Network Security: The basics

Debdeep Mukhopadhyay
and Mainack Mondal

CS 60065
Autumn 2020

What is url?

- Uniform Resource Locators (URLs)
  - a standardized format to describe the location and access method of resources via the internet

<scheme>://<user>:<password>@<host>:<port>/<url-path>?<query-string>

What is url?

- Uniform Resource Locators (URLs)
  - a standardized format to describe the location and access method of resources via the internet

<scheme>://<user>:<password>@<host>:<port>/<url-path>?<query-string>

<https>://<user>:<password>@profile.facebook.com:<port>/x.html?q=user

What is url?

- Uniform Resource Locators (URLs)
  - a standardized format to describe the location and access method of resources via the internet

<scheme>://<user>:<password>@<host>:<port>/<url-path>?<query-string>

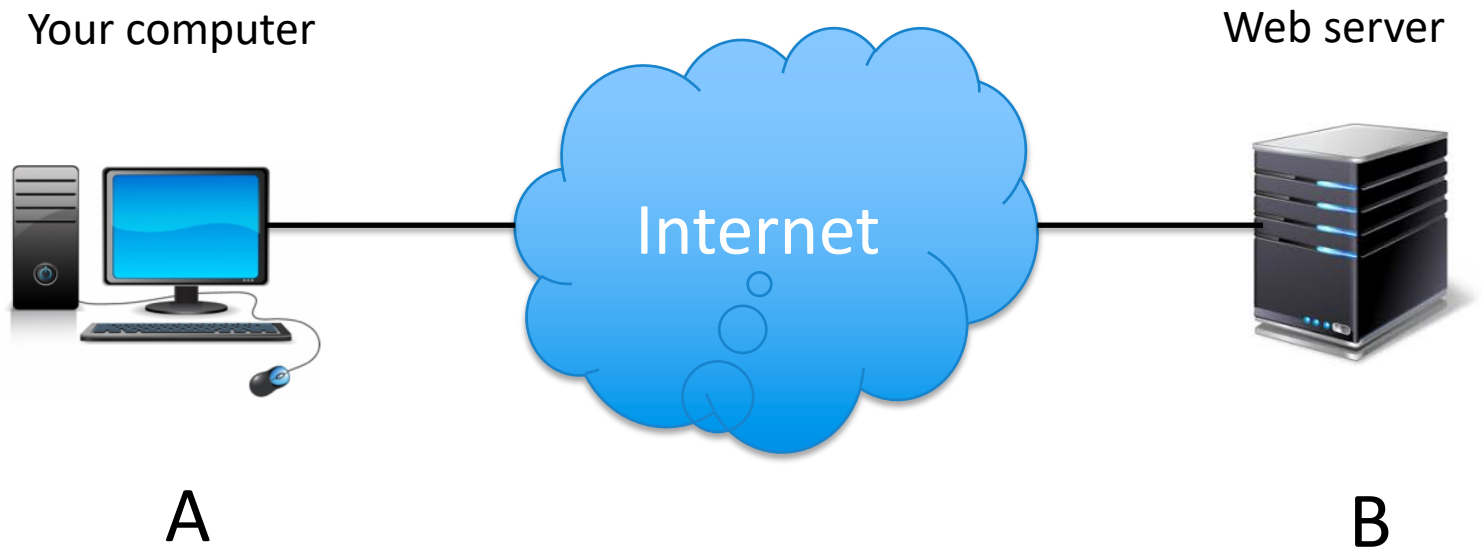
<https>://~~<user>:<password>~~@profile.facebook.com:~~<port>~~/x.html?q=user

