NXNSAttack: Recursive DNS Inefficiencies and Vulnerabilities

Yehuda Afek
Tel-Aviv University

Anat Bremler-Barr
Interdisciplinary Center Herzelia

Lior Shafir
Tel-Aviv University

Outline

- **DNS System - Overview**
- **NXNSAttack: New Vulnerability:**
  - Several variants
- **Mitigation and measurements**
- **Responsible Disclosure**
- **Conclusions**

Outline

ZDNet SECURITY NETWORKING

MUST READ RETURN TO WORK: HOW THE TECHNOLOGY MIX WE RELY ON IS ABOUT TO CHANGE, AGAIN

NXNSAttack technique can be abused for large-scale DDoS attacks

WIRED BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY TRANSPORTATION

FOX NEWS channel Coronavirus U.S. World Opinion Politics Entertainment Business TV Fox Nation Listen More Login Watch TV

Hot Topics George Floyd | Coronavirus | Joe Biden

CYBERCRIME · **Published** 4 days ago

Israeli researchers helped thwart potentially massive cyberattack, study shows

By Christopher Carbone | Fox News

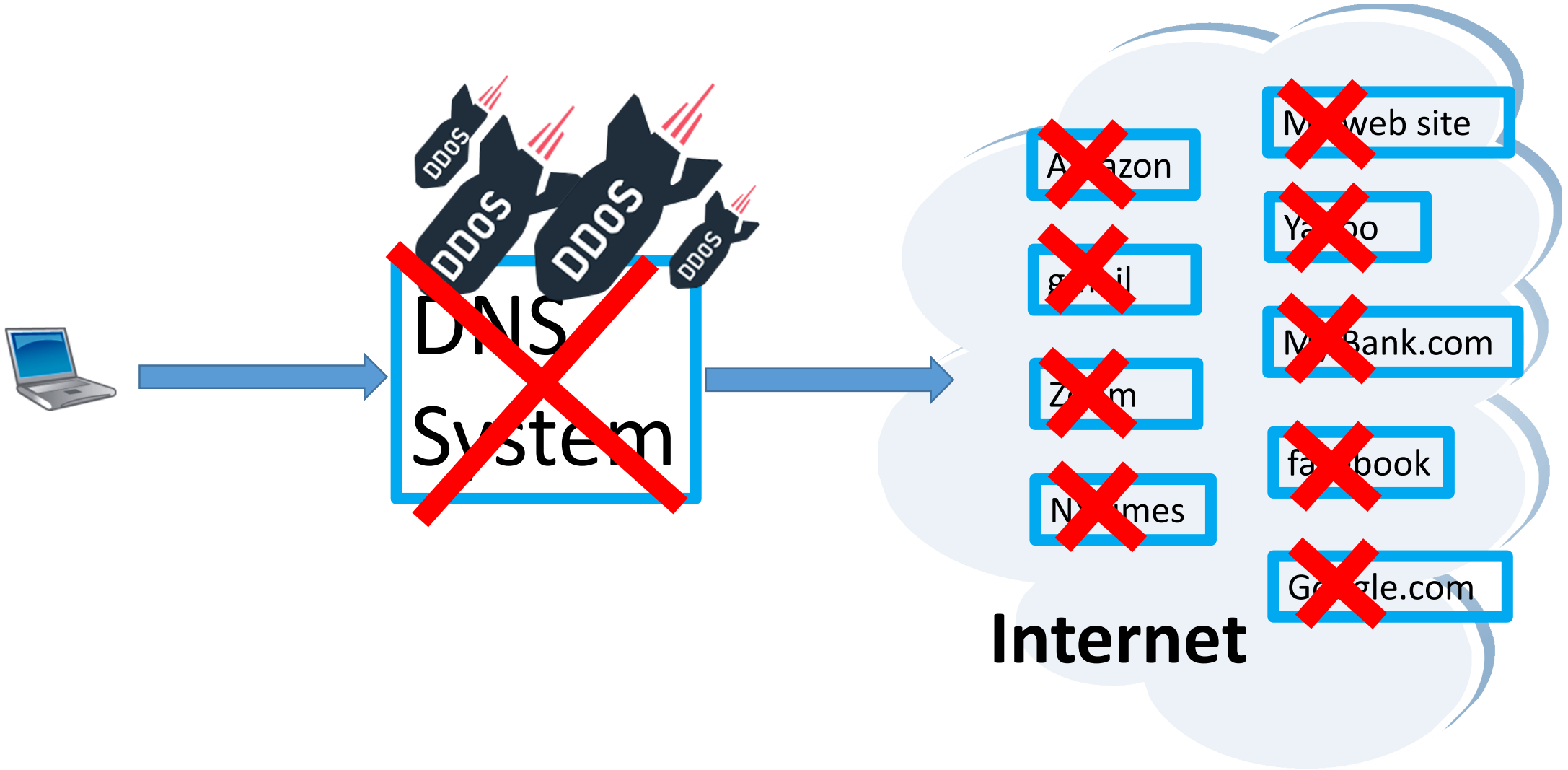
Fox News SciTech

NXNSAttack Vulnerability in the Wild

Vendors

Service Providers

DNS DoSed ➔ Internet useless



This site can't be reached

zoom.us's server DNS address could not be found.

