蒙特利尔 — 运作方式：根服务器运营
东部夏令时间 2019 年 11 月 3 日星期日 — 15:15 至 16:45
ICANN66 | 加拿大蒙特利尔

史蒂夫 • 康特

(STEVE CONTE)： 再过几分钟我们就要开始了。今天的房间很大，如果你们想要坐近一点，那将会很好，这样我们好看清楚大家。这场会议的安排是，先由 RSSAC 给大家做个幻灯片演示，然后进入问答环节，我们会邀请大家提问。我已经迈出了我的一步，你们坐得越近对我越好，当然这只是我的建议。会议马上开始。

安德鲁 • 麦康纳基

(ANDREW MCCONACHIE)： 大家好，我叫安德鲁 • 麦康纳基，是 ICANN 内负责为根服务器系统咨询委员会提供支持的工作人员，今天将由我为大家介绍根服务器系统，我想我在这里能够看到。我喜欢走来走去，所以我不会坐下来，对于坐在比较远的同仁，我得说声抱歉，因为摄像机必须得跟着我。我保证，幻灯片演示比我的照片有趣多了。那么，接下来我们继续吧。

我会与我的同事欧赞 • 萨辛 (Ozan Sahin) 一起来完成演示，他负责第二部分的内容。首先我会概要介绍一下 DNS，这对在座的很多人来说可能是一种回顾，因为我知道，你们已经完成了 DNS101 基础知识的学习，不过我们还是会讲一下。然后，我会解释一下什么是任播，它与单播的区别，以及为什么它对根服务器系统很重要。再然后，我会介绍根服务器系统的现状、节点和它的一点历史情况。

在那之后，欧赞 (Ozan) 会为大家介绍 RSSAC、RSSAC 决策委员会和目前正在开展的根服务器系统发展相关工作。我们开始吧。

DNS 概述。我猜，在座的大多数人应该都已经对互联网上的标识符及它的不同类型有所了解。这张幻灯片讲的是 IP 地址和它们对互联网的重要性。所有连接到互联网的主机都需要一个 IP 地址，目前我们有两种不同类型的地址，分别是 IPv4 和 IPv6。它们是数字标签，不是名称。它们是互联网使用的基本标识符。

为什么要引入 DNS？仅仅使用 IP 地址会带来什么问题？唔，IP 地址很难记，它们还经常变来变去。除此之外，在引入 DNS 之后，还出现了一些现代问题，那就是，IP 地址可以共享。客户端可以有多个 IP 地址，服务器可以有多个 IP 地址，主机也可以有多个 IP 地址，在这种情况下，你要使用哪一个呢？这个时候，域名系统就可以发挥作用了。

大家在有关 DNS101 基础知识的幻灯片演示中可能已经了解到，DNS 系统是一个层次结构，位于顶部的是根区，在根区之下是我们所说的顶级域，这里列出了一些例子，比如 .UK、.ORG、.EDU，在顶级域之下是二级域，然后是三级域，等等等等。通常，我们可以认为域名与 IP 地址之间存在一个映射，如果大家熟悉术语的话，可能知道我们将其称为 A 映射或 AAAA 映射。除此之外我们还有其他映射，域名到邮件服务器的名称之间也存在映射，还有反向 DNS 查询。

这里是一些定义，大家会看到整整两页幻灯片的定义，在深入这个主题之前，我们最好回顾一下这些定义，确保大家熟悉这些术语。这些都是 RSSAC 经常使用的一些术语，不仅仅在我们的文档中，在

这次幻灯片演示中也是如此。第一个术语我在前面已经用到了，是“根服务器系统”，它是一组共同实现根服务器功能的根服务器。稍后我们再来深入探讨这个术语。

然后是“根区”，它实际上就是数据，就像上一张幻灯片我在讲 DNS 层次结构时，现在我们讲的实际上就是根服务器系统帮助分发的数据。根区就是根服务器系统帮助分发的数据。它没有父级，并且包含联系它下面的顶级域所需的全部信息。这张幻灯片上的最后一个术语是“根服务器任播节点”，目前所有根服务器运营商使用的都是任播，当我们在说单个服务器或物理机器时，实际上我们说的就是任播节点。

这里是一些组织角色。我们有根区管理人，它是负责管理根区里面的数据的组织。其实这本质上就是 IANA 职能，涉及的工作包括向运营商分配顶级域名和维护他们的技术管理详细信息，这是什么意思呢？就是当你在解析顶级域名的时候，你需要有一个顶级域名服务器能够响应查询，而运营这个顶级域名的人偶尔可能会想要更新服务器，这个时候他们就必须向根区管理人发送请求。

我们还有根区维护人，目前担任这一角色的组织是 Verisign，它负责从根区管理人处接收数据，将这些数据格式化成一个根区文件，然后最重要的是，对根区文件进行加密签名，并在那之后，将其分发给根服务器运营商。根服务器运营商，目前我们有 12 个根服务器运营商，它们负责管理根区和根区 Hints 文件中指定的 IP 地址上的根服务。它们就是各个运营物理根服务器的组织。

之前我已经讲过一点这方面的内容，现在我们来看看数据与人们如何获取数据之间的区别。一个是提供数据的服务器，另一个是数据本身。根区指的就是数据，它是根区文件，而根服务器系统由根服务器运营商组成，后者运营着负责提供这些数据的服务器。这张幻灯片列出了两者的对比情况。先来看根区，它其实就是一个起点。它列出了所有 TLD 和它们的域名服务器，有了这个数据之后，你才能开始解析。你会前往 TLD 的域名服务器，来解析这些 TLD 下面的域名。根区由 ICANN 根据社群政策加以管理。

如上一张幻灯片所说，它由根区维护人编译并分发给各个根服务器运营商，它就是根服务器提供的信息。根服务器系统是一个由服务器组成的系统，负责使用来自根区的数据响应用户的查询。目前，根服务器系统由 26 个 IP 地址组成，其中 IPv4 地址 13 个，IPv6 地址 13 个，它有 1000 多个物理节点。这个数字一直在不停地变化，随着时间慢慢地上升。现在，我们只能说它有 1000 多。以前我们有一张幻灯片上面明确写出了具体的数字，在那之后这个数字一直在不断更新，所以我们说，“好吧，现在有 1000 多点。”根服务器系统是一个纯粹的技术角色额，它服务于根区，是根服务器运营商的职责所在。

