海得拉巴 — 联合会议：ICANN 董事会和技术专家小组 (TEG)
2016 年 11 月 8 日，星期二 — 16:30 至 18:30 IST
ICANN57 | 印度海得拉巴

戴维 • 康纳德 (David Conrad)：

欢迎大家。本次会议是 ICANN 57 技术专家小组会议，同时也是 TEG 和 ICANN 董事会的联合会议。

我们对已经发布的议程稍微做了变动。最初关于数字对象架构的话题不得不删除。演讲人苏珊 • 沃尔夫 (Suzanne Woolf) 已经表示她身体不太舒服，去休养了。我相信她会回来，但是今天她因为身体原因不能发言了。所以我们从议程中删除了这个话题并相应地增加了一项 — 由我们的好朋友沃伦 (Warren) 来谈谈 IETF 的问题。

如果有人还不知道什么是 TEG，那么我来介绍一下。TEG 专注于前瞻性的技术性问题和技术问题，特别是考虑到这些问题会影响到互联网唯一标识符系统的使用。在 TEG 成员们看来，ICANN 董事会和工作人员在考虑 ICANN 的战略和运营时，应该把这些问题考虑进去。

TEG 是一个非正式小组。它不是咨询委员会。它没有预算。它的职责是向董事会提供建议，而董事会没有义务接受这些建议，除非这些建议来自于专家以及那些看起来很不错的人。

下面介绍本 TEG 的议程：吉姆 • 加尔文 (Jim Galvin) 将介绍特殊名称问题的最新情况，以及问题声明和 SSAC 定义的问题空间的状态；霍华德 • 本 (Howard Benn) 将介绍 ETSI NFV，网络功能虚拟化；实际上由 ICANN 资助，并由约翰 • 莱文 (John Levine) 完成的工作 DNSEXTLANG；最后沃伦将介绍 IETF 相关的问题。

下面有请吉姆。

吉姆 • 加尔文： 谢谢戴维。我看到这里放了幻灯片，非常好。

今天我来做这个介绍，一方面是作为 SSAC 副主席的角色，另一方面也是因为我在 SSAC 内部讨论这个问题的工作组中担任主席一职。

请放下一张幻灯片。

今年的大部分时间，SSAC 都在考虑域名空间的问题、域名的存在、以及由于域名在互联网一般会员社群中的使用而造成的冲突。之所以要在这里介绍一下最新情况，是因为在一些问题的描述上，我们其实已经达成了共识，包括问题空间、我们认为目前的情况如何，以及我们看到的 ICANN 社群所面临的问题。

所以在这里要做的第一件事，就是解释我们所说的“域名空间”的含义。基本上，它是指在由单个标签所组成的树形结构层次中，你可以获得的所有潜在域名。

这不仅仅是 DNS，了解这一点很重要。在想到域名时，大多数人想到的是 DNS。但 DNS 本身实际上是我们在这里所探讨对象的一个子集。

所以我们所研究的问题空间是指在这个树形结构层次中可能存在的全部域名，而 DNS 只是其中的一部分。

在这个社群中观察到的另一件有趣的事就是，域名空间和支持 ICANN 为本行业管理、授权和分配使用 DNS 域名的 DNS 协议也被用于其他地方，而不仅仅是全球公共 DNS，这是一个重要的考量。

为什么我们会有冲突、为什么我们会有这个问题，原因是，事实上域名和 DNS 取得了巨大的成功，以至于被其他人调整后应用到其他地方，这是一件好事。这是一个成功的标志，也是创新和趣事发生的一个机会。

对于我们考虑的这个问题所在的问题空间，最后一件必须理解的事情就是，今天 IETF 所定义的在全球 DNS 中使用的域名，实际上没法严格界定范围。

也就是说，如果我有一个域名而它就是存在，那么我其实没有足够的信息来了解如何处理它。所以，想想你的浏览器，你在一个空文本框内输入了一些东西。大多数浏览器，这是一个组合机会，你们可以输入一些字词来搜索，或者也许输入一些用小圆点隔开的看起来像域名的标签，然后在 DNS 中查找。

但问题是：这实际上，在一般情况下，是不够的。浏览器必须猜测要怎么做。所以这是一个例子。

在你自己的本地环境中，你知道，在你的本地环境中你有一台 DNS 解析器，而在你的电话上以及台式或笔记本电脑上，有其他应用程序和服务，我是说，你有着同样的问题。你可能有或者没有足够的信息，来了解提供给你的名称，看起来像是全球公共 DNS 中域名的标签，是不是真的在它所属的地方。

而事实上，这就是我们所研究的问题空间，也是 ICANN 社群需要了解并在审议中考虑的。

请翻到下一张幻灯片。

那么在看待这个问题时，你知道，也就是看待我们所面临的这些环境和这些事实情况时，我们有了如下发现，那就是，域名空间的使用未经协调其实是产生问题的根源。冲突是源自于名称的使用未经协调这个事实。

所以事实就是，你可以拥有域名，而且有一个应用程序，理解自己所使用的是域名，同时你也可以拥有这样的本地环境，它们所使用的名称本意是指代本地环境中的一些事物。它们的本意不是指代全球 DNS 中的某个名称。

正因如此，才会造成这些名称的冲突。

想想在最近的这次为新 gTLD 开放的申请轮次中，目前有几个名称正处于搁置状态。它们被暂时推迟，与此同时我们正在考

虑如何处理它们，当然 .corp、.home 和 .mail 一直在这些名称当中。申请是为一些名称而提交的。

那是源于这样一个事实 — 我们让这个域名空间在不同的地方使用，所以关于如何处理它们一直是模棱两可的。

所以，域名空间中缺乏两个以上团体之间的协调，这实际上造成了不稳定性。我们有冲突这个事实，造成了模棱两可的态度，而这种模棱两可从根本上说是一个关乎互联网安全性和稳定性的问题。当然，考虑这类重大问题，为社群提供建议，是 SSAC 直接负责的事务。我们指出这些问题，是为了让社群在围绕这类事务制定政策和流程时将它们考虑进去。

显然，至少有两个团体对域名及其出现或存在具有一定影响。

当然，ICANN 明显是其中一个。因为它有一个角色就是根区域名分配与指定的协调人。做出这些决定是 ICANN 的职责所在。

IETF 明显是另一个也扮演着某种角色的组织。它编制了一个列表，名叫特殊名称保留列表，其中囊括了它想要保留和保存，并认可用于技术用途的名称。比如，.LOCAL 就是这个列表上的一个名称。.ONION 是这个列表上的另一个名称。IETF 设立了自己流程来将名称纳入到列表中，并且 ICANN，当然，我们大部分人可能都很熟悉了，也有自己的一套流程和政策来判断允许和不允许哪些名称存在于根区之中。

此外还有其他个人和机构 — 也许我们并不了解。但肯定至少会有一些私人用途。

事实上，这就是 .corp、.home 和 .mail 存在的问题。这些特殊标签在整个互联网中被大量用于私人用途，这就是为什么它们会带来问题。因为它们与可以在根区中使用的名称相冲突，而 ICANN 作为一个社群，必须联合董事会与工作人员一起做出决定。关于如何处理这个问题，如何应对这种不稳定性，我们必须达成一致意见。

所以我想那是这里的最后一张幻灯片。这代表了我们目前的工作进度。我们对我们认为问题空间是什么做出了一个定义和声明，我们认为它很重要。我们也就我们对眼前事实的理解得出了自己的结论。目前下一步就是要编制一系列建议。

如果你们参加了 SSAC 公共论坛就知道 — 这个公共论坛是在本次 ICANN 会议期间最后的会议阶段中举行的 — 实际上我们做出了声明，SSAC 希望在 2017 年第 4 季度结束前向社群提供一系列建议和工作成果。

关于这一点有问题吗？

戴维 • 康纳德： 下面我把发言的机会交给董事会成员或观众席中的成员，现在可以就这个话题提问了。

史蒂夫 • 克罗克 (Steve Crocker)： 谢谢，吉姆。这个介绍使人受益匪浅。请继续。

戴维 • 康纳德： 彼得，请讲。

史蒂夫 • 克罗克： 对。

彼得 • 科赫 (Peter Koch)： 我是来自 DENIC 的彼得 • 科赫。

吉姆，你提出了这个普遍观点，也就是说，存在相似的域和域名空间，ICANN 内部要对这个域名系统承担某种责任，而且事实上 IETF 也要承担其他责任。

那是谁的普遍观点？

吉姆 • 加尔文： 我们承认的是，ICANN 对进入根区的名称要承担一定责任，而且我们只是观察到，还有其他团体在利用这一技术的存在 — 具体地说就是公共 DNS 及其解析协议以及你可以拥有域名这个事实 — 并在其他地方使用这些名称。实际上我们对他们的权限或责任没有任何想法。我们只是承认他们的存在，以及他们所做的事情。而且我们必须承认他们的存在，ICANN 社群也有责任承认这一点，并以某种方式对此做出反应。

彼得 • 科赫： 我还可以提另一个问题吗？

你再次说到了“我们”。这个“我们”是谁？

吉姆 • 加尔文： 哦，是社群，“我们”是指 ICANN 社群。我把自己看成是社群中的一份子。

彼得 • 科赫： 好的。那么我可以说这是你的个人观点吗？我要说的是，在这个特殊问题上不一定是没有争议的，我想提供不同的看法。

你所说的私人用途也可以称为域名抢注。这和我可以在不经你同意的情况下使用你的车，并宣称这是将你的车用作私人用途是同样的道理。

IETF 和 ICANN 之间签署了一个 MoU，而且明确划分了对域名空间承担的各项职责。这个 MoU 和 IETF 或 IETF 的部分成员认为他们有能力和权利通过宣称存在协议问题来分配名称所仰仗的文件，我看到 — 我看到它们存在分歧。因此我想敦促 ICANN 董事会与 IETF 接触，履行他们与这份谅解备忘录有关的职责，然后我们可以以此为起点。谢谢。

吉姆 • 加尔文： 好的。谢谢你，彼得。当然我会将它作为对 SSAC 的意见 —

史蒂夫 • 克罗克： 彼得？

吉姆 • 加尔文： — 以便在 —

史蒂夫 • 克罗克： 彼得？

吉姆 • 加尔文： — 建议的编制工作中考虑。

史蒂夫 • 克罗克： 让我们再继续至少一轮。

彼得 • 科赫： 当然可以。请自便。

史蒂夫 • 克罗克： 谢谢。但是基本上是另一种情况。

虽然我没有 100% 了解最新情况，但大致上有所了解。所以我想要理清几件事，虽然吉姆也谈到了，但是我想要再谈一谈。

有的名称进入根区，大家可以基于进入根区的名称来讨论域名系统。IETF 组织了域名空间的结构，所以在一定程度上，他们也可以讨论名称在 DNS 以外语境下的使用。从现实意义上说存

在的问题就是，本打算在 DNS 以外使用的名称出现在了 DNS 中。“Local host”是其中一个例子，此外还有其他例子。

所以现实问题就是，尽管从理论的角度上，可以说用于域名系统的域名空间和用于其他用途的名称空间是完全独立的，但事实上它们交织在一起。它们彼此交融。虽然有人忽视这一点，不去注意它的后果，但还有一种看法是说：“让我们关注事实，如果有一些通常用于根区访问的名称，当然应该会得到该域不存在的响应，但是如果它们出现，那么让我们将它作为一个客观事实来考虑，因为现实情况就是如此。”然后我们就必须决定要怎么做，是否要禁止这些名称，还是采取一些其他的缓和措施，等等。

