IPv6与DNSSEC

中国科学技术大学 网络信息中心 张焕杰

2020年12月2日

DNS系统简介

DNS系统的IPv6支持

DNSSEC原理介绍

SPF、DKIM、DMARC

中国科大DNS服务介绍

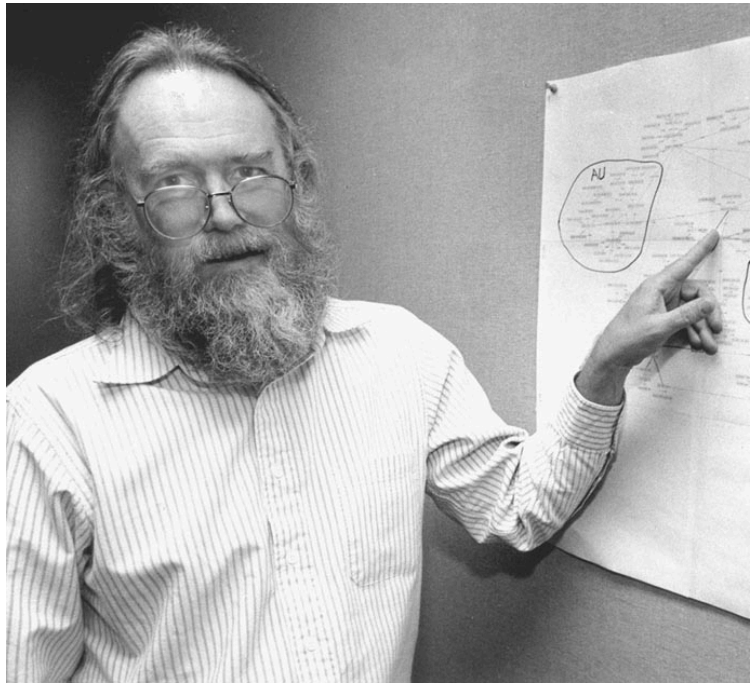
DNS系统简介

很早很早以前，没有DNS

hosts 文件存放着 主机名 和 IP地址 对应关系

- 文件越来越大，没有域的概念，很容易重名
- 每台主机需要拷贝更新，经常过期互相不一致
- 单人管理

1983年11月（距今37年前，距离1981年9月RFC791 IP协议提出2年后）
RFC881: The Domain Names Plan and Schedule (J. Postel)
RFC882: Domain Names - Concepts and Facilities (P. Mockapetris)
RFC883: Domain Names - Implementation Specification (P. Mockapetris)



J. Postel
Information Sciences Institute
University of Southern California

DNS系统的特性

Client-Server工作模式
请求和应答使用UDP/TCP 53

全局分发

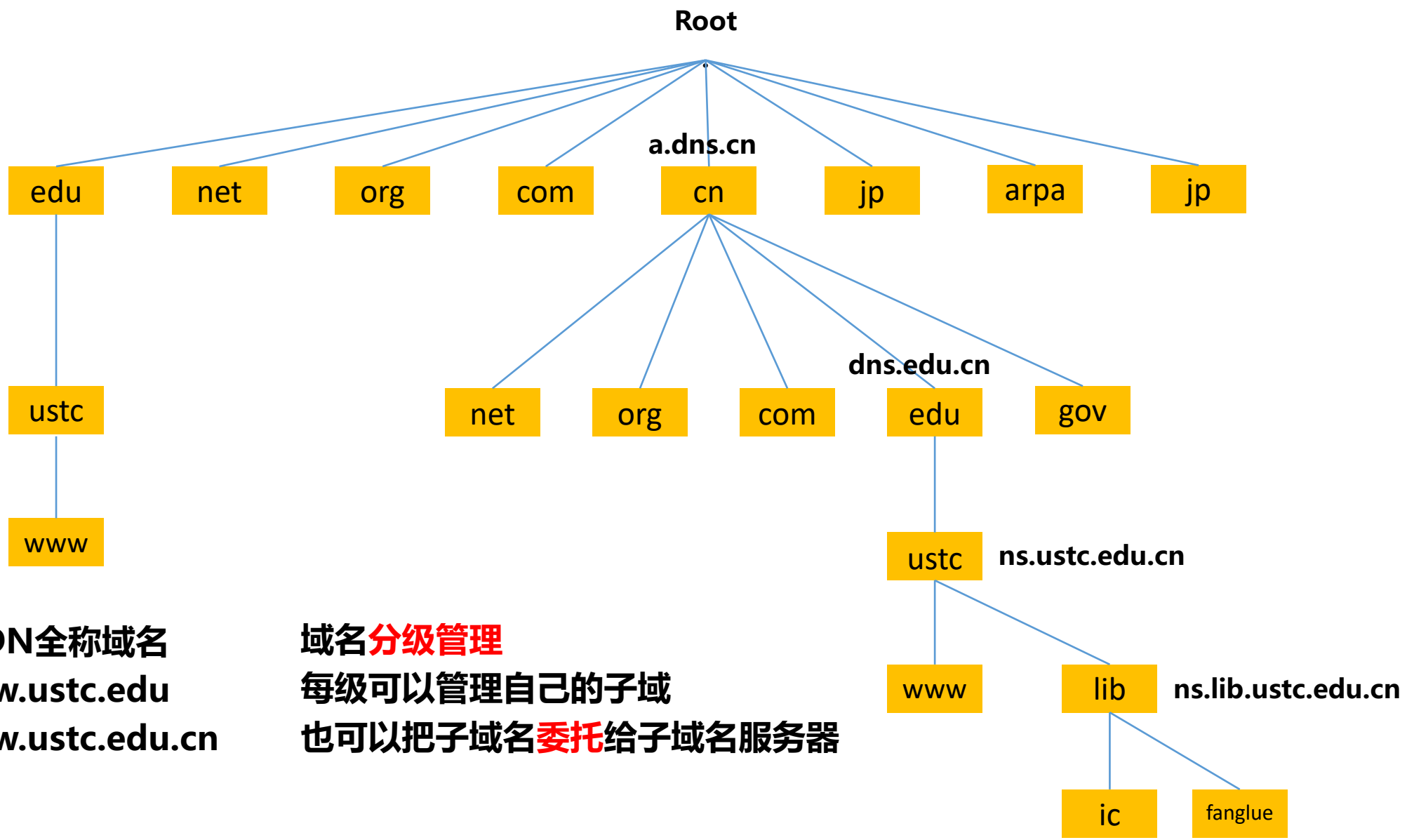
低耦合

可扩展

可靠

动态

DNS域名层次



FQDN全称域名

www.ustc.edu

www.ustc.edu.cn

域名分级管理

每级可以管理自己的子域

也可以把子域名委托给子域名服务器

DNS中资源记录

DNS系统负责解析某个域名，指的是解析资源记录

```
#dig ustc.edu.cn in mx
ustc.edu.cn. 3600 IN MX 10 smtp.ustc.edu.cn.
ustc.edu.cn. 3600 IN MX 10 smtp2.ustc.edu.cn.
ustc.edu.cn. 3600 IN MX 5 smtp1.ustc.edu.cn.
```

Label	TTL	CLASS	Type	RDATA
名字	超时时间 允许中间 设备缓存 最长时间	IN CH	A AAAA NS PTR CNAME MX TXT	

RR Type	含义
A	域名对应的IP v4地址
AAAA	域名对应的IP v6地址
NS	域名委托给另一个域名服务器
PTR	IP对应的域名
CNAME	别名对应到域名
MX	邮件转发服务器
TXT	文字信息

