The Root of the Matter: A Discussion of DNS Security

Mark Allman
International Computer Science Institute

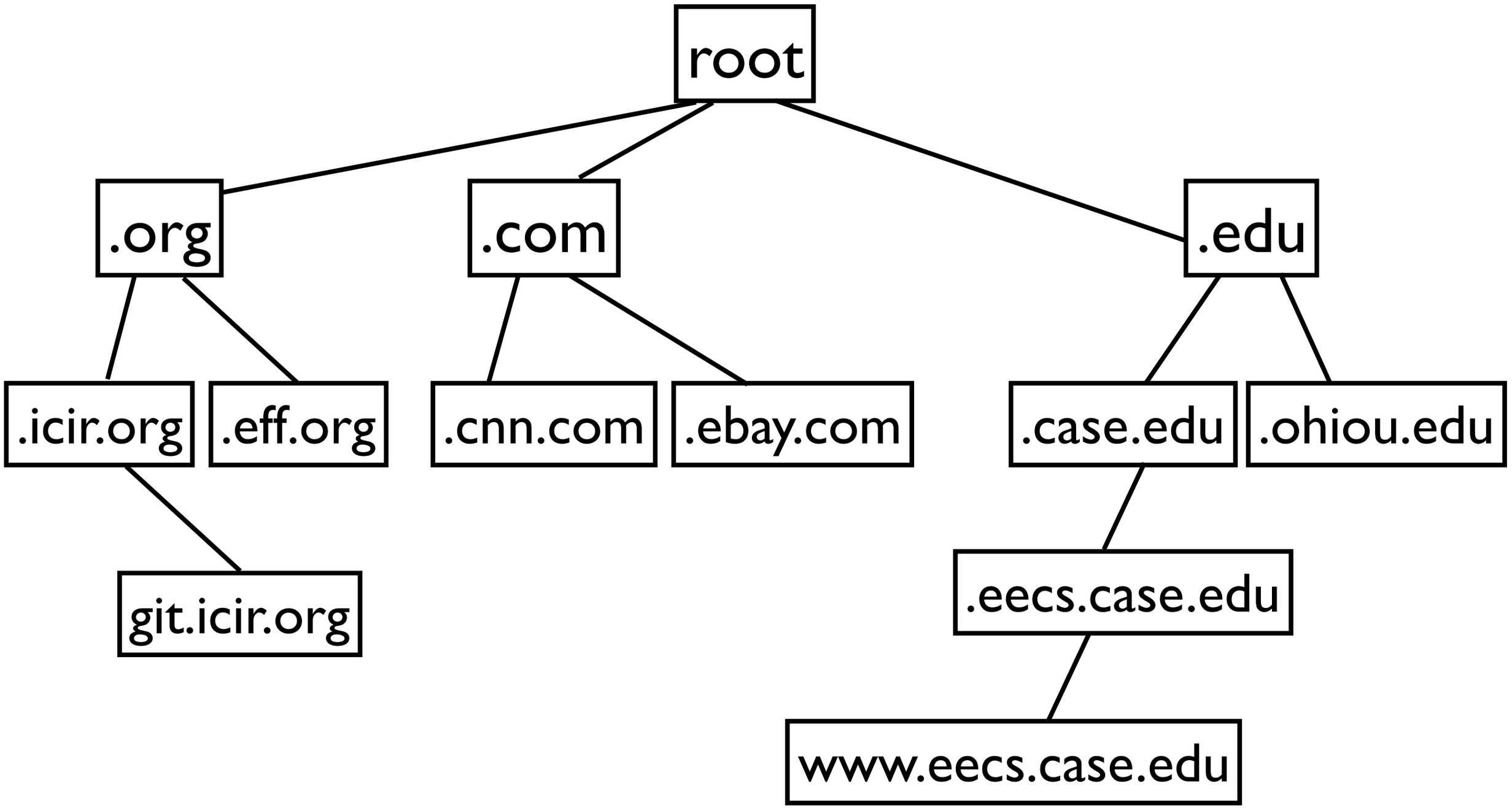
EECS 325 / 425
November 2018

"Like a preacher stealin' hearts in a travelin' show …"

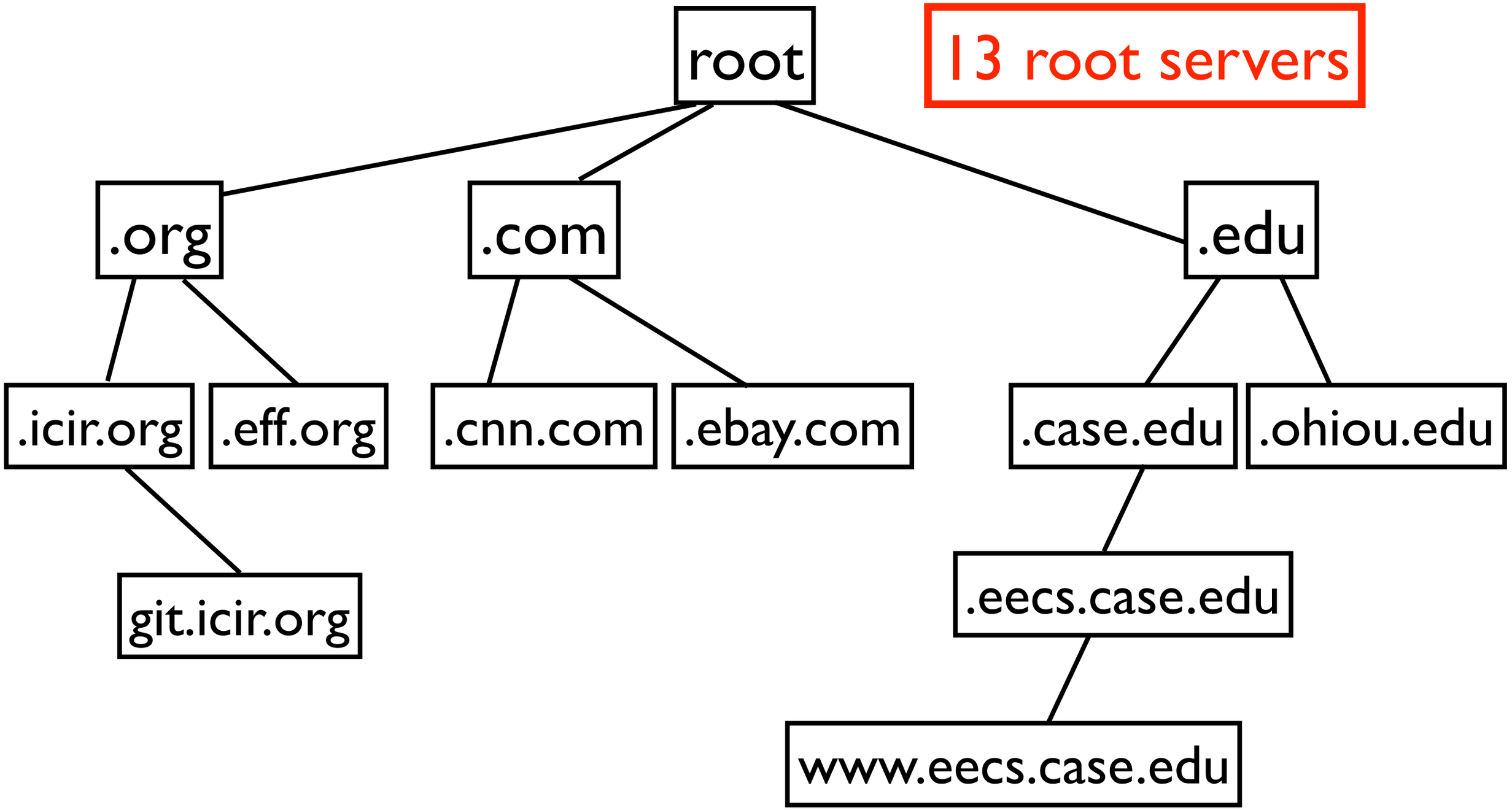
Collaborators

- Michael Bailey, Illinois/UMich
- Owen Bell, Case
- Tom Callahan, Case
- Jake Czyz, UMich
- Nick Feamster, Princeton
- Scott Iekel-Johnson, Arbor
- Ben Jones, Princeton
- Andrew Kalafut, Grand Valley
- Eric Osterweil, Verisign
- Vern Paxson, ICSI & UCB
- Michael Rabinovich, Case
- Kyle Schomp, Case
- Craig Shue, WPI
- Nicholas Weaver, ICSI
- Jing Zhang, UMich

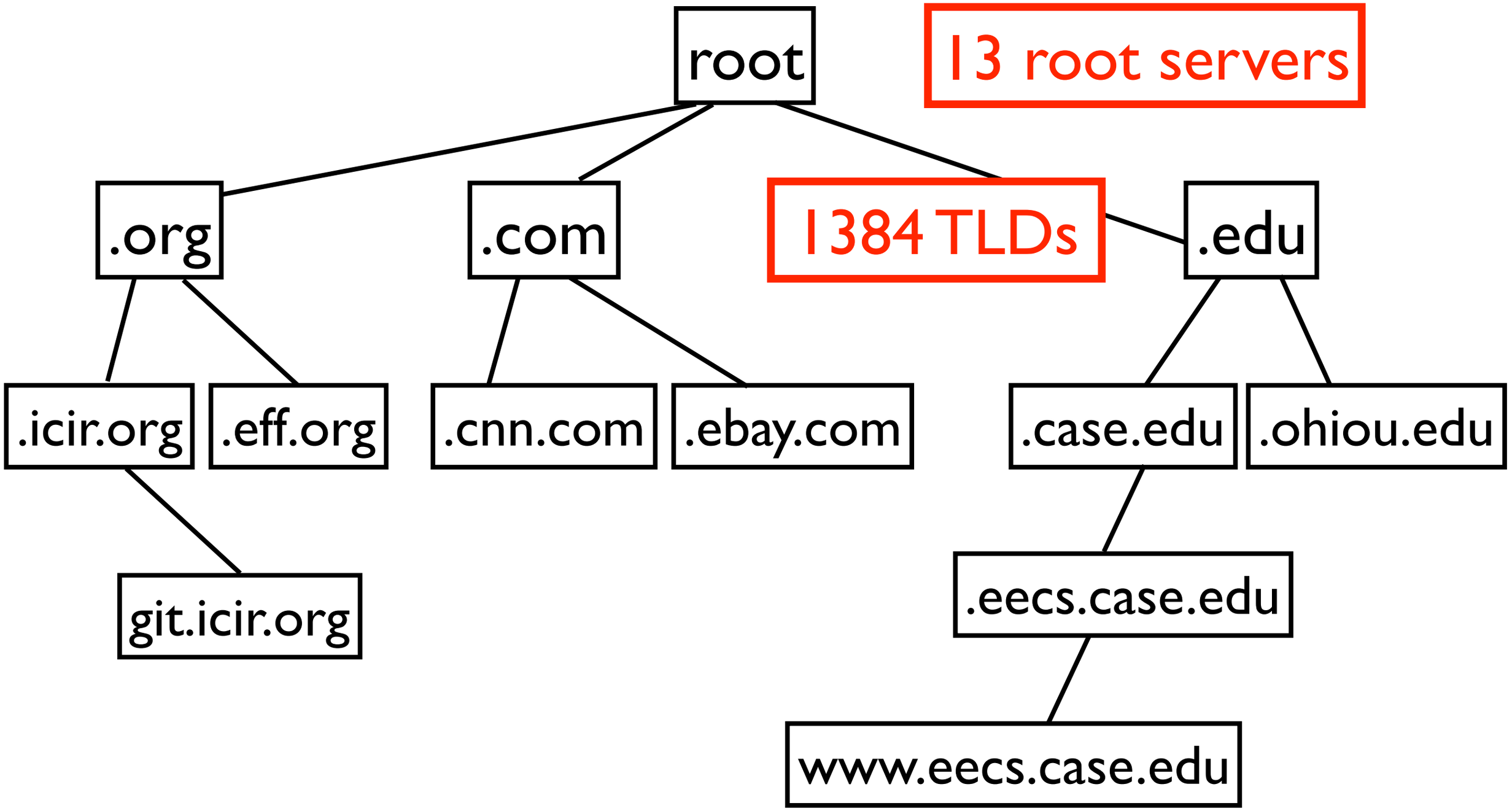
DNS Hierarchy



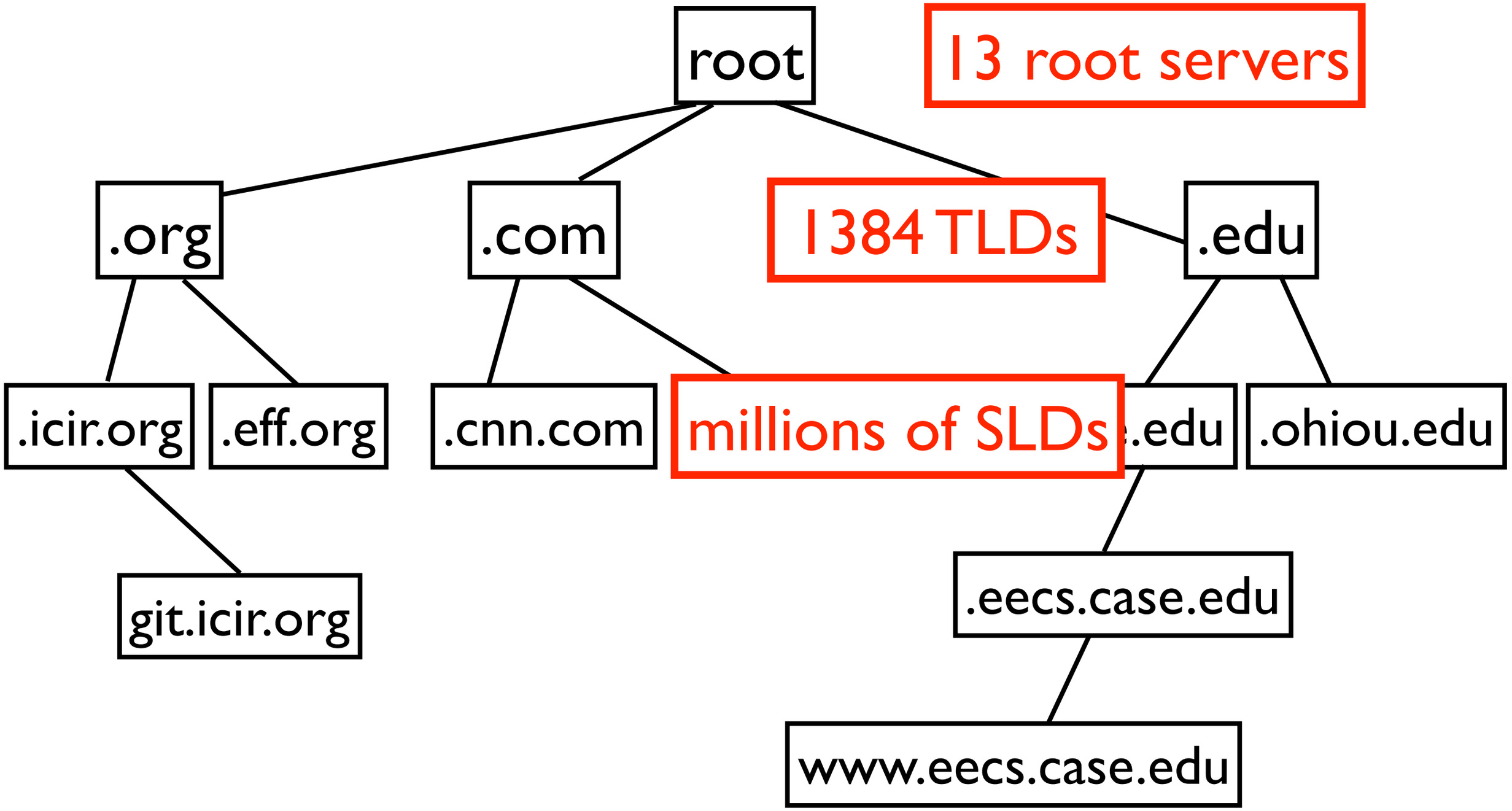
DNS Hierarchy



DNS Hierarchy



DNS Hierarchy



DNS Protocol

DNS Protocol

- DNS, as we use it:
  - connectionless UDP transport
  - single packet request
  - single packet response

DNS Protocol

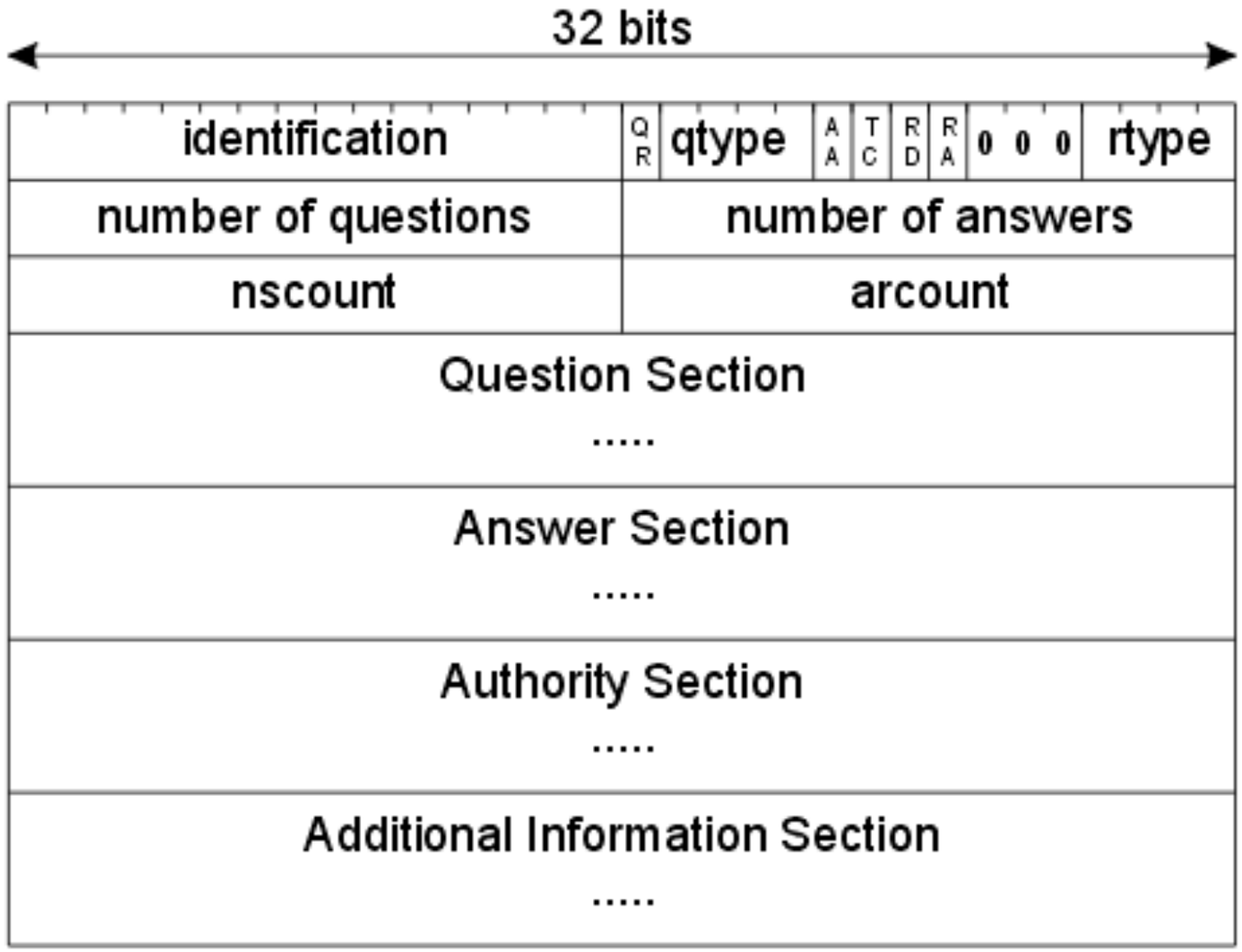
- DNS, as we use it:
  - connectionless UDP transport
  - single packet request
  - single packet response

- However, name resolution is structurally *complex and mysterious* with many hidden components

DNS Protocol

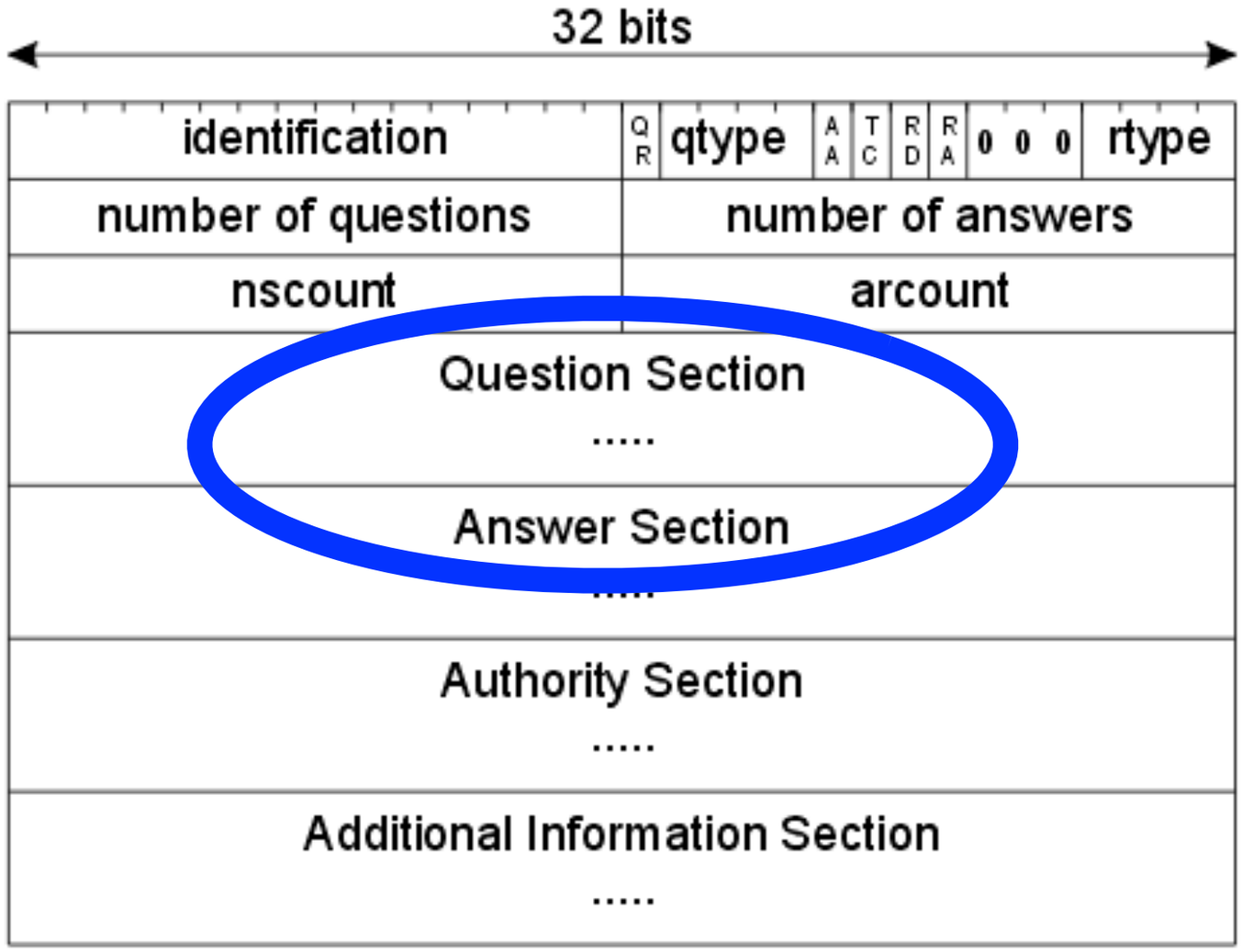
DNS Protocol

DNS server message format

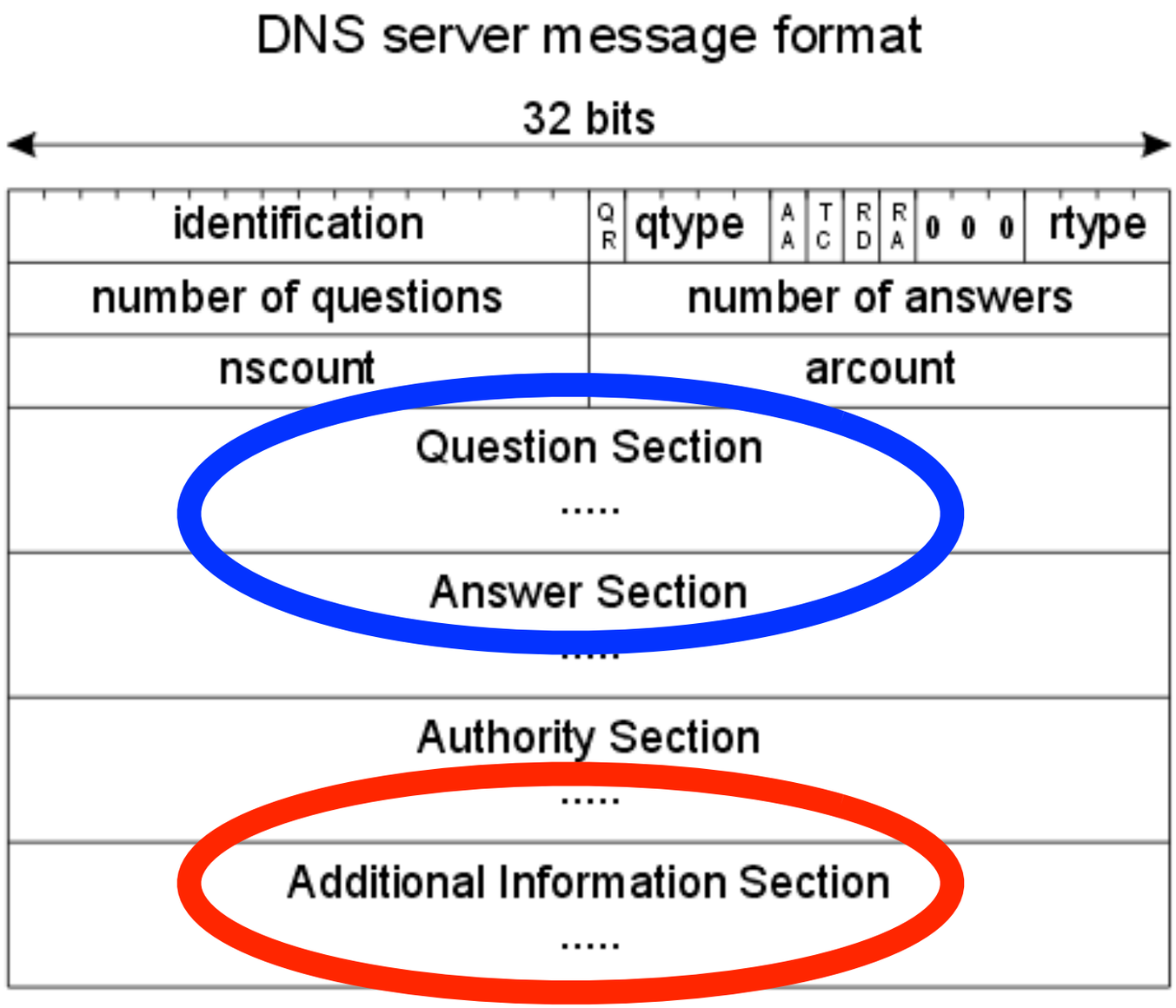


DNS Protocol

DNS server message format



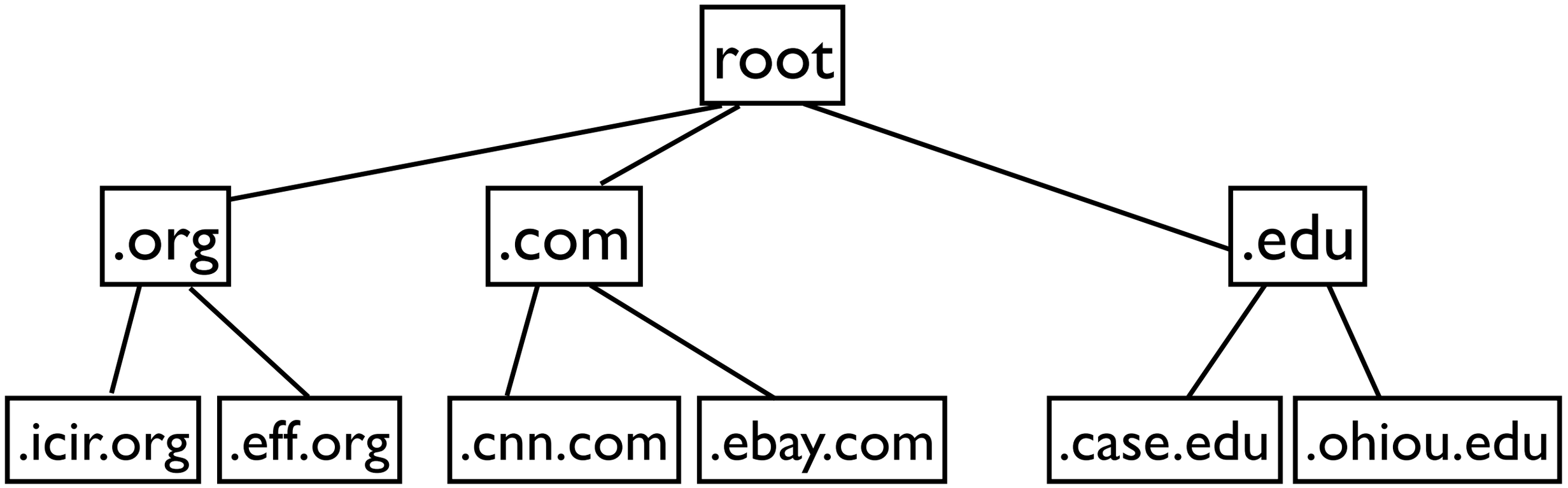
DNS Protocol



DNS Refresher

Goal:

