IPv6 READY

DHCPv6 Interoperability
Test Suite

Technical Document

Revision 1.1.0

IPv6 Forum
TAHI Project (Japan)
UNH InterOperability Lab (USA)

http://www.ipv6forum.org
http://www.ipv6ready.org

MODIFICATION RECORD

Version 1.1.0 September 15, 2009

- Added Group 4 RFC 3633 and Group 5 RFC 3633 + RFC 3646
- Removed Relay-Agent Basic Message Exchanges that includes an Interface ID Option (*Advanced)* tests.

Version 1.0.5 August 1, 2009

- Updated Observable Results from Version 1.0.4 update.

Version 1.0.4 November 14, 2008

- Changed Observable Results to indicate the Confirm-Reply Message does not contain an IA Option. Applies to following Test Cases:
  - Client Initiated: Transmission of Confirm messages
  - Server Initiated: Transmission of Reply messages with NotOnLink
  - Relay-Agent Basic Message Exchanges (B)
  - ADVANCED - Relay-Agent Basic Message Exchanges that includes an Interface ID Option (B)

Version 1.0.3 August 7, 2008

- Cleaned up test setup on:
  - Relay Agent Basic Message Exchange with DNS Configuration Options
  - Relay Agent Basic Message Exchange with DNS Configuration Options and Interface ID Option
  - Layered Relay Agent Basic Message Exchange with DNS Configuration Options
- Fixed topology diagram for Layered Relay Agent Stateless DHCPv6 Basic Message Exchange with DNS Configuration Options part A and B.
- Fixed Appendix (added missing elements and reworded broken ones)
- Fixed Relay-Agent Basic Message Exchanges part F and Relay-Agent Basic Message Exchanges that includes an Interface ID Option part F by adding REF-Router1 so there is a route between networks.
- Fixed Relay-Agent Basic Message Exchanges that includes an Interface ID Option part F observable results.

Version 1.0.2 June 12, 2008

- Added Parts to “Layered Relay-Agent Basic Message Exchange,” “Layered Relay-Agent Basic Message Exchange with DNS Configuration Options,” and “Layered Relay-Agent Stateless DHCPv6 Basic Message Exchange with DNS Configuration Options” to test server vs. Relay, then two test to test relay vs relay
- Added a statement to all section 2 and 3 test setups binding “dhcpv6.test.example.com” to REF-DNS-Server1”
- Added a check for responses to Neighbor Solicitations to:
    - “Client Initiated: Transmission of Release Messages”
    - “Client Initiated: Transmission of Decline Messages”
    - “Relay-Agent Basic Message Exchange” part e and f
    - “Relay-Agent Basic Message Exchange that includes and Interface ID Option” part e and f
- Updated test “Layered Relay-Agent Basic Message Exchange,” “Layered Relay-Agent Basic Message Exchange with DNS Configuration Options,” and “Layered Relay-Agent Stateless DHCPv6 Basic Message Exchange with DNS Configuration Options” to use REF-Client1 instead of TAR-Client1
- Modified Test “Client Initiated: Transmission of Decline Messages,” “Relay-Agent Basic Message Exchange” part f, and “Relay-Agent Basic Message Exchange that includes and Interface ID Option” to clarify addressing issues
- Modified Appendix to require test “Relay-Agent Basic Message Exchange” to be run once per pair of test partners instead of twice per pair.
- Updated “Client Initiated: Transmission of Confirm messages” and “Client Initiated: Transmission of Decline Messages” to allow for assumed status of SUCCESS when no status code is present.
- Modified Required tests
    - Client no longer needs to run:
        - “Layered Relay-Agent Basic Message Exchange”
        - “Layered Relay-Agent Basic Message Exchange with DNS Configuration Options”
        - “Layered Relay-Agent Stateless DHCPv6 Basic Message Exchange with DNS Configuration Options”
        - “Relay-Agent Basic Message Exchange that

includes an Interface ID Option”

    - “Relay-Agent Basic Message Exchange with DNS Configuration Options that includes an Interface ID Option”
    - “Stateless DHCPv6 Relay-Agent Basic Message Exchange with DNS Configuration Options that includes an Interface ID Option”
  - Servers and Relay Agents are allowed to run either:
    - “Relay-Agent Basic Message Exchange” or “Relay-Agent Basic Message Exchange that includes an Interface ID Option”
    - “Relay-Agent Basic Message Exchange with DNS Configuration Options” or “Relay-Agent Basic Message Exchange with DNS Configuration Options that includes an Interface ID Option”
    - “Stateless DHCPv6 Relay-Agent Basic Message Exchange with DNS Configuration Options” or “Stateless DHCPv6 Relay-Agent Basic Message Exchange with DNS Configuration Options that includes an Interface ID Option”
- Modified Appendix to reflect changed requirements
- Removed Interface ID check from “Stateless DHCPv6 Relay-Agent Basic Message Exchange with DNS Configuration Options”
- Fixed minor typos
- Fixed typos in Test “Layered Relay-Agent Basic Message Exchange with DNS Configuration Options” part Band D, “Transmission of Renew Messages for DNS Configuration Options” part B, and “Transmission of Rebind Messages for DNS Configuration Options” part B, “dhcpv6” was mistyped as “dhcpv6.test.example.com”
- Fixed typos in “Layered Relay-Agent Basic Message Exchange with DNS Configuration Options” part A and C, “dhcpv6.test.example.com” was mistyped as “dhcpv6”
- Added Copyright

Version 1.0.1	April 26, 2007
Version 1.0.0	April 25, 2007

ACKNOWLEDGMENTS

The IPv6 Forum would like to acknowledge the efforts of the following organizations in the development of this test suite.

University of New Hampshire – InterOperability Laboratory
TAHI Project

INTRODUCTION

Overview

The IPv6 forum plays a major role to bring together industrial actors, to develop and deploy the new generation of IP protocols. Contrary to IPv4, which started with a small closed group of implementers, the universality of IPv6 leads to a huge number of implementations. Interoperability has always been considered as a critical feature in the Internet community.

Due to the large number of IPv6 implementations, it is important to provide the market a strong signal proving the level of interoperability across various products.

To avoid confusion in the mind of customers, a globally unique logo programme should be defined. The IPv6 logo will give confidence to users that IPv6 is currently operational. It will also be a clear indication that the technology will still be used in the future. To summarize, this logo programme will contribute to the feeling that IPv6 is available and ready to be used.

The IPv6 Logo Program consists of three phases:

Phase I

In a first stage, the Logo will indicate that the product includes IPv6 mandatory core protocols and can interoperate with other IPv6 implementations.

Phase II

The "IPv6 ready" step implies a proper care, technical consensus and clear technical references. The IPv6 ready logo will indicate that a product has successfully satisfied strong requirements stated by the IPv6 Logo Committee (v6LC).

To avoid confusion, the logo "IPv6 Ready" will be generic. The v6LC will define the test profiles with associated requirements for specific functionalities.

Phase III

Same as Phase 2 with IPsec mandated.

Abbreviations and Acronyms

DAD: Duplicate Address Detection
DHCP: Dynamic Host Configuration Protocol
DUID: DHCP Unique Identifier
NUT: Node Under Test
IA: Identity Association
ID: Identifier
TN: Testing Node
TR: Test Router
TAR-XX: Target Device
REF-XX: Reference Device
Client: DHCPv6 Client Device
Server: DHCPv6 Server Device
RelayAgent: DHCPv6 Relay Agent Device
RR: Requesting Router
DR: Delegating Router

TEST ORGANIZATION

This document organizes tests by Section 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 by concatenating the short test suite name, the section number, the group number, and the test number within the group. These elements are separated by periods. The Test Number is the section, group and test number, also separated by periods.

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.

Resource Requirements: The Resource Requirements section specifies the software, hardware, and test equipment that will be needed to perform the test.

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 for that parameter.

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:

[2463] Internet Message Control Protocol (ICMPv6) for the Internet Protocol version 6 (IPv6) Specification, December 1998.

[3315] R. Droms, Editor. Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3315, June 2003.

[3633] IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6, O. Troan, R. Droms, December 2003

[3646] DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6), December, 2003.

[3736] Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6, April, 2004.

TABLE OF CONTENTS

General Requirements

To obtain the IPv6 Ready Logo Phase-2 for DHCPv6, the client, server and relay agent must satisfy all of the following requirements.

Equipment Type

There are five possibilities for equipment types:

DHCP client (or client):
A node that initiates requests on a link to obtain configuration parameters from one or more DHCP servers.

DHCP relay agent (or relay agent):
A node that acts as an intermediary to deliver DHCP messages between clients and servers, and is on the same link as the client.

DHCP server (or server):
A node that responds to requests from clients, and may or may not be on the same link as the client(s).

DHCP-PD Requesting Router:
A node that requests configuration for an IPv6 Prefix according to RFC 3633

DHCP-PD Delegating Router
A node that responds to requests for configuration of an IPv6 Prefix according to RFC 3633.

Advanced Functionality

DHCPv6 Logo consists of these ADVANCED functions.

1. Address Assignment
   - Group1 must be tested
2. DNS Configuration in parallel with Address Assignment
   - Group1 and Group2 must be tested
3. Stateless DHCPv6 for DNS Configuration
   - Group3 must be tested
4. Prefix Delegation
   - Group4 must be tested
5. Prefix Delegation in parallel with DNS Configuration
   - Group5 must be tested

Advanced Functionality Tests	**References**
Adv-1	RFC3315
Adv-2	RFC3315+RFC3646
Adv-3	RFC3736
Adv-4	RFC3633
Adv-5	RFC3633+RFC3646

*These may be combined.

Interoperable device requirement:

Each applicant must be tested against other devices according to the following (All Vendors MUST be different):

1. Client Application
    a. Must be tested against 2 Servers and 2 Relay-Agents
2. Server Application
    a. Must be tested against 2 Clients and 2 Relay-Agents
3. Relay-Agent Application
    a. Must be tested against:
        i. 2 Clients, 2 Servers, and 2 Relay-Agents
    b. 4 Different vendors are required, the vendor in each device type must be different.
4. Requesting Router Application
    a. Must be tested against 2 Delegating Routers
5. Delegating Router Application
    a. Must be tested against 2 Requesting Routers

Tests performed on Client/Server/Relay-Agent/RR/DR

The tests under the Client/Server/Relay-Agent column marked by an "X" must be performed as specified below. If there is no "X" listed under the Client/Server/Relay-Agent/RR/DR column, this test may be omitted.

	Adv-1			Adv-2			Adv-3			Adv-4		Adv-5	
	Client	Server	Relay-Agent	Client	Server	Relay-Agent	Client	Server	Relay-Agent	RR (client)	DR (Server)	RR (client)	DR (Server)
Group 1													
1.1	X	X											
1.2	X	X											
1.3	X	X											
1.4	X	X											
1.5	X	X											
1.6	X	X											
1.7	X	X											
1.8	X	X											
1.9	X	X	X										
1.10a		X	X										
1.10b		X	X										
1.10c			X										
1.10d			X										
Group 2													
2.1				X	X								
2.2				X	X	X							
2.3a					X	X							
2.3b					X	X							
2.3c					X	X							
2.3d					X	X							
2.3e						X							
2.3f						X							
2.3g						X							
2.3h						X							
2.4				X	X								
2.5				X	X								
Group 3													
3.1							X	X					
3.2							X	X	X				
3.3a								X	X				
3.3b								X	X				
3.3c								X	X				
3.3d								X	X				
3.3e									X				
3.3f									X				
3.3g									X				
3.3h									X				
Group 4													
4.1										X	X		
4.2										X	X		
4.3										X	X		
4.4										X	X		
4.5										X	X		
Group 5													
5.1												X	X
5.2												X	X
5.3												X	X

Group 1: RFC 3315

Scope

Tests in this group cover basic interoperability of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Request for Comments 3315.

Overview

These tests are designed to verify the readiness of DHCPv6 client, server and relay agent interoperability vis-à-vis the base specifications of the Dynamic Host Configuration Protocol for IPv6.

Test DHCPInterop.1.1: DHCPv6 Initialization

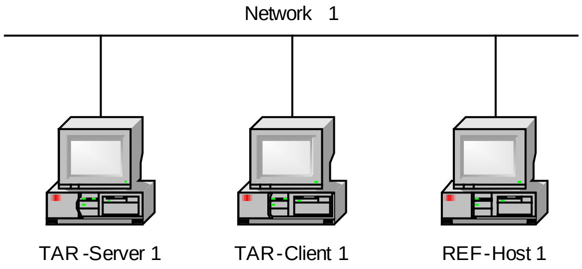
Purpose: To verify that a device can properly interoperate while using DHCPv6.

References:

- [3315] – Section 1.3, 17.1, 17.2
- [2463] – Section 5.5.3

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-Server1, REF-Host1 and enable DHCPv6. Disable DHCPv6 on all devices after test.



Procedure:

1. Configure TAR-Client1 to disable auto-configuration and enable DHCPv6.
2. Observe the packets on Network 1.
3. REF-Host1 transmits an Echo Request to the TAR-Client1's global address.
4. Observe the packets on Network 1.

Observable Results:

Step 2: TAR-Client1 sends a solicit message to the ALL_DHCP_Relay_Agents_and_Servers address. The TAR-Server1 sends an advertise message with the IP address information included. The TAR-Client1 then sends a request message to confirm the IP address and ask for additional information. The TAR-Server1 responds with a Reply message that contains the confirmed address.
Step 4: The TAR-Client1 transmits an Echo Reply in response to the Echo Request from REF-Host1.

Possible Problems:

- If the NUT does not work without the appropriate Router Advertisement, a REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1.

Test DHCPInterop1.2: Client Initiated: Transmission of Confirm messages

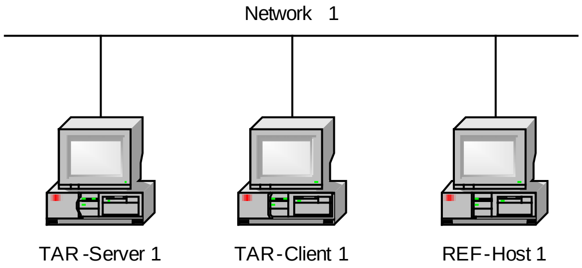
Purpose: To verify a client and server device properly handles Confirm message.

References:

- [3315] – Sections 5.5, 14, 18.1.2 and 18.2.2

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-Server1, REF-Host1 and enable DHCPv6. Disable DHCPv6 on all devices after test.



Procedure:

1. Configure the TAR-Client1 to enable DHCPv6.
2. Observe the messages transmitted on Network 1.
3. Ref-Host1 transmits an Echo Request to the TAR-Client1's global address.
4. Observe the messages transmitted on Network 1.
5. Disconnect the TAR-Client1 from Network 1.
6. Allow enough time to elapse such that the TAR-Client1 recognizes a link down, reconnect the TAR-Client1.
7. Observe the messages transmitted on Network 1.
8. Ref-Host1 transmits an Echo Request to the TAR-Client1's global address.
9. Observe the messages transmitted on Network 1.

Observable Results:

Step 2: The TAR-Client1 performed duplicate address detection on each of the addresses in the IAs it receives in the Reply message from TAR-Server1.
Step 4: The TAR-Client1 sends an Echo Reply in response to the Echo Request from Ref-Host1.
Step 7: The TAR-Client1 transmits a Confirm message to the server. TAR-Server1 responded with a REPLY without a status code option or with a status code option including a status code of 0 (Success) stating that the addresses are appropriate for the link. The REPLY Message does not contain an IA Option.
Step 9: The TAR-Client1 sends an Echo Reply in response to the Echo Request from Ref-Host1.

Possible Problems:

- If the NUT does not work without the appropriate Router Advertisement, a REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1.
- If the NUT device is TAR-Client1, and TAR-Server1 includes an IA Option in the Reply Message to the Confirm, the test may be considered a PASS, providing the Observable Result in Step 9 is satisfied. If the NUT device is TAR-Server1, it must not include an IA Option in the Reply Message to the Confirm, and must be considered a FAIL.

Test DHCPInterop1.3: Client Initiated: Transmission of Renew messages

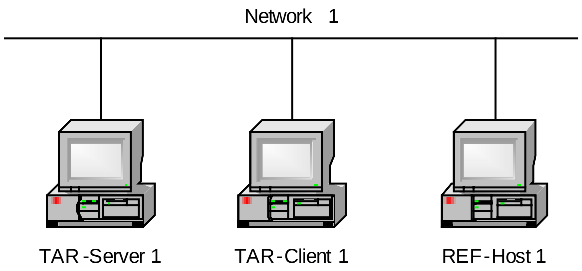
Purpose: To verify a client and server device properly handles Renew messages.

References:

- [3315] – Sections 5.5, 14 and 18.1.3

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-Server1, REF-Host1 and enable DHCPv6. Configure TAR-Server1 sets T1 to 50s and T2 to 80s. Disable DHCPv6 on all devices after test.



Procedure:

1. Configure the TAR-Client1 to enable DHCPv6.
2. The TAR-Client1 should have received IPv6 address information from the TAR-Server1. The TAR-Server1 assigns the T1 and T2 parameters to the TAR-Client1's IA (the TAR-Server1 sets T1 to 50s and T2 to 80s).
3. After time T1 observe the messages transmitted on Network 1.
4. REF-Host1 transmits an Echo Request to the TAR-Client1's global address.
5. Observe the messages transmitted on Network 1.

Observable Results:

Step 3: The TAR-Client1 should send its first Renew message T1 (50) seconds after the reception of the Reply message from the TAR-Server1. The TAR-Client1 transmits a Renew message. TAR-Server1 transmits a properly formatted Reply message in response to the Renew message.
Step 5: The TAR-Client1 transmits an Echo Reply in response to the Echo Request from REF-Host1.

Possible Problems:

- If the NUT does not work without the appropriate Router Advertisement, a REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1.

Test DHCPInterop1.4: Client Initiated: Transmission of Rebind messages

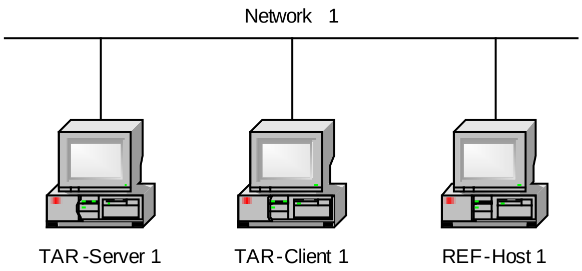
Purpose: To verify a client and server device properly handles Rebind messages.

References:

- [3315] – Sections 5.5, 14 and 18.1.4

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-Server1 and enable DHCPv6. Configure TAR-Server1 sets T1 to 50s and T2 to 80s. Disable DHCPv6 on all devices after test.



Procedure:

1. Configure the TAR-Client1 to enable DHCPv6.
2. Allow enough time for the TAR-Client1 to receive IPv6 address information from the TAR-Server1. The TAR-Server1 assigns the T1 and T2 parameters to the TAR-Client1's IA (the TAR-Server1 sets T1 to 50s and T2 to 80s).
3. Disconnect the TAR-Server1 from Network 1.
4. After time T2 (80s after Reply message), observe the messages transmitted on Network 1.
5. Reconnect the TAR-Server1 to the link and confirm that the TAR-Client1's address is renewed on the next rebind.
6. REF-Host1 transmits an Echo Request to the TAR-Client1's global address.
7. Observe the packets on Network 1.

Observable Results:

Step 4: The TAR-Client1 transmits a Rebind message.
Step 7: The TAR-Client1 transmits an Echo Reply in response to the Echo Request from REF-Host1.

Possible Problems:

- If the NUT does not work without the appropriate Router Advertisement, a REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1.

Test DHCPInterop1.5: Client Initiated: Transmission of Release messages

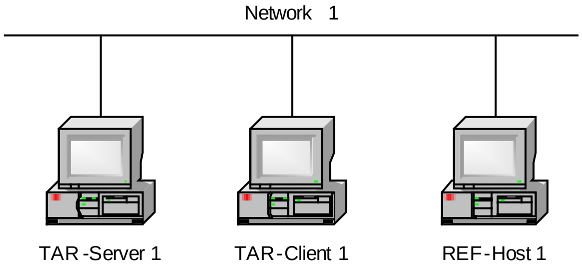
Purpose: To verify that a client and server device transmits properly formatted Release messages and to verify that a client device properly releases IPv6 addresses configured by a server.

References:

- [3315] – Sections 5.5, 14 and 18.1.6

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-Server1 and enable DHCPv6. Disable DHCPv6 on all devices after test.



Procedure:

1. Configure the TAR-Client1 to enable DHCPv6.
2. Allow enough time for the TAR-Client1 to receive IPv6 address information from the TAR-Server1.
3. Configure the TAR-Client1 to release the IPv6 global address.
4. Observe the messages transmitted on Network 1.
5. REF-Host1 transmits an ICMPv6 Echo Request to the TAR-Client1's released address.
6. Observe the messages transmitted on Network 1.

Observable Results:

Step 4: The TAR-Client1 transmits a Release message.
Step 6: The TAR-Client1 must not reply to the Echo Request or Neighbor Solicitations from REF-Host1.

Possible Problems:

- If the NUT does not work without the appropriate Router Advertisement, a REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1.

Test DHCPInterop1.6: Client Initiated: Transmission of Decline messages

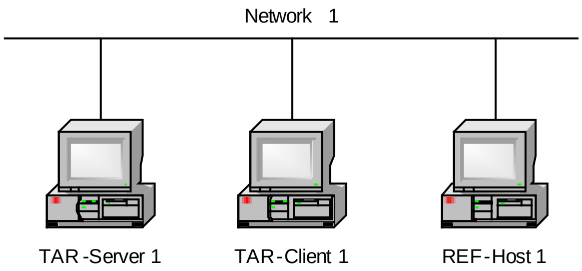
Purpose: To verify that a client and server properly handles the transmission and reception of Decline messages.

References:

- [3315] – Sections 5.5, 14, 18.1.7 and 18.2.7

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-Server1 and enable DHCPv6. Disable DHCPv6 on all devices after test.



Procedure:

1. Configure the TAR-Server1 to have only the address of the REF-Host1 in its address pool.
2. Configure the TAR-Client1 to enable DHCPv6.
3. Allow enough time for the TAR-Client1 to receive IPv6 address information from the TAR-Server1.
4. Observe the messages transmitted on Network 1.
5. TAR-Server1 transmits an ICMPv6 Echo Request to the REF-Host1's global address.
6. Observe the messages transmitted on Network 1.

Observable Results:

Step 4: TAR-Client1 transmits a DAD NS for its global address. The REF-Host1 transmits a solicited NA in response to the DAD NS with non-unique tentative address.

The TAR-Client1 transmits a Decline message. TAR-Server1 transmits a Reply Message.
Step 6: The TAR-Client1 must not reply to the Echo Request or Neighbor Solicitations from TAR-Server1.

Possible Problems:

- If the NUT does not work without the appropriate Router Advertisement, a REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1.

Test DHCPInterop1.7 Server Initiated: Transmission of Advertise messages with NoAddrsAvail

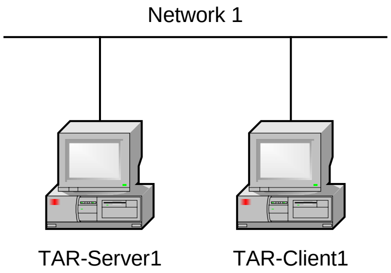
Purpose: To verify a client and server device properly handle Advertise messages with a status code of 2 (NoAddrsAvail).

References:

- [3315] – Section 17.1.3

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-Server1 and enable DHCPv6. Disable DHCPv6 on all devices after test.



Procedure:

1. Configure the TAR-Server1 to have no available addresses.
2. Configure the TAR-Client1 to enable DHCPv6.
3. Observe the messages transmitted on Network 1.

Observable Results:

> **Step 3:** The TAR-Server1 transmits an Advertise message containing the status code 2. The TAR-Client1 must ignore the Advertise message from the TAR-Server1 and not transmit a Request message.

Possible Problems:

- If the NUT does not work without the appropriate Router Advertisement, a REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1.

Test DHCPInterop1.8 Server Initiated: Transmission of Reply messages with NotOnLink

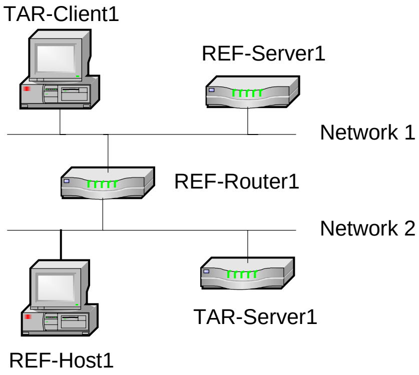
Purpose: To verify a client and server device properly handle Reply messages with NotOnLink.

References:

- [3315] – Section 18.1.8, 18.2.2

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Configure REF-Server1 and TAR-Server1 to have different prefix range for address assignment. Initialize REF-Server1, TAR-Server1, REF-Host1 and enable DHCPv6. Disable DHCPv6 on all devices after test.



