

---

ICANN81 | AGM — 运作方式：根服务器运营  
土耳其时间 2024 年 11 月 10 日星期日 — 13:15 至 14:30

乌尔里希·维瑟

(ULRICH WISSER):

大家好，欢迎参加“根服务器运营的方式”会议。我是乌尔里希·维瑟，是本次会议的参会经理。请注意，会议正在录制中，请大家遵循 ICANN 预期行为标准和 ICANN 社群反骚扰政策。会议期间，只有在问答窗格中提交的问题或意见才会被大声读出来。如果想在会议期间发言，请在 Zoom 中举手。被叫到时，将允许虚拟参会者在 Zoom 中取消麦克风的静音。现场参会者将使用真实麦克风发言。为方便记录，请报上名字，同时保持正常语速。欢迎大家使用聊天功能。请注意，在 Zoom 网络研讨会形式下，私聊只能在讨论组成员之间进行。嘉宾或标准观众向其他标准观众发送的任何消息都会被会议主持人、联席主持人和其他嘉宾看到。现在请肯·雷纳德 (Ken Renard) 发言。

肯·雷纳德:

谢谢。下午好。大家好，我是肯·雷纳德。我是来自美国军方调查实验室 (Army Research Lab) 的根服务器运营商之一。今天我们会先做发言，然后让大家问问题。我会让大家积极互动。很高兴你们来参加本次会议。我们很高兴和大家分享一些工作原理。我有一个遥控器。简单来说，今天我们会探讨一下域名系统 (DNS)，因为这有助于解释根服务器系统如何融入到各种事务中。也就是今天根服务器系统的现状。然后我们会简要介绍任播 (Anycast)，接着谈谈我们，之后再谈谈它们的治理。

---

注：以下内容为针对音频文件的誊写文本。尽管文本誊写稿基本准确，但也可因音频不清晰和语法纠正而导致文本不完整或不准确。该文本仅为原始音频文件的补充文件，不应视作权威记录。

首先我们要了解的事实是，IP 地址是互联网上的基本标识符，这些地址要么是数字，要么是由 1 和 0 组成的字符串。如果你连接到互联网，就有一个 IP 地址。那么这里的问题是，我们人类不善于记忆这些数字。而且这些数字千变万化。这是件好事。这也是开发 DNS 的初衷，为了将数字和数字变化的事实联系起来。更近一点的问题是，IP 地址可以共享，有时多个网站可以共用一个 IP 地址。与此对应的是，单一地址，比如一个网站，实际上可以托管在多个 IP 地址上。所以 DNS 是我们的朋友。它为我们化繁为简，因此得到了大量的应用。在这里我们有域名空间。我们使用 DNS 来查找域名对应的 IP 地址。因此我们有了这个层次分明的域名空间，从顶部的根开始。下面是所有 TLD，也就是顶级域。它们是国家和地区名称，也是通用顶级域 (gTLD)。在第二级之下，在第三级之下，等等。所以 DNS 最常见的用途可能就是查找域名对应的 IP 地址。但是也有其他映射，比如查找某个域的邮件服务器。这就是邮件的工作原理。在很多地址中，你可以使用 IP 地址来查找现有的域名。此外，在 DNS 中还存储了大量安全信息，帮助我们实现网络安全性。下面是对 DNS 的一个很好的描述。DNS 是一个全球分布、松散连贯、可扩展的动态数据库。不妨把它想象成一个电话本。花时间了解一下。这就是在 DNS 中查找域名的过程。这是一个经典的示意图，几乎在每本教科书中都能看到。它对描述这些基本原理很有用。之后我会在上面再加一层。

看一下这个过程，在左侧，有你的手机、网络浏览器、电脑、冰箱、烤面包机、电灯开关，任何连接到互联网的装置都会扮演这个角色，查找域名对应的 IP 地址。你的设备会通过递归解析器来查找这些域名。就是这个中间设备。递归解析器是全球 DNS 的主力军。这里是最多乐趣所在。大部分操作在递归解析器中进行。你的设备

会向本地递归解析器询问地址，这里是 `www.example.com`。递归解析器会找出这个地址是什么。我们在这里描述了这个过程。第一步是，`.com` 在哪里？右上角的方框里是根服务器系统。它会问这个问题。根服务器系统会回答，嘿，虽然我不知道 `www.example.com` 是什么，但我知道 `.com` 数据库在哪里。它会返回给递归解析器。既然递归解析器知道如何进入 `.com` 数据库，就会问同样的问题。`.com` 也会以同样的方式回复。虽然我不知道这个地址，但我可以告诉你 `example.com` 在哪里。这个信息返回到解析器，现在递归解析器就可以询问 `example.com` 数据库，并获得答案。

接下来真正重要的部分是，在这个过程中，递归解析器记住了它获得的每个答案。你的设备会再次询问 `www.example.com` 的地址。由于它已经知道答案，就不必再重复这个三步走的过程。如果你的设备询问的是 `q.example.com`，它可以跳过第一步，直接进入根服务器系统。它可以跳过询问 `.com` 服务器系统的第二步，只走最后一步。这就大大提高了这个过程的效率。信息会被缓存或记忆一段特定的时间。具体对于根而言，是 48 小时。所以每当你询问某某 `.com` 的地址时，递归解析器的效率都会最大化。另外还有一个方面会提高效率，因为使用这个递归解析器的不止你一个人。你和互联网上成百上千的邻居都在使用同一个递归解析器，因此别人以前查找过的任何内容都可能已经被记住。因此，你的设备可能会询问成千上万个 DNS 问题，但实际上它从未为这些事务进入根服务器系统，因为一切都在内存中。所以这大大提高了效率，这里的根服务器系统，即根权威服务器，非常重要，因为它是起点，但也不常用。我们来看下一页。

谈谈缓存和解析。每个 DNS 记录都有一个生存时间值。这是指递归解析器在认为记录已经过时，需要再次查询之前，允许该记录保留的时间。重点是，根服务器只提供顶级域的信息。它只知道 .com 在哪里。它不知道 example.com 在哪里。只知道顶级域。现在有 1450 个顶级域。我们的数据库非常小。

