# 网宿 HttpDNS 方案

(DNS 防劫持方案)

## 接入指南

网宿科技股份有限公司

2019．09

# Content 目录

# 1. 网宿 HttpDNS 简介

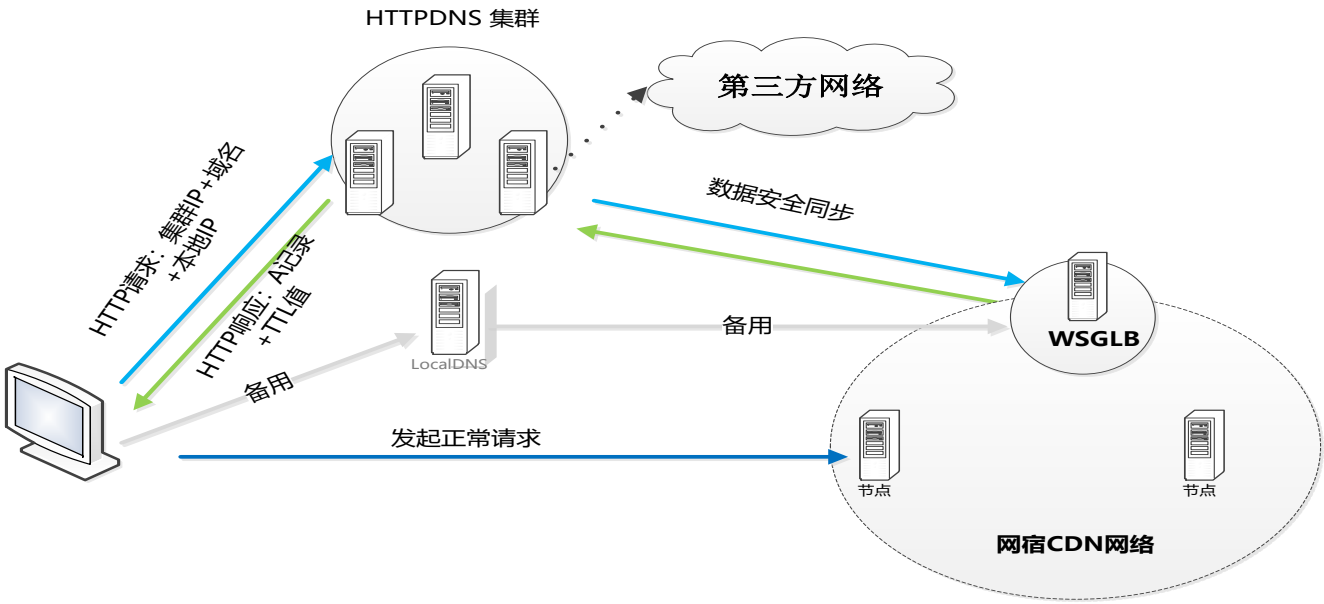
## 1.1. HttpDNS 原理

常规域名解析是通过 DNS 协议进行解析的，其最终结果就是获取域名对应的真实服务器地址，无法绕开 DNS 拦截和故障问题。

而 HttpDNS 则是以 HTTP 的方式代替传统 DNS 协议传递解析结果，能够有效避开 DNS 层面的拦截和故障。客户端通过接口向网宿 HttpDNS 集群发起“DNS 查询”请求，网宿 HttpDNS 集群根据请求携带的域名和 IP 信息，查询 CDN 内部调度策略，通过响应请求的方式，返回给客户端最优节点 IP。客户端得到最优节点 IP，进行正常的业务访问。

