

**Moonv6 Test Suite**  
*DHCP Interoperability*  
*Test Suite*

**Technical Document**  
Revision 1.0



---

*IPv6 Consortium*  
*InterOperability Laboratory*  
*Research Computing Center*  
*University of New Hampshire*

*121 Technology Drive, Suite 2*  
*Durham, NH 03824-3525*  
*Phone: (603) 862-2804*  
*Fax: (603) 862-4181*  
*<http://www.iol.unh.edu>*

## TABLE OF CONTENTS

ACKNOWLEDGEMENTS .....	4
INTRODUCTION .....	5
Common Topology .....	5
TEST ORGANIZATION.....	6
REFERENCES .....	8
GROUP 1: Basic DHCP Services.....	9
Test DHCP.1.1: DHCP Initialization .....	10
Test DHCP.1.2: DHCP Relay Agent .....	12
Test DHCP.1.3: DHCP Authentication.....	14
Test DHCP.1.4: Duplicate Response Messages .....	15
GROUP 2: Client-Initiated Configuration Exchange .....	16
Test DHCP.2.1: Transmission of Confirm messages.....	17
Test DHCP.2.2: Transmission of Renew messages .....	19
Test DHCP.2.3: Transmission of Rebind message .....	21
Test DHCP.2.4: Transmission of Release messages .....	23
Test DHCP.2.5: Reception of Advertise messages .....	25
GROUP 3: Server-Initiated Configuration Exchange.....	26
Test DHCP.3.1: Transmission of Reconfigure messages.....	27
Test DHCP.3.2: Transmission of Advertise messages with NoAddrAvail .....	28
Test DHCP.3.3: Prefix Delegation.....	29

## MODIFICATION RECORD

Draft Version Complete

September 15, 2004

Version 1.0 Complete

November 10, 2005

## **ACKNOWLEDGEMENTS**

**The University of New Hampshire would like to acknowledge the efforts of the following individuals in the development of this test suite. This test suite belongs to the University of New Hampshire InterOperability Lab and is a collaborative effort of those listed below and the participants of Moonv6.**

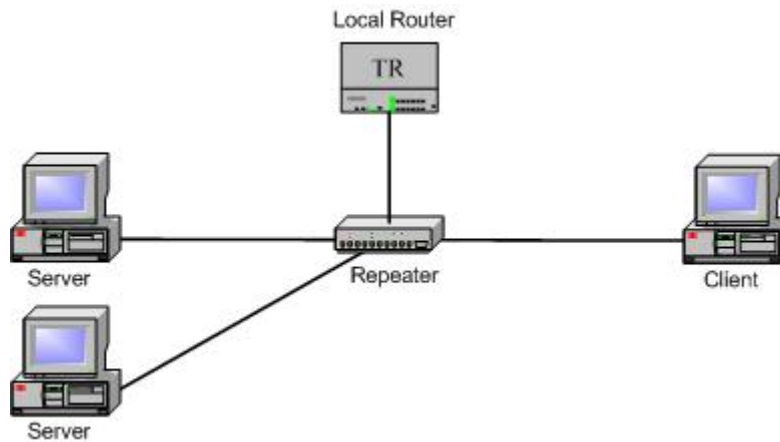
John Brzozowski	Lucent Technologies
Ralph Droms	Cisco Systems
Thomas Peterson	University of New Hampshire
Kari Revier	University of New Hampshire
Benjamin Schultz	University of New Hampshire
Timothy Winters	University of New Hampshire

# INTRODUCTION

## Overview

The University of New Hampshire's InterOperability Laboratory (IOL) is an institution designed to improve the interoperability of standards-based products by providing an environment where a product can be tested against other implementations of a standard. This suite of tests has been developed to help implementers evaluate the functioning of the policy functionality of DHCP products. The tests do not determine if a product conforms to any specifications, nor are they purely interoperability tests. Rather, they provide one method to isolate problems within a device. Successful completion of all tests contained in this suite does not guarantee that the tested device will interoperate with any other devices. However, combined with satisfactory operation in the IOL's semi-production environment, these tests provide a reasonable level of confidence that the Device Under Test will function well in most multi-vendor environments.

