



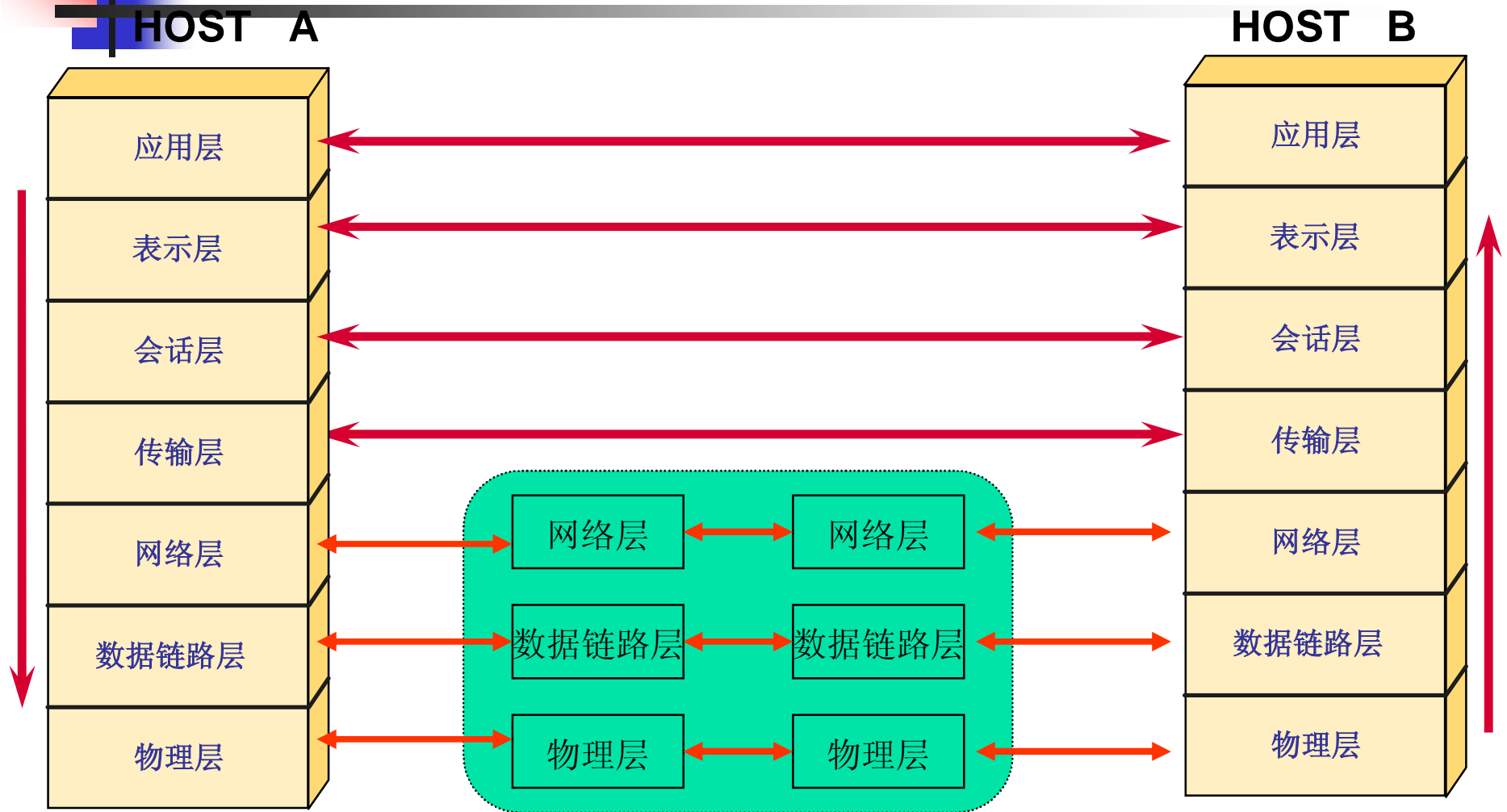
第2章 计算机网络基础知识

2.1 开放系统互联参考模型

2.2 TCP/IP 协议

2.3 局域网与广域网技术

2.1 开放系统互联参考模型 (OSI/RM)





物理层、数据链路层

(1) 物理层(physical layer)

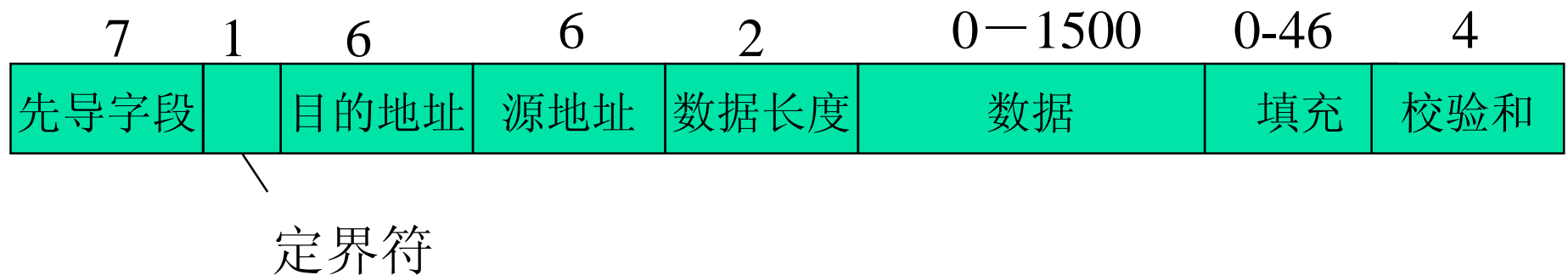
- n 物理层涉及到通信在信道上传输的原始比特流，主要处理与物理传输介质有关的机械的、电气的、功能的和规程的接口。物理层与具体设备有关，如光纤及收发器、网卡和集线器等。

(2) 数据链路层(data link layer)

- n 数据链路层的主要任务是加强物理层传输原始比特的功能，使之对网络层显现为一条无差错的链路。它通过将传输的数据增加同步信息、校验信息及地址信息封装成数据帧；同时提供数据帧传输顺序的控制、差错检测与控制 and 数据流量控制以保证数据传输的正确性。

数据链路层PDU举例

n X802.3 帧格式



MAC地址：BIA地址

数据链路层的广播包：目标MAC地址为1111....111

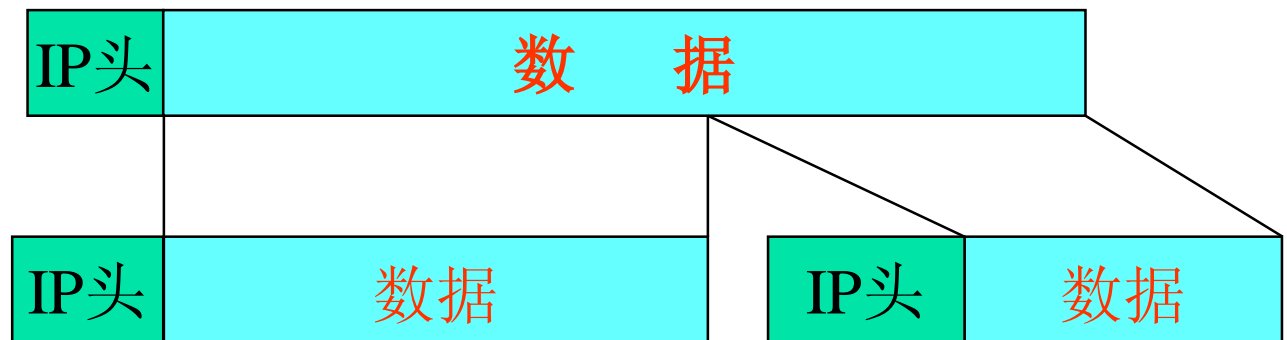


网络层(network layer)

- n 功能 确定数据分组从源端到目的端如何选择路由。即通过路径选择将信息从最合适的路径由发送端传送到接收端，防止通信子网信息流量过大造成网络阻塞及数据丢失。
 - n 编址
 - n 路由
- n 协议数据单元(PDU)
 - n 包、分组 (Packet)
- n 网络层协议
 - n IP, IPX
 - n 网络地址

网络层PDU的封装

网络层的包
与分片（Fragment）



MAC层的
帧



物理层
比特流

010101....01010010100.....10101001010010101010



传输层、会话层

- n 传输层(transport layer)

传输层的基本功能是从会话层接收数据，并且在必要时把它分成较小的单元，传递给网络层，并确保到达对方的各段信息正确无误，从某种意义上讲，传输层使会话层不受硬件技术变化的影响。

- n 会话层(session layer)

会话层允许不同机器上的用户建立会话(session)关系。会话层服务之一是管理对话。会话层允许信息同时双向传输或任一时刻只能单向传输。若属于后者，则类似半双工通信，会话层将记录此时该轮到哪一方了。



表示层、应用层

- n 表示层(presentation layer)

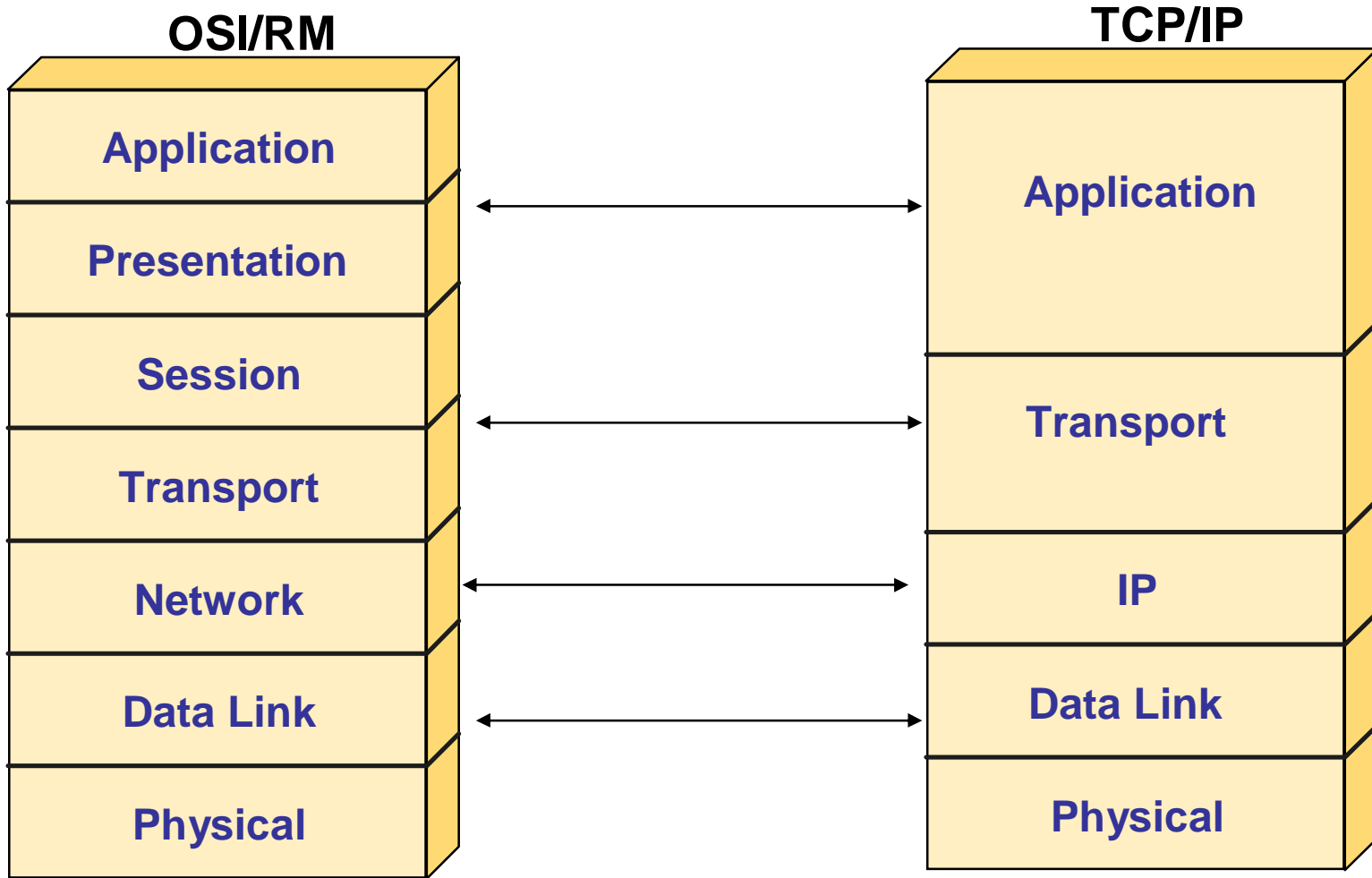
表示层主要完成以下特定的功能：

- ① 对数据编码格式进行转换；
- ② 数据压缩与恢复；
- ③ 建立数据交换格式；
- ④ 数据的安全与保密；
- ⑤ 其他特殊服务。

- n 应用层(application layer)

应用层包含大量人们普遍需要的协议和提供许多应用软件包。例如FTP、E-mail等程序及应用软件包。

OSI参考模型与TCP/IP协议模型



2.2 TCP/IP 协议栈结构

应用层

SMTP	FTP	HTTP	telnet	DNS	SNMP	RPC...
OSPF	BGP	DNS...	NetBIOS	SMB	RIP	

传输层

TCP

UDP

网络层

ICMP

IGMP

IP

ARP

RARP

数据链路层

802.x

X.25

PPP

FR

ATM

....