现在对 DNS 做了一些新的改进。这些基本上不是针对根服务器系统的，但对 DNS 有很大帮助。DNS 安全性，域名系统安全扩展 (DNSSEC)，我们现在可以对 DNS 数据进行加密签名。这样就消除了，或者说安全人员会说，降低了欺骗的风险。中间服务器，解析器，中间的递归解析器能够通过密码校验和验证数据是否正确。因此，你从哪里获得 DNS 信息并不重要，因为你可以验证这些信息是否正确，是否被篡改过。此外还有一些隐私增强功能。事实上，你在询问 www.example.com 时，我们看到这个问题被发送到了根，被发送到了 .com 服务器，以及递归服务器。这里面可能确实有一些敏感信息。现在，从根服务器系统的角度来看，我们看不到你的设备地址，我们只看到递归解析器的地址。因此，我们不会[听不清]特定的机器或设备，只有它们正在使用的递归解析器。还有其他协议，比如 DOT — 基于 TLS 的 DNS、基于 HTTPS 的 DNS 以及 DOQ — 基于 QUIC 的 DNS，实际上都是对消息传输进行加密。这些协议目前在左侧设备和中间服务器即递归解析器之间运行。至于它们在第二步中将如何使用，还有待观察。

好了，下面介绍一下今天的根服务器系统。这里先提供一些定义，根区。这实际上是 TLD 和它们的域名服务器的列表。这就是根区的内容。作为根服务器系统，我们将对其进行滚动。我们稍后还会看到。根服务器系统是根服务器运营商及每个运营商部署的所有基础

设施的集合，这些基础设施是用于互联网查询的计算机。根服务器运营商，你们会经常听到这个词，简称 **RSO**，实际上是维护和运营每个根服务器的组织 — 更深入一点来说。根服务器任播节点其实是一个网络位置。我们有 12 个根服务器运营商，13 个根服务器实体，以及超过 1800 个任播节点。每个运营商在其 IP 地址上操作着全球各地的多台计算机。

根服务器系统咨询委员会 (RSSAC) 是 ICANN 的咨询委员会，由根服务器运营商任命的人员和一些联络人组成。我们向董事会和 ICANN 社群提供有关根服务器运营的建议。再进一步看，区分一下根区和根服务器系统的概念。再次说明，根区是数据。根服务器系统是在互联网上运行的计算机，你可以查询它们，它们会向你发送响应并回答这些问题。这只是整个系统中很小的一部分，同样也是非常重要的。但这些区分其实是出于安全原因和职责分工的目的，这样才能明确角色和责任。

所有这有点像根区管理。如果你是 TLD 经理人，你可能需要更改你的域名服务器地址。这个请求将提交给互联网号码分配机构 (IANA)，那是更改这些信息的地方。更新实际数据库。文件进行所有签名，这就是根服务器系统的起点。我们得到已经签名、已经锁定的表格，然后对其进行管理。我们将该文件发送到我们所有的计算机上，右侧的所有 DNS 解析器都会查询我们的系统。因此，我们只是整个根区管理的一小部分。

我们的历史可以追溯到 1984 年，也就是 40 年前，DNS 诞生，当时有四台根服务器。随着互联网的发展，美国和其他一些国家/地区的网络也在发展壮大，因此需要进一步扩展。后来我们有七台根服务器。我们看到这一增长大都发生在上世纪 80 和 90 年代。我们有根

服务器，不仅根服务器运营商分布在世界各地，每个运营商的计算机也都遍布世界各地。随着时间的推移，我们响应技术需求。这是一项技术服务，我们坚持一些非常重要的原则，这个系统必须在那里运行。它必须始终运行。随着技术的发展、需求的增加、查询量的增加，我们开始响应技术需求。扩展问题。很久以前，13 台根服务器实际上意味着 13 台物理机器。现在，13 台根服务器意味着超过 1800 台机器。因此，任播让我们能够在新的维度上扩展系统，服务一个更庞大的社群。如果你对更多相关历史感兴趣，RSSAC 023 提供了一些有趣的内容。

根服务器标识符及其运营商。这些地址都是公开的。我们都在 IPv4 和 IPv6 地址上运行，这么做已经有一段时间了。现在，你们可以访问一个网站 [root-servers.org](http://root-servers.org)，那里有一张漂亮的小地图，你们可以放大查看，找到这 1800 个节点的位置。这并不一定等同于它们在地理上的位置，因为互联网与地理位置并不完全相同，但你会发现这些服务器的分布非常广泛。你不需要距离某一台服务器很近，因为这是互联网。你可以访问任何一台服务器。从伊斯坦布尔，你可以和任何一台根服务器通信，它们会共享这一信息。它可能会将你路由到一台附近的服务器，也可能会将你路由到一台千里之外的服务器，但你都会得到回应。

在 RSSAC 中制定了一套核心运营原则。由于内容太多，可能读不过来。我相信你们可以看在线幻灯片。我只想说明其中几条。这些都是我们高度重视的，我们要说明第二条原则，即：IANA 是 DNS 根数据的来源。我们通过根区从 IANA 获取数据 — 一个互联网，一个根区。如果你询问互联网上 1800 台服务器中的任何一台，它们查看的都是一模一样的数据库。

多样性是根服务器系统整体的优势。我们有硬件的多样性、软件的多样性和组织的多样性。如果某个硬件供应商出现故障，不会影响整个系统。软件也是一样。如果某个软件有缺陷，只会影响整个系统的一小部分。我们的行业也是如此。我们有政府机构、营利组织、非营利组织和教育机构。任何特定行业的崩溃都不会影响根服务器的运行。RSO 作为根服务器运营商，我们相互之间以及与利益相关方社群之间进行了大量合作和互动。这就是我们开会的原因。在发展和维护根服务器系统的过程中，我们在一些技术问题上密切合作。但我们也是匿名的、自主的和独立的，因此我们不会相互控制。我们没有任何凌驾于彼此之上的权力，而是共同完成这项工作。

关于根服务器系统的几个迷思，我们听说它对互联网流量的去向有很大控制权。这当然不是真的。路由器可以做到这一点。我们提供域名解析过程的一部分。查询由根服务器处理。我们在前面的幻灯片中看到了递归解析器和缓存。实际上，很少有 DNS 查询会联系到根服务器系统。内容由 IANA 控制。我们只是计算机操作员。我们只是根区的 IT 部门。所有的字母，从 A 到 M，都没有特殊含义。它们基本上都是随机分配的。在前面的幻灯片中，最后一个迷思是说根服务器节点接收整个 DNS 查询。如果你查询 [www.example.com](http://www.example.com)，通常完整的问题会出现在我们这里。我们会看到递归解析器询问 [www.example.com](http://www.example.com) 的地址是什么。我们知道，我们只会回答 [.com](http://.com) 在哪里的问题。实际上，有一种叫做限定名称 (QNAME) 最小化的技术，可以让递归解析器缩小查询，这样我们作为根服务器系统看到的就不是 [www.example.com](http://www.example.com) 的地址是什么这个问题。通过递归解析器，我们可以增强隐私保护。



