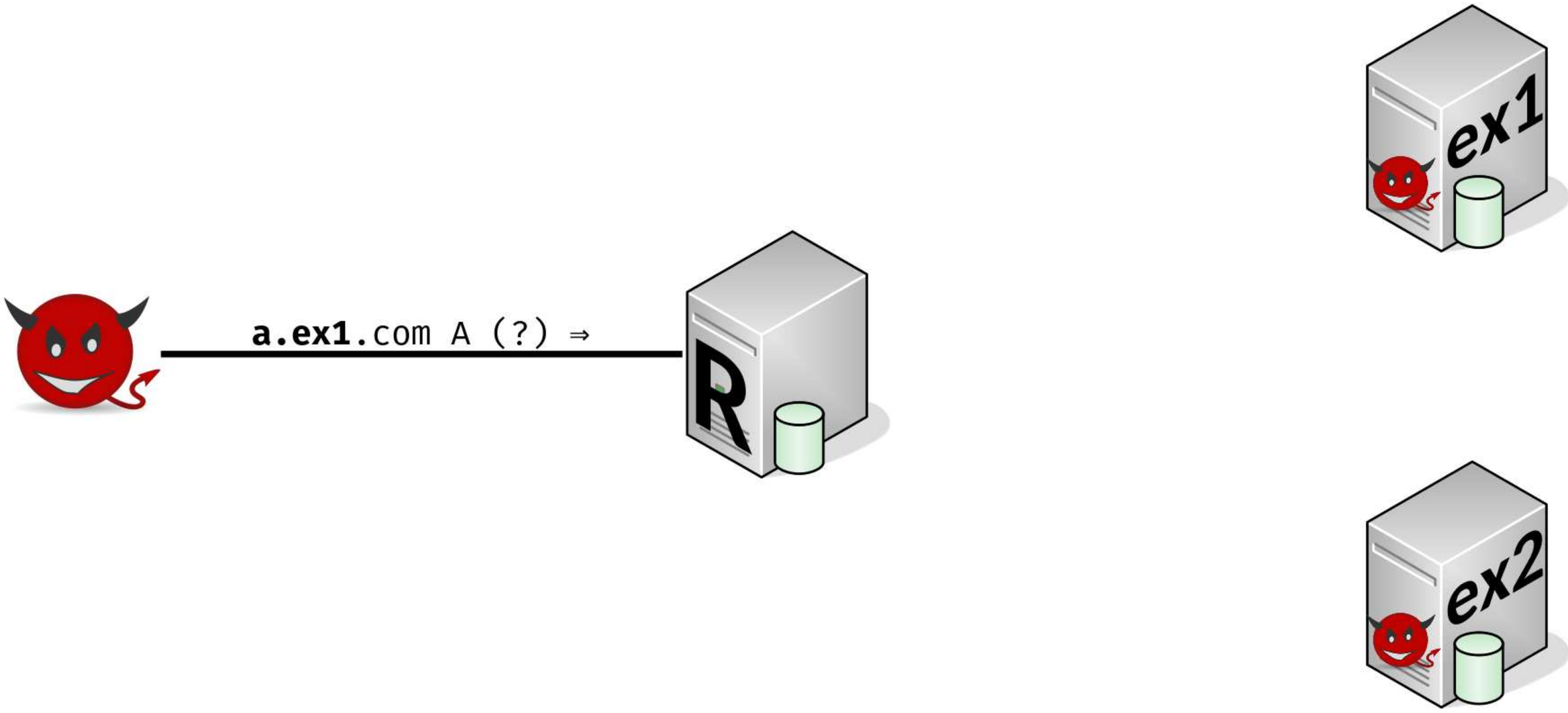
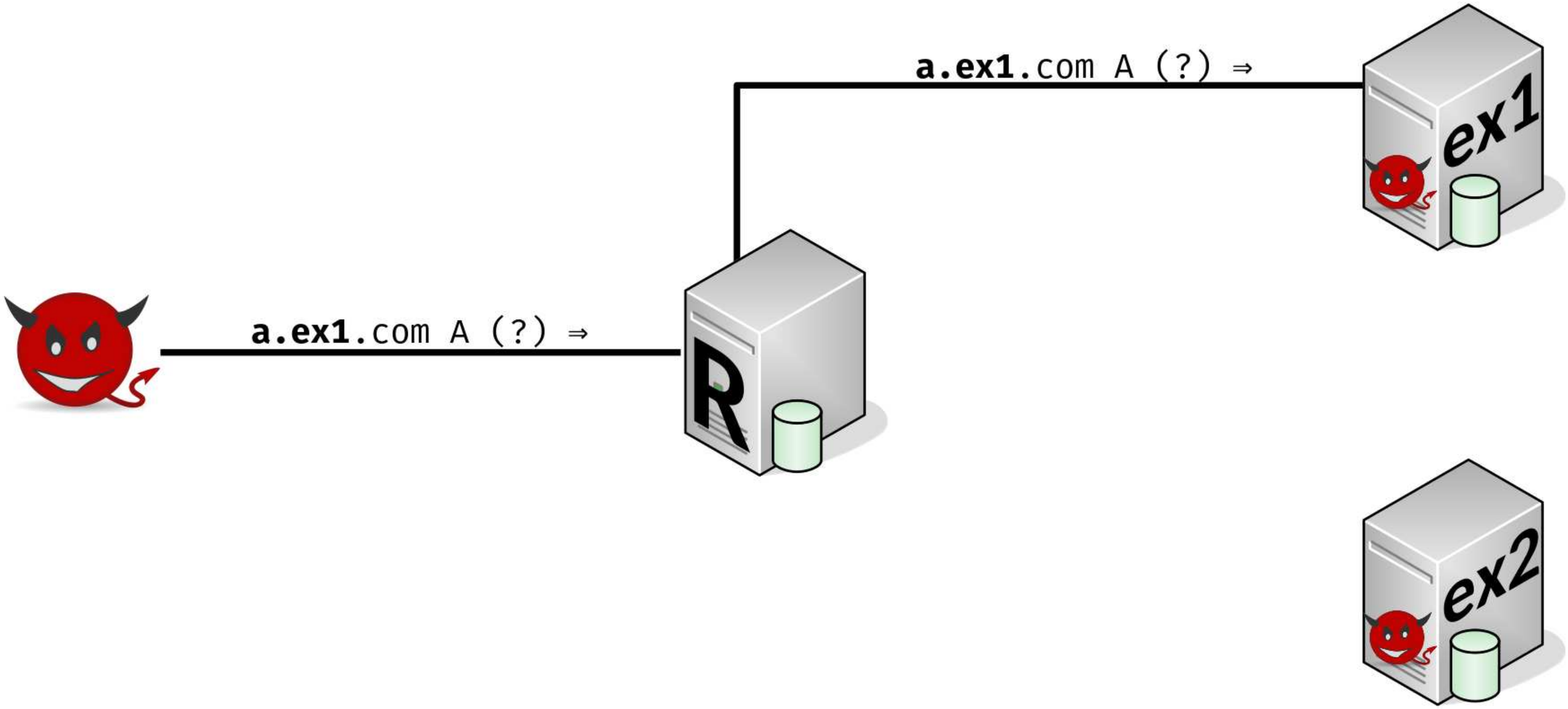
Optimizing Recurrent Pulsing Attacks using Application-Layer Amplification of Open DNS Resolvers

Jonas Bushart

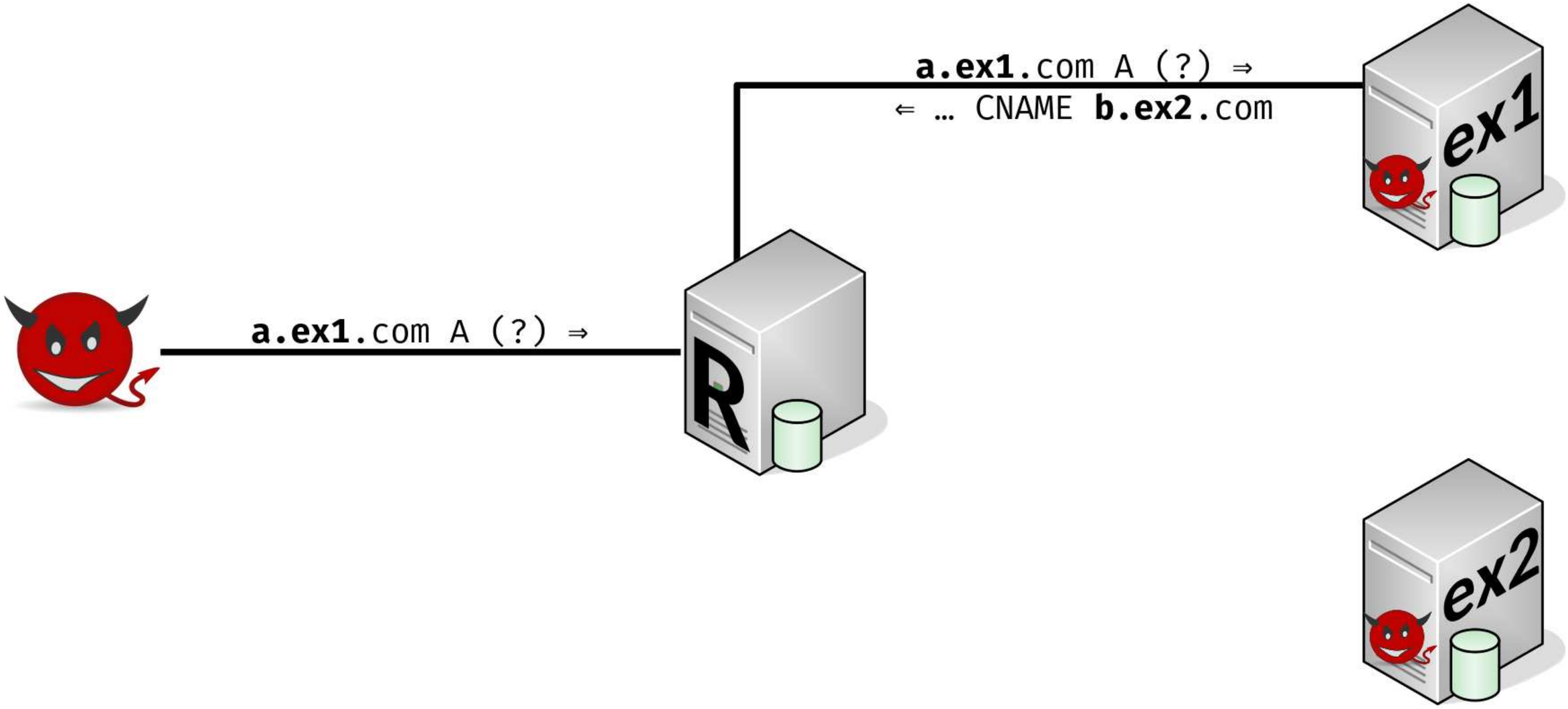
CNAME Chains



CNAME Chains

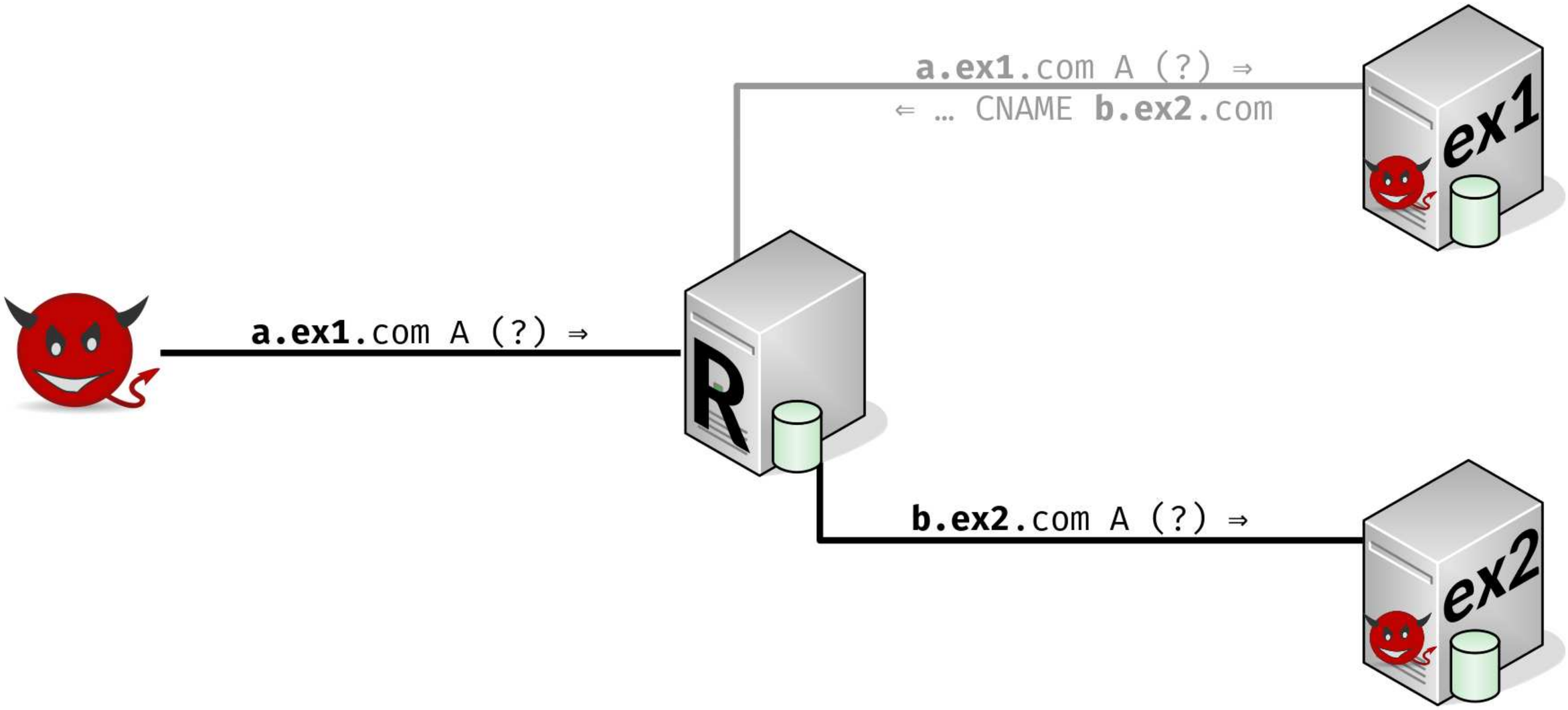


CNAME Chains



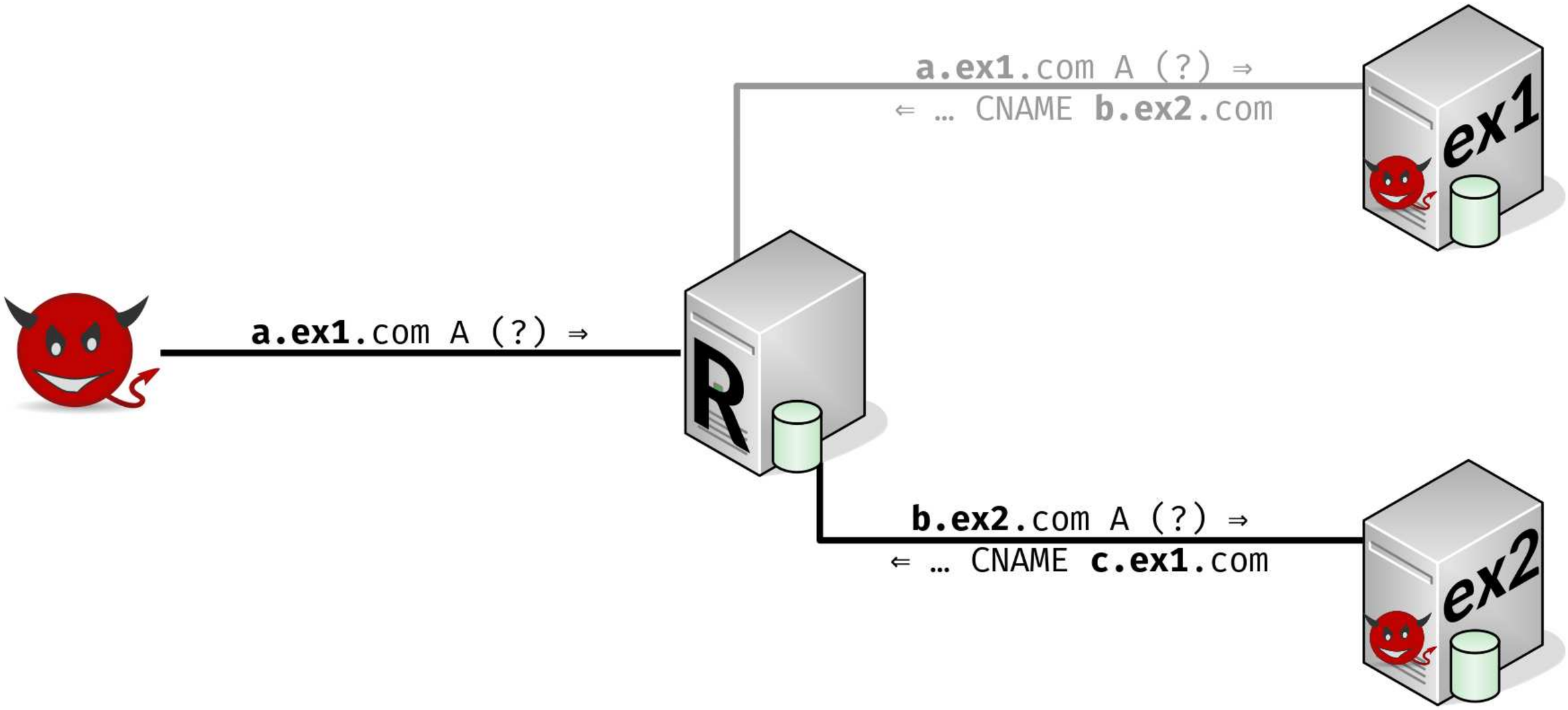
Bushart, J., and Rossow, C. DNS Unchained: Amplified Application-Layer DoS Attacks Against DNS Authoritatives. In *Proceedings of the 21th International Symposium on Research in Attacks, Intrusions and Defenses* (Sept. 2018).

