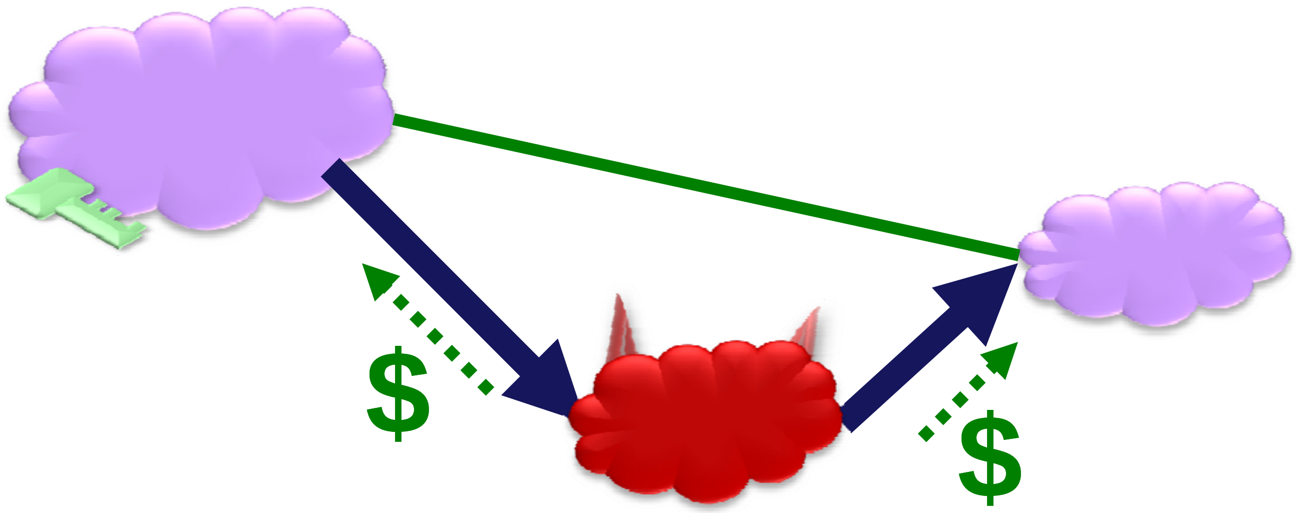
DIMACS Workshop On Secure Routing
March 10, 2010

How Secure are Secure Interdomain Routing Protocols?



Sharon Goldberg
Microsoft Research & Boston University

Michael Schapira
Yale & Berkeley

Pete Hummon
Princeton

Jennifer Rexford
Princeton

Overview

Today, Internet routing is surprisingly insecure

- **Decade of research on secure routing protocols**

Our Goal: Compare the effectiveness of these protocols.

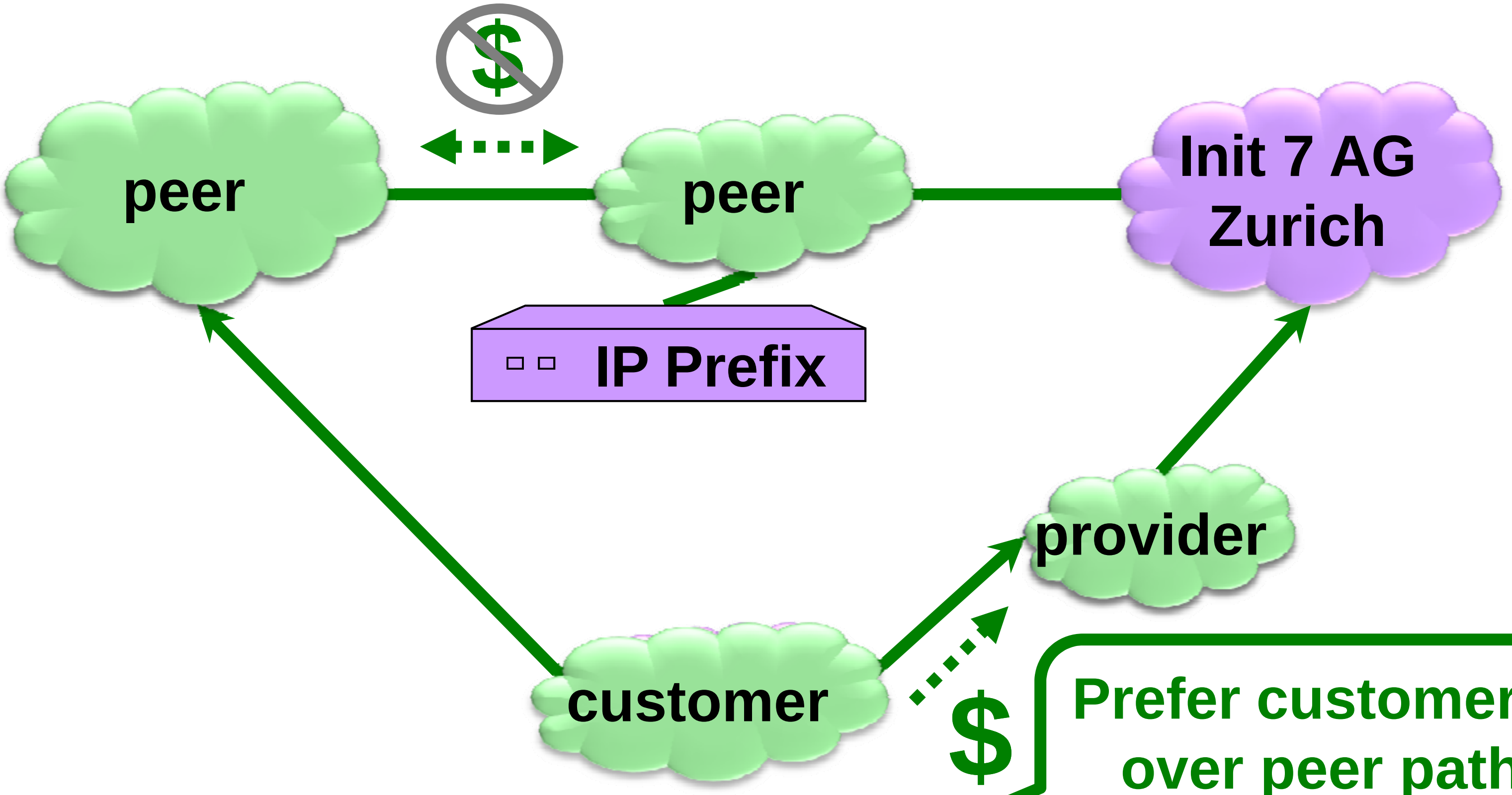
- **Each has a different set of security properties.**
- **How well do they prevent traffic attraction attacks?**

Our approach: Evaluate via simulation on real data.

- **Data: Map of Internet & business relationships**
- **… both [CAIDA] and [UCLA Cyclops]**
- **We use a (standard) model of routing policies**
- **… based on the Gao-Rexford conditions**

BGP: The Internet’s Routing Protocol (1a)

The Border Gateway Protocol (BGP) sets up paths from Autonomous Systems (ASes) to destination IP addresses.



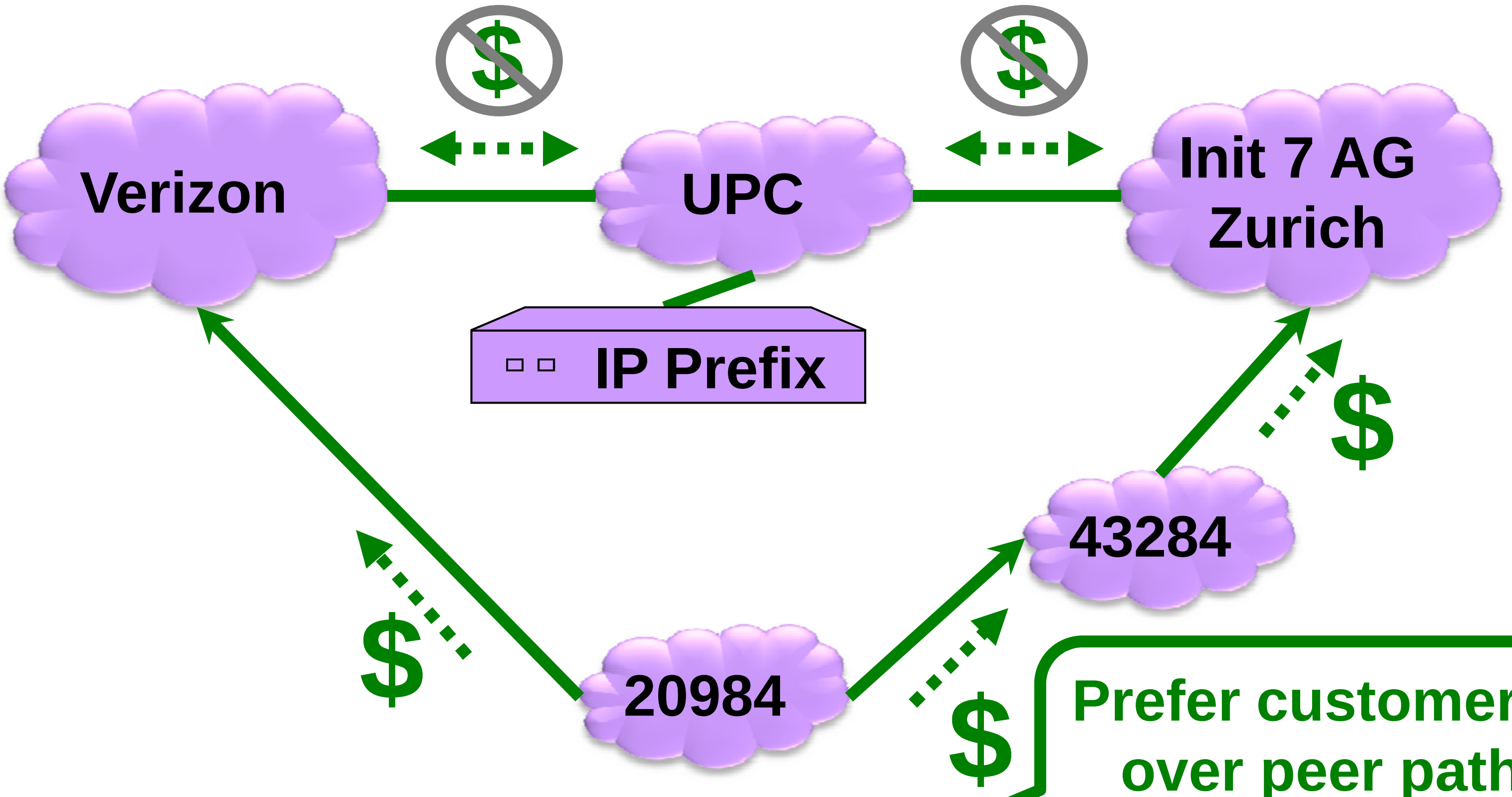
Prefer customer paths
over peer paths
over provider paths

A model of routing policies:

- Prefer cheaper paths. Then, prefer shorter paths.

BGP: The Internet’s Routing Protocol (1b)

The Border Gateway Protocol (BGP) sets up paths from Autonomous Systems (ASes) to destination IP addresses.



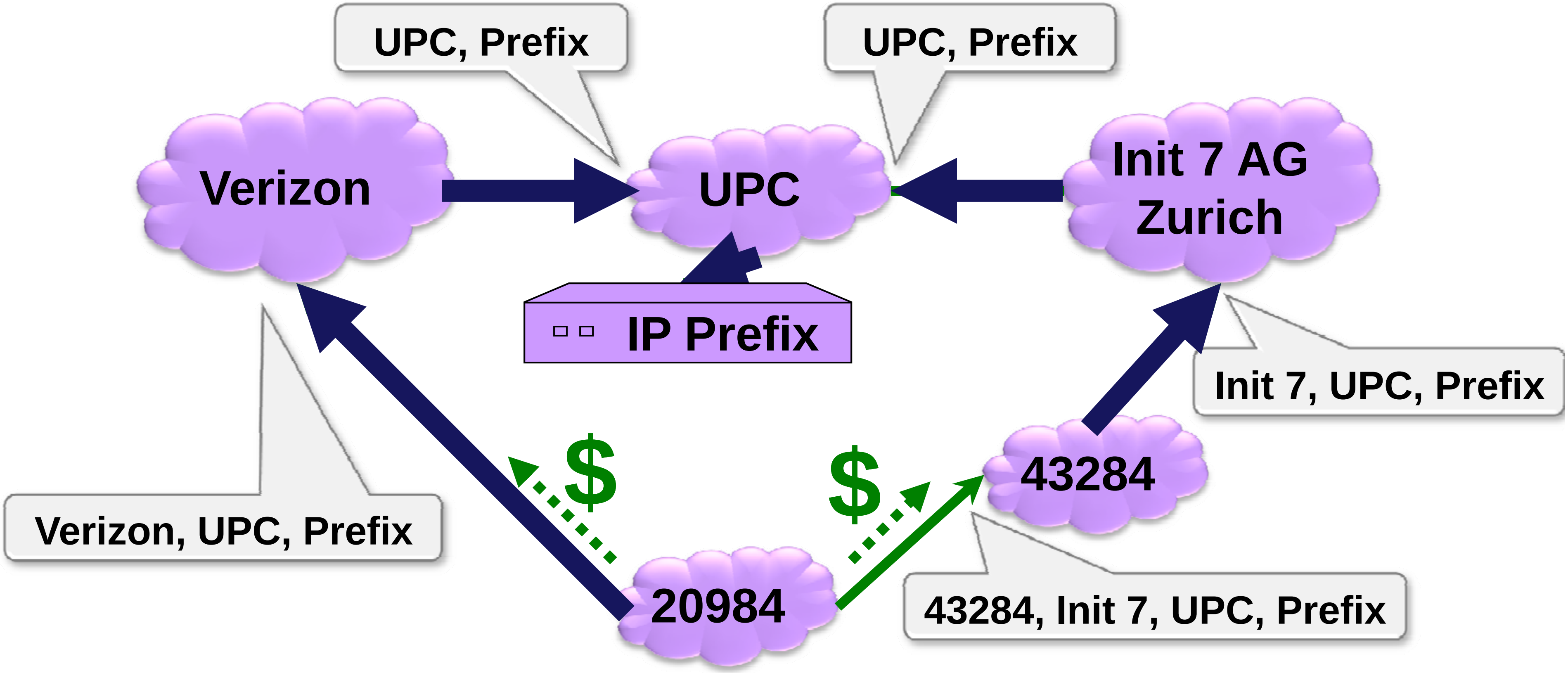
Prefer customer paths over peer paths over provider paths

A model of routing policies:

- Prefer cheaper paths. Then, prefer shorter paths.

BGP: The Internet’s Routing Protocol (2)

The Border Gateway Protocol (BGP) sets up paths from Autonomous Systems (ASes) to destination IP addresses.

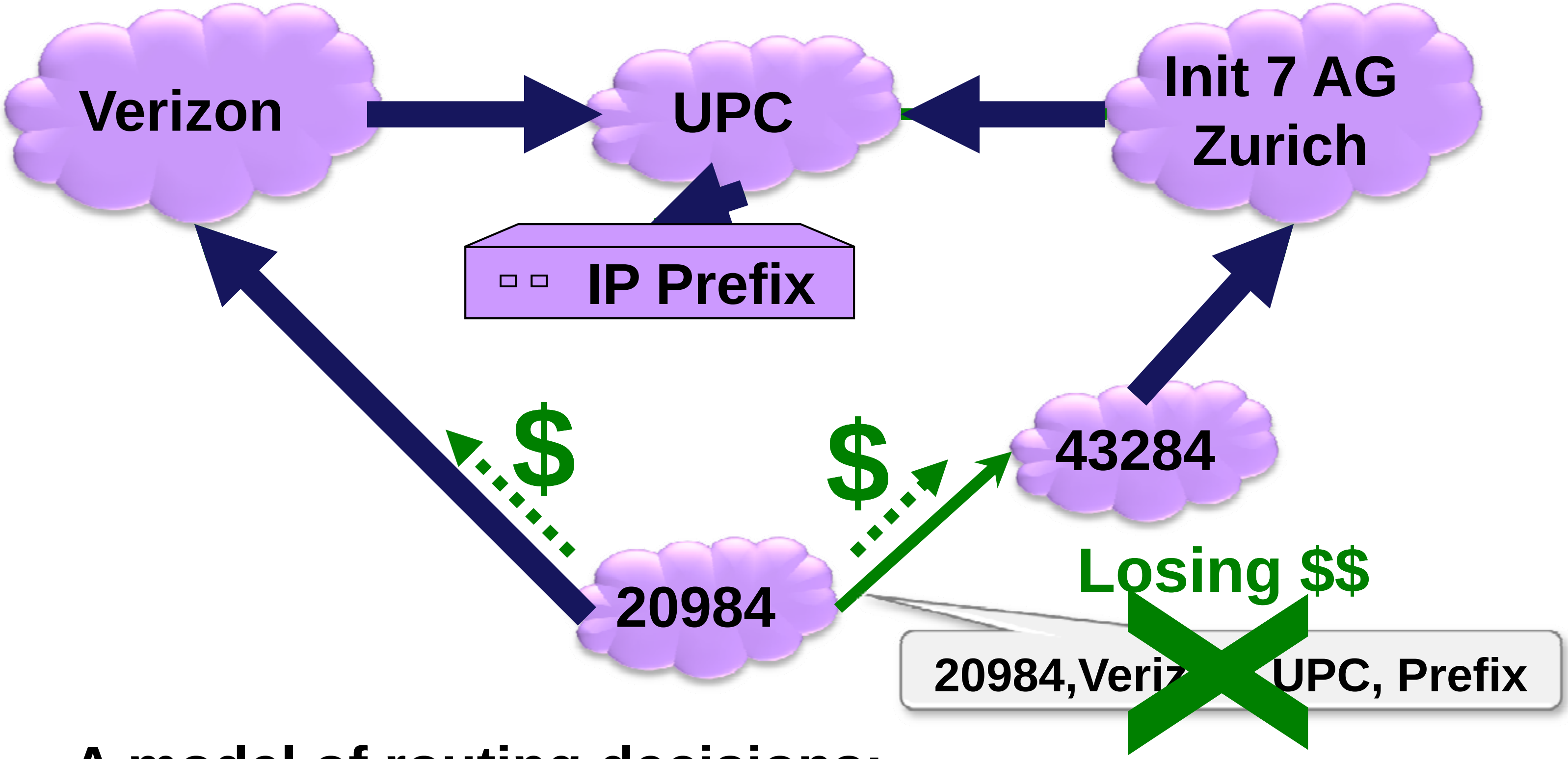


A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.

BGP: The Internet’s Routing Protocol (3)

The Border Gateway Protocol (BGP) sets up paths from Autonomous Systems (ASes) to destination IP addresses.



A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only carry traffic if it earns you money.

This talk

Part 1: A model of Interdomain Routing

Part 2: Secure Routing Protocols and Attacks

Plain BGP

Origin Authentication

Secure BGP

Interlude: Finding the Optimal Attack

Defensive Filtering

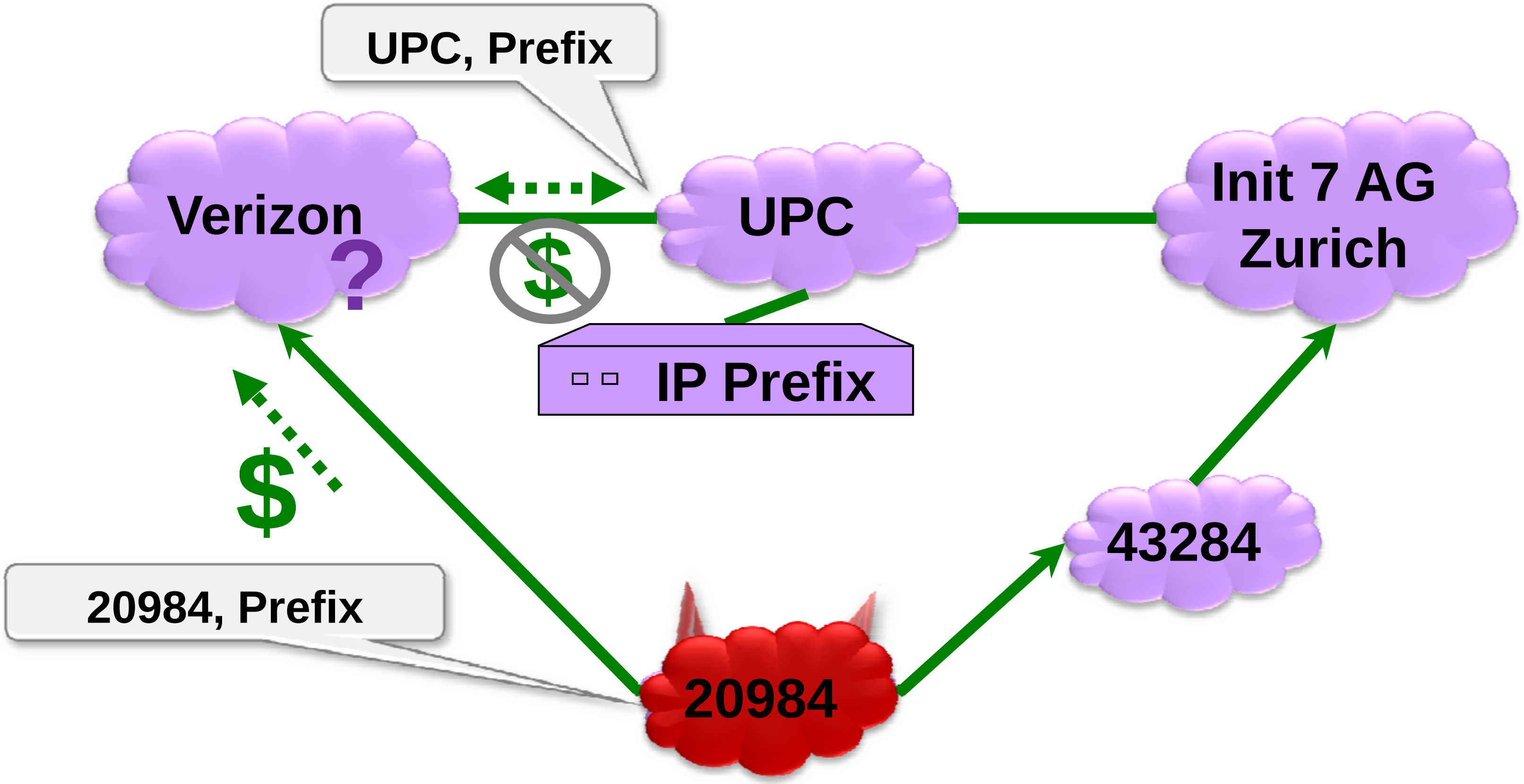
Interlude: Attract more by announcing less

Part 3: Results and Implications

Traffic Attraction Attacks (1)

Attacker wants max number of ASes to route thru its network.

