

mif Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 2, 2015

S. Krishnan
Ericsson
J. Korhonen
Broadcom
S. Bhandari
Cisco Systems
S. Gundavelli
Cisco
August 29, 2014

Identification of provisioning domains
draft-ietf-mif-mpvd-id-00

Abstract

The MIF working group is producing a solution to solve the issues that are associated with nodes that can be attached to multiple networks. This document describes several methods of generating identification information for provisioning them and a format for carrying such identification in configuration protocols.

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 <http://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 March 2, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology	2
3.	Provisioning domain identity format	2
4.	Security Considerations	3
5.	IANA Considerations	3
6.	Acknowledgements	4
7.	Normative References	4
	Authors' Addresses	4

[1.](#) Introduction

The MIF working group is producing a solution to solve the issues that are associated with nodes that can be attached to multiple networks based on the Multiple Provisioning Domains (MPVD) architecture work [[I-D.ietf-mif-mpvd-arch](#)]. This document describes a format for carrying identification information along with a few alternatives for reasonable sources for PVD identification. Since the PVD IDs are expected to be unique, the identification sources provide some level of uniqueness using either a hierarchical structure (e.g. FQDNs and OIDs) or some form of randomness (e.g. UUID and ULAs). Any source that does not provide either guaranteed or probabilistic uniqueness is probably not a good candidate for identifying provisioning domains.

[2.](#) Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

[3.](#) Provisioning domain identity format

The identity of the PVD is independent of the configuration protocol used to communicate it and is formatted as follows.

```

0          1          2          3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   id-type   |   id-length   |                                     |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```



```

+           PVD identity information           +
.           (variable length)                 .
+-----+

```

PVD ID Option

- o id-type: Describes the type of identification information.
This document defines six types of PVD identity information
 - 0x01: UUID [[RFC4122](#)]
 - 0x02: UTF-8 string
 - 0x03: OID [[OID](#)]
 - 0x04: NAI Realm [[RFC4282](#)]
 - 0x05: FQDN
 - 0x06: ULA Prefix [[RFC4193](#)]
 Further types can be added by IANA action.
- o id-length: Length of the PVD identification in octets
not including the id-type and id-length fields.
- o PVD identity information: The PVD identification that is
based on the id-type.

4. Security Considerations

An attacker may attempt to modify the PVD identity provided in a configuration protocol. These attacks can be prevented by using the configuration protocol mechanisms such as SEND [[RFC3971](#)] and DHCPv6 AUTH option [[RFC3315](#)] that detect any form of tampering with the configuration.

A compromised configuration source, on the other hand, cannot easily be detected by a configuration client. The only real way to avoid this is that the PVD identification is directly associable to some form of authentication and authorization information from the owner of the PVD (e.g. an FQDN can be associated with a DANE cert). Then, this attack can be detected by the client by verifying the authentication and authorization information provided inside the PVD container option after verifying its trust towards the PVD owner (e.g. a certificate with a well-known/common trust anchor that).

5. IANA Considerations

This document creates a new registry for PVD id types. The initial values are listed below

```

0x01: UUID [RFC4122]
0x02: UTF-8 string

```


0x03: OID [[OID](#)]
0x04: NAI Realm [[RFC4282](#)]
0x05: FQDN
0x06: ULA Prefix [[RFC4193](#)]

6. Acknowledgements

The authors would like to thank the members of the MIF architecture design team, Ted Lemon, Brian Carpenter, Bernie Volz and Alper Yegin for their contributions to this draft.

7. Normative References

- [I-D.ietf-mif-mpvd-arch]
Anipko, D., "Multiple Provisioning Domain Architecture", [draft-ietf-mif-mpvd-arch-03](#) (work in progress), August 2014.
- [OID] IANA, "PRIVATE ENTERPRISE NUMBERS", SMI Network Management Private Enterprise Codes, <http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers>, March 2013.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), July 2003.
- [RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.
- [RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", [RFC 4122](#), July 2005.
- [RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", [RFC 4282](#), December 2005.

Authors' Addresses

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x42871
Email: suresh.krishnan@ericsson.com

Jouni Korhonen
Broadcom Communications
Porkkalankatu 24
FIN-00180 Helsinki
Finland

Email: jouni.nospam@gmail.com

Shwetha Bhandari
Cisco Systems
Cessna Business Park, Sarjapura Marathalli Outer Ring Road
Bangalore, KARNATAKA 560 087
India

Phone: +91 80 4426 0474
Email: shwethab@cisco.com

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com

