第三讲 网络安全与物理安全

白杨 alicepub@163.com

网络安全的定义

百度百科：

网络安全（Cyber Security）是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

网络安全在不同的应用环境下有不同的解释。针对网络中的一个运行系统而言，网络安全就是指信息处理和传输的安全。它包括硬件系统的安全、可靠运行，操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。**狭义的网络安全，侧重于网络传输的安全**。

第三讲 网络安全与物理安全

① 因特网的起源与发展

② 因特网的体系与架构

③ 常见的网络安全问题与防范

因特网的起源与发展

“因特网和由它使能的所有东西是一个巨大的新前沿，充满了令人惊奇的挑战，为众多创新提供了广阔空间。不要受今天技术的束缚，开动大脑，想象能够做些什么，并去实现它。”
《计算机网络:自顶向下方法(原书第6版)》

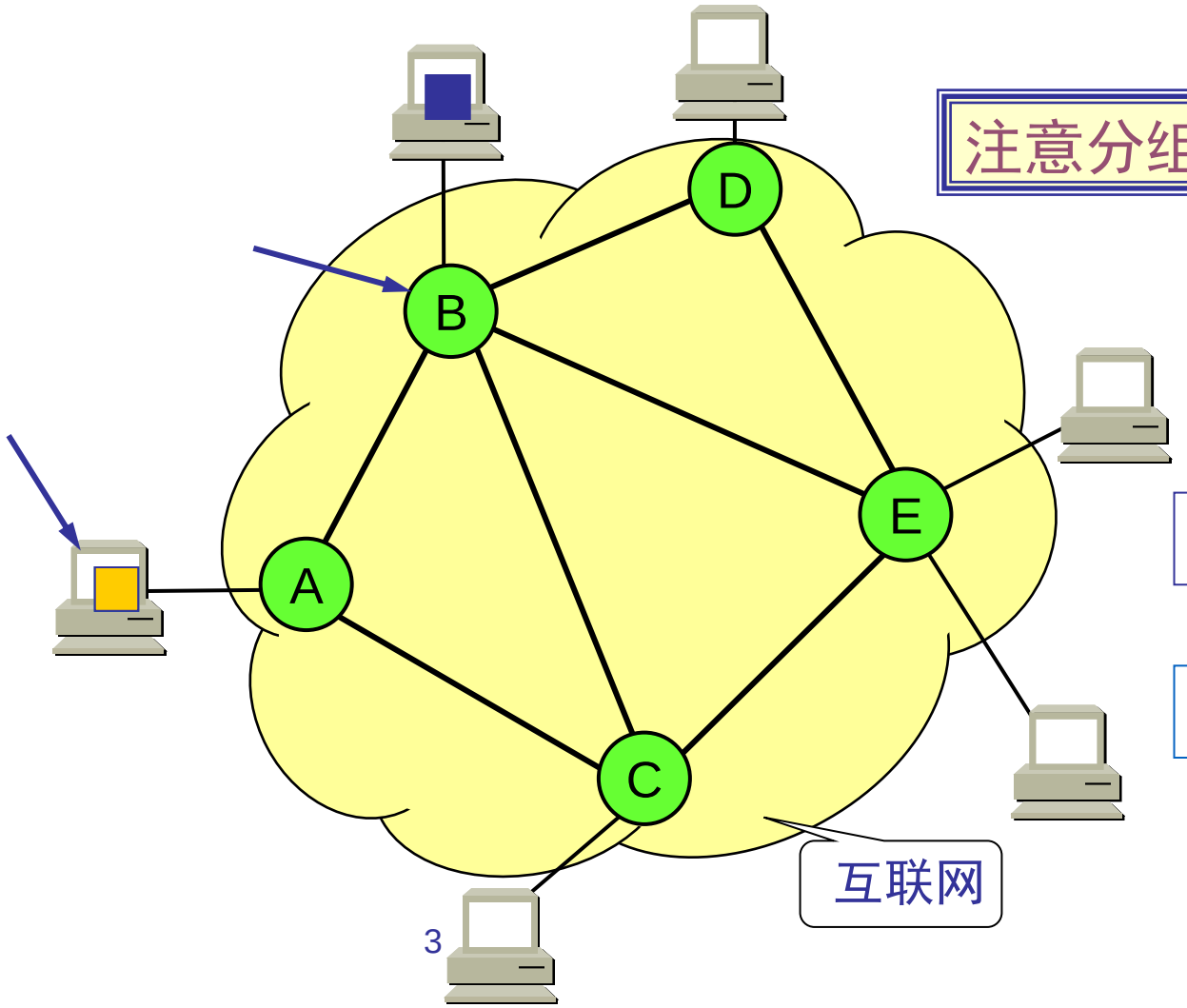
Leonard Kleinrock，加州大学洛杉矶分校（UCLA）计算机科学教授，1961年，他创造的分组交换（packet switching）原理成为因特网的支撑技术。1969年，他在UCLA的计算机成为因特网的第一个节点。

1959年，Kleinrock选择了当时未知的数据网作为研究方向。1962年完成了“大通信网的信息流”论文，其工作1964年发表在MIT出版的“通信网”一书，奠定了分组交换的基础。1963年他进入UCLA大学工作。1969年9月2日，Leonard Kleinrock和他领导的研究小组成功地把一台电脑和一台电冰箱大小的转换装置连接在一起，并在接下来的一个月中使两台电脑通过这台转换装置进行了对话，从而为日后互联网的迅猛发展提供了必要条件。

因特网的起源与发展

- 计算机网络的产生：20 世纪 60 年代美苏冷战时期的产物。
- 60 年代初，美国国防部领导的远景研究规划局ARPA (Advanced Research Project Agency) 提出要研制一种生存性(survivability)很强的网络。
- 传统的电路交换(circuit switching)的电信网有一个缺点：正在通信的电路中有一个交换机或有一条链路被炸毁，则整个通信电路就要中断。
- 如要改用其他迂回电路，必须重新拨号建立连接。这将要延误一些时间。（抗美援朝中著名的上甘岭战役，战士们为接通电话线路，付出了生命的代价。）

因特网的起源与发展-分组交换技术



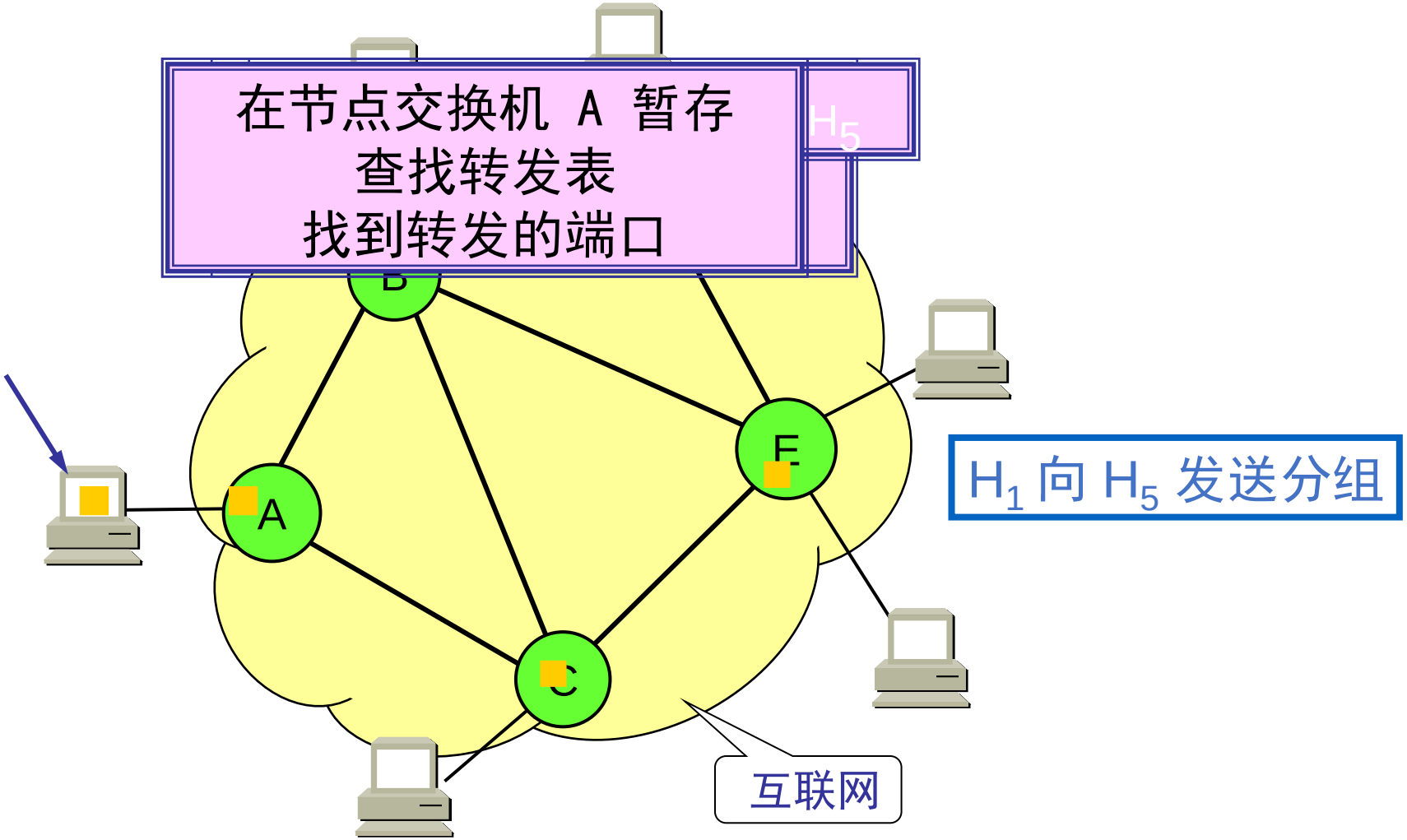
注意分组路径的变化！

H_2 向 H6 发送分组

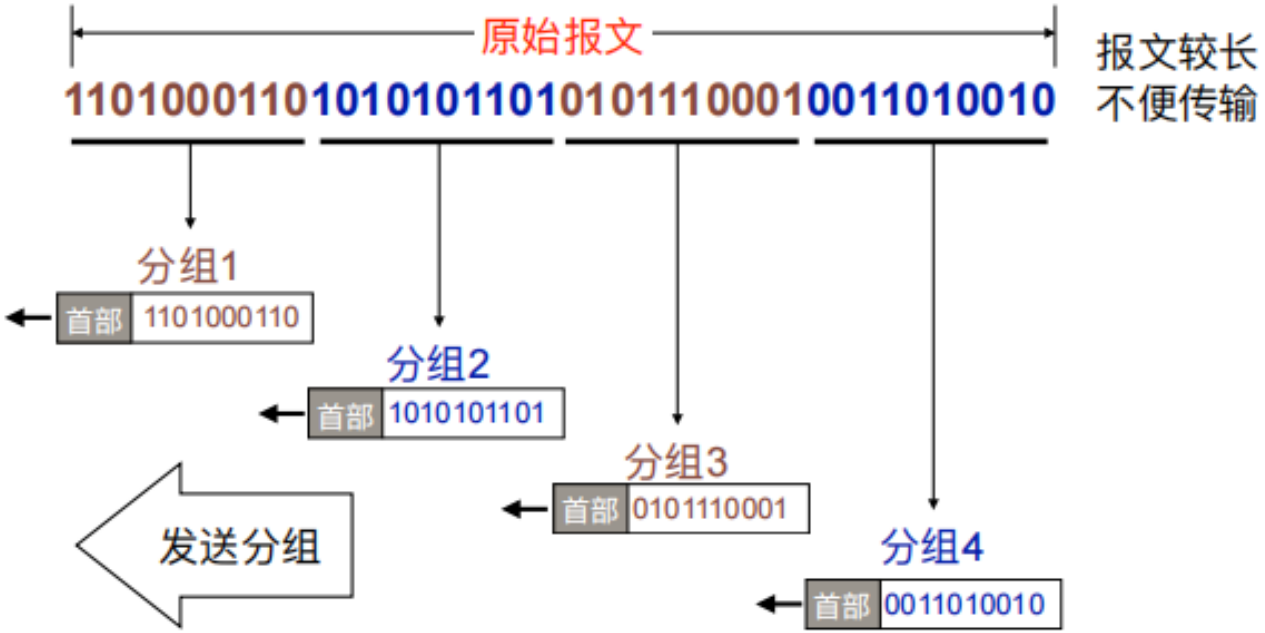
H_1 向 H_5 发送分组

因特网的起源与发展-分组交换技术

- 分组交换的特征是基于标记（lable-based），分组交换在传送连接之前不需要先建立一条通信线路。
- 这种不先建立连接的连网方式，称为无连接（connectionless）
- 分组交换机网由若干个节点交换机（node switch）和连接这些swtich的链路组成。



