# 网络协议分析

# 实验报告

## 网络拓扑发现

吴致远 16041734

黄萍萍 16272203

叶艳雪 16272206

吕岩 16272227

2019 年 5 月

# 一.　实验要求

编程发现某个局域网的网络拓扑，即网络中所有主机和链路，及其相关状态信息（IP 地址、带宽、吞吐量等）。

# 二.　实验步骤

对于例如杭州电子科技大学校园网而言，其拓扑是非常复杂的。网络中存在着防火墙、NAT 等设备，对于我们而言需要使用多角度、多个方向来探索网络结构。

## (一). 基本信息收集

### 1. 公网方向

作为对外提供服务的校园网，其具有大量的公网资源，我们可以通过次来探寻网络拓扑。但在此之前，我们需要知道校园网的公网情况。

《杭州电子科技大学 2017-2018 学年本科教学质量报告》中的“校园信息化”章节是这样描述校园网的

> *学校校园网络建设采取学校自建自维方式，其中无线网络由学校与运营商共建，无线网络服务已覆盖全校区。教学行政区网络服务，由学校*网络信息中心*对师生统一提供；学生生活区网络服务，由*通信运营商*在获得经营权后向学生有偿提供。*

> *校园网的互联网接入带宽情况为，**联通 1.5G、电信 500M、移动 2.0G、教育网 100M**，校园网互联网接入总带宽为 4.1G。校园网目前拥有互联网 IPv4 地址数量近 2200 个，对外提供学校各级域名的权威域名解析服务。校园网已统一部署 IPv6，并在部分区域开展了基于 IPv6 的下一代互联网的研究与应用。*

通过这段文字，我们可以判定出三个信息：

1. 校园网为“教学行政区”。寝室内的网络由通信运营商提供，并不由网络数据中心负责。
2. 校园网接入了联通、电信、移动、教育网四大运营商。由此推测其有一定分流策略。
3. 校园网有 2200 个 IPv4 地址。另外据 2016-2017 年度的报告，校园网有 1 个/64 的 IPv6 地址。而/64 在 IPv6 地址分配建议（RFC7934）中，为单个主机分配的地址，因此在这里我们将其忽略。

对于公网地址，我们可以从 APNIC WHOIS、bgp.he.net 中查询到下列具有相关性的 IPv4 地址分配信息。

1. 电信

这里，我们以学校 Web 反代`218.75.123.181`为例查询。

IP Info | Whois | DNS | RBL

218.75.123.181 (www2.hziee.edu.cn)

| Announced By | | |
|---|---|---|
| **Origin AS** | **Announcement** | **Description** |
| AS4134 | 218.75.0.0/17 | CHINANET Zhejiang province network |
| AS4134 | 218.75.120.0/21 | |

Address has 0 hosts associated with it.

Updated 17 Apr 2019 20:19 PST © 2019 Hurricane Electric

由于分配给学校的 IP 范围小于/24，所以相关信息仅在 WHOIS 中得到了展示。

以 `HangZhou Electron`为关键词在 APNIC WHOIS 中进行查找

inetnum: 218.75.72.80 - 218.75.72.87
netname: HANGZHOU-ELECTRON-INSTITUTE
country: CN
descr: HangZhou Electron Industry Institute
mnt-irt: IRT-CHINANET-ZJ
status: ASSIGNED NON-PORTABLE
mnt-by: MAINT-CN-CHINANET-ZJ-HZ
last-modified: 2012-09-21T12:12:03Z
source: APNIC

inetnum: 218.75.123.160 - 218.75.123.191
netname: HANGZHOU-ELECTRON-COLLEGE
country: CN
descr: Hangzhou City Electron Technology College
status: ASSIGNED NON-PORTABLE
mnt-by: MAINT-CN-CHINANET-ZJ-HZ
last-modified: 2008-09-04T06:55:08Z
source: APNIC