## 1.2. 访拓扑图流程

- 拓扑图



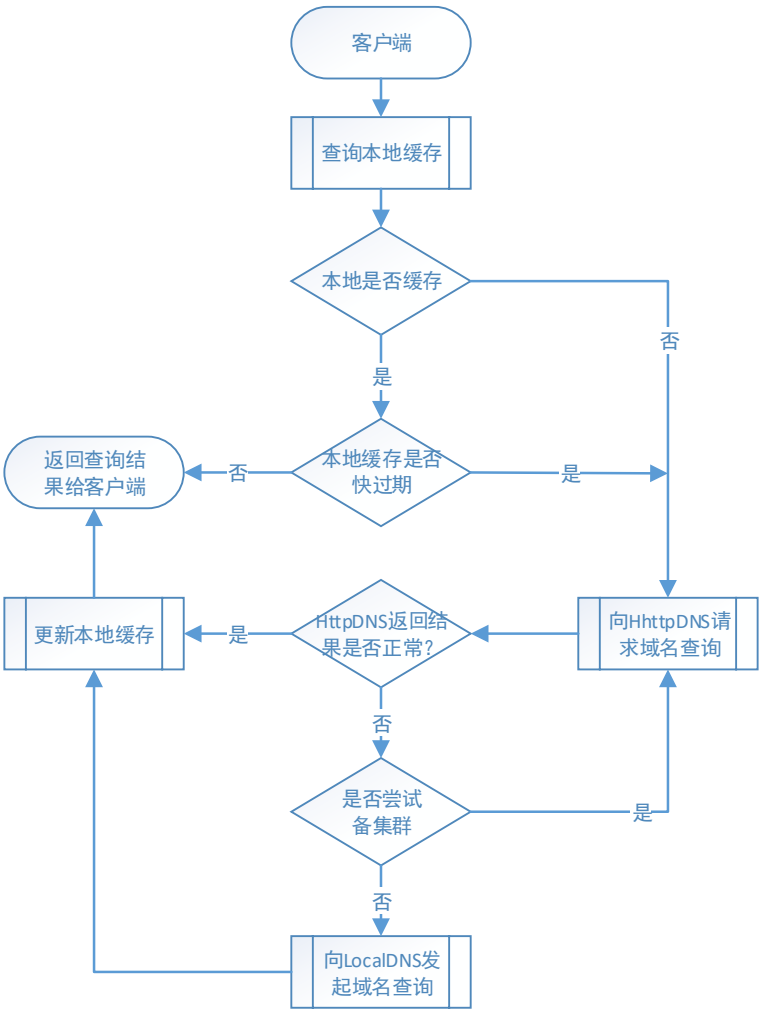

- 访问流程

客户端已根据 **“2.接入指南”** 完成客户端改造，具体客户端与 HTTPDNS 系统的业务流程如下：

1. 客户端向网宿 HttpDNS 中心集群发起查询请求，携带用户域名和终端 IP（可选）。
2. 服务集群查询客户域名的覆盖配置，将域名最佳访问节点 IP 以 HTTP 响应的方式传递给客户端。
3. 客户端，收到响应结果，向节点发起请求。
4. 若客户端向网宿 HttpDNS 集群请求失败，则启用备选，走正常 DNS 解析过程，向 Local DNS 发起请求。
5. LocalDNS 进行递归查询。
6. 最终返回 DNS 结果
7. 客户端拿到最优 IP 后,建立连接,发起正常访问操作

# 2. 接入指南

## 2.1. 客户端逻辑流程图




### 缓存说明

- **缓存策略**

移动互联网用户的网络环境比较复杂，为了尽可能地减少由于域名解析导致的延迟，建议在本地进行缓存。 缓存规则如下：

**① 缓存时间：**

缓存时间建议采用查询得到域名 TTL。在客户端向网宿 HttpDNS 集群发起域名解析请求时，

得到请求响应的实体中会包含域名对应的 TTL 值。

② **缓存更新：**

缓存更新应在以下两种情形下进行：

i. 用户网络状态发生变化时

移动互联网的用户的网络状态由 3G/4G 切 Wi-Fi，Wi-Fi 切 3G/4G 的情况下，其接入点的网络归属可能发生变化。所以用户的网络状态发生变化时，需要重新向网宿 HttpDNS 发起域名解析请求，以获得用户当前网络归属下的最优指向 IP。

ii. 缓存过期时

当域名解析的结果缓存时间到期时，客户端应该向网宿 HttpDNS 重新发起域名解析请求以获取最新的域名对应的 IP。

③ **缓存时间更新优化：**

为了减少用户在缓存过期后重新进行域名解析时的等待时间，建议在 TTL 快过期时（例如达过期时间 75%时）就开始进行域名解析。例如本地缓存的 TTL 为 600s，那么在第 600*0.75=450s 时刻,客户端就应该进行域名解析。

④ **配合缓存的其他建议：**

i. 可在一次 http 请求中同时查询多个域名结果，批量得到结果，减少域名解析的次数，提升了解析效率

ii. 建议在业务允许的情况下，尽量减少域名的数量。如需区分不同的资源，建议通过 url 来进行区分。

## 2.2. 接口使用说明

### 2.2.1. HTTPDNS 服务接入方案（国内，海外）

网宿提供以下 HTTPDNS 服务接入方案,针对不同地区客户提供不同的接入 HTTPDNS 方案：

**1.国内客户：**

⑴在接入过程中，测试期网宿只提供一个测试的 httpdns 服务 IP（测试时由网宿统一提供），如果转正后，可以提供三组 httpDNS 的服务 IP。推荐使用这种方式接入 HTTPDNS 服务。

