互联网名称与数字地址分配机构

标识符技术创新报告

2014 年 5 月 15 日

目录

1. 简介

标识符技术创新（ITI）专家组经互联网名称与数字地址分配机构（ICANN）特许成立，目的如下：

1. 制定关于域名系统（DNS）和其他标识符的技术路线图

2. 制定最佳实践建议和参考体系

3. 为 ICANN 的运营、安全、政策和技术职能部门提供技术指导

4. 在技术问题上与 ICANN 机构社群和公众交流合作

专家组成员于 2013 年 9 月到 10 月选出，保罗·莫卡普利斯（Paul Mockapetris） 被任命为主席。所有成员以个人身份任职，他们所属的组织机构仅用于识别目的：

- 雅里·阿科（Jari Arkko）——互联网工程任务组（IETF）主席
- 里克·鲍威（Rick Boivie）——IBM Thomas J. Watson 研究中心
- 安妮-玛丽·埃克伦-洛温德（Anne-Marie Eklund-Löwinder）——互联网基础设施基金会安全经理
- 杰夫·休士顿（Geoff Huston）——亚太网络信息中心首席科学家
- 庄振宏（James Seng）——黄道（Zodiac Holdings ）首席执行官
- 保罗·维克西（Paul Vixie）——Farsight Security 首席执行官
- 张丽霞 ——加州大学洛杉矶分校波斯特尔（ Postel）计算机科学系主席

2013 年 11 月在温哥华的 IETF 会议上、同月在 ICANN 布宜诺斯艾利斯会议上以及 2014 年 1 月在 ICANN 洛杉矶办事处，分别举行了专家组现场会议。布宜诺斯艾利斯会议向公众开放，一份专家组活动的摘要也于 2014 年 1 月通过两次网络会议呈交。除此之外，还辅以通过电子邮件等进行的电子讨论。报告草案已于 2014 年 2 月发布以征询公众意见。

主席想感谢专家组成员的所有见解和想法，并感谢 ICANN 对专家组的支持。同时感谢 ICANN 的埃利斯·格里琪（Elise Gerich）和爱丽丝·詹森（ Alice Jansen）为专家组的所有工作贡献的想法和支持。

2. 专家组策略

专家组的名称没有异议。由于认识到各类标识符对互联网日益重要，以及 ICANN 在其他标识符的管理方面扮演的角色，专家组的工作范围扩大到超出 DNS 本身。ICANN 目前的工作范围包括但不限于：

- 域名
- 自治系统号码
- IPv4 互联网地址
- IPv6 互联网地址
- 组播寻址
- 端口号码
- 协议号码
- 统一资源标识符（URI）注册
- 管理信息库（MIB）
- 时区数据库

但是，在工作范围扩大的同时，专家组的时间期限从最初的一年压缩到了大约六个月。受此影响，专家组比预期更加注重以 DNS 为导向。

为了弥补压缩的时间，专家组采用了以下原则：

- 尝试记录所有考虑的想法，但只侧重于其中的少数
- 寻找不可抗拒的趋势（例如，互联网扩张、处理器架构方面的趋势）
- 寻找“迫在眉睫”的需求
- 避免将精力集中在“已充分耕耘的领域”（例如，域名系统安全扩展技术（DNSSEC）部署或现有的冲突策略），而是寻找新颖的想法

专家组的核心目的是为 ICANN 的战略规划流程提供参考意见。尽管专家组考虑了与 ICANN 的运营需求接近的想法，但是他们的考虑范围并不局限于由 ICANN 本身来实施的想法。此处讨论的很多想法将最有可能通过 IETF 或其他途径实施。少数想法提出了专家组指出后却尚未讨论的政策问题。

最后，由于分配系统标识符领域的活动数量太多，专家组只是对该空间的活动进行了抽样。读者不应认为专家组了解所有正在进行的活动，也不应认为本报告中未涉及的看法比已经涉及的看法要更加重要。

3. 路线图

标识符在互联网社群中仍旧是一个热点领域。在短期内，新顶级域名 （TLD） 将会上线。脸书公司（Facebook）希望其帐户成为用户在互联网上使用的单点登录凭证，谷歌（Google）帐户也是如此。从长期来看，研究社群有很多不同的项目，包括内容中心网络 （CCN）、信息中心网络（ICN）、命名数据网络 （NDN） 和很多其他变体。虽然研究社群无法就该领域的名称达成一致，但是他们都同意应该通过名称而不是以地址或位置来标识内容，而且缓存应该是随机的。其他提案坚持认为，统一的名称是未来的趋势，对名称进行自行认证应该成为任何新系统的基础。

标识符对任何网络至关重要，因为它们能将网络的组成元素与网络的所有其他组成元素区分开来。此外，现代网络并不是单一的同质域，而是由多种技术混合构建而成，并要求在不同的标识领域之间建立映射。这种映射功能通过多种方式执行。在互联网背景下，最容易看到的标识领域是域名领域，这是一种采用分层结构的名称空间。与这个名称空间相关联的是一种映射功能，可从域名映射到其他标识（例如 IP 地址）。当我们研究标识符的路线图时，需要知道标识符领域和映射功能之间的区别，并关注它们各自的路线图。

对于目前的互联网，专家组发现了一些有可能扩大 DNS 应用的因素，以及一些有可能缩小其应用的因素。这些因素并非全是技术性的，而且其中的困难则似乎更偏向于达尔文式的，而不是因为一些无关痛痒的讲究。

目前扩大应用的因素

- DNS 享有传统优势，因为每台能上网的设备中都实施了 DNS。现有基础的简单增长将扩大其应用。例如，一个想通过防火墙并且在整个互联网被缓存的应用程序会将 DNS 作为现有基础。
- 新 TLD 将尝试打造其品牌。虽然技术社群对此颇有怀疑，但是超过一千个新品牌将努力茁壮成长，有可能会出现创新和一些惊喜。
- 新功能的出现，例如 DNSSEC 的安全功能或基于 DNS 的名称实体验证 （DANE），可能会推动额外的应用。
- DNS 中的新数据可能会扩大其应用，尤其是与 DNSSEC 结合使用以保证真实性时。一名专家组成员倡议发布域名的“诞生日”、注册商和“授权变更后的间隔”，作为基本的信誉信息。其他提案包括将 DNS 用作地址拦截注册、自治系统等等。ICANN 限制了在域名中使用某些标签，实时注册此类标签也许是合适的做法，尤其是在纸质规范有多个字母表时。从实践上来说，这类数据库可为公营或私营。
- “事物互联网（IOT）”对于不同的人来说意味着不同的事物，但基本来说，它包括了一个或多个大型分散性数据库中的大量事物。DNS ，不论是公共 DNS 的一部分，还是一个或多个私营 DNS 数据库，均被看作多个 IOT 架构和原型的基本元素。专家组希望有机会对此问题进行更为全面的探讨，提出进一步的考量，并相信 DNS 在这一系统中扮演着重要角色。