inetnum: 60.191.32.64 - 60.191.32.95
netname: HANGZHOU-ELECTRON-UNIVERSITY

country: CN

descr: HangZhou Electron Technology University

status: ASSIGNED NON-PORTABLE

mnt-by: MAINT-CN-CHINANET-ZJ-HZ

last-modified: 2008-09-04T07:00:33Z

source: APNIC

2. 联通

这里，我们以学校 Web 反代`60.12.8.181`为例查询。


inetnum: 60.12.8.132 - 60.12.8.135

netname: HANGZHOUDIANZIKEJIDAXUEHZ

country: CN

descr: HANGZHOUDIANZIKEJIDAXUE,HANGZHOU,ZHEJIANG

status: ASSIGNED NON-PORTABLE

mnt-by: MAINT-CNCGROUP-ZJ

last-modified: 2010-09-08T16:10:15Z

source: APNIC

inetnum: 60.12.8.160 - 60.12.8.191

netname: HANGZHOUDIANZIKEJIDAXUEHZ

country: CN

descr: HANGZHOUDIANZIKEJIDAXUE,HANGZHOU,ZHEJIANG

status: ASSIGNED NON-PORTABLE

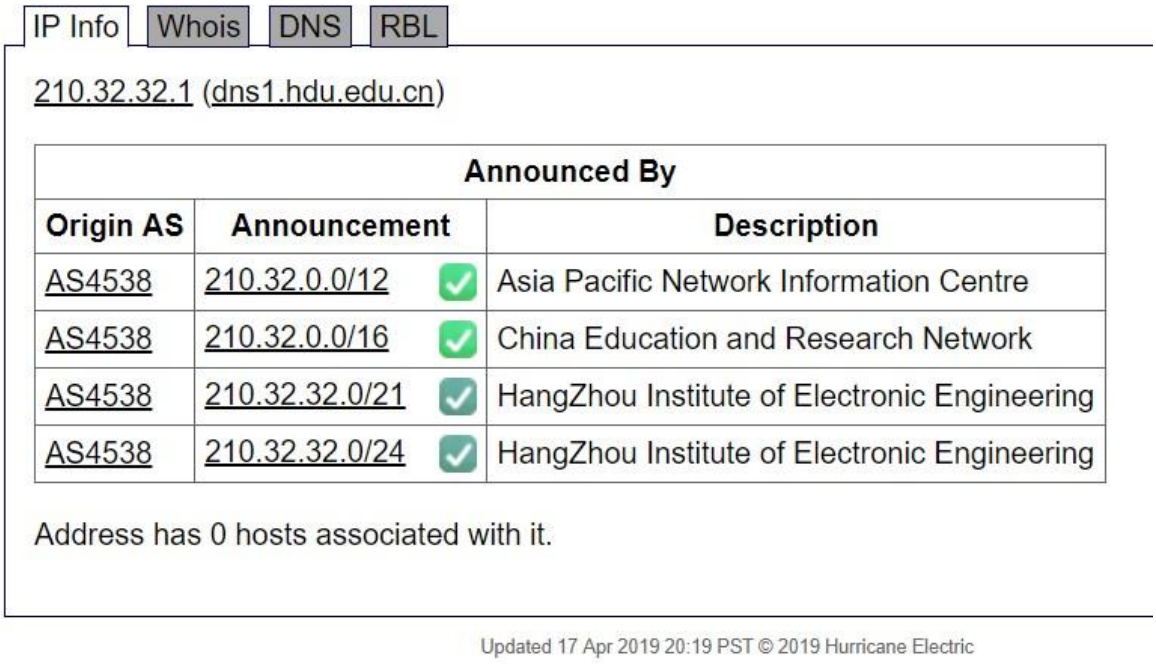
mnt-by: MAINT-CNCGROUP-ZJ

last-modified: 2010-09-08T16:10:15Z

source: APNIC

3. 教育网

这里，我们以学校 DNS 服务器`210.32.32.1`为例进行查询。




由图可知，`210.32.32.0/21`网段是分配给杭州电子工业学院（HangZhou Institute of Electronic Engineering）的。

