



下一代DNS发展论坛
Next Generation DNS Summit

下一代DNS发展报告

NEXT GENERATION DNS DEVELOPMENT REPORT

下一代DNS发展论坛

网络根基 中国贡献

Network Foundation China Contribution

2023 北京

《下一代 DNS 发展报告》

编委会

主 编：毛伟

副 主 编：邢志杰 刘志江

执行主编：庞可

编委会成员：马迪 张绍峰 冯硕 吴琦 江连山

发展下一代 DNS 筑牢数字经济重要网络根基

——毛伟 互联网域名系统国家地方联合工程研究中心（ZDNS）主任

党的二十大报告提出加快建设网络强国、数字中国。中共中央、国务院印发《数字中国建设整体布局规划》，提出到2025年，基本形成横向打通、纵向贯通、协调有力的一体化推进格局，数字中国建设取得重要进展。规划提出，要夯实数字中国建设基础，打通数字基础设施大动脉，畅通数据资源大循环；强化数字中国关键能力，构筑自立自强的数字技术创新体系、筑牢可信可控的数字安全屏障。互联网网络的承载能力与服务，支撑各行业数字化、网络化、智能化发展，为数字基础设施提供安全、稳定、高速的网络环境，其中，互联网关键基础资源发挥着重要作用。

互联网三层架构体系

从互联网体系架构出发，互联网可以简单地分为三层，即：物理设施层、基础资源层、应用层。

物理设施层包括基础网络、传输设备、互联设备、接入系统等，如同信息高速公路；应用层是互联网的各种应用，包括电子商务、电子政务、网络游戏、视频通讯等，犹如跑在高速公路上的汽车。两层中间还有一层基础资源层，由域名系统和路由系统组成，二者组成互联网的寻址解析系统，如同导航系统，“导航”一旦失效就会断网。由于根服务器、顶级域名等互联网关键基础设施就在这一层，也把这一层比作“网络根基”。如果把互联网看作一棵枝繁叶茂的大树，而域名系统就是树根。

从互联网基础设施的资源属性和服务属性两个层面来看：

互联网基础资源：用于命名和定位网络实体的域名、IP地址及各类标识。基础资源是互联网的基础性、战略性资源，是影响和制约互联网上层技术的关键，是互联网

实施有效管理的重要抓手。

互联网基础资源服务：互联网基础资源服务是互联网的基础服务和逻辑基础设施，任何互联网业务应用必须查询基础资源服务获得相关基础资源信息后才能进行数据通信和互联互通，才能使各项业务得以开展和实现。其服务体系是互联网稳定运行和健康发展的基础，是互联网安全和稳定的保障。

互联网基础资源和基础资源服务也伴随域名生命周期两大过程：域名注册和域名解析。域名注册解决互联网基础资源占有问题，保证每个域名的全球唯一性；域名解析解决互联网基础资源服务问题，域名解析就是域名到IP地址的转换过程，域名的解析工作由域名服务器完成。

DNS 面临“三大挑战”、“两大机遇”

当前，DNS这个“导航系统”遇到三大挑战：“断根”、“断服”、“断供”。“断根”是指国家域名被关停，拒绝

中国用户对根服务器访问。当前全球 13 台根服务器，主要位于美国、欧洲等国家和地区，目前在中国部署的均为镜像根服务器。“断服”是指通过顶级域名管理权阻断我国机构域名的全球互联互通，全球约 1500 个顶级域名，中国境内拥有管理权的不足 3%。“断供”是指停止向我国提供域名基础软件和装备，我国运行域名系统软件及设备有数千万套，超过 90% 使用的都是国外域名软件。国际局势变幻莫测，DNS 遇到三大挑战不容忽视，中国需要更安全的网络根基。

同时，域名系统面临两大机遇：处于“中间层”的 DNS 也迎来“上下所需”的两大机遇：**其一，信息网络基础设施信创升级，需要 DNS “向下”承载与融合。**一方面，自主可控是发展数字经济的基础与关键，CPU、服务器、操作系统、数据库等基础软硬件，是数字经济的基础底座，正处于信创升级阶段，DNS 需要多态适配、深度融合；另一方面，网络技术升级发展，5G、IPv6、物联网、工业互联网、卫星互联网等部署推进，需要 DNS 同步升级。**其二，深化数字化转型、发展数字经济需要 DNS 技术“向上”创新突破。**

《“十四五”数字经济发展规划》提出，稳步构建智能高效的融合基础设施，提升基础设施网络化、智能化、服务化、协同化水平，这些要求的实现离不开强有力的 DNS 底层支撑。在金融行业，构建数字金融需要推进大数据、人工智能、区块链技术在金融领域中的深化应用，但这些技术的深化应用离不开强有力的 DNS 的支撑。在数字政府、智慧城市建设过程中，也同样需要网络化、智能化“底座”，这些都需要 DNS 技术的创新突破。

迎接信息网络基础设施升级和发展数字经济两大机遇，亟需打造下一代 DNS，重塑网络根基。下一代 DNS 将从互联网导航系统发展成为支撑数字经济发展的重要网

络根基，向下对接信息网络基础设施的升级，向上更好地支撑各行业数字化转型和数字经济发展。

“下一代 DNS”与“DNS”的区别

D (Domain) 是网络空间，域名系统是互联网治理的重要抓手，是构建网络空间命运共同体的重要元素。

N (Name) 是基础资源，域名以及 IP 地址、网络自治域号 (AS 号) 等是互联网关键基础资源，是战略资源，没有互联网关键基础资源就联不了网。互联网关键基础资源的占有量和质可以衡量国家和企业的“网络规模”以及在全球互联网中的“管理权重”。

S (System) 是软硬件系统，支撑了“D”和“N”，核心技术需要不断创新突破，以筑牢网络核心技术根基。

“下一代 DNS”与“DNS”的具体区别：

网络空间（“D”）：以前采用中心化技术结构、单边治理结构。下一代 DNS 推动去中心化模式，通过采用区块链技术、新型根技术等方案，推动根服务器的扩展和技术升级，实现网络空间的互联互通、共享共治，构建更加公平合理、开放包容、安全稳定、富有生机活力的网络空间。对于企业和机构而言，则是通过“D”，强调整体规划、统一标准，建立符合企业发展战略，规则清晰、流程明确的企业域名使用标准。

互联网关键基础资源（“N”）：以前顶级域名主要分布在海外，重点顶级域名管理权由国外控制。“下一代 DNS”一是要推动顶级域名申请，把握发展机遇，获得更多资源；二是要争取顶级域名的国内管理权：大力发展战略境内的顶级域名，重视顶级域名作为数字化转型重要载体的作用，重视其对数字经济发展的重要

重要支撑作用。

域名系统技术（“S”）：传统 DNS 只是负责简单解析，实现域名到 IP 地址的转换。域名系统从“一对一”到“一对多”、从“人-机”访问到“机-机”访问，随着万物互联，接入系统的暴增，域名访问量也是在爆发式增长，对域名的访问安全、访问效率有很高的要求。下一代 DNS 将在数据赋能、全面感知、可靠传输、智能分析、精准决策等方面实现创新突破。

更安全：通过自主技术、国密算法、威胁管控、数据可信、隐私保护等实现域名解析安全，同时与操作系统、

芯片等基础设施无缝衔接，共同打造自主可控的网络底座。

更高效：以高性能、低延迟、云化、弹性扩缩容、自动编排等特点，满足高并发量下高效调度需求。

更智能：通过大数据分析、智能枢纽、全局负载、算力调度等能力提升万物互联时代终端调度需求。

综上，下一代 DNS 是自主可控的、承载万物互联的智能网络中枢，是支撑网络强国数字中国建设的重要网络根基。

	DNS	下一代 DNS	意义
D- 网络空间 构建网络空间命运共同体	中心化技术架构 单边治理结构	全球互联网 去中心化：采用区块链技术、新型根技术等方案，推动根服务器技术升级 互联互通、共享共治：构建更加公平合理、开放包容、安全稳定、富有生机活力的网络空间 行业 & 企业 整体规划、统一标准：建立符合发展战略，规则清晰、流程明确的企业域名使用标准及规范	为推动全球互联网治理体系贡献中国智慧、中国方案； 建好域名数字基建，服务数字化转型。
N- 基础资源 掌握网络关键基础资源	顶级域名主要分布在在国外 重点顶级域名管理权由国外控制	资源申请 把握发展机遇，积极申请顶级域名、IPv6 地址等互联网关键基础资源，支撑网络发展 国家管理权 大力发展战略境内顶级域名和 IPv6 升级，推进中国数字化转型	提升国际互联网治理话语权重，助力中国品牌国际化。
S- 技术系统 筑牢网络核心技术根基	简单解析，名字到 IP 转换	数据赋能、全面感知、可靠传输、智能分析、精准决策 更安全 自主技术、国密算法、威胁管控、数据可信、隐私保护等 更高效 高性能、低延迟、云化、弹性扩缩容、自动编排等 更智能 大数据分析、智能枢纽、全局负载、算力调度等	构建自主可控、承载万物互联的智能网络中枢

如何发展下一代 DNS

Domian 积极参与国际互联网治理和标准制定，为全球互联网发展贡献中国智慧。

推动网络空间共治，构建网络空间命运共同体。中国机构尤其是互联网技术企业，应积极投身网络空间治理、参与标准制定，“发出中国声音，给出中国方案”，为全球互联网发展治理贡献中国智慧；推动“互联互通、共享共治”的理念在相关国际技术标准、管理规则中形成生动实践。

值得欣慰的是，我们已经看到国内很多机构已经在积极参与，比如华为、清华大学、中国移动、中国电信、中国互联网络信息中心、中科院计算机网络信息中心以及ZDNS等，都积极参与了互联网标准和国际规则的制定。过去20年以来，我国发表过RFC的机构超过29家，中国专家研究实力在国际互联网治理体系中体现优势。

Name 提升数字资产战略意识，助力企业品牌国际化。

中国互联网发展的早期，中国一个国家的IP地址数量甚至比不上美国一所大学多，随着中国互联网的发展，目前中国IPv4和IPv6地址量均居全球第二位。但在域名资源尤其是顶级域名的占有率上，中国内地远远落后于一些发达国家。

提高互联网入口安全意识，筑牢网络基础设施，提升数字资产战略意识；为数字经济的发展以及企业品牌出海，筑牢网络根基。掌握网络关键基础资源。以域名、

IP地址、AS号为代表的互联网关键基础资源，是支撑网络发展和创新的载体，不仅是衡量数字经济发展程度的重要指标之一，也是国际互联网治理话语权的重要体现。中国机构应积极申请互联网顶级域名、IP地址和AS号，掌握更多网络关键基础资源，为数字经济的发展以及品牌出海筑牢网络空间的底座。

System 加强基础技术研究，实现互联网关键技术创新突破。

攻克互联网核心技术、关键技术，提升自主创新能力；从根本上为数字经济发展筑牢安全、高效、智能的网络根基。

在关键技术能力创新方面，国内领先的域名系统技术公司针对关键技术进行了创新突破，比如域名系统基础软件“红枫”，以更安全、更高效、更智能的特点，能够全方位与国外主流DNS软件比肩，“红枫”在很多关键技术指标上已经远远超过国外同类软件，能够解决互联网基础软件“卡脖子”技术难题。

在信创生态体系构建方面，加快推动域名系统技术与国产芯片、操作系统等广泛适配、多态融合，以灵活、无缝的特点，联合打造自主可控的数字信息基础设施。

随着下一代DNS的广泛应用，互联网关键基础资源技术创新与产业发展深度融合，将发挥网络根基对数字经济发展重要支撑作用。需求牵引技术进步，面向数字经济发展的需求，不断探索网络基础技术前沿，中国网络基础技术也将从跟随者到引领者，服务网络中国数字中国建设，并为国际互联网大家庭作出贡献。

CONTENTS

D

第一章 下一代 DNS 为推动网络空间治理贡献中国智慧

第一节 互联网治理	08
第二节 推动构建全球互联网新型治理体系	10
1.2.1 主要国际互联网社群	10
1.2.2 互联网国际社群动态	11
第三节 网络空间治理·中国思考	13
• 勇立时代潮头，以坚决打赢信息领域核心技术攻坚战推动高水平科技自立自强	13
• 推进全球网络空间治理的中国路径	14
第四节 网络空间治理·中国贡献	16
• 互联网基础资源技术协议利用公钥信任链加强安全	16
• BGP 架构原则下的“自治”方案	18

N

第二章 下一代 DNS 助力中国品牌国际化

第一节 全球域名发展统计报告	20
第二节 顶级域名现状及趋势	21
2.2.1 顶级域名属性分析	22
2.2.2 顶级域名应用新趋势	23
2.2.3 顶级域名全球市场概览	24
2.2.4 中国顶级域名市场现状	25
2.2.5 品牌顶级域名应用案例	26
2.2.6 城市顶级域名应用案例	27
第三节 第二轮顶级域名开放动态	29
第四节 中文域名 推动构建更加开放 多样的互联网	30

S

第三章 下一代 DNS 系统技术：包罗万象

第一节 域名技术与数字化变革	32
第二节 包罗万象的 DNS 应用	34
3.2.1 DNS 支撑园区网发展演进的智能互联	34
3.2.2 DNS 联动网络实现业务调度的自动驾驶	36
3.2.3 应用域名大数据保护企业数字品牌	38
3.2.4 DNS 融合 SDP 建立零信任安全增强模型	40
3.2.5 DNS 在算力网络中为海量数据定位算力	41
第三节 DNS 技术升级趋势	42
3.3.1 云边融合、云边协同的 DNS	42
3.3.2 软件定义 DNS	44
3.3.3 有状态 DNS 的深入应用	45

下一代 DNS 为推动网络空间治理贡献中国智慧

第一节 | 互联网治理

互联网与生俱来的“共治”特点， 为网络空间治理未来提供思考

以信息技术为基础的数字技术日益成为重塑世界竞争格局的重要力量，成为大国综合国力较量的制高点。承载上述技术的互联网的应用，不仅涉及到网络基础设施，随着与新一代信息技术与网络基础设施的融合，还渗透到金融、政务、电子商务等多个领域，成为社会治理与人们生活不可或缺的部分。互联网网络基础设施是当今社会最重要的基础设施之一，我国网络规模和用户数量居全球首位，是名副其实的网络大国。在从网络大国迈向网络强国的过程中，重新审视互联网的特性及互联网治理的发展，对我们立足于当下，预见未来或许能够提供更多参考。当下，国际社会普遍认为，网络空间现在已成为领土、领海、领空和太空之外的第五空间。多国调整信息安全战略，明确网络空间地位。互联网作为全

球关键基础设施，以促进技术发展、管理网络资源、规范网络秩序、净化网络环境等为主要议题的互联网治理的重要议题日益凸显。如何充分理解互联网诞生的意义，以及互联网本身的内涵，对网络空间治理的未来路径提出思考。

回溯互联网的发展，1980 年，TCP/IP 诞生；1983 年 1 月 1 日起，ARPANET 主机协议从 NCP 过渡到 TCP/IP。这是一个“标志日”式的转换，要求所有主机同时转换，或者必须通过临时机制进行通信。从此，阿帕网（ARPANET）从 NCP 到 TCP/IP 的过渡意义：被分为满足特定操作要求的军事用途 MILNET 和支持研究需求的非军事社区 ARPANET。

中国自 70 年代后期，中国开始研制光纤通信系统；到 1983 年底已与 45 个国家和地区开通了直达电话和直达电报电路。从阿帕网诞生，到 TCP/IP 协议的应用，

尽管彼时中国互联网恍如与世隔绝，但迅速发展的光纤通信系统，仿佛已经为拥抱互联网的到来张开双臂。1984年，第一批可以请求的域名就在RFC920中被整理发布出来了。其中.com是commercial的缩写，代表商业机构。除.com外，还有.gov代表政府，.edu代表教育界，.mil代表军队，.org代表组织机构，等等。.cn属于国家地区类，这类用两个字符来描述。1984年，第一批可以请求的域名就在RFC920中被整理发布出来了。

1986年，IETF成立，更充分体现了互联网开放共享的精神：没有会员的概念，任何人都可以参与，都可以提交草案，大家通过邮件讨论表达赞同，就会让你拥有自己的互联网标准。在这个阶段，虽然中国尚未全功能接入国际互联网，但互联网精神、互联网社群的意义都已传入中国，第一批中国互联网人热情投入其中，积极尝试互联网连接、主动参与国际互联网会议。

与此同时，上世纪90年代，第一代互联网主要应用于高校与研究机构，虽然社会化程度有限，但技术架构已与国际接轨。此时的互联网最受关注的是其技术特性。互联网具有天生的“去中心化”特质，体现开放与自由的原则，其技术架构体系是彼时的特点。IETF、ICANN、APNIC等国际互联网社群，重点关注的是互联网技术标准制定与技术推进。彼时，除了互联网治理机构，互联网技术架构也是最受关注的话题之一。包括域名系统、协议地址、根服务器等也是当时最热的话题之一。

1994年4月20日，中国全功能接入世界互联网，自此开启了中国互联网发展的新篇章。但中国最初的互联网从业者，融入国际互联网社群，遵循互联网“自下而上”

的特点，努力为互联网做出贡献。

从互联网建立之初，以社群组织或较为松散的论坛为核心的“驻地”就成为各国互联网技术专家热衷的交流平台。让各国的技术专家参与进来，这样的模式一直保持至今。社群论坛成为各国互联网技术工作者热衷的盛会，在这里能够充分体会互联网的共治特点。

网络强国战略，来自于互联网基础资源层的思考

中国互联网起步较晚，但发展迅速。随着各国对网络空间重要性意识的提升，我国对网络基础设施的治理也不断加强，尤其是对互联网基础资源（IP地址、根服务器、域名）的重视程度已经高度提升。随着IPv6时代的到来、域名关键基础资源的分配现状，也带来了网络空间的新问题。

网络资源分配，依然存在不平衡性。中国互联网起步较晚，在根服务器的分配、网络空间资源的占有方面未能获得先机。随着中国网络规模普及、互联网与实体经济的深入融合，改善网络空间权益、提升我国在全球网络空间治理能力，是维持社会稳定及数字经济发展的必然。网络资源的管理权一直是互联网治理的头号难题。

网络核心技术，融合创新能力亟待提升。在我国互联网关键基础设施领域，无论是核心技术突破应用还是产业化程度，与其他发达国家相比仍然存在差距，在互联网关键基础资源领域融合创新能力仍亟待提升。在互联网关键技术领域，仍然存在受制于人的情况。互联网基础设施层面的域名、IP等关键基础资源支撑着互联网发展的底层基础设施，自主可控程度有待提升。

网络根基安全，面临更为严峻的挑战。相较于互联网发展初期，以 5G、人工智能等为代表的新一代信息技术与实体经济深度融合，使网络安全风险被加速传导、渗透、叠加和放大。关键基础设施遭受网络安全攻击的频率日益增长，网络安全呈现出更复杂的特点。

