IPv6 Ready

SRv6 Interoperability Test Specification

Technical Document

Revision 0.0.0a

IPv6 Forum ***http://www.ipv6forum.org***
IPv6Ready ***http://www.ipv6ready.org***

Table of Contents

Acknowledgements

Principle Authors:

CNLabs
BII Group

Commentators:

University of New Hampshire- InterOperability Lab

Introduction

The IPv6 forum plays a major role to bring together industrial actors, to develop and deploy the new generation of IP protocols. Contrary to IPv4, which started with a small closed group of implementers, the universality of IPv6 leads to a huge number of implementations. Interoperability has always been considered as a critical feature in the Internet community. Due to the large number of IPv6 implementations, it is important to give to the market a strong signal proving the interoperability degree of various products.

To avoid confusion in the mind of customers, a unique logo program has been defined. The IPv6 logo gives confidence to users that IPv6 is currently operational. It is also a clear indication that the technology will still be used in the future. This logo program contributes to the feeling that IPv6 is available and ready to be used.

Segment Routing over IPv6 (SRv6) leverages IPv6 extension headers for source routing. SRv6 provides the ability to code directly into each packet header where the traffic should be sent and how the traffic should be treated. Note this document only tests SRv6, and has no testable items for SR MPLS.

Definitions

MTU	Maximum Transmission Unit
RUT	Router Under Test
SR	Segment Routing
SRH	Segment Routing Header
SID	Segment Identifier
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: SR6.IOP.A.B Where each component indicates the following: SR6 – 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.
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:

[SR] C. Filsfils, S. Previdi, L. Ginsberg, B. Decraene, S. Litkowski, R. Shakir, Segment Routing Architecture, RFC 8402.

[IPV6-SRH] C. Filsfils, D. Dukes,S. Previdi, J. Leddy, S. Matsushima, D. Voyer, IPv6 Segment Routing Header (SRH), RFC 8754.

[SRv6] C. Filsfils, P. Camarillo, J. Leddy, D. Voyer, S. Matsushima, Z. Li, Segment Routing over IPv6 (SRv6) Network Programming, RFC 8986.

General Node Requirements

Segment Router:

- Ability to configure Segment Routing Header.
- Ability to add SID.
- Ability to add/process Segment List.
- Ability to process the Segment Left/Last Entry.

Common Test Setup

- Enable SRv6 on the RUT (Router Under Test) and Two TAR-Routers.
- Configure the interfaces as SR Segments/Nodes as mentioned in the Test setup/Topology.
- Configure routes on each router to ensure networks are reachable in every Part.

Common Test Cleanup

- After each of the test procedures, the SR policies, route entries and neighbor caches which are configured or created on the routers should be deleted.

Test Performed on Router

The tests under the Router column marked by an "X" must be performed as specified below. If there is no "X" listed under the Router column, this test may be omitted. In the test environment, there should be two couples of TAR-Router1 and TAR-router2.

	Routers:
SR6Interop.1.1a	X
SR6Interop.1.1b	X
SR6Interop.1.2a	X
SR6Interop.1.2b	X
SR6Interop.1.3a	X
SR6Interop.1.3b	X
SR6Interop.1.3c	X
SR6Interop.1.3d	X
SR6Interop.1.4a	X
SR6Interop.1.4b	X
SR6Interop.1.4c	X
SR6Interop.1.4d	X
SR6Interop.1.4e	X
SR6Interop.1.5a	X
SR6Interop.1.5b	X
SR6Interop.1.6a	X
SR6Interop.1.6b	X

Advanced Functionality Tests

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

End.T:

Test SR6Interop.1.6 - Part B: End.T

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:

Group 1:

Scope

Tests in this group verify that the target Routers are able to engage in various aspects of the IPv6 Segment Routing protocols.

Overview

The following tests verify operations such as .