Procedure:

1. Configure the TAR-Client1 to enable DHCPv6.
2. Allow enough time for the TAR-Client1 to receive IPv6 address information from REF-Server1.
3. Disconnect the TAR-Client1 from Network 1.
4. Allow enough time to elapse such that the TAR-Client1 recognizes a link down; reconnect the TAR-Client1 to Network 2.
5. Observe the messages transmitted on Network 2.
6. Allow enough time for the TAR-Client1 to receive IPv6 address information from TAR-Server1.
7. REF-Host1 transmits an ICMPv6 Echo Request to TAR-Client's new global address.
8. Observe the messages transmitted on Network 2.

Observable Results:

Step 5: The TAR-Client1 transmits a properly formatted Confirm message. The TAR-Server1 transmits a Reply message with the status code 4 (NotOnLink). The Reply Message does not contain an IA Option. The TAR-Client1 then performs DHCP server solicitation and client-initiated configuration.
Step 8: The TAR-Client1 transmits an Echo Reply in response to the Echo Request from REF-Host1.

Possible Problems:

- If the NUT does not work without the appropriate Router Advertisement, REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1 and Network 2.

Test DHCPInterop.1.9: Relay-Agent Basic Message Exchanges

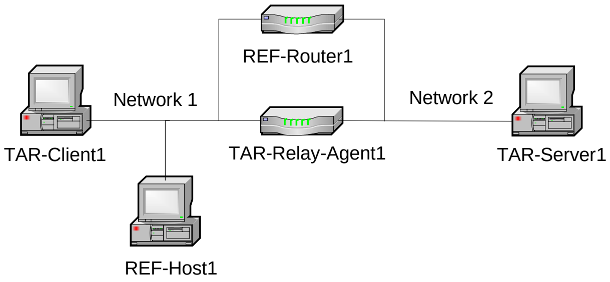
Purpose: To verify that a device can properly interoperate with a DHCPv6 Relay Agent.

References:

- [3315] – Section 20

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Configure REF-Router1 to transmit Router Advertisements with the M and O bit set to 1 on both Network 1 and Network 2. Initialize TAR-Server1, TAR-Relay-Agent1, REF-Host1 and enable DHCPv6. Disable DHCPv6 on all devices after each part. If the TAR Relay Agent supports or requires the use of an Interface-ID Option, it may be configured for this test. Since the use of the Interface ID is an ADVANCED functionality and is not mandatory, this test may be run without the Interface ID.



Procedure:

Part A: Basic Message Exchange

1. Configure TAR-Client1 to disable auto-configuration and enable DHCPv6.
2. Observe the packets on Network 1 and Network 2.
3. REF-Host1 transmits an Echo Request to the TAR-Client1's global address.
4. Observe the packets on Network 1.

Part B: Relay-Agent, Reception of Confirm message

5. Configure TAR-Client1 to disable auto-configuration and enable DHCPv6.
6. Observe the packets on Network 1 and Network 2.
7. Disconnect the TAR-Client1 from Network 1.
8. Allow enough time to elapse such that the TAR-Client1 recognizes a link down, reconnect the TAR-Client1.
9. Observe the packets on Network 1 and Network 2.
10. REF-Host1 transmits an Echo Request to the TAR-Client1's global address.
11. Observe the packets on Network 1.

Part C: Relay-Agent, Reception of Renew Message

12. Configure TAR-Client1 to disable auto-configuration and enable DHCPv6.

13. The TAR-Client1 should have received IPv6 address information from the TAR-Server1. The TAR-Server1 assigns the T1 and T2 parameters to the TAR-Client1's IA (the TAR-Server1 sets T1 to 50s and T2 80s).
14. After time T1 observe the messages on Network 1 and Network 2.
15. REF-Host1 transmits an Echo Request to the TAR-Client1's global address.
16. Observe the packets on Network 1.

Part D: Relay-Agent, Reception of Rebind Message

17. Configure TAR-Client1 to disable auto-configuration and enable DHCPv6.
18. The TAR-Client1 should have received IPv6 address information from the TAR-Server1. The TAR-Server1 assigns the T1 and T2 parameters to the TAR-Client1's IA (the TAR-Server1 sets T1 to 50s and T2 80s).
19. Disconnect TAR-Server1 from Network 2.
20. After time T2 (30s after Renew message), observe the message transmitted on Network 1 and Network 2.
21. Reconnect the TAR-Server1 to Network 2 and confirm that the TAR-Client1's address is renewed on the next rebind.
22. REF-Host1 transmits an Echo Request to the TAR-Client1's global address.
23. Observe the packets on Network 1.

Part E: Relay-Agent, Reception of Release Message

24. Configure TAR-Client1 to disable auto-configuration and enable DHCPv6.
25. Observe the packets on Network 1 and Network 2.
26. Configure the TAR-Client1 to release the IPv6 global address.
27. Observe the packets on Network 1 and Network 2.
28. REF-Host1 transmits an Echo Request to the TAR-Client1's global address.
29. Observe the packets on Network 1.

Part F: Relay-Agent, Reception of Decline Message

30. Configure the TAR-Server1 to have only the address of the REF-Host1 in its address pool.
31. Configure the TAR-Client1 to enable DHCPv6.
32. Allow enough time for the TAR-Client1 to receive IPv6 address information from the TAR-Server1.
33. Observe the messages transmitted on Network 1.
34. TAR-Server1 transmits an ICMPv6 Echo Request to the REF-Host1's global address.
35. Observe the messages transmitted on Network 1.

Observable Results:

- Part A

  Step 2: The TAR-Client1 sends a solicit message to the ALL_DHCP_Relay_Agents_and_Servers address. TAR-Relay-Agent1 transmits a Relay-forward Solicit message in relaying of the Solicit message from TAR-Client1. The TAR-Server1 sends a Relay-reply advertise message with the IP address information included. TAR-Relay-Agent1 transmits an Advertisement message to TAR-Client1. TAR-Relay-Agent1 transmits a Relay-forward Request message in relaying of the Request message from TAR-Client1 to TAR-Server1 and the TAR-Relay-Agent1 transmitted a Reply message in relaying of the Relay-reply Reply message from TAR-Server1 to TAR-Client1 that contains the confirmed address.

  Step 4: The TAR-Client1 transmits an Echo Reply in response to the Echo Request from REF-Host1.

- Part B

  Step 6: The TAR-Client1 sends a solicit message to the ALL_DHCP_Relay_Agents_and_Servers address. TAR-Relay-Agent1 transmits a Relay-forward Solicit message in relaying of the Solicit message from TAR-Client1. The TAR-Server1 sends a Relay-reply advertise message with the IP address information included. TAR-Relay-Agent1 transmits an Advertisement message to TAR-Client1. TAR-Relay-Agent1 transmits a Relay-forward Request message in relaying of the Request message from TAR-Client1 to TAR-Server1 and the TAR-Relay-Agent1 transmitted a Reply message in relaying of the Relay-reply Reply message from TAR-Server1 to TAR-Client1 that contains the confirmed address.

  Step 9: TAR-Relay-Agent1 transmitted a Relay-forward Confirm message in relaying of the Confirm message. TAR-Relay-Agent1 then transmitted a Reply message in relaying of the Relay-reply message from TAR-Server1 to TAR-Client1. The Reply Message does not contain an IA Option.

  Step 11: The TAR-Client1 transmits an Echo Reply in response to the Echo Request from REF-Host1.
- Part C

  Step 14: TAR-Relay-Agent1 transmitted a Relay-forward Renew message in relaying of the Renew message. TAR-Relay-Agent1 then transmitted a Reply message in relaying of the Relay-reply message from TAR-Server1 to TAR-Client1.

  Step 16: The TAR-Client1 transmits an Echo Reply in response to the Echo Request from REF-Host1.
- Part D

  Step 20: TAR-Relay-Agent1 transmitted a Relay-forward Rebind message in relaying of the Rebind message.

  Step 23: The TAR-Client1 transmits an Echo Reply in response to the Echo Request from REF-Host1.
- Part E

  Step 25: The TAR-Client1 sends a solicit message to the ALL_DHCP_Relay_Agents_and_Servers address. TAR-Relay-Agent1 transmits a Relay-forward Solicit message in relaying of the Solicit message from TAR-Client1. The TAR-Server1 sends a Relay-reply advertise message with the IP address information included. TAR-Relay-Agent1 transmits an Advertisement message to TAR-Client1. TAR-Relay-Agent1 transmits a Relay-forward Request message in relaying of the Request message from TAR-Client1 to TAR-Server1 and the TAR-Relay-Agent1 transmitted a Reply message in relaying of the Relay-reply Reply message from TAR-Server1 to TAR-Client1 that contains the confirmed address.

  Step 27: TAR-Relay-Agent1 transmitted a Relay-forward Release message in relaying of the Release message. TAR-Relay-Agent1 then transmitted a Reply message in relaying of the Relay-reply message from TAR-Server1 to TAR-Client1.

  Step 29: The TAR-Client1 does not transmit an Echo Reply in response to the Echo Request from REF-Host1.
- Part F

  Step 33: TAR-Relay-Agent1 transmitted a Relay-forward Decline message in relaying of the Decline message. TAR-Relay-Agent1 then transmitted a Reply message in relaying of the Relay-reply message from TAR-Server1 to TAR-Client1.

  Step 35: The TAR-Client1 does not transmit an Echo Reply in response to the Echo Request from REF-Host1.

Possible Problems:

- Part B: If the NUT device is TAR-Client1, and TAR-Server1 includes an IA Option in the Reply Message to the Confirm, the test may be considered a PASS, providing the Observable Result in Step 9 is satisfied.   If the NUT device is TAR-Server1, it must not include an IA Option in the Reply Message to the Confirm, and must be considered a FAIL.

Test DHCPInterop.1.10: Layered Relay-Agent Basic Message Exchange

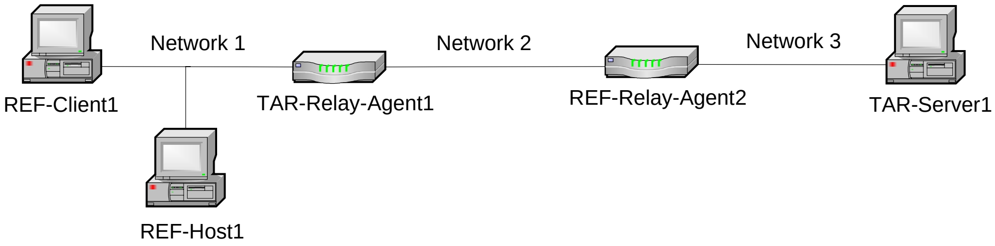
Purpose: To verify that a device can properly interoperate with multiple DHCPv6 Relay Agents.
References:

- [3315] – Section 20

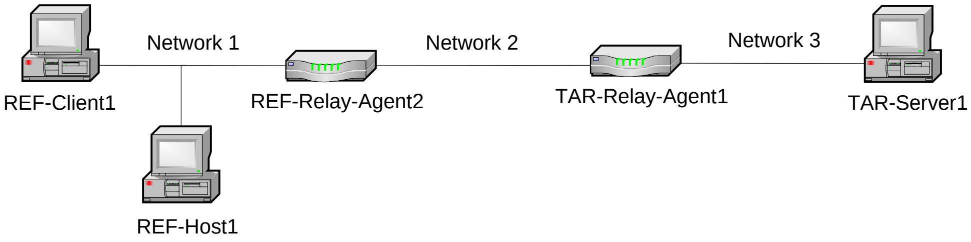
Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-Server1, REF-Client1, TAR-Relay-Agent1, TAR-Relay-Agent2, REF-Host1 and enable DHCPv6. Disable DHCPv6 on all devices after each part.

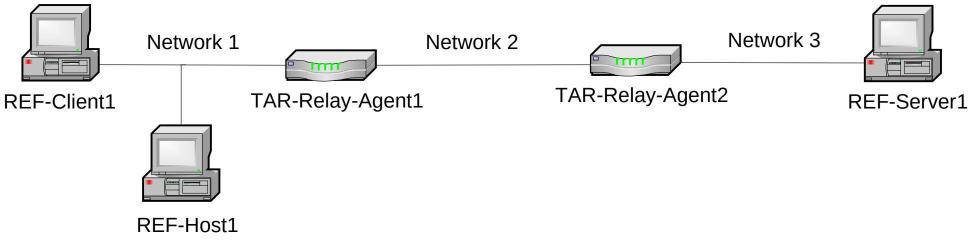
Part A:



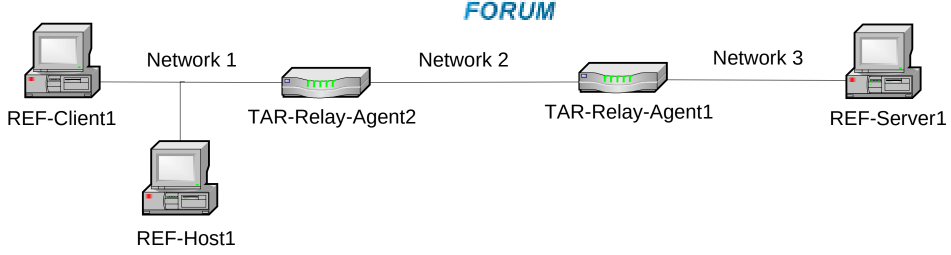
Part B:



Part C:



Part D:



Procedure:

Part A: Basic Message Exchange (Relay Agent to Server)

1. Configure REF-Client1 to disable auto-configuration and enable DHCPv6.
2. Observe the packets on Network 1, Network 2, and Network 3.
3. REF-Host1 transmits an Echo Request to the REF-Client1's global address.
4. Observe the packets on Network 1.

Part B: Basic Message Exchange (Relay Agent to Server)

5. Configure REF-Client1 to disable auto-configuration and enable DHCPv6.
6. Observe the packets on Network 1, Network 2, and Network 3.
7. REF-Host1 transmits an Echo Request to the REF-Client1's global address.
8. Observe the packets on Network 1.

Part C: Basic Message Exchange (Relay Agent to Relay Agent)

9. Configure REF-Client1 to disable auto-configuration and enable DHCPv6.
10. Observe the packets on Network 1, Network 2, and Network 3.
11. REF-Host1 transmits an Echo Request to the REF-Client1's global address.
12. Observe the packets on Network 1.

Part D: Basic Message Exchange (Relay Agent to Relay Agent)

13. Configure REF-Client1 to disable auto-configuration and enable DHCPv6.
14. Observe the packets on Network 1, Network 2, and Network 3.
15. REF-Host1 transmits an Echo Request to the REF-Client1's global address.
16. Observe the packets on Network 1.

Observable Results:

- *Part A*

  Step 2:

  - The REF-Client1 transmitted a solicit message on to the ALL_DHCP_Relay_Agents_and_Servers address.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Solicit message from REF-Client1.
  - REF-Relay-Agent2 transmitted a Relay-Forward message to the TAR-Server1 containing the Relay-Forward message from TAR-Relay-Agent1.
  - TAR-Server1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing:
    - A Relay-Reply containing an Advertise message with the IP address information.
  - The REF-Relay-Agent2 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing the Advertise message.
  - TAR-Relay-Agent1 transmitted an Advertise message to REF-Client1.
  - REF-Client1 transmitted a Request message to the ALL_DHCP_Relay_Agents_and_Servers address.

    - TAR-Relay-Agent1 transmitted a Relay-forward message containing the Request message from REF-Client1 to REF-Relay-Agent2.
    - REF-Relay-Agent2 transmitted a Relay-Forward message containing the Relay-Forward message from TAR-Relay-Agent1 to TAR-Server1.
    - TAR-Server1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing:
        - A Relay-Reply containing a Reply message with the confirmed IP address.
    - REF-Relay-Agent2 transmitted a Relay-Reply message containing a Reply message to TAR-Relay-Agent1.
    - TAR-Relay-Agent1 transmitted a Reply message to REF-Client1 that contains the confirmed address.

    Step 4: The REF-Client1 transmits an Echo Reply in response to the Echo Request from REF-Host1.

- *Part B*

    Step 6:

    - The REF-Client1 transmitted a solicit message on to the ALL_DHCP_Relay_Agents_and_Servers address.
    - REF-Relay-Agent2 transmitted a Relay-Forward message containing the Solicit message from REF-Client1.
    - TAR-Relay-Agent1 transmitted a Relay-Forward message to the TAR-Server1 containing the Relay-Forward message from REF-Relay-Agent2.
    - TAR-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
        - A Relay-Reply containing an Advertise message with the IP address information.
    - TAR-Relay-Agent1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing the Advertise message.
    - REF-Relay-Agent2 transmitted an Advertise message to REF-Client1.
    - REF-Client1 transmitted a Request message to the ALL_DHCP_Relay_Agents_and_Servers address.
    - REF-Relay-Agent2 transmitted a Relay-forward message containing the Request message from REF-Client1 to TAR-Relay-Agent1.
    - TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Relay-Forward message from REF-Relay-Agent2 to TAR-Server1.
    - TAR-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
        - A Relay-Reply containing a Reply message with the confirmed IP address.
    - TAR-Relay-Agent1 transmitted a Relay-Reply message containing a Reply message to REF-Relay-Agent2.
    - TAR-Relay-Agent1 transmitted a Reply message to REF-Client1 that contains the confirmed address.

    Step 8: The REF-Client1 transmits an Echo Reply in response to the Echo Request from REF-Host1.

- *Part C*

    Step 10:

    - The REF-Client1 transmitted a solicit message on to the ALL_DHCP_Relay_Agents_and_Servers address.
    - TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Solicit message from REF-Client1.
    - TAR-Relay-Agent2 transmitted a Relay-Forward message to the REF-Server1 containing the Relay-Forward message from TAR-Relay-Agent1.

    - REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent2 containing:
        - A Relay-Reply containing an Advertise message with the IP address information.
    - The TAR-Relay-Agent2 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing the Advertise message.
    - TAR-Relay-Agent1 transmitted an Advertise message to REF-Client1.
    - REF-Client1 transmitted a Request message to the ALL_DHCP_Relay_Agents_and_Servers address.
    - TAR-Relay-Agent1 transmitted a Relay-forward message containing the Request message from REF-Client1 to TAR-Relay-Agent2.
    - TAR-Relay-Agent2 transmitted a Relay-Forward message containing the Relay-Forward message from TAR-Relay-Agent1 to REF-Server1.
    - REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent2 containing:
        - A Relay-Reply containing a Reply message with the confirmed IP address.
    - TAR-Relay-Agent2 transmitted a Relay-Reply message containing a Reply message to TAR-Relay-Agent1.
    - TAR-Relay-Agent1 transmitted a Reply message to REF-Client1 that contains the confirmed address.

  Step 12: The REF-Client1 transmits an Echo Reply in response to the Echo Request from REF-Host1.

- Part D

  Step 14:

    - The REF-Client1 transmitted a solicit message on to the ALL_DHCP_Relay_Agents_and_Servers address.
    - TAR-Relay-Agent2 transmitted a Relay-Forward message containing the Solicit message from REF-Client1.
    - TAR-Relay-Agent1 transmitted a Relay-Forward message to the REF-Server1 containing the Relay-Forward message from TAR-Relay-Agent2.
    - REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
        - A Relay-Reply containing an Advertise message with the IP address information.
    - TAR-Relay-Agent1 transmitted a Relay-Reply message to TAR-Relay-Agent2 containing the Advertise message.
    - TAR-Relay-Agent2 transmitted an Advertise message to REF-Client1.
    - REF-Client1 transmitted a Request message to the ALL_DHCP_Relay_Agents_and_Servers address.
    - TAR-Relay-Agent2 transmitted a Relay-forward message containing the Request message from REF-Client1 to TAR-Relay-Agent1.
    - TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Relay-Forward message from TAR-Relay-Agent1 to REF-Server1.
    - REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
        - A Relay-Reply containing a Reply message with the confirmed IP address.
    - TAR-Relay-Agent1 transmitted a Relay-Reply message containing a Reply message to TAR-Relay-Agent2.
    - TAR-Relay-Agent1 transmitted a Reply message to REF-Client1 that contains the confirmed address.

  Step 16: The REF-Client1 transmits an Echo Reply in response to the Echo Request from REF-Host1.

Possible Problems:

- If the NUT does not work without the appropriate Router Advertisement, a REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1.

Group 2: RFC 3646

Scope

Tests in this group cover basic interoperability of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Request for Comments 3646.

Overview

These tests are designed to verify the readiness of DHCPv6 client and server interoperability vis-à-vis the specifications of the Dynamic Host Configuration Protocol for IPv6 options for passing a list of available DNS recursive name servers and a domain search list to a client.

Test DHCPInterop.2.1: DHCPv6 Initialization with DNS Configuration Options

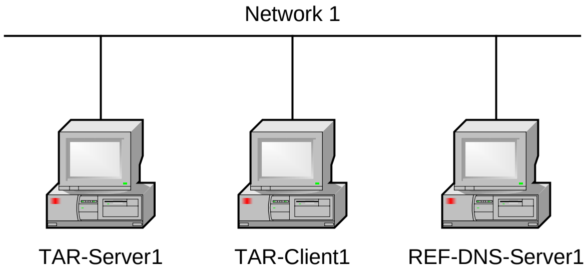
Purpose: To verify that a device can properly interoperate while using DHCPv6 with DNS configuration options.

References:

- [3315] – Section 1.3
- [3646] – Section 3, 4

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-Server1, REF-DNS-Server1 and enable DHCPv6. Configure REF-DNS-Server1 to have a DNS host name of "dhcpv6" in the "test.example.com" domain. Disable DHCPv6 on all devices after each part.



Procedure:

Part A: DNS Recursive Name Server Option

1. Configure TAR-Server1 to include a DNS Recursive Name Server option that includes REF-DNS-Server1's global IPv6 address
2. Configure TAR-Client1 to enable DHCPv6.
3. Allow enough time for the TAR-Client1 to receive IPv6 address information from the TAR-Server1.
4. Configure TAR-Client1 to transmit an Echo Request to "dhcpv6.test.example.com".
5. Observe the packets transmitted on Network 1.

Part B: Domain Search List Option

6. Configure TAR-Server1 to include a DNS Recursive Name Server option that includes REF-DNS-Server1's Global IPv6 address as the name server and a Domain Search List option that includes "test.example.com".
7. Configure TAR-Client1 to enable DHCPv6.
8. Allow enough time for The TAR-Client1 to receive IPv6 address information from the TAR-Server1.
9. Configure TAR-Client1 to transmit an Echo Request to "dhcpv6".
10. Observe the packets transmitted on Network 1.

Observable Results:

- *Part A*
  Step 5: The TAR-Client1 receives an Echo Reply from REF-DNS-Server1.
- *Part B*
  Step 10: The TAR-Client1 receives an Echo Reply from REF-DNS-Server1.

Possible Problems:

- In each part, if the NUT does not have the command that transmits an Echo Request, the NUT can use an alternate command that transmits a DNS Standard Query.
- If the NUT does not work without the appropriate Router Advertisement, a REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1.

Test DHCPInterop.2.2: Relay Agent Basic Message Exchange with DNS Configuration Options

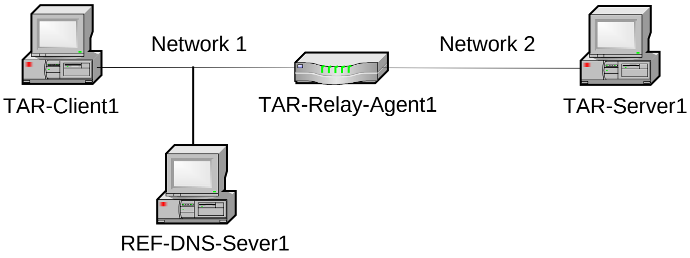
Purpose: To verify that a device can properly interoperate with a DHCPv6 Relay Agent while using DHCPv6 with DNS configuration options.

References:

- [3315] – Section 1.3
- [3315] – Section 20
- [3646] – Section 3, 4

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-Server1, TAR-Client1, TAR-Relay-Agent1, REF-DNS-Server1 and enable DHCPv6. Configure REF-DNS-Server1 to have a DNS host name of "dhcpv6" in the "test.example.com" domain. Disable DHCPv6 on all devices after each part. If the TAR Relay Agent supports or requires the use of an Interface-ID Option, it may be configured for this test. Since the use of the Interface ID is an ADVANCED functionality and is not mandatory, this test may be run without the Interface ID.



Procedure:

Part A: DNS Recursive Name Server Option

1. Configure TAR-Server1 to include a DNS Recursive Name Server option that includes REF-DNS-Server1's Global IPv6 address as the name server.
2. Configure TAR-Client1 to disable auto-configuration and enable DHCPv6.
3. Observe the packets on Network 1 and Network 2.
4. Configure TAR-Client1 to transmit an Echo Request to "dhcpv6.test.example.com".
5. Observe the packets transmitted on Network 1.

Part B: Domain Search List Option

6. Configure TAR-Server1 to include a DNS Recursive Name Server option that includes REF-DNS-Server1's Global IPv6 address as the name server and a Domain Search List option that includes "test.example.com".
7. Configure TAR-Client1 to disable auto-configuration and enable DHCPv6.
8. Observe the packets on Network 1 and Network 2.