在互联网应用繁荣、万物互联蓬勃发展的同时，关注从网络技术为出发点的互联网国际治理，互联网国际治理包括网络技术标准的制定以及网络空间行为规范的建章立制，这对维护国家网络空间利益至关重要。争取更加公平、公正的发展环境，了解互联网国际治理体系也尤为重要。无论中国的机构还是企业，当以互联网本质特点为原则，结合本国发展方向及路径，探索出一条维护互联网发展，有服务网络强国战略的路径：

以互联互通为原则。无论数字技术如何应用发展，无论网络安全事件面临何种困惑，互联互通是互联网诞生的“初心”，也是这一特点吸引了无数互联网网络基础技术工作者，为“互联互通”不断攻克技术难题，提升网络稳定与高效。

以与时俱进为路径。全球数字化发展迅速，互联网已经成为承载万物、托举创新的重要载体。互联网基础技术日渐成为众多行业的技术底座，互联网关键基础设施域名、IP 等承担了互联网标识、地址和路由等关键核心功能，是全球互联互通、网络空间安全稳定的重要基石。如何充分融合各行业数字化转型的路径，同时葆有自己的特点。

第二节 |

推动构建全球互联网新型治理体系

数字技术日新月异，给人类的生产和生活方式带来了巨大变化。互联网联通全球，使全世界日益紧密地结成命运共同体，构建科学、合理、平衡、有效的治理体系，实现全球互联网治理体系共建、共享、共治和共赢，发挥国际互联网社群的重要作用。

1.2.1 主要国际互联网社群

亚太互联网络信息中心（APNIC）

亚太互联网络信息中心（Asia-Pacific Network Information Center，简称 APNIC），是全球五大区

域性因特网注册管理机构之一，负责亚太地区 IP 地址、ASN（自治域系统号）的分配并管理一部分根域名服务器镜像的国际组织。成立于 1993 年，秘书处设于澳大利亚布里斯班。它提供全球性的支持互联网操作的分派和注册服务。这是成员包括网络服务提供商、全国互联网登记，基于会员资格的组织。APNIC 负责亚洲太平洋区域，包含 56 个经济区。

互联网工程任务组 (IETF)

互联网工程任务组 (The Internet Engineering Task Force, 简称 IETF) 成立于 1985 年底，是全球互联网最具权威的技术标准化组织，主要任务是负责互联网相关技术规范的研发和制定，当前绝大多数国际互联网技术标准出自 IETF。

IETF 是一个由为互联网技术工程及发展做出贡献的专家自发参与和管理的国际民间机构。它汇集了与互联网架构演化和互联网稳定运作等业务相关的网络设计者、运营者和研究人员，并向所有对该行业感兴趣的人士开放。任何人都可以注册参加 IETF 的会议。

IETF 的主要任务是负责互联网相关技术标准的研发和制定，是国际互联网业界具有一定权威的网络相关技术研究团体。IETF 大量的技术性工作均由其内部的各种工作组 (Working Group, 简称 WG) 承担和完成。

互联网名称与数字地址分配机构 (ICANN)

互联网名称与数字地址分配机构 (The Internet Corporation for Assigned Names and Numbers, 简称 ICANN) 成立于 1998 年。

作为一个民间的非营利性国际机构，ICANN 的使命是确保互联网标识符的一致和唯一分配符合全球政策。这些政策是由一个多方利益相关者社群制定的，这一社群

具有非常广泛的代表性，包括了面向全球的互联网社群，从域名注册商等中小企业到普通的互联网用户，从技术人员、政府、学术界到民间机构。各利益相关方都能够参与其中，表达自身的利益诉求，通过共识合作解决政策和技术挑战。

ICANN 成立之后，其多利益相关方体系不断完善，从最初的 GNSO、CCNSO、ASO 等支持组织不断发展壮大，为另一些利益相关方群体设立咨询委员会，使他们能在 ICANN 中找到位置，如政府咨询委员会 (GAC)、用户咨询委员会 (ALAC)，安全与稳定咨询委员会 (SSAC) 等相继成立。

国际互联网协会 (ISOC)

国际互联网协会 (Internet Society, 简称 ISOC) 于 1992 年成立。ISOC 组织的使命是“保证开放发展、进化和使用互联网，造福全世界所有人”。它的成员包括个人 (任何人都可以加入) 以及公司、组织、政府和大学。提出成立 ISOC 的构想最早源于 1991 年 6 月在丹麦首都哥本哈根举行的国际网络会议上。创立者希望通过成立一个全球性的互联网组织，使其能够在推动互联网全球化，加快网络互连技术、应用软件发展，提高互联网普及率等方面发挥重要的作用。ISOC 作为一个非政府、非赢利的行业性国际组织，迄今已拥有来自全世界各地的 100 多个组织成员和 20,000 名个人成员。它同时还负责互联网工程任务组 (IETF)，互联网结构委员会 (IAB) 等组织的组织与协调工作。

1.2.2 互联网国际社群动态

IETF 首次组建 DNS 技术标准评审专家委员会

2022 年，作为全世界最重要的互联网技术标准机构，IETF 组建 DNS 技术标准评审专家委员会，这是 IETF

自成立以来首次组建聚焦于 DNS 技术标准的专家委员会，并面向全球遴选了 22 名 DNS 领域技术专家。专家委员会主任由亚太互联网信息中心（APNIC）首席科学家 Geoff Huston（澳大利亚）和 DNS 资深专家 Jim Reid（英国）担任。

IETF 此次成立的 DNS 技术标准评审专家委员会，将负责审阅 IETF 范围内不同领域（以及工作组）所有和 DNS 技术相关的互联网标准草案。这是 IETF 首次面向单一技术（协议）成立专门的标准评审专家委员会。互联网域名系统国家工程研究中心（ZDNS）首席研究员入选专家委员会，以中国专家身份为全球互联网发展贡献中国智慧。

第 55 届 APNIC 社群会议

2023 年 2 月 27 日，第 55 届亚太互联网络信息中心（APNIC）社群会议暨 2023 年度亚太网络运行技术大会（以下简称“大会”）在菲律宾首都马尼拉召开。APNIC 社群会议每年召开两次，每年年初的会议又称“亚太网络运行技术大会”（APRICOT）。参会人员包括：来自全球的互联网国际组织社群领袖、技术专家、从业人员等，共同探讨互联网码号资源的分配政策、运行技术、互联网治理等话题，并以此作为亚太地区网络互联互通协调机制的参考依据。互联网域名系统国家工程研究中心（ZDNS）首席研究员、APNIC 路由安全 SIG 主席马迪出席大会，作为 SIG 主席主持了本次会议期间 APNIC 路由安全论坛，并代表 APNIC 路由安全 SIG 向 APNIC 全体大会报告论坛情况。

第 76 届互联网名称和数字地址分配机构（ICANN）大会

2023 年 3 月 11-16 日，第 76 届互联网名称和数字地址分配机构（ICANN）大会在墨西哥坎昆召开。本次会议以线上 + 线下的形式举办，共计吸引了来自 164 个国家和地区的 2019 名与会者出席此次大会。全球各国

研究机构、技术社群、企业代表共聚一堂，探讨互联网治理相关话题。作为核心议题之一，大会披露了关于第二轮顶级域名开放的最新进展。会中，ICANN 董事会通过了《新通用顶级域名后续程序政策制定过程最终报告》中包含的 98 项建议，并要求 ICANN 组织在 2023 年 8 月 1 日前提交第二轮顶级域名开放时间表。

ICANN 董事会主席特里普蒂 · 辛哈（Tripti Sinha）表示：“我们必须共同努力，确保互联网的弹性、安全性和未来。我们需要共同投入必要的资源和努力来解决棘手的问题，实现我们推出下一轮顶级域名的共同目标。而这需要 ICANN 社群、董事会和组织之间的紧密合作。”

国际互联网协会预计 2023 年底将有超过 50% 的网络支持 RPKI

国际互联网协会（ISOC）互联网技术高级经理阿夫塔布 · 西迪基（Aftab Siddiqui）发文展望了资源公钥基础设施（RPKI）部署态势。阿夫塔布指出，全球互联网路由生态系统面临的安全威胁，（如边界网关协议（BGP）事件）不断增多，但这些威胁大多可以通过实施 MANRS 中列出的 RPKI 部署应用行动措施加以应对。全球路由表中 41.7% 的路由具有有效的路由起源授权（ROA），同比增长约 10%，预计到 2023 年年底将有超过 50% 的网络支持 RPKI。其中，欧洲和南美地区当前 RPKI 部署率较高，分别为 56% 和 45%；MANRS 近 900 家参与方中，约有 66.4% 的机构具有有效的 ROA，高于全球平均水平。阿夫塔布表示，MANRS 社群需要继续举办教育培训活动向全球推广 RPKI，同时提升 IP 地址资源持有者对其 ROA 有效性管理的意识，通过改善网络路由安全提升互联网的安全性和可靠性；他也对网络运行机构实施自治系统提供商授权（ASPA）、边界网关协议路径验证（BGPsec）等路由安全技术表示支持与欢迎。

全球 48 个国家 / 地区举办首届普遍适用日活动

为响应首个普遍适用日（UA 日）倡议，48 个国家 / 地区于 2023 年 3 月 28 日前后举办了 56 场宣传推广和技术培训活动，以促进新通用顶级域（gTLD）和多语种域名（IDN）在全球范围的普遍适用（UA）。 “UA 日”由 ICANN 及 UASG 主导设立，旨在吸引和动员全球技术和语言社群、企业机构、政府部门和国际组织、教育

和科研机构及 DNS 行业主体等利益相关方更好地了解 UA 的益处并推动相关系统支持 UA，助力实现一个支持广泛语言和文字的更具包容性的互联网，促进下一个十亿用户上网。

（以上部分内容参考了中国信息通信研究院《国际互联网基础资源政策动态》）

第三节

网络空间治理 · 中国思考

勇立时代潮头，以坚决打赢信息领域核心技术攻坚战推动高水平科技自立自强

科技是国家强盛之基，创新是民族进步之魂。当前，以互联网为代表的新一代信息技术加速迭代，创新性、渗透性、引领性日益彰显。只有把信息领域核心技术牢牢掌握在自己手中，才能赢得未来发展和竞争的主导权。党的二十大报告提出，到 2035 年我国要“实现高水平科技自立自强，进入创新型国家前列”，强调要“以国家战略需求为导向，集聚力量进行原创性引领性科技攻关，坚决打赢关键核心技术攻坚战”。迈向新时代新征程，我们要始终把创新作为第一动力，坚定不移实施创新驱动发展战略，聚焦信息领域关键核心技术，加快体系化突破，尽快甩掉“卡脖子”的手，努力实现高水平科技自立自强。要加强前沿技术布局，紧紧围绕国家战略需求，加强人工智能、量子信息、集成电路、区块链等重点领域技术突破的总体布局，研究制定前沿技术攻

关路线图，加快推动一批关键核心技术研发突破，着力构建自主可控、安全可靠的信息技术体系。要提升协同攻关能力，充分发挥我国大国大市场优势和全产业链创新应用环境优势，强化国家战略科技力量作用，引导各类要素资源向技术创新领域流动，鼓励龙头企业、高等院校、科研院所组建创新联合体，加强资源共享和协同研发攻关，建立具备全球领先创新力和竞争力的现代信息技术产业体系。要完善创新保障机制，加大对基础学科支持力度，打通信息领域基础研究和技术创新衔接的绿色通道，改革网信人才激励机制和科技评价机制，完善创新投入机制和科技金融政策，推动创新链产业链价值链人才链深度融合，更好释放各类主体创新创造活力。

筑牢安全屏障，以维护网络安全和数据安全促进国家网络安全体系和能力现代化

国家安全是民族复兴的根基，社会稳定是国家强盛的前提。当前，全球范围内网络安全威胁和风险日益突出，针对关键信息基础设施的网络攻击活动时有发生，5G、人工智能、区块链等新技术新应用快速发展带来新的安全隐患，个人隐私数据过度采集和泄露问题突出，维护网络安全和数据安全的重要性和紧迫性更加凸显。党的二十大报告设立专章对“推进国家网络安全体系和能力现代化，坚决维护国家安全和社会稳定”进行深刻阐述，并将强化网络、数据安全保障体系建设作为健全国家网络安全体系的重要内容。迈向新时代新征程，我们要深入贯彻落实总体国家安全观，全面加强网络安全和数据安全保障体系和能力建设，有效防范和化解各类风险。要加强关键信息基础设施安全防护，严格落实网络安全工作责任制，健全关键信息基础设施安全保障体系，持续提升网络安全态势感知、监测预警、风险评估、事件处置等能力。加大金融、能源、电力、通信、交通等重点行业领域信息基础设施网络安全检查力度，加强工业互联

网、车联网等新型融合领域基础设施安全保障。要强化数据安全和个人信息保护，完善数据管理制度体系，建立健全数据安全管理、风险评估、检测认证等机制，压实网络平台主体责任，强化重要数据安全保护。实施数据出境安全评估制度，发挥国家网络安全审查作用，保障数据安全有序流动。深入整治违法违规收集使用个人信息等行为，切实维护广大网民信息安全和合法权益。要夯实网络安全工作基础，推动网络安全教育技术产业融合发展，推进国家网络安全人才与创新基地建设，加快创建世界一流网络安全学院。完善支持网络安全企业发展的政策措施，培育扶持一批具有国际竞争力的龙头企业。健全常态化宣传教育体系，办好国家网络安全宣传周，不断提升全民网络安全意识和防护能力。

——节选自中央宣传部副部长、中央网络安全和信息化委员会办公室主任、国家互联网信息办公室主任庄荣文在《中国网信》2023年第1期上发表的文章《以网络强国建设新成效助力全面建设社会主义现代化国家新征程》

推进全球网络空间治理的中国路径

全球网络空间治理正处在“建章立制”的关键阶段，中国在其中发挥了负责任大国的重要作用。通过有序推进网络空间合作，不断践行网络空间治理的“中国路径”，为构建网络空间命运共同体作出贡献。

一是加强国际协调。纵观全球治理的发展历程，国际协调至关重要。国际关系尤其是大国之间的关系在很大程度上决定了全球治理的权力基础，国际协调在很大程度上体现了治理的领导力，能够缓解全球治理的集体行动

困境。

在全球网络空间治理领域，中美俄欧等主要大国和地区之间的协调尤为重要。无论是在战略层面还是战术需求层面，各方都有展开合作的必要性和可能性。

维护网络空间稳定与促进网络空间发展符合各国的共同利益，应对共同的非传统安全威胁是各国的共同责任，各国在技术和经济领域也存在较强的互补性和依存性。通过加强国际协调，可以增强全球网络空间治理的领导

力，促进网络空间治理的发展。

二是加强数字经济合作。2020年以来，新冠肺炎疫情对全球经济产生了重大冲击，各国经济深受重创，主要大国经济复苏乏力。尽早实现经济复苏是世界各国的当务之急。近年来，数字经济的快速发展已经成为世界经济增长的新动能。全球金融、能源、高端制造、智慧城市以及新型基础设施建设都离不开数字技术的赋能。在数字经济领域加强合作，不仅可以降低网络空间生产的脆弱性，更是推动全球经济复苏的重要动力。为此，需要改善网络空间的供应链等问题，在跨境数据流动方面完善规则，切实加强各国之间的数字经济合作。

三是加强网络安全合作。网络安全合作涉及从打击网络犯罪到维护网络空间战略稳定等多个层面。

首先，在打击网络诈骗、网络黑客、网络色情传播等网络犯罪方面，各国存在较大的合作基础，能够逐渐积累网络安全合作的经验与信任。

其次，在网络攻击方面要形成互不攻击的共识。由于在网络空间中的行为主体具有匿名性和难以溯源性等特点，很难区分相关恶意行为的真正实施主体。正是基于网络空间的这些显著特点，任何一个国家都很难单独应对网络空间安全威胁，确立互不进行网络攻击的原则至关重要。

再次，要维护网络空间战略稳定。网络空间既具有虚拟性，也和物理空间紧密联系。维护网络空间战略稳定，需建立网络安全预防、稳定和信任机制，以在危机和冲突过程中可以有效控制，避免破坏稳定。

四是加强网络基础设施建设。全球网络治理面临的数字

鸿沟问题需要逐步解决，让广大发展中国家更多受益，真正推动网络空间命运共同体的实现。

习近平主席在第二届世界互联网大会开幕式上的讲话中指出：“网络的本质在于互联，信息的价值在于互通。只有加强信息基础设施建设，铺就信息畅通之路，不断缩小不同国家、地区、人群间的信息鸿沟，才能让信息资源充分涌流。”因此，国际社会要加大对全球网络基础设施建设的资金投入，帮助发展中国家改善网络基础设施，让发展中国家能够更加公平地参与全球网络空间治理。

五是完善网络空间规则制定。网络空间技术的不断发展，使得网络空间治理的规则需要不断被完善。目前，国际社会在网络空间治理规则方面的进展比较缓慢，尚不具备有效监督网络行为和强制执行的能力，达成网络空间国际规范存在技术与法律等方面的障碍。

鉴于各国利益诉求以及网络技术发展水平等方面的差异性，国际社会网络空间治理规则的制定推进需要循序渐进。在防范网络恐怖主义、打击网络犯罪等全球公共问题上寻求突破口，不断积累网络空间治理的经验与共识。

此外，在规则实施空间方面，也可以推动双边、地区网络空间治理规则在更大空间实施。总之，全球网络空间治理任重道远，变“规则之争”为“规则共识”仍然需要经历漫长过程。

——节选自外交学院院长、研究员徐坚，外交学院国际关系研究所副所长、副教授凌胜利发表在《中国网信》2023年第1期上的文章《全球网络空间治理的中国作为》。

第四节 |

网络空间治理 · 中国贡献

互联网基础资源技术协议利用公钥信任链加强安全

如何提高互联网技术协议的安全是 IETF 长期研究的重点议题。IETF 互联网基础资源技术协议从默认信任数据转向保障数据来源可信、数据完整和防篡改等方向发展。

(一) 域名系统协议利用公钥信任链加强安全

域名系统协议（DNS）是互联网的核心协议，是一种将域名映射为某些预定义类型资源记录（如 IP 地址）的分布式互联网服务系统。作为一种互联网应用层的资源寻址基础服务，域名服务是其他互联网络应用服务的基础。常见的互联网络应用服务如网页远程访问服务、电子邮件服务、文件远程访问服务等一般都以域名服务为基础，实现资源的寻址和定位。

互联网技术前辈在 1983 年推出 DNS 的时候没有深入考虑数据安全问题，因此 DNS 协议存在天然安全缺陷。DNS 的原始协议是一种轻量级协议，它不能对服务数据内容提供安全保证。DNS 数据在互联网上以明文方式进行传输，数据在传输过程中很容易遭到劫持或篡改。由于 DNS 协议本身不提供数据内容的完整性保护机制，接收方无法判别接收到的消息是否遭到篡改以及来源是否正确。此外，DNS 协议的实现通常以用户数据报协