关于使用根服务器系统的一些建议。如果你运行递归解析器，那么你可以做一些事情，比如检查到你的节点的路由。你可以进行路由跟踪或其他操作，找出每个节点的位置。通常情况下，你会希望有三四个节点在附近。我们对“附近”没有精确的定义。通常是范围或延迟。我们建议你使用 DNSSEC 验证解析器，以防其他人[听不清]你有能力验证该信息是否正确。我们建议参与 DNS 技术社群。RSSAC 的根服务器运营商成员非常有限，但我们也有一个 RSSAC 决策委员会，向 DNS 专家开放。在 RSSAC，我们的很多工作都是在这个决策委员会中完成的。所以如果你想加入，可以登录网站查找决策委员会。上面有如何申请加入的信息。实际上，一些根服务器运营商会要求在你的网络中托管他们的根服务器节点。为此，可以和这里的 RSSAC 成员或根服务器运营商交谈，然后发送电子邮件到 [ask-RSSAC@ICANN.org](mailto:ask-RSSAC@ICANN.org)。我们也会收到。快速看一下。[听不清]大量关于根服务器系统使用情况的统计数据。这只是总体查询量，基本上是平均每天的查询量。我们每天大约要处理总共 1000 亿次查询。听上去很多。其中大部分都是垃圾和配置错误，但我们肯定有大量超额配置。那里有很大的容量。好了，下面请利曼 (Liman) 谈谈任播。

拉斯-约翰·利曼

(LARS-JOHAN LIMAN):

大家好，我叫拉斯·利曼 (Lars Liman)，我在 Netnod 工作，公司运营着一套根服务器。下面我要谈谈任播。任播实际上和 DNS 没有直接关系。它是一种网络手段，我们用它来让根系统的每个运营商分摊多个服务器的负载。肯 (Ken) 提到的所有这 1800 台服务器在不同运营商之间被分成不同规模的组。在总共 1800 个节点中，Netnod



运营着其中大约 75 或 80 个节点。所有服务器都由同一个运营商运营，使用相同的 IP 地址。它有两种，一种是 IPv4，一种是 IPv6。正常情况下，网络上不可能有两台拥有相同 IP 地址的计算机。但是通过任播策略可以做到这一点，我们可以有相同的副本。

我在这里打个比方。如果你带着手机在欧洲旅行，你可以拨打...如果你碰巧遇到需要救护车的紧急情况，你可以用手机拨打 112。接着你就会收到紧急响应中心的电话，它会帮你派遣一辆救护车前往你所在的地方。如果你在荷兰的阿姆斯特丹，拨打 112 后，将接通阿姆斯特丹附近的紧急响应中心。但如果您前往意大利罗马并拨打 112，你的电话就不会转到阿姆斯特丹，而会转到罗马或罗马附近的调度中心。我们使用的就是这个策略，只不过搬到了互联网上。因此，如果你的解析器，也就是协助你在互联网上查找信息的计算机位于阿姆斯特丹，并试图访问某个 IP 地址上的根域名服务器，那么它将到达位于阿姆斯特丹或附近的根域名服务器。如果你的服务器位于罗马，使用相同的 IP 地址，它将到达罗马或罗马附近的服务器。这只是两个例子。现在，我们的服务器分布在全球 75 个地方，其他运营商的服务器也许分布在全球 50 或 200 个地方。有时，我们的服务器位于相同地点，但在大多数情况下，它们在不同的地点。所以这是一整个服务器网络，总有一个离你很近。通过使用这些特定号码联系根服务器，你总能联系到附近的服务器。

我将用几张幻灯片来说明这一点。但在此之前，我还要强调这给我们带来了几个有趣的功能。不过，我还是先介绍幻灯片吧。请放下一张幻灯片。谢谢。在互联网上，互联网数据包会尽量在两台计算机之间选择最短的路径。通常情况下，数据包需要经过多个路由器，或者我将...我稍微用错了术语，应该是网络交换机，它们会将

流量在不同链路之间转发，然后尝试将数据包越转越接近目的地。在不使用任播的正常情况下，数据包会在两个唯一的 IP 地址之间传输。也就是发送地址和接收地址，你会向接收地址发送。所有路由器都会协同工作，将你的数据包发送到终点，目的地，也即你想要到达的服务器。网络上的 DNS 查询是正常的互联网流量。DNS 数据包也没什么特别。因此它们遵循相同的原则。如果你将 DNS 查询从左侧的解析器发送到右侧的 DNS 服务器，它就会通过网络。请播放下一张幻灯片。

现在想象一下，你有三个相同的目的地。它们的工作方式实际上是一样的。它们有相同的 IP 地址。它们有相同的数据库内容。这一点非常重要。而且它们使用相同的网络，以相同的方式连接到网络。数据包从源地址出发，试图到达最近的目的地。实际的工作方式是，目的地会告诉网络：我在这里，我在这里，这是我的 IP 地址。然后，你就会去找离你最近的那个，可以说，你会听到它的声音最大。这样做的好处是，不同的发送源最终会到达不同的地方。请放下一张幻灯片。

左边的绿色发送源会到达左下方的服务器，因为那里离这个来源最近。但右上角的红色发送源会到达右上方的服务器，因为那里离来源最近。因此，根据你在网络上的位置，DNS 查询总是会转到最近的目的地，这在其他上下文中也同样适用。不一定只是 DNS。当然，非常重要的一点是，这些蓝色目的地必须同步。这样，无论你向哪个服务器查询，它们得到的答案都是一样的。根服务器运营商的工作就是确保这些服务器同步，并确保它们拥有的数据最新且正确无误。

