International School
Jinan University

Computer Networks

L12 – Application Layer I

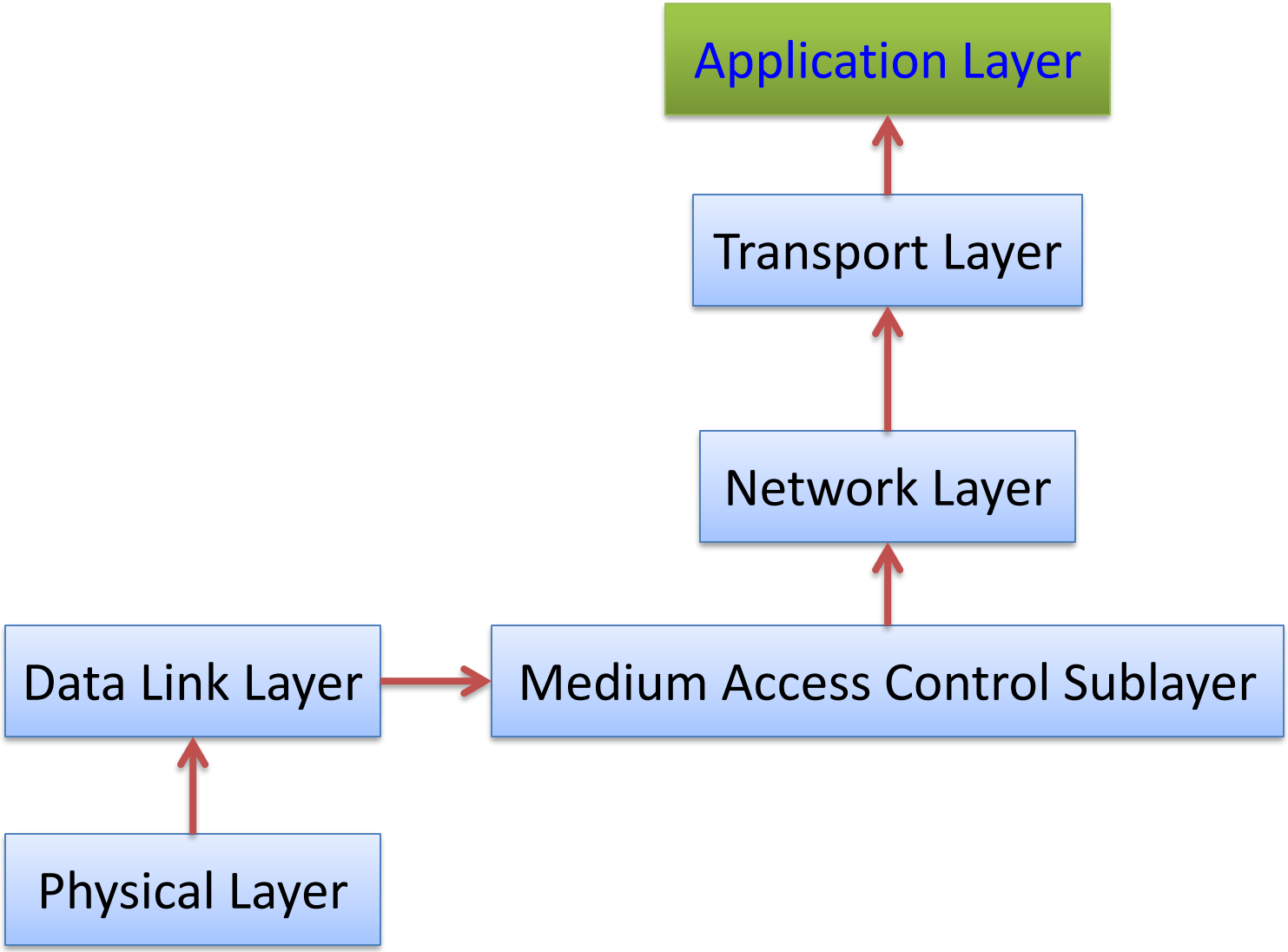
Lecturer: CUI Lin

Department of Computer Science
Jinan University

The Application Layer

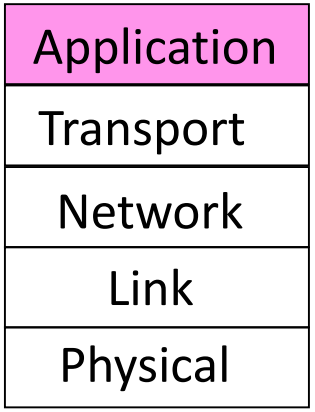
Chapter 7

Roadmap of this course



The Application Layer

- Uses transport services to build applications for users
  - Most use client/server model
  - Also need support protocols, e.g., DHCP



Topics

- DHCP: Dynamic Host Configuration Protocol (Chapter 5.7.4)
- DNS: Domain Name System
- The World Wide Web: HTTP
- Electronic Email

