圣胡安 — 英才每日会议
大西洋标准时间 2018 年 3 月 12 日星期一 — 12:00 至 13:30
ICANN61 | 波多黎各圣胡安

男性发言人（姓名不详）： 早上好。这里是 ICANN 61，3 月 12 日，英才每日会议。

西兰努什 • 瓦尔达尼扬
(SIRANUSH VARDANYAN)： 今天我们举办一场特殊会议，邀请我们的技术专家为大家做演示。今天有一位非常优秀的伙伴也在，让我把话筒首先交给瑞秋，然后请你们向英才计划学员们做个自我介绍，以便大家知道是谁在做演示。

请带着你们的午餐，找个位子坐下来，仔细听。这真的是一场非常有趣的会议，相信你们会喜欢。瑞秋？

瑞秋 • 雷耶斯
(RACHEL REYES)： 大家好。大家下午好。欢迎参加 DNS 基础会议。我们将举行 1.5 场会议。在演示环节结束后，用大概 15-30 分钟时间进行问答环节。

我是瑞秋 • 雷耶斯。是 ICANN 组织的技术支持。坐在我右边的是约翰 • 克莱恩 (John Crain)，稍后将协助我完成问答环节。

约翰 • 克雷恩： 我是约翰 • 克雷恩。我是 ICANN 负责安全性、稳定性和灵活性的首席官员。在过去的 20 到 30 年间，我还参与了根服务器和其他 DNS 服务的运营。

通过那边角落位置的电话接入会议的是迈特 • 拉森 (Matt Larson) 先生，也就是所谓的 DNS 先生。他在 DNS 行业的资历也许比我还要久。

下面我把话筒交给瑞秋。

瑞秋 • 雷耶斯： 好的，在大家吃午餐的时候也请麻烦注意一下我这边。我们开始了。

IP 地址很易于机器使用，对我们而言，记住名字很容易，但记住数字却非常难。

以我为例，我很难记住每个家庭成员的电话号码，但记住他们的名字却很简单，同样的情况也适用于 DNS 系统中的名称和数字。

在互联网早期，名称非常简单。那时还没有域名。这些是 24 个字符组成的单标签名称，指代主机名称。

域名解析就是将 IP 地址映射给名称。在互联网早期，主机文件名称为 HOST.TXT，这就是我们正在更新的部分，是由斯坦福研究院的网络信息中心或称 NIC 来维护的。该文件通过电子邮件由人工更新，每周发布一次，可通过 FTP 下载。那就是互联网早期的情况。

这个系统的问题在于，所有东西都必须人工编辑，所以非常容易出错，而且效率也很低下，因为你得先发送电子邮件，然后再由工作人员更新。并且，当你尝试上传或下载该文件时，需要非常大的带宽。所以这种方式并不能长久。

因此在上世纪 80 年代，人们开始讨论如何替代当前的系统。他们最终研究出这个 DNS 或域名系统概念，它能解决当前的 HOST.TXT 系统问题，也能简化电子邮件路由。在这里的 RFC 中，你们可以找到很多有关要求的文档。RFC 799 和 RFC 819 提供了很多有关要求方面的内容，以及有关 DNS 概念的讨论。

后面我们会简称为 DNS。现在我们将要首先讨论 DNS 系统中使用的术语。目前有 DNS、DNS 数据、解析器、名称服务器、缓存和复制。

我将使用这个图来详细讨论。根解析器也是其中一个将要讨论的术语。还有递归域名服务器，这是向我们的域名服务器发送

查询的服务器。域名服务器在我的左边，也就是你们的右边。随后，这些域名服务器将对递归服务器抛出的查询给予明确的答复。这里有个小气泡写着“缓存”。DNS 系统中使用缓存来实现更高效率和可扩展性。在演示的后半部分，我们会深入讨论这个议题。

域名空间是 DNS 数据库结构的反向树形态。通常，我们读取树形数据结构的方式是自上而下，但在 DNS 世界，我们的读取方式是自下而上。

让我们以这个图为例。读取方式不是“.com.example.www.”，而是“www.example.com..”，这是一个完全限定域名。

在域名空间中，第一个部分是根。第二个部分是所谓的顶级节点，后面跟着二级节点，然后是三级节点。

每个节点都有一个标签。标签可以合法使用的字符仅限字母、数字、连字符或 LDH。

标签可以使用的长度不超过 63 个字符。标签不区分大小写，所以基本上，将 .com 写成 “com” 或“cOm”也没关系。这并不重要。

每个节点都有一个域名。在我们的示例中，将使用这棵树。高亮显示的域名是“www.example.com.”。全部以句点分隔。

我刚才说过，完全限定域名或 FQND 以句点为结尾。大部分时候，当我们搜索域名时，并不需要在结尾处使用句点，只需要输入“example.com”或“www.example.com”。