TTL设置优化

针对不同的资源，设置不同的TTL

如 ustc.edu.cn TTL 3600

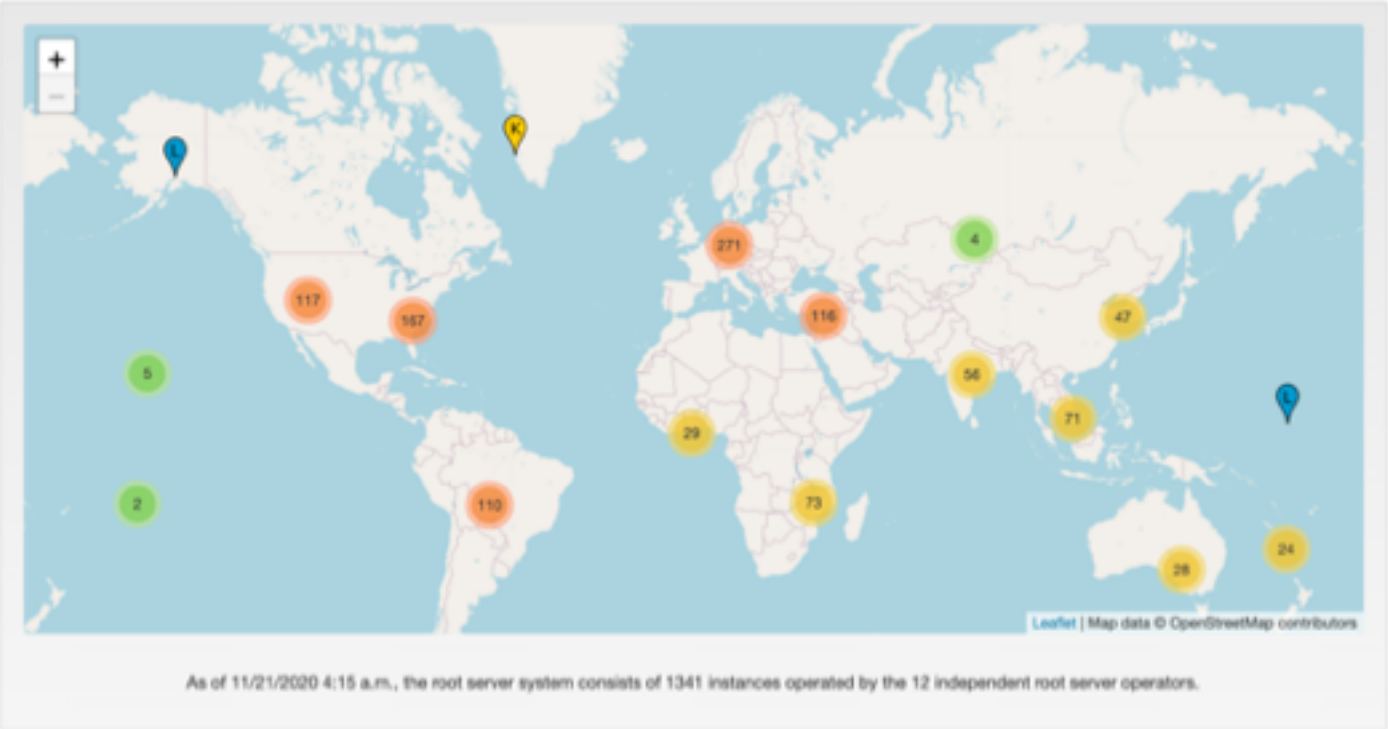
www.ustc.edu.cn TTL 600

不建议设置特别短的TTL

DNS root根服务器

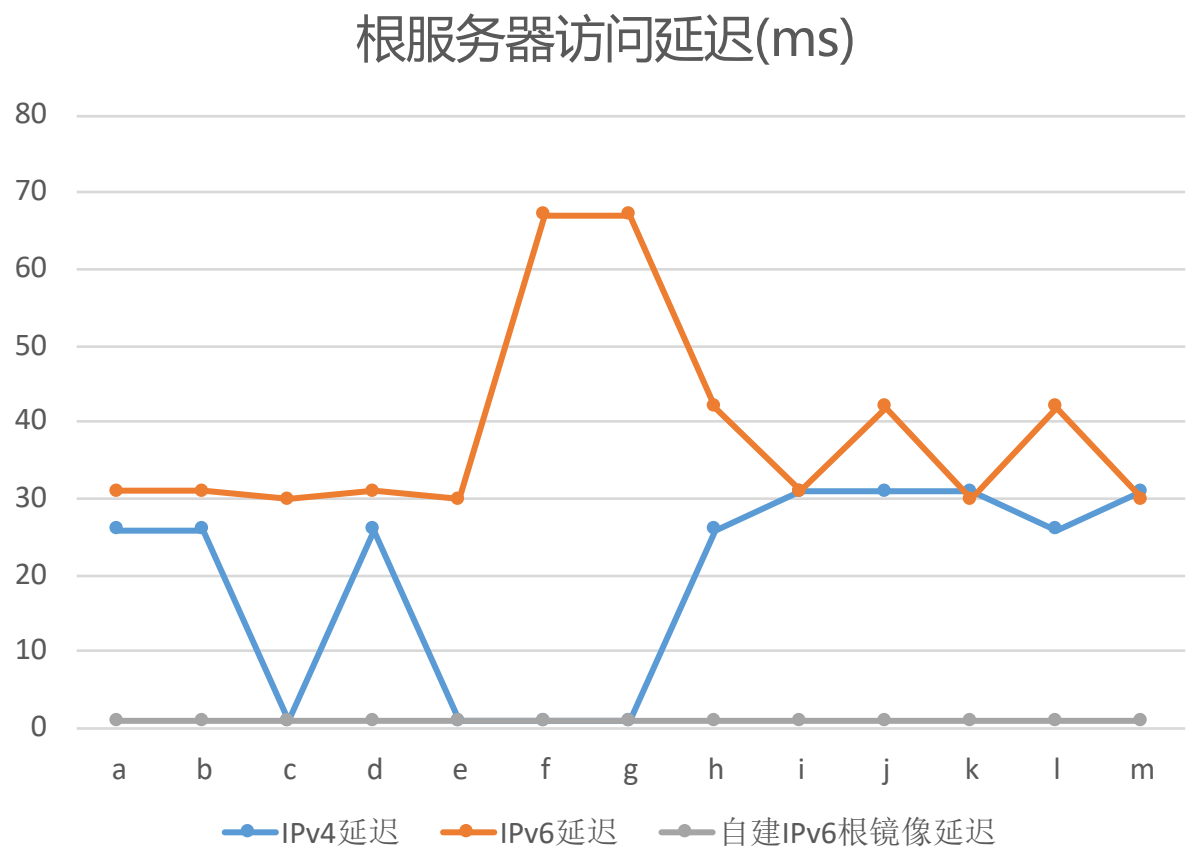
https://root-servers.org/

- 由于UDP数据包长度的原因，根DNS服务器名字最多只有13个，是 [a-m].root-servers.net
- 实际上每个名字（地址）对应有多台提供服务的服务器，或者说存在很多台根DNS服务器，它们具有相同的IP地址
- DNS这种服务，称为AnyCast服务，可以由很多设备使用相同的IP，就近对外提供服务



DNS root根服务器的镜像

- 根服务器的数据是公开的（https://www.iana.org/domains/root/files）
- 网络管理员可以使用上述数据，设置根镜像服务器，供某个范围内使用



测试时间：2020年11月21日 11:30
测试地点：中国科大网络信息中心机房虚拟机
测试方法：
dig -4 @a.root-servers.net
dig -6 @a.root-servers.net
查看返回的Query time: 延迟时间

