计算机网络

第十讲 网络管理与网络安全

申丽萍

电子邮件：shen-lp@cs.sjtu.edu.cn

网络管理

- 网络管理概述
- 网络故障种类
- 网络管理的功能
- 网络管理软件
- 简单网络管理协议SNMP
- 管理信息库MIB

网络管理概述

- 人们需要保证网络安全、可靠、高效地运行，而由于以下因素，网络复杂程度已超出了人们手工的控制范围：
  - 规模不断扩大：节点数从几十到几千。
  - 复杂性不断增加：设备类型增多、功能增强。
  - 异构性：不同的操作系统、通信协议（TCP/IP，IPX，X25等）。
- 网络管理员是负责监控网络软、硬件系统的人。

网络故障种类

- 严重的故障
  - 硬件故障如光纤断裂，交换机断电
  - 软件故障如路由表中的非法路径等
  - 容易检测和诊断
- 部分失效或间断性的故障
  - 网卡偶尔损坏一些位串
  - 路由器偶尔误发一些包等
  - 不易检测和诊断
  - 自动监测和重发机制使网络吞吐量下降、延迟增加

网络管理的功能（1）

- 故障管理

  故障管理是网络管理中最基本的功能之一。用户都希望有一个可靠的计算机网络。当网络中某个组成失效时，网络管理器必须迅速查找到故障并能及时给予排除。分析故障原因对于防止类似故障的再次发生相当重要。网络故障管理包括故障检测、故障诊断和恢复三方面。

网络管理的功能（2）

- 配置管理

  配置管理用于配置网络、优化网络。自动发现网络拓扑结构，根据用户对网络设备参数设置变化对网络进行调整，其功能包括：

  - 设置有关路由操作的参数
  - 修改被管对象的属性
  - 初始化或关闭被管对象
  - 自动发现网络拓扑结构
  - 更改系统的其它配置

网络管理的功能（3）

- 性能管理

  性能管理用于对系统运行及通信效率等系统性能进行监视、预测和评价，其能力包括收集、分析有关被管网络当前的数据信息，和为改善网络性能而采取的网络控制两部分。

网络管理的功能（4）

- 记费管理

  计费管理用于记录网络资源的使用情况，目的是控制和监测网络操作的费用和代价。其作用有：

  - 计算各用户使用网络资源的费用。
  - 规定用户使用的最大费用
  - 当用户为了一个通信目的需要使用多个网络中的资源时，计费管理能计算出总费用。

网络管理的功能（5）

- 安全管理

网络中主要存在以下几大安全问题：

- 数据保密和完整性
- 授权
- 访问控制

相应地，网络安全管理包括对授权机制、访问机制、加密和密钥的管理，维护和检查安全日志以及安全告警等。

网络管理软件

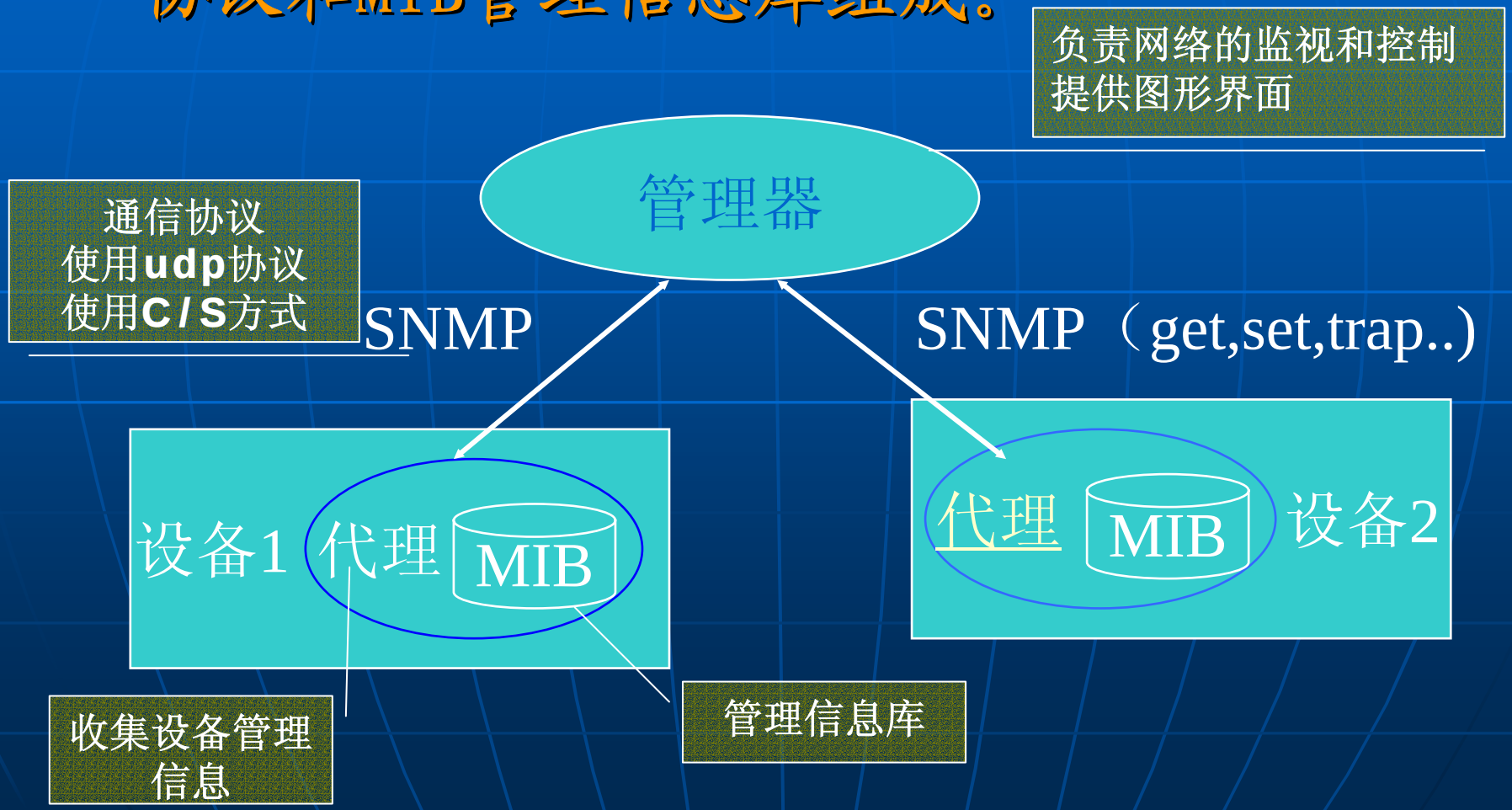
- 网络管理软件收集、监控网络中各种设备和设施的工作参数、工作状态信息，显示给管理员并接受处理，从而控制网络中的设备、软件的工作参数和工作状态，以实现对网络的管理。
- 网络管理软件采用客户/服务器模式
- 为了区分普通应用程序和专为管理员保留的应用程序，网络管理系统中避免使用术语客户和服务器：
  - 管理器（客户）运行在网管工作站上
  - 网管代理（服务器）运行在被管理设备上