(For eavesdropping, dropping, tampering, …)

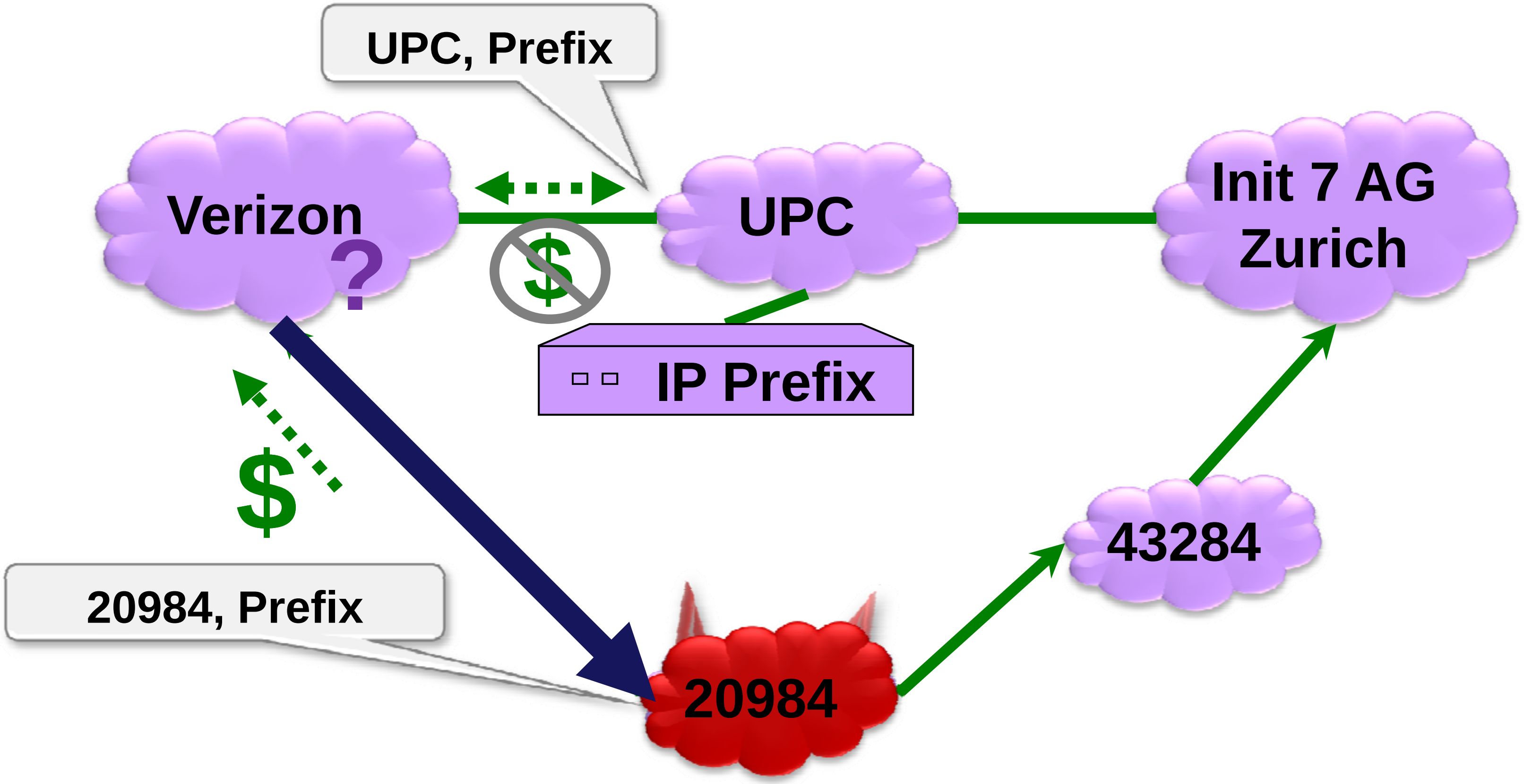


A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only carry traffic if it earns you money.

Traffic Attraction Attacks (2)

Attacker wants max number of ASes to route thru its network.
(For eavesdropping, dropping, tampering, …)

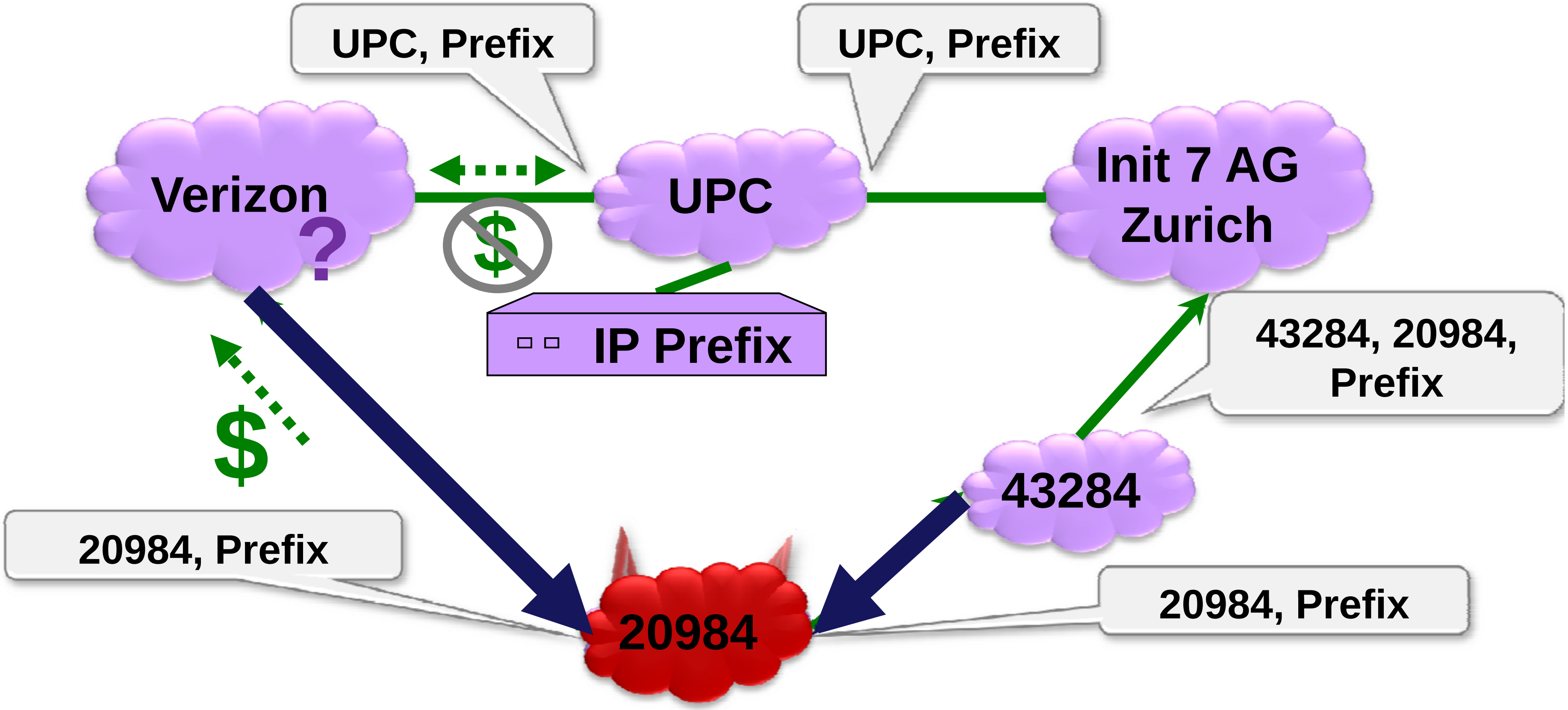


A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only carry traffic if it earns you money.

Traffic Attraction Attacks (3)

Attacker wants max number of ASes to route thru its network.
(For eavesdropping, dropping, tampering, …)



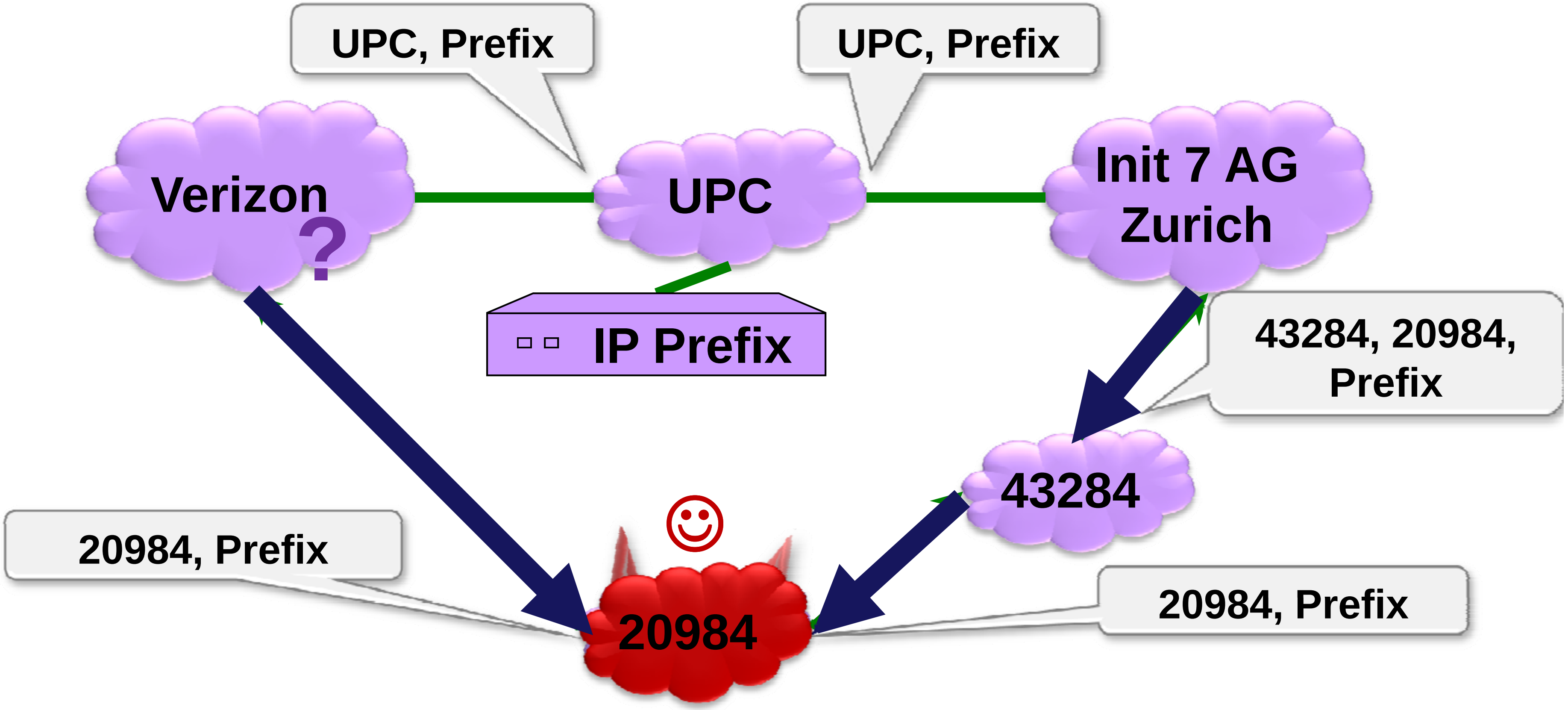
A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only carry traffic if it earns you money.

Traffic Attraction Attacks (4)

Attacker wants max number of ASes to route thru its network.

(For eavesdropping, dropping, tampering, …)

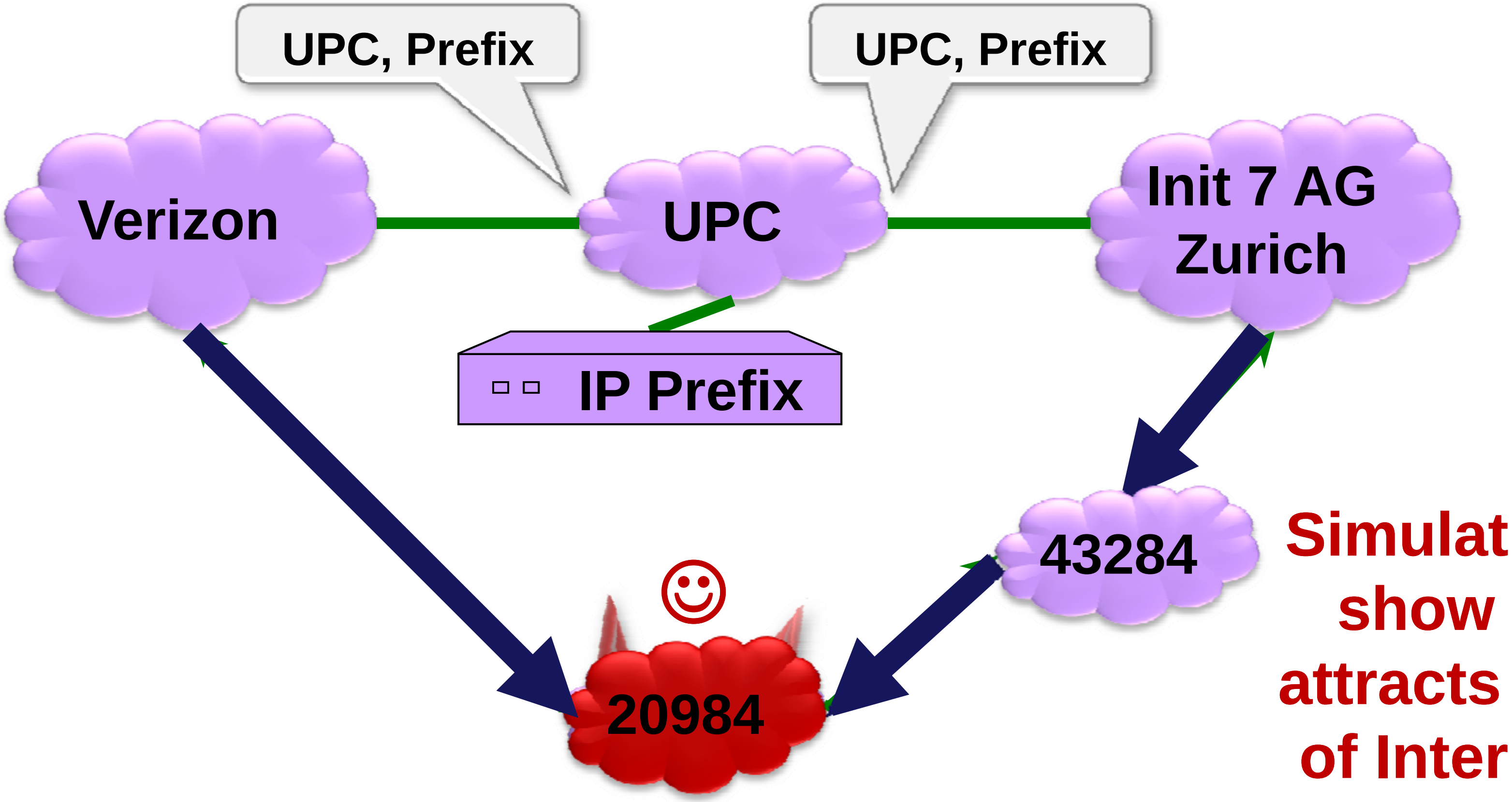


A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only carry traffic if it earns you money.

Traffic Attraction Attacks (5)

Attacker wants max number of ASes to route thru its network.
(For eavesdropping, dropping, tampering, …)



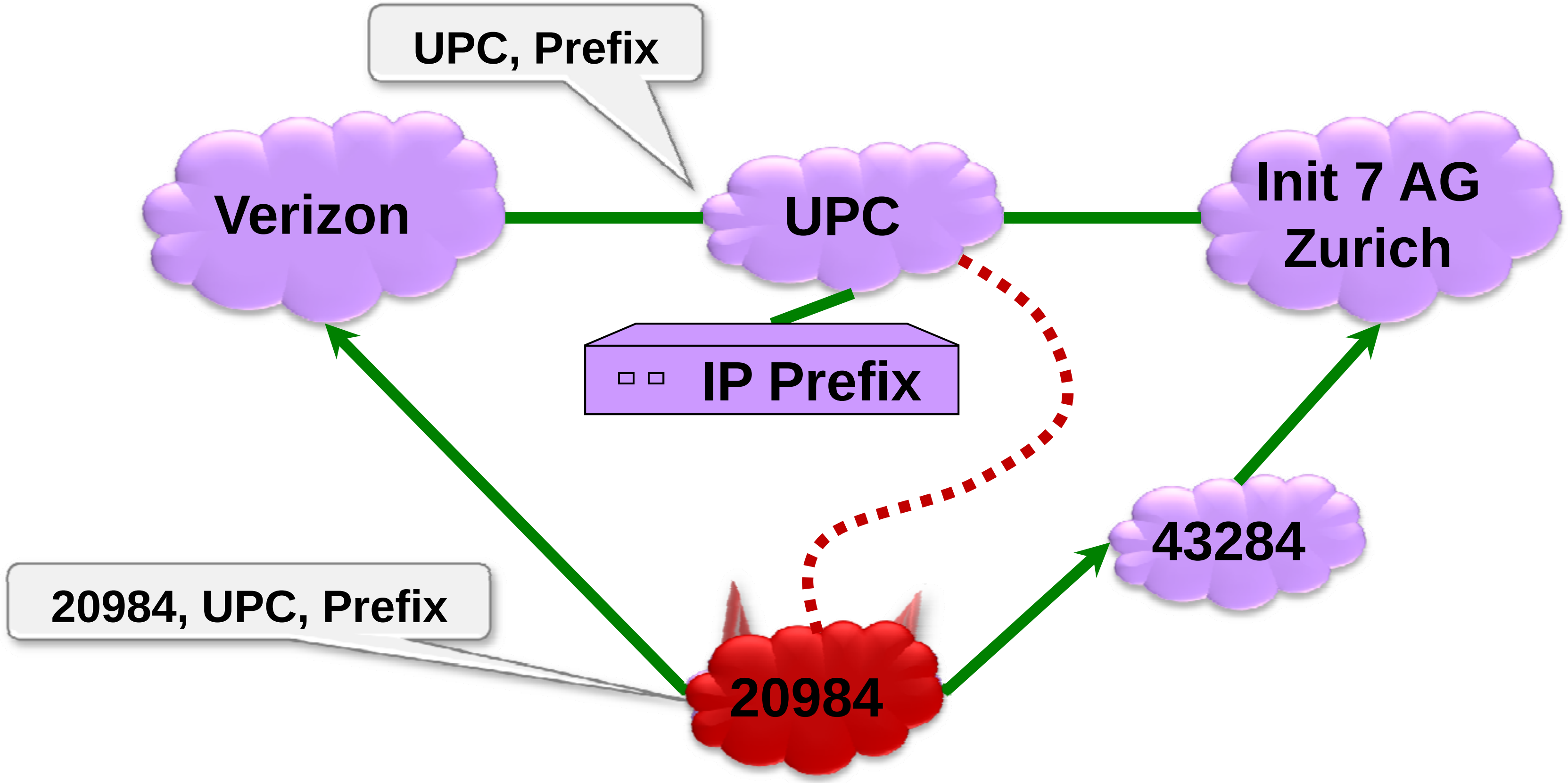
Simulations show he attracts 62% of Internet!

A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only carry traffic if it earns you money.

Security Mechanism: Origin Authentication (1)

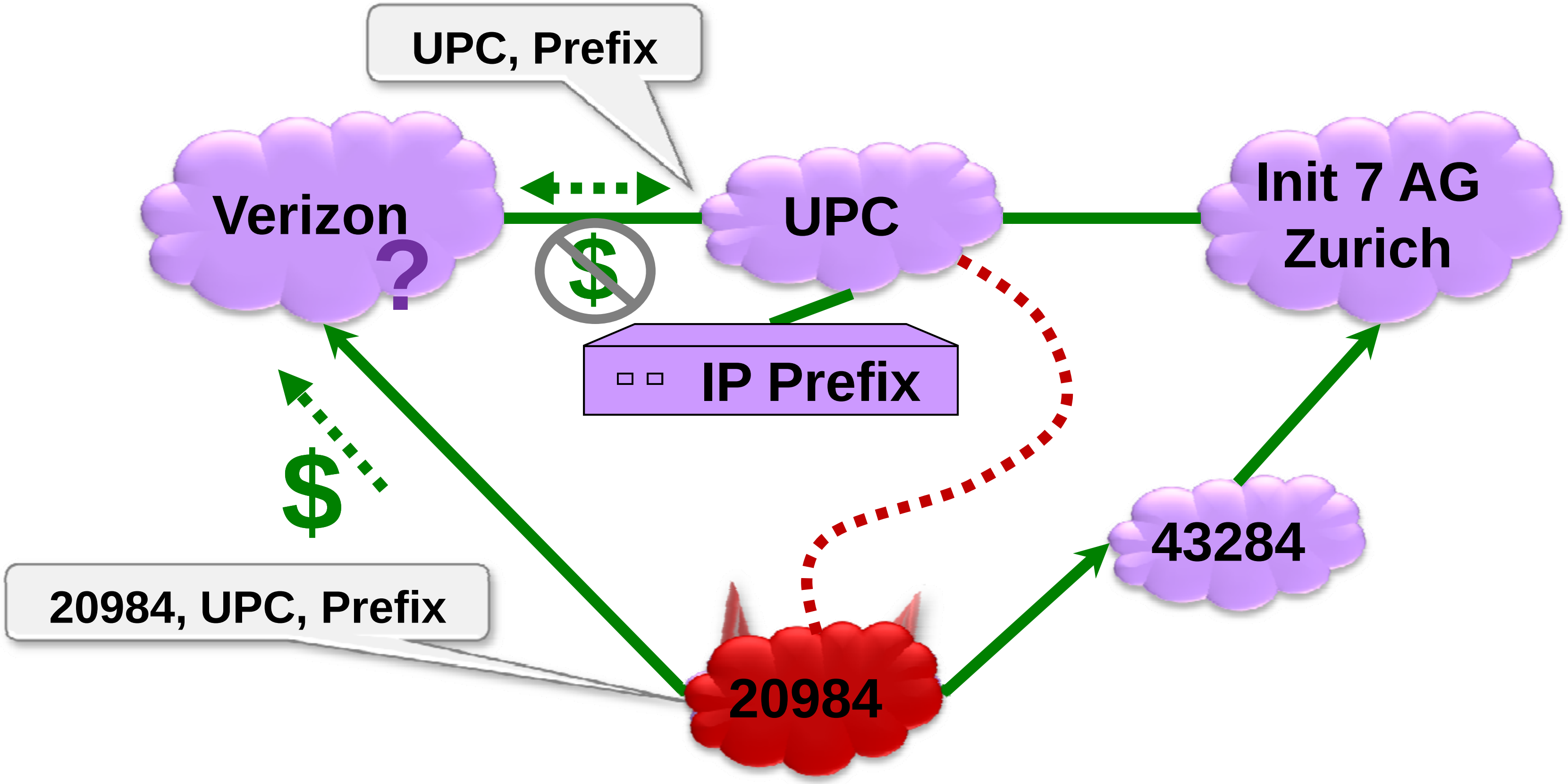
Origin Authentication: A secure database that maps IP Prefixes to their owner ASes.



Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Security Mechanism: Origin Authentication (2)

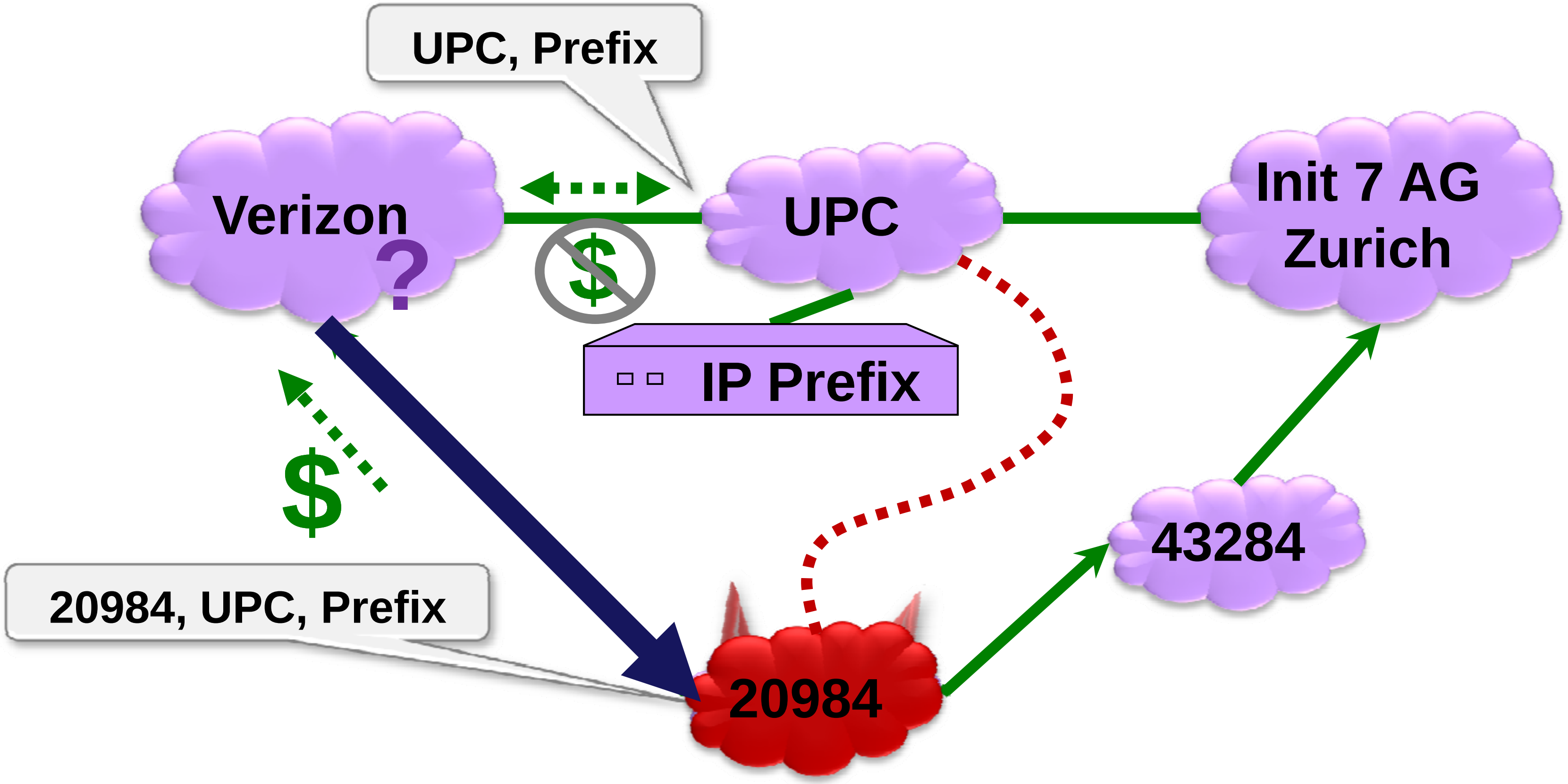
Origin Authentication: A secure database that maps IP Prefixes to their owner ASes.



Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Security Mechanism: Origin Authentication (3)

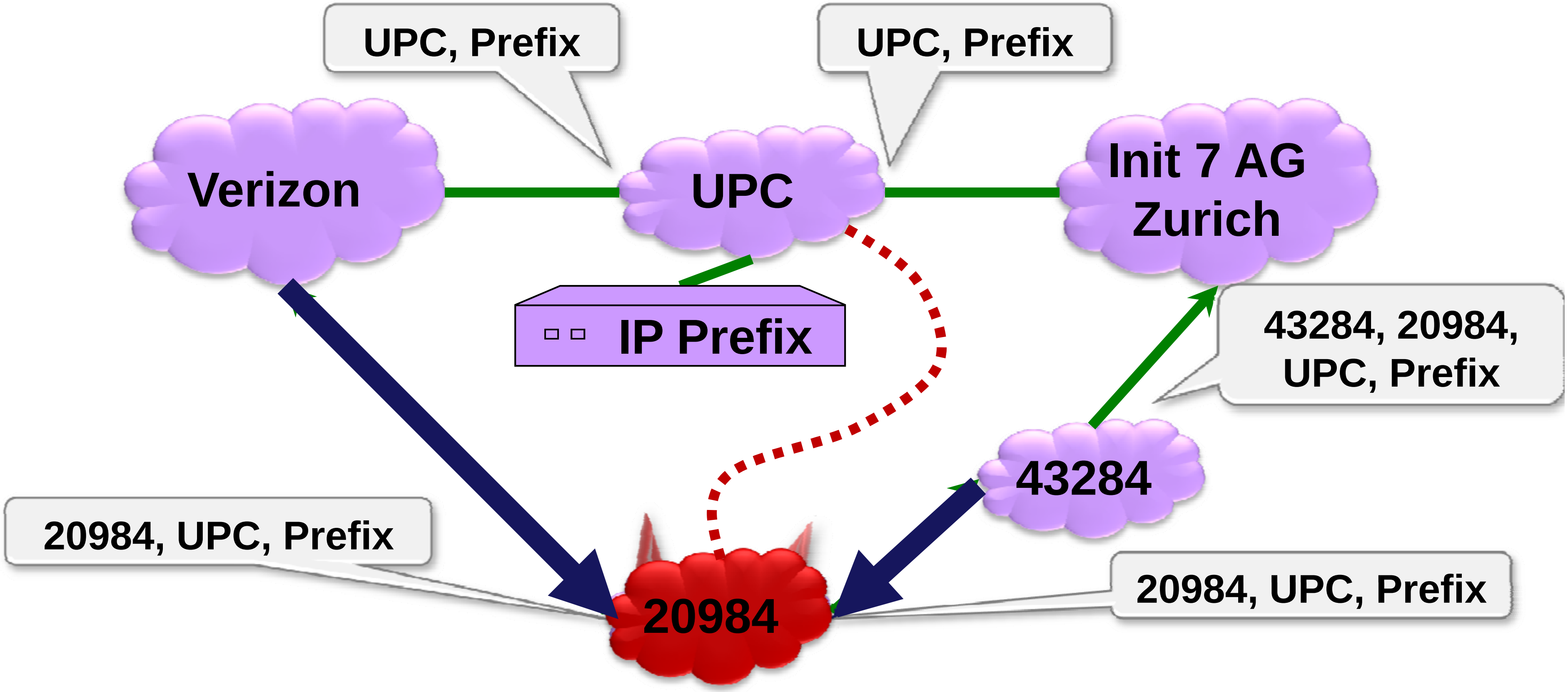
Origin Authentication: A secure database that maps IP Prefixes to their owner ASes.



Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Security Mechanism: Origin Authentication (4)

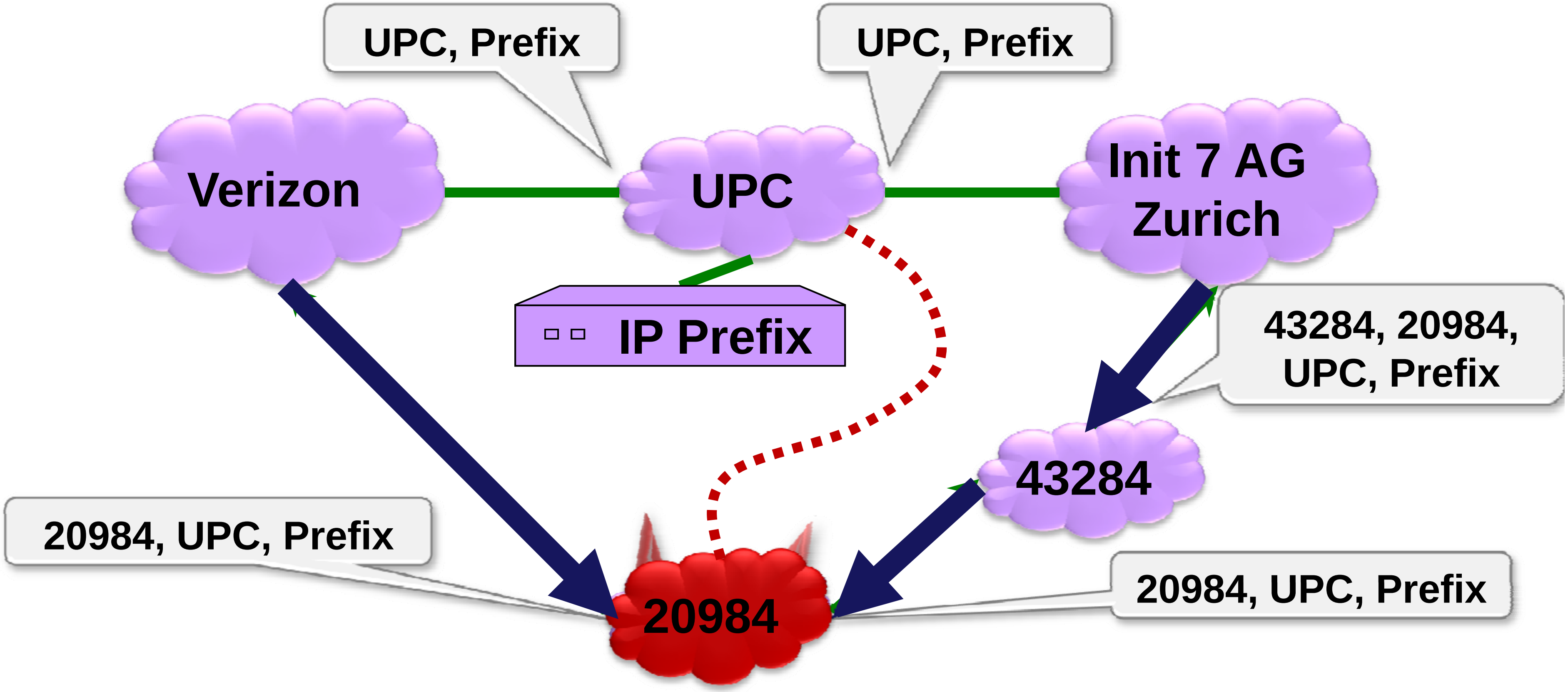
Origin Authentication: A secure database that maps IP Prefixes to their owner ASes.



Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Security Mechanism: Origin Authentication (5)

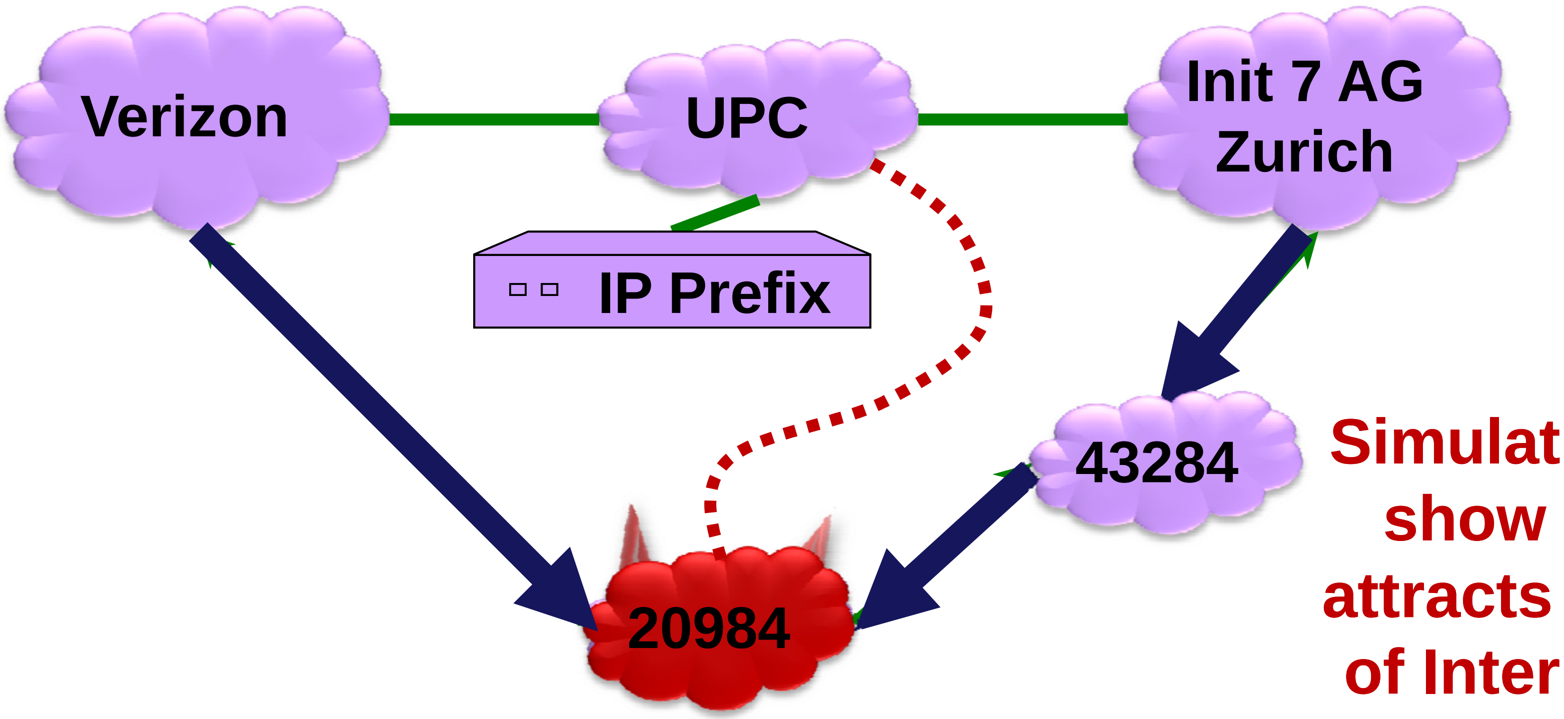
Origin Authentication: A secure database that maps IP Prefixes to their owner ASes.



Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Security Mechanism: Origin Authentication (6)

Origin Authentication: A secure database that maps IP Prefixes to their owner ASes.

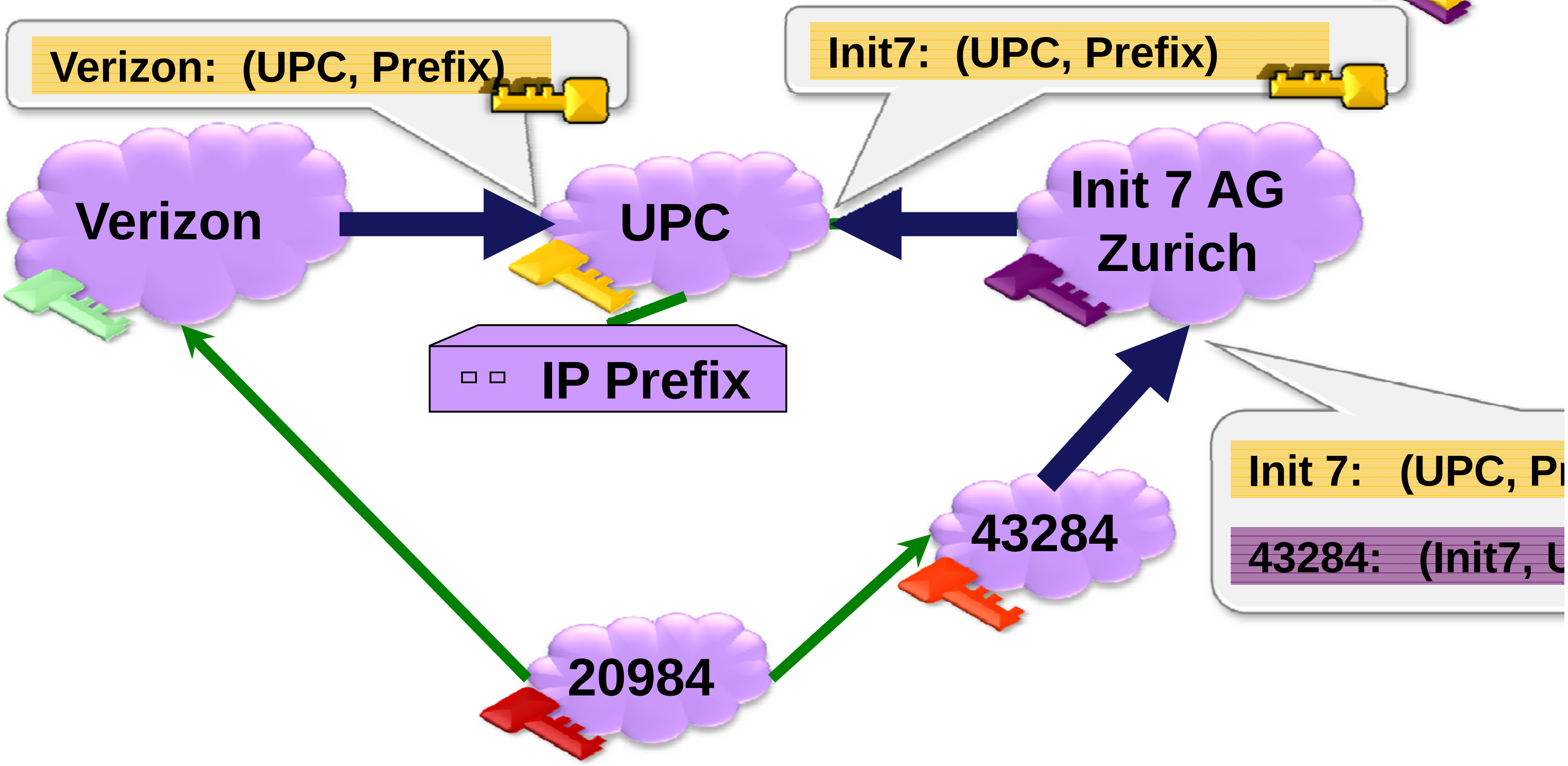


Simulations show he attracts 58% of Internet!

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Security Mechanism: “Secure BGP” [KLS98]

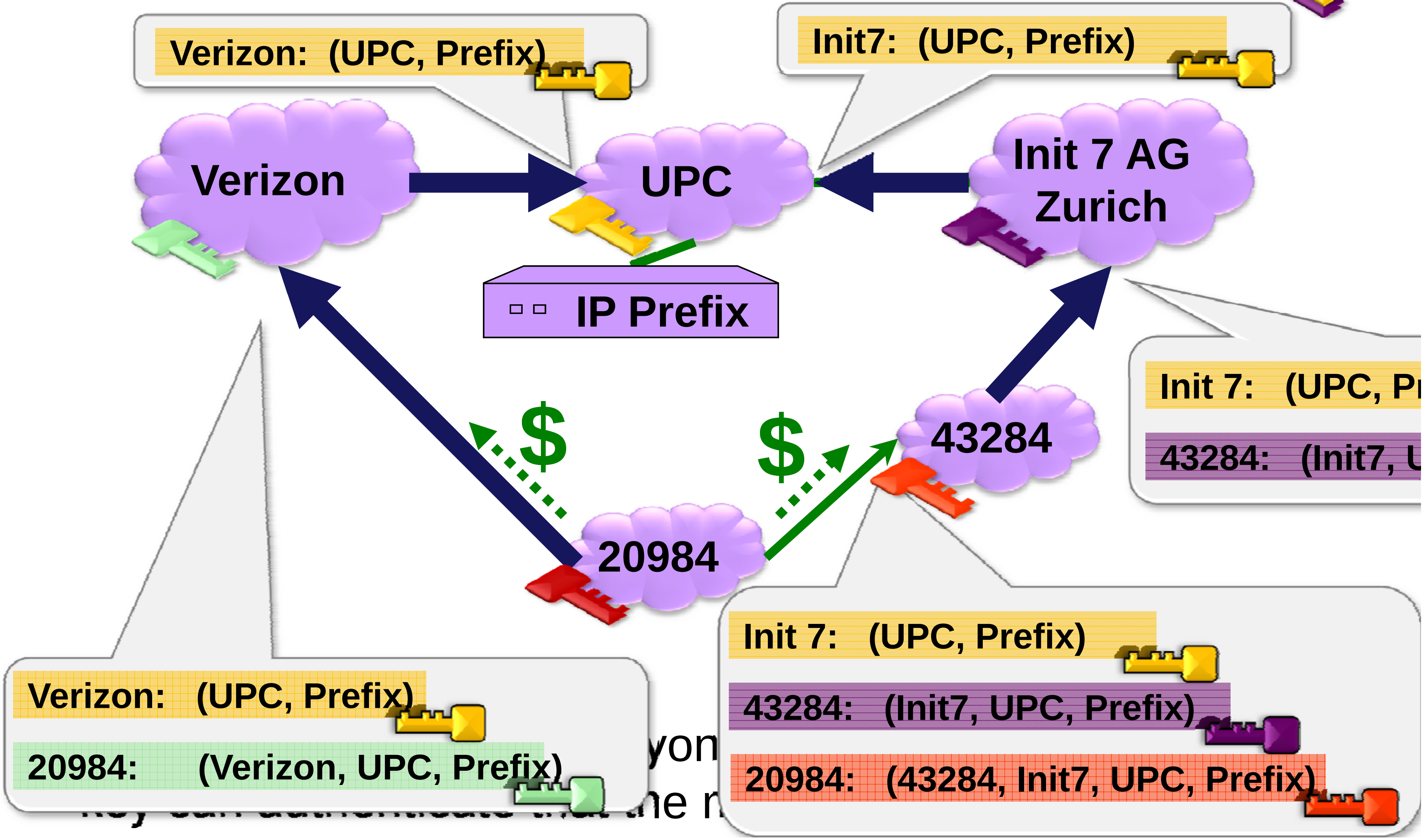
Secure BGP: Origin Authentication +
Cannot announce a path that was not announced to you.



