                 The DHCPv4 Relay Agent Identifier Sub-Option

Abstract

   This document defines a new Relay Agent Identifier sub-option for the
   Dynamic Host Configuration Protocol (DHCP) Relay Agent Information
   option. The sub-option carries a value that uniquely identifies the
   relay agent device within the administrative domain. The value is
   normally administratively configured in the relay agent. The sub-
   option allows a DHCP relay agent to include the identifier in the
   DHCP messages it sends.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc6925.

Table of Contents

1. Introduction

   The Dynamic Host Configuration Protocol for IPv4 (DHCPv4) [RFC2131]
   provides IP addresses and configuration information for IPv4 clients.
   It includes a relay agent capability, in which network elements
   receive broadcast messages from clients and forward them to DHCP
   servers as unicast messages. In many network environments, relay
   agents add information to the DHCP messages before forwarding them,
   using the Relay Agent Information option [RFC3046]. Servers that
   recognize the Relay Agent Information option echo it back in their
   replies.

   This specification introduces a Relay Agent Identifier (Relay-ID)
   sub-option for the Relay Agent Information option. The Relay-ID sub-
   option carries a sequence of octets that is intended to uniquely
   identify the relay agent within the administrative domain. In this
   document, an administrative domain consists of all DHCP servers and
   relay agents that communicate with each other.

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].

   DHCPv4 terminology is defined in [RFC2131], and the DHCPv4 Relay
   Agent Information option is defined in [RFC3046].

3. Example Use Cases

3.1. Bulk Leasequery

   There has been quite a bit of recent interest in extending the DHCP
   Leasequery protocol [RFC4388] to accommodate some additional
   situations. [RFC6926] proposes a variety of enhancements to the
   existing Leasequery protocol. The document describes a use case
   where a relay agent queries DHCP servers using the relay identifier
   to retrieve all the leases allocated through the relay agent.

3.2. Industrial Ethernet

   DHCP typically identifies clients based on information in their DHCP
   messages, such as the Client-Identifier option or the value of the
   chaddr field. In some networks, however, the location of a client --
   its point of attachment to the network -- is a more useful
   identifier. In factory-floor networks (commonly called 'industrial'
   networks), for example, the role a device plays is often fixed and
   based on its location. Using manual address configuration is
   possible (and is common), but it would be beneficial if DHCP
   configuration could be applied to these networks.

   One way to provide connection-based identifiers for industrial
   networks is to have the network elements acting as DHCP relay agents
   supply information that a DHCP server could use as a client
   identifier. A straightforward way to form identifier information is
   to combine something that is unique within the scope of the network
   element, such as a port/slot value, with something that uniquely
   identifies that network element, such as a Relay Agent Identifier.