网络管理软件

- 使用应用层协议进行网络管理的原因：
  - 当由于硬件故障导致网络无法通信时，在哪个层次上进行网络管理都一样。当管理员与各设备的通信状况可定位故障。
  - 网管通信与正常通信在相同的条件下进行，有故障如延迟增加管理员可马上觉察。
  - 网管协议与底层无关，同一协议可被用于各种被管理设备。

网管系统

- 网管系统由网络管理器、网管代理、SNMP协议和MIB管理信息库组成。



简单网络管理协议SNMP（1）

- SNMP协议定义管理器如何与代理进行通信：
  - 请求/应答消息的格式
  - 请求/应答消息的含义
  - 数据编码
- SNMP采用ISO的ASN.1（抽象语法表示）进行编码：
  - 与平台无关，能容纳任意数据类型和任意大小的数据（类型、长度、值）

decimal integer	hexadecimal equivalent	length octet	octets of value (in hex)
27	1B	01	1B
792	318	02	03 18
24,567	5FF7	02	5F F7
190,345	2E789	03	02 E7 89

简单网络管理协议SNMP（2）

- SNMP协议协议没有定义一个很大的命令集，而是采取存取模式：
  - 每个可以执行存、取操作的对象都被赋予一个唯一的名字
  - 管理员用fetch操作获取设备状态信息（get,get-next）
  - 用store操作对设备进行控制（set）
- 重启对象被赋值为0则系统就重启，它是store操作的副产品。

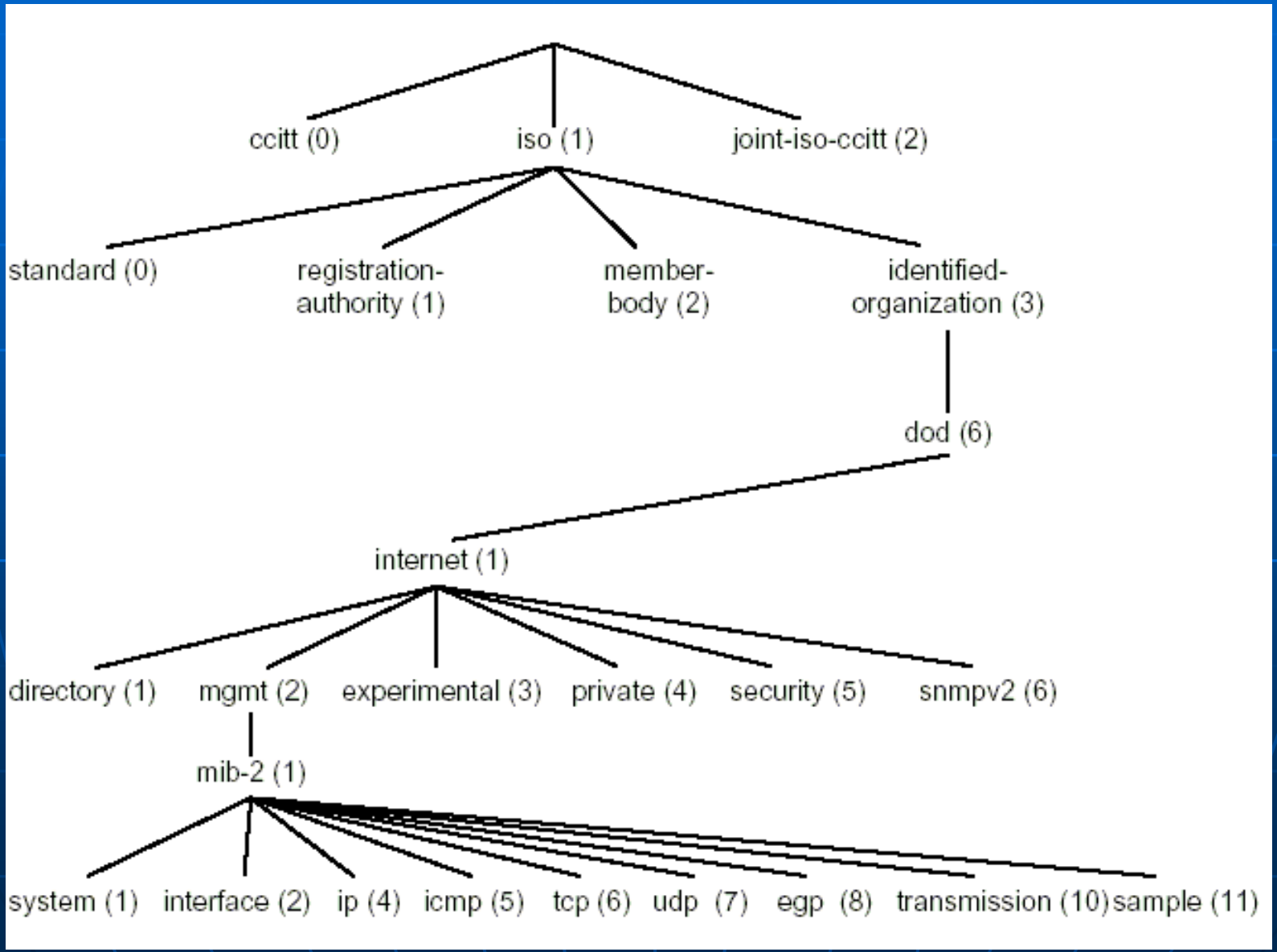
管理信息库MIB（1）

- 我们把所有SNMP可以存取的对象集合称为管理信息库（MIB）
- SNMP并没有定义MIB变量集。所有MIB变量及其意义都是由单独的标准（SMI）来定义的。
- 通信协议和对象定义之间的独立性允许用户可以自定义新的MIB变量。
- MIB变量的命名采用ASN.1标准，所有MIB变量都有很长的有层次的ASN.1名字，并可转化为数字表示形式以便于传输。

Iso.org.dod.internet.mgmt.mib.ip.ipInReceive

数字表示如下：1 .3.6.1.2.1.4.3

管理信息库MIB（2）——部分ASN.1对象命名树



管理信息库MIB（3）

- 尽管ASN.1并不显式支持数组或表结构，但可以通过在表对象名后面加后缀的办法来解决这一问题，使MIB变量可以对应与表或数组。当代理软件遇到表对象名时，会自动抽取其后缀用作索引信息来完成对表的操作。

