

dhc Working Group	R. Droms	
Internet-Draft	Cisco Systems, Inc.	
Intended status: Standards Track	March 25, 2009	
Expires: September 26, 2009		

[TOC](#)

Container Option for Server Configuration draft-ietf-dhc-container-opt-05.txt

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on September 26, 2009.

Copyright Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

In some DHCP service deployments, it is desirable for a DHCP server in one administrative domain to pass configuration options to a DHCP server in a different administrative domain. This DHCP option carries a set of DHCP options that can be used by another DHCP server.

Table of Contents

1.	Introduction
2.	Terminology
3.	Problem statement and requirements for RG DHCP server configuration
4.	Design alternatives
5.	Semantics and syntax of the Container option
5.1.	DHCPv4 Container option
5.2.	DHCPv6 Container option
5.3.	SP server behavior
5.4.	RG client behavior
5.5.	RG server behavior
6.	Security Considerations
7.	IANA Considerations
8.	Change Log
8.1.	Revision -02
8.2.	Revision -03
8.3.	Revision -04
9.	Related Work
10.	References
10.1.	Normative References
10.2.	Informative References
§	Author's Address

1. Introduction

[TOC](#)

In some DHCP service deployments, it is desirable to pass configuration options from a DHCP server in one administrative domain to another DHCP server in a different administrative domain. In one example of such a deployment, an IPTV service provider (SP) may need to provide certain SP domain-specific information to IPTV device(s) located in the consumer domain. This information is sent from the IPTV SP DHCP server to the consumer DHCP server located in the Residential Gateway (RG), which can then be passed along to IPTV device(s) in the subscriber network.

Existing RGs may pass some configuration information received by the RG DHCP client to the RG server for configuration of devices attached to the consumer network. There are several motivations for this option:

- *The devices attached to the consumer network may require different configuration information than the DHCP options provided to the RG.

- *Existing RG DHCP clients are typically not coded to process new DHCP options and, therefore, will be unable to pass those new options to the RG DHCP server.

*Existing RG DHCP clients are typically coded to pass only a fixed list of DHCP options to the RG DHCP server and, therefore, will be unable to pass newly defined options to the RG DHCP server.

The DHCP Container option defined in this document provides a mechanism through which the RG DHCP client can pass DHCP options to the RG DHCP server without explicit knowledge of the semantics of those options. With this option, the SP DHCP server can pass both current and future DHCP options to the RG DHCP server.

The DHCP Container option does not carry IP addresses, IPv6 prefixes or other information about leases. It carries other configuration information.

2. Terminology

[TOC](#)

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 \(Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.\)](#) [RFC2119].

The following terms and acronyms are used in this document:

DHCPv4 ["Dynamic Host Configuration Protocol" \(Droms, R., "Dynamic Host Configuration Protocol," March 1997.\)](#) [RFC2131]

DHCPv6 ["Dynamic Host Configuration Protocol for IPv6" \(Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 \(DHCPv6\)," July 2003.\)](#) [RFC3315]

DHCP DHCPv4 and/or DHCPv6

RG "residential gateway"; the device through which the consumer network connects to the broadband WAN; typically a layer 3 forwarding device

RG DHCP client (or "RG client") the DHCP client in the RG

RG DHCP server (or "RG server") the DHCP server in the RG

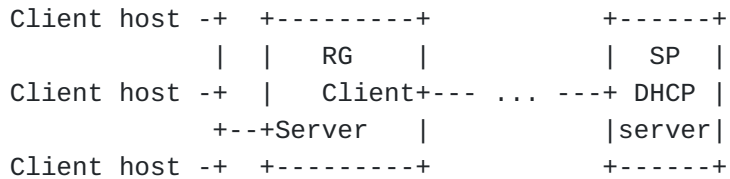
SP DHCP server (or "SP server") the DHCP server managed by the service provider (SP)

This document uses other terminology for DHCPv4 and DHCPv6 as defined in RFC 2131 and RFC 3315, respectively.

3. Problem statement and requirements for RG DHCP server configuration

[TOC](#)

The following diagram shows the components in a network deployment using the DHCP Container option:



In this diagram, the RG client engages in DHCP message exchanges with the SP server to obtain its IP address and other configuration information.

The problem under consideration in this document is to transmit configuration information from the SP DHCP server to hosts, such as computers and set-top boxes, attached to the consumer network. The problem solution has the following requirements:

- *The SP server MUST be able to transmit different configuration information to the consumer devices than the DHCP options provided to the RG.
- *The SP server MUST be able to control which DHCP options are transmitted to the consumer device.
- *There MUST be a way for the SP server to pass DHCP options to be defined in the future to consumer devices.

