Prefix Hijacking Mitigation
Something is better than nothing

James Cowie, Renesys
Tom Daly, Dynamic Network Services
Anton Kapela, Voxel
Todd Underwood, Google

NANOG 46 – June 2009

DYNAMIC NETWORK
SERVICES INCORPORATED

Outline

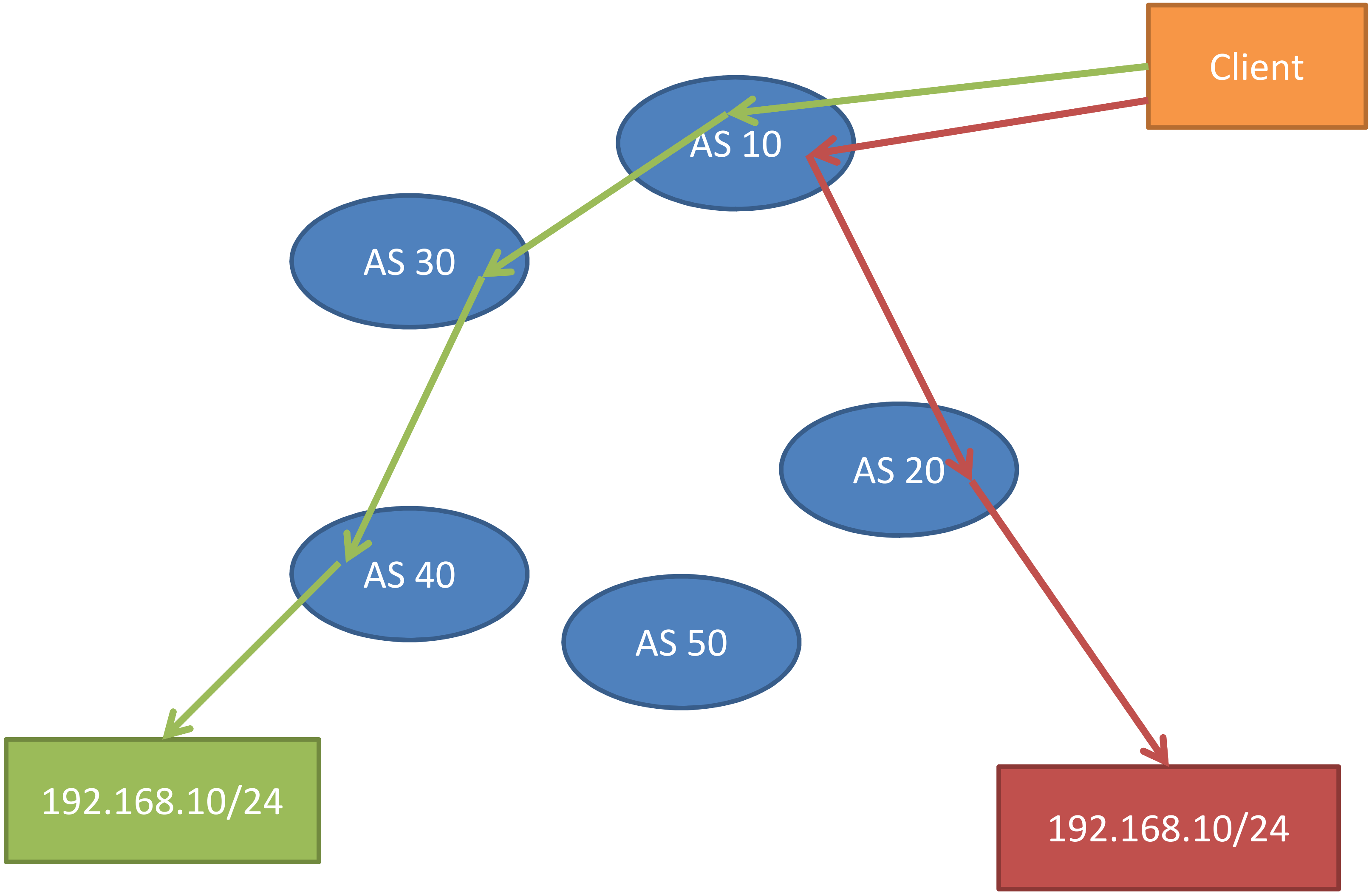
- Introduction to prefix hijacking
- Mitigating against an event
- Experiment
- Questions