Standard mib prefix.ip.ipRouting Table.ipRouteEntry.field.Ipdestaddr

数字表示如下：**1.3.6.1.2.1.4.21.1.7.Ipdestaddr**

网管产品

目前公认的三大网管软件平台是：

1. HP： OpenView
2. IBM： NetView
3. SUN： NetManager。

网络安全

- 网络安全概述
- 网络攻击案例
- 常用攻击手段和工具
- 网络安全的目标
- 加密
- 数字签名
- 防火墙

网络安全概述

- 网络有很多不安全因素：
  - 路由器转发从任何地方来的包。
  - 攻击者可在任何一台联网计算机进行攻击。
  - 攻击手法不断更新，没有一个网络是绝对安全的。
- 每个组织对安全的理解不一样，首先要制定合理的安全策略。
  - 哪些需要保护，保护的规则。
  - 必须覆盖数据的存储、传输和处理，覆盖计算机系统、局域网和其他互连设备。
  - 必须进行性能价格的权衡。

几个网络攻击案例

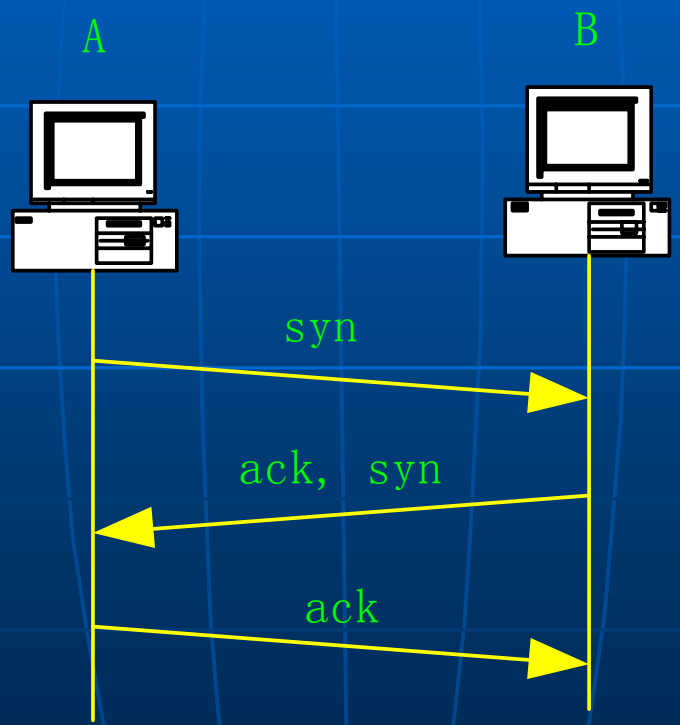
- 94年末，俄罗斯黑客弗拉基米尔·利文与其伙伴从圣彼得堡的一家小软件公司的联网计算机上，向美国CITYBANK银行发动了一连串攻击，通过电子转帐方式，从CITYBANK银行在纽约的计算机主机里窃取1100万美元。
- 在2002年2月7日到11日的短短几天内，黑客连续攻击了包括Yahoo、Buy.com、eBay、Amazon、CNN等许多知名网站，致使有的站点停止服务达几个小时甚至几十个小时之久。它利用攻击者已经侵入并控制的主机（可能是数百，千台），对某一单机发起D.O.S.攻击。在悬殊的带宽力量对比下，被攻击的主机会很快失去反应。这种攻击方式被证实是非常有效的，而且非常难以抵挡。
- 2003年8月，冲击波蠕虫病毒利用微软操作系统的RPC漏洞，使国内大量机器陷入瘫痪，引起公安部的重视。

常用攻击手段和工具

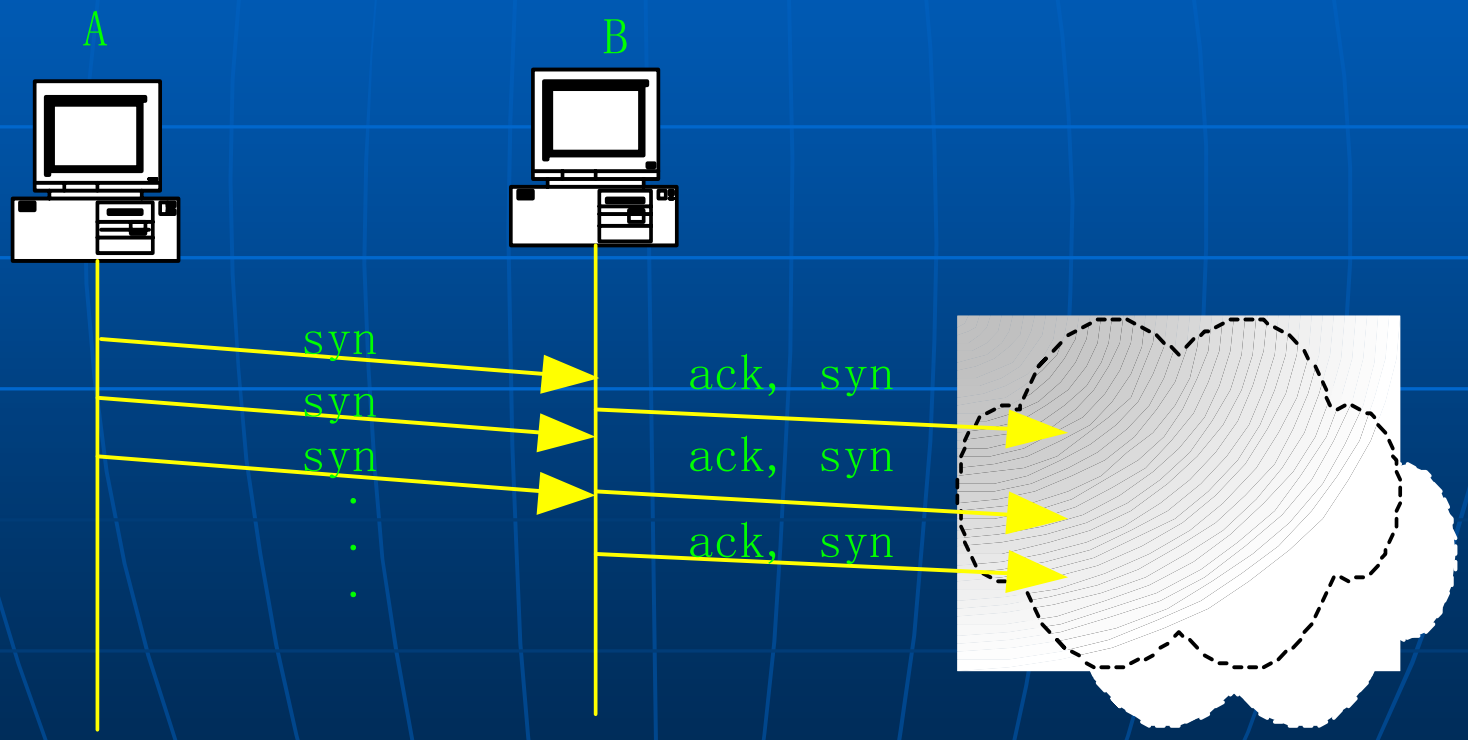
- 电子邮件炸弹
- 特洛伊木马
- 拒绝服务攻击
- IP欺骗攻击
- 病毒
- 扫描器，网络分析器
- 口令攻击

