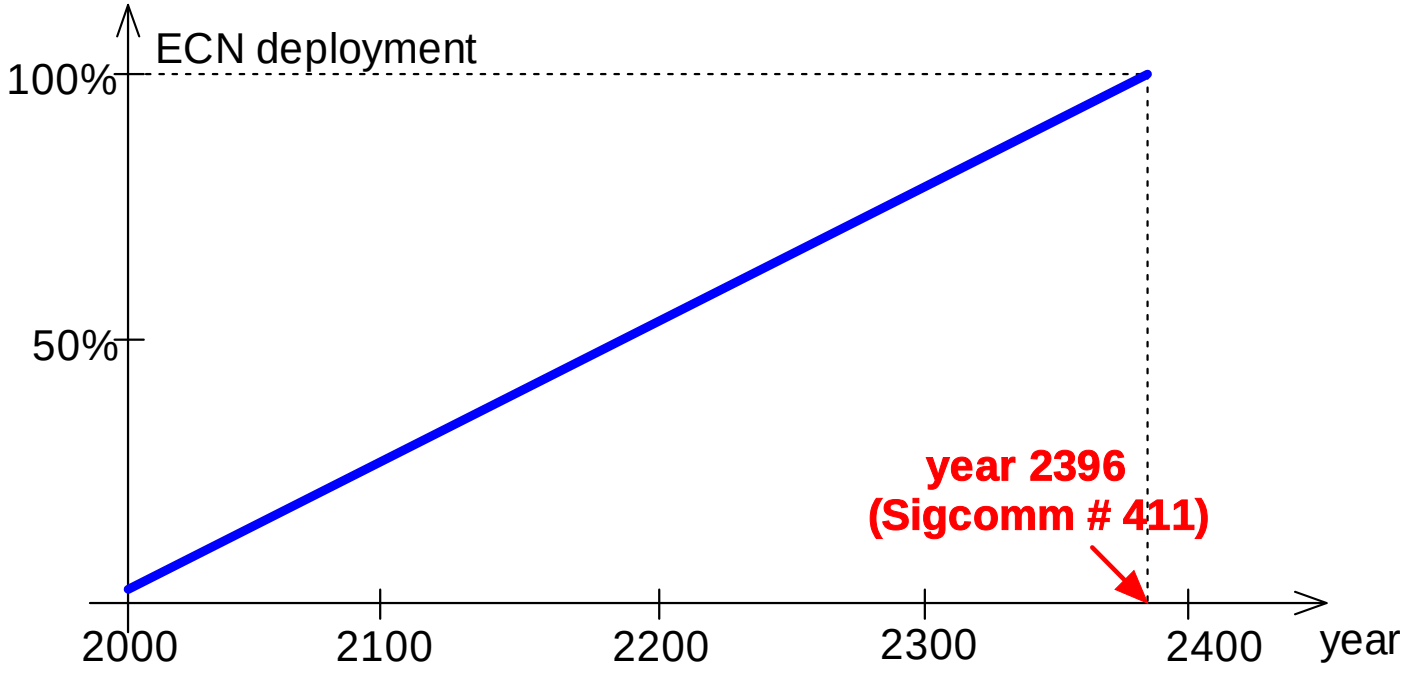
The Power of Explicit Congestion Notification

Aleksandar Kuzmanovic
Northwestern University

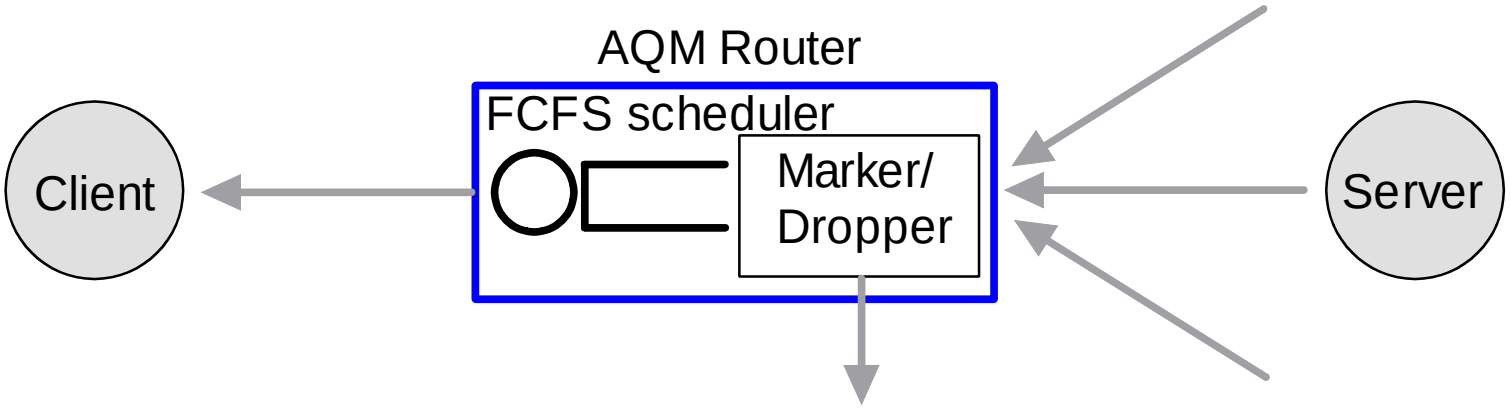
http://www.cs.northwestern.edu/~akuzma/

Motivation

- Recent measurements [PF01,MPF04]:
  - 2000: 1.1% Web servers support ECN
  - 2004: the percent increased to 2.1%
  - Not a single packet was marked in the network



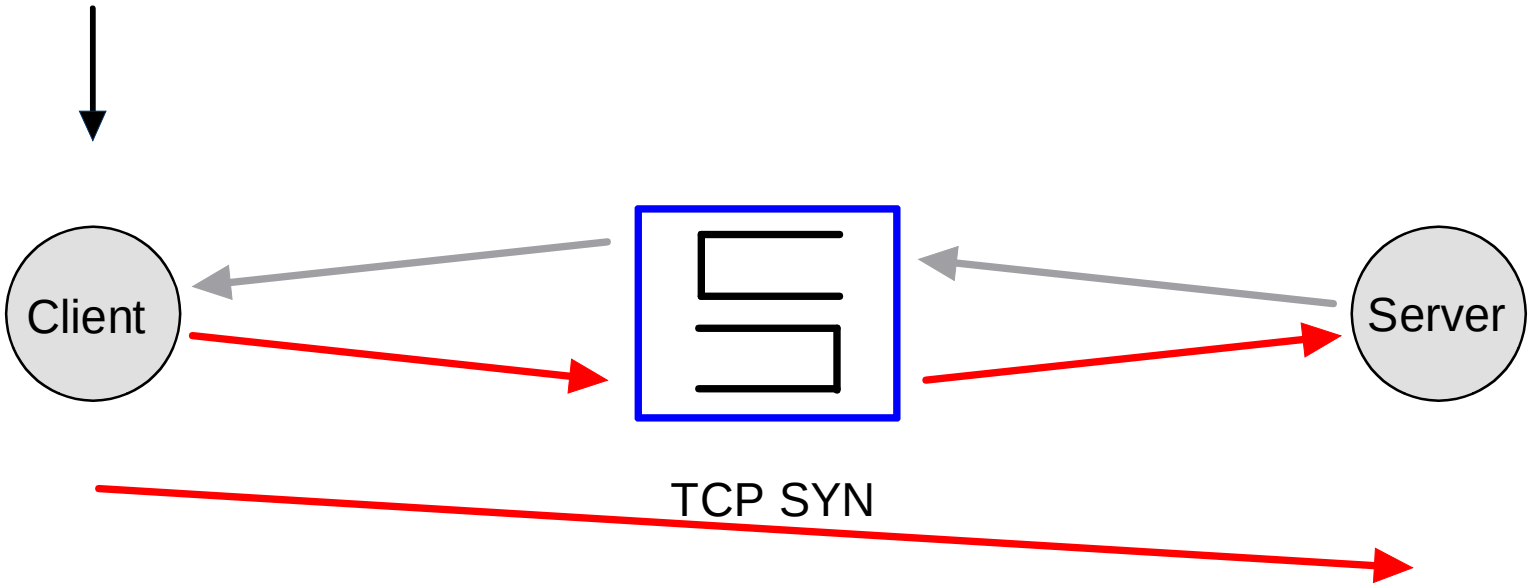
Background



- Active Queue Management (AQM):
  - Simultaneously achieves high throughput and low average delay
  - AQM algorithms can mark (instead of drop) packets
  - The router and both endpoints have to be ECN-enabled