4. Design alternatives

[TOC](#)

The following three designs meet the solution requirements:

- *SP server passes container option to RG client, which forwards contents to RG server; this alternative is the preferred solution
- *RG server does direct DHCP info request to SP server; this alternative is not preferred because it:
 - requires that the RG server include a DHCP client,

- requires that the SP server be able to differentiate between RG client and server requests, and it
- does not scale well, as it at least doubles the load on the SP server.

*RG server passes device requests to SP DHCP server; this alternative is not preferred because it:

- requires that the RG also function as a DHCP relay,
- requires that the RG relay function be configured with the IP addresses of the SP DHCP server(s), and it
- requires that the RG relay function differentiate between DHCP messages that are processed by the RG server and DHCP messages that are processed by the SP server, which does not scale well.

A variant on the preferred design would allow the inclusion of multiple sets of DHCP options intended for different classes of devices in the consumer network; e.g., the design would allow for one set of options for video set-top boxes and a second set of options for VoIP MTAs. The variant would require the specification of rules to be provided by the SP server through which the RG server would differentiate its clients and send the appropriate set of options to each device. At present, there is no requirement for differential configuration of consumer devices and this alternative is not defined in this document.

5. Semantics and syntax of the Container option

[TOC](#)

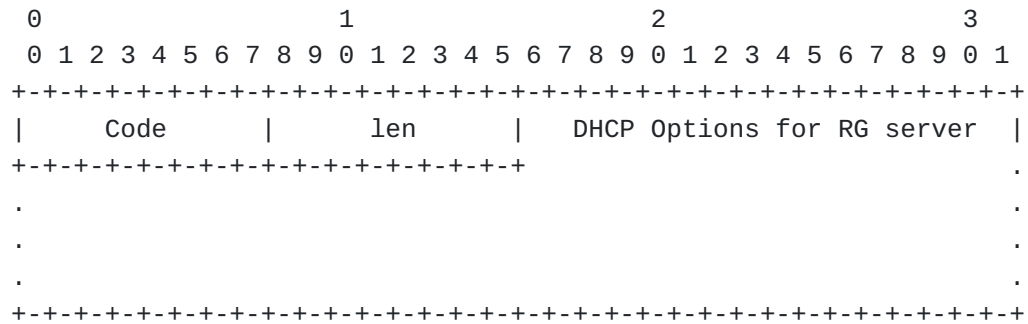
Along with configuration information intended for the RG, the SP server can include the DHCP Container option. When the RG client receives the DHCP Container option, it passes the contents of the option to the RG server. The means through which the information is passed between the RG client and the RG server is out of the scope of this document and left unspecified.

The DHCP options in this container are carried in DHCP message format (option-code/length/value). In this format, the contained options can be passed through a DHCP client to a co-located DHCP server without specific knowledge on the part of the client or the server of the semantics of the options.

[TOC](#)

5.1. DHCPv4 Container option

The DHCPv4 Container option has the following format:



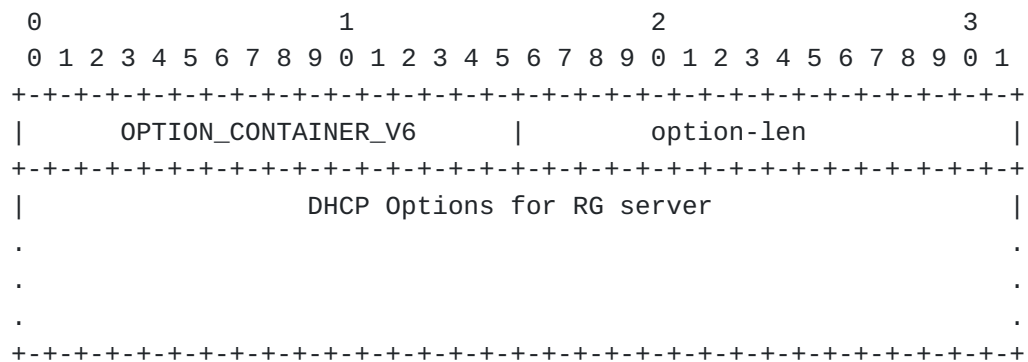
Code OPTION_CONTAINER_V4 (TBDv4)

len Length of options for RG server, in octets

5.2. DHCPv6 Container option

TOC

The DHCPv6 Container option has the following format:



```
option-code    OPTION_CONTAINER_V6 (TBDv6).
```

```
option-len  Length of options for RG server, in octets
```

5.3. SP server behavior

TOC

The SP server MAY include the Container option in any DHCP message sent to an RG client.

