基于Bind与PAT实现校园网域名的智能解析*

孙光懿[1]，宋立巍[2]

(1. 天津音乐学院网络安全和信息化办公室，天津　300171；2. 天津市宁河区城乡居民基本医疗保险服务中心，天津　301500)

摘要：针对校外用户访问天津音乐学院校园网资源所存在的速度瓶颈问题，制定了在校园网中使用Bind9软件架设智能DNS服务器，以及在边界路由器中应用端口地址转换(PAT)技术的联合解决方案.文中介绍了DNS的工作原理，而且还给出了架设智能DNS服务器，以及在边界路由器中应用PAT技术的具体配置过程.测试结果证明，该解决方案可行、有效.实现了校园网域名的智能解析，校外用户可直接通过自身所在的网域对校园网资源进行高速访问.

关键词：Bind软件；端口地址转换；智能DNS

中图分类号：TP393.18　　**DOI**：10.19789/j.1004-9398.2021.02.003

0　引　言

为增加校园网出口带宽，高校常引入中国联通和中国电信等多条互联网运营商出口链路，此举虽然有助于提高校内用户访问互联网资源的速度，但是对于校外用户访问校园网资源来说，仍然存在速度瓶颈问题.为彻底解决这一问题，打破瓶颈，制定了在校园网中使用Bind9软件架设智能DNS服务器[1-5]，以及在边界路由器中应用端口地址转换(port address translation，PAT)技术的联合解决方案.选择使用Bind9软件架设智能DNS服务器，实现校园网域名的智能解析.其可根据不同网域用户的域名解析请求和预先制定的策略，将同一校园网域名解析为各网域所属的公网IP地址.基于就近访问原则，不仅可有效避免不同网络运营商之间的互访，而且还可实现多出口链路的负载分担.如：当中国联通用户访问校园网某个域名时，智能DNS服务器会将该域名解析为中国联通所属公网IP地址；当教育网用户访问校园网某个域名时，智能DNS服务器会将该域名解析为教育网所属公网IP地址；其余类似.在校园网边界路由器中应用PAT技术，是为了使各网域用户可通过访问自身所属的公网IP地址，实现对校园网资源的访问.

1　DNS的工作原理

为使计算机能对域名进行有效识别，工程师开发了一种可自动将域名翻译成IP地址的系统，该系统被命名为DNS[6-7].DNS是一种将域名和IP地址相互映射的分布式数据库.其工作职责就是对网络中的域名进行正向解析和逆向解析.通常DNS的工作过程如下：第一，当客户计算机发起域名解析请求时，操作系统会查询本地HOSTS文件是否存在该请求所对应的记录项，如果存在，则将查询结果直接返回给客户计算机，完成解析；第二，若不存在，需在本地DNS服务器的缓存中查询是否存在与该请求相对应的记录项，如果存在，那么就将查询结果直接返回给客户计算机，完成解析；第三，若仍不存在，那么本地DNS服务器就会把该请求发送到根域名服务器，根域名服务器收到请求后，会给本地DNS服务器返回一个所查询域的DNS服务器地址；第四，本地服务器会向根域名服务器返回的DNS服务器发送解析请求，然后在缓存中查询是否存在与该请求相对应的记录项，如果不存在，则再次返回一个所查询域的DNS服务器地址；第五，重复第四步的操作，直到查询到与请求相对应的记录项为止.

收稿日期：2020-05-08

* 天津市教委科研计划项目成果(2020SK096)

2　Bind概述

Bind软件作为当前使用最为广泛的免费智能域名解析软件,具有高安全性、遵循BSD许可证和支持(查询、IPV6、多链路负载均衡、区域传输及动态更新、多CPU和代码移植)等特点.该软件由Kevin在20世纪80年代初为伯克利的4.3版BSD Unix系统所开发的.经过多年的发展,现今的Bind不仅作为多数Unix系统的标准配置,而且还被各类Windows平台所使用.Bind通过将自身的view功能与访问控制列表技术相结合,对不同网域用户的同一域名解析请求时,可产生不同的解析结果.如当用户试图访问某个域名时,view会根据请求者的源IP地址与自身的IP地址库进行匹配,若匹配成功,则给匹配到的源IP使用不同特定的区域文件,因此,产生不同的解析结果.

