

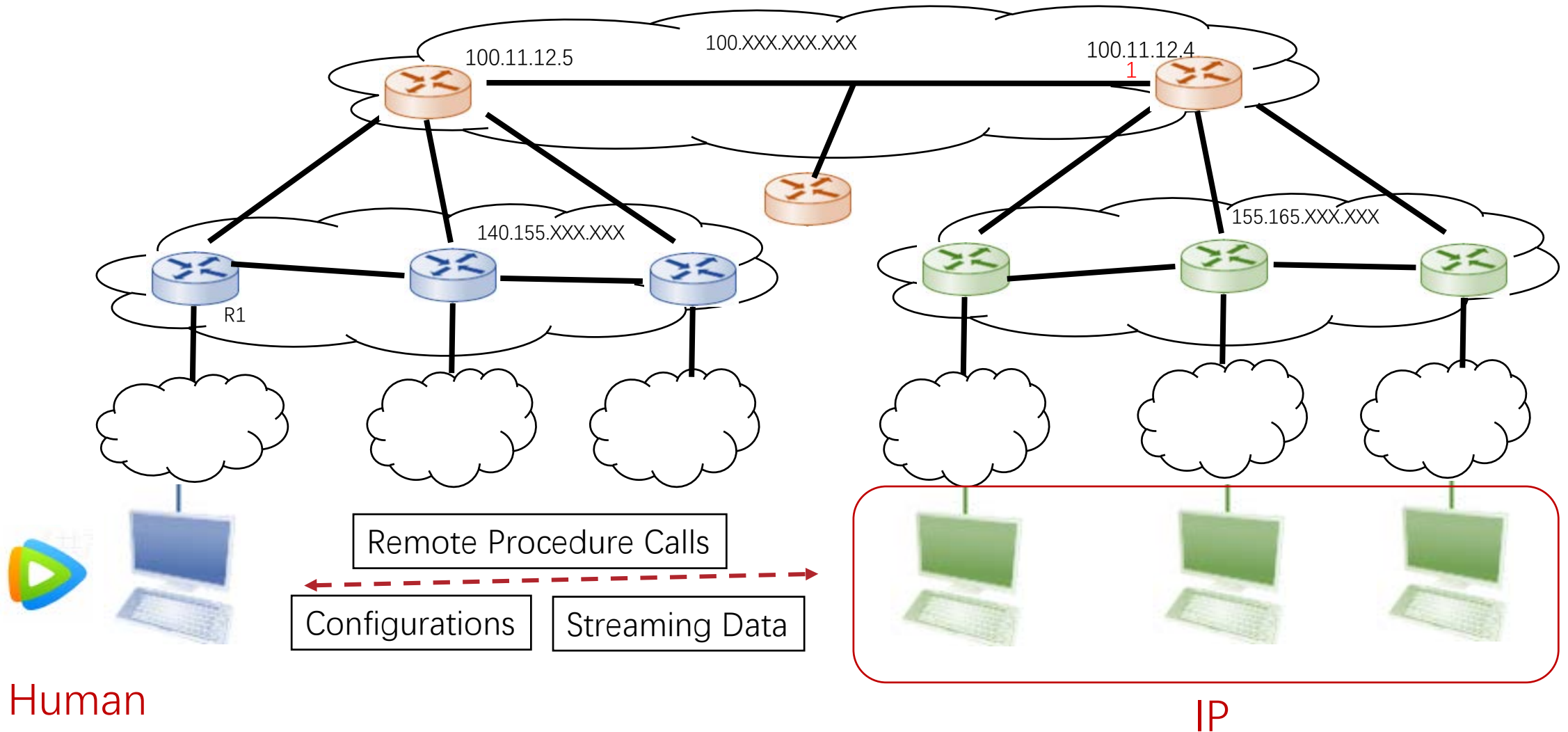


CS120: Computer Networks

Lecture 24. DNS

Zhice Yang

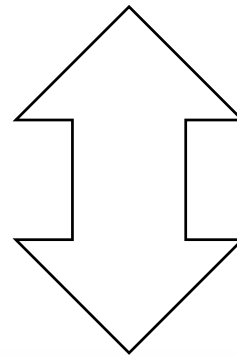
How to Name a Network Host ?



How to Name a Network Host ?

