40º CSBC

# artificialmente humano*ou* humanamente artificial?

## *DESAFIOS PARA A SOCIEDADE 5.0*

REALIZAÇÃO SBC

ORGANIZAÇÃO UFMT INSTITUTO DE COMPUTAÇÃO

PATROCINADORES

nic.br cgi.br Google RioTinto Loggi

APOIO FINANCEIRO

CNPq CAPES MINISTÉRIO DA EDUCAÇÃO PÁTRIA AMADA BRASIL

# str(self)

- Internet Systems Research
  - Monitoring
  - Performance
  - Troubleshooting
  - Security

Ítalo Cunha

UFMG

# str(self)

- Internet Systems Research
  - Monitoring
  - Performance
  - Troubleshooting
  - Security

ROUTE VIEWS 6447

RIPE RIS

ARCHIPELAGO

BGPStream

PeeringDB

PlanetLab

EmuLab

MLAB

caida

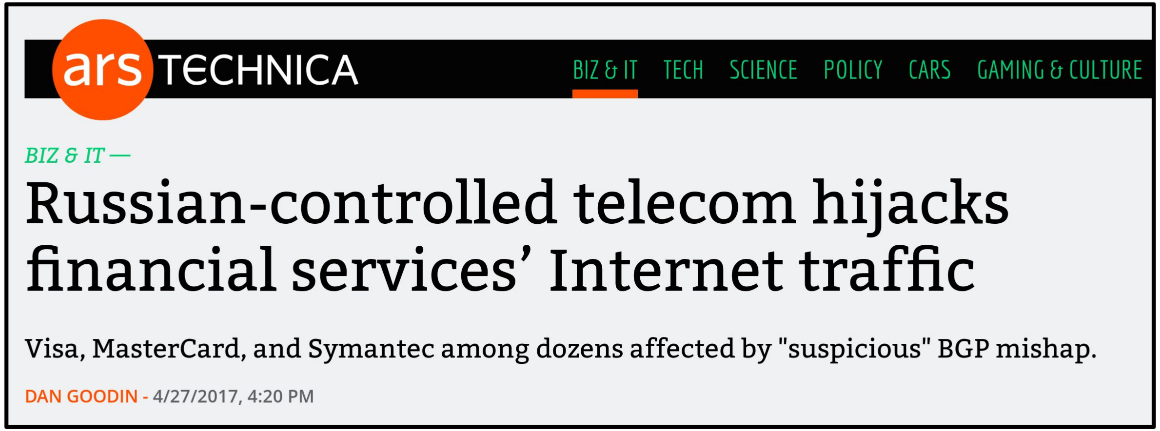
RIPE Atlas

TEAM CYMRU

# PEERING is a routing research testbed

Facilitates executing experiments on the Internet

https://peering.ee.columbia.edu

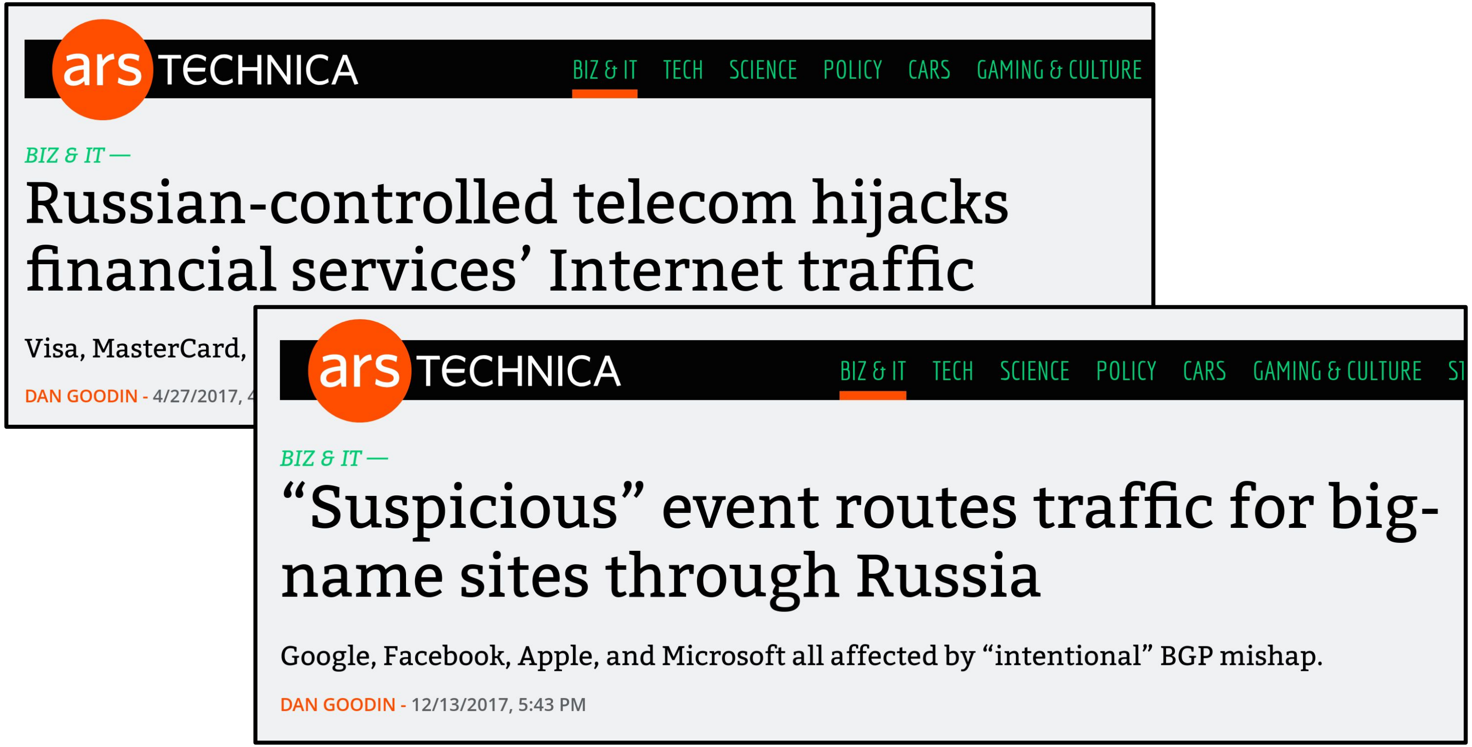


*BIZ & IT —*

# Russian-controlled telecom hijacks financial services’ Internet traffic

Visa, MasterCard, and Symantec among dozens affected by "suspicious" BGP mishap.

DAN GOODIN - 4/27/2017, 4:20 PM



BIZ & IT —

# Russian-controlled telecom hijacks financial services' Internet traffic

Visa, MasterCard,

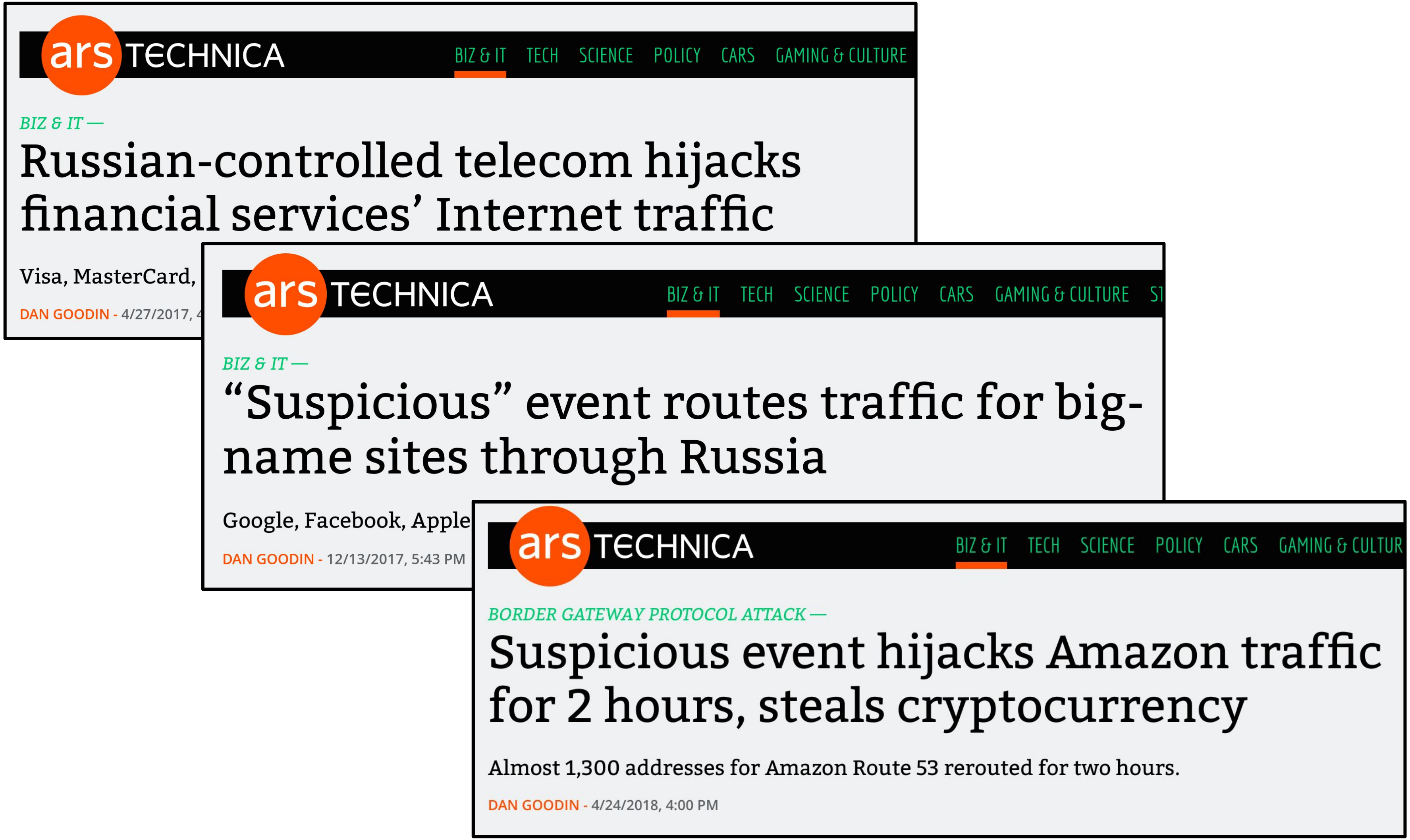
DAN GOODIN - 4/27/2017, 4

BIZ & IT —

# "Suspicious" event routes traffic for big-name sites through Russia

Google, Facebook, Apple, and Microsoft all affected by "intentional" BGP mishap.

DAN GOODIN - 12/13/2017, 5:43 PM



*BIZ & IT —*

Russian-controlled telecom hijacks financial services' Internet traffic

Visa, MasterCard,

DAN GOODIN - 4/27/2017, 4

*BIZ & IT —*

"Suspicious" event routes traffic for big-name sites through Russia

Google, Facebook, Apple

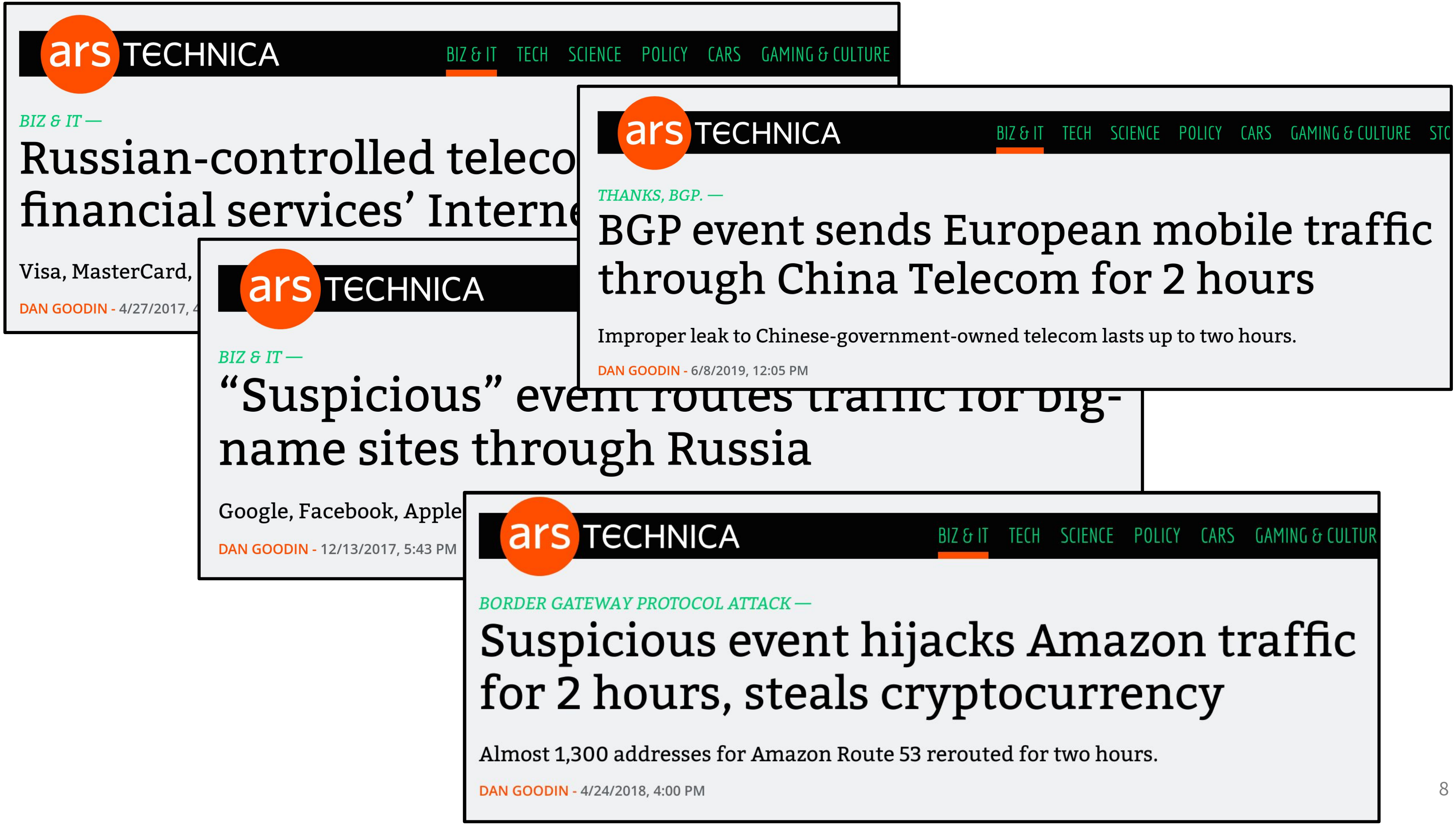
DAN GOODIN - 12/13/2017, 5:43 PM

*BORDER GATEWAY PROTOCOL ATTACK —*

Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

DAN GOODIN - 4/24/2018, 4:00 PM



*BIZ & IT —*

Russian-controlled teleco
financial services' Interne

Visa, MasterCard,

DAN GOODIN - 4/27/2017, 4

*BIZ & IT —*

“Suspicious” event routes traffic for big-name sites through Russia

Google, Facebook, Apple

DAN GOODIN - 12/13/2017, 5:43 PM

*THANKS, BGP. —*

BGP event sends European mobile traffic through China Telecom for 2 hours

Improper leak to Chinese-government-owned telecom lasts up to two hours.

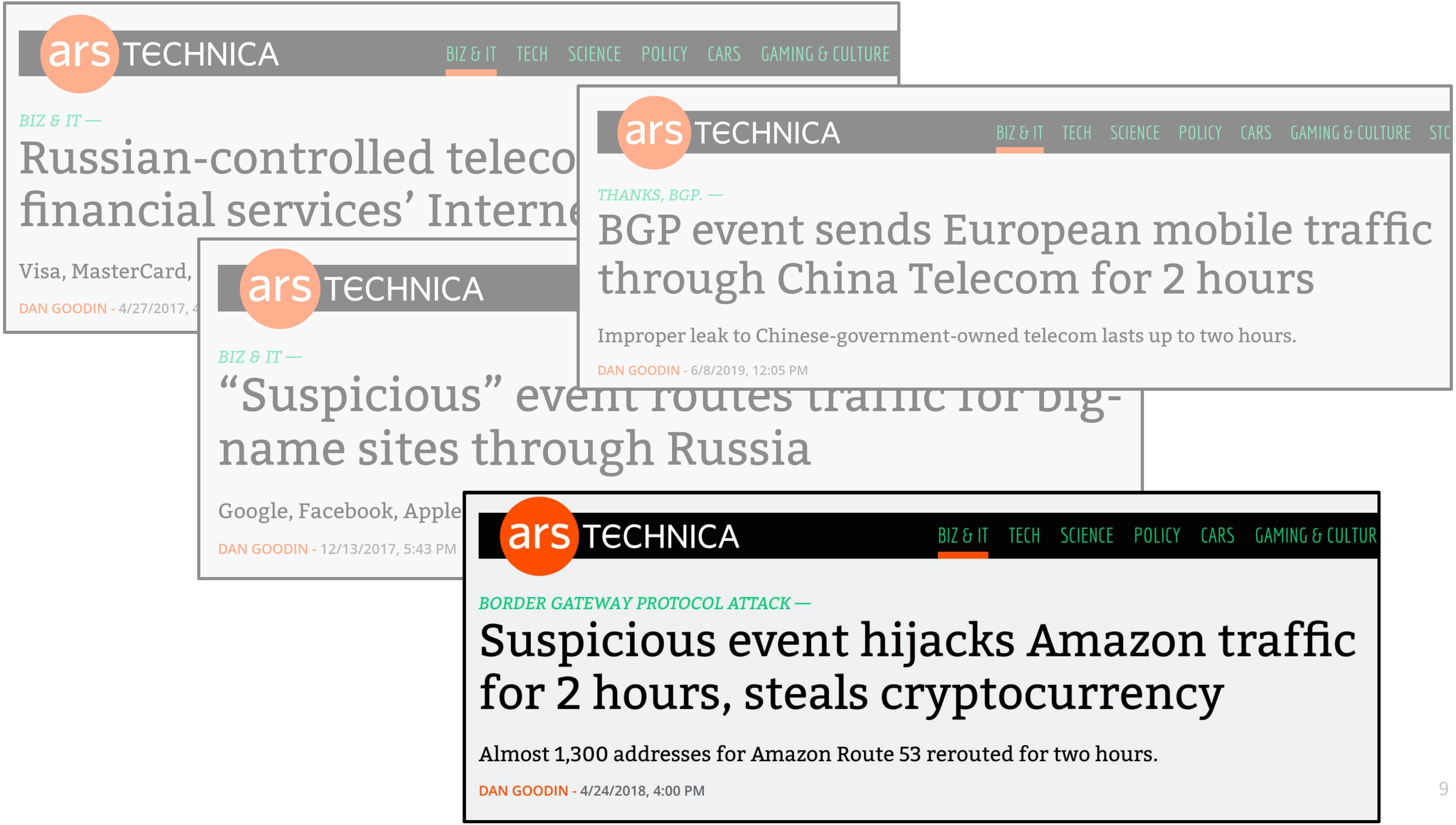
DAN GOODIN - 6/8/2019, 12:05 PM

*BORDER GATEWAY PROTOCOL ATTACK —*

Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

DAN GOODIN - 4/24/2018, 4:00 PM



*BIZ & IT —*

Russian-controlled teleco
financial services' Interne

Visa, MasterCard,

DAN GOODIN - 4/27/2017, 4

*BIZ & IT —*

“Suspicious” event routes traffic for big-name sites through Russia

Google, Facebook, Apple

DAN GOODIN - 12/13/2017, 5:43 PM

*THANKS, BGP. —*

BGP event sends European mobile traffic through China Telecom for 2 hours

Improper leak to Chinese-government-owned telecom lasts up to two hours.

