

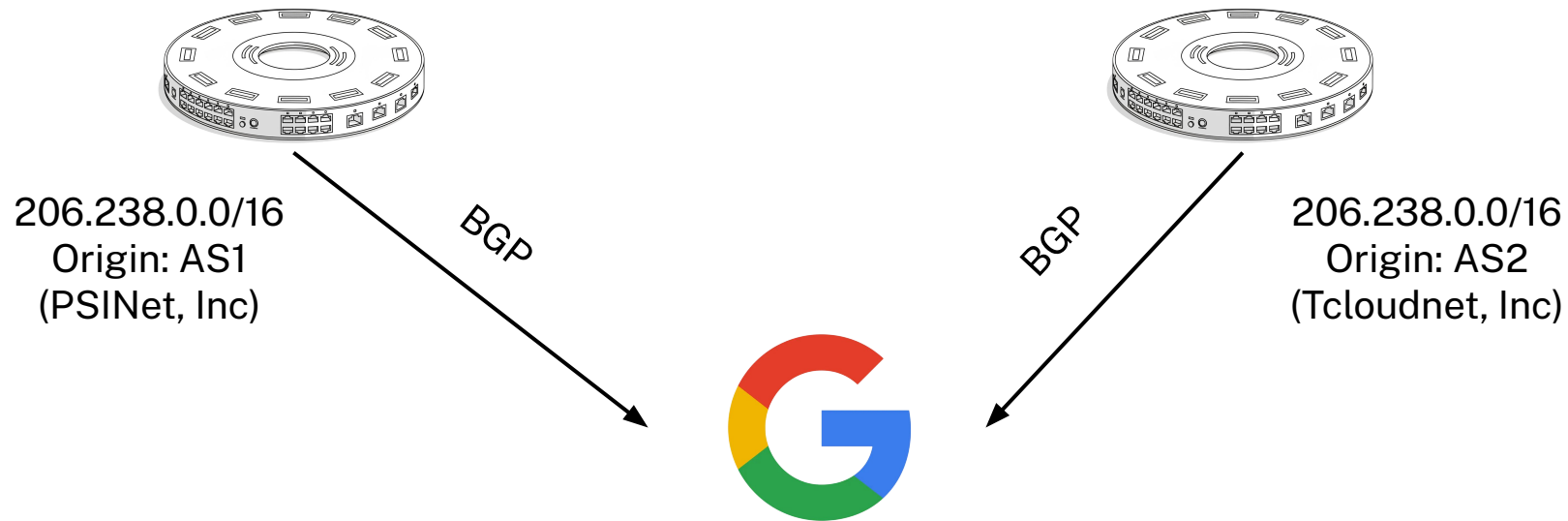
Prefix2Org

Finding Owners of IP Address Space

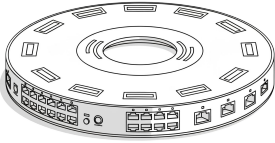
Deepak Gouda, Alberto Dainotti, Cecilia Testart

CS PhD, Georgia Institute of Technology

Aug 7, 2025

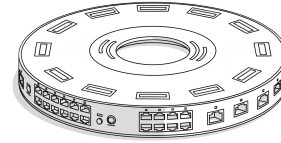


Malicious Hijack or
Misconfiguration?



206.238.0.0/16
Origin: AS1
(PSINet, Inc)