- For Machine
 - IP address
 - Easy to process
- For Human
 - Literal Content
 - Easy to remember
 - e.g.,:

IP Addresses



Name to IP Mapping



Domain Name

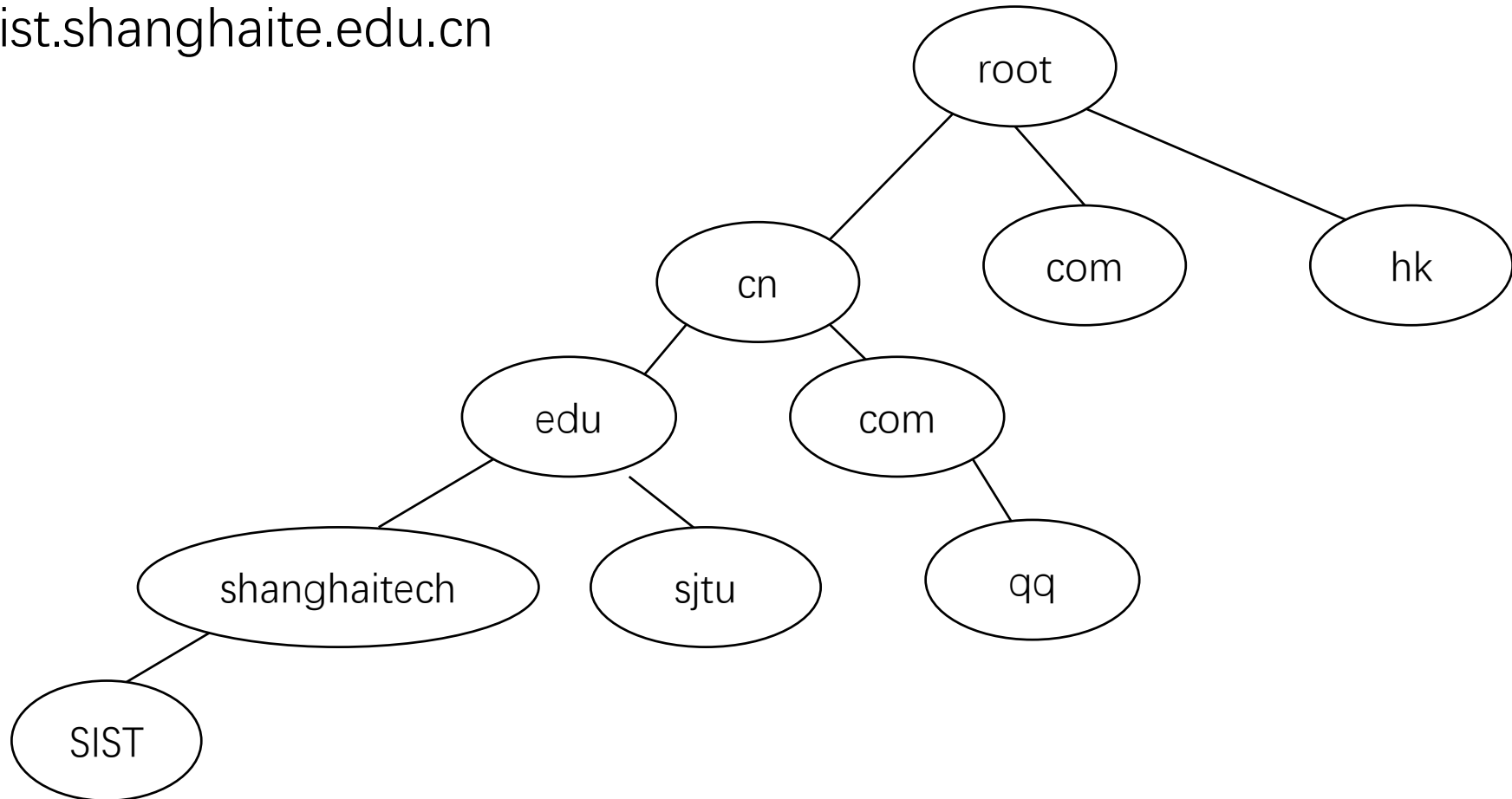
- Domain names are used to address remote servers
 - Web: <http://sist.shanghaitech.edu.cn>
 - Email: yangzhc@shanghaitech.edu.cn
 - FTP: <ftp://sist.shanghaitech.edu.cn>

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
 - scalability
 - Akamai DNS servers alone: 2.2T DNS queries/day
 - single point of failure
 - traffic volume
 - distant centralized database
 - maintenance

