IPv6 Ready

Core Protocols Interoperability Test Specification

Technical Document
Revision 5.1.0

IPv6 Forum *http://www.ipv6forum.org*
Converged Test Specification *http://www.ipv6ready.org*
TAHI Project (Japan)
UNH InterOperability Lab (USA)

© 2026 University of New Hampshire InterOperability Laboratory, Yokogawa Electric Corporation, and IPv6 Forum



Table of Contents

Acknowledgements *3*

Introduction *4*

Definitions *5*

Test Organization *6*

References *7*

General Node Requirements *9*

Test Performed on Host/Router/CN *10*

Advanced Functionality Tests *12*

Possible Problem Summary *13*

Group 1: IPv6 Core Protocol and ICMPv6 Interoperability *14*

Test IP6Interop.1.1: ICMPv6 Echo Interoperability **15**

Test IP6Interop.1.2: Address Autoconfiguration and Duplicate Address Detection **21**

Test IP6Interop.1.3: Processing Router Advertisements - Prefix Discovery **27**

Test IP6Interop.1.4: Processing Router Advertisements- Router Lifetime **30**

Test IP6Interop.1.5: Redirect Function (Host vs Router) **32**

Test IP6Interop.1.6: Path MTU Discovery and Fragmentation **34**

Test IP6Interop.1.7: Processing Router Advertisements- Router Preference **40**

Test IP6Interop.1.8: Processing Router Advertisements- Route Information Option **43**

Test IP6Interop.1.9: Processing Router Advertisements- DNS **47**

Modification Record *50*



Acknowledgements

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

Principle Authors:

University of New Hampshire- InterOperability Lab
Tahi Project

Commentators:

IRISA-INRIA
TTA/IT Testing Laboratory
BII Group
CHT-TL
CNLabs



Introduction

The IPv6 Forum serves as the principal industry body responsible for coordinating the development and global deployment of IPv6, the next-generation Internet Protocol. Unlike IPv4, which was developed and validated within a limited group of implementers, IPv6 has been adopted across a vast and diverse range of implementations worldwide. As a result, ensuring interoperability among these implementations is a fundamental requirement for the continued reliability and growth of the Internet.

To address this requirement, the IPv6 Forum established the IPv6 Ready Logo Program — a unified certification framework designed to provide the market with a verifiable and consistent measure of IPv6 conformance and interoperability. Certification under this program indicates that a product has successfully satisfied the interoperability test requirements defined herein, and that its IPv6 implementation is operationally ready for deployment. The program provides assurance to end users, network engineers, and procurement bodies that certified products will interoperate reliably within IPv6-enabled environments.

This document defines the Core Interoperability test plan used as the basis for IPv6 Ready Logo certification. Like the Core Conformance test plan, it defines the requirements for hosts, routers and constrained nodes. It is intended for use by accredited testing laboratories conducting interoperability evaluations, as well as by implementers seeking to understand the technical requirements against which their products will be assessed.

Definitions

CallBox	Test equipment that emulates a cellular base station and core network.
CN	Constrained Node
DAD	Duplicate Address Detection
HUT	Host Under Test
MTU	Maximum Transmission Unit
NCE	Neighbor Cache Entry
NUT	Node Under Test
RUT	Router Under Test
TLLA	Target Link-layer Address
TN	Test Node
TR	Test Router

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** is the first line of the test page. It will have the following form: IP.IOP.A.B Where each component indicates the following: IP – Test Suite Identifier IOP – Interoperability Test Suite A – Group Number B – Test Number Scripts implementing this test suite should follow this convention, and may also append a character in the set [a-z] indicating a particular test part.
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.
Advanced Functionality	The **Advanced Functionality** gives an indication of whether the test case is covered by one or more optional functions as defined in the Advanced Functionality Tests. These tests may be omitted if the functionality is not supported by the Node Under Test. If this is not in a test case, there are no advanced functionalities listed.
References	The **References** section lists cross-references to the specifications and documentation that might be helpful in understanding and evaluating the test and results
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 and Expected Behavior	The **Procedure and Expected Behavior** table 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 of expected behavior, as needed, as not all steps require observation of results. If any behavior is expected for a procedure, it is to be observed prior to continuing to the next step. Failure to observe any behavior prior to continuing constitutes a failed test. Note, that while test numbers continue between test parts, each test part is to be executed independently (Following Common Test Setup and Cleanup as indicated), and are not cascaded from the previous part.
Possible Problems	The **Possible Problems** 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 these texts:

[SLAAC] Thomson, S., T. Narten, T. Jinmei, IPv6 Stateless Address Autoconfiguration, RFC 4862, September 2007.

[DS-FIELD] Nichols, K., S. Blake, F. Baker, and D. Black, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, RFC 2474, December 1998.

[ECN] Ramakrishnan, K., S. Floyd, and D. Black, The Addition of Explicit Congestion Notification (ECN) to IP, RFC 3168, September 2001.

[ICMPv6] Conta, A., S. Deering M. Gupta, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, RFC 4443, March 2006.

[IPv6-ARCH] Hinden, R., S. Deering, Internet Protocol, Version 6 Addressing Architecture, RFC 4291, February 2006.

[IPv6-SPEC] Hinden, R., S. Deering, Internet Protocol, Version 6 (IPv6) Specification, RFC 8200, July 2017.

[ND] Narten, T., Nordmark, E., and W. Simpson, H. Soliman, Neighbor Discovery for IP Version 6 (IPv6), RFC 4861, September 2007.

[PMTU] McCann, J., S. Deering, J. Mogul, and R. Hinden, Path MTU Discovery for IPv6, RFC 8201, July 2017.

[RFC-5095] Abley. J, Savola, P. Neville-Neil, G. Deprecation of Type 0 Routing Headers in IPv6, RFC 5095, December 2007.

[RFC-4191] R. Draves, D. Thaler, Default Router Preferences and More-Specific Routes, RFC 4191, November 2005.

[RFC-6980] F. Gont, Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery, RFC 6980, August 2013.

[STABLE-ID] F. Gont, A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC), RFC 7217, April 2014.

[RA-DNS] J.Jeong, S. Park, L.Beloeil, and S.Mandadapalli, IPv6 Router Advertisement Options for DNS Configuration, RFC 8106, March 2017.

[RFC-7228] C. Bormann, M. Ersue, A. Keranen. “Terminology for Constrained-Node Networks”. RFC 7228, May 2014.

General Node Requirements

- Host
  - Ability to configure the following information by receipt of Router Advertisement:
    - Global Address
    - Default Router
    - DNS Information
- Router
  - Ability to transmit and configure Router Advertisements with a positive AdvValidLifetime and AdvPreferredLifetime.
  - Ability to transmit and configure Router Advertisements with a positive AdvDefaultLifetime.
  - Ability to transmit and configure Router Advertisements containing DNS Server and DNS Search List.
  - Ability to transmit and configure Router Advertisements containing Default Router Preference.
- CallBox
  - Ability to assign IPv6 address and other information to CN which attaches with it.
  - Ability to switch the packets between nodes and CN.
- CN
  - A node which supports constrained IPv6.
  - Ability to obtain IPv6 addresses from CallBox.
- Host, Router and CN
  - Ability to use a ping6 application and print out results indicating the receipt of an ICMPv6 Echo Reply.
  - Ability to show multicast ping results indicating the receipt of each ICMPv6 Echo Reply.
  - SHOULD support all-nodes multicast address (FF02::1), must support transmit of all-routers multicast address (FF02::2) Echo Request.

Test Performed on Host/Router/CN

The tests under the Host/Router/CN column marked by an "X" must be performed as specified below. If there is no "X" listed under the Host/Router/CN column, this test may be omitted.

Test Case	Host	Router	CN
IP6Interop.1.1a	X	-	X
IP6Interop.1.1b	X	-	X
IP6Interop.1.1c	X	-	X
IP6Interop.1.1d	X	X	X
IP6Interop.1.1e	X	X	X
IP6Interop.1.1f	X	X	X
IP6Interop.1.1g	-	X	-
IP6Interop.1.1h	-	X	-
IP6Interop.1.1i	-	X	-
IP6Interop.1.2a	X	-	-
IP6Interop.1.2b	X	-	-
IP6Interop.1.2c	X	X	-
IP6Interop.1.2d	X	X	-
IP6Interop.1.2e	-	X	-
IP6Interop.1.2f	-	X	-
IP6Interop.1.3a	X	X	-
IP6Interop.1.3b	X	X	-
IP6Interop.1.3c	X	X	-
IP6Interop.1.4a	X	X	-
IP6Interop.1.4b	X	X	-
IP6Interop.1.5	X	X	-
IP6Interop.1.6a	X	X	-
IP6Interop.1.6b	-	X	-
IP6Interop.1.6c	X	-	-
IP6Interop.1.6d	X	X	-
IP6Interop.1.6e	-	X	-
IP6Interop.1.7a	X	X	-
IP6Interop.1.7b	X	X	-
IP6Interop.1.7c	X	X	-
IP6Interop.1.7d	X	X	-
IP6Interop.1.8a	X	X	-
IP6Interop.1.8b	X	X	-
IP6Interop.1.8c	X	X	-
IP6Interop.1.8d	X	X	-
IP6Interop.1.8e	X	X	-
IP6Interop.1.9a	X	X	-

Test Case	Host	Router	CN
IP6Interop.1.9b	X	X	-
IP6Interop.1.9c	X	X	-
IP6Interop.1.9d	X	X	-

Advanced Functionality Tests

The following tests may be omitted if the NUT does not support the advanced functionalities.

