Third Time’s Not a Charm

Exploiting SNMPv3 for Router Fingerprinting

Taha Albakour, Oliver Gasser, Robert Beverly, and Georgios Smaragdakis.

Technische Universität Berlin berlin

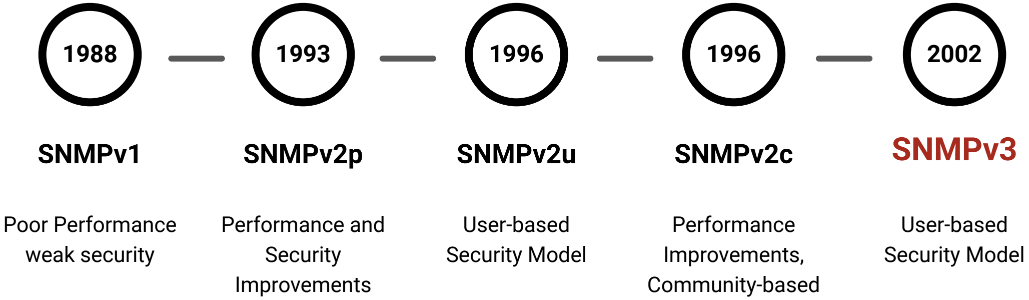
max planck institut informatik

NPS PRAESTANTIA PER SCIENTIAM 1909

TUDelft

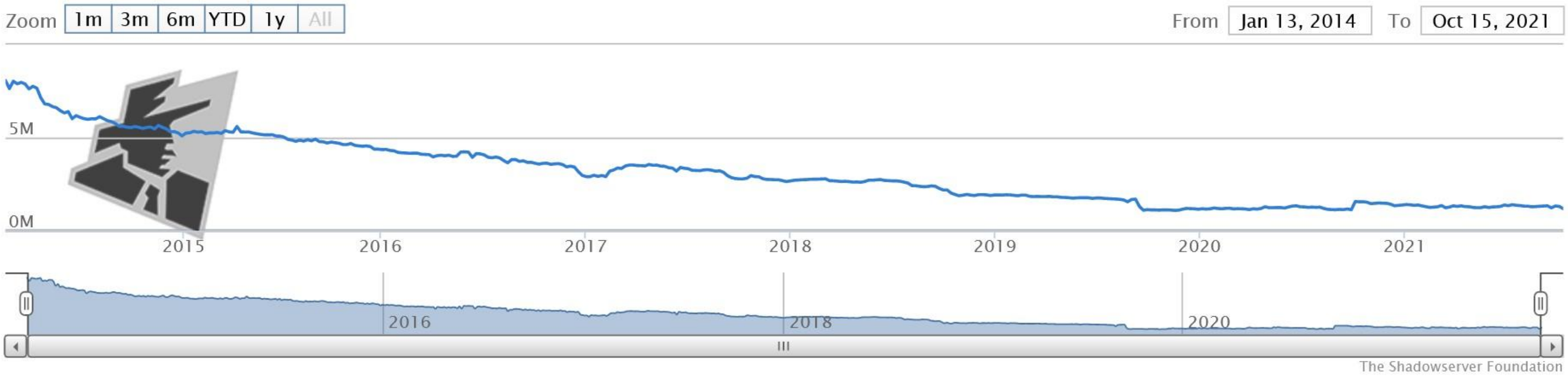
What is SNMP?

- Simple Network Management Protocol (SNMP)
- De facto network management protocol
- Multiple versions over the years



1988	1993	1996	1996	2002
SNMPv1	**SNMPv2p**	**SNMPv2u**	**SNMPv2c**	**SNMPv3**
Poor Performance weak security	Performance and Security Improvements	User-based Security Model	Performance Improvements, Community-based	User-based Security Model

Research Until Now: SNMPv2c



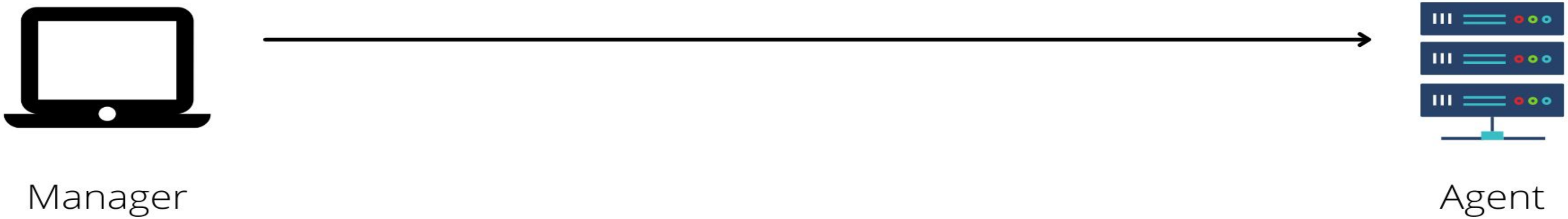
- Currently only ~1.6M SNMPv2c responsive IPs
- No prior work investigated the adoption of SNMPv3