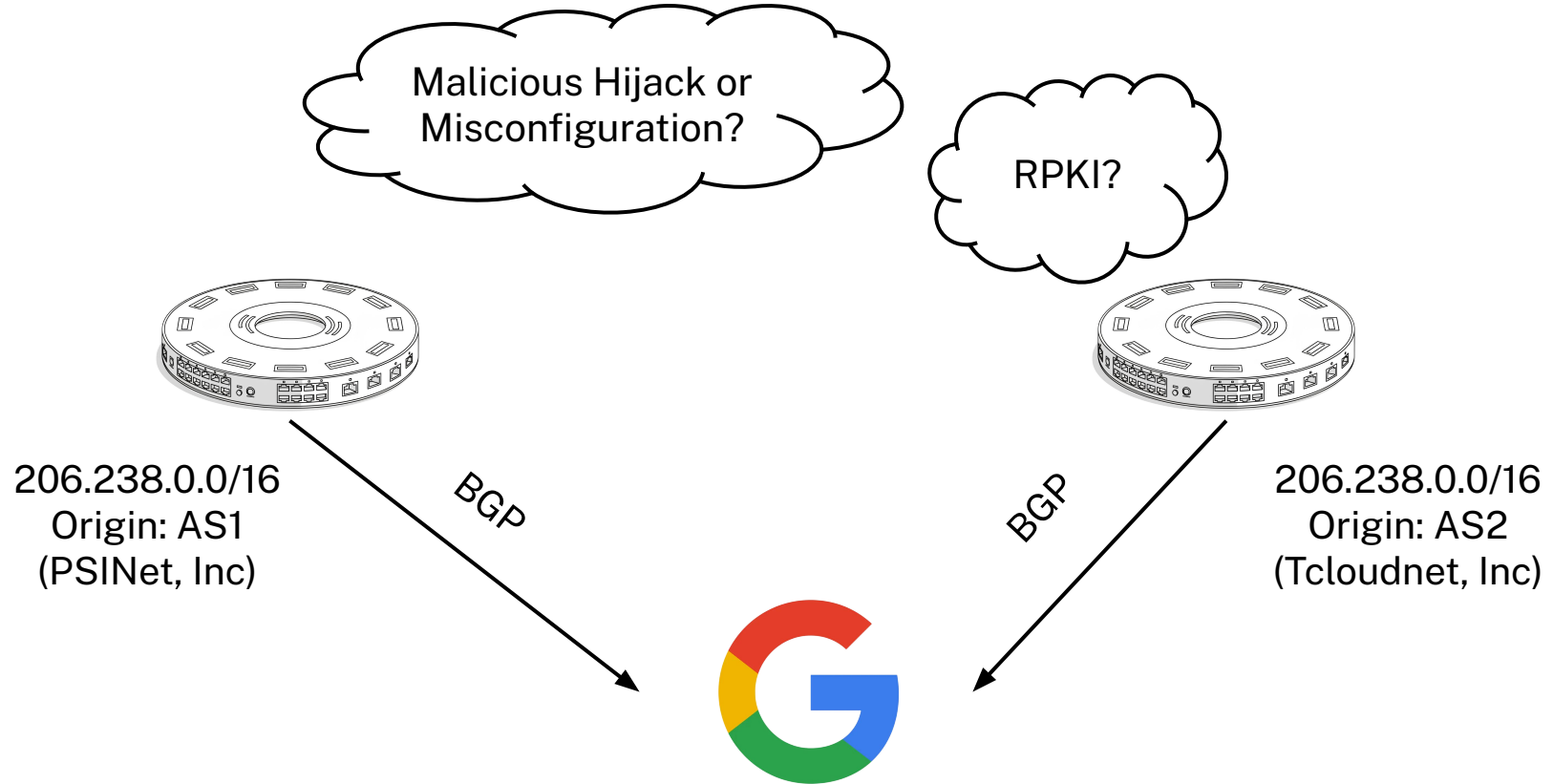
BGP

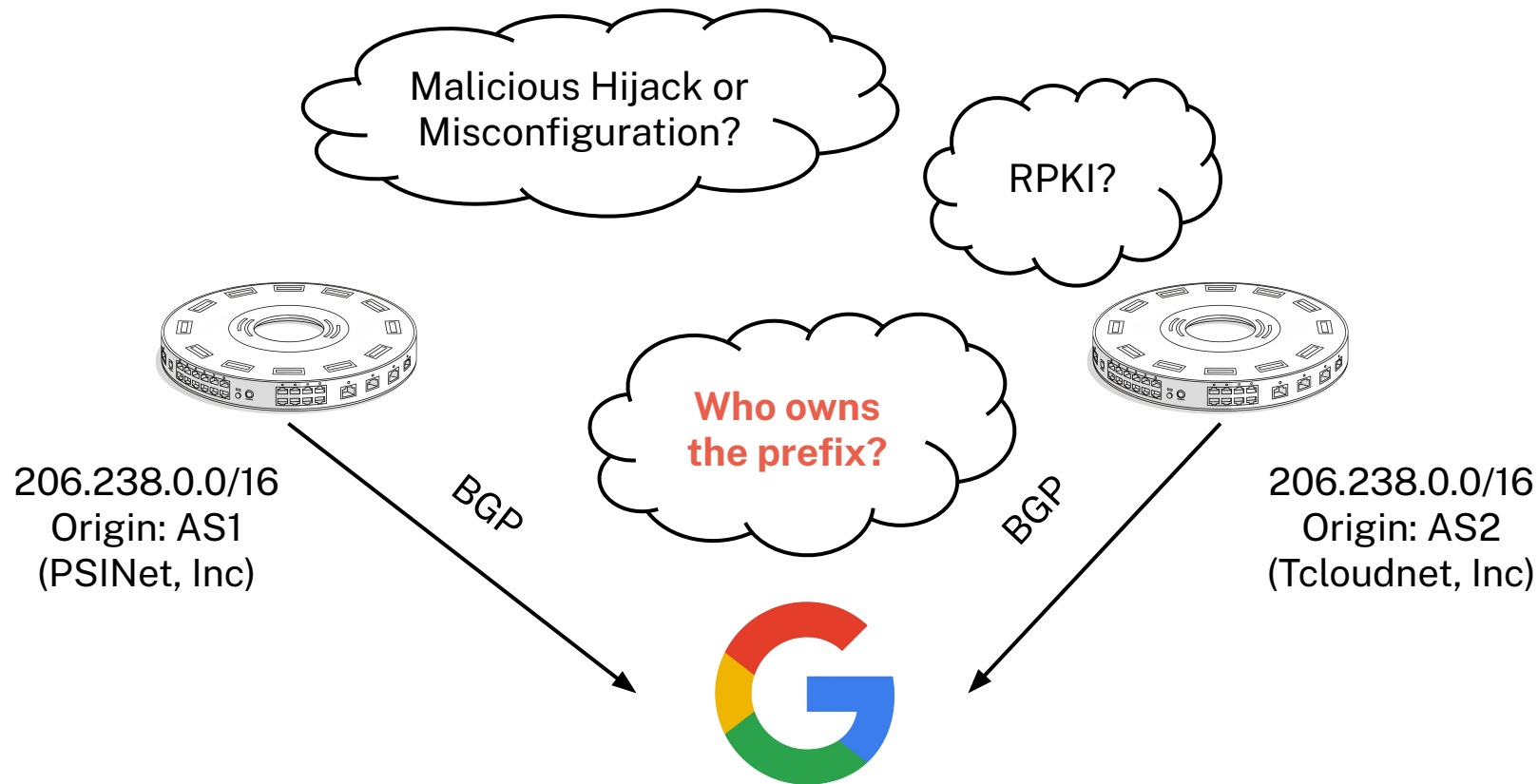


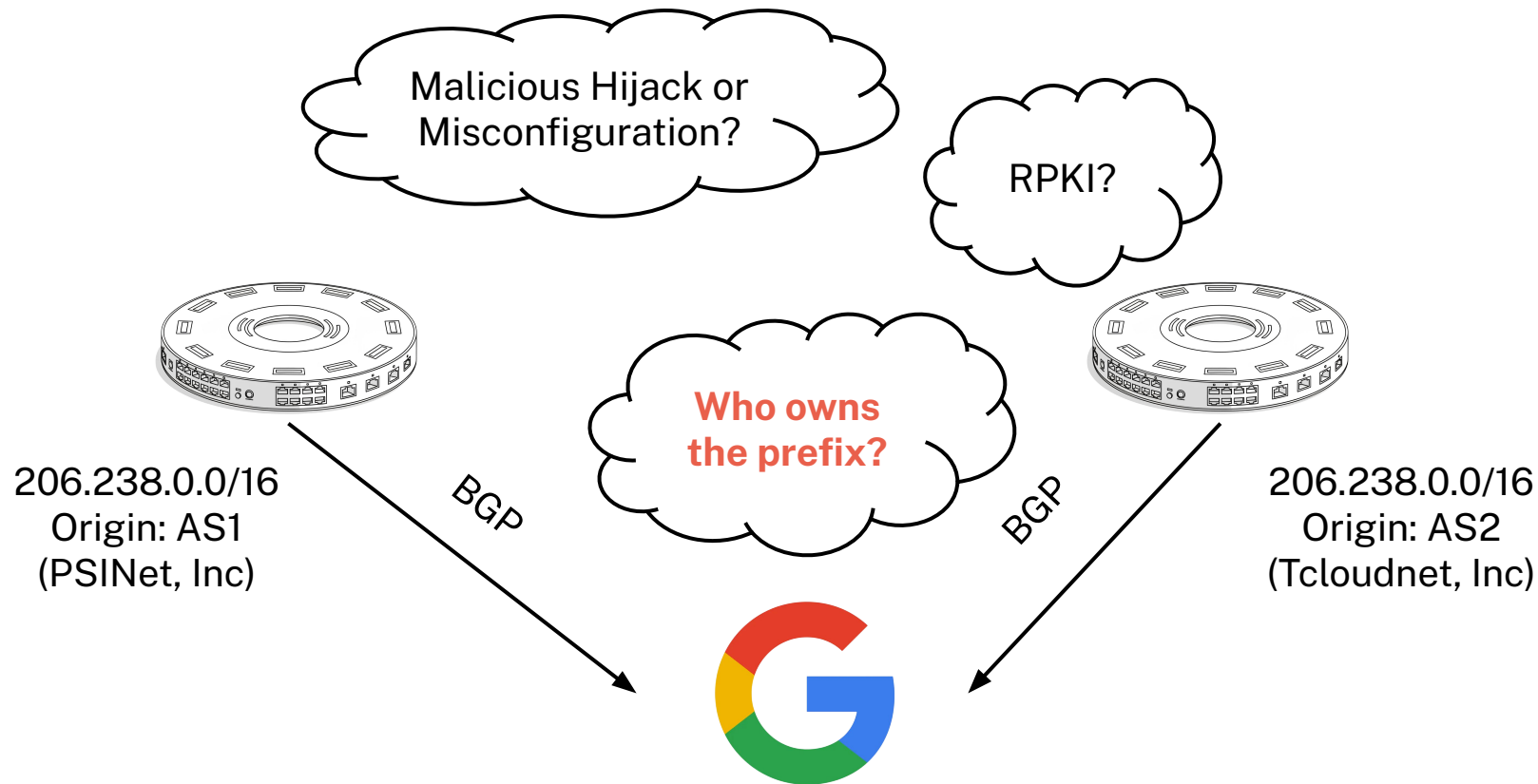
206.238.0.0/16
Origin: AS2
(Tcloudnet, Inc)