测试结论：CERNET内部存在根服务镜像
其中在合肥核心节点设置有c e f g 的IPv4镜像

DNS系统简介

DNS系统的IPv6支持

DNSSEC原理介绍

SPF、DKIM、DMARC

中国科大DNS服务介绍

DNS的IPv6支持，非常简单

① DNS服务器对外解析域名的IPv6地址

原有的DNS服务器，只要增加类似的记录即可

```
www  IN AAAA 2001:da8:d800:642::248
```

② DNS服务器使用IPv6地址提供解析服务

网络接口设置IPv6地址
软件在IPv6协议提供服务

```
listen-on-v6 port 53 { any; };
```

防火墙允许tcp/udp 53端口流量

③ 注册并提供IPv6地址反向解析服务

http://www.nic.edu.cn/RS/templates/cindex.html
IP6.ARPA注册表格
自己DNS服务器上增加相关记录

DNS系统简介

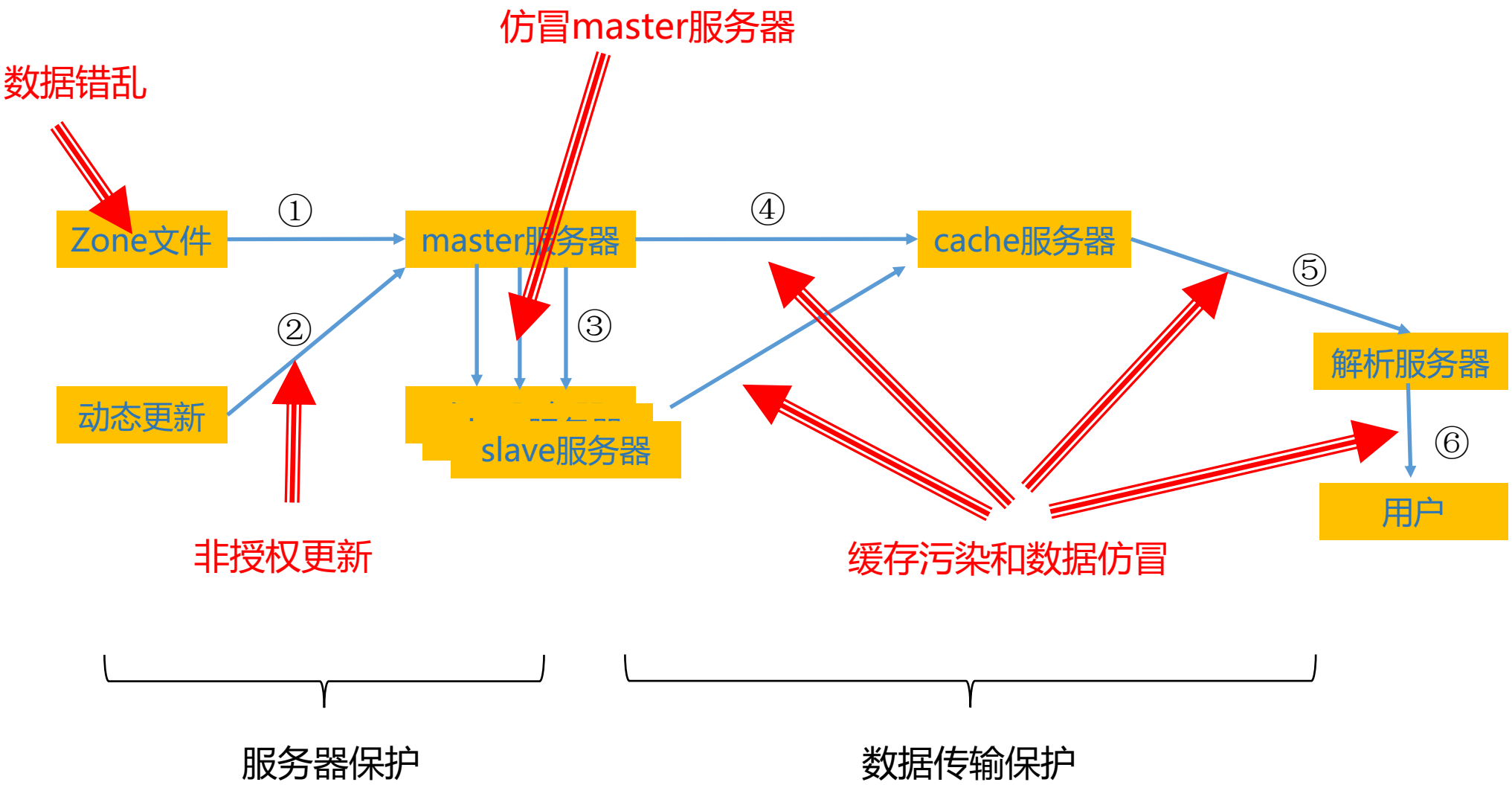
DNS系统的IPv6支持

DNSSEC原理介绍

SPF、DKIM、DMARC

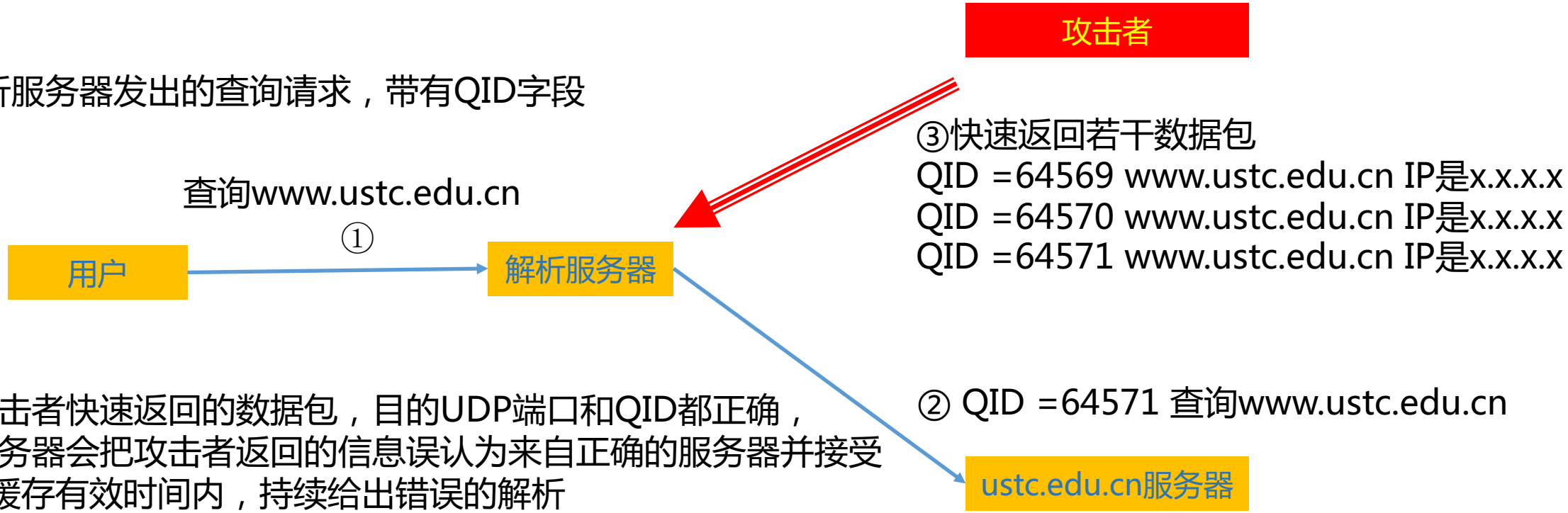
中国科大DNS服务介绍

DNS数据流及隐患


仿冒master服务器
数据错乱
Zone文件
①
master服务器
④
cache服务器
⑤
②
③
解析服务器
动态更新
slave服务器
⑥
用户
非授权更新
缓存污染和数据仿冒
服务器保护
数据传输保护

DNS缓存污染（缓存投毒）攻击

解析服务器发出的查询请求，带有QID字段



如果攻击者快速返回的数据包，目的UDP端口和QID都正确，解析服务器会把攻击者返回的信息误认为来自正确的服务器并接受在TTL缓存有效时间内，持续给出错误的解析

暂时的解决办法是随机化UDP源端口和QID，增大攻击难度

比较彻底的解决：

- 服务器之间使用DNSSEC，即使用现代密码学技术验证杜绝篡改
- 用户到服务器间使用DoT/DoH，即使用TLS加密避免攻击

DNSSEC的工作机制

https://blog.csdn.net/syh_486_007/article/details/50990973
DNSSEC 原理、配置与布署简介　　清华大学 段海新

