专业特色选修课《网络信息安全》

协议安全和VPN技术

Protocol Security and Virtual Private Network

嵩天 教授、博士生导师

songtian@bit.edu.cn

北京理工大学网络空间安全学院

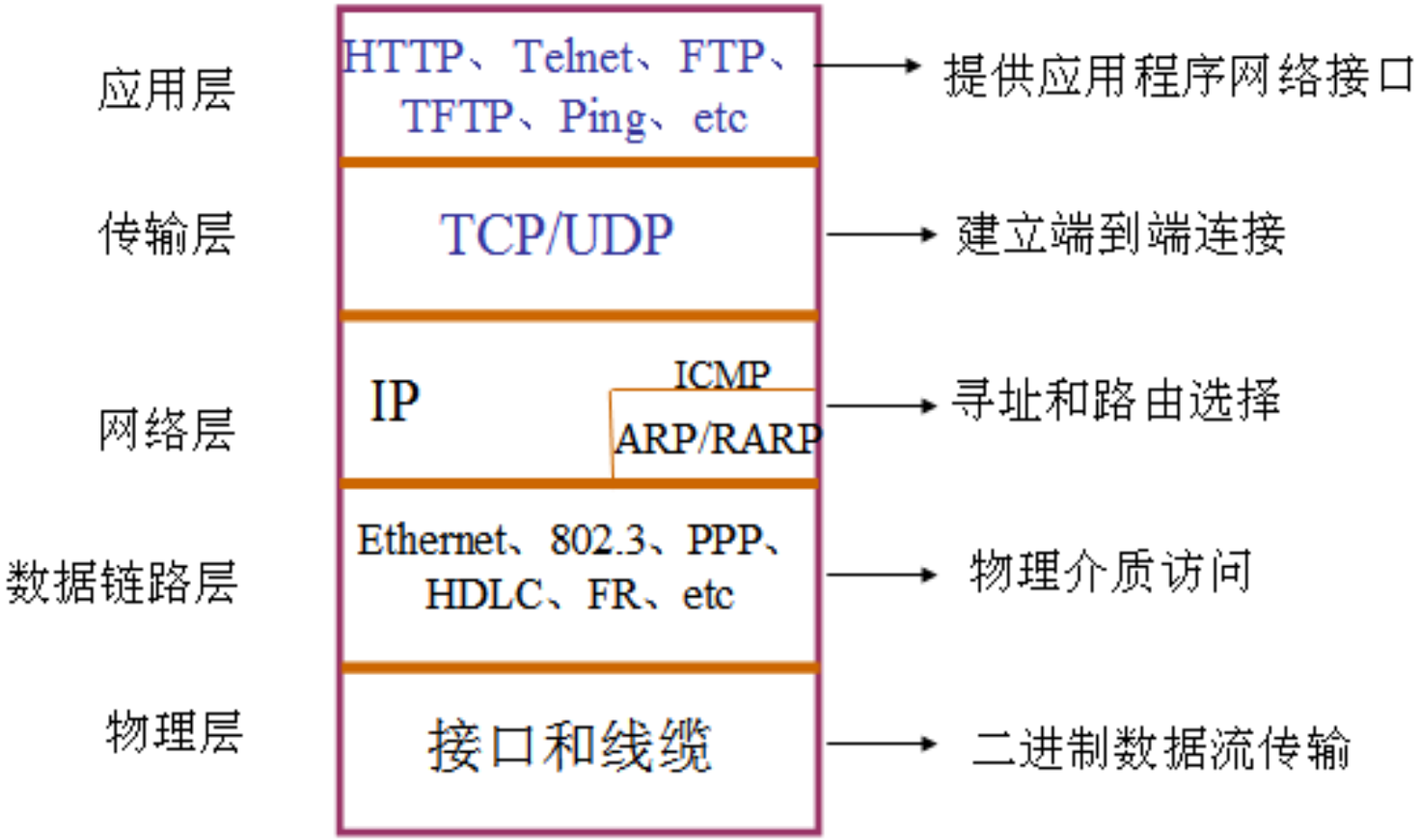
放假回家，想登陆校园网，怎么办？

本节大纲

- 网络协议安全分析
- 安全协议：IPSec
- 安全协议：SSL (TLS)
- VPN技术

北京理工大学 网络信息安全 肖天

网络协议安全分析


应用层
HTTP、Telnet、FTP、
TFTP、Ping、etc
提供应用程序网络接口
传输层
TCP/UDP
建立端到端连接
网络层
IP
ICMP
ARP/RARP
寻址和路由选择
数据链路层
Ethernet、802.3、PPP、
HDLC、FR、etc
物理介质访问
物理层
接口和线缆
二进制数据流传输

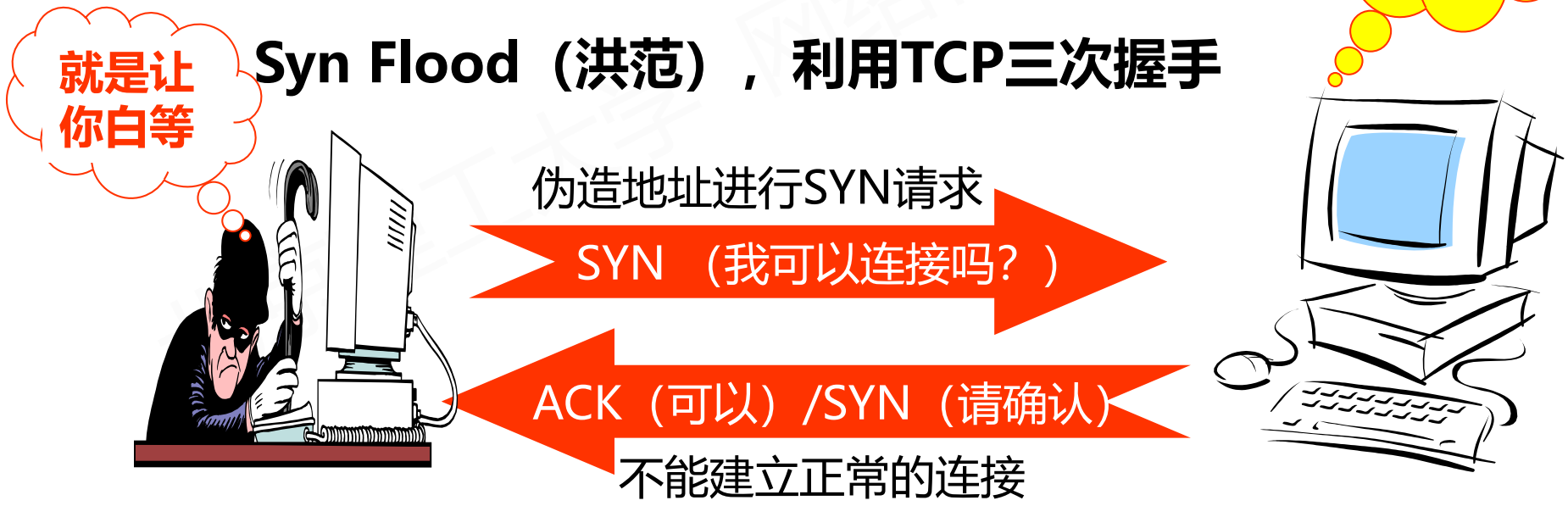
网络协议安全分析

- **网络层**
  - **IPv4协议在设计之初没有考虑安全性**
  - **IP包本身不具备任何安全特性**
  - **网络层的安全威胁主要有**

IP欺骗和ICMP攻击（单向告之）

网络协议安全分析

- **传输层**
  - **TCP和UDP，在设计之初没有考虑安全性**
  - **传输层的安全威胁举例：**
    - **Syn Flood（洪范），利用TCP三次握手**



网络协议安全分析

- **应用层**
  - **包括几百种应用层协议**
  - **安全隐患举例：Telnet、FTP、SMTP、HTTP、NFS等**
  - **Telnet协议**

    以明文的方式发送所有的用户名和密码
  - **FTP协议**

    FTP的可写匿名连接是黑客寻找的目标

网络协议安全分析

- **互联网安全隐患的根源是TCP/IP协议的缺陷**
  - **网络层、传输层存在安全性上的设计缺失**
  - **应用层存在大量的安全隐患，可弥补**
  - **如何在网络层、传输层提高Internet的安全性：**
    - **网络层：IPSec协议族**
    - **传输层：SSL/TLS协议族**

本节大纲

- 网络协议安全分析
- 安全协议：IPSec
- 安全协议：SSL (TLS)
- VPN技术

北京理工大学 网络信息安全 肖天

IPSec概述

- 什么是IPSec?
  - Internet Protocol Security（IPSec），协议族
  - IPSec是保护IP协议安全通信的标准，工作在第三层
  - 将密码安全机制引入IP协议
  - IPSec主要对IP协议分组进行加密和认证
  - IPv6是必须的，对IPv4是可选的
  - 详细：RFC 2401

IPSec概述

- **IPSec包含的具体协议**
  - **AH（认证头）协议**
    - **对整个数据包（除部分字段）进行认证**
    - **AH没有加密性，详细：RFC2402**
  - **ESP（封装安全载荷）协议**
    - **对网络包有效载荷（payload）进行加密**
    - **详细：RFC2406**

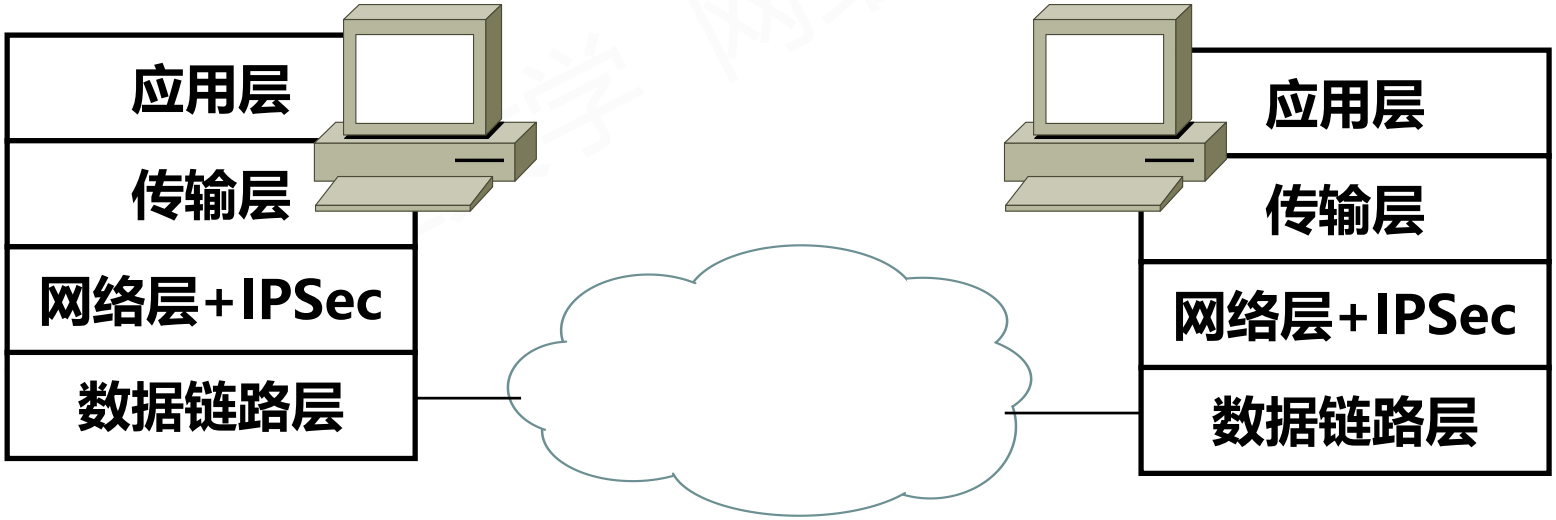
IPSec的工作模式

- 传输模式
- 隧道模式

北京理工大学网络信息安全 蒋天

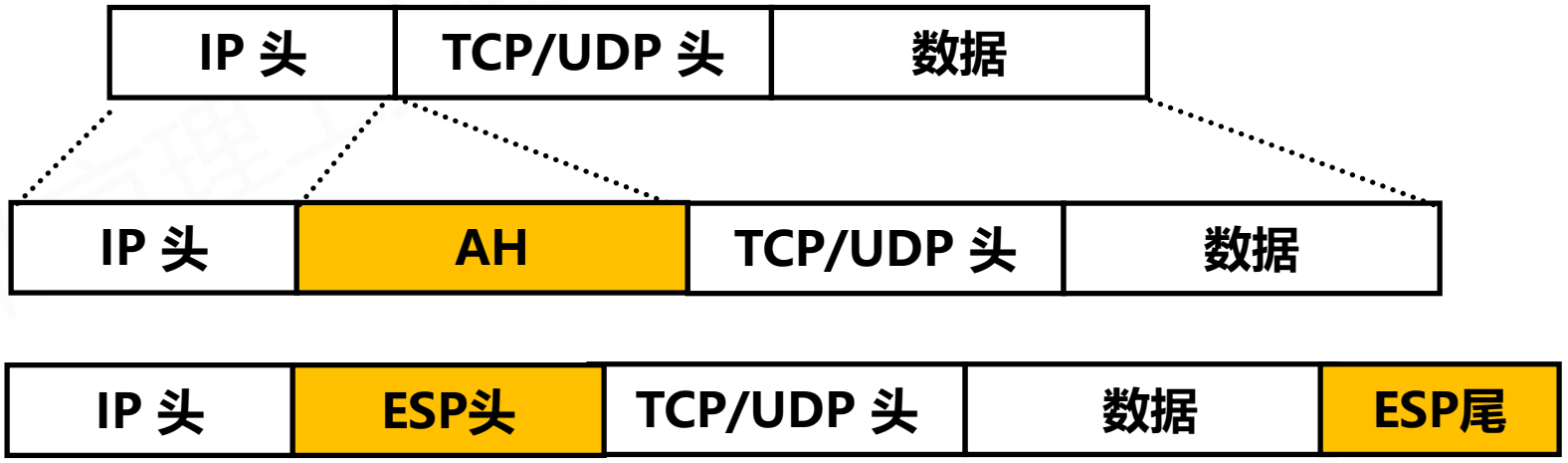
IPSec的工作模式

- **传输模式**
  - 在主机上实现，与操作系统集成
  - 针对用户每个会话提供安全保障



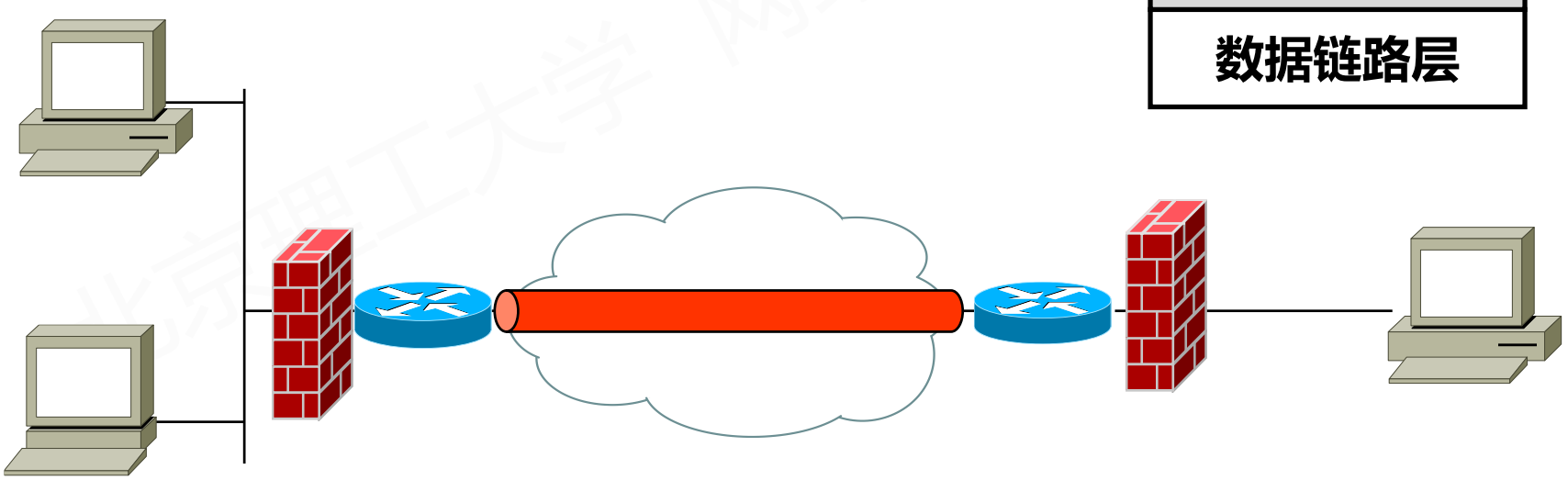
IPSec的工作模式

- **传输模式**
  - 传输模式用于两台主机之间，保护端到端的安全
  - 只对IP数据包的有效负载进行加密或认证
  - 继续使用以前的IP头部，只对IP头部的部分域进行修改



