5G 企业专网 DNS 实现方案探讨

杨少龙，刘英双，魏颖琪，黄粤
（中国电信股份有限公司研究院，广东 广州 510630）

摘　要：在 5G 企业专网中，如何正确地对内外网的域名进行解析，成为专网建设中一个亟须解决的难题。UPF 下沉组网方式下 5G 移动用户无法使用内网 DNS 进行域名解析，针对这一问题，提出了 4 种 5G 企业专网 DNS 的解决方案，并对这 4 种方案进行了对比。

关键字：5G 专网；域名解析；数据分流
中图分类号：TN929.5
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2022118

Research on DNS implementation scheme of 5G enterprise private network

YANG Shaolong, LIU Yingshuang, WEI Yingqi, HUANG Yue
Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

Abstract: How to correctly parse the domain name of the internal and external networks in the 5G enterprise private network? It is a problem that needs to be solved urgently in the construction of the 5G private network. In the UPF sinking networking mode, 5G mobile users cannot use intranet DNS for domain name resolution. Four 5G enterprise private network DNS solutions were proposed and compared.

Key words: 5G private network, DNS, data diversion

0　引言

随着 5G 技术不断发展，5G 企业专网逐渐走向商用，正以独特的技术优势赋能千行百业、助力行业数字化转型。在新一轮数字化浪潮中，各大运营商更加关注 5G 专用网络（private 5G network）在垂直行业的应用，它使用 5G 技术为垂直行业提供具有统一连接性、优化服务和特定区域内安全通信方式的专用网络。例如，中国电信 5G 专网[1]提供 3 种模式：致远、比邻和如翼，用于满足企业个性化的网络需求，如时延要求、可靠性要求、上行速率需求、数据安全和隔离要求等，配合 MEC、天翼云，最大化发挥云边协同优势，为行业客户的数字化应用赋能。

在 5G 专网建设中，低时延、企业数据不出园区、公网中业务不中断等是企业最为显著的诉求。无论在公网还是在内网中，都有成千上万的业务在运营，为便于记住各个服务的访问地址，

收稿日期：2021−10−29；修回日期：2022−03−18

通常采用域名（domain name，DN）进行映射，用户通过访问该域名便可使用其提供的服务。同样，5G 专网内移动用户也希望使用域名访问内网和公网的服务，但一般情况下，5G 专网给移动用户配置的 DNS 是公网的 DNS 服务器，而公网的 DNS 服务器解析不了内网的域名（公网域名服务器没有内网的域名记录），因此用户无法通过域名访问内网服务。如果要在 5G 专网中使用 DNS，必须要正确处理移动用户的 DNS 请求，选择正确的域名服务器进行有效的域名解析。

在内网架设 DNS 服务器的前提下，如何使 5G 专网用户选择到正确的 DNS 服务器，成为电信运营商亟待解决的问题。

1 5G 企业专网 DNS 解决方案

在探讨 5G 专网 DNS 解决方案之前，先了解一下 5G 专网的组网方式。5G 专网建设方案很多，典型的组网方式有两种：独立 5GC 组网方式和 UPF 下沉组网方式。

独立 5GC 组网方式指在一定地域或一定行业范围内，与 5G 公网共享基站，独立部署 5GC-CP（AMF/SMF）、UDM、UPF 等基本网元[2]，通过共享频段实现网络建设、实现数据通信。这种网络部署方式具有数据信息高度保密、网络特性高度定制的特点。独立 5GC 组网方式如图 1 所示。

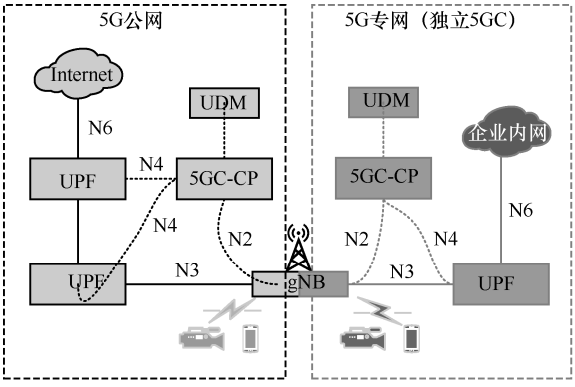


图 1 独立 5GC 组网方式

UPF 下沉组网方式是通过 5G 数据分流技术，将核心网部分功能从运营商核心网下沉至行业客户专网侧，主要是 UPF 下沉至企业专网侧。无线侧可根据需求，利用公网实现或在特定区域加装无线基站设备。这种网络部署方式是部分独享、部分与公众网络共享的模式，能够实现数据本地处理、网络功能定制。UPF 下沉组网方式如图 2 所示。