这张幻灯片描绘了 DNS 查询响应流程的所有详细步骤。我会花点时间简单讲一下这张幻灯片，看看当一台电脑想要解析域名时，它会通过递归域名服务器做些什么。

我们从右边开始，大家可以看到，我们有一位互联网用户，也就是我们所说的客户端，他们正在使用电脑，想要访问 www.example.com。现在，假设这个递归服务器刚刚打开，它的缓存里面没有任何东

西，也就是说，除了知道如何前往根域名服务器之外，其他的它一无所知。那么，用户的电脑首先会做什么呢？它会联系这个递归域名服务器，就是位于图片中间的这个，它会向递归域名服务器发送一条查询请求，说：“你好，www.example.com 的 IP 地址是什么？”

而那个递归域名服务器由于刚打开，缓存里面没有任何东西，它会首先联系根服务器系统，联系根域名服务器。它很有可能会将整条查询请求发送给根域名服务器，问：“你好，www.example.com 的 IP 地址是什么？”根域名服务器会说：“我不知道 www.example.com 的地址，不过我知道如何联系 .COM，顺便说一下，这是这条数据的签名。”

它会向递归域名服务器返回这条数据。然后递归域名服务器说：“好的，很好。现在我知道如何联系 .COM 了，而且我有这个签名，我会使用加密技术，把它与位于递归域名服务器中的根区密钥签名密钥的公钥部分进行对比。好了，对比结果表明，根域名服务器提供的 .COM 地址是正确的，现在，我要联系 .COM。”

然后，递归域名服务器去到 .COM 域名服务器那里，问：“www.example.com 在哪里？”.COM 域名服务器回答说：“我不知道它在哪里，不过我知道 example.com 在哪里，顺便说一下，这是这条数据的签名。”递归域名服务器基本上会重复刚才的做法，说：“好的，很好。现在我有 example.com 的地址了，而且我可以用加密签名来验证它是否正确。”之后，它会去到 example.com 域名服务器那里，后者会提供 www.example.com 的地址以及一个签名。在把这些数据返回递归域名服务器之后，递归域名服务器会

说：“很好，现在我有 www.example.com 的 IP 地址了，而且还有一个签名，我先来完成加密对比。很好，地址是对的。”

只有到现在，递归域名服务器才会回到用户那里，或者回到用户的电脑，说：“这是你要的 IP 地址。”这张图描绘的是，在用户发起一条简单的查询之后，递归域名服务器会经历的递归、迭代，这是个复杂而漫长的过程，只有在整个过程完成之后，它才会向用户返回响应。

这是对我刚才所讲内容的更详细的探讨。根服务器只知道接下来要询问哪个服务器。在上面的例子中，它们只知道如何联系 .COM 服务器，而不知道如何解析整个域名。不过，递归服务器会记住这些响应，它们会把这些响应存在自己的缓存里。

实际上，它们不需要每次都向根服务器发送查询请求，这些缓存信息的存活时间（通常缩写为“TTL”）是两天。也就是说，递归服务器在询问根服务器，比如 .COM 域名服务器，并从后者那里获得响应后，它们会在两天内记住这一信息，之后如果收到相同的查询请求，它们便无需再向根服务器询问，直到这一信息超时为止。

这是对 DNS 的一些现代改进。前面我们谈到了对 DNS 数据的加密签名。这些都是在 DNSSEC（DNS 安全扩展）中定义的。DNSSEC 只是一个简短的术语，用来描述为了通过加密方式确保递归服务器和客户端从根服务器获得正确的信息而需要进行的所有签名和验证服务。此外，由于查询可能会泄露信息，DNS 最近还进行了一些隐私增强。最初或传统的 DNS 只使用基于 53 UDP 或 TCP 的明文传输，为了解决加密 DNS 传输的问题，目前正在开展一些标准化工作。另外我们还有基于 TLS 的 DNS，以及基于 HTTPS 的 DNS。

任播是另一种现代改进技术。目前，所有根服务器运营商采用的都是任播技术，后面我们会有一个部分专门介绍任播技术，到时候我们可以再详细讨论。这样一来，我们就来到了任播简介部分。其实一开始，我们使用的只有单播，单播是指，来自所有源的数据包都传输至同一个目的地，它只有一个目的地，所有源发送的数据包都会到达那个目的地。

基本上就是，一个 IP 地址对应一个服务器，一个 IP 地址对应一个端点。这没问题啊，但是，如果你想要扩展，那情况就不一样了。任播支持扩展，它使扩展变得容易得多，如果你想要增加服务，如果你想要获得更多有效查询，这一点非常重要。此外，它对抵御分布式拒绝服务 (DDoS) 攻击也非常有帮助，如果有人对你的服务发起 DDoS 攻击，而你想要把一些攻击流量转移到许多不同的服务器上，使用任播技术会让事情变得很容易。

在任播中，IP 地址与端点之间的映射发生了变化，它是一个 IP 地址对应多个服务器，对应多个端点。来自不同源的数据包将传输至不同的目的地，但它们仍在与同一个 IP 地址通信，或者说它们仍在向同一个 IP 地址发送流量，只是到达的物理目的地不同而已。由于源距离目的地更近，中间跃点更少，源获得数据的速度将更快。DDoS 攻击流量将被发送至所谓的“沉洞”(Sink Hole) 或最近的节点，而不会影响到其他节点。

这是一个非常简单的单播流量传输的例子，它有一个到单一目的地的最短路径。现在我们已经有了一个源和一个目的地。如果你往其中再加入一个源，它的流量同样会传输至那个目的地。我们再来看看任播，它有多个目的地，这些紫色或蓝色水滴状的东西就是我们

标记的目的地。我们仍然只有一个源，但是大家可以想象以下，如果我们往其中加入一个源，而它距离某个目的地更近，那么来自它的流量将传输至那个目的地。这样一来，它就可以很容易地将流量分散开来。

这是任播真正的好处之一，它最大的好处之一就是对分布式拒绝服务 (DDoS) 攻击的缓解，使得那些使用远离 DDoS 攻击的目的地的源不会受到攻击的影响。如果是本地攻击，无论是地理意义上的本地还是拓扑意义上的本地，攻击流量都会沉入一台服务器，不会影响运营和世界其他地方。这是任播的一大优点。

