



2.3-IP信息收集

无涯老师

上节课内容回顾

联系人信息 (whois、反查、备案)
子域名信息
DNS解析信息

课程大纲

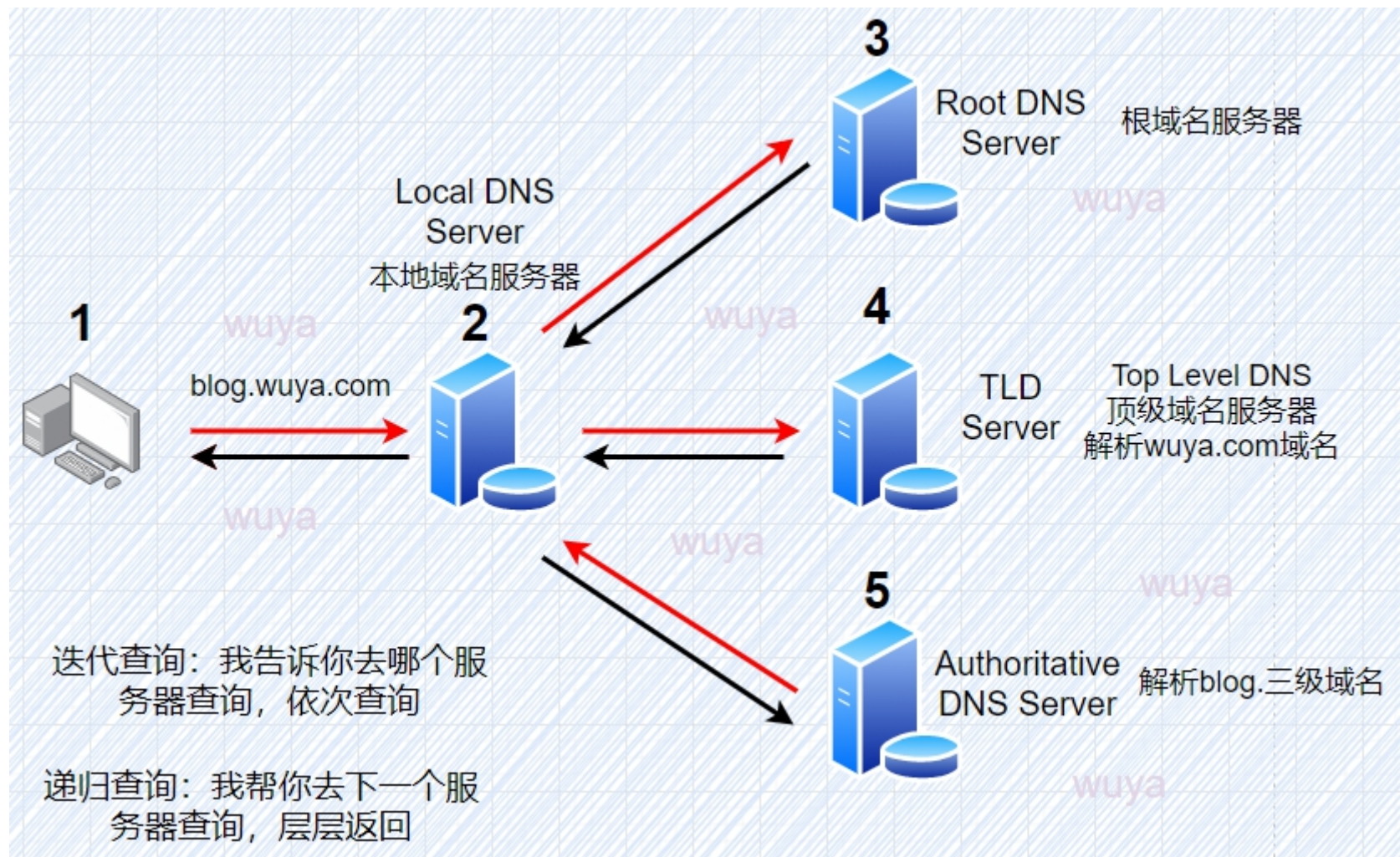
- 1、DNS服务器的类型
- 2、ping / nslookup
- 3、IP归属信息
- 4、如何获取CDN背后的真实IP