Public Key Signature: Anyone who knows UPC’s public key can authenticate that the message was sent by UPC.

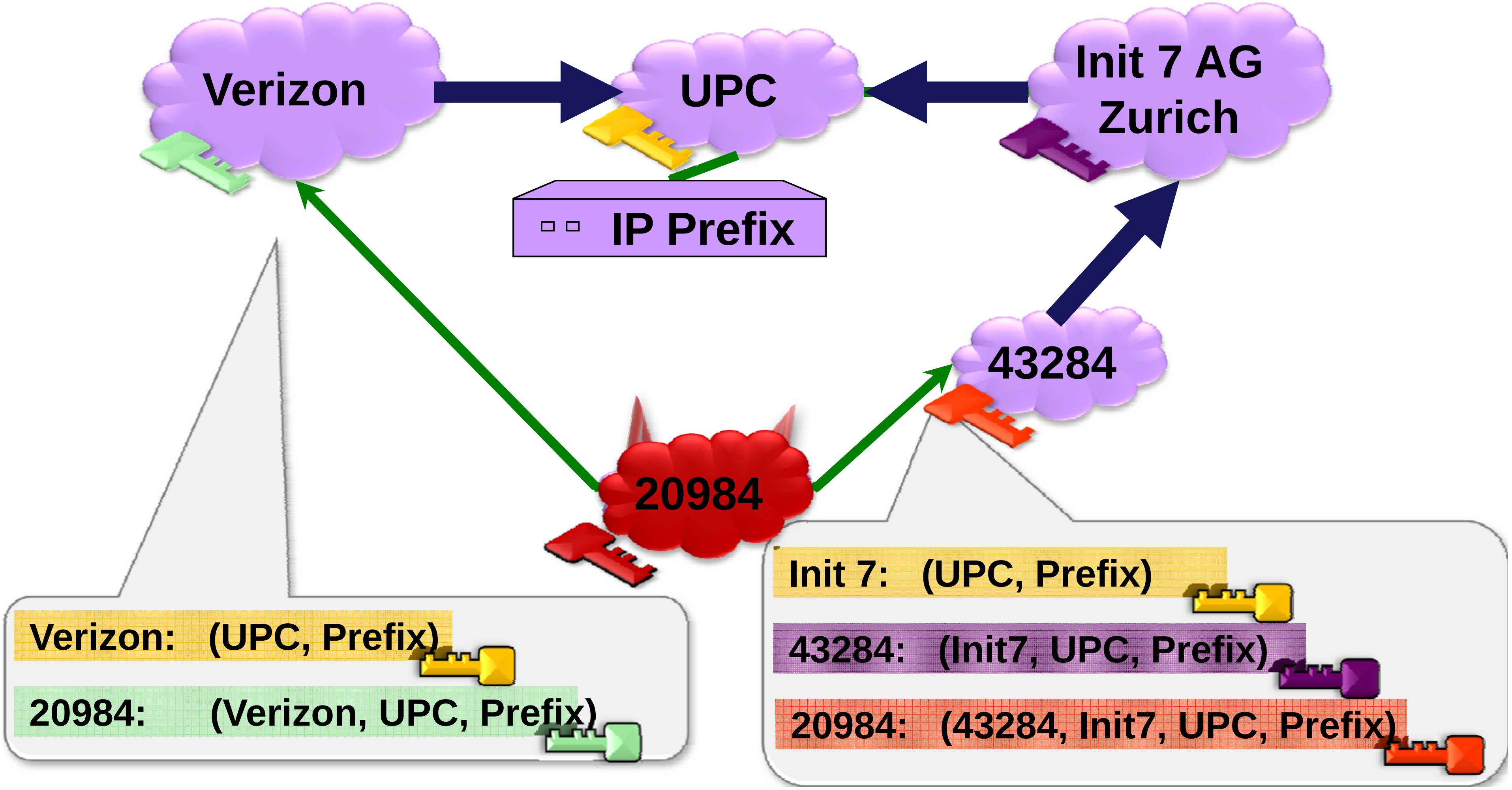
Security Mechanism: “Secure BGP” [KLS98]

Secure BGP: Origin Authentication +
Cannot announce a path that was not announced to you.



Are attacks still possible with Secure BGP? (0)

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



Verizon: (UPC, Prefix)

20984: (Verizon, UPC, Prefix)

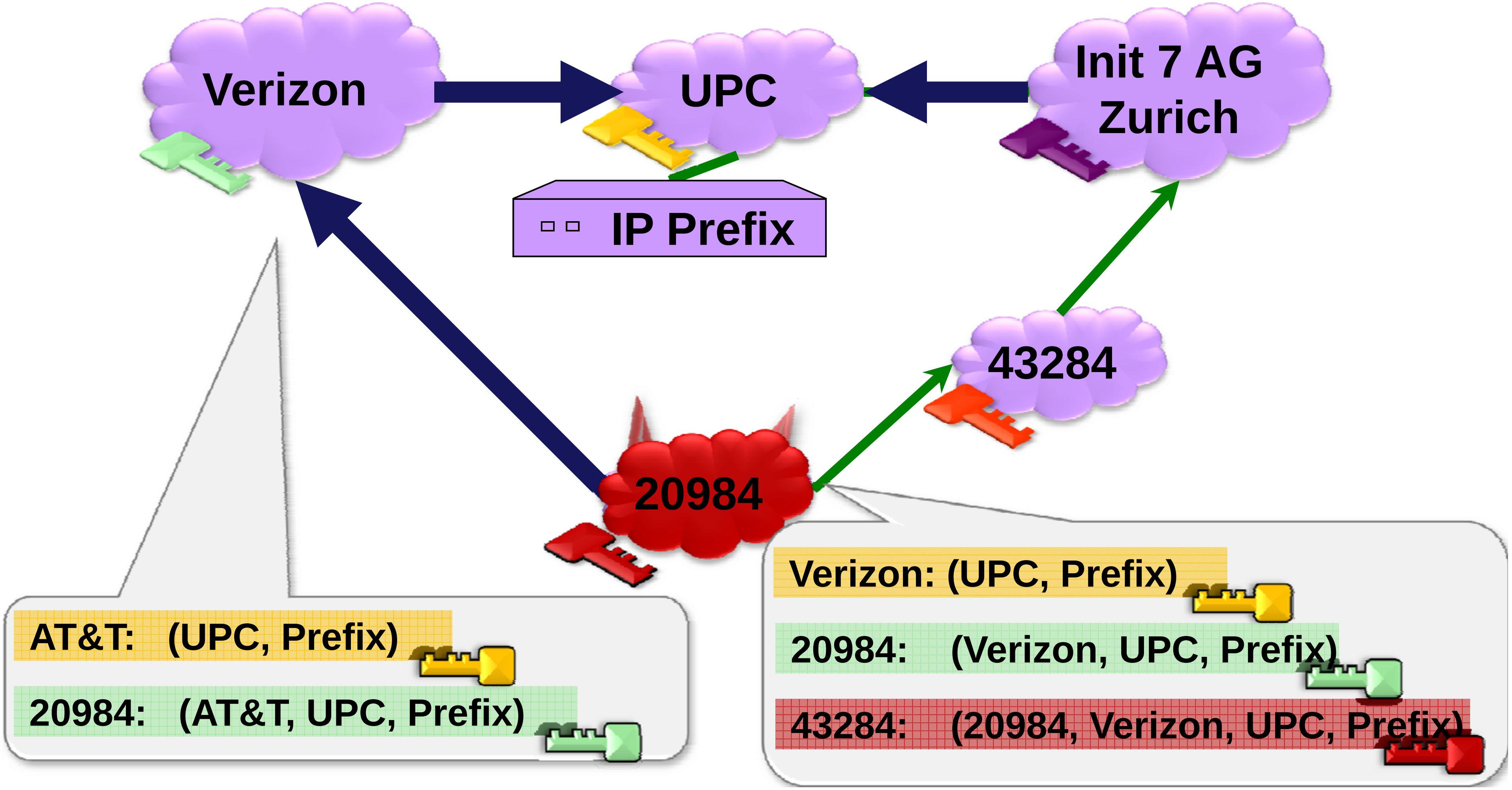
Init 7: (UPC, Prefix)

43284: (Init7, UPC, Prefix)

20984: (43284, Init7, UPC, Prefix)

Are attacks still possible with Secure BGP? (1)

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



AT&T: (UPC, Prefix)

20984: (AT&T, UPC, Prefix)

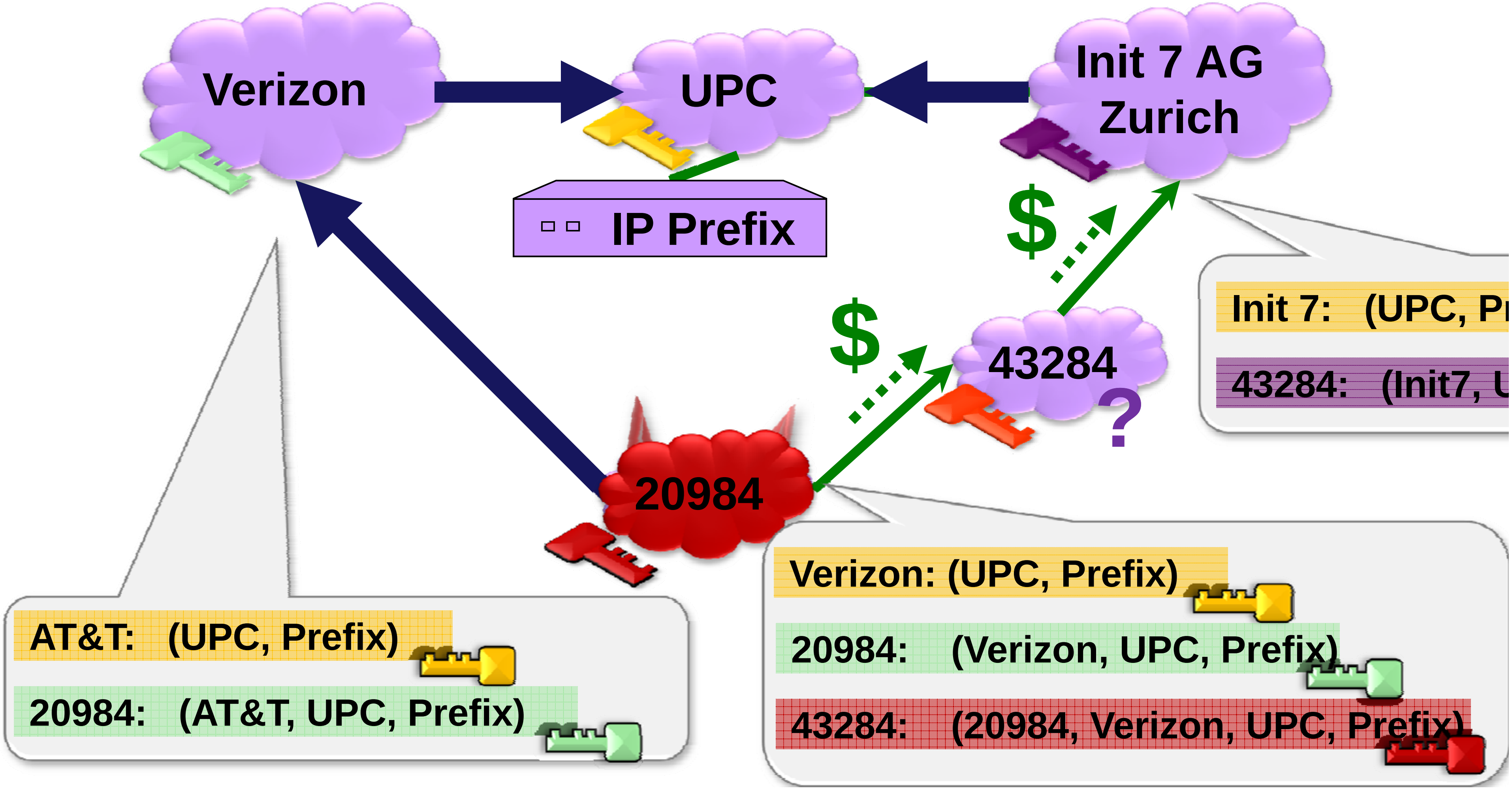
Verizon: (UPC, Prefix)

20984: (Verizon, UPC, Prefix)

43284: (20984, Verizon, UPC, Prefix)

Are attacks still possible with Secure BGP? (2)

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



Init 7: (UPC, Pr

43284: (Init7, U

AT&T: (UPC, Prefix)

20984: (AT&T, UPC, Prefix)

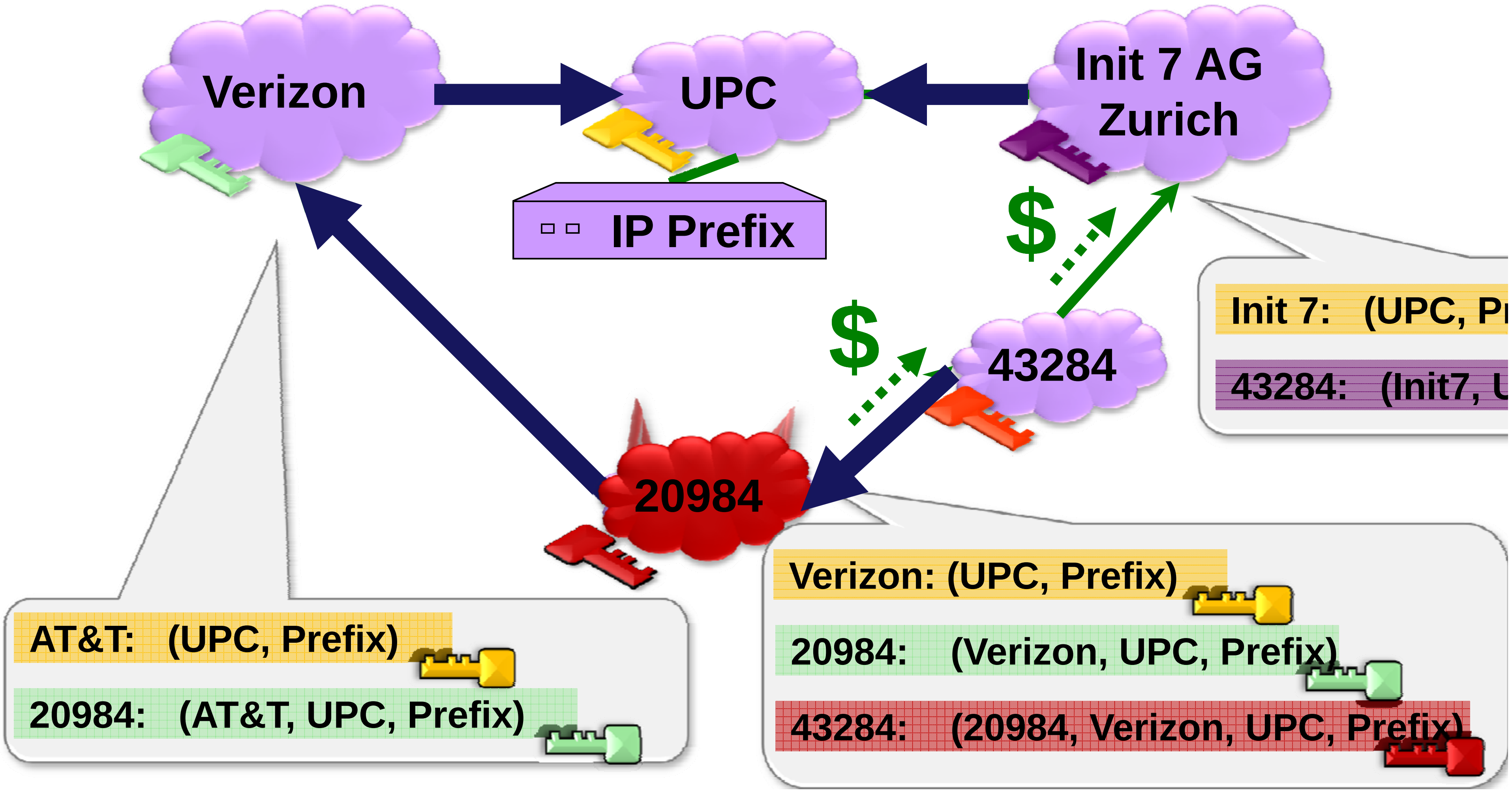
Verizon: (UPC, Prefix)

20984: (Verizon, UPC, Prefix)

43284: (20984, Verizon, UPC, Prefix)

Are attacks still possible with Secure BGP? (2)

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



AT&T: (UPC, Prefix)

20984: (AT&T, UPC, Prefix)

Verizon: (UPC, Prefix)

20984: (Verizon, UPC, Prefix)

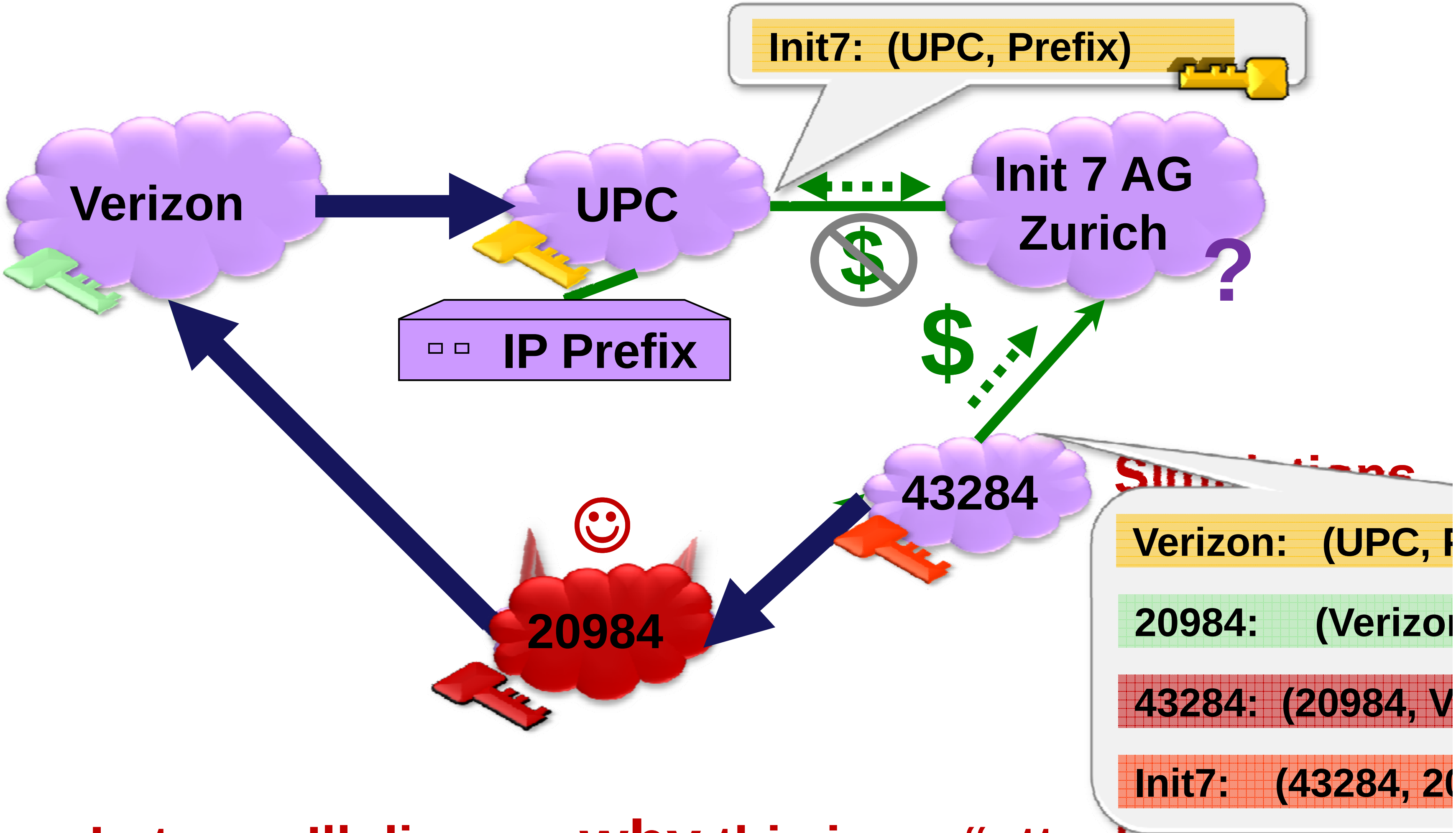
43284: (20984, Verizon, UPC, Prefix)

Init 7: (UPC, Pr

43284: (Init7, U

Are attacks still possible with Secure BGP? (3)

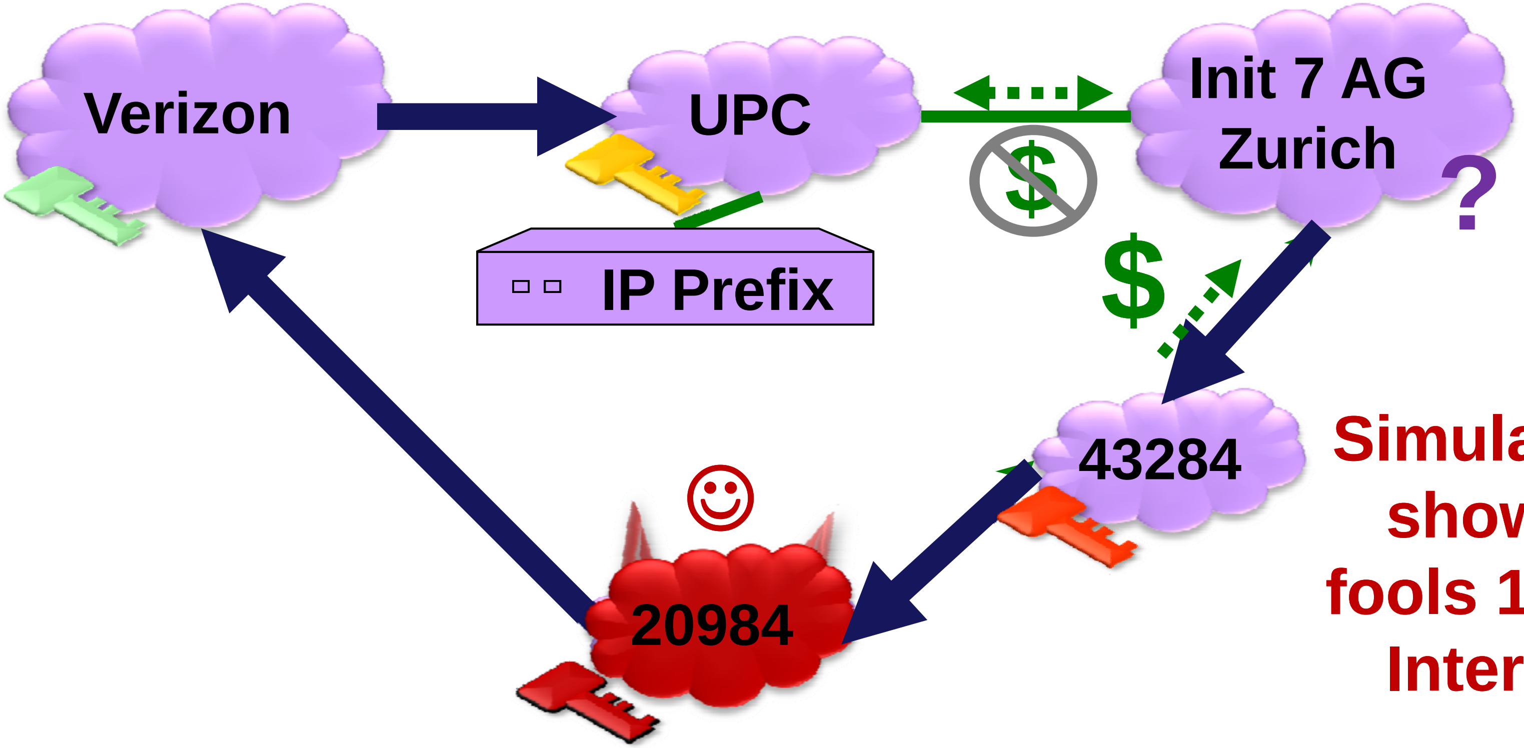
Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



Later we'll discuss why this is an "attack"

Are attacks still possible with Secure BGP? (4)

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

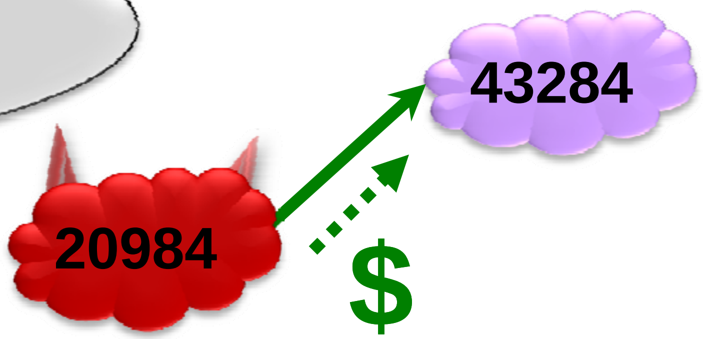


Simulations show he fools 16% of Internet!

