一种评估 DNS 根服务质量的方法

潘蓝兰，延志伟，胡安磊，李晓东
（中国互联网络信息中心 互联网域名管理技术国家工程实验室，北京 100190）

摘　要：域名解析系统是互联网最重要的基础服务之一，其中根域名服务器是权威域名解析的起点。自 2002 年左右，根域名服务器广泛采用 anycast 镜像技术进行全球分散部署。但由于网络环境的复杂性，各地区访问根镜像的效果差异很大。针对中国境内所部署的根镜像服务器进行了全面的监测和分析，提出了一种评估 DNS 根服务安全稳定的方法。该方法能够有效检查本地根镜像的生效情况、不同省份运营商网内及跨网访问差异、根镜像服务路由异常等相关指标，为 DNS 根服务器的部署规划和性能评估起到指导作用。

关键词：域名；根镜像；anycast；域名解析系统

0　引言

域名解析系统（domain name system，DNS）是互联网的核心基础服务之一，主要负责将应用层业务的域名映射为可在网络层寻址的 IP 地址。因此，DNS 是否能够快速、准确、有效地提供服务，会直接影响到互联网业务的用户体验。

DNS 协议整体框架设计于 20 世纪 80 年代[1,2]，从根域名开始，通过顶级域名、二级及以下域名的层次化域名空间授权，实现全球分布式的域名分层管理。

根域名服务器（root name server）是域名解析进行迭代查询的起点，负责返回顶级域名（例如 COM、NET、CN 等）的权威服务器地址。目前，全球共 13 组根域名服务器，域名格式为[A ~ M]. root-servers. net，根据各自的字母标志，简称为 A 根、B 根、…、M 根。考虑到 DNS 分布式解析查询性能、分散 DDOS 攻击风险等现实需求，有 11 个根域名服务器采用 anycast 技术，在全球部署了 500 多个镜像节点，其中 F、I、J、L 四个根均在中国大陆境内共部署了七个镜像节点[3,4]。

由于各个根镜像节点的服务能力、所处网络的带宽资源、所属的国家省份运营商有所不同（各省份运营商网络环境、跨省、跨运营商、跨国流量路由配置等多个相关因素的综合影响），从中国大陆境内各省份运营商访问根域名服务的质量并不均衡[5,6]。所以，通过对根域名服务器进行探测分析，研究如何有效评估根域名服务在不同地区的服务质量的算法，对于根服务器的选址部署和性能评估具有实际意义。

本文根据 DNS 根镜像解析特点[7-9]，基于中国互联网络信息中心（CNNIC）在中国大陆多个省份运营商监测根域名服务的数据进行分析，提出了一种评估 DNS 根域名服务的方法。该方法在根镜像查询时延的基础上，能够快速有效评估根镜像节点的分散部署、不同省份运营商的差异、路由异常、网内及跨网访问差异，对于根域名服务质量的影响。

1　监测数据

从各省运营商的监测节点周期性向[A ~ M]. root-servers. net 根镜像 IP 发起 DNS 查询，记录每次的查询时延，并提取出每次查询的格式化的监测数据项，如表 1 所示。

表 1　监测数据项格式举例

数据项	取值
time	2015-03-24 00:00:32
rtt	80 ms
rtt_status	优
root_server	f. root-servers. net
root_ipv4	192.5.5.241
root_mirror_id	pek2a. f. root-servers. org
root_mirror_loc	北京
probe_ip	xxx. xxx. xxx. xxx
probe_country	中国
probe_prov	福建
probe_isp	电信

下面对上述数据的关键部分进行说明。

1.1　基础数据

查询的时间戳记为 time。

每次根镜像 DNS 查询的时延记录 rtt，单位是毫秒（ms）。根据 rtt 大小可以判断此次查询的服务状态（rtt_status），服务状态集合记为 S，分三个等级：优（good）、良（normal）、差（bad）。如表 2 所示。

表 2　rtt_status 判断

伪代码

```
rtt_status =
(rtt<150)? '优':
(rtt<300)? '良':
'差';
```

本文的 rtt_status 状态阈值根据历史根镜像探测记录设置，国内根镜像的访问时延基本在 150 ms 以内，国外根镜像的访问时延一般在 200 ~ 300 ms 之间。