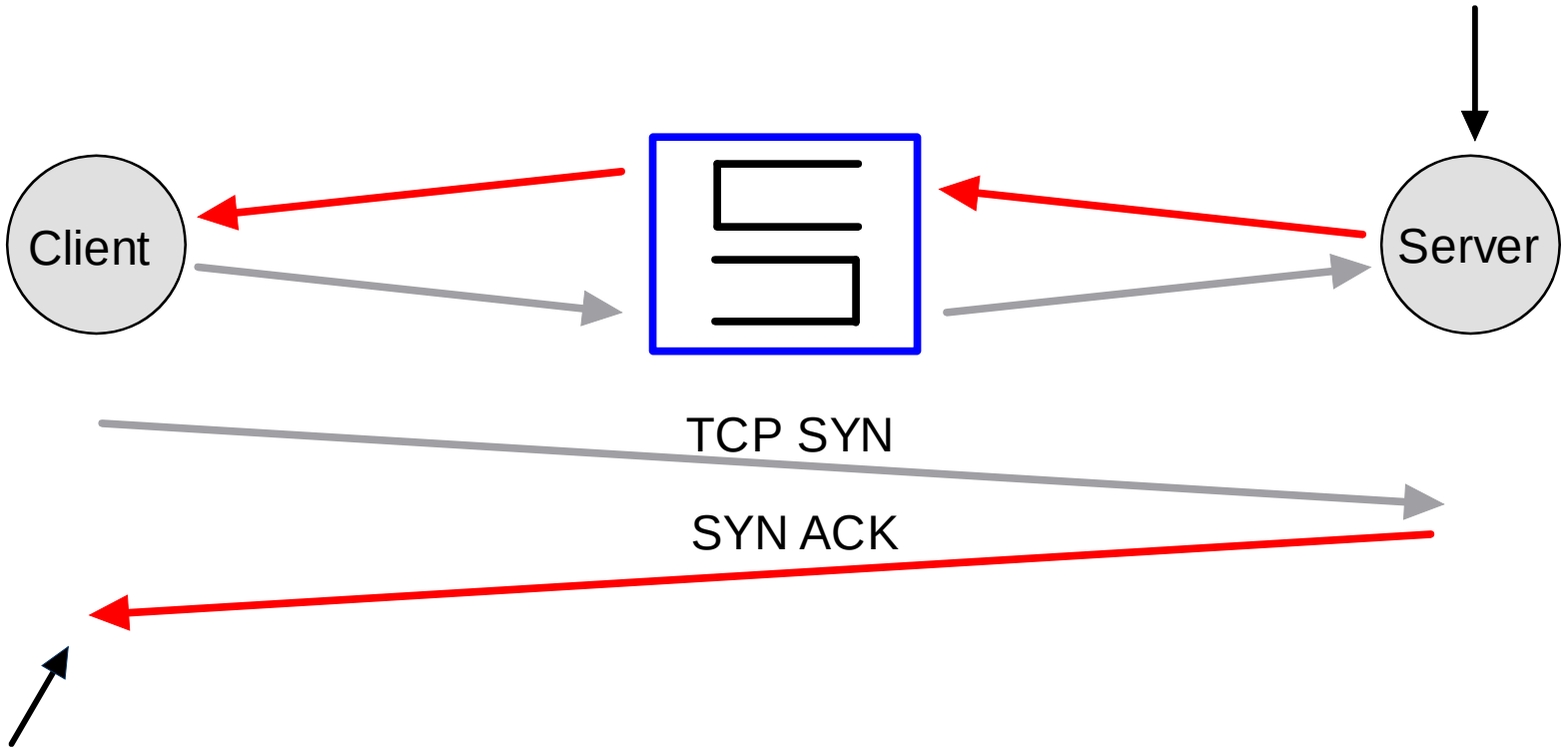
Negotiating ECN Capabilities (I)

Client initiates ECN-capable communication by setting appropriate bits in the TCP SYN packet's **TCP header**



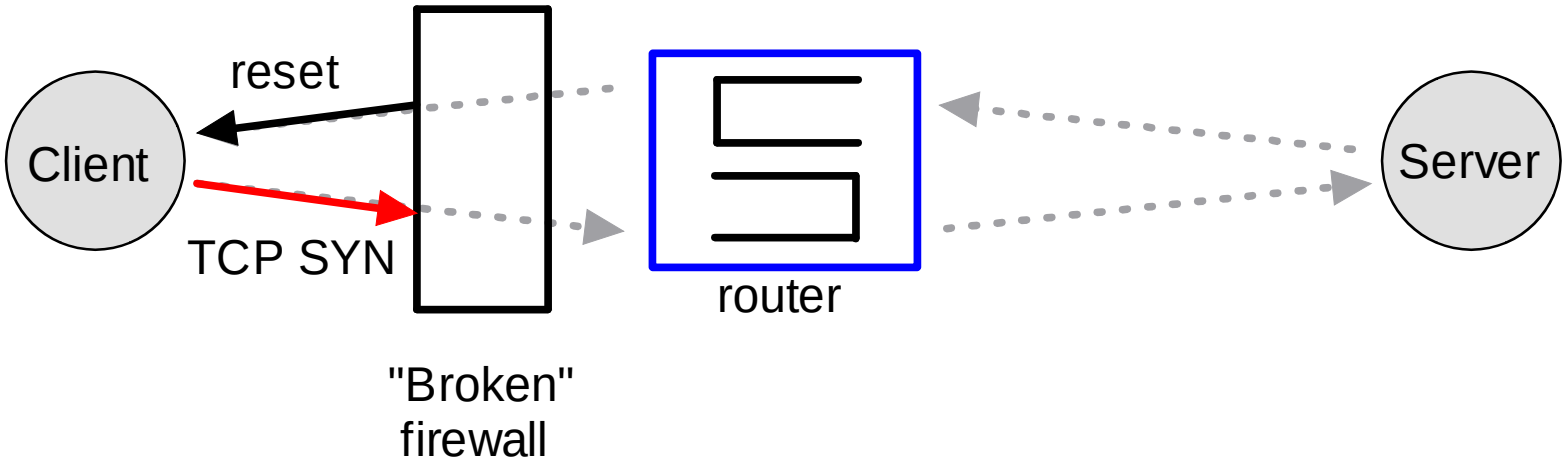
Negotiating ECN Capabilities (II)

An ECN-capable server replies by setting appropriate bits in the SYN ACK packet's **TCP header**



