应用层

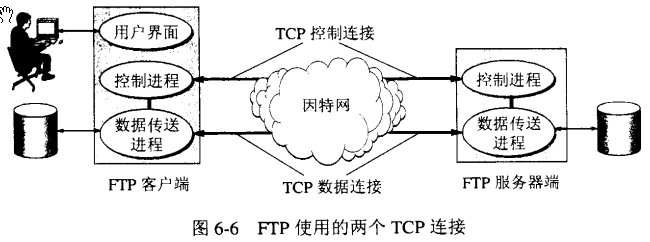
FTP（21）

　FTP屏蔽了各计算机系统的细节，因而适合在异构网络中任意计算机之间传送文件。FTP只提供文件传送的一些基本服务，它使用TCP可靠地运输服务，FTP主要功能是减小或消除在不同系统下处理文件的不兼容性。

　　FTP使用客户端-服务器模型，一个FTP服务器进程可以为多个客户进程提供服务。FTP服务器有两大部分组成：一个**主进程**，负责接受新的请求；还有若干**从属进程**，负责处理单个请求。主进程工作步骤

* 打开熟知端口(21)，使客户进程能够连接上
* 等待客户进程发送连接请求
* 启动从属进程处理客户进程发送的连接请求，从属进程处理完请求后结束，从属进程在运行期间可能根据需要可创建其他一些子进程
* 回到等待状态，继续接受其他客户进程发起的请求，主进程与从属进程的处理是并发进行的

**FTP工作时情况**



　　FTP控制连接在整个会话期间都保持打开，只用来发送连接/传送请求。当客户进程向服务器发送连接请求时，寻找连接服务器进程的熟知端口21，同时还要告诉服务器进程自己的另一个端口号码，用于建立数据传送连接。接着，服务器进程用自己传送数据的熟知端口20与客户进程所提供的端口号码建立数据传送连接，FTP使用了2个不同的端口号，所以数据连接和控制连接不会混乱。

TFTP(69)

TFTP是一个传输文件的简单协议，它其于UDP协议而实现，但是我们也不能确定有些TFTP协议是基于其它传输协议完成的。此协议设计的时候是进行小文件传输的。因此它不具备通常的FTP的许多功能，它只能从文件服务器上获得或写入文件，不能列出目录，不进行认证，它传输8位数据。传输中有三种模式：netascii，这是8位的ASCII码形式，另一种是octet，这是8位源数据类型；最后一种mail已经不再支持，它将返回的数据直接返回给用户而不是保存为文件。

SNMP(163)

TELNET(23)

Telnet协议是[TCP/IP协议](https://baike.baidu.com/item/TCP%2FIP%E5%8D%8F%E8%AE%AE)族中的一员，是Internet[远程登陆](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E9%99%86)服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)工作的能力。在[终端](https://baike.baidu.com/item/%E7%BB%88%E7%AB%AF)使用者的电脑上使用telnet程序，用它连接到[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)。[终端](https://baike.baidu.com/item/%E7%BB%88%E7%AB%AF)使用者可以在telnet程序中输入命令，这些命令会在[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)上运行，就像直接在服务器的控制台上输入一样。可以在本地就能控制[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)。要开始一个telnet会话，必须输入用户名和密码来登录[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)。Telnet是常用的[远程控制](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E6%8E%A7%E5%88%B6)Web[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)的方法。

SMTP(25)

SMTP（Simple Mail Transfer Protocol）即[简单邮件传输协议](https://baike.baidu.com/item/%E7%AE%80%E5%8D%95%E9%82%AE%E4%BB%B6%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE" \t "_blank),它是一组用于由源地址到目的地址传送[邮件](https://baike.baidu.com/item/%E9%82%AE%E4%BB%B6" \t "_blank)的规则，由它来控制信件的中转方式。[SMTP协议](https://baike.baidu.com/item/SMTP%E5%8D%8F%E8%AE%AE)属于[TCP/IP协议簇](https://baike.baidu.com/item/TCP%2FIP%E5%8D%8F%E8%AE%AE%E7%B0%87)，它帮助每台[计算机](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA)在发送或中转信件时找到下一个目的地。通过SMTP协议所指定的[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank),就可以把E-mail寄到收信人的服务器上了，整个过程只要几分钟。SMTP[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)则是遵循SMTP协议的发送[邮件服务器](https://baike.baidu.com/item/%E9%82%AE%E4%BB%B6%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)，用来发送或中转发出的[电子邮件](https://baike.baidu.com/item/%E7%94%B5%E5%AD%90%E9%82%AE%E4%BB%B6)。

它使用由TCP提供的可靠的数据传输服务把邮件消息从发信人的邮件服务器传送到收信人的邮件服务器。跟大多数应用层协议一样，SMTP也存在两个 端：在发信人的邮件服务器上执行的客户端和在收信人的邮件服务器上执行的服务器端。SMTP的客户端和服务器端同时运行在每个邮件服务器上。当一个邮件服 务器在向其他邮件服务器发送邮件消息时，它是作为SMTP客户在运行。

SMTP协议与人们用于面对面交互的礼仪之间有许多相似之处。首先，运行在发送端邮件服务器主机上的SMTP客户，发起建立一个到运行在接收端邮件服务 器主机上的SMTP服务器端口号25之间的TCP连接。如果接收邮件服务器当前不在工作，SMTP客户就等待一段时间后再尝试建立该连接。SMTP客户和服务器先执行一些应用层握手操作。就像人们在转手东西之前往往先自我介绍那样，SMTP客户和服务器也在传送信息之前先自我介绍一下。 在这个SMTP握手阶段，SMTP客户向服务器分别指出发信人和收信人的电子邮件地址。彼此自我介绍完毕之后，客户发出邮件消息。

HTTP(80)

HTTPS(443)

HTTP和HTTPS的区别

HTTP协议—经典面试题

http请求由三部分组成，分别是：请求行、消息报头、请求正文

HTTP（超文本传输协议）是一个基于请求与响应模式的、无状态的、应用层的协议，常基于TCP的连接方式，HTTP1.1版本中给出一种持续连接的机制，绝大多数的Web开发，都是构建在HTTP协议之上的Web应用。

