INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2025-2028

SG11-TD975/GEN

STUDY GROUP 11

Original: English

Question(s): 13/11 Geneva, 3-11 March 2026

TD

Source: Editor

Title: Agreement – draft new Technical Report ITU-T QSTR.SRv6_Conf "Method for verifying conformance to segment routing over IPv6" (Geneva, 3-11 March 2026)

Contact: Krishna Kumar Lahoti
CNLABS
India

Tel: +91 7207580125
E-mail: krishna@cnlabs.in

Abstract: This document contains the output proposed for Agreement of draft new Technical Report ITU-T QSTR.SRv6_Conf "Method for verifying conformance to segment routing over IPv6". It includes the discussion results from the Q13/11 sessions during the SG11 meeting, Geneva, 3-11 March 2026.

No.	Source	Title	Discussion and results
C346R1	Ministry of Communications, Department of Telecommunications (India)	Proposal for agreement of draft Technical Report QSTR.SRv6_Conf "Method for verifying conformance to segment routing over IPv6" (Geneva, 3-11 March 2026)	Accepted with modifications. 1. Editorial/text changes for clarity 2. Acronyms and Abbreviations in alphabetical order 3. Standard numbers in numerical order 4. Addition of table numbers and names 5. Removal of redundant text and standard references 6. Updated Conventions to None

Draft new Technical Report ITU-T QSTR.SRv6_Conf

Method for verifying conformance to segment routing over IPv6

Summary

Segment Routing over IPv6 (SRv6) is a cutting-edge networking technology merging the capabilities of Segment Routing and IPv6. By embedding instructions directly into IPv6 headers, SRv6 simplifies packet forwarding, providing better scalability, flexibility, and network programmability. It facilitates efficient traffic engineering, service chaining, and network slicing and plays a pivotal role in shaping the landscape of next-generation networks.

However, the rapid adoption of SRv6 introduces critical challenges in ensuring conformance, interoperability, and reliability across diverse implementations and deployments. Without testing methodologies, discrepancies in SRv6 implementations can lead to operational inefficiencies, reduced network performance, and barriers to widespread adoption. Addressing this gap is imperative to unlock the full potential of SRv6 and foster trust in its deployment.

This technical report seeks to study test methodologies to ensure the conformance of SRv6 implementations on network devices to the SRv6 standards created by the Internet Engineering Task Force (IETF). The verification of conformance to SRv6 standards is aligned with key IETF RFCs (RFC 8402, RFC 8986, RFC 8754). The technical report will identify key conformance testing requirements, establish rigorous testing methodologies, and outline compliance criteria to ensure consistent and compliant implementations of SRv6 across network devices.

Through detailed verification processes, this technical report will provide network equipment manufacturers, service providers, and regulatory bodies with a structured approach to assess, validate, and certify SRv6 conformance. This effort is pivotal for fostering collaboration within the industry, accelerating the adoption of SRv6, and creating a robust ecosystem of reliable and compliant next-generation networks.

Keywords

Segment Routing, IPv6, SRv6, Conformance

Table of Contents

Draft new Technical Report ITU-T QSTR.SRv6_Conf

Method for verifying conformance to segment routing over IPv6

1. Scope

This Technical Report aims to research methods for verifying conformance to Segment Routing Over IPv6 (SRv6) standards.

The scope of this Technical Report includes the following:

- Identification of core SRv6 standards to verify a device's conformance to SRv6 technology
- Identification of testing cases from core SRv6 standards
- The test topologies required for verifying conformance to SRv6
- SRv6 Conformance Testing – Testing Methodology, Test Procedures and Expected Results
- Relationship with other related standard groups for SRv6

Note: The IETF does NOT identify a subset of SRv6-related specifications as "Core SRv6 Standards". However, since this technical report aims to propose a method to verify conformance only to SRv6 standards, the verification of a device's conformance to certain routing protocols (such as OSPF, BGP and IS-IS) that may be used in conjunction with SRv6, remains out of scope of this technical report. Hence, the term "Core SRv6 Standards" used in this document is a classification specific to ITU-T Study Group 11. Additionally, this technical report neither introduces any new requirements, nor alters the existing requirements from the IETF standards in any manner. It simply aims to provide a test methodology to verify whether a device conforms to specific IETF standards, namely RFC 8402, RFC 8754, and RFC 8986.

Additionally, while conformance to SRv6 standards can guarantee a device's adherence to SRv6 technical specifications, it does not guarantee seamless interoperability. Various factors, such as variability in implementations due to interpretation, support for optional features & extensions, network conditions & security policies, edge cases & unspecified behaviours, may lead to interoperability issues. As such, this technical report neither aims to cover all interoperability issues nor to propose potential solutions to address them.

2. References

The following references contain provisions which, through reference in this text, constitute provisions of this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below. The reference to a document within this Technical Report does not give it, as a stand-alone document, the status of a Recommendation.

[IETF RFC 2119] IETF RFC 2119 (1997)**,** *Key words for use in RFCs to Indicate Requirement Levels.*

[IETF RFC 8402] IETF RFC 8402 (2018), *Segment Routing Architecture*.

[IETF RFC 8665] IETF RFC 8665 (2019), *OSPF Extensions for Segment Routing*.

[IETF RFC 8666] IETF RFC 8666 (2019), *OSPFv3 Extensions for Segment Routing*.

[IETF RFC 8667] IETF RFC 8667 (2019), *IS-IS Extensions for Segment Routing.*

[IETF RFC 8754] IETF RFC 8754 (2020), *IPv6 Segment Routing Header (SRH).*

[IETF RFC 8986] IETF RFC 8986 (2021), *Segment Routing over IPv6 (SRv6) Network Programming.*

[IETF RFC 9252] IETF RFC 9252 (2022), *BGP Overlay Services Based on Segment Routing over IPv6 (SRv6).*

[IETF RFC 9259] IETF RFC 9259 (2022), *Operation, Administration, and Maintenance (OAM) in SRv6 Networks.*

[IETF RFC 9352] IETF RFC 9352 (2023), *IS-IS Extensions to Support Segment Routing over the IPv6 Data Plane*

[IETF RFC 9487] IETF RFC 9487 (2023), *Export of Segment Routing over IPv6 Information in IP Flow Information Export (IPFIX).*

[IETF RFC 9602] IETF RFC 9602 (2024), *Segment Routing over IPv6 (SRv6) Segment Identifiers (SIDs) in the IPv6 Addressing Architecture*

3. Definitions

3.1. Terms defined elsewhere

This Technical Report uses the following terms, as defined elsewhere:

3.1.1. segment [IETF RFC 8402]: An instruction a node executes on the incoming packet (e.g., forward packet according to shortest path to destination, or, forward packet through a specific interface, or, deliver the packet to a given application/service instance).

3.1.2. SID [IETF RFC 8402]: A segment identifier.

3.1.3. SRv6 [IETF RFC 8402]: The instantiation of SR on the IPv6 data plane.

3.1.4. SRv6 SID [IETF RFC 8402]: An iPv6 address explicitly associated with the segment.

3.1.5. SRv6 SID function [IETF RFC 8986]: The function part of the SID is an opaque identification of local behavior bound to the SID.

3.1.6. SRv6 endpoint behavior [b-IETF RFC 8986]: A packet processing behavior executed at an SRv6 Segment Endpoint Node. SRv6 Endpoint behaviors related to traffic engineering and overlay use cases.

3.2. Terms defined in this Technical Report

None

4. Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

IETF Internet Engineering Task Force

IPv6 Internet Protocol version 6

MTU Maximum Transmission Unit

PSID Path Segment Identifier

RUT Router Under Test

SID Segment ID

SL Segment List

SRH Segment Routing Header

SRv6 Segment Routing Over IPv6

TLLA Target Link-layer Address

TN Test Node

TR Test Router

5. Conventions

None

6. Overview

As outlined in the IETF standards RFC 8402, RFC 8986, and RFC 8754, SRv6 provides an advanced approach to routing by encoding instructions, known as Segment Identifiers (SIDs), directly into IPv6 packet headers. This architecture enables advanced functionalities, including:

- Simplification of network operations by eliminating complex signalling protocols.
- Efficient traffic engineering to optimize resource utilization and meet specific Quality of Service requirements.
- Seamless implementation of service chaining and network slicing, crucial for next-generation network architectures.
- Enhanced scalability and flexibility to meet evolving networking demands.

