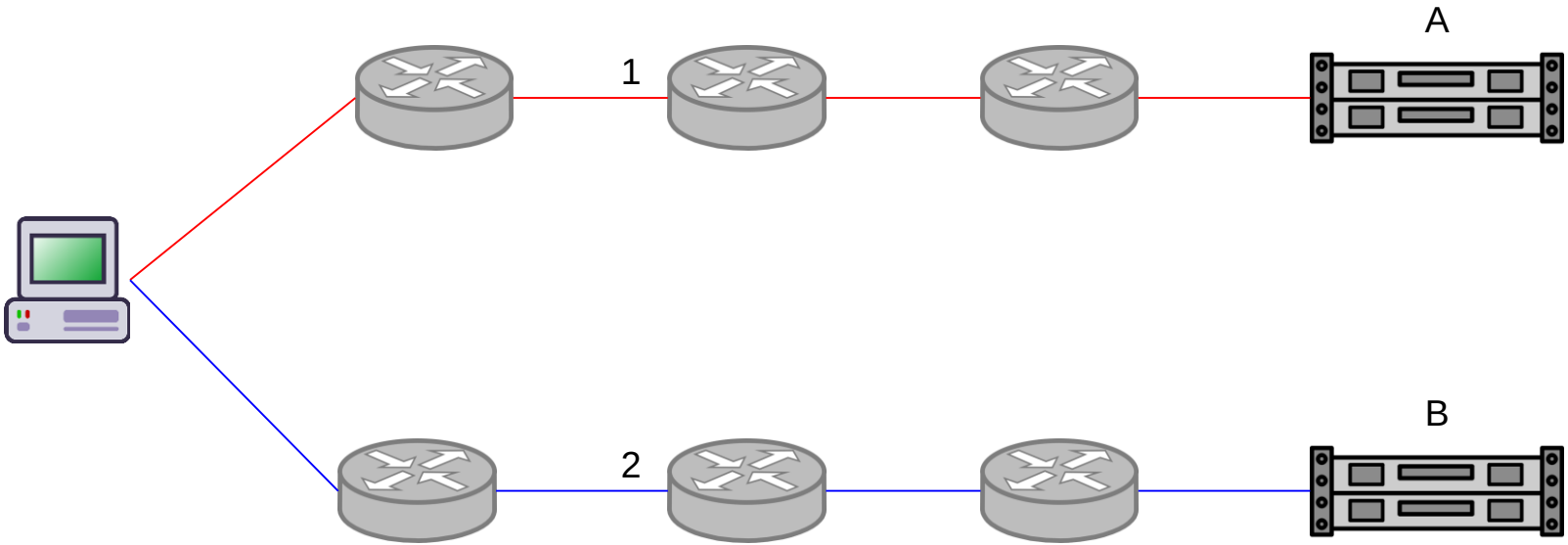
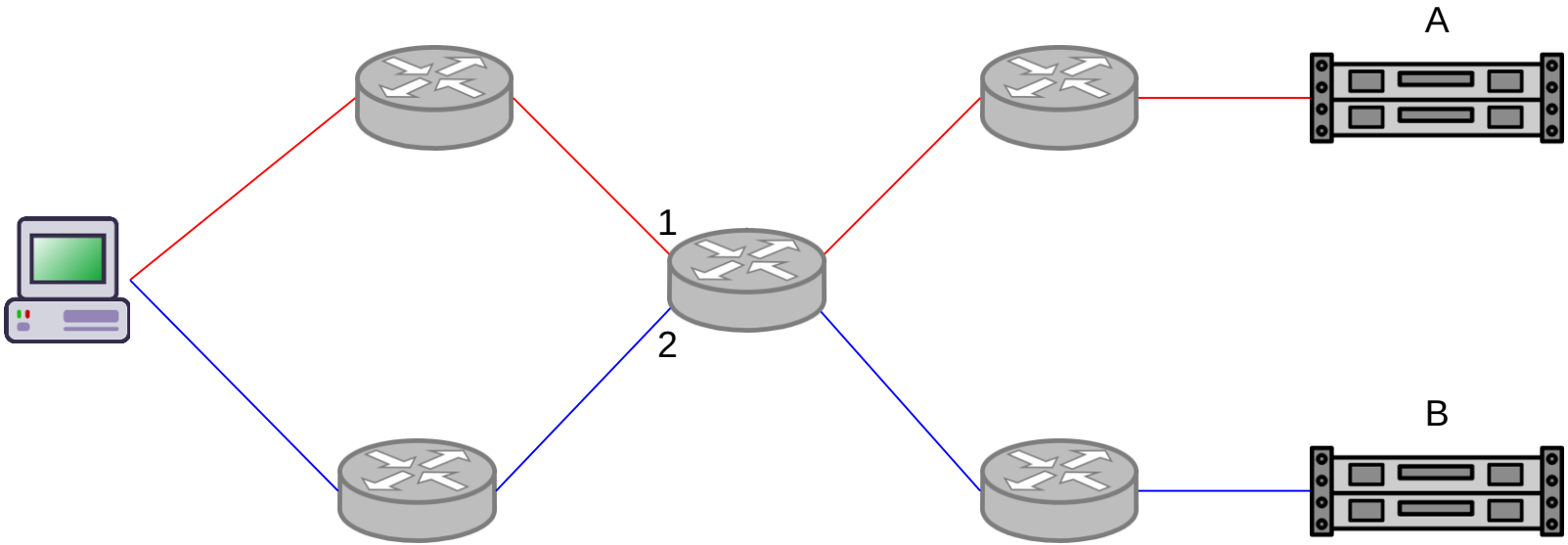
Pushing Alias Resolution to the Limit

Taha Albakour, Oliver Gasser, and Georgios Smaragdakis


A
1
B
2


A
1
2
B

Importance of IP Alias Resolution in Sampling Internet Topologies

Mehmet Hadi Gunes
Department of Computer Science
University of Texas at Dallas
Email: mgunes@utdallas.edu

Kamil Sarac
Department of Computer Science
University of Texas at Dallas
Email: ksarac@utdallas.edu

A Server-to-Server View of the Internet

Balakrishnan Chandrasekaran
Duke University
balac@cs.duke.edu

Georgios Smaragdakis
MIT / TU Berlin / Akamai
gsmaragd@csail.mit.edu

Arthur Berger
MIT / Akamai
awberger@csail.mit.edu

Matthew Luckie
University of Waikato
mjl@wand.net.nz

Keung-Chi Ng
Akamai
kng@akamai.com

Identifying IPv6 Network Problems in the Dual-Stack World

Kenjiro Cho
Sony CSL/WIDE Project
kjc@csl.sony.co.jp

Matthew Luckie
U.Waikato/NLANR/CAIDA
mjl@wand.net.nz

Bradley Huffaker
CAIDA/SDSC/UCSD
bhuffake@caida.org

Don't Forget to Lock the Back Door! A Characterization of IPv6 Network Security Policy

Jakub Czyz*, Matthew Luckie†, Mark Allman‡, and Michael Bailey§
*University of Michigan and QuadMetrics, Inc.; jczyz@umich.edu
†University of Waikato; mjl@wand.net.nz
‡International Computer Science Institute; mallman@icir.org
§University of Illinois at Urbana-Champaign; mdbailey@illinois.edu