目前缩小应用的因素

- DNS 是传统标准，但这也是一项不利因素，因为在无线局域网（WIFI） 接入点、有线和数字用户线路 （DSL） 调制解调器、防火墙、路由器以及互联网软件库中嵌入的 DNS 逻辑常常限制了 DNS 的应用范围和创新。DNS 的实施往往不完全、不是最新或者不符合标准。这些问题阻碍了 DNSSEC 的实施，并使得实施任何新的 DNS 数据类型或功能出现问题。这导致了一些不得已的设计做法，例如只允许使用地址和文本 （TXT） 记录。这种僵化的现象并不是 DNS 所独有的。
- 对搜索窗口和/或标识符空间的控制（“掌控”）存在商业利益。此处的利益在于了解用户在初始自由形式方面的意愿，并将该意愿从开放的互联网上隐藏起来。专家组注意到，为了割据市场，现在设备的趋势是通过硬编码绑定到特定的 DNS 服务，以及使用专有的扩展组件。
- 用户喜欢更加强大的界面。用户和应用程序常采用搜索和其他机制来获得特定信息，而不是输入 DNS 名称。例如，浏览器中用于输入统一资源定位符（URL）的地址栏如今在很大程度上是一个搜索工具。现在最为常见的用户界面是移动设备，不利于打字。语音识别和浏览器栏中其他类型的人工智能（AI）组件会导致不同供应商间的不兼容。例如，专家组成员杰夫·休士顿（Geoff Huston）做了一个实验（参见“建议”部分），在不同浏览器上观察了由“Geoff.Huston”触发的搜索结果，发现不同供应商间几乎没有一致的结果。对于预计用户会审查搜索结果的浏览器搜索而言，这种不一致或许可以容忍，但是对于系统中的配置文件而言，这种不一致可能十分危险——是可能出现冲突的担忧之一。

专家组的意见是，虽然 DNS 的应用可能会从用户界面淡出，但是它可能仍将作为一个基础架构。要做一个类比的话，可以说 DNS 不是面临电子书冲击的纸质书籍，而是通过高级语言访问的计算机指令集。

关于复兴或重组 DNS 是否可行或可取，观点各有不同。相关技术在本报告的“DNS 基础”部分讨论。目前存在一个政策问题，就是 ICANN 是否应该尝试保留和扩展 DNS 系统。如果应该，如何根据 ICANN 社群、IETF（很可能由其来完成相关工作）和互联网中其他方的不同观点，获得一致的架构？

<u>长期设想</u>

有一些长期设想提出采用命名数据网络 （NDN） 模型。其关键理念是通过以下机制进行内容访问：名称、在任何地方进行数字认证、随机缓存以及按照相同路径发出和响应内容请求的数据流方案。对查询进行路由的模型有时被表述为仅对最长前缀匹配路由查找决策采用名称分层，怀疑论者认为这种机制不可扩展。在任何情况下，均需实施软件、硬件和多个网络测试平台。该模型最明显的应用是内容分发，但倡导者声称它适用于过程控制、汽车网络等。

从某种意义上说，DNS 是纯 ICN 的第一种渐进式替代方法，这一点与后来出现的那些尝试只保留 ICN 模型最重要部分的方法相似 [Fayazbakhsh 2013]。其重要性见仁见智。

DNS 通过名称检索数据。它不会尝试通过名称进行路由，然后使用互联网的寻址层来查询内容；这种方案修复了一些人认为 ICN 具有的核心扩展问题。DNS 从某种程度上说名声不太光彩，因为它可以作为用于建立视频隧道传输的工具 [Kaminsky 2004]，并在某些 WIFI 接入点进行身份验证之前，

通过所执行的 DNS 查询建立非法的访问隧道。（谷歌的“谷歌搜索隧道”可返回大约 1,620,000 个搜索结果。）

ICN 提供最长前缀匹配和选择器，可实现媒体传输，这是最初的 DNS 协议规范的查询部分预计到的功能，但从未有所发展。

在任何情况下，假设有人可以制作更大的 DNS 数据包，并添加一些额外的查询字段，则内容服务可以在 DNS 中复制。ICN 对经验证的请求和响应的匹配可能是避免 DNS 放大攻击的最佳方式。

总之，人们可以想象用一种 NDN 方案来代替 DNS，首先从 DNS 工具的一个超集开始，逐渐过渡，花费数年或数十年的时间来完成转换过程。任何用于增强 DNS 架构的尝试都应该可以自由借鉴 NDN。

ICN 绝不会是将来唯一的模型，它仅仅是发展最成熟的模型之一。专家组认为，尝试提炼出其基本原理，然后研究各种组合始终是有用的做法。[Ghodsi2011] 是一个很好的例子，因为它以一种方式将名称、真实身份和公钥基础设施 （PKI） 这三者联系了起来。

最近，对分布式控制 [Newyorker 2014] 和隐私的重视加大，域名币（Namecoin）系统就是一个最有名的例子。目前互联网中存在的 PKI 为大规模监视提供了资源，因此会带来隐私问题。混合使用自行认证对象和 PKI 选入机制，或者同时使用 PKI 和对等 （P2P） 系统也许能解决此问题。ITI 专家组并未探究这一领域，但认为这一领域十分有意思。

4. 运营问题

在 ICANN 的日常运营中，发现了若干问题。这些问题大部分与根域有关。

4.1. 加固根域

由于根基础设施至关重要，因此有若干外部建议表示，专家组应关注可信的计算技术。专家组认为，这类技术对用于编辑和签署根域的系统可能有益处，但是对于专家组来说，更优先的任务是考虑改进签名数据在商用硬件上的分发。斯诺登的爆料提出了目前的系统在设计时可能没有考虑到的一些硬件安全问题，例如 BIOS 感染、硬盘间谍软件等 [Spiegel 2014]。

4.2. 复制

DNS 始终有两种用于分发数据的互补机制：预先规划的区域复制和按需查询。从单条 DNS 数据，即一条资源记录 （RR） 的角度来看，通过查询拉取数据时，数据从其在某个区域中的最初来源开始分发，在一次或多次区域传输中随该区域传播，然后完成其旅程，到达最终目的地。

例如，根域由 ICANN 与威瑞信（Verisign）和美国商务部合作生成，然后通过区域传输分发到所有根服务器。从概念上讲，和在 DNS 中分发任何其他区域一样，这种分发可以通过任何机制进行：采用

磁带和联邦快递 （FEDEX） 递送、通过文件传输协议 （FTP） 或 Rsynch 进行文件传输，更理想的方式是采用增量区域传输，这样可以只发送自旧版以来的更改，而不用发送整个区域。副本可以由 DNS 通知来推送，也可以通过查询变更的轮询策略来拉取。区域传输的安全性可以通过 DNS 事务签名 （TSIG） 和/或任意数量的传输协议来确保，例如互联网协议安全性 （IPSEC）、安全超文本传输协议 （HTTPS） 等。目前有数百个具有根域副本的根服务器实例。