首先生成公钥私钥对

① 使用私钥对DNS资源记录进行签名，以保障不被篡改

② 资源记录的签名信息通过DNS协议发布　　新增RRSIG记录

③ 公钥也通过DNS协议发布，以便另一方进行验证　　新增DNSKEY记录

④ 子域名服务器，使用它的私钥对记录进行签名

⑤ 父域名服务器对子域名的公钥摘要进行签名　　新增DS记录

⑥ 禁止别人仿冒不存在域名应答　　新增NSEC/NSEC3记录

RRSIG记录

资源记录的签名信息

签名算法类型，RSASHA1-NSEC3-SHA1

bbs.ustc.edu.cn一共有4段

签名时间　　KEY编号

```
bbs.ustc.edu.cn. 1200 IN A 202.38.64.3
                 1200 RRSIG A 7 4 1200 (
                 20201220035831 20201120035831 32747 ustc.edu.cn.
                 S2OWLUROSw2b0tvGJtEmNPaVZl2c2CmBxRsE
                 x1hhOP1zIMYTJybE9PLpasW5mcjcAvIsTRwE
                 nVJTQkpdLkBcMfLgmvY/X98dZLorIlg25zYI
                 hYuyhPLN5364MDLMH2yGtZgOKqcl4SGRi0/d
                 b1HyJP7I4ovPbRaZ27fDvauhqqY= )
```

失效时间
签名时间+30天

30天要签名一次
我校是修改DNS文件后签名
一般来说不会30天不改一次

Base64编码的数字签名信息

DNSKEY记录

256 ZSK，257 KSK

签名算法类型，RSASHA1-NSEC3-SHA1

公钥信息

```
ustc.edu.cn. 1200    DNSKEY  256 3 7 (
                AwEAAZ/Me3jG9Lgpyh7kHMHm/jTGttmeaV2i
                xsEY7/cmE03Y5hYoOmkMFBGtq8xaE16hoPVD
                dp6QEzM/S+zMaex5JmkZ3pYwdwoslQ9VbHgT
                nO+nx0nt5j+moYzqiAK5ht2jJkm8vshikyVW
                behMrHrrn1tjbkjPLFriaCftHAPXss13
                ) ; ZSK; alg = NSEC3RSASHA1 ; key id = 32747
        1200    DNSKEY  257 3 7 (
                AwEAAbhtB5jRa0xcRdXjJhSsJhWUv9ZOf3hw
                ...... QmEwDbFXGVN4+TJECo75f5c=
                ) ; KSK; alg = NSEC3RSASHA1 ; key id = 19065
```

Base64编码的公钥信息

NSEC/NSEC3记录

发送一个域名的解析请求，如果仿冒方返回不存在应答怎么办？

Next Secure

简单的理解：

把所有存在的域名前后相连
解析时可以检测是否仿冒了不存在域名应答

攻击者可以用NSEC来穷举域内所有记录，泄漏域名

NSEC3把域名的hash前后相连，攻击者要穷举的话需要花费更多的算力

DS记录

公钥摘要

KEY ID

签名算法类型，RSASHA1-NSEC3-SHA1

签名类型，1=SHA1, 2= SHA256

ustc.edu.cn. IN DS 19065 7 1 4EBE527CCF84FC2
DD62ACFCD464BE008E0FEAF68

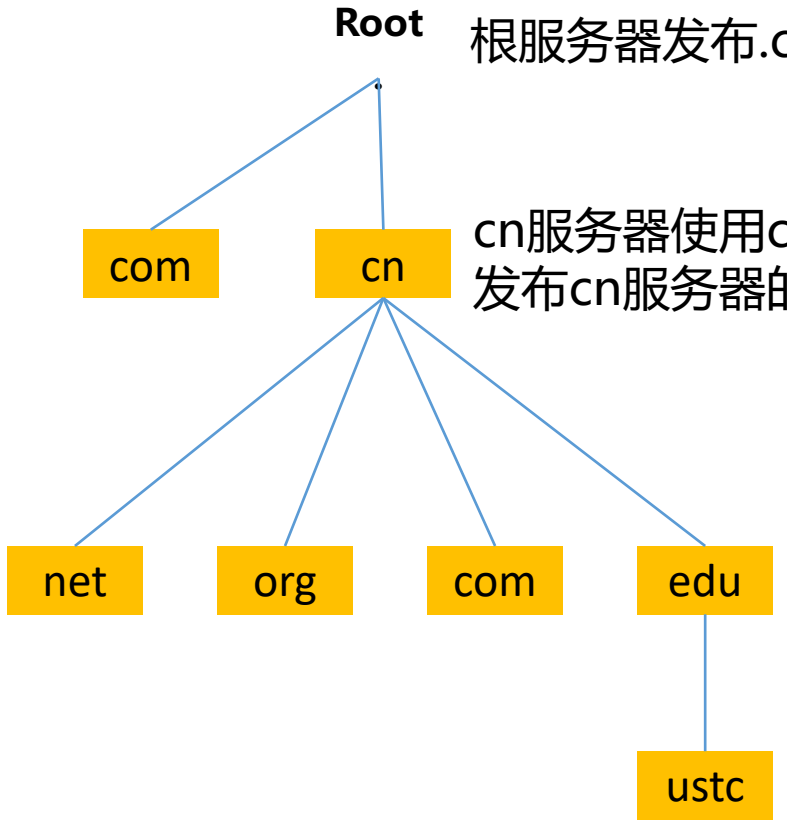
ustc.edu.cn. IN DS 19065 7 2 EBD1C6420F893D8
FF9950ADBF896075D05900643
9419634128566709 8EBD74F1

公钥的摘要

上述内容交给上级域名服务器对外发布，
发布时上级域名服进行签名确保正确
从而形成从根开始的信任链

信任链

根服务器的公钥bind.keys https://www.isc.org/bind-keys/ 存放在每个域名服务器上



根服务器发布.cn服务器的DS记录，并使用根服务器私钥签名

cn服务器使用cn服务器私钥签名
发布cn服务器的DNSKEY记录，.edu.cn服务器的DS记录，

edu.cn服务器使用edu.cn服务器私钥签名
发布edu.cn服务器的DNSKEY记录，ustc.edu.cn服务器的DS记录

ustc.edu.cn服务器使用ustc.edu.cn服务器私钥签名
发布ustc.edu.cn的DNSKEY记录和相关子域记录

ZSK KSK

为什么设置两种类型的KEY？

公钥是公开的，如果有足够的算力和时间可以得到私钥，即破解

密钥长度越长，破解的时间越长，日常使用计算量也越大

DNS SEC主要用来签名验证，因此只要定期更换密钥，确保一定时间内不被破解就行

如果每次更换密钥，都要请求上级域名服务器修改DS记录，太麻烦了

设计了2组密钥长短结合的工作机制：

- ZSK(zone 签名密钥) 短，定期更换，用来对DNS 记录数据签名
- KSK(key签名密钥) 长，破解更难，提交给上级域名服务器，用来对ZSK签名

解析服务器启用DNSSEC验证

对于常用的bind软件，只要增加如下的配置即可

dnssec-validation yes;

无错误

```
$ dig @202.38.64.56 www.sjtu.edu.cn +dnssec +multiline

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42681
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; ANSWER SECTION:
www.sjtu.edu.cn. 560 IN A 202.120.2.119
www.sjtu.edu.cn. 560 IN RRSIG A 8 4 3600 (
                20201220001052 20201120001052 9528 sjtu.edu.cn.
                oQLZnaj6sxiCiLDrDlGb89WxPF6BurkrjGVT13XJqitG
                JDmbrY5i9ortiIn0ZYXcCw7pi8E3FDGZ8fTNDCBoHksV
                UKw/S7CqljGXC6sbyLce0BUc2DR+X9QnshPMkOCbanNK
                QT8OdDHYE8D4sdgxlL4WfB5SM3dPAIxHmEz6M5A= )
```

‘ad’ bit – authenticated data

解析服务器DNSSEC验证失败的例子

dnssec-failed.org 是一个配置错误的测试域

202.38.64.1 DNS服务器未启用
DNSSEC验证，可以返回A记录

```
$ dig @202.38.64.1 dnssec-failed.org +dnssec +multiline

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22565
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; ANSWER SECTION:
dnssec-failed.org. 600 IN A 69.252.80.75
```