Transmitting Echo Requests (Passive Node):
IP6Interop.1.9

Processing Route Information Options (RFC 4191 Type C Host):
IP6Interop.1.8

Router Advertisement DNS (Host Only):
IP6Interop.1.9

Possible Problem Summary

The following test cases have documented possible problems that allow for altered or omitted steps in their procedures. Please see each specific test case listed for more information:

- IP6Interop.1.1: ICMPv6 Echo Interoperability
- IP6Interop.1.3: Processing Router Advertisements – Prefix Discovery
- IP6Interop.1.6: Path MTU Discovery and Fragmentation
- IP6Interop.1.9: Processing Router Advertisements - DNS

Group 1: IPv6 Core Protocol and ICMPv6 Interoperability

Scope

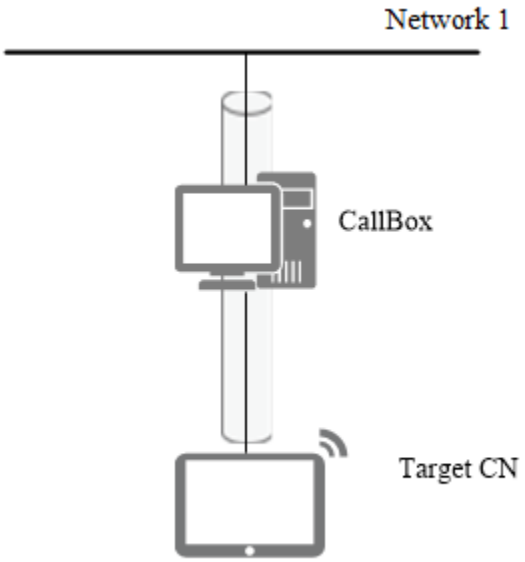
Tests in this group verify that the target devices are able to engage in various aspects of the base IPv6 protocol.

Overview

The following tests verify operations such as ICMPv6, stateless address autoconfiguration, on-link determination, Duplicate Address Detection, path MTU discovery, fragmentation, redirects, communication when configured with multiple prefixes, network renumbering, DNS Servers, DNS Search List, and default router selection.

Setup for CN

If the applicant is a CN device, there must be a CallBox connection between the Network 1 and the CN. The following connection replaces TAR-Host1.



Test IP6Interop.1.1: ICMPv6 Echo Interoperability

Purpose: To verify that a successful ICMPv6 Echo Request, Echo Reply exchange can be achieved in two directions.

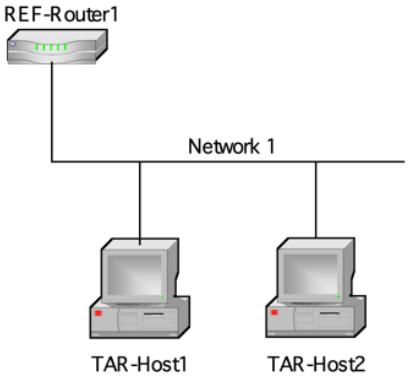
Reference:

- [ICMPv6] – Section 4
- [IPv6-Arch] – Section 2.8

Node Requirements: See General Node Requirements.

Test Setup: For each Part, connect hosts and routers as per the figures below. Allow time for all devices to perform stateless address autoconfiguration and Duplicate Address Detection.

Parts A-C:

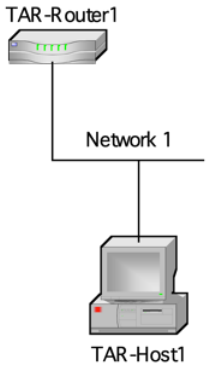


TAR-Host1: Applicant

TAR-Host2: Vendor A/B Host

REF-Router1: any router

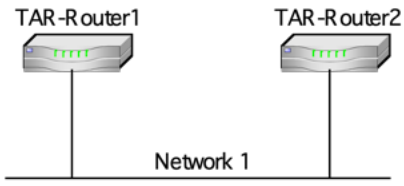
Parts D-F:



TAR-Router1: Applicant (if router) or Vendor C/D Router

TAR-Host1: Applicant (if host) or Vendor A/B Host

Parts G-I



TAR-Router1: Applicant
TAR-Router2: Vendor C/D Router

Procedure:

Part A: Link-Local unicast address (Host vs Host)

Step	Action	Expected Behavior
1.	Transmit ICMPv6 Echo Requests from TAR-Host1 to the link-local address of TAR-Host2.	TAR-Host2 must receive all the ICMPv6 Echo Requests sent from TAR-Host1 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to the Destination Address that was in the Echo Request, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.
2.	Transmit ICMPv6 Echo Requests from TAR-Host2 to the link-local address of TAR-Host1	TAR-Host1 must receive all the ICMPv6 Echo Requests sent from TAR-Host2 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to the Destination Address that was in the Echo Request, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.

Part B: Global Unicast Address (Host vs Host)

Step	Action	Expected Behavior
3.	Transmit ICMPv6 Echo Requests from TAR-Host1 to the Global unicast address of TAR-Host2.	TAR-Host2 must receive all the ICMPv6 Echo Requests sent from TAR-Host1 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to the Destination Address that was in the Echo Request, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.
4.	Transmit ICMPv6 Echo Requests from TAR-Host2 to the Global unicast address of TAR-Host1.	TAR-Host1 must receive all the ICMPv6 Echo Requests sent from TAR-Host2 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to the Destination Address that was in the Echo Request, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.

Part C: Multicast Address (Host vs Host)

Step	Action	Expected Behavior
5.	Disable REF-Router1's interface on Network1.	

6.	Transmit ICMPv6 Echo Requests from TAR-Host1 to the All Nodes multicast address (FF02::1).	TAR-Host2 should receive all the ICMPv6 Echo Requests sent from TAR-Host1 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to TAR-Host2's address, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.
7.	Transmit ICMPv6 Echo Requests from TAR-Host2 to the All Nodes multicast address (FF02::1).	TAR-Host1 should receive all the ICMPv6 Echo Requests sent from TAR-Host2 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to TAR-Host1's address, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.

Part D: Link-Local Unicast Address (Host vs Router)

Step	Action	Expected Behavior
8.	Transmit ICMPv6 Echo Requests from TAR-Host1 to the link-local address of TAR-Router1.	TAR-Router1 must receive all the ICMPv6 Echo Requests sent from TAR-Host1 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to the Destination Address that was in the Echo Request, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.
9.	Transmit ICMPv6 Echo Requests from TAR-Router1 to the link-local address of the TAR-Host1.	TAR-Host1 must receive all the ICMPv6 Echo Requests sent from TAR-Router1 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to the Destination Address that was in the Echo Request, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.

Part E: Global Unicast Address (Host vs Router)

Step	Action	Expected Behavior
10.	Transmit ICMPv6 Echo Requests from TAR-Host1 to the Global unicast address of TAR-Router1.	TAR-Router1 must receive all the ICMPv6 Echo Requests sent from TAR-Host1 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to the Destination Address that was in the Echo Request, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.
11.	Transmit ICMPv6 Echo Requests from TAR-Router1 to the Global unicast address of the TAR-Host1.	TAR-Host1 must receive all the ICMPv6 Echo Requests sent from TAR-Router1 and respond with ICMPv6 Echo Replies. The

		Source Address of the Echo Reply must be equal to the Destination Address that was in the Echo Request, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.

Part F: Multicast Address (Host vs Router)

Step	Action	Expected Behavior
12.	Transmit ICMPv6 Echo Requests from TAR-Host1 to the All Nodes multicast address (FF02::1).	TAR-Router1 should receive all the ICMPv6 Echo Requests sent from TAR-Host1 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to TAR-Router1's address, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.
13.	Transmit ICMPv6 Echo Requests from TAR-Router1 to the All Nodes multicast address (FF02::1).	TAR-Host1 should receive all the ICMPv6 Echo Requests sent from TAR-Router1 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to TAR-Host1's address, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.
14.	Transmit ICMPv6 Echo Requests from TAR-Host1 to the All Routers multicast address (FF02::2).	TAR-Router1 should receive all the ICMPv6 Echo Requests sent from TAR-Host1 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to TAR-Router1's address, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.

Part G: Link-Local Unicast Address (Router vs Router)

Step	Action	Expected Behavior
15.	Transmit ICMPv6 Echo Requests from TAR-Router1 to the link-local address of TAR-Router2.	TAR-Router2 must receive all the ICMPv6 Echo Requests sent from TAR-Router1 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to the Destination Address that was in the Echo Request, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.
16.	Transmit ICMPv6 Echo Requests from TAR-Router2 to the link-local address of TAR-Router1.	TAR-Router1 must receive all the ICMPv6 Echo Requests sent from TAR-Router2 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to the Destination Address that was in the Echo Request, and the Destination Address of the Echo Reply must be equal to

		the Source Address that was in the Echo Request.

Part H: Global Unicast Address (Router vs Router)

Step	Action	Expected Behavior
17.	Transmit ICMPv6 Echo Requests from TAR-Router1 to the Global unicast address of TAR-Router2.	TAR-Router2 must receive all the ICMPv6 Echo Requests sent from TAR-Router1 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to the Destination Address that was in the Echo Request, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.
18.	Transmit ICMPv6 Echo Requests from TAR-Router2 to the Global unicast address of TAR-Router1.	TAR-Router1 must receive all the ICMPv6 Echo Requests sent from TAR-Router2 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to the Destination Address that was in the Echo Request, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.

Part I: Multicast Address (Router vs Router)

Step	Action	Expected Behavior
19.	Transmit ICMPv6 Echo Requests from TAR-Router1 to the All Nodes multicast address (FF02::1).	TAR-Router2 should receive all the ICMPv6 Echo Requests sent from TAR-Router1 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to TAR-Router2's address, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.
20.	Transmit ICMPv6 Echo Requests from TAR-Router2 to the All Nodes multicast address (FF02::1).	TAR-Router1 should receive all the ICMPv6 Echo Requests sent from TAR-Router2 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to TAR-Router1's address, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.
21.	Transmit ICMPv6 Echo Requests from TAR-Router1 to the All Routers multicast address (FF02::2).	TAR-Router2 should receive all the ICMPv6 Echo Requests sent from TAR-Router1 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to TAR-Router2's address, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.

22.	Transmit ICMPv6 Echo Requests from TAR-Router2 to the All Routers multicast address (FF02::2).	TAR-Router1 should receive all the ICMPv6 Echo Requests sent from TAR-Router2 and respond with ICMPv6 Echo Replies. The Source Address of the Echo Reply must be equal to TAR-Router1's address, and the Destination Address of the Echo Reply must be equal to the Source Address that was in the Echo Request.