CNAME Chains



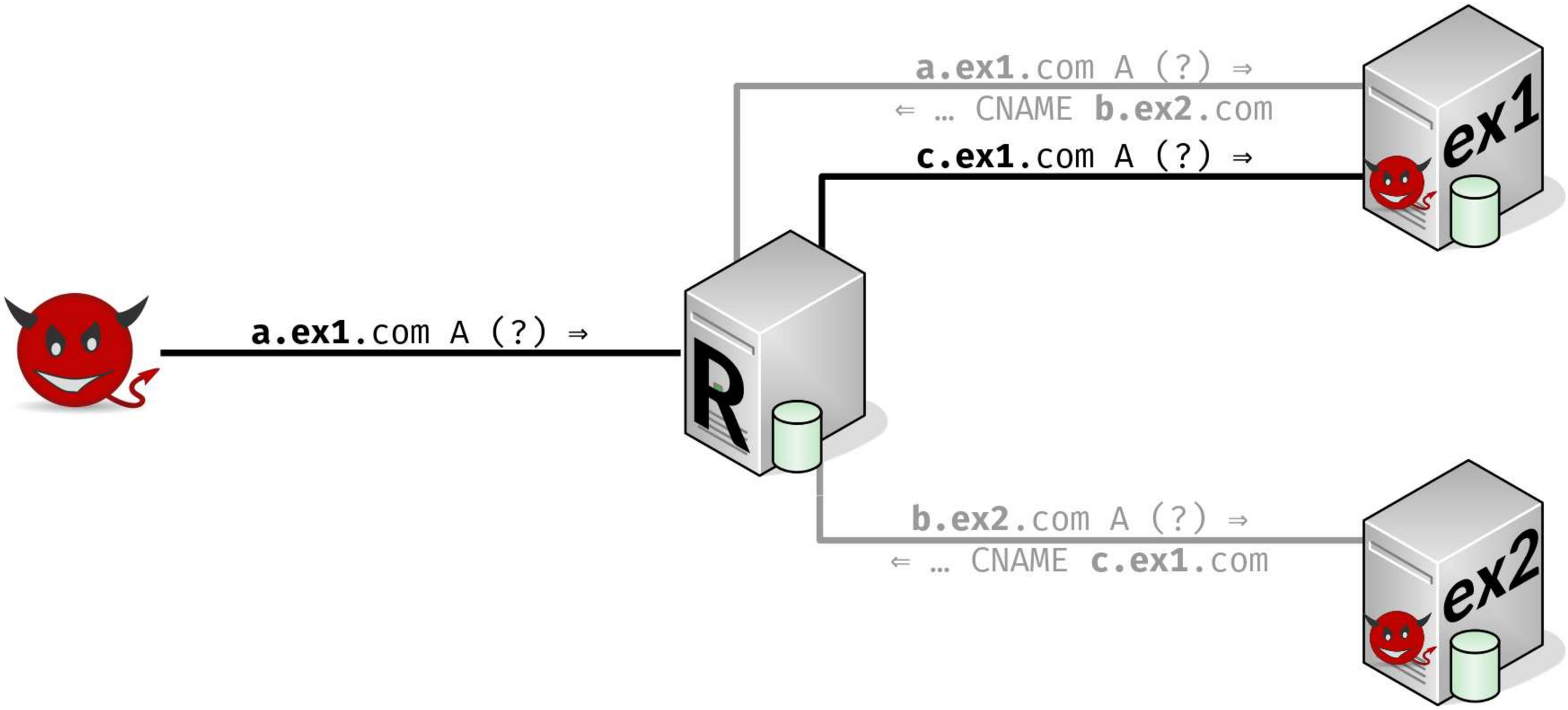
Bushart, J., and Rossow, C. DNS Unchained: Amplified Application-Layer DoS Attacks Against DNS Authoritatives. In *Proceedings of the 21th International Symposium on Research in Attacks, Intrusions and Defenses* (Sept. 2018).

CNAME Chains

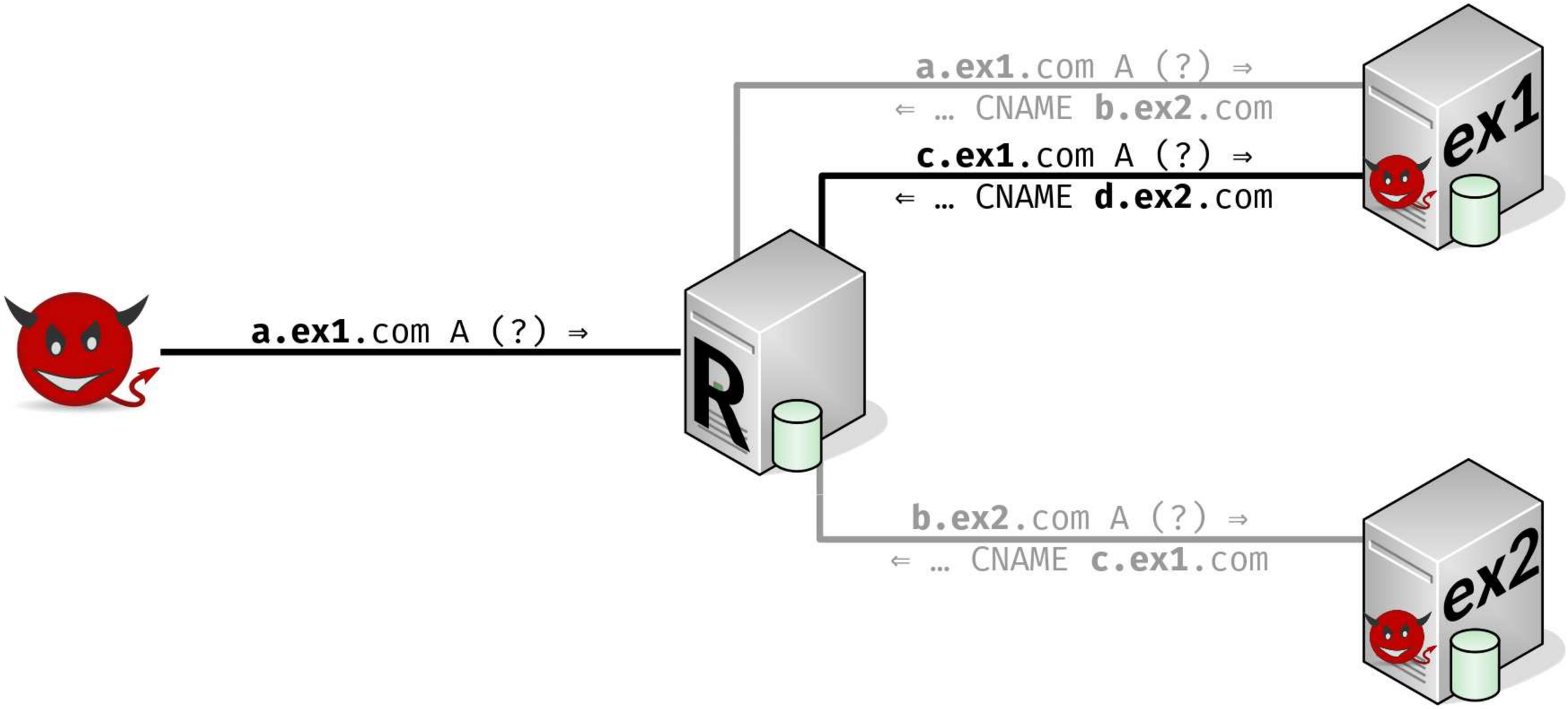


Bushart, J., and Rossow, C. DNS Unchained: Amplified Application-Layer DoS Attacks Against DNS Authoritatives. In *Proceedings of the 21th International Symposium on Research in Attacks, Intrusions and Defenses* (Sept. 2018).

