

阿里云DNS – 打造安全稳定的数字经济基础设施

宋林健 博士

阿里云网络高级架构师

2020/8/12 互联网基础资源论坛，北京网络安全大会

目 录

CONTENT

● 背景：DNS技术趋势和热点

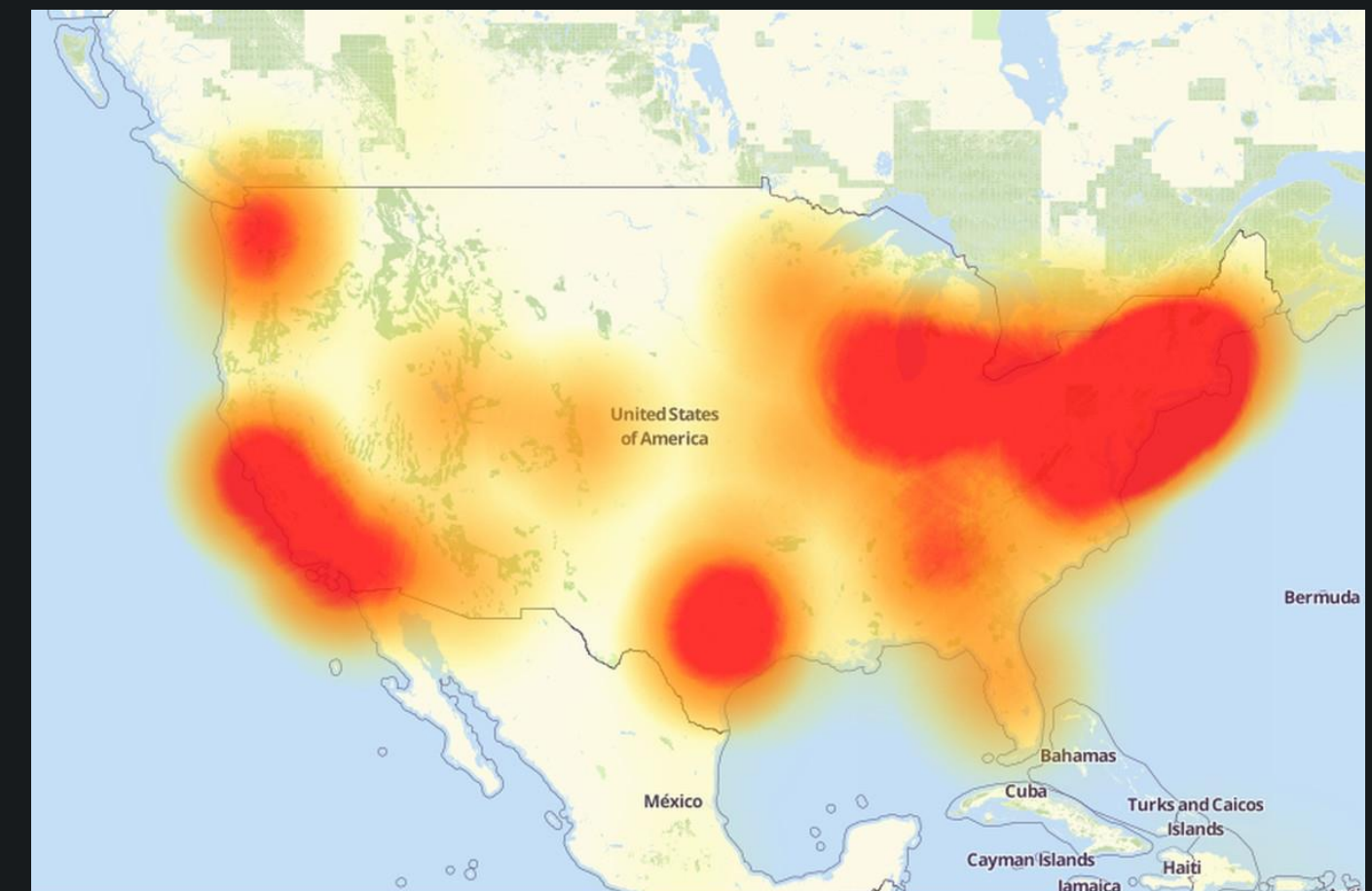
● 阿里云DNS解决方案与实践

● 总结

域名系统DNS安全和故障事件

- 2015年11月部分DNS根服务器被攻击，部分地区访问不畅
- 2016年10月21日美国域名供应商DYN的DNS网络遭受DDOS攻击，导致美国网络大范围瘫痪
- 2019年10月23日云服务公司AWS遭遇了DDoS攻击，持续了15个小时，造成AWS部分服务瘫痪
- 2020年2月27 Cloudflare软件更新搞瘫全球 F、E DNS根服务器瘫痪
- 2020年7月16日 Cloudflare DNS服务器故障导致国内外大量网站无法正常解析访问

其他：DNS劫持、数据篡改、网络钓鱼、域名隐私泄露等



互联网基础资源解析和调度

互联网业务应用

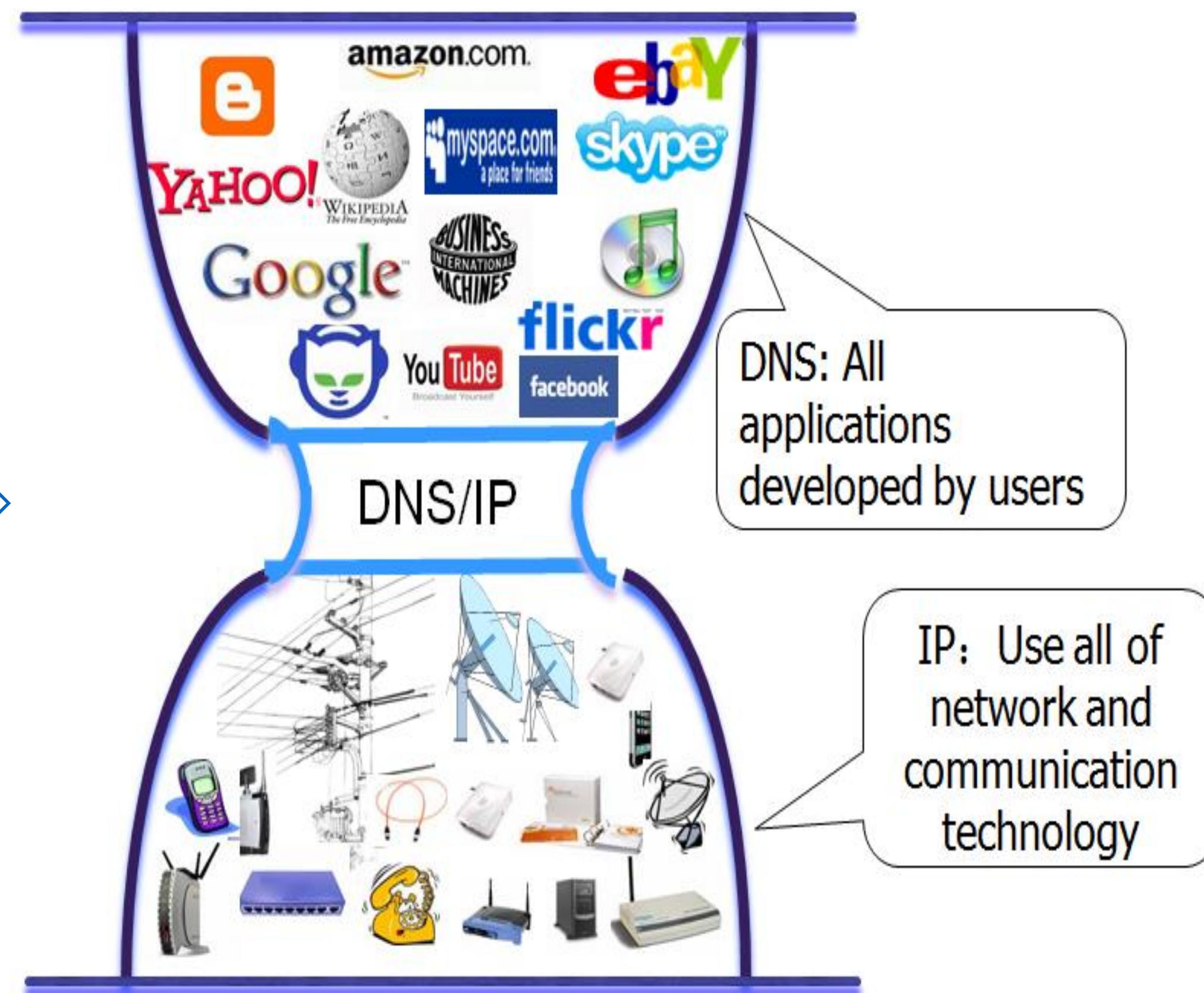
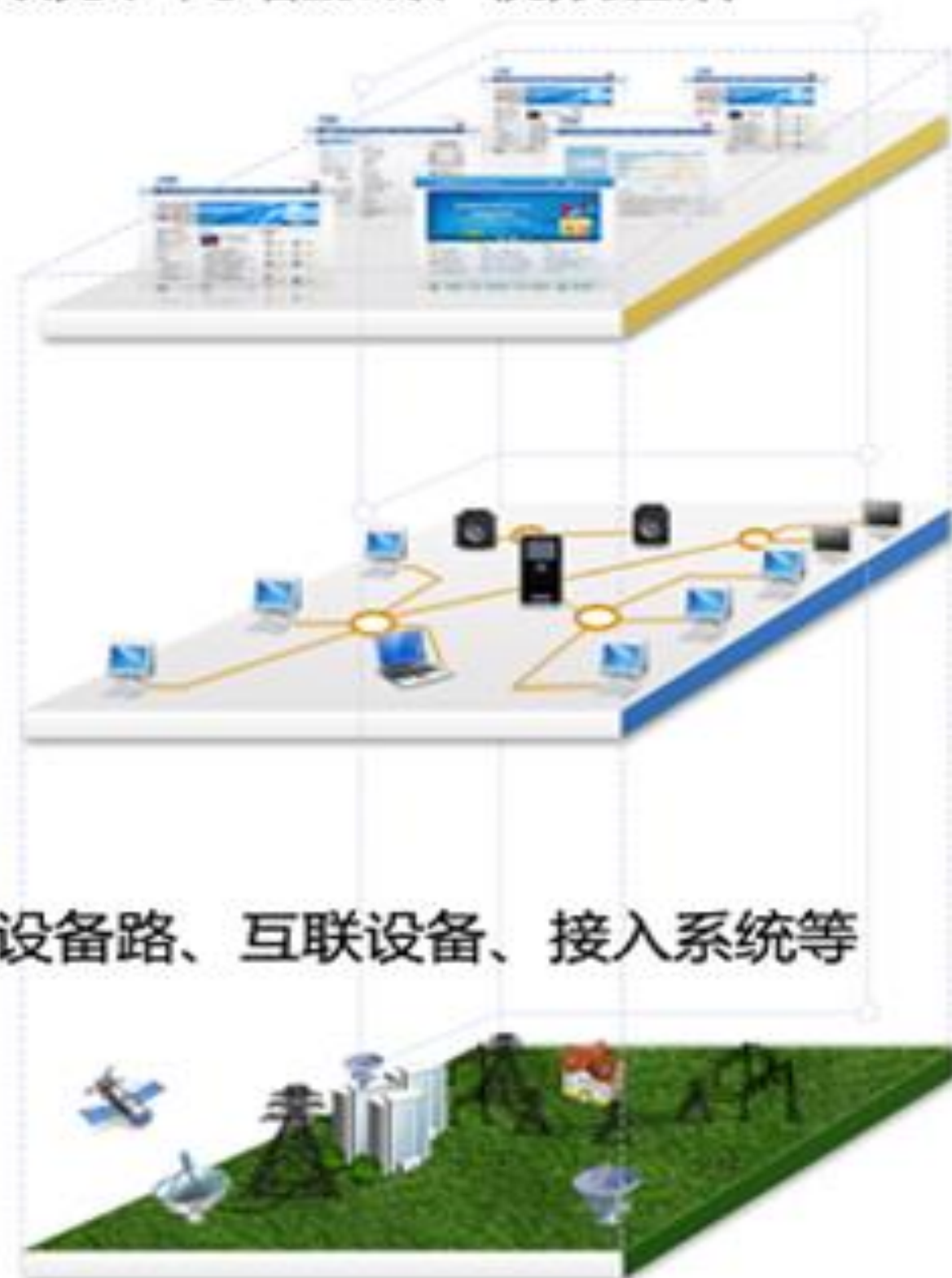
电子商务、电子政务、网络游戏、视频通讯

