第16卷 第8期
2006年8月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol.16 No.8
Aug. 2006

Linux环境下构建支持IPv6的DNS服务器

李润知，陈 刚，赵红领
（郑州大学 省信息网络重点开放实验室，河南 郑州 450052）

摘 要：全面系统介绍了IPv6环境下DNS服务器的搭建。对IPv6地址的特点及表示形式作了简单介绍，从几个方面详细介绍了DNS的工作原理，并对v4/v6环境下的DNS作了分析，详细说明了v6环境下的正向解析和反向解析过程，最后给出了Linux下IPv6 DNS配置过程中需要注意的问题及详细的配置实例。

关键词：Linux；IPv6；DNS；BIND
中图分类号：TP393.07 **文献标识码**：A **文章编号**：1673-629X(2006)08-0204-04

Configure DNS Server Supported IPv6 in Linux

LI Run-zhi, CHEN Gang, ZHAO Hong-ling
(Provincial Key Open Lab. on Information Network, Zhengzhou University, Zhengzhou 450052, China)

Abstract: Introduces the configuration of DNS Server in IPv6. At first, it explains the character and expression on IPv6 address. Secondly, it describes in detail the operation theory from several aspects and analyses DNS in IPv4/IPv6. This paper gives the process of lookup and reverse lookup. At last it gives the questions which need to pay attention and the configuration file in detail.

Key words: Linux; IPv6; DNS; BIND

0 引 言

随着IPv4地址的日趋减少，与IPv6发展相关的技术发展迅速。DNS全称Domain Name Space，透过DNS系统可以由一台机子的domain name查找其IP地址，也可以由IP地址查找其域名。在v4环境下域名解析系统给互联网用户带来极大便利，在v6环境下，地址由32位变成128位之后，DNS Server将如何工作，其和v4下DNS的工作方式有哪些不同，如何配置v6环境下的DNS，这些是需要重点解决的问题。

1 IPv6地址简介

v6地址和v4地址最本质的区别在于由原来的32位变为128位，其表示方法和v4也不同，归纳起来有4点：1)使用十六进制表示；2) 4位一组，中间用":"隔开；3)若以零开头可以省略，全零的组可用"::"表示；4)地址前缀长度用"/xx"来表示[1]。举例：0001:0123:0000:0000:0000:ABCD:0000:0001/96，1:123:0:0:0:ABCD:0:1/96，1:123::ABCD:0:1/96均正确表示了同一个v6地址。

IPv6地址的分类包括单播地址、组播地址和任播地址，其中单播地址根据地址范围又分为全局单播地址、链路本地地址及网点本地地址。其中，链路本地地址由设备自动生成，在本地网络中使用，其以11111111010开头，标识为FE80::/10；而网点本地地址则相当于v4网络中的私有地址，以11111111011开头，标识为FEC0::/10；全局单播地址在全局范围内使用，须进行层次划分及地址聚合，其分配方式如下：顶级地址聚合机构TLA(即大的ISP或地址管理机构)获得大块地址，负责给次级地址聚合机构NLA(中小规模ISP)分配地址，NLA给站点级地址聚合机构SLA(子网)和网络用户分配地址。IPv6地址的层次性在DNS中通过地址链技术可以得到很好的支持。

2 DNS工作原理

2.1 授权机制(delegation)

DNS采用分层管理机制，每个domain因实际需求再细分成许多sub domain，位于最顶端的是一个"root"，接下来是TLD(Top Level Domain)，TLD又分为gTLD及ccTLD；第二层网域名称SLD(Second Level Domain)；上层的domain可以将其分出的某个sub domain的domain name与IP mapping交由另一部机器管理，这个动作称之为授权。通过授权实现了整个Internet的域名管理系统[2~4]。

2.2 DNS的正解/反解机制

对于domain name和IP的映射可以看作是两个命名空间，其中，正解指的是domain name→IP的映射，举个例子来说，www.zzu.edu.cn→202.196.64.4指的是在代表zzu.edu.cn这个sub domain的机器上有一条记录为www→202.196.64.4。同理，反解指的是IP地址到domain