<subdomain>.<domain>.<topdomain>

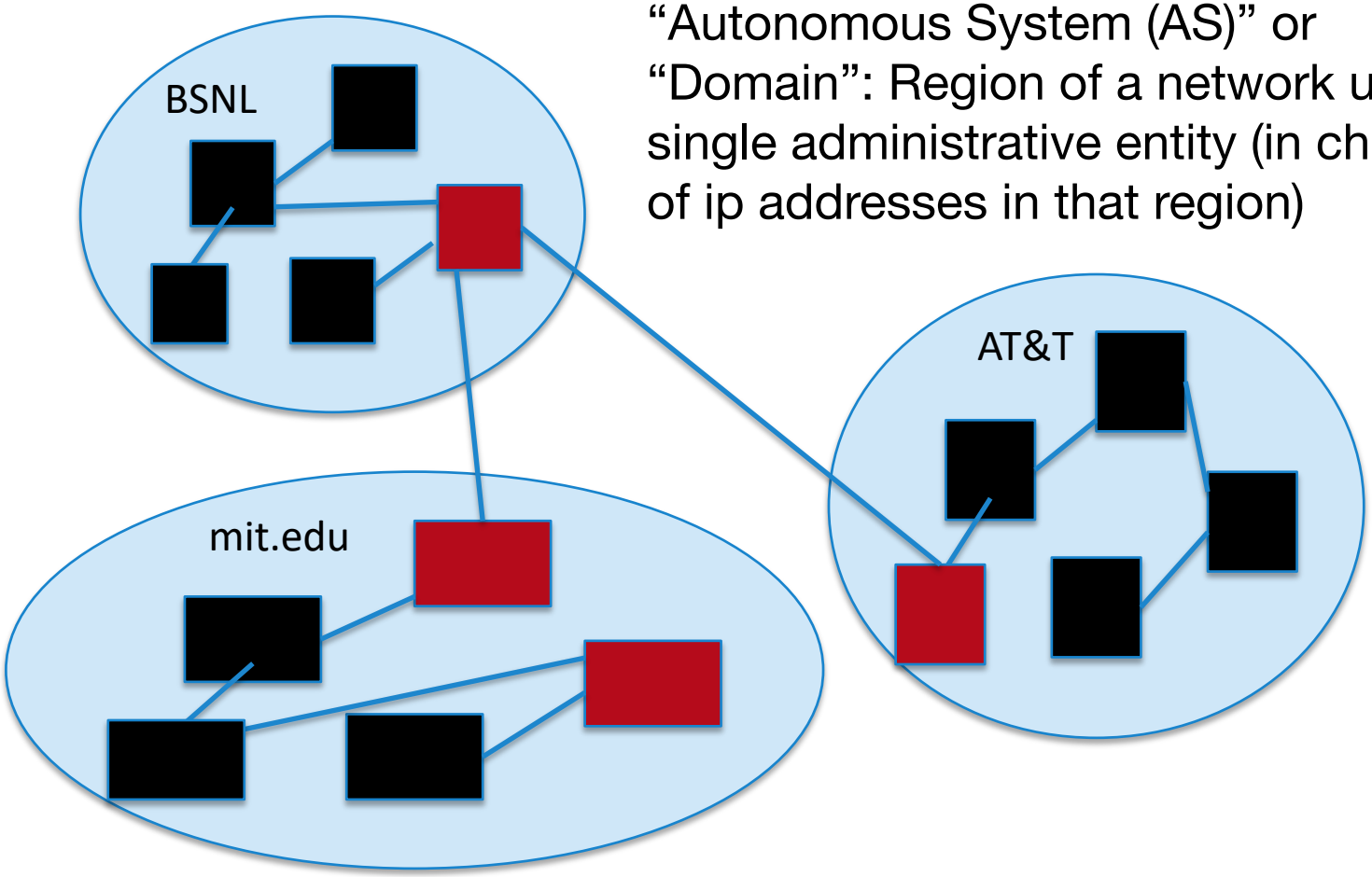
profile.facebook.com

Basics of Computer networks

Basic task of internet



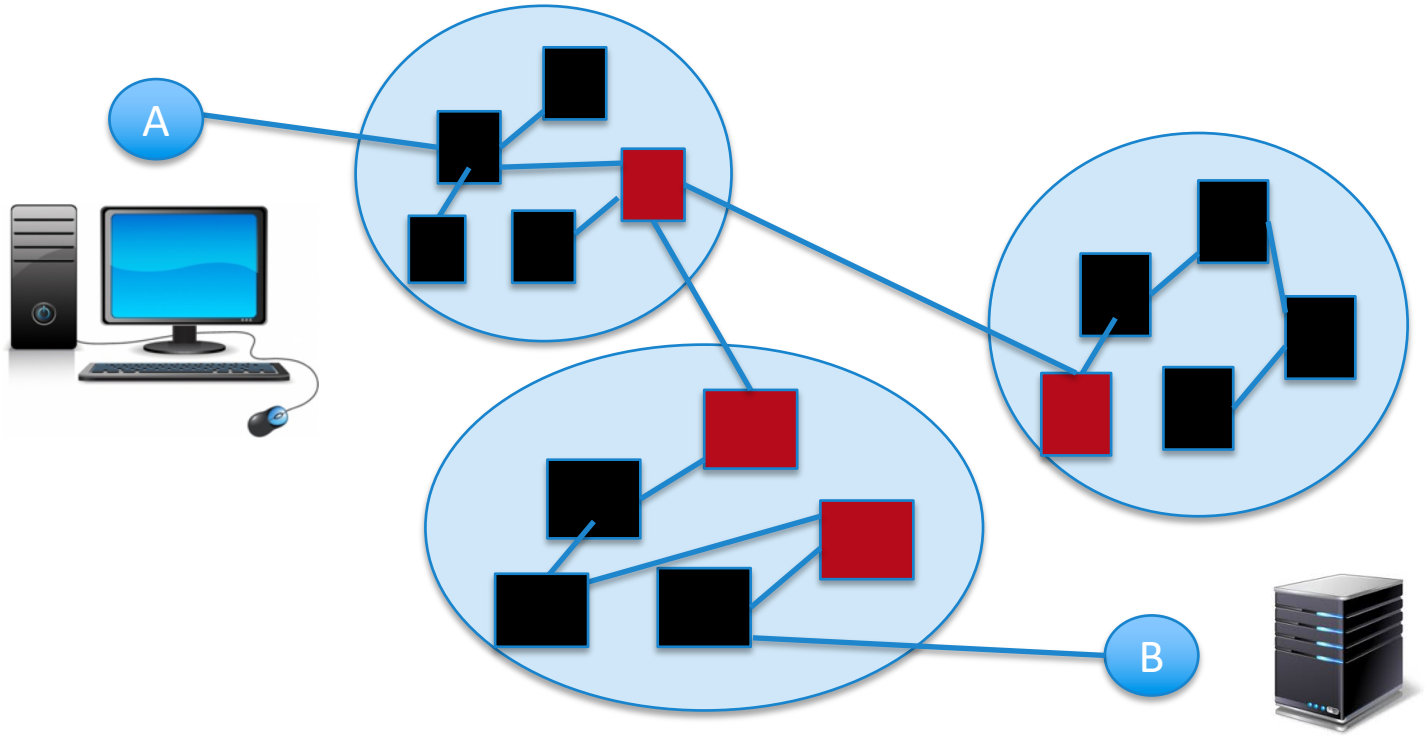
The internet at a glance



"Autonomous System (AS)" or "Domain": Region of a network under a single administrative entity (in change of ip addresses in that region)