互联网基础资源

域名、IP地址等

互联网物理设施

基础网络、传输设备路、互联设备、接入系统等



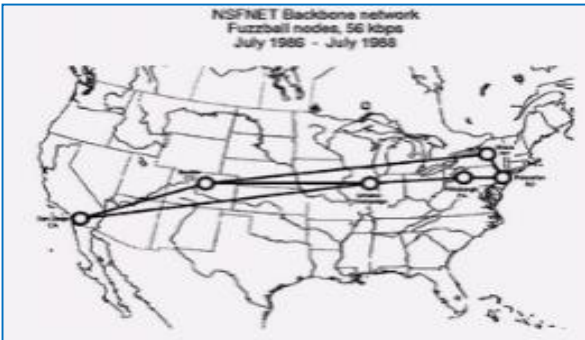
DNS是互联网访问和资源调度的入口，是“互联网的心脏”

DNS功能和角色的演进 – 服务更大的网络规模

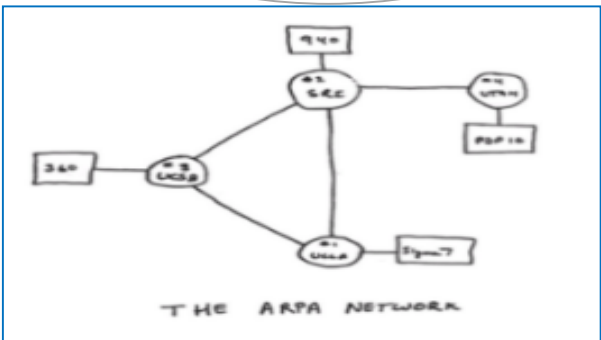
网络用户和连接规模指数型增加，为网络IP寻址调度带来了机遇和挑战

诞生

- 互联网诞生于美国，用于军事和科研
- 接数：4台计算机

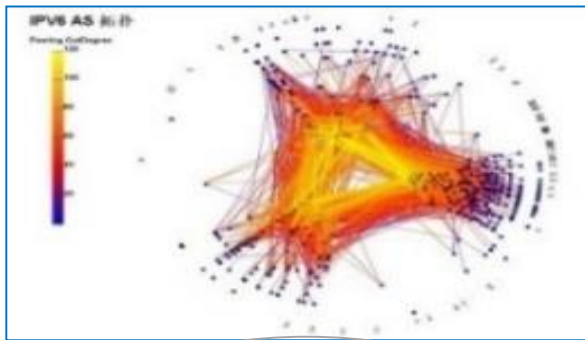


1969



高速普及

- PC机普及
- WWW, HTTP, Web建站技术出现
- PC搜索、门户网站、博客，网络媒体
- 连接数爆发式增长：亿级，域名数量百万级



1980s

1990s

2000s

发展

- TCP/IP协议成为互联网核心协议，开始民用化
- 满足网络规模增长和管理 - DNS协议和系统
- 连接数快速增长：数千台计算机



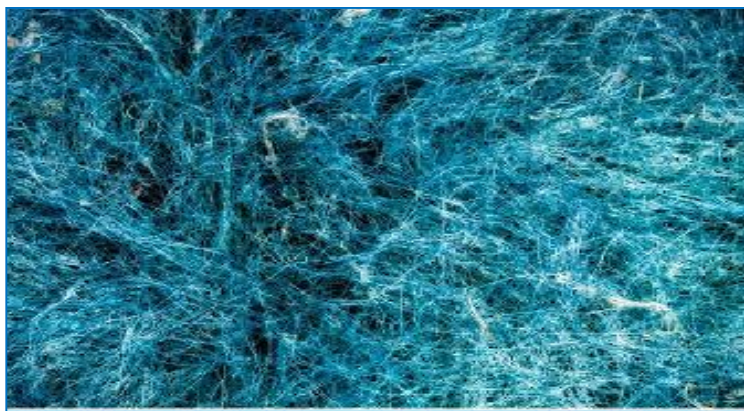
移动互联网+云计算

- 4G、智能手机，APP，H5，云服务等技术
- 移动社交、电子商务、移动视频等应用
- 域名，APP数量超过 五百万
- 十亿终端，百亿连接

万物互联

- 5G，IoT，IPv6，智能终端，工业互联网
- 人人互联、人物互联、物物互联
- 终端百亿，连接数万亿

未来



最初服务于网络连接，域名IP数据库

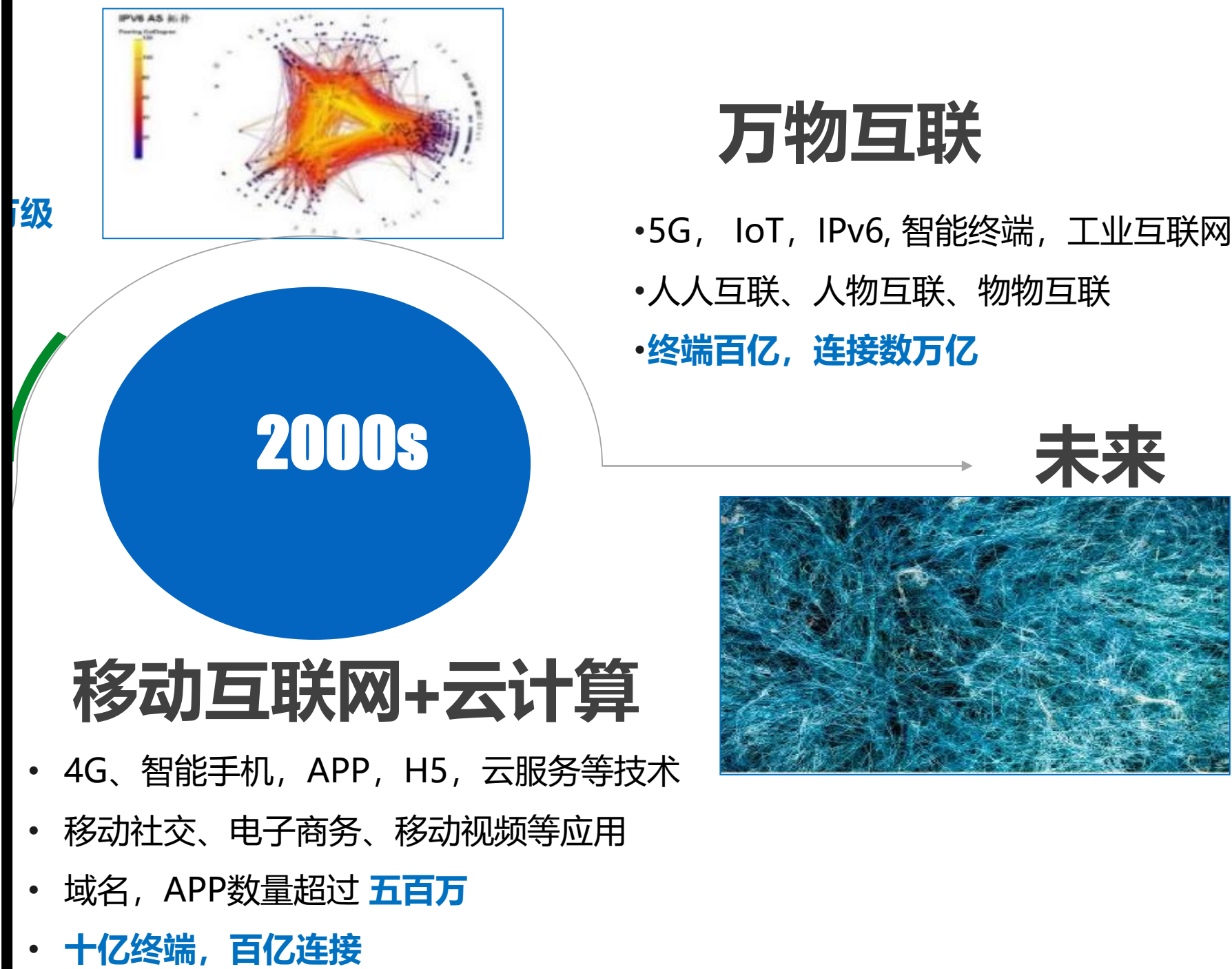


满足网络稳定、安全、高效的智慧大脑

DNS功能和角色的演进 – 以应用和业务为中心

新技术应用和网络治理政策对域名系统提出了新的需求

- **移动互联网**
 - APP端、网、云服务向开发者集中，产生了应用层的DNS场景
 - DNS解耦地址和标识、隔离网络动态变化，保持上层应用稳定
- **云计算**
 - 云上DNS解析量逐步超过了云下传统DNS解析需求，DNS互联互通的目标 变成 快速、安全、稳定的定位和访问云资源
- **IoT物联网**
 - IoT发起的DDoS攻击，IoT/BYOD设备泄露隐私 [ICANN SAC105 : The DNS and the Internet of Things: Opportunities, Risks, and Challenges](#)
 - 工业互联网，多种互联网标识和解析系统共存: OID, ONS, Handle
- **互联网治理和政策**
 - 监管、过滤、数据本地化、根服务器自治等
 - 在断网、“净网” 的风险下保持互联互通



DNS加密和隐私保护

- DNSSEC(RFC4033/4034/4035)并没有特别的针对数据保密和用户隐私性的要求, DNSSEC 唯一的隐私性考虑 是避免区文件被遍历枚举的风险, 增加了NSEC3协议
- 斯诺登事件之后, IAB/IETF开始热议隐私性问题, 陆续发布了相关标准和技术要求: RFC7526 DNS Privacy Considerations, RFC7858 DNS over TLS (DoT) , RFC8484 DNS over HTTPS (DoH)
- 2019年 DNS技术社群发起的 “DNS加密部署计划”, IETF 发起ADD工作组 (<https://datatracker.ietf.org/wg/add/about/>)
- 截止到2020年7月底:
 - 操作系统支持DNS加密: 苹果IOS、微软windows, 谷歌Android
 - 主流浏览器和内核支持DoH: Chrome和Firefox
 - 公共DNS加密服务: Google DNS, Cloudflare DNS, 阿里云公共DNS



ENCRYPTED DNS DEPLOYMENT INITIATIVE

LEARN MORE

We're banding together to globally adopt encrypted DNS.

Encrypted DNS Deployment Initiative

The Domain Name System (DNS) is the Internet's naming protocol, translating names like example.com into the IP addresses of destination servers. Users rely on the DNS for all they do - from using the web to mobile apps, streaming video, email, and more. Our goal is to work together to adopt new encrypted DNS standards on a global basis to improve user privacy & security, while also preserving

目标: 保证DNS机密技术的全球部署和大规模稳定运行

ORGANIZATIONS

adnet.uk, Akamai, APNIC, Bluecat, BT, Cablelabs, CIRA, Charter, Comcast, COX, EFF, CZ.NIC, F5, Georgia Tech, h2m, Infoblox, ISC, ISPA, Microsoft, neta, OX, OXFORD, Sam Knows, Shaw, sky, sinodun, Sprint, TalkTalk, TCPWave, Threat, Verizon

目 录

CONTENT

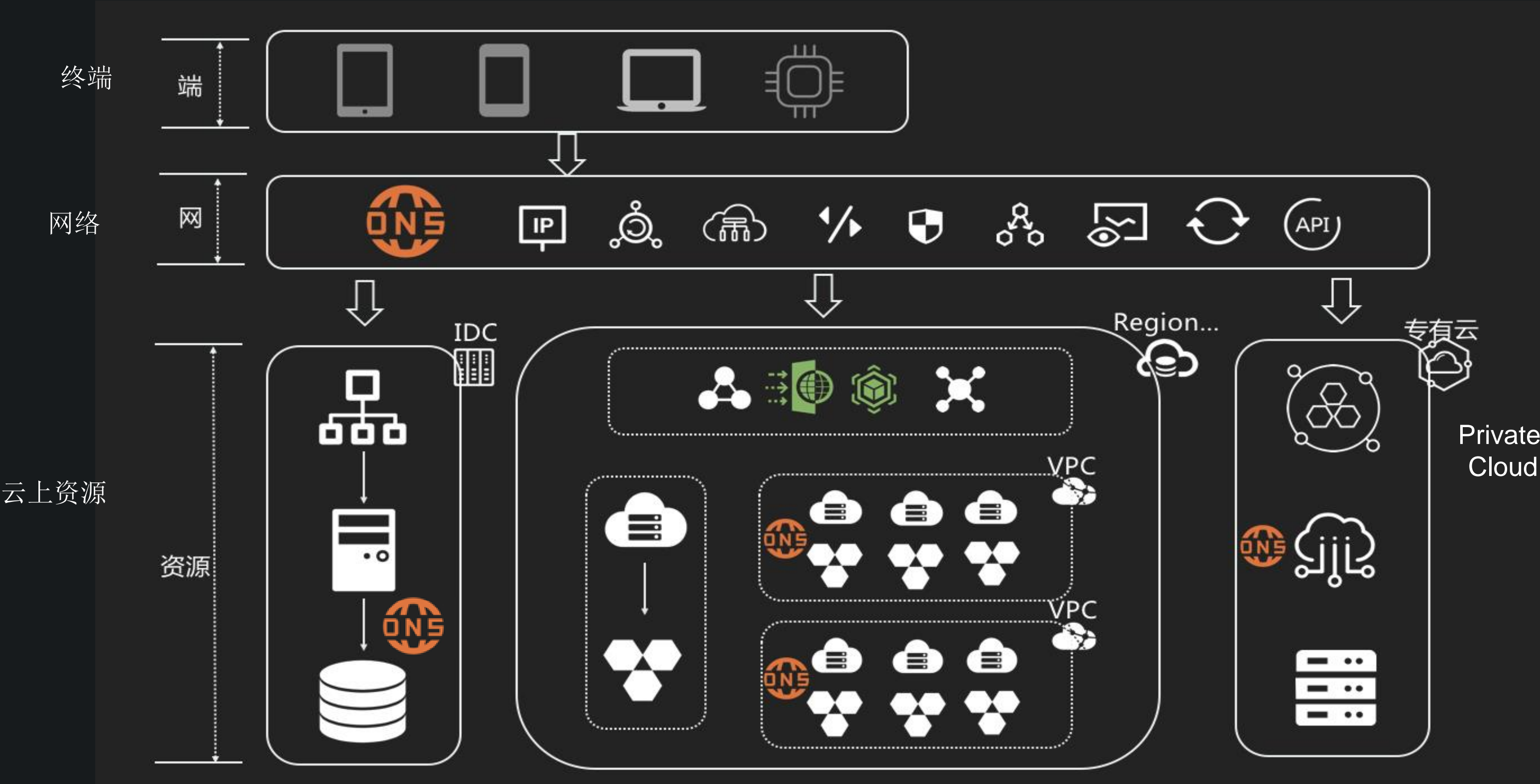
● 背景：DNS技术趋势和热点

● 阿里云DNS解决方案与实践

● 总结

阿里云DNS – 角色和挑战

阿里云DNS提供一站式IP寻址调度服务，让各类型终端快速、安全、稳定的连接云上资源



超大规模

- 服务 **10亿+** 用户和 **1700万+** 域名
- 每天处理 **7000亿** 次查询 (递归和权威)
- 服务内部全球 **21** 区域 和 **百万级别** 虚拟机

