

caida

CSE 291 INTERNET DATA SCIENCE FOR CYBERSECURITY

11 January 2023

**IP Address Spoofing and
Source Address Validation**

OVERVIEW



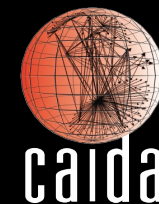
1. Background to support your reading of a research paper *“Network Hygiene, Incentives, and Regulation: Deployment of Source Address Validation in the Internet”* ACM CCS 2019.
2. Please read the paper and be ready to discuss it in class on Wednesday Jan 18th (Mon is a UCSD holiday)
3. Assignment 1, which analyses “spoofers project” data is due Monday Jan 23rd

LEARNING OBJECTIVES



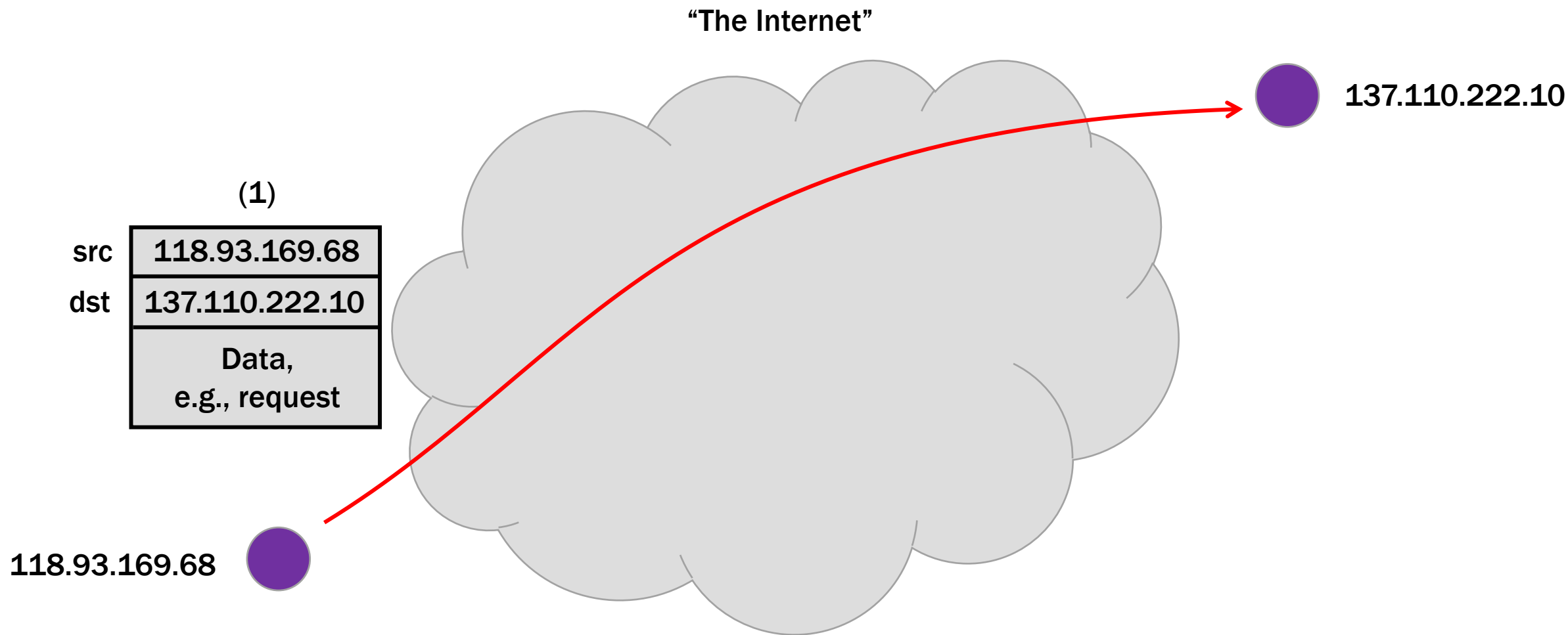
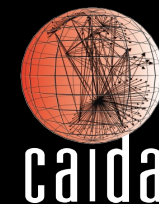
1. Describe IPv4 and IPv6 addresses and prefixes, the basics of BGP and ASes, NAT (refresher for some)
2. Understand DoS attack methods, particularly reflection amplification
3. Describe inbound and outbound spoofing
4. Understand goals of Source Address Validation, and deployment methods for edge and transit networks

IP ADDRESSES

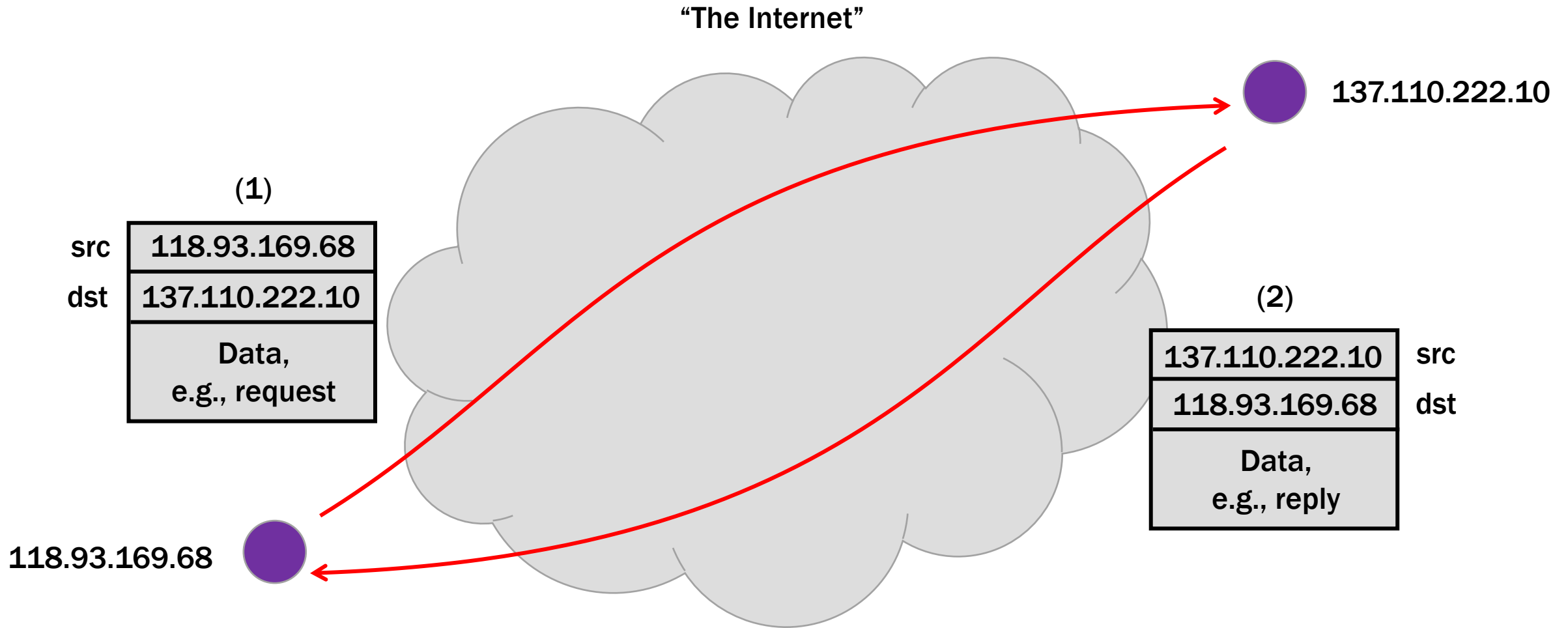


- All Internet-connected devices have IP addresses
 - nearly always an IPv4 (32-bit) address
 - e.g., 137.110.222.10
 - sometimes also an IPv6 (128-bit) address
 - e.g., 2407:7000:9000:ee02:9981:73b1:d13a:73cf

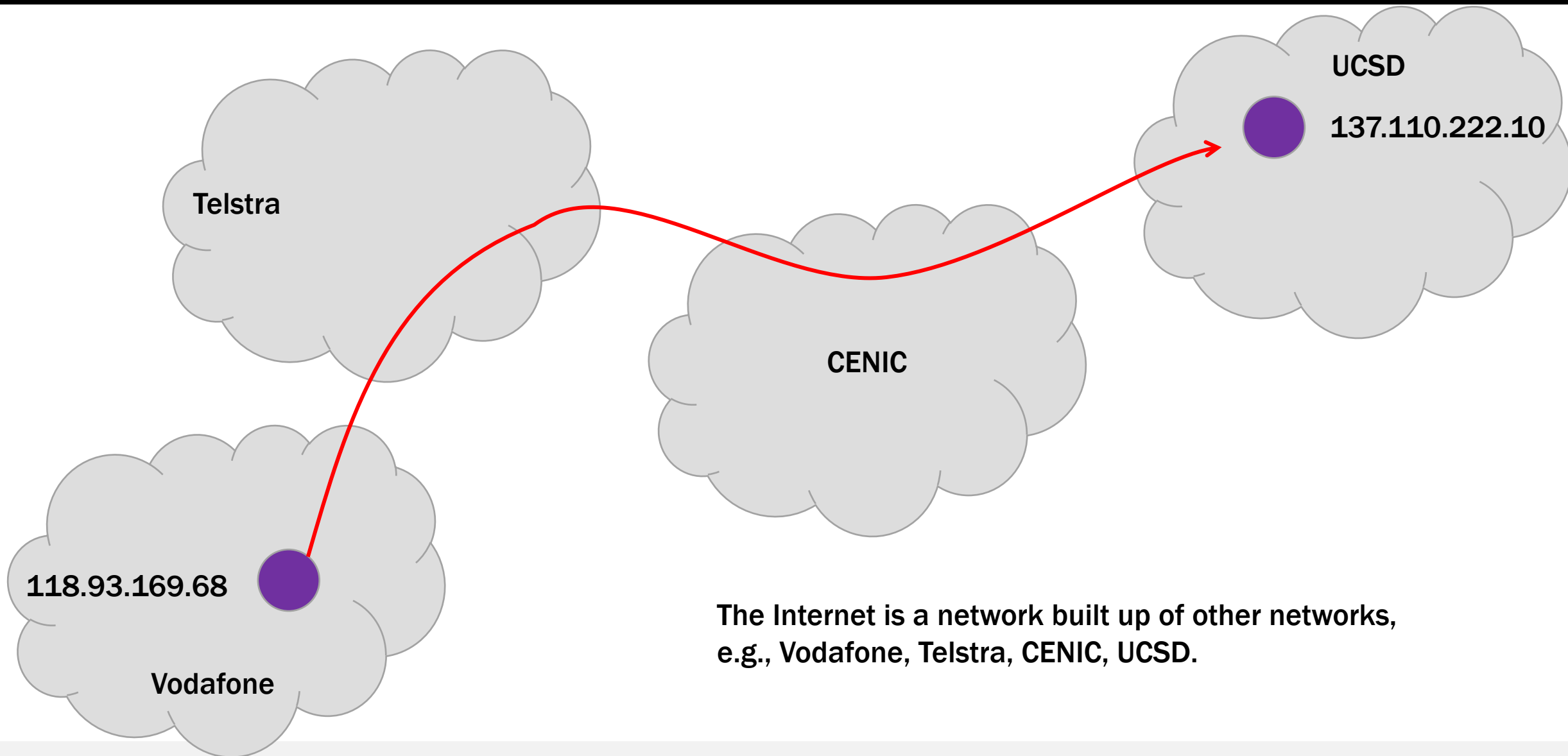
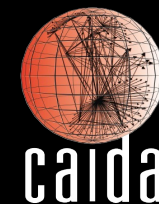
IP PACKET DELIVERY



IP PACKET DELIVERY

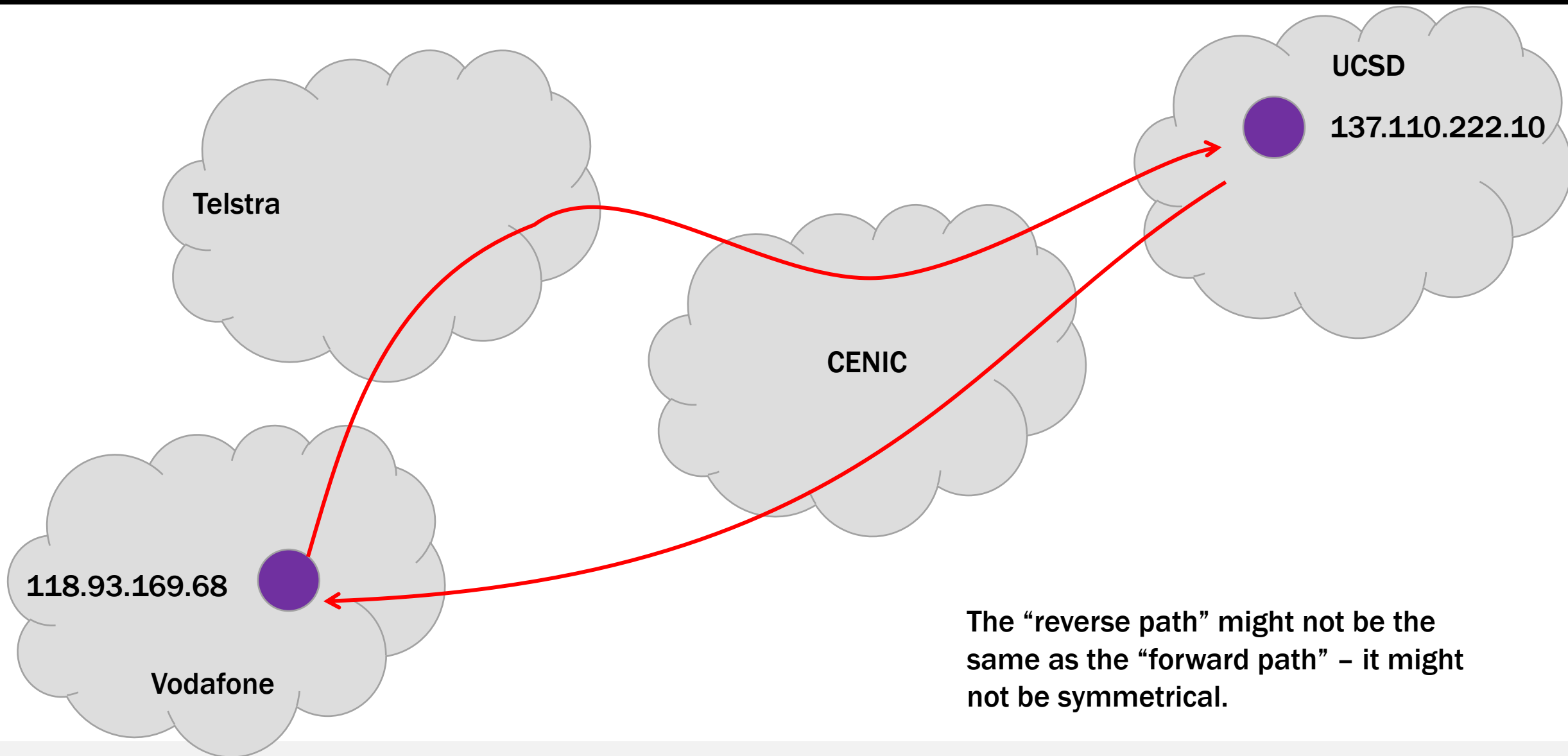
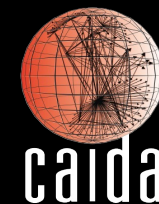


