

中国内地DNS根服务器节点测量研究报告

A Nation-wide View into the Effect of DNS Root Server Instances

刘保君 Baojun Liu

清华大学网络研究院 博士后

Postdoctoral Researcher at Tsinghua University

背景：域名根服务器系统

Background: DNS Root Server System

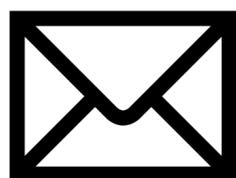
01

互联网域名系统核心网络基础设施

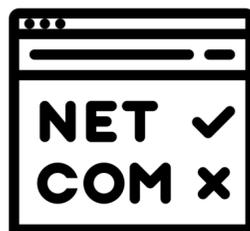
The Importances of Domain Name System (DNS)

互联网的“中枢神经”：通用标识体系，核心基础协议

充当信任锚点

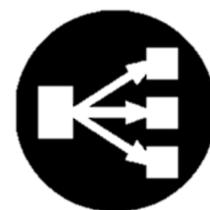


邮件认证

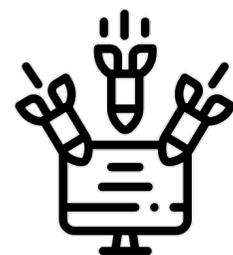


证书申请

支撑上层应用



资源调度



威胁情报

互联网域名系统变迁历史

The Evolution of DNS

从集中式管理，演进至分布式授权



David Clark

* https://en.wikipedia.org/wiki/David_D._Clark



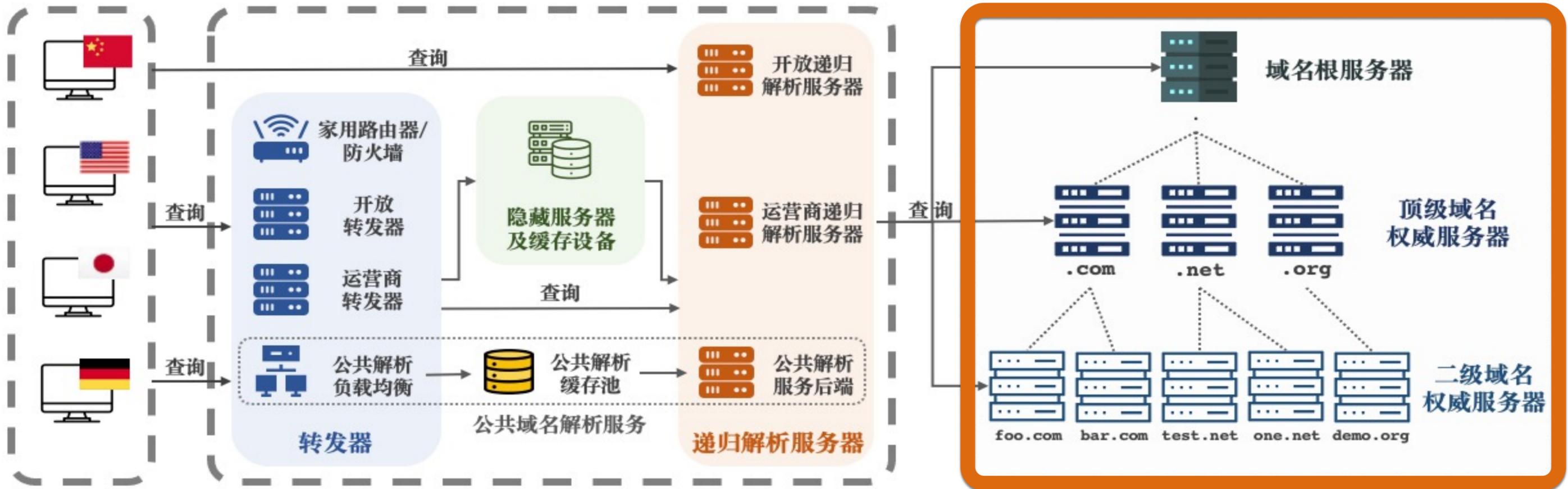
Jon Postel

* https://en.wikipedia.org/wiki/Jon_Postel

全球性分布式网络信息系统

Global Distributed Networking System

开放无边界的特性



域名根服务器系统 101

The Introduction of DNS Root Server System

WHAT

根区文件中包含什么内容？

WHO

谁在运行域名根服务器？

HOW

13个标志符，千余个节点

域名根服务器节点地理位置分布

Distribution of DNS Root Server Instances



* <https://root-servers.org/>

域名根服务器节点地理位置分布

Distribution of DNS Root Server Instances



目前，中国内地共有 21 个根节点

* <https://root-servers.org/>

国内新闻媒体对域名根服务器的报道与解读

News and reports from China on the DNS root server system

环球网

警惕！美国如何能“封杀”伊朗网站？中国专家说出真相

环球时报 刘洋 2021-06-24 06:18

Tr 小字

【环球时报综合报道】美国对伊朗网站的“封杀”举动引起全球网络安全专家的警惕。俄罗斯卫星网22日称，美国司法部查封了超过30个伊朗网站。报道称，此次查封目前仅针对美国管辖范围内的.com和.net网站域名，暂未涉及伊朗网站域名，因此部分网站通过更换伊朗域名.ir已重新上线。

天津大学法学院互联网政策与法律研究中心主任秦安23日接受《环球时报》记者采访时表示，这只是美国网络霸权的牛刀小试。美国不光能查封网站，它甚至能让整个国家从全球互联网版图中消失，核心在于美国控制着绝大部分根服

美国不光能查封网站，它甚至能让整个国家从全球互联网版图中消失，核心在于美国控制着绝大部分根服务器和域名管理服务器

国内新闻媒体对域名根服务器的报道与解读

News and reports from China on the DNS root server system



中国“网根”扎在国外

互联网人士警告 “互联网时代

世界咽喉都在外国人手中”

工信部加快批复国内机构设立根服务器节点

Chinese institutions deploying more and more DNS root server instances

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

统一搜索

看新闻 找文件 查办事 提意见 查数据 要投诉

工业和信息化部 新闻动态 政务公开 政务服务 公众参与 工信数据 专题专栏

首页 > 政务公开 > 政策文件 > 文件发布 > 审批结果

发文机关：工业和信息化部
标 题：工业和信息化部关于同意互联网域名系统北京市工程研究中心有限公司设立域名根服务器（L根镜像服务器）及域名根服务器运行机构的批复
发文字号：工信部信管函〔2019〕173号
成文日期：2019-06-24 发布日期：2019-06-26
发布机构：信息通信管理局 分 类：信息通信管理

工业和信息化部关于同意互联网域名系统北京市工程研究中心有限公司设立域名根服务器（L根镜像服务器）及域名根服务器运行机构的批复

工信部信管函〔2019〕173号

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

统一搜索

看新闻 找文件 查办事 提意见 查数据 要投诉

工业和信息化部 新闻动态 政务公开 政务服务 公众参与 工信数据 专题专栏

首页 > 政务公开 > 政策文件 > 文件发布 > 审批结果

发文机关：工业和信息化部
标 题：工业和信息化部关于同意中国信息通信研究院设立域名根服务器（L根镜像服务器）及域名根服务器运行机构的批复
发文字号：工信部信管函〔2019〕348号
成文日期：2019-11-06 发布日期：2019-11-21
发布机构：信息通信管理局 分 类：信息通信管理

工业和信息化部关于同意中国信息通信研究院设立域名根服务器（L根镜像服务器）及域名根服务器运行机构的批复

工信部信管函〔2019〕348号

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

统一搜索

看新闻 找文件 查办事 提意见 查数据 要投诉

工业和信息化部 新闻动态 政务公开 政务服务 公众参与 工信数据 专题专栏

首页 > 政务公开 > 政策文件 > 文件发布 > 审批结果

发文机关：工业和信息化部
标 题：工业和信息化部关于同意中国互联网络信息中心设立域名根服务器（J、K根镜像服务器）及域名根服务器运行机构的批复
发文字号：工信部信管函〔2019〕405号
成文日期：2019-12-09 发布日期：2019-12-31
发布机构：信息通信管理局 分 类：信息通信管理

