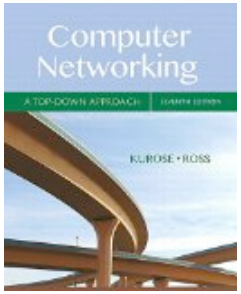
JOHN BOLTON ON OBAMA'S INTERNET HANDOVER: 'WITHIN TEN YEARS, THE INTERNET AS WE KNOW IT WILL END'

by JOHN HAYWARD | 22 Sep 2016 | 2,410

On Thursday's Breitbart News Daily on SiriusXM, former

COMP 375: Lecture 10



- **News & Notes:**
  - Class / Office Hours cancelled Wed - Fri
  - Project #2 due Wed, Feb. 28
- **Reading (Mon, Feb. 26)**
  - Sections 3.1 – 3.3

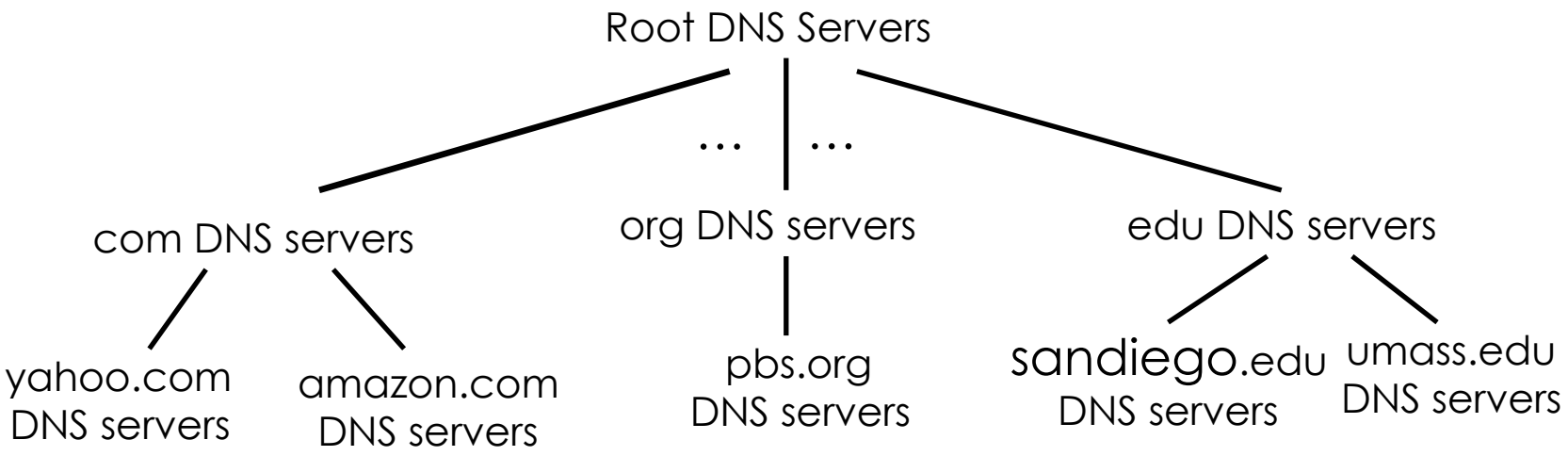
Section 2.4

DOMAIN NAME SERVICE (DNS)

A DNS record contains a TTL that informs how long it is cached.

- *What is the trade-off involved with setting TTL to a large value rather than a small one.*

