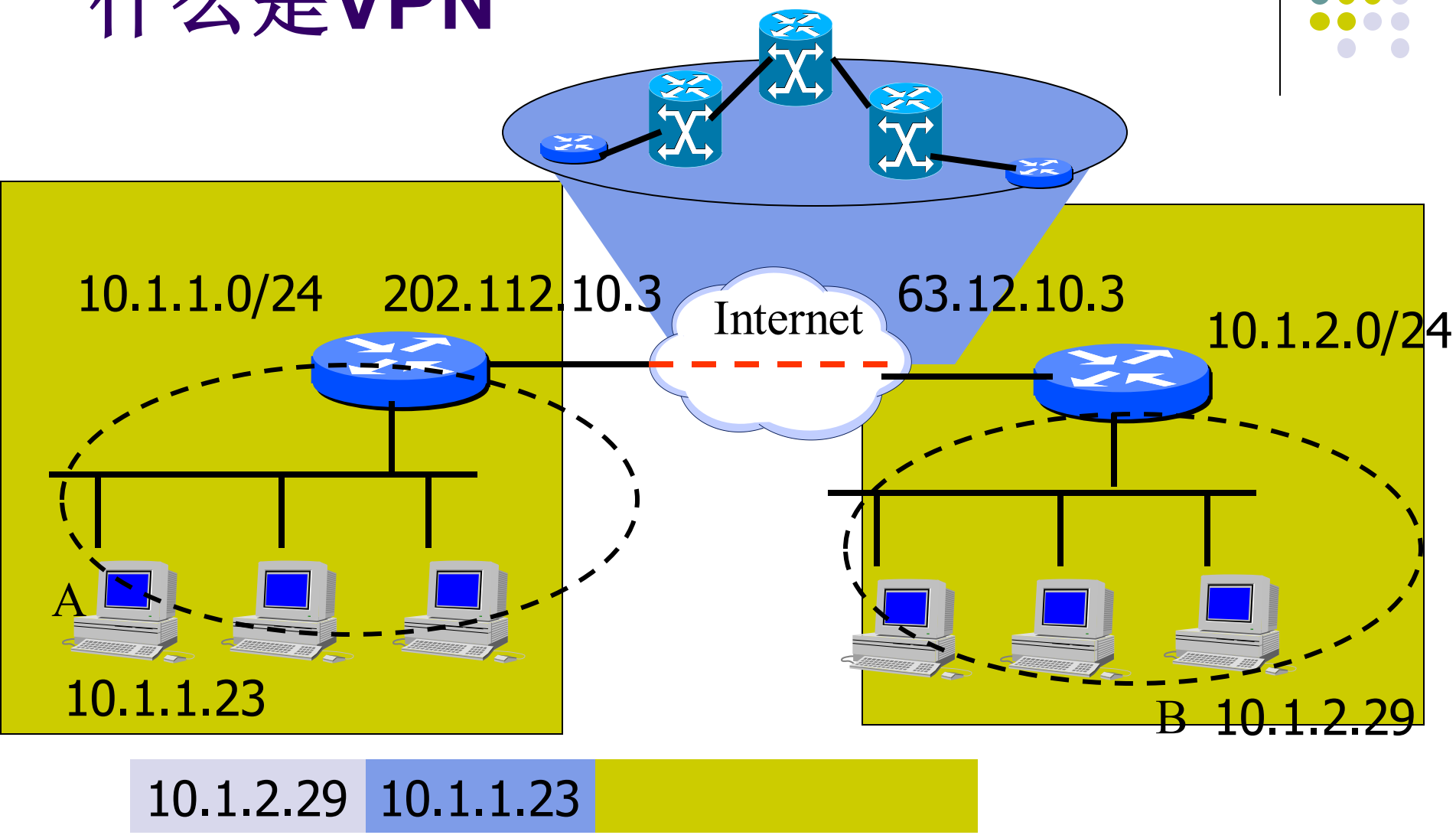


被封装的数据包在外层网络（如：公共互联网络）上传递时所经过的逻辑路径称为隧道

2.2虚拟专网 VPN

- 虚拟专网 VPN(Virtual Private Network)
  - VPN使用户通过公用网络（如Internet)安全地访问企业网络（如Intranet，Extranet)
- 名字含义上理解VPN：
  - 虚拟：不是企业自己用专线连接的，
    - VPN是通过公网提供的，网络内的交换、传输设备都属于公网，不为企业所有
  - 专网：
    - 统一的地址策略，如都用网络号为10的地址，有足够的地址空间，可以很方便的进行子网划分
    - 统一的管理策略，网络虽然跨越公网，但仍可统一规划管理
    - 安全性，具有企业网络的安全性，只有合法用户才可访问，网络上传送的数据只有专网中的用户才可见
    - 服务质量。。。

什么是VPN

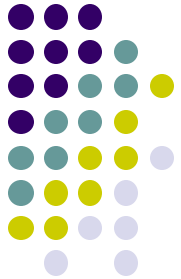


10.1.2.29	10.1.1.23	

VPN的种类

- 从用户类型的角度：
  - 拔号用户：access VPN (VPDN)
    - 用户发起的
    - 接入服务器发起的
  - 企业用户：site-to-site VPN (Intranet , Extranet VPN)

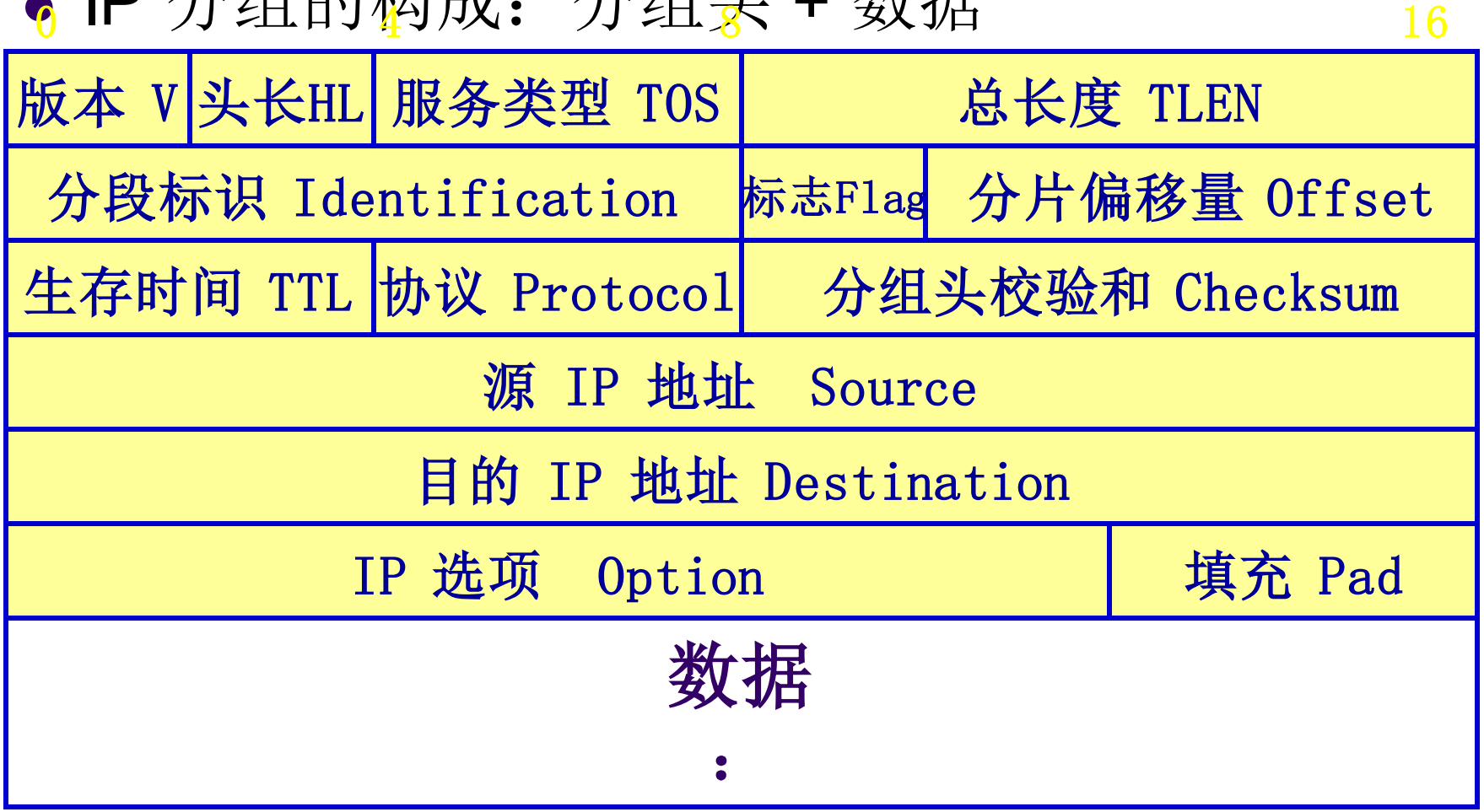
- 从所采用的技术角度：
  - 二层VPN：利用ATM ，FR，MPLS等二层虚连接技术
  - 三层VPN：IP安全隧道技术，MPLS
  - 应用层VPN：SSL VPN



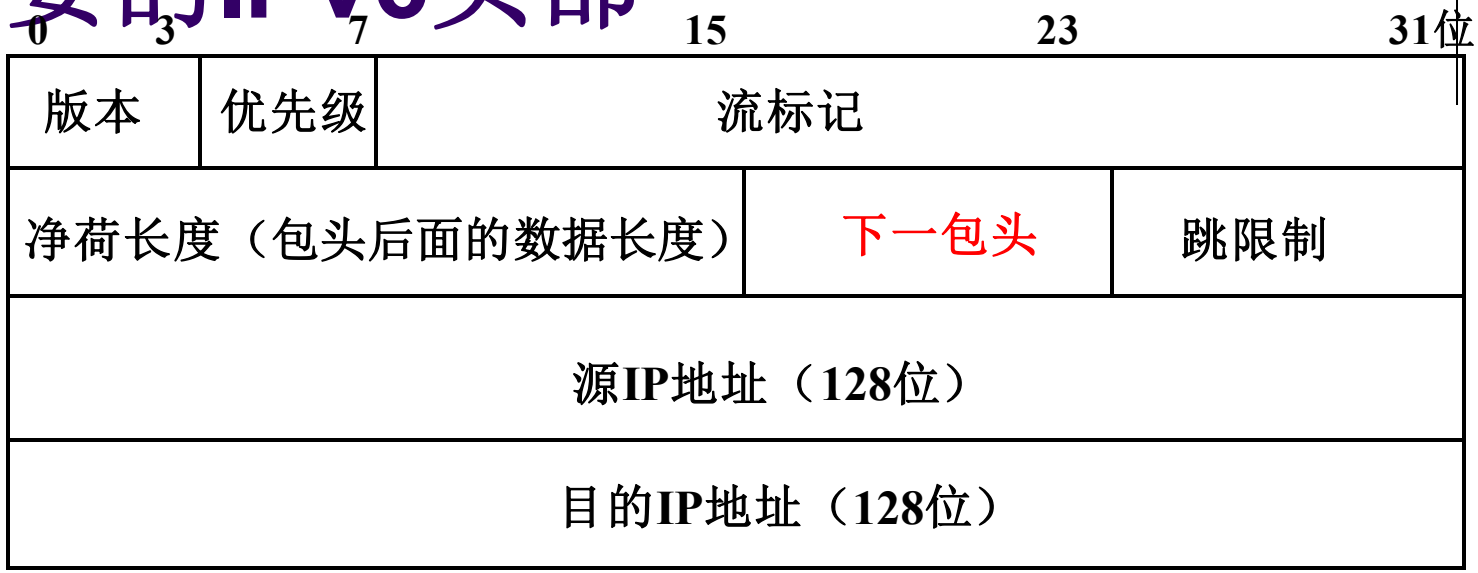
网络层安全协议

IP 分组的结构

- IP 分组的构成：分组头 + 数据



主要的IPv6头部



头部长度固定，使用扩展头标 来处理特殊分组；

删除头校验功能；

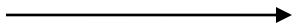
删除分段功能 。

增加了业务量等级和流标记。

IPv6IP分组的扩展包头

IP包的不安全性

- 能很容易伪造IP包的地址、修改内容、重播以前的包及在传输中途拦截并查看包的内容。
- 不能保证IP包：
  - 来自原先要求的发送方（源地址）
  - 包含的是发送方当初放在其中的原始数据
  - 原始数据在传输途中未被其他人看过



用安全的术语描述：

IPSEC安全功能

IPSec

- IPSec为IP及上层（UDP和TCP）提供的保护形式：
  - 数据源验证
  - 无连接数据的完整性验证
  - 数据内容的机密性（是否被人看过）
  - 抗重发保护

