

## 一．绪论

### 1. 计算机网络：

提供的两个功能：**连通性和共享**

### 2. 因特网概述

### 3. 互联网组成

**边缘部分**：有所有连接在因特网上的主机组成。这部分由用户直接使用，用来进行通信和资源共享。

**核心部分**：由大量的网络和连接这些网络的路由器组成。这部分是为边缘部分提供服务的（提供连通性和交换）。

#### **核心部分的交换技术**

电路交换的三个阶段：建立连接——通话——释放连接

在通话时，两用户之间占用端到端的资源，而由于绝大部分时间线路都是空闲的，所以线路的传输速率往往很低。

分组交换 的组成：报文、首部、分组。采用存储转发技术，即收到分组——存储分组——查询路由（路由选择协议）——转发分组。优点：高效、灵活、迅速、可靠。缺点：时延、开销。关键构件：路由器。

报文交换 整个报文传送到相邻结点，全部存储下来之后查询转发表，转发到下一个结点。

### 4. 计算机网络的类别

### 5. 计算机网络的体系结构

#### **网络协议的三要素**

- 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

#### **五层协议的体系结构**

- 物理层：物理层的任务就是**透明地传送比特流**。（注意：传递信息的物理媒体，如双绞线、同轴电缆、光缆等，是在物理层的下面，当做第 0 层。）物理层还要确定连接电缆插头的定义及连接法。
- 数据链路层：**将网络层交下来的 IP 数据报组装成帧**，在两个相邻结点间的链路上“透明”的传送以帧为单位的数据。每一帧包括**数据和必要的控制信息**。在收到数据时，控制信息使收到端直到哪个帧从哪个比特开始和结束。
- 网络层：**选择合适的路由**，使发送站的运输层所传下来的**分组**能够正确无误地**按照地址找到目的站**，并**交付给目的站的运输层**。网络层将运输层产生的报文或用户数据报封装成**分组（IP 数据报）或包**进行传送。
- 运输层：向上一层的进行通信的两个进程之间提供一个可靠的**端对端服务**，使它们看不见运输层以下的数据通信的细节。（TCP、UDP）
- 应用层：直接为用户的应用进程提供服务（HTTP、FTP 等）

OSI 体系结构：物理层、数据链路层、网络层、运输层、会话层、表示层、应用层

TCP/IP 体系结构：网络接口层、网际层 IP、运输层、应用层

## 二．物理层

### 1.导向传输媒体

#### 1.1. 双绞线

双绞线已成为局域网中的主流传输媒体

- 屏蔽双绞线 STP (Shielded Twisted Pair)
- 无屏蔽双绞线 UTP (Unshielded Twisted Pair)

#### 1.2. 同轴电缆

- 细缆（适合短距离，安装容易，造价低）
- 粗缆（适合较大局域网，布线距离长，可靠性好）

#### 1.3. 光纤

光纤有很好的抗电磁干扰特性和很宽的频带，主要用在环形网中

- 多模光纤（用发光二极管，便宜，定向性较差）
- 单模光纤（注入激光二极管，定向性好）

### 2.非导向传输媒体

微波、红外线、激光、卫星通信

通信方式：

- 单向通信（单工）
- 双向交替通信（半双工）
- 双向同时通信（全双工）

## 三．数据链路层

数据链路层使用的信道有两种类型：点对点信道，广播信道

使用点对点信道的数据链路层：

链路：从一个结点到相邻结点的一段物理线路

数据链路：把实现这些协议的硬件和软件加载链路上，现在最常用的方法是使用适配器（即网卡）来实现这些协议的硬件和软件。一般的适配器都包括了数据链路层和物理层这两层的功能。

### 封装成帧

就是在一段数据的前后分别添加首部（帧开始符 SOH 01）和尾部（帧结束符 EOT 04），然后就构成了一个帧。（数据部分≤长度限制 MTU）首部和尾部的一个重要作用就是进行帧定界。帧定界是分组交换的必然要求

### 透明传输

为了达到透明传输（即传输的数据部分不会因为包含 SOH 和 EOT 而出错），在数据中出现控制字符“SOH”或“EOT”的前面插入一个转义字符“ESC”（十六进制 1B），透明传输避免消息符号与帧定界符号相混淆

### 差错检测

现实通信链路中比特在传输中会产生差错，传输错误的比特占比称为误码率 BER，为了保证可靠性，通常通过循环冗余检验 CRC 来做差错检测。差错检测防止无效数据帧浪费后续路由上的传输和处理资源

