RIPE NCC & BGPlay team investigating on…

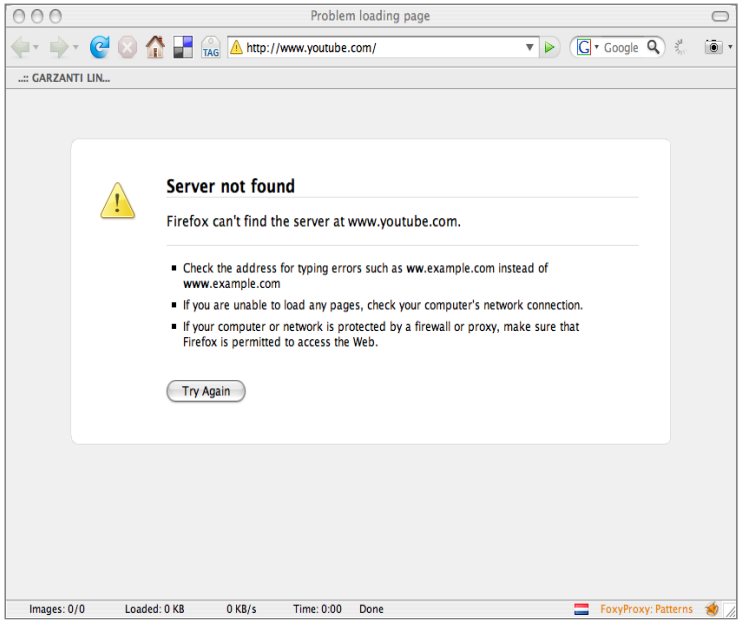
YouTube (Prefix) Hijacking

Tiziana Refice (*Science Group, RIPE NCC*
BGPlay Team, Roma Tre University)

user perspective

YouTube unreachable

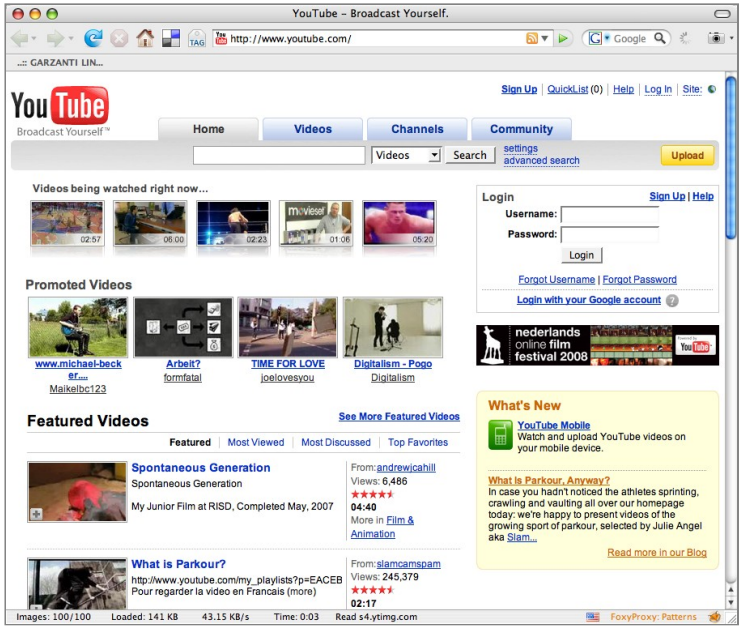
24 February 2008, 18:47 (UTC)