Later we'll discuss why this is an "attack"

Wait! Is this the “best” attack strategy?!?

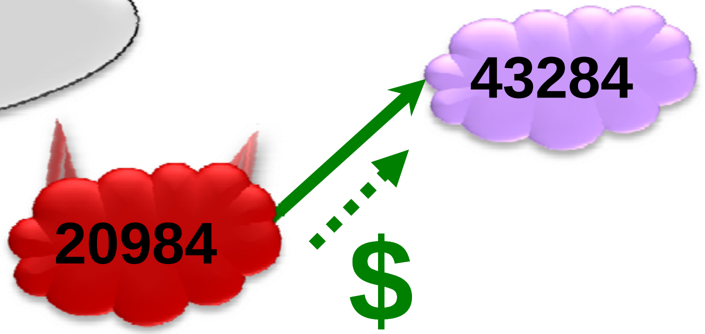
I can’t lie about my business relationship with AS 43284, so I might as well announce the shortest path I can.



Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Wait! Is this the “best” attack strategy?!?

I can’t lie about my business relationship with AS 43284, so I might as well announce the shortest path I can.



But Not Optimal !

Smart ^ **Attack Strategy:** Announce the shortest path I can get away with to all my neighbors!

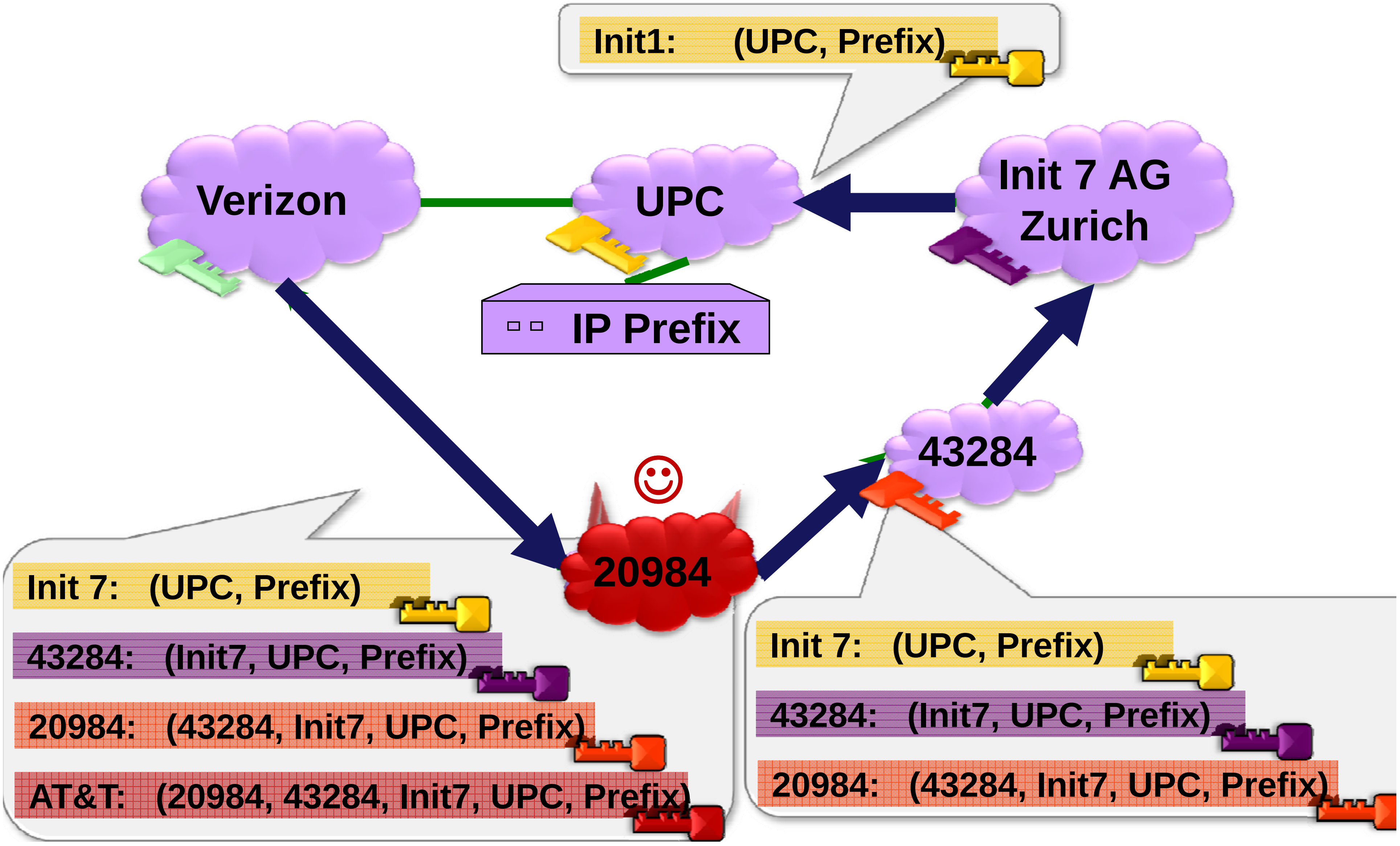
Sometimes announcing to **fewer** neighbors is better**!**

Sometimes **longer** paths are better!

Theorem: it’s NP hard to find the optimal attack strategy.

➔ Smart Attack Strategy **underestimates** damage.

Sometimes longer paths are better! (1)



Init1: (UPC, Prefix)

Init 7: (UPC, Prefix)

43284: (Init7, UPC, Prefix)

20984: (43284, Init7, UPC, Prefix)

AT&T: (20984, 43284, Init7, UPC, Prefix)

Init 7: (UPC, Prefix)

43284: (Init7, UPC, Prefix)

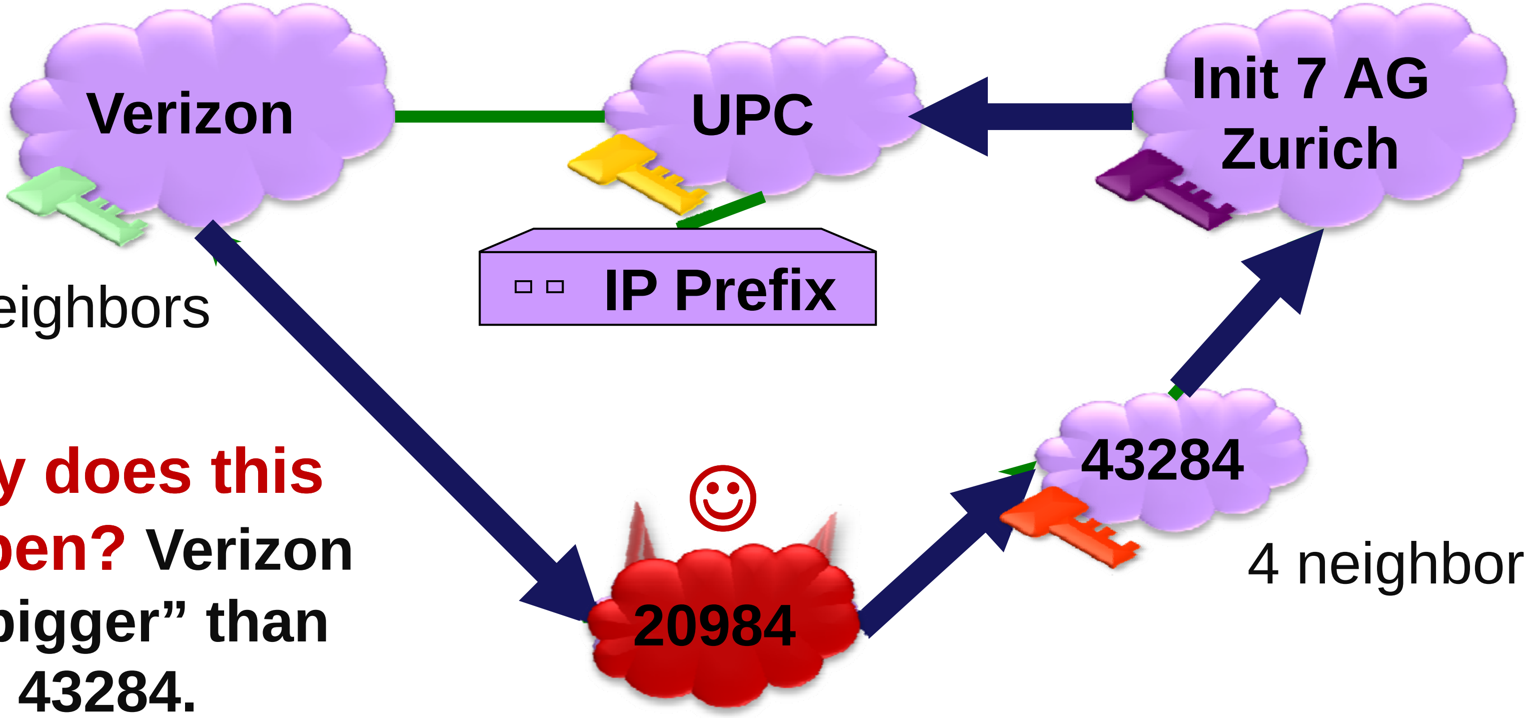
20984: (43284, Init7, UPC, Prefix)

Sometimes longer paths are better! (2)

Simulations show he attracts 56% of Internet!

With the shorter path, he attracts only 16% of Internet!

This is almost as much as attack on insecure BGP: 62%!



517 neighbors

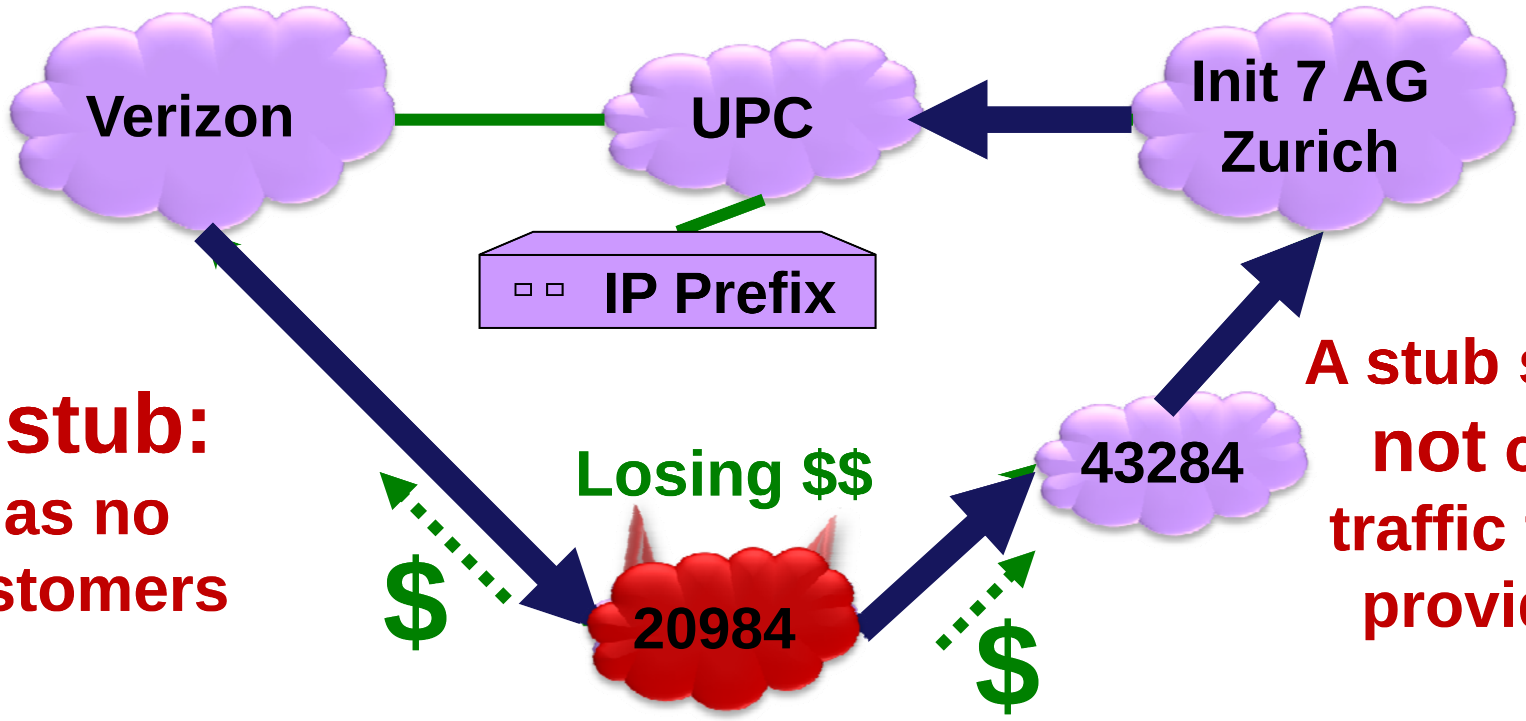
4 neighbors

Why does this happen? Verizon is “bigger” than 43284.

Key Observation: **Who** you announce to is as important as **what** you announce.

Wait! Why is this an “attack”?!?

Has 20984 done anything wrong?
He announces the path he actually uses!



A stub:
has no customers

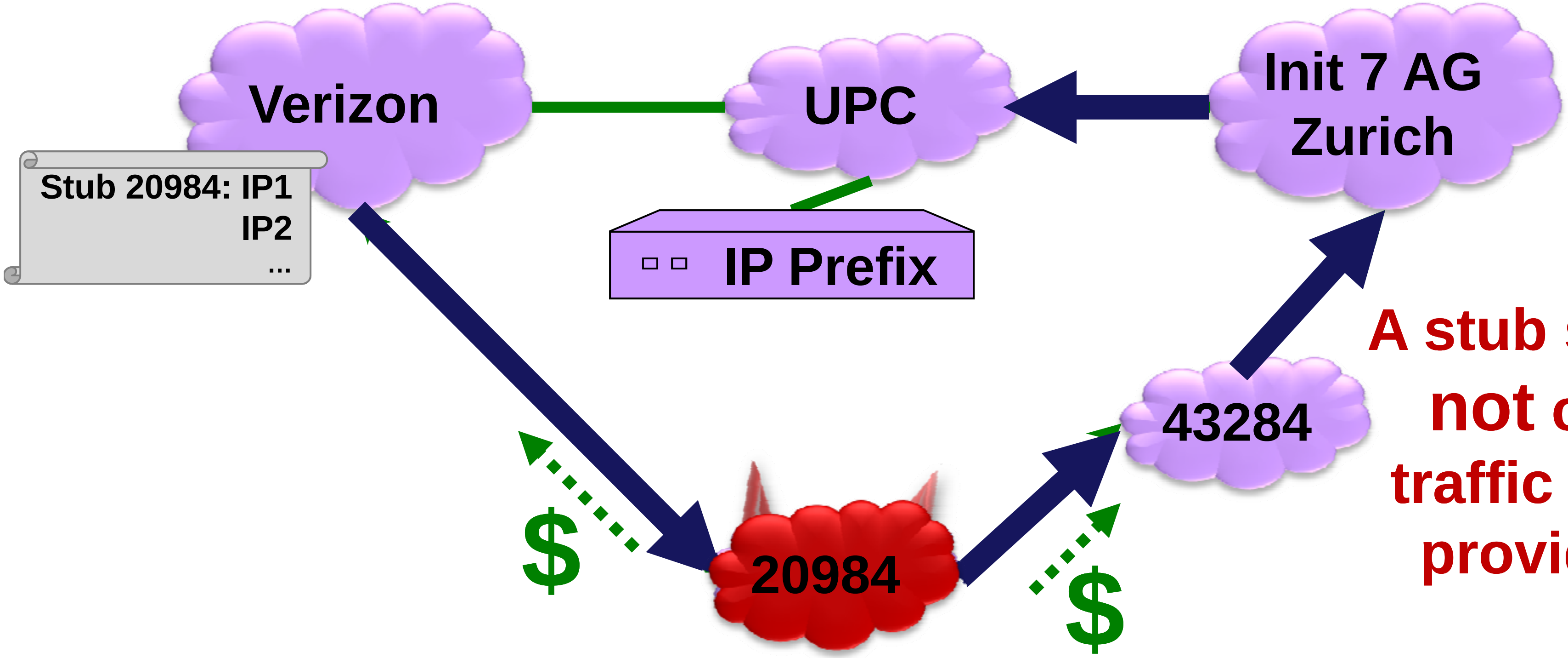
A stub should not carry traffic for its providers.

A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only carry traffic if it earns you money.

Security Heuristic: Defensive Filtering (1)

Defensive Filtering: The provider drops announcements for prefixes not owned by it's stubs.



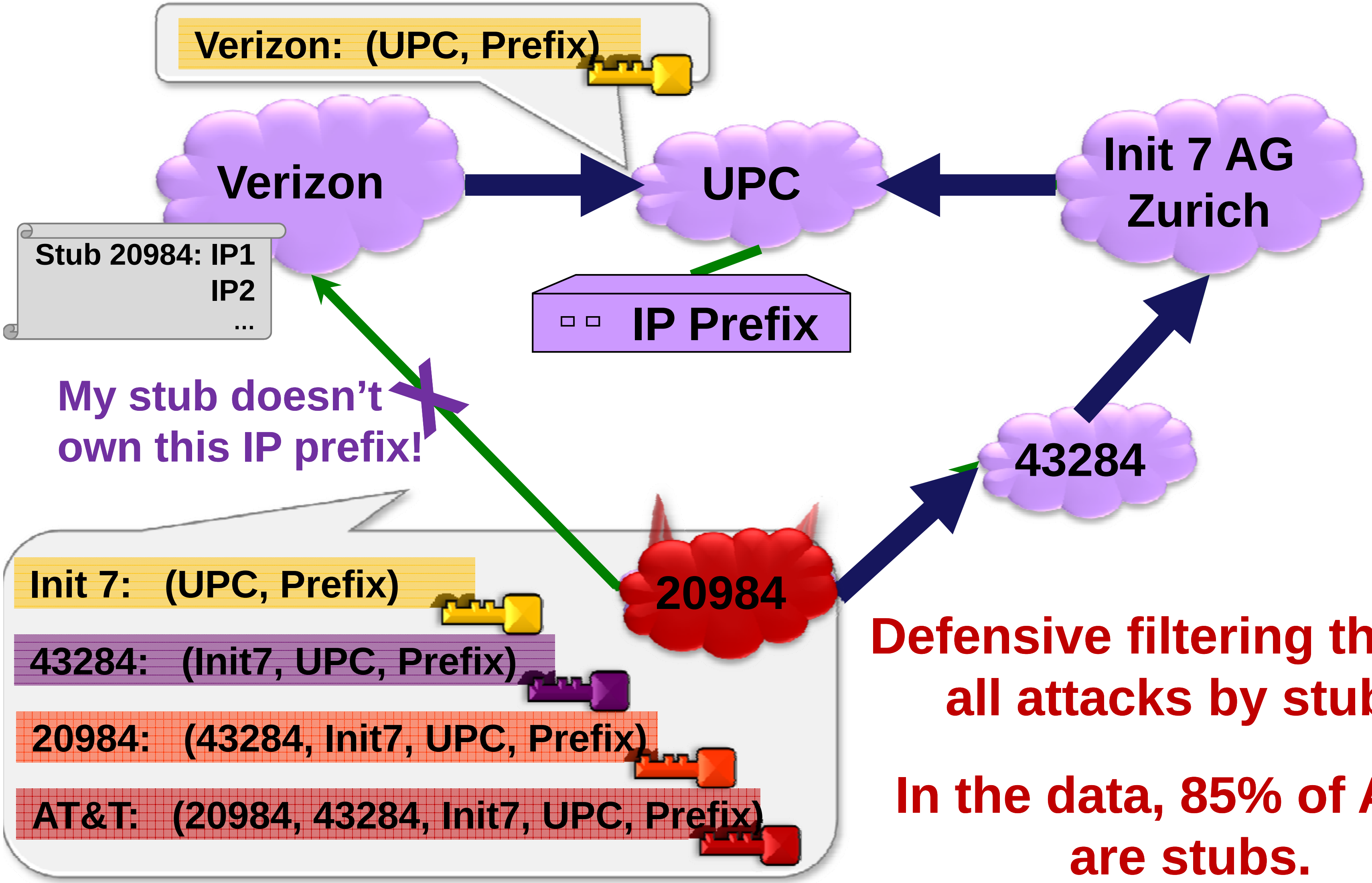
A stub should not carry traffic for its providers.

