BGP Security:
The Threat of Prefix Hijacks

Dr. Franziska Boenisch
SprintML Lab, CISPA Helmholtz Center for Information Security

2008: YouTube offline for multiple hours





HOME / BLOGS

Pakistan Hijacks YouTube: A Closer Look

By **Martin A. Brown**

Technical Lead

February 25, 2008 | Views: 46,366 | Comments: 1



Comparable incidents are common!

For two hours, a large chunk of European mobile traffic was rerouted through China

It was China Telecom, again. The same ISP accused last year of "hijacking the vital internet backbone of western countries."



Written by **Catalin Cimpanu,** Contributor

June 7, 2019 at 12:41 p.m. PT

BGP

Some Twitter traffic briefly funneled through Russian ISP, thanks to BGP



s most likely an error, not an attack.

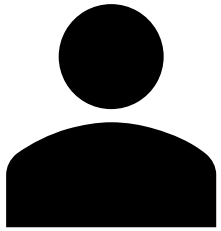
ANDY GREENBERG SECURITY AUG 7, 2014 1:00 PM

Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins

How do we access data on the internet?



Autonomous systems (AS) form the internet





AS1



AS2



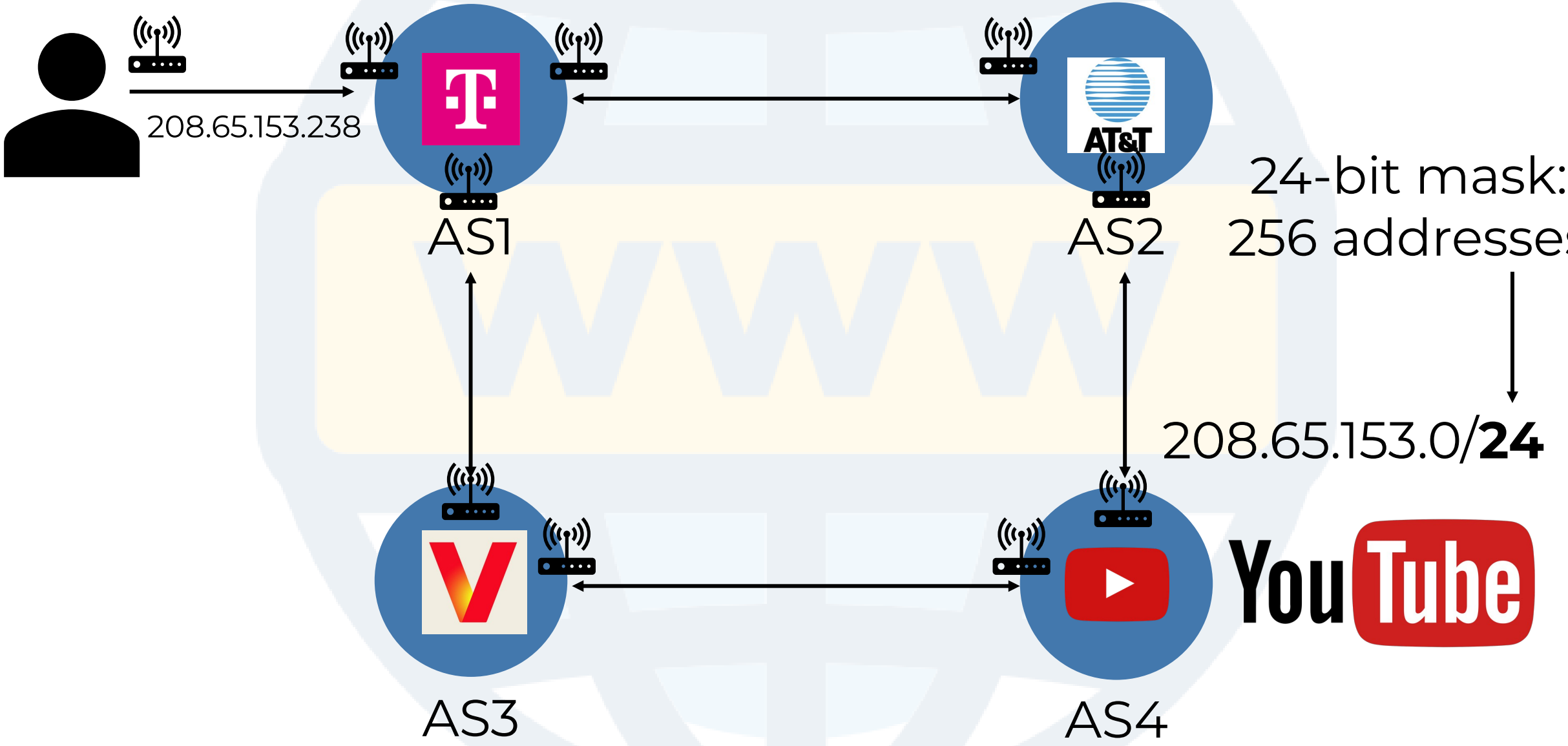
AS3



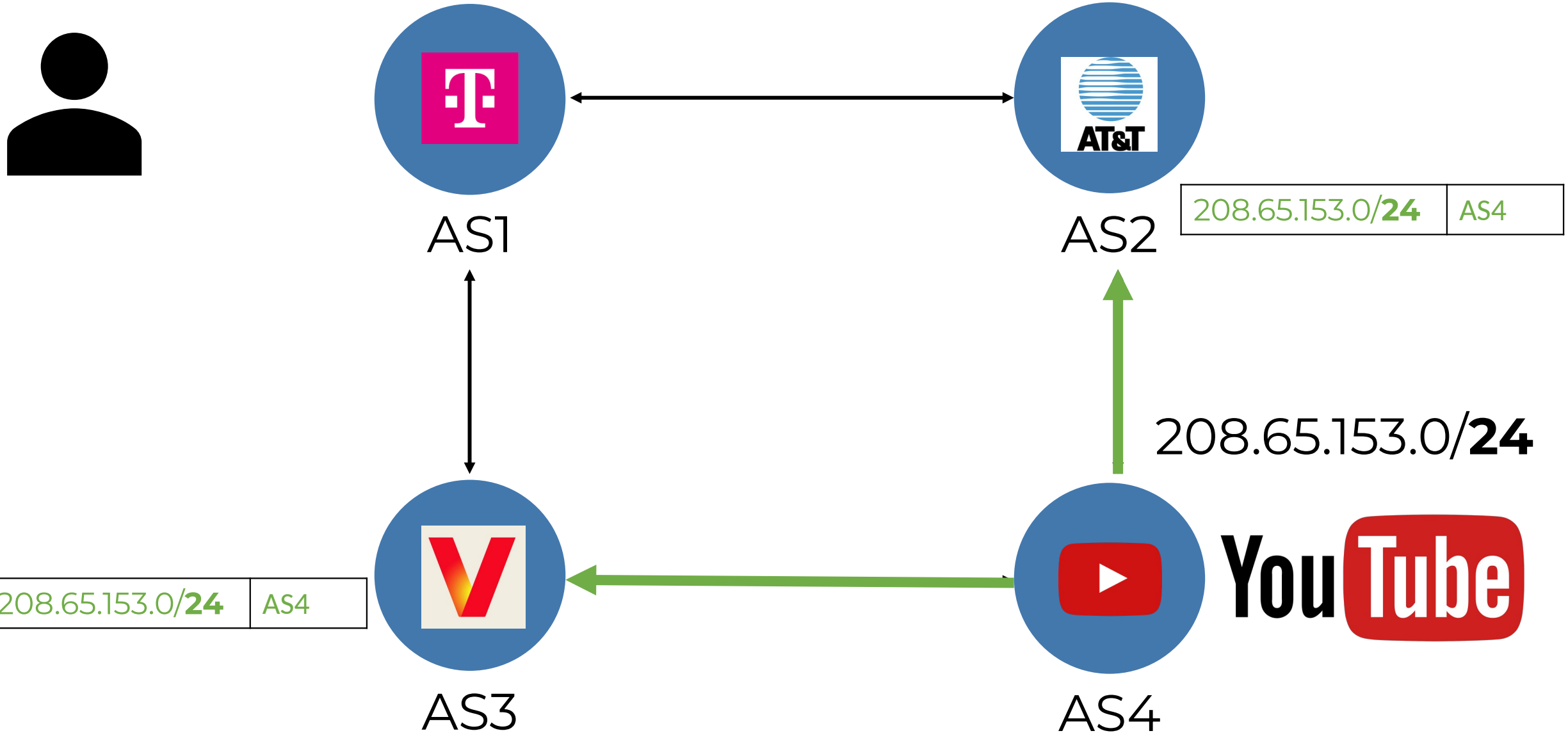
AS4



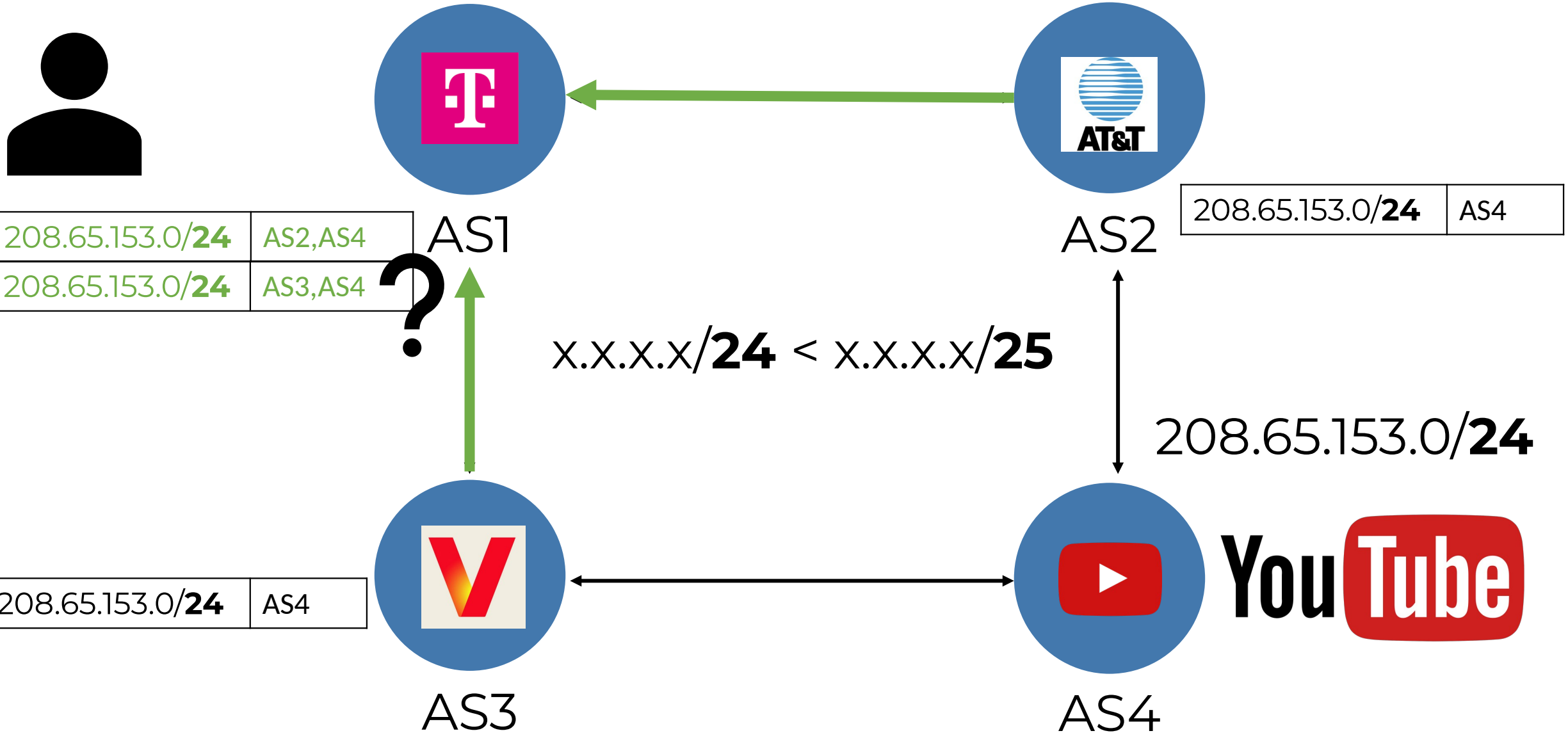
Autonomous systems (AS) form the internet