Test SR6Interop.1.1: SRv6 Enable

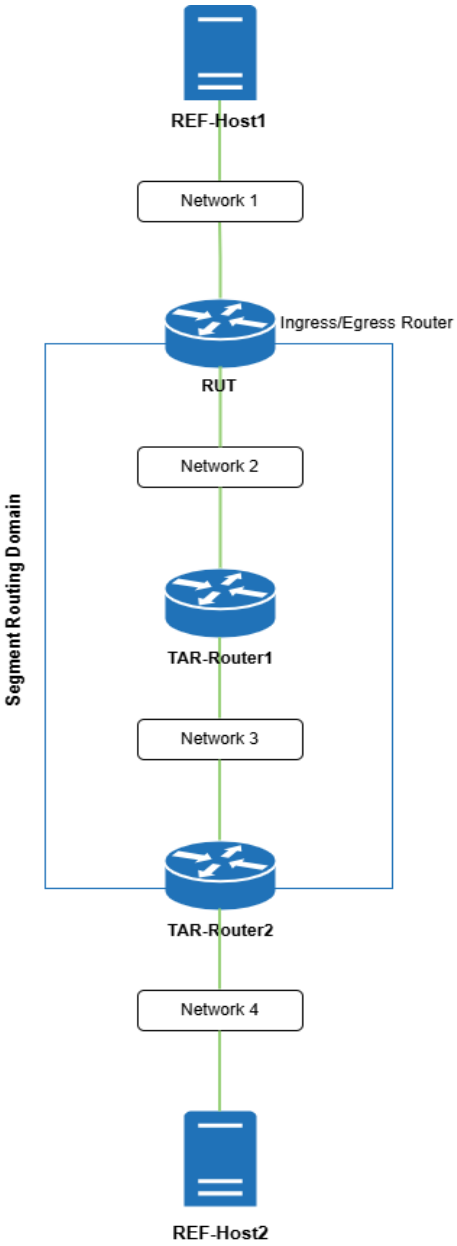
Purpose: Verify the proper behavior of a router with SRv6 SIDs by default.

Reference:

- [SR] – Section 3.1.3

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

For Part A and Part B



Procedure:

Part A: SRv6 disable

Step	Action	Expected Behavior
1.	RUT is not configured for SRv6.	
2.	Transmit an ICMPv6 Echo Request from REF-Host1 to the Global Address of REF-Host2.	The RUT must forward the ICMPv6 Echo Request without an SRH and REF-Host2 should generate an Echo reply.

Part B: SRv6 enable

Step	Action	Expected Behavior
3.	RUT is configured to enable SRv6.	
4.	Configure the RUT SR Policy <TAR-Router1,TAR-router2>	
5.	Transmit an ICMPv6 Echo Request from REF-Host1 to the Global Address of REF-Host2	The RUT must forward the ICMPv6 Echo Request with an outer header and SRH and REF-Host2 should generate an Echo reply.

Test SR6Interop.1.2: Outside and inside domain traffic

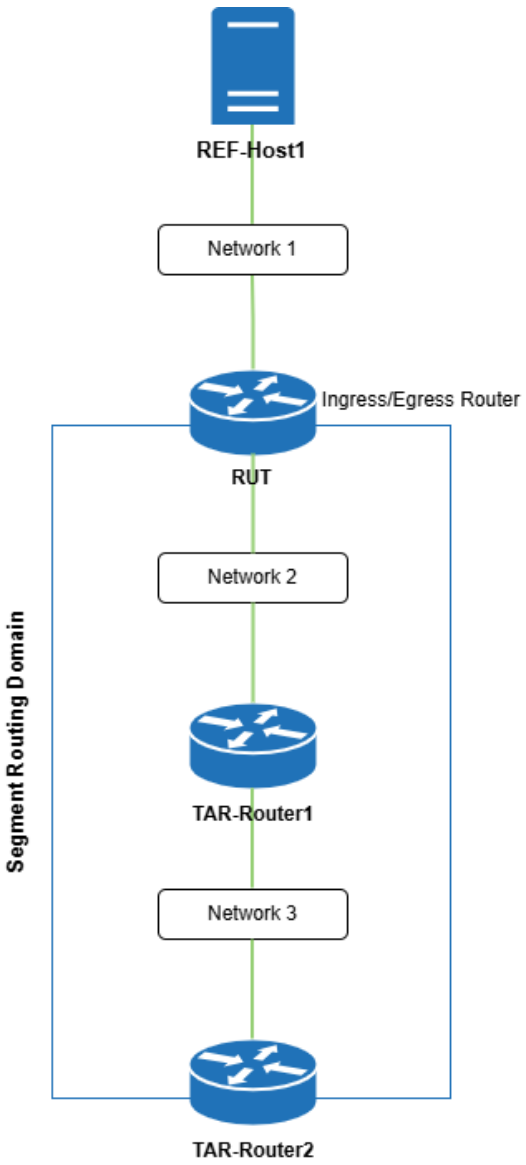
Purpose: Verify that a router properly processes the traffic outside or inside domain.

