Detecting IPv4 Subnets in the Wild

Taha Albakour, **Fariba Osali**,
Max Franke, Georgios Smaragdakis

MAX-PLANCK-INSTITUT FÜR INFORMATIK
UNIVERSITÄT DES SAARLANDES
Technische Universität Berlin
TU Delft

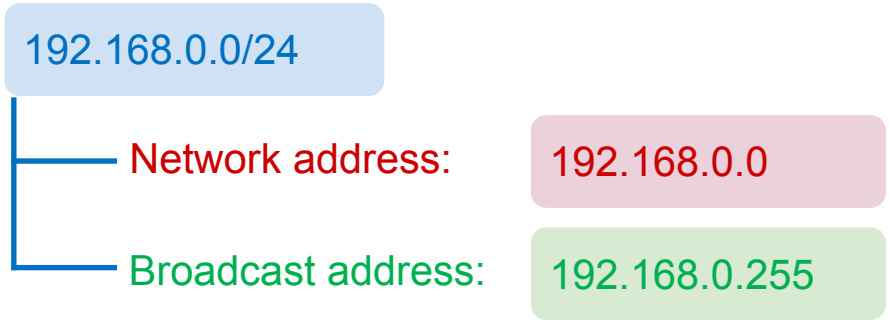
Why Measure Subnets?

- BGP exposes prefixes, not subnets
- Better topology inference
- Better IPv4 resource utilization & network operations
- Abuse handling and blocklisting, geolocations (RFC 9977)

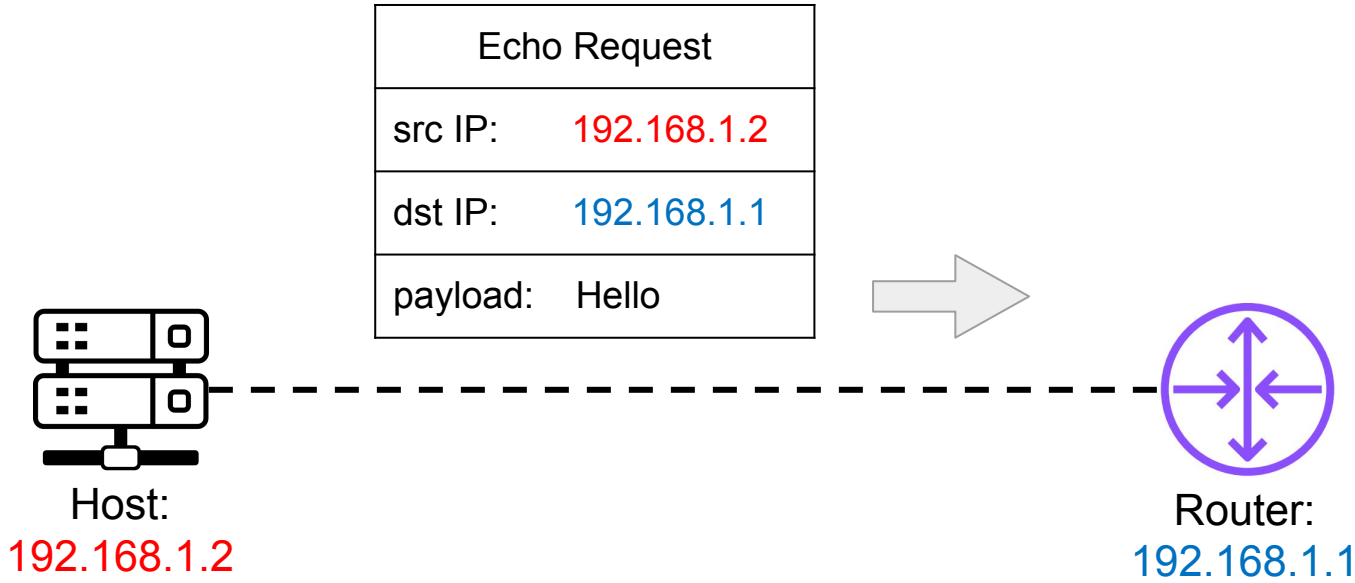
Methodology Overview

- ICMP Echo
  - Infers subnet boundaries indirectly

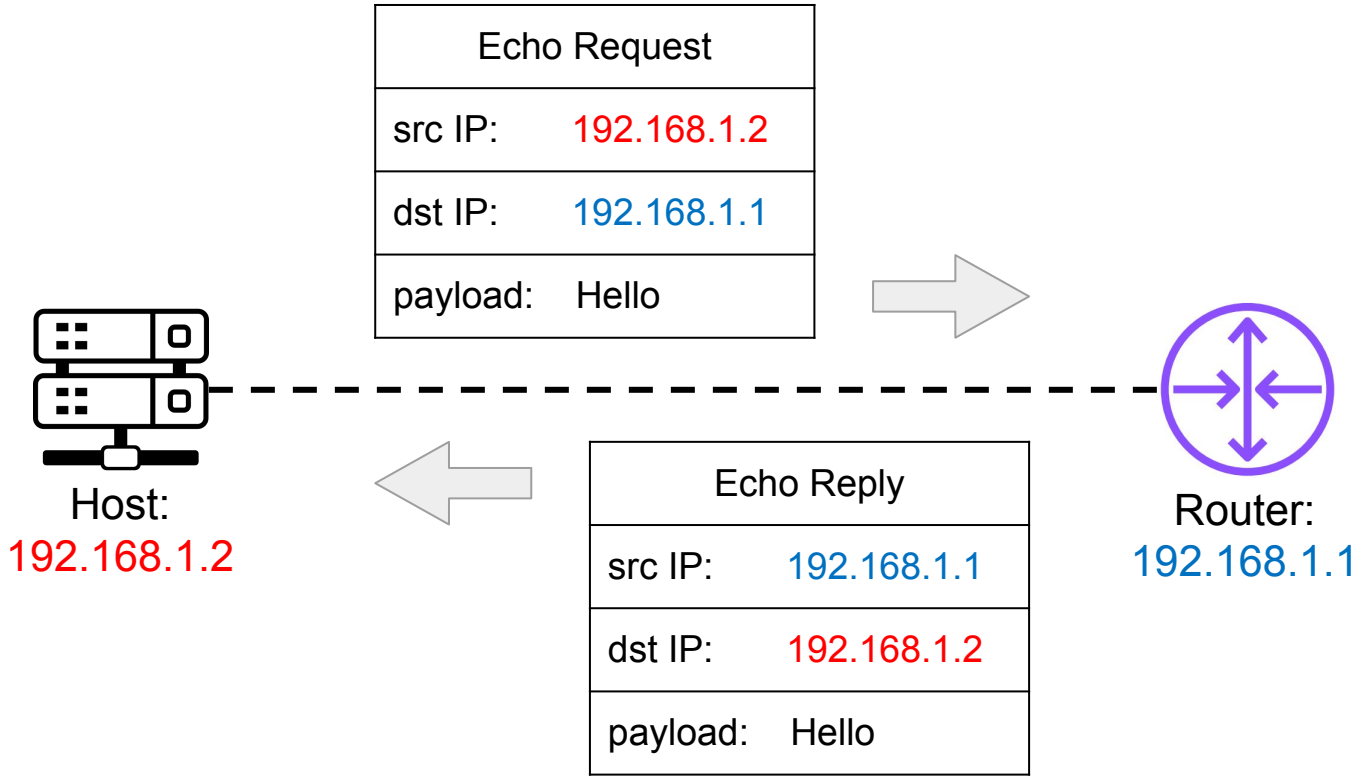
- ICMP Address Mask
  - Directly reveals the subnet mask



