IPv6 CONSORTIUM TEST SUITE

Dynamic Host Configuration Protocol for IPv6

Operations Test Suite

Technical Document

Revision 2.1

University of New Hampshire
InterOperability Laboratory
IPv6 Consortium
http://www.iol.unh.edu

121 Technology Drive, Suite 2
Durham, NH 03824
Phone: +1-603-862-2804
Fax: +1-603-862-0898

Modification Record

June 13, 2005	Version 1.0 • Initial Version
August 15, 2005	Version 2.0 • Changed wording, typos, added needed steps
September 19, 2005	Version 2.1 • Added tests DHCP_CONF.3.2 Part j,k • Fixed typos

ACKNOWLEDGMENTS

The University of New Hampshire would like to acknowledge the efforts of the following individuals in the development of this test suite.

Milen Andonov	University of New Hampshire
Timothy Carlin	University of New Hampshire
Erica Williamsen	University of New Hampshire
Timothy Winters	University of New Hampshire

INTRODUCTION

Overview

Dynamic Host Configuration Protocol (DHCP) for IPv6 is designed to allocate addresses to hosts. In IPv6, there are two alternatives for hosts to acquire their addresses. Stateless auto-configuration can be done through obtaining a prefix from a local router. Stateful auto-configuration can be done through a query to a DHCP server to obtain the IPv6 address. In both cases, DHCP is the best way to obtain Domain name information and DNS information.

The University of New Hampshire's InterOperability Laboratory (IOL) is an institution designed to improve the interoperability of standards based products by providing an environment where a product can be tested against other implementations of a standard. This suite of tests has been developed to help implementers evaluate the functioning of their products supporting DHCP for IPv6. This test suite has been designed to test the interoperability of the device under test with other DHCP for IPv6 capable devices. This test suite focuses on testing configurations of the network that could cause problems when deployed if the device under test does not operate properly with the devices that it is connected to.

The tests do not determine if a product conforms to the DHCP for IPv6 standards but they are designed as interoperability tests. These tests provide one method to isolate problems within the DHCP for IPv6 capable device that will affect the interoperability performance. Successful completion of all tests contained in this suite does not guarantee that the tested device will operate with other DHCP for IPv6 capable devices. However, these tests do provide a reasonable level of confidence that the NUT will function well in many DHCP for IPv6 capable environments.

Acronyms

TN: Testing Node
TR: Testing Router
NUT: Node Under Test
DHCP: Dynamic Host Configuration Protocol
IA: Identity Association
ID: Identifier
DUID: DHCP Unique Identifier

When several entities of the same type are present in a test configuration, a number is appended to the acronym to yield a label for each entity. For example, if there were three testing routers in the test configuration, they would be labeled TR1, TR2 and TR3.

TEST ORGANIZATION

This document organizes tests by group based on related test methodology or goals. Each group begins with a brief set of comments pertaining to all tests within that group. This is followed by a series of description blocks; each block describes a single test. The format of the description block is as follows:

Test Label: The Test Label and Title comprise the first line of the test block. The Test Label is composed of the short test suite name, the group number, and the test number within the group, separated by periods. So, test label DHCP_CONF.1.2 refers to the second test of the first test group in the DHCP Operations Test Suite.

Purpose: The Purpose is a short statement describing what the test attempts to achieve. It is usually phrased as a simple assertion of the feature or capability to be tested.

References: The References section lists cross-references to the specifications and documentation that might be helpful in understanding and evaluating the test and results.

Discussion: The Discussion is a general discussion of the test and relevant section of the specification, including any assumptions made in the design or implementation of the test as well as known limitations.

Test Setup: The Test Setup section describes the configuration of all devices prior to the start of the test. Different parts of the procedure may involve configuration steps that deviate from what is given in the test setup. If a value is not provided for a protocol parameter, then the protocol's default is used.

Procedure: This section of the test description contains the step-by-step instructions for carrying out the test. These steps include such things as enabling interfaces, unplugging devices from the network, or sending packets from a test station. The test procedure also cues the tester to make observations, which are interpreted in accordance with the observable results given for that test part.

Observable Results: This section lists observable results that can be examined by the tester to verify that the NUT is operating properly. When multiple observable results are possible, this section provides a short discussion on how to interpret them. The determination of a pass or fail for each test is usually based on how the NUT's behavior compares to the results described in this section.

Possible Problems: This section contains a description of known issues with the test procedure, which may affect test results in certain situations.

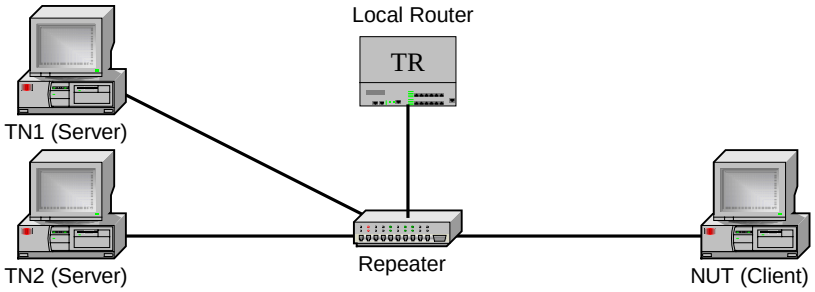
REFERENCES

The following documents are referenced in this text:

- Request for Comments 3315 – Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Droms, R, Ed., Cisco Systems. July, 2003.
- Request for Comments 3646 – DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Droms, R, Ed., Cisco Systems. December, 2003
- Request for Comments 3736 – Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6. Droms, R, Cisco Systems. April, 2004.

TABLE OF CONTENTS

Common Topology



Link A

The common topology involves a client and server device(s) on the same link with one default router. For clarity, there is one global IPv6 address for this link. Some of the tests in this suite will specify the client get a prefix from the TR, other tests will specify the client get a prefix from the server.

The current revision of this test suite is focused on the client device as the NUT and the server device as the TN. Future revisions of this test suite may include server-based DHCP tests, and tests on which the clients and servers are not on the same IPv6 link.

Common Test Setup

Tests in this test suite may refer to a common test setup procedure defined for this section.

Common Test Setup 1.1

Summary: This minimal setup procedure describes a proper Solicit - Advertise - Request - Reply exchange between the NUT and TN1.

1. If the NUT is a client:
   Enable DHCPv6 on the NUT (client). The NUT transmits a Solicit message to the All_DHCP_Relay_Agents_and_Servers address (FF02::1:2). TN1 responds with an Advertise message. The NUT then sends a Request message to TN1 asking for confirmed assignment of addresses and other configuration information. TN1 responds with a Reply message that contains the confirmed addresses and configuration. The Reply message contains an IA_NA option with T1 set to 200 seconds and T2 set to 300 seconds.

Section 1: RFC 3315: Client Specification

Scope

The following tests cover specifications for the client implementation of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Request For Comments 3315.
The scope of the tests includes major functionality groups such as client behavior in client-initiated configuration exchange, client behavior in server-initiated configuration exchange, client behavior in server solicitation, and message validation by client. The section does not offer an exhaustive set of tests, but rather provides test cases to verify the operation of DHCPv6 clients' functionality most commonly implemented in practice.
The section is structured mainly with regard to the above functionality groups. The organization of this section however will tend to depart from the organization of RFC 3315 when grouping based on considerations of test setup and procedure is applied.

Overview

These tests are designed to verify the readiness of a DHCPv6 client implementation vis-à-vis the base specifications of the Dynamic Host Configuration Protocol for IPv6.

Group 1: Client Constants and Message Validation by Client

Scope

The following tests focus on the client's implementation of DHCPv6 constants and the reception of invalid DHCPv6 messages by a server device.

Test DHCP_CONF.1.1: Implementation of DHCP constants

Purpose: To verify that the client transmits messages to the correct DHCP constant address.

References:

- [DHCP 3315] – Section 5.1, 5.2 and 13

Discussion: All_DHCP_Relay_Agents_and_Servers (FF02::1:2) is a link-scoped multicast address used by a client to communicate with neighboring (i.e., on-link) relay agents and servers. All servers and relay agents are members of this multicast group.

