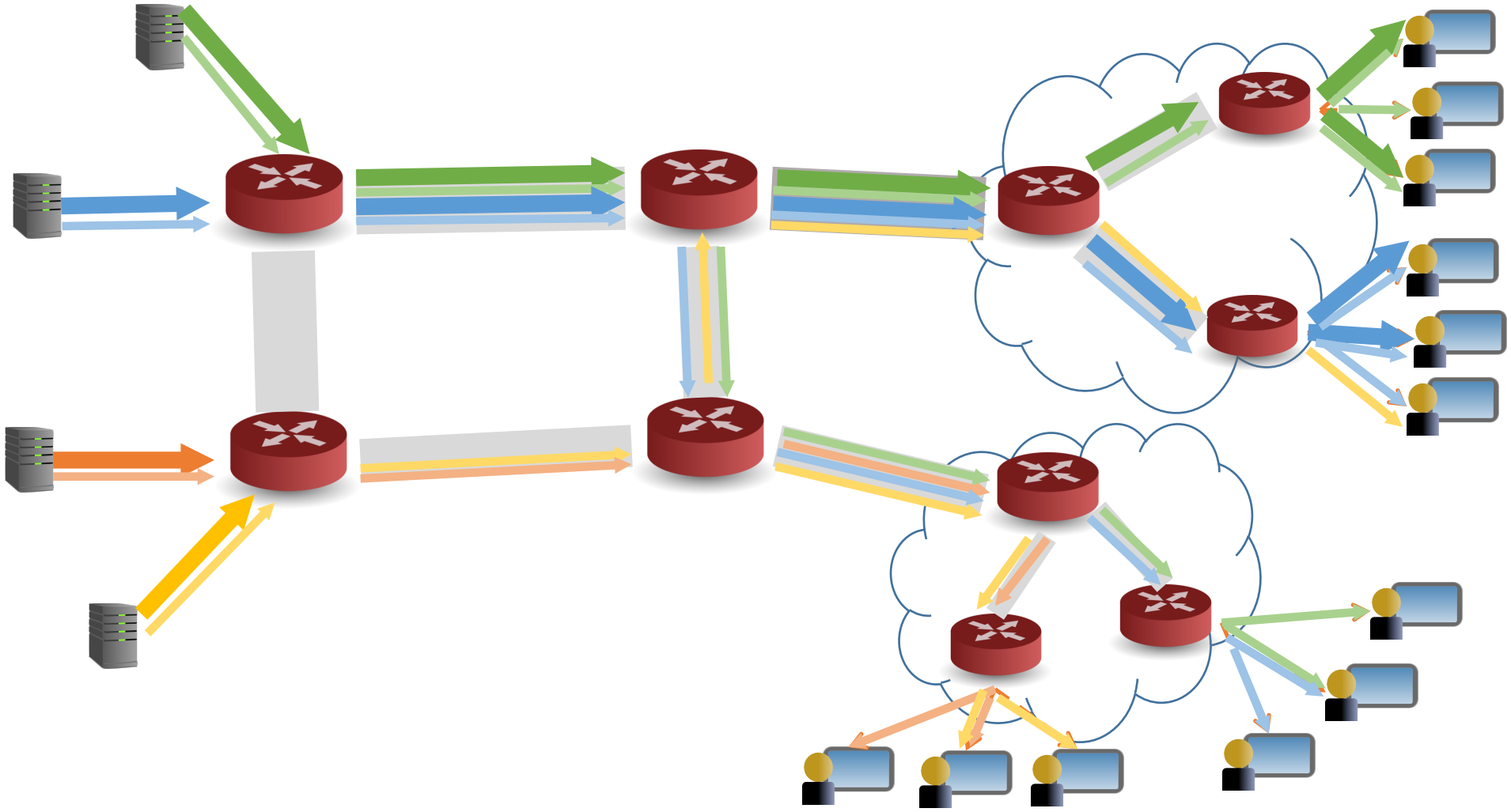
Malicious Overjoining in Multicast

Problem and proposed solution

draft-jholland-cb-assisted-cc

Jake Holland, Akamai Technologies