Previous Approaches

Alias Resolution

- ICMP Common Source Address
- Common IPID Counter
- Protocol-centric

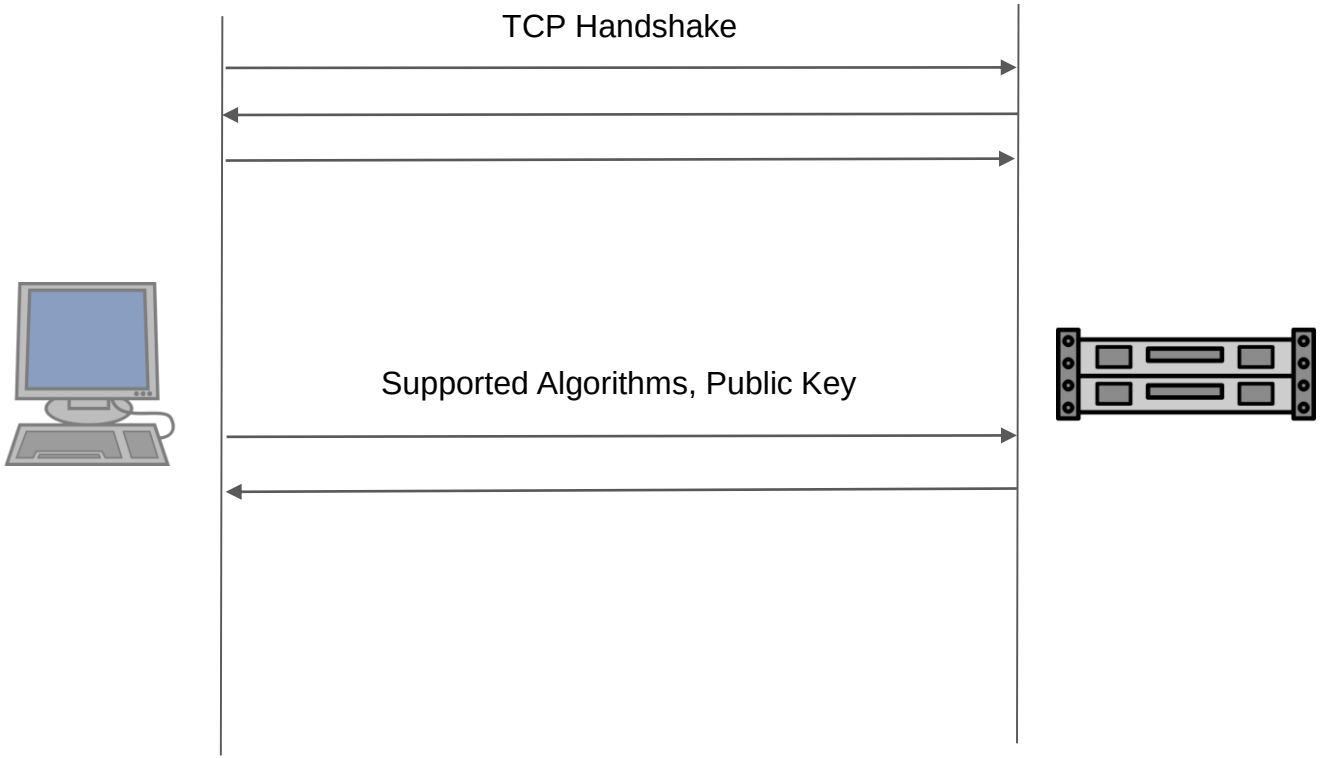
Dual Stack Inference

- DNS PTR Records
- Protocol-centric

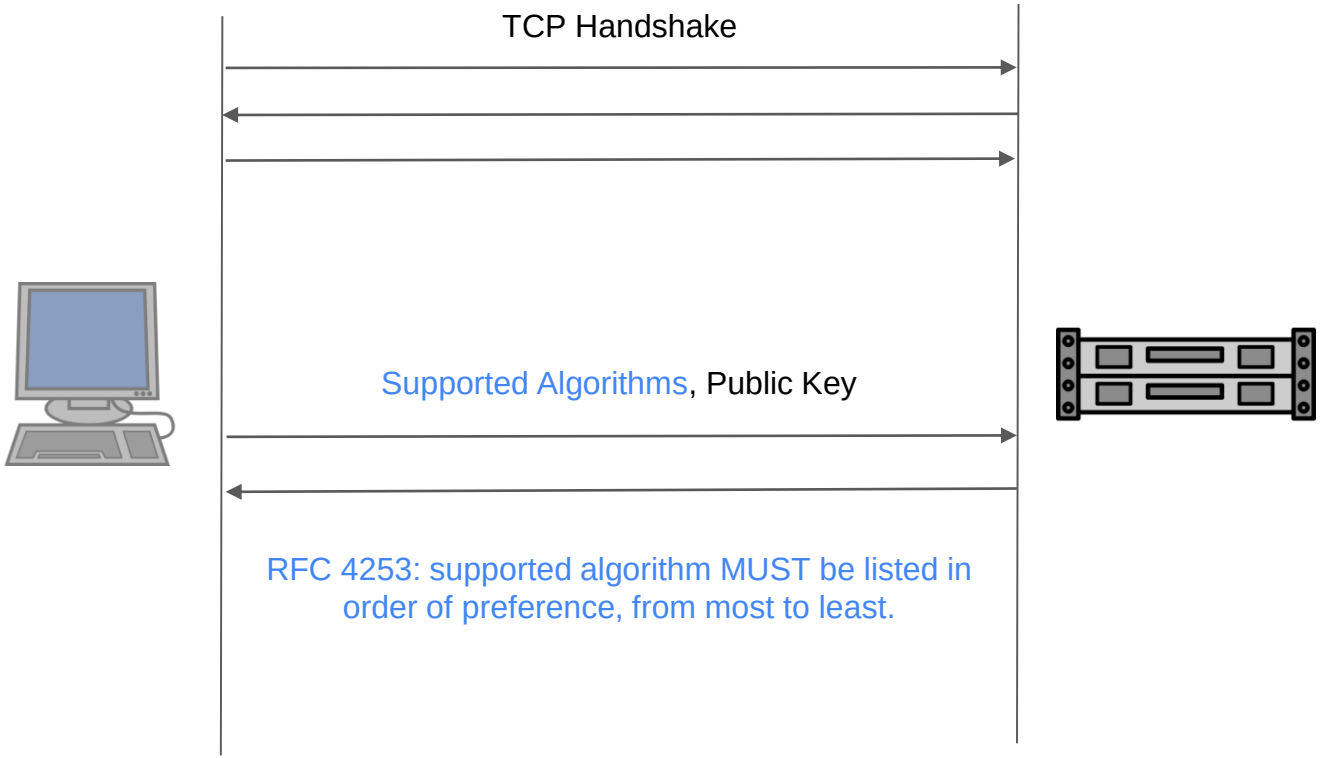
Our Approach

- Identify protocols with unexpected, globally unique host identifier
- We consider two protocols:
  - SSH → Popular
  - BGP → Router
- Group IPs that share the same identifier:
  - Alias sets (IPv4 or IPv6)
  - Dual-Stack sets (IPv4 and IPv6)