INTERNET ROUTING

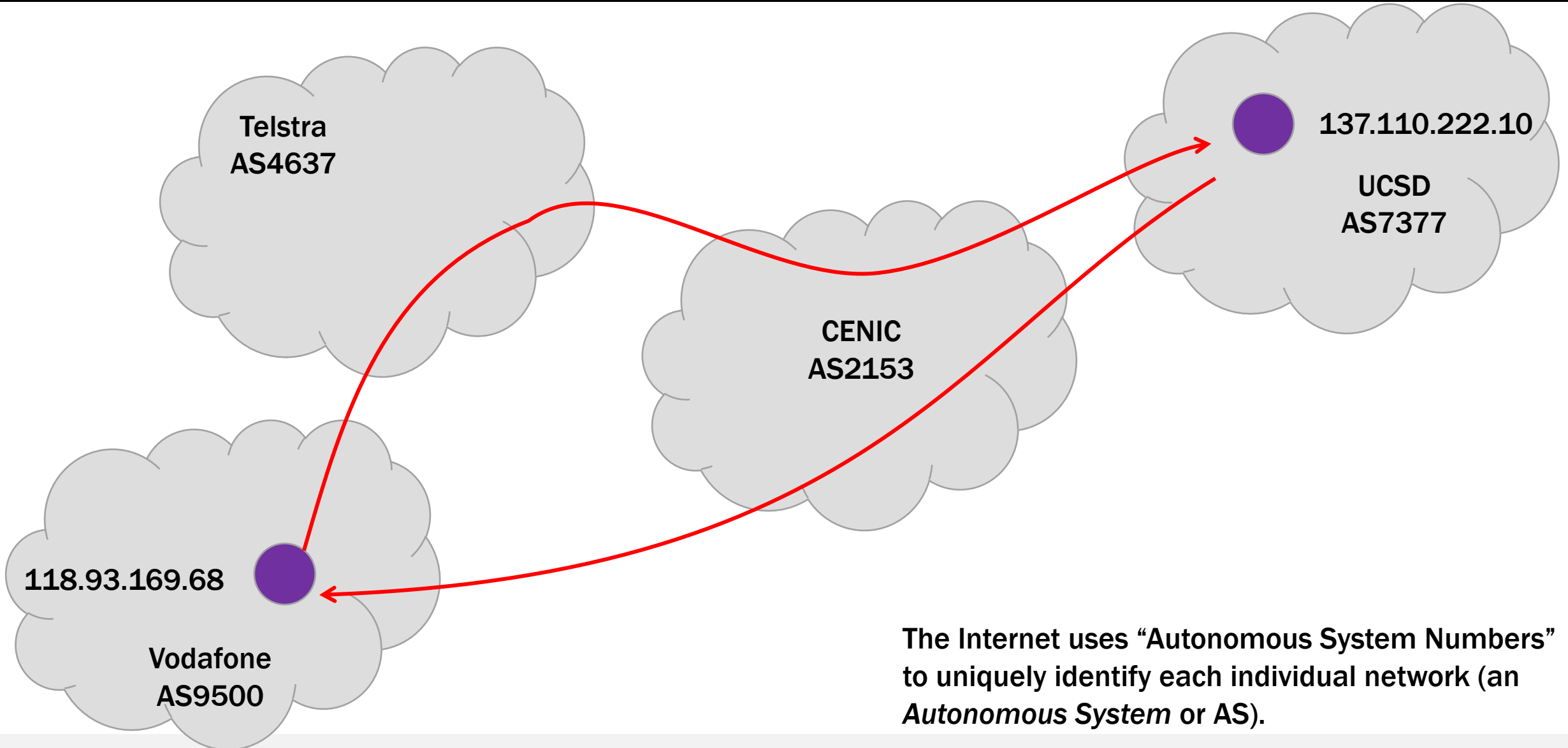


The Internet is a network built up of other networks, e.g., Vodafone, Telstra, CENIC, UCSD.