1.2　根服务器

根服务器（root_server）、根服务器 IP 列表（root_ipv4）取自 Root-Servers 官方网站[3]。每个根服务器的所有根镜像节点共用同一个 IPv4/IPv6 地址。

根镜像 ID（root_mirror_id）、根镜像位置（root_mirror_loc）识别一般可以采用如下两种方法：

1）根域名服务器官方提供的镜像查询接口，直接从监测点发包查询当前访问的镜像 ID[4]。以表 3 的 F 根为例，查询到 root_mirror_id 为 pek2a，根据地名缩写推测 root_mirror_loc 为北京。

表 3　查询当前访问的 F 根镜像

查询

```
$ dig hostname. bind@ f. root-servers. net chaos txt +short
"pek2a. f. root-servers. org"
```

2）提取 traceroute 根域名服务器倒数第 1、2 跳的反向域名中出现的机场代码，或者倒数第 1、2 跳的 IP 所属地理位置。以表 4 的 C 根为例，根据 traceroute 提取第 8 跳节点名称，提取其中机场代码 lax01，推测 root_mirror_id 为 lax，root_mirror_loc 为洛杉矶。

表 4　traceroute 当前访问的 C 根镜像

查询

```
$ traceroute c. root-servers. net
traceroute to c. root-servers. net(192. 33. 4. 12),30 hops max,60 byte packets
1 .(192. 3. 20. 210) 0. 021 ms 0. 007 ms 0. 005 ms
2 10ge-2. 8. 5. 14. 0. la1. colocrossing. com(192. 3. 111. 125) 1. 248 ms 0. 380 ms 1. 276 ms
3 xe-5-2-0. er1. lax112. us. above. net(208. 185. 252. 21) 0. 162 ms 0. 150 ms 0. 144 ms
4 ae6-214. lax20. ip4. gtt. net(173. 241. 131. 169) 0. 218 ms 0. 209 ms 0. 248 ms
5 ae9. mpr1. lax12. us. zip. zayo. com(64. 125. 26. 5) 0. 418 ms 0. 304 ms 0. 346 ms
6 be6461. ccr23. lax05. atlas. cogentco. com(154. 54. 11. 13) 1. 020 ms 10. 177 ms 2. 235 ms
7 be2180. ccr21. lax01. atlas. cogentco. com(154. 54. 41. 57) 1. 073 ms 1. 081 ms 14. 238 ms
8 te1-1. c-root. lax01. atlas. cogentco. com(154. 54. 27. 138) 9. 344 ms 15. 420 ms 15. 473 ms
9 c. root-servers. net(192. 33. 4. 12) 0. 509 ms 0. 590 ms 15. 162 ms
```

收稿日期：2015-06-24；修回日期：2015-09-01

作者简介：潘蓝兰（1986-），女，福建人，硕士，主要研究方向为网络安全（abbypan@ gmail. com）；延志伟（1985-），男，山西人，博士，主要研究方向为网络安全；胡安磊（1979-），男，山东人，硕士，主要研究方向为域名系统安全、网络安全防护和应急；李晓东（1976-），男，山东人，博士，主要研究方向为下一代互联网架构。

1.3 监测节点

监测节点的 IP 地址记为 probe_ip。

监测节点所在的国家记为 probe_country，省份记为 probe_prov，运营商记为 probe_isp。

2 评估算法

根域名服务器服务质量主要取决于是否能够服务器本身能够快速有效响应 DNS 迭代查询，并且在各个主要运营商的不同省份达到相对均衡的网络访问体验。

根据 anycast 服务的特点，部署的根镜像数越多，根镜像连接的运营商个数越多，地区分布越均衡，用户侧就近访问的效果越好。

因此，可以基于根镜像的访问时延、运营商省份差异、根镜像路由生效、网间镜像访问质量等关键点设计监测指标。具体评估方法如下所述。

假设待评估的地区标志为 Z，Z 中选取的运营商集合记为 I，省份集合记为 P。假设待评估的根域名服务器集合记为 R，最多可全选 A ~ M 总共 13 个根，至少选取 1 个根。监测数据的时间区间记为 $[T_s, T_e]$。