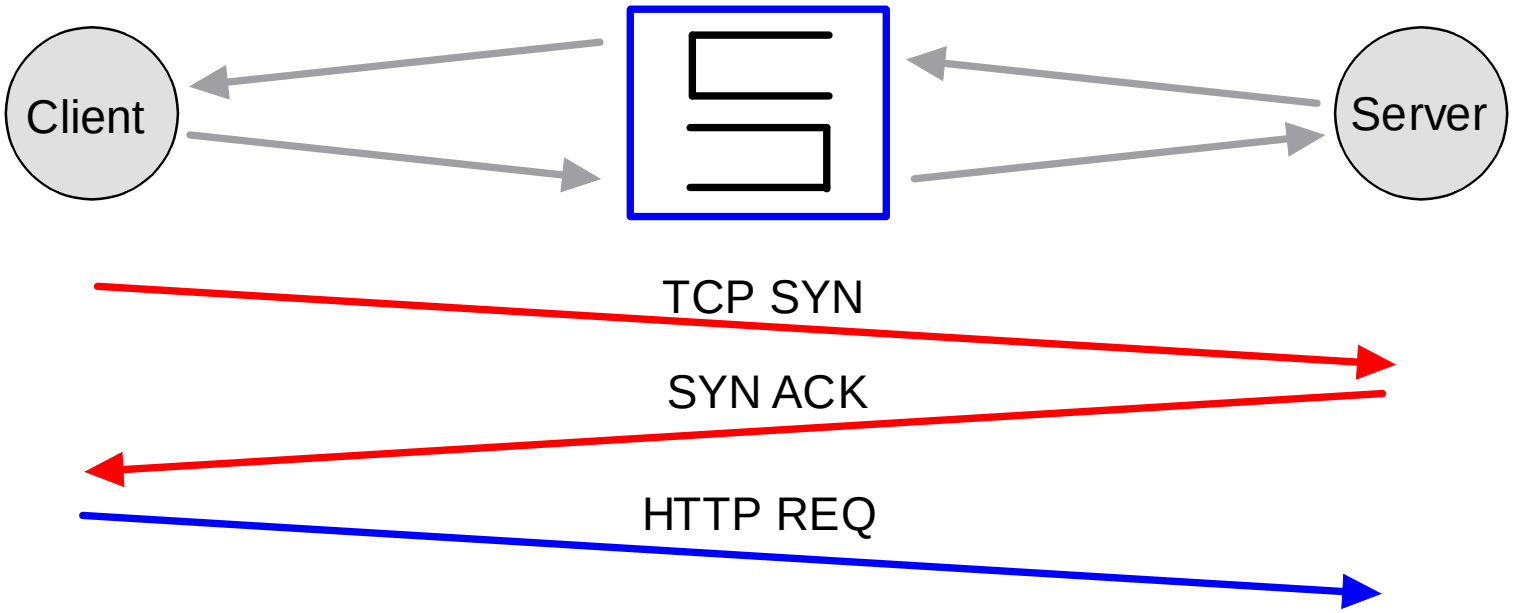
Once the SYN ACK packet arrives, ECN negotiation is completed

Barriers to Adoption of ECN



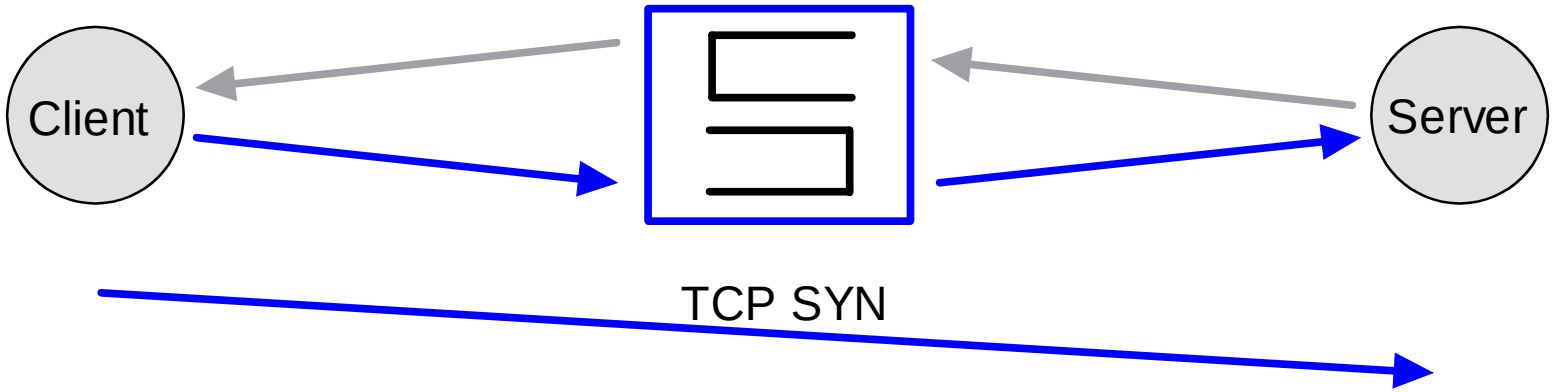
- “Broken” firewalls and load balancers incorrectly reset TCP flows attempting to negotiate ECN
  - The problem addressed in RFC 3360
- Consequences are devastating
- New incentives?

ECN and TCP's Control Packets



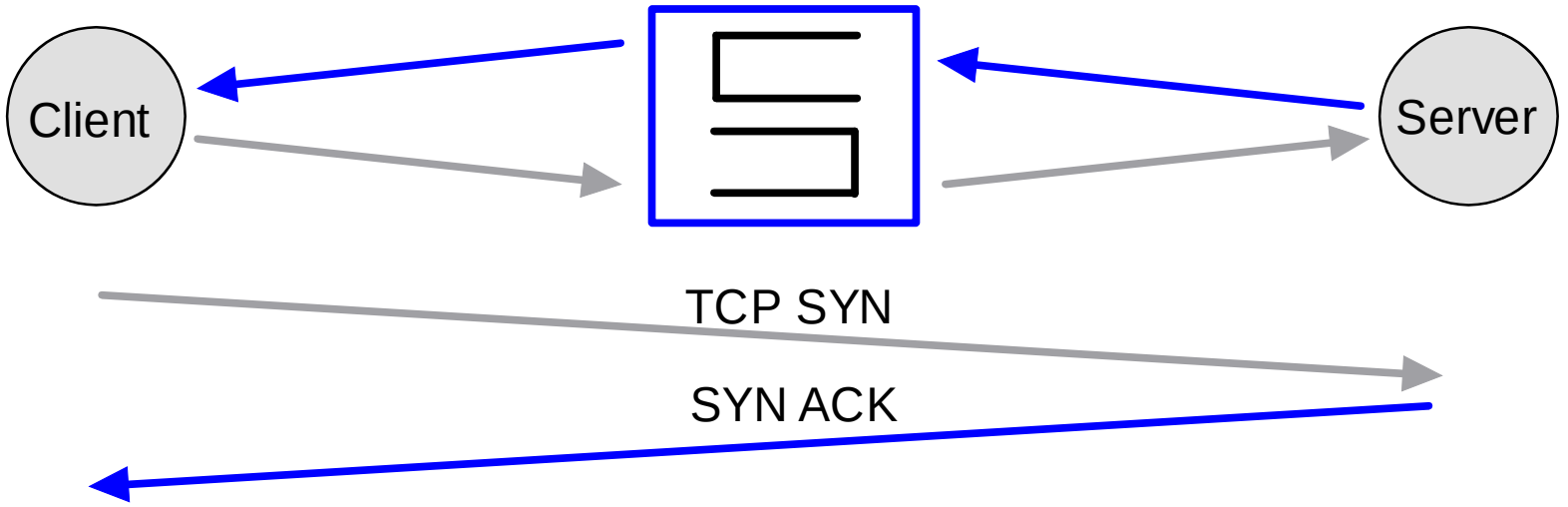
- TCP SYN and SYN ACK packets are dropped during congestion
- Can significantly reduce end-to-end performance
  - RTO = 3 sec (+6 sec, +12 sec, etc.)
- Marking SYN packets?

Marking TCP SYN Packets?



- TCP SYN packets:
  - Security problems
- SYN ACK packets:
  - No security obstacles
  - More relevant
    - Congestion likely to happen from servers to clients

Marking SYN ACK Packets?