BGP





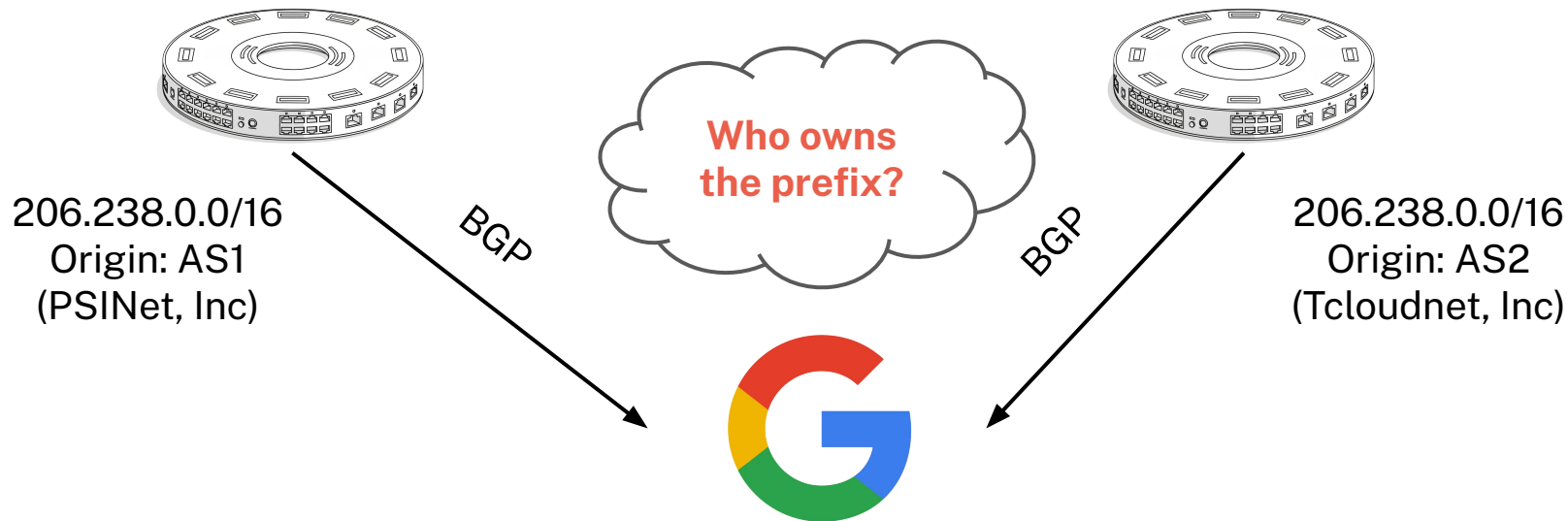




Note: BGP Origin \nRightarrow Ownership!

NetRange	206.232.0.0 - 206.238.255.255
CIDR	206.238.0.0/16, 206.236.0.0/15, 206.232.0.0/14
NetType	Direct Allocation
Organization	PSINet, Inc. (PSI)
RegDate	1995-11-06
source	ARIN

NetRange	206.238.0.0 - 206.238.255.255
CIDR	206.238.0.0/16
NetType	Reassigned
Organization	Tcloudnet, Inc (C09815123)
RegDate	2023-07-14
source	ARIN



Note: BGP Origin \nRightarrow Ownership!

Question

- Why do we have two (valid) WHOIS records for the same prefix?
- Who actually “owns” prefix 206.238.0.0/16?

Part I: Ownership

Focusing on Ownership

NetRange	206.232.0.0 - 206.238.255.255
CIDR	206.238.0.0/16, 206.236.0.0/15, 206.232.0.0/14
NetType	Direct Allocation
Organization	PSINet, Inc. (PSI)
RegDate	1995-11-06
source	ARIN

NetRange	206.238.0.0 - 206.238.255.255
CIDR	206.238.0.0/16
NetType	Reassigned
Organization	Tcloudnet, Inc (C09815123)
RegDate	2023-07-14
source	ARIN

Focusing on Ownership

NetRange	206.232.0.0 - 206.238.255.255
CIDR	206.238.0.0/16, 206.236.0.0/15, 206.232.0.0/14
NetType	Direct Allocation
Organization	PSINet, Inc. (PSI)
RegDate	1995-11-06
source	ARIN

NetRange	206.238.0.0 - 206.238.255.255
CIDR	206.238.0.0/16
NetType	Reassigned
Organization	Tcloudnet, Inc (C09815123)
RegDate	2023-07-14
source	ARIN

Q. What is NetType?

Focusing on Ownership

NetRange	206.232.0.0 - 206.238.255.255
CIDR	206.238.0.0/16, 206.236.0.0/15, 206.232.0.0/14
NetType	Direct Allocation
Organization	PSINet, Inc. (PSI)
RegDate	1995-11-06
source	ARIN

NetRange	206.238.0.0 - 206.238.255.255
CIDR	206.238.0.0/16
NetType	Reassigned
Organization	Tcloudnet, Inc (C09815123)
RegDate	2023-07-14
source	ARIN

Q. What is NetType?

A. Allocation type of the address; indicates usage rights

Focusing on Ownership

NetRange	206.232.0.0 - 206.238.255.255
CIDR	206.238.0.0/16, 206.236.0.0/15, 206.232.0.0/14
NetType	Direct Allocation
Organization	PSINet, Inc. (PSI)
RegDate	1995-11-06
source	ARIN

NetRange	206.238.0.0 - 206.238.255.255
CIDR	206.238.0.0/16
NetType	Reassigned
Organization	Tcloudnet, Inc (C09815123)
RegDate	2023-07-14
source	ARIN

Q. What is NetType?

A. Allocation type of the address; indicates usage rights

Q. How many allocation types exist?

Focusing on Ownership

NetRange	206.232.0.0 - 206.238.255.255
CIDR	206.238.0.0/16, 206.236.0.0/15, 206.232.0.0/14
NetType	Direct Allocation
Organization	PSINet, Inc. (PSI)
RegDate	1995-11-06
source	ARIN

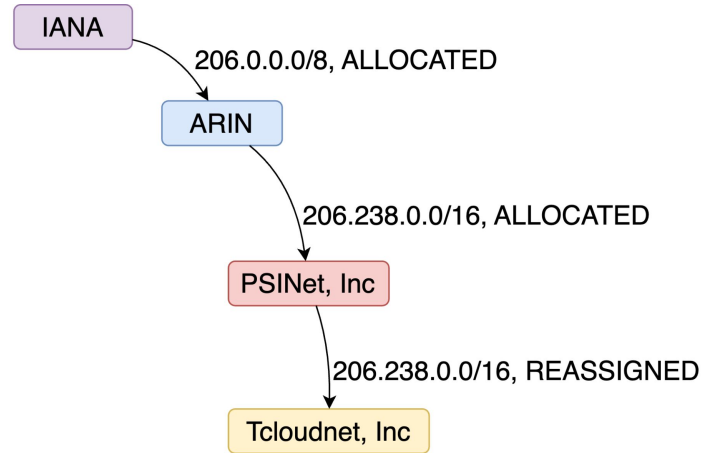
NetRange	206.238.0.0 - 206.238.255.255
CIDR	206.238.0.0/16
NetType	Reassigned
Organization	Tcloudnet, Inc (C09815123)
RegDate	2023-07-14
source	ARIN

Q. What is NetType?

A. Allocation type of the address; indicates usage rights

Q. How many allocation types exist?

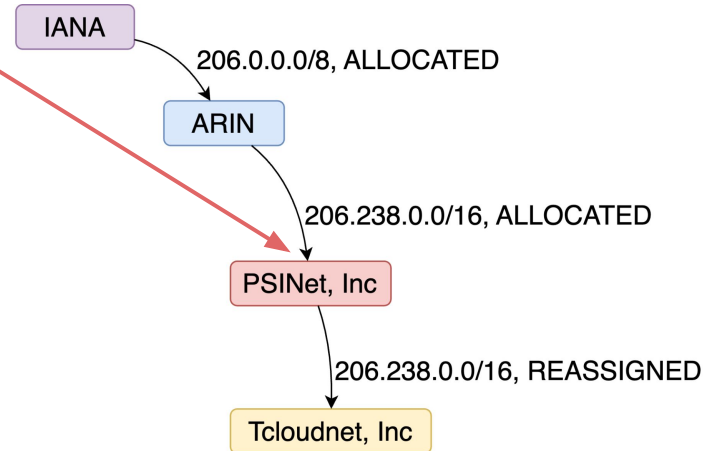
A. Over 20 types across the five RIRs



Direct Allocation from the RIR

PSINet, Inc can

- Use any upstream provider
- Further delegate the address block
- Issue RPKI records



Direct Allocation from the RIR

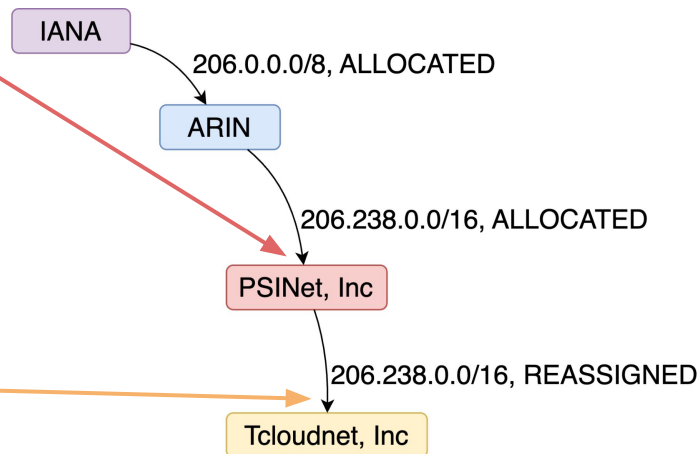
PSINet, Inc can

- Use any upstream provider
- Further delegate the address block
- Issue RPKI records

Delegation from PSINet, Inc

Tcloudnet, Inc

- Hosts services on the addresses
- Is expected to get connectivity from PSINet
- Might not have an ASN too!