202.38.64.56 DNS服务器启用
DNSSEC验证，返回错误

```
$ dig @202.38.64.56 dnssec-failed.org +dnssec +multiline

;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 54472
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
```

常见服务器DNSSEC验证测试对比

	DNSSEC验证	延迟(ms)	备注
1.1.1.1	✔	300	
8.8.8.8	✔	80	
114.114.114.114	否	40	
119.28.28.28	否	12	DNSPod
223.5.5.5.5	否	28	阿里云
101.7.8.9	否	10	CERNET
202.38.64.56	✔	1	中科大用户DNS

结论：国内DNS服务器几乎都不支持DNSSEC验证

权威域名服务器的DNSSEC部署

① 启用DNSSEC功能

② 生成KSK和ZSK

③ 将相关DNSKEY加入域文件（可以用$INCLUDE包含）

④ 对域文件做签名

⑤ 对外服务签名后的文件

⑥ 测试功能

⑦ 将DS记录交给edu.cn管理员发布

ipv6.ustc.edu.cn/index.php?groupid=1

	单位	网站	DNSSEC	v4 HTTP	v4 HTTPS	v4 HTTP2	v6解析	v6 HTTP	v6 HTTPS	v6 HTTP2	评分
1	UPenn	www.upenn.edu	✔	✔	✔	✔	✔	✔	✔	✔	112
2	普林斯顿	www.princeton.edu	✔	✔	✔	✔	✔	✔	✔	✔	109
3	剑桥	www.cam.ac.uk	✔	✔	✔	✔	✔	✔	✔	✔	107
4	耶鲁	www.yale.edu		✔	✔	✔	✔	✔	✔	✔	90
5	IC	www.imperial.ac.uk	✔	✔	✔		✔	✔	✔		80
6	Umich	umich.edu		✔	✔		✔	✔	✔		70
7	ETH	www.ethz.ch		✔	✔		✔	✔	✔		70
8	MIT	www.mit.edu		✔	✔		✔	✔	✔		70
9	清华大学	www.tsinghua.edu.cn		✔	✔		✔	✔	✔		70
10	Caltech	www.caltech.edu	✔	✔	✔	✔					60
11	斯坦福	www.stanford.edu	✔	✔	✔	✔					60
12	UChicago	www.uchicago.edu	✔	✔	✔	✔					60
13	哈佛	www.harvard.edu		✔	✔	✔					50
14	牛津	www.ox.ac.uk		✔	✔	✔					50
15	Columbia	www.columbia.edu		✔	✔						40

DNS系统简介

DNS系统的IPv6支持

DNSSEC原理介绍

SPF、DKIM、DMARC

中国科大DNS服务介绍

SPF、DKIM、DMARC

通过DNS发布一些TXT信息，增强邮件系统的安全性

SPF(Sender Policy Framework)，发布发信IP地址信息，如

```
ustc.edu.cn. 3600 IN TXT "v=spf1 ip4:202.38.64.8 ip6:2001:da8:d800::8 ip6:2001:da8:d800::46 -all"
```

DKIM(DomainKeys Identified Mail)，发布邮件服务器公钥
邮件服务器发出的邮件头From/To/Subject/Date/Message-ID等字段内容进行签名

```
dkim._domainkey.ustc.edu.cn. 3600 IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDJvKz7FR0FC8iH15PgZIW720prG7yeJSc0ZVtrT1Q6pOazbMev
kNTIYap+VQfh0qqrkDq0WXiJJ6IwURaPFluYs5Gxcj84RAX9s2qBhzlGA6HdvRGH8PwnFW4wacM6c8v62aWP/NfslJg+LZ
kRpLJG7e52Fv6RFKhkoNpQYyGfmQIDAQAB"
```

DMARC(Domain-based Message Authentication, Reporting & Conformance)
邮件接收方收到伪造的邮件时，向被伪造的域名管理员发送反馈。

```
_dmarc.ustc.edu.cn. 3600 IN TXT "v=DMARC1; p=quarantine; rua=mailto:postmaster@ustc.edu.cn"
```

邮件SPF和DKIM验证例子

```
Received: from tsinghua.edu.cn (unknown [59.66.3.29])
        by newmailweb.ustc.edu.cn (Coremail) with SMTP id LkAmygAnh3Ck5Khfw47gAA--.24846S2;
        Mon, 09 Nov 2020 14:41:41 +0800 (CST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=tsinghua.edu.cn; s=dkim; h=Received:To:From:Subject:Message-ID:
        Date:User-Agent:MIME-Version:Content-Type:
        Content-Transfer-Encoding; bh=2oxJgIibPkuiasgA36XqVD1jI4PEuaab57
        x9qWOGItQ=; b=AECx5lH57Jp/bWoLoa9rMRGr4I9heVgRcl4Smr/QW0qtTgO6nw
        gmawPoEFkaOVKHWse4gvDoBztnskD9y4Vl+ELM7LCo6MVBw5PBCPb7BohCAalzKi
        DrSlb8NerfnN0Nzv4Ai7VgjZ95/ZDTcZegu1/dnFIh4aByyB4nX8vvjfo=
Received: from [166.111.2.13] (unknown [166.111.2.13])
        by web2 (Coremail) with SMTP id yQQGZQCH_fij5KhfdysAAA--.523S3;
        Mon, 09 Nov 2020 14:41:39 +0800 (CST)
To: james@ustc.edu.cn
From: =?UTF-8?B?6ams5LqR6b6Z?= <myl@tsinghua.edu.cn>
Subject: =?UTF-8?B?6L+Z5qyh5bqU6K+l5Y+v5Lul5LqG?=
Message-ID: <73612b28-c5a4-b7a6-8708-31ce34a0756e@tsinghua.edu.cn>
Date: Mon, 9 Nov 2020 14:42:29 +0800
Authentication-Results: newmailweb.ustc.edu.cn; spf=pass smtp.mail=myl
        @tsinghua.edu.cn; dkim=pass header.i=@tsinghua.edu.cn
```

邮件验证结果

Message ID	<d52a87.42269.1712efae989.Coremail.james@ustc.edu.cn>
Created at:	Tue, Mar 31, 2020 at 1:05 PM (Delivered after 59 seconds)
From:	Zhang Huanjie <james@ustc.edu.cn> Using Coremail Webmail Server Version XT3.(ustc-xl
To:	zhanghuanjie@gmail.com
Subject:	test
SPF:	PASS with IP 2001:da8:d800:0:0:0:0:8 Learn more
DKIM:	'PASS' with domain ustc.edu.cn Learn more
DMARC:	'PASS' Learn more