Prefix Hijacking 101

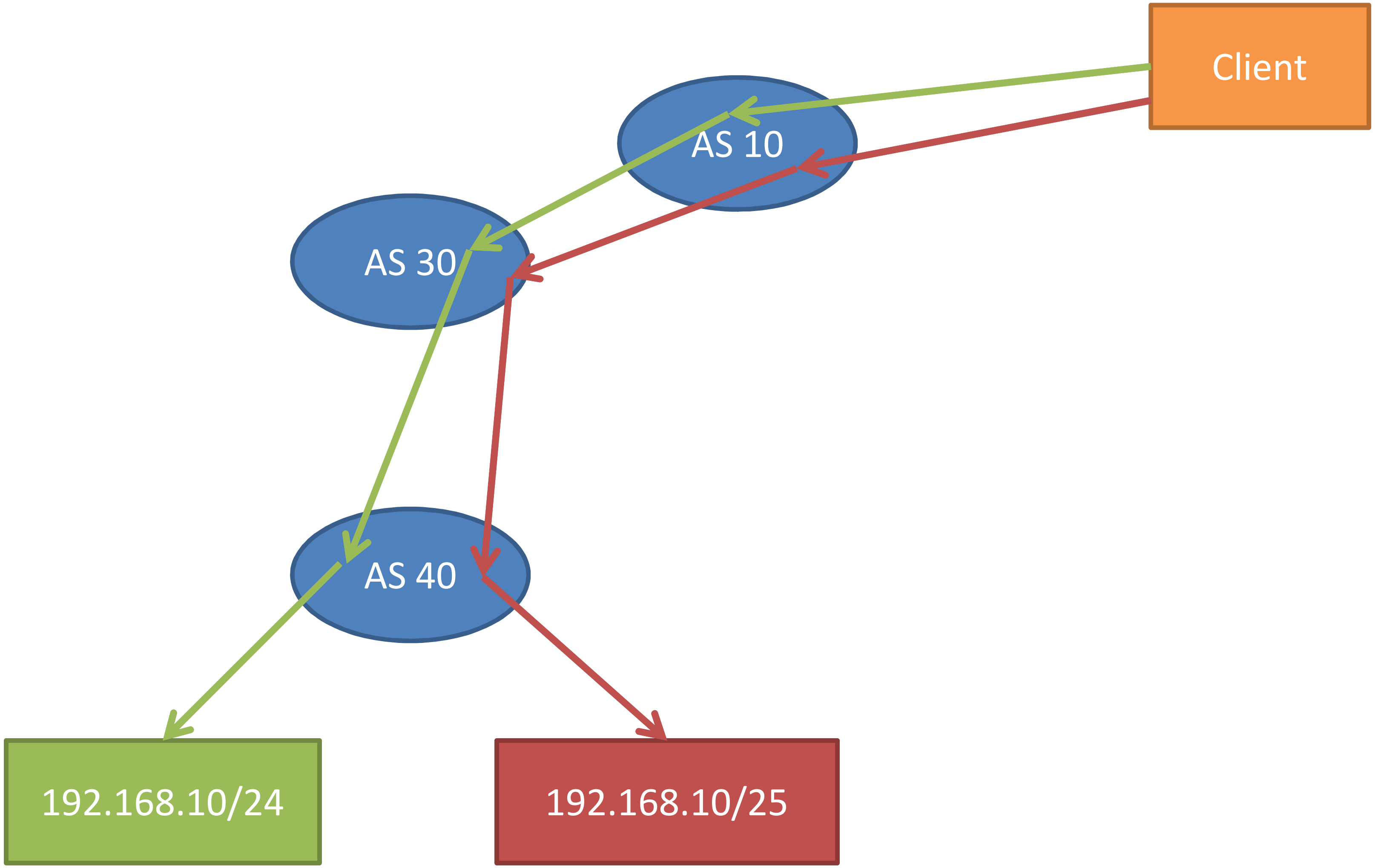
- Announce someone else's prefix
- Announce a more specific of a someone else's prefix

- Synopsis: You are trying to “steal” someone else’s traffic by getting it routed to you.
- Capture, sniff, redirect, manipulate traffic as you wish.

