3019207417-李欣然-第二章作业

Section 2.1

R1：List five nonproprietary Internet applications and the application-layer protocols that they use.

A：

Internet applications	application-layer protocols
电子邮件系统应用	SMTP
Web应用	HTTP
P2P应用，如Torrent	P2P协议，如BitTorrent
Internet目录服务DNS	DNS协议
文件传输	FTP

R5：What information is used by a process running on one host to identify a process running on another host?

A：通过IP地址标识目标主机，再通过目标主机上的目的地端口号来标识进程。

Section 2.2

R11：Why do HTTP, SMTP, and IMAP run on top of TCP rather than on UDP?

A：首先TCP相比于UDP有以下优点：保证数据传输的完整性，保证数据有序到达，面向连接，有拥塞控制功能。

邮件协议SMTP和IMAP需要保证邮件数据的完整性和有序性（邮件可以作为法律凭证）；HTTP需要确保用户在通过浏览器向服务器发送请求时服务器接收到的请求是完整的、格式与发送请求一致的，否则服务器无法做出正确的响应。可以看出这些协议的需求只有TCP能够满足。

P7：Suppose within your Web browser you click on a link to obtain a Web page. The IP address for the associated URL is not cached in your local host, so a DNS lookup is necessary to obtain the IP address. Suppose that *n* DNS servers are visited before your host receives the IP address from DNS; the successive visits incur an RTT of $RTT_1, \ldots, RTT_n$. Further suppose that the Web page associated with the link contains exactly one object, consisting of a small amount of HTML text. Let RTT_0 denote the RTT between the local host and the server containing the object. Assuming zero transmission time of the object, how much time elapses from when the client clicks on the link until the client receives the object?

A：客户端经过DNS查找到包含所请求网页的服务器的ip地址的时间为：

$$RTT_1 + PTT_2 + \ldots + RTT_n$$

获取地址后，需要RTT_0时间建立TCP连接，此外还需RTT_0时间进行文件请求和答复，所以总时长为$2 * RTT_0 + RTT_1 + PTT_2 + \ldots + RTT_n$

P8：Referring to Problem P7, suppose the HTML file references eight very small objects on the same server. Neglecting transmission times, how much time elapses with

a. Non-persistent HTTP with no parallel TCP connections?

HTML文件和每个目标之间都需要建立TCP连接和请求文件传输，因此需要在P7的基础上加上$8*2RTT_0$

$$2*RTT_0+RTT_1+PTT_2+...+RTT_n+8*2RTT_0=18*RTT_0+RTT_1+PTT_2+...+RTT_n$$

b. Non-persistent HTTP with the browser configured for 6 parallel connections?

HTML文件传到客户端后，包含的8个目标可以并行传输，总时间为：

$$2*RTT_0+RTT_1+PTT_2+...+RTT_n+2*2RTT_0=6*RTT_0+RTT_1+PTT_2+...+RTT_n$$

c. Persistent HTTP?

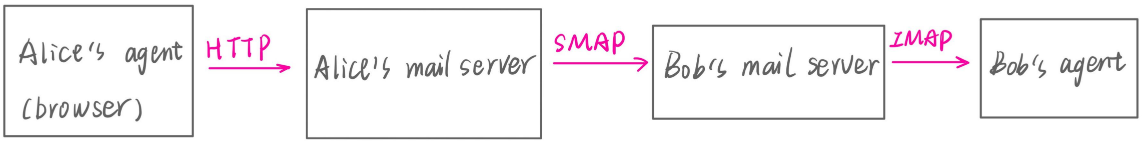
A：持久HTTP连接可以处理多个请求，因此8个目标的请求可以在一个RTT_0内完成，总时间为：

$$2*RTT_0+RTT_1+PTT_2+...+RTT_n+RTT_0=3*RTT_0+RTT_1+PTT_2+...+RTT_n$$

Section 2.3

R16：Suppose Alice, with a Web-based e-mail account (such as Hotmail or Gmail), sends a message to Bob, who accesses his mail from his mail server using IMAP. Discuss how the message gets from Alice's host to Bob's host. Be sure to list the series of application-layer protocols that are used to move the message between the two hosts.