接下来，我要稍微谈谈根服务器系统的历史，然后再说说它的现状。在 1983 年到 86 年，根服务器系统只有 4 个地址，从那时起，它便稳步增长，一直到 1998 年，地址的数量达到了 13 个。也许说“地址”有点不太合适，不过大家可以看到，一直以来，根服务器系统都在不断发展，如今，因为 IPv6 的引入，我们可以说，根服务器系统一共有 26 个地址。其中，IPv4 13 个，IPv6 13 个。实际上，由于使用任播技术，我们可以说有 26 个 IP 地址，IPv4 13 个，IPv6 13 个，但物理节点有 1000 多个。

这里列出了这些根服务器的主机名、IPv4 和 IPv6 地址，以及它们的管理人，也就是当前根服务器系统的根服务器运营商。所有运营商，所有主机名都有与它们关联的 IPv4 和 IPv6 地址。大家可以看到，它们以 A 到 M 来表示。

这张地图是我们从 root-servers.org 下载的，它并不是要准确呈现各个节点的地理位置。大家可以自己访问 root-servers.org 查看这张地图，它就在首页上，然后你们可以放大查看具体的城市，你们可以

从洲开始放大，然后是国家和地区，然后是城市，看看是哪些运营商在这些城市运营服务器或节点。这里只是一个最概括性的呈现，你们可以一直放大，地图软件只是把一些东西进行了分组。

从这里基本上可以看出，世界各个地方都有节点存在，每个洲都有，也许我不应该这么说，因为我不知道南极洲是不是也有节点，大家如果有正确的答案可以来纠正我，不过，至少在除南极洲以外的其他每个洲上，都有节点。大家如果对这个感兴趣，想要深入了解，可以访问 root-servers.org 查看地图，看看你附近的哪个城市有根服务器节点，以及是谁在运营它们，等等等等。

这张图描绘的是根区信息的变更流程，以及这些变更如何配置到实际的根服务器中，之后解析器又要如何接收它们。左边是 TLD 运营商。我们假设某个 TLD 运营商需要请求变更，那么它们会联系 IANA，它们会对 IANA 说：“我们的 TLD，我们的域名服务器现在使用的是这个 IP 地址，我们想要把它变更到另一个 IP 地址。”

它们会告诉 IANA，然后 IANA 会执行一系列的验证程序，确保自己是在和相应的 TLD 运营商对话，同时确保此次变更是良好的变更，不会破坏任何东西。在 IANA 批准变更之后，变更会进行传递，IANA 会告诉根区维护人：“这是新的根区文件。”根区维护人要做的就是更新这一信息，得到下一份根区文件。然后，根区维护人会编译根区并对其进行加密签名，再将其分发给运营商。

在图的右边，所有这些带有“RS”的小气泡都代表着单个节点，我们有很多节点，对于每一个运营商，我们都有很多节点。然后在最右边，我们可以看到，递归解析器正在发送查询和接收响应。以上就是对根区信息变更流程的一个高度概括。

这是有关根服务器运营商的一点更多信息，正如我所说，我们一共有 12 个根服务器运营商，它们主要关注互联网服务的可靠性、稳定性以及所有互联网用户的可访问性。它们通过 RSSAC、根服务器运营社群和其他平台相互配合。它们相当专业，并且是不同类型的组织，它们并不都是非营利性组织，也不都是政府机构，它们在技术、组织、所处地理位置和融资模式方面具有多样化。

这是它们协调的一些方式。我之前提到过一些不同的行业会议和机构，比如 ICANN 和 RSSAC、ITF、RIR 会议、网络运营商团体、DNSORC 等等，除此之外，就像其他任何需要协调的组织一样，它们也会使用其他不同类型的工具。它们会彼此共享数据，定期开展活动，比如桌面演习和应急准备等等。

根服务器运营商的职责包括推动互联网服务的运营和发展；评估和部署建议的技术修改，可能是针对某个协议的修改，比如 DNS 协议，它们通过参与互联网工程任务组来执行这项工作；以及确保始终维持互联网服务的稳定性、可靠性和可达性。但是，运营商不参与政策制定，当然也不参与数据修改。根服务器运营商只负责发布数据，对数据具体是什么不负有责任。

说到这里，这张幻灯片展示了 RSSAC 和我多年来遇到过的一些误解，以及相应的实际情况。第一个误解是认为根服务器控制着互联网流量的去向，实际情况是，数据包路由器控制着互联网流量的去向。根服务器只负责响应递归服务器发送给它们的查询请求。

另一个误解是认为大多数 DNS 查询都是由根服务器处理的，实际情况是，大多数 DNS 查询都不会经由根服务器处理，这主要是因为缓存的存在，因为递归服务器会记住它们从根服务器处获得的答案，

这样一来，在收到相同的问题时，它们就不需要每次都去询问根服务器。再一个误解是，认为根区的管理和服务的提供是一回事。这又回到了数据本身与数据提供之间的区别的问题。数据管理与响应有关数据的查询之间大不相同。

另一个误解是认为某些根服务器地址有特殊的含义。其实，它们都没有任何特殊的含义，确实没有。然后还有一个误解是认为只有 13 个根服务器。不是这样的，因为采用了任播技术，我们有 1000 多个节点，但技术地址只有 13 个。根服务器运营商并不是完全独立地运营，它们会彼此配合，这一点我们在上一张幻灯片上曾经说过。最后一个误解是，认为根服务器运营商只接收查询中的 TLD 部分。

我在讲 DNS 解析的工作原理时，在我所举的例子中，根服务器收到了整个查询字符串，其实这就是传统的工作方式，现在可能有 90% 的情况都是采用这种方式。这就是为什么我们要将“通常”两个字加粗的原因，目前有一种叫做“限定名称最小化”(QNAME Minimization) 的新技术，它是一种新的隐私技术，我想我们应该可以这么界定，它是由 IETF 开发的，旨在改变这一现状，但目前还没有被广泛应用。虽然部署这一新技术的人越来越多，但目前的现实情况是，根服务器运营商通常会接收整条查询。

如果你是一家网络运营商，那么关于 DNS 以及你与根服务器之间的交互，你需要考虑这几点。你可能希望附近有三到四个节点。这里的“附近”既可以是拓扑意义上的，也可以是网络意义上的，不一定非得指地理位置。这样一来，你或许可以建立更多的对等连接，减少延迟。你可以做很多不同的事情。

