mif Working Group   S. Krishnan
Internet-Draft   Ericsson
Intended status: Standards Track   J. Korhonen
Expires: April 21, 2016   Broadcom Corporation
                                                     S. Bhandari
                                                   Cisco Systems
                                                   S. Gundavelli
                                                           Cisco
                                                October 19, 2015

Identification of provisioning domains
draft-ietf-mif-mpvd-id-02

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 April 21, 2016.

Copyright Notice

Table of Contents

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 [RFC7556]. This document describes a format for
carrying identification information along with a few alternatives for
reasonable sources for Provisioning Domain (PVD) identification.
Since the PVD identities (PVD ID) 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. Furthermore, the PVD identity SHOULD only
contain information related to the identification purposes and not
encode additional provisioning domain specific configuration
information. The configuration protocol used and its extensions are
meant for that purpose [I-D.ietf-mif-mpvd-dhcp-support]

[I-D.ietf-mif-mpvd-ndp-support]. The PVD identity 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 [RFC1035]
         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. The length
      of the PVD identity is dependent on the id-type and is
      defined by the document that specifies that kind of ID.

   o PVD identity information: The PVD identification that is
      based on the id-typ.The format of the PVD identity is
      dependent on the id-type and is defined by the document that
      specifies that kind of ID.

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 (such as the OPTION_PVD_AUTH inside OPTION_PVD
[I-D.ietf-mif-mpvd-dhcp-support] or the Key Hash and Digital
Signature inside PVD_CO [I-D.ietf-mif-mpvd-ndp-support]) 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 [RFC1035]
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. The authors also thank Ian
Farrer, Erik Kline, Dave Thaler and Steven Barth for their reviews
and comments that improved this draft.

7. References

7.1. Normative References

[OID]   IANA, "PRIVATE ENTERPRISE NUMBERS", SMI Network Management
             Private Enterprise Codes, http://www.iana.org/assignments/
             enterprise-numbers/enterprise-numbers, March 2013.

[RFC1035]   Mockapetris, P., "Domain names - implementation and
             specification", STD 13, RFC 1035, DOI 10.17487/RFC1035,
             November 1987, <http://www.rfc-editor.org/info/rfc1035>.

[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, DOI
              10.17487/RFC4122, July 2005,
              <http://www.rfc-editor.org/info/rfc4122>.

   [RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The
              Network Access Identifier", RFC 4282, DOI 10.17487/
              RFC4282, December 2005,
              <http://www.rfc-editor.org/info/rfc4282>.

7.2. Informative References

   [I-D.ietf-mif-mpvd-dhcp-support]
              Krishnan, S., Korhonen, J., and S. Bhandari, "Support for
              multiple provisioning domains in DHCPv6", draft-ietf-mif-
              mpvd-dhcp-support-01 (work in progress), March 2015.

   [I-D.ietf-mif-mpvd-ndp-support]
              Korhonen, J., Krishnan, S., and S. Gundavelli, "Support
              for multiple provisioning domains in IPv6 Neighbor
              Discovery Protocol", draft-ietf-mif-mpvd-ndp-support-01
              (work in progress), February 2015.

   [RFC7556] Anipko, D., Ed., "Multiple Provisioning Domain
              Architecture", RFC 7556, DOI 10.17487/RFC7556, June 2015,
              <http://www.rfc-editor.org/info/rfc7556>.

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 Corporation
3151 Zanker Road
San Jose, CA 95134
USA

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