Figure source https://scan.shadowserver.org/snmp/stats/

SNMPv3 Discovery Phase

Manager

Agent

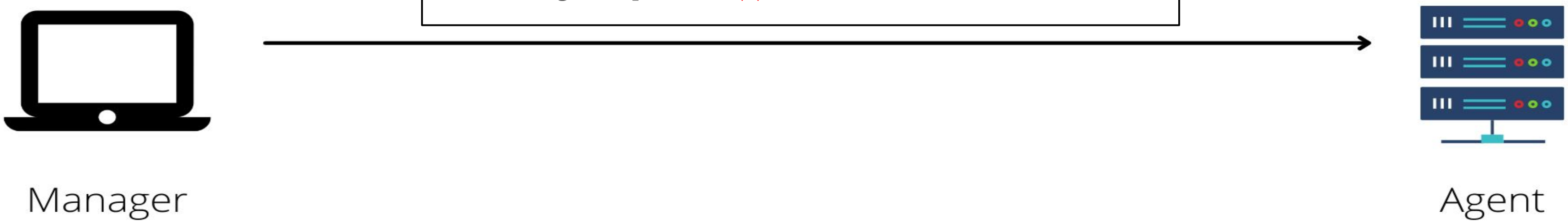


Manager

Agent

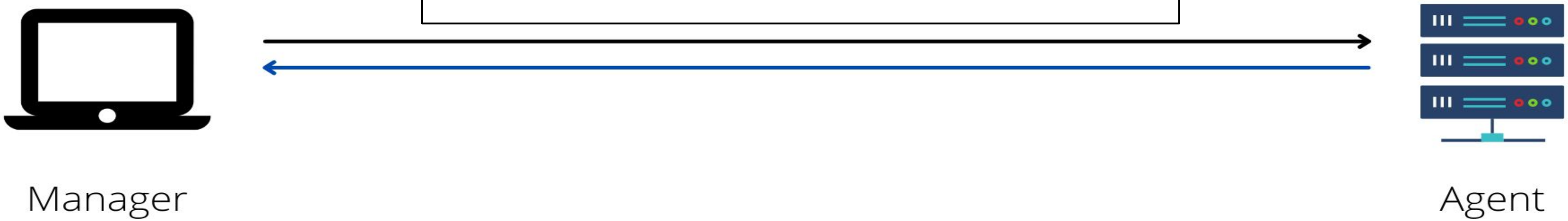
SNMPv3 Discovery Request

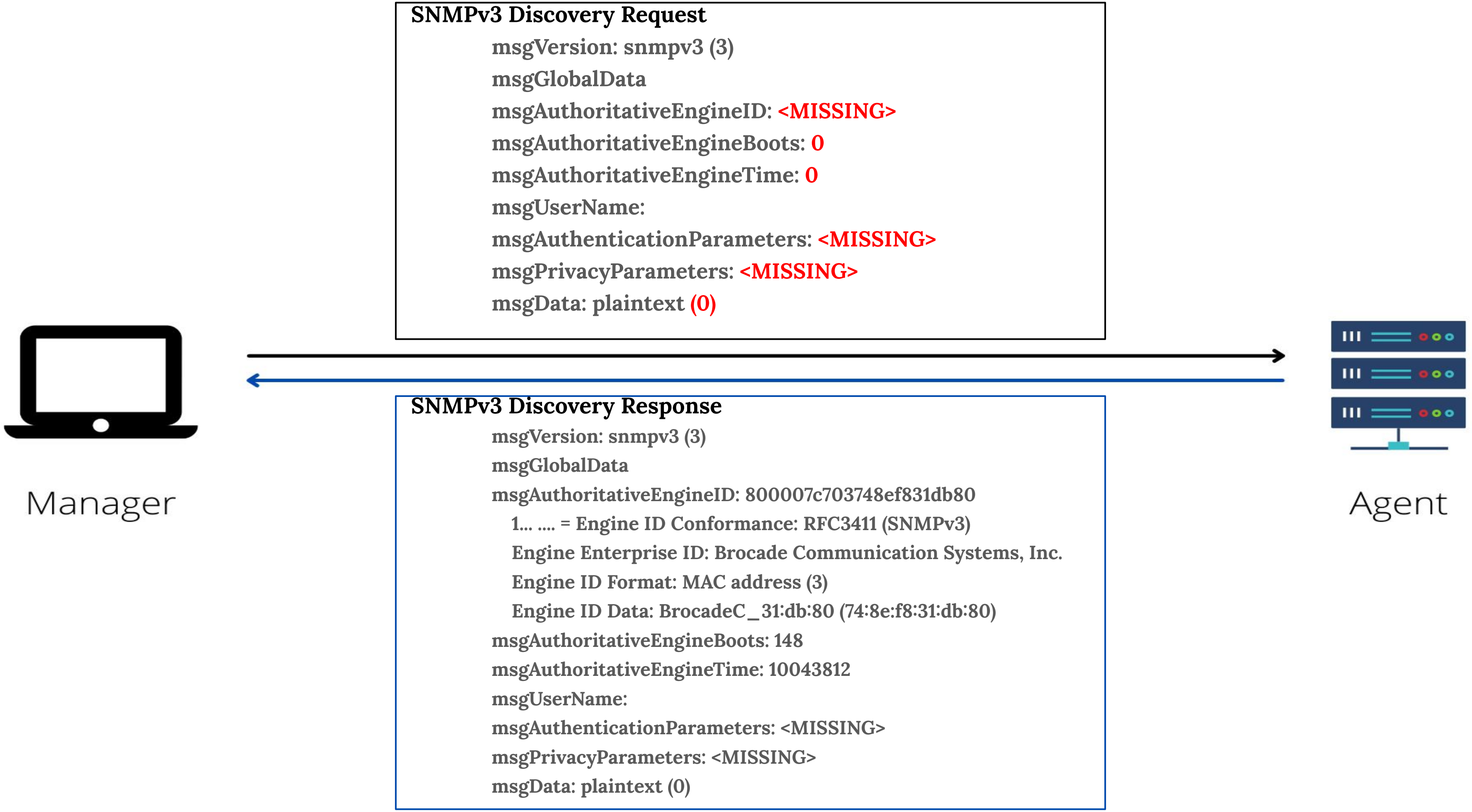
- msgVersion: snmpv3 (3)
- msgGlobalData
- msgAuthoritativeEngineID: **<MISSING>**
- msgAuthoritativeEngineBoots: **0**
- msgAuthoritativeEngineTime: **0**
- msgUserName:
- msgAuthenticationParameters: **<MISSING>**
- msgPrivacyParameters: **<MISSING>**
- msgData: plaintext **(0)**



SNMPv3 Discovery Request

msgVersion: snmpv3 (3)
msgGlobalData
msgAuthoritativeEngineID: <MISSING>
msgAuthoritativeEngineBoots: 0
msgAuthoritativeEngineTime: 0
msgUserName:
msgAuthenticationParameters: <MISSING>
msgPrivacyParameters: <MISSING>
msgData: plaintext (0)



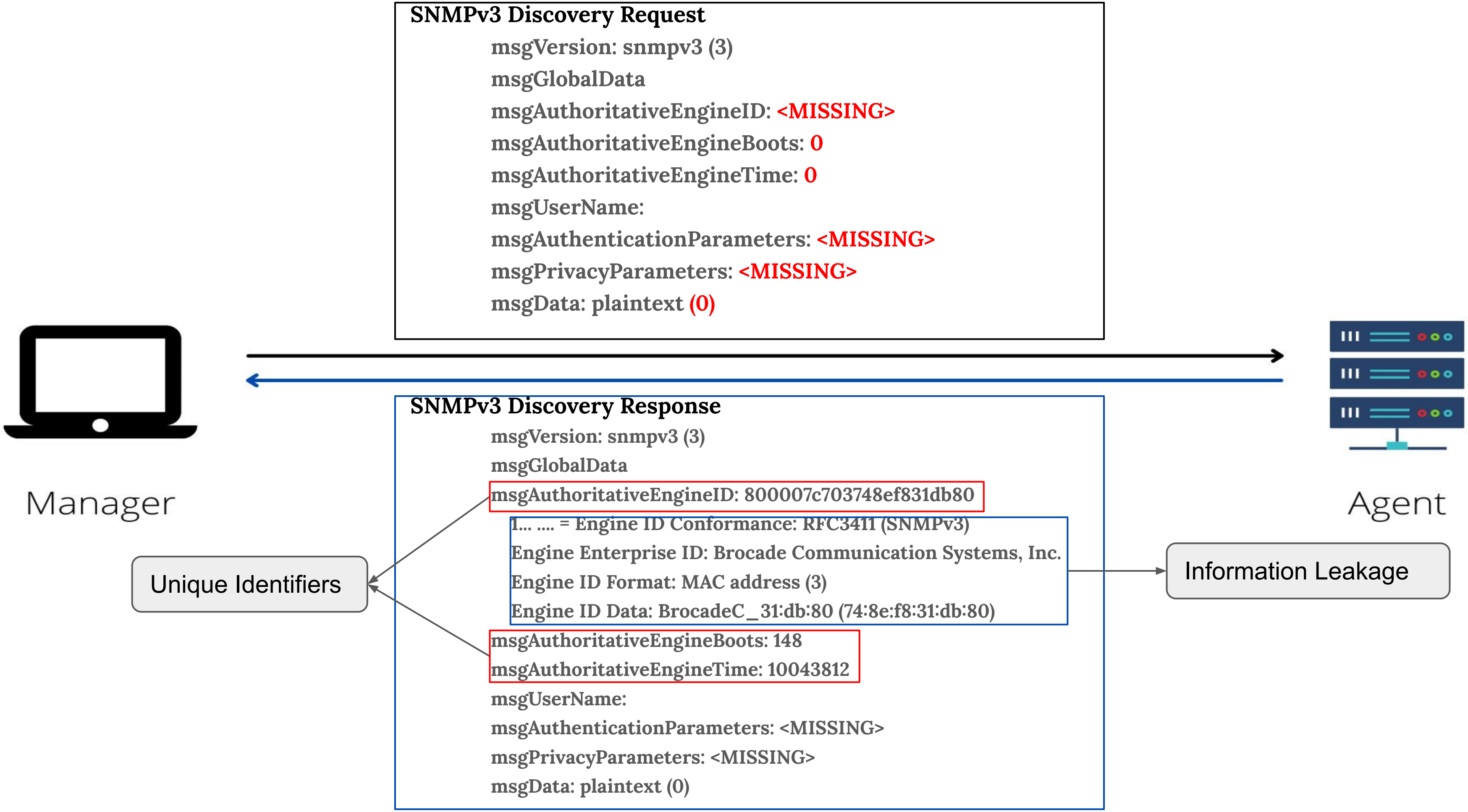


SNMPv3 Discovery Request

```
msgVersion: snmpv3 (3)
msgGlobalData
msgAuthoritativeEngineID: <MISSING>
msgAuthoritativeEngineBoots: 0
msgAuthoritativeEngineTime: 0
msgUserName:
msgAuthenticationParameters: <MISSING>
msgPrivacyParameters: <MISSING>
msgData: plaintext (0)
```