拒绝服务攻击 – Syn Flooding

TCP 三次握手



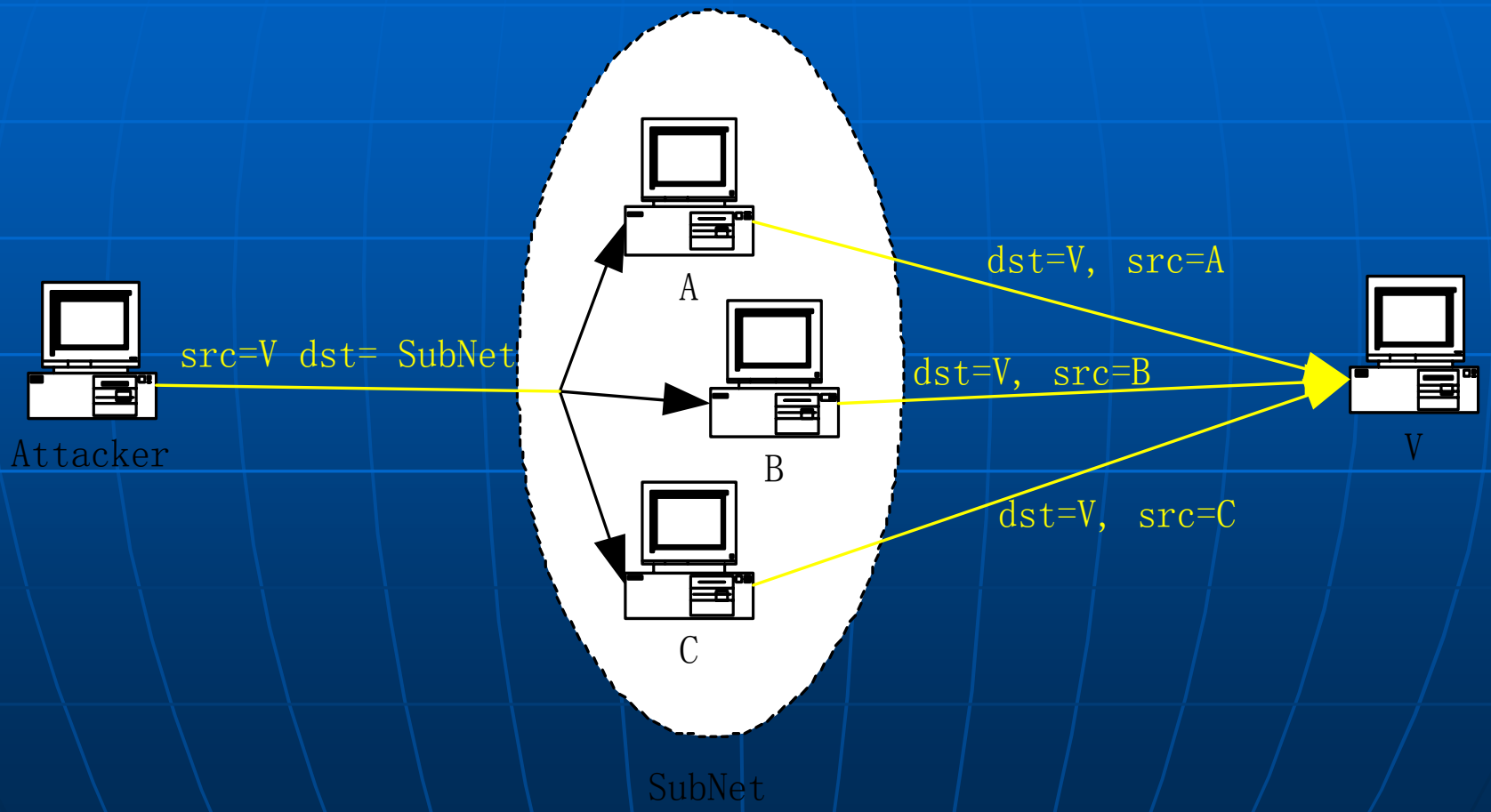
拒绝服务攻击 – Syn Flooding



拒绝服务攻击 - Smurf

是根据一个攻击工具“smurf”而命名的。攻击者发送一个ICMP 回应请求（ECHO REQUEST）报文，目的地址为广播地址，源地址为伪造的攻击目标的地址，将导致广播子网内的所有主机向攻击目标发送应答报文，大量的报文会导致目标主机无法正常工作。

Smurf 攻击原理


Attacker
src=V dst= SubNet
A
B
C
SubNet
dst=V, src=A
dst=V, src=B
dst=V, src=C
V

口令攻击


基于口令的入侵方法
CRACK程序
字典
口令表
加密系统
比较
成功
采用一种方法来尽的方法来尽指定用户的口
哈尔滨工业大学计算机网络中心
34

网络安全的目标

- 数据完整性
- 资源可用性
- 用户身份认证
- 数据保密性
- 不可否认性

数据完整性

完整性指维护信息的一致性，防止非法用户对系统数据的篡改。

实现方法：采用数据加密及校验和技术。

资源可用性

保证合法用户在任何时候都能使用、访问资源，阻止非法用户使用系统资源。

实现方法：访问控制、防火墙、入侵检测等。

用户身份认证

保证通信对方的身份是真实的。

实现方法：帐号-口令，电子证书等。

数据保密性

数据只能为合法用户所使用，让非法用户无法接触或读懂数据。

实现方法：授权和访问控制、数据加密技术。

不可否认性

参与网络通讯过程的各方（用户、实体或者进程）无法否认其过去的参与活动；

实现方法：数字签名等。

加密

- 明文：原始数据（P）
- 密文：加密后的数据（C）
- 加密：明文经算法到密文 C=E（P）
- 解密：密文经算法到明文D（E（P））=P，E与D互为逆变换
- 密钥：控制算法实现的关键值：Ke、Kd

