

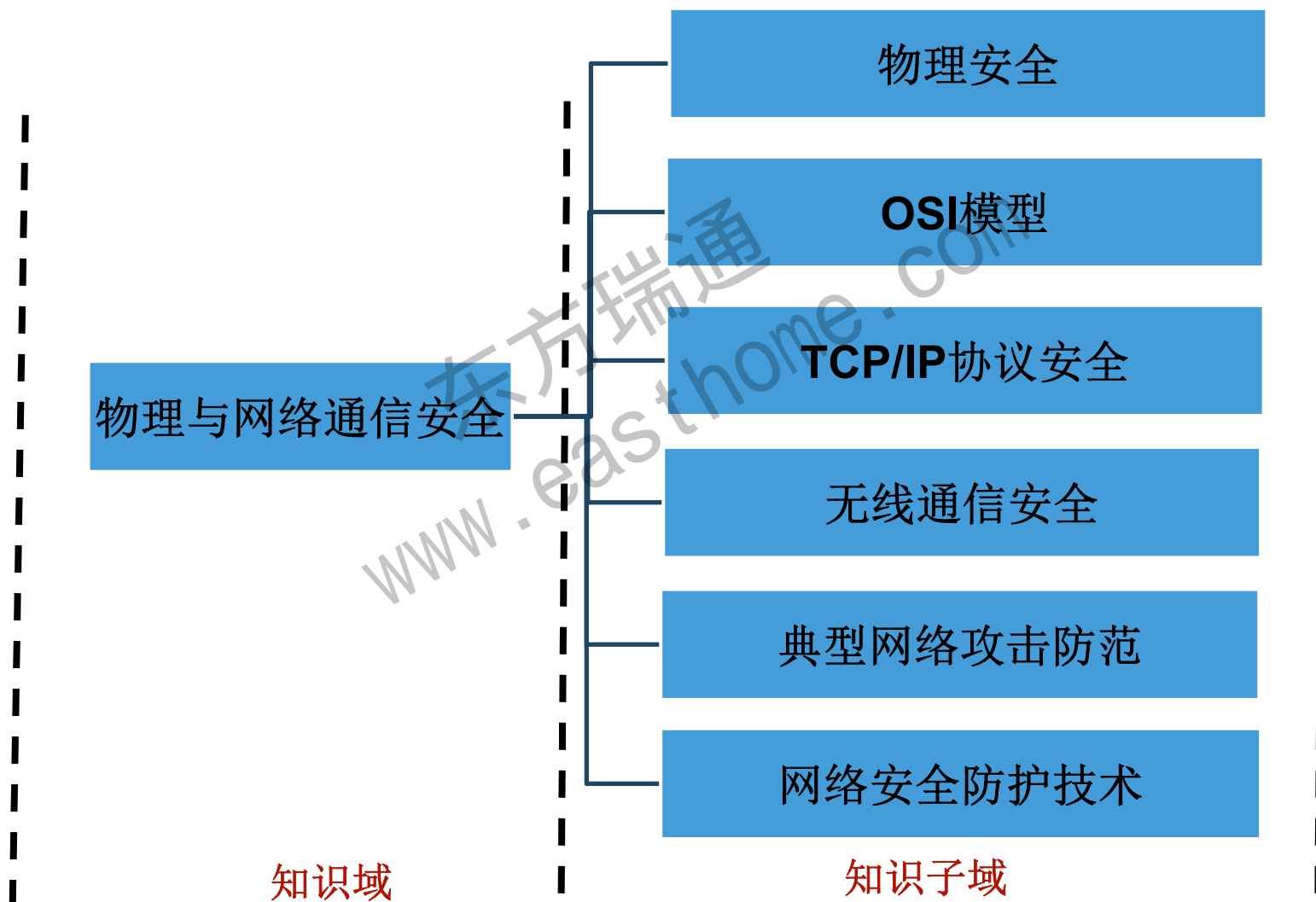
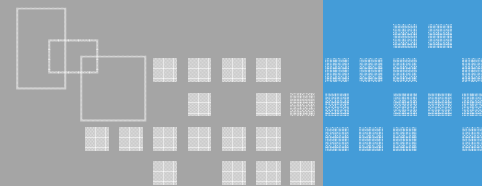


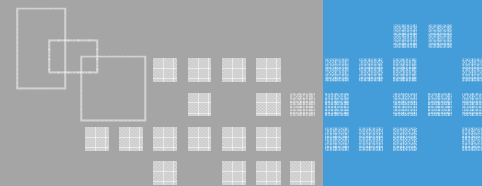
物理环境与网络通信安全

版本：4.2

讲师姓名 机构名称

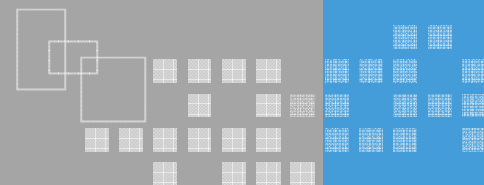
课程内容





❖ 环境安全

- 了解物理安全的重要性；
- 了解场地和环境安全应关注的因素：包括场地选择、抗震及承重、防火、防水、供电、空气调节、电磁防护、雷击及静电等防护技术；



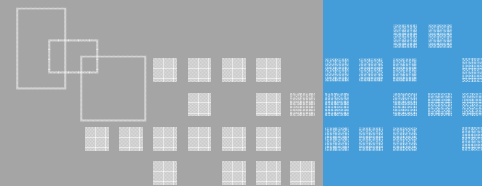
❖ 物理安全的重要性

- 信息系统安全战略的一个重要组成部分
- 物理安全面临问题
 - 环境风险不确定性
 - 人类活动的不可预知性

❖ 典型的物理安全问题

- 自然灾害（地震、雷击、暴雨、泥石流等）
- 环境因素（治安、交通、人流及经营性设施风险）
- 设备安全、介质安全、传输安全

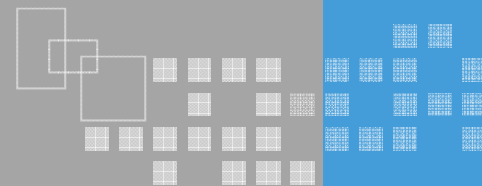
场地选择



- ❖ 区域：避开自然灾害高发区域
- ❖ 环境：远离可能的危险因素
 - 治安、人流量等
 - 加油站、化工厂等
- ❖ 其他：消防、交通便利

东月瑞通
www.easthome.com

抗震及承重



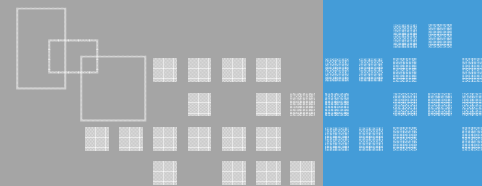
❖ 抗震：国标 《结构抗震设计规范》)

- 特殊设防类
- 重点设防类
- 标准设防类

❖ 承重

- 考虑设计（建筑的设计是否考虑了应对可能的偶然事件）
- 考虑时间因素（建筑有效期）
- 考虑使用因素（正常使用、正常维护）

火灾



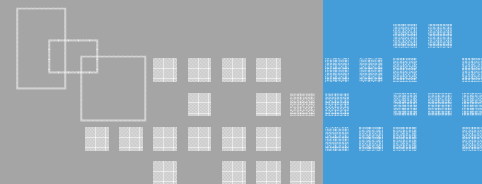
❖ 预防：防火设计及阻燃材料

❖ 检测：火灾探测器

- 感烟
- 感温
- 感光
- 可燃气体探测

❖ 抑制

- 水（较少使用，通常做周边防护）
- 气体：二氧化碳、七氟丙烷、三氟甲烷等



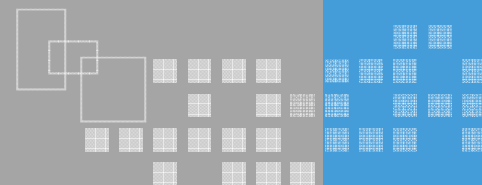
❖ 防水

- 远离水浸威胁（参考场地选择）
- 检测：水浸探测器
- 处置：在应急事件处置中要安排相应的处置流程

❖ 供电

- 双路供电
- 发电机
- UPS

❖ 空气调节

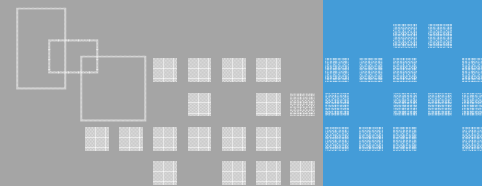


❖ 电磁防护

- 解决电磁辐射产生的信息泄露问题
 - 电磁屏蔽：屏蔽线、屏蔽机柜、屏蔽机房
 - 信号干扰：避免信息还原
 - Tempest技术：对电磁泄漏信号中所携带的敏感信息进行分析、测试、接收、还原以及防护的一系列技术领域的总称