A：如图：



Section 2.4

P18：a. What is a *whois* database?

A：whois数据库可以根据给定的域名或IP地址查询域名信息，也可以用于查询存储注册用户或 Internet 资源（例如 IP 地址、自治系统编号 (ASN) 或域名）的受让人。

b. Use various whois databases on the Internet to obtain the names of two DNS servers. Indicate which whois databases you used.

A：使用 VeriSign Global Registry Services" ("VeriSign") Whois database进行查询：

查询：csdn.net

DNS：VIP3.ALIDNS.COM、VIP4.ALIDNS.COM

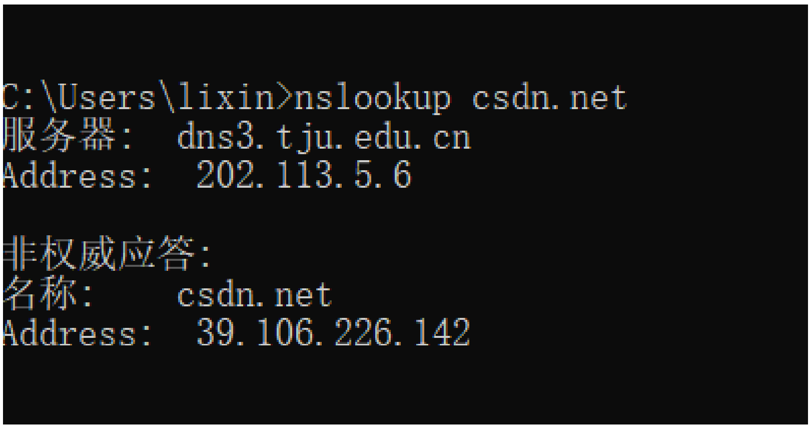
查询：google.cn

DNS：ns2.google.com、ns1.google.com、ns3.google.com、ns4.google.com

c. Use nslookup on your local host to send DNS queries to three DNS servers: your local DNS server and the two DNS servers you found in part (b). Try querying for Type A, NS, and MX reports. Summarize your findings.

A：

csdn.net，Type A：

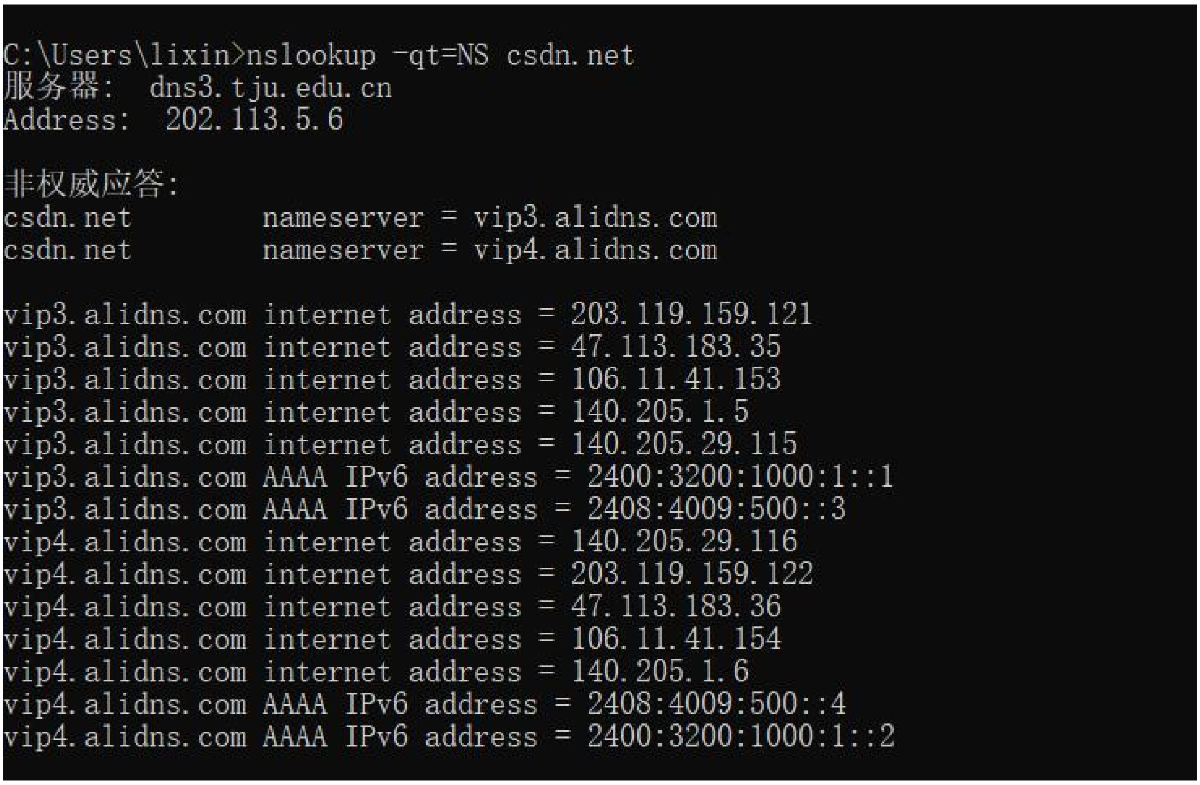


```
C:\Users\lixin>nslookup csdn.net
服务器:  dns3.tju.edu.cn
Address:  202.113.5.6

非权威应答:
名称:    csdn.net
Address:  39.106.226.142
```

