第14章 VPN技术

一 VPN的基本概念和分类

二 PPTP、IPSec、TLS等隧道协议

三 IPSec VPN的原理及应用

四 TLS VPN的原理及应用

五 PPTP VPN的原理及应用

六 MPLS VPN的原理及应用

第14章 VPN技术

一 VPN的基本概念和分类

二 PPTP、IPSec、TLS等隧道协议

三 IPSec VPN的原理及应用

四 TLS VPN的原理及应用

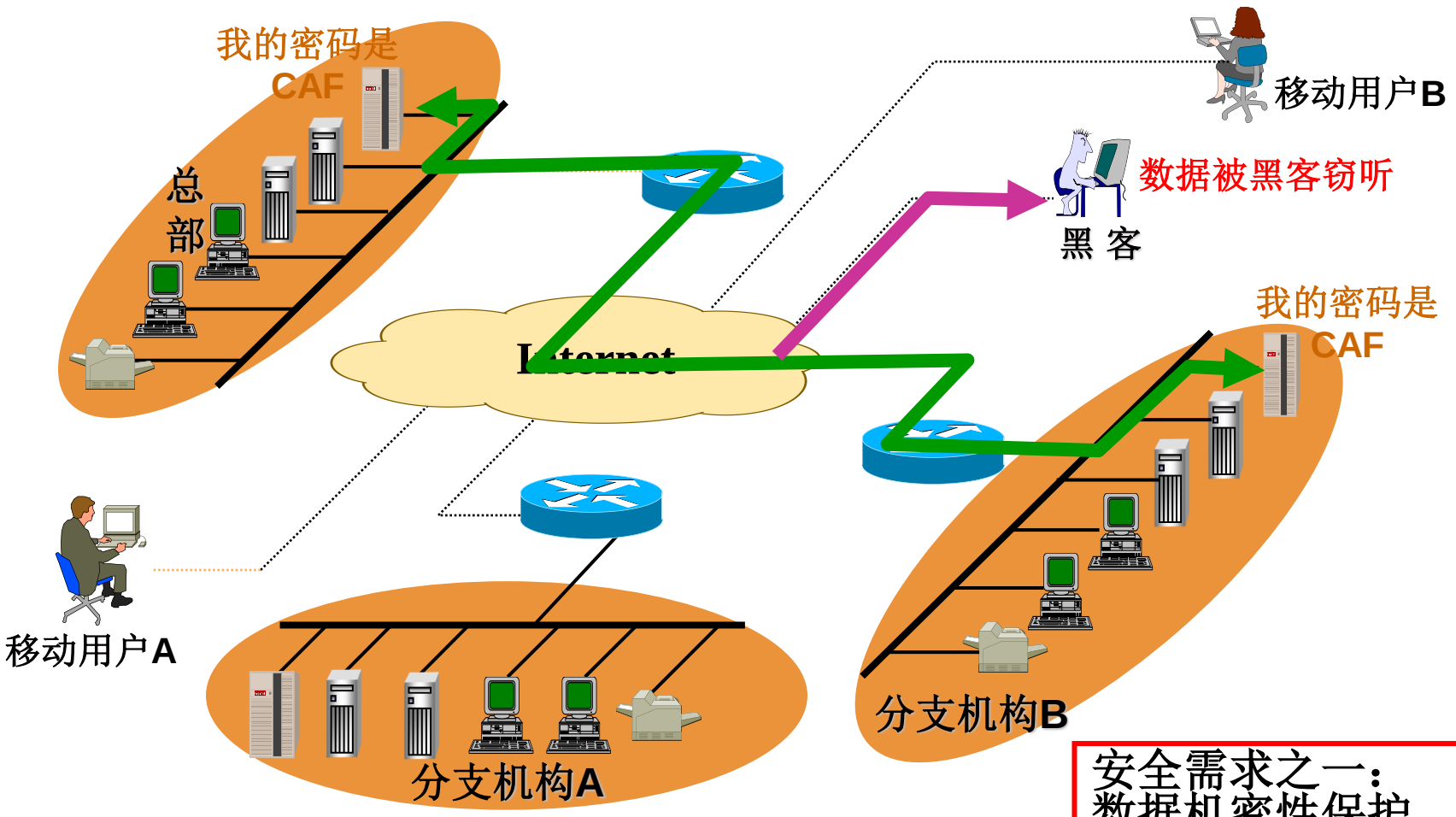
五 PPTP VPN的原理及应用

六 MPLS VPN的原理及应用

信息传输中存在的安全问题

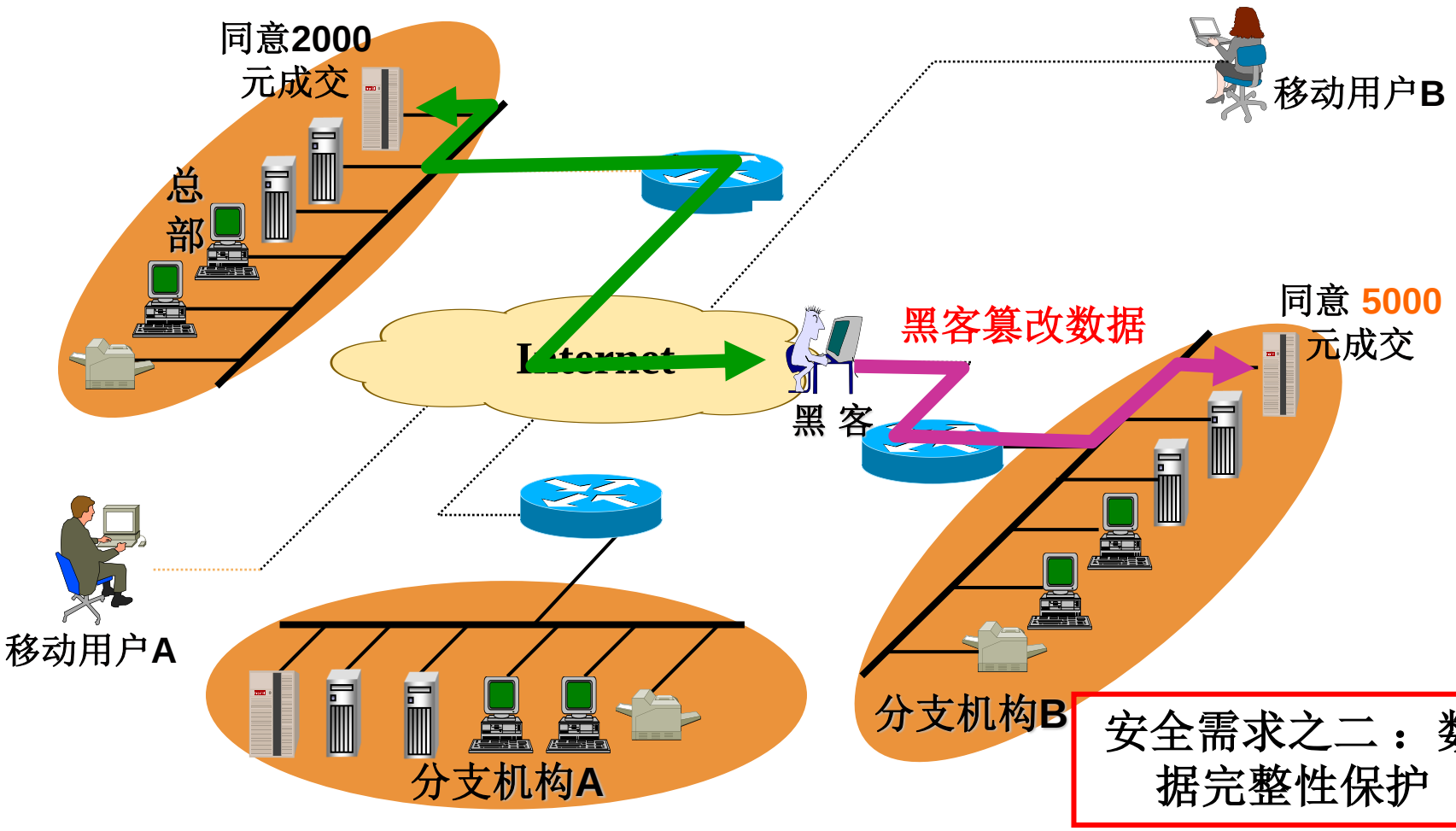
- 信息在传输中可能泄密
- 信息在传输中可能失真
- 信息的来源可能是伪造的
- 信息传输的成本可能很高

信息在传输中可能泄密

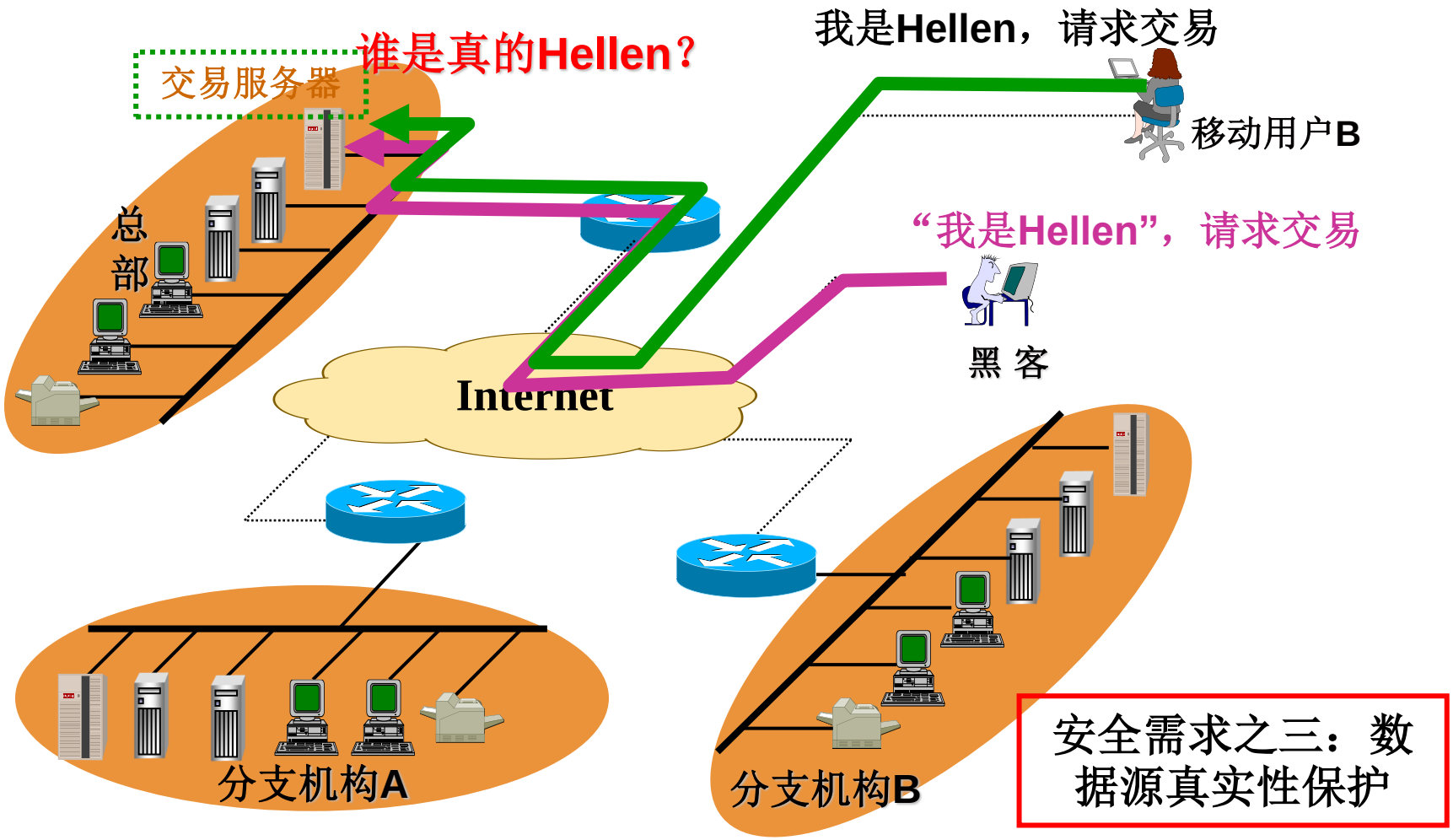


安全需求之一：
数据机密性保护

信息在传输中可能失真

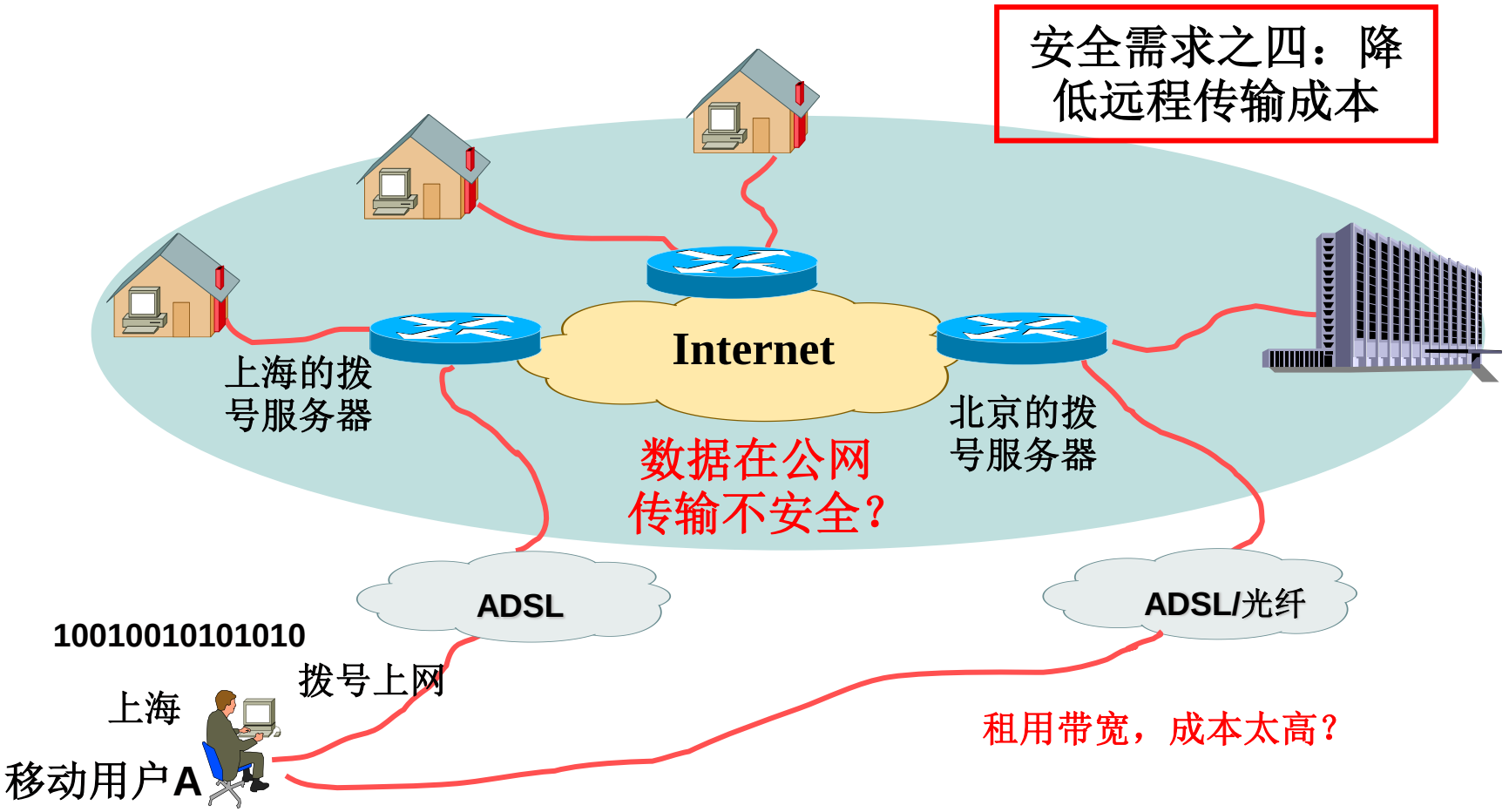

同意2000
元成交
总
部
移动用户B
Internet
黑客篡改数据
黑 客
同意 5000
元成交
移动用户A
分支机构A
分支机构B
安全需求之二：数据完整性保护