user perspective

Back to normal

24 February 2008, 21:03 (UTC)

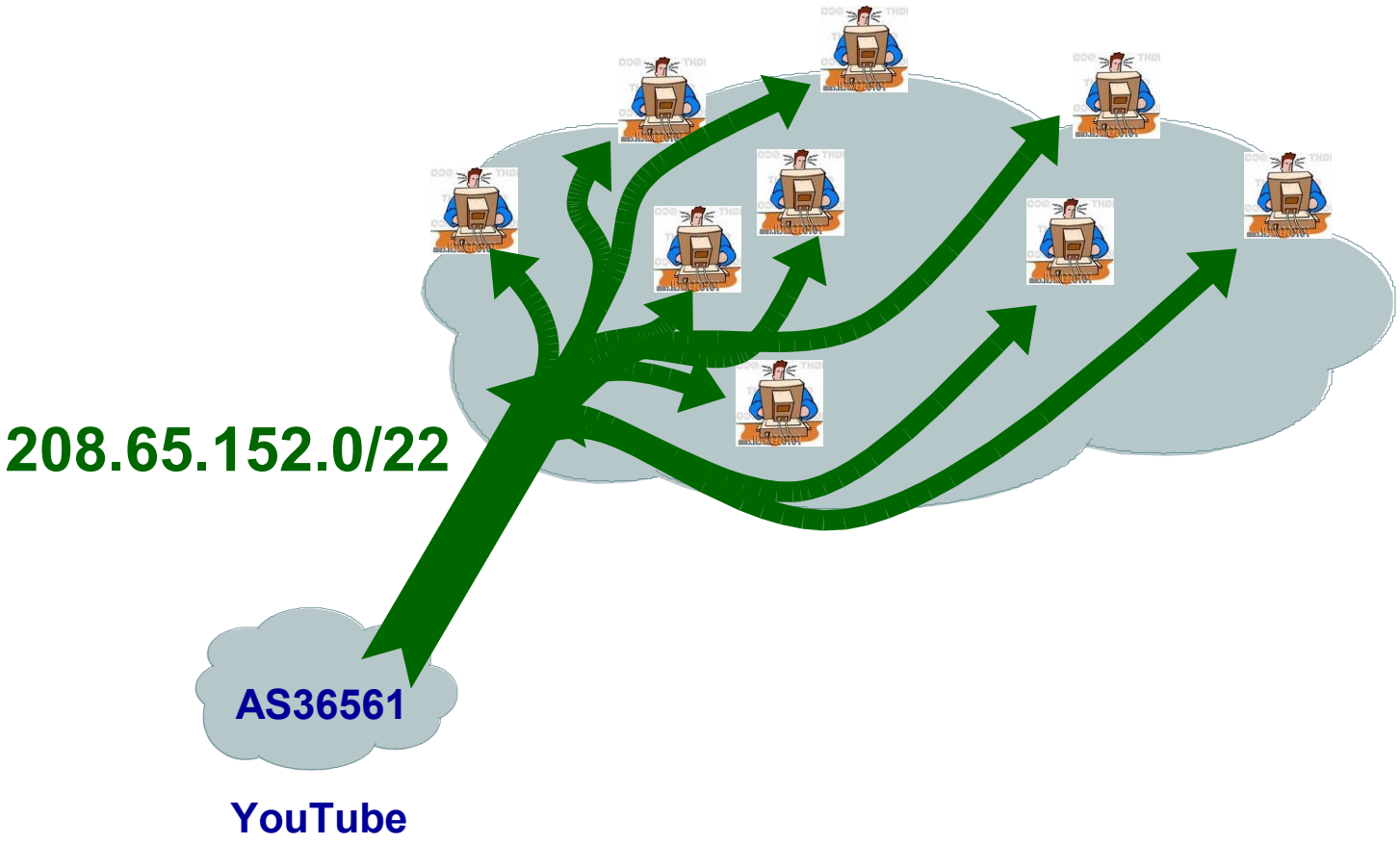


Let's animate the event

- BGPlay video

what happened

