## 域名系统

IP地址是以数字来代表主机的地址，比较难记。为了使用和记忆方便，也为了便于网络地址的分层管理和分配，INTERNET在1984年采用了域名管理系统( DOMAIN NAME SYSTEM)，入网的每台主机都具有类似于下列结构的域名：

主机号.机构名.网络名.最高层域名

域名用一组简短的英文表达，比用数字表达的IP地址容易记忆。例如：北京电报局的一台与INTERNET联网的电脑主机的IP地址是202.96.0.97，域名为PUBLIC.BTA.NET.CN，其含义是: 主机号PUBLIC.北京电报局.网络中心.中国，其中.NET.CN表示为邮电网，我国其它网的域名分别为：.AC.CN 表示为科研网。　　.EDU.CN 表示为教育网。 　　.COM.CN表示为金桥网。

加入INTERNET的各级网络依照域名管理系统的命名规则对本网内的主机命名和分配网内主机号，并负责完成通信时域名到IP地址的转换。对使用者来说，我们绝大部分情况可以不使用IP地址，而直接使用域名，INTERNET上的服务系统自动地转为IP类型的地址。

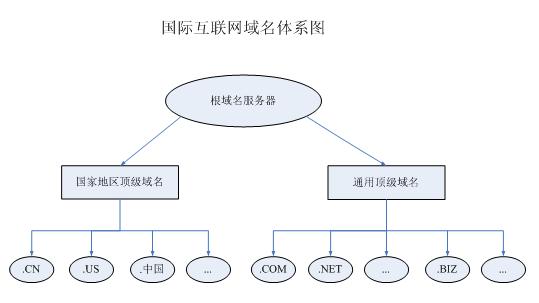
　域名类似于网络上的门牌号码，是用于识别和定位互联网上计算机的层次结构式字符标识，与该计算机的互联网协议（IP）地址相对应。但相对于IP地址而言，更便于使用者理解和记忆。

　　互联网名称与数字地址分配机构（ICANN）负责管理和协调国际互联网络域名系统。国际互联网域名体系中，对顶级域名进行划分，包括：

　　国家和地区顶级域名（Country Code Top Level Domain，简称ccTLD），对应于国家、地区的地理位置，如.CN/.中国代表中国、.US代表美国等；

通用类别顶级域名（Generic Top Level Domain，简称gTLD），对应不同类别，比较常见的如.COM、.NET、.ORG等。近几年ICANN根据域名体系的需要，新增了部分顶级域名的类型，如.BIZ、.INFO等。

<https://www.cnnic.net.cn/jczyfw/CNym/cnymyhfaq/>



一个完整的域名由二个或二个以上部分组成，各部分之间用英文的句号"."来分隔，最后一个"."的右边部分称为顶级域名，最后一个"."的左边部分称为二级域名，二级域名的左边部分称为三级域名，以此类推，每一级的域名控制它下一级域名的分配。如：cnnic.cn是一个二级域名，cnnic.net.cn是一个三级域名。

　　域名可以配置子域名，用户可以自行设置或寻求域名注册服务机构的帮助。子域名（Sub Domain）是个相对的概念，是相对父域名来说的，父域名的下一级就是子域名。域名有很多级，中间用英文的句号"."分开。如：ewhois.cnnic.cn便是 cnnic.cn 的子域。

　　域名属于互联网上的基础服务，基于域名可以提供WWW、EMAIL、FTP等应用服务，如：

　　1、建立一个本人或本单位的主页；

　　2、建立一个本人或本单位的电子邮件系统，实现收发邮件、对外联系的功能；

　　3、在企业、产品的宣传推广中进行使用，如：在名片或广告上显示本人或本单位的主页地址；

　　4、可将域名指向自己的微博，空间。

A domain name is an identification string that defines a realm of administrative autonomy, authority or control within the Internet. Domain names are formed by the rules and procedures of the Domain Name System (DNS). Any name registered in the DNS is a domain name. Domain names are used in various networking contexts and application-specific naming and addressing purposes. In general, a domain name represents an Internet Protocol (IP) resource, such as a personal computer used to access the Internet, a server computer hosting a web site, or the web site itself or any other service communicated via the Internet. In 2015, 294 million domain names had been registered.[1]

<https://investor.verisign.com/releasedetail.cfm?releaseid=920138>

<https://en.wikipedia.org/wiki/Domain_name#cite_note-investor.verisign.com-1>

<http://baike.baidu.com/link?url=GiEb1kS_fFflzEsK6POzEudmmg-Rb9NvWR-sSy_Qxh3hslHkMztO48qYpLU3wXivjZZrNrRWs5AAvOk6ZCjYmK>

## DNS

DNS（Domain Name System，域名系统），因特网上作为域名和IP地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网，而不用去记住能够被机器直接读取的IP数串。通过主机名，最终得到该主机名对应的IP地址的过程叫做域名解析

如果把DNS的体系结构比喻成一棵倒挂的大树，那么毫无疑问，每一条记录就是组成这棵大树必不可少的枝叶了。所谓的DNS记录，其实就是具有特殊功能的一个个数据条目。

A记录

当我们想获取一个域名对应的IP地址，或通过域名方式访问某一网页或程序，此时就需要在这个域名和所属的IP地址间创建一个映射关系。这个关系就是利用在DNS中为此名称创建的A记录。而这个名称可以理解成是某台主机的计算机名如www，它的IP是192.168.1.100，同时，在这台主机安装IIS并创建一个测试页面。当DNS服务器上存在一个abcdef.com的区域，同时，将www这台主机的主DNS后缀设为abcdef.com，现在，我们想在局域网内实现通过www.abcdef.com就可以访问那个测试页面，那么就需要在DNS上做一个A记录，目的是把www.abcdef.com和192.168.1.100对应起来，如下图：