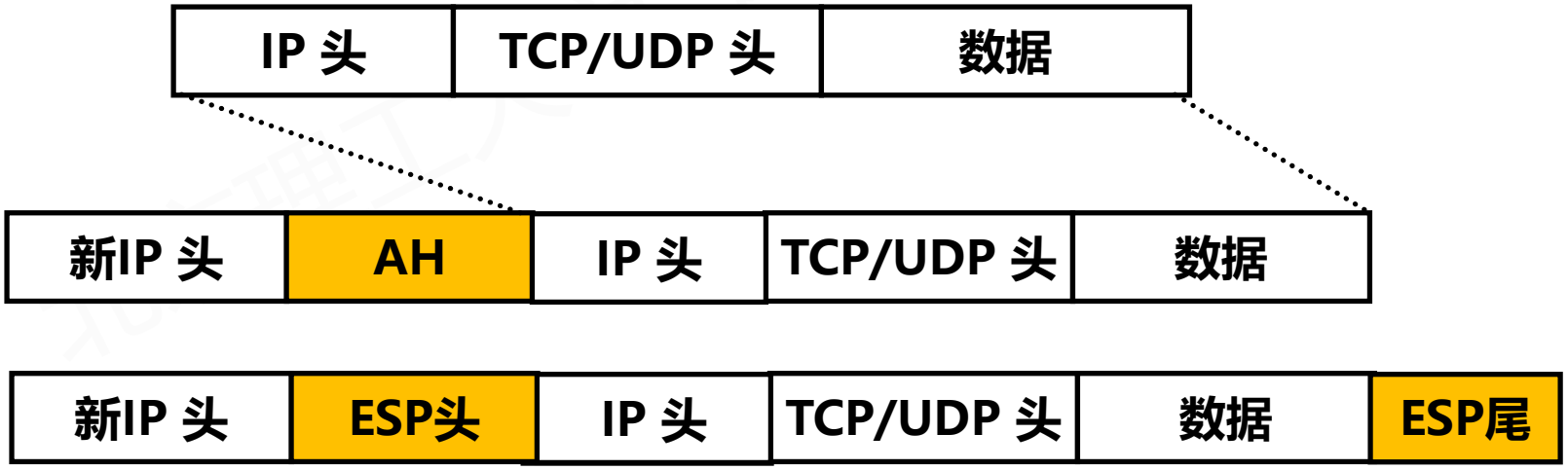
IPSec的工作模式

- **隧道模式**
  - 无需改变操作系统
  - 为局域网内部所有应用提供服务



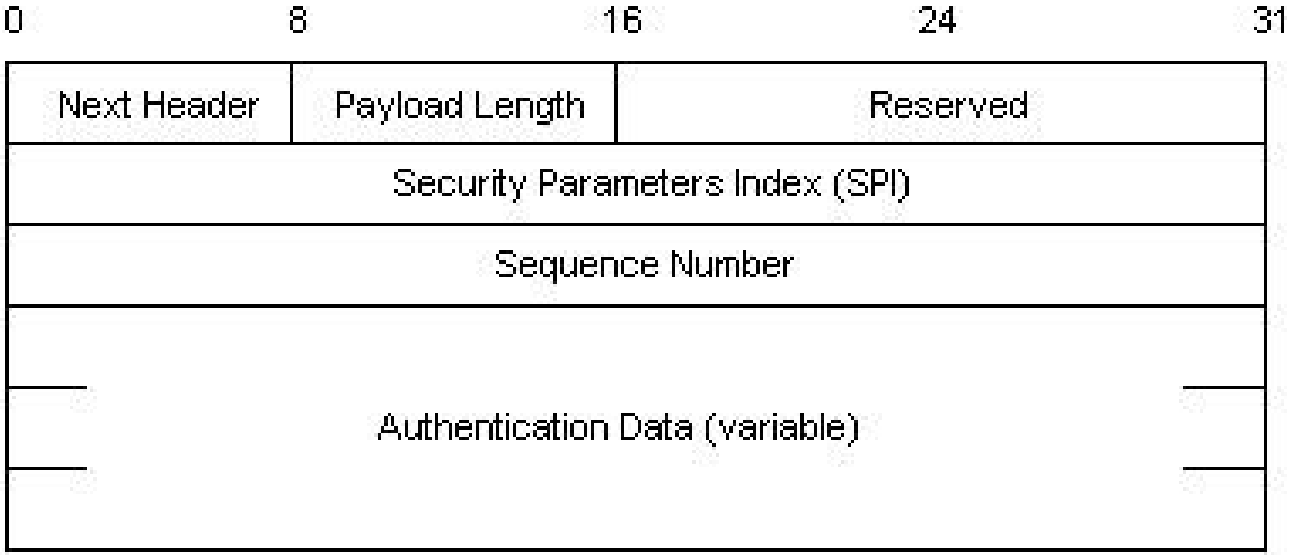
IPSec的工作模式

- **隧道模式**
  - 主机与路由器或路由器之间，保护整个IP数据包
  - 对整个IP数据包进行加密或认证
  - 需要新产生一个IP头



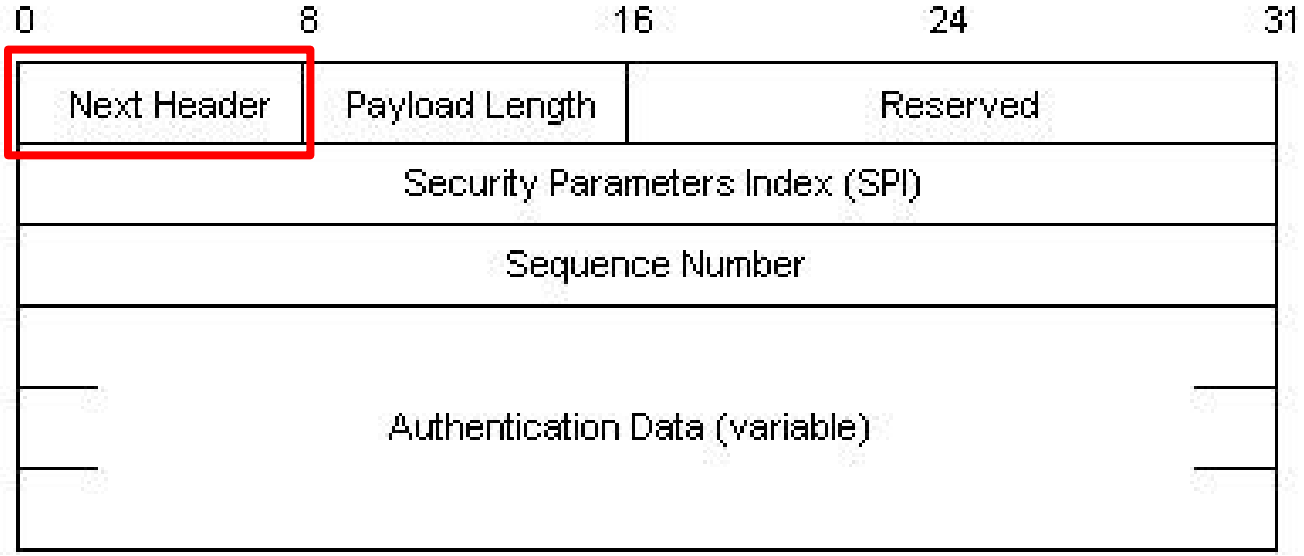
IPSec的认证头

- **认证头（AH）**
  - **AH：Authentication Header**
  - **AH被用来保证被传输分组的完整性和可靠性**



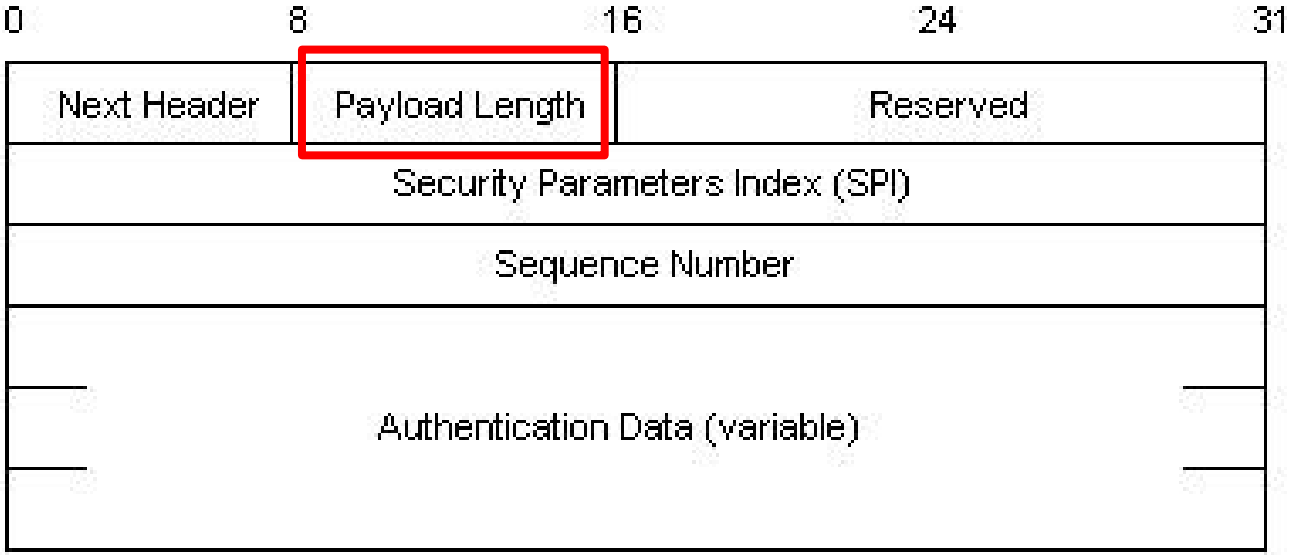
IPSec的认证头

- **Next header（下一个报头）**
  - **8 bit，标识数据载荷中的封装方式或协议**
  - **RFC中定义：0x06-TCP，0x11-UDP协议**



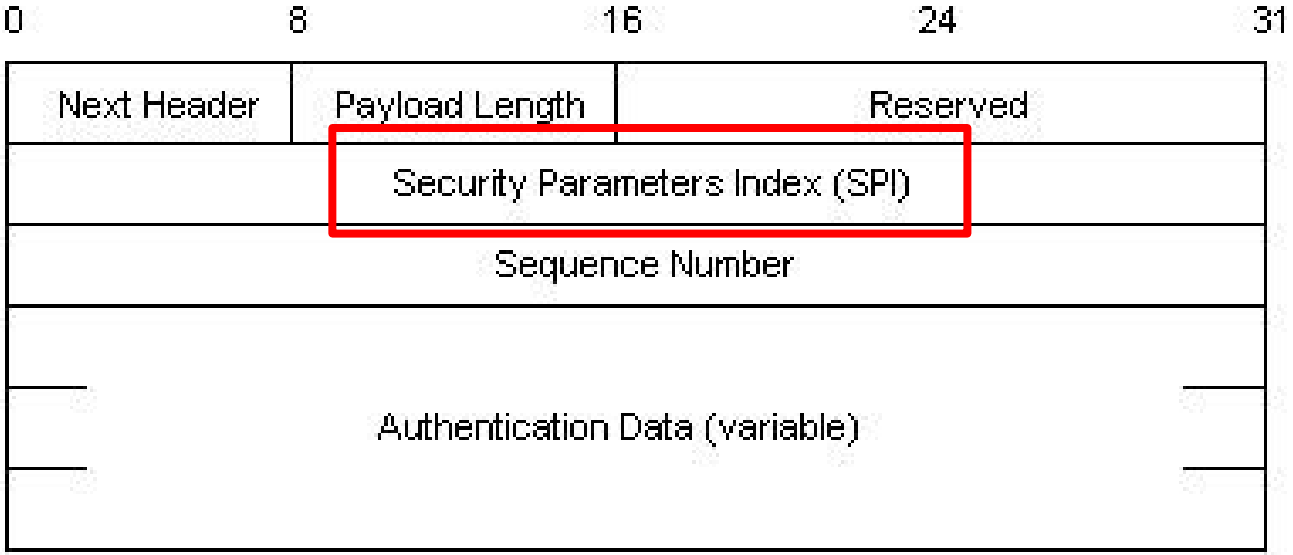
IPSec的认证头

- Payload length（有效载荷长度）
  - 8bit，以 32 位字为单位的认证数据字段的长度
  - AH的长度



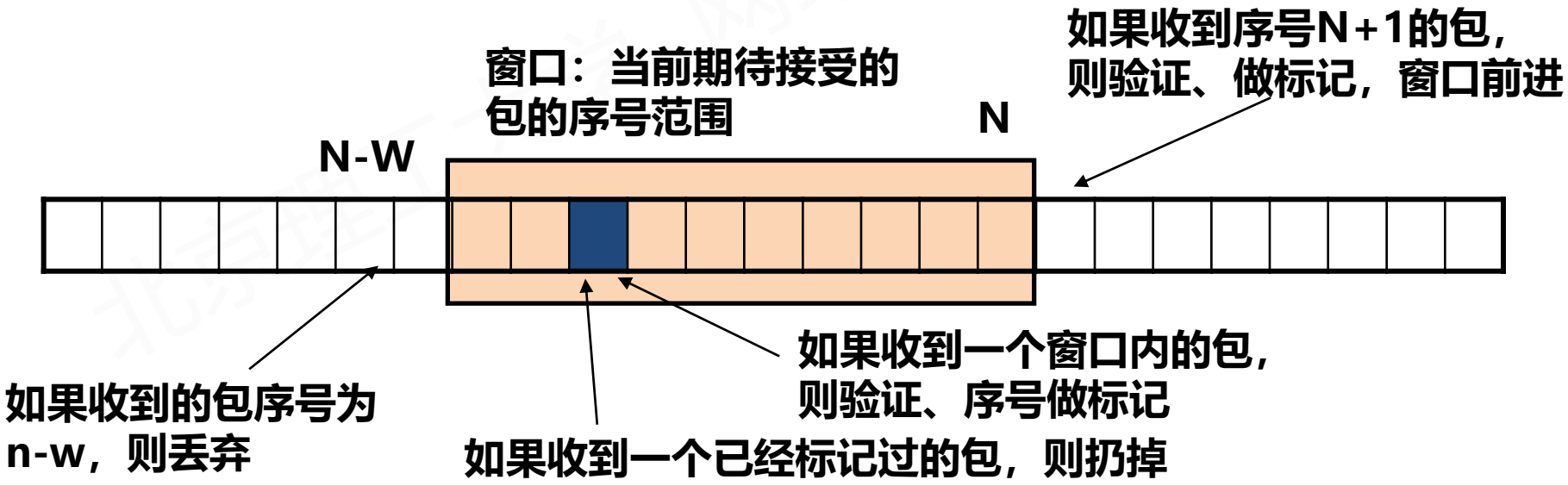
IPSec的认证头

- **Security parameters index （SPI）**
  - **32bit，为数据报识别安全关联的 32 位伪随机值**
  - **SPI 值0，表明“没有安全参数存在”**



