这里将总结计算机网络所有内容。这里以小明访问www.baidu.com为例讲述计算机间通信的所有过程。

DHCP、UDP、IP

小明启动他的电脑A，他的电脑通过一根以太网网线连接到学校的以太网交换机B，交换机又与学校的路由器C。学校有自己的DNS服务器D，同时假定DHCP服务器在路由器C中。小明首先将电脑A与网络连接时，没有IP地址，因此小明的电脑A需要通过DHCP协议获取IP地址以及其它信息。

1. 电脑A上的操作系统，生成一个DHCP请求报文，并将这个报文包装成一个UDP报文段，该UDP报文段的目的端口67（DHCP服务器），源端口68（DHCP客户端）。该UDP报文段则被包装成IP数据包，目的IP为一个广播IP（255.255.255.255），源IP为0.0.0.0。
2. 包含DHCP请求的IP数据包被放置在以太网帧中，该以太网帧的目的MAC为FF:FF:FF:FF:FF:FF。该帧将广播到与交换机相连的所有设备，该帧的源MAC是主机A的MAC。
3. 这个数据帧首先由交换机B收到，交换机B在所有的出口端广播这个数据帧，包括连接到路由器C的端口。路由器收到数据帧后，将记录主机A的MAC地址和对应的出口端。
4. 路由器接C收到该以太网帧，解析出其中的IP数据包，然后再解析出其中的UDP报文段，最后向上分解成DHCP报文，此时DHCP服务器获得了DHCP请求报文。
5. DHCP服务器C分配一个IP地址该主机A，生成一个包含这个IP地址和DNS服务器IP地址的DHCP ACK 报文，这个DHCP ACK报文从上往下，依次包装成UDP报文段，IP数据包，以太网帧。这个以太网帧的目的MAC是主机A的MAC，源MAC地址是服务器C的MAC地址。
6. 这个以太网帧，由路由器C发送给交换机B，交换机在3中已经学习到以太网帧目的MAC地址的出口，故该以太网帧仅被发送给主机A的出口端。同时，交换机也将学习到路由器C的MAC地址及其出口端。
7. 主机A接收到包含DHCP ACK的以太网帧，从该以太网帧中，从下往上，依次抽取IP数据包，UDP报文，DHCP报文。主机A记录下它的IP地址和DNS服务器的IP地址。同时在它的IP转发表中保存默认网关的地址。主机A已经准备好了它的网络组件，可以访问互联网了。

DNS和ARP

小明将[www.baidu.com](http://www.baidu.com) 的url输入到浏览器地址栏中时，启动了一系列的过程，最终使得百度页面出现在浏览器中。要访问[www.baidu.com](http://www.baidu.com)，首先要直到其该网址所在服务器E的IP地址，这是通过DNS协议来完成的。

1. 首先，主机A在本机的DNS缓存中查询，即在hosts文件中查找是否有[www.baidu.com](http://www.baidu.com的IP) 的IP地址映射。若本地DNS缓存中没有，则主机A的操作系统产生一个DNS查询报文，将字符串[www.baidu.com](http://www.baidu.com)放入该报文中，该报文将包装到目的端口为53号（DNS服务器端口）的UDP报文段中，UDP报文被包装成一个IP数据包，该数据包的目的IP地址为本地DNS服务器D的IP地址，源地址为主机A的IP地址。
2. 该IP数据包被封装成以太网帧，该帧将发送到小明学校的网关路由器C中。主机A不知道网关路由器C的MAC地址，为了获得C的MAC地址，需要使用ARP协议。
3. 主机A生成一个目的IP地址为C的IP地址的ARP查询报文，该ARP查询报文被包装到一个具有广播目的地址（FF:FF:FF:FF:FF:FF）的以太网帧中，并向交换机发送以太网帧，交换机接收到该以太网帧后，将广播到所有连接的设备，包括路由器C。
4. 路由器C接收到包含ARP查询报文的以太网帧，发现APR报文的目的IP地址和自己的IP地址匹配。因此，网关路由器生成一个ARP响应报文，包含C的MAC地址和C的IP地址。该ARP报文将装入到一个以太网帧中，其目的MAC为主机A的MAC地址，并将该以太网帧发送给交换机，交换机将帧交付给主机A。
5. 主机A接收到ARP响应报文，从中抽取并保存路由器C的MAC地址。
6. 主机A现在可以将包含DNS查询请求的IP数据包封装成以太网帧，该以太网帧的目的MAC为路由器C的MAC地址。

路由和DNS服务器

1. 网关路由器C抽取以太网帧中的IP数据包，发现该IP数据包的目的IP地址不是自己的IP地址。于是，路由器C查询自己的路由表和根据路由协议（如：RIP、OSPF、BGP），将该IP数据包封装成新的以太网帧后，从对应的出口发出。
2. 该IP数据包通过若干路由器的转发，转发到DNS服务器D。
3. DNS服务器D收到该以太网帧，抽取其中的IP数据包，发现该IP数据包的目的IP地址和自己的IP地址相同，于是抽取其中的DNS请求报文，在自己的数据库中查询包含[www.baidu.com](http://www.baidu.com)的记录，找到对应的DNS源记录。该DNS服务器生成一个DNS响应报文，该DNS回答报文放入UDP数据报中，最终发送给主机A。
4. 主机A收到DNS响应报文，从中抽取出[www.baidu.com](http://www.baidu.com服务器E的IP) 服务器E的IP地址，此时小明可以通过这个IP地址访问[www.baidu.com](http://www.baidu.com服务器E的IP)服务器E。