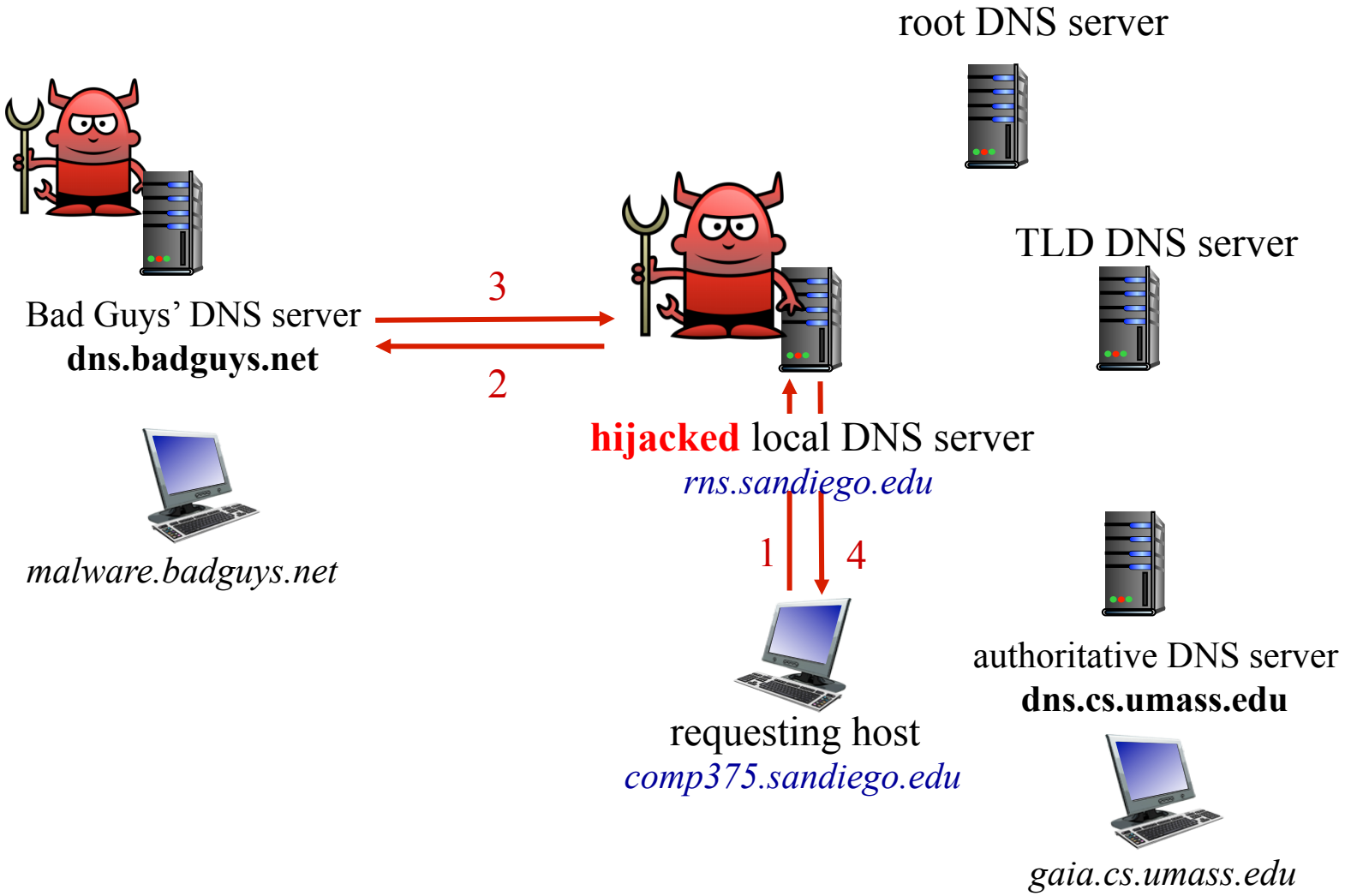
What would change if we wanted to add a new domain (e.g. DrSat.com)?



