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

![Diagram showing ECN deployment from 2000 to 2396 (Sigcomm #411).]
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
Client initiates ECN-capable communication by setting appropriate bits in the TCP SYN packet's **TCP header**.
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?
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Outdated Implementation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

Outdated implementation can cause drastic performance degradations

All SYN packets are dropped

Drop/mark rate

100%

max_p

operating point

min_th max_th

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

SYN ACK packets are NOT dropped
Incremental Deployability

- Scenario

- x% clients: ECN
  (100-x)%: no ECN

ECN+ at servers

ECN at routers

Client pool

Server pool
5% Deployment

Instant gains for ECN-enabled clients
50% Deployment

Gradual degradation for clients not applying ECN
95% Deployment
Testbed Experiments

Client -> 10 Mbps requests -> router

ECN

responses (15 Mbps)

100 Mbps Server pool

Server

no ECN

ECN

ECN+

Server

Server

Server
ECN and Flash Crowds

<table>
<thead>
<tr>
<th>Setup</th>
<th>Average Response Time</th>
<th>Throughput (% of capacity)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RED, no ECN</td>
<td>26 sec</td>
<td>44%</td>
</tr>
<tr>
<td>RED, ECN</td>
<td>4.5 sec</td>
<td>56%</td>
</tr>
<tr>
<td>RED, ECN+</td>
<td>0.5 sec</td>
<td>99%</td>
</tr>
</tbody>
</table>

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