**1、常用的HTTP方法有哪些？**

GET： 用于请求访问已经被URI（统一资源标识符）识别的资源，可以通过URL传参给服务器。

POST：用于传输信息给服务器，主要功能与GET方法类似，但一般推荐使用POST方式。

PUT： 传输文件，报文主体中包含文件内容，保存到对应URI位置。

HEAD： 获得报文首部，与GET方法类似，只是不返回报文主体，一般用于验证URI是否有效。

DELETE：删除文件，与PUT方法相反，删除对应URI位置的文件。

OPTIONS：查询相应URI支持的HTTP方法。

**2、GET方法与POST方法的区别**

区别一：

get重点在从服务器上获取资源，post重点在向服务器发送数据；

区别二：

get传输数据是通过URL请求，以field（字段）= value的形式，置于URL后，并用"?"连接，多个请求数据间用"&"连接，如http://127.0.0.1/Test/login.action?name=admin&password=admin，这个过程用户是可见的；

post传输数据通过Http的post机制，将字段与对应值封存在请求实体中发送给服务器，这个过程对用户是不可见的；

区别三：

Get传输的数据量小，因为受URL长度限制，但效率较高；

Post可以传输大量数据，所以上传文件时只能用Post方式；

区别四：

get是不安全的，因为URL是可见的，可能会泄露私密信息，如密码等；

post较get安全性较高；

区别五：

get方式只能支持ASCII字符，向服务器传的中文字符可能会乱码。

post支持标准字符集，可以正确传递中文字符。

**3、HTTP请求报文与响应报文格式**

请求报文包含三部分：

a、请求行：包含请求方法、URI、HTTP版本信息

b、请求首部字段

c、请求内容实体

响应报文包含三部分：

a、状态行：包含HTTP版本、状态码、状态码的原因短语

b、响应首部字段

c、响应内容实体

**4、常见的HTTP相应状态码**

返回的状态

1xx：指示信息--表示请求已接收，继续处理

2xx：成功--表示请求已被成功接收、理解、接受

3xx：重定向--要完成请求必须进行更进一步的操作

4xx：客户端错误--请求有语法错误或请求无法实现

5xx：服务器端错误--服务器未能实现合法的请求

200：请求被正常处理

204：请求被受理但没有资源可以返回

206：客户端只是请求资源的一部分，服务器只对请求的部分资源执行GET方法，相应报文中通过Content-Range指定范围的资源。

301：永久性重定向

302：临时重定向

303：与302状态码有相似功能，只是它希望客户端在请求一个URI的时候，能通过GET方法重定向到另一个URI上

304：发送附带条件的请求时，条件不满足时返回，与重定向无关

307：临时重定向，与302类似，只是强制要求使用POST方法

400：请求报文语法有误，服务器无法识别

401：请求需要认证

403：请求的对应资源禁止被访问

404：服务器无法找到对应资源

500：服务器内部错误

503：服务器正忙(服务不可用)服务器目前无法使用

**5、HTTP1.1版本新特性**

a、默认持久连接节省通信量，只要客户端服务端任意一端没有明确提出断开TCP连接，就一直保持连接，可以发送多次HTTP请求

b、管线化，客户端可以同时发出多个HTTP请求，而不用一个个等待响应

c、断点续传原理

**6、常见HTTP首部字段**

a、通用首部字段（请求报文与响应报文都会使用的首部字段）

Date：创建报文时间

Connection：连接的管理

Cache-Control：缓存的控制

Transfer-Encoding：报文主体的传输编码方式

b、请求首部字段（请求报文会使用的首部字段）

Host：请求资源所在服务器

Accept：可处理的媒体类型

Accept-Charset：可接收的字符集

Accept-Encoding：可接受的内容编码

Accept-Language：可接受的自然语言

c、响应首部字段（响应报文会使用的首部字段）

Accept-Ranges：可接受的字节范围

Location：令客户端重新定向到的URI

Server：HTTP服务器的安装信息

d、实体首部字段（请求报文与响应报文的的实体部分使用的首部字段）

Allow：资源可支持的HTTP方法

Content-Type：实体主类的类型

Content-Encoding：实体主体适用的编码方式

Content-Language：实体主体的自然语言

Content-Length：实体主体的的字节数

Content-Range：实体主体的位置范围，一般用于发出部分请求时使用

**7、HTTP的缺点与HTTPS**

a、通信使用明文不加密，内容可能被窃听

b、不验证通信方身份，可能遭到伪装

c、无法验证报文完整性，可能被篡改

HTTPS就是HTTP加上加密处理（一般是SSL安全通信线路）+认证+完整性保护

**8、HTTP优化**

利用负载均衡优化和加速HTTP应用

利用HTTP Cache来优化网站

DNS(53)

**解释一下DNS是什么**

域名系统DNS(Domain Name System)是因特网使用的命名系统，用来把便于人们使用的机器名字转换成为IP地址。域名系统其实就是名字系统。DNS使大多数名字都在本地解析(resolve)，仅有少量解析需要在因特网上通信，因此DNS系统的效率很高。由于DNS是分布式系统，即使单个计算机除了故障，也不会妨碍整个DNS系统的正常运行。

域名到IP地址的解析是由分布在因特网上的许多域名服务器程序共同完成的。域名服务器程序在专设的结点上运行，而人们也常把运行域名服务器程序的机器称为域名服务器。

   域名到IP地址的解析过程的要点如下：当某一个应用需要把主机名解析为IP地址时，该应用进程就调用解析程序，并称为DNS的一个客户，把待解析的域名放在DNS请求报文中，以UDP用户数据报方式发给本地域名服务器。本地域名服务器在查找域名后，把对应的IP地址放在回答报文中返回。应用程序获得目的主机的IP地址后即可进行通信。若本地域名服务器不能回答该请求，则此域名服务器就暂时称为DNS的另一个客户，并向其他域名服务器发出查询请求。这种过程直至找到能够回答该请求的域名服务器为止。**因特网的域名结构**

