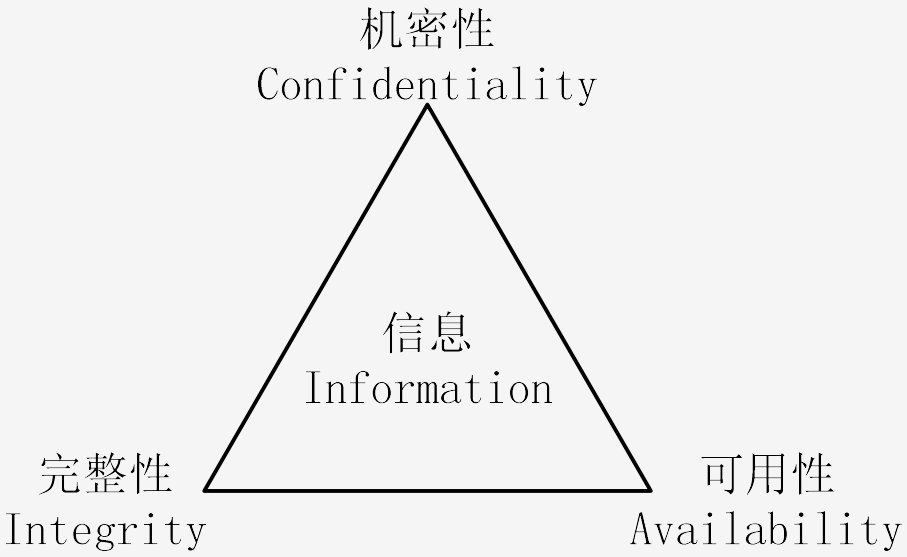
信息安全概述

1.4 信息安全体系结构

⊙ 1.4.1 面向目标的知识体系结构



信息安全的三个基本目标（金三角）

安全层次

⊙物理安全

指对网络及信息系统物理装备的保护。

⊙运行安全

指对网络及信息系统的运行过程和运行状态的保护。

⊙数据安全

指对数据收集、存储、检索、传输等过程提供的保护，不被非法冒充、窃取、篡改、抵赖。

⊙内容安全

指依据信息内涵判断是否违反特定安全策略，采取相应的安全措施。

⊙管理安全

指通过针对人的信息行为的规范和约束，提供对信息的机密性、完整性、可用性以及可控性的保护。

1.4.3 面向过程的信息安全保障体系

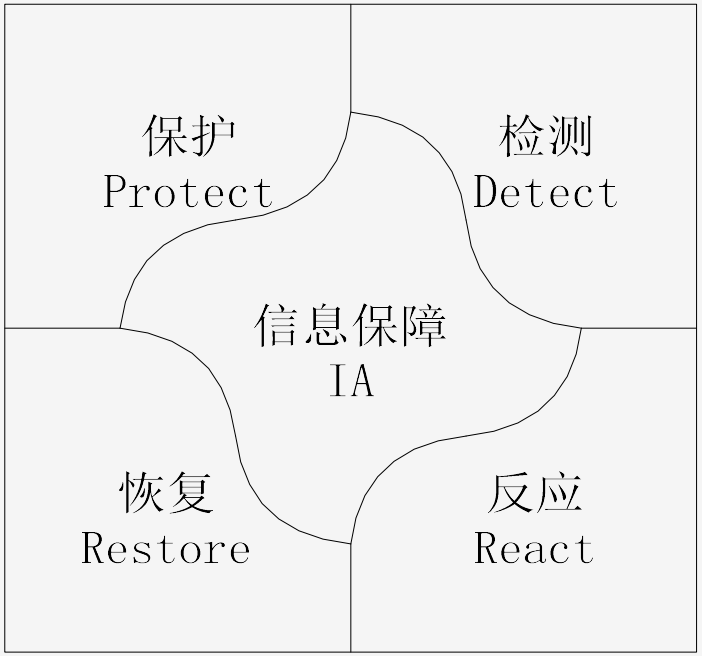
- 美国国防部提出的“信息安全保障体系”为诠释了安全保障的内涵。
- 信息安全保障体系包括四个部分内容，即PDRR。

  保护（Protect）

  检测（Detect）

  反应（React）

  恢复（Restore）



信息保障体系

密钥数量

对称密码算法（symmetric cipher)

- 加密密钥和解密密钥相同，或实质上等同，即从一个易于推出另一个
- 又称秘密密钥算法或单密钥算法

非对称密钥算法（asymmetric cipher)

- 加密密钥和解密密钥不相同，从一个很难推出另一个
- 又称公开密钥算法（public-key cipher)
- 公开密钥算法用一个密钥进行加密, 而用另一个进行解密
- 其中的加密密钥可以公开,又称公开密钥（public key)，简称公钥。解密密钥必须保密,又称私人密钥（private key)私钥，简称私钥