+

- 高性能 (Performance)
- 可靠性和服务保证 (SLA)
- 精准的流量调度
- 多策略负载均衡

阿里云解析DNS是亚洲最大的DNS服务提供商

阿里云DNS – 产品介绍

阿里云DNS是阿里云提供的全系列域名解析服务产品总称，覆盖以下DNS全场景，为企业提供一站式DNS服务体验

- **云解析DNS** 公网权威DNS，域名总量**1700**万+，占全国备案域名的**48%**
- **PrivateZone** 阿里云VPC的内网权威DNS
- **阿里云公共DNS** 公共递归DNS和缓存DNS-- 国内首家支持DoT/DoH，IPv4/IPv6双栈
- **专有云DNS** 基于阿里云专有云的DNS服务
- **全局流量管理 GTM**，实现权重轮询，健康检查，备份切换和故障转移 等功能



云解析DNS



云解析PrivateZone



阿里云公共DNS



专有云NS



全局流量管理



DNS产品页

阿里云DNS – 安全能力

抗DDoS
攻击

联合云盾构建防护网
络， T级安全防护

数据安全
DNSSEC

2020年1月上线
保障数据的一致性

DNS加密
DoH/DoT

2020年四月发布
公共DNS DoH/DoT服务
保护隐私， 安全稳定的连接

DNS根镜像
和应急备份

引入F和J根镜像
建立本地根区备份

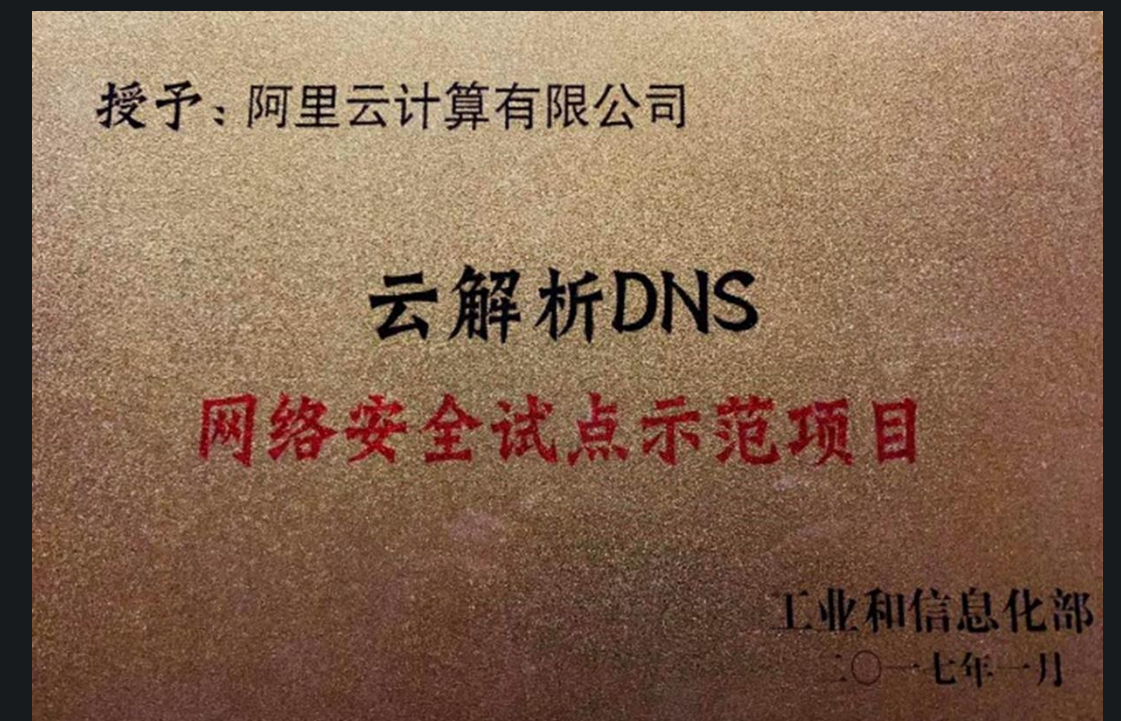
阿里DNS – 安全能力

更稳定

- BGP+ANYCAST技术实现DNS故障的自动转移，可保服务始终在线并稳定运行。
- 全球DNS集群互相备份，可保障服务永不宕机，提供100%服务可用性承诺。
- 解析数据实时同步全球DNS节点，可保障解析数据全网一致性。

更安全


- 流量攻击：全球10T+带宽储备和多个大型流量清洗中心，免费享超大规模DDOS流量攻击防护
- 查询攻击：单集群每秒过亿防护能力，全球40多个集群
- 数据高可用：DNS数据按小时或按天备份，可一键恢复至备份版本，有效防止数据丢失
- 服务双保障：提供辅助DNS，当面对自建DNS异常或业务需要时，支持平滑切换
- 数据安全性：支持DNSSEC，避免DNS劫持/缓存投毒，保障网站访问安全



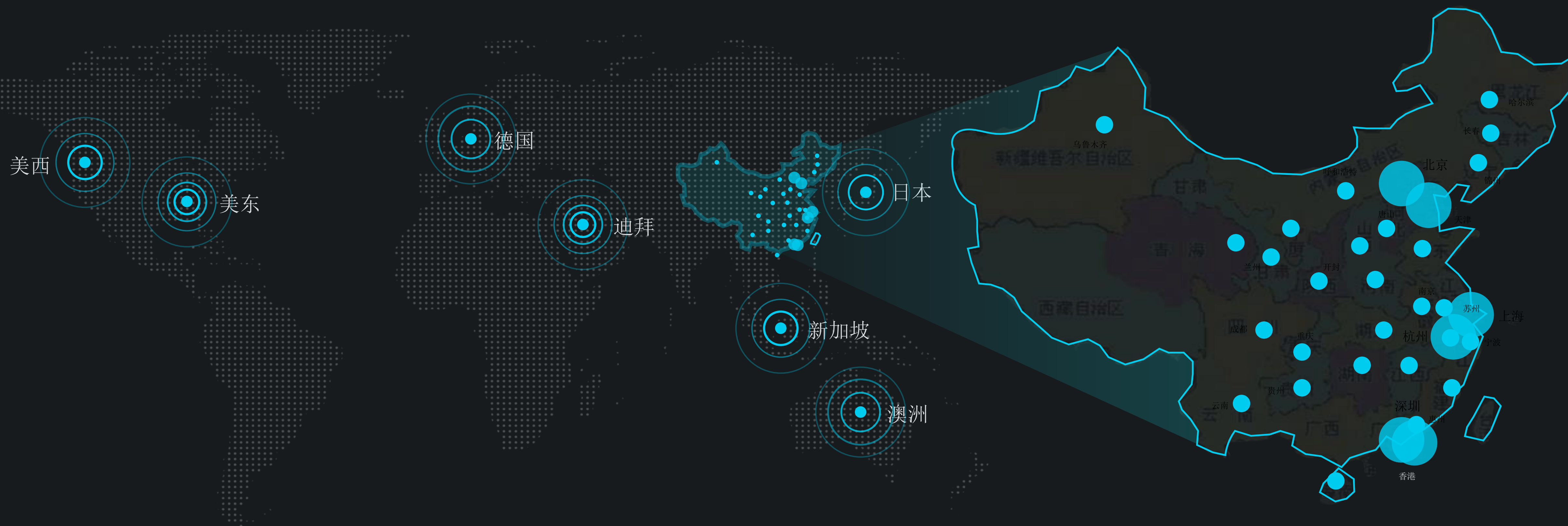
2017年1月 阿里云云解析DNS入选工信部评选的网络安全试点示范项目

2020年3月阿里云云解析DNS被工信部重点推荐，支撑疫情防控和复工复产的网络安全公共服务平台

阿里云DNS - 业务节点分布

Alibaba Cloud | 
Worldwide Cloud Services Partner

有阿里IDC的地方就有DNS集群和DNS流量清洗集群



- **DNS集群与流量清洗集群覆盖全球21个Region，40多个集群，近百个可用区**
- **联合云盾构建防护网络，T级安全防护，保障接入层安全，简化业务网络架构**

阿里云DNS - 安全扩展DNSSEC

DNSSEC对DNS记录签名和校验，是保障DNS数据一致性的技术手段

DNSSEC部署的难度和挑战

1. DNSSEC是可选项，未在全球大规模部署
2. 大规模的DNSSEC签名技术难度和经验
3. 与现有的DNS架构的结合和升级，会带来风险
4. DNSSEC会影响解析性能，性价比低

阿里云DNS为什么部署DNSSEC

1. 来自真实用户的需求 – 用户第一
2. DNS基础安全能力 – 极客精神
3. 相信DNS未来应用场景和潜力
权威网络Repo, 区块链与DNS, Crypto Key...