## Common Topology



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

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

## TEST ORGANIZATION

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

- Test Label:** The test label and title comprise the first line of the test block. The test label is composed by concatenating the short test suite name, the group number, and the test number within the group, separated by periods. The Test Number is the group and test number, also separated by a period. So, test label DHCP.1.2 refers to the second test of the first test group in the DHCP test suite. The test number is 1.2.
- 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.
- Last Modification** The last date this test was modified.
- Discussion:** The Discussion is a general discussion of the test and relevant section of the specification, including any assumptions made in the design or implementation of the test as well as known limitations.
- Test Setup:** The Test Setup section describes the configuration of all devices prior to the start of the test. Different parts of the procedure may involve configuration steps that deviate from what is given in the test setup. If a value is not provided for a protocol parameter, then the protocol's default is used 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 packet 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 DUT 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 DUT'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:

- [ADDRCONF] Thomson, S., T. Narten, IPv6 Stateless Address Autoconfiguration, RFC 2462, December 1998.
  
- [ICMPv6] Conta, A., S. Deering, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, RFC 2463, December 1998.
  
- [IPv6-SPEC] Hinden, R., S. Deering, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, December 1998.
  
- [ND] Narten, T., Nordmark, E., and W. Simpson, Neighbor Discovery for IP Version 6 (IPv6), RFC 2461, December 1998.
  
- [ADDR] Hinden, R., S. Deering, IP Version 6 Addressing Architecture, RFC 2373, July 1998.
  
- [3315] R. Droms, Editor. Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3315, June 2003.

## **GROUP 1: Basic DHCP Services**

### **Scope:**

These following tests are designed to verify basic interoperability of IPv6 DHCP services.

### **Overview:**

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

## Test DHCP.1.1: DHCP Initialization

**Purpose:** To verify that a device can properly interoperate while interacting with DHCP.

**References:** IP, 3315

**Resource Requirements:** Monitor to capture packets, generators

**Last Modification:** September 15, 2004

**Discussion:** There are two alternatives to obtaining address and network information. The four message approach will allow a client to obtain both an IPv6 address and DNS/Domain name information. To accomplish this, a client sends a Solicit message to the All\_DHCP\_Relay\_Agents\_and\_Servers address to find an available DHCP server. The server then responds with an Advertise message. The client then sends a Request message to the server to confirm the address assignment and request additional configuration information. The two message approach allows a client to obtain additional configuration information after it obtains an IPv6 address through stateless auto-configuration. The client first sends an Information-Request message to the All\_DHCP\_Relay\_Agents\_and\_Servers address. The server responds with a Reply message containing the configuration information for the client.

**Test Setup:** Connect the network according to the [Common Topology](#). DHCPv6 is disabled on the client device after each part.

### Procedure:

#### *Part A: Client Server Exchange involving Four Messages*

1. Configure the router to send transmit RA with the M-bit set and O-bit set and advertise a prefix without the A bit (autonomous address-configuration flag) set.
2. Configure the client to disable auto-configuration and enable DHCP.
3. Observe the packet exchange on-link.
4. Confirm that the client received the proper information from the server through the management interface.
5. Observe the packets transmitted between the client and the server.

#### *Part B: Client Server Exchange involving Two Messages*

6. Configure the router to send transmit RA with the M-bit clear and O-bit set.
7. Configure the client to enable auto-configuration and enable DHCP.
8. Observe the packet exchange on-link.
9. Confirm that the client received the proper information from the server through the management interface.
10. Ping the remote router from the client.
11. Observe the packets transmitted between the client and the server.

### Observable Results:

- In Part A, the client should send a solicit message and the server should send an advertise message with the IP address information inside. The client should then send a request message to confirm the IP address and ask for additional information. The server responds with a reply message.
- In Part B, the client should send an information-request message and the server should send an reply message.