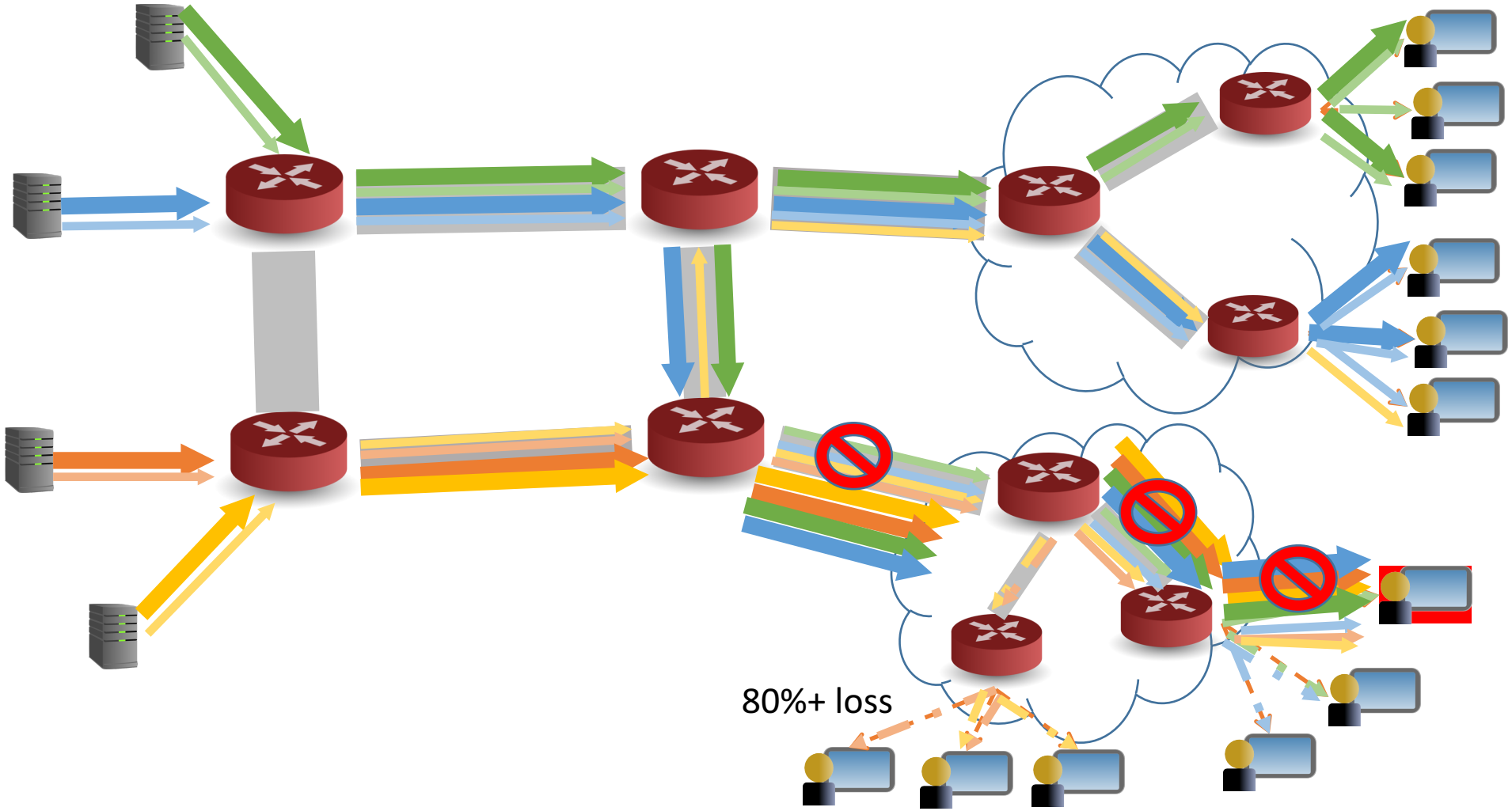
Multicast Utopia



Elements of trouble

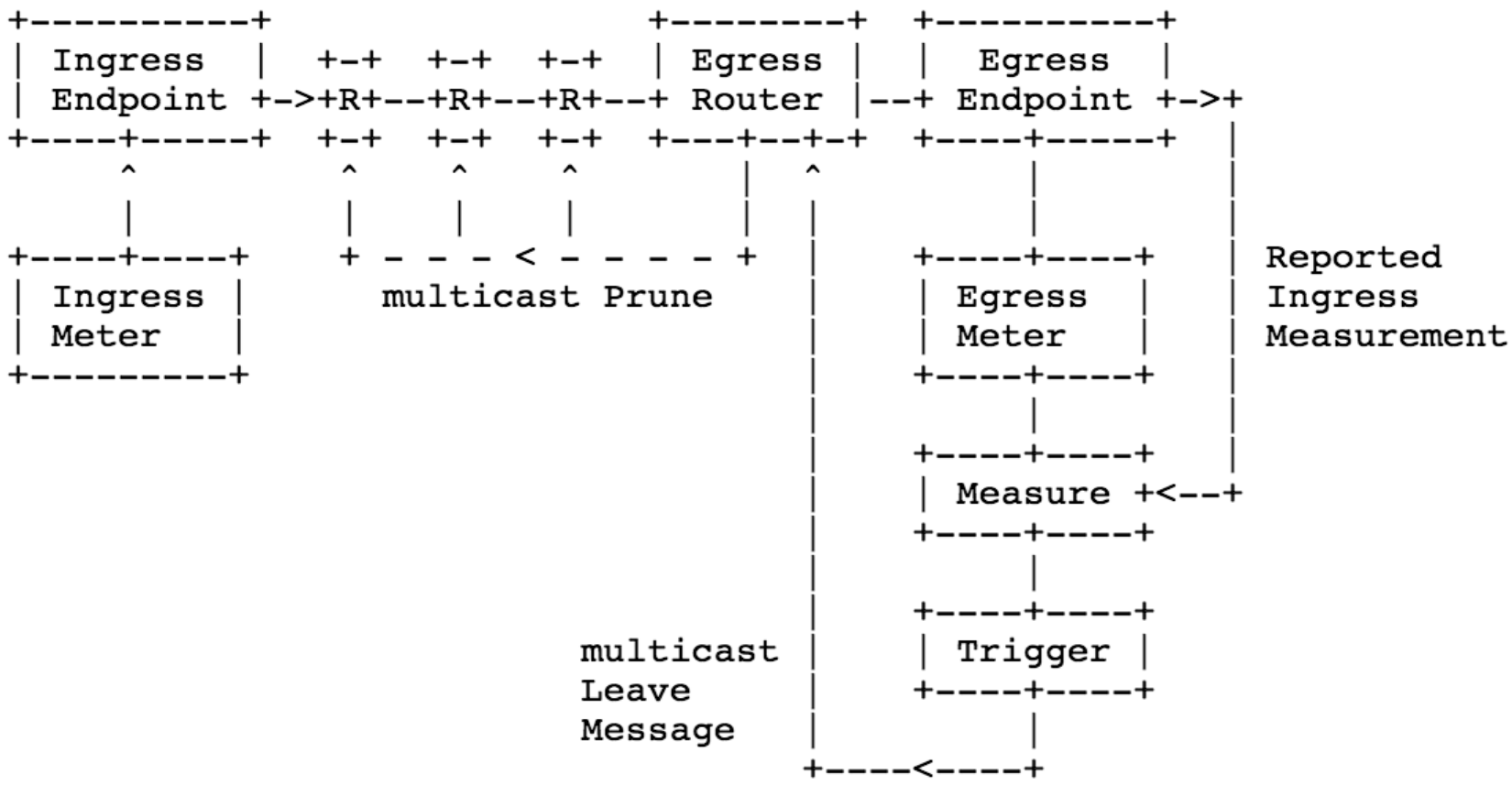
- sending rate does not respond to receivers that don’t feed back
- congestion control depends on well-behaved receivers
  - receiver-based: WEBRC [RFC 3738] (building block of ALC [RFC 5775])
  - feedback-based: NORM [RFC 5740]

