IPv6 Maintenance
Internet-Draft
Intended status: Standards Track
Expires: September 1, 2015

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

February 28, 2015

Support for multiple provisioning domains in IPv6 Neighbor Discovery Protocol
draft-ietf-mif-mpvd-ndp-support-01

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 IPv6 Neighbor Discovery Protocol can be associated with provisioning domains.

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 September 1, 2015.

Copyright Notice

Copyright (c) 2015 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 3
2. Terminology 3
3. PVD Container option 3
4. PVD Identity option 6
5. Set of allowable options 7
6. Security Considerations 7
7. IANA Considerations 7
8. Acknowledgements 8
9. References 8
9.1. Normative References 8
9.2. Informative References 8
Appendix A. Examples 9
A.1. One implicit PVD and one explicit PVD 9
Authors' Addresses 11

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]. One part of the solution requires associating configuration information with Provisioning Domains (PVD). This document describes an IPv6 Neighbor Discovery Protocol (NDP) [RFC4861] mechanism for explicitly indicating provisioning domain information along with any configuration that will be provided. The proposed mechanism uses an NDP 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. The solution defined in this document aligns as much as possible with the existing IPv6 Neighbor Discovery security, namely with Secure Neighbor Discovery (SeND) [RFC3971].

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 (PVD_CO) is used to mark the start of the configuration options that belong to the explicitly identified provisioning domain. The PVD container option MUST encapsulate exactly one PVD identifier option (PVD_ID, see Section 4). The PVD container option MAY occur multiple times in the same NDP message but each of these PVD container options MUST have a different PVD identity specified under its PVD identity option. The PVD container options MUST NOT be nested.

A PVD container is intended to be used in IPv6 Router Advertisement (RA) NDP messages. However, including a PVD container or identity options inside a Router Solicitation (RS) NDP messages is also possible (actually, in this way a host can solicit for information from a specific provisioning domain). The PVD container option MUST NOT be included in a NDP message without accompanying PVD identity option (see Section 4). If, for some reason, the NDP message does not include the accompanying PVD identity option, then the implementation MUST ignore the PVD container option and SHOULD log the event. The PVD container MUST NOT be fragmented i.e., should the IPv6 packet be fragmented, the PVD container and the accompanying PVD

identity MUST both be inside the same fragment.

Since implementations are required to ignore any unrecognized options [RFC4861], the backward compatibility and the reuse of existing NDP options is implicitly enabled. Implementations that do not recognize the PVD container option plain ignore it and also skip PVD container option "encapsulated" NDP options normally without associating them into any provisioning domain (since the implementation has no notion of provisioning domains). For example, the PVD container could "encapsulate" a Prefix Information Option (PIO), which would mark that this certain advertised IPv6 prefix belongs and originates from a specific provisioning domain. However, if the implementation does not understand provisioning domains, then this specific PIO is also skipped and not configured to the interface.

The optional security for the PVD container is based on X.509 certificates [RFC6487] and reuses mechanisms already defined for SeND [RFC3971] [RFC6495]. However, the use of PVD containers does not assume or depend on SeND being deployed or even implemented. The PVD containers SHOULD be signed per PVD certificates, which provides both integrity protection and proves that the configuration information source is authorized for advertising the given information. See [RFC6494] for discussion how to enable deployments where the certificates needed to sign PVD containers) belong to different administrative domains i.e. to different provisioning domains.