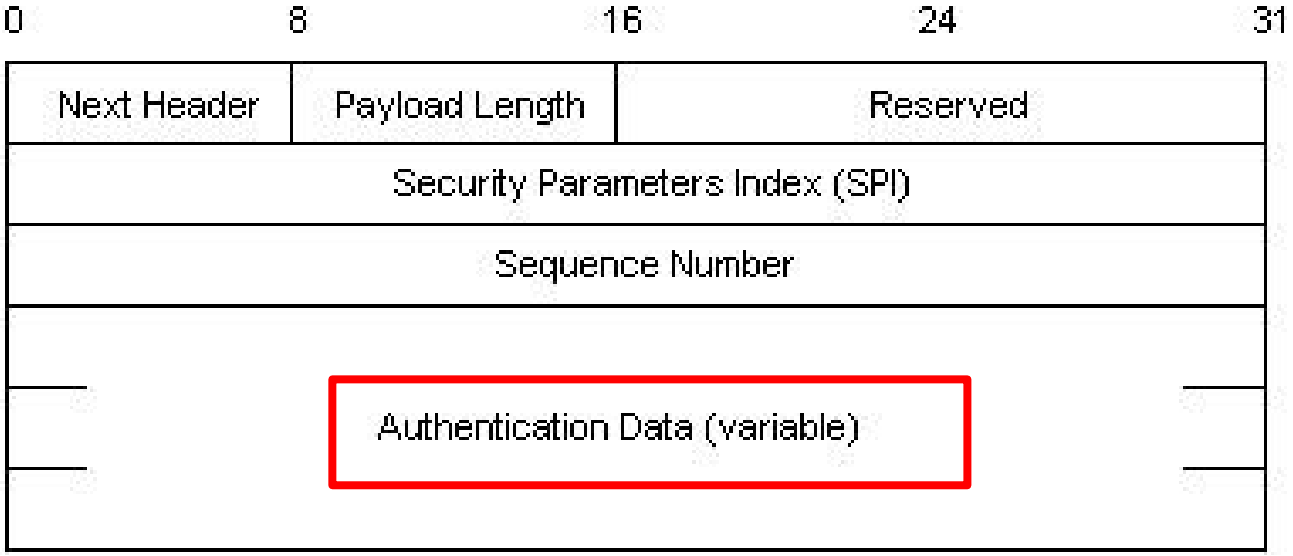
IPSec的认证头

- **Sequence Number（序列号）**
  - 32bit，单调递增的计数器，用来防止重放攻击
  - 重放攻击：攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程



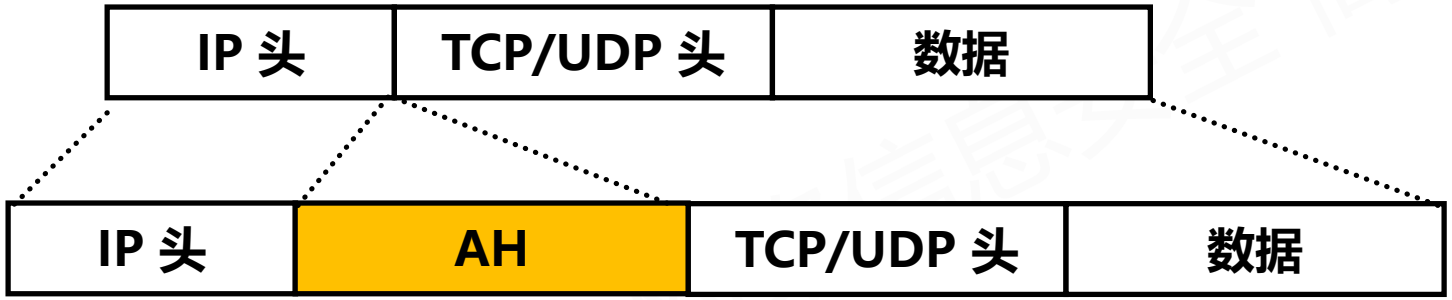
IPSec的认证头

- **Authentication Data（认证数据）**
  - **包含了认证当前包所必须的数据，类似checksum**
  - **支持算法：HMAC-MD5-96、HMAC-SHA-1-96，**