3　实验仿真

天津音乐学院(简称"天音")校园网现为扁平化的大二层架构,其内部部署了1台高性能的思科路由器R1和1台思科6509的3层交换机SW1.整个校园网共有VLAN15(资源服务器区所在网段,IP地址范围211.68.15.1~211.68.15.254)、VLAN16(办公区所在网段,IP地址范围211.68.16.1~211.68.16.254)、VLAN17(宿舍区所在网段,IP地址范围211.68.17.1~211.68.17.254)和VLAN18(DNS服务器所在网段,IP地址范围211.68.18.1~211.68.18.254)4个网段,每个网段用户均使用中国教育科研网公网IP地址(各网段用户之间可以互联互通).校园网网络拓扑如图1所示.需要说明:(1)在路由器R1的f2/0接口处建有f2/0.1、f2/0.2、f2/0.3和f2/0.4这4个子接口(封装802.1Q协议),每个子接口的地址为所对应VLAN的网关地址;(2)S1、S2分别为WEB服务器和智能DNS服务器,C3、C4分别为校园网内用户终端计算机,C5、C6分别为中国联通和中国电信用户终端计算机;(3)校园网内网资源是以绝对URL的形式对外发布的.以主站域名(www.tjcm.edu.cn)为例,当教育网用户(包括校园网用户)访问时,无需在R1中进行端口地址转换,S2(IP地址211.68.18.11)会将其解析为教育网IP地址211.68.15.27.不仅有效避免了校园网多余流量的产生,而且还减轻了边界路由器的并发压力.当中国联通和中国电信等外网用户访问时,情况则略显复杂.智能DNS服务器会根据不同网域用户的解析请求和预先制定的策略,将其解析为各网域所属的公网IP地址.还需在R1中进行端口地址转换,将校园网内网服务器端口,映射到解析后的各网域所属公网地址端口,从而使各网域的用户可通过上述公网IP地址对主站域名进行访问.

相关网络设备接口及IP地址分配如表1所示.R1主要负责与引入的3条互联网运营商出口链路互联、NAT地址转换和数据处理等任务.其中,e0/0接口与中国教育科研网R2的e0/0接口互联,e0/1接口与中国联通R3的e0/1接口互联,e0/2接口与中国

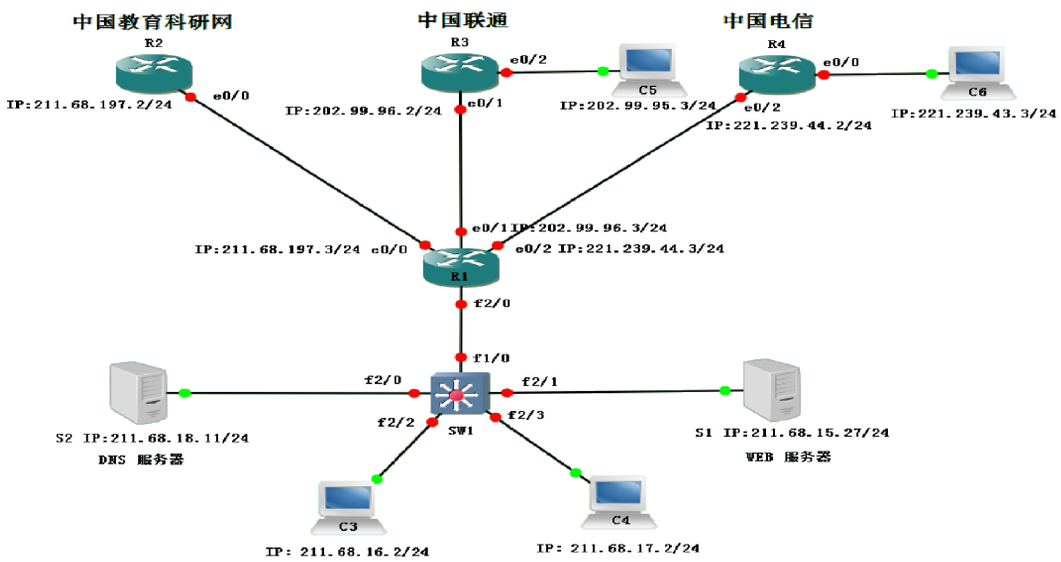

图1　天音校园网网络拓扑

注:R1~R4为路由器.

电信R4的e0/2接口互联.而3层交换机SW1则主要负责连接校园网服务器和用户终端计算机.子网掩码均为255.255.255.0.