A client sends DHCP messages to the ALL_DHCP_Relay_Agents_and_Servers address. A client uses multicast to reach all servers or an individual server. A client may send some messages directly to a server using unicast, if it has received a server unicast option from the server.

Clients listen for DHCP messages on UDP port 546.

Test Setup: Connect the network as described in the Common Topology. Disable router prefix delegation. DHCPv6 is enabled on the client device before each part. DHCPv6 is disabled on the client device after each part.

Procedure:

Part A: Multicast Addresses

1. Enable DHCPv6 on the NUT.
2. Observe the messages transmitted on link.

Part B: UDP ports

3. Enable DHCPv6 on the NUT.
4. Upon reception of a Solicit message from the NUT, TN1 transmits an Advertise message to UDP port 33536.
5. Observe the messages transmitted on link.

Observable Results:

- *Part A*

  Step 2: The NUT should transmit a Solicit message. The destination address of the Solicit message should be FF02::1:2.
- *Part B*

  Step 5: The NUT should send a Destination Unreachable message to TN1 link-local address. The source address of the packet must be the NUT's unicast address. The code field must be set to "4" and the invoking advertise packet included in the Error Message must not exceed minimum IPv6 MTU.

Possible Problems:

- None.

Test DHCP_CONF.1.2: Client Message Validation

Purpose: To verify a client device properly discards all Solicit, Request, Confirm, Renew, Rebind, Decline, Release, Information-request, Relay-forward and Relay-reply messages.

References:

- [DHCP 3315] – Sections 15.2, 15.4, 15.5, 15.6, 15.7, 15.8, 15.9, 15.12, 15.13 and 15.14

Discussion: A client must discard the following messages: Solicit, Request, Confirm, Renew, Rebind, Decline, Release, Information-request, Relay-forward and Relay-reply.

Test Setup: Connect the network as described in the Common Topology. Disable router prefix delegation. Common Test Setup 1.1 is performed before each part. Disable DHCPv6 on the client device after each part.

Procedure:

Part A: Solicit message (type 1)

1. The NUT should receive IPv6 address information from TN1.
2. TN1 transmits a Solicit message to the NUT.
3. Observe the messages transmitted on link.

Part B: Request message (type 3)

4. The NUT should receive IPv6 address information from TN1.
5. TN1 transmits a Request message to the NUT.
6. Observe the messages transmitted on link.

Part C: Confirm message (type 4)

7. The NUT should receive IPv6 address information from TN1.
8. TN1 transmits a Confirm message to the NUT.
9. Observe the messages transmitted on link.

Part D: Renew message (type 5)

10. The NUT should receive IPv6 address information from TN1.
11. TN1 transmits a Renew message to the NUT.
12. Observe the messages transmitted on link.

Part E: Rebind message (type 6)

13. The NUT should receive IPv6 address information from TN1.
14. TN1 transmits a Rebind message to the NUT.
15. Observe the messages transmitted on link.

Part F: Decline message (type 9)

16. The NUT should receive IPv6 address information from TN1.
17. TN1 transmits a Decline message to the NUT.
18. Observe the messages transmitted on link.

Part G: Release message (type 8)

19. The NUT should receive IPv6 address information from TN1.
20. TN1 transmits a Release message to the NUT.
21. Observe the messages transmitted on link.

Part H: Information-request message (type 11)

22. The NUT should receive IPv6 address information from TN1.
23. TN1 transmits an Information-request message to the NUT.
24. Observe the messages transmitted on link.

Part I: Relay-forward message (type 12)

25. The NUT should receive IPv6 address information from TN1.
26. TN1 transmits a Relay-forward message to the NUT.
27. Observe the messages transmitted on link.

Part J: Relay-reply message (type 13)

28. The NUT should receive IPv6 address information from TN1.
29. TN1 transmits a Relay-reply message to the NUT.
30. Observe the messages transmitted on link.

Observable Results:

- *Part A*
  Step 3: The NUT discards the Solicit message from TN1 and does not transmit any packets.
- *Part B*
  Step 6: The NUT discards the Request message from TN1 and does not transmit any packets.
- *Part C*
  Step 9: The NUT discards the Confirm message from TN1 and does not transmit any packets.
- *Part D*
  Step 12: The NUT discards the Renew message from TN1 and does not transmit any packets.
- *Part E*
  Step 15: The NUT discards the Rebind message from TN1 and does not transmit any packets.
- *Part F*
  Step 18: The NUT discards the Decline message from TN1 and does not transmit any packets.
- *Part G*
  Step 21: The NUT discards the Release message from TN1 and does not transmit any packets.
- *Part H*
  Step 24: The NUT discards the Information-request message from TN1 and does not transmit any packets.
- *Part I*
  Step 27: The NUT discards the Relay-forward message from TN1 and does not transmit any packets.
- *Part J*
  Step 30: The NUT discards the Relay-reply messages from TN1 and does not transmit any packets.

Possible Problems:

- None.

Test DHCP_CONF.1.3: Reception of Invalid Advertise message

Purpose: To verify a client device properly handles the reception of invalid Advertise messages.

References:

- [DHCP 3315] – Sections 15.3 and 17.1.3

Discussion: Clients MUST discard any received Advertise messages that meet any of the following conditions:

- the message does not include a Server Identifier option.
- the message does not include a Client Identifier option.
- the contents of the Client Identifier option does not match the client's DUID.
- the "transaction-id" field value does not match the value the client used in its Solicit message.

The client MUST ignore any Advertise message that includes a Status Code option containing the value NoAddrsAvail, with the exception that the client MAY display the associated status message to the user.

Test Setup: Connect the network as described in the Common Topology. Disable router prefix delegation. Enable DHCPv6 on the client device before each part. Disable DHCPv6 on the client device after each part.

Procedure:

Part A: No Server Identifier option

1. When a Solicit message is received from the NUT, TN1 transmits an Advertise message that does not contain a Server Identifier option.
2. Observe the messages transmitted on link.

Part B: No Client Identifier option

3. When a Solicit message is received from the NUT, TN1 transmits an Advertise message that does not contain a Client Identifier option.
4. Observe the messages transmitted on link.

Part C: Client Identifier that does not match the DUID of the client

5. When a Solicit message is received from the NUT, TN1 transmits a properly formatted Advertise message. The Advertise message contains a Client Identifier option whose value does not match the client's DUID.
6. Observe the messages transmitted on link.

Part D: Transaction ID Mismatch

7. When a Solicit message is received from the NUT, TN1 transmits a properly formatted Advertise message. The Advertise message contains a transaction-id field value that does not match the value the client used in its Solicit message.
8. Observe the messages transmitted on link.

Part E: Status Code option containing NoAddrsAvail

9. When a Solicit message is received from the NUT, TN1 transmits a properly formatted Advertise message. The Advertise message contains a Status Code option containing the value NoAddrsAvail (code 2).
10. Observe the Solicit messages transmitted on link.

Observable Results:

- *Part A*

Step 2: The NUT must silently discard the Advertise message. The NUT must not send a Request message based on the received Advertise message.

- *Part B*
  Step 4: The NUT must silently discard the Advertise message. The NUT must not send a Request message based on the received Advertise message.
- *Part C*
  Step 6: The NUT must silently discard the Advertise message. The NUT must not send a Request message based on the received Advertise message.
- *Part D*
  Step 8: The NUT must silently discard the Advertise message. The NUT must not send a Request message based on the received Advertise message.
- *Part E*
  Step 10: The NUT must silently discard the Advertise message. The NUT may display the associated status message to the user.

Possible Problems:

- None.

Test DHCP_CONF.1.4: Reception of Invalid Reply message

Purpose: To verify that a client device properly handles the reception of invalid Reply messages.

References:

- [DHCP 3315] – Section 15.10

Discussion: Clients MUST discard any received Reply message that meets any of the following conditions:

- the message does not include a Server Identifier option.
- the "transaction-id" field in the message does not match the value used in the original message.

