IOTOPS Working Group
Internet-Draft
Intended status: Standards Track
Expires: 17 October 2025

M. Richardson
Sandelman Software Works

15 April 2025

Doing an Inventory of IoT devices using IDevID scanning
draft-richardson-iotops-mud-query-00

Abstract

This document describes a mechanism to do an inventory of devices on a network.

While there are significant abuse and privacy concerns with kind of scanning, the practice of scanning networks and fingerprinting devices has been occuring since the mid 1990s. But, the adhoc methods are not reliable and do not provide any kind of strong device identity.

This document takes the approach that if it will happen, it might as well be reliable and secure.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 17 October 2025.

Copyright Notice

Table of Contents

1. Introduction

Even before the first release of [nmap] in 1998, network operators have wanted to know what systems are on their network.

One way to do this control has been to require authentication before a system can use the Internet in the form of authenticating firewall proxies, including standards work around SOCKSv5 [RFC1929]. For desktop users these mechanisms have been poorly received, and in many environments these controls have been turned off, or are never deployed. The authenticate before Internet use can create be used to create an inventory, but it does not directly create an inventory. Privacy considerations around IP address and MAC address disclosure have increasingly made that level of inventory even less useful [RFC9724].

None of the above heuristics are useful for devices which do not attempt to use Internet. Nor can any kind of person focused authenticated firewall traversal be easily applied to IoT devices. Many enterprises routinely scan DHCPv4 logs to make inventories of devices, but these only help for devices which do IPv4, and which use DHCP. One response is [RFC9686], to allow IPv6 devices to register their name via DHCP, and this is likely to be somewhat useful for some systems.

Enterprises also will collect data from the ARP and IPv6 Neighbor Discovery tables of their routers, and this is probably the most accurate way to create some kind of inventory. But the result are

just ethernet addresses. When they are IEEE OUI derived, it might point to a brand of device, but it might also just point to the brand of Ethernet adapter used. Getting further information out the device can be difficult.

Manufacturer Usage Descriptions (MUD) [RFC8520] are an emerging technology which can provide a reliable link back to not just the manufacturer, but also the device type, and even provide access to ways in which to access the trustworthiness of the device [I-D.birkholz-rats-mud].

This document proposes an active protocol by which the table of MAC addresses can be turned into a MUD URL.

2. Protocol

1. Make IPv6 Link-Local connection to SLAAC-Ethernet derived IPv6 address on port TBD2.

2. Start TLS on this port.

3. Device uses it’s IDevID certificate to respond to TLS request.

4. Do some trivial request over TLS.

5. Extract MUD URL from IDevID certificate.

3. Privacy Considerations

Many.

4. Security Considerations

Even more.

Much potential for abuse by malware.

5. IANA Considerations

This will need a TCP port number allocated, and perhaps also a CoAPS/DTLS port number.

6. Acknowledgements

Hello.

7. Changelog

8. References

8.1. Normative References

[I-D.birkholz-rats-mud]
Birkholz, H. and M. Richardson, "MUD-Based RATS Resources Discovery", Work in Progress, Internet-Draft, draft-birkholz-rats-mud-01, 22 February 2025, <https://datatracker.ietf.org/doc/html/draft-birkholz-rats-mud-01>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", RFC 8520, DOI 10.17487/RFC8520, March 2019, <https://www.rfc-editor.org/info/rfc8520>.

8.2. Informative References

[nmap] "NMAP", 15 April 2025, <https://nmap.org/>.

[RFC1929] Leech, M., "Username/Password Authentication for SOCKS V5", RFC 1929, DOI 10.17487/RFC1929, March 1996, <https://www.rfc-editor.org/info/rfc1929>.

[RFC9238] Richardson, M., Latour, J., and H. Habibi Gharakheili, "Loading Manufacturer Usage Description (MUD) URLs from QR Codes", RFC 9238, DOI 10.17487/RFC9238, May 2022, <https://www.rfc-editor.org/info/rfc9238>.

[RFC9686] Kumari, W., Krishnan, S., Asati, R., Colitti, L., Linkova, J., and S. Jiang, "Registering Self-Generated IPv6 Addresses Using DHCPv6", RFC 9686, DOI 10.17487/RFC9686, December 2024, <https://www.rfc-editor.org/info/rfc9686>.

[RFC9724] Z炭単iga, JC., Bernardos, CJ., Ed., and A. Andersdotter, "State of Affairs for Randomized and Changing Media Access Control (MAC) Addresses", RFC 9724, DOI 10.17487/RFC9724, March 2025, <https://www.rfc-editor.org/info/rfc9724>.

[RFC9726] Richardson, M. and W. Pan, "Operational Considerations for Use of DNS in Internet of Things (IoT) Devices", BCP 241, RFC 9726, DOI 10.17487/RFC9726, March 2025, <https://www.rfc-editor.org/info/rfc9726>.

Author’s Address

Michael Richardson
Sandelman Software Works
Email: mcr+ietf@sandelman.ca