参考: [阿里云DNSSEC技术实践](#)



ikea.cn



现在



阿里云DNS - 安全扩展DNSSEC

Use .XYZ as your Ethereum Wallet!



XYZ and Ethereum have partnered to allow you to pair your .xyz domain with your Ethereum wallet via the main ENS network.



For every wallet, everywhere



ethereum

This means your .xyz domain can harness the power of the DNS to function as an easily memorable custom identifier for your Ethereum wallet, allowing you to manage your assets while retaining security.

<https://gen.xyz/ethereum>

阿里云DNS为什么部署DNSSEC

1. 来自真实用户的需求 – 用户第一
2. DNS基础安全能力 – 极客精神
3. DNS未来应用场景和潜力 – 相信
权威网络Repo, 区块链与DNS, Crypto Key...

参考: [阿里云DNSSEC技术实践](#)



ikea.cn



现在

搭建测试环境, 做DNS软件Gap分析

开始DNSSEC产品研发和测试

2017

2019.1

2019.3


2020.1

跟踪技术讨论和最佳实践

收到客户需求, 开始产品立项和规划

DNSSEC商用版对付费用户正式发布

公共DNS全新升级 - 国内首家DoH/DoT的云解析服务

Alibaba Cloud | 
Worldwide Cloud Services Partner

阿里云公共DNS 免费提供DNS加密解析服务



公共解析服务

[首页](#)[设置帮助](#)[知识中心](#)[节点分布](#)[联系我们](#)

IPv4: 223.5.5.5 / 223.6.6.6
IPv6: 2400:3200::1 / 2400:3200:baba::1

阿里云公共DNS

快速、稳定、智能

[快速设置](#)

IPv4: 223.5.5.5 / 223.6.6.6
IPv6: 2400:3200::1 / 2400:3200:baba::1



国内首家支持DoH/DoT的公共DNS云服务开始公测!

传统的DNS查询和应答采用大都采用UDP明文传输,存在网络监听、DNS劫持、中间设备干扰的风险。为了应对以上挑战,阿里公共DNS对外提供支持DoH/DoT的云服务,为广大的互联网用户提供快速、稳定和安全的DNS解析,欢迎大家使用!

<https://www.alidns.com/>

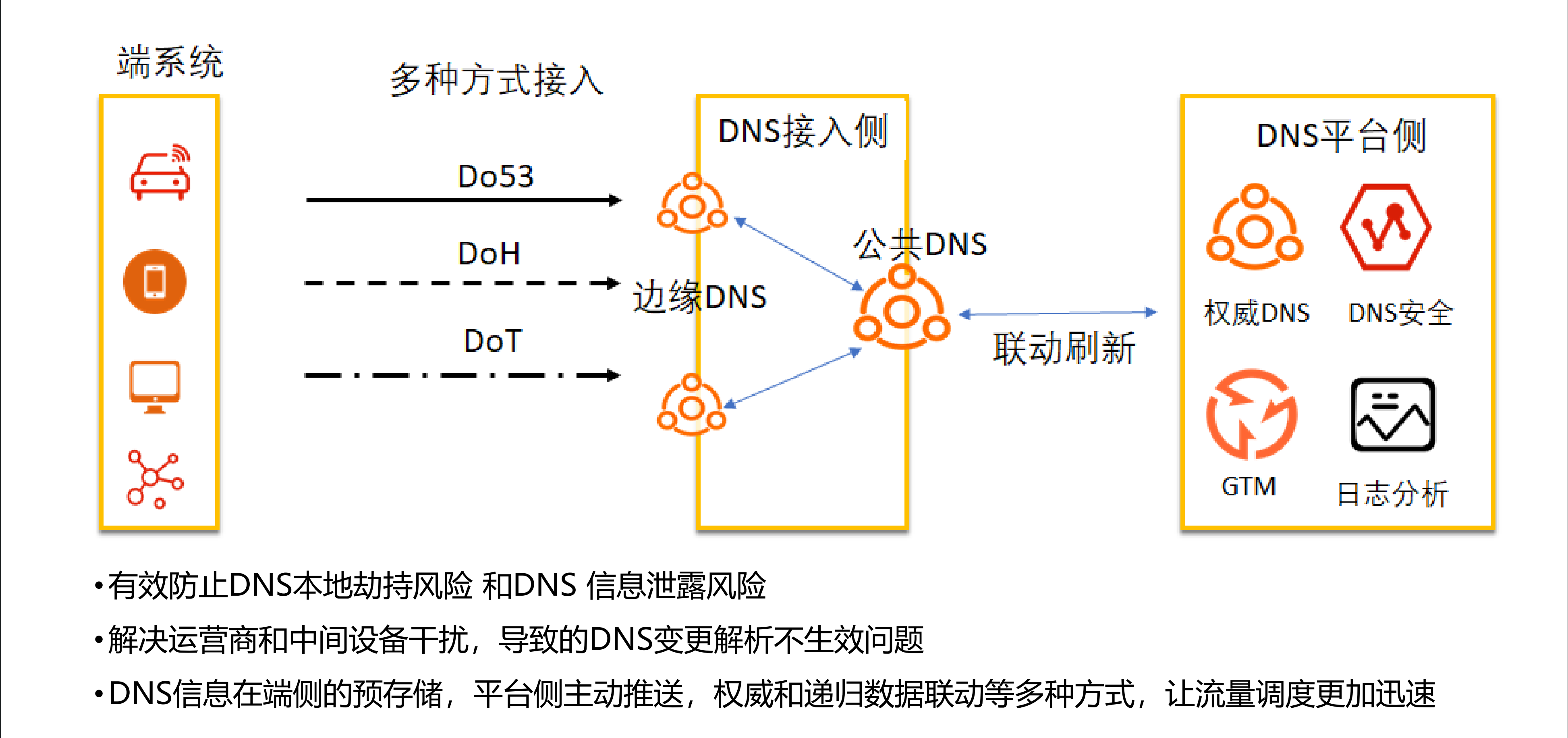
DoH地址: <https://dns.alidns.com/dns-query>
https://alidns_ip/dns-query

DoT地址: [dns.alidns.com](https://dns.alidns.com/dns-query), [alidns_ip](https://alidns_ip/dns-query)