Check: https://bgp.potaroo.net/cidr/autnums.html

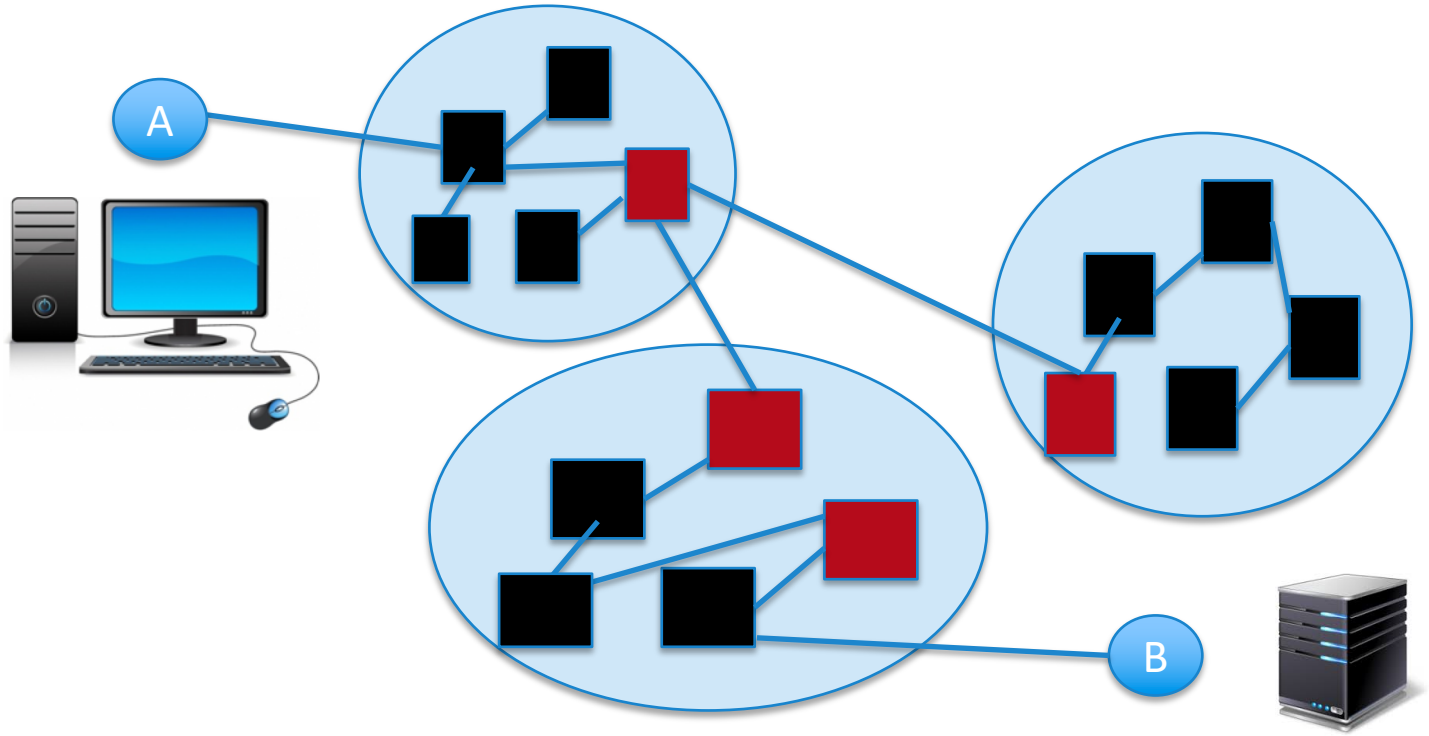
Networking questions: basic diagram



Networking questions: basic diagram

How are machines/devices named?
IP addressing & allocation

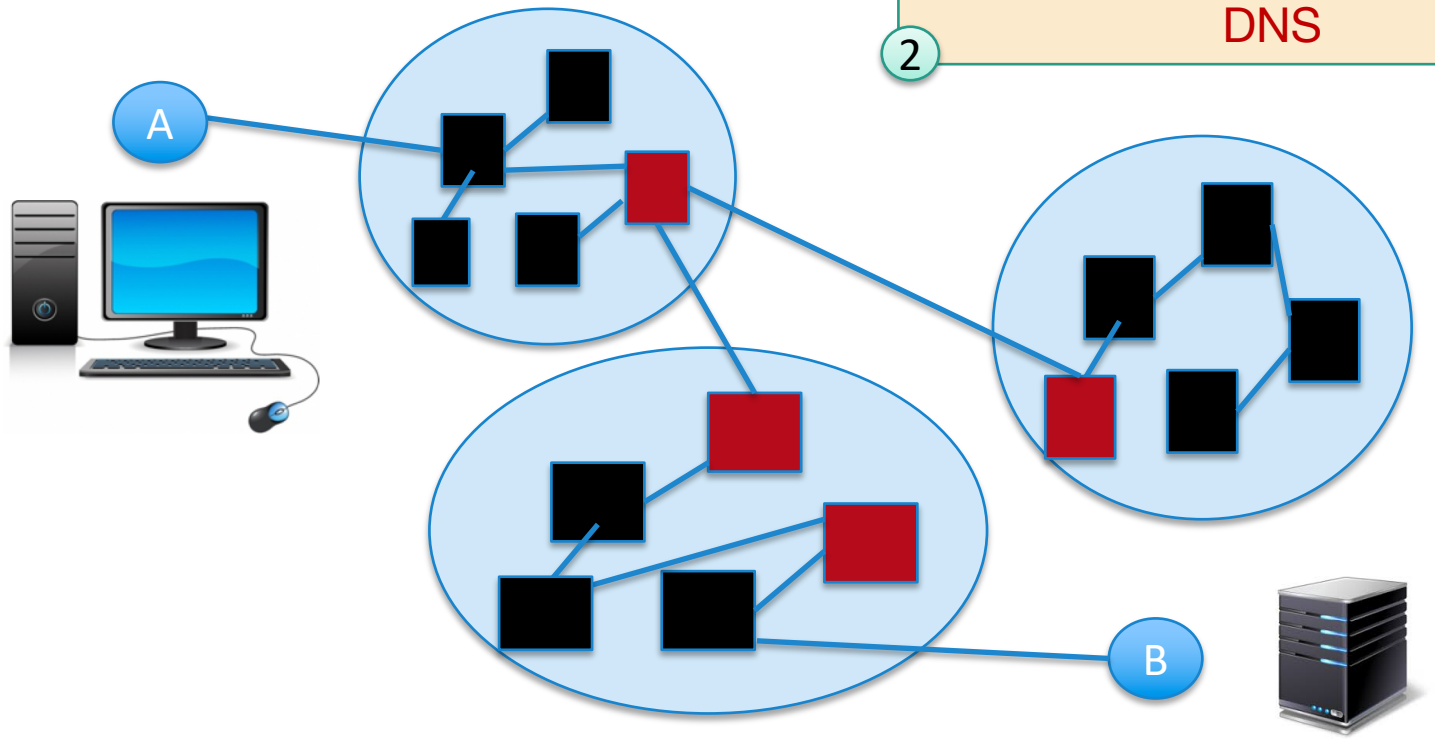
1



Networking questions: basic diagram

1 How are machines/devices named?
IP addressing & allocation

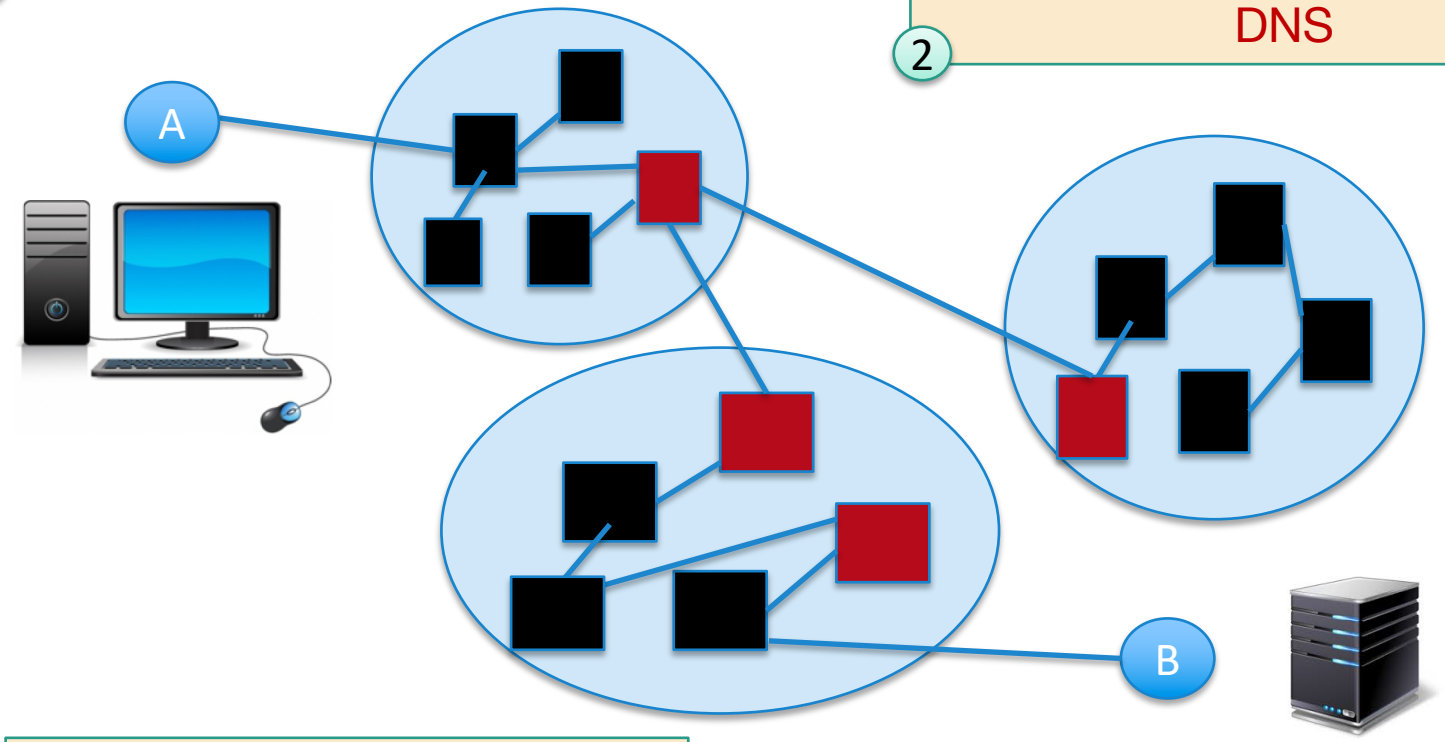
2 How Does A discover B's name?
DNS



Networking questions: basic diagram

1 How are machines/devices named?
IP addressing & allocation

2 How Does A discover B's name?
DNS

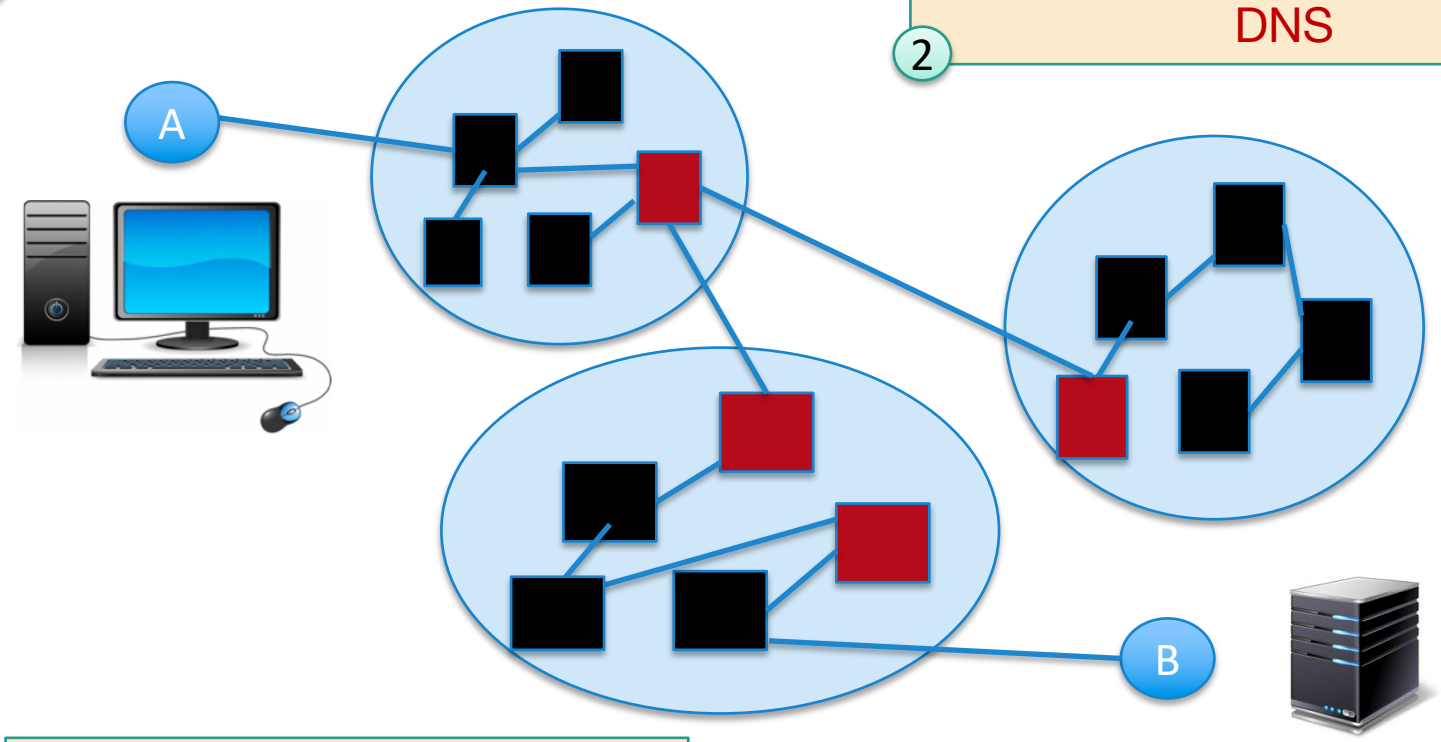


3 How Does A find a path to B?
Routing