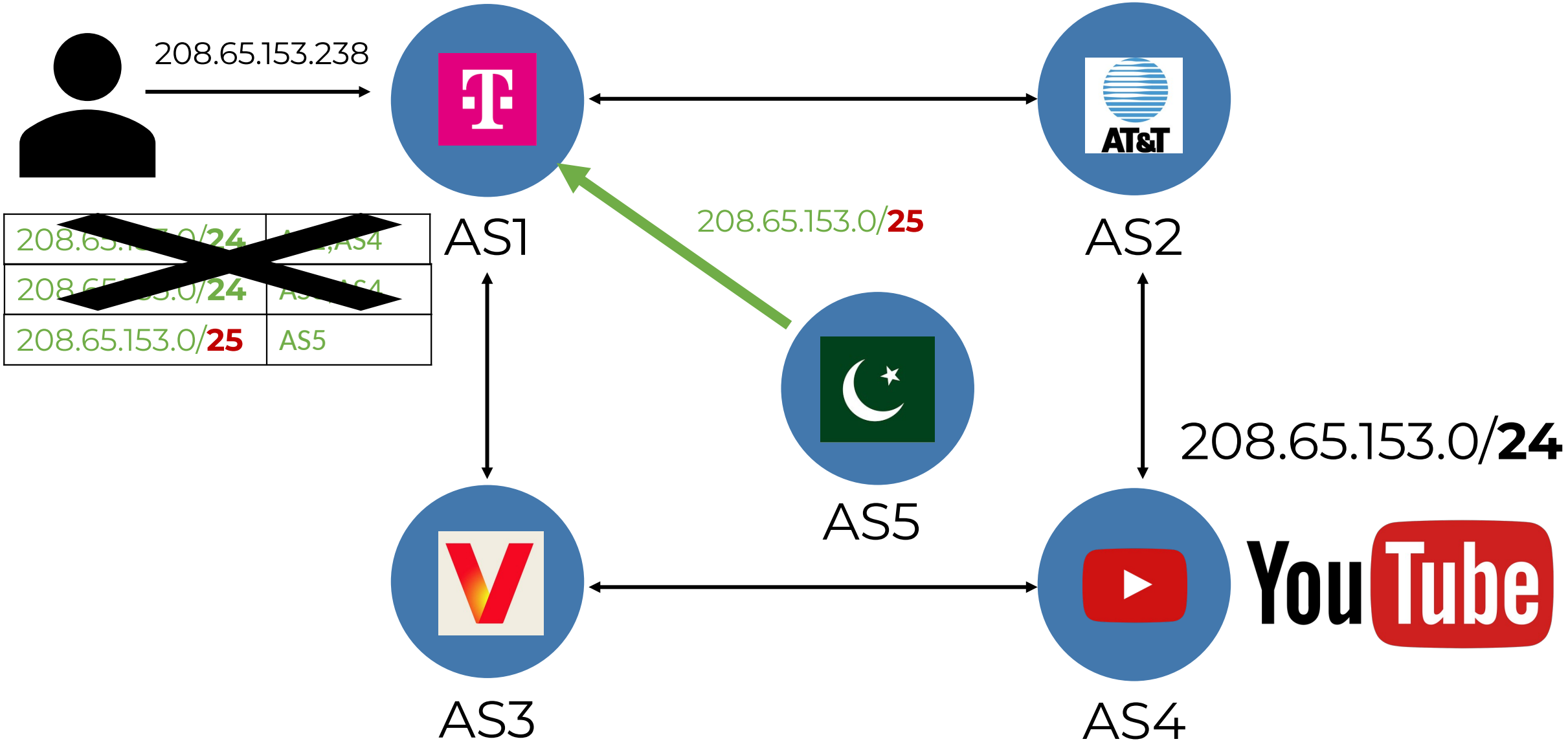
The Border Gateway Protocol (BGP)