域是一个节点，在它下面....在我们的示例中，.com 是域的顶级节点，在它下面的是 .com 地区名称或 .com 域名。

区域属于管理部门，每个 DNS 区都有权力界限，并被授权给一个实体。DNS 区域可以有一个域或者多个域或子域。授权创建了区域。授权区域称为父区域，被创建区域称为子区域。

这个父区域是根区，授权信息给子区域 .com、.uk、.coffee。.com 授权给这个子区域：.foo、.bar 等

我刚才说过，域名服务器负责答复递归服务器抛出的查询。一个区域的域名服务器权威拥有该区域的所有信息。基本上，当你发出查询时，如果递归服务器是空的，它将直接去到区域，因为那里有关于你的查询的明确答案。各区域有多个权威服务器。这是出于效率和冗余使用的考量。

如何在多个权威服务器之间让区域的数据保持同步？我们将这样的 DNS 协议内置到处理区域复制的服务中。使用主要服务器和次要服务器时会发生了这种情况。

主要服务器有明确的区域数据。如果要对一个区域进行更改，必须在主要服务器上执行。另一方面，次要服务器或者所谓的辅助服务器则从另一个权威服务器获取区域数据。这样的过程

称之为区域传输。区域传输实际上是 DNS 服务器与另一个权威服务器之间的通信。

我们要讨论的另一个服务器是区域文件的来源 — 主服务器。但要注意，主服务器并不需要成为你的主要服务器。次要服务器也可以作为你的主服务器使用。

区域传输由次要服务器发起。关于区域传输的处理以及如何对区域文件进行更改，在 RFC 1996 中有着详细的描述。

现在我们来看看 DNS 资源记录。DNS 资源记录就是我们所是说的 RRs。我刚才说过，每个节点都有一个域名。一个域名有多种不同的数据与之相关联，而域名中的这些数据就存储在 RRs 中。

资源记录有许多不同种类，我们只打算讨论其中一些。让我们继续看一下资源记录的格式。资源记录有五个字段：所有者、存活时间或称 TTL、类、类型以及 RDATA。所有者是与资源记录相关联的域名。存活时间是记录可被缓存在服务器中的时间。类是一个用于扩展的机制，大部分资源记录均未使用，因此大多数情况下我们会看到类显示为 IN。类型是记录存储的数据类型。RDATA 是记录承载的数据。

我想，看着这个你们会更加熟悉一点，或者我也可以显示给你们看。这个信息就是所谓的资源记录。如果你们对网络技术比较熟悉，那么就很容易理解我刚才说的话。

[这里有提到]，类型和 RDATA 将始终在必要情况下显示。这些是最常用的资源记录类型：A 数据代表 Ipv4 地址。AAAA 代表 IPv6。NS 是权威域名服务器。SOA 或权限开启始终显示在区域顶点。在我们刚才的例子中，你们会在 .com 上发现 SOA 信息。CNAME 或规范名称是另一个域的别名。MX 代表邮件交换服务器。PTR 是指针，或者用于反向映射。

我说过，还有许多其他资源记录类型。截至 2017 年 12 月，已有 84 种。你们可以访问这个网站，详细了解这些资源记录类型。如果访问那个页面，将会看到这些。

让我们来看一下 A 和 AAAA 记录。我刚才说过，这是 A 记录。它会给你 Ipv4 地址，而 AAAA 则会给你 Ipv6 地址。

域名服务器 (NS) 为区域指定权威域名服务器。它出现在两个位置，父区域和子区域，以此类推。在这个例子中，左边是域名区域，右边是域名服务器，而不是 IP 地址。

这是域名服务器记录标记从父区域到子区域的授权的方式。.Com 有 13 个域名服务器。基本上，这些是 13 个根区。这里显示了从根到 .com 的所有路径。

在授权的过程中，我们还会有一个孤立粘合记录。孤立粘合记录是什么？孤立粘合记录是一个 IPv4 或 IPv6 资源记录。它包括在父记录中，作为授权的一部分。之所以需要一个孤立粘合记录，是因为如果你要查询 www.example.com 的 IP 地址，将直接去到根区。根将向你提供域名服务器的 IP 地址。然后，

你得再次询问域名服务器：“www.icann.org 的 IP 地址是什么？”这将使你陷入循环，而且也无法得到答复，因为它们还没有 IP 地址。这就是我们需要孤立粘合记录的原因。

权限开启记录位于区域顶点。这是 SOA 的一个示例。它有域名服务器。Hostmaster.example.com 是区域的管理员。序列号是文件的当前版本。

刷新 (Refresh) 代表次要域名服务器在检查更新前所需等待的秒数。重试 (Retry) 代表次要域名服务器在重新尝试失败的区域传输前所需等待的秒数。到期 (Expire) 代表次要域名服务器在刷新或到期前可以使用数据的最长秒数。最短秒数是 TTL。

CNAME 或规范名称记录创建从一个域到另一个域的别名。在我的右边，也就是你们的左边是 CNAME，右边是规范名称和别名的目标。请记住，CNAME 创建别名并指向规范名称，但请勿过度使用。请勿创建链或循环。这样你的数据也不会很好。