Networking questions: basic diagram

1 How are machines/devices named?
IP addressing & allocation

2 How Does A discover B's name?
DNS

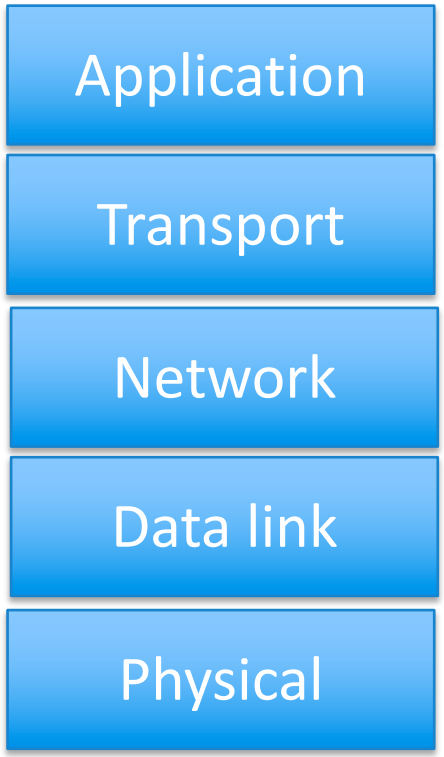


3 How Does A find a path to B?
Routing

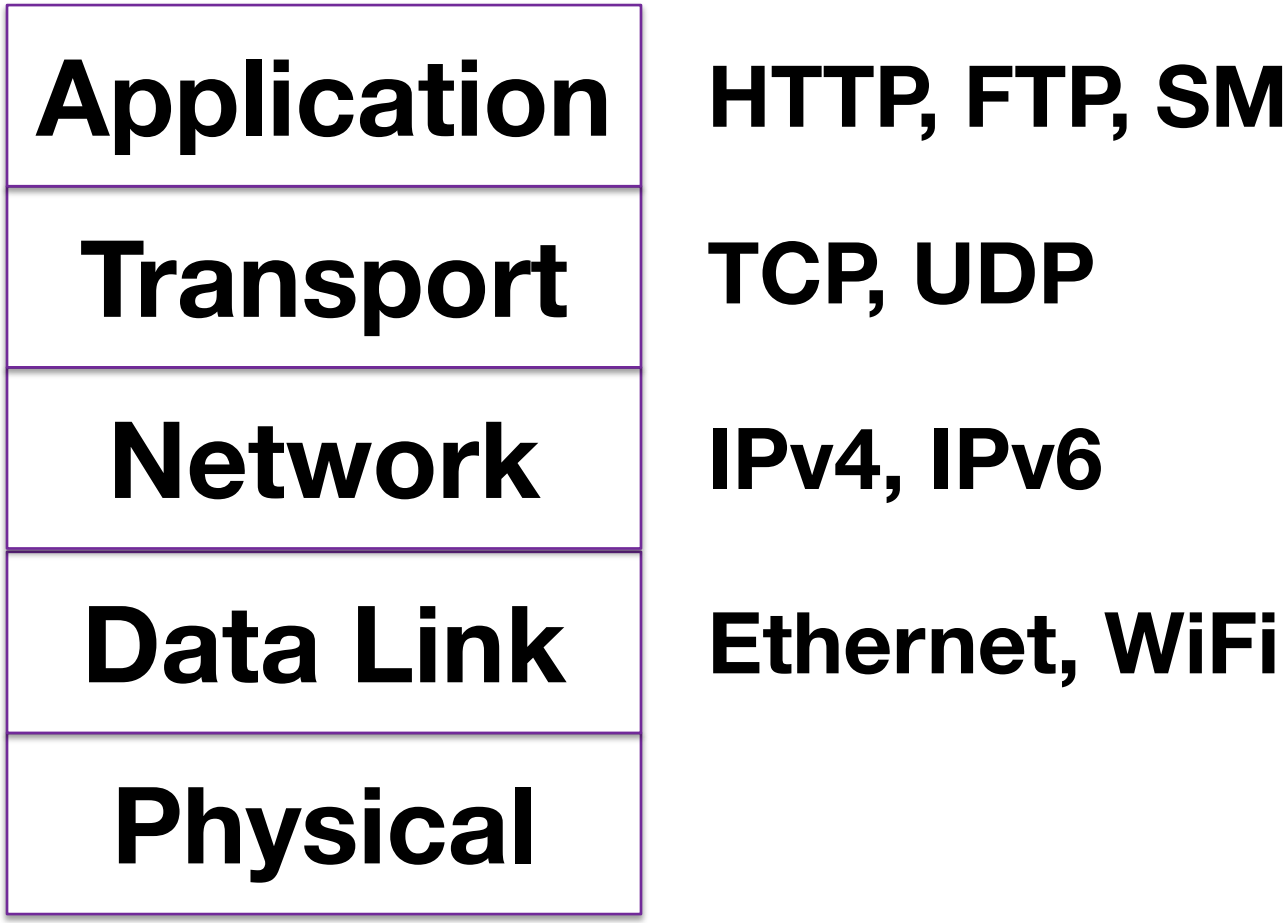
4 How do A and B send data to each other
TCP, UDP

Network layers

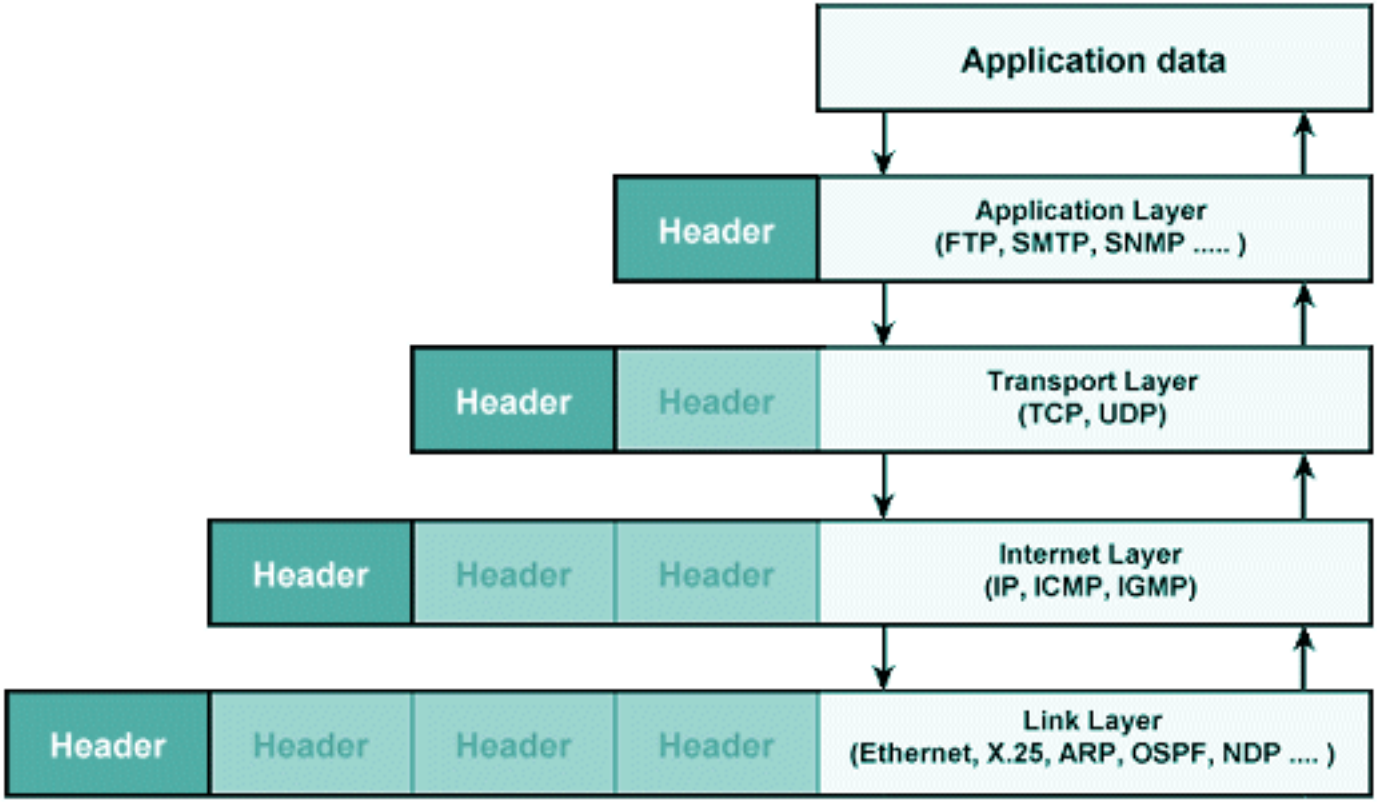
- One layer interacts only with layer above and layer below
- Two layers interact only through the interface between them



Protocols in these different layers



Layer encapsulation

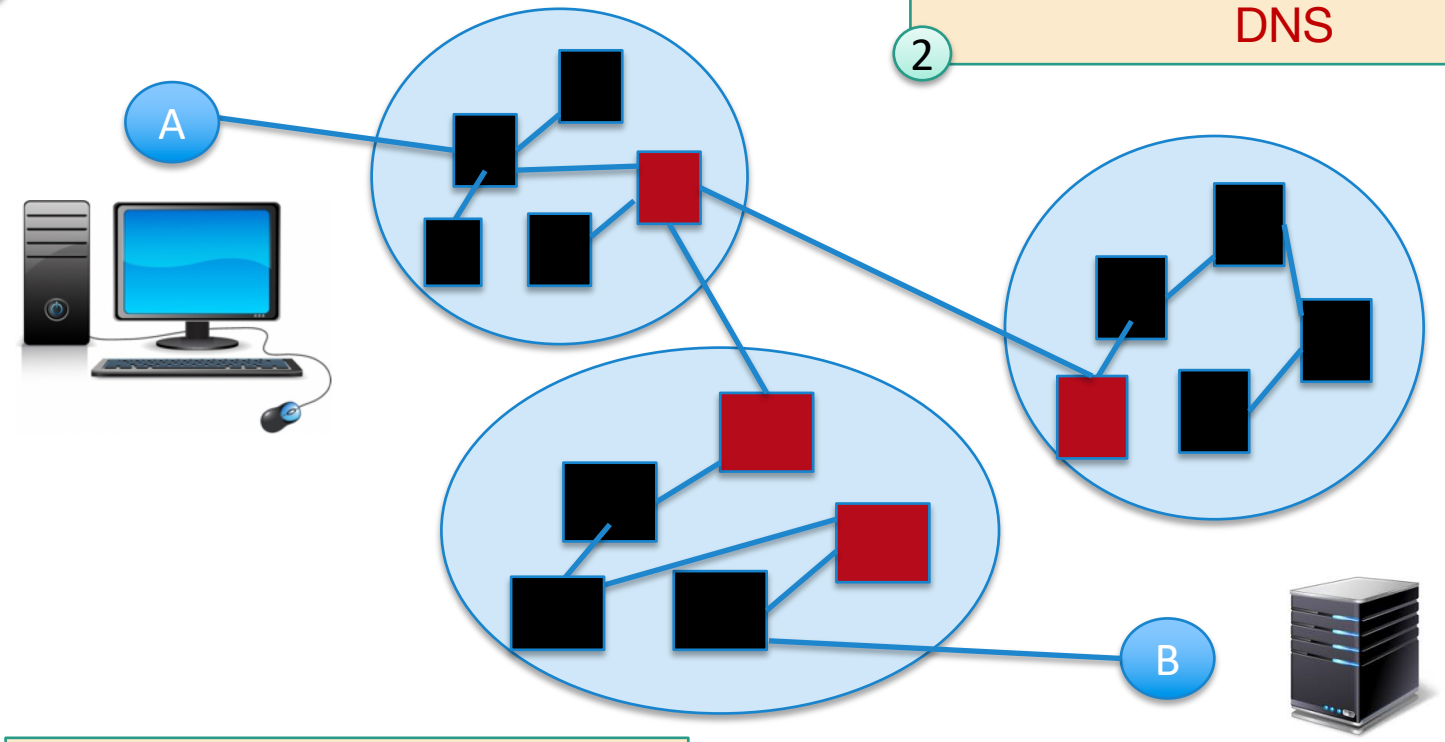


Source: http://www.technologyuk.net/telecommunications/internet/images/tcp_ip_encapsulation.gif

