

DHC Working Group
Internet Draft
Intended status: Standards Track
Expires: March 2011

Rajiv Asati
Cisco Systems

Ralph Droms
Cisco Systems

September 29, 2010

DHCP Relay Agent Configuration Option
draft-asati-dhc-relay-agent-config-00.txt

Abstract

This document defines a Dynamic Host Configuration Protocol (DHCP) Relay Agent Configuration option and associated machinery to configure the Relay Agent.

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), 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/lid-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 March 29, 2011.

Copyright Notice

Copyright (c) 2010 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.....4
- 2. Key Words to Reflect Requirements.....4
- 3. Problem / Requirement.....5
- 4. Relay Agent Configuration Option.....5
- 5. Operation.....6
 - 5.1. DHCP Relay Agent Procedures.....6
 - 5.1.1. DHCP Relay Agent Chaining.....7
 - 5.2. DHCP Server Procedures.....7
 - 5.3. DHCP Client Procedures.....7
- 6. Security Considerations.....8
- 7. IANA Considerations.....8
- 8. Acknowledgments.....8
- 9. References.....9
 - 9.1. Normative References.....9
 - 9.2. Informative References.....9
- APPENDIX A: Applicability.....10
 - A.1. Applicability to MPLS IP/VPN.....10
- Authors' Addresses.....12

1. Introduction

There are scenarios in which a network operator (Service Provider or Enterprise) may desire the relay agent to be dynamically provisioned while facilitating the server-client communication to ultimately facilitate the service activation in a zero-touch manner.

One example is the provisioning of the Provider Edge (PE) router, acting as the relay agent for the Customer Edge (CE) router, acting as the (DHCP) client, during IP/VPN [RFC4364] service activation.

DHCP [RFC2131][RFC3315] is the predominant signaling protocol to dynamically assign IP addresses and other TCP/IP configuration parameters to routers and hosts. DHCP Relay Agent functionality [RFC3046] is specified to facilitate the forwarding of DHCP messages between the client and server through the relay agent.

DHCP server may use one or more sub-options within the "Relay Agent Information" option [RFC3046] appended by Relay Agent, for IP address and other parameter assignment policies to the Client. The "Relay Agent Information" option [RFC3046] is limited to providing the additional information from Relay Agent to the DHCP server to aid the server.

This document proposes a new DHCP option (and sub-options) that the Relay Agent can use to request and receive the desired Relay Agent configuration information and that the DHCP server can use to deliver the requested configuration information. The document also describes the associated procedures and operations for the Relay Agent and Server to achieve the auto-provisioning of VPN information at the PE router acting as the relay agent.

2. Key Words to Reflect Requirements

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 BCP 14, RFC 2119 [RFC2119]. RFC 2119 defines the use of these key words to help make the intent of standards track documents as clear as possible. While this document uses these keywords, this document is not a standards track document.

Additionally, this document freely uses the terms that are defined in [RFC2131][RFC2132][RFC3046].

3. Problem / Requirement

There are other methods to activate the VPN service by auto-provisioning the CE router after it establishes the layer2 connectivity. However, this assumes and requires the adjacent PE router to be provisioned in advance to ensure that the CE gets the IP reachability through the PE router, and is able to participate in the any-to-any VPN such as BGP IP/VPN [RFC4364]. This is one of the key challenges that serve as one of the requirements for the solution prescribed in this document. Another requirement is to make use of the existing signaling protocol(s) and not impose multiple protocols to achieve this.

4. Relay Agent Configuration Option

This document defines a new DHCP Option called the Relay Agent Configuration Option. It is a "container" option for specific sub-options. The format of the Relay Agent Configuration option is:

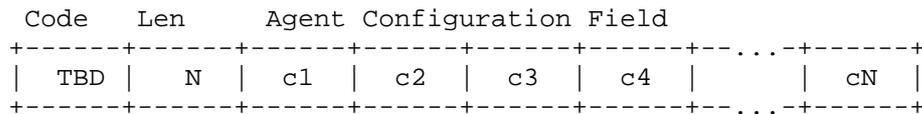


Figure 1 Relay Agent Configuration Option

Code = DHCP Option for Relay Agent Configuration (to be allocated by IANA)

Len = Total number of octets (N) in the Agent Configuration Field (inclusive of all sub-options)

Agent Configuration Field = One or more Sub-options, each encoded as a SubOpt/Length/Value tuple, as shown below:

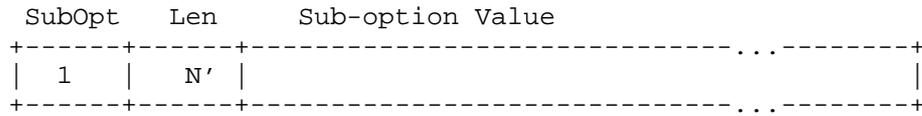


Figure 2 Relay Agent Configuration Sub-Option

SubOpt = DHCP Sub-Option for Relay Agent Configuration (to be allocated by IANA)

Len = Total number of octets (N') in a Sub-option

Sub-option Value = zero or more octets to encode the value.

The sub-options need not appear in any particular order.

5. Operation

5.1. DHCP Relay Agent Procedures

The relay agent adds the DHCP relay agent configuration option (& needed sub-options) in the relayed message to request the relay agent side configuration information from the server.

The addition of this option SHOULD be configurable, and SHOULD be disabled by default. Relay agents SHOULD have separate configurables for each sub-option to control whether it is added to client-to-server packets.

A relay agent adding a Relay Agent Configuration Information Option MUST add it as the last option (but before 'End Option' 255, if present) or the second last option, if option 82 is present, in the DHCP options field of any recognized BOOTP or DHCP packet forwarded from a client to a server.

