

SAC067

IANA 职能的概述与历史



ICANN 安全与稳定咨询委员会 (SSAC) 报告

2014 年 8 月 15 日

序言

这是一份致互联网名称与数字地址分配机构（ICANN）董事会、ICANN 社群以及互联网社群的报告；广义而言是一份 ICANN 安全与稳定咨询委员会（SSAC）报告。此报告提供了互联网号码分配机构（IANA）的职能（即履行什么职能）概述以及该机构是如何从个人的非正式活动¹ 演变成为在当今各种合同与协议背景下可以实施整套结构化活动的历史。了解此背景对于社群考虑将 IANA 职能管理权从美国政府那里移交给其他一些尚未确定结构的机构尤为重要。

本报告是利用来自 SSAC 成员所收集的公共信息以及 SSAC 成员自己个人的回忆录编制而成，因此本报告不包括任何来自机密或者专有资源的信息或者见解。正因如此，本报告中所含的一些信息可能会不准确或者不完整，或者还会有 SSAC 个体成员真诚作出的回忆内容方面存在偏差的情况。在可能的情况下，针对编制本报告所引用的公开文件在正文中或者脚注中提供了统一资源定位符（URL）。

SSAC 主要负责处理互联网名称和地址分配系统安全性与整合性的相关问题。这包括运作问题（例如与正确、可靠地运行根域发布系统有关的问题）、管理问题（例如与地址分配和互联网号码分配有关的问题）以及注册问题（例如与注册管理机构和注册商提供的服务有关的问题）。SSAC 一直从事互联网名称和地址分配服务的威胁评估和风险分析工作，评估哪里存在严重的稳定性和安全性威胁，并据此向 ICANN 社群提供建议。SSAC 不享有监管、强制执行或裁定的职权。这些职能属于其他机构，对于本报告中列出的建议，应根据建议自身的价值予以客观的评估。

本报告末尾列出本报告的编著者列表、关于 SSAC 成员的个人简介和利益披露的参考文档以及 SSAC 成员对报告中各项调查结论或建议的反对意见。

¹ Jon Postel 博士是最初的 IANA，请参阅 RFC 2468 (<http://tools.ietf.org/html/rfc2468>)。

目录

1	简介	5
2	背景与历史	6
2.1	以前 IANA 职能合同的历史	6
2.2	服务于 IETF 的 IANA 职能	7
2.3	IANA 职能合同的历史	9
3	DNS 根域管理职能	10
3.1	根域管理类别	11
3.2	更改请求处理	19
3.3	美国政府的参与	20
4	互联网号码注册管理	21
4.1	互联网号码注册管理功能	22
4.2	更改请求处理	25
4.3	美国政府参与互联网号码资源管理	26
5	协议参数注册表和 .ARPA 顶级域名管理职能	26
5.1	协议参数注册表管理	26
5.2	地址和路由区域 (.ARPA) 顶级域名的管理	28
5.3	美国政府的参与	31
6	.INT 顶级域名的管理	31
7	当前 IANA 职能的工作投入	32

IANA 职能的概述与历史

7.1	DNS 根域管理	32
7.2	互联网号码注册管理.....	33
7.3	协议参数注册表管理.....	33
8	协议	34
8.1	IANA 职能合同	34
8.2	ICANN 和 IETF 之间.....	35
8.3	ICANN 和 RIR 之间.....	36
8.4	ICANN 和根服务器运营商之间.....	36
8.5	ICANN 和国家地区代码顶级域名管理员之间	37
8.6	ICANN 和通用顶级域名管理员之间.....	37
9	总结	37
10	利益、异议和撤回的确认和披露	38
10.1	致谢	38
10.2	利益声明	39
10.3	异议	39
10.4	撤回	39

1 简介

互联网号码分配机构 (IANA) 是一个传统名称, 用于“指代制定和发布互联网协议技术参数分配的技术团队。”² 此技术团队执行一组任务, 涉及对众多使全球互联网正常运行的标识符进行管理或者协调。这些任务目前由互联网名称与数字地址分配机构 (ICANN) 依据一组协议来执行, 包括:

- 1) 与美国商务部下属美国国家电信和信息管理局 (NTIA) 签订的合同;³
- 2) 与互联网工程任务组 (IETF) 签订的谅解备忘录 (MoU);⁴
- 3) 与地区互联网注册局签订的谅解备忘录;⁵
- 4) 与一些根服务器运营商签订的协议;
- 5) 与国家和地区代码顶级域名 (ccTLD) 管理人签订的合同、谅解备忘录以及其他协议; 以及
- 6) 与通用顶级域名 (gTLD) 管理人签订的一系列合同。

按照 ICANN 与 NTIA 之间的当前 IANA 职能合同所述,⁶ IANA 职能如下:

- 1) 域名系统 (DNS) 根域管理;
- 2) 互联网号码注册管理;
- 3) 协议参数注册表管理, 包括“地址和路由参数区域” (. ARPA) 顶级域名的管理; 以及
- 4) “国际条约组织” (. INT) 顶级域名的管理。

本报告描述的内容包括 IANA 职能合同中所包含的活动以及根据 IETF 谅解备忘录所执行的职能——这些职能旨在针对那些关注最上一级互联网唯一标识符系统的管理方法来建立谅解基准。本报告主要关注的是 IANA 职能合同, 但旨在描述与 IANA 职能相关的全部活动, 因为这些活动目前正在执行, 包括那些 IANA 职能之外的活动。

² 请参阅 RFC 2860 中对 IANA 的定义 (<http://tools.ietf.org/html/rfc2860>), 第 3 节。

³ http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf

⁴ 最初 2000 年 3 月的谅解备忘录网址为 <https://www.icann.org/resources/unthemed-pages/ietf-icann-mou-2000-03-01-en> 和 <http://tools.ietf.org/html/rfc2860>。从那时起已经执行了一系列补充协议。

⁵ 请参阅 <https://archive.icann.org/en/aso/aso-mou-29oct04.htm>。

⁶ 除非另有说明, 否则本报告中提及的术语“IANA 职能合同”指的是 ICANN/NTIA 合同, 网址为 http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf。

2 背景与历史

IANA 职能是为最上一级互联网标识符提供协调服务的一组活动。这些职能依照确保这些标识符得以安全、稳定以及可靠的分配、指定以及传播的原则行事，标识符的唯一性涉及定义明确的标识符空间以及标识符分配给谁和/或标识符分配目的记录。

本节提供了 IANA 职能如何演变为这些活动的一些背景和简史，两者均以 IANA 职能合同为背景并且与 IETF 相关。

2.1 以前 IANA 职能合同的历史

在 1968 年 8 月，来自最初四个阿帕网站点的代表们在圣巴巴拉会面。与会者们同意定期会面来讨论如何使用阿帕网，阿帕网是通过美国国防部高级研究计划署 (ARPA) 资助建立的一个通信网络。当时，ARPA 正处于为构建路由器（互联网消息处理器或 IMP）接收投标的过程中。承包商尚未选定（将会是 Bolt, Beranek and Newman 公司，即后来的 BBN 公司），并且对于会存在哪些应用或者协议都没有做出具体计划。

在接下来的几个月里，阿帕网的与会者们对各个站点均进行了访问并且关于针对协议可能采用的应用和架构作了广泛讨论。在 1969 年 3 月，与会者们为自己分配了与他们已做各种话题讨论有关的撰写任务。Steve Crocker 记录了讨论话题之一，实际上就是 RFC 1，并且还承担着整理讨论草稿和笔记的任务。后来这项任务演化为意见征询 (RFC) 3、“文件条约”，以及制定术语“意见征询”。作为创建 RFC 的一部分，Crocker 为每位作者发放了一个 RFC 号码。他还为这个特别代表小组创造了术语“网络工作组”，该小组最初仅包括来自初始四个站点的成员，但后来逐渐增加到五十多名参加人员。在 1971 年 6 月，Crocker 离开了加州大学洛杉矶分校 (UCLA) 加入 ARPA，并让当时还是 UCLA 研究生的 Jon Postel 接管 RFC。

除了分发 RFC 号码之外，Crocker 和 Postel 还负责为各种服务分配端口号码，例如，文件传输协议 (FTP) 端口为 21、Telnet 协议端口为 23 等。BBN 负责选择 IMP 地址，并且在 IMP 地址交付时仅有序列号与之相对应。由于针对 RFC 或者端口号码分配的参与度不足，所以无法使其提高到具备识别功能的水平。

然而，1972 年 5 月，Postel 撰写了 RFC 349，表述如下：

我提议要有一个“沙皇”（我本人？）来分发标准协议所用的官方套接字号码。此“沙皇”还应在可获得主机具体服务的地方对这些套接字号码保持跟踪并发布套接字号码列表。⁷

RFC 349 还包含最初分配的提议列表。这也成为了后来怎样演变为 IANA 职能的示范。

IANA 职能最初是由 Postel 来执行，当时他还是 UCLA 的研究生；在他博士毕业后加入了美国南加州大学信息科学研究所 (USC/ISI)，IANA 职能随之同时迁移。这些职能大部分是在需要时予以执行，并作为美国国防部 (DoD) 所资助的各种研究项目的一个未成文的组成部分，包括多计算机架构、数据库技术、信号处理、气候模拟、人/机通信以及其他项目。⁸ 这些研究项目制定了互联网运营所要依据的协议，并制定了文档和行政结构，使得此协议得以公开发布。随着协调需求的增长，网络研究社群不断依赖于 Jon Postel 博士来记录越来越多标识符的权威列表。这些职能应社群的要求和许可予以执行，这就是后来我们所熟知的“互联网号码分配机构”。然而，针对以及代表网络工作组以及后来的 IETF⁹ 所执行的文档和行政结构直至 20 世纪 90 年代后期才被正式承认为合同语言。因此，可以以两种方式来查看 IANA 职能：一种是服务于 IETF；另一种是根据合同所执行的活动。

2.2 服务于 IETF 的 IANA 职能

从演化为定义互联网的网络协议制定之初，一直都有记录个性化那些协议及其用途的各种运营参数的需求。最初，这些运营参数记录于 RFC 之中，源自网络工程师以及协议设计师小组（他们称自己为“网络工作组”（NWG））的会议。¹⁰ 如前所述，Jon Postel 博士自愿承担记录这些运营参数的角色。

根据 RFC 82 的记载，“网络信息中心”（NIC）作为“一件特殊事宜，未得到 ARPANET 的具体指令”，于 1970 年在斯坦福研究院成立。¹¹ 网络信息中心收藏了 NWG 制定的各种文件（包括 RFC 系列），其中包括收集了全部已分配的号码以及其他参数的“号码分配”RFC。在 1972 年至 1994 年间，这些号码分配 RFC 以各种形

⁷ <http://tools.ietf.org/html/rfc349>

⁸ 例如，ARPA 项目 AF30(602)-4277 “图形化人/机通信” (<http://www.dtic.mil/dtic/tr/fulltext/u2/726623.pdf>) 引自 RFC 33 (<http://www.rfc-editor.org/rfc/rfc33.txt>) 作为“主机对主机协议”制定的资助。

⁹ IETF (<http://www.ietf.org>) 是一个“开放的国际社群，由与互联网体系结构的发展和互联网的平稳运行相关的网络设计人员、运营商、供应商和研究人员组成。”

¹⁰ <http://tools.ietf.org/html/rfc3>

¹¹ 请参阅 <http://www.rfc-editor.org/rfc/rfc82.txt>。

式予以定期发布，最后一个号码分配 RFC (RFC 1700¹²) 表明最新的分配信息保存在在线文本文件中，并且 RFC 的内容“由 catinating [sic] 集合，这些文件以使用最少‘胶水’的形式聚在了一起。”1990 年发布了 RFC 1060，在号码分配 RFC 文本中有记录以来首次使用术语“互联网号码分配机构”。¹³ 2002 年发布了 RFC 3232，¹⁴ 正式作废了号码分配 RFC，将 RFC 1700 化为历史。