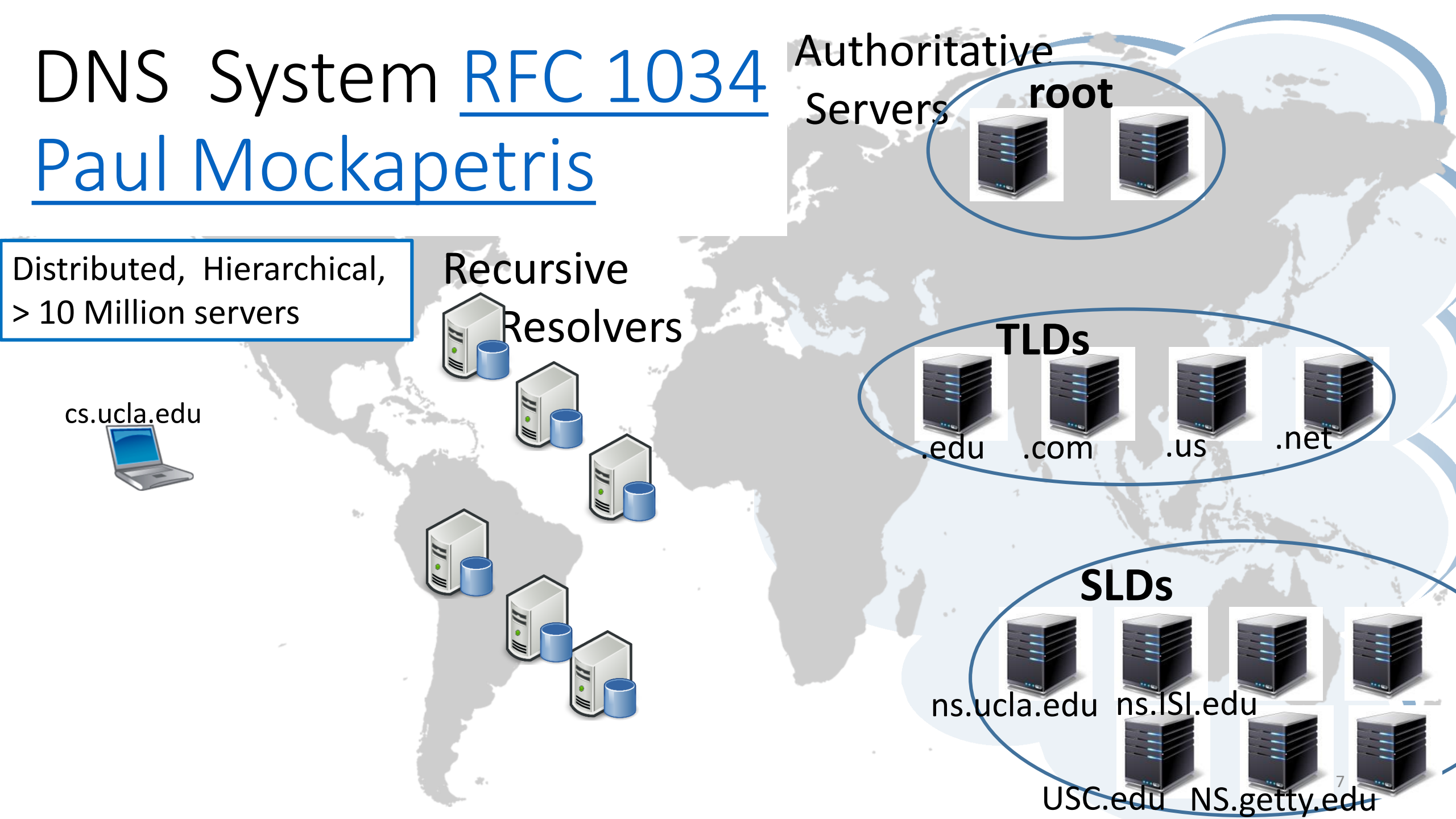
Search Google for zoom us

ERR_NAME_NOT_RESOLVED

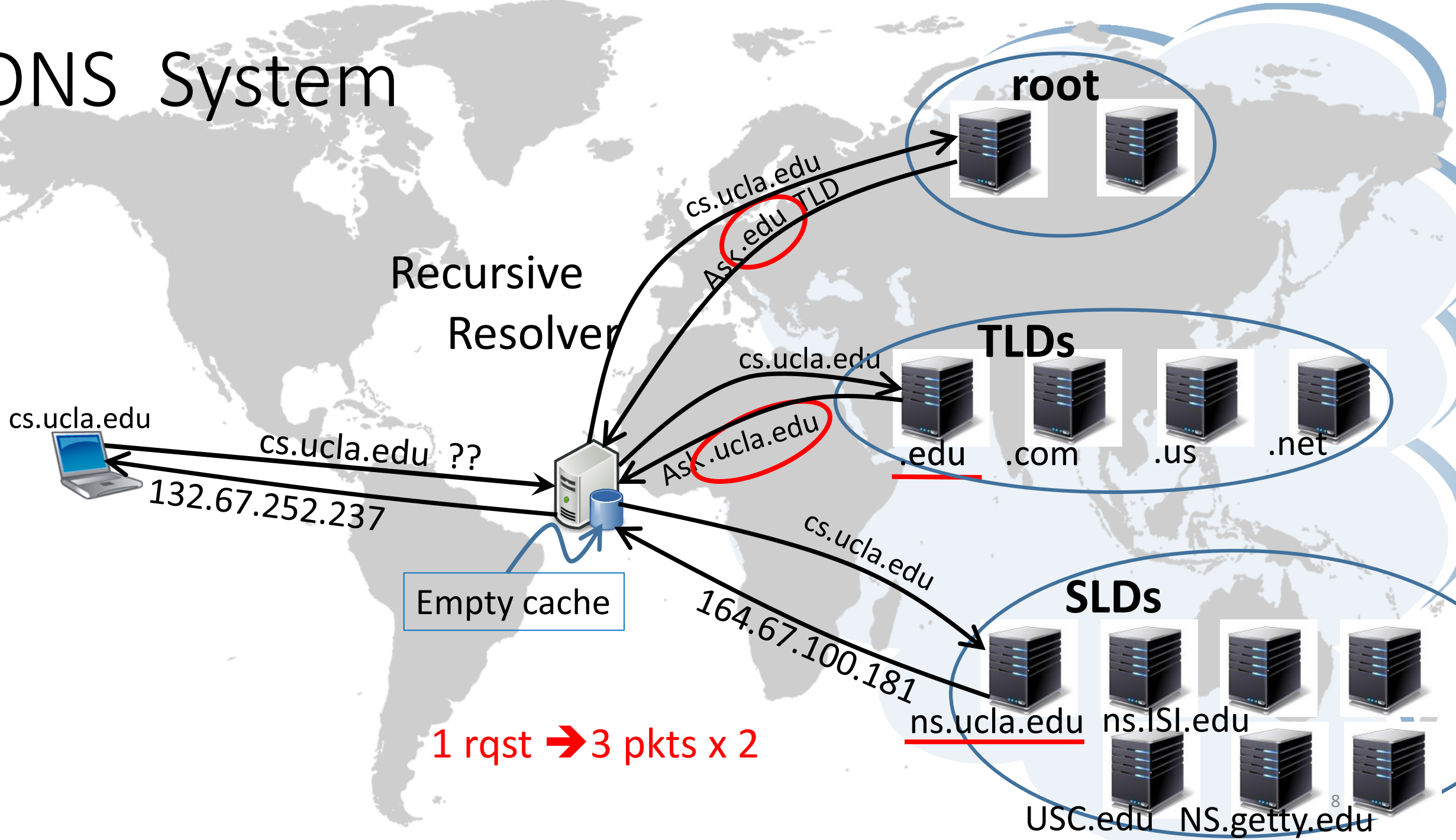
Show saved copy

DNS System RFC 1034 Paul Mockapetris

Distributed, Hierarchical,
> 10 Million servers



DNS System

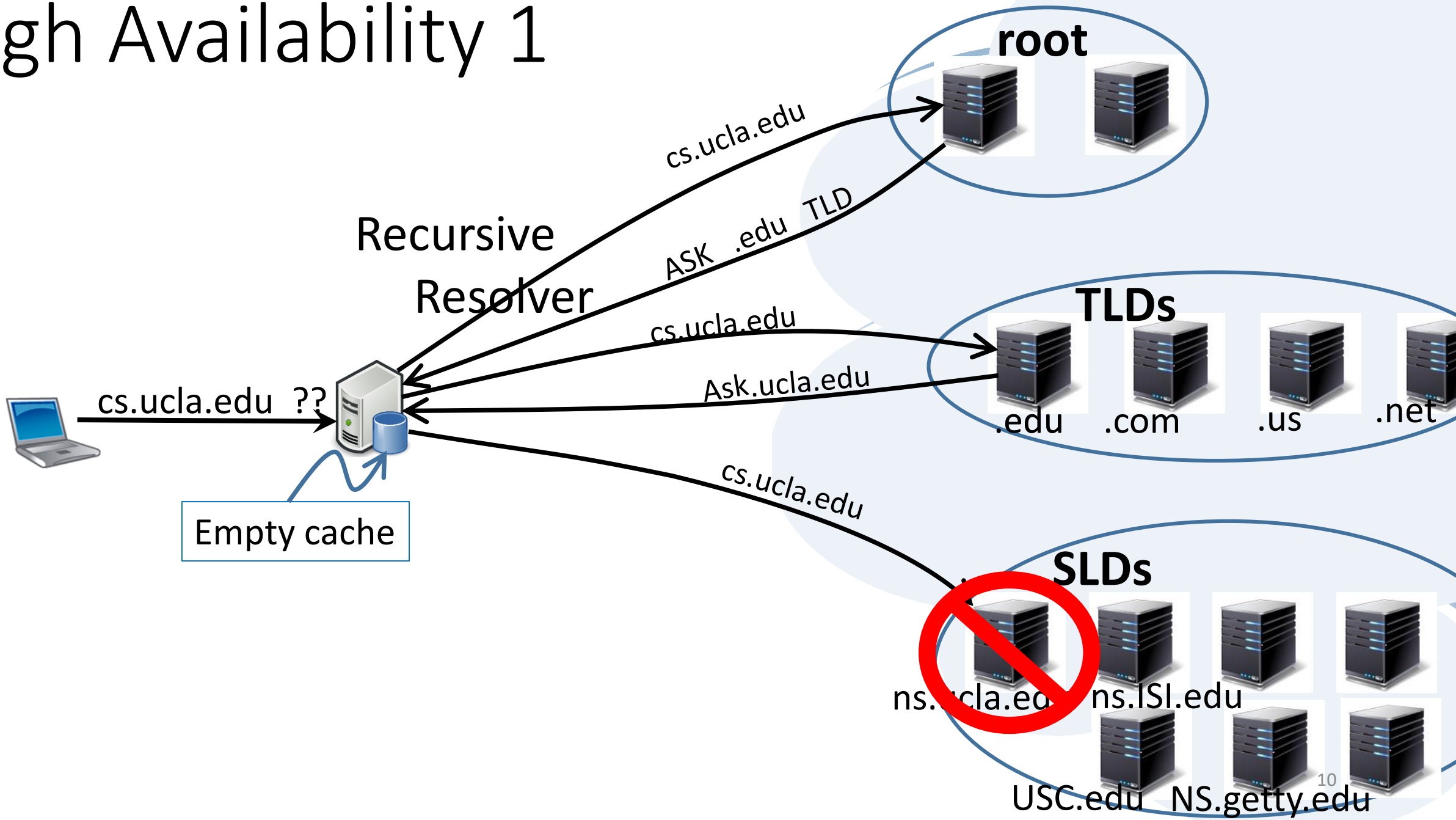

root
cs.ucla.edu
Ask.edu TLD
Recursive
Resolver
TLDs
cs.ucla.edu
cs.ucla.edu