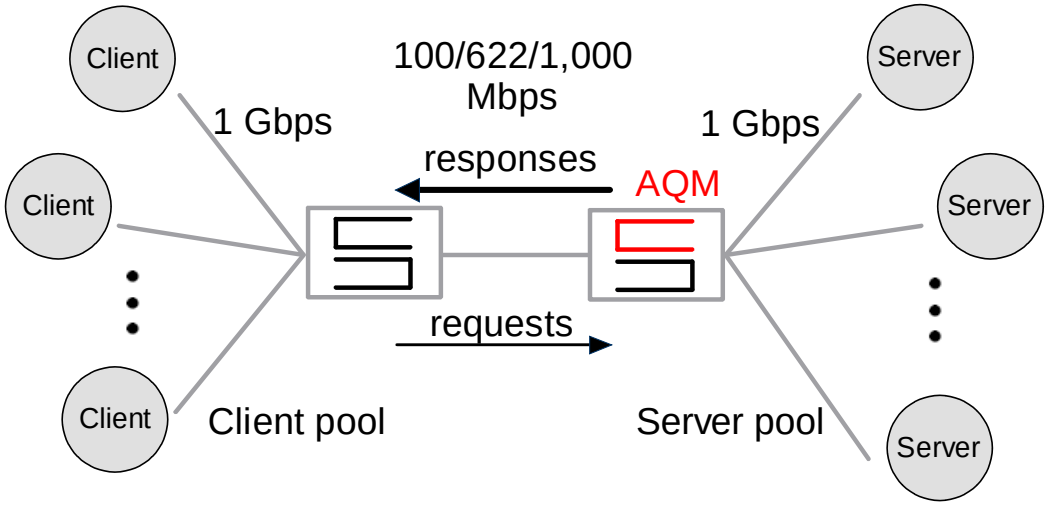


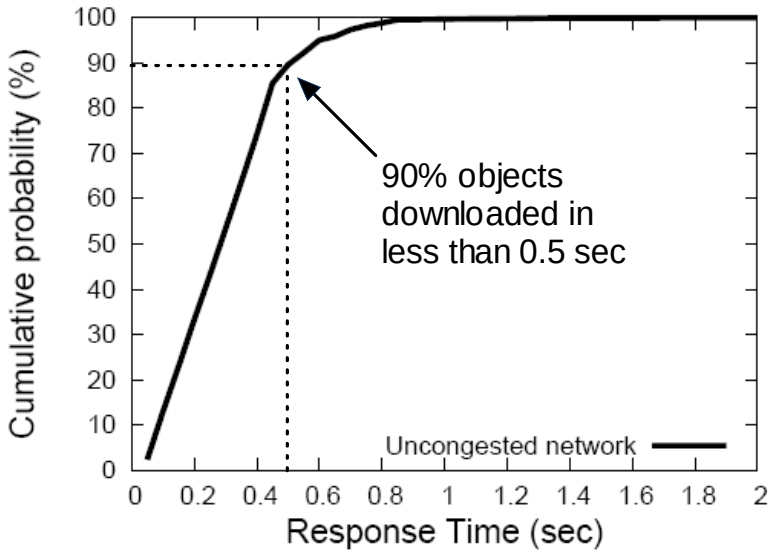
- TCP SYN packets:
  - Security problems
- SYN ACK packets (ECN+):
  - No security obstacles
  - More relevant
    - Congestion likely to happen from servers to clients

Deployment Requirements

- Security
  - No novel security holes
- Performance improvements
  - Necessary to provide incentives to all involved parties
- Incremental deployability
  - What level of deployment is needed to achieve the above improvements?
  - What happens to those who do not apply the change?

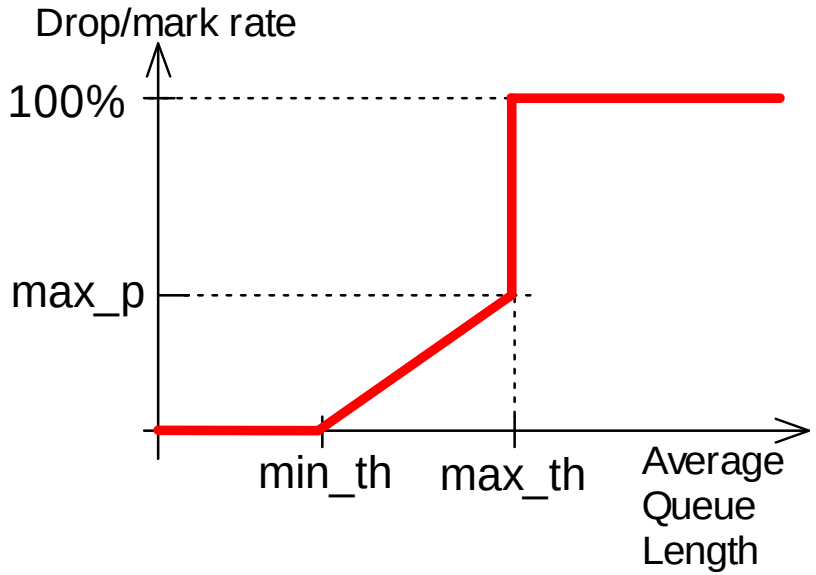
Simulation Scenario





- Light and persistent congestion from servers to clients
- Web and general traffic mixes
- AQM algorithms: Random Early Detection (RED)
  (others in the paper)