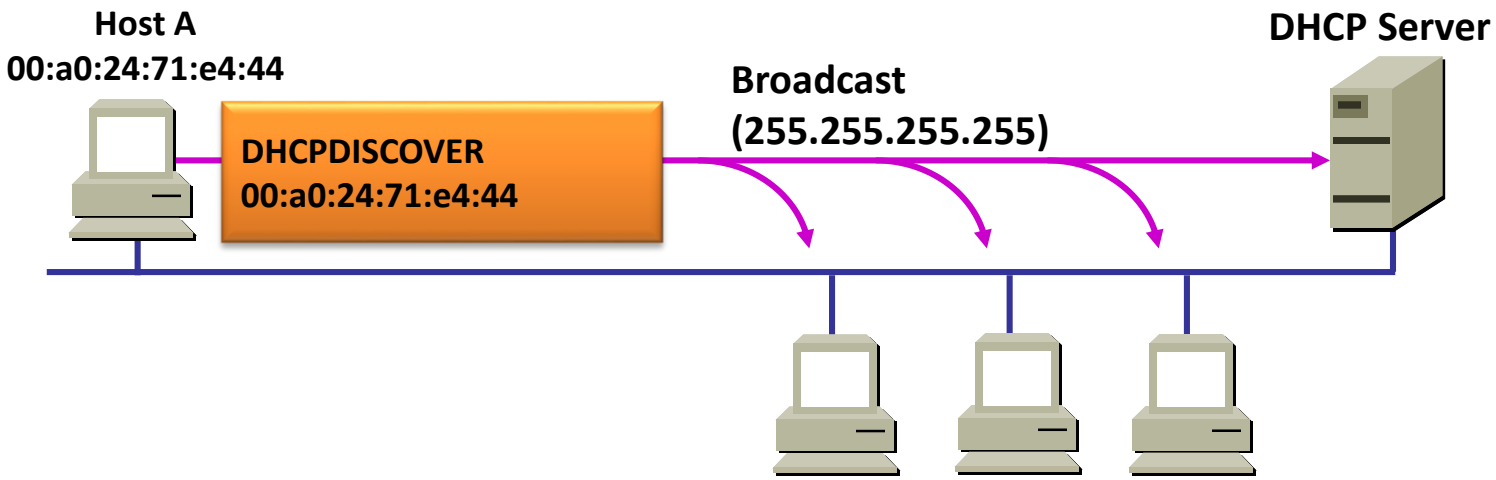
Dynamic Host Configuration Protocol

- DHCP provides plug-and-play networking, no manually work is needed where conflicts are possible
- DHCP can configure:
  - IP address
  - Subnet mask
  - Default gateway
  - DNS gateway

DHCP

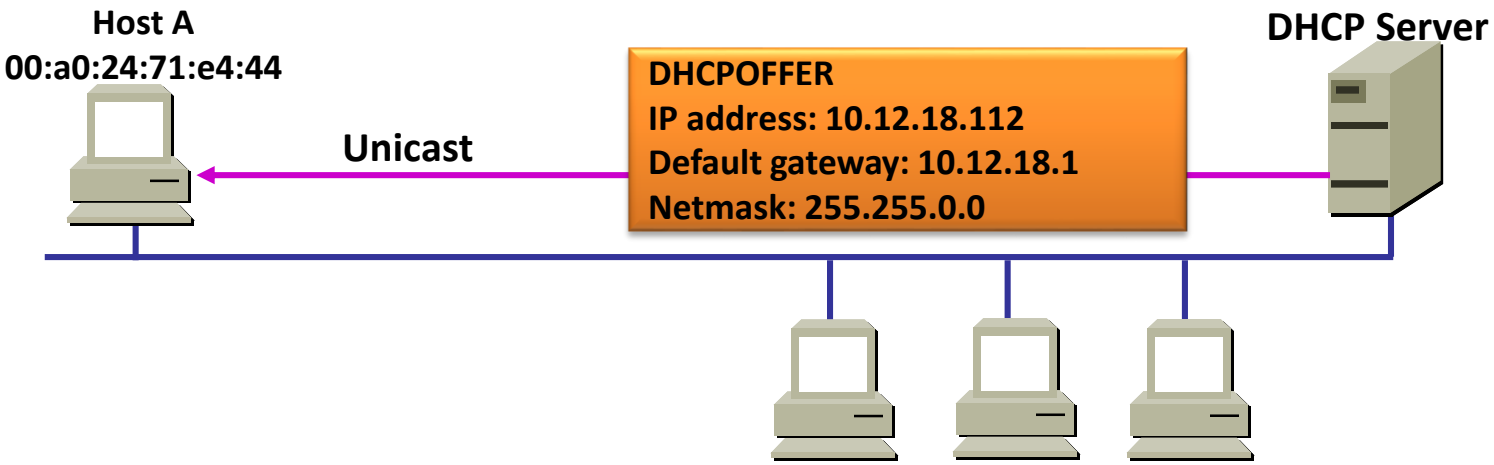
- When computer boots up, it has no IP, but can be identified by Ethernet address
- It broadcasts a DHCP DISCOVER packet, which will be delivered to DHCP server
- Each network has at least one DHCP proxy, which will relay (unicast) the DHCP DISCOVER packet to DHCP server if necessary.
- DHCP server allocates IP address and replies DHCP OFFER packet