当用户想访问根域的数据时，他们会向根域发送查询。这些查询通过两种机制进行路由：首先，查询中的目标 IP 地址会确定一组共享通用任播地址的根服务器，然后路由系统决定这组任播服务器中的哪一个服务器将实际收到该查询。此方案是在进行一项评估后得出的结果。该评估首先采用 3 个具有单播地址的根服务器，然后扩展到 13 个具有负载分担集群的根服务器组织，接下来就是目前的方案（中间还有很多小步骤）。简而言之，“13 个根服务器”实际上是“13 个根服务器组织”，它们最终将区域传输给数百个或数千个单独的服务器[1]。我们只有 13 个根服务器组织和使用任播的原因在于，这种做法比放松 DNS 用户数据报协议 （UDP） 数据包的大小限制要容易得多。目前还存在与添加 IPv6 地址有关的其他大小限制问题。在从根服务器到用户的路径上，可选择通过 DNSSEC 来提供安全性。

多年来，根服务器一直遭受攻击，其中大部分是分布式拒绝服务 （DDOS） 的变体。此类攻击要想成功攻击特定用户，必须中断对 13 个不同根服务器组织的所有任播地址的查询。如果中断对其中一部分任播地址的查询，当查询者知道应避开哪个根服务器时，查询性能将下降。这种中断可以通过让服务器或通往服务器的网络路径无法正常工作来实现，通常以过载为手段。因此，举例来说，在这样的一次攻击中，加利福尼亚的用户会认为斯德哥尔摩的根服务器出现了故障，而斯德哥尔摩的用户观察到的情况则正好相反。对于最近由*匿名*黑客组织带来的威胁，根服务器组织的应对措施是部署更多带宽、服务器并采取高调态度。

当然，攻击无需针对根服务器群，它可以针对用户的互联网连接。当一个攻击僵尸网络与单个企业角力时，虽然造成的损失更为有限，但是攻击者通常更占上风，即使对较大型的企业也是如此。

有些专家组成员已建议企业在内部分发根域和**任何其他关键区域**的副本，这样企业在受到攻击时，可以继续正常运营，至少对 DNS 而言是如此。ICANN 让任何组织都可以轻松取得根域副本，这些组织再做一点工作就可以成为 ICANN 的“L 根”服务器组织中的根服务器实例。还有一个好办法是企业在内部部署足够的 DNS，从而免于受到无法访问外部服务器的威胁或者由注册局、注册商或根服务器运营商等意外或有意采取的行动造成的威胁。

有了 DNSSEC，我们就有办法分发可使用嵌入式数字签名进行验证的区域。专家组认为该原则可以通过保护授权和粘附数据等方式进一步扩展。同时还有可能消除或减少根服务器组织和地址数据。本报告的“建议”部分收录了一个方案，该方案在专家组成员保罗 • 维克西（Paul Vixie）的建议中有详细说明。

[1] 现在，有两个根服务器组织由同一个实体威瑞信（Verisign） 运营。

同时还有重要的政治方面因素。目前有 13 个根服务器组织，一些国家感到他们被忽略了，即使他们可以在其国家内安装所需数量的 ICANN L-根服务器实例。（更不用提一些其他根服务器组织愿意扩展其任播地址群。）所以让我们来解决这个问题。

值得一提的是，目前从技术角度而言没必要因某些人的喜好而更换现有的根服务器系统；我们只需简化根域的复制，同时为其他区域的复制树立榜样。

4.3. 共享区域控制

在上一节，我们讨论了让一些国家想拥有根服务器组织的政治情感。这些考虑可能有充分理由，也可能没有，但毫无疑问目前的根域运营设在美国，并处在美国司法管辖区。

简而言之，根域按一定流程顺序更新：

- ICANN 收到来自 TLD 的更新请求，并检查其中是否有错误
- ICANN 向美国商务部提交变更
- ICANN 向威瑞信（Verisign）提交经批准的变更
- 威瑞信（Verisign）生成经签名的根域并进行分发

是否有一种技术途径可以考虑共享对根域的控制？大家提出了一些理论。有个学派认为数据应该有 N 重签名。然后需要 N 重中的 M 重签名来验证数据。当然，目前关于 M 和 N 的规模大小，以及是否需要或适合采用不同的加密算法等议题还存在争论。

我们无意在此支持某个具体的系统，但是专家组确实认为，良好的设计将启动一项政治流程，确定控制某一特定区域的方式应当被如何共享。我们的目标是为共享区域控制创建一个工具箱，它不仅针对根域，还针对其他区域协调问题。专家组注意到，IETF 的 DNS 运营 （DNSOP） 工作组有两份关于协调 DNSSEC 签名信息的提案，但我们想知道，创建一个通用的工具而不是针对这个具体问题的解决方案，是否会更好。协调正向和反向地址也许是另一种应用。

所以，需要什么呢？我们推测，一个合适的模型必须为所有共享控制参与者提供一系列功能：

- 一个用于初始化共享区域的系统，包括区域本身、规则以及供各个参与者发布请求和行动的独立日志
- 针对特定区域采用适当的自动技术验证
- 每种请求对所有其他可以批准或反对请求或者判定请求超时的参与者可见
- 规则定义对请求的响应
    - 一种规则是一项投票决定，定义请求成功的条件。这可能包括提供延迟，以便所有参与方有时间考虑该请求。
        - 对于国家或地区代码顶级域名 （ccTLD），信息社会世界峰会（WSIS）的规则要求采用 1 票通过制，所以每个 ccTLD 可以单方面更改自己的数据。
        - 其他域名可能采用简单多数通过制

- 指定的延迟可能很重要，这样其他参与方或许能够指出运营问题，让请求者重新考虑
- 不同的条件可能适用于不同的操作，例如新建与编辑等

然后，参与者可以各自运行一个标准算法，以产生一致的状态。这看起来可能有点不切实际，但是拜占庭算法（例如比特币 [Andreesen 2014] 和域名币）表明，此类系统现在是有可能实现的。

（请注意，专家组并没有提出规则建议，我们只是在建议采用一个分布式系统，用于实施社群希望采用的任何规则。）

4.4. 注册局/注册商运营

一些专家组成员认为，ICANN 运营应提供服务级保证，但专家组觉得，这不是他们能推进解决的问题。

4.5. ICANN 应发布哪些数据？

4.5.1. ICANN 参数

在履行互联网号码分配机构（IANA） 职能和执行新 TLD 流程的过程中，以及在别的地方（例如，多语言中的保留标签），ICANN 有很多受其管理的参数集。所有这些参数集都应该在网上公布，可能应该在 DNS 中公布，而且无疑应该在安全表格中公布，以便互联网社群中的任何人都可以直接使用这些参数集。其他提案包括将 DNS 视作一个地址拦截注册、自治系统等等。