对称密钥

- 又叫单密钥、秘密密钥。加密和解密采用相同的密钥，即Ke=Kd 。
  - 加密、解密速度快。
  - 通信双方需要预先协商密钥。
  - 一般采用集中管理和分发密钥。
  - 一旦密钥泄密，安全就不能得到保障。

对称密钥加密方法

- 移位密码，使明文变位不变形

  COMPUTER　　C=CPEOURMT　　密钥d=3

- 替代密码，使明文换字不换形

  COMPUTER　　C=FRPSXWHU　　密钥k=3

- 乘积密码，移位密码和替代密码的有限次组合
- 数据加密标准 DES，使用移位、替代、分组、迭代等方法，明文64位、密钥64位、密文64位

移位加密法

移位加密法是通过重新安排原文字的顺序实现的。如

3 2 6 4 1 5
G E R MA N
l t c a n a
l l o w s t
ud e n t s
t o g e t c
l o s e u p
vi e w s

密钥为GERMAN，明文为：

it can allow students to get close up views

则密文为：

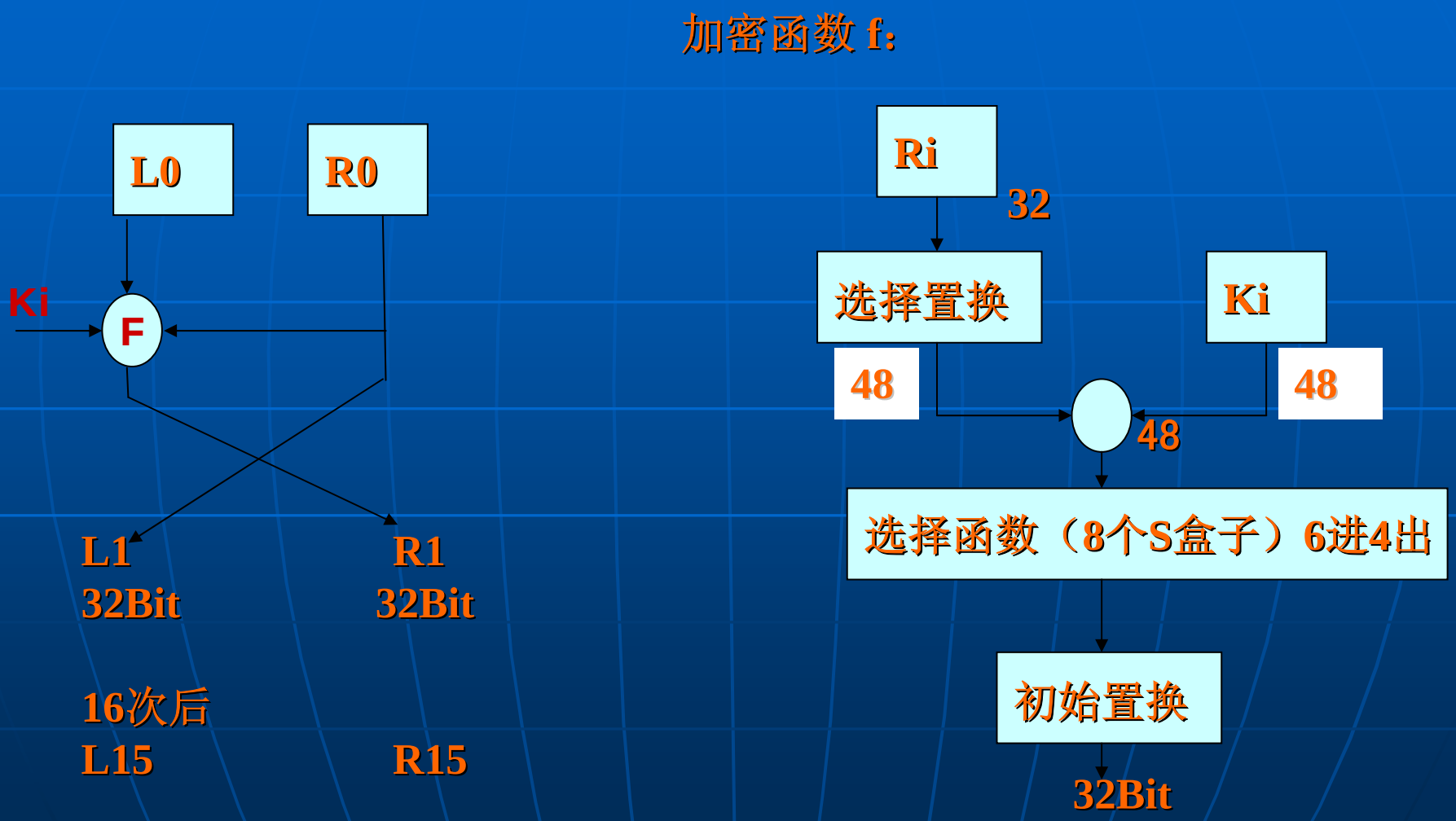
nsttustldooiilutlv awneewatscpcoegse

标准数据加密DES——加密框图

标准数据加密DES——子密钥生成

置换选择1：去8位奇偶校验，出56位
各一半28位，C0、D0
置换选择2：从56位中取48位成子密钥
16个子密钥

标准数据加密DES——乘积变换



标准数据加密DES——解密

64位密文输入，与加密过程一样，但第一次迭代用K16，最后一次用K1；乘积变换时，Ri、Li与加密时相反。

非对称密钥

- 加密和解密使用不同的密码 <Kpub, Kpriv>。Kpub公开，Kpriv由密钥持有人保密。公钥加密算法有RSA 算法等:
  - 用公钥加密，用私钥解密。
  - 加密强度很高，适合在网络环境中使用。
  - 加密、解密速度慢。
  - 一般用于协商、加密共享密钥，数字签

非对称密钥加密法RSA

- 原理：数学上的单向陷门函数，一个方向求解容易，逆向计算非常困难
- “大数分解和素性检测”数论难题：两个大素数相乘，计算结果容易，但将结果分解成两个大素数因子却非常困难

非对称密钥加密法RSA

- 设计:选两个大素数（100位以上）p、q，计算: r=p*q、z=（p-1）*（q-1）
- 选两个正整数d、e，满足: d、e与z互素，且满足: e*d=1（mod z）
- 则: （r，e）为公开密钥，（r，d）为私密密钥
- 加密C=P^e mod r，解密P=C^d mod r
- 明文P长度分组可选，最小为1字节，计算量主要是大数的n次方，速度慢

非对称密钥加密法RSA

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	1	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	5	E
Sender's computation				Receiver's computation		

P=3,q=11, n=33,e=3, d=7

公钥应用示例：电子证书

数字证书是经证书管理中心数字签名的文件。
通常包含以下内容：

- 证书的版本信息；
- 证书的序列号；
- 证书所使用的签名算法；
- 证书的发行机构名称；
- 证书的有效期；
- 证书所有人的名称；
- 证书所有人的公开密钥；
- 证书发行者对证书的签名