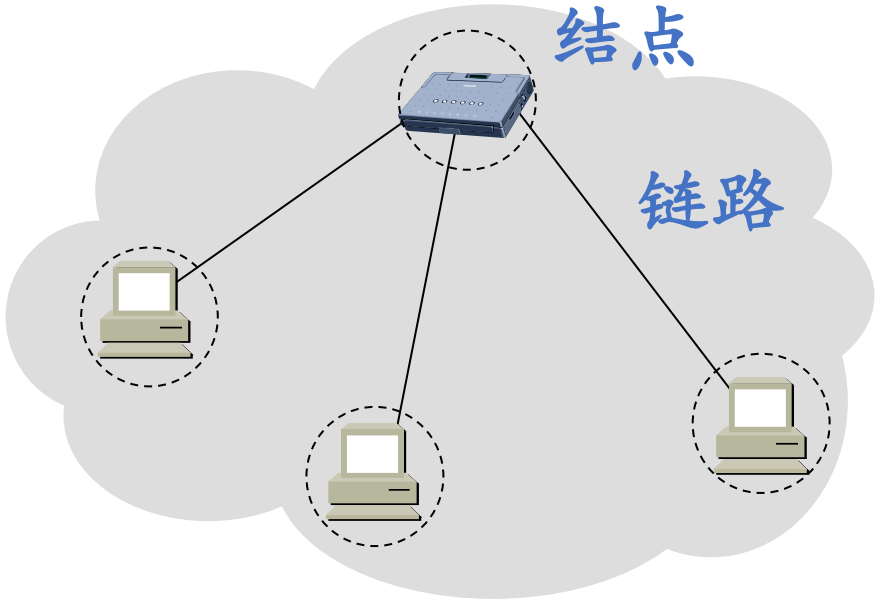
因特网的起源与发展-分组交换技术

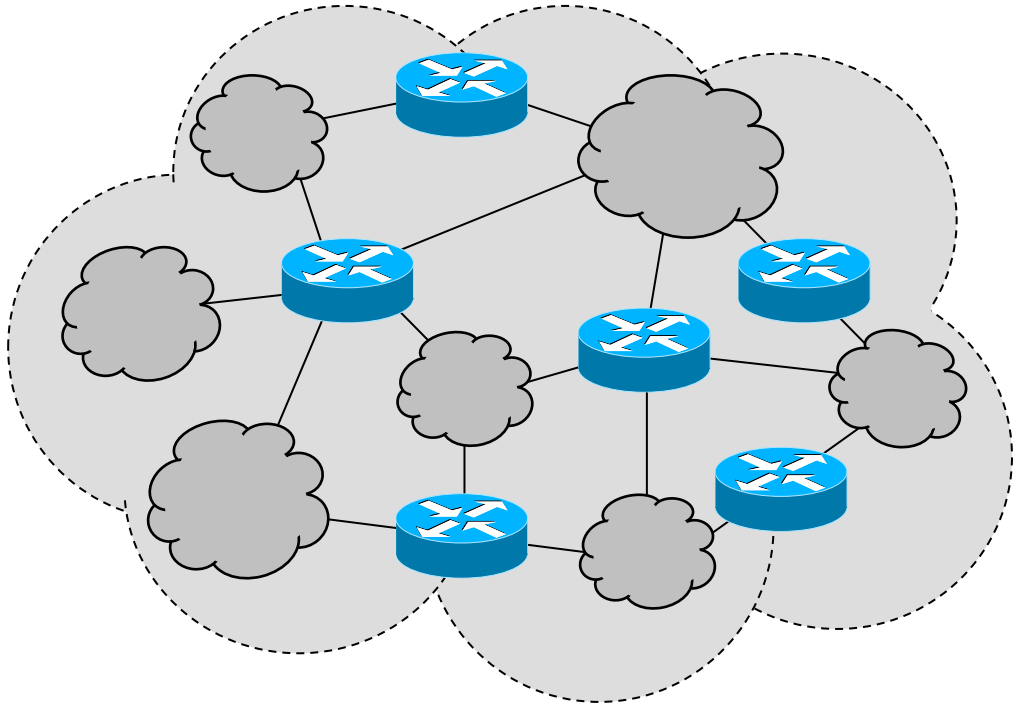


- 每一个分组的首部都含有地址（目的地址和源地址）等控制信息。
- 分组交换网中的结点交换机根据收到的分组首部中的地址信息，把分组转发到下一个结点交换机
- 每个分组在互联网中独立地选择传输路径；
- 用这样的存储转发方式，最后分组就能到达最终目的地。

因特网的相关基本概念

- 网络把许多计算机连接在一起。
- 因特网则把许多网络连接在一起，是“网络的网络”(network of networks)