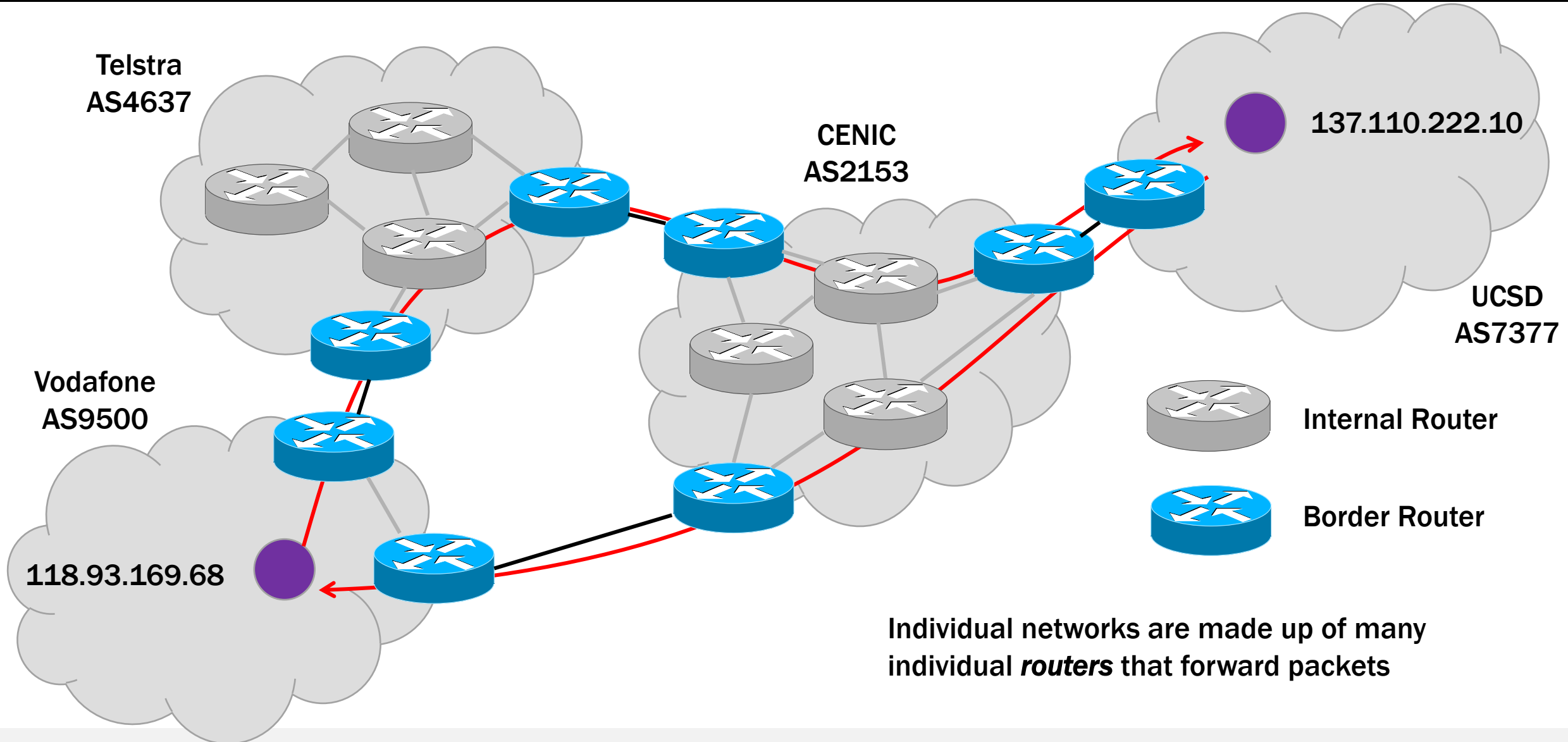
INTERNET ROUTING



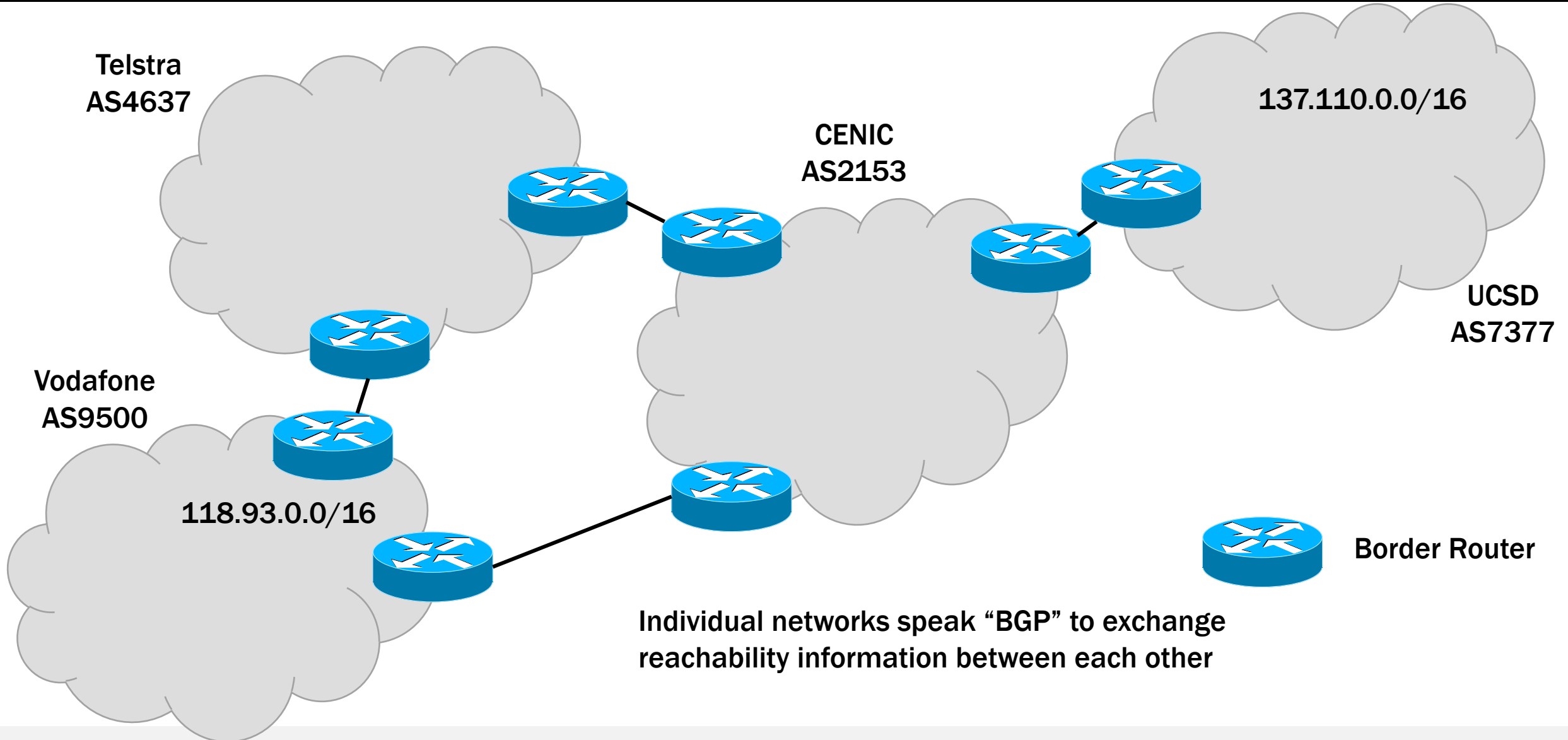
AUTONOMOUS SYSTEMS



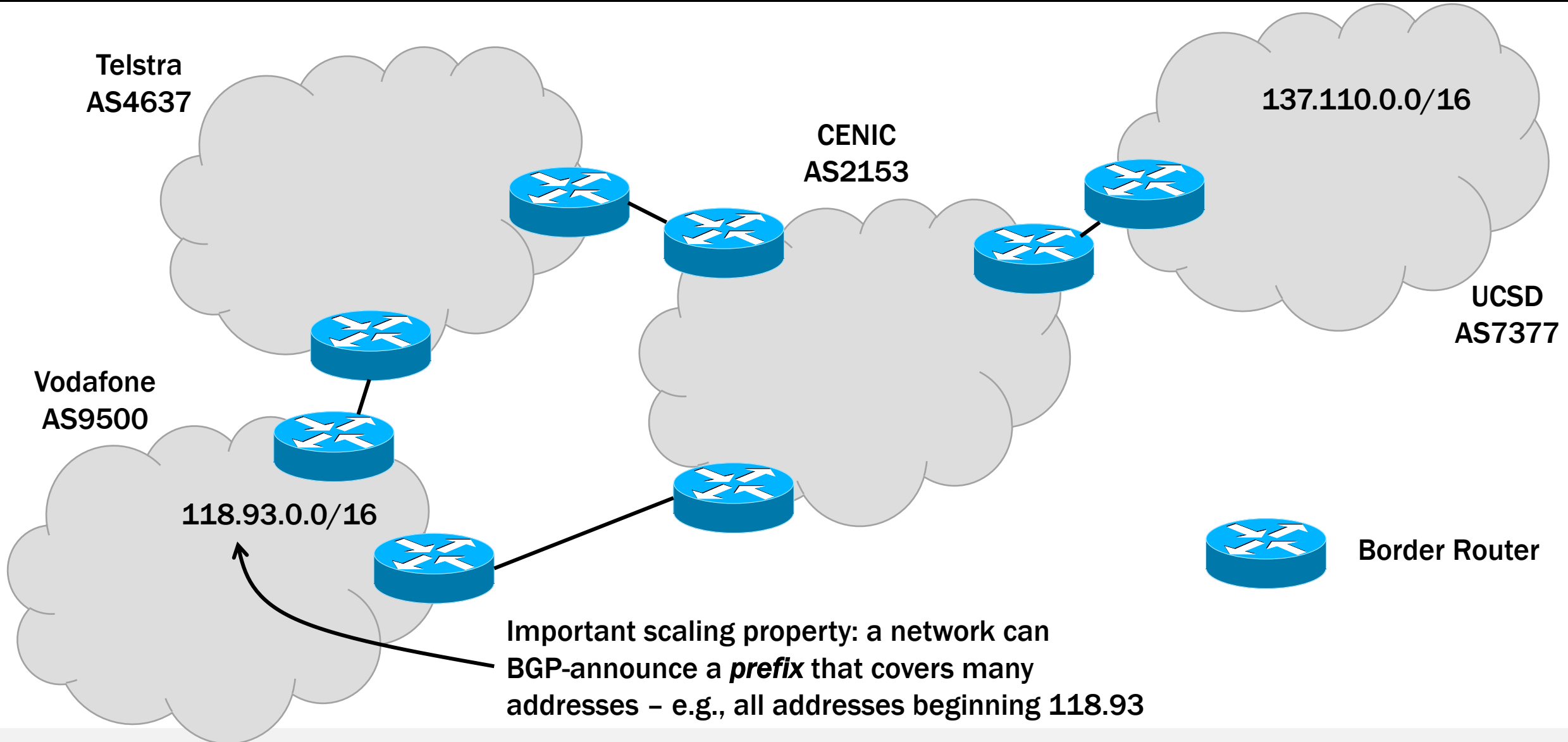
AUTONOMOUS SYSTEMS



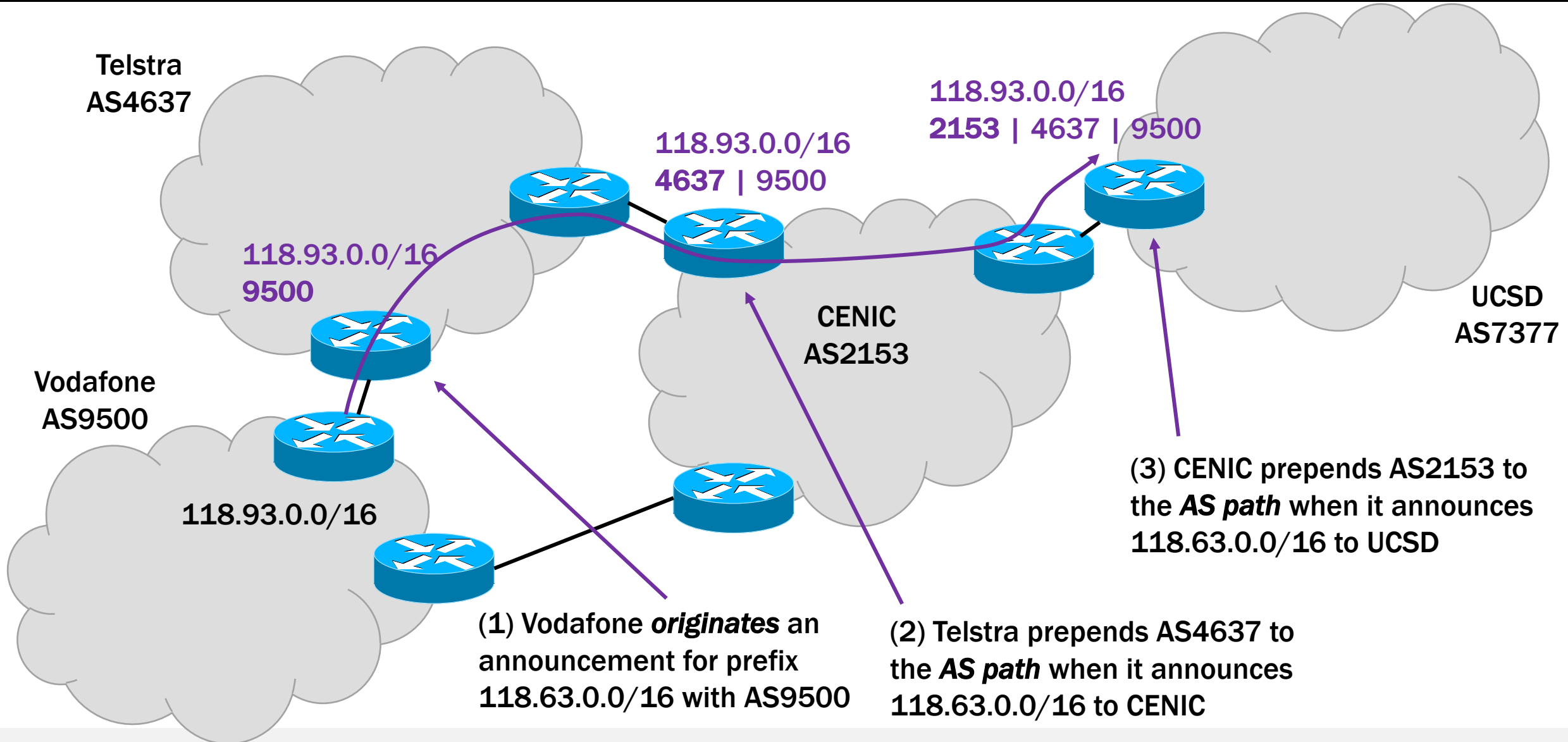
BORDER GATEWAY PROTOCOL



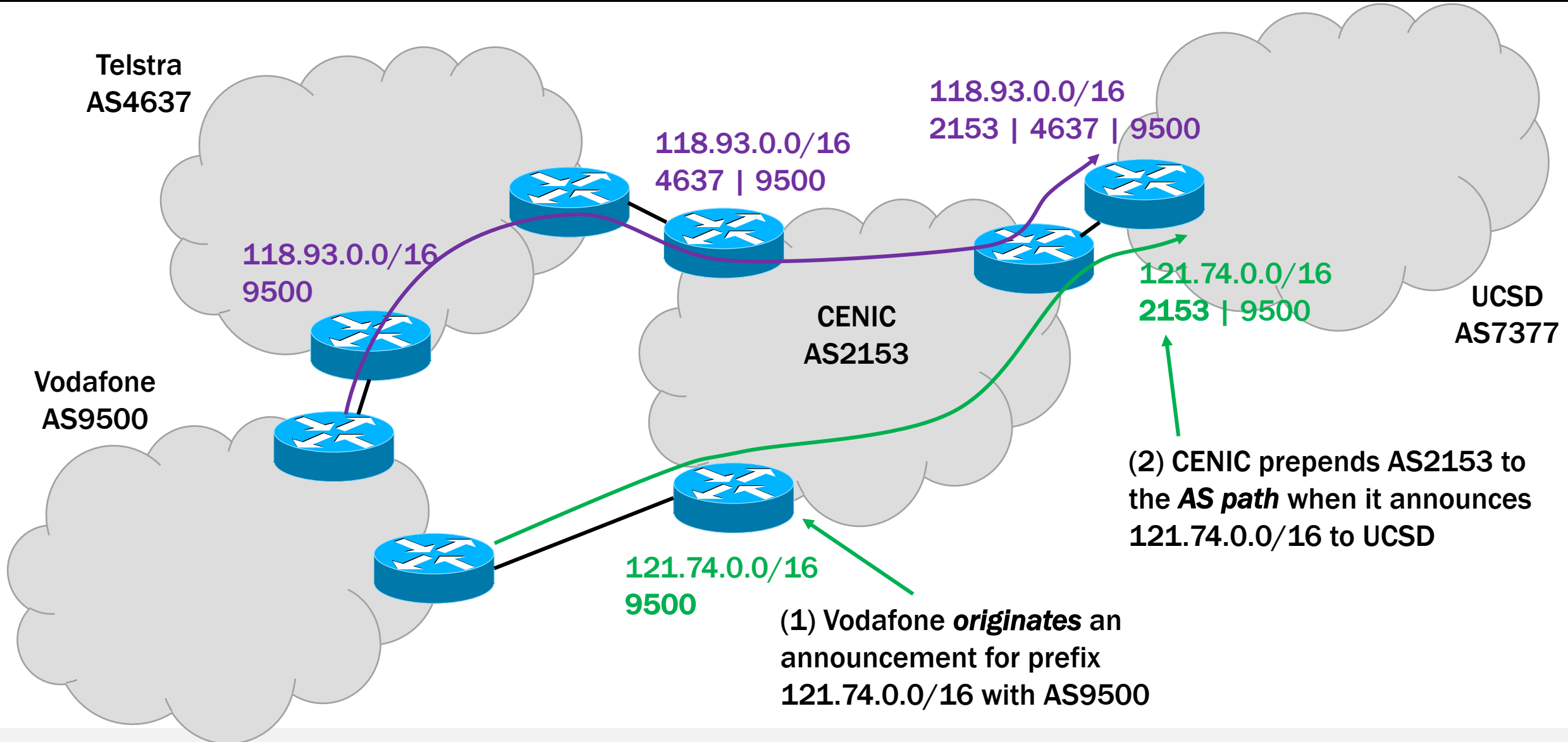
BORDER GATEWAY PROTOCOL



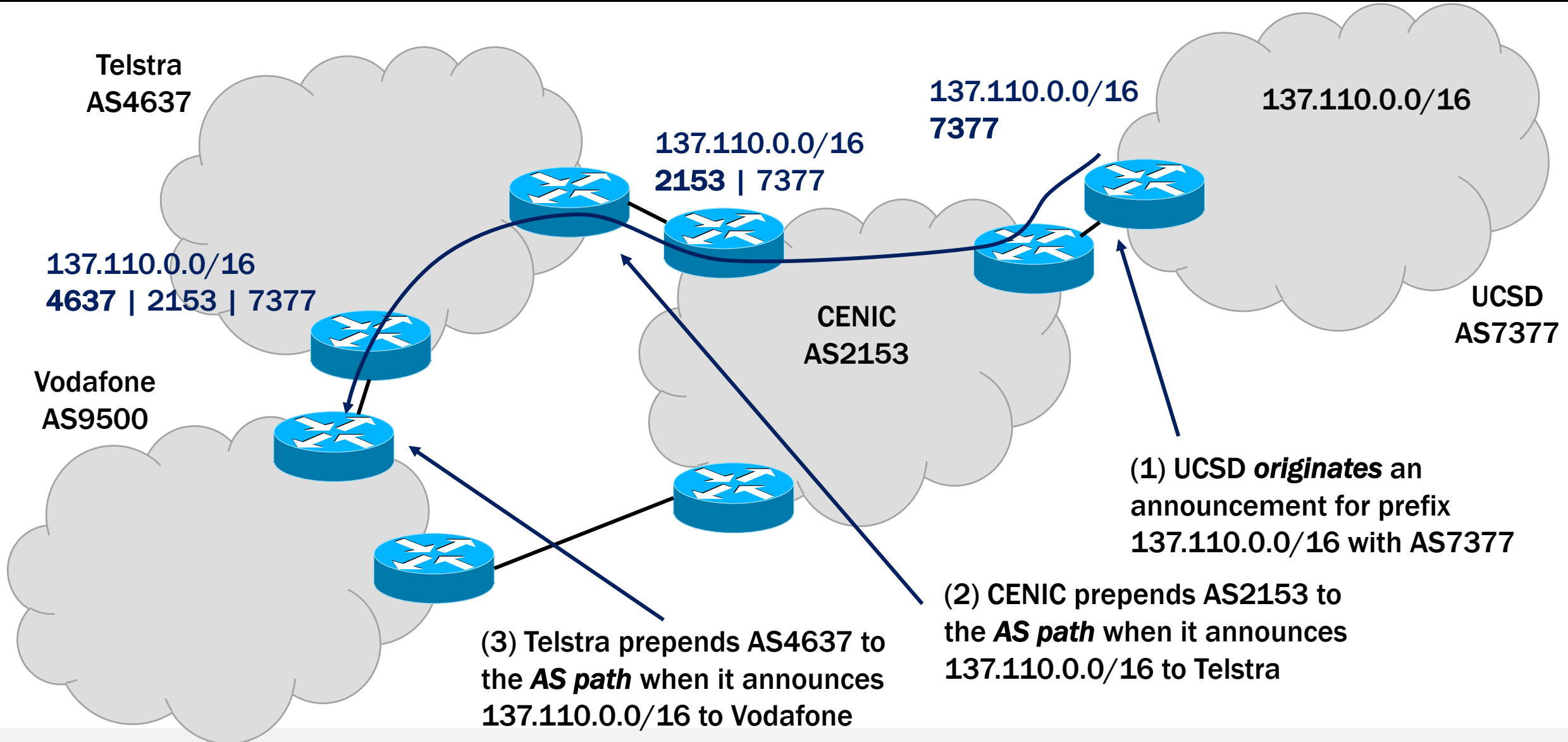