表1 相关网络设备接口及IP地址分配

设备名称	接口	IP地址	网关地址
S1	SW1 f2/1	192.168.15.27	192.168.15.1
S2	SW1 f2/0	211.68.18.11	211.68.18.1
C3	SW2 f2/2	211.68.16.2	211.68.16.1
C4	SW2 f2/3	211.68.17.2	211.68.17.1
C5	R3 e0/2	202.99.95.3	202.99.95.1
C6	R3 e0/0	221.239.43.3	221.239.43.1
R1	e0/0	211.68.197.3	
	e0/1	202.99.96.3	
	e0/2	221.239.44.3	
	f2/0.1	192.168.15.1	
	f2/0.2	192.168.16.1	
	f2/0.3	192.168.17.1	
	f2/0.4	192.168.18.1	
R2	e0/0	211.68.197.2	
R3	e0/1	202.99.96.2	
	e0/2	202.99.95.1	
R4	e0/0	221.239.43.1	
	e0/2	221.239.44.2	

4 在校园网内架设智能DNS

4.1 下载并安装Bind软件

Bind软件可安装在Linux和Windows操作系统中.选择使用Windows Server 2016(标准版)操作系统作为架设智能DNS服务器的平台[8-12].首先,进入http://ftp.isc.org/isc/bind9/9.11.15/目录,下载名为"BIND9.11.15.x64.zip"的压缩包.需要注意的是:(1)为支持新版操作系统,尽量选择下载Bind 9.11以上的版本;(2)根据操作系统的位数,选择合适的Bind版本进行下载;(3)将下载后的Bind压缩包解压缩,以管理员身份运行"BindInstall.exe"文件;(4)为在程序安装过程中自动创建的"Name"账户设置密码,并使该账户对安装目录拥有绝对权限;(5)不要勾选"Start Bind Service After Install"选择框,如勾选,则程序安装后会自动启动Bind服务,届时会有错误提示出现.

4.2 配置Bind

4.2.1 生成rndc.key文件

Rndc(remote name domain controller)是Bind软件自带的一种可用于对域名服务进行远程管理的工具.在不影响DNS服务器工作的情况下,对其数据进行更新并保存生效.当使用Rndc与DNS服务器进行连接时,需要在其通信两端使用共享密钥进行数字证书的认证.通常在DOS窗口下,进入Bind安装目录下的bin子目录,运行rndc-confgen.exe -a命令后,可在Bind安装目录下的etc子目录中生成rndc.key文件,其为密钥文件.

4.2.2 创建rndc.conf文件

如果用户要使用Rndc,需在etc子目录中创建rndc.conf文件.与rndc.key文件不同,rndc.conf文件除了存放密钥信息外,还存放配置信息.其主要定义了要将控制消息发往的DNS服务器,及呈现给默认秘钥的名称.需要注意的是:该文件中key的名称和秘钥,必须与name.conf文件中定义的key名称和秘钥相一致.rndc.conf文件具体内容如下所示:

```
options{
default-key " rndc-key " ;#定义默认秘钥名称为rndc
-key
default-server 127.0.0.1;
default-port 953;#对953端口进行监听
};
key " rndc-key " {
algorithm hmac-md5;#定义秘钥的加密算法
secret " rndc-key==J98UKILOD " ;#定义秘钥的具体
内容
};
```

4.2.3 创建互联网运营商IP地址列表文件

为使Bind9的view功能能够正常工作,要在etc子目录中,分别创建中国教育科研网IP地址列表文件cernet.conf和中国联通IP地址列表unicom.conf.

4.2.4 创建区域数据文件

众所周知,IP地址127.0.0.1为本地回环地址,该地址不属于任何一种有类地址,通常用来将网络中的流量引向自己.由于互联网中的根名称服务器未将127.0.0.1映射到任何一个主机名,为了避免出现用户无法查询127.0.0.1的情况,有必要在etc子目录中,创建区域数据文件localhost.rev,以为该地址提供到主机名的映射.localhost.rev文件包含有用于明确该区域的权威(SOA)记录、用于明确该区域的名称服务器(NS)记录和IP地址到名称的映射(PTR)记录,相关具体内容如下所示:

```
$TTL 86400 #定义资源记录在cache中保留的时间
$ORIGIN 0.0.127.in-addr.appa.
```

```
@ IN SOA ns1.tjcm.edu.cn.sgy.tjcm.edu.cn.(
2007091701;Serial
30800;Refresh
7200;Retry
604800;Expire
300 );Minimum
IN  NS  ns1.tjcm.edu.cn.
1  IN PTR localhost.
```