Reference:

- [SR] - 8.2

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

For Part A and Part B



Procedure:

Part A: Traffic outside domain

Step	Action	Expected Behavior
1.	Configure RUT as an ingress router of the SR Domain. Configure TAR-Router1, and TAR-Router2 as segments in the SR Domain.	
2.	Configure the RUT SR policy <TAR-Router1, TAR-Router2>	
3.	Transmit an ICMPv6 Echo Request from REF-Host1 to TAR-Router2's SID address.	The RUT must filter the traffic and must not forward the ICMPv6 Echo Request to TAR-Router2.

Part B: Traffic inside domain

Step	Action	Expected Behavior
4.	Configure RUT as an egress router of the SR Domain. Configure TAR-Router1, and TAR-Router2 as segments in the SR Domain.	
5.	Configure the TAR-Router2 SR policy <TAR-Router1,RUT>	
6.	Transmit an ICMPv6 Echo Request from TAR-Router2 to the Global Address of REF-Host1.	The RUT must forward the IPv6 packet to REF-Host1 after removing the Outer Header and SRH from the packet.

Test SR6Interop.1.3: Configuring and Processing Segment List

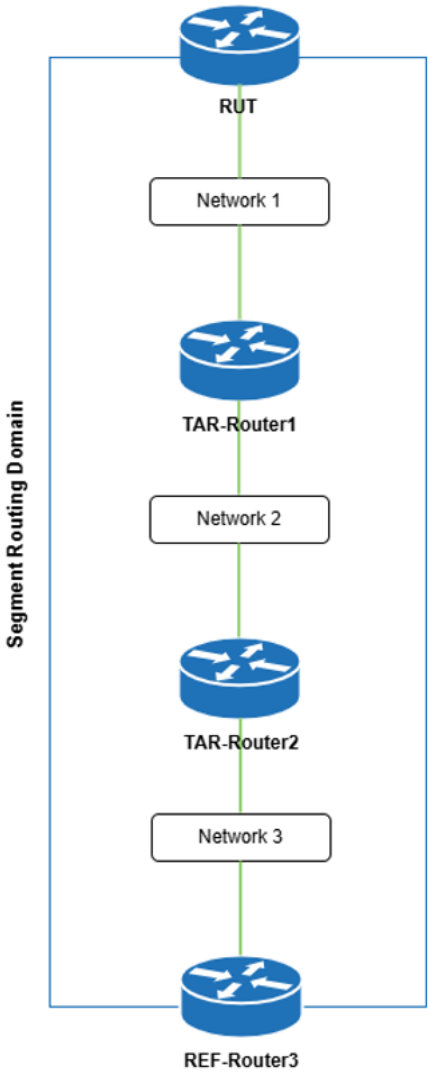
Purpose: Verify that a router properly configures and processes the segment list in the Segment Routing Header (SRH).

Reference:

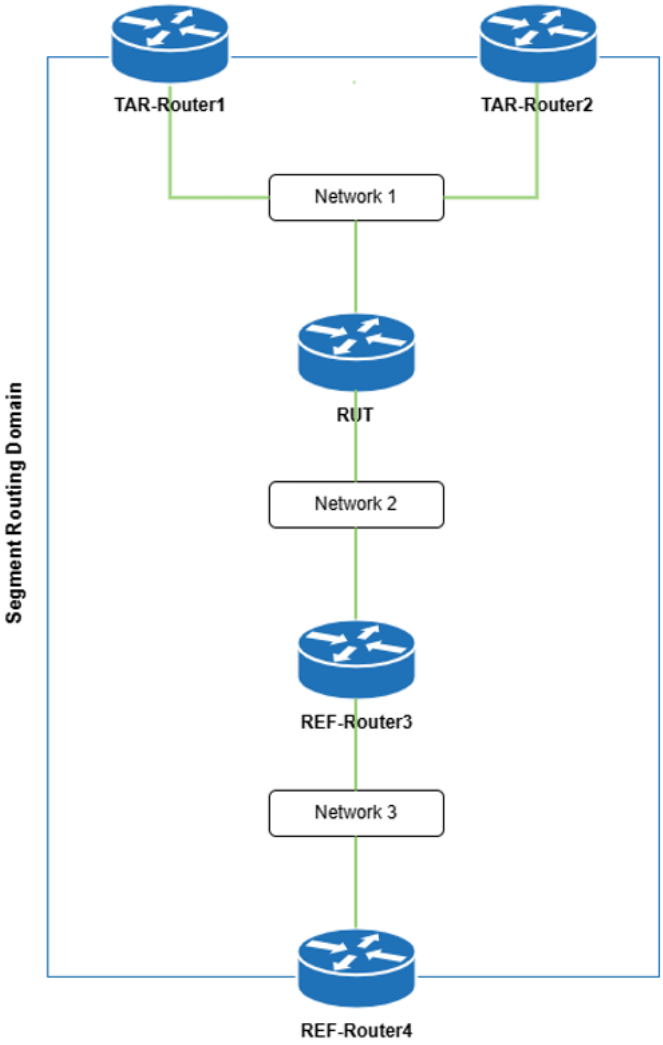
- [IPv6-SRH] – Section 2.1

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

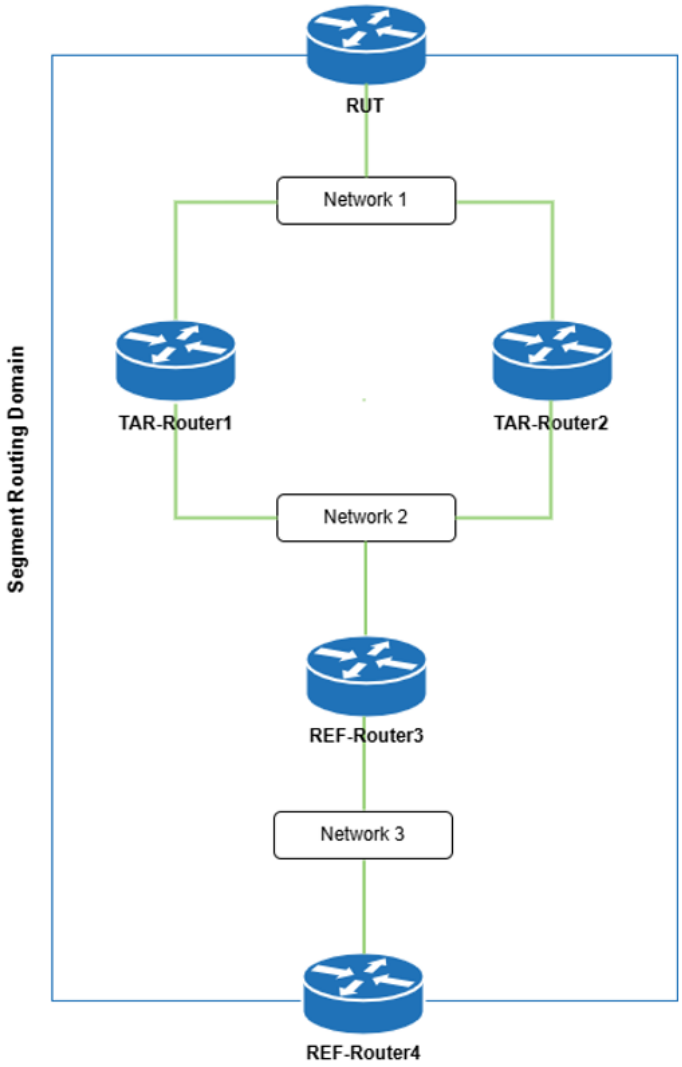
For Parts A and B:



For Part C:


TAR-Router1
TAR-Router2
Network 1
RUT
Network 2
REF-Router3
Network 3
REF-Router4
Segment Routing Domain

For Part D:



Procedure:

Part A: Configuring Segment List

Step	Action	Expected Behavior
1.	Configure the RUT, TAR-Router1, TAR-Router2, and REF-Router3 as segments in the SR Domain.	
2.	Configure the RUT SR policy <TAR-Router1, TAR-Router2, REF-Router3>.	
3.	Transmit an ICMPv6 Echo Request from RUT to the Global Address of REF-Router3.	The RUT must transmit an echo request with the configured SR Policy to the Global

		Address of REF-Router3, and REF-Router3 should respond with an Echo Reply .