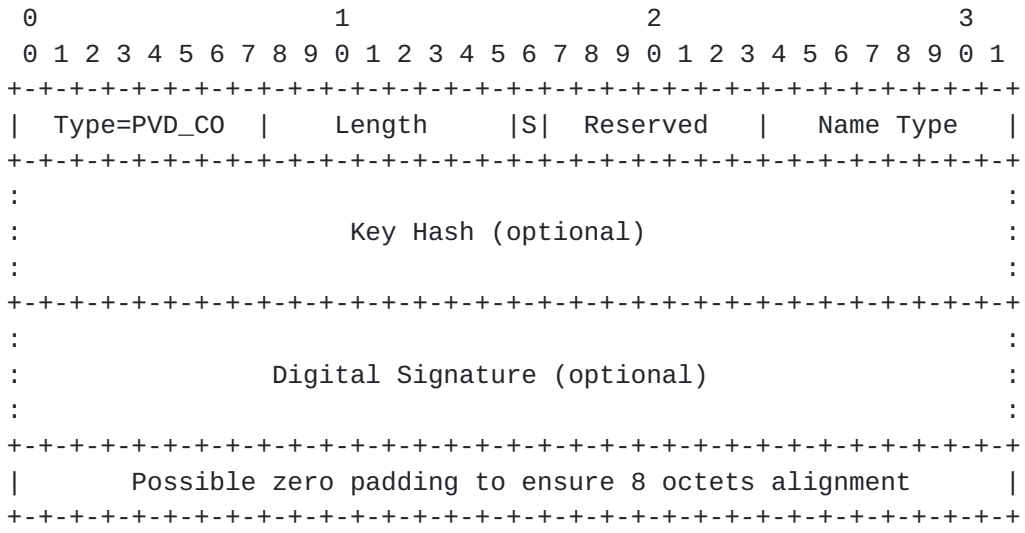

Figure 1: PVD Container Option

Type

PVD Container; Set to TBD1.

Length

Length of the PVD_CO. The actual length depends on the number of "encapsulated" NDP options, the length of the PVD identifier option and the optional Key Hash/Digital Signature/Padding.

S

Security enabled/disabled flag. If S=0 then security (signing) of the PVD_CO is disabled. If S=1 then security (signing) is enabled.

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 [RFC6495]. Name Type values starting from 3 are supported and an implementation MUST at least support SHA-1 (value 3). Note that if S=0 the Name field serves no use.

Key Hash

This field is only present when S=1. 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

This field is only present when S=1. A signature calculated over the PVD_CO option including all option data from the beginning of the option until to the end of the container. The procedure of calculating the signature is identical to the one defined for SeND [RFC3971]. During the signature calculation the contents of the Digital Signature option MUST be treated as all zero.

Implementations MUST ensure that the PVD container option meets the 8 octets NDP option alignment requirement. This MAY imply adding padding zero octets to the tail of the PVD container option until the alignment requirement has been met. The padding is independent of the 'S' flag setting.

If the PVD_CO does not contain a digital signature, then other means to secure the integrity of the NDP message SHOULD be provided, such as utilizing SeND. However, the security provided by SeND is for the entire NDP message and does not allow verifying whether the sender of the NDP message is actually authorized for the information for the provisioning domain.

If the PVD_CO contains a signature and the verification fails, then the whole PVD_CO, PVD_ID and other NDP options MUST be silently ignored and the event SHOULD be logged.

4. PVD Identity option

The PVD identity option (PVD_ID) is used to explicitly indicate the identity of the provisioning domain that is associated with the configuration information encapsulated by the PVD container option. A PVD container option MUST have exactly one PVD identity option. However, the PVD identity option MAY also be included in a NDP message without the PVD container option. In this case it merely serves as a hint of provisioning domain and could, for example, be used in an RS message to solicit information from specific provisioning domains.

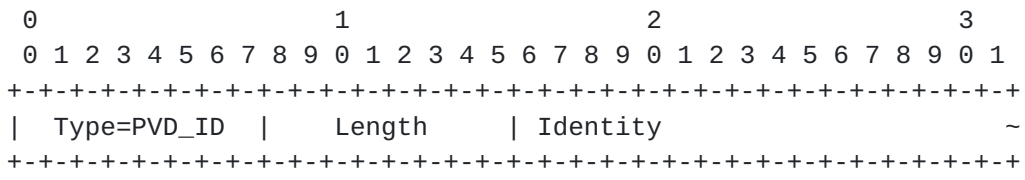

Figure 2: PVD_ID Option

Type

PVD identifier; Set to TBD2.

Length

Length of the PVD_ID.

Identity

The provisioning domain identity. The contents of this field is defined in a separate document [I-D.ietf-mif-mpvd-id]. Note that the Identity field may need to be zero padded at the tail to meets the natural NDP options' alignment.

If the receiver of the PVD identity option does not understand any of

the ID-Types, then anything belonging to this provisioning domain MUST be silently discarded. This would mean the PVD identity option, the PVD container option and all other options.