- 网络(network)由若干结点(node)和连接这些结点的链路(link)组成。
- 连接在因特网上的计算机都称为主机(host)。

因特网的组成

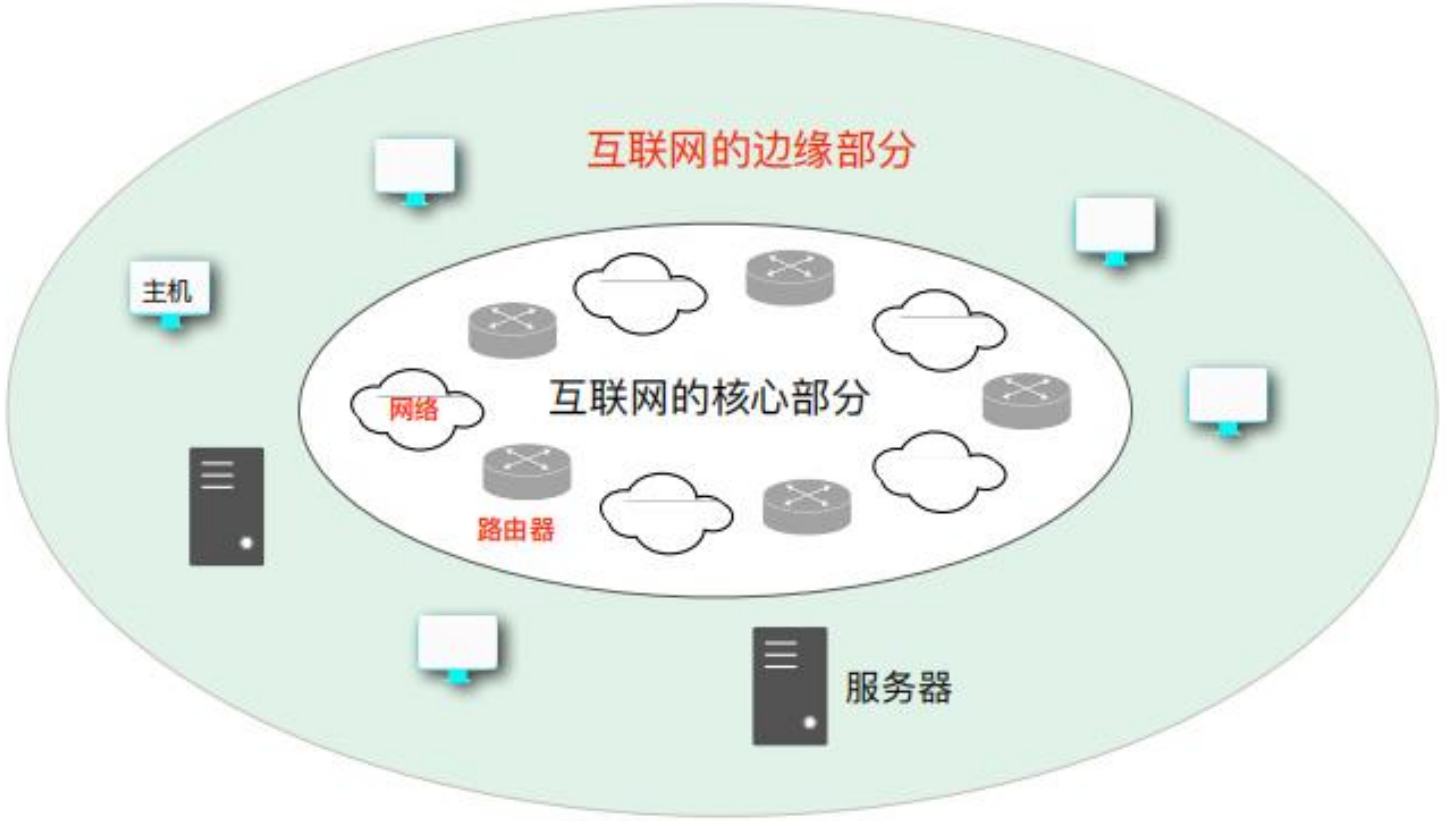
1. 互联网边缘部分：

连接在互联网上的所有的主机，又称为端系统（end system）：

- 小的端系统：个人电脑、智能手机、网络摄像头等。
- 大的端系统：大型计算机：
- 个人、单位或某个ISP

2. 互联网的核心部分

各类网络、路由器等设备

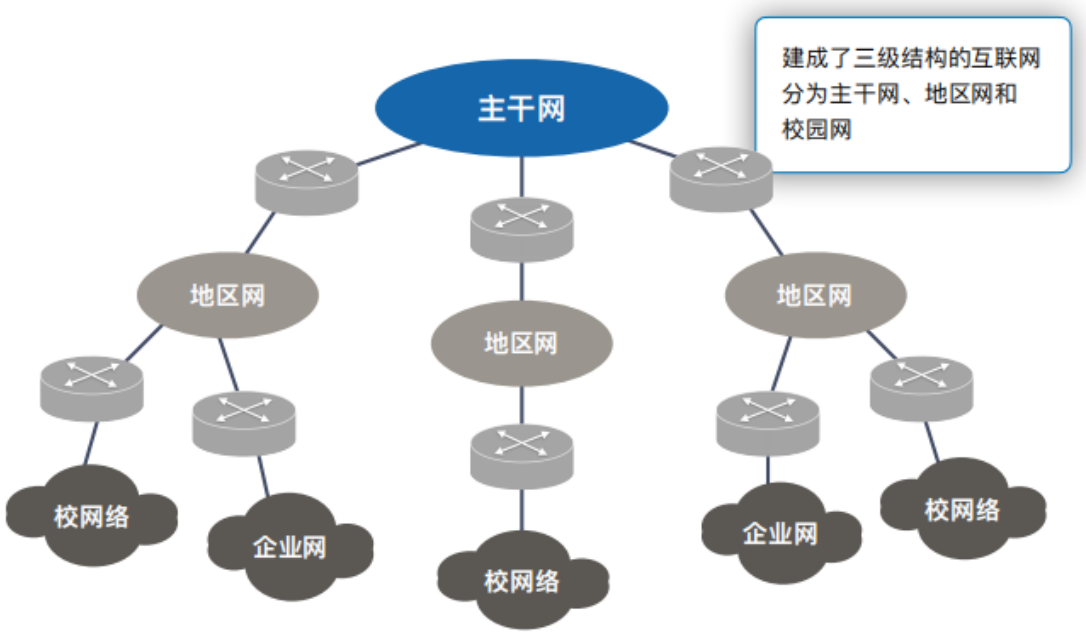


因特网的相关基本概念

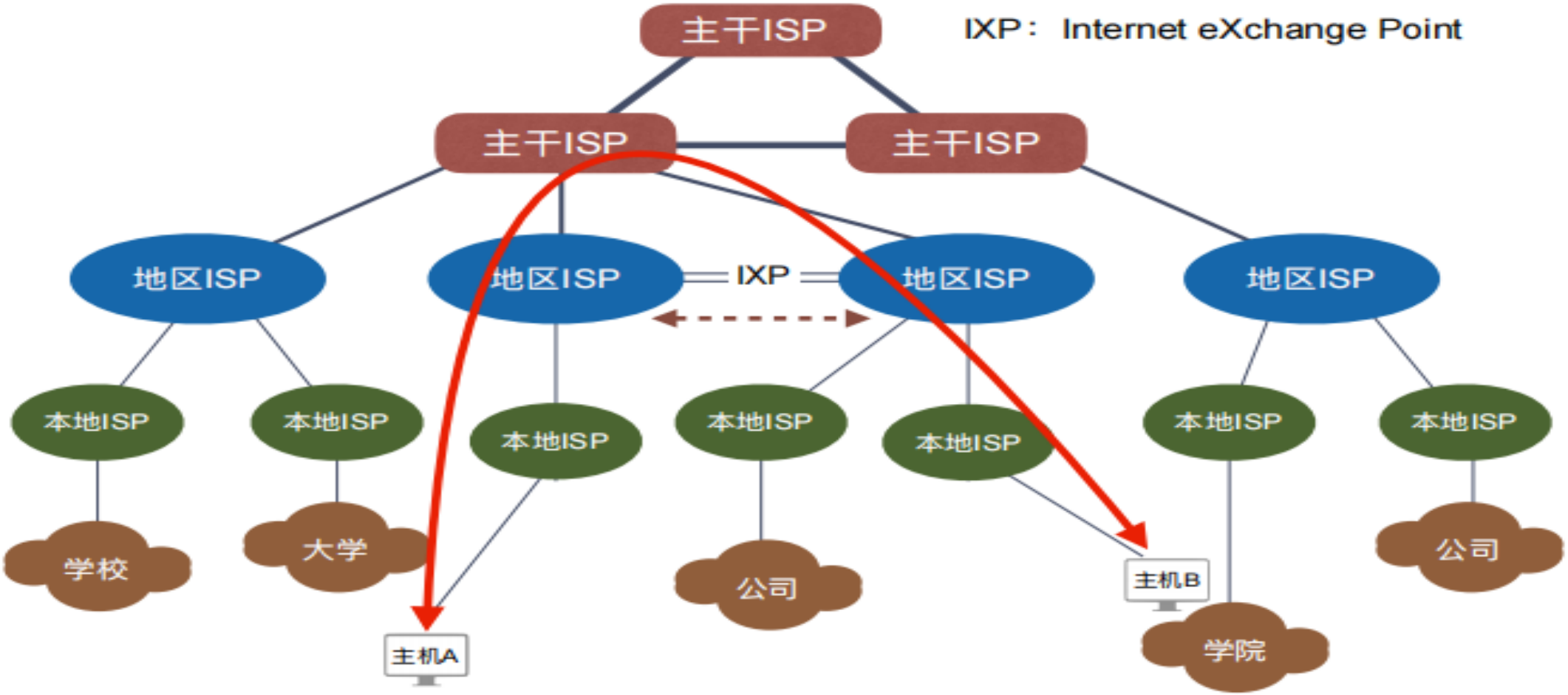
- 起源于美国的因特网现已发展成为世界上最大的国际性计算机互联网。
- internet 和 Internet 的区别（以 i 开始的 internet（互联网或互连网）是一个通用名词，它泛指由多个计算机网络互连而成的网络。以I开始的 Internet（因特网）则是一个专用名词，它指当前全球最大的、开放的、由众多网络相互连接而成的特定计算机网络）

因特网的起源与发展

- 第一阶段是从单个网络 ARPANET 向互联网发展的过程。 1983 年 TCP/IP 协议成为 ARPANET 上的标准协议，人们把 1983 年作为因特网的诞生时间。
- 第二阶段的特点是建成了三级结构的因特网。 三级计算机网络，分为主干网、地区网和校园网（或企业网）。



因特网的起源与发展

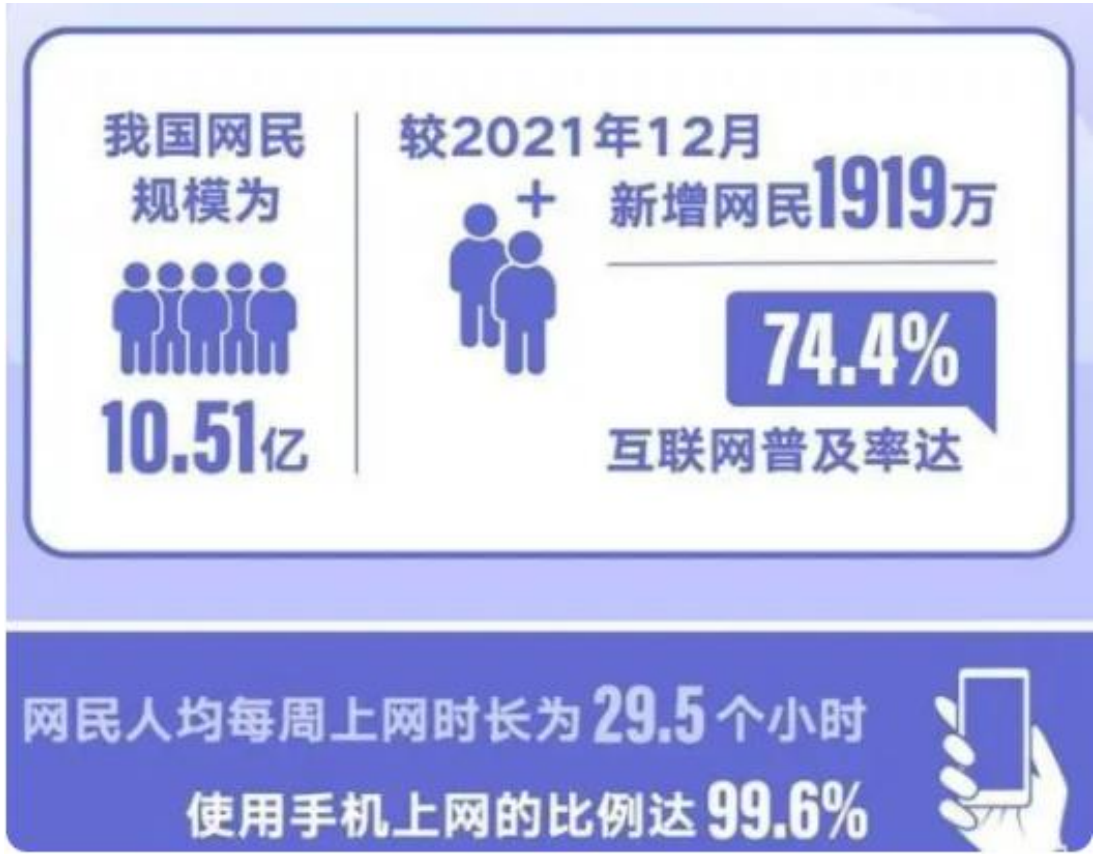

主干ISP
IXP： Internet eXchange Point
主干ISP
主干ISP
地区ISP
地区ISP
IXP
地区ISP
地区ISP
本地ISP
本地ISP
本地ISP
本地ISP
本地ISP
本地ISP
本地ISP
学校
大学
公司
公司
主机A
主机B
学院
主机A → 本地ISP → 地区ISP → 主干ISP → 地区ISP → 本地ISP → 主机B

因特网在我国的发展情况

1. 1980年，铁道部开始进行计算机联网实验。
2. 1989年11月，我国第一个公用分组交换网CNPAC建成运行。
3. 1994年4月20日，我国用 64 kbit/s 专线正式连入互联网，我国被国际上正式承认为接入互联网的国家。
4. 1994年5月，中国科学院高能物理研究所设立了我国的第一个万维网服务器。
5. 1994年9月，中国公用计算机互联网CHINANET正式启动。
6. 到目前为止，我国陆续建造了基于互联网技术的并能够和互联网互联的多个全国范围的公用计算机网络，其中最大规模的就是下面这五个：
   - 中国电信互联网 CHINANET（也就是原来的中国公用计算机互联网）
   - 中国联通互联网 UNINET
   - 中国移动互联网 CMNET
   - 中国教育和科研计算机网 CERNET
   - 中国科学技术网 CSTNET

目前我国现状


我国网民规模达10.51亿
中国互联网络信息中心（CNNIC）
8月31日在北京发布
第50次《中国互联网络发展状况统计报告》
报告显示
截至2022年6月


我国网民规模为
10.51亿
较2021年12月
新增网民1919万
74.4%
互联网普及率达
网民人均每周上网时长为29.5个小时
使用手机上网的比例达99.6%

第三讲 网络安全与物理安全

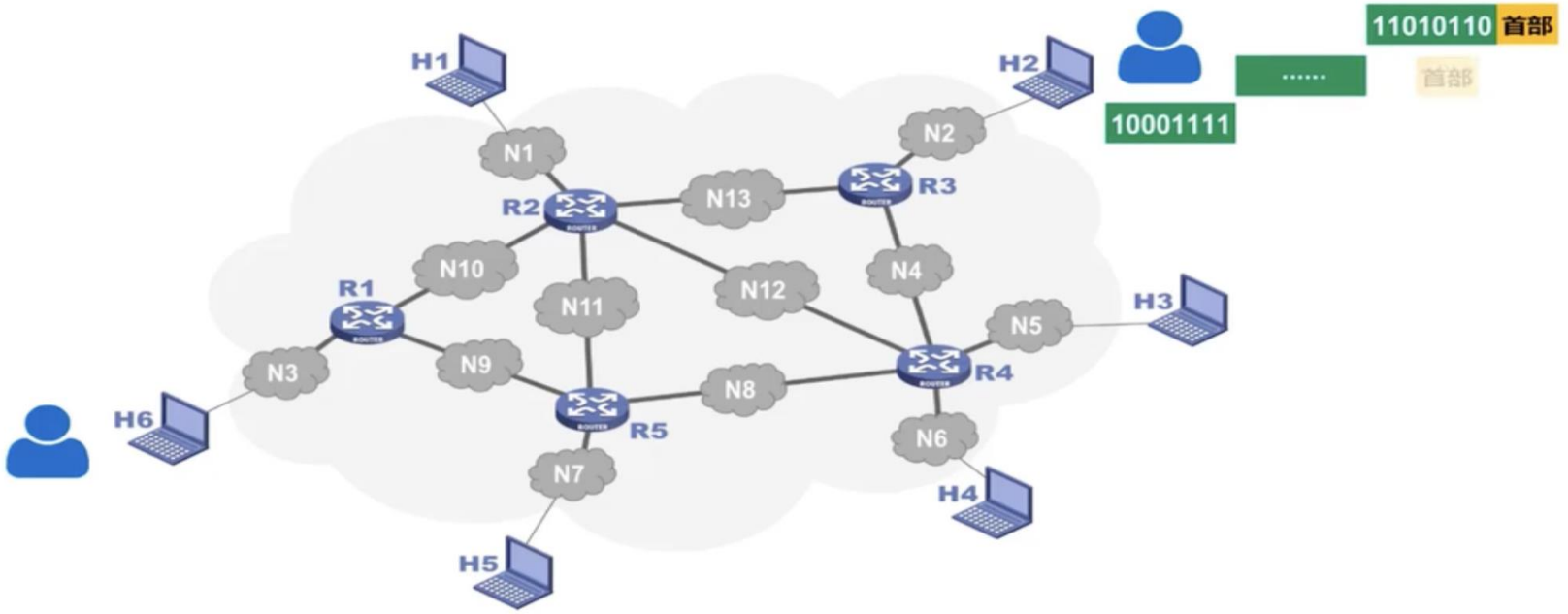
① 因特网的起源与发展

② 因特网的体系与架构

③ 常见的网络安全问题与防范

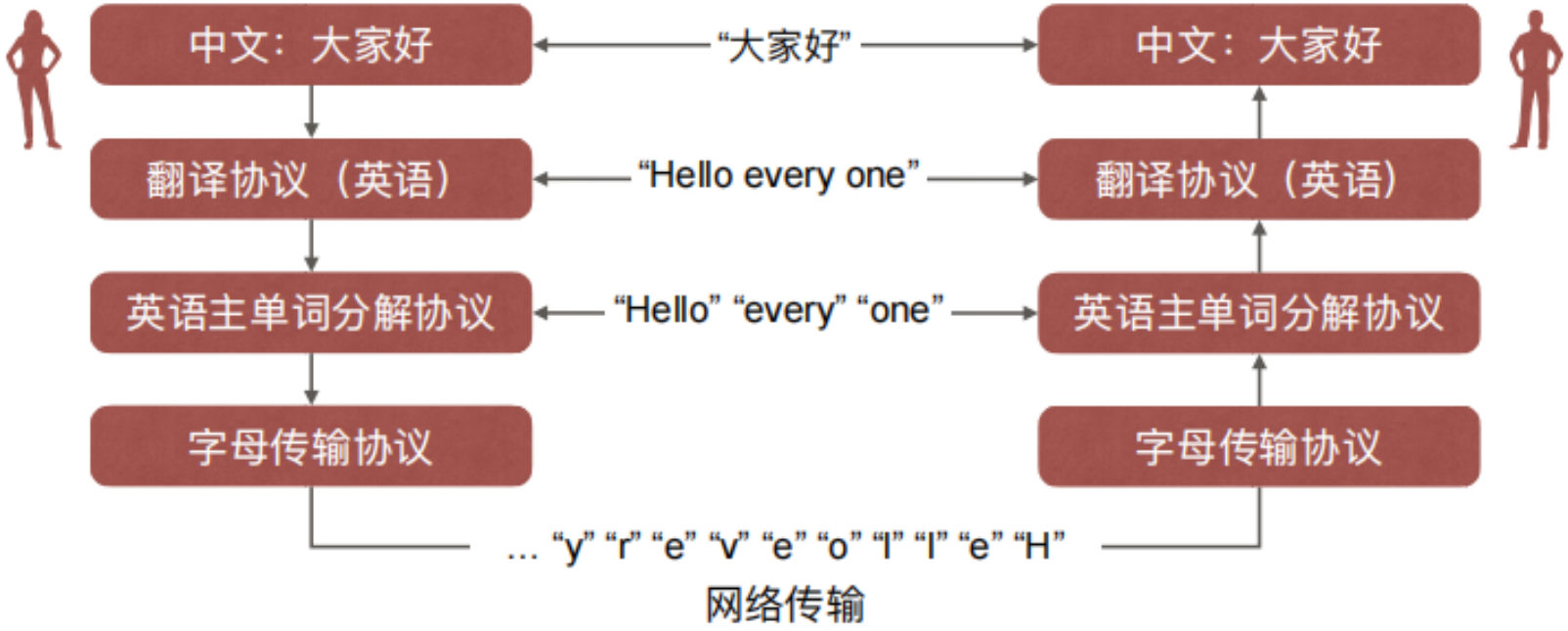
因特网的体系架构

当您从即时通信工具的信息发送栏键入一条消息并发送，最终几乎同时显示在了好朋友的接收窗口中，这个看上去再也简单不过的网络应用，或许您认为完成这个功能几乎不需要花费什么力气。但是为了完成这个相互通信的功能，源/目地计算机以及网络中的通信设备、系统必须高度地协调工作才行，而这种协调是相当复杂的。