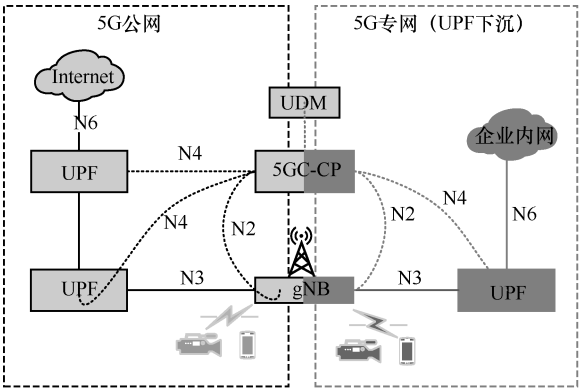


图 2 UPF 下沉组网方式

无论采用上述的两种组网方式，还是采用其他的组网方式，移动用户在接入网络后，均由 5GC 分配指定的 DNS 服务器[3]。通常情况下，给移动用户分配的是 5G 公网的 DNS 服务器，也就意味着用户通过域名访问方式只能访问 5G 公网和 Internet 网上发布的服务，并不能访问企业内部网存在的私有域名对应的服务。究其原因，主要是 5G 公网 DNS 服务器中没有企业内部 DNS 服务器的 DNS 记录，也就无法对其内网域名进行地址转换。这样 5G 专网中的移动用户无法使用内网 DNS 进行域名解析访问内网服务，用户体验较差，同时也未能满足企业内部 DNS 的应用需求。针对这一问题，本文提出了如下 4 种 5G 专网 DNS 解决方案。

1.1 方案 1 签约方式

签约方式指用户数据的签约，需要将 5G 专网用户签约为特定的 DNN 或特定的切片，然后指定特定的 IP 地址为内网的 DNS 服务器。其中

用户签约数据将存储在 5G 公网或者 5G 专网的 UDM，用于与移动用户进行数据交互。UE 注册到该 5G 专网时，就能从 5GC 中获得内网的 DNS 服务器的 IP 地址。UE 的所有 DNS 请求，都可以发往内网的 DNS 服务器。需要特别注意的是 5G 网络中 DNS 没有用户级别，只能基于 DNN 或切片进行网络划分并分配给该网络指定的 DNS 服务器。基于签约方式的 DNS 解决方案业务处理流程如图 3 所示。

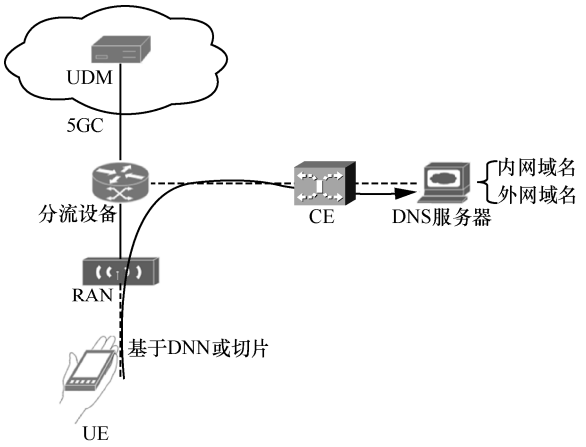


图 3　基于签约方式的 DNS 解决方案业务处理流程

步骤 1　使用已签约的移动用户接入 5G 专网，进行接入验证后，根据签约数据，5G 专网中的 5GC 将会给该用户指定内网 DNS 服务器作为域名解析服务器。

步骤 2　5G 专网移动用户所有 DNS 请求将由 UPF 分流至内网，由内网中的 DNS 服务器进行解析，回复 DNS 请求。

步骤 3　内网中的 DNS 服务器需要能够对因特网及内网的所有域名进行解析，以保证移动用户既可以访问内网服务，也可以访问公网服务。

由于 5G 专网 UE 所有的 DNS 请求将发送到该内网 DNS 服务器上，如果专网 UE 有访问公网的需求，那么要求内网的 DNS 服务器包括内网和公网的域名。内网 DNS 服务器在拥有内网的域名信息的同时，也要能解析公网的域名，这就要求内网的 DNS 服务器能访问公网，当用户请求公网域名解析时，内网的 DNS 服务器能访问公网进行域名解析。这对于那些要求高安全、高隔离的安全敏感型政企客户可能难以接受。

此方案通过签约方式实现，不影响公网用户，也不需要网络进行任何变动，在现有的网络组网中已可以实现，但需要 5G 专网内部 DNS 服务器配合。

1.2　方案 2 DNS 代理方式

DNS 代理方式指通过分流设备把所有的 DNS 请求发往内网的 DNS 服务器，内网 DNS 服务器采用代理方式提供全部域名的解析，包括内网和公网的域名。这种方式下 UE 无特殊签约数据，UE 分配的 DNS 是运营商提供的公众 DNS，但实际提供 DNS 服务的是内网的 DNS 服务器。DNS 代理方式数据流程如图 4 所示。