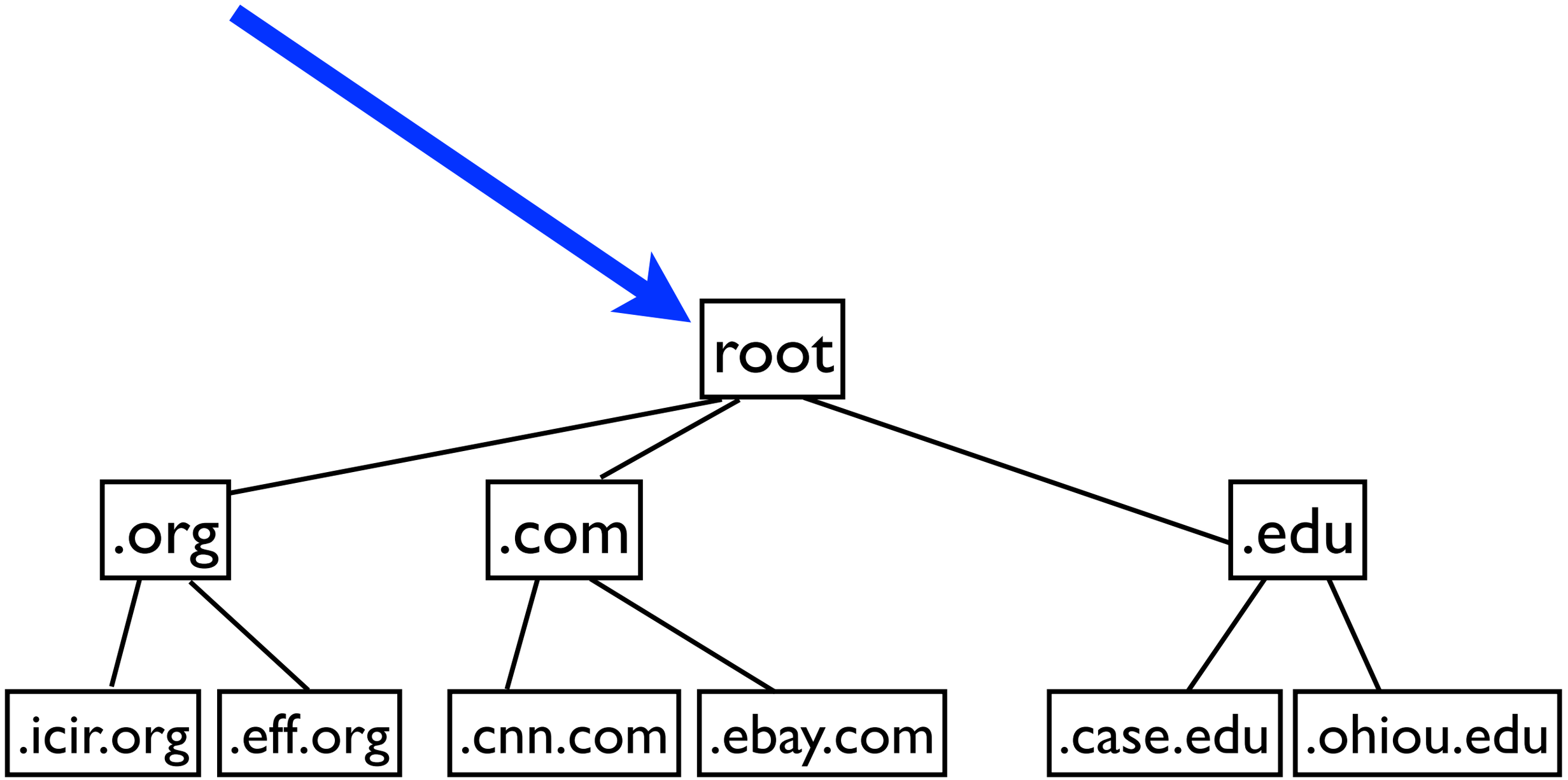
`www.icir.org`



DNS Refresher

Goal:
`www.icir.org`

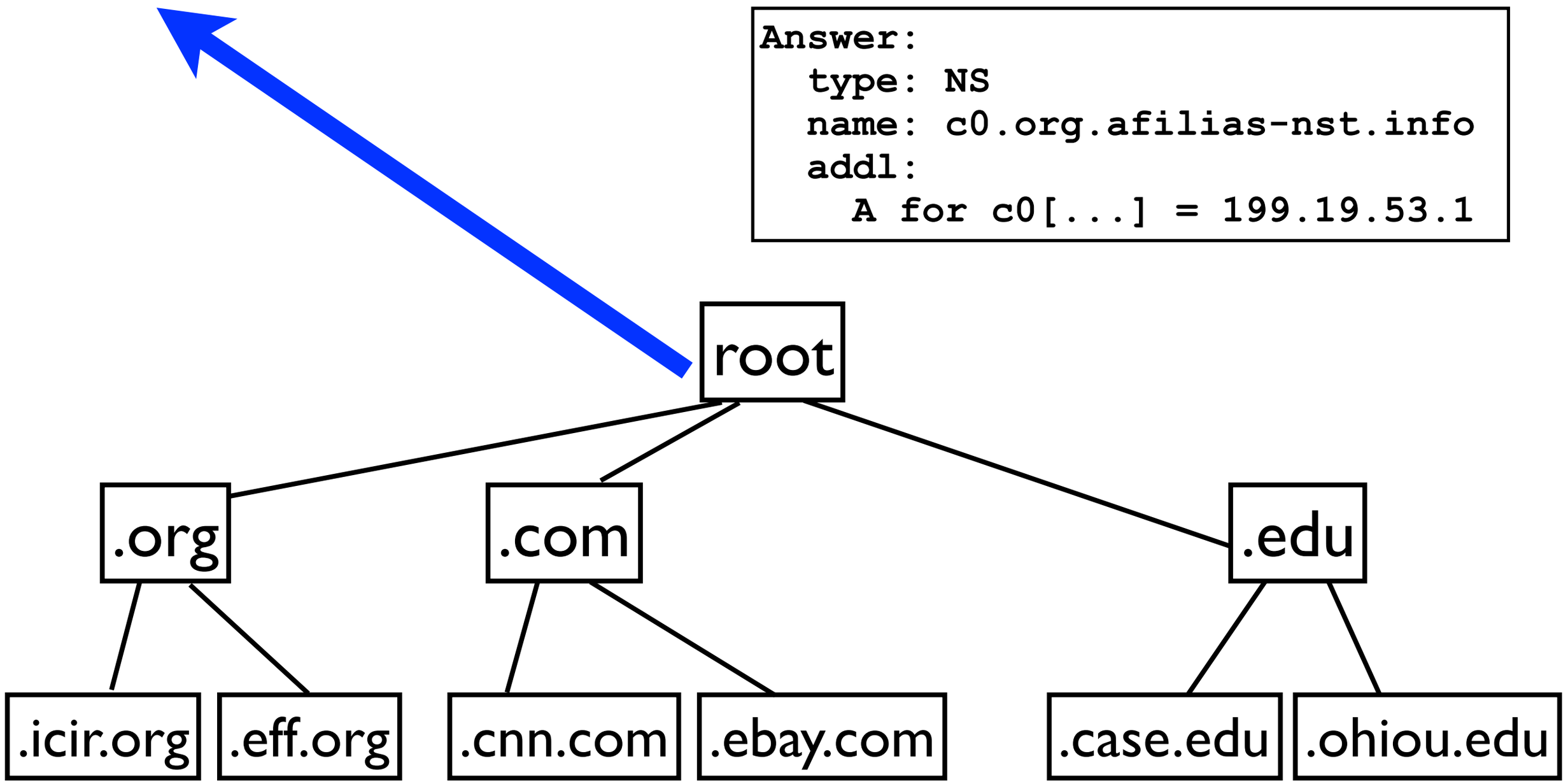
```
Question:
  type: A
  name: www.icir.org
```



DNS Refresher

Goal:
`www.icir.org`

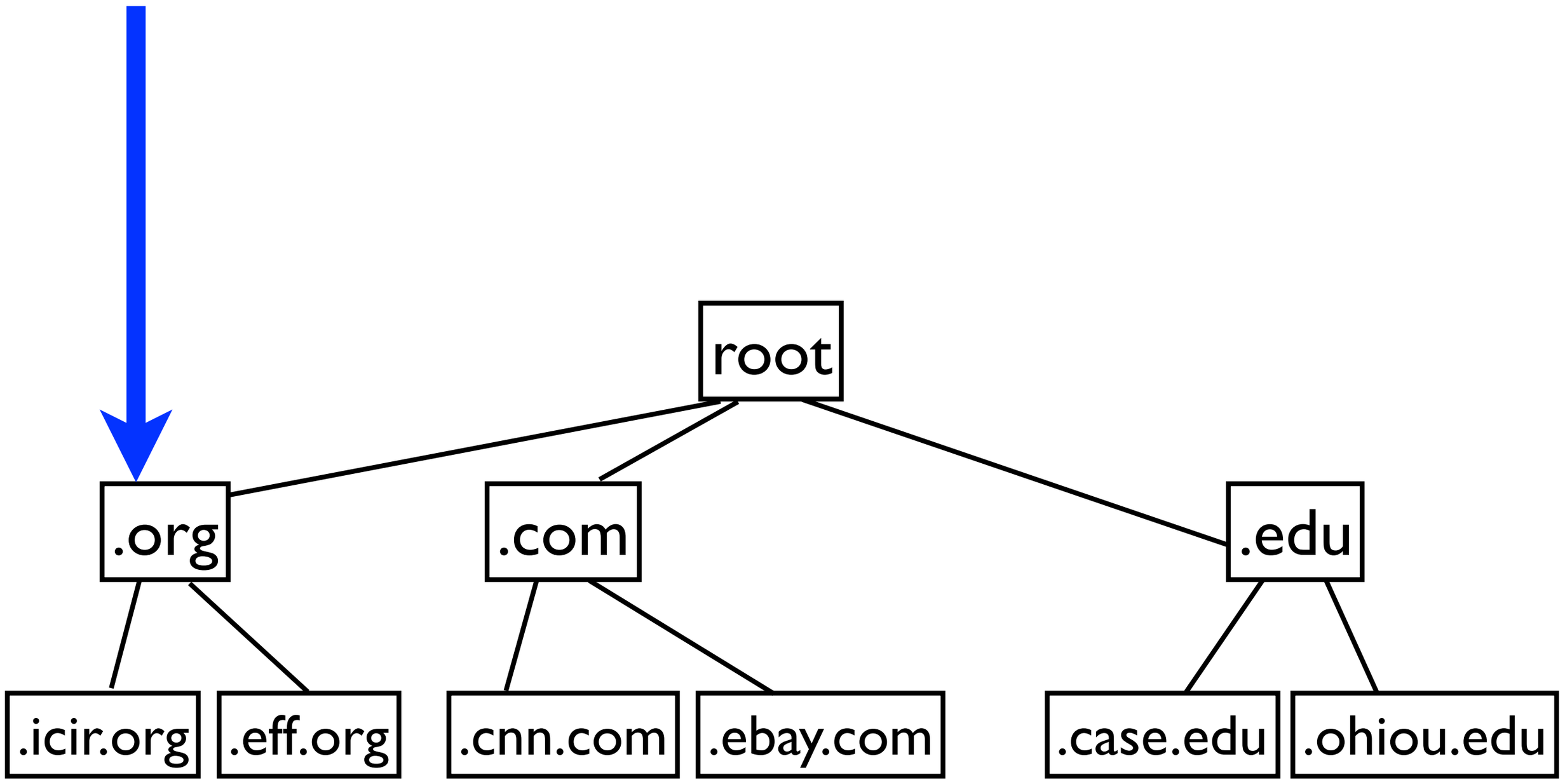
```
Answer:
  type: NS
  name: c0.org.afilias-nst.info
  addl:
    A for c0[...] = 199.19.53.1
```



DNS Refresher

Goal:
`www.icir.org`

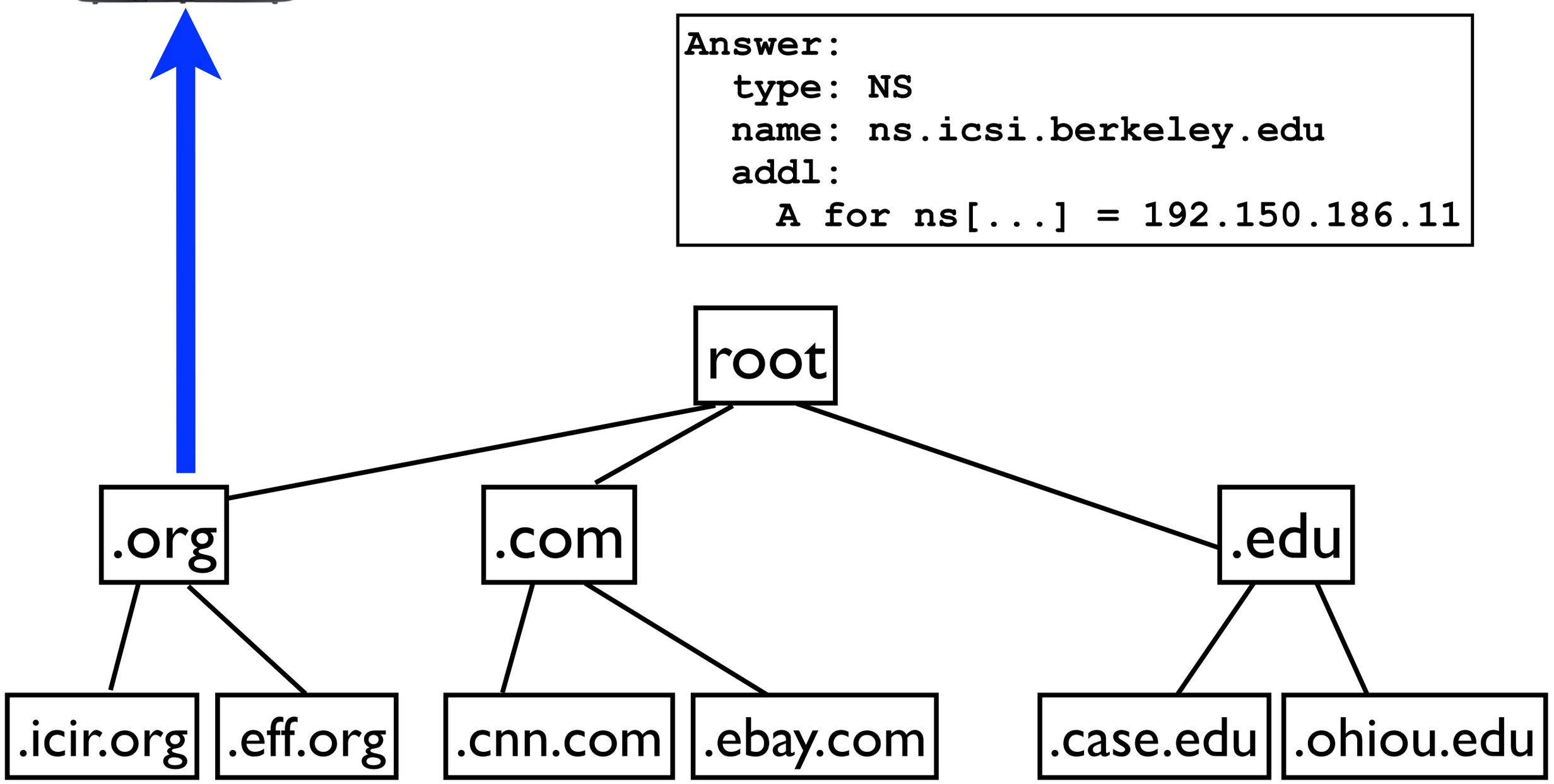
```
Question:
  type: A
  name: www.icir.org
```



DNS Refresher

Goal:
`www.icir.org`

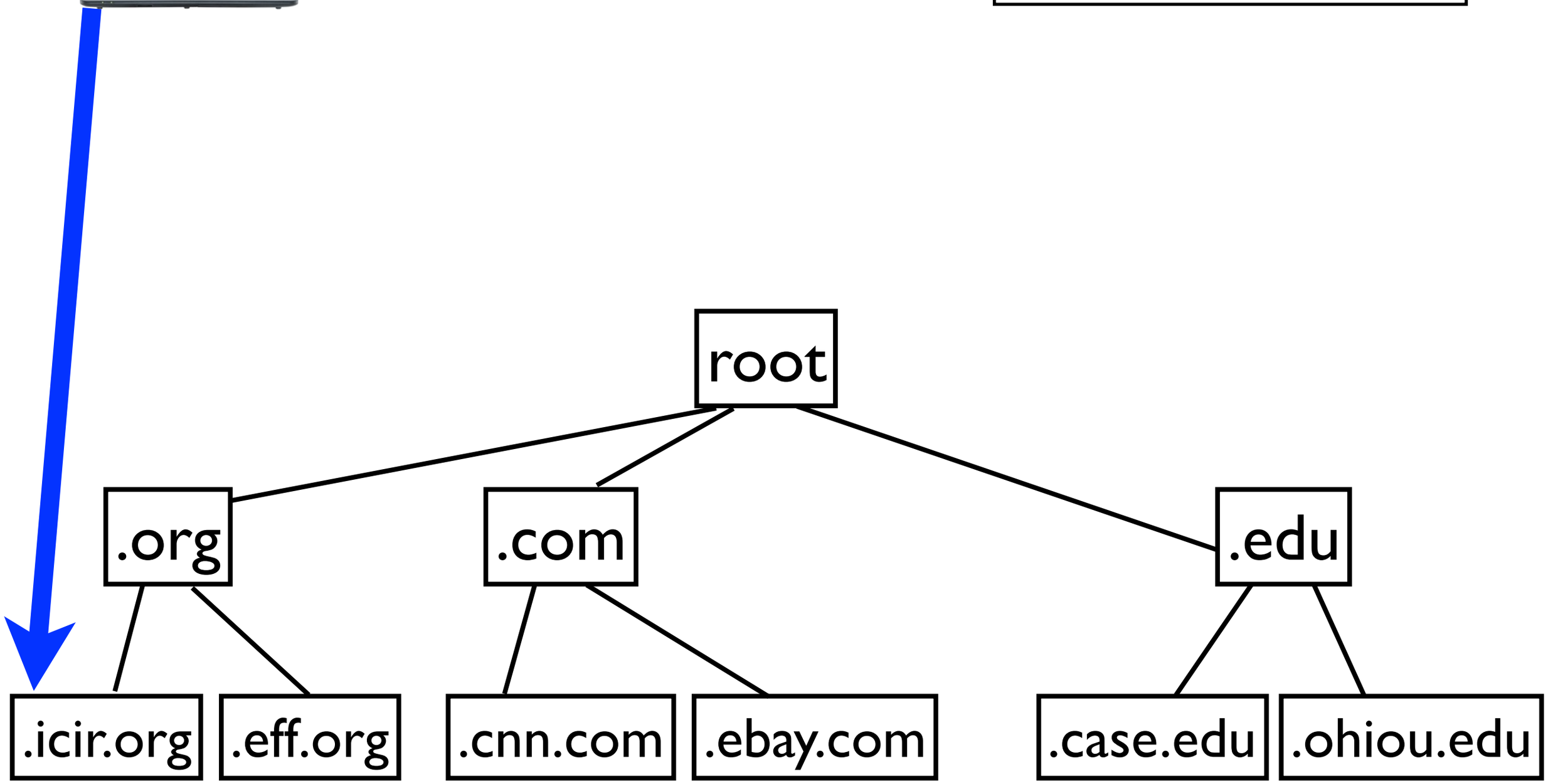
```
Answer:
  type: NS
  name: ns.icsi.berkeley.edu
  addl:
    A for ns[...] = 192.150.186.11
```



DNS Refresher

Goal:
`www.icir.org`

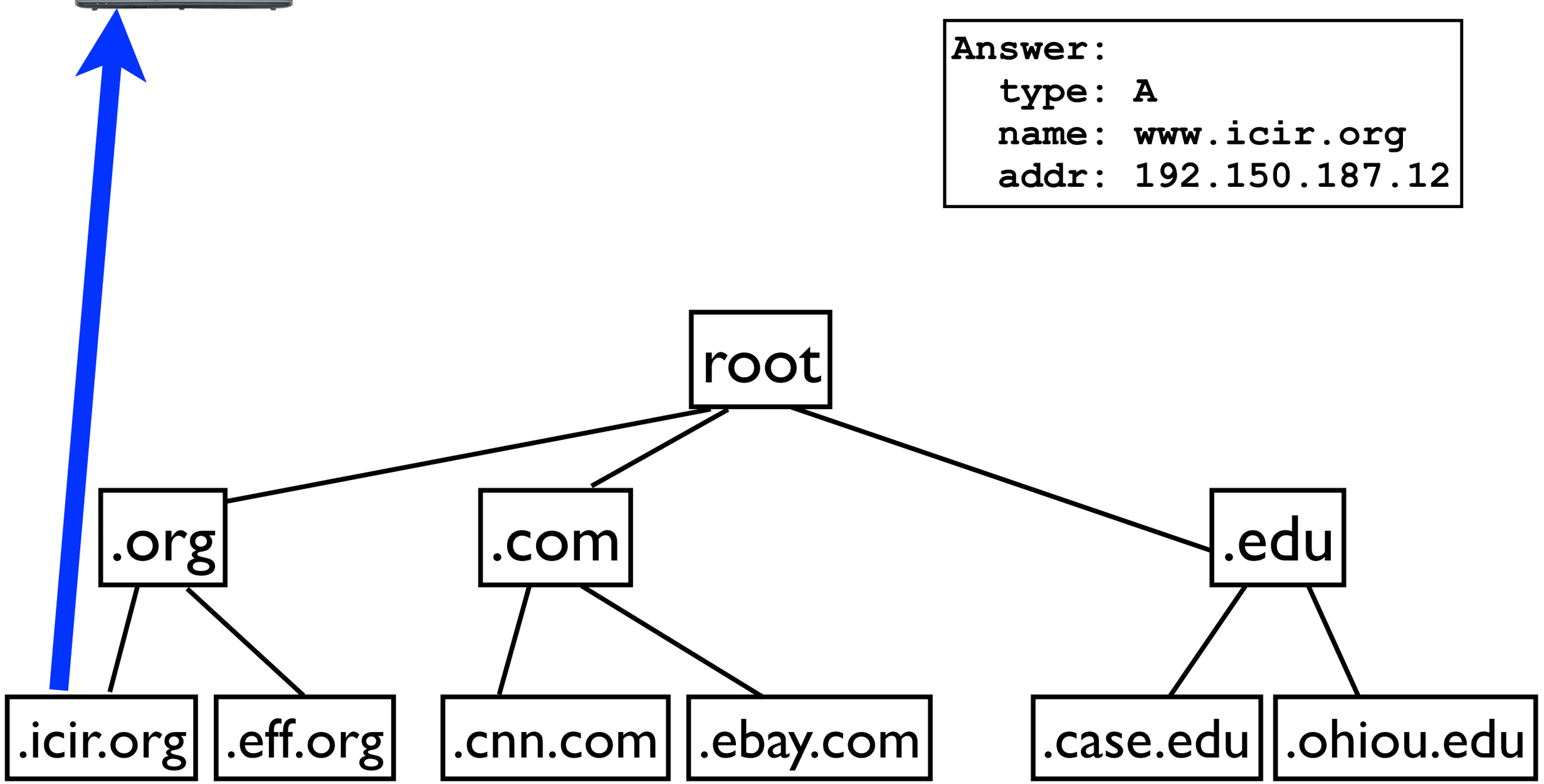
```
Question:
  type: A
  name: www.icir.org
```



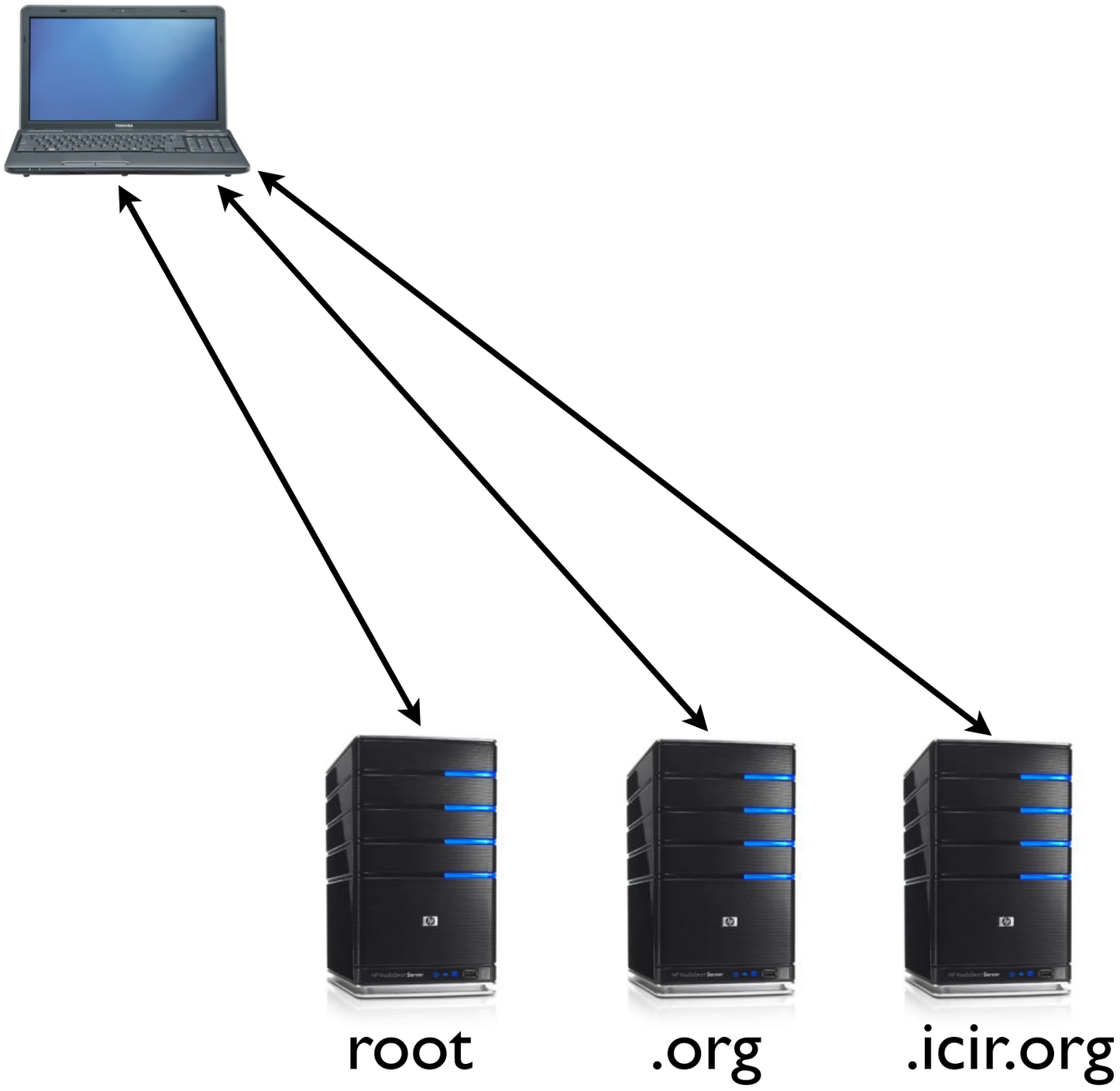
DNS Refresher

Goal:
`www.icir.org`

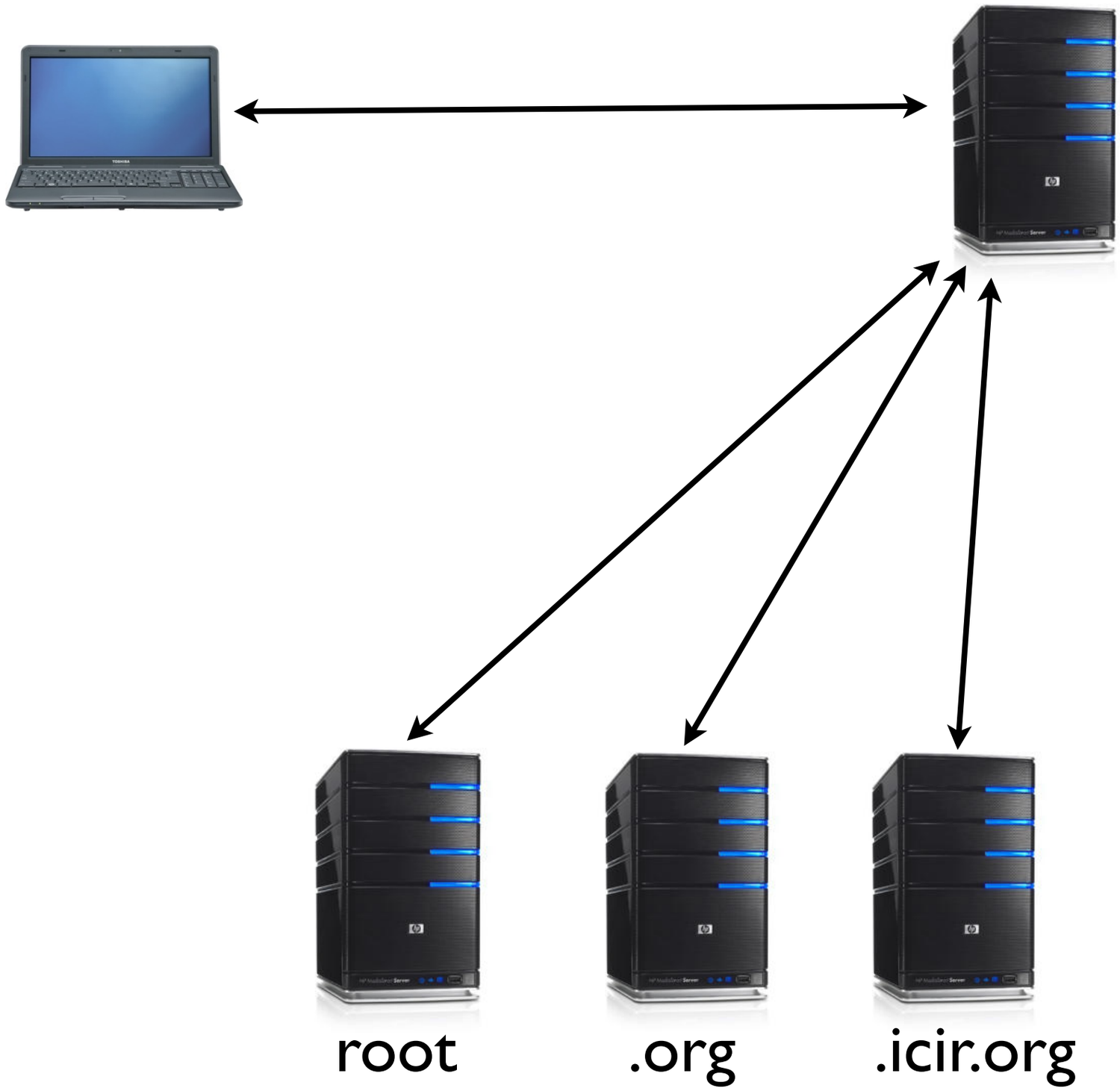
```
Answer:
   type: A
   name: www.icir.org
   addr: 192.150.187.12
```