这里蕴含着很多有趣的功能，你们可能不会立马想到。一是，如果你受到容量耗尽攻击，也称为分布式拒绝服务攻击，这时你可能拥有由小型计算机组成的极为庞大的系统，可能是你家里的网络摄像头，可能是你的笔记本电脑，也可能是你连接到互联网的电视机顶盒，然后它们可能由于受到病毒感染，向某个目的地发送攻击流量。如果你使用单播，也就是早期的模式，所有流量都会到达同一个目的地，因为目的地只有一个。这就意味着，所有攻击流量都会集中到某个目标，该目标将不堪重负，无法正常响应查询。如果使用单播模式，红色区域的机顶盒流量将到达红色目的地，抱歉，是右上方的目的地，而左下方的电视摄像机流量将到达左下方的服务器。你在所有这些节点之间分配流量。而如果你要攻击 1800 个节点，就必须拥有一个由网络摄像头、机顶盒和笔记本电脑组成的庞大网络来进行攻击，才能使它们全部超载。只有当整个系统超载时，它才会停止工作。因此，这种将服务器大规模扩展到上千台的方式为我们提供了应对此类攻击的良好弹性。

另一个你不会马上想到的功能是，如果我们将右上方的服务器完全从网络中移除，中间的路由器就会收到通知。右上方不再有服务器。于是流量就会被转发到下一个最近的节点，也就是右下方的节点。当你停止《边界网关协议》(BGP)，停止 BGP 公告，说这个节点不在了，整个路由器网络就会自动切换，说，哦，我们必须走这条路由，然后这么走。这样就能无缝地继续工作了。当然，右下方的服务器接收的流量会有一点大，但这不是问题，因为它们都有大量超额配置。每台服务器的流量都是正常情况下的数倍。所以这不是问题。这里的功能是，作为根服务器运营商，我可以让我们在英国伦敦的节点停止服务，但你不会注意到。一切都会继续正常运行，而我们也可以进行维护。我们可以安装新的操作系统，或者更换坏

掉的硬盘，或者对计算机进行维护，当一切正常后再恢复服务。哦，现在节点又回到了这里。路径变短了，流量将开始回到重新启用的服务器。因此，这为我们维护这些服务器提供了很大的弹性。如果倒回到 25 年前，当时只有 13 台机器，如果我们要拆掉我们的单台机器，就会使整个根服务器系统失去一定弹性，如果你留心观察就会发现这一点，但现在的弹性要大得多，做这类维护也就容易得多。你甚至不需要告诉对方我们在做维护，因为路由系统会自动重新组合，并继续工作。我就讲到这里，下面请维斯 (Wes) 谈谈根服务器系统咨询委员会及其决策委员会。谢谢。

维斯·哈达克

(WES HARDAKER):

非常感谢利曼。我是维斯·哈达克。我来自根服务器运营商南加州大学 (University of Southern California) 的信息科学院 (Information Sciences Institute)，除此之外，我还担任一些其他职务，稍后我会在相关幻灯片中进行介绍。接下来首先我们要介绍一下 RSSAC 以及 RSSAC 决策委员会。所以先暂停一下技术话题，稍微谈谈管理方面。

那么 RSSAC 是什么？它的目的是就互联网根服务器系统的运营、管理、安全性及完整性相关事宜向 ICANN 社群和董事会提供建议。这里的措辞非常小心，如果你仔细推敲，会发现其范围也非常狭窄。我们不提供关于 DNS 的建议。我们不提供关于 ICANN 的任何其他事务的建议。我们只提供和根服务器系统相关的建议，仅此而已。无关 IANA，也无关 ICANN 的任何其他部分。

既然如此，RSSAC 做什么，又不做什么？首先，我们致力于制定建议，就像我刚刚指出的，主要是向董事会。我们的几乎所有建议都会呈交董事会，但一般来说，我们可以向社群提供指导。比如，我们有一些文件会建议社群关注跟进研究或跟进调查。虽然根服务器运营商在 RSSAC 内有代表，但 RSSAC 自己并不参与任何运营事务。实际上，我们并不讨论利曼刚刚提到的任何事务，和任播有关的事务，或者我们的服务托管方式。这不属于 RSSAC 的范畴。RSSAC 实际上只关注根服务器系统的政策部分。

我们的领导人有 RSSAC 主席杰夫·奥斯博恩 (Jeff Osborn)，以及坐在我对面的 RSSAC 副主席、刚刚做了发言的肯·雷纳德。这个组织本身是由来自每个根服务器运营商的一位主要代表和一位候补代表组成。我想肯之前也提到了，有 13 个根服务器运营商或 12 个根服务器运营商组织，这就意味着在 RSSAC 有 24 位来自 RSO 的代表。此外我们还有其他机构派驻的联络人。我将在下一张幻灯片中详细介绍。

接下来我详细介绍一下 RSSAC 决策委员会，我想利曼或肯已经有所提及。这是一个由主题问题专家组成的志愿者机构，实际上我们的大部分工作都是在这里完成的。RSSAC 本身目前其实不会编写很多[文件]。我们转移了几乎所有这些工作，目的是让更多人来帮助我们。稍后我会谈到这一点。RSSAC 决策委员会成员由 RSSAC 根据他们的意向声明确认。也就是说他们会提交意向声明，稍后的幻灯片中也会[听不清]。

我们和其他一些组织也建立了联络人关系。我们有入驻联络人，他们帮助我们处理 RSSAC 内部事务。一位联络人来自 IANA 职能运营商 PTI。一位来自根区维护人 Verisign，它本身也是一家根服务器运营

商。因此他们在 RSSAC 内扮演了双重角色。我们还有一位联络人来自互联网工程任务组 (IETF) 中的互联网架构委员会。以及一位联络人来自安全与稳定咨询委员会 SSAC。同时我们也有外派联络人。我们在 ICANN 董事会有一个外派联络人。实际上目前就是我本人。所以我也是 ICANN 董事会成员。我们还向 ICANN 提名委员会、客户常任委员会以及根区发展审核委员会 (RZERC) 外派了联络人。最后一个 RZERC，这个委员会主要考量根服务器系统的变更如何运作。它和 RSSAC 不同，RSSAC 更多地是考虑系统如何运作。RZERC 负责的是，如果我们需要做出技术变更，如何实现这些变更。