## 点对点协议：PPP

PPP 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 Protocol)

透明传输的实现方法：

### 1. 字节填充——PPP 使用异步传输

当 PPP 用在异步传输时，就使用一种特殊的字符填充法：将每一个 0x7E 字节变为 (0x7D, 0x5E)，0x7D 转变成为 (0x7D, 0x5D)。ASCII 码的控制字符（即数值小于 0x20 的字符），则在前面要加入 0x7D，同时将该字符的编码加以改变。

### 2. 零比特填充——PPP 使用同步传输

只要发现有 5 个连续的 1，则立即填入一个 0

PPP 协议的工作状态：

链路静止-建立物理层-链路建立-pc 发 LCP-NCP 分配 IP 地址-链路打开，网络层建立。  
(释放时倒过来)

## 使用广播通信的数据链路层

广播信道是一种一对多的通信，局域网使用的就是广播信道

以太网采用 CSMA/CD 协议的方式来协调总线上各计算机的工作。在使用 CSMA/CD 协议的时候，一个站不可能同时进行发送和接收。

## 以太网的 MAC 层

“MAC 地址”又叫做硬件地址或物理地址，实际上就是适配器地址或适配器标识符 EUI-48。高位 24 位：厂家，低位 24 位由厂家自行指派

以太网 V2 的 MAC 帧较为简单，有五个字段组成。

前两个字段分别为 6 字长的目标地址和源地址字段。第三个字段是 2 字节的类型字段，用来标志上一层使用的是什么协议，以便把收到的 MAC 帧的数据上交给上一层的这个协议。后面数据字段 46~1500 字节，FCS 字段 4 个字节。

## 四．网络层

### 网际协议 IP

配套的其他协议：

1. 地址解析协议 ARP：是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。
2. 逆地址解析协议 RARP：是解决同一个局域网上的主机或路由器的硬件地址和 IP 地址的映射问题。
3. 网际控制报文协议 ICMP：提供差错报告和询问报文，以提高 IP 数据交付成功的机会
4. 网际组管理协议 IGMP：用于探寻、转发本局域网内的组成员关系。

### IP 地址：

每一类地址都由 **网络号 net-id** 和 **主机号 host-id** 组成

A 类：地址范围 1.0.0.0 到 126.255.255.255

B 类：地址范围 128.0.0.0-191.255.255.255

C 类：地址范围 192.0.0.0-223.255.255.255

**硬件地址**是数据链路层和物理层使用的地址

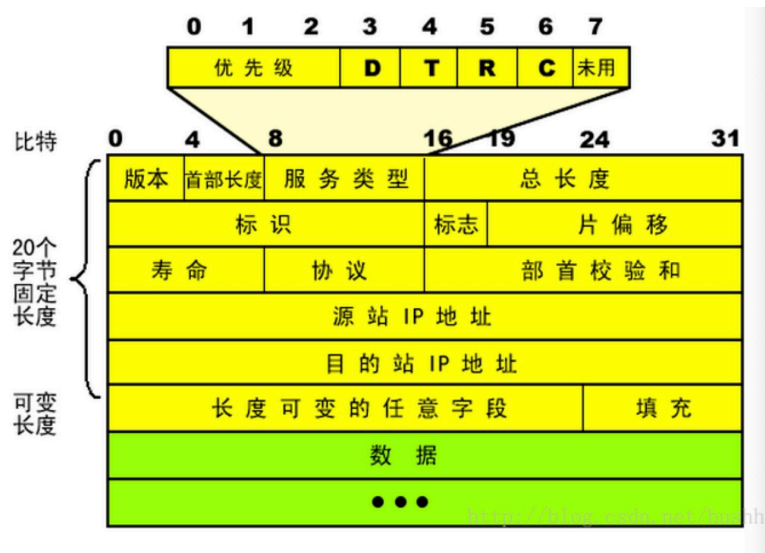
**IP 地址**是网络层和以上各层使用的地址，是一种逻辑地址

### ARP：

ARP 是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。

### IP 数据报：

一个 IP 数据报由首部（20 字节+可选字段）和数据两部分组成



### 网际控制报文协议 ICMP

种类

- ICMP 差错报告报文
- ICMP 询问报文

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

### 路由选择协议

- 内部网关协议 IGP：一个自治系统内部使用的路由选择协议。有多种协议，如 RIP 和 OSPF 协议。
- 外部网关协议 EGP：一个自治系统的边界，将路由选择信息传递到另一个自治系统中。目前使用的就是 BGP