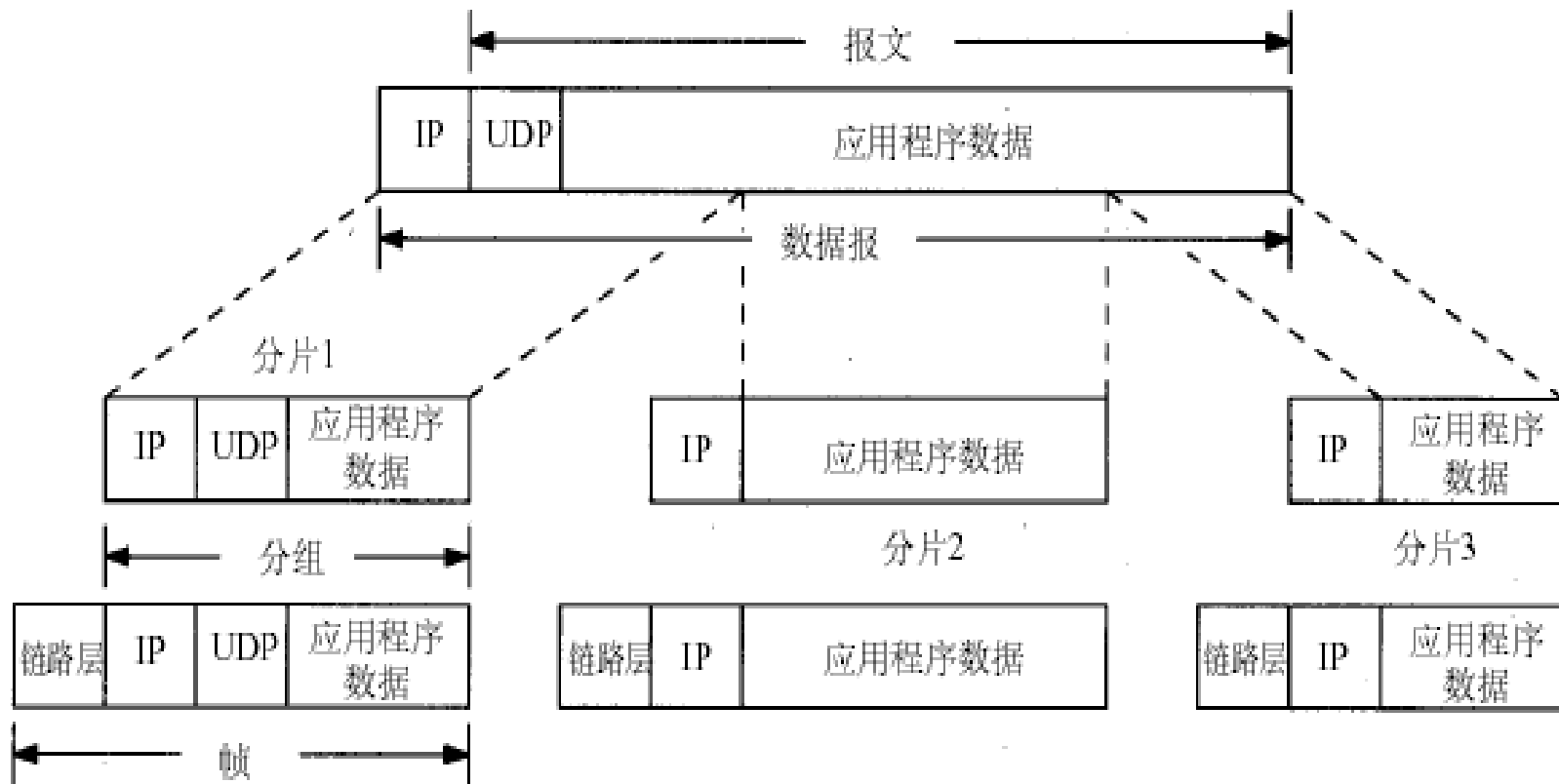
通信介质（铜缆、光纤、卫星、微波等）



IP层（网络层）安全机制

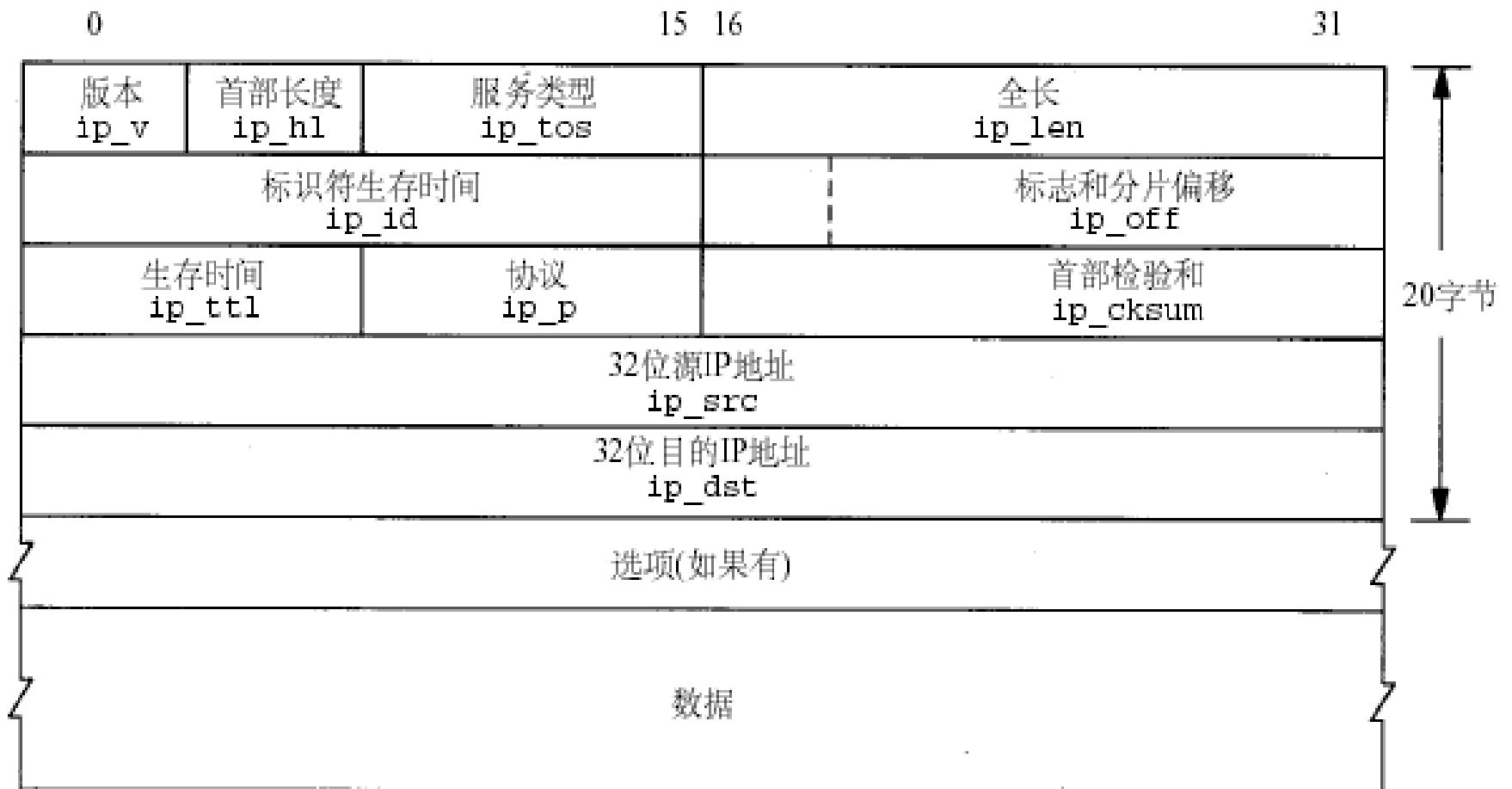
- n IP, ARP/RARP, ICMP
- n 路由协议：RIP, OSPF, BGP等
- n 安全服务
 - n 不提供认证服务
 - n 不提供数据保密性服务
 - n 不提供数据完整性保护
 - n 不提供抗抵赖服务
 - n 不保证可用性—服务质量（QoS）
 - n 通过防火墙可以提供基于IP地址的访问控制

帧、分组、分片、数据报和报文



帧、分组、分片、数据报和报文

IP 包的结构





IP 包的结构

- n VERS: 版本号
- n HLEN: 头的长度(5-60)
- n TOS: 服务类型, 用于服务质量控制
- n Total Length: 总长度 (≤ 65536)
- n Identification: 标识, 同一个包的多个分片具有相同的标识
- n DF (Don't Fragment): 若为1, 表示不允许分片
- n MF (More Fragment): 若为1, 表示后面还有分片
- n Frag Offset: 分片在整个IP包中的位置
- n TTL(Time To Life): 生命周期, 每过一个路由器(网关)减一, 防止包在网络中循环漫游
- n Protocol: 上层协议, 比如1:ICMP, 6:TCP, 17:UDP, BGP:8
- n 头校验和
- n 源地址, 目标地址
- n 选项: 安全性, 源路由, 记录路由, 时间戳



地址解析协议 (ARP/RARP)

n ARP/RARP: IP 地址 \rightarrow 数据链路层地址
ARP IP \rightarrow MAC

相同子网的地址解析:

A \rightarrow ALL: Who has IP x.x.x.x?

B \rightarrow A: My MAC address is x.x.x.x

不同子网的地址解析:

A \rightarrow ALL: who is x.x.x.x(缺省网关)

伪造远端机的连接 广播 局域网

RARP MAC \rightarrow IP 无盘工作站 (Linux) BOOTP TFTP



网络控制消息协议 (ICMP)

n ICMP(Internet Control Message Protocol)

报文类型

目的不可达

超时 (TTL=0) ;

源端抑制;

重定向

回声请求/回声应答

时间戳请求/时间戳应答

ping命令 tracert

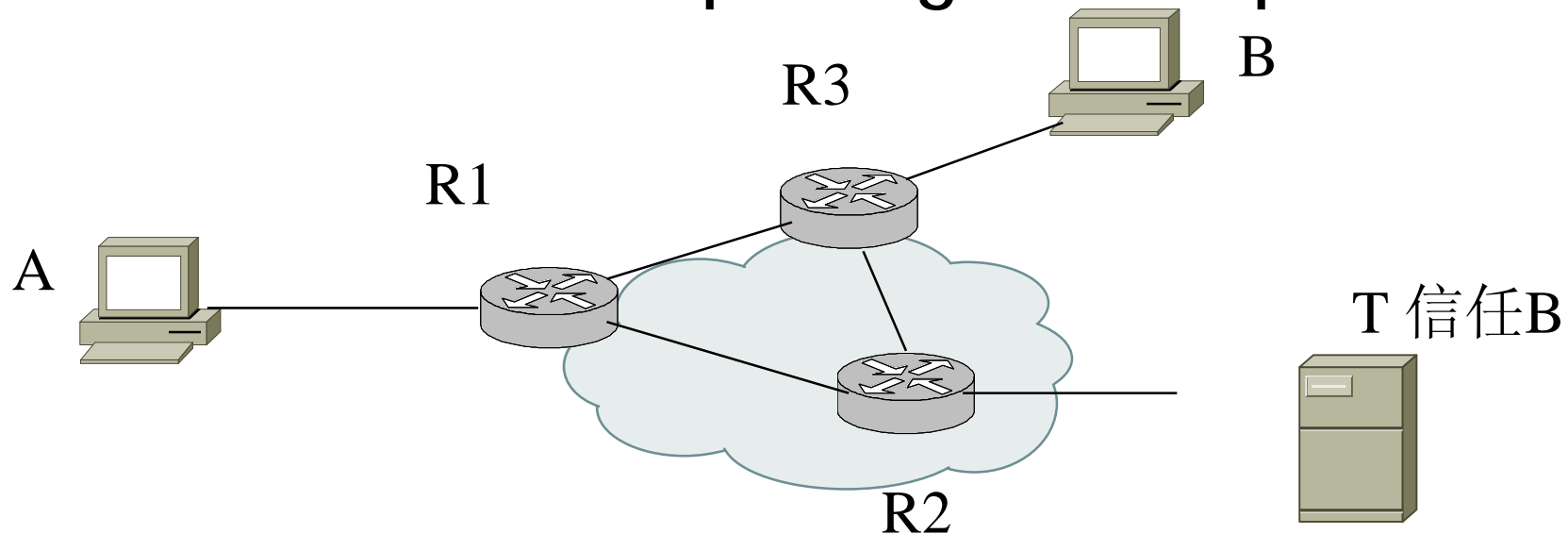


网络层协议安全问题

- n 地址欺骗
 - n IP 地址欺骗
 - n ARP 欺骗
 - n MAC地址欺骗
- n 拒绝服务攻击
 - n ARP 广播风暴
 - n Teardrop
 - n Smurf