2.1 访问时延

如果在某个时间段内，根域名服务器 R_i 在某个省份 P_x 运营商 I_y 的监测数据中，访问质量较好，那么在该省份运营商探测点访问 R_i 的监测数据中，服务状态（rtt_status）为优（good）、良（normal）的比例应该比较高。对此本文设计以下量化指标项：

a) status_rate($P_x, I_y, R_i, S_j, T_s, T_e$) 表示在时间区间 $[T_s, T_e]$ 内，位于省份 P_x 运营商 I_y 的探测点访问根域名服务器 R_i 的监测数据中，服务状态（rtt_status）为 S_j 的比例。可以用于相同运营商不同省份的服务对比。

b) isp_status_rate(I_y, R_i, S_j, T_s, T_e) 表示在运营商 I_y 各省份访问 R_i 状态为 S_j 的 status_rate 均值。可以用于相同地区不同运营商的服务对比。

c) mirror_status_rate(R_i, S_j, T_s, T_e) 表示在地区 Z 各运营商访问 R_i 状态为 S_j 的 isp_status_rate 均值。可以用于相同地区不同根域名服务器的服务对比。

d) main_status_rate(S_j, T_s, T_e) 表示在地区 Z 访问各个根域名服务器状态为 S_j 的 mirror_status_rate 均值。可以用于不同地区根服务的对比。

在地区 Z 访问各个根域名服务器状态为优的 mirror_status_rate 均值作为访问时延水平指标：

rtt_status_level = main_status_rate('优', T_s, T_e)

如果 rtt_status_level 取值较大，则表示地区 Z 访问根服务时延质量较好。

2.2 命中镜像

由于具体路由策略、anycast 生效的范围影响，不同省份运营商访问同一个根域名服务器命中的镜像可能不同。因些，对于已在地区 Z 部署 anycast 镜像的根域名服务器而言，如果地区 Z 的探测点命中该镜像的比例越高，表明根解析就近解析服务的效果越好。对此本文设计以下量化指标项：

a) local_rate(P_x, I_y, R_i, T_s, T_e) 表示在时间区间 $[T_s, T_e]$ 内，位于省份 P_x 运营商 I_y 的探测点访问根域名服务器 R_i 的监测数据中，命中 R_i 在地区 Z 内部署的 anycast 镜像的比例。

b) isp_local_rate(I_y, R_i, T_s, T_e) 表示在运营商 I_y 各省份访问 R_i 的 local_rate 的均值。

c) mirror_local_rate(R_i, T_s, T_e) 表示在地区 Z 各运营商访问 R_i 的 isp_local_rate 均值。

d) main_local_rate(T_s, T_e) 表示在地区 Z 访问根域名服务器集合中各个 R_i 的 mirror_rtt_std 均值。

本文默认假设只有在地区 Z 内部署了 anycast 镜像的 R_i 才进行 isp_local_rate、mirror_local_rate、main_local_rate 的计算。如果 anycast 预设只在指定运营商生效，也可以进一步限制为，只有在地区 Z 的运营商 Iy 网内部署了 anycast 镜像的 R_i 才参与计算。

命中镜像的指标：

local_mirror_level = main_local_rate(T_s, T_e)

如果 local_mirror_level 取值较大，则表示地区 Z 部署的 anycast 镜像生效范围较广。如果地区 Z 并未部署 anycast 镜像，则 local_mirror_level 取值为 0。

2.3 网络异常

一般情况下，在地区 Z 部署了 anycast 镜像的根域名服务器 R_i，访问体验应该优于未部署 anycast 镜像的根域名服务器 R_j。因此，对比地区 Z 内各省份运营商访问 R_i 与 R_j 的服务时延，如果 R_i 时延高于 R_j 的比例较高，则有可能存在跨网路由的特殊处理、或网络状况临时异常，从而导致部署的 anycast 镜像生效范围较小（例如仅限于某个运营商）、或者地区 Z 之内跨运营商访问根镜像的链路状态较差、或者在某些省份运营商访问地区 Z 之内根镜像的链路状态比访问地区 Z 之外的根镜像更差。对此本文设计以下量化指标项：

a) 假设在地区 Z 中，已部署 anycast 镜像的根域名服务器集合为 RY，未部署 anycast 镜像的根域名服务器集合为 RN。rtt_warn ($P_x, I_y, R_i, RN, T_s, T_e$) 表示在时间区间 $[T_s, T_e]$ 内，位于省份 P_x 运营商 I_y 的探测点访问 RY 集合中的 R_i 的 rtt_avg 取值高于 RN 集合中的 rtt_avg 的根域名服务器所占 RN 集合的比例。