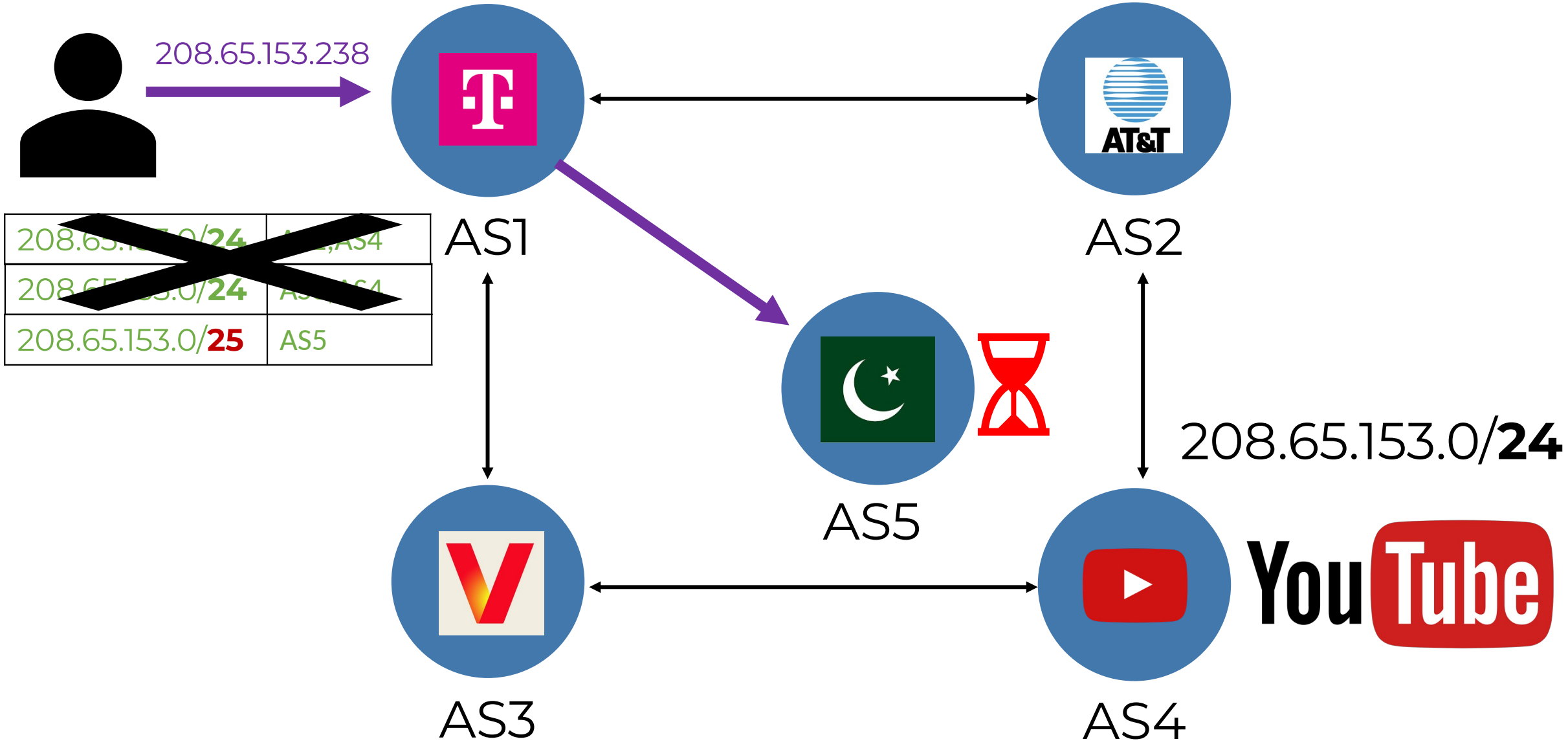
The Border Gateway Protocol (BGP)