Part B: Configuring Segment list without transit node

Step	Action	Expected Behavior
4.	Configure the RUT, TAR-Router2, and REF-Router3 as segments and configure the TAR-Router1 as a Transit Node in the SR Domain.	
5.	Configure the RUT SR policy <TAR-Router2, REF-Router3>.	
6.	Transmit an ICMPv6 Echo Request from RUT to the Global Address of REF-Router3.	The RUT must transmit an Echo Request with the configured SR Policy to the Global Address of REF-Router3 without TAR-Router1 SID. TAR-Router1 must not process the SRH, and it should be visible on Network2.

Part C: Processing the SRv6 Packet based on the Segment list

Step	Action	Expected Behavior
7.	Configure the RUT, TAR-Router1, TAR-Router2 and REF-Router3, and REF-Router4 as segments in the SR Domain	
8.	Configure the TAR-Router1 SR policy <RUT, REF-Router3, REF-Router4>. Configure the TAR-Router2 SR policy <REF-Router3, REF-Router4>. Make sure that the RUT is configured the same for processing the SR policies stated above.	
9.	Transmit an Echo Request from TAR-Router1 to the Global Address of REF-Router4.	The RUT must process the SRH and forward the Echo request to REF-Router4. REF-Router4 should generate an Echo reply to TAR-Router 1.
10.	Transmit an Echo Request from TAR-Router2 to the Global Address of REF-Router4.	The RUT must forward the Echo request to REF-Router4 and must not process the SRH and it should be visible on Network2. REF-Router4 should generate an Echo Reply to TAR-Router2.

Part D: Forwarding the SRv6 Packet based on the Segment list

Step	Action	Expected Behavior

11.	Configure the RUT, TAR-Router1, TAR-Router2, REF-Router3 and REF-Router4 as segments in the SR Domain	
12.	Configure the RUT SR policy <TAR-Router1, REF-Router3>.	
13.	Transmit an Echo Request from RUT to the Global Address of REF-Router4.	The RUT must send an Echo request to REF-Router4 with the first hop through TAR-Router1 and it should be visible on Network2. REF-Router4 should generate an Echo reply.
14.	Configure the RUT SR policy <TAR-Router2, REF-Router3>. Make sure to clear the previous SR policy.	
15.	Transmit an Echo Request from RUT to the Global Address of REF-Router4.	The RUT must send an Echo request to REF-Router4 with the first hop through TAR-Router2 and it should be visible on Network2. REF-Router4 should generate an Echo reply.

Possible Problems:

- None.

Test SR6Interop.1.4: Packet Forwarding behavior of SR Nodes

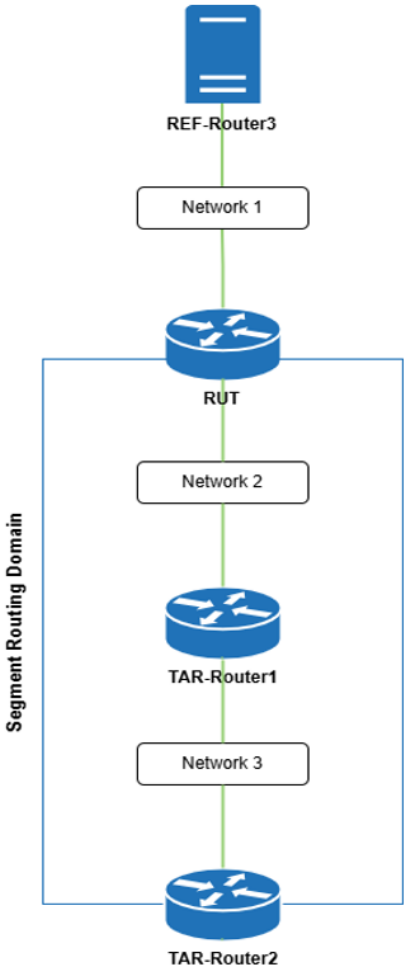
Purpose: Verify the proper behavior of SR nodes when it encounters a Segment Routing Header (SRH).