SRv6's capabilities make it a foundational technology for next-generation networks, but ensuring conformance across diverse implementations is critical to unlocking its full potential. Inconsistent or non-compliant implementations can lead to interoperability issues, diminished performance, and potential network failures.

The proposed method for verifying SRv6 conformance, focuses on verifying adherence to the core specifications and functional requirements outlined in the relevant RFCs. The framework is designed to:

- Validate the correct encoding and processing of SIDs within IPv6 headers.
- Ensure compliance with SRv6's forwarding and processing behavior across network devices.
- Establish clear testing criteria and scenarios to evaluate the performance and reliability of SRv6-enabled networks.
- Identify potential interoperability challenges between SRv6 implementations from different vendors.

This Technical Report aims to develop testing methodologies to ensure that SRv6 implementations conform to relevant IETF standards. The focus is on validating network device behavior to ensure reliable deployment of SRv6, and to foster interoperability within a multi-vendor ecosystem.

7. Relevance of this Technical Report and Existing Standardization Work

This Technical Report aims to create a SRv6 conformance test framework by identifying conformance testing cases, testing methodologies, testing procedures and expected behaviour under various test conditions. Conformance testing ensures that an implementation correctly follows the SRv6 standards. It ensures protocol compliance, improves network reliability, enhances interoperability by providing the foundation for interoperability testing for multi-vendor deployments, reduces deployment risks & costs, and builds confidence among operators and regulators. The following Table 1 provides an analysis of other relevant standards and testing specifications from ITU-T and IETF. Whereas, this technical report aims to create a method for verifying conformance of network devices to SRv6 standards.

Table 1 - Gap Analysis with Existing Standards

S. No.	SDO	Title	Status	Analysis
1	ITU-T	[b-ITU-T Y.3216] (09/2024): Fixed, mobile and satellite convergence – Distributed core network for IMT-2020 networks and beyond	In Force	Recommendation ITU-T Y.3216 specifies the general considerations, requirements, network function enhancements, procedures and security considerations of distributed core network in fixed, mobile and satellite convergence (FMSC) network, in the context of international mobile telecommunications for 2020 (IMT-2020) and beyond. SRv6 is acknowledges as a relevant technology.
2	ITU-T	[b-ITU-T Q.4141] (12/2023): Requirements and signalling of intelligence control for the border network gateway in computing power networks	In force	This Recommendation aims to study the requirements and signalling of intelligence control for the border network gateway in a computing power network (CPN). SRv6 is acknowledged as a relevant technology.
3	ITU-T	ITU-T Y.3657 (12/2023): Big data driven networking – Requirements and capabilities of network visibility	In Force	Recommendation ITU-T Y.3657 specifies requirements and capabilities of network visibility for big-data-driven networking (bDDN). It focuses on the scenario where network infrastructure layer of bDDN corresponds to Internet protocol (IP) bearer network. .
4	ITU-T	ITU-T Q.4070 (02/2023): Test suite for interoperability testing of virtualized broadband network gateways	In force	Recommendation ITU-T Q.4070 specifies the interoperability testing of virtualized broadband network gateway (vBNG), including an overview of the test suite and test cases for interoperability testing of vBNG.
5	ITU-T	QSTR.MPM-SRv6 Methods for the Performance Monitoring of SRv6 Networks	TR	It aims to specify performance monitoring parameters and metrics for measuring performance of SRv6 networks such as Traffic Monitoring, Path Monitoring, Statistical Analysis, Log Analysis, etc.
6	IETF	IETF RFC 8402 (2018), Segment Routing Architecture	Internet Standards Track document	RFC 8402 defines the architecture of Segment Routing (SR), including core concepts such as SIDs, SR policies, control-plane distribution, and both SR-MPLS and SRv6 instantiations. It describes how implementations should support the SR architecture and related behaviors.
7	IETF	IETF RFC 8665 (2019), OSPF Extensions for Segment Routing.	Internet Standards Track document	RFC 8665 defines OSPFv2 extensions to advertise Segment Identifiers (SIDs) and SR capabilities. It specifies how implementations must support SR extensions within OSPF.
8	IETF	IETF RFC 8666 (2019), OSPFv3	Internet Standards	RFC 8666 provides the OSPFv3 extensions needed for SR, including advertisement of SRv6-related attributes. It indicates

		Extensions for Segment Routing.	Track document	how implementations should support SID and SR capability distribution in IPv6 OSPF networks.
9	IETF	IETF RFC 8667 (2019), IS-IS Extensions for Segment Routing.	Internet Standards Track document	RFC 8667 specifies IS-IS extensions for SR, defining TLVs used to advertise SIDs and SR capabilities. It describes how implementations should support SR information distribution in IS-IS networks.
10	IETF	IETF RFC 8754 (2020), IPv6 Segment Routing Header (SRH)	Internet Standards Track document	RFC 8754 specifies the IPv6 Segment Routing Header (SRH), including header format, packet processing rules, and error-handling. It defines how implementations must support SRH insertion, parsing, and forwarding.
11	IETF	IETF RFC 8986 (2021), Segment Routing over IPv6 (SRv6) Network Programming.	Internet Standards Track document	RFC 8986 defines the SRv6 Network Programming model, including endpoint behaviors (End, End.X, End.T, etc.), SID semantics, function execution, and forwarding rules. It dictates how an SRv6 implementation must support specific SRv6 behaviors.
12	IETF	IETF RFC 9252 (2022), BGP Overlay Services Based on Segment Routing over IPv6 (SRv6).	Internet Standards Track document	RFC 9252 standardizes how BGP distributes SRv6 service information and how implementations should support SRv6-based VPN and service overlays. It defines the procedures a conformant implementation must support for SRv6 BGP signaling.
13	IETF	IETF RFC 9259 (2022), Operation, Administration, and Maintenance (OAM) in SRv6 Networks.	Internet Standards Track document	RFC 9259 defines OAM mechanisms for SRv6 networks, such as active probing, path monitoring, and diagnostics. It prescribes how implementations should support SRv6 OAM features and procedures.
14	IETF	IETF RFC 9352 (2023), IS-IS Extensions to Support Segment Routing over the IPv6 Data Plane.	Internet Standards Track document	RFC 9352 defines IS-IS extensions for distributing SRv6-specific SIDs and capabilities. It specifies how implementations must support SRv6 data-plane signaling within the IS-IS protocol.
15	IETF	IETF RFC 9487 (2023), Export of Segment Routing over IPv6 Information in IP Flow Information Export (IPFIX).	Internet Standards Track document	RFC 9487 specifies how SRv6 telemetry and flow information should be exported using IPFIX. It defines data templates and requirements for SRv6-aware instrumentation.
16	IETF	draft-ietf-bmwg-sr-bench-meth-05 Benchmarking Methodology for Segment Routing	Active Internet-Draft	This document defines a methodology for benchmarking Segment Routing (SR) performance for Segment Routing over IPv6 (SRv6) and MPLS (SR-MPLS). It builds upon RFC 2544, RFC 5180, RFC 5695 and RFC 8402. Test parameters include Throughput, Buffer Size, Latency, Frame Loss, System Recovery, Reset, Scaling.

8. Research for Verifying Conformance to SRv6

8.1. Identification of Core SRv6 Standards to Verify Conformance

IETF is a global standards development organization (SDO) creating internet standards (RFCs) for networking protocols and technologies. For SRv6, the IETF has created several standards as mentioned in clause 7

While these standards collectively establish a comprehensive framework for implementing and deploying SRv6 technology in modern networks, identifying “Core SRv6 standards” is essential for the scope of this technical report. These core standards serve as the basis for verifying whether a device conforms to SRv6, helping operators determine if a device has fundamental SRv6 support while ensuring compliance with standards, and enabling regulators to assess adherence to SRv6 specifications for certification and policy enforcement. It must be noted that the IETF does not

identify a subset of SRv6-related specifications as “Core SRv6 Standards” and that the term “Core SRv6 Standards” used in this document is a classification specific to this Technical Report.

After a careful study of all the above-mentioned standards, only three standards *viz*., RFC 8402, RFC 8754, and RFC 8986 are considered as “Core SRv6 standards” that are crucial in the context of this technical report. These RFCs define the fundamental architecture, encapsulation, and network programming model required for SRv6 functionality.