邮件交换记录类型。MX 指定一个邮件服务器和一个邮件目的地偏好。这里的例子是，example.com MX 10 mail.example.com。通信编号 10 和 20 指示电子邮件或优先顺序。数字越低越好。这是我们推荐的[听不清]邮件路由方式。

反向映射。大部分时间，我们只需要查找域名的 IP 地址，但有时则需要查找域名空间而不是 IP 地址。这时，PTR 资源记

录就非常有用了。我们并不会一直使用它，但在网络端，它始终存在。就是这个样子。

我想问下约翰 • 克雷恩，为什么我们要有 in-addr.arpa。

约翰 • 克雷恩： 我们所说的 in-addr.arpa 是反向地址。有些协议会检查它，以便确保名称和地址可以双向映射。

瑞秋 • 雷耶斯： 好的，我们还有其他的资源记录类型，但除了 CDS 和 CDNSKEY 外都很少见到，这两个是 DNSSEC 的一部分。

这是 example.com 区域文件的示例。它有 SOA、域名服务器、IPv6、IPv4、以及 MX 记录和 CNAME。最后一部分是孤立粘合记录。我刚才说过，它申明了 IP 地址。没有这个，将变成循环。

现在我们进入解析流程。我之前提到过，我们有根解析器、递归域名服务器、权威域名服务器。这些服务器共同协作，查询域名空间中的 DNS 数据。

根解析器相对客户端而言是本地解析器。它可以在你的手机中，也可以在你的笔记本电脑中。递归域名服务器，这是向我们的权威域名服务器发送查询的服务器。[权威]域名服务器发送回应查询到答复。

DNS 查询始终包含三个参数，即域名、类、类型，正如我们的示例所展示的那样。

两种类型的查询。根解析器发送递归查询，然后递归域名服务器发送非递归或迭代查询，或者所谓的转介查询。这个我们待会儿再讨论。

我想先跳过这个。

这个必须要讨论，因为假设，当你开始解析流程时，递归服务器还没有就位或者刚刚启动。你就没得选择，只能直接前往根域名服务器，因为根区文件在那里。

域名服务器如何找到根域名服务器？必须经过配置。由服务器管理员进行配置，否则将无法发现它们。

这是根域名服务器列表和根提示文件。NS 是域名服务器。A 是 IPv4 IP 地址。AAAA 是 IPv6 地址。

根区管理非常复杂，我们就不讨论了。我们应该保持简单。如果你们想要详细了解，也许可以给迈特 • 拉森一些巧克力豆，让他花点时间来跟你们探讨一下。现在我们不准备讨论这个。

有两个组织在协作管理区域内容，也即 ICANN 和 Verisign。有 12 个组织在运营权威域名服务器。也许你们会想问，为什么是 12 个，我们明明有 13 个根服务器。那是因为 Verisign 占据了两个：A 服务器和 J 服务器。为什么他们有两个？约翰 • 克

雷恩和迈特 • 拉森可以回答这个问题，不过可能他们不打算讨论这个问题。除非约翰有时间来讲讲事情的来龙去脉？

约翰 • 克雷恩： 我不打算细讲，那只是历史原因。上世纪 90 年代，由于新增了服务器，在重新分配时，并不是所有服务器都被分配给了新的组织，有两个没有。其中一个给到东海岸的 Verisign，他们跟乔恩 • 波斯特尔 (Jon Postel) 以及 ISA 有非常紧密的关系，而另一个留在了 ISA，也即字母 L 服务器，当 ICANN 成立后，L 分配给了 ICANN，J 则留在了 Verisign。所以，这个分配方式是历史原因造成的。

瑞秋 • 雷耶斯： 好的。如果你们想了解某个国家/地区的根服务器，可以前往这个网站：root-servers.org。当然我也可以显示给你们看。假设你们在查找波多黎各的可用根服务器。目前，L 和 J 在波多黎各可用。如果你们想了解此类信息，可以前往这个网站。

另外，我们的这个任播目前正在使用这些根服务器的镜像，将有助于查找你们所在地区最近的 DNS 或根服务器。你们执行搜索时，这个也会很有帮助。如果你们所在地区有镜像，那么就会更有效率。

根区更改流程。正如这页幻灯片所示，这是一个简化版本。实际上背后的流程很多。我们不打算进行讨论，只是让你们概览根区文件如何被更改。

基本上，一开始是由 TLD 管理机构向 IANA 提交更改。然后 IANA 将执行请求，先更新根区数据库，然后创建根区文件，再向所有根服务器发布根区。

现在我们进入解析流程。这是当你们通过手机发起查询时发生的情况。当然不一定非得是从手机发起。也可以从笔记本电脑或其他客户端发起。每个客户端 — 笔记本电脑、手机 — 都有这样一个本地根解析器。

然后它将询问：“www.example.com 的 IP 地址是什么？”这个问题连同 IP 地址 4.2.2.2 将前往递归服务器，然后它将询问：“www.example.com 的 IP 地址是什么？”递归域名服务器将回答：“我不知道，也许根服务器有该信息。”

