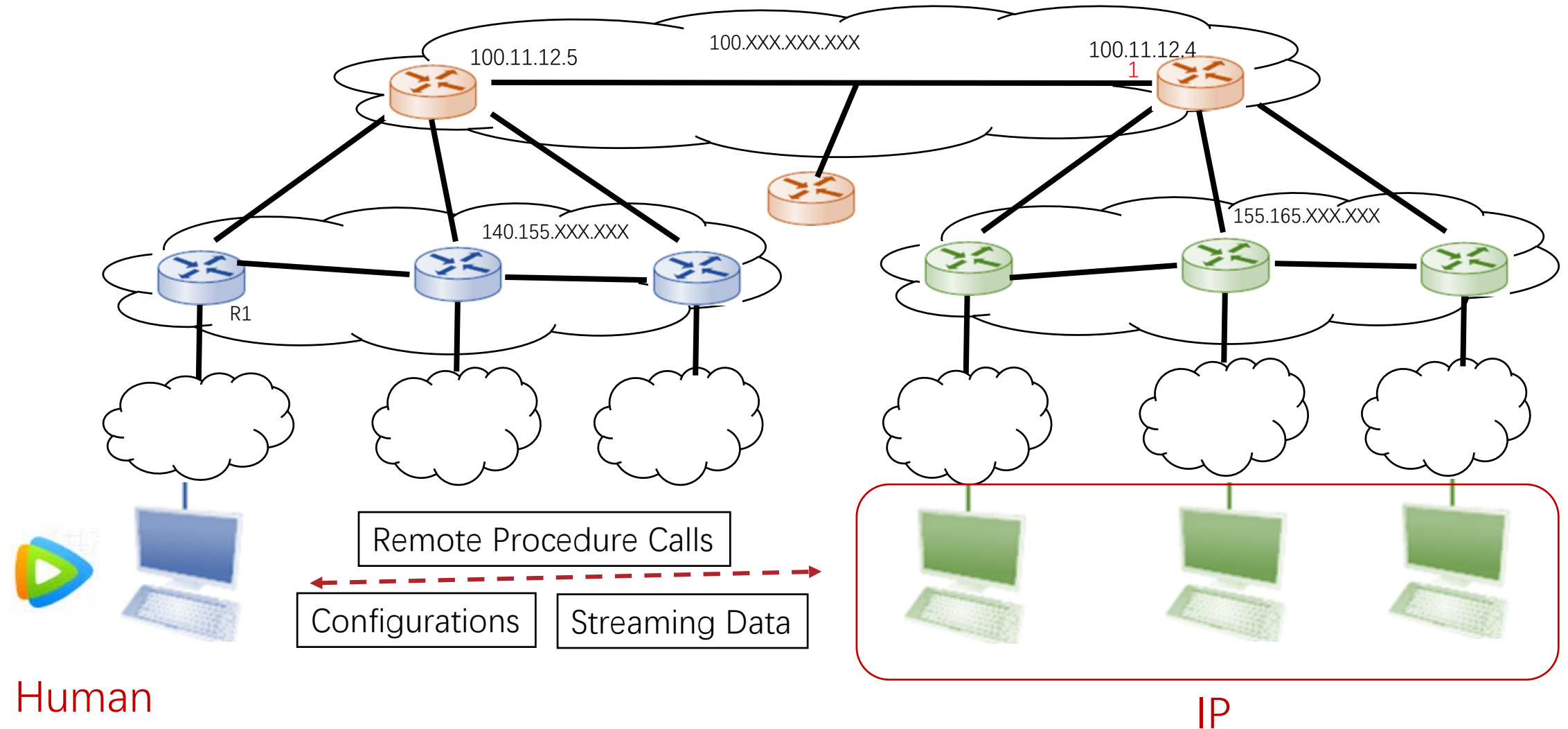# CS120: Computer Networks

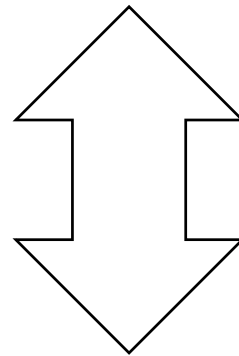## Lecture 25. DNS

Zhice Yang

How to Name a Network Host ?

How to Name a Network Host ?

- For Machine
  - IP address
    - Easy to process

- For Human
  - Literal Content
    - Easy to remember
    - eg:

IP Addresses

Name to IP Mapping

www.shanghaitech.edu.cn

上海科技大学
ShanghaiTech University

国务院.政务

中华人
www.gov.cn

Computer Name

Domain Name System (DNS)