路由问题

n 源地址路由问题 ipconfig, route print

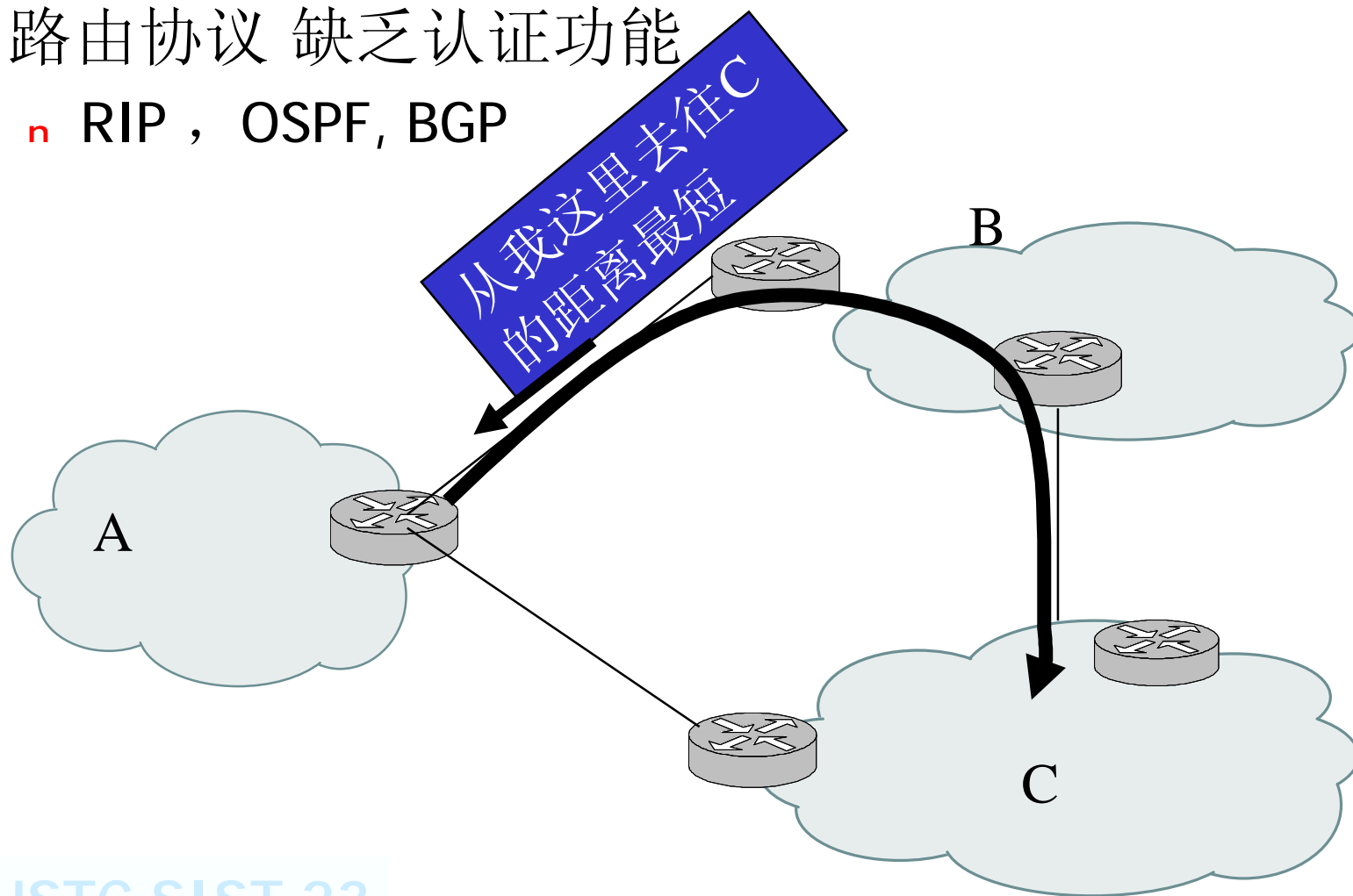


A 假冒 B 的地址访问T, 指定返回的路径必须是R2à R1

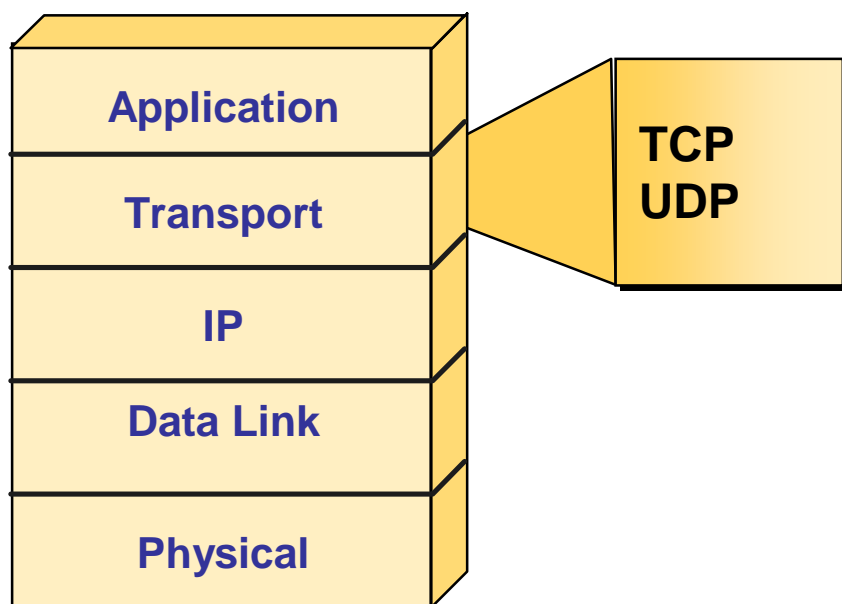
路由黑洞

n 路由协议 缺乏认证功能

n RIP , OSPF , BGP



TCP层（传输层）安全机制



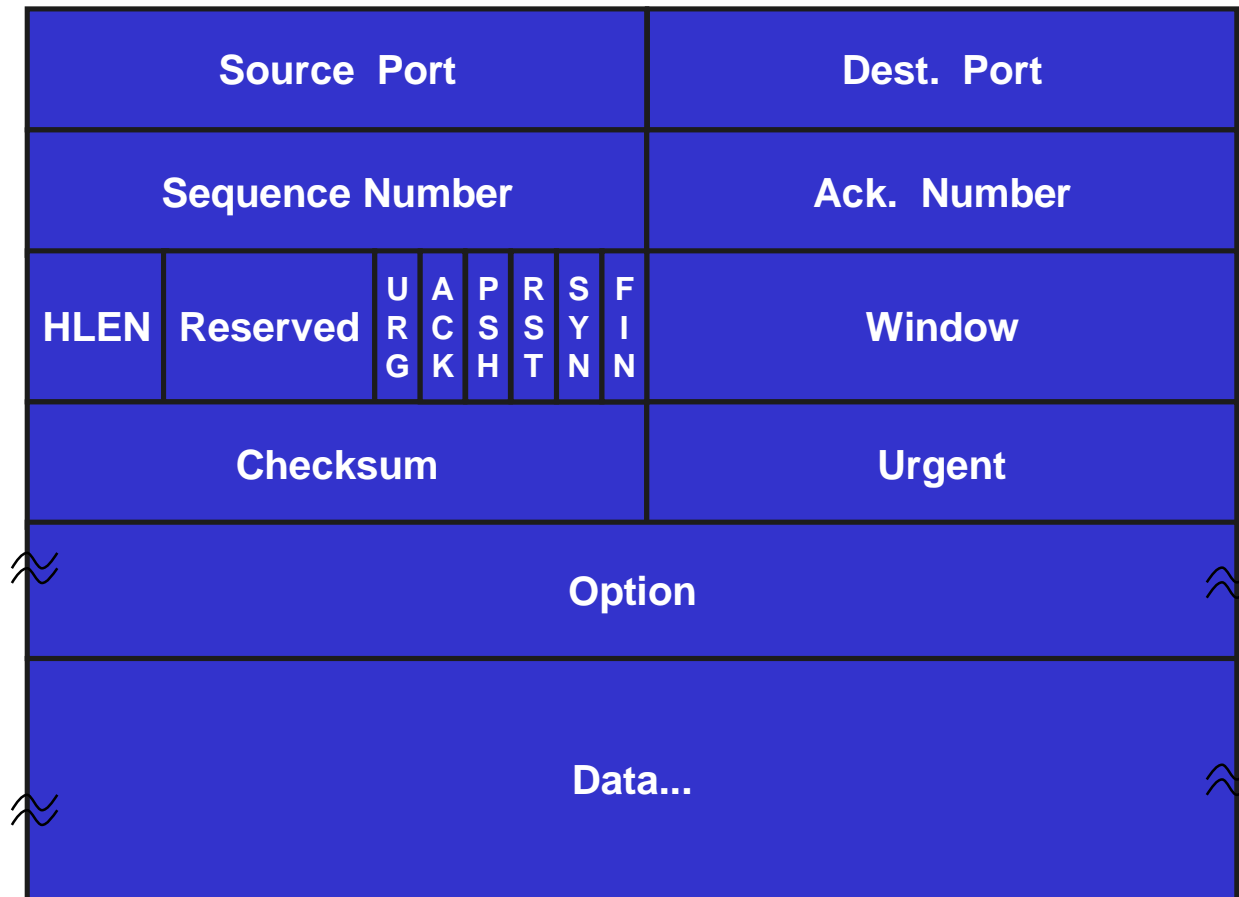
n 安全机制

- ∅ 可以提供基于IP地址的认证，和访问控制
- ∅ 不提供数据保密性、完整性服务
- ∅ 不提供抗抵赖服务
- ∅ 不提供可用性服务，不保证服务质量



TCP Segment Format

0



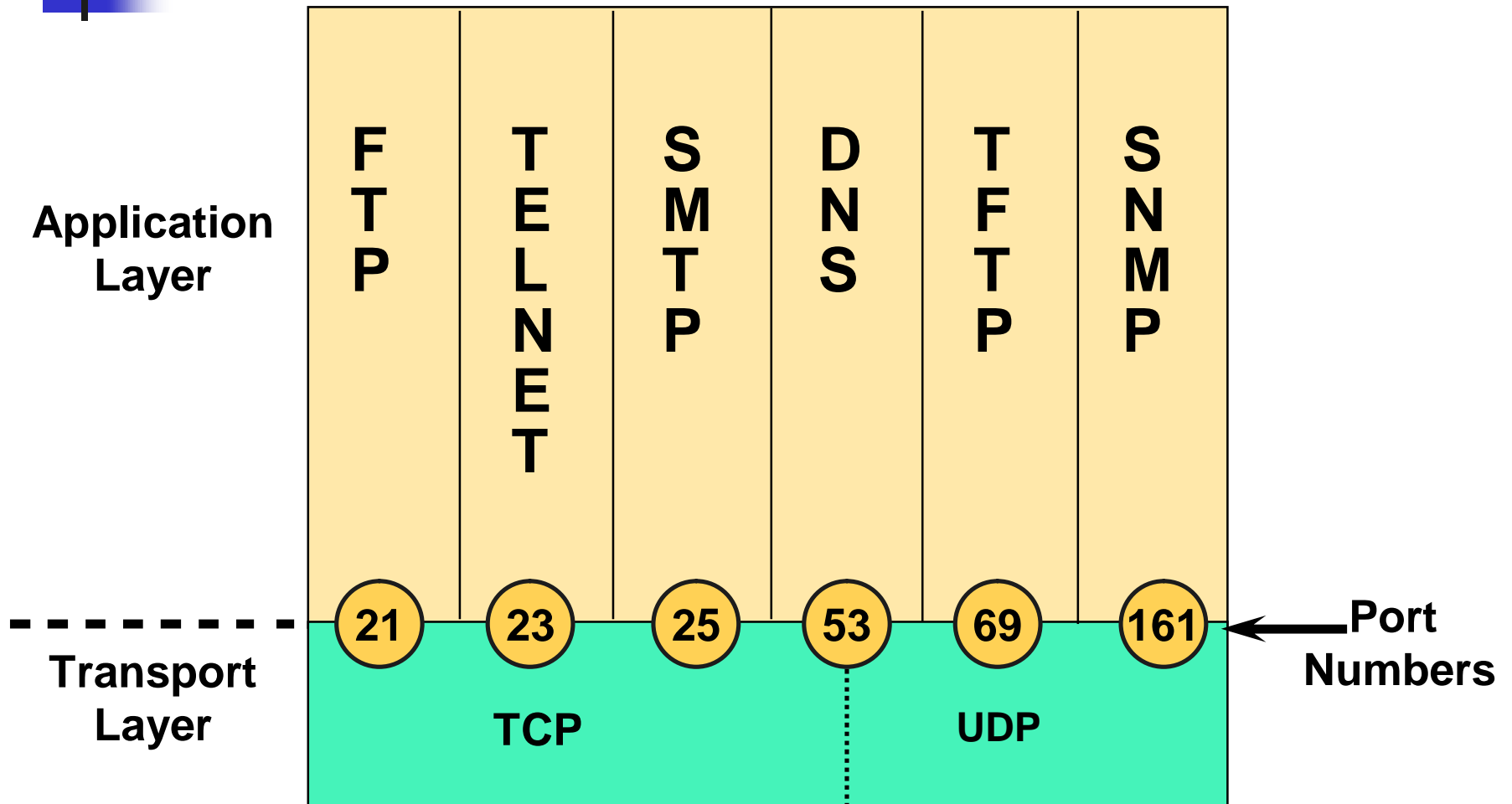


UDP Segment Format

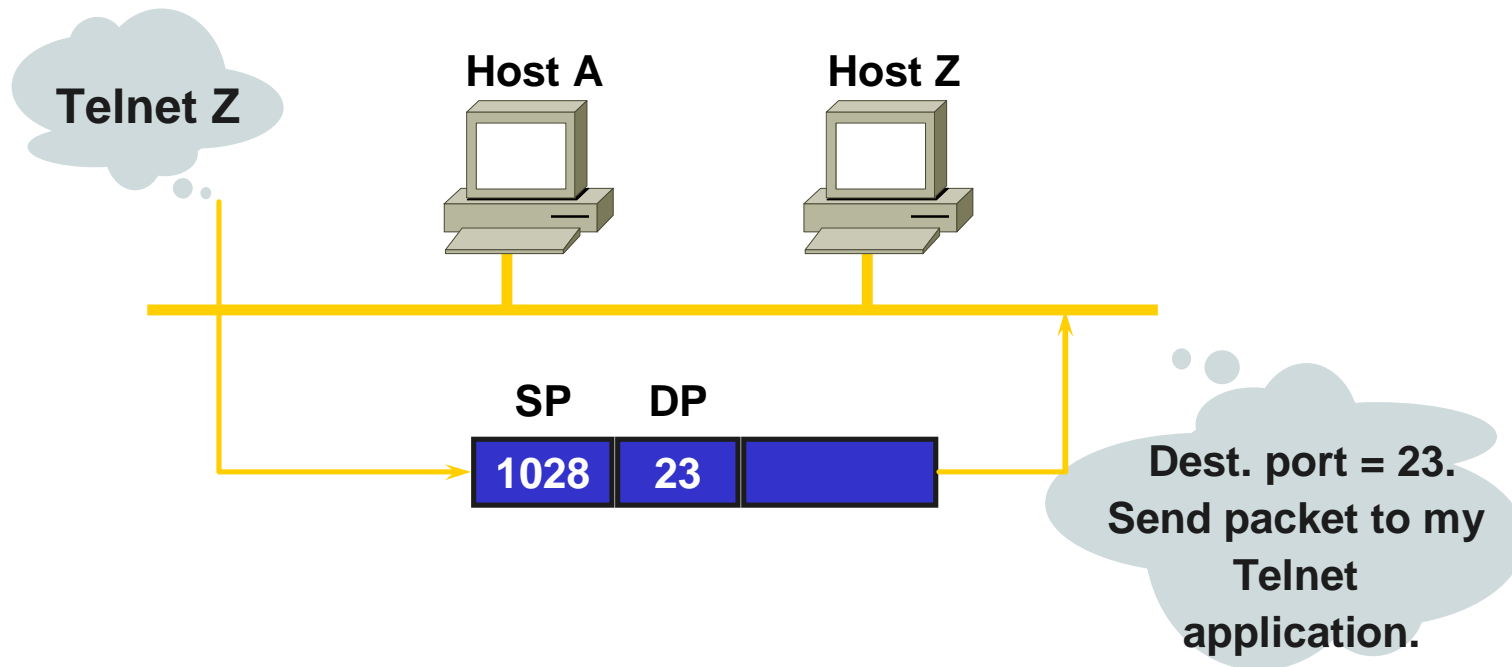
Source Port	Destination Port
Length	Checksum
Data	