其中“非权威应答” 意味着answer来自于其他服务器的缓存，而不是权威的Baidu DNS服务器。缓存会根据ttl（Time to Live）的值定时的进行更新。

csdn.net，Type NS:

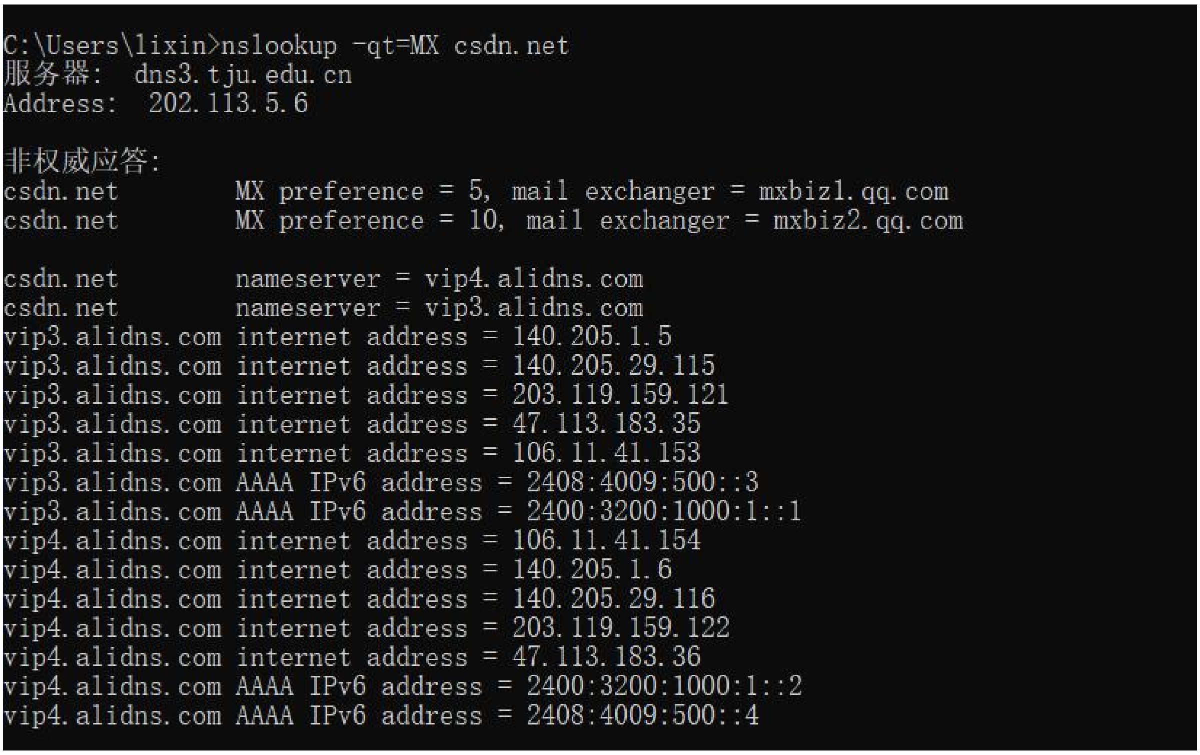


```
C:\Users\lixin>nslookup -qt=NS csdn.net
服务器:  dns3.tju.edu.cn
Address:  202.113.5.6

非权威应答:
csdn.net        nameserver = vip3.alidns.com
csdn.net        nameserver = vip4.alidns.com

vip3.alidns.com internet address = 203.119.159.121
vip3.alidns.com internet address = 47.113.183.35
vip3.alidns.com internet address = 106.11.41.153
vip3.alidns.com internet address = 140.205.1.5
vip3.alidns.com internet address = 140.205.29.115
vip3.alidns.com AAAA IPv6 address = 2400:3200:1000:1::1
vip3.alidns.com AAAA IPv6 address = 2408:4009:500::3
vip4.alidns.com internet address = 140.205.29.116
vip4.alidns.com internet address = 203.119.159.122
vip4.alidns.com internet address = 47.113.183.36
vip4.alidns.com internet address = 106.11.41.154
vip4.alidns.com internet address = 140.205.1.6
vip4.alidns.com AAAA IPv6 address = 2408:4009:500::4
vip4.alidns.com AAAA IPv6 address = 2400:3200:1000:1::2
```

