

# TECHNICAL CODE

## INTERNET PROTOCOL VERSION 6 - DEPLOYMENT SPECIFICATIONS FOR SEGMENT ROUTING OVER INTERNET PROTOCOL VERSION 6

Developed by



Registered by



Registered date: 27 February 2025

## **MCMC MTSFB TC G053:2025**

### **Development of technical codes**

The Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) ('the Act') provides for a Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirements for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

#### **Malaysian Communications and Multimedia Commission (MCMC)**

MCMC Tower 1  
Jalan Impact  
Cyber 6  
63000 Cyberjaya  
Selangor Darul Ehsan  
MALAYSIA

Tel : +60 3 8688 8000  
Fax : +60 3 8688 1000  
Email : [stpd@mcmc.gov.my](mailto:stpd@mcmc.gov.my)  
Website: [www.mcmc.gov.my](http://www.mcmc.gov.my)

OR

#### **Malaysian Technical Standards Forum Bhd (MTSFB)**

Level 3A, MCMC Tower 2  
Jalan Impact  
Cyber 6  
63000 Cyberjaya  
Selangor Darul Ehsan  
MALAYSIA

Tel : +60 3 8680 9950  
Fax : +60 3 8680 9940  
Email : [support@mtsfb.org.my](mailto:support@mtsfb.org.my)  
Website: [www.mtsfb.org.my](http://www.mtsfb.org.my)

## Contents

	Page
Committee representation.....	ii
Foreword .....	iii
0. Introduction.....	1
1. Scope .....	1
2. Normative references .....	1
3. Abbreviation.....	2
4. Terms and definitions .....	3
5. Segment Routing over IPv6 (SRv6).....	5
5.1 Key components of SRv6 architecture.....	6
5.2 Benefits of SRv6 .....	7
5.3 Functionalities and features of SRv6 .....	9
6. SRv6 deployment requirements .....	9
6.1 Deployment phases .....	9
6.2 Best practices for SRv6 deployment.....	12
7. SRv6 security consideration.....	12
7.1 Security vulnerabilities .....	13
7.2 Mitigation strategies .....	13
8. Technical advantages of SRv6.....	14
8.1 Service function chaining .....	14
8.2 Network slicing .....	14
8.3 Load balancing.....	14
8.4 Virtual Private Networks (VPN).....	14
8.5 Advanced routing scenarios.....	14
Annex A Requirements of network components to support SRv6 .....	15
Annex B Essential Request for Comment (RFC)s for SRv6 implementation .....	17
Annex C SRv6 proposed test cases and scenarios.....	18

## **MCMC MTSFB TC G053:2025**

### **Committee representation**

This technical code was developed by the Numbering and Electronic Addressing Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB), which consists of representatives from the following organisations:

American Malaysian Chamber of Commerce

CelcomDigi Berhad

Digital Nasional Berhad

Huawei Technologies (Malaysia) Sdn Bhd

Maxis Broadband Sdn Bhd

Multimedia University

Persatuan IPv6 Malaysia

TM Technology Services Sdn Bhd

TT DOTCOM Sdn Bhd

## **Foreword**

This Technical Code for the Internet Protocol version 6 - Deployment Specifications for Segment Routing over Internet Protocol version 6 ('this Technical Code') was developed pursuant to Section 185 of the Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) by the Malaysian Technical Standards Forum Bhd (MTSFB) under the Numbering and Electronic Addressing Facilities Working Group.

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

(THIS PAGE IS INTENTIONALLY LEFT BLANK)

## INTERNET PROTOCOL VERSION 6 - DEPLOYMENT SPECIFICATIONS FOR SEGMENT ROUTING OVER INTERNET PROTOCOL VERSION 6

### 0. Introduction

Segment Routing over IPv6 (SRv6) simplifies network routing by allowing the data source to determine the entire path a packet will follow, rather than relying on each router along the way to make independent decisions. This is achieved by attaching a series of instructions, or segments, directly to the data packet.

SRv6 provides key advantages over Segment Routing - Multiprotocol Label Switching (SR-MPLS) and other routing methods. By utilising Internet Protocol version 6 (IPv6) addresses for segments, SRv6 enhances flexibility and scalability, making it suitable for managing the growing number of connected devices and data traffic driven by technologies such as 5G, Internet of Things (IoT), and cloud computing. SRv6 also integrates seamlessly with existing IPv6 networks, from the edge to the data centre, improving overall network efficiency. As networks evolve, SRv6 is positioned as a critical technology for supporting future network demands.

The adoption of SRv6 can help Malaysian organisations optimise their network management, enhance performance, support emerging technologies like 5G and IoT, improve security, and reduce operational costs. This positions them for digital transformation and strengthens their global competitiveness.

The widespread adoption of SRv6 across diverse networks introduces several challenges. Without standardised guidelines and best practices, deployment inconsistencies may arise, resulting in interoperability issues between equipment from different vendors. This can impede the seamless integration of SRv6 into existing networks and prevent its full potential from being realised. Additionally, the absence of standardised security measures and traffic management practices can leave organisations vulnerable to inefficiencies and security risks. To overcome these challenges and ensure the successful and secure deployment of SRv6, this Technical Code establishes clear guidelines and best practices.

This Technical Code serves as a comprehensive reference for network architects, planners, implementers, administrators, and security professionals. It is designed to support the following types of networks:

- a) greenfield deployments of SRv6;
- b) networks already using SR-MPLS but considering a transition to SRv6; and
- c) networks already running SRv6 but looking for further enhancements.