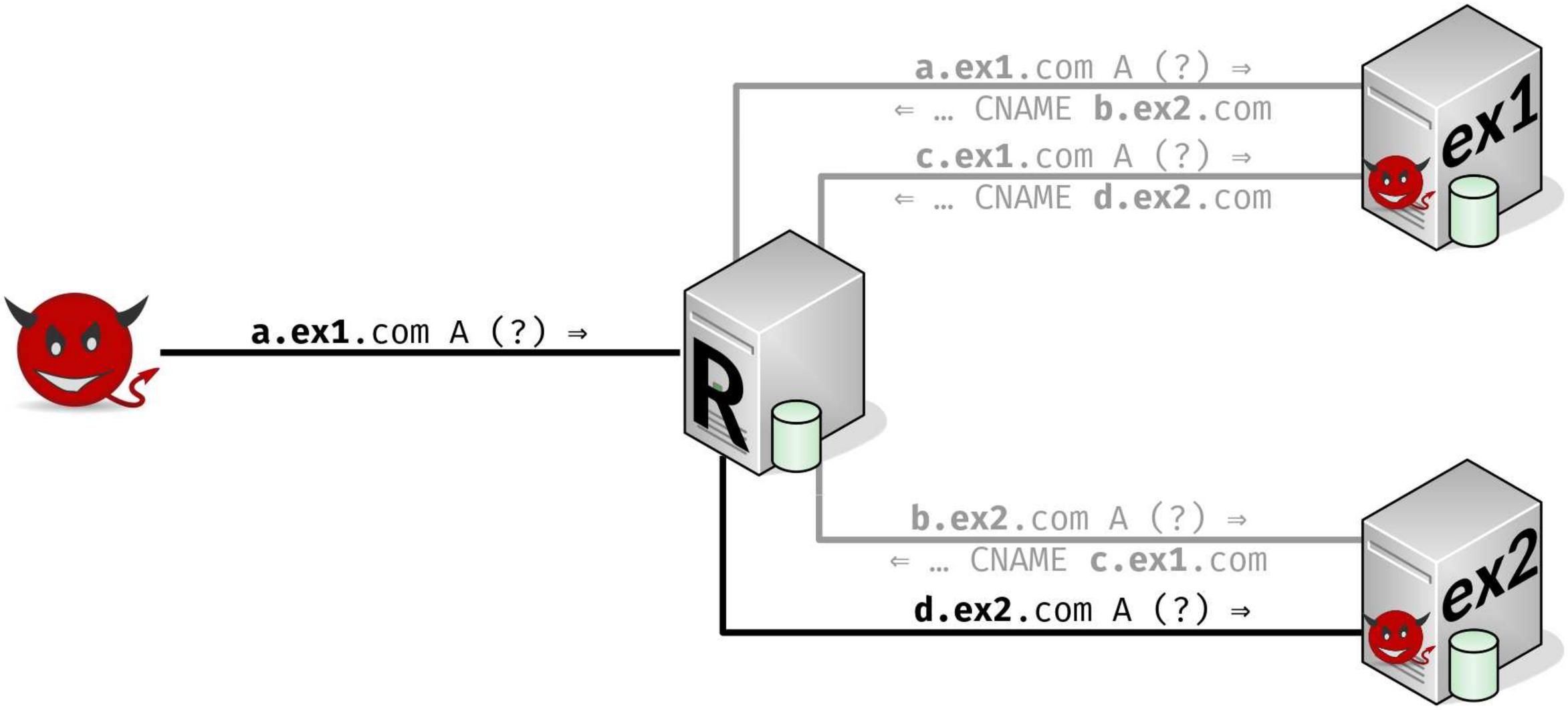
CNAME Chains



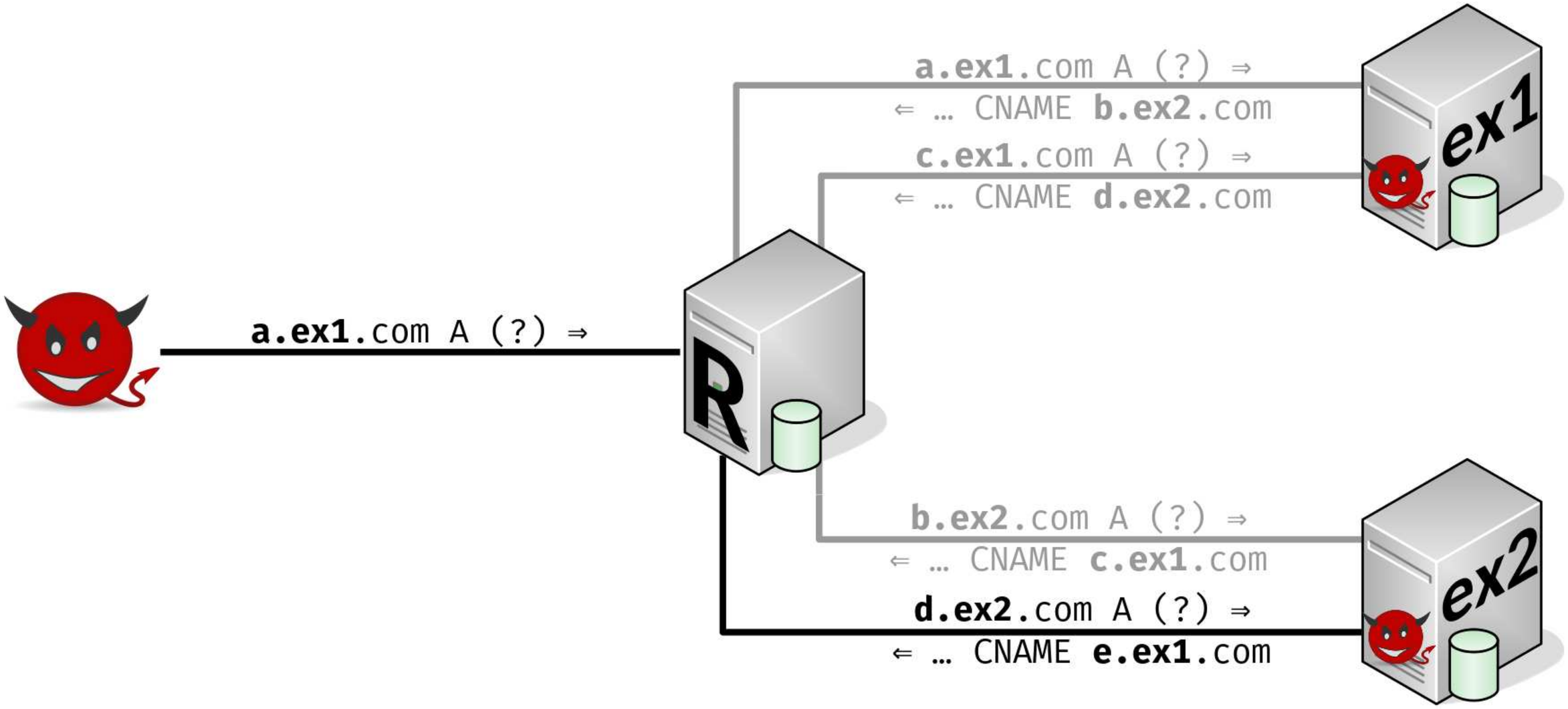
CNAME Chains



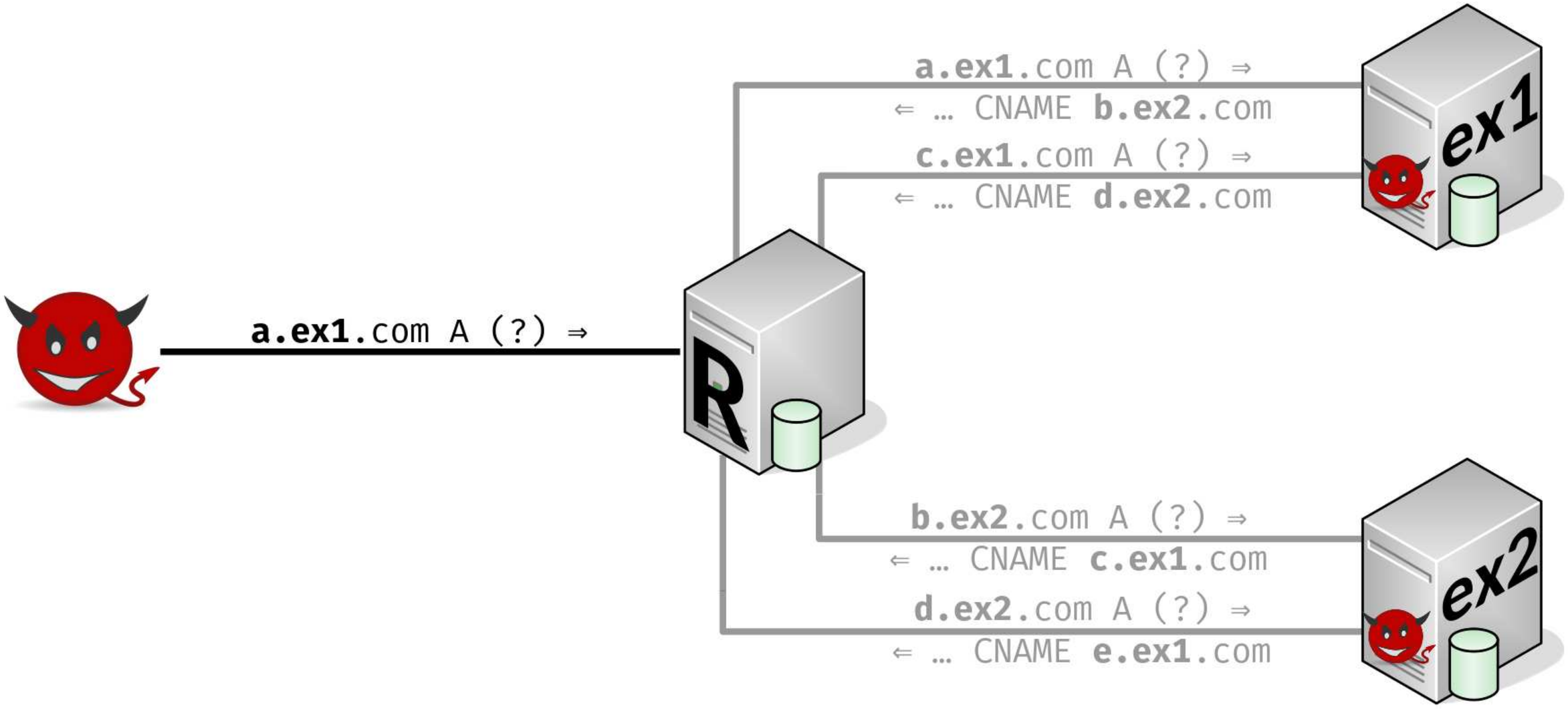
CNAME Chains



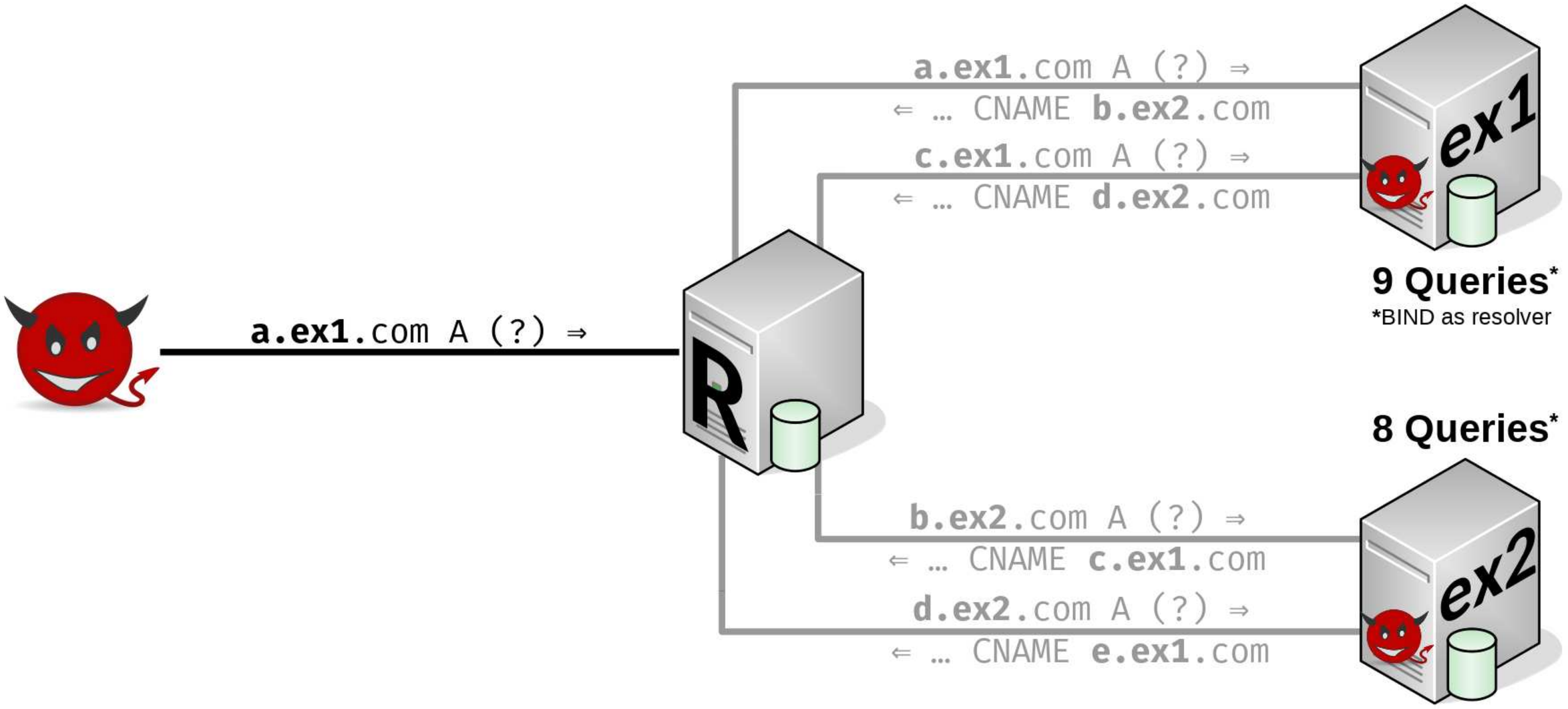
CNAME Chains



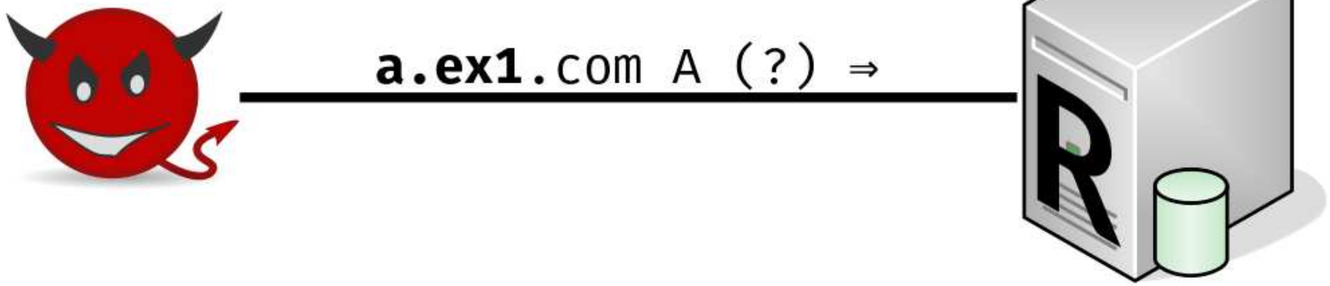
CNAME Chains



CNAME Chains



CNAME Chains – Caching

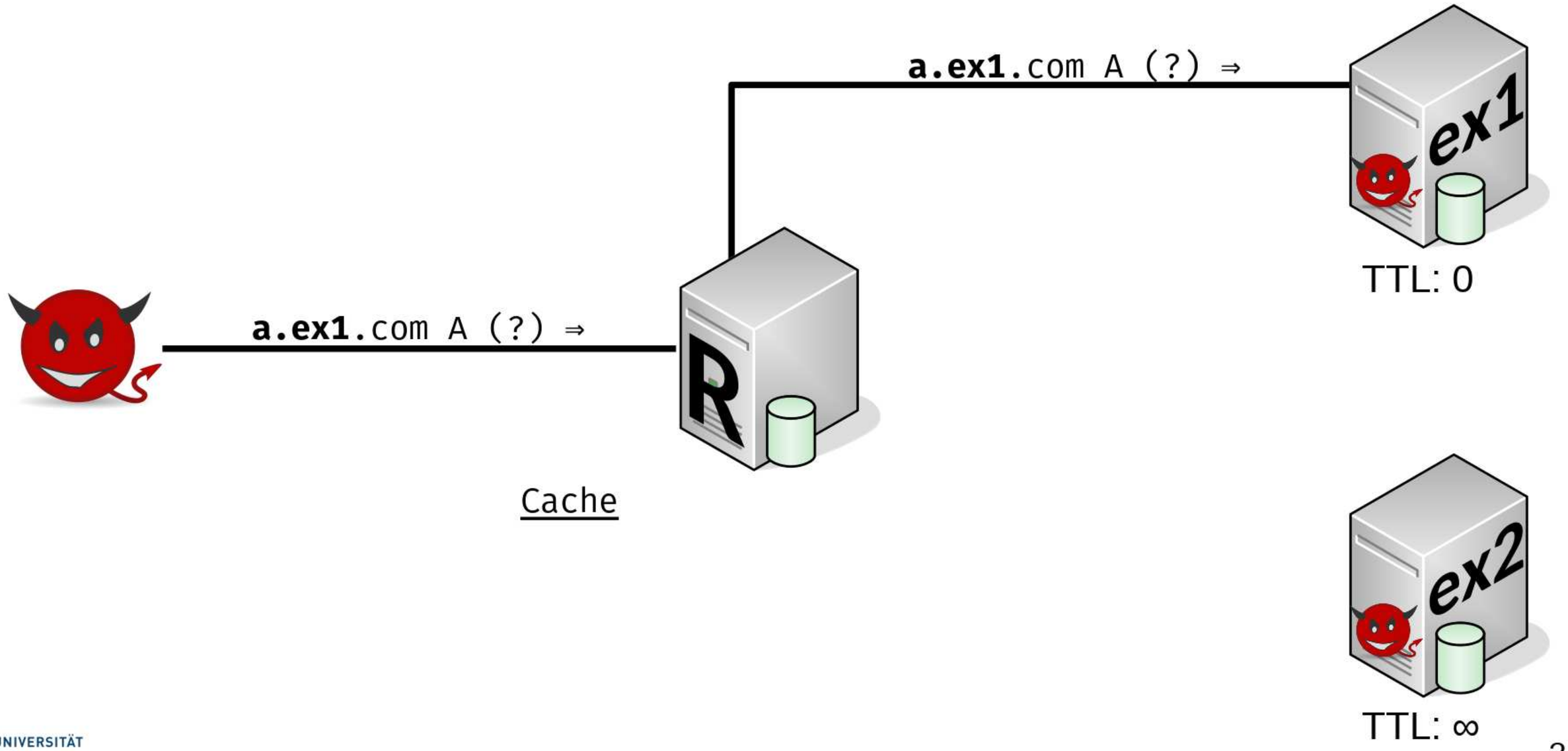


Cache

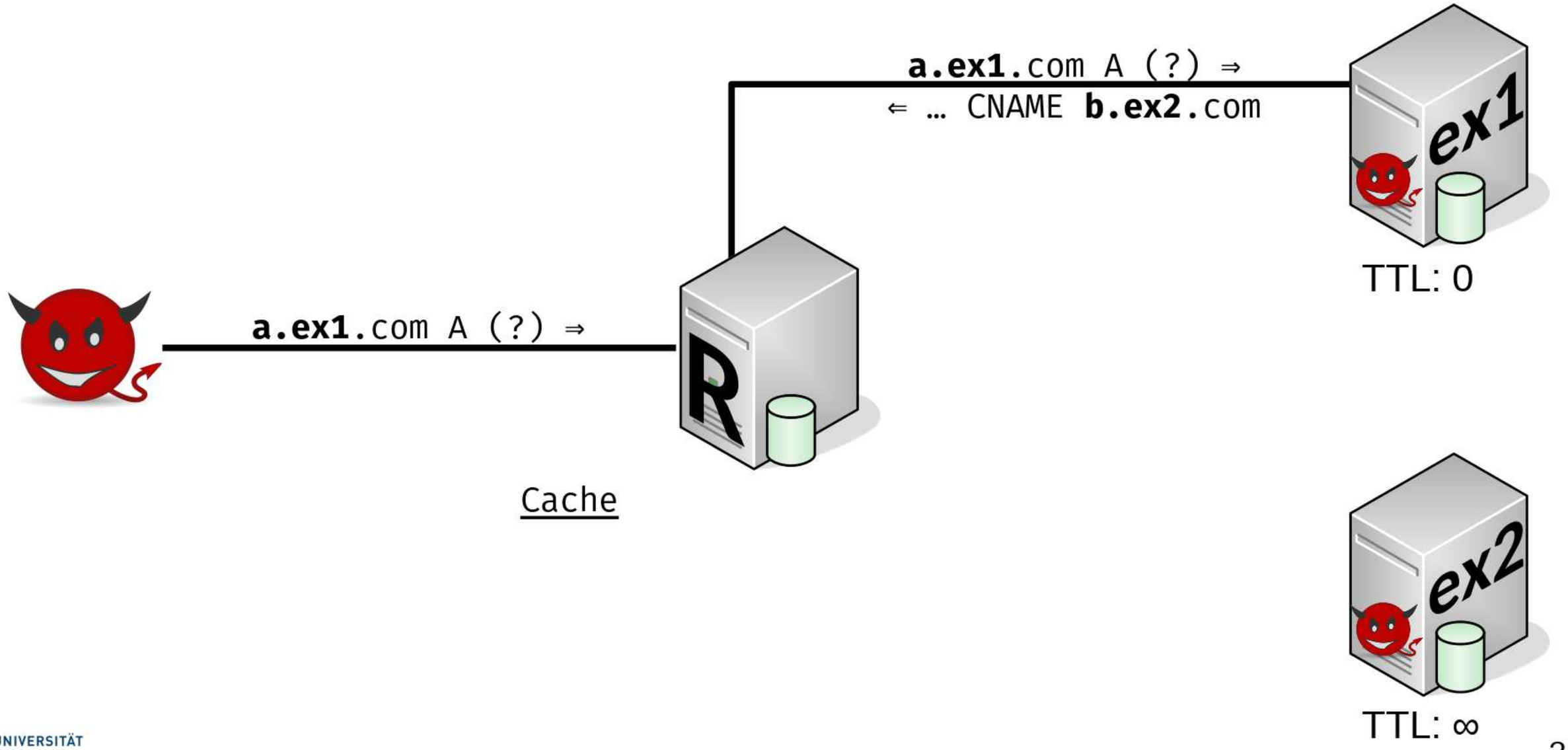
TTL: 0

TTL: ∞

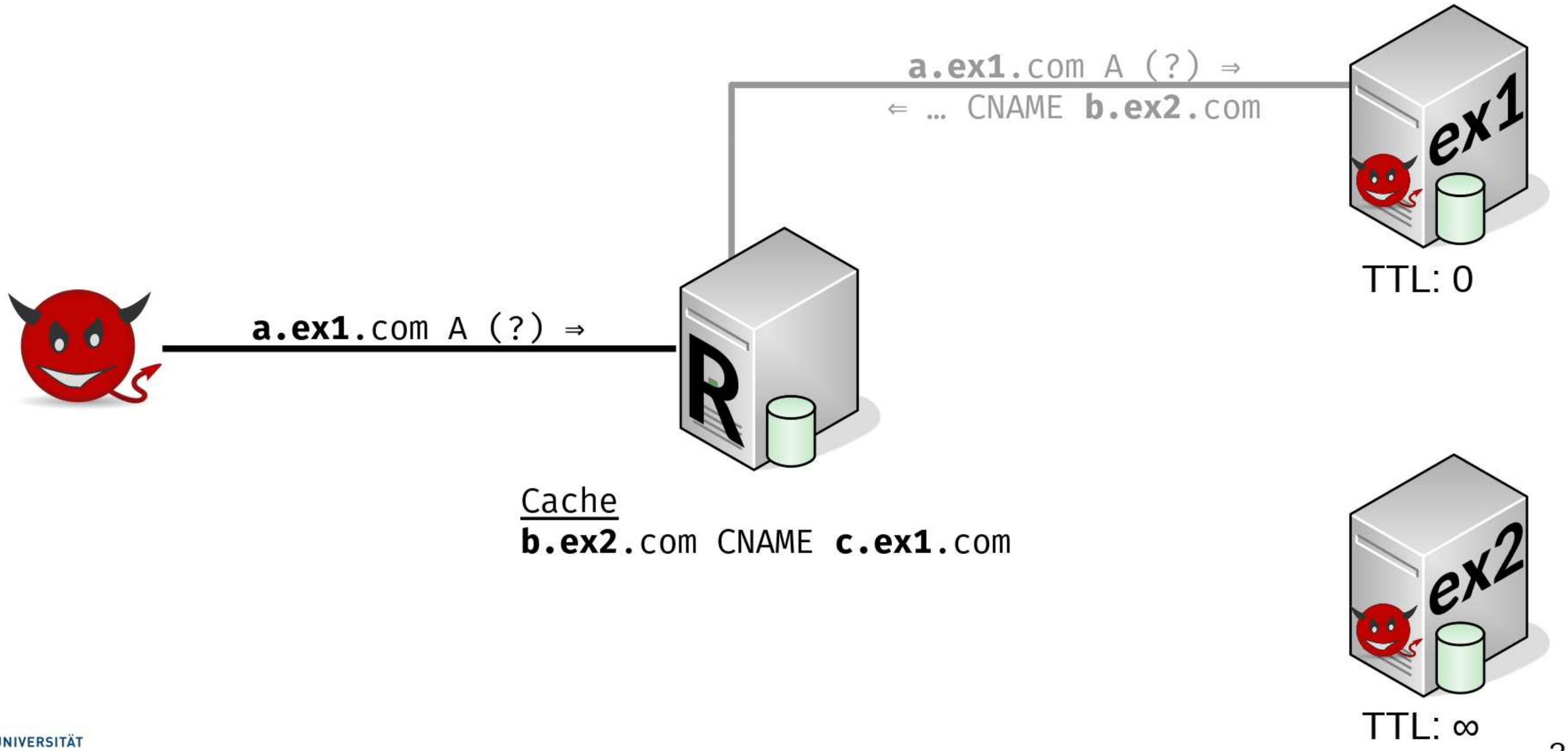