我的理解是，IETF 没有将很多注意力放在某一个政策上，事实上 — 我不是要告诉 IETF 做什么或者不做什么 — 但他们通常会避开政策问题。

所以我的理解是，还有部分成员说：“IETF 没有理由对你所说的域名抢注说三道四。他们只管去用这个名称好了。”它不太像占用私家车的情况。而更像是占用一块没有用过的土地，一块尚未分配或无主的土地，但是有人去使用它。

比如，.ONION 就是一个很好的例子。

在你看来所有这些部分如何配合？它们应该如何配合？

彼得 • 科赫： 好的，谢谢你纠正这个比喻。我们可以从这里说起。如果有人占用了这块土地 — 在这里请不要赋予“占用”过多的贬义 — 那么这时，它就不能再提供给其他任何人。而这就是需要协调的部分。但是在这里，责任应该是简洁明晰的。这不是说要忽略事实，忽略发生的流量，和世界上存在伪造 I.P. 地址一样，我们大家都看到了这个问题，但没有人会做出这里所说的这种反应。就像是说，哦，那么让大家宣布自己的地址，回来，然后就可以获得这个久居于此的地址，因为我们不想忽略事实。

这里的关键点在于，IETF 中的文件和 MOU 显然是矛盾的。而这个矛盾至少是，这两个机构之间没有协调。所有这些，因为有一个域名空间，所以这看起来像域名，走路的方式像域名，味道像域名，那么它很可能就是一个域名。所以这里的责任必须梳理清楚。但我并没看到这一点。

沃伦 • 库马里 (Warren Kumari)： 所以如果 — 抱歉。

戴维 • 康纳德： 下一个是沃伦，之后是琼尼 (Jonne)。

沃伦 • 库马里： 好的，我想插几句。为了提供完整的信息，我想告诉大家 IETF 实际上很长时间以来一直在讨论这个问题，而且最近还

采纳了一个关于特殊用途域名的问题声明。我们经历了 .ONION 的域名分配流程。大家似乎有一个共识，就是这个流程的进展不如预想的顺利，所以在特殊用途域名问题声明的采纳上开展了一个扩展流程。现在我们将尽力完成它，之后就有望进入到一系列解决方案的研究工作中。

吉姆所谈到的文件，SSAC 文件，的确讨论到了诸如需要协调的问题。估计 IETF 文件也将提到诸如此类的问题。所以这就是进展。

目前，IETF 不在处理任何其他特殊用途域名。在我们研究这个问题时，IESG 可能会暂停这个流程。所以有流程正在进行。

我不记得谁是下一个了。

戴维 • 康纳德： 琼尼。

琼尼 • 索尼能 (Jonne Soininen)： 好的，谢谢。看起来，可能最好要区分这些事情。我想史蒂夫做了一点尝试，而且我认为吉姆说得非常好 — 很有表现力，也就是说可以分为三类。直白地说，一类是根，一类是 IETF 中的特殊用途域名，还有一类是域名抢注。看起来，有些问题是其他地方漏掉的，私人用途可以是其中之一。

所以域名抢注，或者私人用途问题，当然不受任何人控制，就像史蒂夫所说的，IETF 没有对其施加任何控制。

关于特殊用途域名，也许不是每个人都知道，它们实际上不是在根中解决。这些不是 DNS 可以解析的域名。比如，.LOCAL 可以通过一个名为组播寻址 DNS 的系统解析，但它不在根本身内。

ONION 是沃伦说到的最近被分配的一个域名 — 多年来 IETF 分配的域名很少。我想有 .EXAMPLE、.TEST。

彼得 • 科赫： 基本上只有 —

琼尼 • 索尼能： .LOCALHOST。

抱歉。

彼得 • 科赫： 基本上只有 .LOCAL。

琼尼 • 索尼能： 还有 .ONION。彼得 • 科赫：其他的都是保留域名。

琼尼 • 索尼能： 在没有制定任何政策之前它们都会保留。

但是在保留的这些域名中，实际上没有一个是 DNS 本身可以解析的。正如它们的名称一样，它们是“特殊用途”。

正如你所知道的，彼得，关于如何实际分配特殊用途域名，IETF 实际上已经拥有一个流程或政策。那也是 .LOCAL 和 .ONION 被保留的依据。而且就像沃伦说的，人们发现这是不够的。现在，IETF 正在研究一个更好的政策。

关于协调，最初，当 IETF 开始研究关于特殊用途域名的政策时，IETF 实际上已经向 ICANN 董事会和 GNSO 发出了一份联络人声明。

我同意你的看法，协调很可能 — 并不完美。但是另一方面，在 ICANN 社群和 ICANN 组织内都有人实际参与到这项工作中。所以我认为实际上，至少有一些协调。但是，看看 SSAC 将要说的，极有可能是在他们的提案中 — 这极有可能需要改善。我可以同意这一点，它需要更多合作与协调。但是我看不到 — 我同意你的看法，那里极有可能存在问题。

但是我不理解你说的 — 除此之外你还试图拐弯抹角地指出还有其他问题，需要更多合作来确保我们负责任地做这项工作。

彼得 • 科赫： 我不想霸占麦克风或者出风头，但是你说这类名称进入了根，并且当然，它们之后再也不能进入根，对，就像 .ONION 或 .LOCAL 或者这些列表上的其他任何域名。但是这个具体的文件绝对不是局限在处理根一级的事务。有的人可能会提出一个所谓的协议元素，它可能会影响到任何现有 TLD 中的某个二级域名。之后可以宣告某个协议元素具有影响，使得某个域名再也不能在全球域名空间中解析。虽然这种情况还没有发生，但是如果它可能在根一级发生，那么就可能在每一个地方发生。

所以，这个域名空间的突出部分和宣告它们是协议问题不仅对根很重要，对 TLD 很重要，而且对其下的每一级都很重要。所以这里没有任何界限。所以我认为这是一个需要从政策面来看的政策问题，而不仅仅是作为技术问题来对待。

戴维 • 康纳德： 好的，请继续回应。

琼尼 • 索尼能： 我想我们同意这一点。而且我认为，这也是为什么 IETF 要研究它，以便基本上解决它的部分原因所在。你说得对，ICANN 和 IETF 需要就此进行对话。我同意。

戴维 • 康纳德： 沃伦。

沃伦 • 库马里： 对，我想琼尼说的基本上就是我要说的。IETF 正在研究这个问题，对吧？

彼得 • 科赫： IETF 实际上在回避这个问题，但是这一点让我们线下再讨论。

沃伦 • 库马里： 我们采纳了一份文件。IETF 也发送了一份联络人声明，其中说到 — 请注意在这个问题上我们应该协调。我在 TEG 小组中多次提到这个问题。IETF 正在研究它，对吧？我们已经采纳了一份文件。这就是进展。虽然它不像某些人期待的那么快，包括我自己，但是我想我们在推进。所以你的一些说法让我有点困惑。

彼得 • 科赫： 好的，谢谢。

琼尼 • 索尼能： 我要指出一点 — 抱歉，戴维。ICANN 社群也在研究这个问题。SSAC 显然正在研究。所以我认为相关工作正在进行。而且就像之前说的，还有改进的空间，但是至少我们已经开了个头。

戴维 • 康纳德： 罗恩。

罗恩 • 达席尔瓦 (Ron da Silva)：

谢谢。到目前为止这是一个良好的对话。但是我的理解是，你希望研究的不仅仅是 IETF 和 ICANN 之间的这个特定保留空间，而是要进一步扩大到域名空间以及存在其他冲突的领域。有些企业甚至更 — 一些消费设备供应商可能会将一些形式和性质都非常像 DNS 的元素注入到域名空间中。

而且，你知道 — 我想我听到的是，将会研究这个更为广阔的域名空间，而且这是一件好事。因为，你知道，你刚刚很快地谈到了寻址。它让我联想到这里存在的一个类似的挑战。有大量的传统空间 — 也就是先于注册管理机构存在的空间 — 历史上它们被分配给了不同的人。

在很多情况下，这些地址从未被路由过。今天它们不在全球互联网中使用。而且，你知道，有的人可能将它们用作内部用途，甚至可能会在公司内部创造一些域名来以静态方式映射到其中一些地址。

这是同样的问题，对吗？之后，从其中一个地址段被售出的那一刻起，就会产生冲突。全世界都遍布着繁荣的转让市场。它被出售给另一家企业或服务提供商使用。但当尝试路由时，会立刻失败。因为这个空间正在多个地方使用，它不会映射到全球互联网。

所以尽管有协调努力，但是你知道，也存在获得一个地址或域名空间时，需要运营商或注册管理机构和注册服务机构以及正

在使用这个域名空间的人之间通力合作的情况。在这些关系方面，通常会签订一些条款和协议。

所以我认为，当你有了这个组合，就没有 — 回到数字的类比，即使你获得一个地址段，也无法保证它们将被路由，除非你反过来与其他提供商通过同级协议做出了安排，或者购买了对它进行路由的服务。之后这就变成了其他某个人的问题，要确保它是全球唯一的，并以一种不与同类概念相冲突的方式在全球路由，因为有人抢注了它。这是一个完美适用的术语。所以域名和地址面临着相似的挑战。

戴维 • 康纳德： 接下来依次是卡韦赫和吉姆。

卡韦赫 • 兰杰巴尔 (Kaveh Ranjbar)： 我想，罗恩，我有一个更好的例子来将它和 I.P. 寻址进行类比。几年前，APNIC 被分配了 111/8，其中包括 1111 和 1.2.3.4。我想当时杰夫 • 休斯顿 (Geoff Huston) 写了一篇文章，因为他在任意给定时间都收到了大约 500 兆字节的流量，所以他们决定基本上保留这个空间。

所以我认为与比如说传统空间被劫持相比，这更接近于我们在根中所看到的情况。

吉姆 • 加尔文： 谢谢。还是吉姆 • 加尔文。

我想要界定一下范围，你知道，也就是 SSAC 将会说什么以及我们看待此事的方式。我的意思是，问题空间显然是一个很大的范围。IETF 明显是关心域名的另一家机构的示例。但是，我们看待我们建议的方式，以及我们要建议的是，考虑 ICANN 职权范围内的工作。

要提出“好，让我们来协调吧”这样的建议很容易，你知道，这个建议似乎再自然不过。但是很快你就会遇到一些有趣的问题，比如你要跟谁协调？为什么？我的意思是，IETF 是一个明显的例子。但是，再次说明，有很多人将域名用于自己的目的，他们称之为私人用途或者域名抢注 — 随便你喜欢怎么描述都行。

所以，显然，我不是说要自始至终同每一个人协调。你没法一概而论地解决这个问题。

所以，你知道，ICANN 确实需要考虑哪些部分是它可以控制的，以及对于它所控制的部分可以做些什么。所以存在一些问题，比如如果有其他人冒出来，他们也有一个正在使用的域名的列表，而这些域名也会造成冲突从而导致模棱两可，该怎么办？我是说，ICANN 关心的，ICANN 社群关心的，以及 ICANN 作为一个组织和 SSAC 作为其下的一个咨询委员会关心的是由这个事实所造成的不稳定性，即，有其他人在使用某种合理的技术，你知道，而且当然对他们来说也是一种理性的选择。

所以我们需要考虑 — ICANN 社群需要考虑它要如何回应此类其他用途和其他列表的存在和出现，它们将时不时地冒出来。它们将随着时间而变化。所有这些意味着什么？新的组织将会出现。你知道，他们都会有自己的工作流程。所以 ICANN 只是需要有一个流程来应对存在这些情况的事实。这是 SSAC 努力的方向，也是我们考虑要特别向社群和 ICANN 组织，当然，更直接的是向董事会建议的。谢谢。