9. Configure TAR-Client1 to transmit an Echo Request to “dhcpv6”.
10. Observe the packets transmitted on Network 1.

Observable Results:

- *Part A*

  Step 3: The TAR-Client1 sends a solicit message to the ALL_DHCP_Relay_Agents_and_Servers address. TAR-Relay-Agent1 transmits a Relay-forward Solicit message in relaying of the Solicit message from TAR-Client1. The TAR-Server1 sends a Relay-reply advertise message with the IP address information included and a DNS Recursive Name Server option. TAR-Relay-Agent1 transmits an Advertisement message to TAR-Client1 containing the DNS Recursive Name Server option. TAR-Relay-Agent1 transmits a Relay-forward Request message in relaying of the Request message from TAR-Client1 to TAR-Server1 and the TAR-Relay-Agent1 transmitted a Reply message in relaying of the Relay-reply Reply message containing the DNS Recursive Name Server option from TAR-Server1 to TAR-Client1 that contains the confirmed address.

  Step 5: The TAR-Client1 receives an Echo Reply from REF-DNS-Server1.
- *Part B*

  Step 8: The TAR-Client1 sends a solicit message to the ALL_DHCP_Relay_Agents_and_Servers address. TAR-Relay-Agent1 transmits a Relay-forward Solicit message in relaying of the Solicit message from TAR-Client1. The TAR-Server1 sends a Relay-reply advertise message with the IP address information included and a Domain Search List option. TAR-Relay-Agent1 transmits an Advertisement message to TAR-Client1 containing the Domain Search List option. TAR-Relay-Agent1 transmits a Relay-forward Request message in relaying of the Request message from TAR-Client1 to TAR-Server1 and the TAR-Relay-Agent1 transmitted a Reply message in relaying of the Relay-reply Reply message containing the Domain Search List option from TAR-Server1 to TAR-Client1 that contains the confirmed address.

  Step 10: The TAR-Client1 receives an Echo Reply from REF-DNS-Server1.

Possible Problems:

- In each part, if the NUT does not have the command that transmits an Echo Request, the NUT can use an alternate command that transmits a DNS Standard Query.
- If the NUT does not work without the appropriate Router Advertisement, a REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1.

Test DHCPInterop.2.3: Layered Relay Agent Basic Message Exchange with DNS Configuration Options

Purpose: To verify that a device can properly interoperate with multiple DHCPv6 Relay Agents while using DHCPv6 with DNS configuration options.

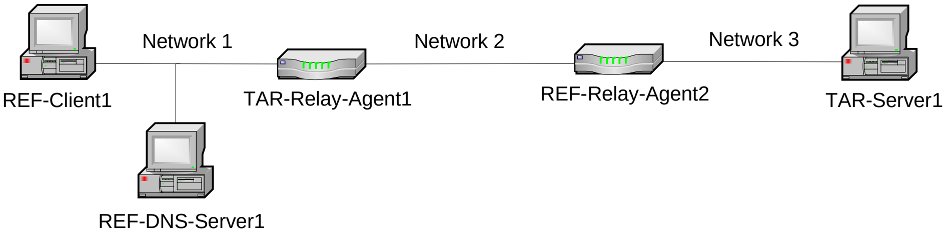
References:

- [3315] – Section 1.3
- [3315] – Section 20
- [3646] – Section 3, 4

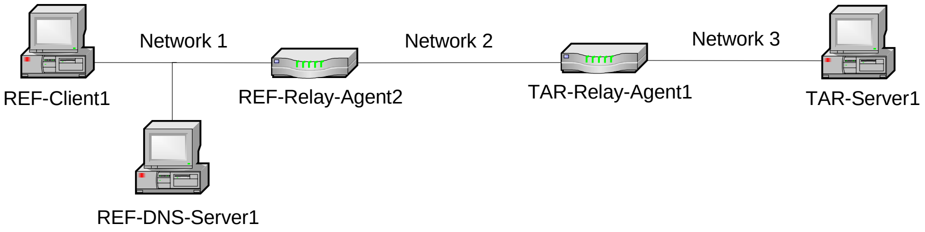
Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-Server1, REF-Client1, TAR-Relay-Agent1, TAR-Relay-Agent2, REF-DNS-Server1 and enable DHCPv6. Configure REF-DNS-Server1 to have a DNS host name of "dhcpv6" in the "test.example.com" domain. Disable DHCPv6 on all devices after each part.

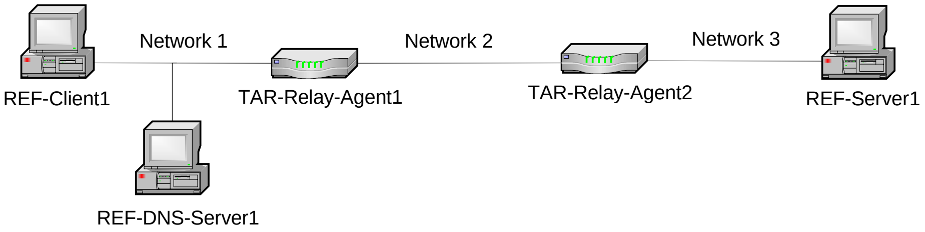
Part A-B:



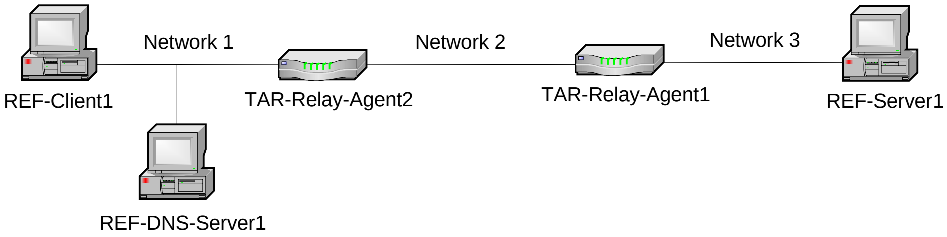
Part C-D:



Part E-F:



Part G-H:



Procedure:

Part A: DNS Recursive Name Server Option(Relay Agent to Server)

1. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1's Global IPv6 address included as the name server.
2. Configure REF-Client1 to disable auto-configuration and enable DHCPv6.
3. Observe the packets on Network 1, Network 2, and Network 3.
4. Configure REF-Client1 to transmit an Echo Request to "dhcpv6.test.example.com".
5. Observe the packets transmitted on Network 1.

Part B: Domain Search List Option(Relay Agent to Server)

6. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1's Global IPv6 address included as the name server and a Domain Search List option that includes "test.example.com".
7. Configure REF-Client1 to disable auto-configuration and enable DHCPv6.
8. Observe the packets on Network 1, Network 2, and Network 3.
9. Configure REF-Client1 to transmit an Echo Request to "dhcpv6".
10. Observe the packets transmitted on Network 1.

Part C: DNS Recursive Name Server Option(Relay Agent to Server)

11. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1's Global IPv6 address included as the name server.
12. Configure REF-Client1 to disable auto-configuration and enable DHCPv6.
13. Observe the packets on Network 1, Network 2, and Network 3.
14. Configure REF-Client1 to transmit an Echo Request to "dhcpv6.test.example.com".
15. Observe the packets transmitted on Network 1.

Part D: Domain Search List Option(Relay Agent to Server)

16. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1's Global IPv6 address included as the name server and a Domain Search List option that includes "test.example.com".
17. Configure REF-Client1 to disable auto-configuration and enable DHCPv6.
18. Observe the packets on Network 1, Network 2, and Network 3.
19. Configure REF-Client1 to transmit an Echo Request to "dhcpv6".
20. Observe the packets transmitted on Network 1.

Part E: DNS Recursive Name Server Option(Relay Agent to Relay Agent)

21. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1's Global IPv6 address included as the name server.
22. Configure REF-Client1 to disable auto-configuration and enable DHCPv6.
23. Observe the packets on Network 1, Network 2, and Network 3.
24. Configure REF-Client1 to transmit an Echo Request to "dhcpv6.test.example.com".
25. Observe the packets transmitted on Network 1.

Part F: Domain Search List Option(Relay Agent to Relay Agent)

26. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1's Global IPv6 address included as the name server and a Domain Search List option that includes "test.example.com".
27. Configure REF-Client1 to disable auto-configuration and enable DHCPv6.
28. Observe the packets on Network 1, Network 2, and Network 3.
29. Configure REF-Client1 to transmit an Echo Request to "dhcpv6".
30. Observe the packets transmitted on Network 1.

Part G: DNS Recursive Name Server Option(Relay Agent to Relay Agent)

31. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1's Global IPv6 address included as the name server.
32. Configure REF-Client1 to disable auto-configuration and enable DHCPv6.
33. Observe the packets on Network 1, Network 2, and Network 3.
34. Configure REF-Client1 to transmit an Echo Request to "dhcpv6.test.example.com".
35. Observe the packets transmitted on Network 1.

Part H: Domain Search List Option(Relay Agent to Relay Agent)

36. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1's Global IPv6 address included as the name server and a Domain Search List option that includes "test.example.com".
37. Configure REF-Client1 to disable auto-configuration and enable DHCPv6.
38. Observe the packets on Network 1, Network 2, and Network 3.
39. Configure REF-Client1 to transmit an Echo Request to "dhcpv6".
40. Observe the packets transmitted on Network 1.

Observable Results:

- *Part A*

  Step 3:

  - The REF-Client1 transmitted a solicit message on to the ALL_DHCP_Relay_Agents_and_Servers address.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Solicit message from REF-Client1.
  - REF-Relay-Agent2 transmitted a Relay-Forward message to the TAR-Server1 containing the Relay-Forward message from TAR-Relay-Agent1.
  - TAR-Server1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing:
    - A Relay-Reply containing an Advertise message with the IP address information and a DNS Recursive Name Server option.
  - The REF-Relay-Agent2 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing the Advertise message.
  - TAR-Relay-Agent1 transmitted the Advertise message to REF-Client1 with the IP address information and DNS Recursive Name Server option.
  - REF-Client1 transmitted a Request message to the ALL_DHCP_Relay_Agents_and_Servers address.
  - TAR-Relay-Agent1 transmitted a Relay-forward message containing the Request message from REF-Client1 to REF-Relay-Agent2.
  - REF-Relay-Agent2 transmitted a Relay-Forward message containing the Relay-Forward message from TAR-Relay-Agent1 to TAR-Server1.
  - TAR-Server1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing:

    - A Relay-Reply containing a Reply message with the confirmed IP address and a DNS Recursive Name Server option.
  - REF-Relay-Agent2 transmitted a Relay-Reply message containing a Reply message to TAR-Relay-Agent1.
  - TAR-Relay-Agent1 transmitted a Reply message to REF-Client1 that contains the confirmed address and a DNS Recursive Name Server option.

  Step 5: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

- *Part B*

  Step 8:

  - The REF-Client1 transmitted a solicit message on to the ALL_DHCP_Relay_Agents_and_Servers address.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Solicit message from REF-Client1.
  - REF-Relay-Agent2 transmitted a Relay-Forward message to the TAR-Server1 containing the Relay-Forward message from TAR-Relay-Agent1.
  - TAR-Server1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing:
    - A Relay-Reply containing an Advertise message with the IP address information and a Domain Search List option.
  - The REF-Relay-Agent2 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing the Advertise message.
  - TAR-Relay-Agent1 transmitted the Advertise message to REF-Client1 with the IP address information and Domain Search List option.
  - REF-Client1 transmitted a Request message to the ALL_DHCP_Relay_Agents_and_Servers address.
  - TAR-Relay-Agent1 transmitted a Relay-forward message containing the Request message from REF-Client1 to REF-Relay-Agent2.
  - REF-Relay-Agent2 transmitted a Relay-Forward message containing the Relay-Forward message from TAR-Relay-Agent1 to TAR-Server1.
  - TAR-Server1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing:
    - A Relay-Reply containing a Reply message with the confirmed IP address and a Domain Search List option.
  - REF-Relay-Agent2 transmitted a Relay-Reply message containing a Reply message to TAR-Relay-Agent1.
  - TAR-Relay-Agent1 transmitted a Reply message to REF-Client1 that contains the confirmed address and a Domain Search List option.

  Step 10: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

- *Part C*

  Step 13:

  - The REF-Client1 transmitted a solicit message on to the ALL_DHCP_Relay_Agents_and_Servers address.
  - REF-Relay-Agent2 transmitted a Relay-Forward message containing the Solicit message from REF-Client1.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message to the TAR-Server1 containing the Relay-Forward message from REF-Relay-Agent2.
  - TAR-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
    - A Relay-Reply containing an Advertise message with the IP address information and a DNS Recursive Name Server option.

- TAR-Relay-Agent1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing the Advertise message.
- REF-Relay-Agent2 transmitted the Advertise message to REF-Client1 containing IP address information and a DNS Recursive Name Server option.
- REF-Client1 transmitted a Request message to the ALL_DHCP_Relay_Agents_and_Servers address.
- REF-Relay-Agent2 transmitted a Relay-forward message containing the Request message from REF-Client1 to TAR-Relay-Agent1.
- TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Relay-Forward message from REF-Relay-Agent2 to TAR-Server1.
- TAR-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
  - A Relay-Reply containing a Reply message with the confirmed IP address and a DNS Recursive Name Server Option.
- TAR-Relay-Agent1 transmitted a Relay-Reply message containing a Reply message to REF-Relay-Agent2.
- TAR-Relay-Agent1 transmitted a Reply message to REF-Client1 that contains the confirmed address and a DNS Recursive Name Server option.

Step 15: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

- *Part D*

  Step 18:

  - The REF-Client1 transmitted a solicit message on to the ALL_DHCP_Relay_Agents_and_Servers address.
  - REF-Relay-Agent2 transmitted a Relay-Forward message containing the Solicit message from REF-Client1.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message to the TAR-Server1 containing the Relay-Forward message from REF-Relay-Agent2.
  - TAR-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
    - A Relay-Reply containing an Advertise message with the IP address information and a Domain Search List option.
  - TAR-Relay-Agent1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing the Advertise message.
  - REF-Relay-Agent2 transmitted the Advertise message to REF-Client1 containing IP address information and a Domain Search List option.
  - REF-Client1 transmitted a Request message to the ALL_DHCP_Relay_Agents_and_Servers address.
  - REF-Relay-Agent2 transmitted a Relay-forward message containing the Request message from REF-Client1 to TAR-Relay-Agent1.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Relay-Forward message from REF-Relay-Agent2 to TAR-Server1.
  - TAR-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
    - A Relay-Reply containing a Reply message with the confirmed IP address and a Domain Search List option.
  - TAR-Relay-Agent1 transmitted a Relay-Reply message containing a Reply message to REF-Relay-Agent2.
  - TAR-Relay-Agent1 transmitted a Reply message to REF-Client1 that contains the confirmed address and a Domain Search List option.

  Step 20: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

- *Part E*

  Step 23:

  - The REF-Client1 transmitted a solicit message on to the ALL_DHCP_Relay_Agents_and_Servers address.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Solicit message from REF-Client1.
  - TAR-Relay-Agent2 transmitted a Relay-Forward message to the REF-Server1 containing the Relay-Forward message from TAR-Relay-Agent1.
  - REF-Server1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing:
    - A Relay-Reply containing an Advertise message with the IP address information and a DNS Recursive Name Server option.
  - The TAR-Relay-Agent2 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing the Advertise message.
  - TAR-Relay-Agent1 transmitted the Advertise message to REF-Client1 with the IP address information and DNS Recursive Name Server option.
  - REF-Client1 transmitted a Request message to the ALL_DHCP_Relay_Agents_and_Servers address.
  - TAR-Relay-Agent1 transmitted a Relay-forward message containing the Request message from REF-Client1 to TAR-Relay-Agent2.
  - TAR-Relay-Agent2 transmitted a Relay-Forward message containing the Relay-Forward message from TAR-Relay-Agent1 to REF-Server1.
  - REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent2 containing:
    - A Relay-Reply containing a Reply message with the confirmed IP address and a DNS Recursive Name Server option.
  - TAR-Relay-Agent2 transmitted a Relay-Reply message containing a Reply message to TAR-Relay-Agent1.
  - TAR-Relay-Agent1 transmitted a Reply message to REF-Client1 that contains the confirmed address and a DNS Recursive Name Server option.

  Step 25: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

- *Part F*

  Step 28:

  - The REF-Client1 transmitted a solicit message on to the ALL_DHCP_Relay_Agents_and_Servers address.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Solicit message from REF-Client1.
  - TAR-Relay-Agent2 transmitted a Relay-Forward message to the REF-Server1 containing the Relay-Forward message from TAR-Relay-Agent1.
  - REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent2 containing:
    - A Relay-Reply containing an Advertise message with the IP address information and a Domain Search List option.
  - The TAR-Relay-Agent2 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing the Advertise message.
  - TAR-Relay-Agent1 transmitted the Advertise message to REF-Client1 with the IP address information and Domain Search List option.
  - REF-Client1 transmitted a Request message to the ALL_DHCP_Relay_Agents_and_Servers address.

- TAR-Relay-Agent1 transmitted a Relay-forward message containing the Request message from REF-Client1 to TAR-Relay-Agent2.
- TAR-Relay-Agent2 transmitted a Relay-Forward message containing the Relay-Forward message from TAR-Relay-Agent1 to REF-Server1.
- REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent2 containing:
  - A Relay-Reply containing a Reply message with the confirmed IP address and a Domain Search List option.
- TAR-Relay-Agent2 transmitted a Relay-Reply message containing a Reply message to TAR-Relay-Agent1.
- TAR-Relay-Agent1 transmitted a Reply message to REF-Client1 that contains the confirmed address and a Domain Search List option.

Step 30: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

- *Part G*

Step 33:

- The REF-Client1 transmitted a solicit message on to the ALL_DHCP_Relay_Agents_and_Servers address.
- TAR-Relay-Agent2 transmitted a Relay-Forward message containing the Solicit message from REF-Client1.
- TAR-Relay-Agent1 transmitted a Relay-Forward message to the REF-Server1 containing the Relay-Forward message from TAR-Relay-Agent2.
- REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
  - A Relay-Reply containing an Advertise message with the IP address information and a DNS Recursive Name Server option.
- TAR-Relay-Agent1 transmitted a Relay-Reply message to TAR-Relay-Agent2 containing the Advertise message.
- TAR-Relay-Agent2 transmitted the Advertise message to REF-Client1 containing IP address information and a DNS Recursive Name Server option.
- REF-Client1 transmitted a Request message to the ALL_DHCP_Relay_Agents_and_Servers address.
- TAR-Relay-Agent2 transmitted a Relay-forward message containing the Request message from REF-Client1 to TAR-Relay-Agent1.
- TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Relay-Forward message from TAR-Relay-Agent2 to REF-Server1.
- REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
  - A Relay-Reply containing a Reply message with the confirmed IP address and a DNS Recursive Name Server Option.
- TAR-Relay-Agent1 transmitted a Relay-Reply message containing a Reply message to TAR-Relay-Agent2.
- TAR-Relay-Agent1 transmitted a Reply message to REF-Client1 that contains the confirmed address and a DNS Recursive Name Server option.

Step 35: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

- *Part H*

Step 38:

- The REF-Client1 transmitted a solicit message on to the ALL_DHCP_Relay_Agents_and_Servers address.
- TAR-Relay-Agent2 transmitted a Relay-Forward message containing the Solicit message from REF-Client1.

- TAR-Relay-Agent1 transmitted a Relay-Forward message to the REF-Server1 containing the Relay-Forward message from TAR-Relay-Agent2.
- REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
  - A Relay-Reply containing an Advertise message with the IP address information and a Domain Search List option.
- TAR-Relay-Agent1 transmitted a Relay-Reply message to TAR-Relay-Agent2 containing the Advertise message.
- TAR-Relay-Agent2 transmitted the Advertise message to REF-Client1 containing IP address information and a Domain Search List option.
- REF-Client1 transmitted a Request message to the ALL_DHCP_Relay_Agents_and_Servers address.
- TAR-Relay-Agent2 transmitted a Relay-forward message containing the Request message from REF-Client1 to TAR-Relay-Agent1.
- TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Relay-Forward message from TAR-Relay-Agent2 to REF-Server1.
- REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
  - A Relay-Reply containing a Reply message with the confirmed IP address and a Domain Search List option.
- TAR-Relay-Agent1 transmitted a Relay-Reply message containing a Reply message to TAR-Relay-Agent2.
- TAR-Relay-Agent1 transmitted a Reply message to REF-Client1 that contains the confirmed address and a Domain Search List option.

Step 40: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

Possible Problems:

- In each part, if the NUT does not have the command that transmits an Echo Request, the NUT can use an alternate command that transmits a DNS Standard Query.
- If the NUT does not work without the appropriate Router Advertisement, a REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1.

Test DHCPInterop.2.4: Transmission of Renew Messages for DNS Configuration Options

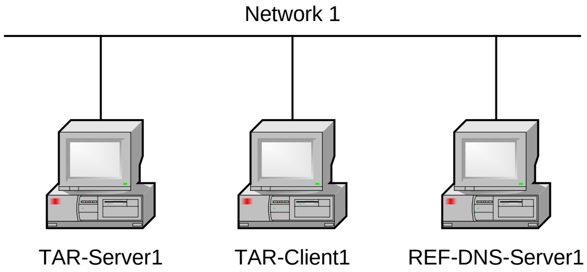
Purpose: To verify that a device can properly transmit a Renew message for DNS configuration options.

References:

- [3315] – Sections 18.1, 18.1.3 and 22.7
- [3646] – Section 3, 4

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Configure TAR-Server1 to set T1 to 50 seconds and T2 to 80 seconds. Initialize TAR-Server1, REF-DNS-Server1 and enable DHCPv6. Configure REF-DNS-Server1 to have a DNS host name of "dhcpv6" in the "test.example.com" domain. Disable DHCPv6 on all devices after each part.



Procedure:

Part A: Renew Message with Option Request Option (DNS Recursive Name Server Option)

1. Configure TAR-Server1 to include a DNS Recursive Name Server option that included REF-DNS-Server1's Global IPv6 address as the name server.
2. Configure TAR-Client1 to enable DHCPv6.
3. Allow enough time for the TAR-Client1 to receive IPv6 address information from the TAR-Server1.
4. Wait T1 seconds (50 seconds).
5. Observe the packets transmitted on Network 1.
6. Configure TAR-Client1 to transmit an Echo Request to "dhcpv6.test.example.com".
7. Observe the packets transmitted on Network 1.

Part B: Renew Message with Option Request Option (Domain Search List Option)

8. Configure TAR-Server1 to include a DNS Recursive Name Server option that includes REF-DNS-Server1's Global IPv6 address as the name server and a Domain Search List option that includes "test.example.com".
9. Configure TAR-Client1 to enable DHCPv6.
10. Allow enough time for the TAR-Client1 to receive IPv6 address information from the TAR-Server1.
11. Wait T1 seconds (50 seconds).

12. Observe the packets transmitted on Network 1.
13. Configure TAR-Client1 to transmit an Echo Request to “dhcpv6”.
14. Observe the packets transmitted on Network 1.

Observable Results:

- *Part A*

  Step 5: The TAR-Client1 transmits a properly formatted Renew message containing an IA_NA option and an Option Request option (DNS Recursive Name Server option). TAR-Server1 must send a Reply message to TAR-Client1 in response to the Renew message.

  Step 7: The TAR-Client received an Echo Reply from REF-DNS-Server1.
- *Part B*

  Step 10: The TAR-Client1 transmits a properly formatted Renew message containing an IA_NA option and an Option Request option (Domain Search List option). TAR-Server1 must send a Reply message to TAR-Client1 in response to the Renew message.

  Step 12: The TAR-Client received an Echo Reply from REF-DNS-Server1.

Possible Problems:

- If the NUT does not work without the appropriate Router Advertisement, a REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1.

Test DHCPInterop.2.5: Transmission of Rebind Messages for DNS Configuration Options

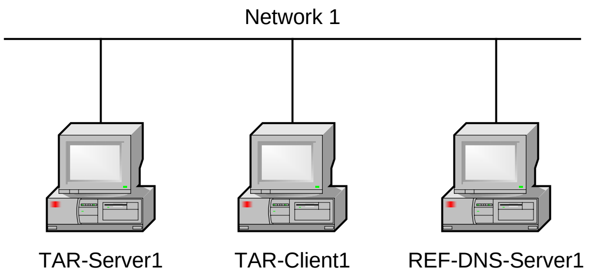
Purpose: To verify that a device can properly transmit a Rebind message for DNS configuration options.

References:

- [3315] – Sections 18.1, 18.1.4 and 22.7
- [3646] – Section 3, 4

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Configure TAR-Server1 to set T1 to 50 seconds and T2 to 80 seconds. Initialize TAR-Server1, REF-DNS-Server1 and enable DHCPv6. Configure REF-DNS-Server1 to have a DNS host name of "dhcpv6" in the "test.example.com" domain. Disable DHCPv6 on all devices after each part.