Same Prefix: Shorter AS Path Wins



Same Path: More Specific Prefix Wins



Advanced Hijacking: Pilosov/ Kapela's MITM Attack

- http://eng.5ninesdata.com/~tkapela
- Create a new path for the hijacked traffic
- Copy/observe/record traffic
- Return it to the rightful originator
- Hide your tracks
- Includes prepending ASes along the return path and TTL modification for traceroute hiding

Impact

- IP space that is in-use: (obvious operational impact)
  - Disrupts traffic, denies service to the traffic
- IP space not in-use (delayed operational impact)
  - Damage to reputation of the target
- *Either way, you may or may not know it is happening!*

Does It Actually Happen?

- Yes!
  - Famously: Youtube:
    http://nanog.org/meetings/nanog43/presentations/Brownyoutube
    - Also, Yahoo, Google, and many, many others
- Not as often as some people think
    - Certainly not a daily or weekly occurrence
    - It may happen (and is worth preparing for it) but is not the biggest threat you face.
- MITM hijacking unlikely so far

Why Doesn't Someone Fix This?

- We try! Sorta:
- Peers don't route-filter each other:
  - http://www.nanog.org/mtg-0510/deleskie.html
- No trust anchors built into the allocation/routing system from the start:
  - Randy Bush asked for one as an Eid present: www.nanog.org/mtg-0602/pdf/bush.pdf
  - Didn't happen 2006, 2007 or 2008
- No way to validate routes in flight:
  - SBGP, soBGP never implemented

Mitigation Overview

- Prepare (most important)
  - Detect
  - Investigate
  - Mitigate (novel suggestion for how)
  - Clean up

Mitigation 0: Prepare

- Ensure prefixes are all provably yours:
  - Gather allocation/SWIP documentation
  - Gather electronic versions of any LOAs from customers
- Register prefixes in IRRs
- Ask providers to accept le /25 and test acceptance and propagation of the /25s in advance
- Ask provider about response procedures to hijackings, DOSes

Mitigation 0: Prepare (cont.)

- Do not put important resources in the same prefixes:
    - Youtube ran DNS in the same prefixes as web/video previously. Limits the scope of damage.
- Providers and peers should be selected on the basis of clue in dealing with this.
- Join security groups, if possible.
- Most importantly: build relationships with as many engineers/managers at major networks as possible. There are the people that are going to help you when this happens to you!

Mitigation 1: Detect (quickly!)

- There are lots of tools that can do this for you. Pick one (or two) and use them.
  - RIPE RIS
  - PHAS
  - BGPMon
  - Renesys
  - Something home grown

Mitigation 1: Detection (How)

- Change in origin ASN
- Change in route propagation through unauthorized / unknown peers
- Origination of a more specific prefix
- Traffic monitoring, etc.

Mitigation 2: Investigate

- Make sure it's a hijacking
- Make sure you understand who is responsible and what routes they are sending to whom
- Gather your evidence carefully

Mitigation 3: Mitigate

- Originate more specifics. Up to those /25s you tested. This *may* help you get your traffic back.
- Contact the “nearest responsible large provider” to the hijack, asking them to route filter.
- Work upstream from yourself and the hijacker, asking for filtering.
- Your RIR/IRR/LOA data may be critical here.