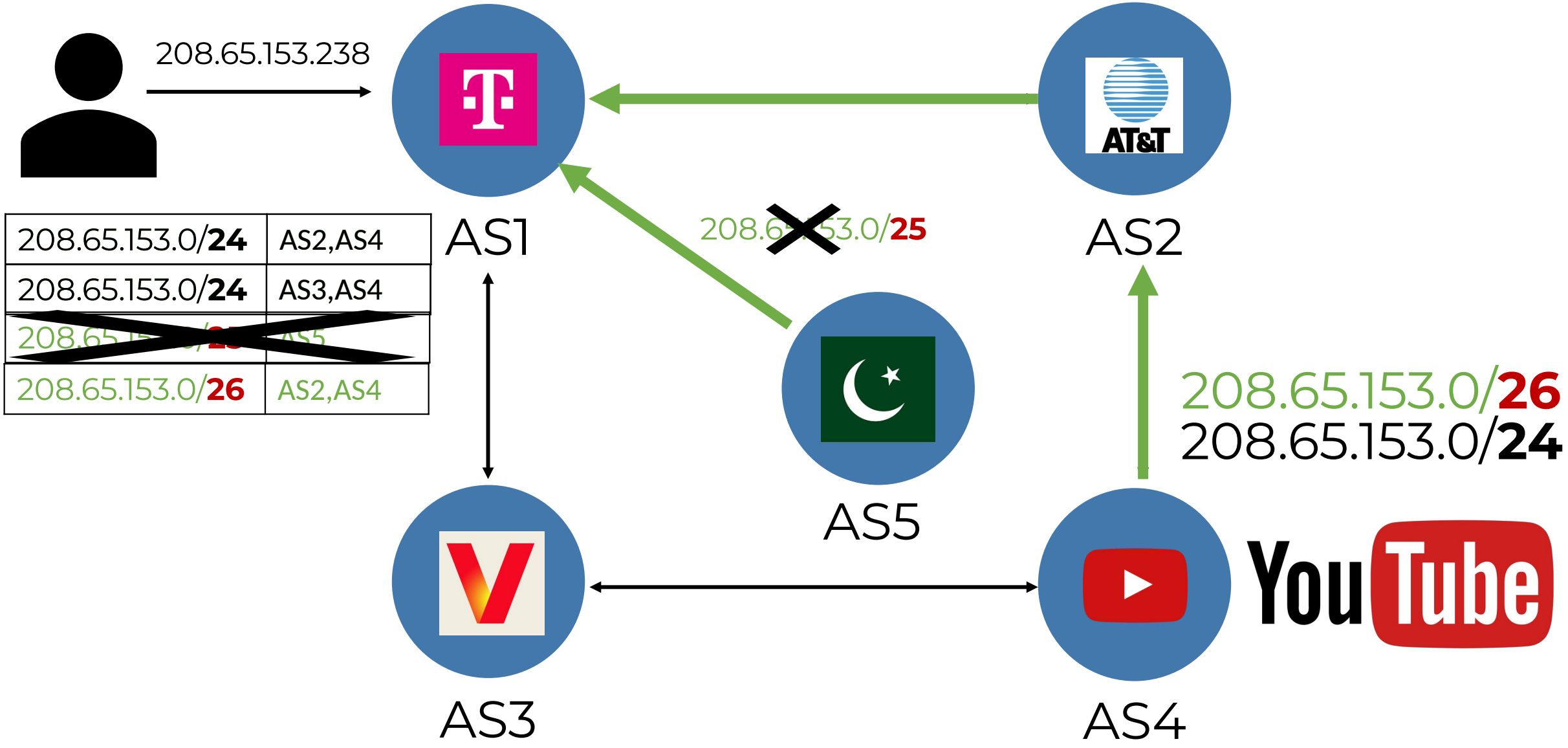
BGP operates on trust



When trust is violated, traffic "goes bad"

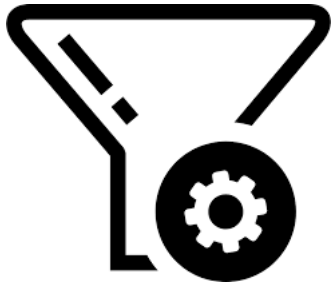


How was the YouTube incident fixed?



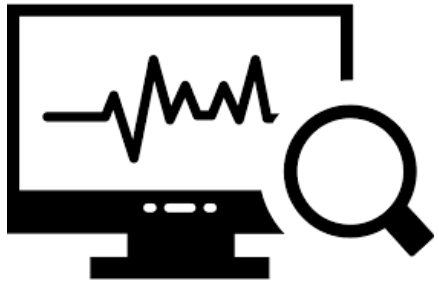
208.65.153.0/**24**	AS2,AS4
208.65.153.0/**24**	AS3,AS4
~~208.65.153.0/25~~	~~AS5~~
208.65.153.0/**26**	AS2,AS4

Naively protecting against BGP hijacks



1) Prefix Filter

Which prefix can customer announce?



2) Monitoring

Do unexpected changes occur?