说明:(1)如果名称服务器使用的是Bind8.2之前的版本,那么在SOA记录中就不应使用$TTL语句,名称服务器会认为存在语法错误,无法正确识别该语句;(2)文件第2行中的$ORIGIN设定,用于指定资源记录来自哪个区域(区域名一定要使用全域名称),如果不进行指定,资源记录的来源以主配置文件中ZONE定义的区域为准;(3)每个区域数据文件中只能有一个SOA记录;(4)文件第3行中的字符“@”用于引用当前区域名,在这里代表0.0.127.in-addr.appa.区域,字符“IN”代表记录类型为Internet类,在SOA后的第1个名称“ns1.tjcm.edu.cn.”为该域主名称服务器,第2个名称“sgy.tjcm.edu.cn.”为该区域负责人的电子邮件地址;(5)SOA记录“()”中的多数字段内容是提供给Slave名称服务器使用的,如Refresh字段内容定义了Slave名称服务器需间隔多久检查一次区域数据是否有更新,Retry字段内容定义了Slave名称服务器在更新时,若出现无法正常与主域名服务器进行连接的情况,需间隔多久再进行重新连接.

4.2.5 创建主配置文件

name.conf是Bind软件默认的主配置文件,主要负责指引名称服务器读取各区域数据文件.通常包含options、controls、view和zone语句.其中:options语句为名称服务器设置全局选项;controls语句决定名称服务器是如何对控制消息进行监控的;view语句使名称服务器可以根据来访者源IP地址的不同,区别回答DNS查询;zone语句定义DNS区域的选项.为使名称服务器正常工作,在etc子目录中,创建主配置文件name.conf.相关具体内容:

```
options {
directory " C:\Program Files\ISC BIND 9\etc";#指定名称服务器的工作目录
version none;#禁止查询名称服务器版本信息
recursion yes;#允许进行递归查询
allow-recursion{#允许所有主机进行递归查询
any;
};
allow-query{ #允许所有主机进行查询
any;
};
forwarders{#对于名称服务器无法查询的域名,将转发到以下DNS进行查询
202.99.96.68;
114.114.114.114;
  };
};
include " /etc/rndc.key "  #引入rndc.key文件
controls {
inet 127.0.0.1 port 953 #只在本地回环地址上对控制消息进行监听
allow {127.0.0.1;} keys { "rndc-key";};#只允许本机使用rndc对DNS服务器进行控制
};
```

当中国教育科研网用户对tjcm.edu.cn域中的资源记录进行查询时,名称服务器会选择读取区域数据文件cernet.zone.

```
include " cernet.conf " #引入中国教育科研网地址列表文件
view "cernet" {                #建立视图cernet
match-clients {cernet;};
#定义根域
zone "."in{#ROOT域配置
type hint;#类型为根名称服务器
file "name.root";#根DNS配置的文件名为name.root
};
#定义反向解析本地域
zone "0.0.127.in-addr.arpa"in {
type master;
file "localhost.rev";
allow-update {none;};
};
#定义域名为tjcm.edu.cn的正向解析区域
zone "tjcm.edu.cn"in {#tjcm.edu.cn域配置
    type master;
    file cernet.zone";
  allow-update {none;};
};
```

其他用户情况类似.需要说明:(1)如果在主配

置文件中出现多个options语句,那么只有第1个options语句有效;(2)当名称服务器启用转发功能时,必须先允许其进行递归查询;(3)如果在主配置文件中没有设置任何视图,那么Bind9会自动创建一个默认视图,并且任何向该名称服务器发送解析请求的主机都将看到该视图;(4)视图语句view一定要在options语句之后出现.