**Possible Problems:** The client may not have the option to disable the auto-configuration

function.

## Test DHCP.1.2: DHCP Relay Agent

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

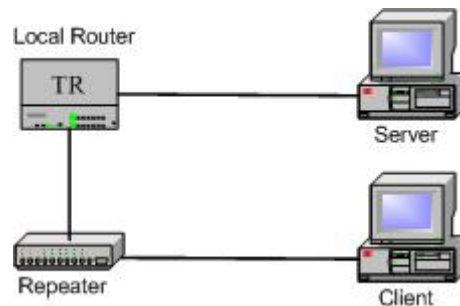
References: IP, 3315

**Resource Requirements:** Monitor to capture packets, generators

**Last Modification:** September 15, 2004

**Discussion:** When a DHCP server is not on-link, the local router can be configured to be a DHCP relay agent. The relay agent looks for DHCP messages and forwards them to a DHCP server on a different link.

**Test Setup:** Connect Devices as shown below.



### Procedure:

#### Part A: Client Server Exchange involving Four Messages

1. Configure the local router as a DHCP relay agent.
2. Configure the router to send transmit RA with the M-bit set and O-bit set and advertise a prefix without the A bit (autonomous address-configuration flag) set.
3. Configure the client to disable auto-configuration and enable DHCP.
4. Observe the packet exchange on-link.
5. Confirm that the client received the proper information from the server through the management interface.
6. Observe the packets transmitted between the client and the server.

#### Part B: Client Server Exchange involving Two Messages

7. Configure the local router as a DHCP relay agent.
8. Configure the router to send transmit RA with the M-bit clear and O-bit set
9. Configure the client to enable auto-configuration and enable DHCP.
10. Observe the packet exchange on-link.
11. Confirm that the client received the proper information from the server through the management interface.
12. Ping the remote router from the client.
13. Observe the packets transmitted between the client and the server.

### Observable Results:

- In Part A, the client should send a solicit message and the server should send an advertise message with the IP address information inside. The client should then send a request message to confirm the IP address and ask for additional information. The server responds with a reply.

- In Part B, the client should send an information-request message and the server should send a reply message. The local router should properly act like a relay.

**Possible Problems:** The client may not have the option to disable the auto-configuration function.

### **Test DHCP.1.3: DHCP Authentication**

**Purpose:** To verify that a device receives an address when DHCP Authentication is enabled.

References: IP, 3315

**Resource Requirements:** Monitor to capture packets, generators

**Last Modification:** November 10, 2005

**Discussion:** When a DHCP server and client have Authentication enabled, HMAC-MD5 may be used. This is to ensure that the client is properly obtaining an address and that the contents of the Information Request or Solicit messages are not tampered with.

**Test Setup:** Connect the network according to the [Common Topology](#). DHCPv6 is disabled on the client device after each part.

#### **Procedure:**

##### *Part A: Client Server Exchange involving Four Messages*

1. Configure the router to send transmit RA with the M-bit set and O-bit set and advertise a prefix without the A bit (autonomous address-configuration flag) set.
2. Configure the client to disable auto-configuration and enable DHCP.
3. Observe the packet exchange on-link.
4. Confirm that the client received the proper information from the server through the management interface.
5. Observe the packets transmitted between the client and the server.

##### *Part B: Client Server Exchange involving Two Messages*

6. Configure the router to send transmit RA with the M-bit clear and O-bit set.
7. Configure the client to enable auto-configuration and enable DHCP.
8. Observe the packet exchange on-link.
9. Confirm that the client received the proper information from the server through the management interface.
10. Observe the packets transmitted between the client and the server.

#### **Observable Results:**

- In Part A, the client should send a solicit message and the server should send an advertise message with the IP address information inside. The client should then send a request message to confirm the IP address and ask for additional information. The server responds with a reply message.
- In Part B, the client should send an information-request message and the server should send a reply message.