议（UDP）为基础，缺乏通信的可靠性保证，这进一步增加了消息篡改或伪造的可能性。例如，自 2008 年以来广受互联网界关注的 Kaminsky 漏洞，就是利用 DNS 协议的这一安全缺陷，伪造 DNS 的请求及响应数据包，使递归服务器缓存并向外应答错误的 DNS 数据（即所谓的 DNS 缓存中毒）。正是由于 DNS 协议所暴露出来的以上安全缺陷，促使 IETF 推出了 DNS 安全扩展协议（DNSSEC）。

DNSSEC 协议是一个针对 DNS 协议的安全扩展，它通过给 DNS 的应答消息添加基于非对称加密算法的数字签名，保证数据未经篡改且来源正确；再通过域名体系自下而上逐级向父域提交自己公共密钥，实现整个域名体系的逐级安全认证。DNSSEC 为 DNS 数据提供了三方面的安全保障：一是数据来源验证，保证 DNS 应答消息来自被授权的权威服务器；二是数据完整性验证，保证 DNS 应答消息在传输途中未经篡改；三是否定存在验证，当用户请求一个不存在的域名时，DNS 服务器也能够给出包含数字签名的否定应答消息，以保证这个否定应答的可靠性。

综上所述，DNSSEC 本质上是在域名系统树型授权体

系的基础上，再建立一套基于密码学手段的签名 / 验证体系，也就是信任链体系，通过信任链上的逐级安全验证，确保 DNS 查询结果的真实可靠性、数据完整性和非否认性。

互联网名称与数字管理机构（ICANN）一直在全球推进 DNSSEC 的部署，2010 年 7 月，ICANN 正式用 DNSSEC 签署根域。为了更好地管理根密钥，ICANN 制订了根密钥管理计划。该计划在全球选择信任社区代表（TCR），负责生成管理根密钥。ICANN 一共选出 21 名 TCR 和一些后备 TCR，所有的候选人都来自互联网社区的个人。其中 14 名 TCR 是密码管理员（CO），美国东海岸和西海岸各 7 名，负责参与生成根密钥。另外 7 名 TCR 是恢复密钥持有人（RKSH），负责硬件安全模块（HSM）内容的备份和管理，用于紧急状态时候恢复 HSM 工作状态。2010 年 6 月，在美国弗吉尼亚州的库尔佩珀（Culpeper）召开了全球第一次 DNSSEC 根密钥生成仪式会议。

ICANN 有两套完全相同的 HSM，分别放在美国东海岸和西海岸，用于根密钥的生成。启动 HSM 的密钥由 CO 保管。根密钥生成仪式，轮流在东西海岸进行。如果 HSM 出现问题或者根密钥出现紧急情况，需要 RKSH 赴美恢复 HSM，重新恢复根密钥。根据 ICANN 制定的根密钥管理规则，没有 TCR 的参与，ICANN 是无法生成根密钥的。通过 TCR 的参与生成和管理根密钥，使 ICANN 的根密钥生成管理更加透明，形成了全球参与根密钥生成管理的局面。

DNSSEC 机制利用公钥信任链机制构建了可信的域名查询体系，全球根服务器中的互联网顶级域名数据需要利用根密钥进行签名，保证数据的安全可信。DNSSEC 只是保证了 DNS 数据的可信性，但是，并没有对 DNS 数据本身进行加密。

（二）资源公钥基础设施协议通过公钥信任链应对路由通告伪造问题

作为支撑互联互通的互联网基础设施，域名系统和域间路由系统对互联网的安全有着至关重要的影响。由于边界网关协议（BGP）缺乏对路由通告内容真实性的保证，因此黑客的蓄意攻击以及错误的网络参数配置都可以导致路由劫持现象的发生。路由劫持对互联网的正常运行影响极大，可能导致大面积的网络瘫痪。于是，IETF 提出了资源公钥基础设施（RPKI）协议。RPKI 的概念最早便诞生于描述安全边界网关协议（S-BGP）方案的论文中。S-BGP 提出了一种附加签名的 BGP 消息格式，用以验证路由通告中 IP 地址前缀和传播路径上自治域（AS）号的绑定关系，从而避免路由劫持。基于这样的设计，数字证书和签名机制被引入 BGP 范畴，并利用了公钥基础设施（PKI）。为验证路由通告签名者所持有的公钥，该签名者的 IP 地址分配上级为其签发证书，一方面，验证其公钥，另一方面，验证该实体对某个 IP 地址前缀的所有权。基于 IP 地址资源分配关系而形成的公钥证书体系，RPKI 的基本框架就此形成。

RPKI 体系由三大关键模块组成：基础资源公钥证书体系（RPKI）、数字签名对象、储存 RPKI 签名对象的分布式 RPKI 资料库。这三大模块能够确保一个实体验证谁是某个 IP 地址或者 AS 号码的合法持有者。RPKI 可以使 IP 地址的合法持有者授权某个 AS 作为该地址的路由源，并进行验证。这种可以验证的授权，可以用来构建更加安全的路由表过滤项。

为了推动 RPKI 的部署，RPKI 架构充分利用了现有的技术和实践。RPKI 的结构可与现有的资源分配体系对应，可以看作是目前资源管理组织运行模式的自然技术延伸，而且现有的资源分配和回收方式在这套新体系中都有明确的相关定义。

(三) 传输服务协议通过公钥信任链应对域名证书伪造和客户端认证问题

互联网上用于安全认证的证书一般由被称为认证机构(CA)颁发。然而, CA模型比较容易受攻击, 在互联网上受信任的CA有成千上万个, 这些CA在理论上可以颁发任何一个证书。一个CA可能存在恶意颁发或者错误颁发不属于互联网域名使用者的证书, 从而形成中间人攻击, 造成互联网安全的隐患。IETF在RFC6698技术标准中提出了基于DNS的名字实体认证协议(DANE)技术, DANE可以通过称为传输层安全认证(TLSA)的DNS资源记录进行域名证书的认证和颁发, 使只有控制域名的实际控制人才能颁发相应域名的安全证书, 保证了TLS证书的安全。DANE使用DNSSEC基础设施存储和签署密钥, 以及TLS使用的证书。DANE提供了将公钥绑定到DNS域名的机制。由于管理公钥数据和管理DNS域名的实体是同一个, 减少了利用域名进行中间人攻击的机会。与域名关联的密钥只

能由该父级域名密钥签名与关联。例如, “example.cn”钥匙只能由“cn”的密钥签名, “cn”的密钥只能由DNS根钥匙签名。任何域名的签名密钥都可以通过使用标准DNSSEC协议查询和分发签名密钥, 通过DANE可以部署用户自签名证书。原本自签名证书被认为是不安全的, 但是通过DNSSEC的加持, 针对域名自有域名的自签名证书在DANE里可以安全使用。

2021年, IETF又成立了网络客户端DANE认证(DANCE)工作组, 利用DANE加强网络客户端相关协议的安全。目前, 相关技术标准正在制定过程中。各种传输服务协议可以通过DANE机制中的公钥信任链应对域名证书伪造和客户端认证问题, 使通信更加安全。

——节选自: 中国互联网络信息中心(CNNIC)研究员姚健康发表在《中国信息安全》杂志上的文章《互联网基础资源技术协议的安全发展趋势》

BGP架构原则下的“自治”方案

总结DNS滥用的政策发展, 主要存在三个争论点: 技术滥用与内容、自上而下与自下而上, 以及责任与义务。互联网的“网”是点与线交织而成的, “点”是不同的自治体, “线”是他们中间的商业关系。这个概念可以影响上述三个DNS滥用的争论点。

我们如果引入BGP架构原则和概念, 或许可以破解以上三个DNS滥用的争论点。

DNS滥用的现实操作涉及三方: 滥用者、中介和监管机构。现行的政策讨论集中在监管机构(如ICANN)

的框架下, 产生自上而下的规管压力。如果要贯彻自治的原则, 则必须在滥用者或中介层面进行操作。

显然, 滥用者不可能自我完善, 否则就不会存在滥用行为。故此, 需要衡量中介是否能采取有效自治措施制止DNS滥用的发生, 以及监管机构如何鼓励并进行有效的自治。如果能满足这两个条件, 自治就可以成为良好的互联网治理元素。

“自治”破解“技术滥用与内容治理”

如果在DNS滥用的议题上确立“自治”原则, 则有望

缓解“技术滥用与内容治理”的争议。支持限制技术滥用一方的主要论据，就是要避免从上而下的硬性规定破坏了言论自由和弹性。DNS 滥用议题被重视，正是因为现行的“自治”方法存在漏洞。因此，需要解决如何鼓励监管机构进行有效的“自治”问题。

中介“自治”让“责任与义务”更明晰

“自治”原则下建立的体制并不是基于法律责任和风险，而是基于义务。在现实环境中，中介投放至 DNS 滥用的资源实质上是一种商业考虑，包括投诉量、反投诉量、投诉方的影响力、政府压力、盈利、自身客户群的反应等。

从商业角度看，DNS 滥用可以理解为一种成本转嫁。出于商业考虑的互联网中介（如注册商）将投入适当的成本，建立自身的法规并处理投诉，如草拟的域名滥用框架（DNS Abuse Framework）倡议提出的“可信通知者”机制，可以应对 DNS 滥用问题。通过建立切实的商业关系并定义各方的责任，中介在这种架构下可维持本身的自治权力，保持治理的弹性，提高治理效率。

——节选自：泛息企业管理咨询（CSC）大中华区总经理关奕斌发表在《中国信息安全》杂志上的文章《从域名系统滥用看互联网治理模式的利与弊》

下一代 DNS 助力中国品牌国际化

随着新一代信息技术的应用及发展，作为互联网第一“入口”的域名，由最初的技术解析符号发展成为互联网关键基础资源，它具备多种属性，是企业 / 城市品牌文化、商业价值及战略意义的重要体现。

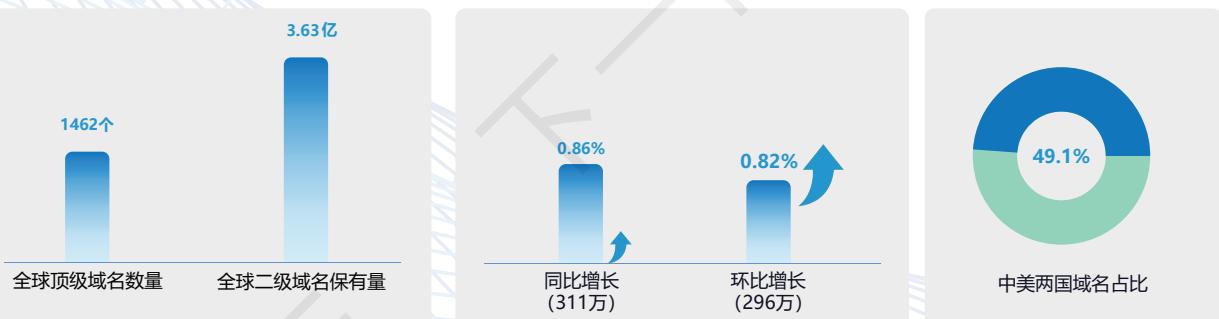
第一节 | 全球域名发展统计报告

根据《全球域名发展统计报告》，对顶级域名全球市场、顶级域名中国市场、国际化顶级域名全球市场、新通用顶级域名全球市场、域名系统 IPv6 支持情况、域名服务性能与安全情况等进行了统计与分析，旨在为相关政府管理机构、域名注册管理机构（注册局）、域名注册服务机构（注册商）、域名注册人与从业人员，以及其

他对域名行业感兴趣的公众提供域名行业发展最新数据分析，以促进行业发展。

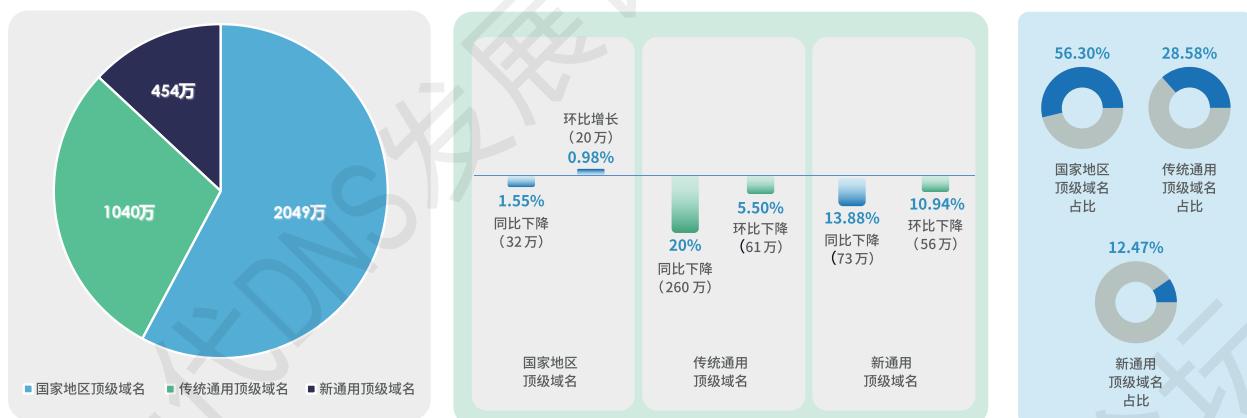
截止到 2023 年 7 月，全球顶级域名数量为 1462 个，保有量达 3.63 亿，同比增长 0.86% (311 万)，环比增长 0.82% (296 万)。中美两国域名总量约占全球域名量一半：49.1%。

全球域名情况



截止到 2023 年第 1 季度末，中国市场域名保有量为 3542 万，同比下降 9.35%（365 万），环比下降 2.65%（96 万）。中国国家与地区代码顶级域名（ccTLD）中最大的 .CN 与 . 中国域名保有量为 2049 万，占中国域名保有量的 56.30%，同比下降 1.55%（32 万），环比增长 0.98%（20 万）。中国传统通用顶级域名（Legacy

gTLD）保有量为 1040 万，占中国域名保有量的 28.58%，同比下降 20.00%（260 万），环比下降 5.50%（61 万）。中国新通用顶级域名（New gTLD）保有量为 454 万，占中国域名保有量的 12.47%，同比下降 13.88%（73 万），环比下降 10.94%（56 万）。



第二节

顶级域名现状及趋势

以顶级域名这一互联网关键基础资源为例，互联网名称与数字地址分配机构（ICANN）于 2012 年 1 月首次开放申请新通用顶级域名，这被称作互联网有史以来最大的变革。在这场变革中，中国企业仅有少数参与其中。彼时中国正迎来“互联网+”的融合时代，促进互联网技术与不同行业深度融合，催生了电商、O2O 等创新商业模式。

根据 ICANN 数据，自 2012 年 1 月首轮新通用顶级域名申请项目启动至 2012 年 5 月申请窗口关闭，共有来自全球 58 个国家和地区的 1930 个新通用顶级域名申请。其中，欧美地区共申请新通用顶级域名 1585 个，中国（含港、澳、台）共申请了 86 个，其申请量仅为欧美地区的 5.4%。

尽管只有短短 4 个月的开放时间，国外互联网巨头、城市政府、金融行业等对此的投入令人瞠目：谷歌在首轮申请中共申请 101 个，最终成功获批 46 个顶级域，包括：.google、.new、.gmail、.谷歌等。谷歌对顶级域名的战略性占有并未就此止步。2015 年前后，在移动互联网的推动下，手机应用软件强势入场，洞察行业趋势变化，谷歌斥资 2500 万美元（约 1.8 亿元人民币）拍下.app 后缀，APP 这一可以概括包括手机端、电脑、云端等各种应用的名称被谷歌以顶级域名的方式收入囊中。

电子商务公司亚马逊在首轮中，成功申请了 55 个顶级域名，包含了通用词和品牌词如：.amazon、.亚马逊、.家电、.食品、.book、.buy 等；2021 年，亚马逊广告业务正式启用了 ads.amazon，其他产品线也陆续启用，如：prime.amazon、kindle.amazon 和 alexa.amazon 等。设立在每一个顶级域名 (.amazon) 之下的二级域名，已经成为亚马逊一个庞大的子业务体系，亚马逊早已不仅仅是电商平台。

除此之外，启用顶级域名的还有：英国巴克莱银行、法国巴黎银行、德意志银行、安盛保险等金融机构；宝马、宾利、大众、丰田、兰博基尼、奥迪等知名车企；苹果、索尼、三星、佳能、飞利浦等全球电子行业头部企业。除了企业与机构，以城市命名的顶级域名也已应用，如东京、纽约、伦敦、巴黎、柏林等城市。

纽约是美国第一个获得顶级域名的城市，时任纽约市长布隆伯格在声明中称：“拥有我们自己的、独一无二的顶级域名 .nyc，可以让纽约市行进在数字世界的前沿，并为我们的企业创造新的商机。他们可以将自己与纽约市这个全球著名的城市联系在一起”。

2.2.1 顶级域名属性分析

品牌聚焦，万象归一

拥有自身品牌顶级域名的组织可以将自身 brand.com/brand.net/brand.cn 等不同域名升级统一到 .brand。企业、品牌与域名三者高度统一可以直接提高品牌的认知度、辨识度、可信度，树立良好品牌形象，是品牌全球化的重要载体。

独家专享，全球唯一

每个顶级域名在全世界具有唯一性和排他性。在全球范围内，如果一个顶级域名被成功申请，其他任何机构都无权再申请相同字符的顶级域名。全球唯一、先到先得的属性决定了其互联网核心稀缺资源的地位，是数字化时代的重要品牌资产。

核心资产，自由分配

自由分配顶级域名下优质二级域名资源，助力品牌在专属网络空间进行集团化管理和子业务建设，并保证全球业务品牌形象统一。此外，可以按照企业和组织的发展需求注册域名，减少精品词汇回购成本。通过申请行业词后缀，可以分配旗下二级域名，整合上下游产业链，为行业体系建立专有网络身份。

自主可控，安全可信

由于历史原因，23 个通用顶级域名主要由美国机构运营管理。新通用顶级域名不依附于其它顶级域名，风险可自控，不受其它组织影响。顶级域名持有方可以直接从顶级域名层面管理、统筹域名的使用，掌握新技术升级的主动权，域名数据的安全性也更有保障。

2.2.2 顶级域名应用新趋势

数字品牌被赋予了丰富的内涵与外延，在全球经济格局下成为数字时代新命题，如何在网络空间建立鲜明品牌标识、保持安全的流量入口，以及建立数字资产维护体系，是中国品牌崛起以及稳健发展的前提。