BORDER GATEWAY PROTOCOL



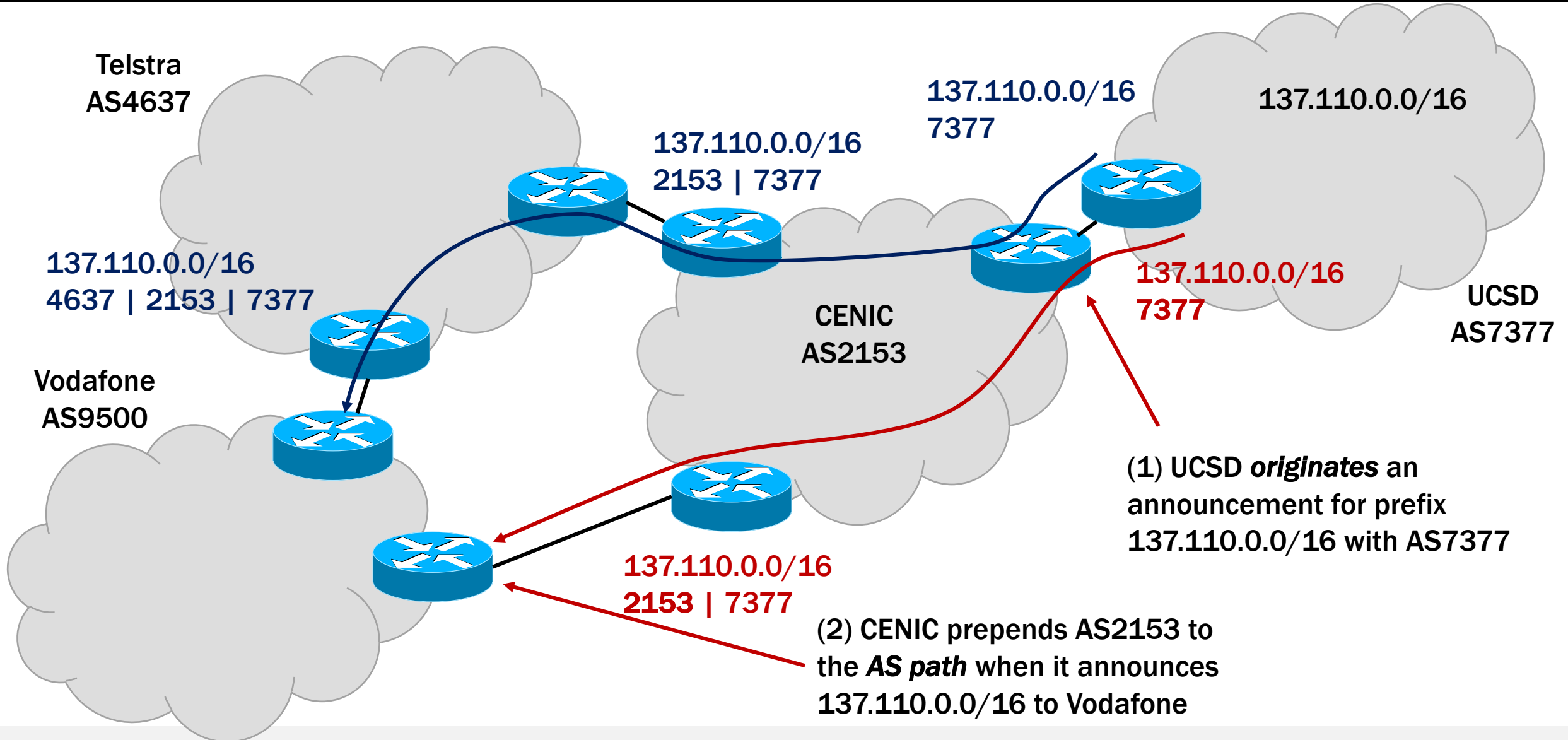
BORDER GATEWAY PROTOCOL



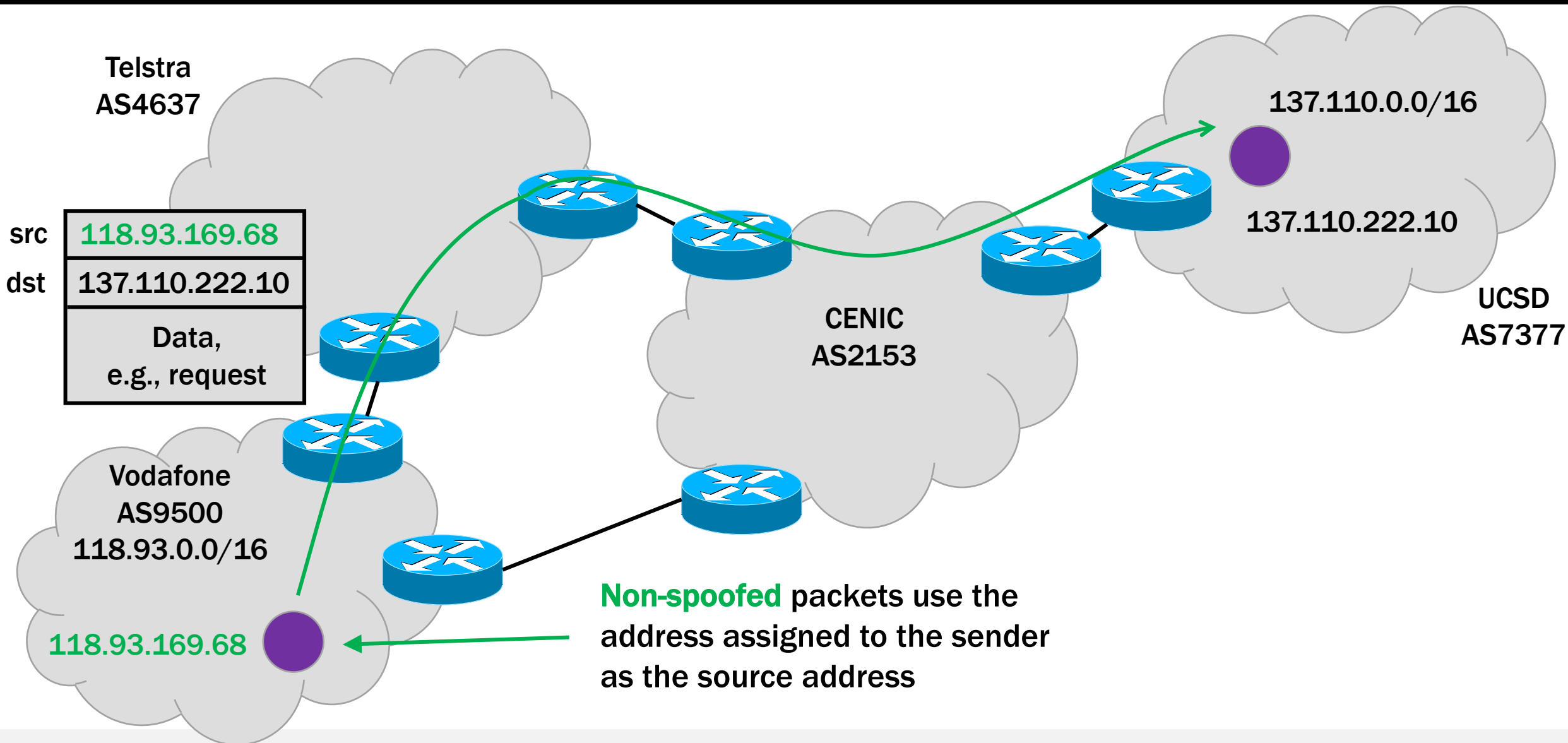
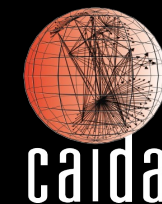
BORDER GATEWAY PROTOCOL



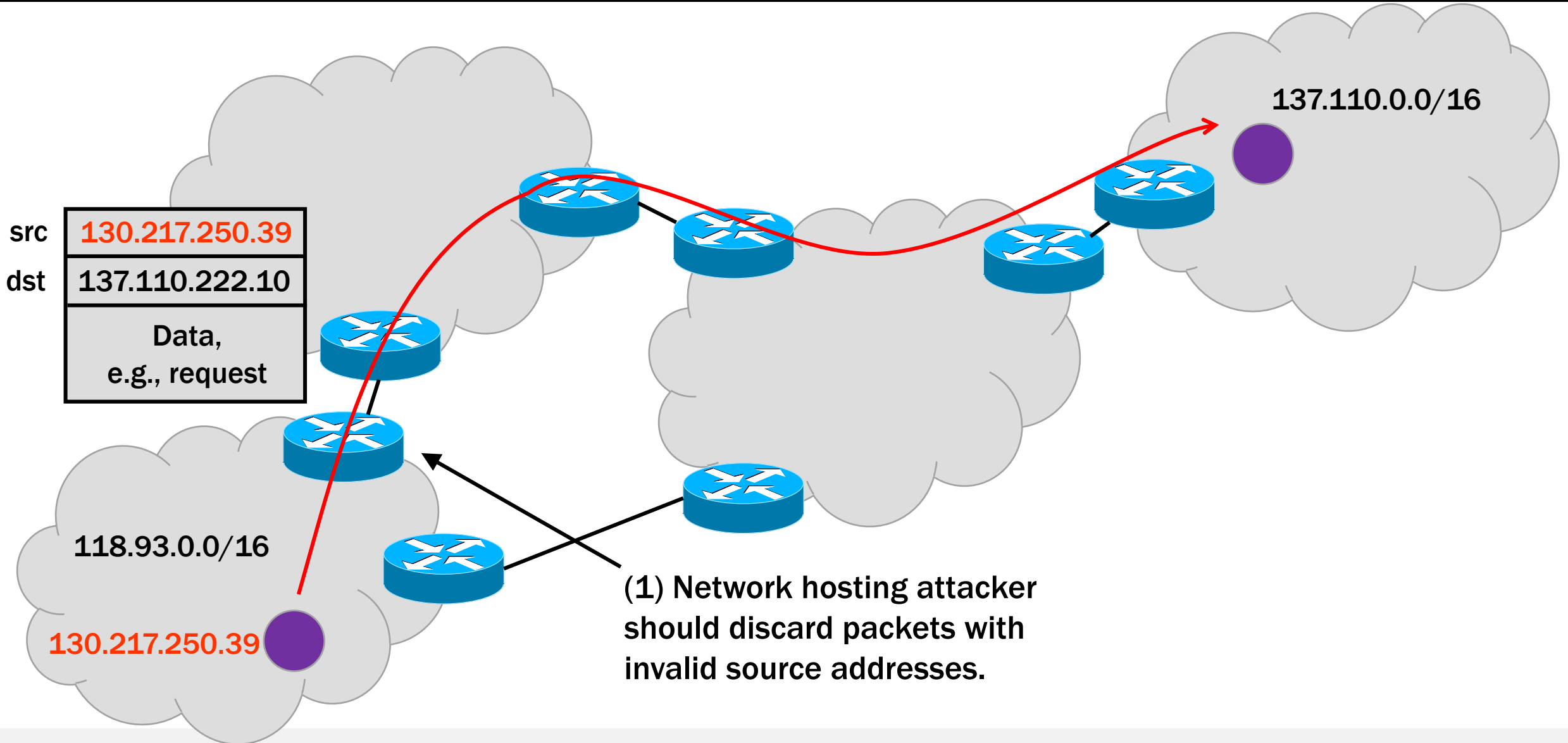
BORDER GATEWAY PROTOCOL



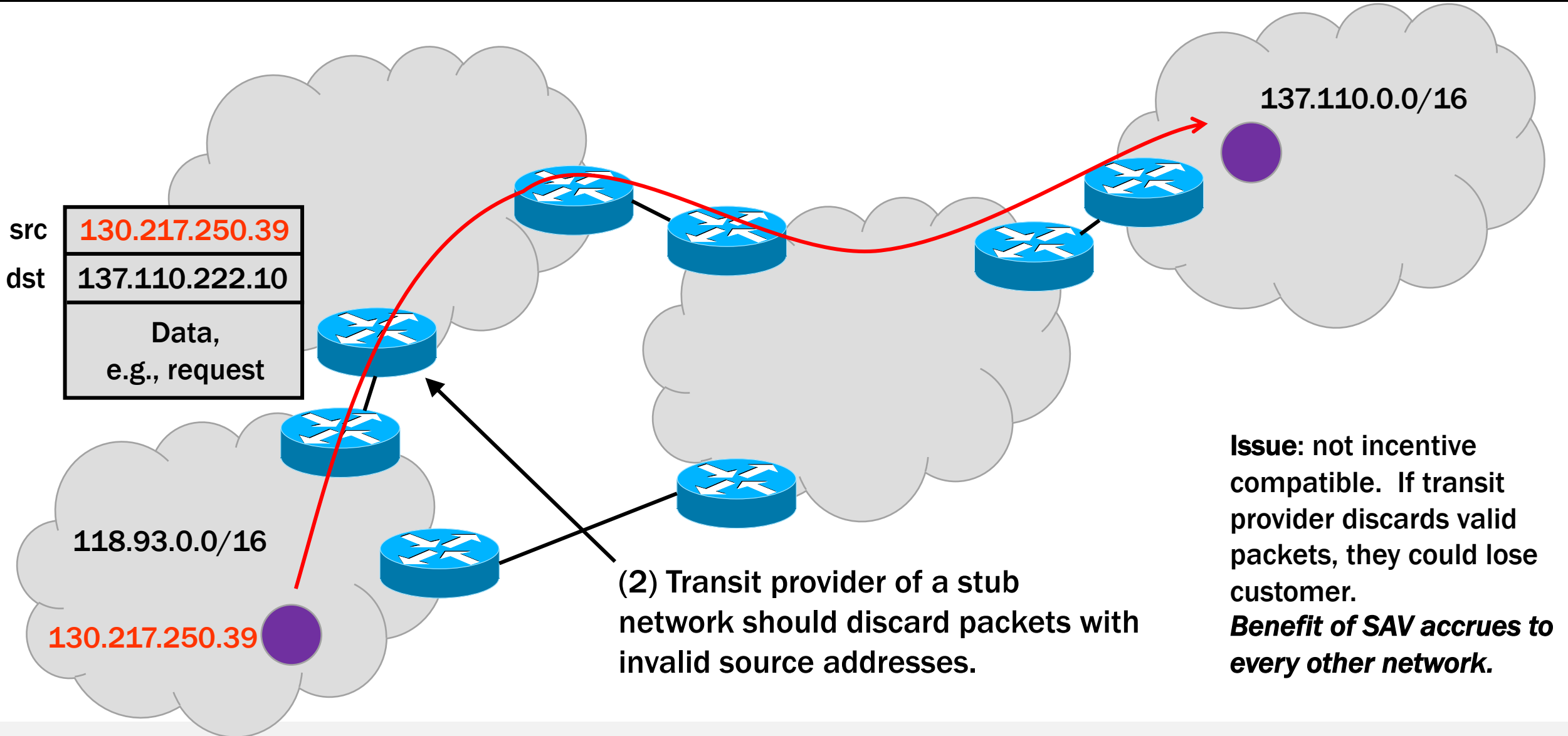
WHAT IS IP SPOOFING?