Domain Name Hierarchy

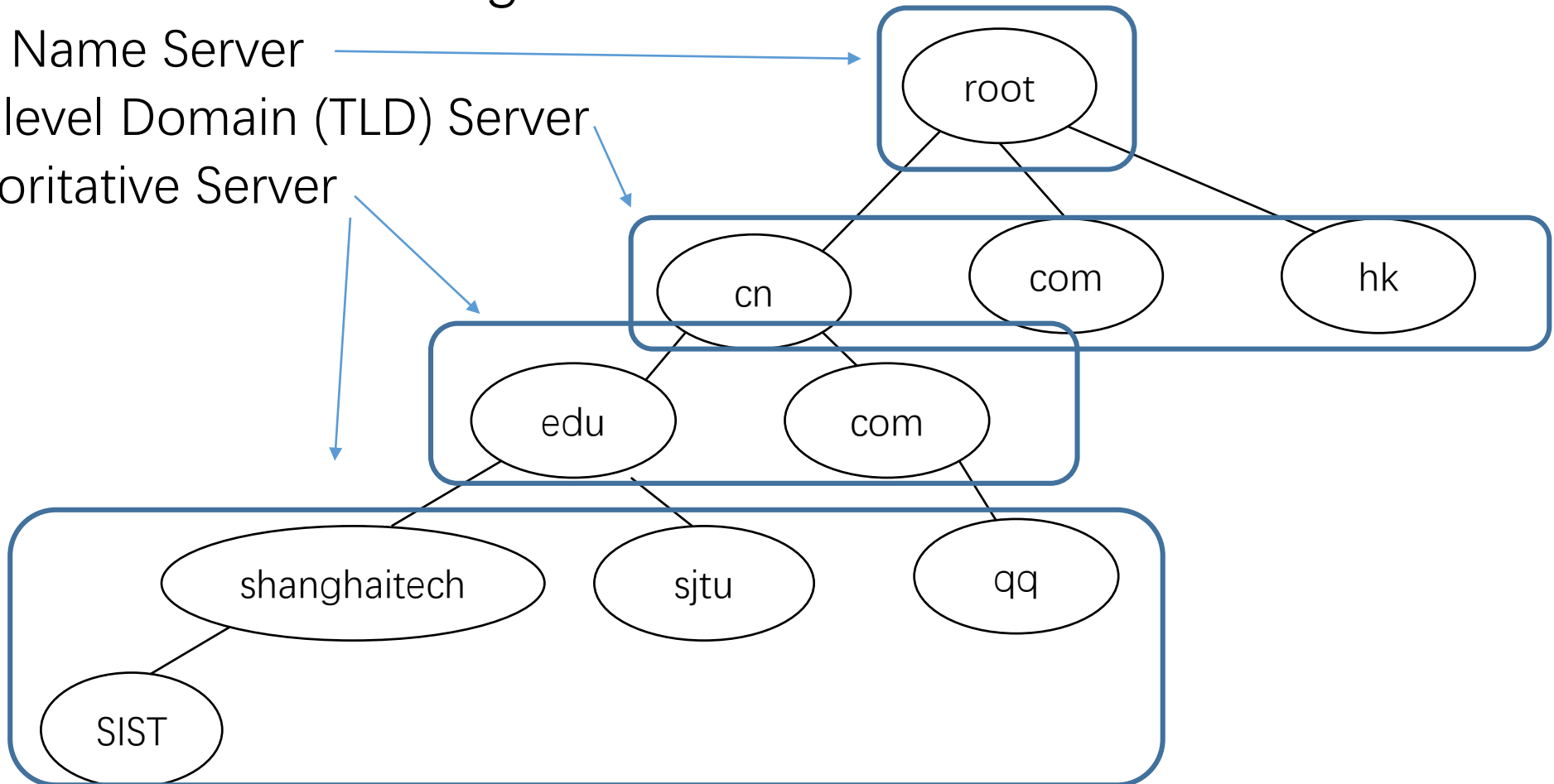
- Domain names are designed with hierarchy
 - e.g.,: sist.shanghaitech.edu.cn