        由于因特网的用户数量较多，所以因特网在命名时采用的是层次树状结构的命名方法。任何一个连接在因特网上的主机或路由器，都有一个唯一的层次结构的名字，即域名(domain name)。这里，“域”(domain)是名字空间中一个可被管理的划分。

        从语法上讲，每一个域名都是有标号(label)序列组成，而各标号之间用点(小数点)隔开。

        如下例子所示：



        这是中央电视台用于手法电子邮件的计算机的域名，它由三个标号组成，其中标号com是顶级域名，标号cctv是二级域名，标号mail是三级域名。

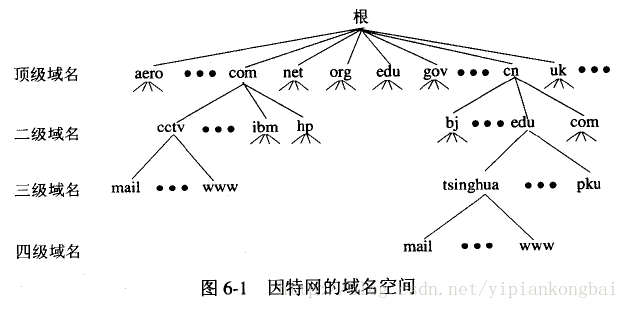
        DNS规定，域名中的标号都有英文和数字组成，每一个标号不超过63个字符(为了记忆方便，一般不会超过12个字符)，也不区分大小写字母。标号中除连字符(-)外不能使用其他的标点符号。级别最低的域名写在最左边，而级别最高的字符写在最右边。由多个标号组成的完整域名总共不超过255个字符。DNS既不规定一个域名需要包含多少个下级域名，也不规定每一级域名代表什么意思。各级域名由其上一级的域名管理机构管理，而最高的顶级域名则由ICANN进行管理。用这种方法可使每一个域名在整个互联网范围内是唯一的，并且也容易设计出一种查找域名的机制。

        域名只是逻辑概念，并不代表计算机所在的物理地点。据2006年12月统计，现在顶级域名TLD(Top Level Domain)已有265个，分为三大类：

        (1)国家顶级域名nTLD：采用ISO3166的规定。如：cn代表中国，us代表美国，uk代表英国，等等。国家域名又常记为ccTLD(cc表示国家代码contry-code)。

        (2)通用顶级域名gTLD：最常见的通用顶级域名有7个，即：com(公司企业)，net(网络服务机构)，org(非营利组织)，int(国际组织)，gov(美国的政府部门)，mil(美国的军事部门)。

        (3)基础结构域名(infrastructure domain)：这种顶级域名只有一个，即arpa，用于反向域名解析，因此称为反向域名。

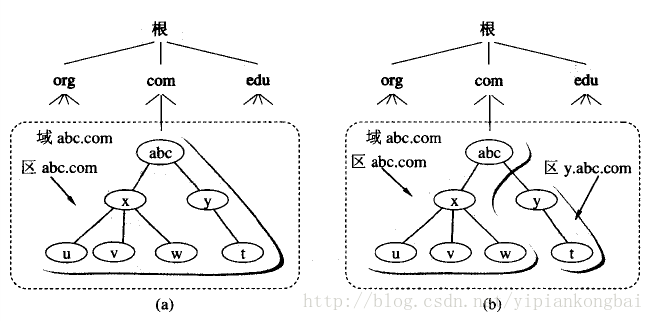


**3、域名服务器**

        如果采用上述的树状结构，每一个节点都采用一个域名服务器，这样会使得域名服务器的数量太多，使域名服务器系统的运行效率降低。所以在DNS中，采用划分区的方法来解决。

        一个服务器所负责管辖(或有权限)的范围叫做区(zone)。各单位根据具体情况来划分自己管辖范围的区。但在一个区中的所有节点必须是能够连通的。每一个区设置相应的权限域名服务器，用来保存该区中的所有主机到域名IP地址的映射。总之，DNS服务器的管辖范围不是以“域”为单位，而是以“区”为单位。区是DNS服务器实际管辖的范围。区 <= 域。

        下图是区的不同划分方法的举例。假定abc公司有下属部门x和y，部门x下面有分三个分布们u,v,w，而y下面还有下属部门t。图a表示abc公司只设一个区abc.com。这是，区abc.com和域abc.com指的是同一件事。但图b表示abc公司划分为两个区：abc.com和y.abc.com。这两个区都隶属于域abc.com，都各设置了相应的权限域名服务器。不难看出，区是域的子集。



        下图是以上图b中abc公司划分的两个区为例，给出了DNS域名服务器树状结构图。这种DNS域名服务器树状结构图可以更准确地反映出DNS的分布式结构。图中的每一个域名服务器都能够部分域名到IP地址的解析。当某个DNS服务器不能进行域名到IP地址的转换时，它就会设法找因特网上别的域名服务器进行解析。

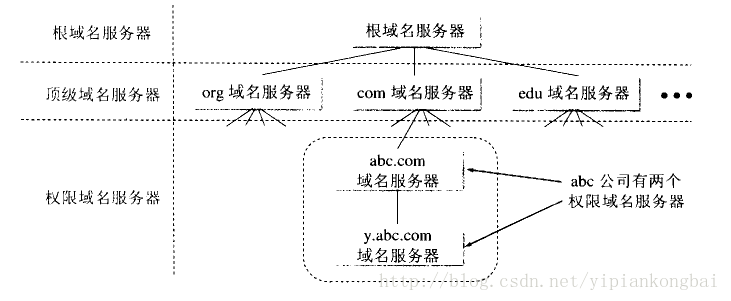
        从下图可以看出，因特网上的DNS服务器也是按照层次安排的。每一个域名服务器只对域名体系中的一部分进行管辖。根据域名服务器所起的作用，可以把域名服务器划分为下面四种不同的类型。