Procedure:

Part A: Renew Message with Option Request Option (DNS Recursive Name Server Option)

1. Configure TAR-Server1 to include a DNS Recursive Name Server option that includes REF-DNS-Server1's Global IPv6 address as the name server.
2. Configure TAR-Client1 to enable DHCPv6.
3. Allow enough time for the TAR-Client1 to receive IPv6 address information from the TAR-Server1.
4. Disconnect the TAR-Server1 from Network1.
5. Wait T2 seconds (80 seconds).
6. Reconnect the TAR-Server1 to Network1.
7. Observe the packets transmitted on Network 1.
8. Configure TAR-Client1 to transmit an Echo Request to "dhcpv6.test.example.com".
9. Observe the packets transmitted on Network 1.

Part B: Domain Search List Option

10. Configure TAR-Server1 to include a DNS Recursive Name Server option that includes REF-DNS-Server1's Global IPv6 address as the name server and a Domain Search List option that includes "test.example.com".
11. Configure TAR-Client1 to enable DHCPv6.

12. Allow enough time for the TAR-Client1 to receive IPv6 address information from the TAR-Server1.
13. Disconnect the TAR-Server1 from Network1.
14. Wait T2 seconds (80 seconds).
15. Reconnect the TAR-Server1 to Network1.
16. Observe the packets transmitted on Network 1.
17. Configure TAR-Client1 to transmit an Echo Request to “dhcpv6”.
18. Observe the packets transmitted on Network 1.

Observable Results:

- *Part A*

  Step 7: The TAR-Server1 transmits a properly formatted Reply message in response to TAR-Client1’s Rebind message.

  Step 9: The TAR-Client1 received an Echo Reply from REF-DNS-Server1
- *Part B*

  Step 16: The TAR-Server1 transmits a properly formatted Reply message in response to TAR-Client1’s Rebind message.

  Step 18: The TAR-Client1 received an Echo Reply from REF-DNS-Server1

Possible Problems:

- If the NUT does not work without the appropriate Router Advertisement, a REF-Router1 can be used to transmit a Router Advertisement with the appropriate parameters on Network1.

Group 3: RFC 3736

Scope

Tests in this group cover basic interoperability of the Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Request for Comments 3736.

Overview

These tests are designed to verify the readiness of DHCPv6 client and server interoperability vis-à-vis the specifications of the Stateless Dynamic Host Configuration Protocol for IPv6.

Test DHCPInterop.3.1: Stateless DHCPv6 Configuration Options exchange

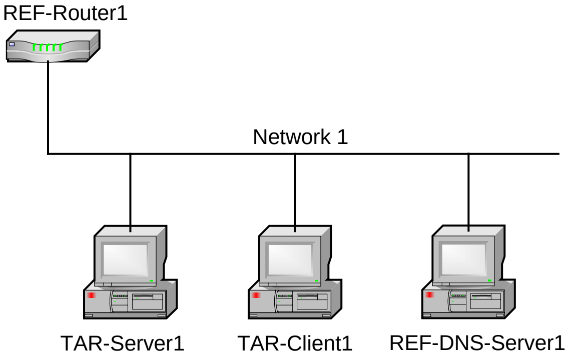
Purpose: To verify that a device can properly interoperate while performing the stateless DHCPv6 Configuration Options exchange.

References:

- [3315] – Section 1.3
- [3646] – Section 3, 4
- [3736] – Section 5.1, 5.2, 5.3

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-Server1 for stateless DHCPv6. Configure REF-Router1 to transmit Router Advertisements for Network 1's prefix with a preferred and valid lifetime of 600 seconds and the O bit set to 1, L and A bits are set to 1. Configure REF-DNS-Server1 to have a DNS host name of "dhcpv6" in the "test.example.com" domain. Disable DHCPv6 on all devices after each part.



Procedure:

Part A: DNS Recursive Name Server Option

1. Configure TAR-Server1 to include a DNS Recursive Name Server option that includes REF-DNS-Server1's Global IPv6 address as the name server.
2. Configure TAR-Client1 to enable stateless DHCPv6.
3. Configure TAR-Client1 to transmit an Echo Request to "dhcpv6.test.example.com".
4. Observe the packets transmitted on Network 1.

Part B: Domain Search List Option

5. Configure TAR-Server1 to include a DNS Recursive Name Server option that includes REF-DNS-Server1's Global IPv6 address as the name server and a Domain Search List option that includes "test.example.com".
6. Configure TAR-Client1 to enable stateless DHCPv6.
7. Configure TAR-Client1 to transmit an Echo Request to "dhcpv6".
8. Observe the packets transmitted on Network 1.

Observable Results:

- *Part A*

  Step 4: The TAR-Client1 received an Echo Reply from REF-DNS-Server1.
- *Part B*

  Step 8: The TAR-Client1 received an Echo Reply from REF-DNS-Server1.

Possible Problems:

- In each part, if the NUT does not have the command that transmits an Echo Request, the NUT can use an alternate command that transmits a DNS Standard Query.

Test DHCPInterop.3.2: Stateless DHCPv6 Relay Agent Basic Message Exchange with DNS Configuration Options

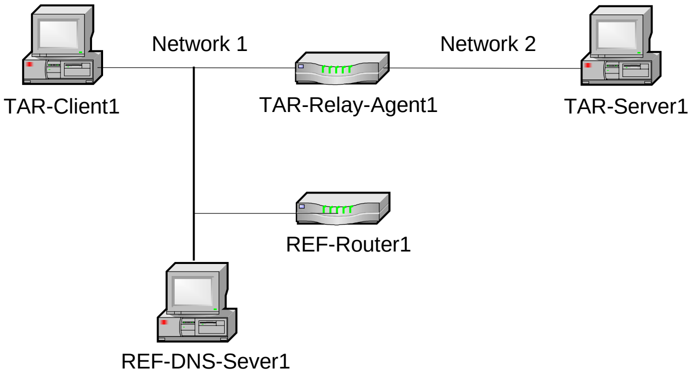
Purpose: To verify that a device can properly interoperate with a DHCPv6 Relay Agent while using DHCPv6 with DNS configuration options.

References:

- [3315] – Section 1.3
- [3315] – Section 20
- [3646] – Section 3, 4
- [3736] – Section 5.1, 5.2, 5.3

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Configure TAR-Server1 to perform Stateless DHCPv6. Configure REF-Router1 to transmit Router Advertisements that include a prefix for Network1 with the O bit set to 1 (L and A bits are 1). Initialize TAR-Server1, REF-DNS-Server1 and enable DHCPv6. Configure REF-DNS-Server1 to have a DNS host name of "dhcpv6" in the "test.example.com" domain. Disable DHCPv6 on all devices after each part. If the TAR Relay Agent supports or requires the use of an Interface-ID Option, it may be configured for this test. Since the use of the Interface ID is an ADVANCED functionality and is not mandatory, this test may be run without the Interface ID.



Procedure:

Part A: DNS Recursive Name Server Option

1. Configure TAR-Server1 to include a DNS Recursive Name Server option that includes REF-DNS-Server1's Global IPv6 address as the name server.
2. Configure TAR-Client1 to enable stateless DHCPv6 and stateless address auto-configuration.
3. Observe the packets on Network 1 and Network 2.
4. Configure TAR-Client1 to transmit an Echo Request to "dhcpv6.test.example.com".
5. Observe the packets transmitted on Network 1.

Part B: Domain Search List Option

6. Configure TAR-Server1 to include a DNS Recursive Name Server option that includes REF-DNS-Server1's Global IPv6 address as the name server and a Domain Search List option that includes "test.example.com".
7. Configure TAR-Client1 to enable stateless DHCPv6 and stateless address auto-configuration.
8. Observe the packets on Network 1 and Network 2.
9. Configure TAR-Client1 to transmit an Echo Request to "dhcpv6".
10. Observe the packets transmitted on Network 1.

Observable Results:

- *Part A*

  Step 3: The TAR-Client1 sends an information request message to the ALL_DHCP_Relay_Agents_and_Servers address. TAR-Relay-Agent1 transmits a Relay-forward Information Request message in relaying of the Information Request message from TAR-Client1. The TAR-Server1 sends a Relay-reply Reply message with the DNS Recursive Name Server option. TAR-Relay-Agent1 transmitted a Reply message in relaying of the Relay-reply Reply message containing the DNS Recursive Name Server option from TAR-Server1 to TAR-Client1 that contains the confirmed address.

  Step 5: The TAR-Client1 received an Echo Reply from REF-DNS-Server1.
- *Part B*

  Step 8: The TAR-Client1 sends an information request message to the ALL_DHCP_Relay_Agents_and_Servers address. TAR-Relay-Agent1 transmits a Relay-forward Information Request message in relaying of the Information Request message from TAR-Client1. The TAR-Server1 sends a Relay-reply Reply message with the Domain Search List option. TAR-Relay-Agent1 transmitted a Reply message in relaying of the Relay-reply Reply message containing the Domain Search List option from TAR-Server1 to TAR-Client1 that contains the confirmed address.

  Step 10: The TAR-Client1 received an Echo Reply from REF-DNS-Server1.

Possible Problems:

- In each part, if the NUT does not have the command that transmits an Echo Request, the NUT can use an alternate command that transmits a DNS Standard Query.

Test DHCPInterop.3.3: Layered Relay Agent Stateless DHCPv6 Basic Message Exchange with DNS Configuration Options

Purpose: To verify that a device can properly interoperate with multiple DHCPv6 Relay Agents while using Stateless DHCPv6 with DNS configuration options.

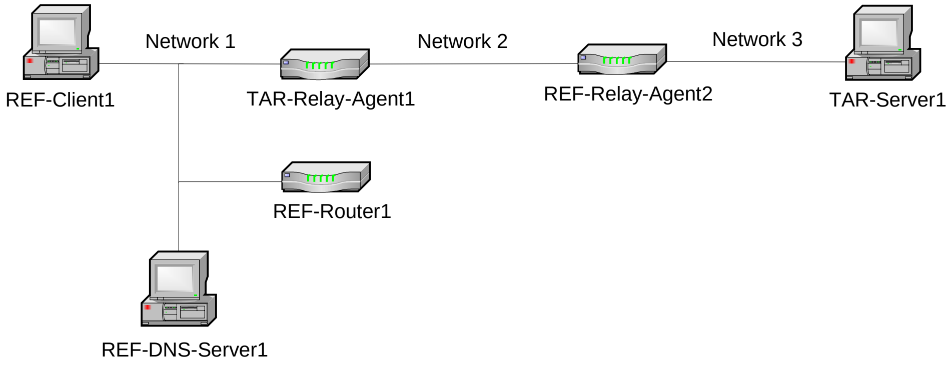
References:

- [3315] – Section 1.3
- [3315] – Section 20
- [3646] – Section 3, 4
- [3736] – Section 5.1, 5.2, 5.3

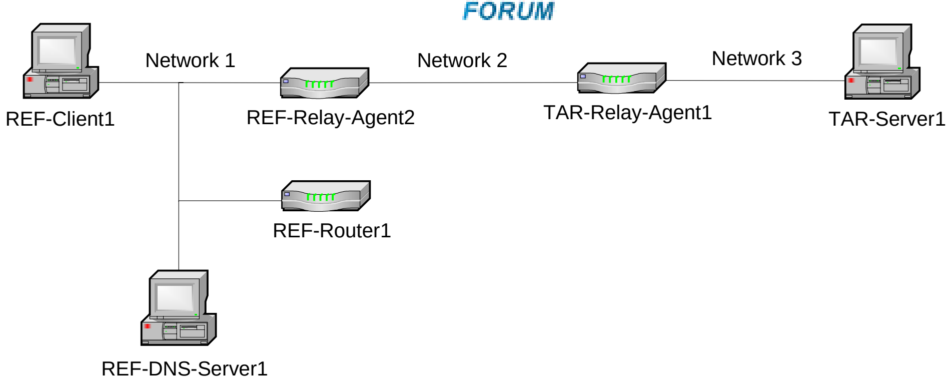
Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Configure TAR-Server1 to perform Stateless DHCPv6. Configure REF-Router1 to transmit Router Advertisements that include a prefix for Network1 with the O bit set to 1 (L and A bits are 1). Initialize TAR-Server1, REF-Client1, TAR-Relay-Agent1, TAR-Relay-Agent2, REF-Host1 and enable DHCPv6. Configure REF-DNS-Server1 to have a DNS host name of “dhcpv6” in the “test.example.com” domain. Disable DHCPv6 on all devices after each part.

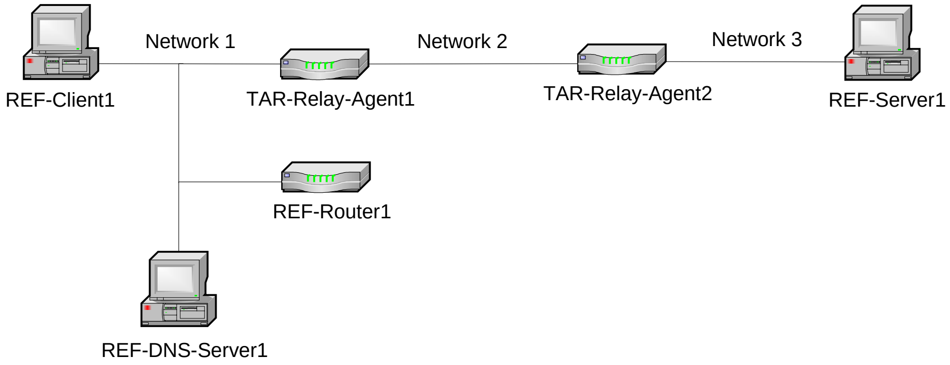
Part A-B:



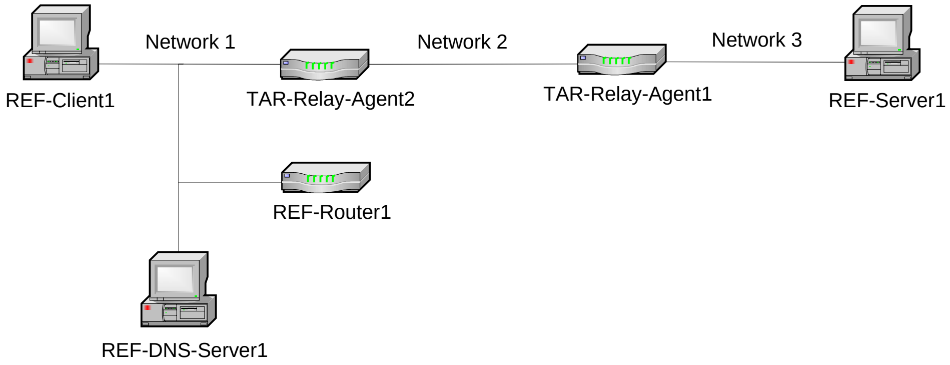
Part C-D:



Part E-F:



Part G-H:



Procedure:

Part A: DNS Recursive Name Server Option(Relay Agent to Server)

1. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1's Global IPv6 address included as the name server.
2. Configure REF-Client1 to enable stateless DHCPv6 and stateless address auto-configuration.
3. Observe the packets on Network 1, Network 2, and Network 3.
4. Configure REF-Client1 to transmit an Echo Request to "dhcpv6.test.example.com".
5. Observe the packets transmitted on Network 1.

Part B: Domain Search List Option(Relay Agent to Server)

6. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1’s Global IPv6 address included as the name server and a Domain Search List option that includes “test.example.com”.
7. Configure REF-Client1 to enable stateless DHCPv6 and stateless address auto-configuration.
8. Observe the packets on Network 1, Network 2, and Network 3.
9. Configure REF-Client1 to transmit an Echo Request to “dhcpv6”.
10. Observe the packets transmitted on Network 1.

Part C: DNS Recursive Name Server Option(Relay Agent to Server)

11. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1’s Global IPv6 address included as the name server.
12. Configure REF-Client1 to enable stateless DHCPv6 and stateless address auto-configuration.
13. Observe the packets on Network 1, Network 2, and Network 3.
14. Configure REF-Client1 to transmit an Echo Request to “dhcpv6.test.example.com”.
15. Observe the packets transmitted on Network 1.

Part D: Domain Search List Option(Relay Agent to Server)

16. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1’s Global IPv6 address included as the name server and a Domain Search List option that includes “test.example.com”.
17. Configure REF-Client1 to enable stateless DHCPv6 and stateless address auto-configuration.
18. Observe the packets on Network 1, Network 2, and Network 3.
19. Configure REF-Client1 to transmit an Echo Request to “dhcpv6”.
20. Observe the packets transmitted on Network 1.

Part E: DNS Recursive Name Server Option(Relay Agent to Relay Agent)

21. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1’s Global IPv6 address included as the name server.
22. Configure REF-Client1 to enable stateless DHCPv6 and stateless address auto-configuration.
23. Observe the packets on Network 1, Network 2, and Network 3.
24. Configure REF-Client1 to transmit an Echo Request to “dhcpv6.test.example.com”.
25. Observe the packets transmitted on Network 1.

Part F: Domain Search List Option(Relay Agent to Relay Agent)

26. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1’s Global IPv6 address included as the name server and a Domain Search List option that includes “test.example.com”.
27. Configure REF-Client1 to enable stateless DHCPv6 and stateless address auto-configuration.
28. Observe the packets on Network 1, Network 2, and Network 3.
29. Configure REF-Client1 to transmit an Echo Request to “dhcpv6”.
30. Observe the packets transmitted on Network 1.

Part G: DNS Recursive Name Server Option(Relay Agent to Relay Agent)

31. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1’s Global IPv6 address included as the name server.
32. Configure REF-Client1 to enable stateless DHCPv6 and stateless address auto-configuration.
33. Observe the packets on Network 1, Network 2, and Network 3.
34. Configure REF-Client1 to transmit an Echo Request to “dhcpv6.test.example.com”.
35. Observe the packets transmitted on Network 1.

Part H: Domain Search List Option(Relay Agent to Relay Agent)

36. Configure TAR-Server1 to include a DNS Recursive Name Server option with REF-DNS-Server1’s Global IPv6 address included as the name server and a Domain Search List option that includes “test.example.com”.

37. Configure REF-Client1 to enable stateless DHCPv6 and stateless address auto-configuration.
38. Observe the packets on Network 1, Network 2, and Network 3.
39. Configure REF-Client1 to transmit an Echo Request to "dhcpv6".
40. Observe the packets transmitted on Network 1.

Observable Results:

- *Part A*

  Step 3:
  - The REF-Client1 transmitted an Information-Request message on to the ALL_DHCP_Relay_Agents_and_Servers address.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Information Request message from REF-Client1.
  - REF-Relay-Agent2 transmitted a Relay-Forward message to the TAR-Server1 containing the Relay-Forward message from TAR-Relay-Agent1.
  - TAR-Server1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing:
    - A Relay-Reply containing a Reply message with a DNS Recursive Name Server option.
  - The REF-Relay-Agent2 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing the Reply message.
  - TAR-Relay-Agent1 transmitted the Reply message to REF-Client1 with the DNS Recursive Name Server option.

  Step 5: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.
- *Part B*

  Step 8:
  - The REF-Client1 transmitted an Information-Request message on to the ALL_DHCP_Relay_Agents_and_Servers address.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Information-Request message from REF-Client1.
  - REF-Relay-Agent2 transmitted a Relay-Forward message to the TAR-Server1 containing the Relay-Forward message from TAR-Relay-Agent1.
  - TAR-Server1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing:
    - A Relay-Reply containing a Reply message with a Domain Search List option.
  - The REF-Relay-Agent2 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing the Reply message.
  - TAR-Relay-Agent1 transmitted the Reply message to REF-Client1 with the Domain Search List option.

  Step 10: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.
- *Part C*

  Step 13:
  - The REF-Client1 transmitted an Information-Request message on to the ALL_DHCP_Relay_Agents_and_Servers address.
  - REF-Relay-Agent2 transmitted a Relay-Forward message containing the Information-Request message from REF-Client1.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message to the TAR-Server1 containing the Relay-Forward message from REF-Relay-Agent2.
  - TAR-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:

    - A Relay-Reply containing a Reply message with a DNS Recursive Name Server option.
  - TAR-Relay-Agent1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing the Reply message.
  - REF-Relay-Agent2 transmitted the Reply message to REF-Client1 containing a DNS Recursive Name Server option.

  Step 15: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

- *Part D*

  Step 18:

  - The REF-Client1 transmitted an Information-Request message on to the ALL_DHCP_Relay_Agents_and_Servers address.
  - REF-Relay-Agent2 transmitted a Relay-Forward message containing the Information-Request message from REF-Client1.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message to the TAR-Server1 containing the Relay-Forward message from REF-Relay-Agent2.
  - TAR-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
    - A Relay-Reply containing an Reply message with a Domain Search List option.
  - TAR-Relay-Agent1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing the Reply message.
  - REF-Relay-Agent2 transmitted the Reply message to REF-Client1 containing a Domain Search List option.

  Step 20: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

- *Part E*

  Step 23:

  - The REF-Client1 transmitted an Information-Request message on to the ALL_DHCP_Relay_Agents_and_Servers address.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Information-Request message from REF-Client1.
  - TAR-Relay-Agent2 transmitted a Relay-Forward message to the REF-Server1 containing the Relay-Forward message from TAR-Relay-Agent1.
  - REF-Server1 transmitted a Relay-Reply message to REF-Relay-Agent2 containing:
    - A Relay-Reply containing a Reply message with a DNS Recursive Name Server option.
  - The TAR-Relay-Agent2 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing the Reply message.
  - TAR-Relay-Agent1 transmitted the Reply message to REF-Client1 with the DNS Recursive Name Server option.

  Step 25: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

- *Part F*

  Step 28:

  - The REF-Client1 transmitted an Information-Request message on to the ALL_DHCP_Relay_Agents_and_Servers address.
  - TAR-Relay-Agent1 transmitted a Relay-Forward message containing the Information-Request message from REF-Client1.
  - TAR-Relay-Agent2 transmitted a Relay-Forward message to the REF-Server1 containing the Relay-Forward message from TAR-Relay-Agent1.
  - REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent2 containing:

- A Relay-Reply containing a Reply message with a Domain Search List option.
- The TAR-Relay-Agent2 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing the Reply message.
- TAR-Relay-Agent1 transmitted the Reply message to REF-Client1 with the Domain Search List option.

Step 30: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

- *Part G*

Step 33:

- The REF-Client1 transmitted an Information-Request message on to the ALL_DHCP_Relay_Agents_and_Servers address.
- TAR-Relay-Agent2 transmitted a Relay-Forward message containing the Information-Request message from REF-Client1.
- TAR-Relay-Agent1 transmitted a Relay-Forward message to the REF-Server1 containing the Relay-Forward message from TAR-Relay-Agent2.
- REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
  - A Relay-Reply containing a Reply message with a DNS Recursive Name Server option.
- TAR-Relay-Agent1 transmitted a Relay-Reply message to TAR-Relay-Agent2 containing the Reply message.
- TAR-Relay-Agent2 transmitted the Reply message to REF-Client1 containing a DNS Recursive Name Server option.

Step 35: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

- *Part H*

Step 38:

- The REF-Client1 transmitted a Information-Request message on to the ALL_DHCP_Relay_Agents_and_Servers address.
- TAR-Relay-Agent2 transmitted a Relay-Forward message containing the Information-Request message from REF-Client1.
- TAR-Relay-Agent1 transmitted a Relay-Forward message to the REF-Server1 containing the Relay-Forward message from TAR-Relay-Agent2.
- REF-Server1 transmitted a Relay-Reply message to TAR-Relay-Agent1 containing:
  - A Relay-Reply containing n Reply message with a Domain Search List option.
- TAR-Relay-Agent1 transmitted a Relay-Reply message to TAR-Relay-Agent2 containing the Reply message.
- TAR-Relay-Agent2 transmitted the Reply message to REF-Client1 containing a Domain Search List option.

Step 40: The REF-Client1 receives an Echo Reply from REF-DNS-Server1.

Possible Problems:

- In each part, if the NUT does not have the command that transmits an Echo Request, the NUT can use an alternate command that transmits a DNS Standard Query.

Group 4: RFC 3633

Scope

Tests in this group cover basic interoperability of the IPv6 Prefix Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6-PD), Request for Comments 3633.

Overview

These tests are designed to verify the readiness of DHCPv6 Requesting Router (Client) and Delegating Router (Server) interoperability vis-à-vis the specifications of the DHCPv6-PD protocol.

Test DHCPInterop.4.1: DHCPv6-PD Basic Message Exchange

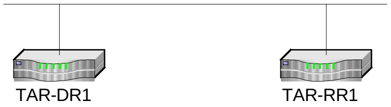
Purpose: To verify that a device can properly interoperate while using DHCPv6-PD

References:

- [3633] – Sections 7, 9 and 12

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-DR and enable DHCPv6. Disable DHCPv6 on all devices after test. Configure TAR-DR1 timer T1 to 50s and T2 to 80s. Disable DHCPv6 on all devices after test.