戴维 • 康纳德： 你知道，既然 SSAC 正在考虑这个问题，我们可能最好是等待一下，看看 SSAC 对此的建议是什么，然后再评估 — 看看技术专家小组要不要在 SSAC 建议的基础上提供一些意见。

另外我要指出的唯一一点就是，我相信 RFC 2860，也就是 IETF 和 ICANN 签订的 MOU，确实说明了 IETF 可以宣布协议。但是除此之外的事项属于政策问题，不是在 MOU 的语境下解决，这就暗示着它不属于 IETF 的工作范畴，因而是 ICANN 的工作。那不一定表示它是 ICANN 的，这确实额外增添了这个特殊话题的复杂性。

接下来，我们进入下一个议题，我忘了具体是什么了。请重新把议程放上来。

好的。对，我想是霍华德。对，是这里。对。那么霍华德，请你来谈谈 ETSI 网络功能虚拟化。

霍华德 • 本
(Howard Benn)：

谢谢。我们的幻灯片可以播放了吗？请放下一张。

好的。

那么 ETSI，你们有些人可能知道，是管理移动社群标准的标准组织。他们实际上在移动世界中也为所有固定电信编写标准，但是以移动标准最为著名，因为过去几年来移动领域一直是最为活跃的领域。

现在，过去十年间，我们已经逐渐从一个用手机打电话的世界，过渡到一个更多人通过手机而不是其他任何媒介访问互联网的世界。所以在我们所处的阶段中，有 80 亿用户 — 全球有 80 亿注册电话卡，SIM 卡，以及约 60 亿用户，我们看到海量的互联网连接。

在移动运营商的核心网络内，对于以下问题一直有着大量的讨论，那就是，我们能否利用互联网行业多年来已经完成的工作 — 用过的数据中心 — 来控制我们的通信，而不是利用我们迄今所拥有的专利硬件和专利软件。

所以在 ETSI NFV 小组内，过去几年来他们一直在做这项工作。他们造就了规范的两个阶段。目前他们正在研究第三个阶段。有一些问题冒出来，我认为在这里就这些问题给社群提供一些讯息会很有用。也许我会在最后谈一谈寻址。

所以从本质上说，我们与同样在这个领域内工作多个组织像 IETF 密切合作，共享今天数据中心内可用的计算、存储和网络设施。

下一张幻灯片。

有一些词语会用到，我不知道有多少人熟悉这些词 — 我自己花了一点时间来把它们搞懂。我们所拥有的是实体经理，简称 EM，他们管理着这些虚拟网络功能。这些基本上就是软件的组成部分，运行着关于软件、通过软件和软件内的执行功能，可能今天还运行着硬件中的执行功能。我们共享资源。所有这些的管理，都是通过一个名为业务流程的东西来实现。我们有管理生命周期的 VNF 经理。这些东西可以提出、扩展、签约并带走。

下一张幻灯片。

我们一直在做的工作，基本上就是尽力映射互联网社群多年来所做的出色工作，看看这些工作如何映射到移动世界中所用的模型上。在这些讨论期间，有几个问题凸显出来。

下一张幻灯片。

第一个是可靠性。在对可靠性的认知方面比较有趣。我认为我们目前所处的阶段就是，我们仍在尽力了解人们愿意忍受什么。如果手机因为信号问题而无法使用，人们显然就会抱怨。但是他们愿意忍受它。

如果手机有信号，但电话却打不通，这种情况现在肯定是不可容忍的，特别是考虑到今天用手机拨打的应急电话数量。

然而，基于互联网的服务，我想尽管用户希望拥有真正的高可靠性，但他们也愿意忍受一些可能不是 100% 可靠的事物。

我不知道这些数字确切来自哪里。我拿到了这些数字。但是大部分移动网络，一年内会中断几分钟，而不是几小时。所以我们可以看到，这里提供的一些数据或许表明，当前的互联网社群不是那么可靠。再次说明，我无法验证这些数据的真伪。请放下一张幻灯片。

我们也需要确保这些系统之间的互用性，这其实就是标准世界的出发点，确保我们有一些协议，能够让不同的供应商提供这个基础架构的不同部分，同时大家又都以一种可靠、无缝衔接的方式协同工作。

下一张。

我们 ETSI 一直在做并携手 GSM 协会一起在做的工作之一，就是开始研究如何着手确立其中一些系统的基准。我们如何解决像可靠性这样的问题。还有像延迟这样的问题。如果你提供一种基于语音并加密的服务，那么延迟问题就至关重要。只有将延迟降到极低的水平才能获得良好的语音质量，所以我们需要着手确立这些服务的基准。下一张幻灯片。

安全性是一个真正的大问题。人们非常担忧一个问题 — 如果你从一个移动运营商处转移到另一处，前者将所有信息都锁在自己的数据中心内，外界无法访问，而后者将你放到一个可能有其他公开可寻址的系统运行的数据中心内，这就可能会给网络攻击、拒绝服务攻击，以及今天互联网上出现的各种各样的问题提供可趁之机。运营商真的担忧这种情况发生。所以 ETSI NFV 小组下设了一个安全性小组，专门研究这一问题并努力提出一些解决方案。但是，当然，在这个问题上我们必须和互联网行业合作。下一张幻灯片。

接下来，另外一个有趣的领域就是，在今天的语音通信世界里，我们有一些像合法拦截这样的手段，这是我们运营所在的大部分国家的一项要求。现在它也开始渗透到互联网社群，所以也许我们可以分享一些这方面的经验。在 ETSI 内部，我们有一个 TC 网络小组，专门研究所有网络安全问题，包括合法拦截，以及如何在提供它们的同时维护终端用户的隐私和系统的安全性。下一张幻灯片。

迁移显然是另一个有趣的领域。在我们所处的系统中，今天的运营商其实都希望在他们进行网络升级时，无论如何都不要中断服务。我们正回过头来和开源社群开展更紧密的合作，他们还不习惯接受如此严苛的要求。所以目前我们正和 OpenStack 开发团队开展非常紧密地合作，努力解决这方面的一些问题。下一张幻灯片。

接下来是和安全性有关的整合。我想，在互联网环境下我们看到，虚拟化已经进行了相当长的一段时间，所以今天有许多提供互联网服务的服务。透过这些服务，你可以从一个应用程序让用户离开另一个应用程序，你可以分隔记忆和存储，你也可以使两个应用程序永远无法并存。我们只需要确保那真正得到加强，并且我们可以保障安全性。你可以想象，如果有人可以进入移动运营商的网络，将会发生什么。所以今天，我知道有的人在上周抵达时，在印度遇到了一些移动漫游上的问题。但是在围绕漫游的问题当中有一个问题是，你可以在世界上任何地方拨打任意电话，任意电话号码，并且或多或少地都能够联系到任何人，不管他们在哪里。所以从网络安全的角度来看，这显然是一个很大的隐患。如果有人可以进入那个网络，就能够在非常短的时间内造成极大的破坏。下一张幻灯片。

在标准方面，我们继续在 ETSI NFV 小组内制定各项标准。我们与 GSMA 开展了非常紧密的合作。GSMA 是一个组织，所有移动运营商都是该组织的成员，所有漫游协议都是在这里纳入。在这里处理着大量关于安全性和用户管理的问题，之后由 ETSI 编写关于诸多事项的标准，例如 NFV、网络安全以及各种各样不同的领域。下一张幻灯片。

我想这是我要讲的最后一张幻灯片了。包里还有一些幻灯片，感兴趣的人可以看一下。先快速介绍一下 NFV 安全工作组。再次提醒，任何想要加入这个工作组的人，你看不到它，因为它

是一个 ETSI ISG。所以任何人都可以加入。你只需要填写一张小小的表格。但是你可以 — 基本上任何人都可以加入这个小组。

我们一直在努力去做的事情之一，就是召集来自互联网领域和来自移动通信领域的安全专家，然后让他们来制定一整套标准。所以就是让那些在像 OpenStack 和开源社群这样的组织中的人员直接来研究移动安全处理的方式问题。我们正从 SIM 卡的使用中转移。有一系列的工作正在进行，所以你可以拥有可下载的凭据用于身份验证，以便进入到一个安全的环境中。因此我们要确保我们可以在移动安全领域借鉴今天的最佳做法。那就是身份验证。我们知道访问移动网络的每一个人，我们知道订阅细节。我们不必知道他们是谁。我想这一点和互联网世界非常不同，在互联网世界里有着非常开放的连接。所以，看看我们能否齐心协力带动这些 — 所以我们可以推动一个更加安全的互联网向前发展。谢谢。

戴维 • 康纳德： 谢谢，霍华德。好的。下面我把发言的机会交给董事会成员或观众席中的成员，现在可以向霍华德提问了。好的，国维。

吴国维 (Kuo-Wei Wu)： 我想提供一个关于我们未来面临的真正的安全性问题的意见。我想和你们当中的一些人分享一点看法。随着物联网和家居设备的普及，我们必须记住这些是家居设备和物联网设备，它们的价格正变得越来越便宜。而且老实说，我看到制造业，看到

他们是如何打造家居设备和物联网的。他们在软件上不花一分钱。而只是到网上获取免费软件。所以不难预见，这些家居设备和物联网一定是安全问题的来源。特别是我要说，在一些国家，如果你购买 PC 或 Mac 硬件，他们会免费赠送任何类型的软件，包括病毒。所以我想在座的各位，你们一定知道只要花很少的钱购买零部件，就可以发起 DDoS 攻击。

所以我认为，如果我们真的要考虑如何解决安全问题，就必须想方设法让制造业步入正确的轨道，从而维持整个互联网的稳定性和安全性。以上是我对这个问题的个人意见。

戴维 • 康纳德： 好的，霍华德。

霍华德 • 本： 这是一个有趣的观点，因为 ETSI 数年来特别研究了 IoT 设备的安全标准。要确保所有制造商都遵守提供的指导非常困难。我认为这是我们所有人将来都会面对的一个真正重大的问题。而且 ETSI 有一个小组名为 NGP，在之前的 TEG 会议中我曾谈到过。他们所研究的一个方面就是，如果我们今天从头开始，互联网将会是什么样子。这项工作得出的结论之一就是，你必须与互联网联合。所以你不能只是随机拥有设备，而不进行某种联合。因此，引起问题的设备可以通过一种非常安全的方式分离出来。我认为我们必须勇敢面对的一个问题是，我们必须在隐私和安全之间划一条界限，并尽力阻止其中一些攻击，而这

正变得越来越困难。最后一个实际上是关于动态 DNS 的，不是吗？这是最初引发问题的根源。所以也许那是另一个问题，我们需要改天探讨。

吴国维： 请问我可以回应一下吗？

戴维 • 康纳德： 可以。

吴国维： 实际上，之前当 DYN 受到攻击时，你知道，你的朋友约翰 • 克莱辛 (John Klensin) 给我写了一封电子邮件。很多年前，当 IETF 在台北开会时，实际上约翰 • 克莱辛非常努力地想要让制造业人士与 IT 人士建立联系。但是非常可惜，这没有发生。因为我必须要说，很多家居设备，你知道，都是在中国台湾制造与组装 — 在中国大陆制造，但是（听不清）中国台湾人。所以实际上约翰提出了一个想法说，可不可以在 IETF 和制造业人士之间建立一个联系或沟通的渠道。以上就是我的意见。

未知说话者： 我要讲讲第二部分，因为第一部分更多的是物联网问题。也许我们可以处理 — ETSI 正在做的工作，我们可以在哥本哈根做这件事。我只想说说这个影响人们参加 IETF 会议的简单形式。我的公司，也就是 World Wide Technologies，我们让很多人参与进来，而且我很乐意为参与 IETF 活动制定预算，我可以说制造