inetnum: 210.32.32.0 - 210.32.39.255

netname: HZIEE-CN

descr: HangZhou Institute of Electronic Engineering

descr: Hangzhou, Zhejiang 310037, China

country: CN

remarks: origin AS4538

mnt-by: MAINT-CERNET-AP

status: ASSIGNED NON-PORTABLE

last-modified: 2008-09-04T06:49:25Z

source: APNIC

## 2. 内网方向

在校园网中，访问学校网站时，学校 DNS 会返回内网地址。由此，我们可以推测出校园网内网地址的一些情况。

- 公共服务

我们查询 www、i、cas、jwc、jxgl 等子域名的 IP。

大部分在 192.168.100.0 - 192.168.102.255 网段。

结合实际，许多学院的网站由`zhanqunfb.split.hdu.edu.cn.`（站群）提供服务，被集中托管于网络中心机房，故其 IP 相近。

- 内网服务

一些学院可能以内网 IP 形式存在的服务，我们尝试在学校网站上找到。

192.168.129.98 财务管理 http://cwgl.hdu.edu.cn

192.168.166.208 理学院重修

192.168.176.32 语言实验教学示范中心 http://wysfzx.hdu.edu.cn

192.168.177.12 7 教多功能厅

10.1.18.137 http://cloud.hdu.edu.cn

10.25.13.100 杭电 CTF http://sec.hdu.edu.cn

10.28.1.17 后勤证照系统

10.110.110.1 实验室安全监控

10.130.5.236 信工教务系统 http://jxgl.hziee.edu.cn

由上可知，校园网使用了 10.0.0.0/8 和 192.168.0.0/16 网段。

## (二). IP 可用性扫描

由于校园网内网网段过多，我们需要进一步缩小范围。由目前的校园网路由配置推断，校园网各网段网关一般设置为 x.x.x.254。因此，我们使用设备进行 ICMP 扫描，获取网段。

这里，我们使用 Bash 脚本进行编写。

```
#!/bin/bash
for ip in 192.168.{1..254}.254
do
        ping $ip -c 1 &> /dev/null
                if [ $? -eq 0 ];then
                        echo $ip is alive ....
                fi
done
```

- **IP 扫描结果见附录 1**

但通过 10.x.x.254 的 Ping，未能发现之前获取的“信工教务系统”。因此我们再尝试 Ping10.x.0.1 进行复核。

为了更好地了解 IP 情况，我们对学校教育网 IP 的 rDNS 信息进行扫描。

```
#!/bin/bash
for ip1 in {32..39}
do
for ip2 in {0..255}
do
        dig +time=1 +tries=1 +short PTR $ip2.$ip1.32.210.in-addr.arpa. @210.32.32.1  &>> /root/hdunet_test/dns.out
                if [ $? -eq 0 ];then
                        echo 210.32.$ip1.$ip2 is alive ....
                fi
done
done
```

由此可以获得 PTR 记录列表：

- **PTR 记录见附录 2**

其中，有如下记录值得注意：

ex8208.net.hziee.edu.cn. 210.32.39.250

fw-xiasha.net.hziee.edu.cn. 210.32.39.251

# (三)路由追踪

通过对 IP 的路由追踪，我们可以通过中间设备返回的 ICMP 报文，来知晓路径，从此推测出网络的结构。

在这里，我们使用 Linux 下的 MTR 程序来进行批量跟踪。其可以从文件读取 hosts，并以 JSON 形式输出，方便我们进行处理。

```
mtr -c 2 -j -F 10.txt > 10.mtr
```

执行完成后，我们获得了如下格式的 JSON 数据。其中的 hubs 中为我们需要的各跳数据。


```
{
  "report": {
    "mtr": {
      "src": "*****",
      "dst": "192.168.182.254",
      "tos": "0x0",
      "psize": "64",
      "bitpattern": "0x00",
      "tests": "2"
    },
    "hubs": [{
      "count": "1",
      "host": "???",
```

```
        "Loss%": 100.00,
        "Snt": 2,
        "Last": 0.00,
        "Avg": 0.00,
        "Best": 0.00,
        "Wrst": 0.00,
        "StDev": 0.00
      },
      {
        "count": "2",
        "host": "192.168.53.245",
        "Loss%": 0.00,
        "Snt": 2,
        "Last": 0.73,
        "Avg": 0.45,
        "Best": 0.16,
        "Wrst": 0.73,
        "StDev": 0.40
      },
      {
        "count": "3",
        "host": "192.168.182.254",
        "Loss%": 0.00,
        "Snt": 2,
        "Last": 2.13,
        "Avg": 2.03,
        "Best": 1.94,
        "Wrst": 2.13,
        "StDev": 0.14
      }]
    }
}
```


由于其输出的内容非标准 JSON，我们还需要将`}\n{`替换为`},\n{`，并在开头和结尾加上`[`和`]`以便进行处理。

## （四）分析数据

这里，我们使用 Node.js 执行 JavaScript 脚本，来分析数据。

```
const source = require('./data');
const mtr_10 = source.a
var mtr_10_dst = new Array();

a = 3
for (var i=0;i<mtr_10.length;i++)
{
    if (mtr_10[i].report.hubs[a-1])
    {
```