csdn.net，Type MX:

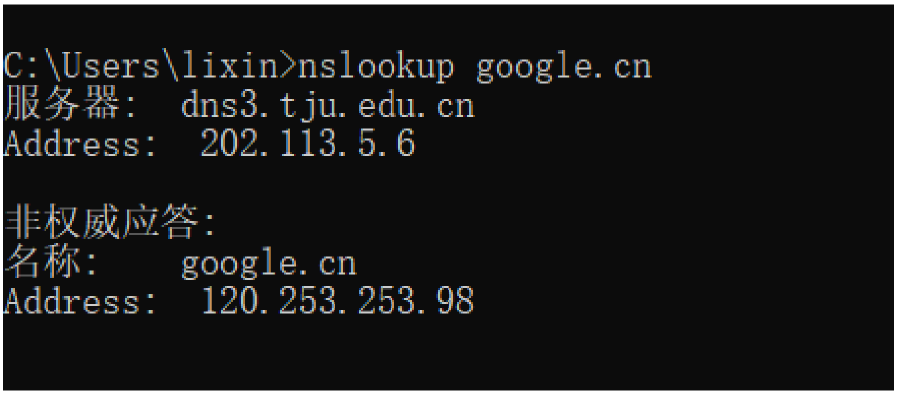


```
C:\Users\lixin>nslookup -qt=MX csdn.net
服务器:  dns3.tju.edu.cn
Address:  202.113.5.6

非权威应答:
csdn.net        MX preference = 5, mail exchanger = mxbiz1.qq.com
csdn.net        MX preference = 10, mail exchanger = mxbiz2.qq.com

csdn.net        nameserver = vip4.alidns.com
csdn.net        nameserver = vip3.alidns.com
vip3.alidns.com internet address = 140.205.1.5
vip3.alidns.com internet address = 140.205.29.115
vip3.alidns.com internet address = 203.119.159.121
vip3.alidns.com internet address = 47.113.183.35
vip3.alidns.com internet address = 106.11.41.153
vip3.alidns.com AAAA IPv6 address = 2408:4009:500::3
vip3.alidns.com AAAA IPv6 address = 2400:3200:1000:1::1
vip4.alidns.com internet address = 106.11.41.154
vip4.alidns.com internet address = 140.205.1.6
vip4.alidns.com internet address = 140.205.29.116
vip4.alidns.com internet address = 203.119.159.122
vip4.alidns.com internet address = 47.113.183.36
vip4.alidns.com AAAA IPv6 address = 2400:3200:1000:1::2
vip4.alidns.com AAAA IPv6 address = 2408:4009:500::4
```