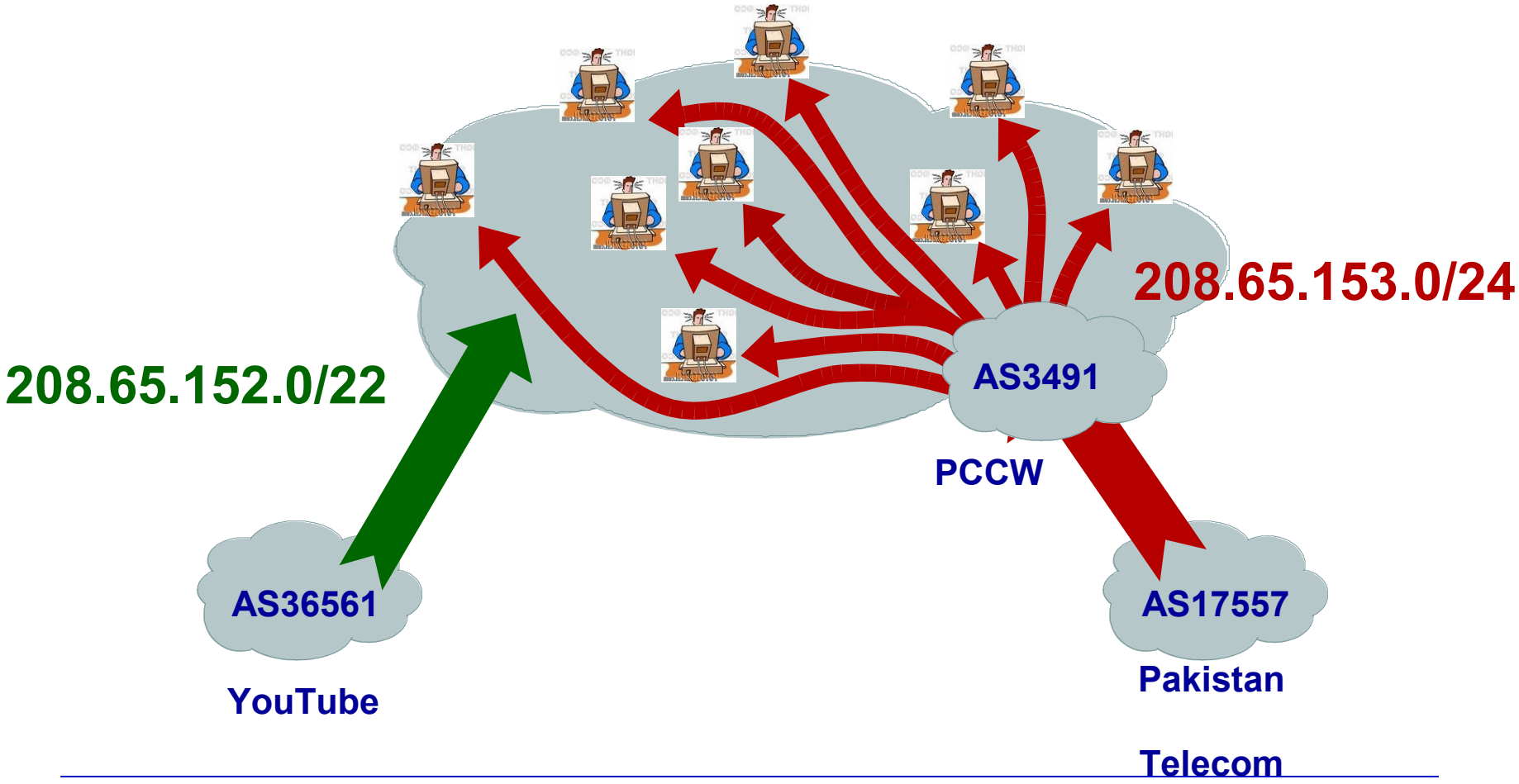
Normal behavior



what happened

Hijacking starts

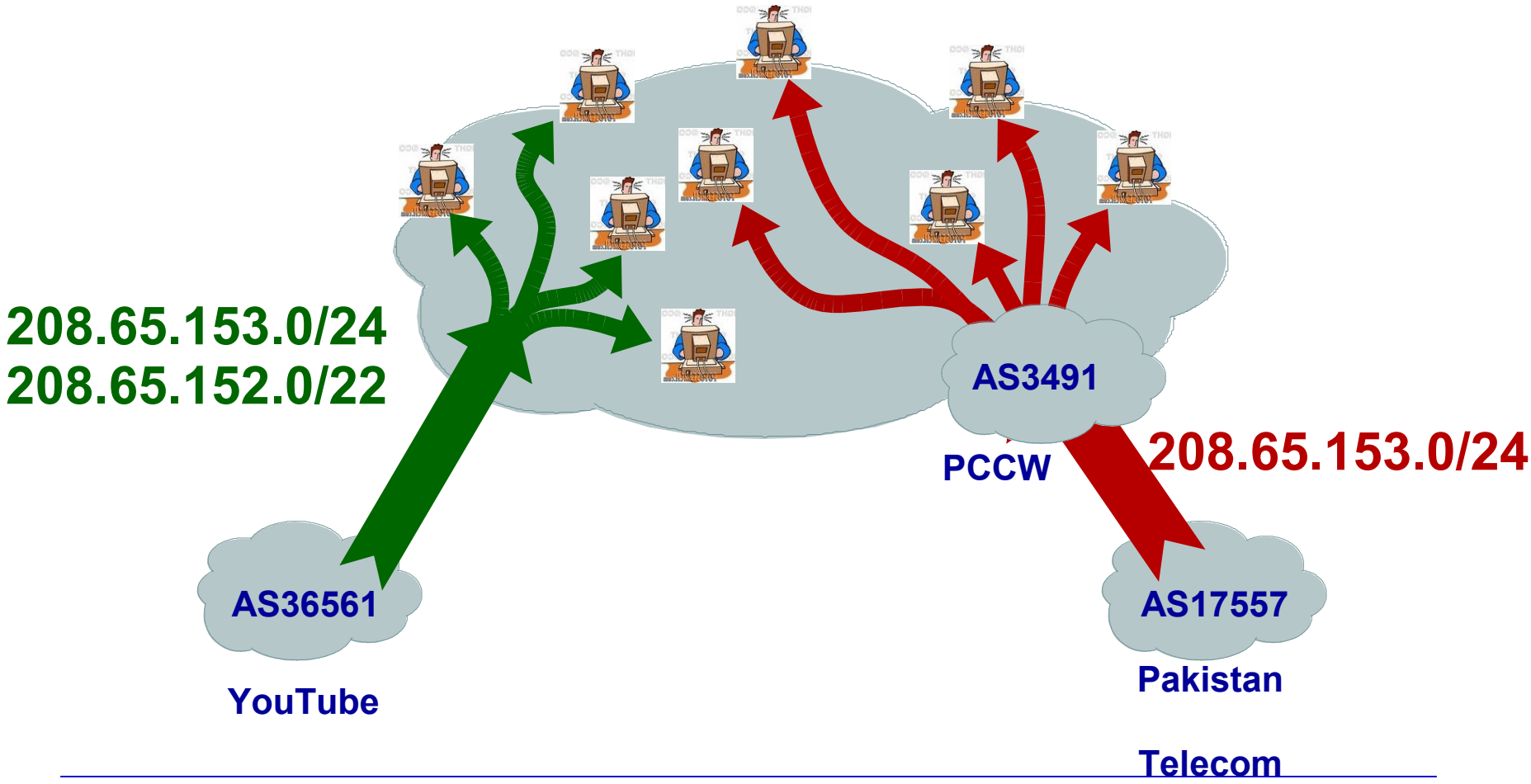
24 February 2008, 18:47 (UTC)