- n No sequence or acknowledgment fields

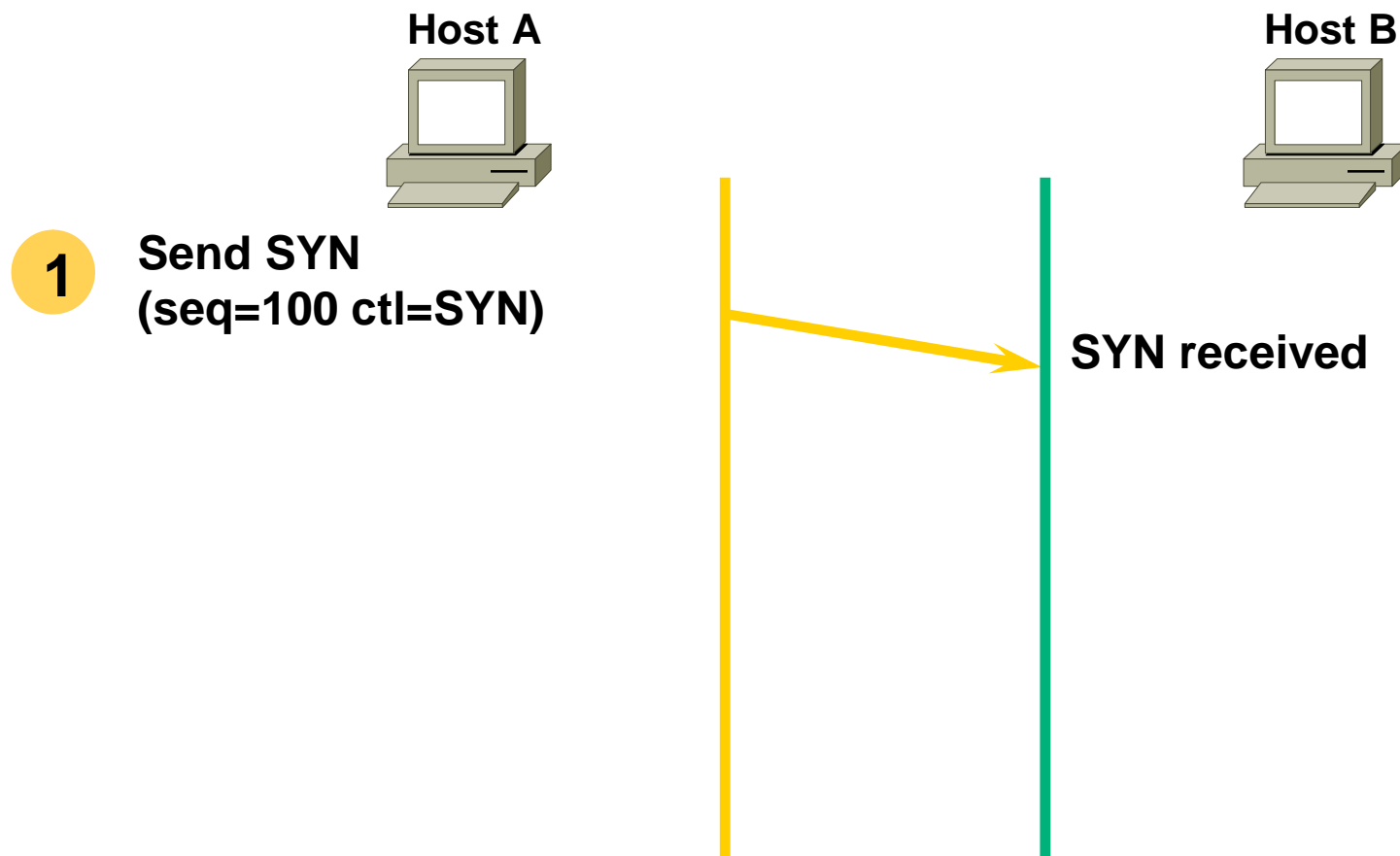
Port Numbers



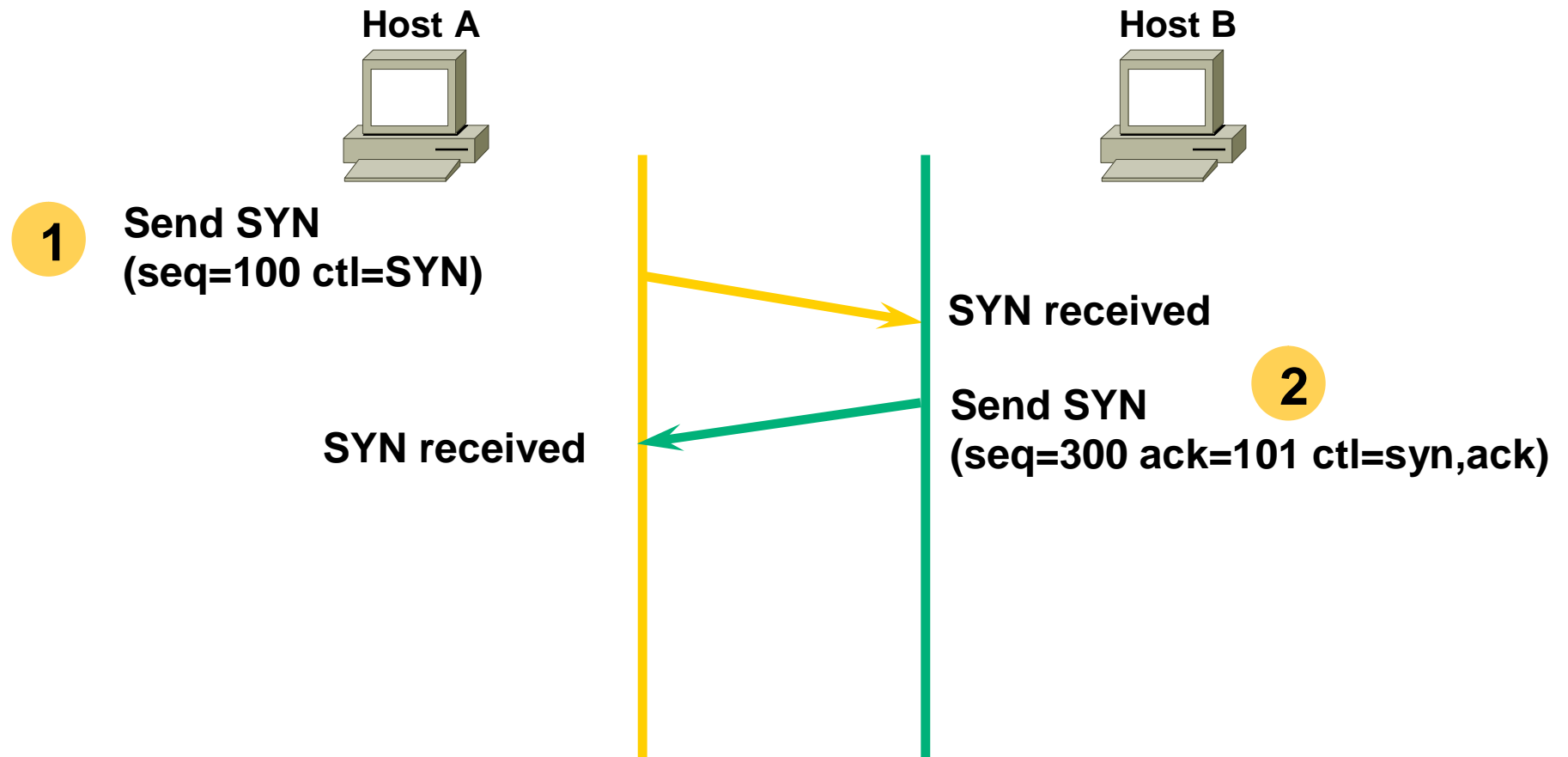
TCP Port Numbers



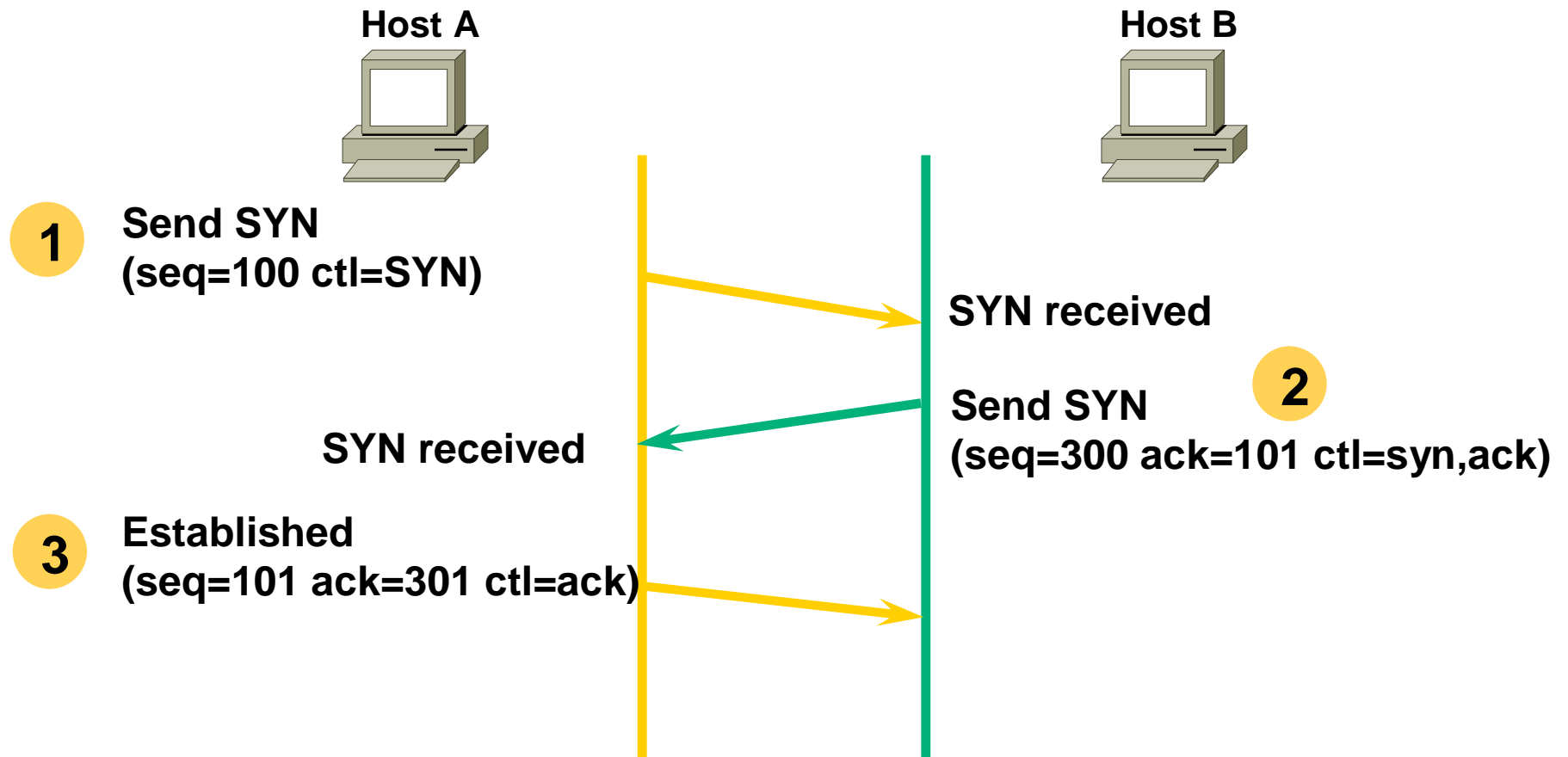
TCP Handshake/Open Connection



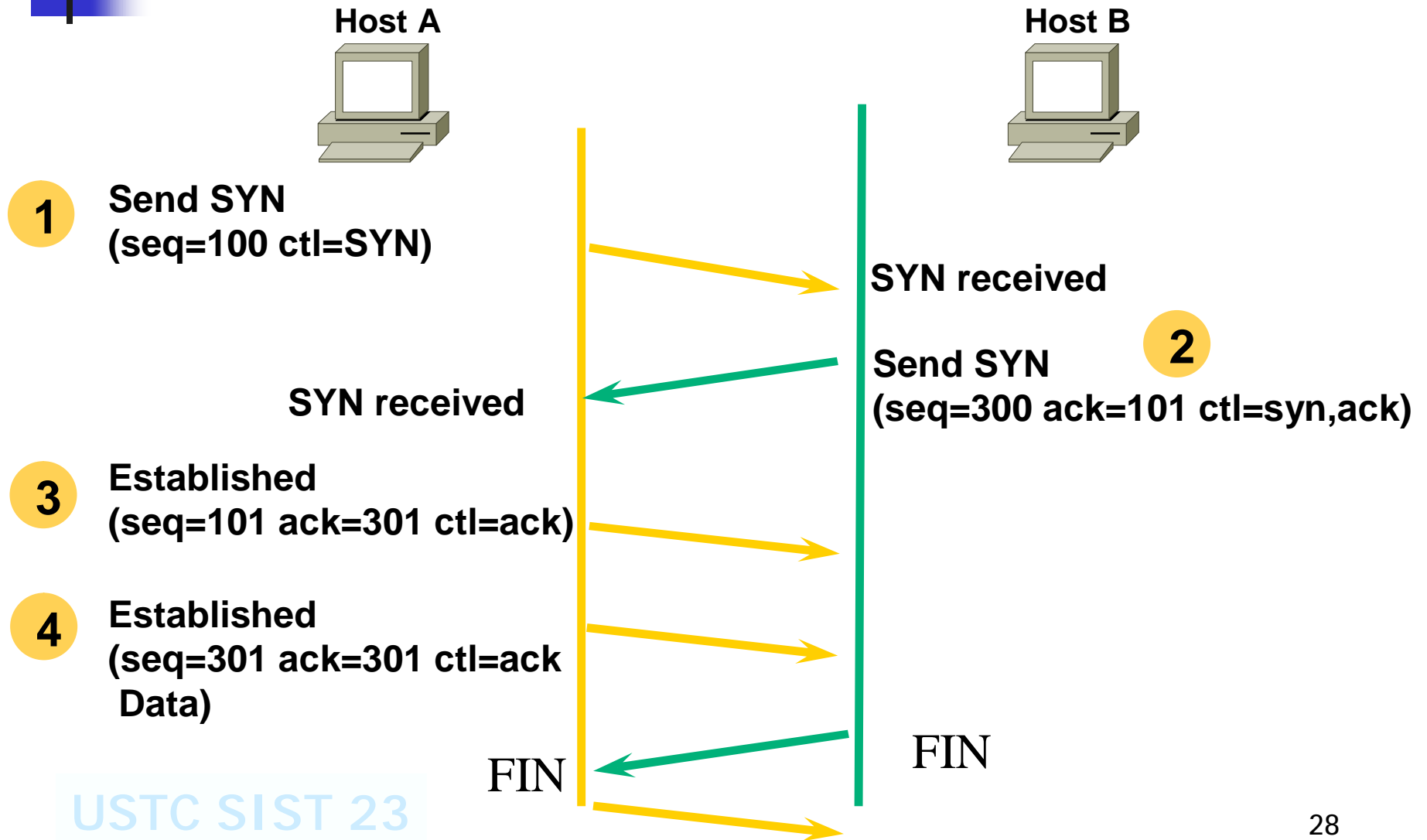
TCP Handshake/Open Connection



TCP Handshake/Open Connection

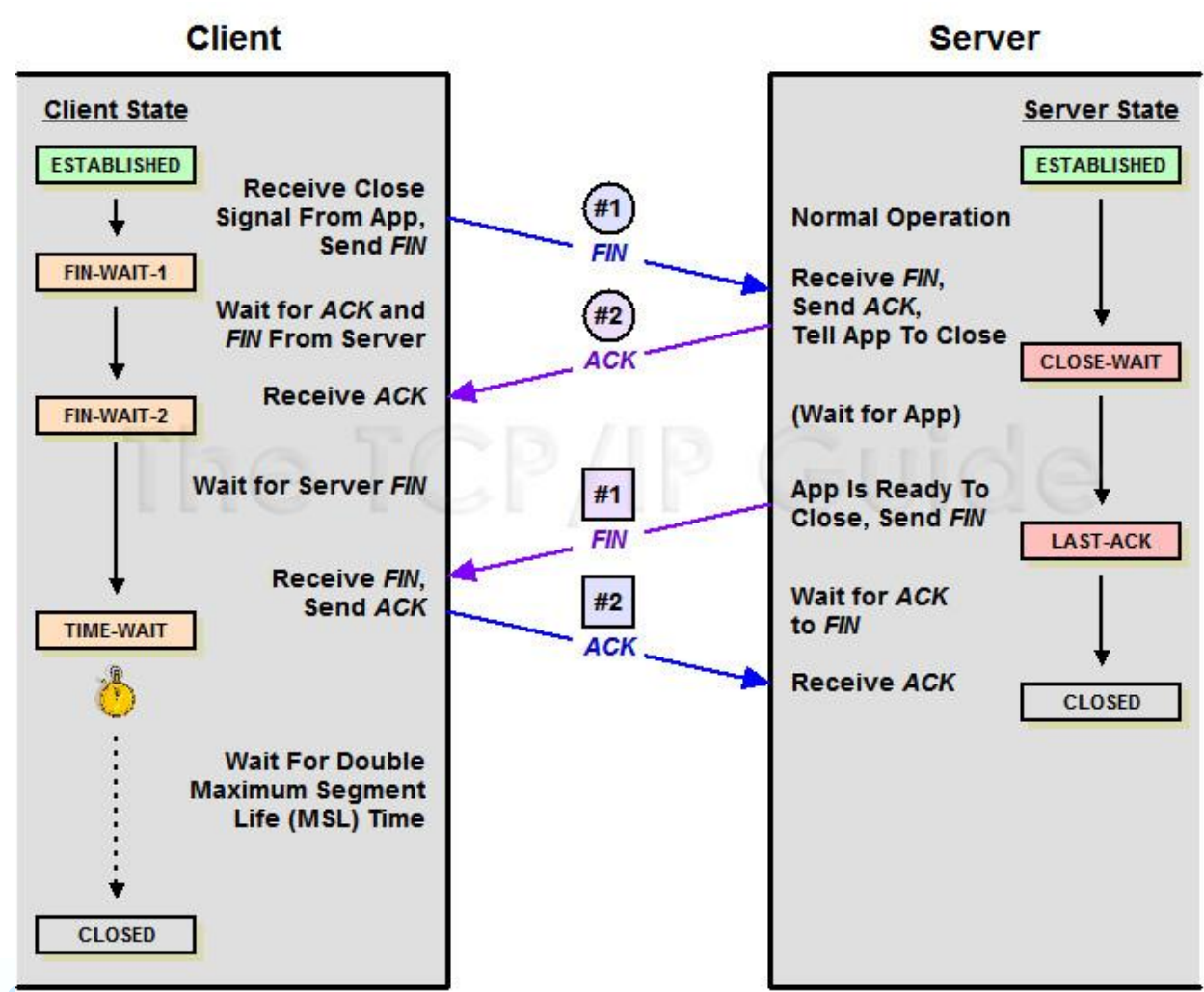


TCP Handshake/Open Connection



TCP协议的四次“挥手” handwave?

- n 需要断开连接的时候，TCP也需要互相确认才可以断开连接，四次交互过程如图所示。



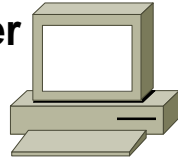


传输层安全问题

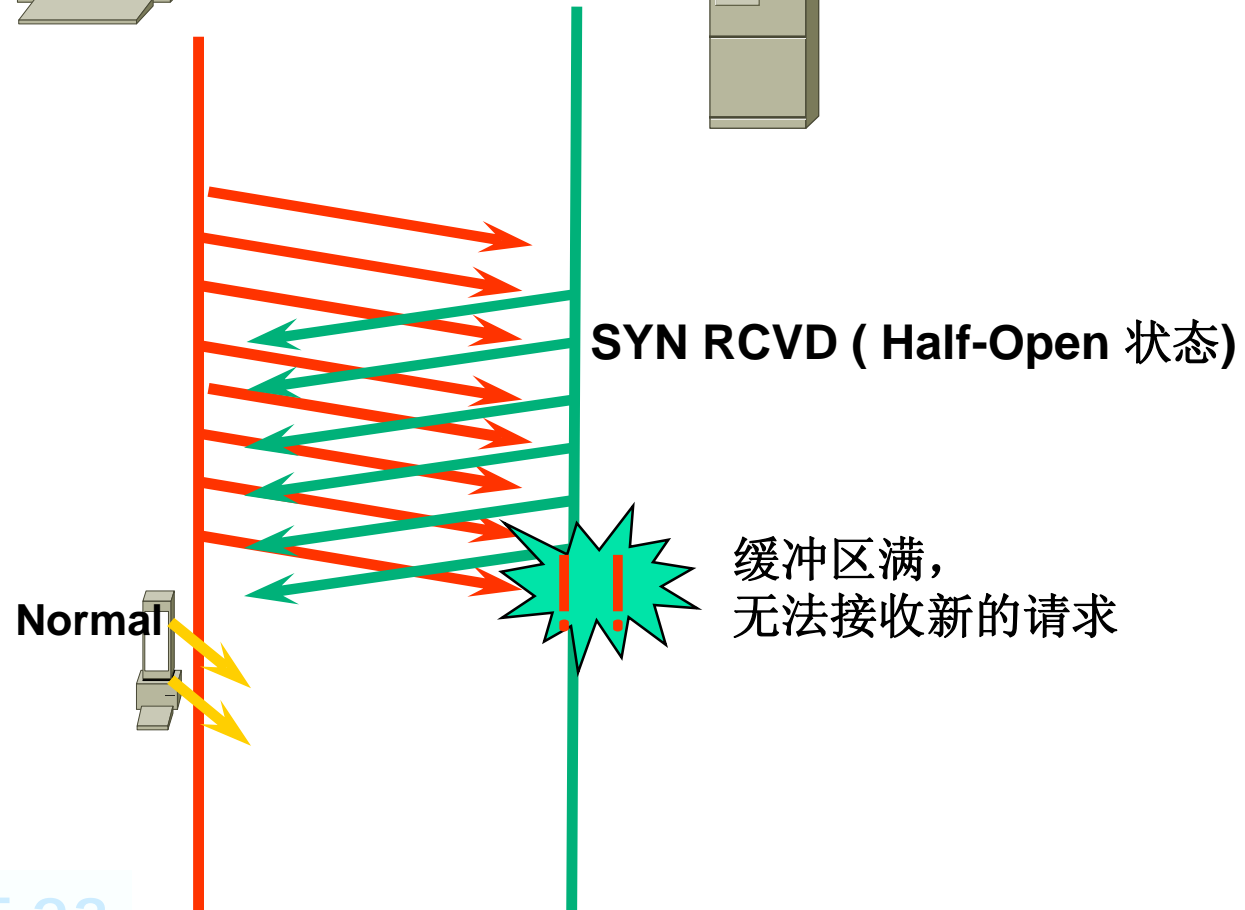