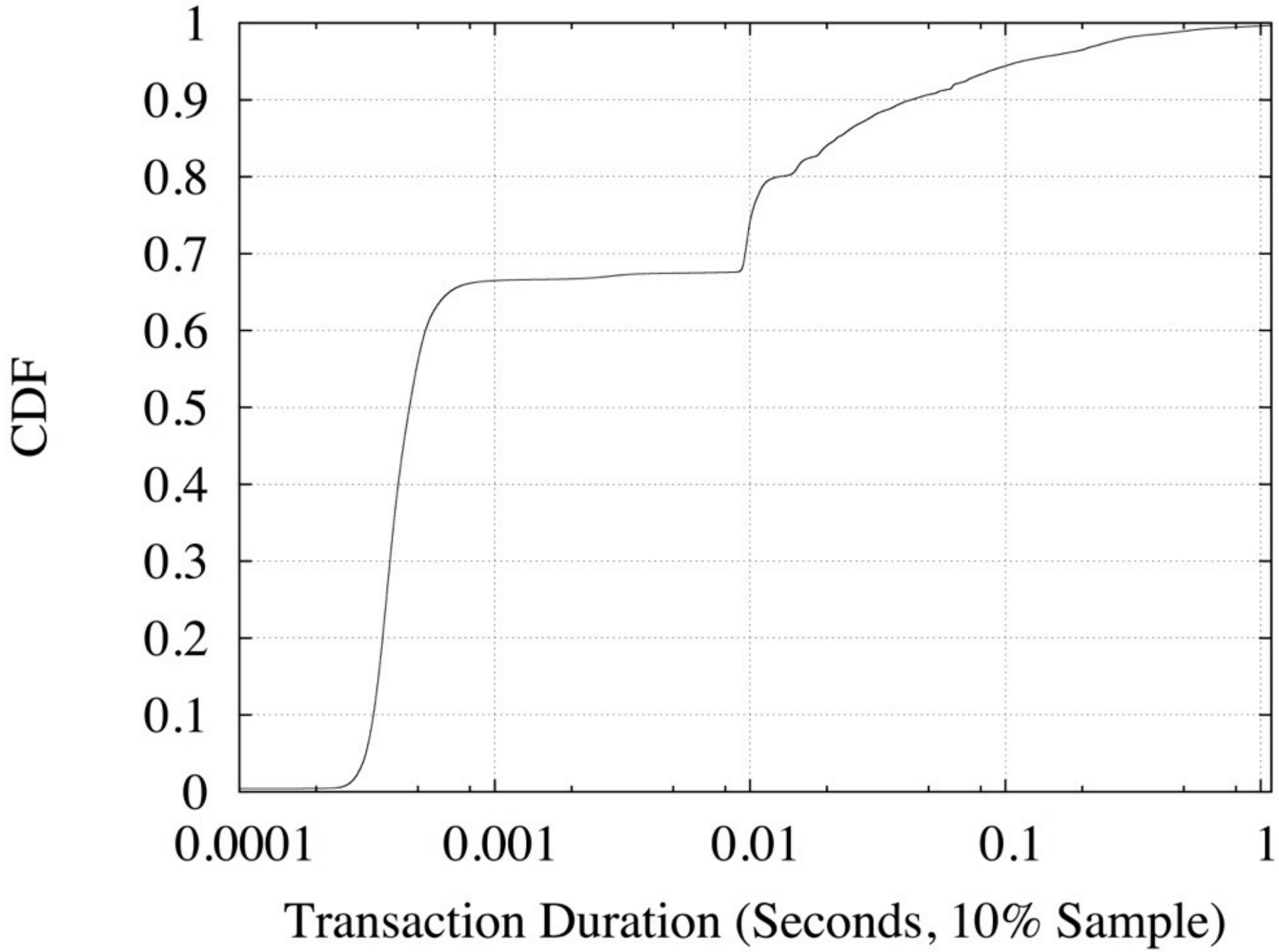
Basic Structure



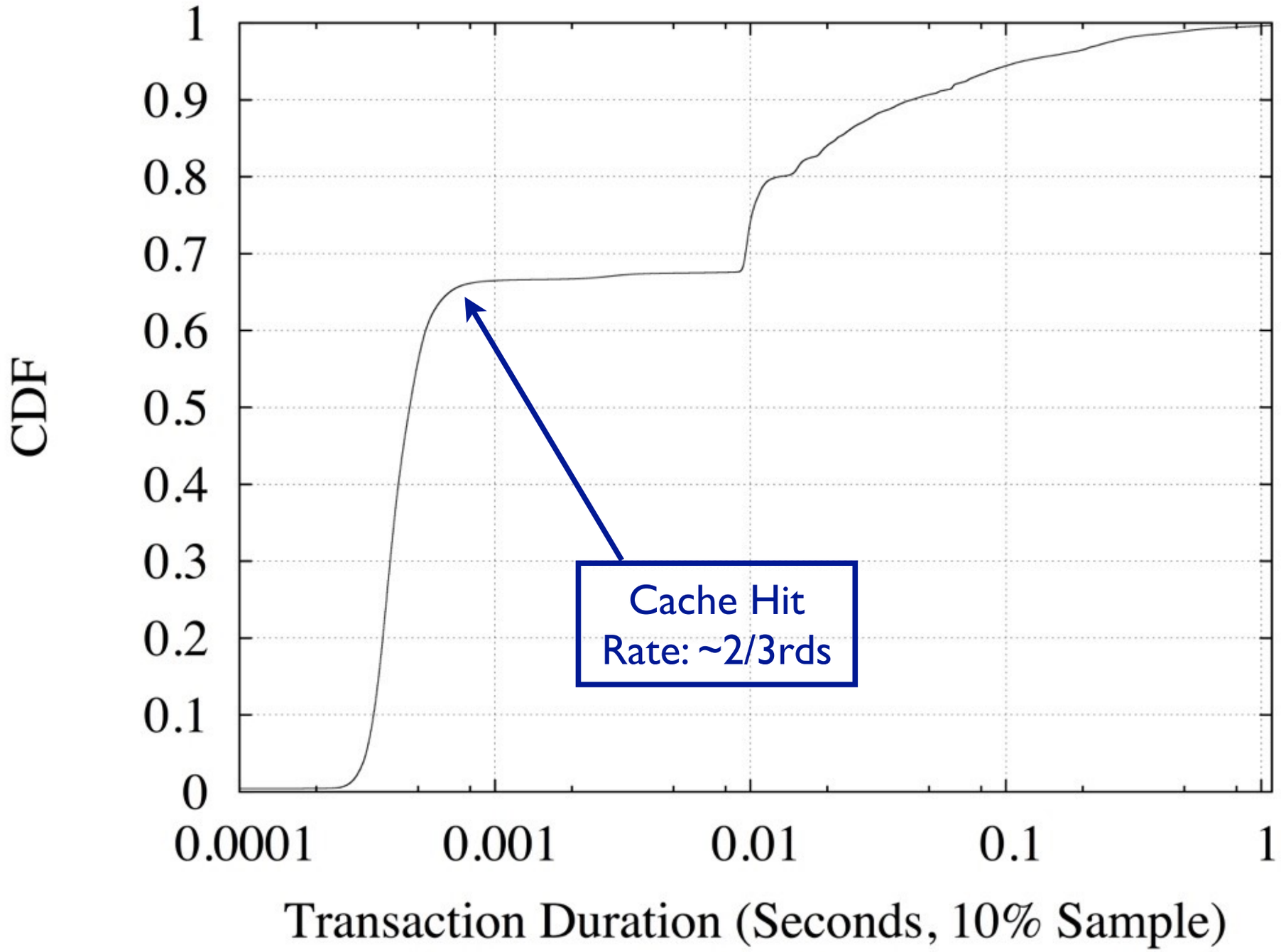
Delegating Resolution



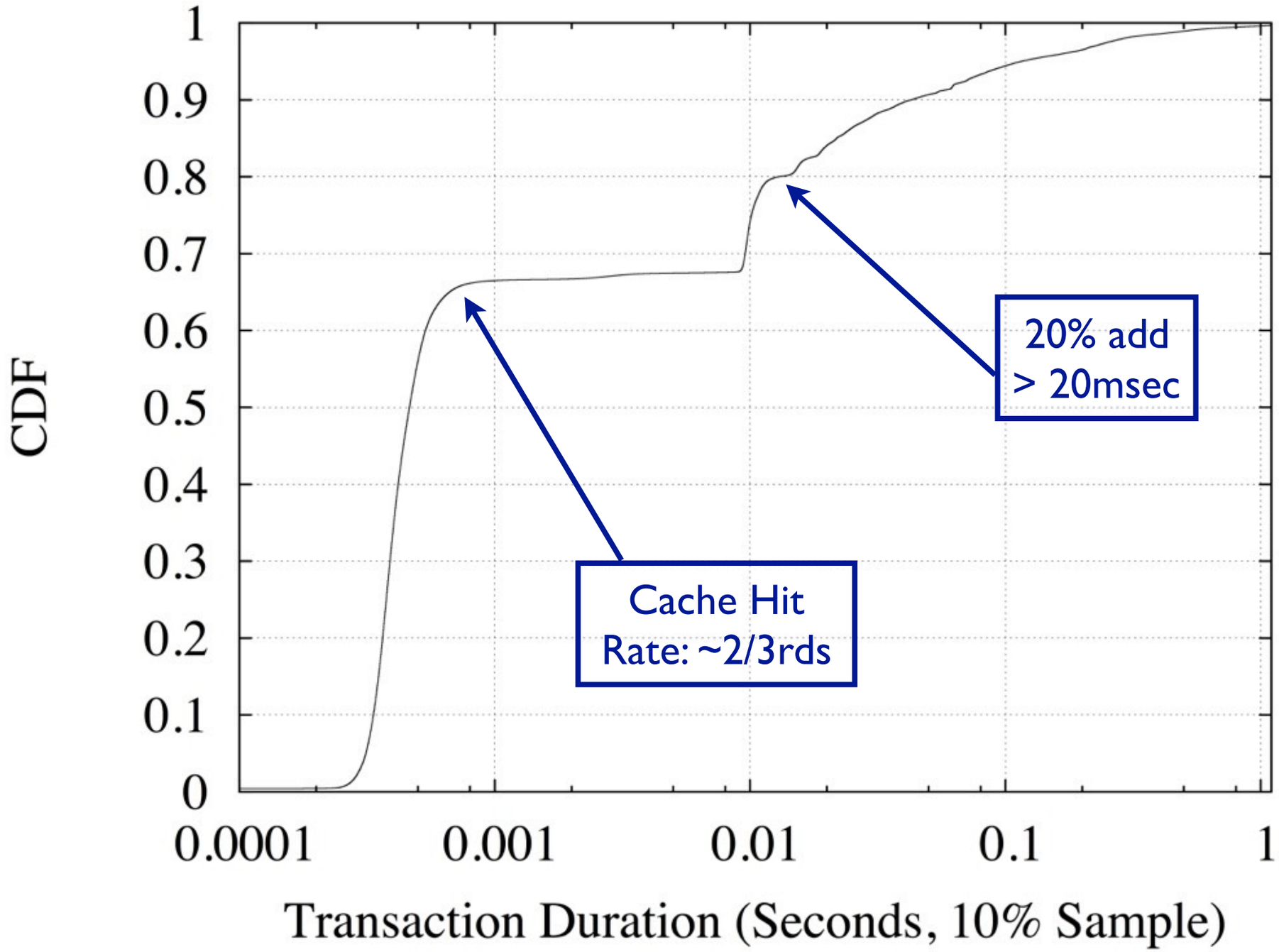
Caching Efficacy



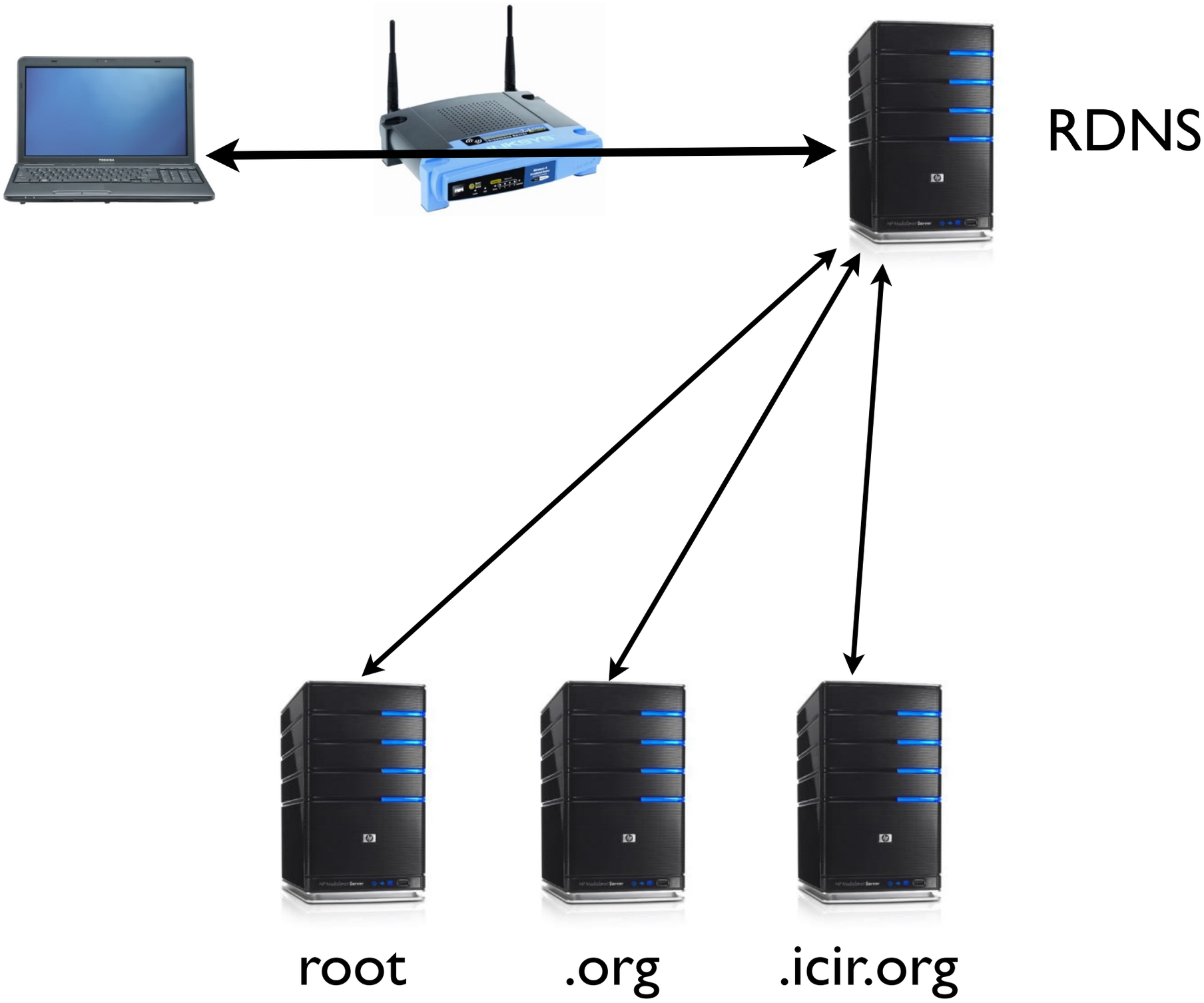
Caching Efficacy



Caching Efficacy



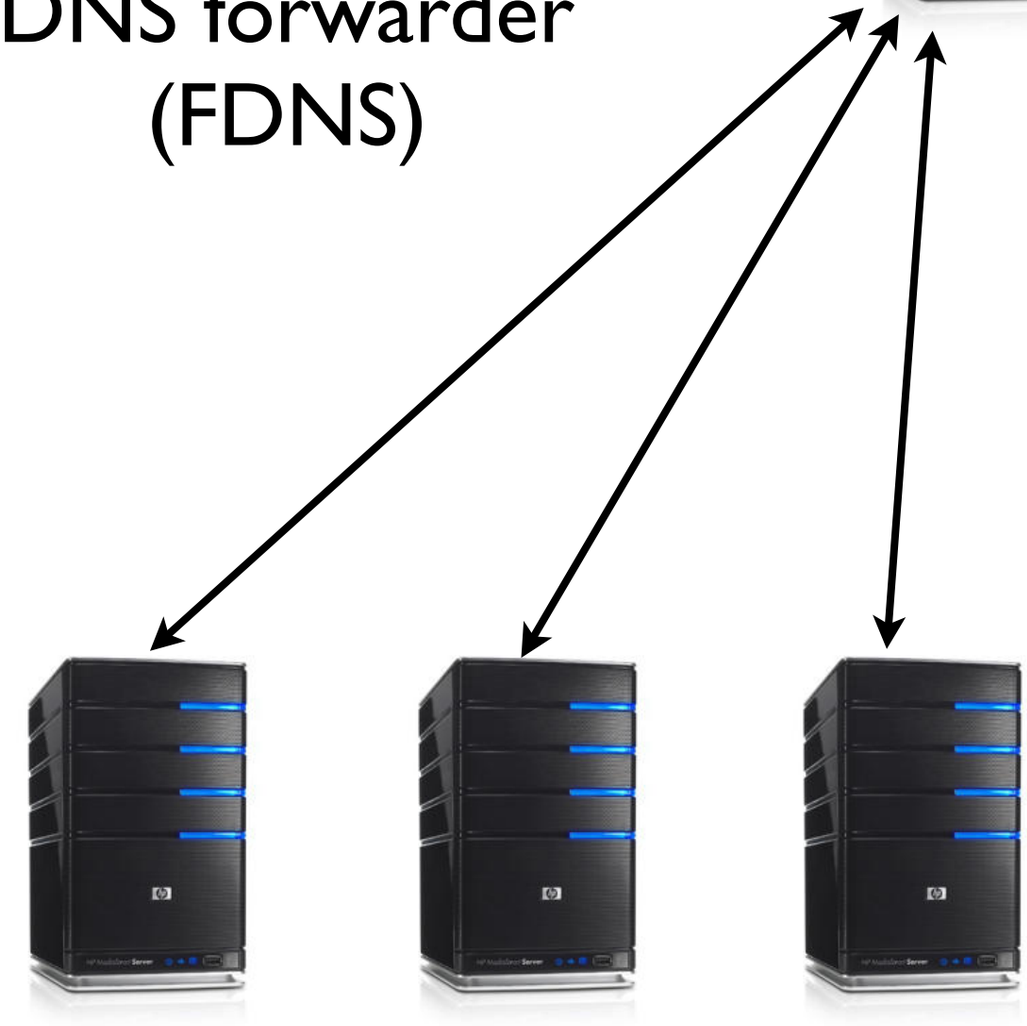
More Delegation!



More Delegation!

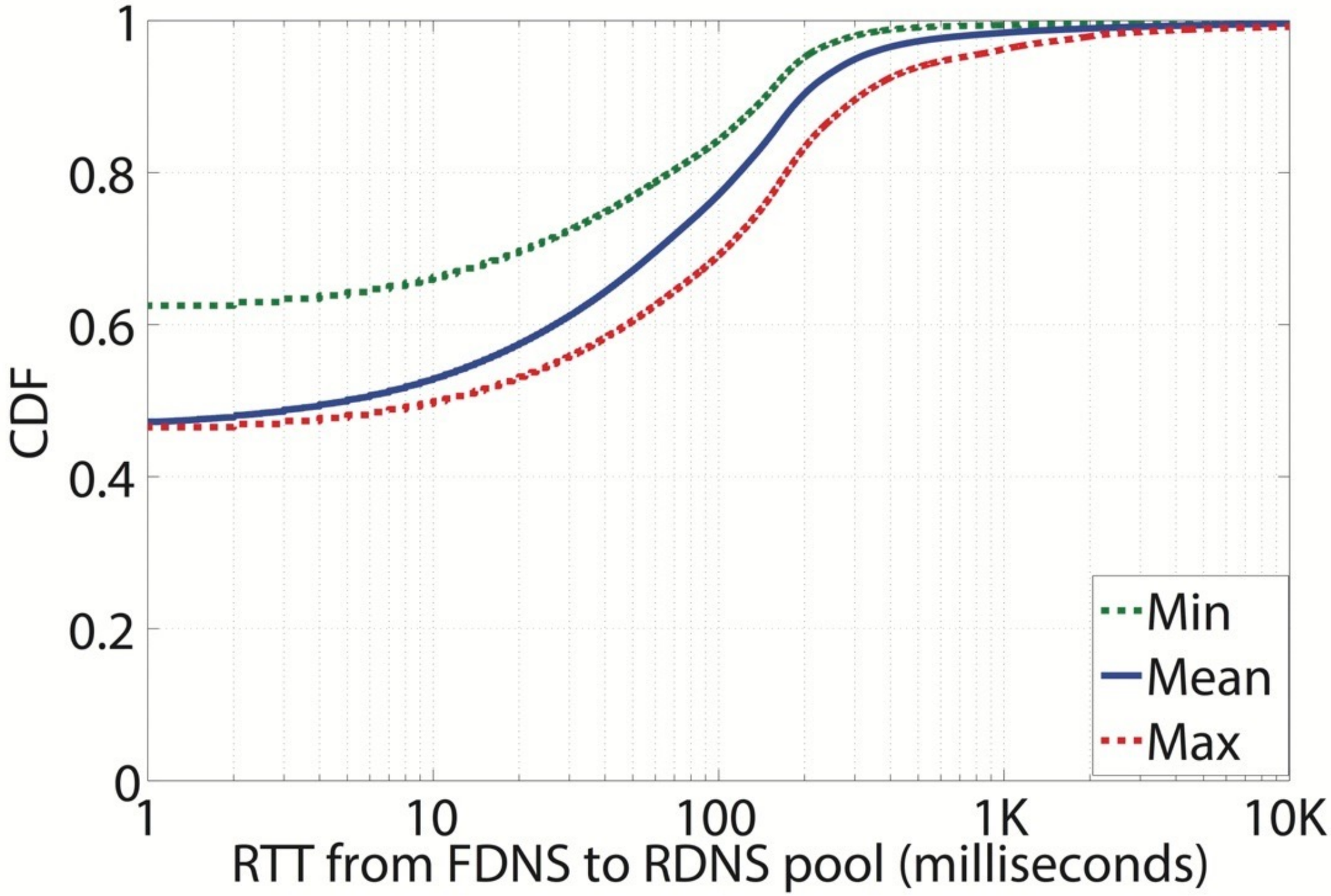
DNS forwarder
(FDNS)

RDNS

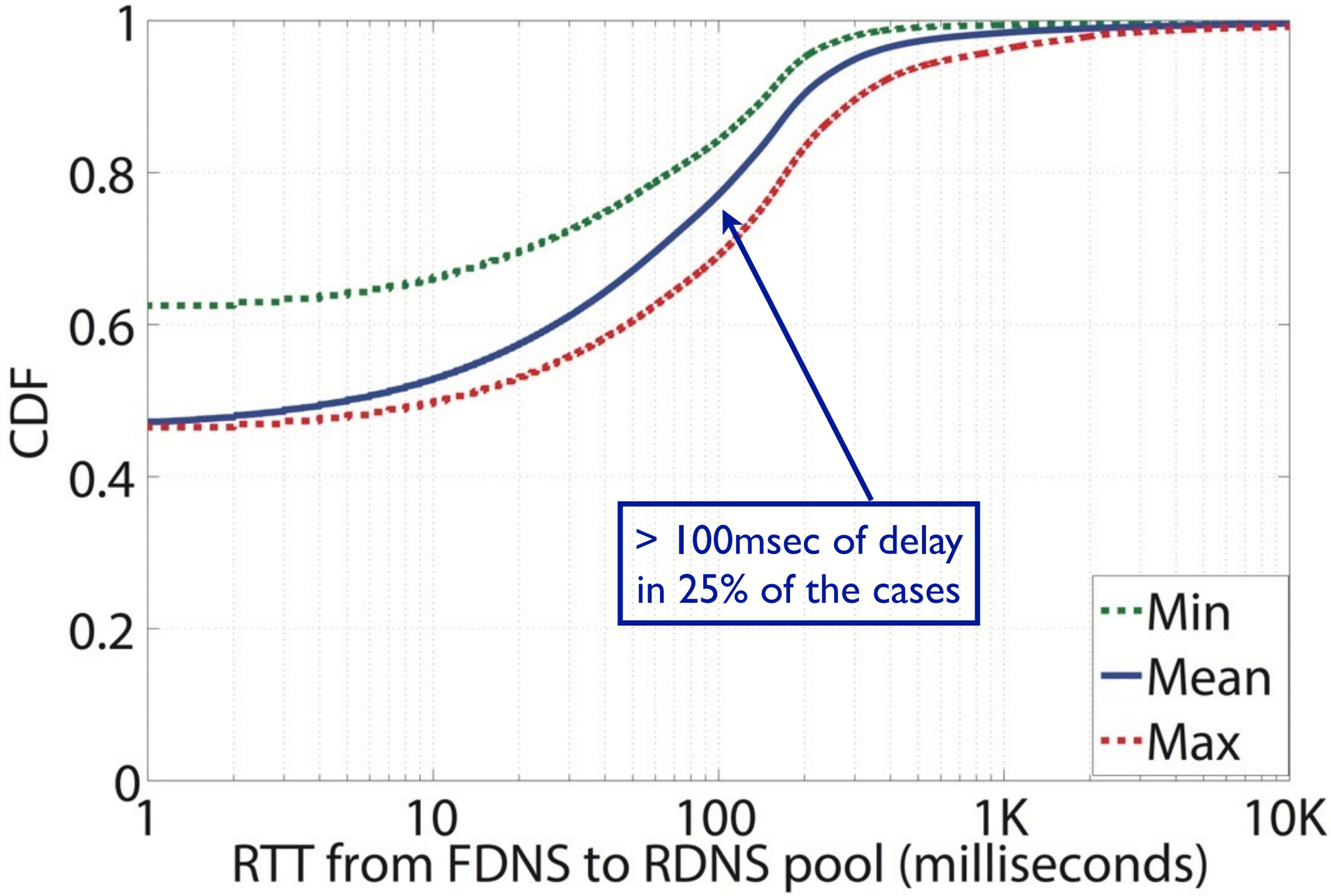


root .org .icir.org

FDNS-to-RDNS Delay



FDNS-to-RDNS Delay



Implementation Diversity

Implementation Diversity

- All like components do not always act the same

Implementation Diversity

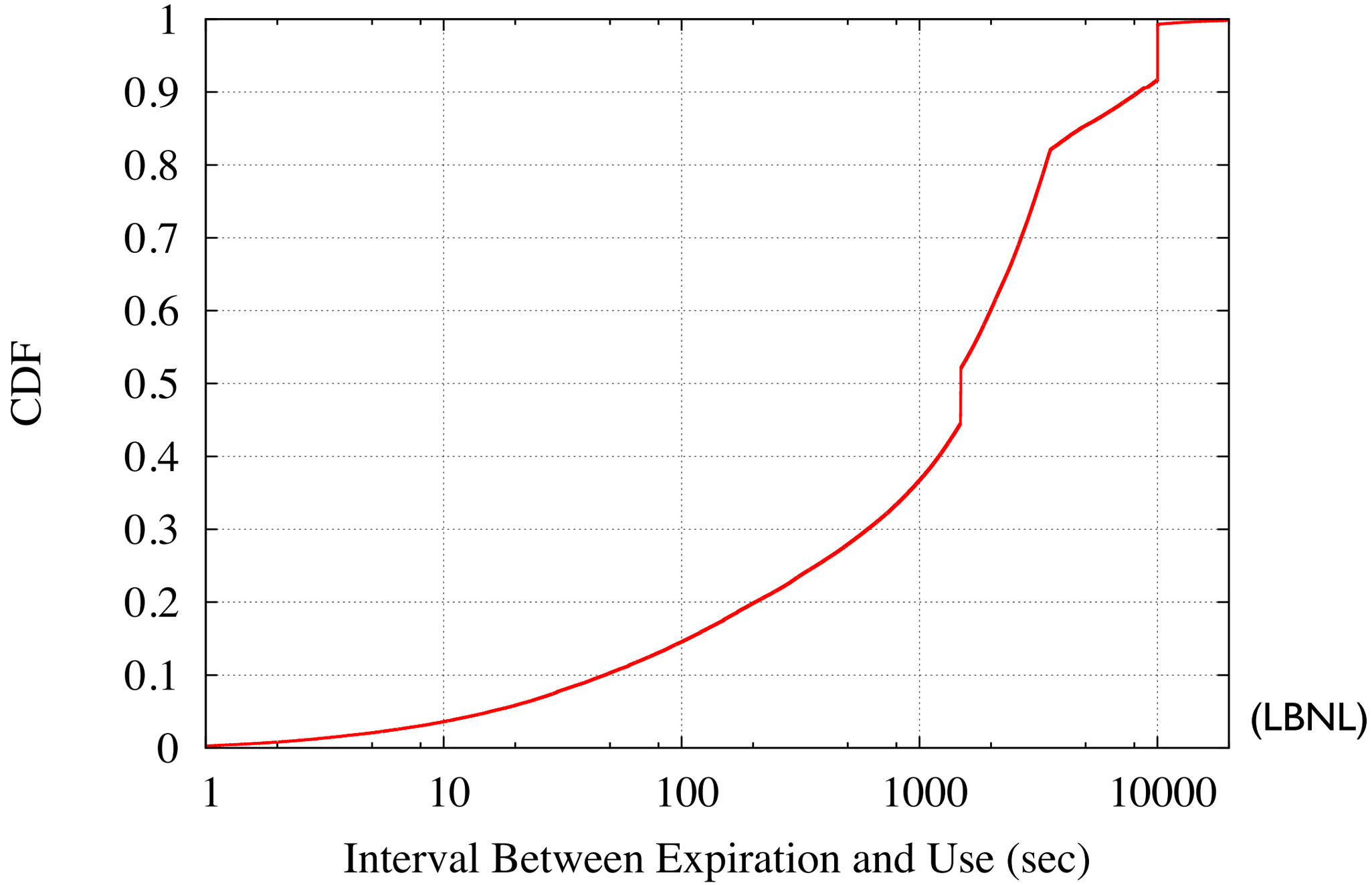
- All like components do not always act the same
- E.g., clients do not always adhere to the TTL

Implementation Diversity

- All like components do not always act the same
- E.g., clients do not always adhere to the TTL

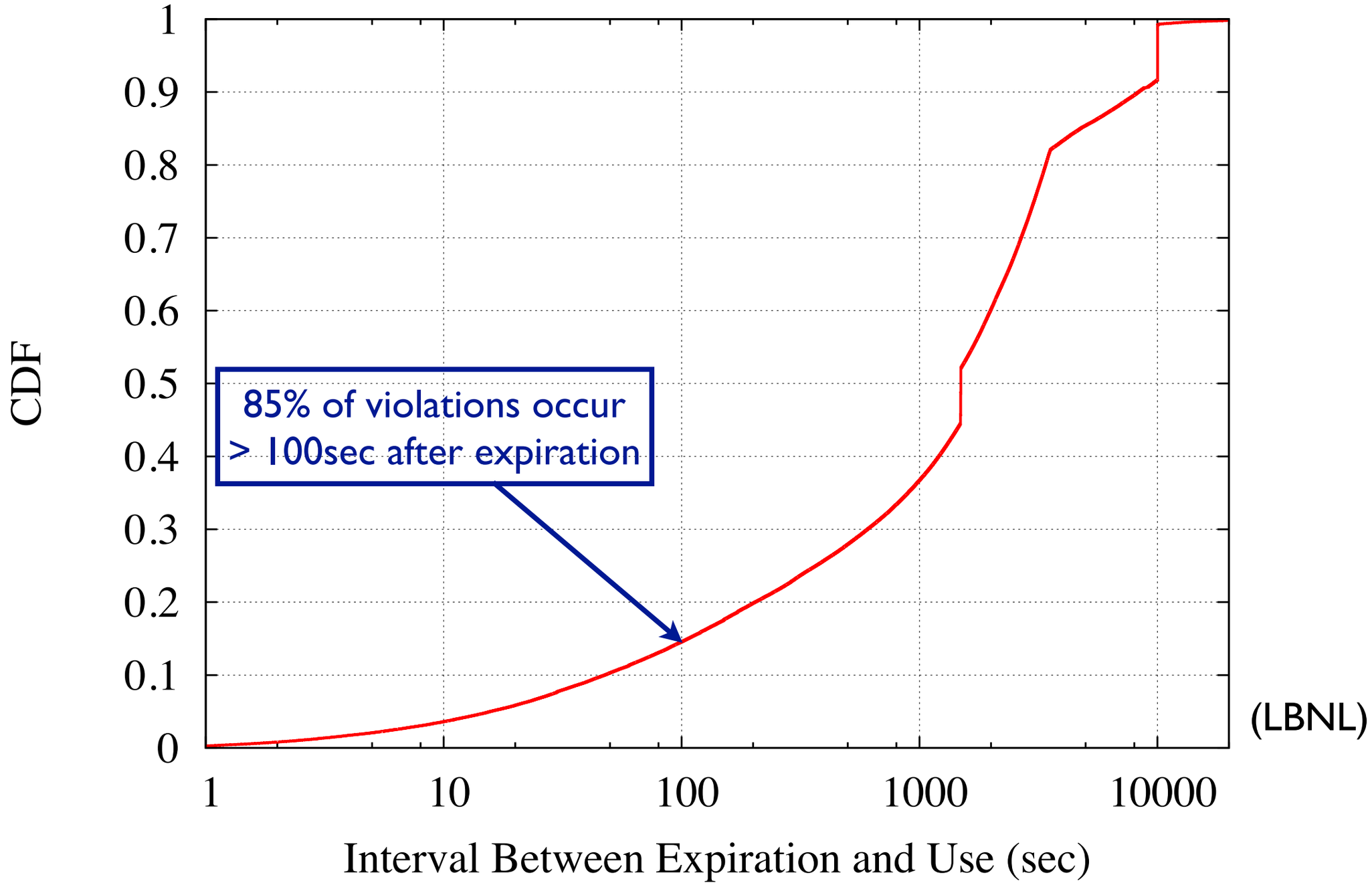
Network	Cnns.	TTL Exp.
ICSI	443K	30%
CCZ	817K	8%
LBNL	6.1M	14%

TTL Violations

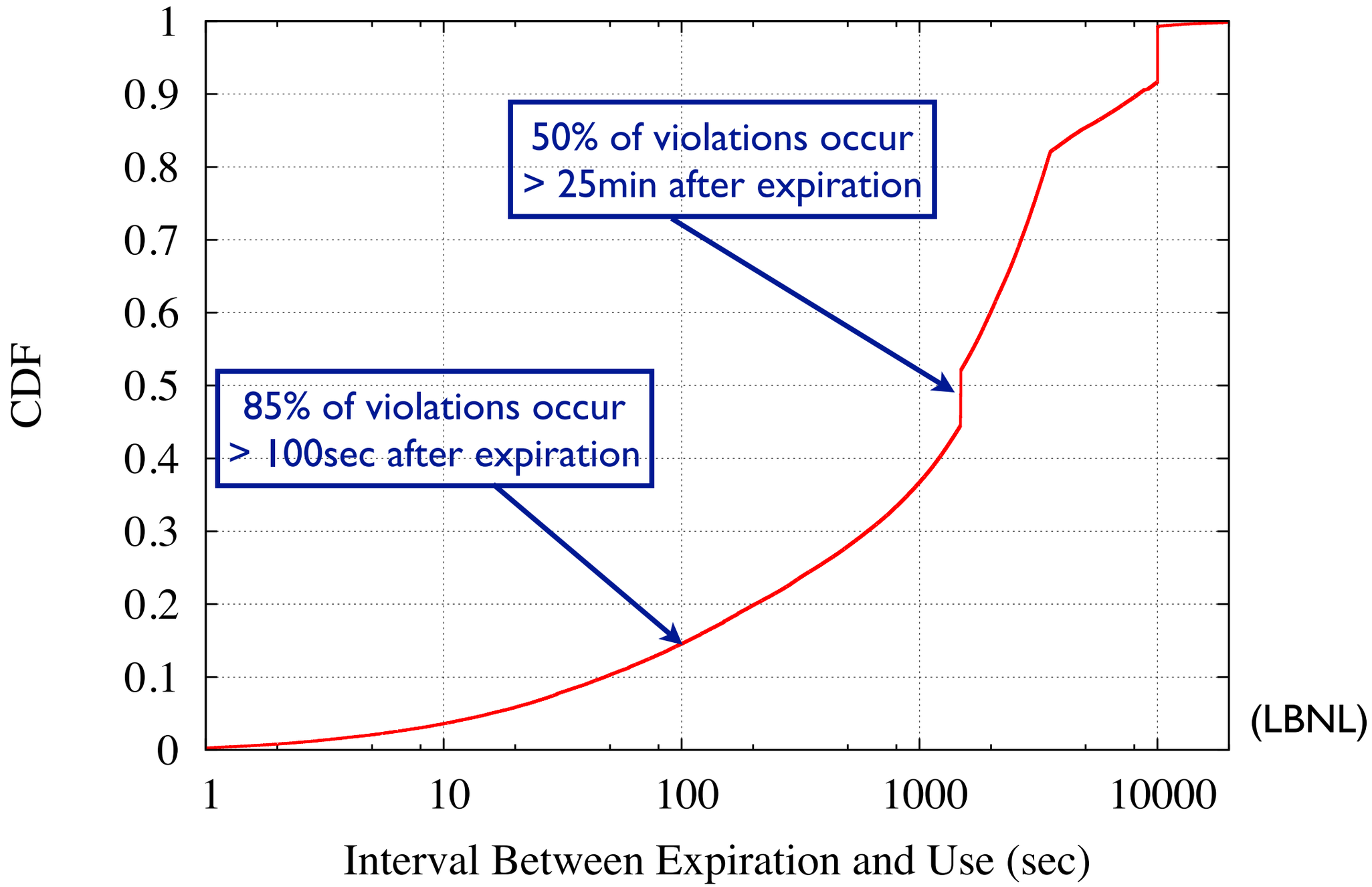


(LBNL)