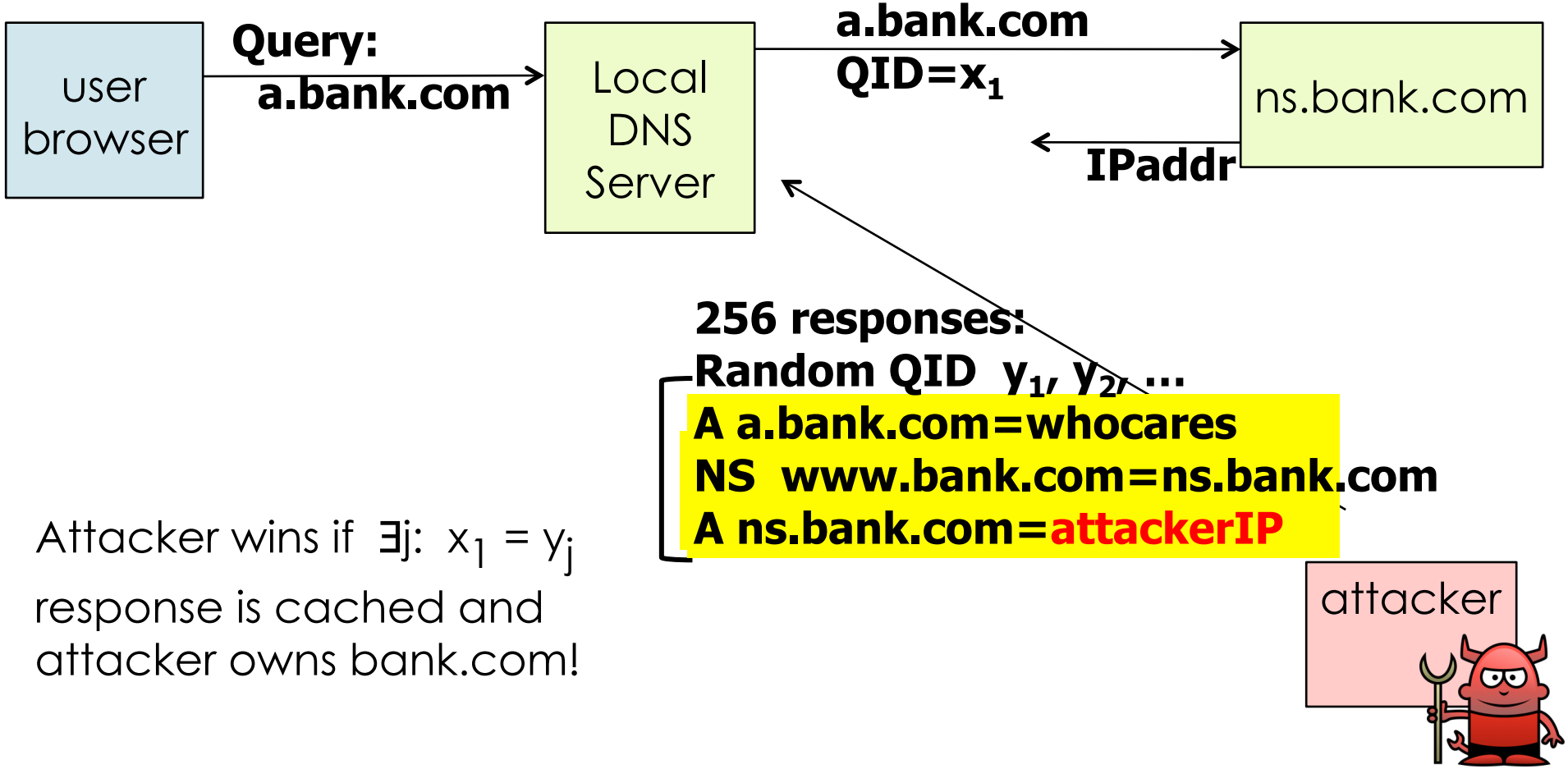
What aspect of DNS seems like it is particularly insecure?

A.	UDP sockets accept packets from any host on the entire Internet.
B.	The TTL allows a mapping to persist for new queries after it has been set.
C.	Attackers can control when recursive DNS servers look up specific domains.
D.	Responses can have additional "helpful information" appended.

DNS is vulnerable when someone hijacks a DNS server.