- DNS Services
  - Hostname to IP address translation
  - Host aliasing
  - Mail server aliasing
  - Load distribution
    - Replicated Web servers: many IP addresses correspond to one name
- DNS Implementation ?
  - Centralize DNS server v.s. Distributed DNS server
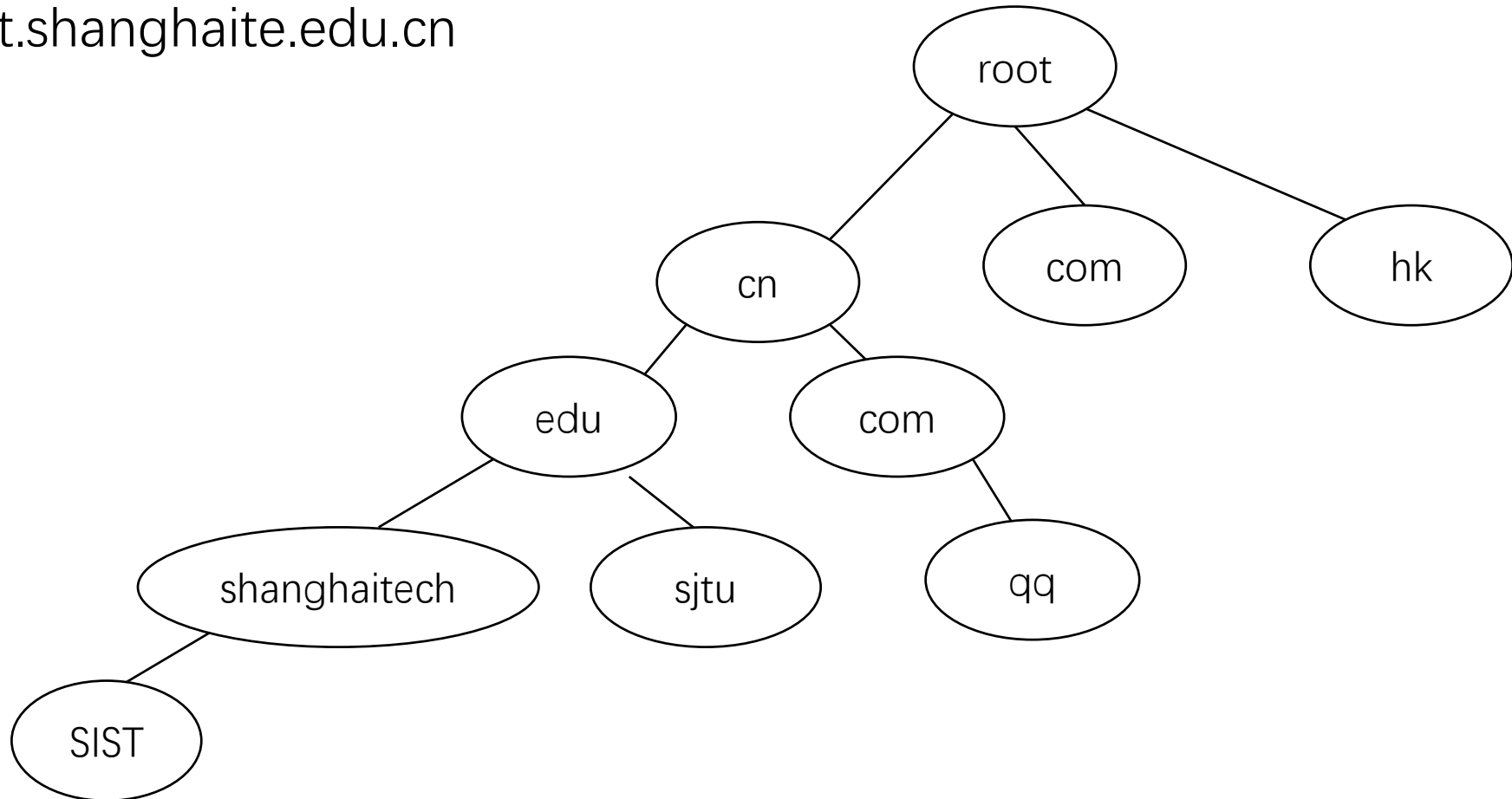
Name in the ID Card

- Should be a unique name
  - China
  - Shanghai
  - Pudong
  - ShanghaiTech
  - Zhice Yang

Domain Name

- Domain names are used to address remote servers
  - Web: http://sist.shanghaitech.edu.cn
  - Email: yangzhc@shanghaite.edu.cn
  - FTP: ftp://sist.shanghaiteh.edu.cn