工业和信息化部关于同意中国互联网络信息中心设立域名根服务器（J、K根镜像服务器）及域名根服务器运行机构的批复

工信部信管函〔2019〕405号

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

统一搜索

看新闻 找文件 查办事 提意见 查数据 要投诉

工业和信息化部 新闻动态 政务公开 政务服务 公众参与 工信数据 专题专栏

首页 > 政务公开 > 政策文件 > 文件发布 > 审批结果

发文机关：工业和信息化部
标 题：工业和信息化部关于同意中国信息通信研究院设立域名根服务器（K根镜像服务器）及域名根服务器运行机构的批复
发文字号：工信部信管函〔2019〕400号
成文日期：2019-12-05 发布日期：2019-12-06
发布机构：信息通信管理局 分 类：信息通信管理

工业和信息化部关于同意中国信息通信研究院设立域名根服务器（K根镜像服务器）及域名根服务器运行机构的批复

工信部信管函〔2019〕400号

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

统一搜索

看新闻 找文件 查办事 提意见 查数据 要投诉

工业和信息化部 新闻动态 政务公开 政务服务 公众参与 工信数据 专题专栏

首页 > 政务公开 > 政策文件 > 文件发布 > 审批结果

发文机关：工业和信息化部
标 题：工业和信息化部关于同意中国互联网络信息中心设立域名根服务器（J、K根镜像服务器）及域名根服务器运行机构的批复
发文字号：工信部信管函〔2019〕405号
成文日期：2019-12-09 发布日期：2019-12-31
发布机构：信息通信管理局 分 类：信息通信管理

工业和信息化部关于同意中国互联网络信息中心设立域名根服务器（J、K根镜像服务器）及域名根服务器运行机构的批复

工信部信管函〔2019〕405号

工信部加快批复国内机构设立根服务器节点

Chinese institutions deploying more and more DNS root server instances

2019-06-26	域名系统北京市工程研究中心	L 根
2019-06-26	中国互联网络信息中心	F I K L 根
2019-11-21	中国信息通信研究院	L 根
2019-12-06	中国信息通信研究院	K 根
2019-12-31	中国互联网络信息中心	J K 根

问题：重新回顾现有技术路线

Research Gap: A Reexamination Study of Technical Roadmap

02

一、理论分析

DNS Implementations Code Analysis

借助引进部署根服务器节点，

究竟能否缓解我国用户对境外根服务器的不合理依赖？

二、实证分析

A Comprehensive Measurement Study

如何系统性评估，

当前我国用户域名解析对境外根服务器的依赖现状？

三、未来设想

To Provide Guidelines to Future Works

如何针对性的改进，

后续根服务器节点的引进以及部署策略？

域名服务器究竟如何选择根服务器节点？

DNS Root Server Slection Algorithms in Popular Recursive DNS Software

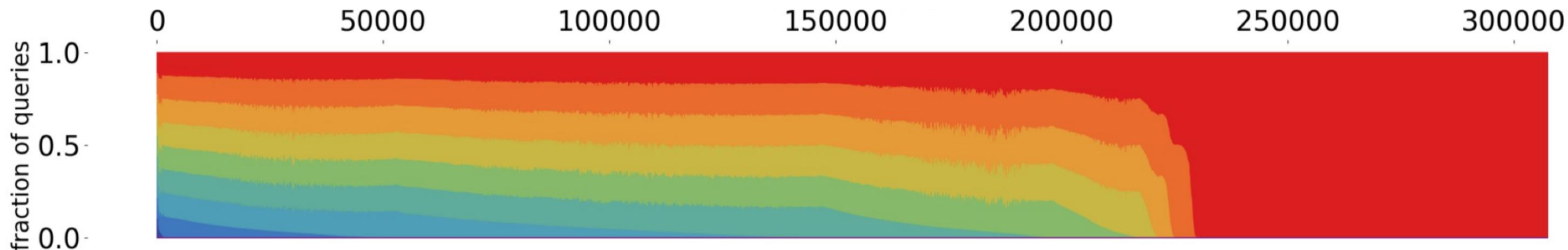
03

递归解析服务器的选根策略

Root Server Selection Algorithms in Mainstream DNS Implementations

一个江湖中流传已久的说法

* 不同根服务器域名的实际效用，存在一定程度差异



主流DNS软件中根节点选择算法分析

Root Server Selection Algorithms in Mainstream DNS Implementations

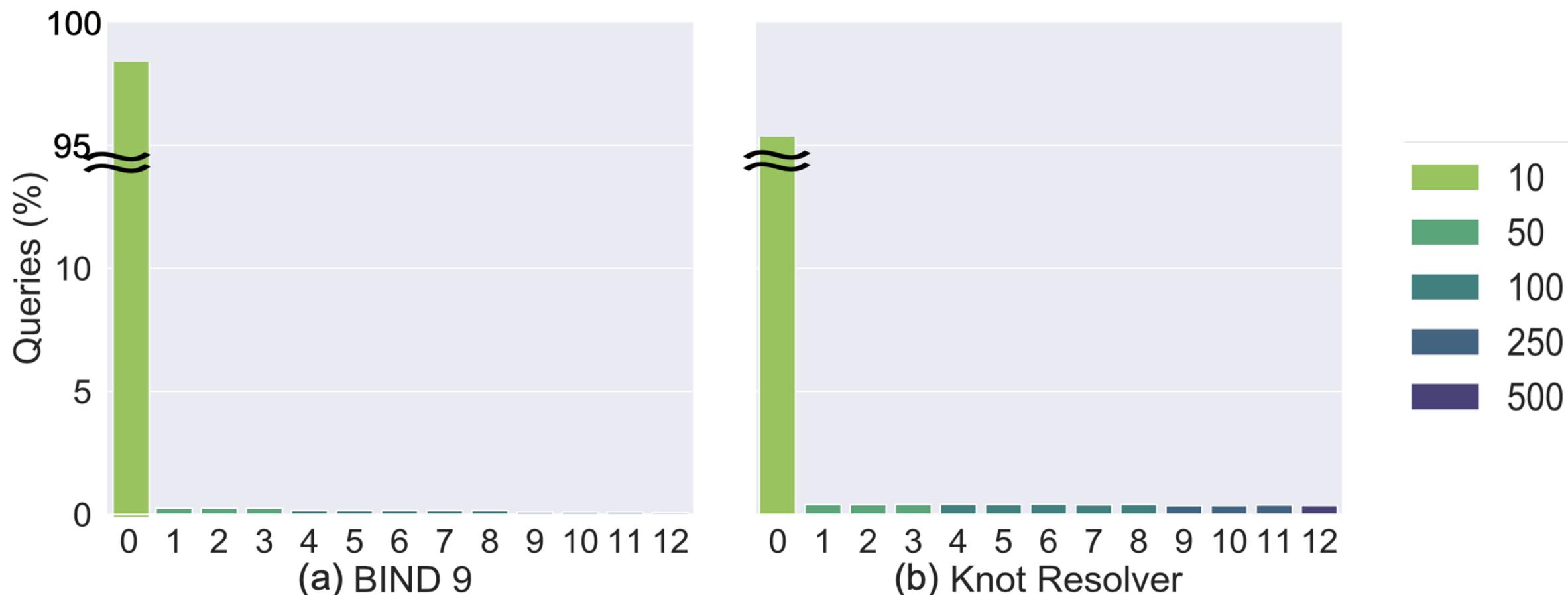
最重要的因素：递归与根节点之间的时延差异 “RFC 1034”