SNMPv3 Discovery Response

```
msgVersion: snmpv3 (3)
msgGlobalData
msgAuthoritativeEngineID: 800007c703748ef831db80
   1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
   Engine Enterprise ID: Brocade Communication Systems, Inc.
   Engine ID Format: MAC address (3)
   Engine ID Data: BrocadeC_31:db:80 (74:8e:f8:31:db:80)
msgAuthoritativeEngineBoots: 148
msgAuthoritativeEngineTime: 10043812
msgUserName:
msgAuthenticationParameters: <MISSING>
msgPrivacyParameters: <MISSING>
msgData: plaintext (0)
```



SNMPv3 Discovery Request

msgVersion: snmpv3 (3)
msgGlobalData
msgAuthoritativeEngineID: <MISSING>
msgAuthoritativeEngineBoots: 0
msgAuthoritativeEngineTime: 0
msgUserName:
msgAuthenticationParameters: <MISSING>
msgPrivacyParameters: <MISSING>
msgData: plaintext (0)

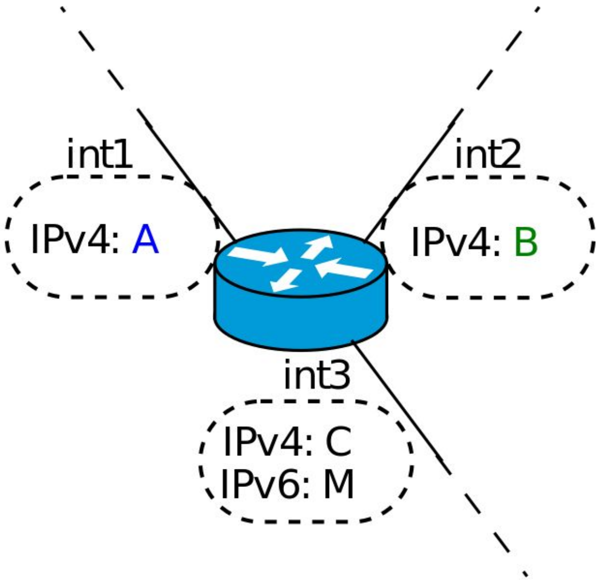
SNMPv3 Discovery Response

msgVersion: snmpv3 (3)
msgGlobalData
msgAuthoritativeEngineID: 800007c703748ef831db80
1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
Engine Enterprise ID: Brocade Communication Systems, Inc.
Engine ID Format: MAC address (3)
Engine ID Data: BrocadeC_31:db:80 (74:8e:f8:31:db:80)
msgAuthoritativeEngineBoots: 148
msgAuthoritativeEngineTime: 10043812
msgUserName:
msgAuthenticationParameters: <MISSING>
msgPrivacyParameters: <MISSING>
msgData: plaintext (0)

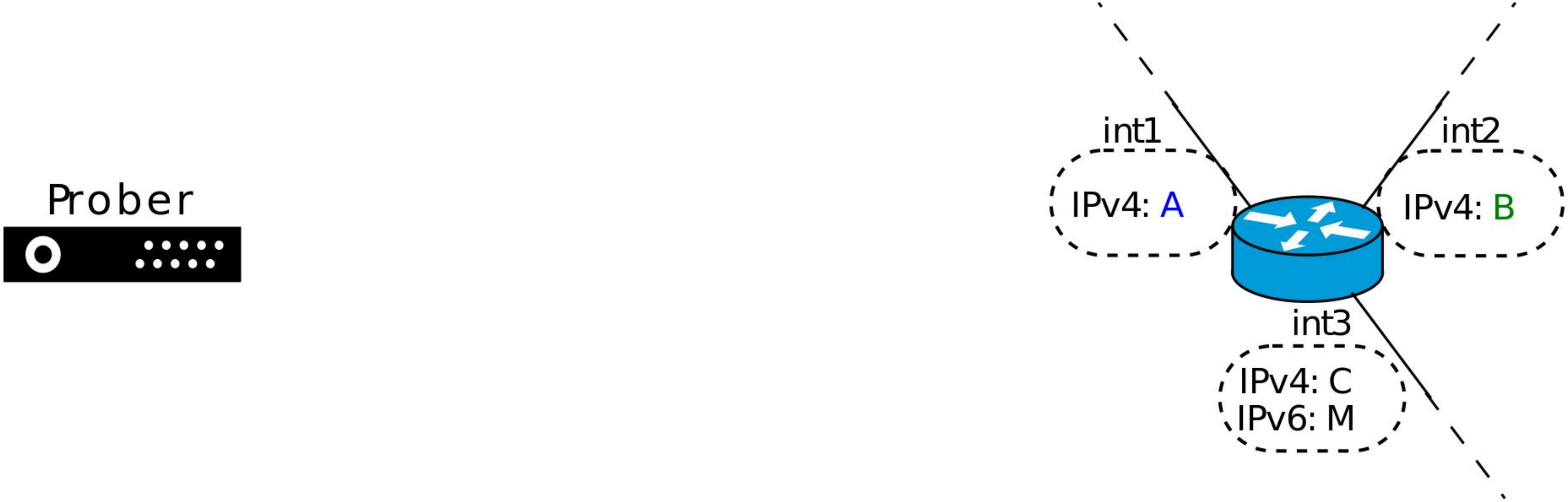
What can we do with SNMPv3 responses?

- **Facilitate many Internet measurement tasks:**
    - **IP alias resolution**
    - **IPv4/IPv6 dual-stack detection**
    - **Device vendor fingerprinting**
    - **Device uptime analysis**
- **With only a single packet per IP!**