另一件事是在解析器中部署 DNSSEC 验证，这可以确保对于在根区中经过签名的数据，你收到的是正确的数据，是没有经过篡改的 IANA 数据，没有人在递归服务器与根服务器及其他权威服务器之间的传输过程中篡改数据。通过部署签名数据 DNSSEC 验证，你可以在本地解析器中验证该数据，这会很有帮助。

如果有兴趣，你还可以参与到 RSSAC 决策委员会中来，贡献你的力量，稍后我的同事欧赞会详细地介绍 RSSAC 和 RSSAC 决策委员会分别是什么。

如果你是一家网络运营商，并且对托管任播节点感兴趣，可以在本次幻灯片演示结束后与我们的 RSSAC 成员交流，当然，你可以在问答环节提出来，或者，你也可以发送邮件到 ASK-RSSAC@ICANN.ORG。

接下里我会把时间交给我的同事欧赞 • 萨辛，由他给大家介绍一些组织方面的东西。

欧赞 • 萨辛： 谢谢安德鲁 (Andrew)。大家好，我叫欧赞，是 ICANN 组织的一员，负责为根服务器系统咨询委员会 (RSSAC) 的工作提供支持。

我们首先来看看 RSSAC 的职责，它的职责范围非常狭窄。根服务器系统咨询委员会的职责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 ICANN 董事会提供建议。

这张幻灯片上有两点关于 RSSAC 应该做的和不应该做的备注。它是主要向 ICANN 董事会提供建议的委员会，但也会向参与整个 DNS 事务的其他 ICANN 机构和其他组织提供建议。虽然根服务器运营商在 RSSAC 内有代表，但 RSSAC 自己并不参与运营事务。

如果你们看 RSSAC 的组织结构会发现，它由根服务器运营商任命的代表组成。除此之外也有这些代表的候补人员以及联络人。另外我们还有一个叫做 RSSAC 决策委员会的机构，它是一个由志愿者主题问题专家、DNS 主题问题专家组成的群体。RSSAC 决策委员会的成员由 RSSAC 基于利益声明确认。如果你想要成为 RSSAC 决策委员会的成员，基本上，你就需要像我的同事安德鲁刚才说的那样，提交你的利益声明，然后 RSSAC 会确认你是否符合资格。

目前我们有两位联合主席，分别是布拉德 • 沃德 (Brad Verd) 和弗雷德 • 贝克 (Fred Baker)，他们都来到了现场。我还想说明一点的是，RSSAC 正在向一位主席/一位副主席的模式过渡。到今年年底，他们将进行副主席的选举。RSSAC 将 — 领导层将会由一位主席和一位副主席组成。

我刚才说过，RSSAC 还有联络人，我们有四位入驻的联络人和四位驻外的联络人，这四位入驻的联络人分别是一位来自 IANA 职能运营商、一位来自根区维护人、一位来自互联网架构委员会，或简称 IAB，还有一位来自安全与稳定咨询委员会，它是 ICANN 系统内的另一个咨询委员会。四位驻外的联络人分别是，一位到 ICANN 董事会、一位到 ICANN 提名委员会、一位到客户常任委员会，以及一位到根区发展审核委员会，或简称 RZERC。

RSSAC 决策委员会拥有 100 多名成员，他们都是 DNS 技术专家。就像我刚才说的，任何感兴趣的人都可以通过提交利益声明，申请成为 RSSAC 决策委员会的成员，为 RSSAC 出版物的编制贡献自己的力量并获得公众的认可。RSSAC 决策委员会确实提高了 RSSAC 的透明度，所以你可以通过成为决策委员会的一部分来参与 RSSAC 的工作。正如我所说，这些都是把他们的专业知识带到出版物中的 DNS 专家。

目前 RSSAC 下设了多个工作小组。其中一个负责研究现代解析器的行为，它会通过基础代码和可用数据集来研究目前已经部署的软件和递归解析器的行为。另一个工作小组主要聚焦根服务器系统的期望及相关指标。它负责制定适用于整个系统范围的、可进行外部验证的指标，用于评估 RSS 作为一个整体，是否正常运行以及及时向终端用户提供正确的响应。

我们有一些工具和机制来帮助提高 RSSAC 和根服务器运营商的透明度。举几个例子，我们有 RSSAC.ICANN.ORG 网页，大家可以访问该网站，查看 RSSAC 成员和 RSSAC 决策委员会成员的名字，还可以阅览出版物。你们也可以找到 RSSAC 电话会议的会议记录。另外，RSSAC 会召开公开会议，如果大家感兴趣，可以参加这些会议。

在 ICANN 公共会议期间，RSSAC 也会与 ICANN 内的其他机构召开会议，就拿这届会议来说，RSSAC 的联合主席会向政府咨询委员会作简要报告，ICANN 董事会将与 RSSAC 召开会议，另外 RSSAC 跟安全与稳定咨询委员会还会召开一次闭门会议。它会与其他机构沟通交流。RSSAC 有一份出版物 000，其中规定了它的运营程序，也增加了它的透明度。

根服务器运营商也有一些工具和机制，它们有 root-servers.org 网页。我记得，刚才我的同事安德鲁向大家展示的描绘世界各地节点的地图就可以在这个网页上找到。除此之外，各个根服务器运营商也有它们自己的网页，它们会就重大活动发布联合报告。同样地，就像安德鲁刚才说的，大家如果有任何问题，可以发送邮件到 ASK-RSSAC@ICANN.ORG，我们会答复大家。

在幻灯片演示的第二个部分，我会谈谈目前正在进行的有关根服务器系统发展的工作。我们先来看看这项工作的时间安排。一年多以前，RSSAC 发布了 RSSAC037 和 RSSAC038。这两份文件基本上提出了一个新的根服务器系统治理模型。然后，ICANN 董事会指示 ICANN 组织对这些文件进行研究。2019 年 4 月，ICANN 组织最终发布了所谓的“概念文件”。2019 年 8 月，针对概念文件的公共评议期结束。各个不同群体纷纷提交了意见。按照设想，在审核完所有意见后，后面的工作将在 2020 年 1 月份之前完成，届时会成立一个治理工作组，该工作组将在 2020 年和 2021 年负责模型的开发。到 2022 年，新模型有望实施。