信息的来源可能是伪造的



安全需求之三：数据源真实性保护

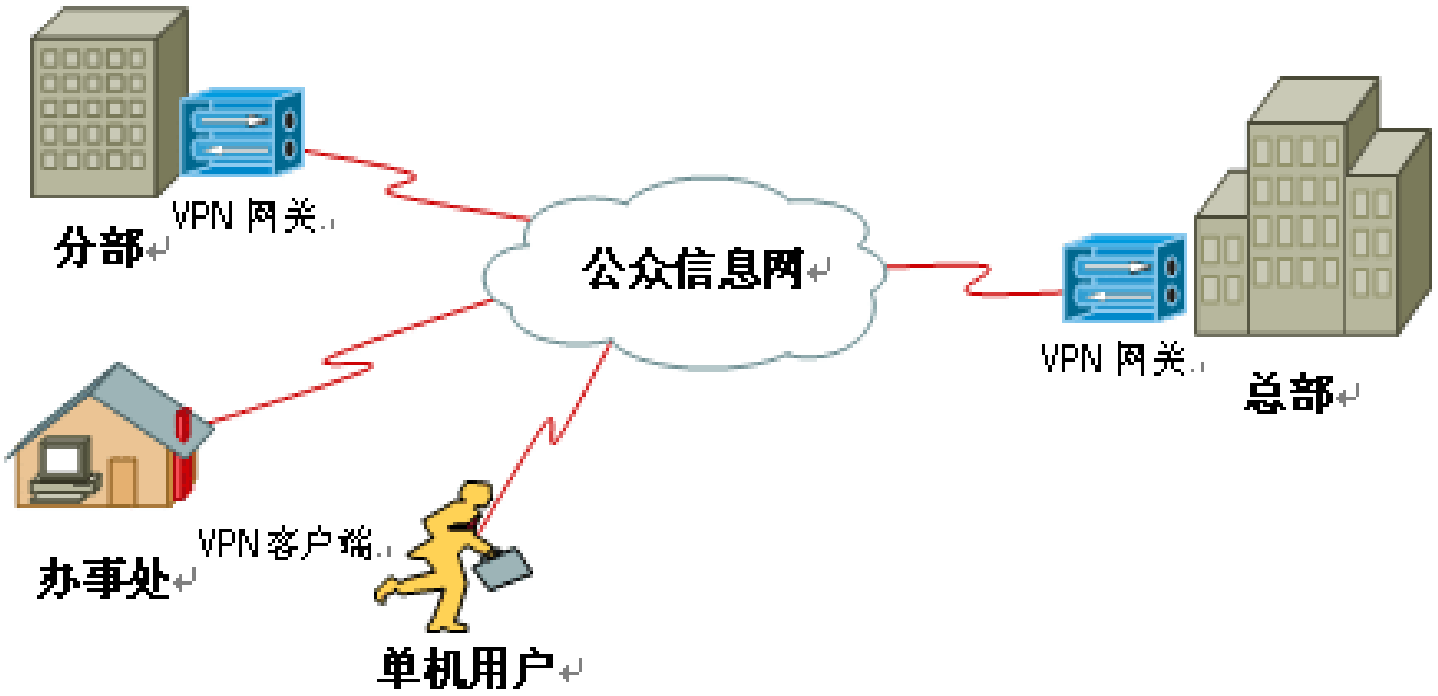
信息传输的成本可能很高



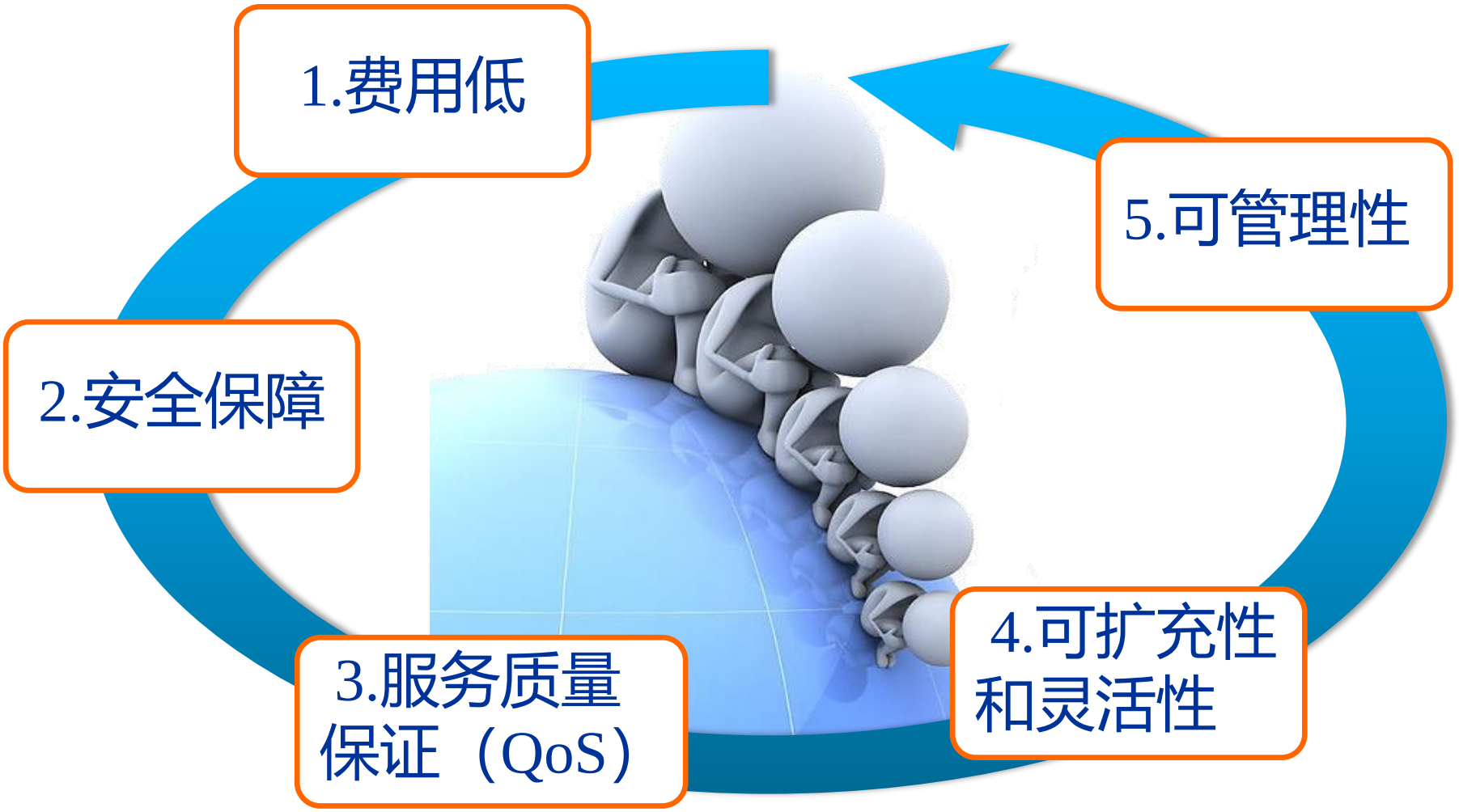
14.1.1 VPN的概念

虚拟专网： VPN (**V**irtual **P**rivate **N**etwork)

- 定义：是指将物理上分布在不同地点的网络通过公用网络连接而构成逻辑上的虚拟子网。



14.1.2 VPN的特点



14.1.3 VPN的分类

① 网关-网关VPN

网关-网关VPN连接

② 远程访问VPN

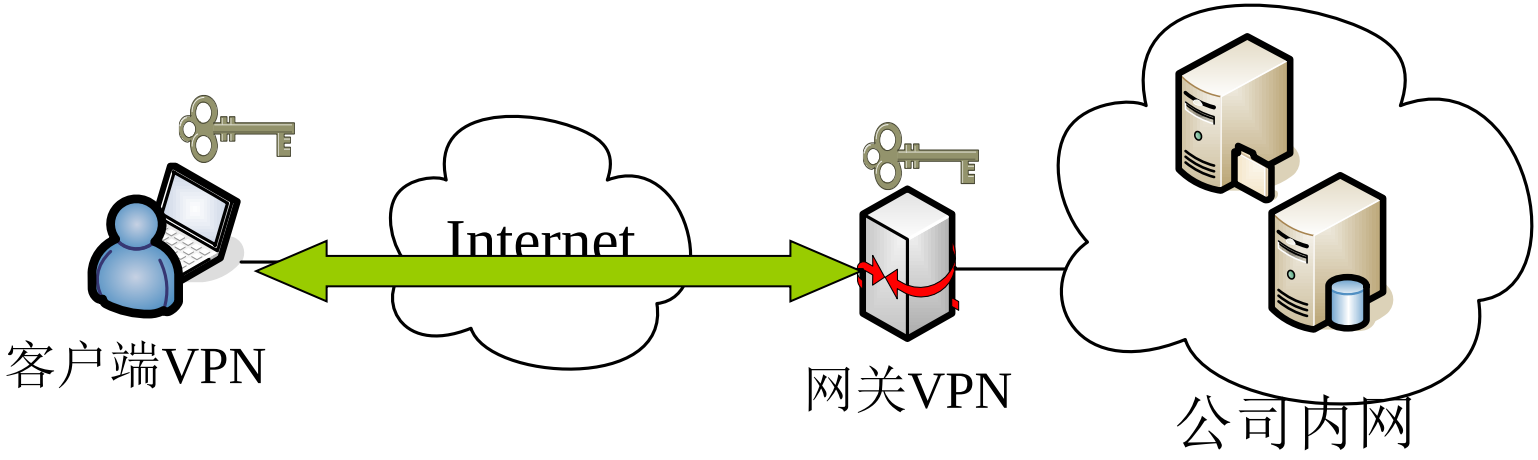
移动用户远程访问VPN

14.1.3 VPN的分类

- Access VPN（远程访问VPN）
- 网关-到网关VPN
  - Intranet VPN（企业内部VPN）
  - Extranet VPN（企业扩展VPN）

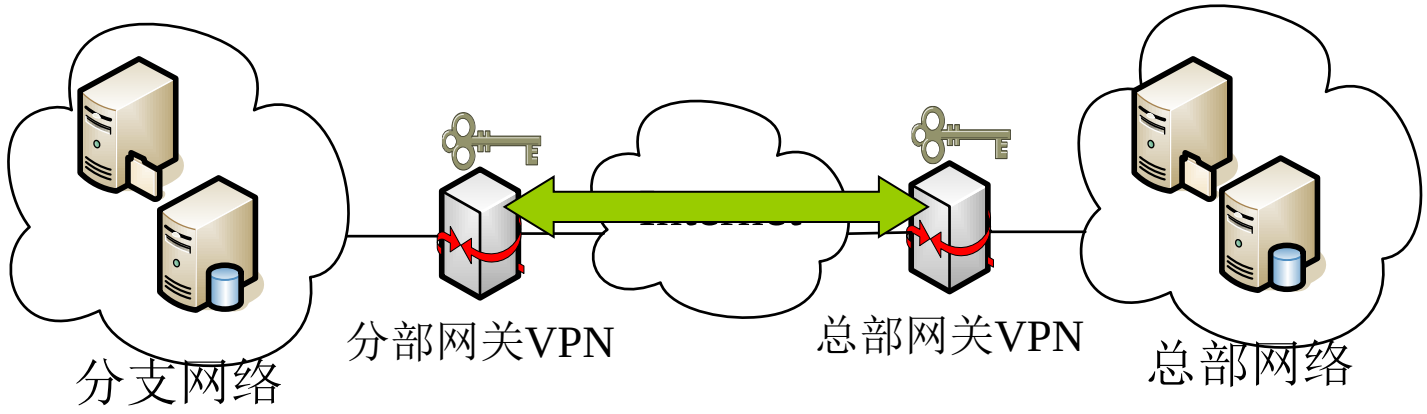
1. Access VPN

- Access VPN与传统的远程访问网络相对应。
- 远端用户只要能使用合法IP地址访问Internet，接入到远端网关即可、可以利用VPN系统在公众网上建立一个**从客户端到网关**的安全传输通道。
- 降低了长途电话，租用光纤及技术支持的费用。
- 适用于企业内部人员流动频繁或远程办公的情况。



2. Intranet VPN

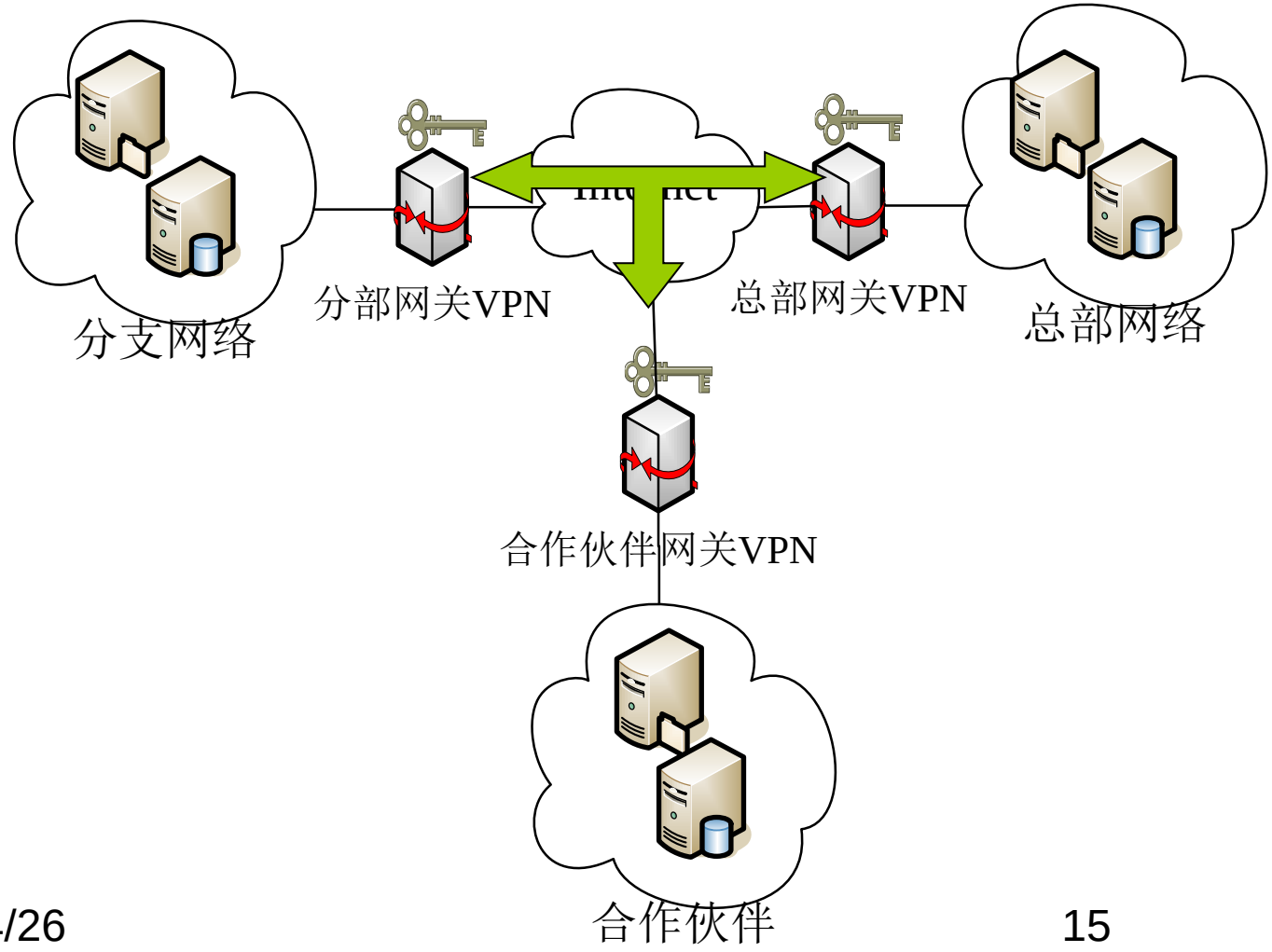
- 如果要进行企业内部异地分支机构的互联，可以使用Intranet VPN方式，这是所谓的**网关对网关VPN**。
- Intranet VPN在异地两个网络的网关之间建立了一个加密的VPN隧道，两端的内部网络可以通过该VPN隧道安全地进行通信，就好像和本地网络通信一样。



3. Extranet VPN

- 如果一个企业希望将客户、供应商、合作伙伴或兴趣群体连接到企业内部网，可以使用Extranet VPN。
- Extranet VPN其实也是一种**网关对网关的VPN**，与Intranet VPN不同的是，它需要在不同企业的内部网络之间组建，需要有**不同协议和设备之间的配合和不同的安全配置**。

Extranet VPN示意图



14.1.4 VPN的关键技术

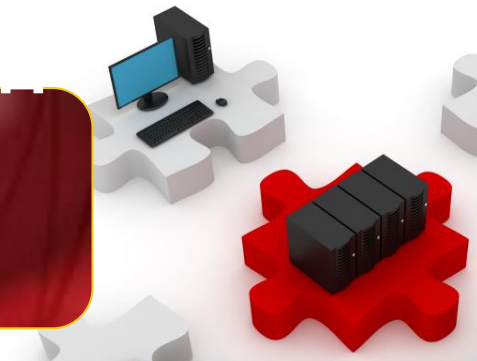
1.隧道技术

2.密码技术

3.密钥管理技术

4.身份认证技术

5.访问控制



VPN技术

1. 密码技术

- 密码技术是实现VPN的关键核心技术之一。
- 一般情况下，在VPN实现中：
  - 双方**大量的通信流量的加密使用对称加密算法**，运算量小、速度快。众多算法中最常用的是DES（Data Encryption Standard）、AES（Advanced Encryption Standard）和IDEA（International Data Encryption Algorithm）
  - 而**在管理、分发对称加密的密钥上采用更加安全的非对称加密技术。**

VPN技术

2. 身份认证技术

- VPN需要解决的首要问题就是网络上用户与设备的身份认证。
- 从技术上说，身份认证基本上可以分为两类：非PKI体系和PKI体系的身份认证。
  - 非PKI体系：UID+PASSWORD
    - PAP，Password Authentication Protocol，口令认证协议
    - CHAP，Challenge Handshake Authentication Protocol，挑战握手认证协议
    - MS CHAP，Microsoft Challenge Handshake Authentication Protocol，微软CHAP
    - RADIUS，Remote Authentication Dial In User Service，远程认证拨号用户服务

VPN技术

- PKI体系
  - 常用的方法是依赖于CA（Certificate Authority，数字证书签发中心）所签发的符合X.509规范的标准数字证书。
  - 通信双方交换数据前，需先确认彼此的身份，交换彼此的数字证书，双方将用此证书进行比较，只有比较结果正确，双方才开始交换数据；否则，不能进行后续通信。

VPN技术

3. 隧道技术

- 隧道技术通过对数据进行封装，在公共网络上建立一条数据通道（隧道），让数据包通过这条隧道传输。
- 生成隧道的协议有三种：第二层隧道协议、第三层隧道协议、第四层隧道协议。

第二层隧道协议

- 第二层隧道协议是在数据链路层进行的，先把各种网络协议封装到PPP包中，再把整个数据包装入隧道协议中，这种经过两层封装的数据包由第二层协议进行传输。
  - L2F（RFC 2341，Layer 2 Forwarding）；
  - PPTP（RFC 2637，Point to Point Tunneling Protocol）；
  - L2TP（RFC 2661，Layer Two Tunneling Protocol）。
- 采用L2TP还是PPTP实现VPN取决于要把控制权放在NAS(Network Access Server)还是用户手中。
- L2TP比PPTP更安全，因为L2TP接入服务器能够确定用户从哪里来。L2TP主要用于比较集中的、固定的VPN用户，而PPTP比较适合移动的用户。

第三层隧道协议

- 在网络层进行的，把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。
  - **IPSec（IP Security），是目前最常用的VPN解决方案；**
  - GRE(RFC 2784, General Routing Encapsulation)。
    - **GRE主要用于源路由和终路由之间所形成的隧道。**例如，将通过隧道的报文用一个新的报文头（GRE报文头）进行封装然后带着隧道终点地址放入隧道中。当报文到达隧道终点时，GRE报文头被剥掉，继续根据原始报文的目标地址进行寻址。
    - **GRE隧道技术是用在路由器中**的，可以满足Extranet VPN以及Intranet VPN的需求。

第四层隧道协议

- 工作在传输层，把网络层数据包或应用数据装入隧道协议中，形成的数据包依靠传输层协议进行传输
  - TLS（Transport Layer Security）：传输层安全性协议
  - TLS/SSL VPN 主要为远程访问VPN（Access-VPN）

VPN技术

4. 密钥管理技术

- 在VPN应用中密钥的分发与管理非常重要。密钥的分发有两种方法：
  - 手工配置：要求密钥更新不要太频繁，否则管理工作量太大，因此只适合于简单网络的情况。
  - 采用密钥交换协议**动态分发**：采用软件方式动态生成密钥，保证密钥在公共网络上安全地传输而不被窃取，适合于复杂网络的情况，而且密钥可快速更新，可以显著提高VPN应用的安全性。

VPN技术

5. 访问控制技术

- 访问控制决定了谁能够访问系统、能访问系统的何种资源以及如何使用这些资源。
- 采取适当的访问控制措施能够阻止未经允许的用户有意或无意地获取数据，或者非法访问系统资源等。

第14章 VPN技术

一 VPN的基本概念和分类

二 PPTP、IPSec、TLS等隧道协议

三 IPSec VPN的原理及应用

四 TLS VPN的原理及应用

五 PPTP VPN的原理及应用

六 MPLS VPN的原理及应用

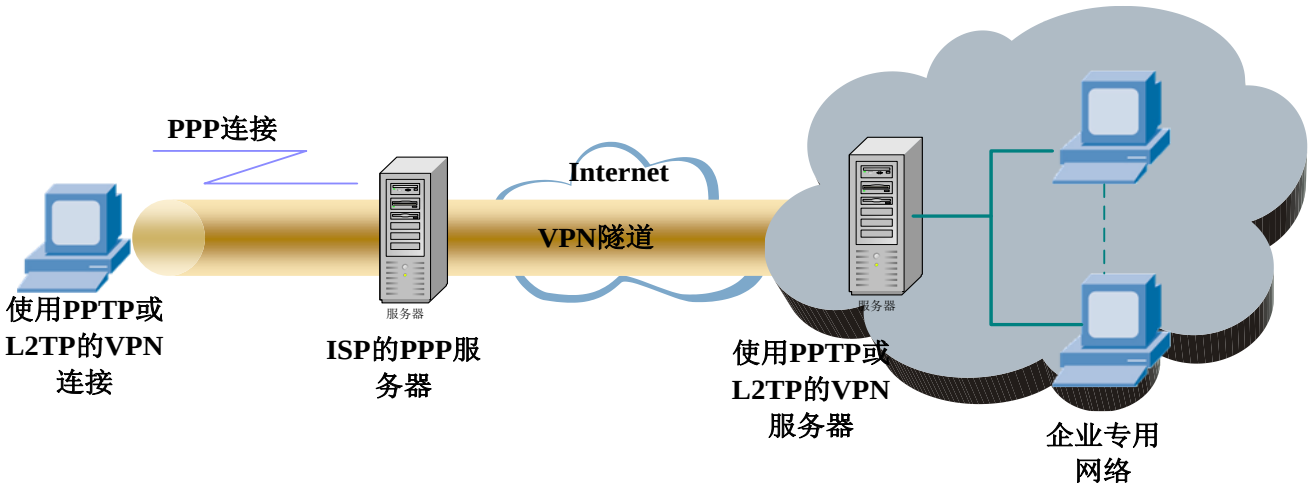
14.2 隧道协议与VPN

定义：

- 指通过一个公用网络（通常是Internet）建立的一条穿过公用网络的安全的、逻辑上的隧道。
- 在隧道中，数据包被重新封装发送。

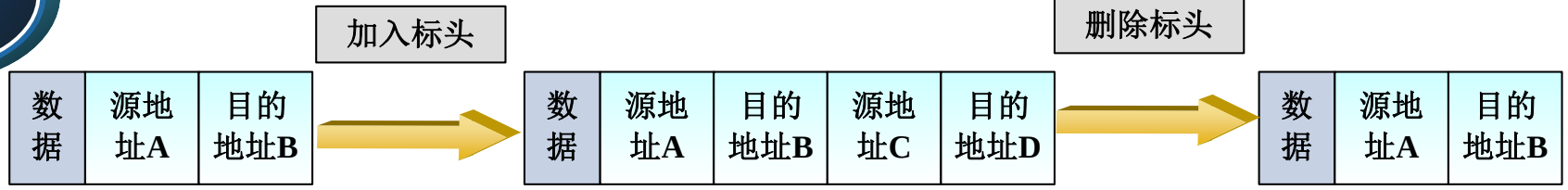
VPN的主要封装协议：

- 第2层的隧道协议
  --包括PPTP、L2TP、L2F等；
- 第3层的隧道协议
  --包括IPSec、GRE等
- 第4层的隧道协议
  --包括SSL、TLS等。

