**网络协议的三个组成要素：**

语法：数据与控制信息的结构或格式 。

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。

同步：事件实现顺序的详细说明。

**物理层的主要任务** ：确定与传输媒体的接口的一些特性。

机械特性 ：指明接口所用接线器的形状和尺寸、引线数目和排列、固定和锁定装置等。

电气特性：指明在接口电缆的各条线上出现的电压的范围。

功能特性：指明某条线上出现的某一电平的电压的意义。

过程特性 ：指明对于不同功能的各种可能事件的出现顺序。

**单向通信**（单工通信）——只能有一个方向的通信而没有反方向的交互。

**双向交替通信**（半双工通信）——通信的双方都可以发送信息，但不能双方同时发送(当然也就不能同时接收)。

**双向同时通信**（全双工通信）——通信的双方可以同时发送和接收信息。

**信噪比(dB) = 10 log10(*S/N* ) (dB)**

**香农公式**  *C* = *W* log2(1+*S*/*N*) (bit/s) 其中：*W* 为信道的带宽（以 Hz 为单位）；*S* 为信道内所传信号的平均功率；*N* 为信道内部的高斯噪声功率。

**编码方式**：不归零制：正电平代表 1负电平代表 0。 归零制：正脉冲代表 1负脉冲代表 0。

曼彻斯特编码：位周期中心的向上跳变代表 0，位周期中心的向下跳变代表 1。但也可反过来定义。

差分曼彻斯特编码：在每一位的中心处始终都有跳变。位开始边界有跳变代表 0，而位开始边界没有跳变代表 1。

**导引型传输媒体** 双绞线 屏蔽双绞线 STP 无屏蔽双绞线 UTP 同轴电缆 光缆

**光纤** 多模光纤 光源发光二极管可以存在多条不同角度入射的光线在一条光纤中传输。

单模光纤 光源 半导体激光

**非导引型传输媒体**  地面微波接力通信 卫星通信

**信道复用技术** 频分复用 时分复用 统计时分复用 波分复用 码分复用

**数据链路层使用的信道** 点对点信道 广播信道

**数据链路层协议三个基本问题：**封装成帧 透明传输 差错检测

**冗余码的计算举例 CRC P75 生成多项式**

**PPP 协议有三个组成部分：**一个将 IP 数据报封装到串行链路的方法。

链路控制协议 LCP (Link Control Protocol)。网络控制协议 NCP (Network Control Protoco**l**

**CSMA/CD 协议工作流程：** 多点接入 载波监听 碰撞检测

**凡长度小于 64 字节的帧都是由于冲突而异常中止的无效帧。**

**PPP 协议的帧格式**PPP 帧的首部和尾部分别为 4 个字段和 2 个字段。P79图3-10

**局域网最主要的特点是：**

1网络为一个单位所拥有；2地理范围和站点数目均有限。

**局域网具有如下主要优点：**

具有广播功能，从一个站点可很方便地访问全网。局域网上的主机可共享连接在局域网上的各种硬件和软件资源。

便于系统的扩展和逐渐地演变，各设备的位置可灵活调整和改变。

提高了系统的可靠性、可用性和残存性。

网络接口板又称为通信适配器 (adapter) 或网络接口卡 NIC (Network Interface Card)，或“网卡”。

**虚拟局域网**

其实只是局域网给用户提供的一种服务，而并不是一种新型局域网。

虚拟局域网 VLAN 是由一些局域网网段构成的与物理位置无关的逻辑组，而这些网段具有某些共同的需求。

每一个 VLAN 的帧都有一个明确的标识符，指明发送这个帧的计算机是属于哪一个 VLAN。

**互联网的网络设计思路：**网络层向上只提供简单灵活的、无连接的、尽最大努力交付的数据报服务。

**虚电路服务与数据报服务的对比 P115**

**网际协议 IP 是 TCP/IP 体系中两个最主要的协议之一。**

**与 IP 协议配套使用的还有三个协议：**

**地址解析协议 ARP (Address Resolution Protocol)**

**网际控制报文协议 ICMP (Internet Control Message Protocol)**

**网际组管理协议 IGMP (Internet Group Management Protocol)**

**硬件地址**（或物理地址）是数据链路层和物理层使用的地址。

**IP 地址**是网络层和以上各层使用的地址，是一种逻辑地址（称 IP 地址是逻辑地址是因为 IP 地址是用软件实现的）。

**ARP 作用：**

从网络层使用的 IP 地址，解析出在数据链路层使用的硬件地址。ARP 用于解决同一个局域网上的主机或路由器的 IP 地址和硬件地址的映射问题。P126 图4-11