If the client included a Client Identifier option in the original message, the Reply message must include a Client Identifier option and the DUID contents of the Client Identifier must match the DUID of the client OR, if the client did not include a Client Identifier option in the original message, the Reply message must not include a Client Identifier option.

Test Setup: Connect the network as described in the Common Topology. Disable router prefix delegation. Enable DHCPv6 on the client device before each part. Disable DHCPv6 on the client device after each part.

Procedure:

Part A: No Server Identifier option

1. Upon the reception of a Solicit message from the NUT, TN1 transmits a valid Advertise message.
2. Upon the reception of a Request message, TN1 transmits a Reply message that does not contain a Server Identifier option.
3. Observe the messages transmitted on link.

Part B: Transaction ID Mismatch

4. Upon the reception of a Solicit message from the NUT, TN1 transmits a valid Advertise message.
5. Upon the reception of a Request message, TN1 transmits a Reply message. The Reply message contains a transaction-id field value that does not match the value the client used in its Solicit and Request messages.
6. Observe the messages transmitted on link.

Part C: No Client Identifier option (optional, client included Client ID option in original message)

7. Upon the reception of a Solicit message from the NUT, TN1 transmits a valid Advertise message.
8. Upon the reception of a Request message, TN1 transmits a Reply message that does not contain a Client Identifier option.
9. Observe the messages transmitted on link.

Part D: Client DUID Mismatch (optional, client included Client ID option in original message)

10. Upon the reception of a Solicit message from the NUT, TN1 transmits a valid Advertise message.
11. Upon the reception of a Request message, TN1 transmits a Reply message that contains a Client Identifier option with a DUID value that does not match the DUID value in the received Request message.
12. Observe the messages transmitted on link.

Part E: Client Identifier option (optional, client does NOT include Client ID option in original message)

13. Upon the reception of a Solicit message from the NUT, TN1 transmits a valid Advertise message.
14. Upon the reception of a Request message, TN1 transmits a Reply message that contains a Client Identifier option.
15. Observe the messages transmitted on link.

Observable Results:

- *Part A*
  Step 3: The NUT must silently discard the invalid Reply message. The NUT does not assign these addresses.
- *Part B*
  Step 6: The NUT must silently discard the invalid Reply message. The NUT does not assign these addresses.
- *Part C*
  Step 9: The NUT must silently discard the invalid Reply message. The NUT does not assign these addresses.
- *Part D*
  Step 12: The NUT must silently discard the invalid Reply message. The NUT does not assign these addresses.
- *Part E*
  Step 15: The NUT must silently discard the invalid Reply message. The NUT does not assign these addresses.

Possible Problems:

- Part C and D may be omitted if the client does not include a Client Identifier option in its original message.
- Part E may be omitted if the client includes a Client Identifier option in its original message.

Test DHCP_CONF.1.5: Reception of Invalid Reconfigure message (This test is currently unavailable)

Purpose: To verify a client device properly discards invalid Reconfigure messages.

References:

- [DHCP 3315] – Section 15.11

Discussion: Clients MUST discard any Reconfigure messages that meet any of the following conditions:

- the message was not unicast to the client.
- the message does not include a Server Identifier option.
- the message does not include a Client Identifier option that contains the client's DUID.
- the message does not contain a Reconfigure Message option and the msg-type must be a valid value.
- the message includes any IA options and the msg-type in the Reconfigure Message option is INFORMATION-REQUEST.
- the message does not include DHCP authentication:
  * the message does not contain an authentication option.
  * the message does not pass the authentication validation performed by the client.

Test Setup: Connect the network as described in the Common Topology. Disable router prefix delegation. Common Test Setup 1.1 is performed before each part. DHCPv6 is disabled on the client device after each part.

Procedure:

Part A: Message is Not unicast to the client

1. The NUT should have received IPv6 address information from TN1.
2. TN1 transmits a properly formatted Reconfigure message. The destination address of the reconfigure message is the NUT's solicited-node multicast address.
3. Observe the messages transmitted on link.

Part B: No Server Identifier option

4. The NUT should have received IPv6 address information from TN1.
5. TN1 transmits a Reconfigure message that does not contain a Server Identifier option.
6. Observe the messages transmitted on link.

Part C: No Client Identifier option

7. The NUT should have received IPv6 address information from TN1.
8. TN1 transmits a Reconfigure message that does not contain a Client Identifier option.
9. Observe the messages transmitted on link.

Part D: No Reconfigure option

10. The NUT should have received IPv6 address information from TN1.
11. TN1 transmits a Reconfigure message that does not contain a Reconfigure Message option.
12. Observe the messages transmitted on link.

Part E: Invalid msg-type value in Reconfigure option

13. The NUT should have received IPv6 address information from TN1.
14. TN1 transmits a Reconfigure message that contains a Reconfigure Message option with a msg-type value of 0.
15. Observe the messages transmitted on link.
16. Repeat Steps 13 through 15 transmitting a Reconfigure message that contains a Reconfigure Message option with a msg-type value of 14.

Part F: IA option included; msg-type is INFORMATION-REQUEST

17. The NUT should have received IPv6 address information from TN1.
18. TN1 transmits a Reconfigure message that contains an IA for IA_NA option. The Reconfigure message also contains Reconfigure Message option with a msg-type value of 11 (INFORMATION-REQUEST).
19. Observe the messages transmitted on link.

Part G: No authentication option

20. The NUT should have received IPv6 address information from TN1.
21. TN1 transmits a Reconfigure message that does not contain an Authentication option.
22. Observe the messages transmitted on link.

Observable Results:

- *Part A*
  Step 3: The NUT must silently discard the invalid Reconfigure message. The client must not respond with a Renew message or an Information-request message.
- *Part B*
  Step 6: The NUT must silently discard the invalid Reconfigure message. The client must not respond with a Renew message or an Information-request message.
- *Part C*
  Step 9: The NUT must silently discard the invalid Reconfigure message. The client must not respond with a Renew message or an Information-request message.
- *Part D*
  Step 12: The NUT must silently discard the invalid Reconfigure message. The client must not respond with a Renew message or an Information-request message.
- *Part E*
  Step 15: The NUT must silently discard the invalid Reconfigure message. The client must not respond with a Renew message or an Information-request message.
- *Part F*
  Step 19: The NUT must silently discard the invalid Reconfigure message. The client must not respond with a Renew message or an Information-request message.
- *Part G*
  Step 22: The NUT must silently discard the invalid Reconfigure message. The client must not respond with a Renew message or an Information-request message.

Possible Problems:

- None.

Group 2: Client Message Creation, Transmission and Termination

Scope

The following tests focus on the DHCP for IPv6 exchange. The messages that are sent by the client will locate servers that will assign the IPv6 addresses and/or additional configuration information pertaining to client IAs. Tests in this section are focused on client devices.

Test DHCP_CONF.2.1: Creation and Transmission of Solicit Messages

Purpose: To verify a client device transmits properly formatted Solicit messages and properly follows the retransmission algorithm for Solicit messages.

References:

- [DHCP 3315] – Sections 5.5, 14, 16, 17.1, 17.1.1 and 17.1.2

Discussion: A client uses the Solicit message to discover DHCP servers configured to assign addresses or return other configuration parameters on the link to which the client is attached.

The client sets the "msg-type" field to SOLICIT. The client generates a transaction ID and inserts this value in the "transaction-id" field.

The client uses a link-local address or addresses determined through other mechanisms for transmitting and receiving DHCP messages.

The client MUST include a Client Identifier option to identify itself to the server. The client includes IA options for any IAs to which it wants the server to assign addresses. The client MUST NOT include any other options in the Solicit message, except as specifically allowed in the definition of individual options.

The first Solicit message from the client on the interface MUST be delayed by a random amount of time between 0 and SOL_MAX_DELAY (1 sec).

RAND is a random number chosen with a uniform distribution between +0.1 and –0.1. The randomization factor is included to minimize synchronization of messages transmitted by DHCP clients.
RT for the first message transmission is based on IRT: RT = IRT + RAND*IRT

RT for each subsequent message transmission is based on the previous value of RT:
RT = 2*RTprev + RAND*RTprev

Test Setup: Connect the network according to the Common Topology. Disable router prefix delegation. DHCPv6 is enabled on the client device before each part. DHCPv6 on the client device is disabled after each part.