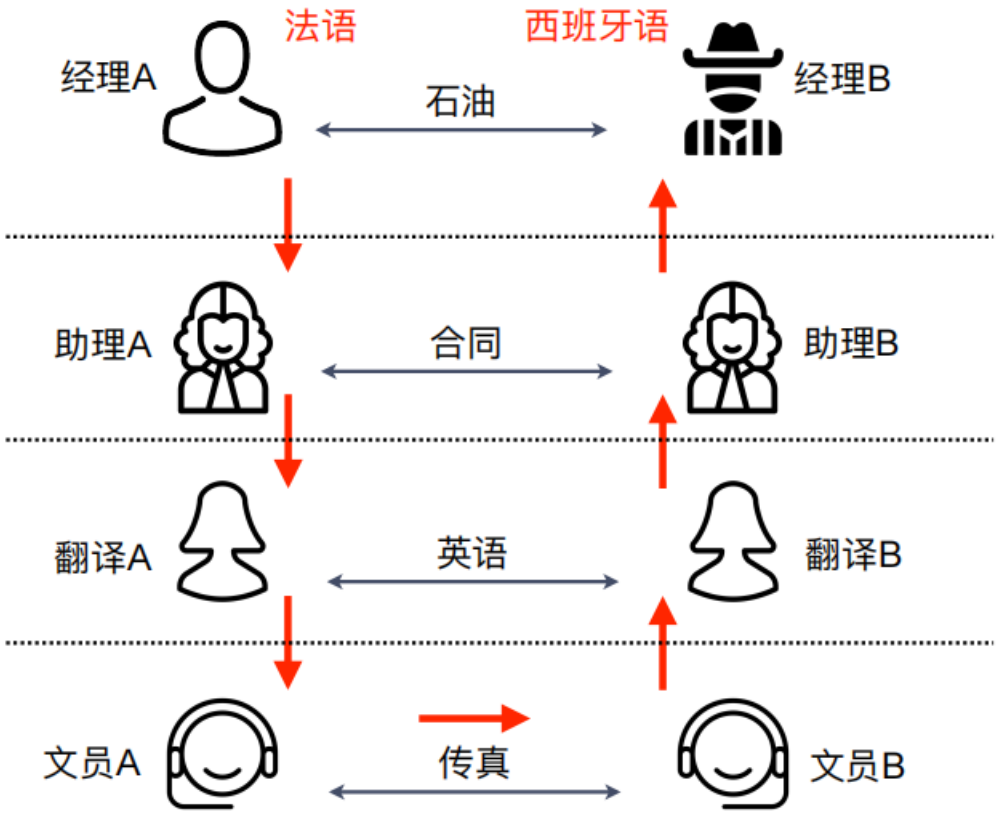
因特网的体系架构

首先信息需要知道他要去的目的地，需要经过计算机的组装、分组，编码变成线缆上适合传输的电信号，穿越不同的省市、国家，甚至大洋深处，经过不同的通信设备的处理，存储/转发，并需要解决传输过程可能会出现的差错问题，最终才能达到目地计算机上，还原并显示出来。



因特网的体系架构

“分层”可将庞大而复杂的问题，转化为若干较小的局部问题，而这些较小的局部问题就比较易于研究和处理。



按功能进行抽象分层：

- 定义层间接口和提供什么服务，层间如何调用服务
- 对等层间的必须遵循的规则（协议）

各层之间是相对独立的；

- 灵活性好；
- 结构上可分割开。
- 易于实现和维护；
- 能促进标准化工作。

因特网的体系架构

- 计算机网络的**体系结构(architecture)**是计算机网络的**各层及其协议**的集合，体系结构就是这个计算机网络及其部件所应完成的功能的精确定义。
- 实现(implementation)是遵循这种体系结构的前提下用何种硬件或软件完成这些功能的问题。
- 体系结构是抽象的，而实现则是具体的，是真正在运行的计算机硬件和软件。
- **网络协议（network protocol），简称为协议**，是为进行网络中的数据交换而建立的**规则、标准或约定**。这些规则明确规定了所交换的数据的格式以及有关的同步问题（同步含有时序的意思）
  ① 传统教学遵循的教学秩序；
  ② 人类社会生活遵循的法律法规；
  ③ 国际关系的基本准则；
  ④ 人与人之间交流的基本礼仪等

协议的三个要素

- 语法：数据与控制信息的结构或格式，（解决交换信息的格式问题）
- 语义：需要发出何种控制信息，完成何种动作以及做出何种响应。（解决做什么的问题）
- 同步：事件实现顺序的详细说明。（什么时间，什么条件下做某一特定操作的规定，解决先做什么后做什么的问题）