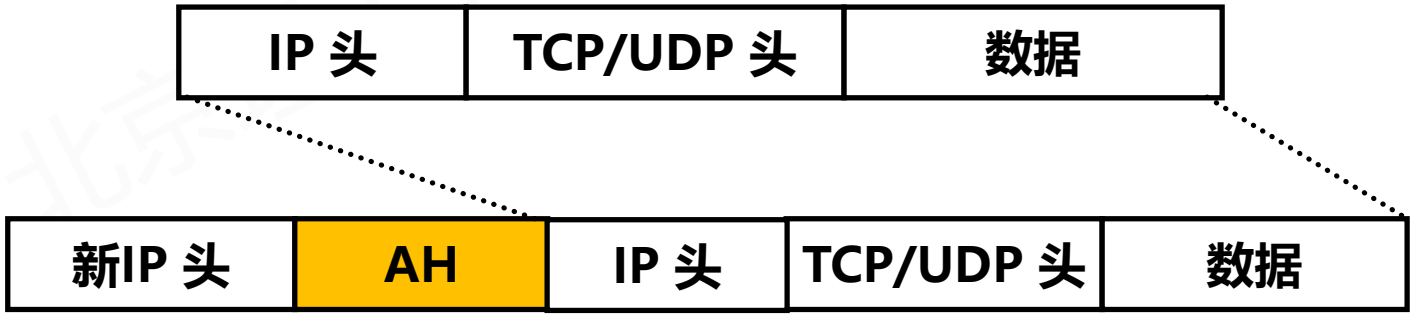


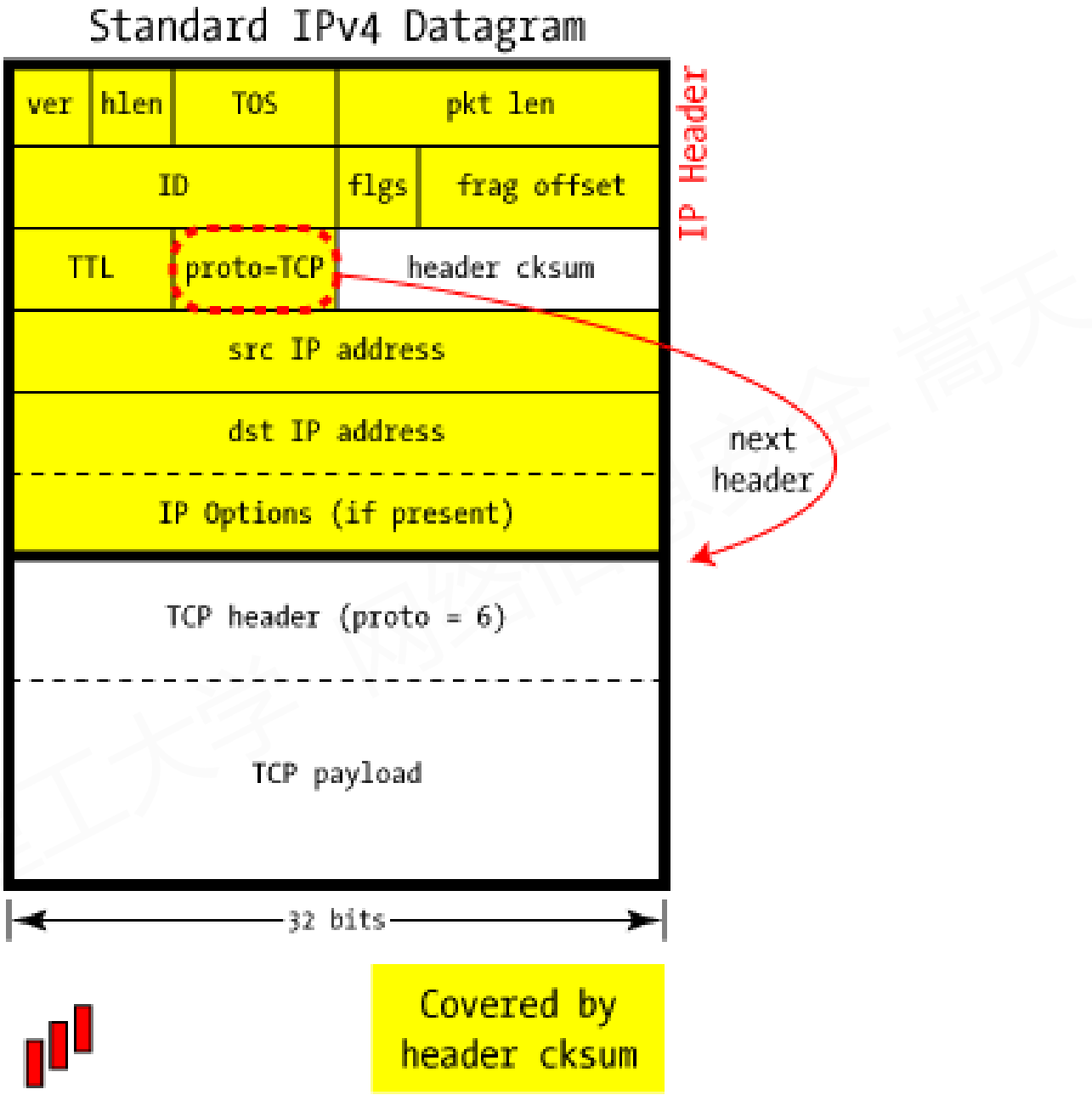
AH协议的工作模式

- **传输模式**

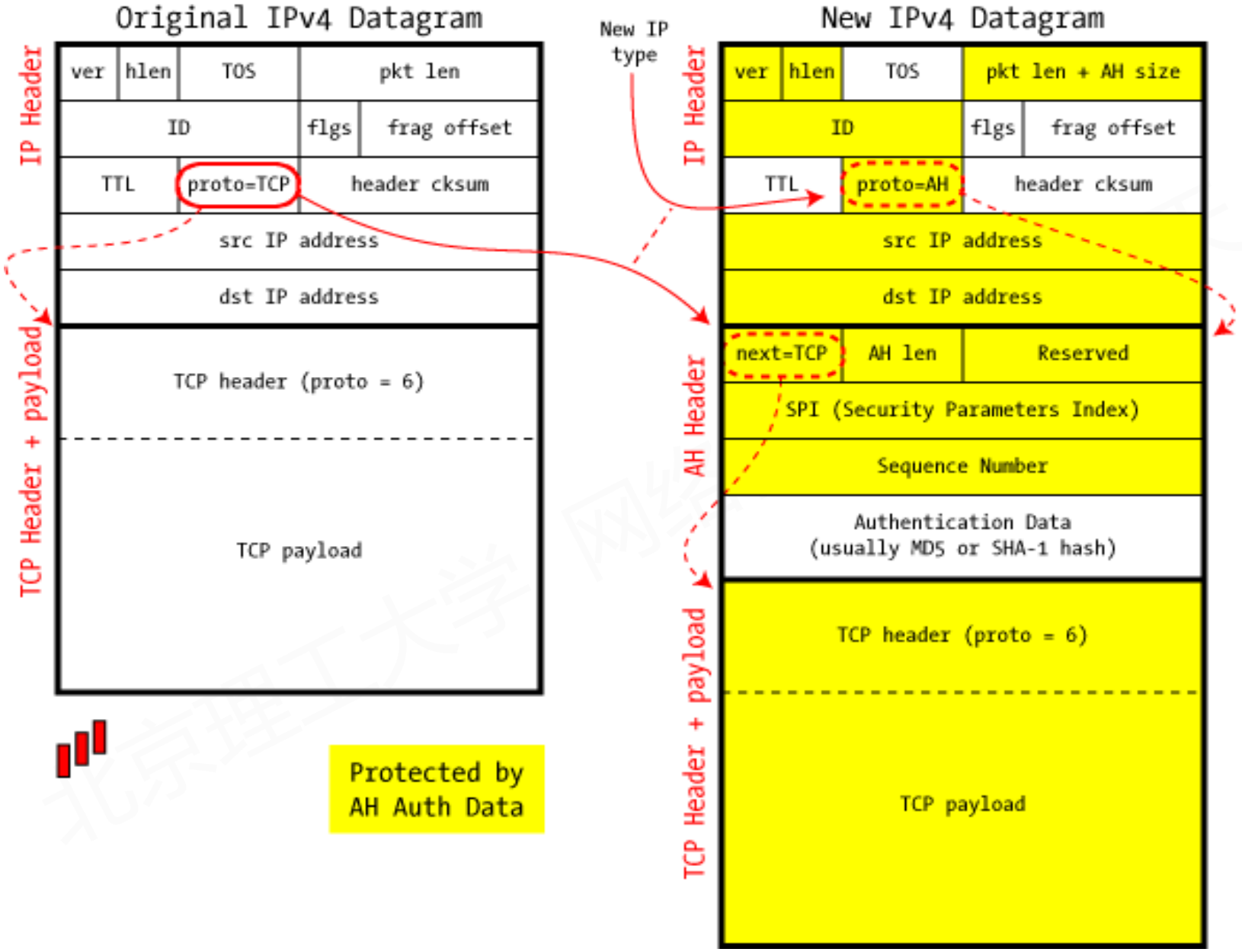


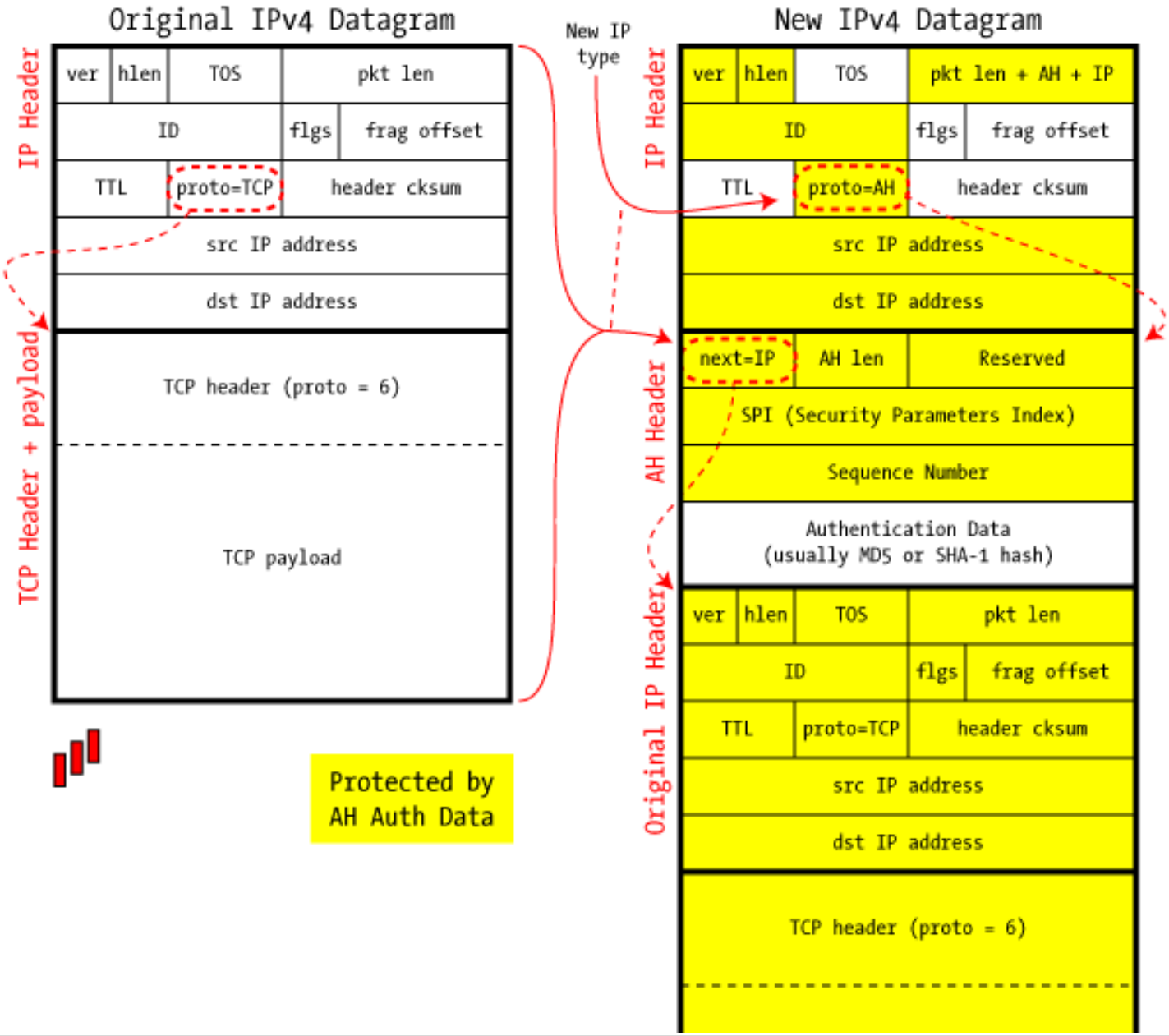
- **隧道模式**



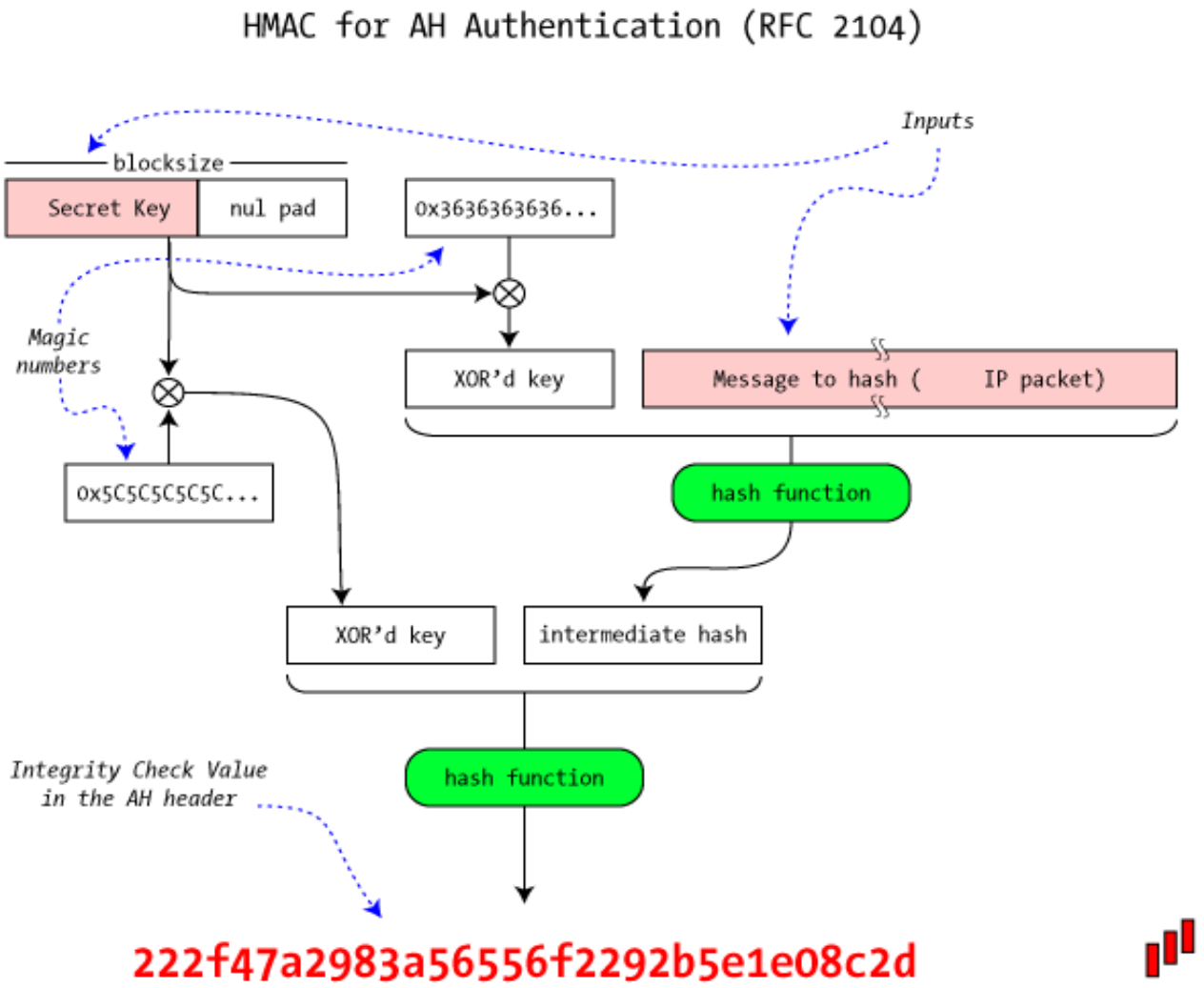

Standard IPv4 Datagram
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
proto=TCP
header cksum
src IP address
dst IP address
IP Options (if present)
IP Header
next header
TCP header (proto = 6)
TCP payload
32 bits
Covered by header cksum

IPSec in AH Transport Mode




IPSec in AH Tunnel Mode
Original IPv4 Datagram
IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
proto=TCP
header cksum
src IP address
dst IP address
TCP Header + payload
TCP header (proto = 6)
TCP payload
New IP type
Protected by AH Auth Data
New IPv4 Datagram
IP Header
ver
hlen
TOS
pkt len + AH + IP
ID
flgs
frag offset
TTL
proto=AH
header cksum
src IP address
dst IP address
AH Header
next=IP
AH len
Reserved
SPI (Security Parameters Index)
Sequence Number
Authentication Data
(usually MD5 or SHA-1 hash)
Original IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
proto=TCP
header cksum
src IP address
dst IP address
TCP header (proto = 6)

IPSec的认证头

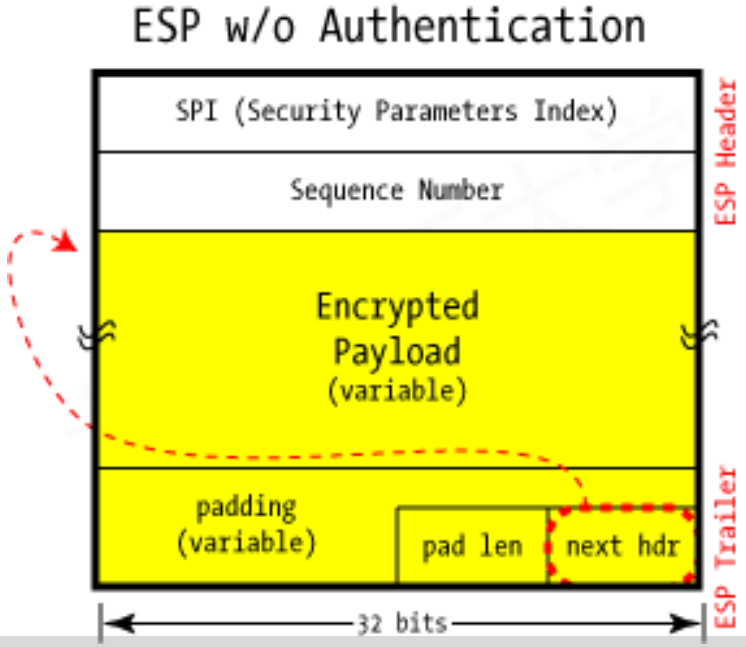

HMAC for AH Authentication (RFC 2104)
Inputs
blocksize
Secret Key
nul pad
0x3636363636...
Magic numbers
XOR'd key
Message to hash (IP packet)
0x5C5C5C5C5C...
hash function
XOR'd key
intermediate hash
hash function
Integrity Check Value in the AH header
222f47a2983a56556f2292b5e1e08c2d

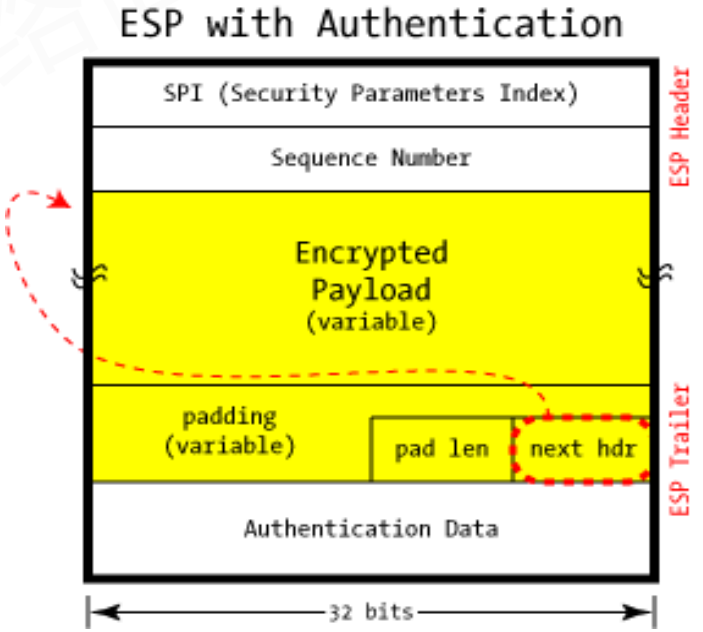
IPSec的认证头

- **几个问题**
  - **AH为何不对整个IP包进行认证?**
  - **AH中Auth Data为何采用Hash方法，而不是checksum?**
  - **AH中Auth Data可否采用其他Hash算法?**
  - **能否从IPSec包中判断出两种工作模式?**

封装安全负载协议

- **封装安全负载（ESP）**
  - **ESP：Encapsulating Security Payload，用来加密**
  - **包括两种方式：带有认证和不带认证，RFC2406**





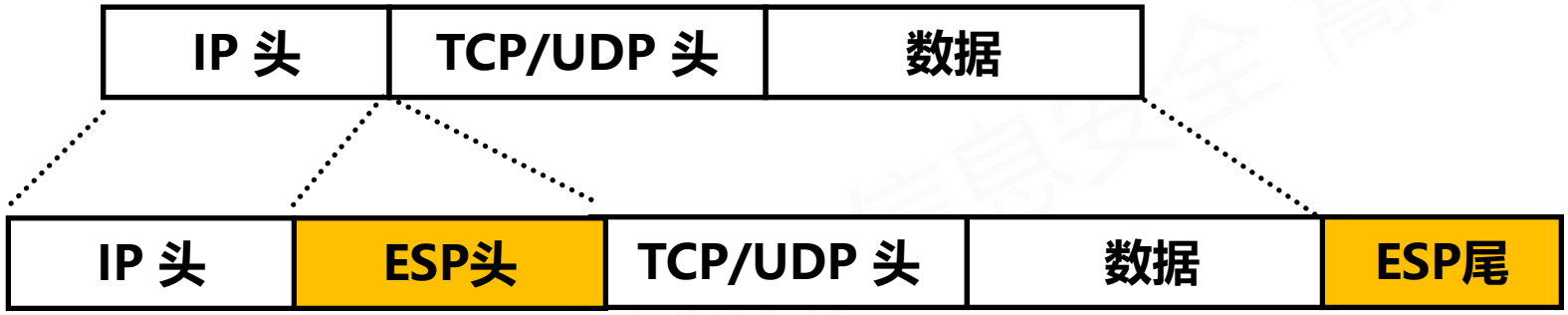
封装安全负载协议

- **加密算法**
  - **密码分组链模式的DES(CBC –DES)**
  - **3DES**
  - **RC5**
  - **IDEA**
  - **CAST**
  - **Blowfish**
  - **其他算法**