OUTBOUND SPOOFING

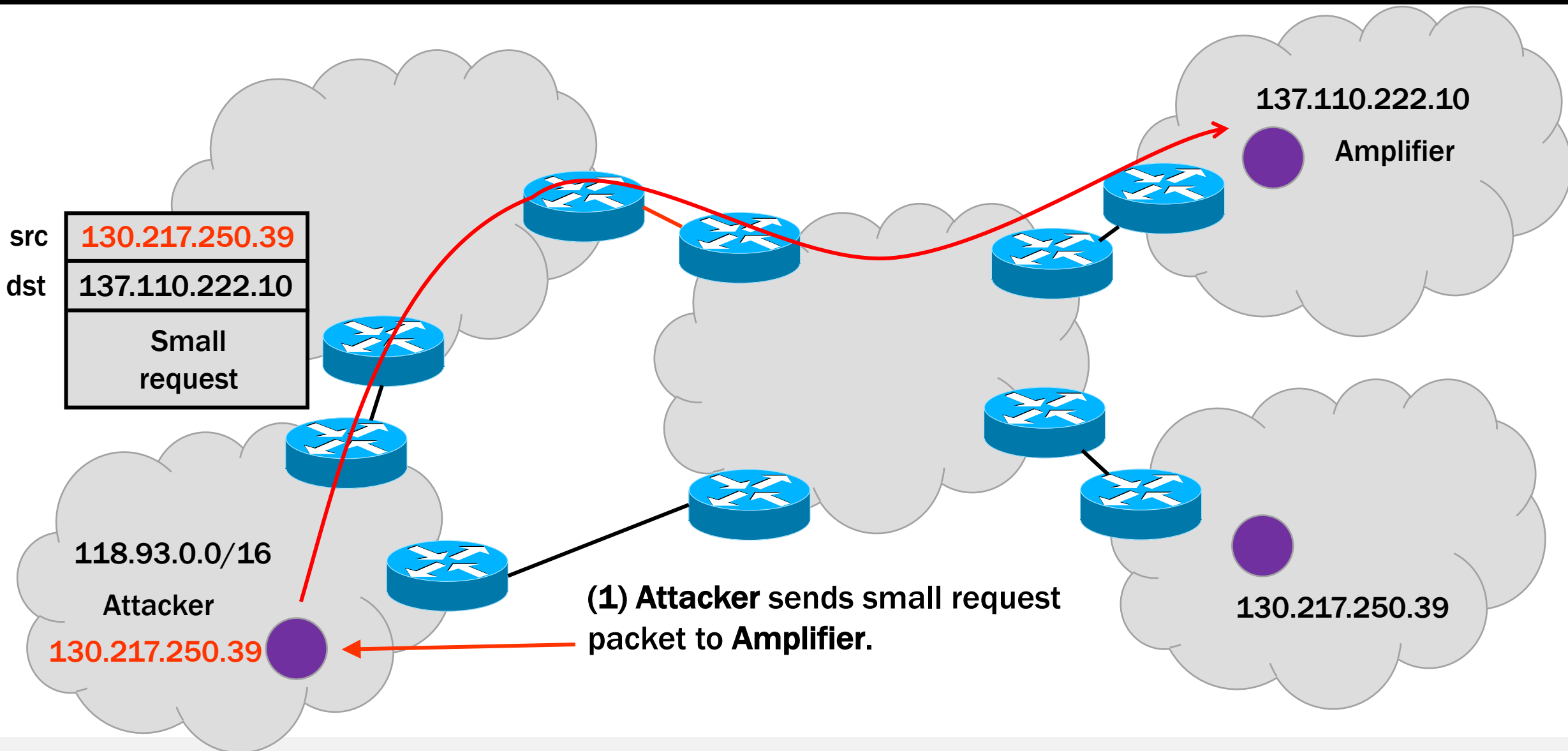
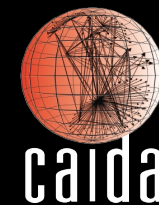


OUTBOUND SPOOFING

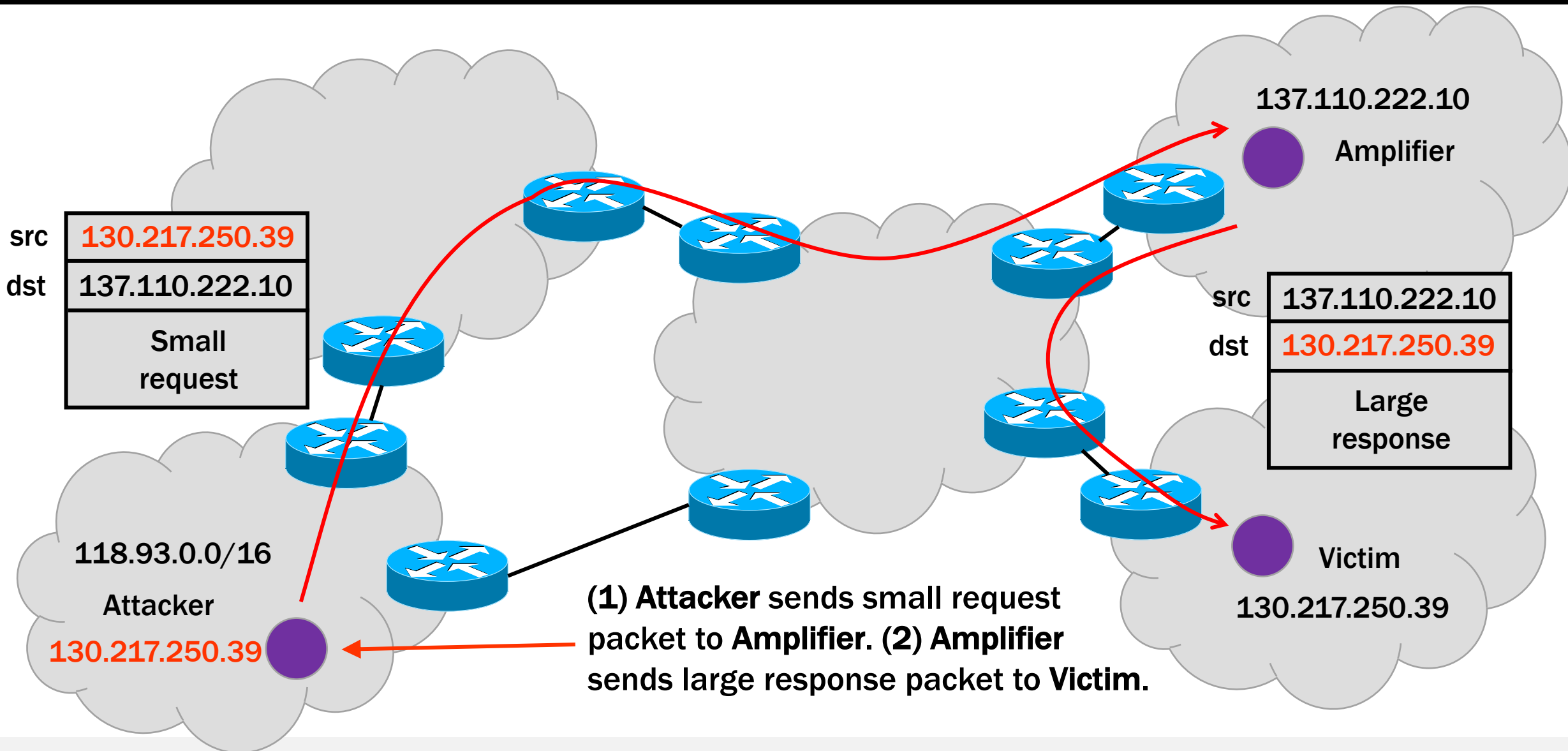
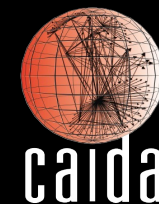


Issue: not incentive compatible. If transit provider discards valid packets, they could lose customer.
Benefit of SAV accrues to every other network.

AMPLIFICATION ATTACKS



AMPLIFICATION ATTACKS



AMPLIFICATION ATTACKS



BIGGEST DDoS ATTACK IN HISTORY hammers Spamhaus

Plucky mail scrubbers battle internet carpet bombers

By [John Leyden](#) 27 Mar 2013 at 17:03

124 SHARE ▼

400Gbps: Winter of Whopping Weekend DDoS Attacks

03/03/2016



Marek Majkowski

How a Massive 540 Gb/sec DDoS Attack Failed to Spoil the Rio Olympics



DAVID BISSON

[Follow @DMBisson](#)

SEP 5, 2016

FEATURED ARTICLES

Gits club GitHub code tub with record-breaking 1.35Tbps DDoS drub

Memcache attacks are going to be this year's thing

By [Iain Thomson](#) in [San Francisco](#) 1 Mar 2018 at 21:10

21 SHARE ▼

DROWNING IN A SEA OF DATA —

Microsoft fend off record-breaking 3.47Tbps DDoS attack

While a crude brute-force attack, DDoSes are growing ever more potent.

DAN GOODIN - 1/29/2022, 12:45 AM

BUILDING A BIGGER DDOS —

New method that amplifies DDoSes by 4 billion-fold. What could go wrong?

New method also stretches out DDoS durations to 14 hours.

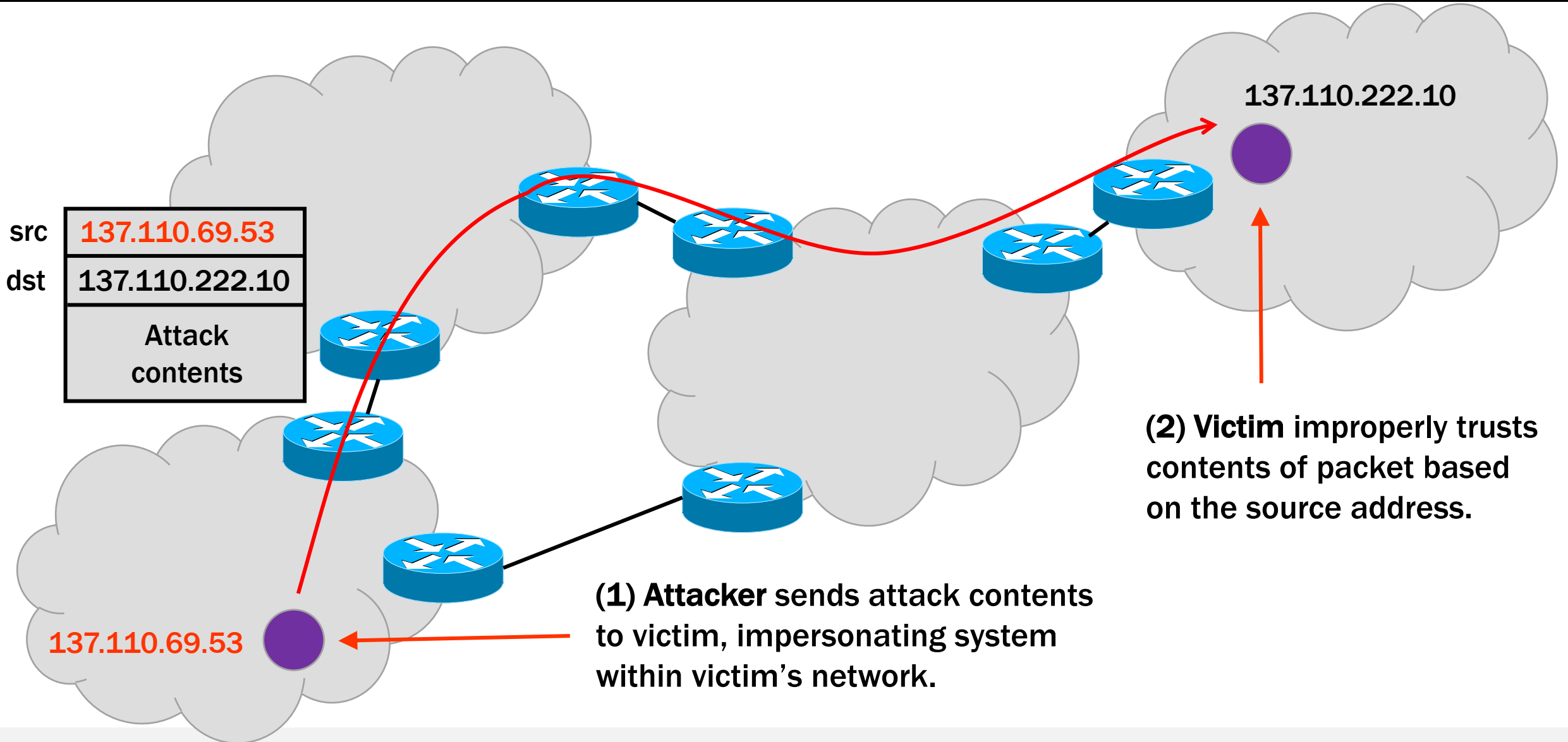
DAN GOODIN - 3/9/2022, 12:15 PM

AMPLIFICATION VECTORS

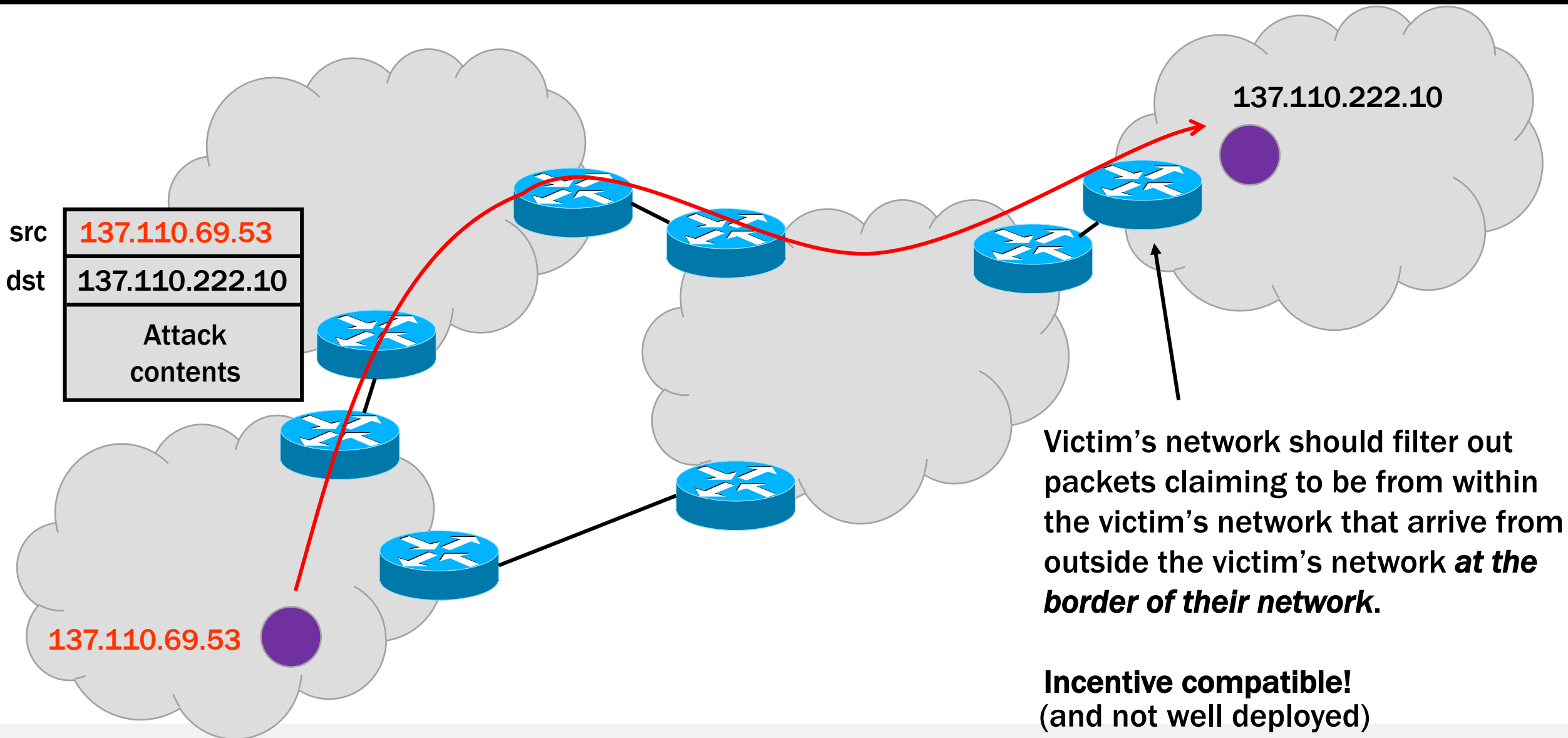
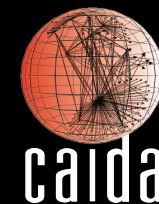


- Amplification attacks tend to use UDP-based request-response protocols without handshake to establish authenticity, e.g.:
 - DNS: send small query, solicit large response (10-20x)
 - NTP: send small 'monlist', solicit large response (>4x) (see "taming the gorilla" paper)
 - memcached: send small GET, solicit large file. (>10000x)
- Protocol designers implementing *cookies* in newer protocols, but hard to retrofit to older protocols.