CNAME Chains – Caching



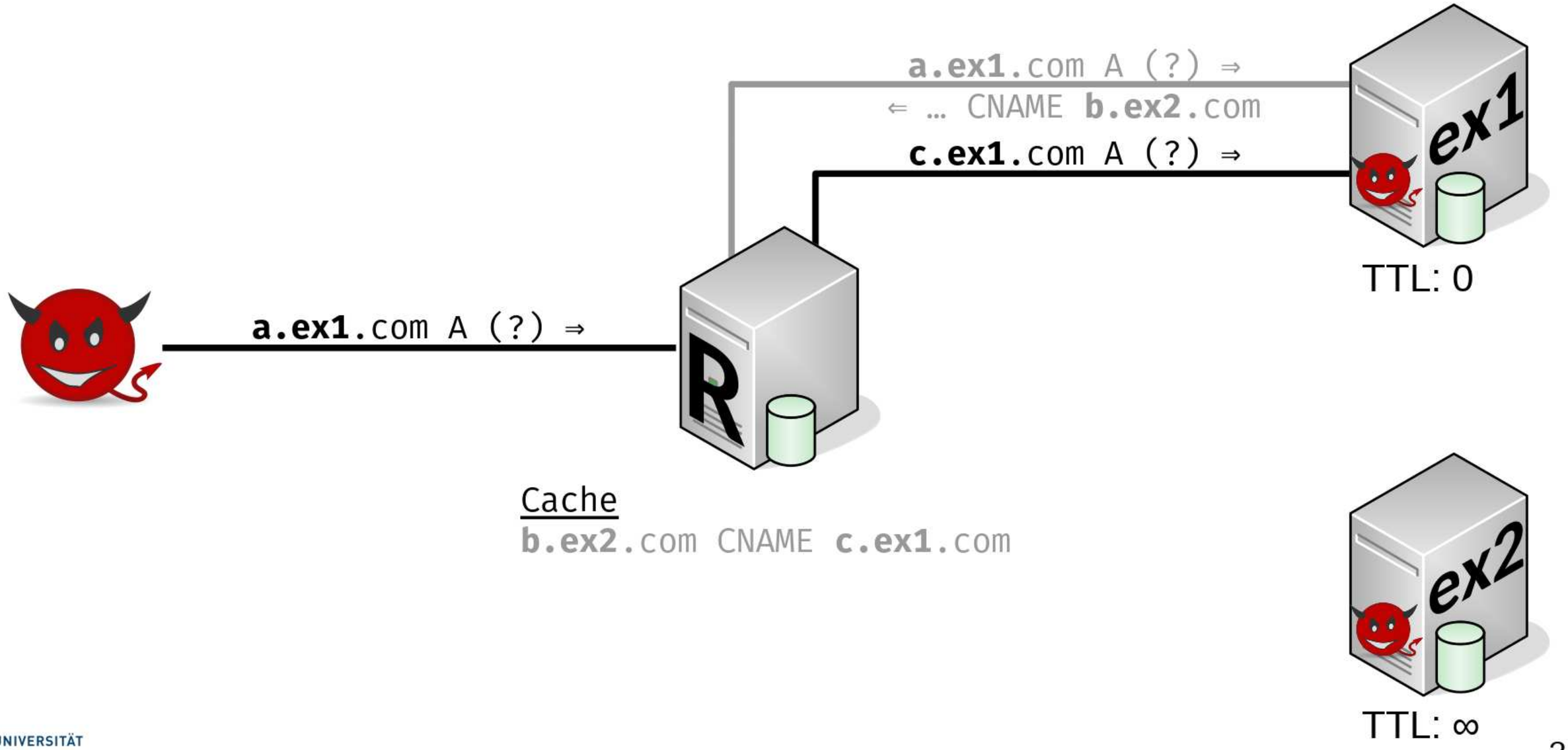
CNAME Chains – Caching



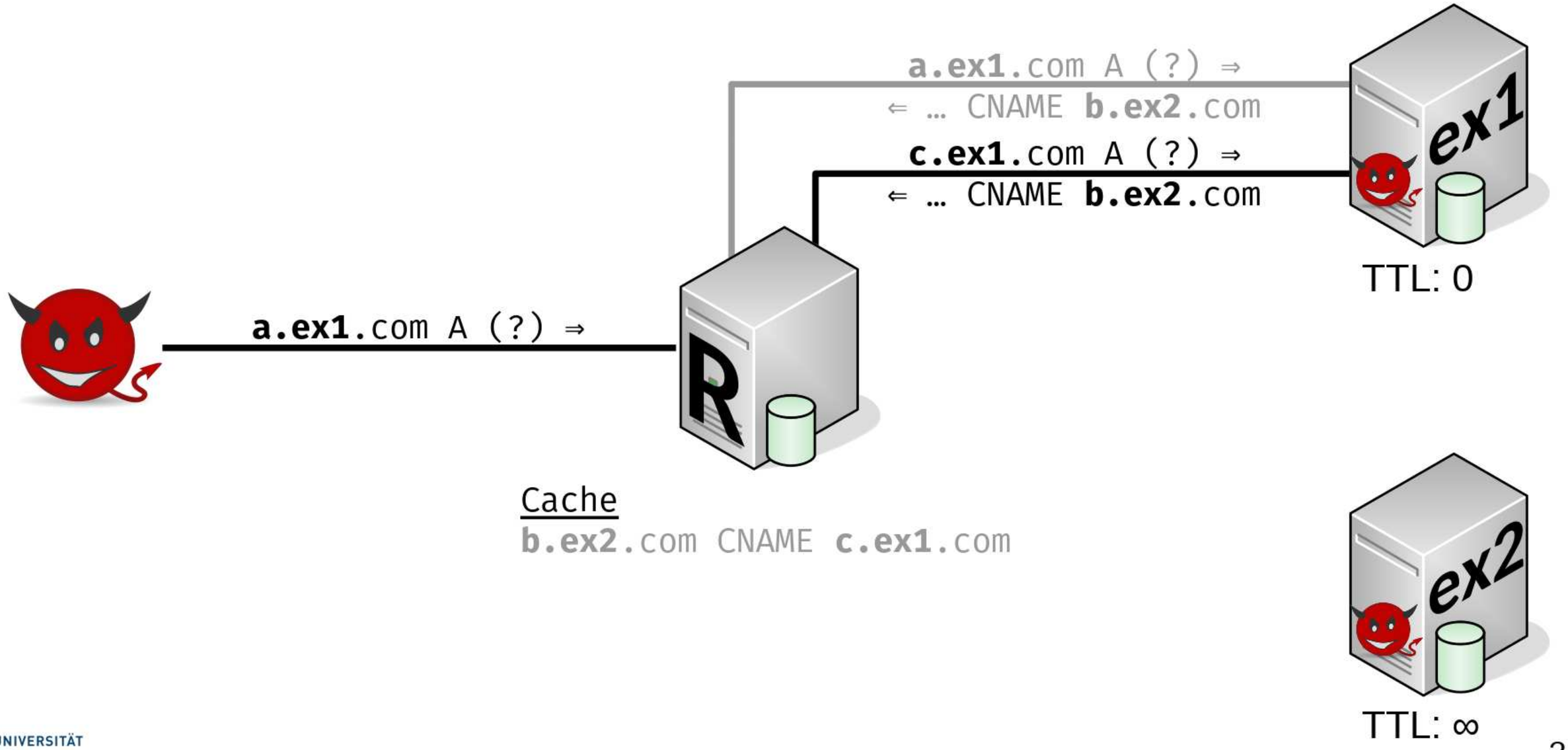
CNAME Chains – Caching



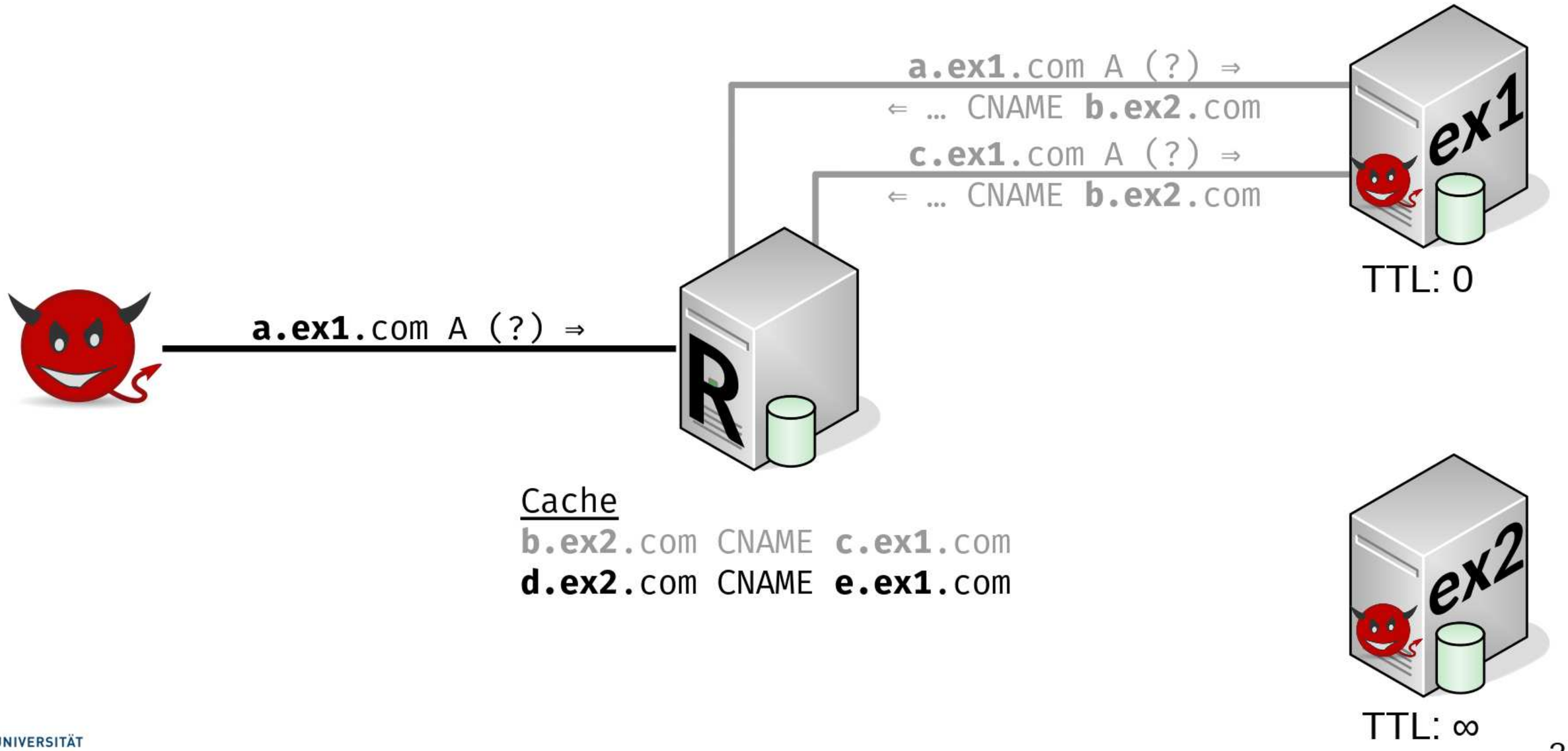
CNAME Chains – Caching



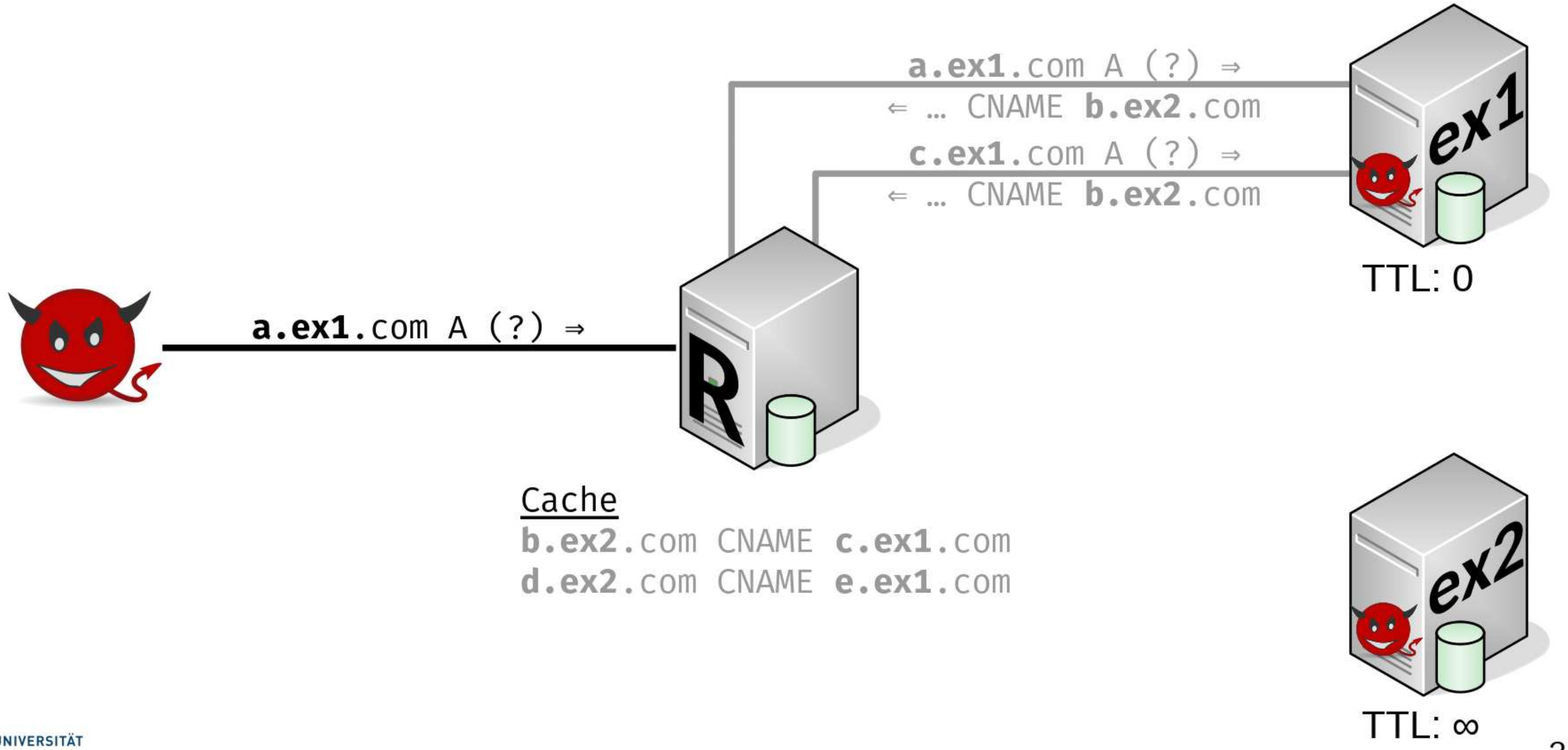
CNAME Chains – Caching



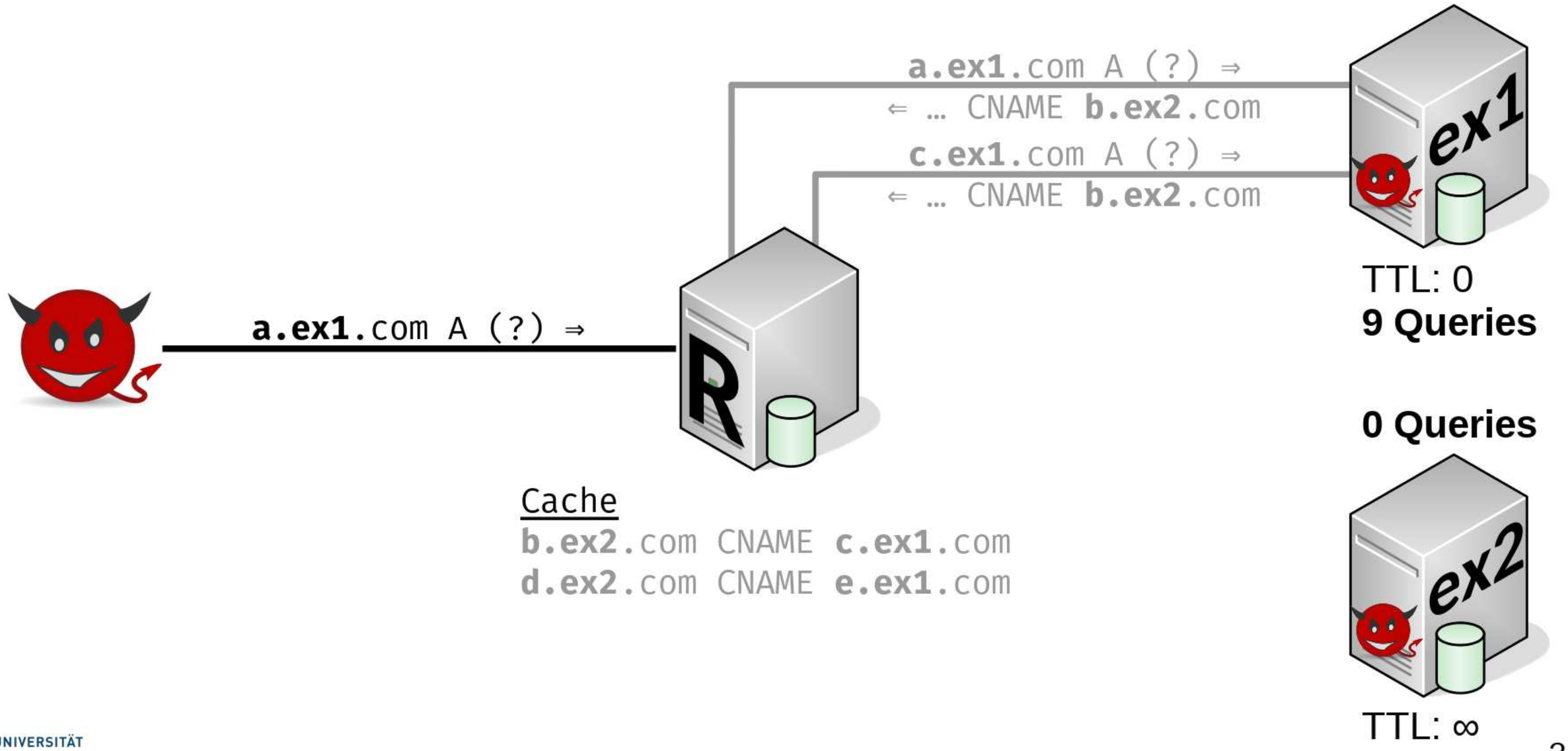
CNAME Chains – Caching



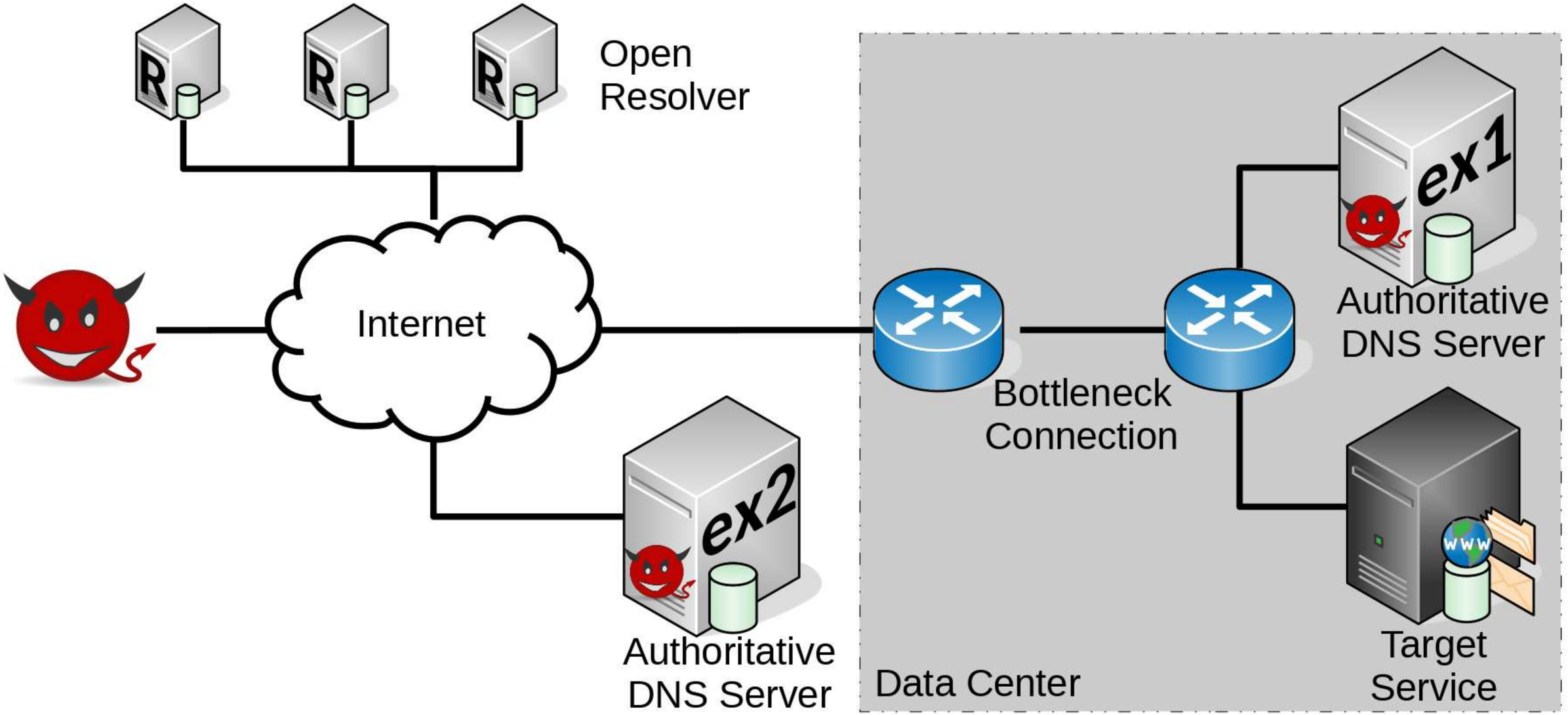
CNAME Chains – Caching



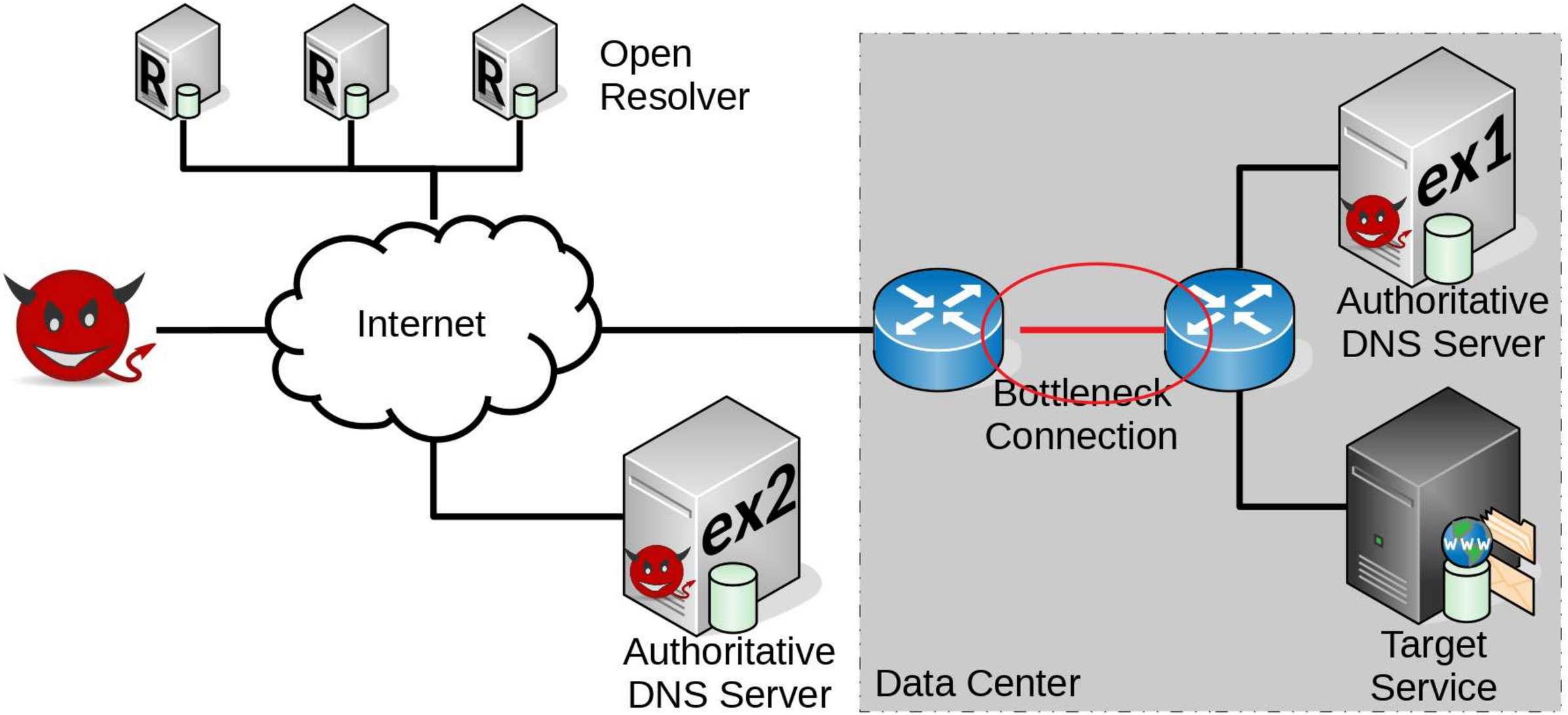
