**DNS污染**

**通过域名无法访问不到网站，但公网IP可正常访问**

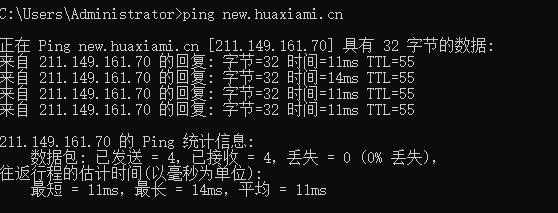
华夏不孕无法访问new.huaxiami.cn，域名无法访问如下图：



**确认DNS是否解析有问题**

1、ping 域名 new.huaxiami.cn

先ping一下域名new.huaxiami.cn，ping 域名后得到解析的ip，如下图：



2 使用IP访问测试

通过ip再访问网站，ip可以正常访问如下图：

3 结论：能够通过 IP地址直接访问网站 页面，但 通过域名却无法访问，这通常说明你的 DNS解析 出现了问题，但网络连接本身没有问题。

查看本机该域名DNS映射

1 查询域名映射

查询本机的该域名映射情况

ipconfig /displaydns

执行后查询本机的该域名映射情况如下图：

2 域名映射结果

从上图中可以看出域名映射的IP与ping出来的可访问IP对不上，确实域名解析出了问题。

3 清除本机使用域名记录

清空本机域名解析结果（有可能之前域名解析错误的），尝试再次解析

ipconfig /flushdns

清空本机DNS解析缓存如下图：



再试，还是有问题，用的是无线网络连接,上层网络设备的dns的问题。

4 本地解析记录

如果解析还有问题，可以在本地手工指定域名与IP对应关系，操作如下：

编辑 C:\Windows\System32\drivers\etc\hosts 文件，增加该域名手工解析记录如下：

[211.149.161.70](http://211.149.161.70) new.huaxiami.cn

小结：

当通过 IP地址 可以正常访问网站，但通过 域名 无法访问时，问题通常出现在DNS解析层面。最常见的原因包括 DNS污染、 DNS缓存 或 DNS配置错误。通过更换DNS服务器、清理DNS缓存或检查 hosts 文件等步骤，通常可以解决问题。

二 DNS污染

DNS污染，也称为DNS劫持或DNS篡改，是一种网络攻击手段，攻击者通过干扰域名解析过程，返回错误的IP地址，导致用户无法访问某些网站或访问被伪造的网站。它主要用于限制或屏蔽用户访问特定的互联网资源，通常由国家、机构或黑客组织实施。

主要原理

当用户输入一个域名（如 www.example.com），DNS服务器负责将域名解析为相应的IP地址。如果DNS污染发生，攻击者会拦截并修改解析请求或响应，返回错误的IP地址。用户可能被引导到虚假站点、完全无法访问目标站点，或被重定向到与预期内容无关的网站。

DNS污染的常见方式

响应篡改：攻击者篡改DNS解析服务器的响应，返回错误的IP地址。

中间人攻击：攻击者拦截并修改客户端与DNS服务器之间的通信。

服务器级劫持：直接在DNS服务器上更改域名记录，使所有用户都被引导到错误的IP地址。

缓存污染：攻击者将恶意的DNS记录存入缓存DNS服务器，导致后续查询结果都受到污染。

如何应对DNS污染

1 使用HTTPS或加密的DNS：

DoH（DNS over HTTPS）：通过加密的HTTPS通道发送DNS请求，防止第三方拦截和篡改。

DoT（DNS over TLS）：使用TLS协议加密DNS请求和响应。

2 使用可靠的DNS服务商：选择不受污染影响的国际DNS服务器，如Google的公共DNS（8.8.8.8）或Cloudflare的DNS（1.1.1.1）。

使用VPN：VPN可以将用户的所有流量通过加密隧道传输，避免本地网络中的DNS污染。

本地hosts文件：通过手动配置本地hosts文件，将域名直接映射到正确的IP地址。

常见DNS污染的现象

无法访问特定网站。

访问网站时跳转到与预期无关的站点。

网站载入缓慢或显示错误页面。

某些应用程序或服务无法正常连接。

这种网络封锁技术通常出现在一些实施互联网内容管控的国家，用于限制特定信息的传播。