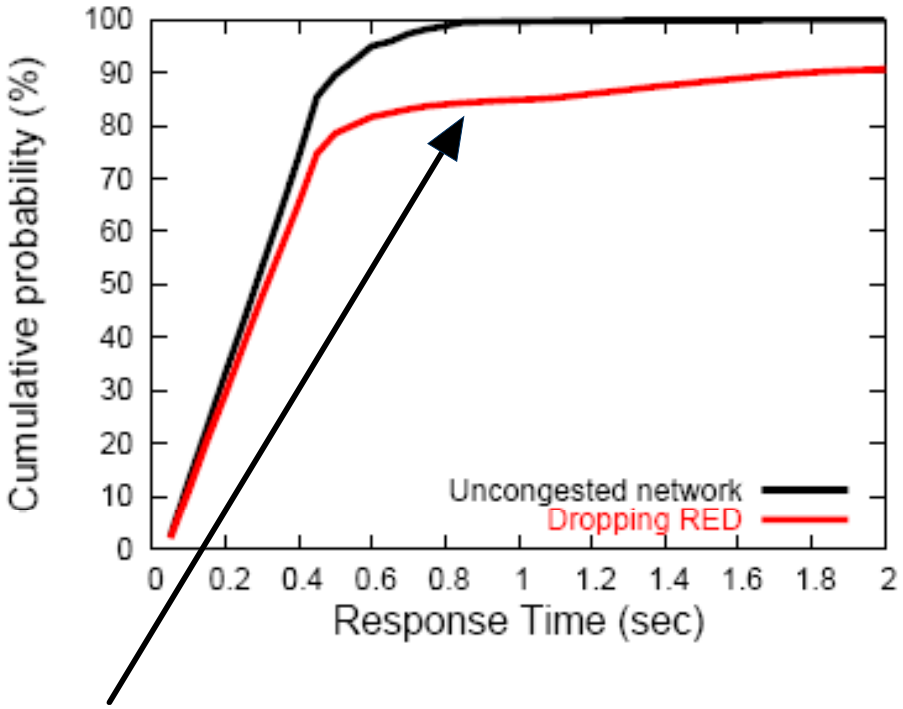
Outdated Implementation

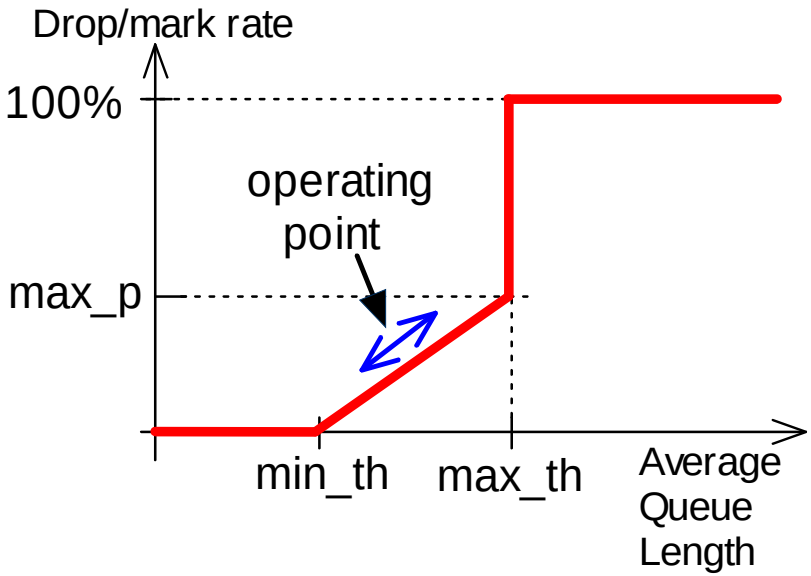


RED's dropping/marking rate as a function of the queue length

- RED (1993)
  - "This notification can consist of dropping or marking a packet."
- RFC 3168 (2001)
  - Guidelines for setting ECN with RED
- Older RED versions still present (e.g., Linux)

