DHC Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 21, 2016

S. Krishnan
Ericsson
J. Korhonen
Broadcom Corporation
S. Bhandari
Cisco Systems

October 19, 2015

Support for multiple provisioning domains in DHCPv6
draft-ietf-mif-mpvd-dhcp-support-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. One part of the solution requires associating configuration information with provisioning domains. This document details how configuration information provided through DHCPv6 can be associated with provisioning domains.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 2
3. PVD Container option 3
4. PVD Identity option 3
5. PVD Authentication and Authorization option 4
  5.1. Authentication is optional 5
6. Set of allowable options 5
7. Behaviour of DHCPv6 entities 5
  7.1. Client and Requesting Router Behavior 5
  7.2. Relay Agent Behavior 6
  7.3. Server and Delegating Router Behavior 6
8. Redistributing configuration information 7
9. Security Considerations 7
10. IANA Considerations 8
11. Acknowledgements 8
12. References 8
  12.1. Normative References 8
  12.2. Informative References 9
Authors' Addresses 9

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]. One part of the solution requires associating configuration information with provisioning domains. This document describes a DHCPv6 mechanism for explicitly indicating provisioning domain information along with any configuration that will be provided. The proposed mechanism uses a DHCPv6 option that indicates the identity of the provisioning domain and encapsulates the options that contain the configuration information as well as any accompanying authentication/authorization information.

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. PVD Container option

The PVD container option is used to encapsulate and group together all the configuration options that belong to the explicitly identified provisioning domain. The PVD container option MUST encapsulate exactly one OPTION_PVD_ID. The PVD container option MAY occur multiple times in the same message, but each of these PVD container options MUST have a different PVD identity specified under its PVD identity option. The PVD container option SHOULD contain at most one (i.e. zero or one) OPTION_PVD_AUTH.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        OPTION_PVD             |         option-length         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +            encapsulated-options (variable length)             .
   .                                                               .
   +---------------------------------------------------------------+
```

Figure 1: PVD Container Option

- o option-code: OPTION_PVD (TBA1)

- o option-length: Length of encapsulated options

- o encapsulated-options: options associated with this provisioning domain.

4. PVD Identity option

The PVD identity option is used to explicitly indicate the identity of the provisioning domain that is associated with the configuration information encapsulated by the PVD container option.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |       OPTION_PVD_ID           |         option-length         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                   PVD identity information                    |
   +                       (variable length)                       +
   +                                                               +
   .                                                               .
   +---------------------------------------------------------------+
```

Figure 2: PVD ID Option

- option-code: OPTION_PVD_ID (TBA2)

- option-length: Length of PVD identity information

- PVD identity information: The provisioning domain identity. The contents of this field is defined in a separate document [I-D.ietf-mif-mpvd-id].