4.5.2. 域名诞生日、活动和范围

DNS 的信誉是一个颇具价值的安全工具。如今，域名的生成日期也需是维护该域名信誉的唯一最具指示性的信息。另一个信息则是域名服务器名称和地址的更新率。有时还须了解的重要信息包括，注册商在生成和管理一个域名时采取了什么方式。新的域名、高更新率和某些注册商都属可疑的信息。因此应当使得这类信息能够大规模实时共享。

范围信息以相似方式讨论，但此工作已由 IETF 在 2014 年 3 月在伦敦举行的下次会议上进行。

4.5.3. LISP 示例

早些时候，有人请专家组考虑让 ICANN 支持一项针对定位符/标识符分离协议 （LISP） 的超级根（Super-root） 服务 [RFC 6830]。正如迪诺 • 法里纳西（Dino Farinacci）等人向我们解释的那样，ICANN 将运行 LISP 服务器作为一项实验性服务，以将请求转发给目前未提供通用连通性的现有 LISP 服务器。ICANN 找到了四台服务器的资源，但是由于一些没有解决的问题，该项目尚未启动：

- 该实验的范围（持续时间等）如何？成功标准是什么？
- 将使用什么软件，由谁提供支持？有两种专有的替代方案。
- 谁拥有策略和运行控制权？
- 应该由 ICANN 还是由地区互联网注册局 （RIR） 来进行此事？
- 如果不牵涉 IP 地址，答案是否会有变化？

没有对此实验采取任何行动。

一些专家组成员感到：“些专家组成仅仅是一类更通用的传输隧道技术的一个实例，并没有引起任何超出目前可行的标识符管理实践范围的新型标识符管理任务，因此‘这种特定的隧道传输形式需要 ICANN 的特别关注和支持’这一情况并未得到明确证明。”

ICANN 应该预计到与新标识符相关的政策和技术问题将会再次出现，并进行相应规划。

4.6. 冲突

很多专家组成员都很熟悉 DNS 冲突问题，虽然关于此问题有很多讨论，但是并没有出现实质性的新方向。专家组觉得，[ICANN 2013] 中所述的现实世界系统原型值得高度推荐。

5. DNS 协议基本情况

我们能否期待 DNS 进行重大修订、升级或焕然一新？包括一些专家组成员在内的很多人要么认为现有的客户群对此十分排斥，要么认为流程不够完善[2]，或者觉得重头来过才是上策。

令人意外的是，专家组一致认为有必要努力发现问题并寻求解决方案，虽然这种做法不一定能解决问题。在本节中，专家组将简述几个多付出一些努力就可以研究的问题。

回顾 DNS 的创新史，既有成功，也有失败。从中学到的一条重要教训是，只有当一项技术能带来特定益处时，才会被人们广泛采用。管理员小心地将他们的区域与全球 DNS 保持连接，并及时更新他们的 A 记录和 MX 记录，不然他们就无法获得邮件或网站流量。但是，在已定义的约 60 个记录类型中，只有不到 10 个会被广泛使用。

创建以 DNS 为基础的应用程序的工作也面临类似的难题。

早期的 DNS RFC 建议了一个将邮件路由到特定邮箱的方法，但从未实施。第二个方案 MX RR 解决了需提供冗余邮件服务器以及跨越组织界限进行邮件路由的问题——此乃当今邮件路由的基础。反垃圾邮件数据库被广泛采用，但没有统一标准。用于邮件验证的各项竞争标准导致使用 TXT RR 进行了两项实施工作，并引发了关于对新类型实施标准化是否有用的讨论。

使用 DNS 对电话和其他媒体路由实施标准化的 E.164 号码映射（E.164 NUMber mapping，缩写为“ENUM”）取得的成功也非常有限。虽然名称权威指针 （NAPTR） 技术被视为一项真正的创新，但 ENUM 设计者忽视了对除目的地电话号码以外的信息进行路由的需求，而且设备制造商更喜欢将价值保留在其专属系统中。

5.1. 总体原则

但凡新设计都应该：

[2] 人们对这一话题的观点各异。有些人认为 IETF 某些特定的（特别是过去的）工作组的流程已经“破裂”。另一些人则认为，有必要采纳 API，而 IETF 并不采纳 API，那么到底谁采纳 API 呢？还有一些人则认为， DNS 工作组的多样性加快了发展与创新，效果要好于整体的愿景。

- 删除大小限制——576 字节最大传输单元 （MTU） 可能比任何其他单一因素更严重地拖累了 DNS；虽然可以在 DNSSEC 不合适时使用 DNS 的扩展名机制 （EDNS0），但是很多硬件和软件都不允许大型数据包通过。
- 保留所有现有 DNS 域名和数据的连接性
- 尽量使实施工作保持一致——如果不同的实施者没有遵守规范，那么一旦发生普通重叠，用户将受到限制
- 允许未来扩展
- 提供使用奖励

5.2. 数据模型

早期的 DNS RFC 设想为不同“级别”的信息和由简单成分组成的新数据类型设定平行名称空间。我们从未探讨过级别的概念。新的数据类型已经有了定义，但最近很多人建议使用专用于任意文本串的通用 TXT 记录来传送数据，并使用另一个级别的标签来代替 RR 类型。

专家组认为，DNS 应在 DNS 携带的元数据中定义自身的 RR 类型和格式，或者 DNS 应该将子标签正式定为最后的数据类型，并将查询扩展为允许更灵活的匹配。

最后，我们需要探讨一下可独立于域名而存在的自签名数据对象。

5.3. 分配

根据资源记录划分的数据和缓存区域结构依照对生存时间 （TTL） 标准的不均等“改进”而实施，并预取过期信息。有必要考虑用一些新的方法来将带序列号的数据组合在一起，以便在刷新缓存数据组时，不会真的传输数据。

专家组还认为可以通过使用现有根域迁移及其他机制，增加复制区域（可能是较小区域）的频率来提高安全性。这些数据无需受到 DNSSEC 保护，因此可以提高未实施 DNSSEC 之处的安全性。

5.4. 应用程序接口 （API）

DNS API 有两种形式：用户界面和 API 级别的名称。无论是哪种形式，我们都可以从允许明确完全限定域名 （FQDN） 的标准句法中受益。如果 UI 中的一系列搜索策略保持一致，将为用户社群带来更好的体验，但还不清楚是否有办法让供应商做到这点。

编程 API 进行了多次修改，但大部分均以失败告终。近期，专家组看到保罗 • 霍夫曼（Paul Hoffman）展示了一款具有异步接口和 DNSSEC 支持功能的新设计。IETF 于 2014 年 3 月在伦敦召开的会议结束后，即立即发表了该报告。具体请参见：http://vpnc.org/getdns-apj/。

但除了 API 之外，在哪里进行 DNSSEC 验证和 DNS 过滤（如有）也是一个问题。专家组一致认为，从技术层面上讲，应允许在终端系统（可能是虚拟机、笔记本电脑、用户环境中的服务器等，具体视用户偏好而定）终止 DNSSEC，尽管由于路由器、防火墙或其他旧版限制等原因，这种做法可能不太可行。同样的，虽然不是每个用户都会选择 DNS 过滤，但应将选择权交给用户。