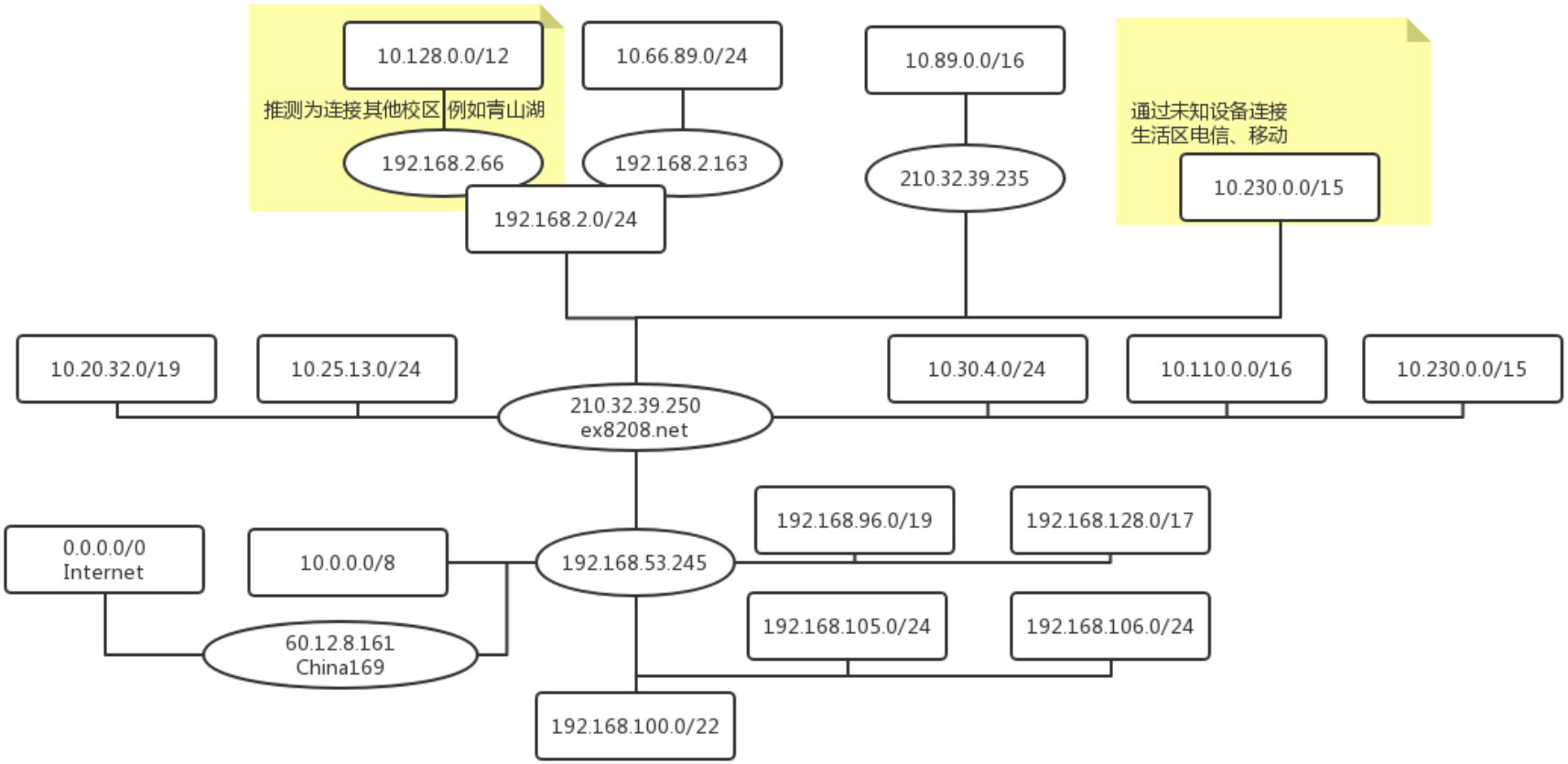
```
        if ((mtr_10[i].report.hubs[a-2].host ==
'???')&&(!mtr_10_dst.includes(mtr_10[i].report.hubs[a-1].host)))
        // if (!mtr_10_dst.includes(mtr_10[i].report.hubs[a-1].host))
        {
            mtr_10_dst.push(mtr_10[i].report.hubs[a-1].host);
            console.log(mtr_10[i].report.hubs[a-1].host);
        }
    }
}
```