收稿日期：2006-02-23
作者简介：李润知(1978-)，女，河南洛阳人，博士研究生，研究方向为网络测量、网络管理。

name 的映射,在此命名空间中,所有的 IP 地址组成一个 in－addr. arpa 的 top domain,然后再根据 IP 层层划分。对 219. 243. 209. 79→ipv6. zzu. edu. cn 来说,表明在代表 209. 243. 219. in－addr. arpa 这个 sub domain 的机器上有一个记录表明 79→ipv6. zzu. edu. cn。如图 1 所示。

2.3 DNS 的查询机制

DNS 的查询通过执行 Name server 的软件,该软件位于记录正解/反解映射的机器上,通过 name server 的软件回应来自其它机器对域名或 IP address 的查询。

在 DNS 查询过程中,有一个起点,当一个 local DNS server 收到来自 client 端关于一个 domain name 的查询时,该 local DNS server 向 root name server 询问,root name server 记录了各 top domain 分别由哪些 DNS server 负责。举个例子,要找 www. zzu. edu. cn 时,root name server 会告诉 local DNS server 哪个 name server 负责. cn 这个 domain,然后 local DNS 再向负责. cn 的 name server 询问关于 edu. cn 是哪个 name server 在负责的,之后 local DNS 向负责 edu. cn 的 name server 询问 zzu. edu. cn 是由哪个 name server 负责的,最后,local DNS 就可以向负责 zzu. edu. cn 的 name server 问到有关 www. zzu. edu. cn 的资料。

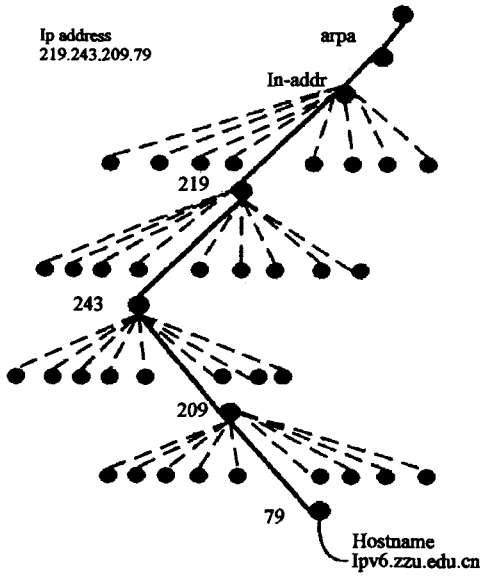

图 1　DNS 正/反解示意图

2.4 Recursive Query 和 Iterative Query

DNS client 发送一个询问给 local DNS server,之后 local DNS 就不断查询找到结果,回传给 client,这种查询成为 recursive query。其工作流程大致如图 2 所示。

另一种查询方式是 iterative query,指的是 local DNS server 向其它 DNS 发出的询问,都只是知道一个更进一步的线索,然后发问者(local DNS)根据线索再去进一步找到答案。

其工作原理如图 3 所示。

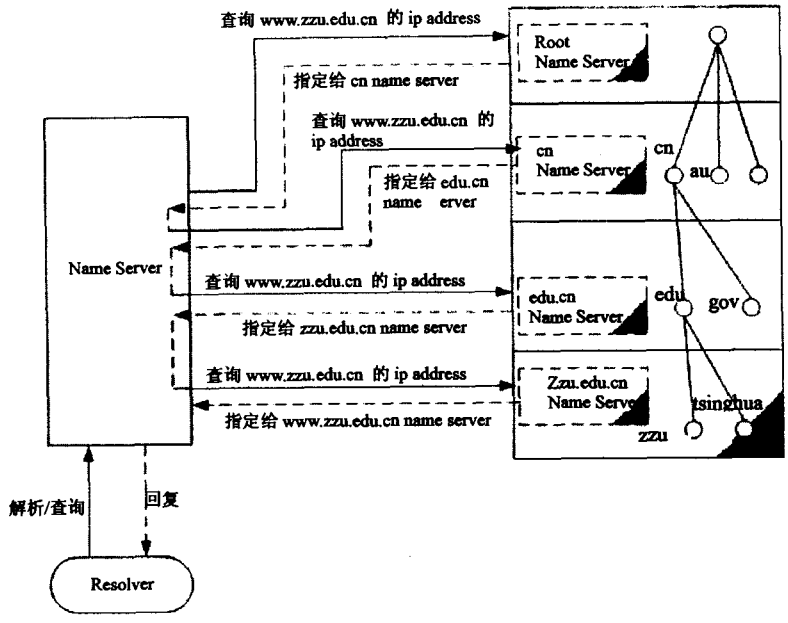

图 2　Recursive Query 流程图

name server A 收到解析器传来的查询指令,向 B 发出查询请求,B 将 A 指定给其它的 name server C,A 又向 C 发出查询指令,C 又指定 D,D 找到后把结果发送给 A,A 完成查询将结果传回给解析器。