主流DNS软件中根节点选择算法分析

Root Server Selection Algorithms in Mainstream DNS Implementations

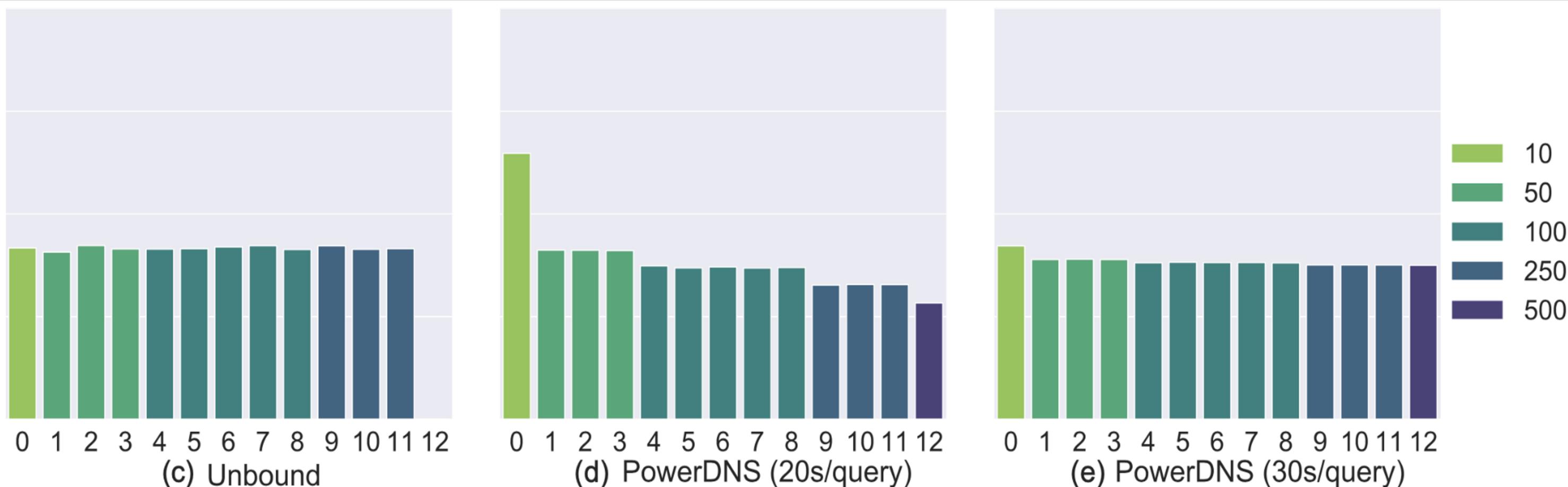
一：BIND 与 Knot Resolver，绝大多数情况选择时延最小的根节点



主流DNS软件中根节点选择算法分析

Root Server Selection Algorithms in Mainstream DNS Implementations

二：Unbound 与 PowerDNS，由于参数未经优化，近乎随机选择根节点



域名服务器至根节点之间的时延如何？

How to measure the network latency between DNS server and root server instances?

04

根服务器节点的实际效用测量

Measuring the Effect of DNS Root Server Instances

“实际效用”：域名解析时延 & 根节点生效范围

借助商业测量平台开展实验，反复筛选实验节点

保留 182个测量节点，覆盖中国内地31个省份

为期一周的测量 2020/11/27 – 2020/12/03

测量实验观测点

移动 24个

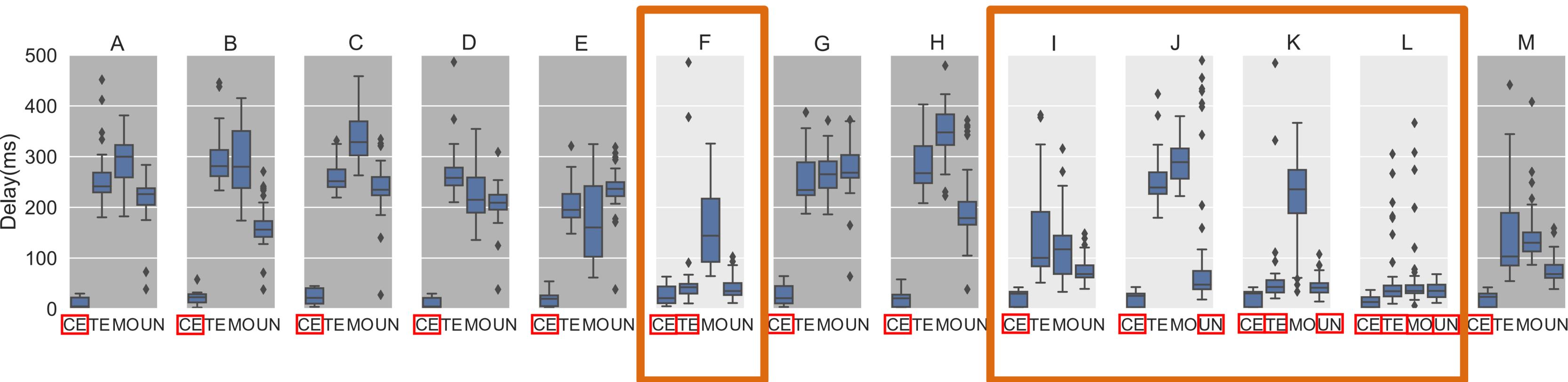
电信 71个

联通 74个

教育网 14个

根服务器节点的网络时延测量结果

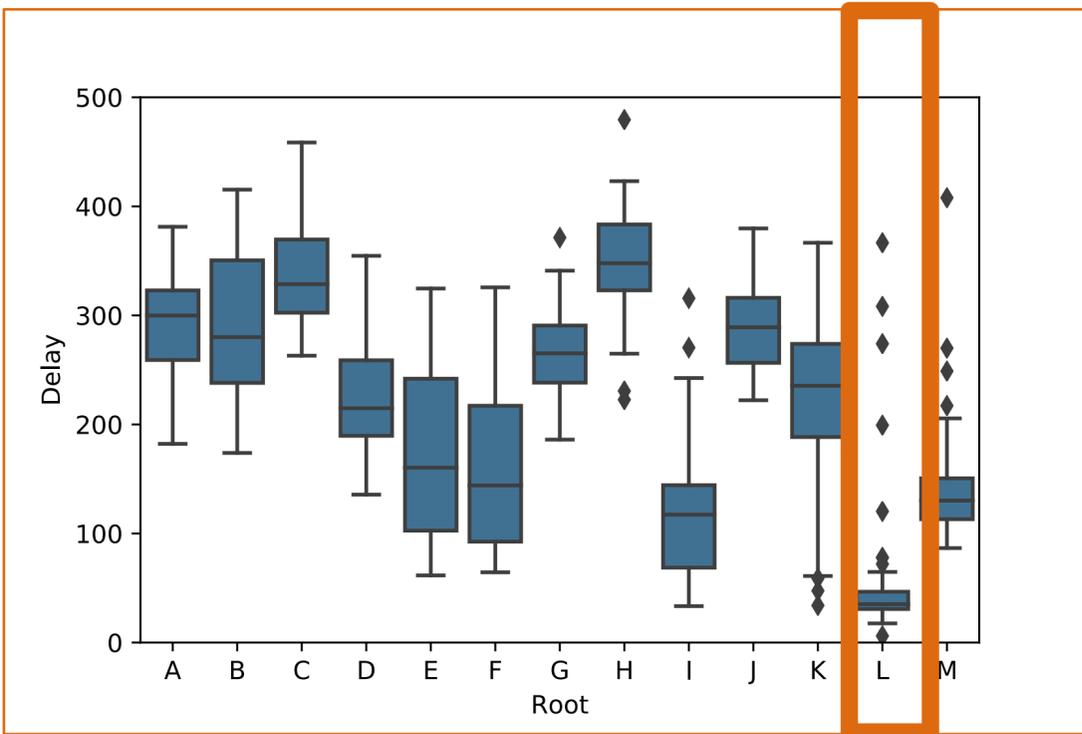
Measurement Results of Network Latency Between End-users and DNS Root Server Instances