01

DNS服务器的类型

DNS解析流程





02 ping / nslookup



PING

Packet Internet Groper
因特网包探索器



 nslookup

```
nslookup -type="MX" baidu.com
```




03 IPI归属



IP归属

<http://ipwhois.cnnic.net.cn/>



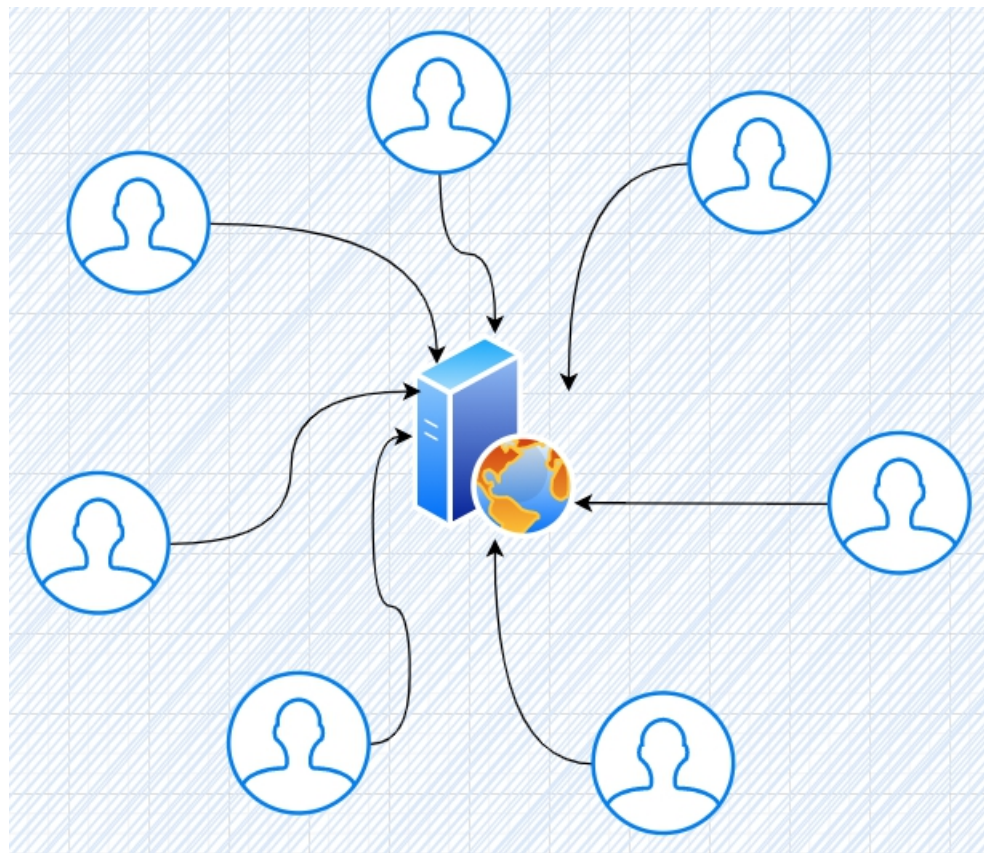