DAN GOODIN - 6/8/2019, 12:05 PM

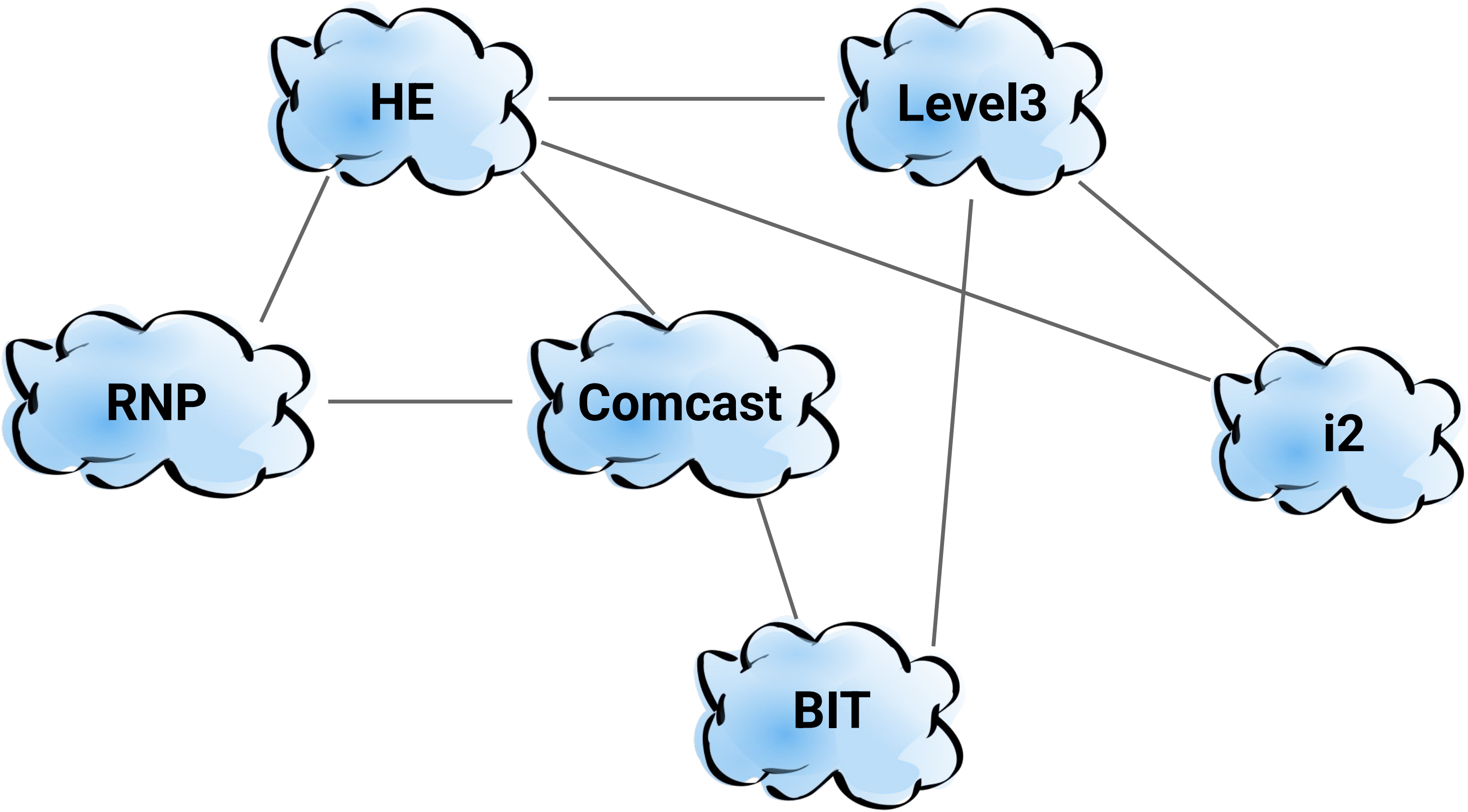
*BORDER GATEWAY PROTOCOL ATTACK —*

Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

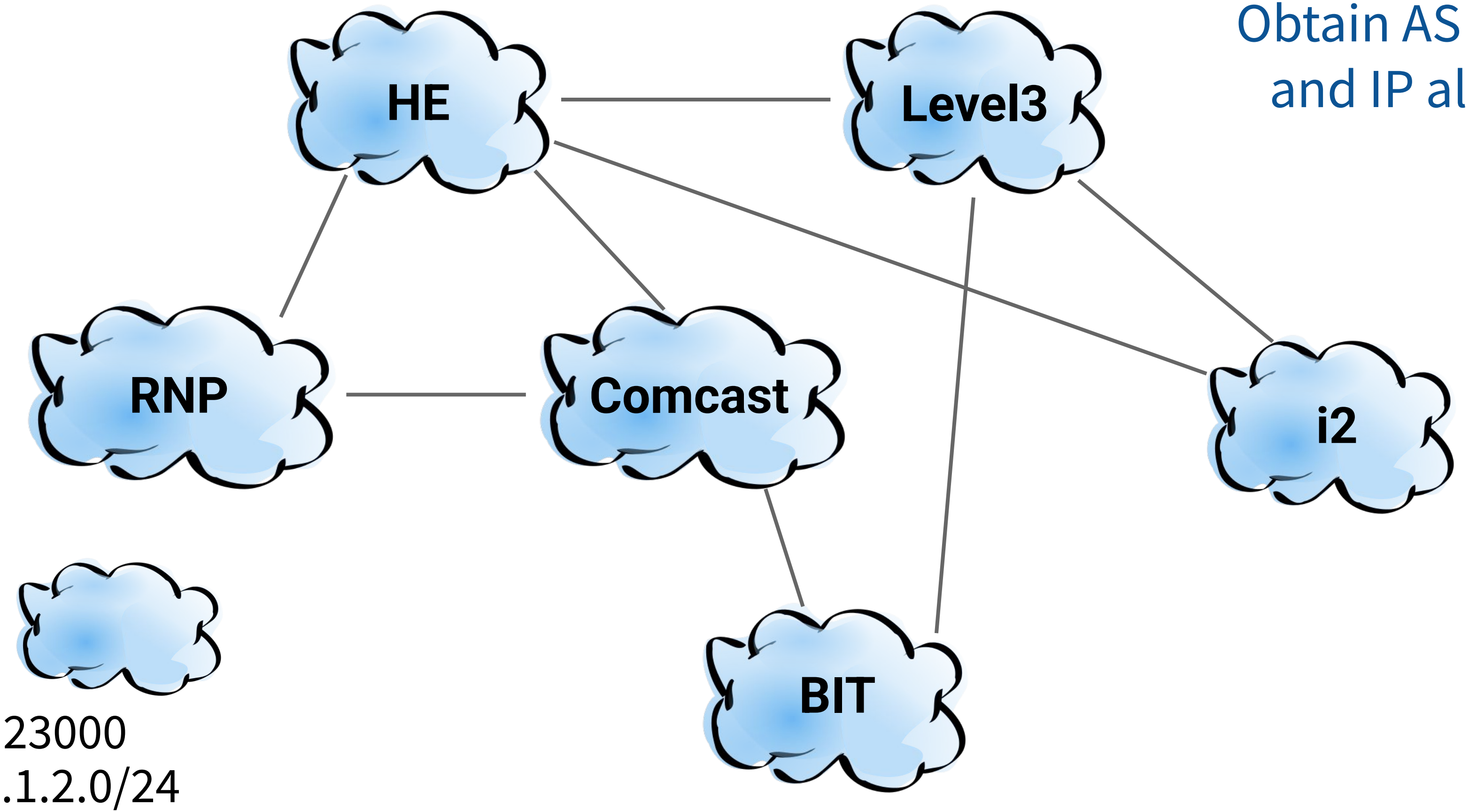
Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

DAN GOODIN - 4/24/2018, 4:00 PM

# Example: Supporting Experimental Prefix Hijacks



# Example: Supporting Experimental Prefix Hijacks

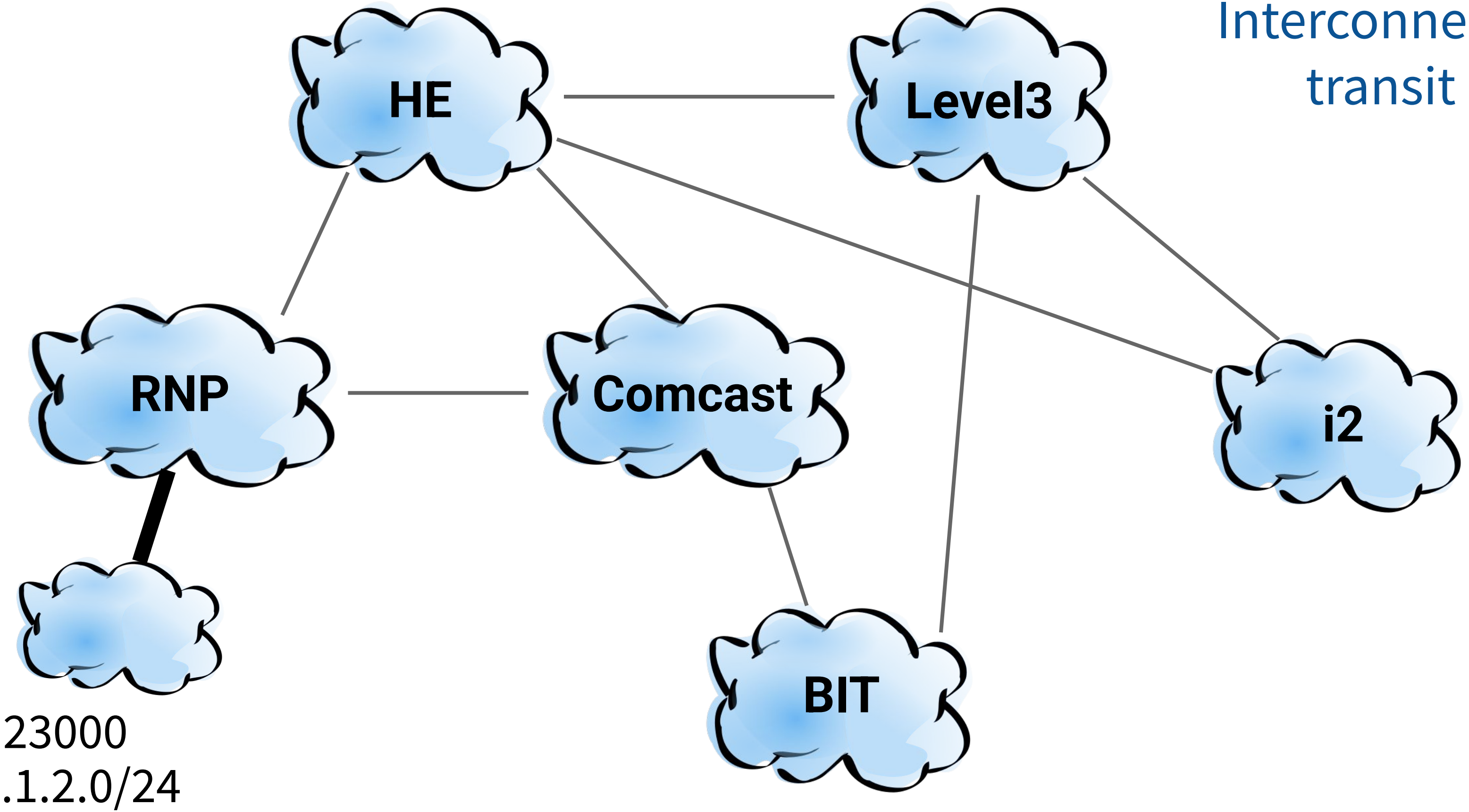


Obtain AS number and IP allocation

AS123000
200.1.2.0/24

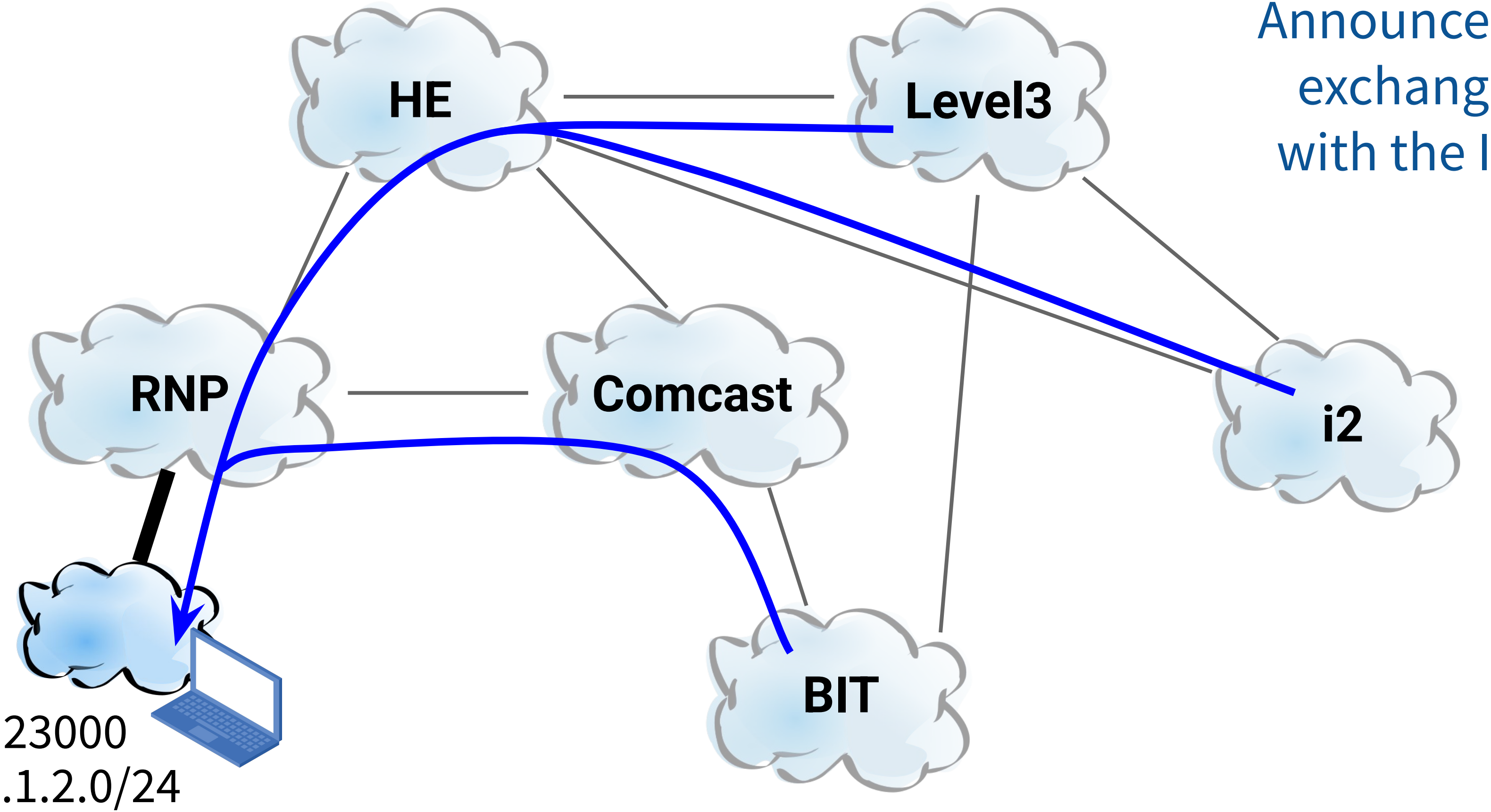
# Example: Supporting Experimental Prefix Hijacks

Interconnect with a transit provider



AS123000
200.1.2.0/24

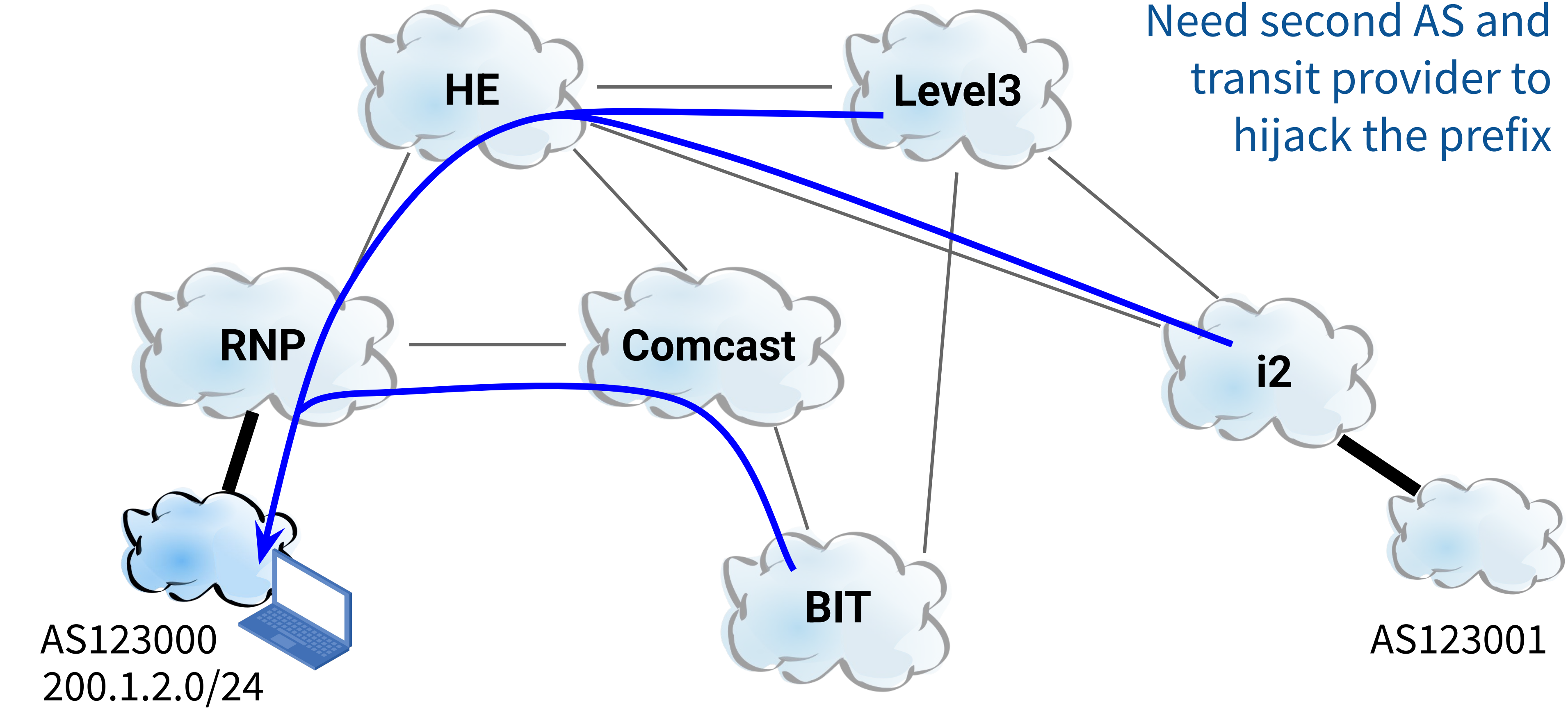
# Example: Supporting Experimental Prefix Hijacks



AS123000
200.1.2.0/24

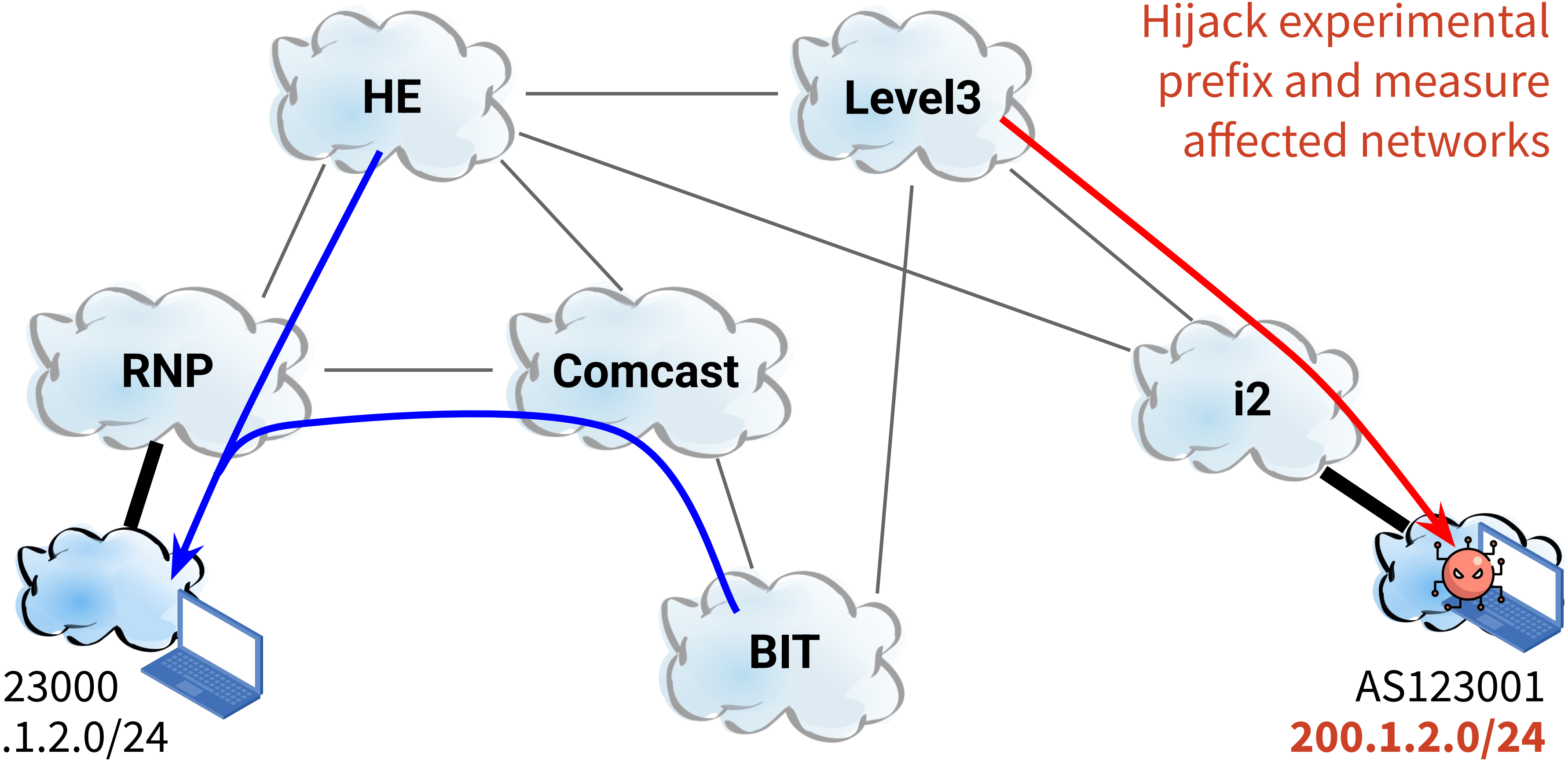
Announce routes, exchange traffic with the Internet