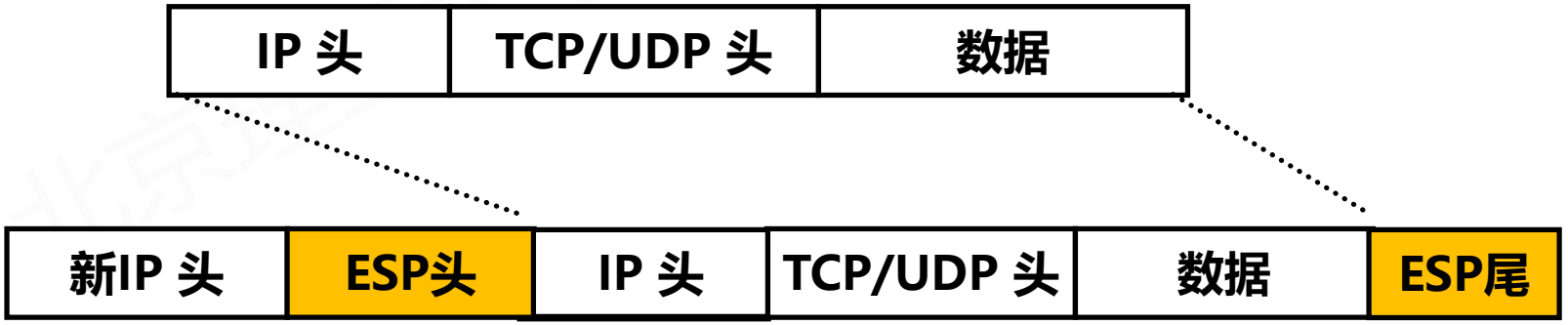
北京理工大学 网络信息安全 蒋天

ESP的工作模式

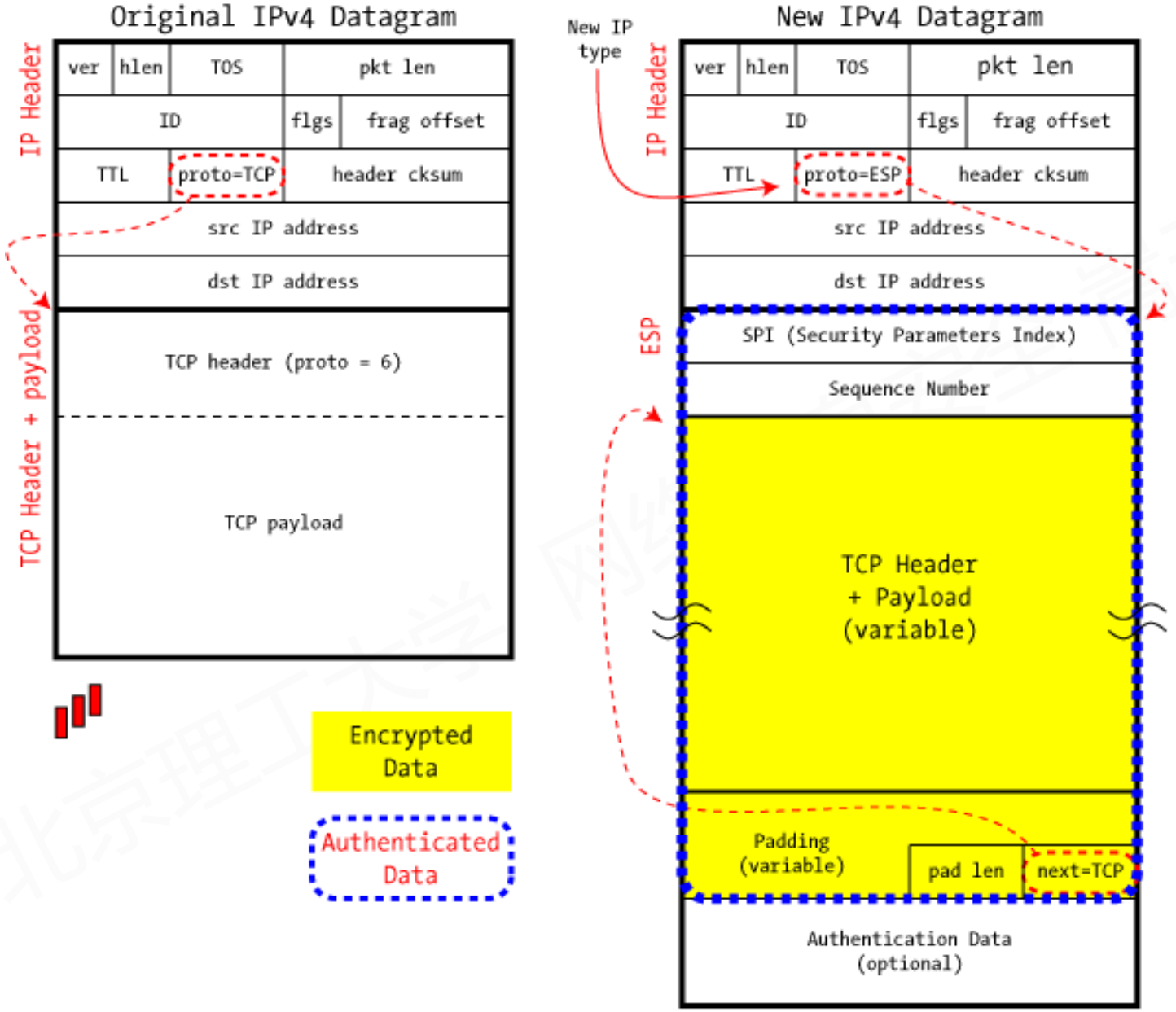
- **传输模式**



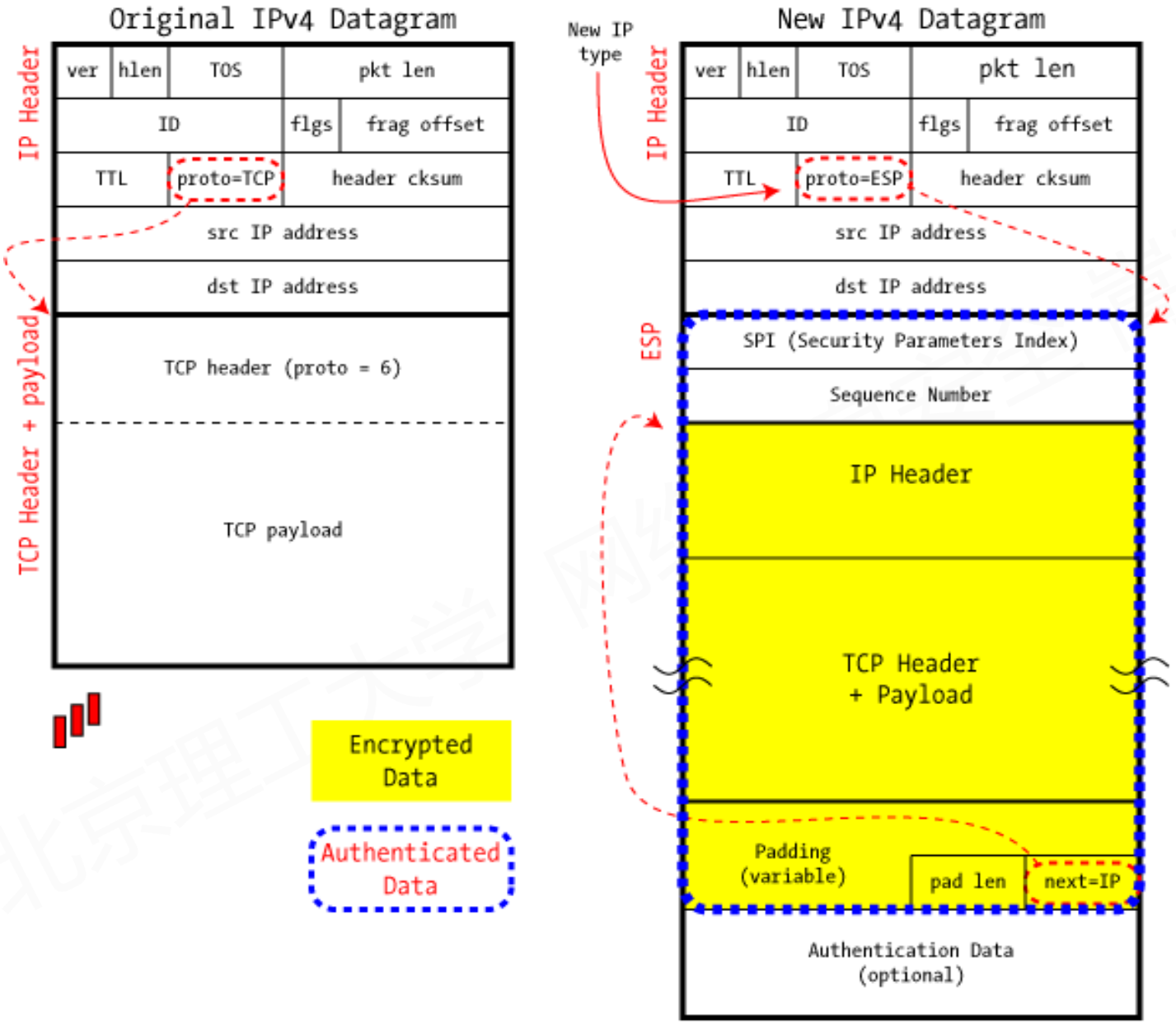
- **隧道模式**



IPSec in ESP Transport Mode



IPSec in ESP Tunnel Mode



本节大纲

- 网络协议安全分析
- 安全协议：IPSec
- 安全协议：SSL (TLS)
- VPN技术

北京理工大学 网络信息安全 肖天

SSL概述

- 什么是SSL?
  - SSL：Secure Sockets Layer，安全套接层
  - TSL：Transport Layer Security，传输层安全
  - 保证网络通信提供安全及数据完整性的安全协议
  - TLS和SSL在传输层对网络连接进行加密
  - TLS和SSL与应用层协议无关
  - 详细：RFC 5246

SSL概述

- **SSL的通信目标**
  - **机密性**

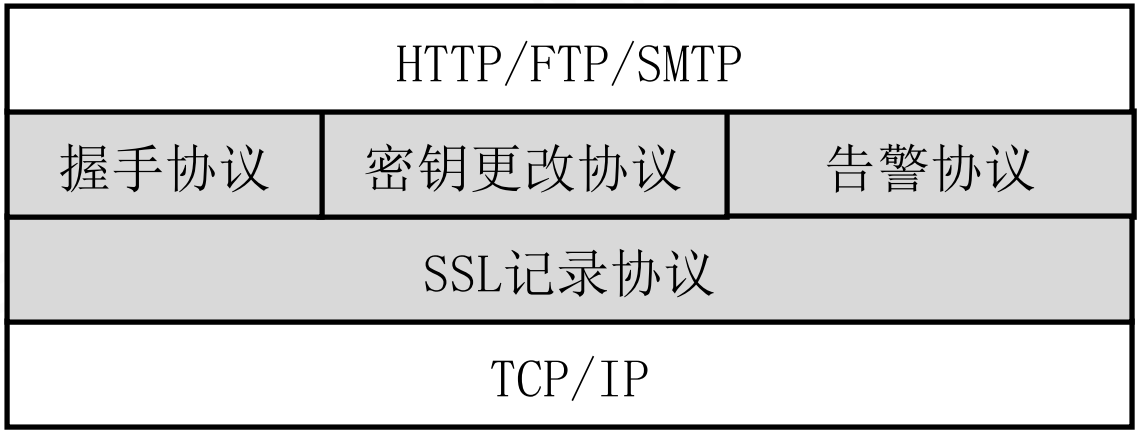
    SSL客户机和服务器之间的数据都经过了加密处理，网络中非法窃听者获得的都是加密后的密文。
  - **完整性**

    利用密码算法和散列（Hash）函数保证数据的完整性
  - **不可否认性**

    利用证书技术和可信的第三方认证，可以让客户机和服务器相互识别对方的身份，SSL要求证书持有者在握手时交换数字证书。

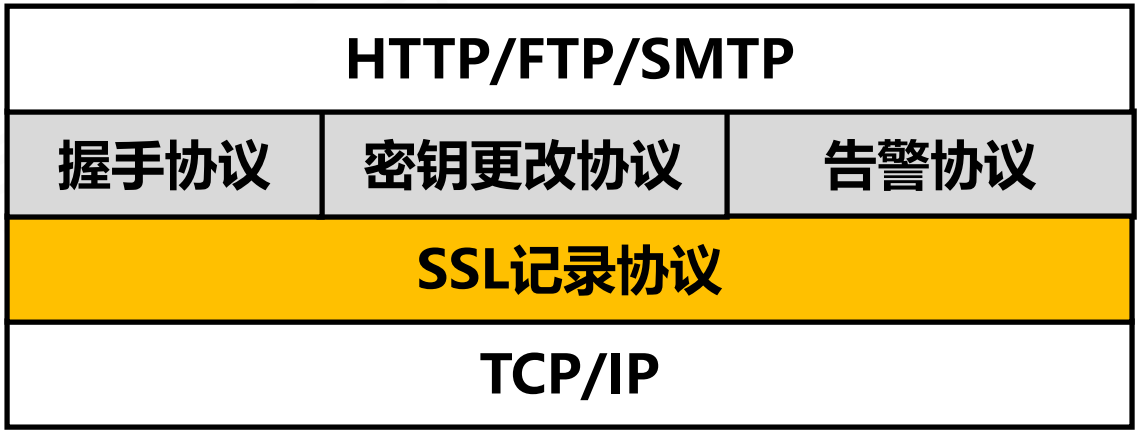
SSL概述

- **SSL的组成**
  - **SSL协议由SSL记录协议、握手协议、密钥更改协议和告警协议组成。**

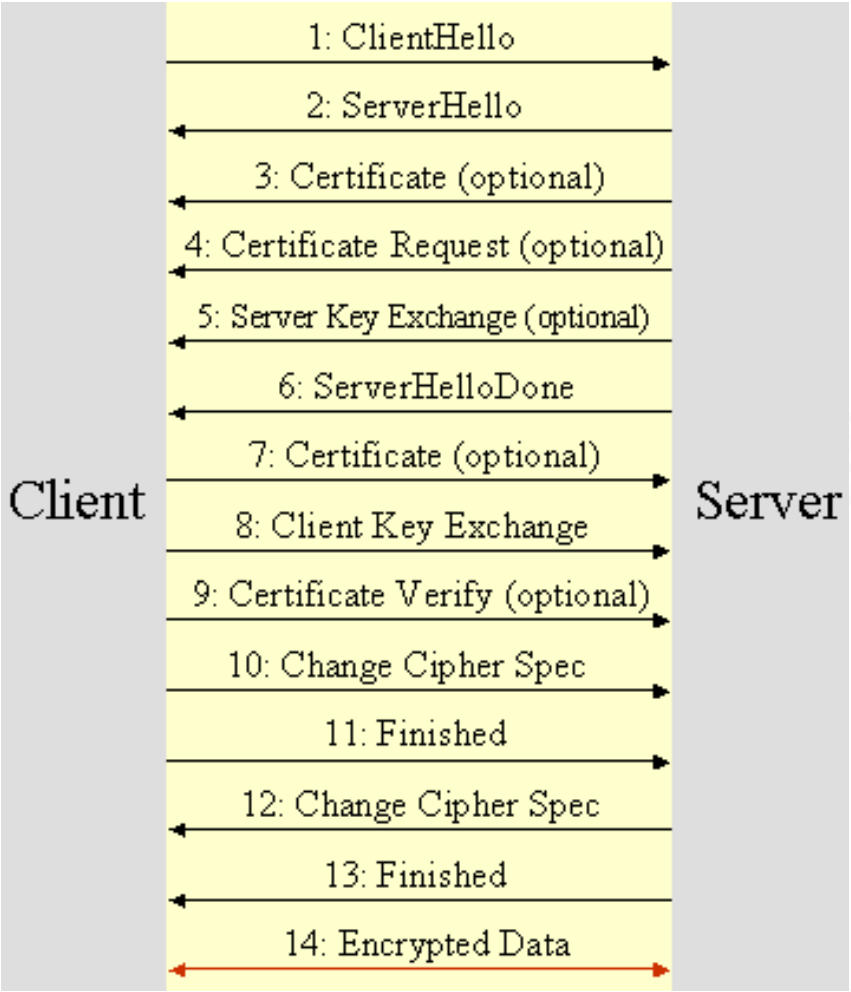


SSL组成

- **SSL记录协议**
  - 为各种高层协议提供基本的安全服务
  - 其工作机制如下：应用程序消息被分割成可管理的数据块(可以选择压缩数据)，并产生一个消息鉴别信息，加密，插入新的文件头，最后在TCP中加以传输；接收端将收到的数据解密，做身份验证、解压缩、重组数据报然后交给高层应用进行处理。