通过这段代码，我们可以获取到各跳的 IP 列表，并对经过特定 IP 的路由进行进一步分析。

- 路由列表见附录

通过分析，我们发现，10.0.0.0/8 中大部分路由都通过 210.32.39.250 进行。而一些特定网段则通过了 210.32.39.250（ex8208.net.hziee.edu.cn）进行路由。ex8208 推测为 Juniper 的 EX8208 以太网交换机。

通过汇聚路由，我们绘制出了校园网推测网络拓扑图（见下页）。


10.128.0.0/12
推测为连接其他校区 例如青山湖
192.168.2.66
10.66.89.0/24
192.168.2.163
192.168.2.0/24
10.89.0.0/16
210.32.39.235
通过未知设备连接
生活区电信、移动
10.230.0.0/15
10.20.32.0/19
10.25.13.0/24
210.32.39.250
ex8208.net
10.30.4.0/24
10.110.0.0/16
10.230.0.0/15
0.0.0.0/0
Internet
10.0.0.0/8
60.12.8.161
China169
192.168.53.245
192.168.96.0/19
192.168.128.0/17
192.168.105.0/24
192.168.106.0/24
192.168.100.0/22

# 三. 实验结论

通过这次实验，我们使用 ICMP 进行了校园网的拓扑发现，推测出了校园网的网络拓扑结构。

但由于时间和条件的限制，实验数据还有进一步打磨的空间。例如 210.32.39.241（xzl-nic.net.hziee.edu.cn，行政楼）、210.32.39.245（sy3n-nic.net.hziee.edu.cn，第三实验楼南楼）等 PTR 记录中存在的 IP 并未被我们追踪到。

# 附录 1　IP 扫描结果

- 192.168.0.0/16

```
192.168.2.254
192.168.95.254
192.168.96.254
192.168.97.254
192.168.98.254
192.168.99.254
192.168.100.254
192.168.101.254
192.168.102.254
192.168.103.254
192.168.104.254
192.168.105.254
192.168.112.254
192.168.120.254
192.168.121.254
192.168.122.254
192.168.123.254
192.168.124.254
192.168.125.254
192.168.126.254
192.168.127.254
192.168.128.254
192.168.129.254
192.168.130.254
192.168.131.254
192.168.132.254
192.168.133.254
192.168.134.254
192.168.135.254
192.168.136.254
192.168.138.254
192.168.142.254
192.168.143.254
192.168.144.254
192.168.145.254
192.168.146.254
192.168.148.254
192.168.149.254
192.168.150.254
192.168.151.254
192.168.152.254
192.168.156.254
192.168.157.254
192.168.158.254
192.168.159.254
192.168.161.254
192.168.162.254
192.168.164.254
192.168.165.254
192.168.166.254
192.168.167.254
192.168.168.254
192.168.169.254
192.168.170.254
192.168.171.254
192.168.172.254
192.168.173.254
192.168.174.254
192.168.175.254
192.168.176.254
192.168.177.254
192.168.178.254
192.168.179.254
192.168.180.254
192.168.181.254
192.168.182.254
192.168.183.254
192.168.184.254
192.168.185.254
192.168.188.254
192.168.189.254
```

```
192.168.190.254
192.168.191.254
192.168.192.254
192.168.194.254
192.168.195.254
192.168.196.254
192.168.197.254
192.168.202.254
192.168.210.254
192.168.211.254
192.168.212.254
192.168.213.254
192.168.214.254
192.168.215.254
192.168.216.254
192.168.217.254
192.168.219.254
```