DHCP



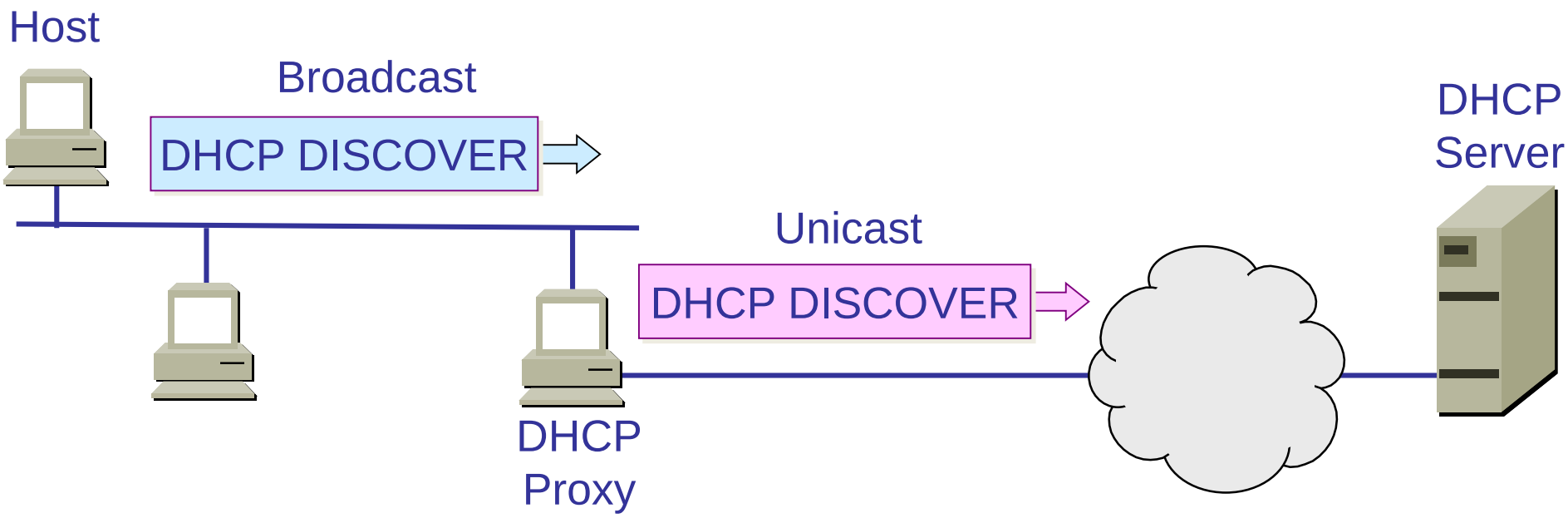
DHCP packets are carried by UDP.
Server: port 67, Host: port 68

DHCP



DHCP packets are carried by UDP.
Server: port 67, Host: port 68

DHCP Proxy



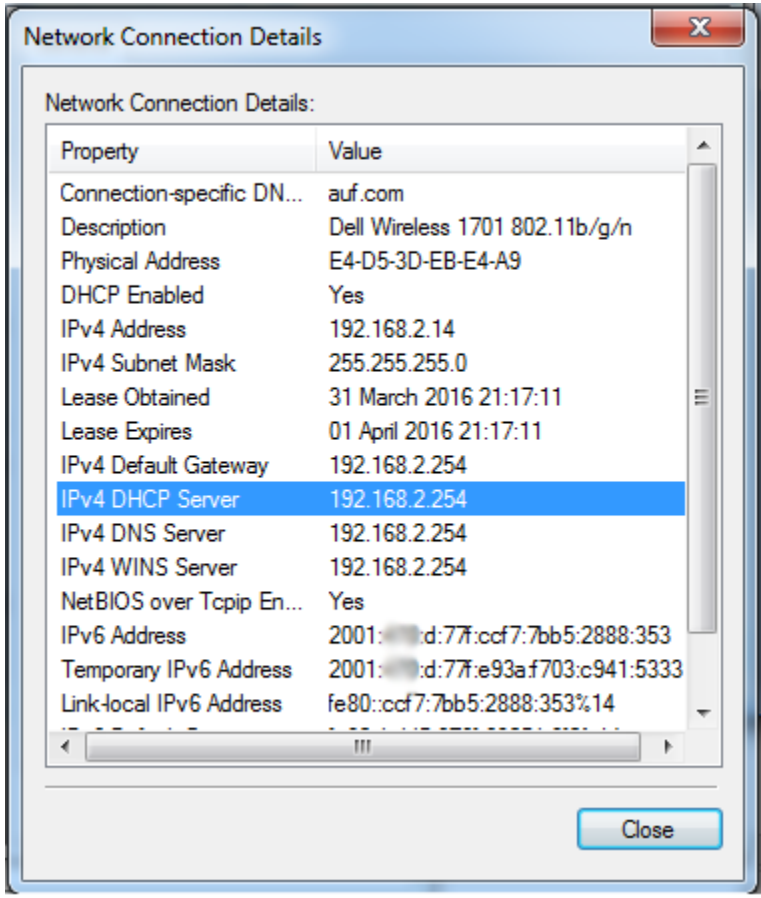
DHCP packets are carried by UDP.
Server: port 67, Host: port 68

DHCP

- Each DHCP server receiving the DHCP DISCOVER will reply DHCP OFFER.
- Host may receive multiple DHCP OFFER packets.
- It will choose one and notify the selected DHCP server.

Lease Period

- Host may leave and don't return the assigned IP to DHCP server
- Solution: IP address assignment is only for a fixed period, i.e., lease period.
- Host can renewal or release the assignment before lease expires.