Mitigation 4: Clean Up

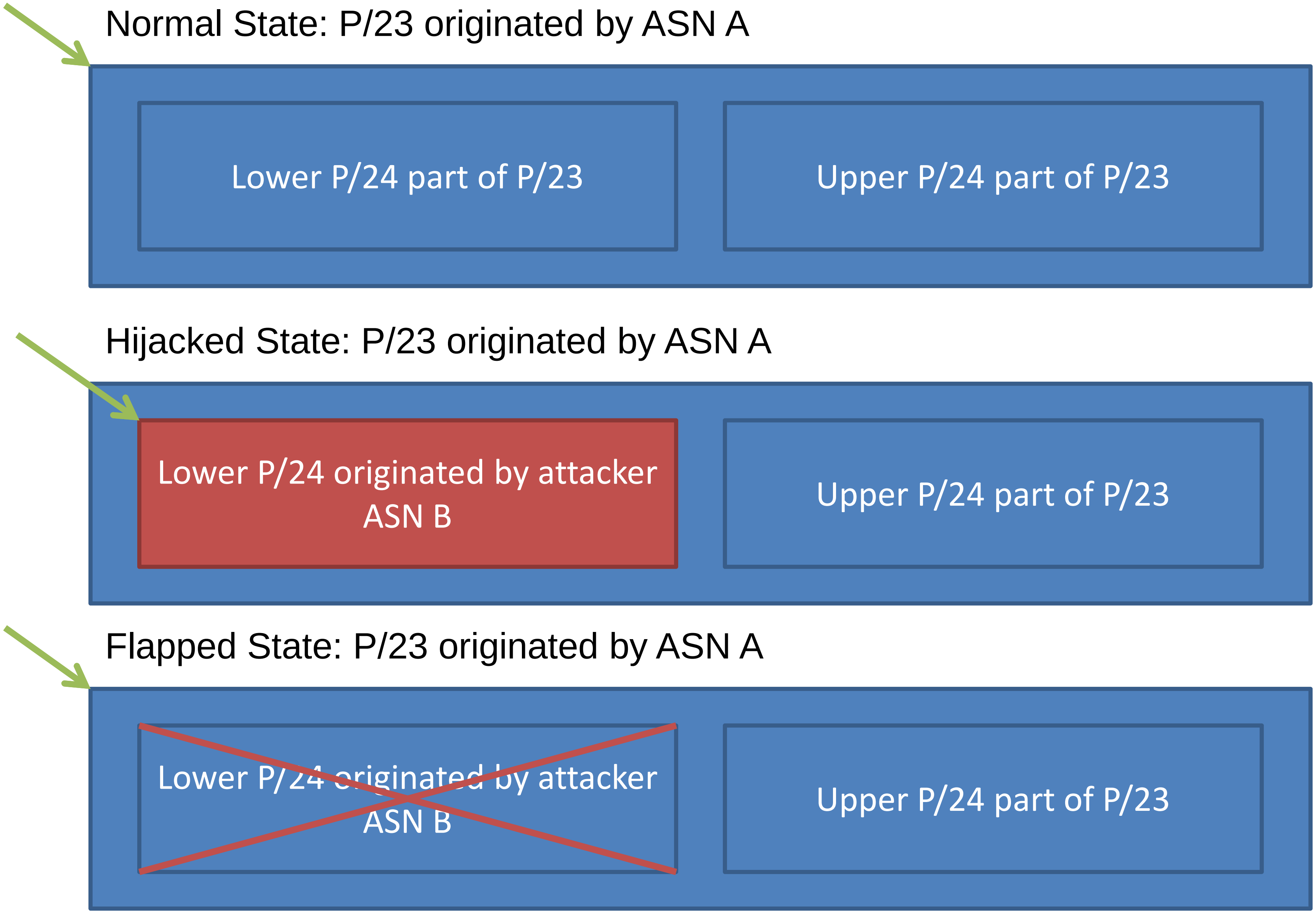
- Get attacker to stop announcing prefixes.
- Get attacker’s upstream to properly filter the attacker.
- Stop originating more specifics from your own network.
- Thank everyone who helped, profusely. Buy them beverages. You'll need their help again soon.

Hypothesis

- Can the affects of route flap dampening be used to mitigate a prefix hijacking?

Mitigation: The Flapping

- Novel concept: flap the hijacked more specific
- Assuming:
  - P/23 is the covering prefix originated by ASNA
  - P/24 is originated from hijacker ASNB
- ASNA should originate and then flap P/24
- P/24 should be flap dampened (at least somewhat) and the covering /23 will catch the traffic



Normal State: P/23 originated by ASN A

Lower P/24 part of P/23

Upper P/24 part of P/23

Hijacked State: P/23 originated by ASN A

Lower P/24 originated by attacker ASN B

Upper P/24 part of P/23

Flapped State: P/23 originated by ASN A

~~Lower P/24 originated by attacker ASN B~~

Upper P/24 part of P/23

Flapping: An Experiment

- The Players:
  - AS33517: Dynamic Network Services
    - Has 216.146.34.0/23, originates 216.146.34.0/23 and 216.146.35.0/24
  - AS16842: Five Nines Data
    - Hijacking 216.146.34.0/24
- AS16842 originates 216.146.34.0/24, stealing half of AS33517's /23.
- AS33517 responds by announcing the stolen /24.
- Observe the steady state.