SSL会话过程



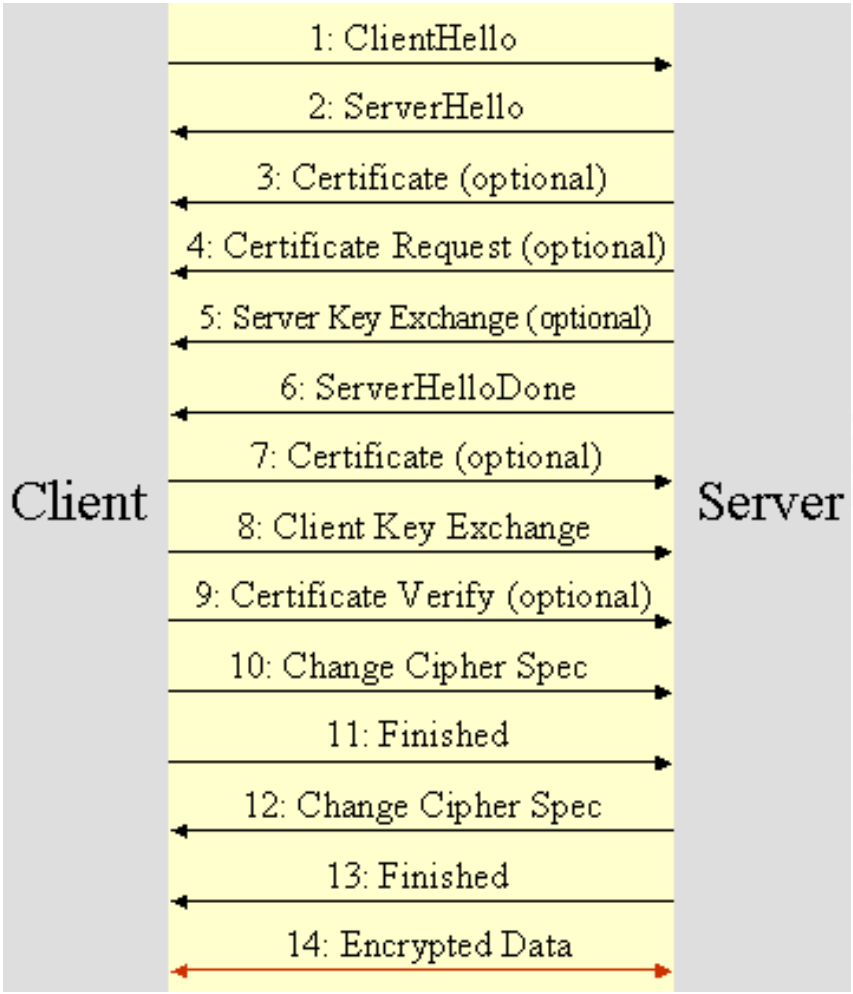
- **1: ClientHello**

  客户端将其SSL版本号、加密设置参数、与session有关的数据以及其它一些必要信息（如加密算法和能支持的密钥的大小等）发送到服务器

- **2: SeverHello**

  服务器将其SSL版本号、加密设置参数、与session有关的数据以及其它一些必要信息发送给客户端。

SSL会话过程



- **3: Certificate**

  服务器发送一个证书或一个证书链到客户端。

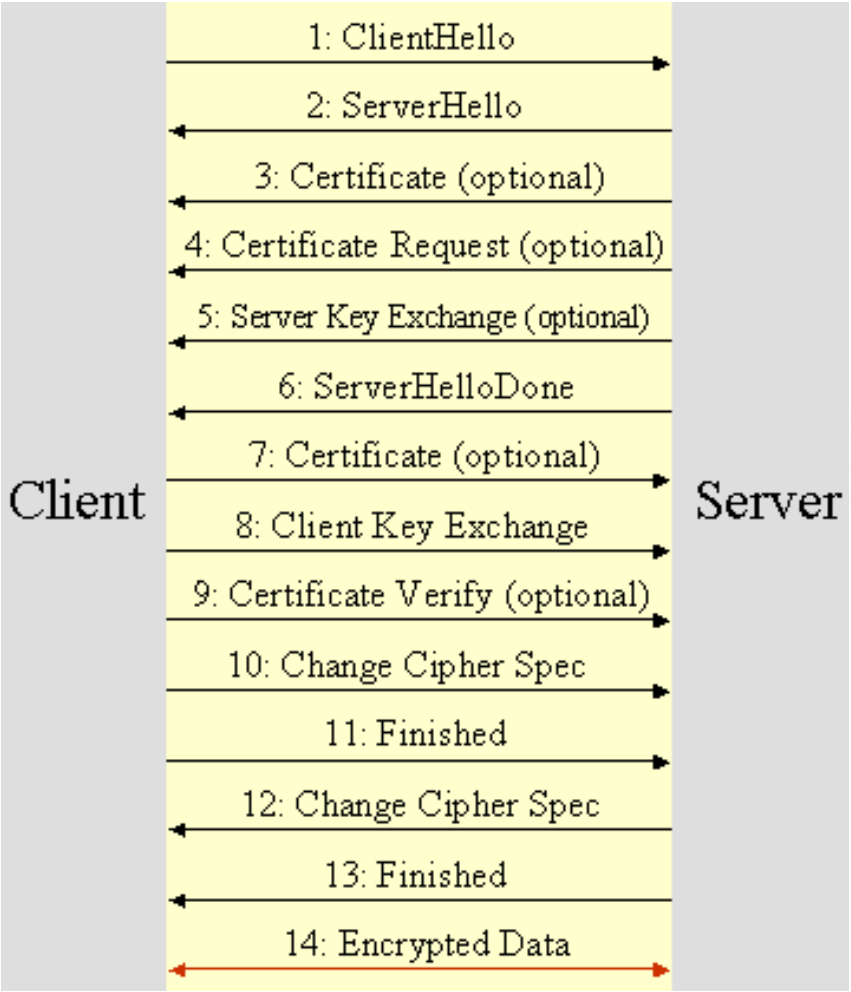
- **4: Certificate Request**

  该消息要求客户端浏览器提供用户证书。

- **5: Server Key Exchange**

  如果服务器发送的公共密钥对加密密钥的交换不是很合适时，则发送一个服务器密钥交换消息。

SSL会话过程



- **6: ServerHelloDone**

  该消息通知客户端，服务器已完成了交流过程的初始化。

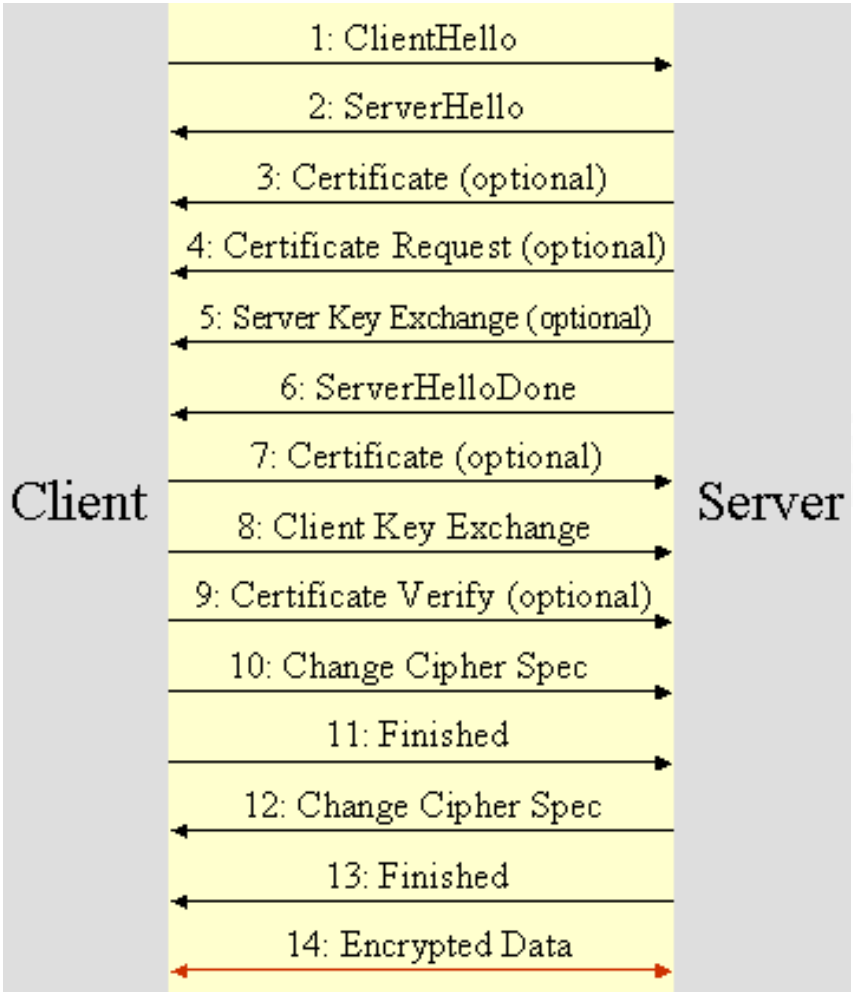
- **7: Certificate**

  客户端发送客户端证书给服务器。

- **8: Client Key Exchange**

  客户端产生一个会话密钥与服务器共享。

SSL会话过程



- **9: Certificate Verify**

  如果服务器请求验证客户端，这个消息允许服务器完成验证过程。

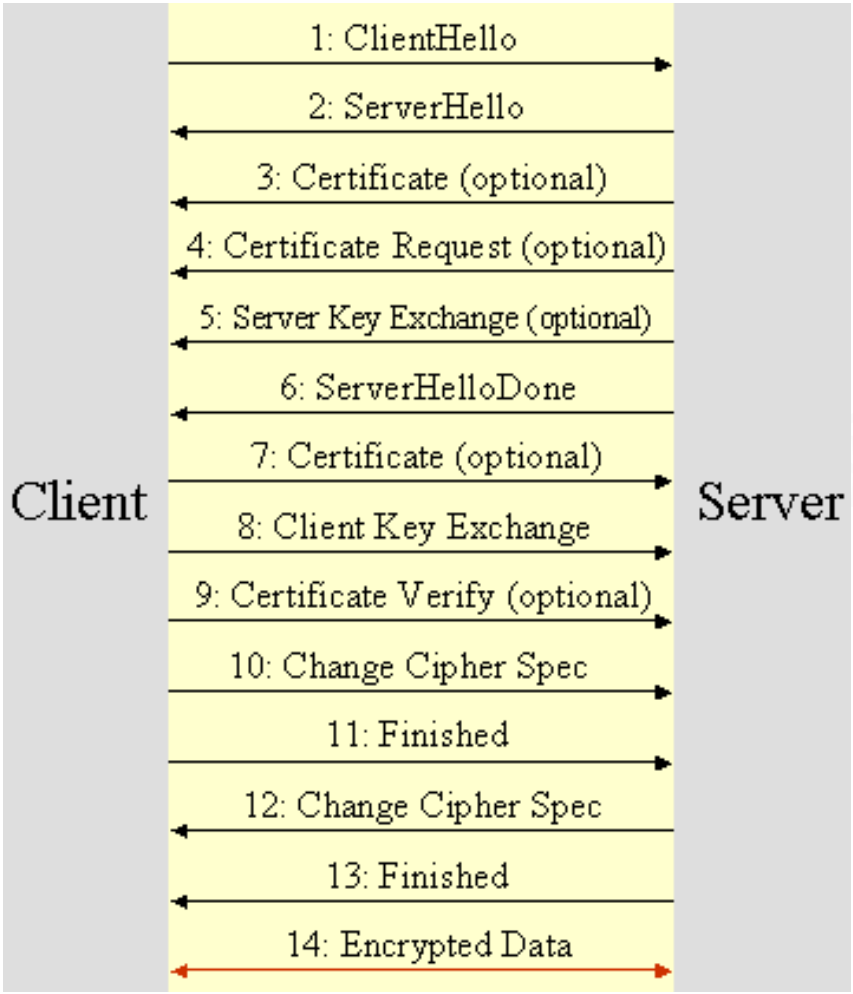
- **10: Change Cipher Spec**

  客户端要求服务器在后续的通讯中使用加密模式。

- **11: Finished**

  客户端告诉服务器它已经准备好安全通信了。

SSL会话过程



- **12: Change Cipher Spec**

  服务器要求客户端在后续的通讯中使用加密模式。

- **13: Finished**

  服务器告诉客户端它已经准备好安全通信了。这是 SSL “握手”完成的标志。

- **14: Encrypted Data**

  开始在安全通信通道上进行加密信息的交流。

SSL实例

- **利用SSL协议来访问网页**
  - **用户：浏览器里输入 https://www.sslserver.com**
  - **HTTP层：将用户需求翻译成HTTP请求，如**

GET /index.htm HTTP/1.1，Host http://www.sslserver.com

  - **SSL协议: 借助下层协议的信道协商出一份加密密钥，并用此密钥来加密HTTP请求。**
  - **TCP层：与web server的443端口建立连接，传递SSL处理后的数据。 接收端与此过程相反。**
  - **SSL在TCP之上建立了一个加密通道，通过这一层的数据经过了加密，因此达到保密的效果**

本节大纲

- 网络协议安全分析
- 安全协议：IPSec
- 安全协议：SSL (TLS)
- VPN技术

北京理工大学 网络信息安全 肖天

VPN概述

- 什么是VPN?
  - VPN：Virtual Private Network，虚拟专用网
  - 常用于连接中大型企业或团体内部网络的通讯方法
  - 利用公共IP网络建立局域网络
  - 可“地理分布”的局域网络
  - 为保证在VPN中传输数据的私密性，需要引入安全协议
  - 安全性是VPN技术的重要组成部分
  - 详细：RFC 2547