Manual Maintenance



Simple Networks

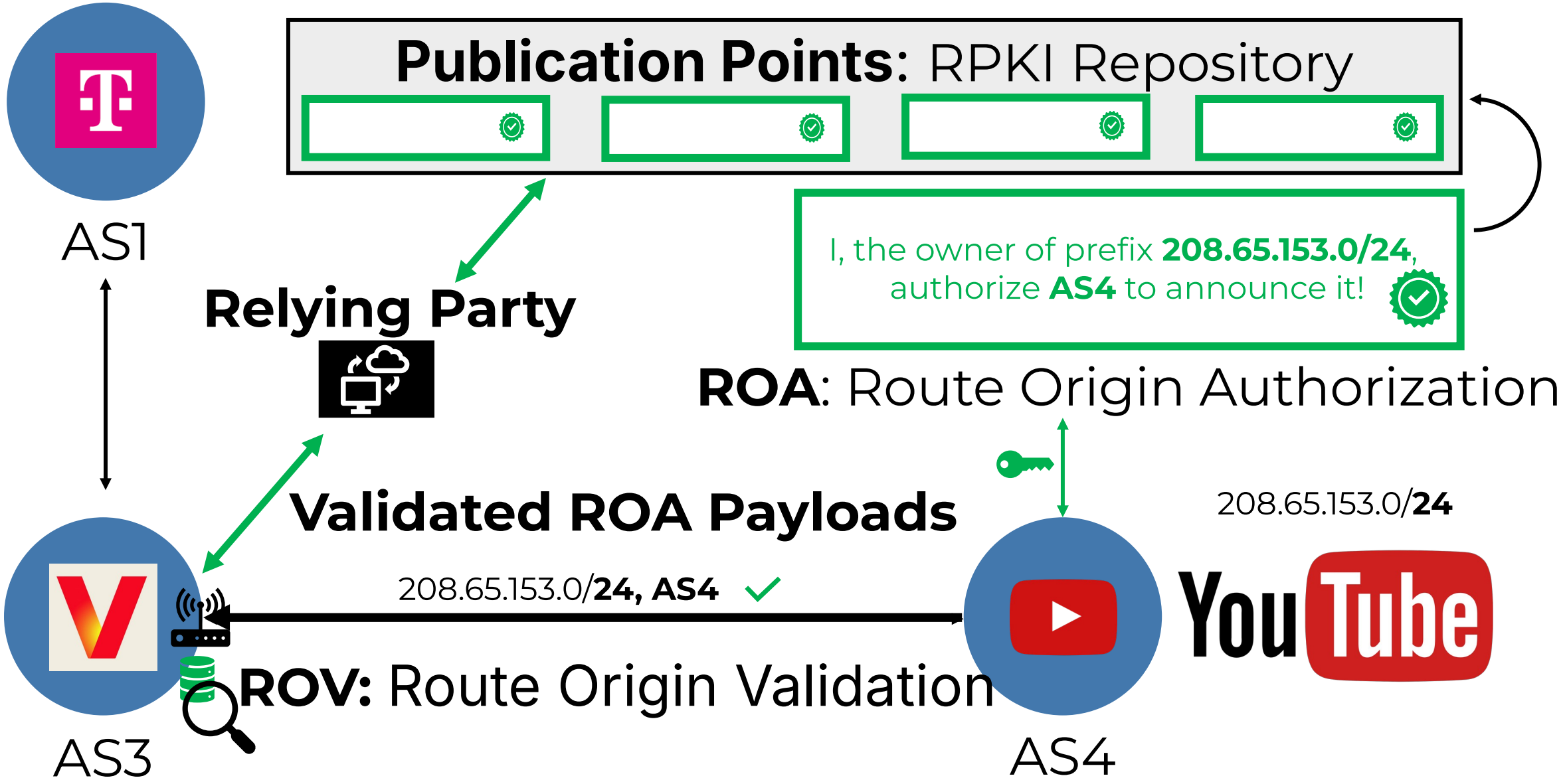


Only Reactive

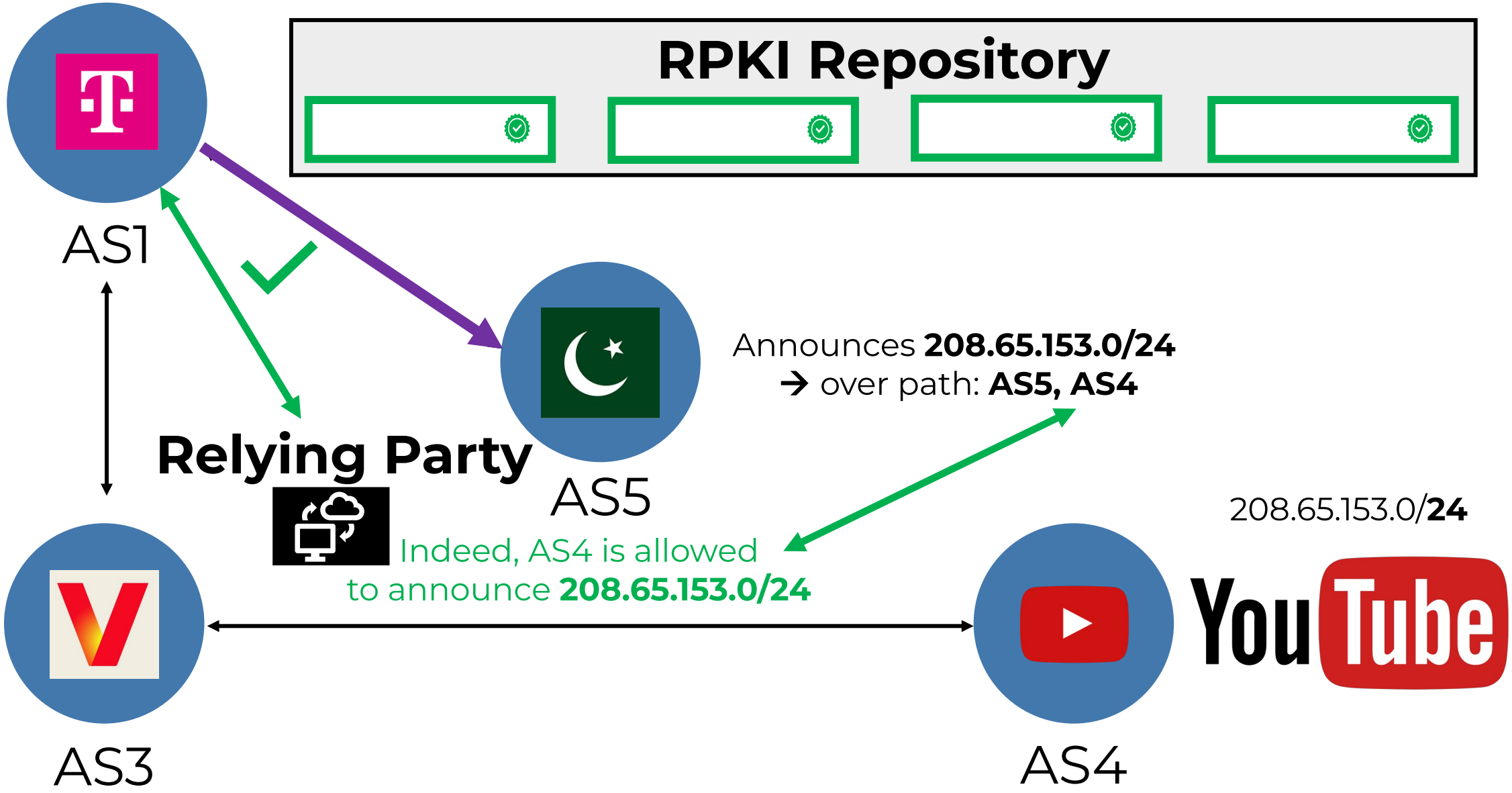


False Positives

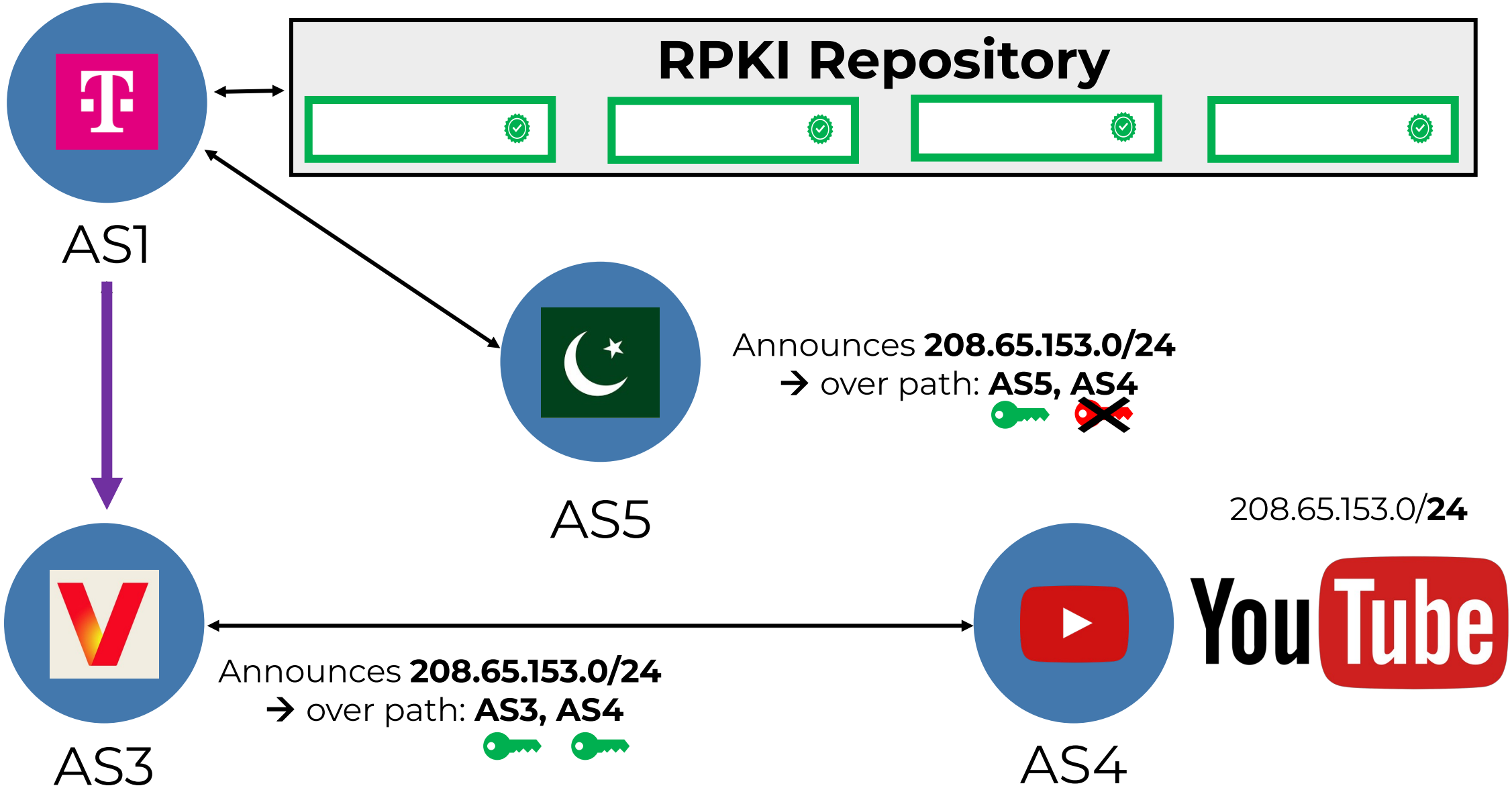
Resource Public Key Infrastructure (RPKI)



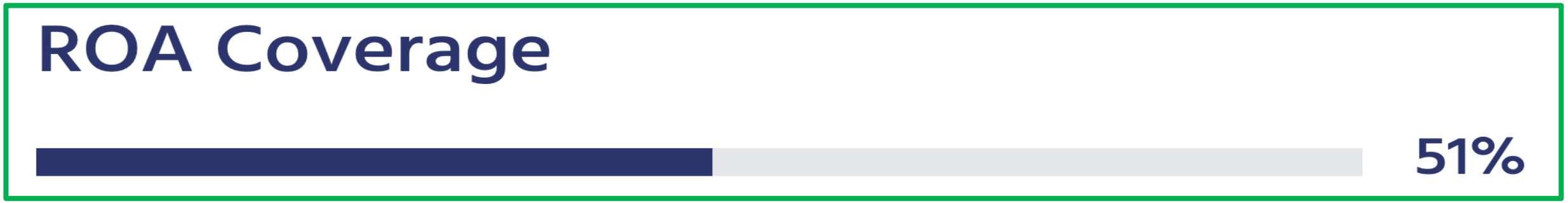
RPKI is limited to "Origin Validation"



BGPSec offers “Path Validation”



Are we there yet?



ROV: 27% of networks