Allocated
Assigned

·
·
·

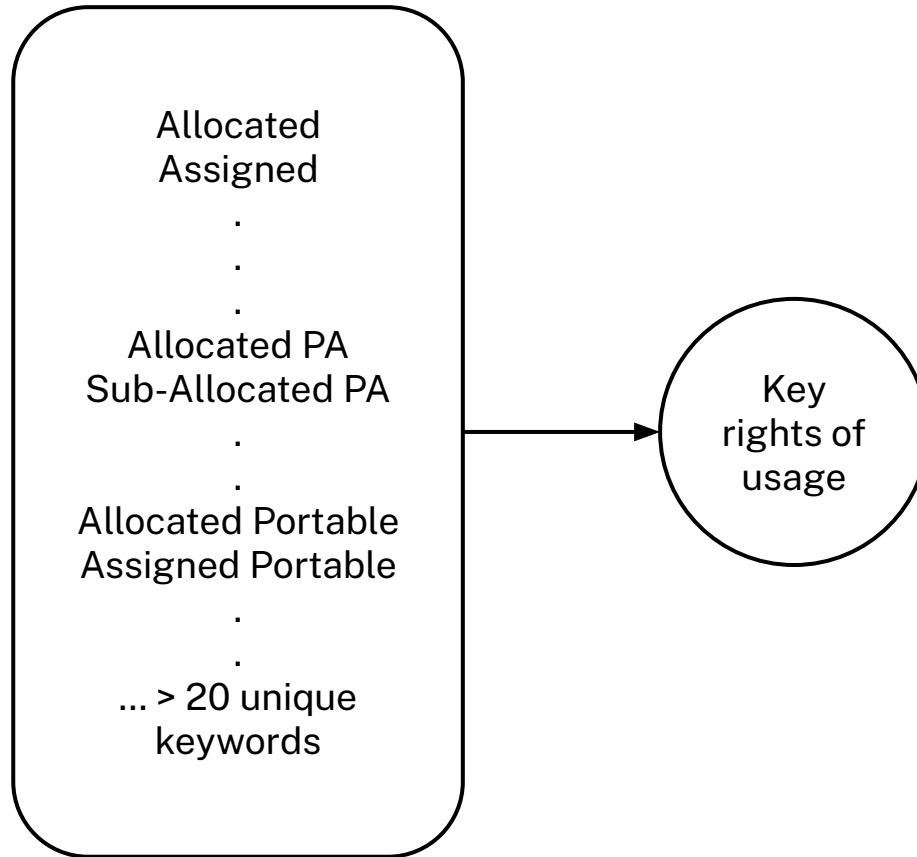
Allocated PA
Sub-Allocated PA

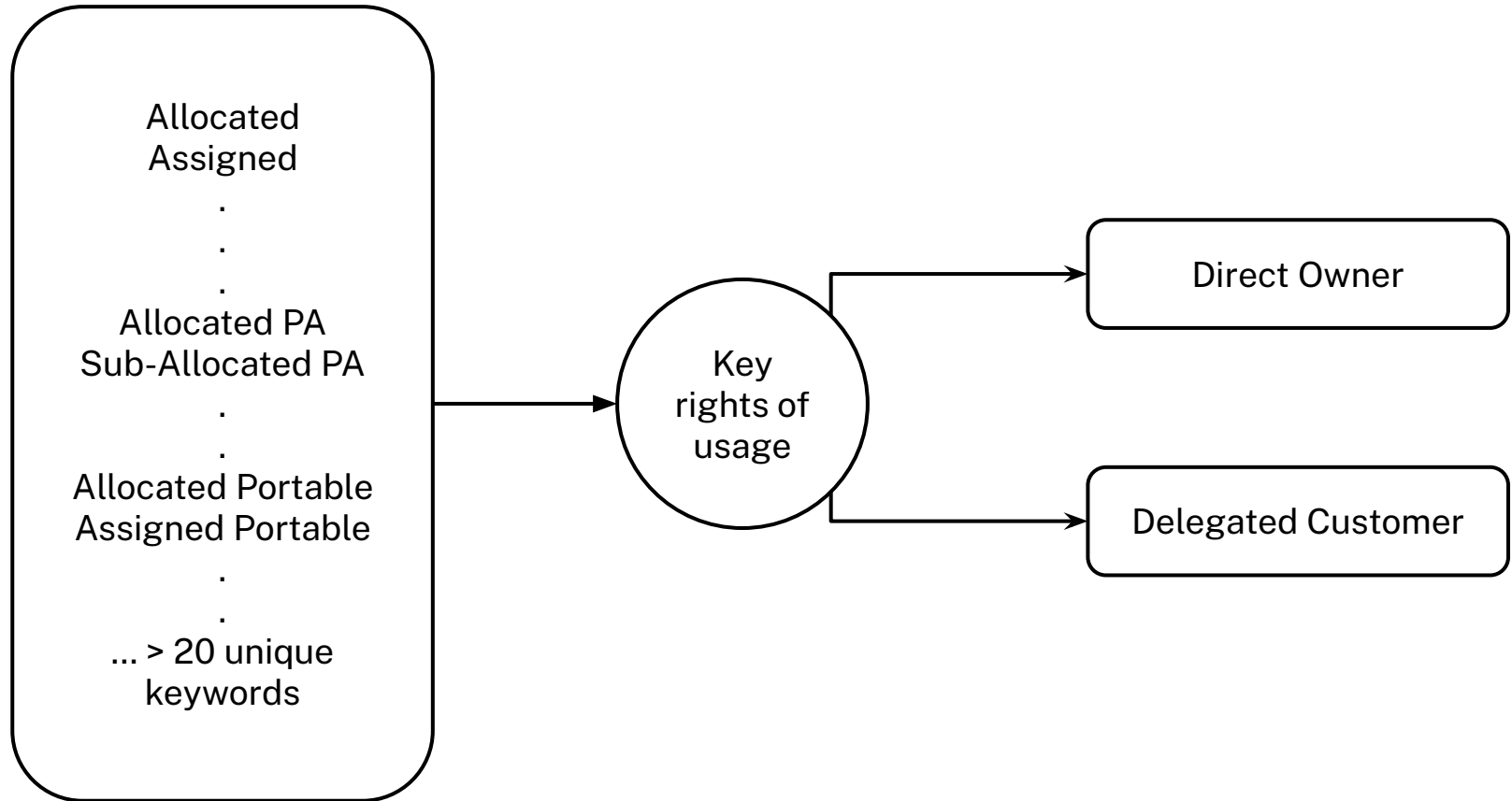
·
·

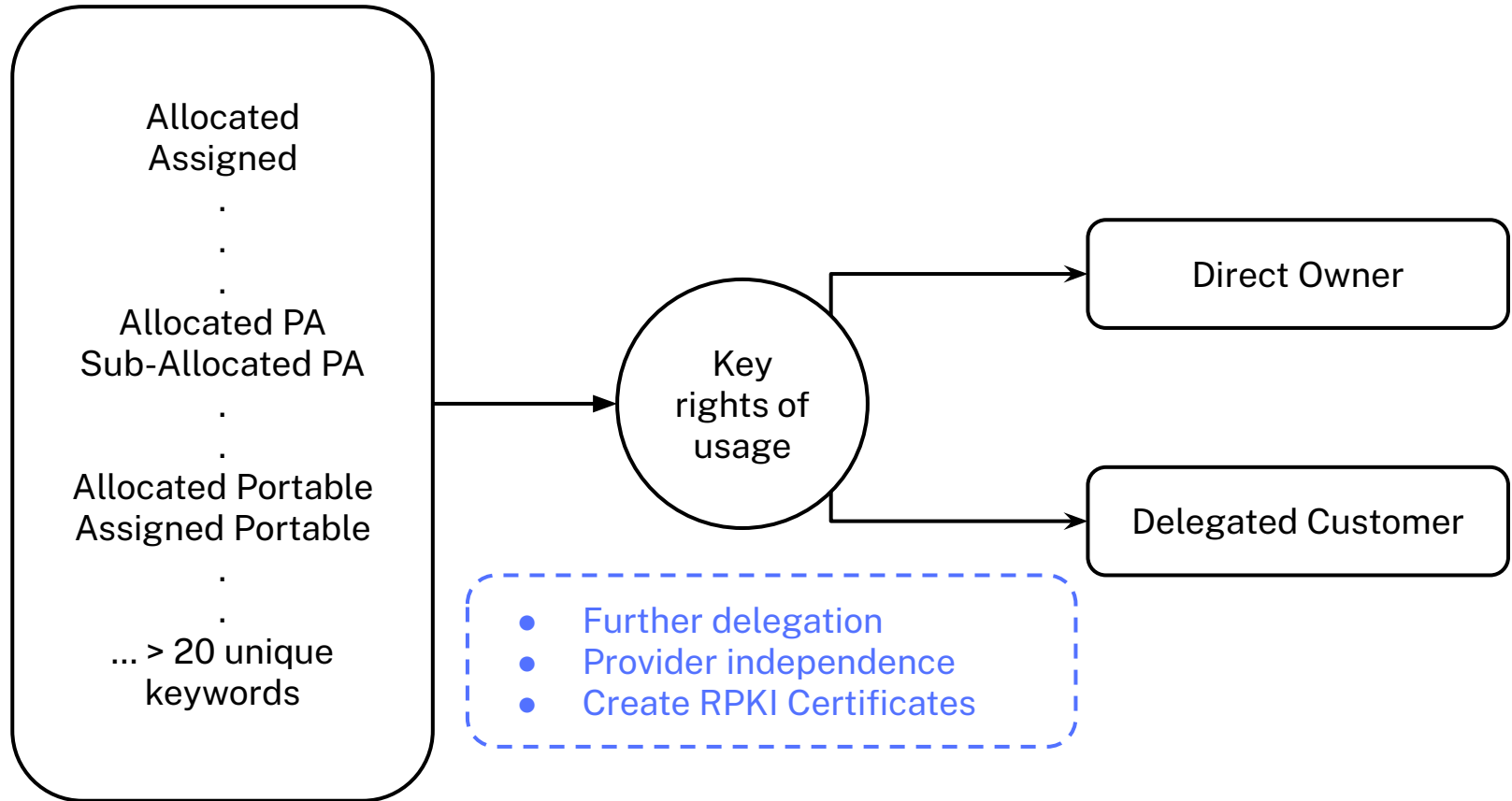
Allocated Portable
Assigned Portable

·
·

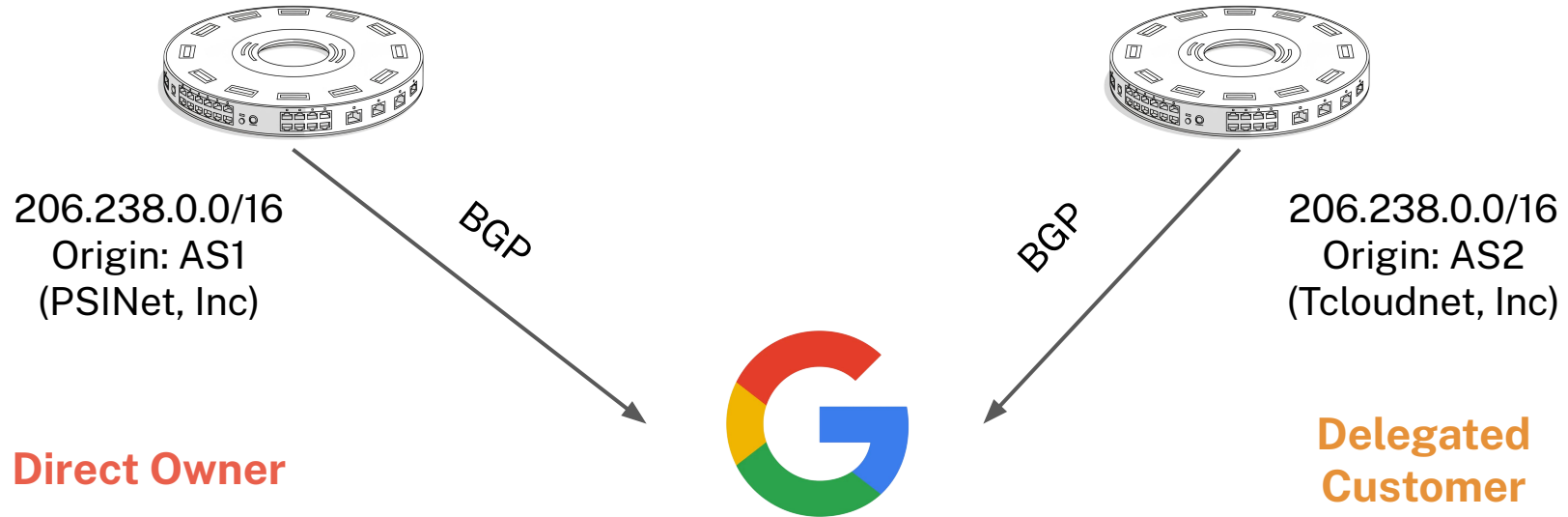
... > 20 unique
keywords







Malicious Hijack or
Misconfiguration!



Applications

- Generate signals to classify BGP hijacks
- RPKI Adoption
- Right abuse contacts
- Longitudinal snapshots of the data
 - Frequent changes in resource delegation
 - IP address acquisitions and transfers

Key Challenges

- Decoupling BGP Origin from IP Ownership
- Creating two consistent ownership levels from 22 inconsistent allocation types
- Inconsistent WHOIS records and organization names

Part II: Organization

Focusing on Organizations

We identify the owner of an IP address using WHOIS, but organizations use **multiple names** on WHOIS!

Focusing on Organizations

We identify the owner of an IP address using WHOIS, but organizations use **multiple names** on WHOIS!

- “Verizon Business” & “Verizon Nederland B.V.”
- “Google LLC” & “Google Fiber Inc”
- “Amazon.com Inc” & “Amazon Web Services”

Focusing on Organizations

Q. How can we link resources under common ownership?

Focusing on Organizations

Q. How can we link resources under common ownership?

NLP/String Processing?

Focusing on Organizations

Q. How can we link resources under common ownership?



NLP/String Processing?

- Error-prone
 - “Amazon.com Inc” & “Amazon Web Services”
 - “Fastly, Inc.” vs “Fastly Network Solution”

Focusing on Organizations

Q. How can we link resources under common ownership?



NLP/String Processing?

- Error-prone
 - “Amazon.com Inc” & “Amazon Web Services”  Match
 - “Fastly, Inc.” vs “Fastly Network Solution”  Not a Match

Focusing on Organizations

Q. How can we link resources under common ownership?

NLP/String Processing?

- Error-prone
 - “Amazon.com Inc” & “Amazon Web Services”  Match
 - “Fastly, Inc.” vs “Fastly Network Solution”  Not a Match

We need more robust way to link resources without relying solely on org names


We use:

- **RPKI Certificates**
- **BGP Data**

Focusing on Organizations

Q. How can we link resources under common ownership?

NLP/String Processing?