我们来看看 RSSAC037 讲了什么。它规定了根服务器系统运营和发展必须遵守的 11 个原则。基本上，它为根服务器系统及其运营商提出了一个初步治理模型。它还通过一系列关于根服务器运营商指定和移除的场景演示了 RSSAC037 模型的运作方式。

在这张幻灯片上，大家可以看到作为 RSSAC037 补充的三条建议。第一条建议是，发起一项流程，确定 RSSAC037 模型的最终版本。然后第二条是，预估根服务器系统和模型开发的成本。在这一点上，初步的精力应该放在时间表的制定上。最后一条建议是，根据

有关问责制、透明度、可持续服务和完整性的原则实施模型的最终版本。

这张幻灯片上是一张描绘拟议模型的图表。大家可以看到，它有三个不同的部分，一个是治理，另一个是 DNS 根区运营，还有一个是根服务器运营商的加入和停用。在治理部分，大家可以看到，它有三个利益相关方，分别是 ICANN 社群、IEFT/互联网架构委员会和根服务器运营商。幻灯片上也列出了拟议模型提出的五项职能。

它们分别是绩效监督和衡量职能；指定和移除职能；财务职能；战略、架构和政策职能；以及秘书处职能。这五项职能全部在模型中提出。然后在幻灯片的底部，大家可以看到这有一些绩效指标，它们将用于根服务器运营商的加入和停用职能。这涉及到根服务器运营商的指定和移除。

我们刚刚谈到了职能，现在我们回过头来看看概念文件，它基于 RSSAC037 模型设想了与五项职能对应的以下结构。一个是根服务器系统治理委员会，另一个是根服务器系统常务委员会，还有根服务器运营商审核小组，最后两项职能是 ICANN 组织的财务职能和秘书处职能。

概念文件概述了一项社群驱动流程，旨在基于 RSSAC38 第一条建议确定新根服务器系统合作与治理模型的最终版本，这是另一份与根服务器系统相关的出版物。流程的第一阶段是，ICANN 组织在 ICANN 董事会的指示下审核和评估 RSSAC037，目前这一阶段已经完成。

第二阶段，就 RSSAC037、概念文件和治理工作组文件发起公众意见征询，刚才我们已经说过了。第三阶段涉及到开发新的根服务器系统合作与治理模型，它有两个工作方向，一个是组织结构方向，另一个是行政管理方向。结构方向治理工作组负责模型的开发，管理方向则负责在 ICANN 组织的领导下规划治理工作组模型的实施。

那么，什么是治理工作组？它的成员组成是怎么样的？它由来自 RSSAC、ccTLD 域名支持组织、注册管理机构利益相关方团体和安全与稳定咨询委员会的代表组成。除此之外，它也有来自 ICANN 董事会、IANA 和根区维护人的联络人。

治理工作组的职责是确定模型的细节。概念文件还规定了治理工作组需要遵守的一些准则，包括制定带清晰里程碑的时间表；开放、透明地工作；必要时征求意见和建议；遵循 RSSAC037 中列出的原则；以及参考 RSSAC037、概念文件和收到的公众意见反馈。

现在，我们进入本次会议的问答环节。今天来到现场的有很多担任 RSSAC 成员的根服务器运营商代表。有请他们上台就座，回答观众的提问。我们为大家准备了一些流动的麦克风，大家如果有问题要问，请举手，这样我们就会给你麦克风。

史蒂夫 • 康特： 在他们准备的时候，我确实有一个问题，不过我们先等所有根服务器运营商代表坐好。我们的第一个问题已经放到幻灯片上了。

发言人（姓名不详）： 我只是想知道，作为一个非技术人员，我想知道你们如何确定何时何地需要增加部署根服务器节点？它与域名服务器有什么区别？什么是递归域名服务器，它与你们常说的域名服务器有什么区别？

弗雷德 • 贝克： 唔，我们会通过扔飞镖，看看它落在哪里，来决定部署新的根服务器。不是啦。实际上我们有一个既定的流程，从需求开始。为什么我们需要一个新的根服务器？为什么我们需要一个新的根服务器运营商？然后，如果确实存在有效的需求，我们会根据一系列原则来评估某个公司或组织是否具备相应的能力。我建议你去看一下 RSSAC037 来寻找答案，因为它 — 它涵盖的内容真的很多。

韦斯 • 哈达克 (WES HARDAKER)： 其实，弗雷德 (Fred)，我觉得他问的是根服务器节点，而不是根服务器运营商。

弗雷德 • 贝克： 哦，好吧。关于根服务器节点，你可以直接来找我们，找某个根服务器运营商，例如，我的公司 ISC，如果你去访问 ISC.ORG 的网页，你会看到它上面写着：“如果想要部署新的根服务器或根服务器节点，请点击此处。”

我想我们大家应该都是这样。然后，我们会跟你联系，讨论你的要求。我们有一些期望，我们希望这个系统能同时支持 IPv4 和 IPv6。你需要有足够的带宽。你需要有电力供应，等等等等。最后，我们

会与你签署谅解备忘录。然后开始运营，我们会运营服务器，它会部署在你的机架上，但由我们来远程运营它。基本上，如果你想要部署新的，你就需要来找我们，然后我们开始沟通。

韦斯 • 哈达克： 我能稍微补充一下吗？我想你听到的应该是，我们会从多个地方了解要求。我们会了解外部的要求，比如人们发来新的互联网交换点等等，这是我们放在最后的 — 新的互联网交换点，来找我们，说：“我们是全新的，什么东西也没有，你们愿意帮忙吗？”我们愿意这样做，因为曾经我们是第一个进来的，不过我们也会了解内部的要求，比如我们如何分析，如何服务世界。

目前我们正在增加部署，试图触达那些在地理上分散的地区，尽可能实现良好的覆盖。总之，这是一个内部指标和外部指标相结合的过程，我们非常重视那些认为自己所在地区没有获得充分服务的任何人的意见。

布拉德 • 沃德： 你在这里听到的是不同的方法，因为每个根服务器运营商都是以自己的方式进行选择。它们可以从需求出发，从实际的流量需求出发，也可以从地缘政治的需求出发。除此之外，还有很多不同的需求可以证明新节点部署的合理性。

至于你问题中的第二部分，递归解析器与权威服务器之间的区别，我们运营的是权威服务器，我们是根区的权威服务器。递归解析器是你在 ISP 内与之对话的部分，它是你与所有权威服务器之间的中间媒介。