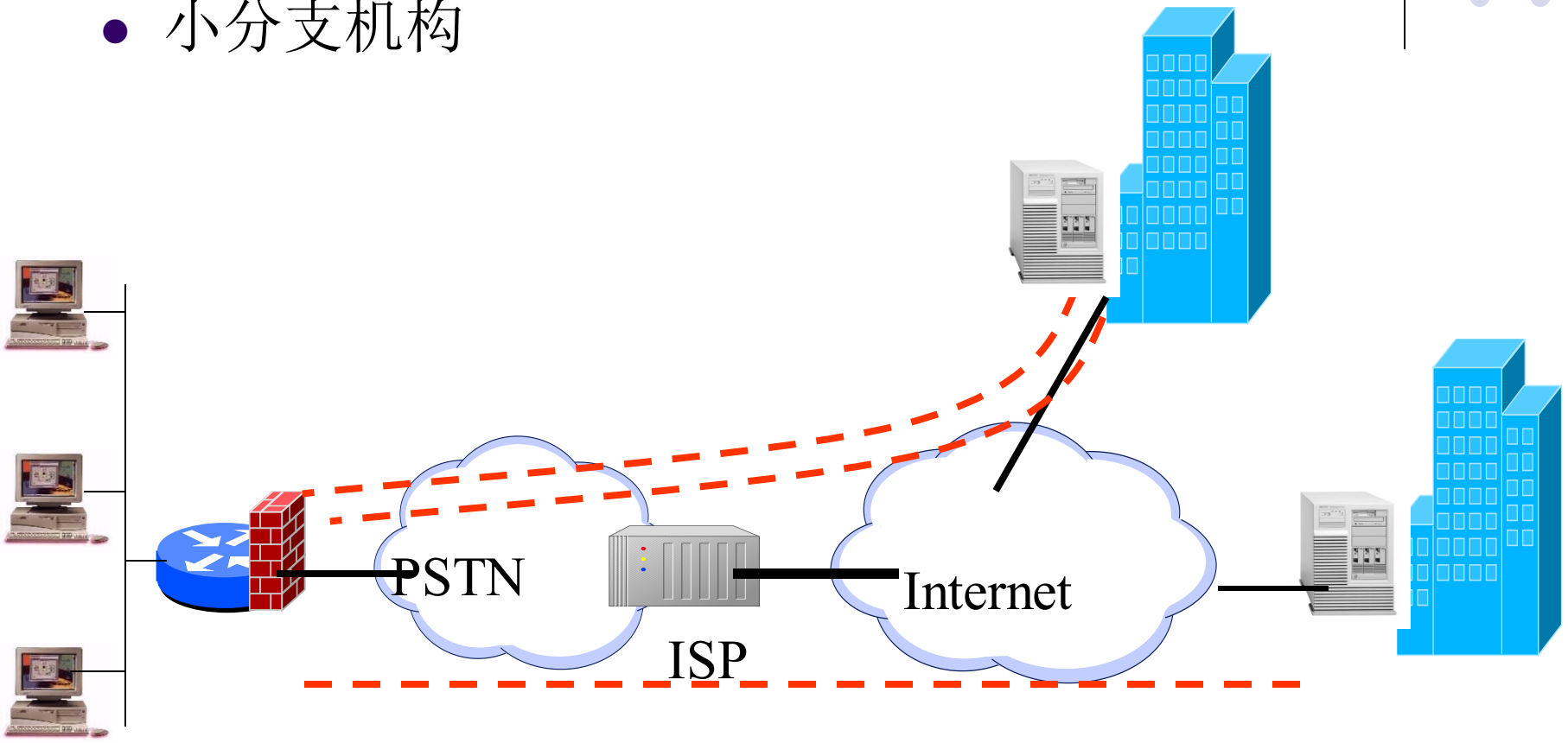
思考：

- IPSEC协议设计：思考比较：传输层安全
  - 实现的安全功能
  - 应用场景：主机节点，网络节点
    - IP层的安全保护：
      - 可能有多个安全策略
      - 更多的密码材料计算

安全性，效率

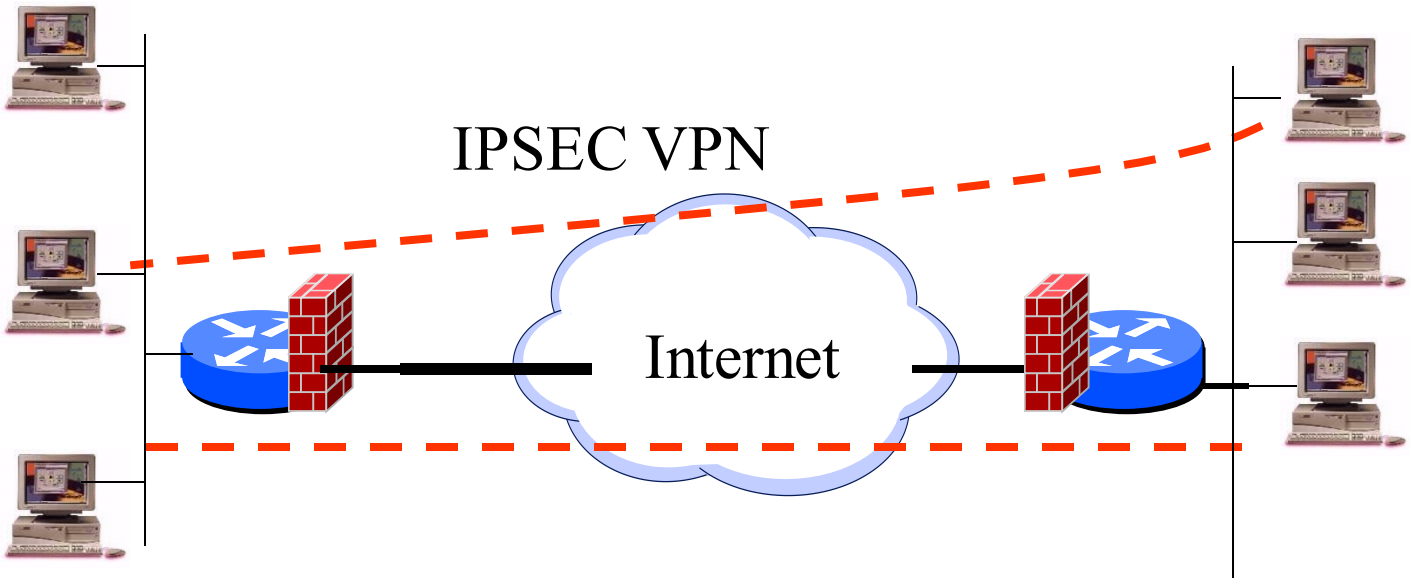
IPSec的应用 - VPN

- 小分支机构

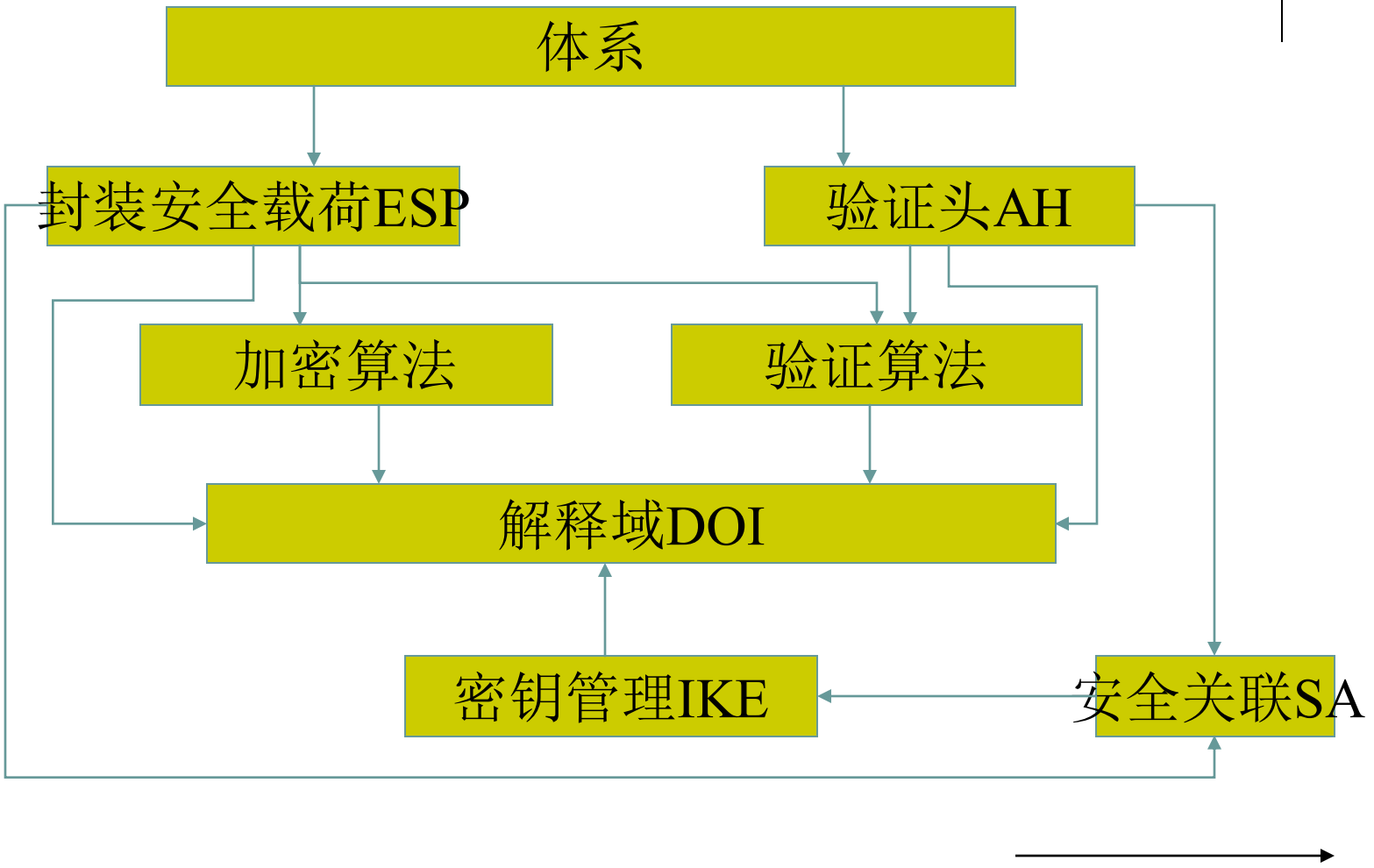


安全隧道

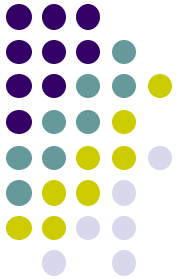
基于主机的VPN



IPSec体系结构

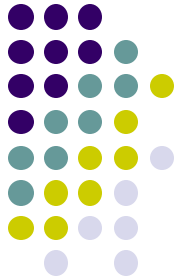


IPSEC的体系结构



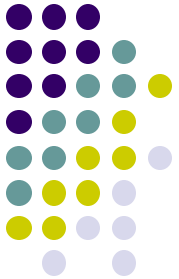
- IPSec体系结构包括以下几个基本部分： AH（Authentication Header，认证头）、ESP（Encapsulating Security Payload，封装安全载荷）、IKE（Internet Key Management，密钥交换协议）、SA（Security Association，安全关联）、DOI（Domain of Interpretation，解释域）、认证和加密算法。
- SA是IPSec的基础，决定通信中采用的IPSec安全协议、散列方式、加密算法和密钥等安全参数，通常用一个三元组（安全参数索引、目的IP地址、安全协议）唯一表示。SA总是成对出现的，对等存在于两端的通信实体，是通信双方协商的结果。

IPSec的体系结构

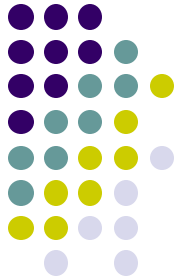


- AH或ESP提供的安全保障完全依赖于它们采用的加密算法，因此，需要一系列强制实行的加密算法。
- IPSec提供的安全服务需要用到共享密钥，因此定义了一种标准的方法，用以动态地验证IPSec参与各方的身份、协商安全服务以及产生共享密钥等---IKE（Internet密钥交换）

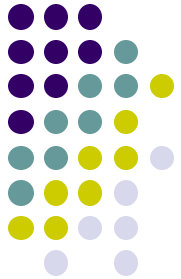
相关RFC



- IETF的IPSec工作组定义了12个RFC，对IPSec的体系、密钥管理、基本协议以及各协议的运行模式。
- IPSec的结构文档（RFC2401）：
  - 定义了IPSec的基本结构，所有具体的实施方案都建立在它的基础上。
  - 定义了IPSec提供的安全服务；
  - 它们是如何使用以及在哪里使用；
  - 数据包如何构建及处理；
  - IPSec处理同策略间如何协调。



- 认证头AH RFC2402
  - 认证、完整性检查，可选的重发保护
- 封装安全净荷ESP RFC2406
  - 机密性 、认证、可选的重发保护、完整性检查
- 定义了协议、载荷头的格式及提供的服务
- 定义了包的处理规则



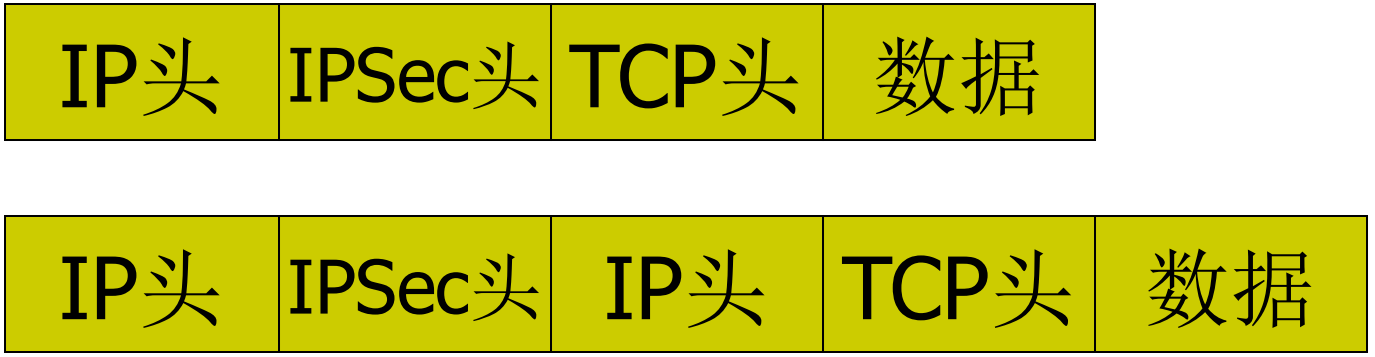
- 安全方面：
  - 基本ISAKMP规范：RFC2408
  - IPSec解释域(DOI)：RFC2407
  - IKE规范本身：RFC2409

IPSec的实施

- IPSec可以在终端主机、网关/路由器或两者中同时进行实施和配置。
  - 在主机实施：
    - 保障端到端的安全
    - 能够实现所有IPSec安全模式
    - 能够逐数据流提供安全保障
    - 在建立IPSec的过程中，能维持用户身份的验证。
  - 在路由器实施
    - 能对通过公共网在两各子网之间流动的数据提供安全保护。
    - 能进行身份验证，并授权用户进入私有网络。VPN

