

# Third Time's Not a Charm

Exploiting SNMPv3 for  
Router Fingerprinting

**Taha Albakour, Oliver Gasser,  
Robert Beverly, Georgios Smaragdakis**

RIPE 83 Academic Session

**SNMP**

# What is SNMP?

- Simple Network Management Protocol
- Example use case: Retrieve various device statistics
- Introduced in the 1980s
- SNMPv3 standardized in 2002

# SNMPv3 request

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

# SNMPv3 response

```
Simple Network Management Protocol
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 response

```
Simple Network Management Protocol
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 response

```
Simple Network Management Protocol
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)
```

**Engine ID: unique and unambiguous identifier**

# How many SNMPv3 responses?



# How many SNMPv3 responses?

Responses

- **12.5M IPv4** addresses
- **140k IPv6** addresses

# How many SNMPv3 responses?

## Responses

- **12.5M IPv4** addresses
- **140k IPv6** addresses
- 22k ASes, of which **8k in the RIPE region**

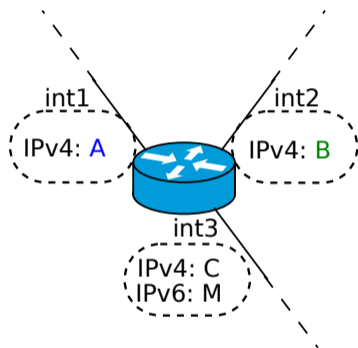
**Why should operators care?**

# Why should operators care?

- Improperly secured SNMPv3 allows anyone to
  - Learn about your **network infrastructure**
  - **Fingerprint** your routers
  - Use this information for **malicious purposes**

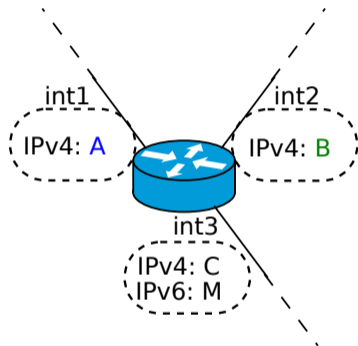
**Learn about your  
network infrastructure**