1987 年日常的互联网地址和自治系统编号的分配由国防数据网络-网络信息中心 (DDN - NIC) 承担，¹⁵ 并且单独跟踪的 RFC 记录了他们的分配直至 1990 年。¹⁶ 在号码分配 RFC 方面，互联网地址和自治系统编号分配的发布后来转为在线形式，并且发布于 1992 年的 RFC 1366¹⁷ 已开始建立地区互联网注册局系统。

1992 年，互联网架构委员会 (IAB)¹⁸ 正式获得国际互联网协会的许可，负责“各种互联网号码分配的管理”以及对“管理互联网协议号码分配的互联网号码分配机构 (IANA)”进行指定。¹⁹

随着 IETF 的演进发展并变得更加正式，进行 IANA 分配时所依据政策的明确性对于互联网协议的持续发展变得更为关键。1998 年，互联网工程指导组 (IESG)²⁰ 强制实行了一项要求，即在某个注册表或某个注册表内容需要创建、修改或删除的任何时候，所有的互联网草案都要提供明确说明，这被称为“IANA 考量”。²¹

2000 年，IETF 与 ICANN 签订了谅解备忘录，确定“由 IANA 代表 IETF 和互联网研究任务组 (IRTF) 来执行技术工作。”此谅解备忘录被记录为 RFC 2860，²² 明确表示 ICANN 会“使 IANA 遵守”的要求是“IANA 将仅分配和注册由 RFC 中规定的标准和程序所指示的互联网协议参数”并且域名和互联网协议 (IP) 地址段的分配“不在此谅解备忘录的范围内。”

自 2000 年以来，IETF 发布了很多其他的 RFC 并且签订了与 IANA 职能相关的很多协议。这些 RFC 以及其他协议将在第 8.2 节中讨论。

¹² 请参阅 <http://tools.ietf.org/html/rfc1700>。

¹³ 请参阅 <http://tools.ietf.org/html/rfc1060>。

¹⁴ 请参阅 <http://tools.ietf.org/html/rfc3232>。

¹⁵ 请参阅 <http://tools.ietf.org/html/rfc1020>。

¹⁶ 请参阅 <http://tools.ietf.org/html/rfc1166>。

¹⁷ 请参阅 <http://tools.ietf.org/html/rfc1366>。

¹⁸ IAB (<http://www.iab.org>) 提供了 IETF 活动的架构监督。

¹⁹ <http://tools.ietf.org/html/rfc1601>，第 2(d) 节和第 2.4 节。

²⁰ IESG (<http://www.ietf.org/iesg>) 负责 IETF 活动以及互联网标准流程的技术管理。

²¹ 请参阅 <http://tools.ietf.org/html/rfc2434>。

²² 请参阅 <http://tools.ietf.org/html/rfc2860>。

2.3 IANA 职能合同的历史

IANA 职能最初按照要求以特殊的风格予以执行，而在 20 世纪 90 年代，随着互联网经历着上升性增长以及商业化，IANA 职能在合同中变得正式化。这一趋势的加强源自 1995 年国家科学基金会 (NSF) 决定准许 Network Solutions (该公司提供 InterNIC²³ 的“注册服务”部分，以与 NSF²⁴ 于 1993 年所达成的一份合作协议为依据) 对分配域名收费。²⁵

1997 年，IANA 职能被记录于美国能源部的 Tera-node 网络技术合同工具之中。²⁶ 这些被指定的职能包括：

- 1) “参数分配”；
- 2) “地址管理”；以及
- 3) “域名系统监督。”

2000 年 2 月，NTIA 签署了首份独立的 IANA 职能合同。²⁷ 此合同与 ICANN 制定，ICANN 是于 1998 年成立的一个机构，是美国加利福尼亚州的一家非营利性公益组织。²⁸ 最初 IANA 职能合同明确的活动内容有：

- 1) “协调技术协议参数的分配”；
- 2) “履行与根管理有关的管理职能”；
- 3) “IP 地址块的分配”；以及
- 4) “其他服务”。

构成 IANA 的职能已随着时间演进。当前的整套职能定义于由 NTIA 在 2012 年 7 月发布的最新版 IANA 职能合同之中²⁹，并且由 IANA 职能运营商 (ICANN) 予以执行，包括：

- 1) DNS 根域管理；
- 2) 互联网号码注册管理；

²³ InterNIC 是针对 NSFNET 进行扩展和协调目录与数据库服务以及信息服务的一个 NSF 项目，并且为非军事的互联网网络提供注册服务。最初的 InterNIC 授予者分别是负责“注册服务”的 Network Solutions、负责“信息服务”的 General Atomics 以及负责“目录和数据库服务”的 AT&T。该计划指南可通过以下链接找到：<http://www.nsf.gov/pubs/stis1992/nsf9224/nsf9224.txt>。

²⁴ 请参阅 <http://archive.icann.org/en/nsi/coopagmt-01jan93.htm>。

²⁵ 请参阅 <http://archive.icann.org/en/nsi/coopagmt-amend4-13sep95.htm>。

²⁶ 请参阅 Jon Postel 和 Joe Bannister 于 2000 年 3 月 15 日发布的“Tera-node 网络技术 (任务 4) 网络基础架构活动 (NIA) 最终报告” (<http://www.osti.gov/scitech/biblio/802104>)。

²⁷ 请参阅 <http://www.ntia.doc.gov/files/ntia/publications/ianacontract.pdf>。

²⁸ 请参阅 <https://www.icann.org/resources/pages/articles-2012-02-25-en>。

²⁹ 请参阅 http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf。

- 3) 协议参数注册表和 .ARPA 顶级域名管理；以及
- 4) .INT 管理。

这些职能中的每个职能均将在后续章节中予以详细描述。

3 DNS 根域管理职能

作为全球互联网的组成部分，DNS 包含以下内容：

- 1) IETF 定义的一组协议规格；
- 2) 实施这些协议的各种软件服务器和客户端应用程序；
- 3) 在其上部署软件的网络基础设施，包括由互联网服务提供商（ISP）和其他组织运营的根域名服务器、其他权威域名服务器³⁰ 以及缓存解析器；
- 4) “域名空间”，*///*可以通过 DNS 协议查找（解析）的所有唯一域名，由客户端（例如，Web 浏览器这样的应用程序或电子邮件服务器）通过 DNS 基础设施发送针对这些域名的查询。IETF 考虑在该基础设施中也包括“技术用途”的域名，这些域名旨在从语句构造上和功能上与 DNS 域名兼容，但不可在 DNS 中进行查找。一个这样的示例是 .local。³¹

DNS 根域管理职能允许通过更新代表 DNS 域名空间的数据库来更改到该域名空间的最高级域名（“root”）。在公共互联网的背景下，DNS 域名空间的最高级别定义为一组域名（称为顶级域名或 TLD），作为 IANA 根域管理职能运营商的 ICANN 与作为根域维护者的 Verisign 和作为根域管理员的 NTIA 合作对这些域名进行协调。例如，当解析程序获得这些协调的数据之后，通过使用根域名服务器发布协调后的根域，域名空间的一致性就可以得到保证。这种协调实现了 DNS 协议所需的“单个根”，³² 这就确保在公共互联网上随时随地地查找域名都会产生域管理员计划中的响应。³³

根据现有的约定和协议，IANA 根域管理职能是用于修改互联网 DNS 的根域的唯一商定机制。因此，对任何顶级域名（国家和地区代码顶级域名、通用顶级域名或者 .INT 或 .ARPA 顶级域名）或者根域自身的更改请求必须通过 IANA 根域管理

³⁰ 其中权威域名服务器针对其所负责域名的查询给出权威答复，并且包括顶级域名服务器、二级域名服务器等。

³¹ 请参阅 <http://www.ietf.org/rfc/rfc6761.txt>。

³² 请参阅 <http://www.ietf.org/rfc/rfc2826.txt>。

³³ DNS 协议中没有限制域名空间的数量，甚至在单个域名类中也没有此类限制（基本上所有的 DNS 事务都在“IN”类中，“IN”代表互联网）；然而，所有域名空间必须完全分离以确保解析的一致性。

职能实施。2013 年 9 月，ICANN 发布了“审计报告”，该报告描述了由根域管理职能实施的更改。³⁴

由于 DNS 具备分布式和层级特性，显然值得注意的是，根域管理职能仅影响根域的内容（即顶级域名的授权和相关资源）和根域自身的有关信息（例如，根域名服务器和关联的地址，以及根域的 DNS 安全扩展（DNSSEC）签名）。与较低级别 DNS（例如，顶级域（二级域，如 EXAMPLE.ORG）以及沿域名空间层级结构往下的域的内容）相关的更改并不通过根域管理职能进行管理，并且不涉及 IANA 职能合同或受其影响。

DNS 根域管理职能是到目前为止政治上最敏感的 IANA 职能。这种政治关注度来源于三个主要因素：

- 1) NTIA 涉足根域管理职能，其角色是 (a) 验证 ICANN（作为 IANA 职能运营商）在处理更改请求时遵循设立的政策和程序，然后是 (b) 授权修改数据和资源。这种涉足程度尽管有限且面向流程，但其可能定期受到美国政府的不正当影响（并因此广受批评），特别是对于国家和地区代码顶级域名的相关更改，这种域名通常被视为国家资源。³⁵
- 2) 根域管理从整体上承担互联网运营的重大风险和潜在的直接风险，因为它可能涉及更改所有互联网用户及其应用程序所依赖的公共域名空间顶点。
- 3) 有关 DNS 根域中确定哪些域名有效的政策决策往往是敏感的。与其对其他 IANA 职能所担当的角色不同，ICANN 对这些决策同时具备政策制定和实施职责。IANA 职能合同目前规定³⁶，负责 IANA 职能运营的员工不再参与 ICANN 的政策制定，但关于同一组织内存在的政策制定和运营是否适当，仍然存在不同的理解。

3.1 根域管理类别

根域管理职能包括五种广泛的职责类别：

- 1) 根域更改；
- 2) 注册（“Whois”）数据更改；
- 3) 授权和再授权；

³⁴ 请参阅 <https://www.iana.org/performance/root-audit> 以了解更多相关信息。

³⁵ 例如，请参阅近期针对 ICANN 的诉讼，其中申诉人主张国家和地区代码顶级域名是一种财产 (<http://domainincite.com/17008-terror-victims-try-to-seize-five-cctlds>)，ICANN 对此的回应是国家和地区代码顶级域名不是财产。

³⁶ 请参阅 2012 年 10 月 1 日授予的 IANA 职能合同的第 C.2.5 节“政策制定与运营者角色的分离”，网址为 http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf。

- 4) 根域名服务器更改；以及
- 5) 根域“密钥签名密钥”(KSK) 管理。

前四种类别涉及可以直接和立即影响互联网运营的修改。因此，NTIA 通过验证 ICANN 在处理更改请求时已遵循设立的政策和程序来明确授权这些更改。第五种类别有运营方面的影响，但这种影响会延迟体现，因此 NTIA 通过其授权的、经过密钥签名密钥 (KSK) 签名的域签名密钥对根域进行 DNSSEC 签名，从而以非明确的方式提供此类授权。³⁷

3.1.1 根域更改

根域更改是修改互联网 DNS 的根域的请求。这些更改包括：

- 1) 添加或移除顶级域名的授权。
- 2) 添加、更改或删除域名服务器及其关联的顶级域名地址或“粘合”记录。
- 3) 添加、更改或删除已支持 DNSSEC 的顶级域名使用的“授权签署人”(DS) 资源记录；以及
- 4) 添加、更改或删除域名服务器及其关联的根域地址或“粘合”记录。