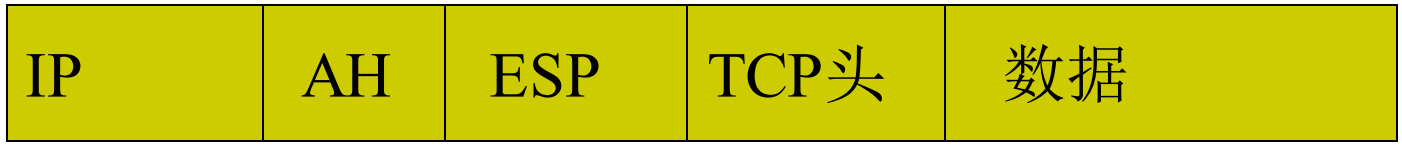
IPSec的模式

- IPSec可以用来保护一个完整的IP载荷，也可以用来保护某个IP载荷的上层协议。是通过两种不同模式来完成的。
- 传送模式（transport mode)：保护上层协议及IP头的部分字段，只用于基于主机的实现
- 通道模式(tunnel mode)：保护整个IP数据报



传送模式

- 在传送模式中，AH和ESP保护的是传输头。
- IPSec组件截获传输层数据，根据需要增加安全协议，然后，调用部分网络功能，增加网络头。
- 所有数据包都需要加密，采用ESP；
- 只对传输层数据进行验证，用AH。
- 只有要求端-端安全保护的时候，才使用传送模式。



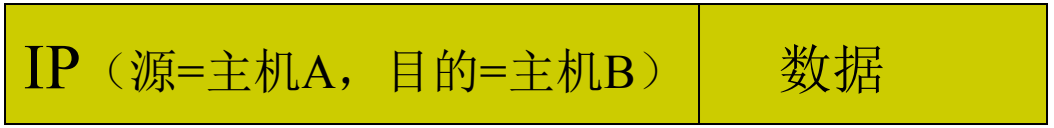
通道模式（隧道）

- 什么时候使用通道模式的IPSec？
  - 当数据包的最终目的地不是安全终点，
  - 安全保护能力需要由一个设备来提供，而该设备不是数据始发点的时候；BITS，BITW
  - 数据包需要保密传送到与实际目的地不同的另外一个目的地的时候；
  - 路由器为自己转发的数据包提供安全服务的时候。

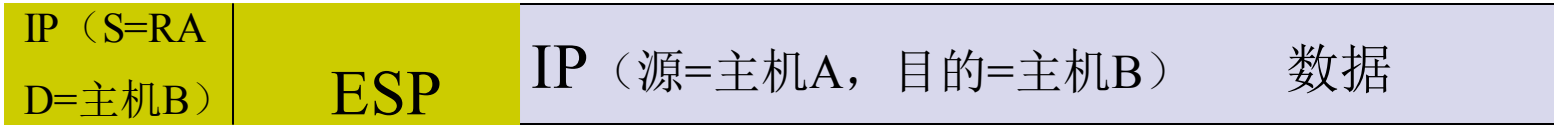
通道模式

- 通道模式中的数据包有2个头：内部头和外部头。
  - 内部头由主机创建
  - 外部头是由提供安全服务的设备添加的。

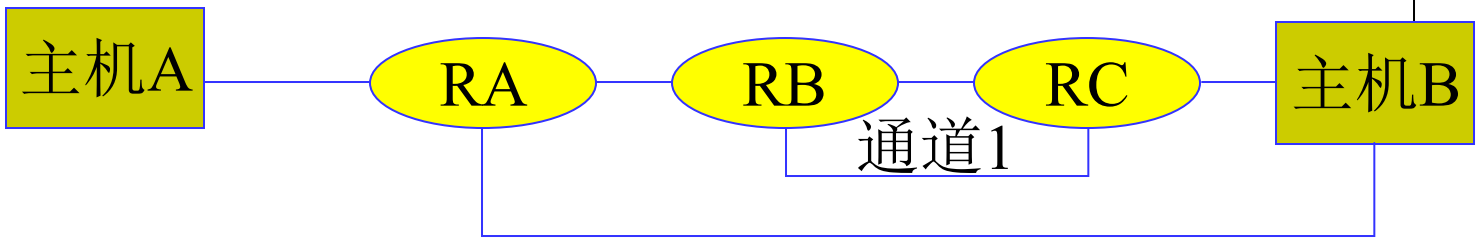
主机A发出的原始数据



经过RA后



嵌套通道：有效通道



主机A发出的原始数据

IP（源=主机A，目的=主机B）	数据

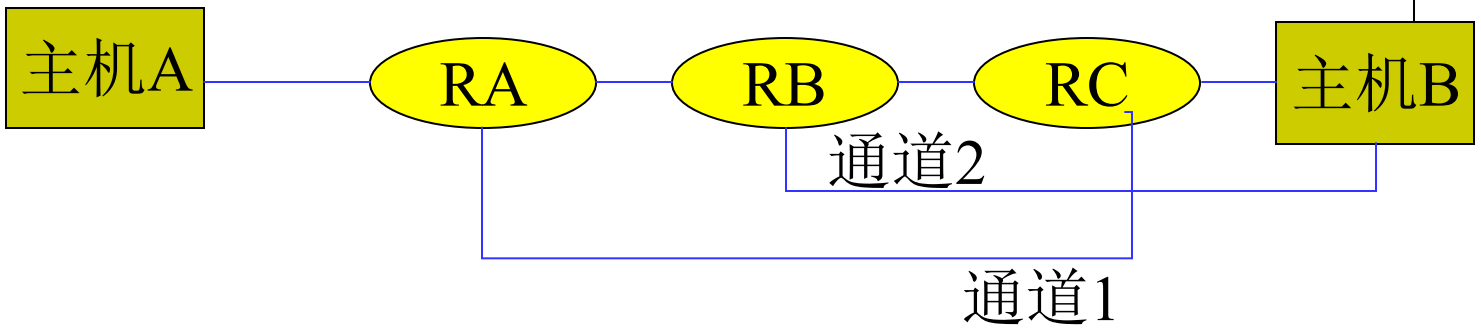
经过RA后

IP（S=RA D=主机B）	ESP	IP（源=主机A，目的=主机B）	数据

经过RB后

IP（S=RB D=RC）	AH	IP（S=RA D=主机B）	ESP	IP（源=主机A，目的=主机B）	数据

嵌套通道：无效通道



主机A发出的原始数据

IP（源=主机A，目的=主机B）	数据

经过RA后

IP（S=RA D=RC）	ESP	IP（源=主机A，目的=主机B）	数据

经过RB后

IP（S=RB D=主机B）	AH	IP（S=RA D=RC）	ESP	IP（源=主机A，目的=主机B）	数据

安全联盟（SA）

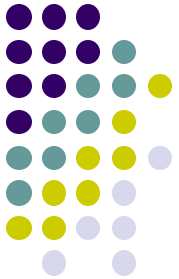
- 安全联盟（Security Associate SA）是构成IPSec的基础。是两个通信实体经协商建立起来的一种协定。
- 决定：
  - 用来保护数据包安全的IPSec协议 (AH,ESP)
  - 算法
  - 密钥
  - 模式
  - 密钥的有效存在期

SA特点

- SA是单向的。

  例如：A与B通信，需要有A的SA（out)对应B的SA(in)； B的SA（out)对应A的SA(in)。可能会不相同。

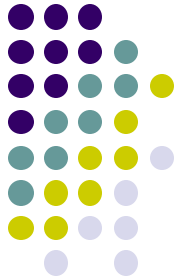
- SA与协议相关。



- SA数据库（SADB）用来维持SA记录。
- 安全策略数据库（SPD）：定义了安全通信特性；什么时间使用什么安全协议；如何对待IP包(对一个包提供的安全服务)。

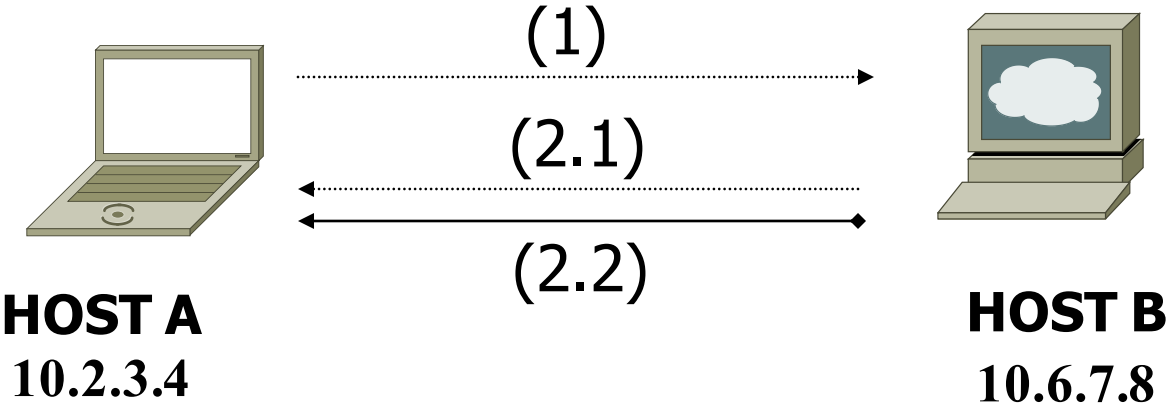
- 如何确定采用什么SA？
  - 安全参数索引 SPI
  - IPSec协议（AH, ESP)
  - 方向

安全参数索引SPI



- 什么是SPI？SPI是一个32位长的数据实体，用于独一无二地标识接收端上的一个SA。
- 由于SA是通信双方约定的密钥、加密算法等参数，需要告诉收方用哪个SA来保护这个数据。
- SPI被当成AH和ESP的一部分，随每个数据包发送。
- 由接收端/目标主机维护SPI与SA之间映射的唯一性。

IPSec配置举例 – 传送模式(1)



(1)

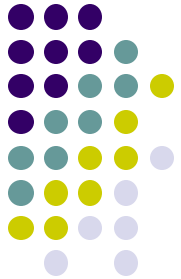
PROTO=AH

ALG=MD5(RFC1826)

KEY=MYSECRETMYSECRET 16 bytes

SPI=1000

IPSec配置举例 – 传送模式(2)



(2.1)

PROTO=AH

ALG=new-HMAC-SHA1(new AH)

KEY=KAMEKAMEKAMEKAMEKAME 20bytes

SPI=2000

(2.2)

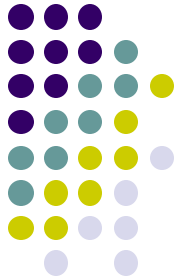
PROTO=ESP

ALG=new-DES-expIV(new ESP)

IV length = 8

KEY=PASSWORD 8bytes

SPI=3000

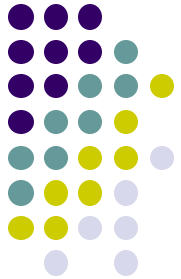


- 问题：
  - SA的管理问题
    - 存储
    - 生成：
      - 静态
      - 动态
    - 删除

SA管理

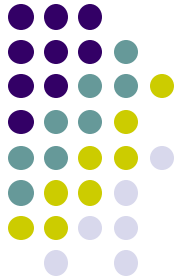
- 创建与删除，SA管理可以是手动的，也可以通过IKE完成。
- IKE（Internet密钥交换协议）
  - IKE代表IPsec对SA进行协商，并对SAD数据库进行填充
  - RFC2409所描述的IKE是一个混合型的协议，是Oakley和SKEME协议的混合，它建立在ISAKMP定义的一个框架上，在ISAKMP规定的框架内运作。
  - ISAKMP（Internet Security Association and Key Management Protocol) Internet安全联盟和密钥管理协议：定义了整套加密通信语言，包括包格式、重发计数器及消息构成。
  - Oakley（基于Diffie-Hellman的密钥交换协议）和SKEME定义了通信双方建立共享的验证密钥所必须采取的步骤。
  - IKE使用ISAKMP语言对这些步骤进行表述。
  - 两个阶段
    - 第一阶段建立IKE安全联盟
    - 第二阶段利用这个既定的安全联盟，为IPsec协商具体的安全联盟

SA的删除



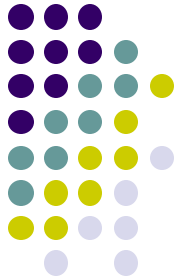
- 可以通过手工或IKE来删除一个SA
  - 存活时间过期
  - 密钥已遭破解
  - 使用SA加密/解密或验证的字节数已经超过策略设定的某个阈值。
  - 另一端要求删除SA
  - 定时更新SA

AH简介



- 应用方式：单独应用/与ESP组合/嵌套
- 对象：主机/安全网关/主机-安全网关
- 保护对象：上层协议和尽可能多的IP报头
- 安全业务
  - 数据源认证：身份验证器
  - 抗重播：唯一的、单向递增的序列号
  - 数据完整性：身份验证器
- 与ESP的不同：AH对外部IP头的各部分进行身份验证。