Procedure:

1. Configure TAR-RR1 to enable DHCPv6-PD
2. Observe the packets transmitted on Network 1.
3. Wait for timer T1 (50s) to expire.
4. Observe the packets transmitted on Network 1.

Observable Results:

Step 2: TAR-RR1 transmits a Solicit Message
TAR-DR1 transmits an Advertise Message to TAR-RR1.
TAR-RR1 transmits a Request Message
TAR-DR1 transmits a Reply Message to TAR-RR1.

Step 4: TAR-RR1 transmits a valid Renew Message with the same prefix as given in the Reply Message from Step 2.

Possible Problems:

- None

Test DHCPInterop.4.2: Requesting Router Initiated: Renew Message

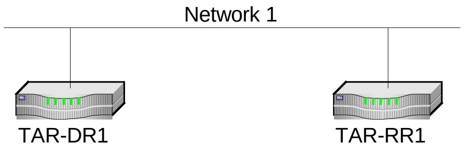
Purpose: To verify that a device can properly interoperate while using DHCPv6-PD

References:

- [3633] – Sections 7, 9 and 12

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-DR and enable DHCPv6. Disable DHCPv6 on all devices after test. Configure TAR-DR1 timer T1 to 50s and T2 to 80s. Disable DHCPv6 on all devices after test.



Procedure:

1. Configure TAR-RR1 to enable DHCPv6-PD
2. Observe the packets transmitted on Network 1.
3. TAR-RR1 should have received IPv6 prefix information from TAR-DR1. The TAR-DR1 assigns the T1 and T2 parameters to TAR-RR1's IA (TAR-DR1 sets T1 to 50s and T2 to 80s).
4. Wait for timer T1 (50s) to expire.
5. Observe the packets transmitted on Network 1.
6. Wait for timer T1 (50s) to expire.
7. Observe the packets transmitted

Observable Results:

Step 2: TAR-RR1 transmits a valid Solicit Message. TAR-DR1 transmits a valid Advertise Message. TAR-RR1 continues with a valid Request Message and TAR-DR1 transmits a valid Reply Message.

Step 5: TAR-RR1 transmits a valid Renew Message with the same prefix as given in the Reply Message from Step 2.

TAR-DR1 transmits a valid Reply Message with status of success.

Step 7: TAR-RR1 transmits a valid Renew Message with the same prefix as given in the Reply Message from Steps 2 and 5.

Possible Problems:

- None

Test DHCPInterop.4.3: Requesting Router Initiated: Rebind Message

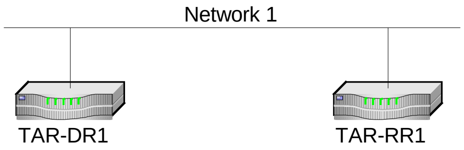
Purpose: To verify that a device can properly interoperate while using DHCPv6-PD

References:

- [3633] – Sections 7, 9 and 12

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-DR and enable DHCPv6. Disable DHCPv6 on all devices after test. Configure TAR-DR1 timer T1 to 50s and T2 to 80s. Disable DHCPv6 on all devices after test.



Procedure:

1. Configure TAR-RR1 to enable DHCPv6-PD
2. Observe the packets transmitted on Network 1.
3. TAR-RR1 should have received IPv6 prefix information from TAR-DR1. The TAR-DR1 assigns the T1 and T2 parameters to TAR-RR1's IA (TAR-DR1 sets T1 to 50s and T2 to 80s).
4. Disconnect TAR-DR1 from Network 1.
5. Wait for timer T2 (80s) to expire and re-enable TAR-DR1's interface on Network 1.
6. Observe the packets transmitted on Network 1.
7. Wait for timer T1 (50s) to expire.
8. Observe the packets transmitted on Network 1.

Observable Results:

Step 2: TAR-RR1 transmits a valid Solicit Message. TAR-DR1 transmits a valid Advertise Message. TAR-RR1 continues with a valid Request Message and TAR-DR1 transmits a valid Reply Message.

Step 6: TAR-RR1 transmits a valid Rebind Message with the same prefix as given in the Reply Message from Step 2.

Step 8: TAR-RR1 transmits a valid Renew Message with the same prefix as given in the Reply Message from Steps 2 and 6.

Possible Problems:

- None

Test DHCPInterop.4.4: Requesting Router Initiated: Release Message

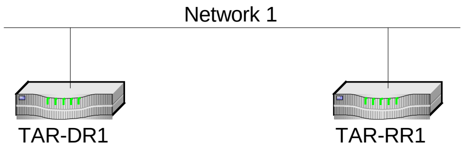
Purpose: To verify that a device can properly interoperate while using DHCPv6-PD

References:

- [3633] – Sections 7, 9 and 12

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-DR and enable DHCPv6. Disable DHCPv6 on all devices after test. Configure TAR-DR1 timer T1 to 50s and T2 to 80s. Disable DHCPv6 on all devices after test.



Procedure:

1. Configure TAR-RR1 to enable DHCPv6-PD
2. Observe the packets transmitted on Network 1.
3. TAR-RR1 should have received IPv6 prefix information from TAR-DR1. The TAR-DR1 assigns the T1 and T2 parameters to TAR-RR1's IA (TAR-DR1 sets T1 to 50s and T2 to 80s).
4. Configure TAR-RR1 to release the IPv6 Prefix.
5. Observe the packets transmitted on Network 1.
6. Wait for time T1 (50s) to expire.
7. Observe the packets transmitted on Network 1.

Observable Results:

Step 2: TAR-RR1 transmits a valid Solicit Message. TAR-DR1 transmits a valid Advertise Message. TAR-RR1 continues with a valid Request Message and TAR-DR1 transmits a valid Reply Message.

Step 5: TAR-RR1 transmits a valid Release Message with the same prefix as given in the Reply Message from Step 2.

TAR-DR1 transmits a valid Reply Message.

Step 7: TAR-RR1 does not transmit a Renew Message with the same prefix as Released in Step 5.

Possible Problems:

- None

Test DHCPInterop.4.5: Delegating Router Initiated: Advertise Message Status NoPrefixAvail

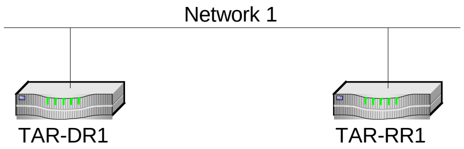
Purpose: To verify that a device can properly interoperate while using DHCPv6-PD

References:

- [3633] – Sections 7, 9 and 12

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-DR and enable DHCPv6. Disable DHCPv6 on all devices after test. Configure TAR-DR1 timer T1 to 50s and T2 to 80s. Disable DHCPv6 on all devices after test.



Procedure:

1. Configure TAR-DR1’s prefix pool to have no available prefixes.
2. Configure TAR-RR1 to enable DHCPv6-PD
3. Observe the packets transmitted on Network 1.

Observable Results:

Step 3: TAR-RR1 transmits a valid Solicit Message. TAR-DR1 transmits a valid Advertise Message. The Advertise Message contains a Status Code Option containing the value NoPrefixAvail (code 6). TAR-RR1 must not Transmit a Request Message.

Possible Problems:

- In Step 1, it may be impossible to configure the Delegating Router to have no available prefixes. In this case, a REF-Requesting Router may be used to drain the Target Delegating Router of available prefixes prior to continuing the test.

Group 5: RFC 3633 + RFC 3646

Scope

Tests in this group cover basic interoperability of the IPv6 Prefix Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6-PD), Request for Comments 3633, as it relates to DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3646.

Overview

These tests are designed to verify the readiness of DHCPv6 Requesting Router (Client) and Delegating Router (Server) interoperability vis-à-vis the specifications of the DHCPv6-PD protocol.

Test DHCPInterop.5.1: DHCPv6-PD Basic Message Exchange with DNS Options

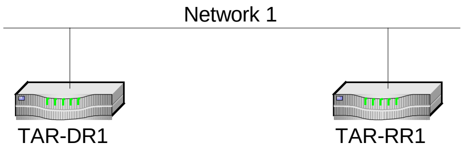
Purpose: To verify that a device can properly interoperate while using DHCPv6-PD

References:

- [3633] – Sections 7, 9 and 12
- [3646] – Sections 3, 4

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-DR and enable DHCPv6. Disable DHCPv6 on all devices after test. Configure TAR-DR1 timer T1 to 50s and T2 to 80s. Disable DHCPv6 on all devices after test.



Procedure:

Part A: DNS Recursive Name Server Option

1. Configure TAR-RR1 to enable DHCPv6-PD - configured to require a DNS Recursive Name Server option in parallel with DHCPv6-PD. Configure TAR-DR1 to provide a DNS Recursive Name Server.
2. Observe the packets transmitted on Network 1.
3. Wait for timer T1 (50s) to expire.
4. Observe the packets transmitted on Network 1.

Part B: Domain Search List Option

5. Configure TAR-RR1 to enable DHCPv6-PD - configured to require a DNS Recursive Name Server option, and Domain Search List option in parallel with DHCPv6-PD. Configure TAR-DR1 to provide a DNS Recursive Name Server as well as a Domain Search List.
6. Observe the packets transmitted on Network 1.
7. Wait for timer T1 (50s) to expire.
8. Observe the packets transmitted on Network 1.

Observable Results:

Part A

Step 2: TAR-RR1 transmits a valid, properly formatted Solicit Message, with the following:

- An Option Request Option for a DNS Recursive Name Server.

TAR-DR1 transmits a valid, properly formatted Advertise Message to TAR-RR1, with the following:

- A DNS Recursive Name Server Option with the configured address.

TAR-RR1 transmits a valid, properly formatted Request Message to TAR-DR1, with the following:

- An Option Request Option for a DNS Recursive Name Server.

TAR-DR1 Transmits a valid, properly formatted Reply Message to TAR-RR1, with the following:

- A DNS Recursive Name Server Option with the configured address.

Step 4: TAR-RR1 transmits a valid Renew Message with the same prefix as given in the Reply Message from Step 2. The Renew Message contains an Option-Request Option for a DNS Recursive Name Server.

Part B

Step 6: TAR-RR1 transmits a valid, properly formatted Solicit Message, with the following:

- An Option Request Option for a DNS Recursive Name Server.
- An Option Request Option for a Domain Search List

TAR-DR1 transmits a valid, properly formatted Advertise Message to TAR-RR1, with the following:

- A DNS Recursive Name Server Option with the configured address.
- A Domain Search List Option with the configured search list.

TAR-RR1 transmits a valid, properly formatted Request Message to TAR-DR1, with the following:

- An Option Request Option for a DNS Recursive Name Server.
- An Option Request Option for a Domain Search List

TAR-DR1 Transmits a valid, properly formatted Reply Message to TAR-RR1, with the following:

- A DNS Recursive Name Server Option with the configured address.
- A Domain Search List Option with the configured search list.

Step 8: TAR-RR1 transmits a valid Renew Message with the same prefix as given in the Reply Message from Step 6. The Renew Message contains an Option-Request Option for a DNS Recursive Name Server, as well as an Option-Request-Option for a Domain Search List.

Possible Problems:

- None

Test DHCPInterop.5.2: DHCPv6-PD Renew Message for DNS Configuration Options

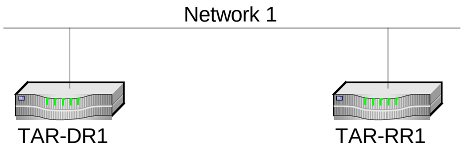
Purpose: To verify that a device can properly interoperate while using DHCPv6-PD

References:

- [3633] – Sections 7, 9 and 12
- [3646] – Sections 3, 4

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-DR and enable DHCPv6. Disable DHCPv6 on all devices after test. Configure TAR-DR1 timer T1 to 50s and T2 to 80s. Disable DHCPv6 on all devices after test.



Procedure:

Part A: DNS Recursive Name Server Option

1. Configure TAR-RR1 to enable DHCPv6-PD - configured to require a DNS Recursive Name Server option in parallel with DHCPv6-PD. Configure TAR-DR1 to provide a DNS Recursive Name Server.
2. Observe the packets transmitted on Network 1.
3. TAR-RR1 should have received IPv6 address information from TAR-DR1. The TAR-DR1 assigns the T1 and T2 parameters to TAR-RR1's IA (TAR-DR1 sets T1 to 50s and T2 to 80s).
4. Wait for timer T1 (50s) to expire.
5. Observe the packets transmitted on Network 1.
6. Wait for timer T1 (50s) to expire.
7. Observe the packets transmitted on Network 1.

Part B: Domain Search List Option

8. Configure TAR-RR1 to enable DHCPv6-PD - configured to require a DNS Recursive Name Server option, and Domain Search List option in parallel with DHCPv6-PD. Configure TAR-DR1 to provide a DNS Recursive Name Server as well as a Domain Search List.
9. Observe the packets transmitted on Network 1.
10. TAR-RR1 should have received IPv6 address information from TAR-DR1. The TAR-DR1 assigns the T1 and T2 parameters to TAR-RR1's IA (TAR-DR1 sets T1 to 50s and T2 to 80s).
11. Wait for timer T1 (50s) to expire.
12. Observe the packets transmitted on Network 1.
13. Wait for timer T1 (50s) to expire.
14. Observe the packets transmitted on Network 1.

Observable Results:

Part A

Step 2: TAR-RR1 transmits a valid Solicit Message with an ORO-DNS Recursive Name Server. TAR-DR1 transmits a valid Advertise Message with a Recursive Name Server Option. TAR-RR1 continues with a valid Request Message with an ORO-DNS Recursive Name Server. TAR-DR1 transmits a valid Reply Message with a DNS Recursive Name Server Option.

Step 5: TAR-RR1 transmits a valid Renew Message with the same prefix as given in the Reply Message from Step 2. The Renew Message has the following:

- An Option-Request Option for a DNS Recursive Name Server.

TAR-DR1 transmits a valid Reply Message with status of success. The Reply has a DNS Recursive Name Server Option.

Step 7: TAR-RR1 transmits a valid Renew Message with the same prefix as given in the Reply Message from Steps 2 and 5. The Renew message contains an ORO-DNS Recursive Name Server.

Part B

Step 9: TAR-RR1 transmits a valid Solicit Message with an ORO-DNS Recursive Name Server, as well as ORO-Domain Search List. TAR-DR1 transmits a valid Advertise Message with a Recursive Name Server Option and Domain Search List option as configured. TAR-RR1 continues with a valid Request Message with an ORO-DNS Recursive Name Server as well as ORO-Domain Search List. TAR-DR1 transmits a valid Reply Message with a DNS Recursive Name Server Option and Domain Search List option as configured.

Step 12: TAR-RR1 transmits a valid Renew Message with the same prefix as given in the Reply Message from Step 9. The Renew Message has the following:

- An Option-Request Option for a DNS Recursive Name Server.
- An Option-Request Option for a Domain Search List.

TAR-DR1 transmits a valid Reply Message with status of success. The Reply has a DNS Recursive Name Server Option as well as a Domain Search List option.

Step 14: TAR-RR1 transmits a valid Renew Message with the same prefix as given in the Reply Message from Steps 9 and 12. The Renew message contains an ORO-DNS Recursive Name Server as well as ORO-Domain Search List.

Possible Problems:

- None

Test DHCPInterop.5.3: DHCPv6-PD Rebind Message for DNS Configuration Options

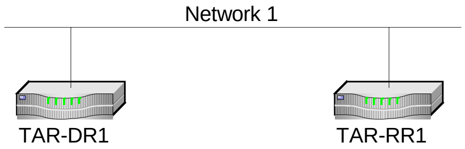
Purpose: To verify that a device can properly interoperate while using DHCPv6-PD

References:

- [3633] – Sections 7, 9 and 12
- [3646] – Sections 3, 4

Node Requirements:
See General Requirements.

Test Setup: For each part, connect the devices as per the figure below. Initialize TAR-DR and enable DHCPv6. Disable DHCPv6 on all devices after test. Configure TAR-DR1 timer T1 to 50s and T2 to 80s. Disable DHCPv6 on all devices after test.



Procedure:

Part A: DNS Recursive Name Server Option

1. Configure TAR-RR1 to enable DHCPv6-PD - configured to require a DNS Recursive Name Server option in parallel with DHCPv6-PD. Configure TAR-DR1 to provide a DNS Recursive Name Server.
2. Observe the packets transmitted on Network 1.
3. TAR-RR1 should have received IPv6 prefix information from TAR-DR1. The TAR-DR1 assigns the T1 and T2 parameters to TAR-RR1's IA (TAR-DR1 sets T1 to 50s and T2 to 80s).
4. Disconnect TAR-DR1 from Network 1.
5. Wait for timer T2 (80s) to expire and re-connect TAR-DR1's interface on Network 1.
6. Observe the packets transmitted on Network 1.
7. Wait for timer T1 (50s) to expire.
8. Observe the packets transmitted on Network 1.

Part B: Domain Search List Option

9. Configure TAR-RR1 to enable DHCPv6-PD - configured to require a DNS Recursive Name Server option, as well as a Domain Search List option in parallel with DHCPv6-PD. Configure TAR-DR1 to provide a DNS Recursive Name Server as well as a Domain Search List.
10. Observe the packets transmitted on Network 1.
11. TAR-RR1 should have received IPv6 prefix information from TAR-DR1. The TAR-DR1 assigns the T1 and T2 parameters to TAR-RR1's IA (TAR-DR1 sets T1 to 50s and T2 to 80s).
12. Disconnect TAR-DR1 from Network 1.
13. Wait for timer T2 (80s) to expire and re-connect TAR-DR1's interface on Network 1.
14. Observe the packets transmitted on Network 1.
15. Wait for timer T1 (50s) to expire.

16. Observe the packets transmitted on Network 1.

Observable Results:

Part A

Step 2: TAR-RR1 transmits a valid Solicit Message with an ORO-DNS Recursive Name Server. TAR-DR1 transmits a valid Advertise Message with a Recursive Name Server Option. TAR-RR1 continues with a valid Request Message with an ORO-DNS Recursive Name Server. TAR-DR1 transmits a valid Reply Message with a DNS Recursive Name Server Option.

Step 6: TAR-RR1 transmits a valid Rebind Message with the same prefix as given in the Reply Message from Step 2. The Rebind Message has the following:

- An Option-Request Option for a DNS Recursive Name Server.

TAR-DR1 transmits a valid Reply Message with status of success. The Reply has a DNS Recursive Name Server Option.

Step 8: TAR-RR1 transmits a valid Renew Message with the same prefix as given in the Reply Message from Steps 2 and 6. The Renew message contains an ORO-DNS Recursive Name Server.

Part B

Step 10: TAR-RR1 transmits a valid Solicit Message with an ORO-DNS Recursive Name Server, as well as ORO-Domain Search List. TAR-DR1 transmits a valid Advertise Message with a Recursive Name Server Option and Domain Search List option as configured. TAR-RR1 continues with a valid Request Message with an ORO-DNS Recursive Name Server as well as ORO-Domain Search List. TAR-DR1 transmits a valid Reply Message with a DNS Recursive Name Server Option and Domain Search List option as configured.

Step 14: TAR-RR1 transmits a valid Rebind Message with the same prefix as given in the Reply Message from Step 10. The Rebind Message has the following:

- An Option-Request Option for a DNS Recursive Name Server.
- An Option-Request Option for a Domain Search List.

TAR-DR1 transmits a valid Reply Message with status of success. The Reply has a DNS Recursive Name Server Option as well as a Domain Search List option.

Step 16: TAR-RR1 transmits a valid Renew Message with the same prefix as given in the Reply Message from Steps 10 and 14. The Renew message contains an ORO-DNS Recursive Name Server as well as ORO-Domain Search List.

Possible Problems:

- None

Appendix-A Required Data

When you apply for an IPv6 Ready Logo Phase-2 (DHCPv6) you need to submit test logs. In this appendix the detail requirement for the test log is described.

1.1 Required Data

As "IPv6 Ready Logo Phase-2" the following interoperability test result data are required.

A) Topology Map

Network topology figures or address list, with IPv6 addresses and MAC address of each attached interfaces, are required. Fig.1 is an example of topology figure.

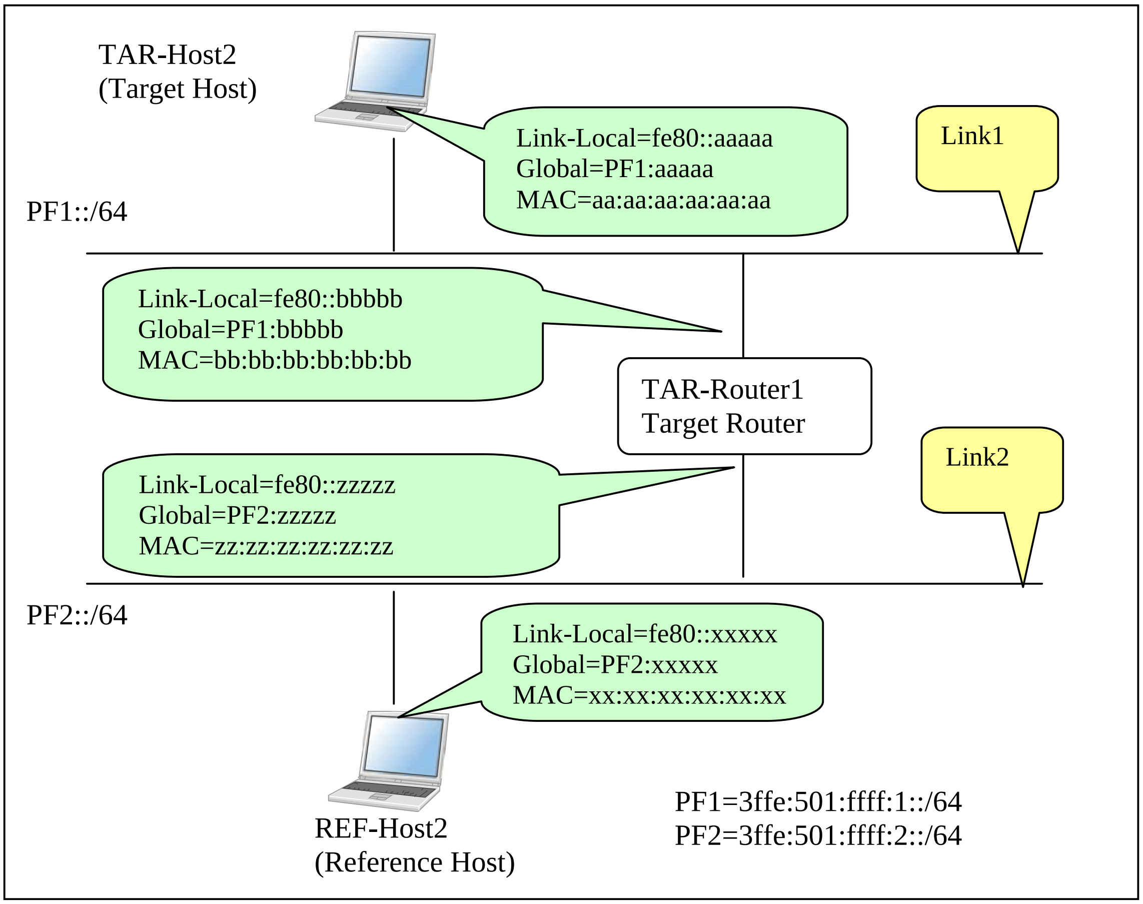


Fig. 1 Topology map example

Fig.2 is an example of address list.

```
TGT_HOST1:
        Link-Local=fe80::aaaa
        Global=PF1::aaaa
        MAC=aa:aa:aa:aa:aa:aa

REF_ROUTER1 [Link0]:
        Link-Local=fe80::bbbb
        Global=PF1::bbbb
        MAC=bb:bb:bb:bb:bb:bb

REF_ROUTER1 [Link1]:
        Link-Local=fe80::yyyy
        Global=PF2::yyyy
        MAC=yy:yy:yy:yy:yy:yy

TGT_HOST2:
        Link-Local=fe80::zzzz
        Global=PF2::zzzz
        MAC=zz:zz:zz:zz:zz:zz
```

Fig. 2 Address List example

B) Command Log

Ping is used as default application. When you run test with ping application, please save the command log into individual files. We allow using other protocol than ICMP Echo Request and Reply. Even though you use other kind of application, please save the command log. Save the command files for each test on each node.

C) Packet Capture File

Capture all packets on each link during the test with a device that is not part of the test. Make individual tcpdump(pcap) format file for each test and link or put the packet dump in a readable HTML file.

If you run tcpdump, please specify packet size as 4096.

e.g.,) tcpdump -i if0 -s 4096 –w 5.1.A.VendorA.Link0.dump

D) Test Result Table

Collect all test result tables in a file and fill the tables as required. This file must contain a table where all passes are clearly marked.

1.2. Data file name syntax

Please use following syntax in the file name.