b) isp_rtt_warn(I_y, R_i, RN, T_s, T_e) 表示在运营商 I_y 各省份访问 RY 集合中的 R_i 的 rtt_warn 均值。

c) mirror_rtt_warn(R_i, RN, T_s, T_e) 表示在地区 Z 各运营商访问 R_i 的 isp_rtt_warn 均值。

d) main_rtt_warn(RY, RN, T_s, T_e) 表示在地区 Z 各运营商访问 RY 中各个根域名服务器的 mirror_rtt_warn 均值。

表 5 rtt_warn 计算方法

伪代码

```
R_i_avg=rtt_avg(P_x,I_y,R_i,T_s,T_e)
warn_num=0
for r in RN
{
    avg=rtt_avg(P_x,I_y,r,T_s,T_e)
    if(R_i_avg>avg){
        warn_num++;
    }
}
RN_length=length(RN)
rtt_warn=warn_num/RN_length
```

网络异常的指标：

route_warn_level = main_rtt_warn(RY, RN, T_s, T_e)

如果 route_warn_level 取值较大，则表示地区 Z 的路由或网络状态存在明显异常。如果地区 Z 并未部署 anycast 镜像，则 route_warn_level 取值为 0。

2.4 省份差异

如果在某个时间段内，根域名服务器 R_i 在某个运营商 I_y 的各个省份访问质量比较均衡，那么在该时段内运营商 I_y 访问 R_i 的监测数据中，各省份的平均访问时延应该相差不大。对此本文设计以下量化指标项：

a) rtt_avg(P_x, I_y, R_i, T_s, T_e) 表示在时间区间 $[T_s, T_e]$ 内，位于省份 P_x 运营商 I_y 的探测点访问根域名服务器 R_i 的监测数据中，访问时延 rtt 的均值。

b) isp_rtt_std(I_y, R_i, T_s, T_e) 表示在运营商 I_y 各省份访问根域名服务器 R_i 的 rtt_avg 除以 100 ms 所得数值集合的标准差。除以 100 ms 的目的是缩放数据，使得标准差取值更加稳定。

c) mirror_rtt_std(R_i, T_s, T_e) 表示在地区 Z 的各运营商访问 R_i 的 isp_rtt_std 均值。

d) main_rtt_std(T_s, T_e) 表示在地区 Z 访问根域名服务器集合

中各个 R_i 的 mirror_rtt_std 均值。

省份差异的指标：

$$rtt\_diff\_level = main\_rtt\_std(T_i, T_e)$$

如果 rtt_diff_level 取值较小，则表示地区 Z 访问根服务体验比较均衡。

2.5 异常监测

基于 3.1 ~ 3.4 节设计的基础指标，可以计算各种场景下根域名服务的整体异常监测指标 main_error_level。根据基础指标的重要程度，可以灵活配置权重及相关阈值，例如表 6 中设计的示例权重，权值最高的是 rtt_status 整体访问质量，其次为 local_mirror 本地镜像命中程度。指标阈值主要参考历史数据进行设置。

3 监测数据分析

当前中国境内已部署 F、I、J、L 共 4 个根域名服务器的 anycast 镜像，集中部署于北京市。

本文抽样选取了 2015.5.10 ~ 2015.5.16 中国境内 32 个省份的重点运营商监测点访问 F 根、L 根的数据进行分析。

3.1 F 根监测和评估结果

表 7 是 F 根监测的指标取值。

表 6　main_error_level 计算方法

伪代码

```
weight={
    rtt_status:8,
    local_mirror:4,
    rtt_warn:2,
    rtt_diff:1
};
main_error_level=0;
if(root_mirror_num_in_the_zone>0){
    if(rtt_status_level<RTT_STATUS_THR){
        main_error_level+=weight{'rtt_status'};
        alert('LOW RTT STATUS LEVEL:'+rtt_status_level);
    }
    if(local_mirror_level<LOCAL_MIRROR_THR){
        main_error_level+=weight{'local_mirror'};
        alert('LOW LOCAL MIRROR LEVEL:'+local_mirror_level);
    }
    if(rtt_warn_level>RTT_WARN_THR){
        main_error_level+=weight{'rtt_warn'};
        alert('HIGH RTT WARN LEVEL:'+rtt_warn_level);
    }
}
    if(rtt_diff_level>RTT_DIFF_THR){
        main_error_level+=weight{'rtt_diff'};
        alert('HIGH RTT DIFF LEVEL:'+rtt_diff_level);
    }
if(main_error_level>0){
        alert('MAIN ERROR LEVEL:'+main_error_level);
}
```

