

**Moonv6 Test Suite**

*DNS Interoperability  
Test Suite*

**Technical Document**

Revision 0.2



---

*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 DNS Services.....	8
Test DNS.1.1: Incremental Zone Transfer .....	9
Test DNS.1.2: Entire Zone Transfer .....	10
Test DNS.1.3: DNS Query.....	11
GROUP 2: DNS with Firewalls and Transition Mechanisms .....	13
Test DNS.2.1: IXFR and AXFR over Static IPv6 Tunnels.....	14
Test DNS.2.2: DNS Query over Static IPv6 Tunnels .....	16
Test DNS.2.3: IXFR and AXFR over IPsec Tunnels.....	18
Test DNS.2.4: DNS Query Across IPsec Tunnels.....	20
Test DNS.2.5: IXFR and AXFR across a Stateful Firewall .....	22
Test DNS.2.6: DNS Query across a Stateful Firewall .....	24

*University of New Hampshire  
Interoperability Laboratory*

**MODIFICATION RECORD**

Draft Version Complete  
Version 0.2 Complete

September 27, 2004  
September 29, 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.**

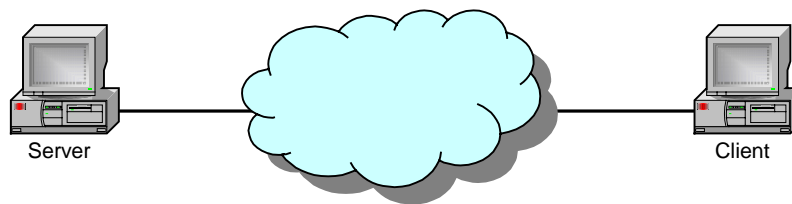
John Brzozowski	Lucent Technologies
Ankur Chadda	University of New Hampshire
Donald Desrosiers	Sun Microsystems
Ralph Droms	Cisco Systems
Alain Durand	Sun Microsystems
Benjamin Schultz	University of New Hampshire

## **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 DNS 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 DNS services over a firewall or IP Tunnel. 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, even if this is not displayed in the figure.

## **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 DNS.1.2 refers to the second test of the first test group in the DNS 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.
  
- [IP] Jon Postel, Editor. Internet Protocol: DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, RFC 791, September 1981.
  
- [UDP] Jon Postel. User Datagram Protocol, RFC 768, August 1980.
  
- [1034] P. Mockapetris. DOMAIN NAMES - CONCEPTS AND FACILITIES, RFC 1034, November 1987.
  
- [1035] P. Mockapetris. DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, RFC 1035, November 1987.
  
- [1995] M. Ohta. Incremental Zone Transfer in DNS, RFC 1995, August 1996.
  
- [3152] R. Bush. Delegation of IP6.ARPA, RFC 3152, August, 2001.
  
- [3363] R. Bush, et. al. Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS), RFC 3363, August 2002.
  
- [3596] S. Thomson, et. al. DNS Extensions to Support IP Version 6, RFC 3596, October, 2003.
  
- [3901] A. Durand and J. Ihen. DNS IPv6 Transport Operational Guidelines, RFC 3901, September, 2004.

## **GROUP 1: Basic DNS Services**

### **Scope:**

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

### **Overview:**

Domain Name System allows host names to be associated with IP addresses. This is essential for network applications to operate in an IPv6 environment.

### **Test DNS.1.1: Incremental Zone Transfer**

**Purpose:** To verify that a server can properly update its zone information.

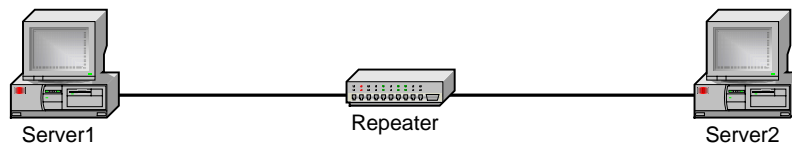
**References:** 1035, 1995

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

**Last Modification:** September 27, 2004

**Discussion:** To optimize propagation of changes to a DNS database, it is necessary to actively notify servers of the change through the DNS NOTIFY extension. The full zone transfer mechanism (AXFR) transfers the entire zone file. Incremental transfer (IXFR) as proposed is a more efficient mechanism, as it transfers only the changed portion(s) of a zone. A secondary name server which requests IXFR is called an IXFR client and a primary or secondary name server that responds to the request is called an IXFR server.

**Test Setup:** Connect Devices as shown below. Ensure that Server1 is configured as the secondary DNS server and Server2 is configured as the primary DNS server.