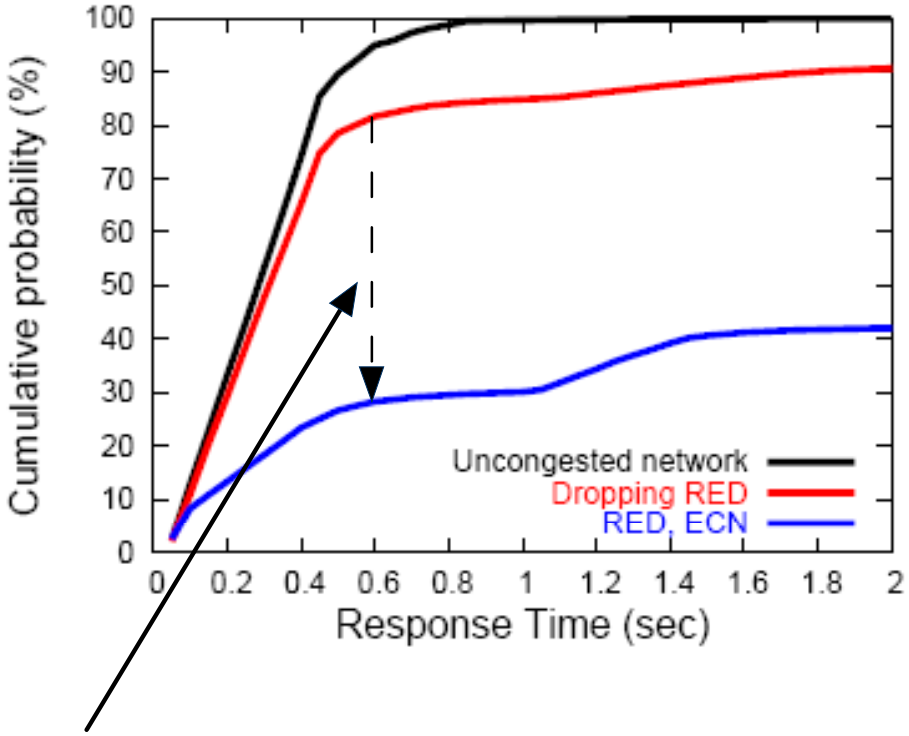
Dropping RED



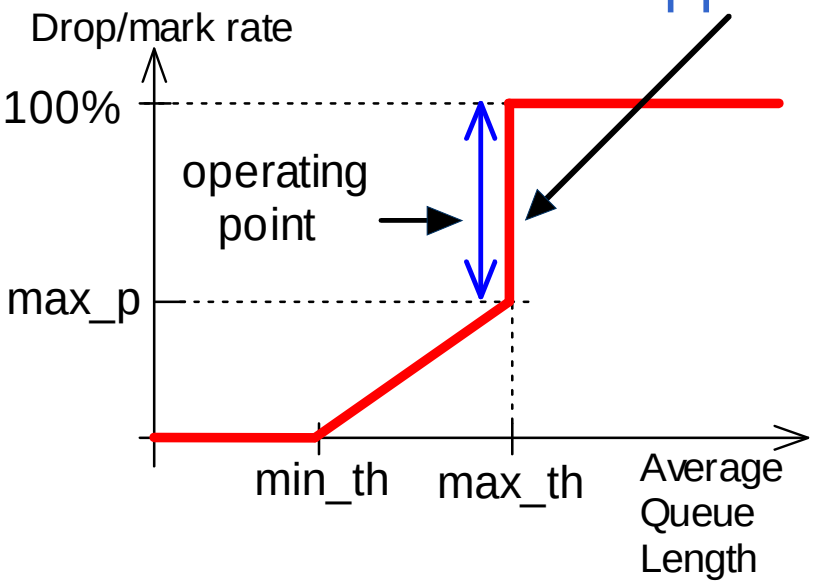


Reduced performance due to congestion

Add ECN



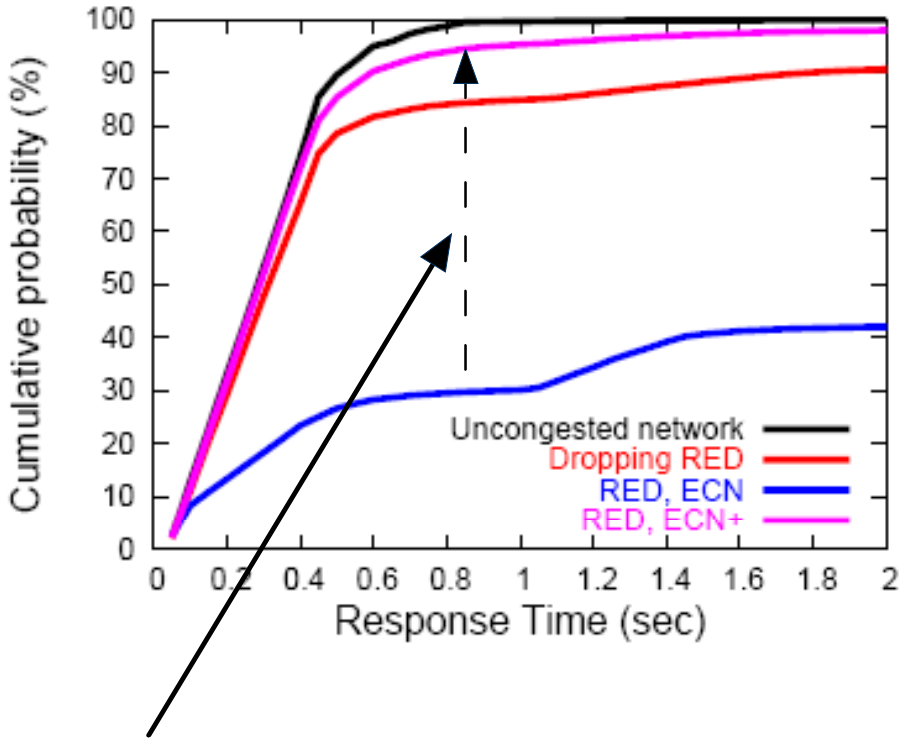
All SYN packets are dropped

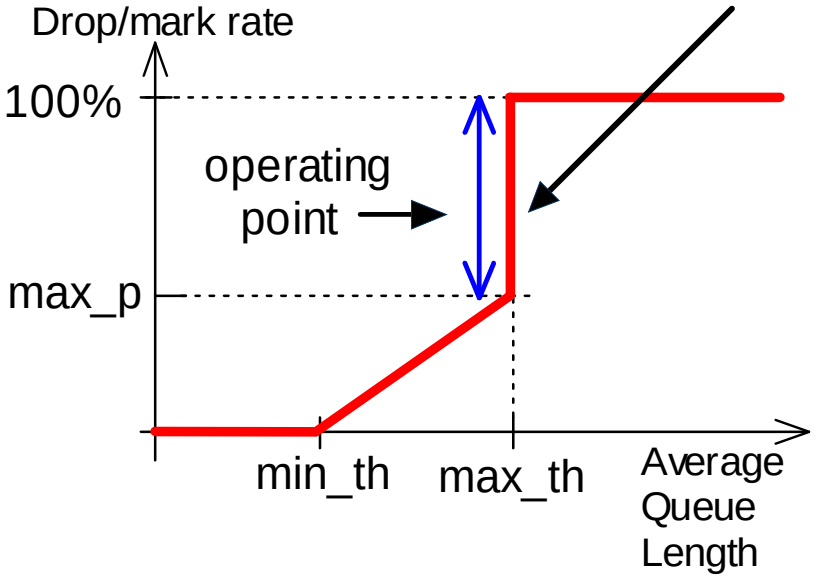