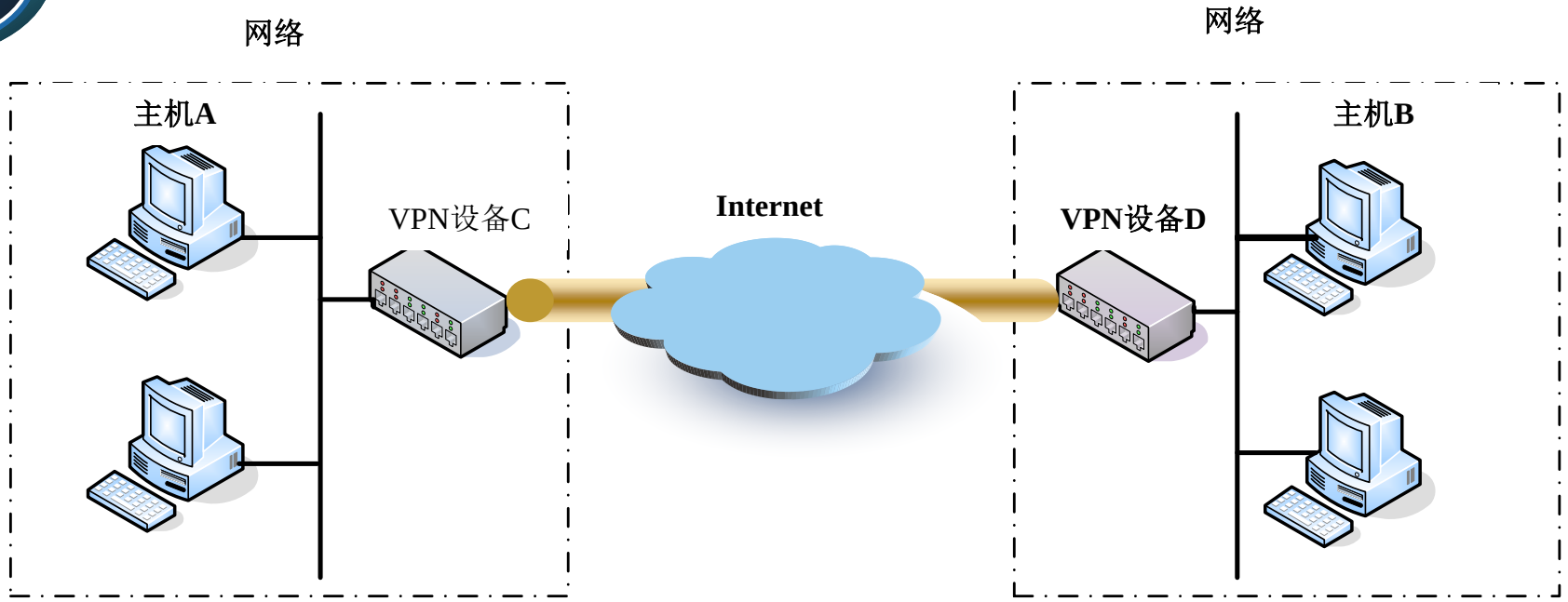


数据包在隧道中的封装及发送过程

封装



发送



14.2.1 第二层隧道协议

PPTP

- 让远程用户拨号连接到本地ISP、通过Internet安全远程访问公司网络资源。
- PPTP具有两种不同的工作模式，即被动模式和主动模式。

L2F

- 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。
- 它将链路层的协议（如HDLC，PPP，ASYNC等）封装起来传送

L2TP

- 在上述两种协议的基础上产生。
- 适合组建远程接入方式的VPN。

14.2.1 第二层隧道协议

优点

- 简单易行

缺点

- 可扩展性都不好
- 不提供内在的安全机制，不能保证企业和企业的外部客户及供应商之间会话的保密性。

14.2.2 第三层隧道协议

IPSec

- 专为IP设计提供安全服务的一种协议。

GRE
--Generic Routing Encapsulation

- 规定了如何用一种网络协议去封装另一种网络协议的方法。

MPLS
--Multiprotocol Label Switching

- 引入了基于标记的机制。
- 它把选路和转发分开，用标签来规定一个分组通过网络的路径。

第14章 VPN技术

一 VPN的基本概念和分类

二 PPTP、IPSec、TLS等隧道协议

三 IPSec VPN的原理及应用

四 TLS VPN的原理及应用

五 PPTP VPN的原理及应用

六 MPLS VPN的原理及应用

14.3.1 IP安全概述

- 大型网络系统内运行多种网络协议（TCP/IP、IPX/SPX和NETBEUA等），这些网络协议并非为安全通信设计。
- IP协议维系着整个TCP/IP协议的体系结构，除了数据链路层外，TCP/IP的所有协议的数据都是以IP数据报的形式传输的。
- TCP/IP协议簇有两种IP版本：版本4（IPv4）和版本6（IPv6）。IPv6简化了IP头，其数据报更加灵活，同时IPv6还增加了对安全性的考虑。

IP安全的必要性

- IPv4在设计之初没有考虑安全性，导致在网络上传输的数据很容易受到各式各样的攻击：比如伪造IP包地址、修改其内容、重播以前的包以及在传输途中拦截并查看包的内容等。因此，通信双方不能保证收到IP数据报的真实性。
- 为了加强因特网的安全性，从1995年开始，IETF着手制定了一套用于保护IP通信的IP安全协议（IP Security，IPSec）。IPSec弥补了IPv4在协议设计时缺乏安全性考虑的不足。

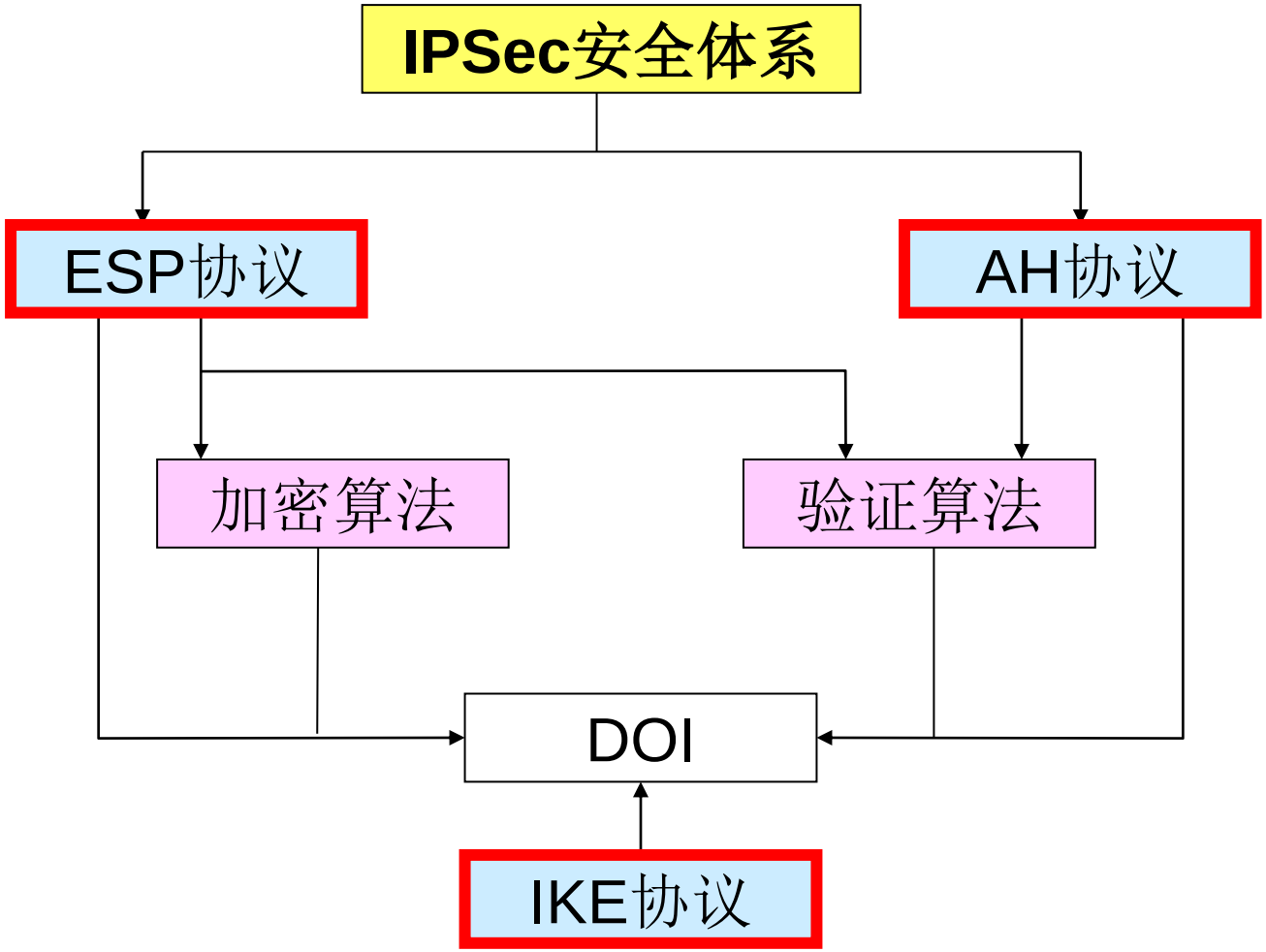
IPSec安全体系结构

- IPSec（IP Security）是一种由IETF设计的端到端的确保**IP层通信安全**的机制。
- IPSec不是一个单独的协议，而**是一组协议**，IPSec协议的定义文件包括了12个RFC文件和几十个Internet草案，已经成为工业标准的网络安全协议。
- IPSec在IPv6中是必须支持的，而在IPv4中是可选的。

IPSec协议族相关的RFC

RFC	内容
2401	IPSec体系结构
2402	AH（Authentication Header）协议
2403	HMAC-MD5-96在AH和ESP中的应用
2404	HMAC-SHA-1-96在AH和ESP中的应用
2405	DES-CBC在ESP中的应用
2406	ESP（Encapsulating Security Payload）协议
2407	IPSec DOI
2408	ISAKMP协议
2409	IKE（Internet Key Exchange）协议
2410	NULL加密算法及在IPSec中的应用
2411	IPSec文档路线图
2412	OAKLEY协议

IPSec体系结构图



IPSec协议簇

- IPSec协议簇主要包括两个安全协议：AH协议和ESP协议。
  - AH协议（Authentication Header，验证头）：可以进行数据源身份验证、保障数据的完整性以及防止相同数据包在因特网重放。
  - ESP协议（Encapsulating Security Payload，封装安全载荷）：具有所有AH的功能，还可以利用加密技术保障数据机密性。
- 虽然AH和ESP都可以提供身份认证，但它们有2点区别：
  - ESP要求使用高强度的加密算法，会受到许多限制。
  - 多数情况下，使用AH的认证服务已能满足要求，相对来说，ESP开销较大。

IPSec协议簇

- 有两套不同的安全协议意味着可以对IPSec网络进行更细粒度的控制，选择安全方案可以有更大的灵活度。
- **AH和ESP可以单独使用，也可以组合使用，**可以在两台主机、两台安全网关（防火墙和路由器），或者主机与安全网关之间使用。

IKE（Internet Key Exchange）

- IKE协议**负责密钥管理**，定义了通信实体间进行身份认证、协商加密算法以及生成共享的会话密钥的方法。
- IKE将密钥协商的结果保留在安全联盟（SA）中，供AH和ESP以后通信时使用。

DOI（Domain of Interpretation ）

- 解释域DOI定义IKE所没有定义的协商的内容；
- DOI为使用IKE进行协商SA的协议**统一分配标识符**。共享一个DOI的协议从一个共同的命名空间中选择安全协议和变换、共享密码以及交换协议的标识符等。
- DOI将IPSec的这些RFC文档联系到一起。

IPSec的功能

- 作为一个隧道协议实现了VPN通信
  - 第三层隧道协议，可以在IP层上创建一个安全的隧道，使两个异地的私有网络连接起来，或者使公网上的计算机可以访问远程的企业私有网络。
- 保证数据来源可靠
  - 在IPSec通信之前双方要先用IKE认证对方身份并协商密钥，只有IKE协商成功之后才能通信。
  - 由于第三方不可能知道验证和加密的算法以及相关密钥，因此无法冒充发送方，即使冒充，也会被接收方检测出来。

IPSec的功能

- 保证数据完整性
  - IPSec通过**验证算法**保证数据从发送方到接收方的传送过程中的任何数据篡改和丢失都可以被检测。
- 保证数据机密性
  - IPSec通过**加密算法**使只有真正的接收方才能获取真正的发送内容，而他人无法获知数据的真正内容。

有关术语

- SA（Security Association，安全关联）
- SAD（Security Association Database，安全关联数据库）
- SP（Security Policy，安全策略）
- SPD（Security Policy Database，安全策略数据库）

SA（Security Association，安全关联）

- SA（Security Association，安全关联）
  - **是两个IPSec实体（主机、安全网关）之间经过协商建立起来的一种协定。**
  - 内容包括采用何种IPSec协议（AH还是ESP）、运行模式（传输模式还是隧道模式）、验证算法、加密算法、加密密钥、密钥生存期、抗重放窗口、计数器等，从而决定了保护什么、如何保护以及谁来保护。
  - 可以说SA是构成IPSec的基础。

SA（Security Association，安全关联）

- 每个SA由三元组（SPI，IP目的地址，IPSec协议）来唯一标识
  - SPI（Security Parameter Index，安全参数索引）是32位的安全参数索引，**用于标识具有相同IP地址和相同安全协议的不同的SA，**它通常被放在AH或ESP头中 。
  - IP目的地址：它是SA的终端地址。
  - IPSec协议：采用AH或ESP。
- **SA是单向**的，在一次通信中，IPSec 需要建立两个SA，一个用于入站通信，另一个用于出站通信。

SAD（Security Association Database，安全关联数据库）

- SAD并不是通常意义上的“数据库”，而是**将所有的SA以某种数据结构集中存储的一个列表。**
- 对于外出的流量，如果需要使用IPSec处理，然而相应的SA不存在，则IPSec将启动IKE来协商出一个SA，并存储到SAD中。
- 对于进入的流量，如果需要进行IPSec处理，IPSec将从IP包中得到三元组（SPI,DST,Protocol），并利用这个三元组在SAD中查找一个SA。

SP（Security Policy）安全策略

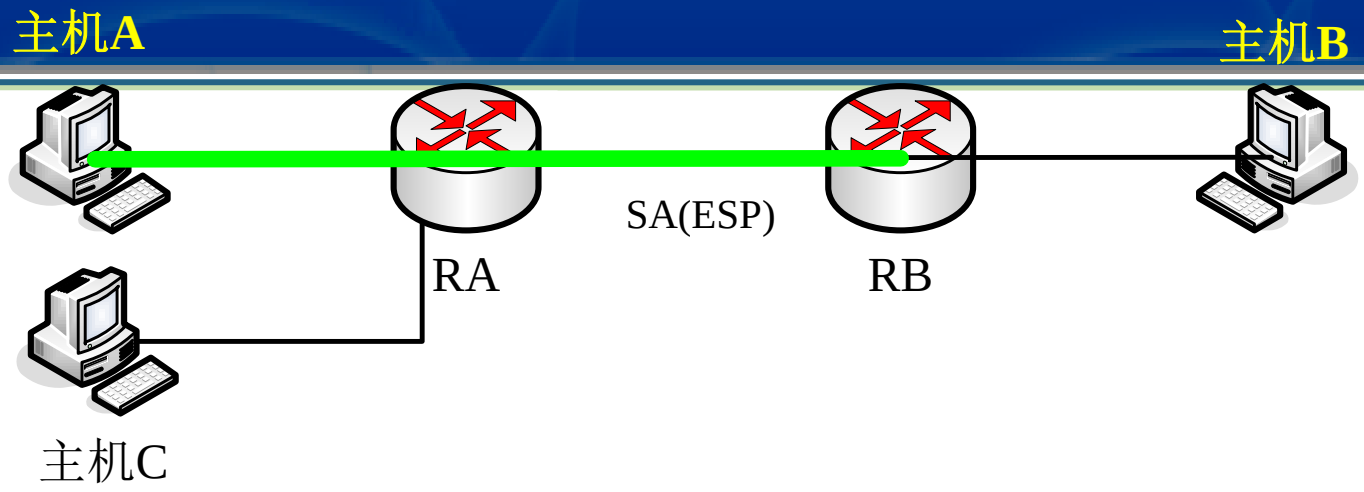
- SP（Security Policy，安全策略）：决定对IP数据包提供何种保护，并以何种方式实施保护。
  - SP主要根据源IP地址、目的IP地址、入数据还是出数据等来标识。
  - IPSec还定义了用户能以何种粒度来设定自己的安全策略，不仅可以控制到IP地址，还可以控制到传输层协议或者TCP/UDP端口等。

SPD（Security Policy Database，安全策略数据库）

- SPD也不是通常意义上的“数据库”，而是将所有的SP以某种数据结构集中存储的列表。

（包处理过程中，SPD和SAD两个数据库要联合使用）

- 当接收或将要发出IP包时，首先要查找SPD来决定如何进行处理。存在3种可能的处理方式：丢弃、不用IPSec和使用IPSec。
  - 丢弃：流量不能离开主机或者发送到应用程序，也不能进行转发。
  - 不用IPSec：对流量作为普通流量处理，不需要额外的IPSec保护。
  - 使用IPSec：对流量应用IPSec保护，此时这条安全策略要指向一个SA。对于外出流量，如果该SA尚不存在，则启动IKE进行协商，把协商的结果连接到该安全策略上。



RB上的SPD

源	目的	处理	隧道本地端点	隧道对方端点	
主机B	主机A	ESP	RB	主机A	
主机B	主机C	转发	无	无	

IPSec的实现方式

- IPSec的实现方式有两种：传输模式（Transport Mode）和隧道模式（Tunnel Mode）。
- AH和ESP都支持这两种模式，因此有四种组合：
  - 传输模式的AH
  - 隧道模式的AH
  - 传输模式的ESP
  - 隧道模式的ESP

IPSec的传输模式

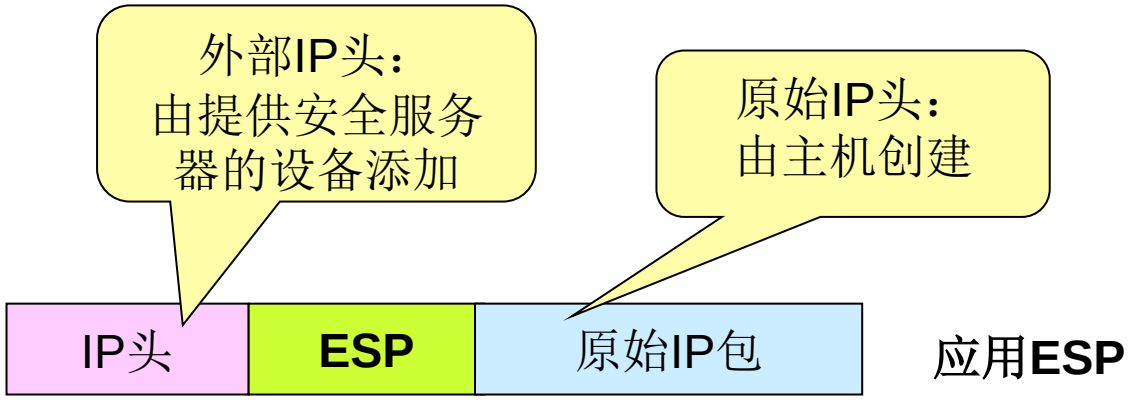
- 采用传输模式时，IPSec只对IP数据包的净荷进行加密或认证。
- 封装数据包继续使用原IP头部，只对部分域进行修改。
- 而IPSec协议头部插入到原IP头部和传输层头部之间。
- 只用于两台主机之间的安全通信