A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only carry traffic if it earns you money.

Security Heuristic: Defensive Filtering (2)

Defensive Filtering: The provider drops announcements for prefixes not owned by it's stubs.



Verizon: (UPC, Prefix)

Verizon

UPC

Init 7 AG Zurich

IP Prefix

Stub 20984: IP1
IP2
...

My stub doesn't own this IP prefix!

43284

20984

Init 7: (UPC, Prefix)

43284: (Init7, UPC, Prefix)

20984: (43284, Init7, UPC, Prefix)

AT&T: (20984, 43284, Init7, UPC, Prefix)

Defensive filtering thwarts all attacks by stubs!

In the data, 85% of ASes are stubs.

This talk

Part 1: A model of Interdomain Routing

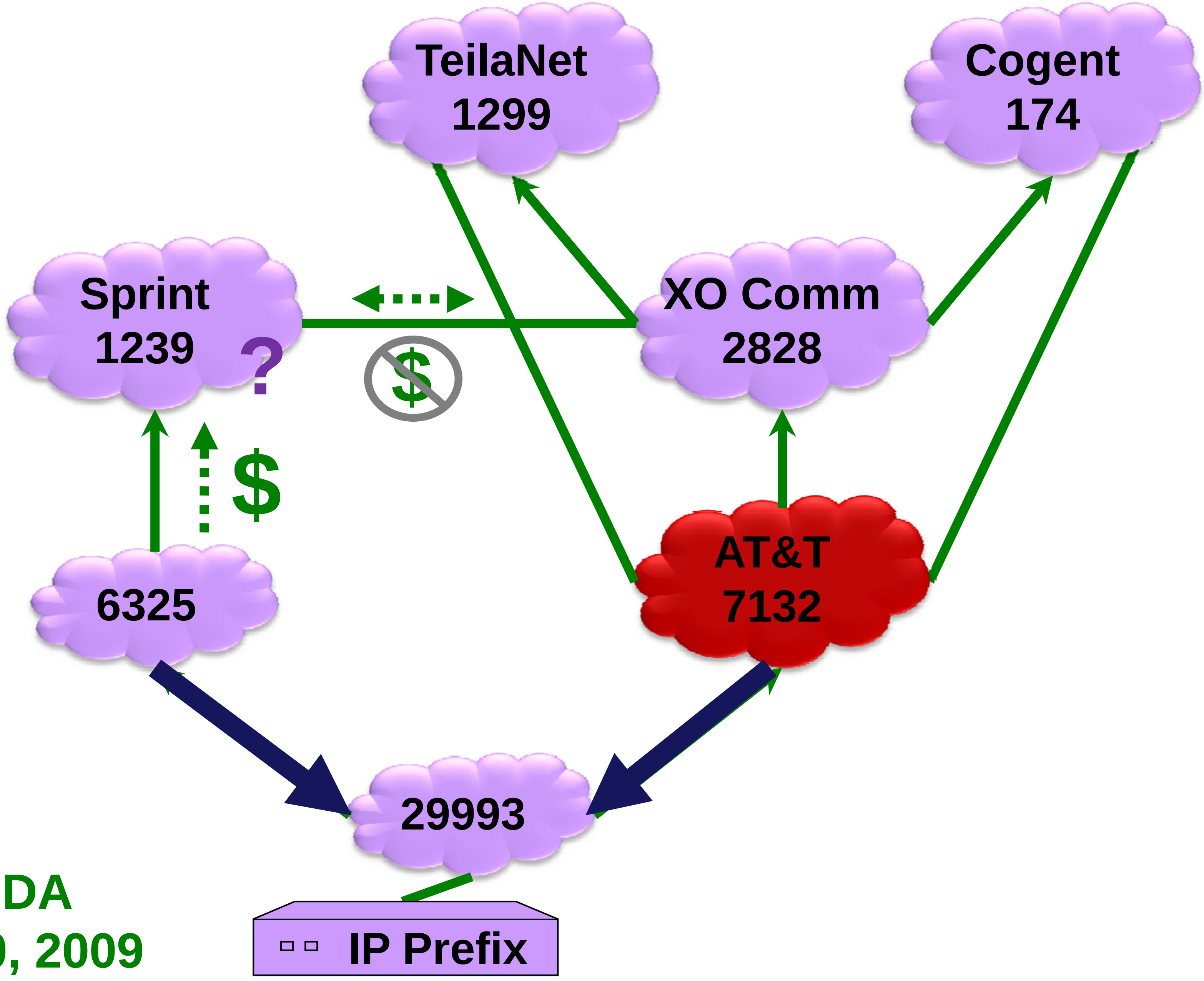
Part 2: Secure Routing Protocols and Attacks

- Plain BGP
- Origin Authentication
- Secure BGP

- Interlude: Finding the Optimal Attack
- Defensive Filtering
- ➡ Interlude: Attract more by announcing less

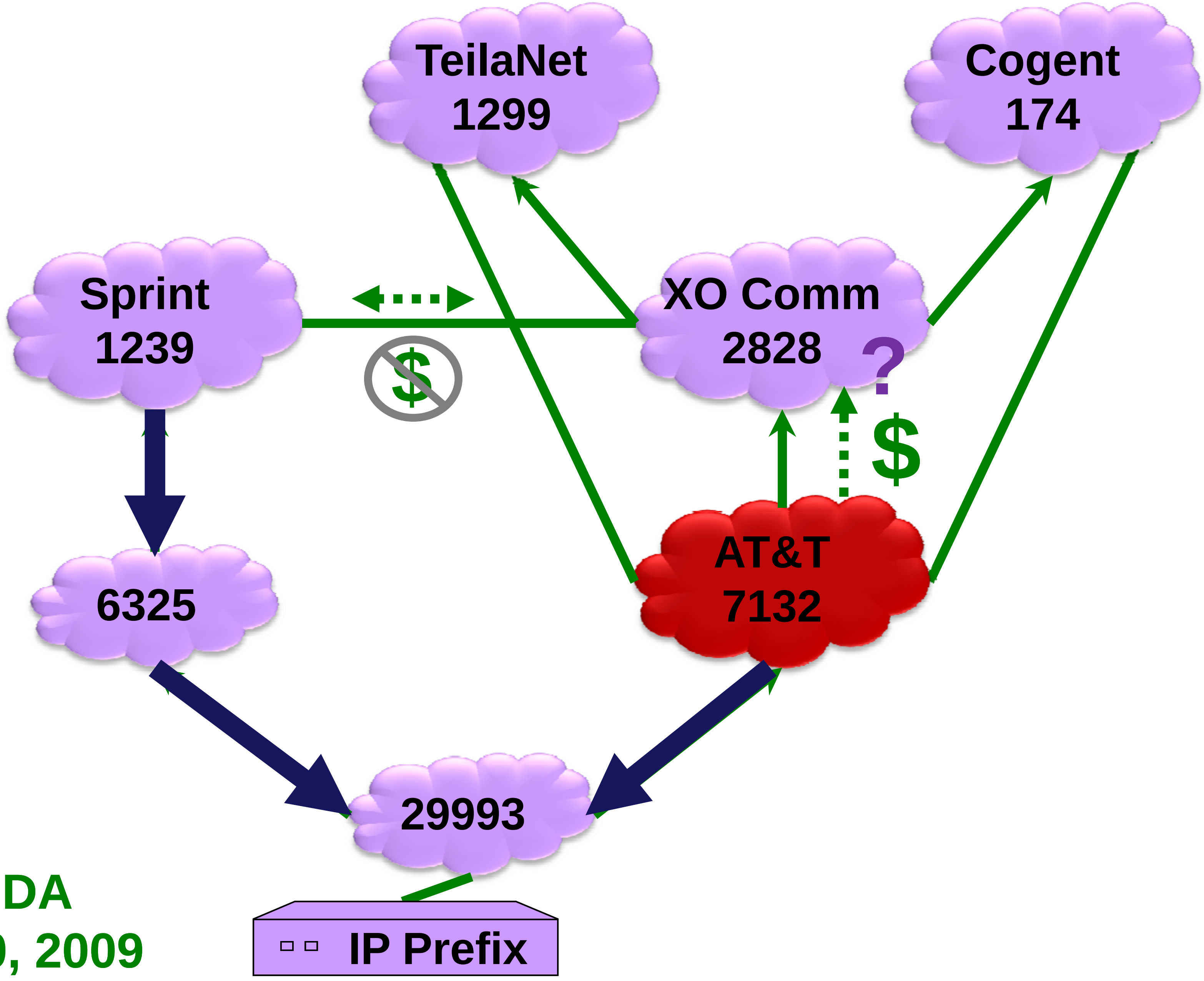
Part 3: Results and Implications

Attract More by Exporting Less (Naïve) ! (1)



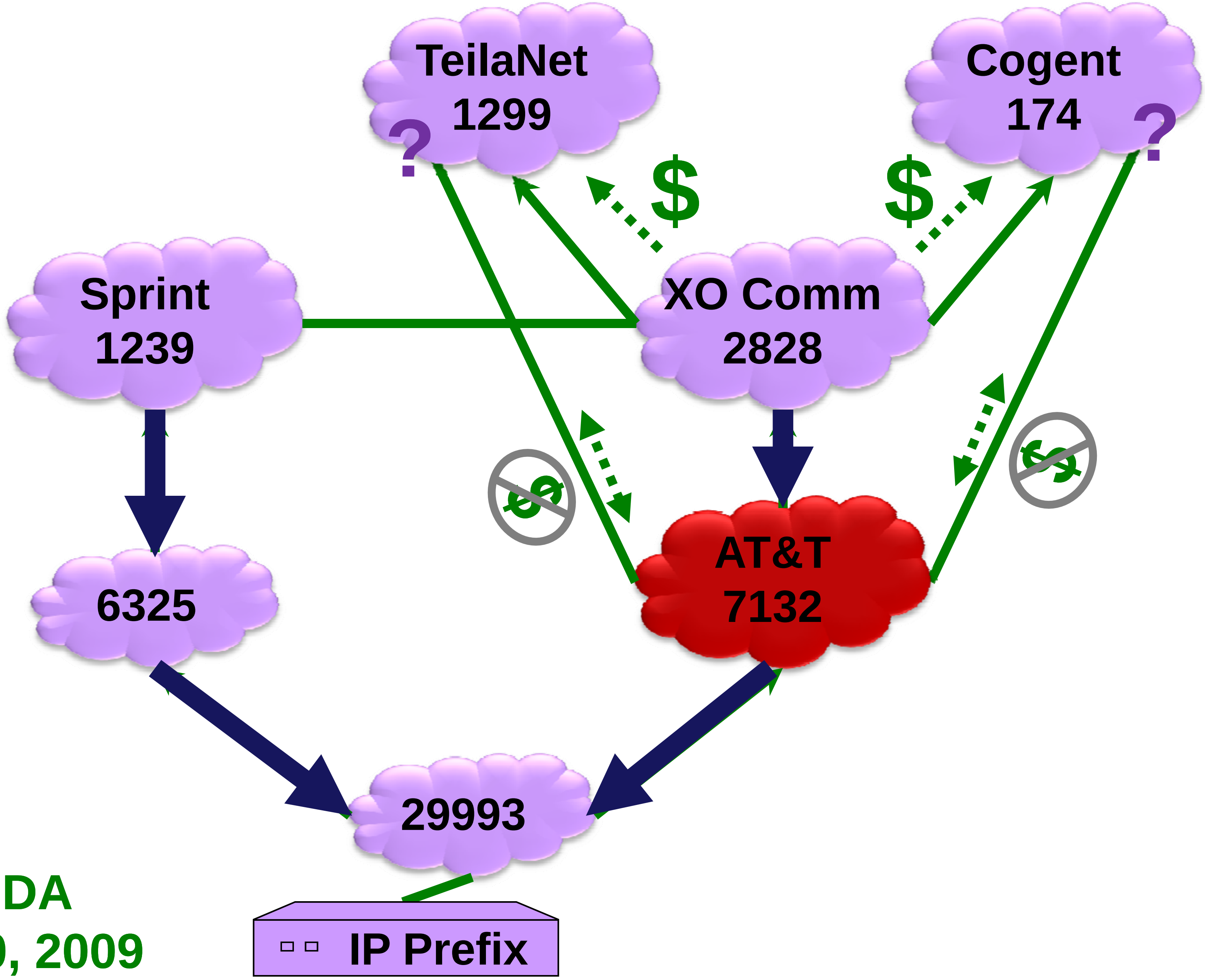
CAIDA
Nov 20, 2009

Attract More by Exporting Less (Naïve) ! (2)



CAIDA
Nov 20, 2009

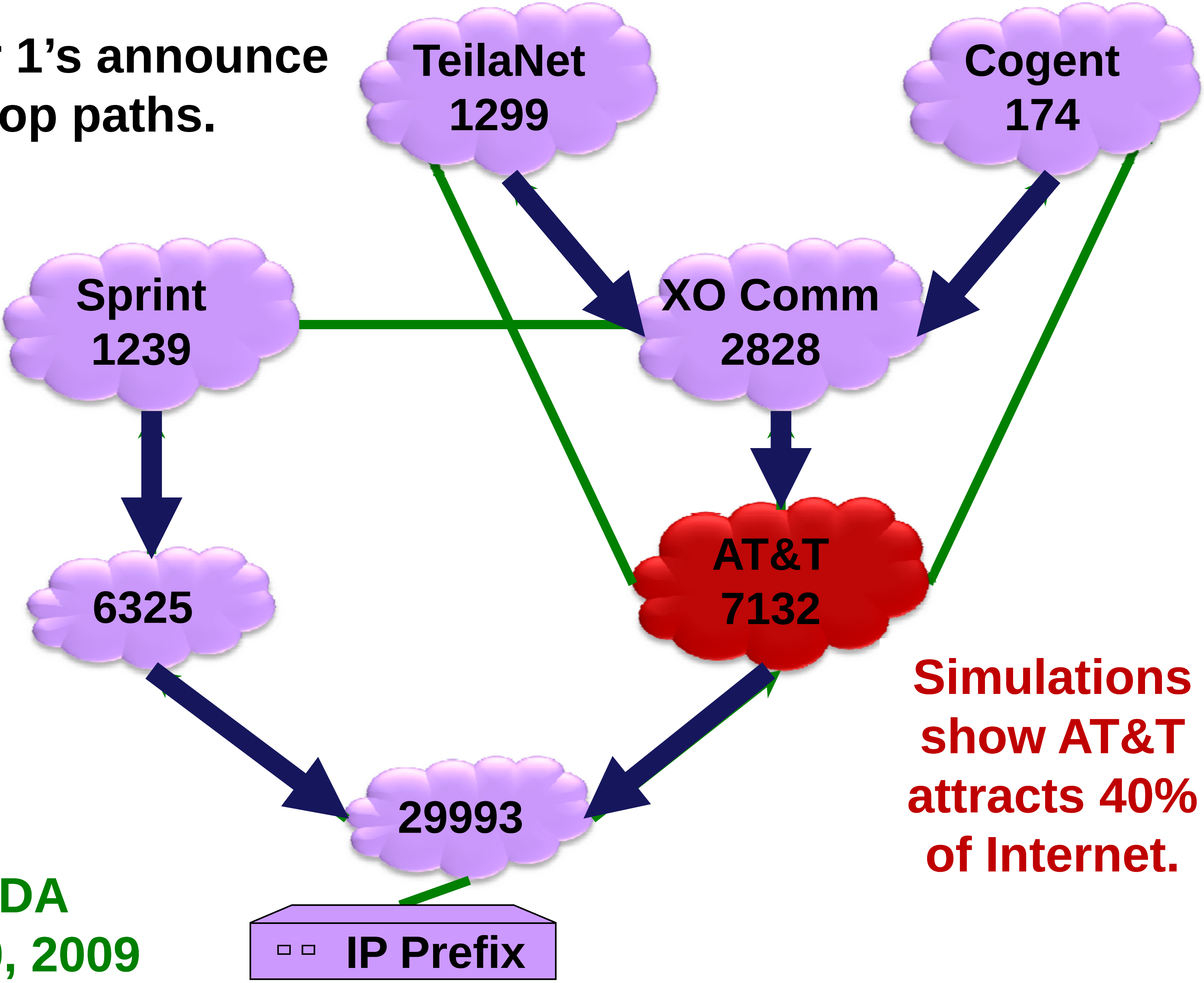
Attract More by Exporting Less (Naïve) ! (3)



CAIDA
Nov 20, 2009

Attract More by Exporting Less (Naïve) ! (4)

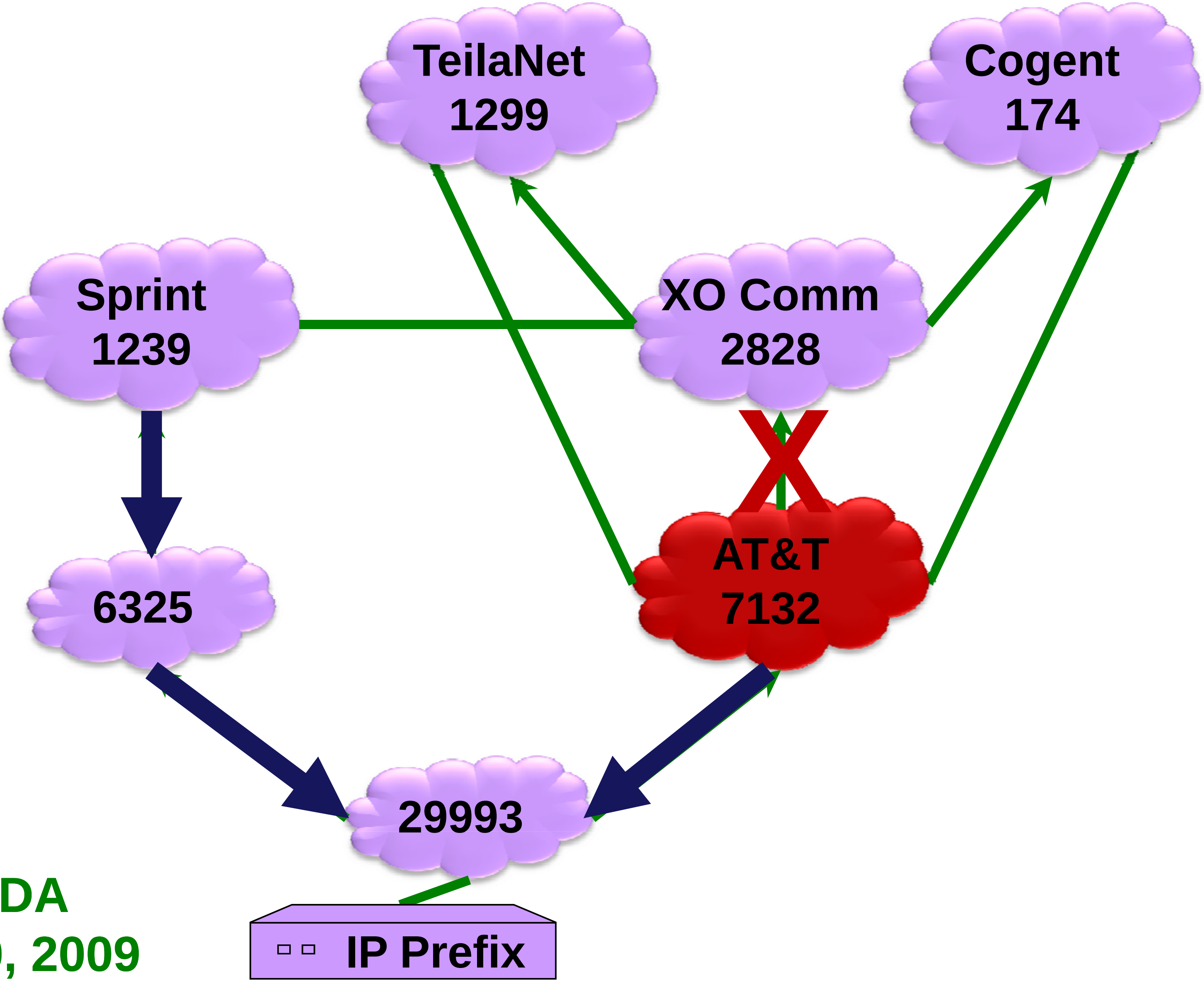
The Teir 1's announce
4 hop paths.



Simulations
show AT&T
attracts 40%
of Internet.