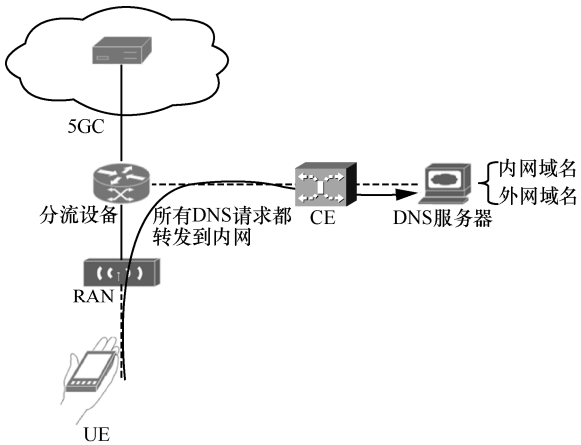


图 4　DNS 代理方式数据流程

此方案要求分流设备能转发 DNS 请求和响应。分流设备转发的依据是：只要是 DNS 请求，一律转发到内网。什么样的数据包是 DNS 请求？只要 UDP 层的目的端口等于 53，该数据包就被认为是 DNS 请求。同样，回复的数据包只要 UDP 层的源端口等于 53，则认为该数据包是 DNS 请求的回应包。

此方案中，需要对无线侧的 GTPU 包信息进行处理，需要了解其数据结构，同时也要对必要信息进行缓存，主要包括 Tied、DNS 请求中的

TransactionID 和 5G 公网 DNS 服务器 IP，用于对 DNS 请求与 DNS 回复进行匹配和修改对应的 GTPU 信息。

方案中关键功能实现集中在分流设备中，其中 DNS 代理方式业务处理流程如图 5 所示。

步骤 1 UE 发送 DNS 请求至 RAN，分流设备接收来自 RAN 侧的所有数据包，对 overlay 中 UDP 层的目的端口等于 53 的所有数据包进行拦截过滤。

步骤 2 拆除 DNS 请求中的 GTPU 包头，将 DNS 请求中的目的地址改成内网对应的 DNS 服务器地址，转发至企业内网。

步骤 3 企业内网 DNS 服务器进行 DNS 解析，若为内网域名，则处理请求并进行 DNS 回复；否则，代理转发至公网 DNS 服务器进行解析并等待回复。

步骤 4 分流设备收到企业内网中 DNS 回复后，根据 TransactionID 找到缓存的 DNS 请求相关信息（公网 DNS 服务器地址、UE 地址等），增加 GTPU 信息，修改 DNS 回复中源地址为公网 DNS 服务器地址，发送至 RAN。

步骤 5 RAN 通过外线将数据传送到 UE。

此方案与方案 1 类似，唯一的区别是不区分内网用户和公网用户，也不需要用户进行特殊的签约。只要用户注册到该 5G 专网，那么所有的 DNS 请求就会指向内网的 DNS 服务器。如果存在公网用户可以接入企业专网的情况，那么同样要求内网的 DNS 服务器包括内网和公网的域名，也就同样要求内网的 DNS 服务器能访问公网。这对于那些要求高安全、高隔离的安全敏感型政企客户同样难以接受。

对上述的处理流程进行实际实验。内网 DNS 服务器均以缓存测试需要的域名解析记录，发送 DNS 请求，使用工具抓包分析，不记空口接入时延，那么该方案时延在 3 ms 左右，DNS 代理方式业务处理时延如图 6 所示。