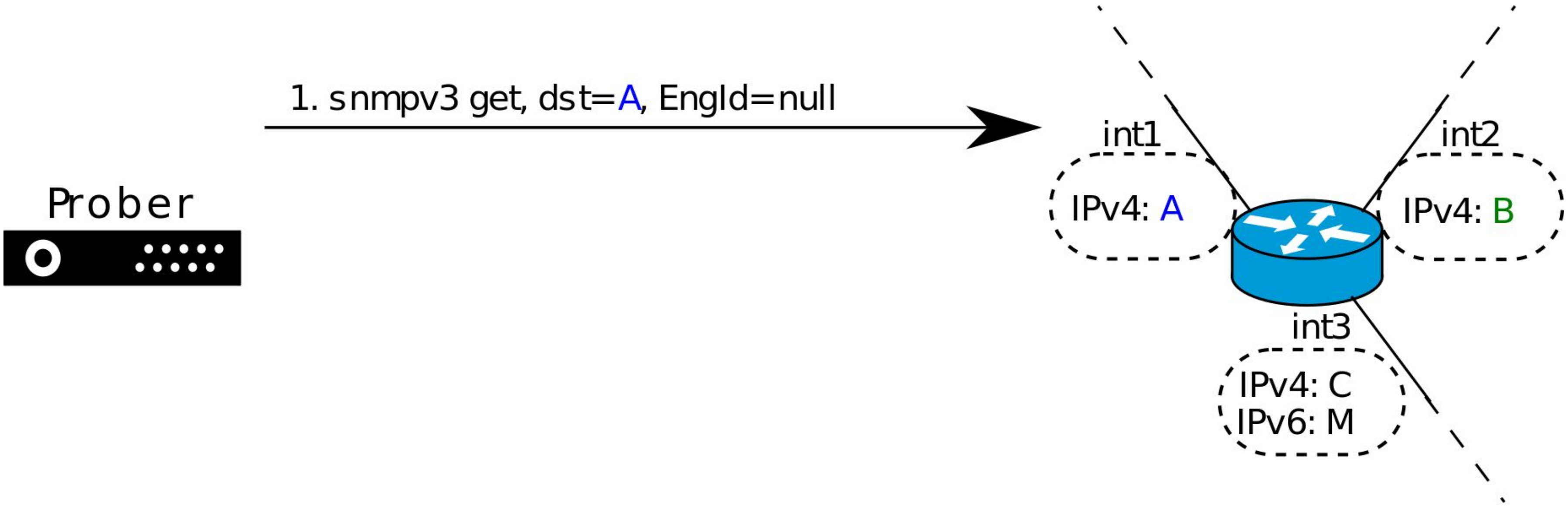
Alias and Dual-Stack Detection



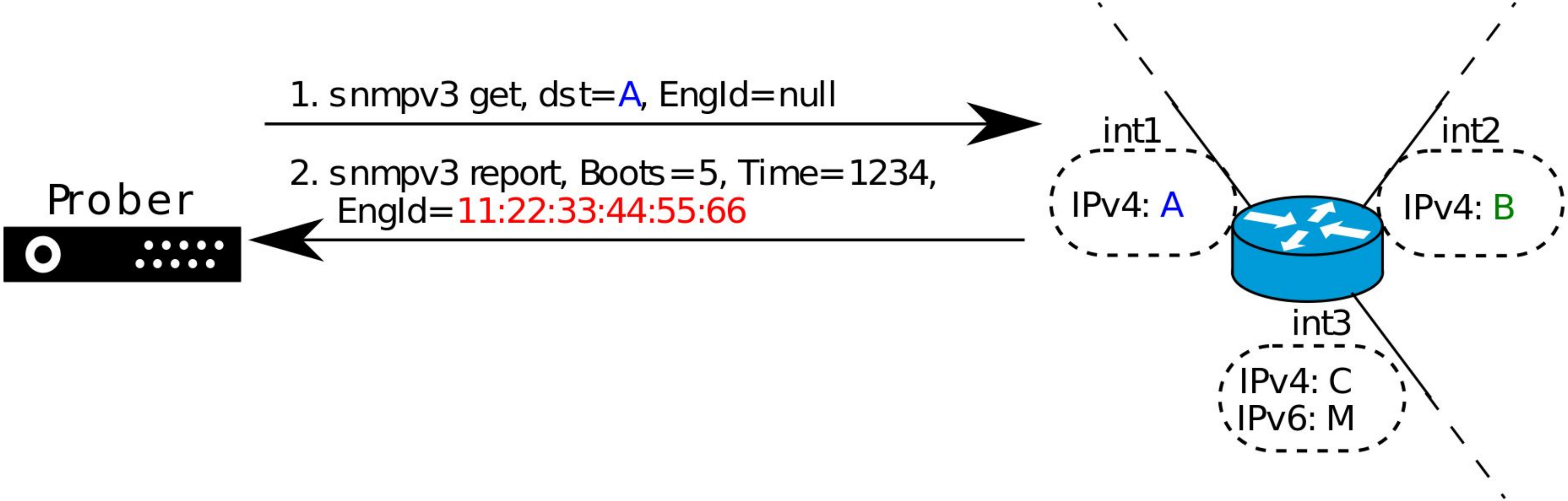
Alias and Dual-Stack Detection



Alias and Dual-Stack Detection

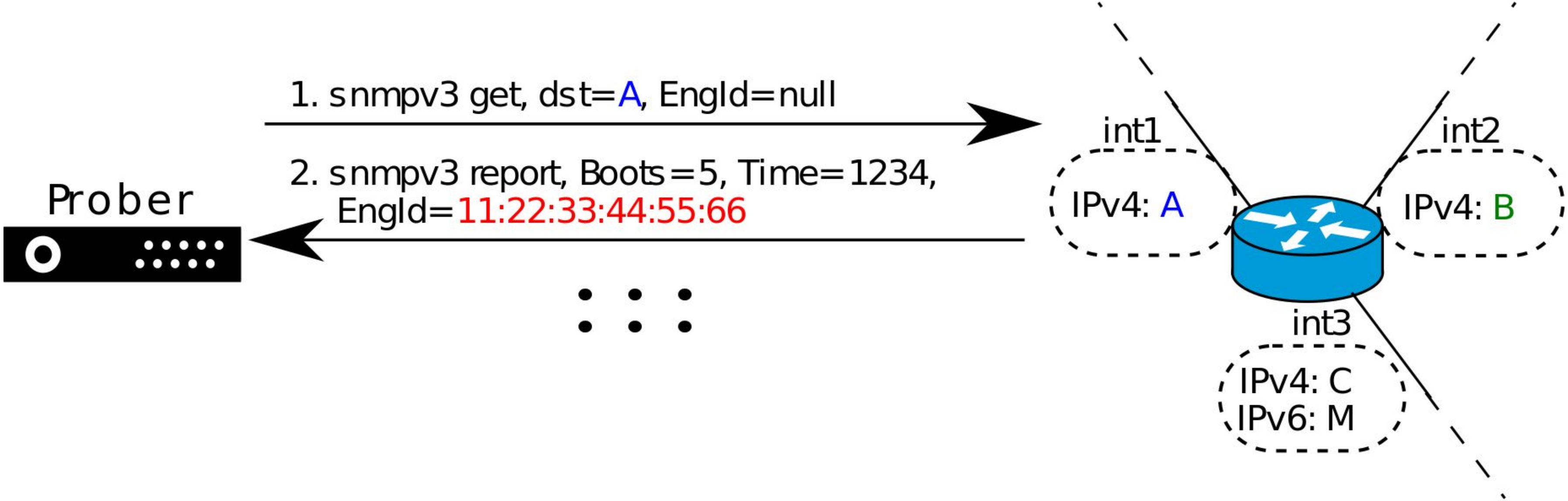


Alias and Dual-Stack Detection

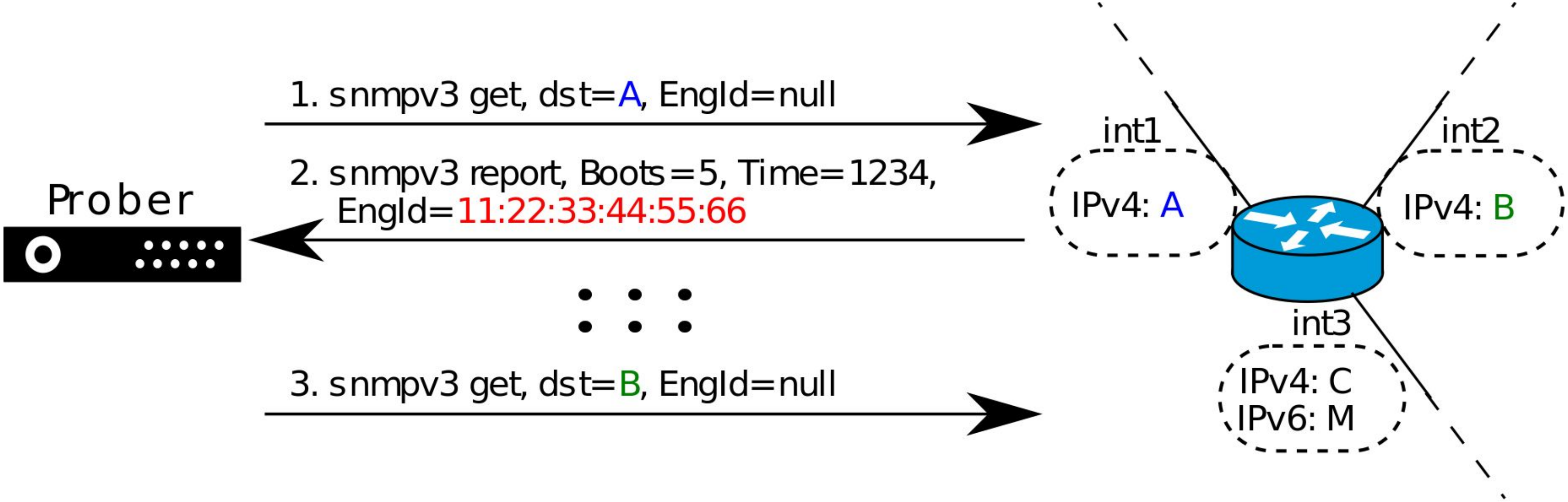


1. snmpv3 get, dst=A, EngId=null
2. snmpv3 report, Boots=5, Time=1234, EngId=11:22:33:44:55:66
Prober
int1
IPv4: A
int2
IPv4: B
int3
IPv4: C
IPv6: M

Alias and Dual-Stack Detection


1. snmpv3 get, dst=A, EngId=null
2. snmpv3 report, Boots=5, Time=1234,
EngId=11:22:33:44:55:66
Prober
int1
IPv4: A
int2
IPv4: B
int3
IPv4: C
IPv6: M

Alias and Dual-Stack Detection

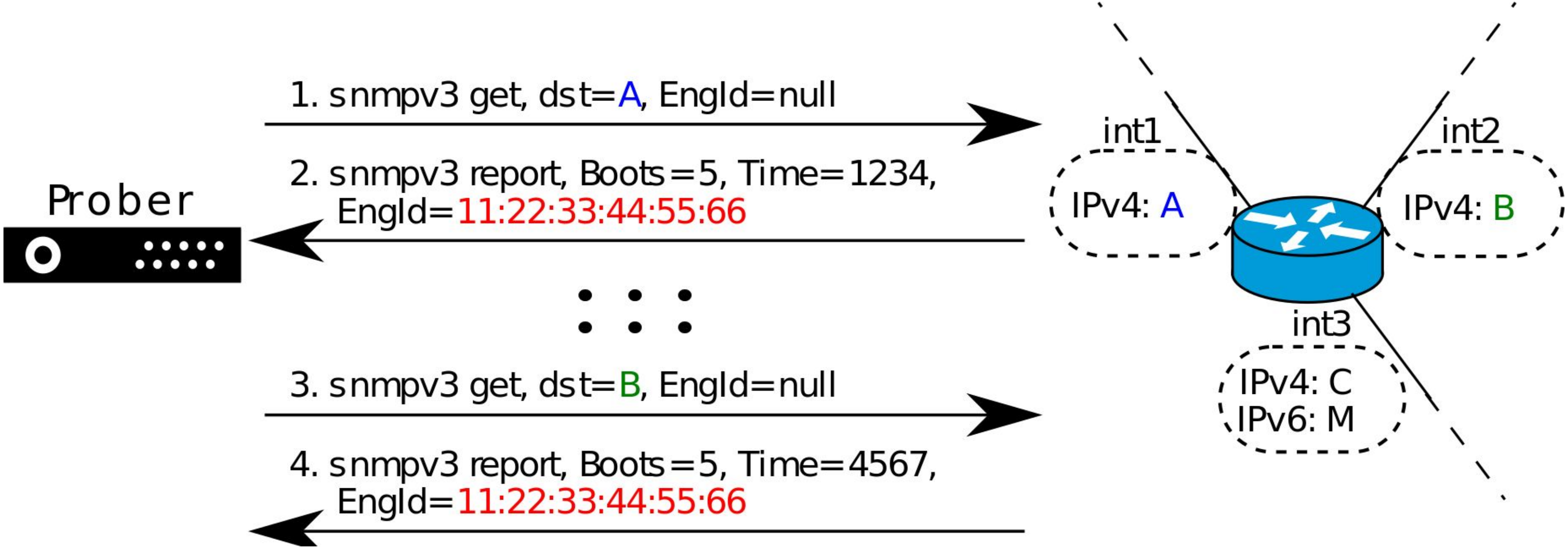