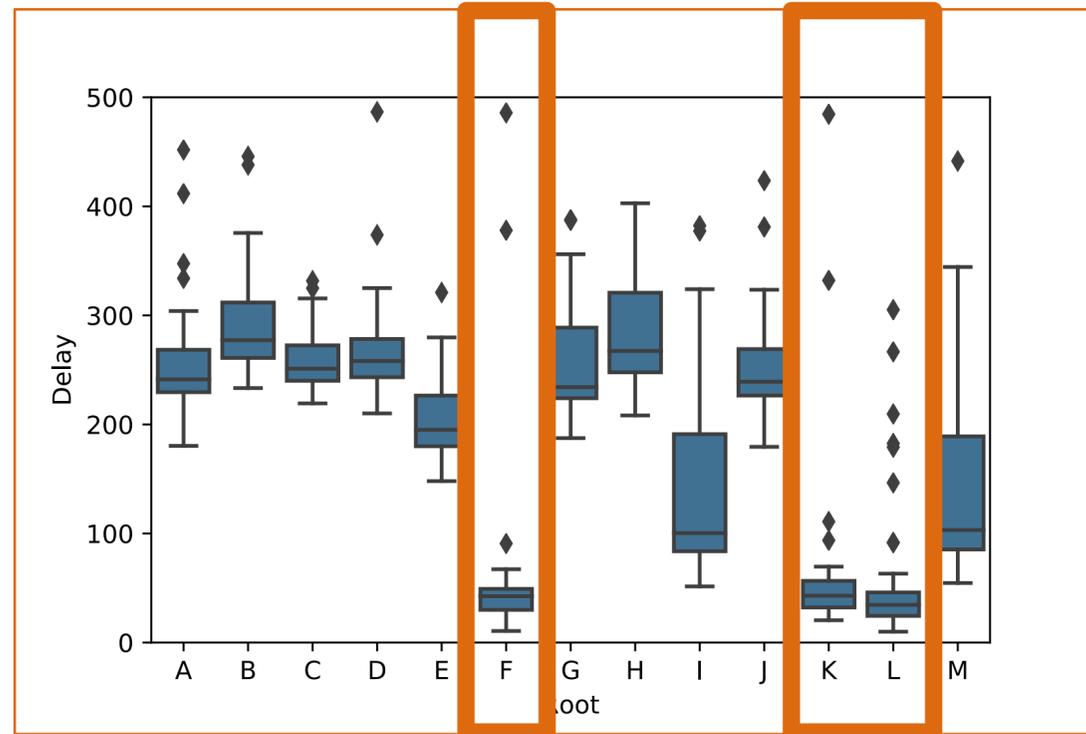
根服务器节点的网络时延测量结果

Measurement Results of Network Latency Between End-users and DNS Root Server Instances

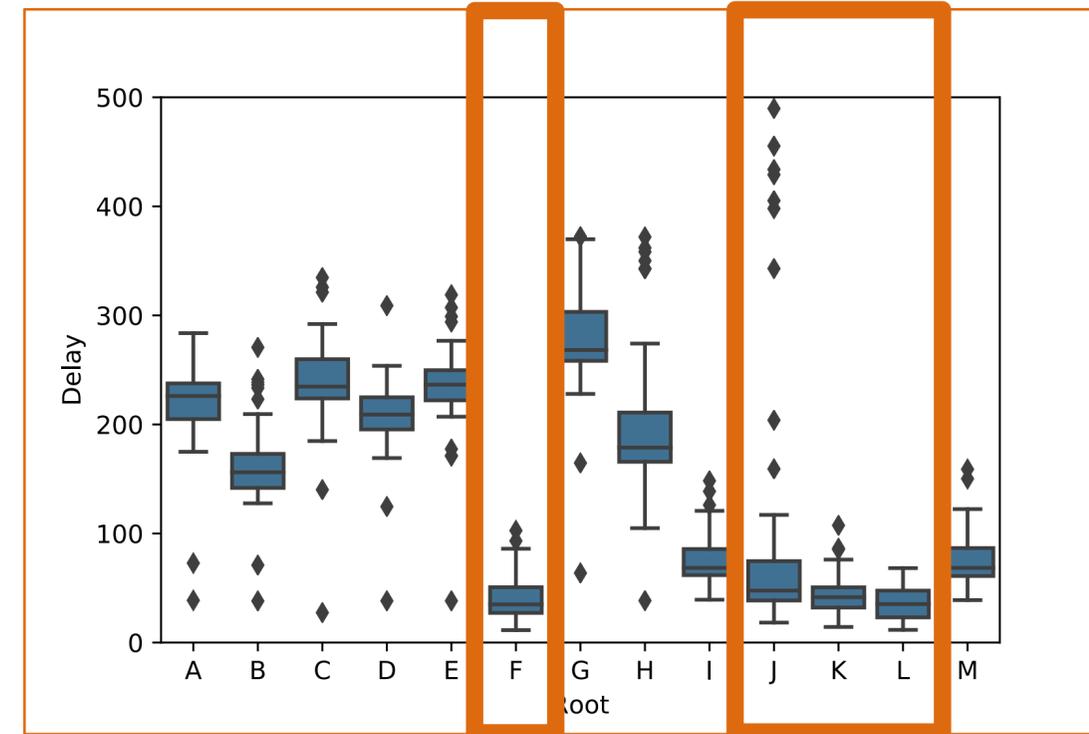
我国内地存在根节点的字母，在部分运营商网络内解析平均时延偏低



移动：L 根时延偏低



电信：F K L 根时延偏低



联通：F J K L 根时延偏低

仍有一些疑问

Some Concerns

一、显著偏低的时延，真的是由于访问了国内授权根节点吗？

二、为什么不同运营商用户之间，根节点访问时延差异很大？

对根节点的查询请求是否出境？

DNS Root Server w/o Domestic Instances

主要难点：

根服务器系统的任播机制，导致难以区分正在使用的根节点。

对根节点的查询请求是否出境？

DNS Root Server w/o Domestic Instances

侧信道：对根节点，发起携带前缀的特定域名查询请求

```
$ dig @f.root-servers.net. youtube.com
```

```
...
```

```
;; QUESTION SECTION:
```

```
;youtube.com.                IN      A
```

```
;; AUTHORITY SECTION:
```

com.	172800	IN	NS	f.gtld-servers.net.
com.	172800	IN	NS	j.gtld-servers.net.
com.	172800	IN	NS	c.gtld-servers.net.
com.	172800	IN	NS	b.gtld-servers.net.
com.	172800	IN	NS	l.gtld-servers.net.

```
...
```

当境内解析时：
查询请求没有经过国际关防，
根节点只会返回顶级域的NS记录

对根节点的查询请求是否出境？

DNS Root Server w/o Domestic Instances

侧信道：对根节点，发起携带前缀的特定域名查询请求

```
$ dig @a.root-servers.net. youtube.com
```

```
...
```

```
;; QUESTION SECTION:
```

```
;youtube.com.                IN      A
```

```
;; ANSWER SECTION:
```

```
youtube.com.                 77      IN      A      159.138.20.20
```