Name Server Hierarchy

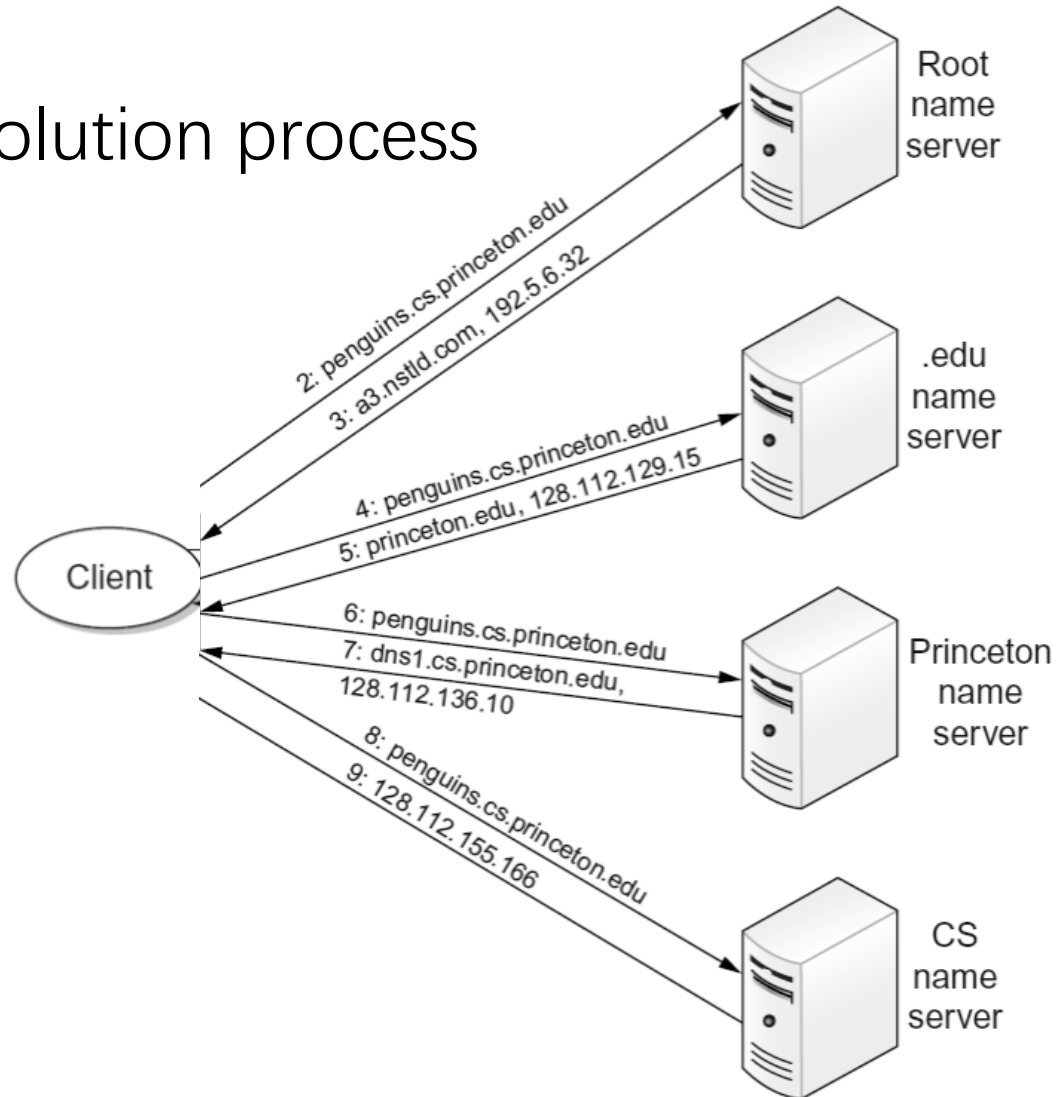
- Domain Names are Managed in Servers

- Root Name Server
- Top-level Domain (TLD) Server
- Authoritative Server



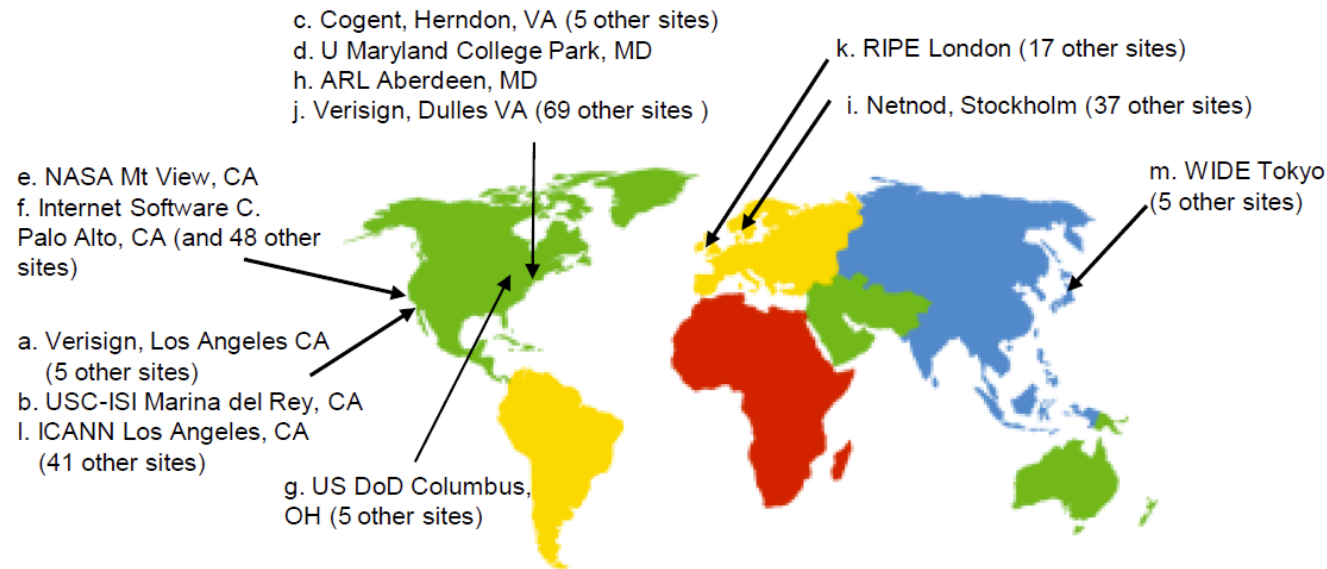
Domain Name Resolution

- Iterative domain name resolution process



Root Name Server

- 13 Logical Root DNS Servers
 - official, contact-of-last-resort by name servers that can not resolve name
 - Multiple Mirrors
 - Managed by ICANN (Internet Corporation for Assigned Names and Numbers)