Possible Problems:

- A passive node may not implement an application for sending Echo Requests.
- Interoperability Partners may not support multicast ping.
    - Part C, if TAR-Host2 doesn't support responding to multicast requests, Step 6 may be omitted.
    - Part F, if TAR-Host1 doesn't support responding to multicast requests, Step 13 may be omitted.
    - Part I, if TAR-Router2 doesn't support responding to multicast requests, Steps 19 and 21 may be omitted.
- CN may not support responding to Echo Requests with an IPv6 Link-Local address, Steps 2, 6, 9, and 12 may be omitted.

Test IP6Interop.1.2: Address Autoconfiguration and Duplicate Address Detection

Purpose: To verify that a device can properly initialize on a network and communicate with other on-link partners.

Reference:

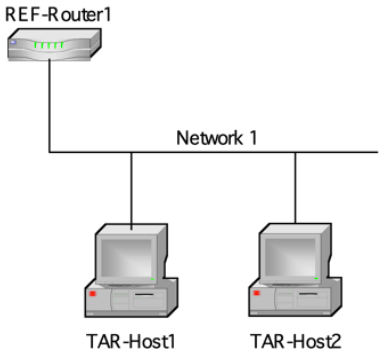
- [SLAAC] – Section 1, 5.4
- [STABLE-ID] – Section 5, 6

Node Requirements: See General Node Requirements.

- TAR-Host2 - Must support the manual configuration of an address.
- TAR-Router2 - Must support the manual configuration of an address.
- REF-Router1 - Must support clearing Neighbor Cache Entries.
- REF-Host1 - Must support clearing Neighbor Cache Entries.
- REF-Host2 - Must support clearing Neighbor Cache Entries.

Test Setup: Connect all devices as per the figure below.

For Parts A-B

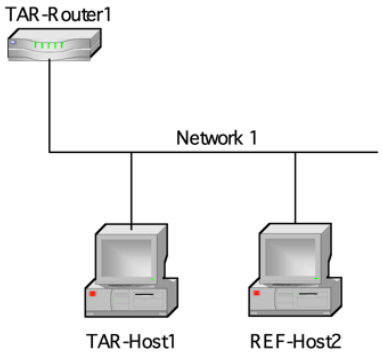


TAR-Host1: Applicant

TAR-Host2: Vendor A/B Host

REF-Router1: any Router

For Parts C-D:

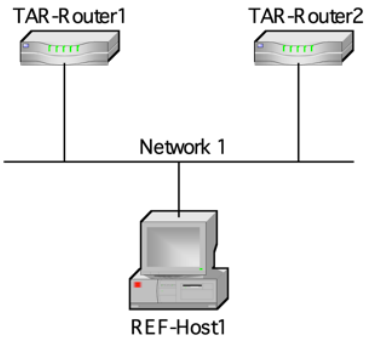


TAR-Router1: Applicant (if router) or Vendor C/D Router

TAR-Host1: Applicant (if host) or Vendor A/B Host

REF-Host2: any Host

For Parts E-F:



TAR-Router1: Applicant
TAR-Router2: Vendor C/D Router
REF-Host1: any Host

Procedure:

Part A: Duplicate Address Detection- Tentative Address Unique (Host vs Host)

Step	Action	Expected Behavior
1.	Disable all interfaces connected to Network1.	
2.	Enable all interfaces on Network1, enabling TAR-Host1 before TAR-Host2.	
3.	Allow time for all devices on Network1 to perform Stateless Address Autoconfiguration and Duplicate Address Detection. Enable REF-Router1 making sure it has cleared its neighbor cache.	
4.	Transmit ICMPv6 Echo Request from REF-Router1 to the Link-Local Address of TAR-Host1.	TAR-Host1 must respond to any Neighbor Solicitations transmitted by REF-Router1 by transmitting a Neighbor Advertisement. TAR-Host1 must respond to the ICMPv6 Echo Requests transmitted by REF-Router1.
5.	Transmit ICMPv6 Echo Request from REF-Router1 to the Link-Local Address of TAR-Host2.	TAR-Host2 must respond to any Neighbor Solicitations transmitted by REF-Router1 by transmitting a Neighbor Advertisement. TAR-Host2 must respond to the ICMPv6 Echo Requests transmitted by REF-Router1.
6.	Repeat Steps 1 through 5, but in Step 2 enable TAR-Host2 before TAR-Host1.	

Part B: Duplicate Address Detection- Tentative Address Duplicated (Host vs Host)

Step	Action	Expected Behavior
7.	Disable all interfaces connected to Network1.	

8.	Configure TAR-Host2 to have the same Link-local Address as TAR-Host1.	
9.	Enable all interfaces on Network1, enabling TAR-Host2 before TAR-Host1.	
10.	Allow time for all devices to perform Stateless Address Autoconfiguration and Duplicate Address Detection. Enable REF-Router1 making sure it has cleared its neighbor cache.	
11.	Transmit ICMPv6 Echo Request from REF-Router1 to the Link-Local Address of TAR-Host1.	TAR-Host2 must respond to any Neighbor Solicitations transmitted by REF-Router1 by transmitting a Neighbor Advertisement. TAR-Host2, and not TAR-Host1, must respond to the ICMPv6 Echo Requests transmitted by REF-Router1.
12.	Allow time for TAR-Host 1 to perform Stateless Address Autoconfiguration and Duplicate Address Detection on a different address then Step 10. Enable REF-Router1 making sure it has cleared its neighbor cache.	
13.	Transmit ICMPv6 Echo Request from REF-Router1 to the Link-Local Address of TAR-Host1 in Step 12.	TAR-Host1 must respond to any Neighbor Solicitations transmitted by REF-Router1 by transmitting a Neighbor Advertisement.
14.	Disable all interfaces connected to Network1.	
15.	Enable all interfaces on Network1, enabling TAR-Host1 before TAR-Host2.	
16.	Allow time for all devices to perform Stateless Address Autoconfiguration and Duplicate Address Detection. Enable REF-Router1 making sure it has cleared its neighbor cache.	
17.	Transmit ICMPv6 Echo Request from REF-Router1 to the Link-Local Address of TAR-Host2.	TAR-Host1 must respond to any Neighbor Solicitations transmitted by REF-Router1 by transmitting a Neighbor Advertisement. TAR-Host1, and not TAR-Host2, must respond to the ICMPv6 Echo Requests transmitted by REF-Router1.
18.	Allow time for TAR-Host 2 to perform Stateless Address Autoconfiguration and Duplicate Address Detection on a different address then Step 16. Enable REF-Router1 making sure it has cleared its neighbor cache.	
19.	Transmit ICMPv6 Echo Request from REF-Router1 to the Link-Local Address of TAR-Host2 in Step 18.	TAR-Host2 must respond to any Neighbor Solicitations transmitted by REF-Router1 by transmitting a Neighbor Advertisement.

Part C: Duplicate Address Detection- Tentative Address Unique (Host vs Router)

Step	Action	Expected Behavior
20.	Disable all interfaces connected to Network1.	
21.	Enable all interfaces on Network1, enabling TAR-Host1 before TAR-Router1.	
22.	Allow time for all devices on Network1 to perform Stateless Address Autoconfiguration and Duplicate Address Detection. Enable REF-Host2 making sure it has cleared its neighbor cache.	
23.	Transmit ICMPv6 Echo Request from REF-Host2 to the Link-Local Address of TAR-Host1.	TAR-Host1 must respond to any Neighbor Solicitations transmitted by REF-Host2 by transmitting a Neighbor Advertisement. TAR-Host1 must respond to the ICMPv6 Echo Requests transmitted by REF-Host2
24.	Transmit ICMPv6 Echo Request from REF-Host2 to the Link-Local Address of TAR-Router1.	TAR-Router1 must respond to any Neighbor Solicitations transmitted by REF-Host2 by transmitting a Neighbor Advertisement. TAR-Router1 must respond to the ICMPv6 Echo Requests transmitted by REF-Host2
25.	Repeat Steps 20 through 24, but in Step 21 enable TAR-Router1 before TAR-Host1.	

Part D: Duplicate Address Detection- Tentative Address Duplicated (Host vs Router)

Step	Action	Expected Behavior
26.	Disable all interfaces connected to Network1.	
27.	Configure TAR-Router1 or TAR-Host1 to have the same address as the other.	
28.	Enable all interfaces on Network1, enabling TAR-Router1 before TAR-Host1.	
29.	Allow time for all devices to perform Stateless Address Autoconfiguration and Duplicate Address Detection. Enable REF-Host2 making sure it has cleared its neighbor cache.	
30.	Transmit ICMPv6 Echo Request from REF-Host2 to the Link-Local Address of TAR-Host1.	TAR-Router1 must respond to any Neighbor Solicitations transmitted by REF-Host2 by transmitting a Neighbor Advertisement. TAR-Router1, and not TAR-Host1, must respond to the ICMPv6 Echo Requests transmitted by REF-Host2.
31.	Allow time for TAR-Host 1 to perform Stateless Address	

	Autoconfiguration and Duplicate Address Detection on a different address then Step 29. Enable REF-Router1 making sure it has cleared its neighbor cache.	
32.	Transmit ICMPv6 Echo Request from REF-Host2 to the Link-Local Address of TAR-Host1 in Step 12.	TAR-Host1 must respond to any Neighbor Solicitations transmitted by REF-Host2 by transmitting a Neighbor Advertisement.
33.	Disable all interfaces connected to Network1.	
34.	Enable all interfaces on Network1, enabling TAR-Host1 before TAR-Router1.	
35.	Allow time for all devices to perform Stateless Address Autoconfiguration and Duplicate Address Detection. Enable REF-Host2 making sure it has cleared its neighbor cache.	
36.	Transmit ICMPv6 Echo Request from REF-Host2 to the Link-Local Address of TAR-Router1.	TAR-Host1 must respond to any Neighbor Solicitations transmitted by REF-Host2 by transmitting a Neighbor Advertisement. TAR-Host1, and not TAR-Router1, must respond to the ICMPv6 Echo Requests transmitted by REF-Host2.