CNAME Chains – Caching



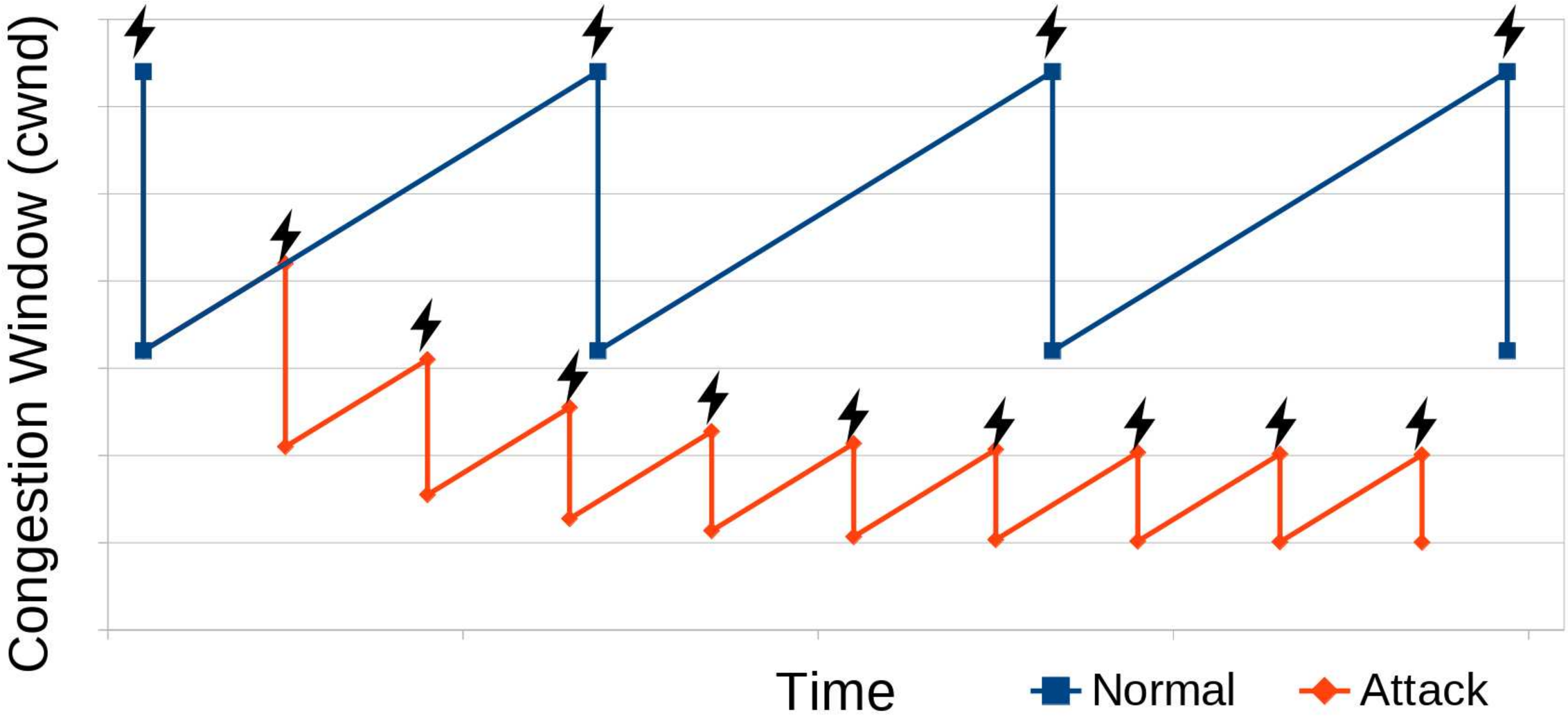
Overview


R
R
R
Open
Resolver
Internet
ex1
Authoritative
DNS Server
Bottleneck
Connection
ex2
Authoritative
DNS Server
Target
Service
Data Center

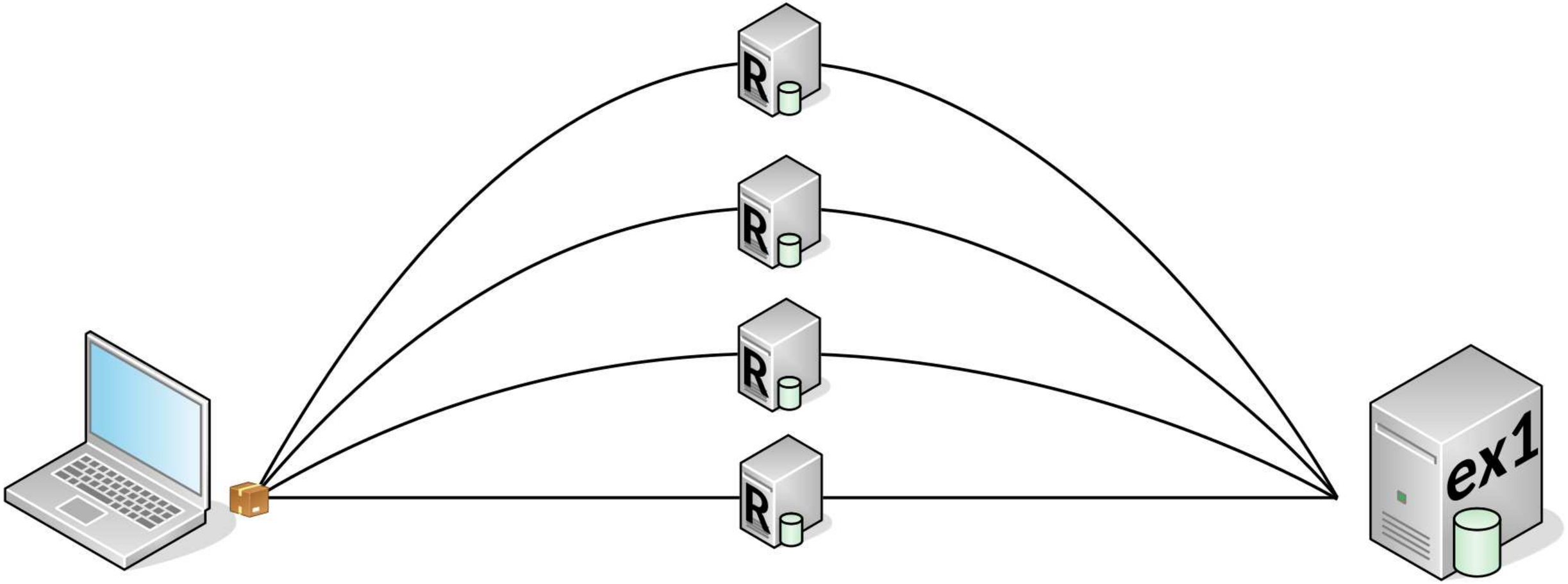
Overview


R
R
R
Open
Resolver
Internet
ex1
Authoritative
DNS Server
Bottleneck
Connection
ex2
Authoritative
DNS Server
Target
Service
Data Center

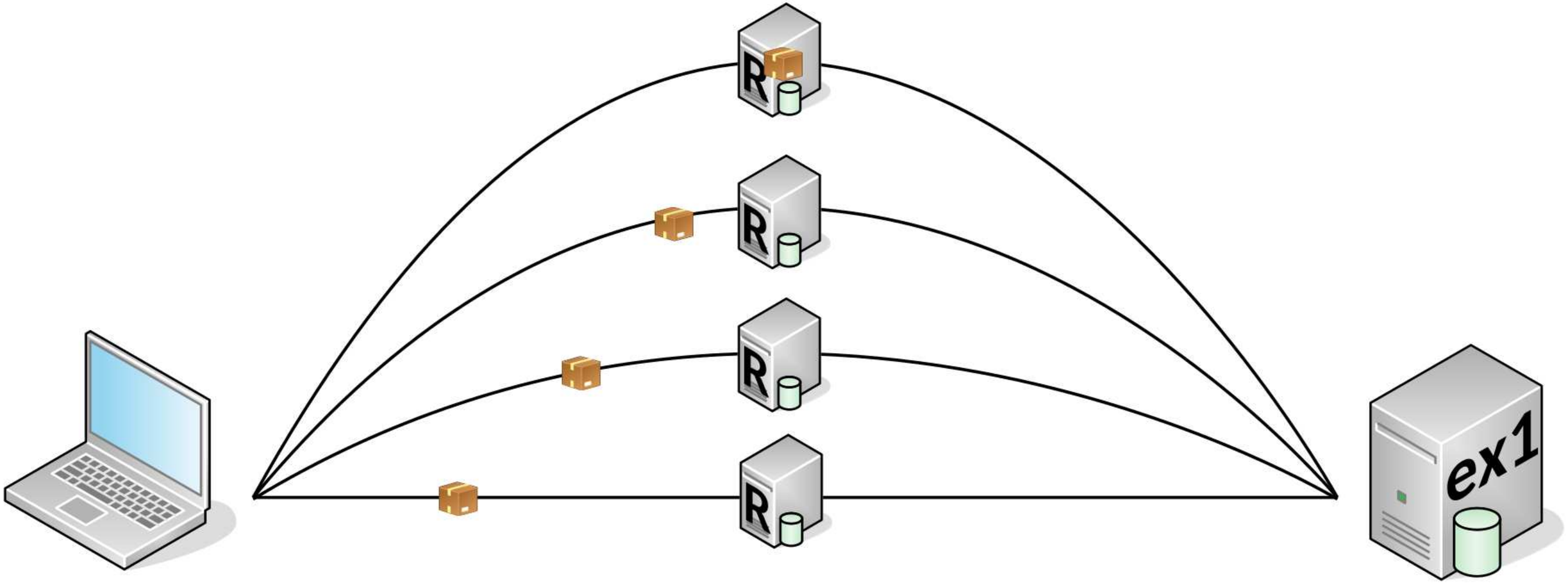
TCP – Reaction to Packet Loss (⚡)