数字签名

- 张三拥有公钥 < Kpub, Kpriv >;将Kpub公开〈电子证书〉;
- 张三用 Kpriv对数据DATA进行加密，然后发送给李四;
- 李四用 Kpub〈电子证书〉对数据DATA进行解密，确认数据来自张三;
- 数字签名实际就是用私钥对一段数据进行加密。在实际中，由于公钥加密速度很慢，所以只对报文摘要进行加密，而不是对整个报文进行加密。

数字签名和数据安全

- 数字签名只保证数据确由发方发出并不能保证数据的安全传输。
- 要保证数据的私有性，还需要进行数据加密。

$$C = encrypt(PUBB, encrypt(PRVA, P))$$

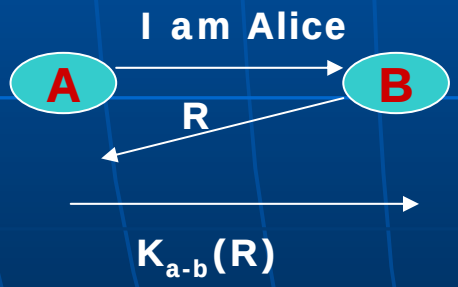
$$P = decrypt(PUBA, decrypt(PRVB, C))$$

加密的应用

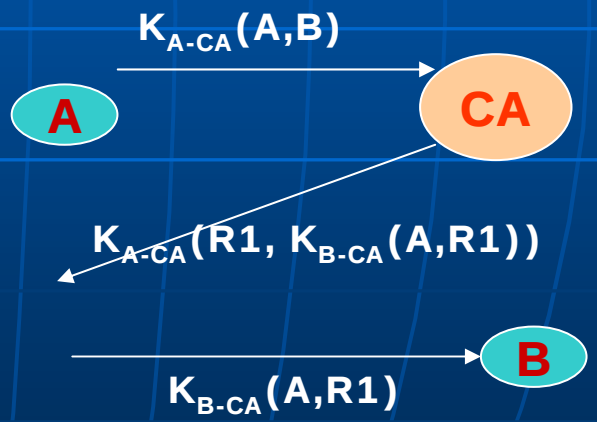
- 信息确由发方发出：数字签名 RSA，私钥加密，公钥解密 。
- 信息传输加密：DES加密明文，RSA加密DES密钥 。
- 信息只传给对方：RSA加密，公钥加密，私钥解密
- 确认信息完整性：文摘MD加密

身份认证（鉴别）

- 验证对方确实是他所声称的身份。
- 通常使用第三方信任机构进行身份认证和产生会话密钥。
- 公开密钥通常需要CA的数字签名。



挑战身份验证



用CA进行身份验证

电子商务中的安全

- 电子商务安全中的三个实体：消费者，商家和银行。
- 安全套接字层（SSL）为消费者和商家的通信提供了安全。
  - SSL在因特网交易中特别是WEB中被广泛应用。
  - SSL属于传输层的安全技术，更确切的，是传输层和应用层之间的会话层的安全技术。
  - 不足之处在于无法认证消费者是否使用盗用的信用卡或者商家是否可靠。
- 安全电子交易为三者之间的通信提供了安全保障。

SSL

- SSL通过以下握手建立安全会话：
  - 客户向服务器发送自己的SSL版本号和密码设置。
  - 服务器发送自己的SSL版本号、密码设置和CA签名证书。（通过菜单文件|属性|证书可以看到）
  - 客户通过可信任认证中心列表（通过菜单工具|Internet选项|内容|发行商可以看到），对服务器进行认证。产生一个会话密钥，用服务器的公共密钥加密后发给服务器。
  - 客户向服务器发送消息，通知服务器以后的消息使用这个会话密钥。并独立发送一个加密的消息结束握手。
  - 客户向服务器发送消息，通知服务器以后的消息使用这个会话密钥。并独立发送一个加密的消息结束握手。
  - SSL握手完成。SSL会话开始。

SET

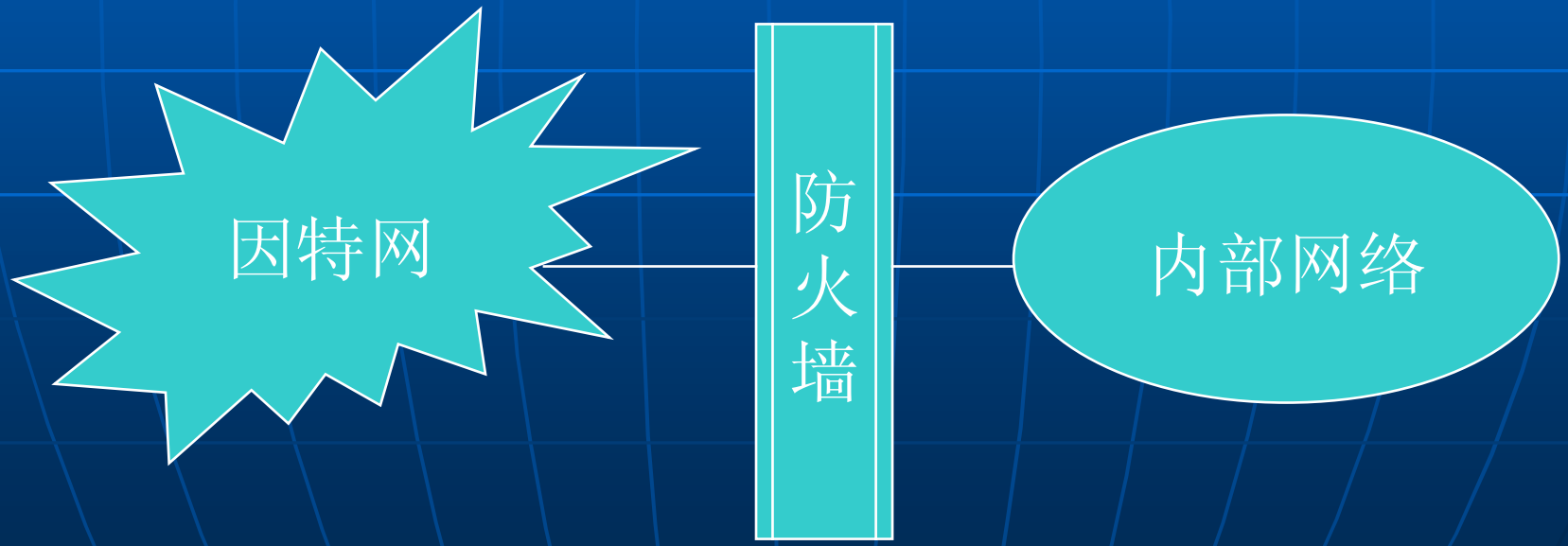
- SET是专为进行安全支付卡交易而设计的:
  - SET协议涉及三方，三方之间传送敏感数据都要进行加密
  - SET协议需要三方都有证书，同时消费者和商家的证书需要银行的签名。
  - 在SET交易中，消费者的支付卡号传送到银行，商家看不到明文的卡号。这个特征防止了欺骗偷盗或者粗心商家泄漏卡号。