The other RFC standards, such as RFC 8665, RFC 8666, RFC 8667, RFC 9252, RFC 9352, and RFC 9433, primarily deal with routing protocol extensions (OSPF, IS-IS, BGP), service overlays, mobile user plane integration, and operational aspects of SRv6 deployment. While these standards are critical for specific use cases, optimizations and interoperability, they are not fundamental requirements for verifying whether a device conforms to the core SRv6 protocol specifications.

Additionally, other SRv6 specifications that are being developed by IETF’s SPRING working group will be reviewed once they are finalized and published. Any new test cases may then be introduced in this document as per ITU-T SG11’s working process.

8.2. Identification of test cases from Core SRv6 standards

As per IETF RFC 2119, the mandatory and optional test cases are derived based on the following keywords used in IETF RFCs to indicate the requirement levels:

- Mandatory - IETF RFC clauses with "MUST, SHALL, MUST NOT, SHALL NOT"
- Optional - IETF RFC clauses with “OPTIONAL, MAY and MAY NOT"
- The IETF RFC clauses with SHOULD and SHOULD NOT are NOT absolutely and truly “optional”, as RFC 2119 defines *“that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course”.* However, as SRv6 is an emerging technology, the test requirements listed below, corresponding to “SHOULD” and “SHOULD NOT” clauses and their adjectives RECOMMENDED/NOT RECOMMENDED are considered “Optional” for this technical report.

Based on the above classification, the Table 2 illustrates the test cases which are identified from RFC 8402, RFC 8754 and RFC 8986 to verify a device’s conformance with SRv6 technology.

Table 2 - Details of Test cases for SRv6 ConformanceS.

No.	Test case	RFC	Clause	Mandatory /Optional	Test Methodology
1	Verify if SRv6 is Enabled	8402	3.1.3	Mandatory	Available
2	Outside Domain Traffic	8402	8.2	Mandatory	Available
3	Leak prevention	8402	8.2	Mandatory	Available
4	Processing SRH with flag 0	8754	2	Mandatory	Available
5	Packet Tagging and Tag Processing	8754	2	Optional	Available
6	Segment Order in the Segment List	8754	2	Mandatory	Available
7	TLV Processing	8754	2.1	Optional	Available
8	Validation of Pad1 TLV	8754	2.1.1.1	Optional	Available
9	Validation of PadN TLV	8754	2.1.1.2	Optional	Available
10	Processing PadN TLV with Zero and Non-Zero Padding	8754	2.1.1.2	Optional	Available
11	HMAC Verification	8754	2.1.2.1	Optional	Available

12	HMAC Digest Truncation	8754	2.1.2.1	Optional	Available
13	HMAC SHA-256 Implementation Verification	8754	2.1.2.2	Optional	Available
14	SR Nodes Behaviour – SourceNode, TransitNode, EndpointNode	8754	4.1, 4.2, 4.3	Mandatory	Available
15	Processing Segments Left Value	8754	4.3.1.1, 4.3.2	Mandatory	Available
16	Decreasing Hop Limit Value	8754	4.3.1.1	Mandatory	Available
		8986	4.1.1		
17	Invalid Packet Handling in Segment Routing	8754	4.3.1.1	Mandatory	
		8986	4.1.1	Available	
18	Processing Upper-Layer Header	8754	4.3.1.2	Mandatory	Available
		8986	4.1.1		
19	Securing the SR Domain	8754	5.1	Mandatory	Available
20	Processing PMTU in SR Domain	8754	5.3	Optional	Available
21	SR Nodes using Flow Label	8754	5.5	Mandatory	Available
22	SID Format	8986	3.1	Mandatory	Available
23	SID Arg Value Unchanged	8986	3.1	Optional	Available
24	SR Endpoint Behavior - End.X (L3 Cross-Connect)	8986	4.2	Optional	Available
25	SR Endpoint Behavior - End.T (Specific IPv6 Table Lookup)	8986	4.3	Optional	Available
26	SR Endpoint Behavior - End.DX6: Decapsulation and IPv6 Cross-Connect	8986	4.4	Optional	Not Available
27	SR Endpoint Behavior - End.DX4: Decapsulation and IPv4 Cross-Connect	8986	4.5	Optional	Not Available
28	SR Endpoint Behavior - End.DT6: Decapsulation and Specific IPv6 Table Lookup	8986	4.6	Optional	Not Available
29	SR Endpoint Behavior - End.DT4: Decapsulation and Specific IPv4 Table Lookup	8986	4.7	Optional	Not Available
30	SR Endpoint Behavior - End.DT46: Decapsulation and Specific IP Table Lookup	8986	4.8	Optional	Not Available
31	SR Endpoint Behavior - End.DX2: Decapsulation and L2 Cross-Connect	8986	4.9	Optional	Not Available
32	SR Endpoint Behavior - End.DX2V: Decapsulation and VLAN L2 Table Lookup	8986	4.10	Optional	Not Available
33	SR Endpoint Behavior - End.DT2U: Decapsulation and Unicast MAC L2 Table Lookup	8986	4.11	Optional	Not Available
34	SR Endpoint Behavior - End.DT2M: Decapsulation and L2 Table Flooding	8986	4.12	Optional	Not Available
35	SR Endpoint Behavior - End.B6.Encaps: Endpoint Bound to an SRv6 Policy with Encapsulation	8986	4.13	Optional	Not Available
36	SR Endpoint Behavior - End.B6.Encaps.Red: End.B6.Encaps with Reduced SRH	8986	4.14	Optional	Not Available
37	SR Endpoint Behavior - End.BM: Endpoint Bound to an SR-MPLS Policy	8986	4.15	Optional	Not Available
38	SR Policy Headend Behavior - H.Encaps: SR Headend with Encapsulation in an SR Policy	8986	5.1	Optional	Not Available
39	SR Policy Headend Behavior - H.Encaps.Red: H.Encaps with Reduced Encapsulation	8986	5.2	Optional	Not Available
40	SR Policy Headend Behavior - H.Encaps.L2: H.Encaps Applied to Received L2 Frames	8986	5.3	Optional	Not Available

41	SR Policy Headend Behavior - H.Encaps.L2.Red: H.Encaps.Red Applied to Received L2 Frames	8986	5.4	Optional	Available
42	Traffic Counters	8986	6	Optional	Available
43	Flow-Based Hash Computation	8986	7	Mandatory	Available

8.3. Test Topologies for Verifying Conformance to SRv6

8.3.1. Common Test Topology – A

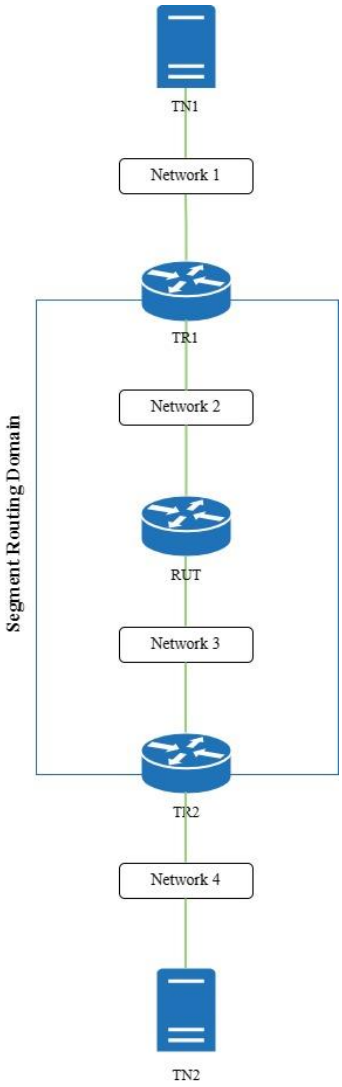

Figure 1 - Common Test Topology-A

Figure 1 shows details of Common Test Topology-A

- TN1 and TN2 are Test Node 1 and Test Node 2. These are IPv6 Hosts. IPv6 Host is a device which is capable of receiving and processing a IPv6 Router Advertisement message from a neighbouring IPv6 Router.
- TR1 and TR2 are Test Router 1 and Test Router 2. These are IPv6 Routers which support SRv6 functionality. IPv6 Router with SRv6 functionality is a device which can send Router Advertisement messages with Segment Routing header.
- RUT is the Router Under Test (RUT). It is an intermediary node within the Segment Routing Domain (SR-domain), and is placed between TR1 and TR2
- Network-1 – The IPv6 network between TR1 and TN1

- Network-2 – The IPv6 network between TR1 and RUT
- Network-3 – The IPv6 network between RUT and TR2
- Network-4 – The IPv6 network between TR2 and TN2