❖ 雷击及静电

- 直击雷：避雷针、法拉第笼
- 感应雷：电涌保护器
- 静电：放电、防静电服



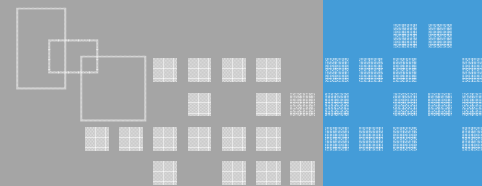
❖ 设施安全

- 了解安全区域的概念及相关防护要求；
- 了解边界防护的概念及相关防护要求；
- 理解审计及监控的概念及相关防护要求。

❖ 传输安全

- 理解同轴电缆、双绞线、光纤等有线传输技术及安全特点；
- 理解无线安全传输技术及安全特点；

设施安全-安全区域与边界防护

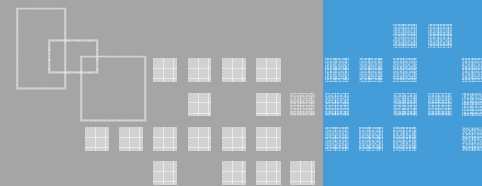


❖ 安全区域

- 建立安全区域，明确物理安全边界
- 对受控区域进行保护，建立屏蔽及访问控制机制

❖ 边界防护

- 所有物理出入通道的防护
 - 门：锁、门禁
 - 窗：铁栅栏
 - 通风口

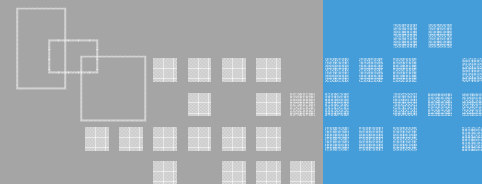


❖ 审计及监控

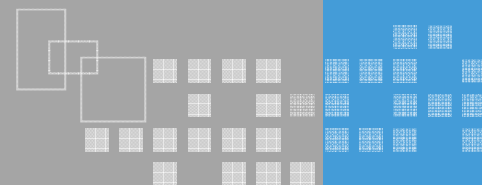
- 对安全区域的出入行为进行记录
- 对非法闯入进行检测

❖ 实现方式

- 出入记录（登记、门禁）
- 闭路电视
- 非法闯入探测（红外微波双鉴探头、玻璃破碎探测器等）
- 安保人员



- ❖ 有线传输：同轴电缆、双绞线、光纤
 - 安全风险：非法接入、破坏
 - 防护措施：保护措施（深埋、套管）、标识
- ❖ 无线传输
 - 安全风险：开放信道
 - 防护措施：加密



❖ OSI 模型

- 理解OSI七层模型构成及每一层的作用；
- 理解协议分层的作用。

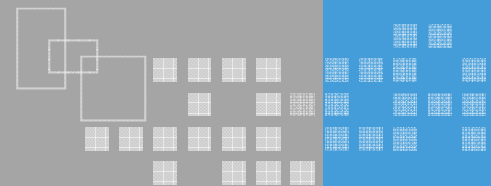
❖ OSI 模型通信过程

- 理解OSI模型通信过程及数据封装、分用等概念

❖ OSI 模型安全体系构成

- 了解OSI模型安全体系的构成；
- 了解OSI模型的五类安全服务、八种安全机制的概念。

ISO/OSI 七层模型结构



- ❖ 模型定义了网络中不同计算机系统进行通信的基本过程和方法
- ❖ 底层协议
 - 偏重于处理实际的信息传输，负责创建网络通信连接的链路，包括物理层、数据链路层、网络层和传输层
- ❖ 高层协议
 - 处理用户服务和各种应用请求，包括会话层、表示层和应用层