# Example: Supporting Experimental Prefix Hijacks



Need second AS and transit provider to hijack the prefix

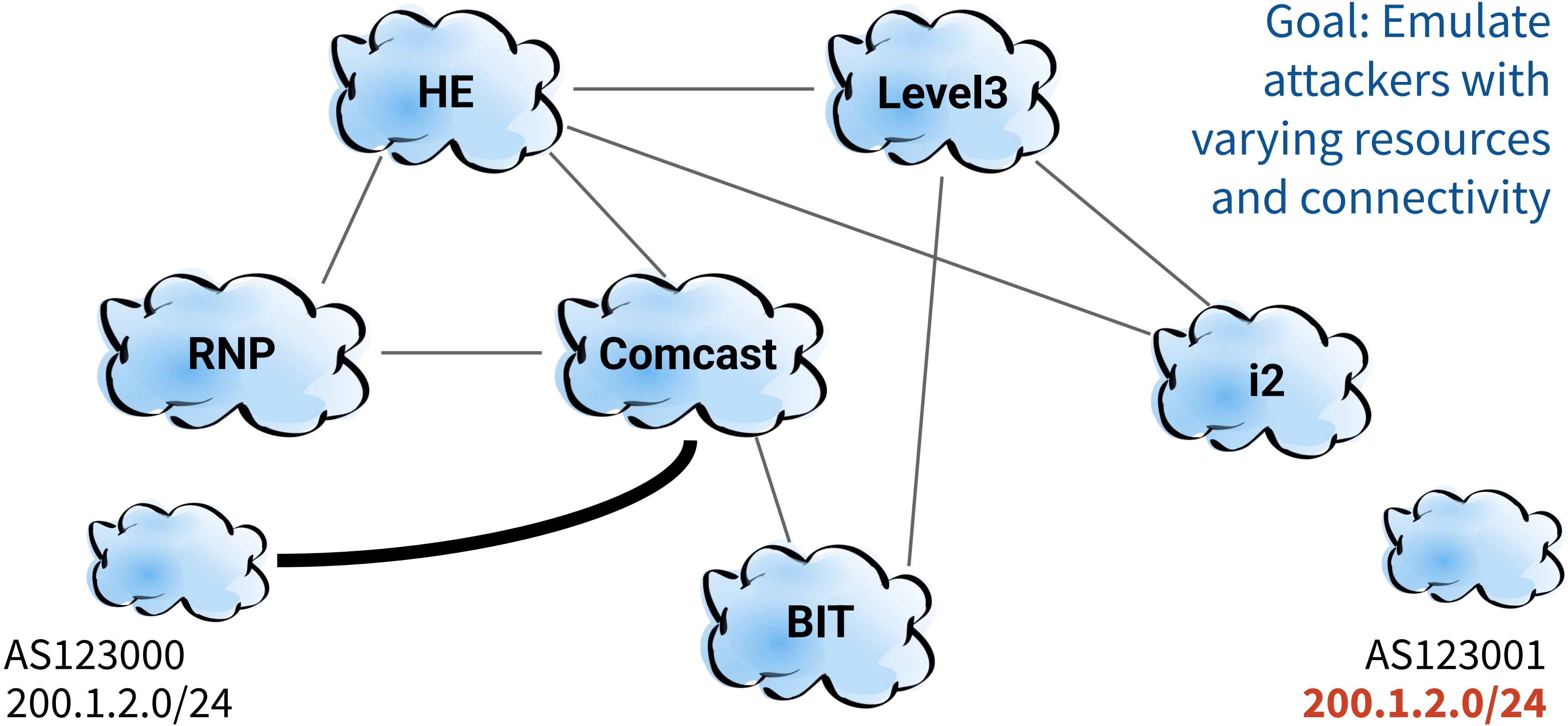
# Example: Supporting Experimental Prefix Hijacks



Hijack experimental prefix and measure affected networks

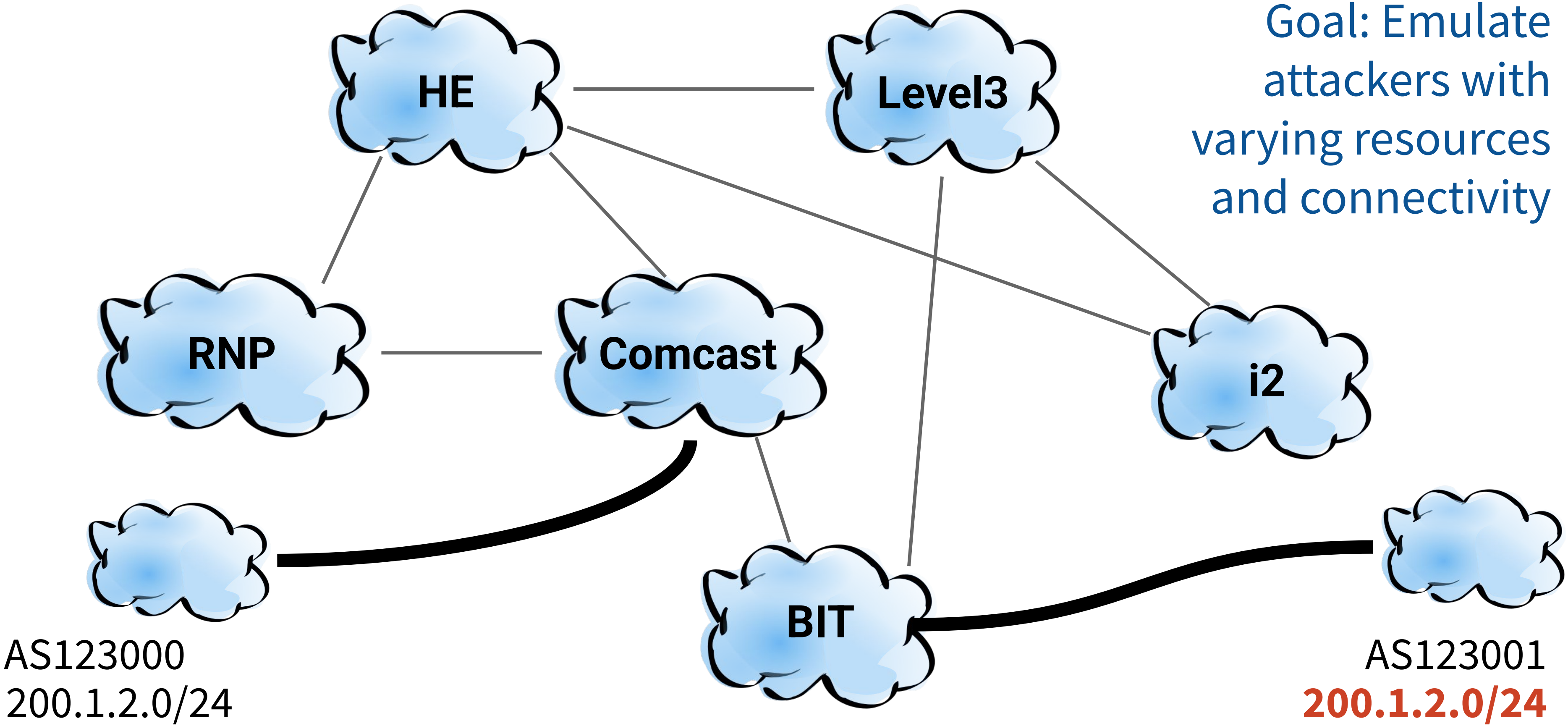
# Want Many Experimental Prefix Hijacks

Goal: Emulate attackers with varying resources and connectivity

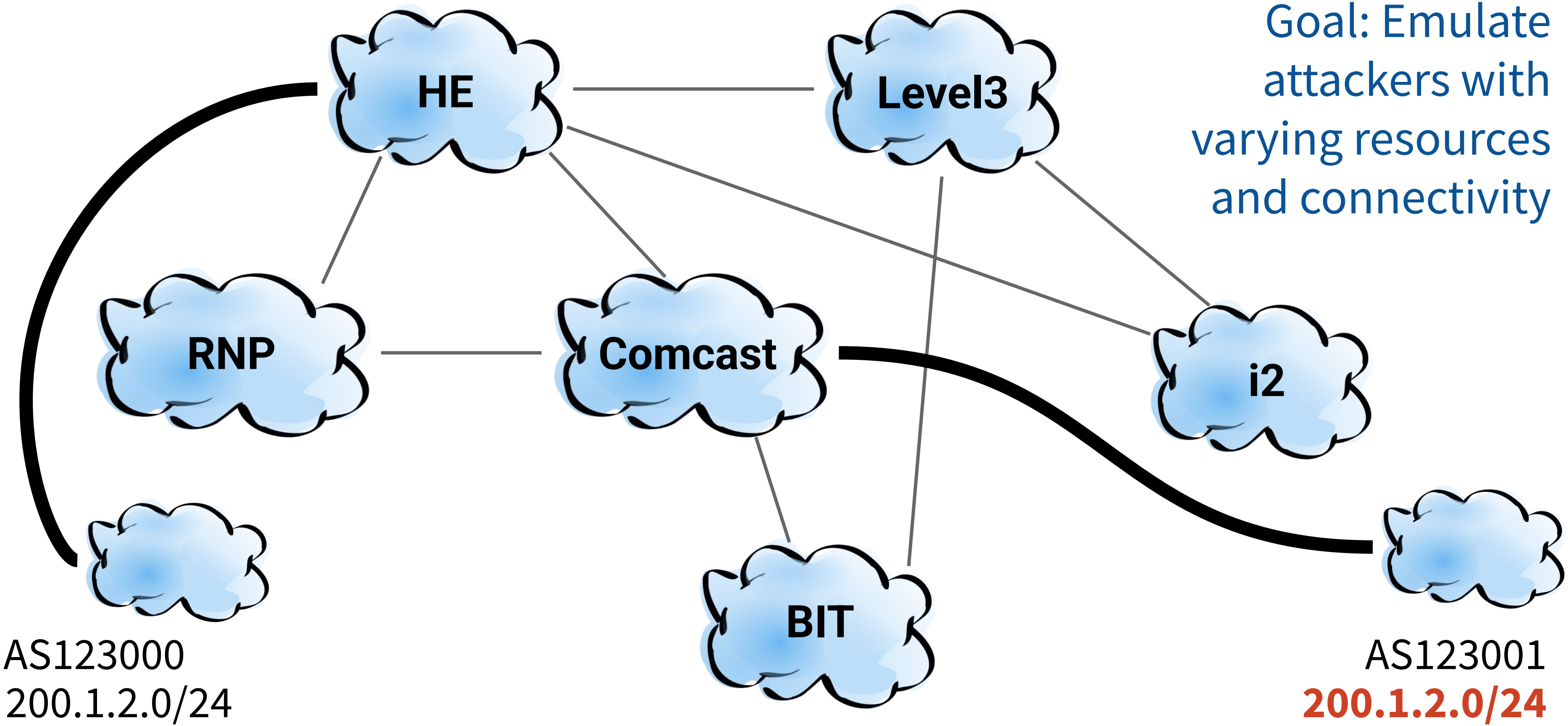


# Want Many Experimental Prefix Hijacks

Goal: Emulate attackers with varying resources and connectivity

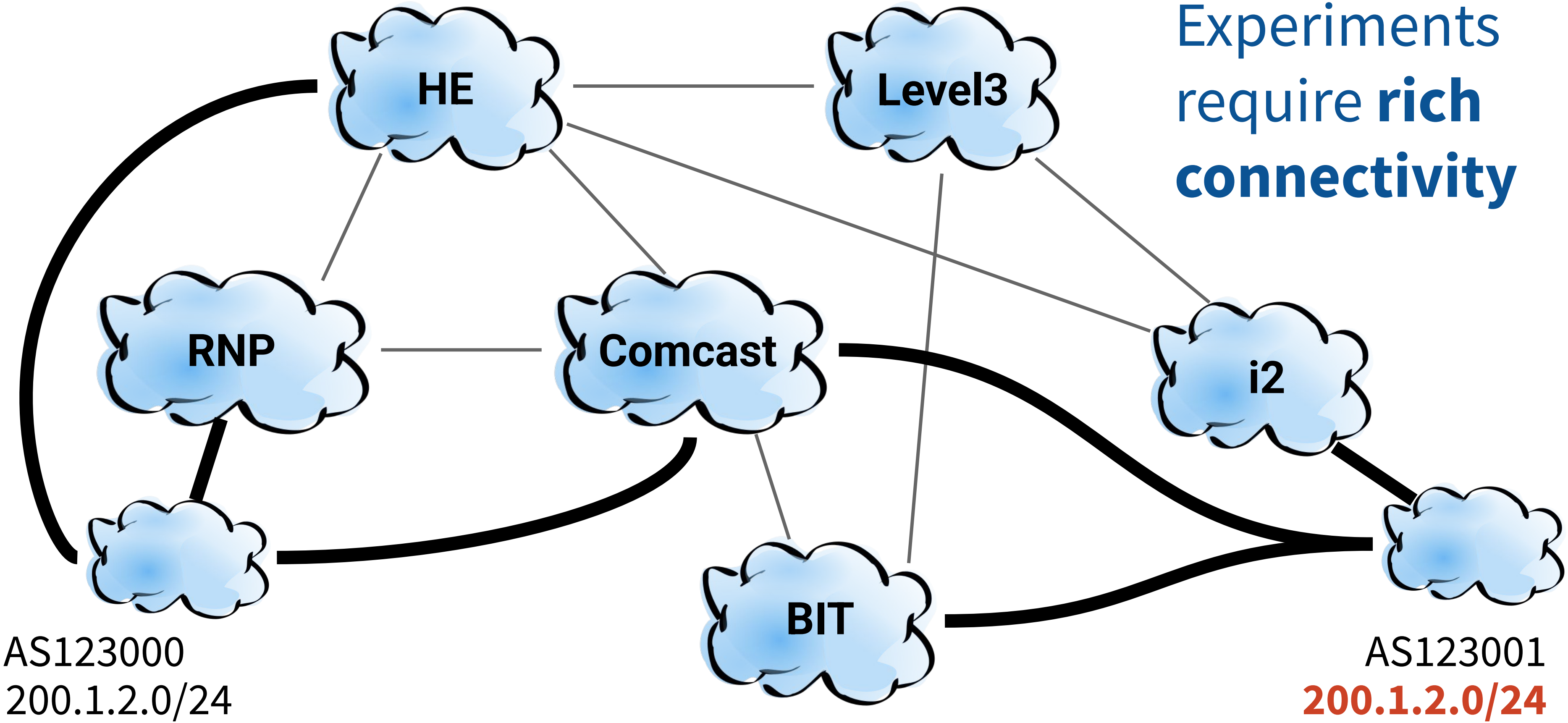


# Want **Many** Experimental Prefix Hijacks



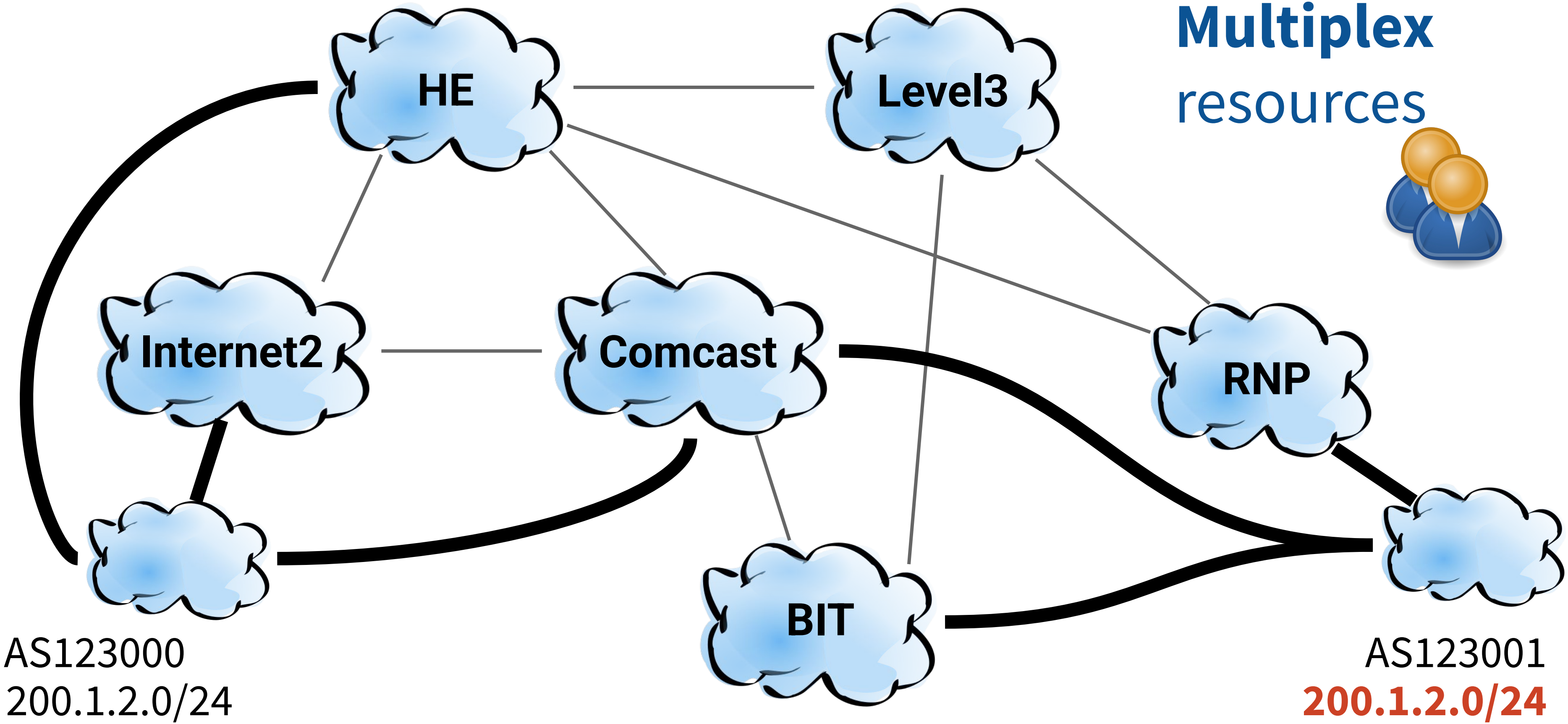
Goal: Emulate attackers with varying resources and connectivity