TTL Violations

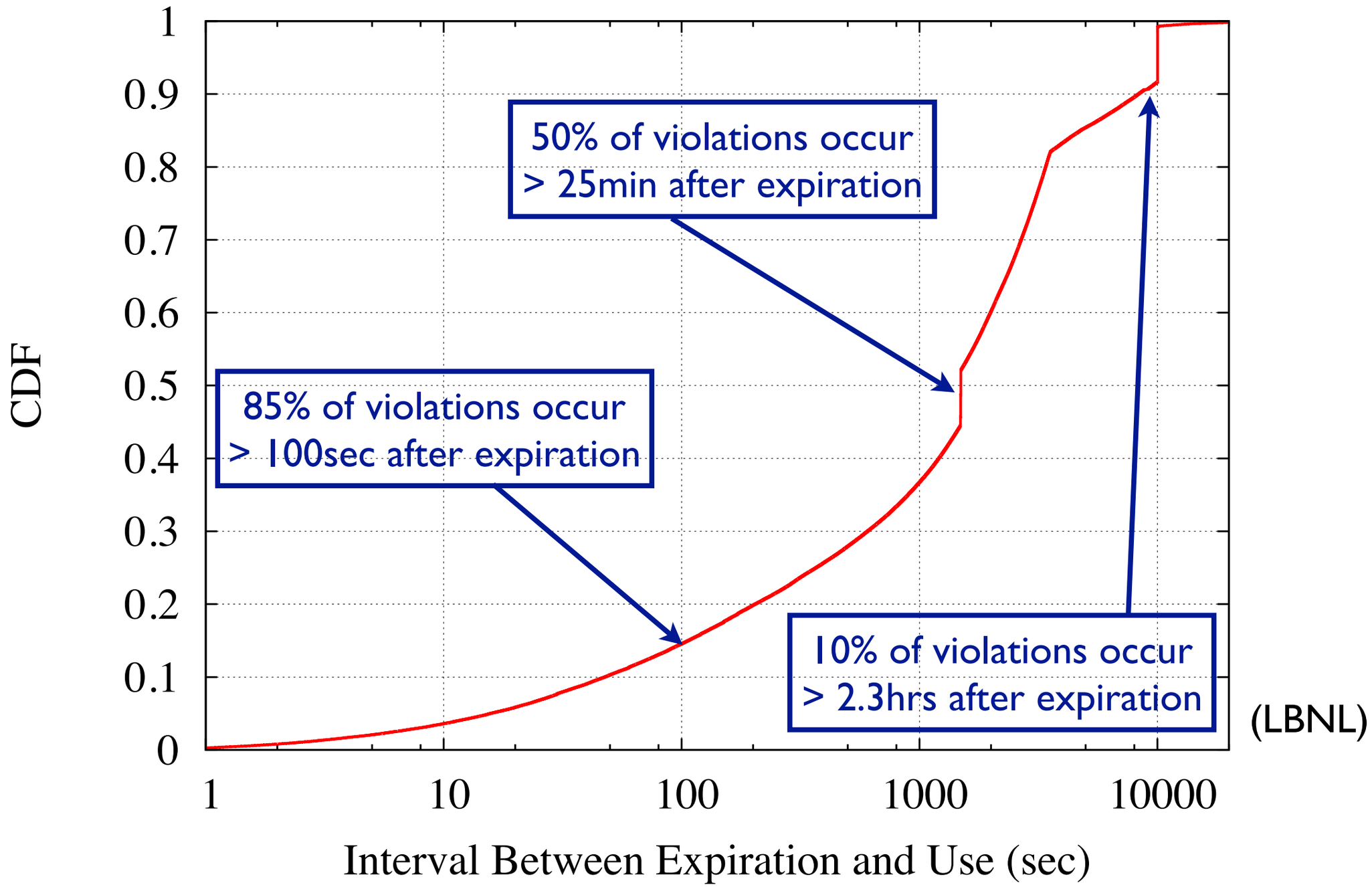


TTL Violations



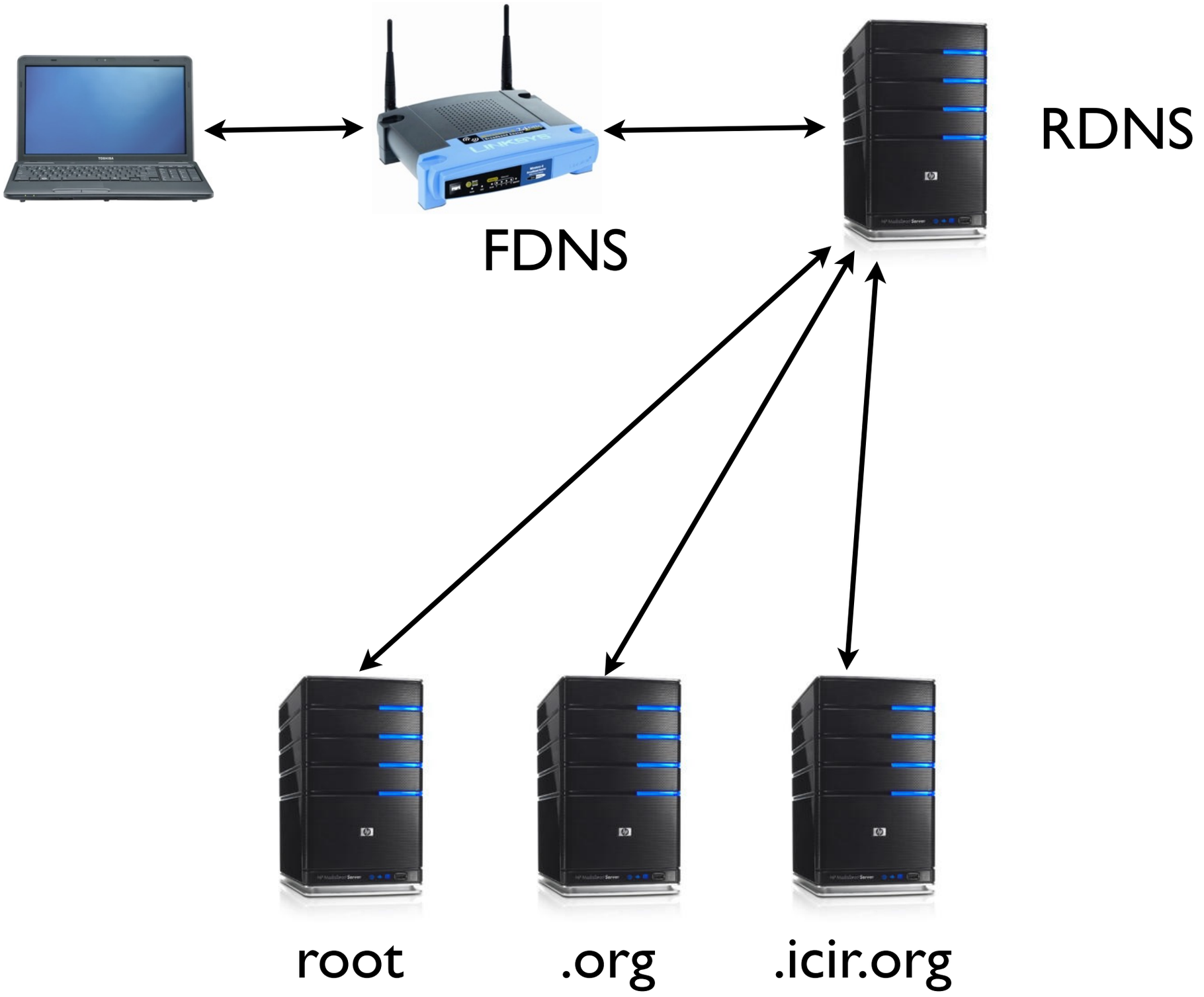
(LBNL)

TTL Violations



(LBNL)

Replication



Replication

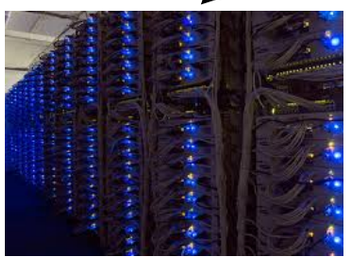
RDNS

root .org .icir.org

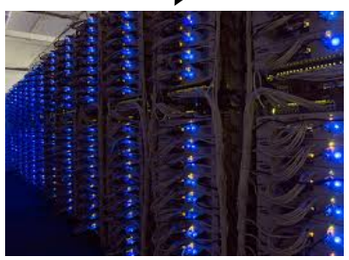
Replication

FDNS

RDNS



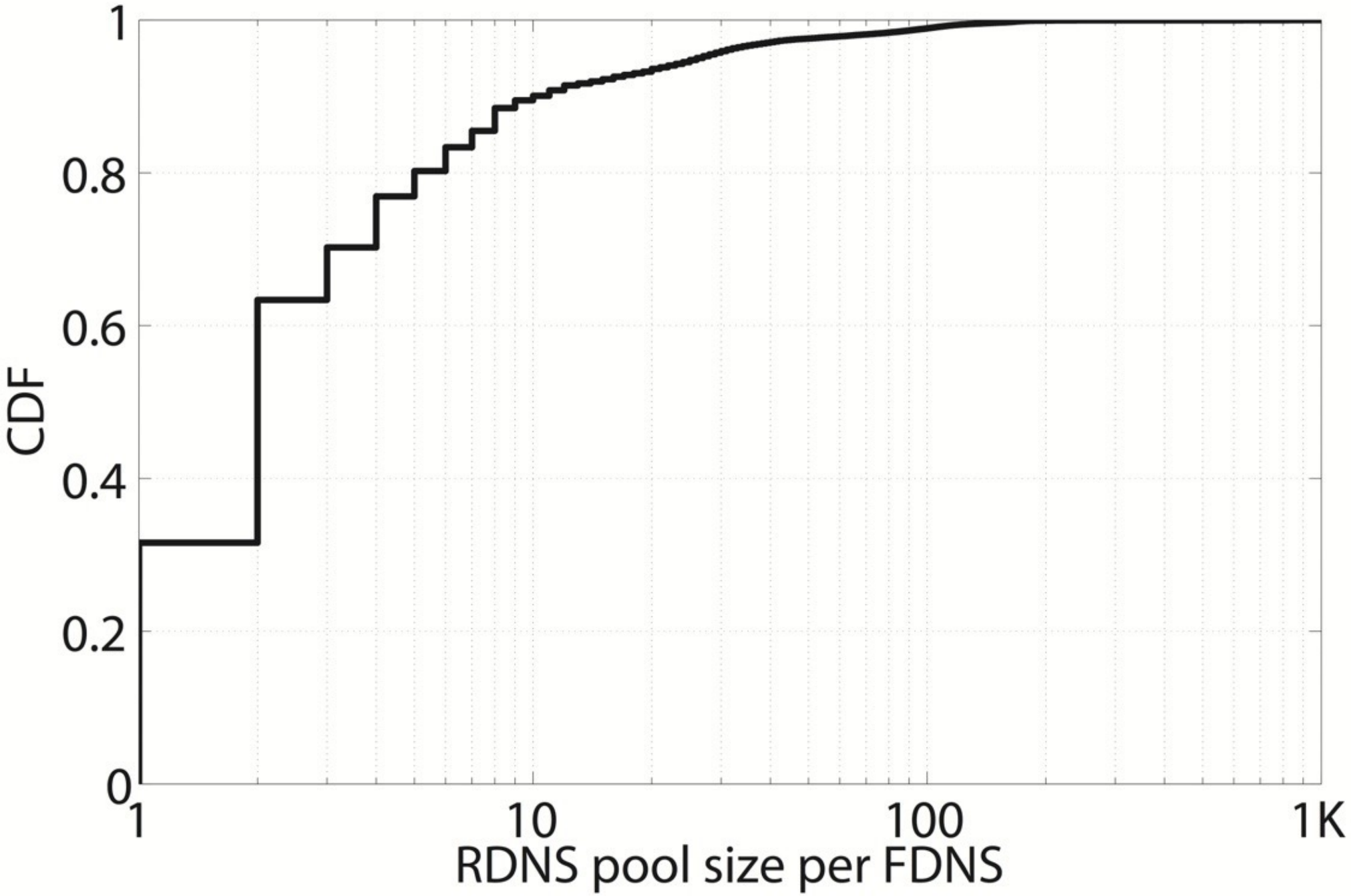
root



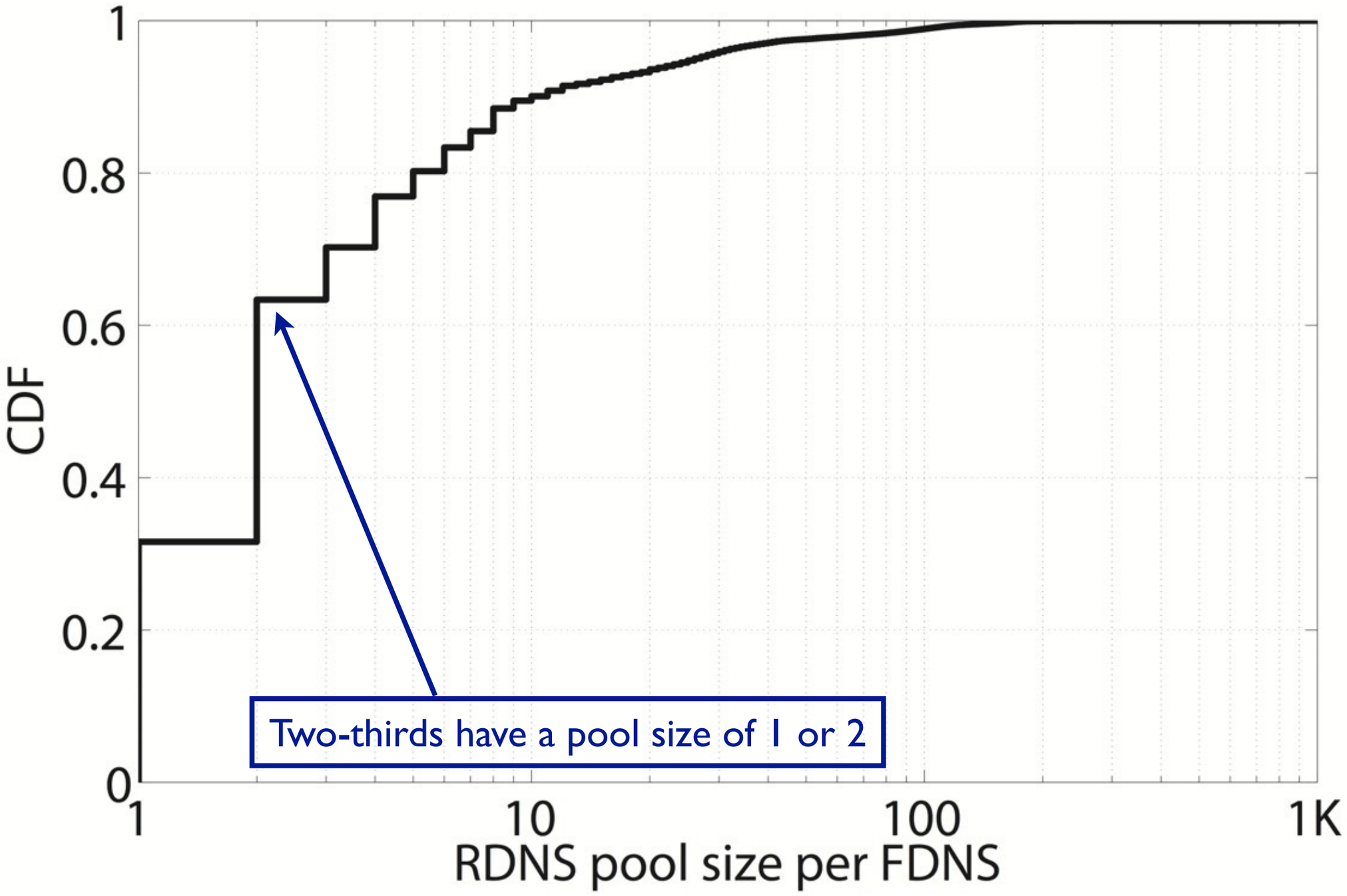
.org

.icir.org

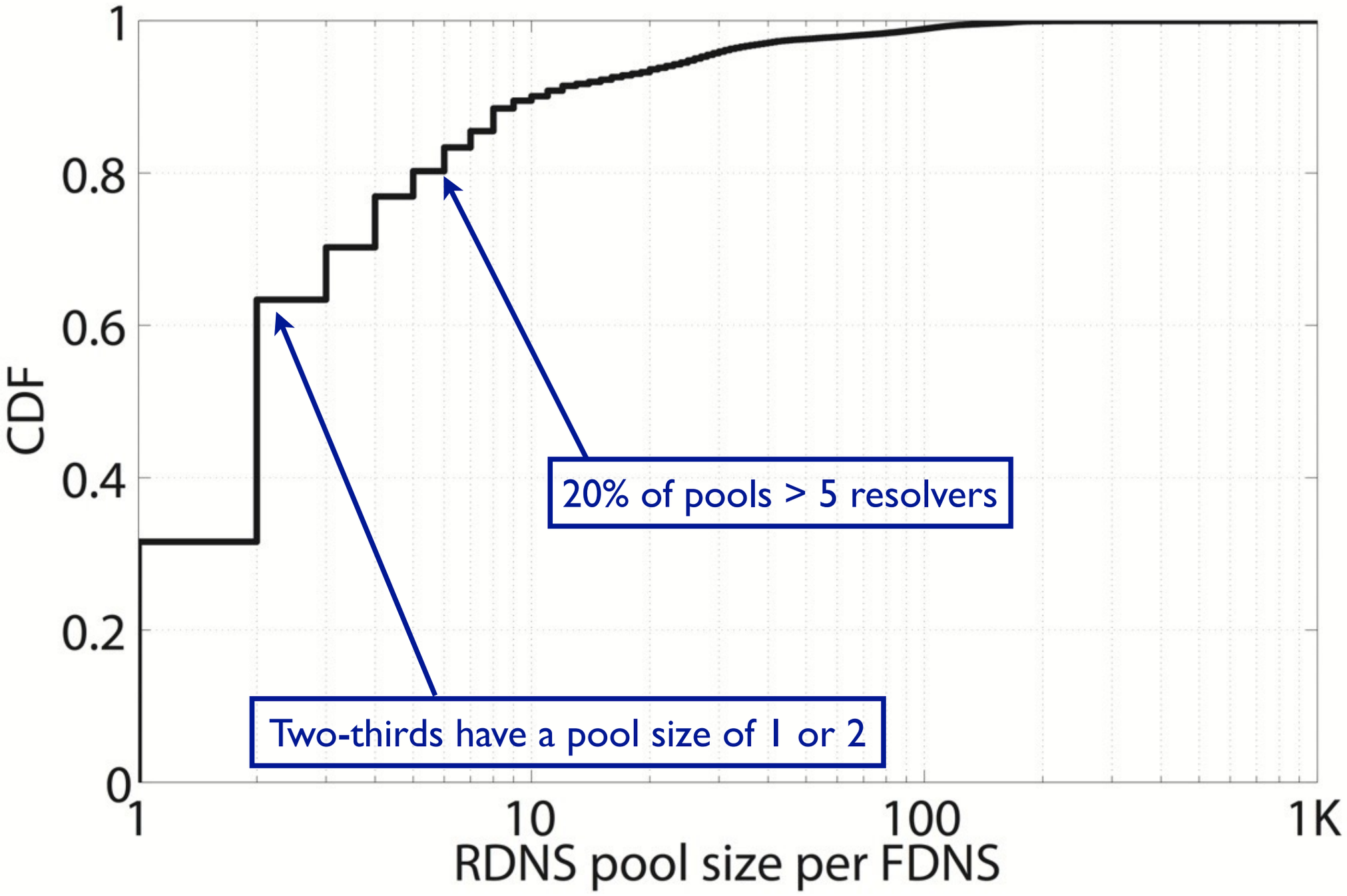
RDNS Pool Size



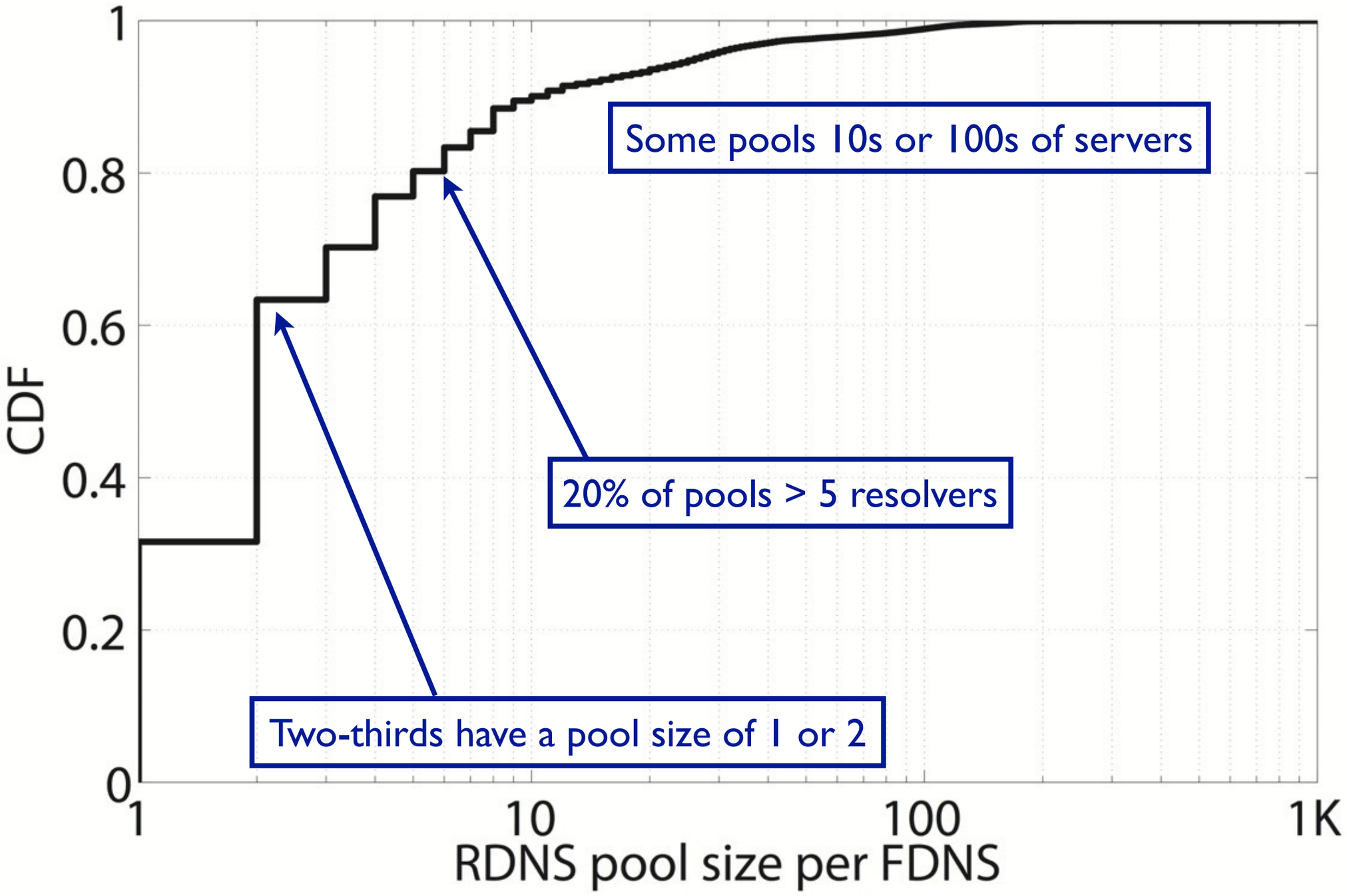
RDNS Pool Size



RDNS Pool Size



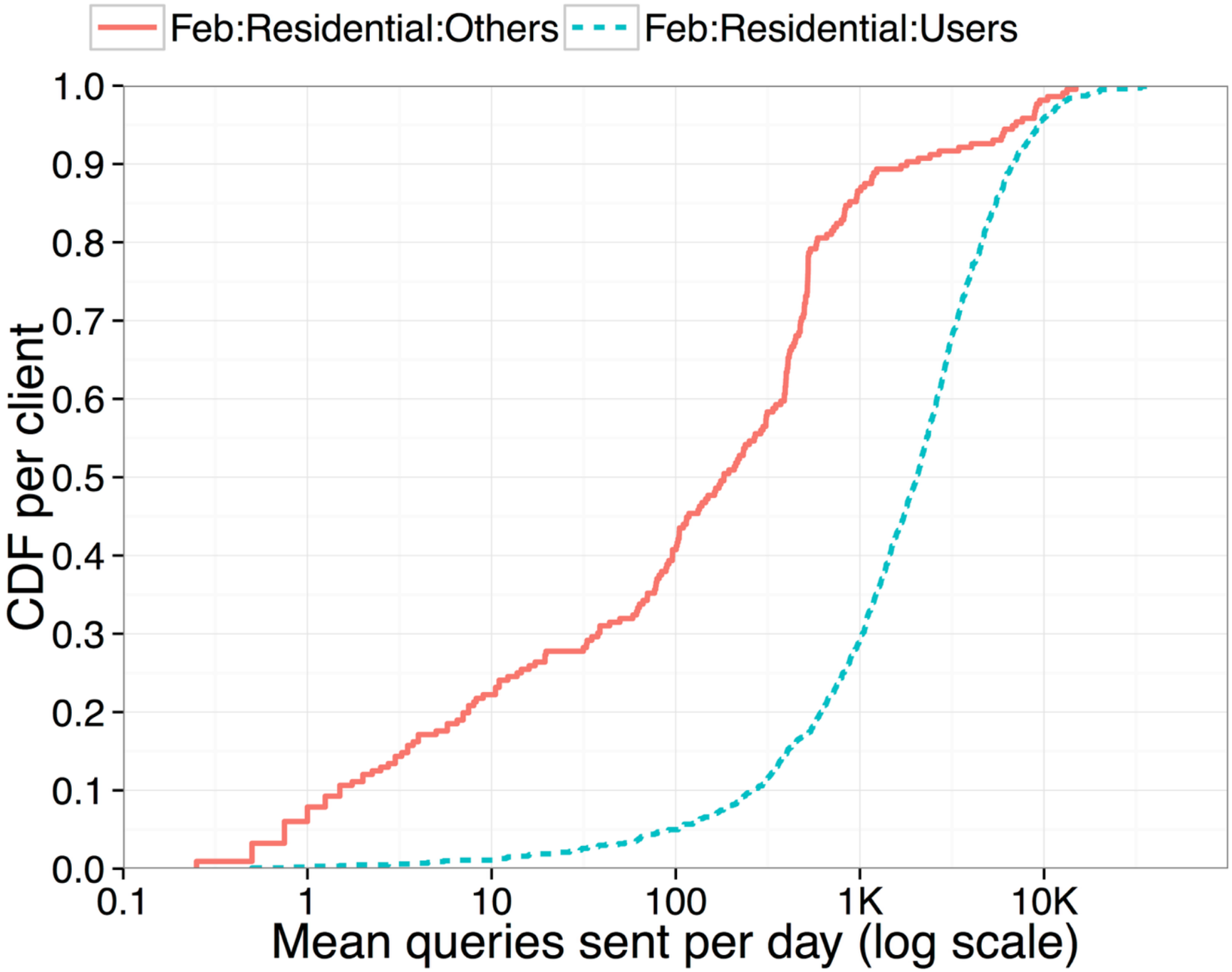
RDNS Pool Size



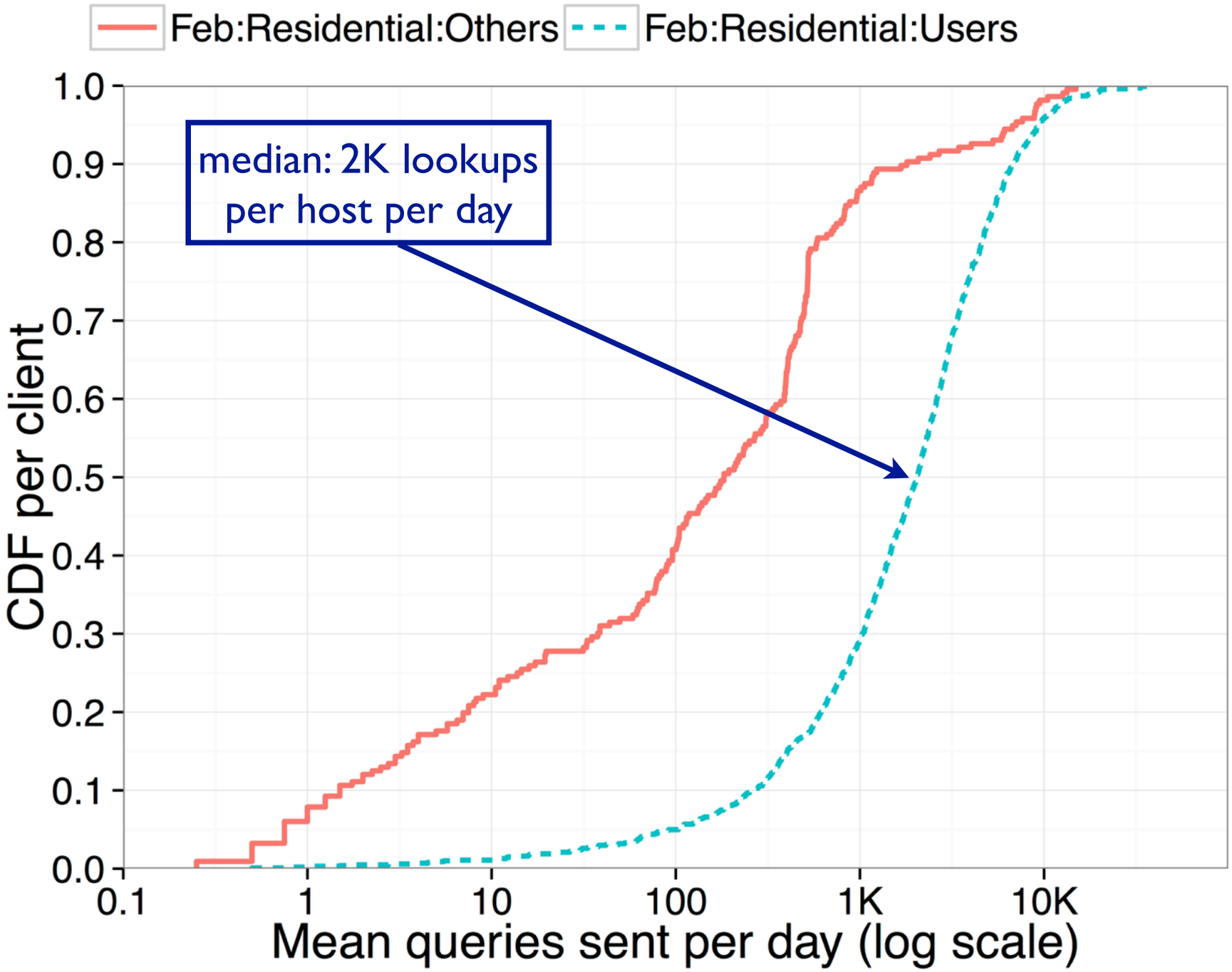
User Behavior

- Moving away from the infrastructure …
- How about user behavior?