# Addresses belonging to routers

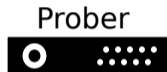


# Addresses belonging to routers

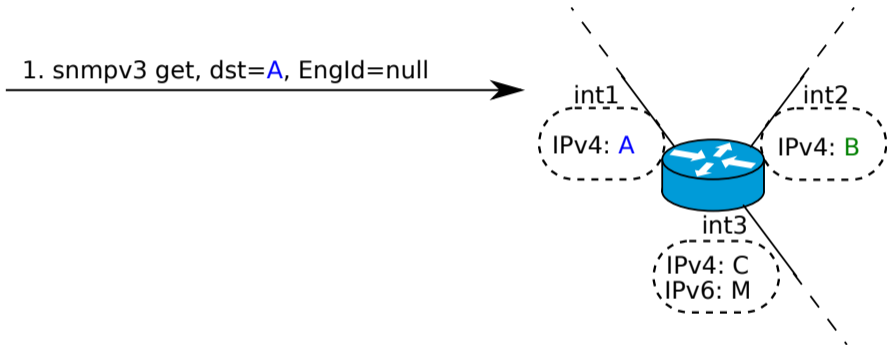
Prober



# Addresses belonging to routers

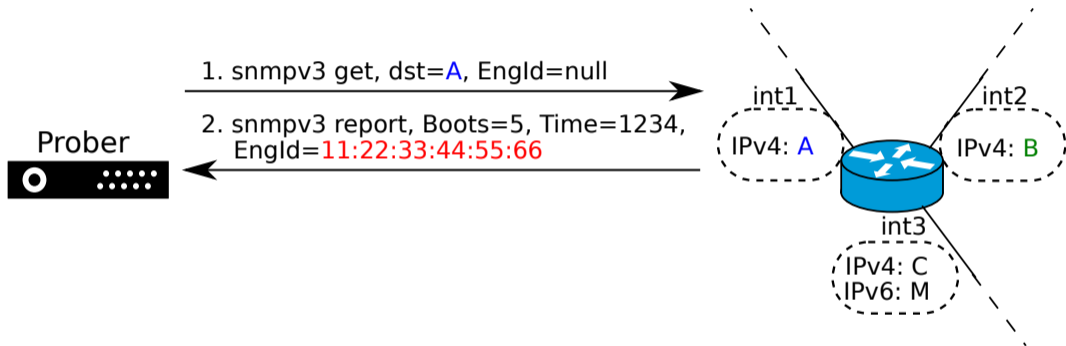


1. snmpv3 get, dst=A, EngId=null

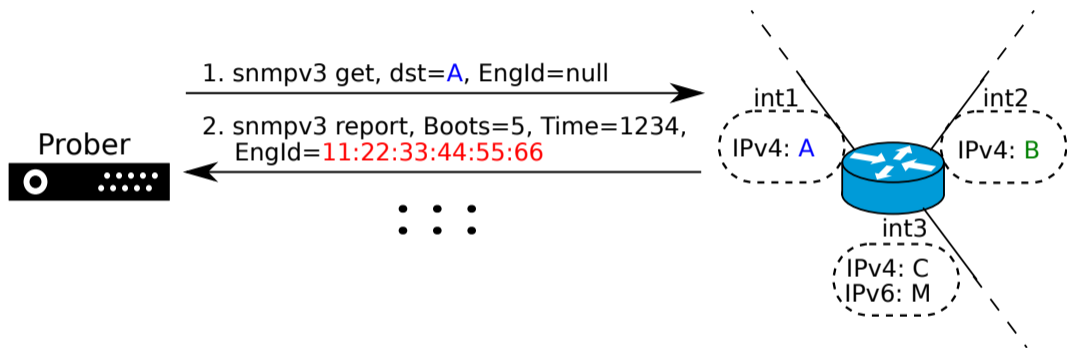




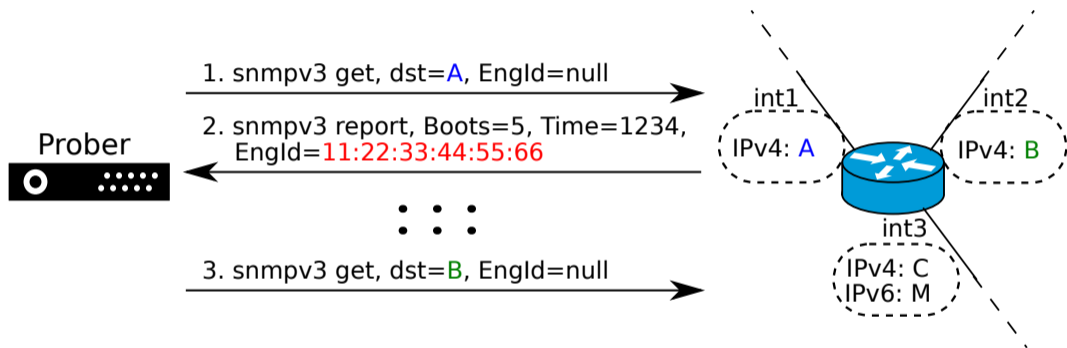
# Addresses belonging to routers



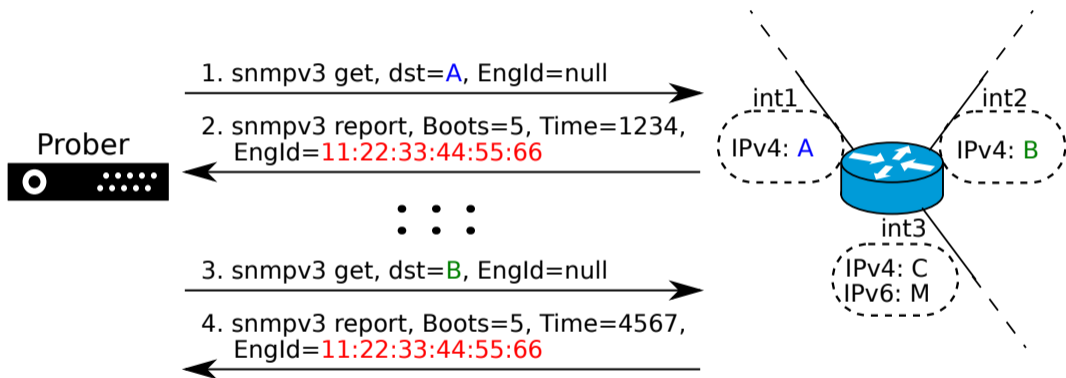
# Addresses belonging to routers



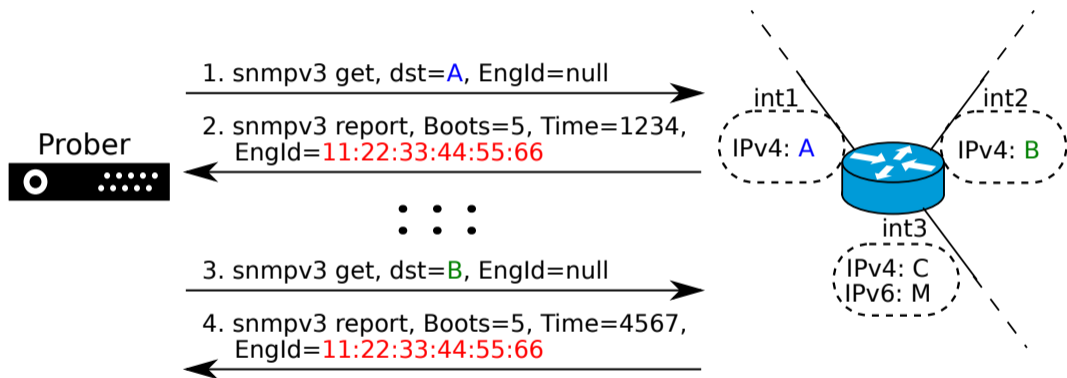
# Addresses belonging to routers



# Addresses belonging to routers



# Addresses belonging to routers



**With a single packet per target IP!**

# How many SNMPv3 devices?

# How many SNMPv3 devices?

- 4.6M devices
- **350k routers**

# How many SNMPv3 devices?

- 4.6M devices
- **350k routers**

**Nice**



# How many SNMPv3 devices?

- 4.6M devices
- **350k routers**

**Nice, but so what?**

**Fingerprint your router**

# Recall: SNMPv3 response

```
Simple Network Management Protocol
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)
```

# Recall: SNMPv3 response

```
Simple Network Management Protocol
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)
```

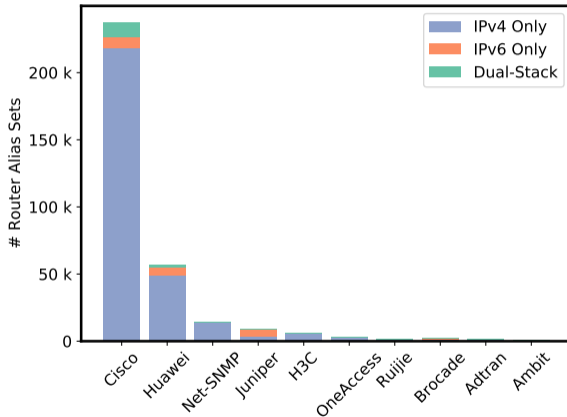
# Recall: SNMPv3 response

```
Simple Network Management Protocol
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)
```