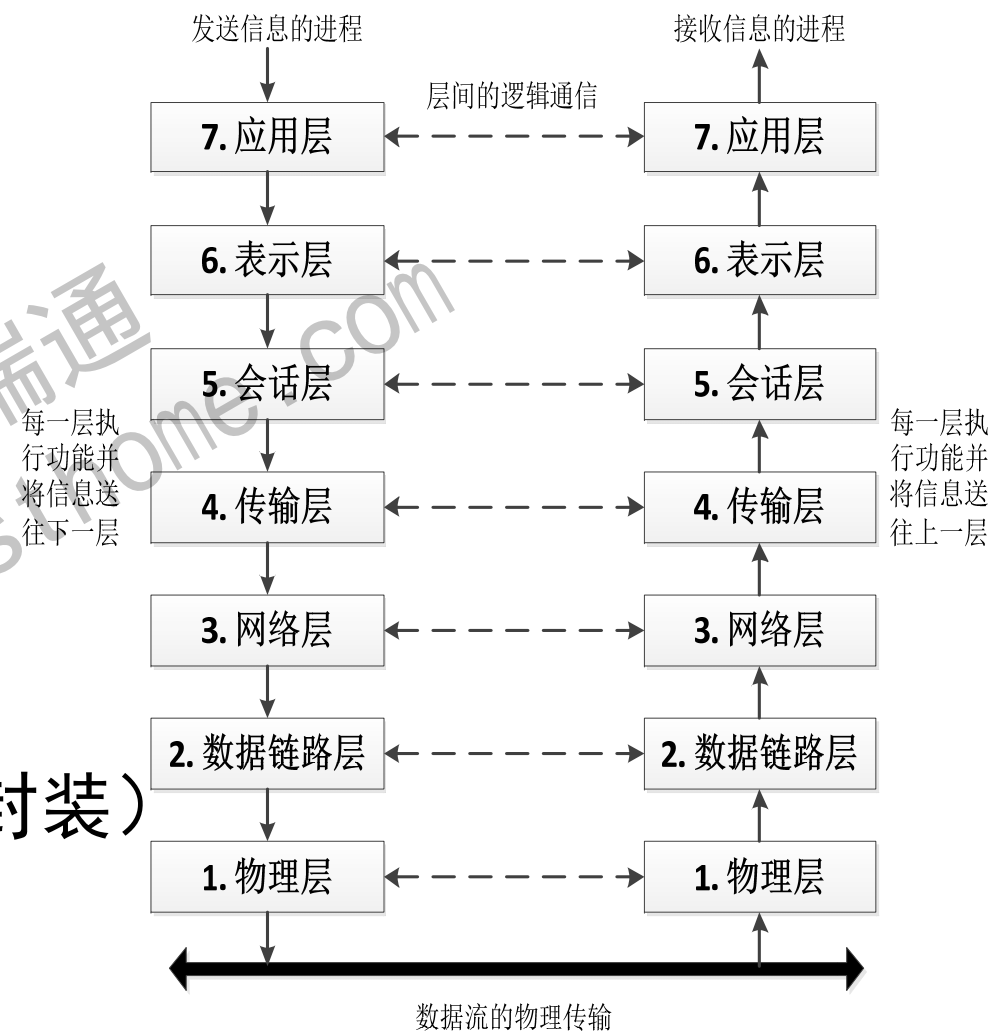


OSI模型特点

❖ 分层结构的优点

- 各层间相互独立
- 降低复杂性
- 促进标准化工作
- 协议开发模块化

❖ 数据封装与分用（解封装）



OSI 安全体系结构

❖ 目标

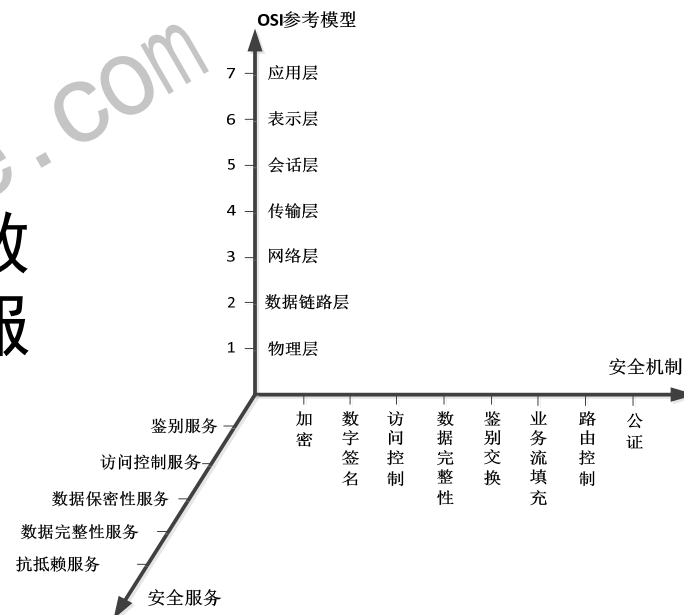
- 保证异构计算机进程与进程之间远距离交换信息的安全

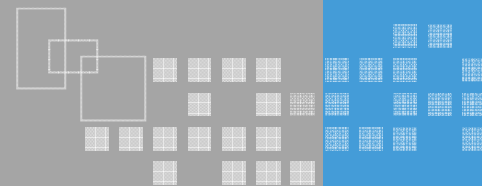
❖ 五类安全服务

- 鉴别服务、访问控制服务、数据完整性服务、数据保密性服务和抗抵赖服务

❖ 八种安全机制

- 加密、数据签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制和公正





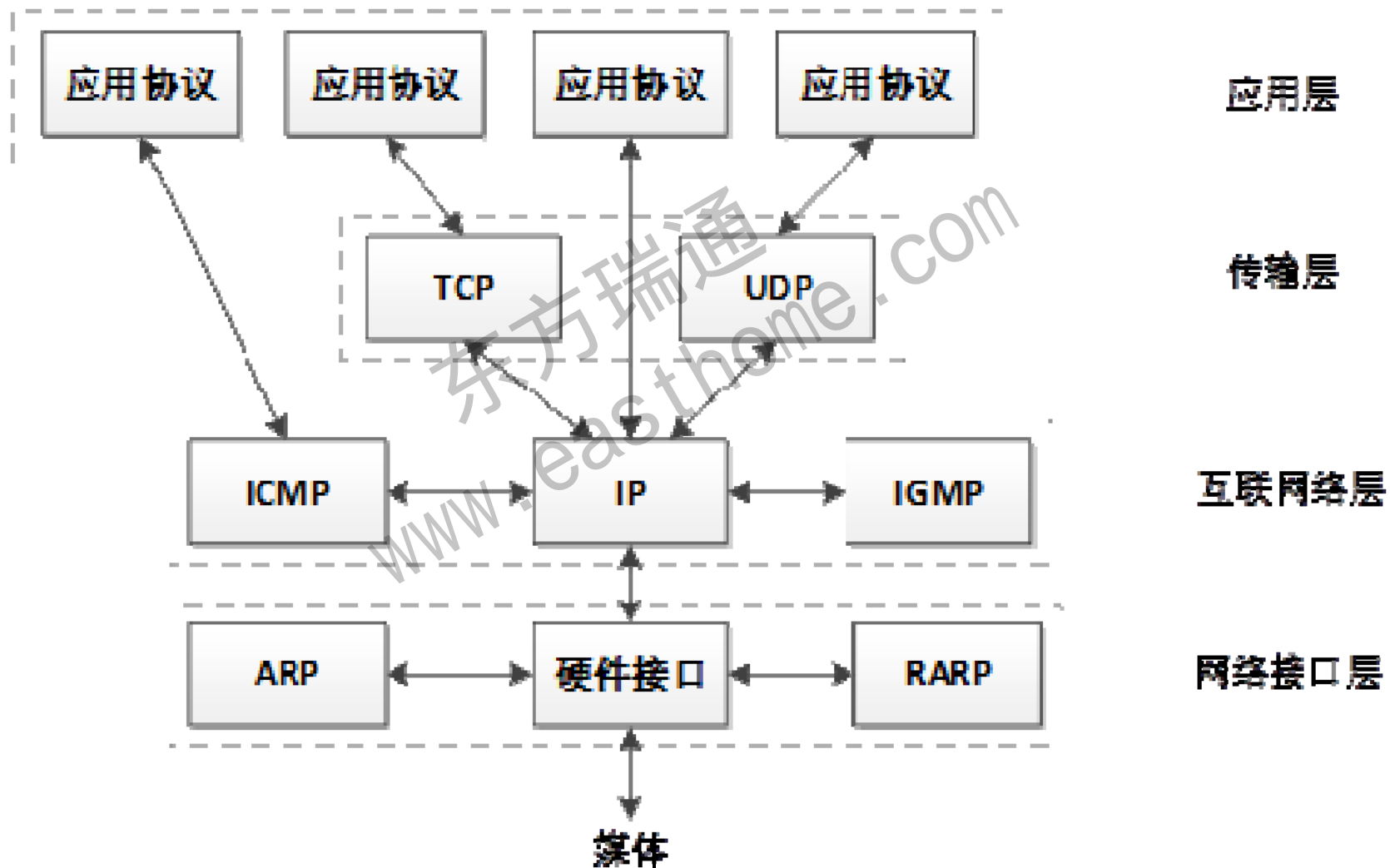
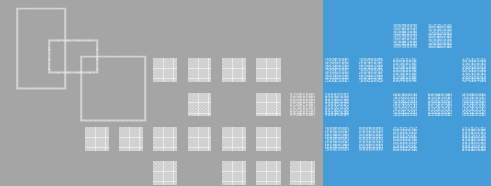
❖ 协议结构及安全问题

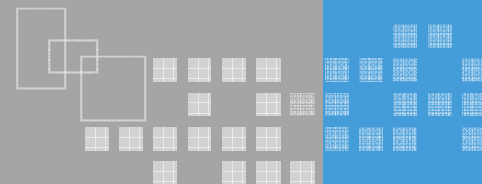
- 了解TCP/IP协议的体系及每一层的作用；
- 了解网络接口层的作用及面临的网络安全问题；
- 了解IP协议的工作机制及面临的安全问题；
- 了解传输层协议TCP和UDP的工作机制及面临的安全问题；
- 了解应用层协议面临安全问题。

❖ 安全解决方案

- 了解基于TCP/IP协议簇的安全架构；
- 了解IPv6对网络安全的价值。

TCP/IP协议结构





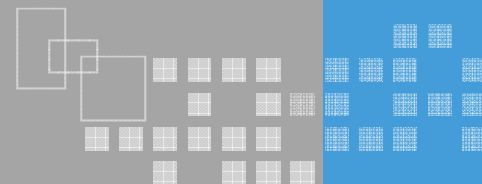
❖ 主要协议

- ARP
- RARP

❖ 安全问题

- 损坏：自然灾害、动物破坏、老化、误操作
- 干扰：大功率电器/电源线路/电磁辐射
- 电磁泄漏：传输线路电磁泄漏
- 欺骗：ARP欺骗
- 嗅探：常见二层协议是明文通信的
- 拒绝服务：mac flooding, arp flooding等

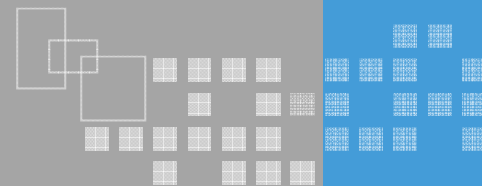
网络互联层核心协议-IP协议



- ❖ IP是TCP/IP协议族中最为核心的协议
- ❖ 目前广泛使用的IPv4提供无连接不可靠的服务

版本	包头长度	服务类型	数据包长度	
标识			标记	偏移
生存期		协议类型	包头校验和	
源IP地址				
目的IP地址				
可选项				
用户数据				

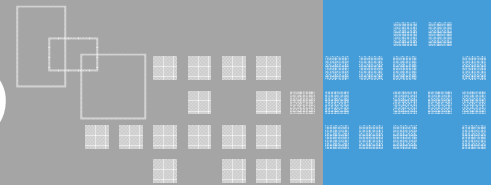
网络互联层安全问题



- ❖ 拒绝服务：分片攻击（teardrop）/死亡之ping
- ❖ 欺骗：IP源地址欺骗
- ❖ 窃听：嗅探
- ❖ 伪造：IP数据包伪造

东瑞通
www.easthome.com

传输层协议-TCP（传输控制协议）



❖ 提供面向连接的、可靠的字节流服务

❖ 提供可靠性服务

- 数据包分块、发送接收确认、超时重发、数据校验、数据包排序、控制流量
-

16位源端口号								16位目的端口号							
32位序号															
32位确认序号															
偏移量	保留位	U	A	P	R	S	F	16位窗口指针							
16位校验和								16位紧急指针							
数据															

传输层协议-UDP（用户数据报协议）

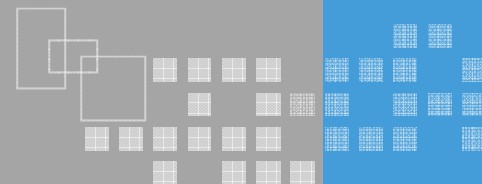
❖ 提供面向事务的简单不可靠信息传送服务

❖ 特点

- 无连接、不可靠
- 协议简单、占用资源少，效率高
-

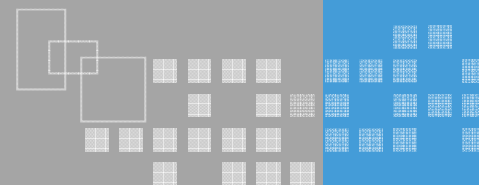
16位源端口号	16位目的端口号
16位UDP报文长度	16位校验和
数据	

传输层安全问题



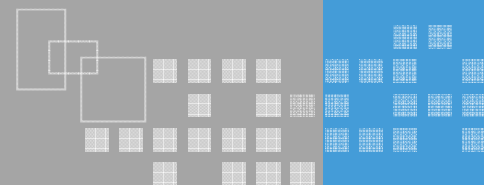
- ❖ 拒绝服务: syn flood/udp flood/Smurf
- ❖ 欺骗: TCP会话劫持
- ❖ 窃听: 嗅探
- ❖ 伪造: 数据包伪造