4.2.6 创建区域数据文件

创建区域数据文件cernet.zone、unicom.zone和tele.zone的主要目的是为tjcm.edu.cn域中的资源记录提供正向解析.上述3个区域数据文件中的SOA和NS资源记录均相同,唯一的区别就是主机www.tjcm.edu.cn的A资源记录各有不同.其中:在cernet.zone中,该主机的A资源记录为www IN A 211.68.15.27;在unicom.zone中,该主机的A资源记录为www IN A 202.99.96.3;在tele.zone中,该主机的A资源记录为wwwIN A 221.239.44.3.其文件cernet.zone的具体内容为:

```
$TTL 86400   #定义资源记录在cache中保留1 d的时间
tjcm.edu.cn. IN SOA ns1.tjcm.edu.cn.sgy.tjcm.edu.cn.(
2007091701;Serial
30800;Refresh
7200;Retry
604800;Expire
300 );Minimum
tjcm.edu.cn. IN NS ns1.tjcm.edu.cn.
localhost.tjcm.edu.cn IN A 127.0.0.1
ns1.tjcm.edu.cn. IN A 211.68.18.11
www.tjcm.edu.cn. IN A 211.68.15.27.
```

当中国教育科研网用户对该主机名进行访问时,名称服务器会将其解析为IP地址211.68.15.27.

从该文件可知:(1)tjcm.edu.cn域有只有1个名称服务器,并且该名称服务器运行在主机ns1.tjcm.edu.cn之上;(2)主机localhost.tjcm.edu.cn和www.tjcm.edu.cn分别被映射为IP地址127.0.0.1和211.68.15.27.

5 在路由器R1中设置PAT地址转换

PAT是一种常见的NAT转换方式,主要包括源和目的NAT[13-16].源NAT是对数据包的源地址进行修改,通常应用在2种情形下:(1)数据包的源地址为内部局部地址,需要将其转换为外部全局地址;(2)数据包源地址为外部全局地址,需要将其转换为外部局部地址.而源和目的NAT正好相反,是对数据包的目的地址进行修改,通常情形为:数据包的目的地址为内部全局地址,需要将其转换为内部局部地址.校园网R1中配置PAT地址转换的详细过程为

```
R1(config)#interface f2/0.1
R1(config-if)#ip nat inside  //定义内部接口
R1(config)#interface f2/0.2
R1(config-if)#ip nat inside
R1(config)#interface f2/0.3
R1(config-if)#ip nat inside
R1(config)#interface e0/0
R1(config-if)#ip nat outside//定义外部接口
R1(config)#interface e0/1
R1(config-if)#ip nat outside
R1(config)#interface e0/2
R1(config-if)#ip nat outside
R1(config)#access-list 1 permit host 202.99.96.3 //定义中国联通公网IP地址,中国联通用户可通过该地址访问主站域名.
R1(config)#access-list 2 permit host 221.239.44.3//定义中国电信公网IP地址,中国教育科研网和中国联通以外的其他互联网运营商用户,可通过该地址访问主站域名.
R1(config)#ip nat pool sgy211.68.15.27 211.68.15.27 255.255.255.0 //定义名为sgy的NAT地址池
R1(config)#ip nat inside destination list 1 pool sgy //对从外部进入的数据包的目的地址进行转换
R1(config)#ip nat inside destination list2 pool sgy
R1 (config) #ip nat inside source static tcp 211.68.15.27 80 202.99.96.3 80 //配置端口映射
R1 (config) #ip nat inside source static tcp 211.68.15.27 80 221.239.44.3 80.
```

6 启动ISC Bind服务

为确保架设的智能DNS服务器能够正常工作,还需启动ISC Bind服务.具体过程为:在DOS窗口下进入Bind软件安装目录,输入命令netstartnamed;如果用户想关闭ISCBind服务,那么输入命令netstopnamed.需要注意的是:用户也可在Windows系统服务中启动或关闭ISC Bind服务.

7　实验测试

以中国联通用户终端计算机C5为例(DNS地址设置为211.68.18.11),使用nslookup和ping命令对天音主站域名进行解析和连通性测试.使用网络测速软件测试其在智能DNS服务器部署前后,访问主站域名的网速,相关结果如表2所示.

表2　终端计算机C5在智能DNS服务器部署前后访问主站域名的网速对比

状态	延迟/ms	上行速率/(Mb·s^{-1})	下行速率/(Mb·s^{-1})
部署前	14.78	3.45	4.5
部署后	3.25	12.86	20.0

(1)使用nslookup命令对天音主站域名进行解析测试.

C5>nslookup

Default Server:ns1.tjcm.edu.cn

Address:211.68.18.11

>www.tjcm.edu.cn

Server:ns1.tjcm.edu.cn

Address:211.68.18.11

Name:www.tjcm.edu.cn

Address:202.99.96.3.