A) Topology Map

Syntax:*Chapter.Section.ON.topology*

For "ON", use the Node’s vendor name which behaved as a client/server target Node(ON).
e.g.,)
If your device is a client, the name should be like following.
ON: Client [vendor: VendorA, model: rHost1, version: 1.0]
1.1.A.VendorA.topology.
If your device is a server, the name should be like following.
ON: Server [vendor: VendorB, model: rRouter1, version: 2.0]
1.1.A.VendorB.topology

B) Command Results

Chapter.Section.Part.SRC.DSTs.result

For "*SRC*", use the vendor name of the node on which the commands were run. If SRC is a REF Host, just specify REF-Host1 as SRC. For "*DSTs*", use the vendor name of the node to which the commands were run, in other words, destination of ping command.
e.g.,)
Typical Naming sample are hereafter.

1.1. DHCPv6 Initialization
1.1.REF.VendorA.result

1.2. Client Initiated: Transmission of Confirm messages
1.2.REF.VendorA.result

C) Captured packet file

Syntax:*Chapter.Section.Part.Target_Node,.Target_Node.Link.dump*

For "*Link*", use the captured link name.
For "*Target_Node*", use Vendor Name of Target Device. Vendor name for Client must be prior to the Vendor name of Server. Vendor name for Relay-Agent must be after to the Vendor name of the Client and Vendor name of Server.
e.g.,)

1.1. DHCPv6 Initialization

1.1.VendorA.VendorB.Network1.dump

1.2. Client Initiated: Transmission of Confirm messages

1.2.VendorA.VendorB.Network1.dump

D) Test Result Table

Syntax: *Device_name_and_version.table*

[If Client is applicant]

Client: VendorA

Server: VendorB, VendorC

Relay Agent: VendorD, VendorE

1.1 Client vs. Server

	VendorB	VendorC
VendorA		

1.2 Client vs. Server

	VendorB	VendorC
VendorA		

1.3 Client vs. Server

	VendorB	VendorC
VendorA		

1.4 Client vs. Server

	VendorB	VendorC
VendorA		

1.5 Client vs. Server

	VendorB	VendorC
VendorA		

1.6 Client vs. Server

	VendorB	VendorC
VendorA		

1.7 Client vs. Server

	VendorB	VendorC
VendorA		

1.8 Client vs. Server

	VendorB	VendorC
VendorA		

1.9 Part A Client vs. Server via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part B Client vs. Server via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part C Client vs. Server via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part D Client vs. Server via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part E Client vs. Server via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part F Client vs. Server via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

2.1 Part A Client vs. Server

	VendorB	VendorC
VendorA		

2.1 Part B Client vs. Server

	VendorB	VendorC
VendorA		

2.2 Part A Client vs. Server via Relay Agent

	VendorB+Vendor D	VendorC+VendorE
VendorA		

2.2 Part B Client vs. Server via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

2.5 Part A Client vs. Server

	VendorB	VendorC
VendorA		

2.5 Part B Client vs. Server

	VendorB	VendorC
VendorA		

2.6 Part A Client vs. Server

	VendorB	VendorC
VendorA		

2.6 Part B Client vs. Server

	VendorB	VendorC
VendorA		

3.1 Part A Client vs. Server

	VendorB	VendorC
VendorA		

3.1 Part B Client vs. Server

	VendorB	VendorC
VendorA		

3.2 Part A Client vs. Server via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

3.2 Part B Client vs. Server via Relay Agent (VendorD)

	VendorB+VendorD	VendorC+VendorE
VendorA		

[If Server is applicant]

Server: VendorA
Client: VendorB, VendorC
Relay Agent: VendorD, VendorE

1.1 Server vs. Client

	VendorB	VendorC
VendorA		

1.2 Server vs. Client

	VendorB	VendorC
VendorA		

1.3 Server vs. Client

	VendorB	VendorC
VendorA		

1.4 Server vs. Client

	VendorB	VendorC
VendorA		

1.5 Server vs. Client

	VendorB	VendorC
VendorA		

1.6 Server vs. Client

	VendorB	VendorC
VendorA		

1.7 Server vs. Client

	VendorB	VendorC
VendorA		

1.8 Server vs. Client

	VendorB	VendorC
VendorA		

1.9 Part A Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part B Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part C Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part D Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part E Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part F Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE

2.1 Part A Server vs. Client

	VendorB	VendorC
VendorA		

2.1 Part B Server vs. Client

	VendorB	VendorC
VendorA		

2.2 Part A Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

2.2 Part B Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

2.3 Part A Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

2.3 Part B Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

2.4 Part A Server vs. two Relay Agents

	VendorD	VendorE
VendorA		

2.4 Part B Server vs. two Relay Agents

	VendorD	VendorE
VendorA		

2.4 Part C Server vs. two Relay Agents

	VendorD	VendorE
VendorA		

2.4 Part D Server vs. two Relay Agents

	VendorD	VendorE
VendorA		

2.5 Part A Server vs. Client

	VendorB	VendorC
VendorA		

2.5 Part B Server vs. Client

	VendorB	VendorC
VendorA		

3.1 Part A Server vs. Client

	VendorB	VendorC
VendorA		

3.1 Part B Server vs. Client

	VendorB	VendorC
VendorA		

3.2 Part A Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE

VendorA		

3.2 Part B Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

3.3 Part A Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

3.3 Part B Server vs. Client via Relay Agent

	VendorB+VendorD	VendorC+VendorE
VendorA		

3.4 Part A Server vs. two Relay Agents

	VendorD	VendorE
VendorA		

3.4 Part B Server vs. two Relay Agents

	VendorD	VendorE
VendorA		

3.4 Part C Server vs. two Relay Agents

	VendorD	VendorE
VendorA		

3.4 Part D Server vs. two Relay Agents

	VendorD	VendorE
VendorA		

[If Relay Agent is applicant]
Relay Agent: VendorA (applicant)
Client: VendorB,VendorC
Server: VendorD, VendorE
Relay Agent: VendorF, VendorG
1.9 Part A Relay Agent vs. Server via Client

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part B Relay Agent vs. Server via Client

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part C Relay Agent vs. Server via Client

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part D Relay Agent vs. Server via Client

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part E Relay Agent vs. Server via Client

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.9 Part F Relay Agent vs. Server via Client

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.10 Part A Relay Agent vs. Server via Client

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.10 Part B Relay Agent vs. Server via Client

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.10 Part C Relay Agent vs. Server via Client

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.10 Part D Relay Agent vs. Server via Client

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.10 Part E Relay Agent vs. Server via Client

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.10 Part F Relay Agent vs. Server via Client

	VendorB+VendorD	VendorC+VendorE
VendorA		

1.11 Part A Relay Agent vs. Server via other Relay Agent

	VendorD	VendorE
VendorA		

1.11 Part B Relay Agent vs. Server via other Relay Agent

	VendorD	VendorE
VendorA		

1.11 Part C Relay Agent vs. Server via other Relay Agent

	VendorF	VendorG
VendorA		

1.11 Part D Relay Agent vs. Server via other Relay Agent

	VendorF	VendorG
VendorA		

2.2 Part A Relay Agent vs. Server via Client (VendorA)

	VendorB+VendorD	VendorC+VendorE
VendorA		

2.2 Part B Relay Agent vs. Server via Client (VendorA)

	VendorB+VendorD	VendorC+VendorE
VendorA		

2.3 Part A Relay Agent vs. Server via Client (VendorA)

	VendorB+VendorD	VendorC+VendorE
VendorA		

2.3 Part B Relay Agent vs. Server via Client (VendorA)

	VendorB+VendorD	VendorC+VendorE
VendorA		

2.4 Part A Relay Agent vs. Server via other Relay Agent

	VendorD	VendorE
VendorA		

2.4 Part B Relay Agent vs. Server via other Relay Agent

	VendorD	VendorE
VendorA		

2.4 Part C Relay Agent vs. Server via other Relay Agent

	VendorD	VendorE
VendorA		

2.4 Part D Relay Agent vs. Server via other Relay Agent

	VendorD	VendorE
VendorA		

2.4 Part E Relay Agent vs. Server via other Relay Agent

	VendorF	VendorG
VendorA		

2.4 Part F Relay Agent vs. Server via other Relay Agent

	VendorF	VendorG
VendorA		

2.4 Part G Relay Agent vs. Server via other Relay Agent

	VendorF	VendorG
VendorA		

2.4 Part H Relay Agent vs. Server via other Relay Agent

	VendorF	VendorG
VendorA		

3.2 Part A Relay Agent vs. Server via Client (VendorA)

	VendorB+VendorD	VendorC+VendorE
VendorA		

3.2 Part B Relay Agent vs. Server via Client (VendorA)

	VendorB+VendorD	VendorC+VendorE
VendorA		

3.3 Part A Relay Agent vs. Server via Client (VendorA)

	VendorB+VendorD	VendorC+VendorE
VendorA		

3.3 Part B Relay Agent vs. Server via Client (VendorA)

	VendorB+VendorD	VendorC+VendorE
VendorA		

Syntax: *Device_name_and_version.table*
[If Requesting Router (Client) is applicant]
Requesting Router: VendorA
Delegating Router: VendorB, VendorC
4.1 RR vs. DR

	VendorB	VendorC
VendorA		

4.2 RR vs. DR

	VendorB	VendorC
VendorA		

4.3 RR vs. DR

	VendorB	VendorC
VendorA		

4.4 RR vs. DR

	VendorB	VendorC
VendorA		

4.5 RR vs. DR

	VendorB	VendorC
VendorA		

5.1 RR vs. DR

	VendorB	VendorC
VendorA		

5.2 RR vs. DR

	VendorB	VendorC
VendorA		

5.3 RR vs. DR

	VendorB	VendorC
VendorA		

Syntax: *Device_name_and_version.table*
[If Delegating Router (Server) is applicant]
Delegating Router: VendorA
Requesting Router: VendorB, VendorC
4.1 DR vs. RR

	VendorB	VendorC
VendorA		

4.2 DR vs. RR

	VendorB	VendorC
VendorA		

4.3 DR vs. RR

	VendorB	VendorC
VendorA		

4.4 DR vs. RR

	VendorB	VendorC
VendorA		

4.5 DR vs. RR

	VendorB	VendorC
VendorA		

5.1 DR vs. RR

	VendorB	VendorC
VendorA		

5.2 DR vs. RR

	VendorB	VendorC
VendorA		

5.3 DR vs. RR

	VendorB	VendorC
VendorA		

1.3. Data Archive

Please organize your data as following directory structure.

```
$Your_Device_ver/
        Conformance/
        Interoperability /
```

Put all interoperability data file in "Interoperability" directory.
Put all Conformance Self-Test results or Conformance Lab test results in "Conformance" directory.
Make a tar.gz format archive file, and put files under "$Your_Device_ver" in it.

Files for NUT acting as Client

```
< Phase-2 DHCPv6>
Your device is a Client
TAR-Client1      : VendorX (Application)
TAR-Server1     : VendorA
             : VendorB
TAR-Relay-Agent1: VendorC
                : VendorD
/app_form_Phase2_DHCPv6.txt
/Conformance
  /DHCPv6_Self_Test_P2_1_0_X.tar
/Interoperability
  /Server.VendorA-Relay.VendorC
    /Results
      /1.1
          1.1.REF-Host1.VendorX.result
          1.1.VendorX.VendorA.Network1.dump
      /1.2
          1.2.REF-Host1.VendorX.result
          1.2.VendorX.VendorA.Network1.dump
      /1.3
          1.3.REF-Host1.VendorX.result
          1.3.VendorX.VendorA.Network1.dump
      /1.4
          1.4.REF-Host1.VendorX.result
          1.4.VendorX.VendorA.Network1.dump
      /1.5
          1.5.REF-Host1.VendorX.result
          1.5.VendorX.VendorA.Network1.dump
      /1.6
          1.6.VendorA.REF-Host1.result
          1.6.VendorX.VendorA.Network1.dump
      /1.7
          1.7.VendorX.VendorA.Network1.dump
      /1.8
          1.8.REF-Host1.VendorX.result
          1.8.VendorX.VendorA.Network1.dump
          1.8.VendorX.VendorA.Network2.dump
      /1.9.A
          1.9.A.REF-Host1.VendorX.result
          1.9.A.VendorX.VendorA.VendorC.Network1.dump
          1.9.A.VendorX.VendorA.VendorC.Network2.dump
      /1.9.B
          1.9.B.REF-Host1.VendorX.result
          1.9.B.VendorX.VendorA.VendorC.Network1.dump
          1.9.B.VendorX.VendorA.VendorC.Network2.dump
      /1.9.C
          1.9.C.REF-Host1.VendorX.result
          1.9.C.VendorX.VendorA.VendorC.Network1.dump
          1.9.C.VendorX.VendorA.VendorC.Network2.dump
      /1.9.D
          1.9.D.REF-Host1.VendorX.result
```

```
   1.9.D.VendorX.VendorA.VendorC.Network1.dump
   1.9.D.VendorX.VendorA.VendorC.Network2.dump
/1.9.E
   1.9.E.REF-Host1.VendorX.result
   1.9.E.VendorX.VendorA.VendorC.Network1.dump
   1.9.E.VendorX.VendorA.VendorC.Network2.dump
/1.9.F
   1.9.F.VendorA.REF-Host1.result
   1.9.F.VendorX.VendorA.VendorC.Network1.dump
   1.9.F.VendorX.VendorA.VendorC.Network2.dump
/1.10.A
   1.10.A.REF-Host1.VendorX.result
   1.10.A.VendorX.VendorA.VendorC.Network1.dump
   1.10.A.VendorX.VendorA.VendorC.Network2.dump
/1.10.B
   1.10.B.REF-Host1.VendorX.result
   1.10.B.VendorX.VendorA.VendorC.Network1.dump
   1.10.B.VendorX.VendorA.VendorC.Network2.dump
/1.10.C
   1.10.C.REF-Host1.VendorX.result
   1.10.C.VendorX.VendorA.VendorC.Network1.dump
   1.10.C.VendorX.VendorA.VendorC.Network2.dump
/1.10.D
   1.10.D.REF-Host1.VendorX.result
   1.10.D.VendorX.VendorA.VendorC.Network1.dump
   1.10.D.VendorX.VendorA.VendorC.Network2.dump
/1.10.E
   1.10.E.REF-Host1.VendorX.result
   1.10.E.VendorX.VendorA.VendorC.Network1.dump
   1.10.E.VendorX.VendorA.VendorC.Network2.dump
/1.10.F
   1.10.F.VendorA.REF-Host1.result
   1.10.F.VendorX.VendorA.VendorC.Network1.dump
   1.10.F.VendorX.VendorA.VendorC.Network2.dump
/2.1.A
   2.1.A.VendorX.REF-DNS-Server1.result
   2.1.A.VendorX.VendorA.Network1.dump
/2.1.B
   2.1.B.VendorX.REF-DNS-Server1.result
   2.1.B.VendorX.VendorA.Network1.dump
/2.2.A
   2.2.A.VendorX.REF-DNS-Server1.result
   2.2.A.VendorX.VendorA.VendorC.Network1.dump
   2.2.A.VendorX.VendorA.VendorC.Network2.dump
/2.2.B
   2.2.B.VendorX.REF-DNS-Server1.result
   2.2.B.VendorX.VendorA.VendorC.Network1.dump
   2.2.B.VendorX.VendorA.VendorC.Network2.dump
/2.3.A
   2.3.A.VendorX.REF-DNS-Server1.result
   2.3.A.VendorX.VendorA.VendorC.Network1.dump
   2.3.A.VendorX.VendorA.VendorC.Network2.dump
```

```
 /2.3.B
   2.3.B.VendorX.REF-DNS-Server1.result
   2.3.B.VendorX.VendorA.VendorC.Network1.dump
   2.3.B.VendorX.VendorA.VendorC.Network2.dump
 /2.5.A
   2.5.A.VendorX.REF-DNS-Server1.result
   2.5.A.VendorX.VendorA.Network1.dump
 /2.5.B
   2.5.B.VendorX.REF-DNS-Server1.result
   2.5.B.VendorX.VendorA.Network1.dump
 /2.6.A
   2.6.A.VendorX.REF-DNS-Server1.result
   2.6.A.VendorX.VendorA.Network1.dump
 /2.6.B
   2.6.B.VendorX.REF-DNS-Server1.result
   2.6.B.VendorX.VendorA.Network1.dump
 /3.1.A
   3.1.A.VendorX.REF-DNS-Server1.result
   3.1.A.VendorX.VendorA.Network1.dump
 /3.1.B
   3.1.B.VendorX.REF-DNS-Server1.result
   3.1.B.VendorX.VendorA.Network1.dump
 /3.2.A
   3.2.A.VendorX.REF-DNS-Server1.result
   3.2.A.VendorX.VendorA.VendorC.Network1.dump
   3.2.A.VendorX.VendorA.VendorC.Network2.dump
 /3.2.B
   3.2.B.VendorX.REF-DNS-Server1.result
   3.2.B.VendorX.VendorA.VendorC.Network1.dump
   3.2.B.VendorX.VendorA.VendorC.Network2.dump
 /3.3.A
   3.3.A.VendorX.REF-DNS-Server1.result
   3.3.A.VendorX.VendorA.VendorC.Network1.dump
   3.3.A.VendorX.VendorA.VendorC.Network2.dump
 /3.3.B
   3.3.B.VendorX.REF-DNS-Server1.result
   3.3.B.VendorX.VendorA.VendorC.Network1.dump
   3.3.B.VendorX.VendorA.VendorC.Network2.dump
/Topology
   1.1.VendorX.topology
   1.2.VendorX.topology
   1.3.VendorX.topology
   1.4.VendorX.topology
   1.5.VendorX.topology
   1.6.VendorX.topology
   1.7.VendorX.topology
   1.8.VendorX.topology
   1.9.A.VendorX.topology
   1.9.B.VendorX.topology
   1.9.C.VendorX.topology
   1.9.D.VendorX.topology
   1.9.E.VendorX.topology
```

```
      1.9.F.VendorX.topology
      1.10.A.VendorX.topology
      1.10.B.VendorX.topology
      1.10.C.VendorX.topology
      1.10.D.VendorX.topology
      1.10.E.VendorX.topology
      1.10.F.VendorX.topology
      2.1.A.VendorX.topology
      2.1.B.VendorX.topology
      2.2.A.VendorX.topology
      2.2.B.VendorX.topology
      2.3.A.VendorX.topology
      2.3.B.VendorX.topology
      2.5.A.VendorX.topology
      2.5.B.VendorX.topology
      2.6.A.VendorX.topology
      2.6.B.VendorX.topology
      3.1.A.VendorX.topology
      3.1.B.VendorX.topology
      3.2.A.VendorX.topology
      3.2.B.VendorX.topology
      3.3.A.VendorX.topology
      3.3.B.VendorX.topology
/Server.VendorB-Relay.VendorD
  /Results
    /1.1
      1.1.REF-Host1.VendorX.result
      1.1.VendorX.VendorB.Network1.dump
    /1.2
      1.2.REF-Host1.VendorX.result
      1.2.VendorX.VendorB.Network1.dump
    /1.3
      1.3.REF-Host1.VendorX.result
      1.3.VendorX.VendorB.Network1.dump
    /1.4
      1.4.REF-Host1.VendorX.result
      1.4.VendorX.VendorB.Network1.dump
    /1.5
      1.5.REF-Host1.VendorX.result
      1.5.VendorX.VendorB.Network1.dump
    /1.6
      1.6.VendorB.REF-Host1.result
      1.6.VendorX.VendorB.Network1.dump
    /1.7
      1.7.VendorX.VendorB.Network1.dump
    /1.8
      1.8.REF-Host1.VendorX.result
      1.8.VendorX.VendorB.Network1.dump
      1.8.VendorX.VendorB.Network2.dump
    /1.9.A
      1.9.A.REF-Host1.VendorX.result
      1.9.A.VendorX.VendorB.VendorD.Network1.dump
      1.9.A.VendorX.VendorB.VendorD.Network2.dump
    /1.9.B
      1.9.B.REF-Host1.VendorX.result
      1.9.B.VendorX.VendorB.VendorD.Network1.dump
      1.9.B.VendorX.VendorB.VendorD.Network2.dump
    /1.9.C
      1.9.C.REF-Host1.VendorX.result
      1.9.C.VendorX.VendorB.VendorD.Network1.dump
      1.9.C.VendorX.VendorB.VendorD.Network2.dump
    /1.9.D
      1.9.D.REF-Host1.VendorX.result
      1.9.D.VendorX.VendorB.VendorD.Network1.dump
      1.9.D.VendorX.VendorB.VendorD.Network2.dump
    /1.9.E
      1.9.E.REF-Host1.VendorX.result
      1.9.E.VendorX.VendorB.VendorD.Network1.dump
      1.9.E.VendorX.VendorB.VendorD.Network2.dump
    /1.9.F
      1.9.F.VendorA.REF-Host1.result
      1.9.F.VendorX.VendorB.VendorD.Network1.dump
      1.9.F.VendorX.VendorB.VendorD.Network2.dump
    /1.10.A
      1.10.A.REF-Host1.VendorX.result
      1.10.A.VendorX.VendorB.VendorD.Network1.dump
      1.10.A.VendorX.VendorB.VendorD.Network2.dump
    /1.10.B
      1.10.B.REF-Host1.VendorX.result
      1.10.B.VendorX.VendorB.VendorD.Network1.dump
      1.10.B.VendorX.VendorB.VendorD.Network2.dump
    /1.10.C
      1.10.C.REF-Host1.VendorX.result
      1.10.C.VendorX.VendorB.VendorD.Network1.dump
      1.10.C.VendorX.VendorB.VendorD.Network2.dump
    /1.10.D
      1.10.D.REF-Host1.VendorX.result
      1.10.D.VendorX.VendorB.VendorD.Network1.dump
      1.10.D.VendorX.VendorB.VendorD.Network2.dump
    /1.10.E
      1.10.E.REF-Host1.VendorX.result
      1.10.E.VendorX.VendorB.VendorD.Network1.dump
      1.10.E.VendorX.VendorB.VendorD.Network2.dump
    /1.10.F
      1.10.F.VendorA.REF-Host1.result
      1.10.F.VendorX.VendorB.VendorD.Network1.dump
      1.10.F.VendorX.VendorB.VendorD.Network2.dump
    /2.1.A
      2.1.A.VendorX.REF-DNS-Server1.result
      2.1.A.VendorX.VendorB.Network1.dump
    /2.1.B
      2.1.B.VendorX.REF-DNS-Server1.result
      2.1.B.VendorX.VendorB.Network1.dump
    /2.2.A
```

```
    2.2.A.VendorX.REF-DNS-Server1.result
    2.2.A.VendorX.VendorB.VendorD.Network1.dump
    2.2.A.VendorX.VendorB.VendorD.Network2.dump
  /2.2.B
    2.2.B.VendorX.REF-DNS-Server1.result
    2.2.B.VendorX.VendorB.VendorD.Network1.dump
    2.2.B.VendorX.VendorB.VendorD.Network2.dump
  /2.3.A
    2.3.A.VendorX.REF-DNS-Server1.result
    2.3.A.VendorX.VendorB.VendorD.Network1.dump
    2.3.A.VendorX.VendorB.VendorD.Network2.dump
  /2.3.B
    2.3.B.VendorX.REF-DNS-Server1.result
    2.3.B.VendorX.VendorB.VendorD.Network1.dump
    2.3.B.VendorX.VendorB.VendorD.Network2.dump
  /2.5.A
    2.5.A.VendorX.REF-DNS-Server1.result
    2.5.A.VendorX.VendorB.Network1.dump
  /2.5.B
    2.5.B.VendorX.REF-DNS-Server1.result
    2.5.B.VendorX.VendorB.Network1.dump
  /2.6.A
    2.6.A.VendorX.REF-DNS-Server1.result
    2.6.A.VendorX.VendorB.Network1.dump
  /2.6.B
    2.6.B.VendorX.REF-DNS-Server1.result
    2.6.B.VendorX.VendorB.Network1.dump
  /3.1.A
    3.1.A.VendorX.REF-DNS-Server1.result
    3.1.A.VendorX.VendorB.Network1.dump
  /3.1.B
    3.1.B.VendorX.REF-DNS-Server1.result
    3.1.B.VendorX.VendorB.Network1.dump
  /3.2.A
    3.2.A.VendorX.REF-DNS-Server1.result
    3.2.A.VendorX.VendorB.VendorD.Network1.dump
    3.2.A.VendorX.VendorB.VendorD.Network2.dump
  /3.2.B
    3.2.B.VendorX.REF-DNS-Server1.result
    3.2.B.VendorX.VendorB.VendorD.Network1.dump
    3.2.B.VendorX.VendorB.VendorD.Network2.dump
  /3.3.A
    3.3.A.VendorX.REF-DNS-Server1.result
    3.3.A.VendorX.VendorB.VendorD.Network1.dump
    3.3.A.VendorX.VendorB.VendorD.Network2.dump
  /3.3.B
    3.3.B.VendorX.REF-DNS-Server1.result
    3.3.B.VendorX.VendorB.VendorD.Network1.dump
    3.3.B.VendorX.VendorB.VendorD.Network2.dump
/Topology
    1.1.VendorX.topology
    1.2.VendorX.topology
    1.3.VendorX.topology
    1.4.VendorX.topology
    1.5.VendorX.topology
    1.6.VendorX.topology
    1.7.VendorX.topology
    1.8.VendorX.topology
    1.9.A.VendorX.topology
    1.9.B.VendorX.topology
    1.9.C.VendorX.topology
    1.9.D.VendorX.topology
    1.9.E.VendorX.topology
    1.9.F.VendorX.topology
    1.10.A.VendorX.topology
    1.10.B.VendorX.topology
    1.10.C.VendorX.topology
    1.10.D.VendorX.topology
    1.10.E.VendorX.topology
    1.10.F.VendorX.topology
    2.1.A.VendorX.topology
    2.1.B.VendorX.topology
    2.2.A.VendorX.topology
    2.2.B.VendorX.topology
    2.3.A.VendorX.topology
    2.3.B.VendorX.topology
    2.5.A.VendorX.topology
    2.5.B.VendorX.topology
    2.6.A.VendorX.topology
    2.6.B.VendorX.topology
    3.1.A.VendorX.topology
    3.1.B.VendorX.topology
    3.2.A.VendorX.topology
    3.2.B.VendorX.topology
    3.3.A.VendorX.topology
    3.3.B.VendorX.topology
/VendorX.table
```