**Possible Problems:** The client may not have the option to disable the auto-configuration function. Authentication may not be supported on the Client or Server devices.

## Test DHCP.1.4: Duplicate Response Messages

**Purpose:** To verify that a device obtains a DHCP address from a network with multiple DHCP servers.

References: IP, 3315

**Resource Requirements:** Monitor to capture packets, generators

**Last Modification:** September 21, 2004

**Discussion:** When there are multiple DHCP servers on a network, the client will receive multiple replies to an Information Request Message or a Solicit Message. The client must obtain the correct addressing information and remain stable in this network situation.

**Test Setup:** Connect the network according to the [Common Topology](#). DHCPv6 is disabled on the client device after each part.

### Procedure:

#### *Part A: Two Servers with Four Message Initialization*

1. Configure the router to send transmit RA with the M-bit set and O-bit set and advertise a prefix without the A bit (autonomous address-configuration flag) set.
2. Configure the client to disable auto-configuration and enable DHCP.
3. Observe the packet exchange on-link.
4. Confirm that the client received the proper information from the server through the management interface.
5. Observe the packets transmitted between the client and the server.

#### *Part B: Two Servers with Two Message Initialization*

6. Configure the router to send transmit RA with the M-bit clear and O-bit set
7. Configure the client to enable auto-configuration and enable DHCP.
8. Observe the packet exchange on-link.
9. Confirm that the client received the proper information from the server through the management interface.
10. Ping the remote router from the client.
11. Observe the packets transmitted between the client and the server.

### Observable Results:

- In Part A, the client should send a solicit message and the servers should both send an advertise message with the IP address information inside. The client should then send a request message to confirm the IP address and ask for additional information. The selected server should respond with a reply message that contains the confirmed address. All devices should remain stable and the client should configure its address.
- In Part B, the client should send an information-request message and the servers should both send a reply message. All devices should remain stable.

**Possible Problems:** The client may not have the option to disable the auto-configuration function. Authentication may not be supported on the Client or Server devices.

## **GROUP 2: Client-Initiated Configuration Exchange**

### **Scope:**

The following tests are designed to verify a client initiates a message exchange with a server or servers to acquire or update configuration information of interest

.

## Test DHCP.2.1: Transmission of Confirm messages

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

**References:** [DHCP 3315] – Sections 5.5, 14 and 18.1.2 and 18.2.2

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

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

When the server receives a Confirm message, the server determines whether the addresses in the Confirm message are appropriate for the link to which the client is attached. If all of the addresses in the Confirm message pass this test, the server returns a status of Success. If any of the addresses do not pass this test, the server returns a status of NotOnLink. If the server is unable to perform this test (for example, the server does not have information about prefixes on the link to which the client is connected), or there were no addresses in any of the IAs sent by the client, the server **MUST NOT** send a reply to the client.

**Test Setup:** Connect the network according to the [Common Topology](#). DHCPv6 is disabled on the client device after each part.

### Procedure:

*Part A: Confirm message format.*

1. Configure the client to disable auto-configuration and enable DHCP.
2. Configure the router to send transmit RA with the M-bit set and O-bit set and advertise a prefix without the A bit (autonomous address-configuration flag) set.
3. Confirm that the client received the proper information from the server through the management interface.
4. Disconnect the client from the link.
5. Allow enough time to elapse such that the client recognizes a link down, reconnect the client.
6. Observe the messages transmitted on the link.

### Observable Results:

- *Part A*

**Step 6:** The client transmits a properly formatted Confirm message between 0 and CNF\_MAX\_DELAY (1 second) to the server containing:

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

Both servers should respond with REPLYs with a status code of 0 (Success) stating that the addresses are appropriate for the link.

**Possible Problems:**

- None.