- n 基于TCP序列号预测的攻击
 - n 信任主机之间的地址欺骗
 - n FIN 或RST 可以终止当前的连接
- n SYN Flood 拒绝服务攻击

SYN Flood

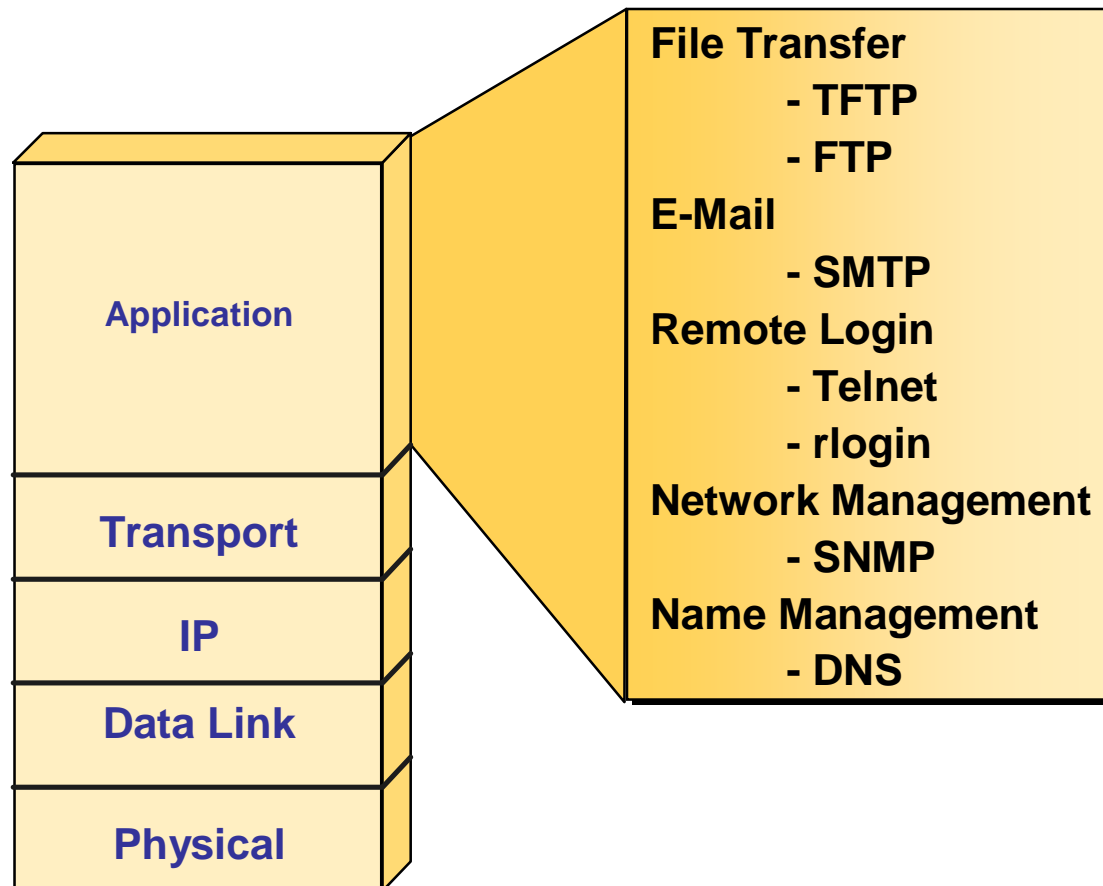
attacker



target



应用层主要功能及安全机制



inetd(UNIX), svchost.exe(Windows) 根据端口启动相应服务程序

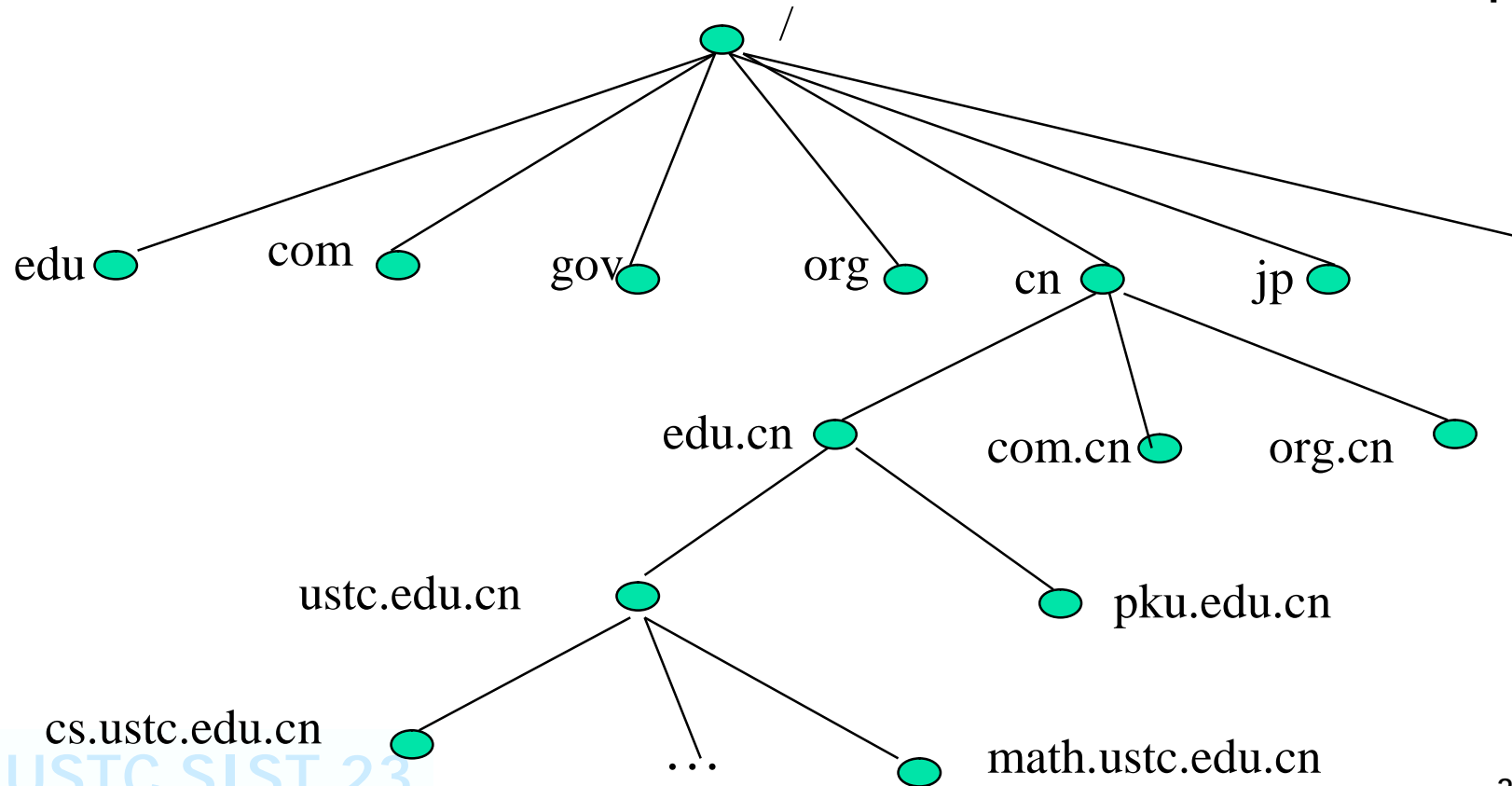


电子邮件协议概述

- n SMTP (Simple Mail Transfer Protocol 简单邮件传输协议): 最常用的电子邮件传送协议;
 - n RFC 821, 1982年公布,
 - n TCP 25 端口
 - n 常用命令
 - n HELO,MAIL ,RCPT,DATA,RSET,VRFY,QUIT...
 - n 没有提供任何安全服务
- n POP3 (Post Office Protocol 3邮局协议): 最常用的电子邮件接收协议 110 端口;
- n IMAP4 (Internet Mail Access Protocol 网络邮件访问协议): 143 端口, 替代POP3, 提供邮件检索和邮件处理的新功能。

