

**Moonv6 Test Suite**

*DHCP Interoperability*

*Test Suite*

**DRAFT**

**Technical Document**

Revision 0.1



---

*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
TEST ORGANIZATION.....	6
REFERENCES .....	7
GROUP 1: Basic DHCP Services.....	8
Test DHCP.1.1: DHCP Initialization .....	9
Test DHCP.1.2: DHCP Relay Agent .....	11
Test DHCP.1.3: DHCP Authentication.....	13
Test DHCP.1.4: Duplicate Response Messages .....	15
Test DHCP.2.1: DHCP over Static IPv6 Tunnels .....	18
Test DHCP.2.2: DHCP Across IPsec and VPN Tunnels.....	20
Test DHCP.2.3: DHCP across a Stateful Firewall .....	21

# MODIFICATION RECORD

Draft Version Complete

September 15, 2004

## **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.**

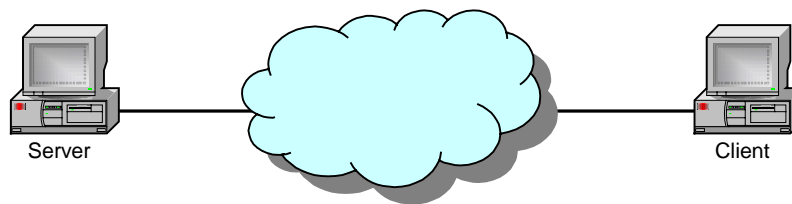
John Brzozowski	Lucent Technologies
Ralph Droms	Cisco Systems
Kari Revier	University of New Hampshire
Benjamin Schultz	University of New Hampshire

# 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.

## Test Configuration



Basic Test Configuration

There are several types of variants of the Basic Test Configuration that are specific to individual tests, such as resolution of DHCP services over a firewall or relay device. This is clearly described in each test and is represented as the cloud in this picture. The "Device Under Test" can be either the Server, the Client or both, as this is an interoperability test. There is usually a router on-link present to complete the auto-configuration process.

## 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.

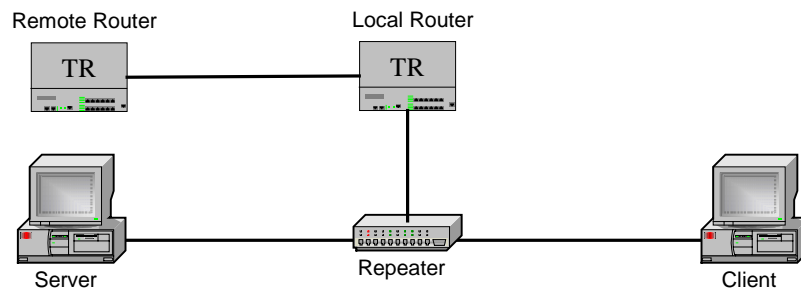
References: IP, 3315

**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 Devices as shown below.



### Procedure:

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

1. If possible, configure the client to disable auto-configuration and enable DHCP.
2. Observe the packet exchange on-link.
3. Confirm that the client received the proper information from the server through the management interface.
4. Do we insert a DNS resolution here to confirm that the info was properly passed??
5. Observe the packets transmitted between the client and the server.

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

6. If possible, configure the client to enable auto-configuration and enable DHCP.
7. Observe the packet exchange on-link.
8. Confirm that the client received the proper information from the server through the management interface.
9. Ping the remote router from the client.
10. Do we insert a DNS resolution here to confirm that the info was properly passed??
11. Observe the packets transmitted between the client and the server.

### Observable Results:

- In Part A, the client should send an information-request message and the server should send an reply message with the DNS and Domain name information inside.
- In Part B, 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 that contains the confirmed messages and the DNS and Domain name information.

**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.

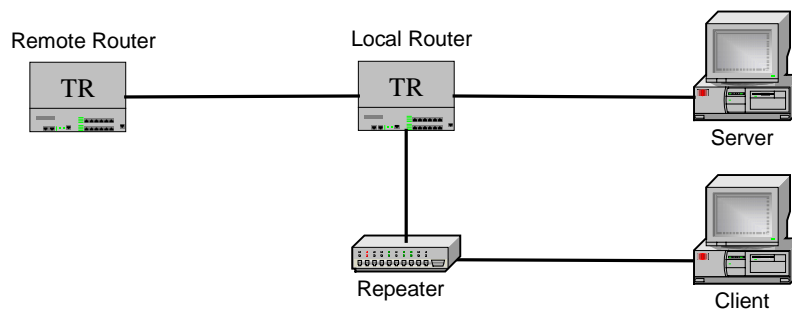
References: IP, 3315

**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. If possible, 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. Do we insert a DNS resolution here to confirm that the info was properly passed??
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. If possible, configure the client to enable auto-configuration and enable DHCP.
9. Observe the packet exchange on-link.
10. Confirm that the client received the proper information from the server through the management interface.
11. Ping the remote router from the client.
12. Do we insert a DNS resolution here to confirm that the info was properly passed??
13. Observe the packets transmitted between the client and the server.