### 1. Scope

This Technical Code provides requirements for deploying and operating SRv6 in Malaysia. It describes the SRv6 technology, use cases, security recommendations, and standards for deployment. SRv6 offers several technical benefits to organisations in Malaysia, particularly those involved in networking, telecommunications, and digital transformation initiatives.

### 2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

## **MCMC MTSFB TC G053:2025**

MCMC MTSFB TC G046, *Internet Protocol version 6 - Security Requirements*  
RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*

RFC 8402, *Segment Routing Architecture*

RFC 8754, *IPv6 Segment Routing Header (SRH)*

RFC 8986, *Segment Routing over IPv6 (SRv6) Network Programming*

RFC 9252, *BGP Overlay Services Based on Segment Routing over IPv6 (SRv6)*

RFC 9259, *Segment Routing over IPv6 (SRv6) Operations, Administration, and Maintenance (OAM)*

RFC 9352, *IS-IS Extensions to Support Segment Routing over IPv6 (SRv6)*

RFC 9433, *Segment Routing over IPv6 (SRv6) for Mobile User Plane*

RFC 9487, *IP Flow Information Export (IPFIX) Information Elements for Segment Routing over IPv6*

RFC 9513, *OSPF Extensions for Segment Routing over IPv6 (SRv6)*

### **3. Abbreviation**

For the purpose of this Technical Code, the following abbreviations apply.

AS	Autonomous System
AI	Artificial Intelligence
BGP	Border Gateway Protocol
BGP-LS	Border Gateway Protocol Link-State
C-SID	Compressed Segment Identifier
DA	Destination Address
DMZ	De-Militarised Zone
EANTC	European Advanced Networking Test Center
ECMP	Equal-Cost Multi-Path
Flex-Algo	Flexible Algorithm
IoT	Internet of Things
IP	Internet Protocol
IP/MPLS	Internet Protocol/Multi-Protocol Label Switching
IPFIX	IP Flow Information Export
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
L3	Layer 3
MPLS	Multiprotocol Label Switching
NFV	Network Functions Virtualisation
OAM	Operations, Administration, and Maintenance
OSPFv3	Open Shortest Path First Version 3
PCE	Path Computation Element

RFC	Request for Comment
SA	Source Address
SFC	Service Function Chaining
SID	Segment Identifier
SLA	Service Level Agreement
SR	Segment Routing
SR-MPLS	Segment Routing - Multiprotocol Label Switching
SR-TEIB	Segment Routing Traffic Information Base
SRH	Segment Routing Header
SRv6	Segment Routing Over IPv6
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VNF	Virtual Network Functions
VPN	Virtual Private Networks

## 4. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.

### 4.1 Border Gateway Protocol (BGP)

Protocol used to exchange routing information between different autonomous systems on the Internet.

### 4.2 Endpoint node

Destination node or egress node in an SRv6 network where the data packet's journey ends. It processes the final segment in the routing instruction and delivers the data packet to the intended application or service.

### 4.3 Flexible Algorithm (Flex-Algo)

A routing method that allows network operators to define custom routing algorithms based on specific constraints and performance metrics. This enables dynamic path computation tailored to the network's requirements, optimising for factors like latency, bandwidth, and reliability. Flex-Algo leverages Segment Routing (SR) to provide these customised routing capabilities.

### 4.4 Intermediate System to Intermediate System (IS-IS)

Interior gateway protocol used to move information efficiently within a computer network.

### 4.5 Multiprotocol Label Switching (MPLS)

A data-carrying technique that directs and carries data from one network node to the next using labels rather than long network addresses, thus avoiding complex lookups in a routing table.

### 4.6 Operations, Administration, and Maintenance (OAM)

A set of network management tools and protocols used to monitor, troubleshoot, and ensure the proper operation of a network, including SRv6.

## **MCMC MTSFB TC G053:2025**

### **4.7 Path Computation Element (PCE)**

Network component that calculates optimal network paths based on policy constraints and traffic engineering objectives, typically used in centralised architectures.

### **4.8 Segment Identifier (SID)**

A unique identifier used in SRv6 to represent a specific instruction or function within the network. Segment Identifier (SID)s can indicate nodes, links, services, or other network resources.

### **4.9 Segment Routing (SR)**

A method of source routing that allows a source node to define the path that a packet will take through the network by including a list of instructions, known as segments, in the packet header.

### **4.10 Segment routing domain**

Contiguous part of the network where SRv6 is deployed. It consists of routers that support SRv6 and share a common set of SIDs and policies.

### **4.11 Segment Routing Header (SRH)**

An IPv6 extension header used in SRv6 that contains a list of SIDs, defining the path a packet should follow through the network.

### **4.12 Segment Routing over IPv6 (SRv6)**

An extension of SR that utilises IPv6 addresses and extension headers to encode routing information, allowing the programming of network paths directly into the IPv6 packet headers.

### **4.13 Service Function Chaining (SFC)**

A process that enables the creation of composite network services consisting of an ordered set of service functions, such as firewalls, load balancers, and deep packet inspection.

### **4.14 Service Level Agreement (SLA)**

A contract between a service provider and a customer that specifies the performance, availability, and other service metrics that the provider guarantees to meet.

### **4.15 Source node**

Originating node or ingress node in the SRv6 network that initiates the data packet and determines the entire path the packet will take by encoding the routing information within the packet headers.

### **4.16 SRv6 controller**

Centralised or distributed controller responsible for managing the SRv6 domain, distributing SIDs, and computing optimal paths.

### **4.17 Transit node**

Intermediate node in an SRv6 network that forwards data packets along their predetermined path. The Transit node processes the SR instructions encoded in the packet headers but does not modify them.