INBOUND SPOOFING ATTACKS



INBOUND SPOOFING ATTACKS

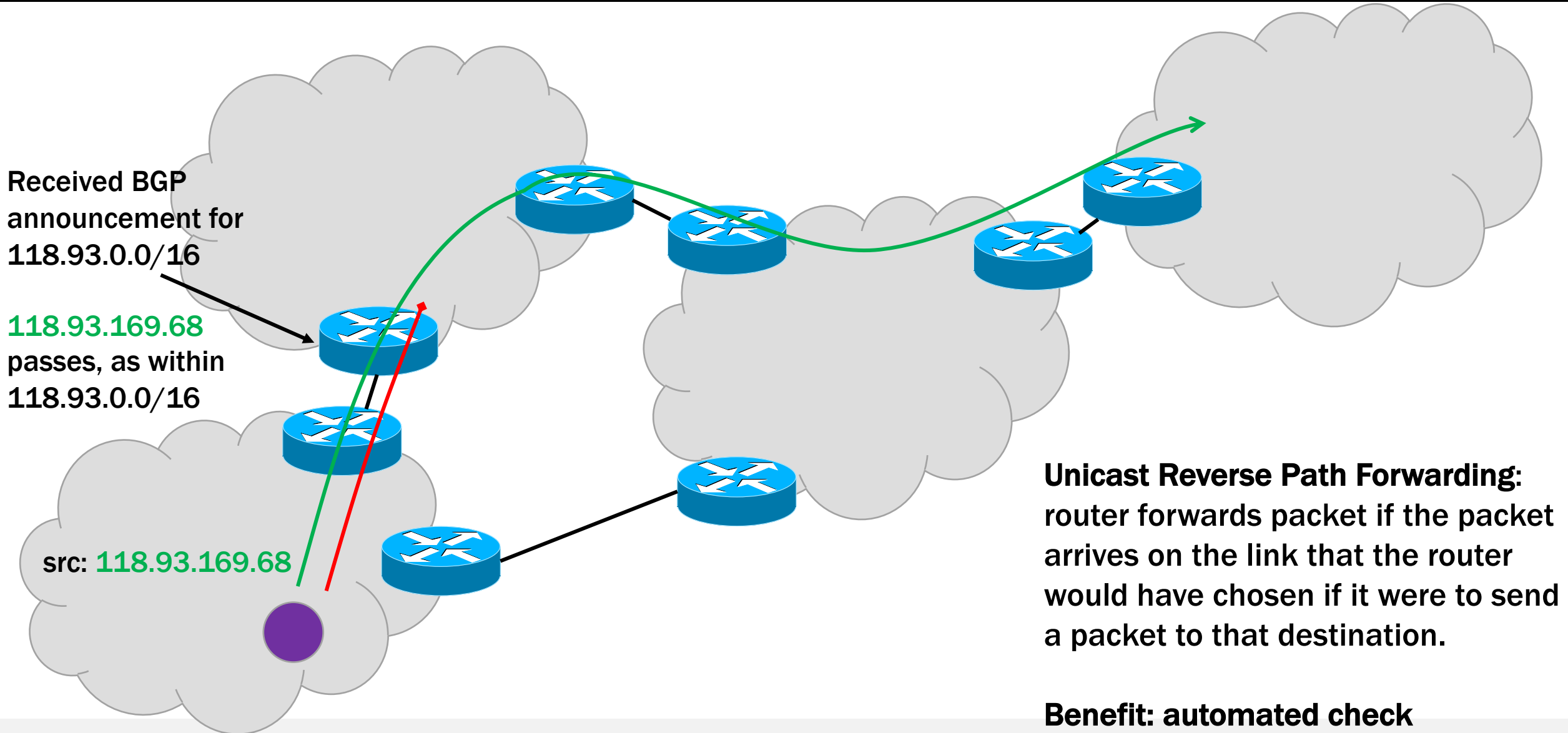


SOURCE ADDRESS VALIDATION

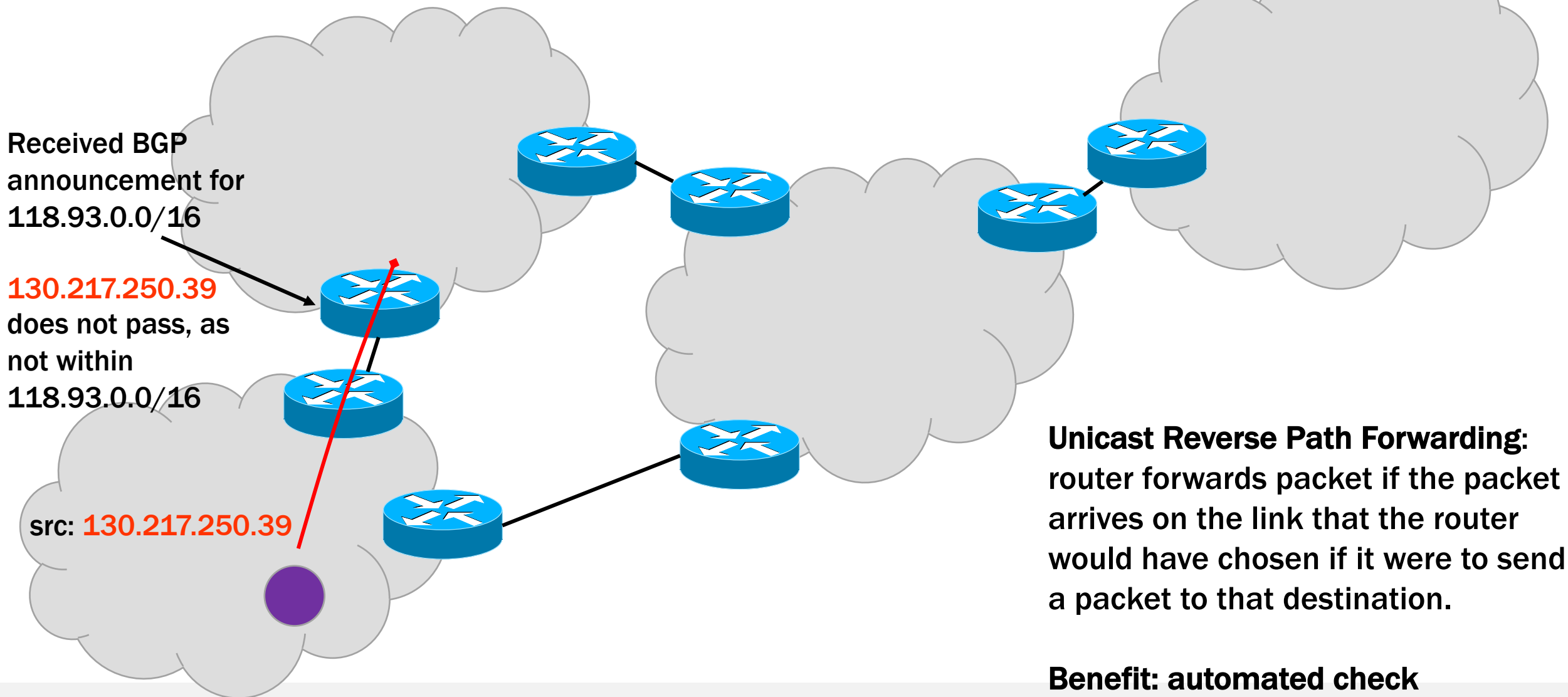
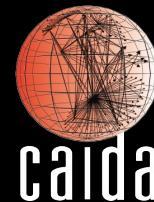


- Also known as SAV
- Goal: filter packets whose source address is not valid given the *attachment point*.
- SAV is only feasible to deploy at the *network edge* because the range of valid addresses at a given router becomes larger the further away that router is from sources that originate traffic.