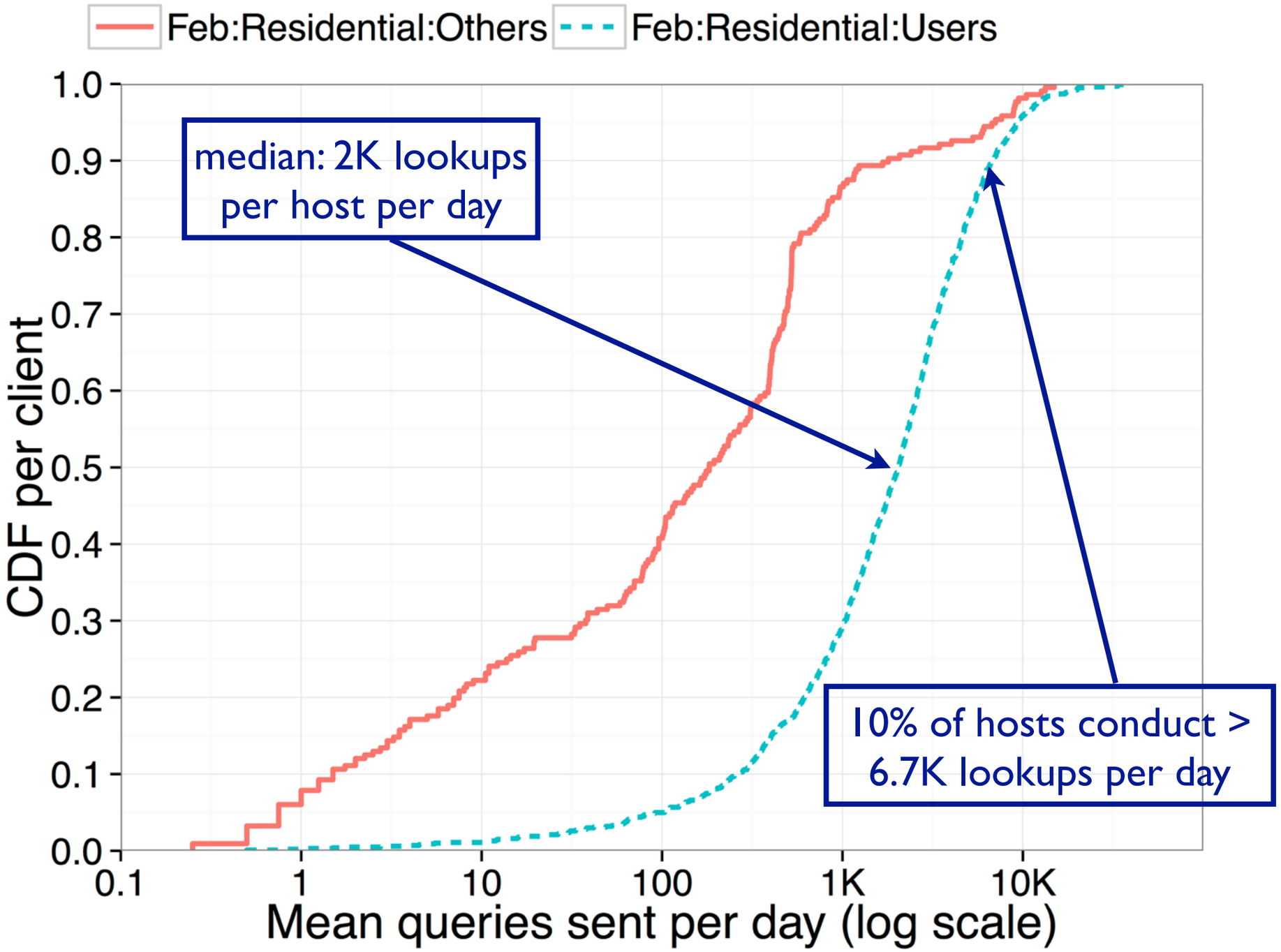
Query Rate


Feb:Residential:Others
Feb:Residential:Users
CDF per client
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
0.1
1
10
100
1K
10K
Mean queries sent per day (log scale)

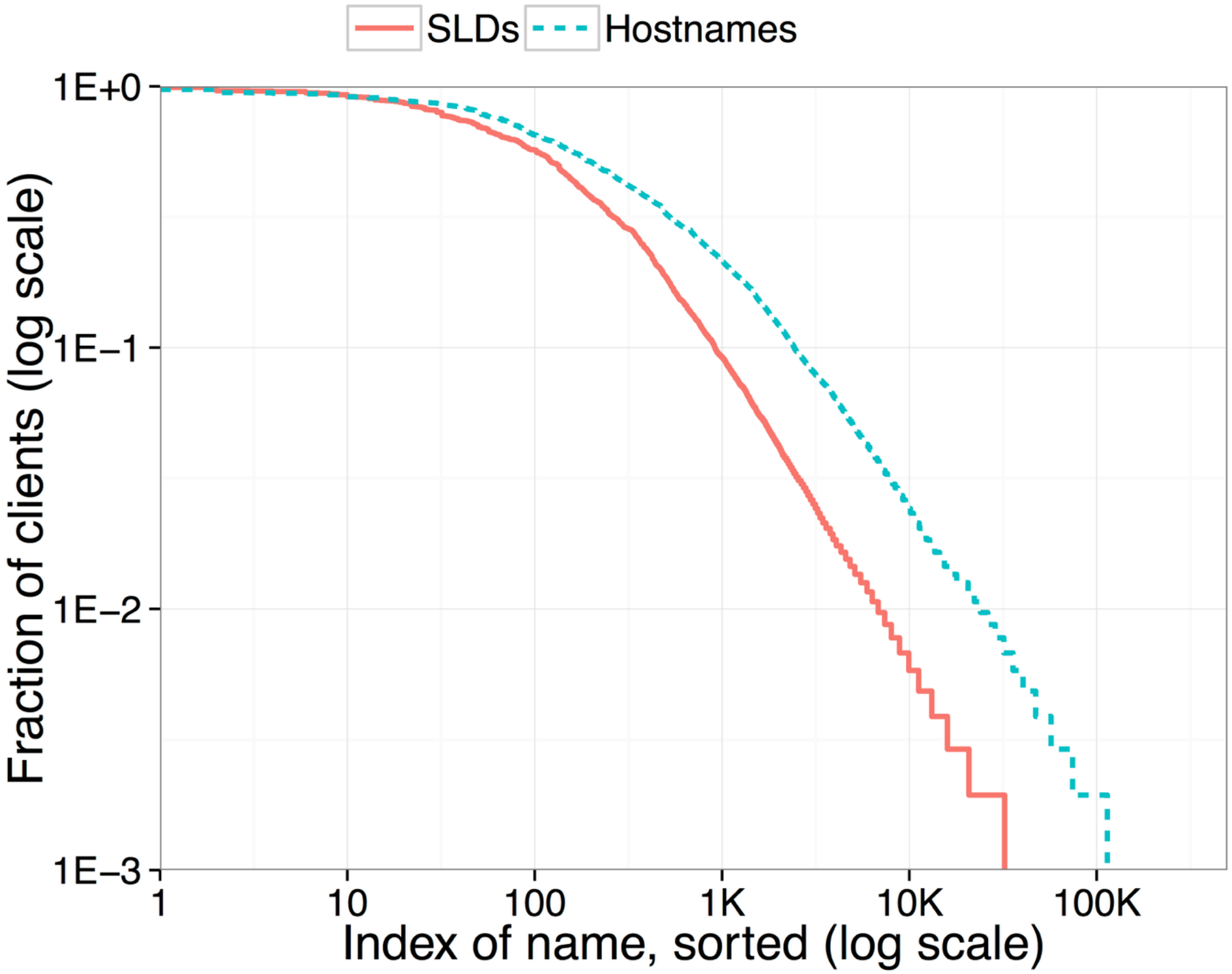
Query Rate


Feb:Residential:Others
Feb:Residential:Users
median: 2K lookups per host per day
CDF per client
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
0.1
1
10
100
1K
10K
Mean queries sent per day (log scale)

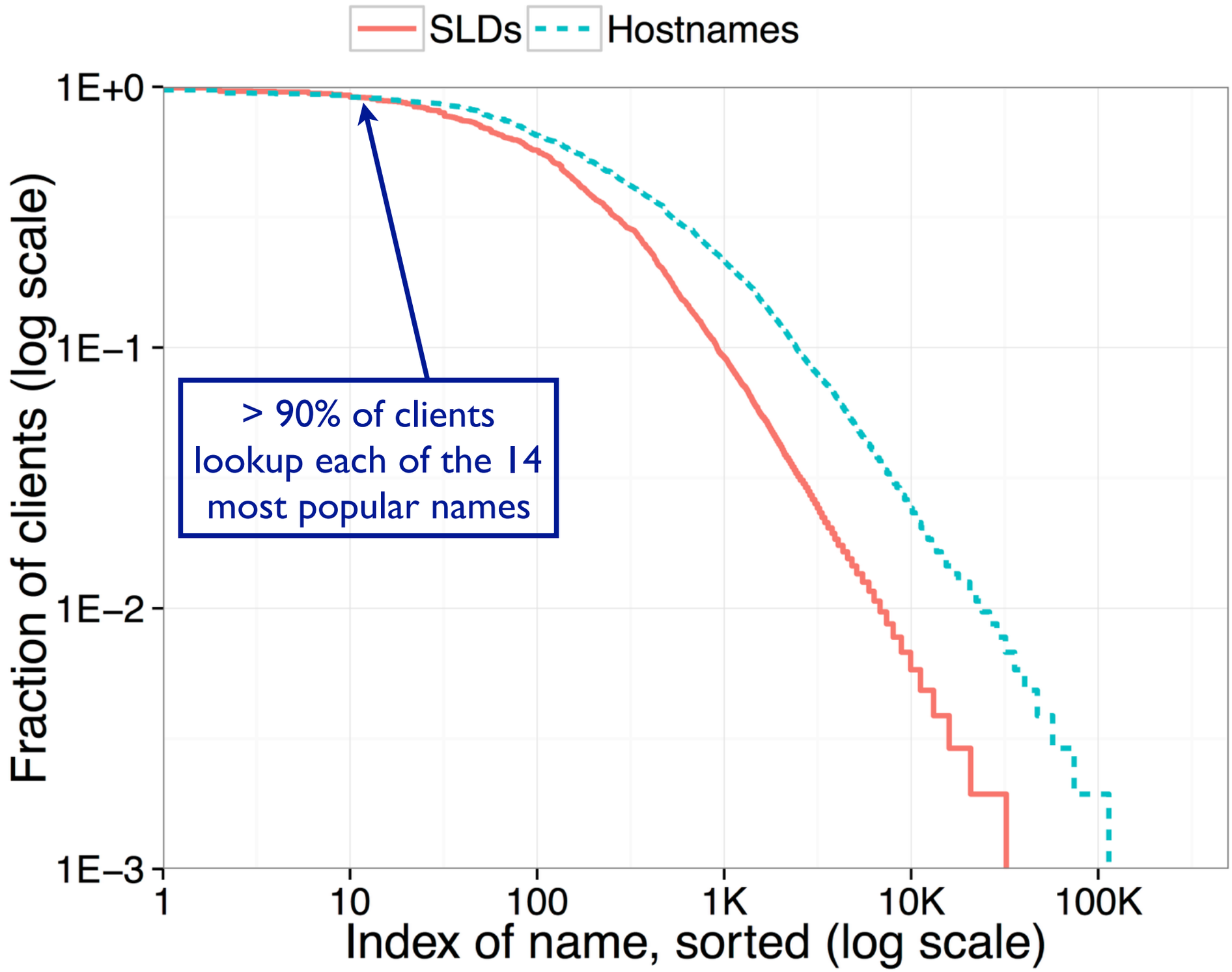
Query Rate


Feb:Residential:Others
Feb:Residential:Users
median: 2K lookups per host per day
10% of hosts conduct > 6.7K lookups per day
CDF per client
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
0.1
1
10
100
1K
10K
Mean queries sent per day (log scale)

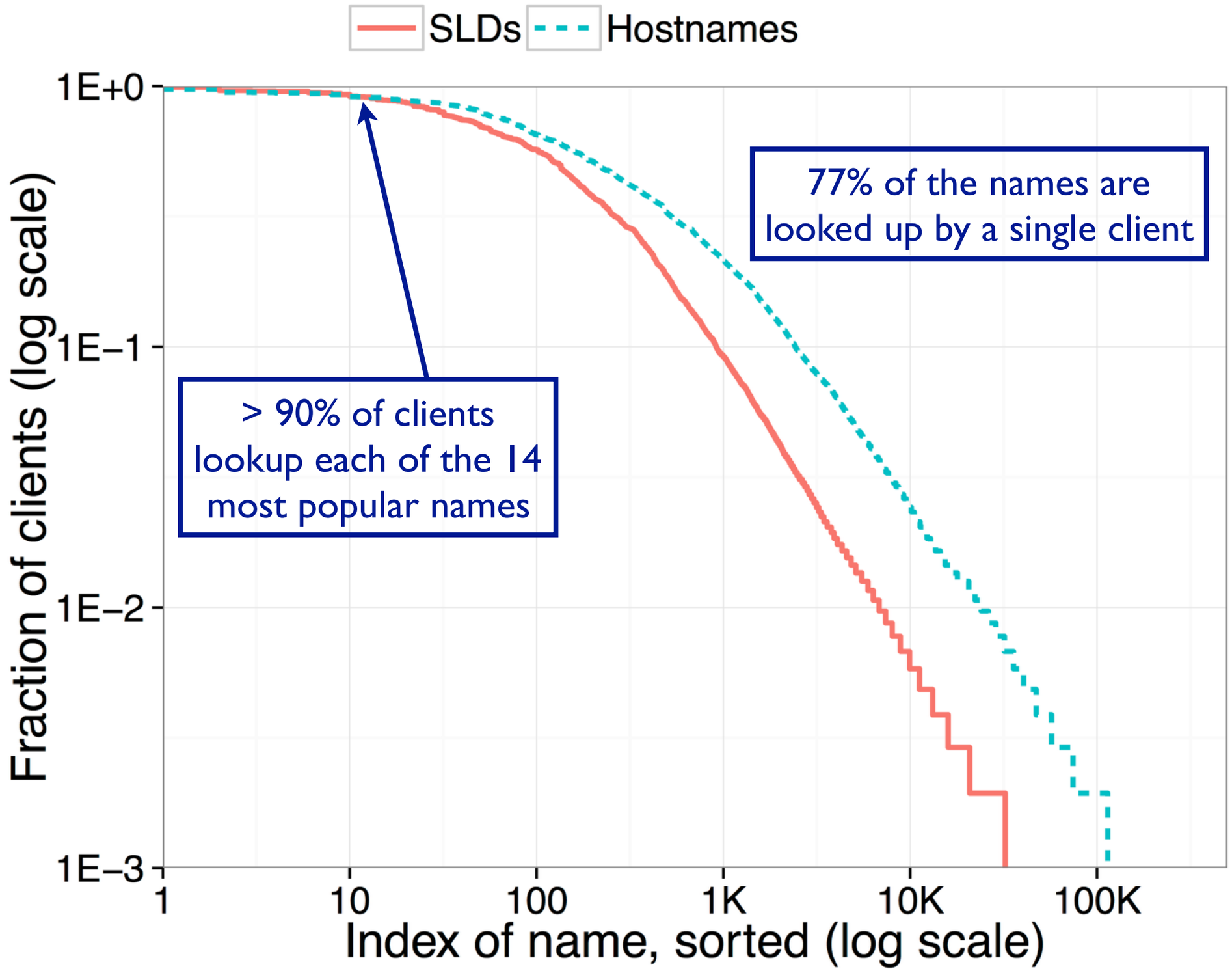
Name Popularity



Name Popularity



Name Popularity



Of Blessings and Curses ....

Of Blessings and Curses ....

- *Open resolvers* are a common component of the DNS ecosystem
  - will answer DNS queries for *any host*

Of Blessings and Curses ....

- *Open resolvers* are a common component of the DNS ecosystem
  - will answer DNS queries for *any host*
- Curse: security issues
  - can circumvent RDNS policy, etc.

Of Blessings and Curses ....

- *Open resolvers* are a common component of the DNS ecosystem
  - will answer DNS queries for *any host*
- Curse: security issues
  - can circumvent RDNS policy, etc.
- Blessing: provide us with myriad *measurement vantage points*

Open Resolvers

Open Resolvers

- 15M open resolvers in 2010
  (Leonard & Loguinov, IMC 2010)

Open Resolvers

- 15M open resolvers in 2010
  (Leonard & Loguinov, IMC 2010)
- 32M open resolvers in 2013

Open Resolvers

- 15M open resolvers in 2010
  (Leonard & Loguinov, IMC 2010)
- 32M open resolvers in 2013
  - mostly cheap home networking gear
  - mostly DNS forwarders

Open Resolvers

- 15M open resolvers in 2010
  (Leonard & Loguinov, IMC 2010)
- 32M open resolvers in 2013
  - mostly cheap home networking gear
  - mostly DNS forwarders
- 15M open resolvers in 2017
  (openresolverproject.org)

DNS Security

DNS Security

- DNS' key flaw:

DNS Security

- DNS' key flaw:
  - all transactions in clear text!
  - no trust, no privacy, no integrity

Security Implications

Security Implications

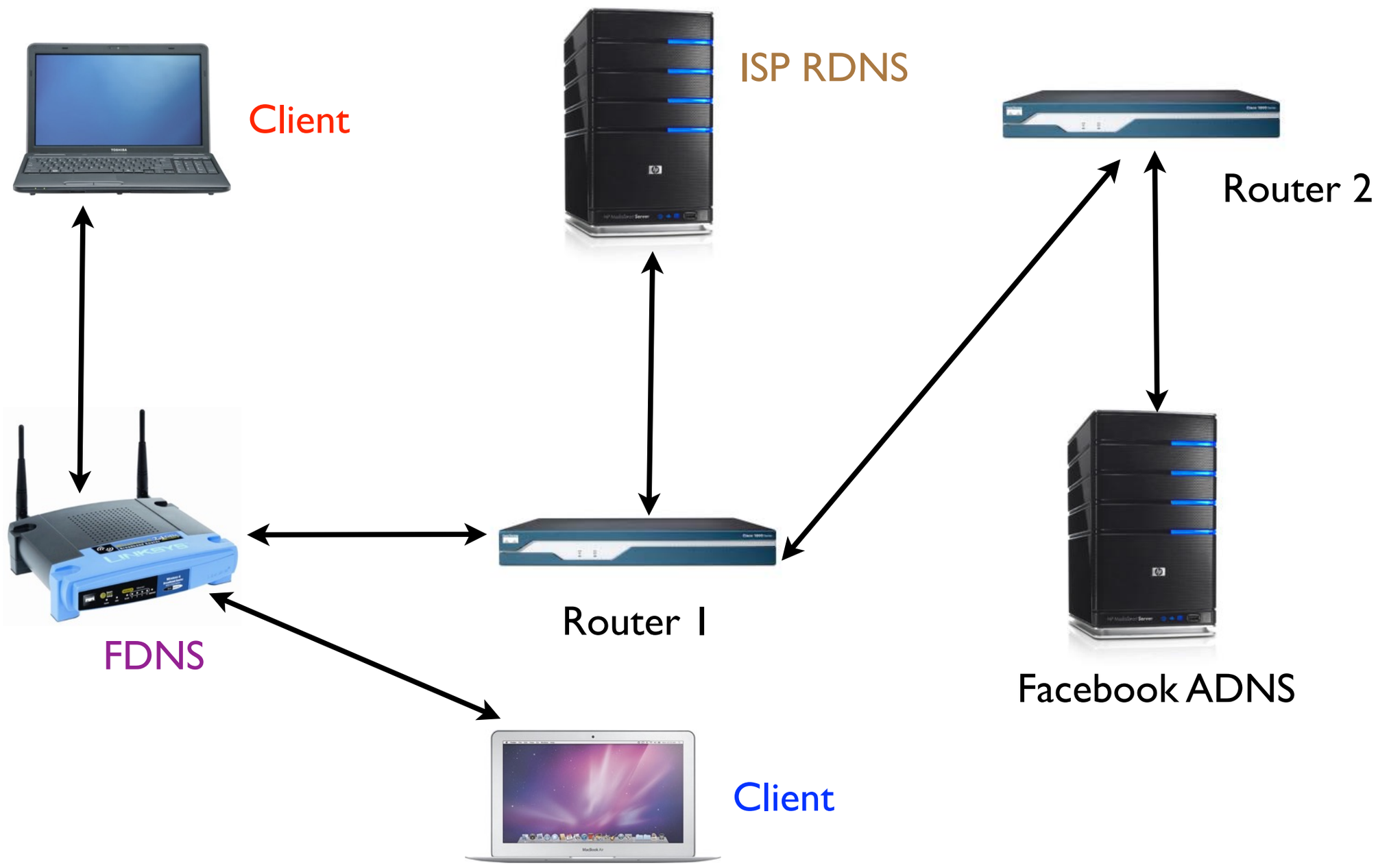
- DNS susceptible to ...
  - ... surveillance
  - ... spoofing
  - ... modification
  - ... injection
  - ... interposition

Security Implications

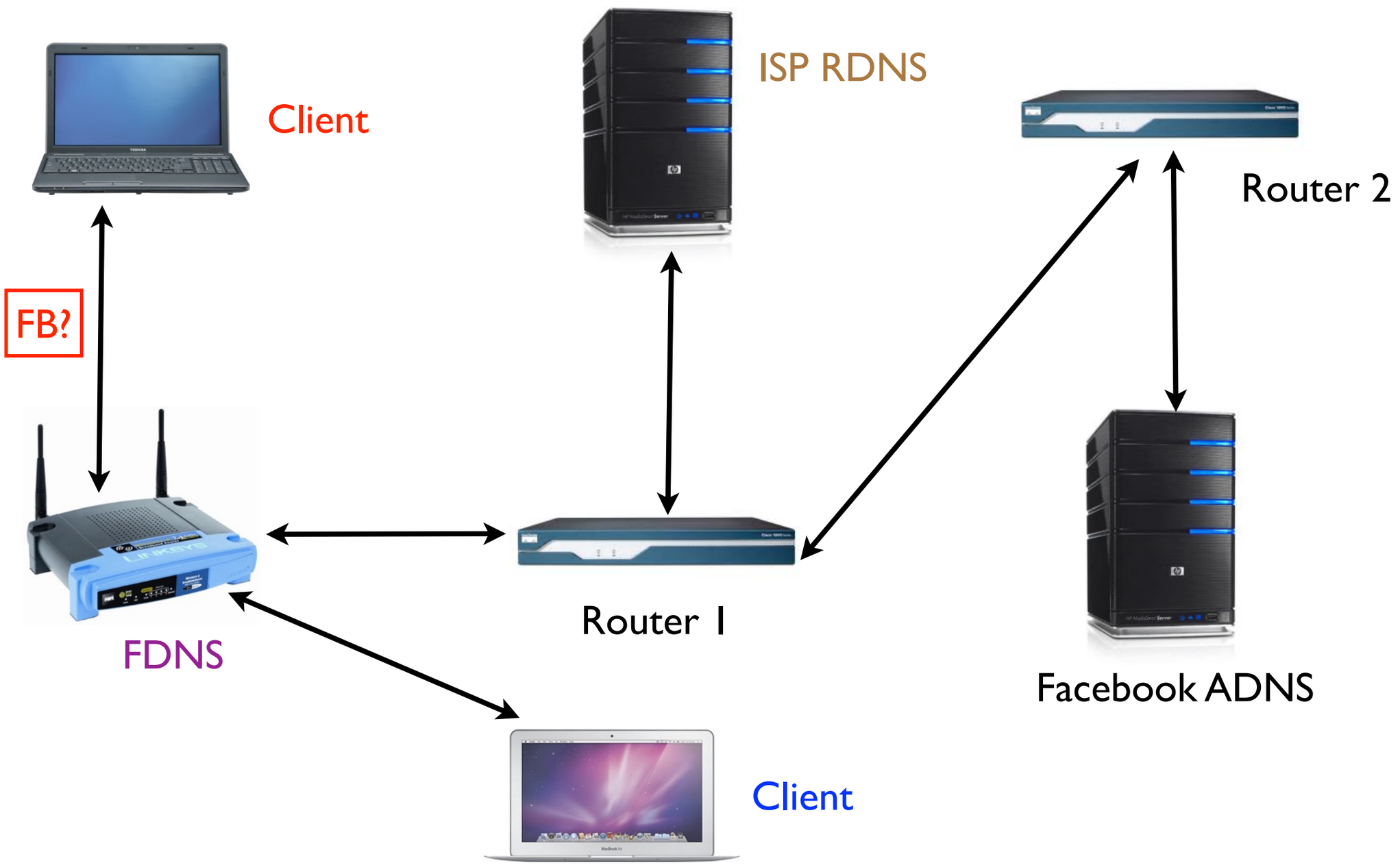
- DNS susceptible to ...
  - ... surveillance
  - ... spoofing
  - ... modification
  - ... injection
  - ... interposition