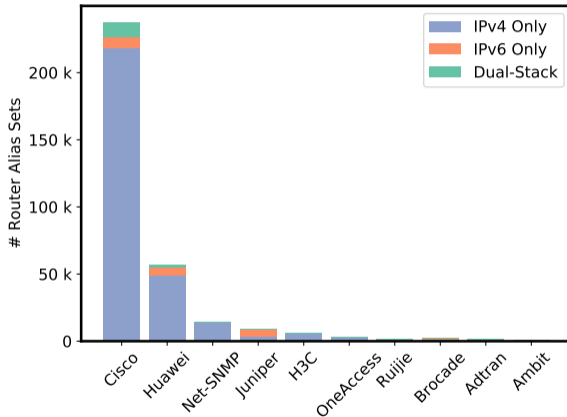
**MAC → vendor fingerprinting!**

# Router vendors

# Router vendors



# Router vendors



**Cisco is dominating!**



# Why is Cisco so dominant?

# Why is Cisco so dominant?

Lab experiments

- Enable **SNMPv2c**

# Why is Cisco so dominant?

Lab experiments

- Enable **SNMPv2c**
- SNMPv3 remains disabled

# Why is Cisco so dominant?

Lab experiments

- Enable **SNMPv2c**
- SNMPv3 remains disabled, **but the devices still respond to SNMPv3 engine ID queries**

# Why is Cisco so dominant?

Lab experiments

- Enable **SNMPv2c**
- SNMPv3 remains disabled, **but the devices still respond to SNMPv3 engine ID queries**

**Devices unknowingly respond to SNMPv3**

# Response by Cisco

# Response by Cisco

- We reached out to Cisco

# Response by Cisco

- We reached out to Cisco, they confirmed the issue



# Response by Cisco

- We reached out to Cisco, they confirmed the issue
- Multiple bug reports and one **CVE from 2012**

# Response by Cisco

- We reached out to Cisco, they confirmed the issue
- Multiple bug reports and one **CVE from 2012**
- New IOS command: `snmp-server drop unknown-user`

# Response by Cisco

- We reached out to Cisco, they confirmed the issue
- Multiple bug reports and one **CVE from 2012**
- New IOS command: `snmp-server drop unknown-user`
- Workaround: Drop packets from untrusted networks