## Test DHCP.2.2: Transmission of Renew messages

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

### References:

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

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

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

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

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

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

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

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

IRT   REN\_TIMEOUT  
MRT   REN\_MAX\_RT  
MRC   0  
MRD   Remaining time until T2

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

**Test Setup:** Connect all devices according to the [Common Topology](#). Disable DHCPv6 on the client device before each part.

### Procedure:

#### *Part A: Renew message format.*

1. Configure the client to disable auto-configuration and enable DHCP.
2. Configure the router to send transmit RA with the M-bit set and O-bit set and advertise a prefix without the A bit (autonomous address-configuration flag) set.
3. Confirm that the client received the proper information from the server through the management interface.

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

**Observable Results:**

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

**Possible Problems:**

- None.

## Test DHCP.2.3: Transmission of Rebind message

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

### References:

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

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

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

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

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

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

IRT REB\_TIMEOUT

MRT REB\_MAX\_RT

MRC 0

MRD Remaining time until valid lifetimes of all addresses have expired

**Test Setup:** Connect the network according to the [Common Topology](#). Disable DHCPv6 on the client device before each part.

### Procedure:

#### *Part A: Rebind message format*

1. Configure the client to disable auto-configuration and enable DHCP.
2. Configure the router to send transmit RA with the M-bit set and O-bit set and advertise a prefix without the A bit (autonomous address-configuration flag) set.
3. Confirm that the client received the proper information from the server through the management interface.
4. Disconnect the server from the link.
5. After time T2 (300s after Renew message), observe the messages transmitted on link.
6. Reconnect the server to the link and confirm that the client's address is renewed on the next rebind.

### Observable Results:

- *Part A*  
**Step 5:** The time from when the client receives the Reply message from the server to when the client transmits the Rebind message is equivalent to (T1+T2).

The client transmits a properly formatted Rebind message to THE SERVER containing

- A “msg-type” field set to the value of REBIND (6).
- A header containing a Transaction ID
- A Client Identifier Option (containing a DUID)
- An IA Address Option with the proper IPv6 address associated with the IA
- An Option Request Option

**Possible Problems:**

- None.

## Test DHCP.2.4: Transmission of Release messages

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

### References:

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

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

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

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

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

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

```
IRT  REL_TIMEOUT
MRT  0
MRC  REL_MAX_RC
MRD  0
```

**Test Setup:** Connect all devices according to the [Common Topology](#). Disable DHCPv6 on the client device after each part.

### Procedure:

*Part A: Release message format and release of received address*

1. Configure the client to disable auto-configuration and enable DHCP.
2. Configure the router to send transmit RA with the M-bit set and O-bit set and advertise a prefix without the A bit (autonomous address-configuration flag) set.
3. Confirm that the client received the proper information from the server through the management interface.
4. Configure the client to release the IPv6 address.
5. Observe the messages transmitted on link.
6. From the router, transmit an ICMPv6 Echo Request to the client for the released address.
7. Observe the messages transmitted on link.

### Observable Results:

- *Part A*
  - Step 5:** The client transmits a properly formatted Release message to THE SERVER containing:
    - A "msg-type" field set to the value of 8 (RELEASE).

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

**Step 7:** The client must not reply to the Echo Request.

**Possible Problems:**

- Part A may be omitted if the client cannot configure to release its IPv6 address.

## Test DHCP.2.5: Reception of Advertise messages

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

### References:

- [DHCP 3315] – Sections 17.1.2 and 17.1.3

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

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

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

**Test Setup:** Connect the devices according to the [Common Topology](#). Enable DHCPv6 on the client device before each part. Disable DHCPv6 on the client device after each part.

### Procedure:

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

1. Configure the client to disable auto-configuration and enable DHCP.
2. Configure server1 to have a Preference of 255.
3. Configure server2 to have a Preference of 0.
4. Configure the router to send transmit RA with the M-bit set and O-bit set and advertise a prefix without the A bit (autonomous address-configuration flag) set.
5. Confirm that the client received the proper information from the server through the management interface.
6. Upon reception of a Solicit message from the client, SERVER1 and SERVER2 transmit properly formatted Advertise messages.
7. Observe the messages transmitted on link.