Outdated implementation can cause drastic performance degradations

Add ECN+

SYN ACK packets are NOT dropped

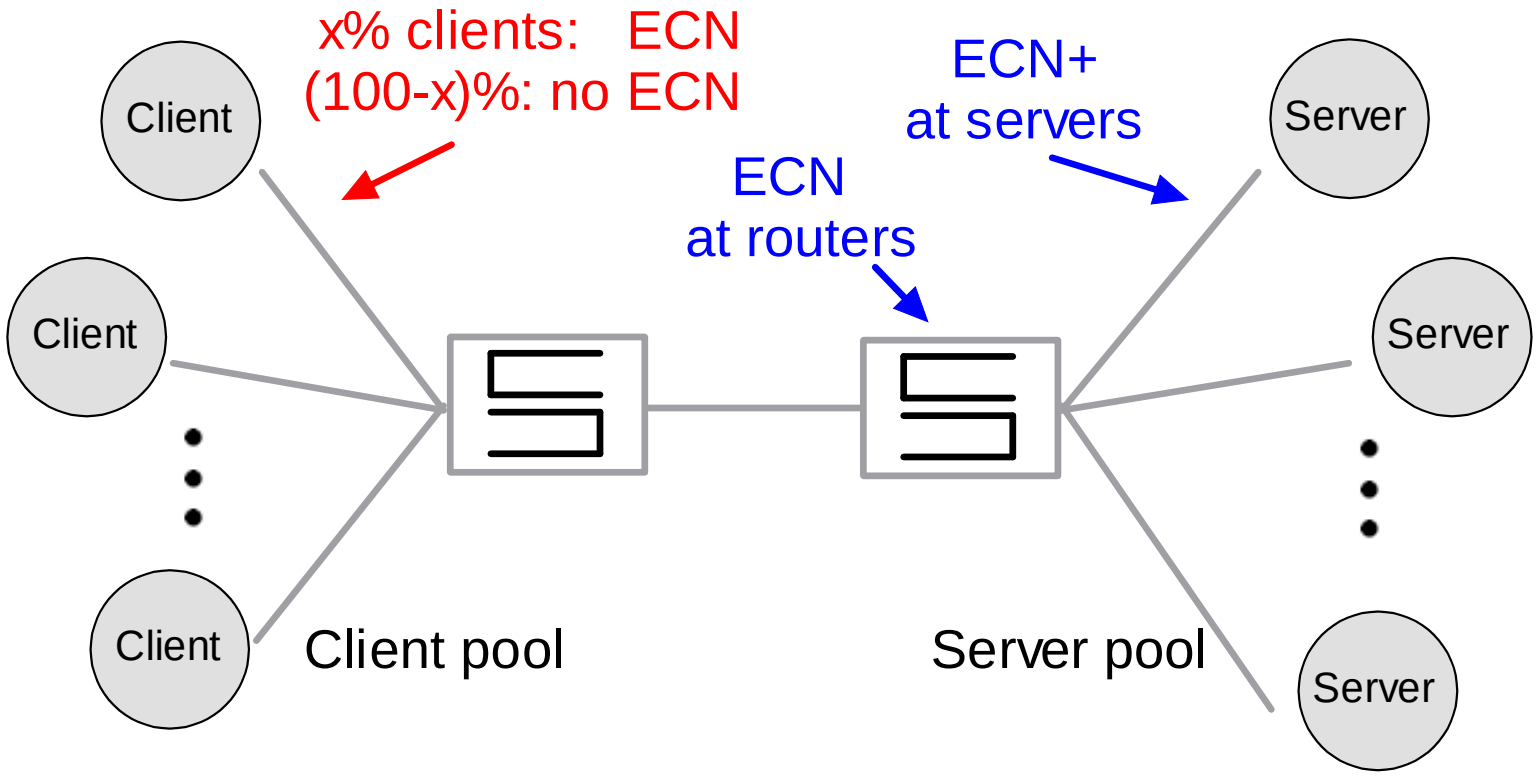




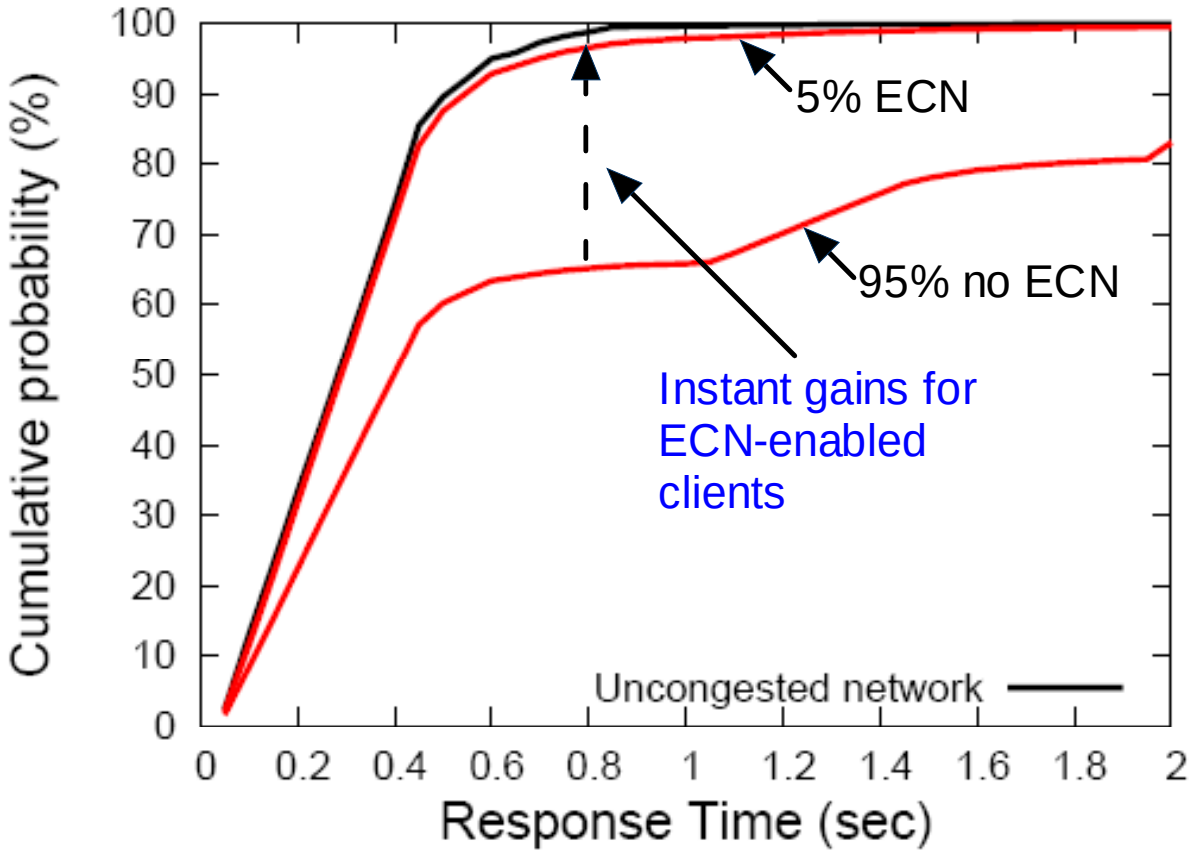
ECN+ systematically improves throughput and response times of all investigated AQM schemes