## 五．运输层

功能：

- 运输层为应用进程之间提供端到端的逻辑通信(但网络层是为主机之间提供逻辑通信)
- 运输层还要对收到的报文进行差错检测
- 运输层需要有两种不同的运输协议，即面向连接的 TCP 和无连接的 UDP

协议：

UDP, TCP

端口：

一些常用的数值端口号：

FTP 21

TELNET 23

SMTP 25

DNS 53

TFTP 69

HTTP 80

SNMP 161

SNMP(trap) 162

UDP：

- UDP 是无连接的，即发送数据之前不需要建立连接。
- UDP 使用尽最大努力交付，即不保证可靠交付，同时也不使用拥塞控制
- UDP 是面向报文的
- UDP 没有拥塞控制，很适合多媒体通信的要求。
- UDP 支持一对一、一对多、多对一和多对多的交互通信
- UDP 的首部开销小，只有 8 个字节

UDP Header																																	
Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Length																<a href="https://Checksum.sdn.net/u014711094">https://Checksum.sdn.net/u014711094</a>															

TCP：

- TCP 是面向连接的运输层协议
- 每一条 TCP 连接只能有两个端点(endpoint)，每一条 TCP 连接只能是点对点的
- TCP 提供可靠交付的服务
- TCP 提供全双工通信
- 面向字节流

TCP 要经过三次握手建立连接，四次挥手断开连接。

源 端 口				目 的 端 口							
序 号											
确认序号											
TCP 首部长		保留		URG	ACK	PSH	RST	SYN	FIN	窗 口	
检 验 和						紧 急 指 针					
可选项											
数据											

## 六．会话层

会话层不参与具体的传输，它提供包括访问验证和会话管理在内的建立和维护应用之间通信的机制。如服务器验证用户登录便是由会话层完成的。

## 七．表示层

提供格式化的表示和转换数据服务。数据的压缩和解压缩，加密和解密等工作都由表示层负责。例如图像格式的显示，就是由位于表示层的协议来支持。

## 八．应用层

**DHCP**: 动态主机配置协议 DHCP：负责给互联网上的计算机提供动态的 IP 地址

## 九．面试题

### 1. tcp 和 udp 的区别？

- TCP 面向连接，UDP 面向非连接即发送数据前不需要建立链接
- TCP 提供可靠的服务（数据传输），UDP 无法保证
- TCP 面向字节流，UDP 面向报文
- TCP 数据传输慢，UDP 数据传输快