5. PVD Authentication and Authorization option

The PVD authentication and authorization option contains information that could be used by the DHCPv6 client to verify whether the configuration information provided was not tampered with by the DHCPv6 server as well as establishing that the DHCPv6 server was authorized to advertise the information on behalf of the PVD per OPTION_PVD basis. The contents of the authentication/authorization information is provided by the owner of the provisioning domain and is completely opaque to the DHCPv6 server that passes along the information unmodified. Every OPTION_PVD option SHOULD contain at most one (i.e. zero or one) OPTION_PVD_AUTH option. If present, the OPTION_PVD_AUTH option MUST be the last option inside the OPTION_PVD option.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |      OPTION_PVD_AUTH          |         option-length         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <+
   |   name-type   |               key-hash                        :  |
   +-+-+-+-+-+-+-+-+                                               :  |
   :                                                               :
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Auth
   :                                                               : info
   :                      digital-signature                        :  |
   :                                                               :  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <+
```

Figure 3: PVD Auth Option

- option-code: OPTION_PVD_AUTH (TBA3)

- option-length: Length of the Auth info

- name-type: Names the algorithm used to identify a specific X.509 certificate using the method defined for the Subject Key Identifier (SKI) extension for the X.509 certificates. The usage and the Name Type registry aligns with the mechanism

defined for SeND [RFC6494][RFC6495].
Name Type values starting
from 3 are supported and an implementation MUST at least support
SHA-1 (value 3).

- key-hash: A hash of the public key using the algorithm identified by the Name Type. The procedure how the Key Hash is calculated is defined in [RFC3971] and [RFC6495].

- digital-signature: A signature calculated over the encapsulating OPTION_PVD including all option data from the beginning of the option while setting the digital-signature field to zero. The procedure of calculating the signature is identical to the one defined for SeND [RFC3971].

5.1. Authentication is optional

The OPTION_PVD_AUTH will be sent only if it is requested in the ORO.If the client does not request this option, it will not get a signed PVD option. Clients that request the OPTION_PVD with the intention of redistributing configuration information to other clients (e.g. CPE routers) SHOULD NOT request the OPTION_PVD_AUTH in the ORO. This allows them to send out a subset of the received options to their clients and also allows them to support PVD unaware clients by sending out the options without PVD information.

6. Set of allowable options

The PVD container option MAY be used to encapsulate any allocated DHCPv6 options but MUST NOT be used to encapsulate another OPTION_PVD option.

7. Behaviour of DHCPv6 entities

This section describes role of DHCPv6 entities involved in requesting and receiving DHCPv6 configuration or prefix and address allocation.

7.1. Client and Requesting Router Behavior

DHCPv6 client or requesting router can request for configuration from provisioning domain in the following ways:

- In the SOLICIT message it MAY include OPTION_PVD_ID requesting configuration for the specific PVD ID indicated in the OPTION_PVD_ID option. It can include multiple OPTION_PVD_ID options to indicate its preference for more than one provisioning domain. The PVD ID it requests is learnt via configuration or any other out of band mechanism not defined in this document.

- In the SOLICIT message include an OPTION_ORO option with the OPTION_PVD option code to request configuration from all the PVDs that the DHCPv6 server can provide.

The client or requesting router parses OPTION_PVD options in the response message. The Client or Requesting router MUST then include all or subset of the received OPTION_PVD options in the REQUEST message so that it will be responsible for the configuration information selected.

If DHCPv6 client or requesting router receives OPTION_PVD options but does not support PVD, it SHOULD ignore the received option(s).

7.2. Relay Agent Behavior

If the relay agent supports both the Relay-Supplied DHCP Option (RSOO) [RFC6422] and the PVD, and it is configured to request configuration data for clients in one or more provisioning domains, then the relay agent MAY include the RSOO in the Relay-Forward message. The RSOO MAY contain zero or more OPTION_PVD options. The relay agent MUST NOT include any OPTION_PVD options into the RSOO unless the client has indicated support for the PVD as described in Section Section 7.1.

7.3. Server and Delegating Router Behavior

If the Server or Delegating router supports PVD and it is configured to provide configuration data in one or more provisioning domains, it selects configuration for the PVD based allocation in the following way:

- If OPTION_PVD option code within OPTION_ORO is not present in the request, it MUST NOT include provisioning domain based configuration. It MAY select configuration and prefix allocation from a default PVD defined.

- If OPTION_PVD_ID is included, it selects information to be offered from that specific PVD if available.

- If OPTION_PVD option code within OPTION_ORO is included, then based on its configuration and policy it MAY offer configuration from the available PVD(s).

When PVD information and configuration are selected for address and prefix allocation the server or delegating router responds with an ADVERTISE message after populating OPTION_PVD.

If OPTION_PVD is not included, then the server or delegating router MAY allocate the prefix and provide configuration as specified in [RFC3315] and[RFC3633] and MUST NOT include OPTION_PVD option in the response.

If OPTION_ORO option includes the OPTION_PVD option code but the server or delegating router does not support PVD, then it SHOULD ignore the OPTION_PVD and OPTION_PVD_ID options received.

If both client/requesting router and server/delegating router support PVD but cannot offer configuration with PVD for any other reason, it MUST respond to client/requesting router with appropriate status code as specified in [RFC3315] and [RFC3633].

Similarly, if the OPTION_PVD is received in the RSOO from the relay agent the above described procedures apply for including the PVD specific configuration information back to the client.

8. Redistributing configuration information

Clients that redistribute configuration information further to legacy clients (e.g. homenet CPEs) after stripping out the PVD information need to exercise caution when removing information from the PVD containers and distributing them as top level options. Configuration information that is consistent within a PVD container may not work equally well when mixed with other top level configuration information or information from other PVD containers. e.g. Using DNS server information from one PVD container while using address/prefix from another may lead to unexpected results.

9. Security Considerations

An attacker may attempt to modify the information provided inside the PVD container option. These attacks can easily be prevented by using the DHCPv6 AUTH option [RFC3315] that would detect any form of tampering with the DHCPv6 message contents.

A compromised DHCPv6 server or relay agent may insert configuration information related to PVDs it is not authorized to advertise. e.g. A coffee shop DHCPv6 server may provide configuration information purporting to be from an enterprise and may try to attract enterprise related traffic. The only real way to avoid this is that the PVD container contains embedded authentication and authorization information from the owner of the PVD. 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).

A compromised configuration source or an on-link attacker may try to capture advertised configuration information and replay it on a different link or at a future point in time. This can be avoided by including some replay protection mechanism such as a timestamp or a nonce inside the PVD container to ensure freshness of the provided information.

10. IANA Considerations

This document defines three new DHCPv6 options to be allocated out of the registry at http://www.iana.org/assignments/dhcpv6-parameters/

OPTION_PVD (TBA1)
OPTION_PVD_ID (TBA2)
OPTION_PVD_AUTH (TBA3)

This document also adds OPTION_PVD (TBA1) into the "Options Permitted in the Relay-Supplied Options Option" registry at http://www.iana.org/assignments/dhcpv6-parameters/

11. Acknowledgements

The authors would like to thank the members of the MIF architecture design team for their comments that led to the creation of this draft. The authors would also thank Ian Farrer and Steven Barth for their reviews and comments.

12. References

12.1. Normative References

[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.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[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>.

[RFC6422] Lemon, T. and Q. Wu, "Relay-Supplied DHCP Options", RFC 6422, DOI 10.17487/RFC6422, December 2011, <http://www.rfc-editor.org/info/rfc6422>.

[RFC6494] Gagliano, R., Krishnan, S., and A. Kukec, "Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND)", RFC 6494, DOI 10.17487/RFC6494, February 2012, <http://www.rfc-editor.org/info/rfc6494>.

[RFC6495] Gagliano, R., Krishnan, S., and A. Kukec, "Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name Type Fields", RFC 6495, DOI 10.17487/RFC6495, February 2012, <http://www.rfc-editor.org/info/rfc6495>.

12.2. Informative References

[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