### Observable Results:

- In Part A, the client should send an information-request message and the server should send a reply message with the DNS and Domain name information inside. The local router should properly act like a relay.

- In Part B, 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 that contains the confirmed messages and the DNS and Domain name information.

**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.

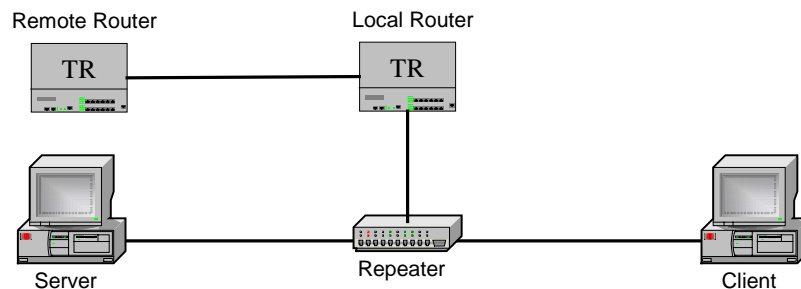
References: IP, 3315

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

**Last Modification:** September 21, 2004

**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 Devices as shown below and enable authentication on both the client and server devices.



#### Procedure:

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

1. Configure the client to disable auto-configuration and enable DHCP.
2. Observe the packet exchange on-link.
3. Confirm that the client received the proper information from the server through the management interface.
4. Do we insert a DNS resolution here to confirm that the info was properly passed??
5. Observe the packets transmitted between the client and the server.

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

6. Configure the client to enable auto-configuration and enable DHCP.
7. Observe the packet exchange on-link.
8. Confirm that the client received the proper information from the server through the management interface.
9. Ping the remote router from the client.
10. Do we insert a DNS resolution here to confirm that the info was properly passed??
11. Observe the packets transmitted between the client and the server.

#### Observable Results:

- In Part A, the client should send an information-request message and the server should send a reply message with the DNS and Domain name information inside.
- In Part B, 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 that contains the confirmed messages and the DNS and Domain name information.

**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.

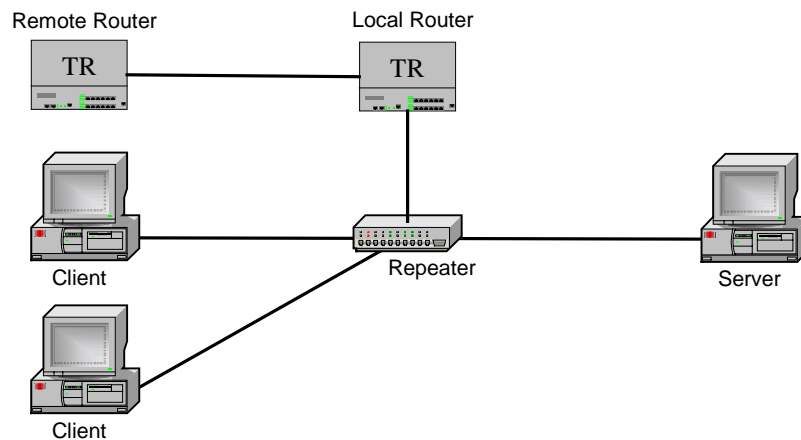
References: IP, 3315

**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 Devices as shown below.



### Procedure:

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

1. Configure the client to disable auto-configuration and enable DHCP.
2. Observe the packet exchange on-link.
3. Confirm that the client received the proper information from the server through the management interface.
4. Do we insert a DNS resolution here to confirm that the info was properly passed??
5. Observe the packets transmitted between the client and the server.

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

6. Configure the client to enable auto-configuration and enable DHCP.
7. Observe the packet exchange on-link.
8. Confirm that the client received the proper information from the server through the management interface.
9. Ping the remote router from the client.
10. Do we insert a DNS resolution here to confirm that the info was properly passed??
11. Observe the packets transmitted between the client and the server.

### Observable Results:

- In Part A, the client should send an information-request message and the servers should both send a reply message with the DNS and Domain name information inside. All devices should remain stable and the client should resolve its address.
- In Part B, 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 servers both respond with a reply message that contains the confirmed messages and the DNS and Domain name information. All devices should remain stable and the client should resolve its address.

Possible Problems: None.

## **GROUP 2: DHCP with Firewalls and Transition Mechanisms**

### **Scope:**

The following tests are designed to verify the functionality of DHCP over different IPv6 transition mechanisms, firewall technologies and VPN tunnels.

### **Overview:**

## Test DHCP.2.1: DHCP over Static IPv6 Tunnels

**Purpose:** To verify that DHCP properly works over static IPv6 tunnels.

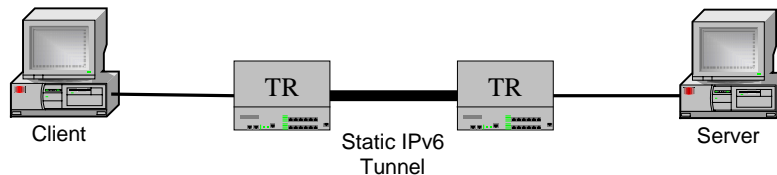
References: IP, 3315

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

**Last Modification:** September 21, 2004

**Discussion:** DHCP should work across any media. In some cases, it may be necessary to have a static IPv6 tunnel between a DHCP server and a DHCP client. This test should confirm that DHCP properly operates in this environment.