例如课堂上课：

- 语法：中文授课，教师与学生按中文语法结构交换信息
- 语义：交换的信息中各字段的含义
- 同步：教师讲，学生听；教师问，学生答；学生问教师答

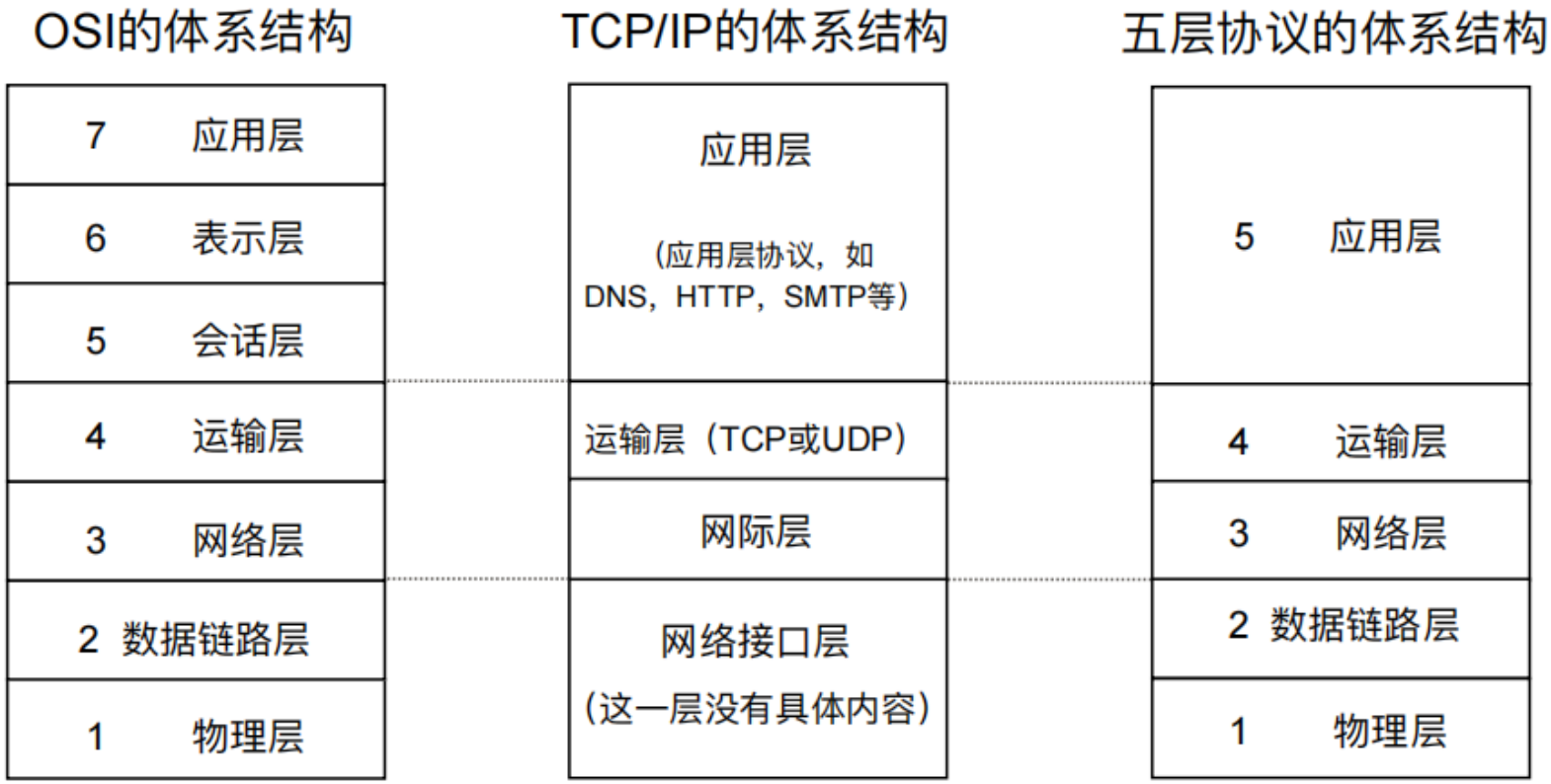
协议的两种形式：

① 一种是使用便于阅读和理解的文字描述。

② 另一种是让计算机能够理解的程序代码。

这两种不同形式的协议都必须能够对网络上信息交换过程做出精确的解释。

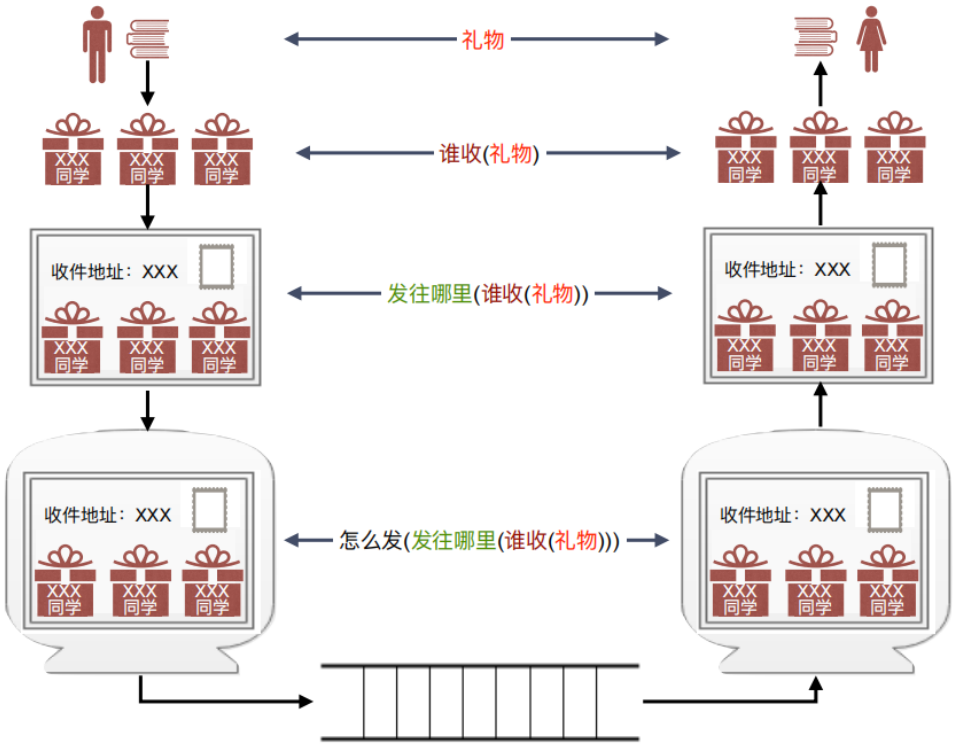
常见的三个体系架构

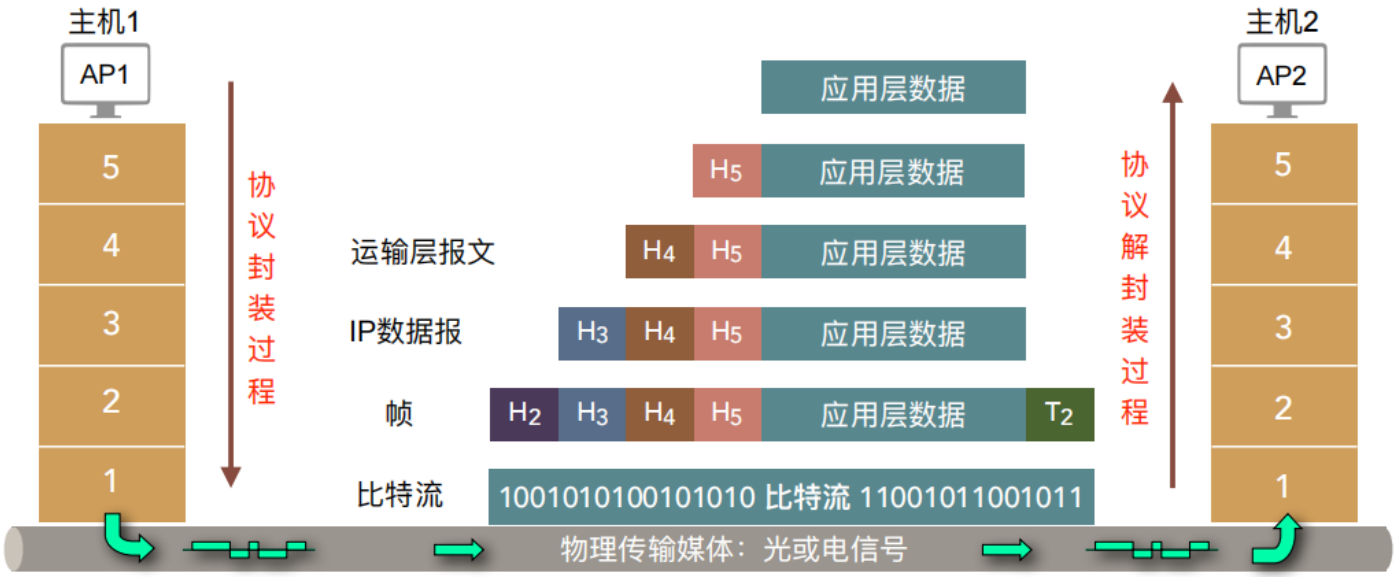


计算机网络三类体系结构

OSI七层协议；TCP/IP四层协议；授课的五层协议

协议与封装

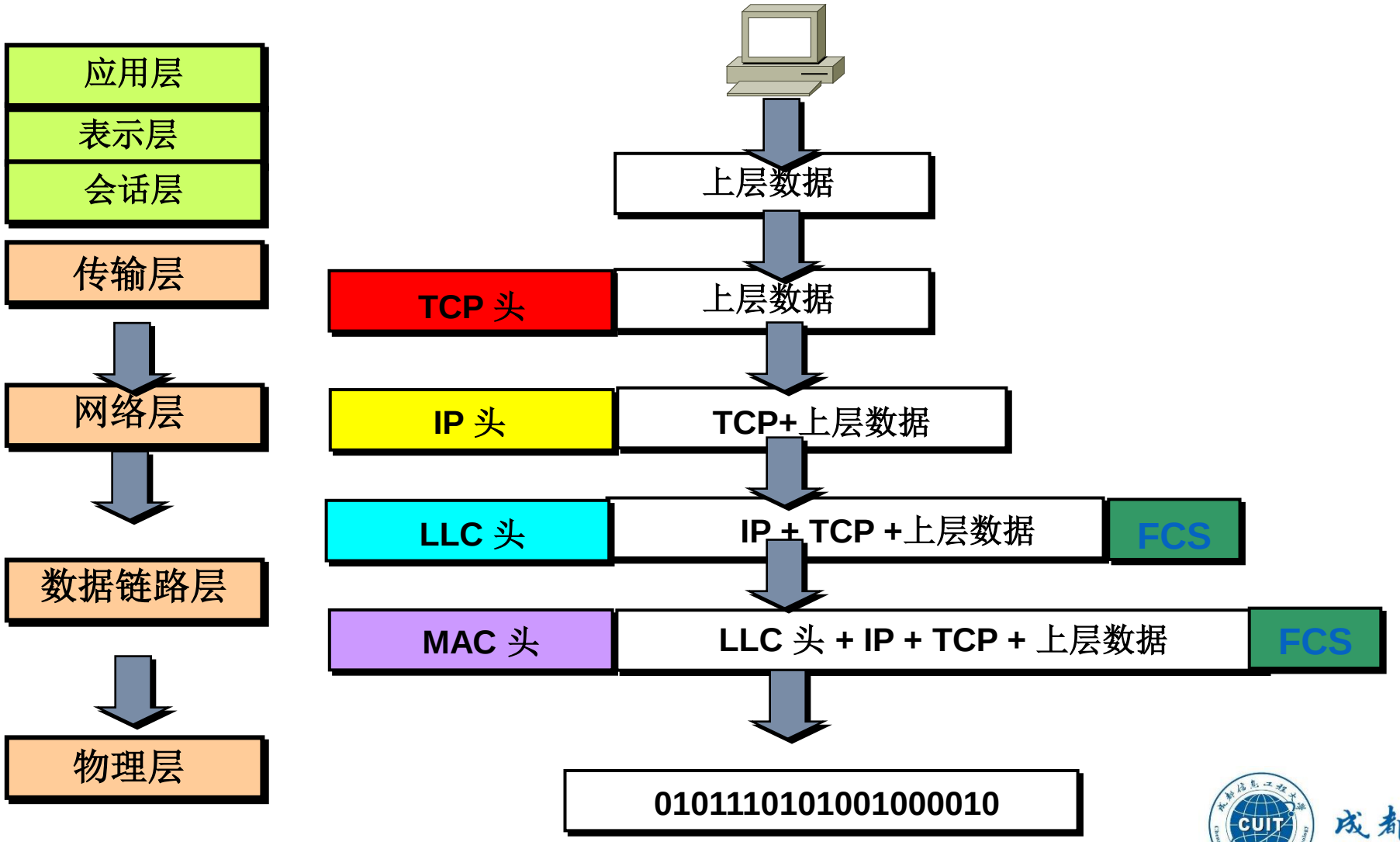




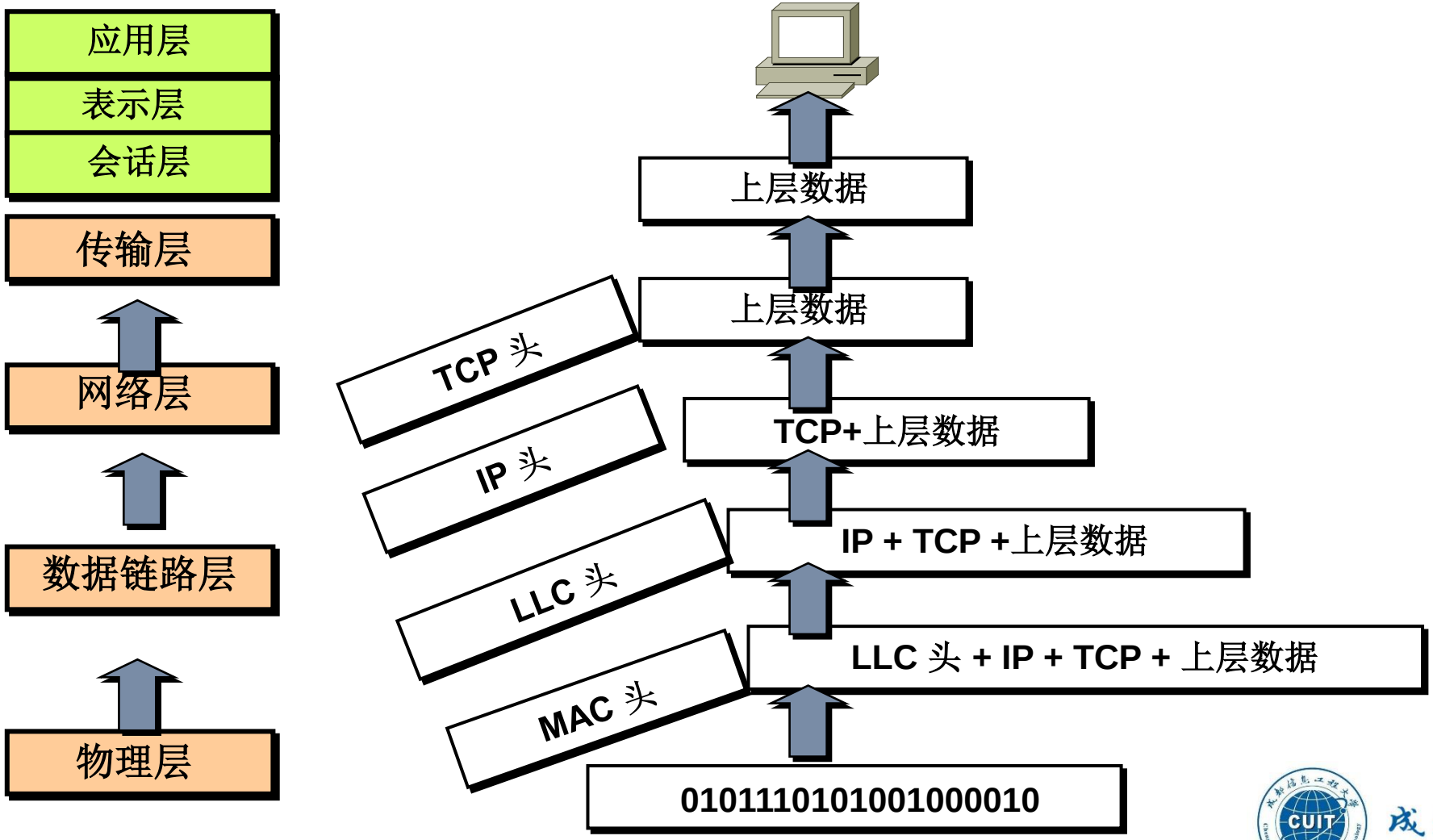
PDU（Protocol Data Unit）：协议数据单元。

OSI参考模型把对等层次之间传送的数据单位称为该层的协议数据单元PDU

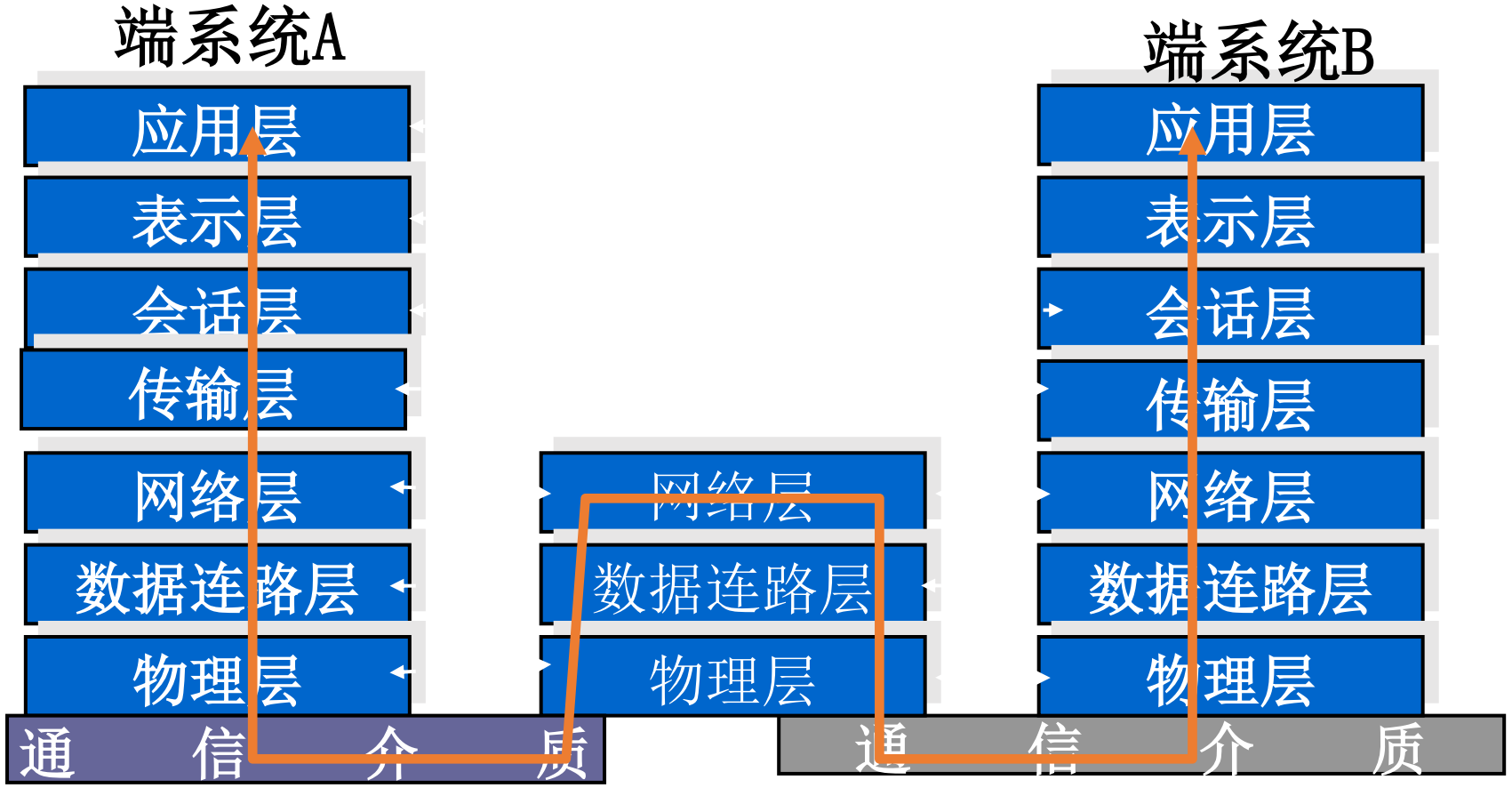
协议与封装-OSI


应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
上层数据
TCP 头
上层数据
IP 头
TCP+上层数据
LLC 头
IP + TCP +上层数据
FCS
MAC 头
LLC 头 + IP + TCP + 上层数据
FCS
0101110101001000010

协议与封装-OSI


应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
上层数据
上层数据
TCP 头
TCP+上层数据
IP 头
IP + TCP +上层数据
LLC 头
LLC 头 + IP + TCP + 上层数据
MAC 头
0101110101001000010

协议与封装-OSI


端系统A
应用层
表示层
会话层
传输层
网络层
数据连路层
物理层
通 信 介 质
网络层
数据连路层
物理层
端系统B
应用层
表示层
会话层
传输层
网络层
数据连路层
物理层
通 信 介 质

第三讲 网络安全与物理安全

① 因特网的起源与发展

② 因特网的体系与架构

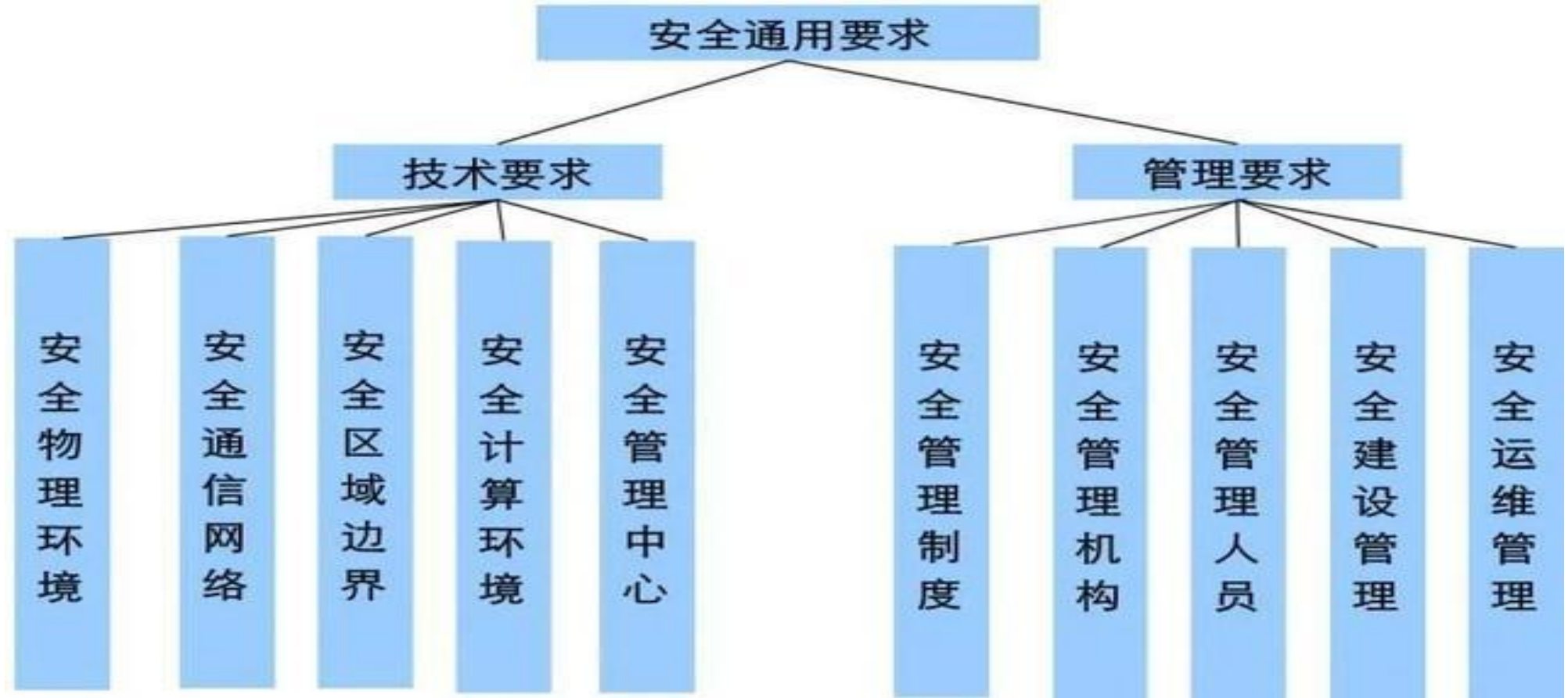
③ 常见的网络安全问题与防范

网络本身存在的安全问题

- 计算机及网络设备设施遭受水灾、火灾、雷击等环境事故，或电力故障、人为破坏、操作失误等外界引起的受损或破坏等，这是网络安全的基本前提。（物理安全）
- 网络组网时的设计是否科学合理？是否配置了相应的安全设备？是否配置了必要的访问控制策略？对外服务与对内服务的区域划分及隔离？等等。（网络设计、组网与配置安全）
- 协议自身的脆弱性问题，因特网基于的是tcp/ip的协议簇，不幸的是该协议簇部分协议对于网络的安全性考虑得并不多（历史原因）。并且，由于tcp/ip协议是公布于众的，如果人们对tcp/ip很熟悉，就可以利用它的安全缺陷来实施网络攻击。（协议安全）
- 窃听与欺骗。利用网上免费提供的工具就很容易对网上的电子邮件、口令和传输的文件进行窃听。对信息发送者或接受者进行冒充。（数据窃听与身份冒充）
- 缺乏安全意识。人们普遍缺乏安全意识，使网络中的保护措施形同虚设。如人们为了避开防火墙代理服务器的额外认证，进行直接的ppp连接从而避开了防火墙的保护。（安全意识与管理）