Multicast with one Compromised Machine



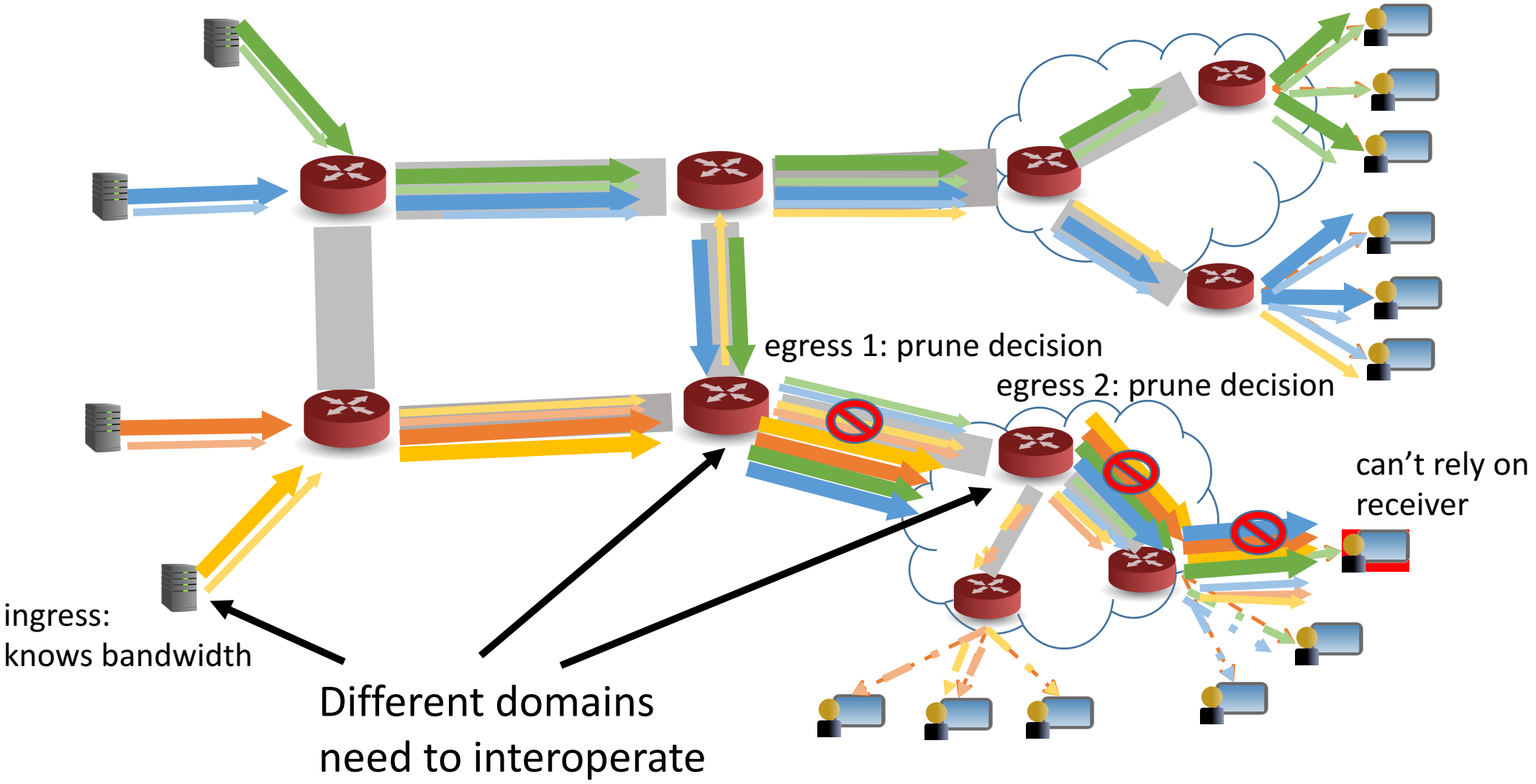
Solution: Circuit Breaker

3.2.1. Use with a multicast control/routing protocol



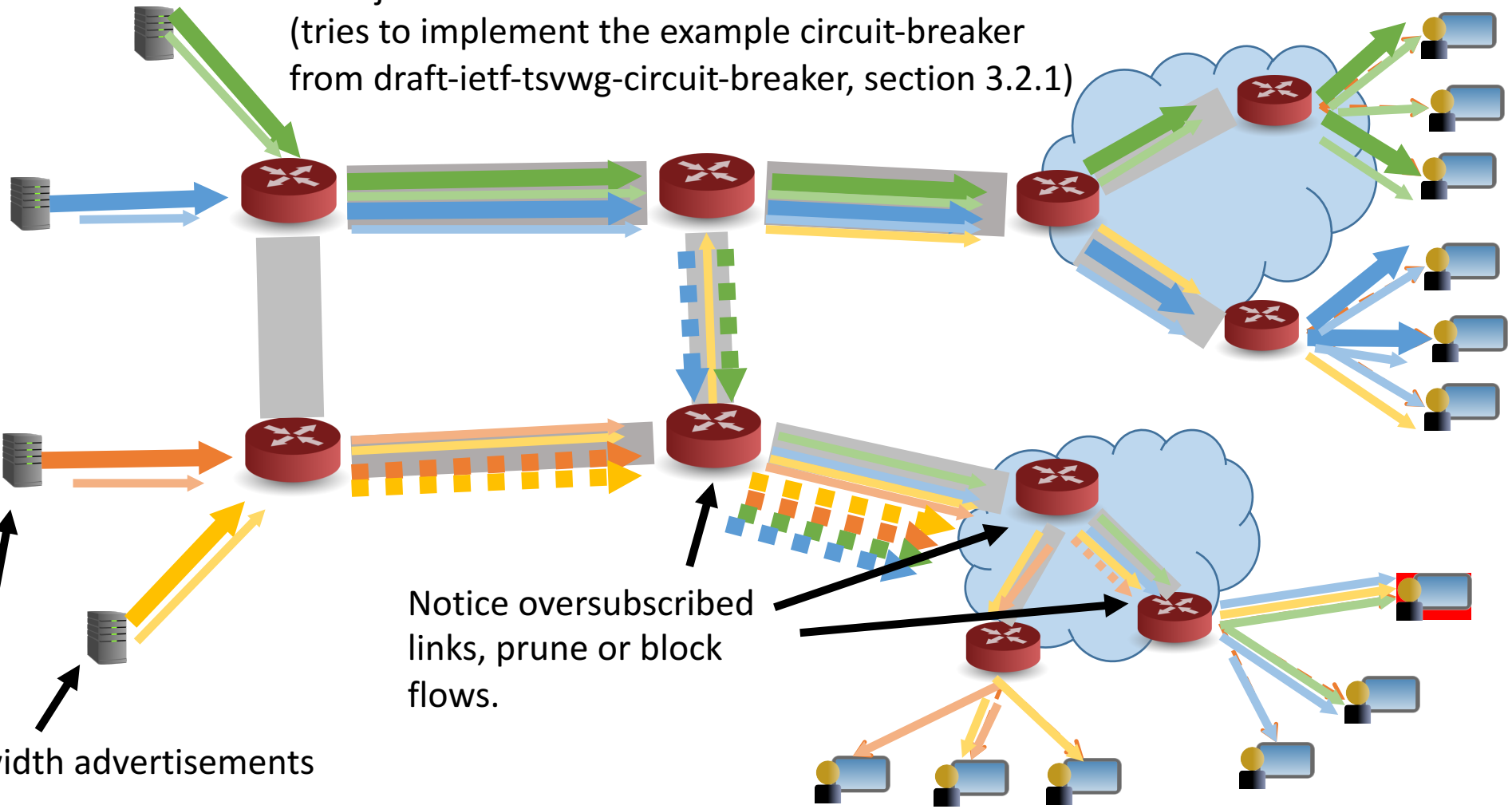
From draft-ietf-tsvwg-circuit-breaker-15

Why it needs to be a standard



Circuit Breaker Assisted Congestion Control

draft-jholland-cb-assisted-cc:
(tries to implement the example circuit-breaker
from draft-ietf-tsvwg-circuit-breaker, section 3.2.1)



Send bandwidth advertisements

Notice oversubscribed
links, prune or block
flows.