1. snmpv3 get, dst=A, EngId=null

2. snmpv3 report, Boots=5, Time=1234,
EngId=11:22:33:44:55:66

3. snmpv3 get, dst=B, EngId=null

Alias and Dual-Stack Detection



1. snmpv3 get, dst=A, EngId=null

2. snmpv3 report, Boots=5, Time=1234, EngId=11:22:33:44:55:66

3. snmpv3 get, dst=B, EngId=null

4. snmpv3 report, Boots=5, Time=4567, EngId=11:22:33:44:55:66

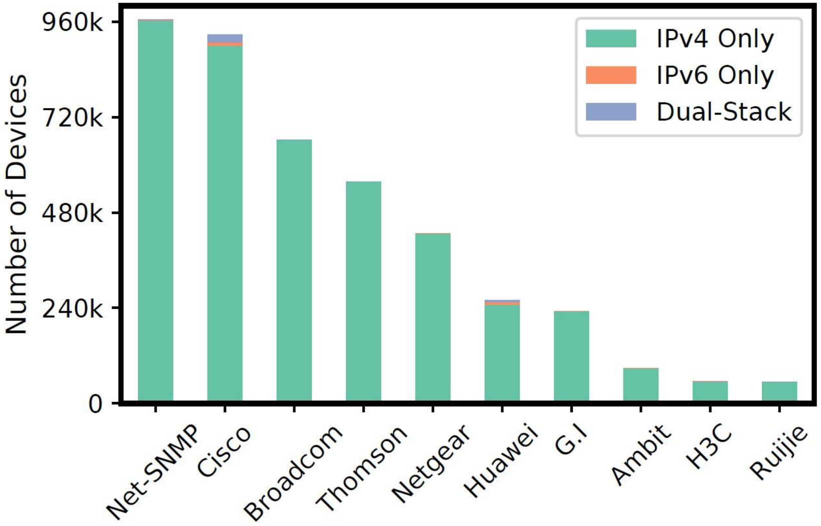
Active Scan Results

- Responses
  - 31M IPv4 addresses
  - 180k IPv6 addresses
- After extensive filtering
  - 12.5M IPv4 addresses
  - 140k IPv6 addresses

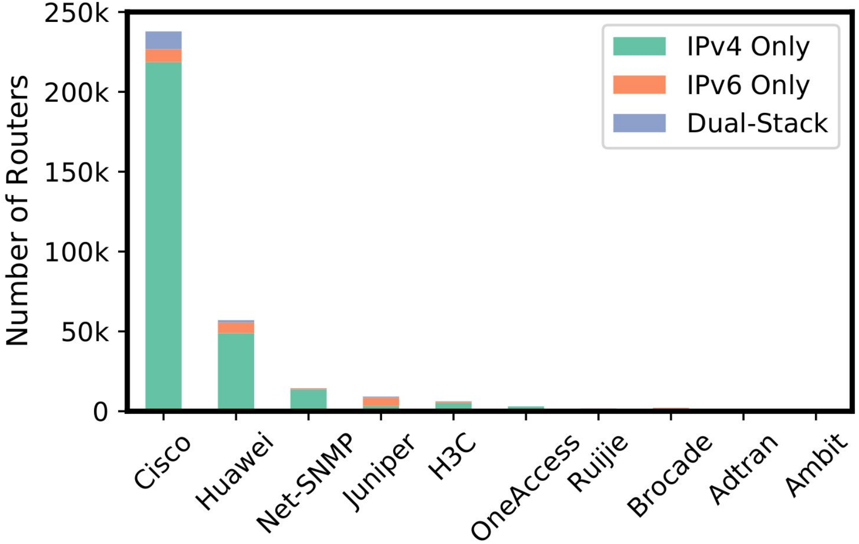
IPv6 hitlist service: https://ipv6hitlist.github.io/
ZMap: https://github.com/zmap/zmap