- Every component of the DNS ecosystem is a *potential adversary*

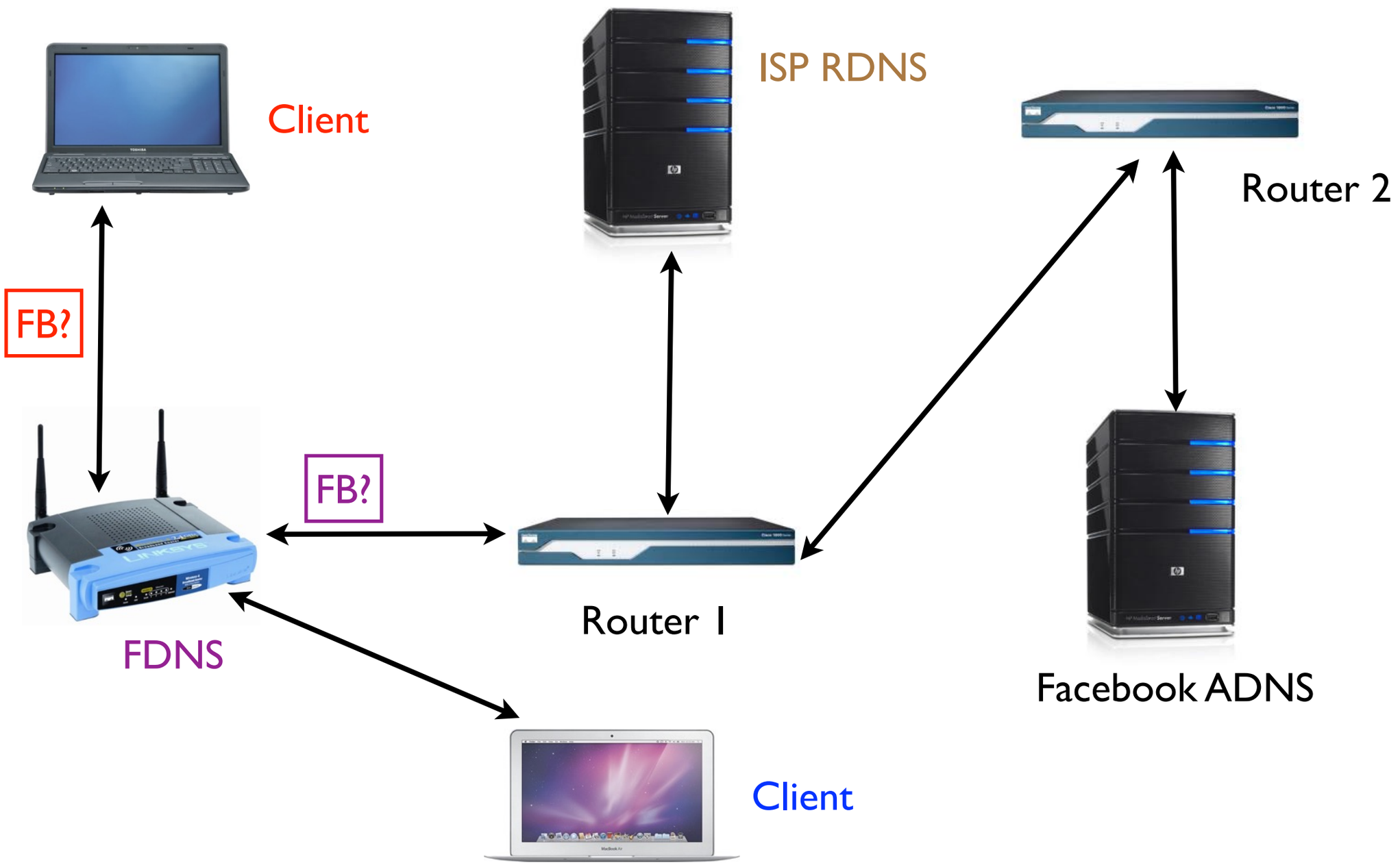
DNS Transaction Example



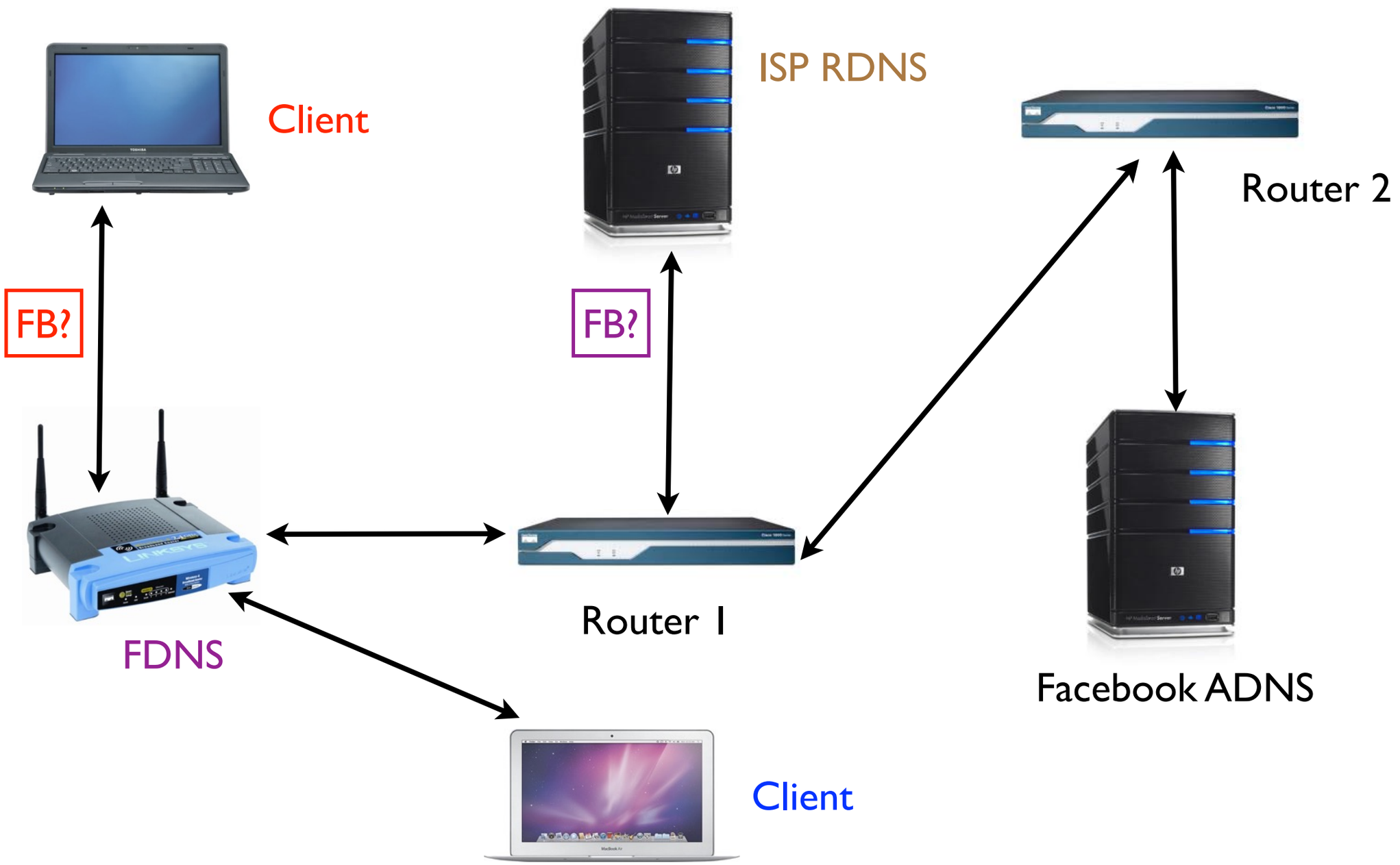
DNS Transaction Example



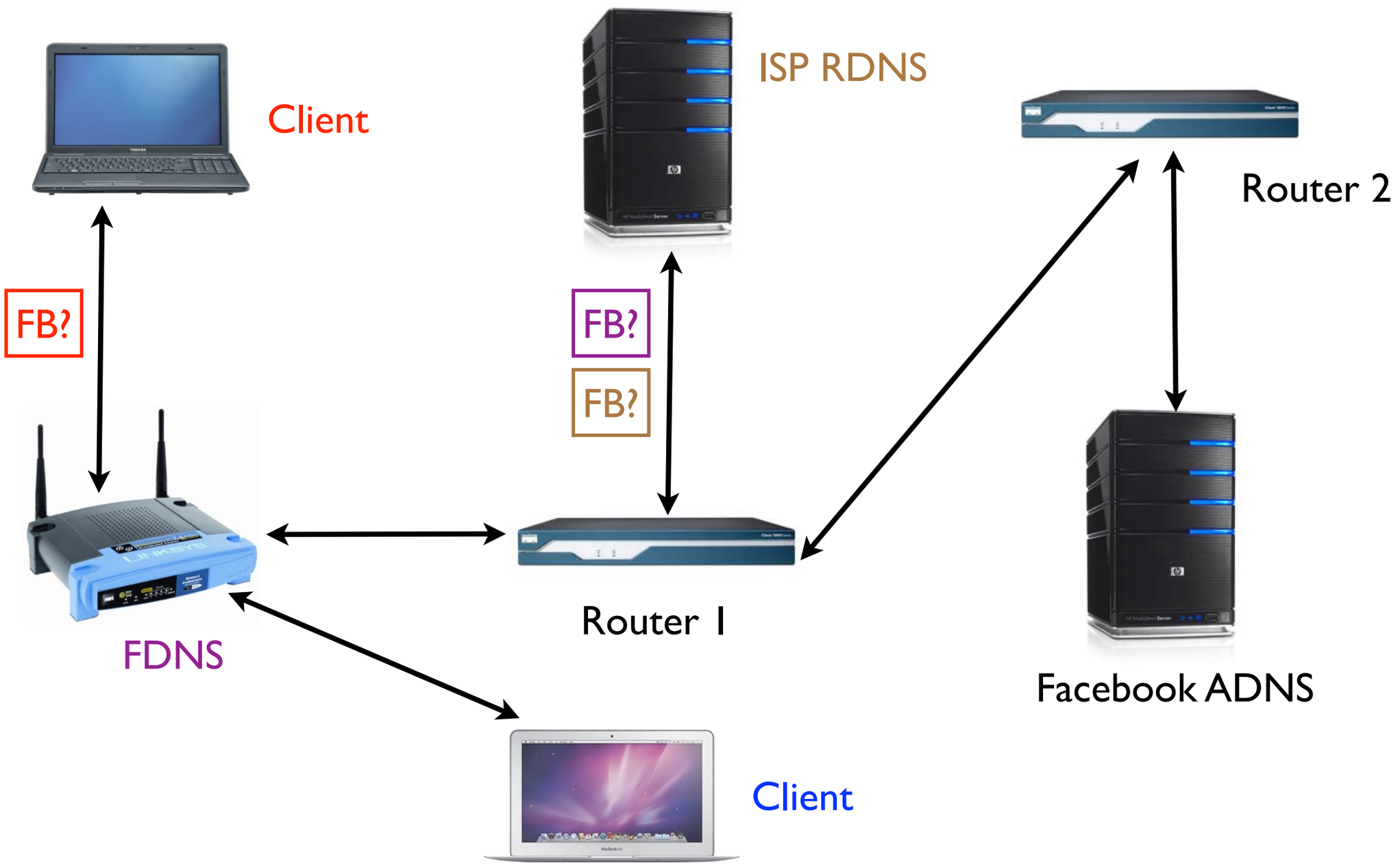
DNS Transaction Example



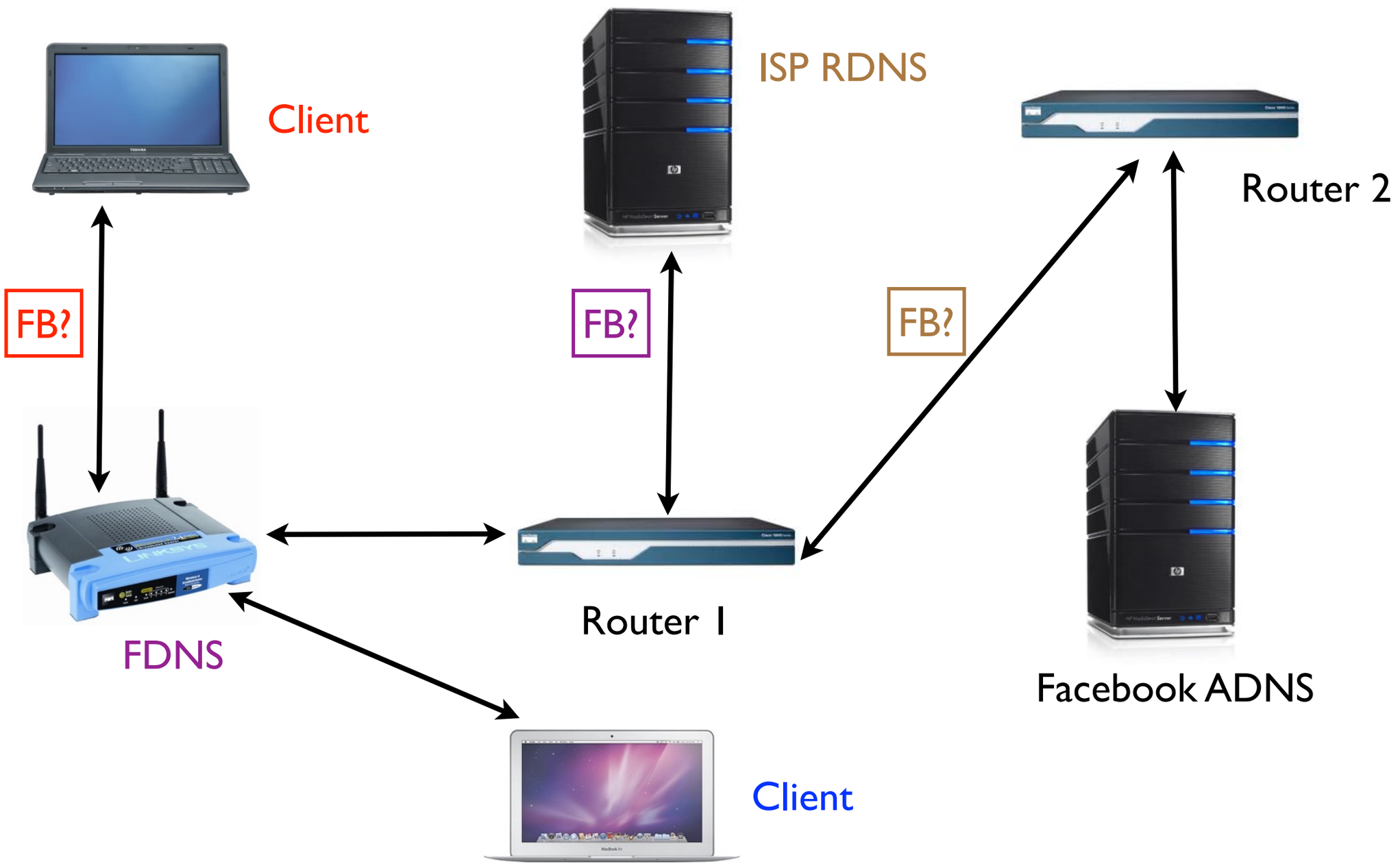
DNS Transaction Example



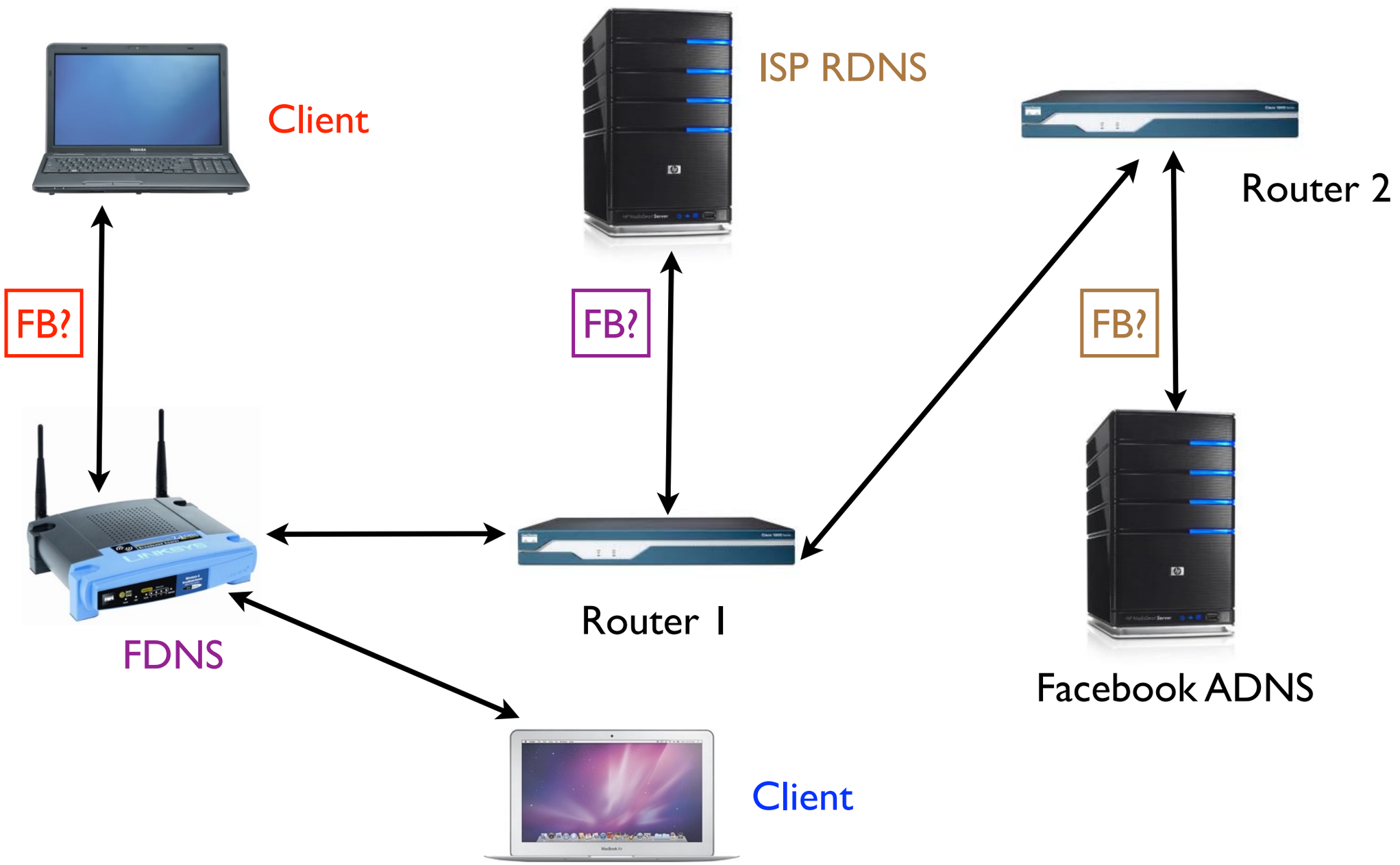
DNS Transaction Example



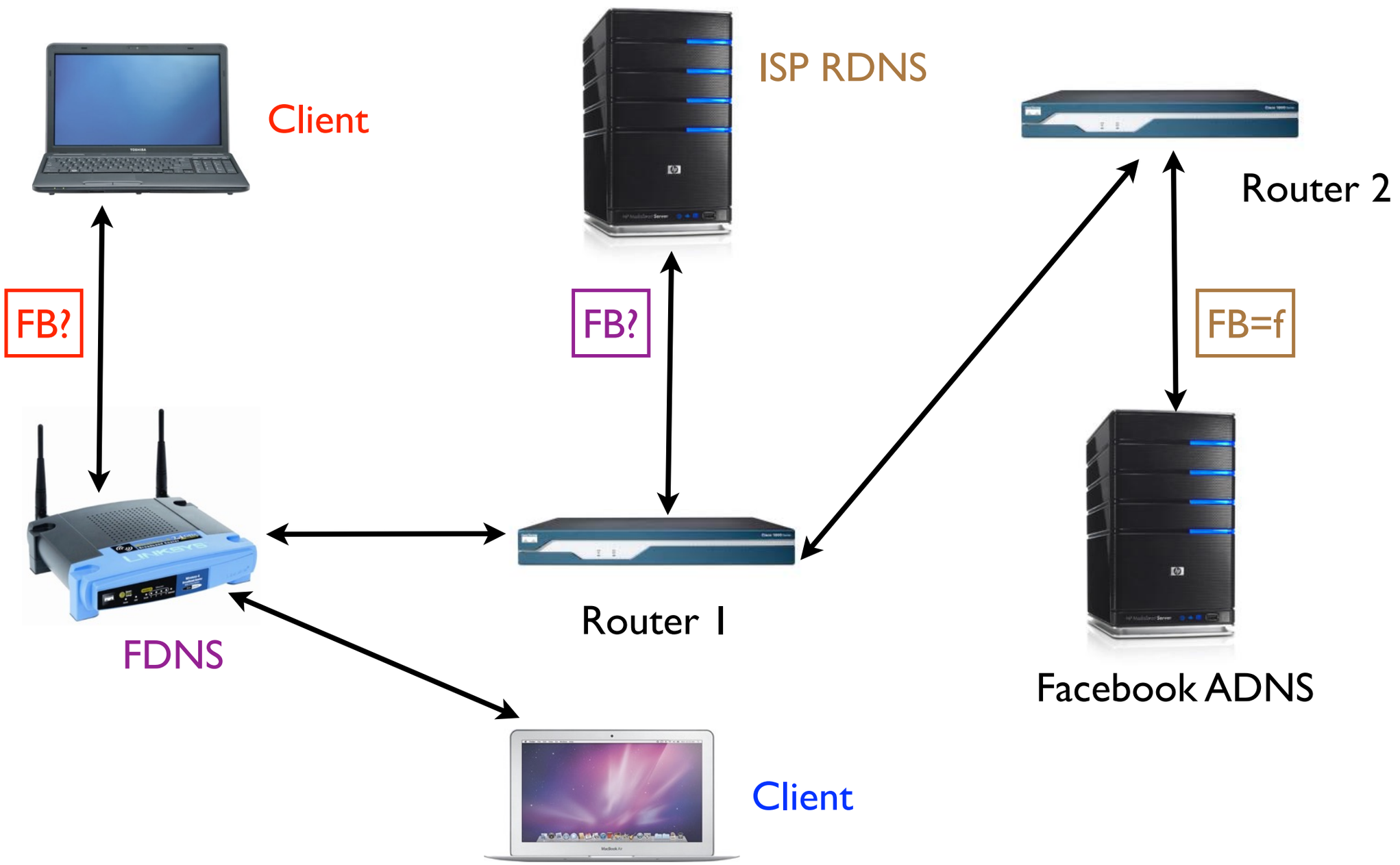
DNS Transaction Example



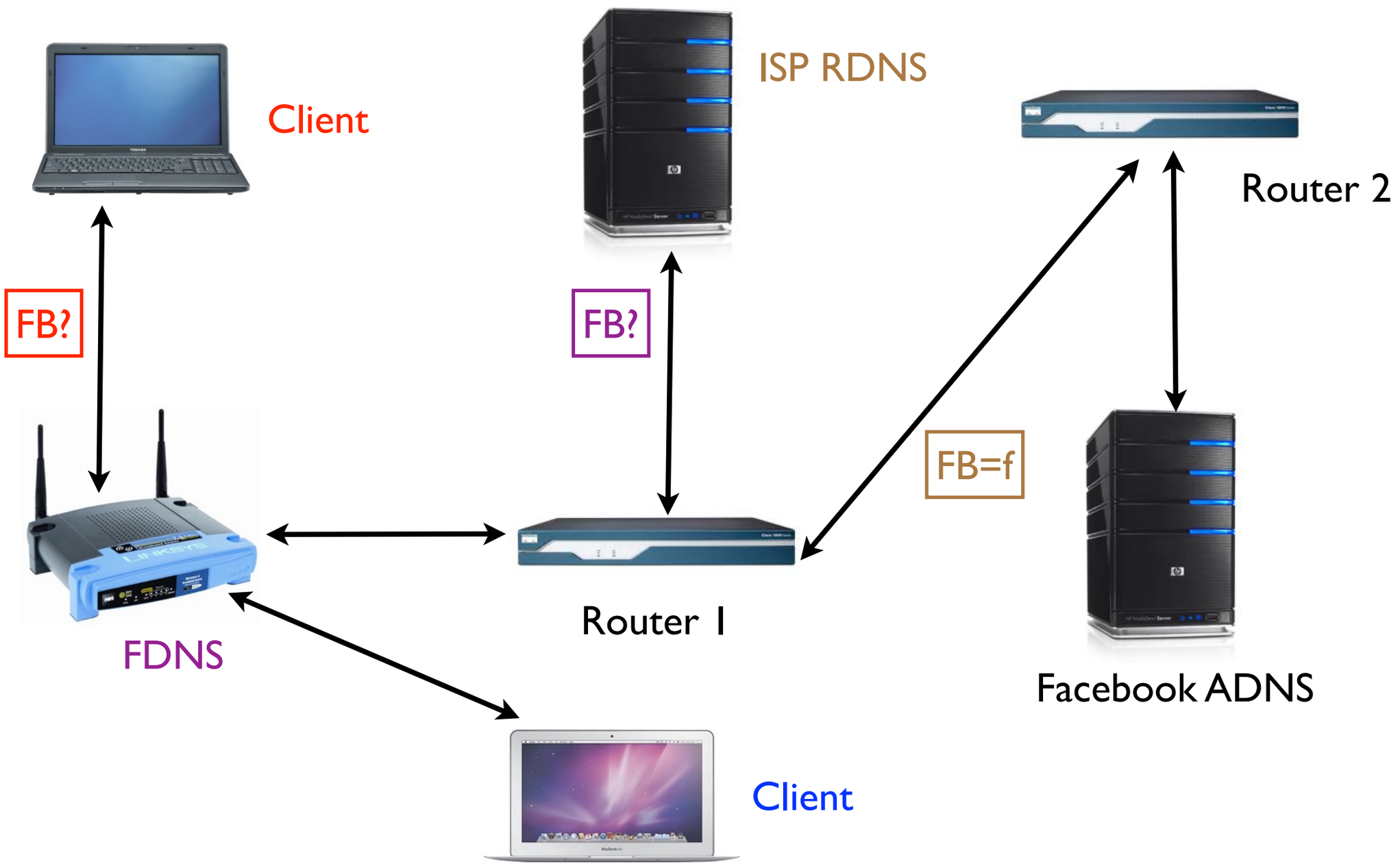
DNS Transaction Example



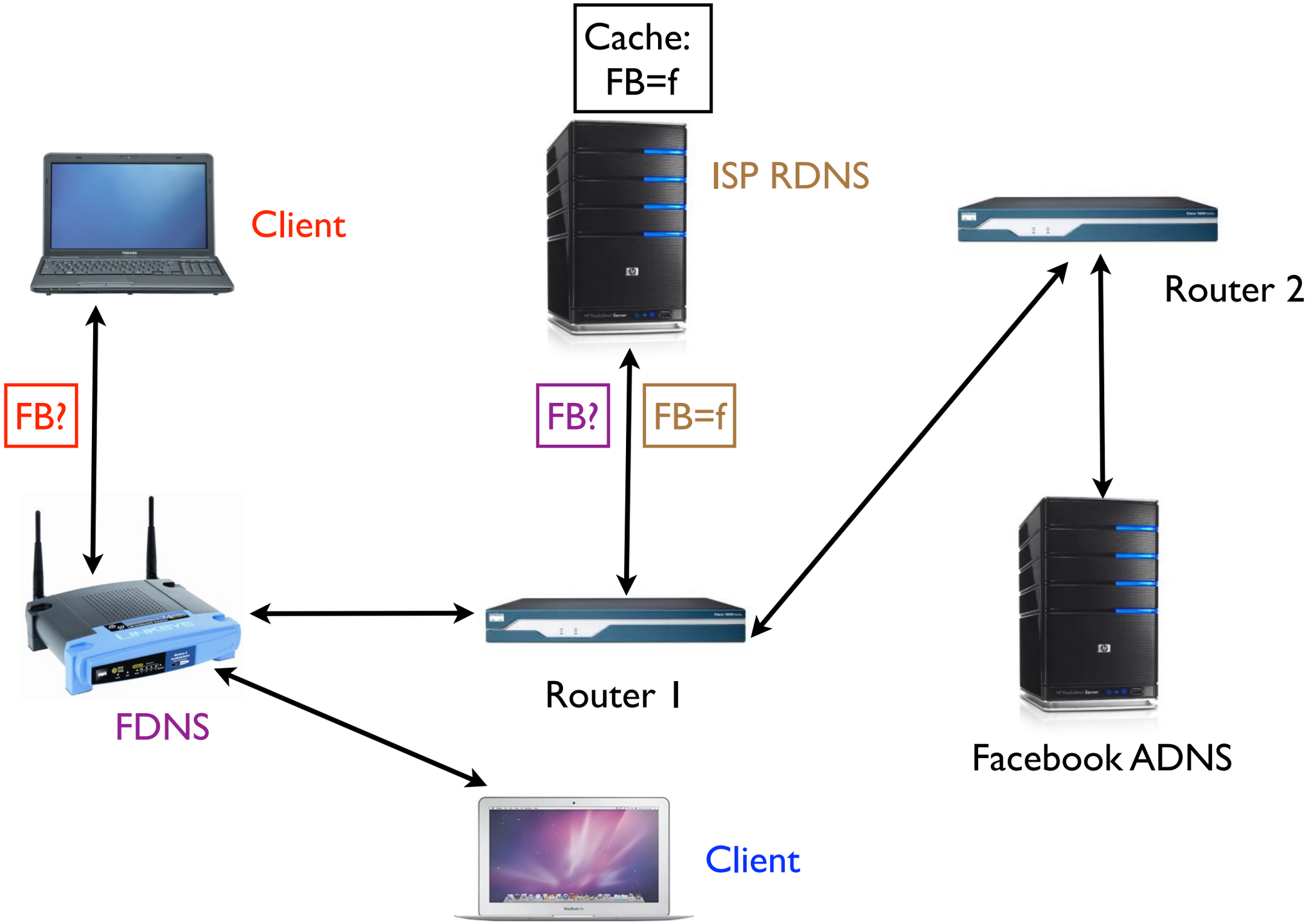
DNS Transaction Example



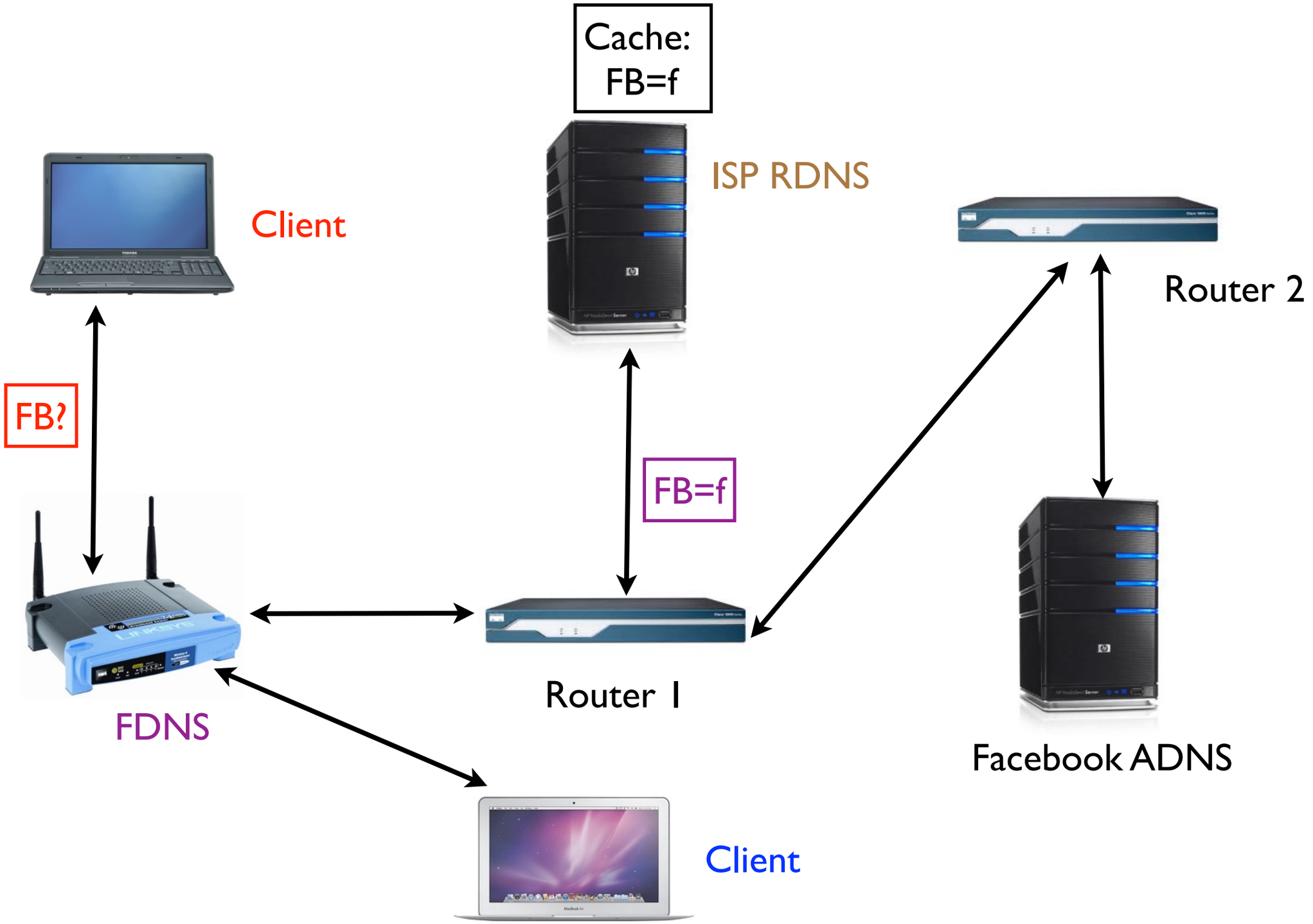
DNS Transaction Example



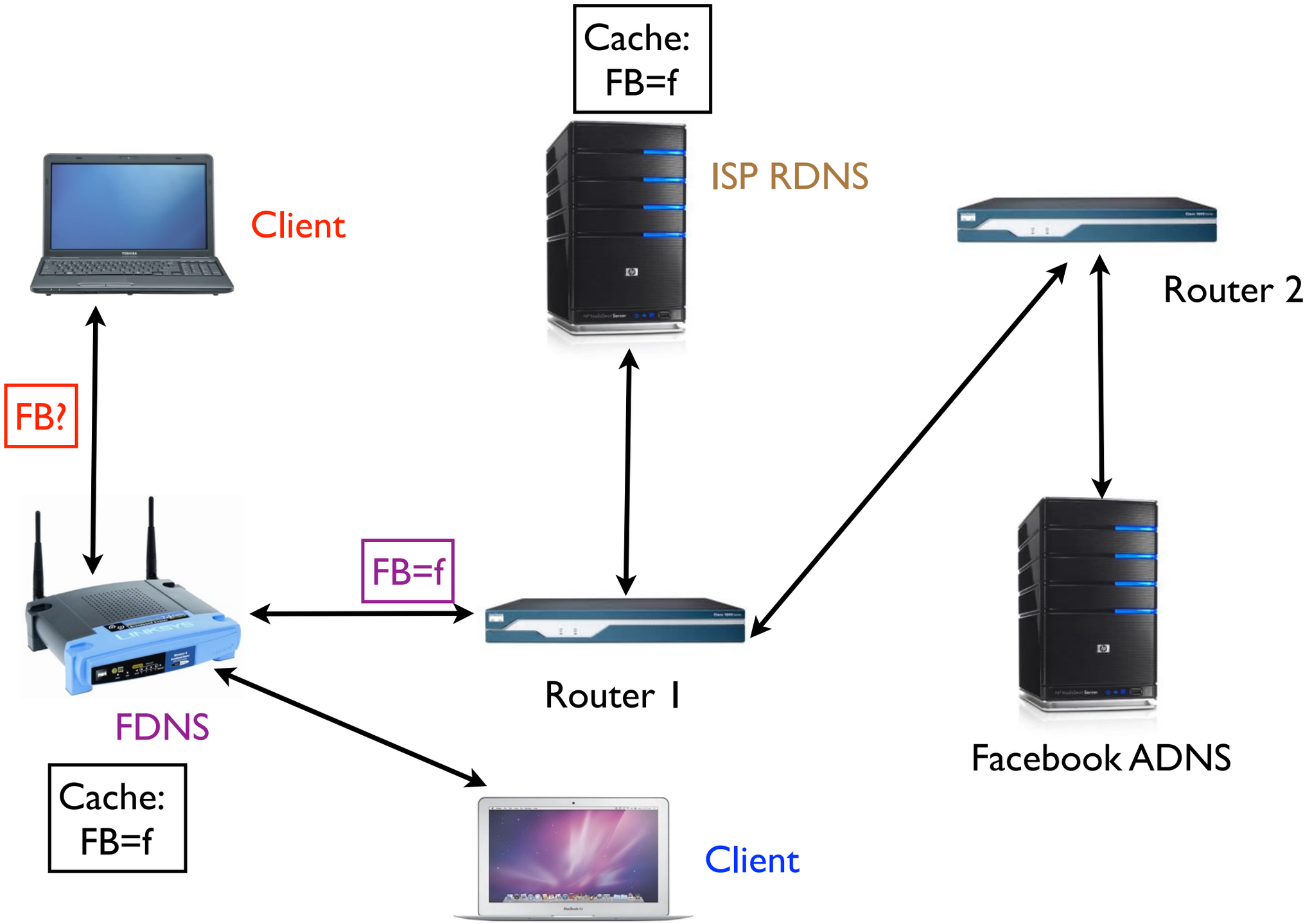
DNS Transaction Example