那么什么是 RSSAC 决策委员会？我之前提到过。它有 100 多名现任成员，全都是 DNS 专家。他们对技术了如指掌。当我们需要深入思考如何改进 DNS，或如何深度研究它和根服务器系统的关系时，就会求助于这些专家。他们全都提交了公开意向声明，表明了他们的 DNS 背景、为何有意加入 RSSAC 决策委员会以及他们的专业程度如何。最重要的是，他们的每项工作都得到了公开认可。在我们所有的 RSSAC 文件中，如果你看一下最后，我们都有一个作者部分，里面基本上列出了为文件做出贡献的每个 RSSAC 决策委员会成员。你会发现，为某个文件做出贡献的人数往往相当多，因为我们得到了很多帮助，我们非常重视他们的意见。

正如我所提到的，决策委员会的目的实际上是让一群 DNS 专家为我们编制的文件带来丰富多样的经验，以确保我们能够全面深入地思考问题，而不是仅仅局限于一个狭窄的范围。如果只有少数几位作者，恐怕无法提供这种多样性。对于“谁做了这项工作”的信息，我们也保持公开透明。决策委员会的工作一般都是开放的。这确实是一个在 RSSAC 内部完成工作的框架。

接下来，我将谈谈根服务器系统治理的演变。这与 RSSAC 的关系不大，但 RSSAC 算是开了个头。当我们在 20 多年前分配第 12 个根服务器运营商时，没有任何程序可以在必要时添加或删除运营商。那么，我们该如何更改运营商呢？2018 年 6 月，RSSAC 决定对这一工作进行某种引导，以确定我们未来要怎么做。我们要如何解决这个问题？因此，我们制定了 RSSAC 37，即根服务器系统的治理方法，包括在 RSS 中添加和删除 RSO 的能力。我们还制定了一系列原则，我想有人已经提到过这些原则，涉及我们的运营方式以及我们为根服务器系统提供的精神，比如我们不过滤流量，我们会回答所有向我们提出的询问，无论这些询问是什么。

该文件发布后，ICANN 董事会根据 RSSAC 38 中的建议指引对其采取了行动，并指示组织成立根服务器系统治理工作组。这项工作目前正在进行中。本周晚些时候将举行五次公开会议，我们正在开发一个治理模型，该模型将保留我们在 RSSAC 37 中记录的 11 条指导原则，包括多样性、协作性和独立性，其中不仅包括根服务器系统利益相关方的代表，还包括其他实体的代表，这些实体将在稍后的幻灯片中介绍。最终，这将成为一份 ICANN 文件，并进入 ICANN 公共评议程序，所以一旦我们完成了治理工作组的成果文件，ICANN 社群也将有机会就这些工作成果发表意见。

根服务器系统的利益相关方，我们实际上在 RSSAC 37 中做了定义，当然，整个 ICANN 社群都是根服务器系统的既得利益者，根服务器运营商也不例外。我们维护这项服务，因此显然我们有确保它持续运行的意愿，IETF 和互联网架构委员会也是如此，互联网工程任务组实际上是维护、编写和开发 DNS 规范的地方，也是进行变更的地方。这是上周在都柏林举行的会议。IETF 的许多参与者本周都来到



了这里，他们显然对根服务器系统有着既得利益，因为他们维护着 DNS 这个整体。因此，在根服务器系统治理工作组中，有许多不同的人代表不同的组织。其中，根服务器运营商各有一名成员，注册管理机构利益相关方团体有两名成员，国家和地区名称支持组织 ccNSO 有两名成员，我刚才提到的互联网架构委员会有两名成员，此外我们还有一些联络员。右边的三个蓝圈是 ICANN 董事会的两名联络员、根区维护人的一名联络员和 IANA 的一名联络员。

演讲部分到此结束。稍后将我们接受提问，在此之前还要为大家提供一些资源。关于 RSSAC 本身的更多信息，当然，我们在 ICANN 内部有一个网页，里面有一个常见问题列表。这部分内容经设计通俗易懂，所以如果你们想了解更多有关根服务器系统的信息，从上到下读一遍就够了，它能消除很多常见的误区。我们还有一个电子邮件清单，ask-RSSAC@ICANN.org，如果你们有关于根服务器系统的问题，或者想了解有关资源的信息，或者有些人写信给我们询问如何在他们的国家或地区部署根服务器系统，通常我们会将你引向常见问题解答部分，因为这是[听不清]。有关决策委员会的更多信息，特别是如果你有兴趣加入决策委员会，我们有一个网页，还有一个邮箱 RSSAC-membership@ICANN.org。如果你们有兴趣成为成员，敬请提交一份意向声明，然后交由 RSSAC 决策委员会审查。正如我前面所说，我们通常会寻找 DNS 专家或其他领域的专业人士，从而很好地帮助决策委员会编制我们的文件。那么，还有什么问题吗？我们有时会中途提问，但本次会议没有。可以是任何问题，无论是技术方面的，还是管理方面的。

---

乌尔里希·维瑟：目前问答窗格里没有问题。提醒一下，请在 Zoom 会议室举手，或在问答窗格写下你的问题。我会读出来。如果你在现场，请走到麦克风前面。好的，请讲。大家上午好。

奥马尔·舒兰

(OMAR SHURAN): 我的问题是关于任播的一个信息性问题。它和 ICANN 管理的根服务器 IMRS 一样吗，还是不一样？

维斯·哈达克：

任播是一项通用路由技术，所有根服务器运营商都会运用这项技术。解析器还是会说，我要去 IMRS 或者我要去 USC ISI 的服务器，然后，当你尝试到达这个特定根服务器运营商的基础设施时，就会根据你的位置进行重定向。所有 12 个运营商，分别在不同的时间开始采用它。老实说，我们是最后一批采用任播技术的运营商。我的前任认为长时间推迟它的采用会更好，以确保它是一个稳定的机制，而现在我们知道它非常稳定。不仅仅是根服务器系统使用它。

乌尔里希·维瑟：好的，问答窗格中没有问题。在座的各位还有什么问题吗？

沃伦·卡穆里

(WARREN KAMURI): 根服务器运营商为什么要做这项工作？我的意思是，这听起来需要大量的财力和物力。你们为什么要花钱和花时间来做事？

---

维斯·哈达克:

这是一个很好的问题，沃伦，你恰好也在 RSSAC 决策委员会中并且知道答案。但我们很感谢你提出这个问题。事实上我们做这项工作有很长时间了，我们完全是为了互联网的利益这么做，回答完毕。它不便宜。我们得不到报酬。我的组织每年都会为投入多少预算来购买新基础设施等等展开激烈的争论。这不是个便宜的流程。你有话说，利曼？