总结来说,resolver 对 local DNS server 都是 recursive query,而 DNS server 之间的查询多是 interative query。一般 DNS server 可以接受 recursive 和 iterative 两种查询方式,但考虑到负载问题,root name server 只接受 iterative query。

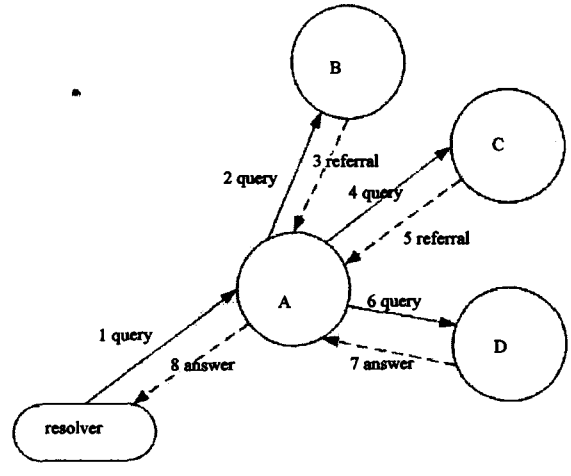

图 3　Iterative Query 流程示意图

2.5 DNS caching

一个查询的过程是,resolver 发出一个 query 给 local DNS,经过多次查询之后,local DNS 将结果返回给 resolver,为了节省反复查询的时间,DNS server 会把查询到的结果暂存一段时间,那么当有其它机器发出相同询问时,可以节省大量查询时间。在本地 local DNS server 存放查询的每步结果成为 DNS caching。

3 IPv4和IPv6 DNS比较

IPv4和IPv6网络中DNS在体系结构上是一致的,都采用树形结构的域名空间,实际上v4和v6共同拥有统一的域名空间,在IPv4到IPv6的过渡阶段,域名可以同时对应于多个IPv4和IPv6的地址。以后随着IPv6网络的普及,IPv6地址将逐渐取代IPv4地址。在处理正解和反解时二者有很大差别。

3.1 v6环境下DNS正向解析

IPv4的地址正向解析的资源记录是"A"记录。IPv6地址的正向解析目前有两种资源记录,即"AAAA"和"A6"记录。其中,"AAAA"是对"A"记录的简单扩展,用来表示域名和IPv6地址的对应关系,并不支持地址的层次性。"A6"在RFC2874中提出,它是把一个IPv6地址与多个"A6"记录建立联系,每个"A6"记录包含IPv6地址的一部分,结合后拼装成一个完整的IPv6地址。"A6"记录方式根据TLA,NLA和SLA的分配层次把128位的IPv6的地址分解成为若干级的地址前缀和地址后缀,构成了一个地址链。每个地址前缀和地址后缀都是地址链上的一环,一个完整的地址链就组成一个IPv6地址。这种思想符合IPv6地址的层次结构,从而支持地址聚合。另外,用户在改变ISP时,要随ISP改变而改变其拥有的IPv6地址。如果手工修改用户子网中所有在DNS中注册的地址,是一件非常繁琐的事情。而在用"A6"记录表示的地址链中,只要改变地址前缀对应的ISP名字即可,可以大大减少DNS中资源记录的修改。并且在地址分配层次中越靠近底层,所需要改动的越少。针对两种资源记录表示形式,分别举例如下:

a.使用"AAAA"来定义IPv6名字解析:

N AAAA 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0

N AAAA 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0

N AAAA 2345:000E:EB22:0001:1234:5678:9ABC:DEF0

b.使用"A6"形式:

N A6 64 ::1234:5678:9ABC:DEF0 SUBNET-1.IP6

SUBNET-1.IP6 A6 48 0:0:0:1:: IP6

IP6 A6 48 0::0 SUBSCRIBER-X.IP6.A.NET.

IP6 A6 48 0::0 SUBSCRIBER-X.IP6.B.NET.