Part E: Duplicate Address Detection- Tentative Address Unique (Router vs Router)

Step	Action	Expected Behavior
37.	Disable all interfaces connected to Network1.	
38.	Enable all interfaces on Network1, enabling TAR-Router1 before TAR-Router2.	
39.	Allow time for all devices on Network1 to perform Stateless Address Autoconfiguration and Duplicate Address Detection. Enable REF-Host1 making sure it has cleared its neighbor cache.	
40.	Transmit ICMPv6 Echo Request from REF-Host1 to the Link-Local Address of TAR-Router1.	TAR-Router1 must respond to any Neighbor Solicitations transmitted by REF-Host1 by transmitting a Neighbor Advertisement. TAR-Router1 must respond to the ICMPv6 Echo Requests transmitted by REF-Host1
41.	Transmit ICMPv6 Echo Request from REF-Host1 to the Link-Local Address of TAR-Router2.	TAR-Router2 must respond to any Neighbor Solicitations transmitted by REF-Host1 by transmitting a Neighbor Advertisement. TAR-Router2 must respond to the ICMPv6 Echo Requests transmitted by REF-Host1
42.	Repeat Steps 37 through 41, but in Step 40 enable TAR-Router2 before TAR-Router1.	

Part F: Duplicate Address Detection- Tentative Address Duplicated (Router vs Router)

Step	Action	Expected Behavior
43.	Disable all interfaces connected to Network1.	
44.	Configure TAR-Router2 to have the same Link-local Address as TAR-Router1.	
45.	Enable all interfaces on Network1, enabling TAR-Router2 before TAR-Router1.	
46.	Allow time for all devices to perform Stateless Address Autoconfiguration and Duplicate Address Detection. Enable REF-Host1 making sure it has cleared its neighbor cache.	
47.	Transmit ICMPv6 Echo Request from REF-Host1 to the Link-Local Address of TAR-Router1.	TAR-Router2 must respond to any Neighbor Solicitations transmitted by REF-Host1 by transmitting a Neighbor Advertisement.TAR-Router2, and not TAR-Router1, must respond to the ICMPv6 Echo Requests transmitted by REF-Host1.
48.	Disable all interfaces connected to Network1.	
49.	Enable all interfaces on Network1, enabling TAR-Router1 before TAR-Router2.	
50.	Allow time for all devices to perform Stateless Address Autoconfiguration and Duplicate Address Detection. Enable REF-Host1 making sure it has cleared its neighbor cache.	
51.	Transmit ICMPv6 Echo Request from REF-Host1 to the Link-Local Address of TAR-Router2.	TAR-Router1 must respond to any Neighbor Solicitations transmitted by REF-Host1 by transmitting a Neighbor Advertisement. TAR-Router1, and not TAR-Router2, must respond to the ICMPv6 Echo Requests transmitted by REF-Host1.

Possible Problems: None.

Test IP6Interop.1.3: Processing Router Advertisements - Prefix Discovery

Purpose: To verify that a device can properly perform prefix discovery.

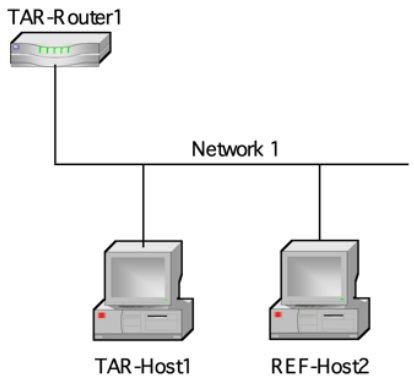
Reference:

- [ND] – Sections 6.3.4, 6.3.5, and 12
- [SLAAC] – Section 4.1

Node Requirements: See General Node Requirements.

- TAR-Host1 - Must support processing a Router Advertisement with multiple Prefixes and assigning multiple Global Addresses to an interface, must support the expiration of Prefix List.
- TAR-Router1 - Must support transmitting a Router Advertisement with positive values for AdvValidLifetime for multiple Prefix Information Options, must be able to transmit Router Advertisement with an AdvValidLifetime set to 30 seconds.
- REF-Host2 - Must support processing a Router Advertisement with multiple Prefixes and assigning multiple Global Addresses to an interface, must support the expiration of Prefix List.

Test Setup: Connect hosts TAR-Host1 and REF-Host2 and router TAR-Router1 to Network1, per the figure below. Re-initialize each interface on Network 1 before each part.



TAR-Router1: Applicant (if router) or Vendor C/D Router

TAR-Host1: Applicant (if host) or Vendor A/B Host

REF-Host2: any host

Procedure:

Part A: Single Prefix Discovery (Host vs Router)

Step	Action	Expected Behavior
1.	Configure TAR-Router1 to transmit Router Advertisements with one	

	Prefix (valid lifetime > 0) and allow time for TAR-Host1 and REF-Host2 to perform stateless address autoconfiguration and Duplicate Address Detection.	
2.	Transmit an ICMPv6 Echo Request from REF-Host2 to the Global Address of the TAR-Host1.	TAR-Host1 must respond to all ICMPv6 Echo Requests from REF-Host2 with ICMPv6 Echo Replies.

Part B: Multiple Prefix Discovery (Host vs Router)

Step	Action	Expected Behavior
3.	Configure TAR-Router1 to transmit Router Advertisements with two prefixes: Prefix1, Prefix2 (valid lifetimes > 0) and allow time for TAR-Host1 and REF-Host2 to perform stateless address autoconfiguration and Duplicate Address Detection.	
4.	Transmit ICMPv6 Echo Requests from REF-Host2 to the Global Address of TAR-Host1 associated with Prefix1.	TAR-Host1 must respond to ICMPv6 Echo Requests from REF-Host2 with ICMPv6 Echo Replies associated with Prefix1.
5.	Transmit an ICMPv6 Echo Request from REF-Host2 to the Global Address of the TAR-Host1 associated with Prefix2.	TAR-Host1 must respond to ICMPv6 Echo Requests from REF-Host2 with ICMPv6 Echo Replies associated with Prefix2.

Part C: Prefix Lifetime expires (Host vs Router)

Step	Action	Expected Behavior
6.	Configure REF-Host2 with a global address that does not expire.	
7.	Configure TAR-Router1 to transmit Router Advertisements with Prefix1 (valid lifetime = 30sec) and allow time for TAR-Host1 and REF-Host2 to perform stateless address autoconfiguration and Duplicate Address Detection. The TAR-Router1 must not transmit additional Router Advertisements after TAR-Host1 receives an address, this can be done by setting the RA interval higher or removing the Router from the link.	
8.	Transmit an ICMPv6 Echo Request from REF-Host2 to the Global Address of the TAR-Host1 associated with Prefix1.	TAR-Host1 must respond to ICMPv6 Echo Requests from REF-Host2 with ICMPv6 Echo Replies associated with Prefix1.
9.	Allow 35 seconds to pass.	

10.	Transmit an ICMPv6 Echo Request from REF-Host2 to the Global Address of the TAR-Host1 associated with Prefix1.	TAR-Host1 must timeout its Prefix1. TAR-Host1 must not respond to ICMPv6 Echo Requests or Neighbor Solicitations from the REF-Host2 with the address associated with Prefix1.

Possible Problems: If TAR-Router1 does not support setting the Prefix Lifetime to 30 seconds, configure TAR-Router1 to advertise the option with the lowest lifetime in step 7 and allow the lifetime to expire in step 9.

Test IP6Interop.1.4: Processing Router Advertisements- Router Lifetime

Purpose: To verify that a device can properly perform Router Discovery.

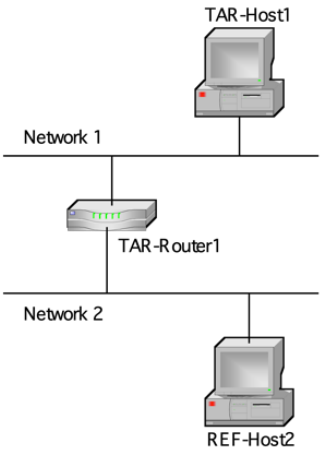
Reference:

- [ND] – Sections 6.3.4

Node Requirements: See General Node Requirements.

- TAR-Host1 - Must support the removal of Default Router from Default Router List after receiving a Router Advertisement with an AdvDefaultLifetime set to zero.
- TAR-Router1 - Must support continuous transmission of Router Advertisements on both Network1 and Network2, must support the transmission of Router Advertisements with the AdvDefaultLifetime set to zero and 600. RA interval must also be configurable.

Test Setup: Connect hosts TAR-Host1 and REF-Host2 and router TAR-Router1 to Network1 and Network2, per the figure below. Router TAR-Router1 route between Network1 and Network2. Allow time for the TAR-Host1 and REF-Host2 to perform stateless address autoconfiguration and Duplicate Address Detection.



TAR-Router1: Applicant (if router) or Vendor C/D Router
TAR-Host1: Applicant (if host) or Vendor A/B Host
REF-Host2: any host

Procedure:

Part A: Router Lifetime value is non-zero (Host vs Router)

Step	Action	Expected Behavior
1.	Configure TAR-ROUTER1 to transmit Router Advertisements with Router Lifetimes set to 600 seconds and Router Advertisement Intervals set to approximately 60 seconds on both Network1 and Network2.	

2.	Transmit an ICMPv6 Echo Request from REF-Host2 to the Global Address of TAR-Host1.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must use TAR-Router1 as its first hop for Network2 and the Echo Reply should be visible on Network2.