Files for NUT acting as Server

< Phase-2 DHCPv6>
Your device is a Server.
TAR-Client1 : VendorA
: VendorB
TAR-Server1 : VendorX (Application)

TAR-Relay-Agent1: VendorC
: VendorD

```
/app_form_Phase2_DHCPv6.txt

/Conformance
  /DHCPv6_Self_Test_P2_1_0_X.tar

/Interoperability
  /Client.VendorA-Relay.VendorC
    /Results
      /1.1
          1.1.REF-Host1.VendorA.result
          1.1.VendorA.VendorX.Network1.dump
      /1.2
          1.2.REF-Host1.VendorA.result
          1.2.VendorA.VendorX.Network1.dump
      /1.3
          1.3.REF-Host1.VendorA.result
          1.3.VendorA.VendorX.Network1.dump
      /1.4
          1.4.REF-Host1.VendorA.result
          1.4.VendorA.VendorX.Network1.dump
      /1.5
          1.5.REF-Host1.VendorA.result
          1.5.VendorA.VendorX.Network1.dump
      /1.6
          1.6.VendorX.REF-Host1.result
          1.6.VendorA.VendorX.Network1.dump
      /1.7
          1.7.VendorA.VendorX.Network1.dump
      /1.8
          1.8.REF-Host1.VendorA.result
          1.8.VendorA.VendorX.Network1.dump
          1.8.VendorA.VendorX.Network2.dump
      /1.9.A
          1.9.A.REF-Host1.VendorA.result
          1.9.A.VendorA.VendorX.VendorC.Network1.dump
          1.9.A.VendorA.VendorX.VendorC.Network2.dump
      /1.9.B
          1.9.B.REF-Host1.VendorA.result
          1.9.B.VendorA.VendorX.VendorC.Network1.dump
          1.9.B.VendorA.VendorX.VendorC.Network2.dump
      /1.9.C
          1.9.C.REF-Host1.VendorA.result
```

```
   1.9.C.VendorA.VendorX.VendorC.Network1.dump
   1.9.C.VendorA.VendorX.VendorC.Network2.dump
/1.9.D
   1.9.D.REF-Host1.VendorA.result
   1.9.D.VendorA.VendorX.VendorC.Network1.dump
   1.9.D.VendorA.VendorX.VendorC.Network2.dump
/1.9.E
   1.9.E.REF-Host1.VendorA.result
   1.9.E.VendorA.VendorX.VendorC.Network1.dump
   1.9.E.VendorA.VendorX.VendorC.Network2.dump
/1.9.F
   1.9.F.VendorX.REF-Host1.result
   1.9.F.VendorA.VendorX.VendorC.Network1.dump
   1.9.F.VendorA.VendorX.VendorC.Network2.dump
/1.10.A
   1.10.A.REF-Host1.VendorA.result
   1.10.A.VendorA.VendorX.VendorC.Network1.dump
   1.10.A.VendorA.VendorX.VendorC.Network2.dump
/1.10.B
   1.10.B.REF-Host1.VendorA.result
   1.10.B.VendorA.VendorX.VendorC.Network1.dump
   1.10.B.VendorA.VendorX.VendorC.Network2.dump
/1.10.C
   1.10.C.REF-Host1.VendorA.result
   1.10.C.VendorA.VendorX.VendorC.Network1.dump
   1.10.C.VendorA.VendorX.VendorC.Network2.dump
/1.10.D
   1.10.D.REF-Host1.VendorA.result
   1.10.D.VendorA.VendorX.VendorC.Network1.dump
   1.10.D.VendorA.VendorX.VendorC.Network2.dump
/1.10.E
   1.10.E.REF-Host1.VendorA.result
   1.10.E.VendorA.VendorX.VendorC.Network1.dump
   1.10.E.VendorA.VendorX.VendorC.Network2.dump
/1.10.F
   1.10.F.VendorX.REF-Host1.result
   1.10.F.VendorA.VendorX.VendorC.Network1.dump
   1.10.F.VendorA.VendorX.VendorC.Network2.dump
/1.11.A
   1.11.A.REF-Host1.REF-Client1.result
   1.11.A.VendorX.VendorC.Network1.dump
   1.11.A.VendorX.VendorC.Network2.dump
   1.11.A.VendorX.VendorC.Network3.dump
/1.11.B
   1.11.B.REF-Host1.REF-Client1.result
   1.11.B.VendorX.VendorC.Network1.dump
   1.11.B.VendorX.VendorC.Network2.dump
   1.11.B.VendorX.VendorC.Network3.dump
/2.1.A
   2.1.A.VendorA.REF-DNS-Server1.result
   2.1.A.VendorA.VendorX.Network1.dump
/2.1.B
```

```
   2.1.B.VendorA.REF-DNS-Server1.result
   2.1.B.VendorA.VendorX.Network1.dump
/2.2.A
   2.2.A.VendorA.REF-DNS-Server1.result
   2.2.A.VendorA.VendorX.VendorC.Network1.dump
   2.2.A.VendorA.VendorX.VendorC.Network2.dump
/2.2.B
   2.2.B.VendorA.REF-DNS-Server1.result
   2.2.B.VendorA.VendorX.VendorC.Network1.dump
   2.2.B.VendorA.VendorX.VendorC.Network2.dump
/2.3.A
   2.3.A.VendorA.REF-DNS-Server1.result
   2.3.A.VendorA.VendorX.VendorC.Network1.dump
   2.3.A.VendorA.VendorX.VendorC.Network2.dump
/2.3.B
   2.3.B.VendorA.REF-DNS-Server1.result
   2.3.B.VendorA.VendorX.VendorC.Network1.dump
   2.3.B.VendorA.VendorX.VendorC.Network2.dump
/2.4.A
   2.4.A.REF-Client1.REF-DNS-Server1.result
   2.4.A.VendorX.VendorC.Network1.dump
   2.4.A.VendorX.VendorC.Network2.dump
   2.4.A.VendorX.VendorC.Network3.dump
/2.4.B
   2.4.B.REF-Client1.REF-DNS-Server1.result
   2.4.B.VendorX.VendorC.Network1.dump
   2.4.B.VendorX.VendorC.Network2.dump
   2.4.B.VendorX.VendorC.Network3.dump
/2.4.C
   2.4.C.REF-Client1.REF-DNS-Server1.result
   2.4.C.VendorX.VendorC.Network1.dump
   2.4.C.VendorX.VendorC.Network2.dump
   2.4.C.VendorX.VendorC.Network3.dump
/2.4.D
   2.4.D.REF-Client1.REF-DNS-Server1.result
   2.4.D.VendorX.VendorC.Network1.dump
   2.4.D.VendorX.VendorC.Network2.dump
   2.4.D.VendorX.VendorC.Network3.dump
/2.5.A
   2.5.A.VendorA.REF-DNS-Server1.result
   2.5.A.VendorA.VendorX.Network1.dump
/2.5.B
   2.5.B.VendorA.REF-DNS-Server1.result
   2.5.B.VendorA.VendorX.Network1.dump
/2.6.A
   2.6.A.VendorA.REF-DNS-Server1.result
   2.6.A.VendorA.VendorX.Network1.dump
/2.6.B
   2.6.B.VendorA.REF-DNS-Server1.result
   2.6.B.VendorA.VendorX.Network1.dump
/3.1.A
   3.1.A.VendorA.REF-DNS-Server1.result
   3.1.A.VendorA.VendorX.Network1.dump
 /3.1.B
   3.1.B.VendorA.REF-DNS-Server1.result
   3.1.B.VendorA.VendorX.Network1.dump
 /3.2.A
   3.2.A.VendorA.REF-DNS-Server1.result
   3.2.A.VendorA.VendorX.VendorC.Network1.dump
   3.2.A.VendorA.VendorX.VendorC.Network2.dump
 /3.2.B
   3.2.B.VendorA.REF-DNS-Server1.result
   3.2.B.VendorA.VendorX.VendorC.Network1.dump
   3.2.B.VendorA.VendorX.VendorC.Network2.dump
 /3.3.A
   3.3.A.VendorA.REF-DNS-Server1.result
   3.3.A.VendorA.VendorX.VendorC.Network1.dump
   3.3.A.VendorA.VendorX.VendorC.Network2.dump
 /3.3.B
   3.3.B.VendorA.REF-DNS-Server1.result
   3.3.B.VendorA.VendorX.VendorC.Network1.dump
   3.3.B.VendorA.VendorX.VendorC.Network2.dump
 /3.4.A
   3.4.A.REF-Client1.REF-DNS-Server1.result
   3.4.A.VendorX.VendorC.Network1.dump
   3.4.A.VendorX.VendorC.Network2.dump
   3.4.A.VendorX.VendorC.Network3.dump
 /3.4.B
   3.4.B.REF-Client1.REF-DNS-Server1.result
   3.4.B.VendorX.VendorC.Network1.dump
   3.4.B.VendorX.VendorC.Network2.dump
   3.4.B.VendorX.VendorC.Network3.dump
 /3.4.C
   3.4.C.REF-Client1.REF-DNS-Server1.result
   3.4.C.VendorX.VendorC.Network1.dump
   3.4.C.VendorX.VendorC.Network2.dump
   3.4.C.VendorX.VendorC.Network3.dump
 /3.4.D
   3.4.D.REF-Client1.REF-DNS-Server1.result
   3.4.D.VendorX.VendorC.Network1.dump
   3.4.D.VendorX.VendorC.Network2.dump
   3.4.D.VendorX.VendorC.Network3.dump
/Topology
   1.1.VendorX.topology
   1.2.VendorX.topology
   1.3.VendorX.topology
   1.4.VendorX.topology
   1.5.VendorX.topology
   1.6.VendorX.topology
   1.7.VendorX.topology
   1.8.VendorX.topology
   1.9.A.VendorX.topology
   1.9.B.VendorX.topology
   1.9.C.VendorX.topology
```

```
    1.9.D.VendorX.topology
    1.9.E.VendorX.topology
    1.9.F.VendorX.topology
    1.10.A.VendorX.topology
    1.10.B.VendorX.topology
    1.10.C.VendorX.topology
    1.10.D.VendorX.topology
    1.10.E.VendorX.topology
    1.10.F.VendorX.topology
    1.11.A.VendorX.topology
    1.11.B.VendorX.topology
    2.1.A.VendorX.topology
    2.1.B.VendorX.topology
    2.2.A.VendorX.topology
    2.2.B.VendorX.topology
    2.3.A.VendorX.topology
    2.3.B.VendorX.topology
    2.4.A.VendorX.topology
    2.4.B.VendorX.topology
    2.4.C.VendorX.topology
    2.4.D.VendorX.topology
    2.5.A.VendorX.topology
    2.5.B.VendorX.topology
    2.6.A.VendorX.topology
    2.6.B.VendorX.topology
    3.1.A.VendorX.topology
    3.1.B.VendorX.topology
    3.2.A.VendorX.topology
    3.2.B.VendorX.topology
    3.3.A.VendorX.topology
    3.3.B.VendorX.topology
    3.4.A.VendorX.topology
    3.4.B.VendorX.topology
    3.4.C.VendorX.topology
    3.4.D.VendorX.topology
/Client.VendorB-Relay.VendorD
 /Results
  /1.1
    1.1.REF-Host1.VendorB.result
    1.1.VendorB.VendorX.Network1.dump
  /1.2
    1.2.REF-Host1.VendorB.result
    1.2.VendorB.VendorX.Network1.dump
  /1.3
    1.3.REF-Host1.VendorB.result
    1.3.VendorB.VendorX.Network1.dump
  /1.4
    1.4.REF-Host1.VendorB.result
    1.4.VendorB.VendorX.Network1.dump
  /1.5
    1.5.REF-Host1.VendorB.result
    1.5.VendorB.VendorX.Network1.dump
```

```
/1.6
   1.6.VendorX.REF-Host1.result
   1.6.VendorB.VendorX.Network1.dump
/1.7
   1.7.VendorB.VendorX.Network1.dump
/1.8
   1.8.REF-Host1.VendorB.result
   1.8.VendorB.VendorX.Network1.dump
   1.8.VendorB.VendorX.Network2.dump
/1.9.A
   1.9.A.REF-Host1.VendorB.result
   1.9.A.VendorB.VendorX.VendorD.Network1.dump
   1.9.A.VendorB.VendorX.VendorD.Network2.dump
/1.9.B
   1.9.B.REF-Host1.VendorB.result
   1.9.B.VendorB.VendorX.VendorD.Network1.dump
   1.9.B.VendorB.VendorX.VendorD.Network2.dump
/1.9.C
   1.9.C.REF-Host1.VendorB.result
   1.9.C.VendorB.VendorX.VendorD.Network1.dump
   1.9.C.VendorB.VendorX.VendorD.Network2.dump
/1.9.D
   1.9.D.REF-Host1.VendorB.result
   1.9.D.VendorB.VendorX.VendorD.Network1.dump
   1.9.D.VendorB.VendorX.VendorD.Network2.dump
/1.9.E
   1.9.E.REF-Host1.VendorB.result
   1.9.E.VendorB.VendorX.VendorD.Network1.dump
   1.9.E.VendorB.VendorX.VendorD.Network2.dump
/1.9.F
   1.9.F.VendorX.REF-Host1.result
   1.9.F.VendorB.VendorX.VendorD.Network1.dump
   1.9.F.VendorB.VendorX.VendorD.Network2.dump
/1.10.A
   1.10.A.REF-Host1.VendorB.result
   1.10.A.VendorB.VendorX.VendorD.Network1.dump
   1.10.A.VendorB.VendorX.VendorD.Network2.dump
/1.10.B
   1.10.B.REF-Host1.VendorB.result
   1.10.B.VendorB.VendorX.VendorD.Network1.dump
   1.10.B.VendorB.VendorX.VendorD.Network2.dump
/1.10.C
   1.10.C.REF-Host1.VendorB.result
   1.10.C.VendorB.VendorX.VendorD.Network1.dump
   1.10.C.VendorB.VendorX.VendorD.Network2.dump
/1.10.D
   1.10.D.REF-Host1.VendorB.result
   1.10.D.VendorB.VendorX.VendorD.Network1.dump
   1.10.D.VendorB.VendorX.VendorD.Network2.dump
/1.10.E
   1.10.E.REF-Host1.VendorB.result
   1.10.E.VendorB.VendorX.VendorD.Network1.dump
   1.10.E.VendorB.VendorX.VendorD.Network2.dump
/1.10.F
   1.10.F.VendorX.REF-Host1.result
   1.10.F.VendorB.VendorX.VendorD.Network1.dump
   1.10.F.VendorB.VendorX.VendorD.Network2.dump
/1.11.A
   1.11.A.REF-Host1.REF-Client1.result
   1.11.A.VendorX.VendorD.Network1.dump
   1.11.A.VendorX.VendorD.Network2.dump
   1.11.A.VendorX.VendorD.Network3.dump
/1.11.B
   1.11.B.REF-Host1.REF-Client1.result
   1.11.B.VendorX.VendorD.Network1.dump
   1.11.B.VendorX.VendorD.Network2.dump
   1.11.B.VendorX.VendorD.Network3.dump
/2.1.A
   2.1.A.VendorB.REF-DNS-Server1.result
   2.1.A.VendorB.VendorX.Network1.dump
/2.1.B
   2.1.B.VendorB.REF-DNS-Server1.result
   2.1.B.VendorB.VendorX.Network1.dump
/2.2.A
   2.2.A.VendorB.REF-DNS-Server1.result
   2.2.A.VendorB.VendorX.VendorD.Network1.dump
   2.2.A.VendorB.VendorX.VendorD.Network2.dump
/2.2.B
   2.2.B.VendorB.REF-DNS-Server1.result
   2.2.B.VendorB.VendorX.VendorD.Network1.dump
   2.2.B.VendorB.VendorX.VendorD.Network2.dump
/2.3.A
   2.3.A.VendorB.REF-DNS-Server1.result
   2.3.A.VendorB.VendorX.VendorD.Network1.dump
   2.3.A.VendorB.VendorX.VendorD.Network2.dump
/2.3.B
   2.3.B.VendorB.REF-DNS-Server1.result
   2.3.B.VendorB.VendorX.VendorD.Network1.dump
   2.3.B.VendorB.VendorX.VendorD.Network2.dump
/2.4.A
   2.4.A.REF-Client1.REF-DNS-Server1.result
   2.4.A.VendorX.VendorD.Network1.dump
   2.4.A.VendorX.VendorD.Network2.dump
   2.4.A.VendorX.VendorD.Network3.dump
/2.4.B
   2.4.B.REF-Client1.REF-DNS-Server1.result
   2.4.B.VendorX.VendorD.Network1.dump
   2.4.B.VendorX.VendorD.Network2.dump
   2.4.B.VendorX.VendorD.Network3.dump
/2.4.C
   2.4.C.REF-Client1.REF-DNS-Server1.result
   2.4.C.VendorX.VendorD.Network1.dump
   2.4.C.VendorX.VendorD.Network2.dump
   2.4.C.VendorX.VendorD.Network3.dump
```

```
/2.4.D
   2.4.D.REF-Client1.REF-DNS-Server1.result
   2.4.D.VendorX.VendorD.Network1.dump
   2.4.D.VendorX.VendorD.Network2.dump
   2.4.D.VendorX.VendorD.Network3.dump
/2.5.A
   2.5.A.VendorA.REF-DNS-Server1.result
   2.5.A.VendorA.VendorX.Network1.dump
/2.5.B
   2.5.B.VendorA.REF-DNS-Server1.result
   2.5.B.VendorA.VendorX.Network1.dump
/2.6.A
   2.6.A.VendorA.REF-DNS-Server1.result
   2.6.A.VendorA.VendorX.Network1.dump
/2.6.B
   2.6.B.VendorA.REF-DNS-Server1.result
   2.6.B.VendorA.VendorX.Network1.dump
/3.1.A
   3.1.A.VendorB.REF-DNS-Server1.result
   3.1.A.VendorB.VendorX.Network1.dump
/3.1.B
   3.1.B.VendorB.REF-DNS-Server1.result
   3.1.B.VendorB.VendorX.Network1.dump
/3.2.A
   3.2.A.VendorB.REF-DNS-Server1.result
   3.2.A.VendorB.VendorX.VendorD.Network1.dump
   3.2.A.VendorB.VendorX.VendorD.Network2.dump
/3.2.B
   3.2.B.VendorB.REF-DNS-Server1.result
   3.2.B.VendorB.VendorX.VendorD.Network1.dump
   3.2.B.VendorB.VendorX.VendorD.Network2.dump
/3.3.A
   3.3.A.VendorB.REF-DNS-Server1.result
   3.3.A.VendorB.VendorX.VendorD.Network1.dump
   3.3.A.VendorB.VendorX.VendorD.Network2.dump
/3.3.B
   3.3.B.VendorB.REF-DNS-Server1.result
   3.3.B.VendorB.VendorX.VendorD.Network1.dump
   3.3.B.VendorB.VendorX.VendorD.Network2.dump

/3.4.A
   3.4.A.REF-Client1.REF-DNS-Server1.result
   3.4.A.VendorX.VendorD.Network1.dump
   3.4.A.VendorX.VendorD.Network2.dump
   3.4.A.VendorX.VendorD.Network3.dump
/3.4.B
   3.4.B.REF-Client1.REF-DNS-Server1.result
   3.4.B.VendorX.VendorD.Network1.dump
   3.4.B.VendorX.VendorD.Network2.dump
   3.4.B.VendorX.VendorD.Network3.dump
/3.4.C
   3.4.C.REF-Client1.REF-DNS-Server1.result
```

```
      3.4.C.VendorX.VendorD.Network1.dump
      3.4.C.VendorX.VendorD.Network2.dump
      3.4.C.VendorX.VendorD.Network3.dump
  /3.4.D
      3.4.D.REF-Client1.REF-DNS-Server1.result
      3.4.D.VendorX.VendorD.Network1.dump
      3.4.D.VendorX.VendorD.Network2.dump
      3.4.D.VendorX.VendorD.Network3.dump
/Topology
      1.1.VendorX.topology
      1.2.VendorX.topology
      1.3.VendorX.topology
      1.4.VendorX.topology
      1.5.VendorX.topology
      1.6.VendorX.topology
      1.7.VendorX.topology
      1.8.VendorX.topology
      1.9.A.VendorX.topology
      1.9.B.VendorX.topology
      1.9.C.VendorX.topology
      1.9.D.VendorX.topology
      1.9.E.VendorX.topology
      1.9.F.VendorX.topology
      1.10.A.VendorX.topology
      1.10.B.VendorX.topology
      1.10.C.VendorX.topology
      1.10.D.VendorX.topology
      1.10.E.VendorX.topology
      1.10.F.VendorX.topology
      1.11.A.VendorX.topology
      1.11.B.VendorX.topology
      2.1.A.VendorX.topology
      2.1.B.VendorX.topology
      2.2.A.VendorX.topology
      2.2.B.VendorX.topology
      2.3.A.VendorX.topology
      2.3.B.VendorX.topology
      2.4.A.VendorX.topology
      2.4.B.VendorX.topology
      2.4.C.VendorX.topology
      2.4.D.VendorX.topology
      2.5.A.VendorX.topology
      2.5.B.VendorX.topology
      2.6.A.VendorX.topology
      2.6.B.VendorX.topology
      3.1.A.VendorX.topology
      3.1.B.VendorX.topology
      3.2.A.VendorX.topology
      3.2.B.VendorX.topology
      3.3.A.VendorX.topology
      3.3.B.VendorX.topology
      3.4.A.VendorX.topology
```

3.4.B.VendorX.topology
3.4.C.VendorX.topology
3.4.D.VendorX.topology
/VendorX.table