以上表述并不意味着禁止用户将这些任务外包给 ISP 或其他服务提供商。

政策和法律条款可能另有规定。

5.5. 查询协议

DNS 查询协议存在两类问题：一类与将申请人的查询/响应传输到服务器有关，另一类与增强查询能力有关。

原来的 UDP 传输问题是传统的 576 字节 MTU 限制引发的。原来的修复方法是退回至 TCP 以实现更大的传输。根域数据的大小可能是 MTU 限制产生广泛影响首个对象，导致了 13 个根服务器的限制；之后，DNSSEC 签名的增加又极大地扩展了答复数据包。其中，EDNS0 被认为可以用来解决这一问题，它也确实取得了某种程度上的成功。但还是存在诸如各种以太网帧大小或 IPv6 的 1280 字节等其他限制，这些限制从根本上约束了 UDP。

此外，EDNS0 也无法解决访问点、路由器、防火墙和其他硬件阻止访问 TCP 端口 53 或限制数据包大小，甚至在透明代理中拦截 DNS 请求（通常对服务不利）的问题。不支持大型数据包、所有 DNS 数据类型和 EDNS0 等的缓存名称服务器中也可能存在类似问题。有些问题可能十分微妙。例如，DNSSEC 数据包在正常情况下可以通过，但在 DNSSEC 密钥滚动（一个常规维护流程）期间可能无法通过，因为在此期间数据包较大。

与此相关的一个问题是 DNS DDOS 攻击，特别是使用反射和放大的攻击。在这些情况下，您需要一种能区分合法流量和攻击流量的方法。对于 DNS 和很多其他协议而言，源地址验证 [BCP 38] 能在极大程度上解决这一问题。专家组对此表示赞成[3]，但这个方法并没有得到广泛部署。流量整形和各种启发式方法会有所帮助，但不能彻底解决问题。各种轻量级的验证机制一直是备选方案。

有个学派认为，要解决传输问题，需要将所有 DNS 流量放入 https: 中。这是因为每个人都从查看安全网站流量中获得既得利益，所以它是一个有保障的路径（有人说这是唯一有保障的路径）。代价是连接状态和有关开销。替代方案包括一些新的事务协议或 UDP 使用方法，两者可能都无法在部分现有用户群中起作用。无论是哪种情况，都存在 DNS 事务是使用传统形式还是新形式的问题。

无论如何传输，都应扩展 DNS 查询协议，以允许更灵活的查询， 其中包括对代替 NSEC 和 NSEC 3 的后续标签的某些访问控制。

CCN 之类全球研究协议从 DNS 中吸取经验，整合了上述所有特点。应对这些新协议的当务之急是找到如何促进现有基础架构升级的方法，同时兼具向后兼容性，而不是在协议科学中寻求新突破。

[3] 全体专家组成员支持 [BCP 38]的内容，某些专家组成员感到，应当将支持这项内容作为专家组的核心建议之一。然而，大部分人也注意到了，自 BCP 于 2000 年出版发表以来，仅有很少的人采纳了这一建议。

6. 观察意见和建议

- DNS 在基础架构中的应用呈上升趋势；而在用户界面 （UI） 中的应用则受到搜索型备选方案、移动界面等因素的影响。
- ICANN 应为保留的标签等内容发布更多 DNSSEC 签名的数据。
- 与 IETF 等小组携手开展研究，确定 2020 年 DNS 的架构愿景。
- 设计开放的根域并发布其原型。
- 为根域设计一个共享区域控制系统。
- 执行冲突检查以测试实施的难易度 [ICANN 2013]。

7. 参考文献

[Andreesen 2014] 安德森（Andreesen）的《为何比特币如此重要》（Why Bitcoin Matters）一文，
http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters

[BCP 38] 弗格森（Ferguson）等，《网络进入筛选：挫败使用 IP 源地址欺诈的服务攻击拒绝》（Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing），RFC 2827，2000 年 5 月。

[DNS/TCP] https://lists.dns-oarc.net/mailman/listinfo/tcp-testing

[Fayazbakhsh 2013] 法耶兹巴克什（Fayazbakhsh）等，《少付出多收货：逐步部署 ICN 》（Less Pain, Most of the Gain: Incrementally Deployable ICN），
Sigcomm 2013

[Ghodsi 2011] 戈德西（Ghodsi）等，《以内容为主导的架构中的命名问题》（Naming in Content-Oriented Architecture），Sigcomm 2011

[Huston 2013] 仅对 TCP 上的 DNS 的研究。

http://www.circleid.com/posts/20130820_a_question_of_dns_protocols/
以及关于 dns 运营的后续线程

[ICANN 2013] 《针对 IT 专业人士发布的域名冲突识别和缓和措施指南》（Guide to Name Collision Identification and Mitigation for IT Professionals），
https://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-05dec13-en.pdf

[Kaminsky 2004] D.凯闵斯基（D. Kaminsky），《DNS 中的隧道音频、视频和 SSH 》（Tunneling Audio, Video, and SSH over DNS），BlackHat 2004

[特别内容] **关于域名和 DNS 的章节**

http://www.afnic.fr/en/about-afnic/news/general-news/6391/show/the-internet-in-10-years-professionals-answer-the-afnic-survey.html

[Mockapetris 88] P.莫卡普利斯（P. Mockapetris）和 K.顿拉普（K. Dunlap），《域名系统的发展》（Development of the Domain Name System），
SIGCOMM 88

[Newyorker 2013]

http://www.newyorker.com/online/blogs/elements/2013/12/the-mission-to-decentralize-the-internet.html?goback=%2Egde_1430_member_5817512945197801473#%21

[RFC 881] J.波斯特尔（J. Postel），《域名规划和安排》（The Domain Names Plan and Schedule），1983 年 11 月

[RFC 882] P.莫卡普利斯（P. Mockapetris），《域名——概念和设施》（Domain Names – Concepts and Facilities），1983 年 11 月

[RFC 883] P.莫卡普利斯（P. Mockapetris），《域名——实施推行和规格》（Domain Names – Implementation and Specification），1983 年 11 月

[RFC 1034] P.莫卡普利斯（P. Mockapetris），《域名——概念和设施》（Domain Names – Concepts and Facilities），1987 年 11 月

[RFC 1035] P.莫卡普利斯（P. Mockapetris），《域名——实施推行和规格》（Domain Names – Implementation and Specification），1987 年 11 月

[Spiegel 2014] http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html

8. 术语表

A 一个用于记录一个 IPv4 地址的 DNS 记录

AAAA 一个用于记录一个 IPv6 地址的 DNS 记录，通常称为“四 A”