- Error-prone
 - “Amazon.com Inc” & “Amazon Web Services”  Match
 - “Fastly, Inc.” vs “Fastly Network Solution”  Not a Match

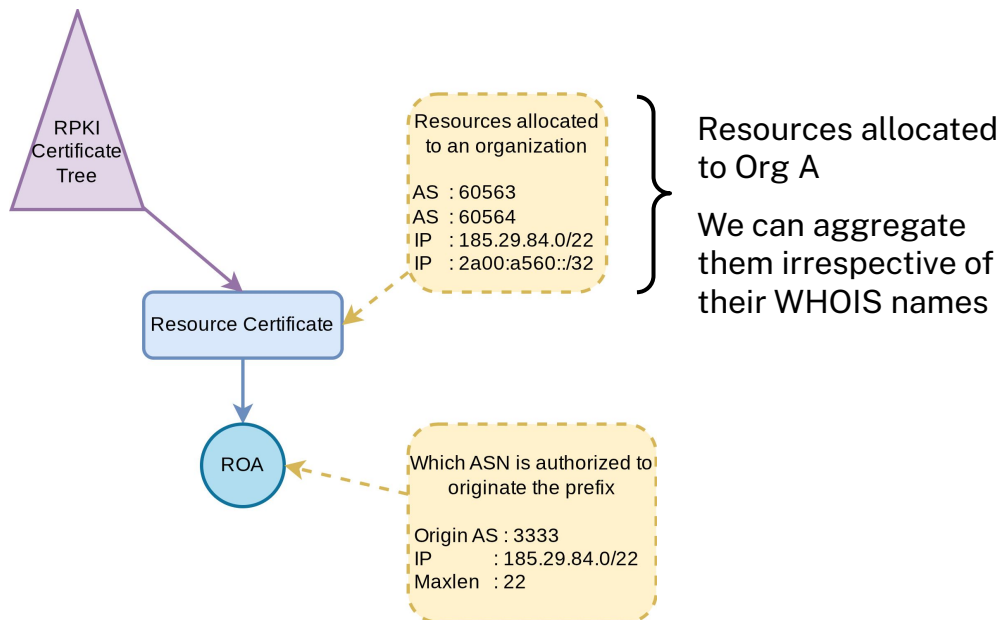
We need more robust way to link resources without relying solely on org names

We use:

- **RPKI Certificates** 
- **BGP Data**

Leveraging RPKI to Infer Shared Resource Ownership

Leveraging RPKI



Methodology

Methodology

Problem: Aggregating resources with shared ownership

Methodology

Problem: Aggregating resources with shared ownership

Solution:

- NLP by itself ➡ error-prone
- RPKI Certificates ➡ not always (some certs put distinct orgs together)
- BGP Origin ASN ➡ not necessarily ownership

Methodology

Problem: Aggregating resources with shared ownership

Solution:

- NLP by itself ➡ error-prone
- RPKI Certificates ➡ not always (some certs put distinct orgs together)
- BGP Origin ASN ➡ not necessarily ownership

We take the individual solutions and use them together:

Similar Name & (Same RPKI Cert | Same BGP Origin)

Dataset Sample

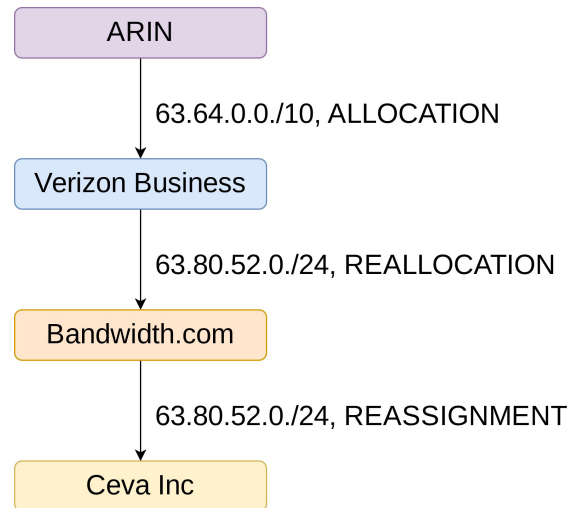
```
1 "63.80.52.0/24": {  
2   "RIR": "ARIN",  
3   "Direct Owner (DO)": "Verizon Business",  
4   "DO Prefix": "63.64.0.0/10"  
5   "DO Allocation Type": "ALLOCATION",  
6   "Delegated Customer(s) (DC)": ["Bandwidth.com  
   Inc.", "Ceva Inc"],  
7   "DC Prefix(es)": ["63.80.52.0/24", "  
   63.80.52.0/24"],  
8   "DC Allocation Type(s)": ["REALLOCATION", "  
   REASSIGNMENT"],  
9   "Base name": "verizon",  
10  "RPKI Certificate": "29:92:C2:35:B0:89...",  
11  "Origin ASN Cluster": "701",  
12  "Final Cluster": "verizon-076541",  
13 }
```

Listing 1: Prefix2Org Dataset for 63.80.52.0/24.

Dataset Sample

```
1 "63.80.52.0/24": {  
2   "RIR": "ARIN",  
3   "Direct Owner (DO)": "Verizon Business",  
4   "DO Prefix": "63.64.0.0/10"  
5   "DO Allocation Type": "ALLOCATION",  
6   "Delegated Customer(s) (DC)": ["Bandwidth.com  
   Inc.", "Ceva Inc"],  
7   "DC Prefix(es)": ["63.80.52.0/24", "  
   63.80.52.0/24"],  
8   "DC Allocation Type(s)": ["REALLOCATION", "  
   REASSIGNMENT"],  
9   "Base name": "verizon",  
10  "RPKI Certificate": "29:92:C2:35:B0:89...",  
11  "Origin ASN Cluster": "701",  
12  "Final Cluster": "verizon-076541",  
13 }
```

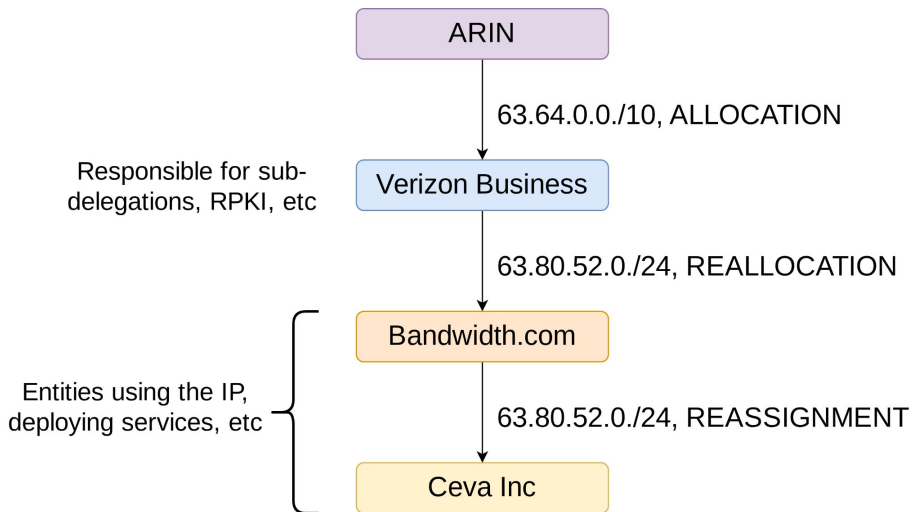
Listing 1: Prefix2Org Dataset for 63.80.52.0/24.



Dataset Sample

```
1 "63.80.52.0/24": {  
2   "RIR": "ARIN",  
3   "Direct Owner (DO)": "Verizon Business",  
4   "DO Prefix": "63.64.0.0/10"  
5   "DO Allocation Type": "ALLOCATION",  
6   "Delegated Customer(s) (DC)": ["Bandwidth.com  
   Inc.", "Ceva Inc"],  
7   "DC Prefix(es)": ["63.80.52.0/24", "  
   63.80.52.0/24"],  
8   "DC Allocation Type(s)": ["REALLOCATION", "  
   REASSIGNMENT"],  
9   "Base name": "verizon",  
10  "RPKI Certificate": "29:92:C2:35:B0:89...",  
11  "Origin ASN Cluster": "701",  
12  "Final Cluster": "verizon-076541",  
13 }
```

Listing 1: Prefix2Org Dataset for 63.80.52.0/24.