根域名服务器：最高层次的域名服务器，也是最重要的域名服务器。所有的根域名服务器都知道所有的顶级域名服务器的域名和IP地址。不管是哪一个本地域名服务器，若要对因特网上任何一个域名进行解析，只要自己无法解析，就首先求助根域名服务器。所以根域名服务器是最重要的域名服务器。假定所有的根域名服务器都瘫痪了，那么整个DNS系统就无法工作。需要注意的是，在很多情况下，根域名服务器并不直接把待查询的域名直接解析出IP地址，而是告诉本地域名服务器下一步应当找哪一个顶级域名服务器进行查询。

顶级域名服务器：负责管理在该顶级域名服务器注册的二级域名。

权限域名服务器：负责一个“区”的域名服务器。

本地域名服务器：本地服务器不属于下图的域名服务器的层次结构，但是它对域名系统非常重要。当一个主机发出DNS查询请求时，这个查询请求报文就发送给本地域名服务器。



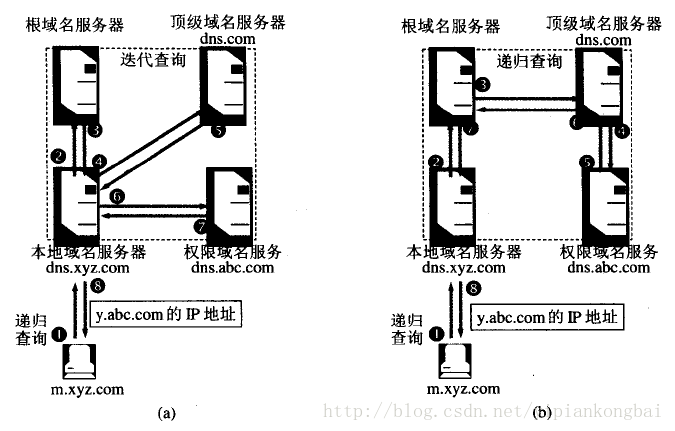
**4、域名的解析过程**

**注意：**

        一、主机向本地域名服务器的查询一般都是采用递归查询。所谓递归查询就是：如果主机所询问的本地域名服务器不知道被查询的域名的IP地址，那么本地域名服务器就以DNS客户的身份，向其它根域名服务器继续发出查询请求报文(即替主机继续查询)，而不是让主机自己进行下一步查询。因此，递归查询返回的查询结果或者是所要查询的IP地址，或者是报错，表示无法查询到所需的IP地址。

       二、本地域名服务器向根域名服务器的查询的迭代查询。迭代查询的特点：当根域名服务器收到本地域名服务器发出的迭代查询请求报文时，要么给出所要查询的IP地址，要么告诉本地服务器：“你下一步应当向哪一个域名服务器进行查询”。然后让本地服务器进行后续的查询。根域名服务器通常是把自己知道的顶级域名服务器的IP地址告诉本地域名服务器，让本地域名服务器再向顶级域名服务器查询。顶级域名服务器在收到本地域名服务器的查询请求后，要么给出所要查询的IP地址，要么告诉本地服务器下一步应当向哪一个权限域名服务器进行查询。最后，知道了所要解析的IP地址或报错，然后把这个结果返回给发起查询的主机。

        下图给出了这两种查询的差别



        下面举一个例子演示整个查询过程：

        假定域名为m.xyz.com的主机想知道另一个主机y.abc.com的IP地址。例如，主机m.xyz.com打算发送邮件给y.abc.com。这时就必须知道主机y.abc.com的IP地址。下面是上图a的几个查询步骤：

        1、主机m.abc.com先向本地服务器dns.xyz.com进行递归查询。

        2、本地服务器采用迭代查询。它先向一个根域名服务器查询。

        3、根域名服务器告诉本地服务器，下一次应查询的顶级域名服务器dns.com的IP地址。

        4、本地域名服务器向顶级域名服务器dns.com进行查询。

        5、顶级域名服务器dns.com告诉本地域名服务器，下一步应查询的权限服务器dns.abc.com的IP地址。

        6、本地域名服务器向权限域名服务器dns.abc.com进行查询。

        7、权限域名服务器dns.abc.com告诉本地域名服务器，所查询的主机的IP地址。

        8、本地域名服务器最后把查询结果告诉m.xyz.com。

        整个查询过程共用到了8个UDP报文。

        为了提高DNS查询效率，并减轻服务器的负荷和减少因特网上的DNS查询报文数量，在域名服务器中广泛使用了高速缓存，用来存放最近查询过的域名以及从何处获得域名映射信息的记录。

        例如，在上面的查询过程中，如果在m.xyz.com的主机上不久前已经有用户查询过y.abc.com的IP地址，那么本地域名服务器就不必向根域名服务器重新查询y.abc.com的IP地址，而是直接把告诉缓存中存放的上次查询结果(即y.abc.com的IP地址)告诉用户。

        由于名字到地址的绑定并不经常改变，为保持告诉缓存中的内容正确，域名服务器应为每项内容设置计时器并处理超过合理时间的项(例如每个项目两天)。当域名服务器已从缓存中删去某项信息后又被请求查询该项信息，就必须重新到授权管理该项的域名服务器绑定信息。当权限服务器回答一个查询请求时，在响应中都指明绑定有效存在的时间值。增加此时间值可减少网络开销，而减少此时间值可提高域名解析的正确性。

        不仅在本地域名服务器中需要高速缓存，在主机中也需要。许多主机在启动时从本地服务器下载名字和地址的全部数据库，维护存放自己最近使用的域名的高速缓存，并且只在从缓存中找不到名字时才使用域名服务器。维护本地域名服务器数据库的主机应当定期地检查域名服务器以获取新的映射信息，而且主机必须从缓存中删除无效的项。由于域名改动并不频繁，大多数网点不需花精力就能维护数据库的一致性。