8.3.2. Common Test Topology – B

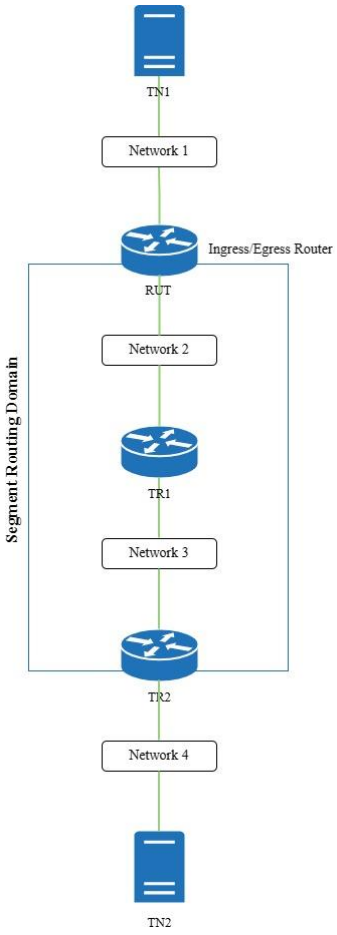

Figure 2 Common Test Topology-B

Figure 2 shows details of Common Test Topology-B

- TN1 and TN2 are Test Node 1 and Test Node 2. These are IPv6 Hosts. IPv6 Host is a device which is capable of receiving and processing a IPv6 Router Advertisement message from a neighbouring IPv6 Router.
- TR1 and TR2 are Test Router 1 and Test Router 2. These are IPv6 Routers which support SRv6 functionality. IPv6 Router with SRv6 functionality is a device which can send Router Advertisement messages with Segment Routing header.
- RUT is the Router Under Test (RUT). It is an Ingress/Egress node at the edge of the Segment Routing Domain (SR-domain), and is placed between TN1 and TR1
- Network-1 – The IPv6 network between RUT and TN1
- Network-2 – The IPv6 network between TR1 and RUT
- Network-3 – The IPv6 network between TR1 and TR2
- Network-4 – The IPv6 network between TR2 and TN2

8.4. SRv6 Conformance Testing – Testing Methodology, Test Procedures and Expected Results

Test SRv6.1.1: SRv6 Enabled

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

Reference:

- RFC 8402 – Section 3.1.3

Test Setup: Test Setup is performed as per Common Topology B.

Procedure: See Table 3

Table 3 - Test Procedure for SRv6 Enabled

Step	Action	Expected Behavior
1.	RUT is not configured for SRv6.	
2.	TN1 transmits an ICMPv6 Echo Request to TN2.	A SRH header must not be appended to the packet.

Possible Problems: None.

Test SRv6.1.2: Outside Domain Traffic

Purpose: Verify that a router properly filters external traffic destined to an address within the domain.

Reference:

- [RFC 8402] - 8.2

Test Setup: Test Setup is performed as per Common Topology B.

Procedure: See Table 4

Table 4 - Test Procedure for Outside Domain Traffic

Step	Action	Expected Behavior
1.	Transmit an ICMPv6 Echo Request from TN1 to TR1 SID address.	The RUT must filter the traffic and not forward the ICMPv6 Echo Request.

Possible Problems: None.

Test SRv6.1.3: Leak prevention

Purpose: Verify that a router does not leak segment routing headers outside of the domain.

Reference:

- [RFC 8402] - 8.2

Test Setup: Test Setup is performed as per Common Topology B.

Procedure: See Table 5

Table 5 - Test Procedure for Leak Prevention

Step	Action	Expected Behavior
1.	TR1 forwards an IPv6 packet with a SRH header to the RUT with an IPv6 address destination of TN1.	The RUT must not forward the SRH to TN1. The RUT must forward the IPv6 packet to TN1 after removing the SRH from the packet.

Possible Problems: None.

Test SRv6.1.4: Processing SRH with flag 0

Purpose: Verify the proper behavior of a router when it encounters a Segment Routing Header (SRH) with a Valid Flag.

Reference:

- [RFC 8754] – Section 2

Test Setup: Test Setup is performed as per Common Topology A.

Packet A

Segment Routing Header
Flag: Zero
Next Header: 58

ICMPv6 Echo Request

Packet B

Segment Routing Header
Flag: Non-Zero
Next Header: 58

ICMPv6 Echo Request

Procedure: See Table 6. Table 7 and Table 8

Table 6 - Test Procedure for Processing SRH with Flag 0 – RUT Sends

Part A: RUT Sends Packet with Flag 0 in SR Header

Step	Action	Expected Behavior
1.	Configure RUT to send an echo request to TR1 with SRH.	The RUT must send an echo request with flag value of 0

Part B: RUT Receives Packet with Flag 0 in SR Header

Table 7 - Test Procedure for Processing SRH with Flag 0 – RUT Receives

Step	Action	Expected Behavior
2.	TR1 transmits Packet A to the RUT. Packet A has an SR Header with a Zero Flag (0x00) and is followed by the ICMPv6 echo request.	The RUT must send an echo reply in response to Packet A.

Part C: RUT Receives Packet with Non-Zero Flag in SR Header

Table 8 - Test Procedure for Processing SRH with Non 0 Flag

Step	Action	Expected Behavior
3.	TR1 transmits Packet B to the RUT. Packet B has an SR Header with a Non-Zero Flag (0x08) and is followed by the ICMPv6 echo request.	The RUT must send an echo reply in response to Packet B.

Possible Problems: None.

Test SRv6.1.5: Packet Tagging and Tag Processing

Purpose: Verify that a router properly sets the tag value and processes the tag field.

Reference:
- [RFC 8754] – Section 2

Test Setup: Test Setup is performed as per Common Topology A.

Procedure: See Table 9 and Table 10

Part A: Tag Not Used at the Source

Table 9 -Test Procedure for Packet Tagging & Tag Processing – Tag Not used at Source

Step	Action	Expected Behavior
1.	TR1 sends a packet, an echo request that contains the tag field to TR2 with a first hop through the RUT.	The "Tag" field in the packet should be zero that is transmitted by RUT.

Part B: Segment Not Requiring Tag Processing

Table 10 - Test Procedure for Processing SRH with Flag 0 – Segment Not Requiring Tag Processing

Step	Action	Expected Behavior
2.	TR1 sends a packet, an echo request to the RUT with an SRH that has the tag field.	The RUT should generate an echo reply without considering the “Tag” field.

Possible Problems: None.

Test SRv6.1.6: Segment Order in the Segment List

Purpose: Verify that the segments in the Segment List of the packet are correctly ordered.

Reference:
- [RFC 8754] – Section 2

Test Setup: Test Setup is performed as per Common Topology B.

SR Policy:

Segment 1: TR1's SID (Action: Forward to Node TR1)
Segment 2: TRX's SID (Action: Forward to Node TRX)
Segment 3: TRY's SID (Action: Forward to Node TRY)

Segment List Order:

Segment List[0]: TRY's SID
Segment List[1]: TRX's SID
Segment List[2]: TR1's SID

Procedure: See Table 11

Table 11 - Test Procedure for Segment Order in Segment List

Step	Action	Expected Behavior
1.	Configure RUT to send a packet to TR2 with a first hop through the TR1 based on the defined SR policy.	Segment List order must correspond with the Segment List order in the transmitted packet as stated above.

Possible Problems: None.

Test SRv6.1.7: TLV Processing

Purpose: Verify that a router properly processes the TLV in the Segment Routing Header.

Reference:
- [RFC 8754] – Section 2.1

Advanced Functionality:
- TLV Processing

Test Setup: Test Setup is performed as per Common Topology A.

Packet A

Segment Routing Header
Hdr Ext Len: 4
TLV 1: Type (1 bytes), Length (1 bytes), Value (6 bytes)
TLV 2: Type (1 bytes), Length (1 bytes), Value (6 bytes)

Packet B

Segment Routing Header
Hdr Ext Len: 3
TLV 1: Type (1 bytes), Length (1 bytes), Value (more than 18 bytes)
TLV 2: Type (1 bytes), Length (1 bytes), Value (more than 10 bytes)

Packet C

Segment Routing Header
Hdr Ext Len: 4
TLV 1: Type (1 byte - unrecognized), Length (1 bytes), Value (6 bytes)
TLV 2: Type (1 bytes), Length (1 bytes), Value (6 bytes)

Procedure: See Table 12, Table 13 and Table 14

Part A: TLV Boundary Check in SRH - Within the Boundary

Table 12 - Test Procedure for TLV Boundary Check in SRH - Within the Boundary

Step	Action	Expected Behavior
1.	TR1 sends a Packet A to RUT with an SRH that contains the TLV within the boundary defined by the Hdr Ext Len field.	The RUT should generate an echo reply.