Ask.ucla.edu
.edu
.com
.us
.net
cs.ucla.edu ??
132.67.252.237
Empty cache
cs.ucla.edu
164.67.100.181
SLDs
ns.ucla.edu
ns.ISI.edu
USC.edu
NS.getty.edu
1 rqst ➔3 pkts x 2

DNS system [RFC 1034, Mockapetris 1987]

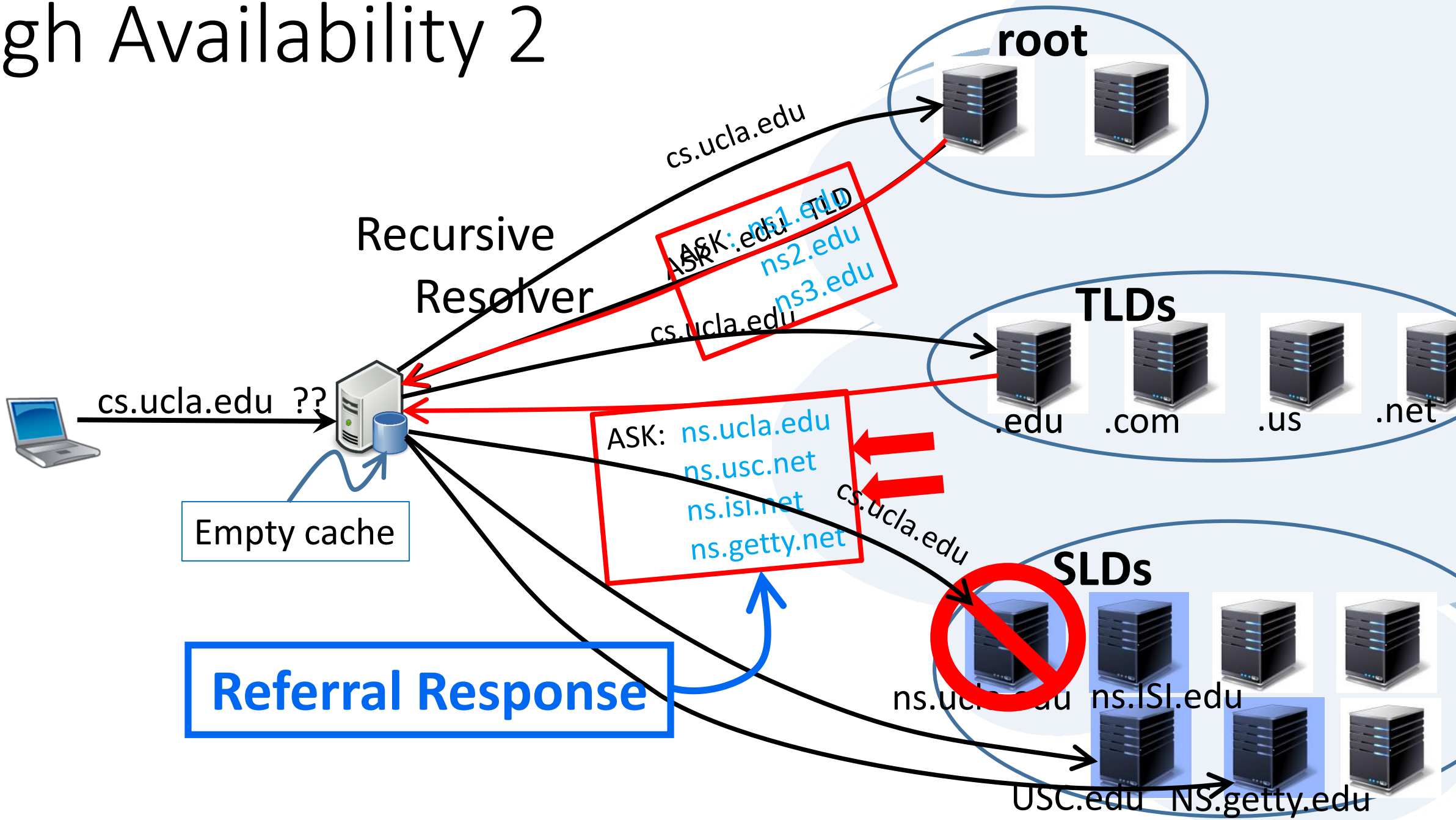
Requirements

- High Availability, 24x7, Fault tolerant
- Quick response
- Low communication overhead
- Authenticate