经典加密技术

- 替代
- 置换

分组密码

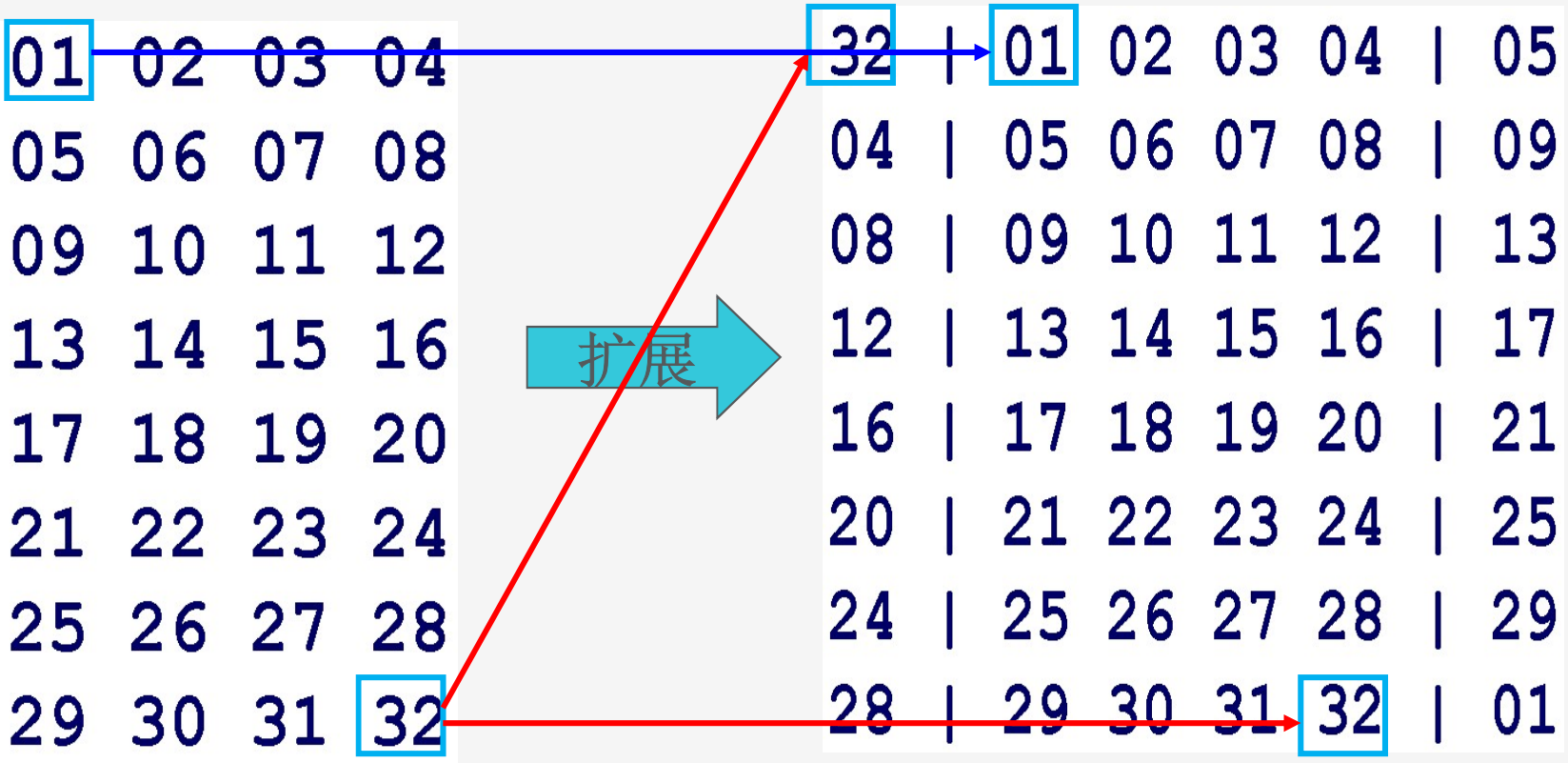
工作方式

将明文分成固定长度的组（块），如64bit一组，用同一密钥和算法对每一快加密，输出也是固定长度的密文。

主要算法

DES、3DES、IDEA、RC2、AES等。

扩展置换E-盒—32位扩展到48位



S-盒的构造

- **DES**中其它算法都是线性的，而**S-**盒运算则是非线性的
- **S-**盒不易于分析，它提供了更好的安全性
- 所以**S-**盒是算法的关键所在

p-盒的构造准则

- P置换的目的是提供雪崩效应
- 明文或密钥的一点小的变动都引起密文的较大变化

Diffie-Hellman密钥交换协议描述

- Alice和Bob协商好一个大素数p，和大的整数g，1<g<p，g最好是F_P中的本原元，即$F_P^* = <g>$
- p和g无须保密，可为网络上的所有用户共享

Diffie-Hellman密钥交换协议描述

- 当Alice和Bob要进行保密通信时，他们可以按如下步骤来做：

  (1) Alice选取大的随机数x，并计算 $X = g^x \pmod P$

  (2) Bob选取大的随机数x′，并计算 $X' = g^{x'} \pmod P$

  (3) Alice将X传送给Bob；Bob将X′传送给Alice

  (4) Alice计算$K = (X')^X \pmod P$; Bob计算$K' = (X)^{X'} \pmod P$,

  易见，$K = K' = g^{xx'} \pmod P$

- 由(4)知，Alice和Bob已获得了相同的秘密值K
- 双方以K作为加解密钥以传统对称密钥算法进行保密通信

RSA密码体制

- 欧拉定理：若整数g和n互素，则$g^{\varphi(n)} \equiv 1 \pmod{n}$；其中φ(n)为比n小，但与n互素的正整数个数，称为φ(n)为欧拉函数。n=pq，φ(n)=(p-1)(q-1)。

- 首先，明文空间P＝密文空间C=Zn.
- 密钥的生成

  选择p,q，p,q为互异素数，计算n=p*q,

  φ(n)=(p-1)(q-1), 选择整数e使gcd(φ(n),e)=1 ,1<e<φ(n),

  计算d,使$d=e^{-1} \pmod{\varphi(n)}$,

  公钥Pk={e,n};私钥Sk={d,p,q}。

- 加密 (用e,n)
  明文：$M<n$，密文：$C=M^e \pmod n$.
- 解密 (用d,p,q)

  密文：C，明文：$M=C^d \pmod n$.