AH头

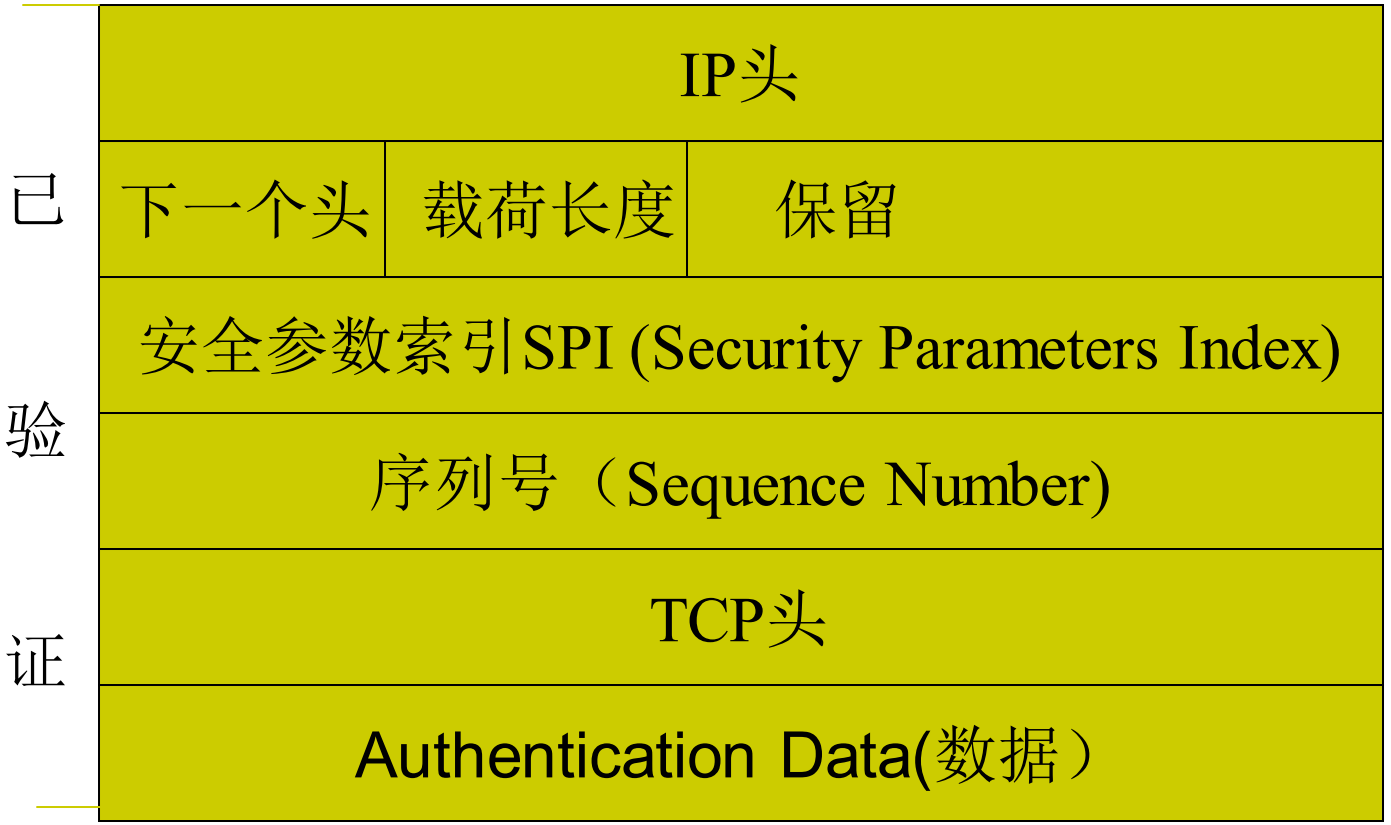


下一个头	载荷长度	保留
安全参数索引SPI (Security Parameters Index)		
序列号（Sequence Number)		
认证数据（变长）（Authentication Data）		

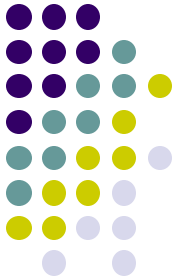
AH报头位置

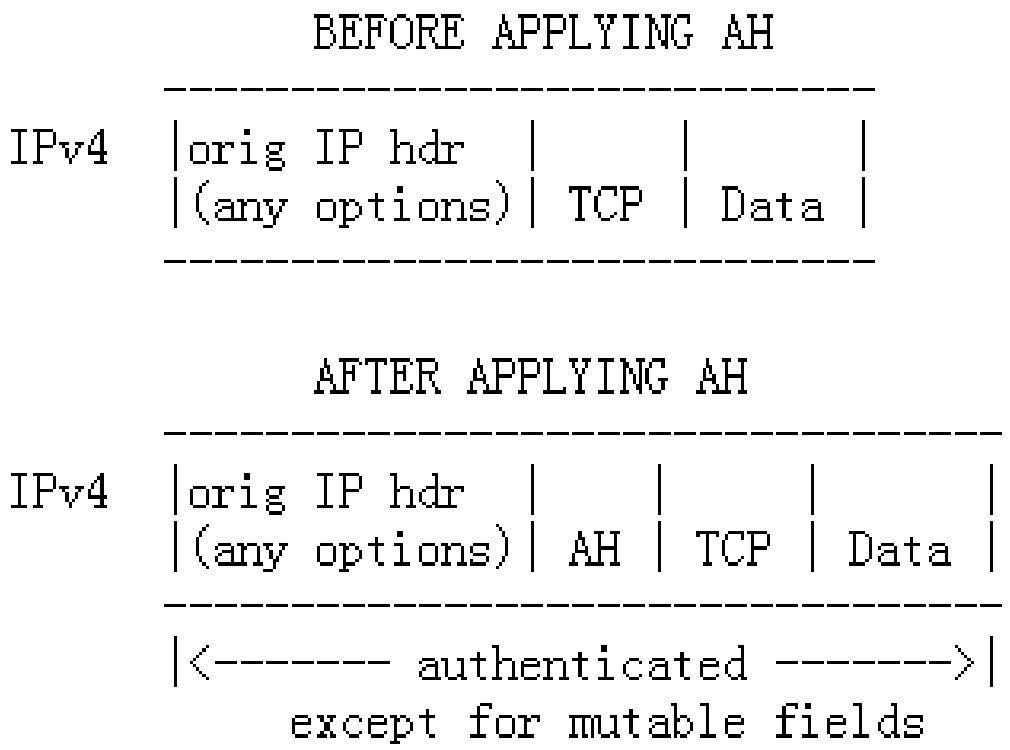
- AH报头在IP头之后
  - IPv4：AH头紧跟在IP头后面，这个IP头的协议字段是51。
  - IPv6：AH在扩展头之后，（包括逐跳、路由选择、分段头），目的地选项之前。

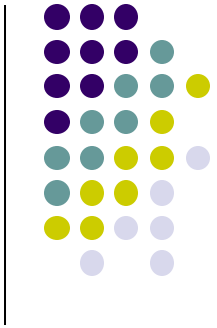
AH模式—传送模式


已
验
证
IP头
下一个头
载荷长度
保留
安全参数索引SPI (Security Parameters Index)
序列号（Sequence Number)
TCP头
Authentication Data(数据）

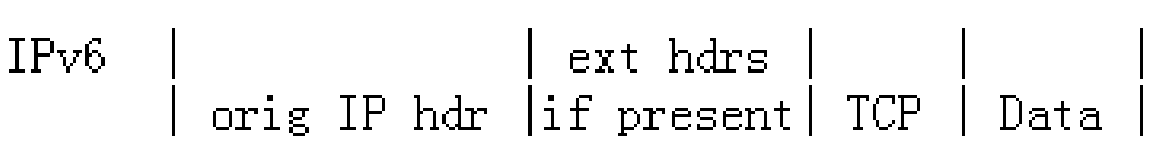
AH模式—传送模式



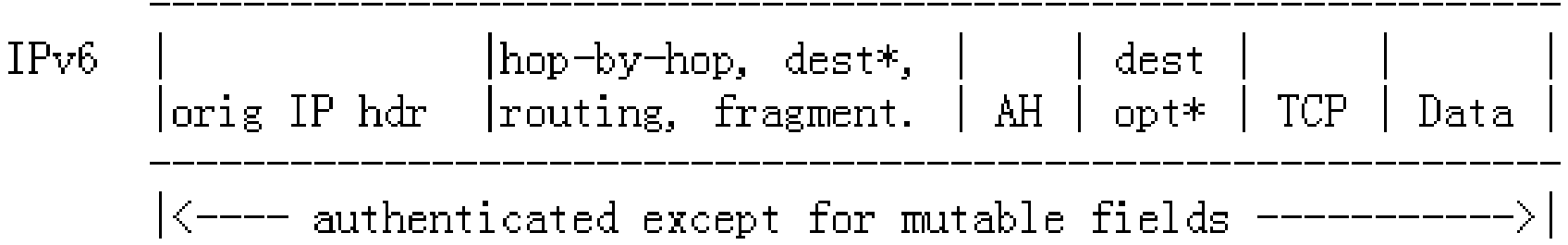

BEFORE APPLYING AH
IPv4
orig IP hdr
(any options)
TCP
Data
AFTER APPLYING AH
IPv4
orig IP hdr
(any options)
AH
TCP
Data
authenticated
except for mutable fields