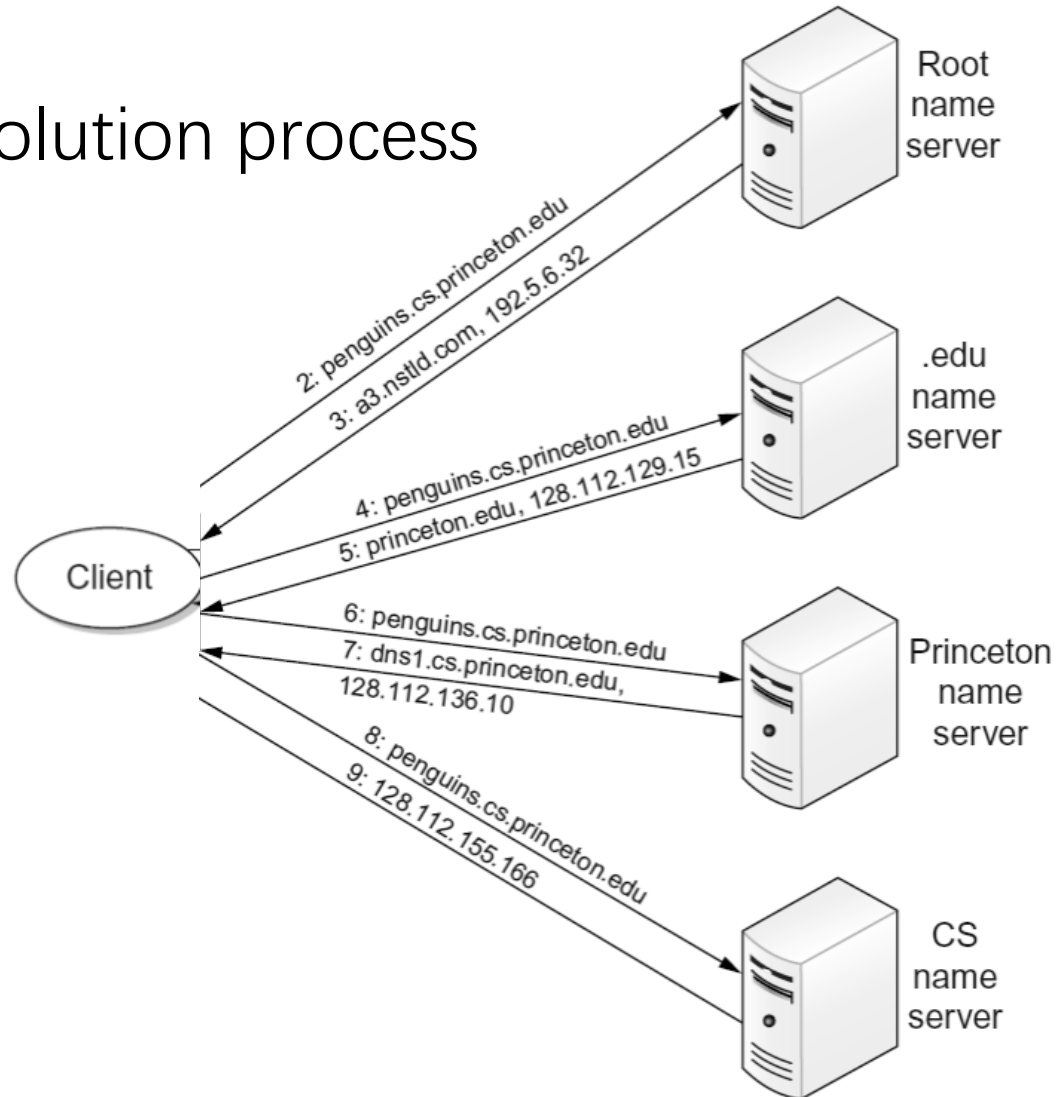


TLD and Authoritative Servers

- 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 ISP
 - Provide authoritative hostname to IP mappings for organization’s named hosts
 - e.g., dns.baidu.com