为什么你的递归域名服务器没有该信息，因为它是一个全新的递归域名服务器。刚刚提到过，空的或全新的递归服务器还没有完整的缓存信息，所以它将直接前往根服务器询问 IP 地址，因为根服务器有根区文件。

然后，根服务器将返回一个转介，“我不知道地址，但我知道 .com 的地址。”所以递归域名服务器将前往 .com 并询问：“www.example.com 的 IP 地址是什么？”然后 .com 域名

服务器将回答：“我不知道，但我知道域名服务器和 ns1.example.com 的 IP 地址。”

现在，递归服务器将前往这个域名服务器 ns1.example.com，然后这个域名服务器将返回 IP 地址或针对查询的确定性答复。然后，递归服务器将返回 IP 地址给根解析器。

这个过程在数秒内完成。不会耗时几分钟。这有点类似于你从手机或笔记本电脑启动一个应用程序。有时候可能需要点时间来加载页面或打开应用程序。但如果你尝试重新加载，就会更快。为什么呢？因为信息已经缓存到你的客户端了。

让我们再看一下。缓存加速了解析流程，因为现在它已经知道了你的根区和域名服务器的名称和 IP 地址。如果你尝试访问或尝试请求“ftp.example.com 的 IP 地址是什么？”，而在此之前我们询问过 www.example.com 的 IP 地址。

现在我们要询问 ftp.example.com 的 IP 地址。那么你的 Safari 或根解析器将再次前往递归域名服务器，但这次将不会返回到根区，而是直接前往域名服务器，因为它已经缓存了信息。使用缓存能让整个流程更高效、更快速。这就是解析流程。

我们这里有一页关于 DNSSEC 的幻灯片。如果你们想深入讨论 DNSSEC，可以参加后续的一些会议。我们这周有关于 DNSSEC 的会议供大家参加吗？

约翰 • 克雷恩： 我看看，实际上我们即将举行一场 DNSSEC 会议。好像是在周三，在本次会议结束前我会通知确切时间。

男性发言人（姓名不详）： 昨天也有个培训。

瑞秋 • 雷耶斯： 好，很好。所以，这只是 DNSSEC 的基础知识。我为大家读一下。通过 DNSSEC，DNS 数据可以拥有数字签名以便于验证。每个区域都有成对的公钥和私钥来运行 DNSSEC。

DNSSEC 中的一些记录包括 DNSKEY，也就是区域的公钥，还有 RRSIG 或数字签名。NSEC 或 NSEC3 是指向区域中下一个名称的指针，DS 是授权签名方。

重申一下，如果你们想要深入了解 DNSSEC，可以参加我们以后举办的 DNSSEC 会议。

域名生态系统类似于这样。我们的注册管理机构有域名和注册人以及注册服务机构的数据库，注册服务机构是介于注册管理机构和注册人之间的主要代理机构，而注册人是域名注册的持有者。

这是域名注册流程，不过我们不打算讨论整个流程。我只是想告诉大家，我们刚刚讨论的是整个域名注册流程的一部分。我

们刚刚讨论的在这里，在权威域名服务器、递归域名服务器以及互联网用户下方。

这就是我在今天的会议上要展示的内容，有人想提问吗？

约翰 • 克雷恩： 在我们进入问答环节之前，我想讲一下关于 DNSSEC 会议的事情。周三的上午 9:00 到下午 3:00，一整天时间探讨 DNSSEC。应该能满足大家的需要。

瑞秋 • 雷耶斯： 好的。

西兰努什 • 瓦尔达尼扬： 现在我们可以开始问答环节了。好的，请。

尼古拉斯 • 费玛莱利 (NICOLAS FIUMARELLI)： 大家好。我是来自乌拉圭的尼古拉斯 • 费玛莱利。你刚刚提到 DNS 不区分大小写，那么国际化域名是否区分呢？

瑞秋 • 雷耶斯： 请迈特来回答这个问题。

迈特 • 拉森： DNS 本身是不区分大小写的。国际化域名在 DNS 的层级之上。请瑞秋将幻灯片切回到开始的几页，关于域名空间的那几页。继续往下。很好。谢谢。

请看这张幻灯片，我想说的是左上方的节点，以 xn-- 开头的那个，我们对国际化域名的处理方式，是在顶层执行。

从用户的角度来说，如果一个应用程序启用了 IDN，用户与之互动，就会看到以国际化字符显示的域名。但应用程序随后得转换为这个 LDH，也就是 DNS 可以识别的字母、数字、连字符格式。

所以从 DNS 的角度来说，它们看起来就是普通的标签，尽管有点可笑。你可以看到 xn-- 是一个代码，意味着这个标签的其余部分是一个编码的 IDN。实际上存在一个名为国际化域名编码 (Punycode) 的特殊编码，它是统一域名编码 (Unicode) 的一个双关语，专门用于为 DNS 中的标签编码 Unicode 字符。