Reference:

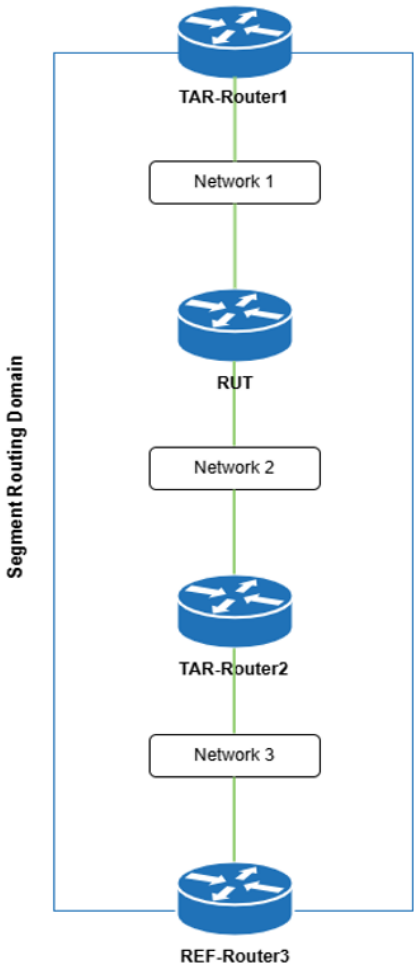
- [IPv6-SRH] – Section 3, Section 4.1, 4.2, 4.3, 5.1

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

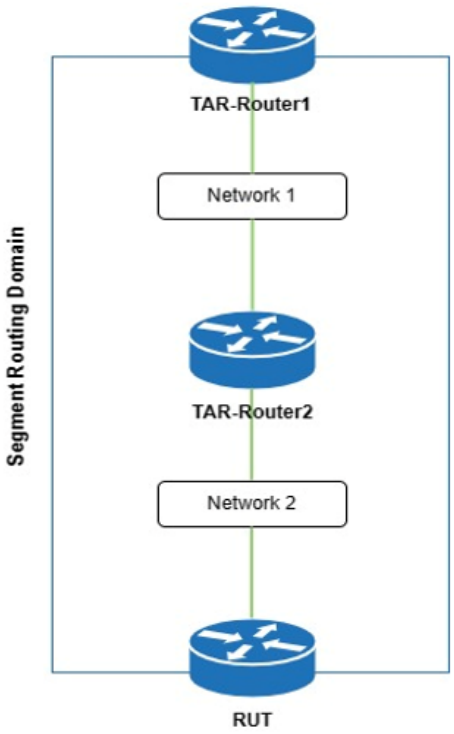
For Parts A and E:



For Parts B and C:



For Part D:



Procedure:

Part A: Source Node - Ingress Router

Step	Action	Expected Behavior
1.	Configure RUT as an ingress router of the SR Domain. Configure TAR-Router1, and TAR-Router2 as segments in the SR Domain.	
2.	Configure the RUT SR policy <TAR-Router1, TAR-Router2>.	
3.	Transmit an ICMPv6 Echo Request from REF-Router3 to the Global Address of TAR-Router2.	RUT should encapsulate the received packet in an outer header with an SRH and must transmit the packet to TAR-Router2 and it should be visible on Network2.

Part B: Transit Node

Step	Action	Expected Behavior

4	Configure the TAR-Router1, TAR-Router2 and REF-Router3 as segments and configure the RUT as a Transit Node in the SR Domain.	
5.	Configure the TAR-Router1 SR policy <TAR-Router2, REF-Router3>.	
6.	Transmit an ICMPv6 Echo Request from TAR-Router1 to the Global Address of REF-Router3.	The RUT must forward the packets to TAR-Router2 and must not process the SRH and it should be visible on Network2.

Part C: Segment Intermediate Node

Step	Action	Expected Behavior
7.	Configure the RUT, TAR-Router1, TAR-Router2, and REF-Router3 as segments in the SR Domain.	
8.	Configure the TAR-Router1 SR policy <RUT, TAR-Router2, REF-Router3>.	
9.	Transmit an ICMPv6 Echo Request from TAR-Router1 to the Global Address of REF-Router3.	The RUT must decrease the Hop limit and Segments Left Value in the SRH and forward the packets to the Global address of REF-Router3.

Part D: Segment End Point Node

Step	Action	Expected Behavior
10.	Configure the RUT, TAR-Router1, and TAR-Router2 as segments in the SR Domain.	
11.	Configure the TAR-Router1 SR policy <TAR-Router2, RUT>.	
12.	Transmit an ICMPv6 Echo Request from TAR-Router1 to the Global Address of RUT.	The RUT must generate an echo reply in response to the echo request using TAR-Router2 as the first hop.