Part B: Router Lifetime value is zero (Host vs Router)

Step	Action	Expected Behavior
3.	Configure TAR-Router1 to transmit Router Advertisements with Router Lifetimes equal to 0 and at a normal interval on Network1, and Router Lifetimes greater than the Router Advertisement Interval on Network2.	
4.	Transmit an ICMPv6 Echo Request from REF-Host2 to the Global Address of TAR-Host1.	TAR-Host1 MUST not transmit an Echo Reply using TAR-Router1 as its first hop or transmit a multicast NS with a target address set to TR1's link-local address.
5.	Configure TAR-ROUTER1 to transmit Router Advertisements with Router Lifetimes set to 600 seconds and Router Advertisement Intervals set to approximately 60 seconds on both Network1 and Network2.	
6.	Transmit an ICMPv6 Echo Request from REF-Host2 to the Global Address of TAR-Host1.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must use TAR-Router1 as its first hop for Network2 and the Echo Reply should be visible on Network2.
7.	Configure TAR-Router1 to transmit Router Advertisements with the Router Lifetime set to 0 on Network1.	
8.	Transmit an ICMPv6 Echo Request from REF-Host2 to the Global Address of TAR-Host1.	TAR-Host1 MUST not transmit an Echo Reply using TAR-Router1 as its first hop or transmit a multicast NS with a target address set to TR1's link-local address.

Possible Problems: None.

Test IP6Interop.1.5: Redirect Function (Host vs Router)

Purpose: Verify the correct interoperability between a device's redirect handling with that of various IPv6 implementations.

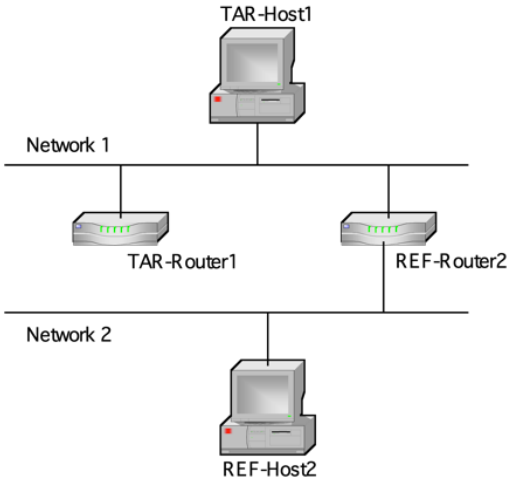
Reference:

- [ND] – Section 4.5, 4.6.3, 8

Node Requirements: See General Node Requirements.

- TAR-Host1 – Must support the Redirect function.
- TAR-Router1 – Must support the configuration of a Static Route and Redirect function.
- REF-Router2 – Must support ceasing Router Advertisement transmission.

Test Setup: Connect all devices, per the figure below. Configure router REF-Router2 to NOT transmit Router Advertisements on Network1. Router TAR-Router1 is not connected to Network2. Configure a static route on TAR-Router1 indicating REF-Router2's Link-local address as the next hop for network Network2. Router REF-Router2 routes between Network1 and Network2. Allow time for the TAR-Host1 and REF-Host2 to perform stateless address autoconfiguration and Duplicate Address Detection



TAR-Router1: Applicant (if router) or Vendor C/D Router
TAR-Host1: Applicant (if host) or Vendor A/B Host
REF-Host2: any host
REF-Router2: any router

Procedure:

Step	Action	Expected Behavior
1.	Transmit an ICMPv6 Echo Request from REF-Host2 to the Global Address of TAR-Host1.	
2.	Allow time for TAR-Router1 to send an ICMPv6 Redirect message to	TAR-Router1 should send an ICMPv6 Redirect message to the TAR-Host1

	TAR-Host1 specifying REF-Router2 as a better first hop.	indicating REF-Router2 as a better first hop to Network2.
3.	Transmit an ICMPv6 Echo Request from REF-Host2 to the Global Address of TAR-Host1.	TAR-Host1 must use REF-Router2 as its first hop for the Echo Reply destined for Network2, indicating that it processed the ICMPv6 Redirect Message and applied it to its Routing Table. REF-Host2 must receive the Echo Reply from TAR-Host1.
4.	Remove the static route on TAR-Router1 configured in the test setup.	

Possible Problems: None.

Test IP6Interop.1.6: Path MTU Discovery and Fragmentation

Purpose: Verify that devices can participate in path MTU discovery and handle fragmentation in an Ipv6 network.

Reference:

- [PMTU] – Section 3,4
- [ICMPv6] – Section 3.2
- [IPv6-SPEC] – Section 4.5, 5

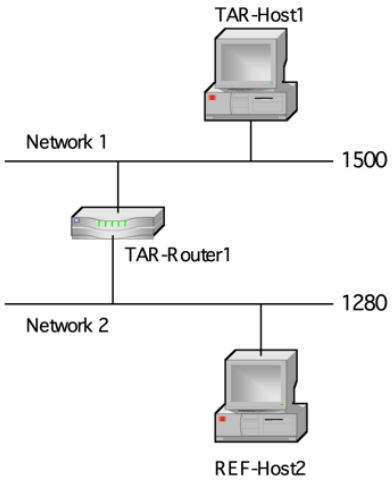
Node Requirements: See General Node Requirements.

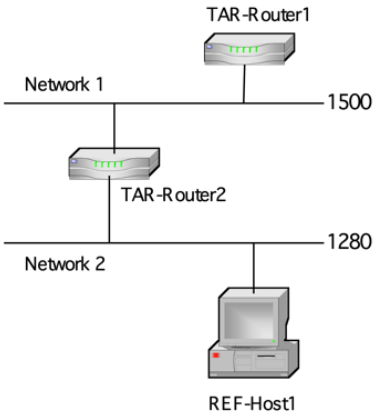
- TAR-Host1 - Must transmit/receive 1500 bytes Echo Requests/Replies, must process Router Advertisement with AdvLinkMTU set to 1280, must support fragmentation and process Packet Too Big messages.
- TAR-Host2 - Must transmit/receive 1500 bytes Echo Requests/Replies, must process Router Advertisement with AdvLinkMTU set to 1280, and must support fragmentation.
- TAR-Router1 - Must transmit/receive 1500 bytes Echo Requests/Replies, must support configuration of Link MTU and transmission of AdvLinkMTU in Router Advertisements, must transmit/receive Packet Too Big message and support fragmentation. Must be able to configure a Static Route.
- TAR-Router2 - Must transmit/receive 1500 bytes Echo Requests/Replies, must support configuration of Link MTU and transmission of AdvLinkMTU in Router Advertisements, must transmit/receive Packet Too Big message and support fragmentation. Must be able to configure a Static Route.
- REF-Router1 - Must support transmission of AdvLinkMTU in Router Advertisements, must be able to configure Static Route, must be able to transmit a Packet Too Big message.
- REF-Router2 - Must support transmission of AdvLinkMTU in Router Advertisements, must be able to configure Static Route, must be able to transmit a Packet Too Big message.
- REF-Host1 - Must transmit/receive 1500 bytes Echo Requests/Replies, must process Router Advertisement with AdvLinkMTU set to 1280 and support fragmentation.
- REF-Host2 - Must transmit/receive 1500 bytes Echo Requests/Replies, must process Router Advertisement with AdvLinkMTU set to 1280 and support fragmentation.

Test Setup: For Part A, connect hosts TAR-HOST1 and REF-HOST2 and router TAR-ROUTER1 to Network1 and Network2, per the figure below. Router TAR-ROUTER1 routes between Network1 and Network2. Allow time for the TAR-HOST1 and REF-HOST2 to perform stateless address autoconfiguration and Duplicate Address Detection. For Parts B through D, connect all devices as per the figure below. Re-boot each device after each part is performed.

Part A:

Part B:





TAR-Router1: Applicant (if router) or Vendor C/D Router

TAR-Router1: Applicant

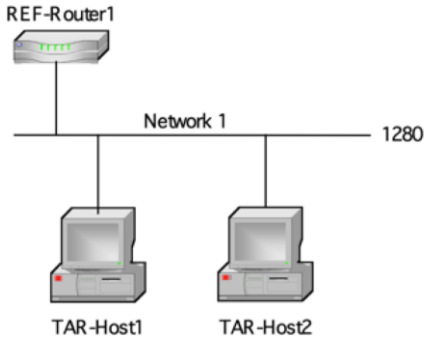
TAR-Host1: Applicant (if host) or Vendor A/B Host

TAR-Router2: Vendor C/D Router

REF-Host2: any host

REF-Host1: any host

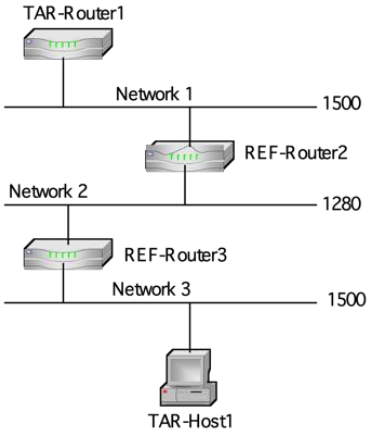
Part C:



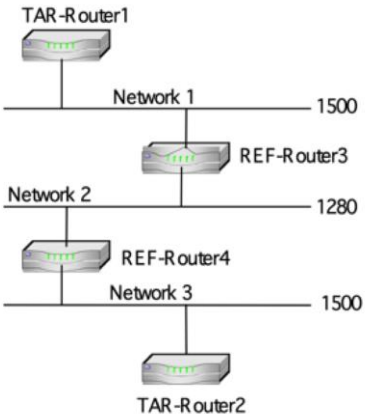
TAR-Host1: Applicant Implementation
TAR-Host2: Vendor A/B Host
REF-Router1: any router

Part D:

Part E:



TAR-Router1: Applicant (if router) or Vendor C/D Router
TAR-Host1: Applicant (if host) or Vendor A/B Host
REF-Router2: any router



TAR-Router1: Applicant Implementation
TAR-Router2: Vendor C/D Router
TAR-Host1: Applicant (if host) or Vendor A/B Host
REF-Router3: any router
REF-Router4: any router
REF-Router3: any router

Procedure:

Part A: PMTU Discovery (Host vs Router)

Step	Action	Expected Behavior
1.	Configure the Network1 interface on TAR-Router1 with a path MTU of 1500 bytes.	
2.	Configure the Network2 interface on TAR-Router1 with a path MTU of 1280 bytes.	