**什么是域名劫持**

[域名](https://baike.baidu.com/item/%E5%9F%9F%E5%90%8D)劫持是互联网攻击的一种方式，通过攻击[域名解析](https://baike.baidu.com/item/%E5%9F%9F%E5%90%8D%E8%A7%A3%E6%9E%90)服务器（DNS），或伪造域名解析服务器（DNS）的方法，把目标网站域名解析到错误的地址从而实现用户无法访问目标网站的目的。**、什么是域名劫持**  
  
   域名劫持就是在劫持的网络范围内拦截域名解析的请求，分析请求的域名，把审查范围以外的请求放行，否则直接返回假的IP地址或者什么也不做使得请求失去响应，其效果就是对特定的网址不能访问或访问的是假网址。  
  
   大家都知道目前提供搜索引擎服务的产品很多，常用的如百度、谷歌、搜狗、有道等，他们应用的技术差别较大，核心技术一般都作为公司的技术机密，我们是不得而知，但都存在一个数据快照，存储在搜索引擎服务器上，当用户输人关键字时，搜索引擎通过搜索功能在快照服务器上检索，并将结果按收录的时间或其他索引进行排序列出，为用户提供信息。  
  
   但在使用过程中，网站如果被植入木马程序，表现为通过搜索引擎搜索到某一网站，搜索结果中的网站名 称、域名均与实际相符，打开这个网站时，前1〜2秒时间，是打开网站域名时的解析，没有异常，但再过1秒钟左右，打开出现的网站却是其他网站或者非法网站，而域名解析的ip地址没有任何异常是完全正确的。  
  
**二、网站域名被劫持了应该怎么办**  
  
1、关闭域名的泛解析  
  
   我们必须要有域名的管理帐号和密码，否则只能通过域名服务商的客服来解决了，当然后面一种办法比较浪费时间。进入了域名管理后台之后就可以点击我们的域名找到带\*号的域名解析，删除掉就可以了。  
  
2、举报大量垃圾页面  
  
   因为我们站长心里也清楚，那些垃圾页面都会成为我们网站的死链。所以我们要把这些死链都解决掉，我们在页面举报内容处写上网站被恶意泛解析就可以了，好的情况就是百度会迅速关注你的站点从而帮你大量的删除，不好的情况恐怕只能我们把那些垃圾页面一个个的举报掉了。  
  
3、看事件管理器，清理Web网点中存在的可疑文件  
  
   Windows网络操作系统中有事件管理器，不管黑客是通过何种方式获取操作权限的，事件管理器中均可以看出异常，通过异常的事件和日期，在Web站中查找该日期内文件的变化情况，对可以执行代码的文件需要特别查看其是否被注人代码或改动，对于新增的可执行代码文件进行清理。  
  
4、配置Web站点文件夹及文件操作权限  
  
   Windows网络操作系统中，使用超级管理员权限， 对Web站点文件及文件夹配置权限，多数设置为读权限，谨慎使用写权限，如果无法获取超级管理员权限，这样木马程序便无法生根，网站域名被劫持的可能便可以降低很多。  
  
5、加强网站的防SQL注入功能  
  
   SQL注人是利用SQL语句的特点，向数据库写内容，从而获取到权限的方法。对于访问MS SQL Server 数据库时，不要使用权限较大的sa默认用户，需要建立只访问本系统数据库的专一用户，并配置其为系统所需的最小权限。  
  
6、咨询网站域名服务商寻求帮助。  
  
  
**三、怎么预防网站域名劫持**  
  
1、在不同的网络上运行分离的域名服务器来取得冗余性。  
  
2、将外部和内部域名服务器分开（物理上分开或运行BIND Views）并使用转发器（forwarders）。外部域名服务器应当接受来自几乎任何地址的查询，但是转发器则不接受。它们应当被配置为只接受来自内部地址的查询。关闭外部域名服务器上的递归功能（从根服务器开始向下定位DNS记录的过程）。这可以限制哪些DNS服务器与Internet联系。  
　　  
3、可能时，限制动态DNS更新。  
  
4、将区域传送仅限制在授权的设备上。  
  
5、利用事务签名对区域传送和区域更新进行数字签名。  
  
6、隐藏运行在服务器上的BIND版本。  
  
7、删除运行在DNS服务器上的不必要服务，如FTP、telnet和HTTP。  
  
8、在网络外围和DNS服务器上使用防火墙服务。将访问限制在那些DNS功能需要的端口/服务上。  
  
9、选择一个企业级的域名公司注册。一些域名公司以消费者和小企业为目标。结果，他们不能为企业提供企业级[域名注册](http://www.abcde.cn/domain/" \t "_blank)商所能提供的安全保护。  
  
10、及时更新安全补丁。确保你的Web服务器使用的是最新的安全补丁，这样黑客就不能利用已知的软件漏洞。否则你就是自找麻烦。因为域名被劫持只是早晚的问题。这是Mohan的客户从没有应用最新MySQL补丁汲取的教训。  
  
11、监控网站的流量去了哪里。如果你看到网站流量神秘地发往位于乌克兰的服务器，就像CheckFree所经历的一样，那网站就可能是出了什么问题。  
  
12、从注册商处请求DNS SEC。DNSSEC——会为你的域名系统添加安全扩展——但不能防止域名被劫持，不过唯一可作为保障的技术就是用户点击网站上的链接后，他/她在点击网页链接与进入你网页之间的那段时间里不会被劫持。

DHCP

什么是DHCP

是一个[局域网](https://baike.baidu.com/item/%E5%B1%80%E5%9F%9F%E7%BD%91)的[网络协议](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%8D%8F%E8%AE%AE)，使用[UDP](https://baike.baidu.com/item/UDP)协议工作， 主要有两个用途：给内部网络或[网络服务](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E6%9C%8D%E5%8A%A1)供应商自动分配[IP地址](https://baike.baidu.com/item/IP%E5%9C%B0%E5%9D%80)，给用户或者内部[网络管理员](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E7%AE%A1%E7%90%86%E5%91%98)作为对所有[计算机](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA)作中央管理的手段，在RFC 2131中有详细的描述。DHCP有3个端口，其中UDP67和UDP68为正常的DHCP服务端口，分别作为DHCP Server和DHCP Client的服务端口；546号端口用于DHCPv6 Client，而不用于DHCPv4，是为DHCP failover服务，这是需要特别开启的服务，DHCP failover是用来做“双机热备”的。