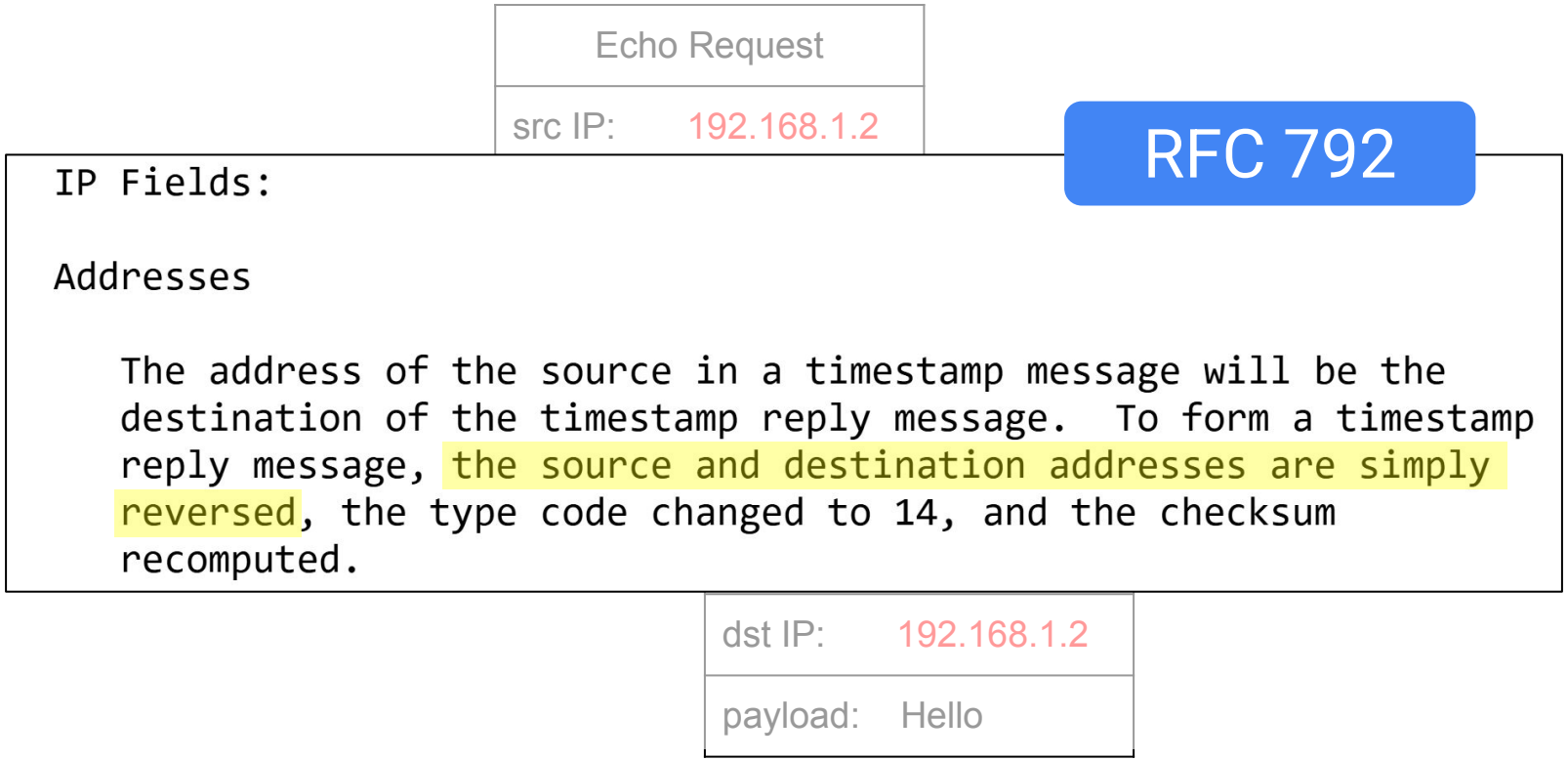
ICMP Messages



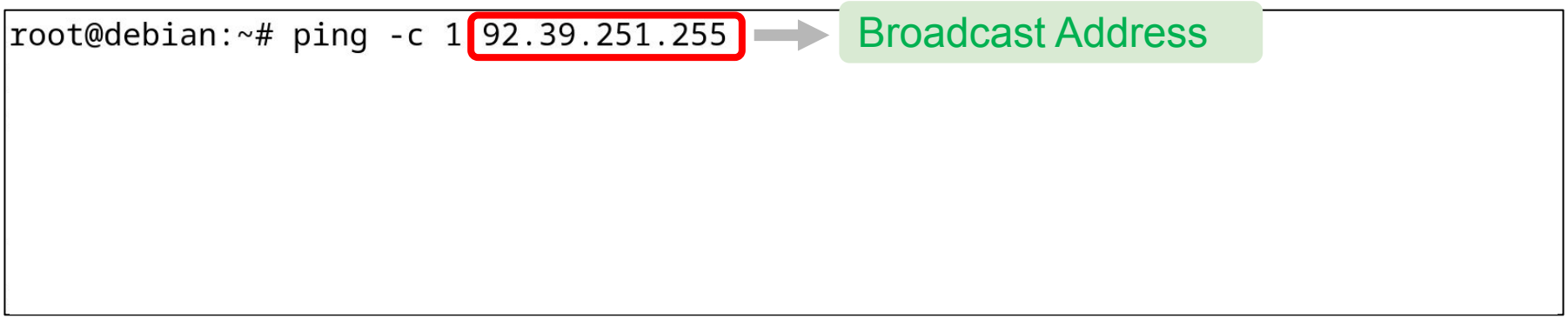
ICMP Messages



ICMP Messages



Source/Destination Mismatch



Source/Destination Mismatch

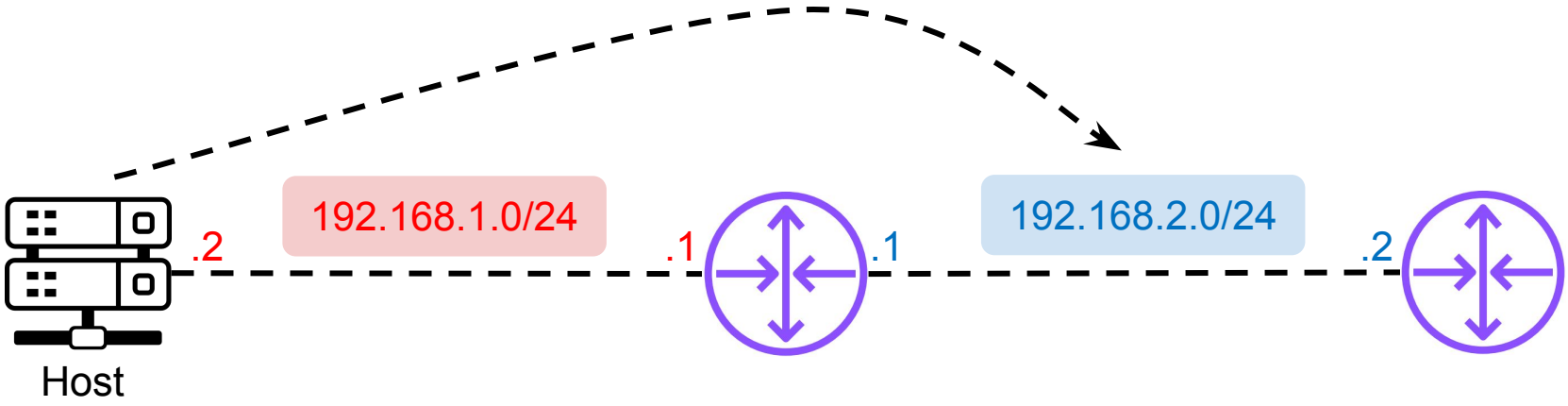
```
root@debian:~# ping -c 1 92.39.251.255
PING 92.39.251.255 (92.39.251.255) 56(84) bytes of data.
64 bytes from 62.100.128.115: icmp_seq=1 ttl=248 time=19.4 ms (DIFFERENT ADDRESS!)

--- 92.39.251.255 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 19.353/19.353/19.353/0.000 ms
```

Broadcast Address

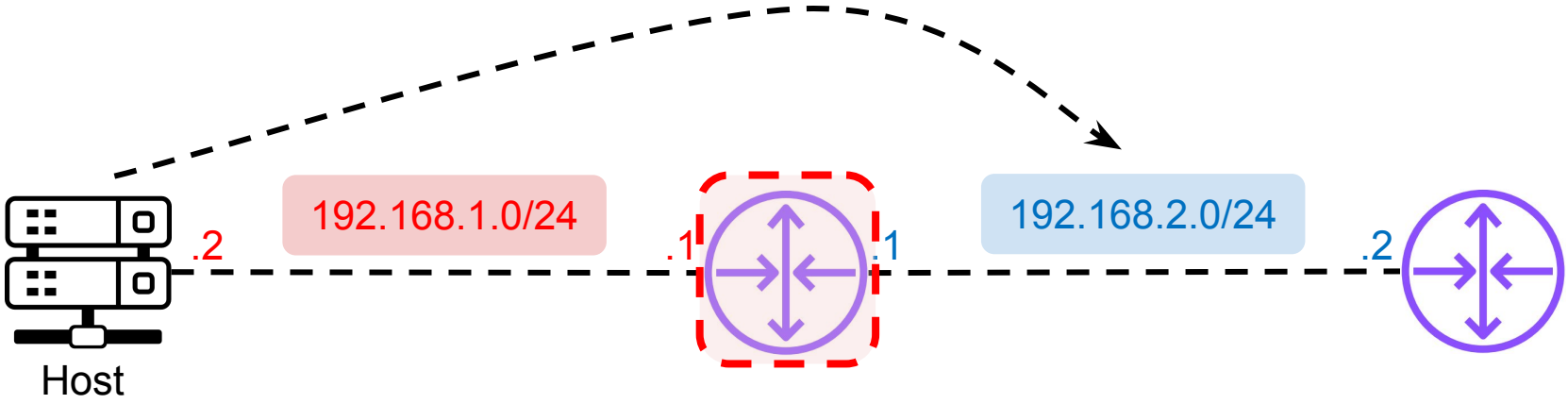
Reasons for Mismatch

- Loopback address
- Load balancer
- Multi-home egress selection
- …
- **Handling of network/broadcast address**