04

如何获取CDN 背后的真实IP

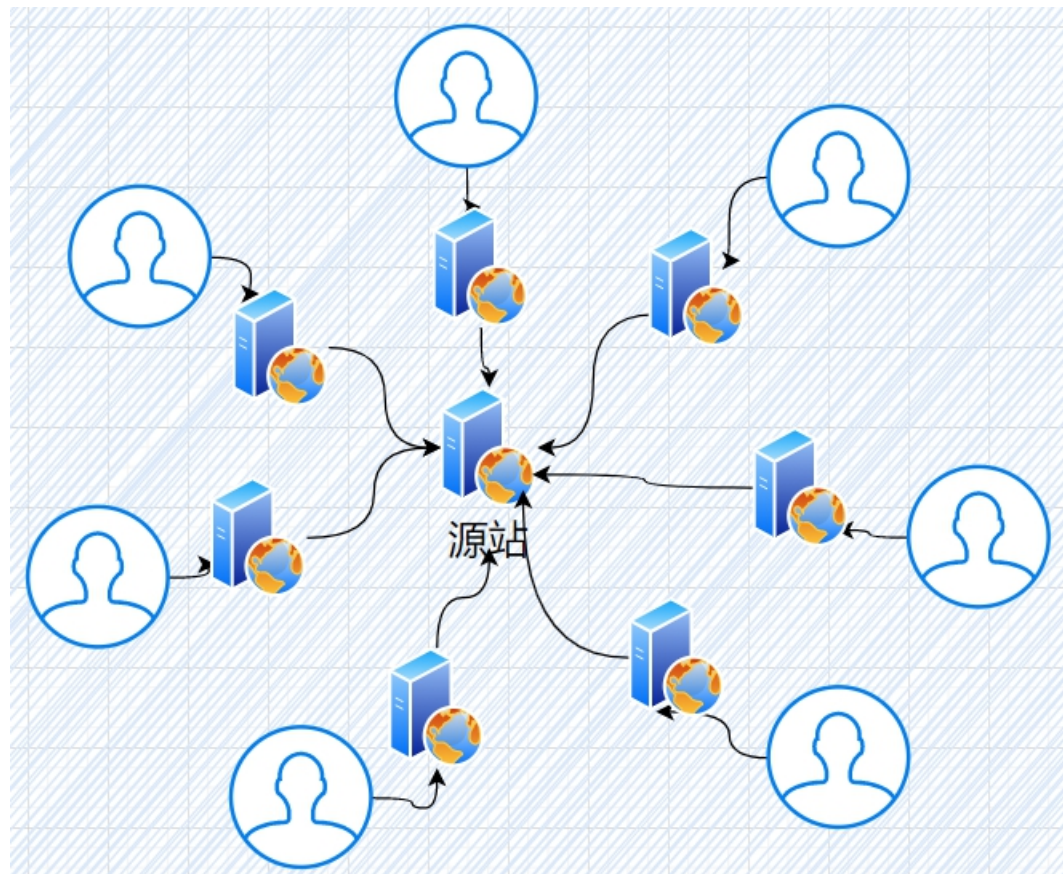
Content Delivery Network

内容分发网络

没有CDN



使用CDN服务



： 常见CDN服务商

CloudFlare/CloudFront.....

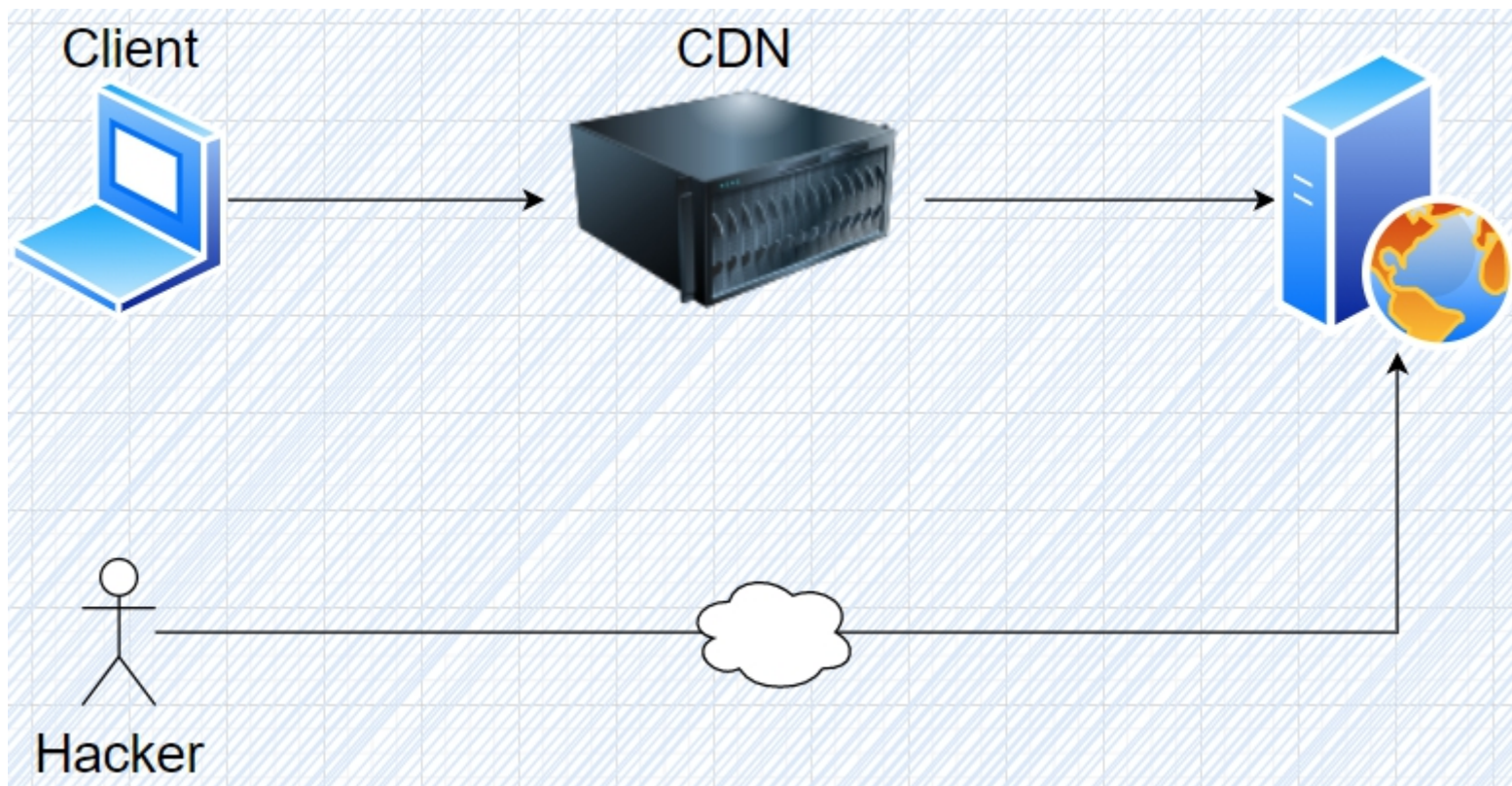
帝联/蓝讯/网宿/七牛云/腾讯/百度/阿里云.....