商或供应商的意见也被带到了那里。但我是以个人名义带来这些意见的，而不是以公司名义，因为 IETF 的贡献感觉大都是由个人正式推动做出的。谢谢。

戴维 • 康纳德： 琼尼，你要评论一下吗？

琼尼 • 索尼能： 我要说的不一定是这个问题，更多的是关于 NFV。不过我们可以先看看杰要说些什么。

杰 • 戴利 (Jay Daley)： 谢谢。杰 • 戴利。真的感谢你，霍华德。这是一个很棒的演讲。我只有一个小问题。你可以谈谈 ETSI 在知识产权方面的工作情况吗？

霍华德 • 本： 当然可以。ETSI IPR 政策是以 FRAND 为基础，也就是“公平、合理、无歧视”地授予许可。关于 ETSI 如何与开源社群互动，我们进行了非常多的讨论，因为很多开源项目都有一个免费 IPR 政策。所以这些讨论仍在继续。我想有一点很明显，那就是开源社群和 ETSI 和 3GPP 社群正在开展更紧密的合作，并且有越来越多的项目正在取得成效。

杰 • 戴利： 好的。还有一个问题。你谈到了 OpenStack 的工作，这让我有点儿惊讶。因为比如在我的国家，有许多政府服务现在都是以 OpenStack 作为底层基础，包括比如说选举事项。所以对它的信任度显然很高。现在，我非常了解电信业人士有时对它有更高的要求，但 ETSI 是不是在贡献代码，还是 ETSI 试图 — 不是。好的。

霍华德 • 本： 就开源 — 就 OpenStack 来说，不是。ETSI NFV 小组只是将他们看到的问题告知 OpenStack 社群，贡献代码的显然是个人，但是 OpenStack 仍然有相同的 IPR 政策，而且我确定该政策将会延续。

目前真正在讨论的唯一一个项目就是 Open MANO，一些相关的工作实际上 — ETSI 希望直接对它做出贡献。我想这是目前在 ETSI 董事会一级引起最多讨论的事项。

戴维 • 康纳德： 琼尼。

琼尼 • 索尼能： 好的，我想补充一点。我想霍华德想要说的是，ETSI 所做的工作就是编制规范。其中有些规范旨在为比如说 OpenStack 或 OPNFV 提供指导。OPNFV 意为 NFV 的开放平台，它是一个组

织，它的工作基本上就是为 NFV 搭建框架，并为一些选择性项目比如 OpenStack 做出贡献。

贡献 — 当我不在的时候我所效力的公司如何运作，霍华德和弗朗西斯科 (Francisco) 的公司又是如何运作，基本上就是，我们直接对 OpenStack 或 Open NFV 做出贡献，而且通常是运用在 ETSI 中在同业间已经达成一致的大量指导性意见。ETSI 本身不 — ETSI 是一个标准组织，它的贡献是由成员推动做出的。所以 ETSI 本身并不做出贡献。

霍华德提到了，有一个名为开源 MANO 的小组，所以开源管理和业务流程实际上是 ETSI 内的一个开源项目。也就是 ETSI 运作的一个事物。它们有点儿像是一个完整的行业。这个开源项目也不是由 ETSI 自身启动的，而是由 ETSI 成员在 ETSI 语境下启动的。希望这样讲对你有帮助。

关于霍华德的介绍，我真正想要强调的一点是关于 NFV 的故事，也就是网络功能虚拟化。现在，电信业正在经历巨大的转变，一些已经在所谓的 IT 世界使用过一段时间的技术，像 OpenStack、云和虚拟化，在电信世界中也开始采用。从专业硬件和专业网元转换到更多地以数据中心驱动的通用硬件和软件架构 — 这些软件有很多开源组件，但也可能是专利软件 — 这基本上创建一个虚拟化平台。在这个平台上，离散网元基本上要么是作为虚拟机运行，要么是作为软件运行。

未知说话者： K.S.拉朱 (K.S. RAJU)：关于第二个问题，我想问你另一件事。有很多电信和有线运营商，他们应用的是翻新后的未知路由器。我在印度看到的情况是，很多宽带运营商、有线电视运营商公司，他们使用一系列盒子来提供互联网和所有服务。他们使用的是翻新后的设备。

所以还有一件事真正影响到本地区的网络安全问题。

那就是，最大的电子产品回收（听不清）是印度和亚太地区。好吗？谢谢。

戴维 • 康纳德： 关于 NFV 还有其他问题吗？好的。那么我们就继续。抱歉，线上有一个。可以。

远程发言： 谢谢戴维。这个问题来自丹麦奥胡斯大学 (University of Aarhus) 的沃尔夫冈 • 科纳沃茨特 (Wolfgang Kleinwachter)。他说，汽车制造商必须遵守国际认可的安全标准。为什么硬件和软件制造商不可以呢？

戴维 • 康纳德： 那是一个有趣的话题。我想，像 ETSI 这样的组织可以提出一些条件和标准，作为制定此类法规的基础。但是我不认为 — 我是说，霍华德，你要谈谈吗？

霍华德 • 本： 这是个危险的主题。我想，这确实是一个有趣的问题。

一个设备是否要先证明符合一系列标准，然后你才能将它连接到互联网？我们这里讨论的是这个问题。就目前而言，不用。

戴维 • 康纳德： 对。确实如此。虽然，考虑到拒绝服务的方式是 — 能力在提升，未来那可能最终是我们的选择。

好的，史蒂夫。

史蒂夫 • 克罗克： 我想了解一下沃尔夫冈的具体主张。

需要符合的现有国际标准是什么？我不知道他确切是指哪方面。

戴维 • 康纳德： 我想他指的是汽车标准方面。如果你的车要上路，它就必须遵守某些规定。

史蒂夫 • 克罗克： 啊。我漏掉了这个。

汽车比互联网要先进得多。抱歉。汽车是一个互联网设备，不是吗？

戴维 • 康纳德： 的确，它正在朝这个方向发展。约翰？

约翰 • 莱文： 汽车有着根本的不同。因为在大多数国家，你需要从政府获得许可证才能在公共道路上行驶，我们最好不要让互联网走到这一步。

戴维 • 康纳德： 那样绝对是最好的。

可以。霍华德？

霍华德 • 本： 好的。要将任何电子产品投放欧洲市场，你需要一个 CE 标志。CE 标志基本上表明你遵守了所有必须遵守的标准。所以每一部手机都必须证明合规。

但是目前，没有哪个合规性文件与你上网的方式有关。

戴维 • 康纳德： 对。我想我们现在可以继续了。

[笑声]

戴维 • 康纳德： 下一个话题是 DNSEXTLANG，主讲人是约翰 • 莱文。

约翰 • 莱文： 谢谢戴维。我很高兴看到，根据议程我很可能会来到这里。我推测那说明你们确定了我的事情，但不能确定我的位置。

所以，这是一类非常不一样的运营问题。

请换到下一张幻灯片。

DNS 数据由记录组成，这些记录有各种各样的类型，已经定义类型的有 70 到 80 种，其中常用的大概有 4 种。

长期以来一直有一个问题，我们为什么没有新的记录类型。因为当我们发明新服务或通过互联网分发新数据类型时，常常需要将它们与不同的记录类型协调。

我是说，比如，保罗•胡特斯 (Paul Wouters) 在 DANE 中一直很活跃，DANE 定义了新的记录类型，以便公布 SSL 证书和诸如此类的事项。

所以它很难的原因是，请看我的幻灯片，我们要通过这个四步的过程来获取你的记录，你知道，也就是从你的大脑到互联网上的过程。第一部分是你得通过某种方式将 DNS 记录放到一个定义上网数据的主文件中。以前，人们是用文本编辑器手动编辑文件，但是现在，你会去找你的注册服务机构或 DNS 提供商，他们拥有某种基于 Web 的东西，可以让你输入一定数量的 DNS 数据。而这个基于 Web 的东西往往很差劲，这就是为什么我们称之为低质量免费软件的原因。

然后，低质量免费软件以某种方式创建自己的文件，传递到 DNS 服务器上 — 主服务器是 — 那是像 BIND、NSD 和 PowerDNS 这样的软件。

然后它再将记录放到公共互联网上。之后如果某个应用程序要使用它，从底部往上，这些应用程序有一些 DNS 库，能让你索取记录，然后这些记录上升到 DNS 缓存，之后就从主文件中检索数据。这就是 DNS 很长一段时间以来的工作方式。

请翻到下一张幻灯片。

现在，当你定义一个新记录类型时，会发生如下情况。

首先，IETF 会公布一个定义记录类型的 RFC，而实施和公布往往会有一定重叠，好吧？

所以你要做的第一件事就是，你要更新库，以便了解新的记录类型。也就是说，不管谁维护库，都必须添加新的记录类型，调试它，提出新的分发，对外进行分发，然后每一个使用库的人都必须更新他们的软件，他们可能会也可能不会这么做。

幸运的是，缓存不需要更新，所以我们不会再谈到它们。

主软件也需要更新，以便理解新的记录类型。那不会成为一个很大的问题，因为更新 DNS 服务器的人很警觉，往往很快就会更新它们。但是再次说明，一旦他们提出了新版本，就要分发新版本，不管是 BIND、NSD 还是其他，人们可能会也可能不会安装新版本。而低质量免费软件永远不会更新。

所以通常，如果你有某个基于 Web 的 DNS 控制台，你知道，那么现在你就可以使用十年前就能使用的四种记录类型。

请放下一张幻灯片。

这里是我们的目标，也就是，当新的记录类型被定义时，我们要让这三个软件自动更新，这样它们就可以马上处理记录类型。

请放下一张。

好的。也就是说，主服务器和库软件，必须理解新记录的句法。它将会有新 RR 类型的名称，以及一堆字段。

它必须理解二进制形式，而且必须能够将文本形式转换成二进制形式，反之亦然。

主软件和库软件必须能够做到这一点。

如果你真的希望人们能找到这些东西，由于它是基于 Web 的，那么你就需要有某种方式，使它能够提示人们注意必要的字段和句法等等。

请放下一张幻灯片。

这里有一个办法。我们提出了一种可以描述记录类型的语言。起初，我说过我们会将它们放到文本文件中。保罗 • 维克西 (Paul Vixie) 提出了一个绝妙的办法，实际上就是在 DNS 本身当中公布描述。这样当你提出一个新的 RR 类型时，就会在

DNS 中公布，然后系统就可以自动找到它们。稍后我会多做一点说明。

完成这些后，你就需要将你的软件升级一次，以便处理扩展语言。完成这一步后，新记录类型就会自动进来。

请放下一张。

这里是对一些记录类型的描述。第一个是邮件交换器，这是一个大家都很熟悉的记录类型，你可以看到它是一个 MX 记录。我们将它描述成邮件交换器，它有一些记录。接下来文本文件也有一些字段，所以这个文本文件也有 — 是一个带有一些字段的记录。

请放下一张。

所以在每个描述中，第一行是 — 比如，这里是一个 SRV 记录，是相对复杂的一个。

所以它表示名称是 SRV。类型编号是 33。“I”的意思是 — DNS 记录有多个类别。这只对互联网类别有益。

之后服务器选择是一条备注，它旨在用于 — 提示用户。

之后第一个字段是优先级，第二个是权重，第三个是端口。每个字段都是双字节的整数。之后有一个域名，也就是目标。

我已经以这种格式，提出了几乎全部现有记录类型的描述。

请放下一张。

最终，为了处理将近每一种记录类型，我提出了 14 种类型。有三种大小的整数，有文本字符串，有域名，有 v4 和 v6 地址，还有所有其他类型。有时间戳，有 32 位和 64 位哈希。有任意的十六进制字段。有 Base64，还有一些其他类型。