Recap

1. How are machines/devices named?
IP addressing & allocation

2. How Does A discover B's name?
DNS



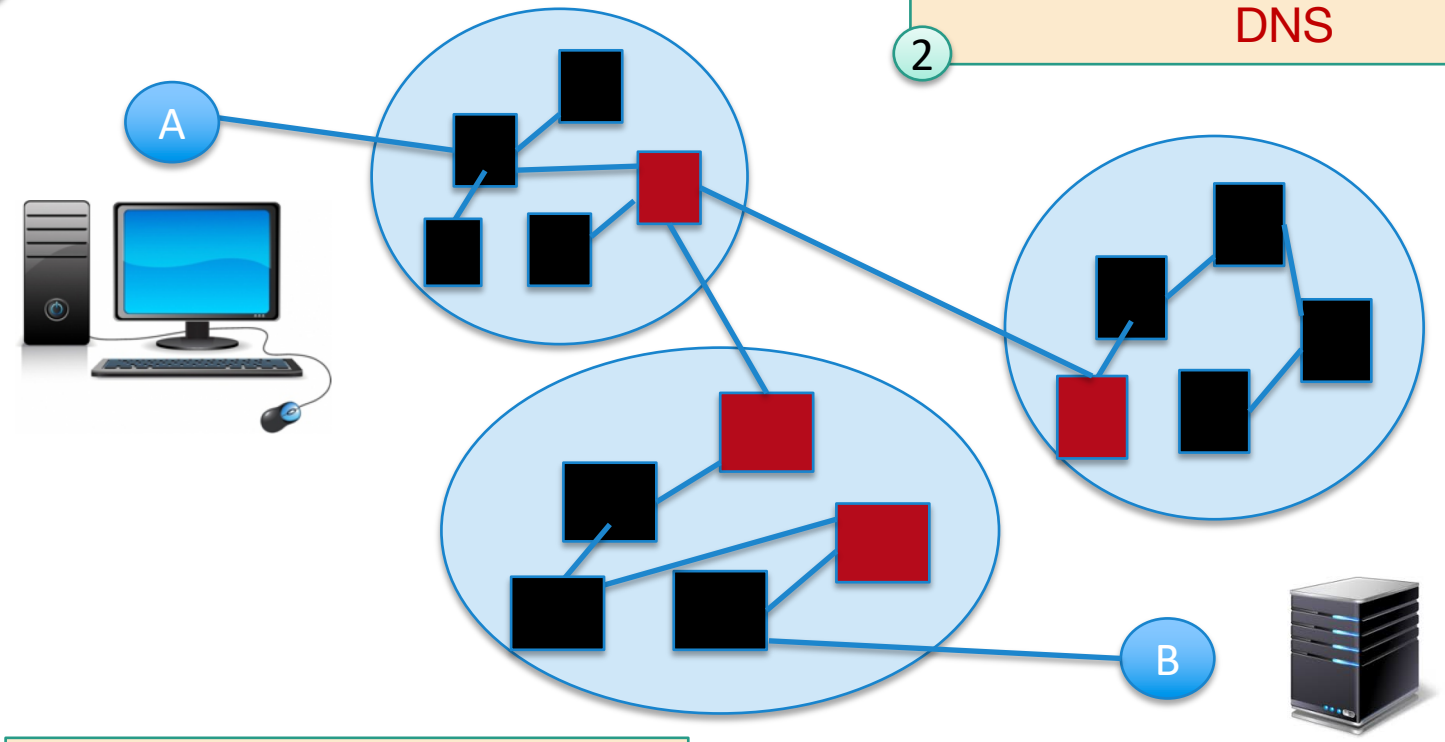
3. How Does A find a path to B?
Routing

4. How do A and B send data to each other
TCP, UDP

Recap

1 How are machines/devices named?
IP addressing & allocation

2 How Does A discover B's name?
DNS



3 How Does A find a path to B?
Routing

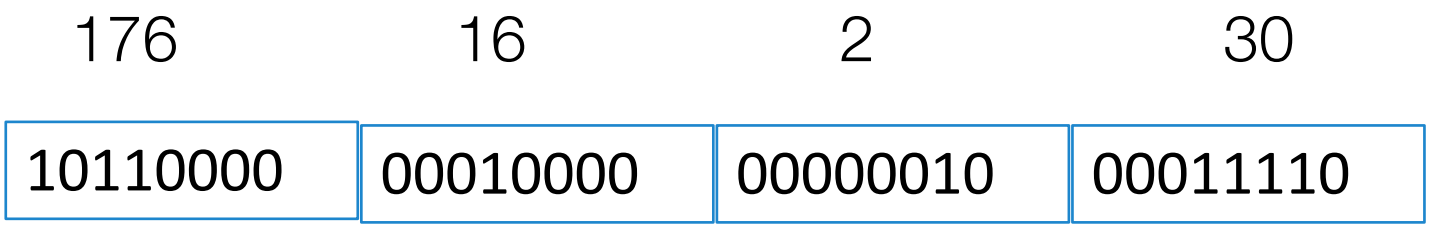
4 How do A and B send data to each other
TCP, UDP

IP addresses (IPv4)

- Unique 32-bit number associated with host

  10110000 00010000 00000010 00011110

- Represented with “dotted quad” notation – e.g., 172.16.2.30



Division of IPv4

- 32 bits are partitioned into a prefix and suffix component
  - Prefix is the network component
  - Suffix is host component

176	16	2	30
10110000	00010000	00000010	00011110

Network bits (23 bits in this case) + host bits (9 bits)

Interdomain routing works on the network prefix
Number of network bits are flexible
Look up CIDR (if network bits are 23 then written as 176.16.2.30/23)

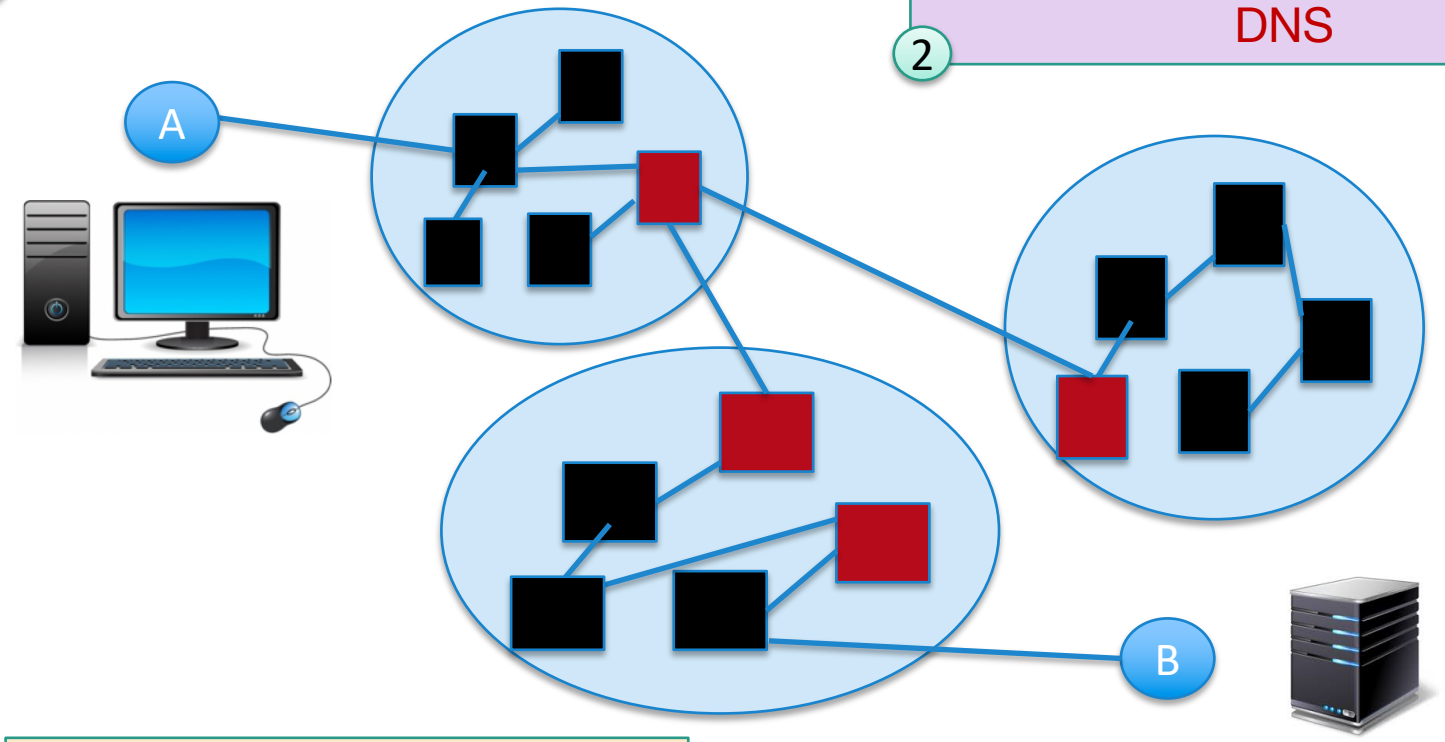
Each interface in your computer gets an ip