1.3 方案 3 DNS 分流方式

DNS 分流方式指通过分流设备识别 DNS 请求中的内网域名和公网域名，内网域名的 DNS 请求发往内网 DNS 服务器，公网域名的 DNS 请

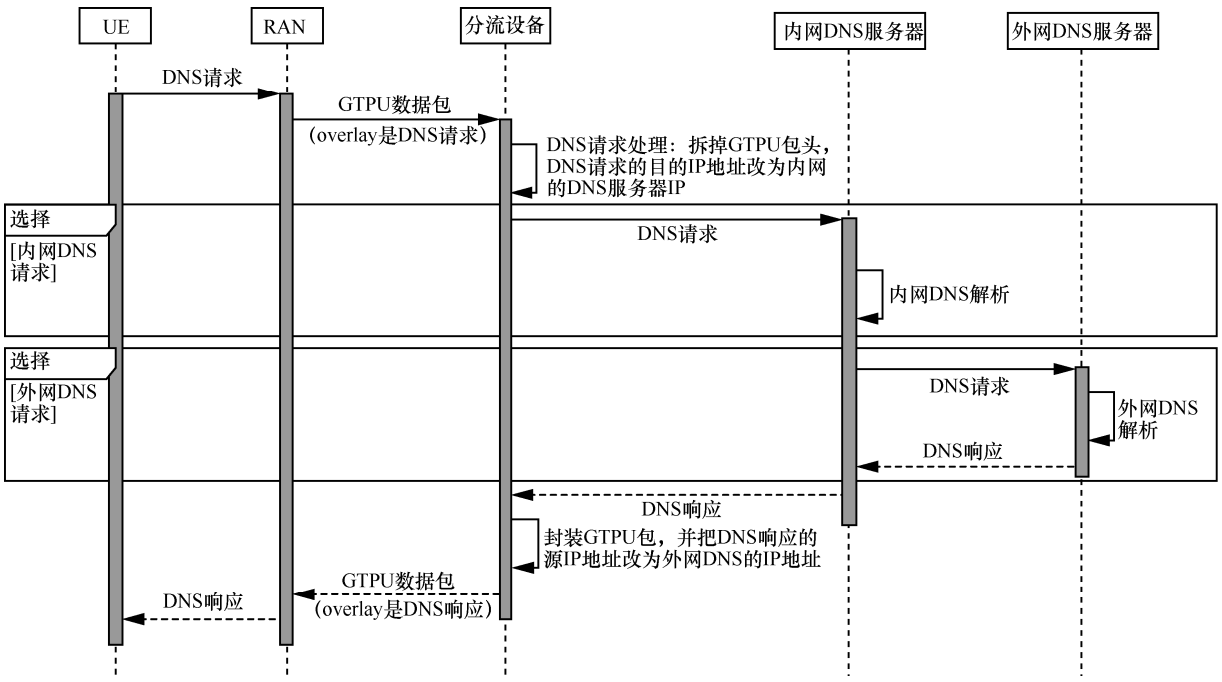


图 5 DNS 代理方式业务处理流程

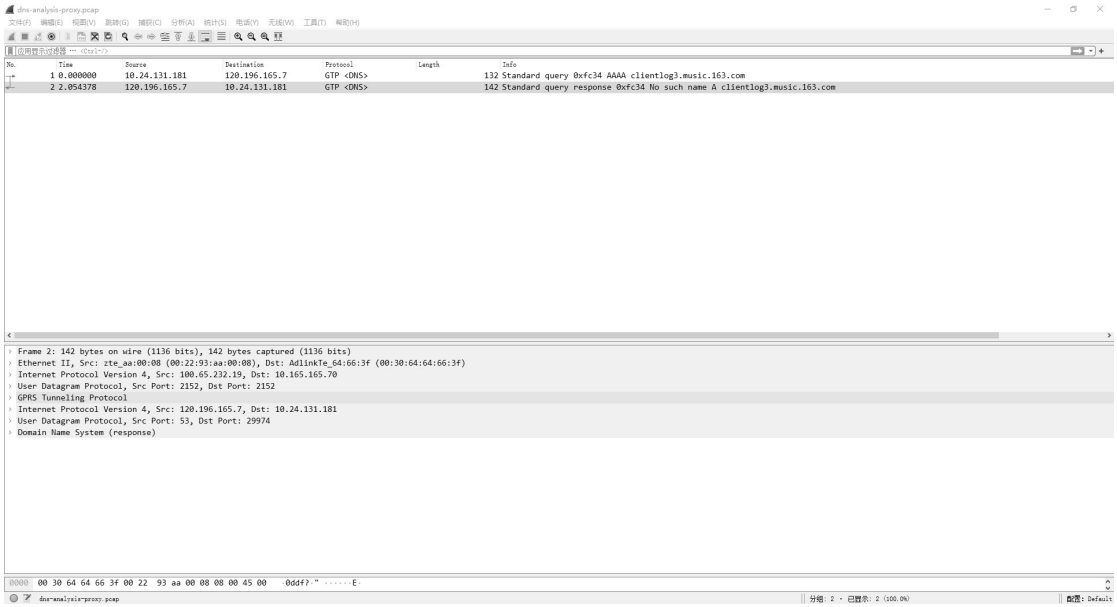


图 6　DNS 代理方式业务处理时延

求发往公网的 DNS 服务器。这种方式下 UE 无特殊签约数据，也无须区分内网和公网用户。DNS 分流方式数据流程如图 7 所示。

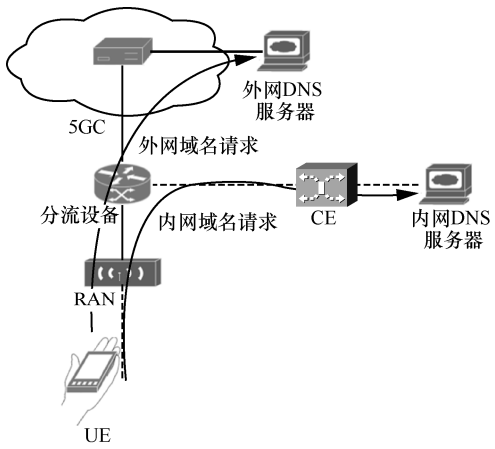


图 7　DNS 分流方式数据流程

分流设备需要预先设置哪些是内网域名。当收到 RAN 发出的 overlay 为 DNS 请求的 GTPU 数据包时，分流设备通过判断 DNS 请求的域名是否包含在设置的内网域名内，如果存在，则拆掉 GTPU 包头，发往内网的 DNS 服务器；如果不存在，则认为是公网的 DNS 域名请求，则原封不动地送往公网的 DNS 服务器进行域名解析。