Topics

- DHCP: Dynamic Host Configuration Protocol (Chapter 5.6.4)
- DNS: Domain Name System
- Electronic Email
- The World Wide Web: HTTP

DNS and Names

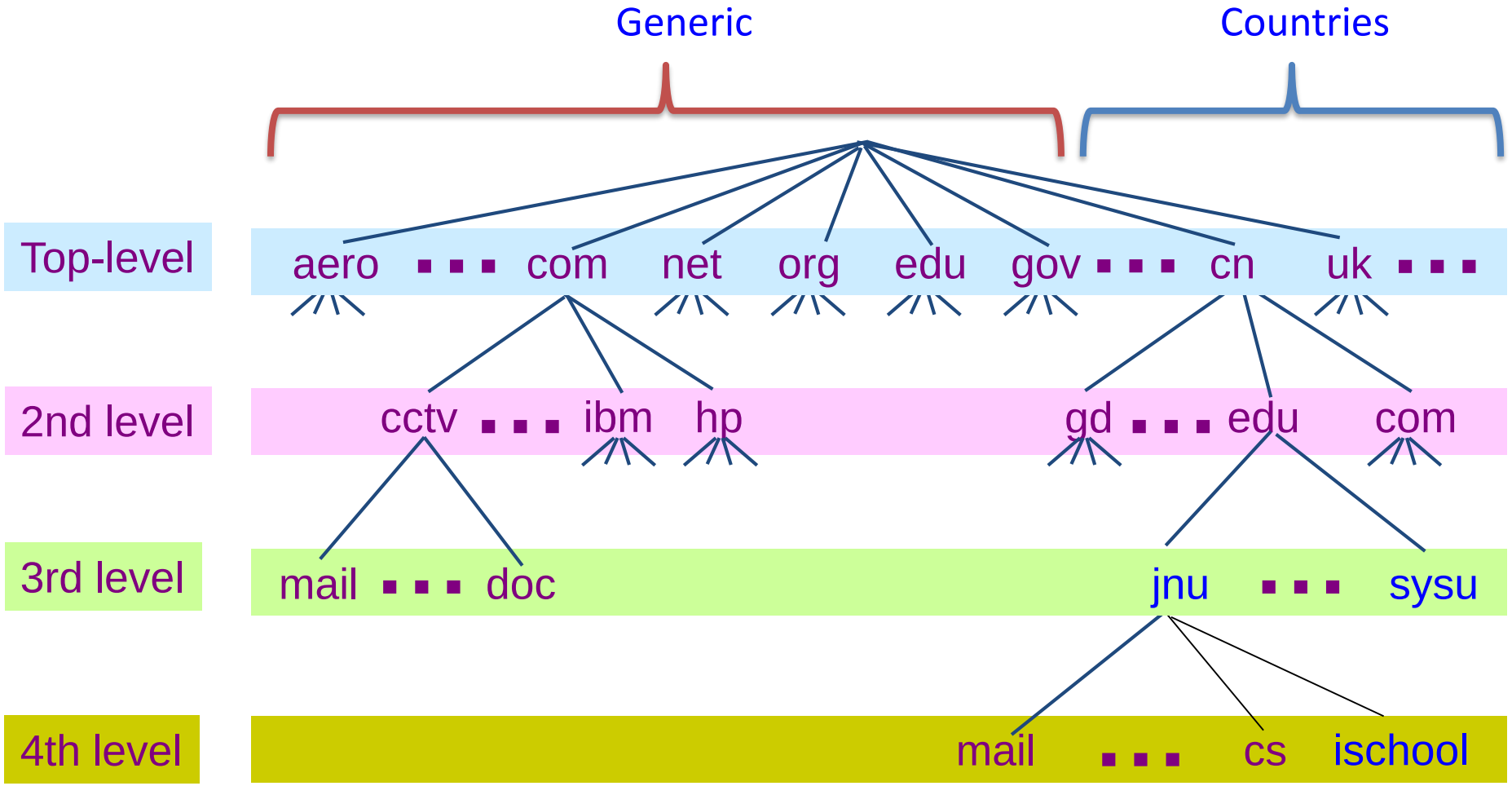
- Internet communication requires IP addresses
- Humans prefer to use computer names
- Need an automated system to translate names to addresses
- Known as Domain Name System (DNS)

Ref. Aug. 25, 2013, a DDoS attack on .CN domain

DNS – Domain Name System

- The DNS resolves high-level human readable names for computers to low-level IP addresses
- DNS is a hierarchical, domain-based naming scheme and a distributed database system, including multiple naming servers.

The DNS Name Space



DNS namespace is hierarchical from the root down

Top-Level Domains

- Over 1506 top-level domains (TLDs) by 2020.11
- Generic domains are controlled by ICANN who appoints registrars to run them
  - com: commercial
  - edu: educational institutions
  - gov: government
  - org: non-profit organization
  - net: network providers
- Country domain: one for each country, support non-Latin alphabets from 2010.
  - cn, uk, jp, hk, .中国, .广东 , .我爱你,.ai,…