Domain Name Hierarchy

- Domain names are designed with hierarchy
  - eg: sist.shanghaite.edu.cn

```
                                    root
                                   /   |    \
                                 cn   com    hk
                                /  \
                             edu   com
                            /   \      \
                  shanghaitech  sjtu    qq
                      |
                    SIST
```
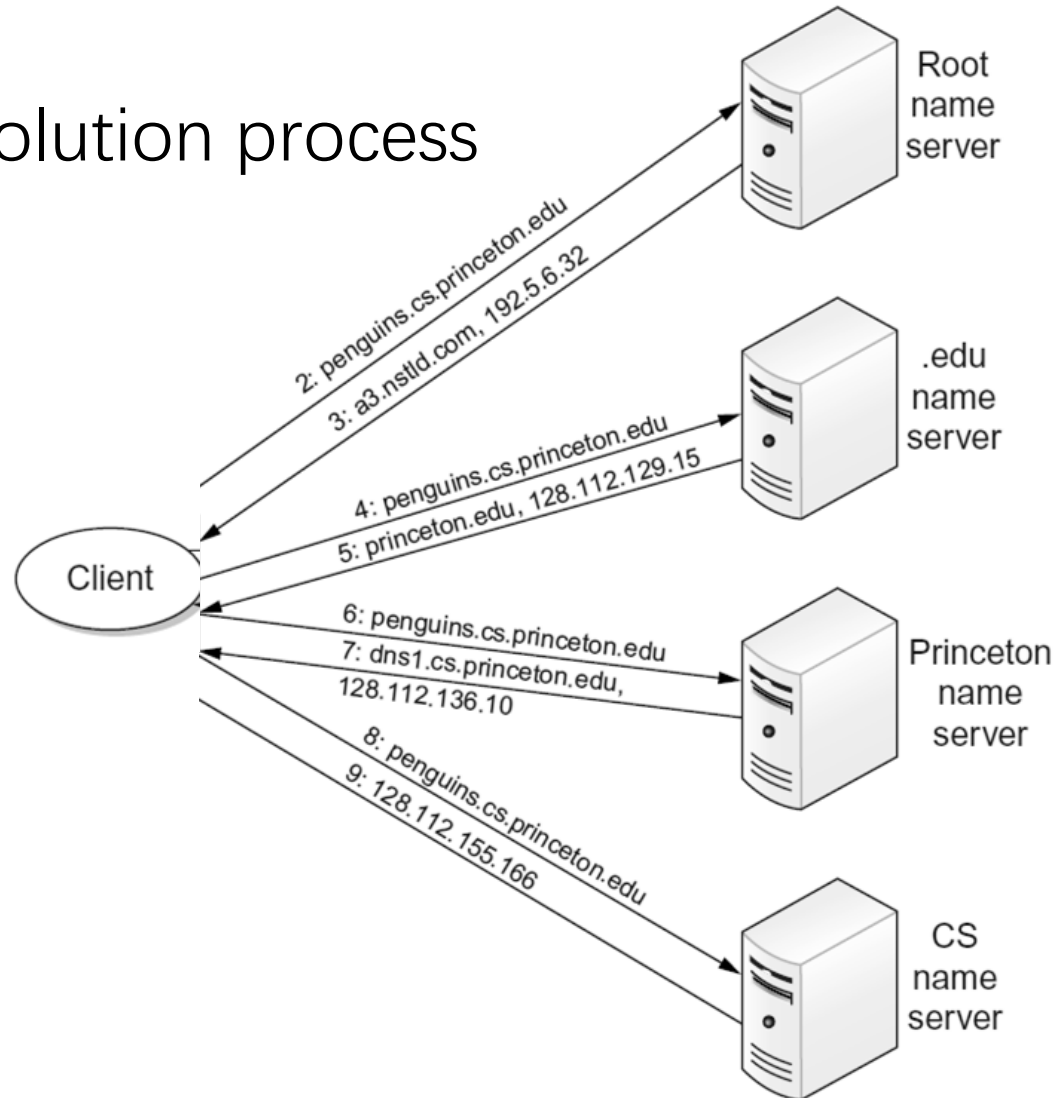
Name Server Hierarchy

- Domain Names are Managed in Servers
  - Root Name Server
  - Top-level Domain (TLD) Server
  - Authoritative Server