表 7　F 根监测指标

监测指标	ISP_A	ISP_B
main_error_level	0	15
rtt_status_level	0.989 956 573	0.078 885 577
local_mirror_level	1	0.117 647 06
route_warn_level	0	0.797 385 621
rtt_diff_level	0.194 078 875	1.112 284 567

ISP_A：local_mirror_level 取值为 1，表示从 ISP_A 多个监测点访问 F 根基本全部命中本地 anycast 镜像；rtt_status_level 取值约 0.99、route_warn_level 取值为 0，表示各省份访问 F 根质量极优；rtt_diff_level 取值约 0.19，表示各省份访问 F 根质量比较均衡。main_error_level 取值为 0，表示 F 根在 ISP_A 总体服务较好。

ISP_B：local_mirror_level 取值为约 0.12，表示从 ISP_B 多个监测点访问 F 根只有小部分命中本地 anycast 镜像；rtt_status_level 取值约 0.08，表示多个省份访问 F 根质量极差；route_warn_level 取值约 0.80，表示 ISP_B 多个省份访问 F 根链路质量比其他多个根服务器差。main_error_level 取值为 15，表示 F 根在 ISP_B 总体服务很差，需要进行链路优化。

图 1 是 F 根访问命中镜像（root_mirror_loc）比例图。在所有访问 F 根的监测记录中，ISP_A 命中国内镜像的比例为 100%；ISP_B 命中国内镜像的比例为 6.21%。与表 7 的指标取值对比检查，可见 local_mirror_level 能够有效地衡量 F 根国内镜像生效情况。

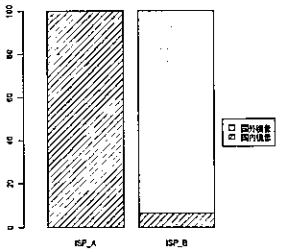

图 1　F 根访问命中镜像

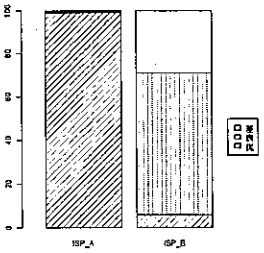

图 2　F 根访问时延状态

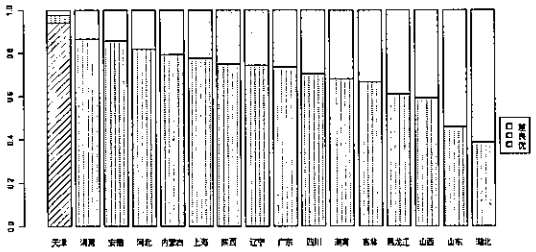

图 3　ISP_B 各省份监测点访问 F 根的时延状态

图 2 是 F 根访问的时延状态（rtt_status）比例图，图 3 是 ISP_B 各省份监测点访问 F 根的时延状态（rtt_status）比例图。在所有访问 F 根的监测记录中，ISP_A 状态为优的比例为 99.02%；ISP_B 状态为优的比例为 5.83%，状态为良的比例为 65.35%。与表 7 的指标取值、图 1 的命中镜像情况对比检查，可见 rtt_status_level 能够有效地衡量 F 根国内访问质量，rtt_warn_level 能够有效发现根镜像访问异常，rtt_diff_level 能够有效发现根镜像访问质量不均衡，ISP_B 的访问质量较差的问题主要在于大部分省份访问未能命中国内镜像。

3.2 L 根监测和评估结果

表 8 是 L 根监测的指标取值。

表 8　L 根监测指标

监测指标	ISP_A	ISP_B
main_error_level	0	0
rtt_status_level	0.807 552 958	0.987 029 158
local_mirror_level	1	1
route_warn_level	0.046 296 296	0
rtt_diff_level	0.806 155 408	0.115 449 219

