Re-ECN:
Adding Accountability for Causing Congestion to TCP/IP
<draft-briscoe-tsvwg-re-ecn-tcp-03>

Bob Briscoe, BT & UCL
Arnaud Jacquet, Alessandro Salvatori & Martin Koyabe, BT

IETF-67 tsvwg Nov 2006

updated draft 03

- Re-ECN: Adding Accountability for Causing Congestion to TCP/IP
  - **updated draft:** draft-briscoe-tsvwg-re-ecn-tcp-03.txt
  - **ultimate intent:** standards track
  - **immediate intent:** hold ECN nonce (RFC3540) at experimental
  - **intent over ensuing months:** build a community around the goal of balancing Internet freedom with fairness through IETF standards process
- events since previous draft 02
  - tried to build above community of interest but they don't focus on the IETF
    - operators, researchers
  - those who do focus on the IETF have a different religion
    - hence "Flow rate fairness: dismantling a religion"
    - draft-briscoe-tsvarea-fair-00.pdf (presented yesterday in tsv-area)
    - see what effect this has on likelihood of forming community
  - revisions to draft (this presentation)

re-ECN recap: solution statement (§1)

- current Internet gives freedom but no fairness
  - the more you take, the more you get; the more polite you are, the less you get
  - but we don't want to lose freedom by enforcing fairness
- solution: allow ISPs to enforce user-specific congestion control fairness

conservative acceptable use policies
  - might want to throttle if unresponsive to congestion (VoIP, video, DDoS)

middle ground
  - might want to cap congestion caused per user (e.g. 24x7 heavy p2p sources, DDoS)
  - evolution of hi-speed/different congestion control

liberal acceptable use policies
  - open access, no restrictions

- IETF shouldn't pre-judge answer to these socio-economic issues
  - Internet needs all these answers – balance to be determined by natural selection
  - 'do-nothing' doesn't maintain liberal status quo, we just get more middlebox kludges
- re-ECN at network layer: goals
  - just enough support for conservative policies without breaking 'net neutrality'
  - nets that allow their users to cause congestion in other nets can be held accountable

new appendix “Argument for holding back the ECN nonce” (§AI)

ECN nonce status

- RFC3168 Addition of ECN to IP (proposed std)
  - reserves codepoint for ECN nonce (no stds language)
- RFC3540 ECN signalling with Nonces (experimental)
  - specifies nonce for TCP/IP (no stds language)
- RFC4340 DCCP (proposed std)
  - “DCCP sender SHOULD set ECN nonces ...”
- RFC4341 TCP-like cc profile for DCCP (proposed std)
  - “The sender will use the ECN Nonce ...“
- RFC4342 TFRC cc profile for DCCP (proposed std)
  - “The sender [uses] ... ECN Nonce Echoes ...”
- running code?

new appendix “Argument for holding back the ECN nonce” (§AI)