Part B: TLV Boundary Check in SRH - Exceeds the Boundary

Table 13 - Test Procedure for TLV Boundary Check in SRH - Exceeds the Boundary

Step	Action	Expected Behavior
2.	TR1 sends a Packet B to RUT with an SRH that contains the TLV that exceeds the boundary defined by the Hdr Ext Len field.	The RUT should discard the packet and send an ICMP Parameter Problem error message (Code 0) to the TR1. The pointer field should be offset to the Hdr Ext Len field.

Part C: TLV with Unrecognized type

Table 14 - Test Procedure for TLV with Unrecognized Type

Step	Action	Expected Behavior
3.	TR1 sends a Packet C to RUT with an SRH that contains the TLV with unrecognized type (i.e., 251).	The RUT should simply discard the packet and it should not send any response to it.

Possible Problems: None.

Test SRv6.1.8: Validation of Pad1 TLV

Purpose: Verify that a router correctly processes the packet that has a Segment Routing Header with Pad1 TLV for Single-Byte Padding and Multiple-Byte Padding requirements.

Advanced Functionality:

- TLV Processing

Reference:

- [RFC 8754] – Section 2.1.1.1

Test Setup: Test Setup is performed as per Common Topology A.

Packet A
Segment Routing Header
PadN TLV, 7 bytes

Pad1 TLV, Type: 0
Single-Byte Padding
ICMPv6 Echo Request

Packet B
Segment Routing Header
PadN TLV, 5 bytes
Pad1 TLV, Type: 0
Pad1 TLV, Type: 0
Pad1 TLV, Type: 0
ICMPv6 Echo Request

Procedure: See Table 15 and Table 16

Part A: Validation of Pad1 TLV for Single-Byte Padding

Table 15 - Test Procedure for Validation of Pad1 TLV for Single-Byte Padding

Step	Action	Expected Behavior
1.	TR1 sends a Packet A to RUT, that has a single Pad1 TLV with the type of 0 in the SRH that requires a single byte of padding.	The RUT must process the packet properly.

Part B: Validation of Pad1 TLV for Multiple-Byte Padding

Table 16 - Test Procedure for Validation of Pad1 TLV for Multiple-Byte Padding

Step	Action	Expected Behavior
2.	TR1 sends a Packet B to RUT, which has a single Pad1 TLV with the type of 0 in the SRH that requires multiple bytes of padding.	The RUT must discard the packet and must not send any response to it.

Possible Problems: Part B can be omitted if RUT limits the number of Pad1.

Test SRv6.1.9: Validation of PadN TLV

Purpose: Verify that a router properly processes the packet that has a Segment Routing Header with PadN TLV for Single-Byte Padding and Multiple-Byte Padding requirements.

Reference:
- [RFC 8754] – Section 2.1.1.2

Advanced Functionality:
- TLV Processing

Test Setup: Test Setup is performed as per Common Topology A.

Packet A
Segment Routing Header
TLV 1: (3bytes)
PadN TLV, 5 bytes
ICMPv6 Echo Request

Procedure: See Table 17

Table 17 - Test Procedure for Validation of PadN TLV

Step	Action	Expected Behavior
1.	TR1 sends a Packet A to RUT, that has PadN TLV with the type of 4 in the SRH that requires multiple bytes of padding.	The RUT must process the packet properly

Possible Problems: None.

Test SRv6.1.10: Processing PadN TLV with Zero and Non-Zero Padding

Purpose: Verify that a router properly processes the packet that has a Segment Routing Header with PadN TLV with Zero and Non-Zero Padding.

Reference:
- [RFC 8754] – Section 2.1.1.2

Advanced Functionality:
- TLV Processing

Test Setup: Test Setup is performed as per Common Topology A.

Packet A
Segment Routing Header
PadN TLV, Type: 4,
Padding 0
Multiple-Byte Padding
ICMPv6 Echo Request

Packet B
Segment Routing Header
PadN TLV, Type: 4,
Padding 2
Multiple-Byte Padding
ICMPv6 Echo Request

Procedure: See Table 18 and Table 19

Part A: Processing PadN TLV with Zero Padding

Table 18 - Test Procedure for Processing PadN TLV with Zero Padding

Step	Action	Expected Behavior
1.	TR1 sends a Packet A to RUT, that has PadN TLV with the type of 4 and the padding field set to 0 that requires variable length padding.	The RUT must process the packet properly

Part B: Processing PadN TLV with Non-Zero Padding

Table 19 - Test Procedure for Processing PadN TLV with Non-Zero Padding

Step	Action	Expected Behavior
2.	TR1 sends a Packet B to RUT, that has PadN TLV with the type of 4 and the padding field set to non-zero that requires variable length padding.	The RUT must discard the packet and must not send any response to it.

Possible Problems: None.

Test SRv6.1.11: HMAC Verification

Purpose: Verify that a Router properly performs HMAC generation and verification process for received packets at SR Segment endpoint nodes.

Reference:
- [RFC 8754] – Section 2.1.2.1

Advanced Functionality:
- TLV Processing

Test Setup: Test Setup is performed as per Common Topology A.

Packet A
Segment Routing Header
HMAC TLV, Type: 5,
Current Segment = Destination address (i.e, RUT's SID)
Correct HMAC key ID
ICMPv6 Echo Request

Packet B
Segment Routing Header
HMAC TLV, Type: 5,
Current Segment = Destination address (i.e, RUT's SID)
Incorrect HMAC key ID
ICMPv6 Echo Request

Procedure: See Table 20 and Table 21

Part A: HMAC Verification Success

Table 20 - Test Procedure for HMAC Verification Success

Step	Action	Expected Behavior
1.	Configure the RUT as SR Segment endpoint node with a valid HMAC Key ID and algorithm.	
2..	TR1 sends Packet A with a correct HMAC to the RUT.	The RUT should successfully validate the HMAC using the specified key and algorithm and should send an echo reply to TR1.

Part B: HMAC Verification Failure

Table 21 - Test Procedure for HMAC Verification Failure

Step	Action	Expected Behavior
3.	Configure the RUT as SR Segment endpoint node with a valid HMAC Key ID and algorithm.	
4.	TR1 sends Packet B with an incorrect HMAC to the RUT.	The RUT should discard the packet and should send an ICMP error message with the code field of 0, pointing to the HMAC TLV in the packet

Possible Problems: None.

Test SRv6.1.12: HMAC Digest Truncation

Purpose: To validate that a router correctly truncates the HMAC digest to 32 octets when the HMAC algorithm produces a digest less than 32 octets.

Reference:
- [RFC 8754] – Section 2.1.2.1

Advanced Functionality:
- TLV Processing

Test Setup: Test Setup is performed as per Common Topology A.

Packet A
Segment Routing Header
HMAC TLV, Type: 5,
HMAC Key ID: 12345,
HMAC Algorithm: SHA-384,
Current Segment = Destination address (i.e., RUT's SID)
Correct HMAC key ID
ICMPv6 Echo Request

Packet B
Segment Routing Header
HMAC TLV, Type: 5,
HMAC Key ID: 12345,
HMAC Algorithm: SHA-224,
Current Segment = Destination address (i.e., RUT's SID)
Correct HMAC key ID
ICMPv6 Echo Request

Procedure: See Table 22 and Table 23

Part A: Digest More than 32 Octets

Table 22 - Test Procedure for HMAC Digest Truncation – More than 32 Octets

Step	Action	Expected Behavior
1.	Configure the RUT as SR Segment endpoint node with a valid HMAC Key ID and algorithm that is known to produce a digest more than 32 octets.	
2.	TR1 sends Packet A to RUT for HMAC verification that has HMAC digest based on the HMAC algorithm and pre-shared key.	The RUT should successfully validate the HMAC using the specified key and algorithm and should send an echo reply to TR1.

Part B: Digest Less than 32 Octets

Table 23 - Test Procedure for HMAC Digest Truncation – Less than 32 Octets

Step	Action	Expected Behavior
1.	Configure the RUT as SR Segment endpoint node with a valid HMAC Key ID and algorithm that is known to produce a digest less than 32 octets.	
2.	TR1 sends Packet B to RUT for HMAC verification that has HMAC digest based on the HMAC algorithm and pre-shared key.	The RUT should successfully validate the HMAC using the specified key and algorithm and should send an echo reply to TR1.