### Observable Results:

- *Part A*  
**Step 7:** After RT seconds has elapsed, the client must choose the information from server1 and send server1 a Request message.

### Possible Problems:

- None.

## **GROUP 3: Server-Initiated Configuration Exchange**

### **Scope:**

The following tests are designed to verify a server initiates a message exchange with a client or clients to send or update configuration information of interest.

## Test DHCP.3.1: Transmission of Reconfigure messages

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

### References:

- [DHCP 3315] – Sections 19.4.1

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

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

**Test Setup:** Connect the devices according to the [Common Topology](#). Disable router prefix delegation on the server. DHCPv6 on the NUT is disabled after each part.

### Procedure:

#### *Part A: Reception of First Reconfigure message*

1. Configure the client to disable auto-configuration and enable DHCP.
2. Configure the router to send transmit RA with the M-bit set and O-bit set and advertise a prefix without the A bit (autonomous address-configuration flag) set.
3. Confirm that the client received the proper information from the server through the management interface.
4. Reconfigure the server and trigger a client reconfigure.
5. Observe the messages transmitted on link.

### Observable Results:

- *Part A*  
**Step 5:** The client must respond with a Renew message or an Information-request message depending on what was reconfigured/triggered.

### Possible Problems:

- None.

## Test DHCP.3.2: Transmission of Advertise messages with NoAddrsAvail

**Purpose:** To verify a server device properly sends messages with a status code of 2 (NoAddrsAvail)

### References:

- [DHCP 3315] – Sections 17.2.2, 17.1.3

**Discussion:** If the server will not assign any addresses to any IAs in a subsequent Request from the client, the server **MUST** send an Advertise message to the client that includes only a Status Code option with code NoAddrsAvail and a status message for the user, a Server Identifier option with the server's DUID, and a Client Identifier option with the client's DUID.

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

**Test Setup:** Connect the devices according to the [Common Topology](#). Enable DHCPv6 on the client device before each part. Disable DHCPv6 on the client device after each part.

### Procedure:

#### *Part A: Transmission of Advertise messages with NoAddrsAvail*

1. Configure the server to have no available addresses.
2. Configure the router to send transmit RA with the M-bit set and O-bit set and advertise a prefix without the A bit (autonomous address-configuration flag) set.
3. Confirm that the client did not receive an address from the server through the management interface.
4. Observe the messages transmitted on link.

### Observable Results:

- *Part A*  
**Step 3:** The client must ignore the Advertise message from the server and not configure an address.

### Possible Problems:

- None.

### Test DHCP.3.3: Prefix Delegation

**Purpose:** To verify a server device properly assigns address to a client device.

#### References:

- [DHCP 3315] – Section 11

**Discussion:** A server selects addresses to be assigned to an IA according to the address assignment policies determined by the server administrator and the specific information the server determines about the client from some combination of the following sources:

- The link to which the client is attached.
- The DUID supplied by the client.
- Other information in options supplied by the client.

**Test Setup:** Connect the devices according to the [Common Topology](#). Enable DHCPv6 on the client device before each part. Disable DHCPv6 on the client device after each part.

#### Procedure:

*Part A: Assigning addresses based on client DUID.*

1. Configure the server send one prefix for all on link clients and one prefix for the client's DUID.
2. Configure the router to send transmit RA with the M-bit set and O-bit set and advertise a prefix without the A bit (autonomous address-configuration flag) set.
3. Confirm that the client received the proper information from the server through the management interface.
4. From the router, transmit an ICMPv6 Echo Request to the client for the address assigned based on the client's DUID.
5. Observe the messages transmitted on link.

#### Observable Results:

- *Part A*  
**Step 5:** The client must send an ICMPv6 Echo Reply indicating the client was assigned an address based on its DUID.

#### Possible Problems:

- None.