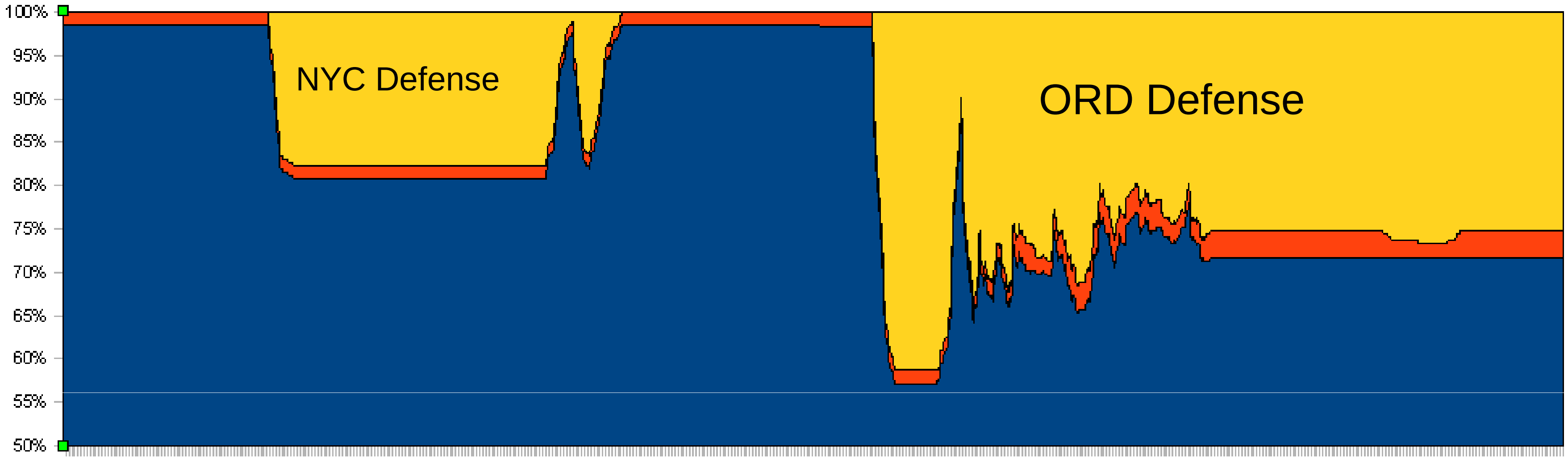
Flapping: An Experiment (2)

- The flapping:
  - AS33517 begins flapping 216.146.34.0/24 in an attempt to suppress the more specific (and get traffic back)
  - Two different geographic sources and rates of flapping were attempted in order to ensure propagation and thresholding did not reduce the effectiveness (NYC and ORD, Quagga and JUNOS)

Flapping: Results/Analysis

- Used BGP update data from Renesys Routing Intelligence and its global peerset.
- Summary: This technique doesn’t work.
  - The rightful owner just becomes a big prefix flapping jerk!