Procedure:

Part A: Solicit message Format

1. Enable DHCPv6 on the NUT.
2. Observe the first Solicit message transmitted on the link.

Part B: Retransmissions

3. Enable DHCPv6 on the NUT.
4. Observe three Solicit messages transmitted on the link.

Observable Results:

- *Part A*

  Step 2: The NUT transmits a properly formatted Solicit message between 0 and SOL_MAX_DELAY (1 sec) containing the following elements:

- Src Address is a link-local for that interface
- The msg-type field was set to the value of 1 (Solicit)
- A header containing a Transaction ID
- A Client Identifier Option (containing a DUID)

- *Part B*

  Step 4: The NUT should properly transmit Solicit messages according to the chart below. The transaction ID is the same for all retransmitted messages.

Solicit Message	Minimum Delay	Maximum Delay
First message	0 seconds	SOL_MAX_DELAY(1 sec)
Second message	0.9 seconds = IRT + RAND*IRT Where IRT=1, RAND=-.1	1.1 seconds = IRT + RAND*IRT Where IRT=1, RAND= +.1
Third message	1.7 seconds = (2*RTprev +Rand*RTprev) where RTprev=.9	2.3 seconds = (2*RTprev +Rand*RTprev) where RTprev=1.1
Fourth message	3.2 seconds = (2*RTprev +Rand*RTprev) where RTprev=.9	4.8 seconds = (2*RTprev +Rand*RTprev) where RTprev=1.1

Possible Problems:

- None.

Test DHCP_CONF.2.2: Message Exchange Termination for Solicit messages

Purpose: To verify that a DHCPv6 client device properly implements the mechanism for message exchange termination for Solicit messages.

References:

- [DHCP 3315] – Sections 14 and 17.1.2

Discussion:
The client transmits the message according to section 14, using the following parameters:

IRT SOL_TIMEOUT
MRT SOL_MAX_RT
MRC 0
MRD 0

If the client is waiting for an Advertise message [...], the client collects Advertise messages until the first RT has elapsed. […] A client MUST collect Advertise messages for the first RT seconds, unless it receives an Advertise message with a preference value of 255. Any Advertise that does not include a Preference option is considered to have a preference value of 0.

If the client receives an Advertise message that includes a Preference option with a preference value of 255, the client immediately begins a client-initiated message exchange by sending a Request message to the server from which the Advertise message was received.

If the client receives an Advertise message that does not include a Preference option with a preference value of 255, the client continues to wait until the first RT elapses. If the first RT elapses and the client has received an Advertise message, the client SHOULD continue with a client-initiated message exchange by sending a Request message.

If the client does not receive any Advertise messages before the first RT has elapsed, it begins the retransmission mechanism described in section 14. The client terminates the retransmission process as soon as it receives any Advertise message, and the client acts on the received Advertise message without waiting for any additional Advertise messages.

Test Setup: Connect the network according to the Common Topology. Disable router prefix delegation. DHCPv6 is enabled on the client device before each part. DHCPv6 on the NUT is disabled after each part.

Procedure:

Part A: No response from Server

1. Enable DHCPv6 on the NUT.
2. Observe at least eight Solicit messages from the NUT.

Part B: Receives Advertise message with Preference Option before first RT elapse

3. Enable DHCPv6 on the NUT
4. Wait until the NUT transmits a Solicit message.
5. TN1 immediately transmits an Advertise message that includes a Preference Option set to 255.
6. Observe the messages transmitted on the link.

Part C: Receives Advertise message without Preference Option before first RT elapse

7. Enable DHCPv6 on the NUT

8. Wait until the NUT transmits a Solicit message.
9. TN1 immediately transmits an Advertise message that does not include a Preference Option.
10. Observe the messages transmitted on the link.

Part D: Receives Advertise message without Preference Option after first RT elapse

11. Enable DHCPv6 on the NUT
12. Wait until the NUT transmits a second Solicit message.
13. TN1 transmits an Advertise message that does not include a Preference Option.
14. Observe the messages transmitted on the link.

Observable Results:

- *Part A*
  Step 2: The NUT must not cease transmission of Solicit messages. The observed RT for any retransmitted Solicit messages should be within the range RT = 2*RTprev + RAND*RTprev, but never greater than SOL_MAX_RT + RAND*SOL_MAX_RT (132 seconds).
- *Part B*
  Step 6: The NUT must transmit a Request message immediately after receiving the Advertise message from the Server.
- *Part C*
  Step 10: The NUT must wait IRT + RAND*IRT (between 0.9 and 1.1) seconds before transmitting a Request message. The NUT must not transmit a Request message immediately after receiving the Advertise message from the Server.
- *Part D*
  Step 14: The NUT must transmit a Request message immediately after receiving the Advertise message from the Server.

Possible Problems:

- If the NUT is configured with either MRC or MRD set to a value other than 0, the NUT will terminate the message exchange according to section 14 of RFC 3315; therefore the above test cases would not apply.

Test DHCP_CONF.2.3: Creation and Transmission of Request messages

Purpose: To verify that a client device transmits properly formatted Request messages and properly implements the mechanism for message exchange termination for Request messages.

References:

- [DHCP 3315] – Sections 5.5, 14 and 18.1.1

Discussion: The client uses the Request messages to populate its Identity Associations (IAs) with addressees and obtain additional configuration information.

The client generates a transaction ID and inserts this value in the "transaction-id" field.

The client places the identifier of the destination server in a Server Identifier option.

The client MUST include a Client Identifier option to identify itself to the server. The client adds any other appropriate options, including one or more IA options.

The client MUST include an Option Request option to indicate the options the client is interested in receiving.

The client includes a Reconfigure Accept option indicating whether or not the client is willing to accept Reconfigure messages from the server.

The client transmits the message according to section 14, using the following parameters:
IRT REQ_TIMEOUT
MRT REQ_MAX_RT
MRC REQ_MAX_RC
MRD 0

Test Setup: Connect all devices according to the Common Topology. Enable DHCPv6 on the client device before each part. DHCPv6 is disabled on the client device after each part.

Procedure:

Part A: Request message format.

1. Upon the reception of a Solicit message from the NUT, TN1 transmits a properly formatted Advertise message.
2. Observe the messages transmitted on the link.

Part B: Retransmission and message exchange termination.

3. Upon the reception of a Solicit message from the NUT, TN1 transmits a properly formatted Advertise message.
4. Observe the messages transmitted on the link.

Observable Results:

- *Part A*

  Step 2: The NUT transmits a properly formatted Request message to TN1 containing:
  - The msg-type field was set to the value of 3 (Request)
  - A header containing a Transaction ID

- A Client Identifier Option (containing a DUID)
- A Server Identifier Option (if unicast is not used)
- An Option Request Option (optional)
- An IA Address Option with the proper IPv6 address associated with the IA

- *Part B*

  Step 4: The NUT must terminate the message exchange after the transmission of REQ_MAX_RC (10) Request messages. The observed RT for any retransmitted Request messages should be within the range RT = 2*RTprev + RAND*Rtprev, but never greater than REQ_MAX_RT + RAND*REQ_MAX_RT (33 seconds).

Possible Problems:

- None.

Test DHCP_CONF.2.4: Creation and Transmission of Confirm messages

Purpose: To verify a client device transmits properly formatted Confirm messages and properly implements the mechanism for message exchange termination for Confirm messages.

References: [DHCP 3315] – Sections 5.5, 14 and 18.1.2

Discussion: In any situation when a client may have moved to a new link, the client MUST initiate a Confirm/Reply message exchange. The client includes any IAs […] assigned to the interface that may have moved to a new link, along with the addresses associated with those IAs[…].

The client sets the "msg-type" field to CONFIRM. The client generates a transaction ID and inserts this value in the "transaction-id" field.