So your WIFI will get one IP address and your wired network connection will get another IP address

Recap

1. How are machines/devices named?
IP addressing & allocation

2. How Does A discover B's name?
DNS



3. How Does A find a path to B?
Routing

4. How do A and B send data to each other
TCP, UDP

DNS (Domain name service)

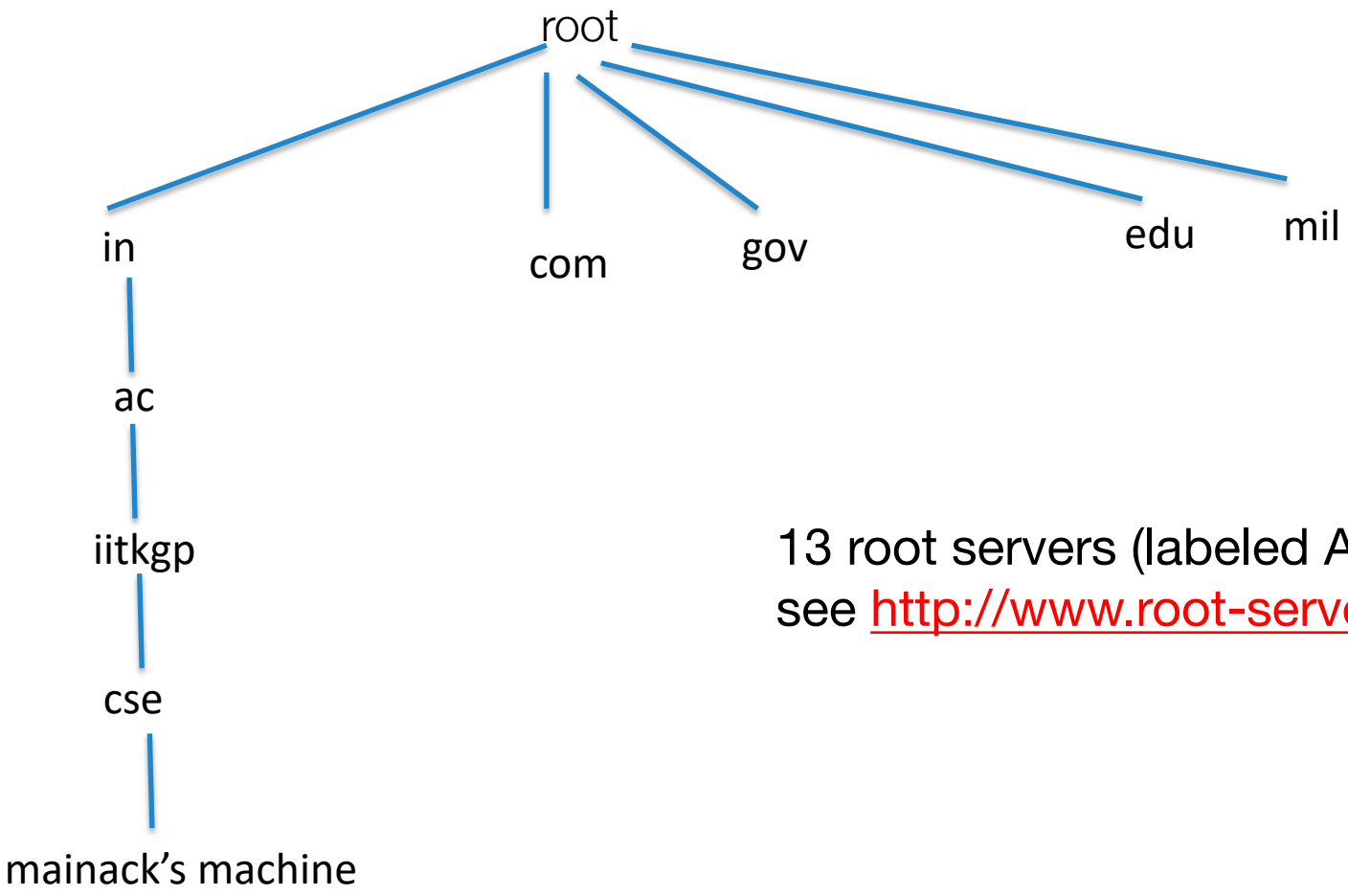
- DNS: Map names to ip addresses
  - Use “dig”

```
mbk-52-31% dig google.com

; <<>> DiG 9.10.6 <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52686
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             286     IN      A       172.217.166.206

;; AUTHORITY SECTION:
google.com.             8526    IN      NS      ns2.google.com.
google.com.             8526    IN      NS      ns3.google.com.
google.com.             8526    IN      NS      ns1.google.com.
google.com.             8526    IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns3.google.com.         41948   IN      A       216.239.36.10
ns3.google.com.         41948   IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         41948   IN      A       216.239.38.10
ns4.google.com.         41948   IN      AAAA    2001:4860:4802:38::a
ns1.google.com.         41948   IN      A       216.239.32.10
ns1.google.com.         41948   IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         41948   IN      A       216.239.34.10
ns2.google.com.         41948   IN      AAAA    2001:4860:4802:34::a

;; Query time: 9 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Wed Sep 16 03:40:51 IST 2020
;; MSG SIZE  rcvd: 303
```

DNS records

- DNS servers store resource records (RRs)
  - RR is (name, value, type, TTL)
- Type = A: (Address) or AAAA (for IPV6)
  - name = hostname
  - value = IP address
- Type = NS: (Name Server)
  - name = domain
  - value = name of dns server for domain
- Type = MX: (Mail eXchanger)
  - name = domain in email address
  - value = name(s) of mail

DNS is hierarchical



13 root servers (labeled A-M;
see http://www.root-servers.org/)

How would I get an IP using DNS?

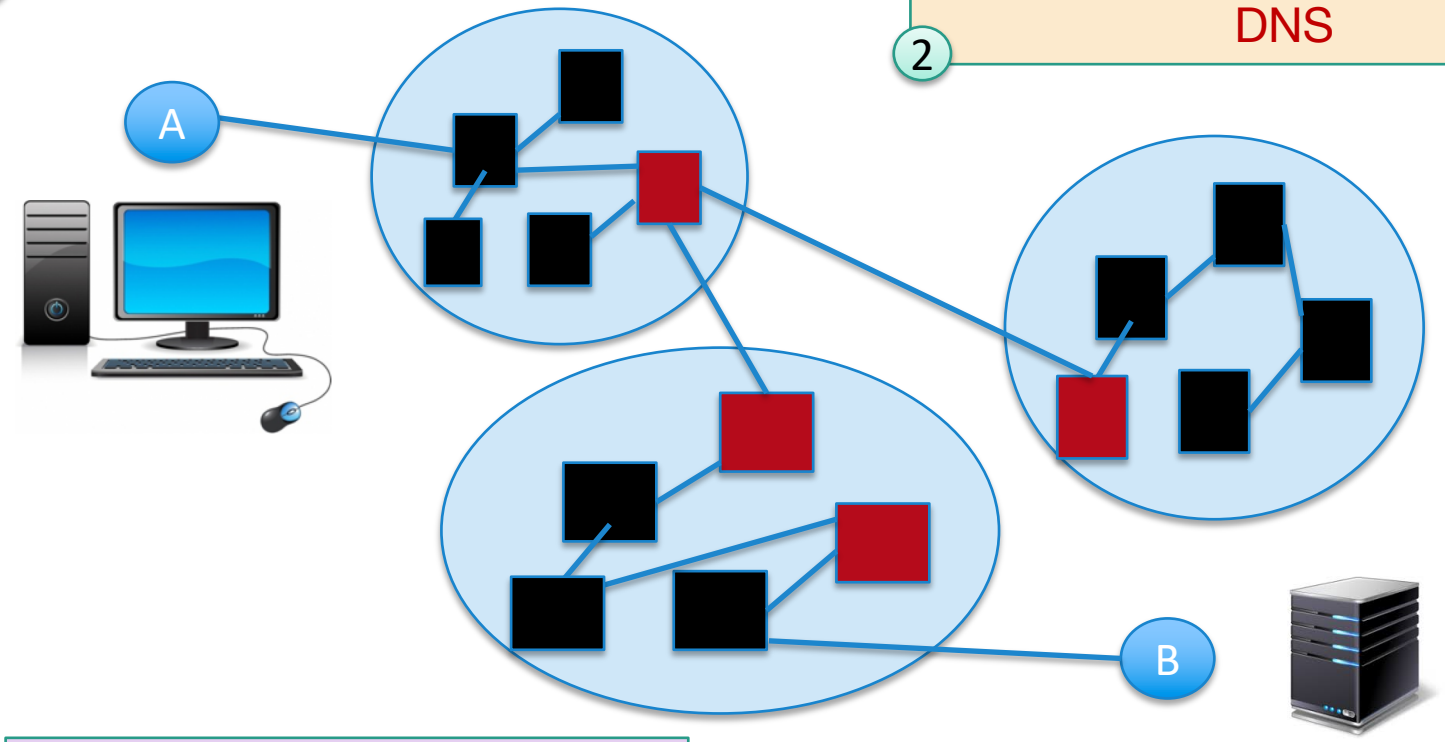
- Happens recursively/iteratively
- Say I am in IIT Kgp and want to access “chris.cs.nyu.edu”
  - My machine will first query local DNS server at IIT Kgp
  - If the name to address mapping is in the cache: return