VPN概述

- **选用VPN的理由**

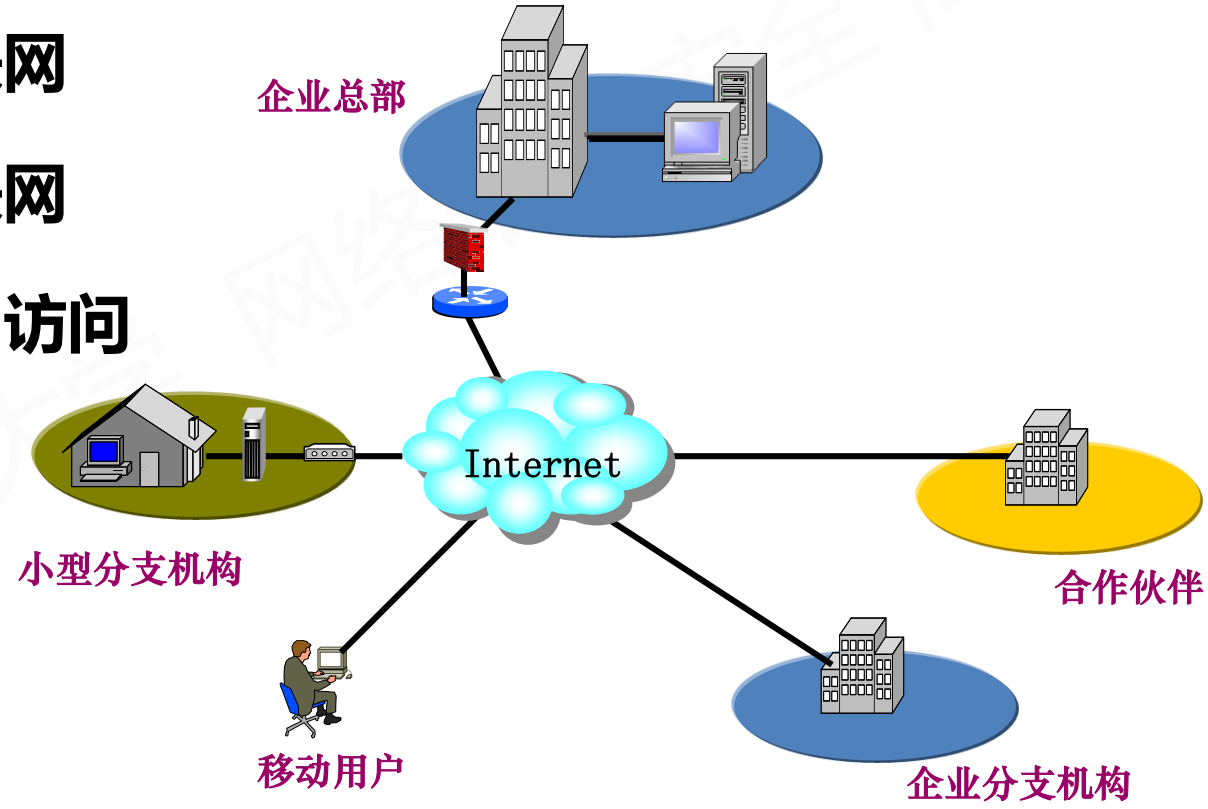
	VPN技术	专线技术
安全性	非常高，保护数据传输的完整性、保密性、不可抵赖性	比较高，建立在对电信部门相信的基础上。
可扩展性	基于TCP/IP技术，只要网络可达，就可以方便扩展。	当地运营商的支持，扩展很不方便。
投资成本	设备一次性投入，不需要支出每月的运营费用。	需要每月支付昂贵的专线租用费用
移动支持	能对Internet上的内部移动用户安全接入，彻底消除地域差异。	只能联通专线覆盖的网络。
带宽	使用各种廉价的宽带介入方式，一般在1~100M。	由于价格昂贵，一般租用的带宽都比较窄。
升级	依赖于设备的升级。	依赖于电信部门。

VPN概述

- **VPN的应用**
  - **可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。**
  - **通过将数据流转移到低成本的网络上，一个企业的虚拟专用网解决方案将大幅度地减少用户费用。**
  - **虚拟专用网还可以保护现有的网络投资。**

VPN概述

- **VPN的应用**
  - **组建企业内联网**
  - **组建企业外联网**
  - **完成远程用户访问**



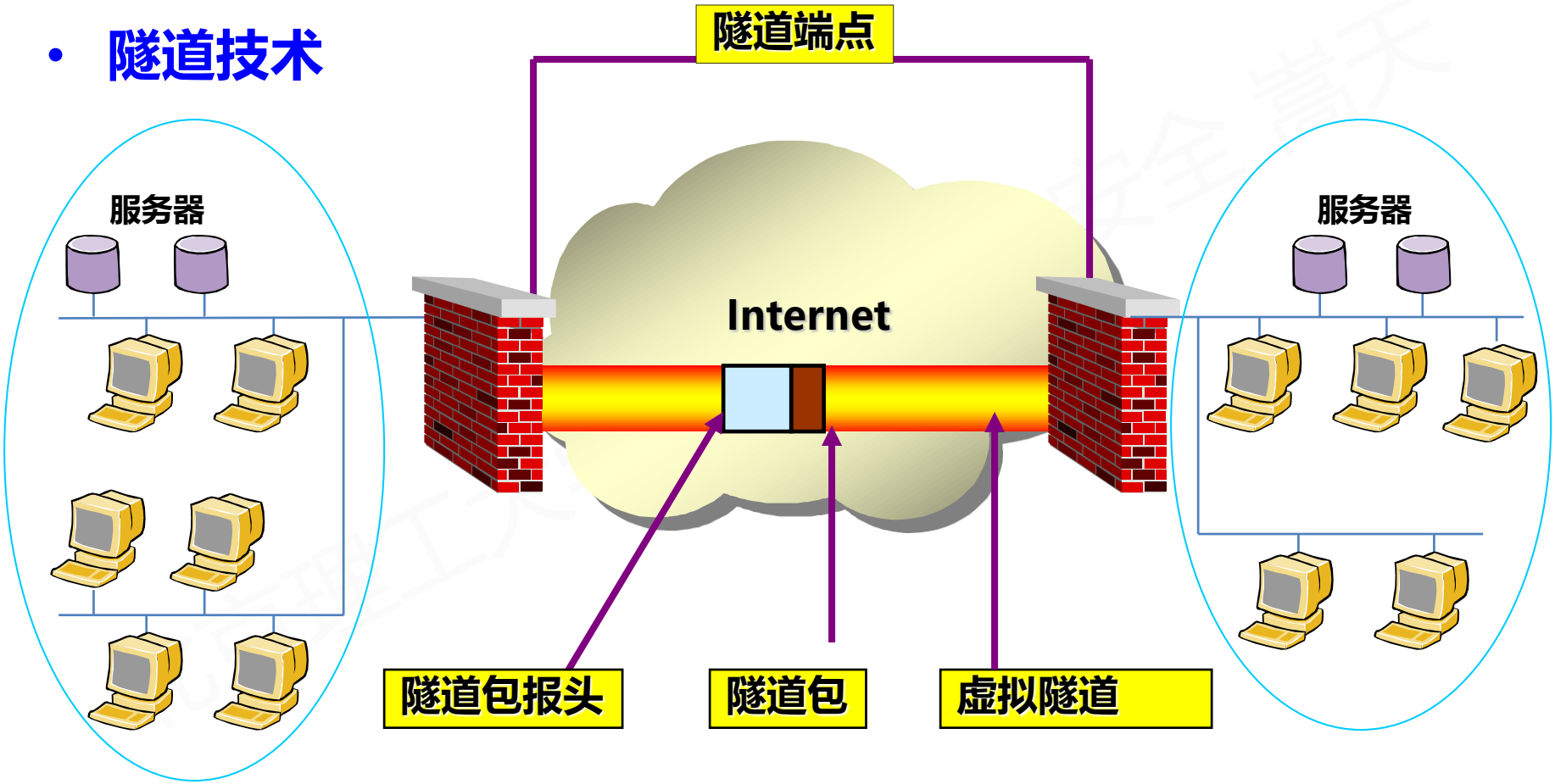
VPN概述

- **VPN的关键技术**
  - 隧道技术
  - 加解密技术
  - 认证技术
- **VPN的种类**
  - SSL/TLS VPN
  - IPSec VPN