根域更改通常涉及五个独立的相关方：³⁸

- 1) 更改申请者，通常是顶级域名的管理者或管理员。³⁹
- 2) 作为 IANA 职能运营商的 ICANN；
- 3) 作为根域管理者的 NTIA；
- 4) 作为根域维护者的 Verisign；以及
- 5) 根服务器运营商。

在最新版本的 IANA 职能合同中，ICANN、NTIA 和 Verisign 称为根域管理合作伙伴（更改申请者和根服务器运营商不必遵守 IANA 职能合同）。虽然 ICANN 与 NTIA 之间（IANA 职能合同）以及 Verisign 与 NTIA 之间（合作协议）均有协议，⁴⁰但在根域管理的背景下，ICANN 与 Verisign 之间没有直接的协议。⁴¹

³⁷ 更具体来说，NTIA 授权由根域维护者 (Verisign) 使用安全密钥响应 (SKR)。SKR 是 ICANN 密钥仪式的产物，并且因此是 ICANN 运用 KSK 的结果。

³⁸ 其中一些相关方扮演多个角色：ICANN 是 IANA 职能运营商以及根服务器运营商；Verisign 是根域维护者，并且是两个根服务器的运营商以及 .COM、.NET 和其他顶级域名的顶级域名管理员；NTIA 则是根域管理员和顶级域名管理员。

³⁹ 现行做法是将顶级域名管理的角色分为三种：“支持组织”或“管理者”、“管理联系人”(AC) 和“技术联系人”(TC)，后两种角色（在理论上）由管理者任命。根域更改通常同时需要 AC 和 TC 角色。

⁴⁰ 1998 年 10 月签订的合作协议各版本修正案发布于 <http://www.ntia.doc.gov/page/verisign-cooperative-agreement>。

图 1 提供了用于根域更改的高级别根域管理流程图。该图中显示的步骤是：

- 1) 更改申请者创建根域更改请求，通常的方法是登录 ICANN 的根域管理系统并更新适当的字段。然后申请者向 ICANN（作为 IANA 职能运营商）提交更改请求。⁴²
- 2) ICANN 接受并验证更改请求之后，会将其转发给 NTIA（作为根域管理员），同时将一份副本发送给 Verisign。
- 3) NTIA 验证 ICANN 在处理更改请求时已遵循设立的政策和程序之后，会在发送给 Verisign 的通知中授权实施更改。该通知使第 2 步中 ICANN 直接发送给 Verisign 的更改请求得以实施。
- 4) Verisign 实施更改请求（通过修改根域文件）之后，它使用 DNSSEC 签名更新后的域并每天两次将新签名的域置于 Verisign 运营的“分布主服务器”中。将更新后的域置于分布主服务器中之后，13 个根服务器就可以专门或自动从这些分布主服务器取出更新后的域。
- 5) 签名更新后的根域并将其放入分布主服务器之后，Verisign 通知 ICANN 和 NTIA 更改已完成。
- 6) 一旦 Verisign 通知 ICANN 更改已完成⁴³ 且 ICANN 已验证更改正确反映在互联网的根域中，ICANN 就会通知申请者，其更改请求已得到处理。

⁴¹ 请参阅 http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf 中第 15 页上的脚注 1 和第 16 页上的脚注 2。

⁴² 顶级域名管理员不需要在提交请求之前更新它们的域，然后；然而在大多数情况下，需要在 ICANN 尝试验证更改请求（步骤 2）之前更新域。

⁴³ ICANN 监控根服务器，在根域中检测到更改或从 Verisign 收到通知之后，它就可以通知申请者更改已完成。

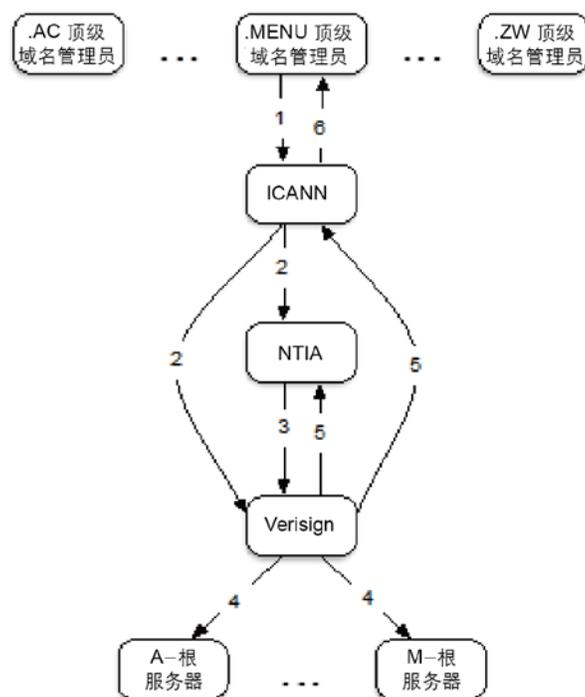


图 1. 根域的域名服务器更改流程

3.1.2 注册 (“WHOIS”) 数据更改

注册数据更改会导致创建、更改或删除与顶级域名关联的注册（也称为 “WHOIS”）数据。这些更改包括修改一个或多个 “支持组织”、“管理联系人” 和 “技术联系人” 的顶级域名联系人信息。这些更改也可能更新与顶级域名关联的其他非 DNS 相关信息（例如，“WHOIS” 服务器）。这些并不是成功解析 DNS 根域中域名的必需数据，但要使管理流程正确而可靠地运作，就会需要用到它们。

注册数据更改涉及三个相关方：

- 1) 更改申请者，通常是顶级域名管理员或管理者；
- 2) 作为 IANA 职能运营商的 ICANN；以及
- 3) 作为根域管理员的 NTIA。

由于注册数据更改不涉及 DNS，而是仅修改由 ICANN 管理的 IANA 顶级域名注册数据库，因此作为根域维护者的 Verisign 和根服务器运营商都不参与其中。

图 2 提供了用于注册数据更改的高级别根域管理流程图，其中标记了每个步骤。这些步骤是：

- 1) 更改申请者创建更改请求并将其提交给 ICANN（作为 IANA 职能运营商）。
- 2) ICANN 接受并验证更改请求之后，会将其转发给 NTIA（作为根域管理员），由其验证 ICANN 已遵循设立的政策和程序。验证 ICANN 遵循适当的程序之后，NTIA 授权 ICANN 进行更改。

- 1) NTIA 授权更改之后，ICANN 更新 IANA 顶级域名注册数据库。
- 2) ICANN 通知申请者更改已完成。

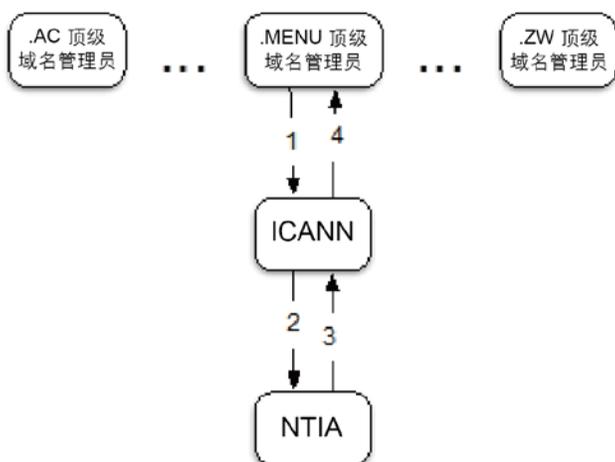


图 2. 注册数据更改流程

3.1.3 授权和再授权

授权是将顶级域名的控制权最初迁移到管理员处。再授权是将顶级域名的控制权从已有的管理员（目前的管理员或预授权管理员）迁移到新管理员处（后期授权管理员）。这些运营涉及四个关键方：

- 1) 预授权顶级域名管理员（在再授权的情况下）；
- 2) 后期授权顶级域名管理员；
- 3) 作为 IANA 职能运营商的 ICANN；以及
- 4) 作为根域管理员的 NTIA。

此类请求仅涉及注册数据更改，或者同时涉及注册数据更改和根域更改。当更改请求同时涉及注册数据更改和根域更改时（即顶级域名管理员更改域的技术配置使之与管理控制的更改保持一致），ICANN 将执行与技术配置更改相关的流程部分。作为根域维护者的 Verisign 将如 3.1.1 节所述进行适当的根域更改。

授权是再授权的简化情况，因为没有预再授权管理员的参与，并且只有在初次将顶级域名放入根域时才会发生授权。⁴⁴ 这种简化减少了参与方的数量，并且降低了争用或延迟的可能性。但是，授权中的步骤在其他方面与再授权相同。

⁴⁴ 从技术上来说，如果从根域中删除顶级域名并在之后重新放入，则也会发生授权。

图 3 提供了用于再授权更改的高级别根域管理流程图，其中标记了每个步骤。这些步骤是：

- 1) 更改申请者创建更改请求并将其提交给 ICANN（作为 IANA 职能运营商）。
- 2) ICANN 接受并验证更改请求之后，会将其同时转发给预再授权和后期再授权顶级域名管理员，并且请求每个管理员通过肯定确认更改请求进行响应。
- 3) 预再授权和后期再授权顶级域名管理员收到更改通知之后，每个管理员会将肯定确认的响应发给 ICANN。
- 4) ICANN 从两位管理员处收到肯定确认之后，将请求转发给 NTIA（作为根域管理员），由 NTIA 验证 ICANN 遵循设立的政策和程序，并且授权实施更改。
- 5) NTIA 授权实施更改之后，ICANN 更新 IANA 顶级域名注册数据库。
- 6) ICANN 同时通知预再授权和后期再授权顶级域名管理员：此项更改请求已完成。

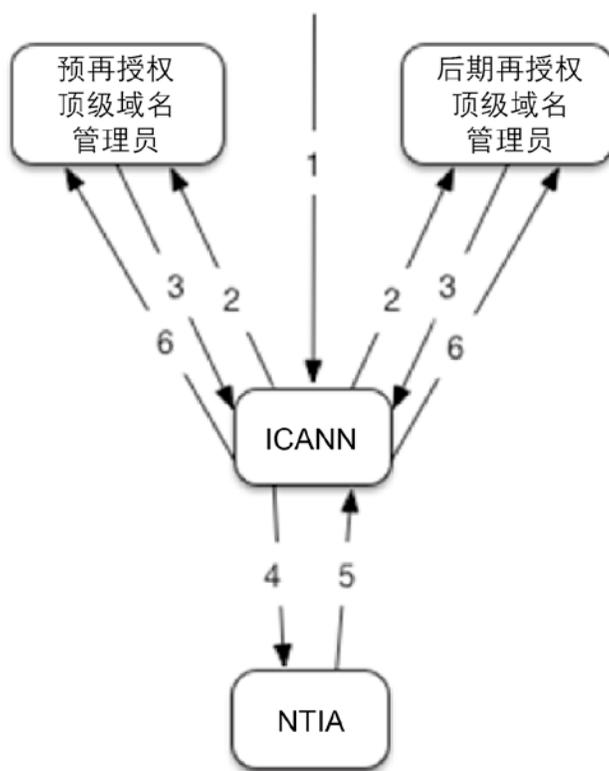


图 3. 根域再授权流程

再授权流程在某种程度上存在争议的关键方面是 RFC 1591⁴⁵ 中提出的要求，即由 IANA 员工验证再授权是否存在“本地社群支持”。这就要求 ICANN 员工从相关社群成员处征询意见并询问他们是否反对控制权的迁移。有时，这种征询意见会导致争议，即政府声称必须进行迁移，而本地互联网社群参与者持反对意见。在这种情况下，用于解决冲突的传统 IANA 方法（直到所有相关方达成一致意见才能继续处理再授权请求）会导致在处理再授权请求时产生大量延迟。