The client MUST include a client Identifier option to identify itself to the server. The client includes IA options for all of the IAs assigned to the interface for which the Confirm message is being sent. The client should set the T1 and T2 fields in any IA_NA options, and the preferred-lifetime and valid-lifetime fields in the IA Address options to 0, as the server will ignore these fields.

The first Confirm message from the client on the interface MUST be delayed by a random amount of time between 0 and CNF_MAX_DELAY.The client transmits the message according to section 14, using the following parameters:

IRT	CNF_TIMEOUT
MRT	CNF_MAX_RT
MRC	0
MRD	CNF_MAX_RD

Test Setup: Connect the network according to the Common Topology. Common Test Setup 1.1 is performed before each part. DHCPv6 is disabled on the client device after each part.

Procedure:

Part A: Confirm message format.

1. The NUT should have received IPv6 address information from TN1.
2. Physically disconnect the NUT interface on Link A.
3. After enough time elapses in which the NUT recognizes a link down situation (5 seconds), reconnect the NUT to Link A.
4. Observe the messages transmitted on the link.

Part B: Retransmission and message exchange termination.

5. The NUT should have received IPv6 address information from TN1.
6. Physically disconnect the NUT interface on Link A.
7. After enough time elapses in which the NUT recognizes a link down situation (5 seconds), reconnect the NUT to Link A.
8. Observe the messages transmitted on the link.

Observable Results:

- *Part A*

Step 4: The NUT transmits a properly formatted Confirm message between 0 and CNF_MAX_DELAY (1 second) to TN1 containing:

- The "msg-type" field was set to the value of 4 (Confirm)
- A header containing a Transaction ID
- A Client Identifier Option (containing a DUID)
- An IA Address Option with the proper IPv6 address associated with the IA

- *Part B*

  Step 8: The NUT must cease the transmission of Confirm messages after CNF_MAX_RD (10 seconds). The observed RT for any retransmitted Confirm messages should be within the range RT = 2*RTprev + RAND*RTprev, but never greater than CNF_MAX_RT + RAND*CNF_MAX_RT (4.4 seconds).

Possible Problems:

- None.

Test DHCP_CONF.2.5: Creation and Transmission of Renew messages

Purpose: To verify a client device properly transmits Renew messages.

References:

- [DHCP 3315] – Sections 5.5, 14 and 18.1.3

Discussion: To extend the valid and preferred lifetimes for the addresses associated with an IA, the client sends a Renew message to the server from which the client obtained the addresses in the IA containing an IA option for the IA. The client includes IA Address options in the IA option for the addresses associated with the IA.

At time T1 for an IA, the client initiates a Renew/Reply message exchange to extend the lifetimes on any addresses in the IA. The client includes an IA option with all addresses currently assigned to the IA in its Renew message.

The client sets the "msg-type" field to RENEW. The client generates a transaction ID and inserts this value in the "transaction-id" field.

The client places the identifier of the destination server in a Server Identifier option.

The client MUST include a Client Identifier option to identify itself to the server. The client adds any appropriate options, including one or more IA options. The client MUST include the list of addresses the client currently has associated with the IAs in the Renew message.

The client MUST include an Option Request option to indicate the options the client is interested in receiving.

The client transmits the message according to section 14, using the following parameters:
IRT REN_TIMEOUT
MRT REN_MAX_RT
MRC 0
MRD Remaining time until T2

The message exchange is terminated when time T2 is reached, at which time the client begins a Rebind message exchange.

Test Setup: Connect all devices according to the Common Topology. Common Test Setup 1.1 is performed before each part. Disable DHCPv6 on the client device before each part.

Procedure:

Part A: Renew message format.

1. The NUT should have received IPv6 address information from TN1. TN1 assigns the T1 and T2 parameters to the NUT's IA (TN1 sets T1 to 200s and T2 to 1000s).
2. After time T1 observe the messages transmitted on link.

Part B: Retransmission and message exchange termination, T1 and T2 non-zero.

3. The NUT should have received IPv6 address information from TN1. TN1 assigns the T1 and T2 parameters to the NUT's IA (TN1 sets T1 to 200s and T2 to 1000s).
4. After time T1 observe the messages transmitted on link.

Observable Results:

- *Part A*

  Step 2: The NUT should send its first Renew message T1 (200) seconds after the reception of the Reply message from TN1.The NUT transmits a properly formatted Renew message to TN1 containing
  - A unicast SRC address
  - A "msg-type" field set to the value of RENEW (5)
  - A header containing a Transaction ID
  - A Server Identifier Option (containing a server DUID)
  - A Client Identifier Option (containing a client DUID)
  - An IA Address Option with the proper IPv6 address associated with the IA.
  - An Option Request Option.
- *Part B*

  Step 4: The NUT must cease the transmission of Renew messages after T2 – T1 (800) seconds. The observed RT for any retransmitted Renew messages should be within the range RT = 2*RTprev + RAND*RTprev, but never greater than REN_MAX_RT + RAND*REN_MAX_RT (660 seconds).

  The transaction ID is the same for all retransmitted messages.

Possible Problems:

- None.

Test DHCP_CONF.2.6: Creation and Transmission of Rebind message

Purpose: To verify a client device properly transmits Rebind messages.

References:

- [DHCP 3315] – Sections 5.5, 14 and 18.1.4

Discussion: At time T2 for an IA (which will only be reached if the server to which the Renew message was sent at time T1 has not responded), the client initiates a Rebind/Reply message exchange with any available server. The client includes an IA option with all addresses currently assigned to the IA in its Rebind message.

The client sets the "msg-type" field to REBIND. The client generates a transaction ID and inserts this value in the "transaction-id" field.

The client must include a Client Identifier option to identify itself to the server. The client must include the list of addresses the client currently has associated with the IAs in the Rebind message.

The client MUST include an Option Request option to indicate the options the client is interested in receiving.

The client transmits the message according to section 14, using the following parameters:
IRT REB_TIMEOUT
MRT REB_MAX_RT
MRC 0
MRD Remaining time until valid lifetimes of all addresses have expired

Test Setup: Connect the network according to the Common Topology. Common Test Setup 1.1 is performed before each part. Disable DHCPv6 on the client device before each part.

Procedure:

Part A: Rebind message format

1. The NUT should have received IPv6 address information from TN1.
2. TN1 does not respond to any Renew messages transmitted after T1.
3. After time T2 (300s after Renew message), observe the messages transmitted on link.

Part B: Retransmission and message exchange termination.

4. The NUT should have received IPv6 address information from TN1.
5. TN1 does not respond to messages transmitted after T1.
6. After time T2 (300s after renew message), observe the messages transmitted on link.

Observable Results:

- *Part A*

  Step 3: The time from when the NUT receives the Reply message from TN1 to when the NUT transmits the Rebind message is equivalent to (T1+T2).

  The NUT transmits a properly formatted Rebind message to TN1 containing
  - A “msg-type” field set to the value of REBIND (6).

- A header containing a Transaction ID
- A Client Identifier Option (containing a DUID)
- An IA Address Option with the proper IPv6 address associated with the IA
- An Option Request Option

- *Part B*

  Step 6: The NUT should send properly formatted Rebind messages to TN1 after T2 (300) seconds. The NUT must cease the transmission of Rebind messages after the valid lifetimes of all addresses have expired. The observed RT for any retransmitted Rebind messages should be within the range RT = 2*RTprev + RAND*RTprev, but never greater than REB_MAX_RT + RAND*REB_MAX_RT (660 seconds).

  The transaction ID is the same for all retransmitted messages.

  Note: After the valid lifetimes of all addresses in the IA have expired, the client may choose to use a Solicit message to locate a new DHCP server and send a Request for the expired IA to the new server, or the client may have other addresses in other IAs, so the client may choose to discard the expired IA and use the addresses in the other IAs.

Possible Problems:

- None.

Test DHCP_CONF.2.7: Creation and Transmission of Information-request message

Purpose: To verify a client device properly transmits Information-request messages.

References:

- [DHCP 3315] – Sections 5.5, 14, 18.1.5, 19.4.1, and 22.19
- [DHCP 3646] – Sections 3 and 4
- [DHCP 3736] – Sections 5.1 and 5.2

Discussion: The client uses an Information-request message to obtain configuration information without having addresses assigned to it.