what happened

YouTube announces /24

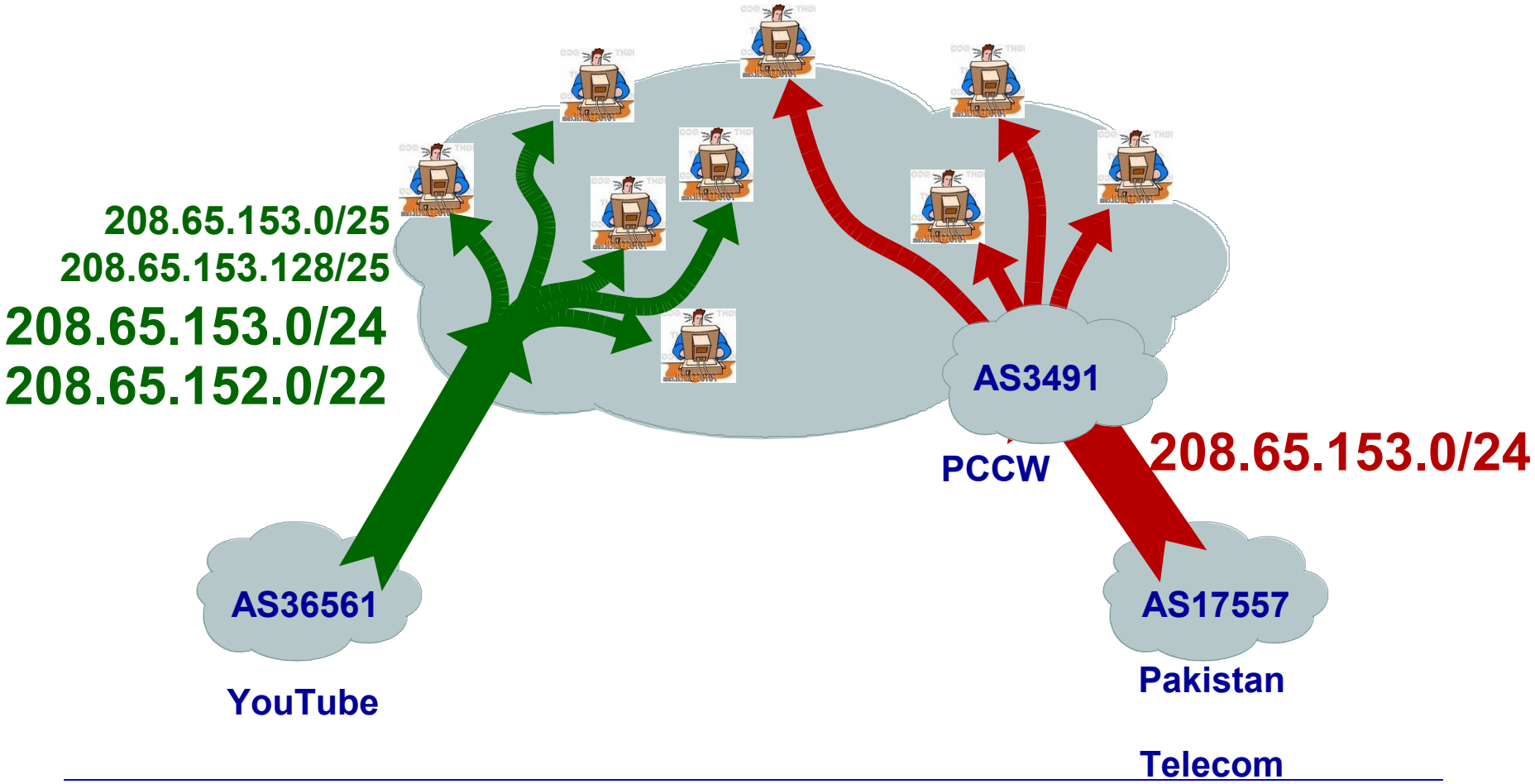
24 February 2008, 20:07 (UTC)