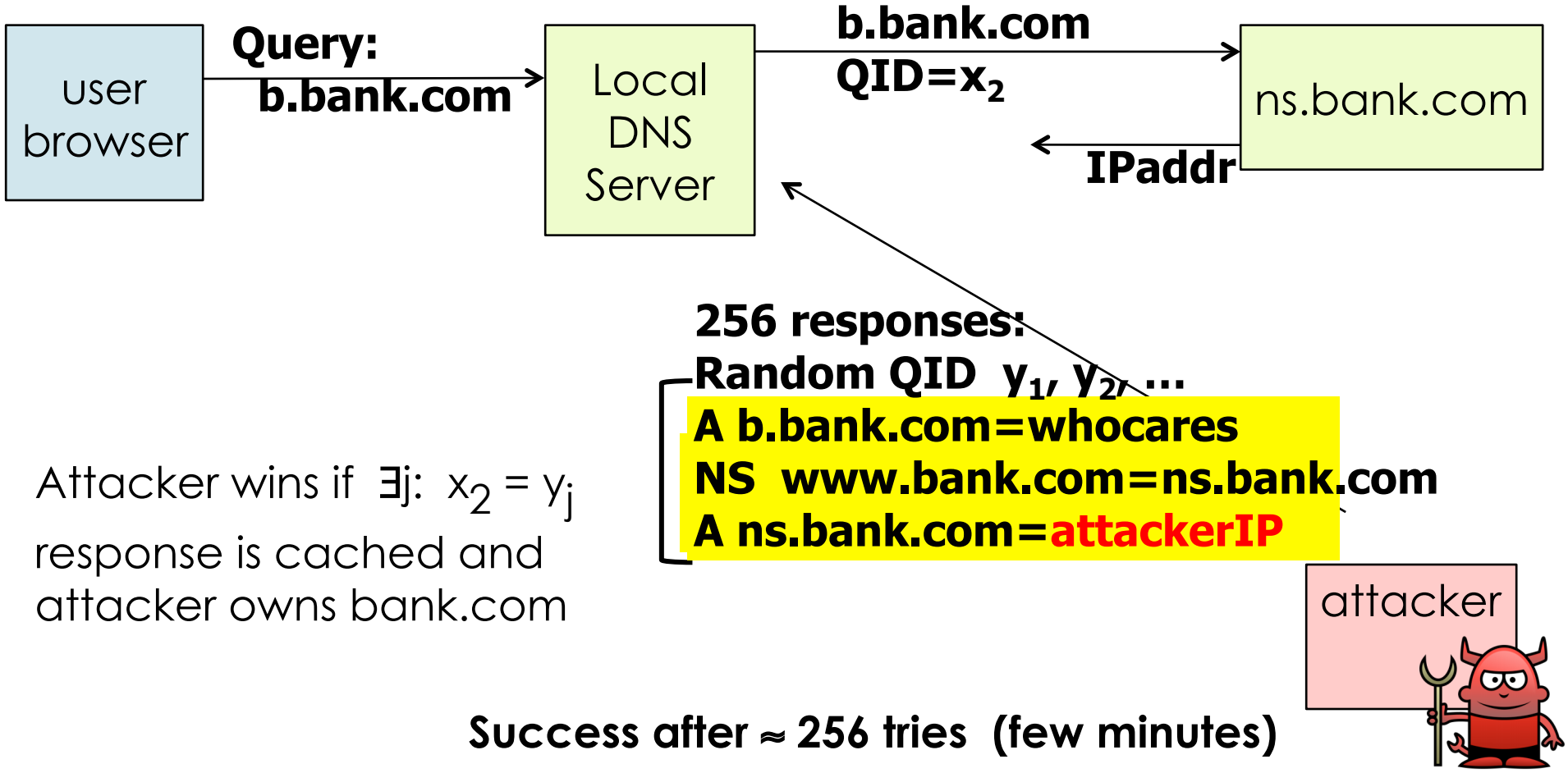
DNS caches can be poisoned by giving bogus additional information.



Attacker wins if $\exists j$: $x_1 = y_j$

response is cached and attacker owns bank.com!

Flooding Local DNS with random requests increases likelihood of success.



Attacker wins if $\exists j$: $x_2 = y_j$

response is cached and attacker owns bank.com

Success after ≈ 256 tries (few minutes)

There are several proposals for improving DNS security.