TLD DNSSEC Report: http://stats.research.icann.org/dns/tld_report/

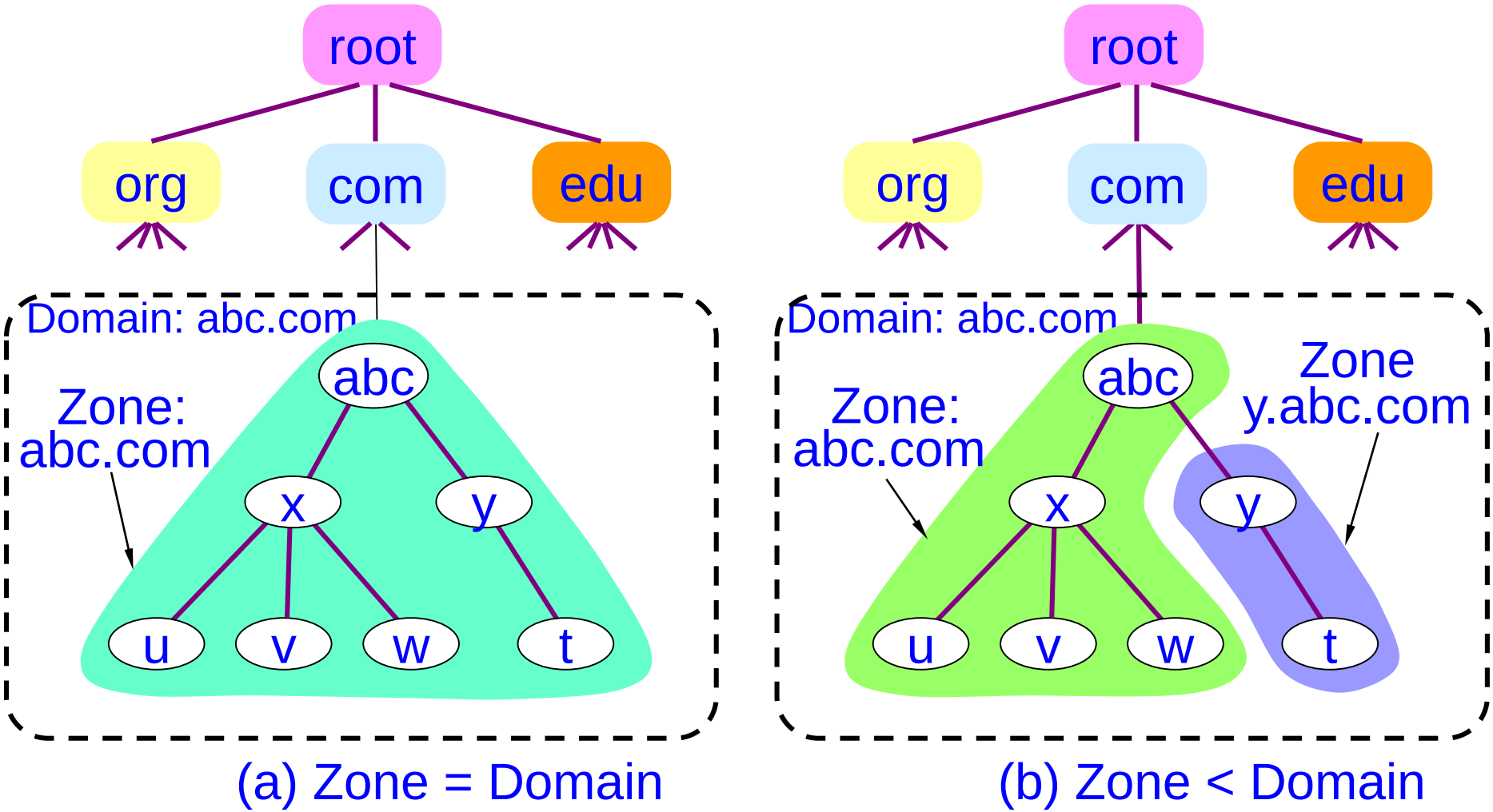
The DNS Name Space

- Each domain is named by the path upward from it to the root, separated by “dot”:
  - cs.jnu.edu.cn
  - jnu.edu.cn
  - gd.cn
- Each component can be up to 63 characters, full path names must not exceed 255 characters

Name Servers

- Name servers contain data for portions of the name space called zones (non-overlapping)
- Each zone has an authoritative name server (授权名称服务器), which is a name server that gives answers in response to questions asked about names in a zone
- Root Name Servers (根域名服务器) have information for each top-level domain (TLD)

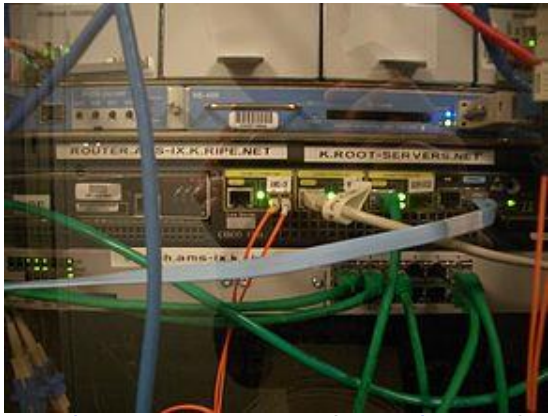
Zone ≠ Domain


root
org
com
edu
Domain: abc.com
Zone:
abc.com
abc
x
y
u
v
w
t
(a) Zone = Domain
root
org
com
edu
Domain: abc.com
Zone:
abc.com
Zone
y.abc.com
abc
x
y
u
v
w
t
(b) Zone < Domain