4. Sub-Option Format

    Format of the Relay Agent Identifier sub-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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |SUBOPT_RELAY_ID|    length     |                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
    .                                                               .
    .                     identifier (variable)                    .
    .                                                               .
    +---------------------------------------------------------------+
```

    Where:

    SUBOPT_RELAY_ID   12

    length   the number of octets in the sub-option
                       (excluding the sub-option ID and length fields);
                       the minimum length is one.

    identifier   the identifying data

5. Identifier Stability

   If the relay identifier is to be meaningful, it has to be stable. A
   relay agent SHOULD use a single identifier value consistently. The
   identifier used by a relay device SHOULD be committed to stable
   storage, unless the relay device can regenerate the value upon
   reboot.

   If the Relay-ID configured in a relay agent is not unique within its
   administrative domain, resource allocation problems may occur as the
   DHCP server attempts to allocate the same resource to devices behind
   two different relay agents. Therefore, a Relay-ID configured in a
   relay agent MUST be unique within its administrative domain. To aid
   in ensuring uniqueness of Relay-IDs, relay agents SHOULD make their
   relay identifiers visible to their administrators via their user
   interface, through a log entry, through a MIB field, or through some
   other mechanism.

   Implementors of relay agents should note that the identifier needs to
   be present in all DHCP message types where its value is being used by
   the DHCP server. The relay agent may not be able to add the Relay
   Agent Information option to all messages, such as RENEW messages sent
   as IP unicasts. In some deployments, that might mean that the server
   has to be willing to continue to associate the relay identifier it

has last seen with a lease that is being RENEWed. Other deployments
may prefer to use the Server Identifier Override sub-option [RFC5107]
to permit the relay device to insert the Relay Agent Information
option into all relayed messages.

Handling situations where a relay agent device is replaced is another
aspect of stability. One of the use cases for the relay identifier
is to permit a server to associate clients' lease bindings with the
relay device connected to the clients. If the relay device is
replaced because it has failed or been upgraded, it may be desirable
for the new device to continue to provide the same relay identifier
as the old device. Therefore, if a relay agent supports Relay-ID,
the Relay-ID should be administratively configurable.

5.1. Identifier Uniqueness

It is strongly recommended that administrators take special care to
ensure that Relay-IDs configured in their relay agents are not
duplicated. There are a number of strategies that may be used to
achieve this.

Administrators may use a strategy to configure unique Relay-IDs. One
such strategy is that a Relay-ID on a relay agent may reuse an
existing identifier or set of identifiers that are already guaranteed
to be unique (e.g., Universally Unique Identifier (UUID) [RFC4122]).

For administrators who are already using a provisioning system to
manage their networking infrastructure, it may work to enumerate
relay agents on the basis of roles and then, as a second step, assign
those roles to specific relay agents or groups of relay agents. In
such a scenario, when a replacement relay agent is first seen by the
DHCP server, it could trigger a configuration event on the
provisioning system, and the new relay agent could be assigned to the
role of the relay agent it is replacing.

It may be that the DHCP server has configurable event notification
and that a duplicate Relay-ID would trigger this notification.
Administrators can take advantage of this feature to work out whether
the duplication is real and unintended or whether the original relay
agent is being replaced.

A network management/provisioning system may also be able to collect
a full list of all relay agents on the network. It may then notice
that more than one device reports the same Relay-ID. In such a case,
the provisioning system could notify the administrator of the fault,
which could then be corrected.

   This is not an exhaustive list of strategies. We suggest an
   additional strategy in the Security Considerations section. If none
   of these strategies will work, administrators are also encouraged to
   consider the specifics of their own network configuration to see if
   there is some way to detect duplicate Relay-IDs other than the ones
   listed here.

6. Security Considerations

6.1. Forged Relay ID Attacks

   Security issues with the Relay Agent Information option and its use
   by servers in address assignment are discussed in [RFC3046] and
   [RFC4030]. The DHCP Relay Agent Information option depends on a
   trusted relationship between the DHCP relay agent and the DHCP
   server, as described in Section 5 of [RFC3046]. While the
   introduction of fraudulent DHCP Relay Agent Information options can
   be prevented by a perimeter defense that blocks these options unless
   the DHCP relay agent is trusted, a deeper defense using the
   authentication sub-option for the DHCP Relay Agent Information option
   [RFC4030] SHOULD be deployed as well. It also helps in avoiding
   duplication of relay identifiers by malicious entities. However,
   implementation of the authentication sub-option for the DHCP Relay
   Agent Information option [RFC4030] is not a must to support the
   Relay-ID sub-option.

6.2. Factory-Floor Scenario

   One possible use case for the Relay-ID sub-option is the automated
   configuration of machines on a factory floor. In this situation,
   various sections of the factory floor might be on their own network
   links with a relay agent interposed between those links and the DHCP
   server. The Relay-ID of each relay agent might cause special
   configurations to be downloaded to those devices to control their
   behavior.

   If a relay agent was deployed on the factory floor in such a
   situation, with an incorrect Relay-ID, there is the potential that
   devices could be misconfigured in a way that could produce incorrect
   results, cause physical damage, or even create hazardous conditions
   for workers.

   In deployment scenarios like this one, administrators must use some
   dependable technique to ensure that such misconfigurations do not
   occur. It is beyond the scope of this document to provide a complete
   list of such techniques.

   However, as an example, a relay agent device intended for use in such
   a scenario could require the use of a hardware token that contains a
   Relay-ID that is physically attached to the installation location of
   the relay agent device and can be connected to and disconnected from
   the relay agent device without the use of special tools. Such a
   relay agent device should not be operable when this hardware token is
   not connected to it: either it should fail because it presents an
   unknown identifier to the DHCP server, or it should simply refuse to
   relay DHCP packets until the token is connected to it.

   A relay agent device that does not provide a clear mitigation
   strategy for a scenario where misconfiguration could have damaging or
   hazardous consequences should not be deployed in such a scenario.

7. IANA Considerations

   IANA has assigned a new sub-option code from the "DHCP Relay Agent
   Sub-Option Codes" registry maintained at
   http://www.iana.org/assignments/bootp-dhcp-parameters.

      Relay Agent Identifier Sub-Option 12

8. Acknowledgments

   Thanks to Bernie Volz, David W. Hankins, Pavan Kurapati, and Ted
   Lemon for providing valuable suggestions.

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.

   [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC
              2131, March 1997.

   [RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC
              3046, January 2001.

   [RFC4030] Stapp, M. and T. Lemon, "The Authentication Suboption for
              the Dynamic Host Configuration Protocol (DHCP) Relay Agent
              Option", RFC 4030, March 2005.

9.2. Informative References

   [RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally
              Unique IDentifier (UUID) URN Namespace", RFC 4122, July
              2005.

   [RFC4388] Woundy, R. and K. Kinnear, "Dynamic Host Configuration
              Protocol (DHCP) Leasequery", RFC 4388, February 2006.

   [RFC5107] Johnson, R., Kumarasamy, J., Kinnear, K., and M. Stapp,
              "DHCP Server Identifier Override Suboption", RFC 5107,
              February 2008.

   [RFC6926] Kinnear, K., Stapp, M., Desetti, R., Joshi, B., Russell,
              N., Kurapati, P., and B. Volz, "DHCPv4 Bulk Leasequery",
              RFC 6926, April 2013.

Authors' Addresses

   Bharat Joshi
   Infosys Ltd.
   44 Electronics City, Hosur Road
   Bangalore 560 100
   India

   EMail: bharat_joshi@infosys.com
   URI: http://www.infosys.com/

   D.T.V Ramakrishna Rao
   Infosys Ltd.
   44 Electronics City, Hosur Road
   Bangalore 560 100
   India

   EMail: ramakrishnadtv@infosys.com
   URI: http://www.infosys.com/

   Mark Stapp
   Cisco Systems, Inc.
   1414 Massachusetts Ave.
   Boxborough, MA 01719
   USA

   Phone: +1 978 936 0000
   EMail: mjs@cisco.com