Lab Testing

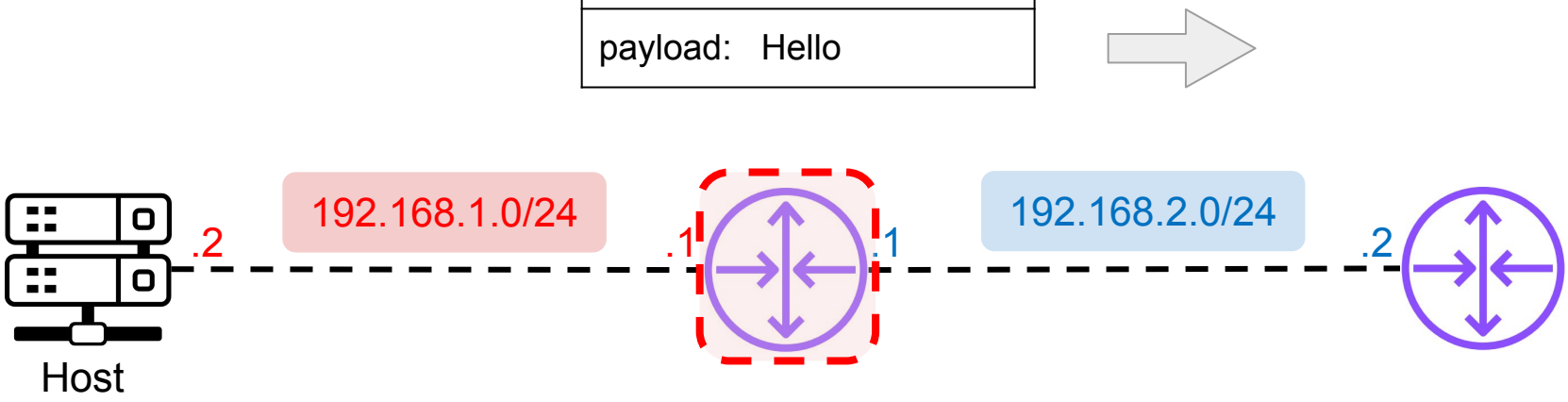


Lab Testing

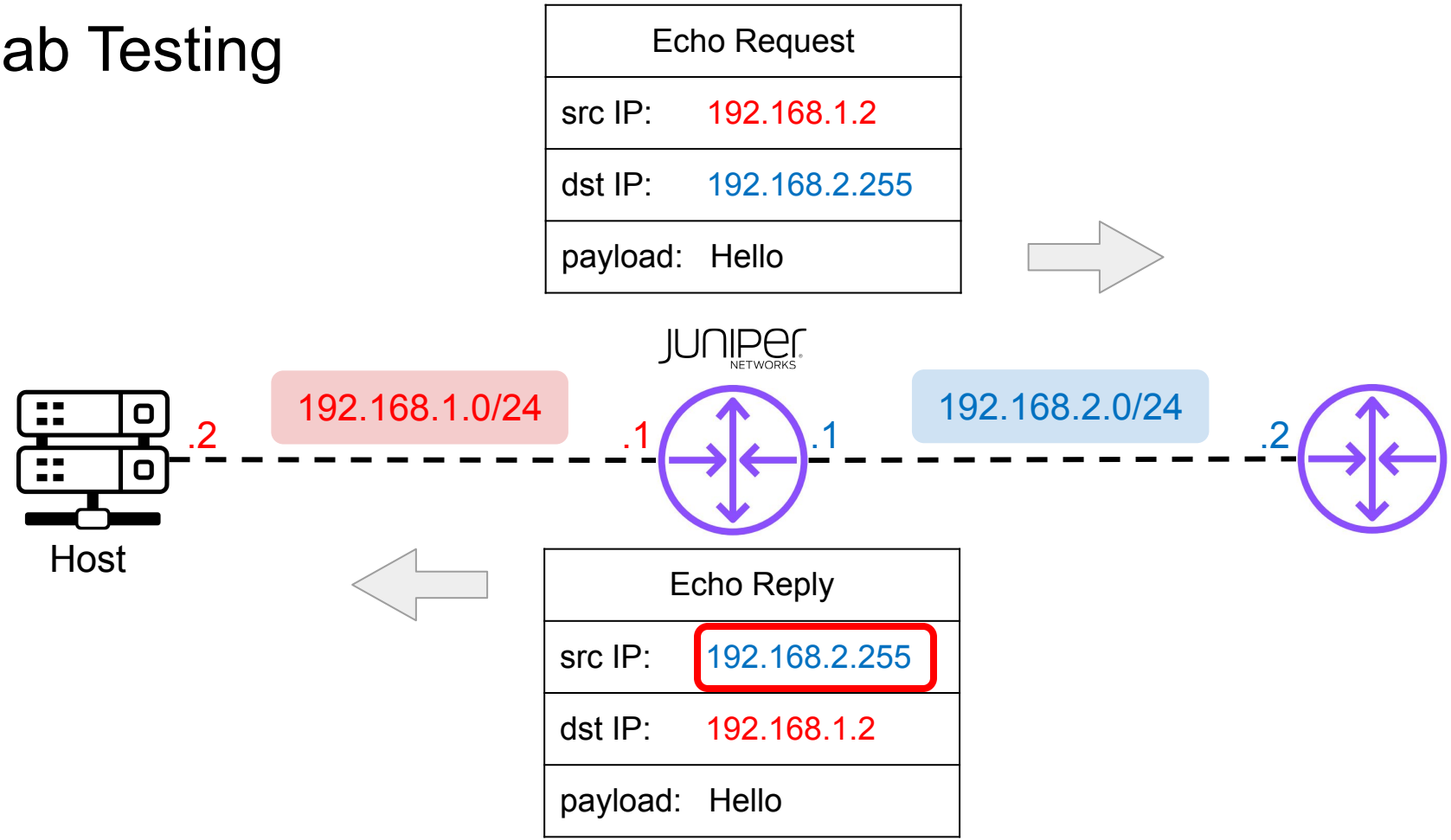


Lab Testing

Echo Request	
src IP:	192.168.1.2
dst IP:	192.168.2.255
payload:	Hello

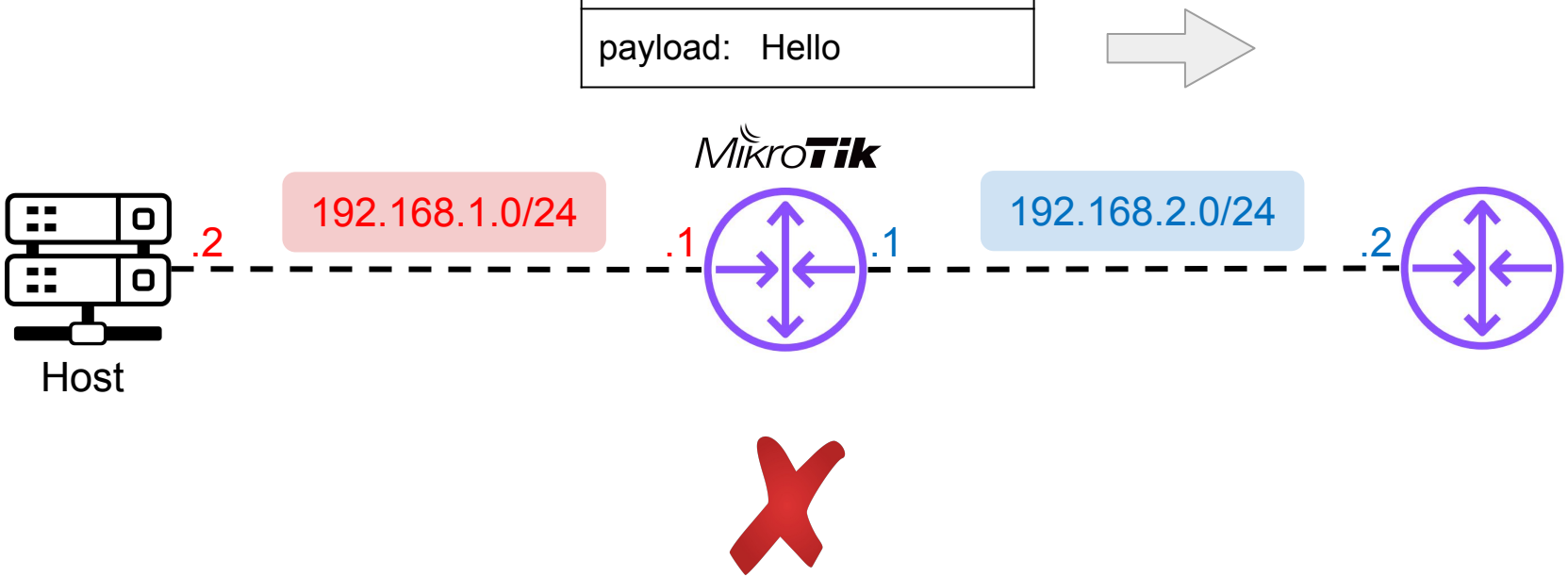


Lab Testing

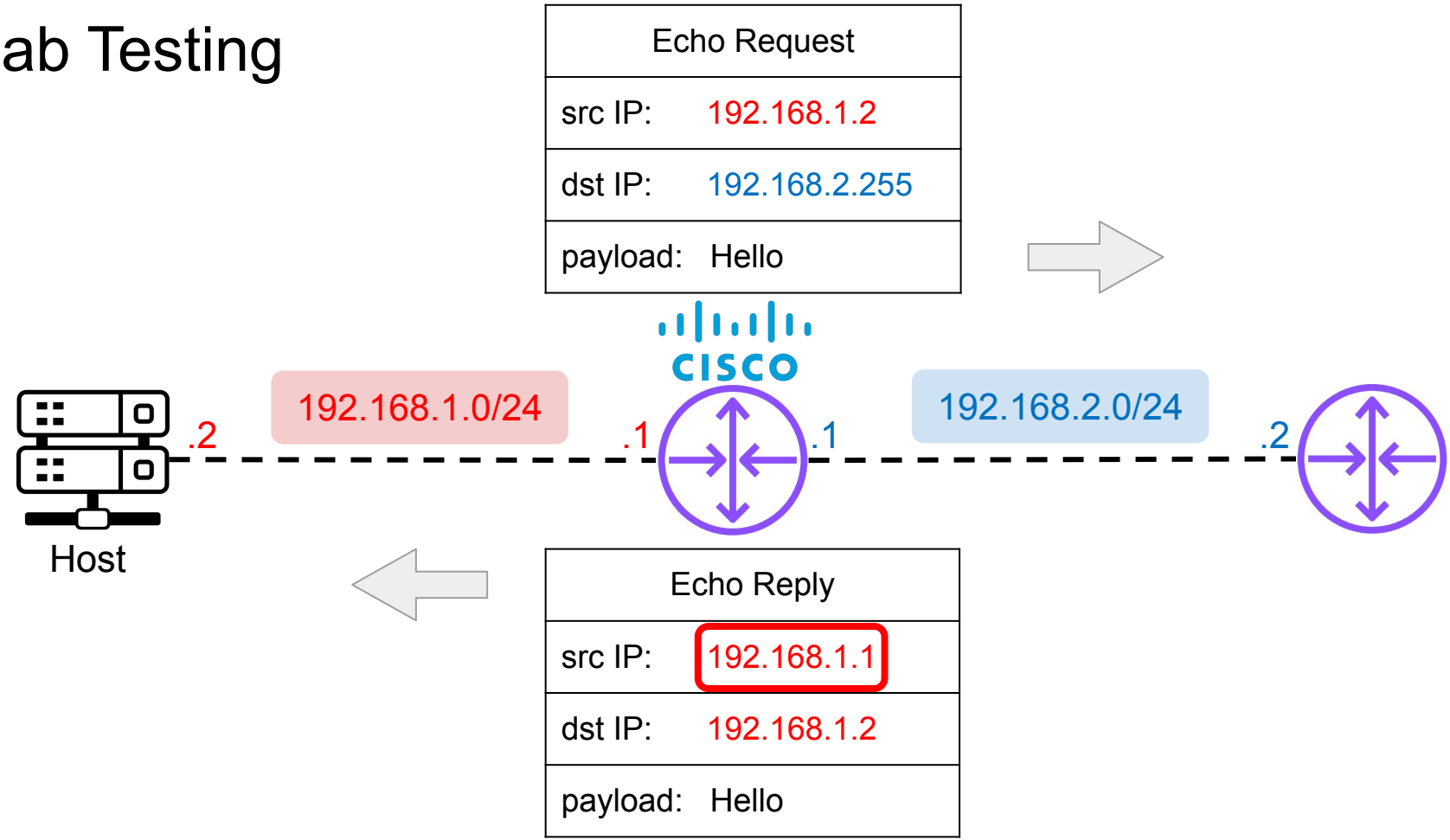

Echo Request