    else: go to upper level dns server
  - The upper level dns server does the same till it hits a DNS server which contains address of “.edu” domains
  - Then it will go down the hierarchy to find “nyu.edu” dns server, which in turn will give “cs.nyu.edu” etc.

Recap

1. How are machines/devices named?
IP addressing & allocation

2. How Does A discover B's name?
DNS



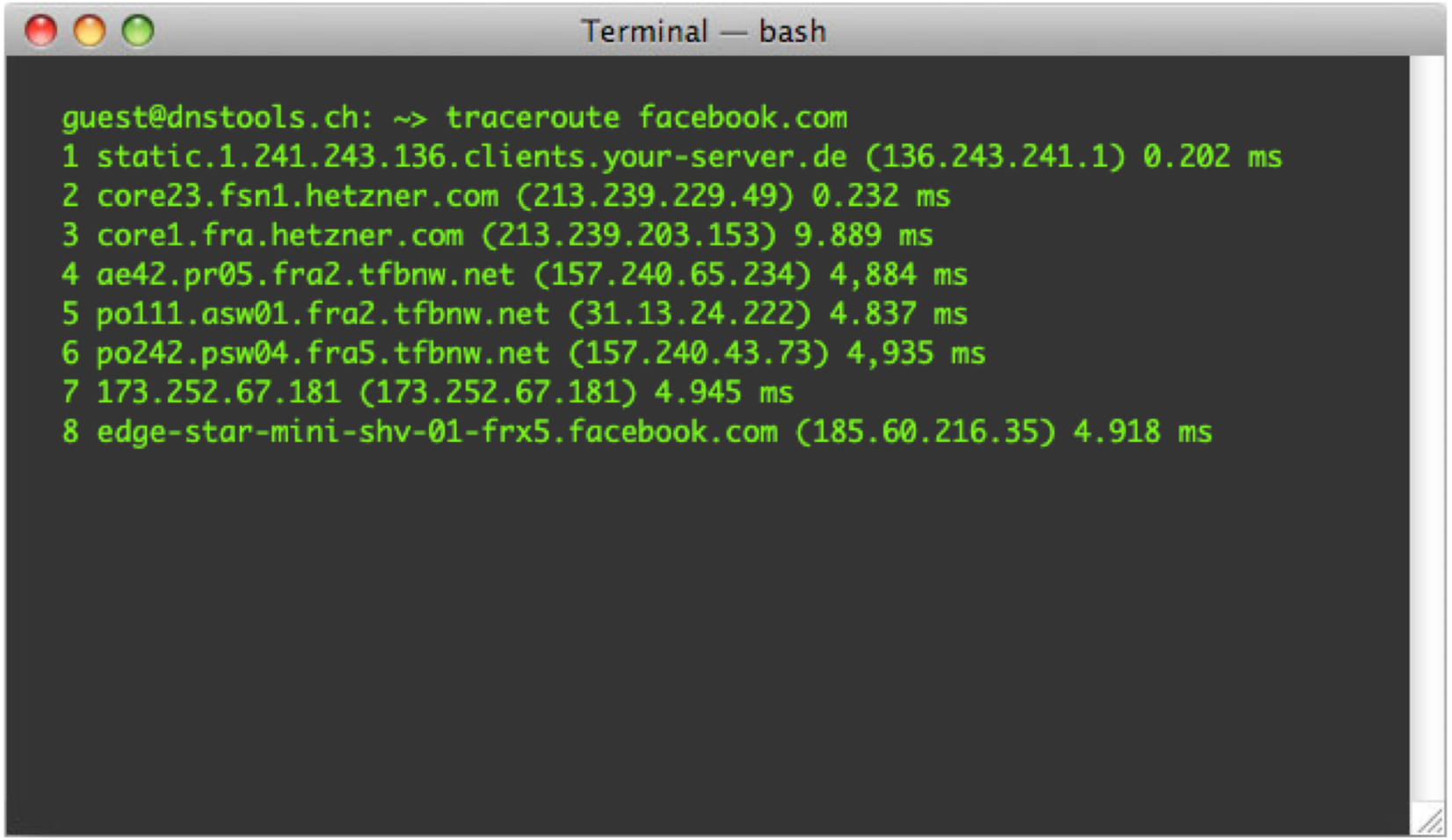
3. How Does A find a path to B?
Routing

4. How do A and B send data to each other
TCP, UDP

Finding path from A to B: routing

- A will send to a “router”
  - The router near A has to find a path to a router close to B
- Goal: determine a “good” path from A to B
- Network modeled as a graph
  - Routers are nodes, internet connections/links as edge
  - Weight on edge: delay, congestion level
  - A node knows only its neighbors and the cost to reach them
  - Stored in a routing table

Finding the route (traceroute)



http://www.dnstools.ch/visual-traceroute.html

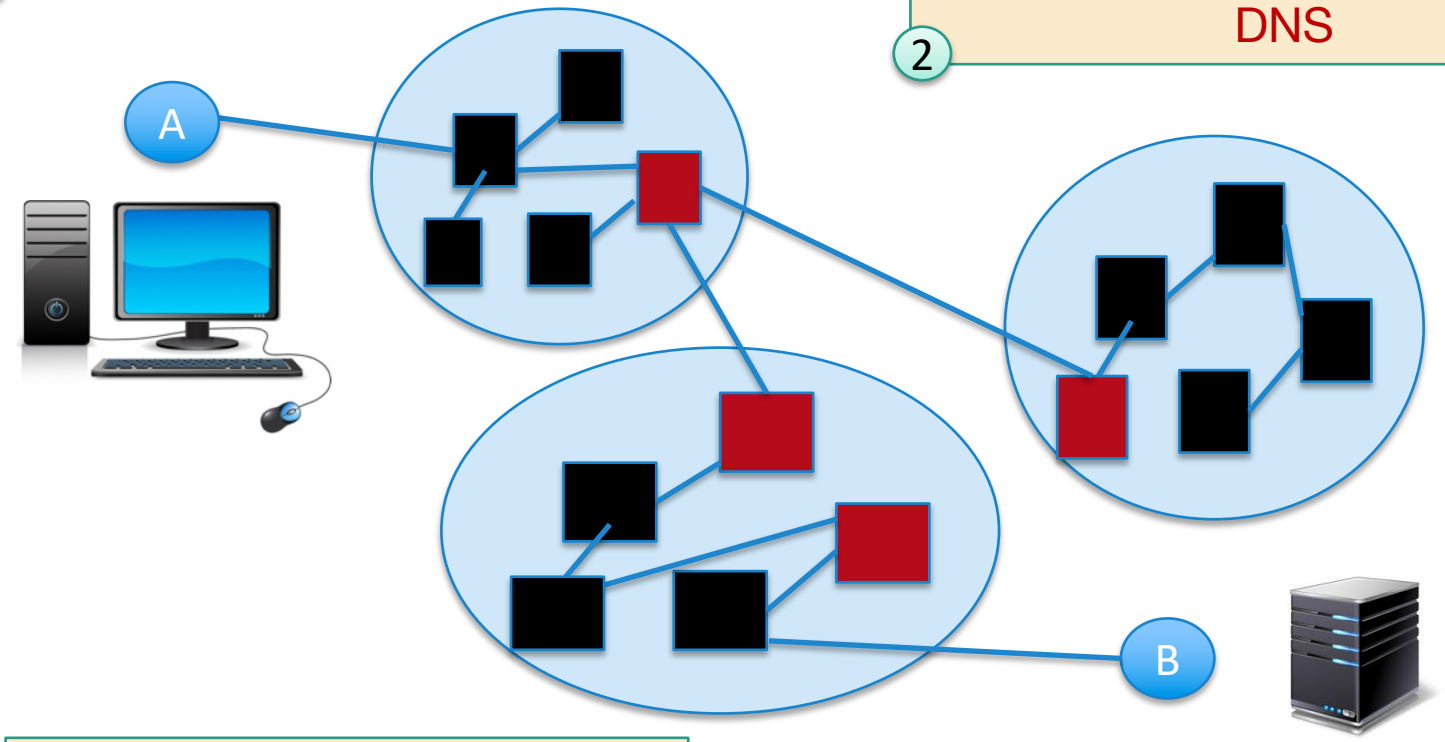
Intra AS and inter AS routing

- Intra-AS: routing within a single AS
  - Trusted domain (within one company)
  - Limited scale (<100,000 nodes)
  - Typically using Link State protocol (e.g. OSPF)
- Inter-AS: routing between AS's (iitkgp.ac.in to nyu.edu)
  - BGP, a Path Vector protocol