此方案中，需要对无线侧的 GTPU 信息和 DNS 信息进行处理，需要了解它们的数据结构，同时也要对必要信息进行缓存，主要包括 Tied、DNS 请求中的 TransactionID 和 5G 公网 DNS 服务器 IP，用于对 DNS 请求与 DNS 回复进行匹配和修改对应的 GTPU 信息。

方案中关键功能实现集中在分流设备中，其中 DNS 分流方式业务处理流程如图 8 所示。

步骤 1　UE 发送 DNS 请求至 RAN，分流设备接收来自 RAN 侧的所有数据包，对 overlay 中 UDP 层的目的端口等于 53 的所有数据包进行拦截过滤。

步骤 2　获取 DNS 请求中需要解析的域名，判断该域名是否存在于分流设备所缓存的内网域名中。

步骤 3　如果请求域名存在于分流设备所缓存的内网域名中，则拆除 DNS 请求中的 GTPU 包头，将 DNS 请求中的目的地址改成内网对应的 DNS 服务器地址，转发至企业内网。由内网解析返回 DNS 响应，分流设备接收到 DNS 响应后，根据 TransactionID 找到缓存的 DNS 请求相关信息，有公网 DNS 服务器地址、UE 地址等，增加

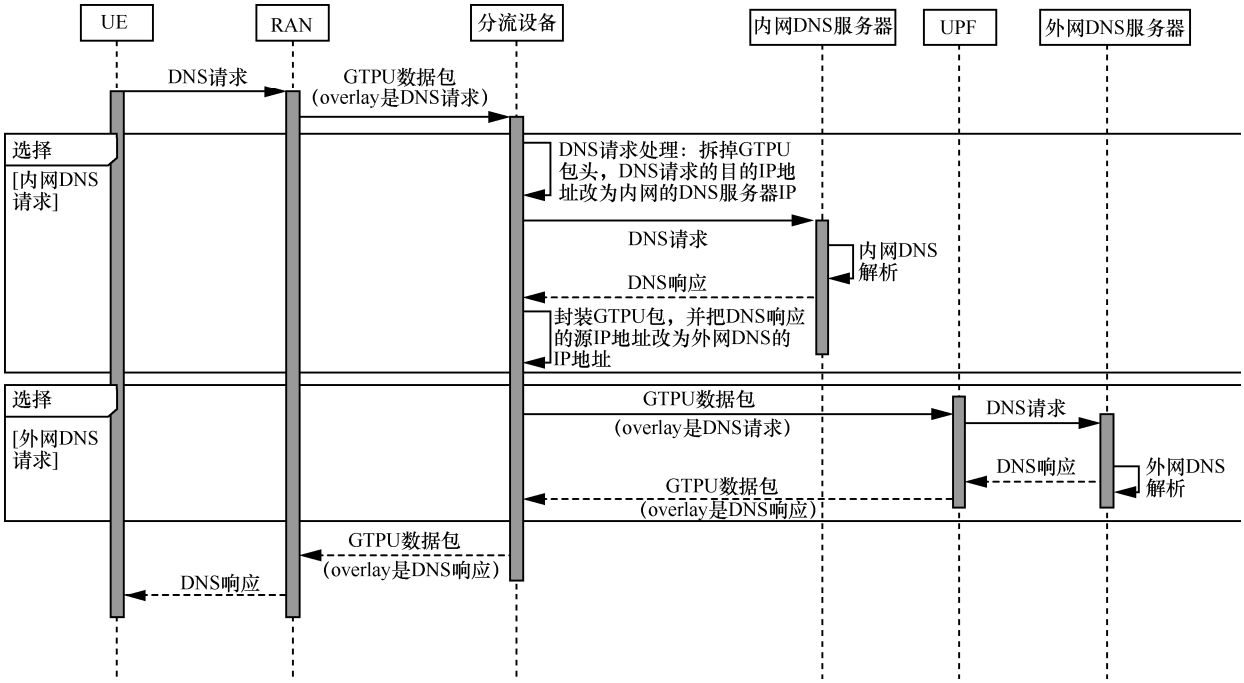


图 8　DNS 分流方式业务处理流程

GTPU 信息，修改 DNS 回复中源地址为公网 DNS 服务器地址，发送至 RAN。

步骤 4　如不存在于分流设备所缓存的内网域名中，将请求转发至 UPF，由其路由至 5G 公网中的 DNS 服务器进行域名解析并返回 DNS 响应。分流设备接收到响应后，无须处理，直接转发至 RAN。