Preliminary Analysis

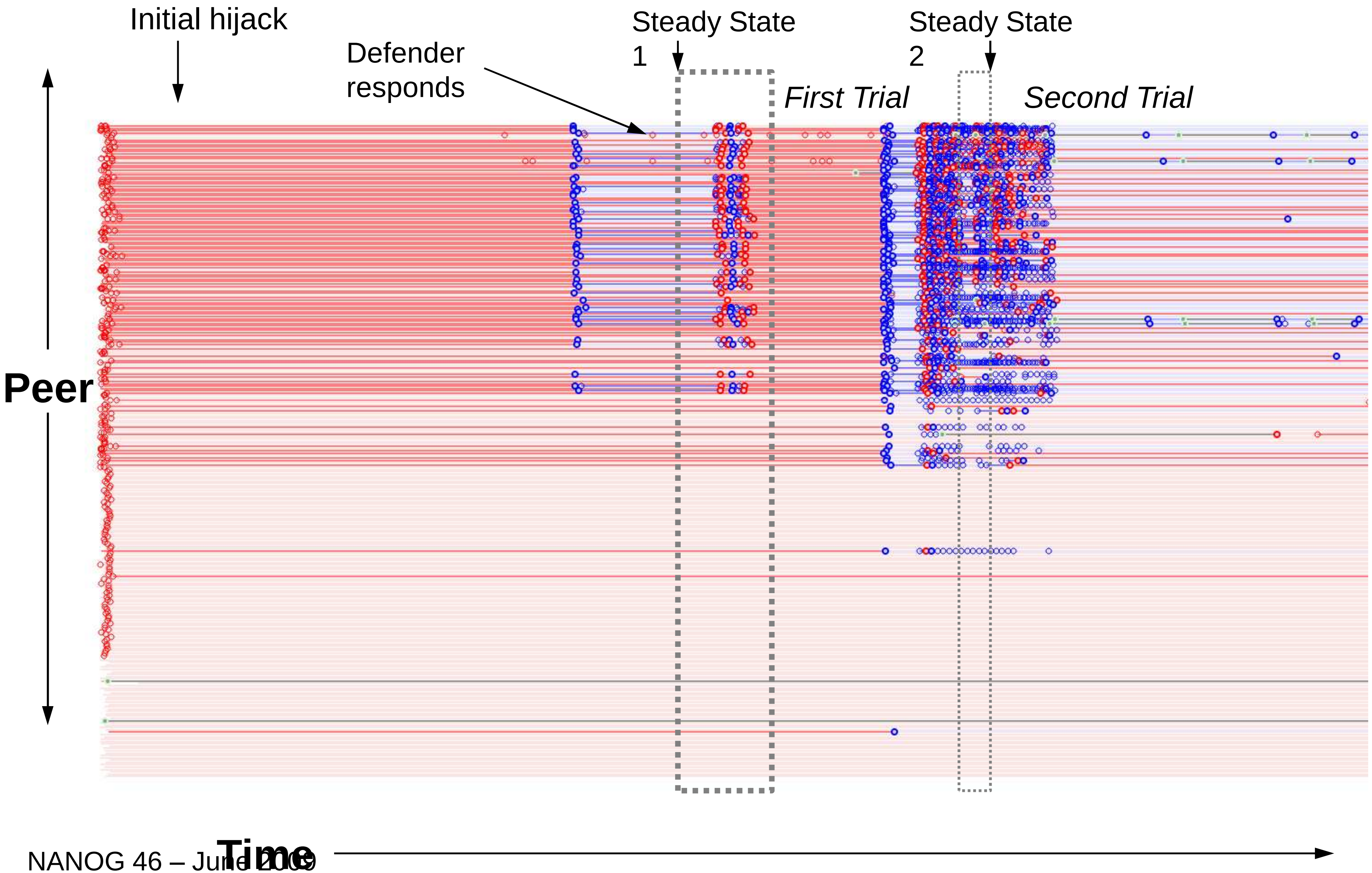


Percentage of peers selecting:

hijacked prefix (AS16842-P/24) in blue
"real" prefix (AS33517-P/24) in yellow
no prefix – withdrawn – in orange