Incidents:
- Q2 2022: > 9000
- Q2 2023: ≈ 7500

https://pulse.internetsociety.org/en/technologies/#metric-roa-coverage

Summary

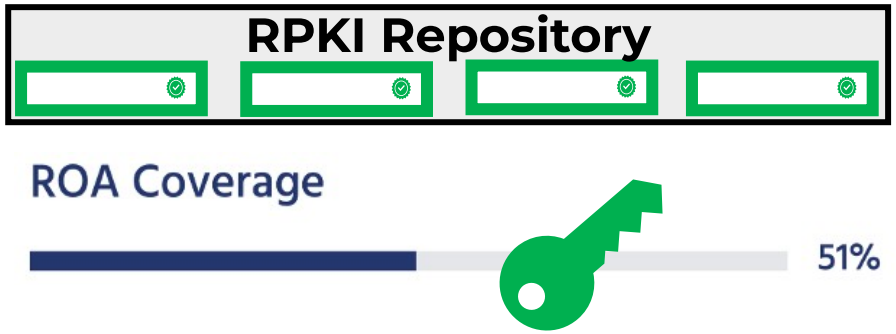




BGP keeps internet together

BGP requires trust





Trust = vulnerable

Defenses *slowly* adopted

Lecture Materials and Discussion

Why do you think adoption of RPKI and BGPSec is so slow, despite clear security benefits?