SUBSCRIBER-X.IP6.A.NET. A6 40 0:0:0011::A.NET.IP6.C.NET.

SUBSCRIBER-X.IP6.A.NET. A6 40 0:0:0011::A.NET.IP6.D.NET.

SUBSCRIBER-X.IP6.B.NET. A6 40 0:0:0022::B-NET.IP6.E.NET.

A.NET.IP6.C.NET. A6 28 0:0001:CA00:: C.NET.ALPHA-TLA.ORG.

A.NET.IP6.D.NET. A6 28 0:0002:DA00:: D.NET.ALPHA-TLA.ORG.

B-NET.IP6.E.NET. A6 32 0:0:EB00:: E.NET.ALPHA-TLA.ORG.

C.NET.ALPHA-TLA.ORG. A6 0 2345:00C0::

D.NET.ALPHA-TLA.ORG. A6 0 2345:00D0::

E.NET.ALPHA-TLA.ORG. A6 0 2345:000E::

3.2 v6环境下DNS反向解析

IPv6反向解析的记录和IPv4一样,是"PTR",但地址表示形式有两种。一种是用"."分隔的半字节十六进制数字格式(Nibble Format),低位地址在前,高位地址在后,域后缀是"IP6.INT."。另一种是二进制串(Bit-string)格式,以"\<"开头,十六进制地址(无分隔符,高位在前,低位在后)居中,地址后加">",域后缀是"IP6.ARPA."。半字节十六进制数字格式与"AAAA"对应,是对IPv4的简单扩展。二进制串格式与"A6"记录对应,地址也象"A6"一样,可以分成多级地址链表示,每一级的授权用"DNAME"记录。和"A6"一样,二进制串格式也支持地址层次特性。

4 Linux下IPv6 DNS的配置

对DNS Server的工作原理有了一定的了解之后,举例来详细说明配置过程。

4.1 DNS Server软件的选取

在Linux主机上首先确定IPv6模块已启动,RedHat 9.0系统默认内核版本为2.4.20-8,已自带IPv6模块,只要在命令行下通过modprobe ipv6将其加载即可[5]。

Linux下搭建DNS Server的软件首选Bind,其有不同的版本,Window DNS是从Bind 4.x改进过来的,另外Bind8.x和Bind9.x从安全性及扩充性方面做了很多改进,为了实现对IPv6DNS的支持,采用Bind v9来实现,bind9.x提供IPv6 socket的DNS查询,支持IPv6资源记录。关于Bind9.x的详细特性建议到Bind的Web站点查阅,Bind的最新版本可以到www.isc.org/products/BIND/去下载。

4.2 IPv6 DNS的配置

Bind软件安装后,会产生几个固有文件,分为两类。一类是配置文件在/etc目录下,一类是DNS记录文件在/var/named目录下。加上其他相关文件,共同设置DNS服务器。named.conf为默认的主配置文件(须手动建立),设置一般的named参数,指向该服务器使用的域数据库信息的源,这类源可以是本地磁盘文件或远程服务器。