尼古拉斯 • 费玛莱利： 谢谢。

迈特 • 拉森： 对了。关于这一点还有更多的背景信息，当我们这么做的时候，有不少人问道：“我们为什么还需要高于 DNS 的层级？为什么不直接把 UTF-8 编进 DNS？让我们在 DNS 中使用 UTF-8 标签吧。”

我们有合理的顾虑不能让 DNS 系统这么做，因为这本身就不是它的设计用途。我们必须得升级整个 DNS 基础设施，并且还必须得升级所有的客户端来将 UTF-8 放进标签。

在我们对 IND 这么做时，背后的想法是:“好吧，我们还必须得升级所有的客户端，但至少我们不需要碰 DNS 基础设施的其他部分。”所以问题在于你想要牵涉多少东西。你想要牵涉所有东西？应用程序和 DNS 基础设施，还是只是应用程序？

西兰努什 • 瓦尔达尼扬： 很好。那边好像有人要提问？有请。

阿布杜卡林 • 欧罗耶德 (ABDULKARIM OLOYEDE)： 谢谢。我想首先就刚才的话题提个问。你刚刚说 DNS 之上还有一层。在我的理解中，这意味着，如果你向 DNS 服务器发送查询，你会把所有的信息都发送给 DNS 服务器。所以现在如何能让 DNS 之上还有一层呢？问完这个问题，我后面还有问题。

迈特 • 拉森： 当然。我说的 DNS 之上的一层是概念上的，但实际上它位于任何能够理解 IDN 的应用程序内部。

例如，在能够理解 IDN 的现代网络浏览器中，你可以键入一些非拉丁字符，然后它会被转化成类似 xn-- 标签的东西。可能是 xn--.，或是 xn--其他内容。以逐个标签为基础进行国际化。然后网络浏览器发送查询，调用根解析器，根解析器将查询发送给域名服务器，该查询的标签中将包含 xn--。

所以，我说 DNS 之上一层的意思是，这是在应用程序中完成的，而不是在 DNS 服务器或解析器中完成的。

阿布杜卡林 • 欧罗耶德： 谢谢。现在提出我的问题。我有两个问题。第一个是，在你进行演示的时候。我不知道我是否因为吃东西而错过了什么，或者你讲的太快了一点。关于区域服务器的部分。你说，它有点复杂。我对区域服务器也有点不明就里。区域服务器是指什么？尤其是当你说到主要区域服务器、次要区域服务器，然后谈到这些区域服务器有点类似辅助服务器和主服务器。你能就这个部分再讲解一下吗？

我的问题的另一部分是 4.2.2.2，意思是不是，如果你发出任何查询，它是所有查询的默认递归服务器？

约翰 • 克雷恩： 如果你是在讨论域名服务器的不同类型，我们一般不会称之为区域服务器，基本上域名服务器有三个类型。在你的笔记本电

脑、手机或者操作系统中，又或者在诸如浏览器的应用程序中，有根解析器。它们只负责答复问题。

然后通常你的 ISP 或者你家中的家庭路由器中，有递归服务器。它们负责传送问题。它们要去到权威服务器。而权威服务器是实际拥有答案的服务器。这也就是我们称它们为权威的原因。它们有权给出答案。实际上，区域文件就位于权威服务器上。

在递归服务器上，有负责发送查询的查询引擎。在这些服务器上存储的有限数据都位于缓存中。所以它有存储器可以记住答案。而根解析器也可能有答案。所以，从你的设备出发的路径永远是向上的。

我记得瑞秋就根区供应的复杂性说过一句。不知道你是不是想问这个问题。那完全是另一回事。那是一个完整的供应系统，而不是域名服务器系统。我想请迈特来谈一下，如果他愿意的话，因为他正在处理其他一些事务。

关于你要使用哪个递归服务器，通常在你设置笔记本电脑或网络时进行定义。当你通过网络连接时，我们会使用动态主机配置协议或 DHCP。它会向你发送你使用的 IP 地址，也可以向你发送你的域名、递归服务器。你可以设置两个。你可以设置一个。你可以设置四个。然后，你的所有查询都会前往已经配置好的服务器。

西兰努什 • 瓦尔达尼扬： 远程参与者有个问题。好的，请先结束这个问题。

迈特 • 拉森： 特别提一下你问到的 4.2.2.2。那是由三级通信 ISP 运营的一个服务器。也就是所谓的开放式递归服务器。通常，无论在哪里有客户端群 — 例如 ISP 为其宽带消费者设立的网络，或者 ICANN 网络下的大厦 — 无论在哪里有带根解析器的客户端群（左上方），都需要在顶层有一个递归服务器。