Device Fingerprinting: Vendors Popularity

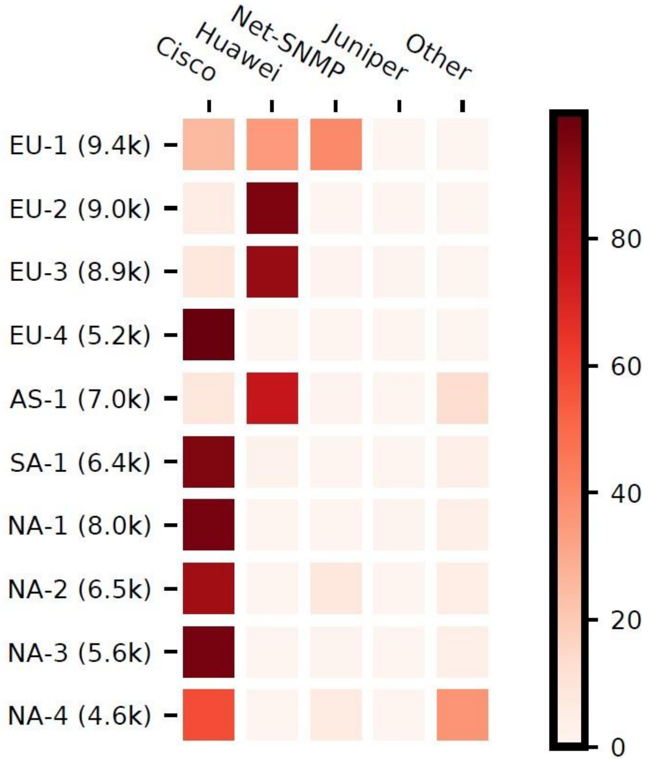
Total Number of Devices: 4.6M



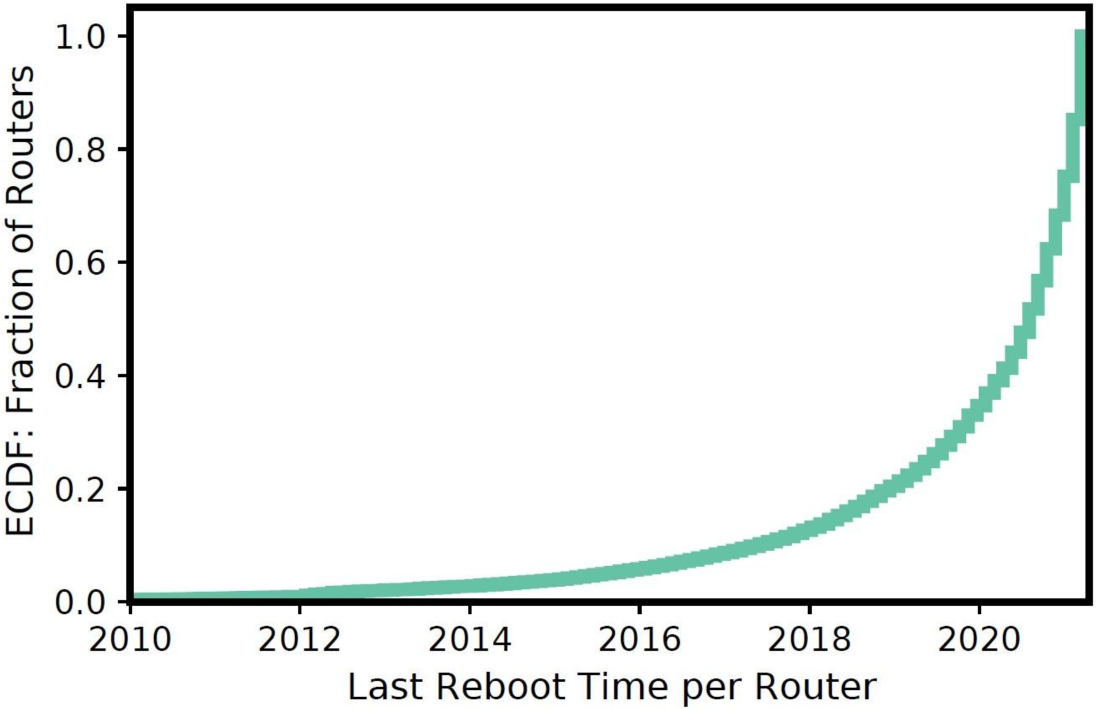
Total Number of Routers: 350k



SNMPv3 Router Vendors Popularity per Network

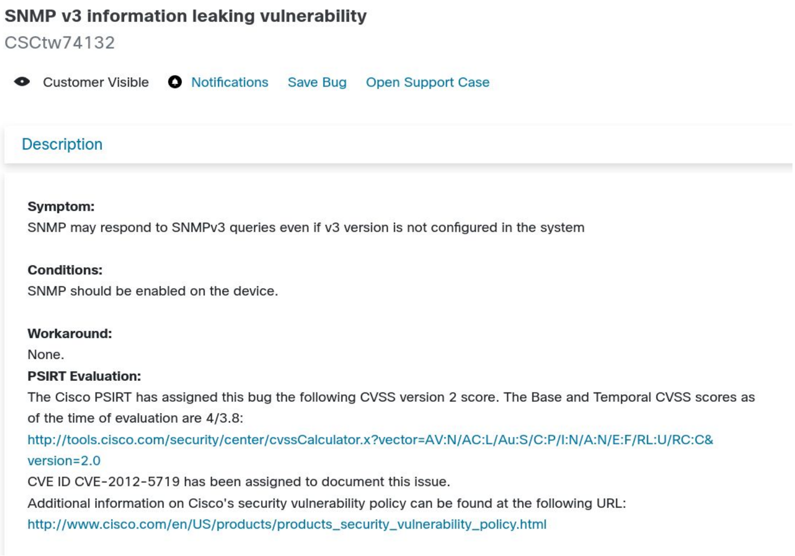


SNMPv3 Routers Last Reboot



Why do so many devices respond?