what happened

YouTube announces /25s

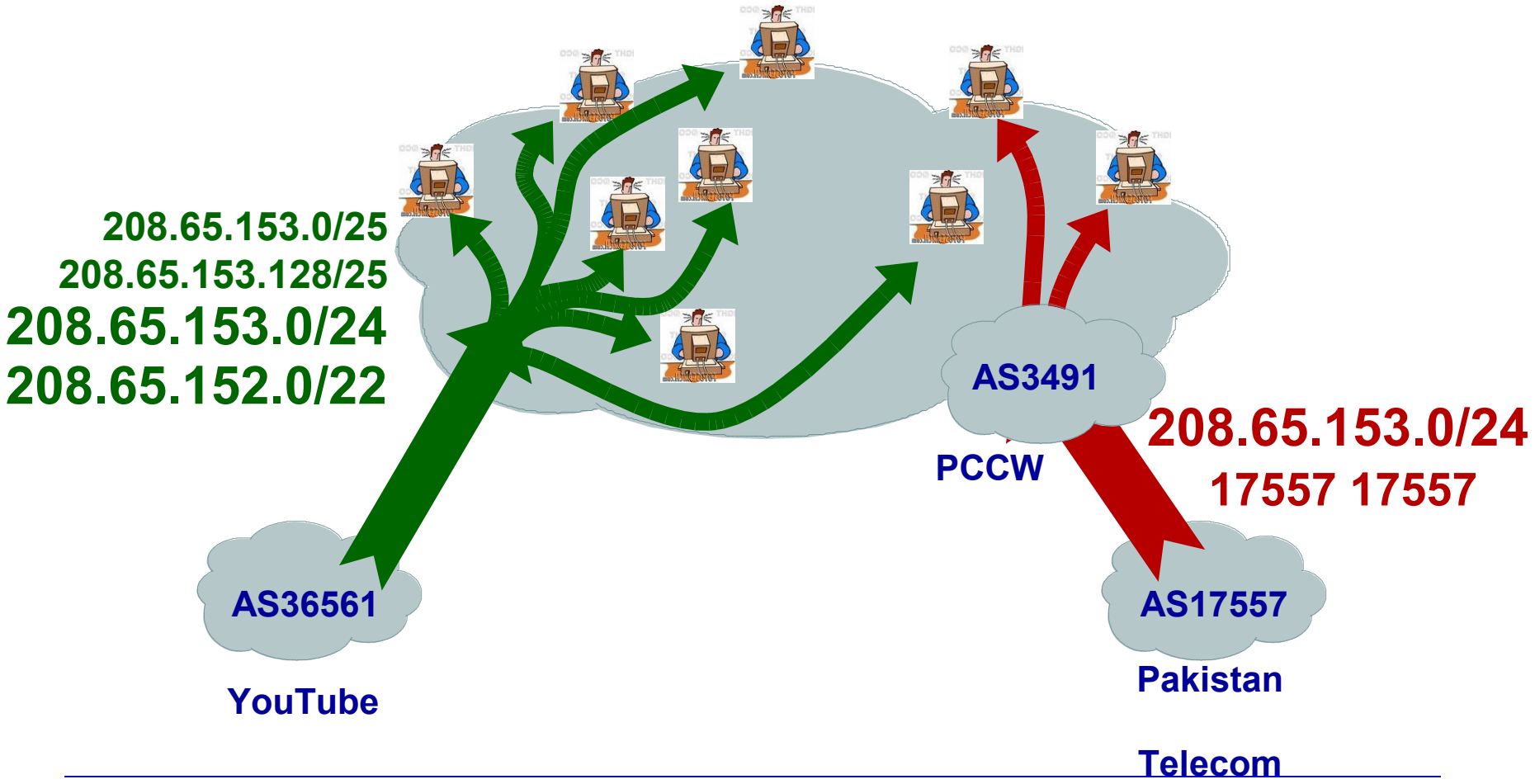
24 February 2008, 20:18 (UTC)