Recap

1. How are machines/devices named?
IP addressing & allocation

2. How Does A discover B's name?
DNS



3. How Does A find a path to B?
Routing

4. How do A and B send data to each other
TCP, UDP

TCP

- Multiplexes between services
- Multi-packet connections
- Handles loss, duplication,& out-of-order delivery
  - all received data ACKnowledged
- Flow control
  - sender doesn’t overwhelm recipient
- Congestion control
  - sender doesn’t overwhelm network

Now attacks…

Network threat model

- Network scanning
  - Attacks on confidentiality
  - e.g., eavesdropping
- Attacks on integrity
  - e.g., spoofing, packet injection
- Attacks on availability
  - e.g., denial of service (DoS)
  - Resource exhaustion (e.g., CPU, memory, B/W)
  - Easy to perform, very difficult to defend

Network Scanning: Ping

- Essential, low-level network utility
- Sends a “ping” ICMP message to a host on the internet

```
mbk-52-11@mbk-52-31:~$ ping google.com
PING google.com (74.125.24.102): 48 data bytes
56 bytes from 74.125.24.102: icmp_seq=0 ttl=48 time=147.814 ms
56 bytes from 74.125.24.102: icmp_seq=1 ttl=48 time=255.837 ms
56 bytes from 74.125.24.102: icmp_seq=2 ttl=48 time=132.909 ms
56 bytes from 74.125.24.102: icmp_seq=3 ttl=48 time=132.484 ms
^C--- google.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 132.484/167.261/255.837/51.511 ms
```

- Destination host is supposed to respond with a “pong”
  - Indicating that it can receive packets
- By default, ping messages are 56 bytes long (+ some header bytes)
  - Maximum size 65535 bytes
- What if you send a ping that is >65535 bytes long?

Ping of death

- ping –s 65535 66.66.0.255
  - Attack identified in 1997
  - IPv6 version identified/fixed in 2013

Network routing: Traceroute

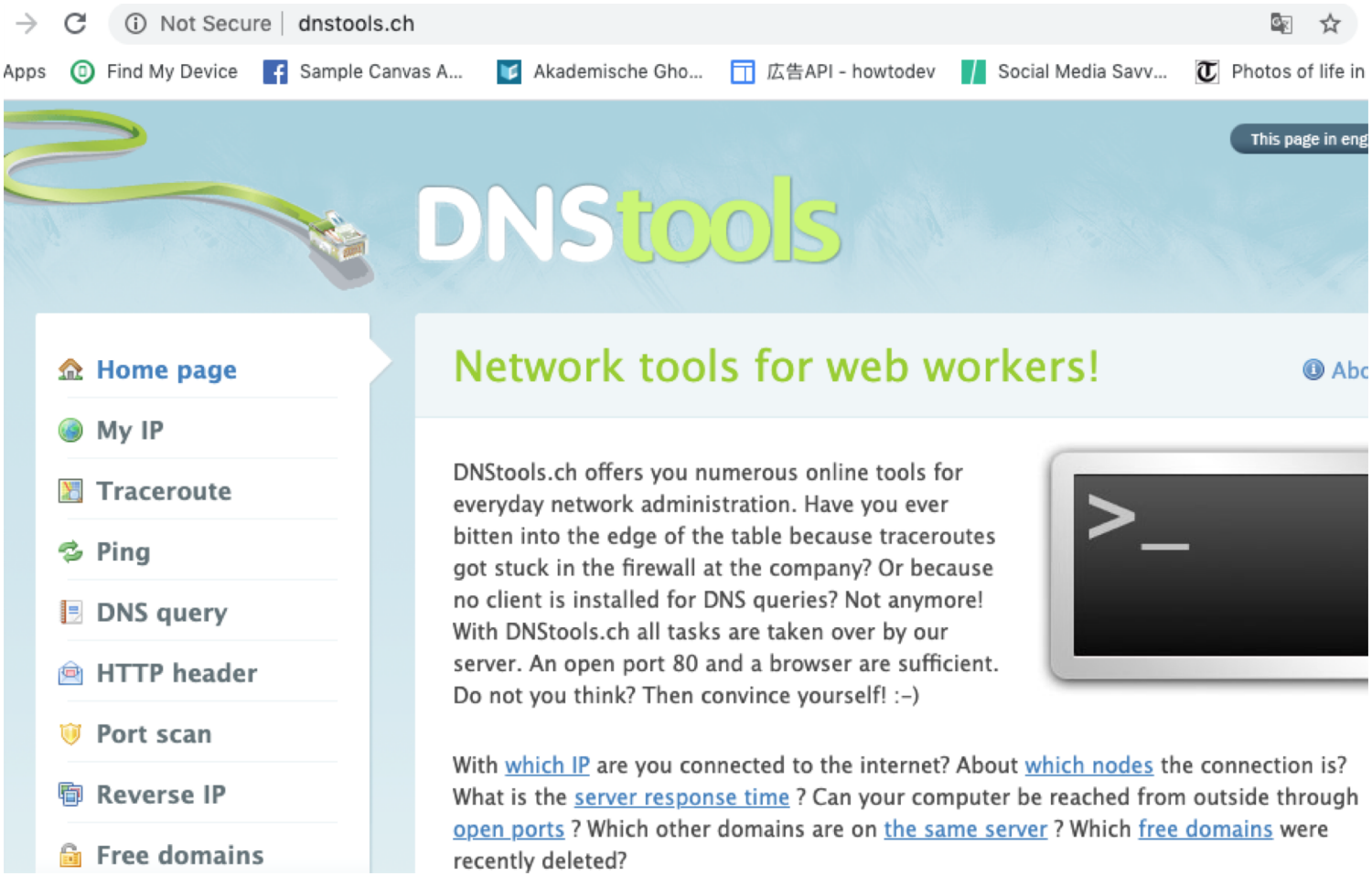
- traceroute – hops between me and host
  - Sends repeated ICMP reqs with increasing TTL

```
mbk-52-11@mbk-52-31:~$ traceroute google.com
traceroute to google.com (74.125.24.113), 64 hops max
 1   10.7.7.1 (10.7.7.1) 153.224ms 87.425ms 88.051ms
 2   169.254.162.187 (169.254.162.187) 88.344ms 99.408ms 172.742ms
 3   169.38.118.136 (169.38.118.136) 212.049ms 123.798ms 89.204ms
 4   50.97.19.254 (50.97.19.254) 103.525ms 87.477ms 87.998ms
 5   50.97.19.249 (50.97.19.249) 118.402ms 128.166ms 129.682ms
 6   50.97.18.170 (50.97.18.170) 117.177ms 117.225ms 257.193ms
 7   27.111.228.30 (27.111.228.30) 321.566ms 192.484ms 214.817ms
 8   108.170.240.164 (108.170.240.164) 162.303ms 237.341ms 247.492ms
 9   216.239.49.224 (216.239.49.224) 290.318ms 207.224ms 125.600ms
 10   72.14.239.65 (72.14.239.65) 124.275ms 131.710ms 167.661ms
 11   *  *  *
 12   *  *  *
 13   *  *  *
 14   *  *  *
 15   *  *  *
 16   *  *  *
 17   *  *  *
 18   *  *  *
 19   *  *  *
 20   74.125.24.113 (74.125.24.113) 174.451ms 202.646ms 122.525ms
```

Port scanning: nmap

```
mbk-52-11@mbk-52-31:~$ nmap cse.iitkgp.in
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-31 02:22 IST
Nmap scan report for cse.iitkgp.in (69.172.201.153)
Host is up (0.19s latency).
Not shown: 998 filtered ports
PORT    STATE  SERVICE
25/tcp  closed smtp
443/tcp open   https

Nmap done: 1 IP address (1 host up) scanned in 54.19 seconds
```

Port scanning on steroids: zmap


Not Secure | dnstools.ch
Apps
Find My Device
Sample Canvas A...
Akademische Gho...
広告API - howtodev
Social Media Savv...
Photos of life in
This page in eng
DNStools
Home page
My IP
Traceroute
Ping
DNS query
HTTP header
Port scan
Reverse IP
Free domains
Network tools for web workers!
Abo
DNStools.ch offers you numerous online tools for everyday network administration. Have you ever bitten into the edge of the table because traceroutes got stuck in the firewall at the company? Or because no client is installed for DNS queries? Not anymore! With DNStools.ch all tasks are taken over by our server. An open port 80 and a browser are sufficient. Do not you think? Then convince yourself! :-)
>_
With which IP are you connected to the internet? About which nodes the connection is? What is the server response time ? Can your computer be reached from outside through open ports ? Which other domains are on the same server ? Which free domains were recently deleted?

Eavesdropping

- Tools: Wireshark, tcpdump, bro …
- Demo of wireshark

Active attacks