之后我还提出了一个转义类型，名为“Z”，它针对的是一个特殊类型，这一类型不能合理地以任何其他方式描述。“Z”类型不是很多，而且它们不适用于广泛使用的记录，所以它其实不是一个很大的问题。

请放下一张。

在 DNS 类型的描述中有多个选项，这里显示了我放入的选项类型，总共有三个。

这里是一个对在 DNSSEC 中使用的 NSEC3 记录的描述。第一个字段，哈希算法，你可以将它定义为一个数字，或者也可以放到一个助记码中。

所以在这里它是说 — 事实上，最初定义的唯一一个算法就是 SHA-1，所以这是说：“如果用户输入 SHA-1，那就表示 1。”在第二个带有标记的字段中，只有一个选择退出标记。事实上，你可以拥有多个字段，多个值，用逗号分隔。有的字段有多种类型。对于加密盐，第四个字段，正好是一个十六进制字

段，用一个计数存储在记录中，所以“C”就表示用一个计数来存储它。

之后有一个 32 位哈希。

接着最后一个字段是类型，有一些记录有 — 这些是记录类型。在本例中，在这个特殊名称存储的是记录类型。

对于 NSEC 和 NSEC3，实际上有一个囊括了所有类型的列表。

所以“L”就表示这是一个类型列表，而不只是单一类型。我不会 — 我是说，你可以看看我的草案，了解有关的细节。但是我在这里试图向你们展示的是一些其实不是很复杂的字段选项，你们可以查看定义它的 RFC，了解有哪些记录类型，并且在几分钟内写一条像这样的描述。

请放下一张。

现在，要更新 —

实际上，请翻回到上一张幻灯片。谢谢。

这个描述给了你们足够的信息，足以让库和主服务器能够分析和逆分析记录。我的意思是，因为它是记录类型而且在本例中是指 1 位 — 一个单字节整数，另一个单字节整数，一个双字节整数，一个计数的十六进制字段，一个 Base32 字段和一个类型列表。有了这个描述，就足以让应用程序软件 — 稍后我会说明 — 可以分析主文件和逆分析二进制。

请继续，再翻到下一张。

现在，对于用户，那是放进备注的位置。

如果我们有一位用户要定义 MX 记录，方法就是你将点击“新记录”，然后它将提示“什么类型：MX”，接着将显示一个小小的表格，就像我在屏幕下方这里所模拟的一样。

它从描述中取出优先级和主机名，然后用户输入了 100 和服务器名称。

输入后，它知道优先级字段中的值必须是符合 16 位的整数，而且主机名的值必须是域名。

所以，也就是说，用户必须对他/她要做什么有所了解。但是通过这种方式，它可以强烈地提示你，因此你得到的东西至少在句法上是正确的。

请放下一张。

所以最后一点是从 DNS 获取数据。保罗的想法是，将记录描述公布在 DNS 中固定的地方。他提议如果你要按数字查找，就到 RRTYPE.ARPA，如果你要按名称查找，就到 RRNAME.ARPA。

所以这里我们有一个假设的 foo 记录，是 999 类型，所以描述位于 999.RRTYPE.ARPA 以及 FOO.RRNAME.ARPA，然后实际描述就作为普通文本记录存储在 DNS 中。它表示 RRTYPE 等于 1，这样你就知道这其实是一个 RR 类型。EN 表示备注为英语。如

果你要国际化，你可以有不同的版本，用你的本地语言撰写不同版本的提示。

接下来，这些字符串是我之前向你们展示过的，记录名称的描述和各个记录类型。

所以其实很容易写软件将它从文本文件中分析出来，并转化为区域文件进行公布。一旦完成了这一项，那么当我们定义新记录类型时，疯狂地挥舞双手，我们安排 — 一旦 RFC 公布，描述放到 DNS 中，那么任何使用这个东西的软件都能够查找它。

请放下一张。

好的。这不是灵丹妙药，并非对你要定义的每一种可能的新 RR 类型都适用，原因有二。一个就是，有些 RR 类型就是有着难以定义的奇怪句法。特别是有一些类型，主字段中的字段顺序和二进制记录中的字段顺序不匹配。所以你知道，如果你真的需要这么做，你可以编写代码来解释我的特殊“Z”记录类型之一。但是一般来说，所有这些类型都已经由服务器处理，而且它们好像不是用户想要放入实际区域文件中的类型。它们通常已经淘汰，像 NSEC 的前身 SEC。

另一个原因是，有一些新 RR 类型实际上需要服务器特殊处理。我的意思是，当我们定义最新的 DNSSEC 版本时，当你的缓存执行了一次 DNSSEC 查找，并找到了 NSEC 记录和签名记录和材料，那么它就必须处理它们。

所以虽然我可以描述记录的句法，但却不能告诉缓存要如何处理它。但是重申一点，这种情况不经常发生。我的意思是，我们只需要发明 DNSSEC 一次，像这样需要语义变化的新记录类型可能十年才出现一次，所以对此我并不担心。这肯定是一个符合 90/10 法则的解决方案，所以...

请翻到下一张幻灯片。

所以在发明了这个之后，我就开始实施它。戴维 • 康纳德非常友好地做了一些安排，以便我能够获得一定的实施支持。规范的草案已经完成。我修改了 Perl DNS 库，以便它可以从文件中读取记录类型，可以从 DNS 中读取记录类型。当它看到一个记录类型带有未知类型名称，或者一个二进制记录带有未知类型编号时，实际上它可以自动即时地向外在 DNS 中查找，找到这个类型，将它提取进来，编译成新的 Perl 代码，即时安装它，然后处理这个记录类型。它实际上非常灵活。现在，我要告诉 DNS 的维护者们如何最好地将它集成到对库的标准分发中。我正在皮东进行概念验证，以展示 Web 事务的工作方式。这些全部都将免费发放，作为开源软件。

所以在这里就是希望，一旦我们完成这件工作，添加新记录类型将变得更加简单，人们将更愿意做这件事。

我的意思是，你知道，我们定义的新记录类型非常少，就是因为存在这样一个认知：你可以定义新记录类型，但没有人会用它。因为，你知道，因为预配软件不能处理它，而且有一些不

愉快的工作方法。特别是，有许多新服务实际上是通过重复利用文本记录来进行，这些记录在某些情况下工作良好，但在大多数情况下被发现具有负面的影响。

所以这大致上是有用的。我很乐意将软件分发给任何感兴趣的人，而且我希望人们使用它。史蒂夫。

史蒂夫 • 克罗克： 谢谢。太酷了。在解决 DNSSEC 部署以及有新资源记录类型，但不确定人们何时会接受它们等等的问题，以及关于是否需要其他事物、是否要使用文本记录或者某种类型的其他资源记录等一系列尚未解决的开放问题的过程中，我完全理解并领会到问题所在。

我记录了一系列问题，其中一个就是原型，你说你正在研究它。那很好。

展望不久的将来，有两类问题在一定程度上关系到成败。

我可以想象一个新的记录类型被定义，并且它的大量使用填充到 DNS 当中，所以忽然之间，全世界的解析器都面对着这个新记录类型，而且必须进入这个“先提取，然后重新配置”的循环中。那可能会导致两个瓶颈。一个是，每个人都同时从同一个地方提取，可以预见，那可能会造成崩溃。所以，简单地将它放到 .ARPA 下，致使其将承受巨大负载，可能是目光短浅的。

另一个瓶颈是，一个正在工作的承受着巨大负载的解析器需要花多长时间才能吸收、重新配置并对此做出响应？它有时间吗？我的意思是，对于高频解析器来说，要做这些事相对来说具有压力。所以那是一系列的问题。

另外，我能清楚地看到这项工作的动机是解决昨天的问题。我们是否了解到任何关于新记录类型可能会被用到的新情况，以及它的使用频率如何？

约翰 • 莱文： 对于第一个关于性能的问题，我一无所知。你知道，在众多因素中它其实取决于缓存策略。你知道，如果我有一个繁忙的服务器并且有一个共享库，那么共享库能否提取记录类型并编译它，以便在系统的每一个进程中使用，或者每一种进程是否都会启动并且必须重新执行，这些问题都会有很大的不同。但是我认为那属于实施质量细节。

就实际记录类型而言，我是说，现在出现了一些新的记录类型，比如 SMIMEA，它是新的，而且很容易描述。有人说过：“如果新记录类型使用的字段像我们以前用过的字段一样，那就没问题。”通过制作一个囊括了所有人尝试定义过的每一个记录类型的清单，我发现近年来人们大体上重复使用了字段类型。没有 — 我是说，对于 EUA48 和 EUA64，有一个新的类型来放置 Mac 地址。但那是几年前的事了，从那以后基本上一直没

有新的字段类型。所以我认为对于我看到的记录类型，看起来运行得还不错。

这也是一个鸡生蛋还是蛋生鸡的问题。如果人们知道使用一个易于描述的字段类型，记录就更容易得到实施，那么人们可能会更倾向于这么做。

戴维 • 康纳德： 杰。

保罗•胡特斯： 对于这个问题我想说一下。我认为在问题和回答之间存在一点儿误解。解析器实际上不用做任何新的工作，因为它们只做线路格式的 DNS，所以它们会获得新的 R 类型和一个编号。它们只要查找编号，并给出二进制数据作为应答。所以在常规 DNS 查询下，没有额外的工作要做。

唯一一个额外的工作就是，当有人要将这个新记录类型添加到他们所拥有的 DNS 区时，必须通过预配软件来进行。所以这不会给服务器带来任何类型的实际负载。

约翰 • 莱文： 事实上不是这样，因为应用程序通常需要分析记录，以便能够实际上从中提取有用的部分。我是说，虽然这种情况不太可能发生，但是如果我要写一个使用 SMIMEA 的应用程序，那么我

的应用程序就需要知道，比如，这里是哈希，这里是类型，这里是数据。所以应用程序需要知道字段是什么。但是再次说明，这类数据应该是我们能够一次性编译的。

保罗•胡特斯： 好的。那么如果你要那么做，那实际上真的很恐怖。因为那样的话你就要将一个词连结到 DNS，而那实际上是 DNS 的一部分。所以那样实际上真的很恐怖。

约翰 • 莱文： 对，但是...