步骤 5　RAN 通过外线将数据传送到 UE。

此方案相较于前两种方案更加安全，无须内网 DNS 服务器访问公网。该方案不区分内网用户和公网用户，也不需要用户进行特殊的签约。相较于 DNS 代理方式，分流设备需要额外设置内网域名，用于区分 DNS 请求时是内网 DNS 请求还是公网 DNS 请求，这样能够更加精准地对 DNS 请求进行分流至内外网。这对于那些要求高安全、高隔离的安全敏感型政企客户更容易接受。

对上述的处理流程进行实际实验，发送内网 DNS 请求，不记空口接入时延，那么该方案产生的时延与 DNS 代理方式时延差不多，均在 3 ms 左右。访问大网域名服务器时延则与未改造的 5G 网络时延一致。

1.4　方案 4 DNS 缓存方式

DNS 缓存方式指在分流设备中缓存 5G 专网的域名解析记录，当 UE 进行专网域名的 DNS 请求时，分流设备直接从 DNS 缓存中把域名解析为相应的 IP 地址，并回复 DNS 响应给 UE。如果 UE 请求的是公网的域名，则透明转发到公网的 DNS 服务器。DNS 缓存方式数据流程如图 9 所示。

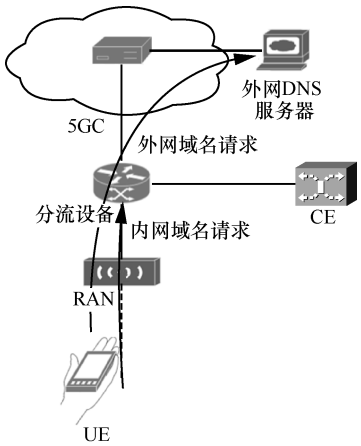


图 9　DNS 缓存方式数据流程

分流设备需要预先设置域名解析记录，此时分流设备也相当于简单的 DNS 服务器。当收到

RAN 发出的 overlay 为 DNS 请求的 GTPU 数据包时，分流设备通过判断 DNS 请求的域名是否存在于分流设备的 DNS 缓存中，如果存在，则生成 DNS 响应数据包，封装 GTPU 包头并回复 DNS 响应给 RAN；如果不存在，则认为是公网的 DNS 域名请求，则原封不动地送往公网的 DNS 服务器进行域名解析。

此方案中，需要对无线侧的 GTPU 信息和 DNS 请求进行处理，需要了解它们的数据结构，同时也要生成对应的 DNS 响应数据包，也需要了解 DNS 响应包数据结构。在生成 DNS 响应数据包时，需要使用到 Tied、DNS 请求中的 TransactionID 和 5G 公网 DNS 服务器 IP 地址，用于组包生成 GTPU 信息和 DNS 响应包。

方案中关键功能实现集中在分流设备中，它充当 DNS 服务器的角色，其中 DNS 缓存方式业务处理流程如图 10 所示。

步骤 1　UE 发送 DNS 请求至 RAN，分流设备接收来自 RAN 侧的所有数据包，对 overlay 中 UDP 层的目的端口等于 53 的所有数据包进行拦截过滤。

步骤 2　拆除 DNS 请求中的 GTPU 包头，将 DNS 请求发送至本地分流设备 LFC 的 DNS 缓存功能模块进行处理，查询分流设备中的 DNS 缓存，查看是否命中 DNS 缓存记录。

步骤 3　如果 DNS 请求命中 DNS 缓存记录，则生成 DNS 响应包，然后交给本地分流设备 LFC 的封包功能模块进行 GTPU 封包，最后发送至 RAN。

步骤 4　如果未能命中 DNS 缓存记录，则认为是公网域名，不做任何处理，直接转发 UPF，由其路由至 5G 公网中的 DNS 服务器。分流设备收到 UPF 回复的 DNS 响应后，不需要进行处理，直接转发至 RAN。