- Lab experiments
  - Cisco IOS 15.2(4)S7 and IOS XR 6.0.1
  - Juniper JunOS 17.3
- Devices unknowingly respond to SNMPv3



SNMP v3 information leaking vulnerability

CSCtw74132

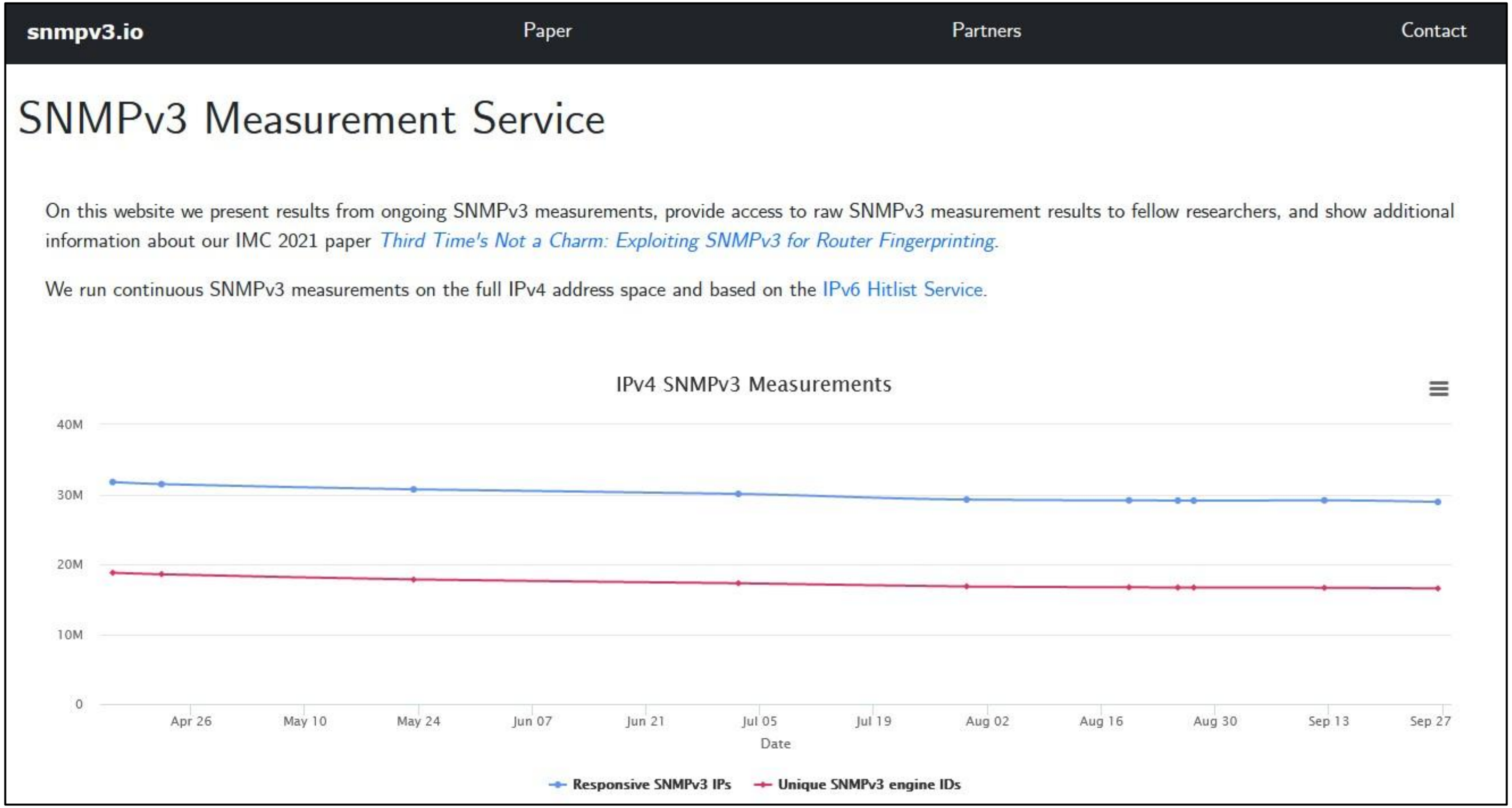
Symptom:
SNMP may respond to SNMPv3 queries even if v3 version is not configured in the system

Conditions:
SNMP should be enabled on the device.

Workaround:
None.

PSIRT Evaluation:
The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4/3.8:
http://tools.cisco.com/security/center/cvssCalculator.x?vector=AV:N/AC:L/Au:S/C:P/I:N/A:N/E:F/RL:U/RC:C&version=2.0
CVE ID CVE-2012-5719 has been assigned to document this issue.
Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

https://snmpv3.io



SNMPv3 Measurement Service

On this website we present results from ongoing SNMPv3 measurements, provide access to raw SNMPv3 measurement results to fellow researchers, and show additional information about our IMC 2021 paper *Third Time's Not a Charm: Exploiting SNMPv3 for Router Fingerprinting*.

We run continuous SNMPv3 measurements on the full IPv4 address space and based on the IPv6 Hitlist Service.

Summary

- SNMPv3 adoption
  - 31M IPs
- Lightweight technique (single packet)
  - IP alias and dual-stack detection
    - 4.6M devices
  - Router vendor fingerprinting and uptime analysis
    - 350k routers
    - 11k networks

Backup Slides

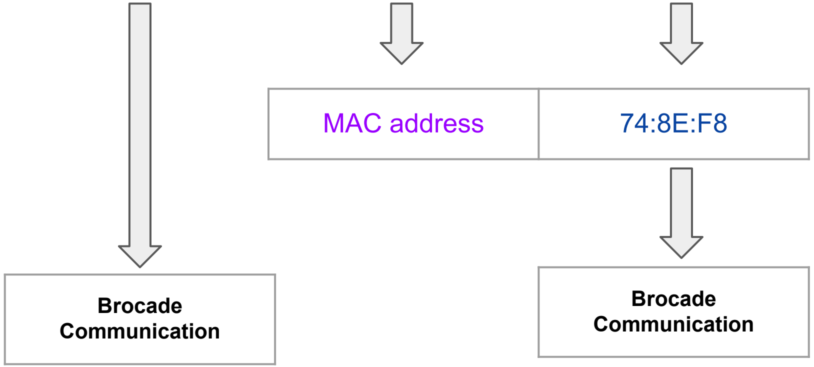
Device Vendor Fingerprinting

Engine ID Structure:

Conformance Bit	Enterprise ID	Engine ID format	Engine ID Data

Example EngineID: 800007c703748ef831db80

8000	07c7	03	748ef831db80

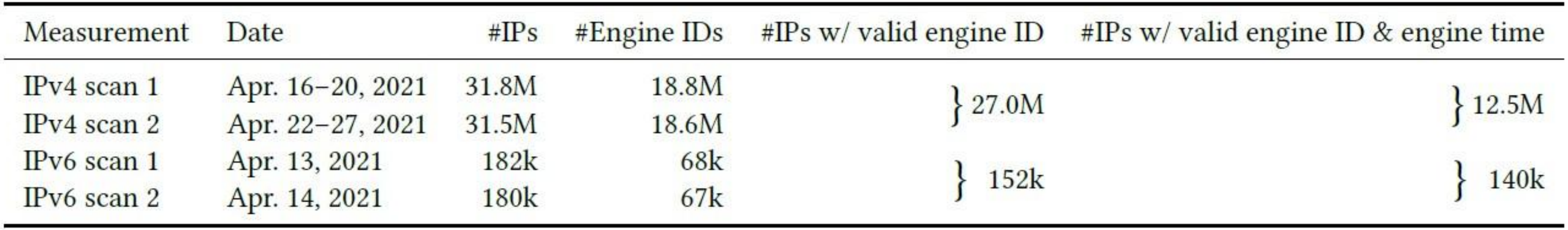


MAC address	74:8E:F8

Brocade Communication

Brocade Communication

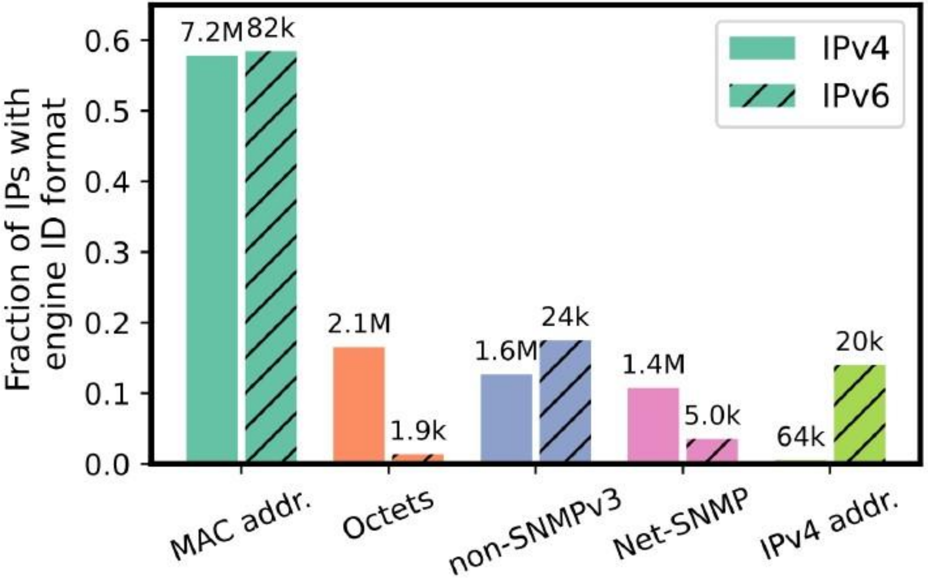
Filtering Responses



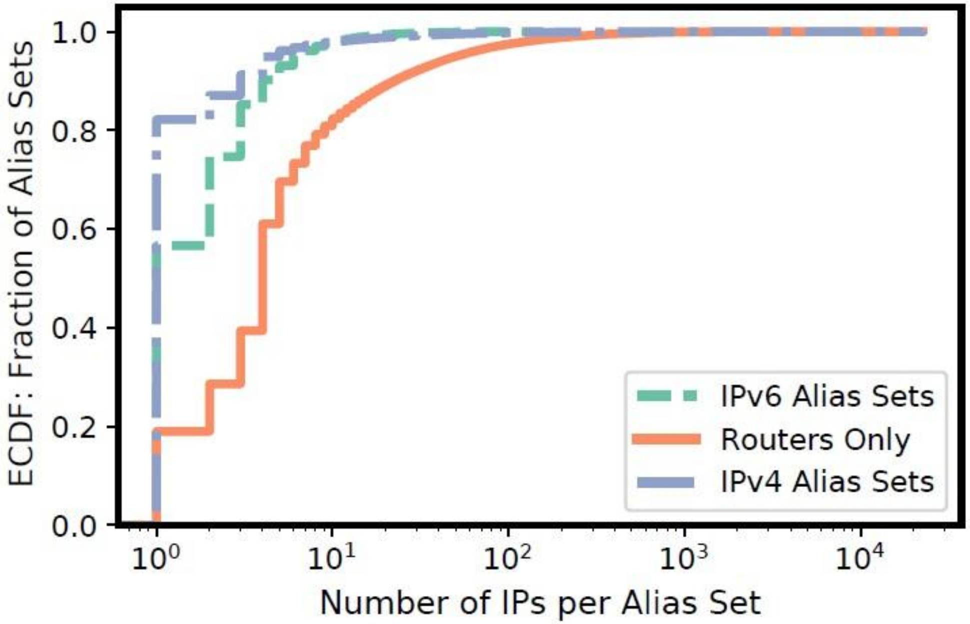
Measurement	Date	#IPs	#Engine IDs	#IPs w/ valid engine ID	#IPs w/ valid engine ID & engine time
IPv4 scan 1	Apr. 16–20, 2021	31.8M	18.8M	} 27.0M	} 12.5M
IPv4 scan 2	Apr. 22–27, 2021	31.5M	18.6M		
IPv6 scan 1	Apr. 13, 2021	182k	68k	} 152k	} 140k
IPv6 scan 2	Apr. 14, 2021	180k	67k		

- Engine ID filters:
  - Missing engine IDs.
  - Inconsistent engine IDs across 2 scans
  - Short engine IDs
  - Formate specific filters
- Engine boot + Engine time filters:
  - Zero Engine time or engine boot
  - Engine time in the future
  - Inconsistent engine boots
  - Inconsistent last reboot time

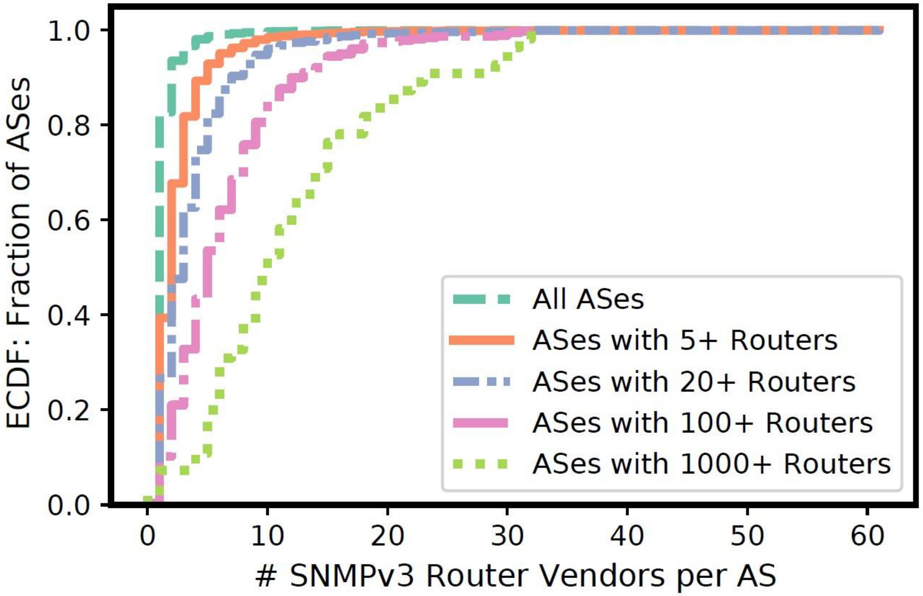
EngineID Formats



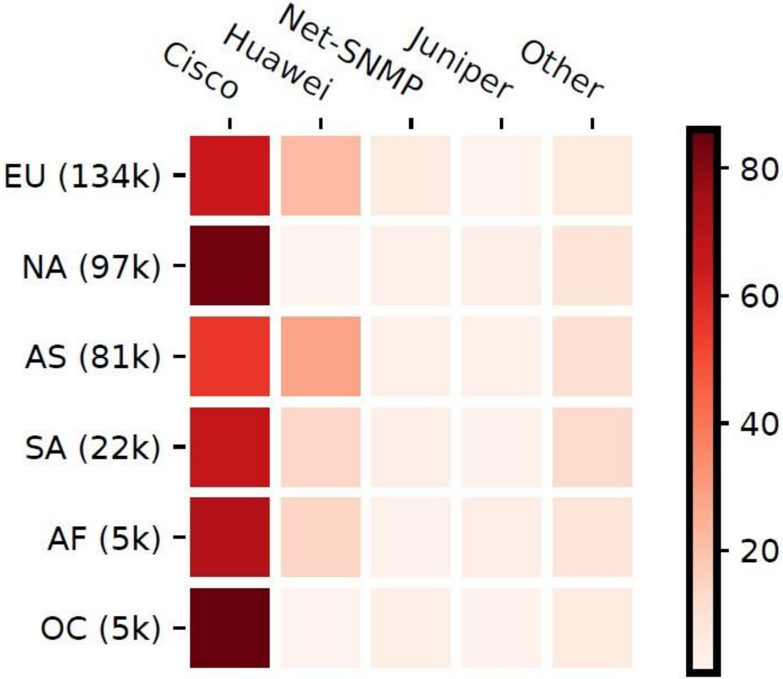
Alias Resolution: IPs per Alias Set



Fingerprinting: Router Vendors Count per AS



Fingerprinting: Router Vendors Popularity per Region


Cisco
Huawei
Net-SNMP
Juniper
Other
EU (134k)
NA (97k)
AS (81k)
SA (22k)
AF (5k)
OC (5k)