在绝大多数的再授权流程中，控制权的转移在相互达成一致的情况下即可实施。然而在某些情况下，目前的顶级域名管理员拒绝配合再授权，或者已无法或不愿意肯定确认再授权请求。缺乏肯定确认的原因包括内部冲突——政府职能瘫痪、内战等，但更常见的原因是由于目前的顶级域名管理员与后期再授权顶级域名管理员就顶级域名应如何运营、谁应为何种再授权付款等方面未达成一致意见。

这些没有相互达成一致的情况可能要花费大量时间（大约数年时间）来解决。但是，这种情况越来越少见，因为 ICANN 和顶级域名管理员职责范围内的顶级域名管理流程已经变得更加正式化。

在许多情况下，根域更改会放入再授权请求中，因为后期再授权顶级域名管理员在承担顶级域名控制权时通常想要更改域名服务器。根域更改发生的时间点可能会改变，但通常按顺序处理更改请求：最先处理管理再授权（或初始授权）请求，然后处理根域更改请求。

3.1.4 根域名服务器更改

虽然没有明确成为 IANA 职能合同的一部分，但对根服务器列表的维护是作为 IANA 根域管理职能的一部分执行的活动。由于 DNS 运营的方式，大多数解析程序需要预先知道至少一个根域名服务器的至少一个 IP 地址，这样才能在缺少顶级域名的域名服务器信息时知道将查询发往何处。当这些解析程序启动时，它们会向最常称为“根提示”的列表中配置的某个根服务器地址发出“初始查询”。这些根提示来源于由作为 IANA 根域管理职能运营商的 ICANN 维护的一个文件。⁴⁶

虽然极为少见，但有时根域名服务器需要更改它们的 IP 版本 4 (IPv4) 地址。此外，启用 IP 版本 6 (IPv6) 的根域名服务器的工作正在持续进行当中，这需要为支持 IPv6 的根域名服务器添加 IPv6 地址。这些请求的处理方式类似于根域更改请求，不同之处在于正在更新的域是 ROOT-SERVERS.NET 而非根域。与根域名服务器更改关联的步骤如下：

⁴⁵ <http://tools.ietf.org/html/rfc1591>

⁴⁶ 根提示文件可在 <http://www.iana.org/domains/root/files> 和 <ftp://ftp.internic.net/domain/named.root> 中找到。

- 1) 根服务器运营商向作为 IANA 职能运营商的 ICANN 发送请求以更新他们的 ROOT-SERVERS.NET 项。
- 2) ICANN 接受并验证更改请求之后，将请求转发给 NTIA（作为根域管理员），同时将一份副本发送给 Verisign。
- 3) NTIA 验证 ICANN 在处理更改请求时遵循设立的政策和程序之后，会在发送给 Verisign 的消息中授权实施更改。该通知使第 2 步中 ICANN 直接发送给 Verisign 的更改请求得以实施。
- 4) Verisign 实施更改请求（修改 ROOT-SERVERS.NET 域）之后，它使用 DNSSEC 签名更新后的域，并将新签名的域置于 Verisign 运营的分布主服务器中，这样就使 13 个根服务器可以自动获得更新后的域。
- 5) 签名更新后的 ROOT-SERVERS.NET 域并将其放入分布式主服务器之后，Verisign 通知 ICANN 和 NTIA 更改已完成。
- 6) 一旦 Verisign 通知 ICANN 更改已完成且 ICANN 已验证更改正确反映在 ROOT-SERVERS.NET 域中，ICANN 就会通知根服务器运营商，其更改请求已得到处理。ICANN 还会更新“根提示”文件并在 IANA.ORG 网站和 [FTP. INTERNIC.NET](http://FTP.INTERNIC.NET) FTP 站点上提供该文件。

3.1.5 根域的 DNSSEC “密钥签名密钥”管理

根据最初的规定，DNS 协议存在一个缺陷，即在 DNS 数据从源（“权威服务器”）流向申请者时可以对其进行修改。申请者通常是称为“递归解析程序”的服务器，该服务器代表客户端应用程序（例如，Web 浏览器、电子邮件客户端等）执行 DNS 查找。IETF 为此缺陷创建了一个修复程序，称为“DNS 安全扩展”（DNSSEC），该程序使用公钥密码系统建立域数据的数字签名，⁴⁷ 将其作为 DNS 数据附带在查询响应中。验证数字签名可确保数据在传输过程中不会被更改。

DNSSEC 的基本要求是在尝试验证所接收域数据的每个递归解析程序中嵌入众所周知的“信任锚”。此信任锚充当验证签名数据的起点，通常在验证响应的递归解析程序中实施（称为“验证递归解析程序”，或直接称为“验证解析程序”）。2010 年 7 月，作为在根域中部署 DNSSEC 的项目的一部分，ICANN（作为 IANA 职能运营商）生成了此信任锚。⁴⁸ 此密钥生成事件发生在第一次根域密钥签名仪式期间，随后的仪式定期举行。每次仪式都作为公开和透明的活动举行，进行网络广播并存档，并且涉及 34 位称为“诚信社群代表”（TCR）的人员。这些 TCR 执行各种角色，比如恢复密钥利益相关方、密钥保管员以及他们的备份。关于当前 TCR 人员及他们所执行角色的清单，请访问 <http://www.root-dnssec.org/tcr/selection-2010/>。

⁴⁷ 从技术上来说，域中具有相同域名的每组资源记录、资源记录类型以及类都会有自己的数字签名。

⁴⁸ <http://www.root-dnssec.org> 中描述了在根域中部署 DNSSEC 的项目。

持续举行的根域密钥签名仪式的目的是使用“密钥签名密钥”（KSK）签名根域“域签名密钥”。⁴⁹ 当前的根域 KSK 是在第一次根域密钥签名仪式中生成的（根信任锚是此 KSK 的公共部分）。接下来，作为根域维护者的 Verisign 使用根域“域签名密钥”对根域进行 DNSSEC 签名，之后将其分发给根服务器。⁵⁰

每个密钥签名仪式的核心职能是从根域维护者处接收一组未签名的公钥材料，这称为密钥签名请求（KSR）；然后产生一组对应的已签名公钥材料，这称为安全密钥响应（SKR）。每个 KSR 的真实性在密钥签名仪式中确认，而产生的 SKR 会送呈给根域维护者。根域管理员负责授权 SKR，然后根域维护者才可以使用该 SKR 发布已签名的根域。

在根域 DNSSEC KSK 管理中，IANA 职能运营商的角色是执行根域密钥签名仪式，确保以可信赖的方式完成管理工作；以某种方式维护根 KSK 以确保它可以得到信任；⁵¹ 并且通过验证递归解析程序来发布准确的根信任锚以供使用。

3.2 更改请求处理

本节概述 IANA 职能运营商在收到更改请求时执行的处理。

3.2.1 更改验证

在所有三个根域管理更改类别中，作为 IANA 职能运营商的 ICANN 负责验证更改请求。除了验证请求在语句构造上正确之外，ICANN 还要确保顶级域名的管理员，具体来说是授权的“管理联系人”和“技术联系人”，同意请求的更改。在过去，这意味着 ICANN 需要通过电子邮件、电话、传真甚至邮递的信件获得同意，并且需要确保在所有相关方都批准的情况下完成更改。⁵² 目前，随着根域管理系统实现自动化，确定申请者是否获得授权的验证工作大部分转移为确定管理员是否有登录凭据。然而，这并没有解决从所有相关方处获得同意的问题。预料之中的情况是，

⁴⁹ 更准确地说，在密钥仪式期间分别签名多个 DNSKEY RRSet。这些 DNSKEY RRSet 包括 KSK 的公共部分以及一个或多个 ZSK 的公共部分。

⁵⁰ 根域 DNSSEC 架构超出了本文档的介绍范围，但简而言之，将密钥签名密钥与域签名密钥分离就可以频繁更改域签名密钥，而无须使用新的信任锚修改全球的每个解析程序。有关更多信息，请访问 <https://www.iana.org/dnssec/icann-dps.txt>。

⁵¹ ICANN 的 KSK 设施实施包括两个分布在不同地点的、对访问进行控制的设施，这些设施具有多层物理安全措施以及通过美国联邦信息处理标准（FIPS）140-3 认证的硬件安全模块和各种安全控制。该系统从整体上旨在满足“高效”（HIGH IMPACT）系统所需的所有 SP 800-53 技术安全控制，这些安全控制与 FIPS 199 中定义的完整性和可用性有关。请参阅 <https://www.iana.org/dnssec/icann-dps.txt> 以获得 KSK DNSSEC 实践的完整声明。

⁵² 请参阅 <https://www.iana.org/help/obtaining-consent> 以获得相关内容的简要介绍。

从所有相关方处获得同意的流程可能会相当耗费时间，特别是在具有不可靠基础设施的位置运营顶级域名时，或者是在顶级域名的联系人详情没有保持更新时。

3.2.2 技术检查

对于根域更改的情况，IANA 员工会验证权威域名服务器的基准技术是否符合条件。<http://www.iana.org/help/nameserver-requirements> 中描述了构成此基准的要求。这些要求的验证工作已具备较高度度的自动化，并且是在根域管理合作伙伴之间实施的根域管理系统的一部分。

3.2.3 特殊指令

在个别情况下，顶级域名将会有超出正常处理流程的要求。这些要求的示例包括：顶级域名管理员提供了关于其如何实现更改请求的额外指令，或者 IANA 员工必须采取额外的步骤来处理请求，例如联系特定的政府机构或部门以获得全部的权限（如管理本国的疆域或需要获得被制裁实体的豁免权的情况）。在这些情况下，IANA 员工维护一组“特殊指令”，在适当的时候实施这些指令以满足与顶级域名关联的特殊情况。当然，由于其特殊性，这些指令可能会对根域管理系统自动化构成挑战，因为它们要求人为干预，并且可能导致延迟。因此，不鼓励使用这些特殊指令。

3.2.4 自动化

前面讨论过，根管理合作伙伴已部署了“根域管理系统”（RZMS），这是自动化许多根域管理流程的软件。RZMS 为顶级域名管理员提供了基于 Web 的用户界面，在该用户界面中可通过编辑表格上的字段来输入更改请求，例如更新顶级域名管理联系人的邮政地址、向 ICANN 提交这些更改请求以进行验证以及跟踪这些更改请求的处理进程。ICANN 执行的请求处理流程可以通过 RZMS 更加快速地进行。根据 ICANN 于 2013 年执行的“客户满意度”调查，⁵³ 80% 的受访者表示他们对使用 RZMS 更改顶级域名和根域数据的时间线“满意”或“非常满意”。

3.3 美国政府的参与

在当前的根域管理职能架构下，影响根域或 IANA 顶级域名注册数据库的每个请求都需要获得根域管理员 NTIA 的明确授权。美国政府的这种参与存在争议，特别是在授权更改国家和地区代码顶级域名的背景下。随着时间的推移，国家和地区代码顶级域名已经被某些组织（特别是政府）视为国家资源。因此，对这些资源的所有

⁵³ 请参阅 <http://www.iana.org/reports/2013/customer-survey-20131210.pdf>。

更改请求进行授权的根域管理员要求就被某些组织认为是侵犯了国家主权（对于国家和地区代码顶级域名的情况）或干涉到国家商务（对于通用顶级域名的情况），即使是根域管理员的参与仅限于验证 ICANN（作为 IANA 职能运营商）在处理更改请求已遵循设立的政策和程序，然后授权实施此更改。虽然有人认为根域管理员负责判断请求的有效性，但根域管理员的角色与所请求更改的实质没有任何关系。

目前，根域管理员验证 ICANN 已遵循设立的政策和程序，而对实施更改的授权是通过基于 Web 的界面在 RZMS 中执行的。顶级域名管理员将根域更改请求输入 RZMS，IANA 职能运营商在其中验证这些请求。IANA 职能运营商验证请求之后，将通知发送给登录此 Web 界面的根域管理员，⁵⁴ 独立审查请求的更改，确认 ICANN 是否已遵循设立的政策和程序，并且授权实施更改（假设其有权这样做）。这种授权会将更改发布给根域维护者进行实施（包括使用 DNSSEC 进行签名以及分发给根服务器）。