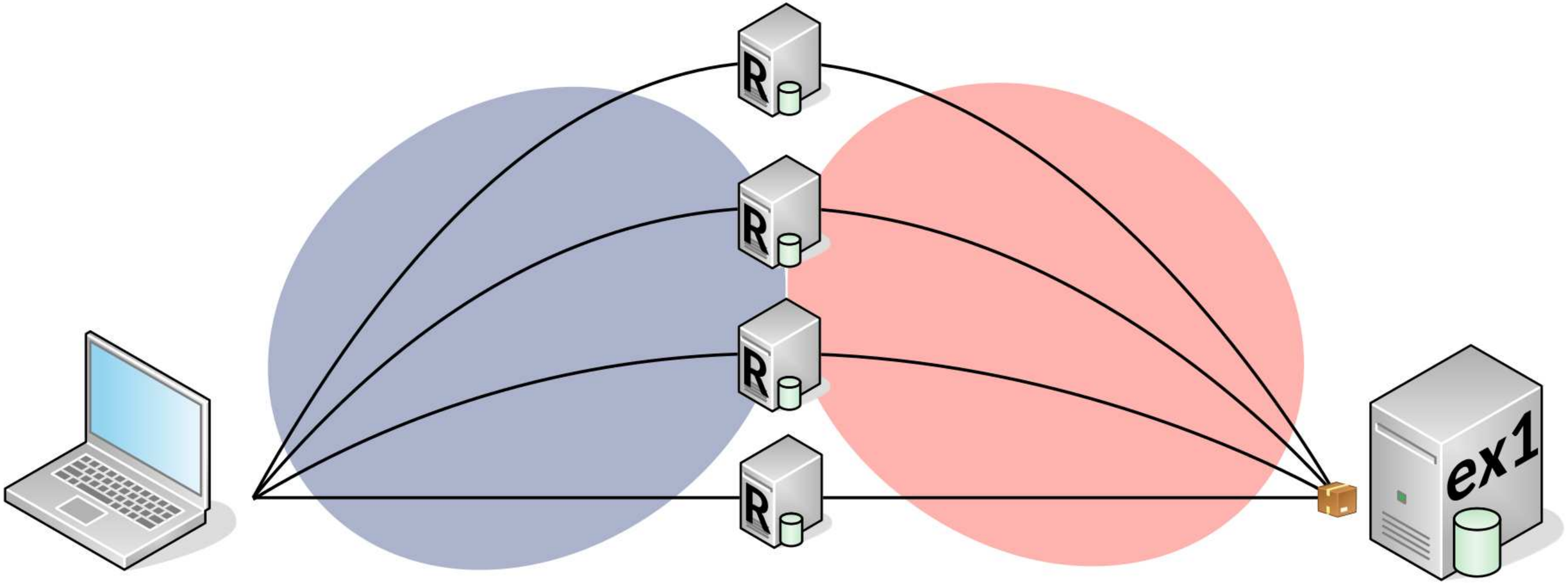
Temporal Lensing



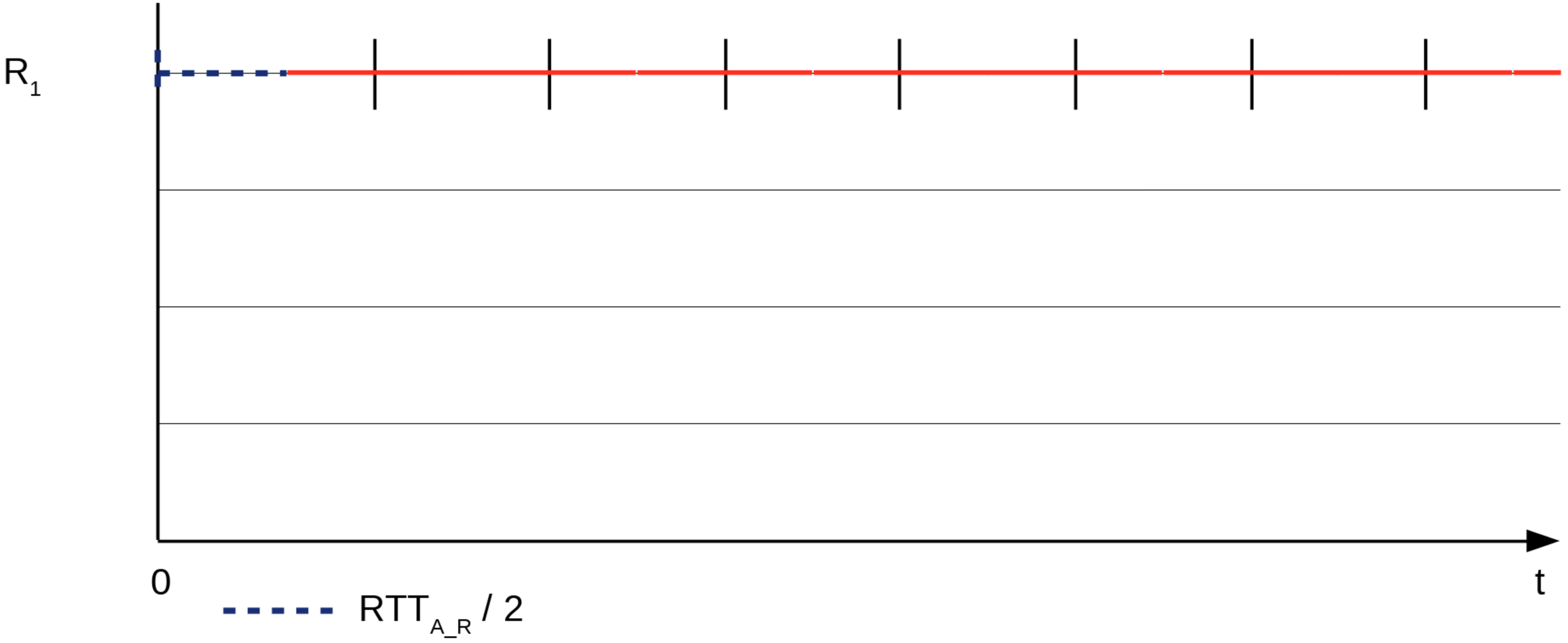
Temporal Lensing



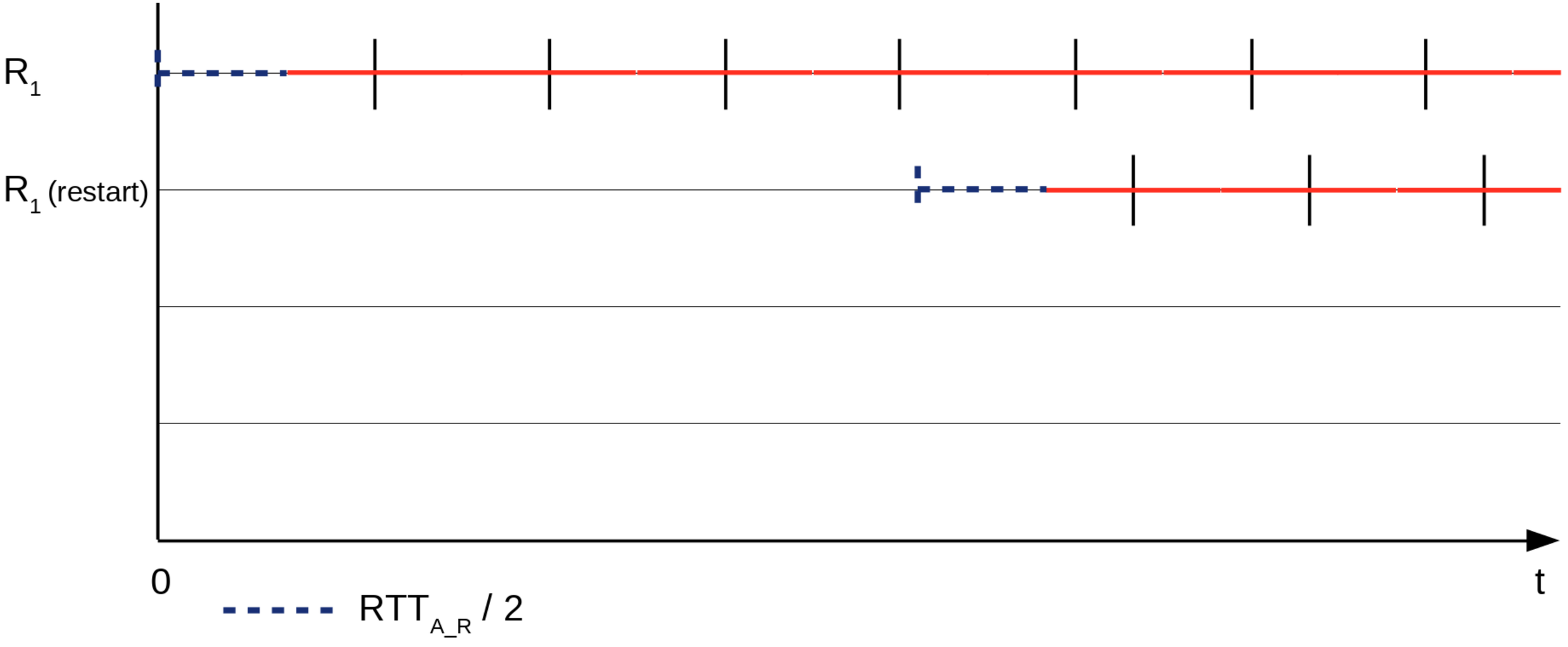
Temporal Lensing



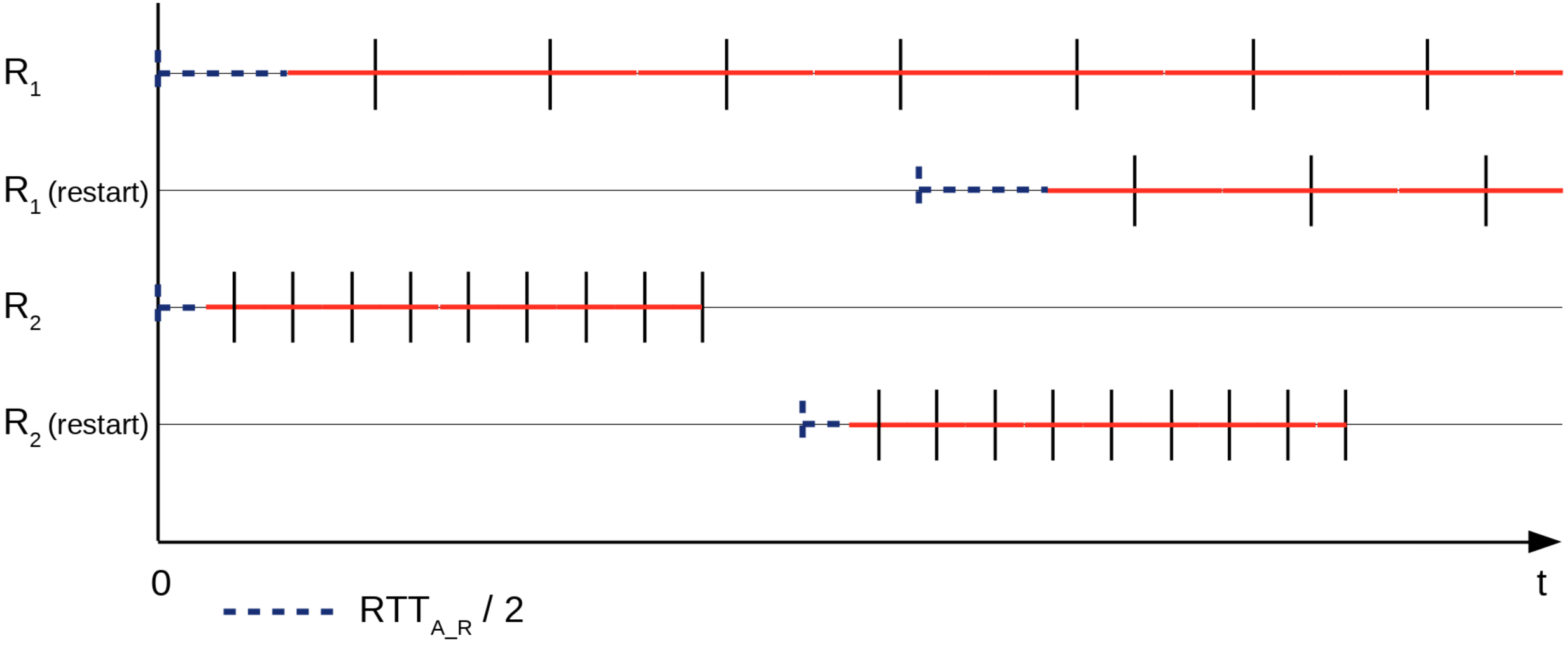
How to Pulse – Aligning Chains (1)



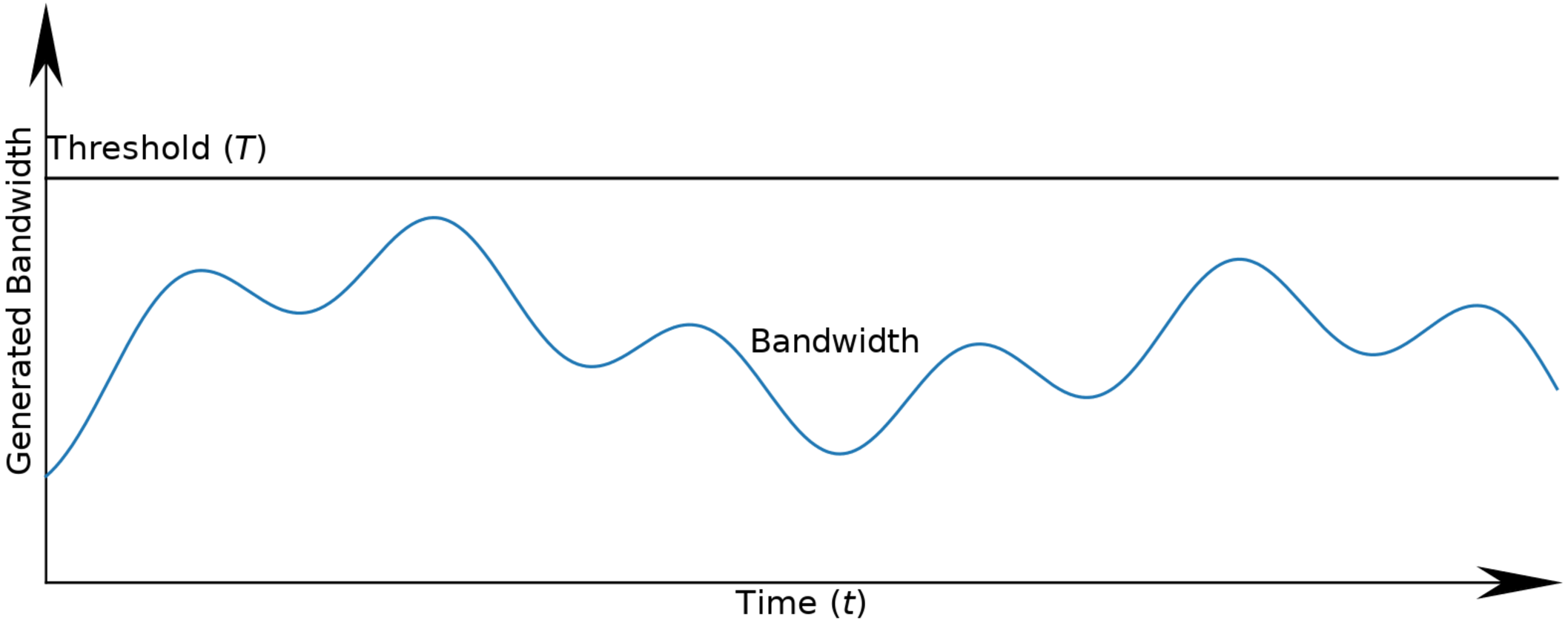
How to Pulse – Aligning Chains (1)



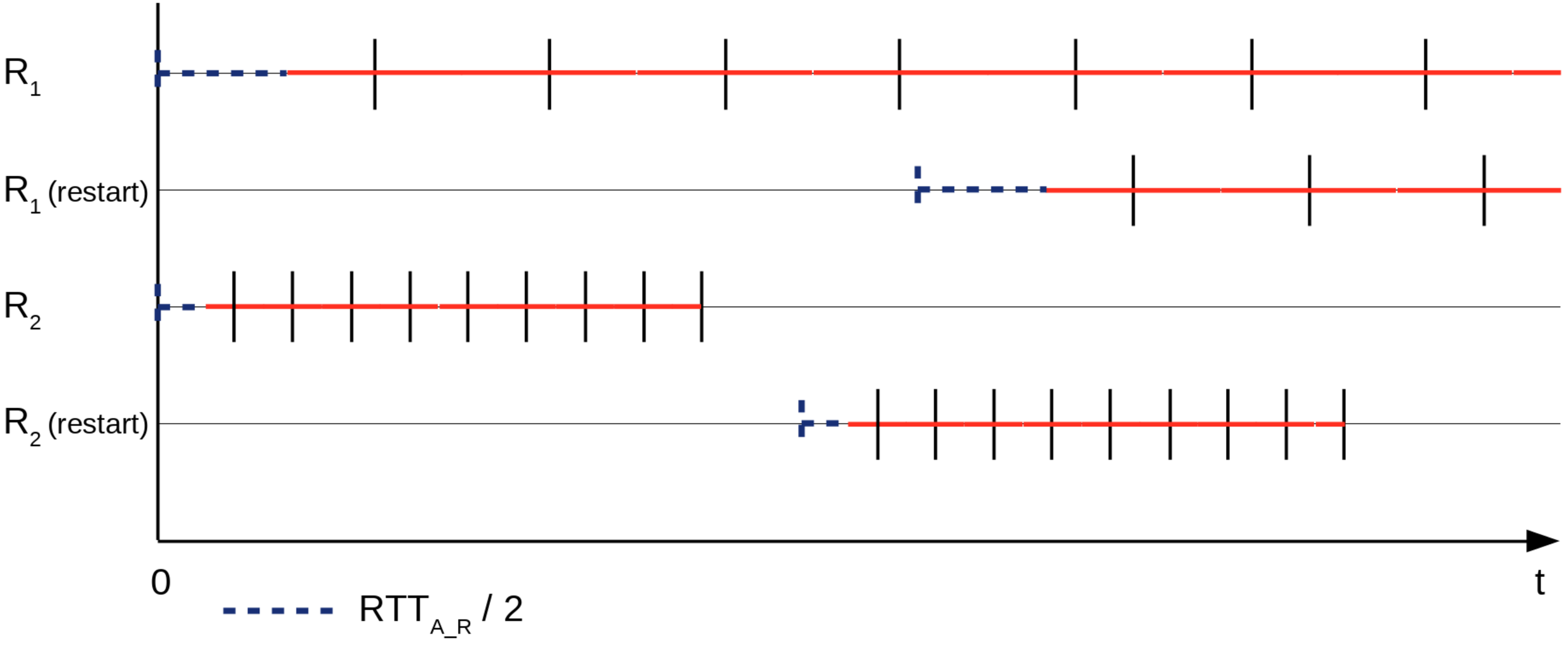
How to Pulse – Aligning Chains (1)