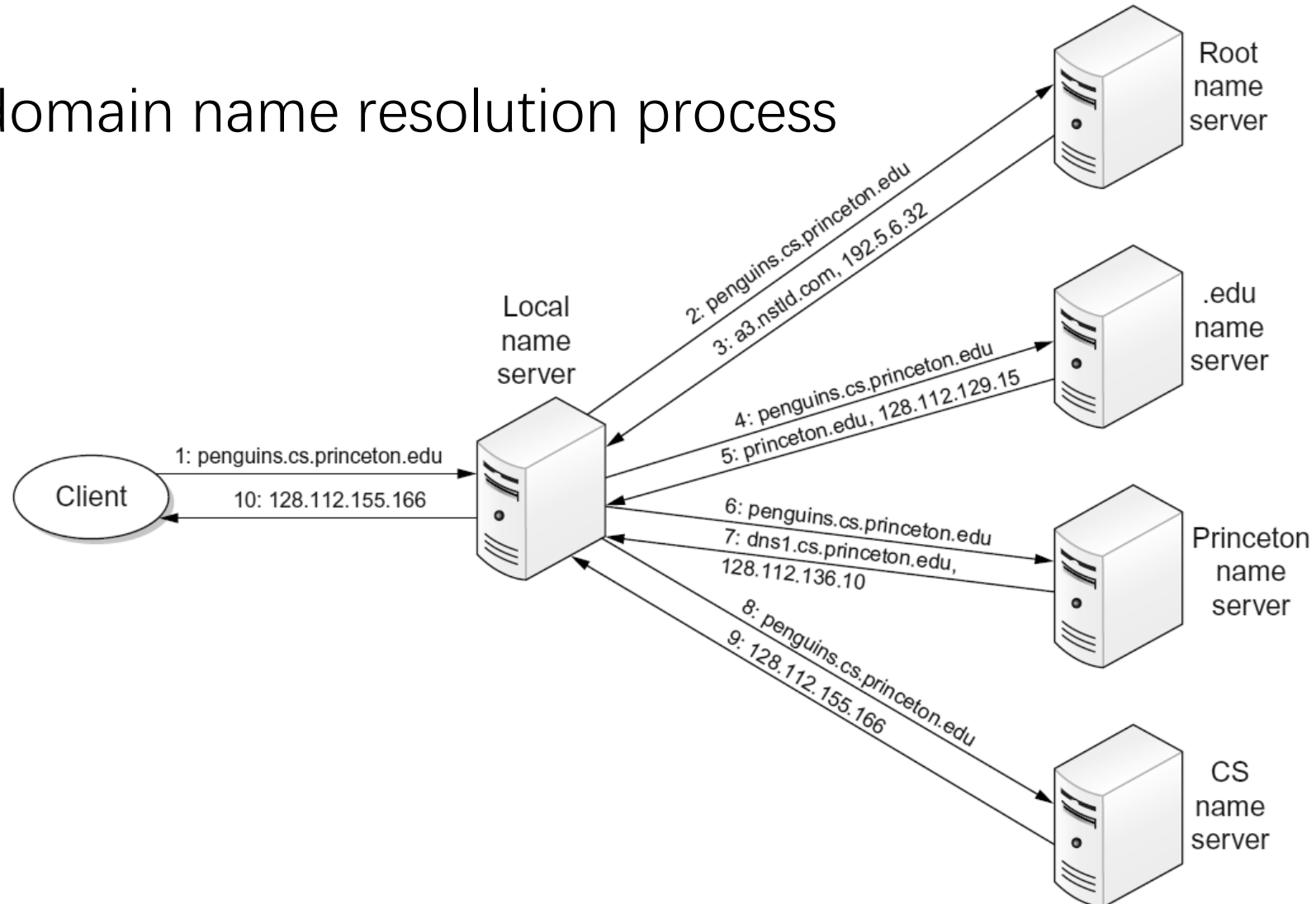
Domain Name Resolution

- Iterative domain name resolution process



Domain Name Resolution

- Iterative domain name resolution process



Local Name Server

- Each ISP (residential ISP, company, university) has one
 - Its IP could be provided by DHCP
 - It could be configured to “big” public DNS servers
 - Examples:
 - Google: 8.8.8.8
 - Cloudflare: 1.1.1.1
 - Baidu: 180.76.76.76
- When host makes DNS query, query is sent to its local DNS server
 - If hit cache, return IP address
 - else, local DNS server forwards the query to DNS hierarchy, i.e., the root name server