(2)使用ping命令对天音主站域名进行连通性测试.

C5>pingwww.tjcm.edu.cn.

正在 Ping www.tjcm.edu.cn[202.99.96.3] 具有32字节的数据:

来自 202.99.96.3 的回复:字节=32、时间=52 ms、TTL=50;

来自 202.99.96.3 的回复:字节=32、时间=51 ms、TTL=50.

(3)使用网络测速软件测试终端计算机C5访问天音主站域名的网速.

通过测试,智能DNS服务器部署后,不同网域的校外用户对主站域名进行访问时,不仅会得到不同的解析结果,而且访问速度也有了明显提升.

8　结束语

通过在天津音乐学院校园网中使用Bind9软件部署智能DNS服务器,并结合端口地址转换技术,不仅有效解决了校外用户访问校园网资源所存在的速度瓶颈问题,而且还提升了校园网的整体性能和效率.随着教育信息化的深入推进,相信智能DNS在校园网中会有更多的应用场景.如多出口链路的流量调度、业务系统负载均衡等,都可以通过智能DNS来实现.

参 考 文 献

[1] 李婕.企业DNS系统的设计与实现[D].北京:北京交通大学,2017.

[2] 王圣元,张宇,李东.DNS权威服务器选择方式研究[J].智能计算机与应用,2017,7(6):122-127.

[3] 张文佳.DNS根区解析自验证关键技术研究[D].哈尔滨:哈尔滨工业大学,2019.

[4] 侯冬青.智能DNS在多出口局域网中的应用研究[J].西昌学院学报(自然科学版),2015,29(1):49-52.

[5] 李程程.DNS系统功能优化与研究[D].北京:北京邮电大学,2014.

[6] 陈正权.多出口环境下校园网域名的智能解析[J].江苏师范大学学报(自然科学版),2012,30(3):31-34.

[7] 李浩.运营商网络中的DNS技术应用及性能优化[D].北京:北京邮电大学,2012.

[8] 张新刚,程新党,王保平,等.智能域名解析技术在多出口校园网资源加速访问中的应用[J].实验室研究与探索,2011,30(8):85-88+107.

[9] 孙光懿.基于GNS3的EIGRP路由设计与实现[J].首都师范大学学报(自然科学版),2019,40(2):16-23.

[10] 赵建勋.基于策略路由和BIND9的校园网快速访问研究[J].信息技术与网络安全,2019,38(5):58-61.

[11] 孙光懿.基于HSRP和STP协议的网络冗余仿真[J].首都师范大学学报(自然科学版),2018,39(3):16-23.

[12] 王圣元.DNS基础设施行为与性能的主动测量研究[D].哈尔滨:哈尔滨工业大学,2017.

[13] 张立成,彭勇华.一种智能DNS的设计与实现[J].计算机系统应用,2012,21(11):194-197.

[14] 丁传炜.基于Active Directory和Bind的域控分离系统的设计与实现[J].焦作大学学报,2015,29(4):80-82.

[15] 哈木拉提.新疆某公司域名系统优化与实现[D].厦门:厦门大学,2014.

[16] 孙光懿,孙光为.校园网网络改造实践研究[J].电脑知识与技术,2016,12(34):45-46+52.

Intelligent resolution of campus network domain name based on Bind and PAT

SUN Guangyi[1], SONG Liwei[2]

(1. Office of Network Security and Information, Tianjin Conservatory of Music, Tianjin 300171; 2. Tianjin Ninghe District Urban and Rural Residents Basic Medical Insurance Service Center, Tianjin 301500)

Abstract: In view of the speed bottleneck of users outside the school accessing the campus network resources of Tianjin Conservatory of Music, a joint solution of using Bind 9 software to set up an Intelligent DNS server in the campus network and port address translation technology in the border router is developed. This paper not only introduces the working principle of DNS in detail, but also gives the specific configuration process of setting up the intelligent DNS server and applying port address translation technology in border router. The test results show that the solution is feasible and effective. After the transformation, the campus network has realized the intelligent resolution of the domain name of the campus network. Users outside the school can directly access the campus network resources through their own domain at high speed.

Keywords: Bind softuare; port address translation; intelligent DNS

(责任编辑:马田田)