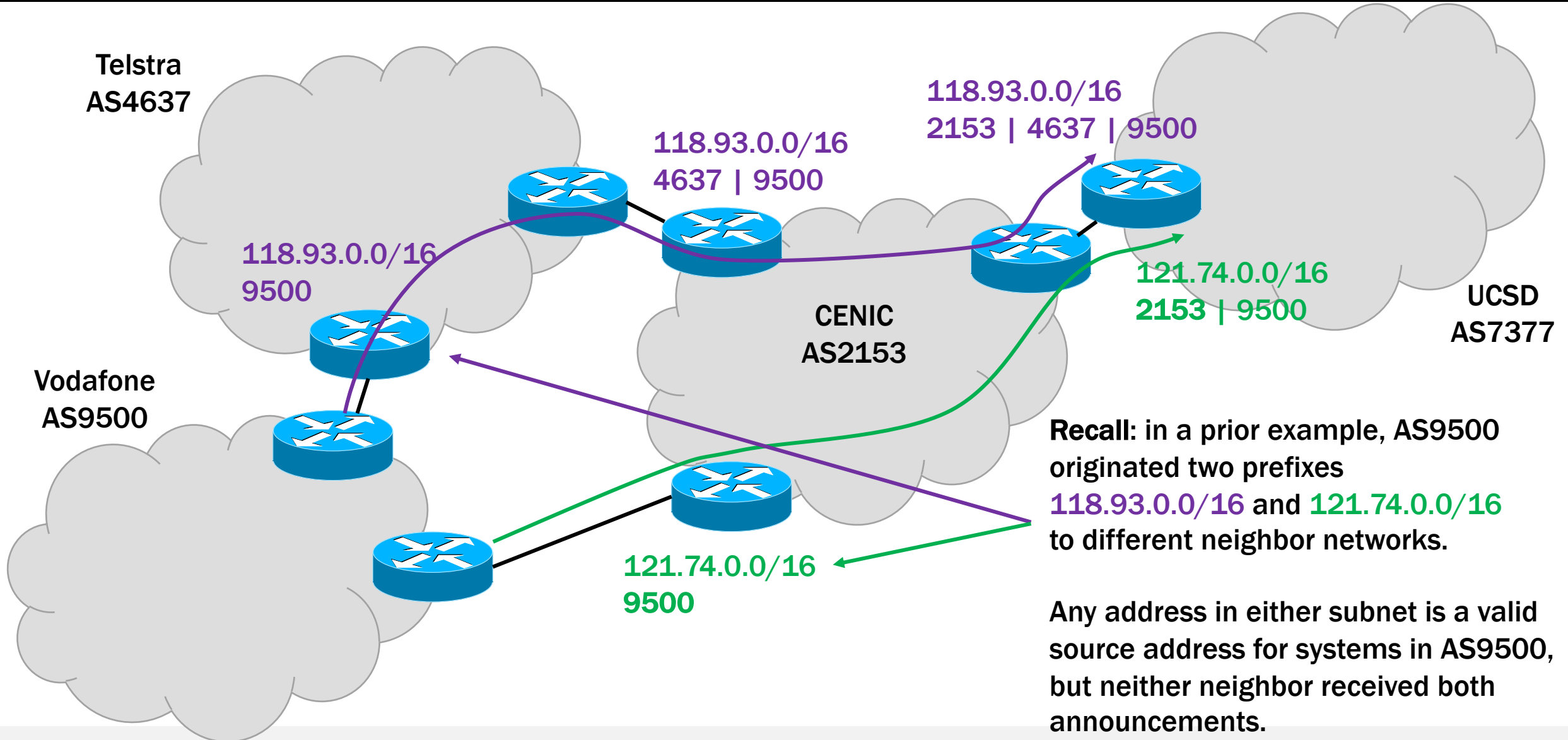
SOLUTION? #1: URPF



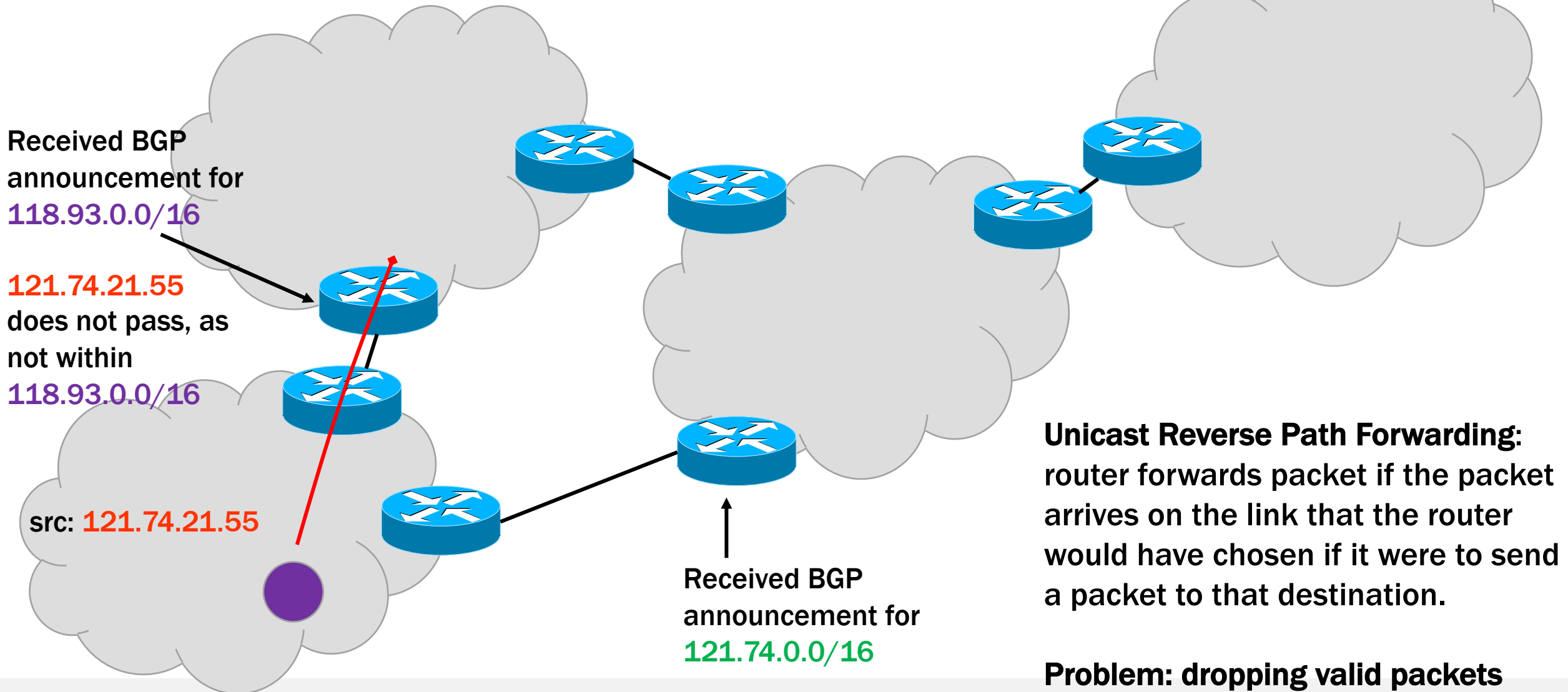
SOLUTION? #1: URPF



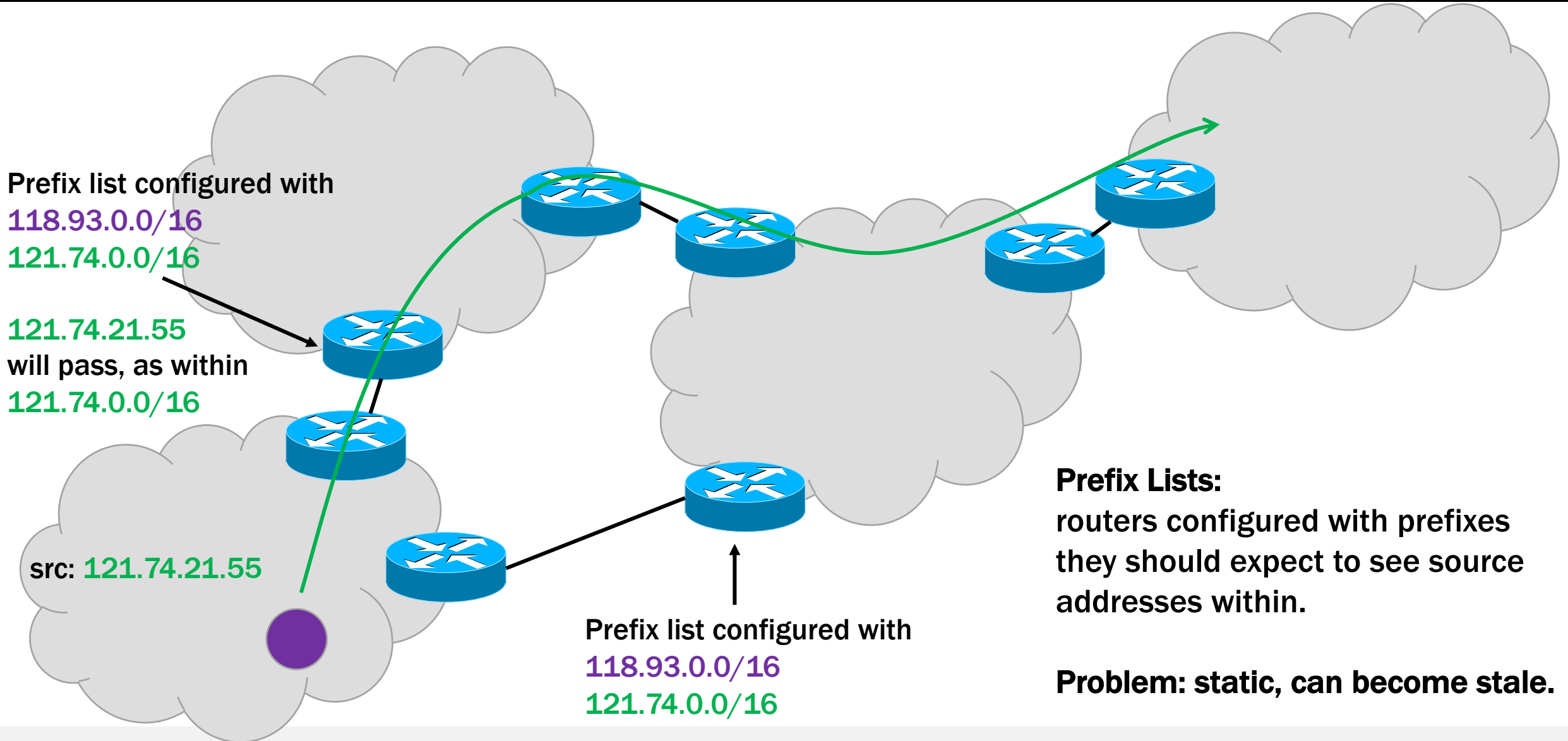
URPF PROBLEM: MULTIHOMING



URPF PROBLEM: MULTIHOMING



SOLUTION? #2: PREFIX LISTS



Prefix Lists:
routers configured with prefixes they should expect to see source addresses within.

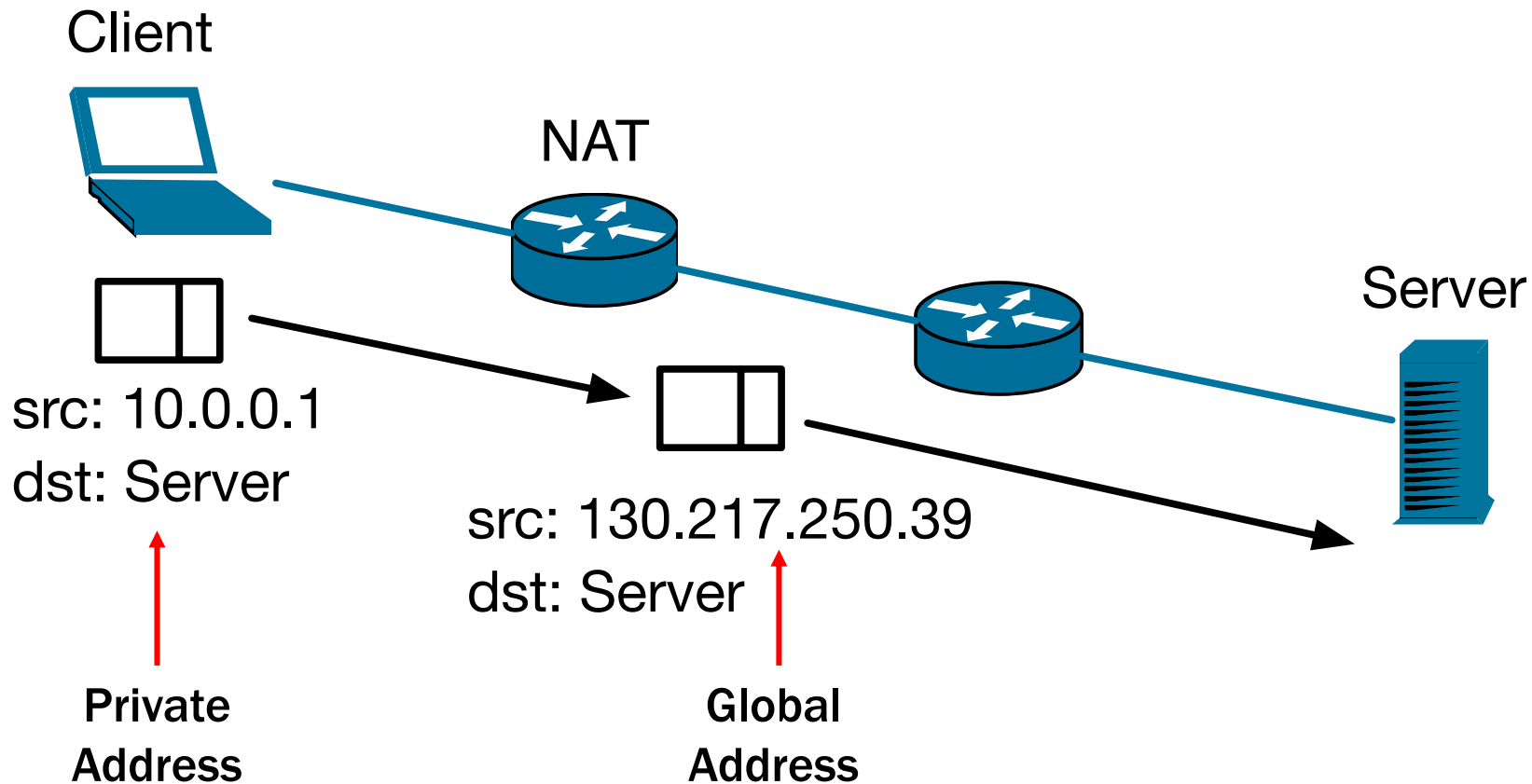
Problem: static, can become stale.

NAT VS. SAV



SAV is different from NAT:

A Network Address Translation (NAT) router modifies the source IP address of forwarded packets

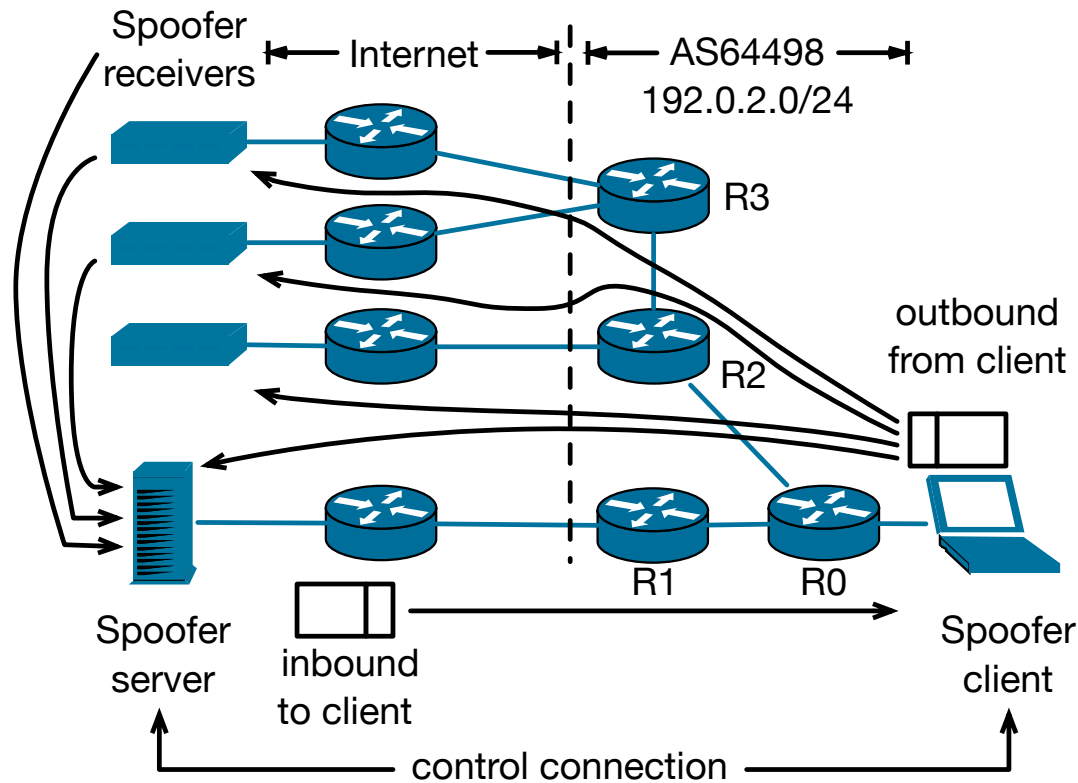


SAV MEASUREMENT ISSUES



- All attempts to study SAV deployment suffer from limited visibility
- *Vantage Point* required in the network to send spoofed packets to determine if the network deployed SAV
- 2023: ~75000 ASes routed on the Internet

THE SPOOFER PROJECT



- We built a measurement infrastructure to support data collection and analysis
 - Crowdsourced collection by volunteers
 - Operators also use our client to check their SAV compliance
 - We continue to operate the platform to study and motivate remediation
 - 2022: tests from ~2300 ASes (3.1%)

<https://spoofer.caida.org/>

SPOOFER PROJECT – CLIENT



Spoof Manager GUI

Scheduler: ready Pause Scheduler

Prober: next scheduled for 2022-09-20 18:35:58 NZST (in about 7 days) Start Tests

Last run: 2022-09-13 17:28:58 NZST

Result history: Hide old blank tests

date	IPv	client address	ASN	outbound private	outbound routable	inbound private	inbound internal	report
2022-09-13 17:28:58	4	118.93.169.166	9500	✓ blocked	✓ blocked			report
	6	2407:7000:9000:ee02::/64	9500	✓ blocked	✓ blocked	✗ received	✗ received	
2022-08-12 12:18:42	4	163.7.134.209		✓ blocked	✓ blocked			report
2022-08-11 12:47:53	4	163.7.137.194	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked	report
	6	2404:138:4011:3e8::/64	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked	