➢ 正常网络层次处理：

- 启用IPSec传输模式之后：

IPSec的隧道模式

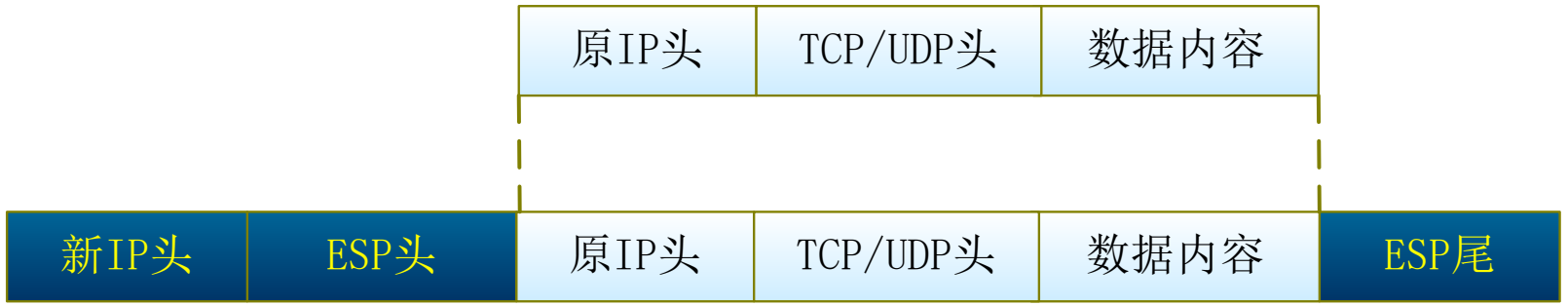
- 隧道模式保护的是**整个IP包**。通常情况下，只要IPSec双方有一方是安全网关或路由器，就必须使用隧道模式。



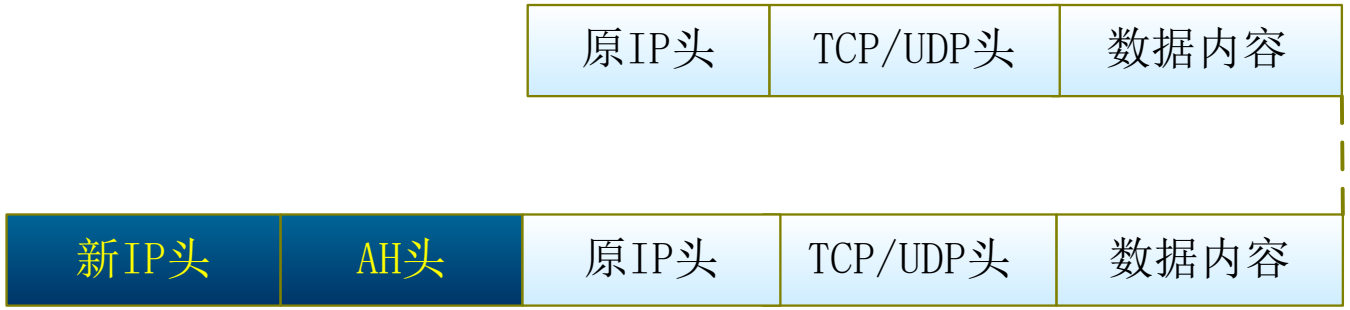
IPSec的隧道模式

- 采用隧道模式时，IPSec对整个IP数据包进行加密或认证。
- 产生一个新的IP头，IPSec头被放在新IP头和原IP数据包之间，组成一新IP头。

IPSec隧道模式的ESP封装示意图



IPSec隧道模式的AH封装示意图



IPSec协议概述

AH、ESP或AH+ESP既可以在隧道模式中使用，又可以在传输模式中使用。

IPSec的功能和模式

功能/模式	认证头协议（AH）	封装安全载荷（ESP）	ESP+AH
访问控制	Yes	Yes	Yes
认证	Yes	Yes	Yes
消息完整性	Yes	Yes	Yes
重放保护	Yes	Yes	Yes
机密性	—	Yes	Yes

14.3.2 IPSec的工作原理

1. IPSec的工作原理类似于包过滤防火墙，可以把它看做是包过滤防火墙的一种扩展。
2. IPSec网关通过查询安全策略数据库（SPD）决定对接收到的IP数据包进行转发、丢弃或IPSec处理。
3. IPSec网关可以对IP数据包只进行加密或认证，也可以对数据包同时实施加密和认证。

无论是进行加密还是进行认证，IPSec都有两种工作模式：传输模式和隧道模式。

IPSec处理(1)—外出处理

- 外出处理过程中，传输层的数据包流入IP层。IP层检索SPD数据库，判断应为这个包提供哪些服务。可能有以下几种情况：
  - 丢弃：简单丢掉；
  - 不应用安全服务：为载荷增添IP头，然后分发IP包；
  - 应用安全服务：如果已建立SA，则返回指向该SA的指针；如果未建立SA，则调用IKE建立SA。按照建立的SA，增添适当的AH和ESP头。

IPSec处理(2)—进入处理

- 收到IP包后，如果包内没有IPSec头，则根据安全策略对包进行检查，决定如何处理：
  - 丢弃：直接丢弃；
  - 应用安全服务：如果没有ipsec头，说明包有问题，丢弃；
  - 不应用安全服务：将包载荷传给上层协议处理。
- 如果IP包中包含了IPSec包：
  - 从IP包中提取三元组(SPI，目标地址，协议)在SAD中检索。根据协议值交给AH层或ESP层处理。协议载荷处理完之后，要在SPD中查询策略，验证SA使用是否得当。

14.3.3 IPSec中的主要协议

IPSec中主要由AH、ESP和IKE三个协议来实现加密、认证和管理交换功能。

1 AH（Authentication Header）

RFC 2402将AH服务定义如下：

- 非连接的数据完整性校验；
- 数据源点认证；
- 可选的抗重放攻击服务。

AH有两种实现方式：传输方式和隧道方式

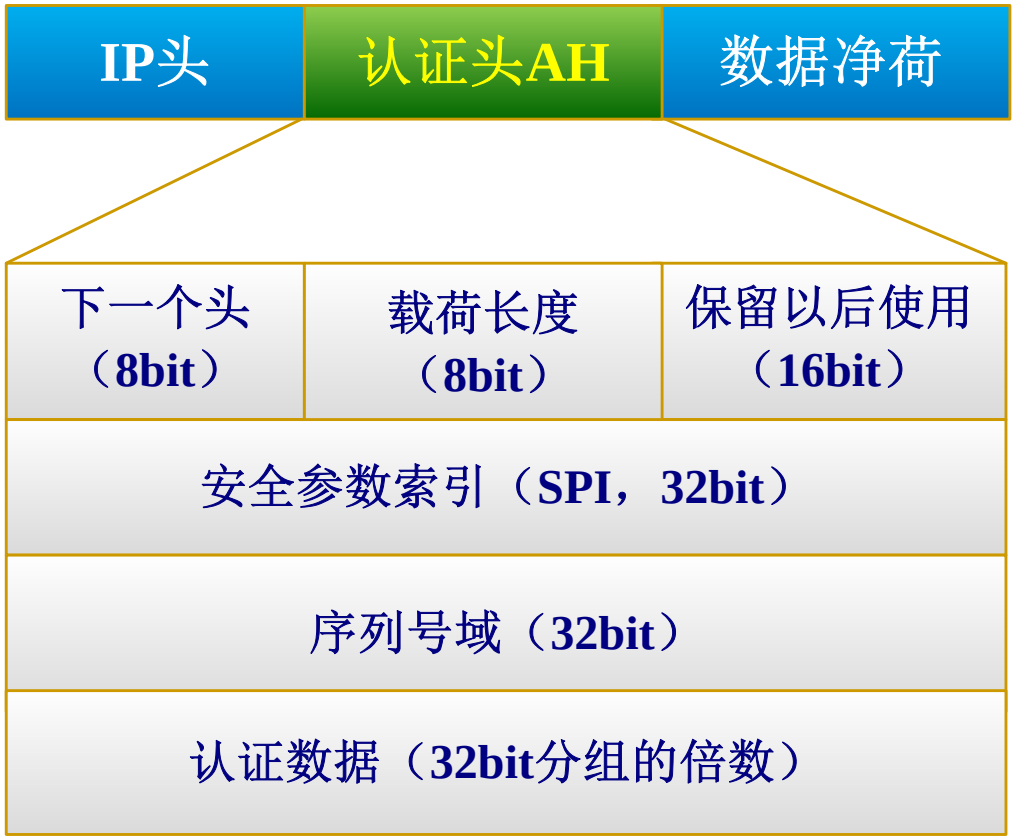
AH只涉及认证，不涉及加密

IPSec安全协议——AH

- AH（Authentication Header，验证头部协议）：RFC2402
  - AH对IP层的数据使用验证算法MAC，从而对完整性进行保护。
  - MAC（Message Authentication Codes，报文验证码），即报文摘要，是从HASH算法演变而来，又称为HMAC，如HMAC-MD5、HMAC-SHA1、HMAC-RIPEMD-160。
  - 通过HMAC可以检测出对IP包的头部和载荷的修改，从而保护IP包的内容完整性和来源可靠性。
  - 不同IPSec系统可用的HMAC算法可能不同，但HMAC-MD5和HMAC-SHA1是必须实现的。

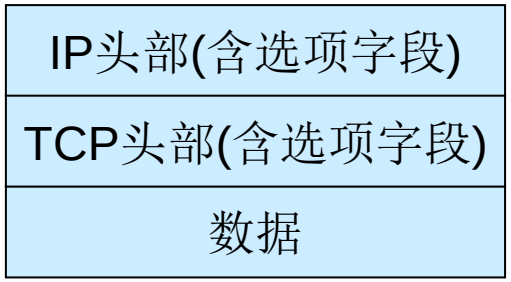
IPSec 安全协议——AH

AH协议和TCP、UDP协议一样，是被IP协议封装的协议之一，可以由IP协议头部中的协议字段判断，AH的协议号是51。

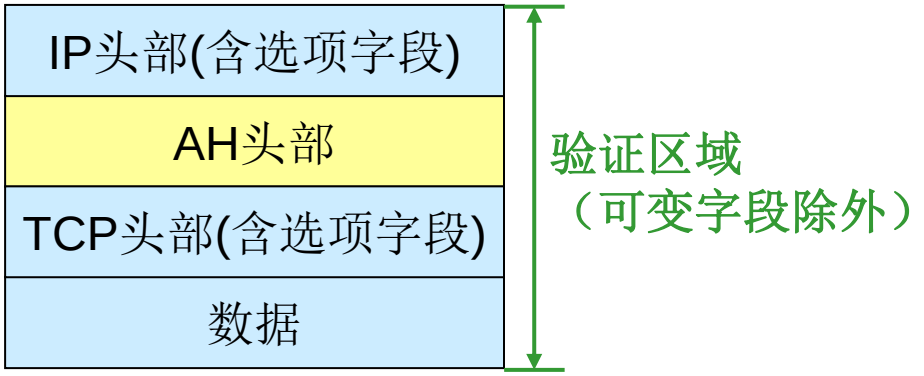


AH运行模式(1)—传输模式

- AH插入到IP头部（包括IP选项字段）之后，传输层协议（如TCP、UDP）或者其他IPSec协议之前。



图a 应用AH之前



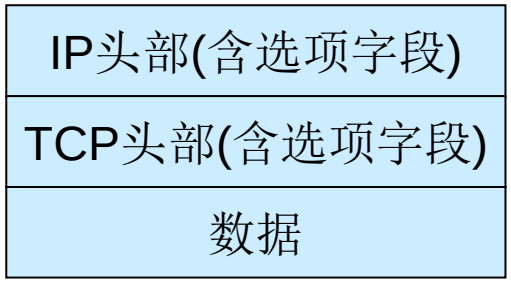
图b 应用AH之后

AH与NAT冲突

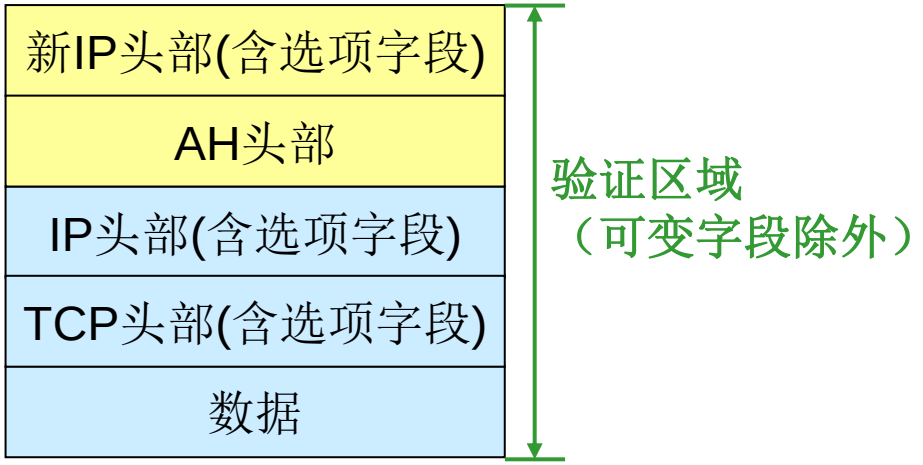
- 被AH验证的区域是整个IP包（可变字段除外），包括IP包头部，因此源IP地址、目的IP地址是不能修改的，否则会被检测出来。
- 然而，如果该包在传送的过程中经过NAT网关，其源/目的IP地址将被改变，将造成到达目的地址后的完整性验证失败。因此，AH在传输模式下和NAT是冲突的，不能同时使用，或者可以说AH不能穿越NAT。

AH运行模式(2)—隧道模式

- 在隧道模式中，AH插入到原始IP头部之前，然后在AH之前再增加一个新的IP头部。



图a 应用AH之前



图b 应用AH之后

- 隧道模式下，AH验证的范围也是整个IP包，因此上面讨论的AH和NAT的冲突在隧道模式下也存在。
- 在隧道模式中，AH可以单独使用，也可以和ESP一起嵌套使用。

数据完整性检查

- 验证过程概括如下：
  - 在发送方，整个IP包和验证密钥被作为输入，经过HMAC算法计算后得到的结果被填充到AH头部的“验证数据”字段中；
  - 在接收方，整个IP包和验证算法所用的密钥也被作为输入，经过HMAC算法计算的结果和AH头部的“验证数据”字段进行比较，如果一致，说明该IP包数据没有被篡改，内容是真实可信的。

IPv4头部中的不定字段和固定字段

版本	首部长度	服务类型	总长度
标识		标志	片偏移
生存时间		协议	首部检验和
源地址			
目的地址			
选项字段			

- 不定字段（在通信过程中可能被合法修改）：
  - 在计算HMAC时先临时用0填充；
  - 另外，AH头部的验证数据字段在计算之前也要用0填充，计算之后再填充验证结果。
- 应被AH保护的内容（在通信过程应该不被修改）：
  - 固定字段；
  - AH头中除“验证数据”以外的其他字段；
  - 数据：指经过AH处理之后，在AH头部后面的数据。传输方式下，指TCP、UDP或ICMP等传输层数据；隧道模式下，指被封装的原IP包。

IPSec安全协议——ESP

2 ESP（Encapsulating Security Payload）

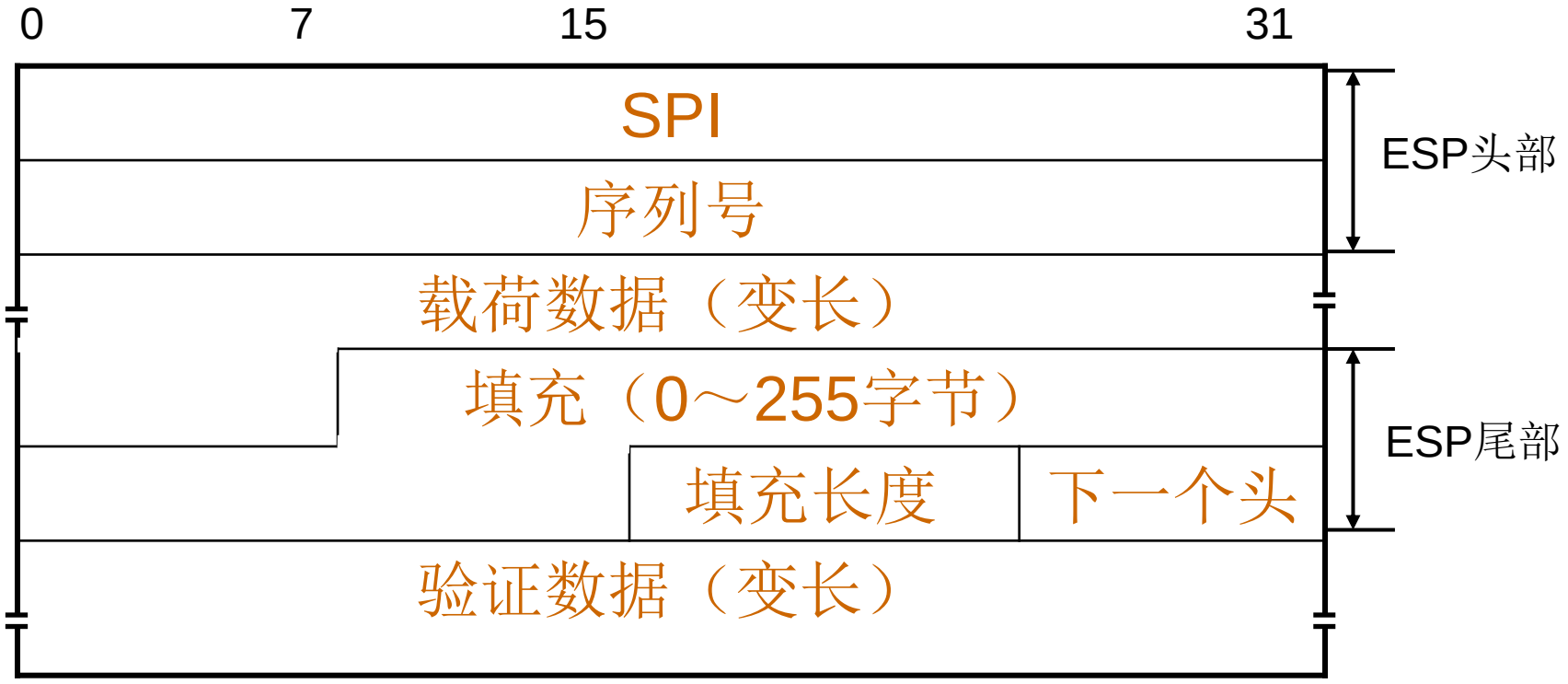
ESP协议主要用于对IP数据包进行加密，此外也对认证提供某种程度的支持。

ESP协议也有两种工作模式：传输模式和隧道模式。

1）与AH相比，ESP验证的数据范围要小一些。ESP协议规定了所有IPSec系统必须实现的验证算法：HMAC-MD5、HMAC-SHA1、NULL。
2）ESP的加密采用的是对称密钥加密算法。不同的IPSec实现，其加密算法也有所不同。为了保证互操作性，ESP协议规定了所有IPSec系统都必须实现的加密算法：DES-CBC、NULL。
3）但ESP协议规定加密和认证不能同时为NULL。即加密和认证必须至少选其一。