13 root name servers worldwide, each may contain multiple machines using anycast

- A.ROOT-SERVERS.EDU. (NS.INTERNIC.NET) 198.41.0.4
- B.ROOT-SERVERS.NET. (NS1.ISI.EDU) 192.228.79.201
- C.ROOT-SERVERS.NET. (C.PSI.NET) 192.33.4.12
- D.ROOT-SERVERS.NET. (TERP.UMD.EDU) 128.8.10.90
- E.ROOT-SERVERS.NET. (NS.NASA.GOV) 192.203.23
- F.ROOT-SERVERS.NET. (NS.ISC.ORG) 192.5.5.241
- G.ROOT-SERVERS.NET. (NS.NIC.DDN.MIL) 192.112.36.4
- H.ROOT-SERVERS.NET. (AOS.ARL.ARMY.MIL) 128.63.2.53
- I.ROOT-SERVERS.NET. (NIC.NORDU.NET) 192.36.148.17
- J.ROOT-SERVERS.NET. (VeriSign) 198.41.0.10
- K.ROOT-SERVERS.NET. (RIPE NCC) 193.0.14.129
- L.ROOT-SERVERS.NET. (ICANN) 198.32.64
- M.ROOT-SERVERS.NET. (WIDE, Japan) 202.12.27.33

http://www.root-servers.org/



A Cisco 7301 router and a Juniper M7i, part of the K root-server instance at AMS-IX (Amsterdam Internet Exchange).

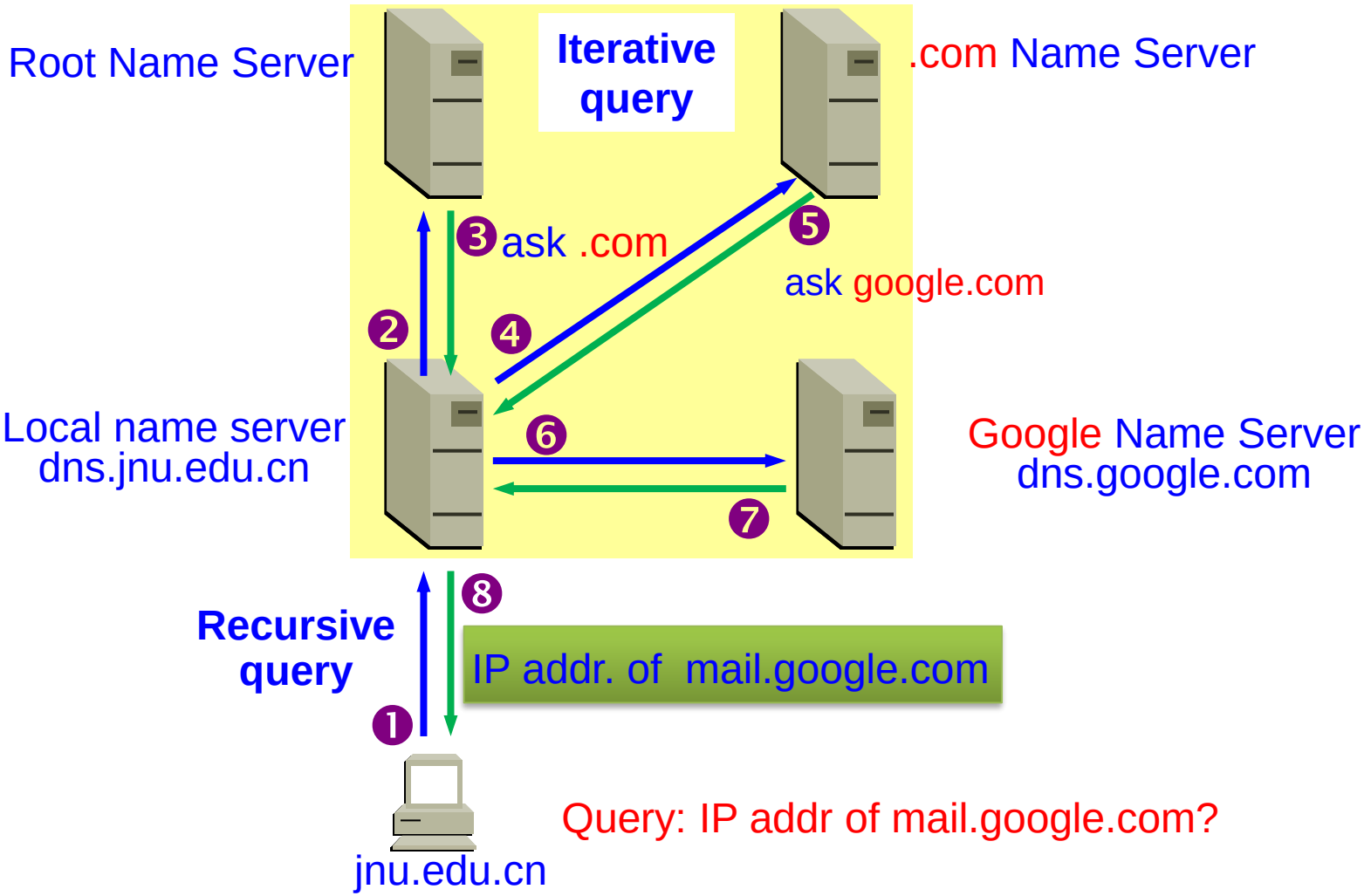
Recursive/Iterative Queries

- There are two types of queries:
  - Recursive queries
  - Iterative (non-recursive) queries
- The type of query is determined by a bit in the DNS query
- Recursive query (递归查询): When the name server of a host cannot resolve a query, the server issues a query to resolve the query
- Iterative queries(迭代查询): When the name server of a host cannot resolve a query, it sends a referral to another server to the resolver