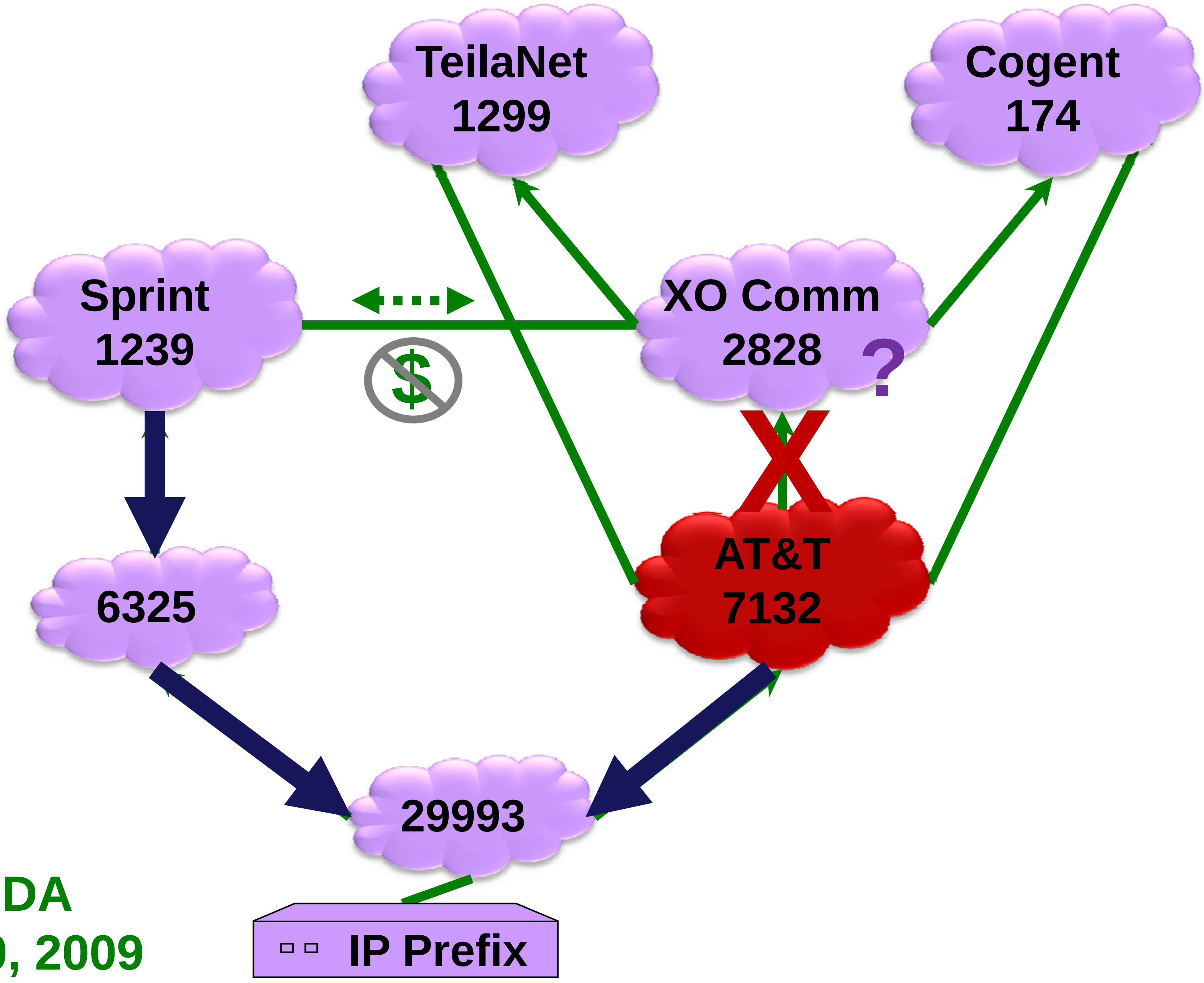
CAIDA
Nov 20, 2009

Attract More by Exporting Less (Clever) ! (1)



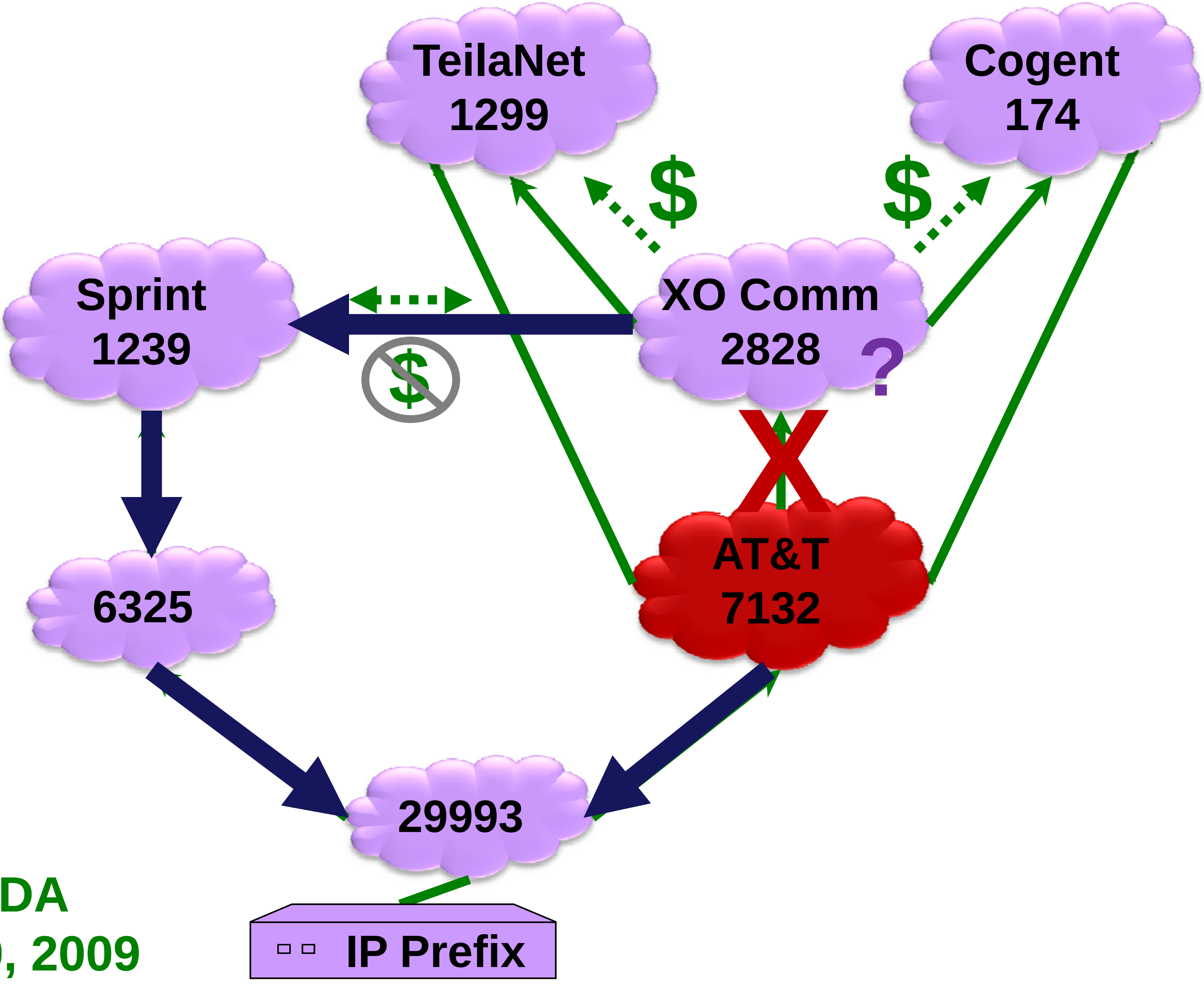
CAIDA
Nov 20, 2009

Attract More by Exporting Less (Clever) ! (2)



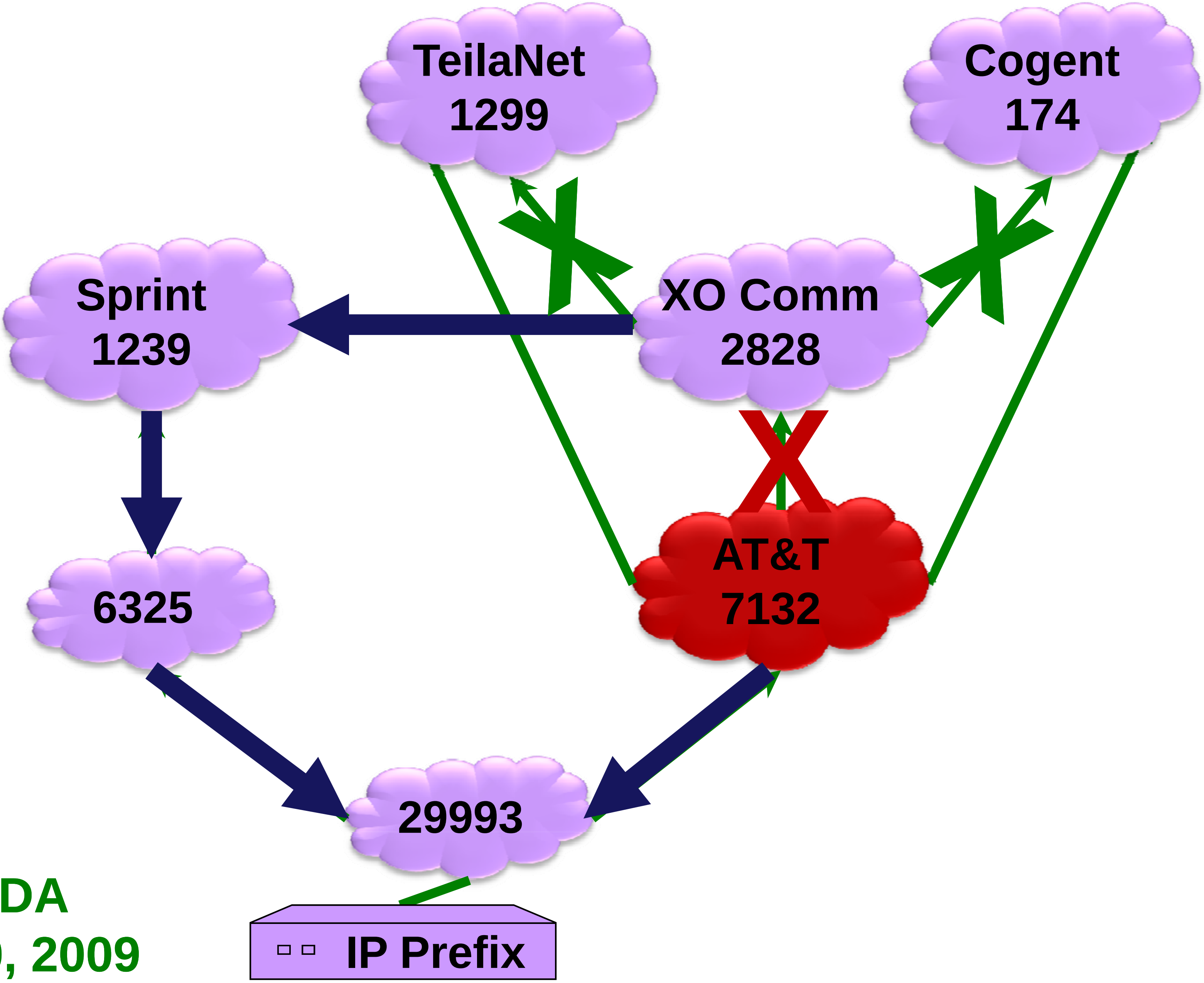
CAIDA
Nov 20, 2009

Attract More by Exporting Less (Clever) ! (3)



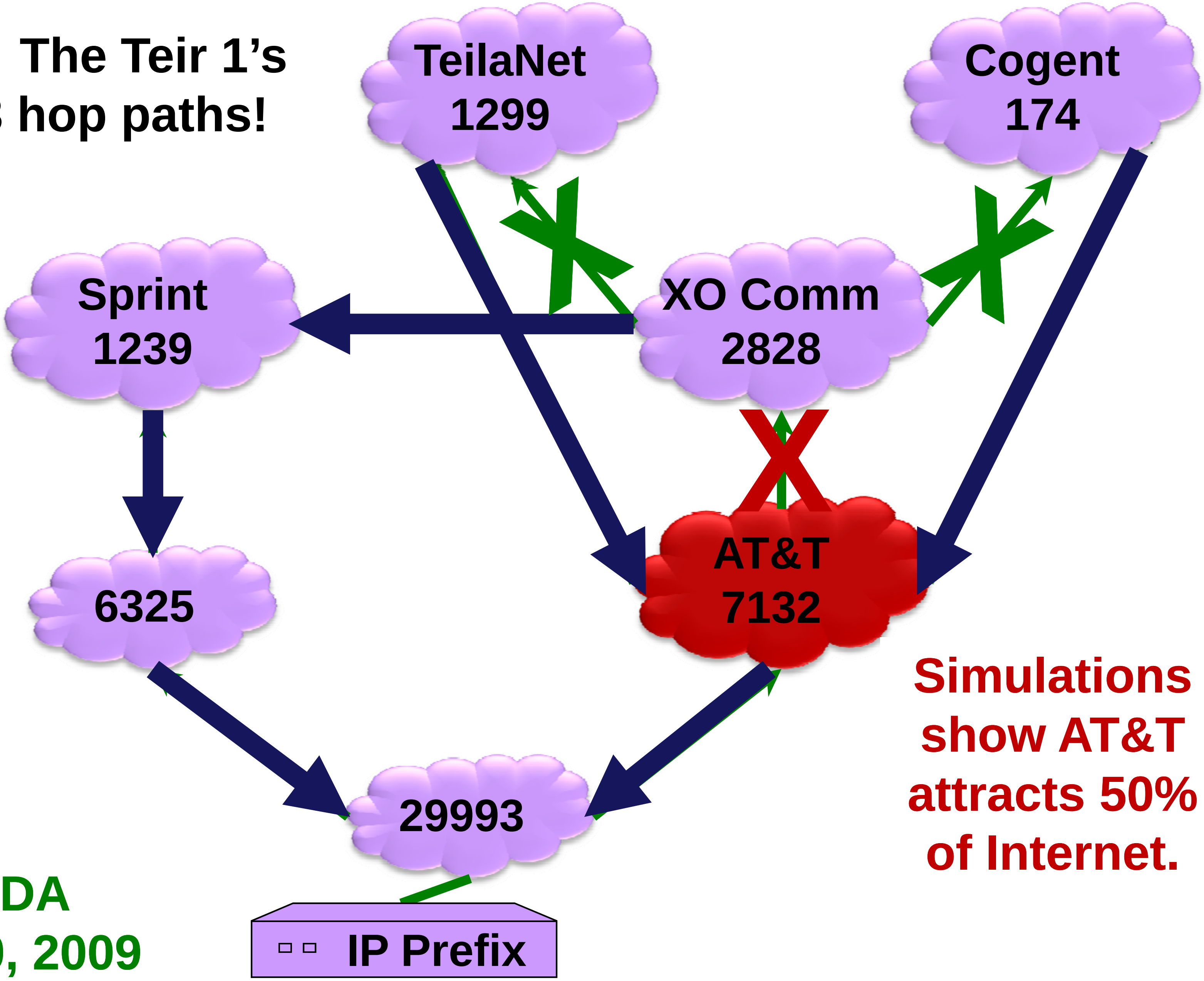
CAIDA
Nov 20, 2009

Attract More by Exporting Less (Clever) ! (4)



CAIDA
Nov 20, 2009

Attract More by Exporting Less (Clever) ! (5)



Why? The Teir 1's use 3 hop paths!

Simulations show AT&T attracts 50% of Internet.

CAIDA
Nov 20, 2009

This talk

Part 1: A model of Interdomain Routing

Part 2: Secure Routing Protocols and Attacks

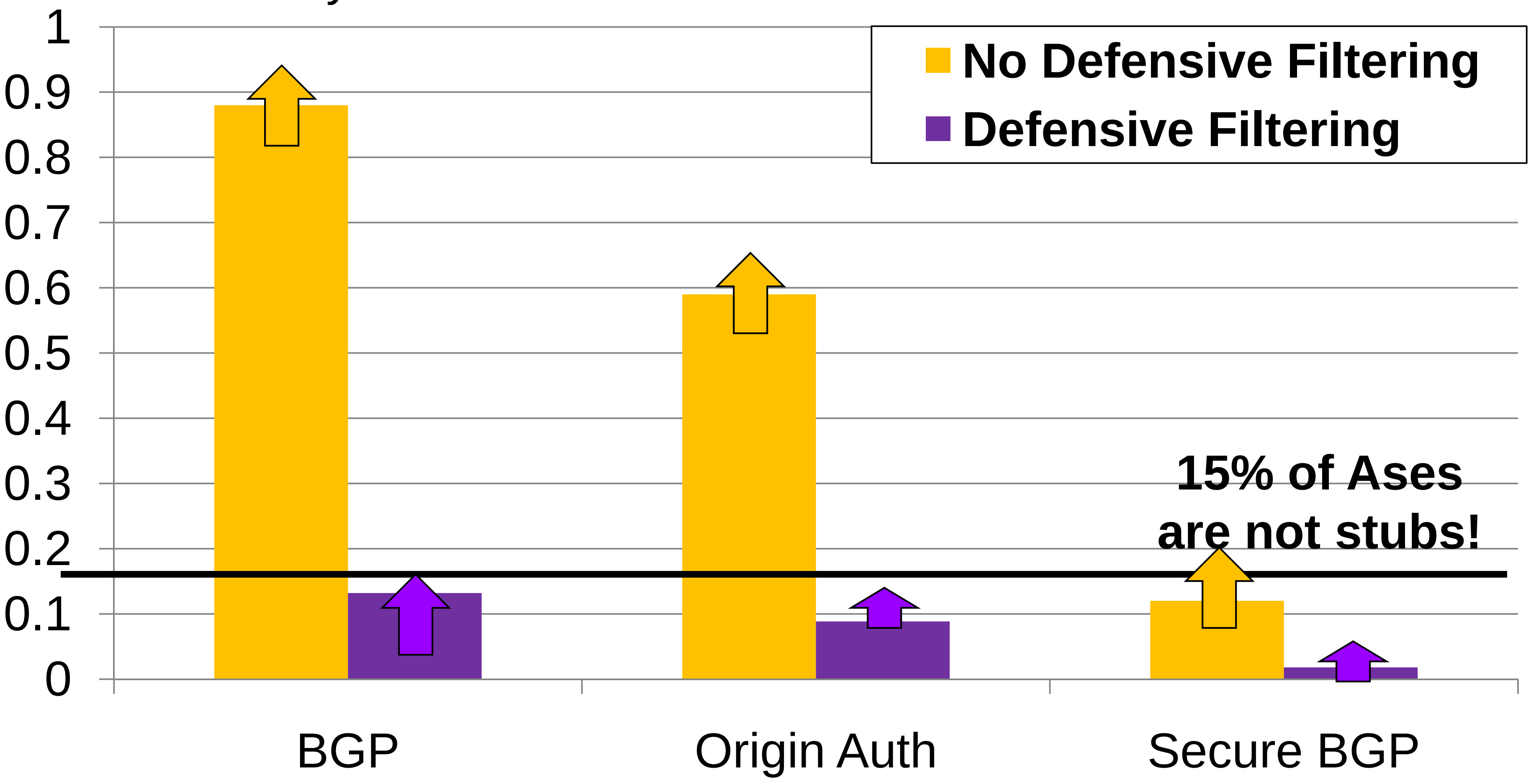
- Plain BGP
- Origin Authentication
- Secure BGP
- Interlude: Finding the Optimal Attack

- Defensive Filtering
- Interlude: Attract more by announcing less

Part 3: Results and Implications

Probability* the Smart Attack attracts 10% of Internet

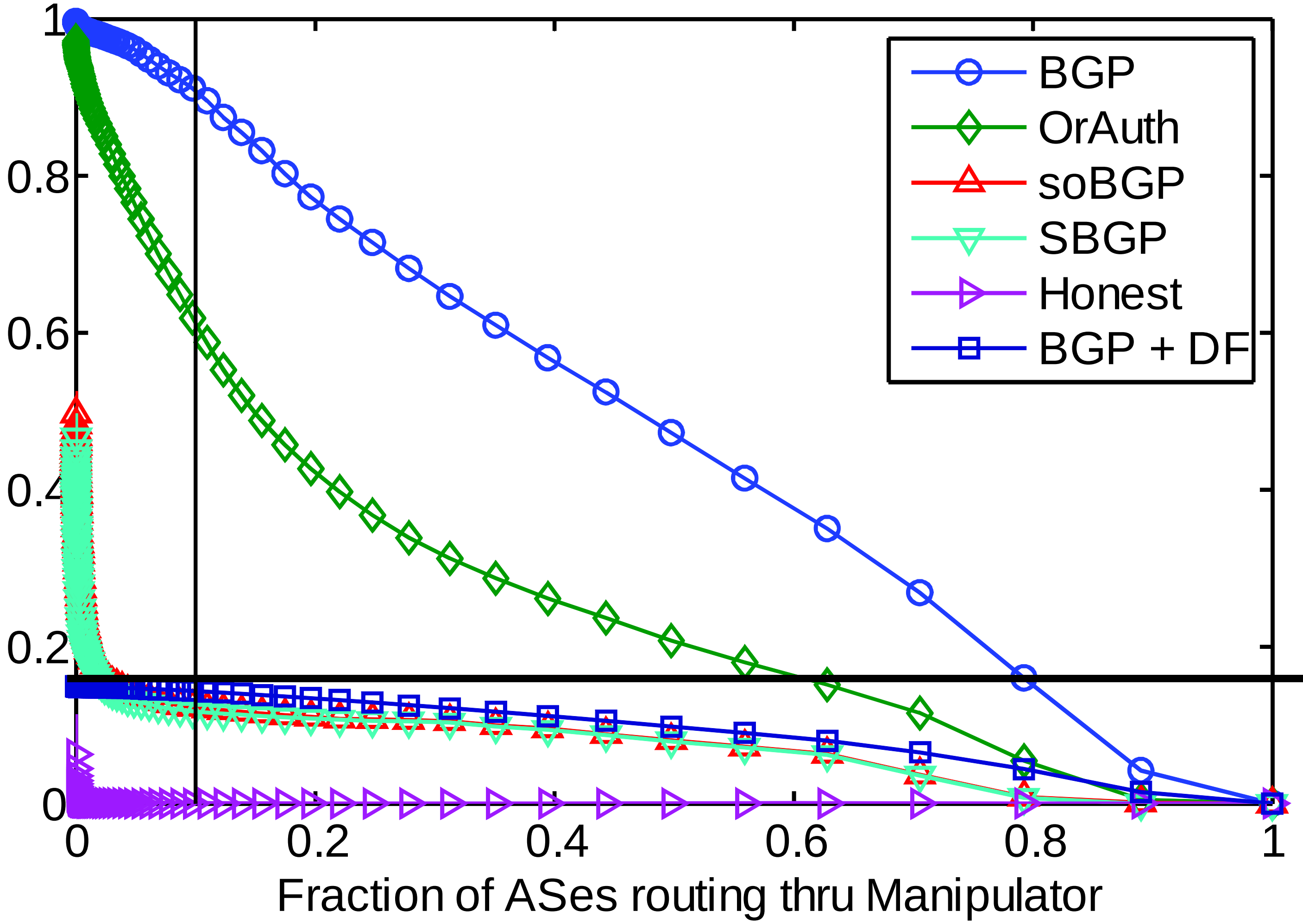
*Probability is taken over random choice of attacker and victim.



Recall that the **Smart Attack Strategy** **underestimates** damage.

Probability* Smart Attack attracts >x% of Internet (1)

*Probability is taken over random choice of attacker and victim.