动态主机配置协议，是一个应用层协议。当我们将客户主机ip地址设置为动态获取方式时，DHCP服务器就会根据DHCP协议给客户端分配IP，使得客户机能够利用这个IP上网。

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）通常被应用在大型的局域网络环境中，主要作用是集中的管理、分配IP地址，使网络环境中的主机动态的获得IP地址、Gateway地址、DNS服务器地址等信息，并能够提升地址的使用率。

DHCP协议采用客户端/服务器模型，主机地址的动态分配任务由网络主机驱动。当DHCP服务器接收到来自网络主机申请地址的信息时，才会向网络主机发送相关的地址配置等信息，以实现网络主机地址信息的动态配置。DHCP具有以下功能：

1. 保证任何IP地址在同一时刻只能由一台DHCP客户机所使用。

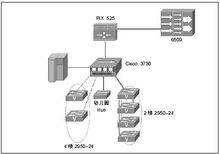
2. DHCP应当可以给用户分配永久固定的IP地址。

3. DHCP应当可以同用其他方法获得IP地址的[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "_blank)共存（如手工配置IP地址的主机）。

4. DHCP[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)应当向现有的BOOTP[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF)提供服务。

DHCP有三种机制分配IP地址：

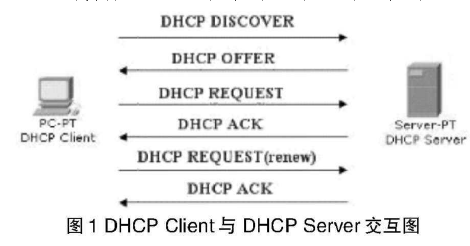
1) 自动分配方式（Automatic Allocation），DHCP服务器为主机指定一个永久性的IP地址，一旦DHCP客户端第一次成功从DHCP服务器端租用到IP地址后，就可以永久性的使用该地址。

[](https://baike.baidu.com/pic/DHCP/218195/0/1e71f724d22034414d088d5f?fr=lemma&ct=single)相关图片

2) 动态分配方式（Dynamic Allocation），DHCP服务器给主机指定一个具有时间限制的IP地址，时间到期或主机明确表示放弃该地址时，该地址可以被其他主机使用。

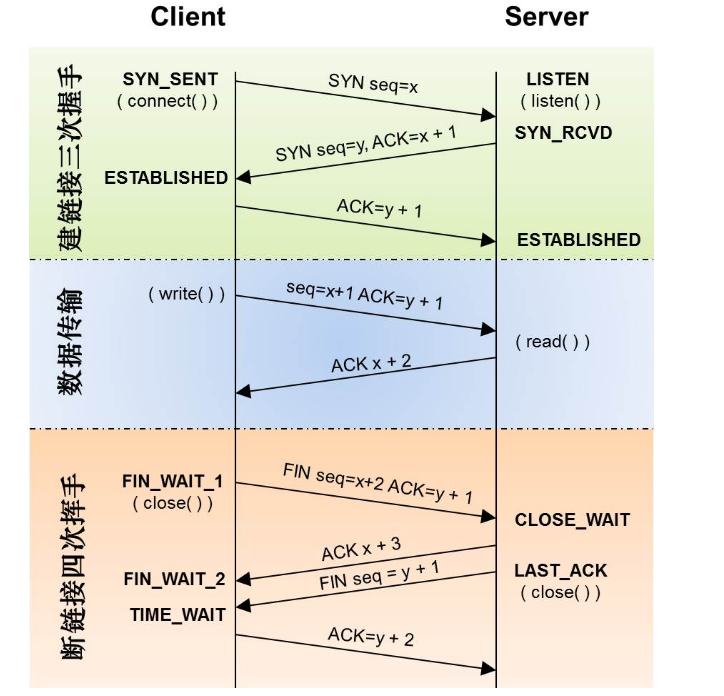
3) 手工分配方式（Manual Allocation），客户端的IP地址是由网络管理员指定的，DHCP服务器只是将指定的IP地址告诉客户端主机。

### ，DHCP的实现

   
DHCP的实现分为4步，分别是：   
第一步：Client端在局域网内发起一个DHCP　Discover包，目的是想发现能够给它提供IP的DHCP Server。   
第二步：可用的DHCP Server接收到Discover包之后，通过发送DHCP Offer包给予Client端应答，意在告诉Client端它可以提供IP地址。   
第三步：Client端接收到Offer包之后，发送DHCP Request包请求分配IP。   
第四步：DHCP Server发送ACK数据包，确认信息。

TCP/IP

三次握手四次挥手



1. 第一次握手：建立连接。客户端发送连接请求报文段，将SYN位置为1，Sequence Number为x；然后，客户端进入SYN\_SEND状态，等待服务器的确认；
2. 第二次握手：服务器收到SYN报文段。服务器收到客户端的SYN报文段，需要对这个SYN报文段进行确认，设置Acknowledgment Number为x+1(Sequence Number+1)；同时，自己自己还要发送SYN请求信息，将SYN位置为1，Sequence Number为y；服务器端将上述所有信息放到一个报文段（即SYN+ACK报文段）中，一并发送给客户端，此时服务器进入SYN\_RECV状态；
3. 第三次握手：客户端收到服务器的SYN+ACK报文段。然后将Acknowledgment Number设置为y+1，向服务器发送ACK报文段，这个报文段发送完毕以后，客户端和服务器端都进入ESTABLISHED状态，完成TCP三次握手。