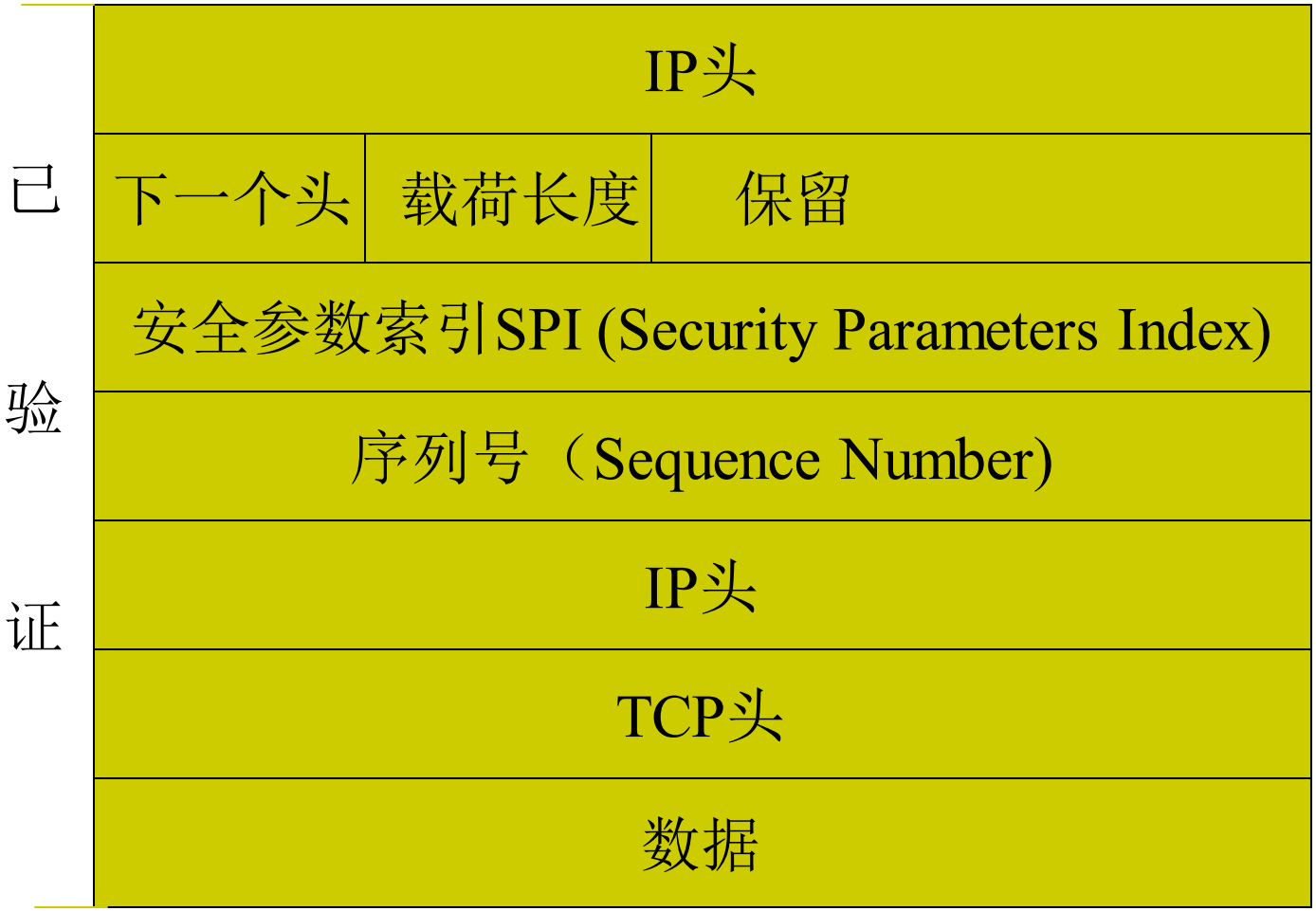
BEFORE APPLYING AH



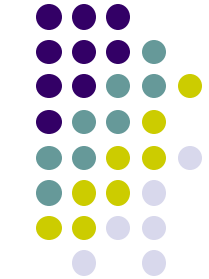
AFTER APPLYING AH

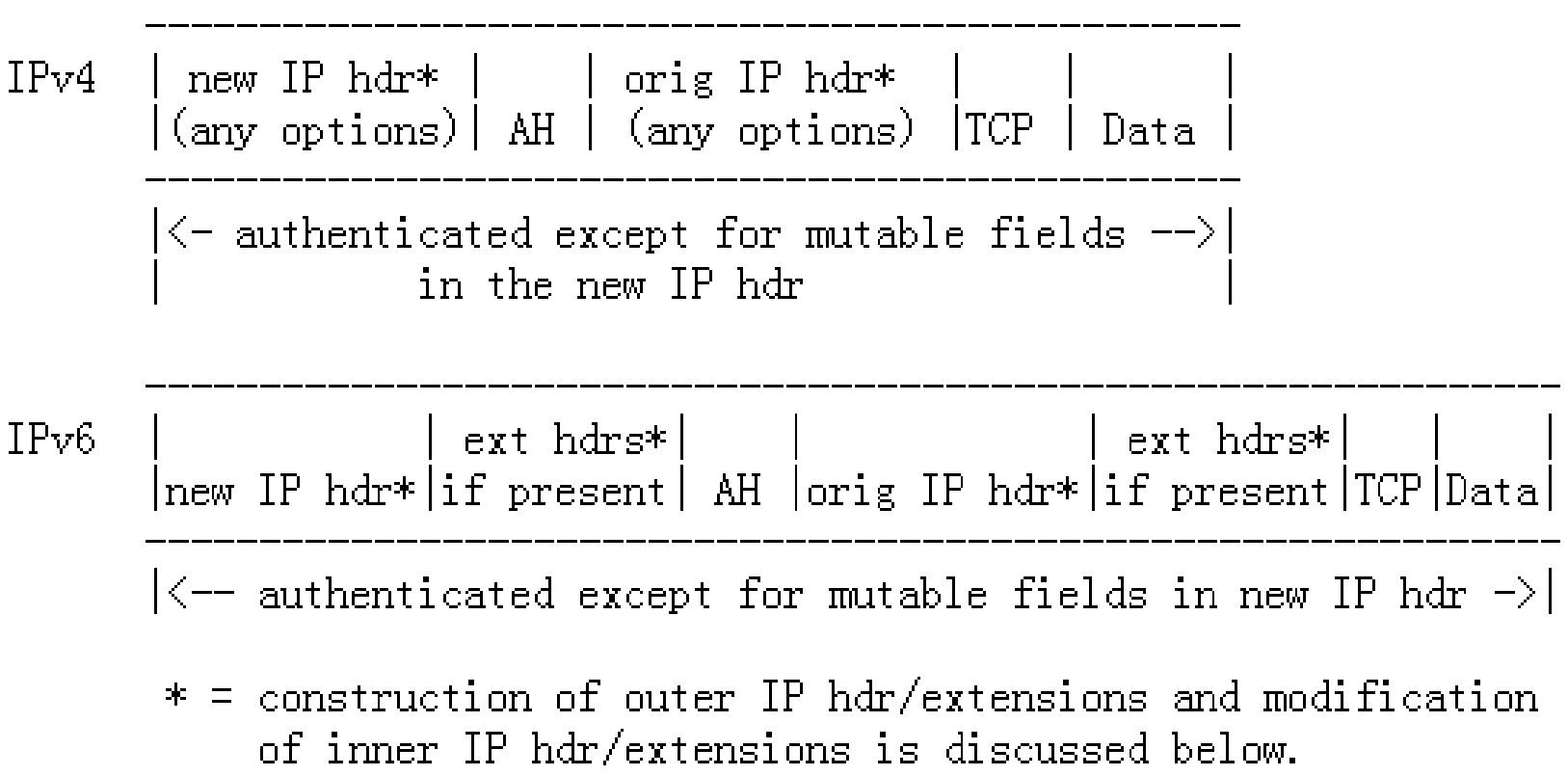


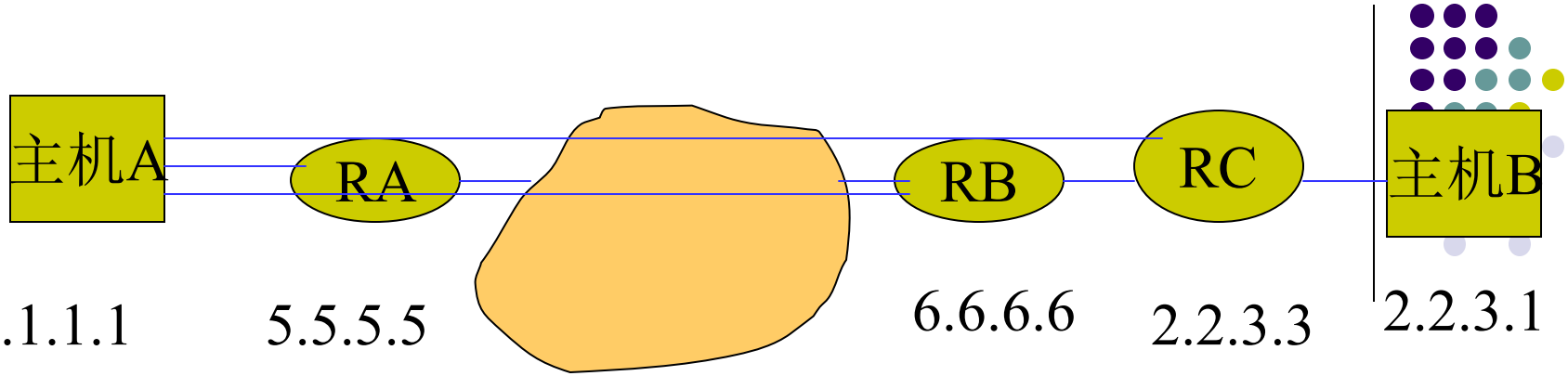
AH模式—通道模式


已
验
证
IP头
下一个头
载荷长度
保留
安全参数索引SPI (Security Parameters Index)
序列号（Sequence Number)
IP头
TCP头
数据

AH模式—通道模式




IPv4
new IP hdr*
(any options)
AH
orig IP hdr*
(any options)
TCP
Data
<- authenticated except for mutable fields ->
in the new IP hdr
IPv6
new IP hdr*
ext hdrs*
if present
AH
orig IP hdr*
ext hdrs*
if present
TCP
Data
<-- authenticated except for mutable fields in new IP hdr ->
* = construction of outer IP hdr/extensions and modification
of inner IP hdr/extensions is discussed below.



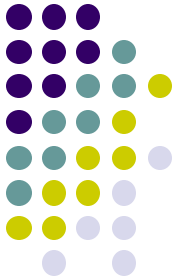
A的SPD

自	到	协议	端口	策略	通道目的地址
1.1.1.1	2.2.3.1	任意	任意	使用HMAC-MD5的通道AH	2.2.3.3
1.1.1.1	2.2.3.3	任意	任意	使用HMAC-MD5的通道ESP	6.6.6.6

A的外出SADB

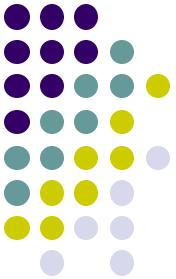
自	到	协议	SPI	SA
1.1.1.1	2.2.3.3	AH通道	11	HMAC-MD5密钥
1.1.1.1	6.6.6.6	ESP通道	12	HMAC-MD5密钥

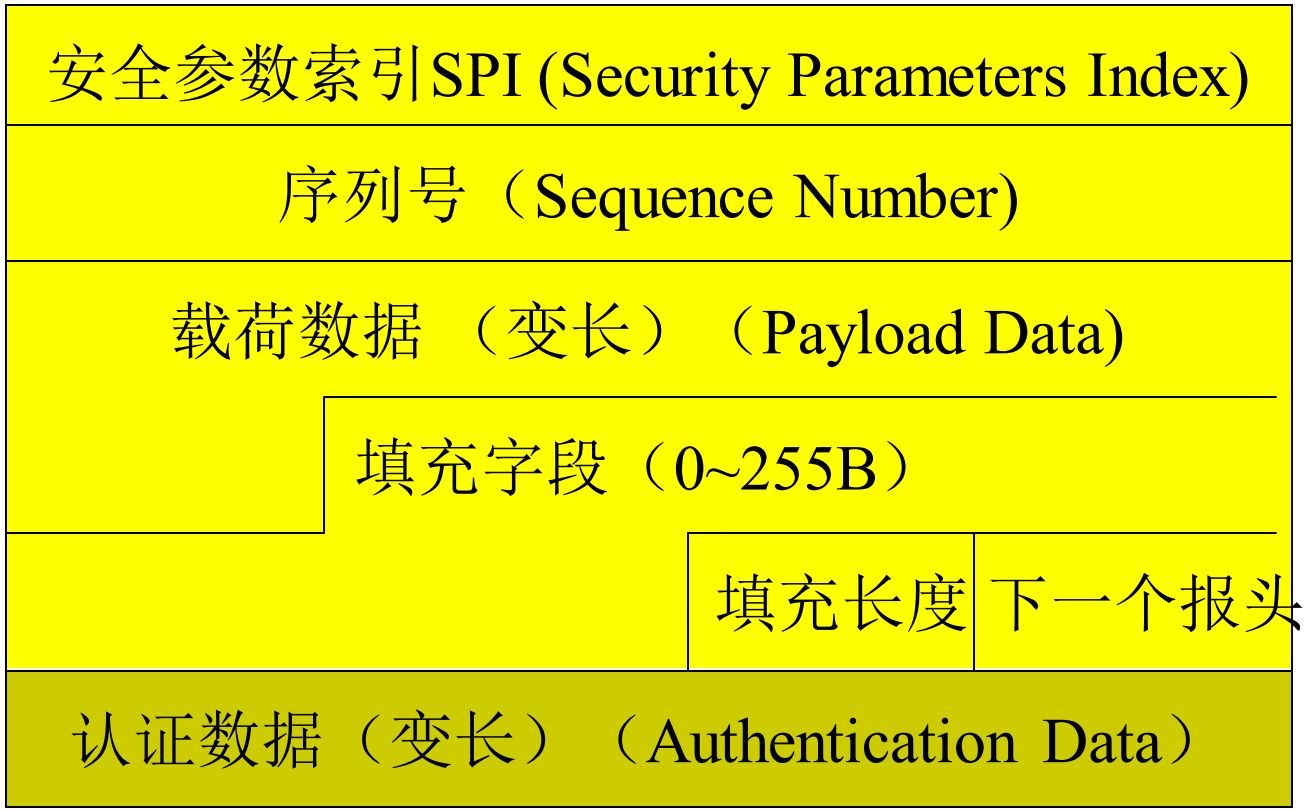
ESP简介



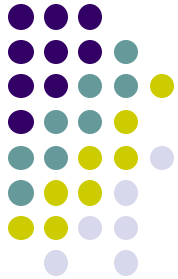
- 应用方式：单独应用/与AH组合/嵌套
- 对象：主机/安全网关/主机-安全网关
- 插入的位置
  - IP报头之后，上层报头之间（传送模式）
  - 被封装的IP报头之前（通道模式）
- 安全业务
  - 机密性：加密器
  - 数据源认证：身份验证器
  - 抗重播：唯一的、单向递增的序列号
  - 数据完整性：身份验证器

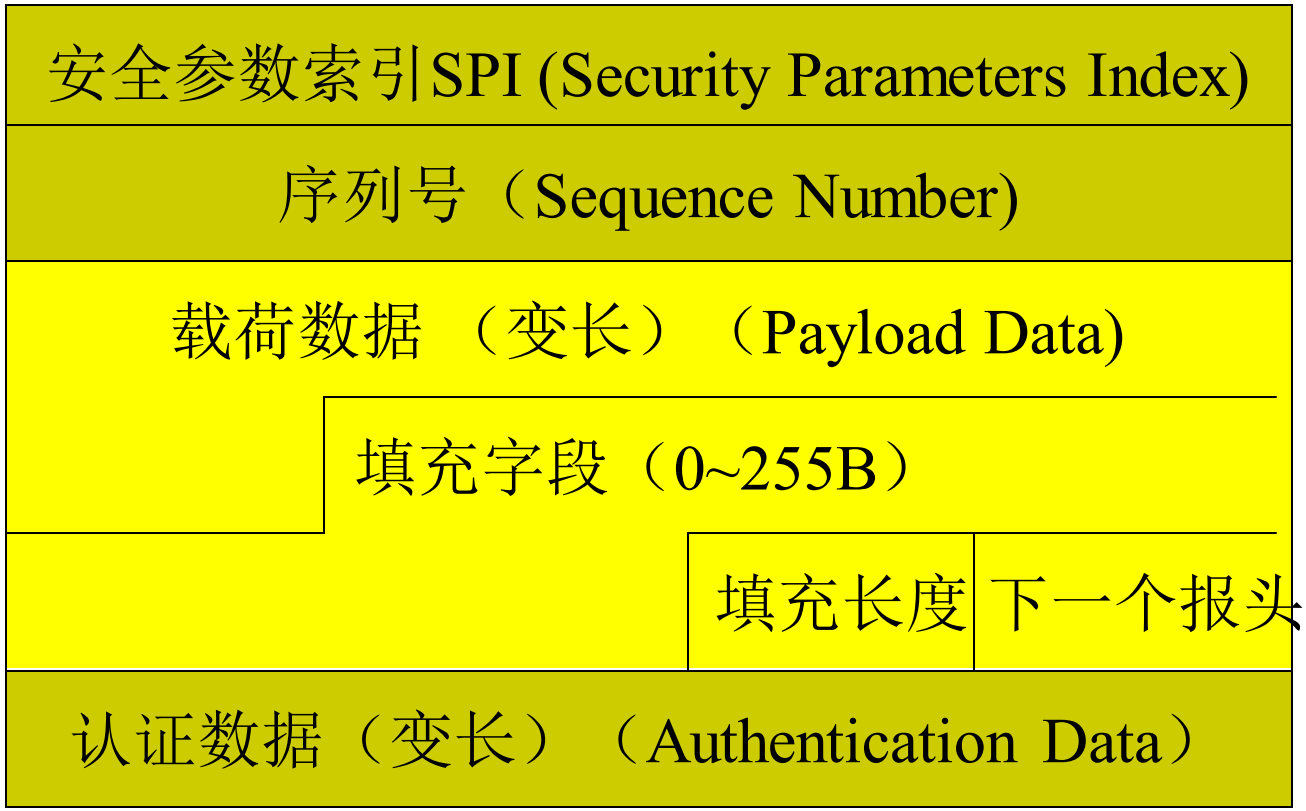
ESP业务范围—认证业务



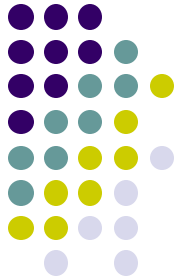


ESP业务范围—加密业务



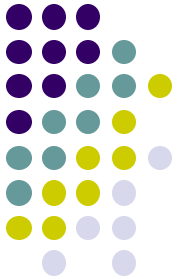


ESP报头内容-- SPI



- 32位的必选字段
- 与目标地址和协议（ESP）结合起来唯一标识处理数据包的特定SA。
- 数值可任选，一般是在IKE交换过程中由目标主机选定。
- SPI经过验证，但是不加密。
- 0~255保留

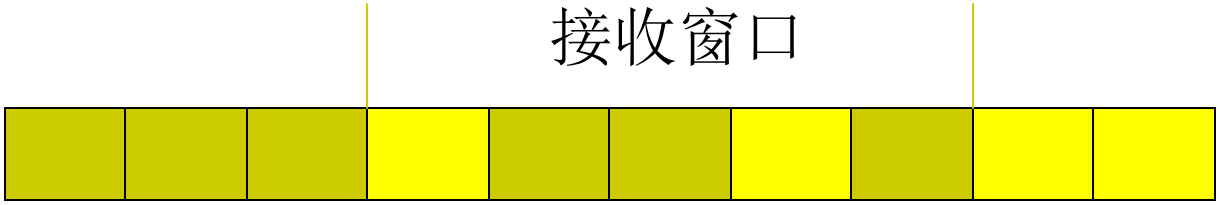
ESP报头内容– 序列号



- 32位的必选字段
- 独一无二、单向递增
- 对序列号的处理由收端确定
- SA开始时，收发端的序列号都设置为0
- 经过验证，但是不加密。

抗重播（Antireplay）

- 使用32位的独一无二、单向递增的序列号+滑动窗口，实现抗重播。
  - 在一个SA内，序列号不重复
  - 接收窗口大于32，推荐64。窗口左端对应起始序列号，右端对应将接收的包号。
  - 落在接收窗口内或右侧的数据包将接收