# Want Many Experimental Prefix Hijacks

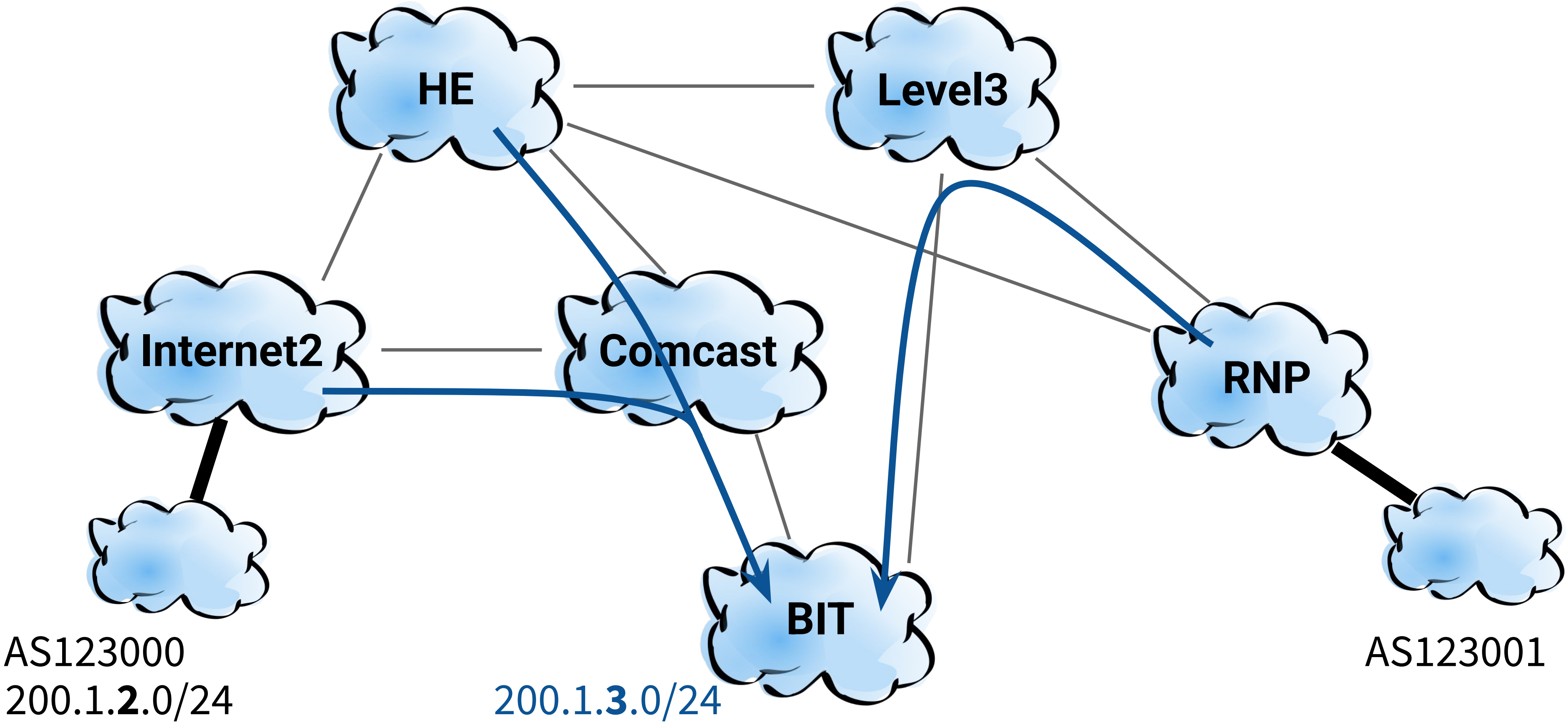


Experiments require **rich connectivity**

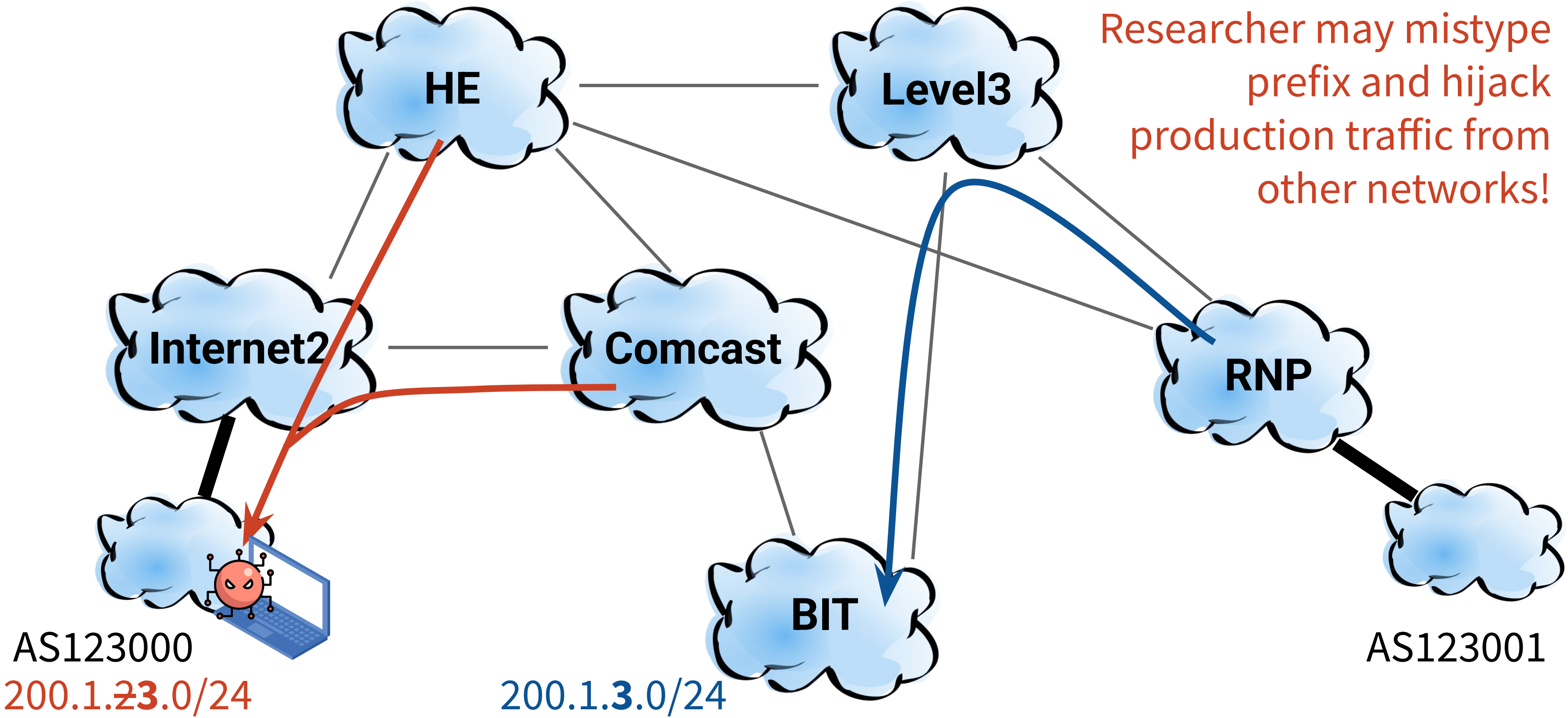
# Want to Run Many Experiments



# Experiments May Disrupt the Internet

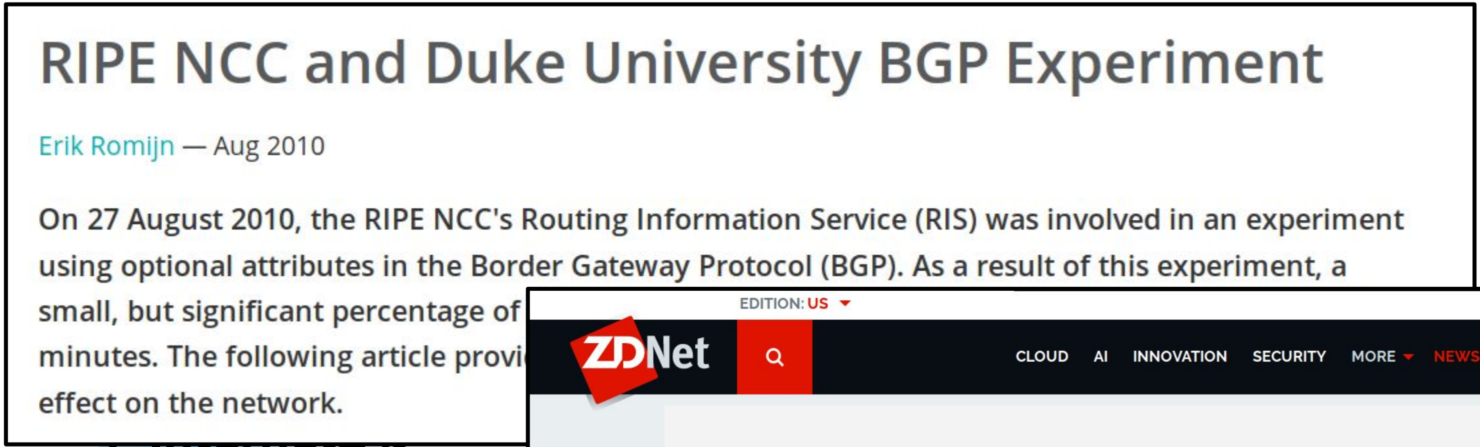


# Experiments May Disrupt the Internet



Researcher may mistype prefix and hijack production traffic from other networks!

# Experiments May Disrupt the Internet



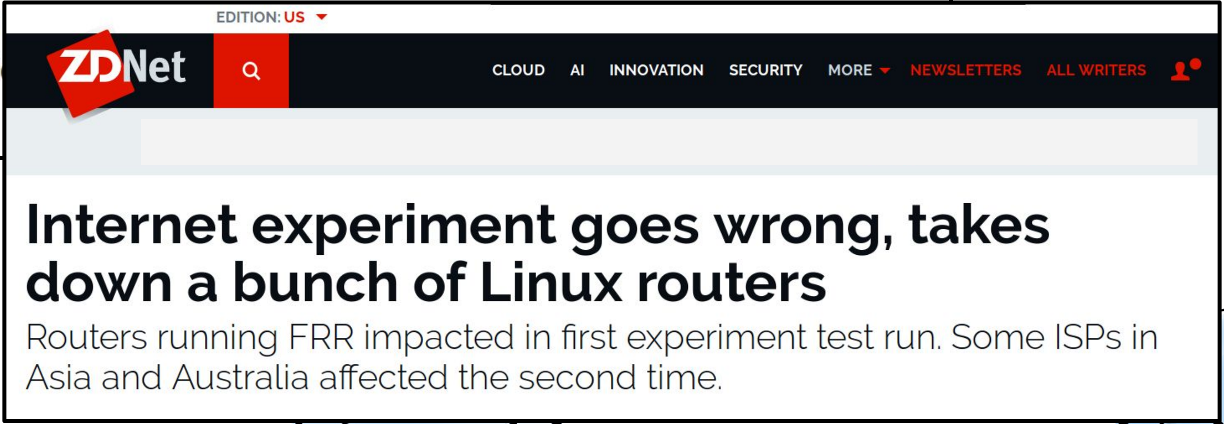
## RIPE NCC and Duke University BGP Experiment

Erik Romijn — Aug 2010

On 27 August 2010, the RIPE NCC's Routing Information Service (RIS) was involved in an experiment using optional attributes in the Border Gateway Protocol (BGP). As a result of this experiment, a small, but significant percentage of

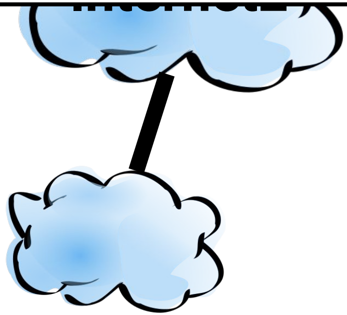
minutes. The following article provi

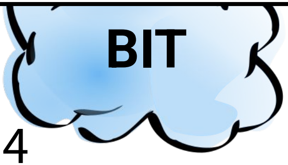
effect on the network.



## Internet experiment goes wrong, takes down a bunch of Linux routers

Routers running FRR impacted in first experiment test run. Some ISPs in Asia and Australia affected the second time.



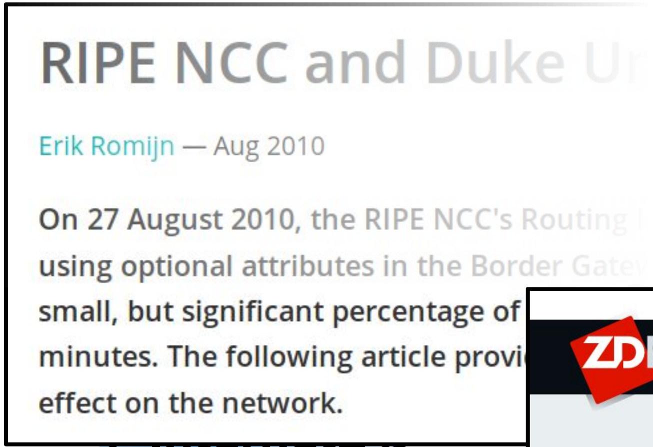


AS123000
200.1.**3**.0/24

200.1.**3**.0/24

AS123001
200.2.3.0/24

# Experiments May Disrupt the Internet

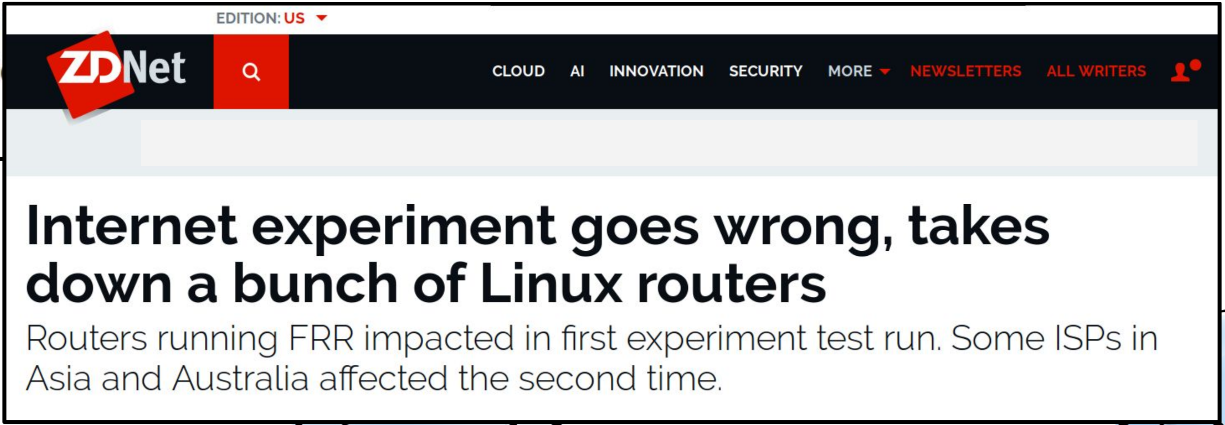


RIPE NCC and Duke U

Erik Romijn — Aug 2010

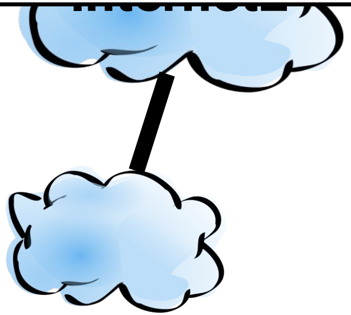
On 27 August 2010, the RIPE NCC's Routing I
using optional attributes in the Border Gatev
small, but significant percentage of
minutes. The following article provi
effect on the network.

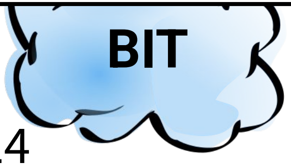
Ensure **safety** against errors and misbehavior



## Internet experiment goes wrong, takes down a bunch of Linux routers

Routers running FRR impacted in first experiment test run. Some ISPs in Asia and Australia affected the second time.





AS123000
200.1.**3**.0/24

200.1.**3**.0/24

AS123001
200.2.3.0/24

# Experiment Goals and Needs Vary

## Control Plane

- Anycast prefixes
- Perform AS-path prepending
- Perform AS-path poisoning
- Attach BGP communities
- **All of the above in ways BGP does not natively support**

## Data Plane

# Experiment Goals and **Needs** Vary

## Control Plane

- Anycast prefixes
- Perform AS-path prepending
- Perform AS-path poisoning
- Attach BGP communities
- **All of the above in ways BGP does not natively support**
- Flap announcements
- Add custom BGP attributes
- Announce /25 or /49 prefixes

## Data Plane

- Send/receive pings/traceroutes
- Host HTTPS Web server
- Host a security honeypot
- Participate in Tor or BitTorrent
- **Transit a university's Youtube traffic**

# Experiment Goals and Needs Vary

## Control Plane

- Anycast prefixes
- Perform AS-path prepending
- Perform AS-path poisoning
- Attach BGP communities
- **All of the above in ways BGP does not natively support**
- Flap announcements
- Add custom BGP attributes
- Announce /25 or /49 prefixes

## Data Plane

- Send/receive pings/traceroutes
- Host HTTPS Web server
- Host a security honeypot
- Participate in Tor or BitTorrent
- **Transit a university's Youtube traffic**
- Control egress at IXPs

Experiments require **control** on both routes and traffic

# Supporting Multiple Experiments

Experiments interact with the real Internet and take time

- BGP announcements take time to converge
- Probing budgets limit ping/traceroute
- Sequence thousands of announcements
- Researchers revise their experiment

Synchronized demand before conference deadlines

# Supporting Multiple Experiments

Experiments interact with the real Internet and take time

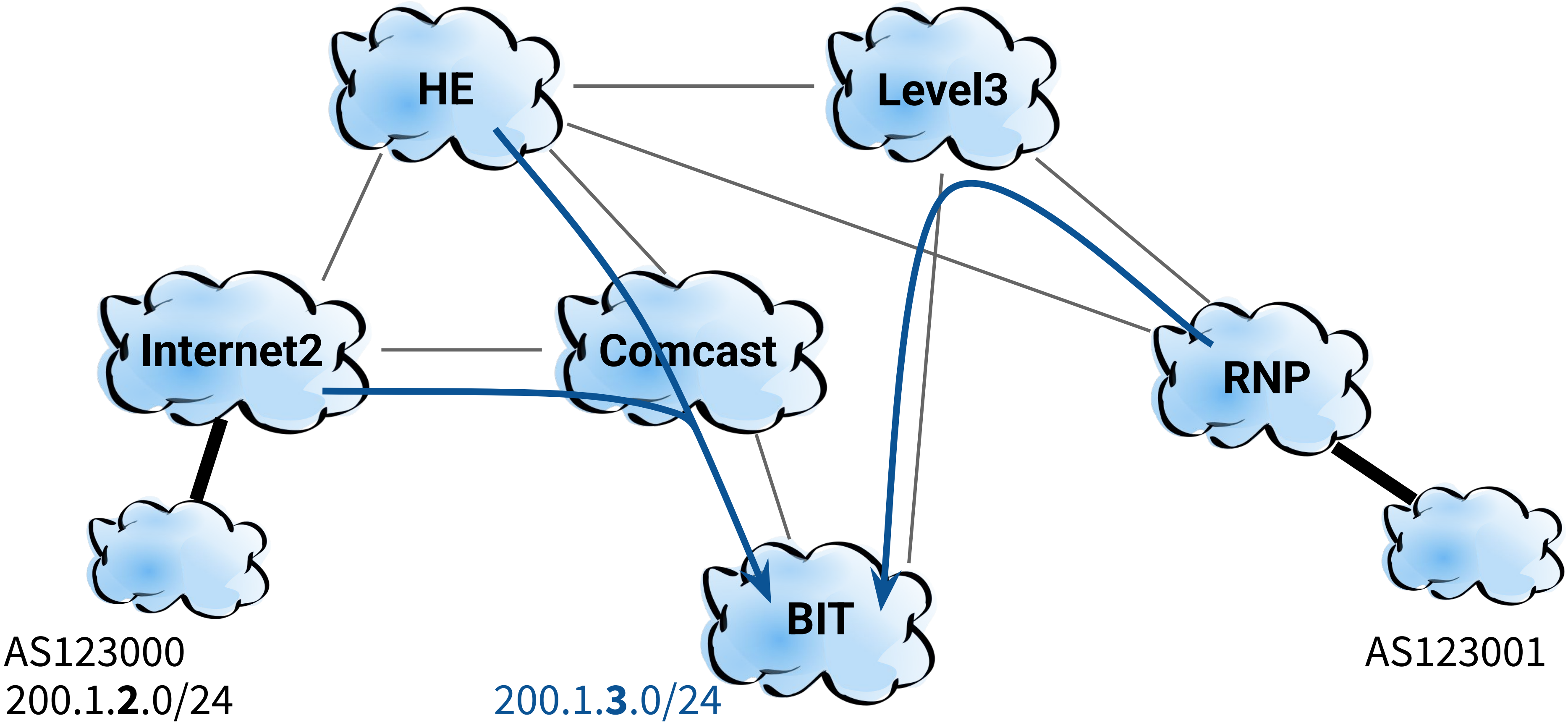
- BGP announcements take time to converge
- Probing budgets limit ping/traceroute
- Sequence thousands of announcements
- Researchers revise their experiment