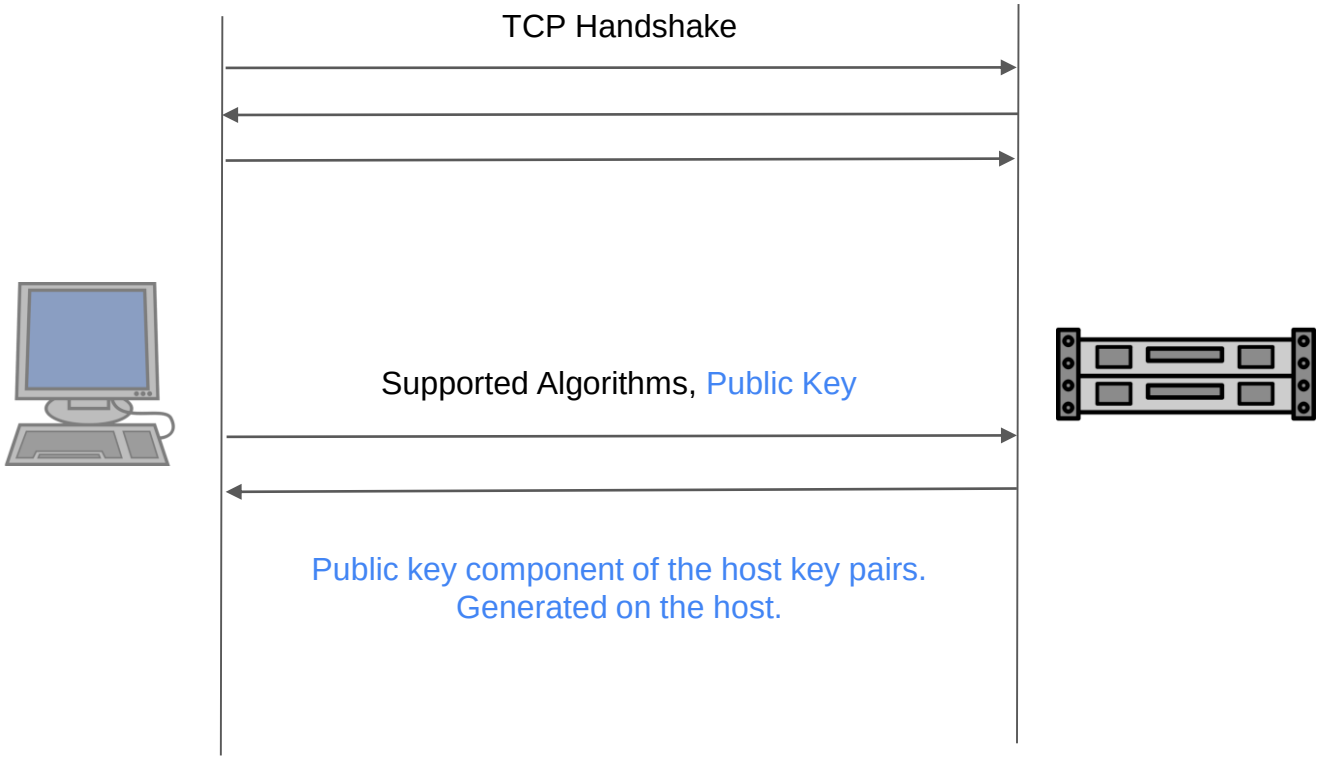
SSH Identifier



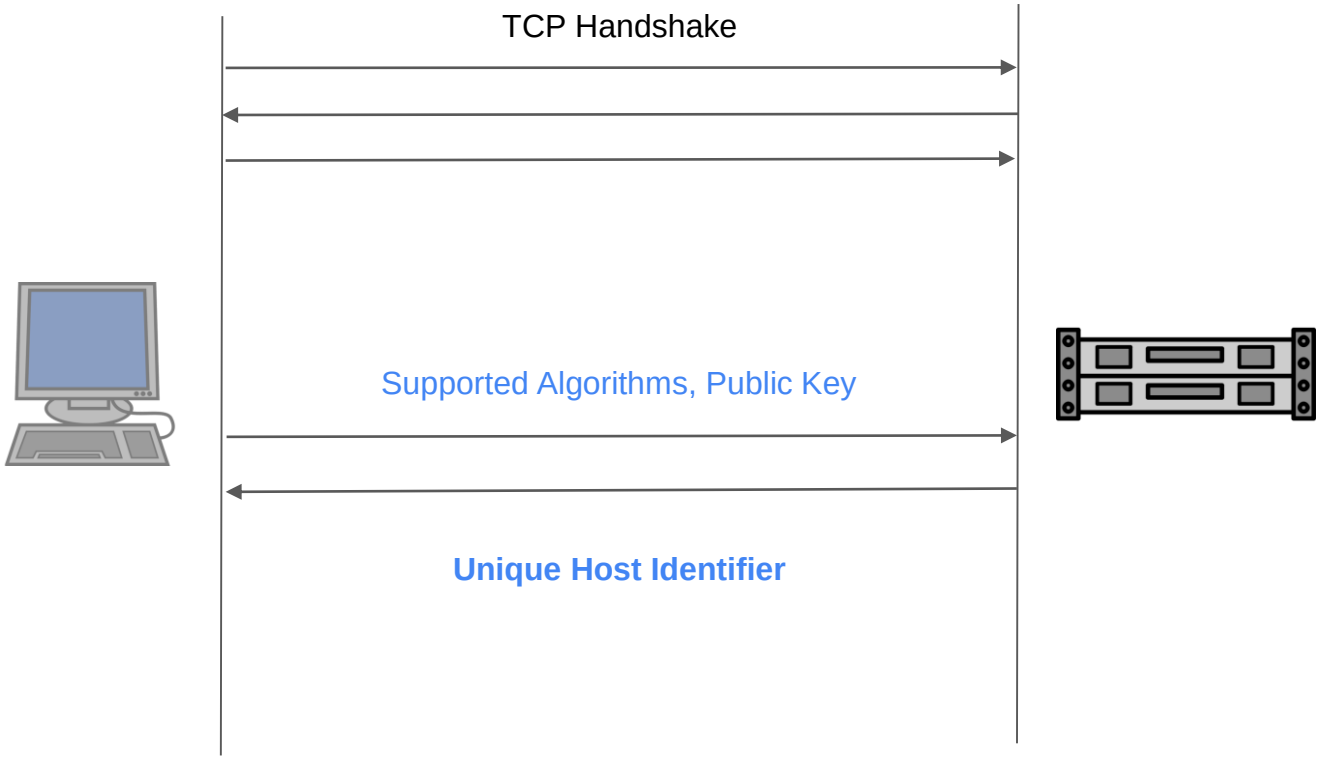
SSH Identifier



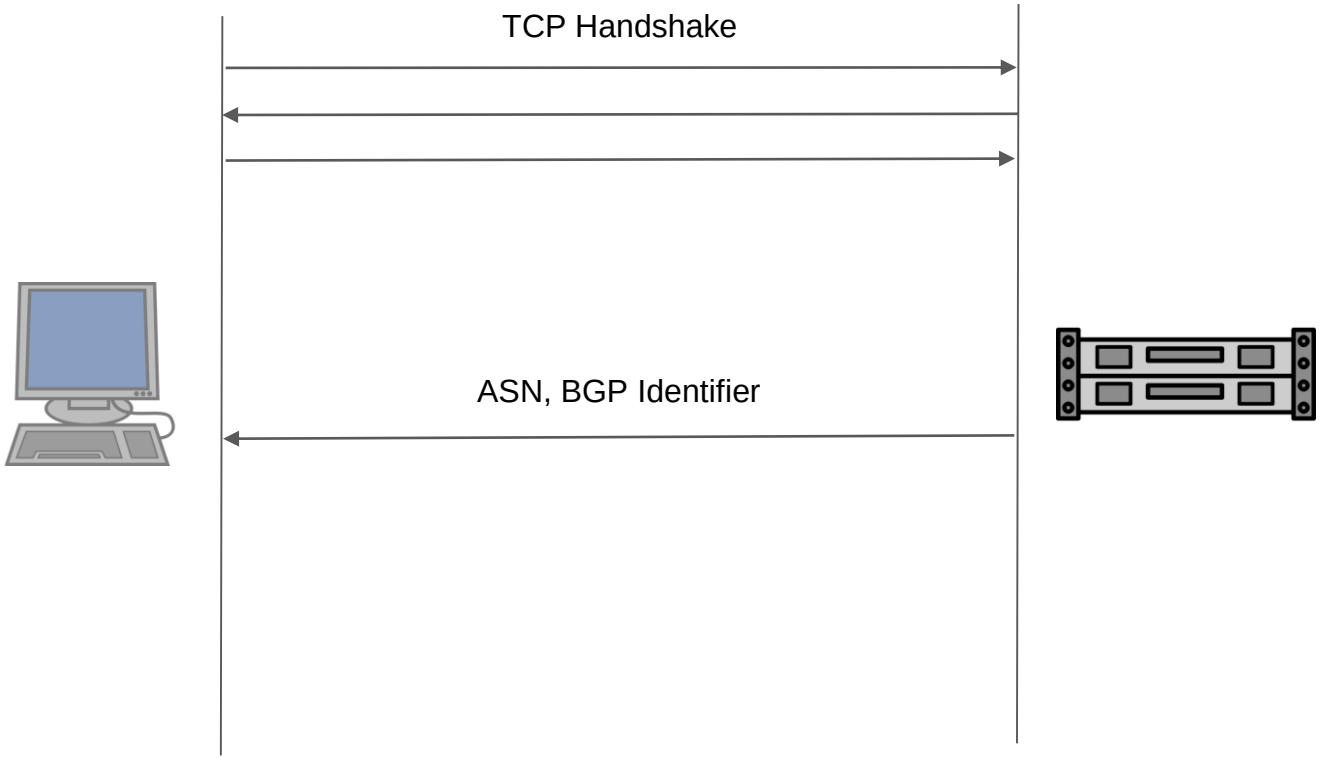
SSH Identifier



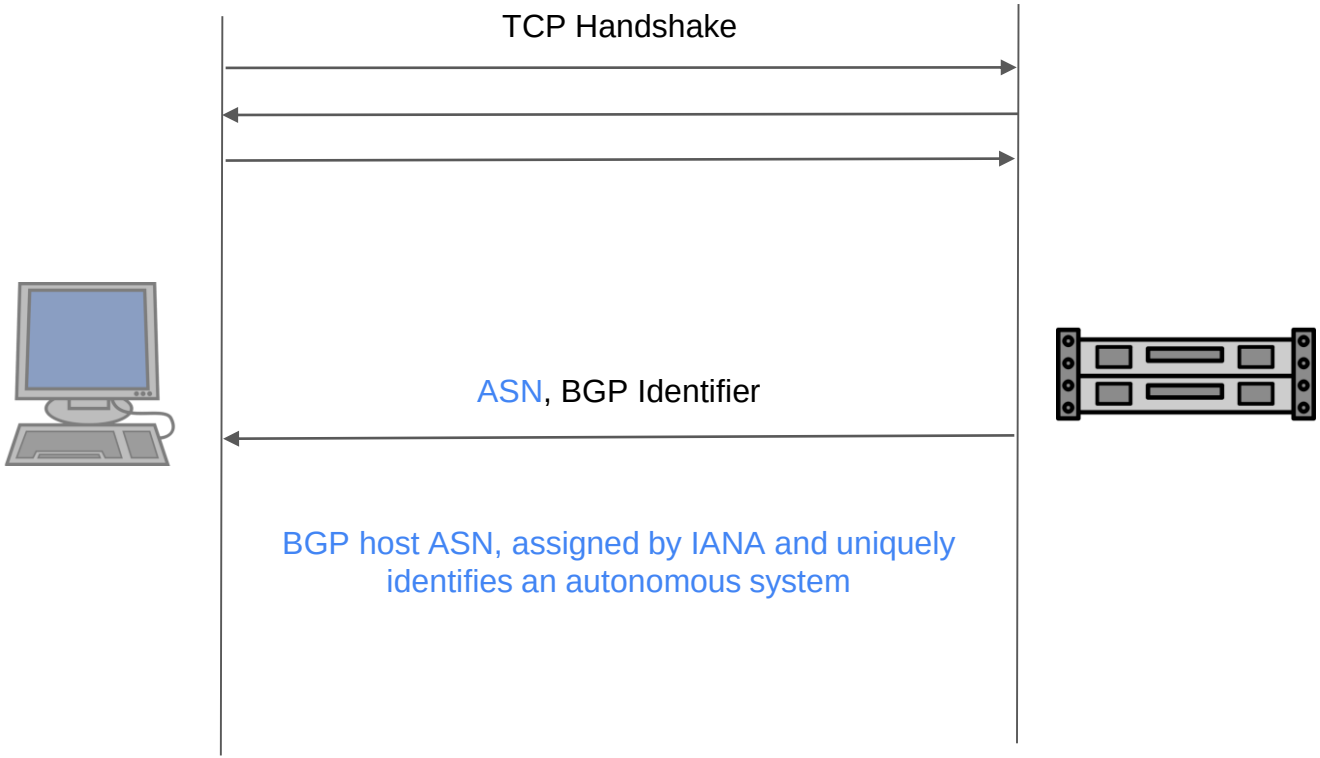
SSH Identifier



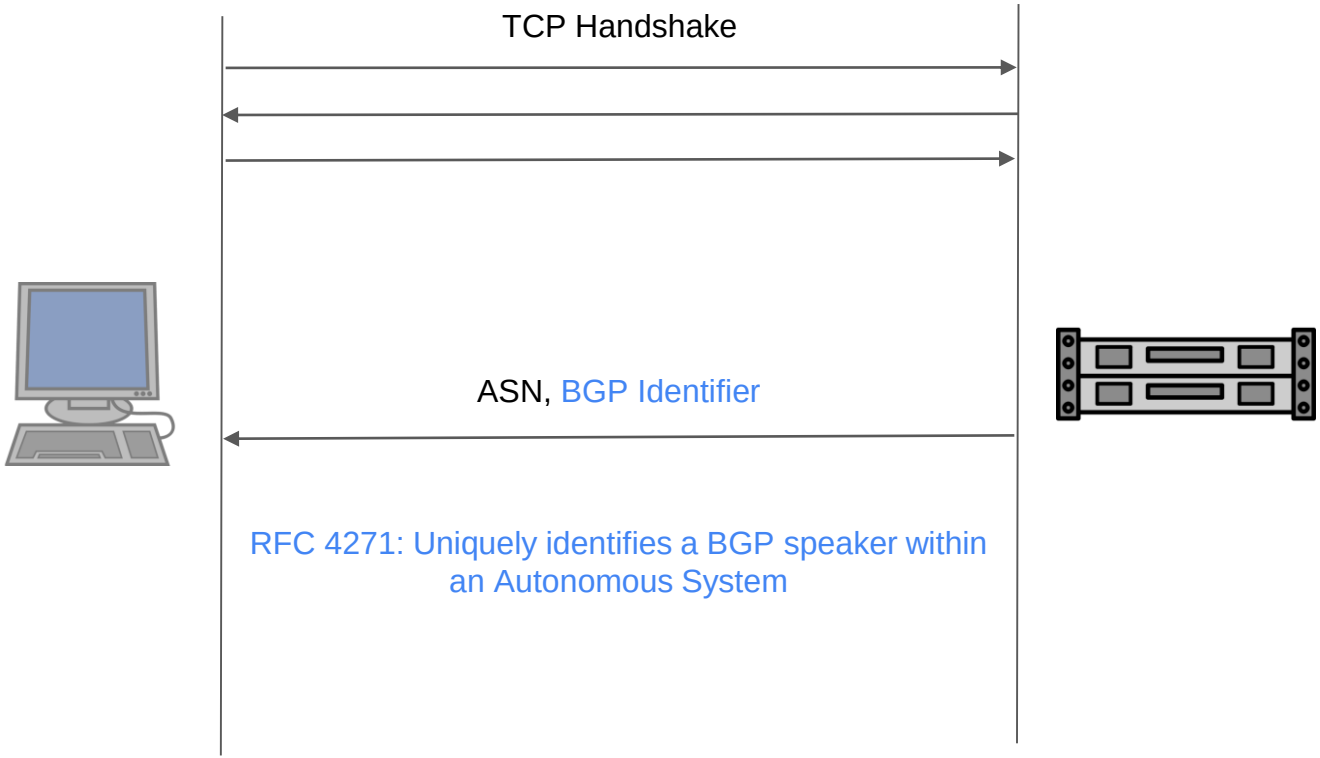
BGP Identifier



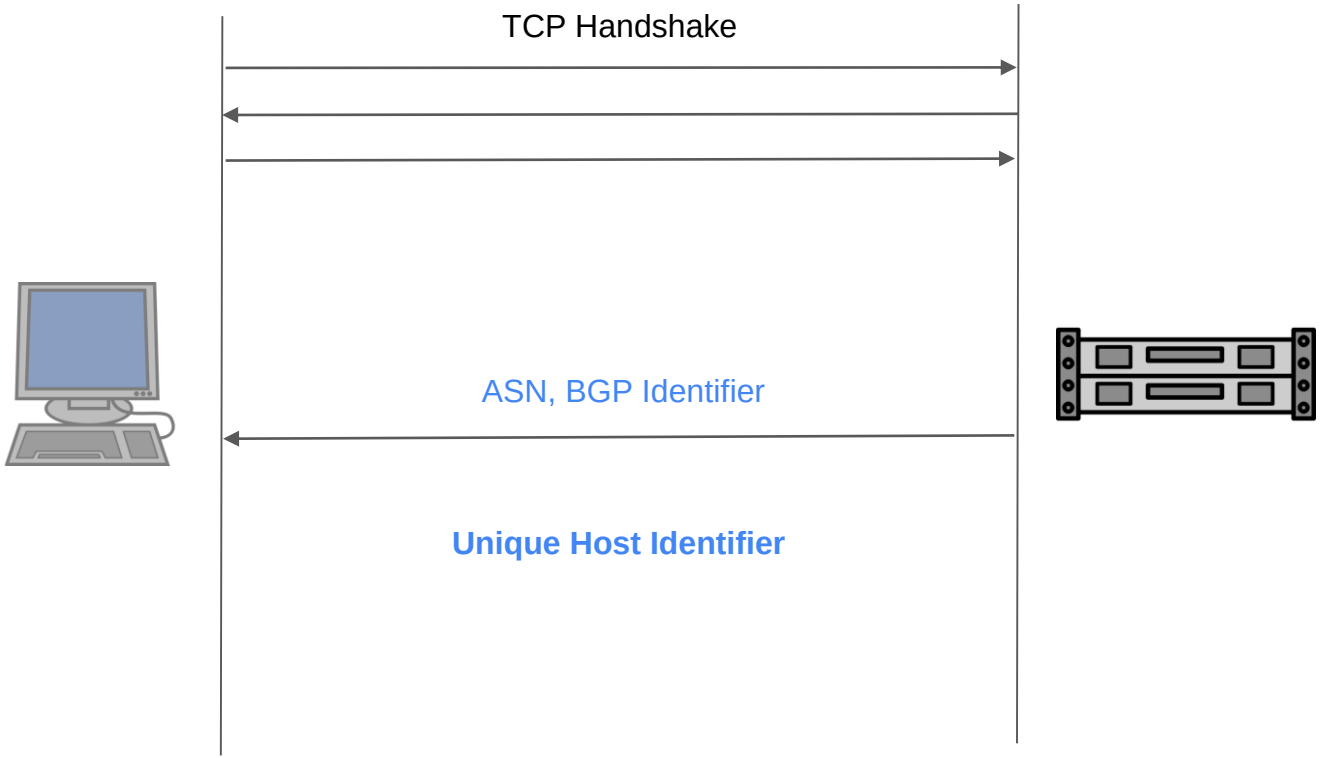
BGP Identifier



BGP Identifier



BGP Identifier



SSH Identifier

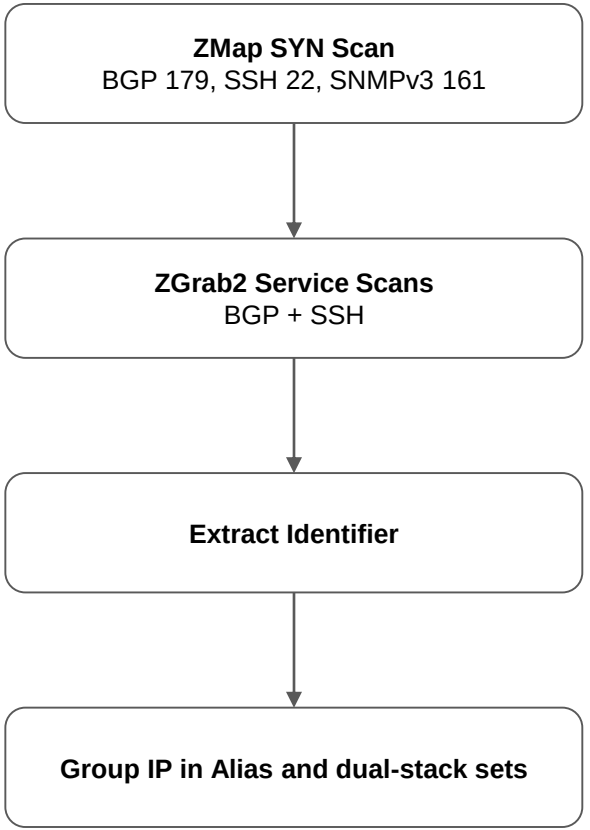
```
SSH Protocol
Protocol: SSH-2.0-
SSH Version 2
 ...
 Key Exchange (method:curve25519-sha256)
  Message Code: Key Exchange Init (20)
  Algorithms
   ...
   kex_algorithms string: curve25519-sha256,..
   server_host_key_algorithms length: 57
   server_host_key_algorithms string:...
   encryption_algorithms_server_to_client length: 108
   encryption_algorithms_server_to_client string: ...
   ...
   mac_algorithms_server_to_client length: 213
   mac_algorithms_server_to_client string: ...
   ...
   compression_algorithms_server_to_client length: 21
   compression_algorithms_server_to_client string:...
 Key Exchange (method:curve25519-sha256)
  Message Code: Elliptic Curve Diffie-Hellman Key Exchange Reply(31)
  KEX host key (type: ssh-ed25519)
   ...
   EdDSA public key length: 32
   EdDSA public key:409fa737033d6a79a1130aff96ee5ee2c39a9...
  ...
```