The client sets the "msg-type" field to INFORMATION-REQUEST. The client generates a transaction ID and inserts this value in the "transaction-id" field.

The client SHOULD include a Client Identifier option to identify itself to the server. The client MUST include an Option Request option if the Information-Request message will be authenticated.

The client MUST include an Option Request option to indicate the options the client is interested in receiving.

The first Information-request message from the client on the interface MUST be delayed by a random amount of time between 0 and INF_MAX_DELAY. The client transmits the message according to section 14, using the following parameters:

IRT INF_TIMEOUT
MRT INF_MAX_RT
MRC 0
MRD 0

Upon receipt of a valid Reconfigure message, the client responds with either a Renew message or an Information-request message as indicated by the Reconfigure Message option.

Test Setup: Connect the network according to the Common Topology. Enable DHCPv6 on the client device before each part. Disable DHCPv6 on the client device before each part.

Procedure:

Part A: Information-request message format, application initiated exchange.

1. Allow the NUT to receive IPv6 prefix information through the Router Discovery process. TN1 transmits a Router Advertisement.
2. If the NUT does not obtain DNS information automatically, enable an application that requires name resolution.
3. Observe the messages transmitted on link.

Part B: Retransmission timer, application initiated exchange.

4. Allow the NUT to receive IPv6 prefix information through the Router Discovery process. TN1 transmits a Router Advertisement.
5. If the NUT does not obtain DNS information automatically, enable an application that requires name resolution.
6. Observe at least eight Information-request messages transmitted by the NUT on link.

Part C: Information-request message format, Server initiated exchange.

7. Common Test Setup 1.1 is performed. The NUT should receive IPv6 address information from TN1.
8. From TN1, transmit a valid Reply message with a DNS Recursive Name Server option.
9. When the NUT has the proper configuration, TN1 transmits a Reconfigure message, with a Reconfigure option with a msg-type field value of 11 (Information-request message).
10. Observe the messages transmitted on link.

Observable Results:

- *Part A*

  Step 3: The NUT transmits a properly formatted Information-request message to TN1 containing:
  - A "msg-type" field set to the value of 11 (INFORMATION-REQUEST).
  - A header containing a Transaction ID
  - An Option Request Option containing a DNS Recursive Name Server option
  - "Should" include a Client Identifier Option
- *Part B*

  Step 6: The first Information-request message from the client on the interface MUST be delayed by a random amount of time between 0 and INF_MAX_DELAY. The observed RT for any retransmitted Information-request messages should be within the range RT = 2*RTprev + RAND*RTprev, but never greater than INF_MAX_RT + RAND*INF_MAX_RT (132 seconds).

  The transaction ID is the same for all retransmitted messages.
- *Part C*

  Step 10: The NUT should send a properly formatted Information-request message to TN1 containing:
  - A "msg-type" field set to the value of 11 (INFORMATION-REQUEST).
  - A header containing a Transaction ID
  - A Reconfigure Accept option
  - An Option Request Option containing a DNS Recursive Name Server option

Possible Problems:

- Part A, B may be omitted if the NUT does not support an application that requires name resolution.

Test DHCP_CONF.2.8: Creation and Transmission of Release messages

Purpose: To verify that a client device transmits properly formatted Release messages and properly implements the mechanism for retransmission and message exchange termination for Release messages; to verify that a client device properly releases Ipv6 addresses configured by a server.

References:

- [DHCP 3315] – Sections 5.5, 14 and 18.1.6

Discussion: To release one or more addresses, a client sends a Release message to the server.

The client sets the "msg-type" field to RELEASE. The client generates a transaction ID and places this value in the "transaction-id" field.

The client MUST include a Client Identifier option to identify itself to the server. The client includes options containing the IAs for the addresses it is releasing in the "options" field. The addresses to be released MUST be included in the IAs.

The client MUST NOT use any of the addresses it is releasing as the source address in the Release message or in any subsequently transmitted message.

The client transmits the message according to section 14, using the following parameters:
IRT REL_TIMEOUT
MRT 0
MRC REL_MAX_RC
MRD 0

Test Setup: Connect all devices according to the Common Topology. Common Test Setup 1.1 is performed before each part. Disable DHCPv6 on the client device after each part.

Procedure:

Part A: Release message format and release of received address

1. Verify that the NUT is configured with the received IPv6 address information from TN1.
2. Configure the client to release the IPv6 address.
3. Observe any messages transmitted by the NUT.
4. From TN1, transmit an ICMPv6 Echo Request to the NUT for the released address.
5. Observe the messages transmitted on link.

Part B: Retransmission and message exchange termination, no Reply message from Server

6. Verify that the NUT is configured with the received IPv6 address information from TN1.
7. Configure the client to release the IPv6 address.
8. Observe the messages transmitted by the NUT.

Part C: Retransmission and message exchange termination, Server responds with Reply message

9. Verify that the NUT is configured with the received IPv6 address information from TN1.
10. Configure the client to release the IPv6 address.
11. Upon reception of the NUT's Release message, TN1 transmits a Reply message to the NUT that includes a Status Code option with value Success for each IA in the NUT's Release message,
12. Observe the messages transmitted on link.

Observable Results:

- *Part A*
  Step 3: The NUT transmits a properly formatted Release message to TN1 containing:
  - A "msg-type" field set to the value of 8 (RELEASE).
  - A header containing a Transaction ID.
  - A Client Identifier Option (containing a DUID)
  - A Server Identifier Option
  - An IA Address Option with the proper IPv6 address associated with the IA

  Step 5: The NUT must not reply to the Echo Request.
- *Part B*
  Step 8: The NUT should transmit at least one properly formatted Release message to TN1, but no more than REL_MAX_RC (5). The observed RT for any retransmitted Release messages should be within the range RT = 2*RTprev + RAND*Rtprev, but never outside the range 22 to 45 seconds. The transaction ID is the same for all retransmitted messages.
- *Part C*
  Step 12: The NUT should transmit a properly formatted Release message to TN1. The NUT should cease the transmission of Release messages upon reception of the Reply message from TN1.

Possible Problems:

- Part A, B, and C may be omitted if the NUT cannot configure to release its IPv6 address.

Test DHCP_CONF.2.9: Creation and Transmission of Decline messages

Purpose: To verify a client device properly creates transmits Decline messages.

References:

- [DHCP 3315] – Sections 5.5, 14, 18.1.7, and 18.1.8

Discussion: If a client detects that one or more addresses assigned to it by a server are already in use by another node, the client sends a Decline message to the server to inform it that the address is suspect.

The client sets the "msg-type" field to DECLINE. The client generates a transaction ID and places this value in the "transaction-id" field.

The client places the identifier of the server that allocated the address(es) in a Server Identifier option.

The client MUST include a Client Identifier option to identify itself to the server. The client includes options containing the IAs for the addresses it is declining in the "options" field.

The client must not use any of the addresses it is declining as the source address in the Decline message or any subsequently transmitted messages.

The client transmits the message according to Section 14, using the following parameters:
IRT DEC_TIMEOUT
MRT 0
MRC DEC_MAX_RC
MRD 0

The client SHOULD perform duplicate address detection on each of the addresses in any IAs it receives in the Reply message before using that address for traffic. If any of the addresses are found to be in use on the link, the client sends a Decline message to the server.

Test Setup: Connect the network according to the Common Topology. Common Test Setup 1.1 is performed before each part. Disable DHCPv6 on the client device before each part.

Procedure:

Part A: Decline message format

1. After receiving a DAD NS from the NUT, TN1 transmits a solicited NA for that tentative address.
2. Observe the messages transmitted on link.
3. TN1 transmits an ICMPv6 Echo Request to the same IPv6 address in the Reply message from TN1.
4. Observe the messages transmitted on link.

Part B: Retransmission and message exchange termination.

5. After receiving a DAD NS from the NUT, TN1 transmits a solicited NA for that tentative address.
6. Observe the messages transmitted on link.