东方瑞通
www.easthome.com



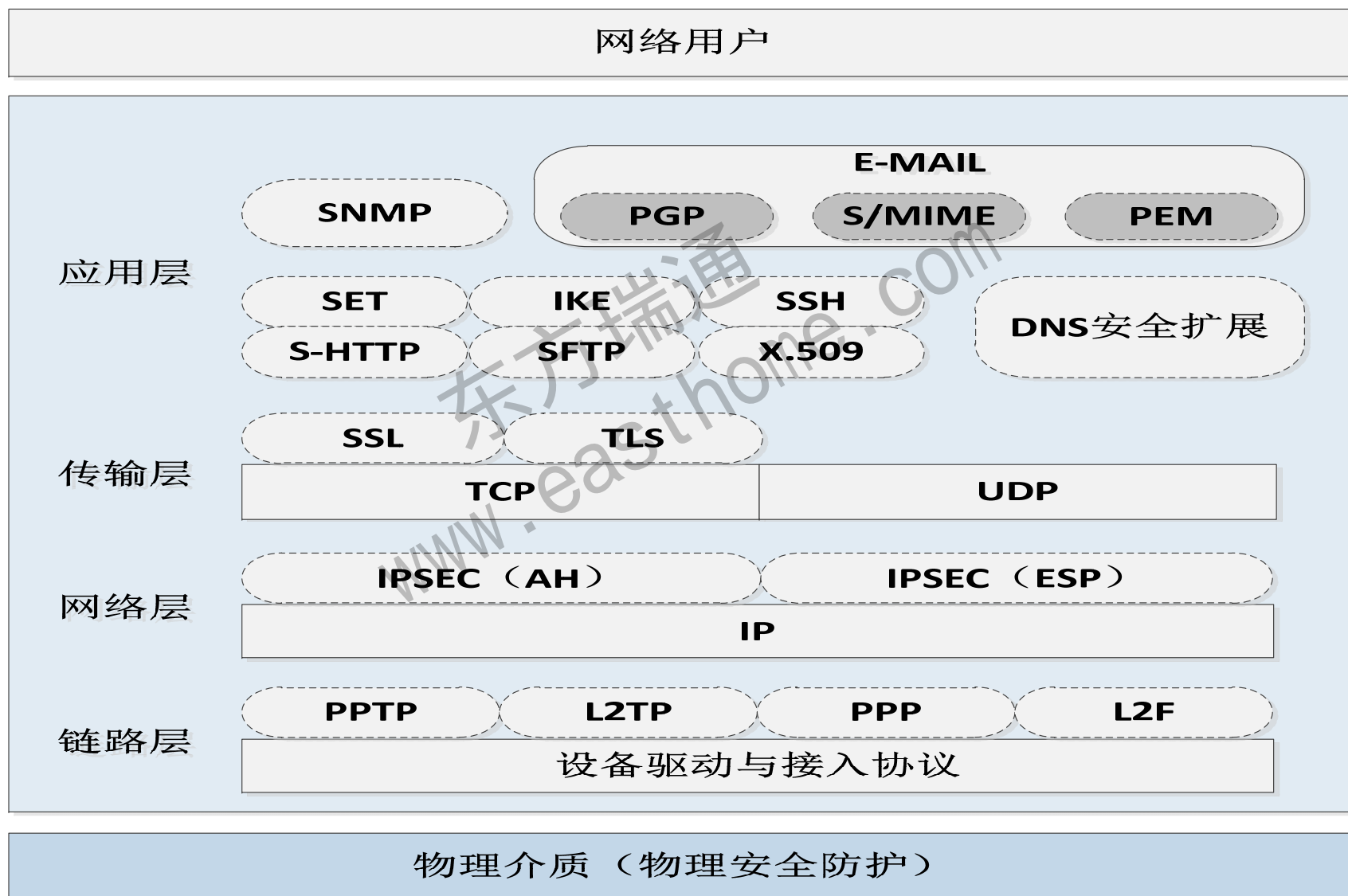
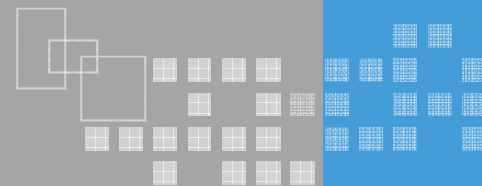
- ❖ 应用层协议定义了运行在不同端系统上的应用程序进程如何相互传递报文
- ❖ 典型的应用层协议
 - 域名解析：DNS
 - 电子邮件：SMTP/POP3
 - 文件传输：FTP
 - 网页浏览：HTTP
 -

应用层协议安全问题

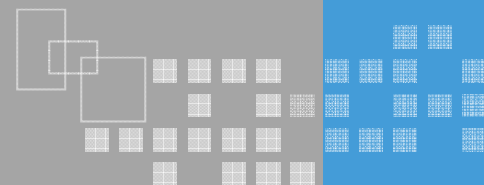


- ❖ 拒绝服务：超长URL链接
- ❖ 欺骗：跨站脚本、钓鱼式攻击、cookie欺骗
- ❖ 窃听：数据泄漏
- ❖ 伪造：应用数据篡改
- ❖ 暴力破解：应用认证口令暴力破解等
- ❖

基于TCP/IP协议簇的安全架构



知识子域：无线通信安全



❖ 无线局域网安全

- 了解无线局域网安全协议WEP、WPA2、WAPI等工作机制及优缺点；
- 理解无线局域网安全防护策略。

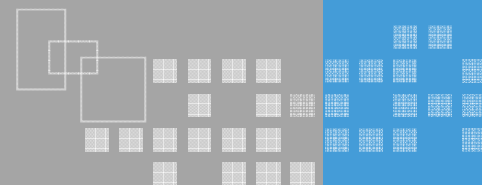
❖ 蓝牙通信安全

- 了解蓝牙技术面临的保密性、完整性、非授权连接、拒绝服务等安全威胁；
- 理解使用蓝牙的安全措施。

❖ RFID通信安全

- 了解RFID的概念及针对标签、针对读写器和针对信道的攻击方式；
- 理解RFID安全防护措施。

无线局域网安全协议-WEP



❖ 提供功能

- 传输加密
- 接入认证（开放式认证、共享密钥认证）

❖ 开放式认证系统

- 通过易于伪造的SSID识别，无保护、任意接入
- MAC、IP地址控制易于伪造

❖ 共享密钥认证

- 弱密钥问题
- 不能防篡改
- 没有提供抵抗重放攻击机制

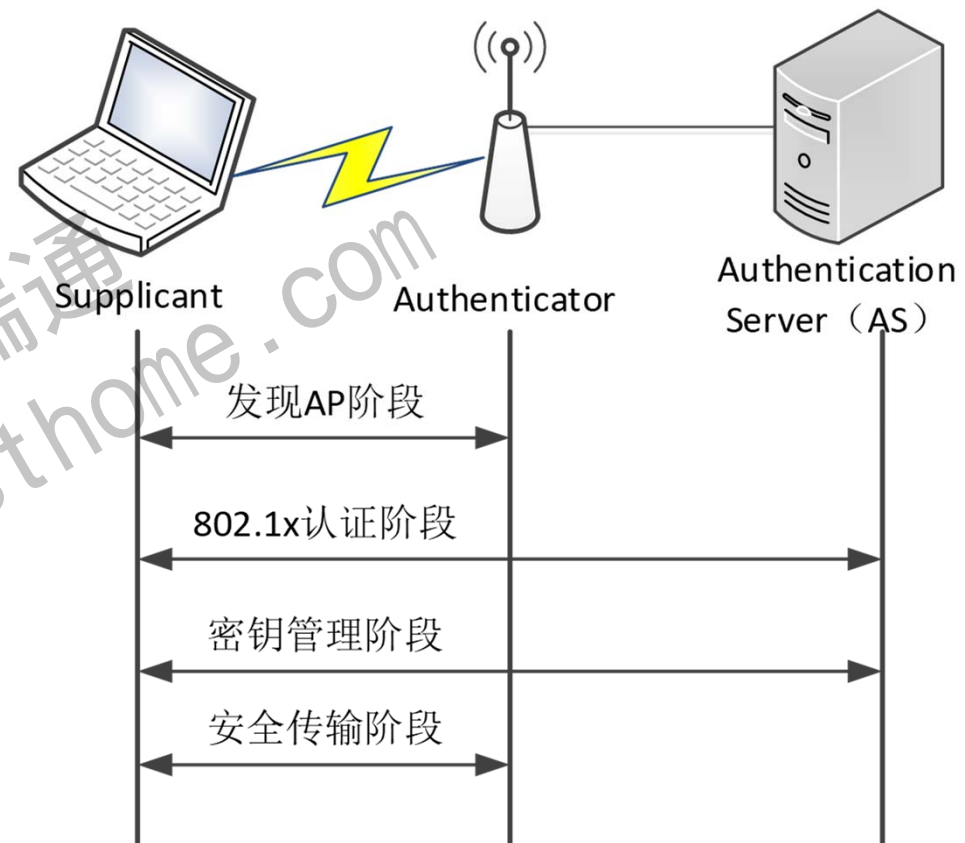
无线局域网安全协议-WPA、WPA2

❖ 802.11i

- WPA (802.11i草案)
- WPA2 (802.11i正式)