  注意：加密和解密是一对逆运算。

RSA算法举例

- 设 p=7， q=17， n=7*17=119； 参数T={n=119}；
- φ(n)=(7-1)(17-1)=96;
- 选择e=5, gcd(5,96)=1; 公钥pk=5;
- 计算d, （ d*e）mod 96=1; d=77; 私钥sk=77;

设:明文m=19

加密： $(19)^{5} \bmod 119 = 66$

脱密： $(66)^{77} \bmod 119 = 19$

RSA算法使用

1.加解密

A的公开密钥为(e,n),B对消息m加密

$c=m^e \mod n$ *给A, 只有A能解密*

$m=c^d \mod n$

特点:

- 和A从来不认识,都可进行保密通讯,只要知道A的公钥.
- 速度慢,不实用.

要求对公开密钥进行保护，防止修改和替换。

RSA算法使用

2.数字签名与身份认证

A的公开密钥为(e,n),私钥为(d,n),A对消息m的数字签名为:$s=H(m)^d \bmod n$, H(x)为公开的散列(hash)函数.
任何人都可验证A对m的签名的有效性 $H(m)=s^e \bmod n$
功能:防止非法篡改、伪造,A的抵赖与否认,对A的假冒等。
要求对公开密钥进行保护，防止修改。

其他公钥算法

- **Rabin密码算法**

  合数模下求解平方根的困难性

- **ElGamal密码算法**

  基于离散对数问题

- **椭圆曲线密码算法**

  代数几何中基于椭圆曲线的点集

一般杂凑函数

- 杂凑值只是输入字串的函数，任何人都可以计算；
- 函数y=H(x),要求将任意长度的x变换成固定长度的y,并满足：

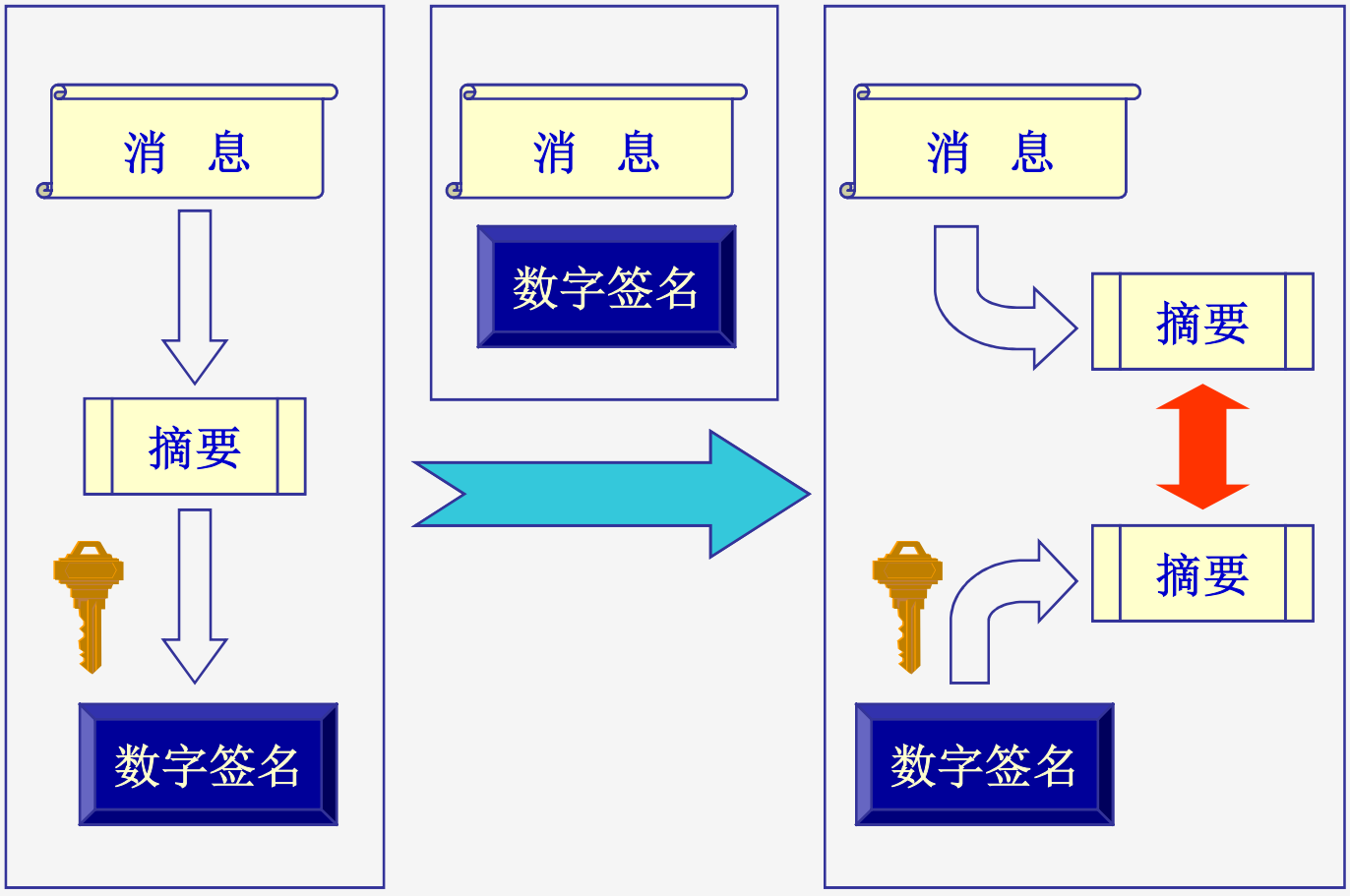
1.单向性,任给y,计算x,使得y=H(x)困难

2.快速性,计算y=H(x)容易

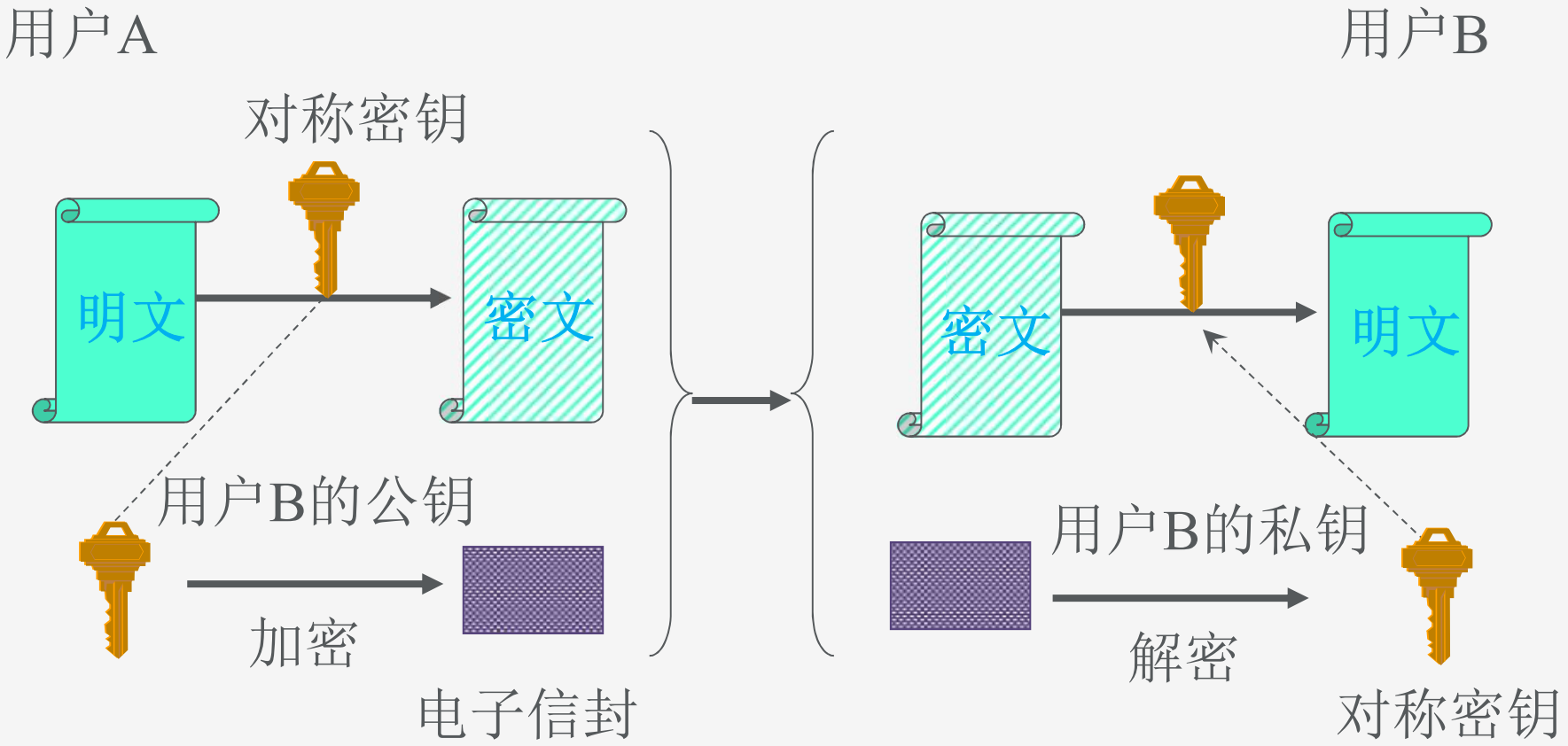
3.无碰撞,寻找$x_1 \neq x_2$,满足$H(x_1)=H(x_2)$是困难的.

- 常用的一般杂凑函数有 MD5, SHA等。

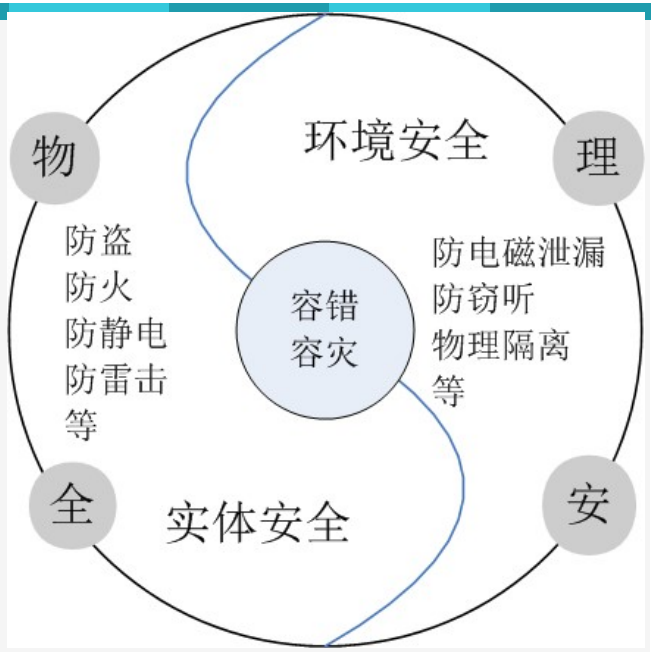
数字签名与验证过程图示



电子信封技术实现



3.1 概述



- 物理安全:实体安全和环境安全
- 解决两个方面问题:

  对信息系统实体的保护;

  对可能造成信息泄漏的物理问题进行防范。
- 物理安全技术包括:

  防盗、防火、防静电、防雷击、防信息泄漏、物理隔离;