例如，.COM 是一个权威服务器，根服务器就是权威服务器，.US 等等也是如此。在大多数情况下，你可能不会直接与我们对话，而是与你的递归解析器对话，然后你的递归解析器会根据需要与我们对话，具体视缓存中有无对应答案而定。希望这样回答能让你满意。

欧赞 • 萨辛： 我们又收到了一个问题。

发言人（姓名不详）： 谢谢。我不知道这是不是问在座各位的，还是说我可能来错房间了。它问的是基于 HTTPS 的 DNS，我的理解是，Firefox 和 Chrome 将在很短的时间内，比如在几周或几个月后，往那个方向过渡，这意味着 95% 的 DNS 流量都可以被加密，我不知道。我看到有人在摇头。

我的重点是，我不知道，如果它会改变，或者只是保持不变但隐藏起来，这会带来什么影响，会如何影响会议开始时你们在幻灯片演示中谈到的 DNS 运作方式？我在整个 ICANN 会议日程中都没有发现有任何专家组讨论这个问题，但它似乎很重要。如果你们没有答案，能不能告诉我，我可以去哪里找到答案？

韦斯 • 哈达克： 我也是互联网架构委员会的成员，该委员会参与了 IEFT 的标准化工作流程。我说一点关于 Firefox 和 Chrome 部署的事实。他们采取的做法非常不同，所以不要弄错了。另一件他们做的事情是，仅仅介于浏览器和解析器之间。

以 Firefox 为例，他们会选择在一个解析器，在 Cloudeflare 中运行的默认解析器，他们会在你的配置中提供一个下拉菜单，这样一来你就可以选择自己希望使用的解析器，默认情况下当月他们会在美国启用它，对于世界其他地方，他们还在寻找其他合作伙伴来做这件事。该解析器不会对系统其他部分进行 DNS 加密，包括根服务器，包括 .COM 等 TLD 服务器、ccTLD 服务器、example.com 等等。

另一方面，Chrome 采取的做法稍微有些不同。他们会去了解你的本地 ISP 解析器是否支持基于 HTTPS 的 DNS，如果支持，这是否在他们的批准列表中，他们会通过 DoH 与 ISP 通信。他们不会像 Firefox 那样，把所有东西都发到同一个位置。这是一种非常不同的部署方式，遗憾的是，人们对此有很多混淆，这是因为信息变化太快了，即使是 Firefox 仅在美国使用 Cloudeflare 也是最近才决定的事情，而下周会发生什么还有待讨论。

两周后，互联网工程任务组 (IETF) 将会在新加坡对这个问题展开更深入的讨论。到时会有一场技术对话。再过几个月，情况就会不同了，现在变化非常快。

布拉德 • 沃德： 我想补充一下。再次重申，目前这只介于发生加密的客户端与解析器之间，它不是解析器与权威服务器之间的问题。要我说的话，这个问题已经在 ICANN 内讨论过了，马拉喀什会议期间有一场围绕这个问题的高关注度主题会议，所以我会回到马拉喀什的议程上来。

我不记得具体是哪一天了，但当时 SSAC 作了一次非常大的幻灯片演示，哦，好像是 CCNSO，那次演示讨论的就是这个问题，而且后面他们也一直在讨论。我知道 SSAC 正在着手这件事，但还有其他工作也正在进行当中。人们对它的关注度很高。

弗雷德 • 贝克： 韦斯 (Wes)，请允许我问一个关于 DNSSEC 的问题：既然一般来说浏览器自己不部署 DNSSEC，而是依赖于其他人来部署，那么，当浏览器使用基于 HTTPS 的 DNS 时，DNS 会经过验证吗？

韦斯 • 哈达克： 这是一个非常好的引导性问题，弗雷德。问得很好。一般来说，大多数人认为安全有两个方面。一个是加密，换句话说，你的数据是否受到保护？然后还有一个问题是你的数据是否真实，是否是实际意义上的正确数据？加密数据也可能是错误的数据。比如说，你可能拿到了错误的加密文件。

在 DNSSEC 中，数据的保护从源头开始，从数据创建的地方开始，在我们的例子中，也就是 IANA，通过根区维护人对该数据进行签名，根区数据的其余部分，实际上，大多数 TLD 和它们下面的内容都会得到签名，这没关系，你可以把它写在一张纸上交给我，我可以读取和扫描它，我可以验证签名，确定它是否是最初从 IANA 创建的数据，并由此一直往下验证。

弗雷德的引导性问题是，DoH 也涉及到数据的完整性，但它仅介于两个端点之间，所以如果上面的实体，如果那个解析器与你展开不安全的对话，它自己是不会知道的，它会直接将未经验证的数据交

给你。一些基于 HTTPS 的 DNS 解析器会执行 DNSSEC 验证。如果你知道，你在受可靠完整性保护的通道上与基于 HTTPS 的 DNS 解析器对话，并且你知道它们会执行验证，那么你的数据可能从头到尾都是安全的。据我所知，Cloudflare 是一个会默认执行验证的解析器，其他的我就不知道了。

布拉德 • 沃德： 不过如果你们感兴趣的话，这个问题还是值得深入研究的。

史蒂夫 • 康特： 这就是你的简单跟进吗？好的。

发言人（姓名不详）： 既然在 HTTPS 环境里，ISP 无法看到数据，那也就是说，他们就再也看不到错误了吗？他们看不到所有这些在他们网络里传输的东西，但是你们还是可以看到？那还有谁能够看到 — 在 DNS 或者 HTTPS 环境里，谁能够看到 DNS 请求？谁不能看到？

韦斯 • 哈达克： 这个问题眼下很难回答，因为就像我刚才所说，到下个月，情况很可能就大不相同了。对于使用 Firefox 的人来说确实是这样的，在他们与其他地方基于 HTTPS 的 DNS 服务提供商通信时，那个基于 HTTPS 的 DNS 服务提供商（比如 Cloudeflare）将能够看到。之后，它会被传输至整个 — 在某个时候，你不得不问问题，你不得不走到某个人面前说：“我需要问一个问题。”

这个你要问的人，比如你要问那个网站在哪里，他们总是能够看到你的问题。总是有人能够知道你问题的内容。另一方面，对于 Chrome，由于他们使用基于 HTTPS 的 DNS 与 ISP 通信，与 ISP 内你的解析器通信，所以这不会改变 ISP 的可见性。