**ICMP 询问报文有两种**

回送请求和回答报文 时间戳请求和回答报文

**ICMP 的应用举例**

PING 用来测试两个主机之间的连通性。

Traceroute 的应用举例用来跟踪一个分组从源点到终点的路径。

**内部网关协议 IGP (Interior Gateway Protocol)**

在一个自治系统内部使用的路由选择协议。目前这类路由选择协议使用得最多，如 RIP 和 OSPF 协议。

**外部网关协议 EGP (External Gateway Protocol)**

若源站和目的站处在不同的自治系统中，当数据报传到一个自治系统的边界时，就需要使用一种协议将路由选择信息传递到另一个自治系统中。这样的协议就是外部网关协议 EGP。

在外部网关协议中目前使用最多的是 BGP-4。

**RIP 协议的三个特点**

仅和相邻路由器交换信息。

交换的信息是当前本路由器所知道的全部信息，即自己的路由表。

按固定的时间间隔交换路由信息，例如，每隔 30 秒。当网络拓扑发生变化时，路由器也及时向相邻路由器通告拓扑变化后的路由信息。

**网络地址转换 NAT** 需要在专用网连接到互联网的路由器上安装 NAT 软件。装有 NAT 软件的路由器叫做 NAT路由器，它至少有一个有效的外部全球IP地址。

所有使用本地地址的主机在和外界通信时，都要在 NAT 路由器上将其本地地址转换成全球 IP 地址，才能和互联网连接。

**TCP/IP 的运输层有两个主要协议：**

用户数据报协议 UDP (User Datagram Protocol)

传输控制协议 TCP (Transmission Control Protocol)

P207 熟知端口号5-2 P205图5-2

**UDP 的主要特点**

1. UDP 是无连接的 2. UDP 使用尽最大努力交付 3. UDP 面向报文 4. UDP 没有拥塞控制5.UDP 支持一对一、一对多、多对一和多对多的交互通信 6.UDP 的首部开销小

**TCP的主要特点**

TCP 是面向连接的运输层协议 每一条 TCP 连接只能是点对点的（一对一）。

TCP 提供可靠交付的服务。 TCP 提供全双工通信。 面向字节流

**TCP传输效率**

第一种机制是 TCP 维持一个变量，它等于最大报文段长度 MSS。只要缓存中存放的数据达到 MSS 字节时，就组装成一个 TCP 报文段发送出去。

第二种机制是由发送方的应用进程指明要求发送报文段，即 TCP 支持的推送 (push) 操作。

第三种机制是发送方的一个计时器期限到了，这时就把当前已有的缓存数据装入报文段（但长度不能超过 MSS）发送出去。

**万维网 WWW (World Wide Web)** 并非某种特殊的计算机网络。

万维网是一个大规模的、联机式的信息储藏所。

**统一资源定位符 URL的格式**

URL 给资源的位置提供一种抽象的识别方法，并用这种方法给资源定位。

URL 相当于一个文件名在网络范围的扩展。因此 URL 是与互联网相连的机器上的任何可访问对象的一个指针。

**SMTP的主要特点**

SMTP 规定了在两个相互通信的 SMTP 进程交换信息的方法。

SMTP 使用客户–服务器方式。

SMTP 基于 TCP 实现客户与服务器的通信。

**网络管理协议 SNMP**

简单网络管理协议 SNMP (Simple Network Management Protocol) 中的管理程序和代理程序按客户–服务器方式工作。

管理程序运行 SNMP 客户程序，向某个代理程序发出请求（或命令），代理程序运行 SNMP 服务器程序，返回响应（或执行某个动作）。

在网管系统中，往往是一个（或少数几个）客户程序与很多的服务器程序进行交互。

**互联网提供的音频/视频服务类型**

流式 (streaming) 存储音频/视频 ——边下载边播放。

流式实况音频/视频 ——边录制边发送 。

交互式音频/视频 ——实时交互式通信。

第五章传输层的TCP/UDP的特点，三次握手，四次挥手，流量控制，拥塞控制，滑动窗口。

第七章主动攻击，被动攻击，两个密码体制特点和优缺点，数字签名，中间人攻击，防火墙，入侵检测系统。

**被动攻击：**被动攻击是指攻击者从网上窃听他人的通信内容。通常把这类攻击成为截获。

**主动攻击方式：**篡改 恶意程序 拒绝服务

**两类密码体制：**对称密钥密码体制和公钥密码体制

**对称密钥密码体制：**加密密钥与解密密钥时使用相同的密码体制。

**公钥密码体制：**使用不同的加密密钥与解密密钥。

**数字签名：**接收者能够核实发送者对报文的签名，即报文鉴别。

接收者确信所受到的数据和发送者发送的完全一样而没有被纂改过，即报文的完整性。

发送者到时候不能抵赖来对报文的签名，即不可否认。

**防火墙**技术是通过有机结合各类用于安全管理与筛选的软件和硬件设备，帮助计算机网络于其内、外网之间构建一道相对隔绝的保护屏障，以保护用户资料与信息安全性的一种技术。

**入侵检测系统**（简称“IDS”）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备，是一种积极主动的安全防护技术。