北京理工大学 网络信息安全 蒋天

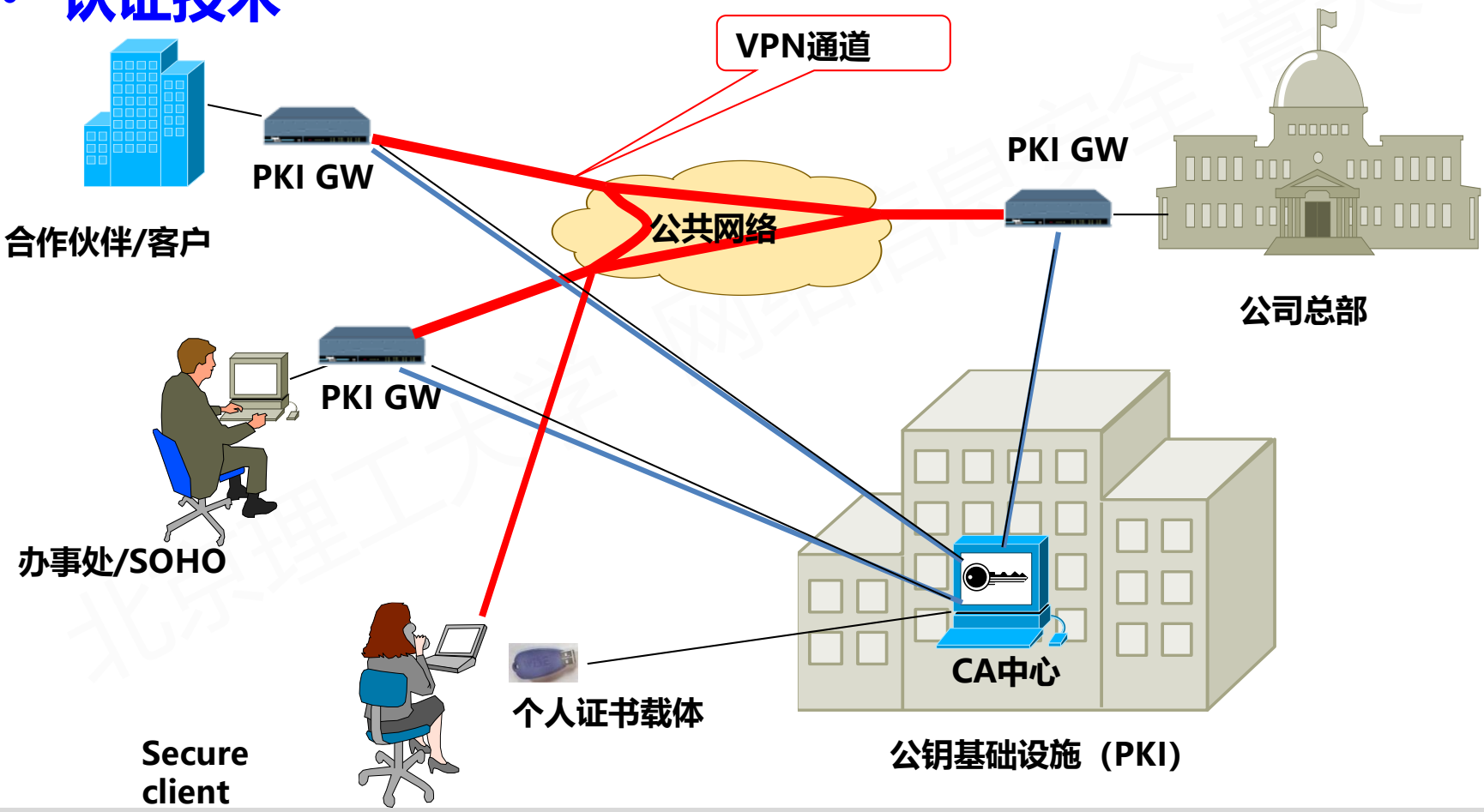
VPN的关键技术

- 隧道技术



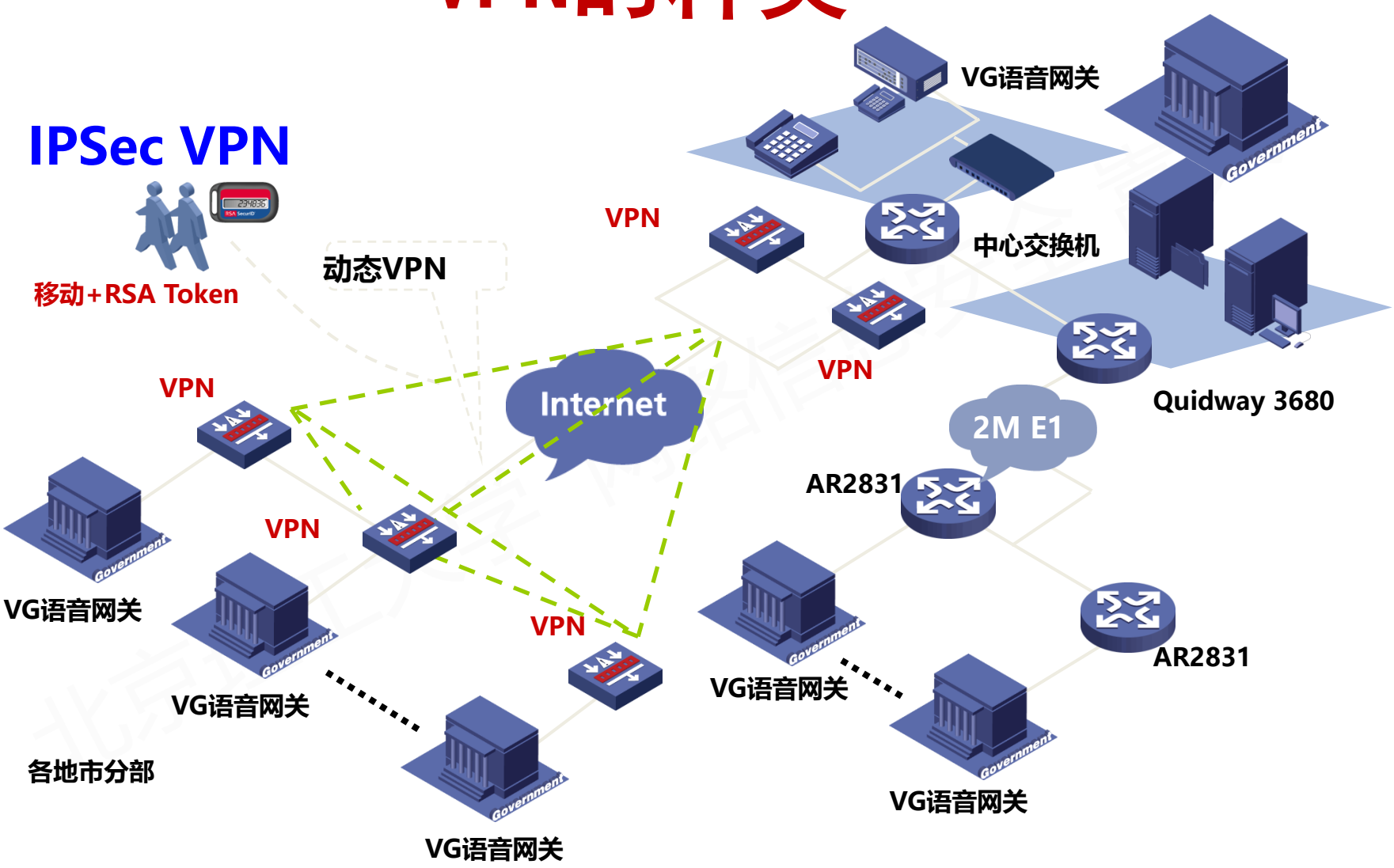
VPN的关键技术

- 认证技术



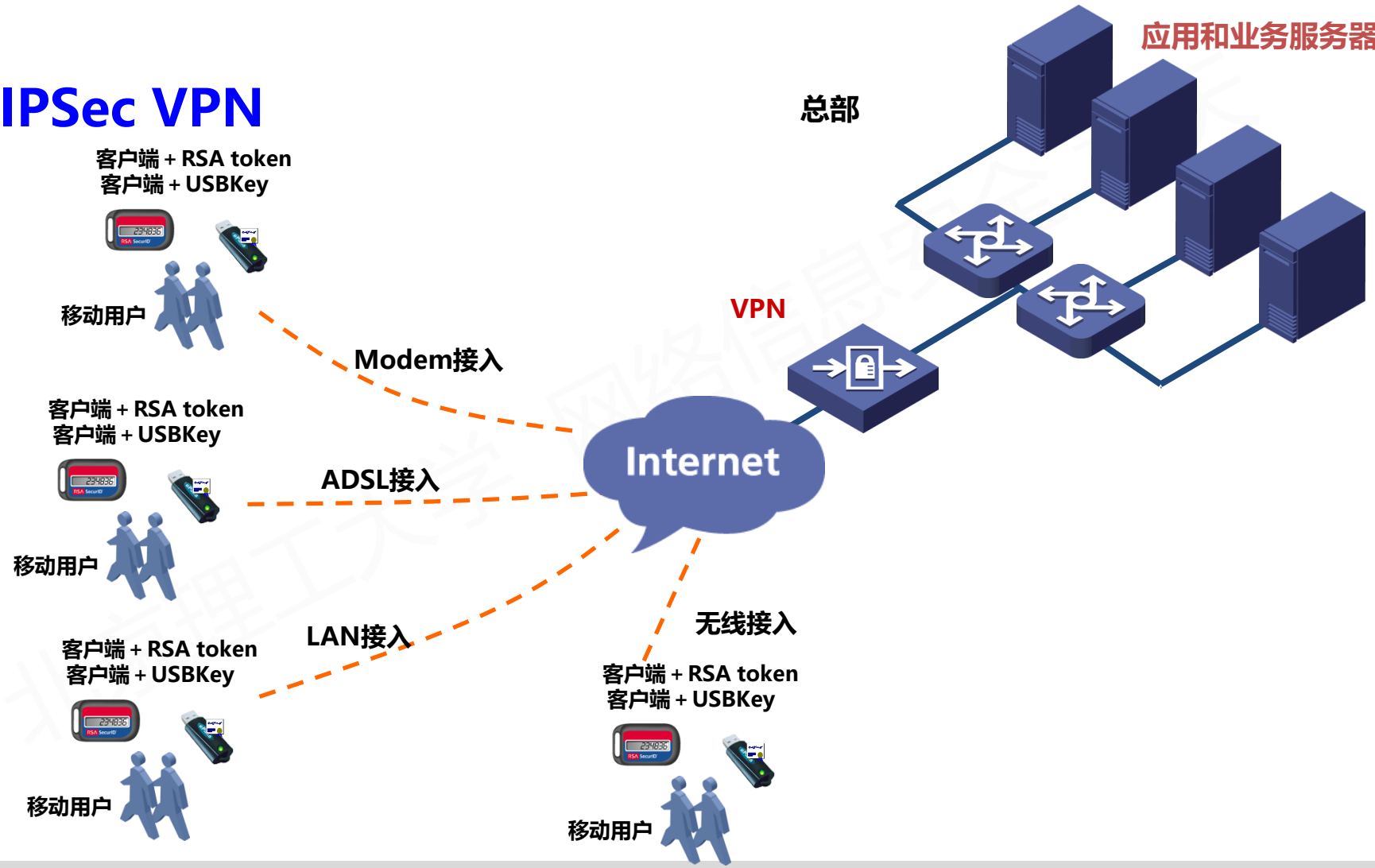
VPN的种类

- **IPSec VPN**



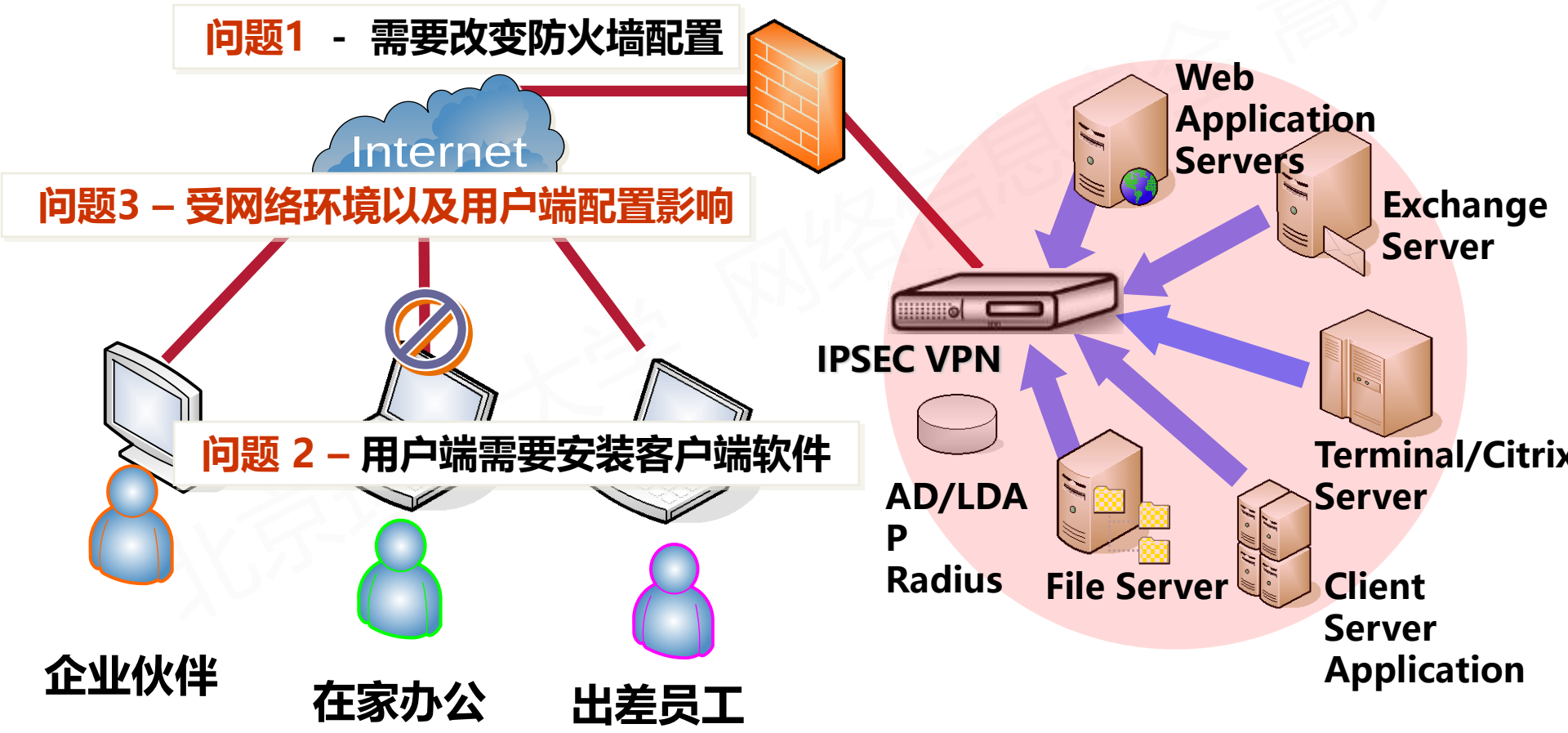
VPN的种类

- **IPSec VPN**



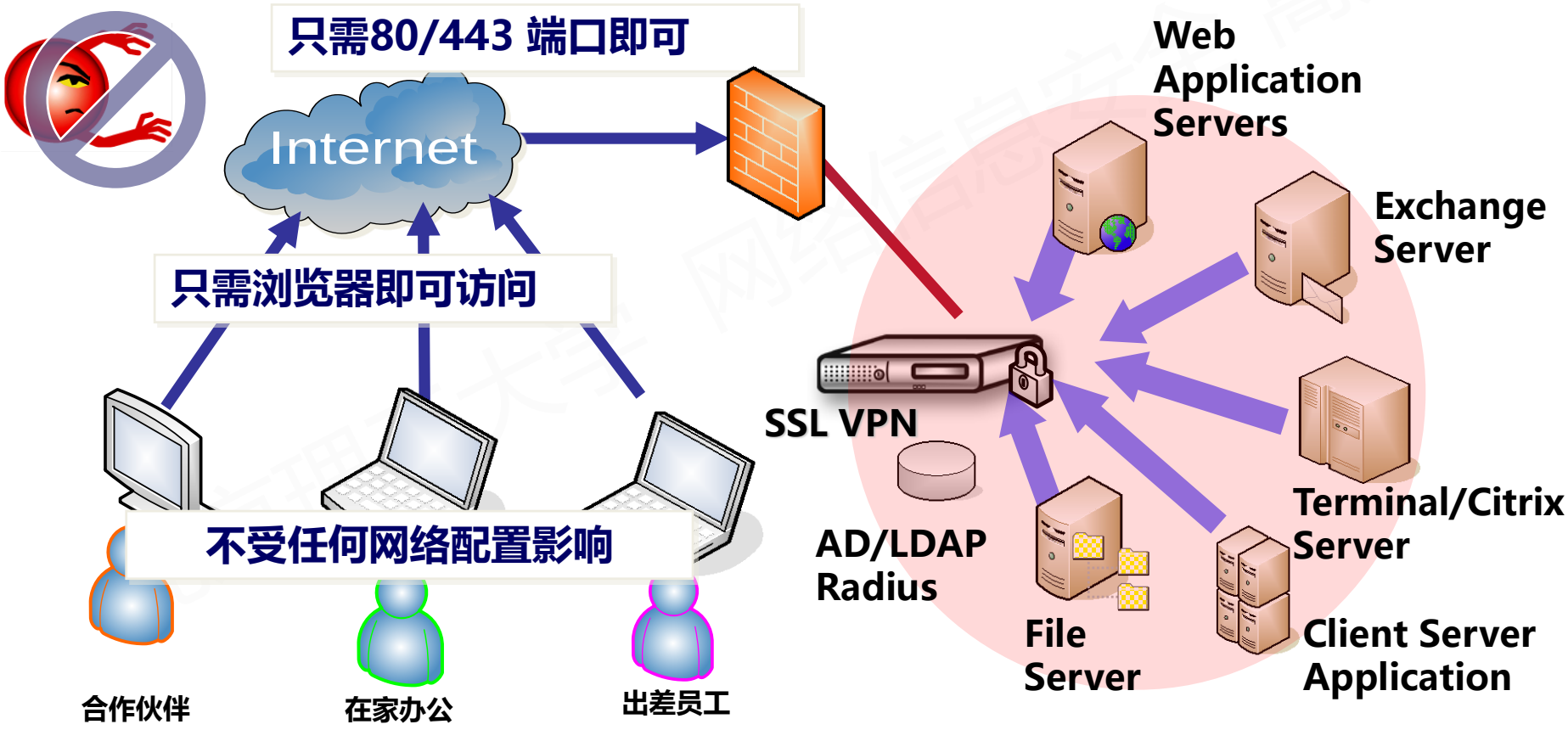
VPN的种类

- IPSec VPN



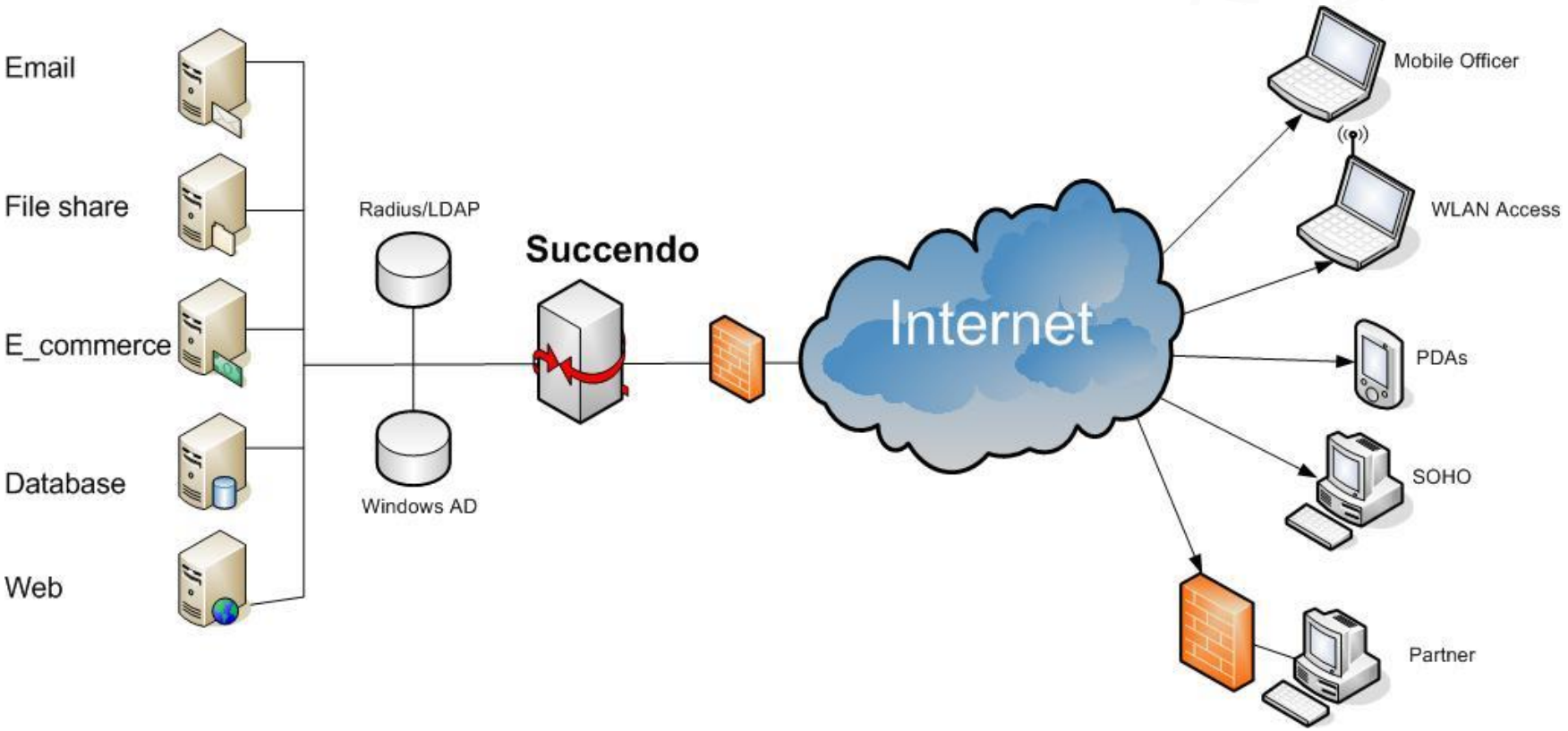
VPN的种类

- **SSL VPN**



VPN的种类

- **SSL VPN**



VPN的种类

- IPSec VPN和SSL VPN的区别

Item	IPsec VPN	SSL VPN
需要安装、配置并管理客户端软件	不需要	需要
维护成本	高	低
防火墙需要改变和配置安全策略	很多	极少
可以进入所有内部网络	可以	不可以
任何计算机都可以使用	不可以	可以

VPN的种类

- IPSec VPN和SSL VPN的区别

Item	IPsec-VPN	SSL VPN
初始设备投资	相同	相同
客户端安装	费用高	不需要安装费用
大量远程用户推广	困难，费用高	简单方便
网络安全等级	好	更好
与应用系统整合	困难	简单
系统扩充性	具备	具备
用户端使用便利性	麻烦	简单

本节总结

- 经过本节的学习，我们知道
  - TCP/IP安全性的根源
  - IPSec的两种模式和AH、ESP协议
  - SSL协议所处层次和会话过程
  - VPN的概念
  - IPSec VPN和SSL VPN的区别