**当境外解析时：
查询请求经过国际关防，
返回一条A记录**

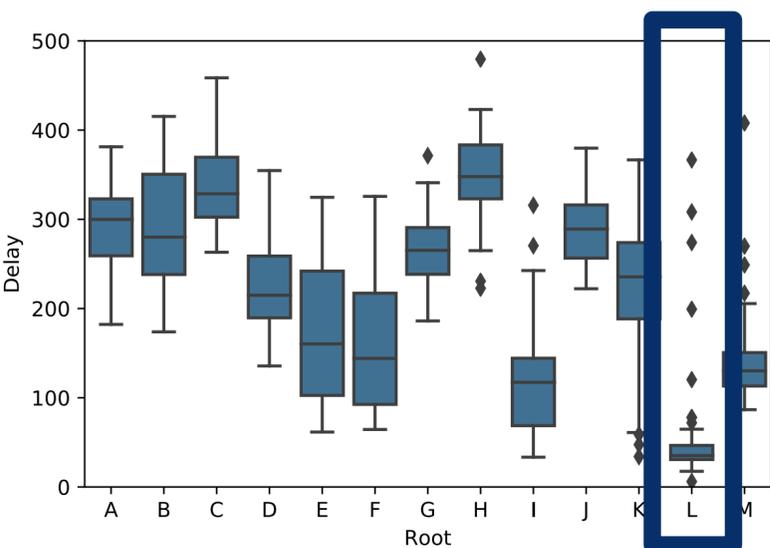
对根节点的查询请求是否出境？

DNS Root Server w/o Domestic Instances



中国移动：L根几乎全部境内解析

Measurement Results of China Mobile's Vantage Points



移动：L根时延偏低

A
B
C
D
E
F
G
H
I
J
K
L
M

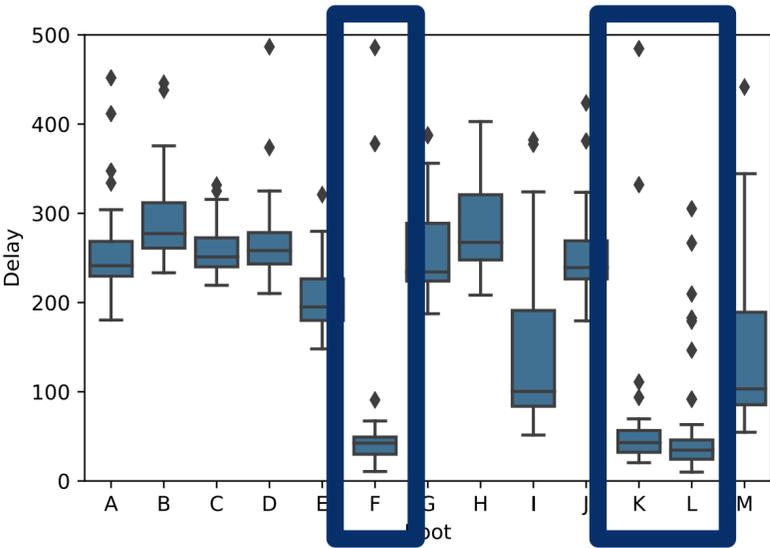


F根，几乎全部出境

I, J, K根，大量出境

中国电信：F K L 根几乎全部境内解析

Measurement Results of China Telecom's Vantage Points



电信：F K L 根时延偏低

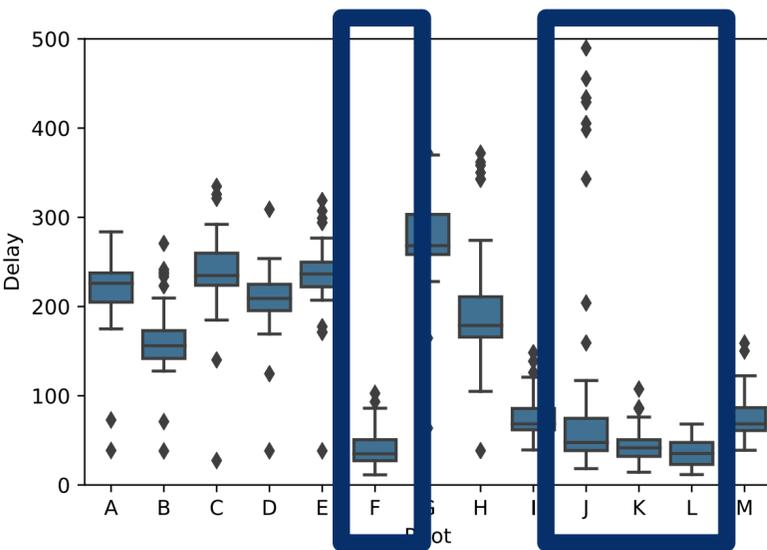
A
B
C
D
E
F
G
H
I
J
K
L
M



I J 根，几乎全部出境

中国联通：J K L 根 几乎全部境内解析

Measurement Results of China Unicom's Vantage Points



联通：F J K L 根时延偏低

M L K J I H G F E D C B A



教育网：所有根域名均为境内解析