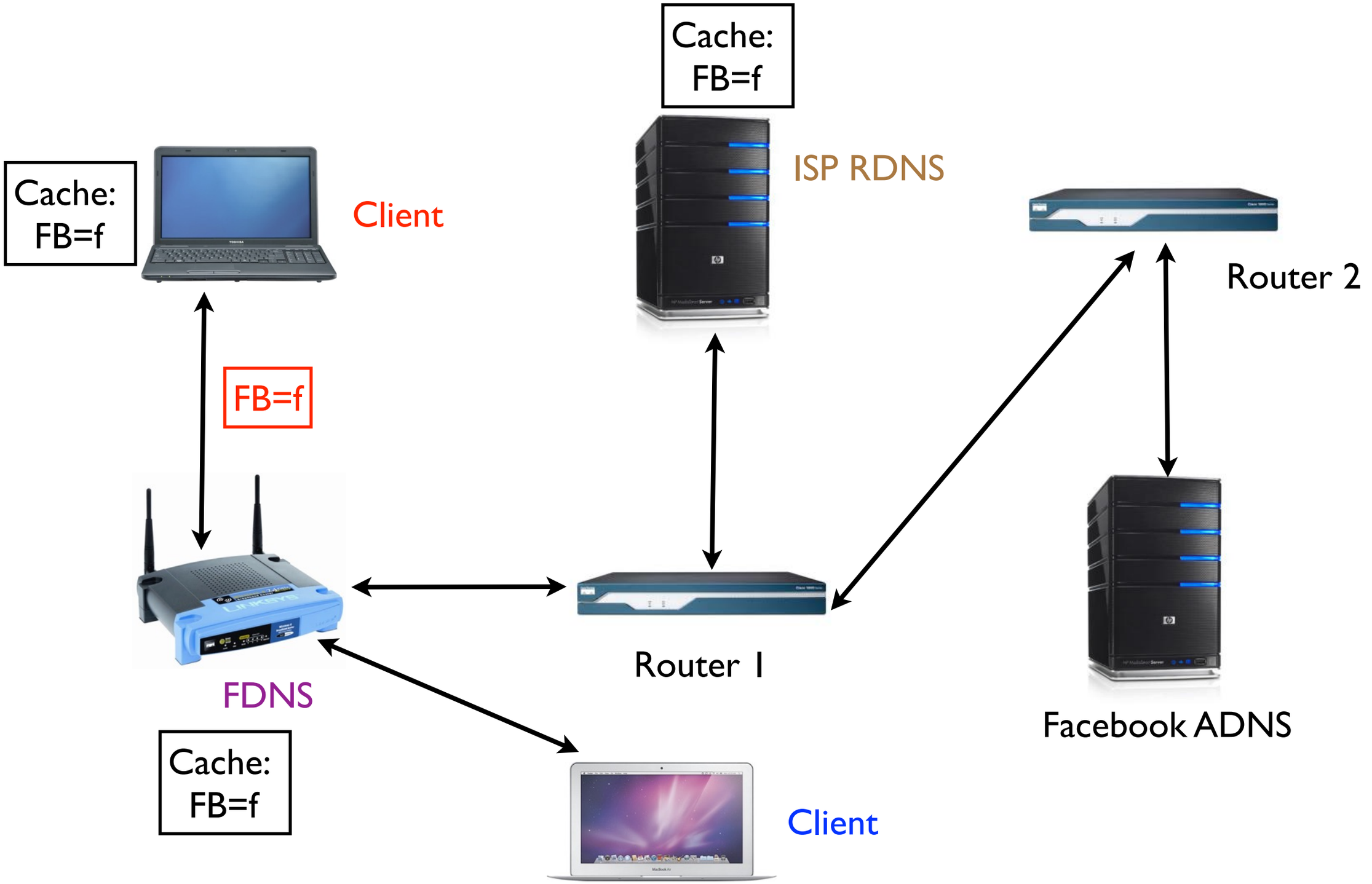
DNS Transaction Example



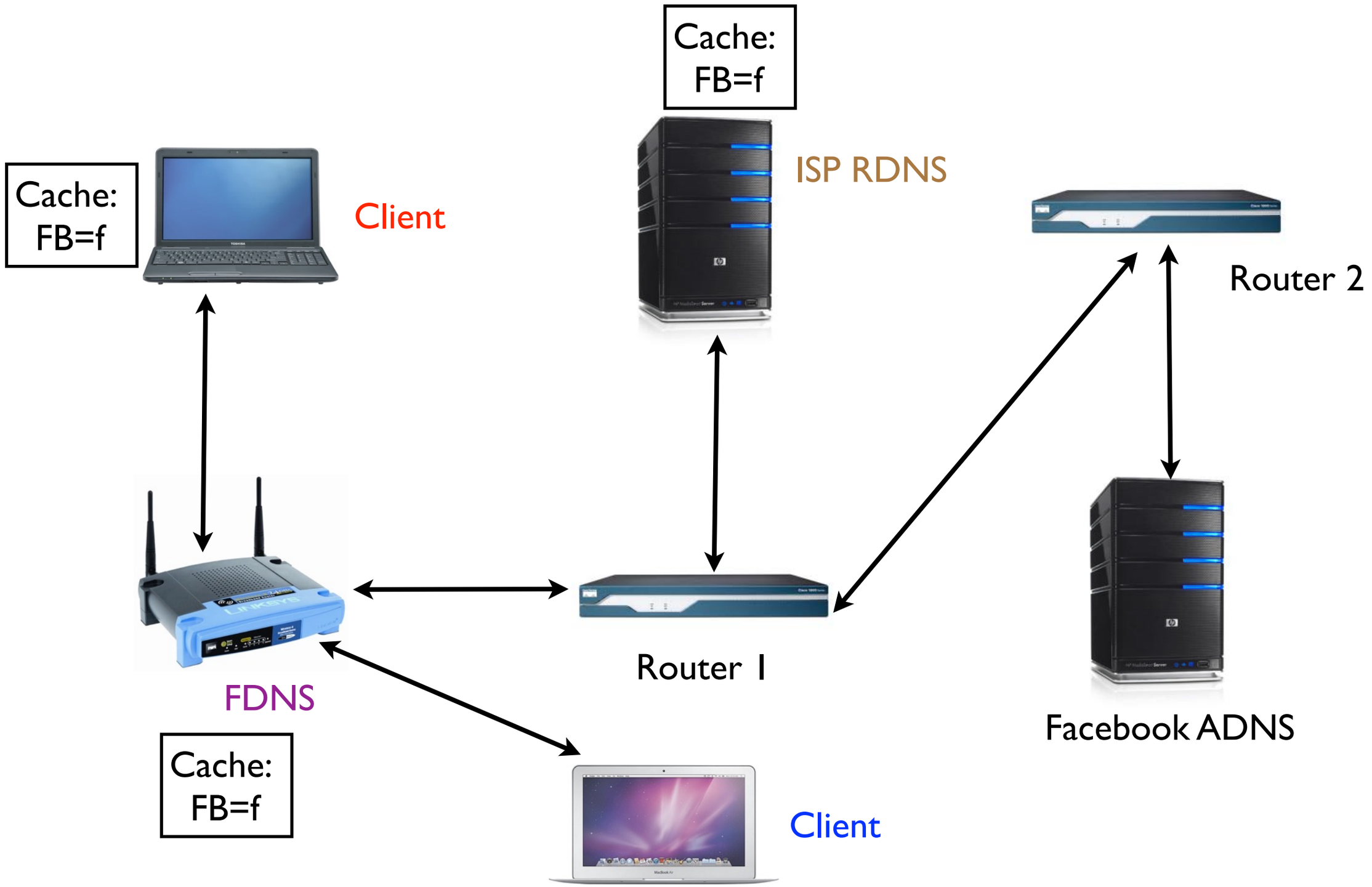
DNS Transaction Example



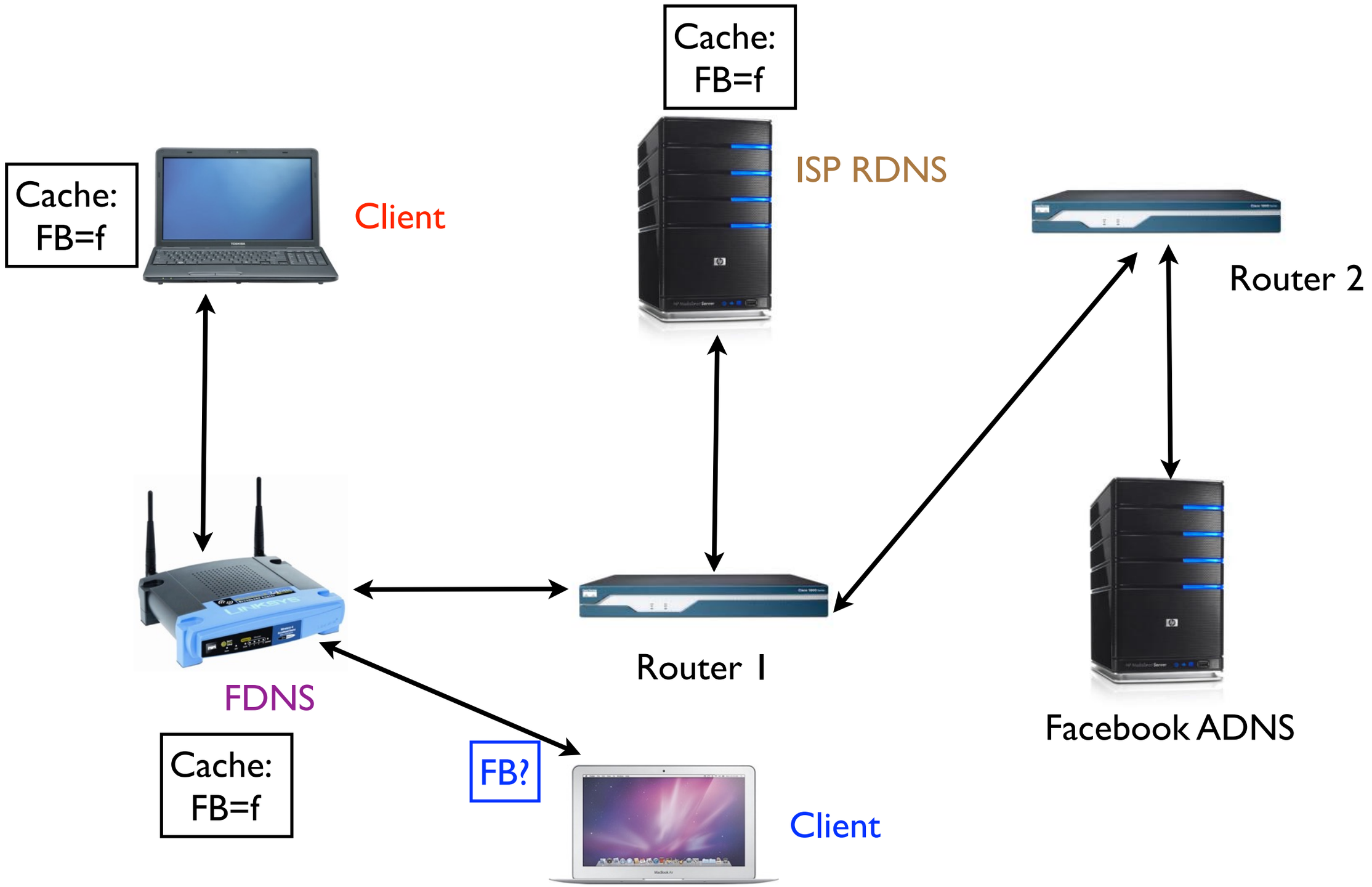
DNS Transaction Example



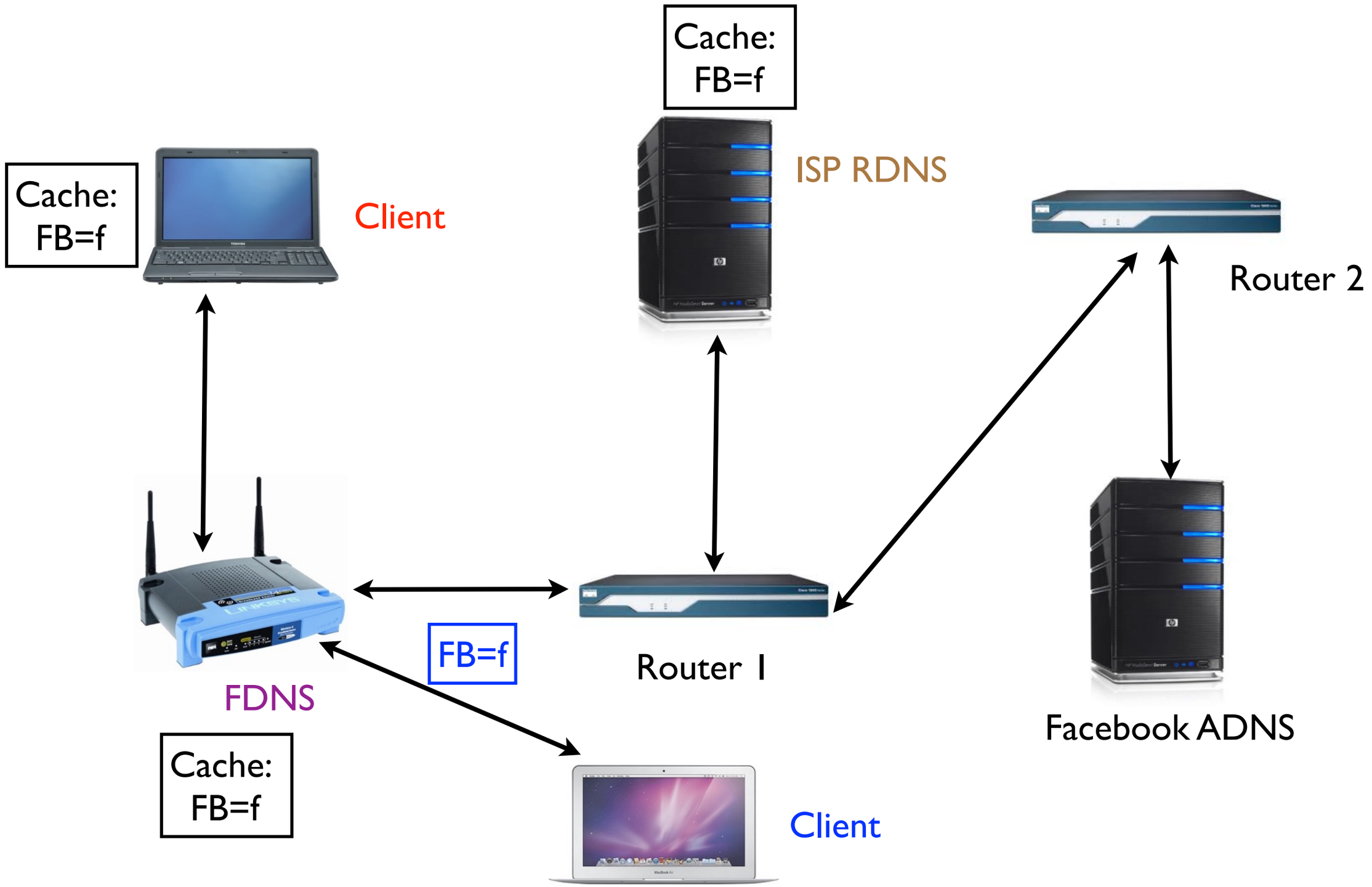
DNS Transaction Example



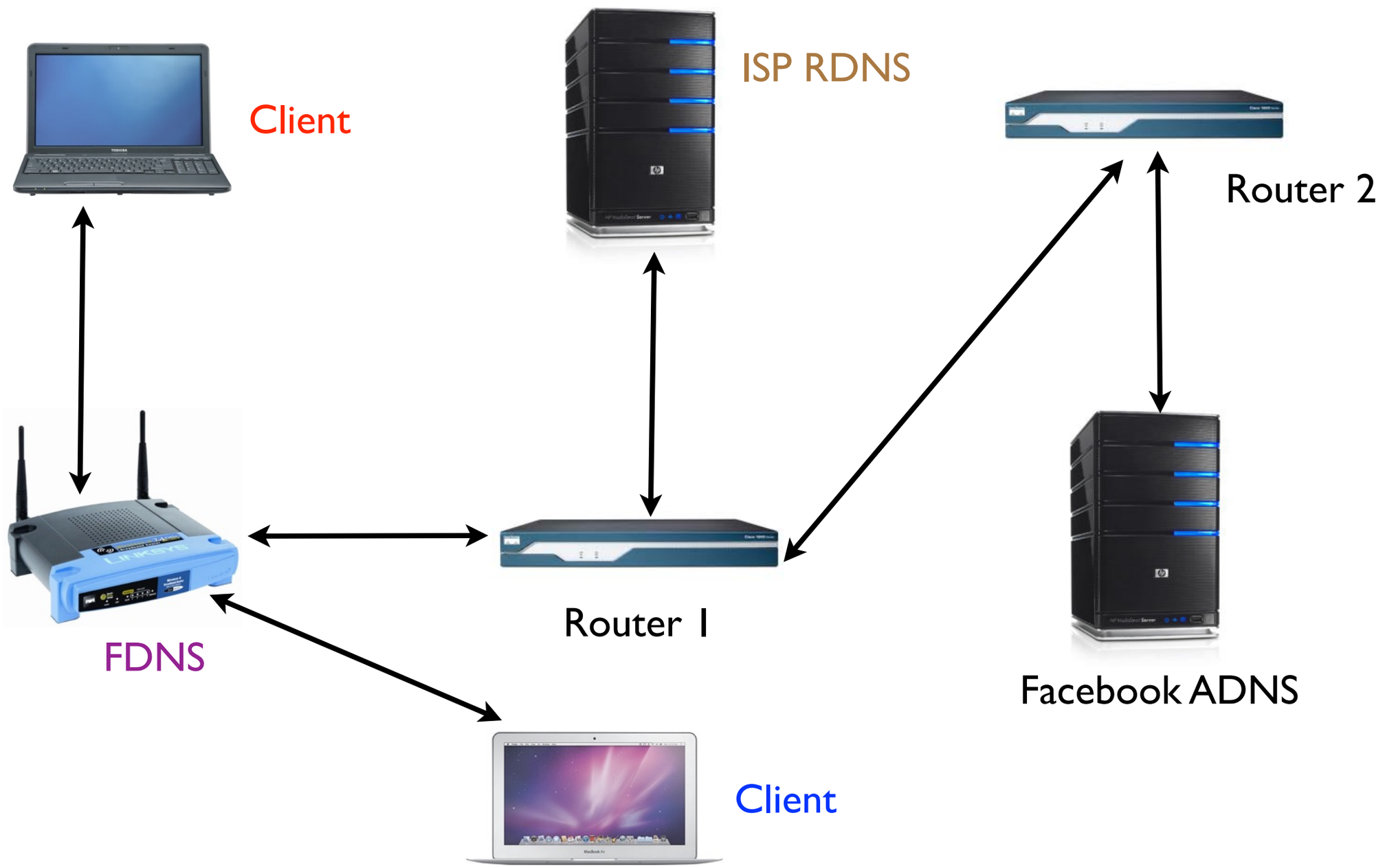
DNS Transaction Example



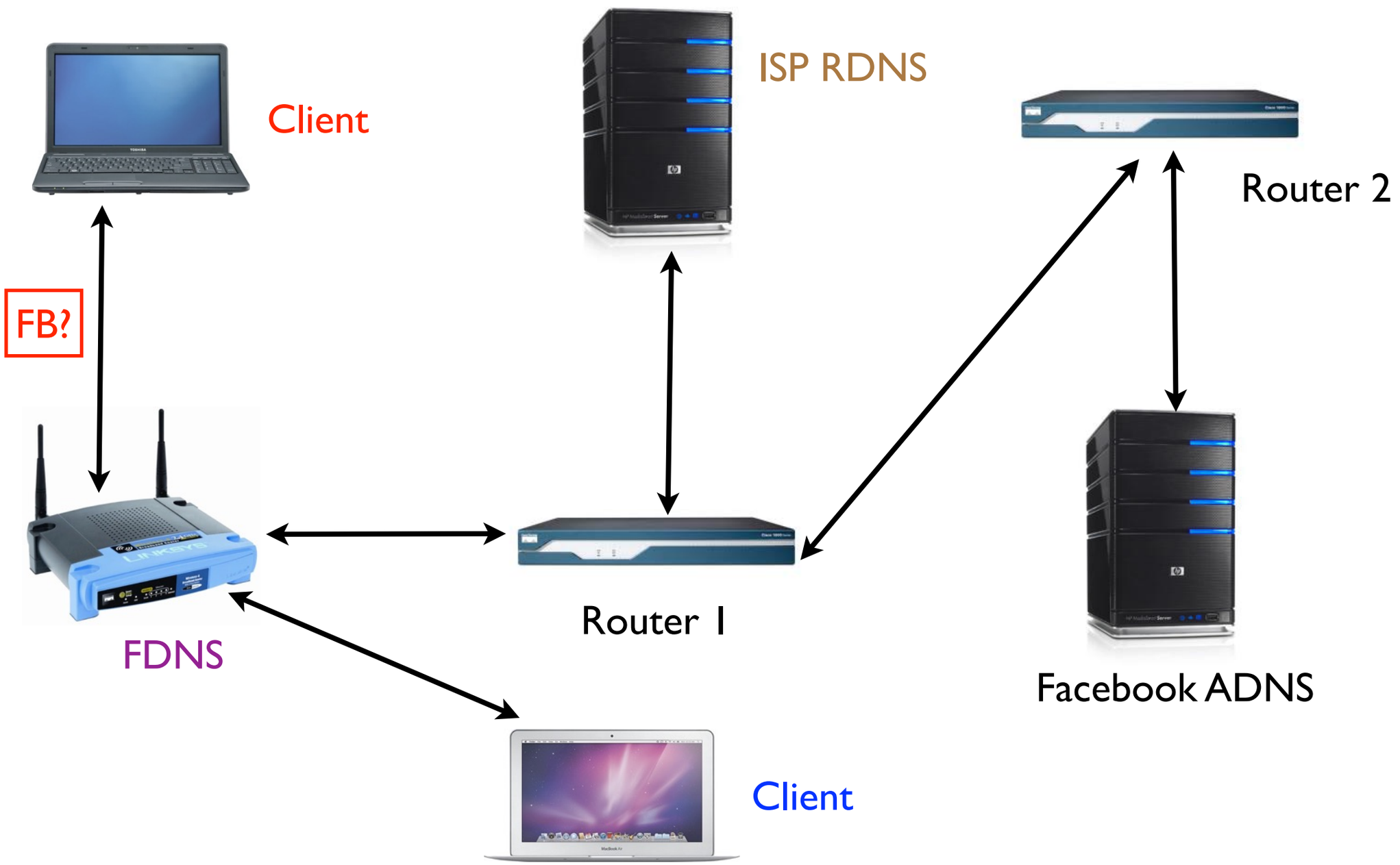
DNS Transaction Example



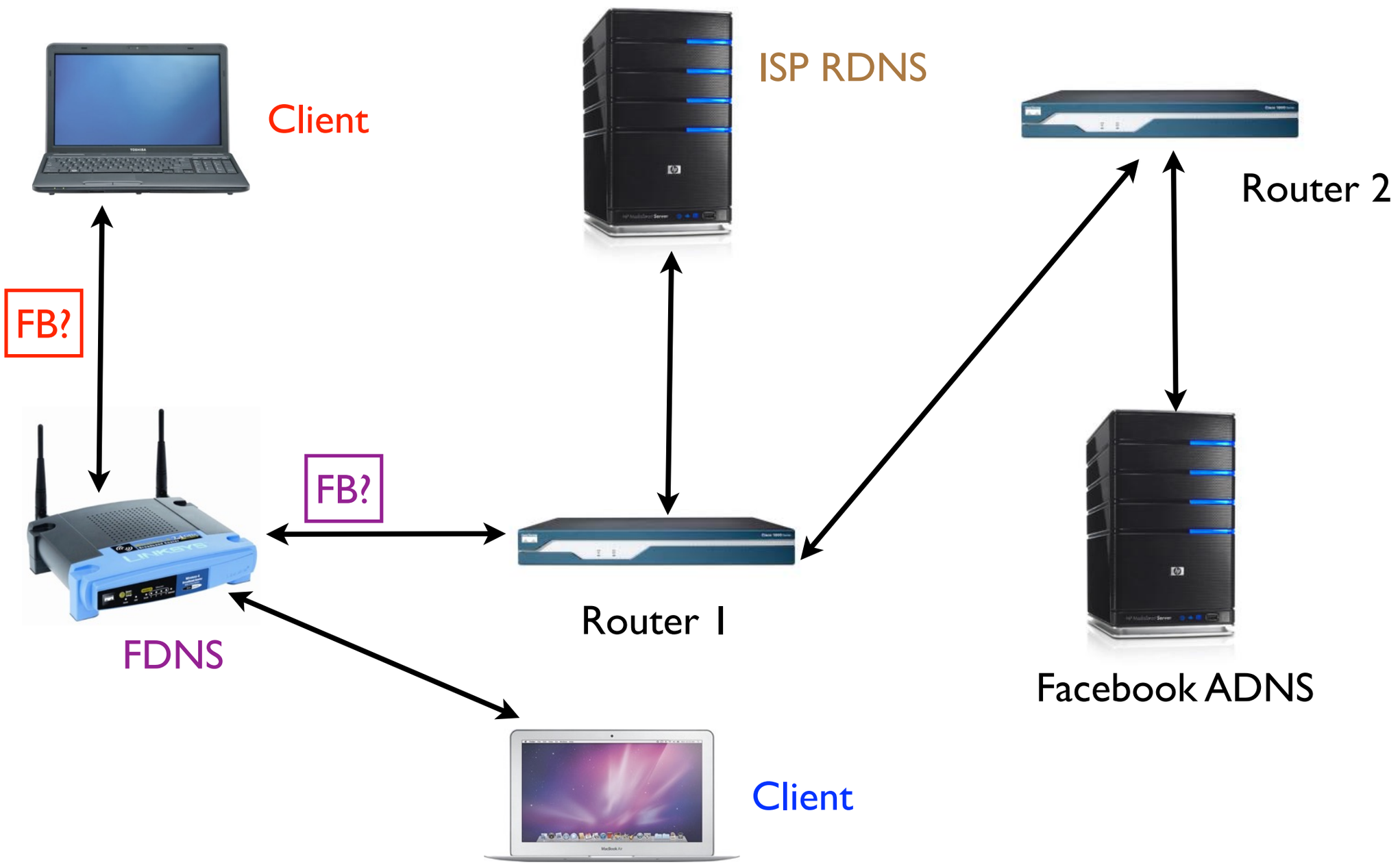
What Can Go Wrong? (1)



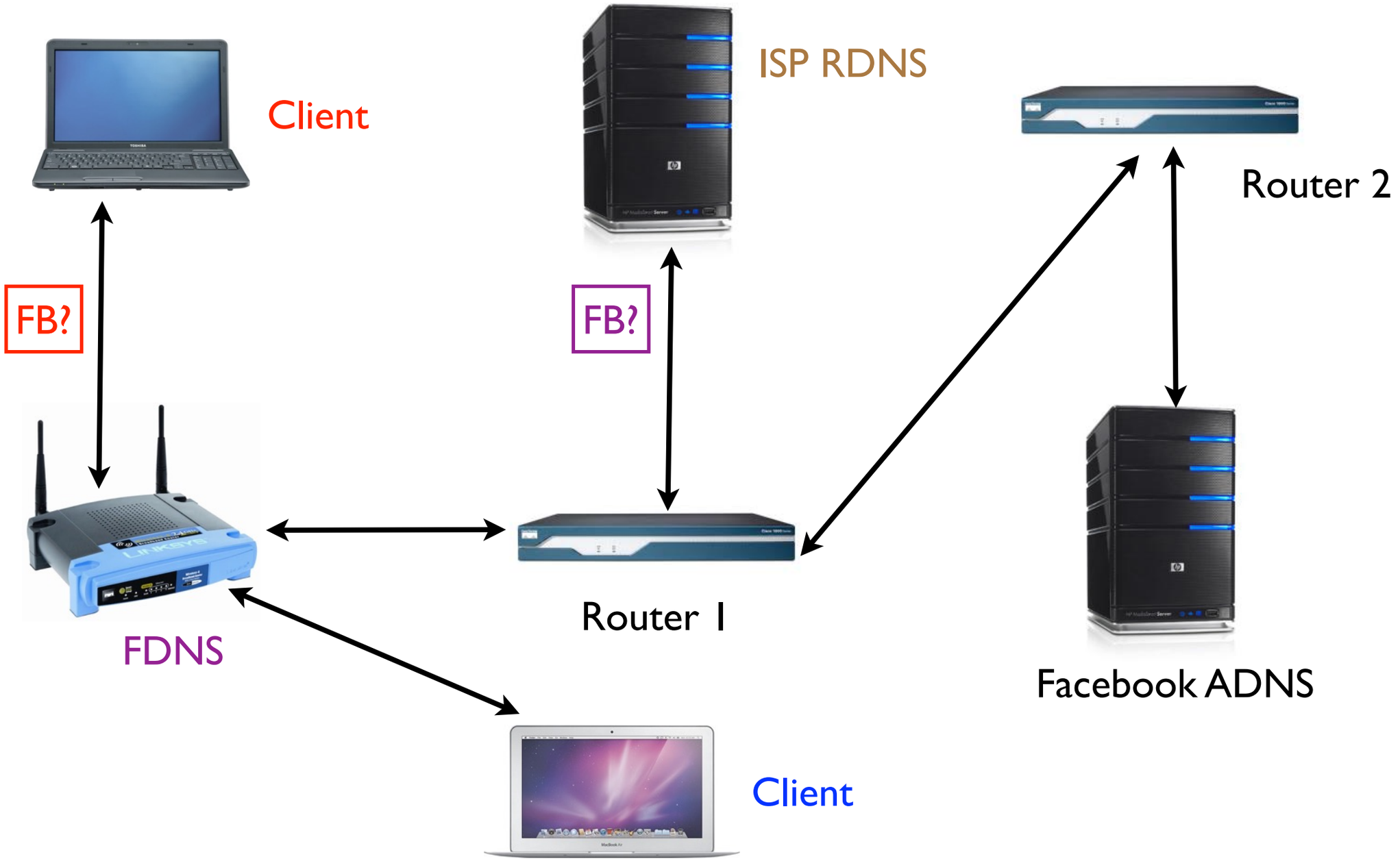
What Can Go Wrong? (1)



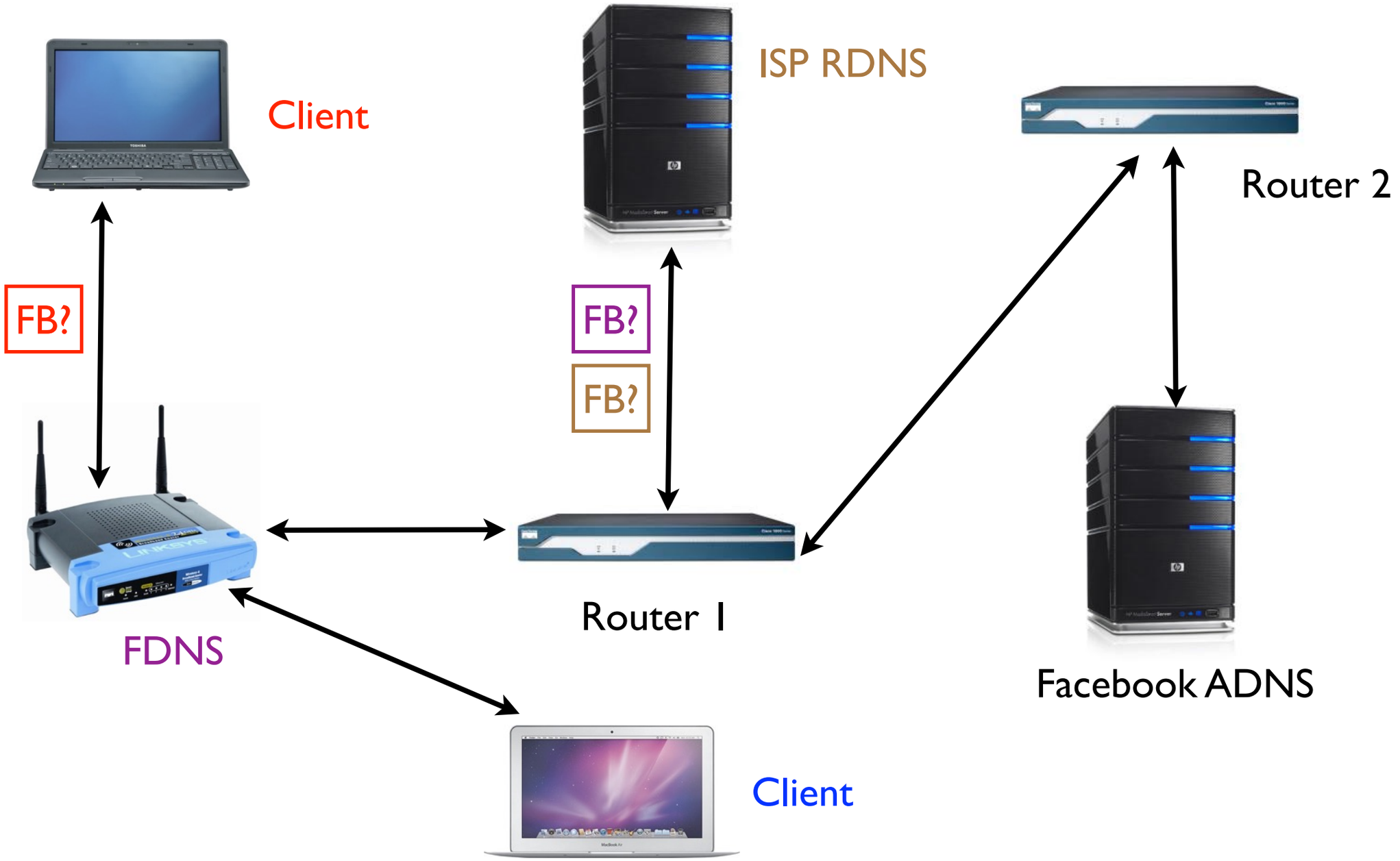
What Can Go Wrong? (1)



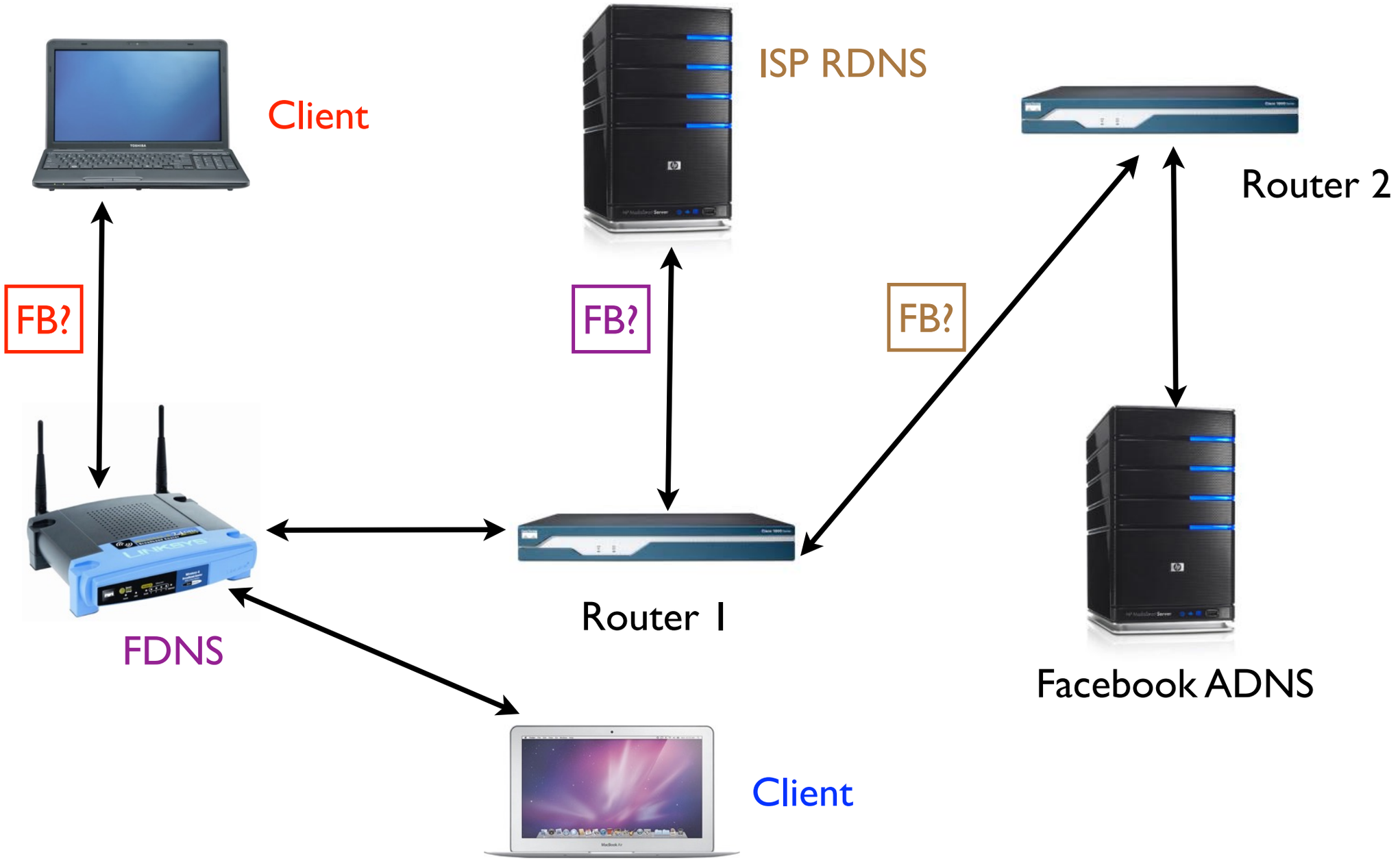
What Can Go Wrong? (1)



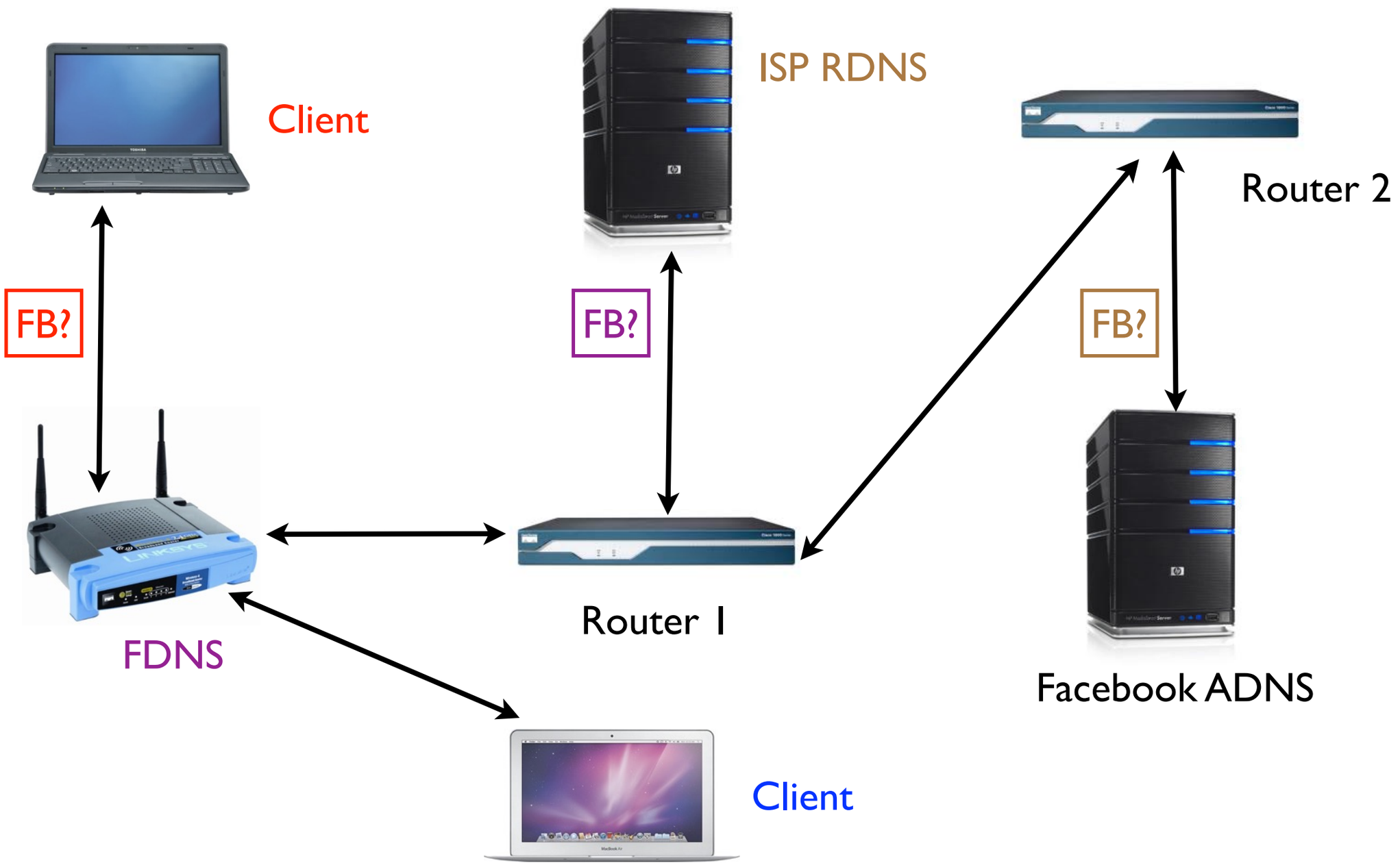
What Can Go Wrong? (1)