ISP_A：local_mirror_level 取值为 1，表示从 ISP_A 多个监测点访问 L 根基本全部命中本地 anycast 镜像；rtt_status_level 取值约 0.81，表示各省份访问 L 根质量 L 根相对较优；rtt_diff_level 取值约 0.81、route_warn_level 取值约 0.05，表示小部分省份访问 L 根质量存在异常。main_error_level 取值为 0，表示 L 根在 ISP_A 总体服务较好。

ISP_B：local_mirror_level 取值为 1，表示从 ISP_B 多个监测点访问 L 根基本全部命中本地 anycast 镜像；rtt_status_level 取值约 0.99、route_warn_level 取值为 0，表示各省份访问 L 根质量 L 根极优；rtt_diff_level 约 0.12，表示极少省份访问 L 根质量存在异常。main_error_level 取值为 0，表示 L 根在 ISP_A 总体服务较好。

图 4 是 L 根访问命中镜像（root_mirror_loc）比例图。在所有访问 L 根的监测记录中，ISP_A 与 ISP_B 全部命中国内镜像，表 8 中 local_mirror_level 取值均为 1。

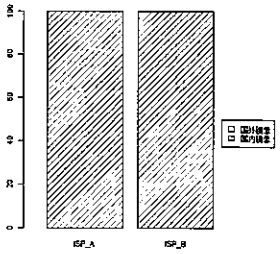

图 4 L 根访问命中镜像

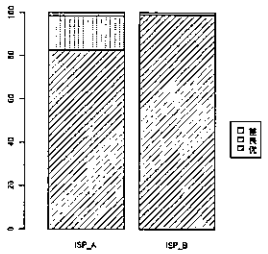

图 5 L 根访问时延状态

图 5 是 L 根访问的时延状态比例图，图 6 是 ISP_A 各省份监测点访问 L 根的时延状态比例图。在所有访问 L 根的监测记录中，ISP_A 状态为优的比例为 85.52%，状态为良的比例为 15.83%；ISP_B 状态为优的比例为 98.71%。与表 8 的指标取值、图 4 的命中镜像情况对比检查，可见 rtt_diff_level 能够有效地衡量 L 根国内各地访问质量差异，rtt_status_level 能够有效地衡量 F 根国内访问质量，rtt_warn_level 能够有效发现根镜像访问异常，ISP_A 部分访问质量较差的问题主要在于小部分省份访问国内镜像的时延较长。

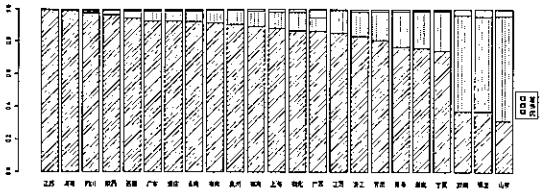

图 6 ISP_A 各省份监测点访问 L 根的时延状态

3.3 F 根与 L 根服务对比分析

对比 3.1 与 3.2 节监测指标数据可见，在中国境内 L 根服务质量整体优于 F 根。在中国境内访问 L 根，基本命中本地 anycast 镜像，只有 ISP_A 少数省份访问时延略长。F 根的问题在于 anycast 本地镜像路由生效范围较小，从 ISP_B 较多省份访问，未能命中本地 anycast 镜像以加速访问。

4 结束语

鉴于根镜像 anycast 节点分散部署，服务生效评估存在相当的复杂性，并且服务状态随时间以及网络链路状态存在波动。

本文结合 CNNIC 探测数据分析，提出了一种评估 DNS 根域名服务的方法。该方法结合查询时延与服务器分布的地理信息，能够快速有效地区分并定位根镜像 anycast 节点在实际部署服务过程中可能出现的各类异常。通过 F 根、实际探测数据，也验证了本文提出的方法的可行性。

本文提出的算法目前主要是针对根镜像的 anycast 服务进行评估，事实上该评估算法框架同样适用于部署了 anycast 其他互联网业务。

此外，由于域名解析服务的分层特性，多数普通用户通过运营商递归 DNS 服务器、google 等公共递归服务器获取域名解析结果。因此，各地区根服务的实际访问质量，一般还与递归 DNS 服务器采用的根 NS 访问选择策略、迭代查询启动时采用的 db. root 等等相关，这也是 Google 提出在本地环回自行搭建根服务[10]以彻底加速递归访问根服务器时延的原因所在。

参考文献：

[1] Mockapetris P V. RFC 882, Domain names-concepts and facilities[S]. US: RFC, 1983.