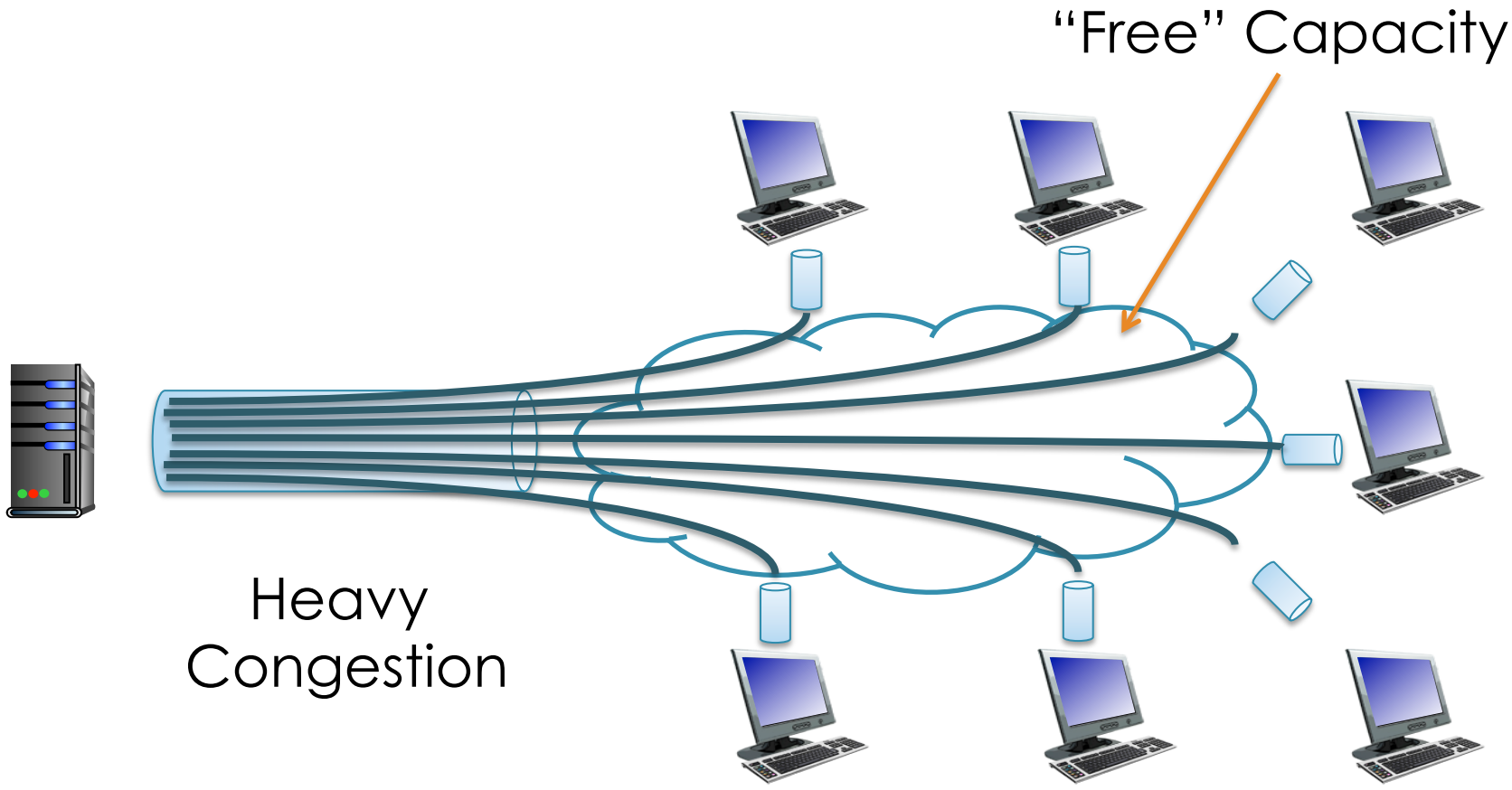
- Use authentication (DNSSEC)
- Reduce probability of success
  - Increase size of query ID
  - Randomize UDP "Source" Port
  - Ask each query twice