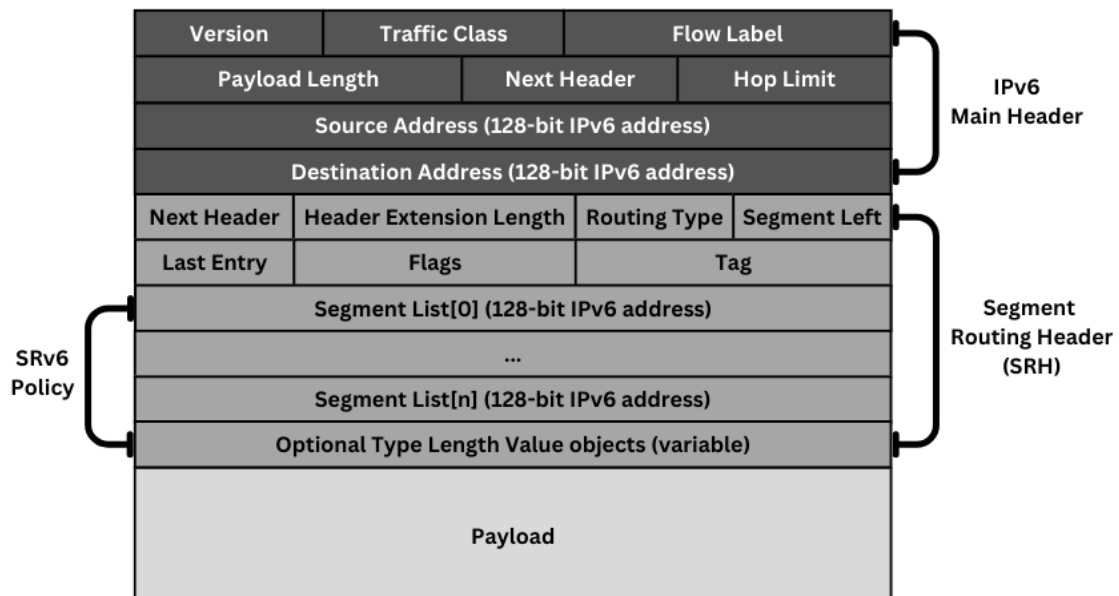
**4.18 Virtual Network Functions (VNFs)**

Software implementations of network functions (such as routing, firewalling, or load balancing) that can run on virtualised hardware.

**5. Segment Routing over IPv6 (SRv6)**

SRv6 is an advanced networking protocol designed to enhance network operations by encoding routing instructions directly into IPv6 packet headers. This protocol simplifies network management, providing more efficient, flexible, and programmable operations through source routing.

SRv6 allows the sender of a packet to define the entire path it will take using SIDs. SIDs are unique identifiers that represent specific network functions or instructions. They are used to create paths, enforce policies, and indicate nodes, links, services, or other network resources, facilitating precise, and dynamic traffic control. Figure 1 shows the structure of the Segment Routing Header (SRH) and its encapsulation within the IPv6 packet structure.



**Figure 1. Structure of the SRH and its encapsulation in the IPv6 packet**

Table 1 provides the explanation regarding the fields within the SRH as illustrated in Figure 1.

**Table 1. Detail of the SRH structure**

No	Structure	No of bit	Details
1	Version	4 bits	Indicates the IP version (6 for IPv6)
2	Traffic class	8 bits	Specifies the packet's priority and differentiates services
3	Flow label	20 bits	Identifies a flow of packets for special handling
4	Payload length	16 bits	Length of the packet's payload (excluding the IPv6 header)

**Table 1. Detail of the structure of SRH (continued)**

No	Structure	No of bit	Details
5	Next header	8 bits	Indicates the type of the next header (e.g., Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or extension headers)
6	Hop limit	8 bits	Maximum number of hops the packet can take before being discarded
7	Source address	128 bits	The IPv6 address of the sender
8	Destination address	128 bits	The IPv6 address of the recipient
9	Next header	8 bits	Identifies the header type following the SRH (e.g., TCP, UDP)
10	Header extension length	8 bits	The length of the SRH in 8-byte units, excluding the first 8 bytes
11	Routing type	8 bits	Set to 4 for segment routing
12	Segments left	8 bits	Indicates the index of the active segment in the segment list
13	Last entry	8 bits	Points to the last segment in the segment list
14	Flags	8 bits	Reserved for future use or specific functionalities
15	Tag	16 bits	Optional field for metadata or traffic classification
16	Segment list	Variable	An ordered list of IPv6 addresses (segments) that define the path the packet should follow
17	Optional type length value objects	Variable	Additional information such as security or policy data

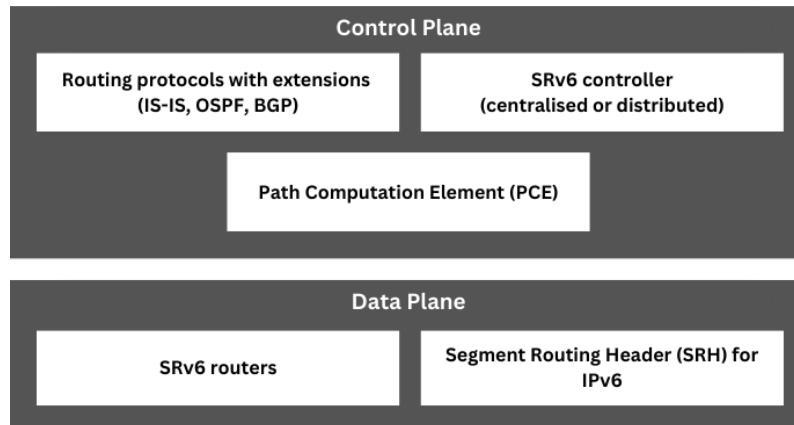
**5.1 Key components of SRv6 architecture**

**5.1.1 Segment routing domain**

A segment routing domain is a part of the network where SRv6 is deployed. It consists of routers that support SRv6 and share common SIDs and policies, ensuring coordinated traffic management and routing.