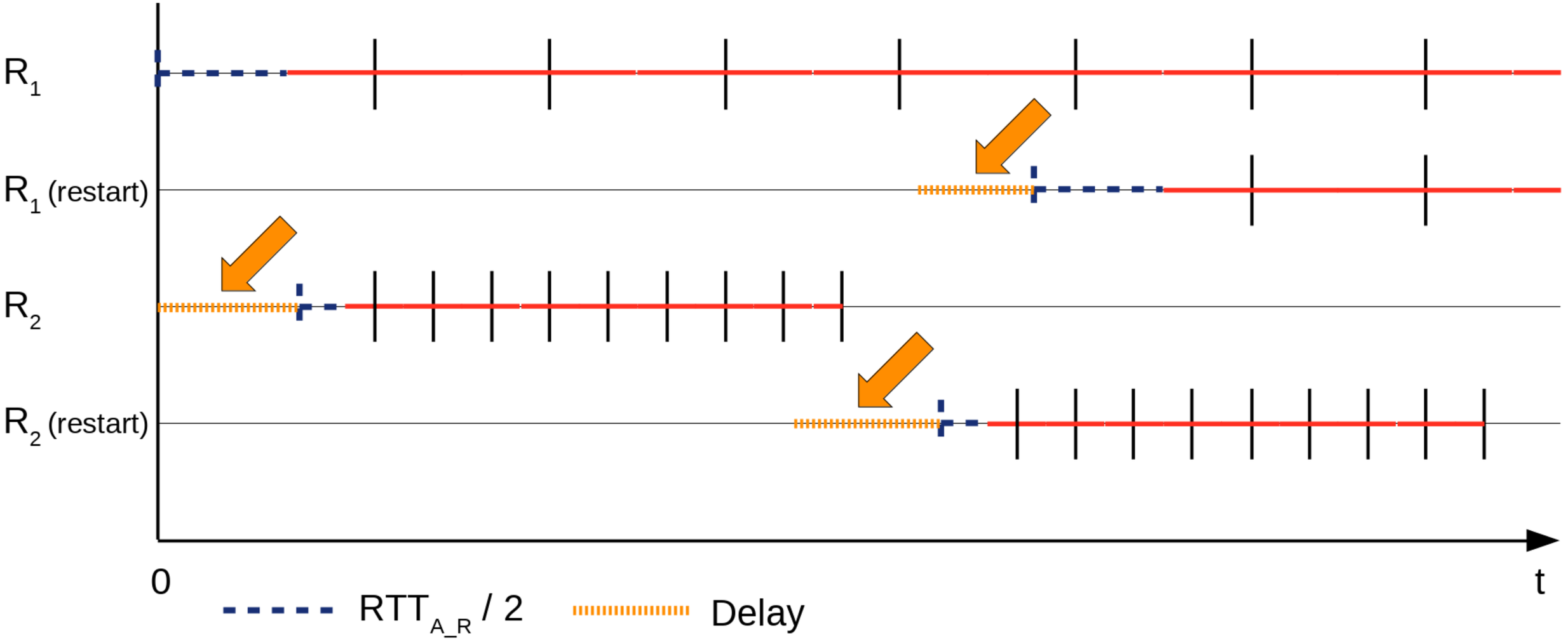
Bandwidth Pattern



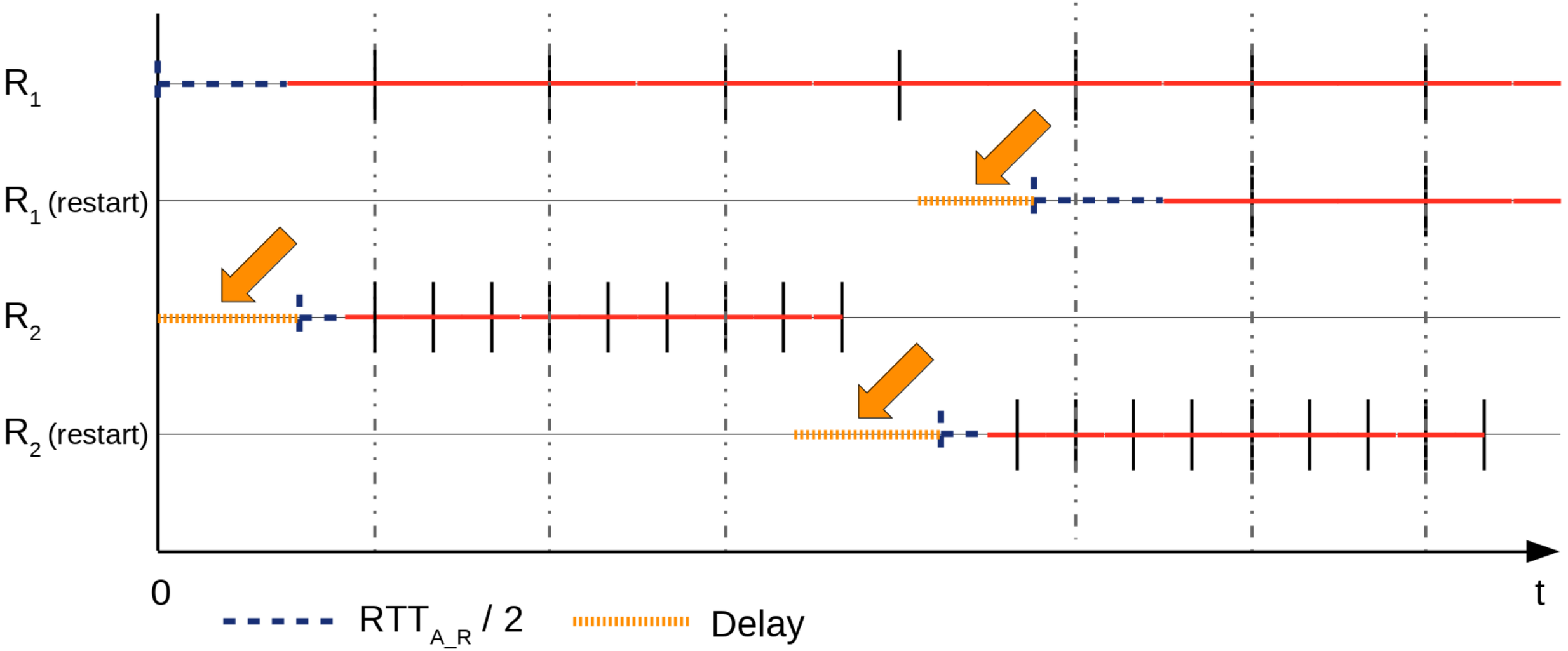
How to Pulse – Aligning Chains (1)



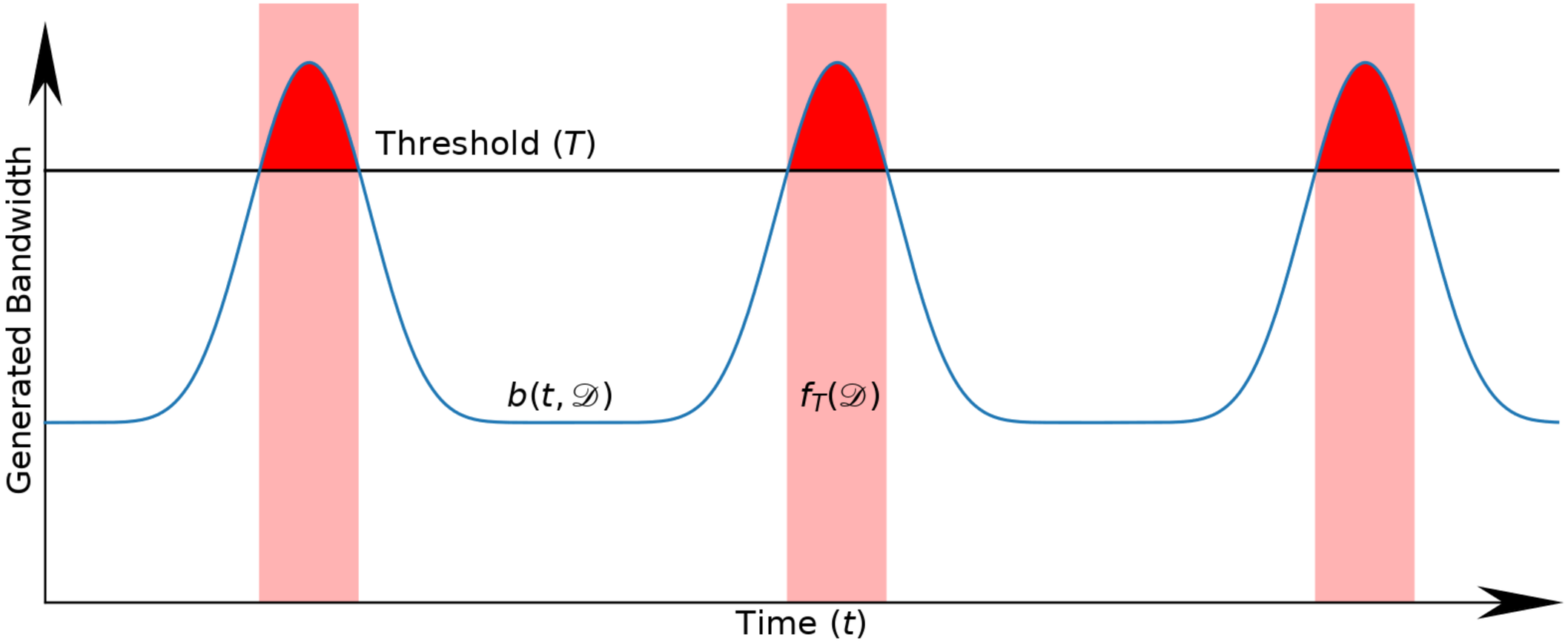
How to Pulse – Aligning Chains (2)



How to Pulse – Aligning Chains (2)



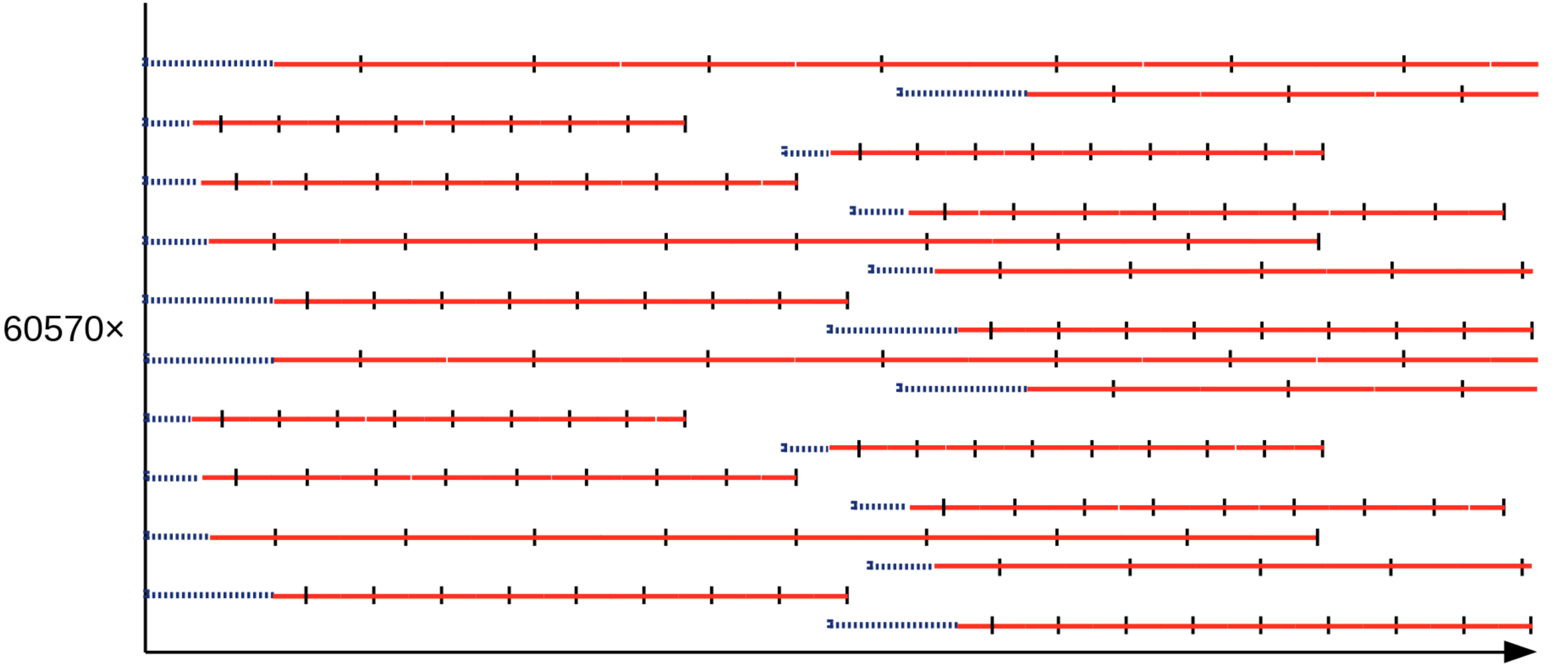
Definition of Success – Time above threshold



$$f_T(\mathscr{D}) = \int s_T(t, \mathscr{D})\, dt \qquad s_T(t, \mathscr{D}) = \begin{cases} 1 & \text{if } b(t, \mathscr{D}) \geq T \\ 0 & \text{else} \end{cases}$$

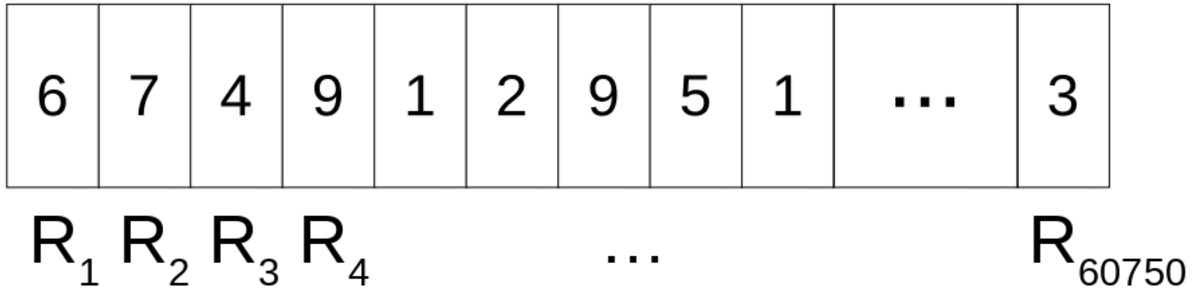
$\mathscr{D}$: Delay values

How to Pulse – Aligning Chains

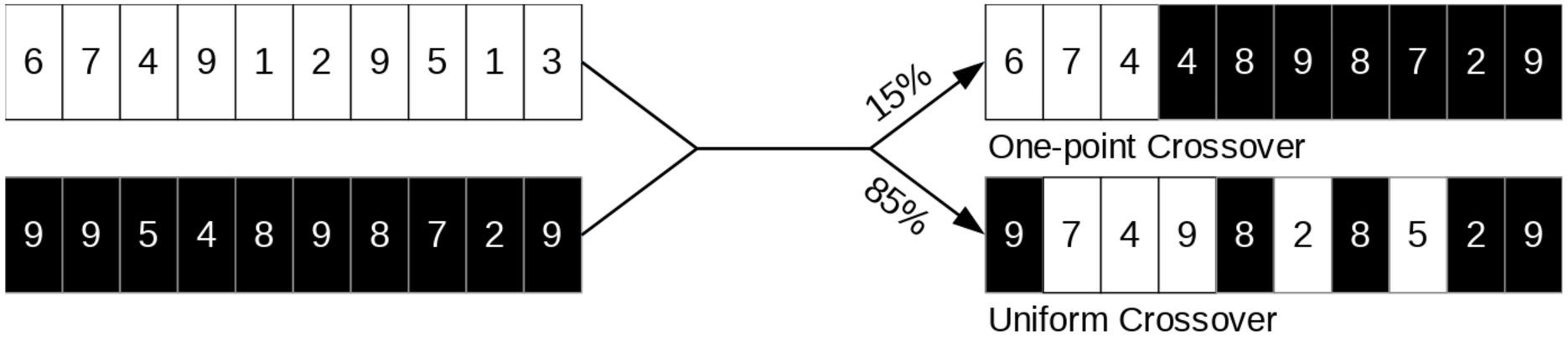


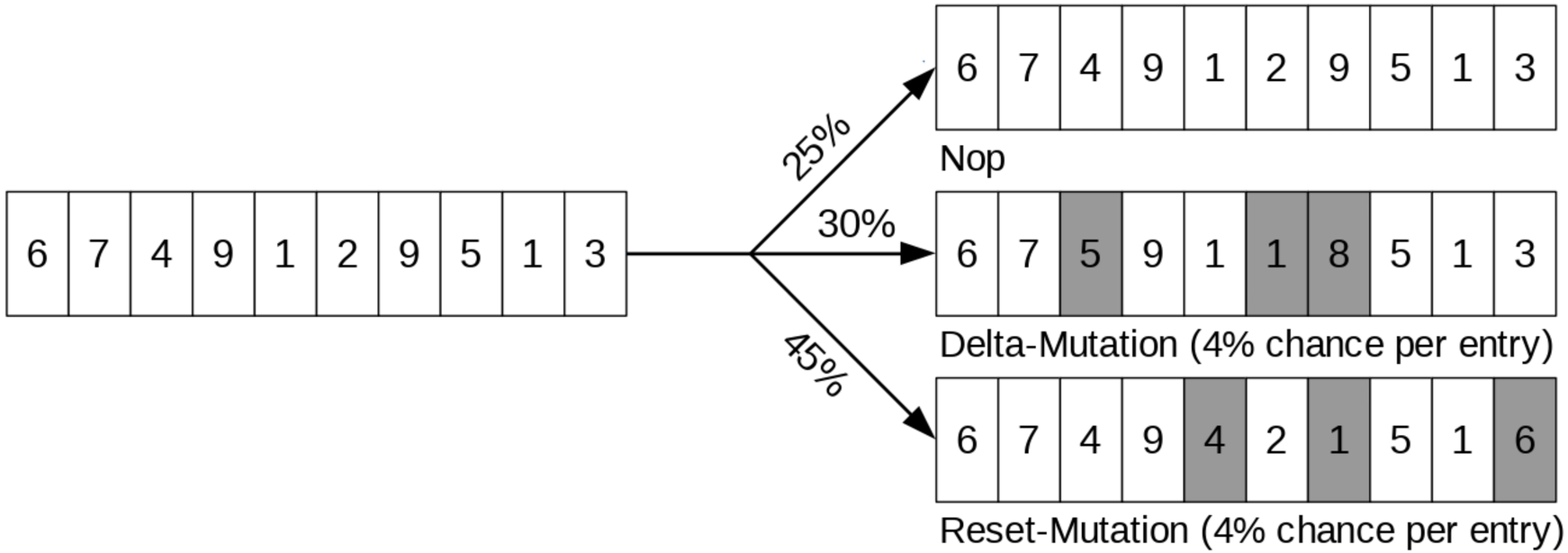
Genetic Algorithm

- **Individual** ($\mathscr{D}$)
  Array of initial delays (in ms)
  One per resolver
  - Uniform Distribution [0, 1500]
- **Population**
  Set of individuals
  Size: 1250
- Selection
  - *Maximizing Selector*
  - 50% of population
- Population replacement with *equal probability*