  基于物理环境的容灾技术和物理隔离技术也属于物理安全技术范畴。
- 物理安全是信息安全的必要前提

  如果不能保证信息系统的物理安全，其他一切安全内容均没有意义。

防电磁信息泄漏

- 主要包括三个层面，

  一是抑制电磁发射，采取各种措施减小“红区”电路电磁发射；

  二是屏蔽隔离，在其周围利用各种屏蔽材料使红信号电磁发射场衰减到足够小，使其不易被接收，甚至接收不到；

  三是相关干扰，采取各种措施使相关电磁发射泄漏即使被接收到也无法识别。

口令更新

- 系统管理员分配临时口令，拥有临时口令的摘要，通过代外方式发给用户
- 用户第一次登陆时，被强制更新口令。
- 新口令的摘要被旧的口令进行对称加密发送到认证系统

门票和门票的分发

- KDC和每个实体之间共享一个秘密密钥，这个密钥成为主密钥。
- 当Alice告知KDC需要和Bob通信时，KDC为Alice和Bob生成一个共享密钥K_{AB}，并分别用Alice和Bob的主密钥加密K_{AB}，再将消息发给Alice，包括用Bob主密钥加密的会话秘钥K_{AB}以及Alice的名字等信息，称为访问Bob的门票

门票和门票的分发

- Alice无法读取该信息中的信息，因为该消息用Bob的主密钥进行加密。
- Bob可以解密门票并获得K_{AB}和Alice的名字。
- Alice和bob可以基于K_{AB}相互认证身份，以及加密会话

- 改进后的假想的对话：

Once per user logon session：

- (1) C → AS ： ID_C || ID_{tgs}
- (2) AS → C ： $E_{KC}[Ticket_{tgs}]$

Once per type of service

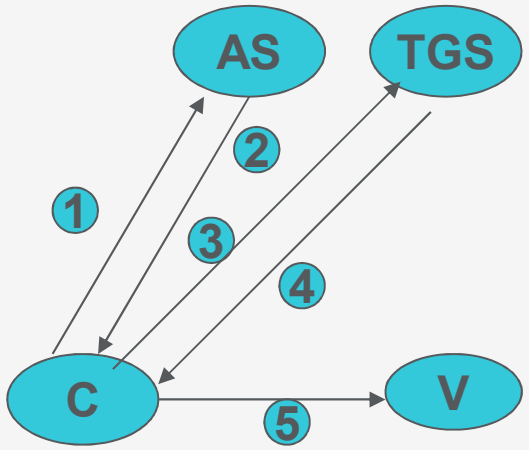
- (3) C → TGS ： ID_C || ID_V || $Ticket_{tgs}$
- (4) TGS → C ： $Ticket_V$