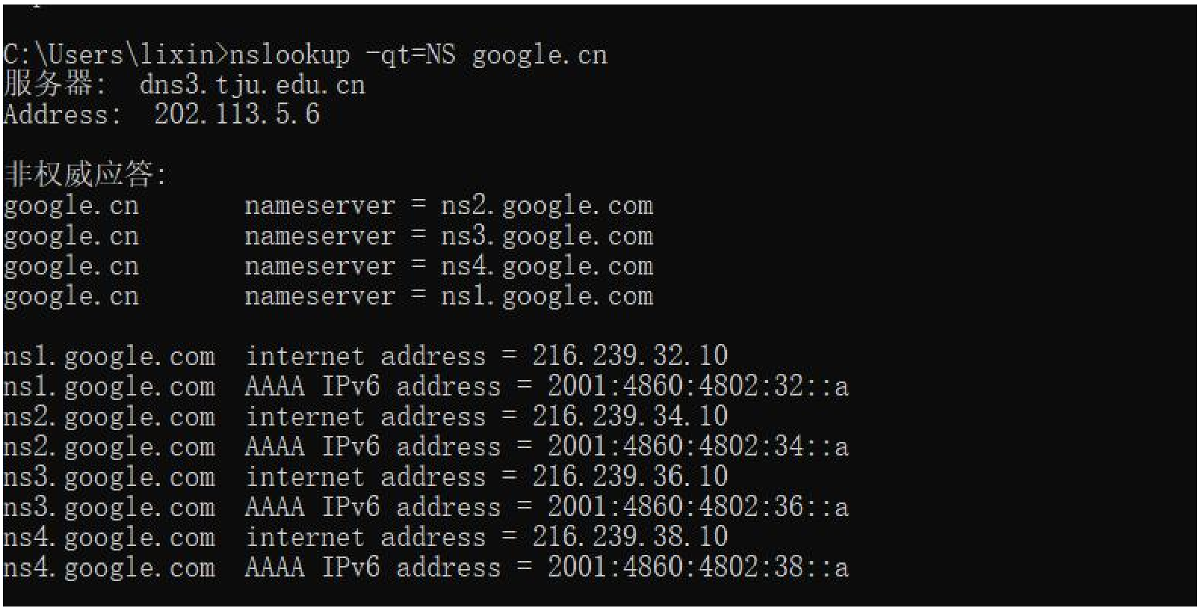
google.cn，Type A:



```
C:\Users\lixin>nslookup google.cn
服务器:  dns3.tju.edu.cn
Address:  202.113.5.6

非权威应答:
名称:    google.cn
Address:  120.253.253.98
```

google.cn，Type NS:

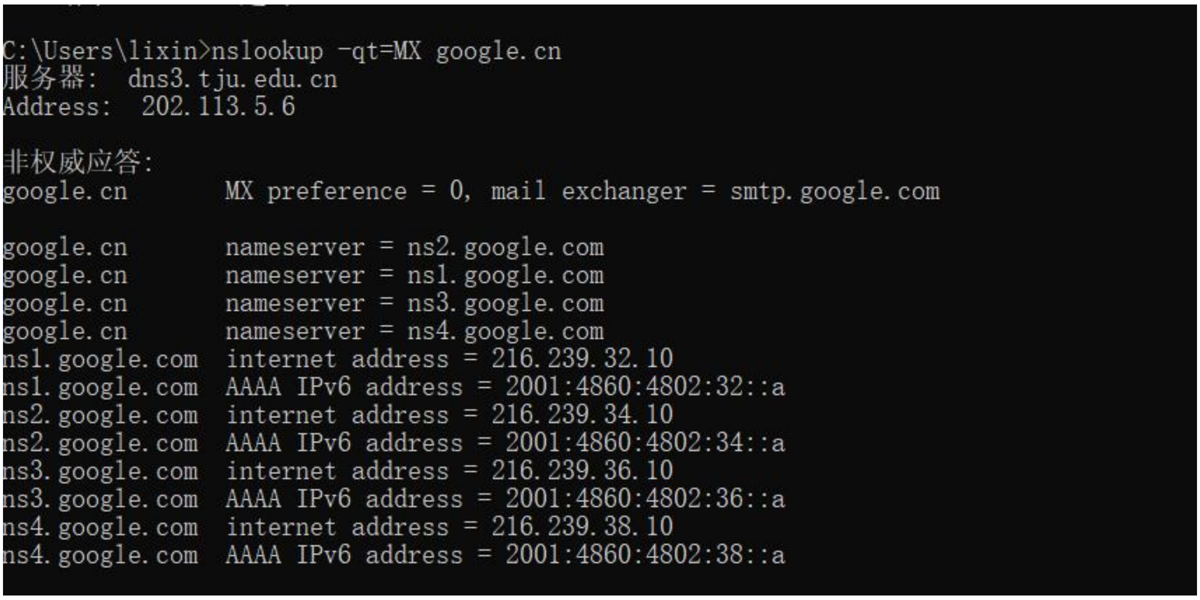


```
C:\Users\lixin>nslookup -qt=NS google.cn
服务器:  dns3.tju.edu.cn
Address:  202.113.5.6

非权威应答:
google.cn       nameserver = ns2.google.com
google.cn       nameserver = ns3.google.com
google.cn       nameserver = ns4.google.com
google.cn       nameserver = ns1.google.com

ns1.google.com  internet address = 216.239.32.10
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  AAAA IPv6 address = 2001:4860:4802:34::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  AAAA IPv6 address = 2001:4860:4802:36::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  AAAA IPv6 address = 2001:4860:4802:38::a
```

google.cn，Type MX:



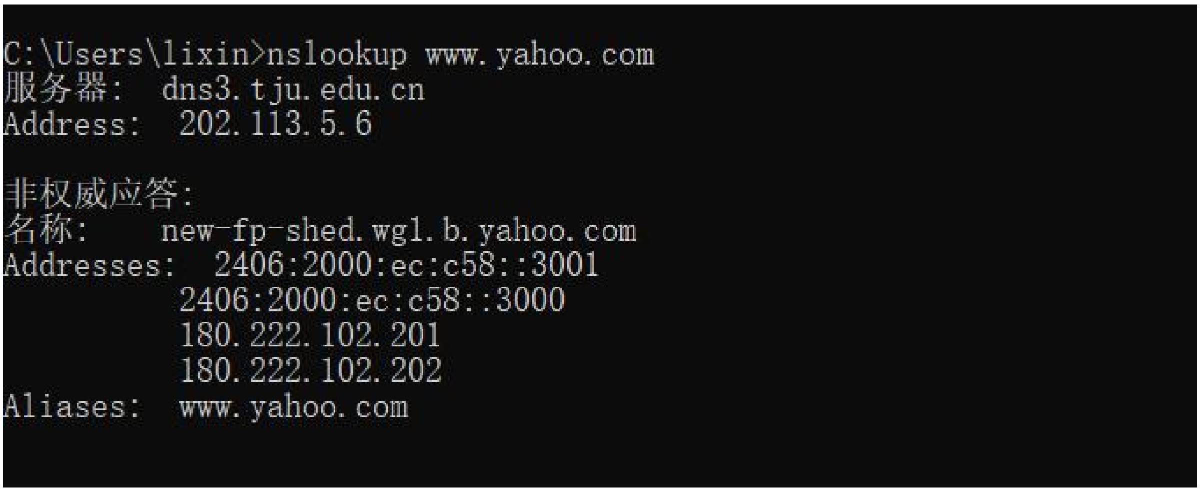
```
C:\Users\lixin>nslookup -qt=MX google.cn
服务器:  dns3.tju.edu.cn
Address:  202.113.5.6

非权威应答:
google.cn       MX preference = 0, mail exchanger = smtp.google.com

google.cn       nameserver = ns2.google.com
google.cn       nameserver = ns1.google.com
google.cn       nameserver = ns3.google.com
google.cn       nameserver = ns4.google.com
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  AAAA IPv6 address = 2001:4860:4802:34::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  AAAA IPv6 address = 2001:4860:4802:36::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  AAAA IPv6 address = 2001:4860:4802:38::a
```

d. Use nslookup to find a Web server that has multiple IP addresses. Does the Web server of your institution (school or company) have multiple IP addresses?