**5.1.2 Control plane components**

The SRv6 controller oversees the SRv6 domain by distributing SIDs and computing optimal paths for traffic flow. Figure 2 provides an overview of the SR architecture, routing protocols enhanced with SRv6 extensions, such as BGP-LS, IS-IS, and Open Shortest Path First Version 3 (OSPFv3), distribute network topology and SID information, enabling efficient routing and network management. The Path Computation Elements (PCE) calculates optimal network paths based on policy constraints and traffic engineering goals, ensuring efficient and effective traffic routing.



**Figure 2. SR architecture overview**

### 5.1.3 Data plane components

SRv6 routers are responsible for processing packets according to the instructions embedded in the SRH. This ensures precise control over packet routing throughout the network. The SRH itself is an IPv6 extension header that contains a list of SIDs. These SIDs define the specific path a packet should take, allowing for exact and programmable routing control within the network.

## 5.2 Benefits of SRv6

SRv6 offers several key benefits that significantly enhance network performance and management. One of the primary advantages is enhanced traffic engineering. SRv6 provides detailed control over traffic paths, optimising network performance and reliability. By efficiently managing traffic loads, it prevents congestion and improves speed, as illustrated in Figure 3.

Another benefit is network slicing, which enables the creation of multiple isolated networks on the same physical infrastructure. This allows for customised network environments for different applications or user groups, thereby improving resource utilisation.

In terms of security, SRv6 enhances traffic isolation and precise path control, which improves overall security. It also supports the integration of security protocols like IPsec, allowing for encrypted data transmission.

Advanced network management is another key benefit. SRv6 reduces complexity compared to traditional protocols, simplifying network configuration and management. The use of a centralised controller enables dynamic adjustments and real-time optimisation, leading to cost savings and greater agility.

SRv6 supports evolving network services and applications, ensuring that infrastructure can adapt to new demands without major overhauls. These benefits collectively make SRv6 a robust and flexible solution for modern networking challenges.

MCMC MTSFB TC G053:2025

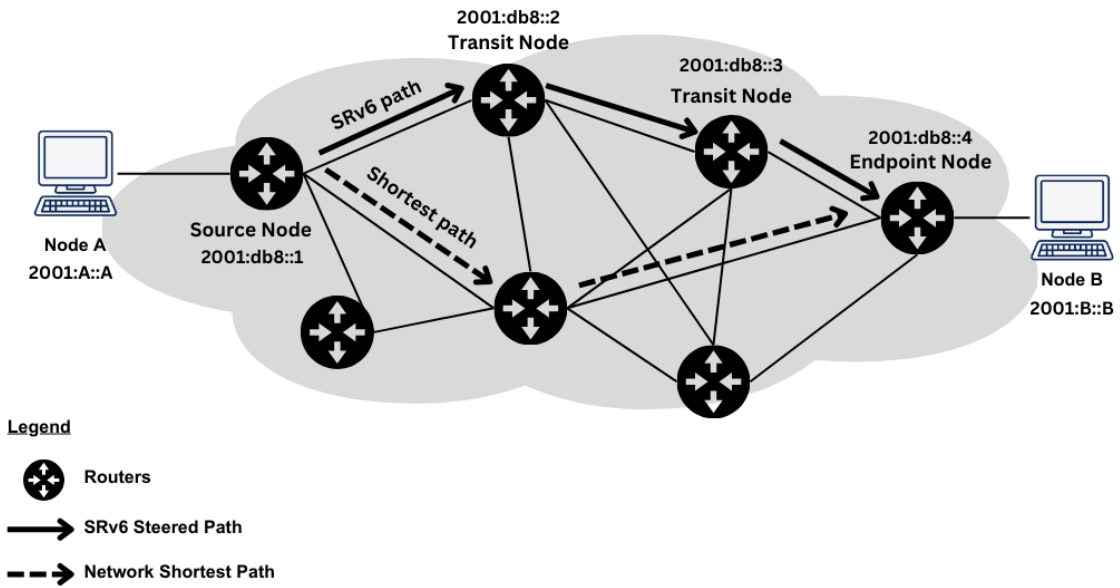


Figure 3. Segment Routing path options

SR-MPLS and SRv6 are 2 approaches to implementing segment routing, each with distinct characteristics. Table 2 shows the comparison between the two based on key factors.

Table 2. Difference between SR-MPLS and SRv6

Features	SR-MPLS	SRv6
Underlying protocol	MPLS (label-based)	IPv6 (address-based)
Addressing	20-bit MPLS labels	128-bit IPv6 addresses
Infrastructure	MPLS-capable devices required	IPv6-capable devices
Scalability	Limited (~1 million labels)	Virtually unlimited
Flexibility	Less programmable	Highly programmable
Operational costs	Higher due to specialised MPLS gear	Lower with IPv6 infrastructure
Use cases	Traditional MPLS networks	All IPv6 Network, including 5G, IoT, cloud, and next generation architectures
Security	Basic MPLS security	Stronger, with IPsec and isolation
Performance	Low latency, high performance	Comparable, with larger headers
Future-readiness	Suited for MPLS environments only	Aligned with IPv6 and future networks

### **5.3 Functionalities and features of SRv6**

SRv6 offers a range of functionalities and features that enhance its capabilities in modern networking environments. One of the key functionalities is service functions and service chaining. Service Function Chaining (SFC)s are sequences of service functions, such as security devices, that packets shall pass through. SFF ensure that packets follow the correct service chain, maintaining the integrity and efficiency of the service flow.