Observable Results:

- *Part A*

  Step 2: The NUT transmits a properly formatted Decline message to TN1 containing:
  - A link-local source address, not the tentative address in Step 1
  - A "msg-type" field set to the value of 9 (DECLINE)
  - A header containing a Transaction ID
  - A Client Identifier Option (containing a DUID)
  - A Server Identifier Option
  - An IA Address Option with the IPv6 address acquired in Step 1 and the proper IA association

  Step 4: The NUT must not reply to the ICMPv6 Echo Request transmitted from TN1.
- *Part B*

  Step 6: The NUT should send a properly formatted Decline message to TN1. The NUT retransmits the second Decline message with a minimum delay of 1.7 seconds and a maximum delay of 2.3 seconds. The NUT retransmits the third Decline message with a minimum delay of 3.2 seconds and a maximum delay of 4.9 seconds. The NUT retransmits a total of DEC_MAX_RC (5) Decline messages. The observed RT for any retransmitted Decline messages should be within the range RT = 2*RTprev + RAND*RTprev, but never outside the range 22 to 45 seconds. The transaction ID is the same for all retransmitted messages.

Possible Problems:

- None.

Group 3: Message Reception

Scope:

The following tests focus on the client's implementation of DHCPv6 and the reception of valid DHCPv6 messages by a client and server device.

Test DHCP_CONF.3.1: Reception of Advertise messages

Purpose: To verify a client device properly handles the reception of Advertise messages.

References:

- [DHCP 3315] – Sections 17.1.2 and 17.1.3

Discussion: Upon receipt of one or more valid Advertise messages, the client selects one or more Advertise messages based upon the following criteria:

- Those Advertise messages with the highest server preference value are preferred over all other Advertise messages.
- Within a group of Advertise messages with the same server preference value, a client MAY select those servers whose Advertise messages advertise information of interest to the client.
- The client MAY choose a less-preferred server if that server has a better set of advertised parameters, such as the available addresses advertised in IAs.

Once a client has selected Advertise message(s), the client will typically store information about each server, such as server preference value, addresses advertised, when the advertisement was received, and so on.

Test Setup: Connect the devices according to the Common Topology. Disable router prefix delegation on the NUT. Enable DHCPv6 on the client device before each part. Disable DHCPv6 on the client device after each part.

Procedure:

Part A: Reception of Multiple Advertise messages with different preference values.

1. Upon reception of a Solicit message from the NUT, TN1 and TN2 transmit properly formatted Advertise messages. The Advertise message from TN1 contains a Preference option of 255, and the Advertise message from TN2 contains a Preference option of 0.
2. Observe the messages transmitted by the NUT on Link A.

Part B: Reception of Multiple Advertise messages with equal preference values.

3. Upon reception of a Solicit message from the NUT, TN1 and TN2 each transmit a properly formatted Advertise message. The Advertise message from TN1 contains a Preference option of 0, and the Advertise message from TN2 contains a Preference option of 0.
4. Observe the Solicit messages transmitted on Link A.

Observable Results:

- *Part A*
  Step 2: After RT seconds has elapsed, the NUT must choose the information from TN1 and send TN1 a Request message.
- *Part B*
  Step 4: After RT seconds has elapsed, the NUT MAY choose the information from TN1 or TN2 and send the chosen server a Request message.

Possible Problems:

- None.

Test DHCP_CONF.3.2: Reception of Reply Messages

Purpose: To verify a client device properly handles the reception of Reply messages.

References:

- [DHCP 3315] – Sections 17.1.4,18.1.8, and 19.4.5

Discussion: If the client includes a Rapid Commit option in the Solicit message, it will expect a Reply message that includes a Rapid Commit option in response. The client discards any Reply messages it receives that do not include a Rapid Commit option.

The client SHOULD perform duplicate address detection [17] on each of the addresses in any IAs it receives in the Reply message before using that address for traffic. If any of the addresses are found to be in use on the link, the client sends a Decline message to the server as described in section 18.1.7.

If the client receives a Reply message with a Status Code containing UnspecFail, the server is indicating that it was unable to process the message due to an unspecified failure condition. If the client retransmits the original message to the same server to retry the desired operation, the client MUST limit the rate at which it retransmits the message and limit the duration of the time during which it retransmits the message.

When the client receives a Reply message with a Status Code option with the value UseMulticast, the client records the receipt of the message and sends subsequent messages to the server through the interface on which the message was received using multicast. The client resends the original message using multicast.

When the client receives a NotOnLink status from the server in response to a Confirm message, the client performs DHCP server solicitation, as described in section 17, and client-initiated configuration as described in section 18.

When the client receives a NotOnLink status from the server in response to a Request, the client can either re-issue the Request without specifying any addresses or restart the DHCP server discovery process (see section 17).

The client examines the status code in each IA individually. If the status code is NoAddrsAvail, the client has received no usable addresses in the IA and may choose to try obtaining addresses for the IA from another server.

When the client receives a Reply message in response to a Renew or Rebind message, the client examines each IA independently. For each IA in the original Renew or Rebind message, the client:

- sends a Request message if the IA contained a Status Code option with the NoBinding status (and does not send any additional Renew/Rebind messages)
- sends a Renew/Rebind if the IA is not in the Reply message
- otherwise accepts the info

When the client receives a valid Reply message in response to a Release message, the client considers the Release event completed, regardless of the Status Code option(s) returned by the server.

When the client receives a valid Reply message in response to a Decline message, the client considers the Decline event completed, regardless of the Status Code option(s) returned by the server.

Test Setup: Connect the devices according to the Common Topology. Disable router prefix delegation on the NUT. Common Test Setup 1.1 is performed for part E, H, I , J, K, L, and M. DHCPv6 on the NUT is disabled after each part.

Procedure:

Part A: Valid Reply message.

1. Common Test Setup 1.1 is performed.
2. Observe the messages transmitted on link.
3. TN1 transmits an Echo Request to the NUT's Global Address.
4. Observe the messages transmitted on link.

Part B: Reply message in response to Solicit message, no Rapid Commit Option.

5. Enable DHCPv6 on the NUT.
6. Configure the NUT to include a Rapid Commit Option in its Solicit message*.
7. Upon reception of the Request message from the NUT, TN1 transmits a properly formatted Reply message that does not include a Rapid Commit Option.
8. Observe the messages transmitted on link.

Part C: Reply message contains UnspecFail.

9. Enable DHCPv6 on the NUT.
10. Upon reception of a Solicit message from the NUT, TN1 transmits a properly formatted Advertise message.
11. Upon reception of a Request message from the NUT, TN1 transmits a properly formatted Reply message containing a Status Code option with a value of UnspecFail.
12. Observe the messages transmitted on link.

Part D: Reply message contain UseMulticast.

13. Enable DHCPv6 on the NUT.
14. Upon reception of a Solicit message from the NUT, TN1 transmits a properly formatted Advertise message with a Server Unicast option containing a valid IPv6 address.
15. Upon reception of a unicast Request message from the NUT, TN1 transmits a Reply message with a Status Code option with the value UseMulticast.
16. Observe the messages transmitted on link.

Part E: Reply message contains NotOnLink in response to a Confirm message.

17. The NUT should have received IPv6 address information from TN1
18. Physically disconnect the NUT from the link on the proper interface.
19. After enough time elapses in which the NUT recognizes a link down situation (5 seconds), reconnect the NUT to the link.
20. Upon reception of a Confirm message from the NUT, TN1 transmits a properly formatted Reply message containing a Status Code option with a value of NotOnLink.
21. Observe the messages transmitted on Link A.

Part F: Reply message contains NotOnLink in response to a Request message.

22. Enable DHCPv6 on the NUT.
23. Upon reception of a Solicit message from the NUT, TN1 transmits a properly formatted Advertise message.
24. Upon reception of a Request message from the NUT, TN1 transmits a properly formatted Reply message containing a Status Code option with a value of NotOnLink.
25. Observe the messages transmitted on Link A.

Part G: Reply message contains NoAddrsAvail in response to a Request message.