TCP协议和HTTP协议

1. 主机A有了服务器E的IP地址，可以生成TCP套接字，首先必须与服务器E进行三次握手。主机A生成一个TCP SYN报文段，其目的端口为80（HTTP），目的IP为服务器E的IP地址，然后封装成IP数据包，发送给网关路由器C。
2. 网关路由器通过路由表和路由协议，将IP数据包通过多次转发，最终发送给服务器E。
3. TCP SYN报文到达服务器E，服务器E也生成一个TCP套接字，产生一个TCP SYNACK报文段，发送给主机A。
4. 主机A接收到TCP SYNACK报文段后，最终可以开始访问[www.baidu.com](http://www.baidu.com)网址了。小明的电脑A的浏览器生成包含要获取的URL的HTTP GET报文。HTTP GET报文则写入到套接字中，该报文为TCP报文段的数据，这个报文将发送给服务器E。
5. 服务器E获得TCP报文，读取HTTP GET报文，生成一个HTTP响应报文，将请求的网页内容放入到HTTP响应的文本中，并将报文发送到TCP套接字中。
6. 包含HTTP响应报文的数据报，最终通过各种路由器转发到小明的电脑A中，电脑A读取套接字中的HTTP响应，并从中获取HTML，最终显示了整个百度网页。

ARP协议：IP地址解析获得MAC地址，局域网内的协议

主机A的IP地址为192.168.1.1，MAC地址为0A-11-22-33-44-01；

主机B的IP地址为192.168.1.2，MAC地址为0A-11-22-33-44-02；

主机A要与主机B通信时：

第1步：主机A在本地ARP中，检查主机B的匹配MAC地址

第2步：没有找到主机B的ARP，则它将询问192.168.1.2的地址，将ARP请求帧广播到本地所有主机。源主机的IP地址和MAC地址都再ARP请求中。本地网络中的每台主机都将接受到ARP请求，并且检查是否与自己的IP地址匹配。如果不匹配，则它丢弃该请求包。

第3步：主机B接受到ARP请求后，将主机A的IP地址和MAC地址映射写到本地ARP缓存中

第4步：主机B将包含其MAC地址的ARP回复消息直接发送会主机A。

ARP攻击：

简单的诈骗攻击，伪造ARP包来诈骗路由器和目标主机

根据ARP的DOS，拒绝服务式攻击，发送大量的ARP包

MAC Flooding，溢出交换机的ARP表，使得所有网络不能通讯

防护：

ARP高速缓存超时设置

IP+MAC的绑定（校园网）

静态ARP缓存表，MAC绑定

自动查询，在某个时间保存一个IP和MAC的数据库，以后定时检查

HTTP1.0与2.0的区别

HTTP1.0利用文本与服务器交互，而HTTP2的基本协议单位为二进制帧流，每帧都有自己的类型旨在实现不同功能，HTTP2帧具有优先级，允许客户端提供排序思路，以让服务器优先处理一部分请求，仍然是以二进制帧的形式返回数

HTTP2.0只适用于HTTPS的场景

HTTP1.0的缺陷

每个请求都需单独建立连接（keep-alive能解决部分问题单不能交叉推送）

每个请求和响应都需要完整的头信息

数据未加密

HTTP2.0的优势

多路复用、压缩头信息、请求划分优先级、支持服务器端主动推送

怎么从一台电脑ping去另一台电脑

直接ping另一台电脑的IP地址，可以验证网络的连通性和统计响应时间和TTL。

Ping的原理使ICMP协议，互联网控制报文协议，是TCP/IP族协议的一个子协议，属于网络层协议，通常用于网络环境的测试。ICMP报文的唯一作用是报告错误。

回答应答，目标不可达、源抑制、超时报文，回路请求

TCP三次握手过程：

1. A准备好建立链接的资源，向B发送SYN请求报文
2. B收到SYN请求报文，B做好准备，向A发送SYN ACK报文
3. A收到SYN ACK报文，A向B发送ACK报文，同时，A也可以向B发送数据。

TCP四次挥手过程

1. A向B发送FIN报文
2. B收到FIN报文，向A发送ACK报文。这时B可以准备关闭了，但是这时B可能还有数据要发送给A。B把所有数据发送完成后，B向A发送FIN报文
3. A收到ACK报文，等待B的FIN报文。
4. A

为什么建立连接时三次握手，而关闭是四次

当server收到client的SYN请求后，可以直接发送SYN ACK报文。但是关闭连接时，server收到client的FIN请求后，不会立即关闭socket，所以只能先回复一个ACK，等待把所有报文发送完后，server才会发送FIN报文。

如果最后一个ACK没有收到，会发生什么？

Server会不断的重发FIN报文，直到收到ACK。

为什么不是两次握手：因为发送方和接受方需要同步序号。序号并不是从0开始的，而实由双方随机产生的序列号，并且都要把这个序列号告诉对方，确保对方能收到。

四次握手的问题：效率低。

TCP四次挥手过程：