(1) 顶级域名正成为互联网品牌自主可控的重要抓手

随着数字化的深入发展，业务线上化、交易线上化，尤其是在券商、银行等金融领域，大量的业务都在线上完成，网络安全、品牌突出性尤为重要。互联网品牌的自主可控来自于两个方面：

一是通过顶级域名，可以构建自主网络空间的安全领地。在顶级域名未开放之前，企业只能注册二级域名，顶级域名的管理权并未在本国，其安全性和自主性受到限制。当线上业务已经成为数字社会的常态，如何实现更加安全且自主可控的品牌，已经成为战略级事项。通过顶级域名的获取实现互联网品牌的安全性，逐渐在全球形成共识。

二是多数跨国经营的企业采用的是各个国家域名相加的方法，注册一个非常长的域名，品牌特点被削弱。顶级域名给企业带来了新的可能性和新的机会，企业有可能通过顶级域名实现自主可控的品牌传播增长。

(2) 顶级域名是企业重要数字资产

智能终端充斥在社会各个角落，让我们的生活更便捷、更高效，越来越多人使用APP等互联网应用，互联网碎片化的出现，网络平台越来越多，一旦无法访问会对企业的正常运营和品牌形象产生严重的影响。无论物联网、智能终端如何发展，顶级域名作为基于国际标准的、开放的互联网设施，是存在于网络上的数字资产。

(3) 顶级域名或许是下一轮一流品牌胜出的关键

全球数字经济是开放和紧密相连的整体，在合作共赢、释放数字活力的同时，需关注互联网基础资源层在数字化进程中的发展与演变。互联网关键基础资源——顶级域名，在数字化进程中体现出数字资产价值和对互联网安全管理的重要作用，也是发挥中国品牌整体优势的重要抓手。

全球数字化浪潮下，从中国制造到中国创造，从中国产品到中国品牌，中国在科技创新发展方面与欧美间的差距正逐渐缩小，但仍然面临诸多挑战与考验。其中，打造中国品牌的持续增长能力是关键之一。历史上，每一次技术变革都会催生新的世界一流品牌，在数字经济浪潮下，能否将在数字化转型过程中累积的优势资源转化成企业的强势品牌资产，成为下一轮一流品牌胜出的关键。

(4) 中国品牌向全球展现的数字通道

万物互联、万物智能，主动触达无处不在，对于品牌的涵义已经不仅仅是品质特征和文化内涵的展现，还意味着超越地域空间范围建立的更泛在的品牌链接与话语体系，这是全球品牌共同面临的现状。对中国品牌而言，重塑数字时代的品牌逻辑，是来自于国际竞争与国内经济发展的双重需求。

数字经济的发展让全球经济结构更加扁平化，令品牌引领高质量发展成为必然。全球数字化带来高效、便捷沟通方式，国家与地区被网络连接在一起，网络形象、网络话语体系占据外界了解品牌的第一入口。在互联网上有所展现的城市、企业，无形中均被赋予了一张“数字名片”。一方面，“数字名片”为更多中国品牌打开国际市场空间；另一方面，也意味着中国品牌置身于更为严峻的市场挑战之中。除了产品在市场上正面交锋，中

国品牌与海外品牌在全球均等的资源占有方面，也站在了同一起跑线。在2012年第一轮顶级域名开放中，谷歌、亚马逊等国际互联网巨头公司已经提前布局，中国企业甚少参与。十年间，中国数字产业化、产业数字化的程度均已大幅提升，对居于全球资源分配格局下的顶级域名，也将是中国品牌向全球展示的数字通道。

(5) 网络知识产权新属性

知识产权从线下延伸至线上，域名是网络知识产权的重要组成部分，越来越多的企业开始意识到网络知识产权的重要性。顶级域名可以保护企业的网络知识产权权益，提升数字品牌的国际影响力。随着互联网、数字科技和人工智能的不断发展，知识产权及商标品牌的内涵和外延也在不断延伸。要适应行业的新属性、新特点。域名和商标有着相似的识别功能，也是品牌在网上的重要体现形式之一。域名属于网络品牌和网络知识产权的范畴，越来越多的机构、企业意识到加强数字品牌建设的重要性，这将有助于提升企业的商标品牌网络保护水平。

2.2.3 顶级域名全球市场概览

截至2023年7月10日，注册量前十的新通用顶级域名为.xyz、.online、.top、.shop、.site、.store、.vip、.live、.app和.club。

(1) 通用类运营情况

截至2023年7月10日，运营中的通用类新通用顶级域名（简称：通用类）共572个，包括各类行业、职业、新闻、科技、贸易等众多社会经济领域，通用类是为了满足不同领域的用户需求，建立独立的在线互动交流平台。

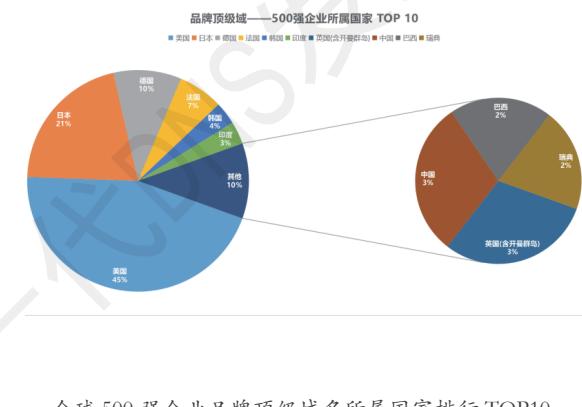
(2) 品牌类运营情况

品牌类新通用顶级域名（简称：品牌类）仅面向企业内部使用，不对公众开放。拥有独立的品牌顶级域名不仅有助于保护企业无形资产，塑造企业全球品牌价值，同时有助于建立专有网络身份，增加用户信任关系。

根据ICANN公布的名单，品牌类是首轮新通用顶级域名申请中的主力军，申请数量为606个，约占总申请数的31%。

截至2023年7月10日，运营中的品牌类共506个，如.walmart、.microsoft、.unicom、.联通、.中信、.citic、.amazon、.google和.baidu等，占运营中的新通用顶级域名总数的45%。

截至2023年7月10日，100家世界500强企业运营着182个品牌顶级域名，并积极通过顶级域名推广旗下产品与服务，例如沃尔玛、亚马逊、苹果、三星、谷歌、微软、宝马、沙特阿拉伯国家石油公司、汇丰、安盛保险、耐克、辉瑞制药、中国工商银行、联通集团、中信集团和阿里巴巴等。



(3) 地理类运营情况

在首轮申请的新通用顶级域名中，目前运营中的地理类新通用顶级域名（简称：地理类）共 52 个。

地理类运营分布

地区	运营数量	所占比例
欧洲	28	53.85%
亚太	15	28.85%
北美	5	9.62%
非洲	4	7.68%

在地理类方面，欧洲表现出了极大的主动性，目前有 28 个地理类处于运营状态，尽管在亚太地区运营的地理类数量超过北美，但中国（含港、澳、台）只有 3 个。

地理类中，12 个是首都城市，其他也多为经济、贸易或旅游等国际化大城市，如纽约、迈阿密、波士顿和悉尼等。地理类的申请有助于推动其当地经济的发展，促进城市发展、内部沟通以及本土文化的保护与推广。地理类也多为开放型顶级域名，允许企业、个人、团体和组织注册与使用，旨在服务本地居民、企业以及商旅客。同时，地理类也成为各个城市的数字品牌，成为全球互联网城市名片。地理类中，二级域名保有量排名前五的分别是.tokyo(东京)、.africa(非洲)、.nyc(纽约)、.berlin(柏林) 和 .london(伦敦)。其中，排名第一的.tokyo 是目前世界上运用最广泛的地理类顶级域名，其运用范围已覆盖到东京生活的方方面面，包括东京地铁 findmy.tokyo，东京银座购物中心 ginza6.tokyo 和东京马拉松的官网 marathon.tokyo 等；.africa 运用范围覆盖到非洲的各个领域，包括为公众提供法律支持的 aln.africa，金融服务的 mchanga.africa 和非洲 DNS 分论坛的官网 dnsforum.africa 等。

(4) 国际化域名 (IDN) 运营情况

IDN 尤其是中文域名取得的成就对多语言互联网的发展至关重要。拉丁字符（英文简称 ASCII）作为首轮申请的主流，申请数量为 1814 个。截至 2023 年 7 月 10 日，运营中的 ASCII 新通用顶级域名数量为 1039 个，占据运营总量的 92%；IDN 申请数量为 116 个，运营中的数量为 91 个，所占比例约为 8%。

截止到 2023 年第 1 季度末，全球共有 91 个国际化通用顶级域名 (IDN gTLD)。在全球域名保有量排名前十的 IDN gTLD 中，有 9 个是中文顶级域名，依次为 .网址、.在线、.公司、.手机、.商城、.商标、.网络、.中文网、.我爱你。

截至目前，中文新通用顶级域名由来自 8 个国家和地区的 35 个机构运营，总数量为 52 个，占全球运营中 IDN gTLD 数量的 57%。其中，超过 47% 的中文顶级域名不是由中国机构运营的，例如美国 Identity Digital 公司运营着.移动、.商店、.娱乐、.游戏和.企业；美国亚马逊公司运营着.亚马逊、.食品、.书籍和.家电；美国谷歌公司运营着.谷歌；新加坡 Temasek 集团运营着.淡马锡等。全球企业对以中国为代表的中文市场看好可见一斑。

2.2.4 中国顶级域名市场现状

从数量上看，虽然与欧美企业申请的数量有较大差距，品牌类仍是中国新通用顶级域名申请的主力军，主要以企业集团品牌或主要业务内容相关字符串命名，共 35 个。

中国运营的通用类顶级域名共 22 个，如 .网址、.ren、.top 和 .fans 等。

中国境内仅广东省运营着 2 个地理类顶级域名——. 广东和 . 佛山，台湾地区运营着 .taipei。

中国新通用顶级域名运营情况

类别	运营数量
通用类	22
品牌类	35
地理类	3

2.2.5 品牌顶级域名应用案例

(1) 谷歌

早在 2012 年，谷歌便开启互联网基础资源层面的布局。谷歌在首轮顶级域名申请中共申请 101 个顶级域名，最终成功获批 46 个，包括：.google、.new、.gmail、.谷歌等。

其中，谷歌利用品牌顶级域 .google 加速布局线上资源，塑造企业品牌价值：推出 grow.google 网站，为用户提供线上培训工具和资源，帮助用户提高专业技能、进行职业规划、发展业务，提升居家办公效率；创建专属网站 families.google，向父母介绍当前在青少年儿童中受欢迎的 APP 和热点，拉近彼此之间的关系；联手美国运通 (American Express) 共同创建 shopsmall.google，利用电子壁画形式向用户展示超过 25 家小型企业的商品，用户可使用谷歌镜头扫描图片，在探索艺术的同时购买自己心仪的产品，将艺术与生活结合，丰富购物体验；推出 ai.google，用于分享最新技术进展、介绍谷歌人工智能相关项目。

(2) 亚马逊公司

亚马逊成功申请了 55 个顶级域名，包含了通用词和品牌词如：.amazon、. 亚马逊、. 家電、. 食品、.book、.buy、.kindle 等。

亚马逊公司申请顶级域名 .amazon 引起亚马逊合作条约组织 (ACTO) 的强烈反对，亚马逊雨林涉及巴西、哥伦比亚、秘鲁、委内瑞拉、厄瓜多尔、玻利维亚、圭亚那和苏利南八个南美国家，如果美国的亚马逊公司掌握了类似 tourism.amazon 这样的地址，南美国家的利益会受到不小影响，一场旷日持久的纷争由此开启。据外媒报道，为获得亚马逊合作条约组织的支持，亚马逊公司曾提出为亚马逊流域国家提供价值大约 500 万美元的电子阅读器和网络托管服务，但被相关国家拒绝。正如 ACTO 执行主任卡洛斯·阿尔弗雷多·拉扎里·特谢拉所说：“这就好像回到了美洲大陆刚被发现的时代，(殖民者)用小镜子等不值钱的物件和土著人换金子”。

最终虽然亚马逊公司在这场争夺中赢得了胜利——亚马逊公司在 2021 年时获得了 3 个品牌顶级域名的运营管理权，即 .amazon、. アマゾン以及 . 亚马逊。但围绕这一顶级域名的争议仍然持续很久，这也侧面表明了顶级域名资源无论是在企业还是国家层面，都具有重要的品牌价值。

拿回 .amazon 所有权后，亚马逊广告业务正式启用了 ads.amazon，其他产品线也陆续启用，如：prime.amazon、kindle.amazon 和 alexa.amazon 等，设立在每一个顶级域名 (.amazon) 之下的二级域名，已经成为亚马逊一个庞大的子业务体系，截止到 2023 年 7 月，亚马逊已经拥有 53 个带有 .amazon 品牌顶级域名后缀的域名。

(3) 奥迪

.audi 是奥迪公司申请的专属顶级域名，是全球汽车厂商最活跃的品牌顶级域名之一，共有近 1700 个二级域名，用于展示品牌旗下的所有系列、产品、新品宣传、客户服务等。奥迪根据品牌战略和产品规划自由分配优质 .audi 域名。通过具有品牌代表性的顶级域名，实现全球战略布局中的品牌统一。

通过数据统计工具可以发现，奥迪的 .audi 域名部分分配给了奥迪的个人经销商。例如 leipzig.audi, potthoff-hamm.audi 和 hahn-schorndorf.audi。和许多汽车品牌一样，奥迪依靠经销商和分销商的网络，其中许多是独立拥有或独立运营的。

奥迪经销商的网页采用了高度统一的模板，提供各经销商展示个性化信息的同时保持一致的品牌形象。通过这种方式，奥迪开始利用品牌顶级域名来实现对其品牌更加集中的控制，同时还可以为特定地区的客户和经销商提供本地化的体验。

除了大量的经销商网站之外，奥迪将品牌顶级域名应用在大型公司项目和个人宣传活动，使奥迪能够构建不影响其现有网站的专用内容。例如 weare.audi 的员工门户网站，以及专注于概念车以及介绍品牌可持续发展的供应链页面的 progress.audi。

e-tron.audi 是奥迪为自己新能源产品线打造的专属线上空间。近年来，随着全球对能源安全和环境保护的认知不断提高，奥迪加大了对新能源车型的投入和推广，以此加快奥迪电气化进程的全球布局。e-tron.audi 这个域名将产品与品牌巧妙地结合起来，体现了奥迪品牌在全球市场电动化战略布局中的决心。

(4) 佳能

2010 年，全球知名的摄影器材制造商佳能 Canon 宣布，启动品牌顶级域名 .canon 的申请，致力于为用户提供更安全可靠的信息服务，使用户登录访问该企业域名时无后顾之忧。2016 年，佳能正式启用以品牌顶级域名 .canon 为后缀的 global.canon 来代替原有官网域名 canon.com。

佳能通过将地域与 .canon 结合的形式，实现全球战

略布局中的品牌统一化。global.canon 作为品牌全球官网，介绍公司企业理念、发展战略、产品及服务、媒体资讯、可持续性发展等内容。而与之对应的是 vn.canon (越南)、in.canon (印度)、hk.canon (香港)、ph.canon (菲律宾) 等国家及地区类官网，这类网站都以当地语言进行建站，提供的内容大致与全球官网一致，满足了各地区不同文化、不同语言的需求。

(5) 中信集团

在中国，也有申请顶级域名这一互联网关键基础资源的先行者。2013 年 3 月，. 中信成为中国境内第一个申请成功的品牌顶级域名，开创了中国企业运营自有品牌顶级域名的先河。经过 10 年的实践，中信集团品牌在全球网络空间中的公信力得以大幅提升，而且对顶级域名的使用已经远远超越品牌价值。.citic 和 . 中信成为中信集团数字化转型过程中的重要基础资源，中信集团以顶级域名为抓手，进行集团化管理和子业务建设，截至 2023 年 7 月，.citic 和 . 中信下二级域名保有量已超过 252 个，由中信集团旗下 85 家子公司陆续启用。在成功提升全球品牌的同时实现了以域名为代表的数字品牌的集中纳管、统建统管。

(6) 联通集团

2016 年 2 月，.unicom 和 . 联通成功入根。2019 年 12 月，联通集团获得工业和信息化部（简称：工信部）批复，成为 .unicom 和 . 联通的域名注册管理机构。

2.2.6 城市顶级域名应用案例

城市品牌在提升城市竞争力方面发挥着非常重要的作用。全球化和信息技术的高速发展催生出了城市数字

品牌这个概念，作为互联网世界的重要基础资源，地理顶级域名（Geographic Top-Level Domains, Geo TLDs）的出现，让建设城市数字品牌的主体和实施方式都得到扩宽。

作为进入城市品牌网站的门牌号，以地名命名的地理顶级域名，为城市和地区带来了全新的在线机遇，正成为照亮城市的数字品牌之光，旨在促进地区旅游业、文化遗产和经济的发展。2012年ICANN首轮顶级域名申请开放期间，世界各地城市或地区纷纷申请自己的顶级域名。

（1）.tokyo

作为亚洲老牌发达国家，日本通过顶级域名这个载体，结合各个城市的既有文化名片：音乐、动漫、电影、艺术、赛事等，应用于塑造城市数字品牌，成为提升城市竞争力的重要思路。

日本首都东京，是日本的政治、经济、文化、交通等众多领域的枢纽和中心，也是世界经济发展度与富裕程度最高的都市之一、世界著名旅游城市之一。东京于2013年11月成功申请.tokyo地理顶级域，截至2023年7月，该域名保有量超过12万个。

例如，findmy.tokyo是东京地铁的官网，findmy.tokyo为访客展示东京地区的名胜古迹、演出节目、美

食佳肴等特色并提供相应地铁线路，为旅客提供坐着地铁游东京的信息服务。

marathon.tokyo是东京马拉松的官网，东京马拉松是世界六大马拉松之一，在该网站上，每年约有35万人注册参加马拉松比赛，而大约每10人中只有1人最终能报名成功。

（2）.nyc

纽约于2014年1月成功申请.nyc地理顶级域名，nyc是New York City三个单词首字母的缩写。截至2023年7月，该域名保有量超过6万个。

chinatown.nyc是纽约唐人街的官方网站，为近50万的纽约华人社群提供了一个线上的归属感。纽约华人占全市总人口的5.95%，他们在这里可以了解唐人街的文化、活动和服务。网站分为特色项目、合作伙伴、唐人街商业改善区和小型企业服务等板块，涵盖了唐人街的美食、地图、资讯等内容。

nft.nyc是纽约NFT行业的官方网站，该网站得到了NFT领域中品牌和项目的赞助和支持，致力于推动市场的发展和教育，并与有兴趣的人群分享最新的知识和经验。自2018年以来，一直为不断壮大的NFT社区搭建交流的桥梁。