If the configuration information, provided by the DHCP server in its response, is already present at the relay agent, then relay agent SHOULD compare the existing configuration with the new one, and in case of a mismatch, logs an error/event.

The relay agent MUST remove the relay agent configuration option from the DHCP response and forward the remaining response to the client.

The operation of relay agent for specific sub-options should be specified with that sub-option.

5.1.1. DHCP Relay Agent Chaining

Relay agents receiving a DHCP packet from an untrusted circuit with giaddr set to zero (indicating that they are the first-hop router) but with a Relay Agent Configuration option already present in the packet SHALL discard the packet and increment an error count.

A trusted circuit may contain a trusted downstream (closer to client) network element (bridge) between the relay agent and the client that MAY add a relay agent option but not set the giaddr field. In this case, the relay agent does NOT add a "second" relay agent option, but forwards the DHCP packet per normal DHCP relay agent operations, setting the giaddr field as it deems appropriate.

The mechanisms for distinguishing between "trusted" and "untrusted" circuits are specific to the type of circuit termination equipment, and may involve local administration.

5.2. DHCP Server Procedures

The DHCP server examines the DHCP options in the incoming request, and constructs the response. The DHCP server may poll any other servers present in the OSS/BSS to construct the requested configuration information, and ultimately include it in the relay agent configuration option/sub-options of DHCP response.

5.3. DHCP Client Procedures

This document doesn't specify any changes to the client functioning.

The new option defined in this document is never passed to the client.

6. Security Considerations

There are no specific security considerations within the scope of this document.

7. IANA Considerations

TBD.

8. Acknowledgments

Thanks to Shwetha Bhandari for providing feedback.

This document was prepared using 2-Word-v2.0.template.dot.

9. References

9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2544] Bradner, S. and McQuaid, J., "Benchmarking Methodology for Network Interconnect Devices", RFC 2544, March 1999.
- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.
- [RFC5695] Droms, R. and Alexander and S., "DHCP Options and BOOTP Vendor Extensions", RFC 5695, March 1997.
- [RFC3315] Droms, et. al., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.
- [RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

9.2. Informative References

- [RFC4364] Rosen, E. and Rekther, Y., "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.

APPENDIX A: Applicability

A.1. Applicability to MPLS IP/VPN

Figure 3 below illustrates a sample MPLS/VPN network topology in which CE1, CE2 and CE3 are part of the same Virtual Private Network (VPN), which is represented by VRF VPN1, say, in the MPLS/VPN network.

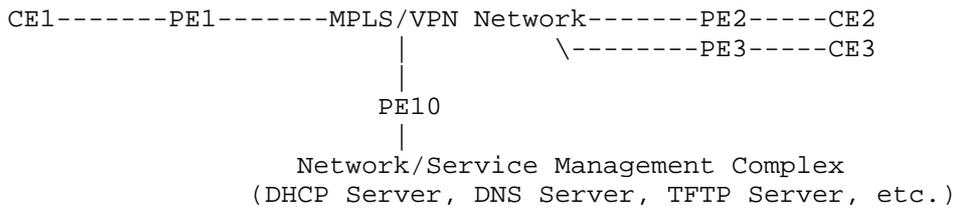


Figure 3 A Sample Network Topology

The "Network/Service Management Complex" is where the DHCP Server, DNS server, TFTP server etc. may reside.

The PE router is assumed to have the DHCP relay agent functionality as suggested in this document. The relay agent functionality may be included globally for all PE-CE interfaces or selectively on individual PE-CE interfaces.

Optionally, the unused PE-CE interfaces at the PE router may be assigned to a default VRF prior to the successful DHCP processing and auto-configuration. This helps to avoid having the CE get the global reachability by accident prior to the DHCP operation completion.

Assuming that the PE-CE interface is ready for the layer1/layer2 connectivity, CE would (be programmed to) broadcast the DHCP request when the layer2 connectivity is established on either all or designated port(s).

- . This ensures that the DHCP request reaches the PE router.
- . The DHCP request may include CE's unique identifier (such as MAC address or S/N or Unique Device Identifier (UDI) etc.) that is already known to the Servers in the Network/Service Management Complex.

PE router upon receiving the DHCP request on a layer2 interface that isn't configured with any IP address, relays it to the DHCP server that may be pre-provisioned.

PE adds the DHCP relay agent configuration option (& needed sub-options) in the relayed message to request the PE side configuration information.

The DHCP server examines the DHCP options in the incoming request, and constructs the response. The DHCP server may poll any other servers present in the OSS/BSS for the PE configuration information, so as to include it in the options/sub-options of DHCP response.

The PE configuration information, in RFC4364 environment, may contain one or more of the following -

- IP address and subnet for PE-CE interface
- VRF Configuration (RD, RT etc.)
- Other PE-CE Interface configuration (description, vrf mapping etc.)
- Selected Routing Protocol instance (for the CE)
- Neighbor and ASN information in case of BGP or EIGRP
- Security, QoS information etc. (for the CE)

If the VRF configuration, provided by the DHCP server in its response, is already present at the PE router, then PE router must compare the existing config with the new one, and logs an error/event that could be sent to the DHCP server or to the OSS/BSS or both, in case of a mismatch.

PE should accept the new config. The error/event log will help to get the operator attention for further validation. New DHCP sub-option is defined for this purpose.

The PE router removes the PE specific information (the new DHCP relay agent configuration option) from the DHCP response and forward the remaining response to the CE router, which will process it as usual (not impacted by this document).

Authors' Addresses

Rajiv Asati
Cisco Systems,
7025 Kit Creek Rd, RTP, NC, 27709
Email: rajiva@cisco.com

Ralph Droms
Cisco Systems,
200 Beaver Brook Road, Boxborough, MA, 01719
Email: rdroms@cisco.com