src IP: 192.168.1.2
dst IP: 192.168.2.255
payload: Hello
JUNIPER NETWORKS
192.168.1.0/24
192.168.2.0/24
.2
.1
.1
.2
Host
Echo Reply
src IP: 192.168.2.255
dst IP: 192.168.1.2
payload: Hello

Lab Testing

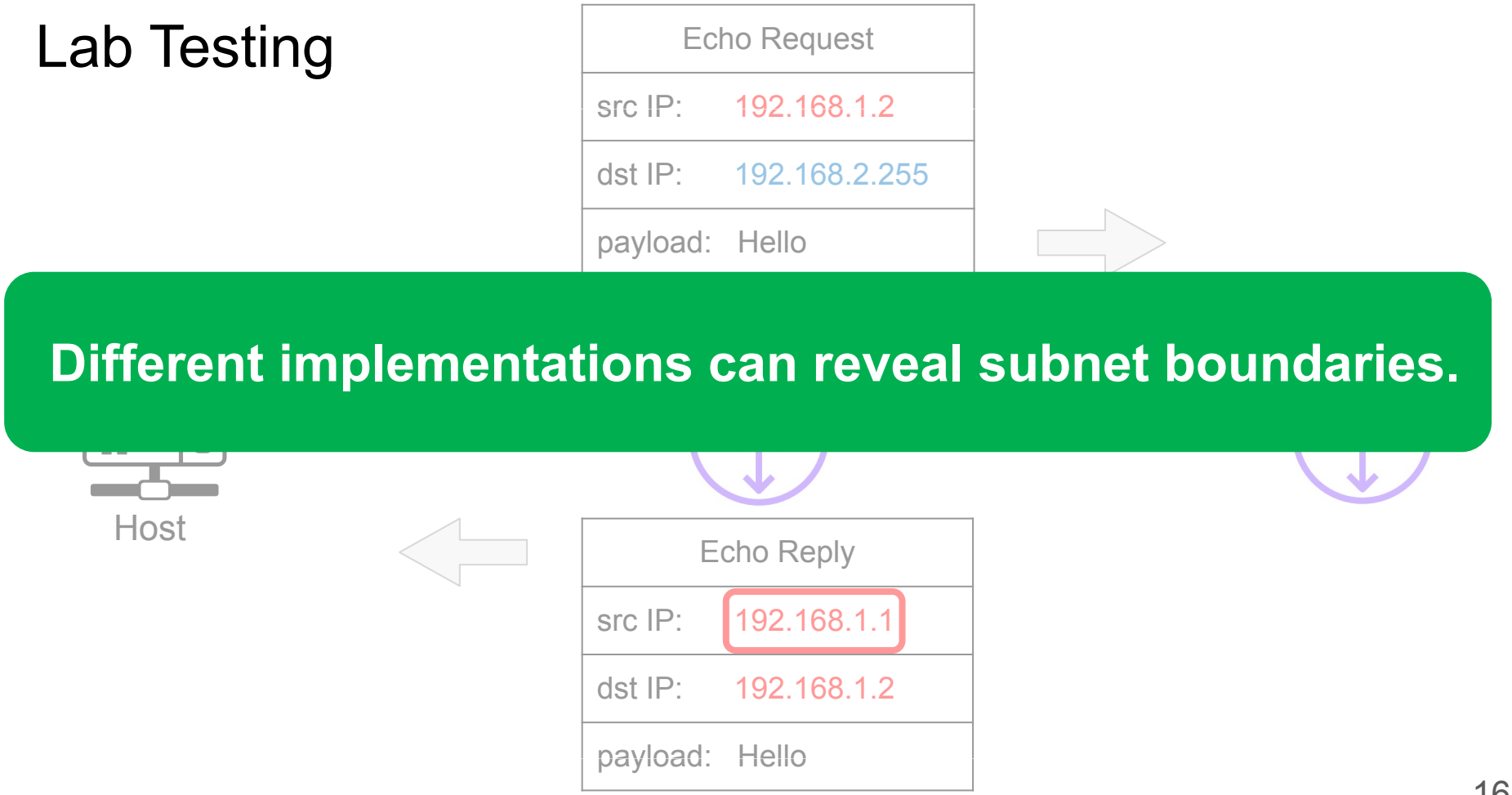
Echo Request	
src IP:	192.168.1.2
dst IP:	192.168.2.255
payload:	Hello