#### **Procedure:**

##### *Part A: IXFR involving IPv4*

1. Configure Server1 to send an IXFR query over IPv4 for an IPv4 zone to Server2.
2. Observe the packet exchange on-link.

##### *Part B: IXFR involving IPv6*

3. Configure Server1 to send an IXFR query over IPv6 for an IPv6 zone to Server2.
4. Observe the packet exchange on-link.

##### *Part C: IXFR involving Dual-Stack*

5. Configure Server1 to send an IXFR query over IPv4 for an IPv6 zone to Server2.
6. Observe the packet exchange on-link.
7. Configure Server1 to send an IXFR query over IPv6 for an IPv4 zone to Server2.
8. Observe the packet exchange on-link.

#### **Observable Results:**

- In Parts A, B and C, Server1 should send out a proper question to Server2. Server2 should send an answer and begin the IXFR.

**Possible Problems:** None.

### **Test DNS.1.2: Entire Zone Transfer**

**Purpose:** To verify that a server can properly update its zone information.

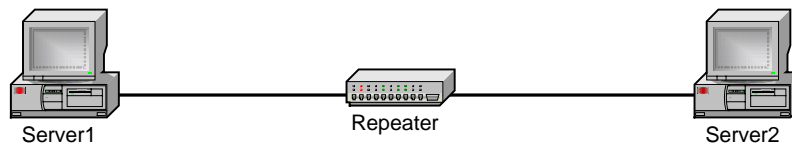
**References:** 1035, 1995

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

**Last Modification:** September 27, 2004

**Discussion:** To propagate changes to a DNS database, it is necessary to actively notify servers of the change through the DNS NOTIFY extension. The full zone transfer mechanism (AXFR) transfers the entire zone file.

**Test Setup:** Connect Devices as shown below. Ensure that Server1 is configured as the secondary DNS server and Server2 is configured as the primary DNS server.



#### **Procedure:**

##### *Part A: AXFR involving IPv4*

1. Configure Server1 to send an AXFR query over IPv4 for an IPv4 zone to Server2.
2. Observe the packet exchange on-link.

##### *Part B: AXFR involving IPv6*

3. Configure Server1 to send an AXFR query over IPv6 for an IPv6 zone to Server2.
4. Observe the packet exchange on-link.

##### *Part C: AXFR involving Dual-Stack*

5. Configure Server1 to send an AXFR query over IPv4 for an IPv6 zone to Server2.
6. Observe the packet exchange on-link.
7. Configure Server1 to send an AXFR query over IPv6 for an IPv4 zone to Server2.
8. Observe the packet exchange on-link.

#### **Observable Results:**

- In Parts A, B and C, Server1 should send out a proper question to Server2. Server2 should send an answer and begin the AXFR.

**Possible Problems:** None.

### **Test DNS.1.3: DNS Query**

**Purpose:** To verify that a device can properly query a DNS server for an IP address.

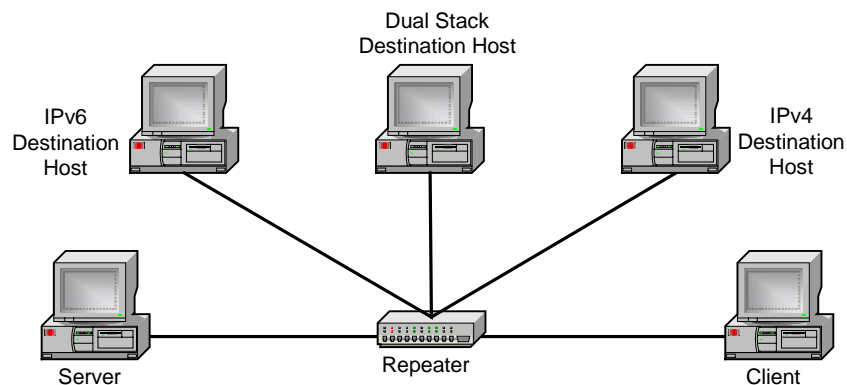
**References:** 1034, 1035

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

**Last Modification:** September 27, 2004

**Discussion:** A host needs to match an IP address to a host name or vice versa if an application is using a name instead of an address. Names are easier for humans to remember and ...

**Test Setup:** Connect Devices as shown below. Ensure the host supports nslookup functionality. Configure the DNS server with the proper files to support the IP address and FQDN mappings for both IPv4 and IPv6. Configure the destination host with the proper address.