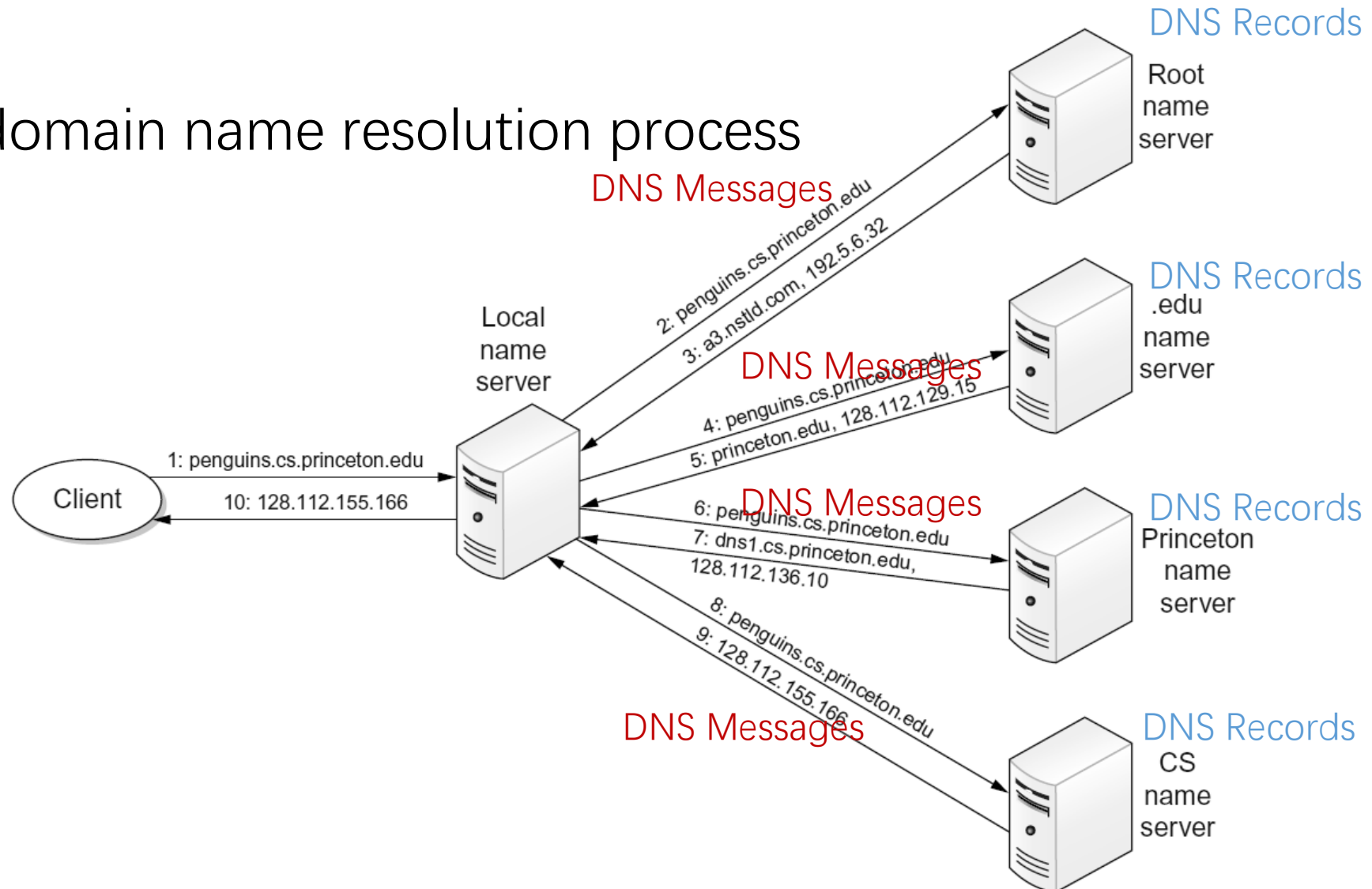


Demo: Default Name Server

- Window: `ipconfig /all`
- Linux: `dig`

Domain Name Resolution

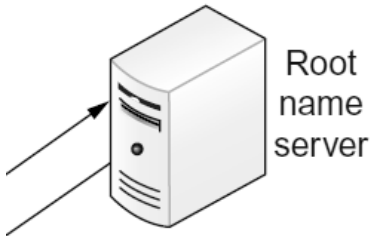
- Iterative domain name resolution process



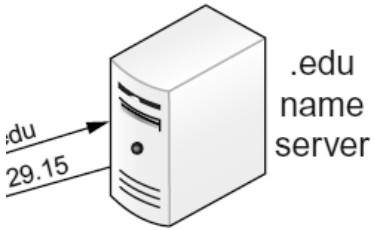
DNS Record

- Format
 - <name, value, type, class, ttl>
- Name
 - The name for this record
 - Determined by type
- Value
 - Could be IP address or other values
 - the value of Name
- Type
 - Four Types
- Class
 - Only one value: IN (internet)
- TTL
 - Time to live
- Type=A (address)
 - Name: hostname
 - e.g., shanghaitech.edu.cn
 - Value: IP address
- Type=NS (name server)
 - Name: domain
 - e.g., .com
 - Value: hostname
- Type=CNAME (canonical name)
 - Name: alias name for some “canonical” (the real) name
 - Value: canonical name
- Type=MX
 - Name: mail server name
 - e.g., mail.google.com, shanghaitech.edu.cn
 - Value: IP address

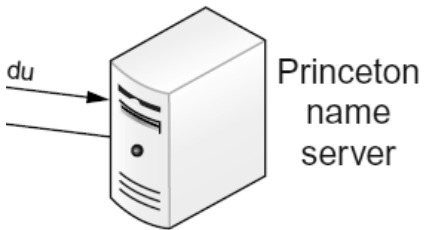
DNS Record