步骤 5　RAN 通过外线将数据传送到 UE。

此方案中分流设备兼具内网 DNS 服务器的功能。但由于分流设备不与公网连通，域名解析的输入和变更主要靠命令进行，所以此方案适合于小规模网络。

对上述的处理流程进行实际实验，发送 DNS 请求，使用工具抓包分析，不计空口接入时延，

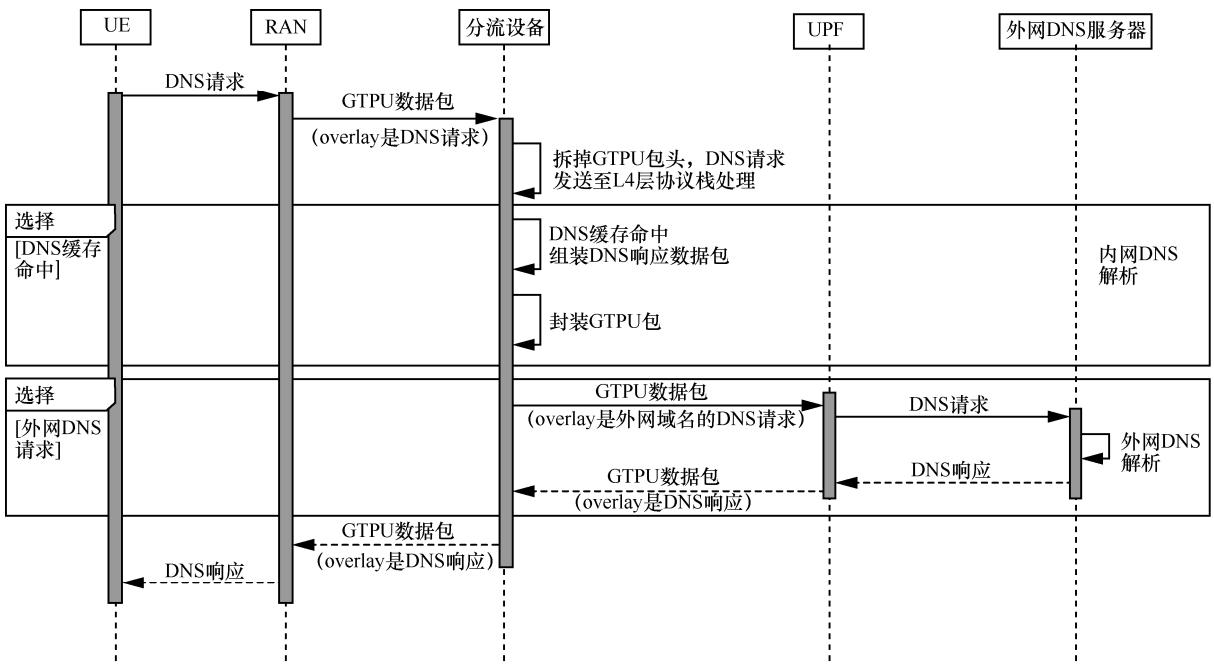


图 10　DNS 缓存方式业务处理流程

那么该方案时延小于 1 ms，DNS 缓存方式时延测试如图 11 所示。

2 5G 企业专网 DNS 方案比较

前面介绍的 4 种 5G 专网 DNS 方案多个维度对比见表 1。

从方案的特点来比较，用户签约方式不需要网络改造，但由于需要用户签约特殊属性，对用户的影响较大，而且需要内网 DNS 连通公网。DNS 代理和 DNS 分流方案基本类似，不需要用户签约，都是在分流设备上做转发；DNS 代理要求内网 DNS 连通内网，DNS 分流不需要。DNS 缓存方式对分流设备要求更高，不但需要转发，更兼具 DNS 解析的功能，DNS 缓存方式不需要内网连通公网。

从方案的安全性来看，4 种方案是不同的。方案安全性的衡量标准主要在于企业内网是否需要连通外网。用户签约和 DNS 代理两种方案要求企业内网必须连通外网，对安全隔离要求比较高的企业来说，这是不可以接受的。DNS 分流和 DNS 缓存不需要企业内网连通外网，因此后两者的方案的安全性相对较高。

从实现难易程度来看，4 个方案实现方式对网络要求不一样，其实现难易程度也有区别。用户签约特殊属性方案签约的是特定的 DNN 或特定的切片，指定域名解析服务器为内网的 DNS 服务器，由 UPF 对专网数据进行企业专网分流，无须改造现有网络，无分流设备研发，相对容易