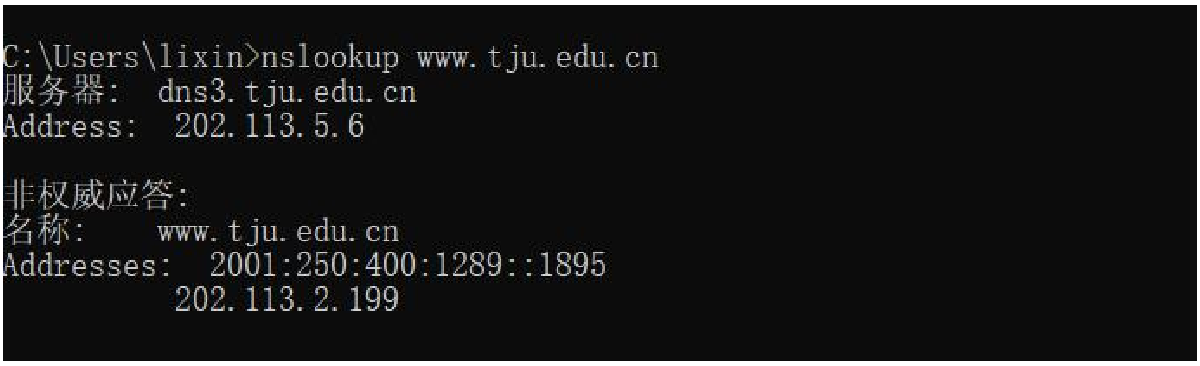
A：www.yahoo.com有多个IP地址：



```
C:\Users\lixin>nslookup www.yahoo.com
服务器:  dns3.tju.edu.cn
Address:  202.113.5.6

非权威应答:
名称:    new-fp-shed.wg1.b.yahoo.com
Addresses:  2406:2000:ec:c58::3001
          2406:2000:ec:c58::3000
          180.222.102.201
          180.222.102.202
Aliases:  www.yahoo.com
```

学校官网www.tju.edu.cn只有一个IP地址：

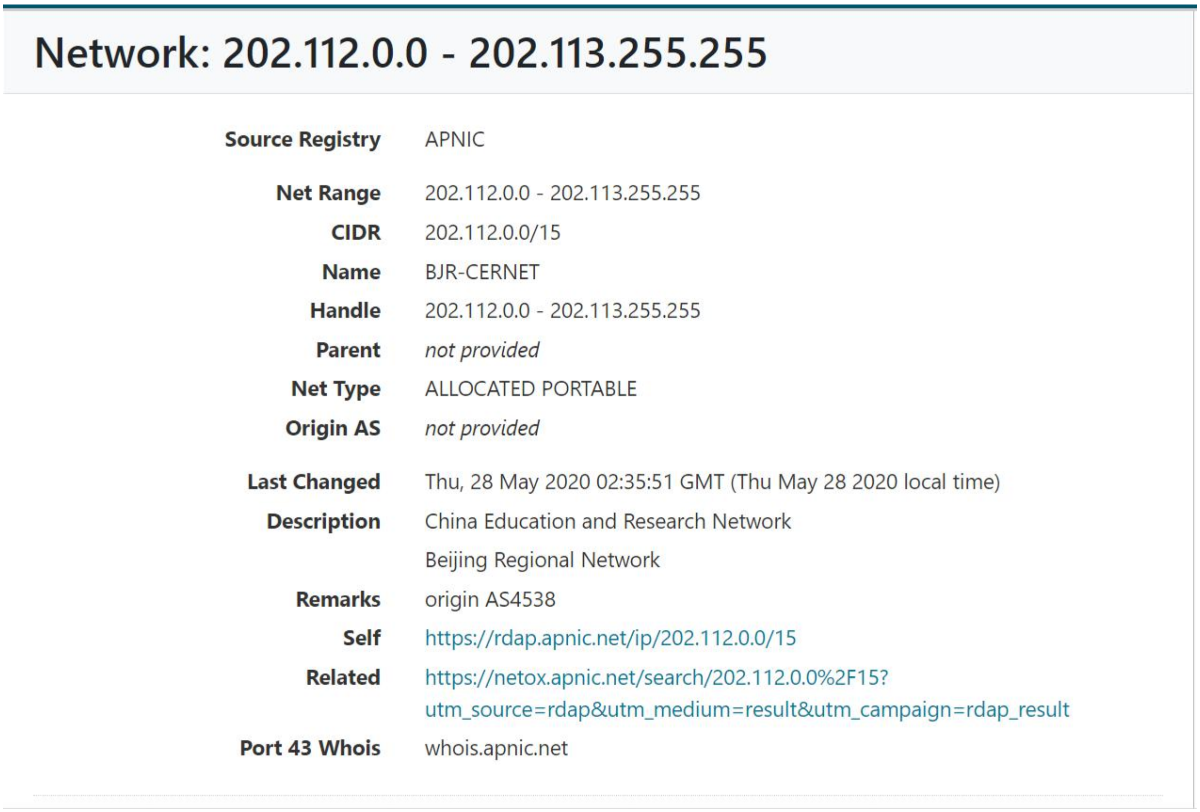


```
C:\Users\lixin>nslookup www.tju.edu.cn
服务器:  dns3.tju.edu.cn
Address:  202.113.5.6

非权威应答:
名称:    www.tju.edu.cn
Addresses:  2001:250:400:1289::1895
          202.113.2.199
```