❖ 802.11i运行四阶段

- 发现AP阶段
- 802.11i认证阶段
- 密钥管理阶段
- 安全传输阶段



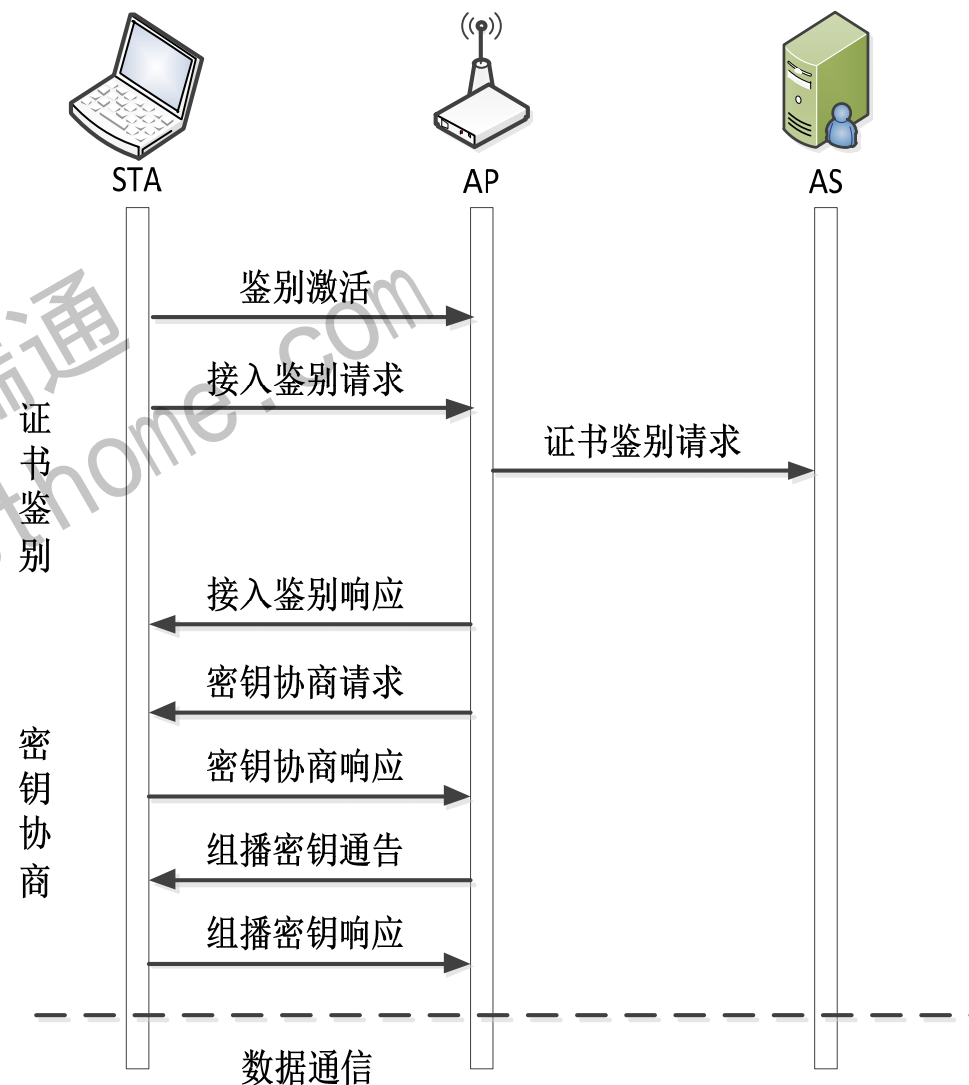
WAPI 无线安全协议

❖ WAPI 的构成

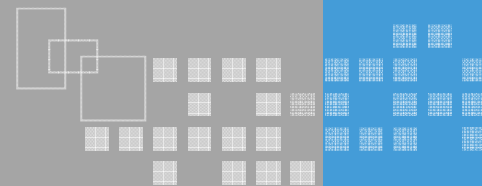
- WAI，用于用户身份鉴别
- WPI，用于保护传输安全

❖ WAPI 的安全优势

- 双向三鉴别（服务器、AP、STA）
- 高强度鉴别加密算法



无线局域网应用安全策略



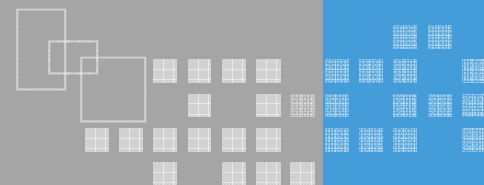
❖ 管理措施

- 组织机构安全策略中包含无线局域网安全管理策略
- 结合业务对无线局域网应用进行评估，制定使用和管理策略

❖ 技术措施

- 加密、认证及访问控制
- 访客隔离
- 安全检测措施

近距离无线通信安全-蓝牙

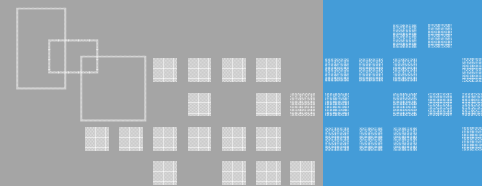


❖ 安全威胁

- 保密性威胁：密钥生成基于配对的PIN
- 完整性威胁：未授权设备实施的中间人攻击
- 可用性威胁：拒绝服务
- 非授权连接

❖ 蓝牙安全应用

- 蓝牙设备选择：技术上应具备抵抗以上威胁的能力
- 蓝牙设备使用：企业应用应建立管理要求

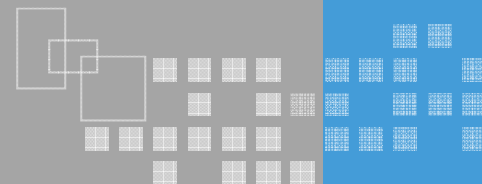


❖ 安全威胁

- 针对标签攻击：数据窃取、标签破解及复制
- 针对读写器的攻击：拒绝服务、恶意代码
- 针对无线信道的攻击：干扰、嗅探

❖ 安全防护

- 重要的RFID标签（例如用于身份鉴别），支持Kill和休眠的标签
- 使用高安全加密算法的标签
- 涉及资金的应用使用在线核查方式



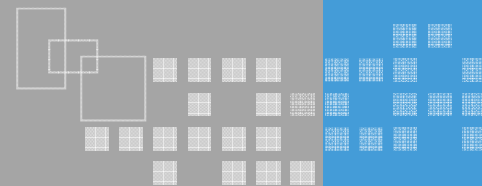
❖ 欺骗攻击

- 了解IP欺骗、ARP欺骗、DNS欺骗等电子欺骗攻击的实现方式及防护措施。

❖ 拒绝服务攻击

- 了解SYN Flood、UDP Flood、Teardrop等拒绝服务攻击实现方式；
- 了解分布式拒绝服务攻击实现方式及拒绝服务攻击应对策略。

网络攻击与防范-欺骗攻击

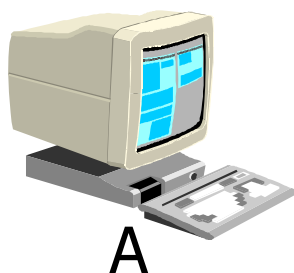


❖ 欺骗攻击 (Spoofing)

- 通过伪造源于可信任地址的数据包以使一台机器认证另一台机器的复杂技术

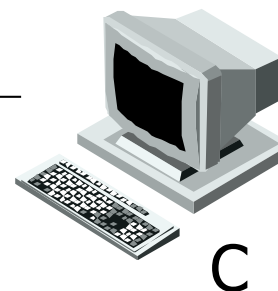
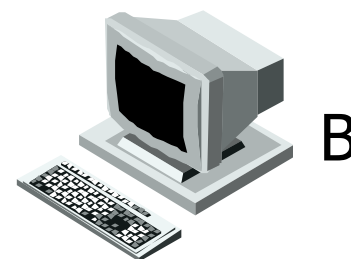
❖ 常见类型

- IP欺骗
- ARP欺骗
- DNS欺骗
-



东方瑞通
www.easthome.com

Hello, I'm B!