3.	Transmit ICMPv6 Echo Request packets whose original packet size is 1500 byte from the Global Address of REF-Host2 to the Global Address of TAR-Host1.	TAR-Host1 must attempt to send the Echo Reply without fragmenting. TAR-Router1 must send an ICMPv6 Packet Too Big Message, and the TAR-Host1 must lower its path MTU estimate and fragment the Echo Reply.

Part B: PMTU Discovery (Router vs Router)

Step	Action	Expected Behavior
4.	Configure the Network1 interface on TAR-Router2 and TAR-Router1 with a path MTU of 1500 bytes.	
5.	Configure the Network2 interface on TAR-Router2 with a path MTU of 1280 bytes.	
6.	Transmit ICMPv6 Echo Request packets whose original packet size is 1500 byte from the Global Address of REF-Host1 to the Global Address of TAR-Router1.	TAR-Router1 should attempt to send the Echo Reply without fragmenting. TAR-Router2 must send an ICMPv6 Packet Too Big Message, and the TAR-Router1 must lower its path MTU estimate and fragment the Echo Reply.
7.	Disconnect TAR-Router1 and TAR-Router2 and switch the roles such that TAR-Router1 is routing between Network1 and Network2 and TAR-Router2 is connected to Network1 only.	
8.	Configure the Network1 interface on TAR-Router1 and TAR-Router2 with a path MTU of 1500 bytes.	
9.	Configure the Network2 interface on TAR-Router1 with a path MTU of 1280 bytes.	
10.	Transmit ICMPv6 Echo Request packets whose original packet size is 1500 byte from the Global Address of REF-Host1 to the Global Address of TAR-Router2.	TAR-Router2 should attempt to send the Echo Reply without fragmenting. TAR-Router1 must send an ICMPv6 Packet Too Big Message, and the TAR-Router2 must lower its path MTU estimate and fragment the Echo Reply.

Part C: Fragmentation/Reassembly (Host vs Host)

Step	Action	Expected Behavior
11.	Configure REF-Router1 to transmit a Router Advertisement with MTU=1280 on Network 1.	
12.	Transmit ICMPv6 Echo Request packets whose original packet size is 1500 byte from the link-local address of TAR-Host1 to the link-local address of TAR-Host2.	TAR-Host1 must send the Echo Request with fragmenting. TAR-Host2 must respond to the fragmented Echo Request sent by TAR-Host1 with an Echo Reply.

13.	Transmit ICMPv6 Echo Request packets whose original packet size is 1500 byte from the link-local address of TAR-Host2 to the link-local address of TAR-Host1.	TAR-Host2 must send the Echo Request with fragmenting. TAR-Host1 must reassemble and respond to the fragmented Echo Request with an Echo Reply.
14.	Transmit ICMPv6 Echo Request packets whose original packet size is 1500 byte from the on-link global address of TAR-Host1 to the on-link global address of TAR-Host2.	TAR-Host1 must send the Echo Request with fragmenting. TAR-Host2 must respond to the fragmented Echo Request sent by TAR-Host1 with an Echo Reply
15.	Transmit ICMPv6 Echo Request packets whose original packet size is 1500 byte from the on-link global address of TAR-Host2 to the on-link global address of TAR-Host1.	TAR-Host2 must send the Echo Request with fragmenting. TAR-Host1 must reassemble and respond to the fragmented Echo Request with an Echo Reply.

Part D: Fragmentation/Reassembly (Host vs Router)

Step	Action	Expected Behavior
16.	Configure a static route on TAR-Router1 for Network 3 using a nexthop of REF-Router2. Configure static routes for Networks 1 and 3 on REF-Router2 and REF-Router3 so they are each the appropriate nexthop. Configure REF-Router3 to transmit Router Advertisements with a Router Lifetime > 0 on Network 3.	
17.	Transmit ICMPv6 Echo Request packets whose original packet size is 1500 byte from TAR-Router1 to TAR-Host1.	If TAR-Router1 attempts to send the Echo Request without fragmenting, then REF-Router2 must send an ICMPv6 Packet Too Big Message, and the TAR-Router1 must lower its path MTU estimate and fragment the Echo Request. TAR-Host1 must respond to the Echo Request sent by TAR-Router1 with an Echo Reply.
18.	Transmit ICMPv6 Echo Request packets whose original packet size is 1500 byte from TAR-Host1 to TAR-Router1.	TAR-Host1 should send the Echo Request with fragmenting. TAR-Router1 must respond to the Echo Request sent by TAR-Host1 with an Echo Reply.

Part E: Fragmentation/Reassembly (Router vs Router)

Step	Action	Expected Behavior
19.	Configure a static route on TAR-Router1 for Network 3 using a nexthop of REF-Router3. Configure static routes for Networks 1 and 3 on REF-Router3 and REF-Router4 so they are each the appropriate nexthop. Configure a static route on TAR-Router2 for Network 1 using a nexthop of REF-Router4.	

20.	Transmit ICMPv6 Echo Request packets whose original packet size is 1500 byte from TAR-Router1 to TAR-Router2.	If TAR-Router1 attempts to send the Echo Request without fragmenting, then REF-Router3 must send an ICMPv6 Packet Too Big Message, and TAR-Router1 must lower its path MTU estimate and fragment the Echo Request. TAR-Router2 must respond to the Echo Request sent by TAR-Router1 with an Echo Reply.
21.	Transmit ICMPv6 Echo Request packets whose original packet size is 1500 byte from TAR-Router2 to TAR-Router1.	TAR-Router2 should send the Echo Request with fragmenting. TAR-Router1 must respond to the Echo Request sent by TAR-Router2 with an Echo Reply.

Possible Problems:

- When the applicant device does not implement an application for sending Echo Requests (Passive Node), or does not allow a user to configure packet size, the following actions take place:
  - If the applicant device is a Host, Part C Steps 12 and 14, and Part D Step 18 may be omitted
  - If the applicant device is a Router, Part D Step 17 and Part E Step 20 may be omitted
- If the applicant device is TAR-Host1 and its application for sending Echo Requests does not allow a user to specify a link-local destination, Part C Step 12 may be omitted
- When the target device is a Host or a Router, these tests may require reverse communication directions if the target device is a passive node and cannot transmit requests to initiate PMTU discovery.
- A node's MTU only supports MTU of 1280 require the reverse communication direction in order to properly test PMTU discovery. When the applicant device uses fixed Path MTU for both directions, following actions take place:
  - If the applicant device is TAR-Host1, Part A may be omitted
  - If the applicant device is TAR-Router1, Part B Step (4-6) may be omitted
- When the target device is a Router, some of these tests require the target device to configure link MTU on an interface. If this is not possible, Part A and Part B Step (7-10) may be omitted

Test IP6Interop.1.7: Processing Router Advertisements- Router Preference

Purpose: To verify that a device can properly perform Router Preference.

Functionality Tag: Mandatory

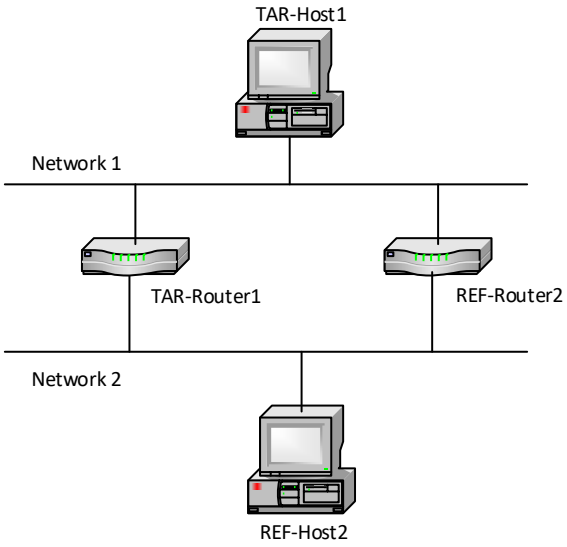
Reference:

- [RFC-4191] – Sections 3.1

Node Requirements: See General Node Requirements.

- TAR-Router1 – Must support transmitting Router Advertisements with Route Preference.
- TAR-Host1 – Must support processing Router Advertisements with Route Preference.
- REF-Router2 – Must support transmitting Router Advertisements with Route Preference

Test Setup: TAR-Router1 and REF-Router2 must configure a Router Advertisement with a long enough Router lifetime to TAR-Host1 and REF-Host2 of fulfilling each test case.



TAR-Router1: Applicant (if router) or Vendor C/D Router
TAR-Host1: Applicant (if host) or Vendor A/B Host
REF-Router1: any Router
REF-Host2: any host

Procedure:

Part A: High Route Preference (Host vs Router)

Step	Action	Expected Behavior
1.	Configure the TAR-Router1 to advertise a Router Preference of High on Network1.	

2.	Configure the REF-Router2 to advertise a Router Preference of Medium on Network1.	
3.	REF-Host2 transmits an Echo Request to TAR-Host1.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must use TAR-Router1 as its first hop for Network2 and the Echo Reply should be visible on Network2.

Part B: Low Route Preference (Host vs Router)

Step	Action	Expected Behavior
4.	Configure the TAR-Router1 to advertise a Router Preference of Low on Network1.	
5.	Configure the REF-Router2 to advertise a Router Preference of Medium on Network1.	
6.	REF-Host2 transmits an Echo Request to TAR-Host1.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must use REF-Router2 as its first hop for Network2 and the Echo Reply should be visible on Network2.

Part C: Change to lower Router Preference (Host vs Router)

Step	Action	Expected Behavior
7.	Configure the TAR-Router1 to advertise a Router Preference of High on Network1.	
8.	Configure the REF-Router2 to advertise a Router Preference of Medium on Network1.	
9.	REF-Host2 transmits an Echo Request to TAR-Host1.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must use TAR-Router1 as its first hop for Network2 and the Echo Reply should be visible on Network2.
10.	Configure the TAR-Router1 to advertise a Router Preference of Low on Network1.	
11.	REF-Host2 transmits an Echo Request to TAR-Host1.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must use REF-Router2 as its first hop for Network2 and the Echo Reply should be visible on Network2.