注: alidns_ip是指 223.5.5.5, 223.6.6.6。

公共DNS全新升级 – 面向智能终端的解决方案

适用于IoT，智能终端，移动app和边缘解析场景下的DNS快速、稳定、安全解析场景



公共DNS还能提供给用户注册和控制台功能，用户可以充分体验云解析能力

注：Do53是传统的基于UDP的DNS访问



产品发布页



钉钉客户群

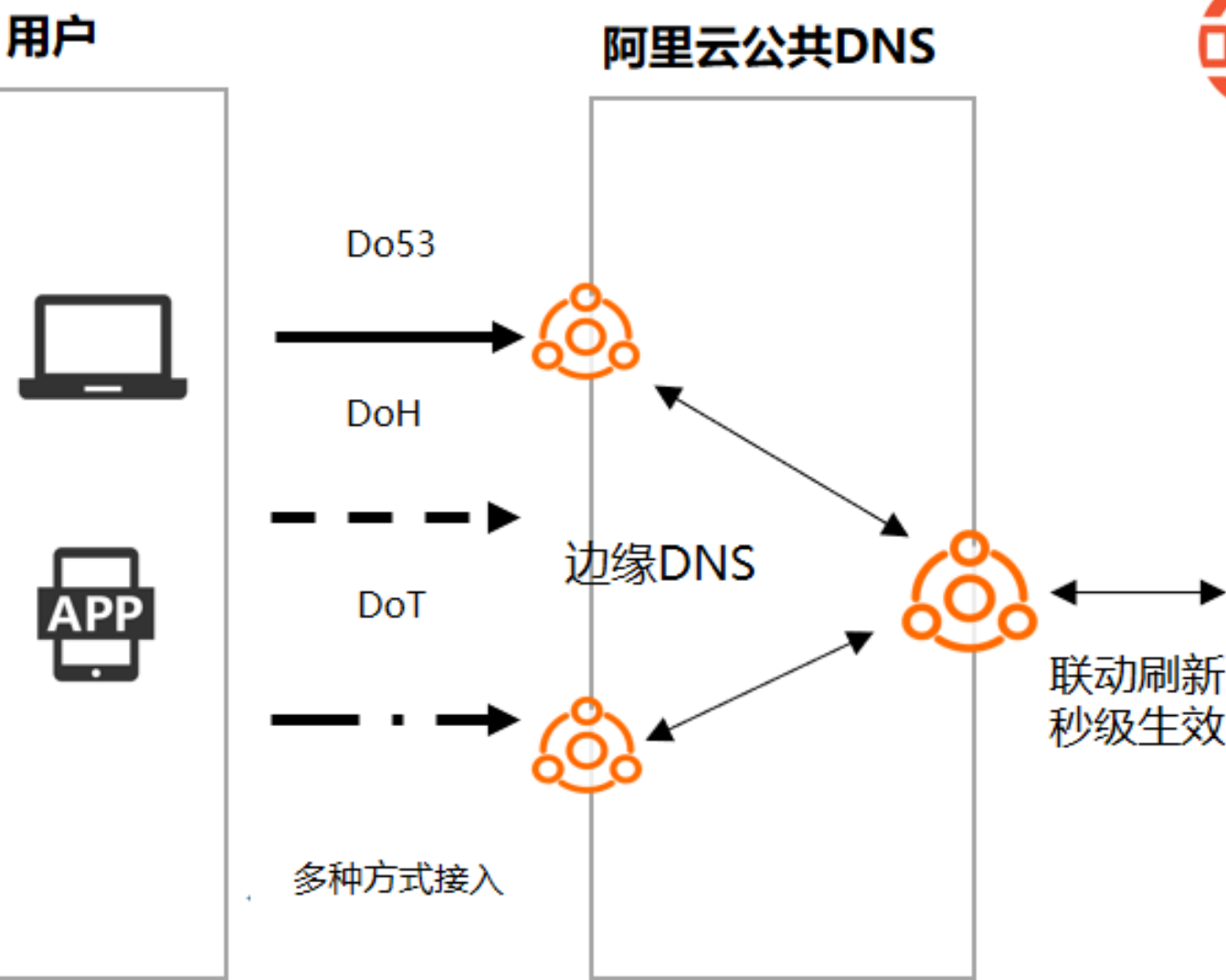
阿里云DNS -安全整体解决方案

面对大流量DDoS攻击导致服务不可用的安全风险，可以通过 阿里云公共DNS+云解析DNS+全局流量管理+高防IP 搭配使用，提高整体防护能力。适用于安全威胁风险较高的行业用户，例如新零售、游戏、视频、直播、金融、自建高防业务类。

■ 阿里云公共DNS

- 有效防止DNS本地劫持风险和DNS信息泄露风险
- 解决运营商和中间设备干扰，导致的DNS变更解析不生效问题
- DNS信息在端侧的预存储，平台侧主动推送，权威和递归数据联动等多种方式，数据变更不受中间设备干扰，让流量调度更加迅速

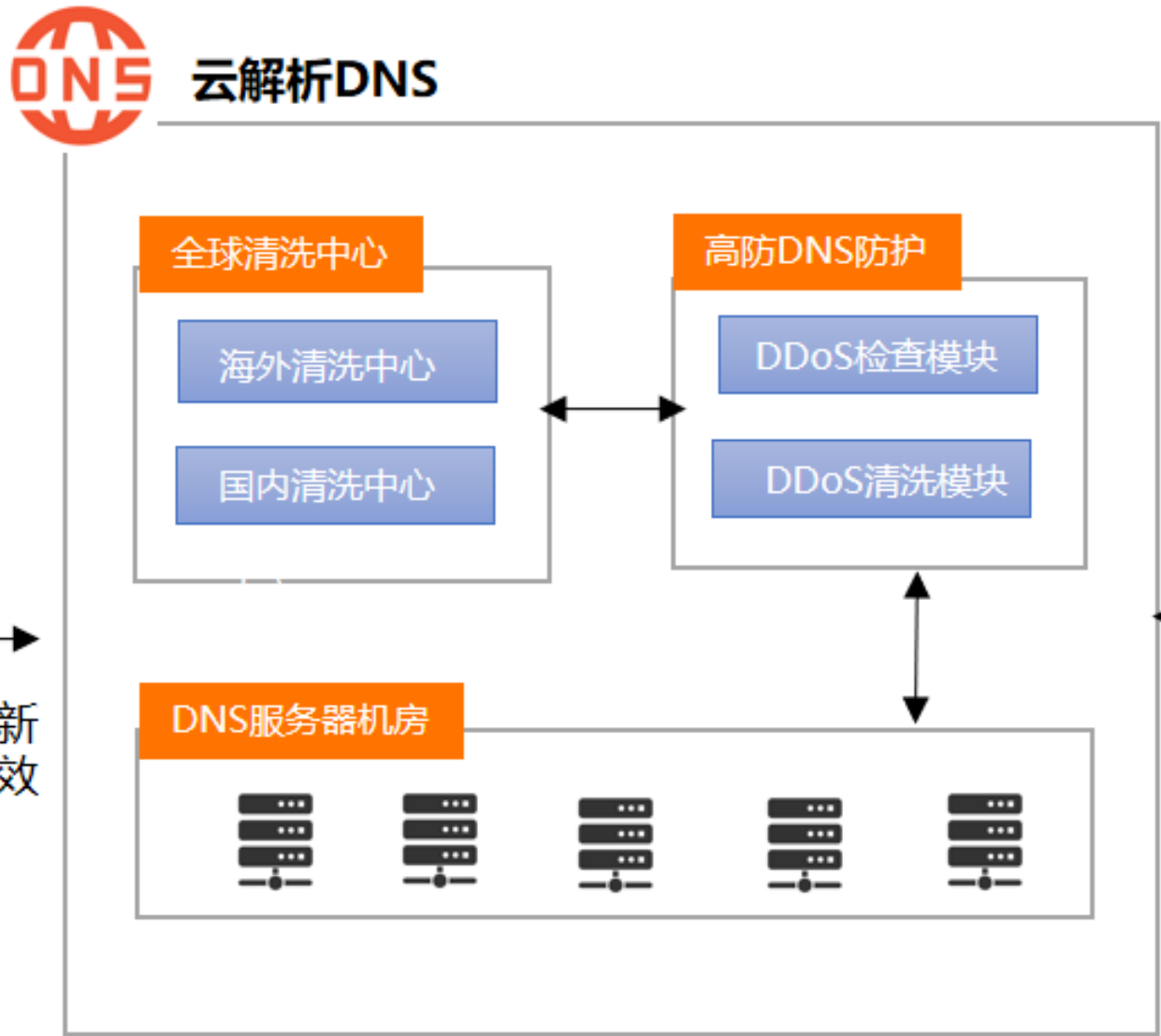
防劫持、生效快



■ 云解析DNS

- 全球10T+带宽储备和多个大型流量清洗中心，轻松应对超大规模DNS DDoS流量查询攻击
- 单集群每秒过亿防护能力，全球40多个集群，DNSQuery攻击全力防御无上限。
- 支持DNSSEC，避免DNS劫持/缓存投毒，保障网站访问安全。