DNS 基础

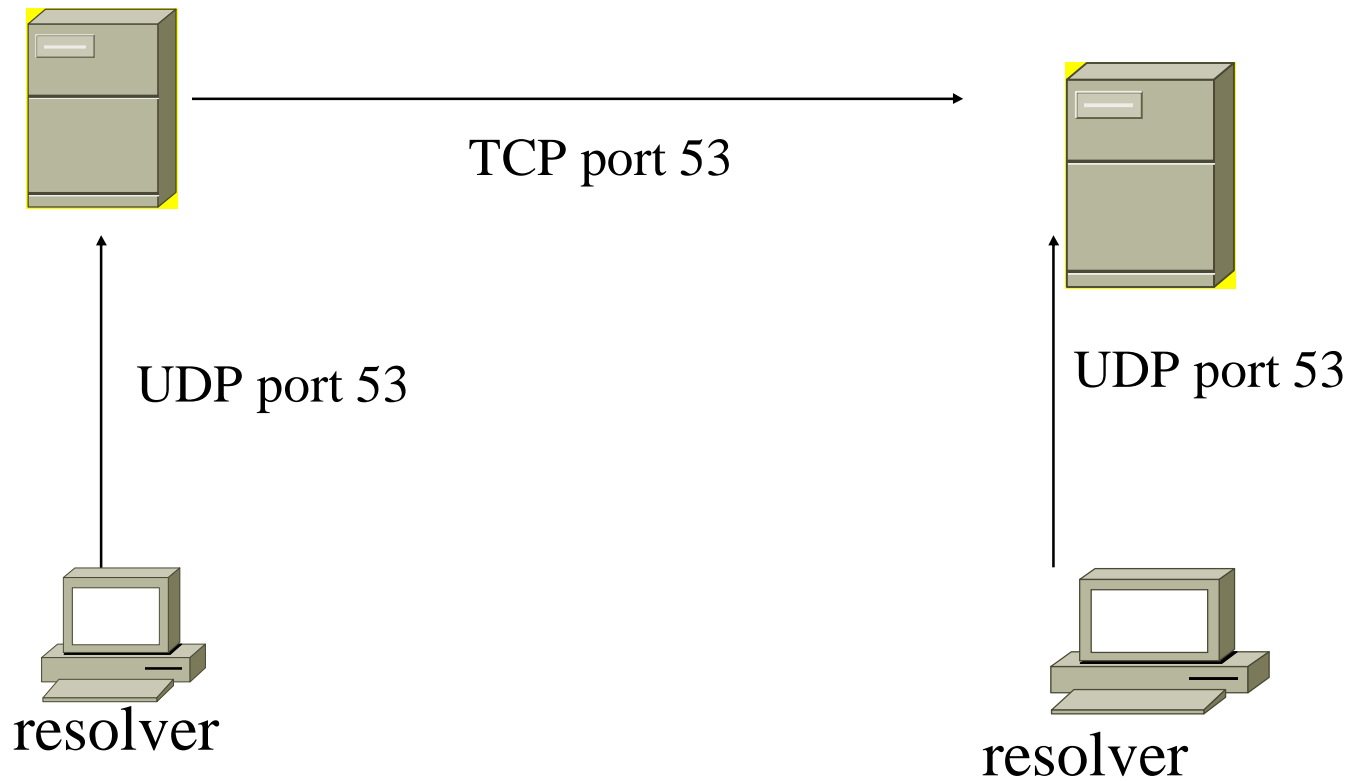
- n 域名服务Domain Name System/Service/Server是最重要的基础设施之一，主要使用UDP协议
- n 分布式数据库， 域名 \rightarrow IP地址 DNS设置、nslookup



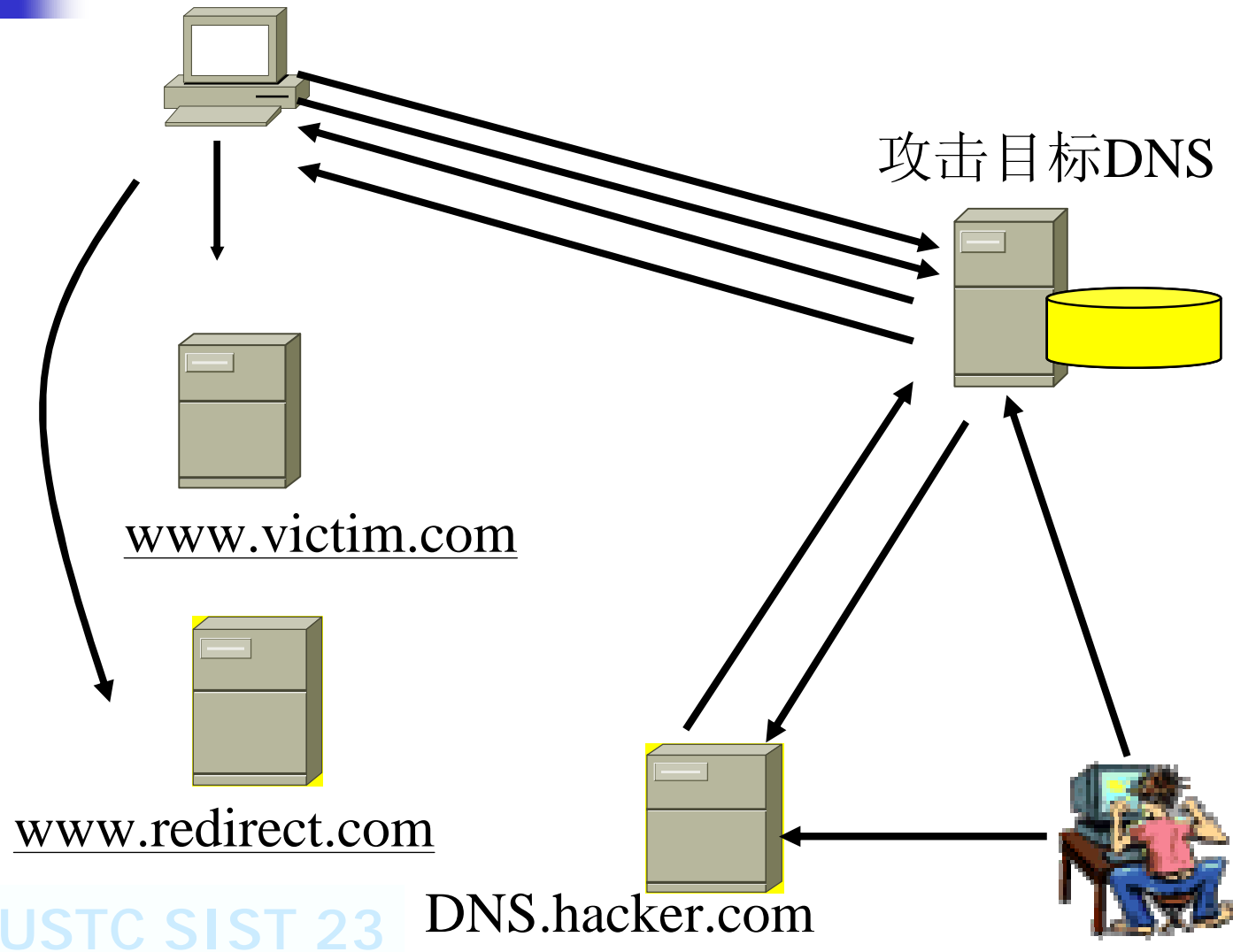
Resolver, Primary & secondary DNS

Primary DNS

Secondary DNS



DNS Cache Pollution





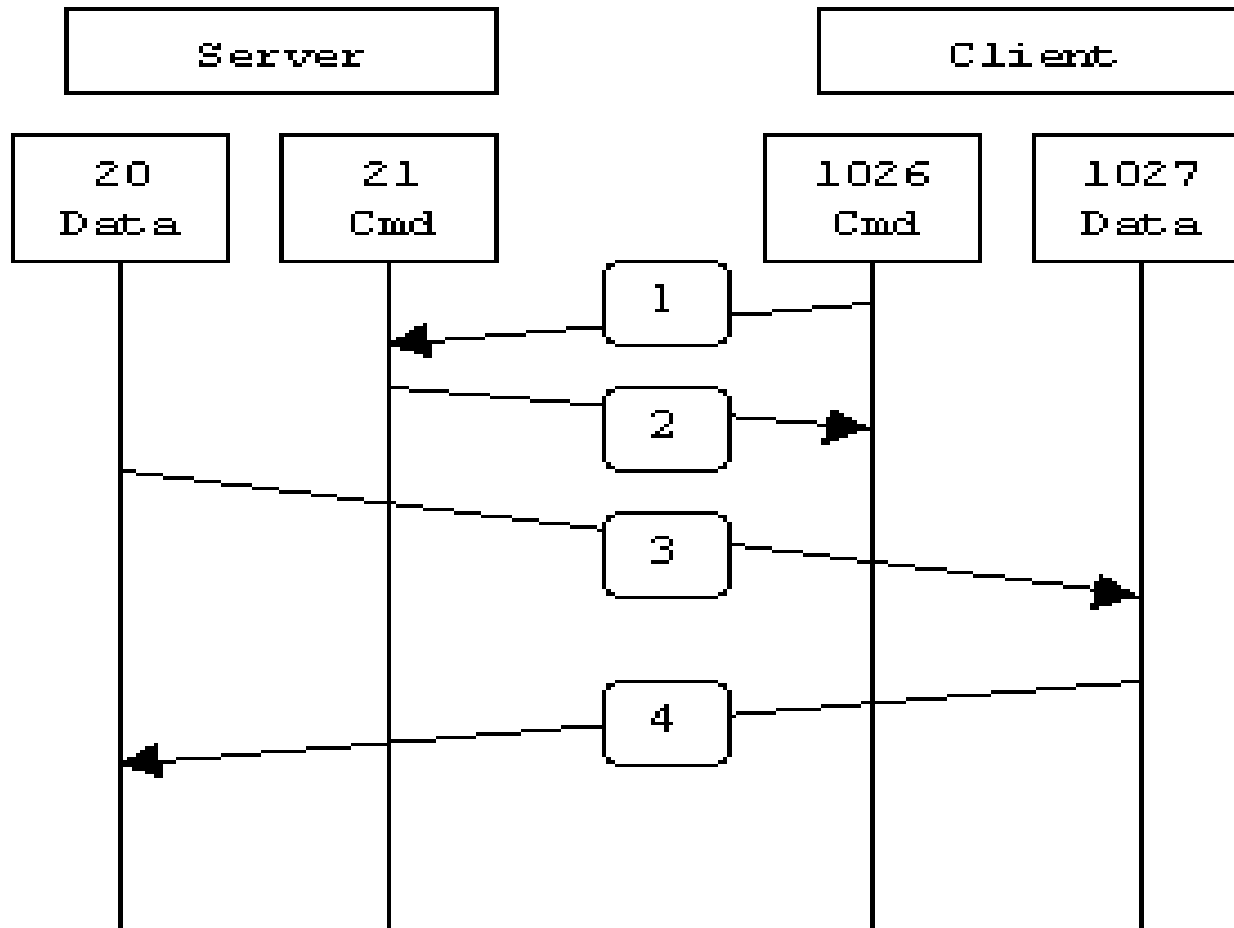
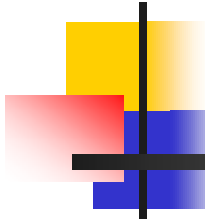
FTP File Transfer Protocol (文件传输协议)

FTP Active主动模式 客户端 命令行、GUI、浏览器

FTPD 21控制端口 20数据端口，命令和数据能够同时传输
小于1024的端口号需root权限

连接过程：

- To FTP server's port 21 from anywhere (Client initiates connection)
- FTP server's port 21 to ports > 1024 (Server responds to client's control port)
- FTP server's port 20 to ports > 1024 (Server initiates data connection to client's data port)
- To FTP server's port 20 from ports > 1024 (Client sends ACKs to server's data port)