拉斯-约翰·利曼:

我想补充一下。这要回到当初互联网还和今天截然不同的时候。今天的互联网携带着巨大的商业价值和流量。但是在 DNS 被发明出来，对根服务器的需求初露端倪时，我们开始需要根服务器提供顶级，也就是最高级的 DNS，那时规模还非常小。我承认，和维斯一样，当 Netnod 的根服务器运营商启动时 — 最初是在斯德哥尔摩的皇家理工学院 (Royal Institute of Technology)，而不是由 Netnod 启动，因为它是分拆出来的 — 它是一个工作站，一台这么大的计算机，放在一间办公室的桌子上。回到那时，它是那么无足轻重。如今我们的系统已今非昔比。它绝对是以专业的方式受到维护。我们有几十名员工参与这项工作，历经 30 多年它的规模已不可同日而语，我们是逐步发展到今天的。但是最初，它只是源于 IANA 提出的一个简单问题，你能为我们做这件事吗？当然。于是我们实现了，而这一直是为互联网社群提供的一项非常重要的服务，我们想要提供这项服务。

从中得到的一个好处，回到肯的介绍部分，就是我们拥有了一些非常多元化的组织。正如你提到的，肯，我们有政府机构，有营利机构，有非营利机构，还有学术机构。至于如何运营，我们都有不同的财务基础。Netnod 以我们的方式筹资来提供这项服务，南加州大

---

学用另一种方式，[听不清]机构有第三种方式，而商业实体有第四种方式。即使财务体系发生重大变化，同一个变化也不会立刻波及到所有的根服务器运营商。这也是一种多样性，这种多样性对持久性，对长期维护这项服务至关重要。谢谢。

维斯·哈达克：

还有其他问题吗？

肯·雷纳德：

我觉得有必要在已经提供的答案基础上再提供另一个答案，因为维斯在大学工作，而我是非营利公司的总裁。现如今，在互联网上，当你说你免费提供某种东西时，肯定会遭人唾弃，他们会说 Facebook 也不向我收费。我想明明白白地回答一下。我的组织编写互联网运营所需的软件，并进行分发。我们的付费者是那些回过头来找我们的人，他们说：“我需要帮助，我能不能向你购买一些支持服务，来支持我从你那里免费获得的软件？”我们的 BIND 软件在全球有一百五十万用户。其中约 100 位用户为获得帮助而向我们付费。此外，在从支持 BIND 和其他开源软件赚到的钱中，我们会拿出 20% 来运营根服务器系统。所以当我们说我们不为它收费时，并不表示我们从兜售你们的所有隐私信息中赚钱。我们不经手隐私信息。我们不经手信息。我们不经手内容。我们所做的只是发送权威服务器的地址，这个权威服务器知道 TLD 在哪里。所以当我们说我们是非营利性，不赚钱时，绝对是你们听过的最真实的表述。我们是名副其实的非营利性，名副其实的不赚钱。我们只做事，如果你不以为然，可能不想听这些话。我们只做事，因为我运营一家由来自 19 个不同国家/地区的 19 个人组成的公司，我们都真心相信单一

---

域名源的互联网本身就弥足珍贵，就算是赚更少的钱为一家非营利性组织工作也无妨。我们确实致力于完成我们的使命。

汉斯·彼得·赫伦

(HANS PETTER HOLEN):

如果没有其他问题，我还可以提供另一个解答，因为既然我们有 12 个运营商，就会有各自不一样的答案，不是吗？我，或者说我的组织，运营 K 根。不要让我再谈服务。我们是一家会员制组织。我们有大约 20,000 名会员，他们为 K 根的运营和其他服务付费。如果你想知道具体的花费，可以查看我们的年报或者活动计划和预算，来了解具体的数字。如果你把这个费用除以会员数，那你可以说他们每年为此支付大约 50 欧元。有很多不同的筹资方法，这是这个系统的优势之一，我们的方法各不相同。每个人都同时遭遇财务危机的情况非常罕见。

乌尔里希·维瑟:

好，我们在问答窗格中有一个问题。RSSAC 与其他团体以及 ICANN 的关系如何，特别是非商业团体？

维斯·哈达克:

RSSAC 和其他选区召开会议，这些选区与我们有着某种直接关系，或者与我们有直接的对话需求，因为我想肯之前也说过，我们为 IANA 提供根服务，对吧？我们保证过，我们得到的数据源来自 IANA。大多数代表 TLD 的 ICANN 选区，比如 ccNSO 或通用名称支持组织 (GNSO)，他们直接与 ICANN 沟通来获得这些 TLD 功能的动态。我们和 IANA 沟通。实际上，运营是我们的主要焦点。我们定期和安全与稳定咨询委员会 (SSAC) 开会。我们定期和 ICANN 董事会开会。

本周我们和地址支持组织 (ASO) 召开了会议。我们在必要时召开会议。我想最近我们还和一般会员咨询委员会 (ALAC) 开了几次会。今早我们和政府咨询委员会 (GAC) 开了会。那也是出于需要。我们一般不喜欢开会，除非有实际需求。所以这一次，我们实际上不会和 ICANN 董事会开会。过去三四次我们都和他们召开了会议。两个组织之间没有直接紧急的需求。我们不想浪费大家的时间，让大家坐下来召开一场内容空洞的会议。

拉斯-约翰·利曼：

但是我要强调一点，我们始终欢迎互动。如果你们认为有些问题涉及根或运营商，那么请过来跟我们交流。如果需要召开会议，我们也会积极布置安排。但是我们不会召开定期会议，除非有问题需要讨论。就像维斯说的，在这个语境下有足够多的会议。我们不需要再为了开会而开会。但是，我们非常欢迎其他团体和个人与我们互动。如果你们有关于根服务器系统的问题，请随时来问我。你们一定能找到我。我有两米高。要找到我很容易。