第三节

第二轮顶级域名开放动态

ICANN 顶级域申请最新动态

2023年3月11-16日，第76届互联网名称和数字地址分配机构（ICANN）大会在墨西哥坎昆召开。作为核心议题之一，大会披露了关于第二轮顶级域名开放的最新进展。会中，ICANN 董事会通过了《新通用顶级域名后续程序政策制定过程最终报告》中包含的98项建议，并要求ICANN组织在2023年8月提交第二轮顶级域名开放时间表。

ICANN 董事会主席特里普蒂辛哈（Tripti Sinha）表示：“我们必须共同努力，确保互联网的弹性、安全性和未来。我们需要共同投入必要的资源和努力来解决棘手的问题，实现我们推出下一轮顶级域名的共同目标。而这需要 ICANN 社群、董事会和组织之间的紧密合作。”

在接下来的时间里，ICANN 将会在各个方面加快发展，为第二轮顶级域名的开放做好准备：

在组织流程方面，ICANN 组织在第77届ICANN大会最后一天，即2023年6月15日之前完成四项成果，包括董事会和通用名称支持组织（GNSO）理事会商定的计划和时间表、工作方法和实施审查小组的工作计划和时间表、处理封闭式通用顶级域名政策工作的项目计划和时间表或其备选方案，以及国际化域名（IDNs）

加速政策制定过程工作组的项目计划。

在资金支持方面，董事会将授权 ICANN 使用2012年顶级域名融资的剩余资金，为实施工作提供高达900万美元的资金。此外，董事会还指示 ICANN 继续其外联和沟通战略，向潜在申请者推广新通用顶级域名计划，重点鼓励对顶级域名认识不足的国家和地区了解并积极申请顶级域名，以提高其对互联网基础资源的使用能力。

在政策层面，计划使用通过预审核的注册局服务供应商（RSP）的顶级域名申请人将不需要再接受技术评估，只需要进行相对简单的系统测试，提高了审核效率。

ICANN 机构启动实施审查小组（Implementation Review Team，简称 IRT），对新一轮顶级域开放计划及章程进行讨论

2023年3月16日，ICANN 董事会就新通用顶级域名后续程序政策制定过程（SubPro）工作组提出的大部分最终建议通过了决议。

在决议中，董事会指示 ICANN 机构提交“ICANN 和通用名称支持组织（Generic Names Supporting Organization，简称 GNSO）理事会商定的工作方法

和 IRT 的工作计划和时间表”。因此，ICANN 机构正在启动 IRT，以“协助工作人员制定政策的实施细节，以确保实施工作符合政策建议的意图”，这是四个相互依存的实施流程之一，也是在新一轮顶级域名开放之前必须完成的重要任务之一。

截至 2023 年 7 月 10 日，IRT 已顺利开展了五次相关会议，对新一轮新通用顶级域名开放的计划相关章程，进行了热烈的讨论。ZDNS 积极参与相关会议，全程参与政策制定，并在会议中积极为中国社群发声，为建立更加透明、高效、公正的新通用顶级域名开放政策做出努力。

ICANN77 会议组建封闭式通用顶级域名 (Closed Generics) 讨论组

第 77 届 ICANN 大会提出封闭式通用顶级域名政策制定、注册局服务供应商 (Registry Service Provider，简称 RSP) 预审核 (Pre-Evaluation)、申请人支持计划 (Applicant Support Program，简称 ASP) 等议题将直接影响后续开放。

为了加快开放进程，ICANN 于 6 月组建了封闭式通用顶级域名讨论组，ZDNS 第一时间加入该讨论组，并全程参与政策讨论。

第四节 |

中文域名 推动构建更加开放、多样的互联网

中文域名作为潜在使用群体最大的国际化域名 (IDN)，对于促进中文地区互联网普遍服务和创新发展、提升网络包容性和多样性、弘扬中华文化和建立文化自信等具有重要战略意义。

《“十四五”信息通信行业发展规划》提出，“完善中文域名应用环境，进一步推动中文域名推广应用。”

《“十四五”数字经济发展规划》提出“大力推进产业数字化转型，鼓励和支持互联网平台、行业龙头企业等立足自身优势，开放数字化资源和能力，帮助传统企业

和中小企业实现数字化转型。”中文域名是推动中国民营企业数字化转型不可或缺的一部分。

中文域名是建设数字中国的重要品牌载体

对于中国人而言，中文域名比英文域名：更易识别品牌特征、更易感知品牌文化、更易传递品牌价值。

随着中国品牌的崛起，制造于中国的产品正远销海内外，但中国企业的品牌传播依然有待提升。很多公司的名字凝聚着丰富的企业文化内涵，域名是向全球展示企业品

牌文化的重要途径，在中文环境下，跳过英文域名这一媒介，能够更迅速传达理念。

中文顶级域名是建设数字中国的重要战略资源

中文顶级域名是互联网关键基础资源，如前文所述，互联网关键基础资源的占有量和质可以衡量国家和企业的“网络规模”和在全球互联网中的“管理权重”。拥有中文顶级域名资源，建立更自主可控的网络根基。

中文域名是传播中华文化的重要途径

汉字，是中国法定的通用语言文字。对我国互联网用户而言，中文域名体现了三大认同：第一个是语言认同，

中国人说中文，用中文域名最方便使用和记忆。第二个是身份认同，作为中国人希望网上用的名字还是现实中的名字。第三个是文化认同，希望在网上能够传播和弘扬中华文化。浏览器地址栏中每一次中文域名的输入，都是中华文化的彰显，都是文化自信的体现。

随着互联网的繁荣，网络空间成为文化传播的重要阵地。中文域名以汉字为表现形式，汉字承载五千年华夏文明、传承历史文脉、彰显文化自信，中文域名是汉字在网络空间的显著标签，有利于推动中外文化交流与文明互鉴，更全面地呈现中国文化的网络形象，为开放、多样的互联网发展增加中国元素。

第一节 | 域名技术与数字化变革

DNS 是域名系统 (Domain Name System) 的缩写，相当于互联网的 GPS (导航系统)。可以将 DNS 看成一个巨大的网络通讯录，当主机访问域名时，DNS 把

网址解析为对应的 IP 地址给终端。DNS 的诞生以及其在网络中扮演的“入口”角色决定了是它将伴随的互联网应用的快速发展并且不断演进。

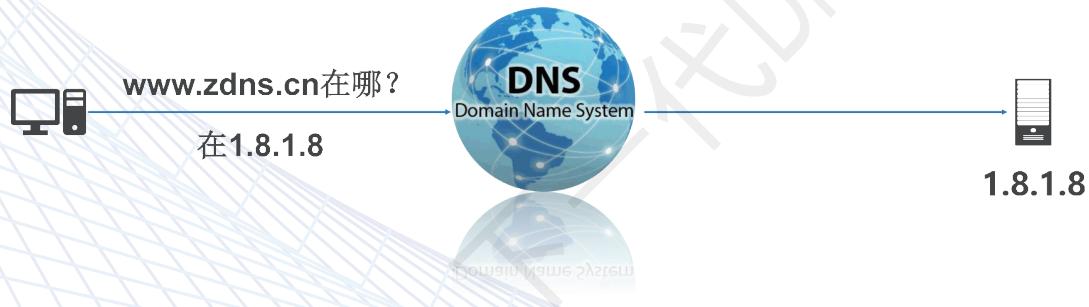
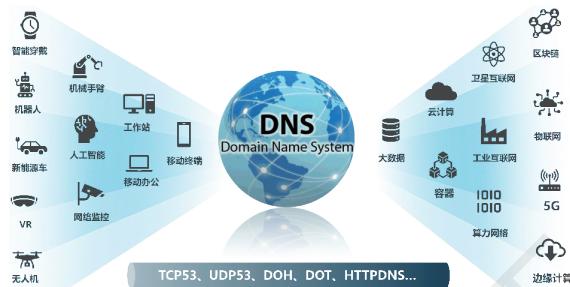


图 (DNS 是应用访问的“入口”)

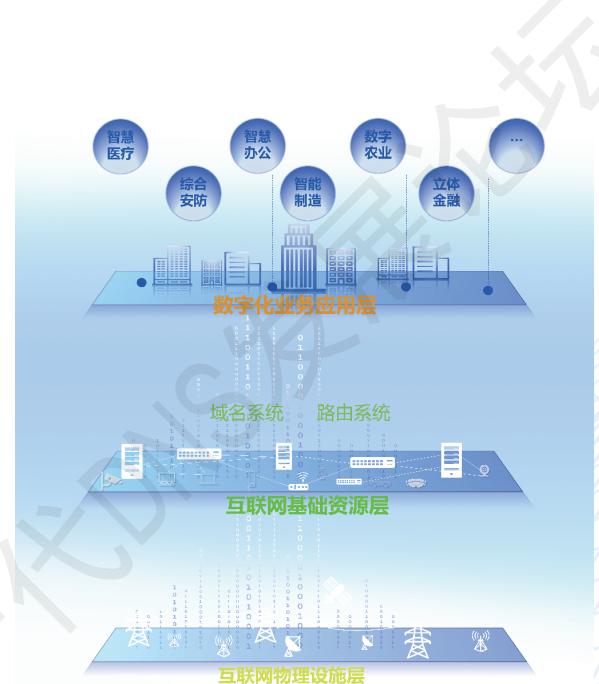
DNS 系统作为应用访问的“入口”链接着终端和应用两端。随着信息技术和网络技术的飞速发展，互联网基础设施层和应用层技术持续演进，DNS 的两端已经发生了极大的变化。

首先，终端的数量正在快速增长，不包括手机、PC 和笔记本电脑，目前我国 IoT 设备数量 2020 年 36.6 亿，2021 年 58.7 亿，2022 年 88.7 亿，预计到 2025 年增长到 173.4 亿台（数据来源：亿欧智库）。同时终端的类型日益丰富，智能家居、可穿戴设备、新能源汽车、机械手臂……“万物互联”时代已经到来。各种类型、海量的终端均需要通过 DNS 这一“入口”链接到网络中实现数据的访问交互，进而催生了域名技术的升级，推动 DNS 向下一代 DNS 全面升级，DNS 要支撑更多的访问场景，支持更重要的角色能力。其次，以大数据、人工智能、物联网、区块链等为代表的新一代信息技术系统需要更安全、更智能的网络底座。DNS 作为应用端的调度及发布枢纽，面对全新的环境，进而要向下一代 DNS 演进，要具备更全面的感知能力，更可靠的安全防护能力，更精准的业务调度和决策能力。



图（DNS 链接的“两端”快速发展）

DNS 在企业数字化中扮演着重要的角色，与企业数字化有着紧密的关系，是企业数字化过程中是一个关键的基础设施，它确保网络的连通性、安全性和可靠性，并提供灵活的业务调度和策略管理功能。下一代 DNS 核心技术沿着数字赋能、全面感知、可靠传输、智能分析、精准决策五大关键特性趋势演进。企业应该充分利用 DNS 的功能和优势，以支持其数字化转型和业务需求的实现。DNS 技术应用价值不断提升，DNS 从原来单一的底层网络基础技术转换成打造包罗万象的应用技术。



图（DNS 是企业数字化的关键基础设施）

第二节 | 包罗万象的 DNS 应用

3.2.1 DNS 支撑园区网发展演进的智能互联

互联网发展初期，园区网主要是园区内企业之间的内部网络，用于实现内部信息共享和通信。随着互联网标准的制定和推广，园区网开始采用标准化的网络协议和技术，尤其是三层路由式交换机的出现，对多个子网的划分放在不同的三层接口，大大提高了网络的带宽，实现了与互联网的连接，网络化、无纸化成为现实。

随着智能移动终端快速普及，Wi-Fi 技术快速发展，园区网逐渐发展成为一个综合性的服务平台，为园区内的企业提供各种企业服务，如智慧办公、立体金融、虚拟课堂等，促进企业之间的合作与交流。随后的阶段园区网开始与物联网技术相结合，实现对园区内各种设备、设施的远程监控和管理，实现智能化的园区运营和管理。同时，园区网开始向云计算和大数据的方向发展，通过

对用户数据进行收集、分析和应用，为园区内的企业和政府提供决策支持和服务优化的参考依据。目前，园区网已经逐渐发展成为一个集创新资源、创新服务、创新孵化于一体的平台，园区内的企业和创业者可以借助园区网的资源和支持，加速创新和创业的过程。

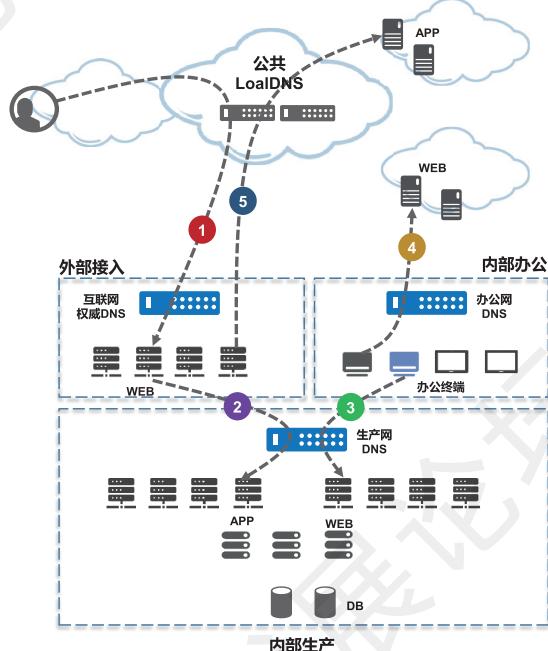
总的来说，园区网的发展演进是从内部网络到与互联网的连接，再到服务平台、物联网应用、大数据应用和创新驱动平台的发展过程，不断提升园区的运营和服务能力，推动园区内的企业创新和发展。DNS 作为网络核心服务从园区网的诞生开始就支撑着园区网络的发展，解决园区网终端对数据的快速、安全、高效的访问，扮演者园区网业务发布的准确、及时、可靠的智能调度枢纽角色。



近年来，针对园区网络的攻击增长迅猛，主要体现在安全办公和终端接入层面。在《IDC 2022 全球 DNS 威胁报告》中指出：过去一年，有 51% 的公司遭遇网络钓鱼，这意味着企业用户的隐私数据（如个人账户的用户名 / 密码、手机号、住址、银行账户密码等）可能被恶意攻击者窃取。28% 的公司终端遭受到木马、蠕虫、恶意软件等植入。DNS 作为访问的入口，在解决园区网网络安全中有多种应用场景：

- 防止恶意域名和网站：DNS 可以用于识别和阻止恶意域名和网站的访问。通过使用反恶意软件、黑名单和白名单等技术，DNS 可以检测并阻止用户访问已知的恶意域名和网站，从而保护企业的网络和用户不受恶意软件、钓鱼网站和其他网络攻击的威胁。
- 拦截和过滤恶意流量：DNS 可以用于拦截和过滤恶意流量，以保护企业的网络和系统免受分布式拒绝服务（DDoS）攻击、僵尸网络和其他恶意流量的影响。通过使用流量分析和区域封锁技术，DNS 可以对流量进行筛选，识别和阻止具有恶意意图的流量。
- 数据泄露和威胁情报：DNS 可以用于监测和检测数据泄露和威胁情报。通过分析 DNS 查询和响应数据，可以发现异常活动和潜在的数据泄露事件，并及时采取措施进行调查和响应，从而提高网络安全的可见性和防御能力。
- 安全分析和调查：DNS 可以作为网络安全分析和调查的重要数据源之一。通过分析 DNS 流量和日志，可以发现潜在的攻击行为、恶意域名和恶意软件的传播路径，从而帮助安全团队快速响应和采取适当的安全措施。

通过以上应用场景，DNS 在网络安全中发挥着重要的作用，帮助保护企业网络和系统免受各种威胁和攻击的影响，并提高安全防御的能力。



同时，在园区网中 DNS 和 SD-WAN (Software-Defined Wide Area Network) 可以结合应用并在业务访问层面的智能优化有多种应用：

- 快速域名解析：园区网络通常包含大量的设备和服务，需要频繁进行域名解析。结合 DNS 和 SD-WAN 技术，提供快速的域名解析服务。SD-WAN 可以优化内部网络流量路由，确保设备和服务能够快速访问到就近的 DNS 服务器，从而加速域名解析过程。
- 分支机构访问园区资源：对于跨园区的分支机构，

SD-WAN 可以提供优化的连接，通过智能路由和负载均衡等功能，确保分支机构与园区内的资源快速、可靠地连接。结合 DNS 技术，可以将分支机构的域名解析请求路由到就近的园区资源，进一步优化分支机构与园区之间的网络连接。

- 安全策略和访问控制：SD-WAN 可以提供统一的安全策略和访问控制，确保园区网络的安全性。结合 DNS 技术，可以通过 DNS 防护策略和黑白名单控制，对域名解析请求进行筛选和过滤，阻止对恶意或不受信任的域名的访问。
- 网络故障恢复：园区网络中的故障可能会导致设备或服务的不可用。SD-WAN 具备故障转移和链路切换的能力，可以实现快速的网络恢复。结合 DNS 技术，可以配置备用的域名解析服务器或备用的 IP 地址，

以备网络故障时的快速切换和恢复。

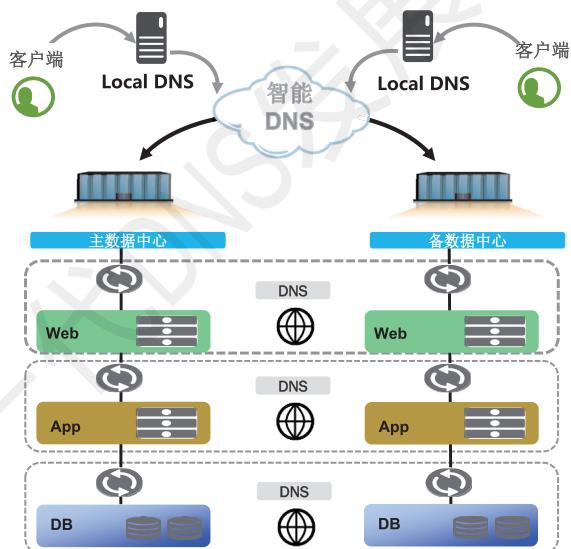
通过结合 DNS 和 SD-WAN 技术，可以提升园区网络的性能、安全性和可靠性，实现快速的域名解析、内容交付加速、分支机构访问优化和网络故障恢复等目标。这种结合可以为园区内的设备、服务和用户提供更好的网络体验和服务质量。

园区网络还在快速的发展，随着 5G、IPv6、云计算、大数据、物联网等技术在园区网中深入应用，园区网将呈现“接入无线化、全球一张网、AI 驱动运维、整网自动化”的典型特征。园区网的边界将从 PC 时代的有清晰边界状态专项云网融合、万物互联的无边界时代。DNS 将始终伴随着园区网的发展与演进不断迭代，提供极简的业务部署、极简的网络运维、极安全的网络体验。