BGP Identifier

```
Border Gateway Protocol - OPEN Message
        Marker: ffffffffffffffffffffffffffffffff
        Length:37
        Type: OPEN Message (1)
        Version: 4
        My AS: 23456
        Hold Time: 90
        BGP Identifier: 148.170.0.33
        Optional Parameters Length: 8
        Optional Parameter: Capability
            Parameter Type: Capability (2)
                  Parameter Length: 2
                  Capability: Route refresh capability (Cisco)
                  Type: Route refresh capability (Cisco) (128)
                  Length: 0
        Optional Parameter: Capability
            Parameter Type: Capability (2)
                  Parameter Length: 2
                  Capability: Route refresh capability
                  Type: Route refresh capability (2)
                  Length: 0
Border Gateway Protocol - NOTIFICATION Message
        Marker: ffffffffffffffffffffffffffffffff
        Length: 21
        Type: NOTIFICATION Message (3)
        Major error Code: Cease (6)
        Minor error Code (Cease): Connection Rejected (5)
```

Data Collection Pipeline

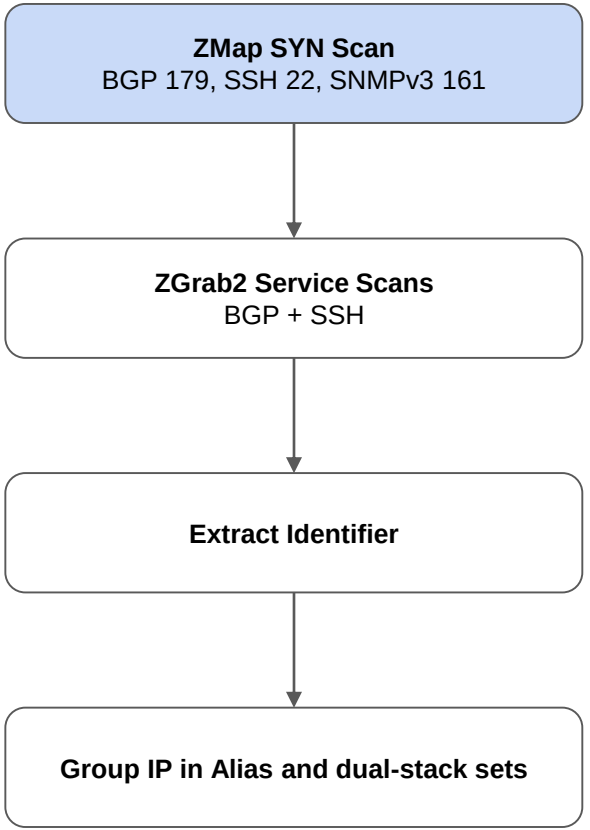
- Active Measurements
  - IPv4: all routable addresses
  - IPv6: Hitlist Service *
  - SSH 22, BGP 179, SNMPv3 161
- Censys IPv4 Dataset **



* https://ipv6hitlist.github.io/
** https://censys.com/

Data Collection Pipeline

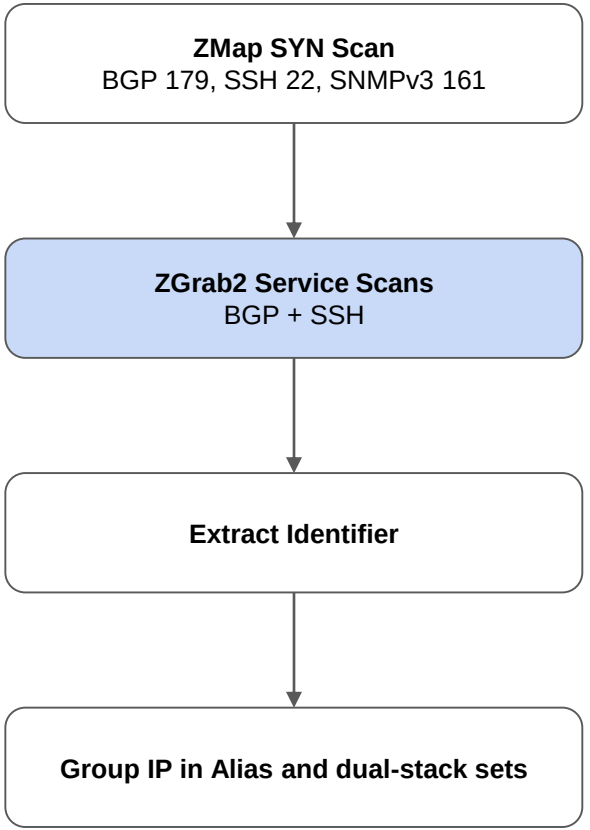
- Active Measurements
  - IPv4: all routable addresses
  - IPv6: Hitlist Service *
  - SSH 22, BGP 179, SNMPv3 161
- Censys IPv4 Dataset **



* https://ipv6hitlist.github.io/
** https://censys.com/

Data Collection Pipeline

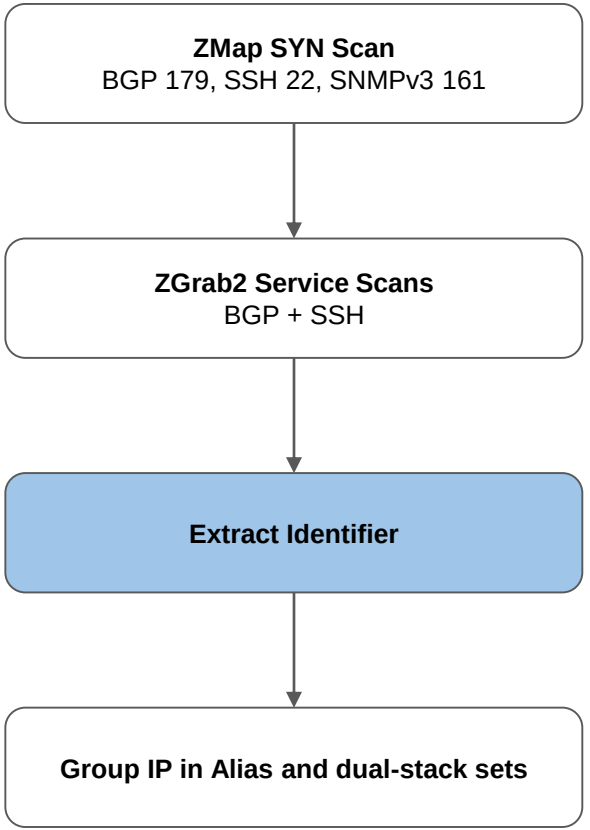
- Active Measurements
  - IPv4: all routable addresses
  - IPv6: Hitlist Service *
  - SSH 22, BGP 179, SNMPv3 161
- Censys IPv4 Dataset **