### 2. 常见的端口及其服务

FTP 21

TELNET 23

SMTP 25

DNS 53

TFTP 69

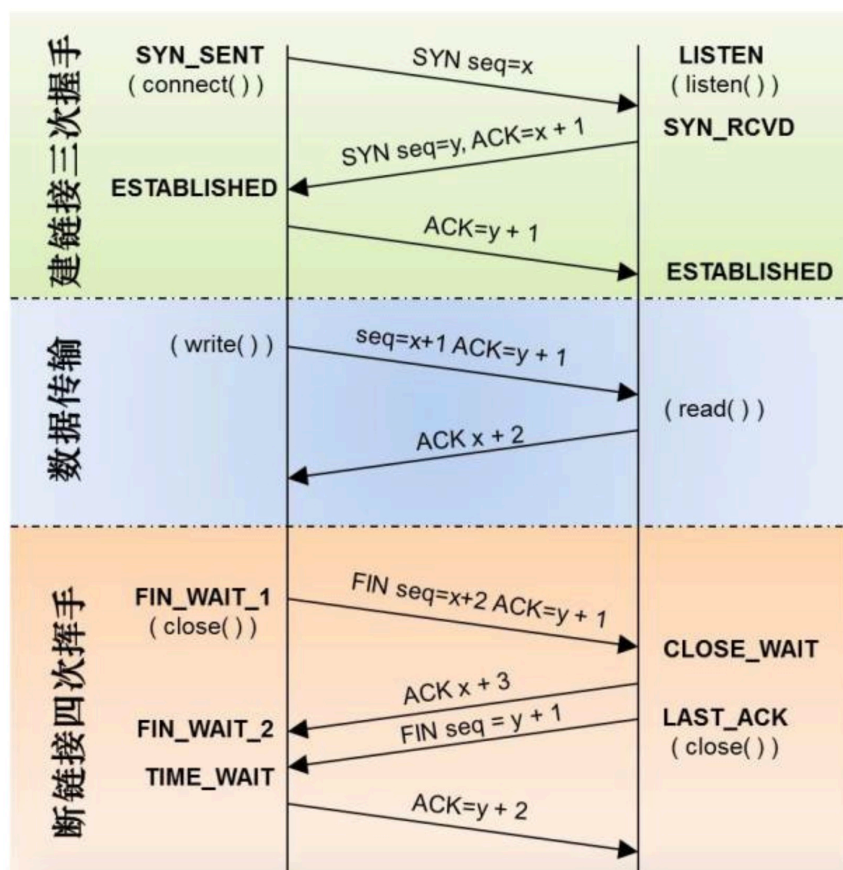
HTTP 80

SNMP 161

SNMP(trap) 162

### 3.简述 TCP3 次握手

三次握手的目的是同步连接双方的序列号和确认号并交换 TCP 窗口大小信息。



#### 4. 有哪些私有保留地址

- A类：10.0.0.0 - 10.255.255.255
- B类：172.16.0.0 - 172.31.255.255
- C类：192.168.0.0 - 192.168.255.255

#### 5. IP 地址分类

IPv4地址共有32bit				
	网络号	地址范围	网络号	主机号
A类	以0开头	1. 0. 0. 0 - 127. 255. 255. 255	8位	24位
B类	以10开头	128. 0. 0. 0 - 255. 255. 255	16位	16位
C类	以110开头	192. 0. 0. 0-223. 255. 255. 255	24位	8位
D类	前四位固定为 1110，后面为多播地址 所以D类地址为多播地址			
E类	前五位固定为 11110，后面保留为今后所用			



## 6. 在浏览器中输入网址之后执行会发生什么？

- 1、客户端浏览器通过DNS解析到http://www.baidu.com的IP地址220.181.27.48，通过这个IP地址找到客户端到服务器的路径。客户端浏览器发起一个HTTP会话到220.161.27.48，然后通过TCP进行封装数据包，输入到网络层。
- 2、在客户端的传输层，把HTTP会话请求分成报文段，添加源和目的端口，如服务器使用80端口监听客户端的请求，客户端由系统随机选择一个端口如5000，与服务器进行交换，服务器把相应的请求返回给客户端的5000端口。然后使用IP层的IP地址查找目的端。
- 3、客户端的网络层不用关系应用层或者传输层的东西，主要做的是通过查找路由表确定如何到达服务器，期间可能经过多个路由器，这些都是由路由器来完成的工作，我不作过多的描述，无非就是通过查找路由表决定通过那个路径到达服务器。
- 4、客户端的链路层，包通过链路层发送到路由器，通过邻居协议查找给定IP地址的MAC地址，然后发送ARP请求查找目的地址，如果得到回应后就可以使用ARP的请求应答交换的IP数据包现在就可以传输了，然后发送IP数据包到达服务器的地址。

## 7.ARP 协议的工作过程

- ( 1 ) 首先，每个主机都会在自己的 ARP 缓冲区中建立一个 ARP 列表，以表示 IP 地址和 MAC 地址之间的对应关系。
- ( 2 ) 当源主机要发送数据时，首先检查 ARP 列表中是否有对应 IP 地址的目的主机的 MAC 地址，如果有，则直接发送数据，如果没有，就向本网段的所有主机发送 ARP 数据包，该数据包包括的内容有：源主机 IP 地址，源主机 MAC 地址，目的主机的 IP 地址。
- ( 3 ) 当本网络的所有主机收到该 ARP 数据包时，首先检查数据包中的 IP 地址是否是自己的 IP 地址，如果不是，则忽略该数据包，如果是，则首先从数据包中取出源主机的 IP 和 MAC 地址写入到 ARP 列表中，如果已经存在，则覆盖，然后将自己的 MAC 地址写入 ARP 响应包中，告诉源主机自己是它想要找的 MAC 地址。
- ( 4 ) 源主机收到 ARP 响应包后。将目的主机的 IP 和 MAC 地址写入 ARP 列表，并利用此信息发送数据。如果源主机一直没有收到 ARP 响应数据包，表示 ARP 查询失败。