完成了三次握手，客户端和服务器端就可以开始传送数据。以上就是TCP三次握手的总体介绍。

1. 第一次分手：主机1（可以使客户端，也可以是服务器端），设置Sequence Number和Acknowledgment Number，向主机2发送一个FIN报文段；此时，主机1进入FIN\_WAIT\_1状态；这表示主机1没有数据要发送给主机2了；
2. 第二次分手：主机2收到了主机1发送的FIN报文段，向主机1回一个ACK报文段，Acknowledgment Number为Sequence Number加1；主机1进入FIN\_WAIT\_2状态；主机2告诉主机1，我“同意”你的关闭请求；
3. 第三次分手：主机2向主机1发送FIN报文段，请求关闭连接，同时主机2进入LAST\_ACK状态；
4. 第四次分手：主机1收到主机2发送的FIN报文段，向主机2发送ACK报文段，然后主机1进入TIME\_WAIT状态；主机2收到主机1的ACK报文段以后，就关闭连接；此时，主机1等待2MSL后依然没有收到回复，则证明Server端已正常关闭，那好，主机1也可以关闭连接了。

至此，TCP的四次分手就这么愉快的完成了。当你看到这里，你的脑子里会有很多的疑问，很多的不懂，感觉很凌乱；没事，我们继续总结。

#### 为什么要三次握手

既然总结了TCP的三次握手，那为什么非要三次呢？怎么觉得两次就可以完成了。那TCP为什么非要进行三次连接呢？在谢希仁的《计算机网络》中是这样说的：

为了防止已失效的连接请求报文段突然又传送到了服务端，因而产生错误。

在书中同时举了一个例子，如下：

“已失效的连接请求报文段”的产生在这样一种情况下：client发出的第一个连接请求报文段并没有丢失，而是在某个网络结点长时间的滞留了，以致延误到连接释放以后的某个时间才到达server。本来这是一个早已失效的报文段。但server收到此失效的连接请求报文段后，就误认为是client再次发出的一个新的连接请求。于是就向client发出确认报文段，同意建立连接。假设不采用“三次握手”，那么只要server发出确认，新的连接就建立了。由于现在client并没有发出建立连接的请求，因此不会理睬server的确认，也不会向server发送数据。但server却以为新的运输连接已经建立，并一直等待client发来数据。这样，server的很多资源就白白浪费掉了。采用“三次握手”的办法可以防止上述现象发生。例如刚才那种情况，client不会向server的确认发出确认。server由于收不到确认，就知道client并没有要求建立连接。”

这就很明白了，防止了服务器端的一直等待而浪费资源。

#### 为什么要四次分手

那四次分手又是为何呢？TCP协议是一种面向连接的、可靠的、基于字节流的运输层通信协议。TCP是全双工模式，这就意味着，当主机1发出FIN报文段时，只是表示主机1已经没有数据要发送了，主机1告诉主机2，它的数据已经全部发送完毕了；但是，这个时候主机1还是可以接受来自主机2的数据；当主机2返回ACK报文段时，表示它已经知道主机1没有数据发送了，但是主机2还是可以发送数据到主机1的；当主机2也发送了FIN报文段时，这个时候就表示主机2也没有数据要发送了，就会告诉主机1，我也没有数据要发送了，之后彼此就会愉快的中断这次TCP连接。如果要正确的理解四次分手的原理，就需要了解四次分手过程中的状态变化。

* FIN\_WAIT\_1: 这个状态要好好解释一下，其实FIN\_WAIT\_1和FIN\_WAIT\_2状态的真正含义都是表示等待对方的FIN报文。而这两种状态的区别是：FIN\_WAIT\_1状态实际上是当SOCKET在ESTABLISHED状态时，它想主动关闭连接，向对方发送了FIN报文，此时该SOCKET即进入到FIN\_WAIT\_1状态。而当对方回应ACK报文后，则进入到FIN\_WAIT\_2状态，当然在实际的正常情况下，无论对方何种情况下，都应该马上回应ACK报文，所以FIN\_WAIT\_1状态一般是比较难见到的，而FIN\_WAIT\_2状态还有时常常可以用netstat看到。（主动方）
* FIN\_WAIT\_2：上面已经详细解释了这种状态，实际上FIN\_WAIT\_2状态下的SOCKET，表示半连接，也即有一方要求close连接，但另外还告诉对方，我暂时还有点数据需要传送给你(ACK信息)，稍后再关闭连接。（主动方）
* CLOSE\_WAIT：这种状态的含义其实是表示在等待关闭。怎么理解呢？当对方close一个SOCKET后发送FIN报文给自己，你系统毫无疑问地会回应一个ACK报文给对方，此时则进入到CLOSE\_WAIT状态。接下来呢，实际上你真正需要考虑的事情是察看你是否还有数据发送给对方，如果没有的话，那么你也就可以 close这个SOCKET，发送FIN报文给对方，也即关闭连接。所以你在CLOSE\_WAIT状态下，需要完成的事情是等待你去关闭连接。（被动方）
* LAST\_ACK: 这个状态还是比较容易好理解的，它是被动关闭一方在发送FIN报文后，最后等待对方的ACK报文。当收到ACK报文后，也即可以进入到CLOSED可用状态了。（被动方）
* TIME\_WAIT: 表示收到了对方的FIN报文，并发送出了ACK报文，就等2MSL后即可回到CLOSED可用状态了。如果FINWAIT1状态下，收到了对方同时带FIN标志和ACK标志的报文时，可以直接进入到TIME\_WAIT状态，而无须经过FIN\_WAIT\_2状态。（主动方）
* CLOSED: 表示连接中断。