Once per service session

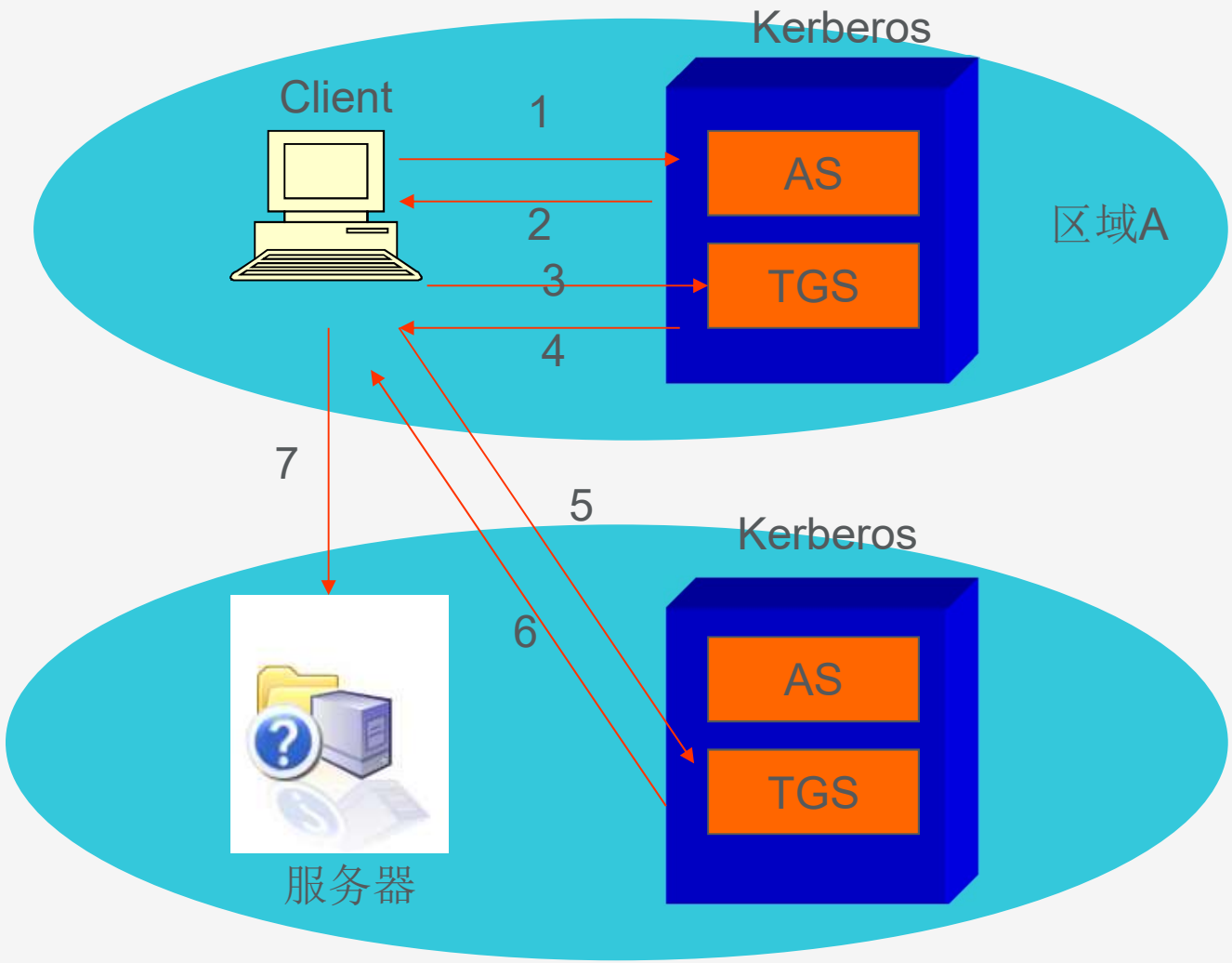
- (5) C → V ： ID_C || $Ticket_V$

$Ticket_{tgs} = E_{Ktgs}[ID_C||AD_C||ID_{tgs}||TS1||Lifetime1]$

$Ticket_V = E_{KV}[ID_C||AD_C||ID_V||TS2||Lifetime2]$



Kerberos区域和多区域的Kerberos



认证机构CA

- 权威的、可信任的、公正的第三方机构
- 认证中心
- PKI的核心
- 数字证书的签发机构
- 证书的产生、管理、存档、发放、以及作废管理

证书

- 公钥体制的一种密钥管理媒介
- 权威性的电子文档，网络身份证
- 证明主体身份及其公钥的合法性
- 含有主体的身份和公钥
- 用CA的私钥签名

证书的撤销

- 证书废止原因
  - 私钥泄密
  - 从属变更
  - 终止使用
  - CA出现问题
- 撤销证书原因
  - CA知道证书细节不真实
  - 证书持有者没有履行职责和登记人协议
  - 证书持有者死亡、违反电子交易规则或者犯罪