Traffic engineering with explicit paths is another crucial feature. By configuring specific paths through the network using SIDs, SRv6 optimises various objectives, such as minimising latency or maximising bandwidth use. This precise control over traffic paths, as shown in Figure 3, enhances overall network performance.

Network programming is also a significant feature of SRv6. Custom SIDs and behaviours can be programmed into the IPv6 extension header, enabling support for innovative services and applications. This flexibility allows for the development and deployment of tailored network solutions that meet specific requirements.

Interfaces and links represent the physical and logical connections between SRv6 routers. These connections support both IPv6 and SRv6 protocols, ensuring seamless integration and operation within the network infrastructure.

The functionalities and features of SRv6 provide powerful tools for network optimisation, security, and flexibility, making it a robust solution for modern networking needs.

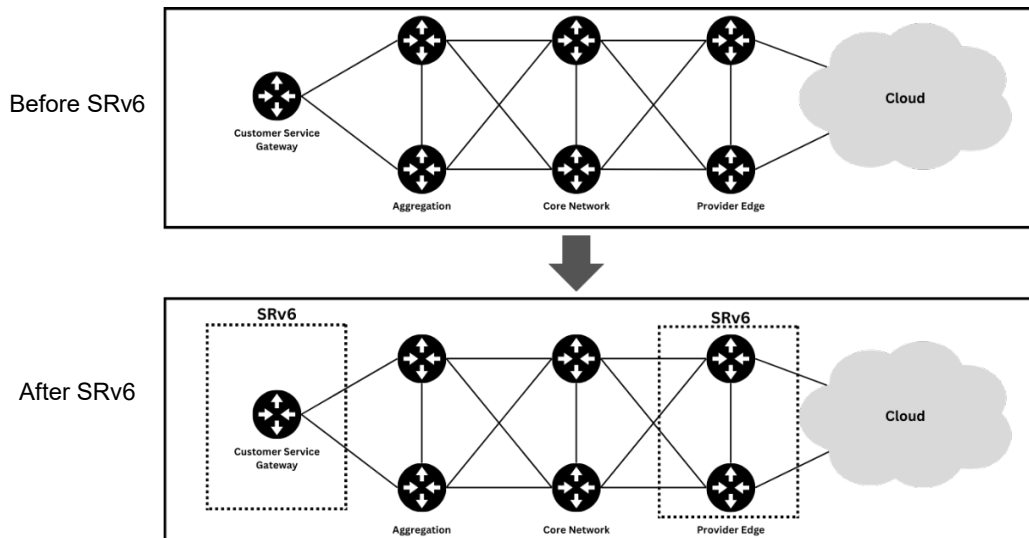
## **6. SRv6 deployment requirements**

SRv6 is designed to be compatible with both existing IPv6 networks and new greenfield deployments, allowing services to be quickly provisioned on demand. This compatibility ensures that organisations can leverage their current infrastructure without extensive network-wide upgrades, while also providing a flexible foundation for new network builds. SRv6 requires configuration only on source nodes and endpoint nodes, thereby reducing deployment time and enhancing operational efficiency.

### **6.1 Deployment phases**

During the initial phase, key devices such as ingress and egress routers shall support SRv6 as shown in Figure 4. For entities with existing infrastructure, subsequent service deployment relies on these supported devices, with transit devices continuing to support IPv6 and forward packets via IPv6 routes. In greenfield deployments, the entire network can be designed with SRv6 capabilities from the start, ensuring optimal performance and flexibility. Future upgrades of transit nodes can be performed on demand to enable value-added services through SRv6 traffic engineering, benefiting both existing and new network environments.

## MCMC MTSFB TC G053:2025



**Figure 4. Before and after the implementation of SRv6**

### 6.1.1 Planning and preparation

The planning and preparation phase for SRv6 deployment involves several key steps as follows:

a) Identify use cases

Determine the specific use cases for implementing SRv6, such as traffic engineering, security enhancements, or network slicing.

b) Assessment

Evaluate the existing network infrastructure to determine its compatibility with SRv6, including hardware and software requirements.

c) Requirements gathering

Identify the specific requirements for SRv6 deployment, including traffic engineering needs, security considerations, and network slicing capabilities.

d) Vendor consideration

Select vendors that support SRv6 features and ensure their products are interoperable with your network.

e) Migration plan

Develop a detailed migration plan for transitioning to SRv6 or create a deployment strategy for greenfield projects.

### 6.1.2 Hardware and software requirements

All devices should generally support IPv6. Key devices, such as the source node and endpoint node, shall support SRv6, as illustrated in Figure 4. The SRv6 functions should adhere to the checklist for network components outlined in Annex A.

Below are the key components for SRv6.

a) Network elements

Upgrade at source and endpoint nodes to support SRv6 encapsulation and forwarding. Verify they can manage SRv6-specific traffic and have the necessary processing power.

b) Network controllers

Whether centralised or distributed, these controllers manage the SRv6 domain. They distribute SIDs and compute optimal paths.

c) Path Computation Elements (PCEs)

These are essential for calculating the best network paths based on policy constraints and traffic engineering objectives.

d) SRv6 routing protocols

Deploy the Segment Routing Traffic Information Base (SR-TEIB) and use routing protocols with SRv6 extensions to manage and distribute SRv6-specific information.

e) Network management tools

Ensure these tools support SRv6 configuration and monitoring. They are critical for maintaining network performance and troubleshooting any issues that may arise.