网络本身存在的安全问题

根据《网络安全等级保护基本要求（GB/T22239-2019）》标准，定义网络安全的通用框架如下：



网络的物理安全

针对物理机房提出的安全控制要求。主要对象为物理环境、物理设备和物理设施等；涉及的安全控制点包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护。

① 2022年6月，负责马来西亚政府服务平台的数据中心大楼起火，使得数据中心电力供应被切断，导致服务器受损停机，SPay应用程序、本地政府门户网站等下线。

② 2022年4月，菲律宾马尼拉最高法院的一个数据中心起火，导致其最高法院的网站瘫痪。

③ 2021年12月，位于印度尼西亚雅加达南部库宁安的“Cyber1DataCenter"大楼起火，导致互联网服务和数据中心业务中断，两名技术人员在此次火灾中不幸遇难。

④ 2021年4月，美国主机托管公司Web NX位于犹他州的奥格登数据中心着火，导致超360万个网站出现故障，约1.5万名客户的资料受到影响，部分客户数据完全丢失且无法恢复。

⑤ 2020年8月，澳洲电信公司Telstra位于英国首都伦敦的托管数据中心UPS故障发生火灾， 并引起宕机。

⑥ 2018年11月，韩国三大电信运营商之一KT位于首尔市中心的大楼发生火灾。由于通信设备受损，此次事故导致韩国的警察、医院、金融等社会基础设施被迫停转。

⑦ 2017年4月，北京邮电大学网络数据中心突发火灾，起火原因系UPS蓄电池组故障。众多北京高校校园网纷纷崩溃。

网络的物理安全

电磁泄漏是指信息系统的电子设备工作时向外辐射电磁波的物理现象。

任何一种电子设备工作时都会产生电磁波，这种电磁波会不同程度地将正在处理的数字信息辐射到空中，或者通过电源线、信号线、地线等传导发射出去，只要在一定距离内使用相应设备就可以接收还原信息，致使数据信息被窃取或浏览。网络终端的电磁辐射尤其以计算机视频显示器最为严重。功率越大、频率越高的电子设备，电磁辐射越强，辐射距离也越远，电磁信号泄漏的风险越大，如计算机机房中配置的网络核心设备。

如果涉密网络中心机房、网络节点、中继站点、网络终端、线路等设备缺乏有效的电磁辐射屏蔽措施，或者不具备电磁辐射信号到达公共区域已衰减到无法被探测的安全距离，或者保密要害部门部位、涉密机房、涉密会议和活动场所周边直线距离20米内架设有移动通信基站、信号转发装置和无线局域网信号收发装置等，就面临着电磁泄漏泄密风险。

网络的物理安全-物理访问控制

物理访问控制（Physical Access Control）：是指在未授权人员和被保护的信息来源之间设置物理保护的控制。常见的门禁分级系统就是控制未授权人员访问不同物理空间的权限的。

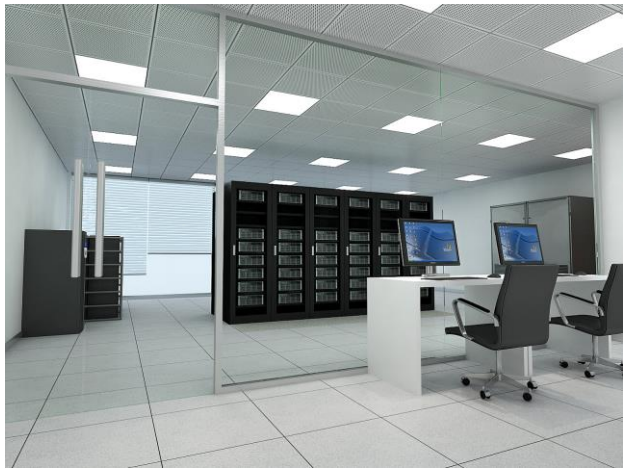
建议：

机房出入口：专人值守并配置电子门禁系统

来访人员控制：申请和审批流程、限制和监控其活动范围、专人陪同

机房划分区域管理：区域之间设置物理隔离、过渡区域、配置第二道门禁

安装摄像头：机房临近入口区域要安装摄像头保证全部范围覆盖



网络的物理安全-防盗窃和防破坏

计算机偷窃行为所造成的损失可能远远超过计算机本身的价值。

建议：

① 应将主要设备放置在机房内
② 应将设备或主要部件进行固定，并设置明显的不易除去的标记
③ 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中
④ 应对介质分类标识，存储在介质库或档案室中
⑤ 应利用光、电等技术设置机房防盗报警系统
⑥ 应对机房设置监控报警系统