数字证书验证

- 验证证书签名者的签名
- 检查证书的有效期
- 检查证书的预期用途是否符合CA在该证书中指定的策略限制
- 确认证书没有被CA撤销

6.2.2 传统病毒

- 传统病毒的代表

  巴基斯坦智囊（Brain）、大麻、磁盘杀手（DISK KILLER）、CIH等。

- 传统病毒一般有三个主要模块组成，包括启动模块、传染模块和破坏模块。

- CIH

  感染Windows95/98环境下PE格式的EXE文件（第一例）

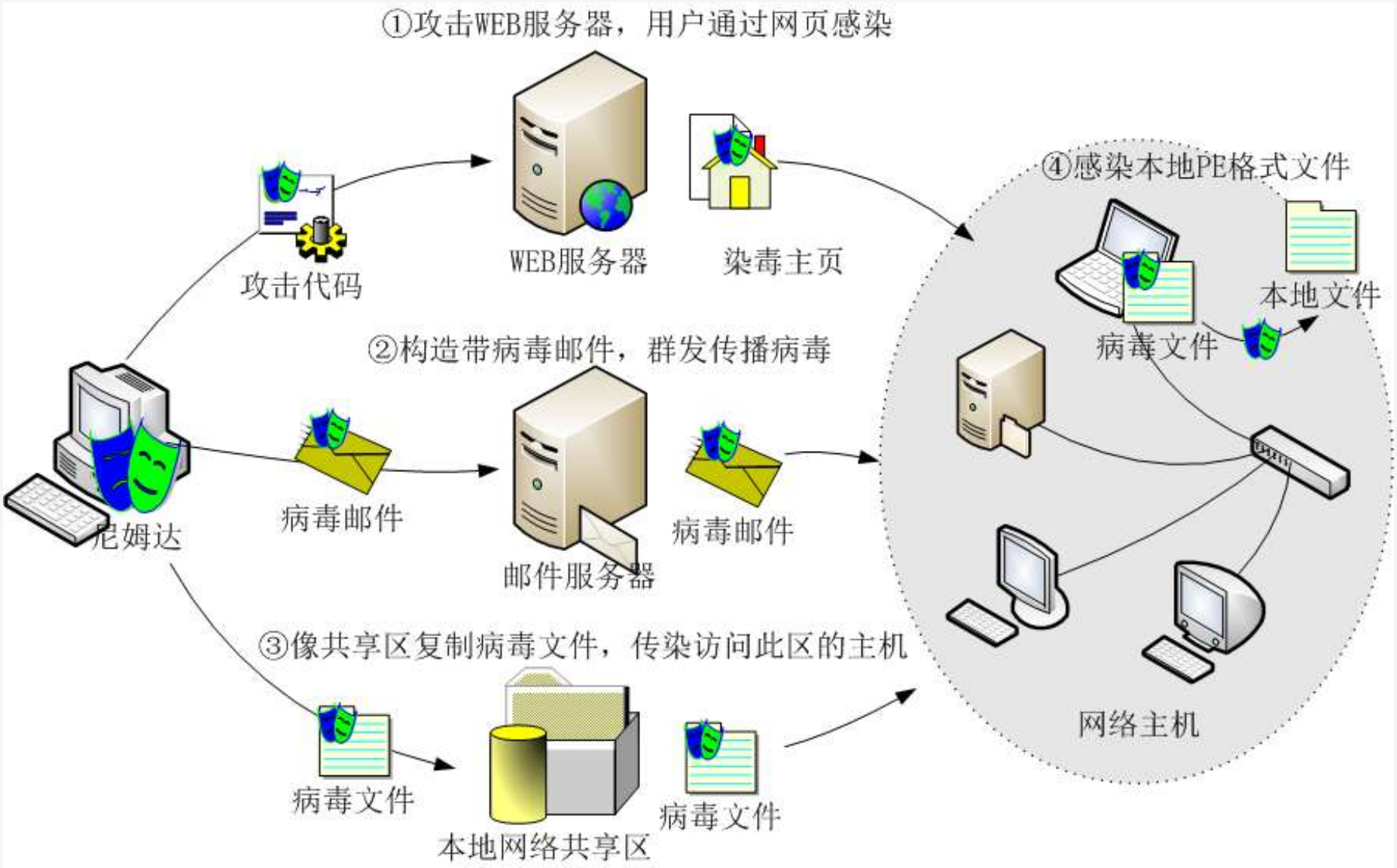
  病毒发作时直接攻击和破坏计算机硬件系统。

  该病毒通过文件复制进行传播。

  计算机开机后，运行了带病毒的文件，其病毒就驻留在Wnidows核心内存里，

  组成：初始化驻留模块、传染模块和破坏模块。

Nimda 传播途径


①攻击WEB服务器，用户通过网页感染
攻击代码
WEB服务器
染毒主页
④感染本地PE格式文件
本地文件
病毒文件
②构造带病毒邮件，群发传播病毒
尼姆达
病毒邮件
邮件服务器
病毒邮件
③像共享区复制病毒文件，传染访问此区的主机
病毒文件
本地网络共享区
病毒文件
网络主机

6.3.1 拒绝服务攻击

- 拒绝服务攻击DoS (Denial of Service)

  DoS并不是某一种具体的攻击方式，而是攻击所表现出来的结果最终使得目标系统因遭受某种程度的破坏而不能继续提供正常的服务，甚至导致物理上的瘫痪或崩溃。

- 通常拒绝服务攻击可分为两种类型，

  第一类攻击是利用网络协议的缺陷，通过发送一些非法数据包致使主机系统瘫痪；

  第二类攻击是通过构造大量网络流量致使主机通讯或网络堵塞，使系统或网络不能响应正常的服务。

Ping of Death

- TCP/IP的规范，一个包的长度最大为65536字节。
- 利用多个IP包分片的叠加能做到构造长度大于65536的IP数据包。
- 攻击者通过修改IP分片中的偏移量和段长度，使系统在接收到全部分段后重组报文时总的长度超过了65535字节。
- 一些操作系统在对这类超大数据包的处理上存在缺陷，当安装这些操作系统的主机收到了长度大于65536字节的数据包时，会出现内存分配错误，从而导致TCP/IP堆栈崩溃，造成死机。

Tear drop

- IP数据包在网络传递时，数据包可能被分成多个更小的IP分片。
- 攻击者可以通过发送两个（或多个）IP分片数据包来实现Tear Drop攻击。
- 第一个IP分片包的偏移量为0，长度为N，第二个分片包的偏移量小于N，未超过第一个IP分片包的尾部，这就出现了偏移量重叠现象。
- 一些操作系统无法处理这些偏移量重叠的IP分片的重组，TCP/IP堆栈会出现内存分配错误，造成操作系统崩溃。

Syn Flood

- 攻击者伪造TCP的连接请求，向被攻击的设备正在监听的端口发送大量的SYN连接请求报文；
- 被攻击的设备按照正常的处理过程，回应这个请求报文，同时为它分配了相应的资源。
- 攻击者不需要建立TCP连接，因此服务器根本不会接收到第三个ACK报文，现有分配的资源只能等待超时释放。
- 如果攻击者能够在超时时间到达之前发出足够多的攻击报文，被攻击的系统所预留所有TCP缓存将被耗尽。

Smurf攻击

- Smurf攻击是以最初发动这种攻击的程序Smurf来命名的，这种攻击方法结合使用了IP地址欺骗和ICMP协议。
- 当一台网络主机通过广播地址将ICMP ECHO请求包发送给网络中的所有机器，网络主机接收到请求数据包后，会回应一个ICMP ECHO响应包，这样发送一个包会收到许多的响应包。
- Smurf构造并发送源地址为受害主机地址、目的地址为广播地址的ICMP ECHO请求包，收到请求包的网络主机会同时响应并发送大量的信息给受害主机，致使受害主机崩溃。
- 如果Smurf攻击将回复地址设置成受害网络的广播地址，则网络中会充斥大量的ICMP ECHO响应包，导致网络阻塞。

缓冲区溢出-堆栈的作用

- 堆栈在子程序调用的时候用来传递参数
- 堆栈用来保存子程序的返回地址
- 堆栈用来保存子程序中的变量

缓冲区溢出

- 缓冲区溢出攻击，是通过重写堆栈中储存的EIP地址的内容，以使程序跳转到指定shellcode处执行
- 主要是由一些不好的编程习惯，比如使用不安全的strcpy和strcat等

缓冲区溢出填充码的作用

- Nop填充
- 找到返回地址
- 重复返回地址填充

Nop sled	Shellcode	重复返回地址

入侵检测系统术语

- **警报**

  IDS向系统操作人员发出入侵正在发生或正在尝试进行的消息。

- **异常**

  用一段时间建立一个主机或者网络活动的轮廓。当一个用户行为或者网络行为与此轮廓距离超过某一个值的时候，需要发出警报，此行为称之为异常

入侵检测系统术语

- 网络入侵特征数据库

  将网络入侵行为抽象成特定的字符集和，通过与网络上或主机上的行为向匹配，发现可能的网络入侵。是基于误用检测系统的重要组成部分。

- 蜜罐（Honeypot）

  模拟存在漏洞的系统，为攻击者提供攻击目标。其在网络中没有任何用途，因此任何连接都是可能的攻击。

  诱惑攻击者在上面浪费时间，延缓对真正目标的攻击

入侵检测系统术语

⊙ 自动响应

一些IDS能够对攻击做出防御性反应

- 重新配置路由器或者防火墙，拒绝来自相同地址的流量
- 发送reset包切断连接

攻击者可以通过信任地址实施攻击，引起设备重新配置，达到拒绝服务攻击的目的

基本概念

- 堡垒主机:Bastion Host
- 堡垒主机是一种配置了安全防范措施的网络上的计算机，堡垒主机为网络之间的通信提供了一个阻塞点，也就是说如果没有堡垒主机，网络之间将不能相互访问。
- 双宿主机:Dual-homed Host