#### **Procedure:**

##### *Part A: Forward query involving IPv4*

1. From the host, query the destination host name through nslookup.
2. Observe the packets transmitted between the client and the server.

##### *Part B: Reverse query involving IPv4*

3. From the host, query the destination host IPv4 address through nslookup.
4. Observe the packets transmitted between the client and the server.

##### *Part C: Forward Query involving IPv6*

5. From the host, query the destination host name through nslookup.
6. Observe the packets transmitted between the client and the server.

##### *Part D: Reverse Query involving IPv6*

7. From the host, query the destination host IPv6 address through nslookup.
8. Observe the packets transmitted between the client and the server.

**[NOTE: I am looking for ideas to test Forward/Reverse queries involving Dual Stack]**

*University of New Hampshire  
Interoperability Laboratory*

**Observable Results:**

- In Part A, the client should properly query the DNS server and obtain the IPv4 address. Nslookup should display the proper address.
- In Part B, the client should properly query the DNS server and obtain the hostname. Nslookup should display the proper host name.
- In Part C, the client should properly query the DNS server and obtain the IPv6 address. Nslookup should display the proper address.
- In Part D, the client should properly query the DNS server and obtain the hostname. Nslookup should display the proper host name.

**Possible Problems:** The client may not support nslookup functionality.

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

### **Scope:**

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

### **Overview:**

Transition mechanisms and firewalls will be extensively used in the deployment of IPv6. Ensuring that DNS properly operates over these various technologies is a key step to the progression of IPv6.

### **Test DNS.2.1: IXFR and AXFR over Static IPv6 Tunnels**

**Purpose:** To verify that DNS zone transfers properly work over static IPv6 tunnels.

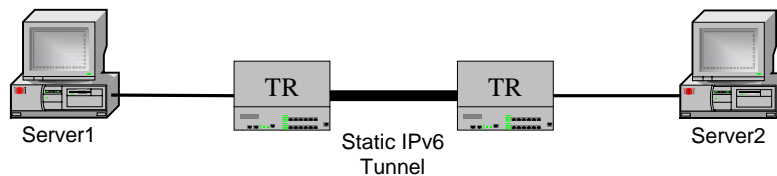
**References:** 1035, 1995

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

**Last Modification:** September 27, 2004

**Discussion:** DNS should work across any media. In some cases, it may be necessary to have a static IPv6 tunnel between two DNS servers. This test should confirm that DNS 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. Ensure that Server1 is configured as the secondary DNS server and Server2 is configured as the primary DNS server.



#### **Procedure:**

##### *Part A: IXFR involving IPv4*

1. Configure Server1 to send an IXFR query over IPv4 for an IPv4 zone to Server2.
2. Observe the packet exchange on-link.

##### *Part B: IXFR involving IPv6*

3. Configure Server1 to send an IXFR query over IPv6 for an IPv6 zone to Server2.
4. Observe the packet exchange on-link.

##### *Part C: IXFR involving Dual-Stack*

5. Configure Server1 to send an IXFR query over IPv4 for an IPv6 zone to Server2.
6. Observe the packet exchange on-link.
7. Configure Server1 to send an IXFR query over IPv6 for an IPv4 zone to Server2.
8. Observe the packet exchange on-link.

##### *Part D: AXFR involving IPv4*

9. Configure Server1 to send an IXFR query over IPv4 for an IPv4 zone to Server2.
10. Observe the packet exchange on-link.

##### *Part E: AXFR involving IPv6*

11. Configure Server1 to send an IXFR query over IPv6 for an IPv6 zone to Server2.
12. Observe the packet exchange on-link.

##### *Part F: AXFR involving Dual-Stack*

13. Configure Server1 to send an IXFR query over IPv4 for an IPv6 zone to Server2.
14. Observe the packet exchange on-link.
15. Configure Server1 to send an IXFR query over IPv6 for an IPv4 zone to Server2.
16. Observe the packet exchange on-link.

#### **Observable Results:**

*University of New Hampshire  
Interoperability Laboratory*

- In Parts A, B and C, Server1 should send out a proper question to Server2. Server2 should send an answer and begin the IXFR.
- In Parts C, D and E, Server1 should send out a proper question to Server2. Server2 should send an answer and begin the AXFR.