AI 人工智能

API 应用程序接口

BCP 当前最佳实践——RFC 中已经确定的下属子集

CCN 内容中心网络

ccTLD 国家或地区顶级域名——分配给特定国家或地区的 TLD，某些时候由第三方运营

DANE 基于 DNS 的名称实体验证

DDOS 分布式拒绝服务

DNS 域名系统——互联网命名系统

DNSOP DNS 运营——与 DNS 运营等问题有关的 IETF 工作组

DNSSEC 域名系统安全扩展技术

DSL 数字用户线路

E.164　一项叫作*国际公共电信编号计划*的 ITU-T 建议，为全球公共交换电话网 （PSTN） 和一些其他数据网络定义编号计划

EDNS0　DNS 的扩展名机制 [RFC 2671]——扩展原始 DNS 规格的大小和字段的标准

ENUM　E.164 号码映射——统一公共交换电话网的国际电话号码系统与互联网地址和识别域名空间的系统，例如路由电话

FEDEX　联邦快递

FQDN　完全限定域名

FTP　文件传输协议

gTLD　通用顶级域名——不与任何国家代码对应的 TLD

HTTPS　超文本传输协议

IANA　互联网号码分配当局

ICANN　互联网名称与数字地址分配机构

ICN　信息中心网络

IEEE　电气和电子工程师协会

IETF　互联网工程任务组

IOT　事物互联网

IP　互联网协议

IPSEC　互联网安全协议

IPv4　互联网协议版本 4

IPv6　互联网协议版本 6

ITI　标识符技术创新——一个 ICANN 战略专家组

LISP　定位符/标识符分离协议 [RFC 6830]

MIB　管理信息库

MTU　最大传输单元——可以顺利通过或通过但不分割的最大数据单元的大小。

MX　邮件交换——一种 DNS 数据类型，可指定处理特定域名的邮件的邮件交换

NAPTR（名称权威指针 ）——在互联网电话中应用最广的一种 DNS 数据类型

NDN 命名数据网络

P2P 对等

PKI 公共密钥基础架构

RFC 征求意见——记录技术和运营类互联网问题的备忘录

RIR 地区互联网注册局——一家管理全球特定区域中互联网号码资源的分配与注册的组织。例如，美洲互联网号码注册局 （ARIN） 负责处理加拿大、美国和很多加勒比群岛及北大西洋群岛的事务。

Rsynch 远程同步协议——可以同步文件和目录，同时使用 delta 编码将数据传输最小化。

RR 资源记录——DNS 中的信息的原子单元

TSIG 事务签名

TTL 生存时间

TXT DNS 中允许自由格式文本字段的文本 RR 类型

UDP 用户数据报协议——互联网的无连接数据报协议

UI 用户界面

URI 统一资源标识符

URL 统一资源定位符

WIFI 无线保真——IEEE 802.11 标准族定义的无线网络标准

9. 专家组成员的建议

请注意，所有建议均根据个人提交的内容逐字记录。

9.1. 庄振宏（James Seng）的建议

技术架构

我深深觉得黑客很喜欢分散式架构。可以这么说，如今的大部分“政策问题”均源于 DNS 和根域的集中化性质。

所以域名币等技术或其他分散式标识符系统深得我心。

但是据我所知，分散式协调标识符系统实际上并没有被广泛采用。所以不管喜欢与否，DNS 系统仍然是我们常用的标识符系统之一。如同在 IETF 中“运行代码”说了算一样，最好的设计未必是赢家。

我不相信多根域或备用根域。正如我在布宜诺斯艾利斯会议上说的那样，我是 RFC 2826 的支持者。多根域、备用根域及所有相关提案只会将政策问题推到另一个层面，并不能解决根本性的政策问题。请注意，这里我说的是政策问题，因为我压根不认为多根域可以解决任何技术问题，它只会徒增技术的复杂性。

ICANN

DNS 及其根域的集中性在某种程度上使得原本简单的 IANA 功能操作成为了如今名为 ICANN 的大型组织。

我参加了 ICANN 在 1999 年举行的首次会议，之后的每次会议我基本上也都参加了。这些年来，我觉得 ICANN 在某些事情上应采取不同的处理方式，例如，我们的立场并不总是一致。

但是，ICANN 是 DNS 标识符协调的“运行代码”。或许有其他更好的设计，可能更简洁更优雅（IETF 社群中的很多人都希望能回到强 • 波斯特尔（Jon Postel）时代的风格），但时光无法倒流，现在更重要的是，虽然还有提升的空间，但实用的设计才是最好的设计。据我们所知，提议的备选方案（ITU）还存在其他问题或情况更糟。

因此，我支持 ICANN，因为它是我们用于协调 DNS 标识符和根域的最佳系统。

DNS 及其系统扩展到其他区域

我没什么兴趣就命名标识符重新设计 DNS 或替代方案。最后，会有一些人或组织来进行协调工作，我们仍会面临相同的政策问题。

我支持并愿意看到原先专为 DNS 设计的 DNS 生态系统（DNS 标准、根域运营、ICANN 等）扩展到其他区域（如 RFID），这样可以汇集更多的社群。从某种意义上说，我们对 IDN 所做的工作是汇集一些用户社群，让他们能够在 DNS 生态系统中使用自己的母语，而不是让他们建立自己的系统。

尽管有人跟我说，如果我们在 DNS 生态系统之外完成 IDN，部署工作可以更快完成（例如，请参见母语关键词），但我认为 IDN 也不差，因为它是 DNS 生态系统的一部分，该系统中有明确的开放标准、开放实施，以及根据 DNS 的合法性建立的公司和对 IDN 注册人和终端用户的保护。

因此，我一点也不担心，我支持探讨如何将 DNS 扩展到原本不是专为其设计的标识符的方法。设计标识符的工程师通常对标识符伴随的政治问题想得太简单，尤其是当这些标识符面向终端用户时。他们可以从 DNS 标识符和 ICANN 的历史中学到一点东西。

根域的政治问题

ICANN 的政治问题以及 ICANN 被很多人视为“互联网治理”的一部分源自 ICANN 在根服务器的协调中充当的角色。

雪上加霜的是，由于历史原因，在 13 个根服务器中，有 11 个位于美国，特别是在斯诺登事件后，更让人们觉得 ICANN 是在美国的掌握之中。

每当有人谈到应在哪些国家设立根服务器时，我们都会用历史或技术原因来侧面回答这个问题，解释说没有办法超过 13 个根服务器。

说是历史原因我还可以接受。

但要说是技术原因，我实在没办法认同。这更像是一个借口，因为我从未看到 IETF 真正在寻找如何扩展到超过 13 个根服务器的方法。这就是为什么在布宜诺斯艾利斯会议期间我说我能想到几个技术解决方案，至少能充当 I-D。我们不能让 ICANN 继续用 IETF/技术原因来当作他们面对的政治问题的借口。我们应告知 ICANN 这个问题是可以解决的，但实施与否则需要由他们自行决定。

此外，更重要的是，根服务器运营并不是宣传的那样。

拥有根服务器并不意味着您就可以立即控制互联网。其实它跟任播根服务器一样乏味。如果根服务器运营机构不遵守根服务器运营的一些最佳实践（如 RFC 2010 和 RFC 2870），它就会给互联网带来很多危害。