网络的物理安全-防雷击和防静电

防雷击建议：

接闪：让闪电能量按照人们设计的通道泄放到大地中去

接地：让已经纳入防雷系统的闪电能量泄放入大地

分流：一切从室外来的导线与接地线之间并联一种适当的避雷器

屏蔽：用金属网/箔/壳/管等导体包裹，阻隔闪电的脉冲电磁场

防静电建议：

接地：静电屏蔽

增湿：静电中和

网络设计与配置安全

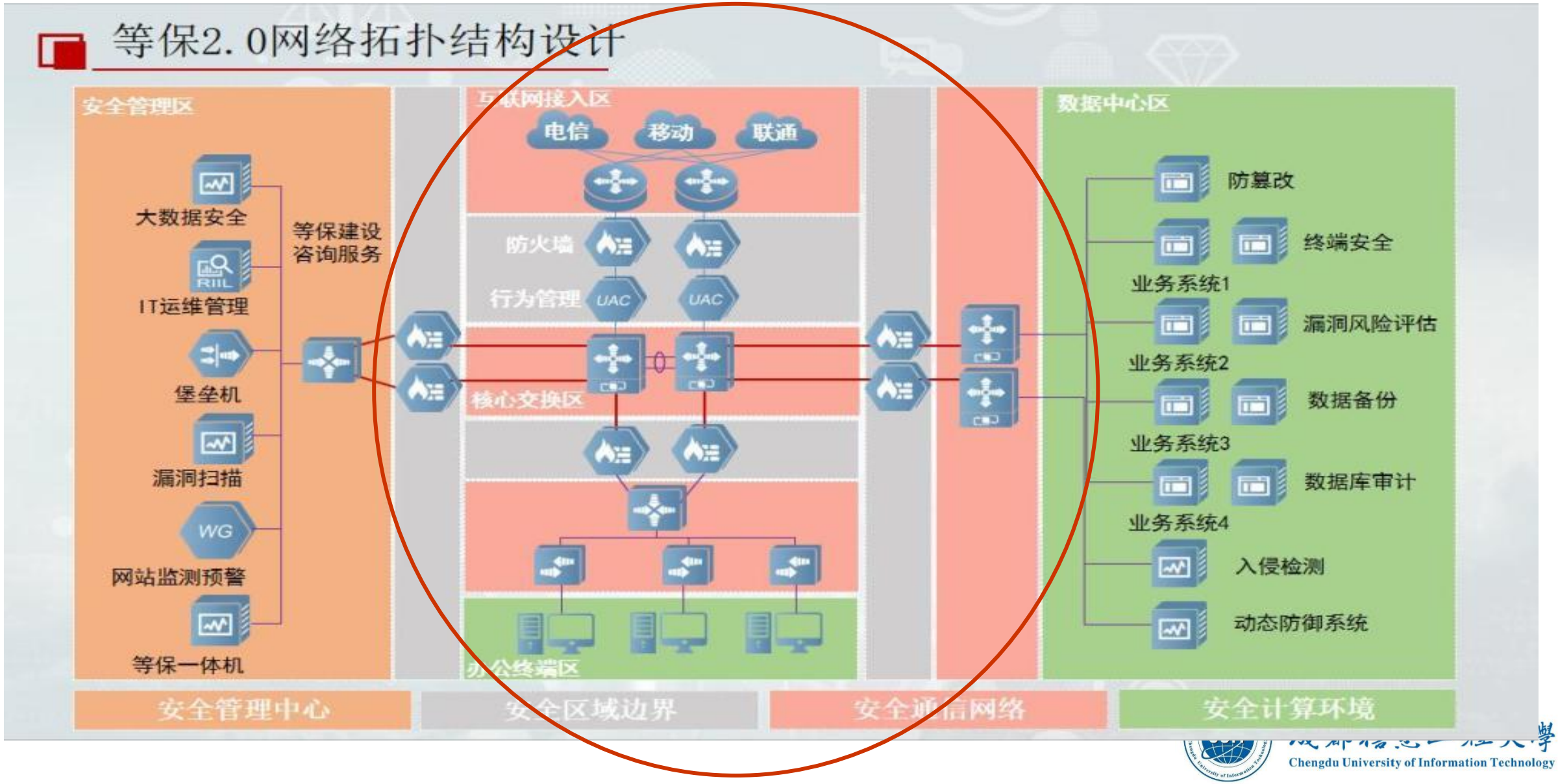
2019年5月，重庆永川某私立医院服务器突然陷入瘫痪，医院业务全面“停摆”。重庆永川公安组织网安刑侦、勘验、管理民警和技术支持专家赶赴现场对该案件进行调查核实。

经过民警和技术专家调查核实，该私立医院因未按照网络安全等级保护制度的要求履行安全保护义务。**医院未安装边界防护设备、未安装日志行为审计设备，未设置数据安全备份策略等其他网络安全技术措施**，使医院业务在互联网上长期处于“裸奔”状态。黑客通过互联网攻破医院系统后植入**勒索病毒**，导致医院业务全面“停摆”。

针对此案，永川公安按照公安部“一案双查”工作要求和《中华人民共和国网络安全法》第五十九条之规定，对医院处以罚款一万元，对直接负责的主管人员处以罚款五千元的行政处罚。

网络设计与配置安全

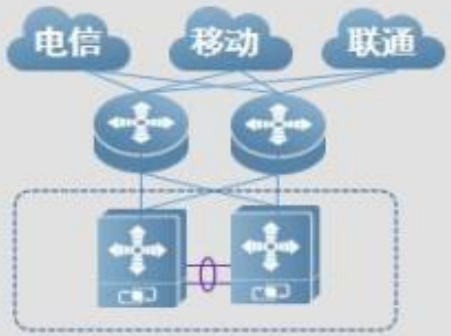
等保2.0网络拓扑结构设计



网络设计与配置安全

安全通信网络设计

等保要求	控制点	对应产品和方案
安全通信网络	网络架构	路由器、交换机、网络规划与配置优化、核心设备/主干链路冗余部署
	通信传输	VPN
	可信验证	可信计算机机制



主干网络链路及设备均采用冗余部署

基于业务管理和安全需求划分出明确边界的网络区域

采用VPN或HTTPS等加密手段保护业务通信

网络设计与配置安全

安全区域边界设计

等保要求	控制点	对应产品和方案
安全区域边界	边界防护	下一代防火墙、身份认证与准入系统
	访问控制	下一代防火墙、WEB应用防火墙、行为管理系统
	入侵防范	入侵检测与防御、未知威胁防御、日志管理系统
	恶意代码和垃圾邮件防范	防病毒网关、垃圾邮件网关、下一代防火墙
	安全审计	行为审计系统、身份认证与准入系统、日志管理系统
	可信验证	可信计算机机制

- 区域边界部署必要的网络安全防护设备，启用安全防护策略
- 建立基于用户身份认证与准入机制，启用安全审计策略
- 采用行为模型分析等技术防御新型未知威胁攻击
- 采集并留存不少于六个月的关键网络、安全及服务器设备日志

网络设计与配置安全

根据国外一家网络安全与合规公司Titania近期发布的一项研究显示，网络配置错误使得公司平均损失年收入的9%左右。

Titania的研究基于对广泛的政府和工业垂直领域的160名高级网络安全决策者的调查。报告还警告说，由于对连接设备的审计不够频繁，使得企业容易受到网络攻击的错误配置可能会在网络上保持数月或数年时间。

该报告还发现，路由器和交换机在很大程度上被忽视了。大多数组织（96%）优先考虑防火墙的配置和审核，但只有4%的组织评估交换机和路由器以及防火墙。

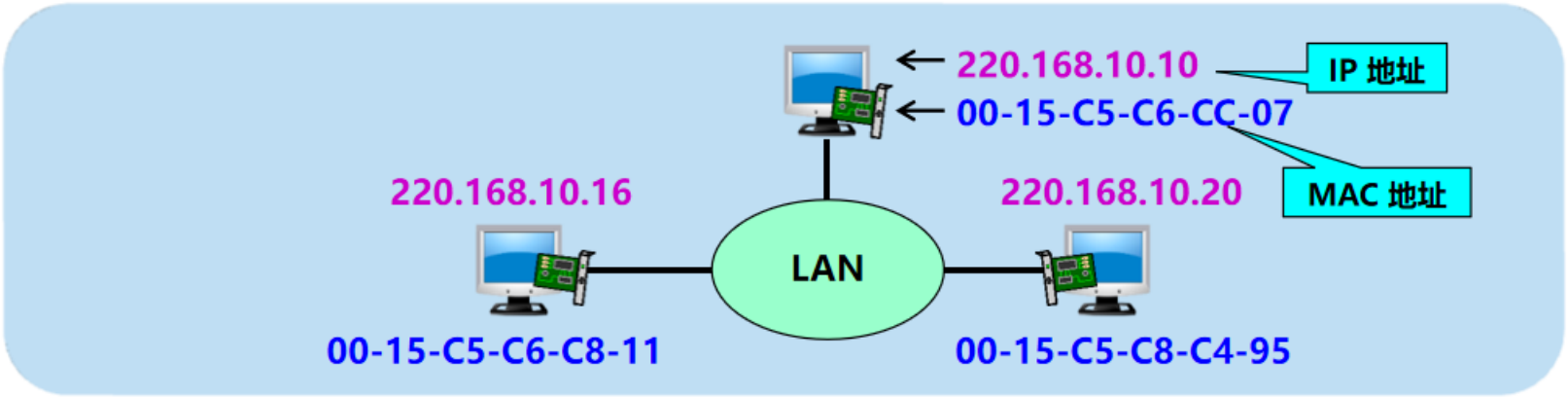
网络设备安全配置检查	主机操作系统安全配置检查	数据库安全配置检查	常见中间件及网络服务安全配置检查
OS 安全、帐号和口令管理、认证和授权策略、网络与服务、访问控制策略、通讯协议、路由协议、日志审核策略、加密管理、设备其他安全配置……	系统漏洞补丁管理、帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制、通讯协议、日志审核功能、防DDOS攻击、剩余信息保护、其他安全配置……	漏洞补丁管理、帐号和口令管理、认证及授权策略、访问控制、通讯协议、日志审核功能、其他安全配置……	漏洞补丁管理、帐号和口令管理、认证及授权策略、通讯协议、日志审核功能、其他安全配置……

TITANIA

Titania完整报告《可利用错误配置对网络安全的影响》：
https://info.titania.com/network-security-impact-report