参数说明，**详见 2.2.2**

⑵https 接入方式（详见 2.2.3）：

a.IP 证书方式接入

b.域名接入方式

**2.海外客户：**

Anycast IP 接入方式，使用 Anycast IP: （由网宿统一提供），保证服务的高可用性。

获取节点 ip 的接口示例：

http://网宿服务 IP/v1/httpdns/clouddns?ws_domain=www.a.com&ws_ret_type=json&ws_cli_IP=1.1.1.1

参数说明，**详见 2.2.2**

### 2.2.2. http 方式

- **客户端请求**

客户端采用 HTTP 方式发起请求，具体内容包括：要查询的加速域名+用户 IP

```
Curl  "http:// httpDNS 服务 ip/v1/httpdns/clouddns?ws_domain= www. chinanetcenter.com.com
&ws_ret_type=json&ws_cli_IP=1.1.1.1 "
```

**参数说明：**

① **httpDNS 服务 ip：** HTTPDNS 调度集群 IP。国内客户测试阶段使用（由网宿统一提供）。

海外地区使用 Anycast IP,：（由网宿统一提供）

②**ws_domain**：客户的请求域名

③**ws_ret_type**：返回包格式，若该值为 json，则返回包格式为 json 格式，若不带该参数，则返回格式为传统的 IP TTL 格式

④**ws_cli_IP** ：客户端 IP，可为空，若为空则表示 HTTPDNS 自动获取建连 IP 作为客户端 IP

- **HttpDNS 响应**

若请求参数带 ret_type=json 则 DNS 解析结果以 json 形式返回，返回格式为：

```
{"msg":"Success","data":{"www.chinanetcenter.com.com":{"ips":["157.185.185.85"],"ttl":300}},"retC
```

```
ode":"0"}
```

若不带 ret_type 则返回普通格式，返回 DNS 解析结果，响应内容格式为：A 记录 TTL 时间

```
157.185.185.85 300
```

客户端根据获取到的 A 记录 IP 进行访问，并根据 TTL 时间实现客户端 DNS 记录缓存。

### 2.2.3. https 方式

#### 1) ip 证书访问的方式

**客户端请求**

客户端采用 HTTPS 方式发起请求，具体内容包括：要查询的加速域名+用户 IP

```
curl –H “edge.wshttpdns.com" https://httpDNS 服务 IP/v1/httpdns/ws_domain=www.
chinanetcenter.com.com& ws_ret_type=json&ws_cli_IP=1.1.1.1" –k
```

**参数说明：**

**①httpDNS 服务 IP**：HTTPDNS 调度集群 IP。海外地区使用 Anycast IP, （由网宿统一提供）

②**ws_domain**：客户的请求域名

③**ws_ret_type**： 返回包格式，若该值为 json，则返回包格式为 json 格式，若不带该参数，则返回格式为传统的 IP TTL 格式

④**ws_cli_IP**： 客户端 IP，可为空，若为空则表示 HTTPDNS 自动获取建连 IP 作为客户端 IP

**Ip 证书访问的验证方式：**

客户端请求主要是告知请求方式，上述例子加了”-k”参数，表示客户端不进行证书校验，对于 APP 端，可采用如下方式完成 httpdns 请求：

- **Android**

```
try {
String url =
"https:// httpDNS 服务 IP /v1/httpdns/clouddns?ws_domain=www.
chinanetcenter.com.com&ws_ret_type=json&ws_cli_IP=1.1.1.1";
```

```
HttpsURLConnection connection = (HttpsURLConnection) new URL(url).openConnection();

connection.setRequestProperty("Host", "edge.wshttpdns.com");
connection.setHostnameVerifier(new HostnameVerifier() {

/*
* 关于这个接口的说明，官方有文档描述：
* This is an extended verification option that implementers can provide.
* It is to be used during a handshake if the URL's hostname does not match the
* peer's identification hostname.
*
* 使用 HTTPDNS 后 URL 里设置的 hostname 不是远程的主机名(如: edge.wshttpdns.com)，
与证书颁发的域不匹配，
* Android HttpsURLConnection 提供了回调接口让用户来处理这种定制化场景。
* 在确认 HTTPDNS 返回的源站 IP 与 Session 携带的 IP 信息一致后，您可以在回调方法中
将待验证域名替换为原来的真实域名进行验证。
*
*/

@Override
public boolean verify(String hostname, SSLSession session) {
return HttpsURLConnection.getDefaultHostnameVerifier().verify("edge.wshttpdns.com",
session);
return false;
}
});

connection.connect();
} catch (Exception e) {
e.printStackTrace();
} finally {
```

```
}
```