**TCP和UDP的区别**

1、基于连接与无连接。  
2、TCP要求系统资源较多，UDP较少。  
3、UDP程序结构较简单。  
4、流模式（TCP）与数据报模式(UDP)。  
5、TCP保证数据正确性，UDP可能丢包。  
6、TCP保证数据顺序，UDP不保证。  
7、TCP面向连接（如打电话要先拨号建立连接）;UDP是无连接的，即发送数据之前不需要建立连接。  
8、TCP提供可靠的服务。也就是说，通过TCP连接传送的数据，无差错，不丢失，不重复，且按序到达;UDP尽最大努力交付，即不保证可靠交付。  
9、TCP面向字节流，实际上是TCP把数据看成一连串无结构的字节流;UDP是面向报文的，UDP没有拥塞控制，因此网络出现拥塞不会使源主机的发送速率降低（对实时应用很有用，如IP电话，实时视频会议等）。  
10、每一条TCP连接只能是点到点的;UDP支持一对一，一对多，多对一和多对多的交互通信。  
11、TCP首部开销20字节;UDP的首部开销小，只有8个字节。  
12、TCP的逻辑通信信道是全双工的可靠信道，UDP则是不可靠信道。  
TCP（Transmission Control Protocol [传输控制协议](https://www.baidu.com/s?wd=%E4%BC%A0%E8%BE%93%E6%8E%A7%E5%88%B6%E5%8D%8F%E8%AE%AE&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YdryRLmWckuHw9P1bdrjTs0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnWDvPjDYnHcs)）是一种面向连接的、可靠的、基于字节流的传输层通信协议，由IETF的RFC 793定义。在简化的计算机网络OSI模型中，完成第四层传输层所指定的功能。  
UDP 是User Datagram Protocol的简称， 中文名是[用户数据报协议](https://www.baidu.com/s?wd=%E7%94%A8%E6%88%B7%E6%95%B0%E6%8D%AE%E6%8A%A5%E5%8D%8F%E8%AE%AE&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YdryRLmWckuHw9P1bdrjTs0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnWDvPjDYnHcs)，是OSI（Open System Interconnection，开放式系统互联） 参考模型中一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务，IETF RFC 768是UDP的正式规范。UDP在IP报文的协议号是17。

**TCP是如何保证可靠性的**

**TCP协议支持数据报传输可靠性的主要方法是确认、超时、重传、校验和以及流量控制。**

（1）校验和——每个TCP报文段都包括检验和字段，校验和用来检查报文段是否出现传输错误，如果报文段出现传输错误，TCP检查出错就丢弃该报文段。

（2）确认——接收端检查报文是否出错，发现出错时就丢弃，不发确认；而发送端TCP就通过检查接收端的确认，判断发送的报文段是否已经正确到达目的地。

（3）超时——发送端根据发出的报文段在超时规定的时间内是否收到确认，从而来判断该报文段是否丢失或传输出错。TCP使用了4种计时器:重传计时器、坚持计时器、保持计时器和时间等待计时器来保证了传输的可靠性。

Tcp

**EGP，IGP？**

答：（1）IGP：内部网关协议，即在一个自治系统内部使用的路由选择协议，如RIP和OSPF。

              （11）RIP是一种分布式的基于距离向量的路由选择协议，要求网络中的每一个路由器都要维护从它自己到其他每一个目的网络的距离向量。距离即是跳数，路由器与直接相连的网络跳数为1，以后每经过一个路由器跳数加1。RIP允许一条路径最多包含15个路由器，因此当距离为16时认为不可达，这因为如此限制了网络的规模，说明RIP只能工作在规模较小的网络中。**RIP的三个要点：仅和相邻路由器交换信息；交换的信息是当前路由器知道的全部信息，即路由表；按固定的时间间隔交换路由信息，如30秒。RIP协议使用运输层的用户数据报UDP进行传送，因此RIP协议的位置位于应用层，但是转发IP数据报的过程是在网络层完成的。RIP是好消息传播的快，坏消息传播的慢。**

**（12）OSPF：最短路径优先，三个要点：采用洪泛法向本自治系统的路由器发送信息；发送的信息就是与本路由器相邻的所有路由器的链路状态，但这只是路由器所知道的部分信息；只有当链路状态发生变化时，路由器才用洪泛法向所有路由器发送此信息。OSPF直接使用IP数据包传送，因此OSPF位于网络层。**

       EGP：外部网关协议，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，如EGP。

# ARP协议(链路层)

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。  
广播发送ARP请求，单播发送ARP响应。

# RARP（链路层）

RARP是逆地址解析协议，作用是完成MAC地址到IP地址的映射，主要用于无盘工作站，因为给无盘工作站配置的IP地址不能保存。工作流程：在网络中配置一台RARP服务器，里面保存着IP地址和MAC地址的映射关系，当无盘工作站启动后，就封装一个RARP数据包，里面有其MAC地址，然后广播到网络上去，当服务器收到请求包后，就查找对应的MAC地址的IP地址装入响应报文中发回给请求者。因为需要广播请求报文，因此RARP只能用于具有广播能力的网络。

# ICMP（网络层）

主要用途是确认IP包是否成功送达目标地址，通知在发送过程中IP包被废弃的原因，改善网络配置等。

理解从输入网址到页面出现的过程

怎么确定打开的当前页面是就是你自己

上不了网该怎么办

URL与URI的区别

1、URI是统一资源标识符，是一个用于标识某一互联网资源名称的字符串。 该种标识允许用户对任何（包括本地和互联网）的资源通过特定的协议进行交互操作。URI由包括确定语法和相关协议的方案所定义。由是三个组成部分：访问资源的命名机制、存放资源的主机名、资源自身的名称，由路径表示。  
比如文件的URL，服务器方式用file表示，后面要有主机IP地址、文件的存取路径（即目录）和文件名等信息。有时可以省略目录和文件名，但“/”符号不能省略。  
例：file://a:1234/b/c/d.txt代表获取资源使用[ftp协议](https://www.baidu.com/s?wd=ftp%E5%8D%8F%E8%AE%AE&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YvmHfsnHKbn1RLuynkPADv0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EPHckn1D4rHTs)，资源目标是a主机的1234端口的b目录下的c目录下的d.txt。  
2、URL是统一资源定位，是对可以从互联网上得到的资源的位置和访问方法的一种简洁的表示，是互联网上标准资源的地址。互联网上的每个文件都有一个唯一的URL，它包含的信息指出文件的位置以及浏览器应该怎么处理它。  
比如百度URL即是[http://www.baidu.com](http://www.baidu.com/)。