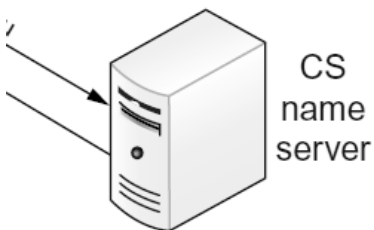
```
<edu,a3.nstld.com,NS,IN>
<a3.nstld.com,192.5.6.32,A,IN>
<com,a.gtld-servers.net,NS,IN>
<a.gtld-servers.net, 192.5.6.30,A,IN>
```



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



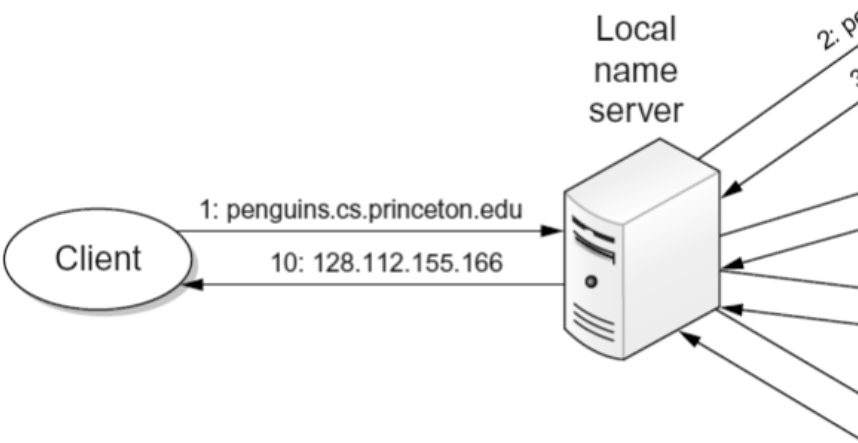
```
<email.princeton.edu,128.112.198.35,A,IN>
<penguins.cs.princeton.edu,dns1.cs.princeton.edu,NS,IN>
<dns1.cs.princeton.edu,128.112.136.10,A,IN>
```



```
<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
 - e.g., 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
 - e.g., gmail.com, shanghaitech.edu.cn
 - Value: mail server name
 - e.g., mail.shanghaitech.edu.cn

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

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
 - 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 (assume DNS miss) to find IP of shanghaitech.edu.cn
- Check local DNS server 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