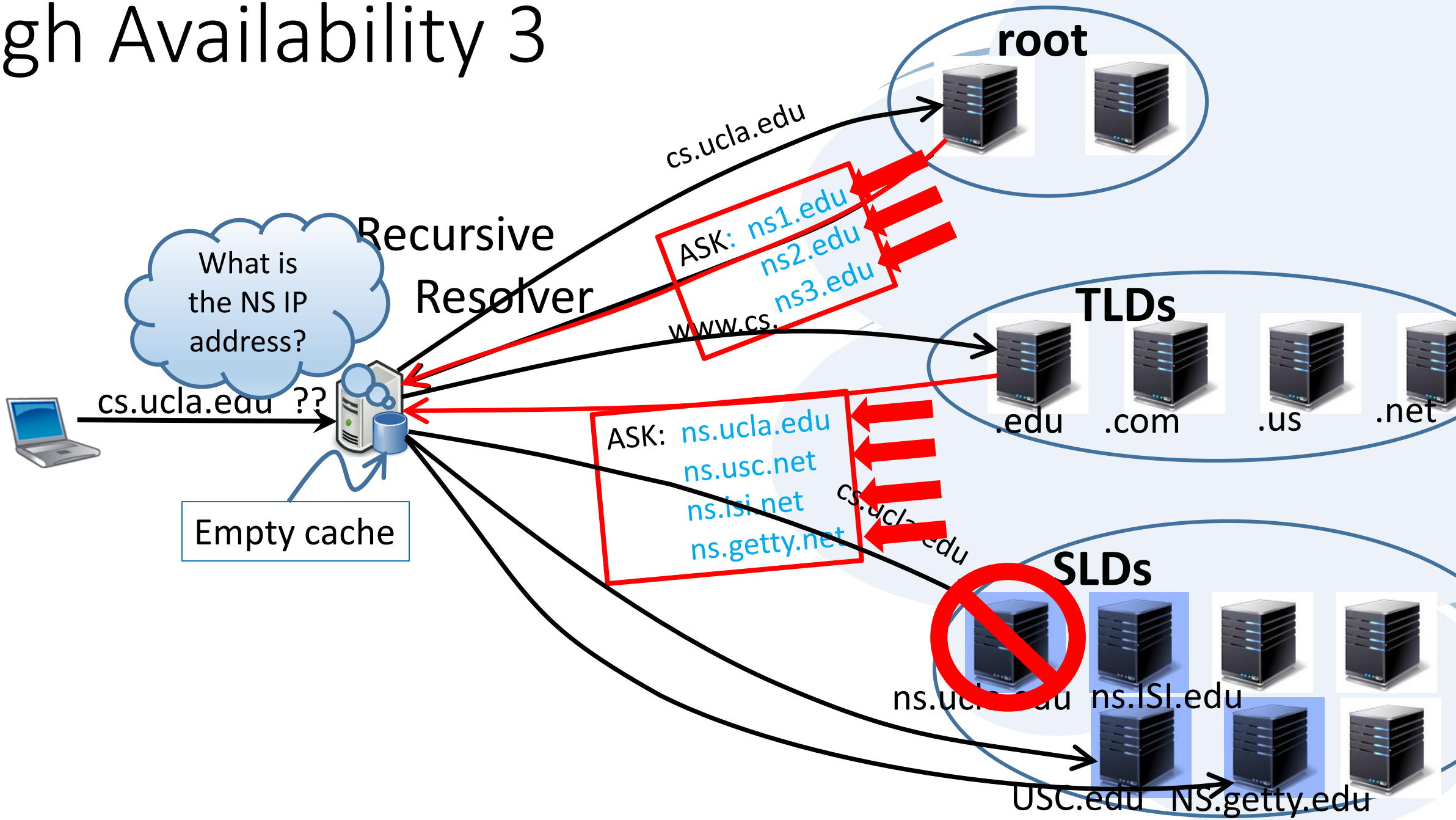
High Availability 1



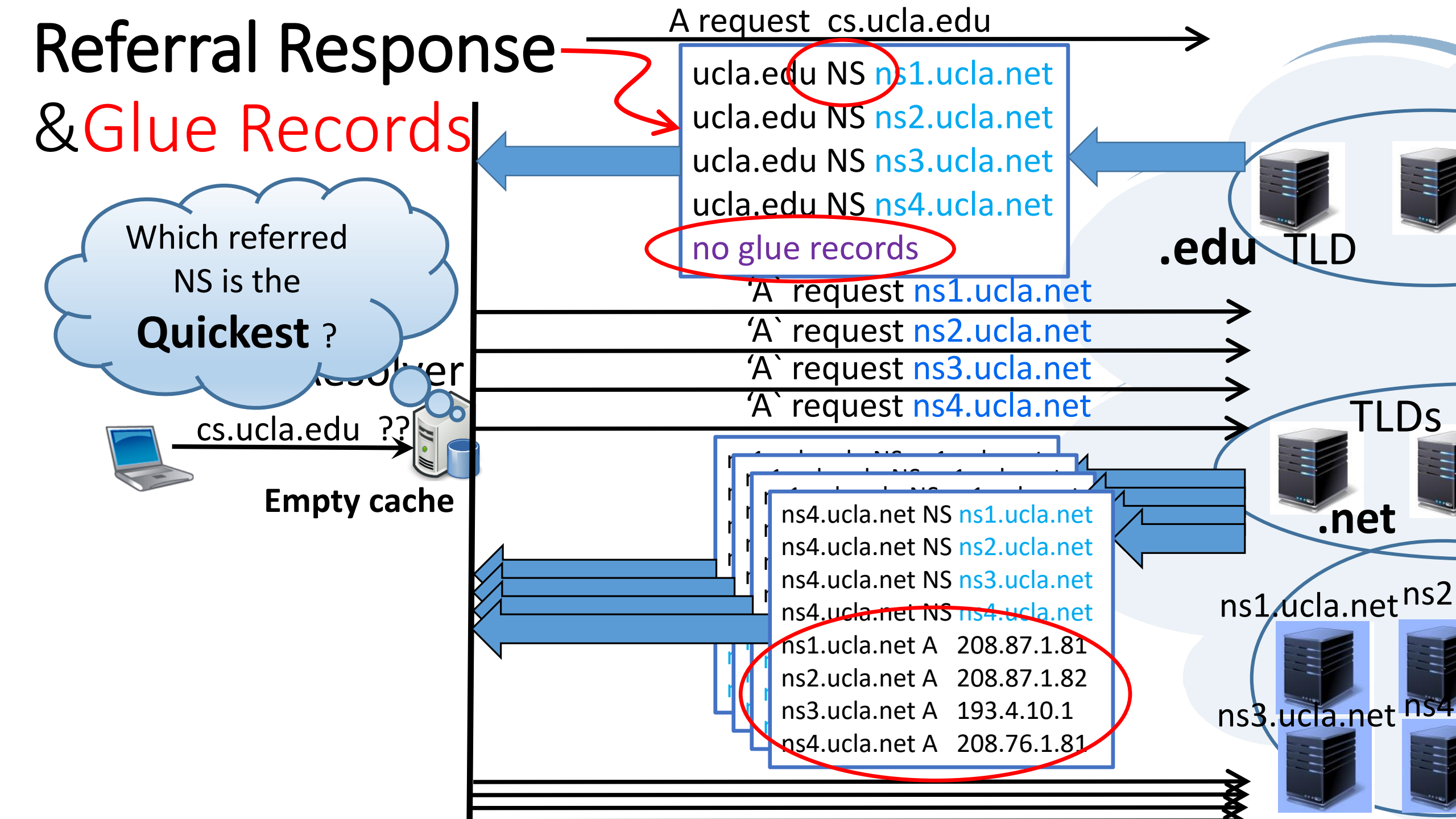
High Availability 2

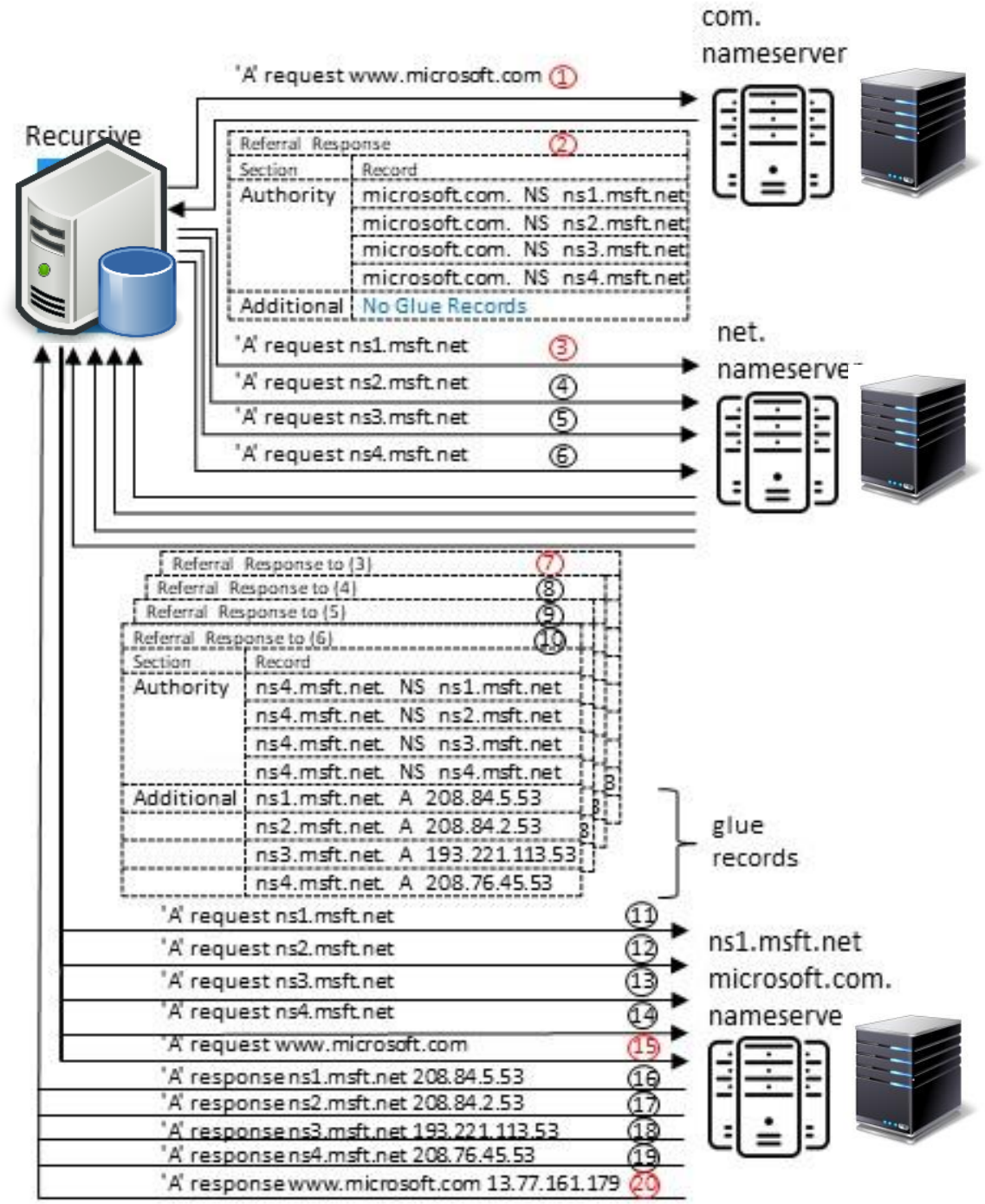


High Availability 3



Referral Response &Glue Records





Practice:

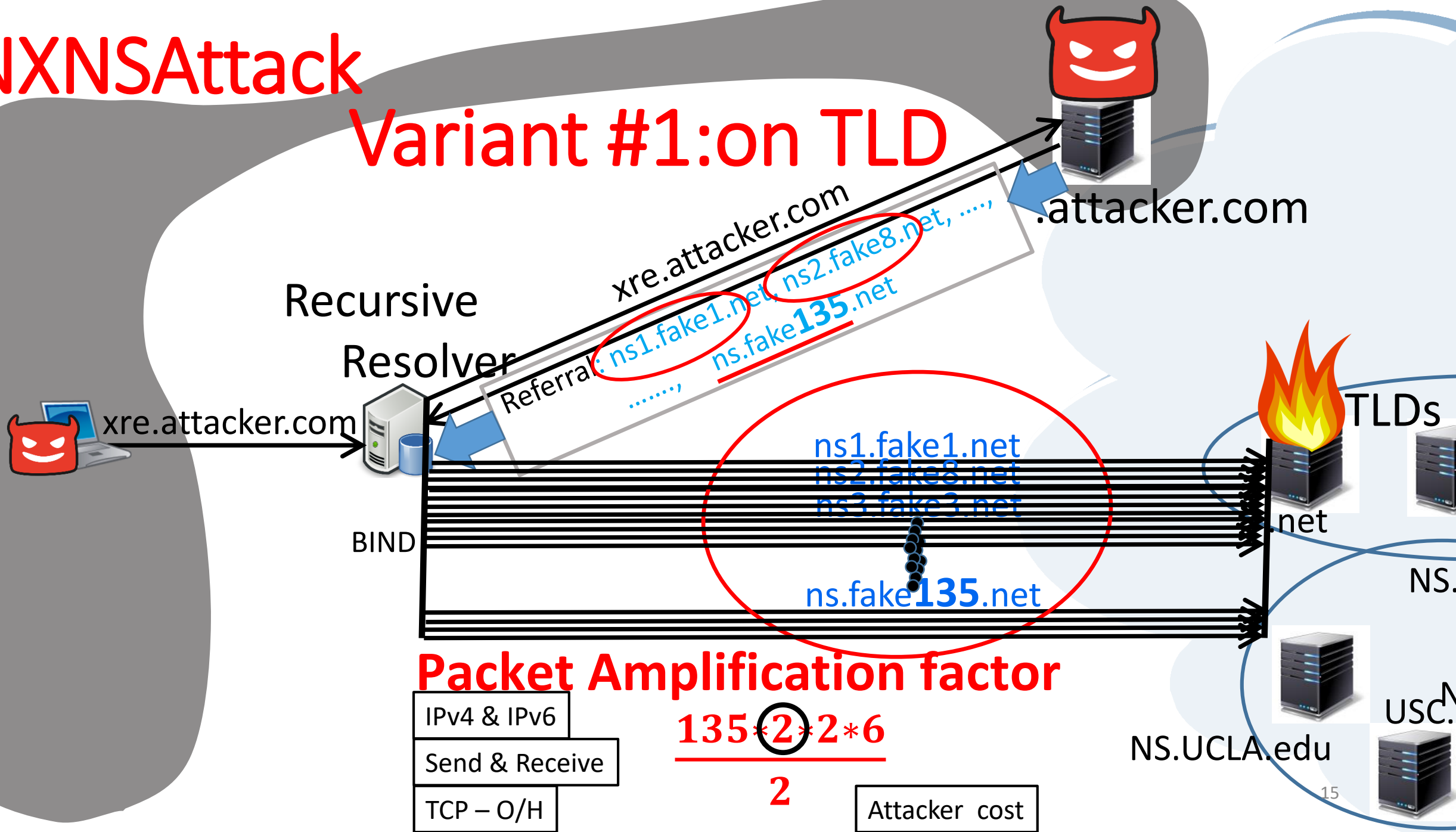
1 rqst microsoft.com ➔
54 (126) pkts !!

Theory:

1 rqst ➔3 pkts x 2

NXNSAttack

Variant #1:on TLD



Packet Amplification factor

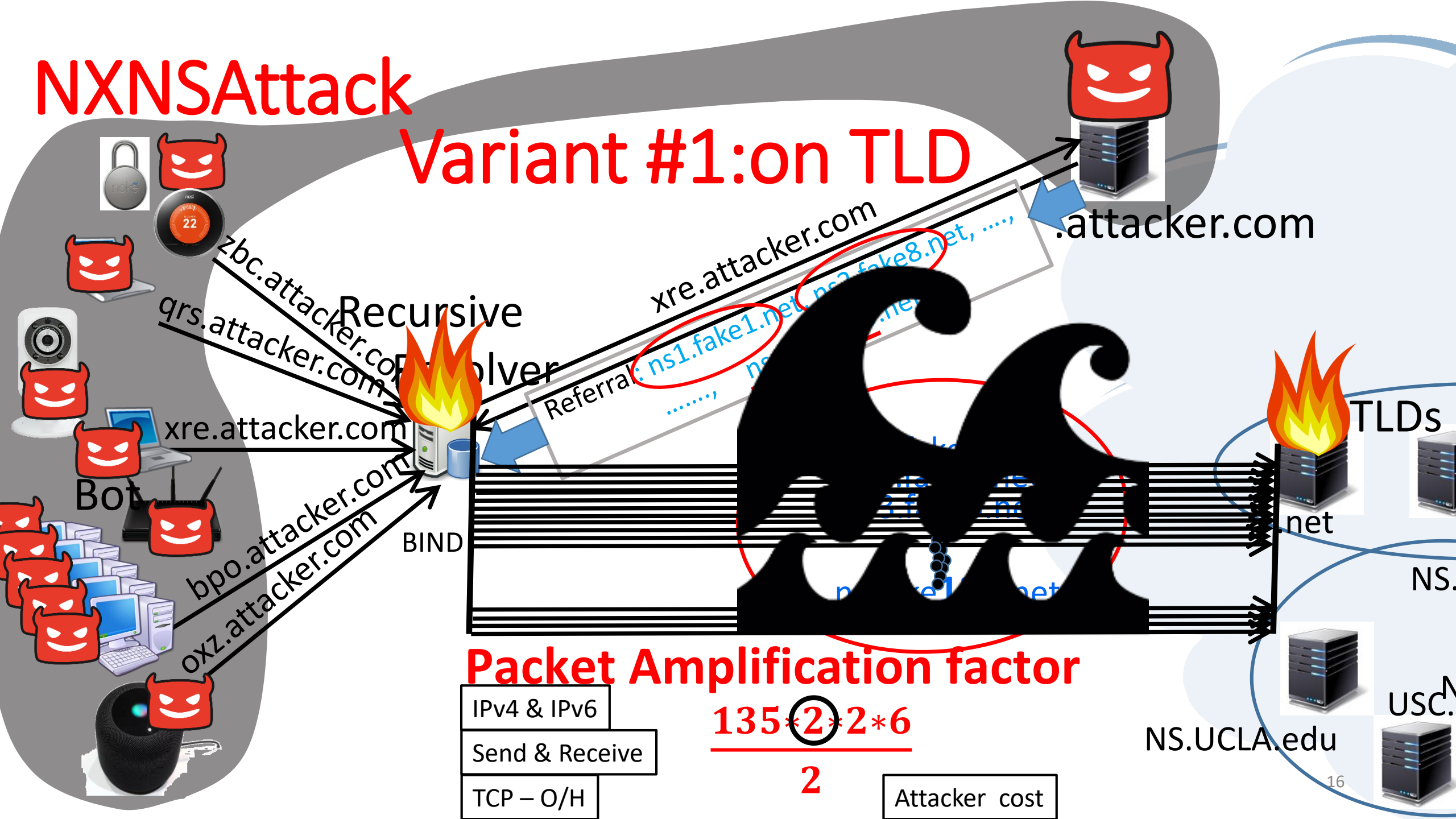
$$\frac{135 * 2 * 2 * 6}{2}$$

- IPv4 & IPv6
- Send & Receive
- TCP – O/H

Attacker cost

NXNSAttack

Variant #1:on TLD



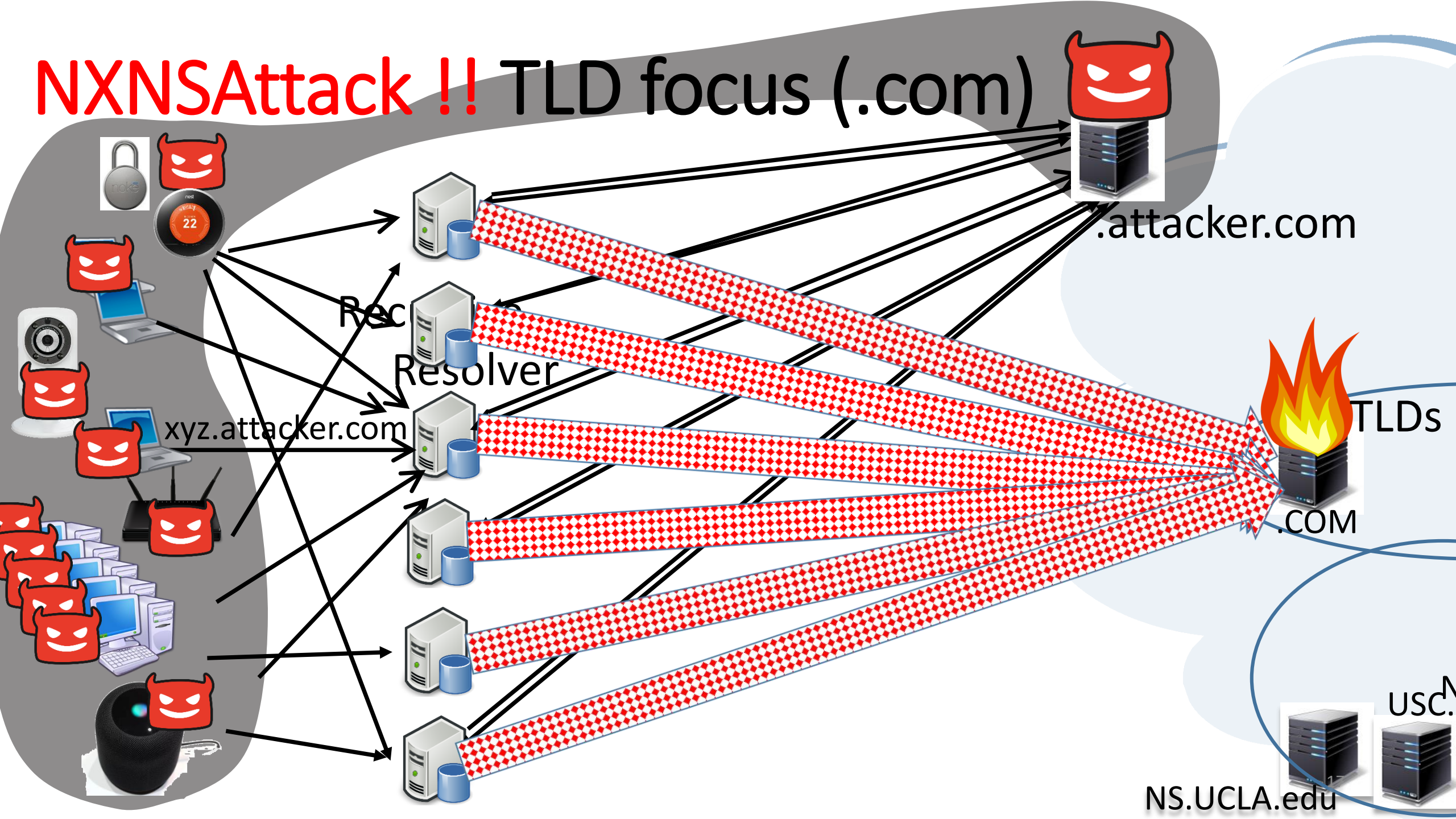
Packet Amplification factor

$$\frac{135 * 2 * 2 * 6}{2}$$

- IPv4 & IPv6
- Send & Receive
- TCP – O/H

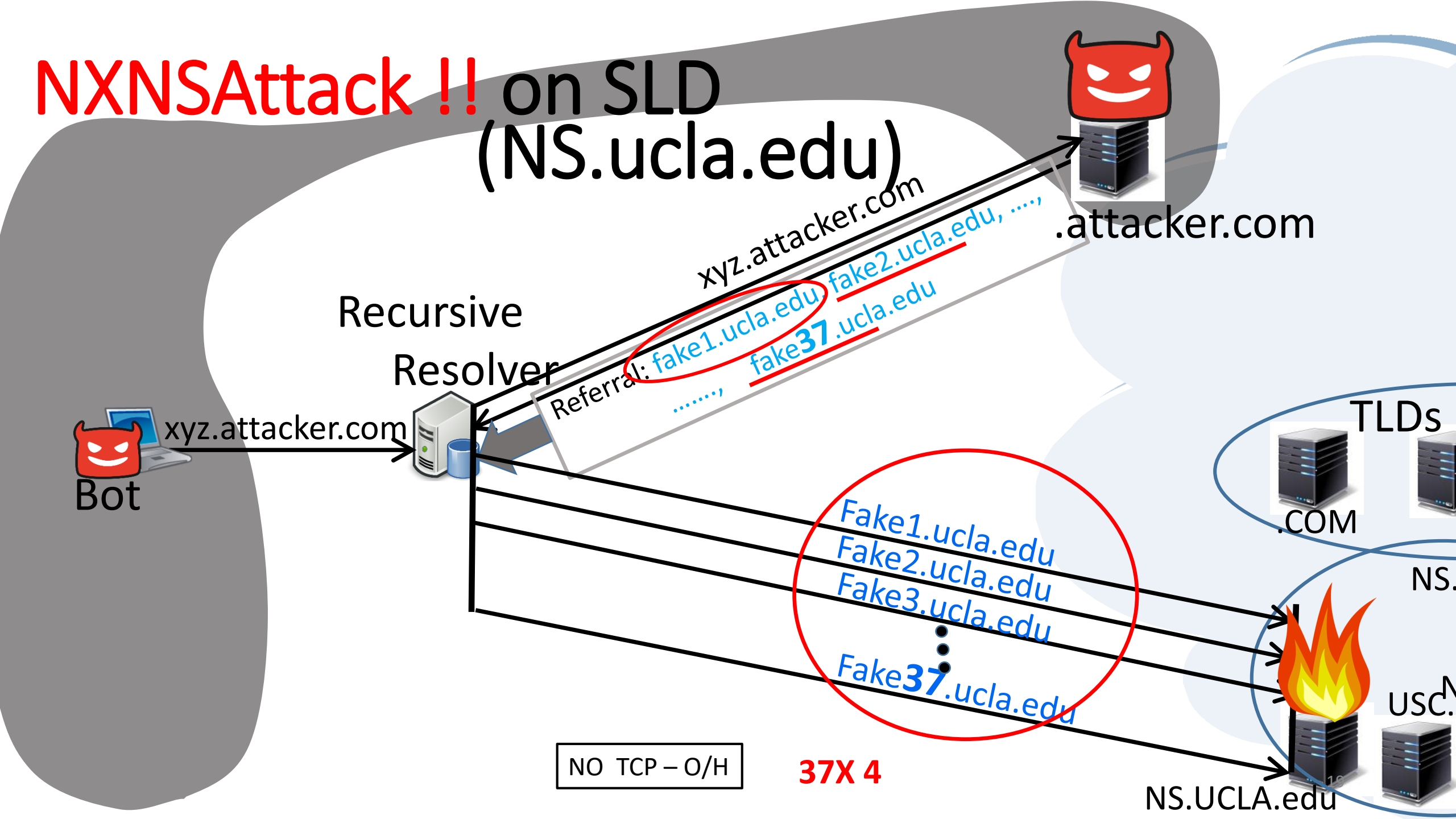
Attacker cost

NXNSAttack !! TLD focus (.com)