  有两个网络接口的计算机系统,一个接口接内部网,一个接口接外部网.
- DMZ(Demilitarized Zone，非军事区或者停火区)

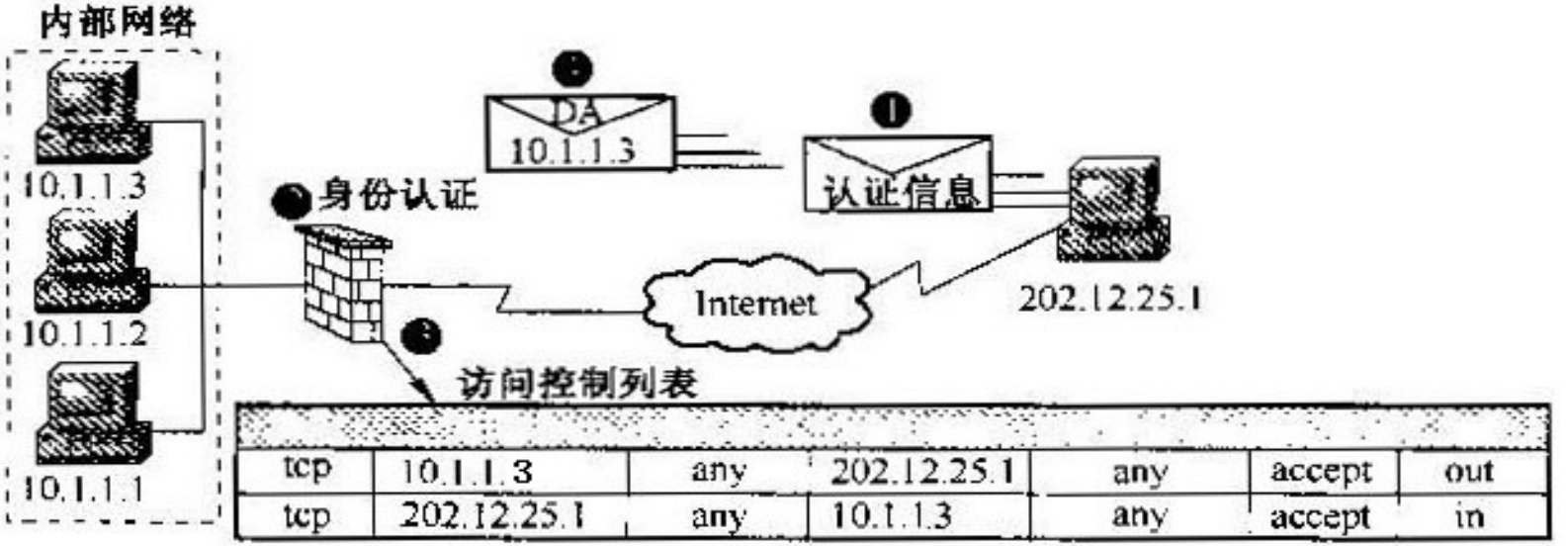
  在内部网络和外部网络之间增加的一个子网

动态访问控制列表（动态包过滤技术）

配置动态访问控制列表，可以实现指定用户的IP数据流临时通过防火墙，进行会话连接，从而实现对数据包的动态过滤。当动态访问控制列表被触发后，动态访问控制列表重新配置接口上已有的访问控制列表，允许指定的用户访问指定的IP地址。在会话结束后，将接口配置恢复到原来的状态。

动态包过滤技术一般结合身份认证机制实现。例如，用户首先发起一个到防火墙的标准Telnet会话，防火墙进行身份验证。如果用户通过身份验证，则激活动态访问控制列表，在防火墙开放一个数据通道，此时，用户便可以暂时通过防火墙访问内部网络目标主机。

动态包过滤技术实例



tcp	10.1.1.3	any	202.12.25.1	any	accept	out
tcp	202.12.25.1	any	10.1.1.3	any	accept	in

① 用户发起一个到防火墙的**Telnet**会话。

② 防火墙接收到**Telnet**数据包分组后，打开**Telnet**会话，提示用户输入认证信息并对用户身份进行验证。

③通过身份认证后，用户退出**Telnet**会话，防火墙访问控制列表内创建一个临时条目。该临时条目可限制用户临时访问的网络范围。

④ 用户通过防火墙交换数据。

⑤ 超过预定超时时间（**Timeout**）后，防火墙将删除这个临时访问控制列表规则，系统管理员也可以手动删除它。

会话结束的判定和临时条目的删除

- 对于TCP会话，检测到两组FIN位被设置的TCP分组后，临时条目一般将在几秒钟内被删除，在检测到RST位被设置的TCP分组后，临时条目将被立即删除（在会话中的两组FIN位被置位的TCP分组表示会话即将结束，几秒钟的时间可以使得会话能完美地结束，设置了RST位的TCP分组表示会话突然关闭）。在超时时间段内，如果没有检测到和特定会话相关的数据分组，临时条目也将被删除。
- 对于UDP和其他协议，会话结束的判定方法不同于TCP。原因在于这些协议被认为是无连接服务，在它们的数据分组内没有会话跟踪信息，因此，通常在超时时间段内没有检测到此UDP会话的任何相关数据分组时，便认为UDP会话结束了。

动态网络地址翻译技术

- 如果NAT映射表由防火墙动态建立，对网络管理员和用户透明，则称之为动态网络地址翻译技术。
- 网络地址翻译技术允许将多个内部IP地址映射成为一个外部IP地址。
- 从本质上讲，网络地址映射并不是简单的IP地址之间的映射，而是网络套接字映射，网络套接字由IP地址和端口号共同组成。
- 这种方法在节省了大量网络IP地址的同时隐藏了内部网络拓朴结构。