MX记录

MX记录即Mail [Exchanger，主要用于邮件服务器，作用是用于定位邮件服务器的地址。如一个用户给user@abcdef.com的用户要发封邮件，此时该用户的所属的邮件系统会通过DNS服务器来查找abcdef.com这个域名的MX记录，如果存在，就会根据这个MX记录来查找对应的A记录，从而得到邮件服务器的IP地址，并将这封邮件发送到这台服务器上。可见，MX记录和A记录是分不开的。总的来说，MX记录是为了让对方找到你的邮件服务器，所以，如果想顺利收信，就必须为你的邮件服务器创建合法有效的MX记录。](mailto:Exchanger，主要用于邮件服务器，作用是用于定位邮件服务器的地址。如一个用户给user@abcdef.com的用户要发封邮件，此时该用户的所属的邮件系统会通过DNS服务器来查找abcdef.com这个域名的MX记录，如果存在，就会根据这个MX记录来查找对应的A记录，从而得到邮件服务器的IP地址，并将这封邮件发送到这台服务器上。可见，MX记录和A记录是分不开的。总的来说，MX记录是为了让对方找到你的邮件服务器，所以，如果想顺利收信，就必须为你的邮件服务器创建合法有效的MX记录。)

txt记录用来保存域名的附加文本信息，txt记录的内容按照一定的格式编写，最常用的是spf格式，spf用于登记某个域名拥有的用来外发邮件的所有ip地址。mx记录的作用是给寄信者指明某个域名的邮件服务器有哪些，spf格式的txt记录的作用跟mx记录相反，它向收信者表明，哪些邮件服务器是经过某个域名认可会发送邮件的。spf的作用主要是反垃圾邮件，主要针对那些发信人伪造域名的垃圾邮件。

按照spf格式在dns中增加一条txt类型的记录，将提高该域名的信誉度，同时可以防止垃圾邮件伪造该域的发件人发送垃圾邮件。

<http://wenku.baidu.com/link?url=J-o7eXI8NnbBK6Y7k9px5GCIKMFzODqv3l8XMWaYFo6tTkE88IEB1E9AGITH8b3LwZpMaQ96L3bKAB8sFO9zWaartbOjNZV714TaOPQRG8q>

## 域名劫持

域名解析（DNS）的基本原理是把网络地址（域名，以一个字符串的形式）对应到真实的计算机能够识别的网络地址（IP地址，比如216.239.53.99 这样的形式），以便计算机能够进一步通信，传递网址和内容等。

由于域名劫持往往只能在特定的被劫持的网络范围内进行，所以在此范围外的域名服务器(DNS)能够返回正常的IP地址，高级用户可以在网络设置把DNS指向这些正常的域名服务器以实现对网址的正常访问。所以域名劫持通常相伴的措施——封锁正常DNS的IP。

如果知道该域名的真实IP地址，则可以直接用此IP代替域名后进行访问。比如访问谷歌 ，可以把访问改为http://216.239.53.99/ ，从而绕开域名劫持。

过程：

由于域名劫持只能在特定的网络范围内进行，所以范围外的域名服务器(DNS)能返回正常IP地址。攻击者正是利用此点在范围内封锁正常DNS的IP地址，使用域名劫持技术，通过冒充原域名以E-MAIL方式修改公司的注册域名记录，或将域名转让到其他组织，通过修改注册信息后在所指定的DNS服务器加进该域名记录，让原域名指向另一IP的服务器，让多数网民无法正确访问，从而使得某些用户直接访问到了恶意用户所指定的域名地址，其实施步骤如下：

一、获取劫持域名注册信息：首先攻击者会访问域名查询站点，通过MAKE CHANGES功能，输入要查询的域名以取得该域名注册信息。

二、控制该域名的E-MAIL帐号：此时攻击者会利用社会工程学或暴力破解学进行该E-MAIL密码破解，有能力的攻击者将直接对该E-MAIL进行入侵行为，以获取所需信息。

三、修改注册信息：当攻击者破获了E-MAIL后，会利用相关的MAKE CHANGES功能修改该域名的注册信息，包括拥有者信息，DNS服务器信息等。

四、使用E-MAIL收发确认函：此时的攻击者会在信件帐号的真正拥有者之前，截获网络公司回馈的网络确认注册信息更改件，并进行回件确认，随后网络公司将再次回馈成功修改信件，此时攻击者成功劫持域名。

缺点：

它不是很稳定，在某些网络速度快的地方，真实的IP地址返回得比窃持软件提供的假地址要快，因为监测和返回这么巨大的数据流量也是要花费一定时间的。

在网上查询域名的正确IP非常容易。一个是利用海外的一些在线IP地址查询服务，可以查找到网站的真实IP地址。在Google上搜索"nslookup"，会找到更多类似的服务。

http://baike.baidu.com/link?url=sybnPtNWlPydrAFl3roj9ZZHkDFCcAt96Bp0raCcYCS3z-8mwskk1eAjwcdWxlo90rYmjgUeVNywQyCIQjY4yK