**Possible Problems:** None.

## Test DNS.2.2: DNS Query over Static IPv6 Tunnels

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

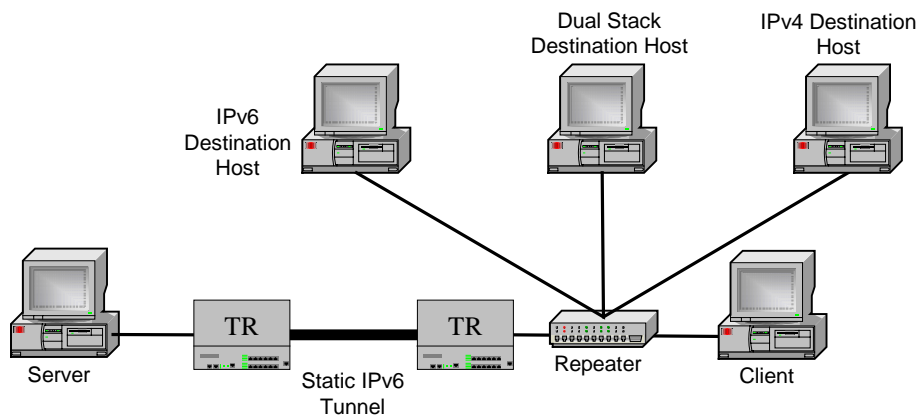
**References:** 1034, 1035

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

**Last Modification:** September 27, 2004

**Discussion:** DNS should work across any media. In some cases, it may be necessary to have a static IPv6 tunnel between two DNS servers. This test should confirm that DNS 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. Ensure the host supports nslookup functionality. Configure the DNS server with the proper files to support the IP address and FQDN mappings for both IPv4 and IPv6. Configure the destination host with the proper address.



### Procedure:

#### Part A: Forward query involving IPv4

1. From the host, query the destination host name through nslookup.
2. Observe the packets transmitted between the client and the server.

#### Part B: Reverse query involving IPv4

3. From the host, query the destination host IPv4 address through nslookup.
4. Observe the packets transmitted between the client and the server.

#### Part C: Forward Query involving IPv6

5. From the host, query the destination host name through nslookup.
6. Observe the packets transmitted between the client and the server.

#### Part D: Reverse Query involving IPv6

7. From the host, query the destination host IPv6 address through nslookup.
8. Observe the packets transmitted between the client and the server.

*University of New Hampshire  
Interoperability Laboratory*

**Observable Results:**

- In Part A, the client should properly query the DNS server and obtain the IPv4 address. Nslookup should be display the proper address.
- In Part B, the client should properly query the DNS server and obtain the hostname. Nslookup should be display the proper host name.
- In Part C, the client should properly query the DNS server and obtain the IPv6 address. Nslookup should be display the proper address.
- In Part D, the client should properly query the DNS server and obtain the hostname. Nslookup should be display the proper host name.

**Possible Problems:** The client may not support nslookup functionality.

### **Test DNS.2.3: IXFR and AXFR over IPsec Tunnels**

**Purpose:** To verify that DNS zone transfers properly work over an IPsec tunnel.

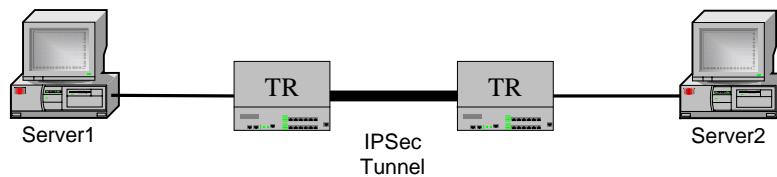
**References:** 1035, 1995

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

**Last Modification:** September 27, 2004

**Discussion:** DNS should work across any media. In some cases, it may be necessary to have a static IPv6 tunnel between two DNS servers. This test should confirm that DNS 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 an IPsec tunnel between the TR devices. Ensure that Server1 is configured as the secondary DNS server and Server2 is configured as the primary DNS server.



#### **Procedure:**

##### *Part A: IXFR involving IPv4*

1. Configure Server1 to send an IXFR query over IPv4 for an IPv4 zone to Server2.
2. Observe the packet exchange on-link.

##### *Part B: IXFR involving IPv6*

3. Configure Server1 to send an IXFR query over IPv6 for an IPv6 zone to Server2.
4. Observe the packet exchange on-link.

##### *Part C: IXFR involving Dual-Stack*

5. Configure Server1 to send an IXFR query over IPv4 for an IPv6 zone to Server2.
6. Observe the packet exchange on-link.
7. Configure Server1 to send an IXFR query over IPv6 for an IPv4 zone to Server2.
8. Observe the packet exchange on-link.