Possible Problems: Part A and Part B can be omitted if RUT do not support the HMAC Algorithm.

Test SRv6.1.13: SR Nodes Behavior

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

Reference:

- [RFC 8754] – Section 3, Section 4.1, 4.2, 4.3

Test Setup: Test Setup is performed as per Common Topology B for Parts A, C and Common Topology A is used for Part B.

Packet A
IPv6 Header
Next Header: 58
Source Address: TN1's Global Address
Destination Address: TR1's Global Address
ICMPv6 Echo Request

Packet B
IPv6 Header
Source Address: TR1's Global Address
Destination Address: TR2's Global Address
Segment Routing Header
Next Header: 58
Segment ID
ICMPv6 Echo Request

Packet C
IPv6 Header
Source Address: TR2's Global Address
Destination Address: RUT's Global Address
Segment Routing Header
Next Header: 58
Segment ID
ICMPv6 Echo Request

Procedure: See Table 24, Table 25 and Table 26

Part A: Source Node

Table 24 - Test Procedure for SR Nodes Behaviour – Source Node

Step	Action	Expected Behavior
1.	Configure the RUT as an SR domain Ingress router.	
2.	TN1 sends Packet A, an echo request to TR1's Global address with a first hop through the RUT.	RUT should configure the SID with SRH within the packet and must transmit the packet to TR1's Global Address.

Part B: Transit Node

Table 25 Test Procedure for SR Nodes Behaviour – Transit Node

Step	Action	Expected Behavior
3.	Configure the RUT as a transit node.	
4.	TR1 transmits Packet B, an Echo Request with a segment in SRH to TR2's Global address with a first hop through the RUT.	The RUT must forward the Echo Request from TR1 to TR2 without processing the SRH.

Part C: Segment Endpoint Node

Table 26 - Test Procedure for SR Nodes Behaviour – Endpoint Node

Step	Action	Expected Behavior
5.	Configure the RUT as a segment endpoint node.	
6.	TR2 sends Packet C, an echo request to RUT's Global address with a first hop through the TR1	The RUT must generate an echo reply in response to Packet C

Possible Problems: None.

Test SRv6.1.14: Processing Segments Left Value

Purpose: Verify that a router properly processes a packet that contains a Segment Routing header with a Segments Left value.

Reference:

- [RFC 8754] – Section 4.3.1.1, 4.3.2

Test Setup: Test Setup is performed as per Common Topology A .

Packet A
IPv6 Header
Source Address: TR1's Global Address
Destination Address: RUT's SID
Segment Routing Header
Next Header: 58
Segments Left: 0
ICMPv6 Echo Request

Packet B
IPv6 Header
Source Address: TR1's Global Address
Destination Address: RUT's SID
Segment Routing Header
Next Header: 58
Segments Left: 1
ICMPv6 Echo Request

Packet C
IPv6 Header
Source Address: TR1's Global Address
Destination Address: TR2's Global Address
Segment Routing Header
Next Header: 58
Segments Left: 1
ICMPv6 Echo Request

Procedure: See Table 27, Table 28 and Table 29

Part A: Segments Left Zero - End Node

Table 27 - Test Procedure for Segments Left Zero - End Node

Step	Action	Expected Behavior
1.	TR1 sends Packet A, an Echo Request to the RUT that has SRH with a Segments Left value of 0.	RUT should respond to the Request by sending an Echo Reply

Part B: Segments Left Non-zero - End Node

Table 28 - Test Procedure for Segments Left Non-Zero - End Node

Step	Action	Expected Behavior
2.	TR1 sends Packet B, an Echo Request to the RUT that has SRH with a Segments Left value of 1.	The RUT must discard the Echo Request and send an ICMP Parameter Problem, Code 0, message to TR1's Global Address. The pointer field must be 0x2B (offset of the Routing Type field of the SRH).

Part C: Segments Left Non-zero - Intermediate Node

Table 29 - Test Procedure for Segments Left Zero - Intermediate Node

Step	Action	Expected Behavior
3.	TR1 sends Packet C, an Echo Request to TR2 with a first hop through the RUT. The Segments Left field is set to 1.	RUT should decrease the Segments Left field to 0 and forward the packet to TR2.

Possible Problems: None.

Test SRv6.1.15: Decreasing Hop Limit Value

Purpose: Verify that a router properly processes the Hop limit value and generates a valid value in transmitted packets.

Reference:
- [RFC 8754] – Section 4.3.1.1
- [RFC 8986] - Sections 4.1 and 4.1.1

Test Setup: Test Setup is performed as per Common Topology A.

Packet A
IPv6 Header
Source Address: TR1's Global Address
Destination Address: TR2's Global Address
Hop Limit: 64
Segment Routing Header
Next Header: 58
Segments Left: 1
ICMPv6 Echo Request

Procedure: See Table 30.

Table 30 - Test Procedure for Decreasing Hop Limit Value

Step	Action	Expected Behavior
1.	TR1 transmits Packet A to TR2's Global Address with a first hop through the RUT. The Hop Limit field is set to 64	The RUT should process the segment left value and forward Packet A to TR2. The Hop Limit field should be decreased to 63

Possible Problems: None.

Test SRv6.1.16: Invalid Packet Handling in Segment Routing

Purpose: Verify that a router generates the appropriate response to an invalid packet in segment routing.

Reference:
- [RFC 8754] – Section 4.3.1.1
- [RFC 8986] - Sections 4.1 and 4.1.1

Test Setup: Test Setup is performed as per Common Topology A.

Packet A

IPv6 Header
Source Address: TR1's Global Address
Destination Address: TR2's Global Address
Segment Routing Header
Next Header: 58
Hdr Ext Len: 6
Segments Left: 2
Last Entry: 3
ICMPv6 Echo Request

Packet B

IPv6 Header
Source Address: TR1's Global Address
Destination Address: TR2's Global Address
Segment Routing Header
Next Header: 58
Hdr Ext Len: 6
Segments Left: 3
Last Entry: 2
ICMPv6 Echo Request

Packet C

IPv6 Header
Source Address: TR1's Global Address
Destination Address: TR2's Global Address
Hop Limit: 0
Segment Routing Header
Next Header: 58
Hdr Ext Len: 6
Segments Left: 1
Last Entry: 1
ICMPv6 Echo Request

Packet D

IPv6 Header
Source Address: TR1's Global Address
Destination Address: TR2's Global Address
Hop Limit: 1
Segment Routing Header
Next Header: 58
Hdr Ext Len: 6
Segments Left: 1
Last Entry: 1
ICMPv6 Echo Request

Procedure: See Table 31, Table 32, Table 33 and Table 34

Part A: Invalid Last Entry

Table 31 - Test Procedure for Invalid last entry

Step	Action	Expected Behavior
1.	TR1 transmits a Packet A, an echo request to the TR2 with a first hop through the RUT. The Last entry field is set to be invalid.	The RUT must discard the Echo Request and send an ICMP Parameter Problem, Code 0, message to TR1's Global Address. The pointer field must be 0x2B (offset of the Routing Type field of the SRH).

Part B: Invalid Segments Left

Table 32 - Test Procedure for Invalid Segments left

Step	Action	Expected Behavior
2.	TR1 transmits a Packet B, an echo request to the TR2 with a first hop through the RUT. The Segments Left field is set to be invalid	The RUT must discard the Echo Request and send an ICMP Parameter Problem, Code 0, message to TR1's Global Address. The pointer field must be 0x2B (offset of the Routing Type field of the SRH).

Part C: Hop Limit == 0

Table 33 - Test Procedure for Hop Limit 0

Step	Action	Expected Behavior

3.	TR1 transmits a Packet C, an Echo Request to TR2 with a first hop of the RUT.	The RUT must discard the ICMPv6 Echo Request from TR1 and must not forward the packet to TR2. The RUT should send a Time Exceeded Message to TR1 with a code field value of 0 (Hop Limit Exceeded in transit) • The Source Address of the Packet should be one of the RUT's unicast addresses used for packet forwarding. • The Destination Address should be the same as TR1's Source Address. • The invoking Echo Request packet included in the Error Message must not exceed minimum IPv6 MTU.