不符合SPF、DKIM的投递反馈邮件

DMARC Report	Report Domain: ustc.edu.cn Submitter: reports.emailsrvr.com Report-ID: 1f1a4ac0-d27e-4b81-885f-22c51...		11-22	6 K
noreply-dmarc-s...	Report domain: lists.ustc.edu.cn Submitter: google.com Report-ID: 5791005340681708282		11-22	4 K
noreply-dmarc-s...	Report domain: lists.ustc.edu.cn Submitter: google.com Report-ID: 5791005340681708282		11-22	4 K
noreply-dmarc-s...	Report domain: ustc.edu.cn Submitter: google.com Report-ID: 10405367896205667815		11-22	6 K
noreply-dmarc-s...	Report domain: mail.ustc.edu.cn Submitter: google.com Report-ID: 1318059499293209774		11-22	6 K
noreply-dmarc-s...	Report domain: lists.ustc.edu.cn Submitter: google.com Report-ID: 5791005340681708282		11-22	4 K
postmaster	Dmarc aggregate report		11-22	3 K
dmarc_reporter	Report Domain: ustc.edu.cn Submitter: umn.edu Report-ID: ustc.edu.cn-1605863342@umn.edu		11-22	4 K
noreply	Report Domain: mail.ustc.edu.cn Submitter: aol.fr Report-ID: <1606007176.673125>		11-22	4 K
noreply	Report Domain: mail.ustc.edu.cn Submitter: ghvxo.in Report-ID: <1606007176.673178>		11-22	4 K
noreply	Report Domain: mail.ustc.edu.cn Submitter: yahoo.com Report-ID: <1606007176.673281>		11-22	5 K
noreply	Report Domain: ustc.edu.cn Submitter: yahoo.com Report-ID: <1606007226.850118>		11-22	4 K
noreply	Report Domain: ustc.edu.cn Submitter: ymail.com Report-ID: <1606007226.853265>		11-22	4 K
noreply	Report Domain: ustc.edu.cn Submitter: aol.com Report-ID: <1606007226.849680>		11-22	4 K
noreply	Report Domain: ustc.edu.cn Submitter: yahoo.com.au Report-ID: <1606007226.852885>		11-22	4 K
noreply	Report Domain: ustc.edu.cn Submitter: cxsst.in Report-ID: <1606007226.849835>		11-22	4 K
noreply	Report Domain: ustc.edu.cn Submitter: yahoo.com.hk Report-ID: <1606007226.853037>		11-22	4 K
noreply	Report Domain: ustc.edu.cn Submitter: mhco.in Report-ID: <1606007226.849923>		11-22	4 K
noreply	Report Domain: ustc.edu.cn Submitter: yahoo.co.in Report-ID: <1606007226.850030>		11-22	4 K

常见服务器DKIM支持情况

	DKIM支持
gmail.com	✓
github.com	✓
163.com	✓
126.com	✓
qq.com	✓
hotmail.com	✓
139.com	否
tsinghua.edu.cn	✓
ustc.edu.cn	✓
ucsd.edu	✓
很多垃圾邮件域	✓

DNS系统简介

DNS系统的IPv6支持

DNSSEC原理介绍

SPF、DKIM、DMARC

中国科大DNS服务介绍

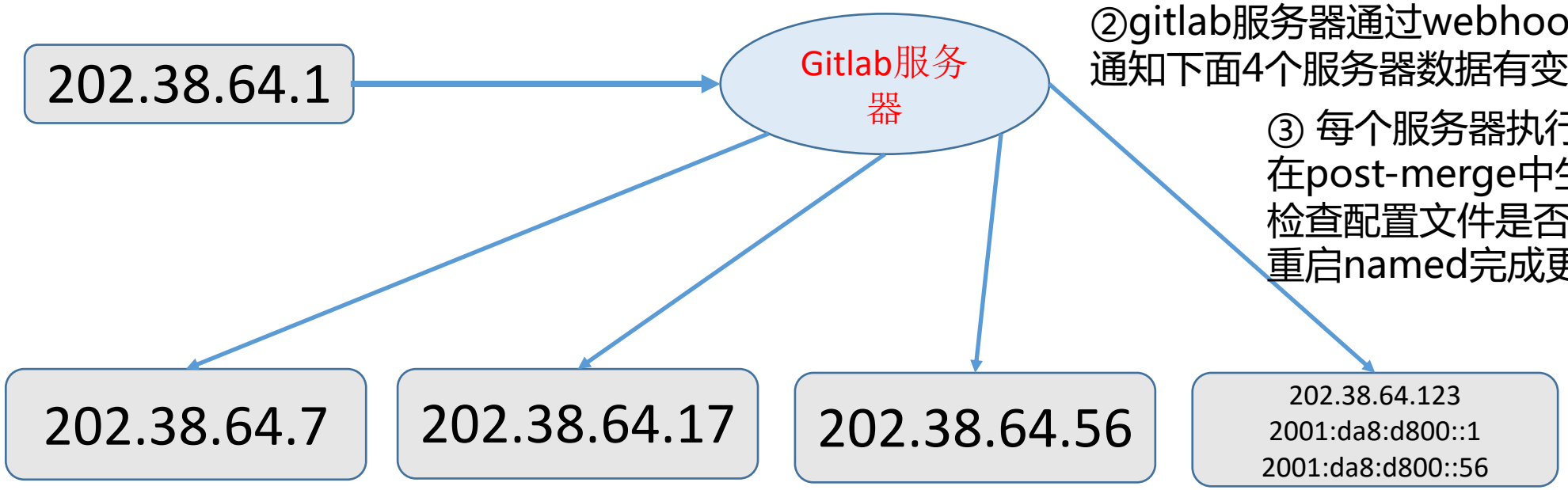
ustc.edu.cn DNS服务介绍

中国科大设置有5台DNS服务器，外加一个根镜像服务器
ustc.edu.cn域有多个view，传统的zone transfer方式无法工作
使用git来管理和同步配置文件

①文件修改后commit时
pre-commit中生成签名文件
检查配置文件是否正确
post-commit中重启named，并push到gitlab

②gitlab服务器通过webhook
通知下面4个服务器数据有变化

③ 每个服务器执行git pull
在post-merge中生成签名文件
检查配置文件是否正确
重启named完成更新



域名服务器的DNSSEC部署测试

https://dnssec-analyzer.verisignlabs.com/ustc.edu.cn

Domain Name: ustc.edu.cn

Analyzing DNSSEC problems for ustc.edu.cn

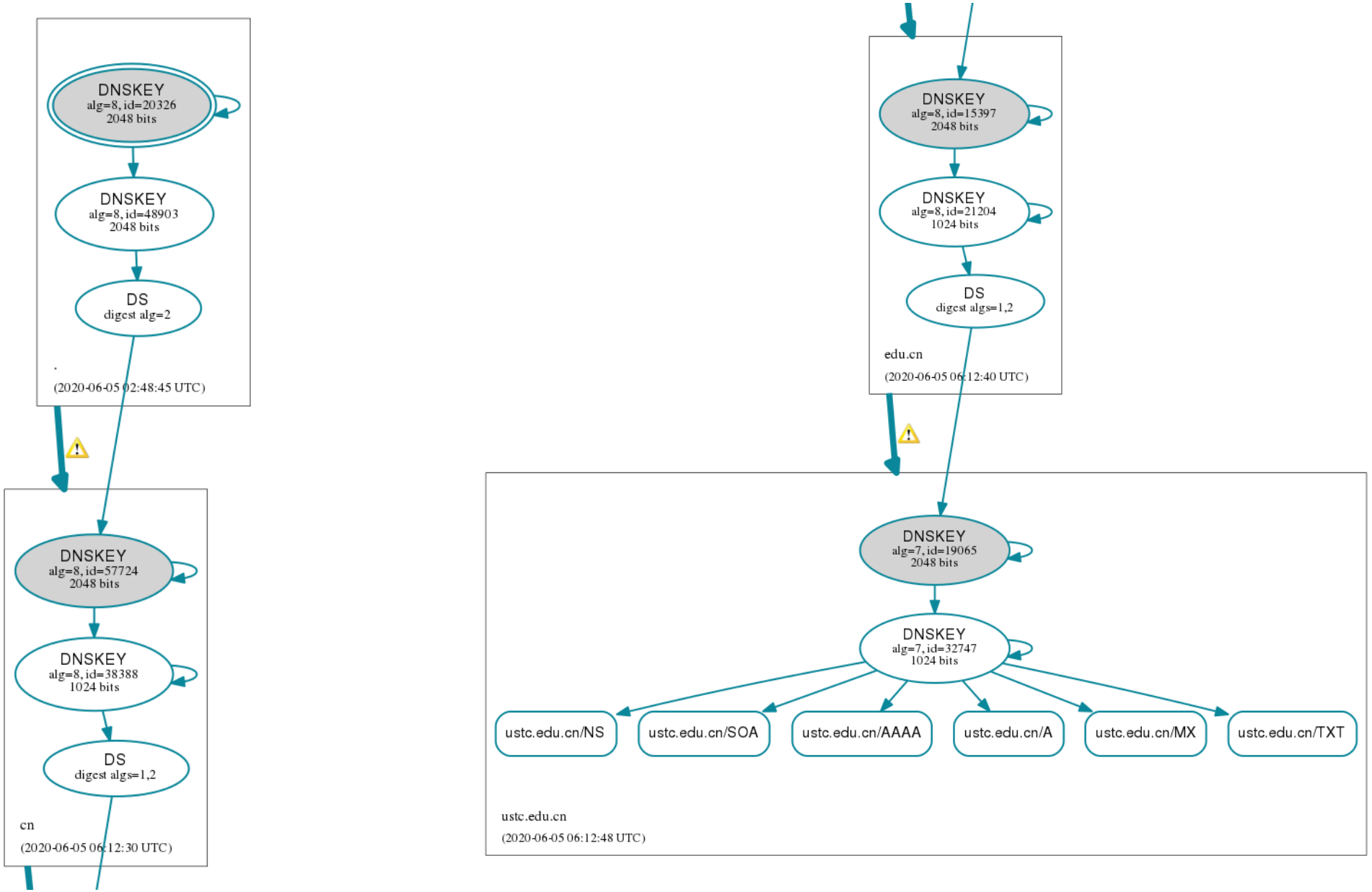
.	Found 2 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
cn	Found 1 DS records for cn in the . zone DS=57724/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=26116 and DNSKEY=26116 verifies the DS RRset Found 2 DNSKEY records for cn DS=57724/SHA-256 verifies DNSKEY=57724/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=38388 and DNSKEY=38388 verifies the DNSKEY RRset
edu.cn	Found 2 DS records for edu.cn in the cn zone DS=15397/SHA-1 has algorithm RSASHA256 DS=15397/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=38388 and DNSKEY=38388 verifies the DS RRset Found 2 DNSKEY records for edu.cn DS=15397/SHA-1 verifies DNSKEY=15397/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=15397 and DNSKEY=15397/SEP verifies the DNSKEY RRset
ustc.edu.cn	Found 1 DS records for ustc.edu.cn in the edu.cn zone DS=19065/SHA-256 has algorithm RSASHA1-NSEC3-SHA1 Found 1 RRSIGs over DS RRset RRSIG=21204 and DNSKEY=21204 verifies the DS RRset Found 2 DNSKEY records for ustc.edu.cn DS=19065/SHA-256 verifies DNSKEY=19065/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=19065 and DNSKEY=19065/SEP verifies the DNSKEY RRset ustc.edu.cn A RR has value 202.38.64.246 Found 1 RRSIGs over A RRset RRSIG=32747 and DNSKEY=32747 verifies the A RRset

