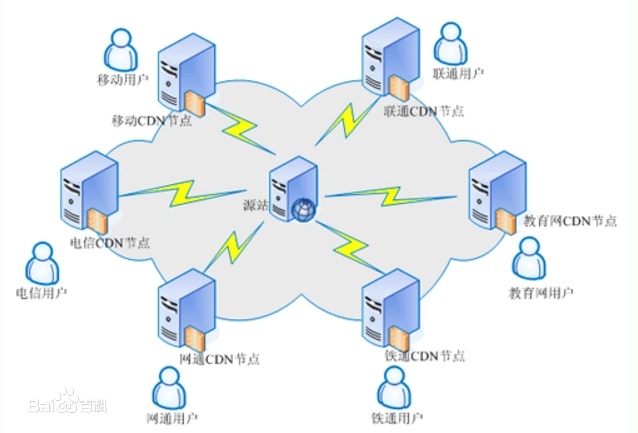
# 5.信息收集：CDN绕过

1. CDN简介
   1. CDN的全称是Content Delivery Network，即[内容分发网络](https://baike.baidu.com/item/%E5%86%85%E5%AE%B9%E5%88%86%E5%8F%91%E7%BD%91%E7%BB%9C/4034265)。CDN是构建在现有网络基础之上的智能虚拟网络，依靠部署在各地的边缘服务器，通过中心平台的负载均衡、内容分发、调度等功能模块，使用户就近获取所需内容，降低网络拥塞，提高用户访问响应速度和命中率。CDN的关键技术主要有内容存储和分发技术。



1. 如何判断目标存在CDN服务?
   1. 利用多节点技术进行请求返回判断
   2. [超级ping](http://ping.chinaz.com/)响应ip不同则存在CND
2. CDN对于安全测试有那些影响?
3. 目前常见的CDN绕过技术有哪些?
   1. 子域名查询
      1. 实例：[xueersi.com](http://xueersi.com/)查找源ip
         1. 写与不写www的区别



* 1. 邮件服务查询
  2. 国外地址请求
  3. 遗留文件，扫描全网
  4. 黑暗引擎搜索特定文件
     1. DNS查找，IP查找，CDN查找，特定文件查找（黑暗搜索引擎）
  5. dns历史记录，以量打量

1. CDN真实IP地址获取后绑定指向地址
2. 更改本地HOSTS解析指向文件