Files for NUT acting as Relay Agent

```
< Phase-2 DHCPv6>
Your device is a Relay Agent.
TAR-Client1     : VendorA
                : VendorB
TAR-Server1     : VendorC
                : VendorD
TAR-Relay-Agent1: VendorE
                  VendorF
                  VendorX (Application)

/app_form_Phase2_DHCPv6.txt

/Conformance
  /DHCPv6_Self_Test_P2_1_0_X.tar

/Interoperability
  /Client.VendorA-Server.VendorC-Relay.VendorE
    /Results
      /1.9.A
          1.9.A.REF-Host1.VendorA.result
          1.9.A.VendorA.VendorC.VendorX.Network1.dump
          1.9.A.VendorA.VendorC.VendorX.Network2.dump
      /1.9.B
          1.9.B.REF-Host1.VendorA.result
          1.9.B.VendorA.VendorC.VendorX.Network1.dump
          1.9.B.VendorA.VendorC.VendorX.Network2.dump
      /1.9.C
          1.9.C.REF-Host1.VendorA.result
          1.9.C.VendorA.VendorC.VendorX.Network1.dump
          1.9.C.VendorA.VendorC.VendorX.Network2.dump
      /1.9.D
          1.9.D.REF-Host1.VendorA.result
          1.9.D.VendorA.VendorC.VendorX.Network1.dump
          1.9.D.VendorA.VendorC.VendorX.Network2.dump
      /1.9.E
          1.9.E.REF-Host1.VendorA.result
          1.9.E.VendorA.VendorC.VendorX.Network1.dump
          1.9.E.VendorA.VendorC.VendorX.Network2.dump
      /1.9.F
          1.9.F.VendorX.REF-Host1.result
          1.9.F.VendorA.VendorC.VendorX.Network1.dump
          1.9.F.VendorA.VendorC.VendorX.Network2.dump
      /1.10.A
          1.10.A.REF-Host1.VendorA.result
          1.10.A.VendorA.VendorC.VendorX.Network1.dump
          1.10.A.VendorA.VendorC.VendorX.Network2.dump
      /1.10.B
          1.10.B.REF-Host1.VendorA.result
          1.10.B.VendorA.VendorC.VendorX.Network1.dump
          1.10.B.VendorA.VendorC.VendorX.Network2.dump
```

```
/1.10.C
   1.10.C.REF-Host1.VendorA.result
   1.10.C.VendorA.VendorC.VendorX.Network1.dump
   1.10.C.VendorA.VendorC.VendorX.Network2.dump
/1.10.D
   1.10.D.REF-Host1.VendorA.result
   1.10.D.VendorA.VendorC.VendorX.Network1.dump
   1.10.D.VendorA.VendorC.VendorX.Network2.dump
/1.10.E
   1.10.E.REF-Host1.VendorA.result
   1.10.E.VendorA.VendorC.VendorX.Network1.dump
   1.10.E.VendorA.VendorC.VendorX.Network2.dump
/1.10.F
   1.10.F.VendorX.REF-Host1.result
   1.10.F.VendorA.VendorC.VendorX.Network1.dump
   1.10.F.VendorA.VendorC.VendorX.Network2.dump
/1.11.A
   1.11.A.REF-Host1.REF-Client1.result
   1.11.A.VendorC.VendorX.Network1.dump
   1.11.A.VendorC.VendorX.Network2.dump
   1.11.A.VendorC.VendorX.Network3.dump
/1.11.B
   1.11.B.REF-Host1.REF-Client1.result
   1.11.B.VendorC.VendorX.Network1.dump
   1.11.B.VendorC.VendorX.Network2.dump
   1.11.B.VendorC.VendorX.Network3.dump
/1.11.C
   1.11.C.REF-Host1.REF-Client1.result
   1.11.C.VendorX.VendorE.Network1.dump
   1.11.C.VendorX.VendorE.Network2.dump
   1.11.C.VendorX.VendorE.Network3.dump
/1.11.D
   1.11.D.REF-Host1.REF-Client1.result
   1.11.D.VendorX.VendorE.Network1.dump
   1.11.D.VendorX.VendorE.Network2.dump
   1.11.D.VendorX.VendorE.Network3.dump
/2.2.A
   2.2.A.VendorA.REF-DNS-Server1.result
   2.2.A.VendorA.VendorC.VendorX.Network1.dump
   2.2.A.VendorA.VendorC.VendorX.Network2.dump
/2.2.B
   2.2.B.VendorA.REF-DNS-Server1.result
   2.2.B.VendorA.VendorC.VendorX.Network1.dump
   2.2.B.VendorA.VendorC.VendorX.Network2.dump
/2.3.A
   2.3.A.VendorA.REF-DNS-Server1.result
   2.3.A.VendorA.VendorC.VendorX.Network1.dump
   2.3.A.VendorA.VendorC.VendorX.Network2.dump
/2.3.B
   2.3.B.VendorA.REF-DNS-Server1.result
   2.3.B.VendorA.VendorC.VendorX.Network1.dump
   2.3.B.VendorA.VendorC.VendorX.Network2.dump
```

```
/2.4.A
   2.4.A.REF-Client1.REF-DNS-Server1.result
   2.4.A.VendorC.VendorX.Network1.dump
   2.4.A.VendorC.VendorX.Network2.dump
   2.4.A.VendorC.VendorX.Network3.dump
/2.4.B
   2.4.B.REF-Client1.REF-DNS-Server1.result
   2.4.B.VendorC.VendorX.Network1.dump
   2.4.B.VendorC.VendorX.Network2.dump
   2.4.B.VendorC.VendorX.Network3.dump
/2.4.C
   2.4.C.REF-Client1.REF-DNS-Server1.result
   2.4.C.VendorC.VendorX.Network1.dump
   2.4.C.VendorC.VendorX.Network2.dump
   2.4.C.VendorC.VendorX.Network3.dump
/2.4.D
   2.4.D.REF-Client1.REF-DNS-Server1.result
   2.4.D.VendorC.VendorX.Network1.dump
   2.4.D.VendorC.VendorX.Network2.dump
   2.4.D.VendorC.VendorX.Network3.dump
/2.4.E
   2.4.E.REF-Client1.REF-DNS-Server1.result
   2.4.E.VendorX.VendorE.Network1.dump
   2.4.E.VendorX.VendorE.Network2.dump
   2.4.E.VendorX.VendorE.Network3.dump
/2.4.F
   2.4.F.REF-Client1.REF-DNS-Server1.result
   2.4.F.VendorX.VendorE.Network1.dump
   2.4.F.VendorX.VendorE.Network2.dump
   2.4.F.VendorX.VendorE.Network3.dump
/2.4.G
   2.4.G.REF-Client1.REF-DNS-Server1.result
   2.4.G.VendorX.VendorE.Network1.dump
   2.4.G.VendorX.VendorE.Network2.dump
   2.4.G.VendorX.VendorE.Network3.dump
/2.4.H
   2.4.H.REF-Client1.REF-DNS-Server1.result
   2.4.H.VendorX.VendorE.Network1.dump
   2.4.H.VendorX.VendorE.Network2.dump
   2.4.H.VendorX.VendorE.Network3.dump
/2.5.A
   2.5.A.VendorA.REF-DNS-Server1.result
   2.5.A.VendorA.VendorX.Network1.dump
/2.5.B
   2.5.B.VendorA.REF-DNS-Server1.result
   2.5.B.VendorA.VendorX.Network1.dump
/2.6.A
   2.6.A.VendorA.REF-DNS-Server1.result
   2.6.A.VendorA.VendorX.Network1.dump
/2.6.B
   2.6.B.VendorA.REF-DNS-Server1.result
   2.6.B.VendorA.VendorX.Network1.dump
```

```
/3.2.A
   3.2.A.VendorA.REF-DNS-Server1.result
   3.2.A.VendorA.VendorC.VendorX.Network1.dump
   3.2.A.VendorA.VendorC.VendorX.Network2.dump
/3.2.B
   3.2.B.VendorA.REF-DNS-Server1.result
   3.2.B.VendorA.VendorC.VendorX.Network1.dump
   3.2.B.VendorA.VendorC.VendorX.Network2.dump
/3.3.A
   3.3.A.VendorA.REF-DNS-Server1.result
   3.3.A.VendorA.VendorC.VendorX.Network1.dump
   3.3.A.VendorA.VendorC.VendorX.Network2.dump
/3.3.B
   3.3.B.VendorA.REF-DNS-Server1.result
   3.3.B.VendorA.VendorC.VendorX.Network1.dump
   3.3.B.VendorA.VendorC.VendorX.Network2.dump
/3.4.A
   3.4.A.REF-Client1.REF-DNS-Server1.result
   3.4.A.VendorC.VendorX.Network1.dump
   3.4.A.VendorC.VendorX.Network2.dump
   3.4.A.VendorC.VendorX.Network3.dump
/3.4.B
   3.4.B.REF-Client1.REF-DNS-Server1.result
   3.4.B.VendorC.VendorX.Network1.dump
   3.4.B.VendorC.VendorX.Network2.dump
   3.4.B.VendorC.VendorX.Network3.dump
/3.4.C
   3.4.C.REF-Client1.REF-DNS-Server1.result
   3.4.C.VendorC.VendorX.Network1.dump
   3.4.C.VendorC.VendorX.Network2.dump
   3.4.C.VendorC.VendorX.Network3.dump
/3.4.D
   3.4.D.REF-Client1.REF-DNS-Server1.result
   3.4.D.VendorC.VendorX.Network1.dump
   3.4.D.VendorC.VendorX.Network2.dump
   3.4.D.VendorC.VendorX.Network3.dump
/3.4.E
   3.4.E.REF-Client1.REF-DNS-Server1.result
   3.4.E.VendorX.VendorE.Network1.dump
   3.4.E.VendorX.VendorE.Network2.dump
   3.4.E.VendorX.VendorE.Network3.dump
/3.4.F
   3.4.F.REF-Client1.REF-DNS-Server1.result
   3.4.F.VendorX.VendorE.Network1.dump
   3.4.F.VendorX.VendorE.Network2.dump
   3.4.F.VendorX.VendorE.Network3.dump
/3.4.G
   3.4.H.REF-Client1.REF-DNS-Server1.result
   3.4.H.VendorX.VendorE.Network1.dump
   3.4.H.VendorX.VendorE.Network2.dump
   3.4.H.VendorX.VendorE.Network3.dump
/3.4.H
```

```
    3.4.H.REF-Client1.REF-DNS-Server1.result
    3.4.H.VendorX.VendorE.Network1.dump
    3.4.H.VendorX.VendorE.Network2.dump
    3.4.H.VendorX.VendorE.Network3.dump
 /Topology
    1.9.A.VendorX.topology
    1.9.B.VendorX.topology
    1.9.C.VendorX.topology
    1.9.D.VendorX.topology
    1.9.E.VendorX.topology
    1.9.F.VendorX.topology
    1.10.A.VendorX.topology
    1.10.B.VendorX.topology
    1.10.C.VendorX.topology

    1.10.D.VendorX.topology
    1.10.E.VendorX.topology
    1.10.F.VendorX.topology
    1.11.A.VendorX.topology
    1.11.B.VendorX.topology
    1.11.C.VendorX.topology
    1.11.D.VendorX.topology
    2.2.A.VendorX.topology
    2.2.B.VendorX.topology
    2.3.A.VendorX.topology
    2.3.B.VendorX.topology
    2.4.A.VendorX.topology
    2.4.B.VendorX.topology
    2.4.C.VendorX.topology
    2.4.D.VendorX.topology
    2.4.E.VendorX.topology
    2.4.F.VendorX.topology
    2.4.G.VendorX.topology
    2.4.H.VendorX.topology
    3.2.A.VendorX.topology
    3.2.B.VendorX.topology
    3.3.A.VendorX.topology
    3.3.B.VendorX.topology
    3.4.A.VendorX.topology
    3.4.B.VendorX.topology
    3.4.C.VendorX.topology
    3.4.D.VendorX.topology
    3.4.E.VendorX.topology
    3.4.F.VendorX.topology
    3.4.G.VendorX.topology
    3.4.H.VendorX.topology
/Client.VendorB-Server.VendorD-Relay.VendorE
 /Results
  /1.9.A
    1.9.A.REF-Host1.VendorB.result
    1.9.A.VendorB.VendorD.VendorX.Network1.dump
    1.9.A.VendorB.VendorD.VendorX.Network2.dump
```

```
/1.9.B
    1.9.B.REF-Host1.VendorB.result
    1.9.B.VendorB.VendorD.VendorX.Network1.dump
    1.9.B.VendorB.VendorD.VendorX.Network2.dump
/1.9.C
    1.9.C.REF-Host1.VendorB.result
    1.9.C.VendorB.VendorD.VendorX.Network1.dump
    1.9.C.VendorB.VendorD.VendorX.Network2.dump
/1.9.D
    1.9.D.REF-Host1.VendorB.result
    1.9.D.VendorB.VendorD.VendorX.Network1.dump
    1.9.D.VendorB.VendorD.VendorX.Network2.dump
/1.9.E
    1.9.E.REF-Host1.VendorB.result
    1.9.E.VendorB.VendorD.VendorX.Network1.dump
    1.9.E.VendorB.VendorD.VendorX.Network2.dump
/1.9.F
    1.9.F.VendorX.REF-Host1.result
    1.9.F.VendorB.VendorD.VendorX.Network1.dump
    1.9.F.VendorB.VendorD.VendorX.Network2.dump
/1.10.A
    1.10.A.REF-Host1.VendorB.result
    1.10.A.VendorB.VendorD.VendorX.Network1.dump
    1.10.A.VendorB.VendorD.VendorX.Network2.dump
/1.10.B
    1.10.B.REF-Host1.VendorB.result
    1.10.B.VendorB.VendorD.VendorX.Network1.dump
    1.10.B.VendorB.VendorD.VendorX.Network2.dump
/1.10.C
    1.10.C.REF-Host1.VendorB.result
    1.10.C.VendorB.VendorD.VendorX.Network1.dump
    1.10.C.VendorB.VendorD.VendorX.Network2.dump
/1.10.D
    1.10.D.REF-Host1.VendorB.result
    1.10.D.VendorB.VendorD.VendorX.Network1.dump
    1.10.D.VendorB.VendorD.VendorX.Network2.dump
/1.10.E
    1.10.E.REF-Host1.VendorB.result
    1.10.E.VendorB.VendorD.VendorX.Network1.dump
    1.10.E.VendorB.VendorD.VendorX.Network2.dump
/1.10.F
    1.10.F.VendorX.REF-Host1.result
    1.10.F.VendorB.VendorD.VendorX.Network1.dump
    1.10.F.VendorB.VendorD.VendorX.Network2.dump
/1.11.A
    1.11.A.REF-Host1.REF-Client1.result
    1.11.A.VendorD.VendorX.Network1.dump
    1.11.A.VendorD.VendorX.Network2.dump
    1.11.A.VendorD.VendorX.Network3.dump
/1.11.B
    1.11.B.REF-Host1.REF-Client1.result
    1.11.B.VendorD.VendorX.Network1.dump
    1.11.B.VendorD.VendorX.Network2.dump
    1.11.B.VendorD.VendorX.Network3.dump
/1.11.C
    1.11.C.REF-Host1.REF-Client1.result
    1.11.C.VendorX.VendorF.Network1.dump
    1.11.C.VendorX.VendorF.Network2.dump
    1.11.C.VendorX.VendorF.Network3.dump
/1.11.D
    1.11.D.REF-Host1.REF-Client1.result
    1.11.D.VendorX.VendorF.Network1.dump
    1.11.D.VendorX.VendorF.Network2.dump
    1.11.D.VendorX.VendorF.Network3.dump
/2.2.A
    2.2.A.VendorB.REF-DNS-Server1.result
    2.2.A.VendorB.VendorD.VendorX.Network1.dump
    2.2.A.VendorB.VendorD.VendorX.Network2.dump
/2.2.B
    2.2.B.VendorB.REF-DNS-Server1.result
    2.2.B.VendorB.VendorD.VendorX.Network1.dump
    2.2.B.VendorB.VendorD.VendorX.Network2.dump
/2.3.A
    2.3.A.VendorB.REF-DNS-Server1.result
    2.3.A.VendorB.VendorD.VendorX.Network1.dump
    2.3.A.VendorB.VendorD.VendorX.Network2.dump
/2.3.B
    2.3.B.VendorB.REF-DNS-Server1.result
    2.3.B.VendorB.VendorD.VendorX.Network1.dump
    2.3.B.VendorB.VendorD.VendorX.Network2.dump
/2.4.A
    2.4.A.REF-Client1.REF-DNS-Server1.result
    2.4.A.VendorD.VendorX.Network1.dump
    2.4.A.VendorD.VendorX.Network2.dump
    2.4.A.VendorD.VendorX.Network3.dump
/2.4.B
    2.4.B.REF-Client1.REF-DNS-Server1.result
    2.4.B.VendorD.VendorX.Network1.dump
    2.4.B.VendorD.VendorX.Network2.dump
    2.4.B.VendorD.VendorX.Network3.dump
/2.4.C
    2.4.C.REF-Client1.REF-DNS-Server1.result
    2.4.C.VendorD.VendorX.Network1.dump
    2.4.C.VendorD.VendorX.Network2.dump
    2.4.C.VendorD.VendorX.Network3.dump
/2.4.D
    2.4.D.REF-Client1.REF-DNS-Server1.result
    2.4.D.VendorD.VendorX.Network1.dump
    2.4.D.VendorD.VendorX.Network2.dump
    2.4.D.VendorD.VendorX.Network3.dump
/2.4.E
    2.4.E.REF-Client1.REF-DNS-Server1.result
    2.4.E.VendorX.VendorF.Network1.dump
    2.4.E.VendorX.VendorF.Network2.dump
```

```
   2.4.E.VendorX.VendorF.Network3.dump
/2.4.F
   2.4.F.REF-Client1.REF-DNS-Server1.result
   2.4.F.VendorX.VendorF.Network1.dump
   2.4.F.VendorX.VendorF.Network2.dump
   2.4.F.VendorX.VendorF.Network3.dump
/2.4.G
   2.4.G.REF-Client1.REF-DNS-Server1.result
   2.4.G.VendorX.VendorF.Network1.dump
   2.4.G.VendorX.VendorF.Network2.dump
   2.4.G.VendorX.VendorF.Network3.dump
/2.4.H
   2.4.H.REF-Client1.REF-DNS-Server1.result
   2.4.H.VendorX.VendorF.Network1.dump
   2.4.H.VendorX.VendorF.Network2.dump
   2.4.H.VendorX.VendorF.Network3.dump
/3.2.A
   3.2.A.VendorB.REF-DNS-Server1.result
   3.2.A.VendorB.VendorD.VendorX.Network1.dump
   3.2.A.VendorB.VendorD.VendorX.Network2.dump
/3.2.B
   3.2.B.VendorB.REF-DNS-Server1.result
   3.2.B.VendorB.VendorD.VendorX.Network1.dump
   3.2.B.VendorB.VendorD.VendorX.Network2.dump
/3.3.A
   3.3.A.VendorB.REF-DNS-Server1.result
   3.3.A.VendorB.VendorD.VendorX.Network1.dump
   3.3.A.VendorB.VendorD.VendorX.Network2.dump
/3.3.B
   3.3.B.VendorB.REF-DNS-Server1.result
   3.3.B.VendorB.VendorD.VendorX.Network1.dump
   3.3.B.VendorB.VendorD.VendorX.Network2.dump
/3.4.A
   3.4.A.REF-Client1.REF-DNS-Server1.result
   3.4.A.VendorD.VendorX.Network1.dump
   3.4.A.VendorD.VendorX.Network2.dump
   3.4.A.VendorD.VendorX.Network3.dump
/3.4.B
   3.4.B.REF-Client1.REF-DNS-Server1.result
   3.4.B.VendorD.VendorX.Network1.dump
   3.4.B.VendorD.VendorX.Network2.dump
   3.4.B.VendorD.VendorX.Network3.dump
/3.4.C
   3.4.C.REF-Client1.REF-DNS-Server1.result
   3.4.C.VendorD.VendorX.Network1.dump
   3.4.C.VendorD.VendorX.Network2.dump
   3.4.C.VendorD.VendorX.Network3.dump
/3.4.D
   3.4.D.REF-Client1.REF-DNS-Server1.result
   3.4.D.VendorD.VendorX.Network1.dump
   3.4.D.VendorD.VendorX.Network2.dump
   3.4.D.VendorD.VendorX.Network3.dump
```

```
  /3.4.E
    3.4.E.REF-Client1.REF-DNS-Server1.result
    3.4.E.VendorX.VendorF.Network1.dump
    3.4.E.VendorX.VendorF.Network2.dump
    3.4.E.VendorX.VendorF.Network3.dump
  /3.4.F
    3.4.F.REF-Client1.REF-DNS-Server1.result
    3.4.F.VendorX.VendorF.Network1.dump
    3.4.F.VendorX.VendorF.Network2.dump
    3.4.F.VendorX.VendorF.Network3.dump
  /3.4.G
    3.4.H.REF-Client1.REF-DNS-Server1.result
    3.4.H.VendorX.VendorF.Network1.dump
    3.4.H.VendorX.VendorF.Network2.dump
    3.4.H.VendorX.VendorF.Network3.dump
  /3.4.H
    3.4.H.REF-Client1.REF-DNS-Server1.result
    3.4.H.VendorX.VendorF.Network1.dump
    3.4.H.VendorX.VendorF.Network2.dump
    3.4.H.VendorX.VendorF.Network3.dump
 /Topology
    1.9.A.VendorX.topology
    1.9.B.VendorX.topology
    1.9.C.VendorX.topology
    1.9.D.VendorX.topology
    1.9.E.VendorX.topology
    1.9.F.VendorX.topology
    1.10.A.VendorX.topology
    1.10.B.VendorX.topology
    1.10.C.VendorX.topology
    1.10.D.VendorX.topology
    1.10.E.VendorX.topology
    1.10.F.VendorX.topology
    1.11.A.VendorX.topology
    1.11.B.VendorX.topology
    1.11.C.VendorX.topology
    1.11.D.VendorX.topology
    2.2.A.VendorX.topology
    2.2.B.VendorX.topology
    2.3.A.VendorX.topology
    2.3.B.VendorX.topology
    2.4.A.VendorX.topology
    2.4.B.VendorX.topology
    2.4.C.VendorX.topology
    2.4.D.VendorX.topology
    2.4.E.VendorX.topology
    2.4.F.VendorX.topology
    2.4.G.VendorX.topology
    2.4.H.VendorX.topology
    3.2.A.VendorX.topology
    3.2.B.VendorX.topology
    3.3.A.VendorX.topology
```

3.3.B.VendorX.topology
3.4.A.VendorX.topology
3.4.B.VendorX.topology
3.4.C.VendorX.topology
3.4.D.VendorX.topology
3.4.E.VendorX.topology
3.4.F.VendorX.topology
3.4.G.VendorX.topology
3.4.H.VendorX.topology
/VendorX.table

Files for NUT acting as Requesting Router (Client)

< Phase-2 DHCPv6>
Your device is a Requesting Router
TAR-RR1 : VendorX (Application)
TAR-DR1 : VendorA
: VendorB

```
/app_form_Phase2_DHCPv6.txt
/Conformance
  /DHCPv6_Self_Test_P2_1_0_X.tar
/Interoperability
  /DR.VendorA
    /Results
      /4.1
          4.1.VendorX.VendorA.Network1.dump
      /4.2
          4.2.VendorX.VendorA.Network1.dump
      /4.3
          4.3.VendorX.VendorA.Network1.dump
      /4.4
          4.4.VendorX.VendorA.Network1.dump
      /4.5
          4.5.VendorX.VendorA.Network1.dump
      /5.1
          5.1.VendorX.VendorA.Network1.dump
      /5.2
          5.2.VendorX.VendorA.Network1.dump
      /5.3
          5.3.VendorX.VendorA.Network1.dump

    /Topology
          4.1.VendorX.topology
          4.2.VendorX.topology
          4.3.VendorX.topology
          4.4.VendorX.topology
          4.5.VendorX.topology
          5.1.VendorX.topology
          5.2.VendorX.topology
          5.3.VendorX.topology

  /Server.VendorB
    /Results
      /4.1
          4.1.VendorX.VendorB.Network1.dump
      /4.2
          4.2.VendorX.VendorB.Network1.dump
      /4.3
          4.3.VendorX.VendorB.Network1.dump
      /4.4
          4.4.VendorX.VendorB.Network1.dump
      /4.5
          4.5.VendorX.VendorB.Network1.dump
  /5.1
     5.1.VendorX.VendorB.Network1.dump
  /5.2
     5.2.VendorX.VendorB.Network1.dump
  /5.3
     5.3.VendorX.VendorB.Network1.dump

 /Topology
     4.1.VendorX.topology
     4.2.VendorX.topology
     4.3.VendorX.topology
     4.4.VendorX.topology
     4.5.VendorX.topology
     5.1.VendorX.topology
     5.2.VendorX.topology
     5.3.VendorX.topology
```

Files for NUT acting as Delegating Router (Server)

```
< Phase-2 DHCPv6>
Your device is a Delegating Router
TAR-DR1        : VendorX (Application)
TAR-RR1        : VendorA
               : VendorB

/app_form_Phase2_DHCPv6.txt
/Conformance
  /DHCPv6_Self_Test_P2_1_0_X.tar
/Interoperability
  /RR.VendorA
    /Results
      /4.1
          4.1.VendorX.VendorA.Network1.dump
      /4.2
          4.2.VendorX.VendorA.Network1.dump
      /4.3
          4.3.VendorX.VendorA.Network1.dump
      /4.4
          4.4.VendorX.VendorA.Network1.dump
      /4.5
          4.5.VendorX.VendorA.Network1.dump
      /5.1
          5.1.VendorX.VendorA.Network1.dump
      /5.2
          5.2.VendorX.VendorA.Network1.dump
      /5.3
          5.3.VendorX.VendorA.Network1.dump

    /Topology
          4.1.VendorX.topology
          4.2.VendorX.topology
          4.3.VendorX.topology
          4.4.VendorX.topology
          4.5.VendorX.topology
          5.1.VendorX.topology
          5.2.VendorX.topology
          5.3.VendorX.topology

  /RR.VendorB
    /Results
      /4.1
          4.1.VendorX.VendorB.Network1.dump
      /4.2
          4.2.VendorX.VendorB.Network1.dump
      /4.3
          4.3.VendorX.VendorB.Network1.dump
      /4.4
          4.4.VendorX.VendorB.Network1.dump
      /4.5
          4.5.VendorX.VendorB.Network1.dump
```

```
 /5.1
    5.1.VendorX.VendorB.Network1.dump
 /5.2
    5.2.VendorX.VendorB.Network1.dump
 /5.3
    5.3.VendorX.VendorB.Network1.dump

/Topology
    4.1.VendorX.topology
    4.2.VendorX.topology
    4.3.VendorX.topology
    4.4.VendorX.topology
    4.5.VendorX.topology
    5.1.VendorX.topology
    5.2.VendorX.topology
    5.3.VendorX.topology
```

1.4. Network Traffic Application

In the test results, "ping" is the default application to send ICMP echo request. If the target device does not have "ping" application, it is possible to use any other application that behaves like the "ping" application and passes traffic through the network.