正如约翰所说，网络运营商负责提供递归服务器，当你接入网络时，你的设备就会获得递归服务器的 IP 地址以自行配置。

但是，你并不是一定要用那个递归服务器。你可以使用其他的服务器。有很多广受欢迎的开放式递归服务器，它们接受来自任何人的查询。你可以将这些第三方递归服务器称为公共递归服务器。也许最受欢迎的是 Google Public DNS，因为它有一个非常好记的地址 8.8.8.8。如果你愿意，可以在手机上配置根解析器。然后也可以更改其配置，让其前往 8.8.8.8 而不是 ISP 分配给你的递归服务器。

另外一些受欢迎的开放式 DNS 也已经存在很长时间了。当第一次有人提议把递归服务器放在网络之外，然后由他们来提供服务的时候，这些服务器就出现了。Verisign 有。PCH 也有，名为 Qaud9、9.9.9.9。还有很多其他公共服务器，4.2.2.2 就是其中之一，也已经存在很长时间了。

西兰努什 • 瓦尔达尼扬： 谢谢。远程参与者有个问题，来自非洲的[听不清]。“非洲正在稳步发展中，存在能力提升的需求。除了填补发展中国家空白的英才计划之外，ICANN 或者在这一方面 DNSSEC 有什么行动计划来提升能力？在政策方面，我们非洲要做些什么？”

约翰 • 克雷恩： 能力培养，我们在讨论 DNS，所以我会围绕 DNS 来谈谈能力培养。我们一直在与社群共同努力。特别是我们工作组，我们做了大量的能力培养工作，大量培训。具体到非洲，你们很可能会看到类似 AfriNIC 的组织，或者如果去到 AFNOG 或 AfTLD（例如 AF 顶级域），你们很可能会看到他们在提供这类培训。我们与他们紧密合作，提供支持。

另外还有名为网络新创企业资源中心的组织，也深度参与了非洲 DNS 和其他基础设施问题的培训指导。

具体到 DNSSEC，我们在非洲地区同时与 AFNOG 和基本上所有的 AF、非洲组织合作完成了许多培训。虽然我不确定下一次培训的时间安排，但我想在五月和六月期间，会安排一些 DNSSEC 实际操作培训。

所以我们在那里非常活跃，但我们也依赖当地专业人士的支持。如果要在全球范围内做培训，那可是个大工程，而且也不是 ICANN 的工作。当然，ICANN 是个小组织。有些人觉得它太大了，但实际上它仍然是个小组织。所以我们接触了当地的技

术社群，通过向他们提供资料或者与他们合作改进他们的资料来帮助他们。这方面比其他方面开展得要好。

我们在一些在线学习平台上开展工作，这将让我们有能力提供线上学习，也能让我们更方便地把资料翻译成各种不同语言。

所以，尽管我们不是全球性的大学，但我们也确实花了很多时间去做教育培训。你们看看我的头衔，其中包含“安全性、稳定性和灵活性”，充满了对生态系统的关注。你们要做的改进是，确保人们能更好地获取知识和有能力构建更好的系统。

西兰努什 • 瓦尔达尼扬： 谢谢。兰登？

兰登 • 泰利福德 (LENDON TELESFORD)： 大家好。我是来自格林纳达的兰登。我不确定这个问题是关于 DNS 的还是整个系统的。我也不确定是不是有可能，但我还是打算问一下。在刚刚的演示中，提到了任播和根服务器的不同镜像。我的问题是，在客户端服务器和任播方案内，有什么样的机制来防止会影响距离感知的 DDoS 攻击？这类攻击会让客户端不知道访问哪个服务器来获得响应。

约翰 • 克雷恩： 我还在思考这个问题。你打算回答吗？

迈特 • 拉森： 好吧，我不是太清楚你所说的客户端不知道访问哪个服务器是什么意思。我想在我的回答中再次使用层的概念。任播是 DNS 下方的一层。我们有 DNS，而任播属于互联网路由系统。

让我们来看看根服务器系统，我确信现在每个 IP 地址都是任播。假设我们有一个准备向 L 根发送查询的递归域名服务器。从 DNS 层，它会说：“我要向这个 IP 地址发送查询。”

但当它进入路由层，网络本身将不得不传输一个数据包，而网络中的路由器将会看到，在该 IP 地址可用的多个网络位置上，实际存在着多个镜像。根据 BGP 路由协议，我们会说，有不同的网络宣称可以路由到该特定网络。所以在整个互联网上，会有多个网络说：“我可以到达 L 根。”“我可以到达 L 根。”“我可以到达 L 根。”

而路由器将使用来自 BGP 的信息来做出决定。“从我的角度，哪条才是去往 L 根的最佳路径？”所有的路由器都会这样。也就是说，当你说“我要向 L 根发送数据包”，那么根据你在网络中的位置，你会前往“最近”的镜像。不仅仅取决于地理距离。也不仅仅取决于延迟。所有的因素都会影响 BGP 路由政策。

我也不确定什么因素会让客户端不知所措。可能发生的情况是，当某个镜像遭受攻击时，它会变得超出负荷，而运营商通常的做法是，配置任播配置中的域名服务器，当该域名服务器可用时，则会告诉网络：“我在这里，你们可以推广我的路由，我还在。”但如果路由变得拥堵以至于崩溃，如果它很从容地发生故障，则会告诉网络：“噢，我不行了。我无法再接受 DNS 查询了。”然后网络会重新计算，把网络流量发送到别的地方。