Resolution (解析)

- Finding the IP address for a given hostname is called resolution and is done with the DNS protocol
  - Host usually sends a recursive query to the local name server
  - If the local name server cannot answer, the local name server becomes DNS client, sending iterative queries to other name server
- DNS protocol:
  - Runs on UDP port 53, retransmits lost messages

Iterative queries for local name server



DNS Cache

- To reduce DNS traffic, name servers caches information on domain name/IP address mappings
  - All answers, including partial answers, will be cached on name servers.
  - Greatly reduces steps in a query and improves performance
  - Cache entries expires after Time_to_live
  - Note: If an entry is sent from a cache, the reply from the server is marked as “unauthoritative”

DNS Records

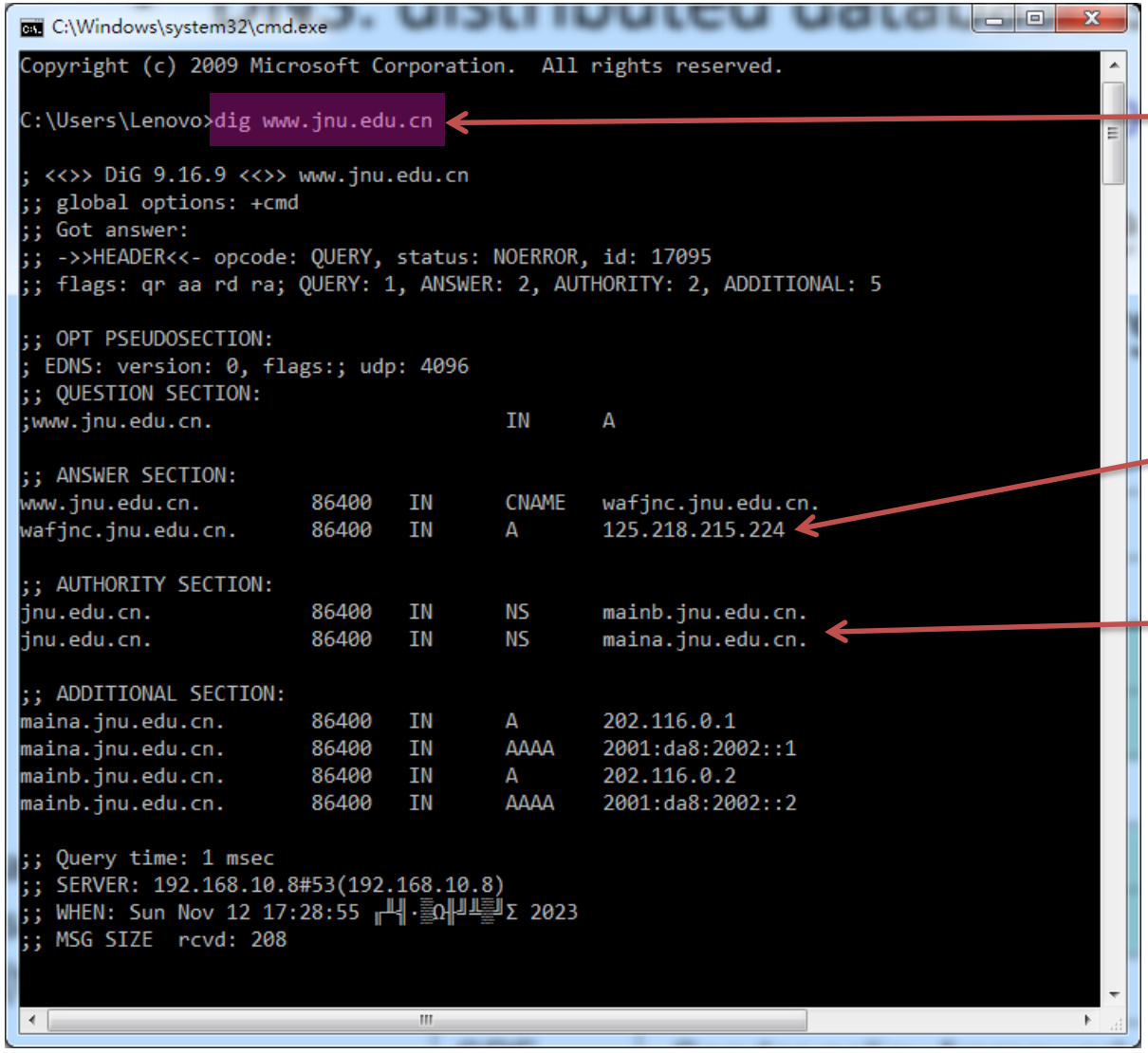
- DNS: distributed database storing resource records (RR)
  - RR format: (name, value, type, ttl)
- Key resource records in the namespace are IP addr. (A/AAAA) and name servers (NS), but there are others too (e.g., MX)

Mail server

alias name for some "canonical" (the real) name

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text

DNS Records Example (using *dig*)