5. Set of allowable options

The PVD container option MAY be used to encapsulate any allocated IPv6 NDP options, which may appear more than once in a NDP message. The PVD container option MUST NOT be used to encapsulate other PVD_CO option(s).

6. Security Considerations

An attacker may attempt to modify the information provided inside the PVD container option. These attacks can easily be prevented by using SeND [RFC3971] or per PVD container signature that would detect any form of tampering with the IPv6 NDP message contents.

A compromised router may advertise configuration information related to provisioning domains it is not authorized to advertise. e.g. A coffee shop router 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 provisioning domain container contains embedded authentication and authorization information from the owner of the provisioning domain. 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 provisioning domain 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. This specification does not define a replay protection solution. Rather it is assumed that if replay protection is required, the access network and hosts also deploy existing security solutions such as SeND [RFC3971].

7. IANA Considerations

This document defines two new IPv6 NDP options into the "IPv6 Neighbor Discovery Option Formats" registry. The options TBD1 and TBD2 are described in Section 3 and Section 4.

8. 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.

9. References

9.1. Normative References

[I-D.ietf-mif-mpvd-id]
Krishnan, S., Korhonen, J., Bhandari, S., and S. Gundavelli, "Identification of provisioning domains", draft-ietf-mif-mpvd-id-00 (work in progress), August 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC6494] Gagliano, R., Krishnan, S., and A. Kukec, "Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND)", RFC 6494, February 2012.

[RFC6495] Gagliano, R., Krishnan, S., and A. Kukec, "Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name Type Fields", RFC 6495, February 2012.

9.2. Informative References

[I-D.ietf-mif-mpvd-arch]
Anipko, D., "Multiple Provisioning Domain Architecture", draft-ietf-mif-mpvd-arch-10 (work in progress), February 2015.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, February 2012.

Appendix A. Examples

A.1. One implicit PVD and one explicit PVD

Figure 3 shows how the NDP options are laid out in an RA for one implicit provisioning domain and one explicit provisioning domain. The example does not include security (and signing of the PVD container). The assumption is the PVD identity consumes 14 octets.

The explicit provisioning domain ("starducks.example.com" in a NAI Realm format) contains a specific PIO for 2001:db8:abad:cafe::/64 and the MTU of 1337 octets. The implicit provisioning domain configures a prefix 2001:db8:cafe:babe::/64 and the link MTU of 1500 octets. There are two cases: 1) the host receiving the RA implements provisioning domains and 2) the host does not understand provisioning domains.

1. The host recognizes the PVD_CO and "starts" a provisioning domain specific configuration. Security is disabled, thus there are no Key Hash or Digital Signature fields to process. The prefix 2001:db8:abad:cafe::/64 is found and configured on the interface. Once the PVD_ID option is located the interface prefix configuration for 2001:db8:abad:cafe::/64 and the MTU of 1337 octets can be associated to the provisioning domain found in the PVD_ID option.

   The rest of the options are parsed and configured into the implicit provisioning domain since there is no encapsulating provisioning domain. The interface is configured with prefix 2001:db8:cafe:babe::/64. The implicit provisioning domain uses the link MTU of 1500 octets, whereas the "starducks.example.com" provisioning domain uses the MTU of 1337 octets (this means when packets are sourced using 2001:db8:abad:cafe::/64 prefix the link MTU is different than when sourcing packets using 2001:db8:cafe:babe::/64 prefix).

2. The host ignores the PVD_CO (including the PVD_ID and other options) and ends up configuring one prefix on its interface (2001:db8:cafe:babe::/64) with a link MTU of 1500 octets.