Measurement Results of CERNET's Vantage Points

教育网内存在自建根节点，去往根服务器的请求均为境内解析



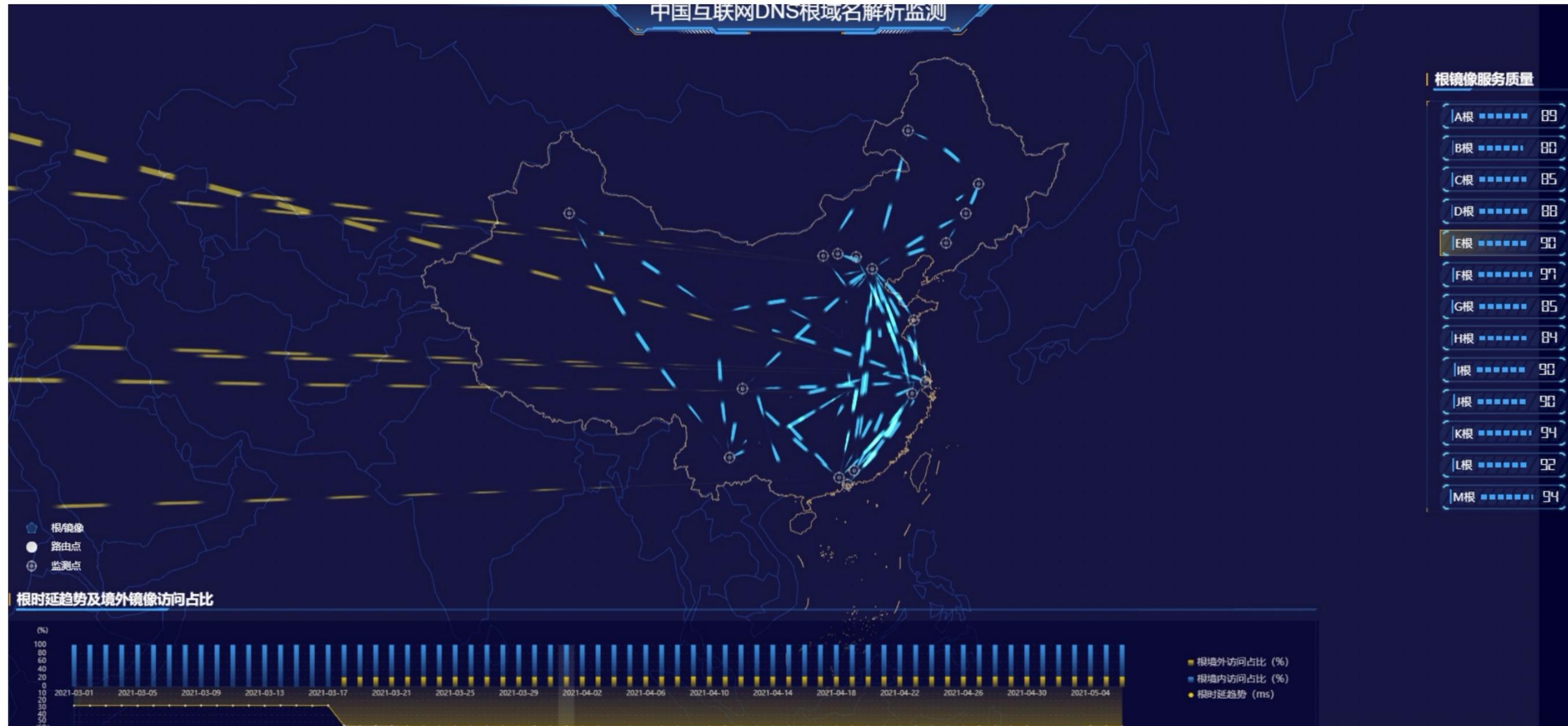
中国互联网根服务器节点安全监测系统

Measurement Platform of DNS Root Server Instances

05

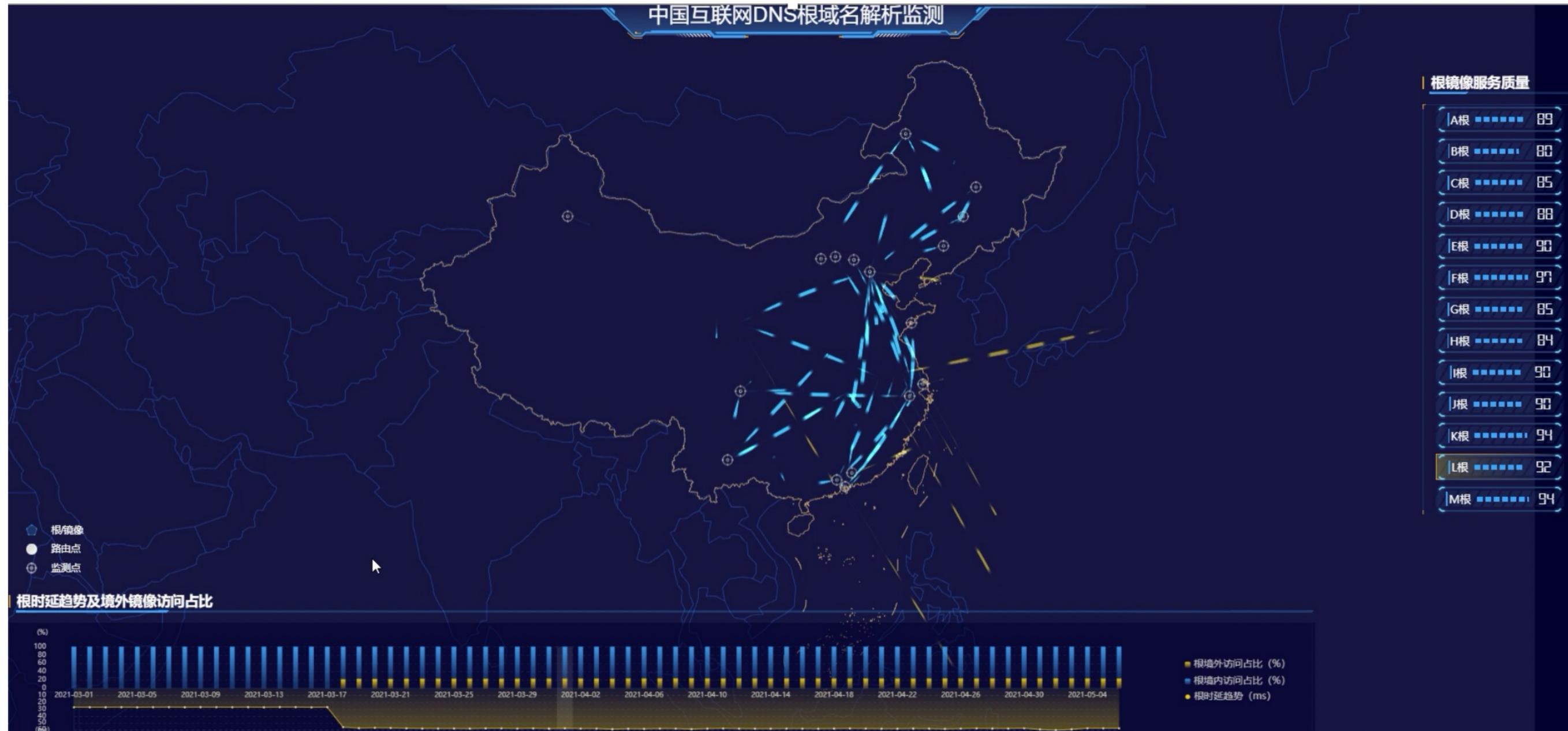
E 根 中国内地无根节点 流量全部出境

Measurement Platform of Chinese DNS Root Server Instances: Root E



L根 中国内地有根节点 大量境内解析

Measurement Platform of Chinese DNS Root Server Instances: Root L



内地根服务器节点网络时延测量结果

Measurement Conclusion

一、国内部署根节点，有助于一定程度上改善根节点外部依赖

二、国内可能存在“一定规模”的未授权根节点

我国内地根服务器节点的可用性分析

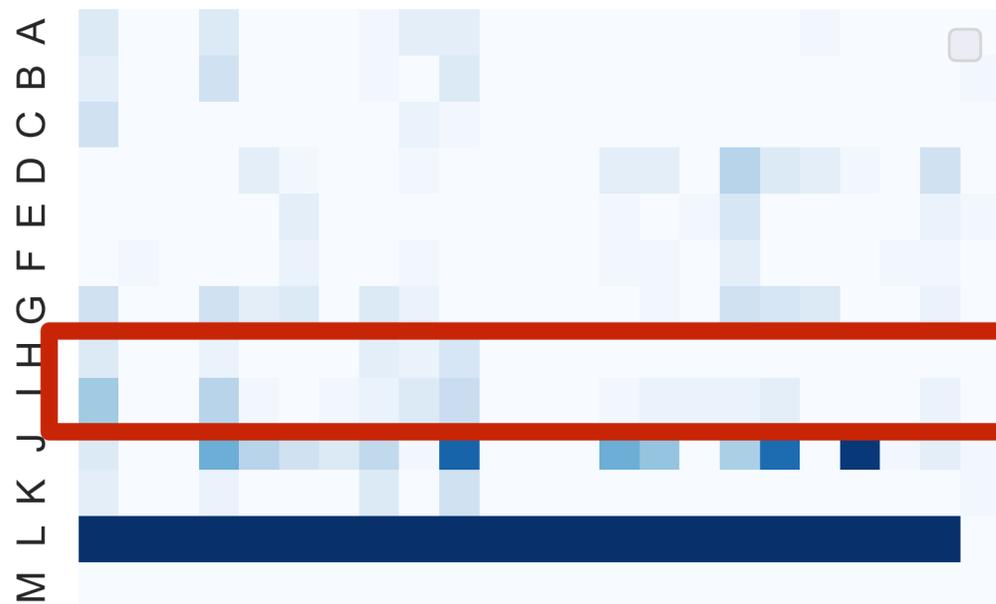
Anailability Anaysis of DNS Root Server Instances