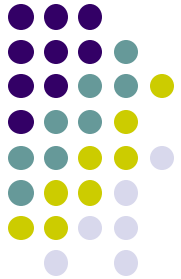
ESP报头内容– 载荷数据

- 变长的必选字段，整字节数长
- 包含由下一个报头字段描述的数据
- 加密同步数据
- 可能包含加密算法需要的初始化向量（IV），IV是没有加密的。

ESP报头内容–填充项

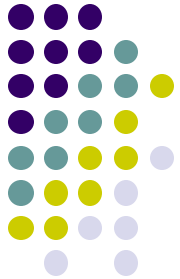
- 为什么需要填充？
  - 加密算法可能要求整数倍字节数
  - 保证认证数据字段对齐
  - 隐藏载荷真实长度，实现部分通信流保密，但是增加传输量
- 缺省填充方法：1~2~3~4……
- 可指定填充内容和接收端处理，发送者可添加0~255字节。

ESP报头内容—填充长度



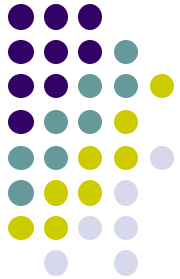
- 必选字段
- 表示填充字段的长度
- 合法的填充长度是0~255，0表示没有填充

ESP报头内容—下一个报头



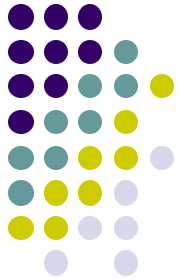
- 8比特长必选字段
- 表示在载荷中的数据类型
- 通道模式下，这个值是4，表示IP-in-IP；传送模式下是背后数据的类型，由RFC1700定义，如：TCP为6。

ESP报头内容—认证数据



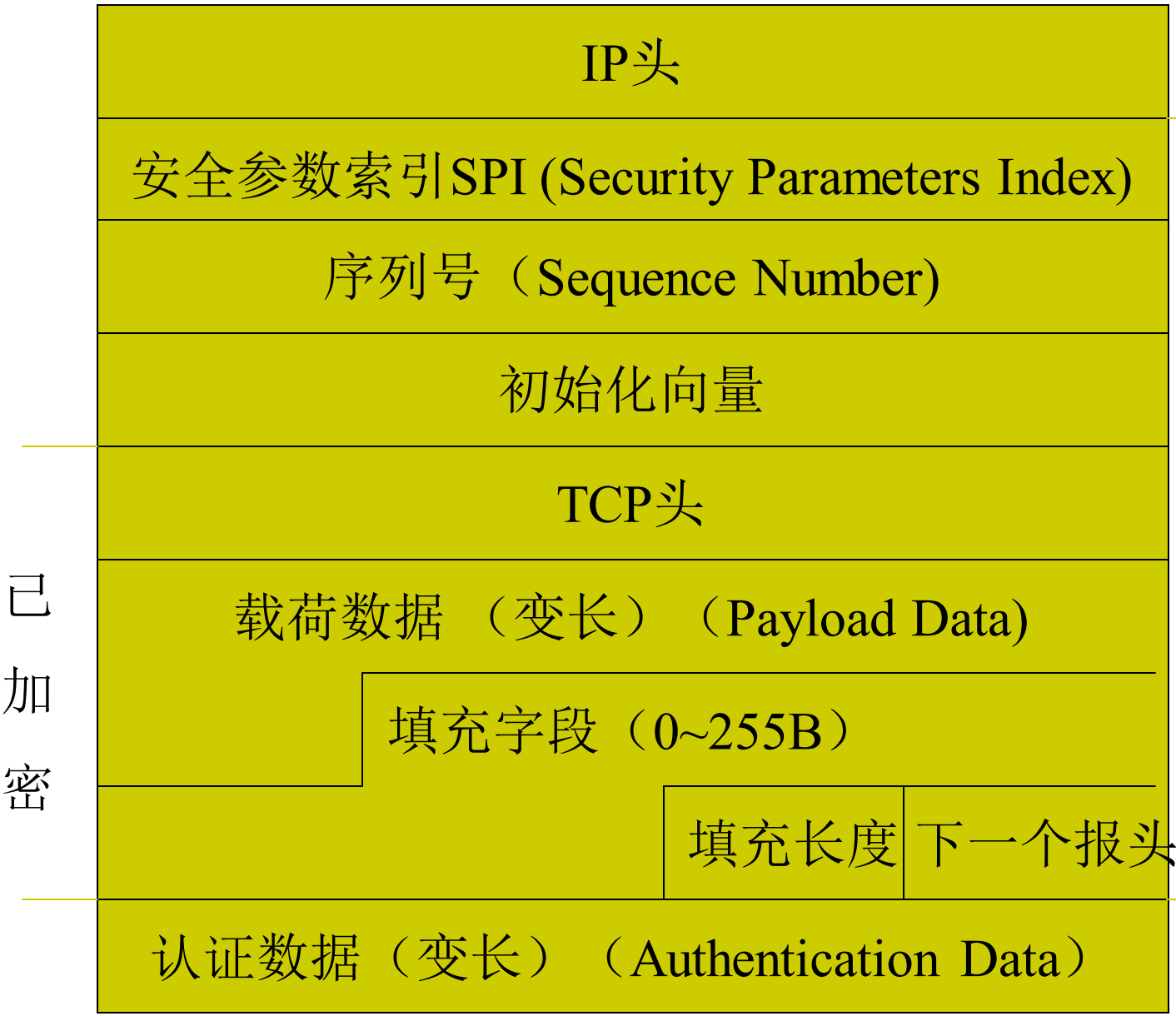
- 变长的可选字段，只有SA中包含了认证业务时，才包含这个字段。
- 认证算法必须指定认证数据的长度、比较规则和验证步骤。

ESP报头位置



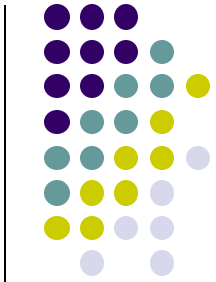
- ESP报头在IP头之后
  - IPv4：ESP头紧跟在IP头后面，这个IP头的协议字段是50。
  - IPv6：ESP在扩展头之后，（包括逐跳、路由选择、分段头），目的地选项之前。

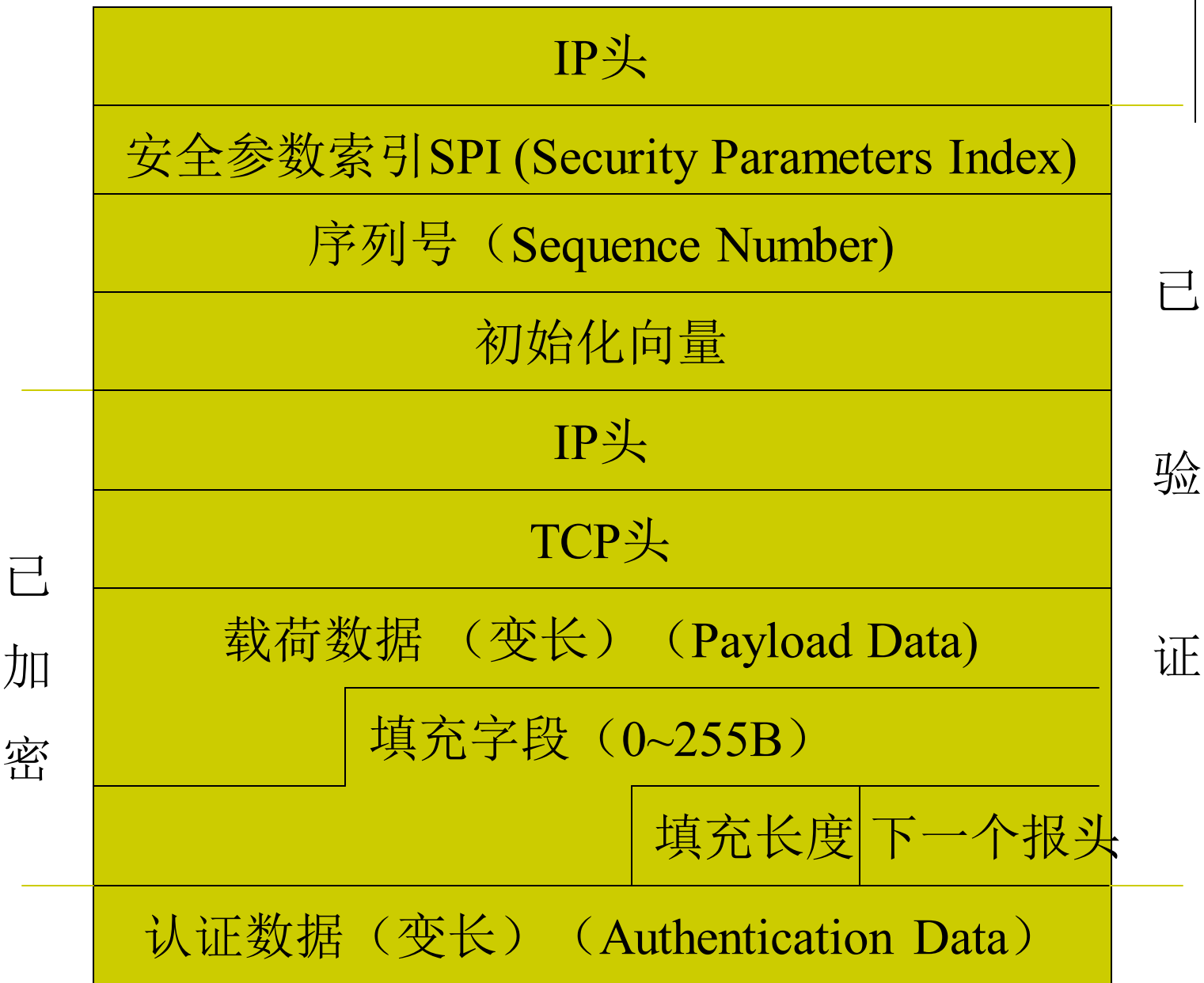
ESP模式—传送模式



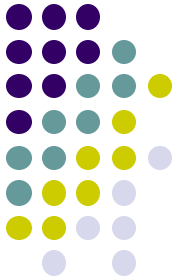
注意与AH的区别

ESP模式—通道模式



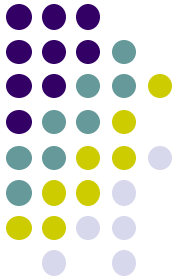

IP头
安全参数索引SPI (Security Parameters Index)
序列号（Sequence Number)
初始化向量
IP头
TCP头
载荷数据 （变长）（Payload Data)
填充字段（0~255B）
填充长度
下一个报头
认证数据（变长）（Authentication Data）
已加密
已验证

ESP算法—加密算法



- 由SA指定
- ESP为使用对称加密算法设计
- 可满足同步加密要求
- 块模式/流模式加密
- 可以为NULL

ESP算法—认证算法

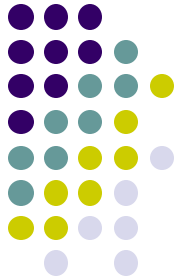


- 由SA指定
- 点到点时的算法：对称加密算法/单向HASH函数
- 多播时的算法：与非对称签名算法结合的单向HASH函数

ESP处理—出站处理

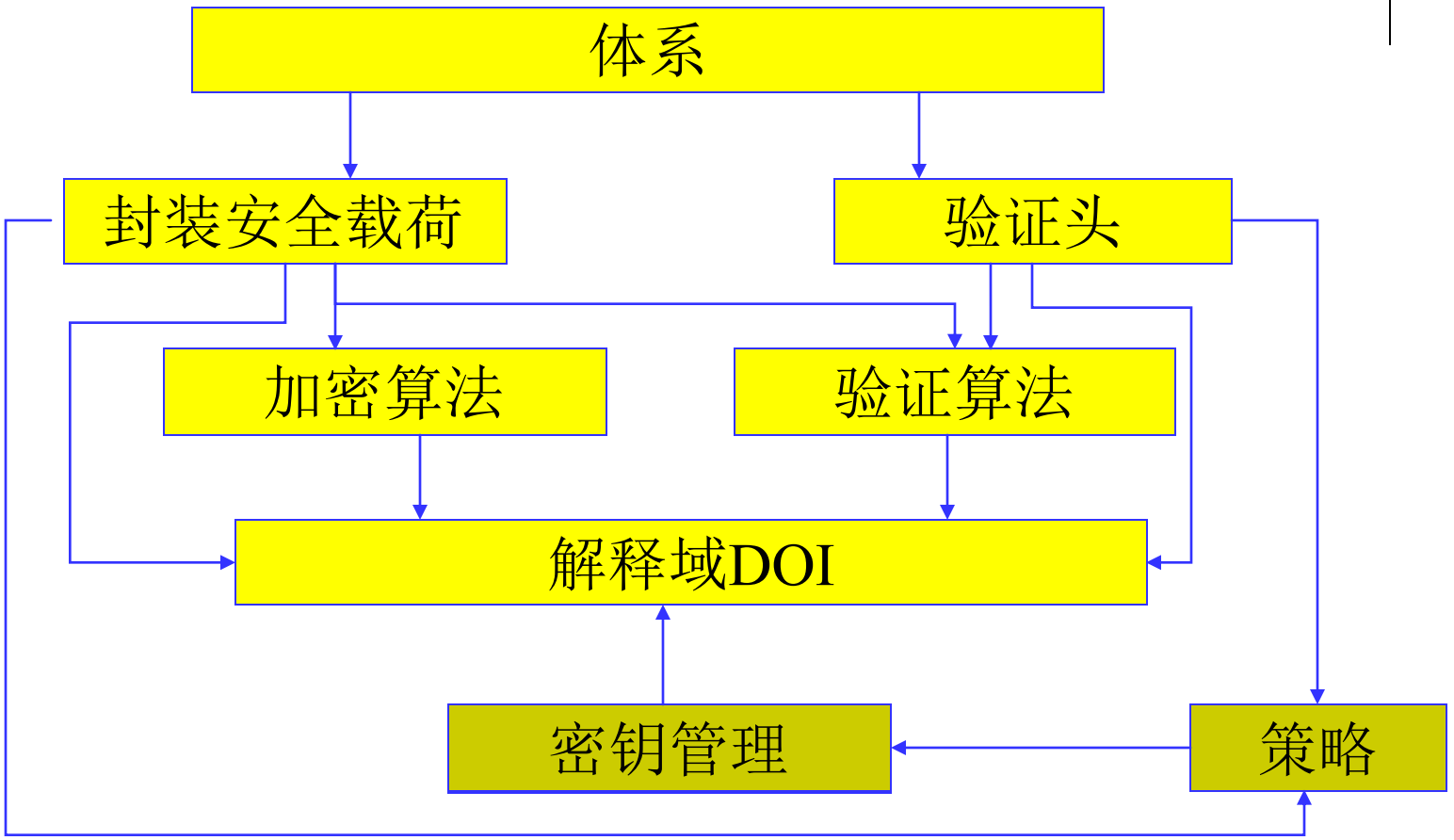
- SA查找
- 分组加密
  - 先封装，填充，后加密。
  - 先加密，后认证。可以加速接收端检测和拒绝速度；可以对分组进行并行处理。
- 序列号生成
- 完整性检查值ICV计算
- 重新计算IP头校验
- 分段：
  - 传送模式下，ESP应用于整个分组。如果在路由器被分段，接收时，先重组，后处理。
  - 通道模式：用于分段。