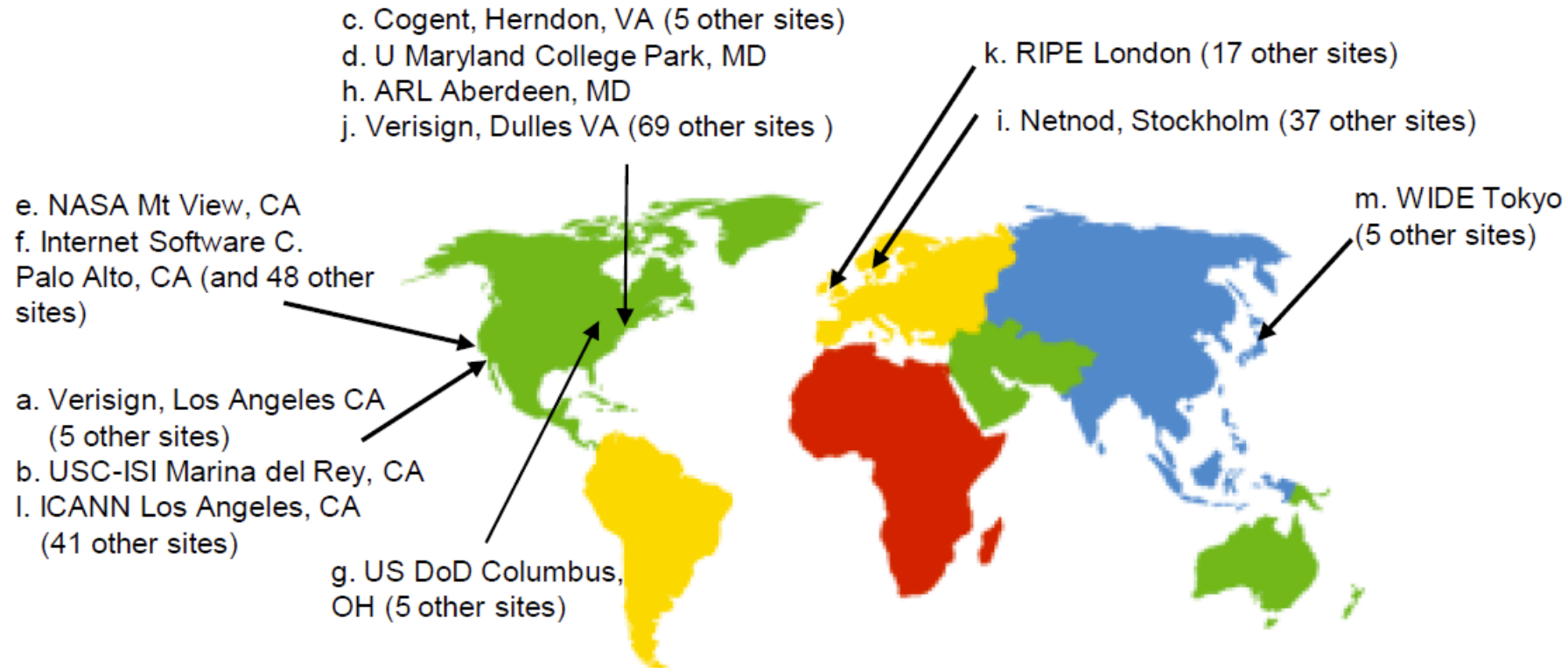# Domain Name Resolution

- Iterative domain name resolution process

2: penguins.cs.princeton.edu
3: a3.nstld.com, 192.5.6.32

4: penguins.cs.princeton.edu
5: princeton.edu, 128.112.129.15

6: penguins.cs.princeton.edu
7: dns1.cs.princeton.edu,
128.112.136.10

8: penguins.cs.princeton.edu
9: 128.112.155.166

Client

Root name server

.edu name server

Princeton name server
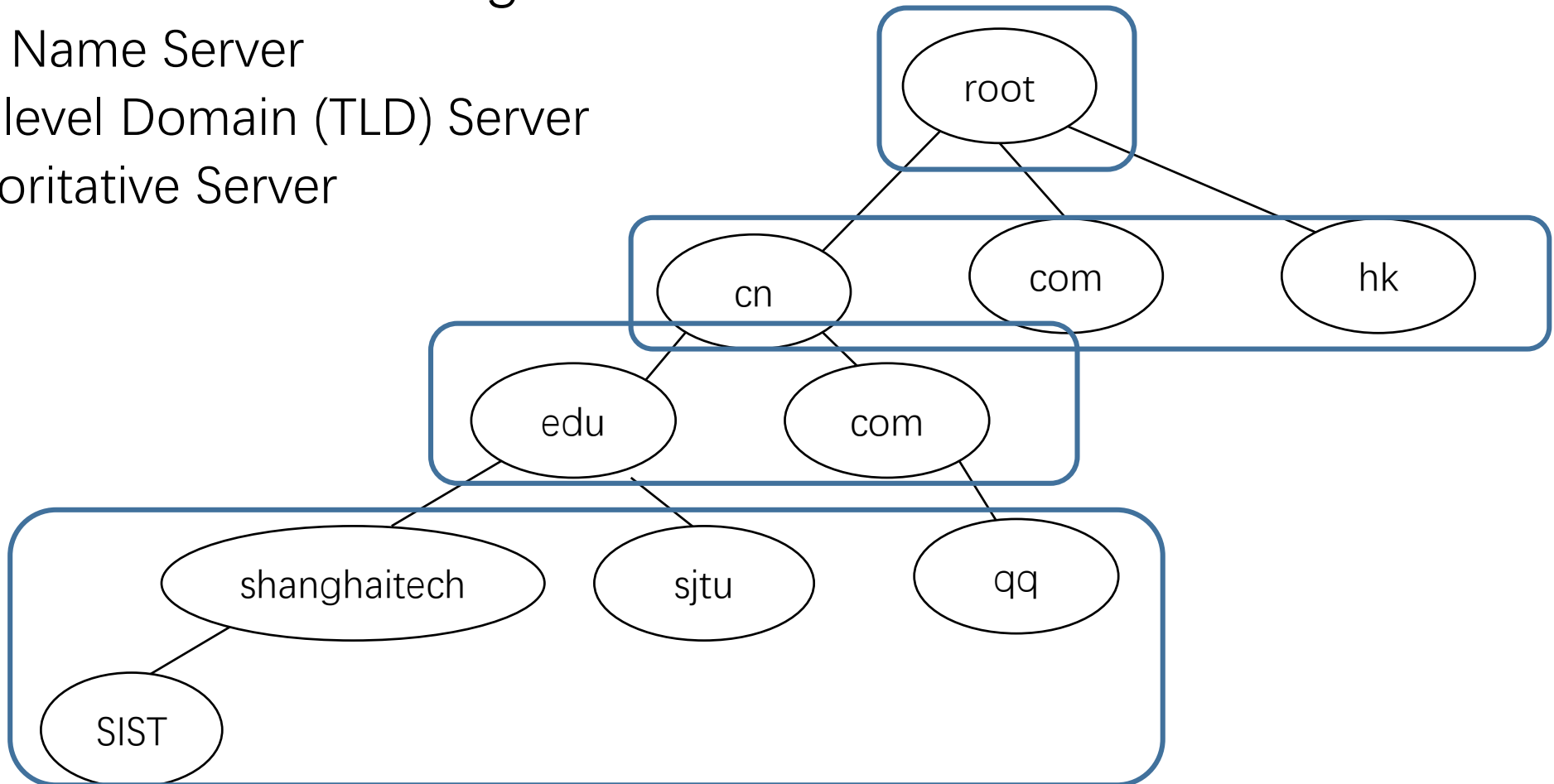
CS name server

Root Name Server

- 13 Logical Root DNS Servers
  - Multiple Mirrors

c. Cogent, Herndon, VA (5 other sites)
d. U Maryland College Park, MD
h. ARL Aberdeen, MD
j. Verisign, Dulles VA (69 other sites)