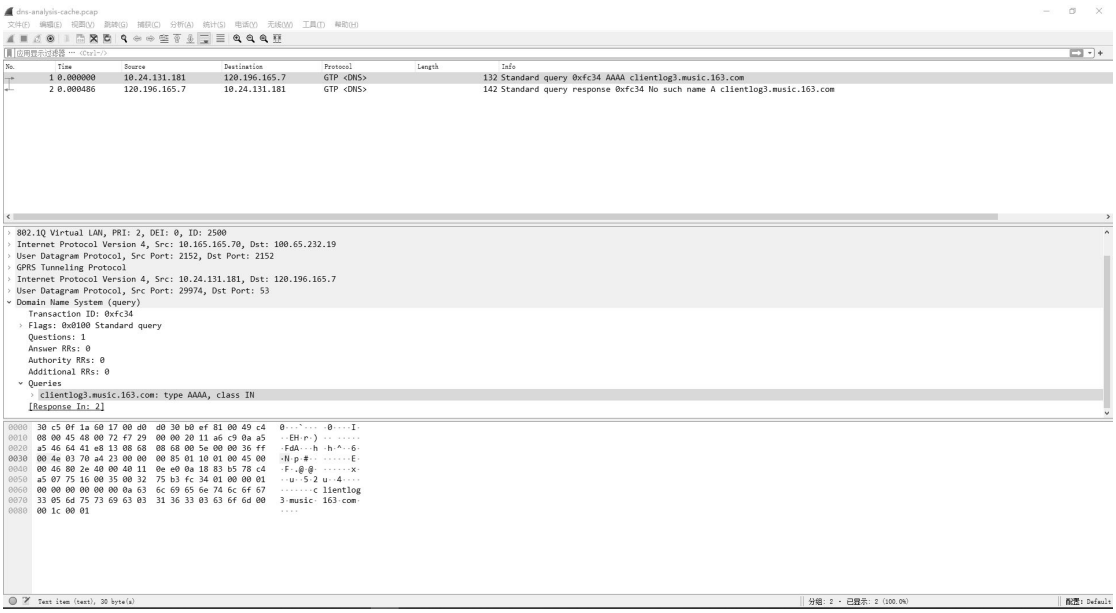


图 11 DNS 缓存方式时延测试

表 1 4 种 5G 专网 DNS 方案多个维度对比

方案	用户签约	DNS 代理	DNS 分流	DNS 缓存
需要用户签约特殊属性	需要	不需要	不需要	不需要
是否网络改造	不需要	需要	需要	需要
是否需要内网连通公网	需要	需要	不需要	不需要
实现难易度	容易	一般	一般	较高
适合场景	大中规模	中规模	中规模	小规模

实现。其他 3 个方案都需要对 5G 网络进行改造。对现有 5G 网络改造，会涉及网络规划、数据分流（需要增加分流设备以实现不同用户内外网 DNS 数据的分流）、软件开发实现上存在不同难度。另外对企业内网的要求也影响实现的难易程度：如对企业内网有特殊要求，对不同方案落地会有影响；如企业内网可通外网，用户 DNS 数据可全分流至企业内网，无须对 DNS 数据区分内外网区分进行分流，分流设备功能实现简单，对方案实现难易程度会有所降低。DNS 缓存方式既需要对网络进行改造，同时也需要区分内外网的 DNS 请求，因此实现难度是最高的。

从适用场景来看，4 种方案有各自的适应场景。方案适用场景的主要衡量标准有两点：网络改造实施难易程度和方案落地后维护难易程度。用户签约方式不需要网络改造，不影响原有的网络拓扑，相当于是透明接入，所以在网络改造实施方面能够很好地适用于大中规模企业。DNS 代理方式由统一的内网 DNS 服务器解析内外网域名请求；DNS 分流方式区分内外网 DNS 请求由分流器分流至内外网 DNS 服务器解析，两者实施难度一般，所以能适用于中规模企业。DNS 缓存方式需要进行网络改造，由本地 DNS Cache 处理内网 DNS 请求。本地 DNS Cache 需要结合内网域名对应 IP 地址的变化设置和维护一个内网 DNS 记录，需要根据企业内网域名变化维护方案中对应设备配置。企业规模越大，后期维护工作量就越大，因此 DNS Cache 方式只适合于小规模企业。

综上所述，4 种方案各有自身的特点，实现难度不一样，适用的企业应用场景也各不相同。5G 专网用户可以根据自身的情况进行选择。

3　结束语

DNS 用域名代替难记的 IP 地址，使用户能很方便访问网络，但在 5G 企业专网中，由于域名有内网域名和外网域名的区别，使得 DNS 在 5G 企业专网的实际应用迎来了新的挑战。本文提出了 4 种解决 5G 企业专网内 DNS 选路的方案：用户签约、DNS 代理、DNS 分流和 DNS 缓存。每一种方案有每一种的方式和特点，各有千秋。

业界对 5G 企业专网一直寄予厚望。对于 5G 专网而言，资费定价、服务差异化、网络安全等仍然面临着艰巨的挑战，需要产业界的持续投入和探索。尽管在发展过程中伴随着一定的挑战，但随着技术的不断完善，专网部署数量也开始不断增加。相信不久的未来，5G 企业专网一定能得到更多的部署和应用，真正实现 5G 赋能千行百业的目标。

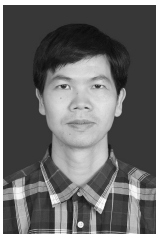
参考文献：

[1] 中国电信集团有限公司. 中国电信 5G 定制网产品手册[R]. 2020.
China Telecom Group Co., Ltd. China Telecom 5G customized network product manual[R]. 2020.

[2] 3GPP. Technical specification group services and system aspects; system architecture for the 5G system (5GS): TS23.501[S]. 2008.

[3] 3GPP. Technical specification group services and system aspects; procedures for the 5G system (5GS): TS 23.502[S]. 2008.

[作者简介]



杨少龙（1978− ），男，中国电信股份有限公司研究院工程师，主要从事行业应用产品与解决方案的研究与开发工作。

刘英双（1988− ），男，中国电信股份有限公司研究院工程师，主要从事行业应用产品与解决方案的研究与开发工作。

魏颖琪（1974− ），女，中国电信股份有限公司研究院高级工程师，主要从事产品研发工作。

黄粤（1981− ），男，中国电信股份有限公司研究院工程师，主要从事行业应用产品与解决方案的研究与开发工作。