此外，IANA 职能合同授权报告要求，这包括每月执行进度报告、执行标准报告、客户服务调查的结果以及一份最终报告，其中归档“标准运营程序，包括描述在 IANA 职能执行中使用的技术、方法、软件和工具”。⁵⁵ 该合同还包括在安全流程和根域管理中维护审计数据的要求。⁵⁶

4 互联网号码注册管理

此功能管理 IPv4 地址（例如 192.0.2.123）、IPv6 地址（例如 2001:db8::1:be3f）和自治系统编号（ASN，例如，AS 64496 和 AS 65551）。ASN 可作为 ISP 将成批的地址进行分组的标记，用于互联网的路由系统中。IANA 互联网号码注册管理功能遵循一组全球政策，该政策由地区互联网注册局（RIR）系统中的区域管理、自下而上、形成共识的政策定义流程定义。在将整套政策提交给 ICANN 进行审批前，必须得到所有 5 个 RIR 的一致同意。这些政策的详细内容参见 <http://www.icann.org/en/resources/policy/global-addressing>。这些政策说明通过哪些流程以及在哪些情况下可将互联网号码分配给 RIR。

IANA 互联网号码注册管理功能分配的号码在管理上有明确的唯一性，以此体现其可用性和价值。也就是说，以 IPv4 为例，IPv4 地址为简单的 32 位整数，数值

⁵⁴ 尝试连接 Web 界面的客户端必须提供有效的 X.509 (SSL) 客户端证书。

⁵⁵ 请参阅 http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf，第 C.4.2、C.4.4、C.4.5 和 C.4.6 节。

⁵⁶ 请参阅 http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf，第 C.5.1 和 C.5.2 节。

范围从 0 至 4,294,967,295，实质上任何设备均可由该范围内的数字配置。⁵⁷ 然而，如果该设备已成功连接至互联网，则分配给该设备的号码（地址）相对于分配给直接连接至互联网的任何其他设备的地址**必须**具有唯一性。具有顶级 IANA 互联网号码注册管理功能的互联网号码注册系统确保此唯一性。

4.1 互联网号码注册管理功能

在日常实践中，互联网号码注册管理功能包括：

- 1) 将成批的 IPv4 地址分配至 RIR，并将那些分配的地址记录在 IPv4 地址注册表中，详细内容参见 <http://www.iana.org/assignments/ipv4-address-space>；
- 2) 创建、修改或删除与 IPv4 地址块相关的 IN-ADDR.ARPA 授权，从而协助 IPv4 地址命名 DNS 中的映射；⁵⁸
- 3) 将成批的 IPv6 地址分配至 RIR 并将那些分配地址记录在 IPv6 地址注册表中，详细内容参见 <http://www.iana.org/assignments/ipv6-unicast-address-assignments>；
- 4) 创建、修改或删除与 IPv6 地址块关联的 IP6.ARPA 授权，从而协助 IPv6 地址为 DNS 中的映射命名；⁵⁹
- 5) 将成批的自治系统编号分配至 RIR，并将那些分配号码记录在自治系统编号注册表中，详细内容参见 <http://www.iana.org/assignments/as-numbers>；
- 6) 在建立 RIR 前，从地区注册局或收到分配号码的机构处接收返回的成批地址或自治系统编号；以及
- 7) 更新 IANA 网站上的 IPv4、IPv6 和自治系统编号注册表。

4.1.1 IPv4 地址管理历史背景

IPv4 地址池管理拥有悠久的历史，早在 20 世纪 80 年代，初期分配号码记录在最早的“号码分配”RFC 中。随着互联网的演进发展，那些地址的管理方法发生了

⁵⁷ 某些地址范围具有特殊的含义，例如，“此计算机”或“组播寻址”，这是由将可用性限制为常规地址的软件定义的。

⁵⁸ 通过颠倒八位位组的顺序、附上“.IN-ADDR.ARPA”并使用 DNS“指示器”(PTR)资源记录，IN-ADDR.ARPA 授权能够将 IP 地址（例如 192.0.2.143）映射回一个名称，将该域名（即，“143.2.0.192.IN-ADDR.ARPA”）与其主机名称（例如，“MYPC.EXAMPLE.COM”）、RFC 1034 中定义的映射规范关联。目前，此功能主要用于于登陆系统，进而将用户友好名称与 IP 地址和某些反垃圾邮件系统关联，因为许多传送垃圾邮件的计算机为家庭计算机，它们已受到恶意软件攻击且未设置其 IN-ADDR.ARPA 域。

⁵⁹ IP6.ARPA 对于 IPv6 的功能与 IN-ADDR.ARPA 对于 IPv4 的功能相同，如 RFC 3596 中所述 (<http://tools.ietf.org/html/rfc3596>)。

重大变革。最初，互联网协议的设计人员以为只会出现少数的大型网络，其与国家垄断的电话网共存。结果，首个寻址模型实现了多达 256 个网络，而每个网络拥有多达 16,777,216 个主机。

网络的分配很简单：负责网络的人员（大部分人员都属于极少数网络研究者群体）会联系“号码沙皇”（Jon Postel 博士）并索要一个网络号码。将无偿提供网络号码列表中的下一个号码，并且无明确的或书面使用条款，这种方法在当时很适用，因为连接的网络只针对一个研究活动，这类活动已经规定了相互信任并共同遵守不成文的行为和互动规范的内容。

然而，后来，网络运营者发现一个规格无法满足所有需求，并且除了几个大型网络之外还有可能出现大量的小型网络。自从按顺序分配网络号码后，设计出了一个有趣的规律：如果地址的第一位为“0”，那将为“A类”网络，最多能够容纳 16,777,216 个主机。如果前两位为“10”，那将为“B类”网络，最多能够容纳 65,536 个主机，如果前三位为“110”，那将为“C类”网络，最多能够容纳 256 个主机。此数学划分意味着将出现多达 128 个“A类”网络（地址涵盖 0.0.0.0 - 127.255.255.255），32,768 个“B类”网络（涵盖 128.0.0.0 - 191.255.255.255），以及 2,097,152 个“C类”网络（涵盖 192.0.0.0 - 223.255.255.255）。

根据地址的前三⁶⁰位对地址空间进行的“分类”划分意味着之前所做的所有划分可作为祖父级划分，并且为新网络分配的尺寸仍具有灵活性。如果他们请求“A类”，那么分配大体上就是“有求必应”的事，即便会询问请求者“为什么？”，且根据 DoD 合同，Jon Postel 博士所负责的维护网络号码列表的后勤工作转由斯坦福研究院（现为斯坦福国际研究院）运营的“网络信息中心”执行。

在 80 年代中期，分配的大部分网络号码为“B类”，因为人们认为“A类”过大，而“C类”过小。⁶¹对网络号码使用情况的预测表明“B类”将于 90 年代中期耗尽。⁶²除了引发后来 IPv6 的情况出现外，“B类”耗尽这些预测也导致“无类”寻址产生，其中固定的类别界线已经模糊，中型网络请求者不会得到“B类”网络号码，而会得到足以满足其实际需求的一套连续性“C类”网络号码。

到 90 年代中期，随着互联网越来越多地被用于商业用途（美国尤其如此⁶³），“无类”寻址产生的“C类”网络的扩张对互联网路由系统造成极大的压力：当时的路由器只识别“有类”寻址，没有足够的内存容纳所有公布的网络，并且指示某

⁶⁰ 另外还有两类地址：“D类”（前四位为“1110”），用于“组播寻址”；以及“E类”（前四位为“1111”），保存供以后使用。然而，本文不对以上地址分类进行探讨。

⁶¹ 请参阅 <http://tools.ietf.org/html/rfc1517>，第 1 节。

⁶² 请参阅 <http://www.watersprings.org/pub/id/draft-solensky-csharp-00.txt>，“背景”部分。

⁶³ 在美国以外，大部分机构认为最终会采用基于 OSI 的协议，因此地址请求主要来自位于美国的机构。一些此类讨论已列于 20 世纪 80 年代末期至 20 世纪 90 年代初期的 RFC 中，例如 RFC 1287 (<http://www.ietf.org/rfc/rfc1287.txt>) 第 1.2 节。

个网络是否可访问的更新信息占据着路由器“中央处理器（CPU）”的全部容量。此外，互联网的国际化发展产生了政治压力，因为针对的是分散的分配系统，而非美国国内的一个中央系统。为了限制路由系统的增长，并分布网络分配机制，创建并使用了 RIR 系统⁶⁴，以确保仅提供经实际网络要求证实的分配地址。

历史的发展和互联网的部署方式导致 IPv4 地址的分配不平等：在很早以前（80 年代末期以前）采用互联网的机构（例如大学）能够在基本无证实的情况下获取大批地址，而后来的进入者——甚至国家级网络——也必须在向分配机构证实后才能获取地址。这种不平等分配在今天还是个政治问题，而随着人们使用非分配的 IPv4 地址池，这个问题尤其严重。

4.1.2 IPv4 地址管理

分配 IPv4 地址的流程已作为 IANA 功能的一部分记录以下链接中：<https://www.icann.org/resources/pages/allocation-ipv4-rirs-2012-02-25-en>。然而，自 2011 年 2 月 3 日起，由于 IANA 互联网号码管理功能所管理的 IPv4 免费地址池已耗尽，该政策被废弃。今天，IANA 互联网号码管理功能的相关政策被命名为“IANA IPv4 资源枯竭后分配机制的全球政策”⁶⁵，它描述了将地址空间返回至 IANA 互联网号码管理功能提供者的过程可被重新分配给 RIR。一旦满足该政策，IANA 员工便可修改 IPv4 地址注册表⁶⁶，按照政策的要求进行分配。

4.1.3 IPv6 地址管理

IPv6 地址空间远远大于 IPv4 空间，甚至由 IETF 指定用于“正常”（“全球单播”）IPv6 地址以及由互联网号码注册系统分配的一部分 IPv6 地址空间都远远大于 IPv4 地址的全部空间。⁶⁷ 此外，由于全球政策，⁶⁸ 由 IANA 互联网号码管理功能分配给 RIR 的 IPv6 地址块尺寸非常大——每个 RIR 获得全球单播地址空间的 1/4096⁶⁹，因此在目前子分配政策的情况下，以后 RIR 不太可能需要大量额

⁶⁴ 撰写此报告时，共有 5 个 RIR，每个 RIR 负责一个特定的地理区域：AfrinIC（非洲）、APNIC（亚太地区）、ARIN（北美和部分加勒比海地区）、LACNIC（拉丁美洲和部分加勒比海地区）以及 RIPE-NCC（欧洲、中东和前苏联国家）。

⁶⁵ 请参阅 <https://www.icann.org/resources/pages/allocation-ipv4-post-exhaustion-2012-05-08-en>。

⁶⁶ 请参阅 <http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml>。

⁶⁷ 它实际上是 42, 535, 295, 865, 117, 307, 932, 921, 825, 928, 971, 026, 432 地址。

⁶⁸ 请参阅 <http://www.icann.org/en/resources/policy/global-addressing/allocation-ipv6-rirs>。

⁶⁹ 即 83, 076, 749, 736, 557, 242, 056, 487, 941, 267, 521, 536 地址。

外的地址块。⁷⁰ 当然，1974 年定义原始 32 位 IP 地址空间时，其设计者也曾发表过该空间“永远不可能耗尽”的言论。

将 IPv6 地址块分配给 RIR 的流程类似于 IANA 互联网号码管理功能运营商在 IPv4 免费库耗尽前分配 IPv4 地址块的流程。分配 IPv6 地址的全球政策规定何时 IANA 员工可执行分配（当 RIR “可用空间”低于规定标准或者不足以满足未来 9 个月的要求）以及分配的规模。收到满足全球政策标准的 RIR 请求后，IANA 员工可修改 IPv6 “IPv6 全球单播地址分配”注册表⁷¹ 并向 RIR 通知其分配的地址。