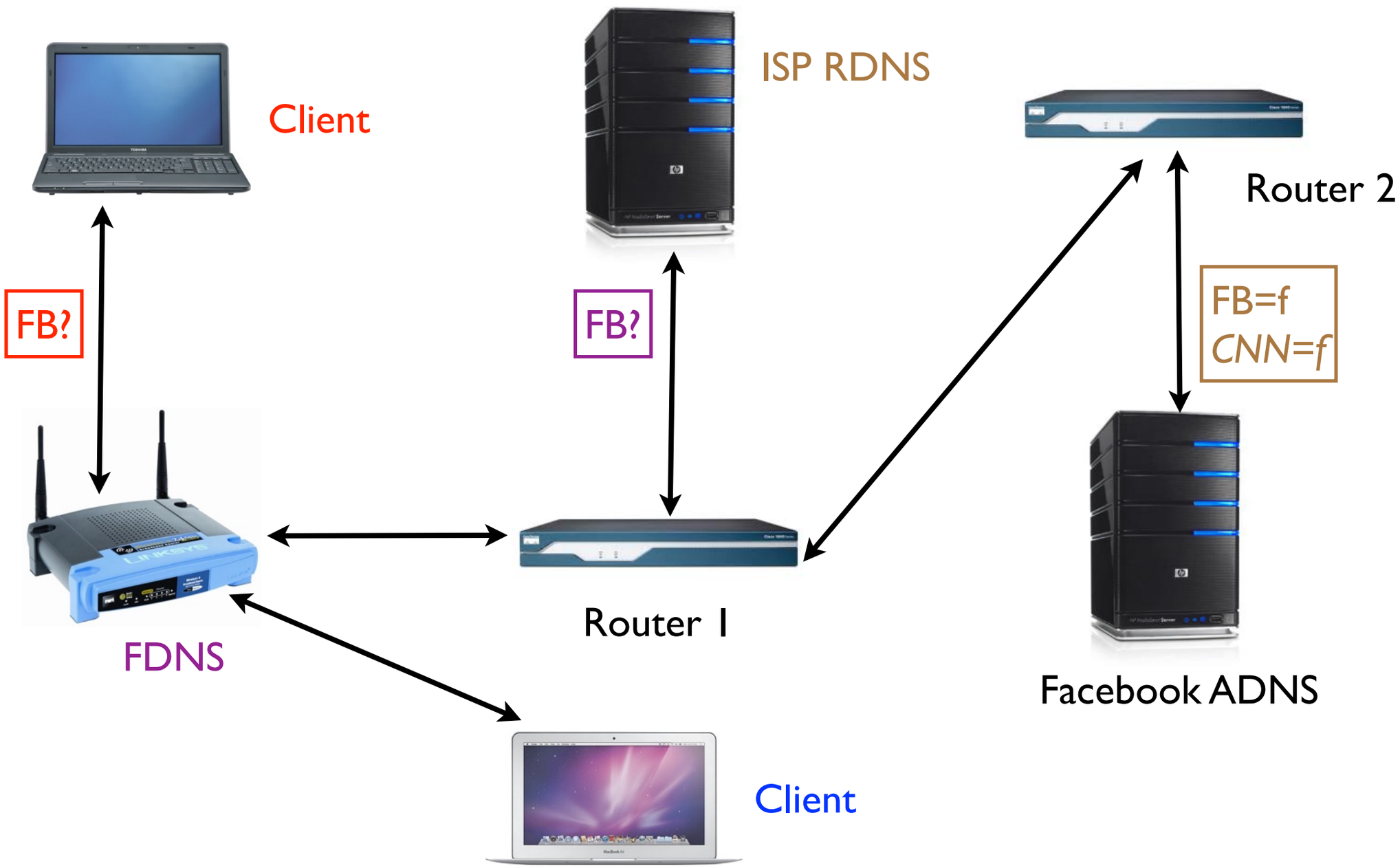
What Can Go Wrong? (1)



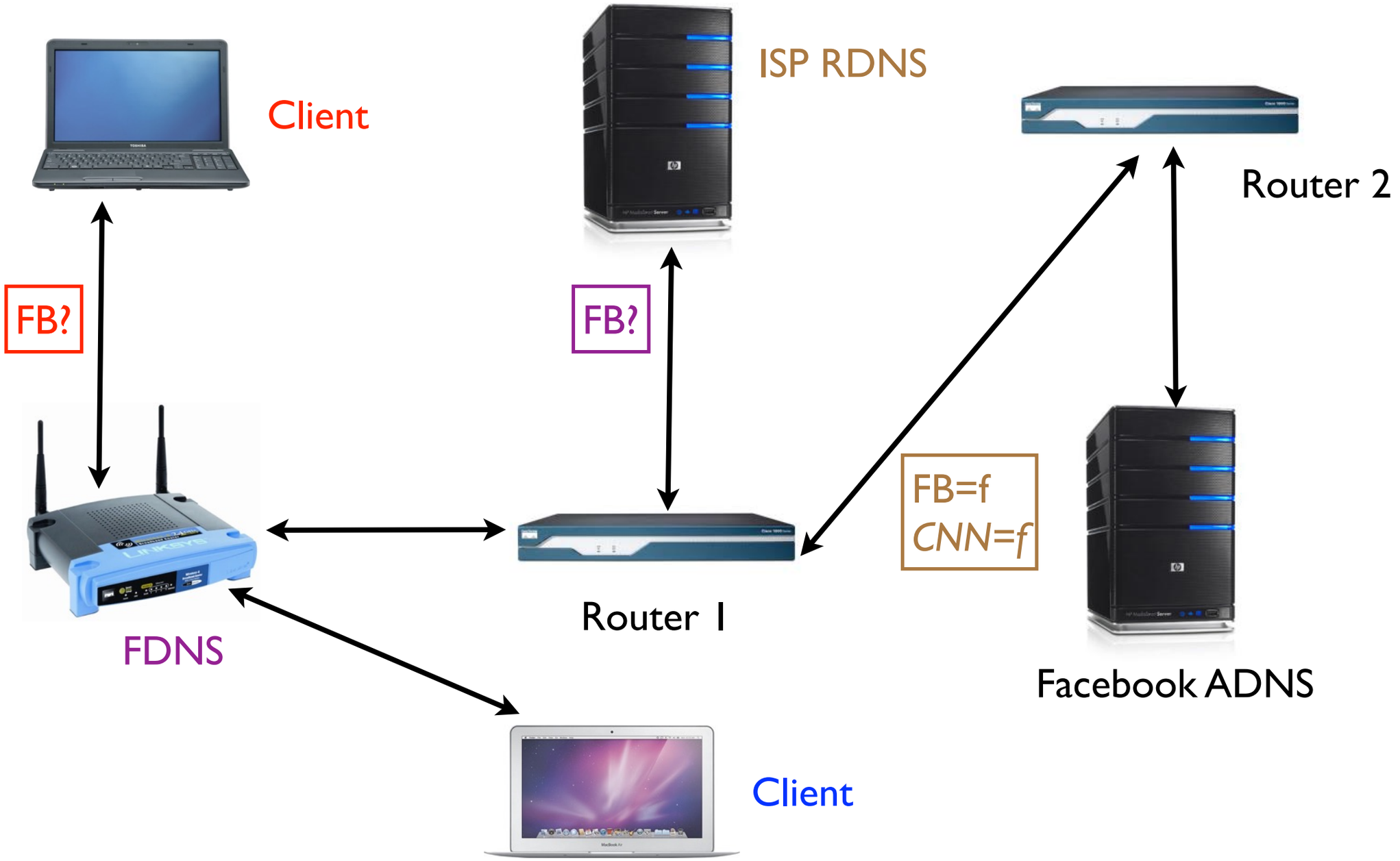
What Can Go Wrong? (1)



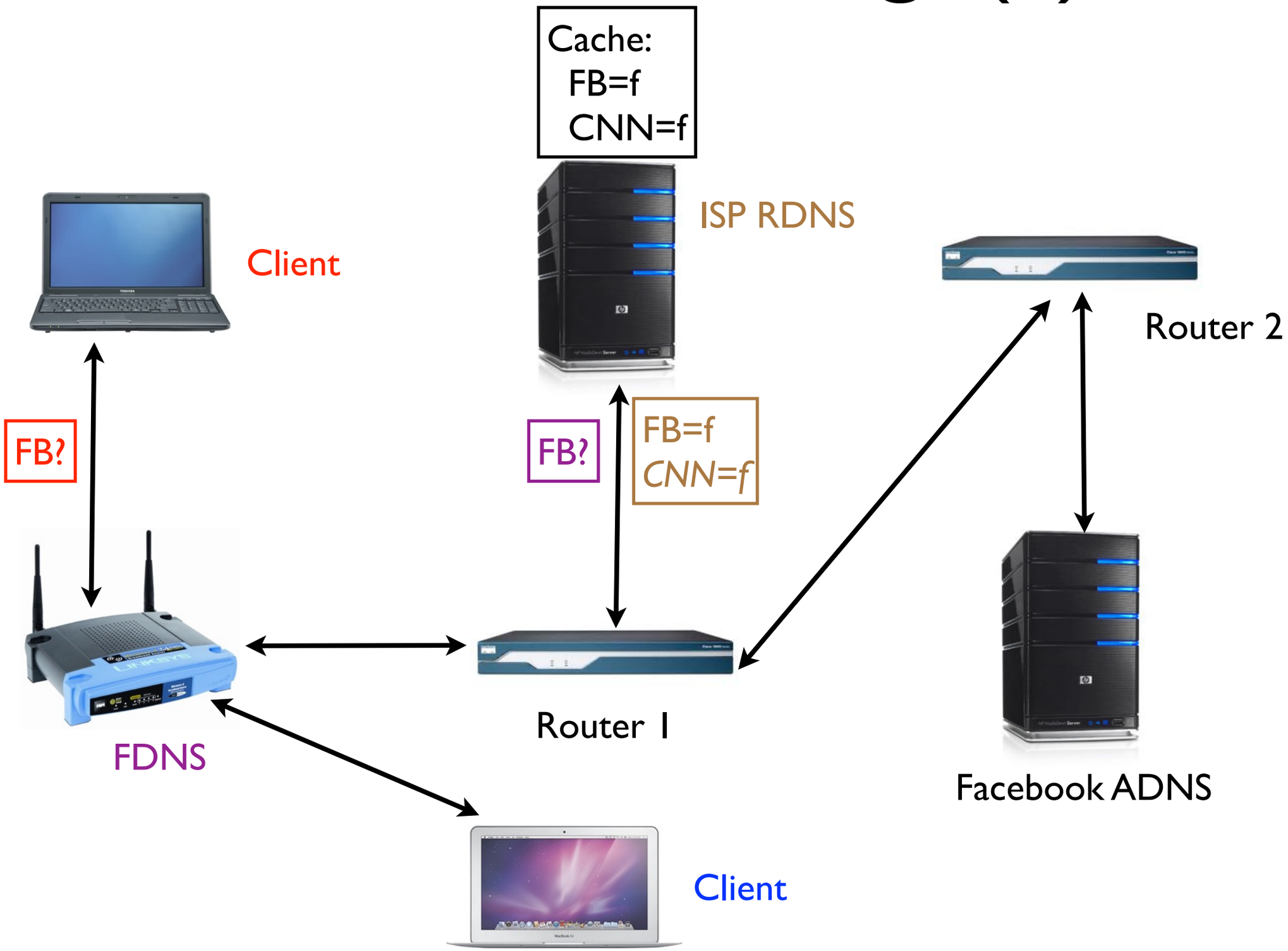
What Can Go Wrong? (1)



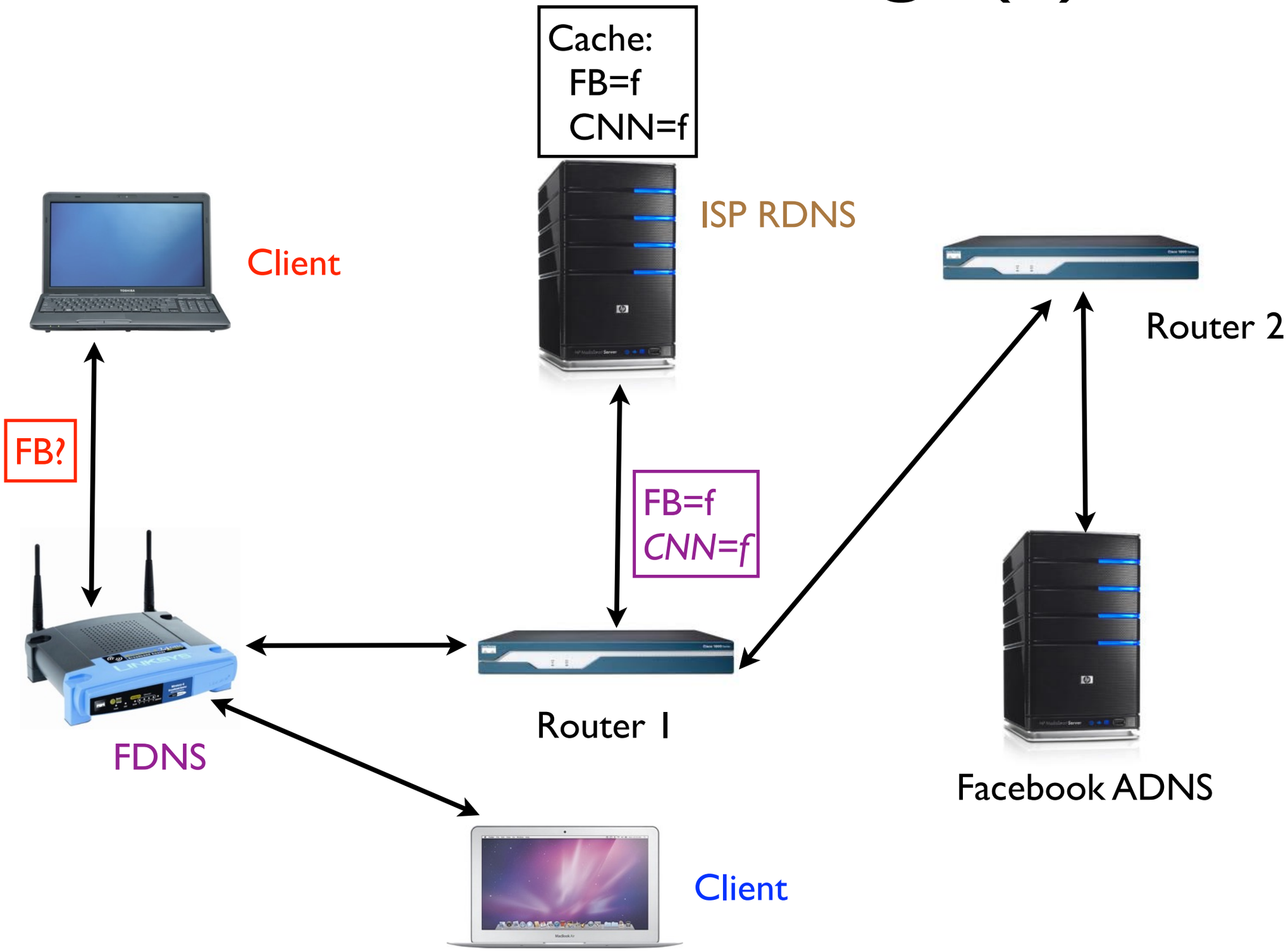
What Can Go Wrong? (1)



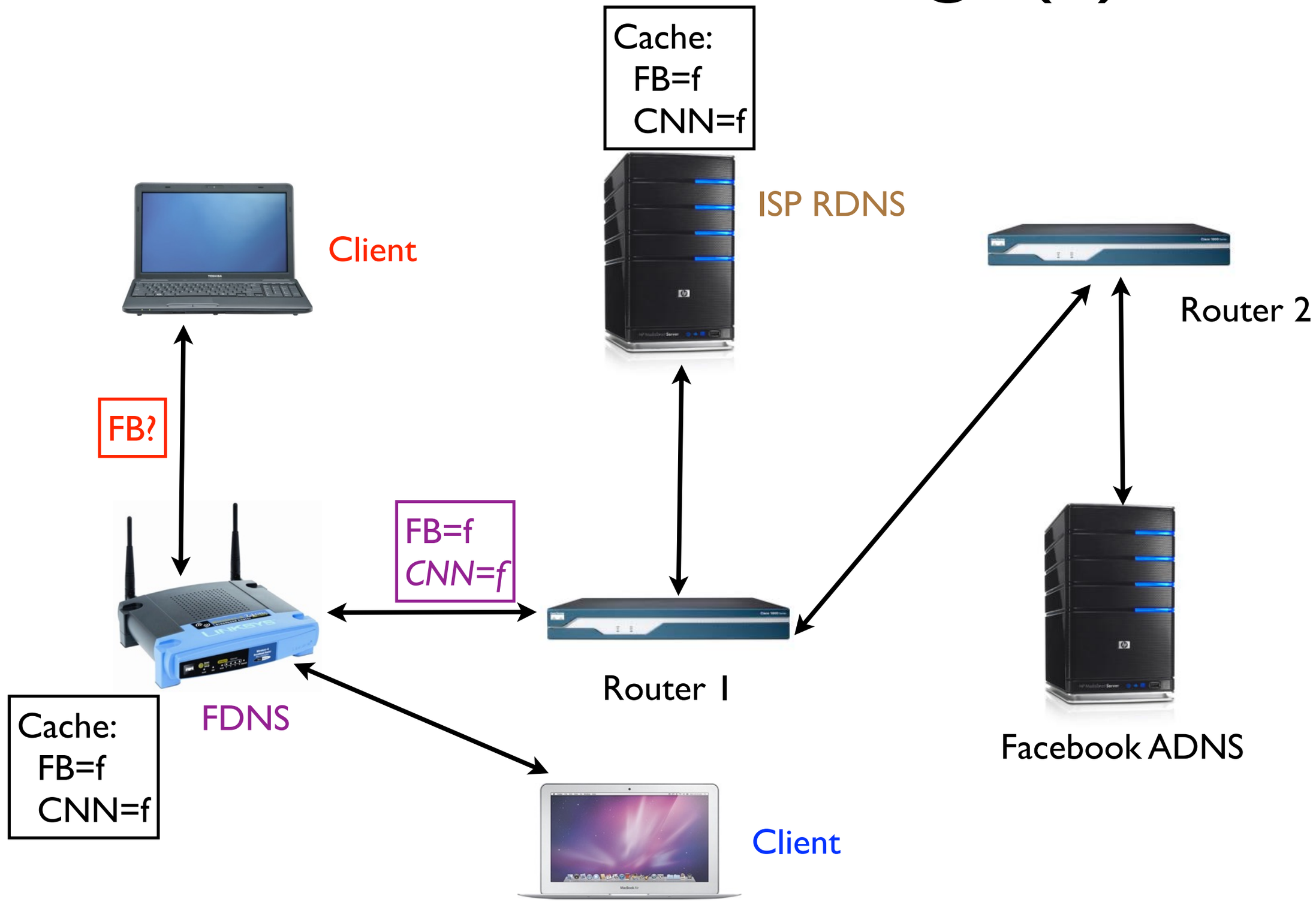
What Can Go Wrong? (1)



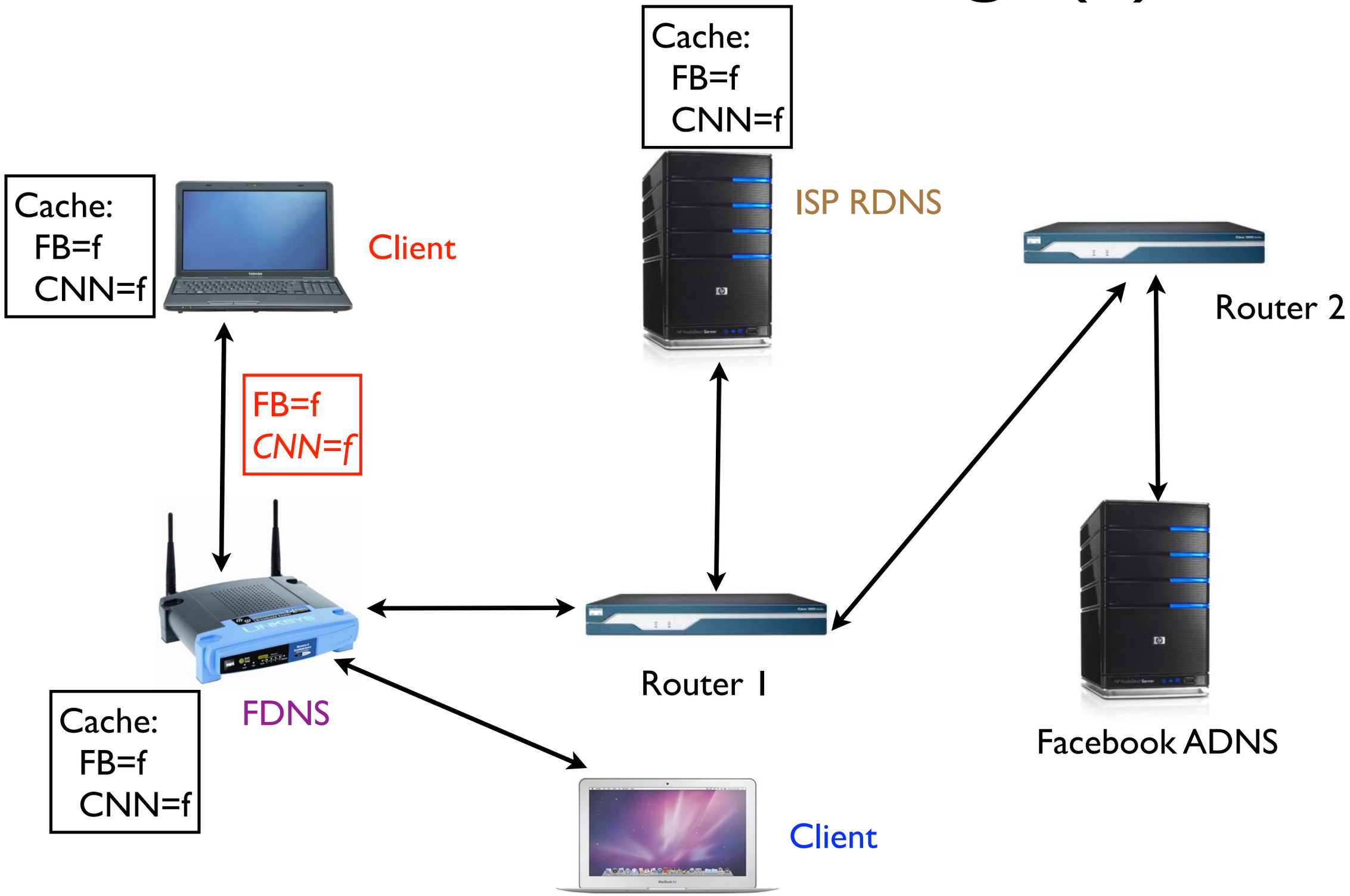
What Can Go Wrong? (1)



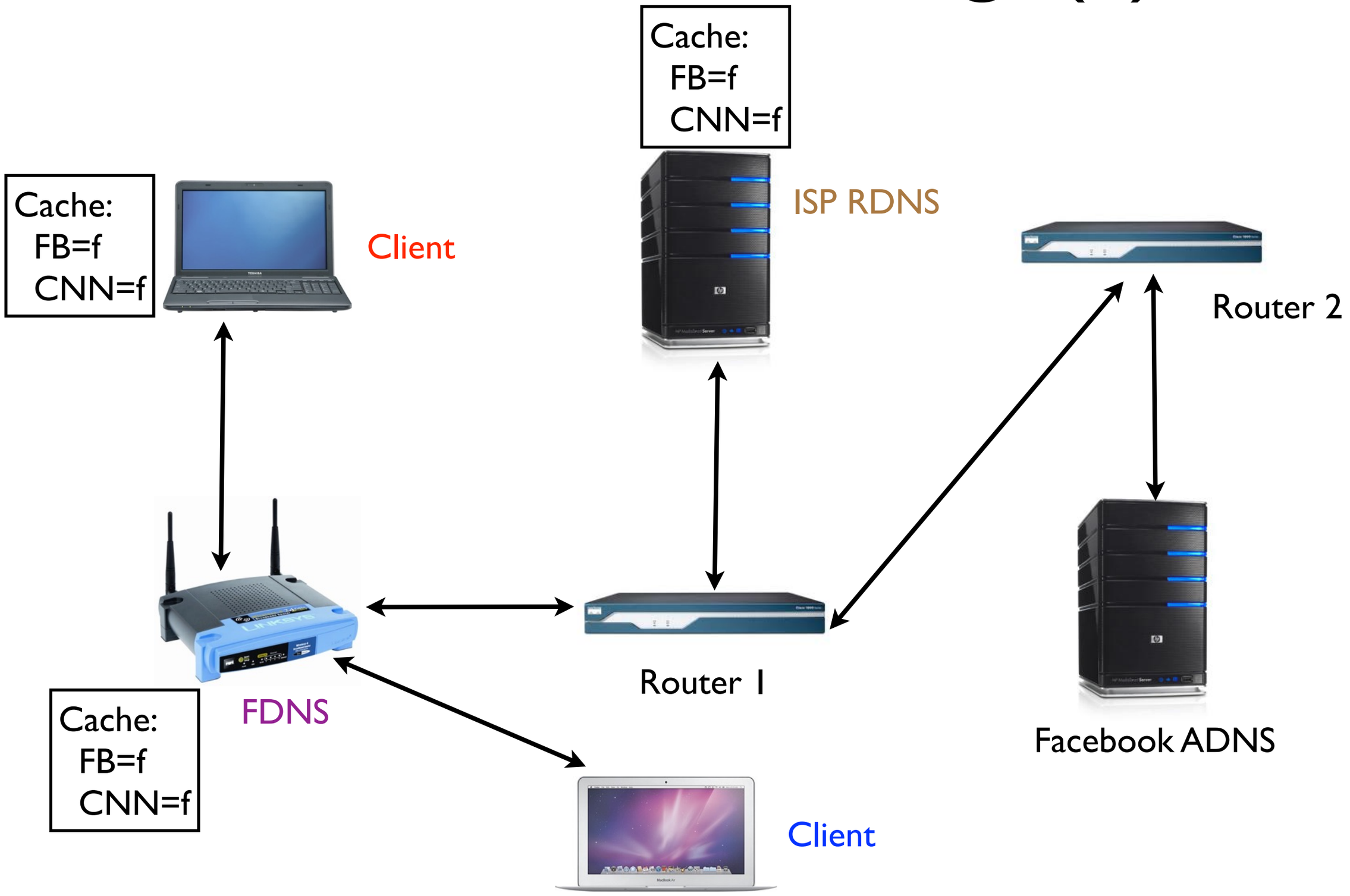
What Can Go Wrong? (1)



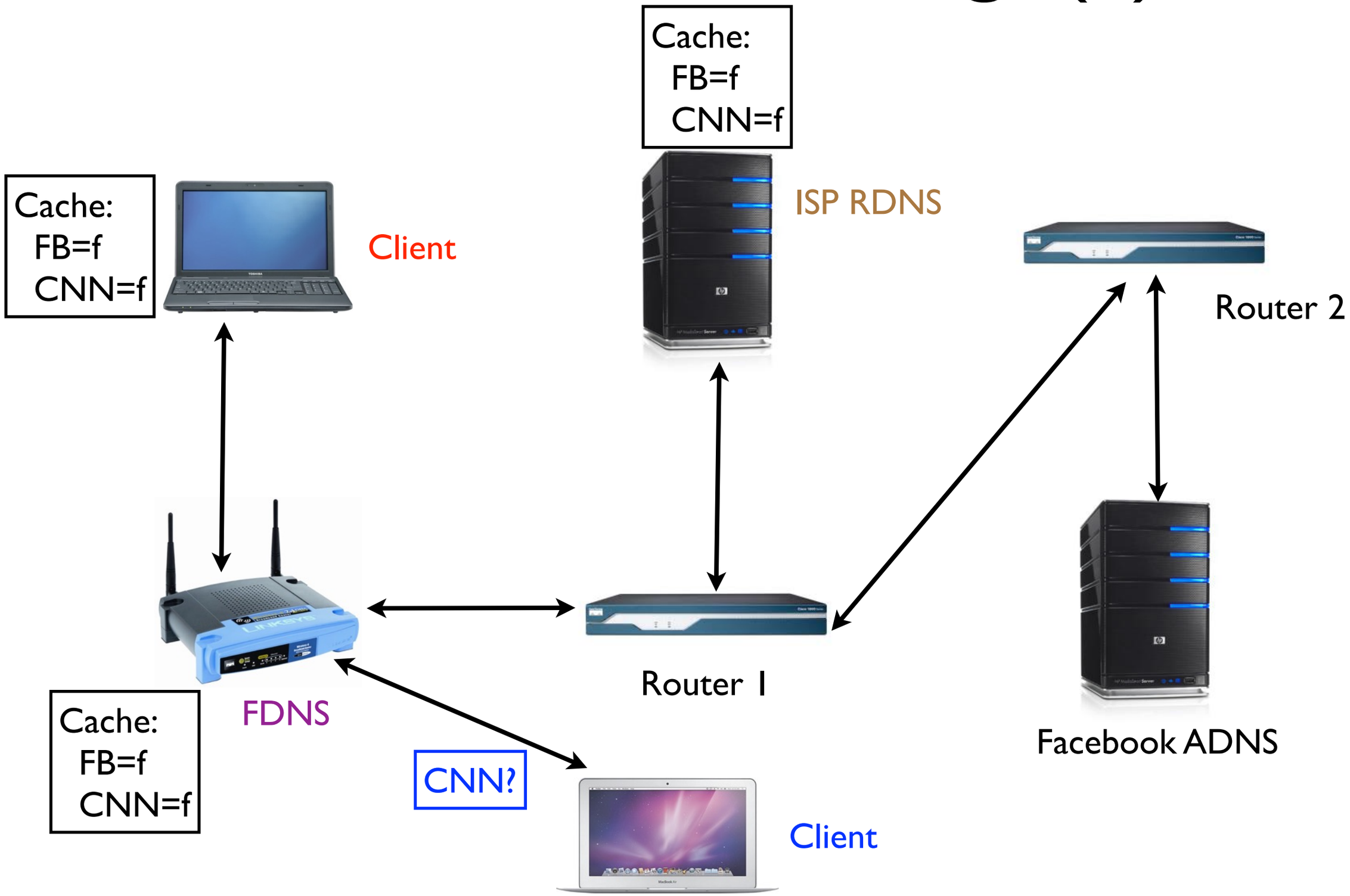
What Can Go Wrong? (1)



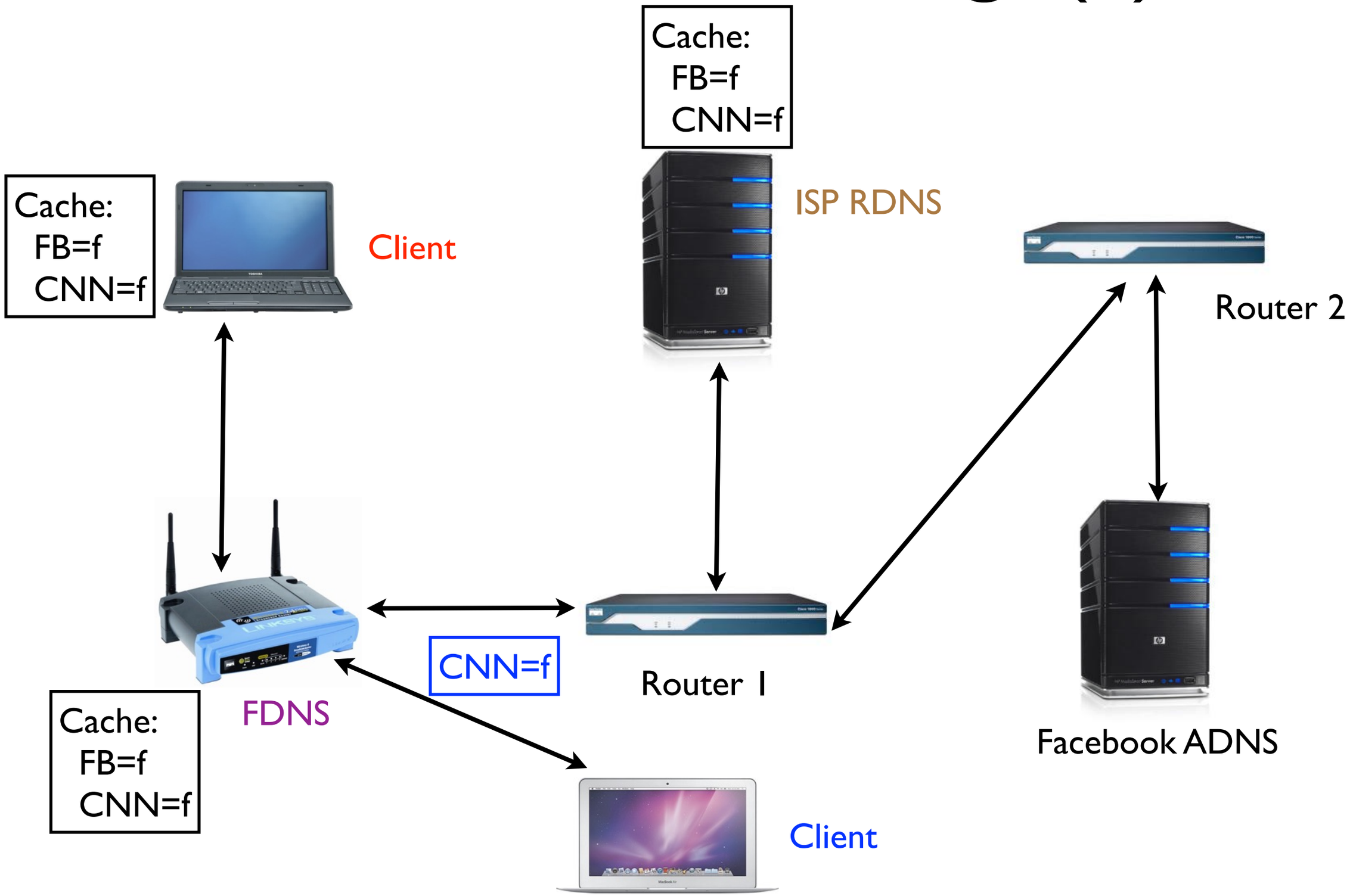
What Can Go Wrong? (1)



What Can Go Wrong? (1)



What Can Go Wrong? (1)



ADNS Lying

ADNS Lying

- ADNS lying is prevented via implementation of bailiwick rules
  - prevents names from outside an ADNS' control from being accepted in responses

ADNS Lying

- ADNS lying is prevented via implementation of bailiwick rules
  - prevents names from outside an ADNS' control from being accepted in responses

- Out of 1.09M open resolvers scanned we find 749 cases where bogus names are cached by part of the DNS infrastructure