Section 2.5

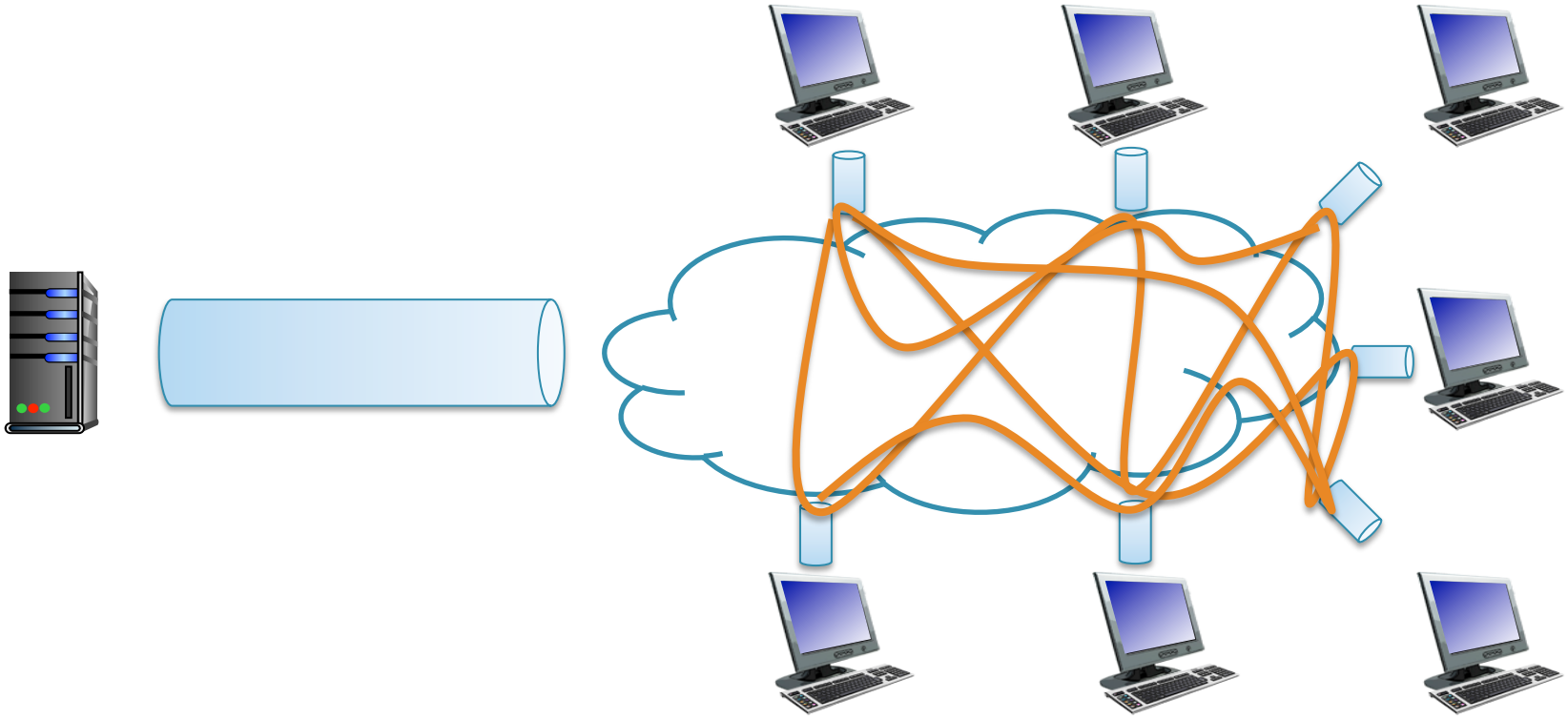
PEER-TO-PEER FILE DISTRIBUTION

What is the best way to distribute a file to a large number of people?

In the Client/Server model, a server has a heavier burden than clients.