k. RIPE London (17 other sites)

i. Netnod, Stockholm (37 other sites)

e. NASA Mt View, CA
f. Internet Software C.
Palo Alto, CA (and 48 other sites)

m. WIDE Tokyo (5 other sites)

a. Verisign, Los Angeles CA
   (5 other sites)
b. USC-ISI Marina del Rey, CA
l. ICANN Los Angeles, CA
   (41 other sites)

g. US DoD Columbus, OH (5 other sites)

TLD and Authoritative Servers

- Top-level Domain (TLD) Servers
  - Responsible for com, org, net, edu, aero, jobs, museums, and all top-level country domains, e.g.: uk, fr, ca, jp
  - "Big Six" Domains
    - .edu, .com, .gov, .mil, .org and .net
    - Based in the U.S.
    - Managed by Internet Corporation for Assigned Names and Numbers (ICANN)
- Authoritative Servers
  - Maintained by organization or service provider
  - Provide authoritative hostname to IP mappings for organization's named hosts
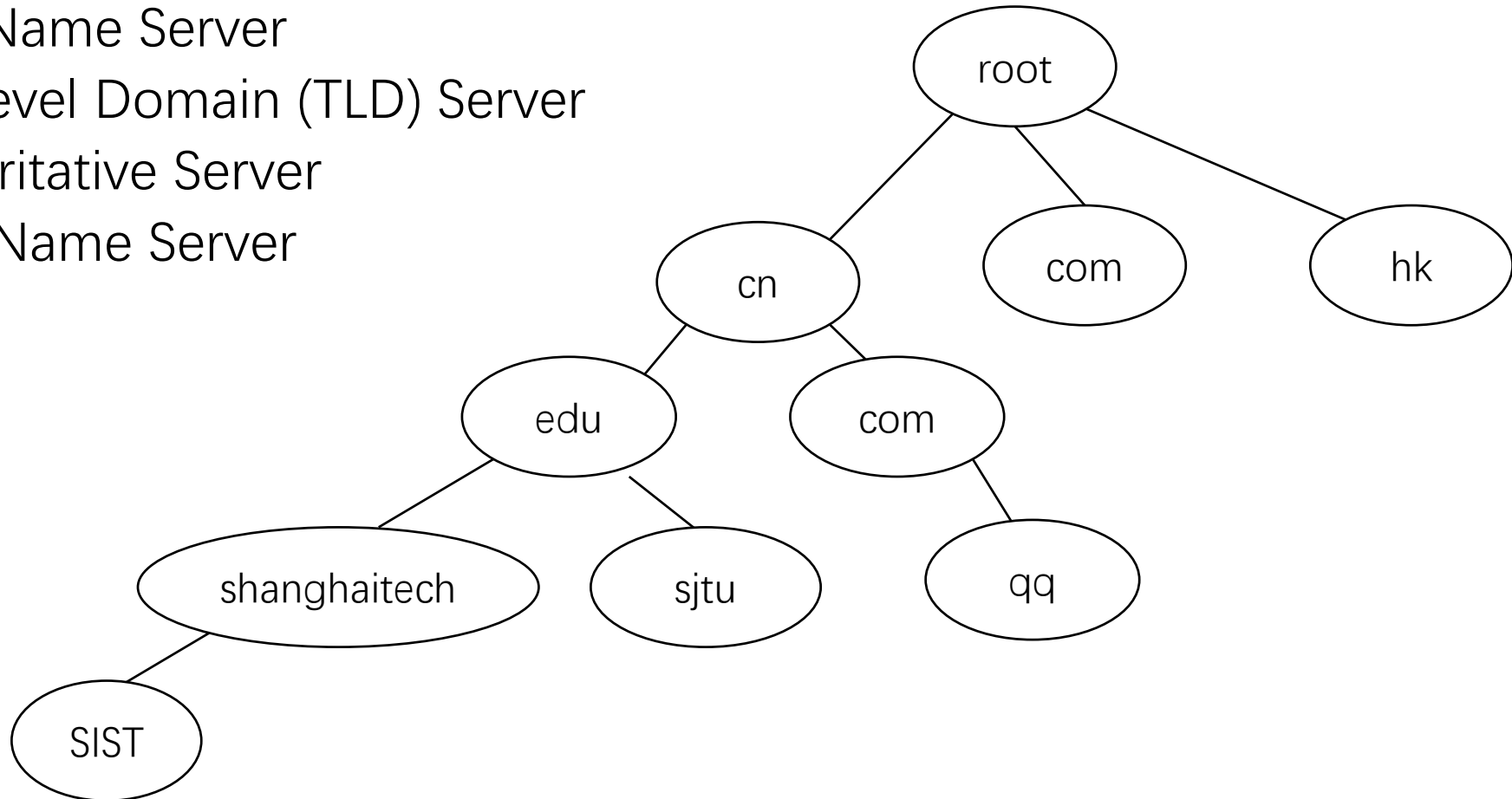   - eg., dns.baidu.com