06

根节点难以“共享”：从若干异常现象谈起

The Availability of Root Server Instances: Case Study

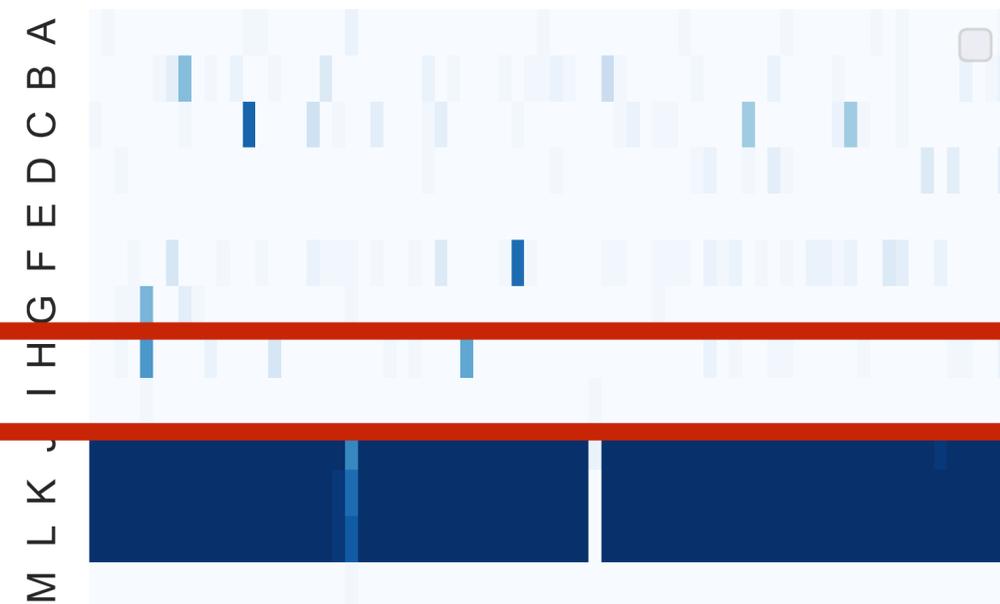
北京存在 1 根节点，但三大运营商对 1 根的查询请求全部出境



中国移动



中国电信



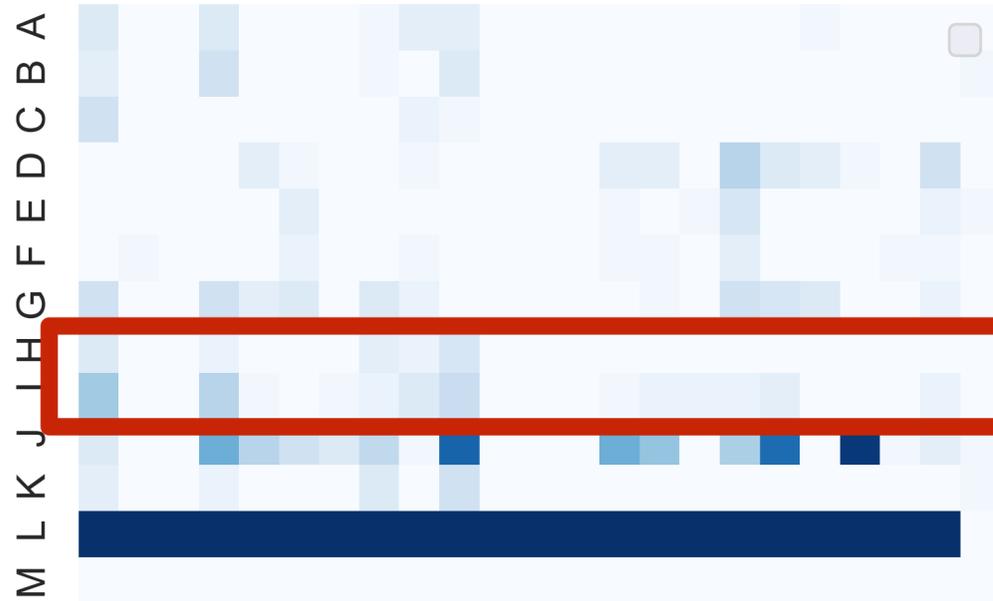
中国联通

1 根，几乎全部出境

根节点难以“共享”：从若干异常现象谈起

The Availability of Root Server Instances: Case Study

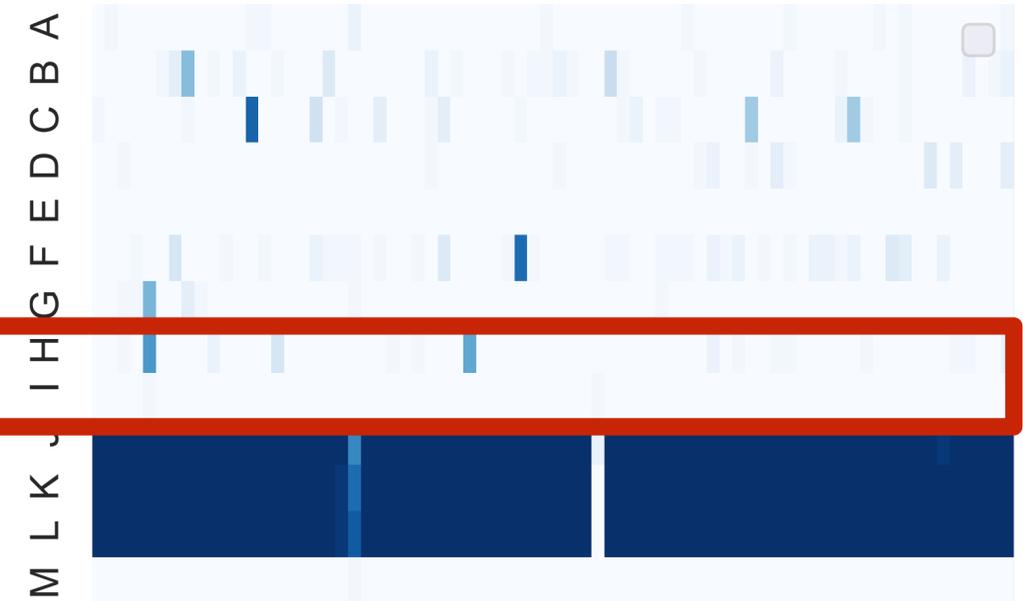
解释：I 根仅服务科技网，物理上位于科技网内，逻辑上位于关防外



中国移动



中国电信



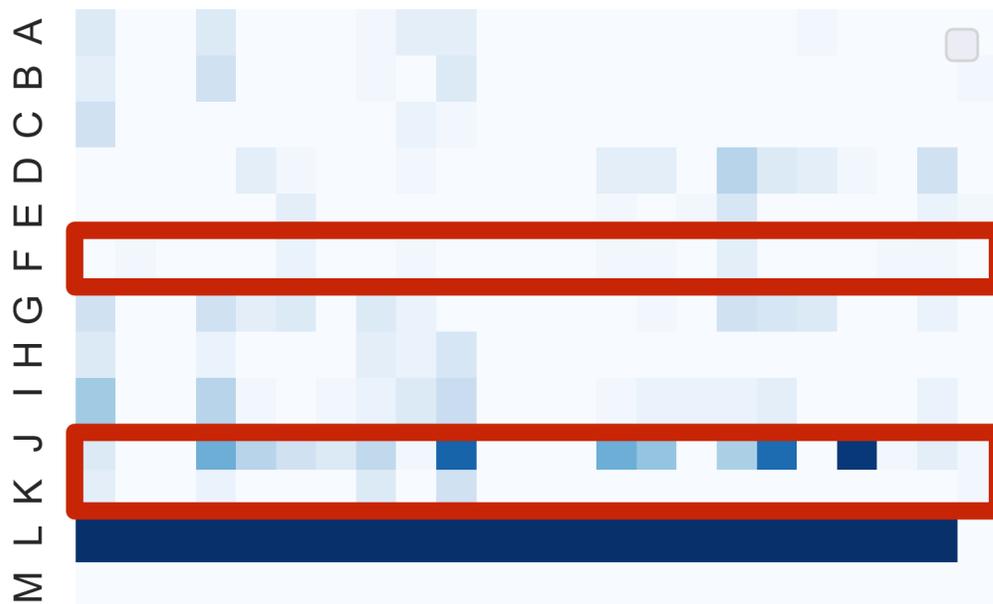
中国联通

I 根，几乎全部出境

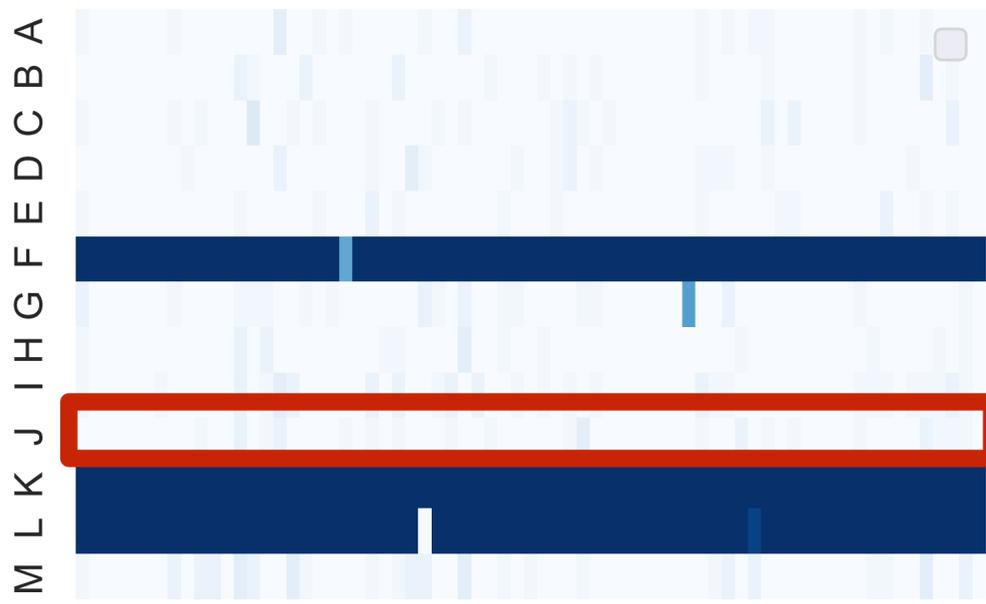
根节点难以“共享”：从若干异常现象谈起

The Availability of Root Server Instances: Case Study