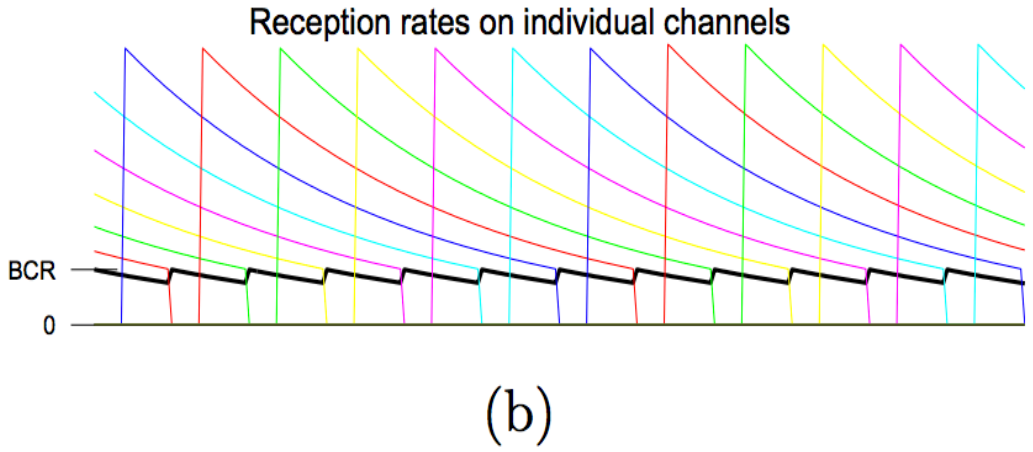
+ optional PIM population count for fair pruning decisions
(RFC 6807, experimental)

Receiver-driven Congestion Control

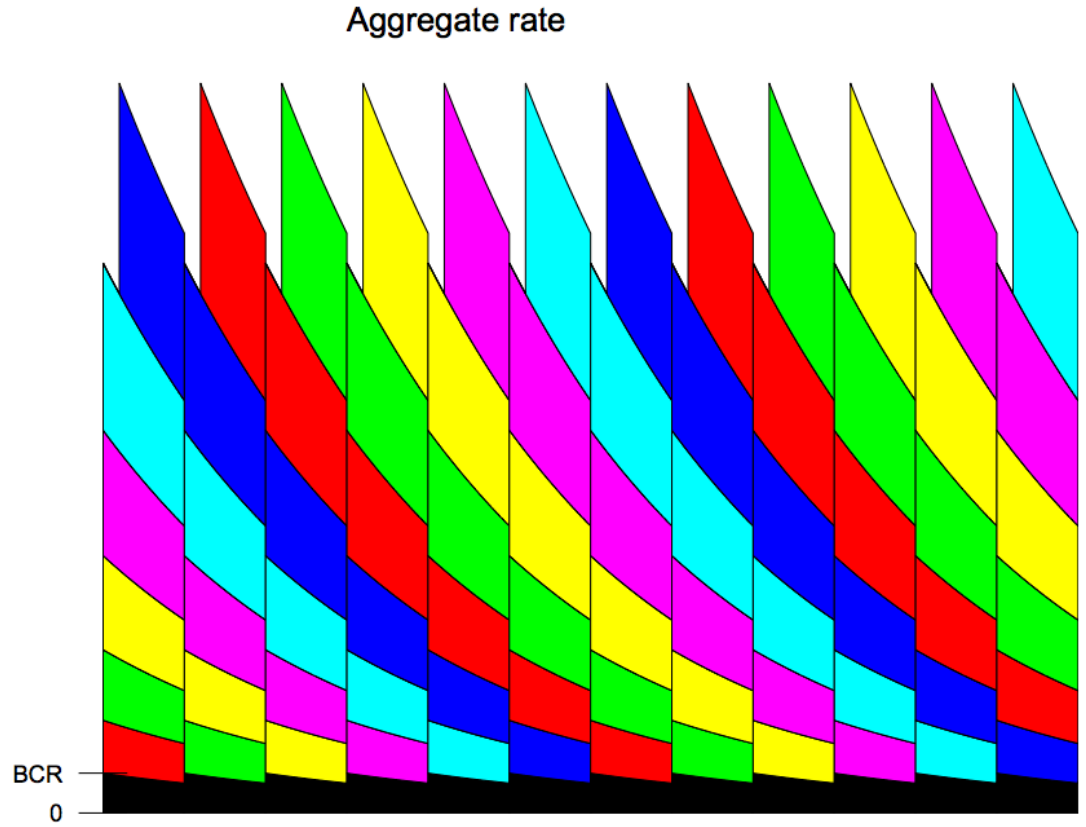
- WEBRC: RFC 3738 (experimental), 2002
  - referenced by ALC: RFC 5775 (proposed standard)