Query for:
www.jnu.edu.cn

IP addresses of
www.jnu.edu.cn

Name server

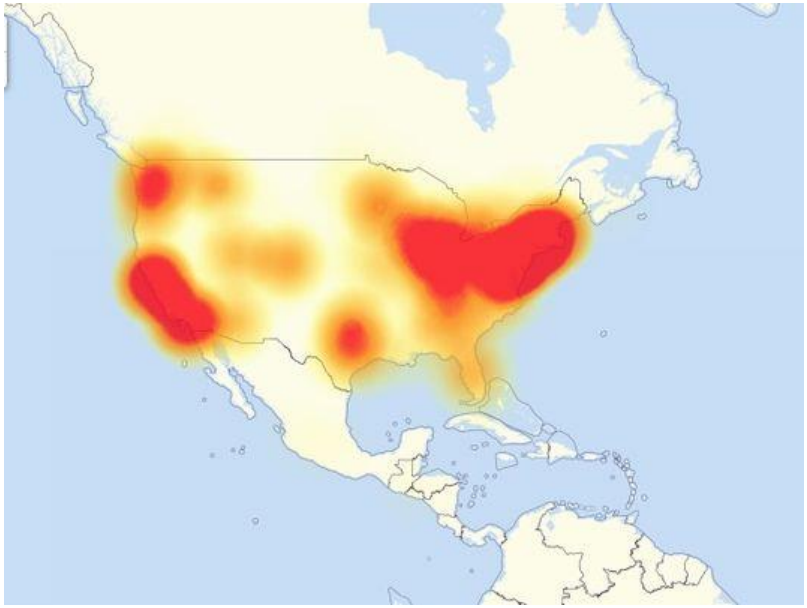
DNS more…

- On windows:
  - *ipconfig /displaydns* to show local DNS cache
  - *nslookup [domain name]*
  - *hosts* file for windows:
    "C:\Windows\System32\drivers\etc"
- Google public DNS:
  - IPv4: 8.8.8.8 and 8.8.4.4
  - IPv6: 2001:4860:4860::8888 and 2001:4860:4860::8844

DNS spoofing/poisoning

2016 Dyn cyberattack

- Oct 21, 2016, DoS attacks targeting DNS provider Dyn made major Internet platforms and services unavailable to large swathes of users in Europe and North America.
- Hacked home devices caused massive Internet outage



More info: https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

Linux.org's DNS Got Hijacked

- The domain of “Linux.org” was Hijacked on 2018.12.07
- Linux.org was pointed to a page exclaiming "G3T 0WNED L1NUX N3RDZ", which also included a NSFW picture, some abusive language, etc.
- More details

A bit more about Root Name Server

- The DNS root zone is the top-level DNS zone, served by 13 root server clusters
- Root zone file (about 2 MB): a list of names and IP addresses of the authoritative DNS servers for TLDs
  - Before 2016, controlled by National Telecommunications and Information Administration (NTIA) of the United States Department of Commerce
  - Since 2016.09, it has been overseen by the ICANN
- As of 2023-11-12, the root server system consists of 1766 instances operated by the 12 independent root server operators.

Root name server in China

- Sep. 3rd, 2019: First ICANN Managed Root Server Instance (L) Installed in Shanghai
- By Nov. 2023:
  - 8 in Beijing,
  - 3 in Guangzhou (A, L, K)
  - 2: Zhengzhou, Xi'ning, Wuhan, Hangzhou, Shanghai, Kunming
  - 1: Nanning, Shenyang, Chongqing, Haikou, Guiyang
  - 9 in Hong Kong, 10 in Taiwan

DNS and IPv6 in China

- 2017-11-26:
  - The General Office of the State Council of P.R. China issued an action plan for promoting the large-scale deployment of Internet Protocol Version 6 (IPv6).
  - The plan points out the significance of IPv6, and the general requirements and major goals of the work, including in terms of internet infrastructure and network security.

国务院办公厅印发《推进互联网协议第六版（IPv6）规模部署行动计划》

Yeti DNS Project (雪人计划)

- 2017-11-27:
  - Participants: China, Japan, USA…
  - 25 IPv6 root name servers have been deployed, 4 of them are in China
  - First Public IPv6 DNS:
    - Primary: 240c::6666
    - Secondary: 240c::6644

https://www.yeti-dns.org/


C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\Users\ >ping -6 240c::6666
正在 Ping 240c::6666 具有 32 字节的数据:
来自 240c::6666 的回复: 时间=182ms
来自 240c::6666 的回复: 时间=190ms
来自 240c::6666 的回复: 时间=164ms
240c::6666 的 Ping 统计信息:
数据包: 已发送 = 3, 已接收 = 3, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 164ms, 最长 = 190ms, 平均 = 178ms
Control-C
^C
C:\Users\ >nslookup -qt=AAAA www.cnnic.cn 240c::6666
服务器: UnKnown
Address: 240c::6666
DNS request timed out.
timeout was 2 seconds.
非权威应答:
名称: www.cnnic.cn
Address: 2001:dc7:dd01:0:218:241:97:42

DNS over HTTPS

- DNS over HTTPS (DoH)
  - Perform remote DNS resolution via the HTTPS protocol
  - Increase user privacy and security by preventing eavesdropping and manipulation of DNS data by man-in-the-middle attacks
  - Google and the Mozilla Foundation are testing/deploying versions of DNS over HTTPS

Thank you!

Q & A