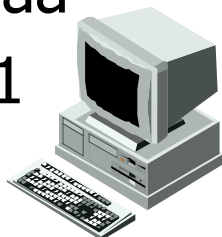
ARP欺骗实现

❖ ARP协议实现特点

- ARP协议特点：无状态，无需请求可以应答
- ARP实现：ARP缓存

aa:aa:aa:aa:aa

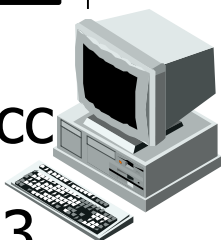
192.168.1.1



AA:AA:AA:AA:AA
192.168.1.1
Hello

CC:CC:CC:CC:CC

192.168.1.3



CC:CC:CC:CC:CC
192.168.1.1
Hello

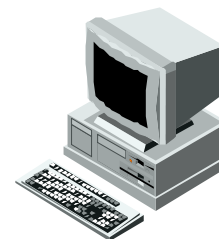
MAC cc:cc:cc:cc:cc is 192.168.1.1

Internet地址

192.168.1.1

物理地址

cc:cc:cc:cc:cc



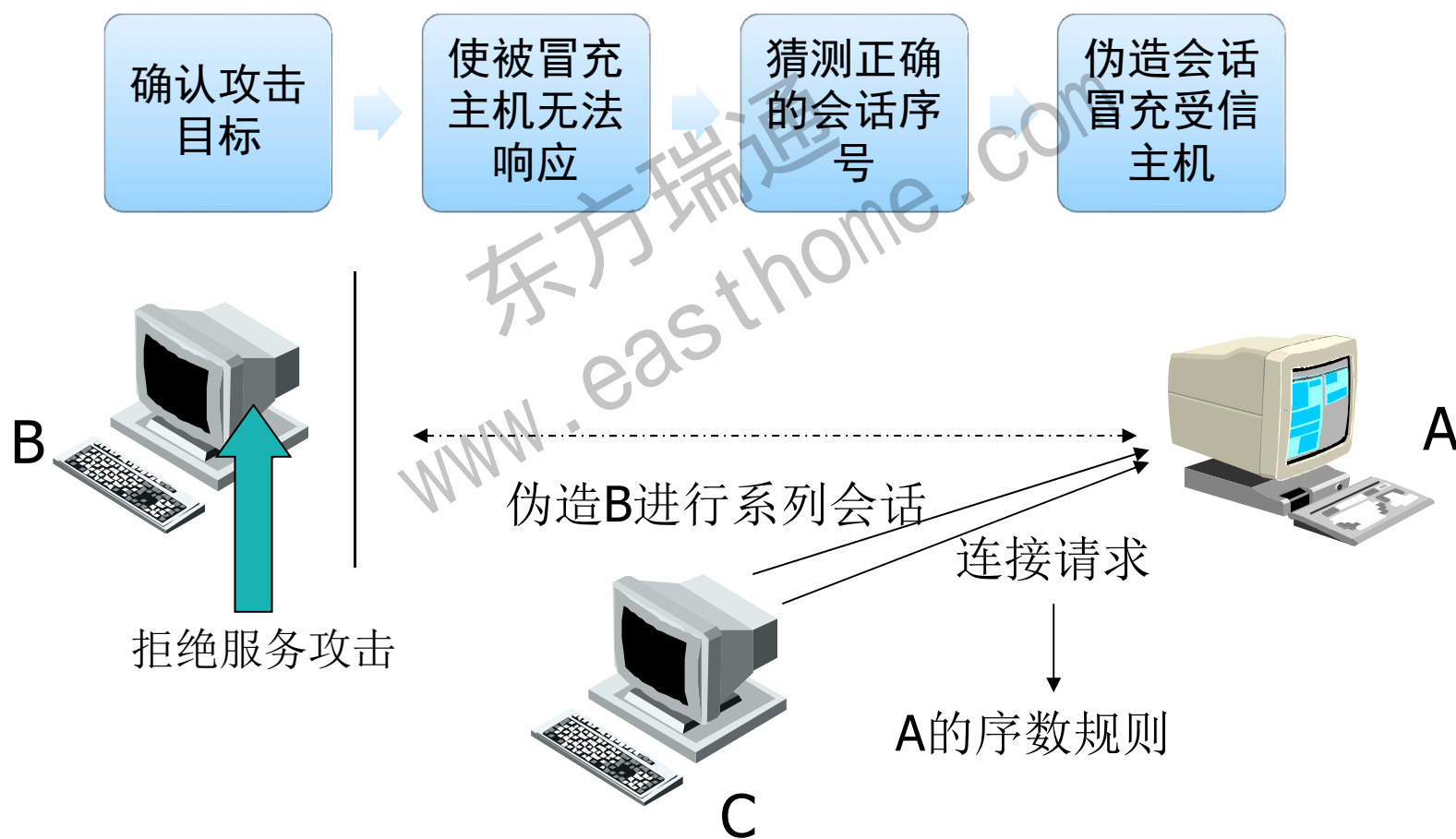
收到，我会缓存！

bb:bb:bb:bb:bb

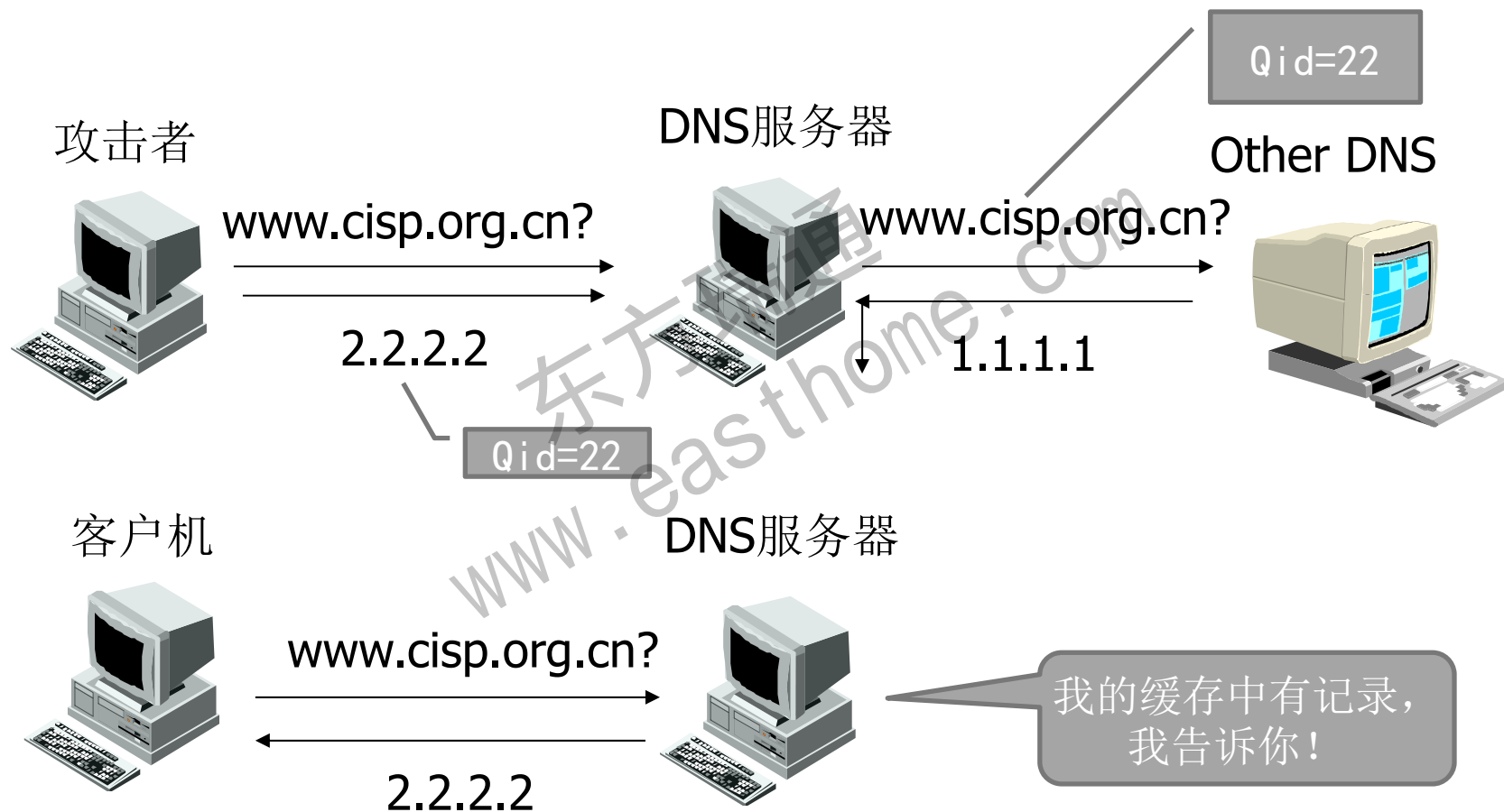
192.168.1.2

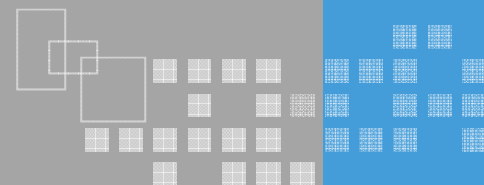
典型攻击：IP欺骗

❖ IP欺骗是一系列步骤构成的攻击



DNS欺骗-攻击实现






❖ 拒绝服务攻击

- 让被攻击的系统无法正常进行服务的攻击方式

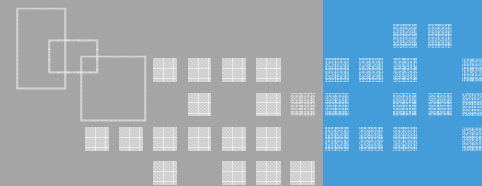
❖ 拒绝服务攻击方式

- 利用系统、协议或服务的漏洞
 - 利用TCP协议实现缺陷
 - 利用操作系统或应用程序的漏洞
- 目标系统服务资源能力
 - 利用大量数据挤占网络带宽
 - 利用大量请求消耗系统性能
- 混合型