[笑声]

戴维 • 康纳德： 杰。

杰 • 戴利： 谢谢。杰 • 戴利。

很好，约翰。我知道曾经有人尝试过某种非常类似于 DNS 方案的东西，并且研究出了一种很好的方式来描述 DNS 方案中的 DNS，以及所有不同类型字段和事物的所有分类。DNS 方案提供了一些相关的深入信息，但是无论如何，它没有了下文。关于这个问题我要说几点。

首先，你如何对这里在二进制数据中所表达的信息呈现给终端用户的方式进行国际化？

约翰 • 莱文： 我正在考虑。个别记录不会 — 唯一一个可能需要国际化的，就是将要呈现给用户的字符串字段。

杰 • 戴利： 我指的就是这个，对。

约翰 • 莱文： 对，我是说，除此之外，像 — 你知道 — I.P. 地址不需要国际化。这是一个很好的问题。这个话题还没有人真正考虑过。文本记录中的字符串是八位，很简洁。你可以在那里存储 Unicode。你也可以在那里存储 UTF-8，如果你愿意的话。但是据我所知，没有人这么做。

所以我认为答案就是，如果在 IETF 一级我们确定要在 DNS 中存储非 ASCII 文本数据，那么不管我们决定做什么，我都需要解决如何描述的问题。

杰 • 戴利： 对。不过，我的意思是，虽然，目前那些 — 名称实际上不会以任何方式出现在 DNS 中。因此，如果有人向其他人呈现它们，他们将从其他地方获取它们，或者对使用哪种语言做出一个选

择。如果它进入到 DNS 内部，那么对于其中每一项你都需要另一个语言版本。突然之间，你就不得不对你所提供的数据层面增加另外一个维度。

约翰 • 莱文： 哦，实际上 — 幻灯片不在了。但是实际上在 DNS 版本中，在记录中有一个语言标记。

杰 • 戴利： 不不不。但是有很多信息都用它来编码。

我要说的另一点是，这里有一个 EPP 的类比，在 EPP 中出现的情况应该考虑到。EPP 有一个 — 它的核心是一个非常固定和明确的数据模型。

再次说明，我知道有人曾经提出了一个很好的点子，建议 EPP 应当有一个机制，描述应该提供给它的数据，而不是实际上包括数据。因为当不同注册管理机构的人向其中添加新数据时，例如公司编号或诸如此类的信息，必须经历一个扩展。

约翰 • 莱文： 对。

杰 • 戴利： 如果添加的话。但是如果 EPP 处于另一个层面，更具描述性，那么包含一个这些标准化字段的列表 —

约翰 • 莱文： 对。

杰 • 戴利： — 那样将会更好。我只是建议这两个东西实际上可能有利于整合。因为新记录可能也需要一段时间在 EPP 内编码，以便于在各方之间传输，所以这里存在一定联系。

约翰 • 莱文：当然。 这个概念听起来有些类似，虽然我不确定在实施中存在多少共同点。

戴维 • 康纳德： 韦斯

韦斯 • 哈达克 (Wes Hardaker)： 谢谢。韦斯 • 哈达克，USC/ISI。我有几点意见。这是一个好办法。我喜欢。我有几个请求。首先，不要将国际化格式放到记录本身当中，因为它们数量庞大。为什么不把它放到一个标签里，这样当我要查询英语时，就只会获得一次响应，而不是一个超大型的数据包。

约翰 • 莱文： 我考虑过这一点。问题有两个。一是：如何处理缺省值？你可以用星号，但那样会很难看而且不简洁。

韦斯 • 哈达克： 我（听不清）星号，但是 —

约翰 • 莱文： 对。除此之外，如果你真的想要做好，双字母语言代码是一个例子。但是事实上，英语是一种语言，它关联到许多国家。这类事项在真实数据库中将会很琐碎，并且在 DNS 中是令人绝望的。

韦斯 • 哈达克： 但是为容纳所有这些信息而给你返回一个巨大的数据包也很令人绝望。

约翰 • 莱文： 对，我知道。

韦斯 • 哈达克： 考虑一下。

约翰 • 莱文： 不。事实上，早前有一个版本将语言标记放到名称中。我把它移到了数据中，这是为了更方便查找。如果大家认为它们并不繁冗，那么我可以把它放回到名称中。

韦斯 • 哈达克： 同时不要忘记，特别是在 DNS 中，显示格式的最近趋势是抛开位数，并且实际上开始加入个别字词。比如，看看 DANE，我们实际上对它进行了更新，加入了表明它们实际映射对象的关键词，而不是让它拥有类型代码 0、1、2、3。

约翰 • 莱文： 它确实是这么做的。

韦斯 • 哈达克： 好的。很好。

那么，最后，最有趣的情况是，当有人向比如说注册服务机构捏造了一个记录，并且实际上颠倒了字段，或者让用户加入完全错误的数据，并最终将他们插入的数据留在有问题的区域内，这时的安全后果就很耐人寻味了 — 如果这不算是一个真正的安全问题的话。这值得思考。

约翰 • 莱文： 对，你肯定承受着风险 — 你肯定处于描述维护者的支配下，你知道？当你更新库时，会有相同的问题。它会变得更慢。

韦斯 • 哈达克： 你没明白我的意思。如果我可以捏造 .ARPA 数据，那么实际上我就可以通过你所使用的任何应用程序，使你加入一些可能截然不同的数据。

约翰 • 莱文： 对。

韦斯 • 哈达克： 我可以把词改为“密码”，比如说。

维 • 康纳德： 这就是为什么我们会有 DNSSEC。

史蒂夫？

史蒂夫 • 克罗克： 你的意见非常好，韦斯。

我刚才在想，如果你公布一个描述，之后需要编辑它，不管是因为出了错也好，还是后来有更新也好，在我看来，这时你似乎必须要更改关键词，以便在整个网络中触发更新。否则，旧的描述将永远使用下去。

约翰 • 莱文： 我没有深入思考过这个问题，但是我 — 我是说，我们因为描述 RR 类型的 RFC 描述错误而需要更新 RFC 的这种情况十分罕见。所以我希望我们能够让人们同样谨慎，我们不是 — 我们不能犯那样的错误。

史蒂夫 • 克罗克： 但这是互联网。

约翰 • 莱文： 好吧，对。

[笑声]

你肯定可以想到一些方式，比如应用版本标记或者超时之类。但是 — 但是我希望避免解决这个问题，除非有人说服我这个问题确实需要解决，因为它会使事情变得更加复杂。

戴维 • 康纳德： 杰。

杰 • 戴利： 好的，恕我冒昧。但我确实不明白为什么这个非要放到 DNS 中，它和发现新 RR 和 TTL 等等有什么关系。你知道，这是一个动态系统，一个实时系统，才能以这种方式查找。我不理解为什么它不可以是一个已经公布的静态文件，这样人们就不必在每次查找时都要获取它。

我的意思是，你是不是期待有一个软件每几个小时确认一下，看看有没有任何新的 —

约翰 • 莱文： 现有的实施是去查找 — 当它看到一个记录类型而不具备相关描述时，它会去看看能否找到一个描述，你知道，然后在本地缓存。

杰 • 戴利： 好。好的。所以情况就是，看到一个不知道的东西时才会去查找。

约翰 • 莱文： 对。

杰 • 戴利： 好的。谢谢。

戴维 • 康纳德： 保罗，你要发表意见吗？不要？好的。非常感谢约翰。

下面我们要有请沃伦 • 库马里来谈谈 IETF 目前正在进行的工作。沃伦，有请。

沃伦 • 库马里： 那么，好的。大家好。我是沃伦 • 库马里，这是保罗•胡特斯。我们都是 IAB 指派到 TEG 的代表。下面我快速介绍一下 IETF 部分工作的最新情况。我将试着点击，看看它会不会工作。噢，可以。

那么这份演示文稿实际上涵盖几个不同的事项。我会先跳过第一个演示，然后根据时间看看要不要回过头来介绍它。或者我们将转到另一个演示文稿，里面也包含了这个内容。

那么，DNS 中的信任锚信号知识。这份文件要解决什么问题？很快我们就要轮转 DNSSEC KSK。这是好事。如果你们想要获取更多信息，这里有一个 URL 和一些日期。

不幸的是，实际引入新密钥的流程是一个名为 5011 的 RFC，而有些域名服务器不支持 5011。它们要么写于 5011 出来之前，要么就是决定不实施它。

大部分实施是支持 5011 的，但其中有很多实施禁用了 5011 支持。这是因为，当我们一开始引入 DNSSEC 并进行所有推介、DNSSEC 研讨会和诸如此类的活动时，我们有大量示例包括了一个配置，说这是根区密钥，始终相信这是根区密钥，不想换来换去那么麻烦。只对该配置进行剪切和粘贴的人将会使用旧的根区密钥。它将不会轮转。

所以这里有一个类似于维恩图的图表，因为维恩图很不错。它表明在所有 DNSSEC 解析器中，有一些支持 5011，有一些实际上启用了它。不幸的是，我们无法衡量其中任何一个圆圈的大小。事实上并非如此。我们知道有多少 DNSSEC 解析器。我们不知道其中有多少执行 5011，有多少打开了它。

所以这是 KSK 轮转计划的一个摘录。它的内容大体上就是我说的，这真的很难衡量。但是我们现在有一个文件，可能有助于我们做这件事。我想它是“DNSOP 信任管理”草案，也就是密钥标记管理。我不记得确切的名称了。

基本上它说的就是这个。解析器在正常进行 RFC 5011 处理时，常常会发送一个查询，对它所知道的信任锚的一个列表进行编码。所以在这个例子中，我们有一个 KSK 所在的信任锚名为 1984。我们要轮转到一个名为 4242 的信任锚。所以解析器首先发送查询，查找 ta-1984。

当密钥轮转开始时，它开始发送包含 1984-4242 的查询。一旦密钥轮转实际完成，它就将发送包含 ta-4242 的查询。

这样，它就能让在根区观察流量的人了解到拥有旧密钥的用户占多大百分比，拥有旧密钥和新密钥的用户占多大百分比，以及只拥有新密钥的用户占多大百分比。

相同的信息也以一种不同的方式编码并插入到一个 EDNS 选项中。那基本上是一码事，只是采用一种不同的方式编码。这么做的好处在于，在密钥轮转完成之前，你就可以知道谁实际上将会中断，以及你可能要通知谁来修复它。

所以，对，这是否切实解决了问题？不幸的是，其实没有。在 RFC 5011 支持之前进行的部署，显然也会在此文件公布之前进行。这就意味着我们仍然无法衡量用户的百分比。而且，这份文件目前正在 IETF 讨论。我们希望它可以在不久后公布。

实际上工作组的最后一次电话会议已经结束，所以相对来说它应该会很快公布。但是在人们真正实施和解析代码之前，还要经历一段时间。之后一旦它实施后，在真正部署之前还要经历一段时间。

所以，下次 KSK 轮转之前 — 不管距离现在还要多少年 — 实际上我们都有望能够获得更多有用的数据。

有问题吗？抱歉我讲得很快。因为我们想挤出时间来讲解另一份演示文稿。

戴维 • 康纳德： 史蒂夫？

史蒂夫 • 克罗克： 两件事，一个直接相关，还有一个是引申出的问题。直接相关的问题是，关于发出什么密钥信号，你让我突然想到，它相当于发出什么算法信号。所以我不 — 好的。你说是，这个事实意味着在使用什么机制以及如何使用方面的一些协调是考虑周详的。

可能要花时间进行另一场讨论。但是我忽然想到，你提出的关于我们不知道不属于我们的所有这些解析器在哪里的意见，与我们不久前进行过的一个关于网络上的设备的讨论类似，我们不知道这些设备的安全状况如何。

你可以想象要在网络上注册所有设备的情形。这是一件令人心里发毛的大事。也许有的人会讨论说，以某种方式注册，或者将网络上所有的 DNS 解析器放到一个位置，这样如果出现问题就可以联系它们，或者它们就可以满足某些标准等等。只要把一个石子扔到池塘里，然后退后以免水花溅到身上。

沃伦 • 库马里： 没错，我们曾经讨论过可能要纳入一些像解析器版本或新算法或诸如此类的东西。但是我们决定，更好的方法是先将它公布，然后可能可以撰写第二份文件，来描述你们知道的那些算法的编码方式。

杰？

杰 • 戴利： 好。提前说一声抱歉，如果我说得太多的话。请告诉我。在我看来，关于解析器，我们似乎有很多不了解的地方。而且我认为，有的人，比如戴维，可以做一些工作，以便让我们了解一些事情是什么版本的什么解析器做的。这是其中一个。以家长为中心还是以孩子为中心是另一个非常重要的问题。