Lab Testing

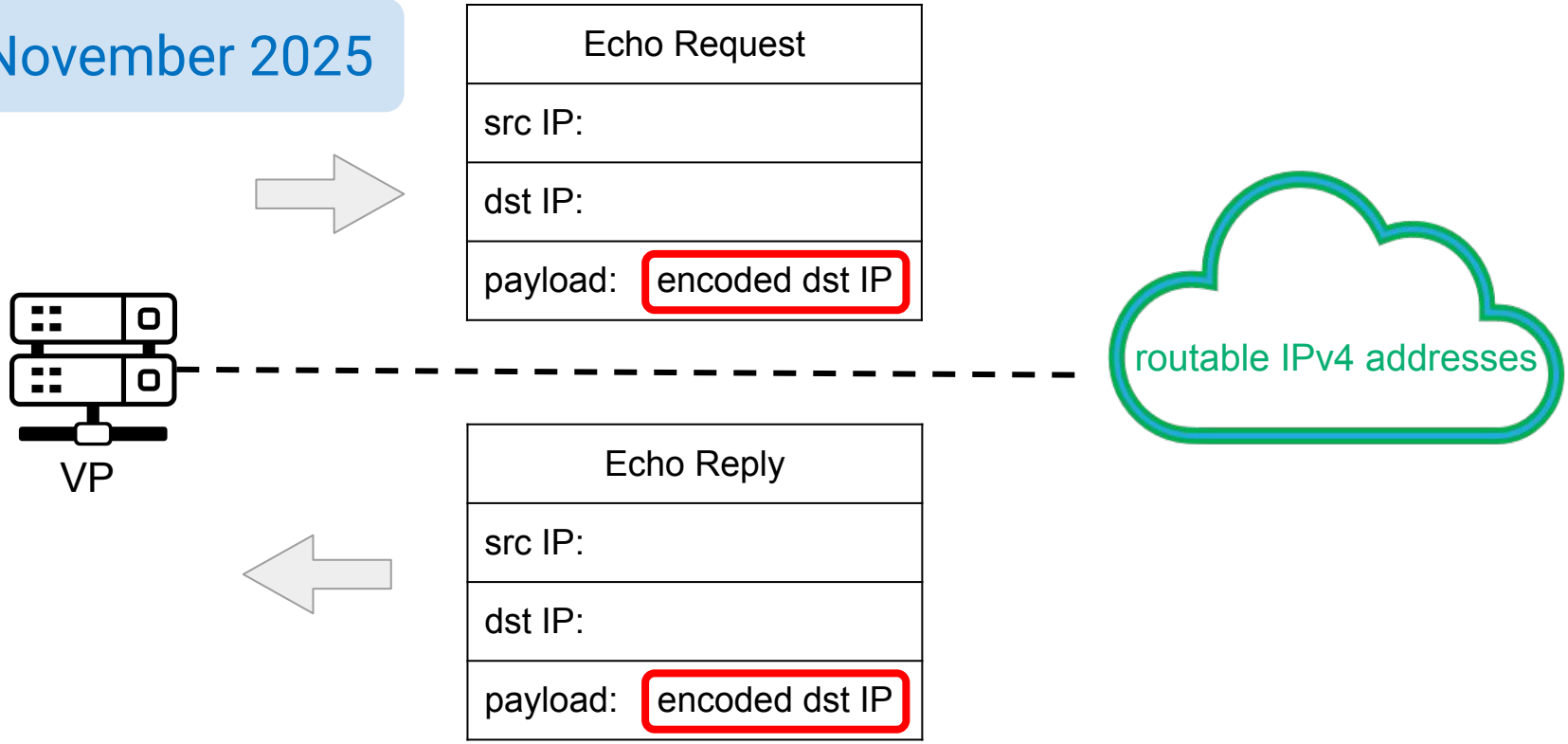

Echo Request
src IP: 192.168.1.2
dst IP: 192.168.2.255
payload: Hello
CISCO
192.168.1.0/24
192.168.2.0/24
.2
.1
.1
.2
Host
Echo Reply
src IP: 192.168.1.1
dst IP: 192.168.1.2
payload: Hello

Lab Testing


Echo Request
src IP: 192.168.1.2
dst IP: 192.168.2.255
payload: Hello
Different implementations can reveal subnet boundaries.
Host
Echo Reply
src IP: 192.168.1.1
dst IP: 192.168.1.2
payload: Hello

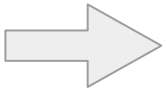
Measurement

November 2025

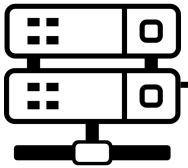


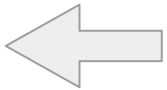
Measurement (Expected)

November 2025



Echo Request	
src IP:	A.A.A.A
dst IP:	B.B.B.B
payload:	B.B.B.B



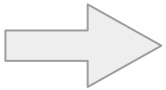


Echo Reply	
src IP:	B.B.B.B
dst IP:	A.A.A.A
payload:	B.B.B.B

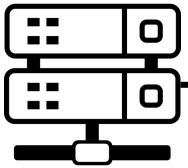
RFC 792

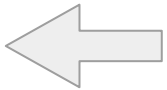
Measurement (Mismatch)

November 2025



Echo Request	
src IP:	A.A.A.A
dst IP:	B.B.B.B
payload:	B.B.B.B





Echo Reply	
src IP:	C.C.C.C
dst IP:	A.A.A.A
payload:	B.B.B.B

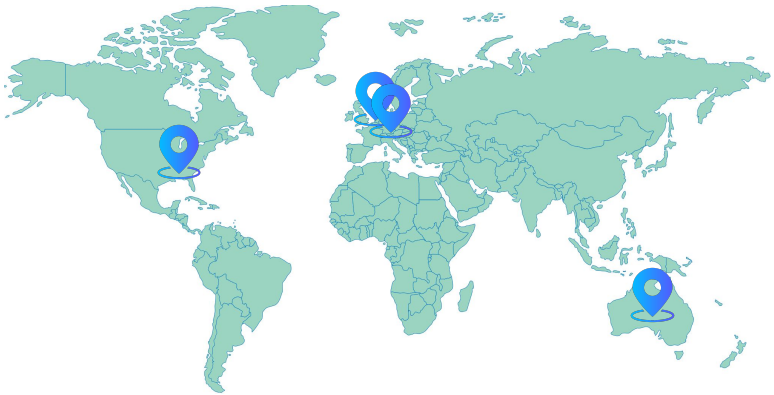
RFC 792

Detected Subnets and Vantage Point Impact

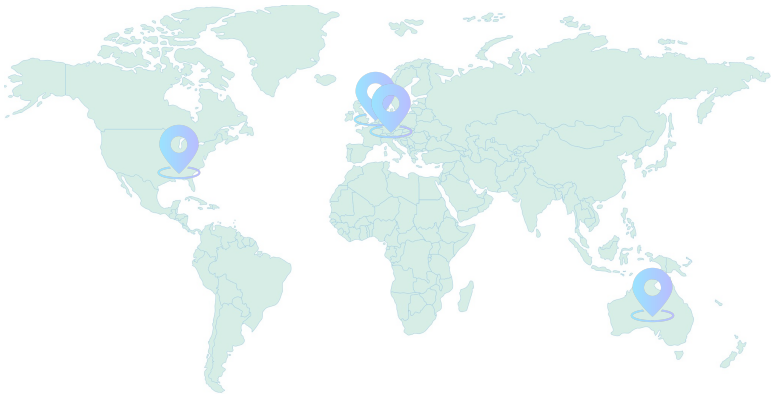
	Address	Subnet
ICMP Echo	5.2M	2.05M

Detected Subnets and Vantage Point Impact

	Address	Subnet
ICMP Echo	5.2M	2.05M

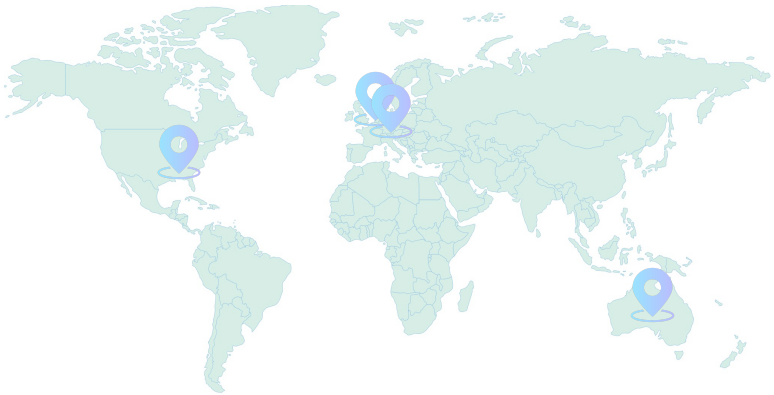


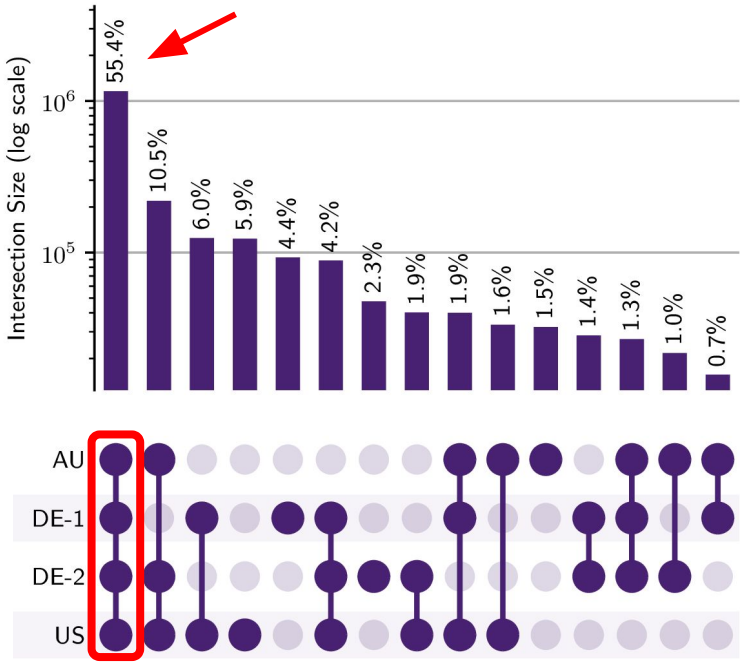
Detected Subnets and Vantage Point Impact