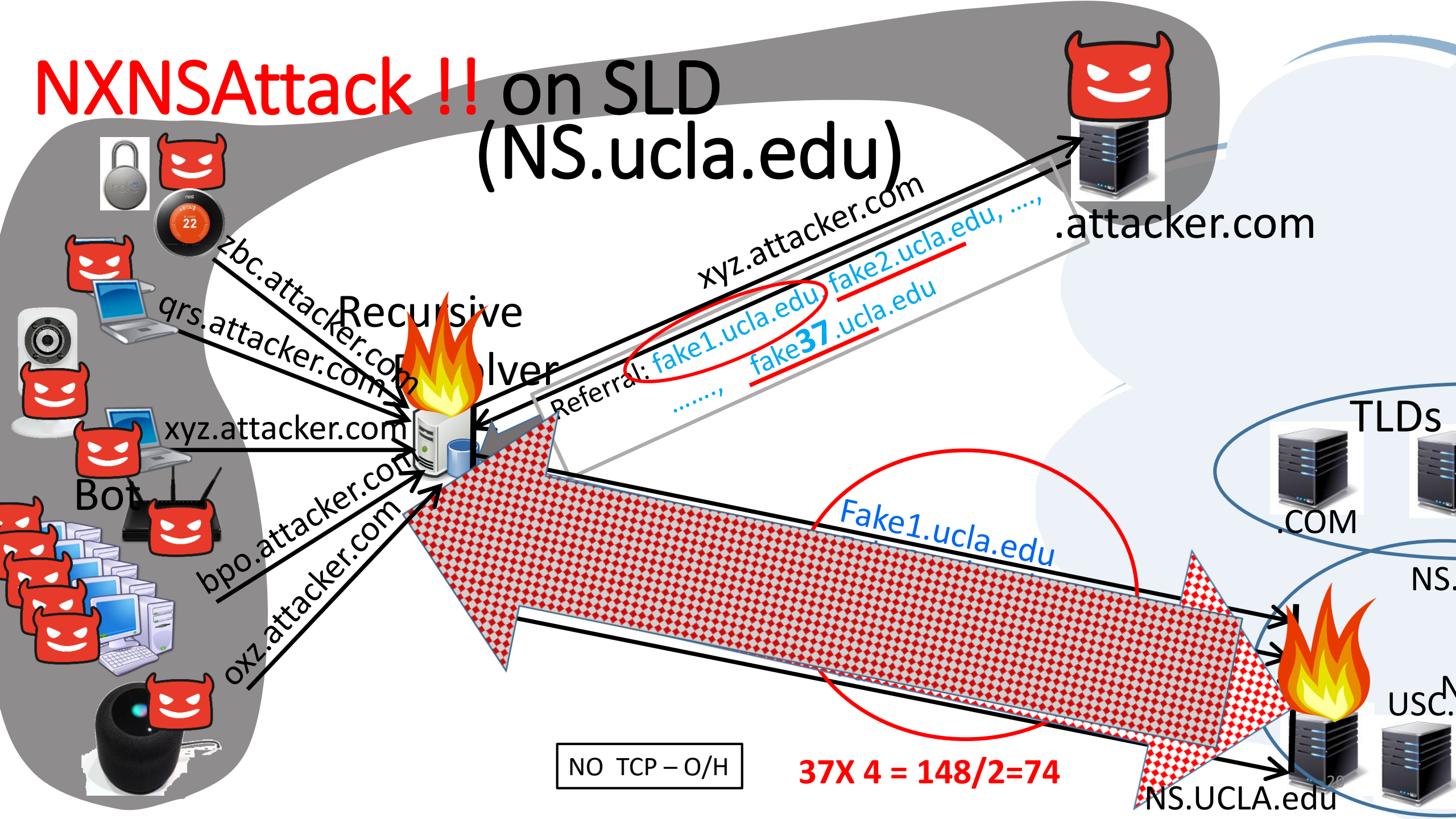


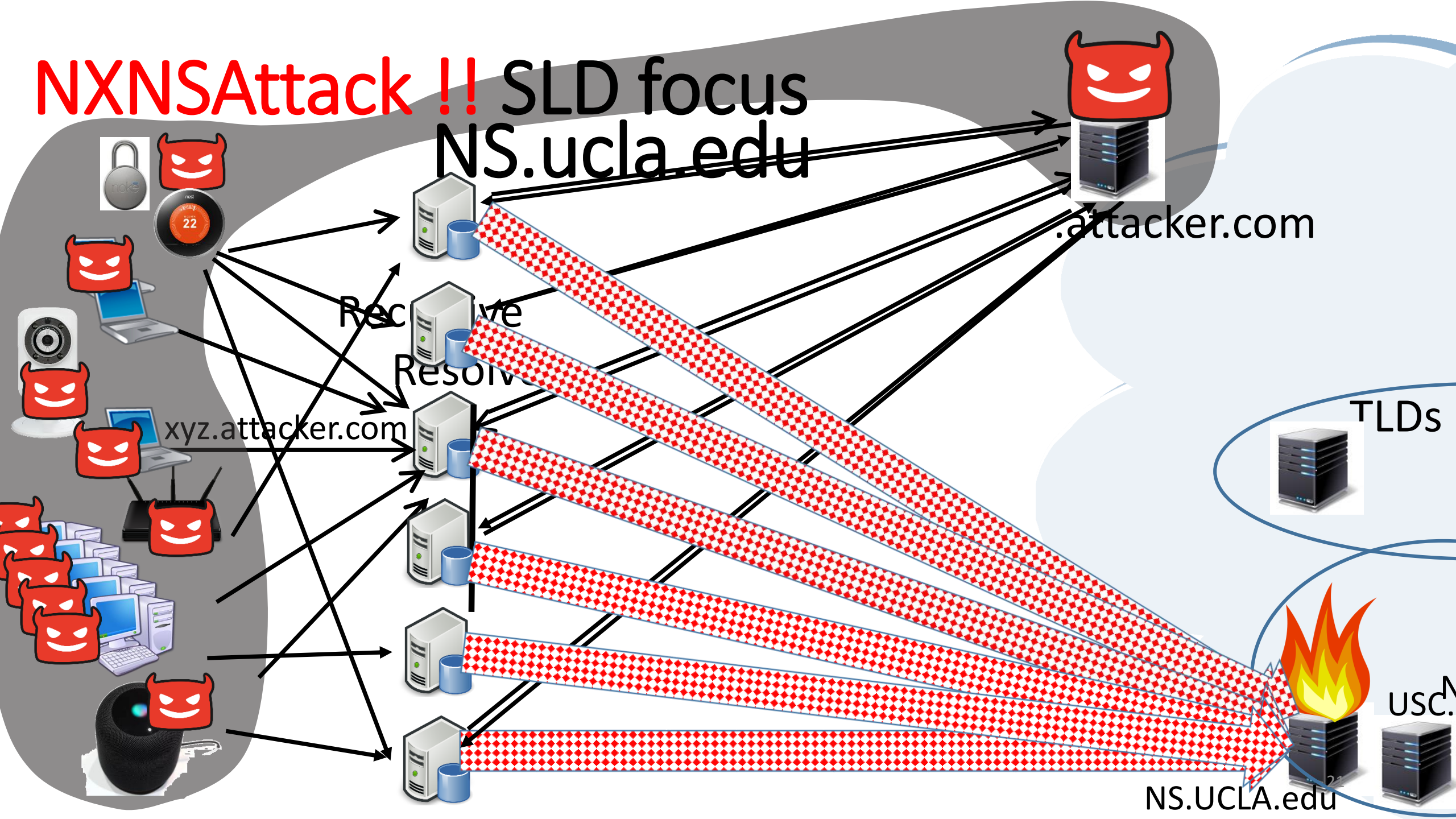
Other Variations

NXNSAttack !! on SLD (NS.ucla.edu)

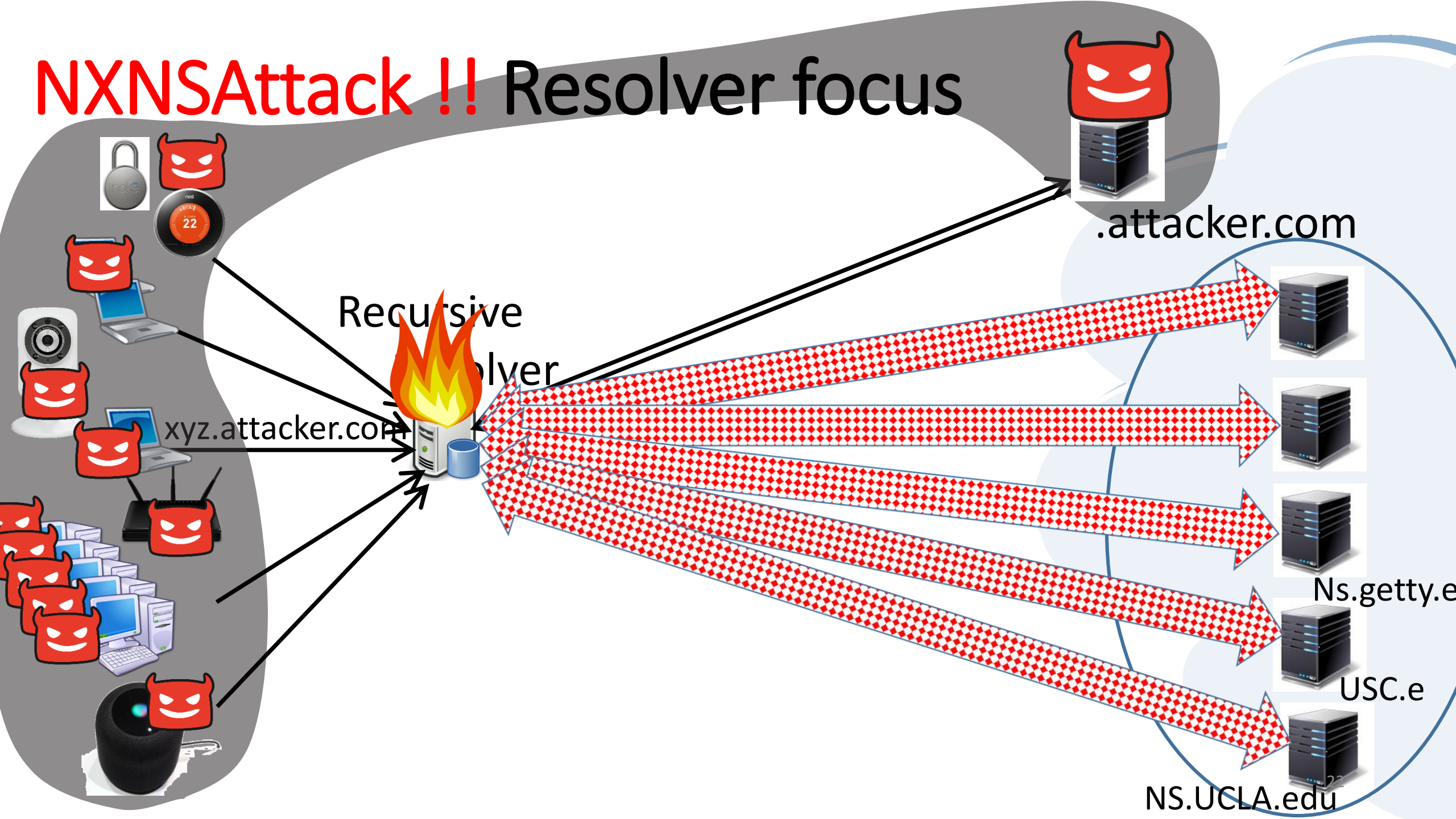


NXNSAttack !! on SLD (NS.ucla.edu)