4.1.4 自治系统编号管理

IANA 互联网号码注册管理功能将自治系统编号（ASN）的地址块分配给 RIR，以子分配至请求的机构。最初，仅有 65,536 个 ASN（即，ASN 的协议字段其宽度为 16 位）；然而，IETF 将 ASN 空间扩展至 32 位或超过 40 亿 ASN，2006 年，第一批 32 位 ASN 被发放给 RIR。

虽然不到 500 个未分配的 16 位 ASN 一直处于 IANA 免费库中，但它们正在快速向 32 位转换，16 位 ASN 空间耗尽后不太可能出现重大问题。

4.2 更改请求处理

由于只有 5 个 RIR，且 IANA 互联网号码功能分配给 RIR 的互联网号码资源块的耗尽问题很少发生且可预测，因此 RIR 的更改请求和额外资源请求可直接通过 IANA 功能员工和 RIR 员工之间的互动得到验证。

ICANN 已开发软件⁷²，使用提供给 5 个 RIR 的 ICANN 分配客户证书，将对 IN-ADDR.ARPA 和 IP6.ARPA 区域的更改自动化。除了⁷³ ICANN 作为 IANA 功能运营商直接管理的异常情况以外，RIR 管理 IN-ADDR.ARPA 和 IP6.ARPA 区下的所有授权。

⁷⁰ 由 IANA 互联网号码注册功能分配给每个 RIR 的地址块为足够的地址空间，每个 RIR 可将 IPv6 地址提供给超过一百万的 ISP（而每个 ISP 能够支持 65,000 多个客户）。目前，所有 RIR 的总成员少于 20,000 个 ISP。

⁷¹ 请参阅 <http://www.iana.org/assignments/ipv6-unicast-address-assignments>。

⁷² ICANN 为此用途开发的技术流程和协议已记录于 <http://tools.ietf.org/html/draft-manderso-n-rdns-xml-01>。

⁷³ 异常情况与个人 IPv4 地址——10.IN-ADDR.ARPA 关联的授权（请参阅 RFC 1918，<http://tools.ietf.org/html/rfc1918>）——以及 IPv4 组播寻址相关。

4.3 美国政府参与互联网号码资源管理

从历史角度看，NTIA 未授权 IANA 功能运营商单独分配地址块或自治系统编号。过去，在全球政策实施前，NTIA 确实审阅已被 ICANN 董事会接受的这些全球政策，但此类审阅不代表其具有审批职能。

5 协议参数注册表和 .ARPA 顶级域名管理职能

由于所用注册表数量较多，此 IANA 职能消耗了与 ICANN 的 IANA 职能合同相关的大部分人力资源。⁷⁴ 协议参数为公认（公开记录存档）数字或字符串，这些数字或字符串在主要由 IETF 定义的协议实施中使用。

“地址和路由参数区域”顶级域名在使用 DNS 作为全球级分布式数据库来查询特殊兴趣值的协议中使用。在大多数情况下，这些值由应用程序使用，互联网用户不会直接看到它们。最初，美国国防部使用“.ARPA”域名标签来引用阿帕网（互联网的前身）上的主机；在 2000 年，此域名标签经过重新命名⁷⁵，如今，此域名标签则用作协议。

5.1 协议参数注册表管理

如上文所述，协议参数是在协议实施中使用的值。这些值经过定义，因此，同一协议的不同实施可以在不使用其他信息的情况下交互操作。例如，协议参数包括以下内容：

- 1) 最常用互联网协议 IPv4 的版本号 (4)；⁷⁶
- 2) 万维网使用的“端口” (80) 或“服务名称”（超文本传输协议 (http)）；⁷⁷
- 3) 主要在网络管理应用程序中使用的专用企业号，例如，“1.3.6.1.4.1.5901”（或者使用助记符号，“iso.org.dod.internet.private.enterprise.nominum”）；⁷⁸

⁷⁴ 有关所有协议参数注册表的列表，请访问 <http://www.iana.org/protocols>。

⁷⁵ 请参阅 <http://tools.ietf.org/search/rfc3172>，附录 A。

⁷⁶ 有关各 IP 版本号的协议参数注册表，请访问 <http://www.iana.org/assignments/version-numbers/version-numbers.xhtml#version-numbers-1>。

⁷⁷ 有关端口/服务名称注册表，请访问 <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>。

⁷⁸ 有关 PEN 注册表，请访问 <http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers>。

- 4) “发件人政策框架”资源记录的 DNS 资源记录类型码 (99) 和助记符号 (SPF)。⁷⁹

独立协议参数注册表的总数超过 1,000，每个注册表都包含一个文本文件，此文件用于说明已经注册的参数和值。各注册表都具有自己的创建、修改和删除政策。某些注册表只含一个或两个值，其他一些注册表则包含数万个值。某些注册表很少进行修改，其他一些注册表则每天或每周更新一次。IETF、IESG 或 IAB 定义 RFC 文档的“IANA 考量”章节（必需章节）中最常见的协议参数及其创建、修改或删除政策。在大多数情况下，可以认为协议参数注册表主要与存档相关，在这些注册表中定义的信息为永久的值分配记录，但更改这些注册表不会直接影响互联网的运行。若要使其中一个注册表的更改影响互联网的运行，协议实施者需要创建或更新协议实施以便反映这些新值，然后在互联网上部署这些实施。

检查一个特殊注册表（提供 IPv4 和 IPv6 的 IP 版本号注册表）的工作方式可能会有助于理解 IANA 协议参数注册表功能的作用。很早就在互联网的前身中制定的约定规定网络中各数据包的前 4 位为此数据表所用协议的版本。这样，可以在网络上同时使用多个版本的互联网协议，计算机可以查看它收到的数据包的前四位，然后将此数据包发送至一款软件中，此软件能够理解此数据包所用的 IP 版本。随着新版本互联网协议的出现，协议开发者社区同意分配下一连续版本号并让当时充当“互联网号码分配机构”（IANA）的 Jon Postel 博士记录此号码。

RFC 750，即发布于 1978 年的“号码分配”，记录了表 1 中列出的 5 种不同互联网协议版本。

位	十进制	描述
0000	0	1977 年 3 月版本
0001	1	1978 年 1 月版本
0010	2	1978 年 2 月 A 版
0011	3	1978 年 2 月 B 版
0100	4	1978 年 9 月第 4 版

表 1. IP 版本注册表（截至 1979 年）

“1978 年 9 月第 4 版”互联网协议成为 IPv4 的基础，IPv4 最终成为互联网的底层协议。

但是，互联网协议的发展并未停止。截至 1980 年，名为“流协议”的新协议已经出现；它的开发者申请为其分配一个 IP 版本号，最后，此协议分到了版本号“0101”（十进制的 5）。互联网协议的下一重要发展事件出现在 20 世纪 90 年代早

⁷⁹ 有关 DNS 资源记录注册表，请访问 <http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4>。

期，当时，IPv4 的限值问题已经得到解决，IETF 的协议开发者社区针对“新一代互联网协议”创建了许多不同的备选方案。1994 年，Jon Postel 博士（仍在充当 IANA）分配了互联网协议版本号 6 至 9。此外，由于早期版本的互联网协议（版本 0 至 3）已经不再使用，他从 IP 版本号注册表中删除了版本号 0 至 3。最终的注册表列于表 2 中。

位	十进制	关键字	版本
0000	0	（保留）	
0001	1	（未分配）	
0010	2	（未分配）	
0011	3	（未分配）	
0100	4	IP	互联网协议
0101	5	ST	ST 数据报模式
0110	6	SIP	简单互联网协议
0111	7	TP/IX	新一代互联网
1000	8	PIP	P 互联网协议
1001	9	TUBA	在大地址上使用的 TCP 和 UDP

表 2. IP 版本注册表（截至 1994 年）

随着互联网的不断发展，新版本的互联网协议可能会被 IETF 标准化。如果出现这种情况，待分配的下一版本号将为二进制“1010”（十进制的 10）。但是，代替 Jon Postel 博士履行此职能并且履行协议参数注册表管理职能的 IANA 职能运营商将使用常规的例行协议和参数注册表程序进行注册表的实际修改，就像更改任何其他协议参数一样。

5.2 地址和路由区域（.ARPA）顶级域名的管理

.ARPA 顶级域名的管理包括在 .ARPA 内的二级域中添加授权并修改与 .ARPA 区域有关的授权（和 DNSSEC）信息。.ARPA 区域的更改由⁸⁰ IAB 授权，通常奉 IETF 工作组的命令。

.ARPA 区域的内容由 ICANN 作为 IANA 的职能运营商进行管理；目前，尽管 IANA 职能合同指定此责任将转交 ICANN，但仍由 Verisign 使用 DNSSEC 签署 .ARPA 区域并将签署区域分给域名服务器。⁸¹

⁸⁰ 有关 IAB 对 ARPA 区域的更改的授权责任，请参阅 RFC 3172 (<http://tools.ietf.org/html/rfc3172>)。

⁸¹ 请参阅 ICANN 对 IANA 职能合同 RFP 的响应，第 1 卷，第 1.2.9.1.4 节 http://www.ntia.doe.gov/files/ntia/publications/icann_volume_i_elecsub_part_1_of_3.pdf

IANA 职能合同中未提及其管理的 .ARPA 区域中各二级域名必须使用特殊协议。在编写此报告时，子域及其用途为：

- E164.ARPA。此子域名用于 ENUM 协议，⁸² 它有助于转换电话号码（ITU-T 的 E.164 标识符建议书）以便在互联网中使用。IAB 已经授权由 RIPE-NCC 管理此区域并通过书信往来与 ITU 商讨此区域的管理。有关 IAB 的 E164.ARPA 管理说明书，请参阅 <http://www.ripe.net/data-tools/dns/enum/iab-instructions>。
- IN-ADDR.ARPA。此子域名供 DNS 用于实现 IPv4 地址与域名之间的映射。例如，如果 IPv4 地址为 192.0.2.1，可以通过以下方法发现对应此地址的域名：先颠倒这些数字的顺序，在这些数字之间加上“.”，在后面加上“.IN-ADDR.ARPA”，然后通过 PTR（指针）查找最终域名“1.2.0.192.IN-ADDR.ARPA”。这些映射专业上称作“反向域名解析”，目前主要用于生成日志消息，这些消息中的 IP 地址更易于人们阅读。

IN-ADDR.ARPA 区域中的 228 条目对应一些最高级地址块，这些地址块已经作为 IANA 互联网号码注册管理职能的一部分分配（或者在某些情况下保留），它们的范围为 1.IN-ADDR.ARPA 到 239.IN-ADDR.ARPA。⁸³ 大多数授权都针对接收地址块分配的 RIR 运行的域名服务器。但是，在分配超过 1,600 万相邻地址块时，⁸⁴ 这些授权都针对接收这些地址块的公司；例如，惠普公司（HP）分到 16.0.0.0/8，16.IN-ADDR.ARPA 的域名服务器由 HP 管理。只有负责最终用户所在区域的 RIR 才能更改这些“旧的”授权，而非最终用户组织与 ICANN 的直接互动。

- IN-ADDR-SERVERS.ARPA。此子域名包含在 IN-ADDR.ARPA 区域中用于进行查找的域名服务器。⁸⁵

⁸² <http://tools.ietf.org/rfc/rfc6116.txt>

⁸³ 240 到 255 的地址块留待以后使用（它们是 RFC 1112 定义的“E 级”地址的前身）。在 255 地址块中，“全部”地址 255.255.255.255 由 RFC 919 保留供“有限广播”使用。在 1 到 239 的可能地址块中，只有 228 可以代表 IN-ADDR.ARPA。