For further information on the necessary RFCs for SRv6 implementation, see Annex B.

### 6.1.3 Initial deployment

The initial deployment phase focuses on preparing essential components for SRv6 operations, which are as follows.

- a) Upgrade the source node and endpoint node to support SRv6 encapsulation. This approach minimises network disruption and allows for rapid service deployment.
- b) Configure SRv6-capable devices to handle SIDs and implement basic SRv6 policies. This step ensures that the upgraded nodes can efficiently manage SRv6-specific traffic and adhere to the defined routing policies.

### 6.1.4 Incremental upgrades

Incremental upgrades, which involve a phased approach to gradually enhance the network's SRv6 capabilities, require careful planning and execution, with the following considerations being essential for effective implementation and integration:

- a) These upgrades should be performed on-demand to enable advanced services through SRv6 traffic engineering. It is crucial to verify compatibility, ensuring all SRv6-capable devices integrate smoothly with the existing network infrastructure.
- b) Comprehensive testing to prevent any integration issues and ensure seamless operation. This guarantees a smooth transition while maximising the benefits of SRv6 deployment.

## **MCMC MTSFB TC G053:2025**

### **6.1.5 Full deployment and optimisation**

During the full deployment phase, the focus should be on enhancing network performance and security. Leveraging SRv6 enables organisations to efficiently manage data traffic while ensuring robust data protection. The following key aspects should be considered.

#### a) Traffic engineering

SRv6 provides supports for traffic engineering. Based on this, traffic engineering policies can be created and implemented in a structured manner.

#### b) Security integration

Data security can be enhanced by using SRv6. The components of SRv6 that can be used to enhance data security include encryption and network slicing.

### **6.2 Best practices for SRv6 deployment**

SRv6 deployment should follow the following best practices to ensure optimal performance and security.

- a) IPv6 needs to be deployed in the network infrastructure.
- b) Start by upgrading source nodes and endpoint nodes to reduce network disruption. Plan future upgrades for transit nodes to fully utilise SRv6 features.
- c) Make sure SRv6-capable devices work well with the existing network. Conduct thorough testing to prevent integration problems.
- d) Interoperability test should be conducted by the accredited laboratory once the relevant test case is available in the future to ensure seamless SRv6 functionality across devices from various vendors.
- e) Use SRv6's traffic engineering to improve network performance. Create policies that take advantage of SRv6's ability to manage traffic efficiently.
- f) Provide comprehensive training for network staff on SRv6. Ensure detailed documentation is available to support ongoing maintenance and troubleshooting.
- g) Implement monitoring tools to track SRv6 performance. Regularly review network metrics to identify and address potential issues proactively.
- h) Regularly review and update SRv6 policies to adapt to changing network demands and security requirements. This helps in maintaining optimal network performance and security over time.
- i) Ensure sufficient vendor support throughout the migration. Work closely with sufficient vendor supports to ensure you are using the latest SRv6 features and updates. Vendor support can also assist in troubleshooting and optimising deployment.

For further details on testing and scenarios, see Annex C.

## **7. SRv6 security consideration**

The SRH is an extension header of IPv6 used by an IPv6 source to list one or more intermediate nodes (segments) that a packet shall traverse to reach its destination. While SRH enhances routing flexibility and programmability, it also introduces specific security concerns. These concerns shall be addressed to protect the network from potential threats.

## **7.1 Security vulnerabilities**

SRv6 is subjected to the various attack vectors and vulnerabilities that need to be addressed to ensure secure deployment.

The following are examples of several SRv6 related attacks.

a) SID spoofing

Malicious actors may attempt to spoof SIDs to manipulate traffic paths.

b) Path manipulation

Unauthorised modification of SRv6 paths can lead to traffic hijacking or rerouting.

c) DoS attacks

DoS attacks targeting SRv6 nodes can disrupt network services.

d) SID injection

Insertion of unauthorised SIDs into the SRv6 domain can compromise network integrity and security.

e) SID list exhaustion

Excessive SIDs can be injected to exhaust resources and disrupt network operations.

## **7.2 Mitigation strategies**

It is essential to implement effective mitigation strategies to address the security vulnerabilities identified in SRv6. These strategies will help safeguard the network against potential threats and ensure secure deployment.

The recommended measures are, but not limited to, the following.

a) Authentication and authorisation

Implement robust authentication and authorisation mechanisms to ensure that only trusted entities can interact with SRv6 nodes and modify SR policies.

b) Traffic encryption

Use encryption protocol to protect SRv6 traffic from interception and manipulation.

c) Ingress filtering

Apply ingress filtering at network entry points to block malicious traffic and unauthorised SIDs.

d) Rate limiting

Implement rate limiting on SRv6 nodes to mitigate the impact of DoS attacks.

e) Regular security audits

Conduct regular security audits to identify and address vulnerabilities promptly.

For a more comprehensive overview of IPv6 security, refer to the document MCMC MTSFB TC G046.

### **8. Technical advantages of SRv6**

#### **8.1 Service function chaining**

SFC allows the creation of complex network services by forwarding packets through a sequence of Virtual Network Functions (VNF). SRv6 uses SIDs to steer packets through these service functions. If a service function does not support SRv6, an SR proxy can handle the SRv6 traffic and route it correctly to the service function.

#### **8.2 Network slicing**

SRv6 supports the creation of Service Level Agreement (SLA)-based network slices from user applications through the transport network to the data centre. This logical separation, combined with SRv6 traffic engineering, ensures tailored service treatment for latency-sensitive applications and optimises bandwidth utilisation. For example, a telecom provider can create distinct virtual networks for streaming video, IoT, and regular internet traffic, each with specific performance characteristics.