Part D: Change to higher Router Preference (Host vs Router)

Step	Action	Expected Behavior
12.	Configure the TAR-Router1 to advertise a Router Preference of Low on Network1.	
13.	Configure the REF-Router2 to advertise a Router Preference of Medium on Network1.	
14.	REF-Host2 transmits an Echo Request to TAR-Host1.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must use REF-Router2 as its first hop for Network2 and the Echo Reply should be visible on Network2.
15.	Configure the TAR-Router1 to advertise a Router Preference of High on Network1.	
16.	REF-Host2 transmits an Echo Request to TAR-Host1.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must use TAR-Router1 as its first hop for Network2 and the Echo Reply should be visible on Network2.

Possible Problems: None.

Test IP6Interop.1.8: Processing Router Advertisements- Route Information Option

Purpose: To verify that a device can properly perform Route Preference using Router Information Options.

Advanced Functionality:

- Processing Route Information Options (RFC 4191 Type C Host):

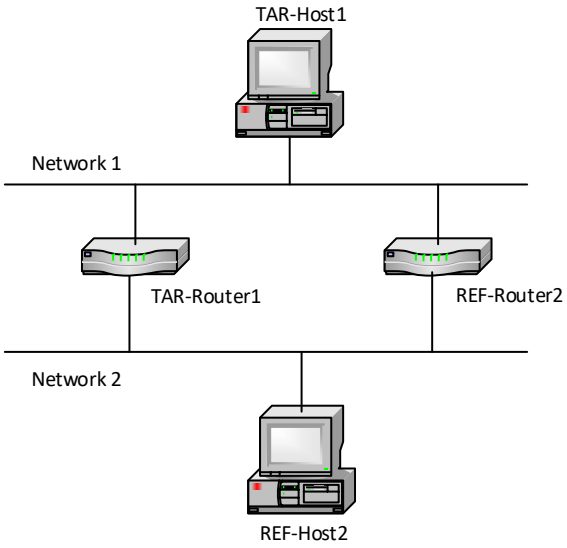
Reference:

- [RFC 4191] – Sections 3.1

Node Requirements: See General Node Requirements.

- TAR-Router1 – Must support transmitting Router Advertisements with Route Information Options, including setting the lifetime and prefix.
- TAR-Host1 – Must support processing Router Advertisements with Router Preference and Router Information Options.
- REF-Router2 – Must support transmitting Router Advertisements with Route Preference

Test Setup: Connect hosts TAR-Host1 and REF-Host2 and routers TAR-Router1 and REF-Router2 to Network1 and Network2, per the figure below. Routers TAR-Router1 and REF-Router2 routes between Network1 and Network2. Allow time for the TAR-Host1 and REF-Host2 to perform stateless address autoconfiguration and Duplicate Address Detection.



TAR-Router1: Applicant (if router) or Vendor C/D Router
TAR-Host1: Applicant (if host) or Vendor A/B Host
REF-Router1: any Router
REF-Host2: any host

Procedure:

Part A: Router Information Option High (Host vs Router)

Step	Action	Expected Behavior
1.	Configure the REF-Router2 to advertise a Router Preference of Medium on Network1.	
2.	Configure the TAR-Router1 to advertise a Router preference of Medium and a Route Information Option with a prefix of ::/0 with a High preference on Network 1.	
3.	REF-Host2 transmits an Echo Request to TAR-Host1.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must use TAR-Router1 as its first hop for Network2 and the Echo Reply should be visible on Network2.

Part B: Route Information Option Low (Host vs Router)

Step	Action	Expected Behavior
4.	Configure the REF-Router2 to advertise a Router Preference of Medium on Network1.	
5.	Configure the TAR-Router1 to advertise a Router preference of Medium and a Route Information Option with a prefix of ::/0 with a Low preference on Network 1.	
6.	REF-Host2 transmits an Echo Request to TAR-Host1.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must use REF-Router2 as its first hop for Network2 and the Echo Reply should be visible on Network2.

Part C: Route Information Option with a Prefix Length of 96 (Host vs Router)

Step	Action	Expected Behavior
7.	Configure the REF-Router2 to advertise a Router Preference of Medium on Network1.	
8.	Configure the TAR-Router1 to advertise a Router preference of Medium and a Route Information Option with a Network 2 prefix having a length of 96 with a High preference on Network 1.	

9.	REF-Host2 transmits an Echo Request to TAR-Host1 with a source address in the /96 prefix.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must use TAR-Router1 as its first hop for Network2 and the Echo Reply should be visible on Network2.

Part D: Route Information Option with a Prefix Length of 32 (Host vs Router)

Step	Action	Expected Behavior
10.	Configure the REF-Router2 to advertise a Router Preference of Medium on Network1.	
11.	Configure the TAR-Router1 to advertise a Router preference of Medium and a Route Information Option with Network 2 prefix having a length of 32 with a High preference on Network 1.	
12.	REF-Host2 transmits an Echo Request to TAR-Host1 with a source address in the /32 prefix.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must use TAR-Router1 as its first hop for Network2 and the Echo Reply should be visible on Network2.

Part E: Route Information Option with a Lifetime of 0 (Host vs Router)

Step	Action	Expected Behavior
13.	Configure the REF-Router2 to advertise a Router Preference of Medium on Network1.	
14.	Configure the TAR-Router1 to advertise a Router preference of Medium and a Route Information Option with a prefix of ::/0 with a High preference on Network 1.	
15.	REF-Host2 transmits an Echo Request to TAR-Host1.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must use TAR-Router1 as its first hop for Network2 and the Echo Reply should be visible on Network2.
16.	Configure the TAR-Router1 to advertise a Router preference of Medium and a Route Information Option with a prefix of ::/0 with a lifetime of zero on Network 1.	
17.	REF-Host2 transmits an Echo Request to TAR-Host1.	REF-Host2 should send an Echo Request with a Destination Address of the TAR-Host1's Global Address. TAR-Host1 must

		use REF-Router2 as its first hop for Network2 and the Echo Reply should be visible on Network2.

Possible Problems: None.

Test IP6Interop.1.9: Processing Router Advertisements- DNS

Purpose: To verify that a device can properly discover DNS information from Router Advertisements.

Advanced Functionality:

- Router Advertisement DNS (Host Only):
- Transmitting Echo Requests (Passive Node):

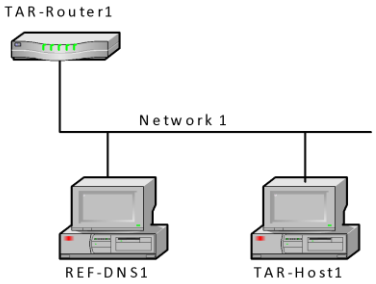
Reference:

- [RA-DNS] – Sections 5.1 and 5.2

Node Requirements: See General Node Requirements.

- TAR-Router1 – Must support transmitting Router Advertisements with RDNSS and DNSSL Options including setting the lifetimes of those options.
- TAR-Host1 – Must support processing Router Advertisements with RDNSS and DNSSL Options.
- REF-DNS1 – Must support responding to the DNS Queries for AAAA Records.

Test Setup: Connect hosts TAR-Host1 and REF-DNS1 and router TAR-Router1 to Network1. Allow time for the TAR-Host1 and REF-DNS1 to perform stateless address autoconfiguration and Duplicate Address Detection.



TAR-Router1: Applicant (if router) or Vendor C/D Router
TAR-Host1: Applicant (if host) or Vendor A/B Host
REF-DNS1: any DNS server

Procedure:

Part A: Recursive DNS Option (Host vs Router)

Step	Action	Expected Behavior
1.	Configure the TAR-Router1 to advertise a Router Advertisement with a RDNSS Option including REF-DNS1 as the Server.	
2.	Transmit ICMPv6 Echo Request packets with a destination of	TAR-Host1 must transmit a DNS Query to REF-DNS1 for node1.test.example.com. REF-DNS1 will respond with REF-DNS1 as

	"node1.test.example.com" from TAR-Host1.	the answer to the query. TAR-Host1 must transmit an Echo Request to REF-DNS1. REF-DNS1 will transmit an Echo Reply which should be visible on Network1.

Part B: Recursive DNS Option lifetime 0 (Host vs Router)

Step	Action	Expected Behavior
3.	Configure the TAR-Router1 to advertise a Router Advertisement with a RDNSS Option including REF-DNS1 as the Server.	
4.	Transmit ICMPv6 Echo Request packets with a destination of "node1.test.example.com" from TAR-Host1.	TAR-Host1 must transmit a DNS Query to REF-DNS1 for node1.test.example.com. REF-DNS1 will respond with REF-DNS1 as the answer to the query. TAR-Host1 must transmit an Echo Request to REF-DNS1. REF-DNS1 will transmit an Echo Reply which should be visible on Network1.
5.	Configure the TAR-Router1 to advertise a Router Advertisement with a RDNSS Option including REF-DNS1 as the Server with a lifetime of 0.	
6.	Transmit ICMPv6 Echo Request packets with a destination of "node1.test.example.com" from TAR-Host1.	TAR-Host1 must not transmit a DNS Query to REF-DNS1 for node1.test.example.com or transmit an Echo Request to REF-DNS1.

Part C: Search List Option (Host vs Router)

Step	Action	Expected Behavior
7.	Configure the TAR-Router1 to advertise a Router Advertisement with a DNSSL Option with a Search List of test.example.com.	
8.	Transmit ICMPv6 Echo Request packets with a destination of "node1" from TAR-Host1.	TAR-Host1 must transmit a DNS Query to REF-DNS1 for node1.test.example.com. REF-DNS1 will respond with REF-DNS1 as the answer to the query. TAR-Host1 must transmit an Echo Request to REF-DNS1. REF-DNS1 will transmit an Echo Reply which should be visible on Network1.

Part D: Search List Option with a Lifetime of 0 (Host vs Router)

Step	Action	Expected Behavior
9.	Configure the TAR-Router1 to advertise a Router Advertisement with a DNSSL Option with a Search List of test.example.com.	