Incremental Deployability

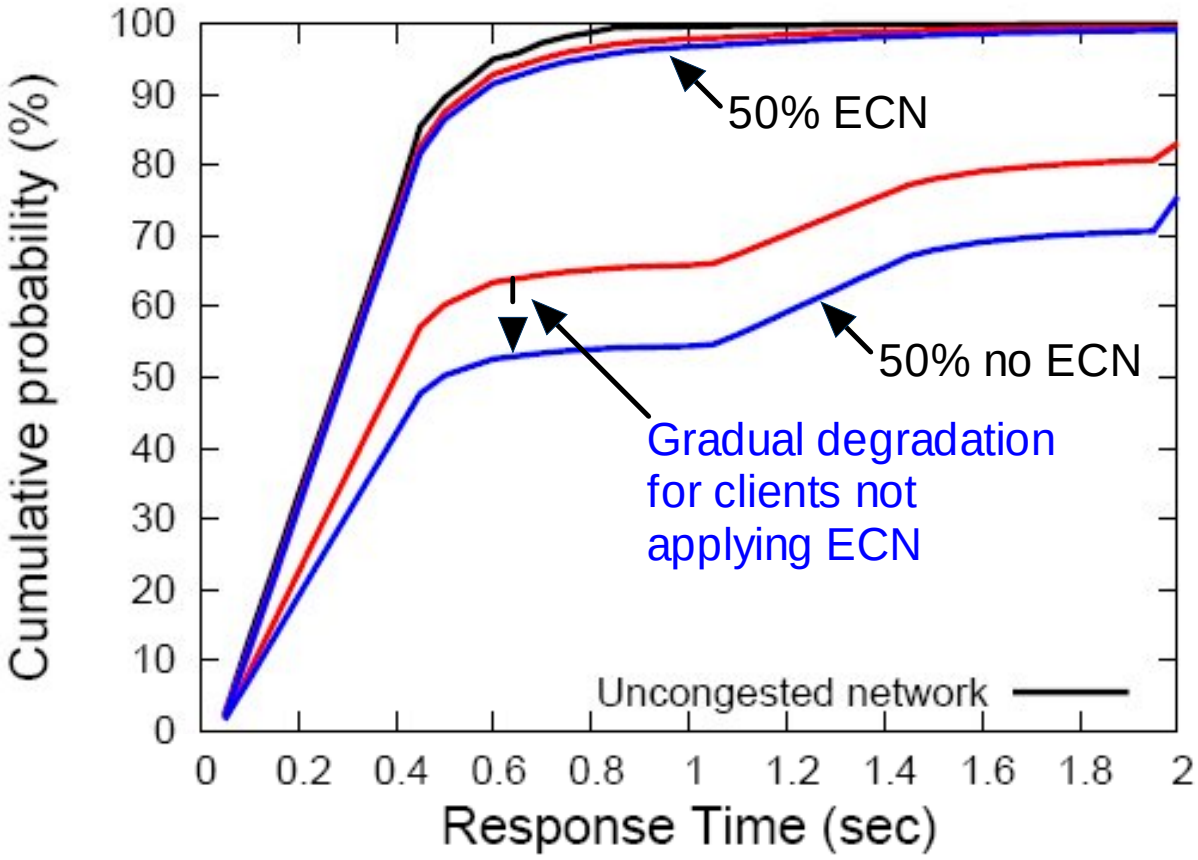
- Scenario



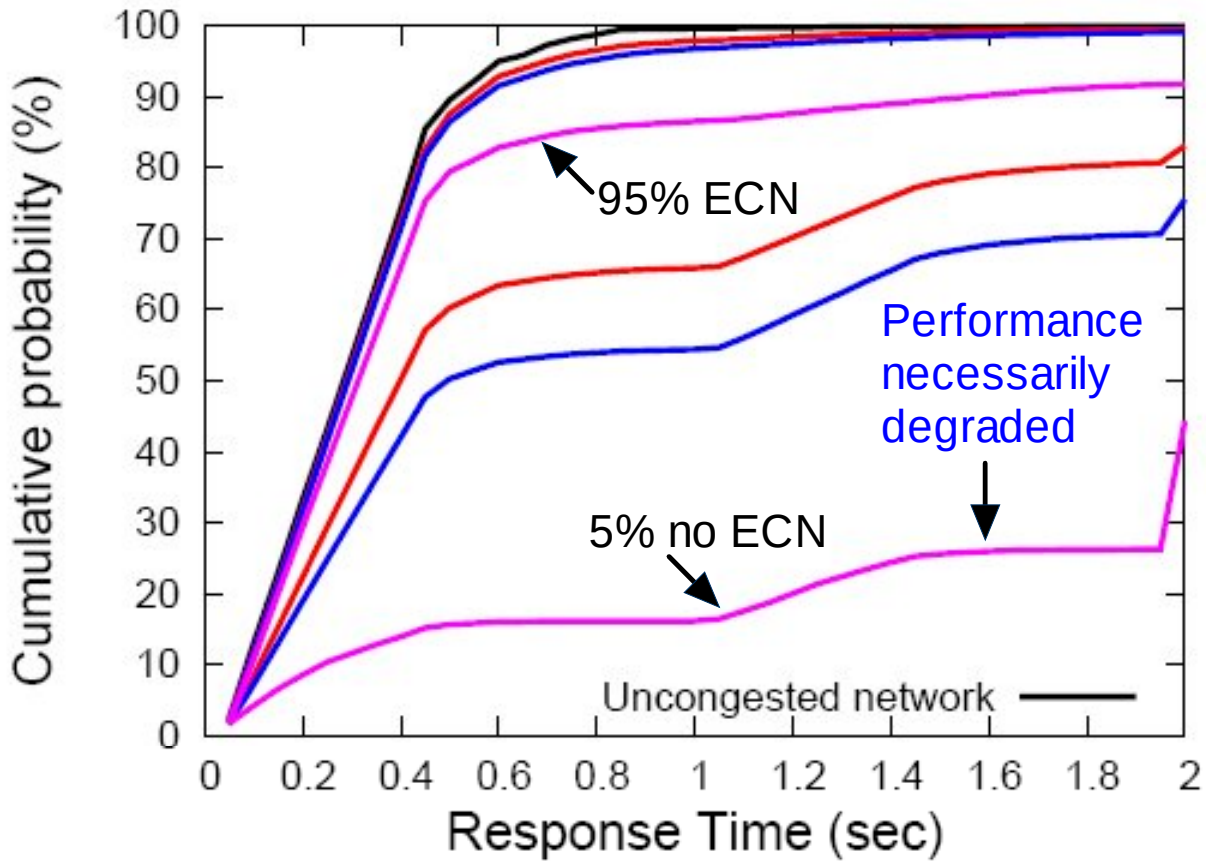
5% Deployment



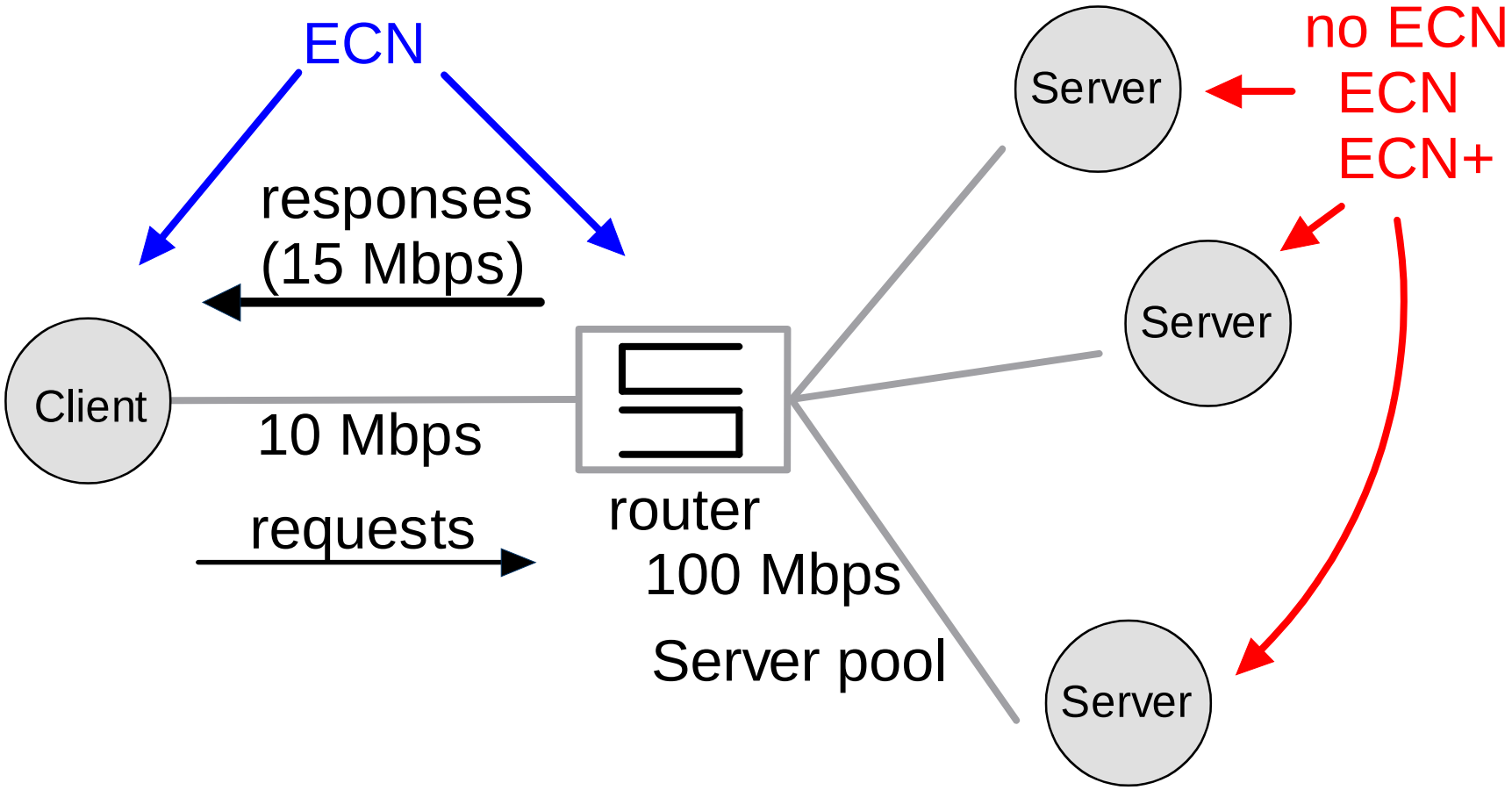
50% Deployment



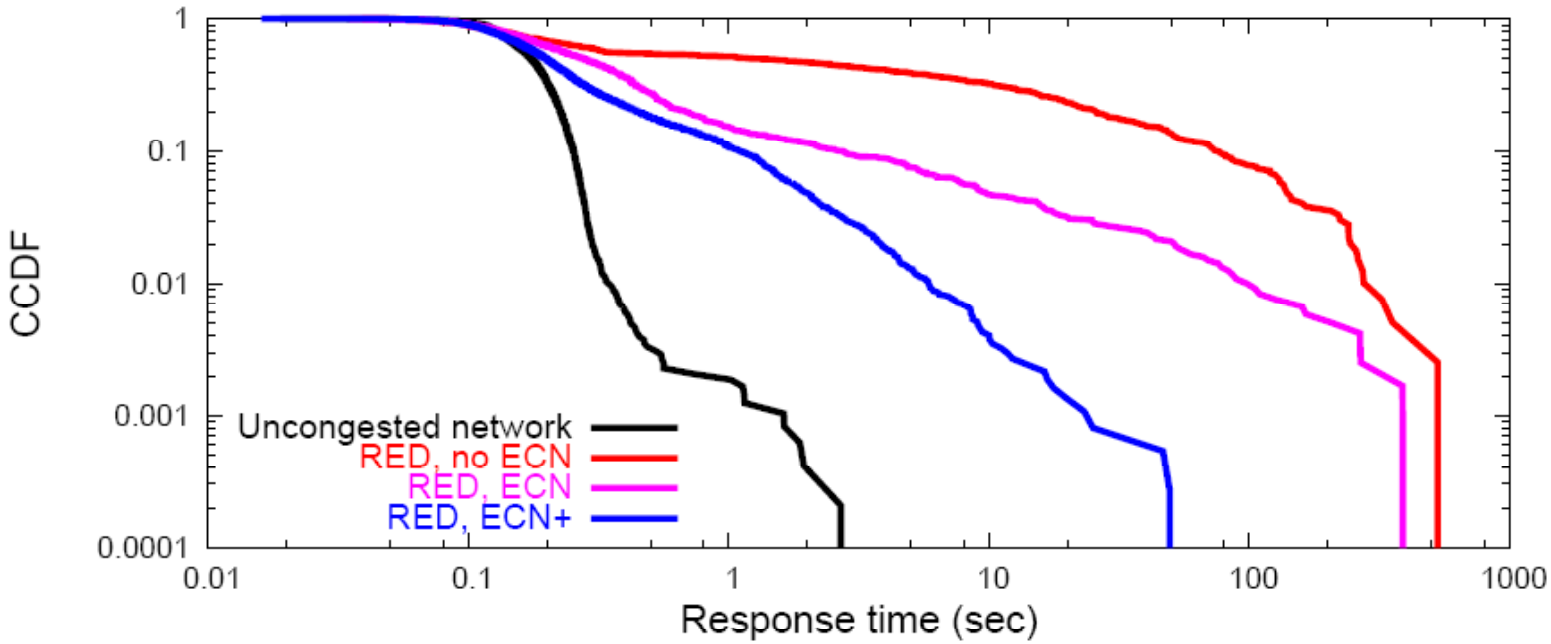
95% Deployment



Testbed Experiments



ECN and Flash Crowds



	Average Response Time	Throughput (% of capacity)
RED, no ECN	26 sec	44%
RED, ECN	4.5 sec	56%
RED, ECN+	0.5 sec	99%

Reasonable performance despite huge congestion

Conclusions

- Security
  - No novel security holes
- Incremental deployability
  - Instant benefits for clients applying the change
  - Gradual degradation for those not applying the change
- Incentives
  - Providers, clients, and servers
- Implementation
  - Wrong or outdated implementation can significantly reduce deployment and performance