这在很大程度上取决于部署情况，而 Chrome 和 Firefox 在这方面的情况大不相同。另外就是你的邮件阅读器，目前没有任何邮件阅读器计划使用基于 HTTPS 的 DNS。如果你在网络浏览器中处理邮件，那么就有人会看到。这个问题不是简单的“是”或“不是”的问题。我这么说明白了吗？

弗雷德 • 贝克： 现在似乎是谈论限定名称最小化的好时机了。这是 IETF 正在处理的一个项目，将在将来某个时候应用到你身边的一些软件上。它的目的是尽可能减少信息泄露，同时使问题获得解答。举个例子，如果我要查询 www.example.com，我可能会问我的递归服务器，而递归服务器会说：“我不知道 .COM 在哪里，我还没有找到它。”

然后，与现在将整个域名字符串发送给根服务器的做法不同，它只会将 .COM 发送给根服务器，这样一来根服务器就会知道它是在问 .COM，并向它返回该顶级域名的地址，然后，递归服务器再去问 example.com 的地址。这样的话，就只有该递归解析器才能看到这一信息。你们可能希望看到限定名称最小化。

发言人（姓名不详）： 另一个方面是整合。过去，如果你有成千上万的人使用同一个递归解析器，是的，没错，该递归解析器就会知道是你发送的请求，但现在，如果你从同一递归解析器处收到了成千上万条请求，它不一定能够将这些请求与具体的个人对应起来，与使用该递归解析器的许多人之中的某个人对应起来。

史蒂夫 • 康特： 谢谢。下一个问题已经发到了幻灯片上。

发言人（姓名不详）： 我想知道，DSO 现在是否还会保留日志，如果是，他们需要遵守什么隐私方面的规定吗？只是出于兴趣，我想问一下，DSO 如何获得域名服务运营资金？

布拉德 • 沃德： 你是说 RSO 吗？我们听到你一直在说 DSO，我只是想确认一下，其实你想说的是 RSO，对吗？

发言人（姓名不详）： 是的，抱歉。

布拉德 • 沃德： 好的，那我们倒回去看一下。我没有听清你问题中的第一部分，但最后关于他们如何获得资金的部分，这个很容易回答。目前，他们没有资金支持，参与的都是志愿者。随着互联网自然扩展，志愿者开始运营这些根服务器，并且他们的数量随着时间的推移不断增多，这基本上是 82 年到 98 年之间的事情，在 1998 年之后，就没有新的根服务器出现了。我记得在 2001 年，任播技术引入并开始为根服务器所使用，自此，我们从只有 13 个标识符，13 个服务器，一直到现在，我们已经拥有 1000 多个服务器，但它们的地址还是那 13 个。得益于任播技术，我们才能够实现更远、更宽泛的覆盖，而所有这一切都是每个组织自己出资完成的。好了，你还记得问题的其他部分吗？或者你能重复一遍吗？

发言人（姓名不详）： 我想知道，你们是否会保留请求日志，关于这一点是否有任何隐私规定？

布拉德 • 沃德： 我能为你提供的唯一参考是每年所谓的“Diddle 收集”，它是一种被称为“Diddle”的日志，收集了 48 小时的数据，便于研究人员了解互联网在特定的某天做了哪些事情。所有根服务器运营商都可以做出贡献，以及很多其他 TLD、ccTLD 和大型组织、大型 DNS 运营商都是如此，这是一项社群工作，该数据会被存储在 DNS 数据库中，如果要访问数据库，你必须先成为成员，签署一些保密文件什么的。

韦斯 • 哈达克： 还有一点，那就是很多运营商在将数据交给 OARC 之前都会对数据进行匿名化，这意味着他们会匿名化 IPS，通常，发出请求的 IP 地址是最初的解析器，所以不会关联到特定的终端用户电脑，而是会关联到提供数据的解析器。我觉得尤其是最近，尤其是自从开始实施 GDPR 以来，大多数运营商都会执行匿名化，不过你必须和他们每一个进行对话，我不记得目前谁在执行匿名化，执行到什么程度了。

欧赞 • 萨辛： 我们还有一个问题。

发言人（姓名不详）： 首先，我得向你们道歉，因为我觉得这个问题很难回答。在前面的幻灯片中，我注意到，大多数拥有根服务器 IP 地址的组织都是美国组织，我想知道，在美国政府这个并不会真正致力于中立的环境中，什么可以确保，或者有什么机制可以用于确保互联网根服务器保持中立？

弗雷德 • 贝克： 对于这个问题，答案可能不止一个，不过我要说的是，RSSAC 目前正在着手的一件事是如何评估这个系统。其中一个评估指标，其中一个我们关心的事情是，接受评估的根服务器运营商 — 虽然我们会对所有根服务器运营商进行评估，但每一次只会针对其中一个 — 我们关心的是，它们是否在为来自 IANA 的系统提供服务。

如果你从特定服务器收到的根区数据存在不同，这就违反了我们认为相当重要的一些东西。这将是一个非常不好的事情。我们会下载信息，比如每隔几分钟，就从 IANA 下载信息，我们会在一段时间内提供服务，我们会下载更多信息。我们会始终如一地传输从 IANA 获得的信息。

然后我们会来看，IANA 向我们传输了什么？TLD、ccTLD、gTLD 则会转身告诉 IANA，我有这些名称，它们拥有与之相关的记录，IANA 是中立方，它会做到中立的。我认为，在中立的问题上，我们只能依赖于 IANA 的道德规范，依赖于 ccTLD 的道德规范，依赖于根服务器运营商的道德规范，希望它们以企业的身份来做这件事。这样能否回答你的问题？

韦斯 • 哈达克： 弗雷德，在你继续之前，我再补充一点。我强烈建议你去读一下 RSSAC023，也就是编号 023 的文件，它基本上就是根服务器系统到目前为止的发展史。事实上，在今天早些时候的 RSSAC 会议上，我们曾讨论过这个问题，那场会议是对所有人开放的。

它解释了我们是如何评估那些当前负责提供服务的组织的，其实这完全是由历史决定，20 年来都没有改变，RSSAC037 的目标之一是建立一个架构，规定自 20 年前最后一个人做出变更以来，未来我们要如何变更这个流程，这个问题目前正在讨论之中。