10.	Transmit ICMPv6 Echo Request packets with a destination of "node1" from TAR-Host1.	TAR-Host1 must transmit a DNS Query to REF-DNS1 for node1.test.example.com. REF-DNS1 will respond with REF-DNS1 as the answer to the query. TAR-Host1 must transmit an Echo Request to REF-DNS1. REF-DNS1 will transmit an Echo Reply which should be visible on Network1.
11.	Configure the TAR-Router1 to advertise a Router Advertisement with a DNSSL Option with a Search List of test.example.com with a lifetime of 0.	
12.	Transmit ICMPv6 Echo Request packets with a destination of "node1" from TAR-Host1.	TAR-Host1 must not transmit a DNS Query to REF-DNS1 for node1.test.example.com or transmit an Echo Request to REF-DNS1.

Possible Problems:

- If TAR-Router1 does not support setting the Recursive DNS Server Option lifetime to 0, configure TAR-Router1 to advertise the option with the lowest lifetime and allow the lifetime to expire in step 5.
- If TAR-Router1 does not support setting the DNS Search List Option lifetime to 0, configure TAR-Router1 to advertise the option with the lowest lifetime and allow the lifetime to expire in step 11.

Modification Record

Version 5.1.0 — November 10, 2026

- Added Constrained Node (CN) support.
- Added CallBox and CN device requirements to General Node Requirements, and updated the multicast ping requirements to apply to Host, Router and CN.
- Updated Test Performed on Host/Router to Test Performed on Host/Router/CN, with a CN column showing that 1.1a–1.1f apply to CNs.
- Added Setup for CN to Group 1, where a CallBox connection between Network 1 and the CN replaces TAR-Host1.
- Added a possible problem to 1.1 allowing Steps 2, 6, 9, and 12 to be omitted for CNs that do not respond to Echo Requests with an IPv6 Link-Local address.
- Rewrote the Introduction to describe the IPv6 Ready Logo Program and the scope of this document.
- (FORMAT) Updated the title page and fonts to match the Core Protocols Conformance test specification.
- (FORMAT) Reformatted the Test Performed on Host/Router/CN section as a table.
- (TYPO) Fixed "multicast request" to "multicast requests" in the 1.1 possible problems and "ping result" to "ping results" in General Node Requirements.

Version 5.0.6 — January 4, 2024

- Added Passive Node to Advanced Functionality section.
- Updated Possible Problem section of 1.6 to omit certain steps if the NUT is passive or cannot configure packet size.
- Updated expected preference value for second RIO in 1.8 Part E.
- Fix FQDN typo in 1.9 Part D.
- Fixed references section of 1.2 and 1.3.
- Re-organized possible problems to not overlap with advanced functionality
- Add Functionality Tag to indicate advanced functionality per test case.
- Add Possible Problem Summary page
- Added AdvPreferredLifetime in General Node requirements for router.
- Fixed the test step 28 in 1.2 Part D
- Fixed the test setup in 1.6.
- Updated the test procedures in 1.7 & 1.8.
- Fixed the test setup in 1.8.
- Replaced REF-Host2 with REF-DNS1 in 1.9 Part D expected behavior.
- Fixed typo Advertisements/Advertisements

Version 5.0.5 — January 26, 2022

- Added Advanced Functionaly 1.9 Router Advertisment for DNS to match Conformance.

Version 5.0.4 — November 3, 2021

- Removed incorrect Echo Reply requirement at end of Step 12.

Version 5.0.3 — June 1, 2021

- Added Possible Problem in 1.1 from 5.0.1 back as it was incorrectly removed in 5.0.2.
- Added a reference to 8200 in test 1.6.



Version 5.0.2	March 11, 2021 • Added Possible Problem to 1.3 for Routers that can't set the Prefix lifetime to zero. • Added Possible Problems for Router that don't support setting DNS Server Option and DNS Search List Option to the lowest values. • Corrected Network 2 to Network 1 in 1.9. • Corrected REF-Router1 to REF-Host2 in 1.2D.
Version 5.0.1	September 18, 2020 • Added a Possible Problem to 1.1 to allow Interoperability partners that don't support responding to multicast addresses.
Version 5.0.0	January 17, 2019 • Update formatting of test cases • Changed 1.2 to set the link-local address on the non-applicant to remove possible problems. • Added Steps for Host to support Stable-ID which requires finding a new address. • Added 1.7 and 1.8 for RFC 4191 Support. • Added 1.9 for DNS in Router Advertismeents (RFC 8106). • Updated the Possible Problem in 1.6 to explicitly say what to do for MTU of 1280. • Added Advanced Functionality for 1.8. • Added Possible Problem to 1.3C regarding minimum Prefix Lifetime
Version 4.0.5	September 8, 2018 • Remove Phase1/Phase 2 References.
Version 4.0.4	March 22, 2010 • Updated IP6Interop.1.6 Possible problems to be more clear and added clarification in Observable results for parts E, F
Version 4.0.3	July 7, 2009 • Updated IP6Interop.1.6 Possible problems to be more clear
Version 4.0.2	April 7, 2009 • IP6Interop.1.2 – Added Possible problems that EUI-64 is not required.
Version 4.0.1	September 5, 2008 • Fixed Images
Version 4.0.1a2	August 26, 2008 • Fixed Typos
Version 4.0.1a1	August 21, 2008 (internal review) • Inserted topology requirement examples for all tests.
Version 4.0.0	May 28, 2008 – Major Version Release
Version 4.0.0.b1	April 9, 2008 (Major Version Up) Public Review
Version 4.0.0.a2	March 25, 2008 (Major Version Up) Internal Review • Updated Version number to cooridate with Core Test Specification • Removed Test IP6Interop1.7 due to mandate RFC 5095 • Clarified node requirements for Phase-1 • Clarified Tests Required for Special Device
Version 3.0.0.a1 (released)	March 20, 2008 (Major Version Up) Internal Review • RFC 4291 Support – Added Reference to test IP6Interop.1.1
Version 2.9.0	October 9, 2007 • Update to RFC 4861 – No changes necessary • Update to RFC 4862 – No changes necessary



- IP6Interop.1.3A, removed redundant initialization steps (2-4).
- Added Copyright information
- Added Reference to [RH0]
- IP6Interop.1.7: added possible problem due to deprecation of RH0
- Added Test IP6Interop.1.4A for RA router lifetime > 0 for Phase-1 requirement.

Version 2.8.4 April 4, 2007

- Fixed Typo

Version 2.8.3 January 26, 2007

- Updated RFC 4443 – No changes necessary
- Updated Test 1.6, added the word “packet” after 1500 byte Echo Request.

Version 2.8.2 Nov 6, 2006

- IP6Interop.1.3C, added observable results: TAR-Host1 not respond to ICMPv6 Echo Requests or NS from REF-Host2
- IP6Interop.1.6D,E, added to observe Network 3 in procedure

Version 2.8.1 July 19, 2006

- Fixed Typos

Version 2.8.0 September 14, 2005

- Test IP6Interop.1.4, added support for one interface router
- Test IP6Interop.1.6, changed size of packets to 1500 (A-E)
  - Added support for one interface router
- Test IP6Interop.1.7A, added support for one interface router
- Added Node Requirements to each test

Version 2.7.6 July 12, 2005

- Test IP6Interop.1.3, add Possible Problems.

Version 2.7.5 June 27, 2005

- Test IP6Interop1.6, add Possible Problems.

Version 2.7.4 June 10, 2005

- Fixed Typos.

Version 2.7.3 June 7, 2005

- Fixed Typos.

Version 2.7.2 June 2, 2005

- Test IP6Interop.1.6 part B, fixed topology
- Test IP6Interop.1.7 added requirement for Ref-Host

Version 2.7.1 May 26, 2005

- Test IP6Interop.1.6 Part B, added steps 9-13, to reverse the roles of TAR-Routers.
- Added Phase I-II requirements to Tests performed on Host/Routers

Version 2.7.0 March 29, 2005

- Test IP6Interop.1.2 all Parts, added step to check neighbor cache.
  - Parts A, C and E, specified boot-up order
  - Parts B, D and F, added DAD for both targets.
- Test IP6Interop.1.3, added initialization step to Test Setup.
- Test IP6Interop1.4, changed Step 5 to ping from REF-Host2
  - Fixed Observable results, Step 3 for on-link assumption.
- Test IP6Interop1.6 Part B, added new test: PMTU Discovery
- Test IP6Interop1.6 Part C, added steps 14 through 17.
- Test IP6Interop1.6 Part D and E, fixed results for steps 22 and 27.
- Test IP6Interop1.7 Part B, added steps 7 through 10.
- Removed references to Record interface information.



- Removed IP6Inerop1.6a from being a Phase-I requirement.

Version 2.6.1 February 11, 2005

- Added Test Setup: to record info documentation.

Version 2.6 January 18, 2005

- Test IP6Interop.1.2, Procedure
  Steps 1, 7, 13, 19, 25 and 31: changed “interface” to “device”
- Test IP6Interop.1.4b- Removed.
- Test IP6Interop.1.5, procedure /results: changed the direction of the ICMP Echo Request from REF-Host2 to TAR-Host1.
- Test IP6Interop.1.6b
  Added REF-Router1 to transmit RA with MTU=1280.

Versions 2.5 December 15, 2004

- Test IP6Interop.1.4a, b
  Added Observable Results.
  Step 9 and 15: TAR-Host1 MUST not transmit a multicast NS with a target set to TR1’s link-local address.

Version 2.4 December 9, 2004

- Test IP6Interop.1.4a, b
  Changed Observable Results.
  Step 9 and 15: TAR-Host1 MUST not transmit an Echo Reply using TAR-Router1 as its first hop.

Version 2.3.1 October 3, 2004
Version 2.3 September 27, 2004
Version 2.2 September 12, 2004
Version 2.1 September 10, 2004
Version 2.0 September 8, 2004
Version 1.0 September 2, 2004