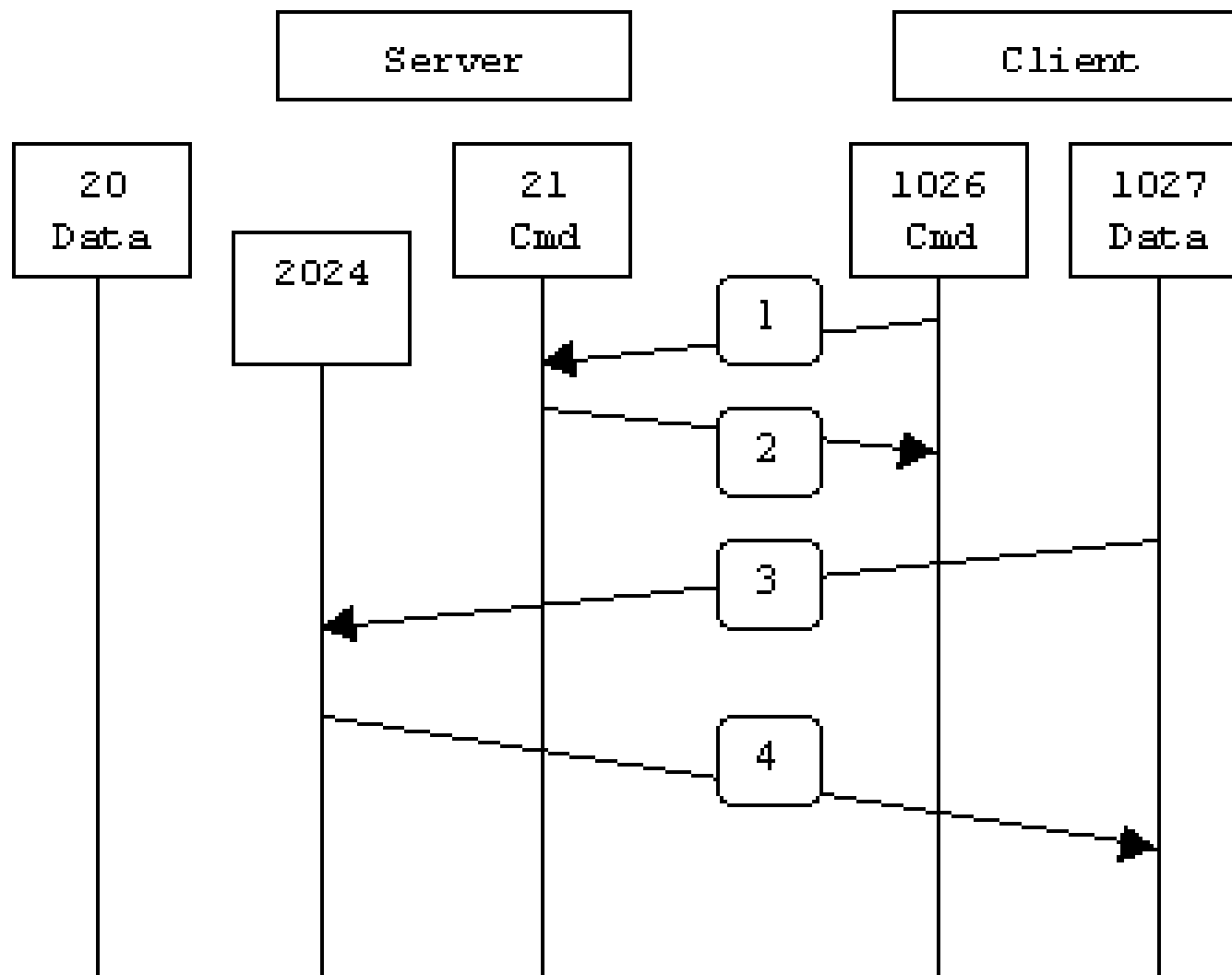
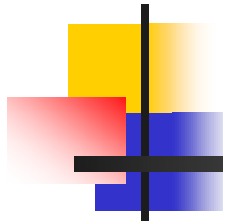
问题 1 FTP bounce attack from server

2 Firewall: step 3 is blocked （禁止主动连接）



Passive FTP 被动

- n To FTP server's port 21 from anywhere (Client initiates connection)
- n FTP server's port 21 to ports > 1024 (Server responds to client's control port)
- n To FTP server's ports > 1024 from anywhere (Client initiates data connection to random port specified by server)
- n FTP server's ports > 1024 to remote ports > 1024 (Server sends ACKs and data to client's data port)





Telnet服务

- n Telnet是TELecommunications NETwork的缩写，其名字具有双重含义，既指应用也是指协议自身。
- n Telnet给用户提供了一种通过网络登录远程服务器的方式。命令行方式，高效
- n Telnet通过端口23工作。
- n 与FTP、POP类似，明文传输，不安全
- n SSH Secure Shell 建立在应用层和传输层基础上的安全协议



Web服务

- n Web服务是目前最常用的服务，使用HTTP协议，默认Web服务占用80端口
- n 在Windows平台下一般使用IIS（Internet Information Server）作为Web服务器。
- n UNIX/Linux apache, PHP等
- n 不安全，明文传输
- n HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer）



常用的网络服务端口

n 常用服务端口列表

端口	协议	服务
21	TCP	FTP服务
25	TCP	SMTP服务
53	TCP/UDP	DNS服务
80	TCP	Web服务
135	TCP	RPC服务
137	UDP	NetBIOS域名服务
138	UDP	NetBIOS数据报服务
139	TCP	NetBIOS会话服务
443	TCP	基于SSL的HTTP服务
445	TCP/UDP	Microsoft SMB服务
3389	TCP	Windows终端服务



NETBIOS 会话层/传输层协议

- n NETBIOS over TCP/IP(NBT) 在网络属性中可禁止该协议
- n UDP端口137 NETBIOS名称管理服务 + lmhosts文件 名称解析 IP \rightarrow NETBIOS名
- n NetBIOS名 16个字符=15个用户字符+0x20
唯一名 unique name 一对一通信
组名 group name 多机间通信



NETBIOS 会话层/传输层协议

- n TCP端口 139 会话层应用
 面向连接 可靠有序
 文件和打印共享
- n UDP端口 138 NETBIOS数据报
 无连接 不可靠 无序
 发送给单一NetBIOS名或广播到组名
 浏览网络邻居
- n 命令nbtstat -n



NETBIOS 会话层/传输层协议

- n 端口445 直接主机TCP (Direct Host TCP)

- n SMB (Server Message Block) MS设计

Windows 2k/xp SMB over TCP

通过修改注册表可禁止445端口监听

HKLM\System\CurrentControlSet\Services\NetBT\Parameters TransportBindName置空

Windows NT: SMB over NBT 137, 138 (UDP) and 139 (TCP).



NETBIOS 会话层/传输层协议

If the client has NBT enabled, it will always try to connect to the server at both port 139 and 445 simultaneously. If there is a response from port 445, it sends a RST to port 139, and continues its SMB session to port 445 only. If there is no response from port 445, it will continue its SMB session to port 139 only, if it gets a response from there. If there is no response from either of the ports, the session will fail completely.



SMB, NetBEUI & ISAKMP

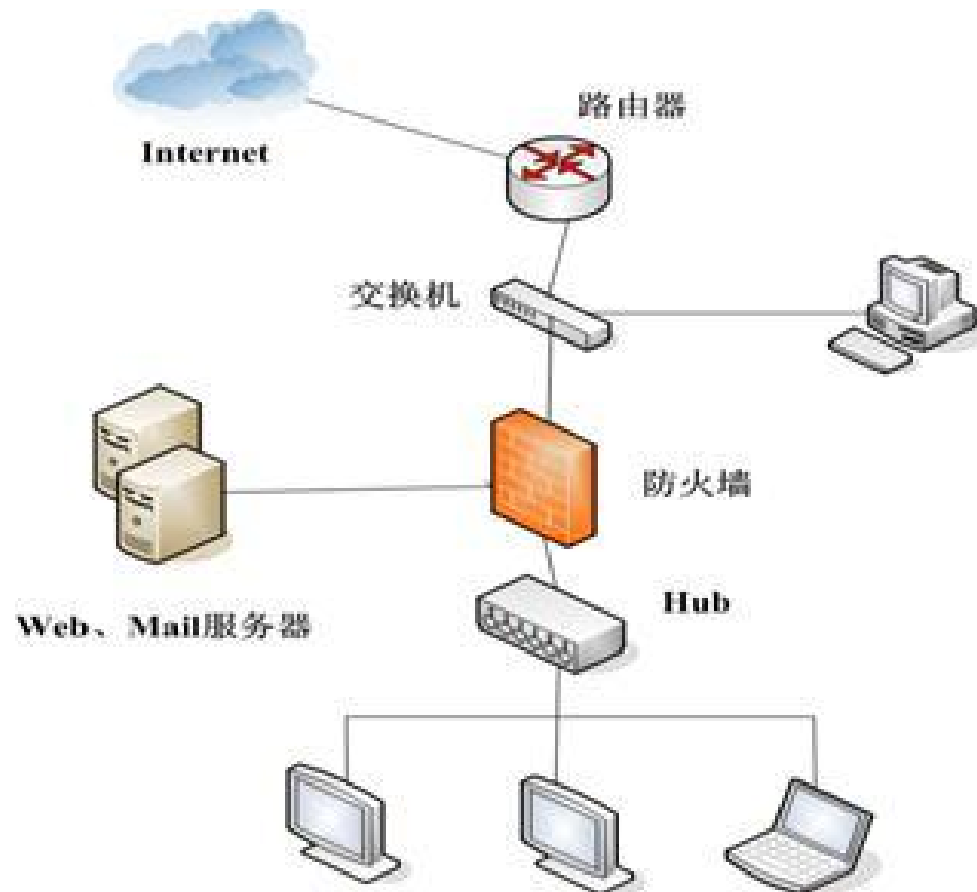
- n Samba – Unix/Linux与Windows互连 网络邻居 文件和打印共享
- n SMB 认证协议CIFS(Common Internet File System)
- n NetBIOS Extended User Interface(NetBEUI)
同一网段 无网络层 非路由
- n UDP 端口500 Internet Security Association and Key Management Protocol (ISAKMP)
IPSec 和VPN 使用



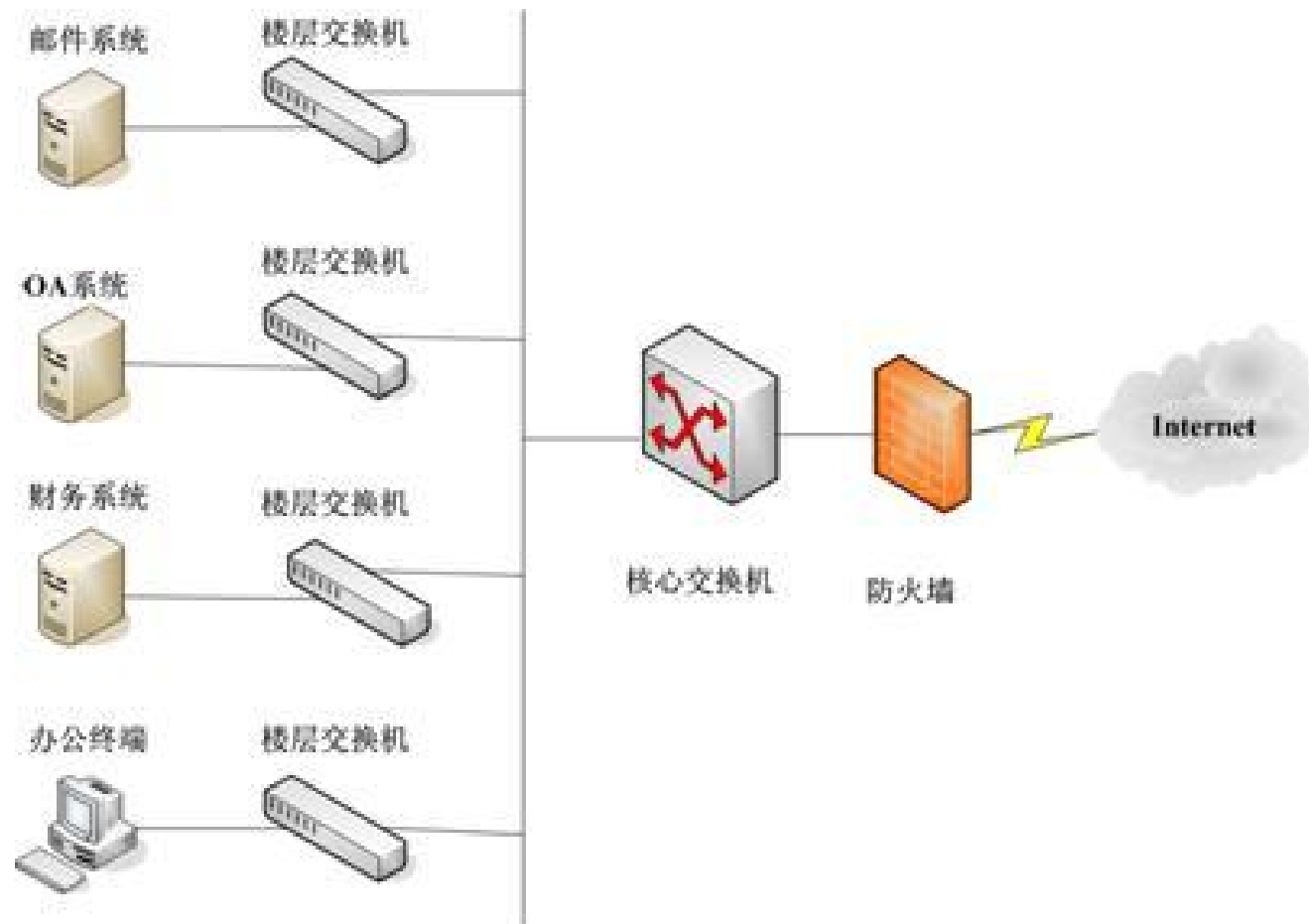
2.3局域网与广域网技术

- n 利用局域网技术，把地理位置分散的计算机有机地连接在一起，达到相互通信、共享硬件、软件和信息等资源的系统
- n 按局域网的规模分类，局域网分成小型局域网、中型局域网、大型局域网**3**类。