⁸⁴ 事实上，16,777,216 的倍数至少反映 24 位地址，又称为“/8s”。由于 IN-ADDR.ARPA 域名按照地址（反向）的八位位组划分，接受整个 /8 的组织可以获得 IN-ADDR.ARPA 区域中八位位组的授权。

⁸⁵ 关于 IN-ADDR-SERVERS.ARPA 和 IP6-SERVERS.ARPA 的使用，在 RFC 5855 (<http://tools.ietf.org/html/rfc5855>) 中做了详细介绍。

- IP6.ARPA。此子域名对 IPv6 的用途与 IN-ADDR.ARPA 对 IPv4 的用途相同。例如，给定 IPv6 地址 2001:db8:1000:9700::dead:beef，可以通过以下方法发现对应此地址的域名：先颠倒这些十六进制数字的顺序（在“::”的简写位置⁸⁶ 插入合适数量的 0），在这些数字之间加上“.”，在后面加上“IP6.ARPA”，然后通过 PTR（指针）查找最终域名“F. E. E. B. D. A. E. D. 0. 0. 0. 0. 0. 0. 0. 0. 7. 9. 0. 0. 0. 1. 8. B. D. 0. 1. 0. 0. 2. IP6. ARPA”。

如 IN-ADDR.ARPA 一样，IP6.ARPA 区域中的条目反映针对 RIR 的顶级地址块分配，这些分配由 IANA 职能运营商将其作为互联网号码注册管理职能的一部分完成。但是，与 IN-ADDR.ARPA 不同，此区域没有“旧的”分配，因为 IPv6 地址空间都已经分给 RIR 或留作 IETF 使用。

- IP6-SERVERS.ARPA。此子域包含在 IP6.ARPA 区域中用于进行查找的域名服务器。
- IPV4ONLY.ARPA。此子域供 IPv6 的一个过渡协议使用，可以检测是否使用了 DNS64 过渡技术 (RFC 6147)，以及了解在访问网络上进行协议过渡时使用的 IPv6 前缀。
- IRIS.ARPA。此子域供“互联网注册信息服务”使用，这种服务是“交叉注册互联网服务协议” (CRISP)⁸⁷ 的实施，此协议用于最终替换“域名注册公共数据库” (WHOIS) 协议，作为在互联网上查找注册信息的机制。IRIS/CRISP 协议未能获得人们的普遍接受。
- URI.ARPA。此子域用于在“动态授权发现系统” (DDDS)⁸⁸ 中注册“统一资源标识符”。此系统在 2002 年制定，未能获得人们的普遍接受。
- URN.ARPA。此子域用于在“动态授权发现系统” (DDDS) 中注册“统一资源名称”。此系统在 2002 年制定，未能获得人们的普遍接受。

.ARPA 区域中仅有的其他条目为“起始授权机构” (SOA)、域名服务器 (NS) 和此区域自身的 DNSSEC 相关记录。

⁸⁶ 请参阅 <http://tools.ietf.org/html/rfc5952>。

⁸⁷ 请参阅 <http://tools.ietf.org/html/rfc3707>。

⁸⁸ 请参阅 <http://www.ietf.org/rfc/rfc3401.txt>。

5.3 美国政府的参与

实际上，美国政府没有直接参与协议参数注册表管理职能。

由于 IETF 社区和 NTIA 相对于 IANA 职能合同和 RFC 3172 具有相对独立且潜在竞争性的机构声明，.ARPA 区域的管理在理论上有些复杂。

IETF RFC 3172 声明：

互联网架构委员会 (IAB) 具有与互联网名称与数字地址分配机构 (ICANN) 合作管理 “arpa” 域的职责。

且

根据此文档条款，应由 IANA 按照 IAB 与 ICANN 就 IANA [RFC 2860] 达成的谅解备忘录来运作管理 [arpa] 域。

但是，IANA 职能合同⁸⁹ 的第 C.2.9.1 节将 .ARPA 区域的管理作为一项 IANA 职能包括在内。

在实践中，此潜在问题还未出现。由于 IANA 职能运营商管理的 .ARPA 区域和子域非常稳定且可能平均每年接收到一次更新请求，所以其不会与美国政府就 .ARPA 区域的管理角色出现争执。⁹⁰ 此外，NTIA 不担任 .ARPA 区域的日常管理角色。

6 .INT 顶级域名的管理

.INT 区域在 1988 年引入根域并于 1994 年记录在 RFC 1591 中，最初专供

根据国际条约或国际数据库建立的 [...] 组织使用。⁹¹

最初，IETF 意在将 IN-ADDR.ARPA 域作为 IP4.INT 重定位到 .INT 区域中，并建立用途与 IP6.ARPA 相同的 IP6.INT 域；将 .INT 委托给国际电信联盟 (ITU) 秘书处。但是，在发布 RFC 3172 后，IETF 社区决定重新命名 .ARPA 区域以便用作“国际数据库”。

构成“根据国际条约建立的组织”的当前定义请参阅 <http://www.iana.org/domains/int/policy>，并且并非没有任何争议。尤其是第 3 条准则规定：

⁸⁹ 请参阅 http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf，第 6 页。

⁹⁰ 过去，人们关注 NTIA 参与管理哪些 .ARPA 子域；在了解 NTIA 只参与管理 .ARPA 区域而非其子域后，这些关注度有所下降。

⁹¹ 请参阅 RFC 1591 (<http://tools.ietf.org/html/rfc1591>)，第 2 节（第 2 页）。

所建立的组织必须被广泛认为具有独立的国际法人资格，而且必须是国际法律主体并受国际法律约束。此声明或条约必须已经建立此组织。如果所建立组织为秘书处，它必须具有法人资格。例如，它必须能够签订合同以及成为法律程序的一方。

此项法人身份要求已经成功阻止与条约相关的许多组织获得 .INT 授权。

截至 2014 年 7 月 15 日，共有 184 份 .INT 区域授权。这期间出现了几件历史趣事（例如 TPC.INT⁹² 和 YMCA.INT⁹³），根据 .INT 政策中记录的所有条件，.INT 区域中的绝大多数条目都对应国际条约组织。

6.1.1 美国政府参与 .INT 顶级域名的管理

NTIA 在 .INT 域的日常运营中并不担当任何角色。由于人们认为 .INT 管理属于一项 IANA 职能，有关美国政府参与制定管理政策的问题仍旧没有解决，例如 .INT 域的获得条件。

7 当前 IANA 职能的工作投入

本节向读者介绍目前在执行某些 IANA 职能时涉及的工作规模的一些背景信息。此数据来自 2013 年 9 月至 2014 年 4 月期间 IANA 根据与美国政府签订的 IANA 职能合同的第 C.4.4 节发布的统计数据。⁹⁴

7.1 DNS 根域管理

在 8 个月的测量期间，共处理 485 项 DNS 根域管理事务，大多数事务都与 ICANN 的新通用顶级域名项目相关。表 3 中的“更改请求”指对根域文件或 IANA 顶级域名注册（“WHOIS”）数据库的更改。标记为“ccTLD 再授权”和“gTLD 授权”的行分别介绍了国家和地区代码顶级域名（ccTLD）与通用顶级域名（gTLD）的授权和再授权。

事务	2013 年 9 月	2013 年 10 月	2013 年 11 月	2013 年 12 月	2014 年 1 月	2014 年 2 月	2014 年 3 月	2014 年 4 月
更改请求	21	22	25	24	57	24	35	18
ccTLD 再	0	1	0	0	0	0	0	3

⁹² TPC.INT 域指的是“电话公司”（对电影“中央调查局”（*The President's Analyst*）的引用，<http://www.imdb.com/title/tt0062153/>），是使用互联网绕过标准电话服务用于传真的早期实验（大约 1993 年）。有关 TPC.INT 的简要介绍，请参阅 <http://museum.media.org/invisible.net/project/tpc.int.html>，其运营原则记录于 <http://tools.ietf.org/html/rfc1703>。

⁹³ YMCA.INT 域与基督教青年会有关。

⁹⁴ 此数据的获取地址为 <http://www.iana.org/performance/metrics>。

授权								
gTLD 授权	0	4	28	41	49	41	35	58
总计	21	27	53	65	106	65	70	78

表 3. DNS 根域管理事务

表 4 介绍与请求的处理时间相关的数据，⁹⁵“平均值”、“第 90 个百分位”、“最大值”和“SLC”列分别代表一条请求的处理天数的平均值、处理完 90% 请求的天数、一条请求的最多处理天数和 ICANN 的服务水平承诺（ICANN 承诺的处理 IANA 职能合同中的具体请求所花费的天数）。

事务	平均值	第 90 个百分位	最大值	SLC
更改请求	5	14	39	21
gTLD 再授权	6	13.5	23	30

表 4. DNS 根域管理的处理时间（天）

7.2 互联网号码注册管理

在 8 个月的测量期间，共处理 3 条互联网号码注册管理请求。其中，在 2013 年 9 月处理两条请求，在 2014 年 2 月处理一条请求。完成这三条请求的平均时间为 1.92 天，第 90 个百分位为 3.56 天，最大值为 3.71 天，所有值都没有超出地址支持组织的谅解备忘录中规定的 7 天的服务水平承诺。

7.3 协议参数注册表管理

在 8 个月的测量期间，共处理 2695 条协议参数注册表管理事务。在表 5 中，这些事务分成以下几个类别：

- 1) “IANA 考量” — IANA 员工实施 RFC 的“IANA 考量”章节和某些互联网草案中规定的指示。⁹⁶
- 2) “草案审查” — IANA 员工在 IETF “最后征求意见”阶段或 IESG 请求审查时审查所有互联网草案。
- 3) “端口注册表” — 创建、修改或删除 IANA 端口注册表中的条目。

⁹⁵ 由于样本数量有限，因此数据不具备统计学意义，此表并未列出 3 条国家和地区代码顶级域名授权/再授权请求的处理时间。平均时间为从 IANA 收到请求到 Verisign 最终完成请求后的所有时间的度量值。换句话说，它将衡量请求者、IANA、NTIA 和 Verisign 的系统性能。

⁹⁶ 此类别也包含互联网草案的更新引用。

IANA 职能的概述与历史

- 4) “PEN 注册表” — 创建、修改或删除 IANA 专用企业号注册表中的条目。
- 5) “其他注册表” — 创建、修改或删除注册表或注册表内容，例如媒体类型、TRIP ITAD 号码等。

事务	2013 年 9 月	2013 年 10 月	2013 年 11 月	2013 年 12 月	2014 年 1 月	2014 年 2 月	2014 年 3 月	2014 年 4 月
IANA 考量	51	46	48	36	71	64	45	75
草案审查	67	62	55	64	53	59	37	44
端口注册表	19	12	8	16	22	22	15	17
PEN 注册表	177	197	183	174	187	173	181	176
其他注册表	38	28	17	17	29	19	42	49
总计	352	345	311	307	362	337	320	361

表 5: 协议参数注册表事务

在编写此报告时，协议参数注册表管理请求的处理时间数据不可用。

8 协议

本节概述了与 IANA 职能承包商相关的正式或非正式协议。

8.1 IANA 职能合同

NTIA 维护着一个网页⁹⁷，上面提供全部 IANA 职能合同的副本以及自 2000 年 10 月 1 日以来的修改记录。

在 1997 至 2000 年 10 月 1 日这段时间，IANA 职能作为美国国防部高级研究计划署 Tera-Node 项目的任务 4 执行。⁹⁸ 由于 NSF 允许 Network Solutions 对域名收费，增加了 IANA 职能的审查工作，因此，创建了任务 4。1997 年以前很难找到关于“IANA 职能”的详细参考资料，非正式资料表明 1997 年以前不存在关于 IANA 职能的记录文档。

在美国国防部高级研究计划署停止为 Tera-Node 项目提供资金（包括为 IANA 职能提供资金）后，建立 NTIA IANA 职能合同之前，曾出现一段短暂的时间，IANA