大多数工程师可能会明白我所说的内容，但大部分 ICANN 人员可能不会懂。

所以在选择根服务器运营机构时需要极其慎重，因为它是互联网标识符稳定性的关键，并且其中大部分是以信任为基础的。但无论喜欢与否，信任都不是一个工程问题。

——庄振宏（James Seng）

http://chineseseoshifu.com/blog/dnspod-in-china.html

尽管 DNSPod 会使得 DNS“破裂”，但它为何能在中国市场取得成功。

9.2. DNS 解析和搜索列表应用程序行为——杰夫·休士顿（Geoff Huston）

无——不进行任何 DNS 查找

从不——查找基名称，但不应用搜索列表

预先——应用搜索列表，如果返回 NXDOMAIN，则查找基名称

之后——查找基名称，如果返回 NXDOMAIN，则应用搜索列表

总是——不查找基名称，只应用搜索列表

基础操作系统 DNS 解析器库行为

系统	绝对 *server.*	相对单个标签 *server*	相对多个标签 *www.server*
MAC OSX 10.9	从不	总是	从不
Windows XP	从不	总是	之后
Windows Vista	从不	总是	从不
Windows 7	从不	总是	从不
Windows 8	从不	总是	从不
FreeBSD 9.1	从不	预先	之后
Ubuntu 13.04	从不	预先	之后

MAC 和 Windows 平台上的浏览器行为

MAC OSX 10.9

	server.	*server*	*www.server*
Chrome （31.0.1650.39 beta）	从不	总是	预先
Opera （12.16）	从不	总是	从不
Firefox （25.0）	之后*	总是	之后*
Safari （7.0 9537.71）	无**	无**	无**

* 添加前缀“www.”，然后尝试在“www.”前加前缀，再加上搜索列表

** Safari 似乎能识别 TLD，当域名不是 TLD 时不会执行 DNS 查找

Windows 8.1

	server.	*server*	*www.server*
Explorer （11.0.900.16384）	无	无	从不
Firefox （25.0）	从不*	总是	从不
Opera （17.0）	无	无	无**
Safari （5.1.7 7534.57.2）	从不*	总是***	从不

* 添加前缀“www”

** OPERA 能识别授权的 TLD，只会在最后一个标签是 TLD 的情况下询问

*** 添加前缀“www”和后缀“.com”

9.3. 对一致性的看法和转换建议——杰夫·休士顿（Geoff Huston）

如果回顾域名系统的起源，会发现所谓的“主机文件”是早期把人用名称融入电脑网络环境的一项尝试。阿帕网使用网络节点命名模型，该模型上每个连接的节点都有一个本地配置文件、包含所有其他阿帕网节点名称的主机文件以及每个节点的协议地址。对于阿帕网连接节点中主机文件的多个实例，并不强制要求一致性，当时也没有任何方法在网络中分配主机文件的副本。该主机文件的用途是提供更易记忆的名称来取代更冗长的协议层级地址。用户可以通过符号名称来识别网络节点，之后通过查找主机文件，符号名称会被转换为特定协议的二进制地址。随着阿帕网的发展壮大，主机文件的大小和更新速率以及维持准确的本地主机的开销也随之增加。因此对主机文件格式进行了标准化 （RFC952），并定义了中央主机文件服务 （RFC953），这可以替代主机文件的很多本地副本。

之后它又被域名系统 （DNS） 取代，最初在 1983 年的 RFC 882 和 RFC 883 中注明。将名称转换为易于记忆的字符串后再发送到特定协议的服务地址的机制是由将主机文件转换到 DNS 来实现的。

该标识符空间有许多特性，据观察，DNS 涵盖一个适用于人类交流的名称空间，同时拥有足够正式的结构以便让计算机应用程序以确定的方式操纵名称。DNS 名称空间是一个分层结构空间，允许名称空间被有效地用于查找完全匹配，同时还允许名称空间的分布式管理框架。只要可以在 DNS 名称层级的任何一个区域内避免标签冲突，就可以在整个 DNS 名称空间中避免名称冲突，使名称的唯一性可以在 DNS 的背景下得到妥善管理。DNS 在映射功能方面很灵活，可用于从一个结构名称空间映射到我们服务点上任何其他形式的命名资源。DNS 应保持一致，即就 DNS 中前后一致的名称条目而言，在不同的查询位置和不同的查询时间，对该名称的查询均应提供相同的答案。它还允许参考一致性，即 DNS 名称可以在各方之间传送并参考服务位置的一致资源。DNS 并不旨在取代目录系统或搜索系统。如果在 DNS 中查询的名称存在完全匹配，DNS 查询将返回映射值作为查询结果，否则查询将返回匹配失败。

作为用于支持通过网络实现人机交互的标识符名称空间，DNS 名称空间模型经历了一系列变化，主要是针对在交流中人们使用标识符的模式。我们倾向于以不太精确的方式使用标识符，其中包括使用本地语言和文字的本地环境元素。随着时间的推移，我们已经吸收了 DNS 作为一种与网络资源和服务进行人机交互的形式所发挥的作用，可以一种人们使用起来更“自然”的方式来支持这种交互。

RFC1034 建议在 DNS 名称说明中使用缩写，将不以“称说结尾的名称称为“相对名称”，并且如 RFC1034 中指出的那样，“相对名称大多出现在用户界面，其解释视具体的实施而定。”通常情况下，这种本地解释涉及标签的本地搜索列表，允许用户指定一个域名的初始部分，并继续根据本地应用程序或名称解析软件的惯例添加一个本地定义的后缀，以形成一个完整的 DNS 名称。

在 Web 浏览器提供的用户界面中，这种通过使用名称后缀选择性阻断 DNS 标识符空间的形式更高级，Web 浏览器的常见做法是提取一个 URL 的 DNS 标识符组成部分并应用名称转换以在前面加上字符串“识符组成部，然后再增加本地定义的后缀（通常为“.com”）。如此一来，用户指定的标识符与后续 DNS 查询所用的标识符名称就产生了关联，但未必相同。

进一步扩大本地名称转换的用途的是，以美国 ASCII 以外的语言文字形成的标识符能映射到 DNS（IDN：RFC5891）。以下是明确定义的流程，用户输入的标识符被转换为构成 DNS 查询的编码标签字符串。在这种情况下，转换是准确定义的，因此 IDN 标准的多个实践旨在支持将标识符以既定文字映射到编码 DNS 名称形式。

人机互动模式的进一步升级是将搜索词和 URL 统一作为对浏览器的输入。此时，如果用户没有在浏览器上输入完整规范的 URL，浏览器将尝试更新。

9.4. 当今标识符的一些问题——保罗·维克西（Paul Vixie）

1. 根域的弹性

如今，DNS 系统十分依赖根服务器的可用性、容量和可访问性。若一家企业、互联网服务提供商、国家或用户维护自有的根域副本（或多份副本），并使用这些副本文件来解析域名，而不是每次都到“真正的”根服务器上去寻找，则这些企业、互联网服务提供商、国家或用户将能够更好地防范根服务器上的袭击，并能在与真实根服务器断开连接时，和真实根服务器暂不可用、负荷过大或受到袭击时，这些企业、互联网服务提供商、国家或用户仍旧能够正常运作。