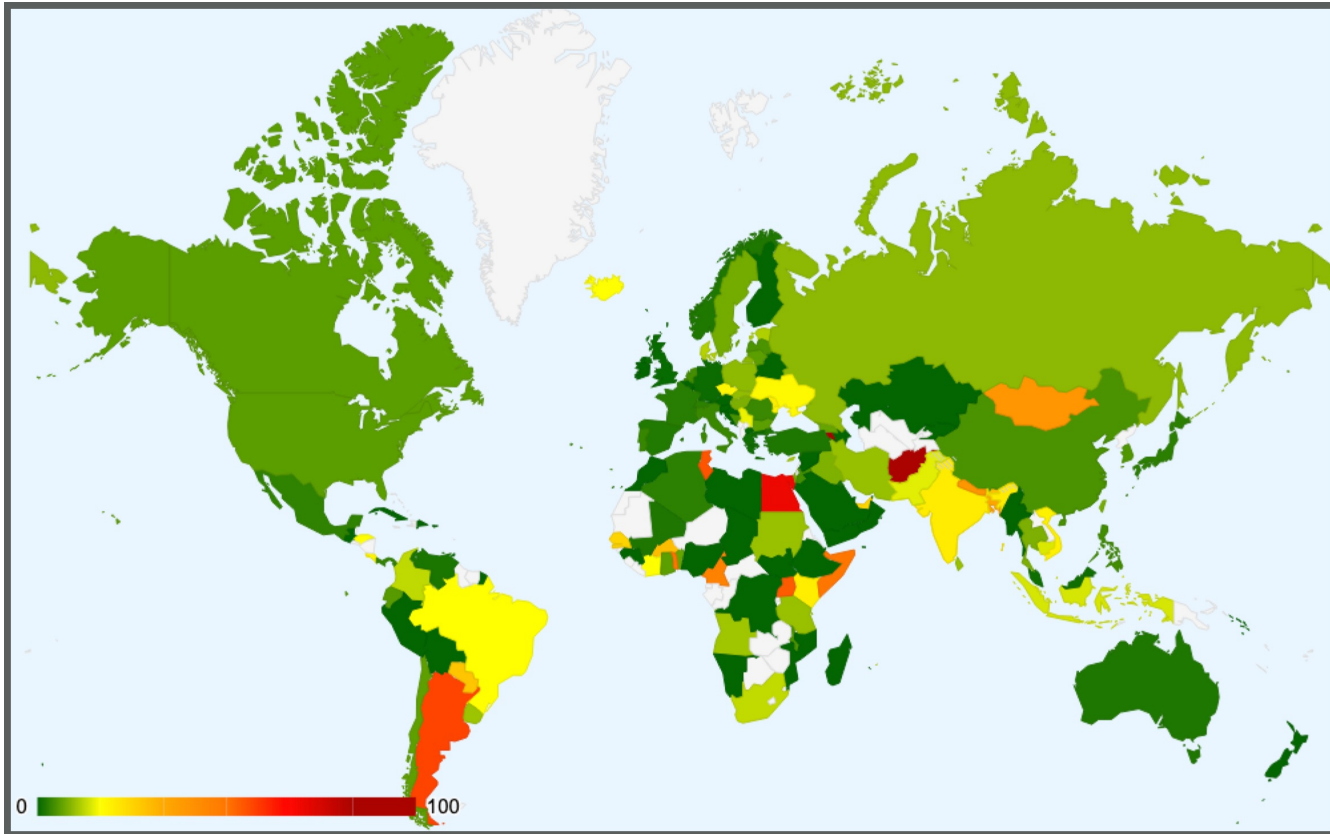
Show Console

**Client with GUI for
Windows, MacOS, and
Linux automatically tests
networks once per week**

Open source: C++

<https://spoofer.caida.org/>

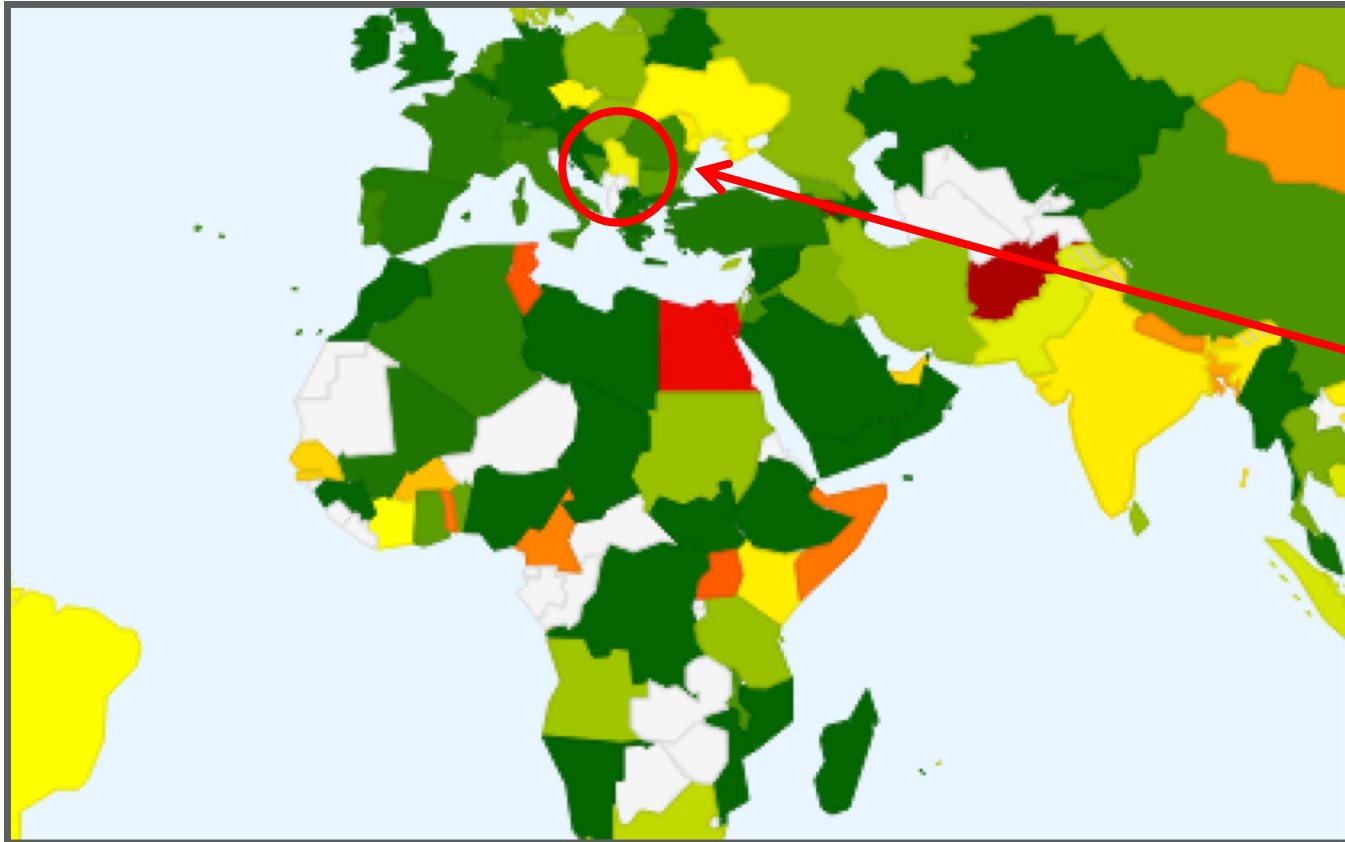
SPOOFER PROJECT – DATA



**We publicly share
anonymized data, in
raw form via an API,
and broken down by
AS and Country**

<https://spoofer.caida.org/>

SPOOFER PROJECT – DATA



**e.g, 15.4% of tested
prefixes in Serbia in
past year did not block
spoofed packets**

<https://spoofer.caida.org/>

SPOOFER PROJECT – DATA



Session	Timestamp (UTC)	Client IP Block	ASN	Country	NAT	Outbound Private Status	Outbound Routable Status	Adj SpooF Prefix Len	Results
1262746	2021-12-02 18:56:06	87.237.203.x/24	51859	srb	no	blocked	blocked	/28	Report
1262746	2021-12-02 18:56:06	2a04:2e40:xx::/40	51859	srb	no	blocked	blocked	/64	Report
1262722	2021-12-02 18:15:06	2a04:2e40:xx::/40	51859	srb	no	blocked	blocked	/64	Report
1262628	2021-12-02 14:38:04	91.222.5.x/24	51859	srb	no	blocked	blocked	/28	Report
1262628	2021-12-02 14:38:04	2a04:2e40:xx::/40	51859	srb	no	blocked	blocked	/64	Report
1262609	2021-12-02 14:13:13	91.222.4.x/24	51859	srb	yes	blocked	✓ blocked	none	Report
1262607	2021-12-02 14:08:53	91.222.4.x/24	51859	srb	yes	blocked	✓ received	/8	Report
1262541	2021-12-02 12:17:00							none	Report
1262244	2021-12-01 23:12:00							none	Report
1262068	2021-12-01 17:20:00							none	Report
1255912	2021-11-24 22:05:00							none	Report

We publicly show fine-grained outcomes of recent tests, anonymizing Client IP Blocks, if user has not configured client to not show results publicly

<https://spoofer.caida.org/>

SPOOFER PROJECT – DATA



Session	Timestamp (UTC)	Client IP Block	ASN	Country	NAT	Outbound Private	Outbound Routable	Adj SpooF Prefix Len	Results	
1262746	2021-12-02 18:56:06	87.237.203.x/24	Addresses anonymized: IPv4: /24 IPv6: /40				blocked	us	/28	Report
1262746	2021-12-02 18:56:06	2a04:2e40:xx::/40					blocked		/64	Report
1262722	2021-12-02 18:15:06	2a04:2e40:xx::/40					blocked		/64	Report
1262628	2021-12-02 14:38:04	91.222.5.x/24	51859	srb	no	blocked	blocked	/28	Report	
1262628	2021-12-02 14:38:04	2a04:2e40:xx::/40	51859	srb	no	blocked	blocked	/64	Report	
1262609	2021-12-02 14:13:13	91.222.4.x/24	51859	srb	yes	blocked	✓ blocked	none	Report	
1262607	2021-12-02 14:08:53	91.222.4.x/24	51859	srb	yes	blocked	✓ received	/8	Report	
1262541	2021-12-02 12:17:07	87.116.172.x/24	31042	srb	yes	rewritten	rewritten	none	Report	
1262244	2021-12-01 23:12:16	93.87.27.x/24	8400	srb	yes	rewritten	received	none	Report	
1262068	2021-12-01 17:20:17	82.214.94.x/24	25467	srb	yes	blocked	blocked	none	Report	
1255912	2021-11-24 22:05:49	93.87.27.x/24	8400	srb	yes	rewritten	received	none	Report	

<https://spoofer.caida.org/>

SPOOFER PROJECT – DATA



Session	Timestamp (UTC)	Client IP Block	ASN	Country	NAT	Outbound Private Status	Outbound Routable Status	Adj SpooF Prefix Len	Results
1262746	2021-12-02 18:56:06	87.23							Report
1262746	2021-12-02 18:56:06	2a04							Report
1262722	2021-12-02 18:15:06	2a04							Report
1262628	2021-12-02 14:38:04	91.22							Report
1262628	2021-12-02 14:38:04	2a04							Report
1262609	2021-12-02 14:13:13	91.222.4.x/24	51859	srb	yes	blocked	✓ blocked	none	Report
1262607	2021-12-02 14:08:53	91.222.4.x/24	51859	srb	yes	blocked	✓ received	/8	Report
1262541	2021-12-02 12:17:07	87.116.172.x/24	31042	srb	yes	rewritten	rewritten	none	Report
1262244	2021-12-01 23:12:16	93.87.27.x/24	8400	srb	yes	rewritten	received	none	Report
1262068	2021-12-01 17:20:17	82.214.94.x/24	25467	srb	yes	blocked	blocked	none	Report
1255912	2021-11-24 22:05:49	93.87.27.x/24	8400	srb	yes	rewritten	received	none	Report

NATs behave differently:
 Some may block spoofed traffic
 Some uselessly rewrite
 Some do not rewrite and pass spoofed packets

<https://spoofer.caida.org/>

SPOOFER PROJECT – DATA



Session	Timestamp (UTC)	Client IP Block	ASN	Country	NAT	Outbound Private Status	Outbound Routable Status	Adj SpooF Prefix Len	Results	
1262746	2021-12-02 18:56:06	87.237.203.x/24	51859	srb	no	blocked	blocked	/28	Report	
1262746	2021-12-02	<div style="border: 1px dashed black; padding: 5px; text-align: center;"> <p>Our client evaluates the source addresses in the widest prefix that the network will forward</p> </div>						→	/64	Report
1262722	2021-12-02							→	/64	Report
1262628	2021-12-02							→	/28	Report
1262628	2021-12-02 14:38:04							2a04:2e40:xx::/40	51859	srb
1262609	2021-12-02 14:13:13	91.222.4.x/24	51859	srb	yes	blocked	✓ blocked	none	Report	
1262607	2021-12-02 14:08:53	91.222.4.x/24	51859	srb	yes	blocked	✓ received	/8	Report	
1262541	2021-12-02 12:17:07	87.116.172.x/24	31042	srb	yes	rewritten	rewritten	none	Report	
1262244	2021-12-01 23:12:16	93.87.27.x/24	8400	srb	yes	rewritten	received	none	Report	
1262068	2021-12-01 17:20:17	82.214.94.x/24	25467	srb	yes	blocked	blocked	none	Report	
1255912	2021-11-24 22:05:49	93.87.27.x/24	8400	srb	yes	rewritten	received	none	Report	

<https://spoofer.caida.org/>

SPOOFER PROJECT – DATA



Session	Timestamp (UTC)	Client IP Block	ASN	Country	NAT	Outbound Private Status	Outbound Routable Status	Adj SpooF Prefix Len	Results
1262746	2021-12-02 18:56:06	87.237.203.x/24	51859	srb	no	blocked	blocked	/28	Report
1262746	2021-12-02 18:56:06	2a04:2e40:xx::/40	51859	srb	no	blocked	blocked	/64	Report
1262722	2021-12-02 18:56:06	2a04:2e40:xx::/40	51859	srb	no	blocked	blocked	/64	Report
1262628	2021-12-02 18:56:06	2a04:2e40:xx::/40	51859	srb	no	blocked	blocked	/28	Report
1262628	2021-12-02 18:56:06	2a04:2e40:xx::/40	51859	srb	no	blocked	blocked	/64	Report
1262609	2021-12-02 14:13:13	91.222.4.x/24	51859	srb	yes	blocked	✓ blocked	none	Report
1262607	2021-12-02 14:08:53	91.222.4.x/24	51859	srb	yes	blocked	✓ received	/8	Report
1262541	2021-12-02 12:17:07	87.116.172.x/24	31042	srb	yes	rewritten	rewritten	none	Report
1262244	2021-12-01 23:12:16	93.87.27.x/24	8400	srb	yes	rewritten	received	none	Report
1262068	2021-12-01 17:20:17	82.214.94.x/24	25467	srb	yes	blocked	blocked	none	Report
1255912	2021-11-24 22:05:49	93.87.27.x/24	8400	srb	yes	rewritten	received	none	Report

Some networks go from forwarding spoofed packets to blocking them (green ticks)

<https://spoofer.caida.org/>

SPOOFER PROJECT – API



Spoofers API 1.0.0

[Base URL: /]

Session ⌵

GET /sessions Retrieves the collection of Session resources.

Parameters Cancel

Name	Description
timestamp[before] string (query)	<input type="text" value="timestamp[before]"/>
timestamp[strictly_before] string (query)	<input type="text" value="timestamp[strictly_before]"/>

- CAIDA provides an API that allows the public to query our data, receiving JSON responses
- Your first assignment uses the API to conduct analyses

<https://www.caida.org/projects/spoofers/data-api/>

MANRS



- Mutually Assured Norms for Routing Security
- ISOC-led effort to encourage deployment of various best practices (SAV, RPKI, correct contact information)
- Participants publicly *aspire* to deploy best practices
- Your first assignment examines MANRS participant deployment of SAV using spoofer project data.

<https://www.manrs.org/>