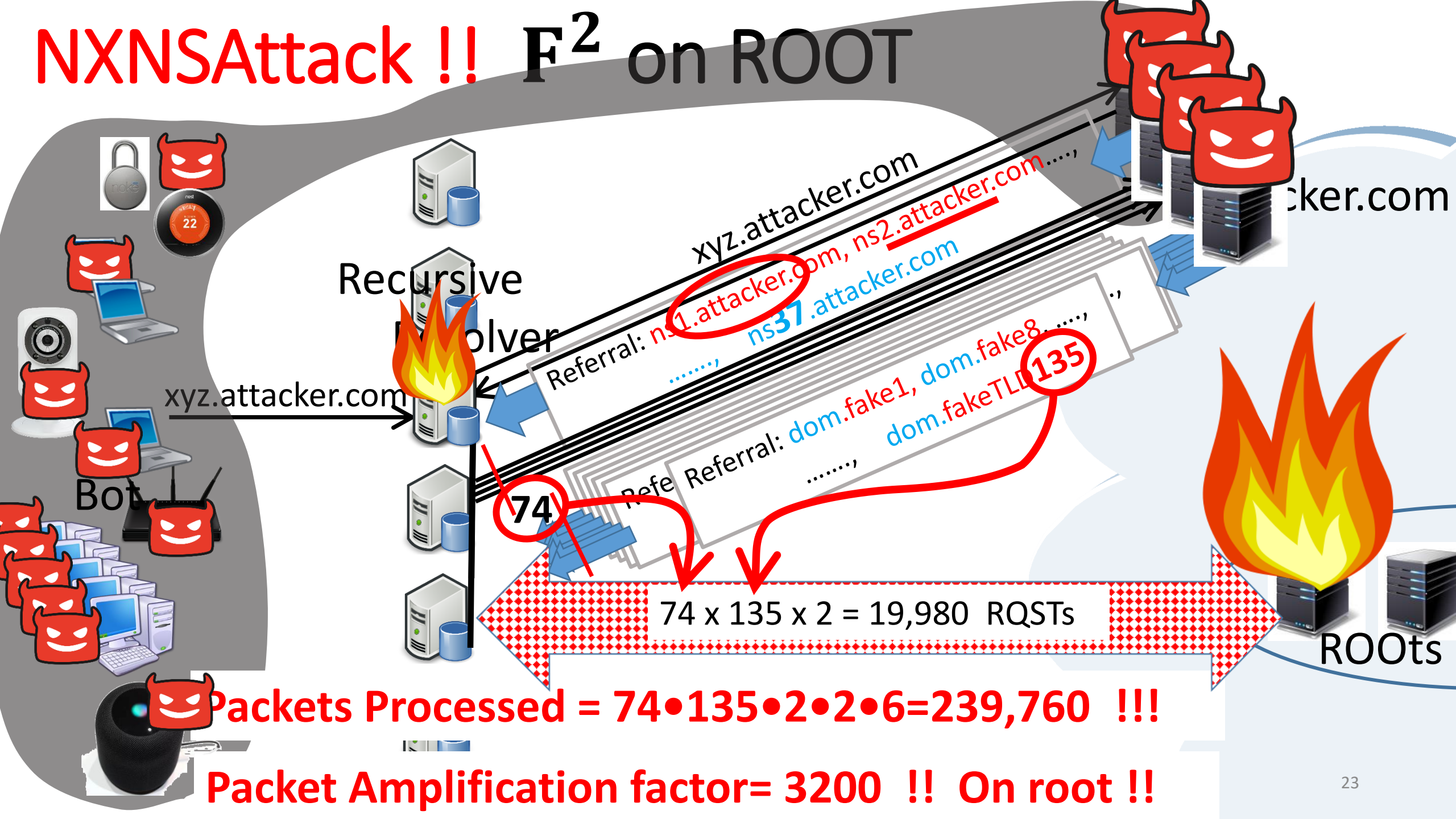



NXNSAttack !! SLD focus
NS.ucla.edu
.attacker.com
Rec ve
Resolv
xyz.attacker.com
TLDs
NS.UCLA.edu

NXNSAttack !! Resolver focus



NXNSAttack !! F^2 on ROOT



Packets Processed = 74•135•2•2•6=239,760 !!!

Packet Amplification factor= 3200 !! On root !!

Acquiring / controlling an Authoritative

- Option 1: $1 and 5 minutes, to acquire a new domain name

  Dynamic association with any Authoritative

- Option 2: DNS hijacking attacks

  Gain operators' credentials to manipulate zone-files

Amplifications in the wild

Public DNS recursive resolver (IP)	Max # of delegations = F/2	Victim cost C_v^{pkt}	PAF
CloudFlare (1.1.1.1)	24	96	48x
Comodo Secure (8.26.56.26)	140	870	435x
DNS.Watch (84.200.69.80)	135	972	486x
Dyn (216.146.35.35)	50	408	204x
FreeDNS (37.235.1.174)	50	100	50x
Google (8.8.8.8)	15	60	30x
Hurricane (74.82.42.42)	50	98	49x
Level3 (209.244.0.3)	135	546	273x
Norton ConnectSafe (199.85.126.10)	140	1138	569x
OpenDNS (208.67.222.222)	50	64	32x
Quad9 (9.9.9.9)	100	830	415x
SafeDNS (195.46.39.39)	135	548	274x
Ultra (156.154.71.1)	100	810	405x
Verisign (64.6.64.6)	50	404	202x

Table 3: Firepower and PAF of public resolvers as a response to a single request in the NXNSAttack.

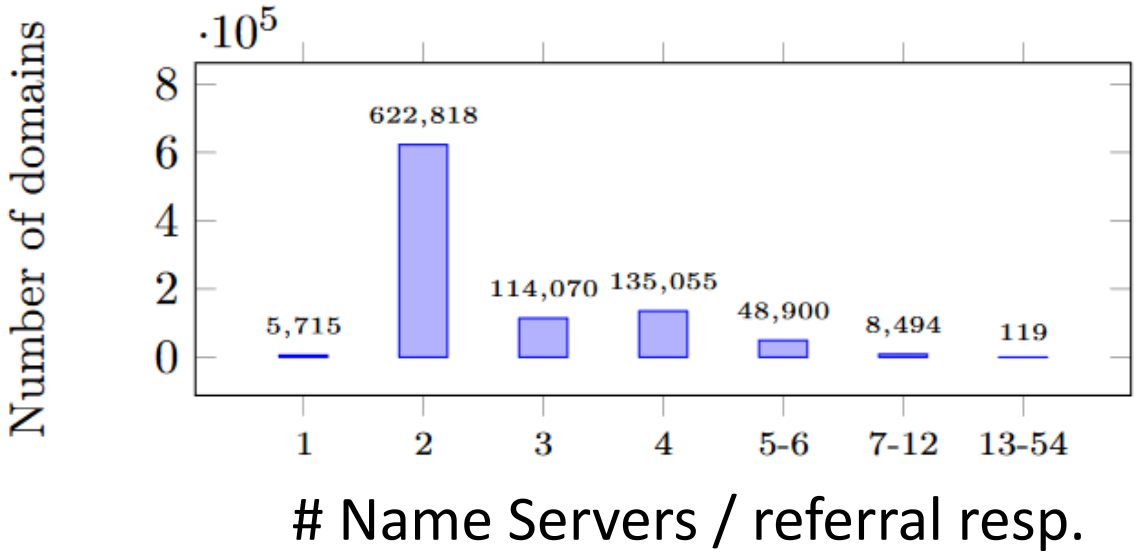
Mitigation

- MaxFetch(k) – Resolve NS-names k at a time, not all at once
  - Amortized on several queries

- MaxBreadth – bound # of NS-names per referral response

- Detect NX NS replies (NLnetLabs)

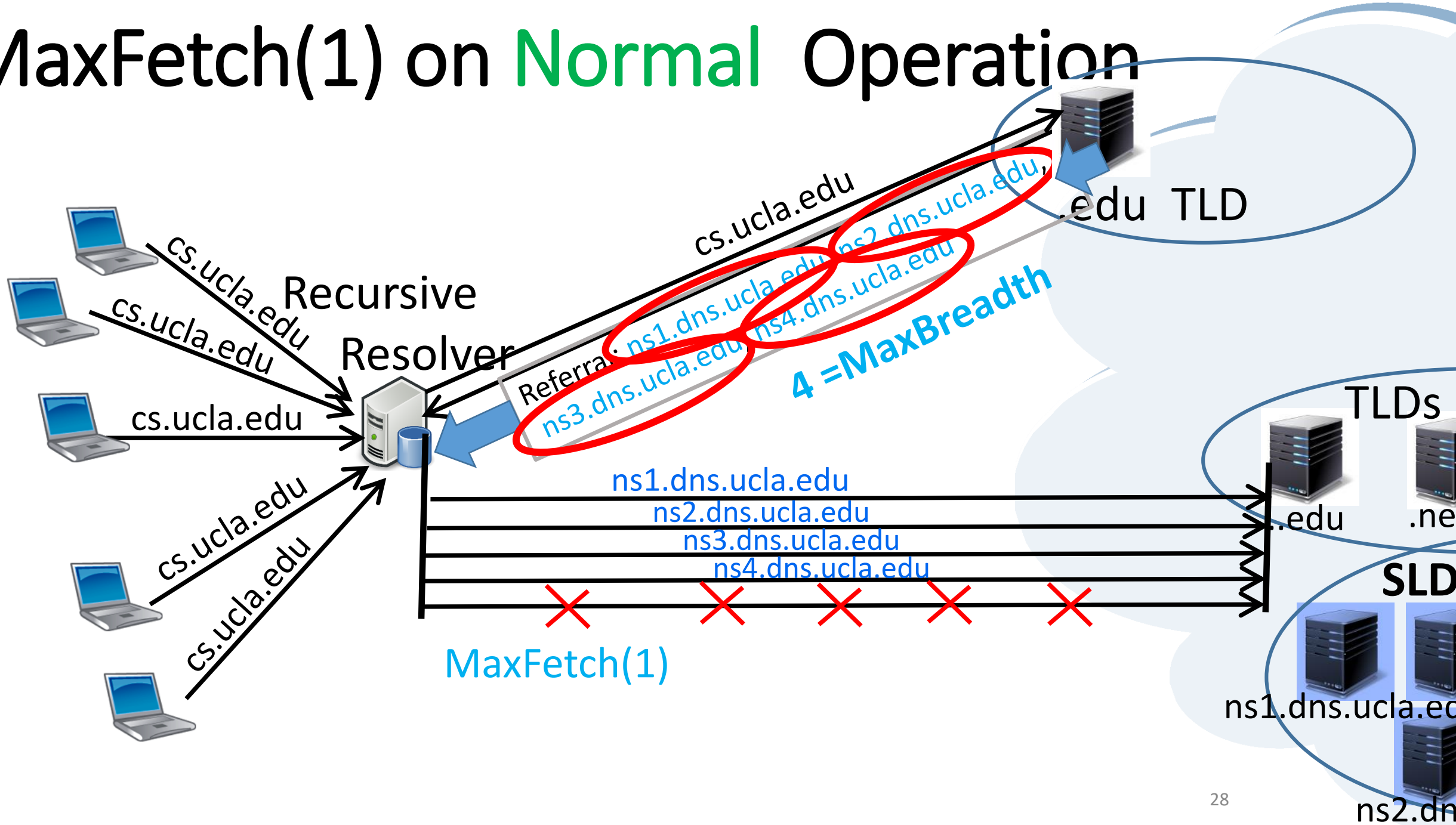
- DNSSEC – NSEC (Petr Špaček)