#### **8.3 Load balancing**

SRv6 is compatible with existing IPv6 networks, enabling quick provisioning of services on demand. It requires configuration only at source and endpoint nodes, reducing deployment time and enhancing operational efficiency.

#### **8.4 Virtual Private Networks (VPN)**

SRv6 integrates seamlessly with IPv6 infrastructure, simplifying network management. SRv6 Virtual Private Networks (VPN) use SIDs to define paths for VPN traffic between endpoints. These SIDs are chained in the SRv6 header, guiding packets through the network. BGP advertises and distributes the necessary SIDs for VPN connectivity.

#### **8.5 Advanced routing scenarios**

SRv6 supports seamless routing across different Autonomous System (AS), an essential feature for large-scale networks where traffic traverses multiple administrative domains. This capability ensures efficient and reliable inter-AS routing.

**Annex A**  
(normative)

**Requirements of network components to support SRv6**

**Table A.1. Requirements of network components to support SRv6**

IETF specification	Document title	Node functions		
		Ingress node	Transit node	Egress node
RFC 8200	Internet Protocol, Version 6 (IPv6) Specification	Basic IPv6 processing and forwarding	Basic IPv6 processing and forwarding	Basic IPv6 processing and forwarding
RFC 8402	Segment Routing Architecture	Only follow SRv6 requirements	Only follow SRv6 requirements	Only follow SRv6 requirements
RFC 8754	IPv6 Segment Routing Header (SRH)	Insert SRH and define the segment list	Forward packets based on the active SID without processing SRH	Process the packet according to the final SID's instructions
RFC 8986	Segment Routing over IPv6 (SRv6) Network Programming	Ensure correct formatting of SRH and SID list	Perform standard IPv6 forwarding	Execute the function associated with the final SID (e.g., decapsulation, function execution)
RFC 9252	BGP Overlay Services Based on Segment Routing over IPv6 (SRv6)	Implement BGP for overlay services in SRv6	Forward BGP overlay traffic	Process BGP overlay services based on SIDs

**MCMC MTSFB TC G053:2025**

**Table A.1. Requirements of network components to support SRv6 (continued)**

IETF specification	Document title	Node functions		
		Ingress node	Transit node	Egress node
RFC 9259	Segment Routing over IPv6 (SRv6) Operations, Administration, and Maintenance (OAM)	Implement OAM functionality	Support OAM packets for network monitoring	Process OAM packets for troubleshooting and monitoring
RFC 9352	IS-IS Extensions to Support Segment Routing over IPv6 (SRv6)	Implement IS-IS protocol extensions	Forward IS-IS IPv6 routing updates	Use IS-IS for route computation and updates
RFC 9433	Segment Routing over IPv6 (SRv6) for Mobile User Plane	Implement SRv6 on user plane for mobile network	Forward user plane traffic	Process the SRv6 user plane according to the final SID's instructions
RFC 9487	IP Flow Information Export (IPFIX) Information Elements for Segment Routing over IPv6 (SRv6)	Send IP Flow information to collector including SRv6 elements	Send IP Flow information to collector including SRv6 elements	Send IP Flow information to collector including SRv6 elements
RFC 9513	OSPF Extensions for Segment Routing over IPv6 (SRv6)	Implement OSPFv3 protocol extensions	Forward OSPFv3 routing updates	Use OSPFv3 for route computation and updates

**Annex B**  
(informative)

**Essential Request for Comment (RFC) for SRv6 implementation**

SRv6-capable network devices should support the following RFCs to ensure a comprehensive SRv6 implementation. The following list is not exhaustive:

- a) RFC 8402: Segment Routing Architecture
- b) RFC 8754: IPv6 Segment Routing Header (SRH)
- c) RFC 8986: Segment Routing over IPv6 (SRv6) Network Programming
- d) RFC 9252: BGP Overlay Services Based on Segment Routing over IPv6 (SRv6)
- e) RFC 9256: Segment Routing Policy Architecture
- f) RFC 9259: Operations, Administration, and Maintenance (OAM) in Segment Routing over IPv6 (SRv6)
- g) RFC 9352: IS-IS Extensions to Support Segment Routing over the IPv6 Data Plane
- h) RFC 9513: OSPFv3 Extensions for Segment Routing over IPv6 (SRv6)

These RFCs help ensure that SRv6 implementations are thorough and work well with other network components.

**Annex C**  
(informative)

**SRv6 proposed test cases and scenarios**

**C.1 Test case and scenarios of SRv6**

The following test cases and scenarios should be considered to ensure SRv6 readiness and interoperability. These are not the only tests to be done but are important:

<b>Test case/scenario</b>	<b>Explanation</b>
SRv6 locator SID advertisement by IS-IS	Check that IS-IS correctly advertises SRv6 locator SIDs
Signalling BGP-Based Layer 3 (L3) services over SRv6 core and verifying BGP peer establishment	Test the signalling of L3 services over the SRv6 core and ensure BGP peers are correctly established
IPv6 Segment Routing Header (SRH) encapsulation to the packet	Make sure the SRH is correctly added to IPv6 packets
Forwarding both IPv4 and IPv6 packets over SRv6 core	Verify that both IPv4 and IPv6 packets can be forwarded over the SRv6 core
Flex-Algo locator advertisement and reception	Test the advertisement and reception of Flex-Algo locators to ensure they work properly
SRv6 network programming validation	Check the functionalities of SRv6 network programming, including Endpoint and SR Policy Headend behaviours
SRv6 network programming validation	Check the functionalities of SRv6 network programming, including Endpoint and SR Policy Headend behaviours
Segment routing policy architecture verification	Ensure the SR policy architecture works correctly, including controller-based policy installation
OAM testing	Make sure OAM features for SRv6, like PING and Traceroute, are working
OSPFv3 extensions for SRv6 testing	Verify that SRv6 capabilities and locators are correctly advertised and handled using OSPFv3 extensions

These tests will help ensure that the SRv6 implementation is ready and can work well with other systems.