Deeper Analysis

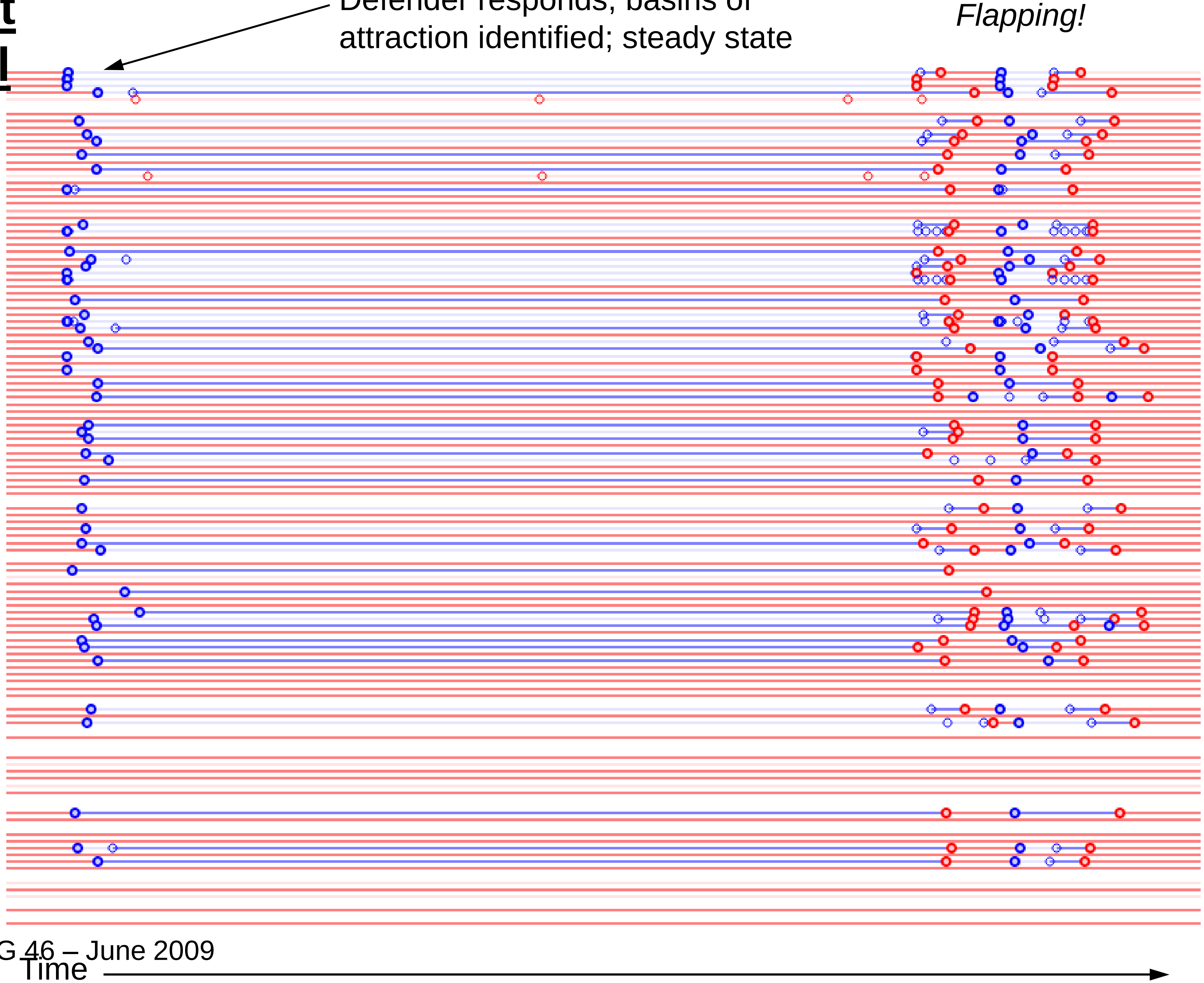
- Horizontal lines are individual peers.
- Each circle is an update.
- First slide shows the whole peer tableau, with the “contested zone” on top, and the “closer to the attacker zone” down below (never in play; note the lack of withdrawals/dampening).
- Subsequent slides zero in on the contested zone, where the defender has a chance.


Initial hijack
Defender responds
Steady State 1
Steady State 2
First Trial
Second Trial
Peer
Time

First Trial

Defender responds, basins of attraction identified; steady state

Flapping!