Genetic Algorithm – Crossover & Mutation

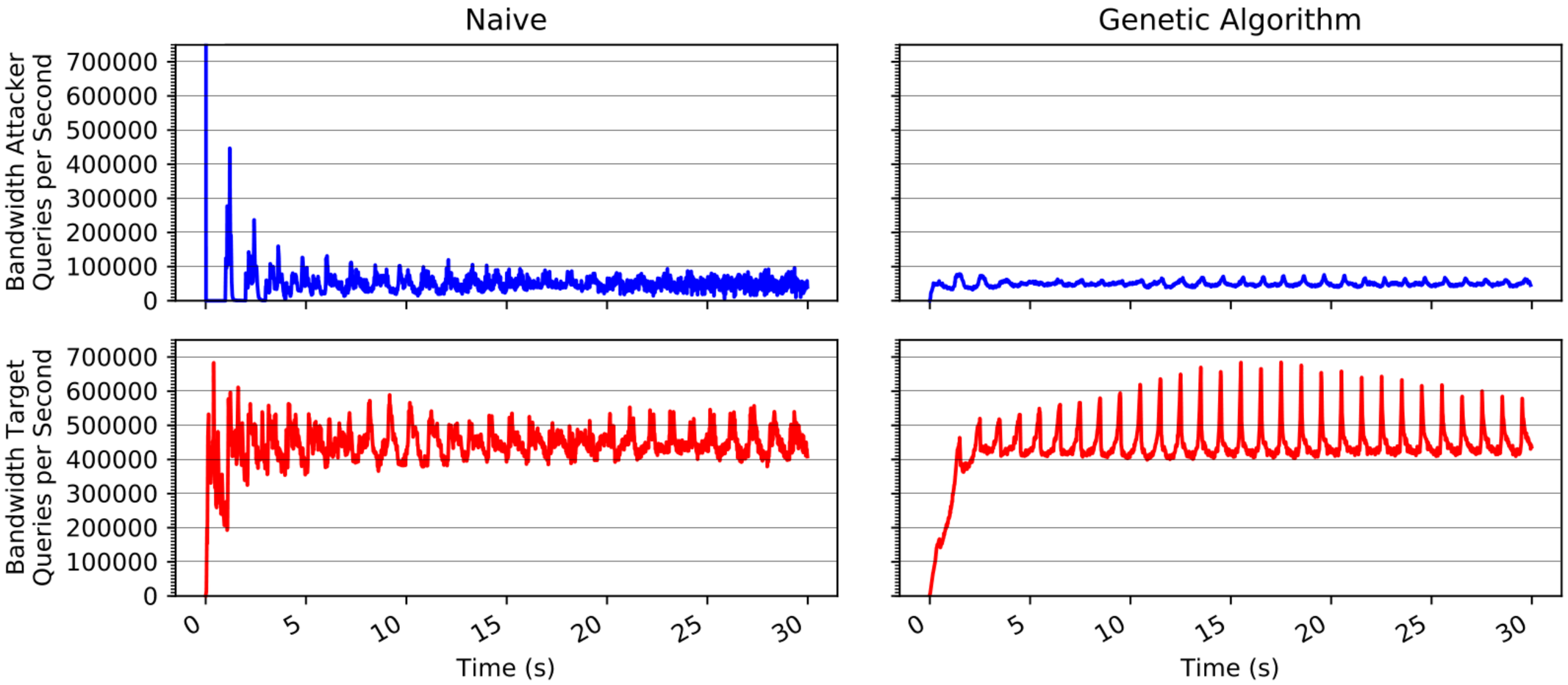




Task

- 60570 Resolver
  - Measured timing for Europe and US based authoritative DNS server
  - Attacker based in Europe
- Finding a solution took
  - 2 hours
  - 5000 iterations
- “Naive” Solution
  - Start each chain as soon as possible
  - Every 1s + RTT_{R_ex1}

Results


Naive
Genetic Algorithm
Bandwidth Attacker
Queries per Second
Bandwidth Target
Queries per Second
700000
600000
500000
400000
300000
200000
100000
0
0
5
10
15
20
25
30
Time (s)

Limitations

- Concrete Time Model
  - Stable RTT
  - Optimize probability function of packet arrival

- Only optimizes initial delays
  - Allow more synchronization points
  - Con: much more complex problem

Countermeasures

Pulsing and Packet Loss

- TCP's Congestion Signal
  - Use RTT instead of packet loss
  - TCP Vegas or TCP BBR (**B**ottleneck **B**andwidth and **R**ound-trip propagation time)
- Other protocols: QUIC

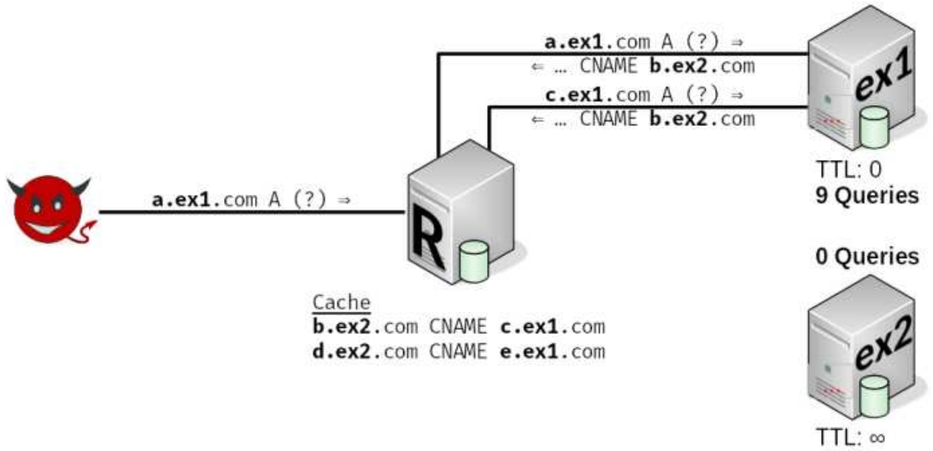
DNS and CNAME-Chains

- Authoritative Servers
  - Detect chains, requires periodic checks
- Lower Limits for TTL
  - Used for DNS-based failover
- Recursion Depth Limit
  - Only **8** CNAME entries needed
  - Resolvers up to **33** entries

Summary

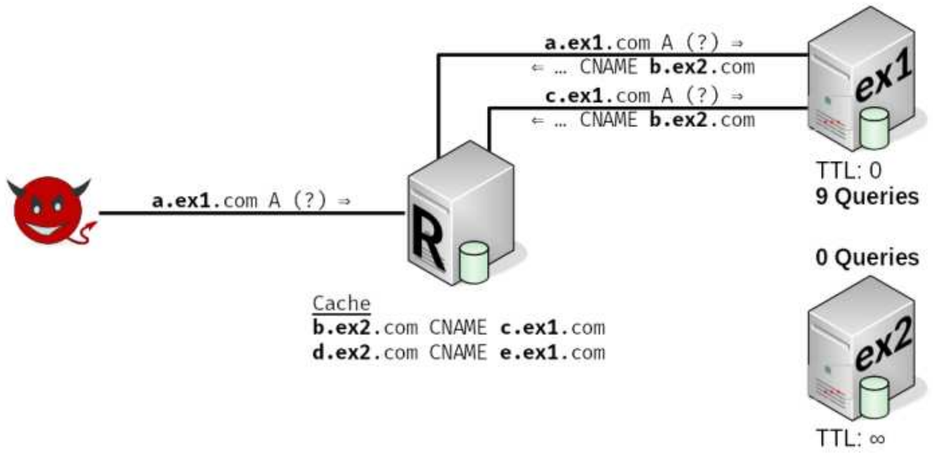
Summary

CNAME Chains – Caching

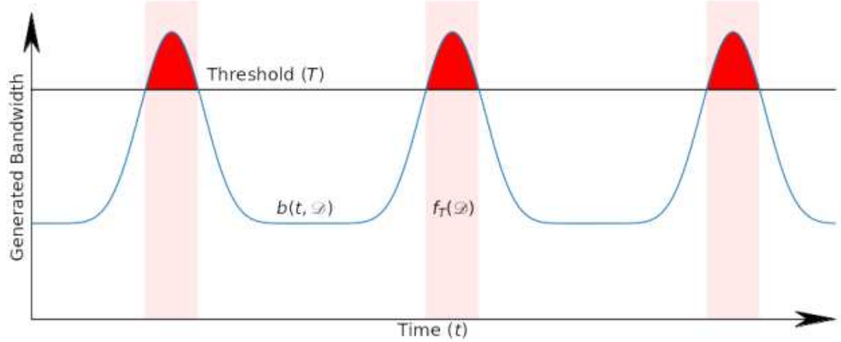


Summary

CNAME Chains – Caching



Definition of Success: Time above threshold

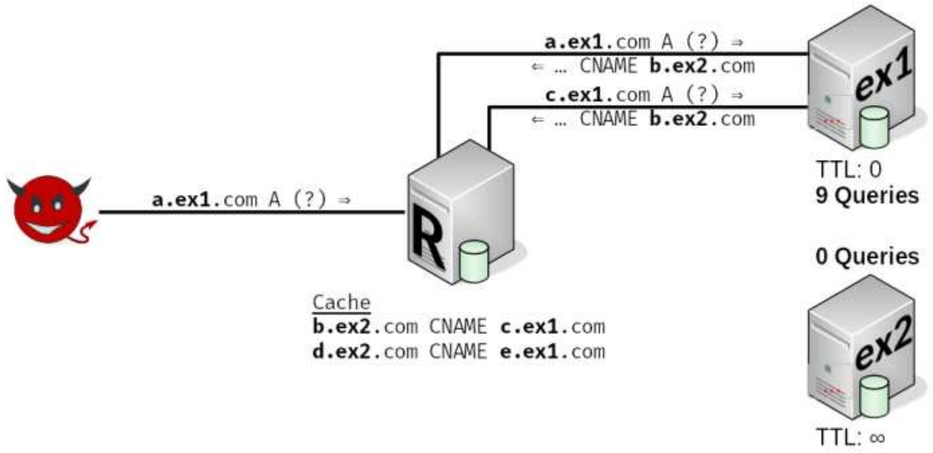


$$f_T(\mathscr{D}) = \int s_T(t,\mathscr{D})\,dt \qquad s_T(t,\mathscr{D}) = \begin{cases} 1 & \text{if } b(t,\mathscr{D}) \geq T \\ 0 & \text{else} \end{cases}$$

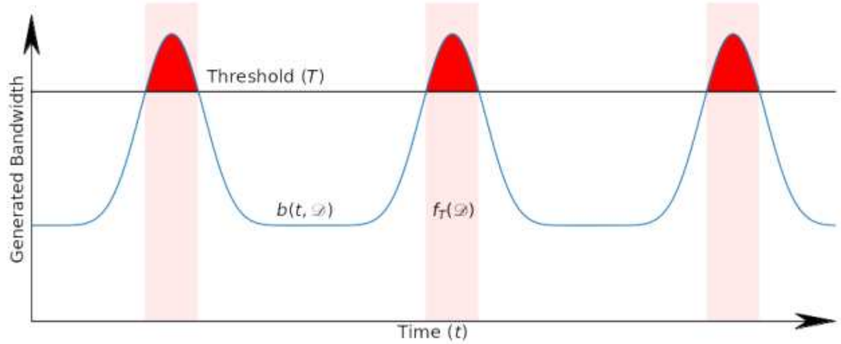
$\mathscr{D}$: Delay values

Summary

CNAME Chains – Caching



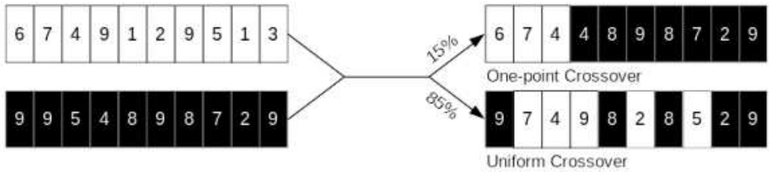
Definition of Success: Time above threshold

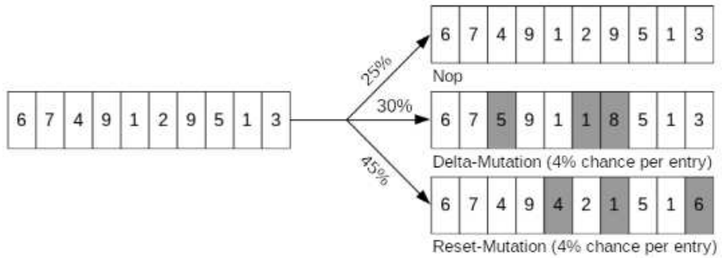


$$f_T(\mathscr{D}) = \int s_T(t,\mathscr{D})\,dt \qquad s_T(t,\mathscr{D}) = \begin{cases} 1 & \text{if } b(t,\mathscr{D}) \geq T \\ 0 & \text{else} \end{cases}$$

$\mathscr{D}$: Delay values

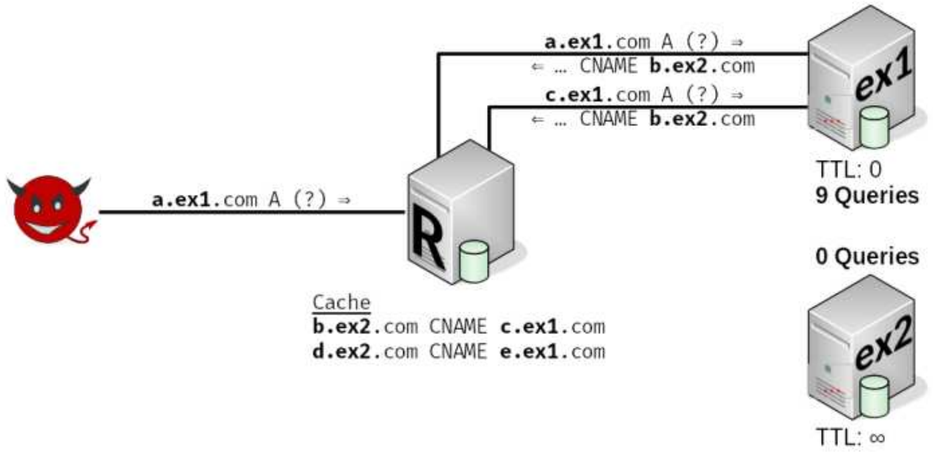
Genetic Algorithm – Crossover & Mutation



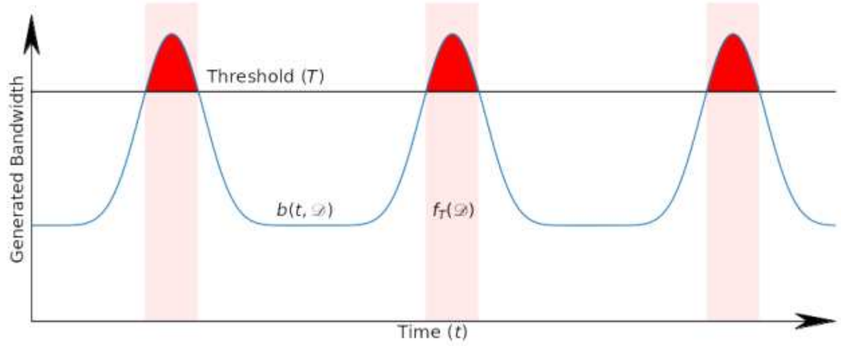


Summary

CNAME Chains – Caching



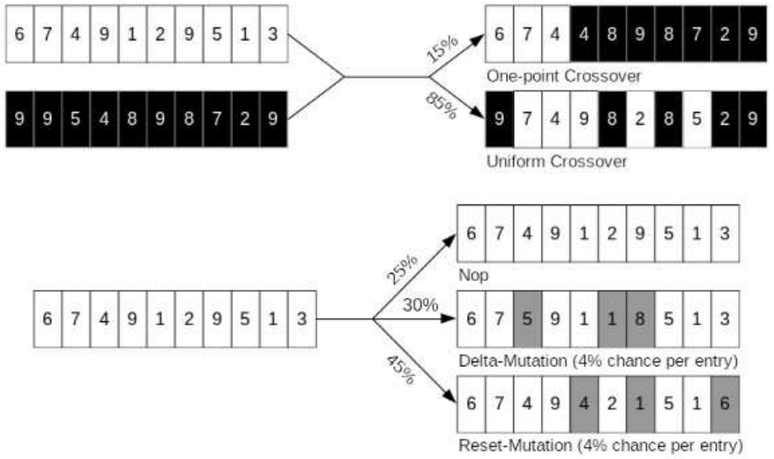
Definition of Success: Time above threshold



$$f_T(\mathscr{D}) = \int s_T(t,\mathscr{D})\,dt \qquad s_T(t,\mathscr{D}) = \begin{cases} 1 & \text{if } b(t,\mathscr{D}) \geq T \\ 0 & \text{else} \end{cases}$$

$\mathscr{D}$: Delay values

Genetic Algorithm – Crossover & Mutation



Results