⁹⁷ 请参阅 <http://www.ntia.doc.gov/page/iana-functions-purchase-order>。

⁹⁸ 请参阅 <http://www.osti.gov/scitech/servlets/purl/802104>。

职能在这段时间未得到明确资金供给。在此期间，当时存在的 RIR（RIPE-NCC 和 APNIC）直接向美国南加州大学信息科学研究所（USC/ISI）提供资金，资助 IANA 职能的运营。

当前的 IANA 职能合同对于美国政府来说显然是零成本，ICANN 为执行 IANA 职能而索要的任何费用必须以成本收回为基础。

8.2 ICANN 和 IETF 之间

被称为“关于互联网号码分配机构技术工作的谅解备忘录”的 RFC 2860 为 IETF 和 ICANN 之间的谅解备忘录。此谅解备忘录于 2000 年 6 月发布，为 ICANN 管理 IETF 相关资源达成一致奠定了基础。这些资源明确包括：

- 1) 互联网协议参数（第 4.1 节）
- 2) 用于技术用途的域名（第 4.3(a) 节）；
- 3) 用于特殊用途的地址块（第 4.3(b) 节）；和
- 4) 试验性分配不被视为政策性问题的域名或地址（第 4.3(c) 节）。

谅解备忘录还要求 ICANN 制定并免费公开“关于每个当前分配的信息，包括针对被分配人的合同信息”；提供在线请求协议参数分配的设施；并审阅 IETF “最后决定”中的所有文件，以确定问题或疑虑，并向 IESG 提出这些问题或疑虑。

被称为“地址与路由参数区域（‘arpa’）的管理指南与运营要求”的 RFC 3172 描述了 IETF（具体来说为 IAB）和 ICANN 之间就应如何管理 ARPA 域问题所达成的协议。RFC 中的附录为 NTIA 致 ICANN 的一封信，请求 ICANN “按照 IAB 的指导与互联网技术社区共同管理 arpa 顶级域名。”

被称为“定义 IETF 协议参数注册局运营商的角色与职能”的 RFC 6220 提供了注册局职能的说明和要求，以记录分配的协议参数值及其相关语义用途。

除了各种 RFC 以外，IETF 社群也与 ICANN 就 IANA 职能的执行问题签订了具体协议。这些协议在 <http://iaoc.ietf.org/contracts.html> 的 IANA 章节中作为“补充协议”发布，详细说明了为执行 IANA 职能所需的服务和特定服务等级。

IETF 社群中很多人认为 IETF 只负责为各种 IANA 职能授权，因为所有这些授权都是对正确管理协议所需活动进行的授权，该协议通过 IETF 公开、达成共识的流程制定；因此，NTIA 是从权威的角度参与 IANA 职能所描述的活动，与这些协议的实施和管理无关。

8.3 ICANN 和 RIR 之间

ICANN 于 2004 年 10 月与号码资源组织 (NRO)⁹⁹ 签订了谅解备忘录。¹⁰⁰ 谅解备忘录指定号码资源组织 (NRO) 履行 ICANN 地址支持组织 (ASO) 的职责, 并就可用 IP 地址池和 ASN 池的问题以广义政策术语定义 IANA 和 RIR 之间的互动交流。

因为 IETF 在其自己的域内, RIR 曾经声称对进一步分配 IP 地址和 ASN 有政策权力, 而 IANA 在 RIR 社群内部主要负责实施以地区为基础、自下而上、形成共识的政策流程。

8.4 ICANN 和根服务器运营商之间

根服务器的运营商为独立实体, 但不包括由 Verisign 与 NTIA 根据合作协议运营的 A-根服务器, 在没有任何正式协议或服务级别承诺的情况下提供根服务。¹⁰¹

2002 年 7 月, 互联网系统联合会 (ISC) 作为 F-根服务器的运营商与 ICANN 就“根服务器运营问题”签订谅解备忘录。¹⁰² 此谅解备忘录承认 ICANN 和运营商 ISC 之间的关系, 相应地也承认 IANA 根域管理功能和 F-根服务器。随后, ISC 和 ICANN 于 2007 年 12 月签订了“共同责任协议” (MRA)¹⁰³, 该协议重申了此前谅解备忘录中说明的谅解, 投入充足的资源履行相应的职责, 并承诺在互利问题上展开合作。ICANN 董事会于 2008 年 1 月 23 日正式批准此协议。¹⁰⁴

虽然其他根服务器运营商已经签订类似的 MRA, 但 F-根协议却与众不同。然而, ICANN 和 Netnod (I-根服务器运营商) 通过信函往来^{105, 106} 各自认可彼此作为根域权威机构和根服务器运营商的角色; 并且 RIPE-NCC (K-根服务器运营商) 和 WIDE (M-根服务器运营商) 与 ICANN 交换了类似的认可工具。^{107, 108}

这些协议并非类似于通常在“管理 DNS”和类似服务的商业双方执行的合同。未来如有需要, 它们确实为更详细的协议内容提供了依据。同时值得注意的是 L-根

⁹⁹ 请参阅 <https://www.nro.net>。

¹⁰⁰ 请参阅 <http://archive.icann.org/en/aso/aso-mou-29oct04.htm>。

¹⁰¹ 请参阅 http://www.ntia.doc.gov/files/ntia/publications/amend11_052206.pdf。

¹⁰² 请参阅 <http://www.icann.org/en/groups/rssac/model-root-server-mou-21jan02-en.htm>。

¹⁰³ 请参阅 <http://archive.icann.org/en/froot/ICANN-ISC-MRA-26dec07.pdf>。

¹⁰⁴ 请参阅 <https://www.icann.org/news/announcement-2008-01-23-en>。

¹⁰⁵ 请参阅 <http://www.icann.org/en/news/correspondence/lindqvist-to-twomey-08may09-en.pdf>。

¹⁰⁶ 请参阅 <http://www.netnod.se/sites/default/files/ICANN-AUTONOMICA-Iroot.pdf>。

¹⁰⁷ 请参阅 <http://www.ripe.net/internet-coordination/news/about-ripe-ncc-and-ripe/ripe-ncc-and-icann-commit-to-ongoing-dns-root-name-service-coordination>。

¹⁰⁸ 请参阅 <https://www.icann.org/en/system/files/files/murai-to-twomey-06may09-en.pdf>。

服务器由 ICANN 运营；但是不存在运营根服务器所依据的正式协议或服务级别承诺。还需注意的是这些协议与 ICANN 相关，但不必遵守 IANA 职能合同。

ICANN 的章程规定咨询委员会——“根服务器系统咨询委员会” (RSSAC)¹⁰⁹ 向 ICANN 的董事会和委员会汇报根服务器系统的运营情况。2013 年 1 月修改了 ICANN 章程，调整了 RSSAC 的组建方式。¹¹⁰ RSSAC 自那时开始重组，加入了所有根服务器运营商机构的正式代表。它设立了正式机制，以加入更大的 ICANN 社群，例如董事会和提名委员会。它还指派了一组 DNS 及相关网络技术专家与根服务器运营商协作，从而为运营商、董事会和章程中描述的更大社群提供分析结果和建议。相比以往，这为 ICANN 社群与根服务器运营商互动提供了更具组织化的平台。

8.5 ICANN 和国家地区代码顶级域名管理员之间

ICANN 已经与不同国家和地区代码顶级域名管理员签订了大量协议，协议记录参见 <http://www.icann.org/en/about/agreements/cctlds>。这些协议与 ICANN 相关，但不必遵守 IANA 职能合同。

8.6 ICANN 和通用顶级域名管理员之间

ICANN 已经与通用顶级域名管理员签订了大量合同协议，协议记录参见 <http://www.icann.org/en/about/agreements/registries>。这些协议与 ICANN 相关，但不必遵守 IANA 职能合同。

9 总结

IANA 职能由对于持续协调唯一标识符所必需的活动组成，这些标识符对于互联网的运营很重要。从前，美国南加州大学信息科学研究所 (USC/ISI) 的 Jon Postel 博士及其团队在收到请求，并经技术研究社群同意后临时执行 IANA 职能；后来，随着与美国政府签订更多的正式合同，并与 IETF 和 RIR 等组织签订谅解备忘录，IANA 职能承担越来越多的义务。

根据 IANA 职能合同规定，IANA 职能包括：

- 1) DNS 根域管理，即对 DNS 根域和相关数据库进行修改。
- 2) 互联网号码注册管理，即从 IPv4、IPv6 和自治系统编号注册分配号码并对其进行修改。

¹⁰⁹ 请参阅 <http://rssac.icann.org>

¹¹⁰ 请参阅 <http://www.icann.org/en/about/governance/bylaws/proposed-revisions-rssac-03jan13-en.pdf>。

- 3) 协议参数注册表和 .ARPA 顶级域名管理，即创建协议参数注册表以及创建、修改并删除这些注册表的条目。
- 4) 管理 .INT 区域。

RFC 2860 记录了 IETF 和 ICANN 之间的谅解备忘录，它指定了 ICANN 的实体地位，负责确保协议参数注册表保持更新状态。RFC 3172 描述了将 .ARPA 域重新指派至“地址和路由参数区域”并指派 IAB 管理该域。

通过 NTIA，美国政府的主要职能为 DNS 根域管理，充当根域管理员。但是美国政府也提供了大量的隐式服务，包括确保 ICANN 拥有一定程度问责制的机制。

10 利益、异议和撤回的确认和披露

为确保透明度，以下章节为读者提供了关于 SSAC 流程中四个方面的信息。“确认”部分列出了为此文档的编制做出贡献的 SSAC 成员、外部专家和 ICANN 员工。利益披露部分表明了所有 SSAC 成员的个人简介，以此披露出在本报告编制过程中，可能与参与成员出现的任何真实、明显或潜在的利益冲突。“异议”部分为各成员提供了一个空间，就本文档的内容或制定本文档的流程发表不同看法。“撤回”部分确认将自己从此报告相关主题讨论中撤回的个体成员。除了“异议”和“撤回”部分中列出的成员以外，本文档获得了 SSAC 其他所有成员的一致批准。

10.1 致谢

SSAC 感谢以下成员和外部专家抽出宝贵时间和精力为撰写和审阅本报告做出重要贡献。

SSAC 成员

乔·阿贝先生 (Joe Abley)
亚普·阿克爾惠斯先生 (Jaap Akkerhuis)
唐·布卢门撒尔先生 (Don Blumenthal)
莱曼·查宾先生 (Lyman Chapin)
大卫·康拉德先生 (David Conrad)¹¹¹
史蒂夫·克罗克先生 (Steve Crocker)
帕特里克·法特斯特罗姆先生 (Patrik Fältström)
吉姆·高尔文先生 (Jim Galvin)
马克·科斯特斯先生 (Mark Kosters)
杰森·利文古德先生 (Jason Livingood)

¹¹¹ 大卫·康拉德先生曾作为 SSAC 成员参与本报告的编写工作，目前担任 ICANN 的 CTO。

IANA 职能的概述与历史

丹尼·麦克弗森先生 (Danny McPherson)
拉姆·莫汉先生 (Ram Mohan)
鲁斯·蒙蒂先生 (Russ Mundy)
苏珊娜·伍尔夫女士 (Suzanne Woolf)

ICANN 员工

朱莉·赫德伦女士 (Julie Hedlund)
帕特里克·琼斯先生 (Patrick Jones)
芭芭拉·萝丝曼女士 (Barbara Roseman)
史蒂夫·盛先生 (Steve Sheng)
乔纳森·斯普林先生 (Jonathan Spring)

10.2 利益声明

SSAC 成员的个人简介和利益声明列于以下链接中：<https://www.icann.org/resources/pages/biographies-2014-06-06-en>。

10.3 异议

无异议。

10.4 撤回

无撤回要求。