- IOS

使用 NSURLSession/NSURLConnection 接口来完成，

**HttpDNS 响应**

若请求参数带 ret_type=json 则 DNS 解析结果以 json 形式返回，返回格式为：

```
{"msg":"Success",
"data":{"www.chinanetcenter.com.com":{"ips":["157.185.185.85"],"ttl":300}},
"retCode":"0"}
```

若不带

ret_type 则返回普通格式，返回 DNS 解析结果，响应内容格式为：A 记录 TTL 时间

```
157.185.185.85    300
```

客户端根据获取到的 A 记录 IP 进行访问，并根据 TTL 时间实现客户端 DNS 记录缓存。

**2) 域名 https 访问的方式**

**客户端请求**

```
curl “https://httpDNS 集群域名/v1/httpdns/clouddns?ws_domain=www.
chinanetcenter.com.com&ws_ret_type=json&ws_cli_IP=223.104.212.138”
```

**参数说明：**

①httpDNS 集群域名： 使用 edge.wshttpdns.com 这个 httpDNS 调度域名。

②**ws_domain**：客户的请求域名

③**ws_ret_type**：返回包格式，若该值为 json，则返回包格式为 json 格式，若不带该参数，则返回格式为传统的 IP TTL 格式

④**ws_cli_IP** ：客户端 IP，可为空，若为空则表示 HTTPDNS 自动获取建连 IP 作为客户端 IP

**HttpDNS 响应**

若请求参数带 ret_type=json 则 DNS 解析结果以 json 形式返回，返回格式为：

```
{"msg":"Success",
"data":{"www. chinanetcenter.com.com":{"ips":["157.185.185.85"],"ttl":300}},
"retCode":"0"}
```

若不带

ret_type 则返回普通格式，返回 DNS 解析结果，响应内容格式为：A 记录 TTL 时间

```
157.185.185.85    300
```

客户端根据获取到的 A 记录 IP 进行访问，并根据 TTL 时间实现客户端 DNS 记录缓存。

### 2.2.4. 多频道查询

支持同一个 HttpDNS 请求中带多个频道请求（多个域名以分号分隔）；并且在响应的时候，根据网宿自定义的个数，返回多个频道的解析 A 记录。下面以 http 方式的形式举例，https 的情景类似：

- **客户端请求**

```
http://ip/v1/httpdns/clouddns?ws_domain=www.
chinanetcenter.com.com;www.quansucloud.com&ws_ret_type=json
```

- **HTTPDNS 响应（非 json 格式）**

```
36.250.248.66 300
222.138.255.254 300

112.91.133.117 300
```

- **HTTPDNS 响应（json 格式）**

```
{"msg":"Success",
"data":{"www.quansucloud.com":{"ips":["112.91.133.117"],"ttl":300},"www.
chinanetcenter.com.com":{"ips":["36.250.248.66","222.138.255.254"],"ttl":300}},
"retCode":"0"}
```

## 2.3. 注意事项

- **故障切换策略**

  虽然网宿 HttpDNS 集群已经接入 BGP Anycast，并实现了多地跨机房容灾。但为了保证在最坏的情况下客户端域名解析依然不受影响。建议采用以下的故障切换保障策略：

  ① 第一步先向首选网宿 HttpDNS 集群发起域名查询请求。

  ② 如果查询返回的结果不是一个 IP 地址（结果为空、结果非 IP、连接超时等），则尝试下一个集群或者直接通过本地 LocalDNS 进行域名解析。超时时间建议为 5s。注意，返回结果为空可能情况为参数错误或者域名未开启 HttpDNS 服务，返回的状态码仍然是 200。

- **日志记录**

  为了方便排查问题，需要记录提供服务的 HTTPDNS IP 是哪一个，以及日志输出记录是获取到哪些节点 ip 等相关信息。建议采用以下的日志记录策略：

  ① 记录提供服务的 HTTPDNS 服务 IP 信息

  ② 记录通过 HTTPDNS 集群获取到的节点 IP 信息

  ③ 记录访问资源时所使用的节点 IP 信息

  ④ 记录客户端的 IP 信息

# 附录 1 错误码

| retCode | 含义 |
| --- | --- |
| 0 | 成功 |
| 1 | 参数错误 |
| 2 | 请求超时 |
| 3 | 其他错误 |