Detected Subnets and Vantage Point Impact

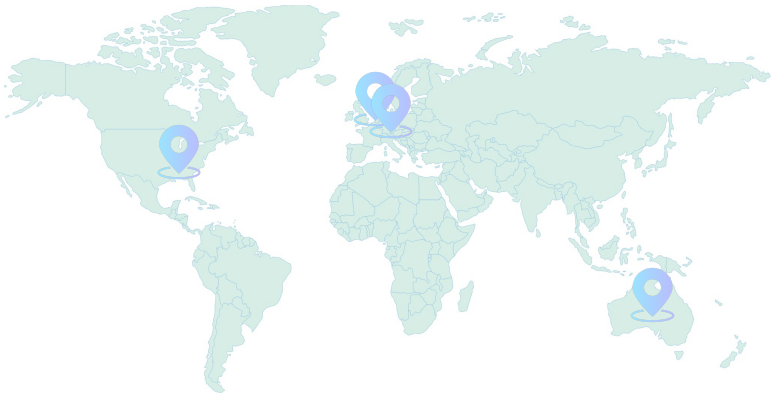
- 55% discovered by all VPs

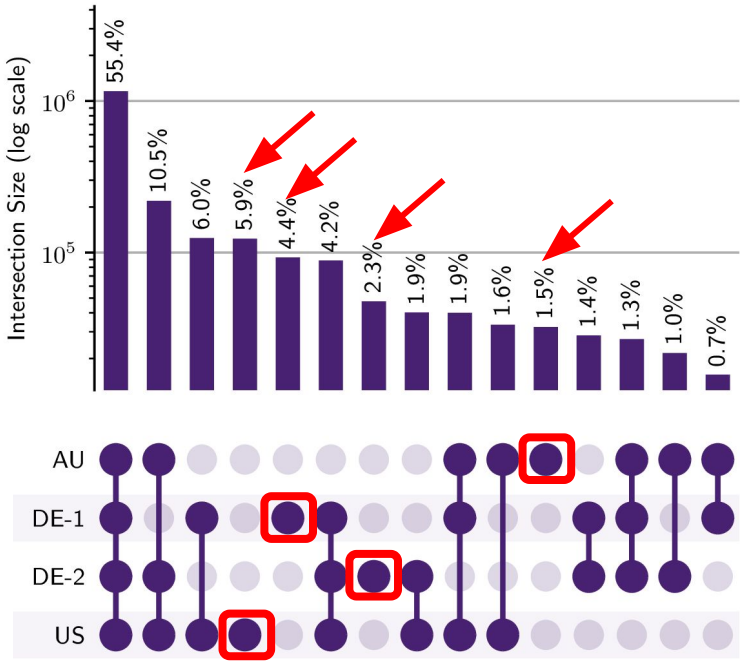




Detected Subnets and Vantage Point Impact

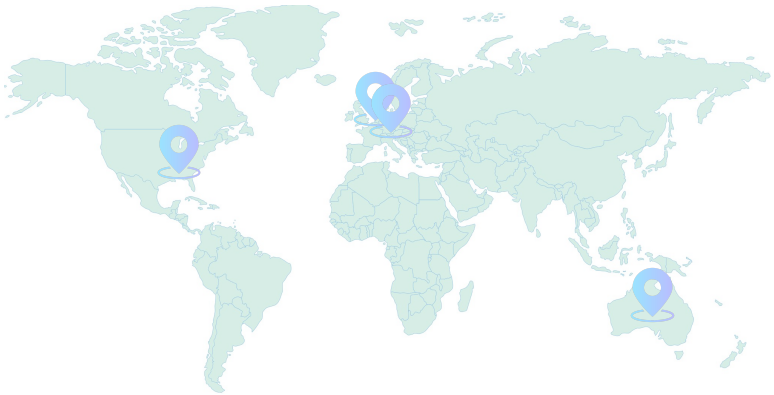
- 55% discovered by all VPs
- 14% discovered by only one VP

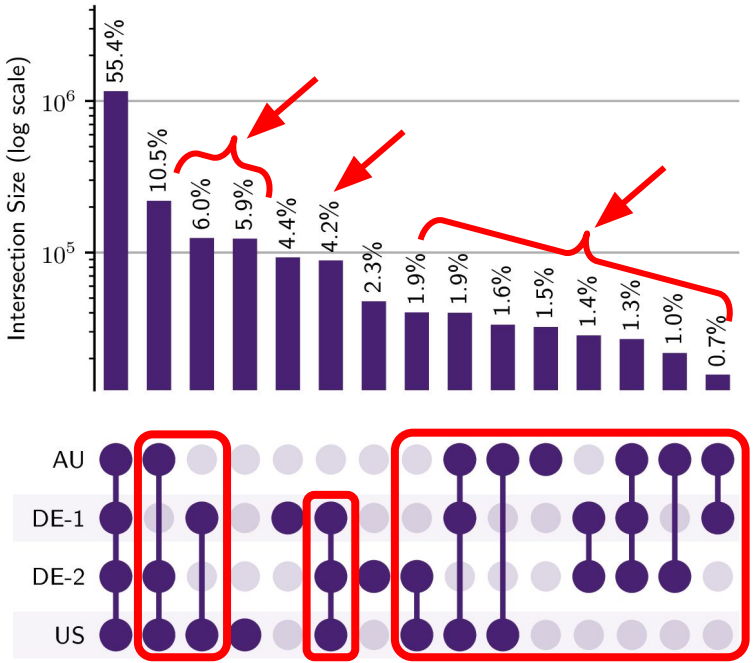




Detected Subnets and Vantage Point Impact

- 55% discovered by all VPs
- 14% discovered by only one VP
- 31% discovered by two or three VPs

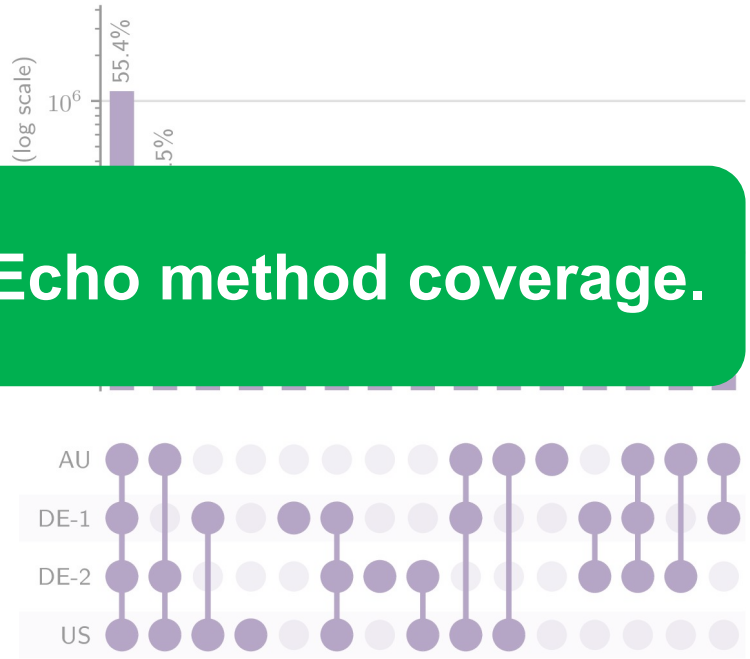




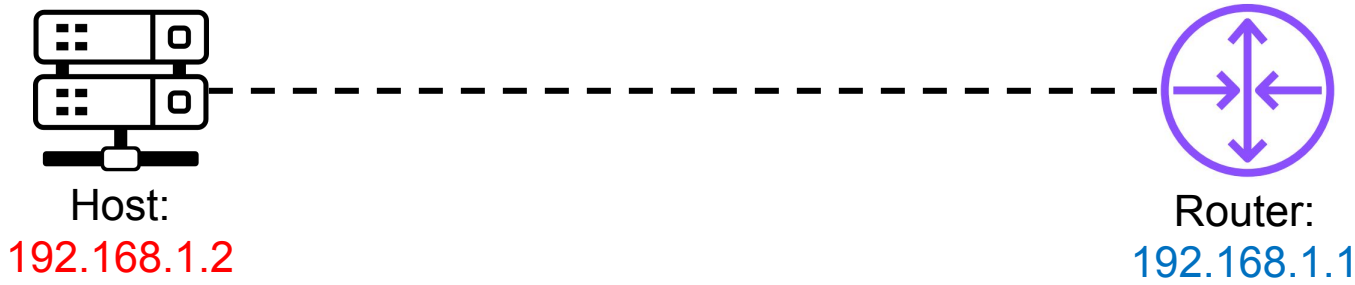
Detected Subnets and Vantage Point Impact

- 55% discovered by all VPs
- 14% discovered by only one VI

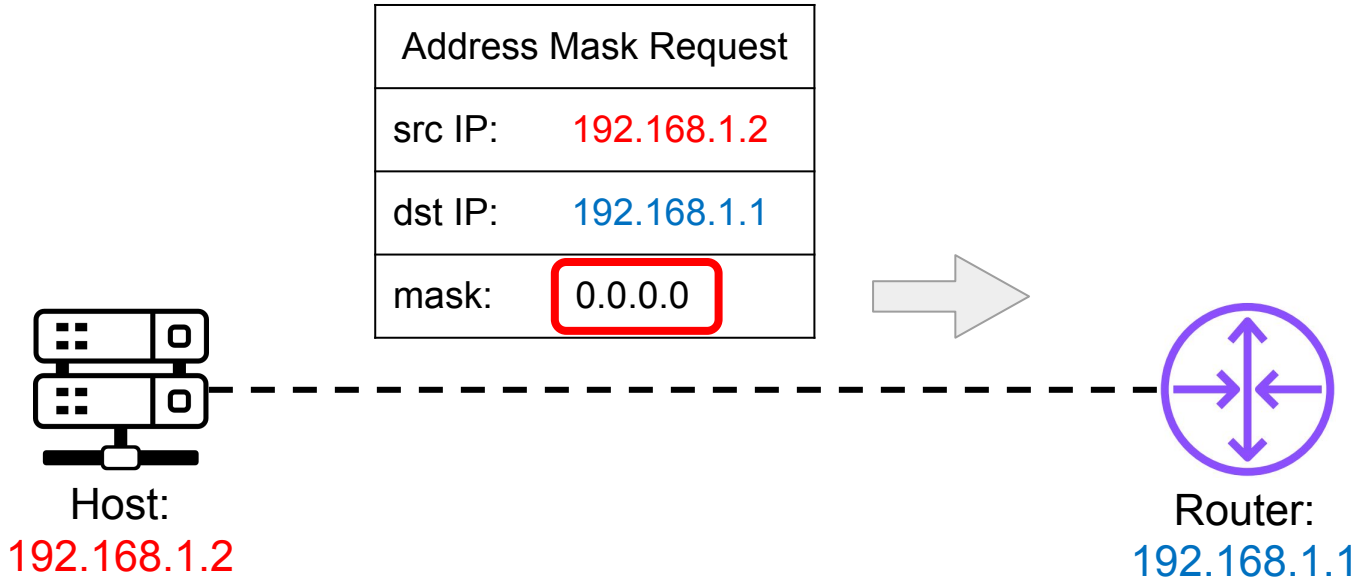
VPs can greatly affect the ICMP Echo method coverage.