ESP头部格式

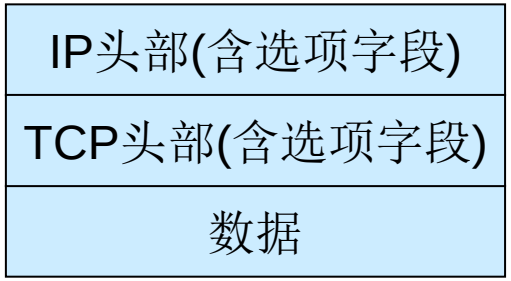
- ESP协议和TCP、UDP协议一样，是被IP协议封装的协议之一，可以由IP协议头部中的协议字段判断，ESP的协议号是50。



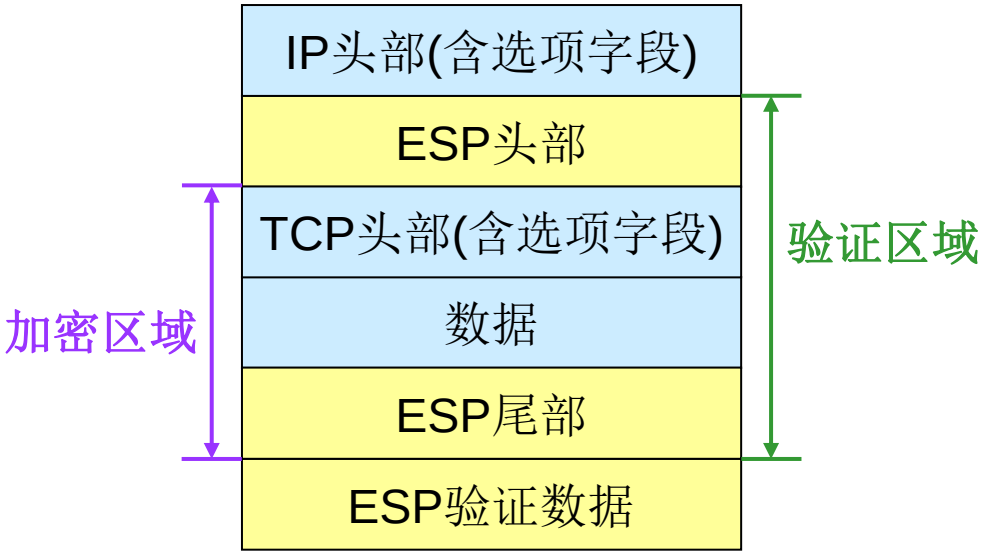
ESP运行模式(1)—传输模式

- 保护的是IP包的载荷；
- ESP插入到IP头部（包括IP选项字段）之后，任何被IP协议所封装的协议（如传输层协议TCP、UDP、ICMP，或者IPSec协议）之前。

ESP传输模式示意图



图a 应用ESP之前

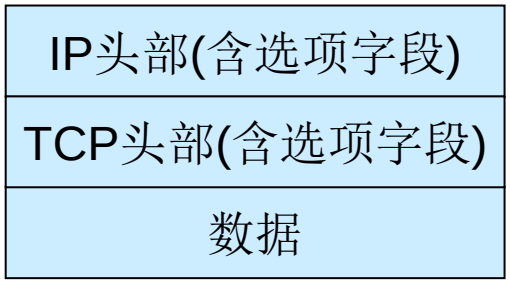


图b 应用ESP之后

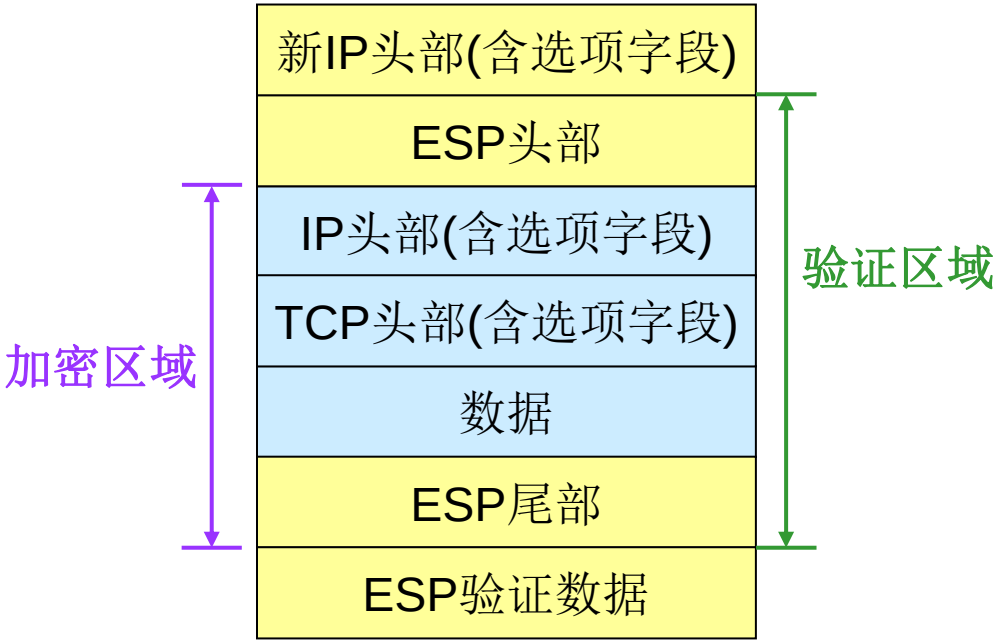
- ESP加密不包括SPI、序号字段和验证数据；
- ESP的验证不包括IP头部：
  - 优点：不存在与NAT冲突的问题；
  - 缺点：除了ESP头部之外，任何IP头部字段都可以修改，只要保证其校验和计算正确，接收端就不能检测出这种修改。所以，**ESP传输模式的验证服务要比AH传输模式弱一些。**如果需要更强的验证服务并且通信双方都是公有IP地址，应该采用AH来验证，或者将AH认证与ESP验证同时使用。

ESP运行模式(2)—隧道模式

- 保护的是整个IP包，对整个IP包进行加密；
- 在隧道模式中，ESP插入到原始IP头部之前，然后在ESP之前再增加一个新的IP头部。



图a 应用ESP之前



图b 应用ESP之后

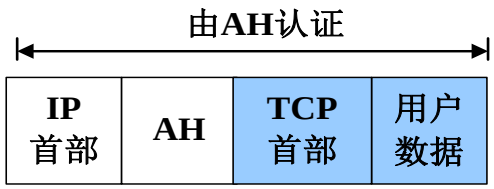
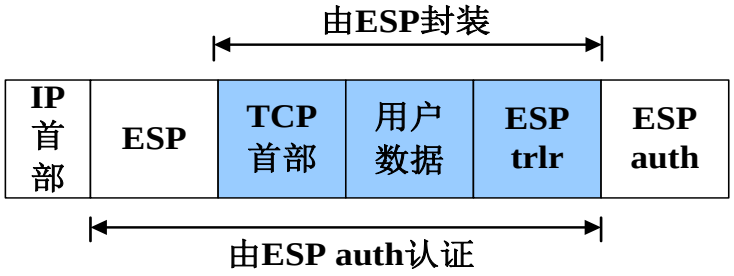
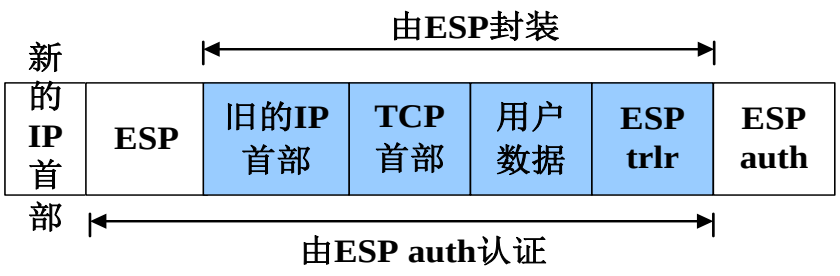
- ESP隧道模式的验证和加密能够提供比ESP传输模式更加强大的安全功能，因为隧道模式下对整个原始IP包进行验证和加密，可以提供数据流加密服务；而ESP在传输模式下不能提供流加密服务，因为源、目的IP地址不被加密。
- 不过，隧道模式将占用更多的带宽，因为增加了一个额外的IP头部。
- 尽管ESP隧道模式的验证功能不像AH传输模式或隧道模式那么强大，但ESP隧道模式提供的安全功能已经足够了。

ESP处理

- 根据ESP采用的模式来具体处理。
- 注意：
  - 密文是得到验证的，而验证中包括未加密的明文.
  - 所以：外出报文—先加密；进入报文—先验证。

14.3.1 IPSec协议概述

- IPSec协议使用认证头标AH和封装安全净载ESP两种安全协议来提供安全通信。两种安全协议都分为隧道模式和传输模式。
- 传输模式用在主机到主机的通信，隧道模式用在其它任何方式的通信。

	传输模式	隧道模式
AH	认证TCP、UDP或ICMP首部和数据	认证IP首部和数据
		
ESP	封装TCP、UDP或ICMP首部和数据	封装IP首部和数据
		

14.3.3 IPSec中的主要协议

3 IKE（Internet Key Exchange）

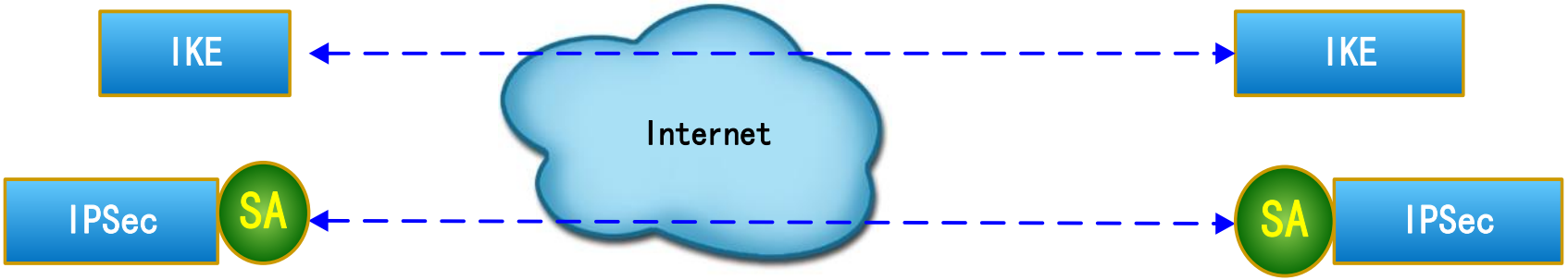
IKE用于动态建立安全关联（SA，Security Association）

IKE协议分两个阶段：

- 第一阶段：建立IKE安全关联，即在通信双方之间协商密钥；
- 第二阶段：利用这个既定的安全关联为IPSec建立安全通道。

IKE图解

（a）IKE建立SA



（b）IPSec可以建立安全通道

Internet密钥交换

- Internet密钥交换（IKE）用于动态建立SA。
- IKE属于一种混合型协议，由RFC2409定义，包含了3个不同协议的有关部分：ISAKMP、Oakley和SKEME ，还定义了自己的两种密钥交换方式。
- IKE并非为IPSec专用，只要其他协议需要，都可用它协商具体的安全服务。

ISAKMP协议

- ISAKMP（Internet Security Association Key Management Protocol，Internet安全联盟密钥管理协议）：RFC2408。
- 定义了协商、建立、修改和删除SA的过程和包格式。
- ISAKMP只是为协商、修改、删除SA的方法提供了一个通用的框架，并没有定义具体的SA格式。这个通用的框架是与密钥交换独立的，可以被不同的密钥交换协议使用。
- ISAKMP报文可以利用UDP或者TCP，端口都是500，一般情况下常用UDP协议。

ISAKMP包头部格式

- ISAKMP报文的头部是固定长度的，包含了维护状态、处理载荷必要的信息。

ISAKMP包头部格式

（1）发起方Cookie（Initiator Cookie）：64位

- Cookie可以帮助通信双方确认一个ISAKMP报文是否真的来自对方。
- 在发起方，如果收到的某报文的应答方Cookie字段和以前收到的该字段不同，则丢弃该报文；同样，在应答方，如果收到的某报文的发起方Cookie和以前收到的该字段不同，则丢弃该报文。这种机制可以防止DOS攻击。

ISAKMP包头部格式

- 尽管Cookie的生成方法在实现不同的ISAKMP时可能不同，但无论发起方还是响应方，Cookie必须满足两个条件：
  - Cookie必须是用各自的机密信息生成的，该机密信息不能从Cookie中推导出来；
  - 对于一个SA，其Cookie是惟一的，也就是说对于一次SA协商过程，Cookie不能改变。
- 常用的一个生成Cookie的方法是对下述信息进行HASH（MD5、SHA1或其他HASH算法）之后，取结果的前64位：

源IP地址＋目的IP地址＋UDP源端口＋UDP目的端口＋随机数＋当前日期＋当前时间

ISAKMP包头部格式

（2）应答方Cookie(Responder Cookie)：64位

- 应答方的Cookie，紧跟在发起方Cookie之后

（3） 下一个载荷（Next Payload）：4位

- 表示紧跟在ISAKMP头部之后的第一个载荷的类型值。

（4） 主版本（Major Version）：4位

- 表示ISAKMP协议的主版本号。

（5） 次版本（Minor Version）：4位

- 表示ISAKMP协议的次版本号。

（6） 交换类型（Exchange Type）：8位

- 表示该报文所属的交换类型。

ISAKMP包头部格式

（7） 标志（Flags）：8位

- 目前只有后3位有用，其余保留，用0填充。后3位的含义从最后一位往前依次为：
  - 加密位（encryption），0x01。加密位如果是1，表示ISAKMP头部后面的所有载荷都被加密了；如果是0，表示载荷是明文，没有加密。
  - 提交位（commit），0x02。用于确保在发送被保护的数据之前完成SA协商。
  - 纯验证位（Authentication Only），0x04。主要由哪些希望为ISAKMP引入密钥恢复机制的人使用。

（8） 报文ID（Message ID）：32位

- 包含的是由第二阶段协商的发起方生成的随机值，这个惟一的报文标识可以惟一确定第二阶段的协议状态。

（9） 报文长度（length）：32位

- 以字节为单位表示了ISAKMP整个报文（头部 +若干载荷）的总长度。

ISAKMP的载荷

- ISAKMP双方交换的内容称为载荷（payload）。对于一个用基于ISAKMP的密钥管理协议交换的消息来说，其构建方法是：将ISAKMP所有载荷链接到一个ISAKMP头。
- 目前定义了13种载荷，它们都是以相同格式的头开始的。

ISAKMP定义的载荷类型值

载荷类型	值
None	0
SA载荷（Security Association）	1
建议载荷（Proposal）	2
变换载荷（Transform）	3
密钥交换载荷（Key Exchange）	4
身份载荷（Identification）	5
证书载荷（Certificate）	6
证书请求载荷（Certificate Request）	7
HASH载荷（Hash）	8
签名载荷（Signature）	9
NONCE载荷（Nonce）	10
通知载荷（Notification）	11
删除载荷（Delete）	12
厂商载荷（Vendor）	13
保留	*14-127*
私有用途	*128-255*

ISAKMP载荷头部

不论何种载荷，都有一个相同格式的载荷头部

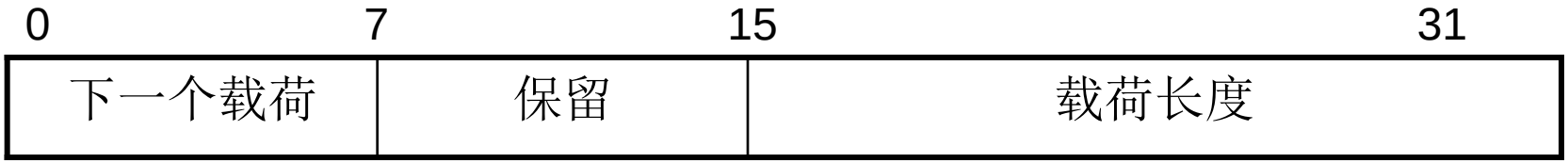
（1）下一个载荷（Next Payload）：8位

- 表示紧跟在本载荷后面的下一个载荷的类型。
- 第一个载荷的类型在ISAKMP头部中指明，最后一个载荷的Next Payload类型为0。

（2） 保留（reserved）：8位，全0

（3） 载荷长度（Payload Length）：16位

- 以字节为单位表示的载荷长度（包括载荷头部），定义了每个载荷的边界。




0
7
15
23
31
发起方Cookie
应答方Cookie
KE
主版本
次版本
交换类型
标志
报文ID
报文长度
Nonce
0
KE载荷长度
KE载荷数据
Vendor
0
Nonce载荷长度
Nonce载荷数据
ISAKMP头
KE载荷
Nonce载荷

ISAKMP协商阶段

- 阶段1
  - 这个阶段要协商的SA可以称为ISAKMP SA（在IKE中可以称为IKE SA），该SA是为了保证阶段2的安全通信。
- 阶段2
  - 这个阶段要协商的SA是密钥交换协议最终要协商的SA，当IKE为IPSec协商时可以称为IPSec SA，是保证AH或者ESP的安全通信。
- 阶段2的安全由阶段1的协商结果来保证。阶段1所协商的一个SA可以用于协商多个阶段2的SA。

ISAKMP交换类型

- 交换类型定义的是在通信双方所传送的载荷的类型和顺序，比如一方先发送什么载荷，另一方应如何应答等。这些交换模式的区别在于对传输信息的保护程度不同，并且传输的载荷多少也不同。

交换类型	值
None	0
基本交换（Base）	1
身份保护交换（Identity Protection）	2
纯认证交换（Authentication Only）	3
积极交换（Aggressive）	4
信息交换（Informational）	5
ISAKMP 将来使用	*6-31*
DOI专用	*32-239*
私有用途	*240-255*

- ISAKMP本身没有定义具体的密钥交换技术。对于IPSec而言，已定义的密钥交换就是IKE。IKE交换的最终结果是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SA。

IKE交换模式

- IKE基于两个阶段ISAKMP来建立安全联盟SA，第一阶段建立SA，第二阶段用IKE SA建立IPSec的SA
- 第一阶段
  - 主模式
  - 积极模式/野蛮模式

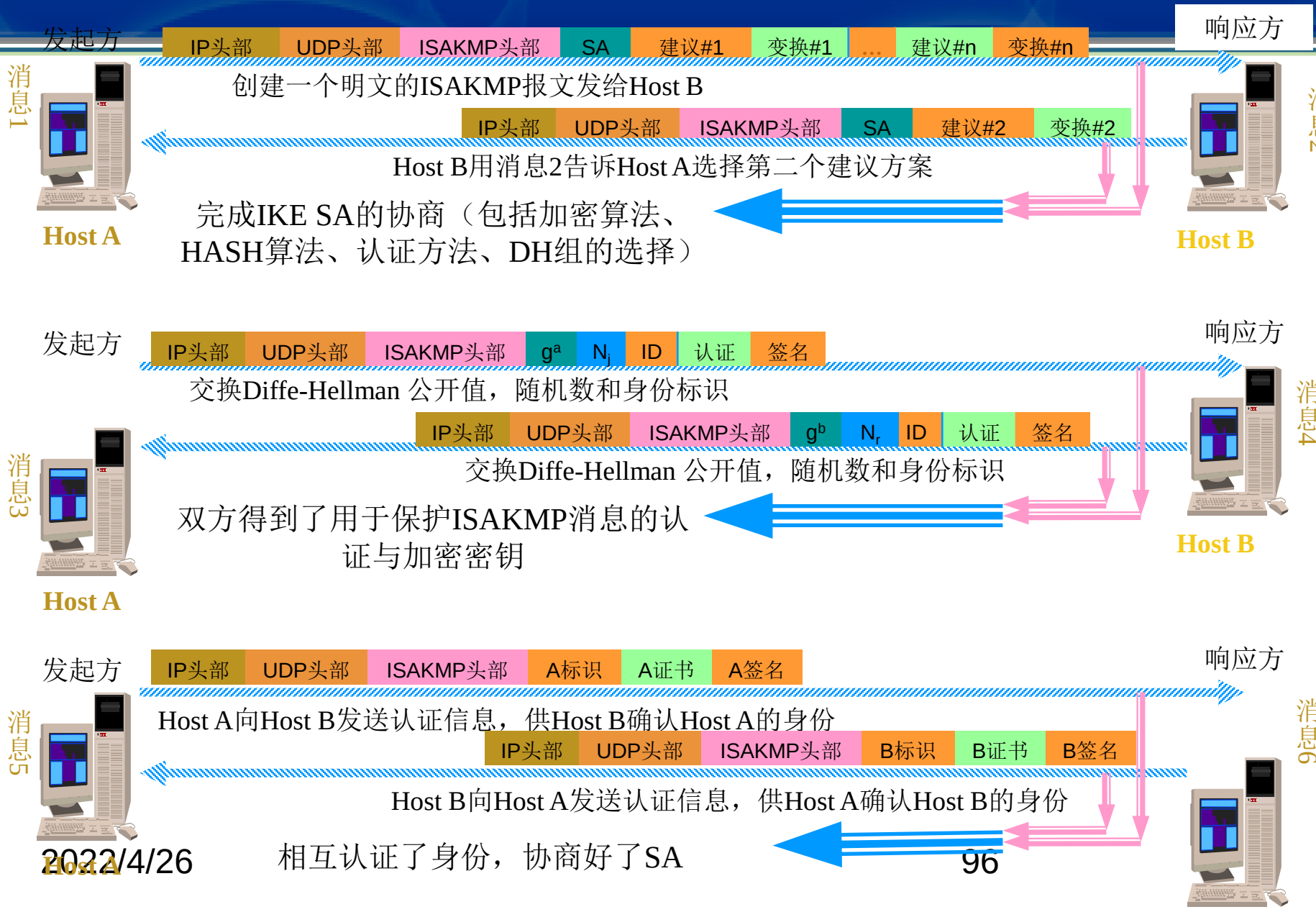
  （建立IKE SA，建立验证过的密钥，是其他交换的前提条件）
- 第二阶段
  - 快速模式