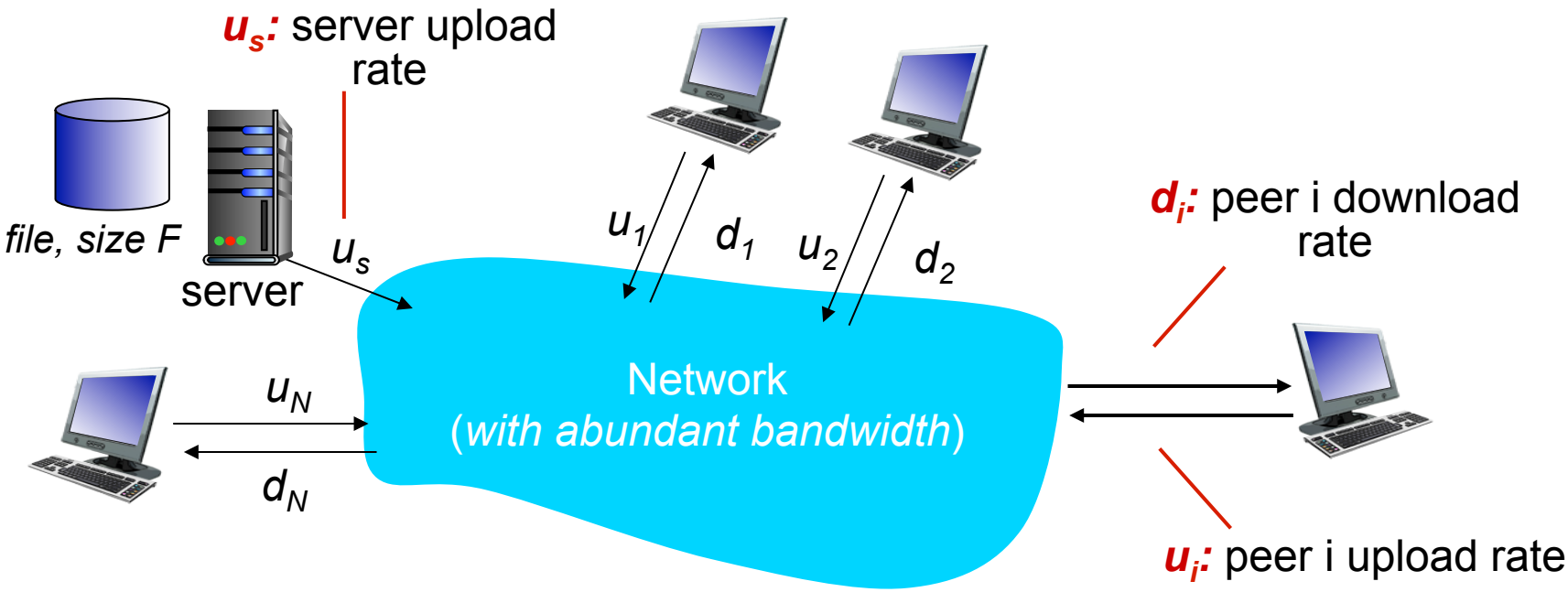


In the P2P model, everyone shares the burden.



Determining file distribution time will require knowledge of transfer rates of all entities.

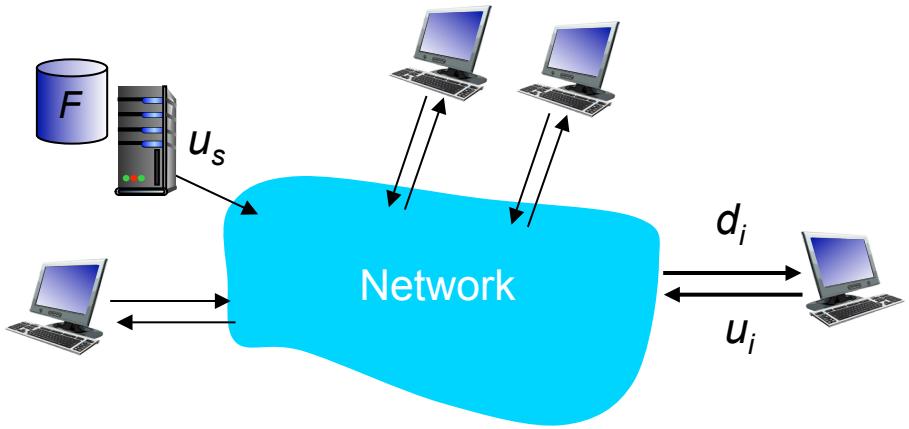
How much time to distribute a file (size: *F*) from one server to *N peers*?



What dictates the **minimum** time for a server to distribute a file of size F to *N* clients?

A.	The MAX of the time it takes any client to download the file.
B.	The MAX of the time it takes for the server to upload N*F bits, **and** the time it takes the client with the lowest download rate to download the file.
C.	The MIN of the time it takes for the server to upload N*F bits, **and** the time it takes the client with the lowest download rate to download the file.

Time to distribute with C/S usually limited by upload rate of the server.

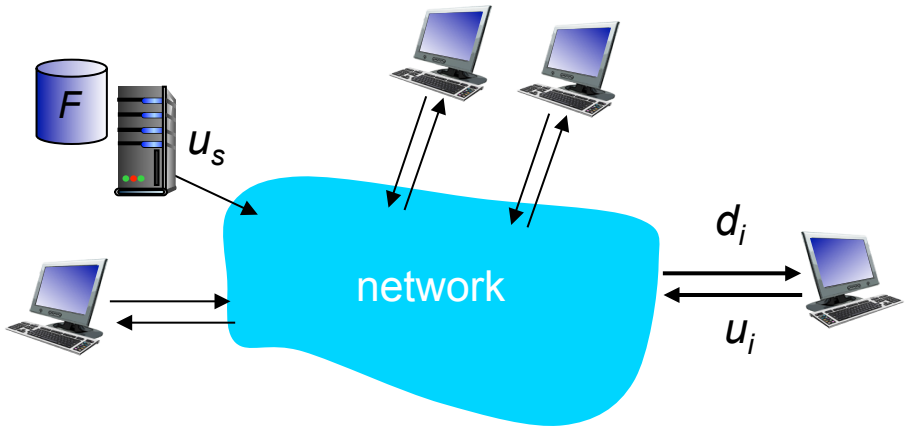


$$D_{c\text{-}s} \geq max\{NF/u_s, F/d_{min}\}$$

What dictates the **minimum** time to distribute the same file in a P2P network?