Part D: Hop Limit == 1

Table34 -Test Procedure for Hop Limit 1

Step	Action	Expected Behavior
4.	TR1 transmits a Packet D, an Echo Request to TR2 with a first hop of the RUT.	The RUT must discard the ICMPv6 Echo Request from TR1 and must not forward the packet to TR2. The RUT should send a Time Exceeded Message to TR1 with a code field value of 0 (Hop Limit Exceeded in transit) • The Source Address of the Packet should be one of the RUT's unicast addresses used for packet forwarding. • The Destination Address should be the same as TR1's Source Address. • The invoking Echo Request packet included in the Error Message must not exceed minimum IPv6 MTU.

Possible Problems: None.

Test SRv6.1.17: Processing Upper-Layer Header

Purpose: Verify that a router properly processes the upper-layer header of an SRH packet.

Reference:
- [RFC 8754] – Section 4.3.1.2
- [RFC 8986] - Sections 4.1 and 4.1.1

Test Setup: Test Setup is performed as per Common Topology A.

Procedure: See Table 35 and Table 36

Part A: Upper-Layer Header needs to be processed

Table 35 - Test Procedure for Upper Layer Header Processing

Step	Action	Expected Behavior
1.	TR1 transmits an ICMPv6 Echo Request with an SRH to the RUT.	The RUT must generate an echo reply in response to Packet A.

Part B: Upper-Layer Header needs to be discarded

Table 36 - Test Procedure for Upper Layer Header Discarding

Step	Action	Expected Behavior
2.	TR1 transmits a UDP echo request to the RUT, which contains an SRH.	The RUT must not transmit an Echo Reply to TR1. The RUT should transmit an ICMPv6 Parameter Problem message to TR1. The Code field should be 4 (SR Upper-layer header error). The Pointer field should be offset of the SR upper-layer header.

Possible Problems: If UDP Traceroute is enabled, Part B can be omitted

Test SRv6.1.18: Securing the SR Domain

Purpose: Verify that a router properly processes the packet from outside of the SR domain.

Reference:
- [RFC 8754] – Section 5.1

Test Setup: Test Setup is performed as per Common Topology B.

Packet A
IPv6 Header
Source Address: TN1's Global Address
Destination Address: TR1's Global Address
Next Header: 58
ICMPv6 Echo Request

Packet B
IPv6 Header
Source Address: TN1's Global Address
Destination Address: TR1's Global Address
Segment Routing Header
Next Header: 58
Segment ID
ICMPv6 Echo Request

Procedure: See Table 37 and Table 38

Part A: Forwarding Interdomain Packet without SID

Table 37 Test Procedure for Securing SR domain – without SID

Step	Action	Expected Behavior
1.	Configure the RUT as an SR domain Ingress router.	
2.	TN1 transmits Packet A, an Echo Request to TR1's Global Address with a first hop through the RUT.	The RUT must add the SRH with TR1's SID and forward the echo request to TR1.

Part B: Forwarding Interdomain Packet with SID

Table 38 - Test Procedure for Securing SR domain – with SID

Step	Action	Expected Behavior
3.	Configure the RUT as an SR domain Ingress router.	
4.	TN1 transmits Packet B to TR1's Global Address with a first hop through the RUT, an Echo Request that has the SR Header with a Segment ID.	The RUT must discard the packet and not forward the echo request to TR1.

Possible Problems: None.

Test SRv6.1.19: Processing PMTU in SR Domain

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:
- [RFC 8754] – Section 5.3

Test Setup: Test Setup is performed as per Common Topology A for Part A. The Common Topology B is used for Part B.

Procedure: See Table 39 and Table 40

Part A: RUT Receives Packet Too Big Message

Table 39 - Test Procedure for PMTU – RUT Receives Packet Too Big

Step	Action	Expected Behavior
1.	Configure TR1 to have an MTU of 1400 on Network 1.	
1.	TR1 forwards an Echo Request from TN1 to the RUT with a packet size equal to 1500 octets.	The RUT should transmit an Echo Reply to TN1.
2.	TR1 transmits a Packet Too Big message to the RUT, which contains an MTU field with a value of 1400.	
3.	TR1 forwards an Echo Request from TN1 to the RUT with a packet size equal to 1500 octets.	The RUT should correctly fragment its response to the Echo Request using TR1 as a first hop, indicating the RUT processed the Packet Too Big message. The fragmented packets must not be larger than 1400 octets in size
4.	TR1 transmits a Packet Too Big message to the RUT, which contains an MTU field with a value of 1280	
5.	TR1 forwards an Echo Request from TN1 to the RUT with a packet size equal to 1500 octets.	The RUT should correctly fragment its response to the Echo Request using TR1 as a first hop, indicating the RUT processed the Packet Too Big message. The fragmented packets must not be larger than 1280 octets in size.

Part B: RUT Transmits Packet Too Big Message

Table 40 - Test Procedure for PMTU – RUT Transmits Packet Too Big

Step	Action	Expected Behavior
6.	Configure the RUT as an SR domain Ingress Node.	
7.	Configure the RUT Network1 interface with a path MTU of 1280 bytes on the RUT.	
8.	TN1 sends an Echo Request to TR1 with a packet size equal to 1500 octets.	RUT should transmit a Packet Too Big message to the TN1, which contains an MTU field with a value of 1280.
9.	TN1 sends fragmented echo requests after processing the Packet Too Big message from the RUT.	RUT should forward the fragmented Echo Requests to TR1.

Possible Problems: None.

Test SRv6.1.20: SR Nodes using Flow Label

Purpose: Verify that a router properly processes and generates the Flow Label.

Reference:
- [RFC 8754] – Section 5.3

Test Setup: Test Setup is performed as per Common Topology B for Parts A and B. The Common Topology A is used for Parts C and D.

Packet A
IPv6 Header
Source Address: TN1's Global Address
Destination Address: TR1's Global Address
Flow Label: 214375
Next Header: 58
ICMPv6 Echo Request

Packet B
IPv6 Header
Source Address: TR1's Global Address
Destination Address: TR2's Global Address
Flow Label: 214375
Next Header: 58
ICMPv6 Echo Request

Packet C
IPv6 Header
Source Address: TR1's Global Address
Destination Address: RUT's SID
Flow Label: 214375
Next Header: 58
ICMPv6 Echo Request

Procedure: See Table 41, Table 42, Table 43and Table 44

Part A: Imposing Flow Label for Interdomain Packet

Table 41 - Test Procedure for Imposing Flow Label for Interdomain Packet

Step	Action	Expected Behavior
1.	Configure RUT as an SR Domain Ingress Router.	
2.	TN1 sends Packet A, an Echo Request to TR1 with a first hop through RUT.	The RUT must impose a flow label computed based on the packet and forward the packet to TR1.

Part B: Imposing Flow Label for Intradomain Packet

Table 42 - Test Procedure for Imposing Flow Label for Intradomain Packet

Step	Action	Expected Behavior
3.	Configure RUT to send an Echo Request to TR1 with a Flow Label.	The RUT should generate a flow label in the transmitted packet. The flow label field must be non-zero.

Part C: Forwarding a packet with Flow Label

Table 43 Test Procedure for Forwarding a packet with Flow Label

Step	Action	Expected Behavior
4.	Configure the RUT as a Transit Node.	
5.	TR1 sends Packet B, an Echo Request to TR2 with a first hop through RUT.	The RUT must forward the Echo Request from TR1 to TR2. The Flow Label field must be unchanged in the forwarded packet.

Part D: Receiving a packet with Flow Label

Table 44 Test Procedure for Receiving a packet with Flow Label

Step	Action	Expected Behavior
6.	TR1 sends Packet C, an Echo Request to RUT.	The RUT must generate an Echo Reply. The Flow Label field in the packet must be non-zero.

Possible Problems: Part A, B and D may be omitted if the device under test does not support the process of the Flow Label.

Test SRv6.1.21: SID Format

Purpose: Verify that a router properly formats the SID.

Reference:

- [RFC 8986] - Section 3.1

Test Setup: Test Setup is performed as per Common Topology B.

Packet A
IPv6 Header
Source Address: TN1's Global Address
Destination Address: TR1's Global Address
ICMPv6 Echo Request

Procedure: See Table 45

Table 45 - Test Procedure for SID Format

Step	Action	Expected Behavior
1.	TN1 sends Packet A an ICMPv6 Echo Request to TR1's Global address with a first hop through the RUT.	The RUT should configure the SID with an SR Header within the packet and must transmit the packet to TR1's Global Address. The remaining bits of the SID must be zero.