网络层安全IPSEC

- IPSEC为所有的上层应用提供网络层的安全服务。
- 可以提供根据IP地址的身份认证。
- 无法进行基于用户的身份认证。
- 身份认证头（AH）可以提供身份认证和数据完整性安全
- 封装安全负载（ESP）可以提供数据完整性、身份认证和保密性。
- IPSEC在发送安全数据之前，先要进行握手建立网络层逻辑连接，即安全协定（SA），此连接是单工的。

防火墙

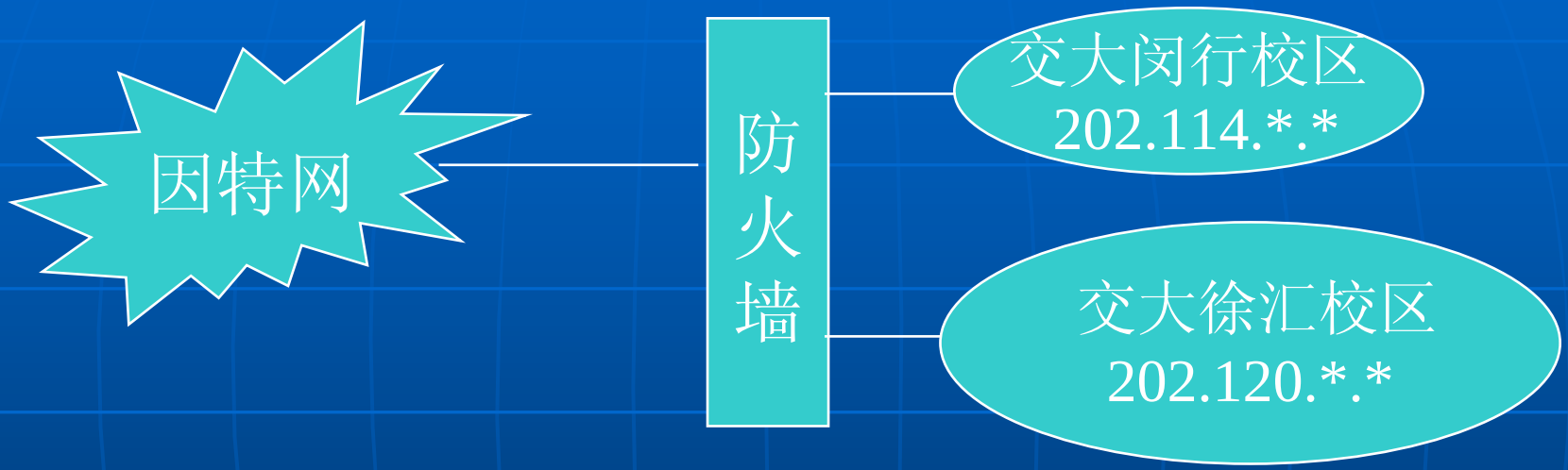
防火墙是在本地网与外部网之间的界面上构筑的保护层，保护内部网不受外部非法用户的攻击，是一个或一组网络设备。



包过滤技术

- 建立在网络层及传输层上，按源IP、目的IP、协议类型、端口号进行过滤。
- 容许符合安全规则的数据包通过，阻止非法数据包。
- 外部合法数据与内部网络近似直接通信，速度快、费用小、安全性低。
- 安全规则：
  - 没有被列为容许访问的都是被禁止的，保守，但安全。
  - 没有被列为禁止访问的都是被容许的，开放，不安全。

防火墙配置示例



允许: 202.114.*.* →*: FTP
允许: 202.120.*.* →*: FTP
允许: 202.114.*.* →*: WWW
允许: 202.120.*.* →*: WWW
允许: * → 202.120.*.* : WWW
缺省: 全部拒绝

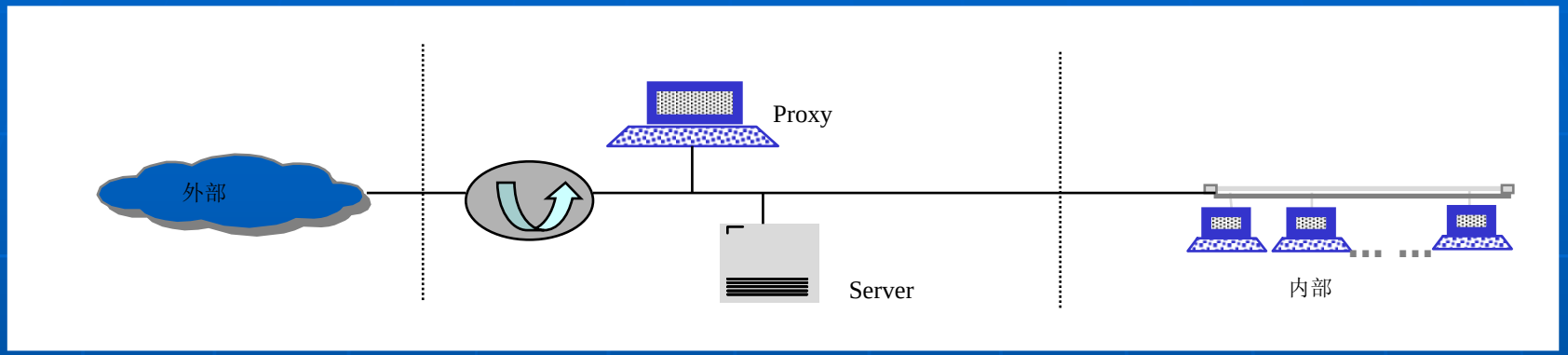
包过滤技术的缺点

- 不检测应用层数据内容
  - 无法防止对应用层协议的攻击
  - 无法防止对特定应用程序的攻击
  - 无法进行用户身份认证
- 无法防止来自网络内部的攻击
  - 统计表明，大多数攻击来自网络内部