Synchronized demand before conference deadlines

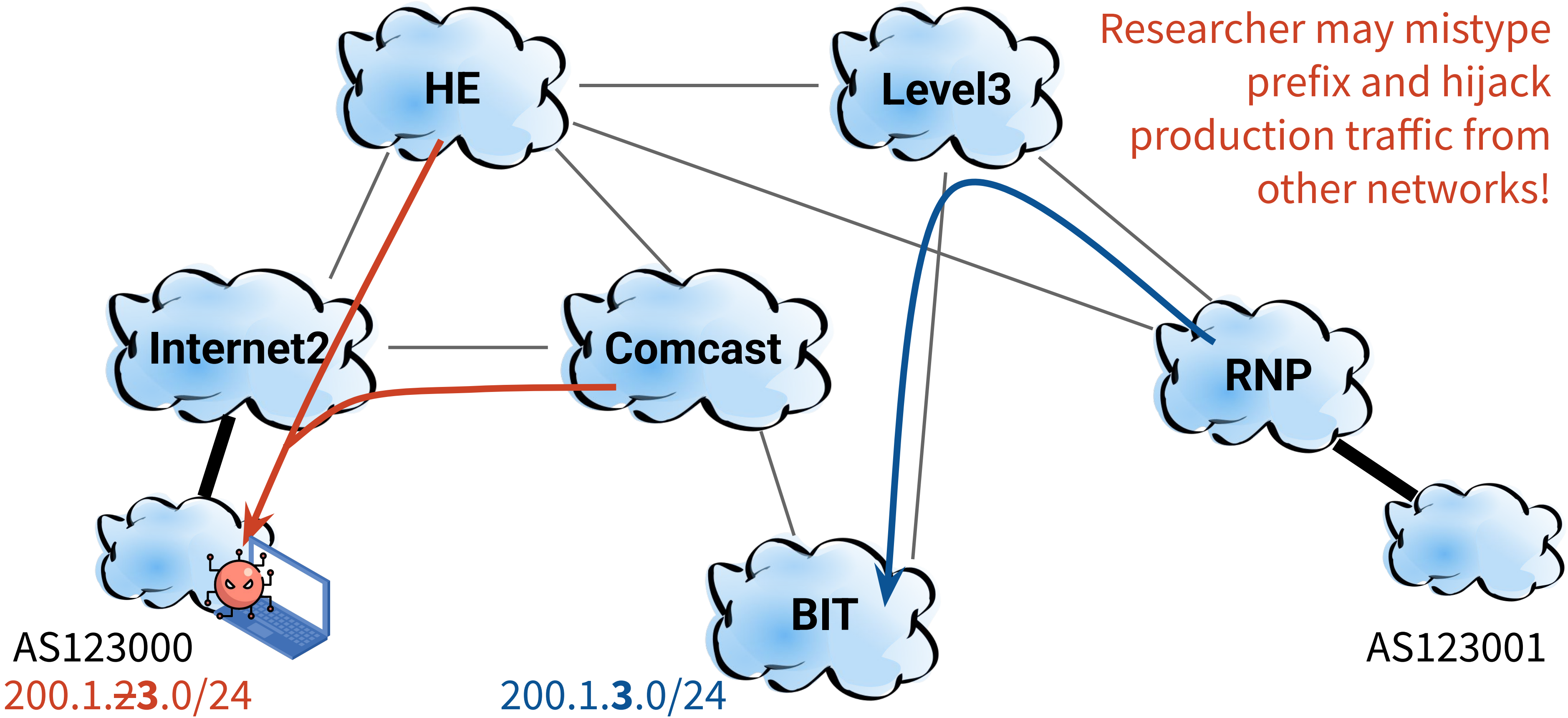
Support **concurrent** experiments

- Multiplex resources
- Isolate experiments

# Experiments May Disrupt the Internet

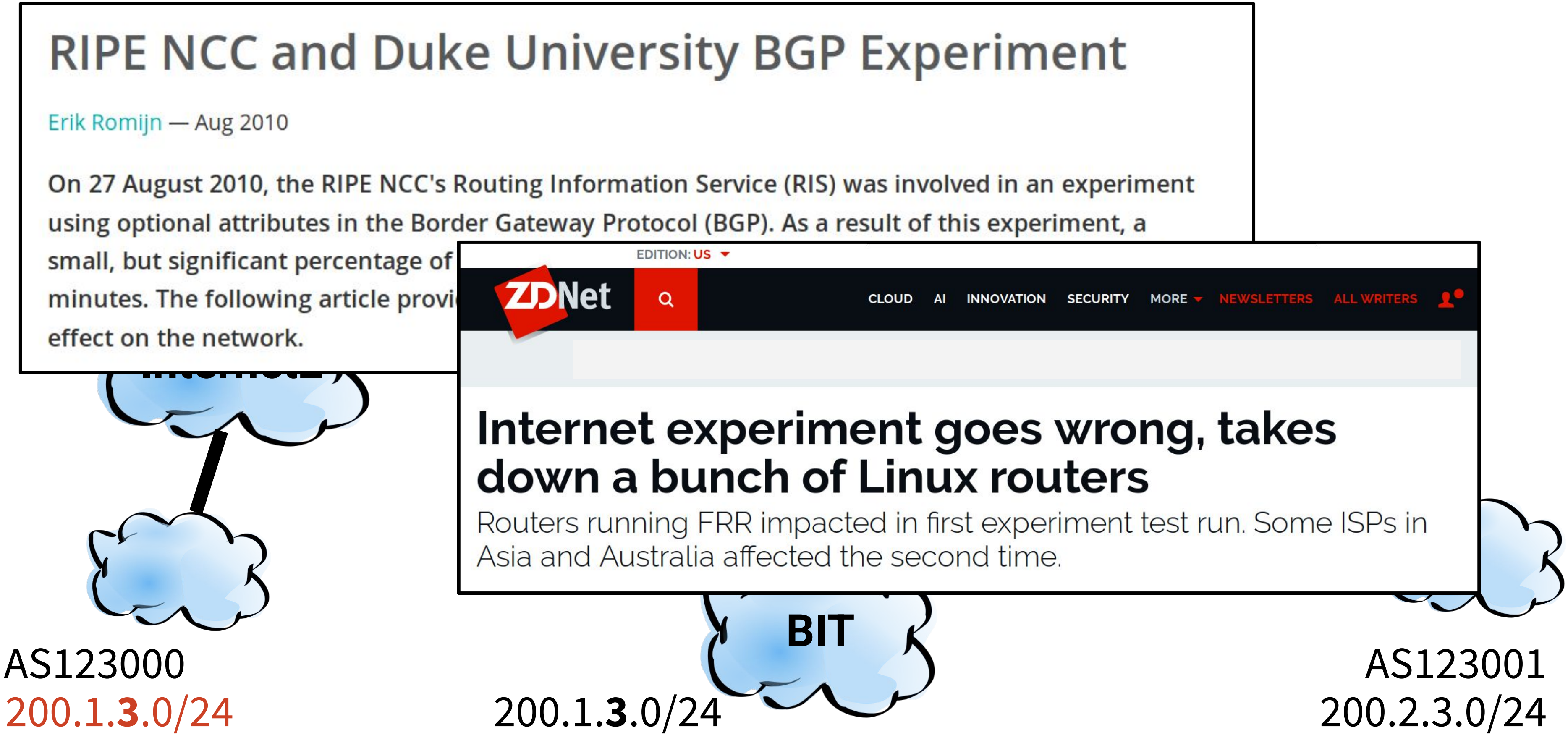


# Experiments May Disrupt the Internet



Researcher may mistype prefix and hijack production traffic from other networks!

# Experiments May Disrupt the Internet



## RIPE NCC and Duke University BGP Experiment

Erik Romijn — Aug 2010

On 27 August 2010, the RIPE NCC's Routing Information Service (RIS) was involved in an experiment using optional attributes in the Border Gateway Protocol (BGP). As a result of this experiment, a small, but significant percentage of
minutes. The following article provi
effect on the network.

## Internet experiment goes wrong, takes down a bunch of Linux routers

Routers running FRR impacted in first experiment test run. Some ISPs in Asia and Australia affected the second time.

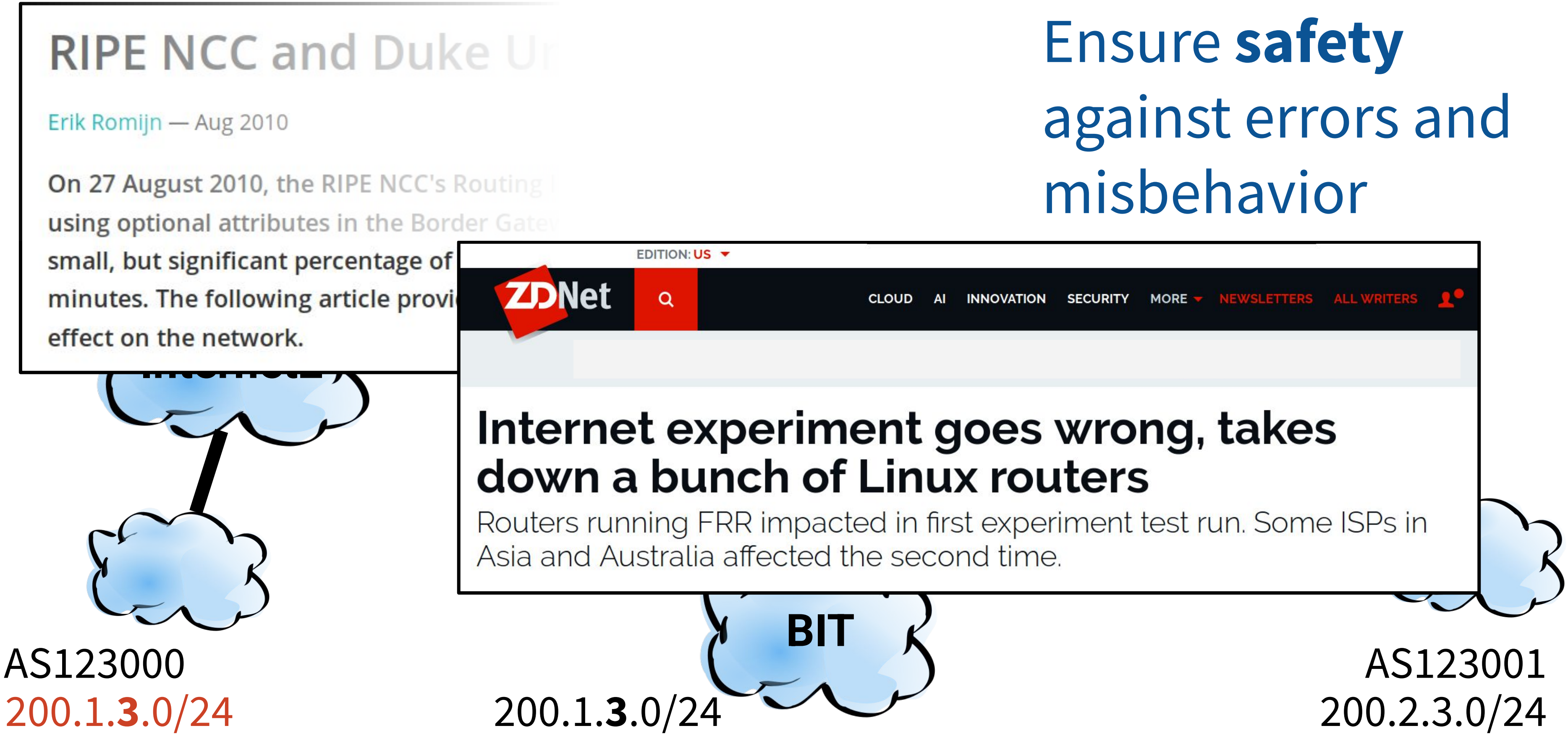
AS123000
200.1.**3**.0/24

200.1.**3**.0/24

AS123001
200.2.3.0/24

# Experiments May Disrupt the Internet

Ensure **safety** against errors and misbehavior



RIPE NCC and Duke Ur

Erik Romijn — Aug 2010

On 27 August 2010, the RIPE NCC's Routing I
using optional attributes in the Border Gatev
small, but significant percentage of
minutes. The following article provi
effect on the network.

EDITION: US

ZDNet

CLOUD AI INNOVATION SECURITY MORE NEWSLETTERS ALL WRITERS

## Internet experiment goes wrong, takes down a bunch of Linux routers

Routers running FRR impacted in first experiment test run. Some ISPs in Asia and Australia affected the second time.

# Requirements for a Routing Research Testbed

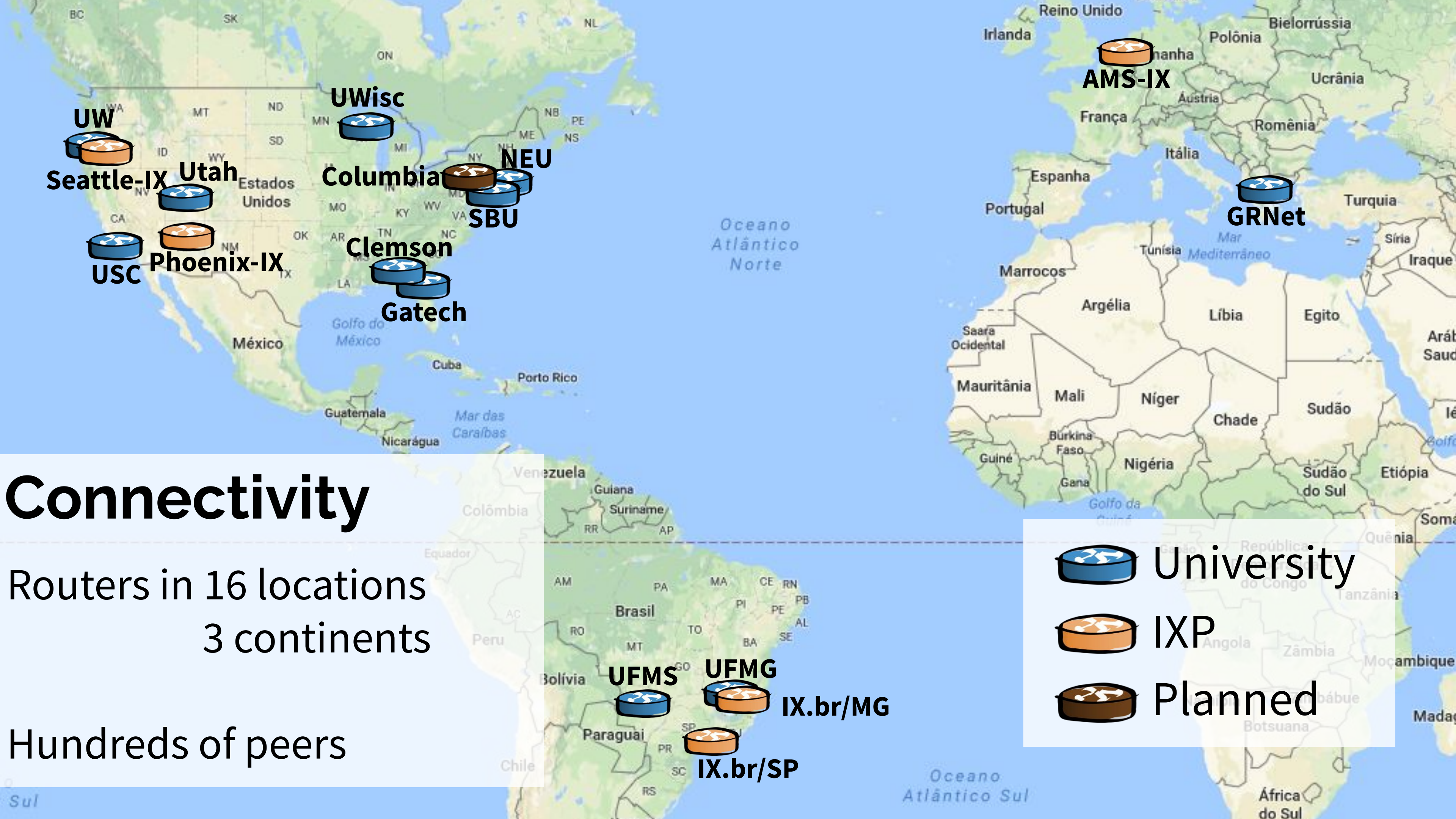
1. Rich **connectivity** to hundreds of networks
2. Delegate **control** over routes and traffic to experiments
3. Provide **representative** infrastructure
4. Support **concurrent** experiments
5. Ensure **safety** against errors and misbehavior