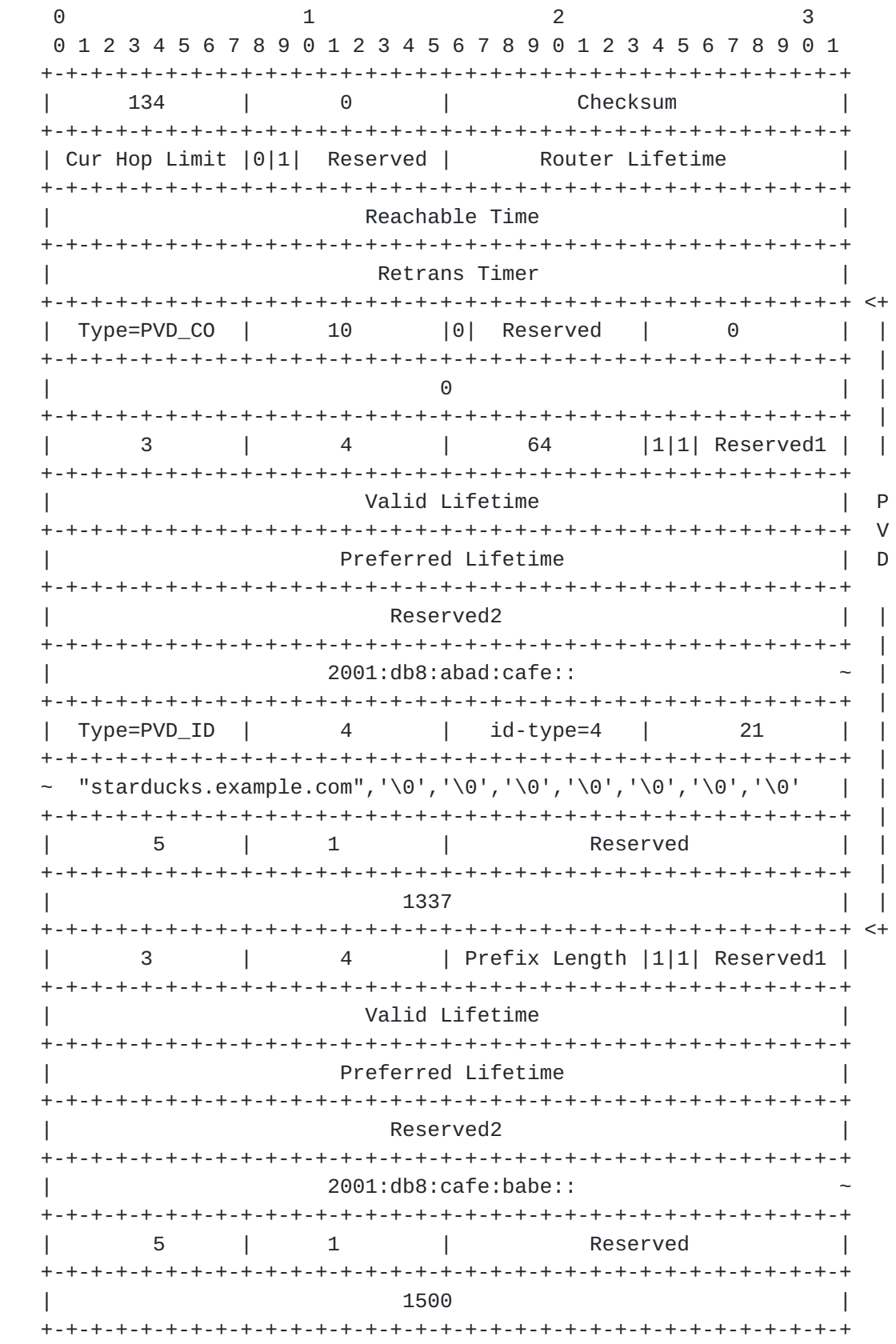
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
134
0
Checksum
Cur Hop Limit
0|1|
Reserved
Router Lifetime
Reachable Time
Retrans Timer
Type=PVD_CO
10
0|
Reserved
0
0
3
4
64
1|1|
Reserved1
Valid Lifetime
Preferred Lifetime
Reserved2
2001:db8:abad:cafe::
Type=PVD_ID
4
id-type=4
21
"starducks.example.com",'\0','\0','\0','\0','\0','\0','\0'
5
1
Reserved
1337
3
4
Prefix Length
1|1|
Reserved1
Valid Lifetime
Preferred Lifetime
Reserved2
2001:db8:cafe:babe::
5
1
Reserved
1500
PVD

Figure 3: An RA with one implicit PVD and one explicit PVD

Authors' Addresses

Jouni Korhonen
Broadcom Corporation
3151 Zanker Road
San Jose, CA 95134
USA

Email: jouni.nospam@gmail.com

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

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

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

Email: sgundave@cisco.com