Move your mouse over any ⊗ or ⚠ symbols for remediation hints.

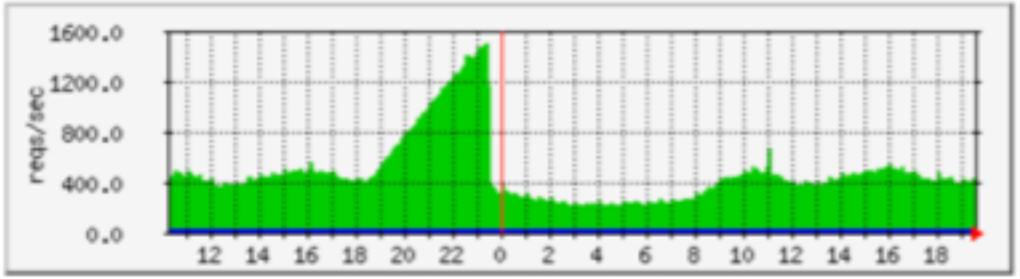
Want a second opinion? Test ustc.edu.cn at dnsviz.net.

域名服务器的DNSSEC部署测试

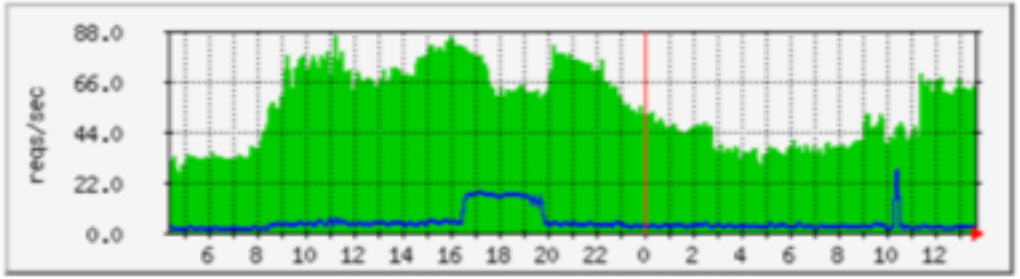
https://dnsviz.net/d/ustc.edu.cn/dnssec/



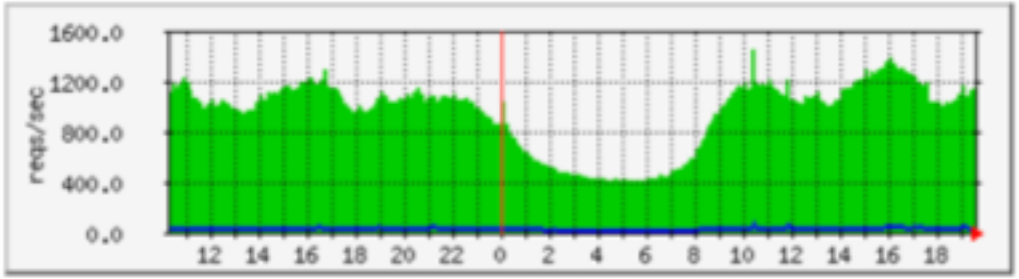
服务器的运行监测-查询统计和带宽统计



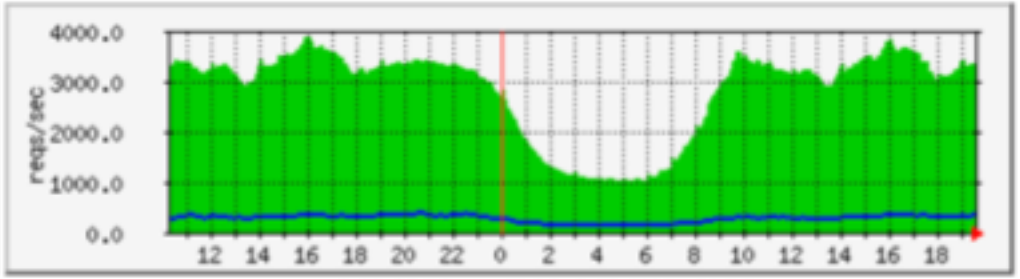
DNS查询统计 10分钟查询详细统计



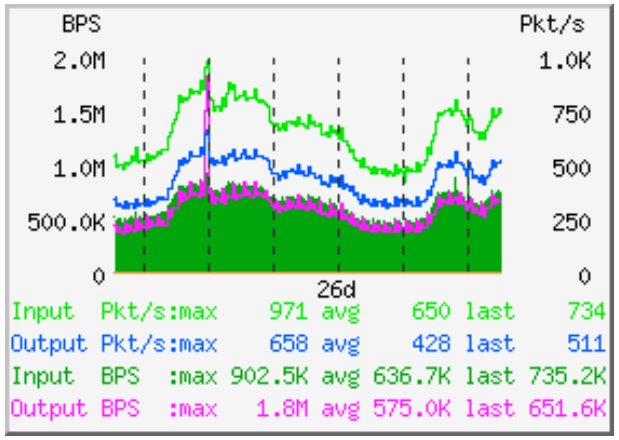
DNS查询统计 10分钟查询详细统计

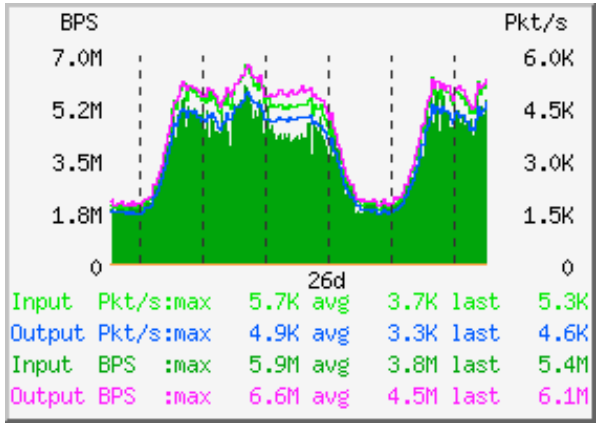


DNS查询统计 10分钟查询详细统计



DNS查询统计 10分钟查询详细统计





服务器的运行监测-查询统计

更多历史记录 更新时间：Tue Nov 24 19:30:02 CST 2020

各类型查询统计

A	147040
AAAA	70901
PTR	16671
TYPE65	5144
DNSKEY	1356
DS	825
MX	773
TXT	757
SPF	449
SRV	350

ClientIP排名

113.110.245.62	5686	608
222.195.93.75	5016	1757
202.38.75.150	4786	559
202.38.64.46	4611	666
202.38.87.87	4478	555
210.45.123.248	3852	1628
202.38.88.88	2560	1099
171.112.38.27	2256	326
219.137.230.36	1938	87
202.38.81.108	1890	756