##### *Part D: AXFR involving IPv4*

9. Configure Server1 to send an IXFR query over IPv4 for an IPv4 zone to Server2.
10. Observe the packet exchange on-link.

##### *Part E: AXFR involving IPv6*

11. Configure Server1 to send an IXFR query over IPv6 for an IPv6 zone to Server2.
12. Observe the packet exchange on-link.

##### *Part F: AXFR involving Dual-Stack*

13. Configure Server1 to send an IXFR query over IPv4 for an IPv6 zone to Server2.
14. Observe the packet exchange on-link.
15. Configure Server1 to send an IXFR query over IPv6 for an IPv4 zone to Server2.
16. Observe the packet exchange on-link.

*University of New Hampshire  
Interoperability Laboratory*

**Observable Results:**

- In Parts A, B and C, Server1 should send out a proper question to Server2. Server2 should send an answer and begin the IXFR.
- In Parts C, D and E, Server1 should send out a proper question to Server2. Server2 should send an answer and begin the AXFR.

**Possible Problems:** None.

### **Test DNS.2.4: DNS Query Across IPSec Tunnels**

**Purpose:** To verify that DNS properly works across an IPSec tunnel.

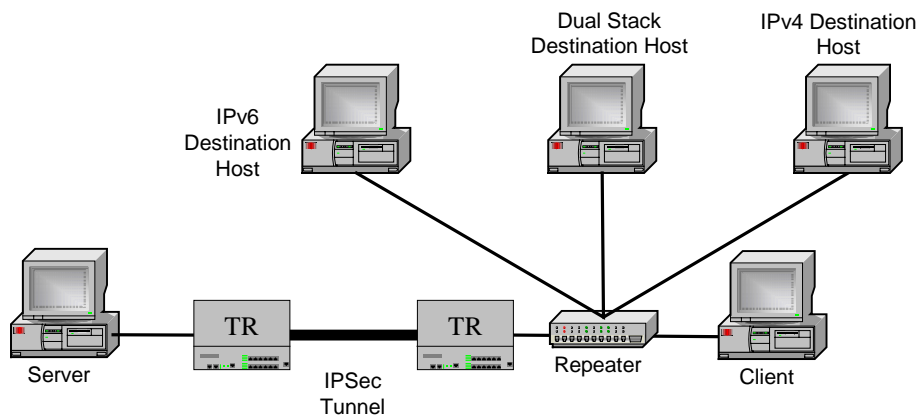
**References:** 1034, 1035

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

**Last Modification:** September 27, 2004

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

**Test Setup:** Connect Devices as shown below. Make sure IPv6 is configured on all links with static routing. Configure an IPSec tunnel between the TR devices. Ensure the host supports a nslookup functionality. Configure the DNS server with the proper files to support the IP address and FQDN mappings for both IPv4 and IPv6. Configure the destination host with the proper address.



#### **Procedure:**

##### *Part A: Forward query involving IPv4*

1. From the host, query the destination host name through nslookup.
2. Observe the packets transmitted between the client and the server.

##### *Part B: Reverse query involving IPv4*

3. From the host, query the destination host IPv4 address through nslookup.
4. Observe the packets transmitted between the client and the server.

##### *Part C: Forward Query involving IPv6*

5. From the host, query the destination host name through nslookup.
6. Observe the packets transmitted between the client and the server.

##### *Part D: Reverse Query involving IPv6*

7. From the host, query the destination host IPv6 address through nslookup.
8. Observe the packets transmitted between the client and the server.

*University of New Hampshire  
Interoperability Laboratory*

**Observable Results:**

- In Part A, the client should properly query the DNS server and obtain the IPv4 address. Nslookup should be display the proper address.
- In Part B, the client should properly query the DNS server and obtain the hostname. Nslookup should be display the proper host name.
- In Part C, the client should properly query the DNS server and obtain the IPv6 address. Nslookup should be display the proper address.
- In Part D, the client should properly query the DNS server and obtain the hostname. Nslookup should be display the proper host name.

**Possible Problems:** The client may not support nslookup functionality.

### **Test DNS.2.5: IXFR and AXFR across a Stateful Firewall**

**Purpose:** To verify that DNS zone transfers properly work across a stateful Firewall.

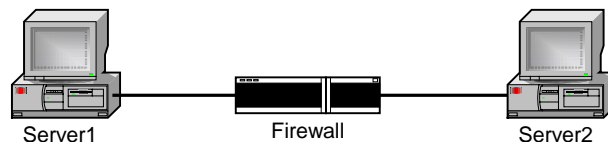
**References:** 1035, 1995

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

**Last Modification:** September 27, 2004

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

**Test Setup:** Connect Devices as shown below. Properly configure the firewall to allow the DNS servers to access each other.