* https://ipv6hitlist.github.io/
** https://censys.com/

Data Collection Pipeline

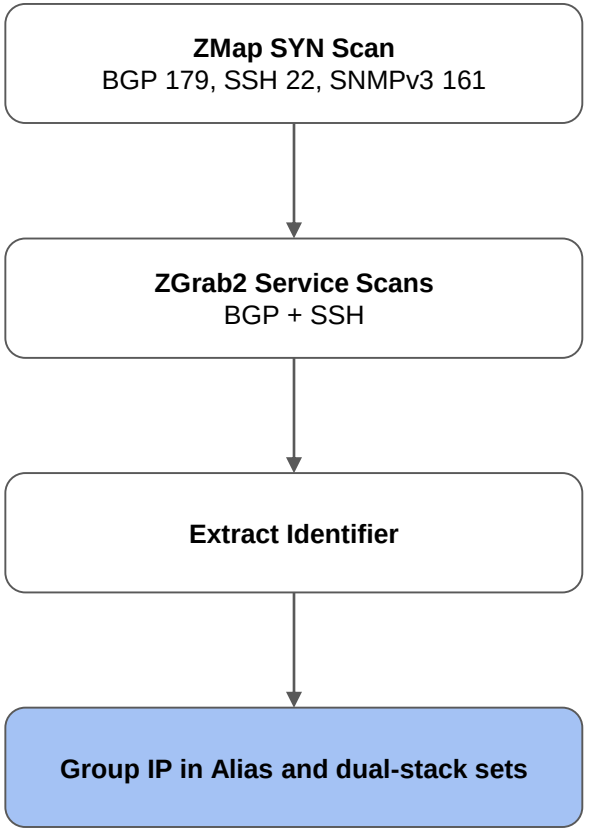
- Active Measurements
  - IPv4: all routable addresses
  - IPv6: Hitlist Service *
  - SSH 22, BGP 179, SNMPv3 161
- Censys IPv4 Dataset **



* https://ipv6hitlist.github.io/
** https://censys.com/

Data Collection Pipeline

- Active Measurements
  - IPv4: all routable addresses
  - IPv6: Hitlist Service *
  - SSH 22, BGP 179, SNMPv3 161
- Censys IPv4 Dataset **



* https://ipv6hitlist.github.io/
** https://censys.com/

Alias Sets

	IPv4			IPv6
Source	Active	Censys	Union	Active
SSH	505k (3.2M)	699k (4.6M)	926k (5.7M)	47k (226k)
BGP	12k (175k)	12k (175k)	12k (175k)	8.3k (48k)
SNMPv3	557k (6.1M)	n/a	557k (6.1M)	16.7k (71k)
Union	1.04M	708k	1.4M (11.8M)	66k

Alias Sets

	IPv4			IPv6
Source	Active	Censys	Union	Active
SSH	505k (3.2M)	699k (4.6M)	926k (5.7M)	47k (226k)
BGP	12k (175k)	12k (175k)	12k (175k)	8.3k (48k)
SNMPv3	557k (6.1M)	n/a	557k (6.1M)	16.7k (71k)
Union	1.04M	708k	1.4M (11.8M)	66k

Alias Sets

	IPv4			IPv6
Source	Active	Censys	Union	Active
SSH	505k (3.2M)	699k (4.6M)	926k (5.7M)	47k (226k)
BGP	12k (175k)	12k (175k)	12k (175k)	8.3k (48k)
SNMPv3	557k (6.1M)	n/a	557k (6.1M)	16.7k (71k)
Union	1.04M	708k	1.4M (11.8M)	66k

Alias Sets

	IPv4			IPv6
Source	Active	Censys	Union	Active
SSH	505k (3.2M)	699k (4.6M)	926k (5.7M)	47k (226k)
BGP	12k (175k)	12k (175k)	12k (175k)	8.3k (48k)
SNMPv3	557k (6.1M)	n/a	557k (6.1M)	16.7k (71k)
Union	1.04M	708k	1.4M (11.8M)	66k

Alias Sets

	IPv4			IPv6
Source	Active	Censys	Union	Active
SSH	505k (3.2M)	699k (4.6M)	926k (5.7M)	47k (226k)
BGP	12k (175k)	12k (175k)	12k (175k)	8.3k (48k)
SNMPv3	557k (6.1M)	n/a	557k (6.1M)	16.7k (71k)
Union	1.04M	708k	1.4M (11.8M)	66k

Alias Sets

	IPv4			IPv6
Source	Active	Censys	Union	Active
SSH	505k (3.2M)	699k (4.6M)	926k (5.7M)	47k (226k)
BGP	12k (175k)	12k (175k)	12k (175k)	8.3k (48k)
SNMPv3	557k (6.1M)	n/a	557k (6.1M)	16.7k (71k)
Union	1.04M	708k	1.4M (11.8M)	66k

- 97% of IPs respond to one protocol
- SNMPv3-only: 40% in IPv4, 25% in IPv6

Dual Stack Sets

	IPv4 Addresses	IPv6 Addresses	Dual Stack Sets
SSH	1.05M	771k	634k
BGP	78k	16.3k	4.2k
SNMPv3	1.1M	45k	21k
Union	2.2M	830k	650k

Dual Stack Sets

	IPv4 Addresses	IPv6 Addresses	Dual Stack Sets
SSH	1.05M	771k	634k
BGP	78k	16.3k	4.2k
SNMPv3	1.1M	45k	21k
Union	2.2M	830k	650k

Dual Stack Sets

	IPv4 Addresses	IPv6 Addresses	Dual Stack Sets
SSH	1.05M	771k	634k
BGP	78k	16.3k	4.2k
SNMPv3	1.1M	45k	21k
Union	2.2M	830k	650k

Dual Stack Sets

	IPv4 Addresses	IPv6 Addresses	Dual Stack Sets
SSH	1.05M	771k	634k
BGP	78k	16.3k	4.2k
SNMPv3	1.1M	45k	21k
Union	2.2M	830k	650k

Dual Stack Sets

	IPv4 Addresses	IPv6 Addresses	Dual Stack Sets
SSH	1.05M	771k	634k
BGP	78k	16.3k	4.2k
SNMPv3	1.1M	45k	21k
Union	2.2M	830k	650k

IPv6 only sets:

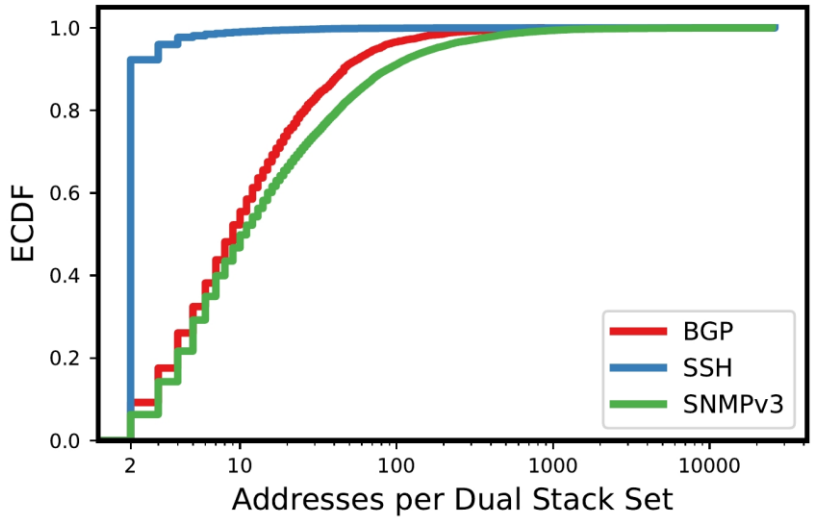
- SSH: 22.8%
- BGP: 75%
- SNMPv3: 86%

Why?

- Different v4/v6 security policies *
- IPv6 hosts only

* Jakub Czyz, Matthew Luckie, Mark Allman, and Michael Bailey. 2016. Don’t Forget to Lock the Back Door! A Characterization of IPv6 Network Security Policy

Dual Stack Set Size



- 90% SSH contains a single IPv4 and a single IPv6 addresses
- BGP and SNMPv3 10-100 addresses

Validation

- Compare a random sample with MIDAR
- Cross protocol validation
- Only consider exact match
- Disagreements due to lack of response on all interfaces

	Sample Size	Agree	Disagree
SSH-MIDAR	**8.5k**	**8.1K**	**366**
SSH-BGP	**1.34k**	**1.29k**	**52**
SSH-SNMPv3	**13.6k**	**13.2k**	**398**
BGP-SNMPv3	**1.84k**	**1.76k**	**87**

Validation

- Compare a random sample with MIDAR
- Cross protocol validation
- Only consider exact match
- Disagreements due to lack of response on all interfaces

	Sample Size	Agree	Disagree
SSH-MIDAR	**8.5k**	**8.1K**	**366**
SSH-BGP	**1.34k**	**1.29k**	**52**
SSH-SNMPv3	**13.6k**	**13.2k**	**398**
BGP-SNMPv3	**1.84k**	**1.76k**	**87**

Validation

- Compare a random sample with MIDAR
- Cross protocol validation
- Only consider exact match
- Disagreements due to lack of response on all interfaces

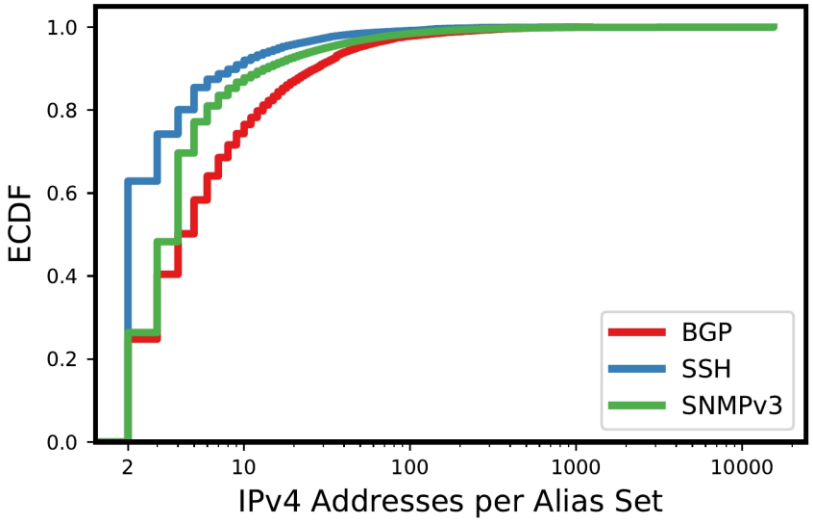
	Sample Size	Agree	Disagree
SSH-MIDAR	**8.5k**	**8.1K**	**366**
SSH-BGP	**1.34k**	**1.29k**	**52**
SSH-SNMPv3	**13.6k**	**13.2k**	**398**
BGP-SNMPv3	**1.84k**	**1.76k**	**87**

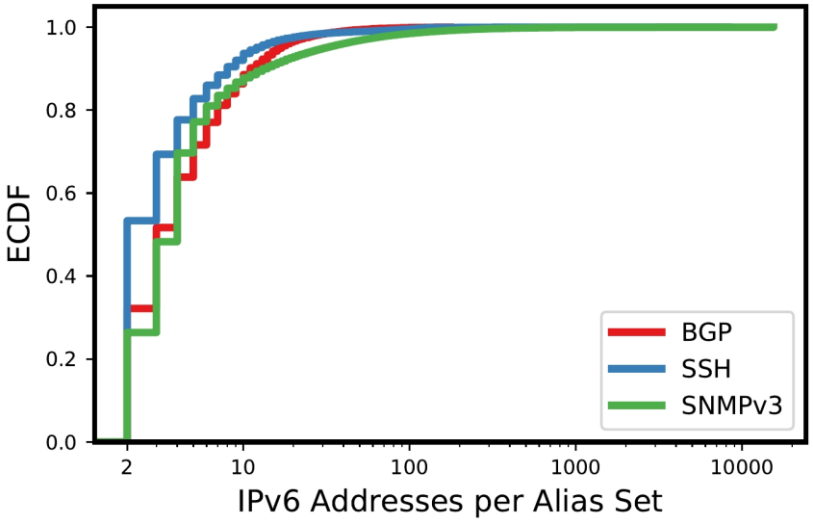
Conclusion

- Utilized a unique host identifier via SSH and BGP:
  - Resolve IP alias in IPv4 and IPv6
  - Infer dual stack hosts
- Largest alias and dual-stack sets to date
- Complement existing work
- Data available at https://routerfingerprinting.github.io/

European Research Council
Established by the European Commission

Alias Set Size





- Most sets contains less that 100 IPs
- SSH mostly 2 IPs per set
- BGP and SNMPv3 likely to contain more IPs per set

Scanning Results

	Active measurements		Censys		Union	
Protocol	# IPs	# ASN	# IPs	# ASN	# IPs	# ASN
SSH	15.9M	46.1k	21.7M	47.6k	24.4M	48.9k
BGP	364k	6.5k	391k	7k	409k	7.5k
SNMPv3	20.8M	50.2k	n.a	n.a	n.a	n.a
Union	36.7M	59.6k	22.1M	48.5k	24.7M	49.7k
SSH (IPv6)	1.01M	10.8k	n.a	n.a	n.a	n.a
BGP (IPv6)	67k	3.1k	n.a	n.a	n.a	n.a
SNMPv3 (IPv6)	337k	10.8k	n.a	n.a	n.a	n.a
Union	1.3M	14.4k				