ESP处理—入站处理



- 重组
- SA查找
- 序列号认证
- ICV验证
- 分组解密
- IP包重新整理和提交

Internet密钥交换—IKE协议



介绍的内容

- 简介
- IKE协议
  - IKE SA的参数
  - 两个阶段的交换
- IKE安全性分析与改进

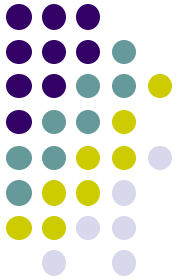
简介

- RFC2409：Internet Key Exchange——Internet密钥交换协议（IKE协议）。一种混合型协议。
- IKE协议的作用：
  - 代表IPSec对SA进行协商；
  - 对SADB数据库进行填充。
- 最终结果：一个通过验证的密钥以及建立在双方同意基础上的安全联盟（IPSec SA）。
- 使用UDP端口500来进行通信

简介

- ISAKMP、Oakelay和SKEME这三个协议构成了IKE的基础。
  - 沿用ISAKMP的信息结构、交换和阶段
  - 借鉴并规范了Oakelay的模式
  - 采用SKEME的密钥更新技术

IKE—Internet密钥交换



- 协商SA：IKE利用ISAKMP语言来定义SA协商和密钥交换需要的信息。
- 生成安全的密钥：通过安全的交换过程实现。

思考：

想想TLS，网络层安全协议与传输层安全协议区别

密钥交互机制的设计要求

IPSEC应如何设计SA协商和密钥交换过程

IKE协议—密钥生成过程

- IKE使用了两个阶段的交换。第一阶段建立IKE的SA；第二阶段利用这个协商好的IKE SA，为IPSec协商具体的SA，对消息提供源验证、完整性以及机密性保护。
- IKE定义了2个阶段一交换，1个阶段二交换。
  - 阶段一的交换：主模式（身份保护交换）；野蛮（积极）模式（野蛮交换）（当使用公共密钥加密来验证时，积极模式仍然提供身份保护）
  - 阶段二的交换：快速模式交换
- 效率：由于使用ISAKMP阶段，实现中可以在需要时完成快速的密钥交换。单个第一阶段协商可以用 于多个第二阶段的协商。而单个第二阶段协商可以请求多个安全联盟。

IKE协议--消息和载荷

- IKE消息的构建：报头+载荷
- 载荷为构造消息提供建筑模块。

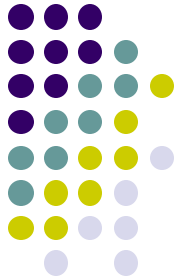
报头

=0 in phase one

Cookie + message ID : identification

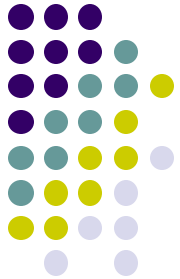
解释

- 发起者和接受者的cookie由通信双方创建，对双方进行验证。
- “下一载荷” ：紧随在头之后的ISAKMP载荷编号。
- 主版本 4比特：1—RFC2408，0—以前
- 次版本4比特：0—RFC2408，1—以前
- 交换类型：交换的具体类型
- 标志字段：ACE
  - E 加密位：1—加密跟随在头后的所有载荷，0—不加密
  - C提交位：用来实现密钥交换的同步
  - A认证位：1—通知载荷只采用认证安全业务，未应用加密业务。



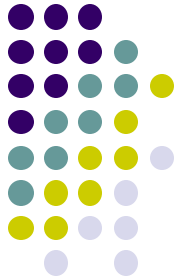
- 需要设计哪些载荷？
  - 满足协议的功能要求：
    - SA协商：内容？
    - 密钥交互：方法？所需材料？
    - 管理，异常处理
  - 安全性要求：
    - 安全威胁
    - 保障方法

IKE协议的安全保护：cookie



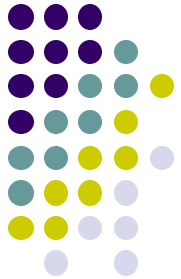
- 为了抵御DOS攻击，密钥交换前先采用cookie交换，以确认对方能收到回应，然后才进行密钥交换和计算。
- Cookie是一些必要信息的HASH值，一般包括双方IP地址、端口号、秘密随机数、日期和时间。特点：
  - 每个cookie绑定于特定通信方IP，攻击者不能把一个cookie用于其他IP。
  - 生成者能验证自己生成的cookie，其他人无法伪造。
  - Cookie生成有足够快的速度。

IKE协议的安全保护：nonce



- 伪随机数nonce在IKE交换中随信息一起发送，在一定程度上防止重播攻击。

IKE协议的安全保护：完整性保护



- IKE协议通过交换验证载荷（包含散列值或数字签名）保护交换消息的完整性，并进行身份认证。

IKE协议--载荷类型

- 共13种载荷。其中14~127保留，128~255私用

载荷类型	值	载荷类型	值
NONE	0	证书请求载荷	7
SA载荷	1	散列载荷	8
建议载荷	2	签名载荷	9
变换载荷	3	nonce载荷	10
密钥交换载荷	4	通知载荷	11
ID载荷	5	删除载荷	12
证书载荷	6	Vendor ID载荷	13

IKE协议--载荷类型

- 散列载荷：一个散列函数的输出结果。
- 签名载荷：一个数字签名。
- Nonce载荷：一些伪随机信息，当前时间。
- 密钥交换载荷（KE）：包含执行一次密钥交换所必须的信息， Diffie-Hellman交换的公共信息。
- 安全联盟载荷（SA）、建议载荷、变换载荷：定义要建立的SA的具体内容。
- 证书请求载荷、证书载荷：请求、交换证书
- 验证载荷：验证信息
- ID载荷：是x的身份识别载荷。x可以是“ii”或“ir”，分别表示第一阶段协商中的ISAKMP发起者和响应者；也可以是“ui”或“ur”，分别表示第二阶段的用户发起者和响应者。

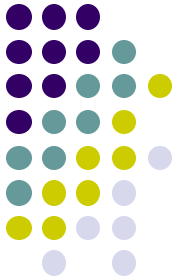
IKE载荷链接形成消息

发起者cookie				
响应者cookie				
KE	主版本	副版本	交换类型	标志
消息ID				
消息长度				
NONCE	0		KE载荷长度	
KE载荷				
0	0		NONCE载荷长度	
NONCE载荷				

SA载荷、建议载荷与变换载荷
—通过构造消息进行SA策略协商

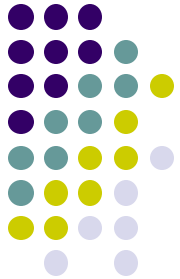
NONCE	保留	载荷长度	
解释域DOI			
情境（situation）			
proposal	保留	载荷长度	
建议编号=1	协议ID	SPI大小	变换数=2
SPI（可变）			

transfer	保留	载荷长度
变换编号=1	变换ID	保留
SA属性		
0	保留	载荷长度
变换编号=2	变换ID	保留
SA属性		



0	保留	载荷长度	
建议编号=1	协议ID	SPI大小	变换数=1
SPI（可变）			
Transfer	保留	载荷长度	
变换编号=1	变换ID	保留	
SA属性			

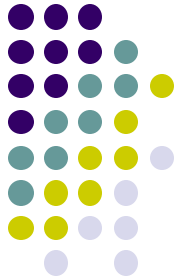
？通信双方在一个不安全的网络中如何协商生成一个密钥？



- 复习传输层TLS的机制，不同之处？如何设计IPSEC的密钥交换？效率，安全
- 算法：

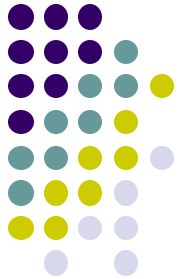
IKE协议采用D-H算法生成第一阶段IKE SA的密钥

IKE协议的安全保护：身份验证



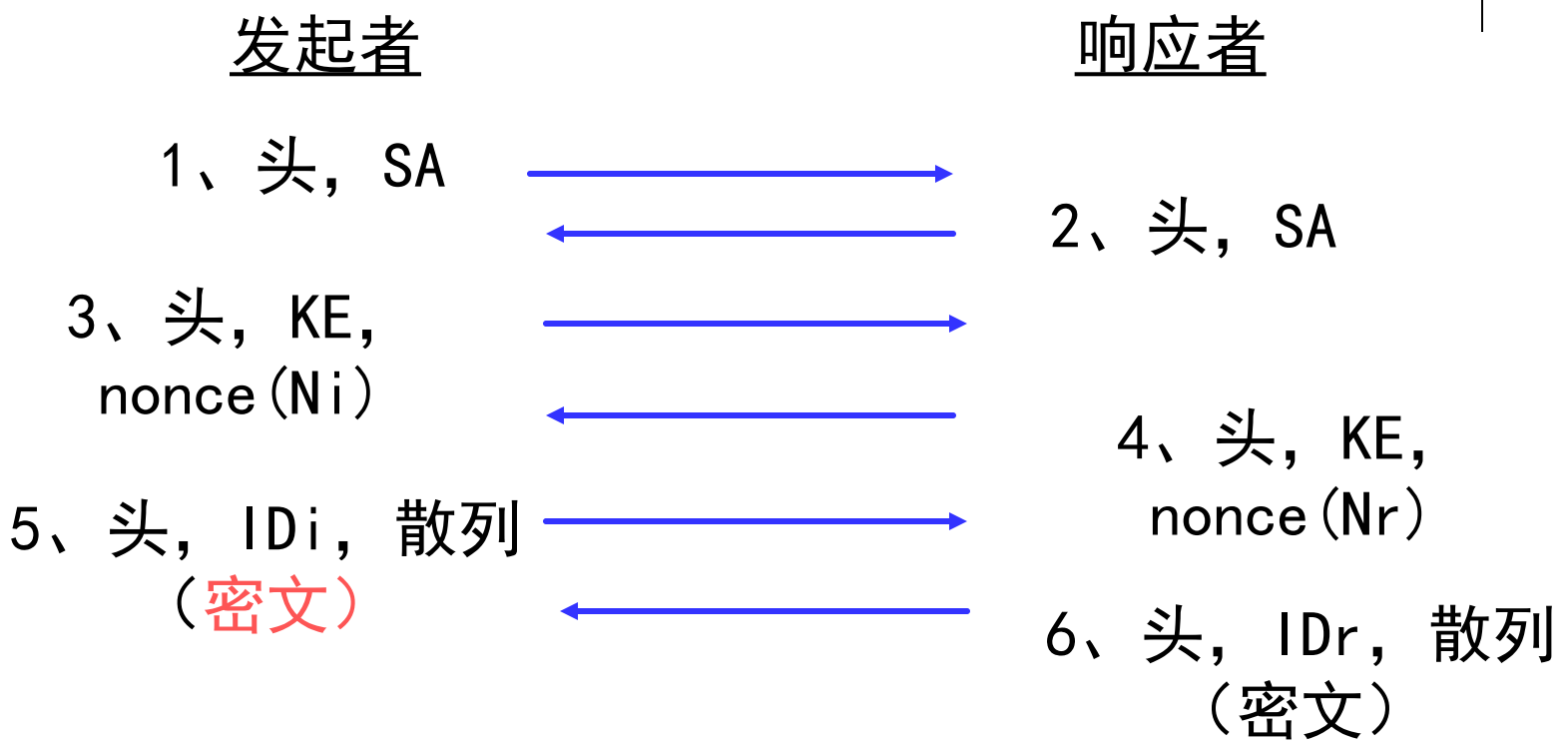
- 主模式或积极模式中都允许四种不同的验证方法
  - 预共享密钥
  - 公钥签名认证方式
  - 公钥加密的认证方式
  - 改进的公钥加密认证方式

IKE协议第一阶段--主模式交换



- 主模式包括三个步骤，用到六条消息。
- 三个步骤：
  - 模式协商
  - 一次Diffie-Hellman交换和一次nonce交换
  - 对对方身份的验证
- 特点：身份保护以及对ISAKMP协商能力的完全利用。

随预共享密钥使用的主模式：



SKEYID = prf(pre-shared-key, Ni_b | Nr_b)