3.2.2 DNS 联动网络实现业务调度的自动驾驶

DNS 从诞生开始就承担着作为应用访问“入口”的角色，伴随着互联网的快速发展，业务的快速增长，DNS 承担起了“业务调度”的角色，从传统 DNS 转型为智能 DNS。智能 DNS 在业务调度层面有许多应用，以下是一些常见的应用示例：

- (1) 负载均衡和流量调度：智能 DNS 可以根据服务器的负载情况和流量状况，将用户请求智能地分发到最适合的应用服务器。它可以根据服务器的性能、可用性和地理位置等因素进行决策，以确保负载均衡和优化用户体验。
- (2) 故障转移和高可用性：智能 DNS 可以监测服务器的可用性，并在服务器故障时自动将用户请求转移到备用服务器上。这样可以实现高可用性，确保业务的连续性，并提供无缝的用户体验。



图（智能 DNS 业务调度示意图）

- (3) 地理位置感知和全局流量管理：智能 DNS 可以根据用户的地理位置将其请求定向到最近的服务器，从而减少延迟并提高响应速度。它还可以根据用户的地理位置管理全局流量，以优化网络资源的利用和业务的传递。
- (4) 策略调度和业务优先级：智能 DNS 可以根据事先定义的策略和业务优先级，对客户端请求进行调度。例如，可以根据用户的用户组、访问权限、设备类型或其他参数，将请求发送到适当的服务器或服务，以实现个性化的业务调度。
- (5) 多数据中心业务调度：智能 DNS 可以用于管理不同数据中心的业务流量。根据数据中心的业务健康情况、可用性和地理位置等因素，它可以决定将请求发送到哪个数据中心或云服务，从而优化资源利用和业务性能。

随着企业数字化转型的进程不断加速，对业务访问的连续性、可靠性、稳定性提出了更高的要求，更多的开始关注如何进一步提升用户的访问体验。以我国金融行业为例：银行过去基于智能 DNS 要实现“两地三中心”的业务调度，而未来面临的是“三地六中心”或“多云多中心”的调度，这对 DNS 的调度以及处置能力提出更高的要求。

智能 DNS 从“应用感知”进一步走到“网络感知”进而实现全链路感知，且基于全链路的质量情况实现业务调度的自动化和智能化，实现业务调度的“自动驾驶”。

2022 年 ZDNS 联合华为发布“金融应用多活网络联合解决方案（IAA）”，在原有 DNS 感知应用的基础上，整合了华为 iMaster NCE-FabricInsight 产品中客户端至应用服务器的带宽、收发包数、访问延时、网络故障等关键指标，使 DNS 服务器可以基于用户的实际访问效果以及网络感知的真实情况进行更智能的调度。

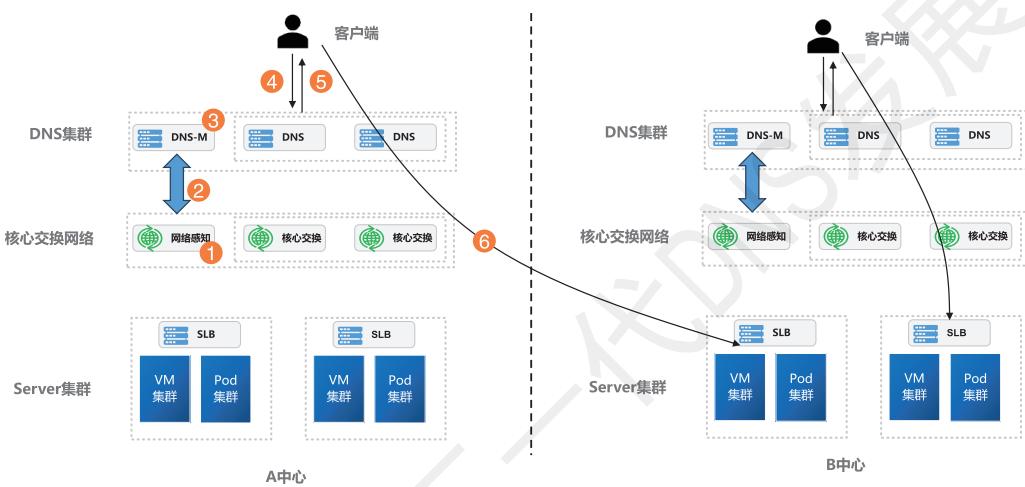


图 (DNS 与网络联动实现业务调度)

基于网络联动的业务调度“自动驾驶”过程：

- (1) 某网络服务商通过网络设备感知客户端至数据中心 A 中服务连通性，确认某局点客户端当前无法访问数据中心 A 中的业务；
- (2) ZDNS 通过内部接口从华为 NCE-FabricInsight 平台上获取客户端至数据中心 A 中业务的联通情况；
- (3) ZDNS 基于接口获取到的端到端网络层数据，再结合自身对业务的健康检查做出智能判断，确认某局点的客户端无法访问数据中心 A 的业务。同时，ZDNS 智能解析节点会将判断结果同步至整

个 DNS 解析集群；

- (4) 客户端向 ZDNS 的智能解析节点发起域名请求，获取业务的 IP 地址；
- (5) ZDNS 基于客户端源 IP 判断出数据中心 A 中的业务无法提供访问，因此将客户端请求引导至数据中心 B，此时返回数据中心 B 中的业务 IP；
- (6) 客户端成功访问数据中心 B 中的业务。

在实际使用效果来看，从过去的“已拥塞，再调度”升级为“未拥塞，先调度”，实现了从传统的“业务容灾”升级为“体验优化”。

3.2.3 应用域名大数据保护企业数字品牌

DNS 是互联网上存储域名与 IP 地址映射关系的一个分布式数据库，使用 DNS，用户可以方便的用域名访问互联网，而不用关心复杂难记的 IP 地址。同时，域名和 IP 地址更是企业应用链接网络进行数字化转型的重要标识。

在网络空间中，域名不但为企业的应用提供了便捷的访问入口，其自身还有着极其重要的品牌属性和商业价值。随着互联网业务快速发展，域名空间也在快速的扩张，企业开始关注自己的数字品牌在网络空间中的竞争力以及存在的一些极其隐蔽的威胁。例如：某企业拥有域名“10086.cn”，那么该企业对 10086.cn、10086.wang、10086.top 等域名的关注就要格外的注意，因为这涉及到企业的品牌影响。

“被动 DNS”（Passive DNS）的应用和推广为企业数字品牌的保护打开了新的通道，基于域名大数据技术并与人工智能结合后能高效、智能的帮助企业做好数字品牌的保护。被动 DNS 是 Florian Weimer 在 2004 年提出并发明的一项技术，因为我们发现有一些问题，光靠传统的 DNS 是很难解决，例如：

- 一个域名过去曾指向到何处？
- 特定网络范围内的 IP 地址对应的所有域名有哪些？
- 对于一个给定的名称服务器，它托管了哪些域名？
- 有哪些域名指向给定的 IP 网络？
- 一个域名下存在哪些子域名？

与 DNS 查询的方式相反，被动 DNS 属于反向获取或对网络空间中 DNS 数据信息的查询。它可将互联网的域名系统中可用的 DNS 数据信息重建到数据库中，以便研究人员对其进行检索和查询。这些数据信息是从生产网络中获取到的，不仅包含了当前的 DNS 数据，

也包括了历史记录中的一些 DNS 数据映射。发明被动 DNS 技术的初衷，是为了防止网络攻击，事实上，它的确在这方面起到了突出的作用。除此之外，它还可以被用在其他的应用场景中，而品牌保护正是一个好的应用场景。



(1) 识别需要关注、需要管理的域名资源

企业数字品牌层面通常关注两类内部不可见的域名资源。第一类是内部不可见域名资源，即由企业内部其他域名使用部门注册的二级域名、三级域名；第二类是外部不可见域名资源即被域名投资人等第三方持有的优质域名，不法分子注册的仿冒、滥用、侵权域名等。通过被动 DNS 技术可以对源二级域名或源子域名所在的二级域名进行实时、历史 DNS 解析数据挖掘，返回在相同二级域名基础上建立的三级、四级以及更深层子域名列表的测绘。并返回过去一年内观测活跃过的所有子域名列表及 DNS 解析指向资源，可以对特定关键字、关键域名进行全网搜索，并结合 DGA（域名生成算法）等技术，寻找关联的域名资源。这个层次的分析通常可以用于帮助企业识别需要关注、需要管理的域名资源。

(2) 发现并打击域名滥用、侵权行为保护企业品牌

结合 WHOIS 数据源，可以继续分析共享相同注册人姓

通过对某一品牌关键字进行模糊匹配查询，可以找出与您企业名称或注册商标名称类似而没有经过任何授权的域名，特别是仿冒域名往往会出现新注册域名 (NOD) 中，通过及时发现，通报，关停未授权域名，可以及时消除由此产生的品牌负面影响，降低企业用户数据被钓鱼的安全风险。在此领域中最为常见的应用场景如下：

名、共享相同联系人信息、共享相同的地址元素的关联域名，即通过一个域名可以找到与这个域名具有强关联的其他域名，可以对这些域名进行网站内容抓取、分析等操作，确定域名是否存在滥用、侵权等行为。这个层次的分析可以协助品牌用户以较高的效率发现并打击域名滥用、侵权行为。同时，通过源网站域名 DNS 解析实时和历史记录，可以挖掘具有相同、相似解析行为的其他域名，通过对域名一段时间内进行过的 A 记录、AAAA 记录、CNAME 记录、NS 记录、MX 记录等活跃解析记录进行分析，以及跳转至目标域名、重定向到目标域名等行为，供相关应用分析和进一步溯源。

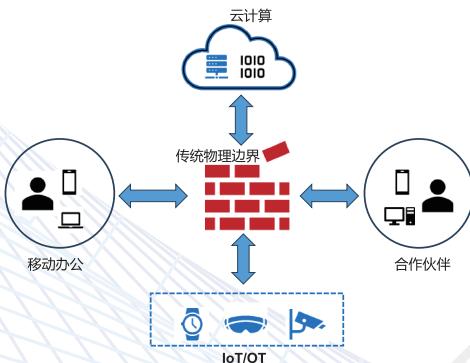
被动 DNS 主要是基于互联网的域名大数据进行历史追踪分析，结合 WHOIS 历史数据，可以发现域名过去由谁持有、解析到什么目标、跳转到哪里，供品牌用户在回购某个域名时进行分析。另外，此项技术应用在企业局域网络或者专有云网络的环境中同样适用。

3.2.4 DNS 融合 SDP 建立零信任安全增强模型

近年来，信息与通信（ICT）技术发展迅速，企业将新技术应用于商业环境，快速推动了其数字化应用与发展。与此同时，也出现了许多信息安全方面的问题，如用户信息泄露和盗用、病毒引起的数据丢失、外包攻击导致的业务停顿等，对企业和社会的发展产生了极大的影响。

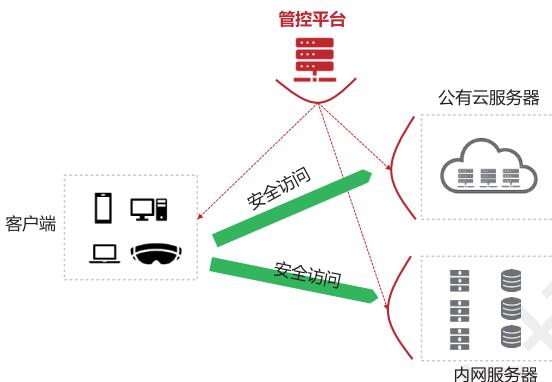
随着云计算、大数据、移动互联网、物联网（IoT）、第五代移动通信（5G）等新技术的崛起与快速发展，传统的安全边界模型逐渐瓦解，原因有两点：

- (1) 内网很难保证 100% 安全，黑客可以轻松劫持边界设备，并从内部攻击企业应用。同时随着自带设备（BYOD）、外包工作人员和合作伙伴的存在，边界内部设备不断增加，漏洞也在不断的增加。
- (1) 越来越多的数据正在“走出”内网。除了传统数据中心，企业还利用外部的云计算资源，如 IaaS、PaaS、SaaS 等。移动办公、物联网、大数据应用导致数据不再局限于内部网络。



图（传统安全边界瓦解图）

企业的内部设备数量快速增加，且企业的应用程序还在不断地向外迁移，传统安全解决方案将用户的请求回传到数据中心，以进行身份验证和数据包检查，进而无法很好的实现规模化。而基于零信任理念的 SDP（软件定义边界）架构逐渐的替代传统 IT 架构的安全模型，成为满足企业未来数字化转型需求的最佳方案。



图（基于零信任理念的 SDP 图）

另外，在基础网络核心服务领域一直有一个大家熟知的最佳实践，那就是“DDI（DNS，DHCP，IPAM）”。域名系统（DNS）是一个分层的命名系统，它将人类可读的域名映射到计算机可识别的互联网协议（IP）地址，定位和寻址全球设备，对于可靠的互联网运营和连接至关重要。几乎每个网络连接都是以 DNS 查询开始。动态主机配置协议（DHCP）是一种自动配置协议服务，可在连接时将 IP 地址分配给网络设备，这对于将设备连接到网络至关重要。每个设备都必须有一个 IP 地址才能通信。互联网协议地址管理（IPAM）是企业在私有网络上管理 DNS 和 DHCP 的系统。IPAM 系统可以对网络中如何分配和解析 IP 地址提供计划、跟踪和管理。

通过集中式的 DDI 解决方案，网络管理员可以从单一管理平台获得对其网络的可见性和控制权。一个架构设计良好的 DDI 会使用 IPAM 集成 DNS 和 DHCP 服务的数据，以便每个服务都能及时感知其他服务的变化。例如，当 DNS 知道了 DHCP 分配给客户端的 IP 地址，自身就会进行相应的更新，这样，即便客户端 IP 地址是由 DHCP 动态分配的，私有 DNS 仍然可以通过主机名来解析客户端。DDI 组合具有独特的优势，可以记录网络上的人员、人员的去向以及（更重要的是）去过的地方，为企业提供可见性和控制力。

信息安全始终是多层级的，而基于 SDP 的零信任是一种有效的方案，通过集成企业安全基础架构的许多其他组件增强零信任安全的处置模型，最终使企业受益。通过将企业管理的 DDI（DNS, DHCP, IPAM）系统与 SDP 结合，可以为企业提供改进的安全可见性和控制力，在很大程度上提高企业安全性并帮助企业在零信任安全之旅中更上一层楼。在相关应用层面的实践举例如下：

（1）DNS 向 SDP 提供上下文和元数据

DNS 和企业管理的 DDI 可以提供有关设备和网络行为的上下文信息，并将此上下文信息作为零信任 SDP 系统的输入，可以为其是否允许用户访问网络提供决策支持，从而增强零信任访问控制决策能力。

（2）SDP 控制器将策略结果发布到 DNS

SDP 控制器可以将访问策略结果发布到本地 DNS 服务器，以便提供一层额外的控制。DNS 系统可以使用来自 SDP 控制器的零信任上下文信息和决策，扩展 SDP 的覆盖范围，并有效地使企业 DNS 成为一个关键的零信任策略执行点。

企业 DDI 通过过滤已知的不良站点和检测失陷指标（IoC）可以提升企业的安全性。将企业 DDI 系统与 SDP 系统结合，实现互相集成和增强，可进一步提升企业的安全性、韧性和响应能力。DNS 可以为 SDP 控

制器提供增强的上下文设备和活动信息，以便后者更好地实施安全策略决策。DNS 系统也可以使用来自 SDP 控制器的零信任上下文信息和决策结果，扩展 SDP 的覆盖范围，并有效地使企业 DNS 成为一个关键的零信任策略执行点。这两个系统都可以通过集成而受益。

3.2.5 DNS 在算力网络中为海量数据定位算力

新型数字化技术和业务的兴起，以及信息数据的爆炸式增长，IDC《未来算力推动企业迈向数字化 2.0》白皮书报告，预计 2024 年全球数据总量将达到 142.6 ZB。对各类数字化应用的支撑以及对海量数据进行处理，都需要大量的算力资源。新型业务催生了边缘计算的诞生，未来算力节点将出现泛在化的特性，“云一边一端”多级泛在算力将逐步落地部署并成为典型的算力基础架构，“随时随地，无限算力”成为新兴的业务诉求。算力网络将算力等资源与网络协同统一，结合用户需求提供最优的资源配置策略，同时提高多级算力资源的协同工作效率，成为网络技术发展的新方向。

从用户视角来看，不同位置的资源并不是“平等”关系，需要综合考虑用户到资源距离的不同（即网络空间距离）、网络状况的好坏、资源报价不同等多方面因素选择最优资源。如何将算力、存储等资源与网络结合，更好地为用户提供最合适的资源服务，成为一个非常重要的研究点。

算力网络通过无处不在的网络连接，整合多级算力、存储等资源孤岛，结合网络信息（如带宽、时延等）与不同类型的用户需求，为用户提供最佳的资源分配方案，进而实现整网资源的最优化使用。算力网络可提高云、边、端多级算力协同工作效率及整网资源利用率，保证服务灵活动态部署和用户体验的一致性，用户无须关心各类基础资源的位置和部署状态，由网络协同调度各类资源。算力网络作为资源分配与网络连接的一体化解决

方案，将成为未来网络技术体系的重要组成部分。

面向分布式算力交换架构，借鉴域名解析系统（DNS）在互联网流量调度中起到的重要作用，当算力需求方存在某算力资源需求时，通过 DNS 解析获得该算力资源的 IP 地址，进而基于 IP 协议实现路由可达。基于域名寻址定位算力的机制可分为三个步骤：

（1）算力路由注册

使用 URL 语言将算力、存储等资源划分成标准化单元进行统一标识，形成算力域名。这么做的好处是当算力资源池 IP 地址发生变化时，不影响算力域名，从而保证算力调度的正常开展。此外，也提高了算力资源的易读性、可管理性和通用性。

（2）算力权威信息维护

算力服务者向 DNS 上报本地计算集群的算力域名与 IP 地址，形成面向全局的算力权威记录。

（3）算力寻址

算力需求者通过算力解析，将分配到的 URL 标识映射成算力域名对应的 IP 地址信息，通过网络设备建立与算力资源服务者的网络连接，基于新型互联网交换中心扁平网络架构，高效、便捷地调用相应的算力。

在互联网基础设施不断迭代升级的今天，DNS 的解耦设计、功能扩展和成熟运行机制对新兴技术领域形成了有力支撑。在未来，面向特定场景的 DNS 部署机制、标准研究和性能优化是十分重要的研究领域。

第三节 |

DNS 技术升级趋势

3.3.1 云边融合、云边协同的 DNS

随着云技术的发展和普及，很多企业的基础设施和上层应用开始向“云”转型，在云化升级的过程中甚至不少企业在构建网络时完全以云作为基础架构，没有部署传统的数据中心架构。然而，企业存在更多的现状是云和本地传统网络并存的架构，它们网络可能以云为主、以传统基础架构为辅，且云和基础的传统网络之间存在着业务互访、策略呼应、运维统管等“云边协同”的场景。