Part E: Segment End Point Node - Egress Router

Step	Action	Expected Behavior
13.	Configure RUT as an Egress router of the SR Domain and configure TAR-Router1 and TAR-Router2 as segments in the SR Domain	
14.	Configure the TAR-Router2 SR policy <TAR-Router1, RUT>.	

15.	Transmit an ICMPv6 Echo Request from TAR-Router2 to the Global Address of REF-Router3.	The RUT must decapsulate the received echo request that has SRH from TAR-Router2 and must forward the IPv6 packet to REF-Router3 after removing the Outer Header and SRH from the packet.

Possible Problems:

- None.

Test SR6Interop.1.5: SRv6 PMTU

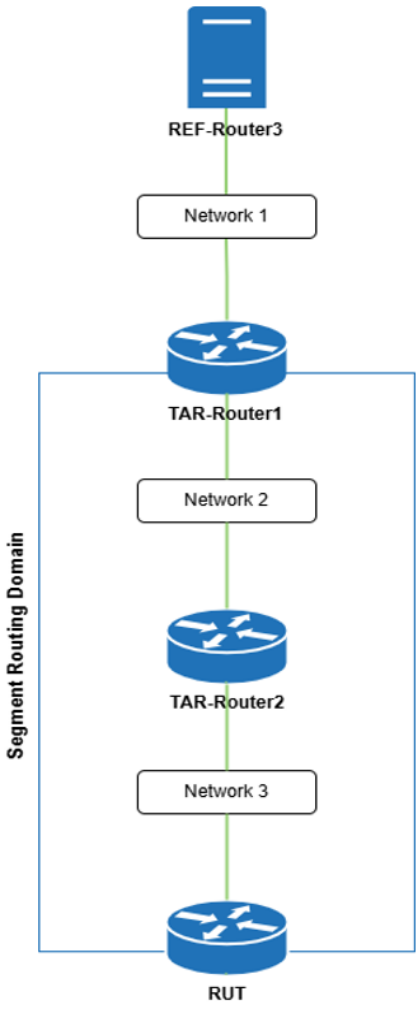
Purpose: Verify that a router properly reduces its estimate of the Path MTU when it receives a Packet Too Big message and to check that a router properly generates a Packet Too Big message when it receives a packet with greater MTU.

Reference:

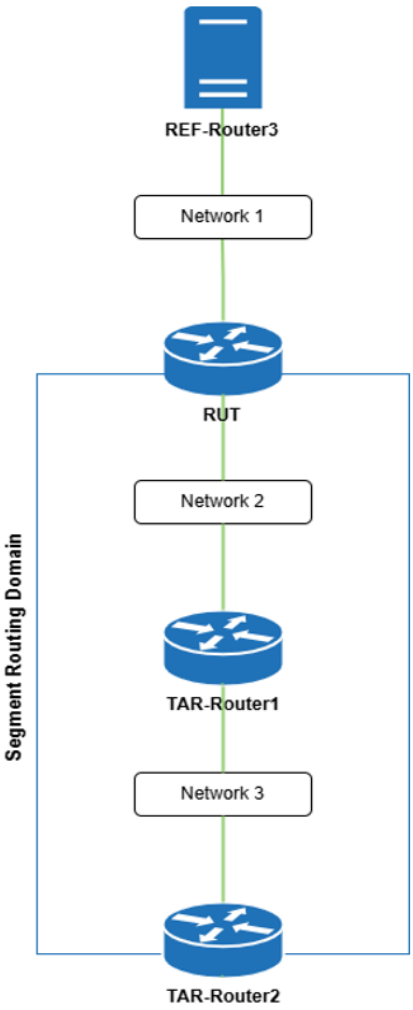
- [IPv6-SRH] – Section 3, Section 4.1, 4.2, 4.3, 5.1

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

For Part A:



For Part B:



Procedure:

Part A: Processing Packet Too Big Message

Step	Action	Expected Behavior
1.	Configure TAR-Router1 as an ingress router of the SR Domain and configure RUT, TAR-Router2 as segments in the SR Domain.	
2.	Configure the TAR-Router1 SR policy <TAR-Router2, RUT>.	
3.	Transmit an ICMPv6 Echo Request with a packet size equal to 1420 octets from REF-Router3 to the Global Address of RUT.	TAR-Router1 should encapsulate the received packet in an outer header with an SRH and must transmit the packet to RUT and it should be visible on Network2. RUT should generate an echo reply.
4.	Configure the TAR-Router1 Network1 interface with a path MTU of 1280 bytes and configure the RUT SR policy <TAR-Router2, TAR-Router1>.	
5.	Transmit an ICMPv6 Echo Request with a packet size equal to 1420 octets from RUT to the Global Address of REF-Router3.	If RUT attempts to transmit the echo request without fragmenting, TAR-Router1 should transmit a Packet Too Big message to the RUT, which contains an MTU field with a value of 1280. RUT must lower its path MTU estimate and fragment the Echo Request, REF-Router3 must respond to the Echo Request with an Echo Reply