或许，如果我们获得了更多相关数据，就能重启采集他们指纹的工作。那时我们至少也可以知道我们所做的调查，如果我们完成了统计上正确的调查，那么就可以将它们匹配到我们对这些事务了解的情况，届时就可以给我们提供一些可推断的数据。

戴维 • 康纳德： 那实际上就是我的团队正在研究的领域。保罗 • 霍夫曼 (Paul Hoffman) 正在对解析器实施进行研究，罗伊 (Roy) 正在研究 DNS 分析方法，以帮助大家了解解析器的人口统计特征。

杰 • 戴利： 好的，太好了。

戴维 • 康纳德： 而且我们将会公布结果。

杰 • 戴利： 那太好了。我们正在撰写有关识别以家长为中心和以孩子为中心的材料，所以我或许可以提供帮助。

戴维 • 康纳德： 好的，不错。

罗恩？

罗恩 • 达席尔瓦： 好。最后这个关于尽力解决解析器的一些分析方法并做出一些决定的意见提得很好。

我也想知道，你们将采取哪些主动沟通措施，来联系运行着不同解析器的人群。我的意思是，你们如何解决这个问题？我知道这里有一个很大的差距，未来会发生什么还是未知数。你们将会采取哪些措施来至少进行一些主动的沟通？

戴维 • 康纳德： 在 KSK 轮转中，我们实际上有一个非常详尽的沟通计划。它已经在 ICANN 网站上公布，/kskroll，我想是 /#communications。但是你可以滚动到这个页面下方。它接近页面的最下方。

实际上我们目前的一个想法是，既然我们可以访问邮件根服务器查询数据，实际上可以看到我们所收到查询的来源 I.P. 地址。通过取模，我们将淘汰掉根服务器中的垃圾。然后反向查找这些 DNS 地址，或者在 WHOIS 中查找，以便识别正在运行它们的 ISP 或者正在运行那些解析器的网络。接着便联系他们说，哦，你好，顺便说一下，大概一年内会发生一些与你有关的事。你可能要了解一下。

我们也会看看能否确定相关解析器实际上是否正在进行 DNSSEC，那显然会使它们比你的日常解析器更有趣。但那是一个正在研究的领域。丹尼尔。

丹尼尔 • 达戴勒 (Daniel Dardailler)： 我只有一个问题。对于谁能请求解析器的 KSK，你们有没有做任何限制？

（离开麦克风。）

沃伦 • 库马里： 实际上是解析器通过执行一个相似名称的查询来将它播发到根。所以这个查询是一个完全限定字符串。它将会向上到达信任锚点。所以它将到达根，它将在根服务器上出现。那是它唯一会出现的地方。

丹尼尔 • 达戴勒： 因为万一密钥泄露，看起来就像在宣传我拥有错误的密钥。

戴维 • 康纳德： 亚普。

亚普 • 阿克休伊斯 (Jaap Akkerhuis)： 亚普 • 阿克休伊斯，NLnet Labs 实验室。我听说上周杰夫和乔尔 (Joel) 实际上宣布拥有 95% 的解析器的映射，这也是我所从事的领域，所以你们或许可以确认他们在做哪些工作。

戴维 • 康纳德： 抱歉，谁有那个映射？

亚普 • 阿克休伊斯： 杰夫 • 休斯顿和乔尔。

戴维 • 康纳德： 好的。我有时会跟他们交流。对于这个主题还有没有其他问题？如果没有的话，我想我们还有更多内容。

沃伦 • 库马里： 是的。我想我们可以换到另一份演示文稿。所以这是一个 — 不是这个，是另外一份演示文稿。

这本来是一个预计长达半小时的演示。但是我只有大概 15 分钟来插入这个内容，看看能不能压缩一下。所以我会很快地做一个介绍。如果我讲得太快了，请提出来。

那么，DNSSEC 提供肯定和否定应答的验证。肯定应答就是，比如，你查找 www.example.com，返回了 19216811 和一个签名，证明它是正确的。比较少人知道的是，它也提供否定应答的验证。比如你查找 login.example.com，如果这个域名不存在，你会收到一个来自 DNSSEC 的应答，告诉你它不存在，并且你还会收到一个签名来证明这一点。

生成签名从 CPU 的角度来说是一个代价十分高昂的操作，所以 DNSSEC 尽一切可能避免这么做。它采取了一个聪明的办法，那就是 NSEC，全称为 Next Secure。它所做的就是，提取区域中确实存在的所有域名，并将它们按字母顺序分类，然后对它们之间的所有空间签名。那就意味着，它不需要知道某人可能会查询什么，也不需要即时分配应答。

这有点费解。我举一个例子来说明。这里有人查找 .BELKIN。我选择它是因为它是一个在根中十分常见的字符串，而且是一个并不存在的 TLD。那么这里有人查找 .BELKIN。我收到一个

响应说，NXDOMAIN，基本上这个域不存在，而且我也进一步向下得到一个 NSEC 记录。这个 NSEC 记录说，在 .BEER 和 .BENTLEY 之间不存在任何域名。进一步向下有大量 cryptogoop，证明那是真的。所以现在，我的解析器可以去看看。它看到 Belkin 是介于 .BEER 和 .BENTLEY 之间，它知道那不存在，因为它得到了一个签名，证明了这一点。

所有这些确实很有趣，但那为什么有用呢？

在 IETF 的这份文件草案《IETF DNSOP 积极的 NSEC》中说到，递归解析器可以利用 NSEC 记录中的信息来合成应答。目前，如果解析器需要查找比如说 .BELIEVE，尽管它是在 .BEER 和 .BENTLEY 之间，但仍要专门对 .BELIEVE 进行另外一次查找。它会进行一次查找，将它发送到根，根会发回应答，等等。这份文件中指出，不要那么麻烦。如果你已经有一个 NSEC 记录，证明该域名不存在，就只需要使用它并立即用它答复。

所以这么做有很多好处。我看一下时间。它改善了用户隐私保护，因为它意味着用户查找的不存在的域名不会向外泄漏到互联网。它减少了延迟。解析器可以立即答复。它也提高了性能，因为解析器不需要发出查询。它还有另外一个优点，改善了 DDoS 的弹性。目前存在着许多 DDoS 攻击，攻击者查找许多不存在的域名，他们询问递归服务器，递归服务器接着询问权威服务器。如果这么做的次数足够多，权威服务器将会过载。通过使递归解析器直接从缓存进行应答，没有附加的查

询，权威服务器永远也看不到这些查询。再次说声抱歉，我确实讲得很快。

那么这真的有用吗？这是 5 月 12 号的一个例子，当时是一个周五的下午，因为周五下午的事情总是比较多。当时来自 RIPE 的科林 (Collin) 和卡韦赫发给我一个问题，称谷歌接受的 K 根垃圾查询骤增。这些垃圾查询好像是随机字符串，还有一些类似于 IP 地址，但格式不正确。请停止这么做。这让我们很烦恼。当他们实际联系到我时，大约是世界协调时的中午。不知道大家能不能看清楚这个图，当时的查询数量开始上升。因为我在谷歌工作，所以我们开始在谷歌公共 DNS 中调查，看看这是由什么造成的。是不是有潜在缺陷，还是有人更改了代码，或者发生了什么？可能我们被用作了一个 DoS 反射器，是不是有人在向我们发送这些查询，然后我们将它们转发，从而造成了这个问题？更令人担心的是，为什么这看起来像是自然增长。DoS 攻击通常在 4/8 启动，扩散，然后停止。这更令人担心，因为它看起来在增长，而且可能会持续增长。

在进行了一番调查之后，我们发现不仅仅是谷歌公共 DNS 在发送这些查询。有很多解析器都在发送。于是我们松了一口气，至少不是我们。但它到底是什么引起的，我们能不能阻止它呢？

继续调查后我们发现，有一个新的蠕虫正在互联网上扩散，它正在感染接入点，而且好像在感染一家名为 Ubiquity 的公司所生

产的家用路由器。在攻击中，它们会感染一台机器或者感染一个接入点，然后对一个特定类型的字符串进行查找，看它能否到达互联网。而这个字符串正好看起来很像它。先是随机字符串，然后是随机的一系列八进制数。所以现在至少我们知道它不仅仅是我们的问题。但是让我们看看能不能对此做些什么。

那么对于时间我要怎么做？这是一个从谷歌公共 DNS 到 B 根服务器的查询的图表，B 根服务器是由韦斯所在的 USC/ISI 运行的。我不知道大家能否看到这些数字，在最左边，攻击开始之前，谷歌每秒向 B 根发送大约 500 个查询。当攻击开始时，也就是这个向上的大尖峰，它激增到了大约 2,500 个，谷歌公共 DNS 已经内置了这个软件。我们只是没有启用它。我们在受影响最大的地点将它 100% 打开，你们可以看到这里出现了大幅度的下降。我刚才说过，当时是周五。我们避免在周五做出生产变更。所以我们一直等到了星期一。之后我们在全部地点的半数机器上将它打开。它第二次下降。我们让它工作了一周时间。最后，向右边，我们在所有地点将它 100% 打开。之后你们可以看到在最右边，现在发送到 B 根的查询数量接近于每秒 30 到 40 个。所以，你知道，大约 10 倍的降幅。

这份文件实际上说了什么？主要就是我在一开始时所说的。如果你有一个 NSEC 记录证明某个域不存在，那么甚至都不用查找它。只需要用它来答复。而且，如果你有一个涵盖它的通配符记录，那么也不用查找它。只需要使用那个信息，并立即返回应答。就是这样。

所以稍微总结一下，目前在根收到的查询中有大约 60% 的查询将得到域不存在的应答 NXDOMAIN。这些有点像虚假查询、垃圾查询。如果人人都这么做，那么到达根的虚假查询将降至 1% 左右。抱歉我仓促地完成了这个介绍。希望它勉强还算连贯。有问题吗？

戴维 • 康纳德： 有人要向沃伦提问吗？我有一个问题 — 关于 NSEC 3。

沃伦 • 库马里： 对。这也执行 NSEC 3。它不会使用带有选择退出的 NSEC 3，因为实际上你不能那么做。但是对于 NSEC 3 — NSEC 3 的工作方式和 NSEC 几乎相同。只是它不是对存在其中的域名排序，而是对区域中存在所有哈希排序，你只要看 — 检查你查找的域名，哈希是否匹配。基本上是一码事，只是将哈希摆在第一。

戴维 • 康纳德： 拉姆，你 —

拉姆 • 莫罕 (Ram Mohan)： 沃伦，我在和董事会的一些同事沟通，他们都表示这里的技术太深奥了，他们有点听不明白。所以也许你可以高度概括一下它的意思，以及问题是什么，这样可能会有助于理解。

沃伦 • 库马里： 当然，对。抱歉。我说得太快了。高度概括起来其实就是，如果部署了它，就可以减少到根以及到其他域的垃圾查询数量。它提高了用户隐私性。它提高了性能。它减少了最终到达权威服务器的查找次数。我想概括起来主要就是这些。如果大家想要更详细地了解，我很乐意更慢地来说明一下。

拉姆 • 莫罕： 谢谢，沃伦。

韦斯 • 哈达克： 大家好，我是来自 USC/ISI 的 B 根，我想要说的是谢谢你。托你的福，我的寻呼机在那段时间都没有响起。

杰 • 戴利： 拉姆，我认为董事会从这个主题和上个主题可以得到的信息是，解析器的发展多年来一直没有得到很多关注，如果它能够从行业中得到更多更有意义的关注的话，那么就可以解决一系列的问题，或者可以采取预防措施以使今后出现的其他新问题更加容易处理。