Possible Problems: None.

Test SRv6.1.22: SID Arg Value Unchanged

Purpose: Verify that a router properly leaves the Arg value unchanged when of a routed SID.

Reference:

- [RFC 8986] - Section 3.1

Test Setup: Test Setup is performed as per Common Topology A.

Packet A
IPv6 Header
Source Address: TR1's Global Address
Destination Address: TR2's Global Address
Segment Routing Header
Next Header: 58
Segment ID LOC: TR2
Segment ID FUNCT: 0
Segment ID ARG: 0
ICMPv6 Echo Request

Procedure: See Table 46

Table 46 -Test Procedure for SID Arg Value Unchanged

Step	Action	Expected Behavior

1.	TR1 sends Packet A an ICMPv6 echo request with an SID and an SR Header that includes an ARG value to TR2's Global address with a first hop through the RUT.	The RUT should forward the echo request. The ARG value should remain unchanged.

Possible Problems: None.

Test SRv6.1.23: SR Endpoint Behavior - End.X (L3 Cross-Connect)

Purpose: Verify that a router properly displays Endpoint with L3 Cross-Connect behavior. The codepoint for the SID is bound to behavior 0x0005.

Reference:
- [RFC 8986] - Section 4.2

Test Setup: Test Setup is performed as per Common Topology A.

Packet A
IPv6 Header
Source Address: TR1's Global Address
Destination Address: TR2's Global Address
Segment Routing Header
Next Header: 58
Segments Left: 2
Last Entry: 2
Segment ID LOC: DUT
Segment ID FUNCT: 0x0005
Segment ID ARG: 0
ICMPv6 Echo Request

Procedure: See Table 47

Table 47 - Test Procedure for SR Endpoint Behavior - End.X (L3 Cross-Connect)

Step	Action	Expected Behavior
1.	TR1 sends Packet A an ICMPv6 echo request with a SID with an SR Header to the TR2's Global address with the first hop through RUT . The SIDs list indicates <RUT, TR2>.	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 TR2

Possible Problems: None.

Test SRv6.1.24: SR Endpoint Behavior - End.T (Specific IPv6 Table Lookup)

Purpose: Verify that a router properly displays Endpoint with specific IPv6 table lookup behavior. The codepoint for the SID is bound to behavior 0x0009.

Advanced Functionality:
- End.T

Reference:

- [RFC 8986] - Section 4.3

Test Setup: Test Setup is performed as per Common Topology A.

Packet A
IPv6 Header
Source Address: TR1's Global Address
Destination Address: TR2's Global Address
Segment Routing Header
Next Header: 58
Segments Left: 2
Last Entry: 2
Segment ID LOC: RUT
Segment ID FUNCT: 0x0009
Segment ID ARG: 0
ICMPv6 Echo Request

Procedure: See Table 48

Table 48 - Test Procedure for SR Endpoint Behavior - End.T (Specific IPv6 Table Lookup)

Step	Action	Expected Behavior
1.	TR1 sends Packet A an ICMPv6 echo request with a SID with an SR Header to TR2's Global address with the first hop through RUT. The SIDs list indicates <RUT, TR2>.	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.

Test SRv6.1.25: SR Policy Headend Behavior - H.Encaps.L2.Red: H.Encaps.Red Applied to Received L2 Frames

Purpose: Verify that the DUT acting as an SR Policy Headend, correctly performs H.Encaps.L2.Red when receiving L2 frames.

Reference:

- [RFC 8986] - Section 5.4

Test Setup: Test Setup is performed as per Common Topology A.

Packet A
Ethernet Frame
Source MAC Address: TR1's MAC Address
Destination MAC Address: RUT's MAC Address
Payload: IPv4/IPv6 packet

Procedure: See Table 49

Table 49 - Test Procedure for H.Encaps.Red Applied to Received L2 Frames

Step	Action	Expected Behavior

1.	Configure DUT with multi SID SR Policy with SID List = <SID1, SID2>	
2.	TR1 sends Packet A to DUT.	DUT identifies SR Policy bound to this ingress and forward the encapsulated packet to TR2 by adding IPv6 header with DA = SID1 & SRH contains only SID2
3.	Configure DUT with single SID SR Policy with SID List = <SID1>	
4.	TR1 sends Packet A again to the DUT.	DUT identifies SR Policy bound to this ingress and forward the encapsulated packet to TR2 by adding only the IPv6 header with DA = SID1 & no SRH.

Possible Problems: None.

Test SRv6.1.26: Traffic Counters

Purpose: Verify that the DUT maintains per-SID packet and byte counters

Reference:
- [RFC 8986] - Section 6

Test Setup: Test Setup is performed as per Common Topology A.

Packet A
IPv6 Header
Source Address: TR1's Global Address
Destination Address: SID-X (Local SID on DUT)
Segment Routing Header
Next Header: 58
Segments Left: 1
Segment List: <SID-X, Next-SID>
ICMPv6 Echo Request

Procedure: Table 50
Table 50 - Test Procedure for Traffic Counters

Step	Action	Expected Behavior
1.	Retrieve the current packet and byte counters for SID-X on the DUT.	DUT should maintain and display the initial packet and byte counter values
2.	TR1 sends 5 valid SRv6 packets (Packet A) to the DUT, all targeting SID-X.	DUT processes all packets successfully according to the configured SID behavior. No packets should be dropped.
3.	Retrieve the SID-X counters again from the DUT.	Packet counter MUST increase by 5. Byte counter MUST increase by the sum of bytes in the 5 packets.
4.	TR1 sends malformed or invalid SRv6 packets (e.g., incorrect SRH, bad Segments Left).	DUT MUST drop these packets or generate ICMP errors

5.	Retrieve the SID-X counters again from the DUT.	SID counters MUST remain identical to the values recorded in Step 3.

Possible Problems: None.

Test SRv6.1.27: Flow-Based Hash Computation

Purpose: Verify that the DUT includes the IPv6 Source Address, IPv6 Destination Address, and IPv6 Flow Label of the outer IPv6 header when performing flow-based hashing

Reference:
- [RFC 8986] - Section 7

Test Setup: Test Setup is performed as per Common Topology A.

Procedure: See Table 51

Table 51 - Test Procedure for Flow-Based Hash Computation

Step	Action	Expected Behavior
1.	Configure two ECMP paths on the DUT toward the same destination.	
2.	Send two IPv6 test traffic from DUT with same SA, DA, but different Flow Label values & Capture the outgoing interface/path selection for each flow.	Traffic with different Flow Labels MUST be forwarded on different ECMP paths, proving the Flow Label is included in hashing.
3.	Change only the Source Address, keeping DA and Flow Label constant; send the two IPv6 traffic again.	Changing only SA MUST change the selected ECMP path.
4.	Change only the Destination Address, keeping SA and Flow Label constant; send the two IPv6 traffic again.	Changing only DA MUST change the selected ECMP path.

Possible Problems: None.

9. Relationship with other related standard groups for SRv6

The IETF is the primary body responsible for establishing the standards for SRv6, including its architecture, implementation, deployment, and Operations, Administration, and Maintenance (OAM). The work presented in this Technical Report only complements the IETF's efforts by identifying the testing cases derived from IETF standards for SRv6. It is important to emphasize that this technical report does not seek to specify any aspects of SRv6 nor introduce any new requirements for SRv6, outside of IETF's work.

10. Conclusion

This Technical Report delivers a structured methodology for verifying a router's conformance to SRv6 by identifying the core SRv6 standards (RFC 8402, RFC 8754, and RFC 8986) and extracting their technical testing cases. These cases were translated into comprehensive test procedures, associated expected behaviours, and objective compliance criteria. The resulting framework provides manufacturers, operators, and testing bodies with a consistent and reproducible approach for assessing SRv6 implementations, thereby supporting interoperability, reliability, and alignment with international standards.

Bibliography

[b- ITU-T Q.4070] ITU-T Q.4070 (2023), *Test suite for interoperability testing of virtualized broadband network gateways*

[b- ITU-T Q.4141] ITU-T Q.4141 (2023), *Requirements and signalling of intelligence control for the border network gateway in computing power networks*

[b- ITU-T Y.3216] ITU-T Y.3216 (2024), *Fixed, mobile and satellite convergence – Distributed core network for IMT-2020 networks and beyond*

[b- ITU-T Y.3657] ITU-T Y.3657 (2023), *Big data driven networking – Requirements and capabilities of network visibility*

_____