传统 DNS 是在企业本地部署和管理的，然而，就像许多企业 IT 基础设施云化升级一样，由企业管理的 DNS

也开始转向云端，注重云端的管理、云与边的联动和融合等。

以国内某企业为例，为加速业务发展，企业对 IT 基础设施进行全面的升级，尝试将更多的业务迁移至互联网的公有云中，借助公有云平台的能力，快速实现了应用的云化升级。企业可在多个云上快速发布应用，对应用的质量进行全链条监控，能够在全国某些区域内进行业务的 A/B 测试，系统的可靠性、连续性得到大幅提升。同时，企业的本地传统网络也开始向云化转型，构建本地的云网络架构以及私有云平台，实现了面向企业本地多业务线条的多租户私有云业务中心。然而，DNS 作

为业务访问的入口，在云化升级的过程中却面临前所未有的挑战：

- (1) 企业本地面向互联网的 DNS 仍然是传统架构，应用上云，业务快速发展，但 DNS 的抗攻击能力没有本质提升。
- (2) 企业在公有云 VPC 中的业务也需要 DNS 调度，在公有云和本地私有云之间的业务交互时多套 DNS 策略管理混乱。
- (3) 企业虽然构建了智能 DNS 系统，但 DNS 对应用的感知还局限于自己本地网络边界之中，而企业对应用的感知已经通过云化升级实现了全链条的监控，存在明显的短板。
- (4) 企业在多云架构下的域名空间管理处于完全混乱的状态，缺少有效的手段评估域名空间是否存在滥用以及域名资源的整体使用情况。
- (5) 无论是私有云还是公有云，其中云上的应用必然有访问互联网业务的需求，面向互联网访问的过程中对域名的数据缺少安全的评估与统一的监控。

由此可见，企业的业务发展催生了基础设施和上层应用向云化转型升级，DNS 作为应用的访问入口和信息发布枢纽也会伴随云化共同升级。DNS 在云化升级的过程中有以下几大趋势：

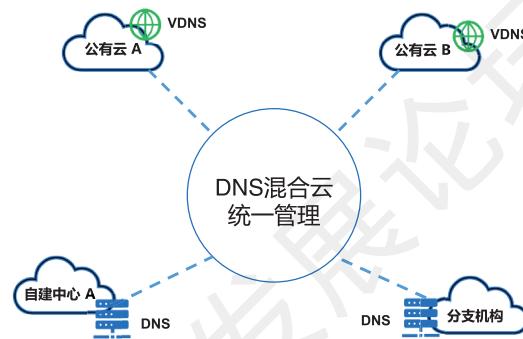
(1) 通过公有云 DNS 提升企业 DNS 系统的“上限”

公有云 DNS 将与企业本地 DNS 共同对外提供服务，借助公有云平台的节点分布和高可用，企业 DNS 系统整体的性能上限将大幅，DNS 系统的抗攻击能力大大增强。云边协同的 DNS 系统为企业提供了一键灾备的能力和全球分布式发布的能力，企业的业务连续性大幅提升。DNS 的 SaaS 服务提供商甚至参考 CDN 的技术为企业实现了云端 DNS 加速能力，企业的权威 DNS 数

据不会泄露到云端，且仍然可同时使用云边两套 DNS 对外发布业务。

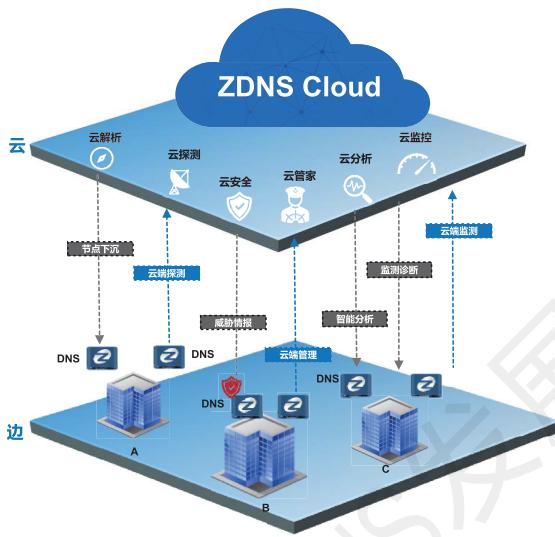
(2) DNS 业务多云统管，DNS 服务多云联动

企业在向云化升级转型的过程中会出现多云管理的场景，包括公有云与企业私有云或者多个公有云之间。所以，DNS 的关联也已经开始转向云端，具备多云统管的能力，便于企业对域名系统的集中运维和策略控制。同时，企业要考虑 DNS 管理平面的安全及容灾，如：云端管理一旦出现问题，本地如何接管；云与本地管理的安全策略等。目前部分商业版 DNS 已经提供多云部署和统一管理的能力，管理员可在统一的平台上操控所有 DNS 集群。



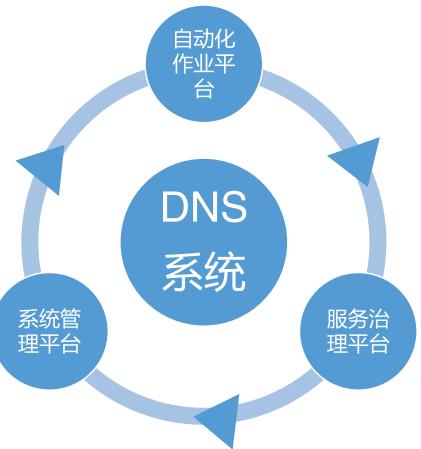
(3) DNS 云边联动，云上资源云下调度，云下状态云上感知

企业 DNS 系统在云化升级后会实现“云 DNS”与本地“边 DNS”的深度融合，为应用及终端用户提供更智能的发布与访问调度能力。本地 DNS 系统通调用云端的探测节点实现对应用更加真实和准确的健康感知能力，通过动态更新云端的域名数据（威胁情报、域名库等）、IP 数据实现对访问安全和体验的升级。另外，云上 DNS 平台可感知云下 DNS 和业务系统的负载情况、安全态势，并及时的调整调度算法分担访问压力，及时开启安全防御机制。



4) 建立统一的 DNS 服务治理平台，合理使用域名空间

DNS 服务治理的核心是对域名空间的管理，如：云内、云外的应用对域名的使用情况，对 IPv6 域名的访问情况，多云之间域名级联访问的情况，不同资产对互联网域名访问的情况。通过建立域名服务治理平台掌握域名空间的变化，了解域名访问的态势，并进一步提升和优化 DNS 系统的策略，摆脱 DNS “救火式”的运维困局，实现从 DNS 系统运维到 DNS 业务运营的升级。



3.3.2 软件定义 DNS

软件定义 DNS (Software-Defined DNS) 是一种将域名系统 (DNS) 功能虚拟化和集中管理的方法。它通过软件定义网络 (SDN) 技术，使 DNS 基础设施能够以更灵活、可扩展和可编程的方式进行部署和配置。

传统的 DNS 架构通常包括分布在不同地点的多个 DNS 服务器，它们相互协作以提供域名解析服务。然而，这种分散的架构可能导致管理和配置复杂性，且 DNS 目前作为应用发布的重要系统，在面对网络中的流量变化和业务健康感知时需要更加灵活的策略。软件定义 DNS 的主要思想是将 DNS 系统的域名解析的功能从固定的范式中解耦出来，使其以软件接口的形式对外建联。管理员通过使用类似 SDN 控制器的管理平台，以“面向应用”的方式集中管理整个 DNS 基础设施，包括 DNS 解析规则、流量路由和负载均衡等。未来软件定义 DNS 的技术升级趋势如下：

(1) DNS 与虚拟化、云化的融合

随着云计算和虚拟化技术的普及，软件定义 DNS 将更多地与虚拟化和云平台集成。传统的 DNS 架构依赖于物理硬件设备，而软件定义 DNS 可以通过在虚拟机或容器中运行来实现更高的灵活性和可扩展性。未来，软件定义 DNS 将更加紧密地与云服务提供商合作，为云环境中的应用程序提供快速、可靠的域名解析服务。

(2) 自动化与编程能力的增强

软件定义 DNS 的发展趋势之一是提供更强大的自动化和编程能力。管理员可以使用 API 和编程接口，以编程方式配置和管理 DNS 解析规则、流量路由和策略等。这样的能力使得 DNS 的管理更加灵活和可自动化，有助于应对动态变化的网络环境。未来，软件定义 DNS 将进一步提升自动化水平，实现自动化的配置、监控和故障恢复，减轻管理员的工作负担。

(3) 安全性与防御能力的强化

随着网络安全威胁的不断增加，软件定义 DNS 的发展也聚焦于增强安全性和防御能力。软件定义 DNS 可以与其他安全解决方案集成，如防火墙、入侵检测系统 (IDS) 和威胁情报平台，以增强对恶意活动的检测和阻止。未来，软件定义 DNS 将进一步发展安全智能，利用机器学习和人工智能技术，实时监测和识别潜在的安全威胁，并主动应对和阻止攻击。

(4) 大数据与智能分析的应用

软件定义 DNS 可以收集大量的 DNS 流量数据，并利用大数据和智能分析技术进行实时分析和洞察。这样的分析可以揭示潜在的安全威胁、网络故障和性能问题，帮助管理员做出更明智的决策和采取相应的措施。未来，软件定义 DNS 将借助大数据和智能分析的力量，实现更精准的故障诊断、性能优化和容量规划。

(5) 边缘计算的驱动

随着边缘计算的兴起，将 DNS 功能推向网络边缘也成为一种趋势。软件定义 DNS 可以在边缘节点上部署，以提供更快速和低延迟的域名解析服务。这对于需要在边缘进行计算和服务交付的场景尤为重要。未来，软件定义 DNS 将与边缘计算相结合，为边缘场景下的应用提供高效、可靠的 DNS 支持。

软件定义 DNS 正在不断演进和发展，通过虚拟化和集中管理，软件定义 DNS 为域名系统带来了更大的灵活性、安全性和智能化。未来，随着云计算、大数据分析、多云集成和边缘计算的发展，软件定义 DNS 将继续推动 DNS 技术的创新，构建更强大、高效的域名系统，助力互联网的持续发展。

3.3.3 有状态 DNS 的深入应用

传统的 DNS 是一种“单播”的设计，基于 UDP 无连

接的 DNS 通信方式，只有域名解析和应答的过程，没有状态的标记。所以，传统的 DNS 更适合用于查询相对静态的数据，在轮询频率不是太高的情况下，能够有效地返回更新结果。

随着应用的快速发展，为了满足特定专用网络低时延、高可靠的 DNS 的演进需求，让终端实时获取服务信息的变化，通过有状态 DNS 解析来实现可扩展的服务发现机制成为工业界的共识，也是 IETF 的标准化方向，未来此技术将深度应用。具有面向连接和状态管理功能的有状态 DNS 技术，可以有力支撑 DNS 服务发现机制在订阅管理、解析状态管理等范畴的技术要求。

有状态 DNS (DNS Stateful Operations, RFC8490) 指客户端向 DNS 服务器主动订阅关注的资源记录集合，从而获得信息更新的异步通知。它改变了传统 DNS 的尽力而为模式，把 DNS 查询变成一种可靠的面向连接的主动推送机制，可减少 DNS 查询延迟和网络负载，提高实时性和准确性，确保 DNS 记录的一致性和可用性。

相比较于现有的基于 UDP 无连接的传统 DNS 通信方式，有状态 DNS 具备以下优势：

- 基于可靠的会话链接 (TCP/TLS)，提供更为安全的 DNS 数据交互。
- 基于持久的长链接，建立流式 DNS 数据传输，减少交互损耗。
- 基于有状态 DNS 的订阅 / 推动模式，可以有效的提高 DNS 数据生效的实时性。
- 基于有状态 DNS 机制，可以很好的实现基于 DNS 的服务发现机制，为现有的服务发现机制提供补充。
- 使用有状态 DNS 的 middlebox 机制，可以提高 DNS 系统的高可用性，减少 DNS 服务的单点故障。

结合有状态 DNS 上优势和深入应用，DNS 生态 / 应用

会得到改善：

- DNS 灾备切换：现有的 DNS 灾备切换方案受制于 DNS TTL 机制，时效性依赖于 DNS 记录的 TTL 时间，因此很难做到实时的切换。结合有状态 DNS 的订阅机制，客户端可以订阅特定的 DNS 记录，在这些 DNS 记录发生切换后，就会立刻收到 DNS 消息推送，从而可以实时的进行新老记录的切换。这对于一些对切换时间敏感的应用 / 场景有很好的帮助。
- 实时通知：有状态 DNS 技术通过向客户端推送解析结果，可以实时通知客户端域名解析结果的变化，避免了客户端频繁查询的需求。这在实时性要求高的场景下非常有用，例如在线游戏、实时视频等应用。
- 服务发现：利用泛域名（wildcard）+ 有状态 DNS 机制，可以实现一套简单的、分布式的服务发现体系。通过多点订阅方式，关注某个域下的 DNS 记录实时变化，可以构建起一套分布式的服务发现集群。该机制简单易用，并可以水平扩展，对现有的服务

发现机制是一种很好的补充。

- 态势感知：基于有状态 DNS 机制，态势感知系统通过订阅关注的 DNS 记录，实时获取这些记录的地址变化情况，可以给出这些记录的历史变化情况，为数据分析提供帮助；同时结合网络流量分析，可以分析记录域名变化对用户访问的影响，从而给出一些参数（比如域名 TTL、用户侧缓存配置、路由配置）的优化建议。
- 负载均衡：有状态 DNS 技术可以让 DNS 服务器控制解析结果的推送，使得可以实现负载均衡。DNS 服务器可以根据不同客户端的位置、负载情况等因素，动态调整解析结果的推送策略，从而提高整个系统的可用性和性能。
- 数据安全性：传统的 DNS 查询将解析结果暴露给了所有的客户端，存在一定的安全风险。而有状态 DNS 技术将解析结果直接推送给客户端，可以避免解析结果被第三方窃取的风险，提高了数据的安全性。

构建可扩展的 RPKI 依赖方系统部署机制

作 者：马迪 互联网域名系统国家工程研究中心（ZDNS）首席研究员

来 源：本文转载自《中兴通讯技术》2023年第1期

关键词：RPKI；路由安全；互联网码号资源管理

前言

互联网码号资源公钥基础设施（RPKI）依赖方系统是各类网络运行机构开展 RPKI 应用实践的一个关键环节。RPKI 依赖方系统的研发和部署，既需要处理 RPKI 核心功能的“普遍性”问题，又需要兼顾网络互联互通特征的“特殊性”问题。相关解决方案需要考虑 RPKI 依赖方系统应当有哪些组件，各个组件如何在网络上分布，以及以何种逻辑关系分布。面向 RPKI 依赖方系统的核心功能，梳理了影响 RPKI 依赖方系统运行效能的 4 对矛盾，并提出了一种可扩展的 RPKI 依赖方系统部署机制，包含软件层面的解耦机制和硬件层面的部署机制。

研究背景

自 2012 年国际互联网工程任务组（IETF1）完成基础协议的标准化工作以来，历经国际互联网体系结构委员会（IAB2）的背书 [1] 以及国际互联网路由安全自律协定（MANRS3）项目面向全球网络运行机构的推广倡议，互联网码号资源公钥基础设施（RPKI）已成为解决当前

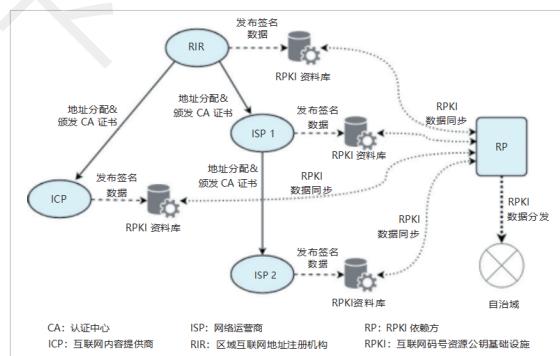
互联网域间路由安全问题的技术路线共识。RPKI 的理念肇始于互联网安全协议专家 S.KENT 博士的论文 [2]，并通过对传统的基于 X.509 公钥基础设施进行扩展 [3]，进入到 IETF 的工业标准体系。

RPKI 的部署和运行是一个复杂的系统工程，需要网络运行机构（网络运营商、互联网交换中心、内容分发网络服务商等）、RPKI 数据服务机构（互联网 IP 地址注册机构、RPKI 依赖方系统服务商等）以及路由器制造商等角色的配合和协调。其中，RPKI 依赖方（RP）系统充当了地址管理系统和路由控制系统之间 RPKI 数据传递的桥梁，是连接 RPKI 数据供给侧和 RPKI 数据需求侧的 RPKI 生态关键环节。

RPKI 依赖方系统的部署，涉及网络运行机构的路由控制策略、安全保障策略和地址分配策略，需要统筹网络规模、拓扑结构、互联互通策略以及地址资源分配格局等要素。这些要素会因应业务和技术的演进而随之变化。设计一个既可以处理 RPKI 依赖方系统功能诉求的“普遍性”问题，又能兼顾具体网络（及其变化）“特殊性”问题的可扩展部署机制，是 RPKI 技术在网络运营商、互联网交换中心等网络运行机构落地应用的关键。

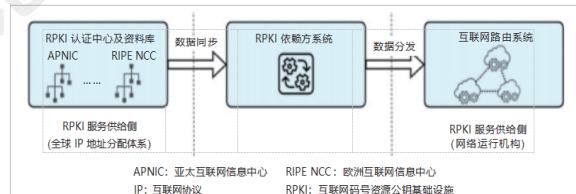
RPKI 原理简介

RPKI 是一种公钥证书基础设施。基于当前全球的互联网码号资源分配关系，RPKI 构建了一个面向 IP 地址及互联网自治系统 (AS) 号码的授权认证体系，并以 X.509 证书扩展及若干签名对象的形式加以呈现。如图 1 所示，RPKI 体系中的码号资源分配者在分配资源的同时，为下游节点签发资源证书（基于 X.509 证书的扩展）。依托 RPKI 提供的认证功能，互联网码号资源 (IP 地址及 AS 号码) 的最终用户单位 (资源持有者) 通过签发相关数据对象，来完成路由通告相关信息的发布（例如路由起源授权等）。作为 RPKI 认证体系的依赖方，参与域间路由交互的网络运行机构（例如网络运营商、互联网交换中心等）定期从 RPKI 资料库系统（基于码号资源分配关系组织起来的分布式数据存储体系）同步资源证书以及包括各类基于 RPKI 的数据对象，并将经过验证的信息推送给边界路由器，供其在接收路由通告时进行真伪判断。