Part B: Transmitting Packet Too Big Message

Step	Action	Expected Behavior
6.	Configure RUT as an ingress router of the SR Domain and configureTAR-Router1, TAR-Router2 as segments in the SR Domain.	
7.	Configure the RUT SR policy <TAR-Router1, TAR-Router2>.	
8.	Transmit an ICMPv6 Echo Request with a packet size equal to 1420 octets from REF-Router3 to the Global Address of TAR-Router2.	RUT should encapsulate the received packet in an outer header with an SRH and must transmit the packet to TAR-Router2 and it should be visible on Network2. TAR-Router2 should generate an echo reply.
9.	Configure the RUT Network1 interface with a path MTU of 1280 bytes and configure the TAR-	

	Router2 SR policy <TAR-Router1, RUT>.	
10.	Transmit an ICMPv6 Echo Request with a packet size equal to 1420 octets from TAR-Router2 to the Global Address of REF-Router3.	TAR-Router2 should attempt to send the Echo Request without fragmenting, RUT should transmit a Packet Too Big message to the TAR-Router2, which contains an MTU field with a value of 1280.TAR-Router2 must lower its path MTU estimate and fragment the Echo Request, REF-Router3 must respond to the Echo Request with an Echo Reply

Possible Problems:

- None.

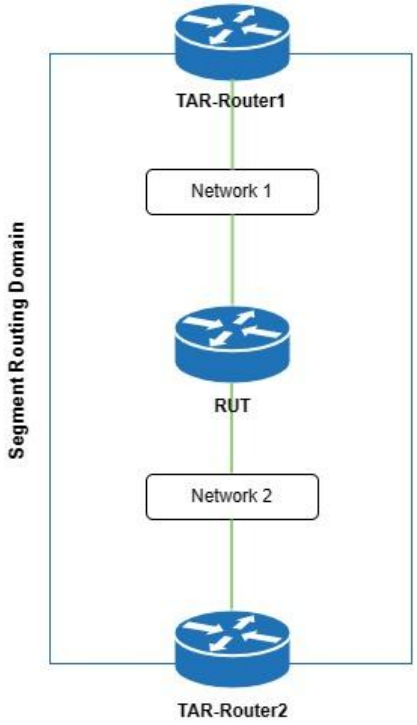
Test SR6Interop.1.6: SRv6 Endpoint Behavior

Purpose: Verify the proper behavior of a router with End.X and End.T codepoint.

Reference:

- [SR] – Section 4.2, 4.3

Test Setup: Connect all the devices as per the figure below.
For Part A and Part B



Procedure:

Part A: End.X

Step	Action	Expected Behavior
1.	Configure SID codepoint to End.X on RUT.	
2.	Transmit an ICMPv6 Echo Request with SR Header from TAR-Router1 to the RUT, The SIDs list indicates <RUT, TAR-Router2>	The RUT should process the SRH, decrement the IPv6 Hop Limit by 1, decrement Segments Left by 1, update IPv6 DA with Segment List[Segments Left], Submit the packet to the IPv6 module for transmission to TAR-Router2.

Part B: End.T

Step	Action	Expected Behavior
3.	Configure SID codepoint to End.T on RUT.	
4.	Transmit an ICMPv6 Echo Request with SR Header from TAR-Router1 to the RUT, The SIDs list indicates <RUT, TAR-Router2>	The RUT should process the SRH, decrement IPv6 Hop Limit by 1, decrement Segments Left by 1, update IPv6 DA with Segment List[Segments Left], Set the packet's associated FIB table to T, Submit the packet to the egress IPv6 FIB lookup for transmission to the new destination

Possible Problems:

- None.

Modification Record

Version 0.0.0 December 9, 2024

- Draft for RFC8402.
- Draft for RFC8754.
- Draft for RFC8986