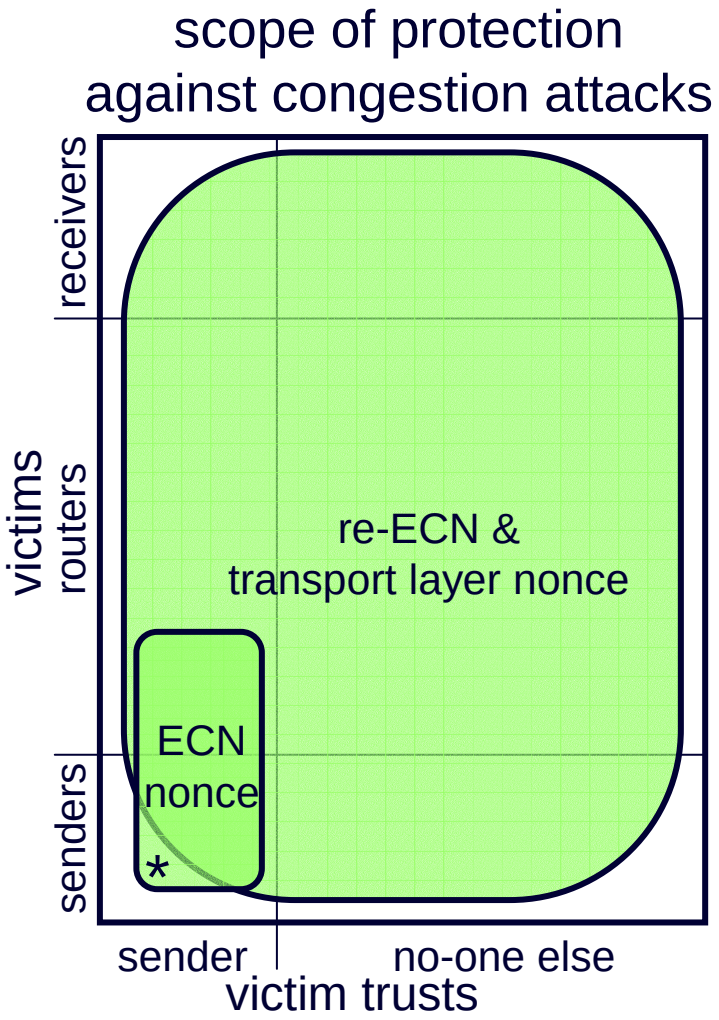
ECN nonce usefulness

- attack detected: suppression of congestion info in f/b loop
  - detection of attack: only by the sender
  - potential attackers: other routers, receivers, or senders
  - who stands to gain: sender and/or receiver
- potential victim of attack: a congested router
  - victim relies for defence on potential attacker, who gains from the attack
    - responsible servers are possibly an important set of senders
    - router only defended if *all* senders behave responsibly
  - alternative: re-ECN protects against all suppression of f/b
    - and against senders not responding to the f/b
- potential (secondary) victim of attack: sender’s transport
  - assumes sender shares its *own* resources only based on each flow’s *network* congestion
    - without a sharing policy for its own congestion
    - the ECN nonce allows such a sender to limit receivers who lack feedback integrity
  - alternative: a nonce at the transport layer ‘would’ give the same protection...
    - detects early acks
    - detects suppression of feedback about drop
      - but not suppression of ECN feedback

new appendix “Argument for holding back the ECN nonce” (§AI)

ECN nonce usefulness

- re-ECN and a transport layer nonce defend against wide range of attacks
  - ECN nonce defends against a small subset
  - and only one outside re-ECN’s range (*)
    - a sender that uses network ECN to allocate its own resources, can limit a lying receiver
    - sender can contain this attack without nonce
- IP header bits used to do this:
  - ECN nonce $^1/_4$b (leaving last bit)
  - re-ECN $^3/_8$b (using last bit)
- one common codepoint
  - re-ECN negotiates its use, but ECN nonce doesn’t
- propose to hold back ECN nonce
  - to see if we can find a coding to do both
  - to see if we can prevent (*) another way
  - develop a transport layer nonce



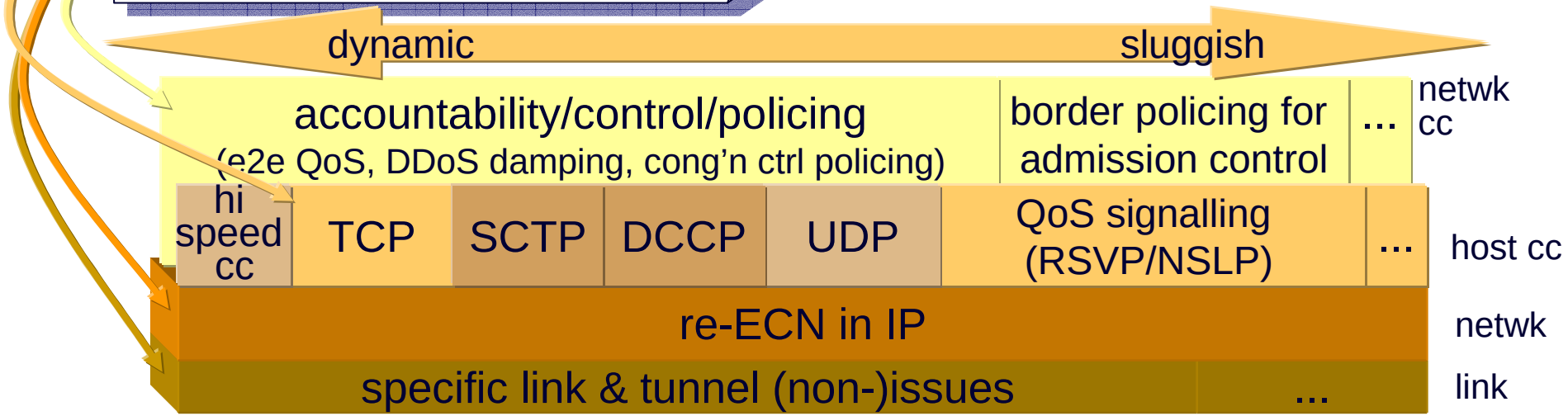
recap doc roadmap

Re-ECN: Adding Accountability for Causing Congestion to TCP/IP
draft-briscoe-tsvwg-re-ecn-tcp-03

intent

§3: overview in TCP
§4: in TCP & other transports
§5: in IP
stds

§6: accountability apps *inform'l*



guidelines for adding re-ECN to other transports

- main focus of <draft-briscoe-tsvwg-re-ecn-tcp-03>
  - IP (§5)
  - TCP (§4.1)
- added very brief sections giving guidelines for
  - DCCP (§4.2.3)
  - SCTP (§4.2.4)
  - spec would have to be a new I-D in each case
- focus of <draft-briscoe-tsvwg-re-ecn-border-cheat-01>
  - RSVP/NSIS transports (‘re-PCN’)
  - proposed technique to extend PCN-based admission control
    - Internet wide (edge-edge) – many untrusting domains
- our current focus
  - controlling fairness between current transports & hi-speed congestion control

Re-ECN:
Adding Accountability for Causing Congestion to TCP/IP

<draft-briscoe-tsvwg-re-ecn-tcp-03>

Q&A