- RLM (McCanne, Vetterli, Jacobson, 1996)
- RLC (Iannaccone, Rizzo, 1999)
- PLM (Legout, Biersack, 2000)
- FLID-DL (Byers, Horn, Luby, Mitzenmacher, Shaver, 2002)
- PSLM (Li, Munro, Kaleshi, 2005)

WEBRC (receiver view)



(b)



Images: Luby, M. and V. Goyal, "Wave and Equation Based Rate Control Using Multicast Round Trip Time: Extended Report", p6

WEBRC (sender view)

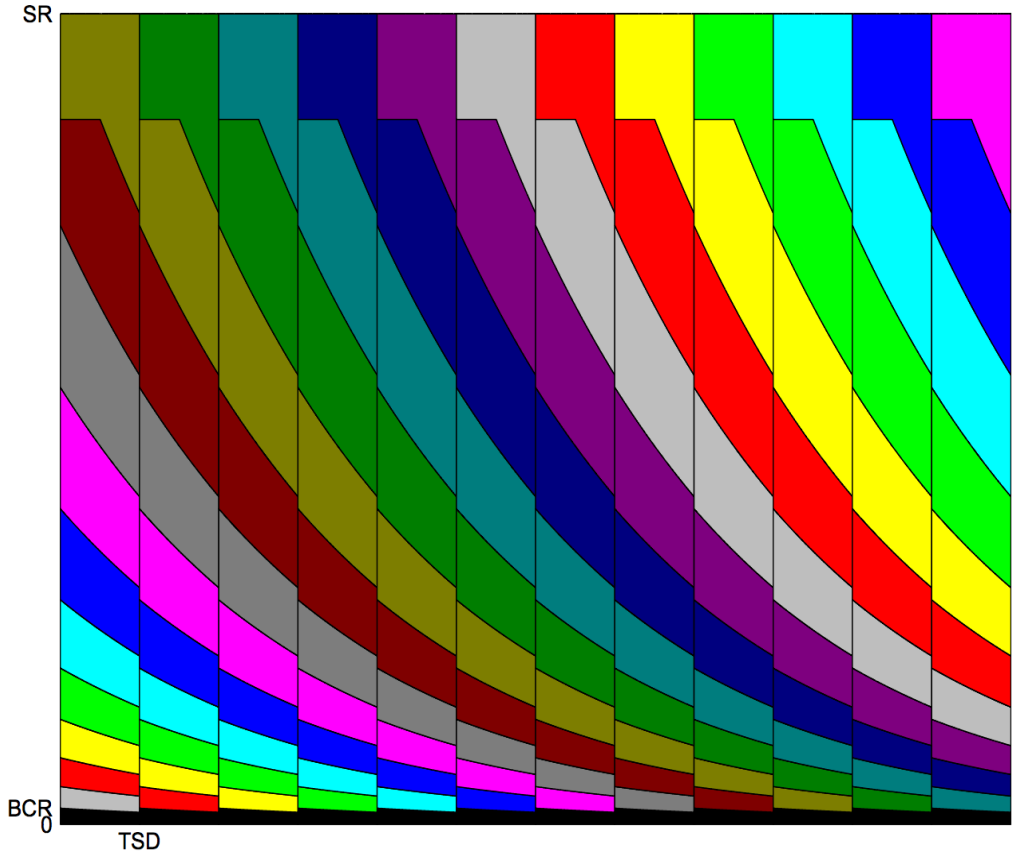


Fig. 15. Server output totalled over all channels is constant. Here

Non-responsive if receiver doesn't leave.

"Note there is no way at the transport layer to prevent a join message propagating to the next-hop router."
- draft-ietf-tsvwg-rfc5405-bis-19, 4.1

Image: Luby, M. and V. Goyal, "Wave and Equation Based Rate Control Using Multicast Round Trip Time: Extended Report", p20

Non-solutions

- Limit the group count for receivers
  - attacker joins only higher-bandwidth flows
  - a few compromised machines join disjoint sets of flows
  - attack capacity is total bandwidth from active senders on the internet
- Use feedback-driven congestion control instead
  - vulnerable to DOS by under-reporting rate
  - If anyone can receive HD video, you still have the same problem (attacker joins high-bandwidth flows and doesn't feed back)
  - can't scale as well
- Bandwidth limit for multicast (or UDP)
  - this is still a DoS for multicast (though it does keep the network safe)