**What else?**

# Monitoring the SNMPv3 landscape

# Monitoring the SNMPv3 landscape

snmpv3.io

Paper

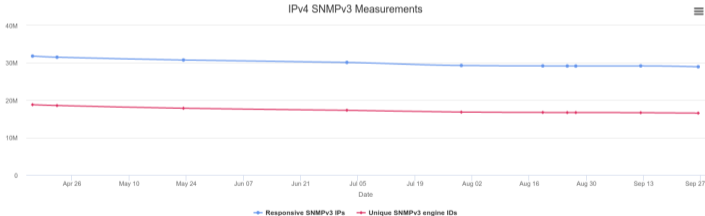
Partners

Contact

## 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](#).



# Monitoring the SNMPv3 landscape

snmpv3.io

Paper

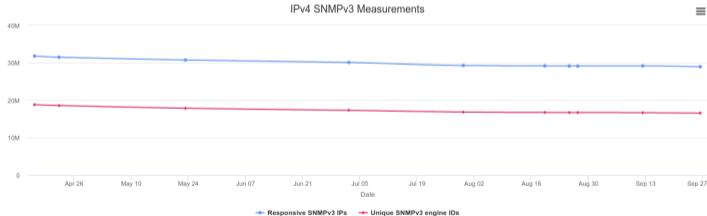
Partners

Contact

## 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](#).



<https://snmpv3.io>

# Conclusion



# Conclusion

# Conclusion

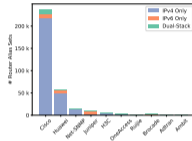
```
Simple Network Management Protocol
msgVersion: snmpv3 (3)
msgGlobalData
msgAuthoritativeEngineID: 880987c783748ef831db80
1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
Engine Enterprise ID: Brocade Communication Systems, Inc.
Engine ID Format: MAC address (3)
Engine ID Data: BrocadeC_311db180 (7418e1f8:311db180)
msgAuthoritativeEngineBoots: 148
msgAuthoritativeEngineTime: 10843812
msgUserName:
msgAuthenticationParameters: <MISSING>
msgPrivacyParameters: <MISSING>
msgData: plaintext (0)
```

Engine ID to **identify devices**

# Conclusion

```
Simple Network Management Protocol
msgVersion: snmpv3 (3)
msgGlobalData
msgAuthoritativeEngineID: 880987c783748ef831db80
1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
Engine Enterprise ID: Brocade Communication Systems, Inc.
Engine ID Format: MAC address (3)
Engine ID Data: BrocadeC_311db180 (7418e1f8:311db180)
msgAuthoritativeEngineBoots: 148
msgAuthoritativeEngineTime: 10843812
msgUserName:
msgAuthenticationParameters: <MISSING>
msgPrivacyParameters: <MISSING>
msgData: plaintext (8)
```

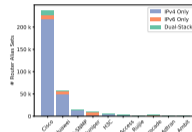
Engine ID to **identify devices**



**Cisco** dominates SNMPv3

# Conclusion

```
Simple Network Management Protocol
msgVersion: snmpv3 (3)
msgGlobalData
msgAuthoritativeEngineID: 880987c783748ef831db80
1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
Engine Enterprise ID: Brocade Communication Systems, Inc.
Engine ID Format: MAC address (3)
Engine ID Data: BrocadeC_311db180 (7418e1f8:311db180)
msgAuthoritativeEngineBoots: 148
msgAuthoritativeEngineTime: 10843812
msgUserName:
msgAuthenticationParameters: <MISSING>
msgPrivacyParameters: <MISSING>
msgData: plaintext (8)
```



Engine ID to **identify devices**

**Cisco** dominates SNMPv3

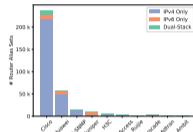


Issue is **known for years**

# Conclusion

```
Simple Network Management Protocol
msgVersion: snmpv3 (3)
msgGlobalData
msgAuthoritativeEngineID: 880987c783748ef831db80
1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
Engine Enterprise ID: Brocade Communication Systems, Inc.
Engine ID Format: MAC address (3)
Engine ID Data: BrocadeC_311db180 (7418e1f8:311db180)
msgAuthoritativeEngineBoots: 148
msgAuthoritativeEngineTime: 10843812
msgUserName:
msgAuthenticationParameters: <MISSING>
msgPrivacyParameters: <MISSING>
msgData: plaintext (8)
```

Engine ID to **identify devices**



**Cisco** dominates SNMPv3

**CVE-2012-0718** (from [Cisco](#) entry in National Vulnerability Database (NVD))  
CISCO Security Advisory (SA) 2012-0718: Cisco Catalyst 3750 series 4-port Gigabit Ethernet switches are affected by a Denial of Service (DoS) vulnerability. The vulnerability is caused by a buffer overflow in the switch's CPU. An attacker can exploit this vulnerability by sending a specially crafted packet to the switch. The vulnerability is present in all versions of the switch's software that are affected by this advisory. The vulnerability is being fixed in the next software release. Cisco is not responsible for any damage caused by this vulnerability.

Issue is **known for years**



**SNMPv3.io**