named.ca

指向根域名服务器

named.local

用于在本地转换回送地址

named.hosts

将主机名映射为IP地址

named. rev

用于反向域的、将 IP 地址映射到主机名的区文件

vi /etc/named. conf

配置举例如下:

```
vi /etc/named.conf
options {
directory"/var/named";
/*
If there is a firewall between you and nameservers you want
to talk to, you might need to uncomment the query-source
directive below. Previous versions of BIND always asked
questions using port 53, but BIND 8.1 uses an unprivileged
port by default.
*/
// query-source address * port 53;
};
controls {
  inet 127.0.0.1 allow {localhost;} keys {rndckey;};
};
zone"." IN {
  type hint;
  file"named.ca";
};
zone"localhost" IN {
  type master;
  file"localhost.zone";
  allow-update{none;};
};
zone"0.0.127.in-addr.arpa" IN {
  type master;
  file"named.local";
  allow-update{none;};
};
zone"zzu.edu.cn" IN {
  type master;
  file"zzu.edu.cn.zone";
  allow-update{none;};
};
zone"ipv6-addr.arpa" IN {
  type master;
  file"ipv6-addr.arpa.zone";
  allow-update{none;};
};
vi/var/named/zzu.edu.cn.zone
$TTL 86400
@ IN SOA ipv6.zzu.edu.cn. ljy.zzu.edu.cn. (
        2005070800 ; serial
        228800 ; refresh
        7200 ; retry
        604800 ; expiry
        86400 ) ; Minimum TTL
  IN NS ipv6.zzu.edu.cn.
  MX 10 main ; Primary Mail Exchanger
  MX 20 main1 ; Secondary Mail Exchanger
www IN AAAA 3ffe:321f:0000:07c2:0000:0000:0000:0000
ipv6 IN AAAA 3ffe:321f:0000:07c2:0000:0000:0000:0001
mail IN AAAA 3ffe:321f:0000:07c2:0000:0000:0000:0002
ftp IN AAAA 3ffe:321f:0000:07c2:0000:0000:0000:0003
bbs IN AAAA 3ffe:321f:0000:07c2:0000:0000:0000:0004
vi /var/named/ipv6-addr.arpa.zone
$TTL 86400
@ IN SOA ipv6.zzu.edu.cn. ljy.zzu.edu.cn. (
        2005070800 ; serial
        228800 ; refresh
        7200 ; retry
        604800 ; expire
        86400 )
@ IN NS ipv6.zzu.edu.cn.
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.c.7.0.0.0.0.f.1.2.
3.e.f.f.3 IN PTR www.zzu.edu.cn.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.c.7.0.0.0.0.f.1.2.
3.e.f.f.3 IN PTR ipv6.zzu.edu.cn.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.c.7.0.0.0.0.f.1.2.
3.e.f.f.3 IN PTR mail.zzu.edu.cn.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.c.7.0.0.0.0.f.1.2.
3.e.f.f.3 IN PTR ftp.zzu.edu.cn.
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.c.7.0.0.0.0.f.1.2.
3.e.f.f.3 IN PTR bbs.zzu.edu.cn.
```

4.3 测试 DNS

首先启动 DNS,在命令行方式输入/etc/rc. d/init. d/named restart, DNS 的测试可使用 nslookup 和 dig 工具,在相关的"DNS 协议"文章中有详细的测试例子,不再赘述。

5 总　结

从理论介绍到范例配置文档系统全面介绍了 IPv6 环境下 DNS 服务器的搭建。在对 IPv6 地址的特点及表示形式作了简单介绍之后,文章详细介绍了 DNS 的工作原理,其中展开分析了 DNS 的正/反解机制及两种查询方式 Recursive Query 和 Iterative Query 的工作流程。给出 DNS 理论介绍之后,对 v4/v6 环境下的 DNS 作了分析对比,详细说明了 v6 环境下的正向解析和反向解析过程,最后通过配置给出了 Linux 下 IPv6 DNS 配置过程中需要注意的问题及详细的配置实例。

参考文献:

[1] Hinden R, Deering S, IETF. RFC 2373, IP Version 6 Addressing Architecture[S]. www. ietf. org/rfc/rfc2373. txt, 1998-07.

[2] DONG Zhong-kai. DNS introduction[EB/OL]. http://turtle.ee.ncku.edu.tw/tung/dns/, 1999-05.

(下转第 230 页)

计算节点可靠性的同时还计算了节点的不可靠性,而且不可靠性要重要于可靠性,这也是现实模型中经常采用的方法。这种机制可以使得欺骗者受到严重的惩罚。同时由于可靠的节点不一定可信,因此采用这种体制可以避免某些恶意的节点积累很高的可靠性以后,转而对其他的可靠节点进行诽谤攻击的行为。目前的 BT 社区广泛地采用了这种模型。

关于 P2P 的信任管理还有其他的一些模型,比如 Abererand 和 Despotovic 等提出的 Complaint - based system,Kamvar 提出的 Eigen Trust Scheme 等模型。不管哪种信任模型,最终的目的是给出一个量化的节点信任值,P2P 的访问控制则依赖于节点的信任值。

4 基于信任域的访问控制

通过上述信任管理模型计算出每个节点的信任值,然后针对每个节点的信任值,采用相应访问控制策略,就可以实施对相应节点的访问控制了[7]。由于 RBAC 采用了策略和表达分开的思想,因此在 P2P 的网络中可以对所有节点根据信任值划分为若干个域,对于信任值和可靠性高的节点可以划分到比较高的信任域中,从而可以获得比较高的访问控制权限。针对可靠性和信任域,笔者定义一个信任域为 D。其模型可以简单表示为图 1。