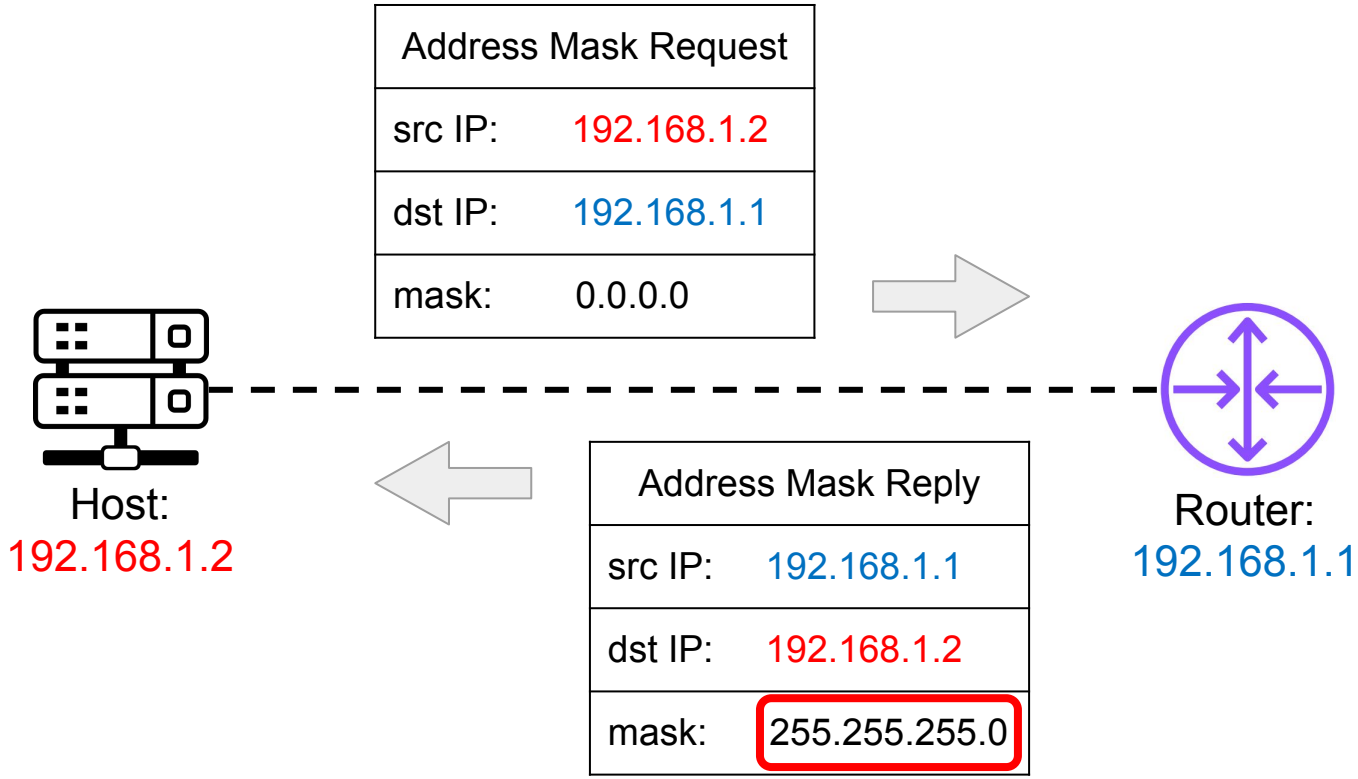
ICMP Address Mask



ICMP Address Mask



ICMP Address Mask

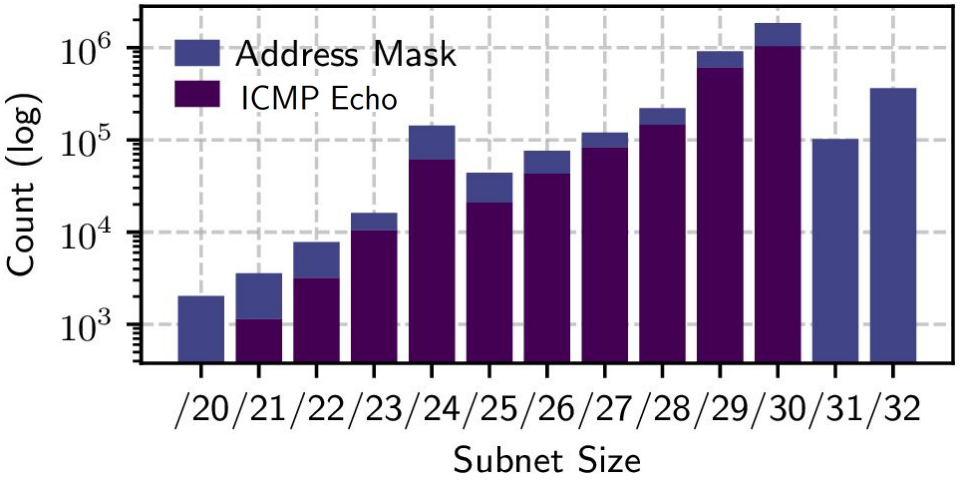


Detected Subnets in Both Methods

	Address	Subnet
ICMP Echo	5.2M	2.05M
Addr. Mask	2.31M	1.82M

Detected Subnets in Both Methods

	Address	Subnet
ICMP Echo	5.2M	2.05M
Addr. Mask	2.31M	1.82M

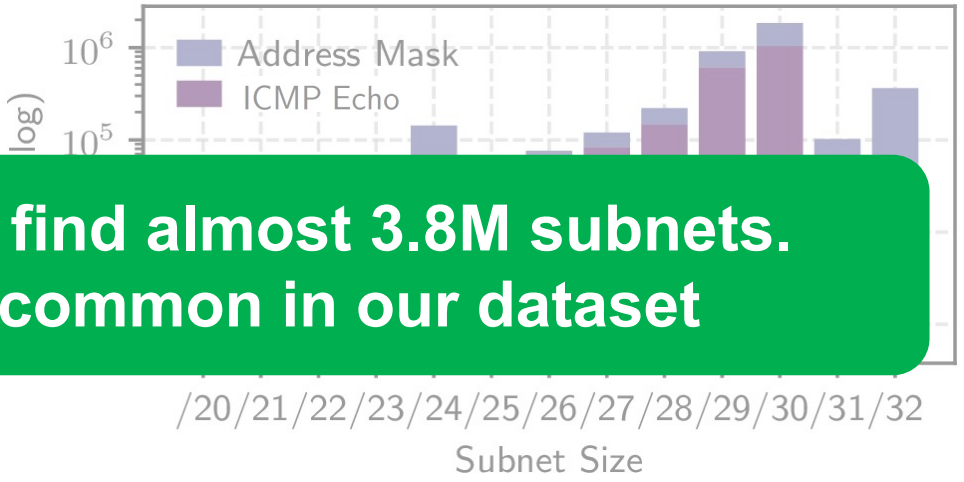


- 25k subnets with overlap in both methods

Detected Subnets in Both Methods

	Address	Subnet
ICMP Echo	5.2M	2.05M

With both methods, we find almost 3.8M subnets. /30 and /31 are most common in our dataset