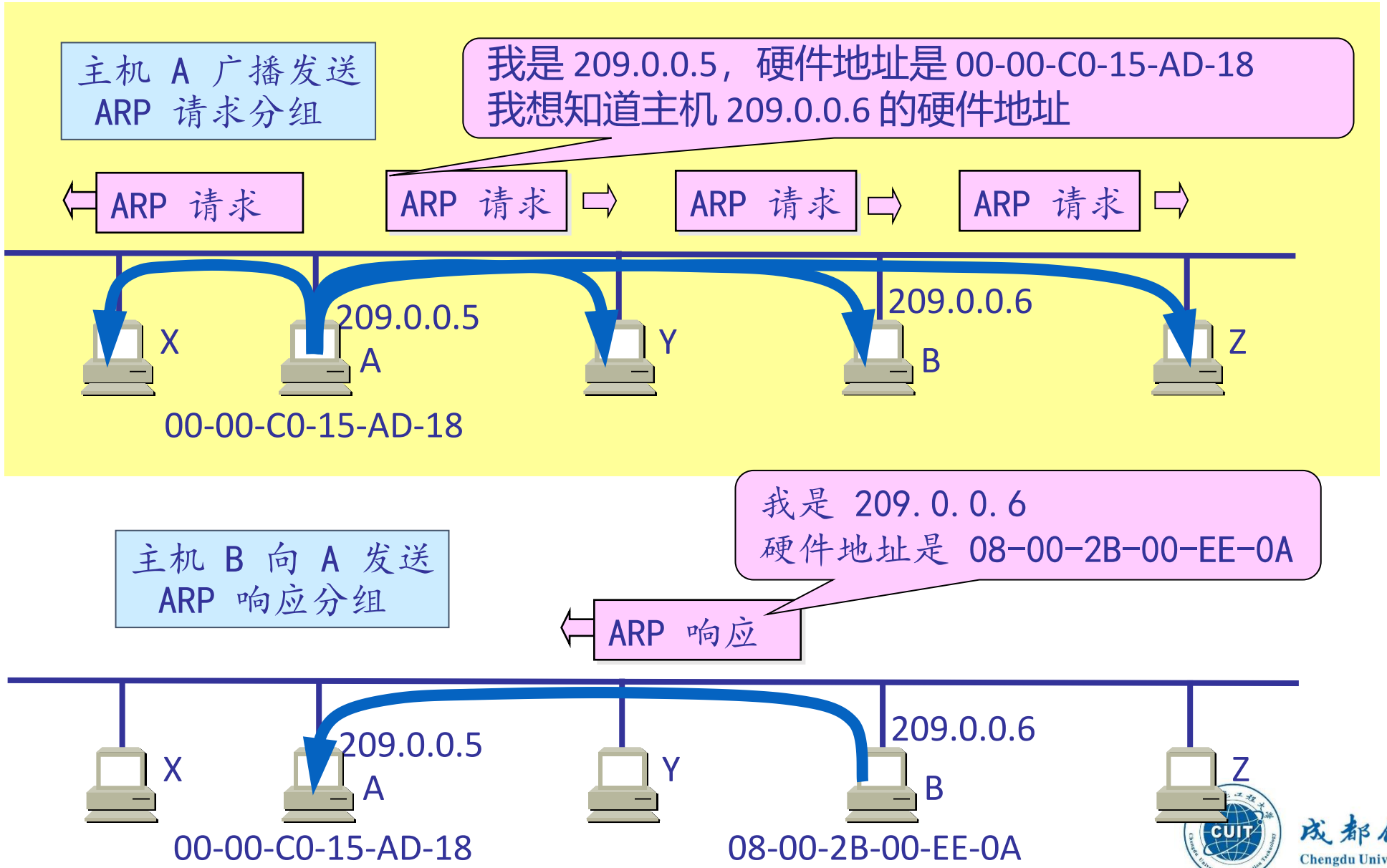
协议的安全–ARP欺骗

- 实现 IP 通信时使用了两个地址：
  1. IP 地址（网络层地址）
  2. MAC 地址（数据链路层地址）



ARP协议：在已知某接口“IP”地址的前提下，求得其对应的物理地址的协议（RFC826）。

协议的安全–ARP欺骗


主机 A 广播发送
ARP 请求分组
我是 209.0.0.5，硬件地址是 00-00-C0-15-AD-18
我想知道主机 209.0.0.6 的硬件地址
ARP 请求
ARP 请求
ARP 请求
ARP 请求
X
209.0.0.5
A
Y
209.0.0.6
B
Z
00-00-C0-15-AD-18
主机 B 向 A 发送
ARP 响应分组
我是 209. 0. 0. 6
硬件地址是 08–00–2B–00–EE–0A
ARP 响应
X
209.0.0.5
A
Y
209.0.0.6
B
Z
00-00-C0-15-AD-18
08-00-2B-00-EE-0A

协议的安全-ARP欺骗

当计算机接收到ARP应答数据包的时候，就会对本地的ARP缓存进行更新，将应答中的IP和MAC地址存储在ARP缓存中。

因此，当局域网中的某台机器B向A发送一个自己伪造的ARP应答，而如果这个应答是B冒充C伪造来的，即IP地址为C的IP，而MAC地址是伪造的，则当A接收到B伪造的ARP应答后，就会更新本地的ARP缓存，这样在A看来C的IP地址没有变，而它的MAC地址已经不是原来那个了。在A上C的MAC地址被改变成一个不存在的MAC地址，这样就会造成网络不通，导致A不能Ping通C，这就是一个简单的ARP欺骗。

主要欺骗方式：

1. 伪装成被攻击主机广播ARP请求
2. 伪装成被攻击者进行ARP应答
3. 伪装成网关进行ARP应答

协议的安全–ARP欺骗

- 实施IP+MAC地址的静态绑定策略

① 用户将网关IP地址与网关MAC地址绑定

② 网关路由器将用户IP与用户MAC绑定

- 使用ARP防护软件，它们除了本身来检测出ARP攻击外，防护的工作原理是一定频率向网络广播正确的ARP信息。
- 使用一些具有ARP防护功能的路由器

存在ARP欺骗的根本原因？

数据窃听

网络嗅探（Network sniffer）最早是为网络管理人员配备的工具，网络管理员可以利用嗅探随时掌握网络的实际情况，查找网络漏洞和检测网络性能，通过嗅探器分析网络流量，找出问题或进行网络诊断。

在黑客的手中，嗅探器就变成了一个黑客利器，就像是电话监控能听到其他人通过电话的交谈一样，嗅探能捕获在网络中传输的数据信息（窃听），以读取或截获任何网络数据包中的文本信息。此类信息包括：用户名、密码、密钥、银行账号、交易记录等任何有价值的内容。我们可以简单地将此类攻击在技术上等同于物理窃取。

① 将网卡置于“混杂模式”（promiscuous），此时网卡能够接收到一切通过它的数据，而不管实际上数据的目的地址是不是指向它（通常情况下，网卡只接受目地地址跟网卡mac地址一致、以及广播数据

② 使用集线器设备（hub）可以直接捕获所有流经集线器的网络流量（如今集线器已经被交换机所取代）

③ 嗅探器将使用大量虚假的请求发往交换机，以填满交换机的交换表。交换表满后，交换机将不得不把网络流量，以“广播”的形式发往所有端口，进而方便攻击者进行嗅探。

数据窃听-常见的嗅探工具

(1) Wireshark

作为一款开源的数据包捕获器和分析器，Wireshark支持Windows和Linux等操作系统。而作为Tcpdump的替代品，该工具是基于GUI的。Wireshark使用pcap去监控和捕获那些来自网络接口的数据包，并根据IP地址、协议和许多其他参数，对数据包进行过滤。不同的数据包可以基于相关性被分组或标记。据此，我们可以按需进行选择和分解。

(2) dSniff

dSniff可以被用于对各种网络协议进行分析和密码嗅探。它可以从FTP、Telnet、POP、rLogin、Microsoft SMB、SNMP、以及IMAP等协议中获取信息。

(3) Microsoft network monitor

顾名思义，它可以被用于针对网络数据包进行捕获、分析、以及故障排查。在功能上，该软件支持大量(300多种)协议、无线监控模式、以及碎片消息的重组等。

(4) Debookee

一款付费工具，可用于监控和分析网络。不论目标设备是笔记本电脑、网络设备、甚至是电视，它都可以拦截和分析来自其所在子网中数据流量。通常，Debookee能够提供如下三种模块：

网络分析模块：扫描已连接的设备，拦截子网中的流量，扫描TCP端口，对HTTP、DNS、TCP、以及DHCP协议在网络层面上进行分析和监控，分析VoIP呼叫等。

WiFi监控模块：提供覆盖范围内的各种AP、无线客户端、WiFi统计等详细信息。

SSL/TLS解密模块：支持监控和分析各种安全协议。

数据窃听-如何防范？

(1) **连接到受信任的网络中**：请不要为了“蹭网”，连接隔壁咖啡店提供的不受信任的免费Wi-Fi。攻击者往往会利用用户缺乏网络安全意识的特点，**在公共网络中实施流量嗅探**，或者自行**创建与既有网络ID相似的新网络**，以诱骗受害者“入局”。特别是在机场，您会发现有许多名称类似“免费机场Wi-Fi”的无线网络。说不定其中就暗藏着攻击者的嗅探器节点。因此，请您只连接到家庭或办公室之类受信任的网络中。

(2) **加密!加密!加密!重要的事情说三遍**：请对离开本系统的所有流量进行加密，以确保即使流量被嗅探到，攻击者也将无法理解其“字面意思”。例如：使用了**HTTPS协议加密流量的网站，显然比只使用HTTP的网站更加安全。**当然，值得注意的是：单纯的加密也并非万无一失，攻击者很可能会通过捕获大量的数据，运用解密工具来寻找特征，进而破解。因此，请您根据深度防御原则(defense in depth principle)，做好多层次的安全加固。

(3) **网络扫描和监控**：您必须定期对目标网络进行扫描，以查找可能以span模式捕获流量的入侵尝试，或是任何类型的恶意设备。此外，我们还需要实时监控目标网络，以尽早发现那些处于混杂模式的设备，以及网络中被安置的嗅探器。

身份冒充—IP地址欺骗

攻击者伪造IP数据包包头，使显示的信息源不是实际的来源，就像这个数据包是从另一台计算机上发送的（冒充另一个计算机系统），从而隐藏发送者的真实身份。

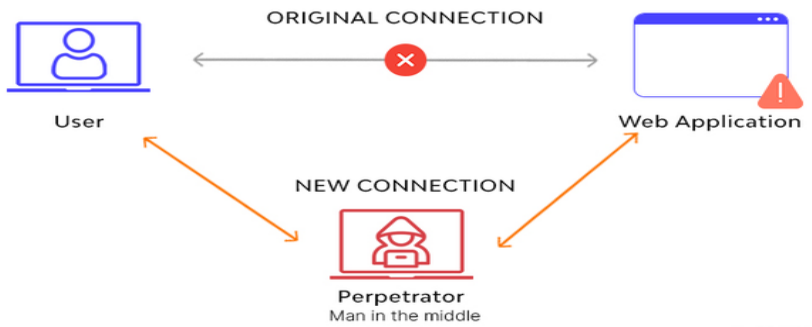
IP地址欺骗通常用作拒绝服务(DoS)、分布式拒绝服务(DDoS)或中间人(MitM)攻击的启动点。

拒绝服务(DoS)：通过制造并发送大流量无用数据，造成通往被攻击主机的网络拥塞，耗尽其服务资源，致使被攻击主机无法正常和外界通信。这涵盖了几种相关的欺骗攻击和技术，它们结合起来形成了整个攻击。

分布式拒绝服务(DDoS)：与单一来源的 DoS 攻击不同，DDoS 攻击倾向于以网络基础设施为目标，试图用大量流量使其饱和。而 DDoS 攻击是从**僵尸网络**发起的——感染恶意软件的大型连接**设备集群（通常包括个人电脑、手机、不安全的物联网设备，甚至来自公共云服务的资源）**允许攻击者进行远程控制。

中间人 (MitM)攻击：通过在数据到达用户连接的服务器之前拦截，攻击者可以使用虚假网站与用户进行交互以窃取信息。在MITM 攻击中，所涉及到达目的地之前，中间人就非法修改或访问了消息。

一旦攻击者通过欺骗 IP 地址获得对个人通信帐户的访问权限，就可以跟踪该通信的任何方面：窃取信息、将用户引导到虚假网站等。



身份冒充—IP地址欺骗如何防范？

- **通过在路由器或防火墙上开启对数据包的过滤**：最基本的形式是不允许任何外部进入的数据包使用单位内部的地址作为IP地址的源地址。
- **防范信任关系欺骗**：保护自己免受信任关系欺骗攻击最容易的方法就是不使用信任关系，可以有效防止IP欺骗，但这并不是最佳的解决方案。不过可以通过做一些事情使信任关系的暴露达到最小，限制拥有信任关系的人员，相比控制建立信任关系的机器数量，决定谁真正需要信任关系更加有意义。
- **进行加密通信**。加密技术是可以防范会话劫持攻击为数不多的方式之一。如果攻击者不能读取传输数据，那么进行会话劫持攻击也是十分困难的。无论何时当用户连入到一个远端的机器上，特别是当从事敏感工作或是管理员操作时，都应当使用安全协议。
- **限制保护措施**。允许从网络上传输到用户单位内部网络的信息越少，那么用户将会越安全，这是个最小化会话劫持攻击的方法。攻击者越难进入系统，那么系统就越不容易受到会话劫持攻击。

安全意识与管理

案例一

2019年2月，南京某研究院、无锡某图书馆因**安全责任意识淡薄、网络安全等级保护制度落实不到位、管理制度和技术防护措施严重缺失**，导致网站遭受攻击破坏。南京、无锡警方依据《网络安全法》第21条、第59条规定，对上述单位分别予以5万元罚款，对相关责任人予以5千元、2万元不等罚款，同时责令限期整改安全隐患，落实网络安全等级保护制度。

案例二

2020年8月13日10时30分许，三河市公安局行宫东大街派出所民警在对三河某燃气有限公司进行网络安全检查时发现，**该单位未建立安全培训和考核制度，没有对信息安全进行等级保护，未落实网络安全保护责任**。三河市警方根据《中华人民共和国网络安全法》第33条、第34条、第36条、第38条和第59条规定，依法对该公司警告处罚。

网络安全等级保护2.0中有关管理要求

➢ 安全管理制度

针对整个管理制度体系提出的安全控制要求，涉及的安全控制点包括安全策略、管理制度、制定和发布以及评审和修订。

➢ 安全管理机构

针对整个管理组织架构提出的安全控制要求，涉及的安全控制点包括岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查。

➢ 安全管理人员

针对人员管理提出的安全控制要求，涉及的安全控制点包括人员录用、人员离岗、安全意识教育和培训以及外部人员访问管理。

➢ 安全建设管理

针对安全建设过程提出的安全控制要求，涉及的安全控制点包括定级和备案、安全方案设计、安全产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评和服务供应商管理。

➢ 安全运维管理

针对安全运维过程提出的安全控制要求，涉及的安全控制点包括环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理和外包运维管理。

THE END