SCAN ME

Further Reading

SCAN ME

Video Lecture

SCAN ME

BETA: AI Podcast

More Questions and more discussions!

Should RPKI and BGPSec be mandatory for critical infrastructure providers? What would be the pros and cons?

How much security is ‘enough’ in Internet routing? Is partial protection (like origin validation only) worth it?

Where is BGP Executed?

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

⟵ BGP: TCP, port 179

https://www.imperva.com/learn/application-security/osi-model/

BGP Route Selection Algorithm

- Prefer the highest LOCAL_PREF
  - Local Preference (LOCAL_PREF) is an administrative setting within an AS, Higher values are preferred.
- Prefer the shortest AS_PATH
  - Fewer AS hops are preferred. Example: AS_PATH {100 200 300} → Longer path; AS_PATH {400 500} → Shorter path (preferred)
- Prefer the lowest ORIGIN code
  - Origin types: IGP (Interior Gateway Protocol) → Preferred; EGP (Exterior Gateway Protocol); Incomplete (Unknown Source)
- Prefer the lowest MED (Multi-Exit Discriminator)
  - MED is used to influence inbound traffic from other ASes. Lower values are preferred.
- Prefer eBGP over iBGP routes
  - eBGP routes (from external ASes) are preferred over iBGP routes (from within the same AS).
- Prefer the lowest IGP metric to the next-hop
  - The shortest internal path to the BGP next-hop is preferred.
- Prefer the oldest route
  - If all else is equal, the most stable route is chosen.
- Prefer the lowest Router ID
  - The tie-breaker: The router with the lowest BGP Router ID wins.

What does BGP Store in Routing Tables

- The **destination prefix** (e.g., 192.168.1.0/24).
- The **AS path** (list of ASes the route has traversed).
- The **next-hop IP address** (the router that should receive the packet next).
- Various **BGP attributes** (Local Pref, MED, etc.) used for selecting the best path.

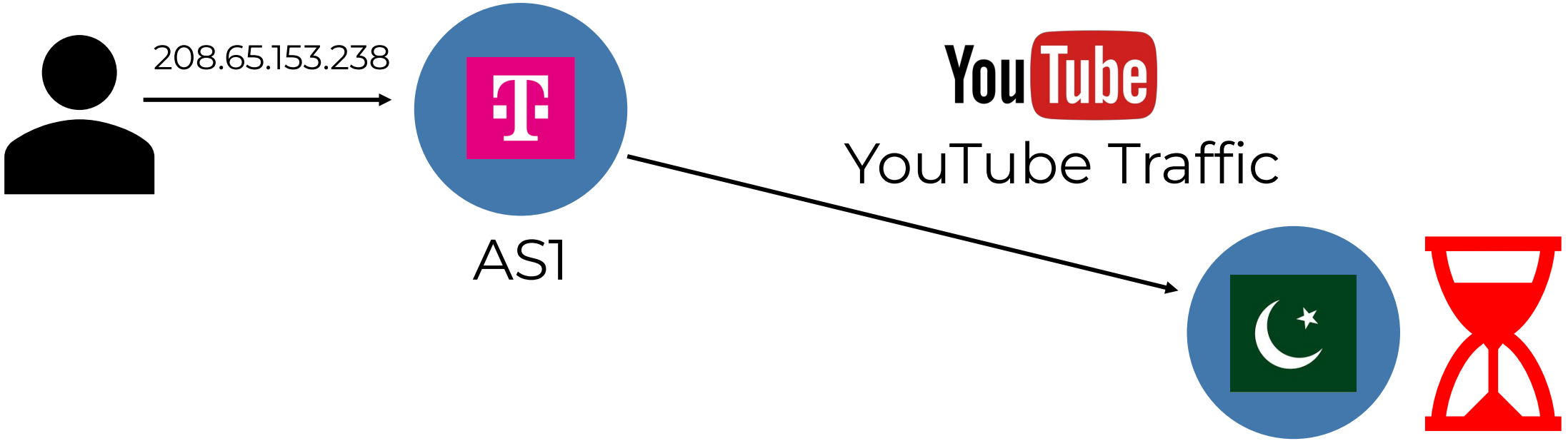
Example: BGP Table Entry

BGP table entry for reaching **192.168.1.0/24** might look like this:

Destination Next-Hop AS Path Local Pref MED

192.168.1.0/24 203.0.113.1 65010 65020 100 0

BGP hijacks cause service risks



Misrouted packages can be:

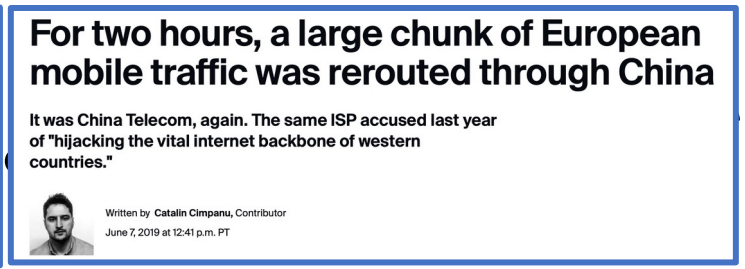

HOME / BLOGS

Pakistan Hijacks YouTube: A Closer Look

By Martin A. Brown
Technical Lead

February 25, 2008 | Views: 46,366 | Comments: 1

Black-holed


For two hours, a large chunk of European mobile traffic was rerouted through China

It was China Telecom, again. The same ISP accused last year of "hijacking the vital internet backbone of western countries."

Written by **Catalin Cimpanu**, Contributor
June 7, 2019 at 12:41 p.m. PT

Eavesdropped


ANDY GREENBERG SECURITY AUG 7, 2014 1:00 PM

Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins

Misled

Activities

Chain of Trust