**Test Setup:** Connect Devices as shown below. Only configure static routing and IPv4 on the link between the TR devices. Configure a static IPv6 Tunnel over that IPv4 link.



### Procedure:

#### Part A: Four Message Initialization

1. Configure the client to disable auto-configuration and enable DHCP.
2. Observe the packet exchange on-link.
3. Confirm that the client received the proper information from the server through the management interface.
4. Do we insert a DNS resolution here to confirm that the info was properly passed??
5. Observe the packets transmitted between the client and the server.

#### Part B: Two Message Initialization

6. Configure the client to enable auto-configuration and enable DHCP.
7. Observe the packet exchange on-link.
8. Confirm that the client received the proper information from the server through the management interface.
9. Ping the remote router from the client.
10. Do we insert a DNS resolution here to confirm that the info was properly passed??
11. Observe the packets transmitted between the client and the server.

### Observable Results:

- In Part A, the client should send an information-request message and the server should both send a reply message with the DNS and Domain name information inside.
- In Part B, 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 that contains the confirmed messages and the DNS and Domain name information.

**Possible Problems:** None.

## Test DHCP.2.2: DHCP Across IPsec Tunnels

**Purpose:** To verify that DHCP properly works across an IPsec tunnel.

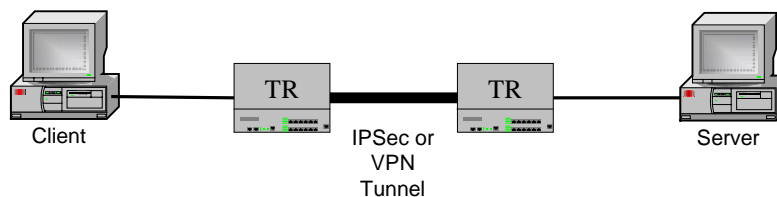
References: IP, 3315

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

**Last Modification:** September 21, 2004

**Discussion:** DHCP should work across any media. In some cases, it may be necessary to have an IPsec or VPN tunnel between a DHCP server and a DHCP client. This test should confirm that DHCP properly operates in this environment.

**Test Setup:** Connect Devices as shown below. Make sure IPv6 is configured on all links with static routing. Ensure an IPsec tunnel is configured between the TR devices.



### Procedure:

#### Part A: Four Message Initialization over an IPsec Tunnel

1. Configure the client to disable auto-configuration and enable DHCP.
2. Observe the packet exchange on-link.
3. Confirm that the client received the proper information from the server through the management interface.
4. Do we insert a DNS resolution here to confirm that the info was properly passed??
5. Observe the packets transmitted between the client and the server.

#### Part B: Two Message Initialization over an IPsec Tunnel

6. Configure the client to enable auto-configuration and enable DHCP.
7. Observe the packet exchange on-link.
8. Confirm that the client received the proper information from the server through the management interface.
9. Ping the remote router from the client.
10. Do we insert a DNS resolution here to confirm that the info was properly passed??
11. Observe the packets transmitted between the client and the server.

### Observable Results:

- In Part A, the client should send an information-request message and the server should both send a reply message with the DNS and Domain name information inside.
- In Part B, 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 that contains the confirmed messages and the DNS and Domain name information.

**Possible Problems:** None.

### Test DHCP.2.3: DHCP across a Stateful Firewall

**Purpose:** To verify that DHCP properly works over a stateful Firewall.

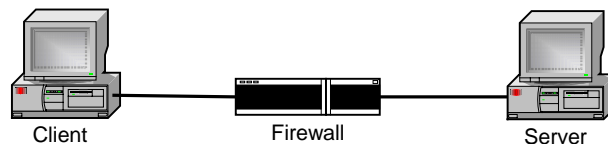
References: IP, 3315

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

**Last Modification:** September 21, 2004

**Discussion:** DHCP should work across a stateful firewall, if the firewall is properly configured. This test should confirm that DHCP properly operates in this environment.

**Test Setup:** Connect Devices as shown below. Properly configure the firewall to allow the DHCP client to access the DHCP server and vice versa.



#### Procedure:

##### *Part A: Four Message Initialization*

1. Configure the client to disable auto-configuration and enable DHCP.
2. Observe the packet exchange on-link.
3. Confirm that the client received the proper information from the server through the management interface.
4. Do we insert a DNS resolution here to confirm that the info was properly passed??
5. Observe the packets transmitted between the client and the server.

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

6. Configure the client to enable auto-configuration and enable DHCP.
7. Observe the packet exchange on-link.
8. Confirm that the client received the proper information from the server through the management interface.
9. Ping the remote router from the client.
10. Do we insert a DNS resolution here to confirm that the info was properly passed??
11. Observe the packets transmitted between the client and the server.

#### Observable Results:

- In Part A, the client should send an information-request message and the server should both send a reply message with the DNS and Domain name information inside.
- In Part B, 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 that contains the confirmed messages and the DNS and Domain name information.

**Possible Problems:** None.