肯·雷纳德：

根服务器运营商 — 根服务器组织一共有 12 个。现场就有 7 个，所以我们可以举手。我们都在这里。

乌尔里希·维瑟：

好，问答窗格中还有一个问题。能否再介绍一下任播运营商及其和 RSSAC 的关系，如果有的话？

拉斯-约翰·利曼：

任播运营商。就是我们。我们运营任播网络注意，我们不必在互联网上对路由器做任何特殊操作。所以，以 Netnod 为例，我们运营位于不同地点的 75 个服务器，那是我们的服务器。我们操作它们。我们把它们运到分配的地点。请人帮我们把它们安装到机架上，再用必要的电缆将它们连接到网络、电源等等。但是之后，我们会登录系统并进行操作，这台服务器将公告这一关系（我们需要谈判进入这个关系），它将向网络上游的下一个路由器进行公告。它将公告，现在 Netnod 的根服务器在这里，是这个 IP 地址。请把流量带给我。所以并不需要有一个特定的任播运营商。在这 1800 台服务器中，不同的根服务器运营商运营属于他们自己的部分。其中每个服务器装置，都可以是不止一台物理机柜。对这个根服务器运营商来说，它可以是几台服务器和一个本地路由器。这个集群或组合将向最近的路由器公告，我在这里。向我发送流量。以上就是需要做的全部工作。谢谢。

乌尔里希·维瑟：

日常除了正常运行之外，根运营商是否还必须满足一些法律或技术要求？

[汉斯·彼得·赫伦：]

我们往往会说，互联网不受监管，或不受任何政府管辖。对于 ICANN 的政策流程或 RIR 或其他人来说，确实是如此。但是每一个运营商都在某个国家/地区拥有某种法律实体，因此受到该国/地区的法律约束。欧洲网络协调中心 (RIPE NCC) 位于欧洲，我们必须遵守欧洲法律。这里我的同事们来自美国。他们必须遵守美国法律。这些法律没有具体规定我们该如何运营。但是随着新法律的出台，



---

对关键基础设施的运营提出了新的要求。这在不同国家/地区以不同的节奏进行。所以现在是激动人心的时候。

拉斯-约翰·利曼：

我想补充一下，因为这个问题也问到了技术规范。回答是肯定的，有几个技术规范。比如，我们必须遵守 IETF 即互联网工程任务组在特定技术标准中规定的 DNS 协议。还有一份文件描述了对根服务器响应 DNS 查询的期望，由互联网架构委员会与根服务器运营商合作发布。但是 RSSAC，正如我们所说，编制了一份服务水平期望文件，这份文件已经发布或很快就要发布。即使还没有发布，也很快了。里面对运营商提出了对根的一系列期望，包括响应的技术限制、响应时间、从新数据的发布到该数据在端节点上更新的间隔，等等。所以没错，有一些技术期望。

维斯·哈达克：

我想你说的是 RSSAC 047。我再补充一点，我们不能只监控我们的设备是否正常运行。我想，不管是根服务器、DNS 服务器、文件服务器还是网络服务器，任何网络的管理都会给你留下深刻印象。我们必须创建大量图表，并寻找大量警报，这才是真正能迅速唤醒我的问题，而不仅仅是服务器是否正常运行、运行速度是否太慢、流量是否过大等问题。磁盘空间是否不足？基础设施运行中有大量的细节，当某个地方出错时，你必须立即知晓。当有新情况出现，而我们之前没有考虑过监控时，我做的第一件事就是写一个新的东西来监控，所以我有一位同事十分擅长创建非常有趣的图表，我整天都在看这些图表。

拉斯-约翰·利曼:

还有大量的经验。我说过，我们大概有 10 个人在操作这个系统，而每个根服务器运营商都有很多操作员。不光是在座的几个人，我们都是处理这些事务的人，虽然我很少触及根服务器的技术细节，但是，根服务器运营商在运行 DNS 服务器方面的经验或许可以以世纪为单位计算。如果你把运行 DNS、查看 DNS 内容、DNS 流量、数据包内容、更新程序、监控、网络流量工程等方面的大量经验放在一起，那么所有这些都是运营根服务器的一部分。我们在各自的组织中都拥有这方面的专业知识，所以这不仅仅是在座的几个人的事情。

[尤素福 (YUSUF): ]

我叫尤素福，我来自伊斯坦布尔的[马尔马拉大学 (Marmara University)]。我的问题是，你们如何了解在某个地区是否有足够的节点，比如在伊斯坦布尔，有七个节点。你们怎么知道它们够不够，谁负责检查确认？

汉斯·彼得·赫伦:

虽然我只能代表根服务器运营商之一的 K 根，但 RIPE NCC 还运营着全球测量网络，拥有超过 13,000 个测量探针。我们利用该测量网络和其他来源查看网络中探针所在位置的延迟情况，以确保我们在各个部分都能提供良好的服务。现在，所有根服务器运营商都可以使用这种方法，有些运营商还使用其他测量方法，看看他们认为自己提供的服务是否良好。如果你对此特别感兴趣，RIPE NCC 还接受托管节点的开放申请，所以你可以与我们联系，比如在你的本地互联网服务提供商 (ISP) 申请一个托管节点。如果你认为应该有更多分布，可以联系我们讨论。其他根服务器运营商也可能有其他方法，

这就是多样性的魅力所在。我们没有一种共同的方法，而有 12 种不同的方法，所以即使我的方法不对，别人也可能有更好的方法。

维斯·哈达克：

值得一提的是，在任播出现之前，互联网运行得很好，有 13 台服务器。实际上你不必位于某一台的附近，正如我们前面介绍的，缓存可以让 ISP 的 DNS 服务器变得更快。这并不是因为你附近有一台根服务器，只有极少数问题会真正到达根服务器，所以到达根服务器并不重要。

[塔希尔 (TAHIR): ]

大家好，我是伊斯坦布尔理工大学的塔希尔。我想问一个问题，在任播中，我们有分布在各地的等价服务器。但它们拥有的数据或信息呢？你们是否存在同步问题，或者需要多久同步一次？你们有相关的在线离线程序吗？

肯·雷纳德：

是的，所有这些服务器都必须保持松散同步。根区正常一天可能会更新一到三次。我们会测量并公布更新速度等等，请参考 RSSAC 002。通常根区发布后，就会在所有基础设施上发布。全部发送出去可能需要几秒钟。但如果节点位于连接性不佳的偏远位置，就需要一段时间才能到达。因此，我们很少遇到同步问题。这种情况确实存在。但有一些 DNS 协议参数规定，如果该区的版本过于陈旧，就停止提供服务。因此我们希望避免出现数据太旧的情况，尤其是 DNS 签名不再有效的情况，因为它们也有有效期。