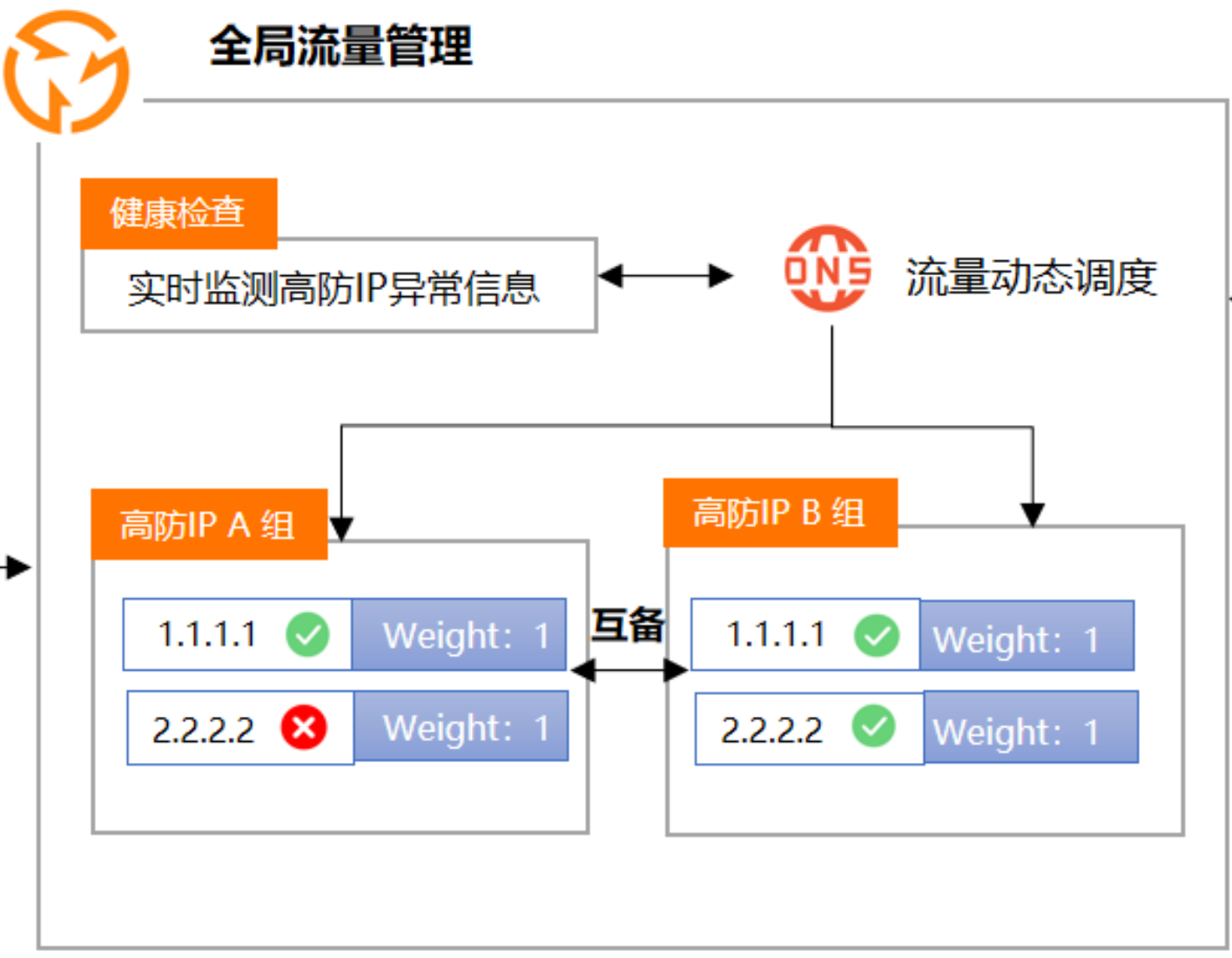
DNS抗攻击，业务安全更可靠



■ 全局流量管理

- 权重轮询：IP地址轮询暴露，攻击无法一次性实现瘫痪目的。
- 健康检查：及时发现IP地址异常、故障信息
- 备份切换：多地址池互为备份，对业务全局兜底
- 故障屏蔽：故障地址，可动态摘除