应用网关和代理技术

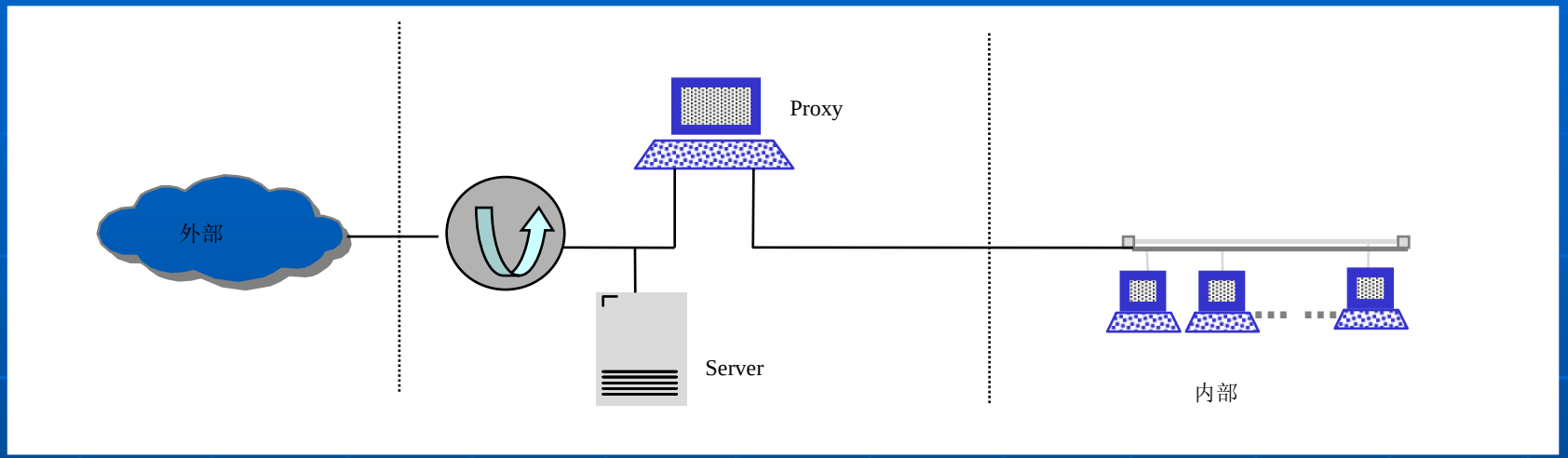
- 应用网关技术：建立在应用层上的协议过滤，针对特定的应用及过滤规则进行工作。
- 代理服务器技术 ：上述两个技术中一旦外部数据流满足规则，则与内部的计算机网络建立起直接联系，存在危险。代理服务器是将跨越防火墙的通信分为两段，内、外计算机网络的连接由两个终止于代理服务器上的“连接”来实现，真正实现内、外隔离。 安全性高，实现复杂，速度低 。

屏蔽主机型防火墙



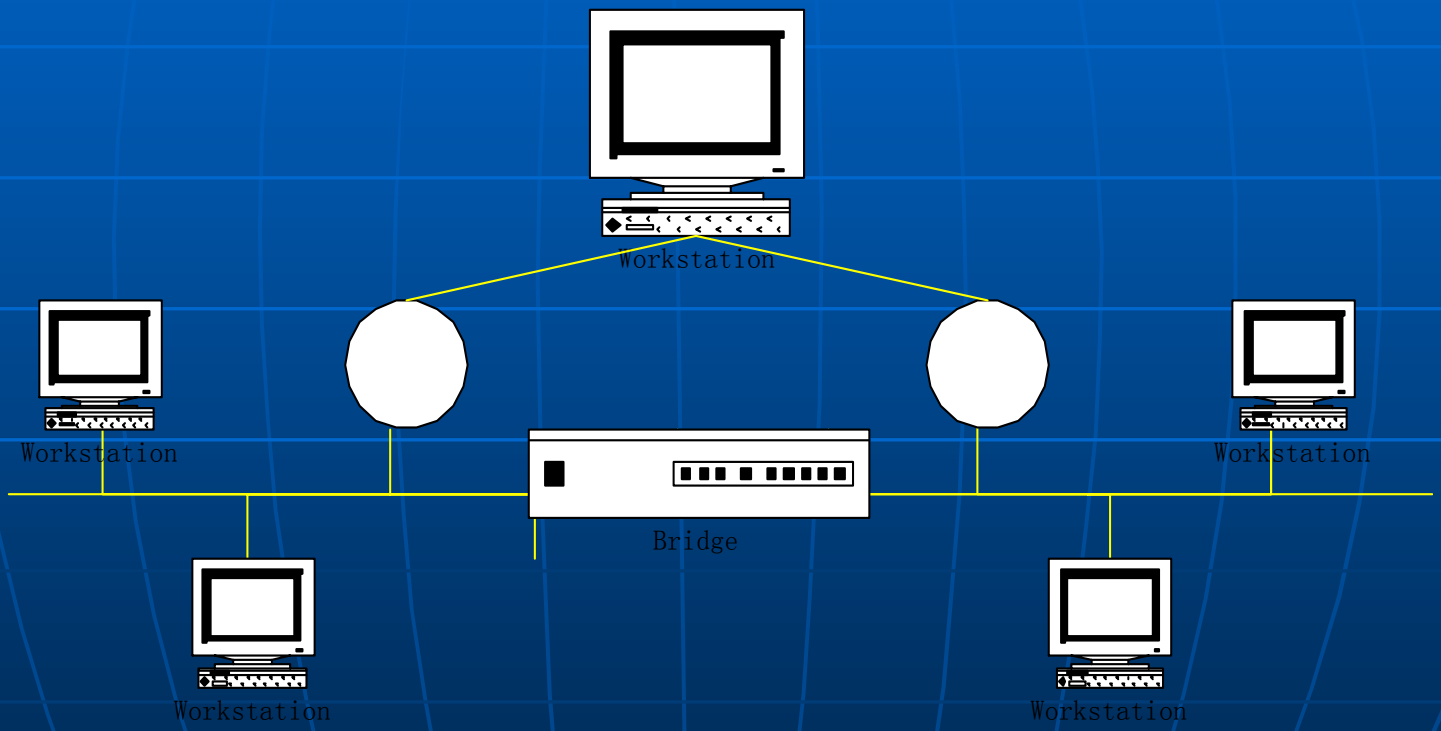
- 包过滤与代理技术相结合
- 过滤规则是外部网只能到达代理或公开服务器，由主机代理完成与内部网的连接
- 内部网可通过主机代理或直接经包过滤器与外部连接
- 物理连接上，内部网仍存在危险

双穴网关型防火墙



- 代理主机有两个网络接口
- 物理上将内、外网络分开，外部网只能通过主机代理完成与内部网的连接
- 内部网也只能通过主机代理与外部连接

入侵检测


Workstation
Workstation
Workstation
Bridge
Workstation
Workstation