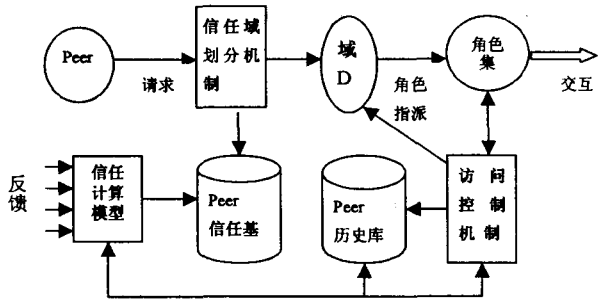

图 1 基于信任域划分的访问控制模型

信任模型可以是现有的成熟的信任管理模型,其对信任基的计算依赖于节点的历史记录系统反馈、名声和社区背景等因素,将计算的结果表示为信任基,供信任划分机制查询。信任域划分机制则通过信任基的查询,根据节点的查询结果,将节点划分到相应的信任域 D,而访问控制中的角色指派则可以将某一个信任域指派到角色集的一个角色上,从而实现从节点到角色的指派。

该模型的关键在于如何根据节点信任值和可靠性划分信任域,以及不同的信任域可以指派何种角色,计算模型的实施要通过相应的统计模型实现。

5 总 结

通过信任模型将复杂的 P2P 访问控制转换为对每个节点信任值的计算,简化了访问控制的实施,同时也可以利用现有的成熟访问控制模型来进行 P2P 的访问控制。目前关于 P2P 的信任管理正在进行深入研究,也有一些模型在类似在线交易的系统中使用。通过信任管理模型建立 P2P 的访问控制策略,是一种切实可行的方法。促进 P2P 环境下的应用健康正常的发展要有完善的技术,更重要的是如何通过信任管理建立良好的道德和信任体系。没有好的信任管理模型,必将使 P2P 成为谎言和欺骗的温床。

参考文献:

[1] Tran H, Hitchens M, Varadharaj V, et al. A Trust based Access Control Framework for P2P File - Sharing Systems[A]. Proceedings of the 38th Hawaii International Conference on System Sciences, 2005 [C]. Washington, DC, USA: IEEE Computer Society, 2005.

[2] Gupta R, Somani A K. Reputation Management Framework and Its Use as Currency in Large - Scale Peer - to - Peer Networks, p2p[A]. Fourth International Conference on Peer - to - Peer Computing (P2P'04)[C]. Washington, DC, USA: IEEE Computer Society, 2004. 124 - 132.

[3] Dewan P, Dasgupta P. Securing P2P Networks Using Peer Reputations: Is there a silver bullet? [A]. consumer communications & networking conferece[C]. Nevada, USA: CEA, 2005.

[4] Neil D, Garcia - Molina H, Beverly Y. Open problems in data - sharing peer - to - peer systems[A]. The 9th Int'l Conf on Database Theory (ICDT)[C]. Siena, Italy: [s. n.], 2003. 1 - 15.

[5] Li Xiong, Ling Liu. A Reputation - Based Trust Model for Peer - to - Peer eCommerce Communities[A]. 2003 IEEE International Conference on E - Commerce Technology (CEC'03)[C]. New York: IEEE Comput Soc, 2003. 275 - 286.

[6] Selcuk A A, Uzun E, Pariente M R. A Reputation - based Trust Management System for P2P Networks[A]. In: 4th IEEE/ACM International Symposium on Cluster Computing and the Grid[C]. Chicago, Illinois: [s. n.], 2004.

[7] 张书钦,芦东昕,杨永田. 对等网络中基于信任的访问控制研究[J]. 计算机科学,2005(5):31 - 33.

(上接第 207 页)

[3] Thomson S, Huitema C, IETF. RFC 1886, DNS Extensions to support IP version 6[S]. www. ietf. org/rfc/rfc1886. txt, 1995 - 12.

[4] Crawford M, Huitema C, IETF. RFC 2874, DNS Extensions to Support IPV6 Address Aggregation and Renumbering[S]. www. ietf. org/rfc/rfc2874. txt, 2000 - 07.

[5] WANG Ling - fang, ZHANG Yu, LI Ying - hua. Implementing Cisco IPV6 Networks[M]. Beijing: Posts & Telecom Press, 2003.