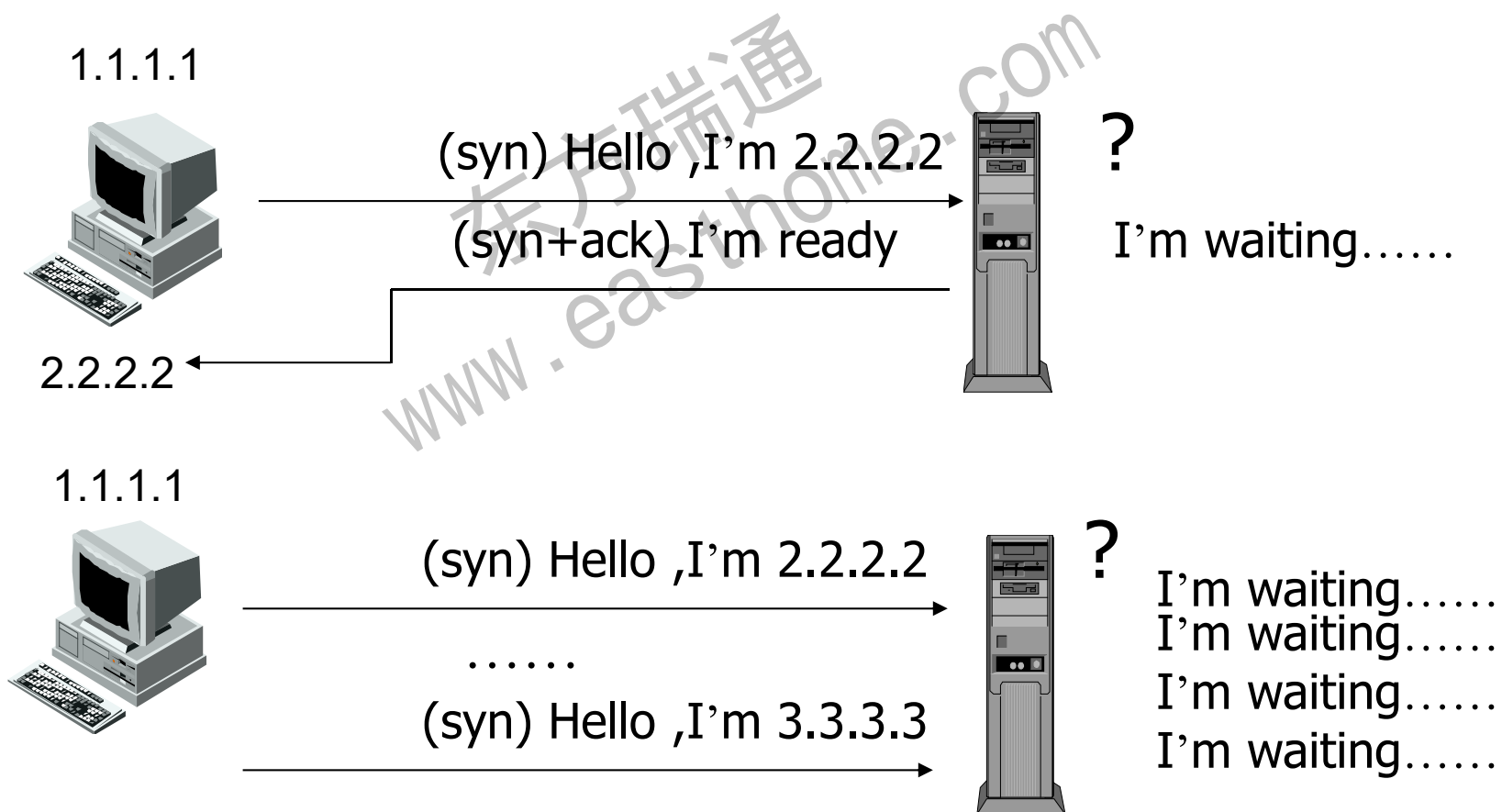


拒绝服务
是一类攻
击方式的
统称！

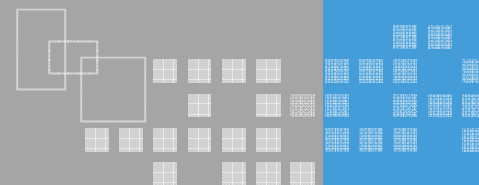
典型攻击：SYN Flood



❖ 原理：伪造虚假地址连接请求，消耗主机连接数



网络攻击与防范-拒绝服务攻击

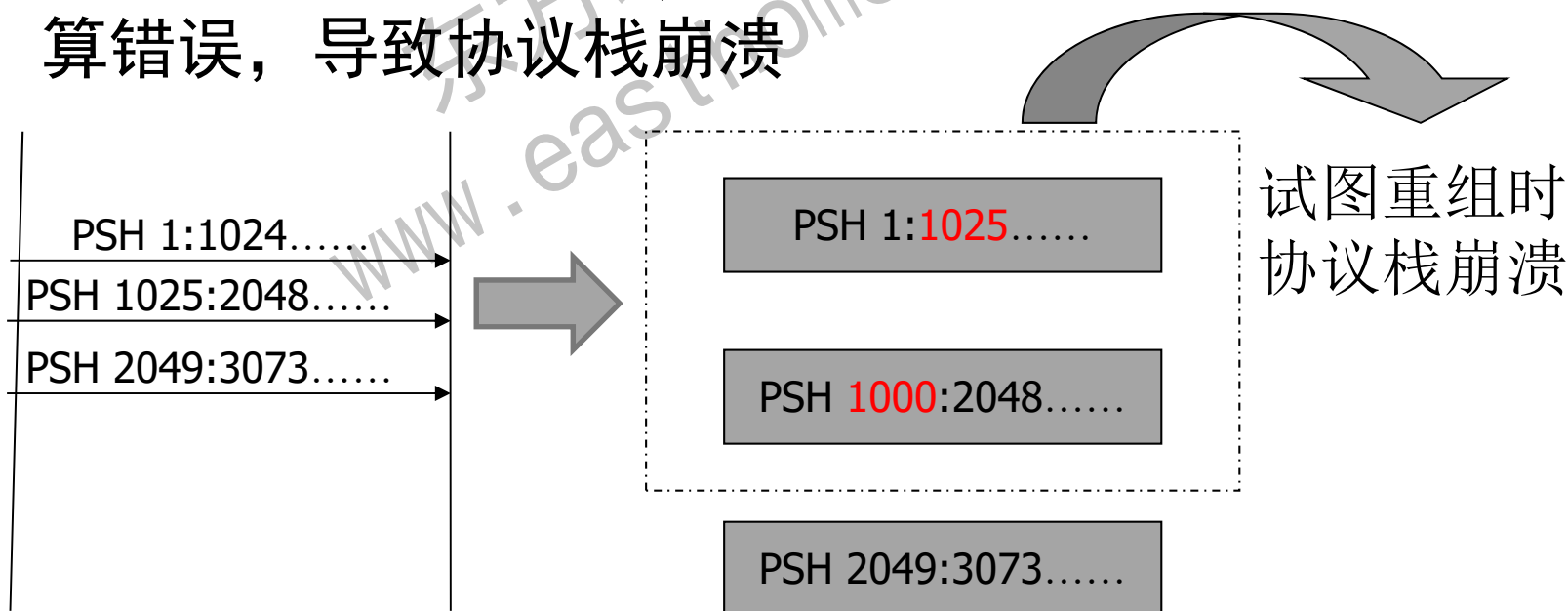


❖ UDP Flood

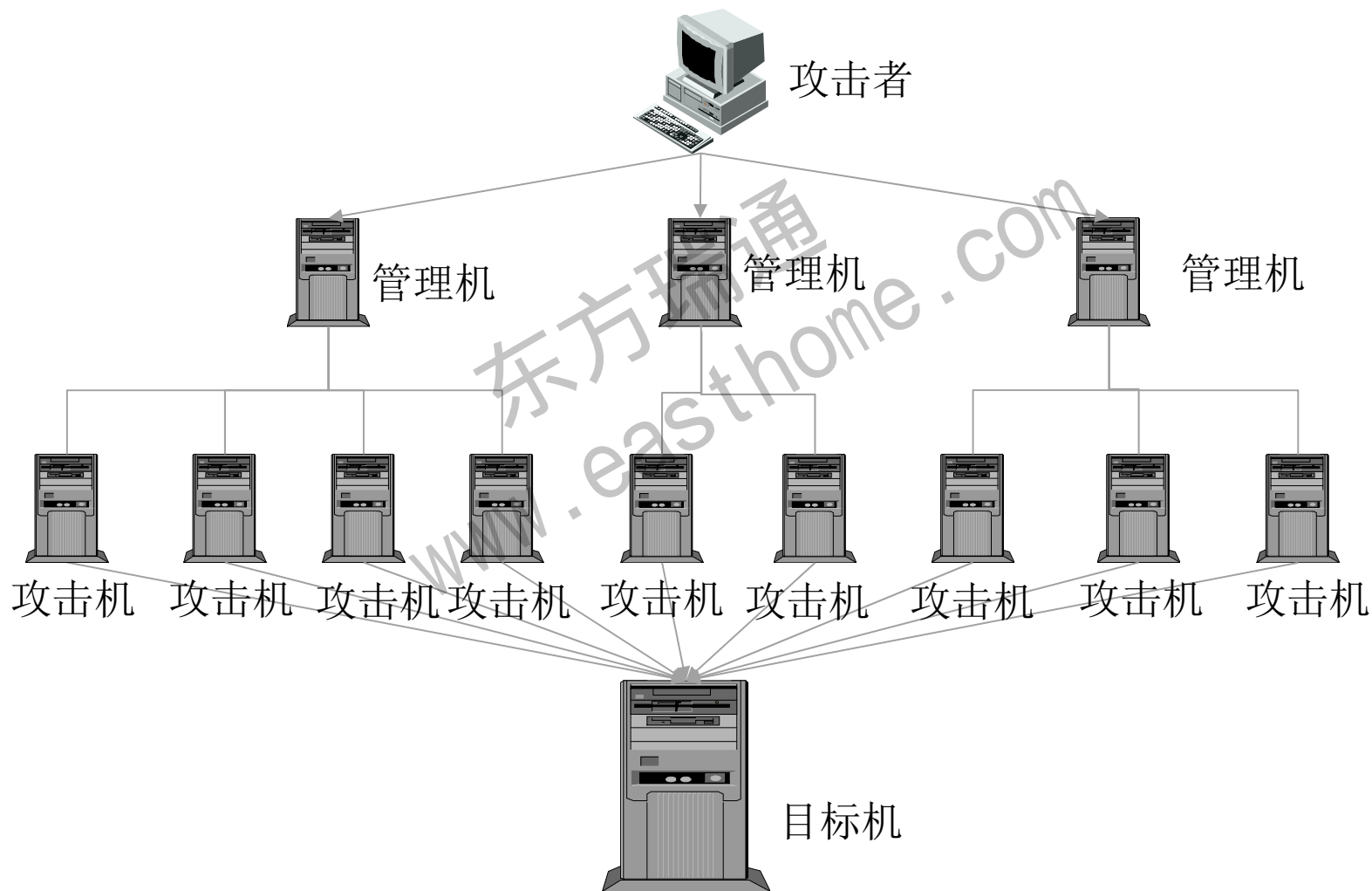
- 利用UDP协议实现简单、高效，形成流量冲击

❖ Teardrop

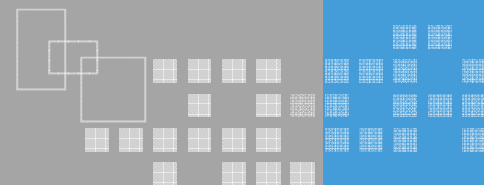
- 构造错误的分片信息，系统重组分片数据时内存计算错误，导致协议栈崩溃



网络攻击与防护-分布式拒绝服务攻击 (DDoS)



拒绝服务攻击的防御



❖ 管理防御

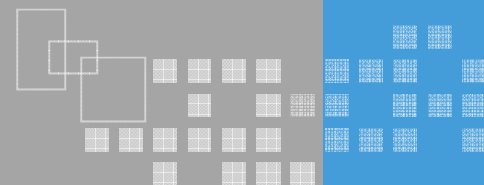
- 业务连续性计划（组织共同承担，应对DoS攻击）
- 协调机制（运营商、公安部门、专家团队）