**C.2 Use case of SRv6 deployment in Malaysia**

The deployment of SRv6 in Malaysia aims to address the increasing need for a more adaptable and future-ready network architecture, capable of supporting next-generation technologies such as 5G, cloud services, Artificial Intelligence (AI), and the IoT. The decision to migrate to SRv6 was driven by the protocol's native IPv6 capabilities, which enhance scalability, simplify network management, and improve traffic engineering functionalities. These attributes make SRv6 an ideal solution for future-proofing infrastructure while enabling Malaysia's broader digital transformation.

Before SRv6 deployment, the core network relied on Internet Protocol/Multi-Protocol Label Switching (IP/MPLS) for traffic forwarding and traffic engineering. While MPLS played a key role in managing network traffic, the shift towards an IPv6-dominant environment required a more scalable and flexible solution. SRv6's programmability offers a sustainable and forward-looking approach.

The migration timeline for SRv6 has been influenced by multiple factors, including hardware and software readiness and the optimisation of routing protocols. Although SRv6's native IPv6 functionality simplifies aspects of the transition, thorough protocol optimisation and network-wide testing have been necessary to ensure seamless operations. The network's existing dual-stack (IPv4/IPv6) configuration has expedited some processes, though the overall migration timeline remains dependent on infrastructure readiness and external factors.

### **C.3 Challenges and Benefits of SRv6 Migration**

Several key challenges emerged during the SRv6 migration in Malaysia, including:

a) Hardware and software readiness

Ensuring vendor-provided hardware and software fully support SRv6 has been an ongoing process. Different vendors have adopted SRv6 capabilities at varying speeds, necessitating careful evaluation of product roadmaps to ensure alignment with long-term network requirements.

b) Industry standards

While SRv6 is built on IETF standards (e.g., RFC 8986), some aspects of the technology are still evolving. Adaptability is crucial to ensure that the deployment aligns with best practices as industry standards continue to develop.

c) Interoperability across vendors

A key deployment consideration is ensuring vendor neutrality and interoperability. Although SRv6 is an open standard, ensuring that different vendors' implementations work seamlessly together in a multi-vendor environment has required extensive testing and validation to prevent disruptions.

d) Concurrent operations

A major focus during the transition has been ensuring that the new SRv6 solution can operate concurrently with existing systems. This has allowed for the maintenance of seamless service continuity, avoiding disruptions while gradually migrating to SRv6.

e) Upskilling the workforce

The migration to SRv6 has required upskilling engineering teams to manage the complexities of the new protocol. Comprehensive training programmes have been implemented to ensure smooth operations and efficient network management.

The implementation of SRv6 yields the following benefits.

a) Simplified network architecture

SRv6 simplifies the network by embedding routing instructions directly into IPv6 headers, eliminating the need for separate control planes and overlay protocols. This reduces network complexity and operational overhead.

## **MCMC MTSFB TC G053:2025**

### b) Advanced traffic engineering

The network leverages SRv6 for dynamic path selection and load balancing, ensuring optimal use of network resources and reduced latency for critical applications.

### c) Service Level Agreement (SLA) adherence

The SRv6-enabled network guarantees consistent bandwidth, low latency, and minimal packet loss, allowing the organisation to provide detailed SLA reports, enhancing transparency and reliability for enterprise customers.

### d) Scalability and flexibility

SRv6 enhances the network's ability to dynamically manage resources, making it ideal for cross-domain connections and large-scale networking. It also supports the transition to a cloud-network synergy model, offering customised service bundles for diverse enterprise needs.

## **Acknowledgements**

### **Numbering and Electronic Addressing Working Group**

#### **Working Group Leaders**

Ts Adil Hidayat Rosli (Chair)	My6 Initiatives Berhad
Mr Lee Wei Han (Vice Chair)	Maxis Broadband Sdn Bhd
Ts Mohd Faizal Abdul Raup (Secretary)	TM Technology Services Sdn Bhd

#### **Drafting Committee Members**

Professor Emeritus Dr Sureswaran Ramadass (Draft Lead)	Persatuan IPv6 Malaysia
Ms Nurul Amirah Zarifah Norazaruddin (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Lee Wei Han	Maxis Broadband Sdn Bhd
Dr Navaneethan C. Arjuman	Multimedia University
Ts Adil Hidayat Rosli	My6 Initiatives Berhad
Dr Mohamed Elnour Abdelhafez Fadul	Persatuan IPv6 Malaysia
Ts Mohd Faizal Abdul Raup	TM Technology Services Sdn Bhd
Ts Hanaffy Geoffrey Ramli	CelcomDigi Berhad

#### **Contributors**

Ts Salim Mohammad Ghani	American Malaysian Chamber of Commerce
Mr Mohd Suffian Ramli	Digital Nasional Berhad
Mr Wang Xiaoping	Huawei Technologies (Malaysia) Sdn Bhd
Mr Alex Lim Yau Chong	Huawei Technologies (Malaysia) Sdn Bhd
Ms Azura Mat Salim	TM Technology Services Sdn Bhd
Mr James Chin Sze Yih	TT DOTCOM Sdn Bhd