MX类型查询统计

mail.ustc.edu.cn	271
ustc.edu.cn	190
ustc.edu	54
bbs.ustc.edu.cn	14
mail.ustc.edu	11
sent4promos.com	10
dawningw580i	8
cfa.ustc.edu.cn	8
cnbfp.cn	7
tbjdrfx.cn	6

ClientIP排名

202.38.64.46	173
47.100.6.242	8
202.127.204.32	8
99.80.34.120	6
3.248.186.18	6
202.38.95.62	6
31.13.115.140	5
31.13.115.138	5
139.99.128.97	5
99.80.34.123	4

A类型查询统计

liveupdate7.drivergenius.com	1874
mirrors.ustc.edu.cn	1823
www.baidu.com	1469
daisy.ubuntu.com	1469
test.vod05.icntvcdn.com.cdn.cnispgroup.com	1460
finder-res-test.meizu.com.m.alikunlun.com.mmycdn.cn	1452
teredo.ipv6.microsoft.com	1399
test.vod06.icntvcdn.com.mmycdn.com	1239

ClientIP排名

113.110.245.62	4623
222.195.93.75	4351
210.45.123.248	3460
202.38.75.150	2288
171.112.38.27	2216
202.38.64.46	2150
202.38.88.88	2143
202.38.87.87	1691

AAAA类型查询统计

ts.qq.com	4624
cu-cn-north00002.gala.convection.cn	1575
blackip.ustc.edu.cn	1079
api.miwifi.com	1049
daisy.ubuntu.com	916
ntp.ubuntu.com	905
mirrors.ustc.edu.cn	838
reputation.api.nsfocus.com	758

ClientIP排名

202.38.87.87	2512
202.38.75.150	2368
202.38.64.46	1399
210.45.64.20	1030
113.110.245.62	975
202.38.87.146	833
211.86.158.161	830
222.195.92.10	806

服务器的iptables规则

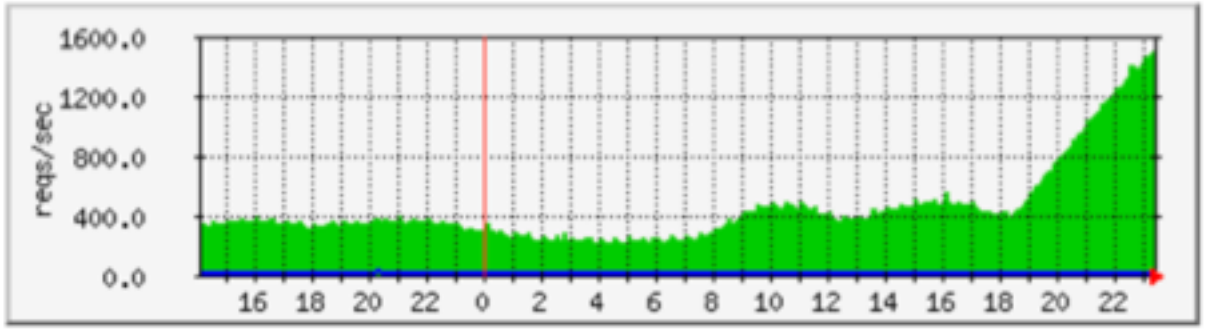
bind named软件对于非授权递归解析请求，会发送REFUSED应答响应
可以被用来做DDoS攻击
对这类应答响应做限速 对于202.38.64.1 2/3数据包，1/2流量可以丢弃

```
iptables -N refuseout
iptables -A refuseout -j ACCEPT -m limit --limit 10/sec
iptables -A refuseout -j DROP
iptables -A OUTPUT -m u32 -p udp --sport 53 --u32 "28&0xFFFF=0x8105" -j refuseout
iptables -A OUTPUT -m u32 -p udp --sport 53 --u32 "28&0xFFFF=0x8115" -j refuseout
```

有些明显异常的IP，可以直接过滤

异常的IP地址过滤

`Daily' Graph (5 Minute Average)



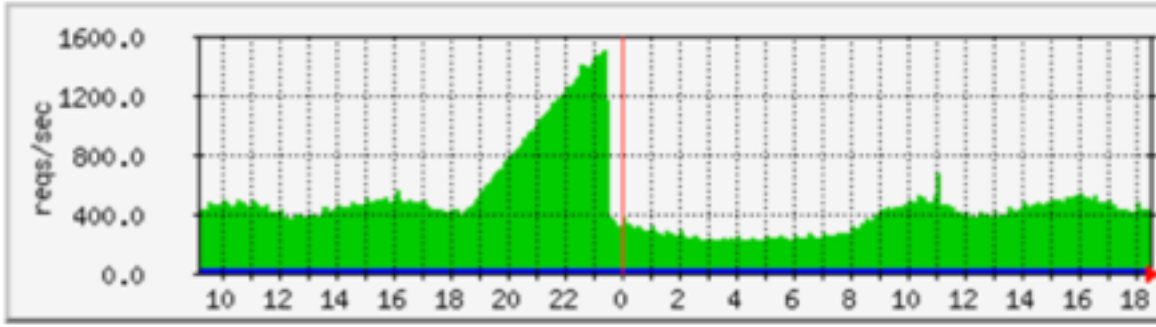
	Max	Average	Current
Requests:	1497.0 per sec	441.0 per sec	1498.0 per sec
Failures:	19.0 per sec	4.0 per sec	3.0 per sec

```
180.107.192.29#64192 (p2plive-ws.douyucdn.cn): view CHINANET:
180.107.192.29#64192 (p2plive-ws.douyucdn.cn): view CHINANET:
180.107.192.29#64192 (p2plive-ws.douyucdn.cn): view CHINANET:
180.107.192.29#64192 (p2plive-ws.douyucdn.cn): view CHINANET:
180.107.192.29#64192 (p2plive-ws.douyucdn.cn): view CHINANET:
180.107.192.29#64192 (p2plive-ws.douyucdn.cn): view CHINANET:
180.107.192.29#64192 (p2plive-ws.douyucdn.cn): view CHINANET:
180.107.192.29#64192 (p2plive-ws.douyucdn.cn): view CHINANET:
```

ClientIP排名

180.107.192.29	663709	9
219.137.230.36	5314	380
202.38.75.150	5156	605
211.86.158.7	4559	252
202.38.64.46	3834	615
202.38.87.87	2652	347
113.116.104.107	2539	312
222.195.93.75	2323	681
171.112.38.27	1896	217
211.86.158.38	1639	248

`Daily' Graph (5 Minute Average)



	Max	Average	Current
Requests:	1497.0 per sec	471.0 per sec	401.0 per sec
Failures:	5.0 per sec	3.0 per sec	3.0 per sec

简单的总结

DNS系统的IPv6和DNSSEC支持：未观察到带来负面影响

SPF、DKIM、DMARC：越来越多的邮件服务商开始支持

参考资料：

https://wiki.apnictraining.net/

https://github.com/bg6cq/ITTS

https://ipv6.ustc.edu.cn

http://ipv6c.cn/

谢谢！