- 10.0.0.0/8

```
10.0.0.1
10.1.0.1
10.1.13.254
10.1.15.254
10.1.16.254
10.1.17.254
10.1.18.254
10.1.19.254
10.1.20.254
10.1.21.254
10.1.31.254
10.1.130.254
10.1.131.254
10.1.132.254
10.1.133.254
10.1.150.254
10.2.0.1
10.2.10.254
10.2.11.254
10.2.12.254
10.2.13.254
10.2.14.254
10.2.15.254
10.2.16.254
10.2.17.254
10.2.18.254
10.2.19.254
10.2.20.254
10.3.0.1
10.3.10.254
10.3.12.254
10.3.16.254
10.3.19.254
10.3.21.254
10.3.41.254
10.3.42.254
10.3.48.254
10.3.49.254
10.3.63.254
10.6.0.1
10.6.10.254
10.6.11.254
10.6.12.254
10.6.128.254
10.7.0.1
10.7.1.254
10.8.0.1
10.8.1.254
10.8.2.254
10.8.10.254
10.9.0.1
10.9.10.254
10.9.11.254
10.9.12.254
10.10.0.1
10.10.10.254
10.10.11.254
10.10.12.254
10.10.16.254
10.18.0.1
```

10.18.1.254
10.18.5.254
10.18.10.254
10.20.0.1
10.20.1.254
10.20.17.254
10.20.20.254
10.20.24.254
10.20.32.254
10.20.33.254
10.20.34.254
10.20.35.254
10.20.36.254
10.20.37.254
10.20.38.254
10.21.0.1
10.21.10.254
10.21.11.254
10.21.12.254
10.21.13.254
10.21.14.254
10.21.15.254
10.21.16.254
10.21.17.254
10.22.0.1
10.22.10.254
10.22.11.254
10.22.12.254
10.22.13.254
10.22.14.254
10.23.2.254
10.23.3.254
10.23.5.254
10.23.6.254
10.23.10.254
10.23.11.254
10.23.12.254
10.23.13.254
10.23.64.254
10.24.0.1
10.24.1.254
10.24.7.254
10.25.0.1
10.25.1.254
10.25.3.254
10.25.4.254
10.25.8.254
10.25.9.254
10.25.10.254
10.25.11.254
10.25.12.254
10.25.13.254
10.25.99.254
10.26.0.1
10.26.1.254
10.26.2.254
10.28.0.1
10.28.1.254
10.28.2.254
10.28.12.254
10.28.15.254
10.28.16.254
10.28.18.254
10.29.0.1
10.29.10.254
10.30.1.254
10.30.2.254
10.30.3.254
10.30.4.254
10.34.0.254
10.60.0.1
10.60.1.254
10.61.0.254
10.61.1.254
10.61.2.254
10.61.4.254
10.61.6.254
10.61.7.254
10.61.16.254
10.62.0.254
10.62.1.254

```
10.63.0.254
10.63.1.254
10.63.2.254
10.63.3.254
10.63.4.254
10.63.5.254
10.63.6.254
10.63.7.254
10.63.8.254
10.63.9.254
10.63.10.254
10.63.11.254
10.63.12.254
10.63.15.254
10.63.100.254
10.63.101.254
10.63.110.254
10.63.206.254
10.65.0.1
10.65.1.254
10.65.3.254
10.65.4.254
10.65.5.254
10.65.6.254
10.65.7.254
10.66.0.1
10.66.3.254
10.66.5.254
10.66.7.254
10.66.9.254
10.66.11.254
10.66.13.254
10.66.15.254
10.66.17.254
10.66.19.254
10.66.21.254
10.66.23.254
10.66.25.254
10.66.27.254
10.66.29.254
10.66.31.254
10.66.33.254
10.66.35.254
10.66.37.254
10.66.39.254
10.66.41.254
10.66.43.254
10.66.45.254
10.66.47.254
10.66.49.254
10.66.89.254
10.89.1.254
10.89.2.254
10.89.127.254
10.110.0.1
10.110.0.254
10.128.0.1
10.129.0.1
10.130.0.1
10.131.0.1
10.140.0.1
10.143.0.1
10.230.0.1
10.231.0.1
```