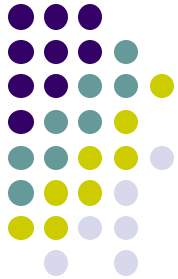
_b指：载荷的数据部分，不包括IKE通用头

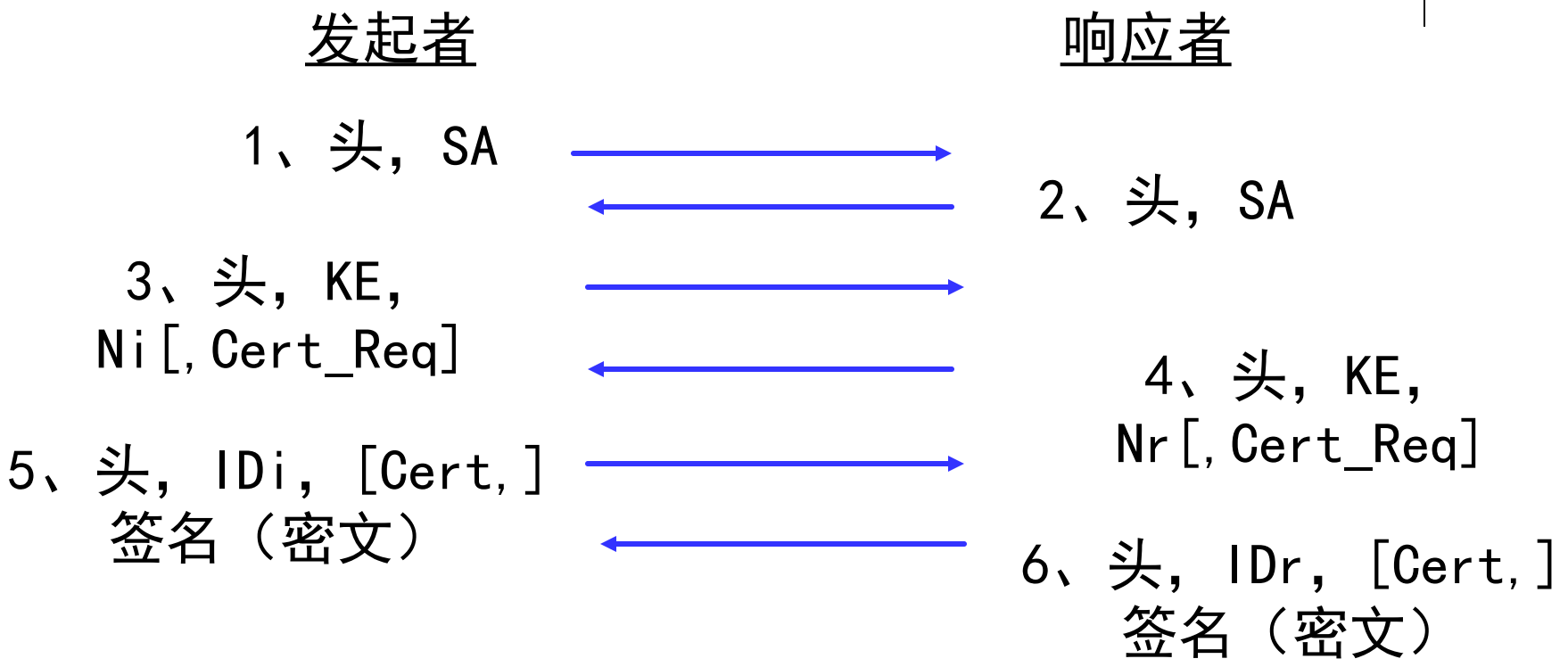
前提：已知双方IP

HASH的计算方法：

- 为了验证交换中的双方，协议的发起者产生HASH_I，响应者产生HASH_R，其中：
  - HASH_I = prf(SKEYID, g^xi | g^xr | CKY-I | CKY-R | SAi_b | IDi_b)
  - HASH_R = prf(SKEYID, g^xr | g^xi | CKY-R | CKY-I | SAi_b | IDr_b)
    - SAi_b是SA的数据部分（除去通用报头）也就是由发起者所提供的DOI、 situation,所有的proposal、所有的transform。
    - IDi_b就ID的数据部分（ID类型，端口， 协议）
    - CKY-I和CKY-R分别是发起者和响应者的cookie。
    - g^xi和g^xr分别是DH中发起者和响应者的公共值。
- 对于使用数字签名的验证，HASH_I和HASH_R是经过签名并效验的；对于使用公共密钥加密 验证或共享密钥的验证，HASH_I和HASH_R直接验证交换。

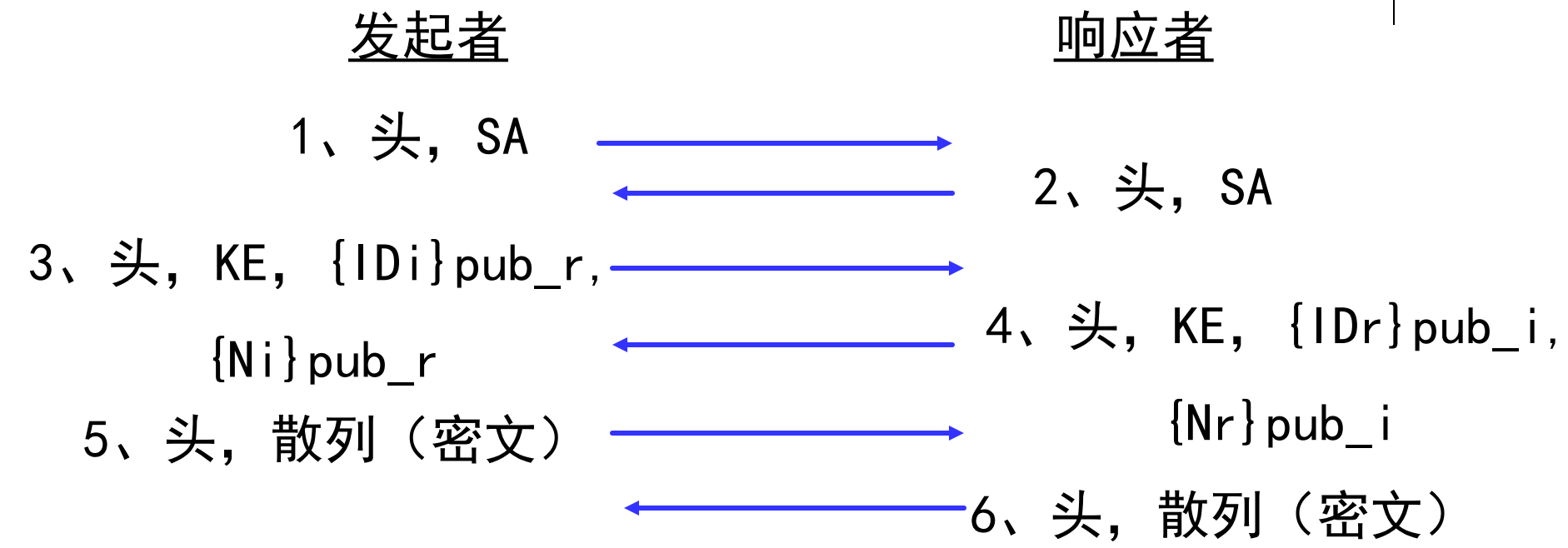
随公共密钥签名使用的主模式：





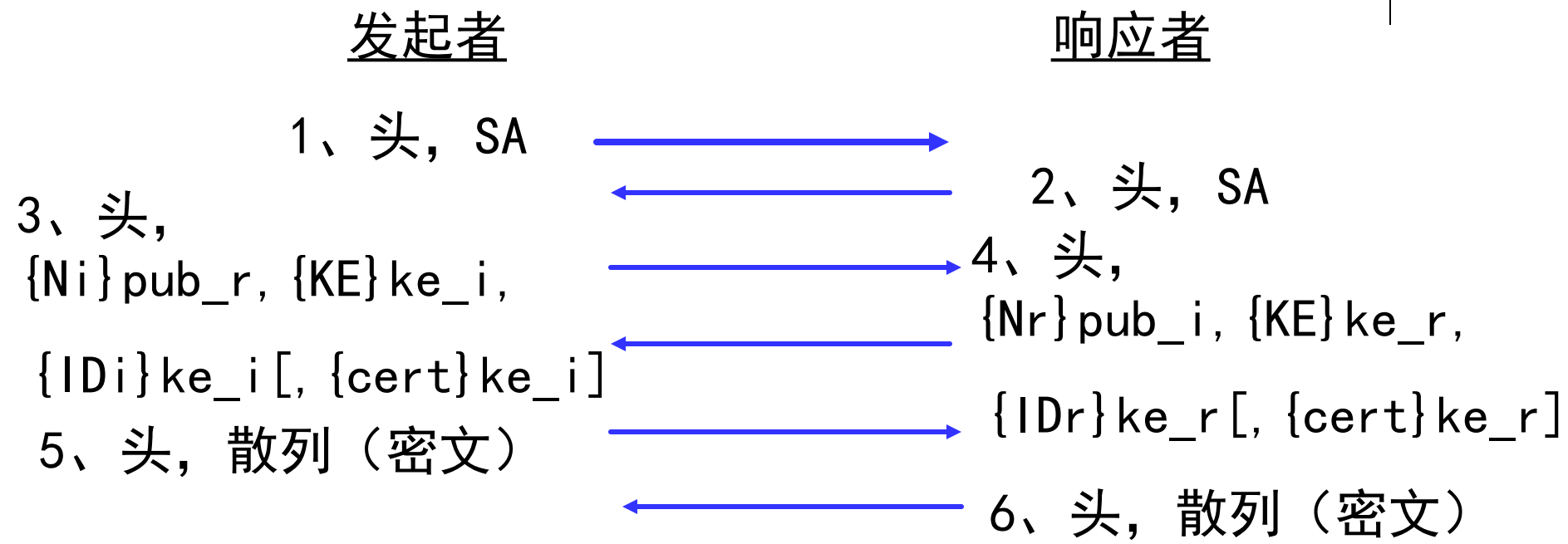
SKEYID = prf(Ni_b | Nr_b, g^xy)

公共密钥加密的标准方法

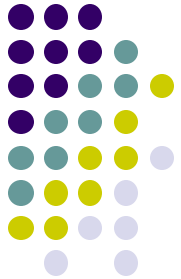


SKEYID = prf(hash(Ni_b | Nr_b), CKY-I | CKY-R)

公共密钥加密的修订方法

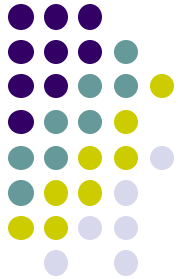


双方的身份（以及证书） 使用协商的对称加密算法（从SA负载中获得）来加密，其密钥是从当前时间（nonce）中衍生而来。



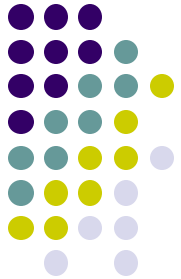
- 对称加密密钥是从解密的当前时间（nonce）中衍生出来的
  - Ne_i = prf(Ni_b, CKY-I)
    Ne_r = prf(Nr_b, CKY-R)
  - K = K1 | K2 | K3 and
    K1 = prf(Ne_i, 0)
    K2 = prf(Ne_i, K1)
    K3 = prf(Ne_i, K2)
  - …..

IKE协议第一阶段—积极模式交换



- 用途：建立一个验证的SA和密钥，随后可以用它为其他安全协议建立SA。
- 与主模式的差别：只用到主模式一半的消息；限制了消息的数量；限制了协商能力，不提供身份保护。
- 交换过程：
  - 发起者在第一条消息里提供一个保护套件列表、Diffie-Hellman公共值、nonce以及身份资料。
  - 接受者回复一个选定的保护套件列表、Diffie-Hellman公共值、nonce、身份资料以及一个验证载荷（预共享密钥和加密的nonce验证--散列载荷；基于签名的验证—签名载荷）。
  - 发起者回答一个验证载荷。

例：使用签名的积极模式



HDR, SA, KE, Ni, IDii

-->

<--

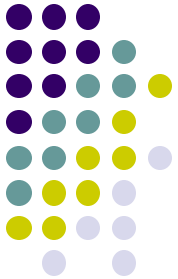
HDR, SA, KE, Nr, IDir, [CERT,]
SIG_R

HDR, [CERT,] SIG_I

-->

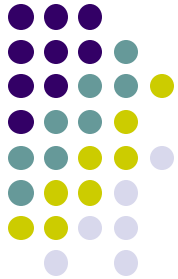
<--

为什么用积极模式交换？



- 积极模式交换功能非常有限。
- 为什么使用？
  - 在需要进行远程访问的时候，由于发起者的地址不可能被响应者提前知道，而且双方都打算使用预共享密钥验证方法，要建立IKE SA，这是唯一可行的交换方式。
  - 如果发起者已经对策略有非常全面的理解，能更快速地创建IKE SA。

IKE协议第二阶段--快速模式交换



- 建立好IKE SA之后，可以用它为其他安全协议（IPSec）生成相应的SA。
- 在一次快速模式交换中，通信双方需要协商拟订IPSec SA的各项特征，并生成密钥。
- IKE SA保护快速模式交换的方法：对其进行加密，并对消息进行验证。
- 快速模式交换的信息：SA，nonce，可选的Diffie-Hellman公共值，身份信息。

快速模式交换

发起者　　响应者

1、头，散列1，SA，
Ni[,KE][,IDci,IDcr]
（密文）

2、头，散列2，SA，
Nr[,KE][,IDci,IDcr]
（密文）

3、头，散列（密文）

快速模式交换中信息的安全性完全依赖

第一阶段产生的IKE SA保护！

IPSec的应用

- 端到端的安全保护：
  - 好处：
  - 问题：

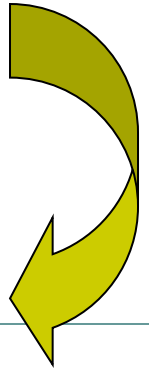
    无法识别要传送的是何种包，防火墙、QOS等

    IPSEC　VPN 配置复杂

    对动态地址支持依赖厂家们的解决方案

例：

- 设置扩展ACL，表明对哪些数据施行IPSEC
- 在安全集配置模式下：创建或修改安全转换集
- 安全策略修改模式，配置创建或修改安全策略
- 在隧道入口（出口）对应的端口上应用安全策略
- 在全局配置模式下开启/关闭ipsec功能



```
设置安全策略的加密访问控制列表
        match address access-list-id
设置安全策略的对端
                set peer ip-address
设置安全策略的安全转换集
                set transform-set transform-set-name
设置安全策略的各个密钥
                set session-key {inbound|outbound} {ah spi hex-key-string |
esp spi cipher hex-key-string [authenticator hex-key-string]}
```

例:

```
access-list 101 permit ip host 10.1.1.23 host 10.1.2.29
access-list 101 deny   ip any any

crypto ipsec transform-set myset1 ah-md5-hmac
mode tunnel

crypto map mymap1 1 ipsec-manual
set transform-set myset1
set session-key i ah 256 0123456789abcdef0123456789abcdef
set session-key o ah 256 fedcba9876543210fedcba9876543210
set peer 63.12.10.3
match address 101
```