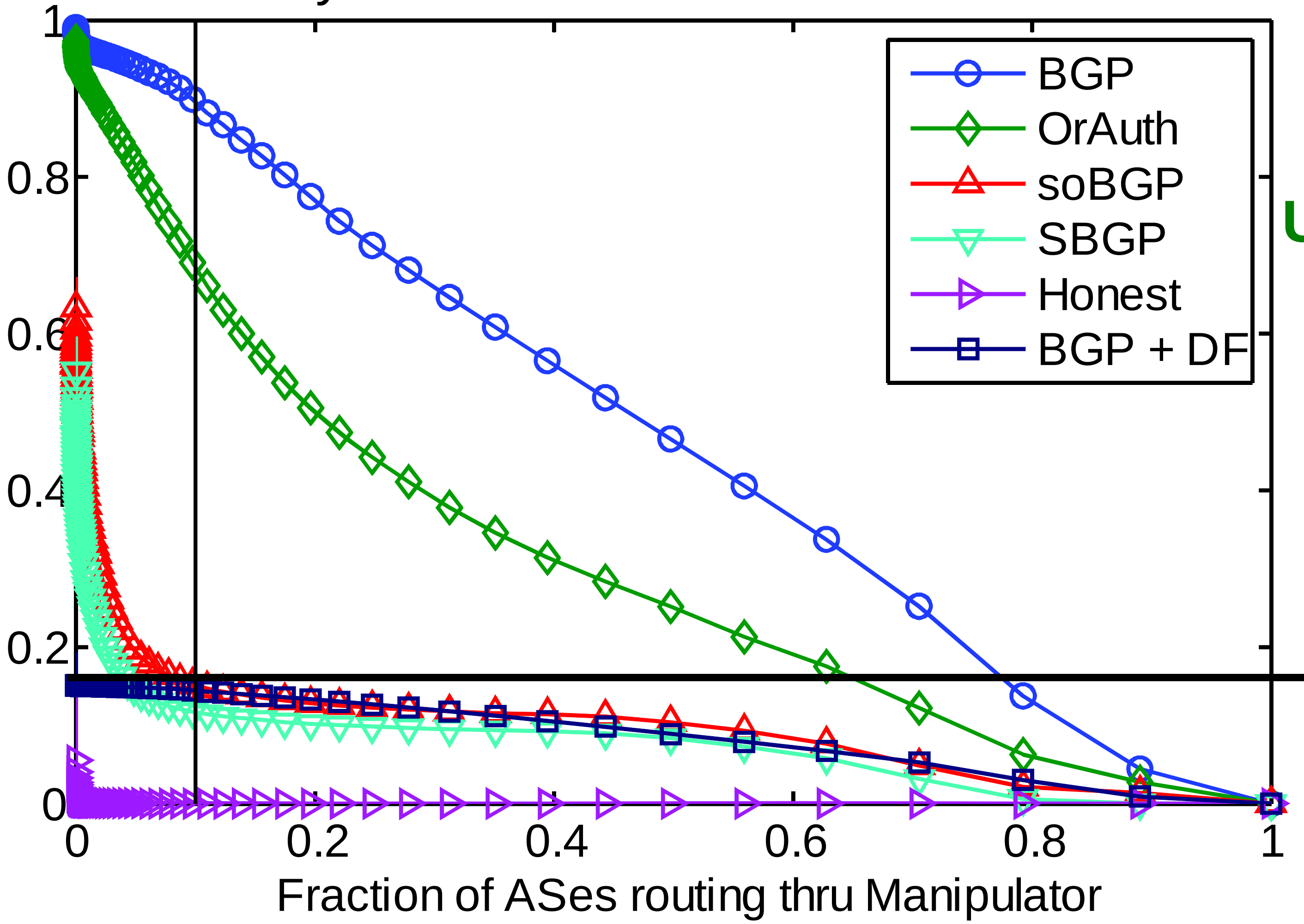
**CAIDA
Nov 20, 2009**

**15% of Ases
are not stubs!**

Recall that the **Smart Attack Strategy** **underestimates** damage.

Probability* Smart Attack attracts >x% of Internet (2)

*Probability is taken over random choice of attacker and victim.



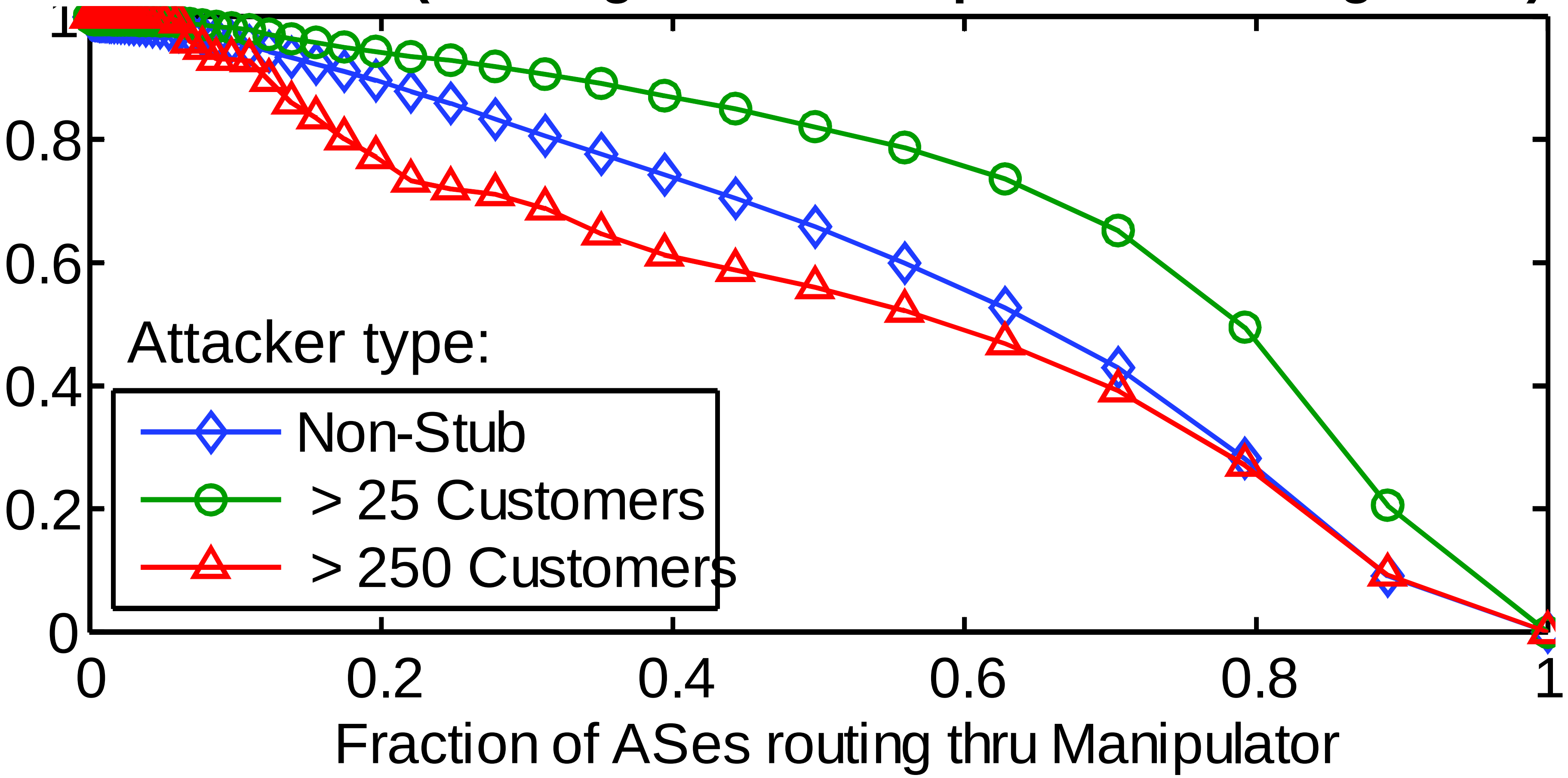
UCLA Cyclops
Nov 20, 2009

15% of Ases
are not stubs!

Recall that the **Smart Attack Strategy** **underestimates** damage.

Tier 2's are the most effective attackers

Probability* of Attracting >x% of the Internet
Attack on BGP (i.e. Originate victim prefix to all neighbors)



*Probability is over random victim and attacker from different classes

Conclusions (1) : Theory & Simulations

1) **Who you tell is as important as what you say.**
   - **Secure BGP constrains the paths announced**
   - **… but not to whom they are announced.**

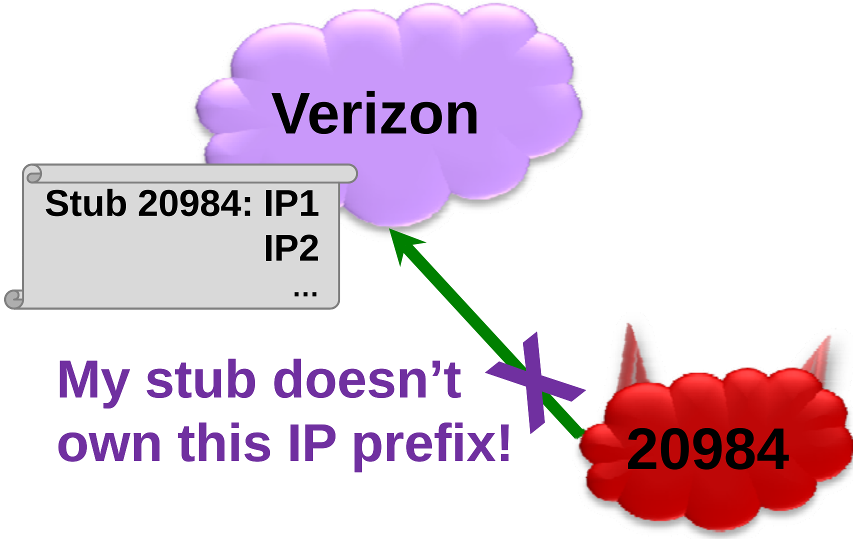
2) **Finding the optimal attack is NP hard**
   - **Announcing shortest paths is not always optimal**
   - **Exporting to all neighbors is not always optimal**
   - **➔ its hard to rigorously compare secure protocols**

3) **Defensive filtering is crucial even with Secure BGP**
   - **How to find incentives for providers to police stubs?**

Conclusions (2): Implementing Defensive Filtering

Today: The provider locally keeps a list of the prefixes that its stubs own.

Relies on altruism & trust



Verizon

Stub 20984: IP1
IP2
...

My stub doesn’t own this IP prefix!

20984

Also, maintaining this list is annoying and hard.
But, we could use the origin authentication database!

Origin Authentication: A secure database that maps IP Prefixes to their owner ASes.

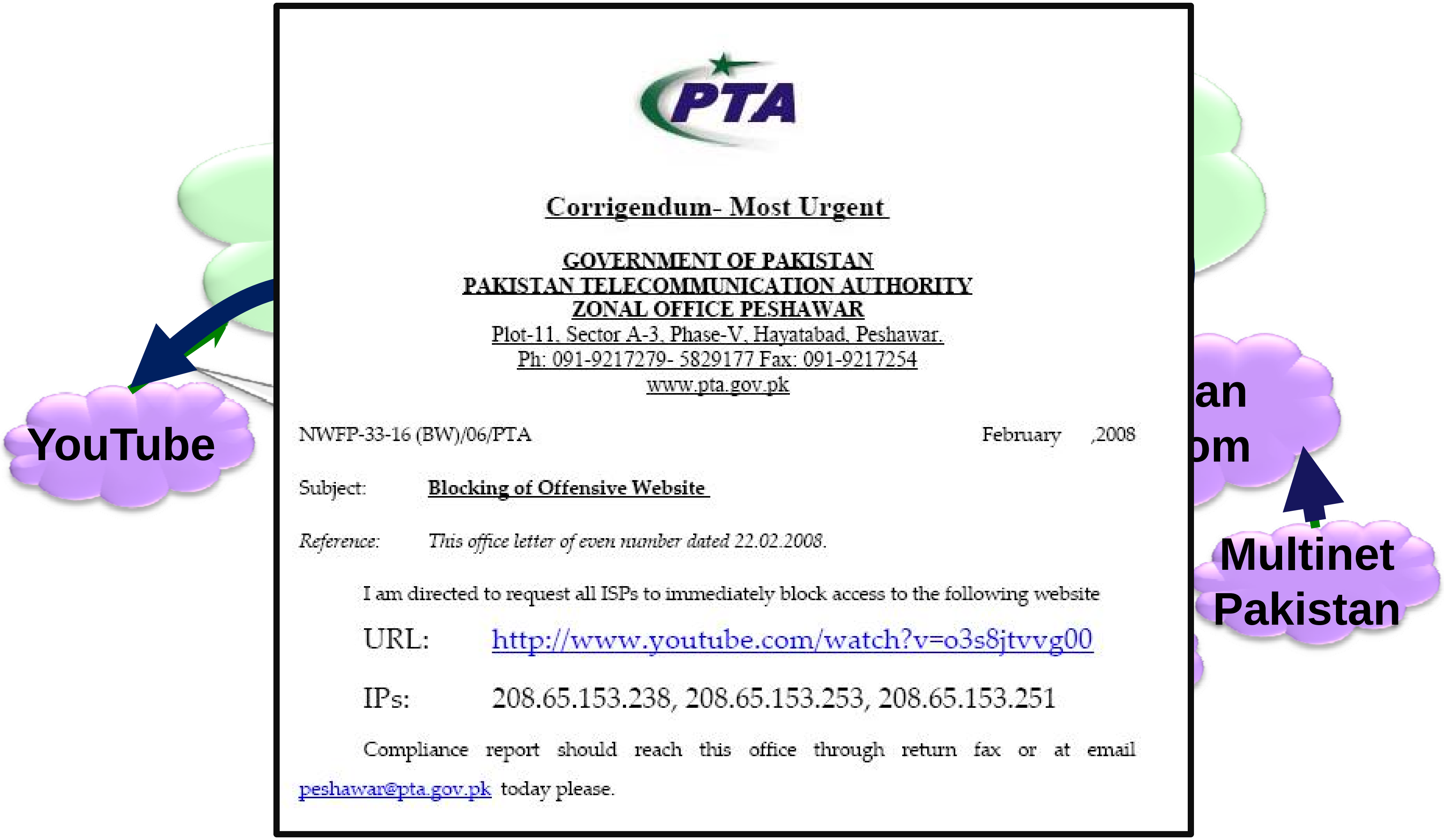
⇒Add defensive filtering to the origin authentication standard

Thanks!

Tech Report Available:
https://www.cs.bu.edu/~goldbe

How Secure is Routing on the Internet Today? (1)

February 2008 : Pakistan Telecom hijacks Youtube


YouTube
an
om
Multinet
Pakistan

PTA

Corrigendum- Most Urgent

GOVERNMENT OF PAKISTAN
PAKISTAN TELECOMMUNICATION AUTHORITY
ZONAL OFFICE PESHAWAR
Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.
Ph: 091-9217279- 5829177 Fax: 091-9217254
www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA February ,2008

Subject: **Blocking of Offensive Website**

Reference: This office letter of even number dated 22.02.2008.

I am directed to request all ISPs to immediately block access to the following website

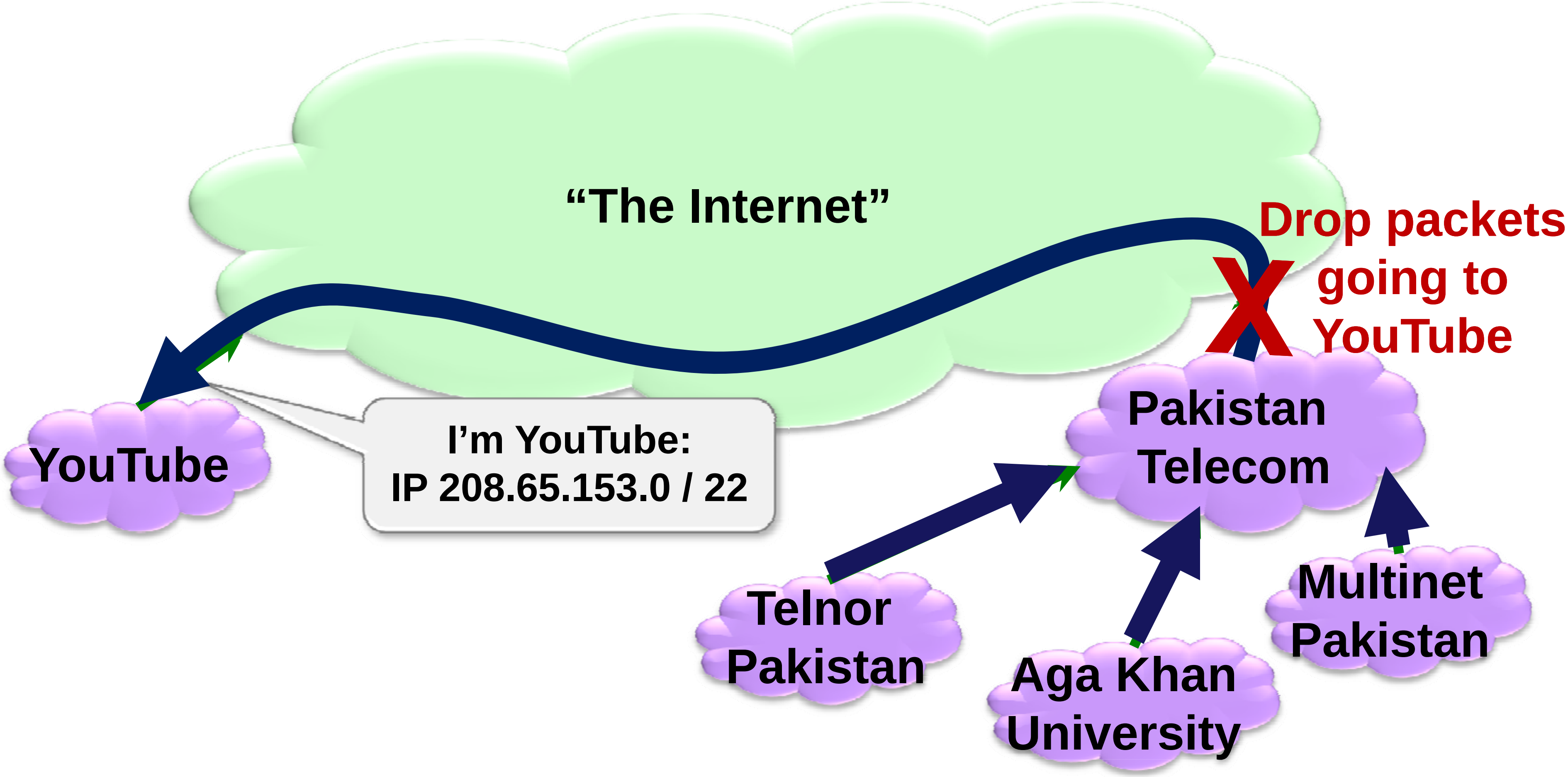
URL: http://www.youtube.com/watch?v=o3s8jtvvg00

IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.

How Secure is Routing on the Internet Today? (2)

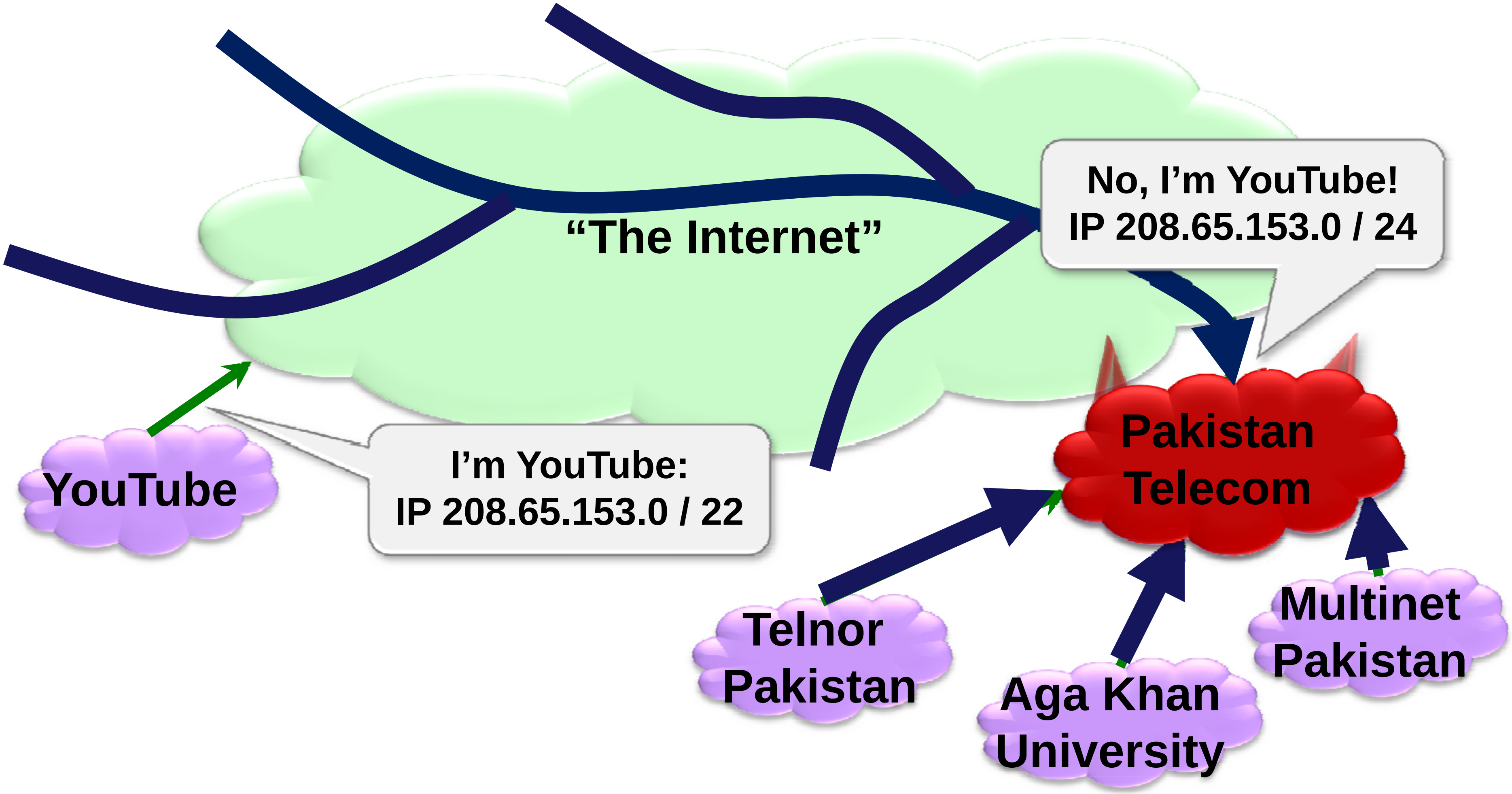
Here's what should have happened….



Block your own customers.

How Secure is Routing on the Internet Today? (3)

But here's what Pakistan ended up doing…



Draw traffic from the entire Internet!