what happened

AS17557 prepending

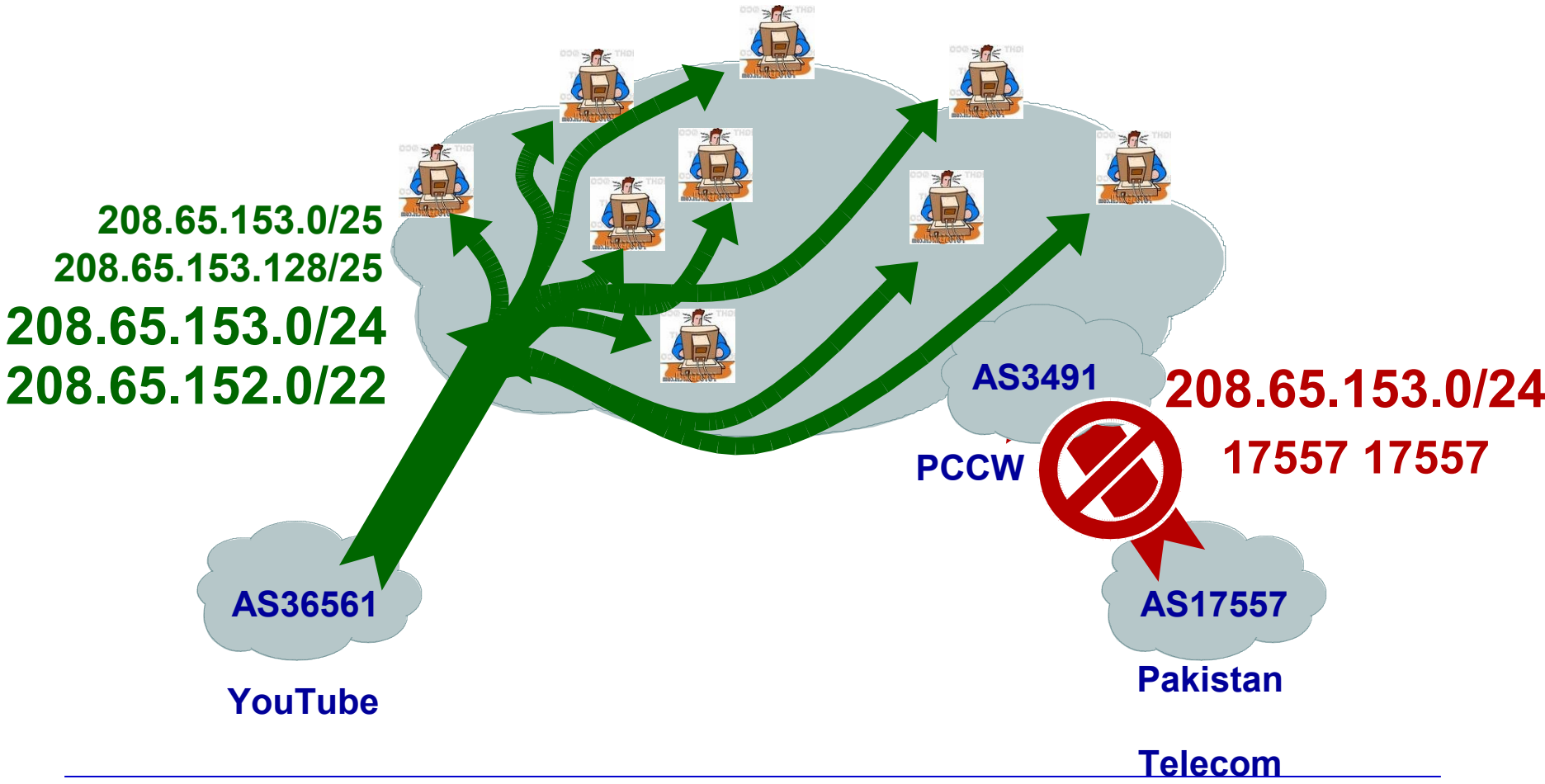
24 February 2008, 20:51 (UTC)