# Connectivity

Routers in 16 locations

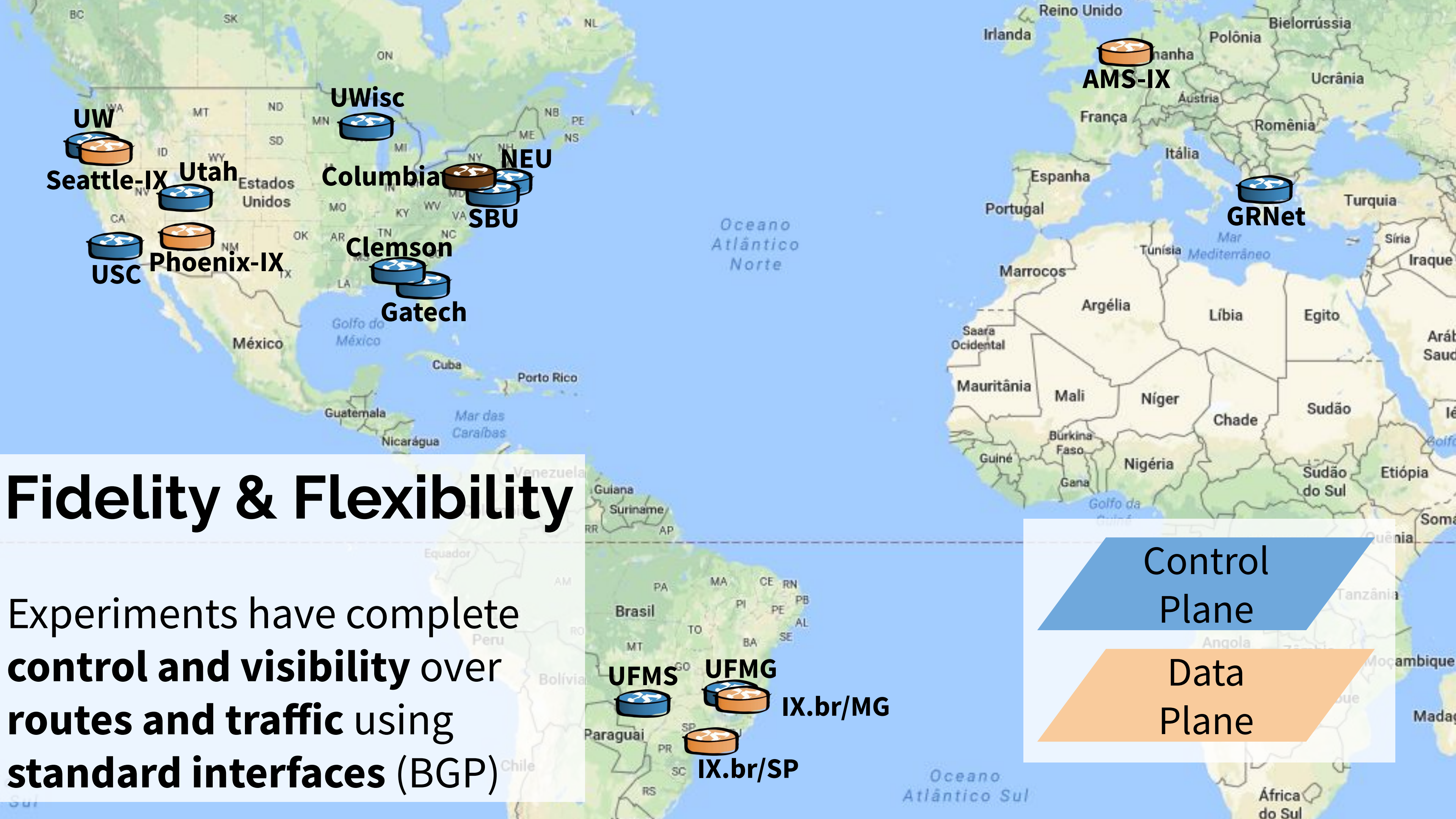
3 continents

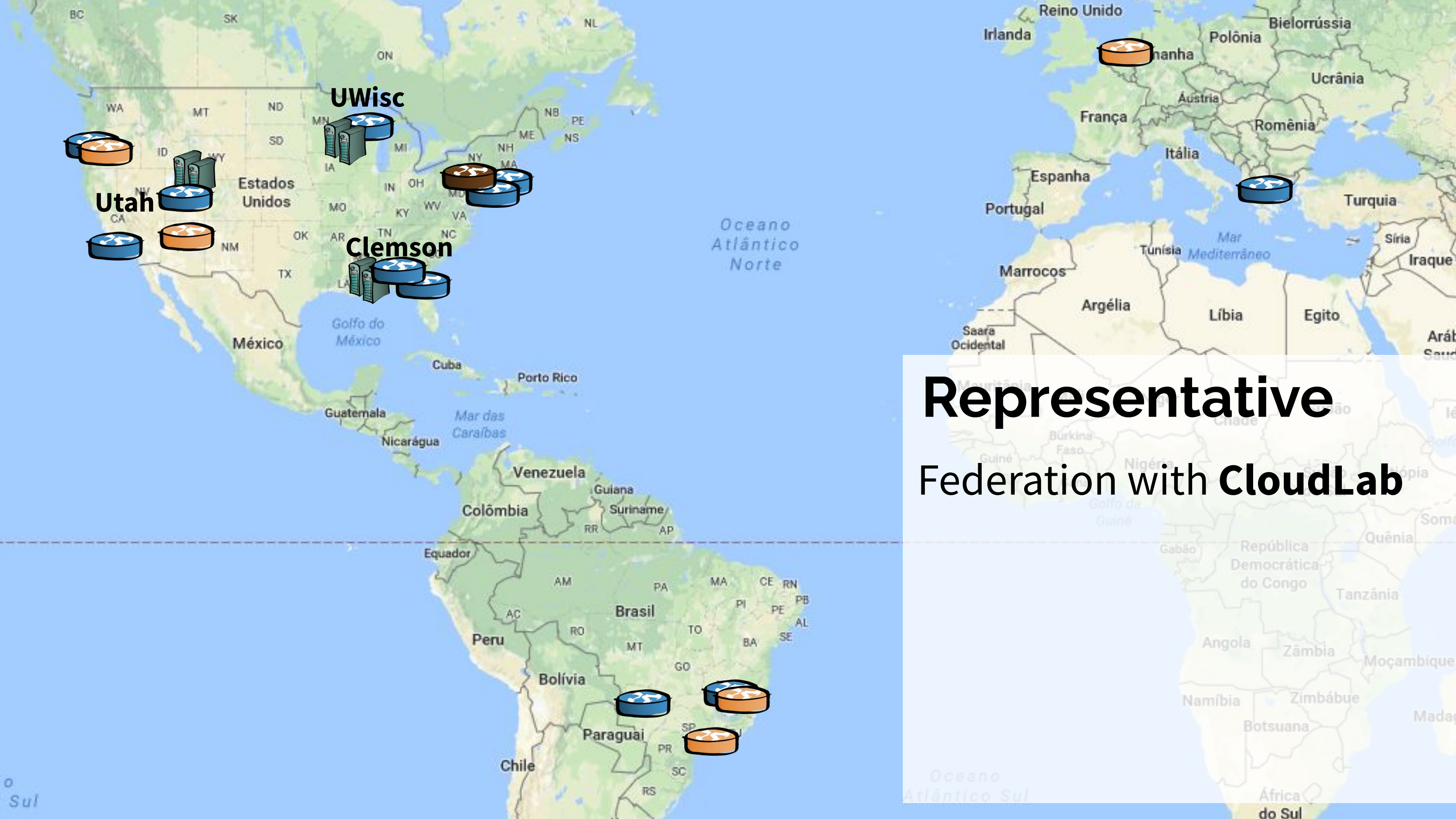
Hundreds of peers



# Fidelity & Flexibility

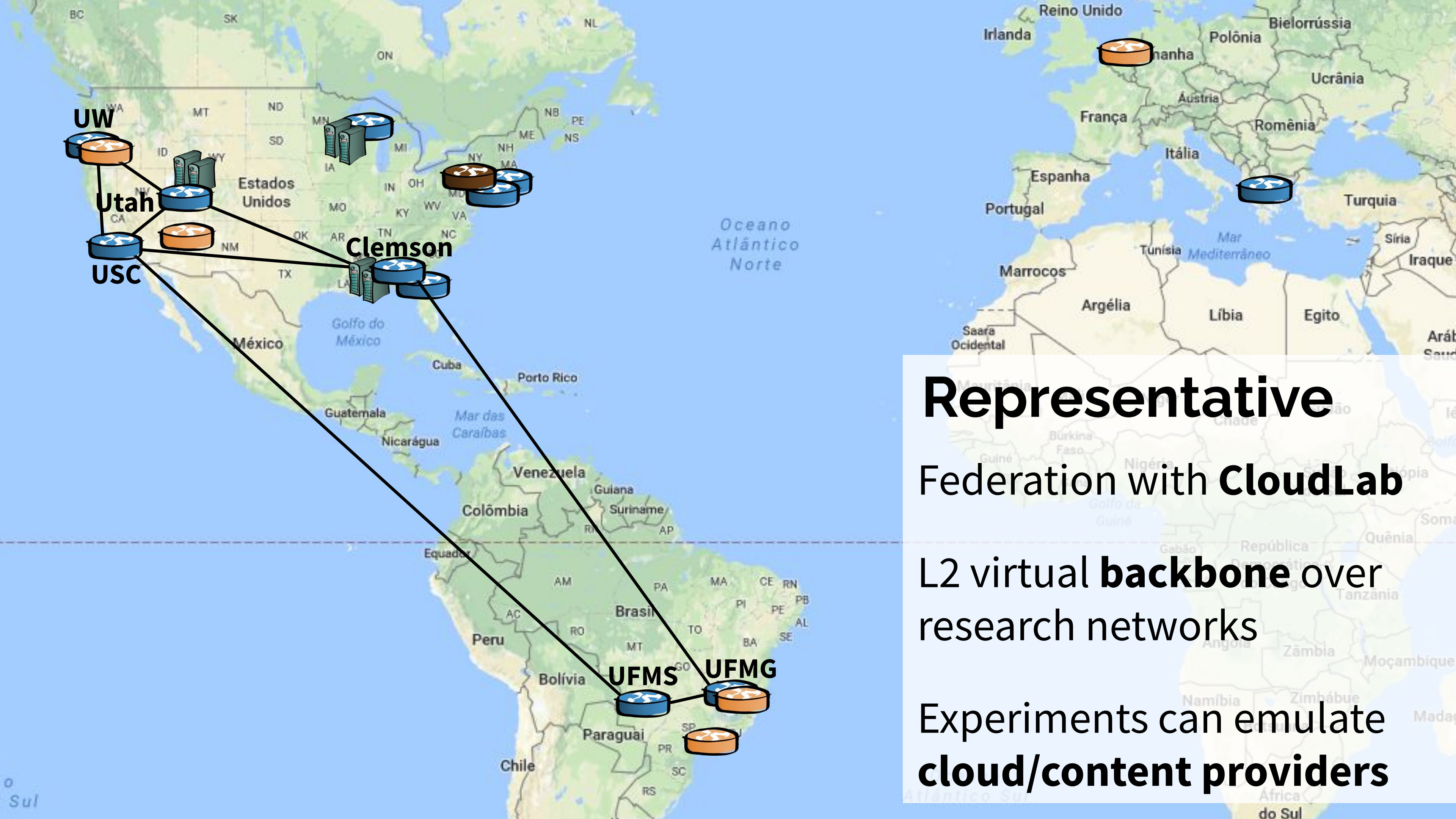
Experiments have complete **control and visibility** over **routes and traffic** using **standard interfaces** (BGP)





# Representative

Federation with **CloudLab**

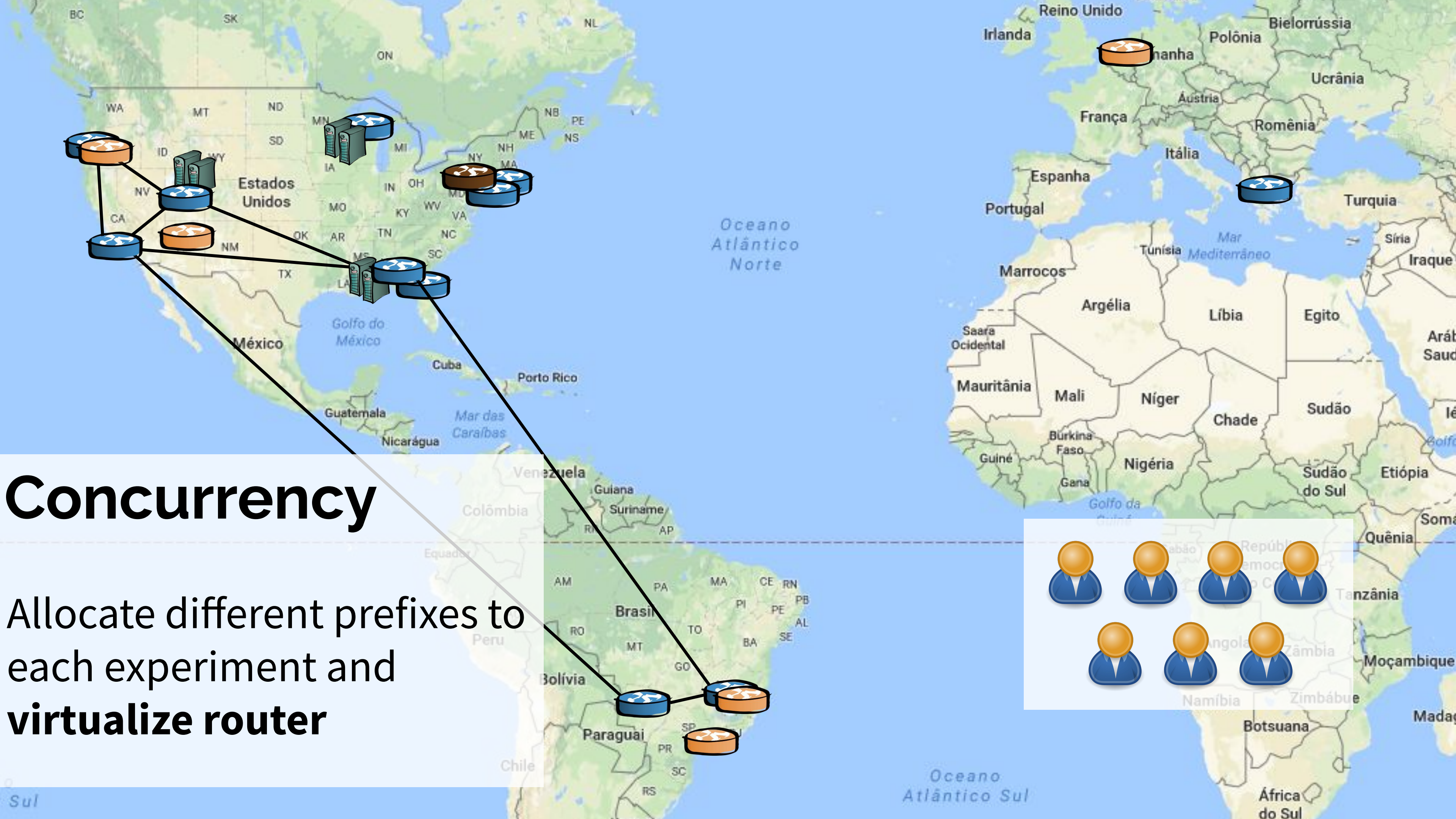


# Representative

Federation with **CloudLab**

L2 virtual **backbone** over research networks

Experiments can emulate **cloud/content providers**



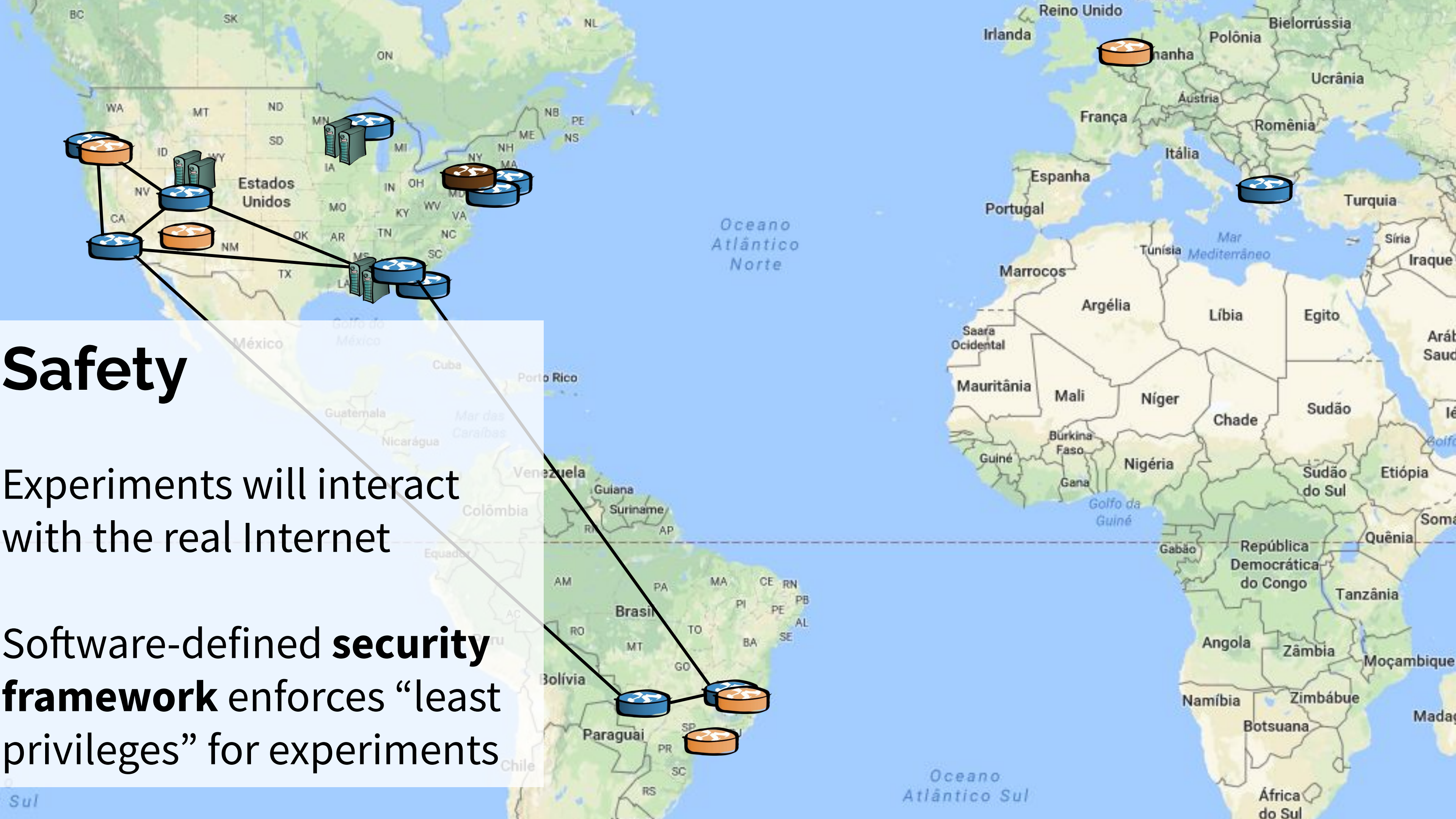
# Concurrency

Allocate different prefixes to each experiment and **virtualize router**

# Safety

Experiments will interact with the real Internet

Software-defined **security framework** enforces “least privileges” for experiments



# PEERING requirements

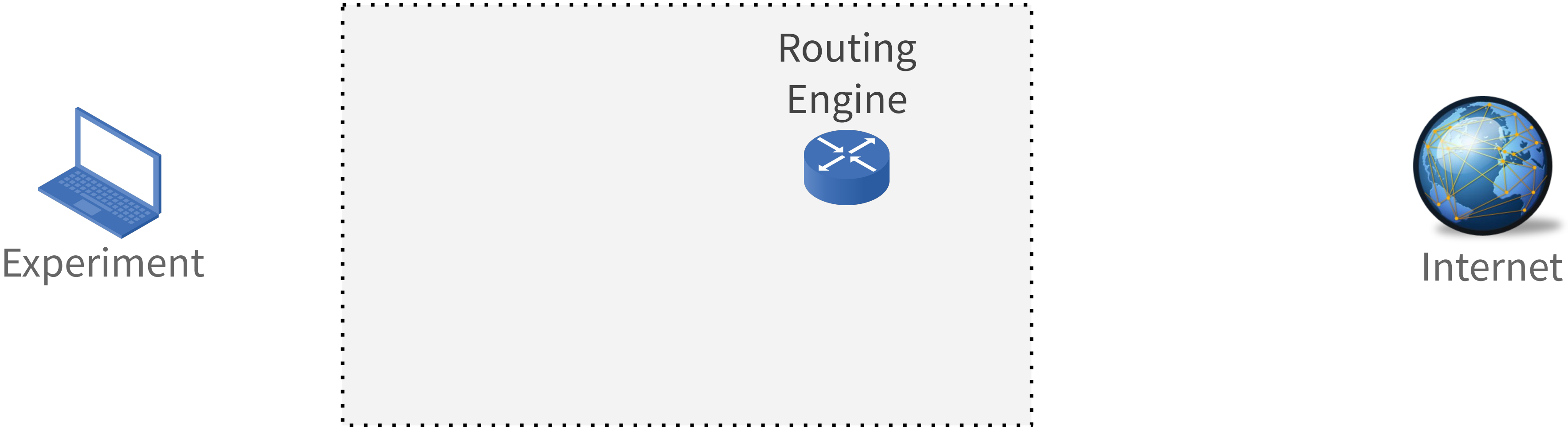
- Achieve **connectivity** to hundreds of networks
    - Combine university and IXP sites
- Delegate **control** over routes and traffic to experiments
    - Integrate layer 2, IP, and BGP in novel ways
- Provide **representative** infrastructure
    - Federate with other testbeds and collaborate with research networks
- Support **concurrent** experiments
    - Allocate and isolate distinct IP prefixes to each experiment
- Ensure **safety** against errors and misbehavior

# PEERING's Security Framework

Experiment

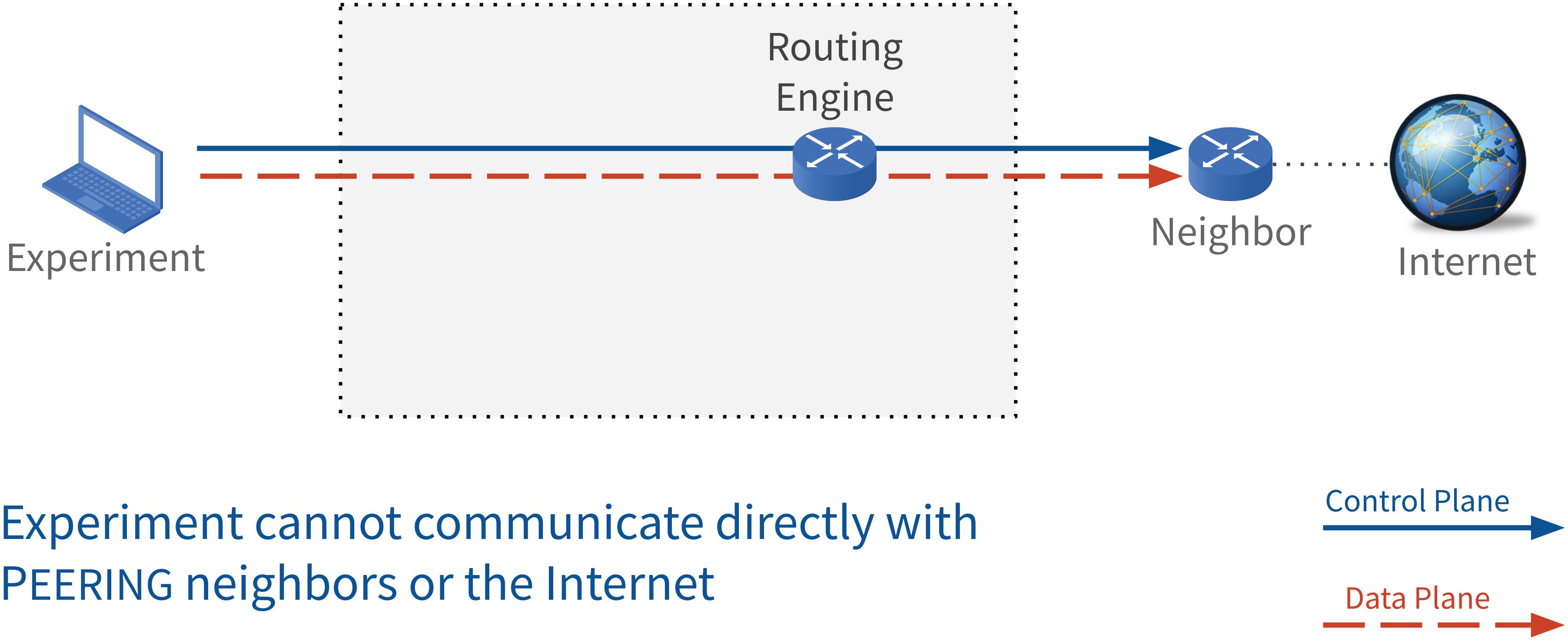
Internet

# PEERING's Security Framework



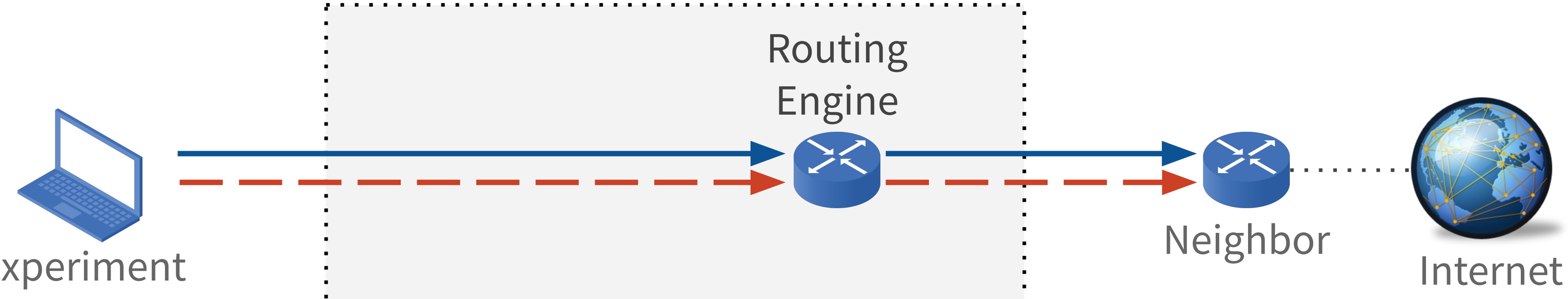
Interpose between experiment and Internet to enforce security

# PEERING's Security Framework



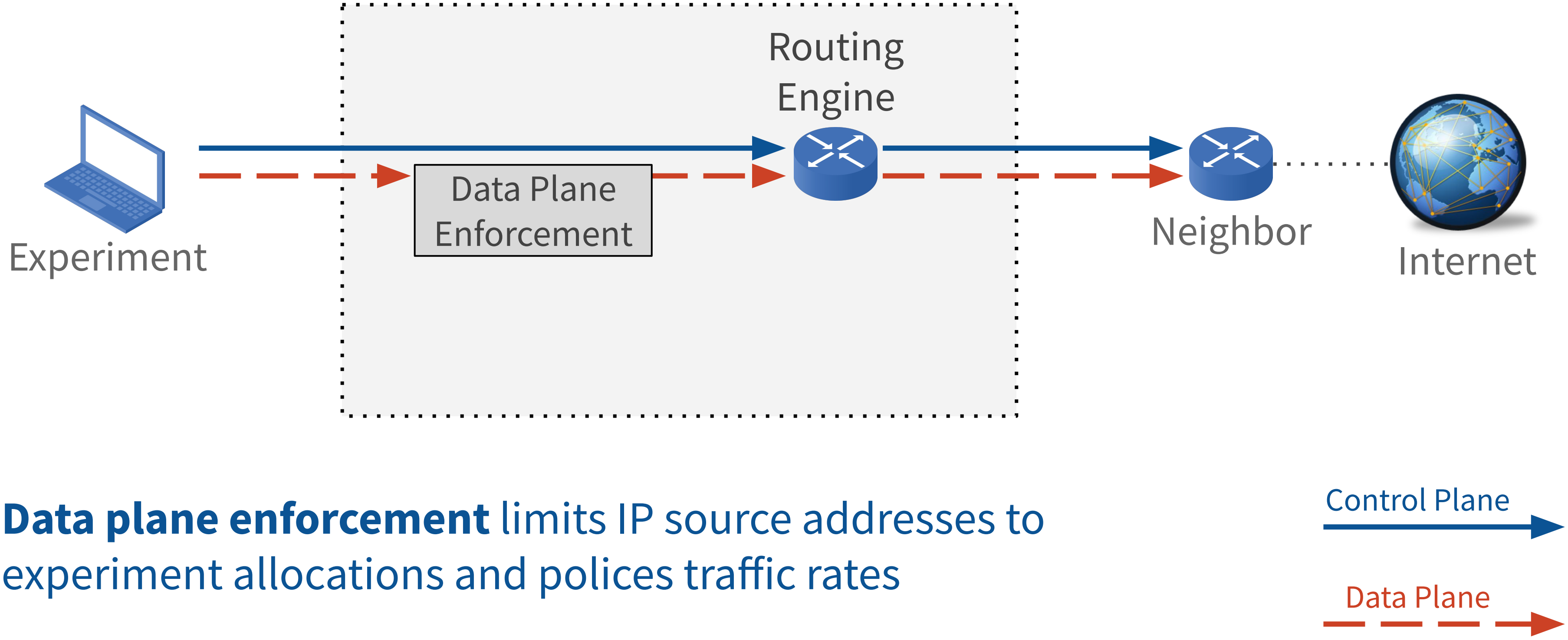
Experiment cannot communicate directly with PEERING neighbors or the Internet