Domain Name Resolution

- Iterative domain name resolution process
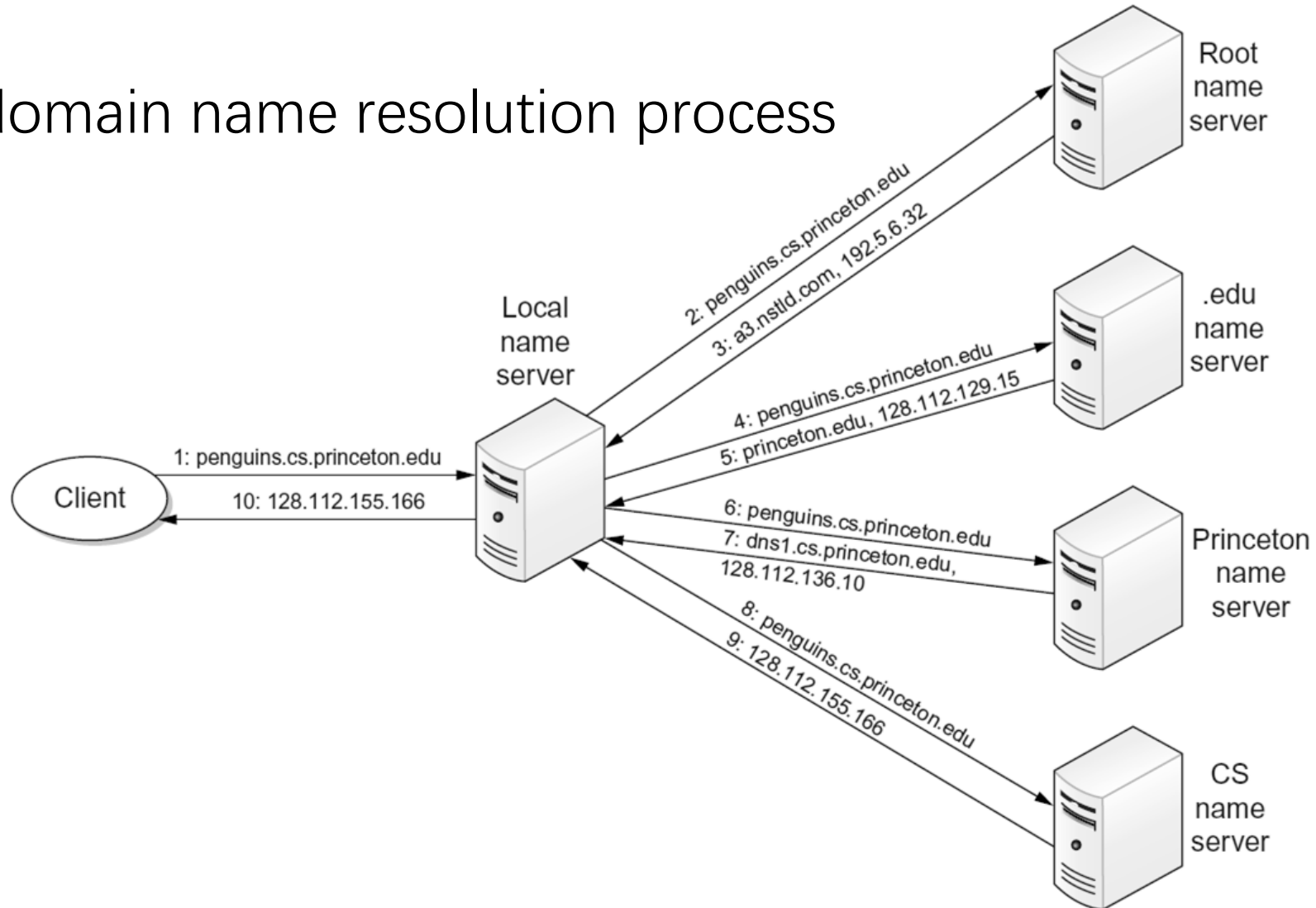
Domain Server Hierarchy

- Domain Names are Managed in Servers
  - Root Name Server
  - Top-level Domain (TLD) Server
  - Authoritative Server
  - Local Name Server

Local Name Server

- Each ISP (residential ISP, company, university) has one
  - It could be provided by DHCP
  - It could be configured to "big: local DNS servers
    - Examples:
      - Google: 8.8.8.8
      - Cloudflare: 1.1.1.1
      - Baidu: 180.76.76.76
    - For reliability, security, etc.