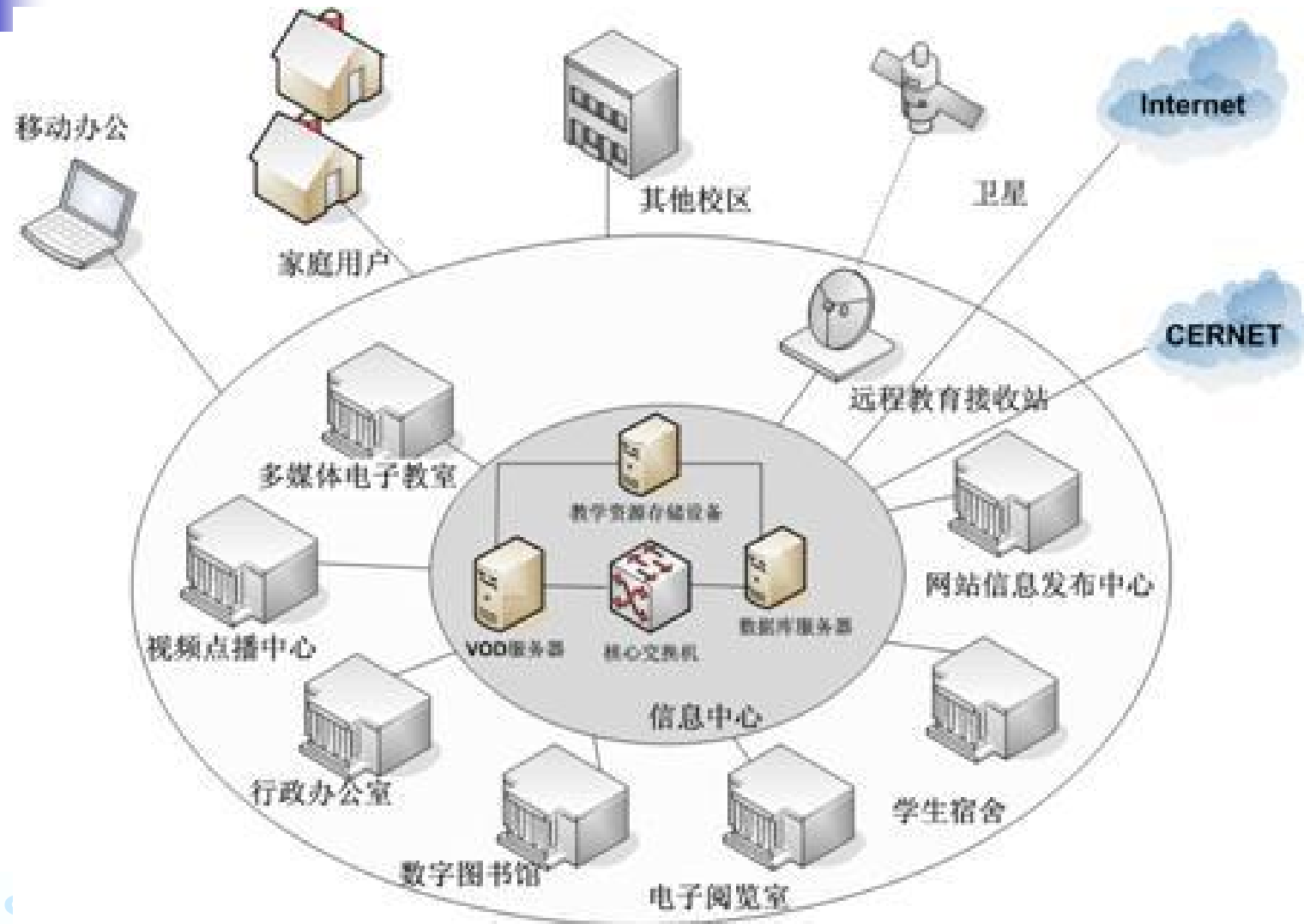
小型局域网



中型局域网



大型局域网(校园网、城域网)





局域网的特点及拓扑结构

1. 局域网地理范围一般在0.01km~20km之间;
2. 局域网是专用网。一般由一个部门专有, 不需要使用公共通信设施连网, 专线使得局域网具有较好的信道质量。
3. 局域网的数据传输率高, 误码率低;
4. 局域网使用共享信道技术, 具有独特的介质访问控制方式;
5. 局域网价格低廉, 组网容易, 使用方便

星型、总线型、树型、环型、不规则网状等多种类型。



IEEE 802模型 局域网的标准

IEEE 802模型的特点

- n 局域网种类繁多，使用的传输介质各种各样，接入方法也不相同，为此IEEE 802在数据链路层中专门划分出一个传输介质访问控制（MAC，Medium Access Control）子层来进行传输介质访问控制，并用逻辑链路控制（LLC，Logical Link Control）子层处理逻辑上的链路。
- n 局域网的拓扑结构比较简单，且多个站点共享传输信道，在任意两个节点之间只有惟一的一条链路，不需要进行路由选择和流量控制，因而它不需要定义网络层，只具备OSI/RM低两层的功能就可以了。由于考虑到局域网要互连，所以在LLC子层之上设置了网际层。
- n 其他高层功能往往与具体的实现有关，通常包含在网络操作系统中。
- n 物理层还是需要的，并且物理层往往也分为两个子层。

IEEE 802模型 局域网的标准





IEEE 802 标准系列

- n IEEE 802.1A, 概述和体系结构;
- n IEEE 802.1B, 寻址、网际互联及网络管理;
- n IEEE 802.2, LLC协议;
- n IEEE 802.3, CSMA/CD访问方法及物理层规范;
- n IEEE 802.4, 令牌传送总线访问方法及物理层规范;
- n IEEE 802.5, 令牌传送环访问方法及物理层规范;
- n IEEE 802.6, 城域网 (MAN) 标准;
- n IEEE 802.7, 宽带局域网标准;
- n IEEE 802.8, 光纤局域网标准;
- n IEEE 802.9, 综合数据/语音网络标准;
- n IEEE 802.10, 网络安全与保密标准;
- n IEEE 802.11, 无线局域网标准;
- n IEEE 802.12, 100BASE-VG标准;
- n
- n IEEE 802.14, 有线电视网 (CATV Broadband) 标准;
- n IEEE 802.15, 无线个人网络 (WPAN) 标准;
- n IEEE 802.16, 无线宽带局域网 (BBWA) 标准;

IEEE 802标准之间的关系



局域网的主要设备

终端设备

- 服务器
- 工作站
- 网络打印机和绘图仪

网络传输设备

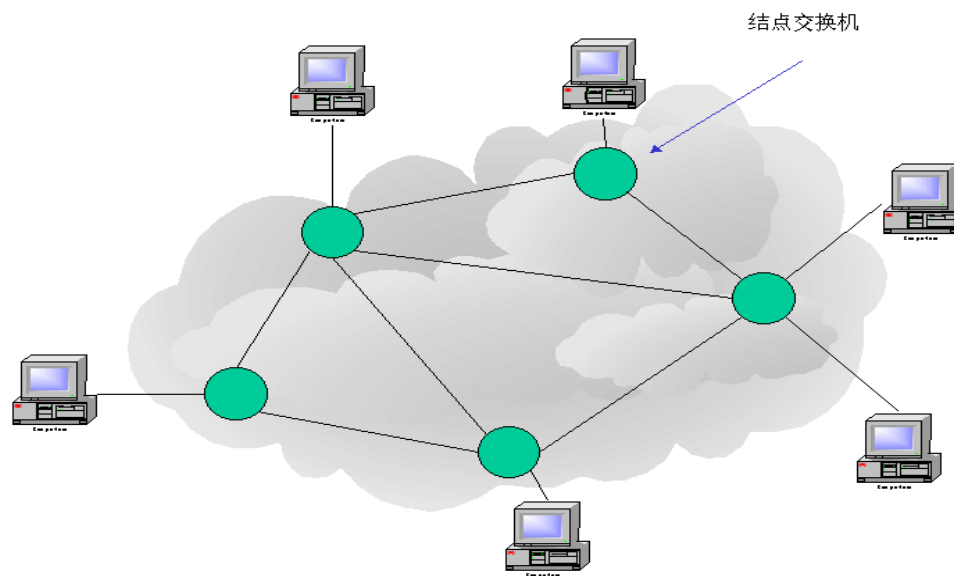
- 网卡
- 集线器
- 交换机
- 防火墙

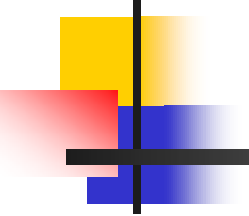
传输介质

- 双绞线
- 铜轴电缆
- 光纤
 - ①多模光纤
 - ②单模光纤

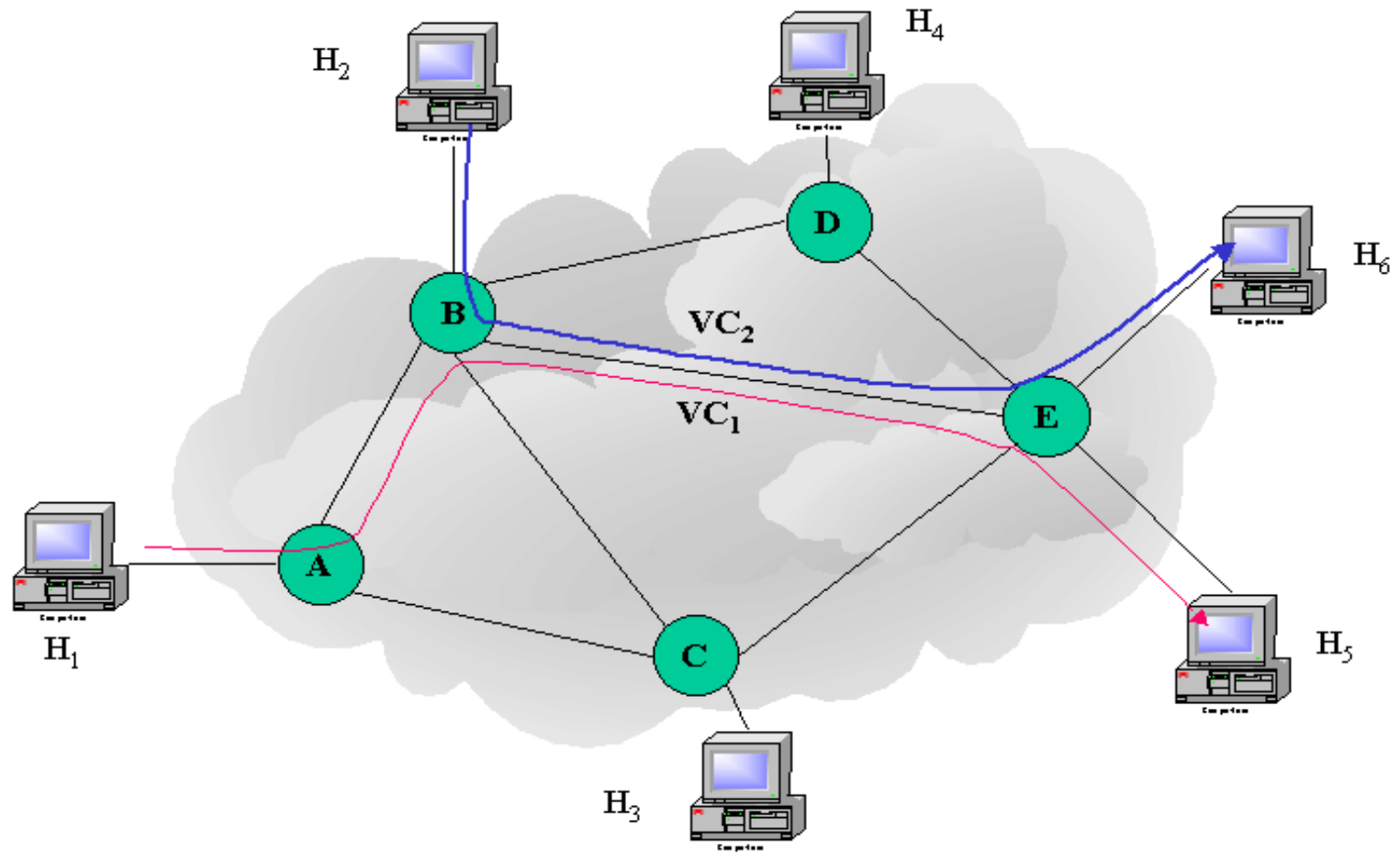
广域网的基本概念

- n 由相距较远的局域网或城域网互连而成，通常是除了计算机设备以外，还要涉及一些电信通讯方式
- n 与局域网区别之一在于需要向广域网服务提供商申请广域网服务
- n 对照OSI参考模型，广域网技术主要位于底层的3个层次，分别是物理层，数据链路层和网络层。



- 
- n 点对点链路 提供的是一条预先建立的从客户端经过运营商网络到达远端目标网络的广域网通信路径。
 - n 电路交换 通过运行商网络为每一次会话过程建立，维持和终止一条专用的物理电路。
 - n 包交换，网络设备可以共享一条点对点链路通过运营商网络在设备之间进行数据包的传递。包交换主要采用统计复用技术在多台设备之间实现电路共享。**ATM**，帧中继，**SMDS**以及**X.25**等都是采用包交换技术的广域网技术。
 - n 虚拟电路 一种逻辑电路，可以在两台网络设备之间实现可靠通信。虚拟电路有两种不同形式，分别是交换虚拟电路（**SVC**）和永久性虚拟电路（**PVC**）。

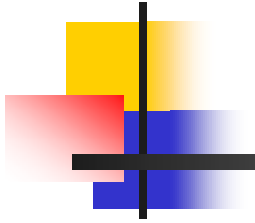
虚电路





广域网的技术

- n 利用电信服务商所提供的通信方式
 - n X.25 CCITT (ITU) 建议的一种协议，它定义终端和计算机到分组交换网络的连接。
 - n 帧中继
 - n ISDN 综合业务数字网 (Integrated Service Digital Network)，其最初的目标是综合语音和非语音服务。
 - n SMDS Switched Multimegabit Data Service (通过电话网实现) 交换式多兆位数据服务
 - n ATM 异步传输模式(Asynchronous Transfer Mode)，虚电路交换方式



- n xDSL 数字用户线路, Digital Subscriber Line
 - n ADSL = Asymmetrical Digital Subscriber Line
 - n SDSL = Symmetrical Digital Subscriber Line
- n DDN Digital Data Network
 - n 是利用数字信道传输数据信号的数据传输网
 - n 传输媒介有光缆、数字微波、卫星信道以及用户端可用的普通电缆和双绞线



广域网设备

- n 广域网交换机
- n 接入服务器
- n 调制解调器
- n 信道服务单元（**CSU**）/数据服务单元（**DSU**）
类似数据终端设备到数据通信设备的复用器
- n **ISDN**终端适配器是用来连接**ISDN**基本速率接口（**BRI**）到其它接口，从本质上说，**ISDN**终端适配器就相当于一台**ISDN**调制解调器。



小结

1. OSI/RM 以及TCP/IP协议分层模型
应用层、传输层、网络层、数据链路层
每层协议举例：ARP, ICMP, TCP, UDP, SMTP等
2. 主要协议数据单元的结构及字段含义
IP, TCP, UDP
3. TCP/IP协议简
4. 局域网/广域网技术