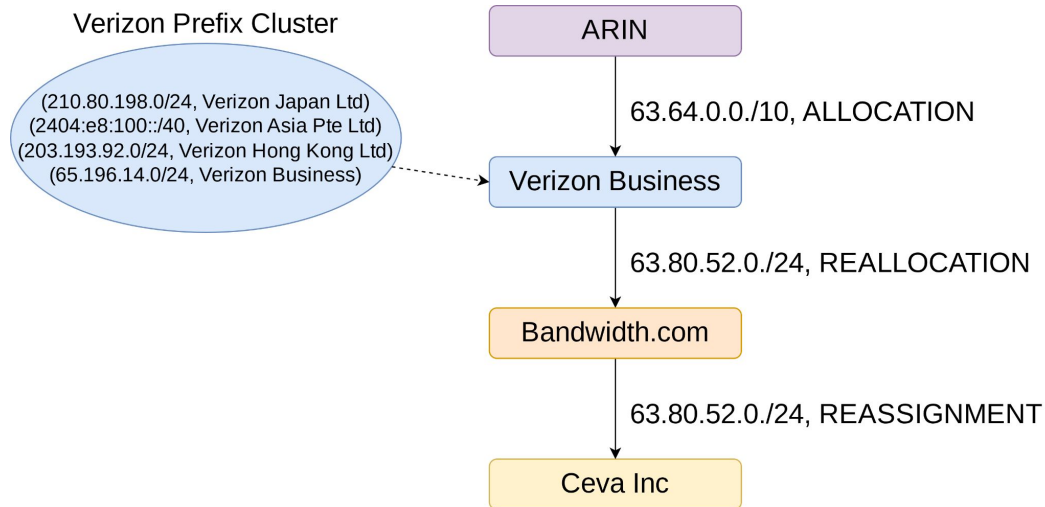


Part I: Ownership

Dataset Sample

```
1 "63.80.52.0/24": {  
2   "RIR": "ARIN",  
3   "Direct Owner (DO)": "Verizon Business",  
4   "DO Prefix": "63.64.0.0/10"  
5   "DO Allocation Type": "ALLOCATION",  
6   "Delegated Customer(s) (DC)": ["Bandwidth.com  
   Inc.", "Ceva Inc"],  
7   "DC Prefix(es)": ["63.80.52.0/24", "  
   63.80.52.0/24"],  
8   "DC Allocation Type(s)": ["REALLOCATION", "  
   REASSIGNMENT"],  
9   "Base name": "verizon",  
10  "RPKI Certificate": "29:92:C2:35:B0:89...",  
11  "Origin ASN Cluster": "701",  
12  "Final Cluster": "verizon-076541",  
13 }
```

Listing 1: Prefix2Org Dataset for 63.80.52.0/24.



Part II: Organization

Questions!

deepakgouda@
deepakgouda@gatech.edu

Additional Slides

Allocation Types

RIR	Direct Owner	Delegated Customer
ARIN	Allocation	Reallocation Reassignment
LACNIC	Allocated Assigned	Reallocated Reassigned
RIPE	Allocated PA Assigned PI Legacy‡ Allocated-BY-RIR† Assigned Anycast Allocated-Assigned PA	Assigned PA Assigned† Sub-Allocated PA Allocated-By-LIR† Aggregated-By-LIR†
AFRINIC	Allocated PA Assigned PI Allocated-BY-RIR† Assigned Anycast	Assigned PA Sub-Allocated PA
APNIC	Allocated Portable Assigned Portable	Allocated Non-Portable Assigned Non-Portable

‡ : IPv4 allocations only † : IPv6 allocations only

Table 1: Allocation type values used across five RIRs.

Leveraging RPKI

```
$ rpkgi-client -vvf rpkgi.afrinic.net/repository/afrinic/-RyaVXksG3JGcT_syDoE0La_EpE.cer
File: -RyaVXksG3JGcT_syDoE0La_EpE.cer (raw, json)
Hash identifier: kljHECTmvpNid+IYIn38dIy28uN7Bz5LgccbMswBIAo=
Subject key identifier: F9:1C:9A:55:79:2C:1B:72:46:71:3F:EC:C8:3A:04:D0:B6:BF:12:91
Authority key identifier: 2B:57:89:7A:7C:A9:64:C3:C8:B7:F7:BD:DA:A7:A4:DA:34:A9:8F:80
Certificate issuer: /CN=AFRINIC/serialNumber=2B57897A7CA964C3C8B7F7BDDAA7A4DA34A98F80
Certificate serial: 3301
Authority info access: rsync://rpki.afrinic.net/repository/04E8B0D80F4D11E0B657D8931367AE7D/afrinic-ca.cer
Manifest: rsync://rpki.afrinic.net/repository/member_repository/F36D9765/17D92B5C92DC11EEBFDD584DD25BE465/-RyaVXksG3
caRepository: rsync://rpki.afrinic.net/repository/member_repository/F36D9765/17D92B5C92DC11EEBFDD584DD25BE465/
Notify URL: https://rrdp.afrinic.net/notification.xml
Certificate not before: Wed 01 Jan 2025 05:40:25 +0000
Certificate not after: Tue 31 Mar 2026 00:00:00 +0000
Subordinate resources: AS: 37129
                        IP: 102.211.216.0/22
                        IP: 196.22.131.0/24
                        IP: 197.157.228.0/22
Validation: OK
Signature path: rsync://rpki.afrinic.net/repository/afrinic/K1eJenypZMPIt_e92qek2jSpj4A.crl
                rsync://rpki.afrinic.net/repository/afrinic/K1eJenypZMPIt_e92qek2jSpj4A.mft
                rsync://rpki.afrinic.net/repository/04E8B0D80F4D11E0B657D8931367AE7D/afrinic-ca.cer
                rsync://rpki.afrinic.net/repository/04E8B0D80F4D11E0B657D8931367AE7D/62gPOPXwxu0s0a4vQZYUBLAmbHY.crl
                rsync://rpki.afrinic.net/repository/04E8B0D80F4D11E0B657D8931367AE7D/62gPOPXwxu0s0a4vQZYUBLAmbHY.mft
                rsync://rpki.afrinic.net/repository/AfrINIC.cer
Signature path expires: Fri 18 Apr 2025 00:06:12 +0000
```

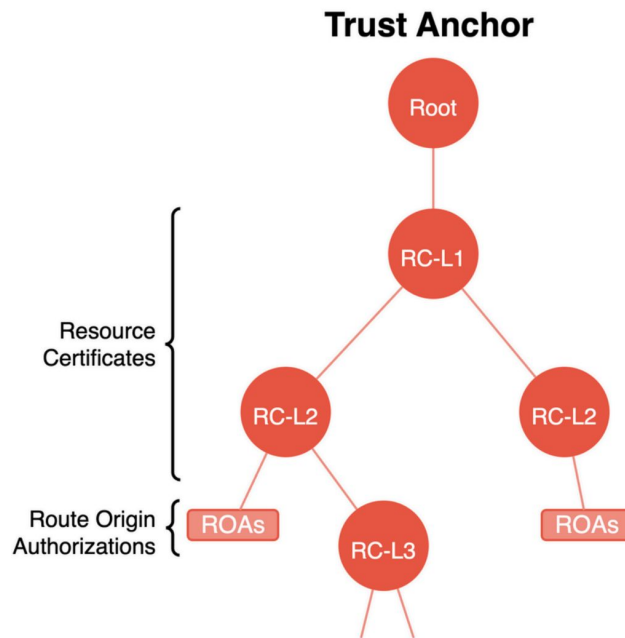
Resources allocated
to certificate holder