DNS Hijacking

- When host makes DNS query, query is sent to its local DNS server
  - If hit cache, return IP address
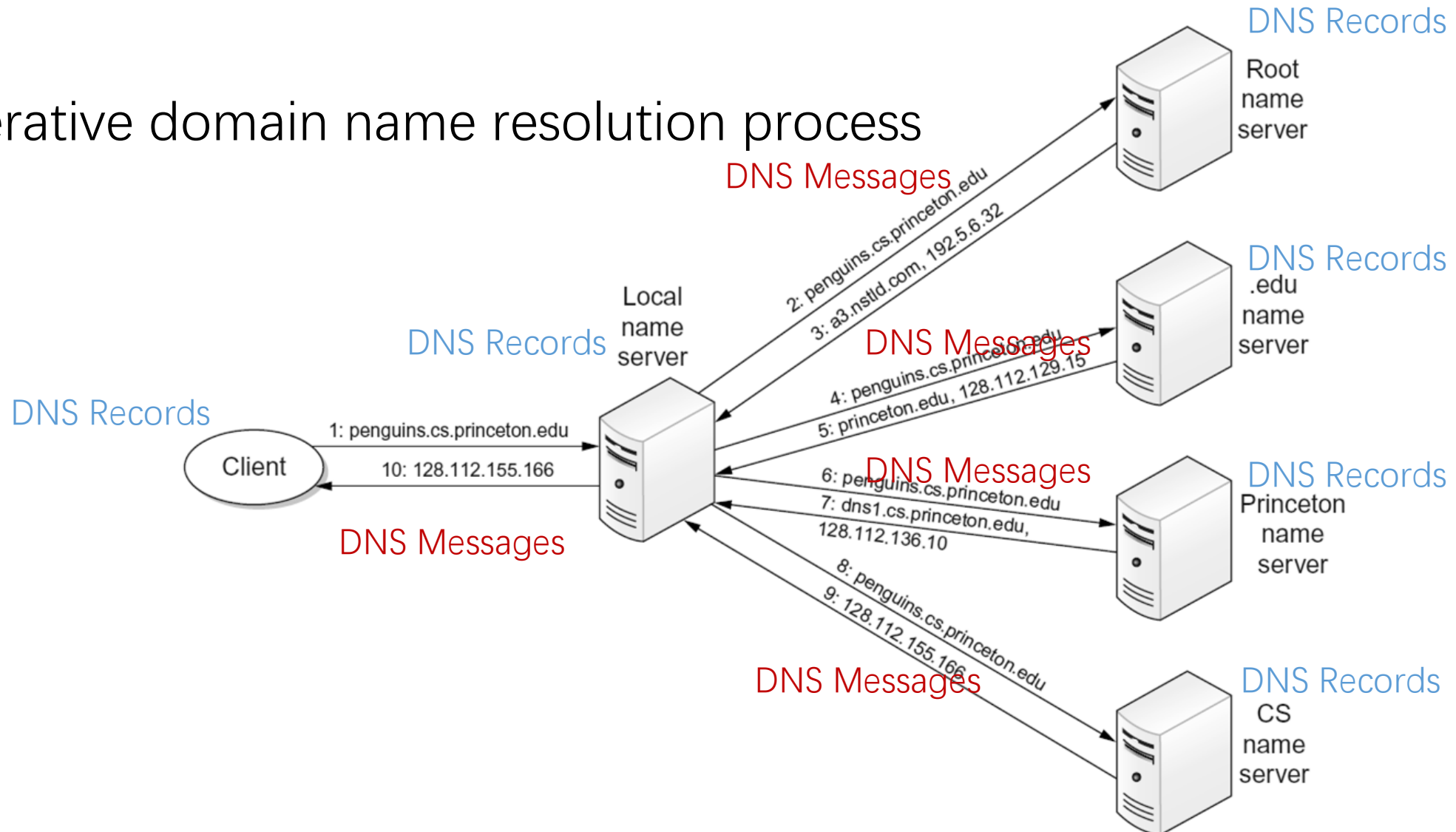 - else, forward the query to DNS hierarchy, i.e., the root name server

Demo: Default Name Server

- Window: ipconfig /all
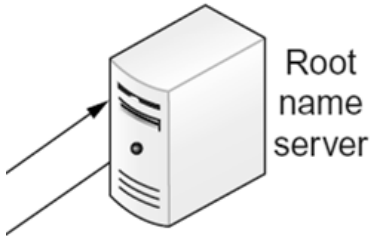- Linux: dig

Domain Name Resolution

- Iterative domain name resolution process

DNS Records
Root name server

DNS Messages

2: penguins.cs.princeton.edu
3: a3.nstld.com, 192.5.6.32

DNS Records
.edu name server

DNS Records Local name server

DNS Messages
4: penguins.cs.princeton.edu
5: princeton.edu, 128.112.129.15

DNS Records

Client

1: penguins.cs.princeton.edu
10: 128.112.155.166

DNS Messages
6: penguins.cs.princeton.edu
7: dns1.cs.princeton.edu, 128.112.136.10

DNS Records
Princeton name server

DNS Messages

DNS Messages

8: penguins.cs.princeton.edu
9: 128.112.155.166

DNS Messages

DNS Records
CS name server

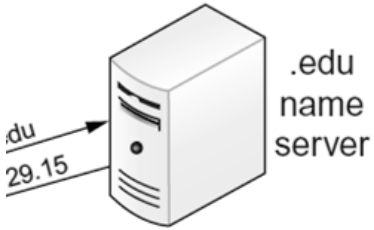# DNS Record

- Format
  - <name, value, type, class, ttl>
- Name
  - The name for this record
  - Determined by type
- Value
  - Could be IP address or other values
  - Determined by type
- Class
  - Only one value: IN (internet)
- TTL
  - Time to live