  （为IPSec协商安全服务）

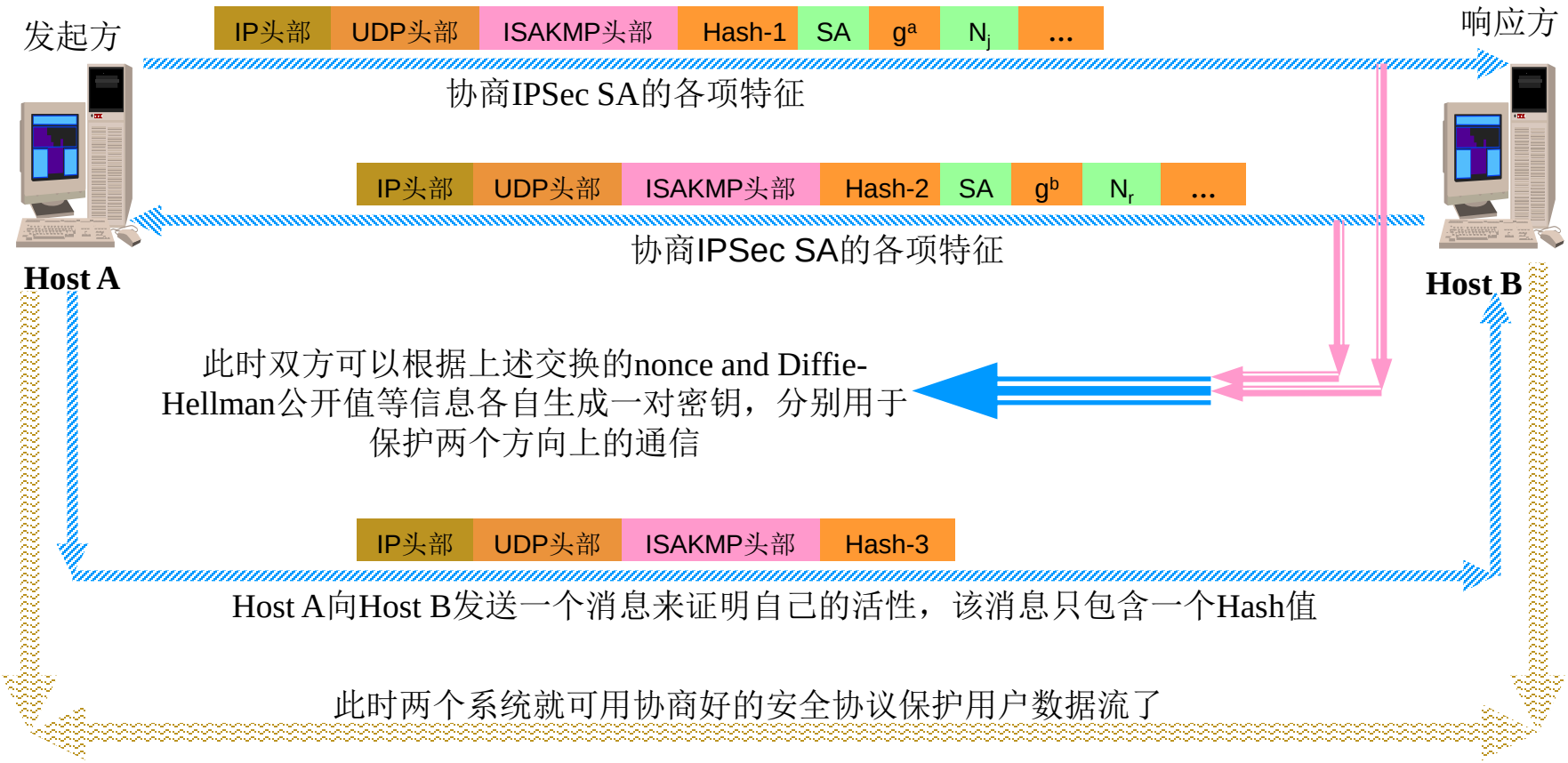
IKE身份认证方式

- 基于预共享字符串（Pre_Shared Key）
  - 双方事先通过某种方式商定好一个双方共享的字符串。
- 基于数字签名（Digital Signature）
  - 利用数字证书来表示身份，利用数字签名算法计算出一个签名来验证身份。
- 基于公开密钥（Public Key Encryption）
  - 利用对方的公开密钥加密身份，通过检查对方发来的该HASH值作认证。
- 基于修正的公开密钥（Revised Public Key Encryption）
  - 对上述方式进行修正。

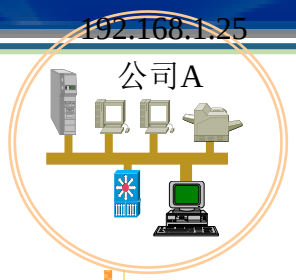
IKE第一阶段（主模式）

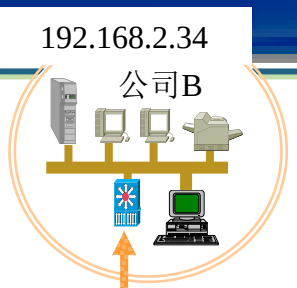

发起方
响应方
IP头部 UDP头部 ISAKMP头部 SA 建议#1 变换#1 ... 建议#n 变换#n
消息1
创建一个明文的ISAKMP报文发给Host B
IP头部 UDP头部 ISAKMP头部 SA 建议#2 变换#2
消息2
Host B用消息2告诉Host A选择第二个建议方案
完成IKE SA的协商（包括加密算法、HASH算法、认证方法、DH组的选择）
Host A
Host B
发起方
响应方
IP头部 UDP头部 ISAKMP头部 g^a N_j ID 认证 签名
交换Diffe-Hellman 公开值，随机数和身份标识
IP头部 UDP头部 ISAKMP头部 g^b N_r ID 认证 签名
消息3
消息4
交换Diffe-Hellman 公开值，随机数和身份标识
双方得到了用于保护ISAKMP消息的认证与加密密钥
Host A
Host B
发起方
响应方
IP头部 UDP头部 ISAKMP头部 A标识 A证书 A签名
消息5
Host A向Host B发送认证信息，供Host B确认Host A的身份
IP头部 UDP头部 ISAKMP头部 B标识 B证书 B签名
消息6
Host B向Host A发送认证信息，供Host A确认Host B的身份
相互认证了身份，协商好了SA
Host A
Host B

IKE第二阶段


发起方
响应方
IP头部 UDP头部 ISAKMP头部 Hash-1 SA g^a N_j ...
协商IPSec SA的各项特征
IP头部 UDP头部 ISAKMP头部 Hash-2 SA g^b N_r ...
协商IPSec SA的各项特征
Host A
Host B
此时双方可以根据上述交换的nonce and Diffie-Hellman公开值等信息各自生成一对密钥，分别用于保护两个方向上的通信
IP头部 UDP头部 ISAKMP头部 Hash-3
Host A向Host B发送一个消息来证明自己的活性，该消息只包含一个Hash值
此时两个系统就可用协商好的安全协议保护用户数据流了

一个完整的IPSecVPN工作原理





Source Address	Destination Address	Secure Service	Others
192.168.1.25	192.158.2.34	AH, ESP	……
192.158.1.25	192.168.2.35	绕过、丢弃	……
SPD中的数据项类似于防火墙的配置规则			

SPI	Destination Address	Security Protocol
256	192.168.1.25	AH
257	192.168.1.25	ESP
258	192.168.2.34	AH
259	192.168.2.34	ESP

SPI	Security Protocol	Algorithm	Key	Others
256	AH	HMAC-MD5	010	……
257	ESP	DES CBC 4	101	……
258	AH	HMAC-SHA-	001	……
259	ESP	3DES CBC	110	……
SAD中包含每一个SA的参数信息，如算法、密钥等				

负 载
IP 头

查找SPD数据库决定为流入的IP数据提供哪些安全服务

查找对应SA的参数

建立相应的SA

写入SAD

要求建立安全相应的关联

对原有数据包进行相应的安全处理

通过IKE建立安全关联，产生或者刷新密钥

VPN网关A

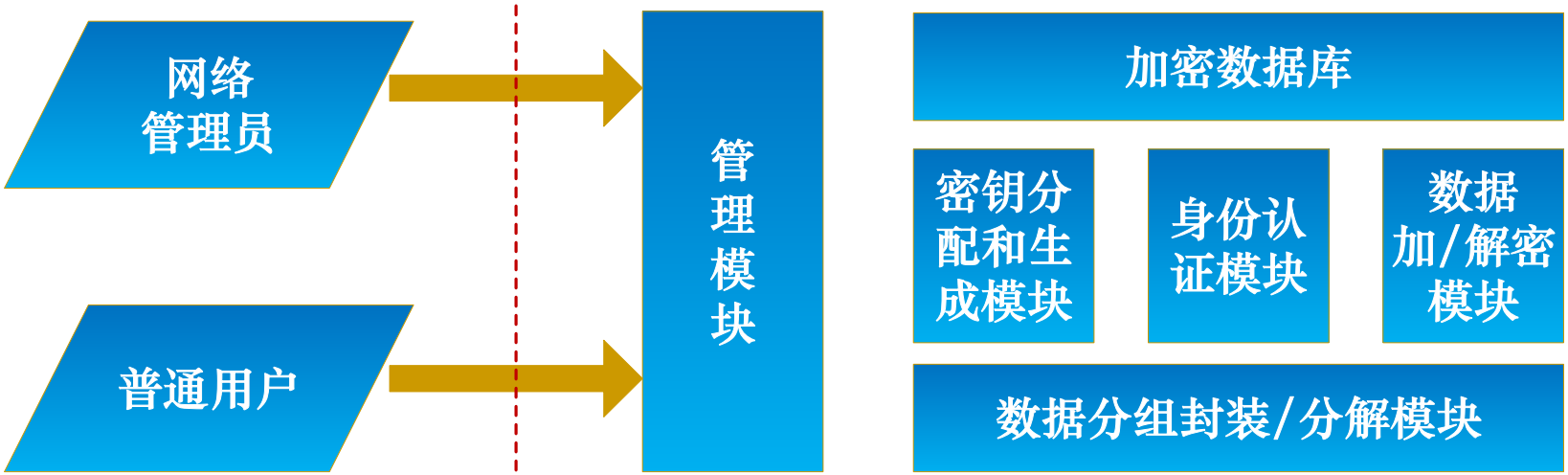
VPN网关B

外IP头 | AH头 | ESP头 | 内IP头 | 负 载 | ESP尾

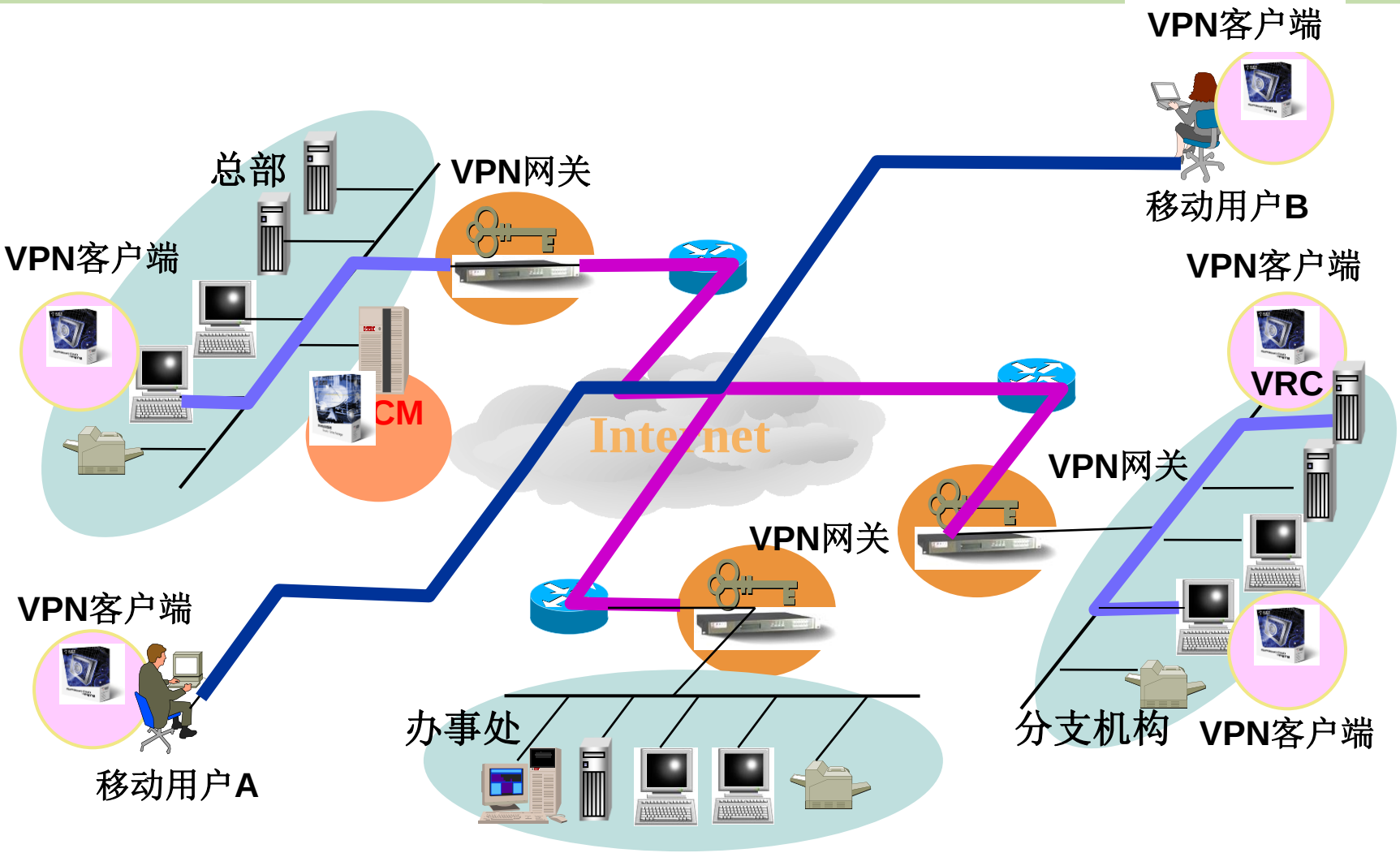
Internet

14.3.5 IPSec VPN的构成

- 管理模块
- 数据加/解密模块
- 密钥分配和生成模块
- 数据分组封装/分解模块
- 身份认证模块
- 加密函数库



VPN的部署


VPN客户端
移动用户B
总部
VPN网关
VPN客户端
CM
Internet
VPN客户端
VRC
VPN网关
VPN网关
VPN客户端
移动用户A
办事处
分支机构
VPN客户端

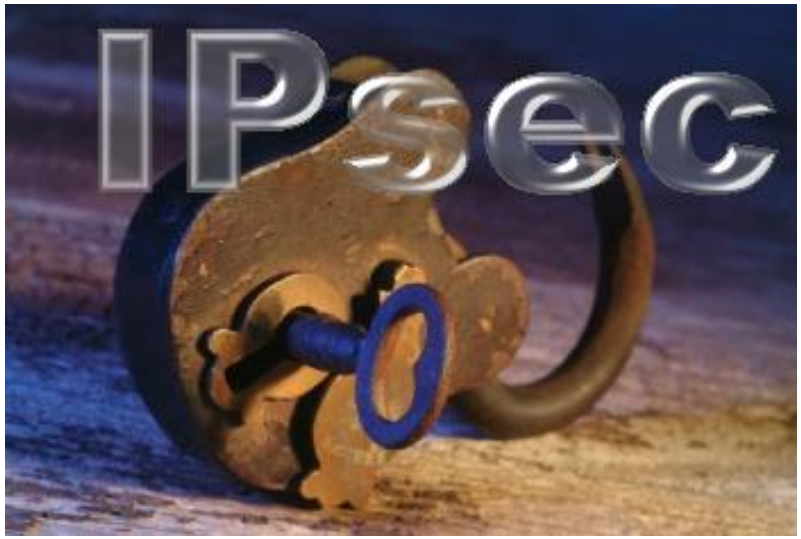
IPSecVPN的缺陷

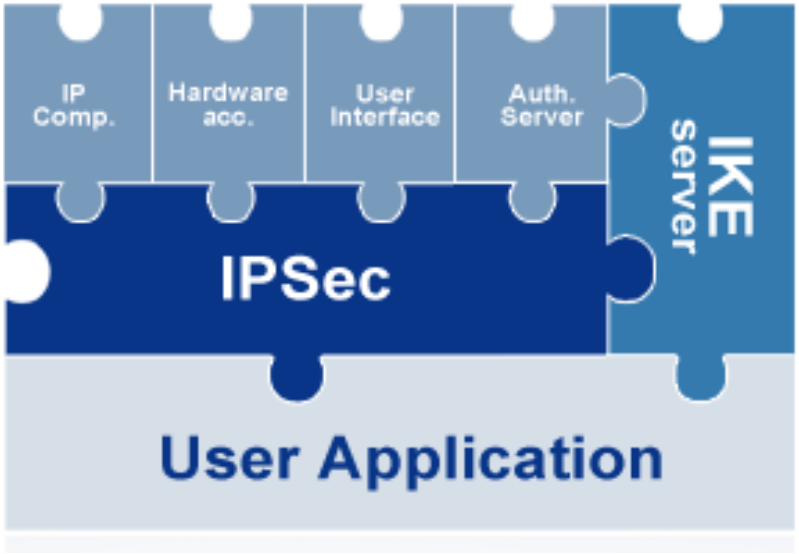
- IPSec VPN通信性能低。由于IPSec VPN在安全性方面比较高，影响了它的通信性能
- IPSec VPN需要客户端软件，可能带来了与其他系统软件之间兼容性问题的风险
- 安装和维护困难
- 实际全面支持的系统比较少，很少有能运行在其它PC系统平台的，如Mac、Linux、Solaris 等
- 不易解决网络地址转换(NAT)和穿越防火墙的问题

14.3.6 IPSec的实现

- FreeS/WAN是Linux操作系统中包含的IPsec VPN实现方案。
- 在网上可以找到其开放的源代码下载网址：

www.freeswan.org





第14章 VPN技术

一 VPN的基本概念和分类

二 PPTP、IPSec、TLS等隧道协议

三 IPSec VPN的原理及应用

四 TLS VPN的原理及应用

五 PPTP VPN的原理及应用

六 MPLS VPN的原理及应用

引入

- 随着VPN技术的发展，L2TP和IPSEC的缺陷日益突出，急需一种新型的VPN代替，SSL VPN就是在这样的条件下诞生！

14.4.1 SSL VPN概述

- SSL VPN也称做传输层安全协议（TLS）VPN。
- TLS协议主要用于HTTPS协议中。TLS也可以作为构造VPN的技术。
- TLS VPN的最大优点是用户不需要安装和配置客户端软件。
- 只需要在客户端安装一个IE浏览器即可。
- 由于TLS协议允许使用数字签名和证书，故它能提供强大的认证功能。