拉姆 • 莫罕： 谢谢。我也要鼓励正在沟通这个问题的董事会同事不要有顾虑，直接站出来发言，而不是通过我来传话。

戴维 • 康纳德： 还有其他问题吗？好的，约翰。

约翰 • 莱文： 你知道目前它已经在哪里实施了吗？

沃伦 • 库马里： 我知道其中一些地方。谷歌公共 DNS 实施了。它也在 Unbound 中得到了实施，Unbound 是两个标准的大型递归平台之一。除了 Unbound 以外，另一个是 ISC 的 BIND。

戴维 • 康纳德： 好的。非常感谢。如果没有其他问题，我们就继续讨论其他事情。TEG 或者观众席中有没有人有话要说？米谷嘉朗好像有。

米谷嘉朗 (Yoshiro Yoneya)： 我是米谷嘉朗。在 DNSSEC 研讨会期间，有一个关于如何部署 BCP38 来过滤欺骗性源门户风险查询的问题。这类欺骗性查询或欺骗性数据包会被用于这些攻击。所以部署 BCP38 对减少此类攻击非常重要。所以我认为，这里很适合探讨这个问题。因为运营实践是如何解释 IETF，但是运营 — 所以思考这个问题对运营商团体以及对 ICANN 也很重要。

戴维 • 康纳德： 我知道 SSAC 公布了几份关于部署诸如 BCP38 等事项的价值的文件。有人提到过，SSAC 可能有必要重申一下 BCP38 的价值。但它好像不是 TEG 本身会直接关注的一个话题。拉姆，你有什么要说的吗？

拉姆 • 莫罕： 谢谢。我要提供一些 — 接下来我会放下技术人员的身份，并以董事会成员的身份向 TEG 提供一些反馈意见。这有点儿奇怪，因为我是一名技术人员，对吧？但是感觉可能有几件事 — 在我们下一次开会时，可能应该考虑做几件事，以使它更像一个对话和讨论。第一个建议是，在我们拿到议程和话题后 — 我们要有一个高度概括，类似于执行摘要，解释问题是什么，它为什么重要，以及你们为什么应该关心它的原因。因为我认为这是一个被漏掉的核心事项。因为对于我们技术人员而言，你知道，你读到这个话题，并且理解你为什么应该关心它。但是如果你不是，那么 — 我感觉有时其中的一些话题，我们讨论它的方式，对于非技术人士而言只能说，对，那是技术专家的事。让那些人去研究它。所以这是一条反馈意见。

第二点就是，在会议的议程收集阶段，我认为可能可以做的就是，邀请董事会方面的人，特别是非技术人士提供建议，了解他们可能对什么类型的话题感兴趣。我认为这么做会很有用。

最后一点，我注意到，人们强烈需要某种一致的指导类会议。也许我们可以录制这些会议的视频并提供给大家。那不仅仅是

个别会议，而实际上是一系列会议。这样它就能成为某种信息库以及某种入门培训材料。这么做不仅仅是为了董事会，实际上也是为了重视这些话题的社群中的其他人员。我经常听到社群中的人走过来说，哦，ICANN，你们只制定政策。但是在这里我们也处理技术问题。我担心即使是我们这种程度的技术，对本次会议的很多与会者而言理解起来都有点困难。

戴维 • 康纳德： 沃伦，请讲。

沃伦 • 库马里： 谢谢，这确实是非常有用的反馈，几乎就是我想要说的。TLG，也就是 TEG 下的一个分组，它的目的就是将董事会与技术资源对接，或者类似于此。所以我想，我们非常欢迎董事会就他们感兴趣或者希望深入了解的方面提出问题。关于你所说的指导，刚才有人提到了 BCP38。董事会是否想要快速了解一下它是什么，它和什么有关，有没有用。或者，董事会是否想要更多地了解一些技术事项、最新信息、小型指导。这些不用在这里这么大的会议室进行，而是可以在其他某个地方。对于你们想要更多地了解的事项，我们可以研究一下，并尝试提供一个通俗易懂的形式。

戴维 • 康纳德： 我想显然大家对指导的深度感兴趣。我们已经完成的事项之一就是 — 首先如何为社群中的新加入者提供一系列指导。我们内部一直在讨论，你知道，也许可以通过很多不同的方式进行延伸。我想，如果在董事会级别有人对特定话题的针对性指导感兴趣，我知道我的团队会兴高采烈地做准备。而且我确信在 TEG 和 TLG 中也有大量资源能够提供指导。

关于议程方面，我一直在努力寻找为 TEG 确定议项的最佳方式。我尝试过几种不同的方法，直接请教董事会成员，直接请教 TEG，亲力亲为地准备材料。到目前为止，这些方法的效果确实都不理想。所以，我一直在征求更多意见，特别是董事会对哪一类事项最感兴趣。因为，你知道，这是一个专为向你们提供意见而设的小组。你知道，技术专家将在各种地方彼此交流，这通常不太合适。所以当然希望大家提供更多意见。我看到有几个人举手。先从拉姆开始。

拉姆 • 莫罕： 戴维，我很快地举一个例子。几周前，在新闻中广泛报告了一个对网络基础设施的攻击事件，而且你知道 — 从董事会的角度来说，有几个问题，不是关于已经报导的内容，而是关于它意味着什么的问题。你知道，我们是如何关注它的。

所以这是一种对材料的解读和分析 -- 看起来它是有必要的。

戴维 • 康纳德： 沃伦？

沃伦 • 库马里： 那么，对，显然董事会成员确实很忙，而且抽出大概两小时的时间来讨论没有给他们提供价值的东西并不划算。所以，我非常希望听到任何反馈，比如，这是不是技术性太强了，完全离题了，那么什么信息才有用，等等。

戴维 • 康纳德： 玛盾？

玛盾 • 波特曼 (Maarten Botterman)： 好的。谢谢。我因为无知，所以才来到这里。这是我第一次参加这个会议。但是我来到这里是因为这与我们的使命密切相关，这就是为什么我想要更多地利用这个机会。

一开始，我想“太好了，我终于可以了解一下你们所做的工作。”但是如果这个会议真的也希望为像我这样的人提供信息的话，那么对，请让我们先制作一个指导材料。因为我同意，有些问题在稍作介绍之后可能会变得更加简单。

第二，请按照你们想要的水平来进行介绍，也许有人会很感兴趣，并且能够从中获得一些深入的认识。我真的很欣赏这一点。

非常感谢你们为此所做的努力。

戴维 • 康纳德： 史蒂夫？

史蒂夫 • 克罗克： 谢谢。我同意所有关于调整的意见，但是我要讲一点，在这个背景下，我认为这种参与，甚至是与此有关的意见，其实都非常宝贵。

这提供了一个非同寻常的窗口，使董事会能够了解到正在出现的技术问题，而且在提高对这些问题的认识和敏感性方面发挥着巨大的作用，即使我们不能完全理解其中的细节。

所以我非常满意，并且要保证这里传递的不仅仅是批评或负面意见。相反，我认为我们在这里开展的是一个意义重大的流程。显然，它还可以微调并将随着时间而发展，但是基本上我对它非常满意。

戴维 • 康纳德： 接下来是帕特里克？

帕特里克 • 弗斯特朗姆 (Patrik Faltstrom)： 非常感谢。帕特里克 • 弗斯特朗姆，来自 SSAC 的 TEG 成员。

拉姆，我想澄清一点。你更多地是要求在介绍之前有一个问题陈述，而不是说技术层次太深吧？

拉姆 • 莫罕： 对，没错，帕特里克。我不是说技术性太强了，应该削弱一点。而是说在一开始的时候就要说明我们为什么提出这个问题、为什么认为它很重要，然后再深入讲解技术，这样就能提供一些背景信息。

戴维 • 康纳德： 谢林？

谢林 • 查拉比 (Cherine Chalaby)： 我非常喜欢本次会议，特别是第一个和最后一个话题。从背景的角度出发，我发现它们非常有用。

我认为我们 — 在我看来 TEG 与董事会召开会议这个说法并不清楚，我认为你们很可能是和董事会的一部分成员开会，那些对议题感兴趣的成员或者能够理解议题的成员。

所以如果我们想要让董事会更多地参与进来，让每个人都能参与进来，那么我想我们必须做下面两件事中的一件。要么提前发送一些材料，让大家对主要议题有所准备，而且或许还能稍微提高讨论的水平。

我们也要做一个工作，史蒂夫，我们要向 TEG 明确我们希望达到什么样的互动水平。在我看来，这一点还不是非常清楚。谢谢。

史蒂夫 • 克罗克： 对。关于董事会在多大程度上参与，基本方法 — 我将承担起我们的责任 — 特别是和戴维互动，既然技术专家小组过来，希望与董事会互动，那么董事会就必须与之进行一些互动。

另一方面，你我都非常清楚，董事会的日程非常紧张，所以我们没有正式要求每一位董事会成员必须出席。我们没有将它作为董事会的唯一事项来安排。

所以实际情况就是我们在这里所看到的，大部分董事会成员都来了。在任何情况下，这大体符合 — 不管怎么说，我们在董事会尽量做到的，不是让每一个人去做每一件事，而是我们分成了多个委员会、工作组等等。

所以这实际上董事会的一个临时版，我们自己选择参加。

我数了一下，包括来提前离开的马跃然 (Goran) 在内，我想我们有 10 位 — 如果我没记错的话，有 10 位董事会成员来到这里。董事会成员一共有 20 位，包括联络人在内，所以是一半。而且显然是更优秀的一半，因为我们选择来到这里。

[笑声]

史蒂夫 • 克罗克： 虽然这是开玩笑，但是自己选择实际上有积极的作用。

我不觉得这个参与范围有何不妥。我的意思是，我们有几个人可以理解这里的信息，但更重要的是下一批人，像你这样没有技术背景但是对技术很感兴趣的人 — 以及其他几个坐在台上的人。

我们随时可以调整流程，所以 — 但是我 — 正如我之前说过的，我对这种参与性以及它所具有的作用非常满意。当然它还可以调整。

戴维 • 康纳德： 沃伦？

谢林 • 查拉比： 我可以快速回应一下吗？

戴维 • 康纳德： 抱歉。

谢林 • 查拉比： 谢谢史蒂夫的说明。我想，管理期望很重要。并且我也认为你已经说得非常清楚了，我很想看看 TEG — 他们对与董事会的这种互动水平感觉怎么样。那也会是很好的反馈。谢谢。

戴维 • 康纳德： 沃伦？

沃伦 • 库马里： 最后很快地讲一点。我知道每个人都很忙，但是如果你们有时间的话，请向戴维或芭芭拉 (Barbara) 或者其他人提供反馈，告诉我们怎么样才能把它做得更好，对你们更有用 — 你知道，哪些有用，哪些没有用等等。未来我们将尽量使它们变得更加有用。

谢林 • 查拉比： 即时反馈一下。这非常有用，也非常非常有帮助。谢谢。

戴维 • 康纳德： 现在实际上距离感谢 IANA 移交相关社群的宴会还有八分钟。我也要提醒各位，在 Westin 酒店的 Casbah 大厅有一个鸡尾酒会。我们有两辆车，一辆会在大概 5 分钟或 7 分钟后出发，第二辆会在 7:15 出发。在 Westin 酒店 Casbah 大厅举办的宴会将在 7:30 开始，9:30 结束，那里有酒 — 对。稍等。抱歉。

（离开麦克风。）

7:00 — 好。有意思，我的日程表上不是这样，但是没关系。所以是 7:00 和 7:30。这两辆车分别在 7:00 和 7:30 出发。希望在那里见到大家，如果没有见到，我会代你们把酒喝光。

[文稿完毕]