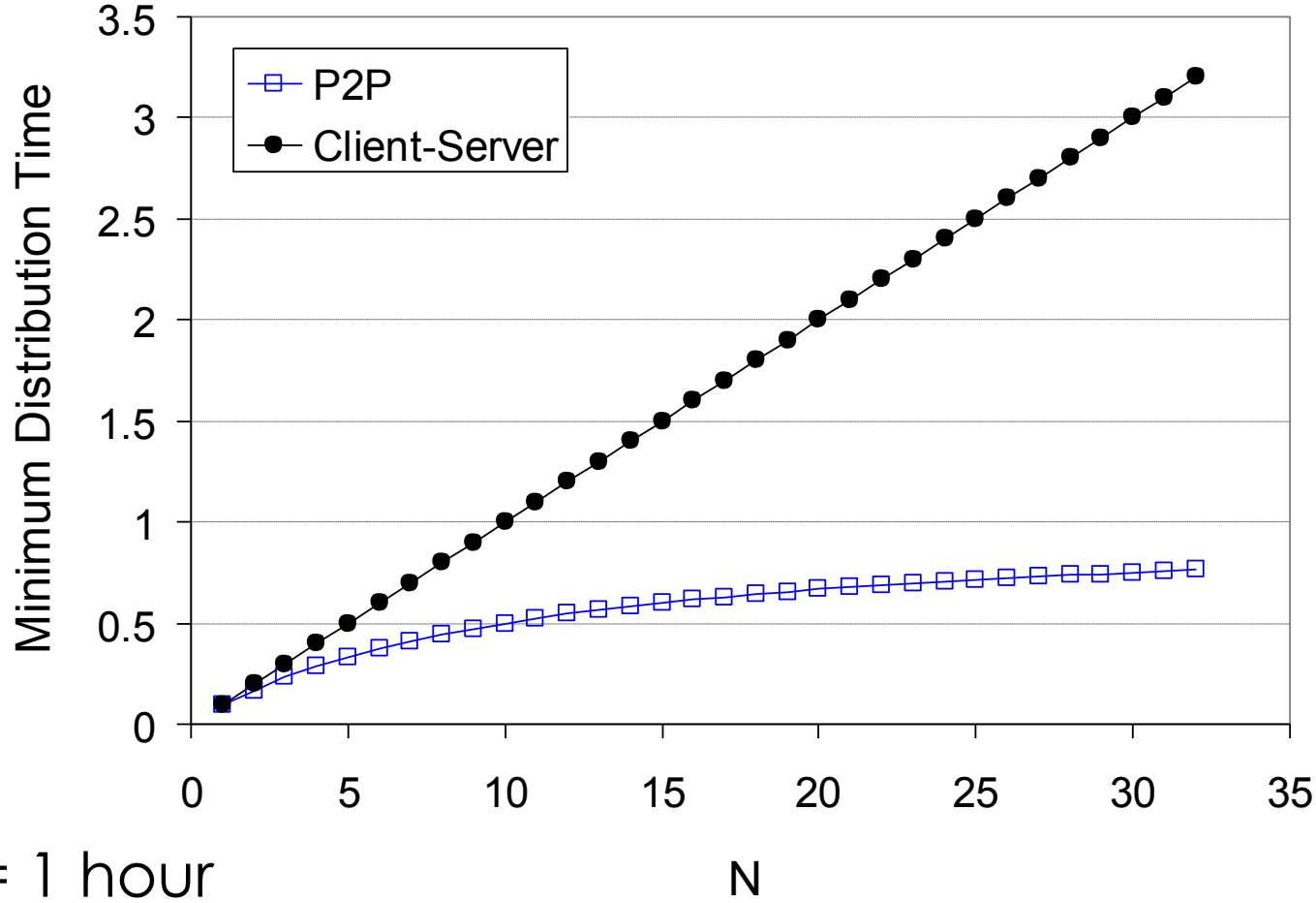
A.	N*F divided by the total upload bandwidth of peers and server.
B.	MAX of answer A and the time it takes the original server to upload the file.
C	MAX of answer B and the download speed of the *slowest* peer

P2P distribution time *usually* limited by aggregate upload bandwidth.



$$D_{P2P} \geq max\{F/u_{s,}, F/d_{min,}, NF/(u_s + \Sigma u_i)\}$$

C/S increases linearly with time, P2P is logarithmic.



- F/u_i = 1 hour
- $u_s = 10*u_i$
- $d_{min} \geq u_s$