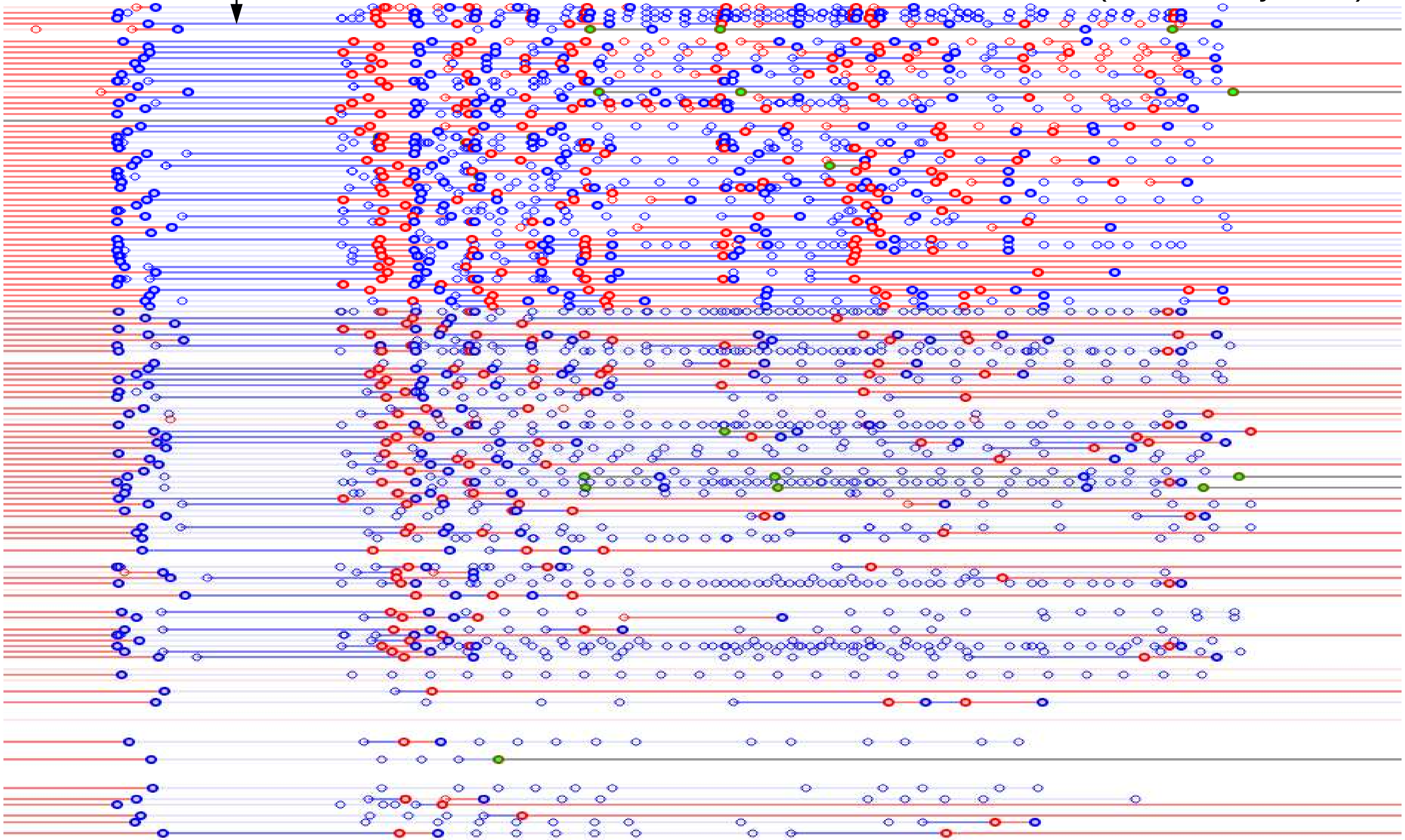
Second Trial

(Steady State)

Flapping! Green circles are (rare) withdrawals.

On balance, blue circles (defender) are
being turned into red circles (attacker), **not** dampened.

Remember, this is the defender's turf to lose (note steady state).



Conclusion

- The steady-state originator always has the advantage (older route in tables)
- In this case, the defender has all the ground to lose.
- Duplicate originations help get some traffic back.
- Flapping severely hurts the defenders attempt to get traffic back.

Open Questions

- Does anyone still flap dampen?
- Does this work at all?
- How much do you have to flap to keep it working?
- Could this strategy be effective?
- Are we all insane for even thinking it would work?

Thank You

James Cowie, Renesys
Tom Daly, Dynamic Network Services
Anton Kapela, Voxel
Todd Underwood, Google