what happened

Hijacking stops

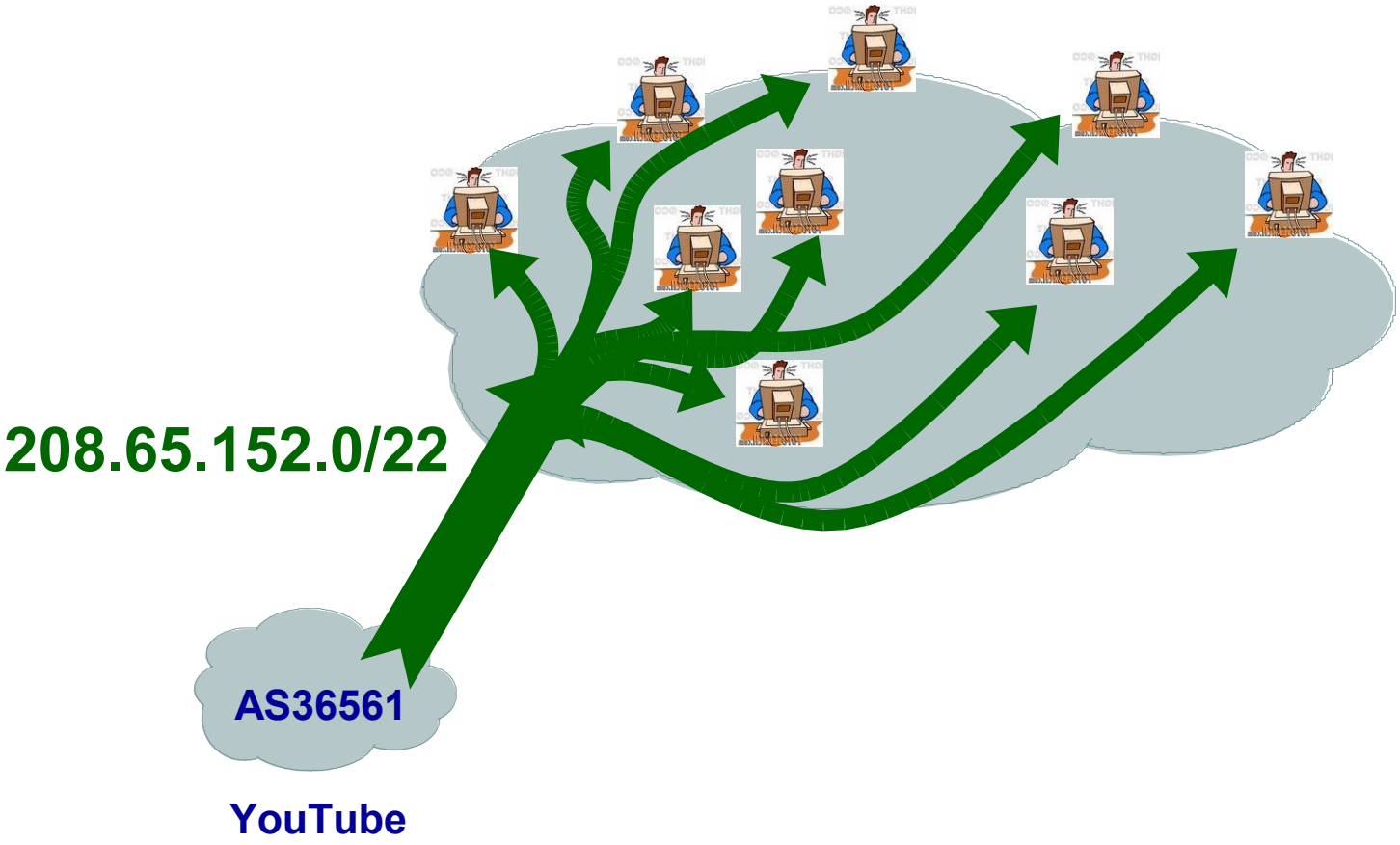
24 February 2008, 21:01 (UTC)



what happened

Back to normal

since 24 February 2008, 21:03 (UTC)