兰登 • 泰利福德： 所以在路由器端，路由路线的决定是基于预填充的 BGP 信息？

迈特 • 拉森： 不是预填充的。它一直在变。每个网络，每个所谓的自治系统编号，从 BGP 的角度来看也是一个网络，自治系统是一个集合路由的网络，它会自己进行宣传：“我有这些 IP 地址。”

因此，每个执行 BGP 的路由器都会持续说：“这些是我认识的网络”，而其他路由器会听到并实时确定所有的东西在哪里。这是运作原理的极简版本，BGP 一直在实时发挥作用。

约翰 • 克雷恩： 补充一下，这并不是任播所必然导致的。这是围绕在任播前的，因为你会看到，通往节点的路径有许多条。如果有人在宣

传某个网站，如果距离很远，那么很可能只会发现一条发送路径，但如果距离相当近，则会发现多条路经通向它。当天返回时也是同样的道理。所以这是已经被发现的一个路由技巧，后来用于增添更多服务器。对于任播，没有技术性更改。只是一个路由技巧。

兰登 • 泰利福德： 我想，我只是想知道是不是有绕开路由技巧的方法。

约翰 • 克雷恩： 我认为没有那样的方法。现在的路由也有自己的安全性问题，但主要是跟路由而不是任播有关。路由确实有一些安全性问题，或者说缺乏安全性的问题可能也是设置路由的一个很好的方式。但对于任播并不如此。

西兰努什 • 瓦尔达尼扬： 谢谢。有请那边发言。

萨尼尔 • 艾纳 • 萨米 (SHABNIL ANAL SAMI)： 大家好。我是来自斐济的萨尼尔。我的问题是，如果一个国家想要设立根服务器，有什么最佳方式有助于决定要设立哪种服务器？比如 13、A、L、F 等？或者说得根据地区或什么人来设立？

约翰 • 克雷恩： 根据你决定跟谁去探讨这个问题。首先我要说的是，并不是一个国家，只有一个网络或网络运营商才会想要设立镜像。他们可以前往 root-servers.org，看看运营商列表。我们是其中一个运营商。我觉得我们在斐济也有一个运营商，当然其他人也有。

你可以直接联系那些运营商，询问他们开出的条件。每个运营商可能稍有不同，不会区别很大。目前全球有 990 个镜像或位置。所以要添加的话，就去联系一下好了。你可以前往 root-servers.org 网站，那里有每个运营商的链接，你可以看到他们的相关文档以及联系方式。我也很乐意在线下提供帮助。

萨尼尔 • 艾纳 • 萨米： 我只是有点顾虑该设立哪种，L 还是 F，所以只是去问问就好了吗？因为我看到波多黎各设立了 L，斐济也设立 L，所以有点困惑这种区域性的东西。谢谢。

约翰 • 克雷恩： 是的，这是一个区域性问题。通常也是个关系问题。斐济即将设立第二个根服务器，之所以设立 L 是因为，我们有位员工萨维 • 沃西亚 (Save Vocea) 在那里。所以很多情况下，主要取决于你的现有关系，或者打算与网站上哪个运营商建立关系，“噢，这个看起来不错。”

同时，你做这件事的财务标准也可能不太一样。举例来说，我们 ICANN 有一项解决方案，如果你支付服务器和上线的费用，那么所有的工作都可以交给我们。而其他人，你给了他们钱，他们只是发货给你一台服务器。机型也稍有不同，你需要弄清楚哪个适合你。

在 DNS 看来，所有的根服务器都是平等的。它们都会给你相同的答案。从查询的角度来看，它们的工作方式完全一样。所以实际上取决于业务关系和你认识的人。

萨尼尔 • 艾纳 • 萨米： 好，谢谢。

西兰努什 • 瓦尔达尼扬： 还有其他问题吗？好的，请讲。

男性发言人（姓名不详）： 我有两个问题。如果能够确保从各个国家/地区的注册管理机构正确复制区域，而不会像几年前发生的那样[听不清]错误？第二个问题是，各个国家设立的根服务器镜像是全球[听不清]的一部分吗？只是这个根的[听不清]的一部分。例如，L 根只拥有全部[听不清]的一部分，还是拥有全部记录呢？