概括地讲，RPKI 生态有 3 个组成部分：RPKI 供给侧、RPKI 依赖方、RPKI 需求侧。如图 2 所示，RPKI 供给侧包含全球分布的 RPKI 认证中心 (CA) 以及用于存储 RPKI 资源证书和各类 RPKI 数据对象的分布式

RPKI 资料库系统。RPKI 需求侧是当前互联网的域间路由系统，由部署在不同网络自治域的边界网关协议 (BGP) 路由器组成。RPKI 依赖方是连接“供给”和“需求”的桥梁，负责收集 RPKI 供给侧产生的数据并加以验证后交付给 RPKI 需求侧参考使用。



▲图 2 RPKI 的生态结构

RPKI 数据尽可能快速、完整、准确地从供给侧扩散至需求侧的关键在于 RPKI 依赖方。全盘考察 RPKI 的运行机制，并结合相关 RPKI 依赖方系统的运行实践，笔者归纳了影响 RPKI 依赖方系统效能的 4 对矛盾：

矛盾 1：RPKI 资料库（发布点）越来越多，与实时感知全球 RPKI 数据更新情况之间的矛盾；

矛盾 2：RPKI 数据对象数量越来越多，与快速同步全球 RPKI 数据之间的矛盾；

矛盾 3：RPKI 数据授权链（深度和广度）越来越复杂，和快速构建全球 RPKI 数据认证路径之间的矛盾；

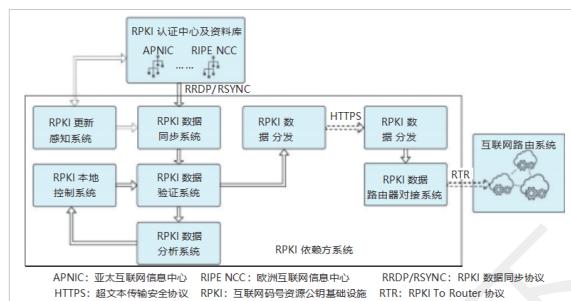
矛盾 4：RPKI 依赖方系统集中化趋势（远离网络边缘），和路由器快速获得 RPKI 认证数据之间的矛盾。

以上矛盾既有在“RPKI 基本原理范畴”的普遍性，又有在“网络互联互通特征范畴”的特殊性，因此需要构建一个能够因应网络规模和信任模型变化而灵活调整的可扩展 RPKI 依赖方系统部署机制。该机制映射至解决方案层面，即 RPKI 依赖方系统应当有哪些组件，组件如何在网络上分布及以何种逻辑关系进行分布。

RPKI 依赖方系统组件的功能解耦机制

可扩展 RPKI 依赖方系统部署机制在“RPKI 基本原理范畴”的首要任务是，通过对 RPKI 依赖方系统核心功能实施解耦，形成彼此“正交”的 RPKI 依赖方系统的组件布局。按此原则，基于 IETF RFC8897[4]，笔者从工程实践的角度梳理了 RPKI 依赖方系统在理论上的最低技术要求，包括：同步 RPKI 资料库的数据、处理 RPKI 资源证书、处理 RPKI 数据签名对象、分发验证过的 RPKI 认证信息以及本地化控制。一个具备 IETF RFC8897 所列举功能的系统，可以称为 RPKI 依赖方系统。

RPKI 依赖方系统在全球各个网络内的部署已逾 10 年，形成了一些运行实践和讨论。笔者在起草 IETF 标准和进行 RPKI 系统设计的工作中，有两点体会：在部署层面，RPKI 依赖方系统的功能仍需要进一步模块化（正交化）；在运行层面，IETF RFC8897 所列举的功能无法满足商用路由控制系统对 RPKI 依赖方系统的需求。为此，构建可扩展的 RPKI 依赖方系统的第一步是将其核心功能模块化，并给出各个模块彼此解耦之后的逻辑关系（接口关系）。图 3 是笔者对 RPKI 依赖方系统的设计思考和建议。



▲图 3 RPKI 依赖方系统组件

（1）更新感知系统

将“更新感知”功能同“数据同步”功能进行解耦，是互联网内容分发范畴常见的工程设计思路。当这一思路被应用到 RPKI 体系时，更新感知系统便成为了一个独立的 RPKI 依赖方系统组件。该系统采用实时或不定时的方式获得 RPKI 资料库（RPKI 数据发布点）的数据更新情况，并将这些更新信息传递给数据同步系统。

（2）数据同步系统

数据同步系统以“全量”或“增量”的方式，将 RPKI 资料库内发布的各类 RPKI 资源证书及 RPKI 数字签名对象下载到本地网络，以形成与 RPKI 资料库一致的且具有一定时效的数据副本。在当前的 RPKI 生态中，数据同步系统和 RPKI 资料库之间的接口已经在 IETF 形成标准 [5]。

（3）数据验证系统

数据验证系统先后对相关证书及数据签名对象进行语法检查和 RPKI 逻辑验证。其中，语法检查包括检查相关数据格式是否符合技术标准、是否在有效期内等，RPKI 逻辑验证包括验证 PKI 数字签名、验证相关的互联网码号资源包含关系 [6] 以及其他与 RPKI 授权体系相关的逻辑验证等。

（4）数据分析系统

RPKI 是一个分布式系统，因此位于不同 RPKI 授权体系子树上的数据可能存在冲突关系（码号资源分配、授权信息等）。数据分析系统旨在根据一定的算法，辅之以 WHOIS 数据、BGP 广播存档数据等带外数据，对潜在的冲突关系进行检测，给出可能的（本地化）修正方案，并输出至本地控制系统。

(5) 本地控制系统

出于网络管理和安全保障的需求，网络运行机构可能希望以“本地过滤和添加”的形式建立 RPKI 路由认证数据的本地视图，对来自全球 RPKI 的数据进行覆盖。本地控制系统对“验证缓存”直接进行操作，增加或删减相关的路由认证数据条目。工业界将这种操作称为 RPKI 本地化控制 (SLURM)。SLURM 配置文件格式已经在 IETF 形成标准 [7]。

(6) 数据分发系统

经过验证并最终可以供给路由器进行 RPKI 路由认证的数据称为“验证缓存”。基于“主从模型”，数据分发系统将“验证缓存”从一个网络节点分发至其他一个或多个有信任关系的网络节点，实现 RPKI 验证数据的共享。对于数据分发系统，RPKI 意义上的数字签名已不复存在，其完整性依赖于传输信道（如超文本传输安全协议）。

(7) 路由器对接系统

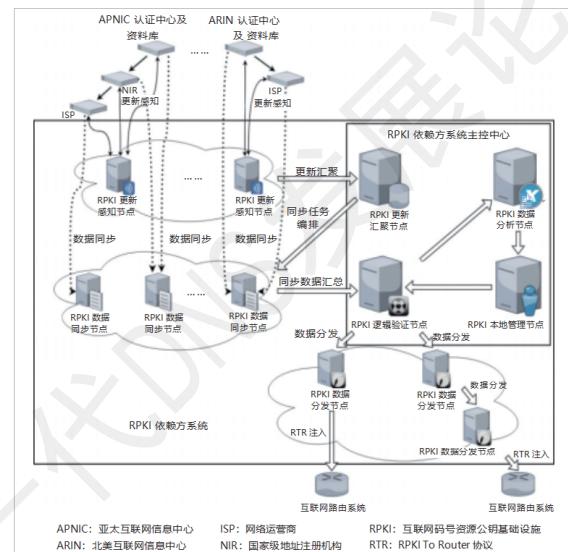
RPKI 供给侧形成的路由认证数据，通过同步、验证、分发、本地化处理，最终形成副本，然后经路由器对接系统，注入至 BGP 路由器。基于“客户端 - 服务器”操作模型，维护“验证缓存”的网络节点充当服务器，同时路由器充当客户端。两者之间的通信由一种 RTR 的 IETF 标准化协议承载 [8]。

RPKI 依赖方系统组件在规模网络上的编排机制

基于 RPKI 依赖方系统核心组件的解耦机制，本节探讨可扩展 RPKI 依赖方系统部署机制在“网络互联互通特征范畴”的特殊性，就如何将相关组件编排在网络运行机构所管理的云和网的不同位置，设计一个能够适配各类规模网络（骨干网运营商、互联网交换中心、内容

分发网络服务商等）的 RPKI 依赖方系统组件部署机制（框架）。

针对前文所述 RPKI 依赖方系统的 4 对矛盾，面向一个规模网络的一般特征，笔者建议在 RPKI 依赖方系统的组件颗粒度上展开相关设计，包括：一个 RPKI 依赖方系统北向分布式节点群组、一个 RPKI 依赖系统南向分布式节点群组和一个 RPKI 依赖方系统主控中心。如图 4 所示，北向分布式节点群组面向 RPKI 供给侧，从分布式的 RPKI 资料库获取 RPKI 原始数据，包含 RPKI 更新感知节点和 RPKI 数据同步节点；南向分布式节点群组面向 RPKI 需求侧，将验证过的 RPKI 路由认证数据分发给分布式网络的边界路由器，即 RPKI 数据分发节点的集合；主控中心负责 RPKI 数据的验证和其他综合处理任务，包含 RPKI 更新汇聚节点、RPKI 逻辑验证节点、RPKI 本地管理节点、RPKI 数据分析节点等。



▲图 4 规模网络上的 RPKI 依赖方系统组件部署示例

RPKI 依赖方系统的各个组件在该架构下的部署机制如下：

(1) 更新感知系统

鉴于 RPKI 资料库的全球分布特征，更新感知系统相应地采用分布式的更新获取方法。该系统拥有“更新感知模块”和“更新汇聚模块”。前者部署在分布式的“更新感知节点”之上。全体“更新感知节点”按照一定的编排算法各自分工，完成对 RPKI 资料库的遍历，并传递给负责整合更新信息的“更新汇聚节点”。“更新汇聚节点”再将更新信息传递至数据同步系统。

全球大型运营商（例如 Tier 1 ISP）或头部流量的互联网交换中心，可以考虑将更新感知系统的寻址信息（域名、IP 地址等）和接口方式公布出去，供相关的 RPKI 发布点主动推送更新信息。

(2) 数据同步系统

面向全球 RPKI 资料库的分布特征，数据同步系统也采用分布式的部署形态，根据一定的编排算法，将同步任务分散至不同的“数据同步节点”。“更新汇聚节点”负责运行该编排算法，在统筹更新任务来源、同步节点数量、同步节点分布位置等要素的前提下，实现同步任务的动态分配。多个“数据同步节点”的分布采用和“更新感知节点”类似的策略。

(3) 数据验证系统

面向 RPKI 的数据验证系统的核心是建立数据对象之间的关联，包括经典公钥基础设施（PKI）体系下的数字签名验证路径构建，以及 RPKI 特有的码号资源包含关系验证。这种“关联性”的验证任务（证书路径验证、资源包含关系验证）由数据验证系统的 RPKI 逻辑验证模块负责。该模块站在全局视角，以集中化的方式对来自不同“数据同步节点”的合规数据进行综合处理，并以“RPKI 逻辑验证节点”的形式部署在网络运行机构的网运中心（NOC）。数据验证系统的语法检查模块不涉及对数据关联性的验证，可以部署在“数据同步节

点”之上，对相关数据进行语法合规检查，实现“边同步，边语法检查”的高效机制。合规数据会汇聚至“RPKI 逻辑验证节点”。

(4) 数据分析系统

数据分析系统承担的是 RPKI 数据同步、验证等任务之外的旁路功能，宜独立部署在专用的 RPKI 数据分析节点之中。

(5) 本地控制系统

本地控制系统将连同其他一些面向 RPKI 的互联网码号资源本地管理支撑系统（可视化、运行监控等），部署在专用的 RPKI 本地管理节点之中。

(6) 数据分发系统

鉴于数据分发系统的核心任务是将 RPKI 验证缓存从集中管理的 RPKI 依赖方系统主控节点分发至分布式部署的路由控制系统，其部署节点宜根据网络运行机构所辖自治域的数量和管理机制进行规划，以方便 BGP 边界路由器在就近获取 RPKI 验证缓存的同时，在网络运行机构的网络管理边界之内形成一致的 RPKI 数据视图。数据分发系统部署在数据分发节点之上，并根据该系统所定义的“主从模型”使相关节点（“分发服务器模块”与“分发客户端模块”）形成一个有序的数据共享体系。

(7) 路由器对接系统

路由器对接系统部署在面向路由器服务的末梢数据分发节点之上。

RPKI 依赖方系统主控中心可部署在网络运行机构的 NOC 之中。北向分布式节点群组的节点数量和分布规则，可结合网络拓扑以及去 RPKI 资料库之“远近”（路由及寻址）情况量体裁衣。南向分布式节点群组的节点数量和分布规则，可参考网络运行机构的网络互联互通情况和管理机制进行规划设计。

总结与展望

RPKI 依赖方系统连接 RPKI 供给侧和 RPKI 需求侧，是各类网络运行机构开展 RPKI 应用实践的一个关键环节。RPKI 依赖方系统的研发和部署，既需要关注 RPKI 核心功能的“普遍性”问题，又需要兼顾网络互联互通特征的“特殊性”问题。相关解决方案需要考虑 RPKI 依赖方系统有哪些组件，各个组件如何在网络上分布，以及以何种逻辑关系分布。因此，各类网络运行机构使用 RPKI 依赖方系统实施路由认证，不仅是简单的软硬件集成，更需要设计能够“因地制宜”涵盖功能编排、部署方法及运行机制的一揽子解决方案。

面向 RPKI 依赖方系统的核心功能，本文梳理了影响 RPKI 依赖方系统运行效能的 4 对矛盾，并提出了一种可扩展的 RPKI 依赖方系统部署机制，包含软件层面的解耦机制和硬件层面的部署机制。本文相关论述是对 RPKI 依赖方系统在规模网络运行机构内进行服务模式设计的宏观思考。骨干网运营商、CDN 服务商和互联网交换中心，在互联互通格局和码号资源管理等范畴具有不同特征。面向这些特征，探索如何在现有网络运维管理系统上增量部署 RPKI 依赖方系统组件以及对应的运行机制，是 RPKI 路由认证领域下一步值得深入研究的问题。

参考文献

- [1] IAB. IAB statement on the RPKI [EB/OL].[2022-11-25].
<https://www.iab.org/documents/correspondence-reports-documents/docs2010/iab-statement-on-the>
- [2] rpki/
[3] KENT S, LYNN C, SEO K. Secure border gateway protocol(S-BGP)[J]. IEEE journal on selected areas in communications, 2000, 18(4): 582-592 . DOI : 10 . 1109/49 .839934
- [4] LYNN C, KENT S, SEO K X . 509 extensions for IP addresses and AS identifiers [EB/OL] . [2022-11-25] . <http://mirror.cogentco.com/pub/rfc/pdf/rfc3779.txt.pdf>
- [5] MA D, KENT S. Requirements for resource public key Infrastructure(RPKI) relying parties [EB/OL] . [2022-11-25] .
<https://www.ietf.org/rfc/rfc8897.pdf>
- [6] BRUIJNZEELS T, MURAVSKIY O, WEBER B, et al . The RPKI repository delta protocol (RRDP) [EB/OL] . [2022- 11-25] . <https://www.rfc-editor.org/rfc/pdfrfc/rfc8182.txt.pdf>
- [7] HUSTON G, MICHAELSON G, MARTINEZ C, et al . Resource public key infrastructure (RPKI) validation reconsidered[EB/OL].[2022-11-25].
<https://www.rfc-editor.org/rfc/pdfrfc/rfc8360.txt.pdf>
- [8] MA D, MANDELBERG D, BRUIJNZEELS T. Simplified local Internet number resource management with the RPKI (SLURM) [EB/OL].[2022-11-25].
<https://www.rfc-editor.org/rfc/pdfrfc/rfc8416.txt.pdf>
- [9] BUSH R, AUSTEIN B . RPKI to router protocol [EB/OL]. [2022- 11-25].
<https://www.rfc-editor.org/rfc/pdfrfc/rfc8210.txt.pdf>

后记

当前，新一代信息技术触发的新应用、新产业为互联网发展带来新的挑战与机遇。互联网与数字技术、产业融合加速发展，成为数字经济提质增效新引擎。互联网从最初的“连接”作用，发展成为全球各国数字社会的底座与根基。

尽管我国互联网用户人数居全球第一，从网络规模覆盖上，中国是名副其实的网络大国，但与网络强国相比，中国还有较大差距。在互联网基础资源拥有数量、关键技术突破等方面，仍有较大提升空间。随着数字经济蓬勃发展，数字化应用与基础网络的连接日益紧密，网络根基的安全与高效对经济发展、社会生活都举足轻重。在重视互联网上层应用与万物互联终端迅速发展的同时，更应关注网络基础设施建设，这也是我国数字信息基础设施建设的底座与根基。网络基础设施发展离不开互联网治理、资源、技术，作为网络大国，中国如何参与全球互联网治理体系、如何争取网络空间的关键资源、如何升级网络核心技术，这不仅是迈向网络强国的必经之路，也是数字中国建设过程中，网络基础技术升级的必然。

2022年《下一代DNS发展报告》以立足全局、着眼未来的视角，以鉴往知来、与时俱进的思考首次全面、系统推出下一代DNS体系，获得广泛关注。

《2023年下一代DNS发展报告》继续以开放、前瞻、务实的风格，打开研讨空间：

开放性。正如互联网的出现，是无数技术集群产生的结

果；对互联网未来发展的思考，依然需要多方参与。本报告在D、N部分，重点收录了中国专家、学者的观点，这也正是互联网治理体系下，中国智慧的体现；同时增加了国际互联网社群动态，以呼吁和鼓励更多中国机构、互联网企业，体会互联网开放包容、共享共治的特点，在发展中放眼全球，积极参与互联网治理。

前瞻性。互联网既是技术的化身，也依赖于技术进步。网络基础技术正在发挥着更重要的连接作用，不仅是支撑互联网繁荣创新的根本，也是深入到各行业的万物互联的智能中枢。总结技术应用当下、探知技术发展的未来，是本报告S部分重点体现的内容，也是中国互联网工程师对DNS技术发展与时俱进的思考。

务实。下一代DNS体系探讨的标准、资源、技术，已不仅是理论根基，相较于上一年内容，报告增加了更多来自于市场侧对技术和产品的需求反馈。需求牵引技术进步，技术推动产品创新，这是下一代DNS技术产品化、产品产业化的基石，也是更广阔的空间与未来。

保持专注、勇于探索，适时总结、持续提升——《下一代DNS发展报告》体现出DNS行业从业者的实践与思考。下一代DNS产品正逐步在各行业领域应用，成为自主可控、承载万物互联的智能网络中枢，但随着数字技术的深入与发展，下一代DNS的内涵与外延依然需要以发展的眼光不断研究、实践。望远山而力行，携手更多互联网人，筑牢网络根基，支撑未来发展。

欢迎批评指正。