# 附录 2　PTR 记录

```
210.32.32.1   dns1.hdu.edu.cn
210.32.32.2   proxy.hziee.edu.cn
210.32.32.3   aaa.hziee.edu.cn
210.32.32.6   ftp.hziee.edu.cn
210.32.32.7   windowsupdate.hziee.edu.cn
210.32.32.8   mx.hdu.edu.cn
210.32.32.9   bbs.hziee.edu.cn
210.32.32.10  dns2.hdu.edu.cn
210.32.32.11  vod.hziee.edu.cn
```

```
210.32.32.12  www.taotian.com
210.32.32.14  stu.hziee.edu.cn
210.32.32.18  smtp1.hdu.edu.cn
210.32.32.28  mail.hdu.edu.cn
210.32.32.32  nat-for-cernet.net.hziee.edu.cn
210.32.32.33  nat2-for-cernet.net.hziee.edu.cn
210.32.32.69  test.hziee.edu.cn
210.32.32.100 master.hziee.edu.cn
210.32.32.250 ex8208.hziee.edu.cn
210.32.32.254 gw-cernet.hziee.edu.cn
210.32.33.155 er.lib.hdu.edu.cn
210.32.33.200 lib.hziee.edu.cn
210.32.33.210 ftp.lib.hziee.edu.cn
210.32.33.220 mail.lib.hziee.edu.cn
210.32.34.34  nat4-for-cernet.net.hziee.edu.cn
210.32.34.116 cloud.hdu.edu.cn
210.32.39.0   network-for-lib.net.hziee.edu.cn
210.32.39.14  gateway-for-lib.net.hziee.edu.cn
210.32.39.15  broadcast-for-lib.net.hziee.edu.cn
210.32.39.16  network-for-se.net.hziee.edu.cn
210.32.39.22  gateway-for-se.net.hziee.edu.cn
210.32.39.23  broadcast-for-se.net.hziee.edu.cn
210.32.39.24  network-for-cs.net.hziee.edu.cn
210.32.39.30  gateway-for-cs.net.hziee.edu.cn
210.32.39.31  broadcast-for-cs.net.hziee.edu.cn
210.32.39.32  network-for-xj.net.hziee.edu.cn
210.32.39.38  gateway-for-xj.net.hziee.edu.cn
210.32.39.39  broadcast-for-xj.net.hziee.edu.cn
210.32.39.189 lib-nic.net.hziee.edu.cn
210.32.39.190 nic-lib.net.hziee.edu.cn
210.32.39.194 lib.net.hziee.edu.cn
210.32.39.197 nic-dmz-2.net.hziee.edu.cn
210.32.39.198 lib-dmz-2.net.hziee.edu.cn
210.32.39.208 xdjx-lib.net.hziee.edu.cn
210.32.39.209 xzl-lib.net.hziee.edu.cn
210.32.39.210 sy2n-lib.net.hziee.edu.cn
210.32.39.211 sy2z-lib.net.hziee.edu.cn
210.32.39.212 sy2b-lib.net.hziee.edu.cn
210.32.39.213 sy3n-lib.net.hziee.edu.cn
210.32.39.214 sy3b-lib.net.hziee.edu.cn
210.32.39.215 sy4-lib.net.hziee.edu.cn
210.32.39.216 sy5-lib.net.hziee.edu.cn
210.32.39.217 jx5n-lib.net.hziee.edu.cn
210.32.39.225 nic.net.hziee.edu.cn
210.32.39.227 nic-cernet.net.hziee.edu.cn
210.32.39.228 nic-chinanet.net.hziee.edu.cn
210.32.39.229 lib-chinanet.net.hziee.edu.cn
210.32.39.230 nic-dmz-1.net.hziee.edu.cn
210.32.39.231 lib-dmz-1.net.hziee.edu.cn
210.32.39.232 borderline.net.hdu.edu.cn
210.32.39.240 xdjx-nic.net.hziee.edu.cn
210.32.39.241 xzl-nic.net.hziee.edu.cn
210.32.39.242 sy2n-nic.net.hziee.edu.cn
210.32.39.243 sy2z-nic.net.hziee.edu.cn
210.32.39.244 sy2b-nic.net.hziee.edu.cn
210.32.39.245 sy3n-nic.net.hziee.edu.cn
210.32.39.246 sy3b-nic.net.hziee.edu.cn
210.32.39.247 sy4-nic.net.hziee.edu.cn
210.32.39.248 sy5-nic.net.hziee.edu.cn
210.32.39.249 jx5n-nic.net.hziee.edu.cn
210.32.39.250 ex8208.net.hziee.edu.cn
210.32.39.251 fw-xiasha.net.hziee.edu.cn
210.32.39.252 fw-wenyi.net.hziee.edu.cn
210.32.39.253 gateway.hziee.edu.cn.32.210.in-addr.arpa
210.32.39.254 fw-xiasha-cnc.net.hziee.edu.cn
```