26. Enable DHCPv6 on the NUT.

27. Upon reception of a Solicit message from the NUT, TN1 transmits a properly formatted Advertise message.
28. Upon reception of a Request message from the NUT, TN1 transmits a properly formatted Reply message containing a Status Code option with a value of NoAddrsAvail for the IAs for which the NUT requested configuration.
29. Observe the messages transmitted on Link A.

Part H: Reply message contains NoBinding in response to a Renew message.

30. The NUT should have received IPv6 address information from TN1. TN1 assigns the T1 and T2 parameters to the NUT's IA (TN1 sets T1 to 200s and T2 to 300s).
31. Upon reception of a Renew message from the NUT, TN1 transmits a properly formatted Reply message containing a Status Code option with a value of NoBinding for the IAs for which the NUT requested configuration.
32. Observe the messages transmitted on Link A.

Part I: Reply message contains NoBinding in response to a Rebind message.

33. The NUT should have received IPv6 address information from TN1. TN1 assigns the T1 and T2 parameters to the NUT's IA (TN1 sets T1 to 200s and T2 to 300s).
34. Upon reception of a Rebind message from the NUT, TN1 transmits a properly formatted Reply message containing a Status Code option with a value of NoBinding for the IAs for which the NUT requested configuration.
35. Observe the messages transmitted on Link A.

Part J: Reply message contains no IA in response to a Renew message.

36. The NUT should have received IPv6 address information from TN1. TN1 assigns the T1 and T2 parameters to the NUT's IA (TN1 sets T1 to 200s and T2 to 300s).
37. Upon reception of a Renew message from the NUT, TN1 transmits a properly formatted Reply message that does not contain the IAs the NUT requested configuration.
38. Observe the messages transmitted on Link A.

Part K: Reply message contains no IA in response to a Rebind message.

39. The NUT should have received IPv6 address information from TN1. TN1 assigns the T1 and T2 parameters to the NUT's IA (TN1 sets T1 to 200s and T2 to 300s).
40. Upon reception of a Rebind message from the NUT, TN1 transmits a properly formatted Reply message that does not contain the IAs the NUT requested configuration.
41. Observe the messages transmitted on Link A.

Part L: Reply message contains UnspecFail in response to a Release message.

42. The NUT should have received IPv6 address information from TN1
43. Configure the client to release the IPv6 address.
44. Upon reception of the NUT's Release message, TN1 transmits a Reply message to the NUT that includes a Status Code option with value UnspecFail for the IA in the NUT's Release message.
45. Observe the messages transmitted on Link A.
46. From TN1, transmit an ICMPv6 Echo Request to the NUT for the released address.
47. Observe the messages transmitted on Link A.

Part M: Reply message contains UnspecFail in response to a Decline message.

48. After receiving a DAD NS from the NUT, TN1 transmits a solicited NA for that tentative address.
49. Upon reception of the NUT's Decline message, TN1 transmits a Reply message to the NUT that includes a Status Code option with value UnspecFail for the IA in the NUT's Release message.
50. Observe the messages transmitted on Link A.
51. From TN1, transmit an ICMPv6 Echo Request to the NUT for the released address.
52. Observe the messages transmitted on Link A.

Observable Results:

- *Part A*

  Step 2: The NUT should perform duplicate address detection on each of the addresses in any IAs it receives in the Reply message from TN1 before using that address for traffic. The NUT transmitted DAD NS for each of its addresses.
  Step 4: The NUT should transmit an Echo Reply to TN1.
- *Part B*

  Step 8: The NUT must discard the Reply message. The NUT must continue transmitting its request message. The NUT must not perform DAD on any addresses.
- *Part C*

  Step 12: The NUT must continue transmitting its Request message. The NUT must terminate the message exchange after the transmission of REQ_MAX_RC (10) Request messages. The observed RT for any retransmitted Request messages should be within the range RT = 2*RTprev + RAND*Rtprev, but never greater than REQ_MAX_RT + RAND*REQ_MAX_RT (33 seconds).
- *Part D*

  Step 16: The NUT should resend the original Request message to the server using multicast through the interface on which the Reply message from TN1 was received.
- *Part E*

  Step 21: The NUT should begin a DHCP server solicitation and transmit a Solicit message to the All_DHCP_Relay_Agents_and_Servers address (FF02::1:2).
- *Part F*

  Step 25: The NUT should begin a DHCP server solicitation and transmit a Solicit message to the All_DHCP_Relay_Agents_and_Servers address (FF02::1:2), or retransmit the Request message (with the same transaction ID) without specifying any addresses.
- *Part G*

  Step 29: The NUT may begin a DHCP server solicitation and transmit a Solicit message to the All_DHCP_Relay_Agents_and_Servers address (FF02::1:2).
- *Part H*

  Step 32: Upon reception of the Reply message from TN1, the NUT should transmit a Request message with a Server ID option identifying TN1 for each of the IAs that the NUT included in the Renew message. The NUT did not send any additional Renew messages.
- *Part I*

  Step 35: Upon reception of the Reply message from TN1, the NUT should transmit a Renew/Rebind message.
- *Part J*

  Step 38: Upon reception of the Reply message from TN1, the NUT should transmit a Renew/Rebind message.
- *Part K*

  Step 41: Upon reception of the Reply message from TN1, the NUT should transmit a Request message with a Server ID option identifying TN1 for each of the IAs that the NUT included in the Renew message. The NUT did not send any additional Rebind messages.
- *Part L*

Step 45: Upon reception of the Reply message from TN1, the NUT did not send any additional Release messages.

Step 45: Upon reception of the Echo Request message from TN1 to the released address, the NUT did not send an Echo Reply message.

- *Part M*

  Step 50: Upon reception of the Reply message from TN1, the NUT did not send any additional Decline messages.

  Step 52: Upon reception of the Echo Request message from TN1 to the configured address, the NUT did not send an Echo Reply message.

Possible Problems:

- *In part B, if the NUT cannot be configured to include a Rapid Commit Option in its Solicit message, the test cannot be performed.

Test DHCP_CONF.3.3: Reception of Reconfigure messages (This test is currently unavailable)

Purpose: To verify a client device properly handles the reception of Reconfigure messages.

References:

- [DHCP 3315] – Sections 19.4.1

Discussion: Upon the receipt of a valid Reconfigure message, the client responds with either a Renew message or an Information-request message as indicated by the Reconfigure Message option (as defined in section 22.19). The client ignores the transaction-id field in the received Reconfigure message. While the transaction is in progress, the client silently discards any Reconfigure messages it receives.

The client ignores any additional Reconfigure messages until the exchange is complete. Subsequent Reconfigure messages cause the client to initiate a new exchange. The server can discontinue retransmission of Reconfigure messages to the client once the server receives the Renew or Information-request message from the client.

Test Setup: Connect the devices according to the Common Topology. Disable router prefix delegation on the NUT. Common Test Setup 1.1 is performed before each part. DHCPv6 on the NUT is disabled after each part.

Procedure:

Part A: Reception of First Reconfigure message

1. The NUT should have received IPv6 address information from TN1.
2. TN1 transmits a properly formatted Reconfigure message.
3. Observe the messages transmitted on link.

Part B: Reception of multiple Reconfigure message

4. The NUT should have received IPv6 address information from TN1.
5. TN1 transmits two properly formatted Reconfigure messages.
6. Observe the messages transmitted on link.

Part C: Reception of subsequent Reconfigure messages

7. The NUT should have received IPv6 address information from TN1.
8. TN1 transmits a properly formatted Reconfigure message.
9. Observe the messages transmitted on link.
10. Once TN1 receives a Renew message or an Information-request message, TN1 transmits a properly formatted Reconfigure message.
11. Observe the messages transmitted on link.

Observable Results:

- *Part A*
  Step 3: The client must respond with a Renew message or an Information-request message.
- *Part B*
  Step 6: The client must respond with a Renew message or an Information-request message. The client must silently ignore the second Reconfigure message and not respond with any messages.

- *Part C*
  Step 9: The client must respond with a Renew message or an Information-request message.
  Step 11: The client must respond with a new Renew message or an Information-request message as a new exchange had been initiated.

Possible Problems:

- None.