❖ 技术防御

- 安全设备（防火墙、抗DoS设备）
- 增强网络带宽
- 自身强壮性（风险评估、补丁、安全加固、资源控制）

❖ 监测防御

- 应急响应（构建监测体系）



❖ 边界安全防护

- 了解防火墙、安全隔离与信息交换系统的实现技术、部署方式、作用及局限性；
- 了解IPS、UTM、防病毒网关等边界安全防护技术的概念。

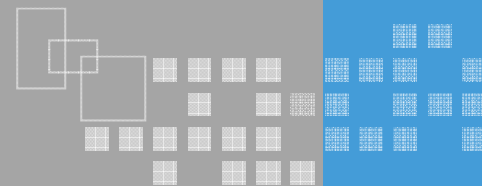
❖ 检测与审计

- 了解入侵系统、安全审计的作用、分类、实现技术、部署方式及应用上的局限性；

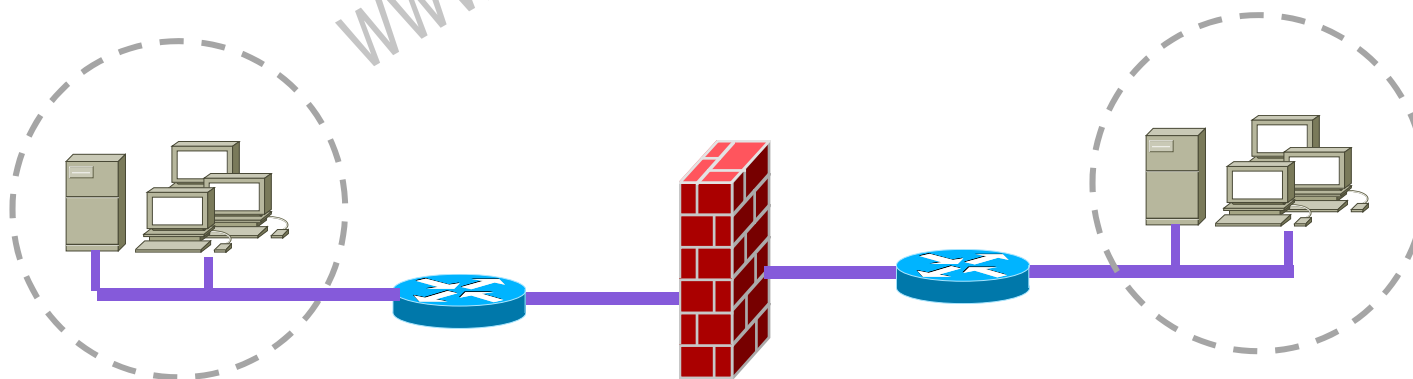
❖ 接入管理

- 了解VPN的作用、关键技术及应用领域；
- 了解网络准入控制的作用。

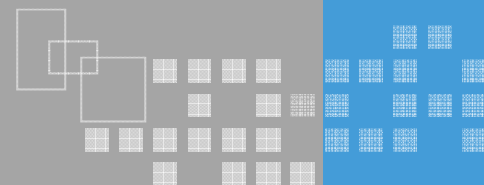
边界安全防护-防火墙



- ❖ 控制：在网络连接点上建立一个安全控制点，对进出数据进行限制
- ❖ 隔离：将需要保护的网络与不可信任网络进行隔离，隐藏信息并进行安全防护
- ❖ 记录：对进出数据进行检查，记录相关信息



防火墙的主要技术



❖ 静态包过滤

- 依据数据包的基本标记来控制数据包
- 技术逻辑简单、易于实现，处理速度快
- 无法实现对应用层信息过滤处理，配置较复杂

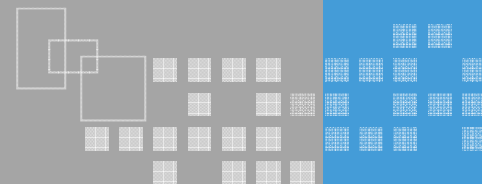
❖ 应用代理

- 连接都要通过防火墙进行转发
- 提供NAT，隐藏内部网络地址

❖ 状态检测

- 创建状态表用于维护连接，安全性高
- 安全性高但对性能要求也高
- 适应性好，对用户、应用程序透明

防火墙的部署



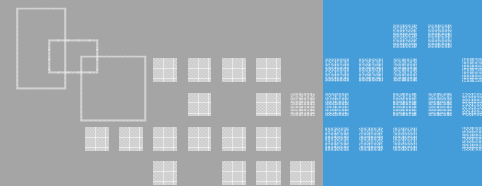
❖ 防火墙的部署位置

- 可信网络与不可信网络之间
- 不同安全级别网络之间
- 两个需要隔离的区域之间

❖ 防火墙的部署方式

- 单防火墙（无DMZ）部署方式
- 单防火墙（DMZ）部署方式
- 双防火墙部署方式

边界安全防护-网闸等

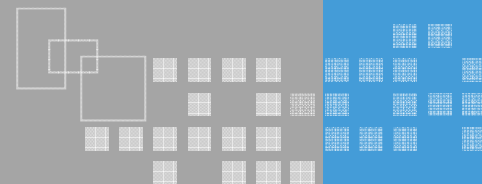


❖ 物理隔离与交换系统（网闸）

- 外部处理单元、内部处理单元、中间处理单元
- 断开内外网之间的会话（物理隔离、协议隔离）
- 同时集合了其他安全防护技术

❖ 其他网络安全防护技术

- IPS
- 防病毒网关
- UTM
-



❖ 入侵检测系统的作用

- 主动防御，防火墙的重要补充
- 构建网络安全防御体系重要环节

❖ 入侵检测系统功能

- 发现并报告系统中未授权或违反安全策略行为
- 为网络安全策略的制定提供指导

入侵检测系统

❖ 分类

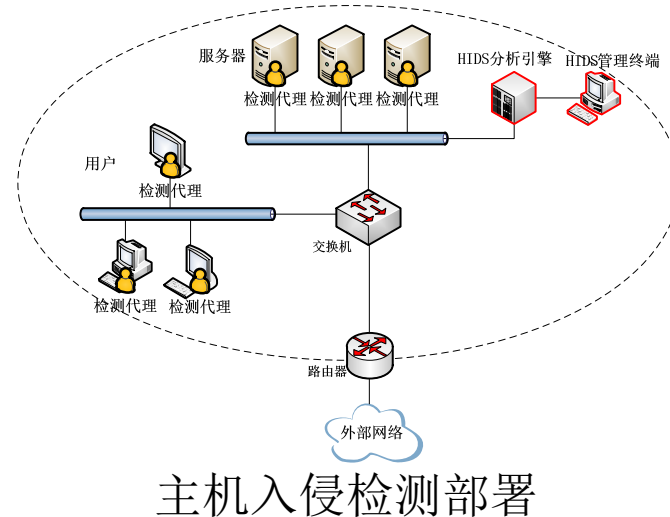
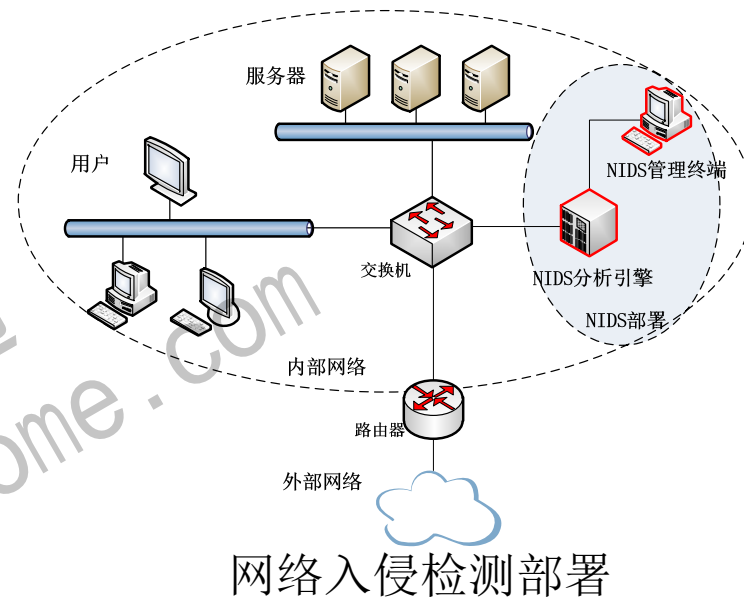
- 网络入侵检测
- 主机入侵检测

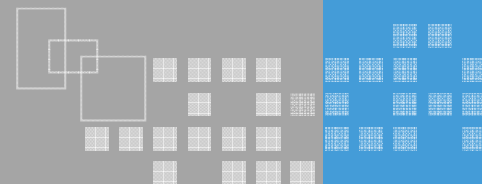
❖ 检测技术

- 误用检测
- 异常检测

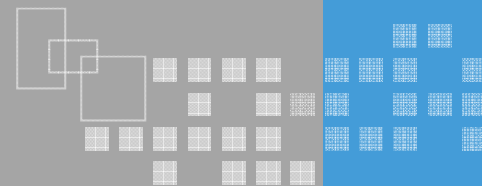
❖ 部署

❖ 局限性





- ❖ 虚拟专用网络 (Virtual Private Network, VPN)
 - 利用隧道技术，在公共网络中建立一个虚拟的、专用的安全网络通道
- ❖ VPN实现技术
 - 隧道技术
 - 二层隧道：PPTP、L2F、L2TP
 - IPSEC
 - SSL
 - 密码技术



❖ 物理和环境安全

- 环境安全、设施安全、传输安全

❖ OSI七层模型

❖ TCP/IP协议安全

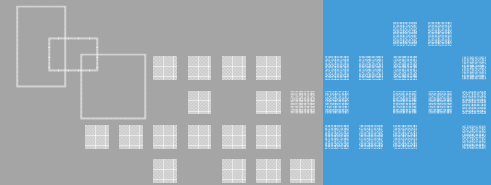
❖ 典型网络攻击与防范

- 电子欺骗（ARP欺骗、IP欺骗、DNS欺骗）
- 拒绝服务攻击（SYN Flood、UDP Flood、Teardrop）
与分布式拒绝服务攻击

❖ 网络安全设备

- 防火墙、网闸、IDS、VPN等

邀请您参与讲师考评





谢谢，请提问题！

东方瑞通
www.easthome.com