Leveraging RPKI

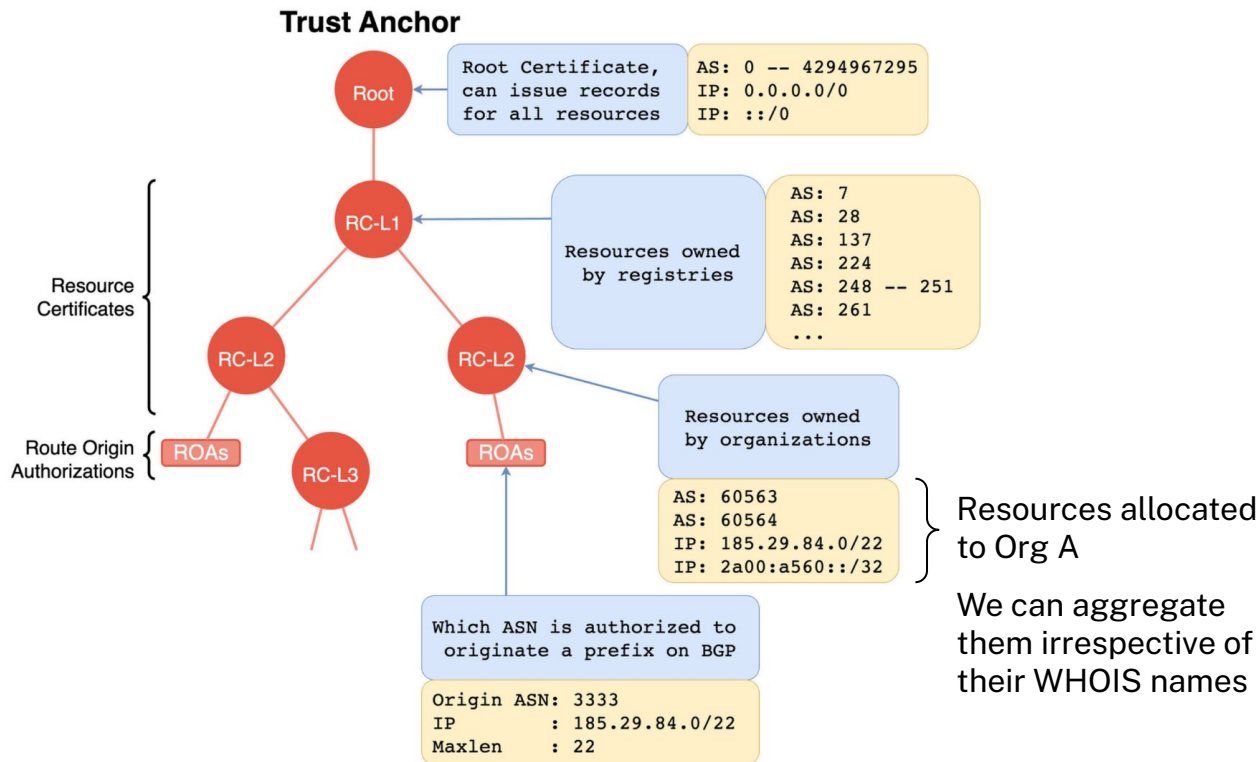
Two kinds of certificates in RPKI

- **Resource Certificates (RC):** Specify the resources that the certificate holder can exercise control over
- **Route Origin Authorization (ROA):** Indicates the ASN authorized to originate a prefix in BGP

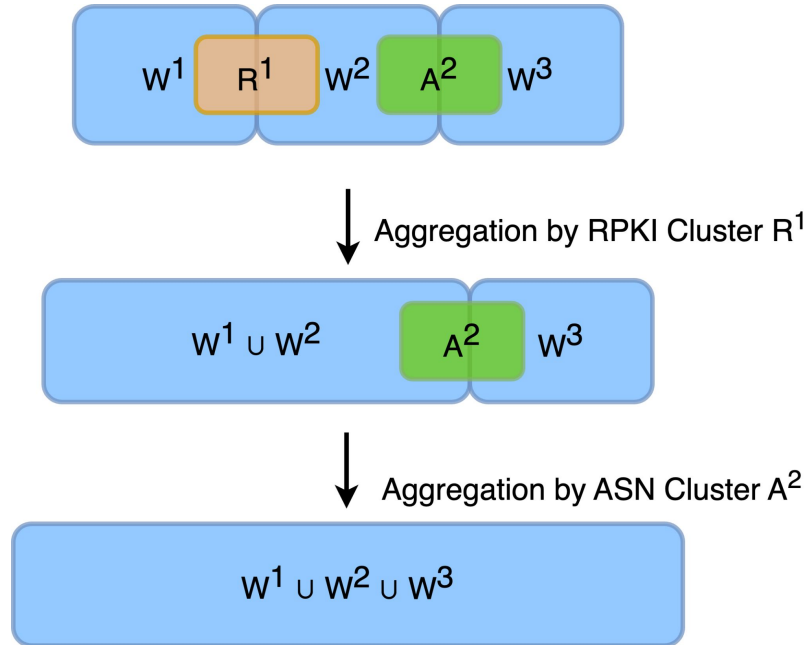
Key Idea: All prefixes within a single Resource Certificate are administered by the same entity



Leveraging RPKI



Clustering Methodology

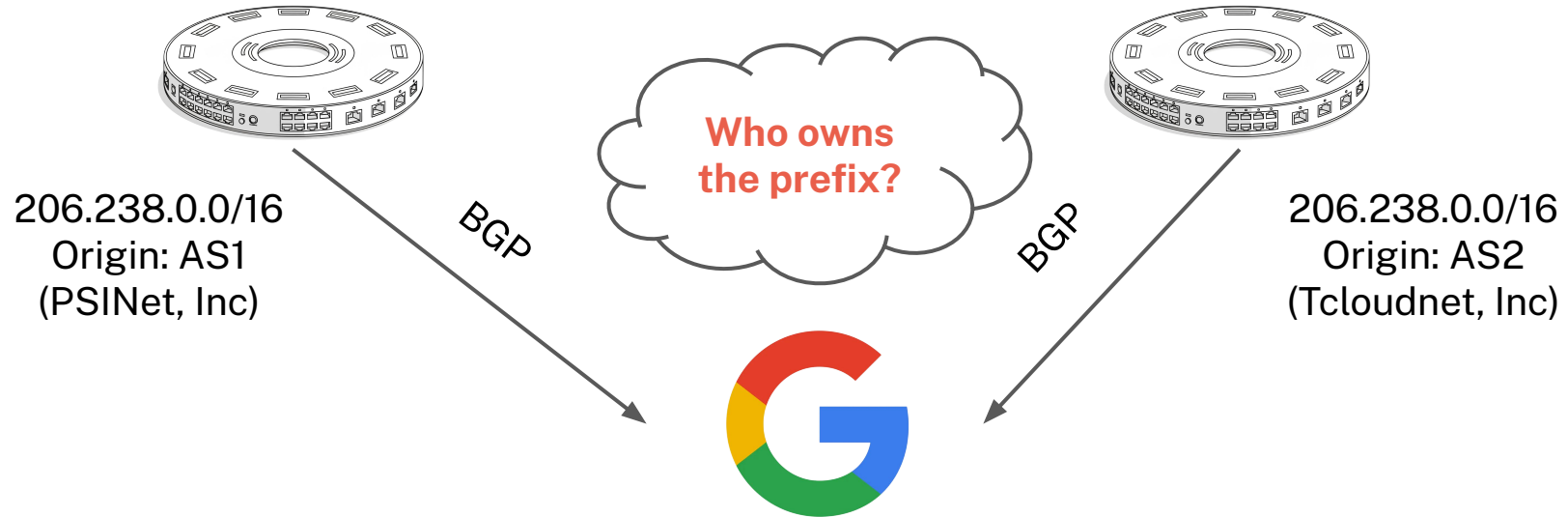


Further Applications

- Longitudinal snapshots of the data
 - Frequent changes in resource delegation
 - IP address acquisitions and transfers

CIDR	206.236.0.0/15, 206.232.0.0/14, 206.238.0.0/16
NetType	Direct Allocation
Organization	PSINet, Inc. (PSI)

CIDR	206.238.0.0/16
NetType	Reassigned
Customer	Tcloudnet, Inc (C09815123)



Note: BGP Origin \nRightarrow Ownership!