实现流程（以阿里云为例）

<https://www.zhihu.com/question/36514327/answer/1604554133>

1. 当终端用户（北京）向www.a.com下的指定资源发起请求时，首先向LDNS（本地DNS）发起域名解析请求。
2. LDNS检查缓存中是否有www.a.com的IP地址记录。如果有，则直接返回给终端用户；如果没有，则向授权DNS查询。
3. 当授权DNS解析www.a.com时，返回域名CNAME www.a.tbcdn.com对应IP地址。
4. 域名解析请求发送至阿里云DNS调度系统，并为请求分配最佳节点IP地址。
5. LDNS获取DNS返回的解析IP地址。
6. 用户获取解析IP地址。
7. 用户向获取的IP地址发起对该资源的访问请求。

如何找出真实IP



如何获取CDN背后的真实IP


- 1、超级ping
- 2、历史DNS
- 3、通过子域名查询IP
- 4、国外主机解析
- 5、其他

国外访问

https://asm.ca.com/zh_cn/ping.php
<http://host-tracker.com/>
<http://www.webpagetest.org/>
<https://dnscheck.pingdom.com/>

邮件

```
Received: from mail.abc.com (unknown [218.117.211.62])  
    by newmx32.qq.com (NewMx) with SMTP id  
    for <670...528@qq.com>; Tue, 28 Apr 2020 16:54:57 +0800  
X-QQ-SPAM: true  
X-QQ-FEAT: KBpiTUYH2KyEXwQSbQ2gX7M3q6/lN9sJYvipB7xICpOL7MBAegsDH+pOWaQMj  
    eRTWbF5WxQ7su0VCZ+mVJ35+yGD8NeGMw4+hrJB7m2eH9eBMjtDbAFh8yu4SdcKxoPW6w7E  
    9nMs3GAibuAZz4hTCAg/7GFGovZcprl07/6LZS9mkNa7nKNvfIQMuBBmb4x7q+jg3D+yHAU  
    oUI9cNXbol7Mid+z3vhfnypnEnFW9gH3QflIde2HUKgM9vKvSH5I9Y/EPTimVkJy6SttRHP  
    SymbdQRIT4988PsU5MQFHvhAY=  
X-QQ-MAILINFO: M9mpTqh4QKvq7HMaLmVGaPw/iL6hcy76VxqFmjsoZgowAjp0U1YnKBsaM  
    hSK9asn/cjiRBoj6NIHaw86jDvpyXxLxcjXmpP0rFGc6liqJrG1/wU1tctQf13pEFSp9D1W  
    i4RmJPvIzrgFPC+yjPSxXuY=  
X-QQ-mid: mxsza31t1588064096tw2kxgryn  
X-QQ-ORGSender: admin@test.com
```





Thank you for watching

无涯老师