[2] Mockapetris P V. RFC 1034, Domain names-concepts and facilities [S]. US: RFC, 1987.

[3] IANA. root-servers. org[EB/OL]. http://root-servers. org/.

[4] Abley J, Manderson T. A summary of various mechanisms deployed at l-root for the identification of anycast nodes[EB/OL]. [2014-05-29]. http://tools. ietf. org/html/draft-jabley-dnsop-anycast-mapping-04.

[5] Jung J, Sit E, Balakrishnan H, *et al.* DNS performance and the effectiveness of caching[J]. IEEE/ACM Trans on Networking, 2002, 10 (5): 589-603.

[6] 李恩宝，张文东，王超. 域名系统的部署及安全性分析与建议[J]. 信息安全与通信保密，2010(5)：81-83.

[7] 范文. 基于 Anycast 技术部署 DNS 系统设计与实现[D]. 济南：山东大学，2013.

[8] 彭巍，曹维华，李文云，等. 基于全局 anycast 的智能域名系统架构演进研究[J]. 广东通信技术，2014，34(5)：14-17.

[9] 杜跃进，张兆心，王克，等. 基于贡献度分析的 DNS 服务质量评价模型[J]. 南京理工大学学报：自然科学版，2013(6)：833-838.

[10] Kumari W, Hoffman P. Decreasing access time to root servers by running one on loopback[EB/OL]. [2015-05-15]. https://tools. ietf. org/html/draft-wkumari-dnsop-root-loopback-01.

(上接第 284 页)

参考文献：

[1] Bellovin S M, Merritt M. Encrypted key exchange: password-based protocols secure against dictionary attacks[C]//Proc of IEEE Computer Society Symposium on Research in Security and Privacy. 1992: 72-84.

[2] Abdalla M, Pointcheval D. Simple password-based encrypted key exchange protocols [C]//Proc of the 25th Annual International Cryptology Conference. 2005: 191-208.

[3] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks[C]//Proc of the 19th International Conference on the Theory and Application of Cryptographic Techniques. 2000: 139-155.

[4] Bresson E, Chevassut O, Pointcheval D. Security proofs for efficient password-based key exchange[C]//Proc of the 10th ACM Conference on Computer and Communications Security. 2003: 241-250.

[5] Bresson E, Chevassut O, Pointcheval D. New security results on encrypted key[C]//Proc of the 7th International Workshop on Theory and Practice in Public Key Cryptography. 2004: 145-158.

[6] Bellovin S M, Merritt M. Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise[C]//Proc of the 1st ACM Conference on Computer and Communications Security. 1993: 244-250.

[7] Boyko V, Mackenzie P, Patel S. Provably secure password authentication and key exchange using Diffie-Hellman[C]//Proc of the 19th International Conference on the Theory and Application of Cryptographic Techniques. 2000: 156-171.

[8] Mackenzie P. More efficient password-authenticated key exchange [C]//Proc of Cryptographers' Track at RSA Conference. 2001: 361-377.

[9] Mackenzie P. The PAK suite: protocols for password-authenticated key exchange discrete mathematics and theoretical computer science, 2002-46[R]. [S. l.]: DIMACS Technical, 2002.

[10] Gentry C, Mackenzie P, Ramzan Z. A method for making password-based key exchange resilient to server compromise[C]//Proc of the 25th Annual International Cryptology Conference. 2006: 142-159.

[11] Cash D, Kiltz E, Shoup V. The twin Diffie-Hellman problem and applications[J]. Journal of Cryptology, 2009, 22(4): 470-504.

[12] Farash M, Attari M. An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps[J]. Nonlinear Dynamics, 2014, 77(1): 399-411.

[13] Lee C C, Li C T, Hsu C W. A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps[J]. Nonlinear Dynamics, 2013, 73(2): 125-132.

[14] Menezes A. Another look at HMQV[J]. Journal of Mathematical Cryptology, 2007, 1(1): 47-64.

[15] Krawczyk H. Hmqv: a high-performance secure Diffie-Hellman protocol [C]//Proc of the 25th Annul International Cryptology Conference. 2005: 546-566.