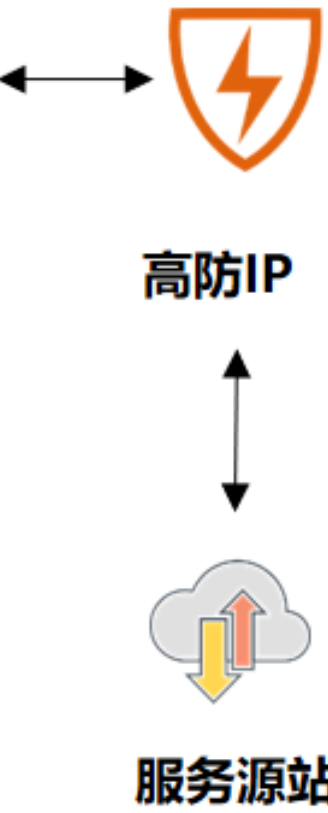
容灾备份，业务安全双保险



■ DDoS 高防IP

- 将对网站或应用的攻击流量，引流到高防IP，确保源站的稳定可靠
- 全球防护，10T防御

网站防护

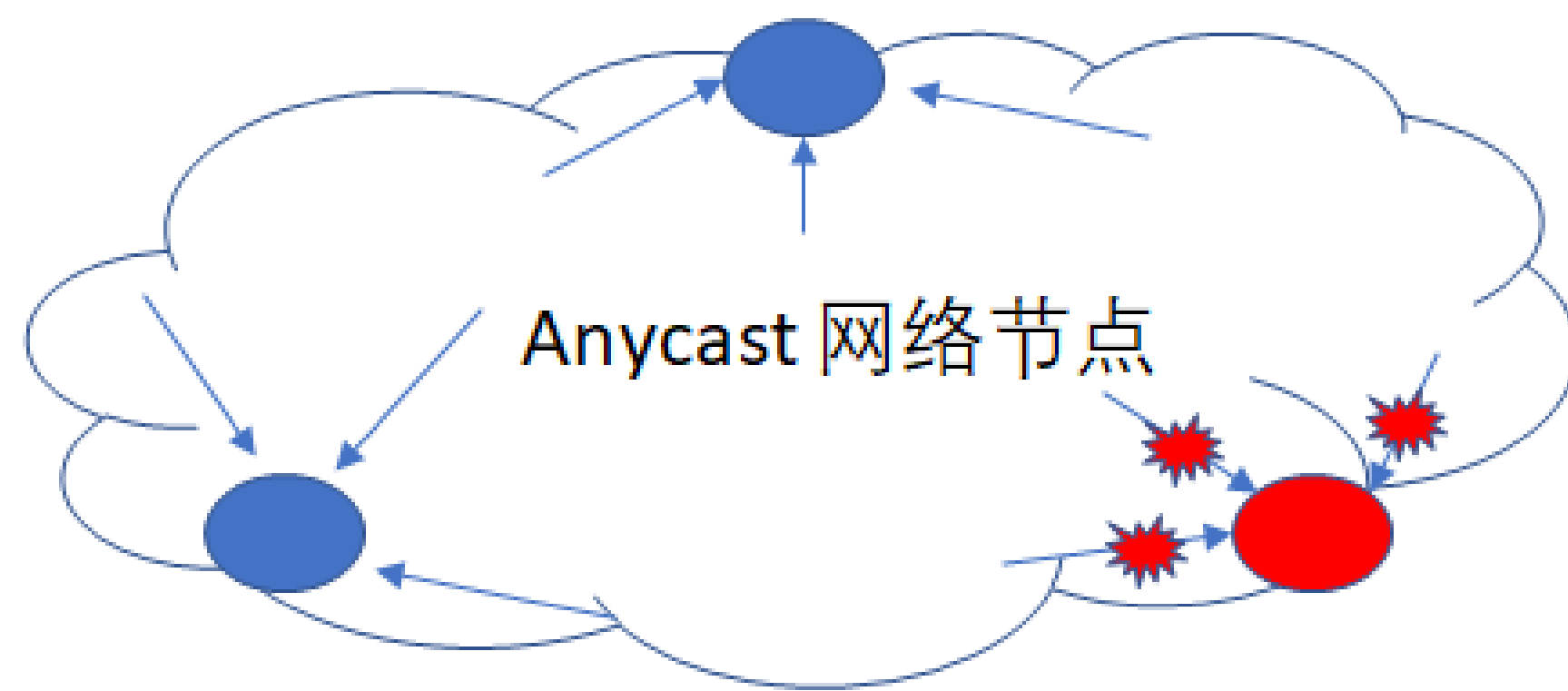


阿里云参与引入DNS根镜像

阿里云的根服务器工作主要是以优化网络性能，增加DNS高可用为目标

1. 引入根镜像能够根服务器失效减少故障

比如：双十一期间印尼IDC localDNS访问根服务器 报警 Timeout

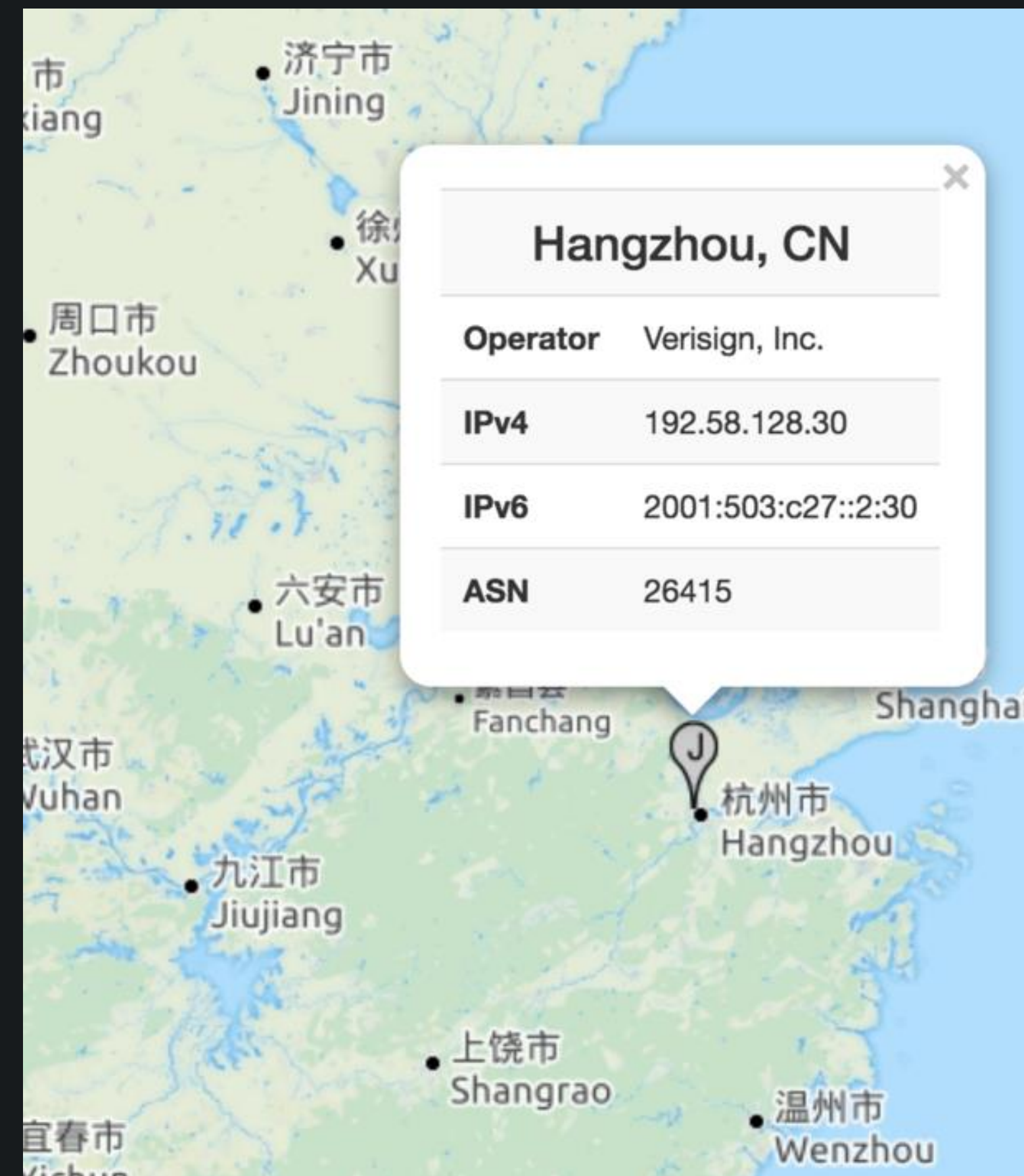


遭受DDoS攻击时，采用网络流量隔离的安全策略

2. 引入根镜像能够减少DNS根区访问延迟

跨洋 > 200ms, 跨国 > 50ms, 国内ISP 10~50ms, 同Region < 5ms

3. 采用本地根区备份方案做为应急机制，防止根服务器不可用



DNS根服务器去中心化的相关工作和讨论

- ICANN的做法: Hyper-Local Root

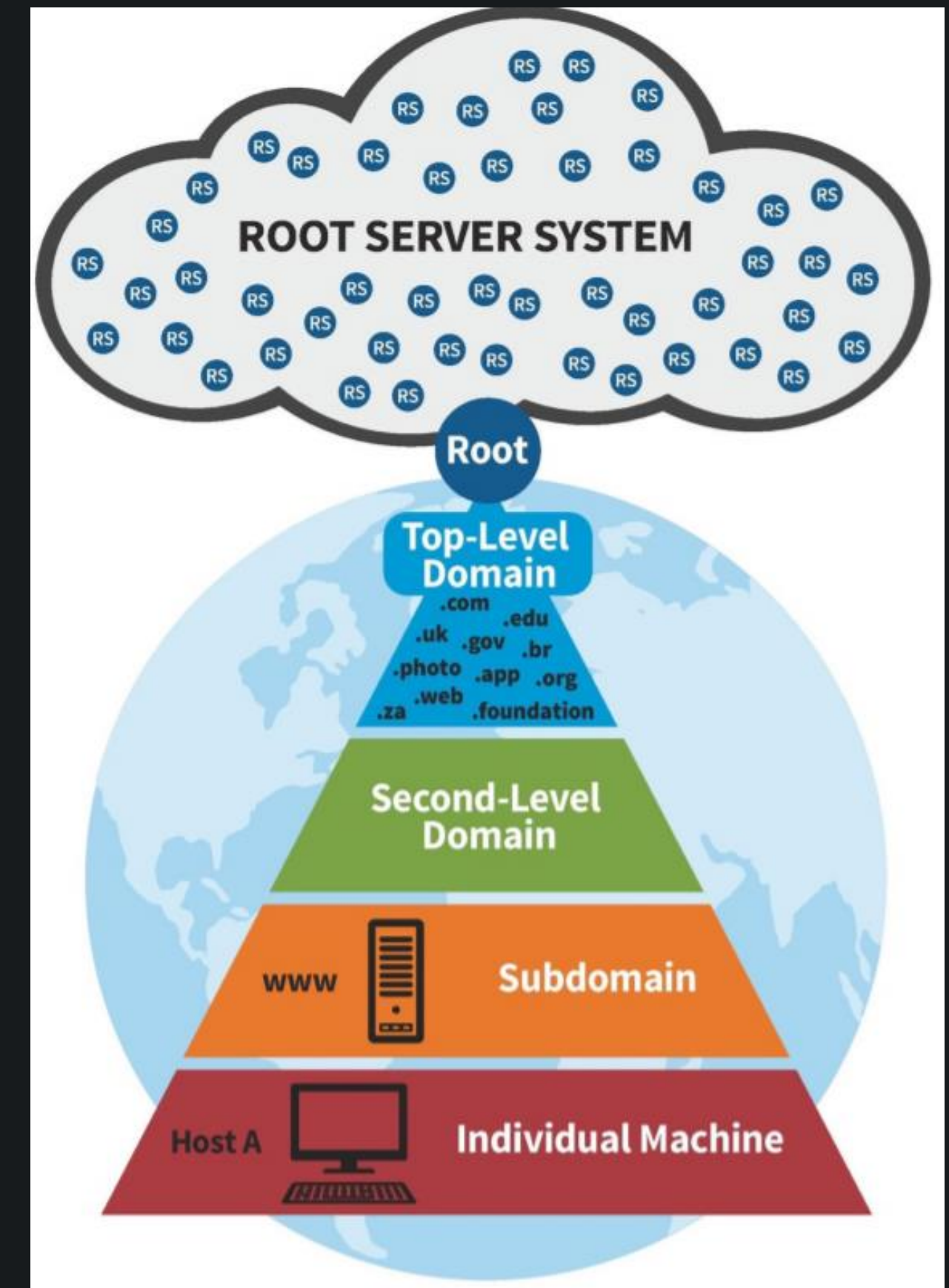
- 类似RFC7706的方式在各个地区镜像根区数据, 响应根区查询

- RFC8483模式(Yeti Model)

- 多棵树, 多个根服务器入口; 一棵树, 多个签名者

- 去中心化模式

- 信任网络 VS. 信任根, 区块链DNS等模式
- 由域名持有者 (registrar/registry) 签名, 发布数据在去中心化的网络中, 形成数据分享平台。
- 去中心化的DNS 挑战在于性能和实时性, 适合存储和分享相对静态的根和TLD的域名“索引”信息



对根服务器问题的一些思考

- 目标：保持互联网互联互通的前提下，加强域名解析生态的“内循环”