e. Use the ARIN whois database to determine the IP address range used by your university.

A：查询到www.tju.edu.cn的IP地址范围是202.112.0.0 - 202.113.255.255



Network: 202.112.0.0 - 202.113.255.255

Source Registry	APNIC
Net Range	202.112.0.0 - 202.113.255.255
CIDR	202.112.0.0/15
Name	BJR-CERNET
Handle	202.112.0.0 - 202.113.255.255
Parent	*not provided*
Net Type	ALLOCATED PORTABLE
Origin AS	*not provided*
Last Changed	Thu, 28 May 2020 02:35:51 GMT (Thu May 28 2020 local time)
Description	China Education and Research Network Beijing Regional Network
Remarks	origin AS4538
Self	https://rdap.apnic.net/ip/202.112.0.0/15
Related	https://netox.apnic.net/search/202.112.0.0%2F15?utm_source=rdap&utm_medium=result&utm_campaign=rdap_result
Port 43 Whois	whois.apnic.net

f. Describe how an attacker can use whois databases and the nslookup tool to perform reconnaissance on an institution before launching an attack.

A：攻击者可以使用whois数据库和nslookup工具来确定目标机构的IP地址范围、DNS服务器地址等信息。

g. Discuss why whois databases should be publicly available.

A：对于被攻击者而言，使用whois可以通过分析攻击数据包的源地址追踪到攻击者所在域的信息。

Section 2.5

P22：Consider distributing a file of *F* = 20 Gbits to *N* peers. The server has an upload rate of u_s = 30 Mbps, and each peer has a download rate of d_i = 2 Mbps and an upload rate of *u*. For *N* = 10, 100, and 1,000 and *u*= 300 Kbps, 700 Kbps, and 2 Mbps, prepare a chart giving the minimum distribution time for each of the combinations of *N* and *u* for both client server distribution and P2P distribution.

A：客户端-服务器的最小分发时间为：

$$d_{cs} \geq max\{\frac{NF}{u_s}, \frac{F}{d_{min}}\}$$

P2P最小分发时间为：

$$d_{p2p} \geq max\{\frac{F}{u_s}, \frac{F}{d_{min}}, \frac{NF}{u_s+\sum u_i}\}$$

代入题目数据计算得：

客户端-服务器：

	N=10	N=100	N=1000
u=300kbps	10240s	68266.667s	68266.667s
u=700kbps	10240s	68266.667s	68266.667s
u=2mbps	10240s	68266.667s	68266.667s

p2p:

	N=10	**N=100**	**N=10001**
u=300kbps	10240s	34538.076s	63411.708s
u=700kbps	10240s	20821.604s	28699.803s
u=2mbps	10240s	10240ss	10240s