# PEERING's Security Framework



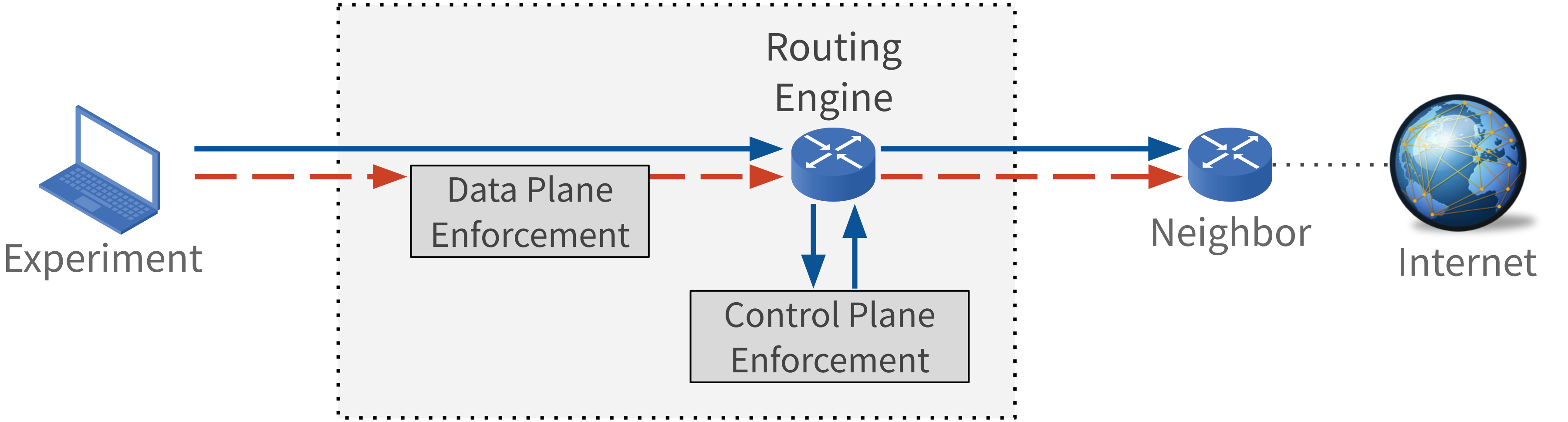
Existing **routing engines** and Linux traffic control do not support general security policies

# PEERING's Security Framework



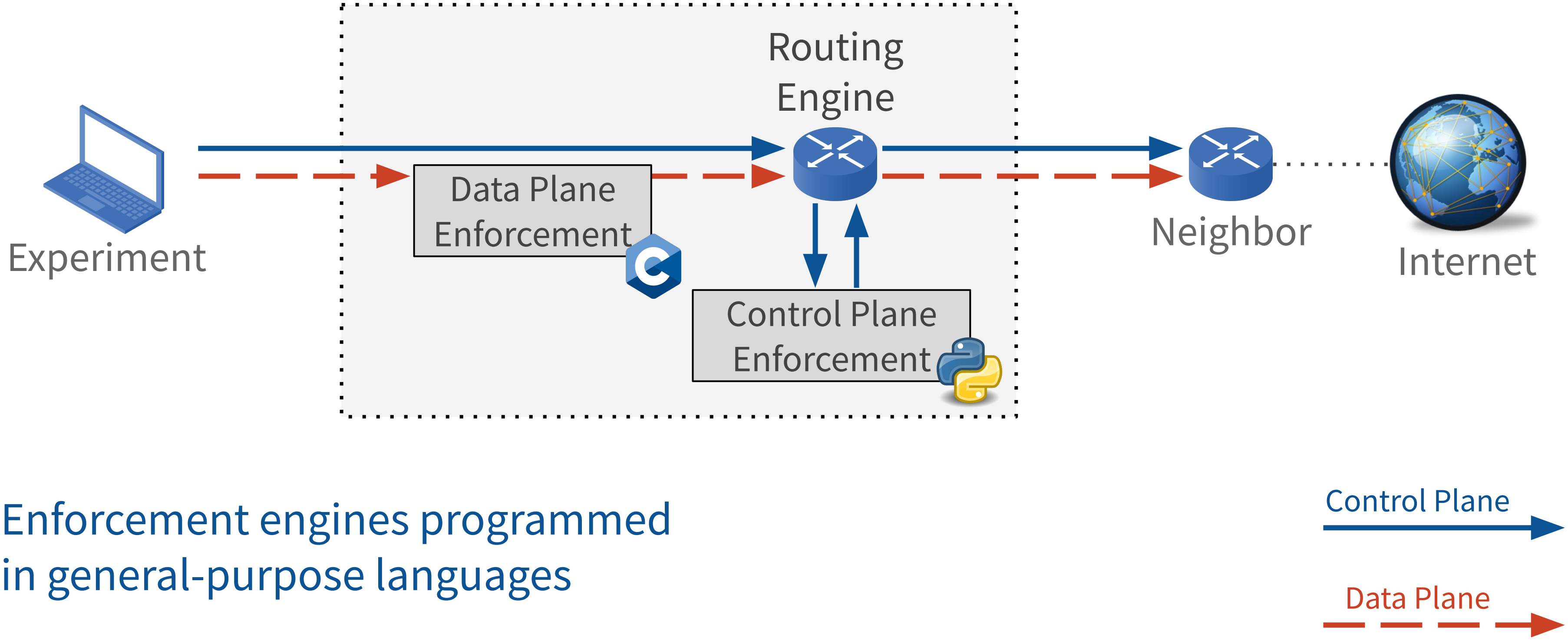
**Data plane enforcement** limits IP source addresses to experiment allocations and polices traffic rates

# PEERING's Security Framework



**Control plane enforcement** limits BGP update rate and contents

# PEERING's Security Framework



Enforcement engines programmed in general-purpose languages

# Capabilities Framework

Per-experiment capabilities enforced by security framework

| | |
|---|---|
| ● AS-path prepending | (AS-path length) |
| ● AS-path poisoning | (number of targets) |
| ● Maximum prefix length | (/25 and /49) |
| ● Propagate communities | (number of communities) |
| ● Origin AS numbers | (set) |

# Capabilities Framework

Per-experiment capabilities enforced by security framework

- AS-path prepending (AS-path length)
- AS-path poisoning (number of targets)
- Maximum prefix length (/25 and /49)
- Propagate communities (number of communities)
- Origin AS numbers (set)

Facilitates deployment of new types of experiments

“Principle of least privilege” capability allocation

# 40+ Experiments Have Used PEERING

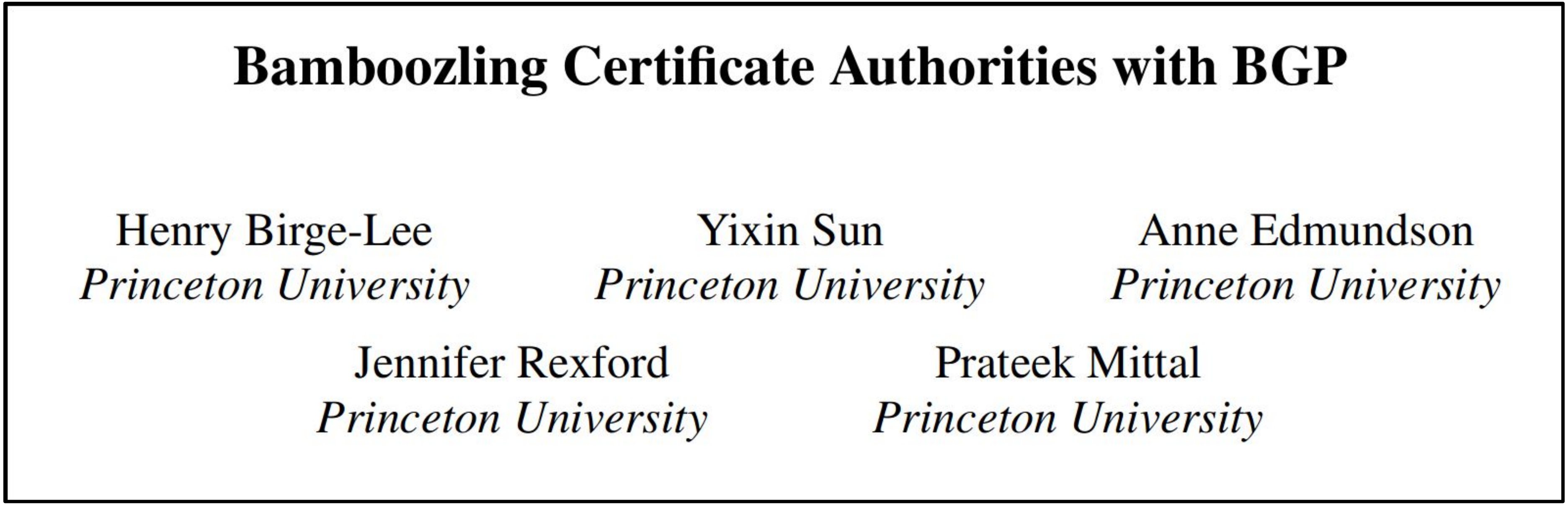
Security research used PEERING to

- Demonstrate targeted, stealth traffic interception attacks (2019, ACM CCS)
- Evaluate prefix hijack detection systems (2018, ACM/IEEE ToN)
- Evaluate impact of remote blackholing attacks (2018, ACM IMC)
- Demonstrate false certification of domain ownership (2018, USENIX Security)
- Characterize challenges in characterizing RPKI deployment (2018, ACM CCR)
- Demonstrate routing attacks against cryptocurrencies (**2017**, IEEE S&P)
- Demonstrate countermeasures against attacks on Tor (2017, IEEE S&P)
- Demonstrate traffic attraction attacks to deanonymize Tor users (2015, USENIX Security)

# 40+ Experiments Have Used PEERING

Security research used PEERING to

- Demonstrate targeted, stealth traffic interception attacks (2019, ACM CCS)
- Evaluate prefix hijack detection systems (2018, ACM/IEEE ToN)
- Evaluate impact of remote blackholing attacks (2018, ACM IMC)
- Demonstrate false **certification of domain** ownership (2018, USENIX Security)
- Characterize challenges in characterizing RPKI deployment (2018, ACM CCR)
- Demonstrate routing attacks against cryptocurrencies (**2017**, IEEE S&P)
- Demonstrate countermeasures against attacks on Tor (2017, IEEE S&P)
- Demonstrate traffic attraction attacks to deanonymize Tor users (2015, USENIX Security)



**Bamboozling Certificate Authorities with BGP**

Henry Birge-Lee
*Princeton University*

Yixin Sun
*Princeton University*

Anne Edmundson
*Princeton University*

Jennifer Rexford
*Princeton University*

Prateek Mittal
*Princeton University*

- Demonstrated false certification of domain ownership
  - And then how to proxy *encrypted* traffic to a website

# Hosting a Website on PEERING

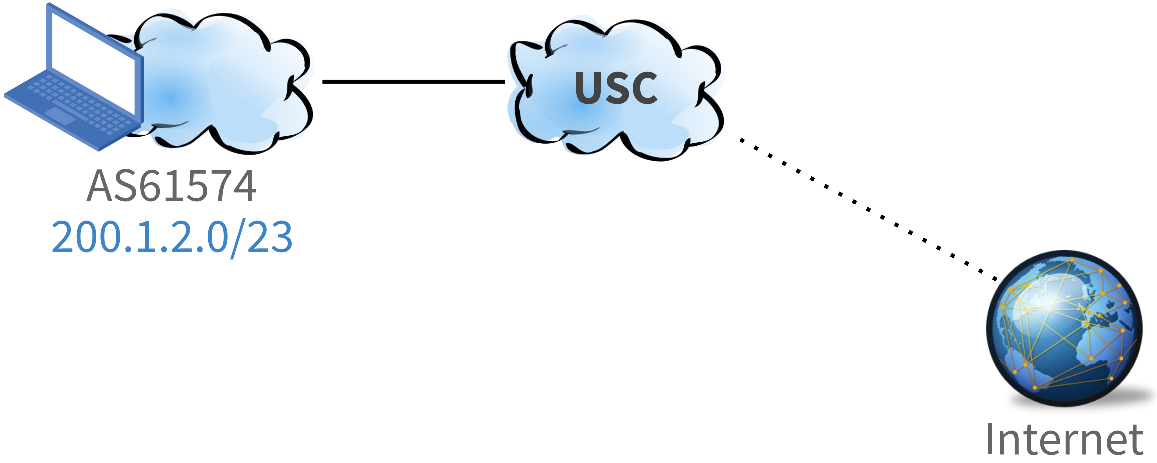
- Get ASN and IP prefix allocation

# Hosting a Website on PEERING

AS61574
200.1.2.0/23

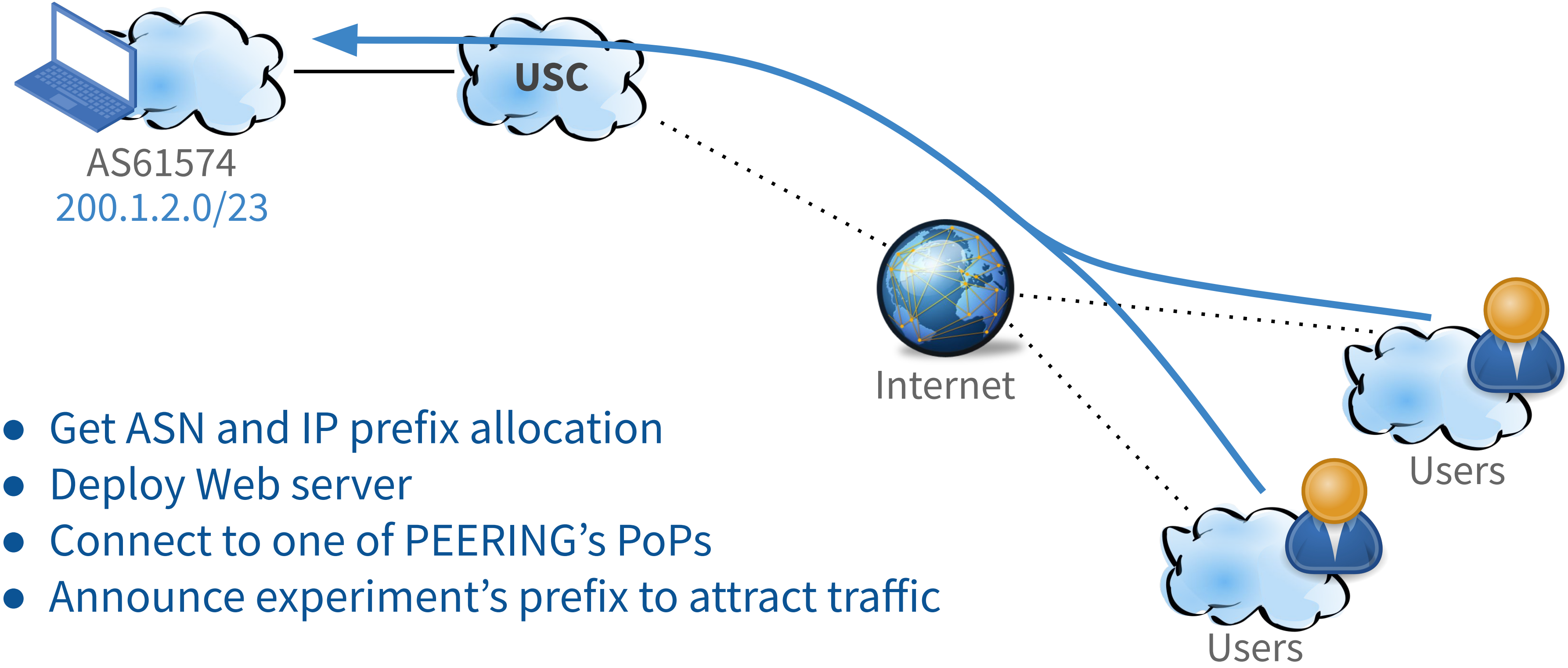
- Get ASN and IP prefix allocation
- Deploy Web server

# Hosting a Website on PEERING



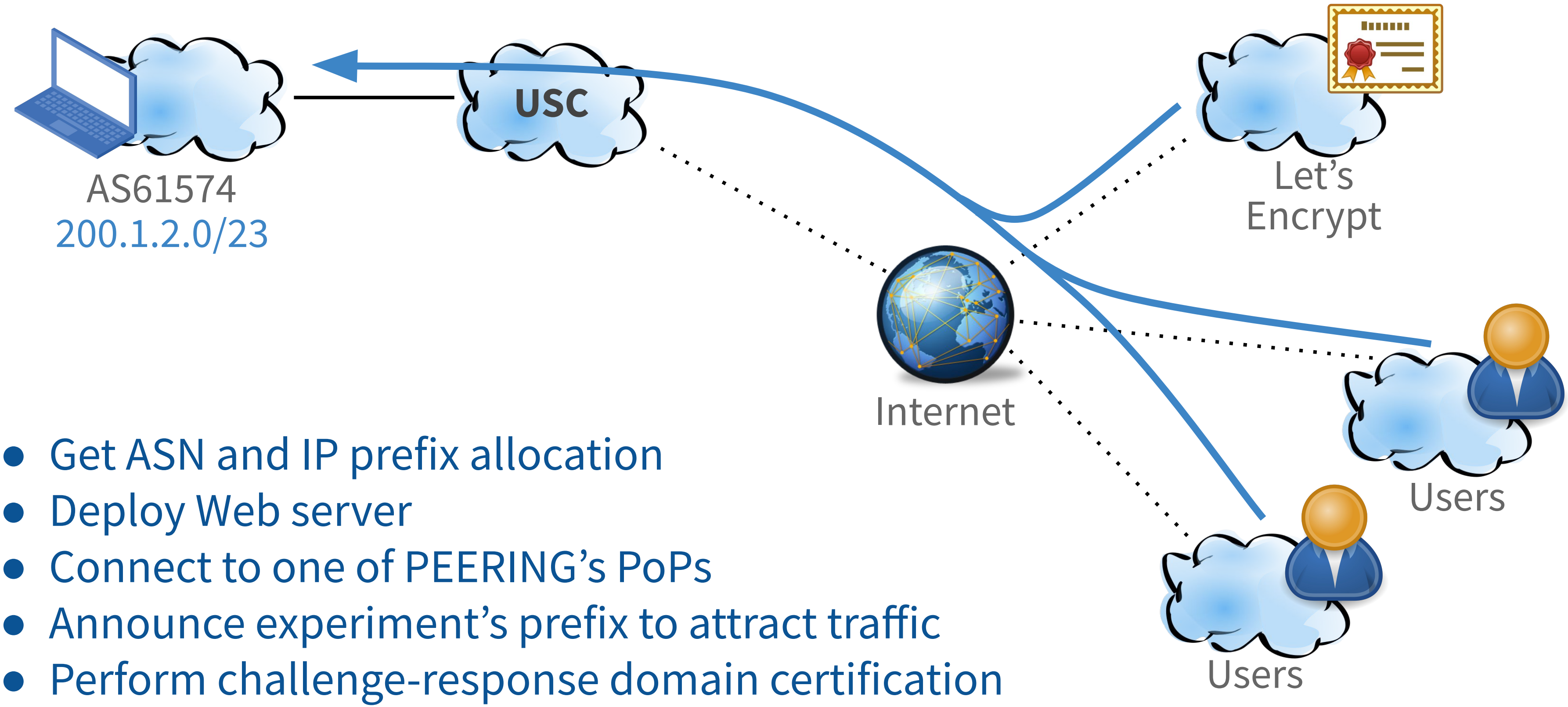
- Get ASN and IP prefix allocation
- Deploy Web server
- Connect to one of PEERING's PoPs

# Hosting a Website on PEERING



- Get ASN and IP prefix allocation
- Deploy Web server
- Connect to one of PEERING’s PoPs
- Announce experiment’s prefix to attract traffic