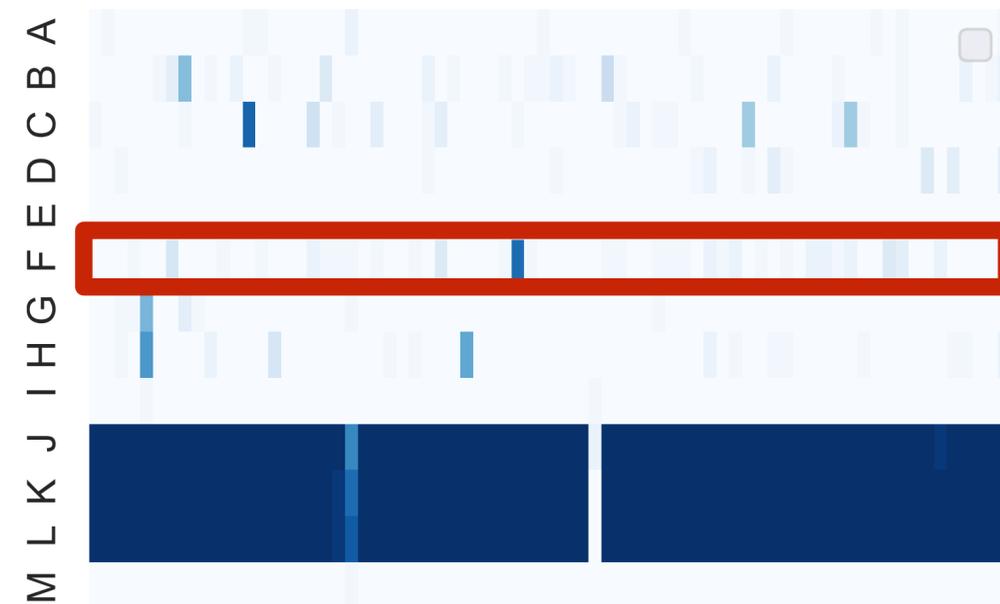
F 根 仅对电信有效，J 根 仅对联通有效，F J K 根对移动几乎无效



中国移动



中国电信

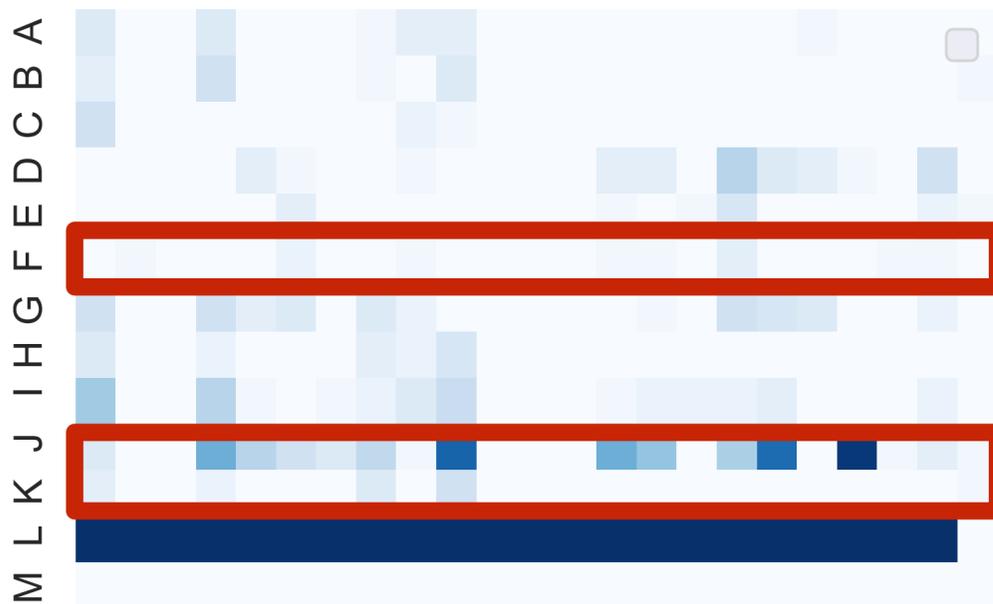


中国联通

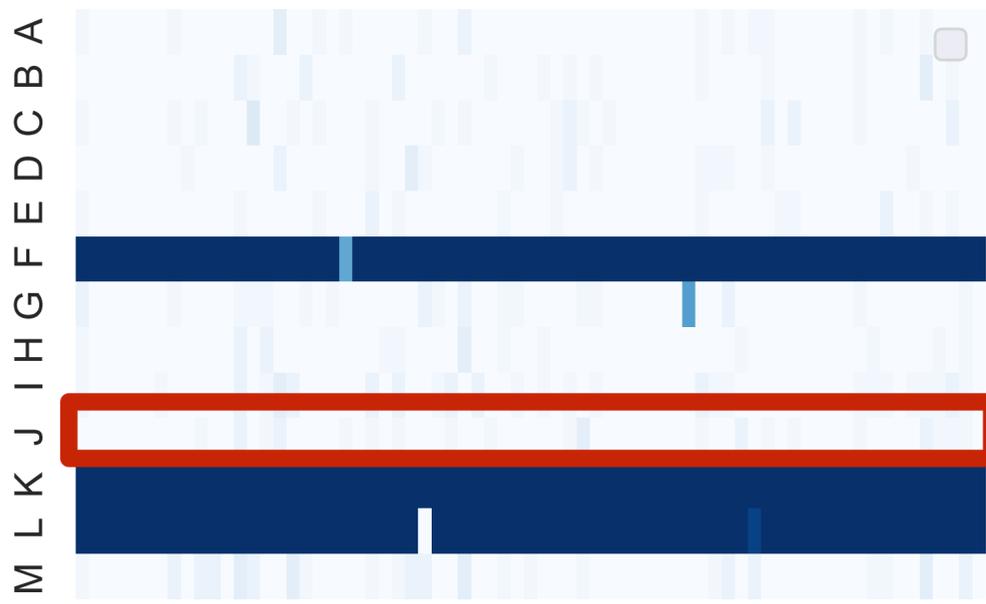
根节点难以“共享”：从若干异常现象谈起

The Availability of Root Server Instances: Case Study

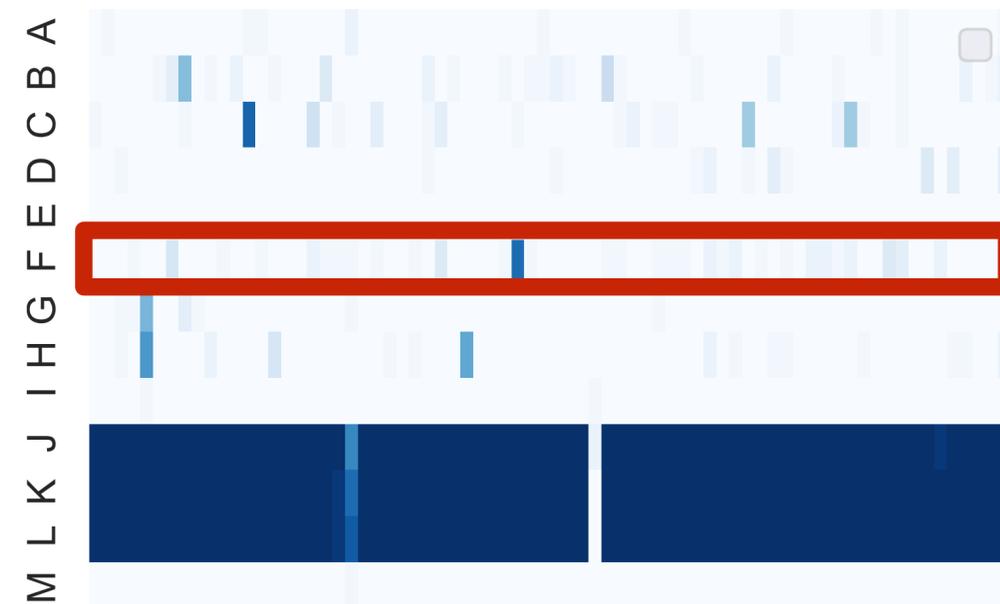
解释：中国内地根节点位于运营商内； BGP 路由通告范围被限制。



中国移动



中国电信



中国联通

总结与建议

Conclusion and Recommendation

07

总结与建议

Summary and Recommendations

- 1) 递归服务器运营者，尽可能避免随机选择根节点
- 2) 大型网络运营商，改善根节点的互联互通特性
- 3) 根节点运营者，尽可能避免使用未授权的根节点

欢迎交流讨论

lbj@tsinghua.edu.cn