- 根服务器层面

全国备案的递归服务器组成联盟（电信运营商DNS，国内公共DNS等），统一标准，与大的国内域名注册局（比如.CN）和DNS服务商（比如阿里DNS）做数据联动，DNS访问无需经过根服务器查询域名授权索引信息，域名解析过程不依赖根服务器。

- 其他权威域名层面

加强.CN的注册和使用，尽量不依赖.COM和.NET。实现DNS权威域名注册和解析的“内循环”

目 录

CONTENT

● 背景：DNS技术趋势和热点

● 阿里云DNS解决方案与实践

● 总结

总结

- 域名系统DNS不断适应和满足新的技术应用发展、新政策的要求，是互联网 资源定位、流量调度、服务高可用、网络安全策略实施 不可或缺的核心基础设施和抓手
- 从安全角度看，在IoT和云时代普通企业已经不具备能力与攻击者对抗，大型的云厂商具有更多的网络资源，云计算弹性，业务理解和对抗经验，大数据智能化的方案来应对安全的新挑战
- 阿里云DNS 全力助力阿里云打造安全稳定的数字经济基础设施，提供T级别的DDoS攻击防御，DNSSEC数据一致性，DoH/DoT隐私保护，根区高可用性等，多次获得国家部委的奖励和认可
- 站在国家网络基础设施的角度，互联网域名和标识解析系统的安全稳定值得大家携手共建，在保持互联互通的前提下，加强域名解析生态 “内循环”

欢迎加入阿里云DNS团队

阿里DNS团队隶属阿里巴巴云智能事业群，是亚洲最大的DNS厂商，每天访问量超过7000亿，全球40多个集群，数千台机器的部署规模，基于云计算丰富的上下游场景，依托IT资源强大的交付生态圈，团队一直在拓展应用寻址和调度服务边界，并致力于新技术场景下的下一次标识寻址服务的探索。

2020年，标识寻址和调度服务正处于机遇期，我们在北京/杭州期待您的加入，抓住加入阿里经济体下一个独角兽的机会！



招聘岗位



奥运会全球指定云服务商