- 25k subnets with overlap in both methods

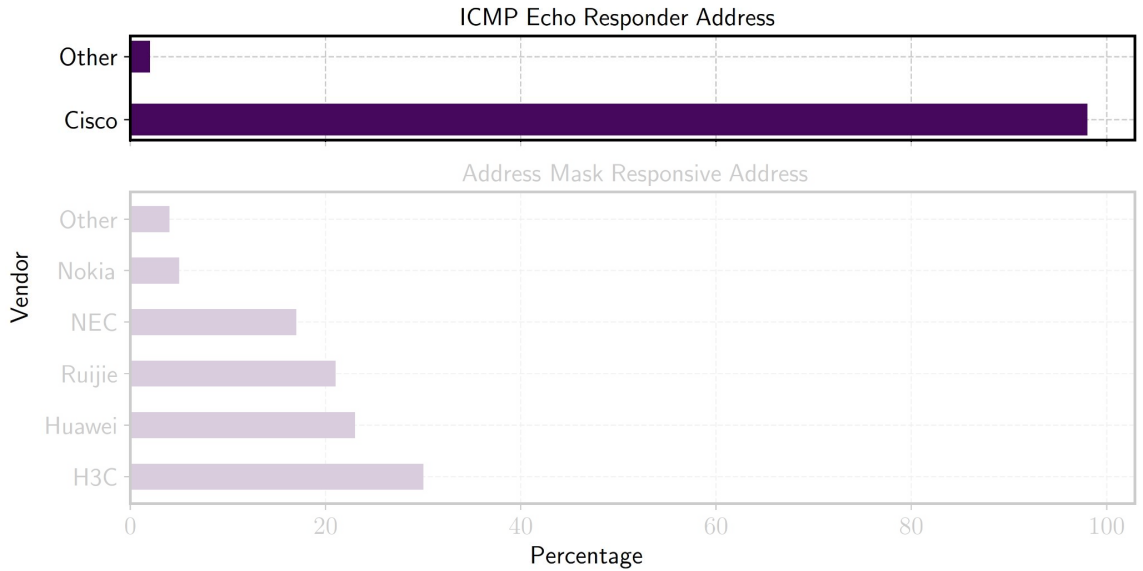
Vendor Patterns

- Fingerprinting using SNMPv3*

* Taha Albakour et al. 2021. Third Time's not a Charm: Exploiting SNMPv3 for Router Fingerprinting (IMC' 21) `

Vendor Patterns

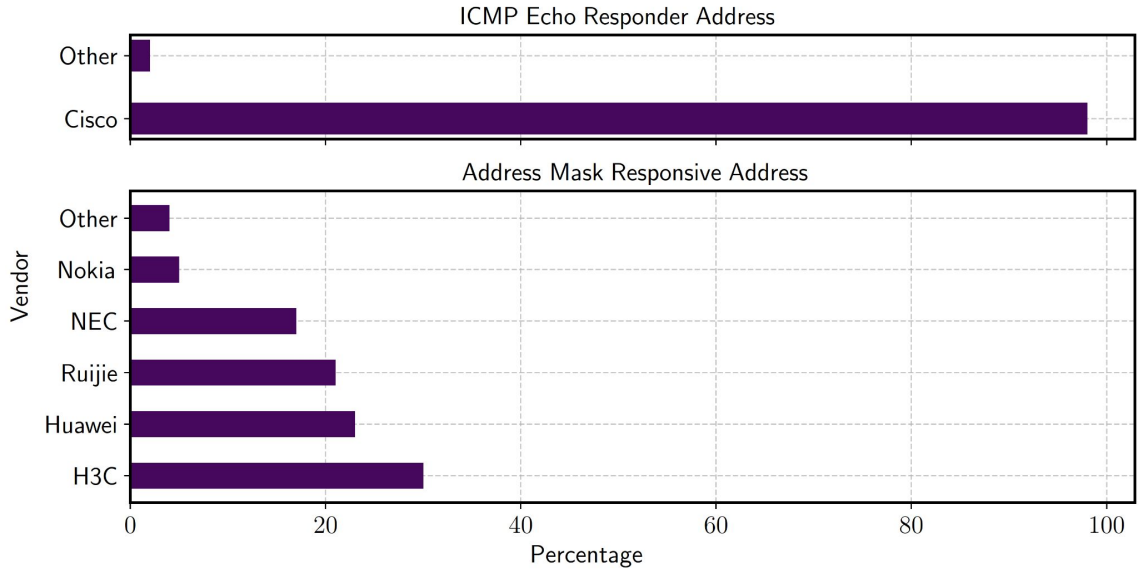
- Fingerprinting using SNMPv3*
- ICMP Echo: 44% of responder addresses identified
- Address Mask: 27% of responsive addresses identified



* Taha Albakour et al. 2021. Third Time's not a Charm: Exploiting SNMPv3 for Router Fingerprinting (IMC' 21) `

Vendor Patterns

- Fingerprinting using SNMPv3*
- ICMP Echo: 44% of responder addresses identified
- Address Mask: 27% of responsive addresses identified

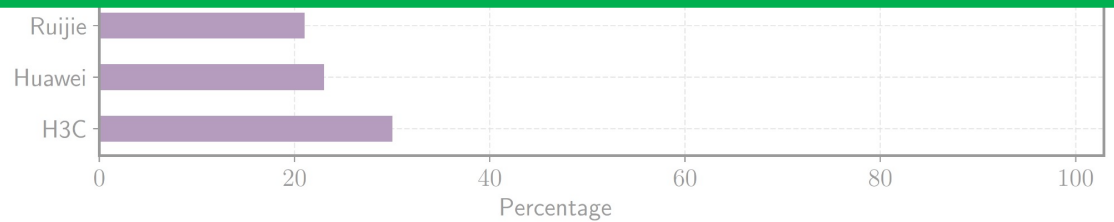


* Taha Albakour et al. 2021. Third Time's not a Charm: Exploiting SNMPv3 for Router Fingerprinting (IMC' 21) `

Vendor Patterns

- Fingerprinting using SNMPv3*
- ICMP Echo: 44% of responder addresses identified

The ICMP Echo method is only applicable to Cisco devices. In contrast, several vendors allow ICMP address mask replies by default, making this method applicable over the Internet.



* Taha Albakour et al. 2021. Third Time's not a Charm: Exploiting SNMPv3 for Router Fingerprinting (IMC' 21) `

Summary

We exploit ICMP quirks to detect subnets

- Lenient specifications and implementation differences
- 5.2M src/dst mismatch in ICMP Echo

Deprecated ICMP Address Mask Request

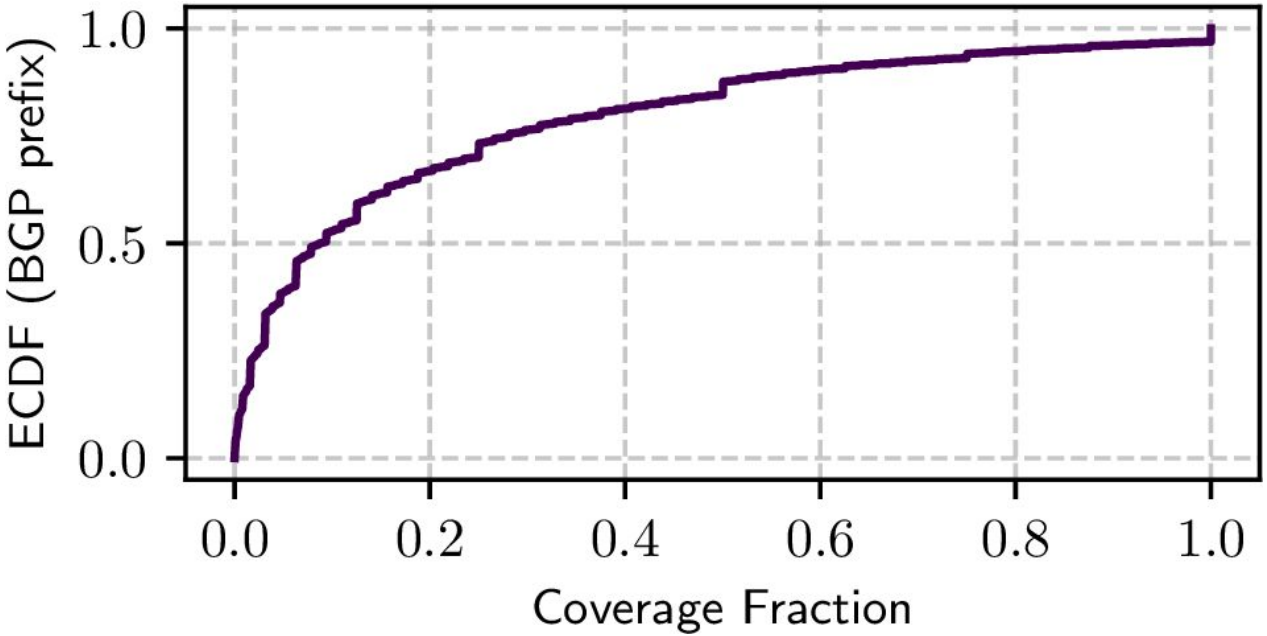
- More than 2M responsive addresses
- Multiple vendors enabled by default

Detect 3.8M subnets of varying sizes

Additional Slides

BGP Coverage

- 159.8k BGP prefixes (10%)
- 40% coverage for 20% prefixes



Exact Match in BGP Data

- 1.7% (35~k) of detected subnets have exact BGP prefix match
- Highest fraction of one-to-one match:
  - /24s (27k)
  - /22s (2.5k)
  - /23 (2.4k)
  - /20s (1k)

Remaining matches vary in size with /16s (50) and /32 (6)

Filtering Mismatch Response

192.168.0.0/30			
192.168.0.0	192.168.0.1	192.168.0.2	192.168.0.3
✓ 192.168.1.1	192.168.0.1	192.168.0.2	192.168.1.1
✗ 192.168.1.1	192.168.1.1	192.168.0.2	192.168.1.1
✗ 192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1
✗ 192.168.1.1	192.168.2.1	192.168.2.2	192.168.1.1