SSLVPN的特点

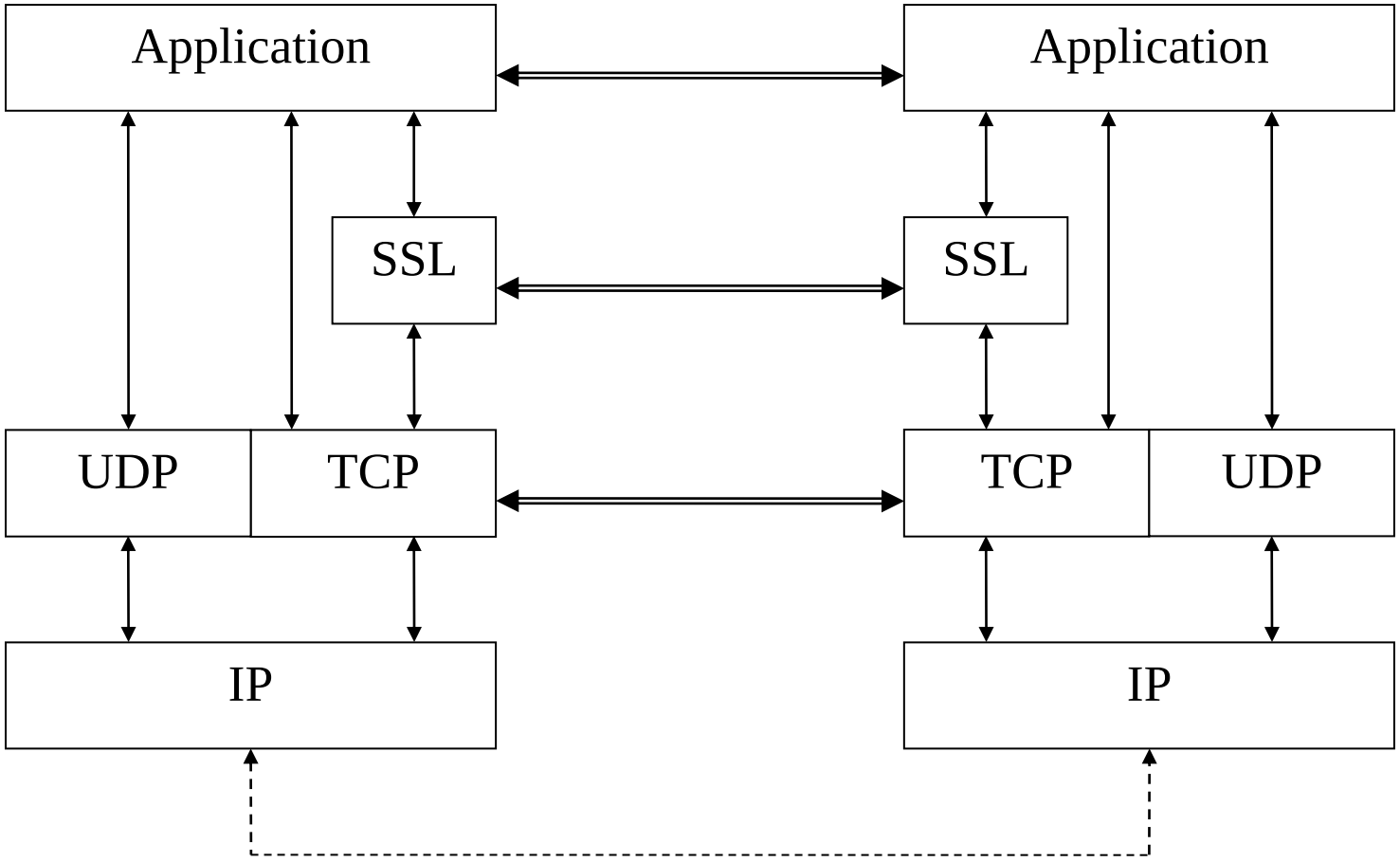
- SSL VPN可在NAT代理装置上以透明模式工作；
- SSL VPN不会受到安装在客户端与服务器之间的防火墙等NAT设备的影响，穿透能力强；
- SSL VPN将远程安全接入延伸到IPSec VPN扩展不到的地方，降低了部署和支持费用 ；
- 客户端安全检查和授权访问等操作，实现起来更加方便。
- SSL VPN可以在任何地点，利用任何设备，连接到相应的网络资源上。

可以说从功能上讲，SSL VPN是企业远程安全接入的最佳选择。

TLS/SSL 概述

- SSL（Secure Socket Layer）安全套接层是一种运行在两台机器之间的安全通道协议；也可以运行在SSL代理和PC之间；
- 功能：保护传输数据（加密），识别通信机器（认证）；
- SSL提供的安全通道是透明的，几乎所有基于TCP的协议稍加改动就可以直接运行于SSL之上；
- 目前，IETF将SSL作了标准化，推出TLS传输层安全协议（RFC 2246）整合取代，它工作在TCP之上。TLS1.0与SSL3.0的差别非常微小。

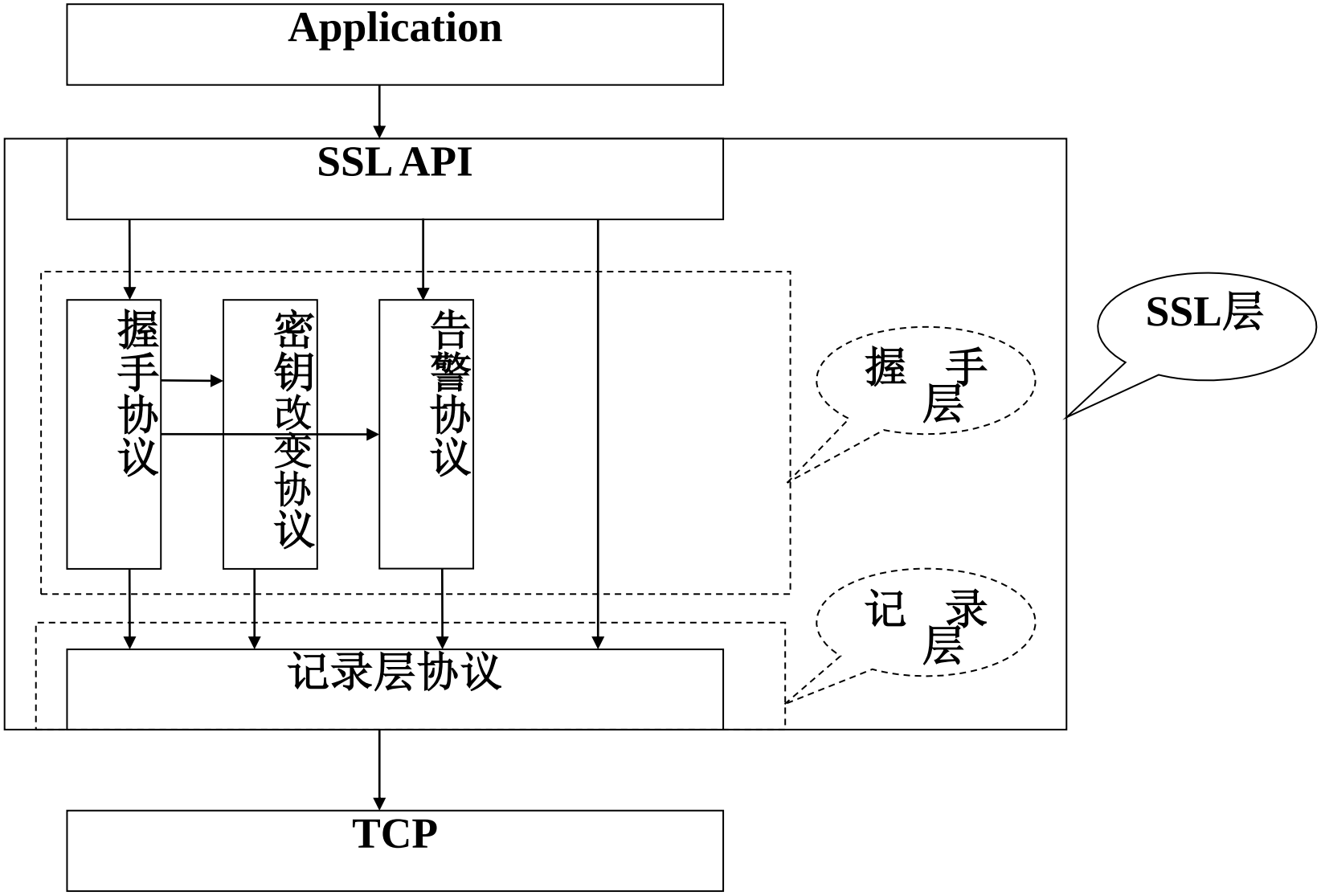
SSL在协议栈的位置



SSL协议组成

- 握手协议：
  - 对服务器进行认证；
  - 确立用于保护数据传输的加密密钥；
- 记录协议：
  - 传输数据；
- 告警协议
- SSL连接分为两个阶段，即握手和数据传输阶段；传输任何应用数据之前必须先完成握手。

SSL体系结构



14.4.2 TLS VPN的原理

TLS VPN的实现主要依靠下面三种协议的支持

1 握手协议

握手协议的功能：

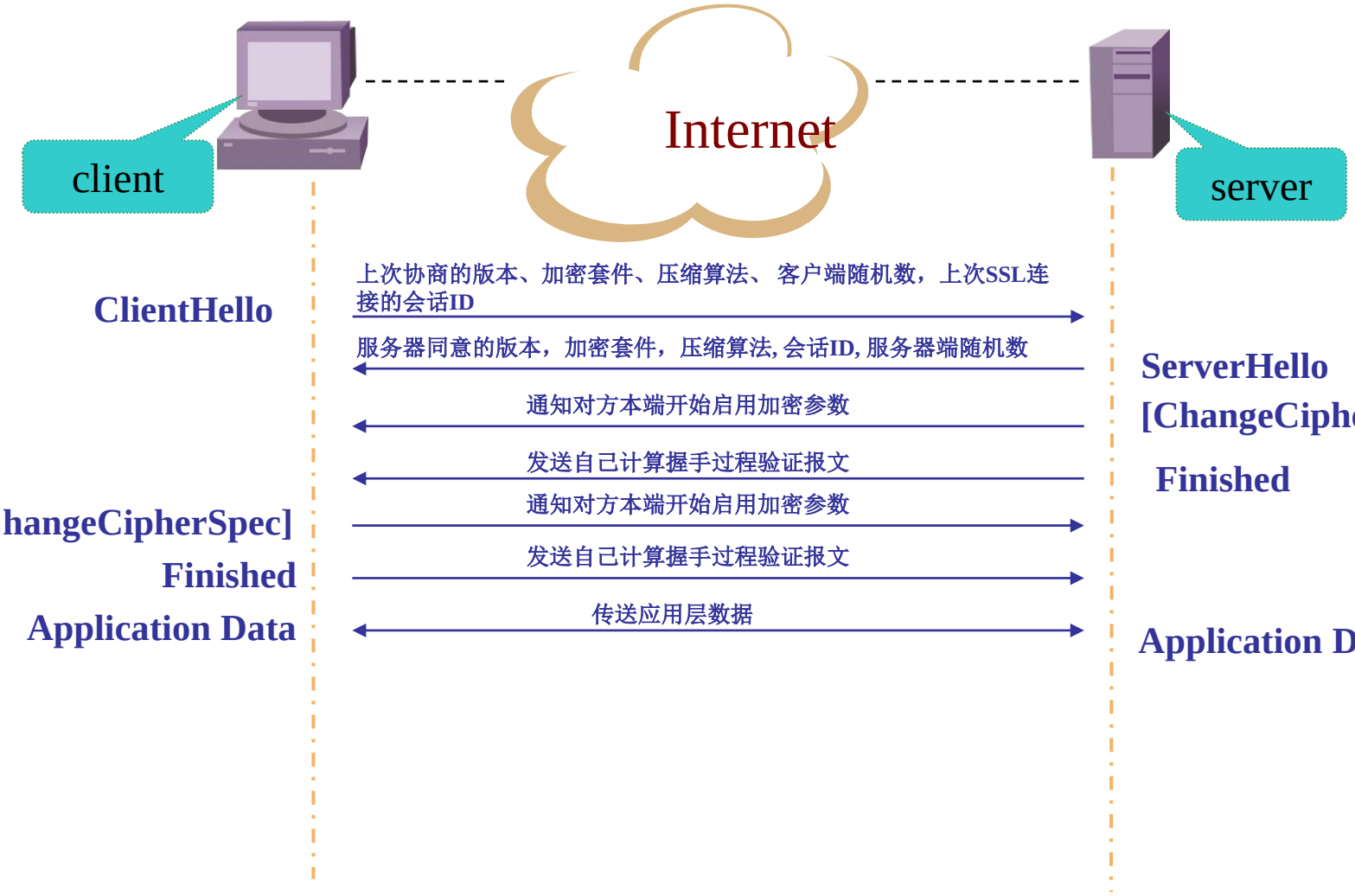
- 协商SSL协议的版本。
- 协商加密套件。
- 协商密钥参数。
- 验证通讯双方的身份(对客户端的身份认证可选)
- 建立SSL连接

SSL握手协议的握手过程

- 无客户端认证的全握手过程
- 会话恢复过程
- 有客户端认证的全握手过程

无客户端认证的全握手过程

会话恢复过程

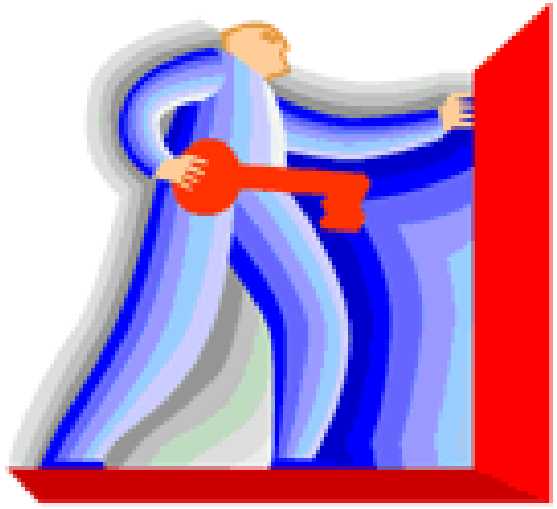

client
Internet
server
ClientHello
上次协商的版本、加密套件、压缩算法、 客户端随机数，上次SSL连接的会话ID
服务器同意的版本，加密套件，压缩算法, 会话ID, 服务器端随机数
ServerHello
通知对方本端开始启用加密参数
[ChangeCipherSpec]
发送自己计算握手过程验证报文
Finished
[ChangeCipherSpec]
通知对方本端开始启用加密参数
Finished
发送自己计算握手过程验证报文
Application Data
传送应用层数据
Application Data

有客户端认证的全握手过程

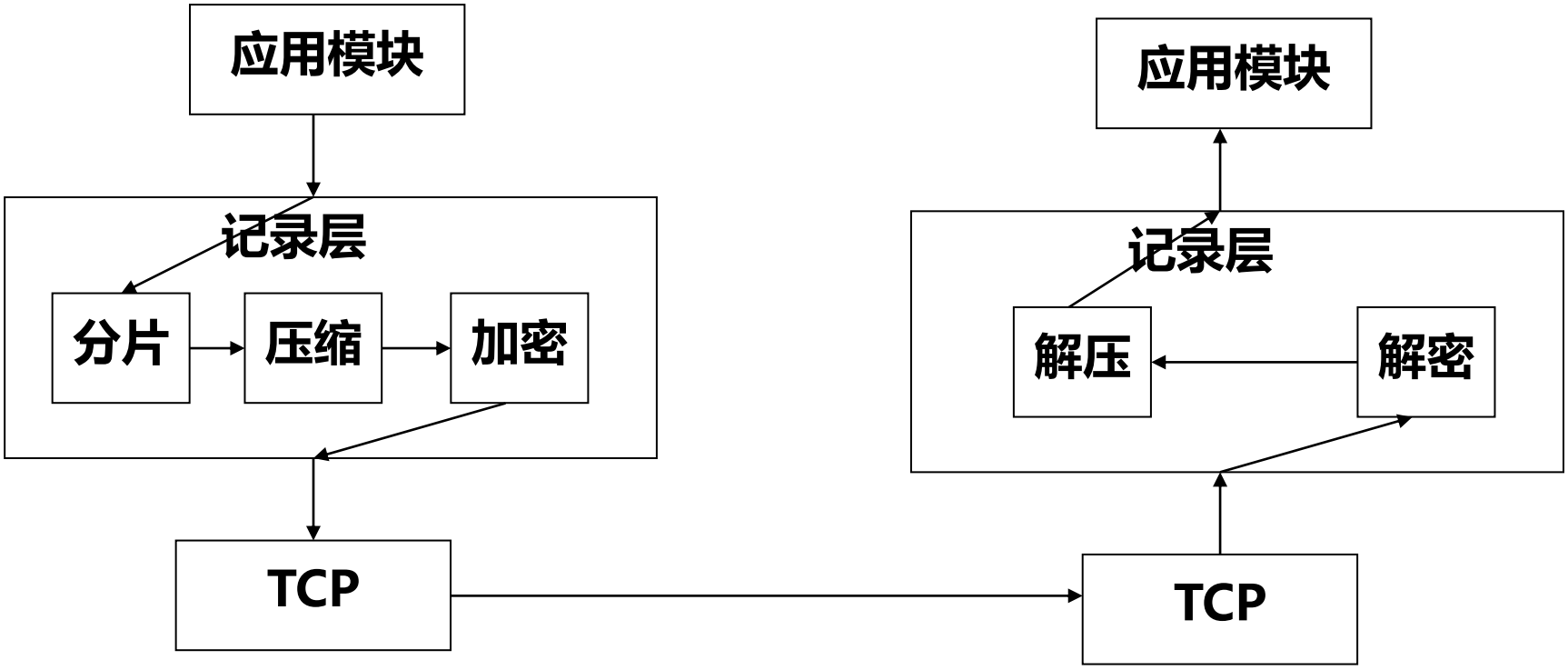
14.4.2 TLS VPN的原理

2 TLS记录协议

- 保护传输数据的私密性，对数据进行加密和解密
- 验证传输数据的完整性，计算报文的摘要
- 提高传输数据的效率，对报文进行压缩
- 保证数据传输的可靠和有序



SSL记录层的工作流程



14.4.2 TLS VPN的原理

3 警告协议

- 警告协议用于提示何时TLS协议发生了错误，或者两个主机之间的会话何时终止。
- 只有在TLS协议失效时告警协议才会被激活。



14.4.2 TLS VPN的原理

TLS VPN的实现方式

在企业的防火墙后面放置一个TLS代理服务器。

用户欲安全地连接到公司网络

- 首先要在浏览器上输入一个URL(Universal Resource Locator)；
- 该连接请求将被TLS代理服务器取得；
- 用户通过身份验证；
- TLS代理服务器提供用户与各种不同应用服务器之间的连接。

SSLVPN的分类

- 按照SSLVPN的实现方式，可以分为以下三类：
  - 基于Web代理的SSLVPN
  - 基于端口转发的SSLVPN
  - 基于隧道的SSLVPN

基于Web代理的SSLVPN

- 无须安装任何客户端，真正的跨平台方案
- 仅支持基于Web方式的访问
- 非Web应用需要进行应用转换，将基于C/S的Email、FTP、SSH等应用以Web的形式重新实现，实现起来复杂
- 对于Web页面中的链接，需要进行URL替换