Mitigation

- MaxFetch(k) – Resolve NS-names k at a time, not all at once
  - Amortized on several queries
- MaxBreadth – bound # of NS-names per referral response
- Detect NX NS replies (NLnetLabs)
- DNSSEC – NSEC (Petr Špaček)
- Going only downwards in the DNS hierarchy (draft rfc)

MaxFetch(1) on Normal Operation



MaxFetch(1), Amplification down 74➔3

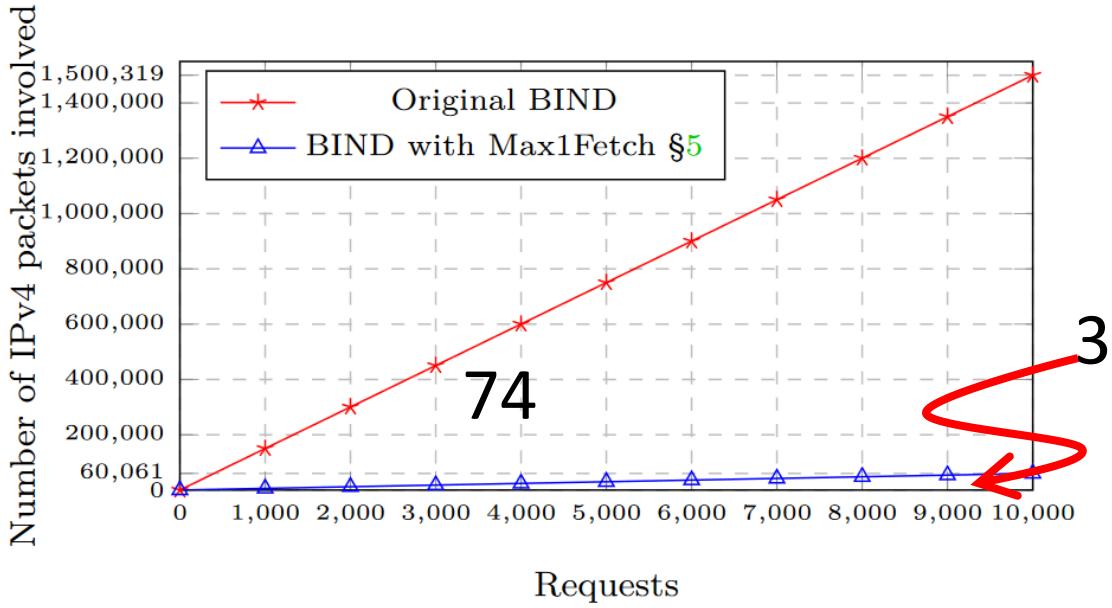
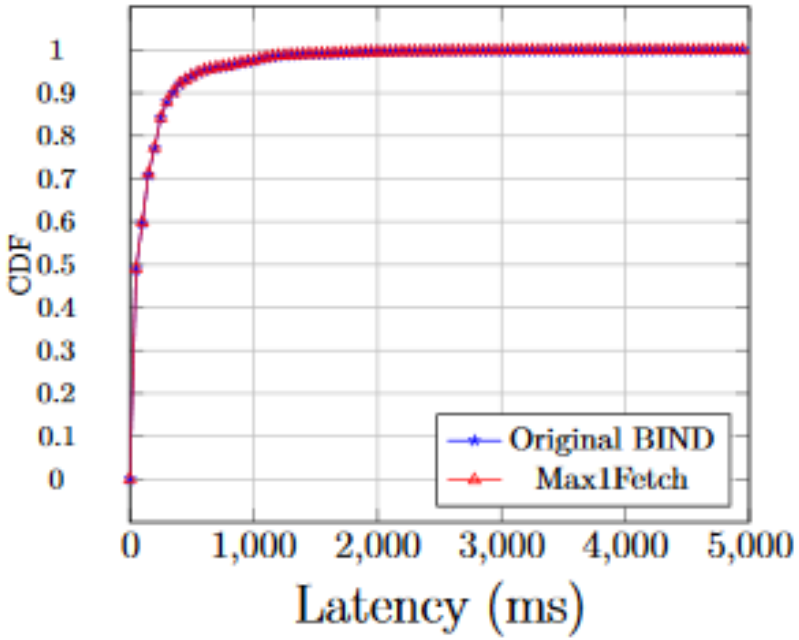


Figure 7: NXNSAttack long-lived simulation against an SLD authoritative server. A Constant PAF of 75x in the original BIND compared with PAF 3x of Max1Fetch (see §5). Recall that attacker cost is $2 \cdot$ #requests.

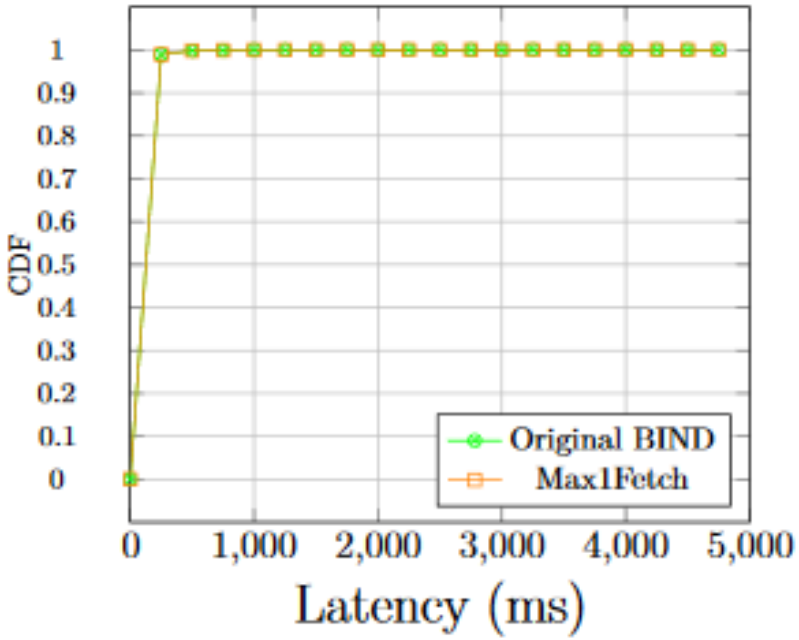
MaxFetch(1) no effect on latency

- No observed failures

- Latency slightly improved !!

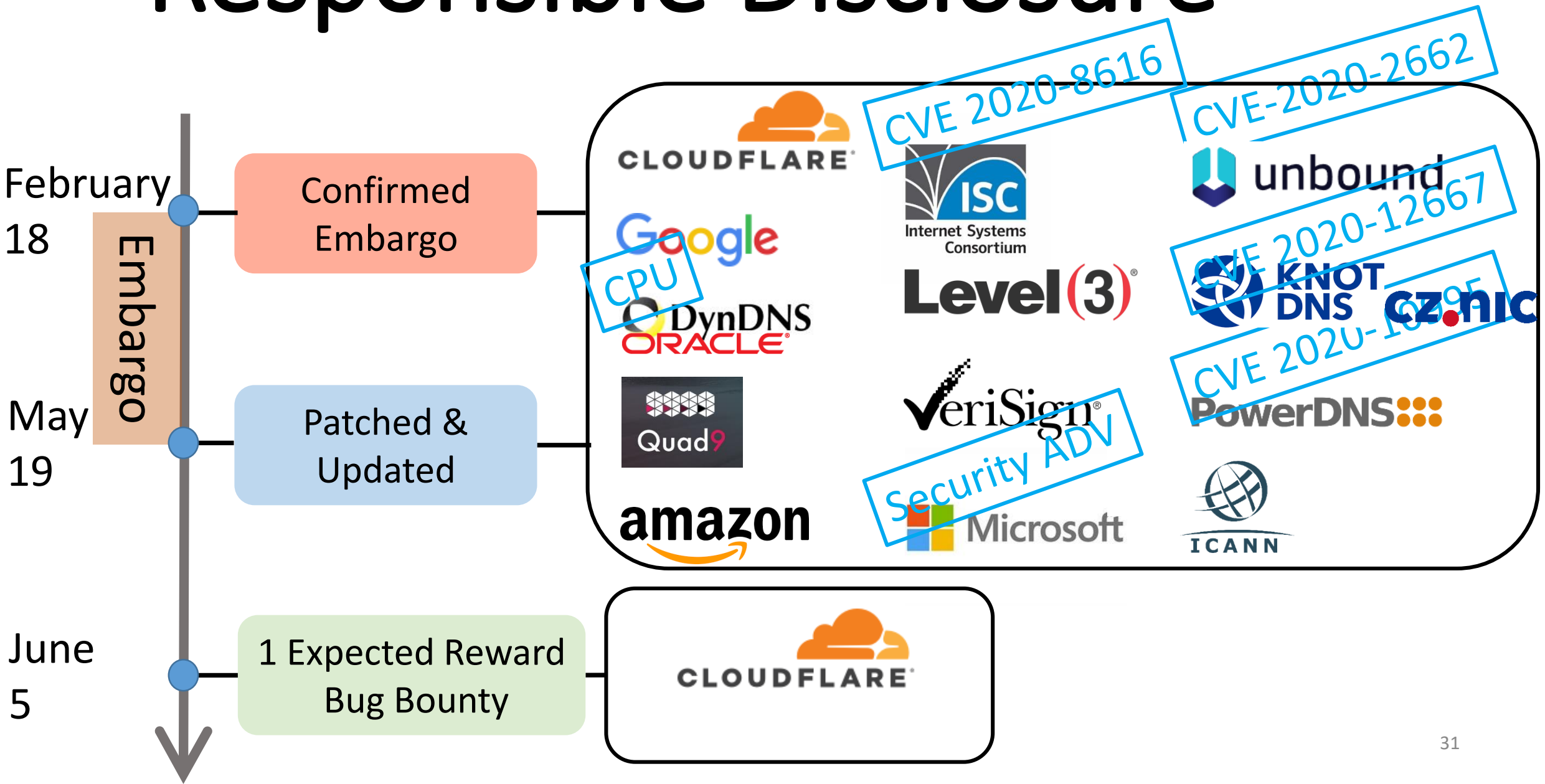


(a) 100K top domains



(b) Campus trace

Responsible Disclosure



Conclusions

- Mirai X 800 !!
- Worrisome, Fatal flaw
- Could there be another similar flaw?
- Formal/automatic verification methods
- Trade offs: Availability ←→Vulnerability

  Response time ←→Vulnerability
- Re-design

Thank you

http://cyber-security-group.cs.tau.ac.il/