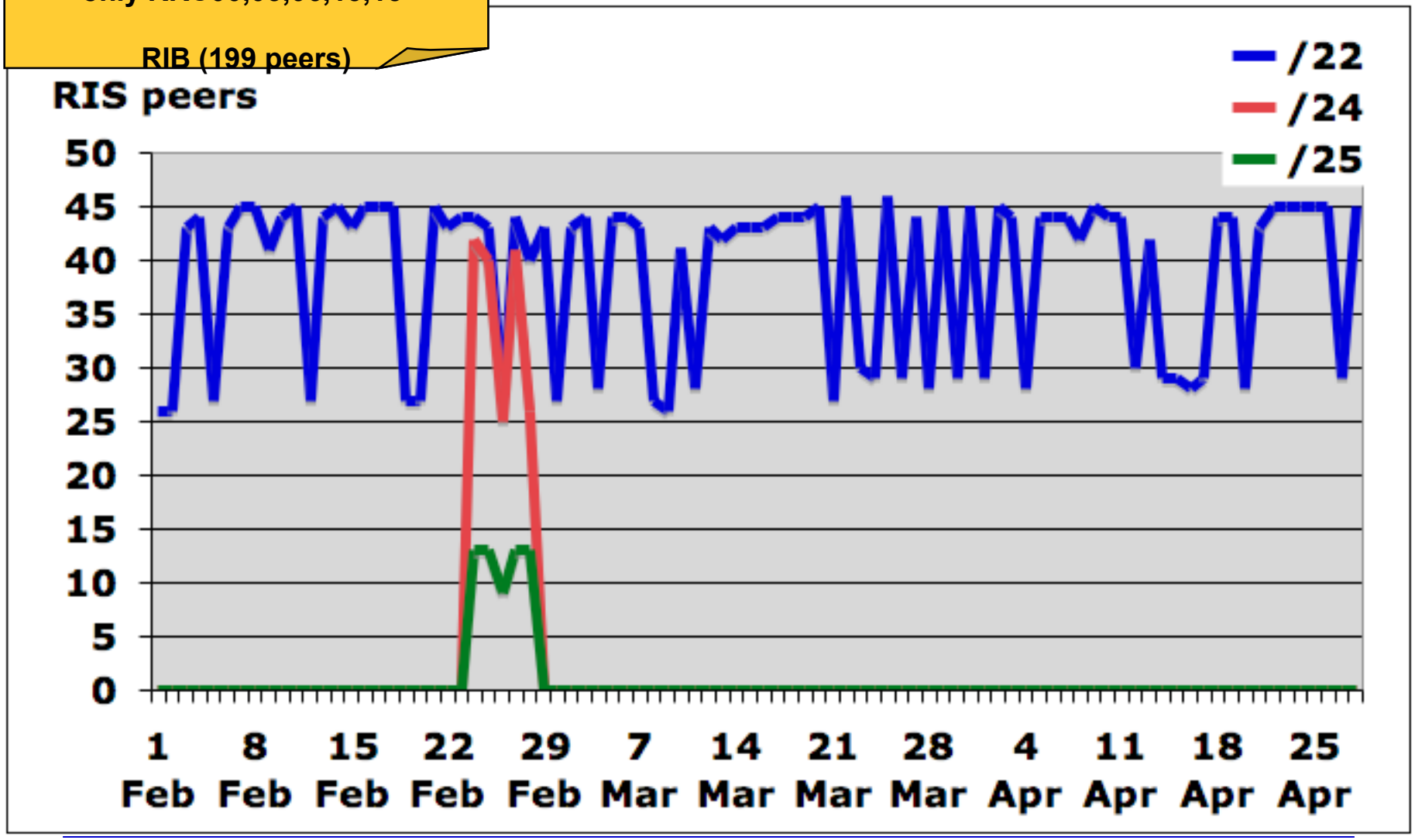
RIPE NCC

statistics

Visibility of YouTube's prefixes

only RRC00,03,06,13,15

RIB (199 peers)



The lesson for customers

If it happens to me, what should I do?

- How to ***react*** the problem
  - Announcing the hijacked route mitigates the problem, but it does not solve it completely
    - If you need to announce a /24, stop announcing it after the hijacking stops
  - Announcing /25 does not help much
  - Collaborate with your upstream provider(s) for quick resolution
- How to ***prevent*** the problem
  - Nothing yet

The lesson for ISPs

If it happens to me, what should I do?

- How to ***react*** to the problem
  - ISPs should have procedures in place to help customer(s)
  - ISPs should have procedures in place to to communicate with peer(s) and upstream provide(s)
- How to ***prevent*** the problem

ROUTE FILTERING

Further analyses follow …

- Please ask your questions afterwards