更重要的是，前面我在讲 DNSSEC 时也说过，如果你要做 DNSSEC 验证，让数据从上到下都经过验证，这样你就会知道它没有经过修改，其实它经哪个国家和地区传输真的不重要，它是完全独立于政治的，因为从技术上讲，要伪造这些数据 [听不清] 不可能。这是我能够告诉你的最安全的做法，就是一定要使用 DNSSEC 验证解析器。

布拉德 • 沃德： 我再稍微补充一点，RSSAC037 目前已经发布了，所有人都可以去看一下，它里面列出了根服务器运营商定义的指导原则。其中一项指导原则就是保持中立，这是一个非政治的观点，不涉及政治，我们必须服务于 IANA 向我们提供的根区。至于有关美国的言论，那纯粹是自然发展的结果。互联网在美国兴起，在美国发展，他们需要根服务器运营商，所以才有了现在这个局面，所以说，除了自然发展以外再无其他原因。

弗雷德 • 贝克： 而且，在美国以外，我们也有根服务器运营商，我们在瑞典有一个，在荷兰有一个，在日本也有一个。

史蒂夫 • 康特： 我们来看看下一位的问题，坐在那边被挡住光的地方，在你的右边。

发言人（姓名不详）： 我知道，拒绝服务和分布式拒绝服务攻击就像许多安全问题一样，是一种猫捉老鼠的游戏，攻击者越强大，安全机制就会变得越强大，反之亦然，并且一贯如此。那么，你们到底做了什么来持续保护根服务器免遭攻击？RSSAC 会不会与 SSAC 开会讨论如何保护根服务器，或者你们是怎么做的？

布拉德 • 沃德： 首先我能够告诉你的是，最近根服务器运营商发布了一份文件，你可以直接从那里面找到答案。它介绍了当今根服务器系统面临着哪些威胁，以及它们要做什么和已经做了什么来缓解这些主要的威胁。

至于 RSSAC，RSSAC 会与董事会还有 SSAC 展开对话，讨论根服务器系统面临的任何威胁，这就是为什么我认为 — 前面有人提到过基于 HTTPS 的 DNS 和基于 TLS 的 DNS 问题，我们已经讨论过了，以及在发生类似的事情时，会给基础设施带来什么影响。这些对话每时每刻都在发生。不过，它们不涉及到运营，有关运营的问题都在根服务器运营商内部或之间讨论，在发生 DDOS 或其他事情时，它们才会共享信息，共同缓解问题。

韦斯 • 哈达克： 布拉德，可以在哪里找到那份文件？

布拉德 • 沃德： 抱歉。那不是 RSSAC 的文件，它位于根服务器的网页上，可以访问 www.root-servers.org 找到，我记得它就在网页的最上面。

发言人（姓名不详）： 很好，非常感谢。我能问最后一个问题吗？我知道，DNSSEC 配置错误的服务器也有可能会引起扩大化攻击，并且我知道，目前大家都在推进 DNSSEC 的部署，我很好奇，有没有什么方法可以推进增强的 DNSSEC 配置服务器？比如说，增加速率限制和采用其他方法？我知道早在 2013 年，ICANN 曾围绕加强 DNS 安全展开了大量的讨论。

韦斯 • 哈达克： 你能澄清一下你的问题吗？关于 DNSSEC 配置错误的服务器可能会引发问题这里，因为它实在是太宽泛了，或许你能再稍微具体一些。

发言人（姓名不详）： 举个例子，如果有人部署了 DNSSEC 配置错误的服务器，其他人对他发起基于 UDP 的攻击，冒充 IP 地址，这种情况下，你能做的基本上就只有收集一系列 DNSSEC 配置错误的服务器，而这，将会使得攻击扩大，带来比正常 DNS 放大攻击更严重的影响。

韦斯 • 哈达克： 你是在担心反射攻击。DNSSEC 将大量的数据添加到签名中，因此签名变得非常大，密钥变得非常大，你说的一点都没错，特别是在过去，DNSSEC 常常被用作反射攻击，你可以假装从你想要攻击的地址发送一个非常小的数据包，然后就会有大量的流量传输到那个地址。

但是现在，大多数服务器，这里我不仅仅是指根服务器，我是说大多数服务器都采用了称为“响应速率限制”的技术，这有什么作用呢？简单来说，它会限制服务器问太多问题，如果遇到服务器发送的问题太多，它会直接切断它们，说：“我不再回答你的问题了。你仍然可以与我通信，但是你必须使用 TCP。”这就使得 IP 地址欺骗很难实现。

每个权威服务器的设置是非常非常不同的。我可以告诉你，在大多数人使用它之前，你会看到每天的流量高峰，因为每个人都在使用它，但是在几年之后，你会发现，大多数人的流量图会变得相当平坦，因为人们意识到这不再是可行的方法。你不会再经常看到 DNSSEC 反射攻击了。但现在，我相信它们在某个地方仍然存在。

史蒂夫 • 康特： 好的，非常感谢。在座的各位还有其他问题吗？我看了一下线上，线上已经没有问题了。最后一次提问的机会。

韦斯 • 哈达克： 大家都提出了很好的技术问题，谢谢大家。

史蒂夫 • 康特： 我想要感谢安德鲁和欧赞为我们带来了精彩的演示。我还要感谢我们的根服务器运营商为大家答疑解惑，另外，我想要厚着脸皮宣传一下，我知道今天已经快结束了，但对于“运作方式”系列会议，五点钟在 512G 房间，我们有一场全新的会议。亚伦 (Aaron) 会过来谈谈地区互联网注册管理机构，它们是做什么的，以及这方面的一

些基础知识。我诚挚地邀请大家继续与我们一起，五点钟，在 512G 房间，参加聚焦地区互联网注册管理机构的会议。好了，谢谢大家。谢谢你，安德鲁，谢谢你，欧赞，也谢谢大家的宝贵时间。

韦斯 • 哈达克： 我能再说一句吗？

史蒂夫 • 康特： 请讲。

韦斯 • 哈达克： 很遗憾，我去不了，时间上有冲突，抱歉，史蒂夫。还有一场面向新人的 DNSSEC 会议也在五点钟开始。

史蒂夫 • 康特： 好吧，这样的话，你得选择一下立场了。谢谢大家。

[会议记录结束]