优点：可以用于任何客户端，兼容各种平台访问，智能终端能无缝支持

缺点：支持的应用少，需要为新的应用进行Web转化

基于Web代理的SSLVPN举例

- 内网服务器链接：

  https://sslvpnip/http/serverip/path/xx.html

需要将该页面中的所有的链接全部替换为类似的链接，包括静态链接、动态链接等

存在问题：性能影响较大；

由于Web技术繁多，替换不完全

基于端口转发的SSLVPN

- 对于FTP、EMAIL、OA、TELNET、远程桌面、数据库等用户经常使用的C/S应用，如果采用Web应用转换，对每一种应用单独处理，工作量很大；此外，也改变了用户的使用习惯，不为用户所接受
- 对于这些应用，采用端口转发技术，客户端需要运行一个较小的ActiveX插件或Java applet程序，在本地端口监听；访问企业内网的应用数据发送到该监听端口，该程序将收到的数据通过浏览器的SSL连接传输到网关，网关再转发给内网服务器。
- 支持多种TCP应用

端口转发原理

- 端口转发表

服务器地址	服务器端口	本地监听地址	本地监听端口
Server1	80	127.0.0.1	8080
Server2	21	127.0.0.1	2121

- 用户访问：

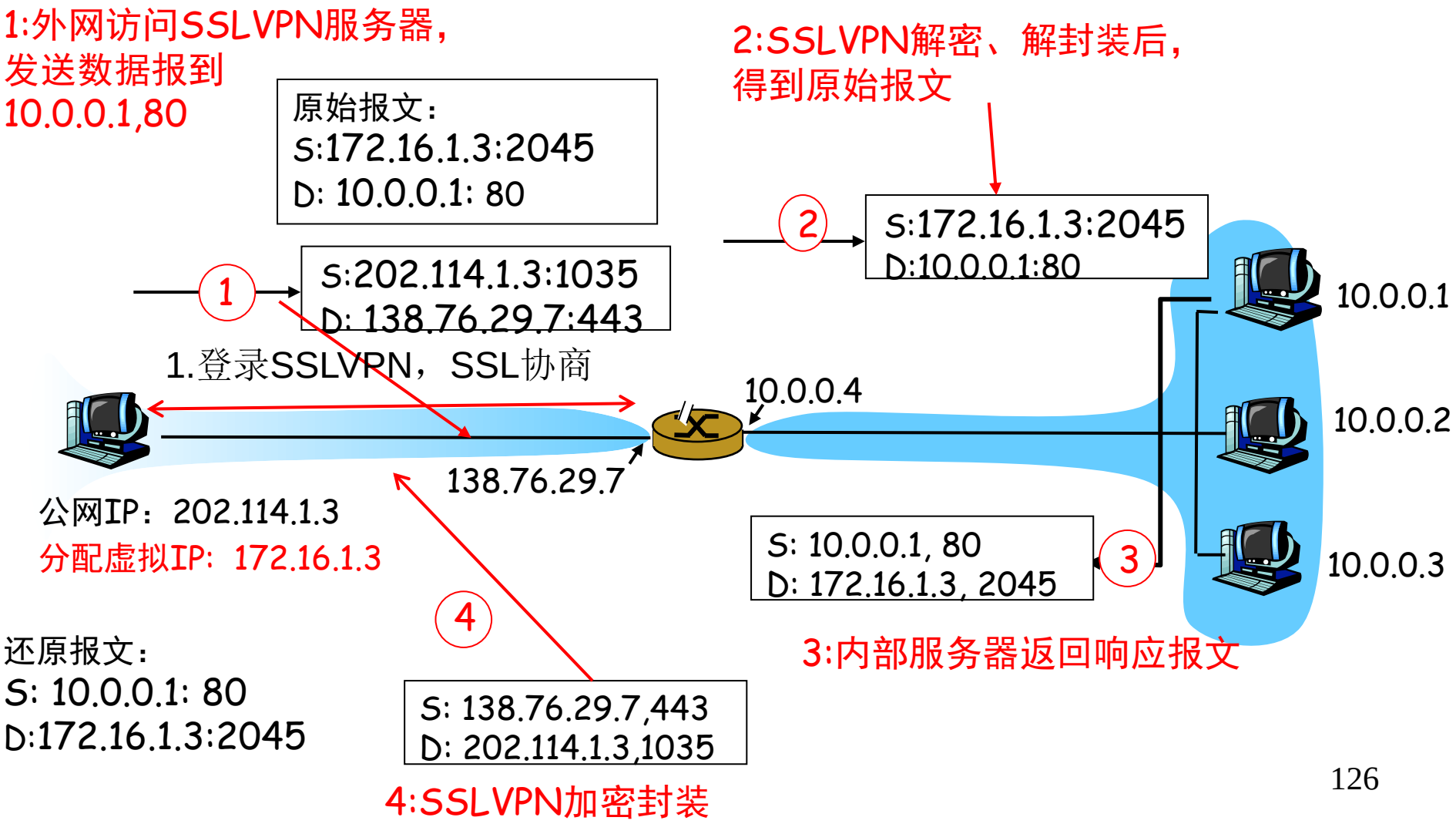
http://127.0.0.1:8080 ➔server1:80

ftp://127.0.0.1:2121 ➔server2:21

基于隧道的SSLVPN

- 采用跟IPSecVPN类似的技术，需要安装客户端软件，以及虚拟网卡
- 到内网服务器的IP报文（虚拟IP→内网服务器）会被客户端软件进行SSL协议封装（真实IP→SSL VPN网关地址），到对端的SSLVPN网关设备再解密解封装，还原为原始IP报文，交给内网服务器
- 能支持基于TCP、UDP、ICMP协议的各种应用
- 因工作在套接字层，无IPSecVPN的NAT穿越问题
- 缺点：平台兼容性不够好
- 开源代码：OpenVPN

基于隧道的SSLVPN



14.4.3 TLS VPN的优缺点

优点

- 无须安装客户端软件
- 适用于大多数设备
- 适用于大多数操作系统
- 支持网络驱动器访问
- 不需要对网络做改变
- 较强的资源控制能力
- 费用低且有良好安全性
- 可绕过防火墙进行访问
- 已内嵌在浏览器中

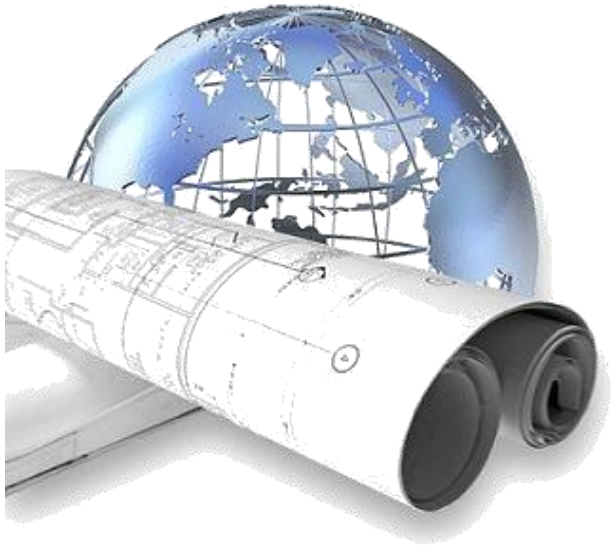
缺点

- 认证方式单一
- 应用的局限性很大
- 只对应用通道加密
- 不能对消息进行签名
- LAN连接缺少解决方案。
- 加密级别通常不高
- 不能保护UDP通道安全
- 是应用层加密，性能差
- 不能访问控制
- 需CA支持

14.4.4 TLS VPN的应用

- 在客户与TLS VPN的通信中，人们通常采用TLS Proxy技术来提高VPN服务器的通信性能和安全身份验证能力。
- 主要用于访问内部网中的一些基于Web的应用：

电子邮件　内部网页浏览　其他基于Web的查询工作



14.4.5 TLS VPN与IPSec VPN比较

选项	TLS VPN	IPSec VPN
身份验证	单向身份验证 双向身份验证 数字证书	双向身份验证 数字证书
加密	强加密 基于Web浏览器	强加密 依靠执行
全程安全性	端到端安全 从客户到资源端全程加密	网络边缘到客户端 仅对从客户到VPN网关之间通道加密
可访问性	适用于任何时间、任何地点访问	限制适用于已经定义好受控用户的访问
费用	低（无须任何附加客户端软件）	高（需要管理客户端软件）
安装	即插即用安装 无须任何附加的客户端软、硬件安装	通常需要长时间的配置 需要客户端软件或硬件
用户的易使用性	对用户非常友好，使用非常熟悉的Web浏览器 无须终端用户的培训	对没有相应技术的用户比较困难 需要培训
支持的应用	基于Web的应用 文件共享 E-mail	所有基于IP协议的服务
用户	客户、合作伙伴用户、远程用户、供应商等	更适合在企业内部使用
可伸缩性	容易配置和扩展	在服务器端容易实现自由伸缩，在客户端比较困难
穿越防火墙	可以	不可以

14.4.5 TLS VPN与IPSec VPN比较

- TLS VPN有很多优点，但并不能取代IPSec VPN。
- IPSec VPN主要提供LAN-to-LAN的隧道安全连接。
- 在为企业高级用户提供远程访问及为企业提供LAN-to-LAN隧道连接方面，IPSec具有无可比拟的优势。
- 目前，IPSec VPN的厂商也开始研究如何让IPSec VPN兼容TLS VPN，以增强可用性。如果成功，IPSec VPN的扩展性将大大加强，生命力也将更长久。

第14章 VPN技术

一 VPN的基本概念和分类

二 PPTP、IPSec、TLS等隧道协议

三 IPSec VPN的原理及应用

四 TLS VPN的原理及应用

五 PPTP VPN的原理及应用

六 MPLS VPN的原理及应用

14.5.1 PPTP VPN概述

- PPTP VPN最早是Windows NT 4.0支持的隧道协议标准，是PPP的扩展。
- 增强了PPP的认证和加密功能。
- PPTP的主要功能是开通VPN隧道，它还是采用原来的PPP拨号建立网络连接。
- PPTP的两个主要任务是“封装”和“加密”。

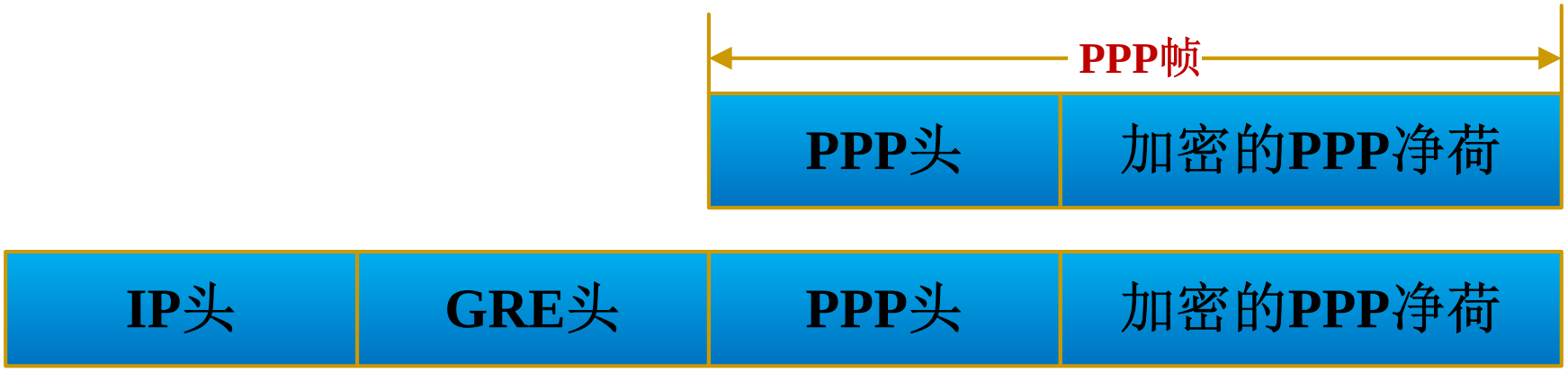
PPTP本身不提供加密服务，只是对先前已加密的PPP帧进行封装。

所谓的“加密”实际上是PPP通过MS-CHAP和EAP-TLS协议建立会话密钥。

然后再对净荷部分采用MPPE机制进行加密。

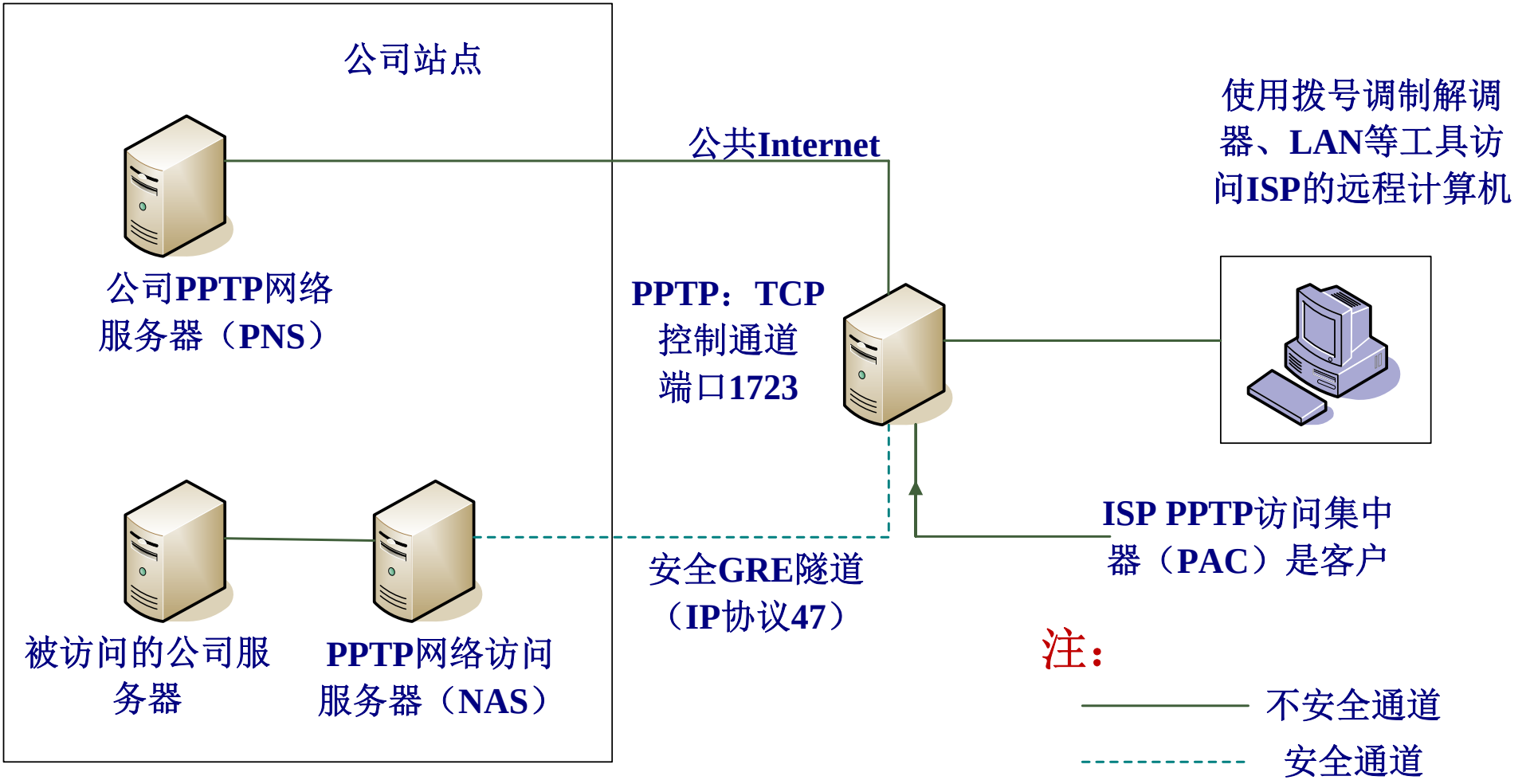
14.5.1 PPTP VPN概述

- PPP帧在PPTP中的数据封装方式



14.5.2 PPTP VPN的原理

PPTP VPN构成示意图



14.5.2 PPTP VPN的原理

- PPTP基于C/S结构，它将认证和连接设置功能分离开来，在其他类型的VPN中，这两个功能是统一的。
- PPTP正是利用了“NAS功能分解”机制的支持，才能在Internet上实现VPN。
- PPTP定义了三个功能实体：

1. PPTP访问集中器（PAC，PPTP Access Server）
2. 网络访问服务器（NAS，Network Access Server，有时称RAS）
3. PPTP网络服务器（PNS，PPTP Network Server）

14.5.2 PPTP VPN的原理

建立PPTP连接

- 首先需要建立客户端与本地ISP的PPP连接。
- 成功接入Internet，再就是建立PPTP连接。
- 从最顶端的PPP客户端、PAC 和PNS服务器之间开始，由已经安装好PPTP的PAC建立并管理PPTP任务。

14.5.3 PPTP VPN的优缺点

思路

- 远程Windows用户通过拨号网络中的远程访问服务（RAS）与本地ISP进行PPP拨号连接。
- 当PPP连接建立后，VPN客户再使用VPN连接选项进行二次拨号。

优点

- 它不依赖于TCP/IP协议族，可以与Novell的IPX或Microsoft的NetBEUI协议一起使用。

缺点

- 由于PPTP中没有定义加密功能，使PPTP VPN的安全性在所有类型的IP VPN中最低。

PPTP与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。
- 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。

第14章 VPN技术

一 VPN的基本概念和分类

二 PPTP、IPSec、TLS等隧道协议

三 IPSec VPN的原理及应用

四 TLS VPN的原理及应用

五 PPTP VPN的原理及应用

六 MPLS VPN的原理及应用

14.6.1 MPLS VPN的概述

- 多协议标记交换(MPLS:Multiprotocol Label Switching)
- MPLS VPN是一种基于MPLS技术的IP VPN。
- MPLS技术可以大大加快路由器交换和转发数据包的速度。
- MPLS由Cisco的标记交换技术演变而来，已成为IETF的标准协议，是标记转发的典范。
- 与传统的网络层技术相比，它引入了以下一些新概念：

流（Flow）、标记（Label）、标记交换（Label Swap）、MPLS节点（MPLS Node）、MPLS域（MPLS Domain）、MPLS边界节点（MPLS Edge Node）、标记交换路径（LSP，Label Switched Path）、标记交换路由器（LSR，Label Switching Router）、标记分发协议（LDP，Label Distribution Protocol）

14.6.2 MPLS VPN的原理

- MPLS VPN中，每个VPN子网分配一个独一无二的标示符，它与用户的地址连接形成转发表中独一无二的地址（VPN-IP地址）。
- VPN转发表中包括与VPN-IP地址对应的标签，通过它将数据送到相应地址。

这种方案的优势：

- 通过相同的网络结构支持多种VPN，不必为每一个用户建立单独的VPN网络连接。
- 服务提供商可以为租用者配置一个网络以提供专用的IP网服务，而无须管理隧道。
- QoS服务可与MPLS VPN无缝结合，为每个VPN网络提供特有的业务策略。
- MPLS VPN用户能够使用他们专有的IP地址上网，无须网络地址转换（NAT）帮助。

14.6.3 MPLS VPN的优缺点

优点

- 降低了成本。
- 方便了用户
- 提高了资源利用率
- 安全性高
- 提高了网络速度
- 业务综合能力强
- 提高了灵活性和可扩展性
- MPLS的QoS保证
- 适用于城域网（PAN）这样的网络环境

缺点

- 由于ATM技术本身目前备受争议，故MPLS VPN的价值大打折扣。
- 本身没有采用加密机制，因此MPLS VPN实际上并不十分安全。

本章小结

- VPN的概念、分类
- VPN的关键技术：隧道技术、身份认证、访问控制、密码技术、密钥管理
- 不同层次的VPN技术：
  - 二层：L2F、PPTP、L2TP
  - 三层：IPSec、GRE
  - 四层：SSLVPN
- IPSecVPN
  - 主要协议：
    - AH：认证头协议，主要功能：验证，NAT穿越问题
    - ESP：主要功能：加密、验证，无NAT穿越问题
    - IKE：密钥交换，分两个阶段
  - 运行模式：
    - 隧道模式：用于任何通道
    - 传输模式：仅用于主机到主机的安全通道
  - 术语：SA、SAD、SP、SPD

本章小结（续）

- SSLVPN：
  - SSLVPN特点
  - TLS协议：握手协议、告警协议、记录协议
  - SSLVPN分类：基于Web、端口转发、隧道方式
- PPTP VPN
- MPLS VPN

谢谢！