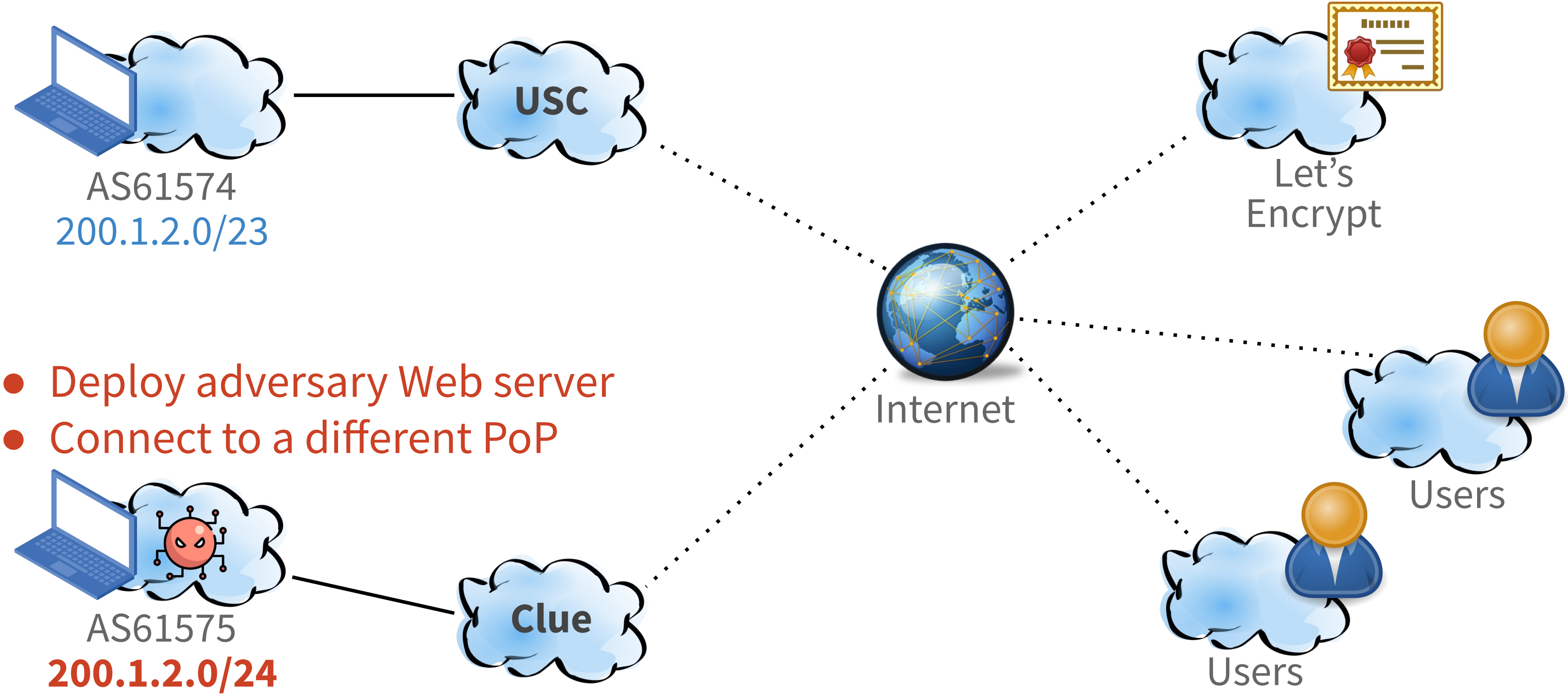
# Obtaining a Certificate



- Get ASN and IP prefix allocation
- Deploy Web server
- Connect to one of PEERING’s PoPs
- Announce experiment’s prefix to attract traffic
- Perform challenge-response domain certification

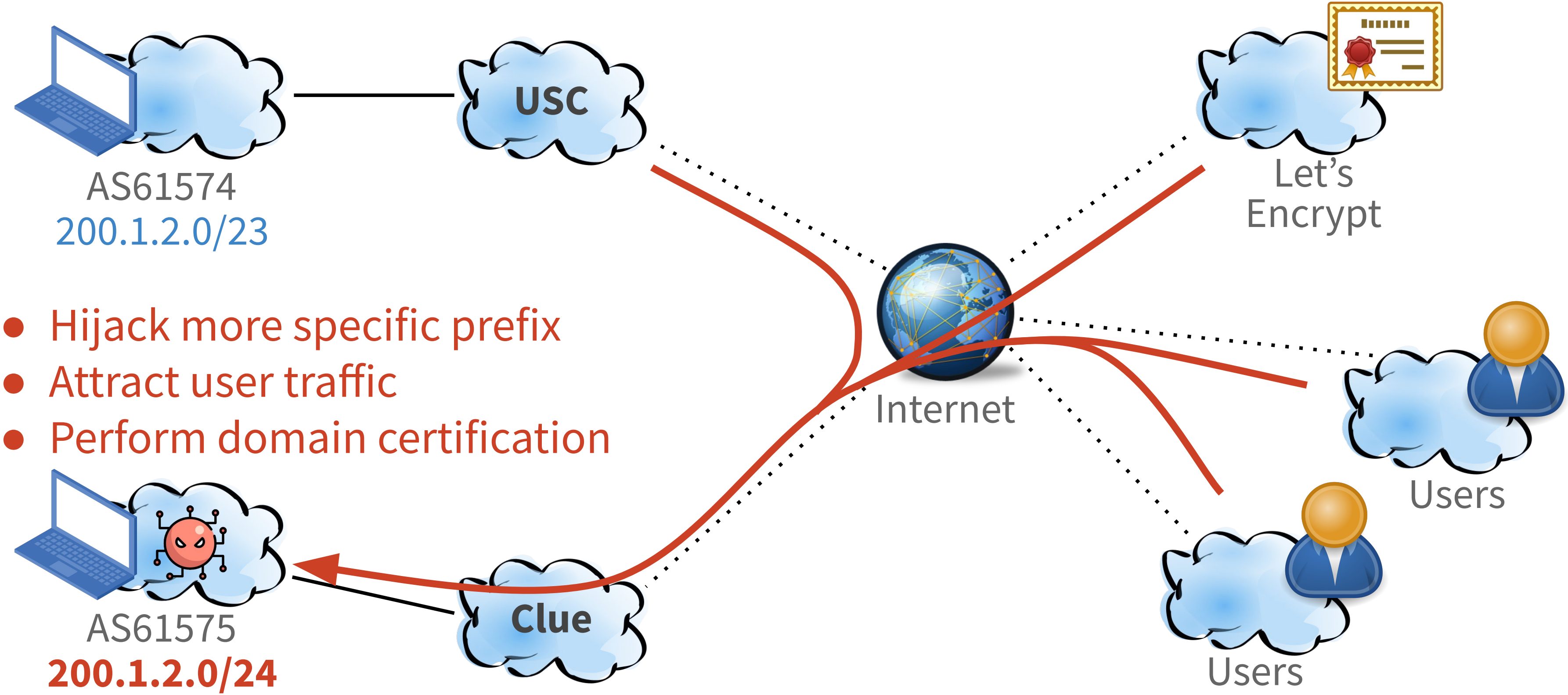
# Obtaining a False Certificate

- Deploy adversary Web server
- Connect to a different PoP

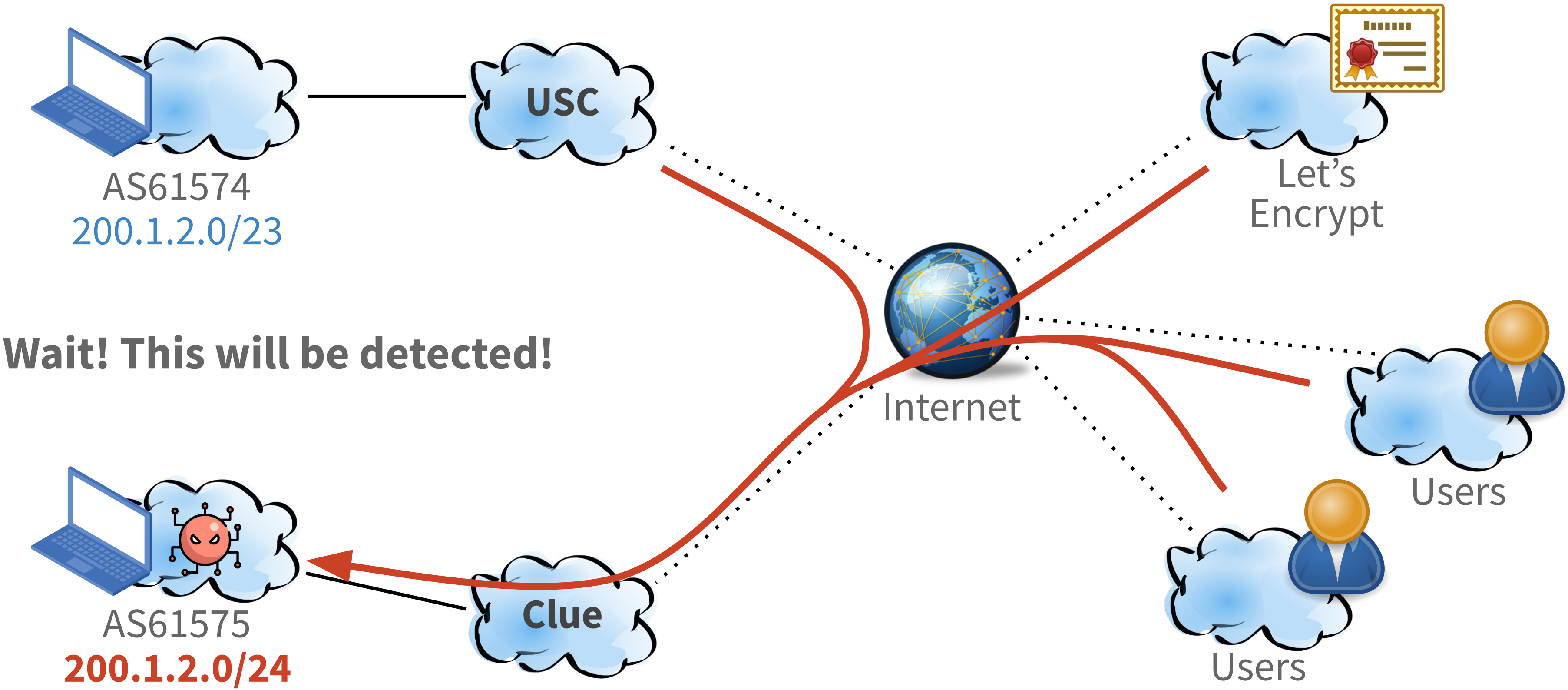


# Obtaining a False Certificate

- Hijack more specific prefix
- Attract user traffic
- Perform domain certification

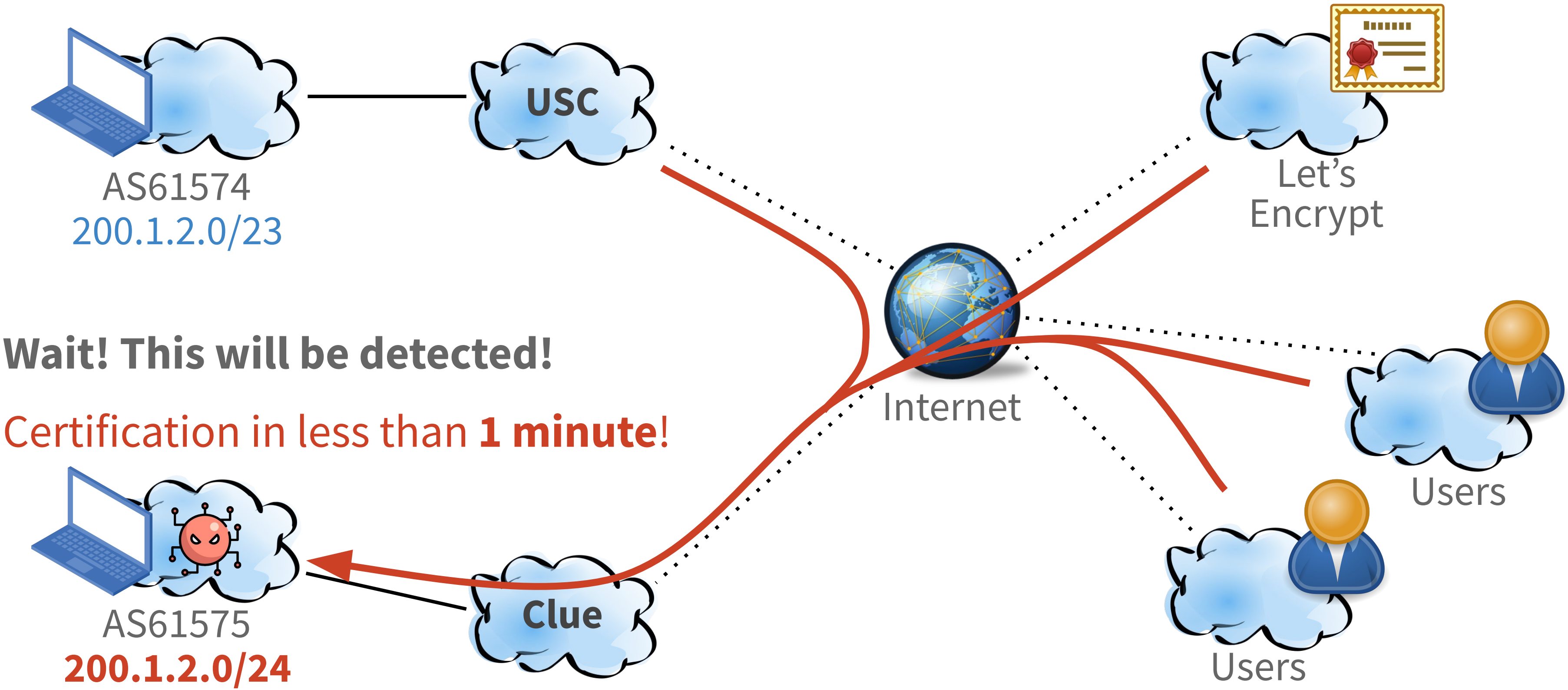


# Obtaining a False Certificate



**Wait! This will be detected!**

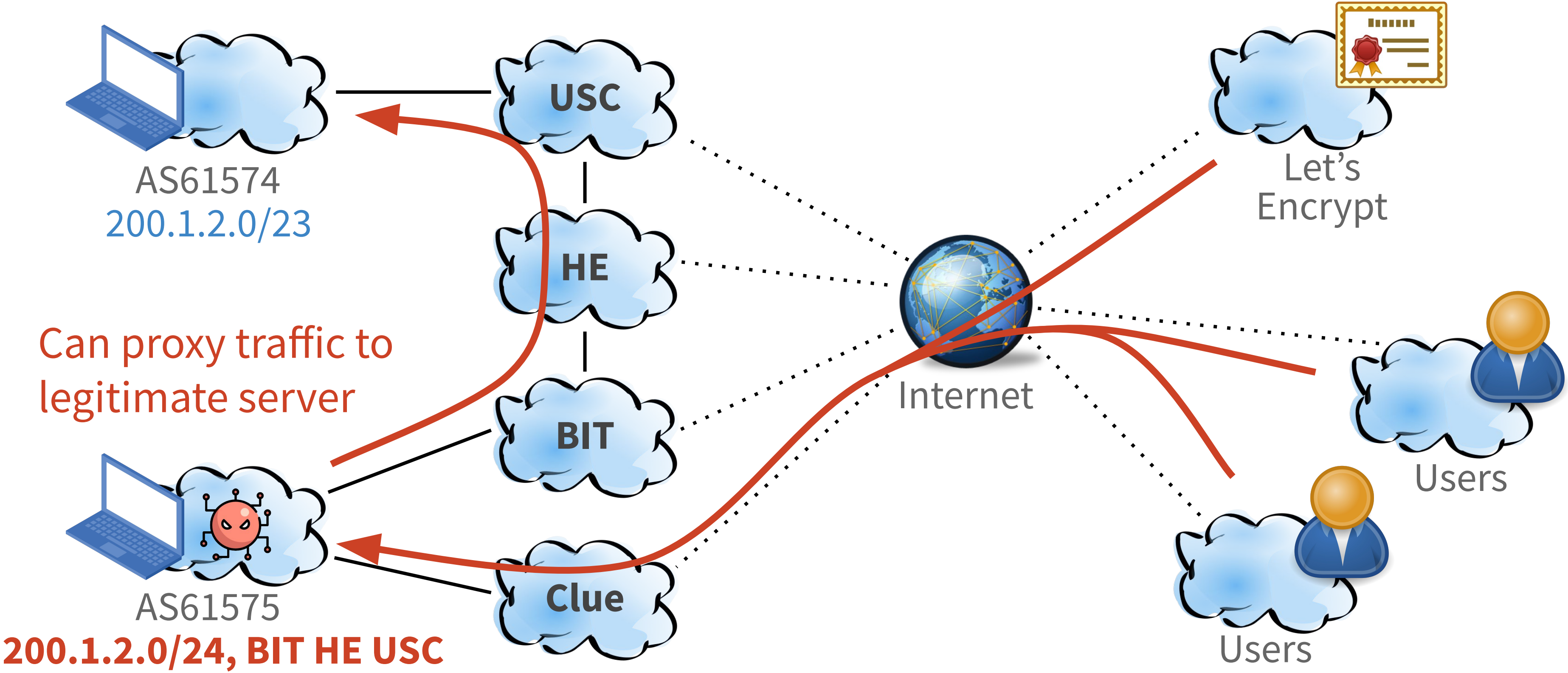
# Obtaining a False Certificate



**Wait! This will be detected!**

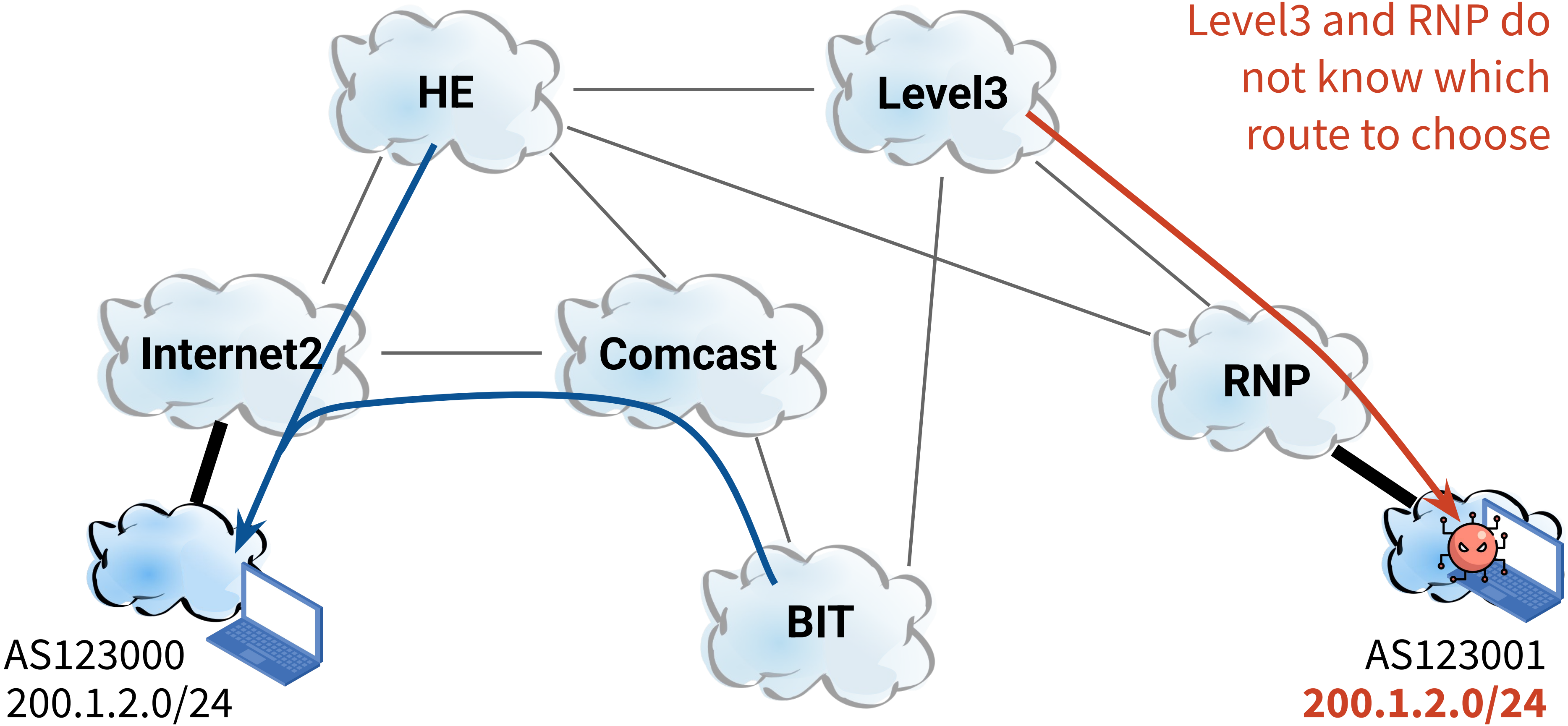
Certification in less than **1 minute**!

# Eavesdropping on a Website’s Traffic



Can proxy traffic to legitimate server

# Example: Prefix Hijacks



Level3 and RNP do not know which route to choose