The policy through which the SP server is instructed to include a Container option for an RG client, and the policy determining the contents of the Container object are out of scope of this document and left unspecified.

5.4. RG client behavior

[TOC](#)

The RG client MUST pass the contents of the received Container option to the RG server without alteration. The details of the implementation through which the RG client parses the content of the Container option and passes the options to the RG server are out of scope for this document and left unspecified.

5.5. RG server behavior

[TOC](#)

The RG server MUST discard any options related to IP address assignment, IPv6 prefix delegation or operation of the DHCP protocol itself.

The Container option provides a mechanism through which the SP might be able to unilaterally control the configuration settings passed from a RG DHCP server to a host in the subscriber network. This configuration channel must be handled with some care if the subscriber is to retain desired control over the host configurations. The following behaviors limit the degree to which the SP can control host configuration:

- *The RG server MAY discard any undesired options, as determined by policy in the RG.
 - *The RG server MUST return to any DHCP client only those options requested by the DHCP client in a Parameter Request List option (DHCPv4 option code 55) or an Option Request option (DHCPv6 option code 6).
-

6. Security Considerations

[TOC](#)

A rogue server can use this option to pass invalid information to the RG client, which would then be passed to the Client hosts. This invalid information could be used to mount a denial of service attack or a man-in-the-middle attack against some applications.

Authentication of DHCP messages ([RFC 3118 \(Droms, R. and W. Arbaugh, "Authentication for DHCP Messages," June 2001.\)](#) [RFC3118] and section

20 of [RFC 3315 \(Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 \(DHCPv6\)," July 2003.\)](#) [RFC3315]) can be used to ensure that the contents of this option are not altered in transit between the DHCP server and client.

7. IANA Considerations

[TOC](#)

When this document is published, IANA is asked to assign an option tag from the "BOOTP Vendor Extensions and DHCP Options" registry for OPTION_CONTAINER_V4 (TBDv4).

When this document is published, IANA is asked to assign an option code from the "DHCPv6 Option Codes" registry for OPTION_CONTAINER_V6 (TBDv6).

8. Change Log

[TOC](#)

If this document is accepted for publication as an RFC, this change log is to be removed before publication.

8.1. Revision -02

[TOC](#)

*Corrected a cut-and-paste error in section "DHCPv6 Container option": The Time Protocol Servers option -> The DHCPv4 Container option

*Added text to section "RG Server Behavior" to address policy management concerns

8.2. Revision -03

[TOC](#)

Corrected several typos (thanks to Alfred Hoenes for his review).

[TOC](#)

8.3. Revision -04

Corrected additional typos (again, thanks to Alfred Hoenes for his review).

Added pointer to "CableLabs' DHCP Options Registry" as background for this option.

9. Related Work

[TOC](#)

The Container option is based on the CableLabs eRouter DHCP Container vendor-identifying vendor-specific option, as defined in ["CableLabs' DHCP Options Registry" \(CableLabs, "CableLabs' DHCP Options Registry \(CL-SP-CANN-DHCP-Reg-I02-080306\)," March 2008.\)](#) [eRouter].

10. References

[TOC](#)

10.1. Normative References

[TOC](#)

[RFC2119]	Bradner, S. , " Key words for use in RFCs to Indicate Requirement Levels ," BCP 14, RFC 2119, March 1997 (TXT , HTML , XML).
[RFC2131]	Droms, R. , " Dynamic Host Configuration Protocol ," RFC 2131, March 1997 (TXT , HTML , XML).
[RFC3118]	Droms, R. and W. Arbaugh, " Authentication for DHCP Messages ," RFC 3118, June 2001 (TXT).
[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 (TXT).

10.2. Informative References

[TOC](#)

[eRouter]	CableLabs, " CableLabs' DHCP Options Registry (CL-SP-CANN-DHCP-Reg-I02-080306) ," March 2008.
-----------	---

Author's Address

[TOC](#)

	Ralph Droms
--	-------------

	Cisco Systems, Inc.
	1414 Massachusetts Avenue
	Boxborough, MA 01719
	USA
Phone:	+1 978.936.1674
Email:	rdroms@cisco.com