- Type=A
  - Name: hostname
    - eg.: shanghaitech.edu.cn
  - Value: IP address
- Type=NS
  - Name: domain
    - e.g.: .com
  - Value: hostname
- Type=CNAME
  - Name: alias name for some "canonical" (the real) name
  - Value: canonical name
- Type=MX
  - Name: mail server name
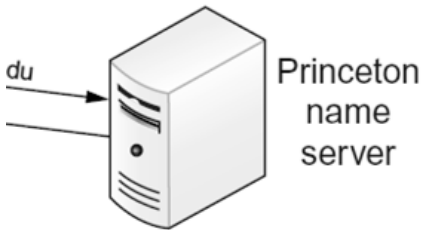   - eg.: mail.google.com, shanghaitech.edu.cn
  - Value: IP address

DNS Record

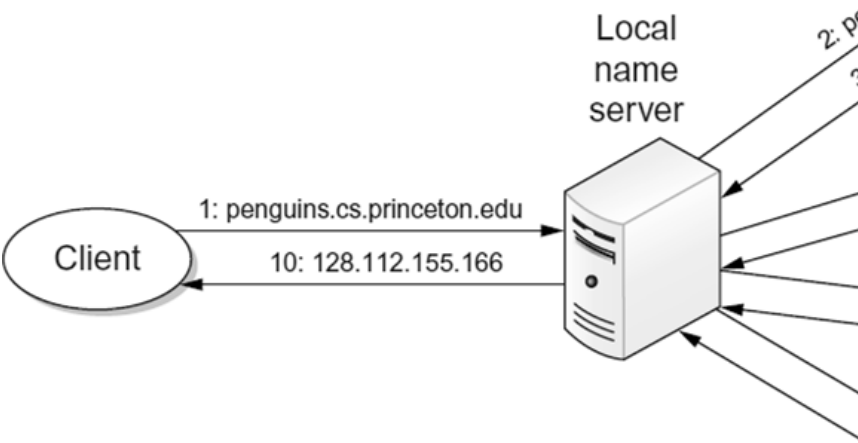**Root name server**

```
<edu,a3.nstld.com,NS,IN>
<a3.nstld.com,192.5.6.32,A,IN>
<com,a.gtld-servers.net,NS,IN>
<a.gtld-servers.net, 192.5.6.30,A,IN>
```

.edu name server

```
<princeton.edu,dns.princeton.edu,NS,IN>
<dns.princeton.edu,128.112.129.15,A,IN>
```

Princeton name server

```
<email.princeton.edu,128.112.198.35,A,IN>
<penguins.cs.princeton.edu,dns1.cs.princeton.edu,NS,IN>
<dns1.cs.princeton.edu,128.112.136.10,A,IN>
```

CS name server

```
<penguins.cs.princeton.edu,128.112.155.166,A,IN>
<www.cs.princeton.edu,coreweb.cs.princeton.edu,CNAME,IN>
<coreweb.cs.princeton.edu,128.112.136.35,A,IN>
<cs.princeton.edu,mail.cs.princeton.edu,MX,IN>
<mail.cs.princeton.edu,128.112.136.72,A,IN>
```

- Type=A
  - Name: hostname
    - eg.: shanghaitech.edu.cn
  - Value: IP address
- Type=NS
  - Name: domain
    - e.g.: .com
  - Value: hostname
- Type=CNAME
  - Name: alias name for some "canonical" (the real) name
  - Value: canonical name
- Type=MX
  - Name: mail server
    - eg.: gmail.com, shanghaitech.edu.cn
  - Value: mail server name
    - eg,: mail.shanghaitech.edu.cn

18

DNS Record

```
<'root', a.root-servers.net,NS,IN>
<a.root-servers.net, 198.41.0.4,A,IN>
```

- Type=A
  - Name: hostname
    - eg.: shanghaitech.edu.cn
  - Value: IP address
- Type=NS
  - Name: domain
    - e.g.: .com
  - Value: hostname
- Type=CNAME
  - Name: alias name for some "canonical" (the real) name
  - Value: canonical name
- Type=MX
  - Name: mail server
    - eg.: gmail.com, shanghaitech.edu.cn
  - Value: mail server name
    - eg,: mail.shanghaitech.edu.cn

19

Demo: DNS Query

- Linux & windows: dig
- Online:
  - https://www.diggui.com

DNS Caching

- Once (any) name server learns mapping, it caches mapping
  - Cache entries timeout (disappear) after some time (TTL)
- DNS Caching Exists in Every Place of the Hierarchy
  - TLD servers cache root name server IP address
  - Local DNS servers cache names of high-frequency
  - OS and browser of PC caches names of high-frequency
  - etc.

Demo: Local Host Caching

- Windows
  - ipconfig /displaydns
- Linux
  - Has no OS DNS caching
- Network Browser
  - chrome://net-internals/#dns

How to Reach shanghaitech.edu.cn?

- Check local cache to find IP of shanghaitech.edu.cn
- Check local DNS server (IP is known) to find IP of shanghaitech.edu.cn
  - Same subnet: use ARP to find DNS server's MAC
  - Different subnet: use ARP to find gateway's MAC, then route the DNS query to the local DNS server
- Local DNS server resolves IP of shanghaitech.edu.cn
  - Reply to host
- Connect to the IP of shanghaitech.edu.cn
  - Same subnet: ARP
  - Different subnet: Routing

Reference

- Textbook 9.3