迈特 • 拉森： 不，所有的根服务器都拥有同样的信息。只有一个根区包含信息，每个根服务器都拥有同样的信息。

你能重复一下第一个问题吗？

男性发言人（姓名不详）： 例如，当注册管理机构[听不清]。

西兰努什 • 瓦尔达尼扬： 提醒一下：我们有翻译服务。你可以用母语提问。

男性发言人（姓名不详）： 好的。

迈特 • 拉森： 好极了。好极了。

西兰努什 • 瓦尔达尼扬： 所以尽管用吧。

男性发言人（姓名不详）： 好的。请稍等一下。

西兰努什 • 瓦尔达尼扬： 对了。需要耳机的请尽快戴上。

女性发言人（姓名不详）： 喂喂。你们听到英文翻译了吗？你们听到英文了吗？好，很好。谢谢。

男性发言人（姓名不详）： [通过翻译]当每个国家和地区的记录在类似 ccTLD 的区域有一项记录时，当注册管理机构在区域中有一项记录并且发布和分发到整个 DNS 区时，如果能够确保发布的是正确的记录，在发布和分发的过程中不出错？因为据我所知，过去曾发生过这样的问题。

约翰 • 克雷恩： 是有过一些问题。我想确认一下术语和技术。不管是 ccTLD 或 gTLD，当它们发布由来自数据库的数据组成的区域时，它们有责任确保数据的正确性。实际上一旦发布出去，如果 DNSSEC 签署了区域，而当你在鉴定 DNS 查询时，你就能确保得到它们发布的准确数据。

那就是最终的情况了。那是在发布和 DNS 端。在所有其他方面，则与网络安全性、数据安全性和数据完整性有关。过去确实出现过问题，因为有人攻入了 ccTLD 系统，我想你说的可能是这件事。

男性发言人（姓名不详）： 是的。

约翰 • 克雷恩： 在真正安全的网络中，不会发生这种事。我想，人们在这方面会一直保持敏感。我们 ICANN 和我们在注册管理机构的朋友们，尤其是我的安全性工作组会怎么做呢，当他们发现问题时，会马上联系我们，我们将帮助他们进行恢复。我们将经常帮助他们，也会找专家来帮助他们重新设计他们的系统。

我们已经有了一些案例，我想我知道你说的是哪个，不过我不打算指明了。我们已经有了一些案例，他们遭遇 SQL 注入式攻击的案例。那是针对他们系统的特定攻击类型。

不法之徒、坏人趁机更改大型组织的记录，并把网络服务器地址指向别处。所以从外界来看，似乎是网络服务器被劫持了。但事实上并不是。是注册管理机构的系统。

那次，我们花了大量时间与注册管理运行机构共同努力，他们现在有了一个全新的系统，有了更多诸如审核的对抗手段。他们已经从过去的错误中得到教训并继续前进，那是在泄露事件中你能够做到的。你要了解泄露是如何发生的，然后修正系统，从中吸取教训并改进流程。

不过那并不意味着，其他的一些 ccTLD 或者甚至 gTLD 将永远不会再次被黑客攻入，因为那不现实。我们看到，许多资金雄厚的巨头公司也会被攻击。

男性发言人（姓名不详）： 非常感谢。

西兰努什 • 瓦尔达尼扬： 好的，请讲。

杰森 • 海因德
(JASON HYNDS)： 我是杰森，我想补充一下。

西兰努什 • 瓦尔达尼扬： 请先陈述自己的姓名。

杰森 • 海因德： 噢，抱歉。好的。我是来自巴巴多斯的杰森 • 海因德。约翰，我的补充问题是，你们是否曾发布过什么内容来帮助注册管理运行机构在泄露事件发生前加以避免？

约翰 • 克雷恩： 我刚刚说过，跟我们的合作伙伴携手进行能力培养，我们已经累积给运营商做了成千上万小时的培训，主要围绕“如何确保网络安全？”“如何监控网络？”当然，在座的运营商社群也有自己的分组，共享了非常多的最佳实践并互帮互助，包括工程方面的协助。

在隶属于拉美地区的牙买加，有个名叫 LACTLD 的组织，汇集了该地区所有的或者绝大多数的注册管理机构。他们会举办例行会议，举办技术会议，当其中一家出现问题时，其他家会施以援手。

所以他们并不会独自面对问题。而是整个社群共同面对。通过培训和互助，那里一片热火朝天。

西兰努什 • 瓦尔达尼扬： 大家有问题要问吗？似乎没有问题了。

我建议大家参加周三的 DNSSEC 工作坊，时间是上午 9 点到中午。

男性发言人（姓名不详）： 到下午 3:00。

西兰努什 • 瓦尔达尼扬： 到下午 3:00。

男性发言人（姓名不详）： 时间很长。

西兰努什 • 瓦尔达尼扬： 是的，在中场的午餐时间，我们会有个英才会议。但不管怎么说，请尽量参加那次工作坊。非常非常重要。

最后还有什么要说的吗？

瑞秋 • 雷耶斯： 谢谢大家出席本次会议。非常感谢。也要谢谢约翰和迈特，帮我完成问答环节。

西兰努什 • 瓦尔达尼扬： 感谢我们的口译员和技术人员。我个人也非常感谢迈特、约翰还有瑞秋付出宝贵时间。我知道在这次会议期间你们都非常忙，非常感谢你们能来并且为英才计划的学员们做这场演示。请为我们的演讲嘉宾鼓掌。

现在我们可以散会了。谢谢。

[文稿完毕]