#### **Procedure:**

##### *Part A: IXFR involving IPv4*

1. Configure Server1 to send an IXFR query over IPv4 for an IPv4 zone to Server2.
2. Observe the packet exchange on-link.

##### *Part B: IXFR involving IPv6*

3. Configure Server1 to send an IXFR query over IPv6 for an IPv6 zone to Server2.
4. Observe the packet exchange on-link.

##### *Part C: IXFR involving Dual-Stack*

5. Configure Server1 to send an IXFR query over IPv4 for an IPv6 zone to Server2.
6. Observe the packet exchange on-link.
7. Configure Server1 to send an IXFR query over IPv6 for an IPv4 zone to Server2.
8. Observe the packet exchange on-link.

##### *Part D: AXFR involving IPv4*

9. Configure Server1 to send an IXFR query over IPv4 for an IPv4 zone to Server2.
10. Observe the packet exchange on-link.

##### *Part E: AXFR involving IPv6*

11. Configure Server1 to send an IXFR query over IPv6 for an IPv6 zone to Server2.
12. Observe the packet exchange on-link.

##### *Part F: AXFR involving Dual-Stack*

13. Configure Server1 to send an IXFR query over IPv4 for an IPv6 zone to Server2.
14. Observe the packet exchange on-link.
15. Configure Server1 to send an IXFR query over IPv6 for an IPv4 zone to Server2.
16. Observe the packet exchange on-link.

#### **Observable Results:**

- In Parts A, B and C, Server1 should send out a proper question to Server2. Server2 should send an answer and begin the IXFR.
- In Parts C, D and E, Server1 should send out a proper question to Server2. Server2 should send an answer and begin the AXFR.

*University of New Hampshire  
Interoperability Laboratory*

**Possible Problems:** None.

## Test DNS.2.6: DNS Query across a Stateful Firewall

**Purpose:** To verify that DNS properly works across a stateful Firewall.

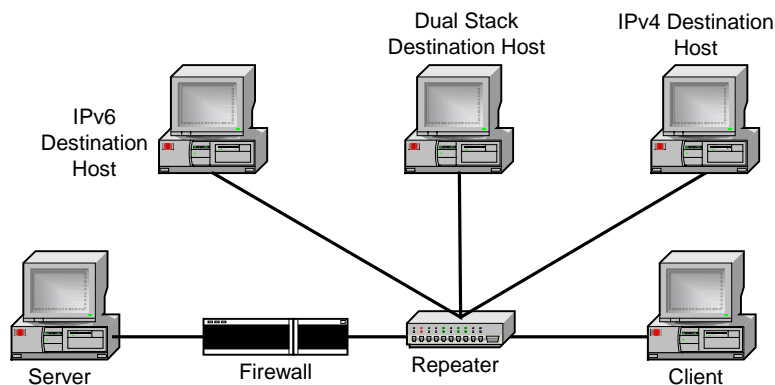
**References:** 1034, 1035

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

**Last Modification:** September 27, 2004

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

**Test Setup:** Connect Devices as shown below. Properly configure the firewall to allow the DNS servers to access each other.



### Procedure:

#### Part A: Forward query involving IPv4

1. From the host, query the destination host name through nslookup.
2. Observe the packets transmitted between the client and the server.

#### Part B: Reverse query involving IPv4

3. From the host, query the destination host IPv4 address through nslookup.
4. Observe the packets transmitted between the client and the server.

#### Part C: Forward Query involving IPv6

5. From the host, query the destination host name through nslookup.
6. Observe the packets transmitted between the client and the server.

#### Part D: Reverse Query involving IPv6

7. From the host, query the destination host IPv6 address through nslookup.
8. Observe the packets transmitted between the client and the server.

### Observable Results:

- In Part A, the client should properly query the DNS server and obtain the IPv4 address. Nslookup should be display the proper address.
- In Part B, the client should properly query the DNS server and obtain the hostname. Nslookup should be display the proper host name.
- In Part C, the client should properly query the DNS server and obtain the IPv6 address. Nslookup should be display the proper address.

*University of New Hampshire  
Interoperability Laboratory*

- In Part D, the client should properly query the DNS server and obtain the hostname. Nslookup should be display the proper host name.

**Possible Problems:** The client may not support nslookup functionality.