维斯·哈达克：

值得一提的是，在你再次询问之前，根区中的每条记录都允许你记忆两天。所以请记住，实际上所有记录的有效期都是两天。

拉斯-约翰·利曼：

同样，任播也在这里发挥了作用。因为如果我们通过监控系统，对所有系统进行监控，我们检查的一个参数是，系统是否正常更新。如果我们发现它没有正常更新，而我们又无法快速修复，我们就会关闭它。关闭该节点后，流量就不会再流向该节点。流量会流向另一个已更新的节点，我们可以趁机解决问题。当问题得到解决后，我们再把它打开。这再一次证明，任播对你我都有利。

[朱奈德·米亚吉  
(JUNAID MIYAJI): ]

大家好，我叫朱奈德·米亚吉，来自孟加拉国，这是我第一次亲临现场参加 ICANN 会议。我想提一个问题。几天前，我们国家遇到了互联网关闭的问题。但在那个时候，我发现尽管我们与整个互联网断开了连接，但我们的 IX 网络却运行正常。只是那时我们无法解析任何 DNS，因为没有在互联网上连接 DNS，就无法解析任何域名。那么，你们有没有什么选项之类的东西可以让根区与 IX 网络，即本地互联网协同工作，或者有没有其他办法，让像我这样的个人可以缓存根区的记录，特别是我们国家的记录？谢谢。

拉斯-约翰·利曼：

好的。要解析一个普通 DNS 域名，不仅需要根服务器，还需要下面的各级服务器。这样一来，选择的数量很快就会爆炸，所以你需要缓存大量数据。话虽如此，根区毕竟是公开信息，所以你可以下载。稍后我可以告诉你如何下载。IETF 有一份文件，介绍了如何在

本地解析器中操作该区。你可以在你的解析器中运行该根区的副本，这样它就不必与根域名服务器通信。然后你就可以只靠自己。你可以定期复制该区，并从一些开放节点进行所谓的区传输。运营商有一些节点，可以让你自动复制该区。如果你的网络关闭，无法复制新版本，它将继续使用旧版本，我相信最长可达一周左右。所以，这个问题是有办法解决的。不过，我相信，在这次断网期间，孟加拉国的根服务器可能仍在工作，但下一跳可能是 `com` 服务器或...抱歉，我不记得孟加拉国的顶级域了。但同样，下面的步骤也可能行不通，因为下几级的服务器可能在孟加拉国境外，对此我们无能为力。

维斯·哈达克：

在孟加拉国实际上有六台根服务器，它们很可能还在继续工作。

[朱奈德·米亚吉：]

很抱歉，但遗憾的是，我尝试了各种方法，就像你提到的那样，自己做 DNS 服务器，缓存根记录，使其成为解析器。遗憾的是，这些都不起作用，所以我才问了这个问题。另外，在关闭期间，我们...我尝试了无数种方法让它以任播方式工作，但根本行不通。另外，你提到的解析记录的方法对我来说也行不通。我想我可能犯了一些技术之类的错误。那么，有没有什么办法可以让我联系到一些技术人员或技术方面的帮助...

维斯·哈达克：

你提到了好几件事。它有两部分，对吧？假设你要查找一个网站的名称，比如 `example`，这个网站正在运行，我会选择南极洲，不在某个国家，对吧？如果某个地区不在互联网上，可能是由于飓风之

类的自然灾害造成，不管是不是政治原因，都没有办法到达那里，对吧？网络服务器在南极洲，就算你能查到也没用，对吧？另一方面，如果 DNS 服务器，比方说你要查找 `example.com`，如果 `example.com` 的 DNS 服务器在南极洲，而你由于某种原因被切断了连接，比如电缆被切断，那也没关系。你的 ISP 可以从根开始，你会获得它，因为它就在那里，但根服务器无法修复你对外部环境的访问。根服务器不能为你解决这个问题。

[朱奈德·米亚吉：]

谢谢你，但我想我忽略了一点。我承认这一点。我说的是 IX 网络，我们在本地网络中有一些服务器，比如我的服务器在孟加拉国达卡。所以它应该能够解析托管在达卡的网站，而不是孟加拉国境外的网站，但它希望解析托管在孟加拉国境内的域名。这些网站与 IX 网络合作，我们可以直接通过 IP 进行解析，但无法使用根区解析域名。这才是我要问的。

卡尔·如斯 (KARL REUSS)：

我们与一家 PCH 即数据包清算所合作，提供大量任播节点。我们与它们合作，在他们的基础设施上运行我们的服务器，他们帮助许多国家/地区设置交换点，并为其顶级域托管自己的内部 DNS。这类工作需要许多东西进行设置并使其正常工作，而且除非所有东西都损坏，否则很难对它们进行测试。你需要进行大量故障排除，以确保它设置正确。我们可以与你合作。我知道我们在孟加拉国有服务。我们可以查看你所看到的一些情况，看看是否有任何设置不当

---

的地方。有几个部分，根服务器只是其中之一。根服务器可能运行正常，但还有很多东西可能出错。

[汉斯·彼得·赫伦：]

我可以补充一下，我认为这是一个非常有趣的问题，实际上只有极少数国家/地区进行过大规模测试。如果失去了与世界其他地方的连接，如何保持国内基础设施的运行？一些国家/地区已经进行了测试，有人质疑他们这样做的原因。有人说他们是为了切断本国与外界的联系。有人说是为了自卫。这种测试本身就被认为具有争议性。我认为，作为工程社群的一员，我们应该聚集在一起研究这个问题，看看在危机期间，如何尽可能地让一个网络子集正常运行。因为现在世界上有的国家/地区正在发生武装冲突，有的正在遭受自然灾害等等。无论我们能做什么来理解它，并确保互联网保持弹性，我认为这都是值得一试的。但就像我说的，根服务器只是其中一个很小的部分。我认为这更适合那些同时从事 DNS 中其他活动的同事。

卡尔·如斯：

看来我们通过 PCH 在孟加拉国提供了很多服务。似乎那里很多该有的东西都有了，我想只是没有完全设置好。

维斯·哈达克：

很遗憾，你的问题不在于根服务器。它更可能在于 .bd 或者一些其他基础设施。但还需要分析。还有其他问题吗？



---

乌尔里希·维瑟：                   我想我们已经超时了。谢谢各位的到来。

[会议记录结束]