2. IP 地址欺诈

带有伪造源地址的 IP 包是目前犯罪分子使用的最重要的工具之一，以避免他们的犯罪目标使用互联网。通过使用大量电脑假冒犯罪目标的身份发送这类 IP 包，袭击者可以生成大量“响应”流量，使得返回犯罪目标的网络链接出现满负荷或超负荷的状况。

3. 域名系统域名到地址的映射快速通量

目前，犯罪分子通常采用执法机构无法跟踪或关闭他们的犯罪活动的方式滥用 DNS 系统。如今，“僵尸网络行家”可能使用一系列被劫持的设备（即“僵尸网络”），从事各种违法犯罪的活动，包括：发送垃圾邮件、启动 DDOS 袭击，使用各种恶意软件感染其他设备。通过在 DNS 系统中快速更改域名到地址的映射，僵尸网络行家们能够将其犯罪活动从一批被劫持的设备上快速移至另一批被劫持的设备上，从而避免执法部门尝试对这些犯罪活动的跟踪和关闭行为。

我们建议 ICANN 与互联网社群中的其他成员合作

（1） 提高根域的弹性，

（2） 应对 IP 地址欺诈使用问题，

（3） 应对 DNS 域名到地址映射快速通量的问题。

9.5. 根域通用任播——保罗·维克西（Paul Vixie）

概述

我们建议 IANA 为 DNS 根域制作几个额外的形式，以便允许通用任播和运营研究。这里的“通用任播”是指顶点 NS 记录只列出两个名称服务器的根域，与之有关的“知名”地址（如 A 和 AAAA 记录所述）可以由任何人托管。这里的“运营研究”包括对仅 IPv6 根名称服务和“新 gTLD”冲突效果的大规模公开测试。此方法将根名称服务视为未受管理的实用工具，而不是受管理的实用工具。

背景信息

在 DNSSEC 出现之前，根域的通用任播无法安全可靠地部署，这是因为没有 DNSSEC，任何响应服务器可以使用任意 DNS 根域数据（包括新 TLD 或重新授权的现有 TLD）进行配置。有了 DNSSEC，递归名称服务器运营商现在可以配置 DNSSEC 验证，如此一来，来自通用任播根名称服务器的任何 gTLD 信息就必须使用 IANA 根域签名密钥 （ZSK） 进行 DNSSEC 签名才能获得 IANA 的批准。

现有和旧版根名称服务器系统受到的批评包括缺乏抵御 DDoS 攻击的能力，需要注意的是，即使现在每个根名称服务器运营商都在进行大规模任播，全世界仍然只有几百个名称服务器可以权威地对 DNS 根域做出回应。我们还担心，甚至是纯本地通信也需要访问根名称服务器系统，否则本地客户端就无法发现本地服务。在如同互联网一样遍及全球的分布式系统中，关键服务应做到均匀分布。

详情

可以构建几种有用的变体。首先，基本通用任播将允许任何名称服务器运营商来操控流向根名称服务器系统的流量，并在本地进行回应。IANA 将生成在顶点有一组不同的 NS 记录的其他版本的根域，并进行数字签名（和 DNSSEC）。这些 NS 记录将指出地址没有分配到任何特定的根名称服务器运营商（RNSO）而是交由 IANA 托管以供任何或所有相关方使用的名称服务器。IANA 将要求从 RIR（如 ARIN 或 APNIC）进行基础架构微分配，如若干 IPv4 24 位前缀和若干 IPv6 48 位前缀，用于根域的通用任播。

当前根域的第二个变体将提供上述通用任播，但会指出只有 IPv6 连接（以存在 AAAA 记录表示）且没有 IPv4 连接（以缺乏 A 记录表示）的名称服务器。该变体将促进仅 IPv6 网络中的运营研究。

当前根域的第三个变体将提供上述通用任播，但会纳入所有已知的新 gTLD 的授权，包括那些在其他方面没有准备好进行授权的域名（如 .CORP 和 .HOME）。这些新 gTLD 将被授权予 IANA 自己运营的名称服务器，用于测量目的。每个新 gTLD 都将被分配通配符 A 和 AAAA 记录，其地址将到达 IANA 运营的 Web 服务器，用于测量目的。

影响

鉴于互联网路由的分层特性，任播地址块可以在多个级别进行通告。在笔记本电脑上运行的虚拟机 （VM） 可能有自己的名称服务器进程，它可以收听适当的知名地址，在这种情况下，没有根名称服务查询会离开该 VM。笔记本电脑本身也可以操控以这些知名地址为目标的出站流量，这对其他 VM 或笔记本电脑上运行的其他进程很有用。这台笔记本电脑的无线路由器上游可能有收听这些地址的服务器，在这种情况下，没有根名称服务器查询会离开该无线局域网。ISP 可能会操作收听这些知名地址的服务器，以便为任何及所有没有操作自己的服务器的用户服务。最后，全球互联网预计将有多家将路由告知知名地址块的运营商，不仅仅是现有的 12 个根名称服务器运营商。

这样做的积极影响是具有更大的潜在灵活性，并减少根名称服务延时。负面影响是会降低诊断能力，更容易“路由中毒”或被“劫持”根名称服务流量。无论如何，让 DNSSEC 验证被普遍应用以减少这类劫持风险是十分重要的。我们希望攻击者得到结果是“受害者失去根名称服务”而不是“受害者看到一个不同的 DNS 名称空间”。

示例

以下示例显示了每个根域变体的顶点 NS 记录组，包括地址粘合。在进行 DNSSEC 签名之前，该数据将被纳入变体根域，还会发布为“根提示”文件。iana-servers.net 显示的数据也将显示于实际的 iana-servers.net 区域。这些示例需要进行四个 IPv4 微分配和六个 IPv6 微分配。

变体 1：通用任播

```
. IN NS anycast-1.iana-servers.net.
. IN NS anycast-2.iana-servers.net.
$ORIGIN iana-servers.net.
anycast-1 IN AAAA 2001:?:1::1
anycast-1 IN A ?.?.1.1
anycast-2 IN AAAA 2001:?:2::2
anycast-2 IN A ?.?.2.2
```

变体 2：通用仅 IPv6 式任播

```
. IN NS v6only-1.iana-servers.net.
. IN NS v6only-2.iana-servers.net.
$ORIGIN iana-servers.net.
v6only-1 IN AAAA 2001:?:3::1
```

v6only-2 IN AAAA 2001:?:4::2

变体 3：gTLD 冲突研究任播

. IN NS gtldstudy-1.iana-servers.net.
. IN NS gtldstudy-2.iana-servers.net.
$ORIGIN iana-servers.net.
gtldstudy-1 IN AAAA 2001:?:5::1
gtldstudy-1 IN A ?.?.5.1