TECHNICAL CODE

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

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date:

MCMC MTSFB TC G0XX: 2024

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
Website: www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Level 3A, MCMC Tower 2Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8680 9950
Fax : +60 3 8680 9940
Email : support@mtsfb.org.my
Website: www.mtsfb.org.my

Contents

Page

Committee representation

This technical code was developed by 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

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.

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

0. Introduction

Segment Routing over IPv6 (SRv6) is a modern technique for routing data across networks. It simplifies the process by letting the data source determine the entire path the data will follow, rather than leaving 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 offers several benefits over traditional routing methods and even over Segment Routing (SR) with Multiprotocol Label Switching (MPLS). By using IPv6 addresses for the segments, SRv6 provides more flexibility and scalability. It is well-suited for managing the massive growth in connected devices and data driven by technologies like 5G, IoT, and cloud computing. Additionally, SRv6 seamlessly integrates with IPv6 networks from the edge to the data centre, making network management more efficient. As networks continue to evolve, SRv6 is poised to become a crucial technology for future developments.

1. Scope

This Technical Code provides requirements for deploying and operating SRv6 in Malaysia. It describes on SRv6 technology, use cases, security recommendations, and standards for deployment.

This Technical Code assists network administrators, security professionals, and technical personnel in properly deploying SRv6, achieving improved traffic management, network segmentation, and enhanced security.

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 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.

BGP	Border Gateway Protocol
C-SID	Compressed Segment Identifier
DA	Destination Address
DMZ	De-Militarised Zone
ECMP	Equal-Cost Multi-Path
Flex-Algo	Flexible Algorithm
IP	Internet Protocol
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
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
SRH	Segment Routing Header
SRv6	Segment Routing Over IPv6
VNF	Virtual Network Functions
VPN	Virtual Private Network

4. Terms and definitions

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

4.1 Segment Routing (SR)

SR is 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.

4.2 Segment Routing over IPv6 (SRv6)

SRv6 is 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.

4.3 Segment Identifier (SID)

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

4.4 Segment Routing Header (SRH)

The Segment Routing Header (SRH) is an IPv6 extension header used in SRv6 that contains a list of SIDs, defining the path a packet should follow through the network.

4.5 Segment routing domain

A Segment Routing Domain is a 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.

4.6 SRv6 Controller

An SRv6 Controller is a centralised or distributed controller responsible for managing the SRv6 domain, distributing SIDs, and computing optimal paths.

4.7 Path Computation Element (PCE)

A Path Computation Element (PCE) is a network component that calculates optimal network paths based on policy constraints and traffic engineering objectives, typically used in centralised architectures.

4.8 Service Function Chaining (SFC)

Service Function Chaining (SFC) is 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.

4.9 Virtual Network Functions (VNFs)

Virtual Network Functions (VNFs) are software implementations of network functions (such as routing, firewalling, or load balancing) that can run on virtualised hardware.

4.10 Service Level Agreement (SLA)

A Service Level Agreement (SLA) is a contract between a service provider and a customer that specifies the performance, availability, and other service metrics that the provider guarantees to meet.

4.11 Multiprotocol Label Switching (MPLS)

MPLS is 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.

4.12 Border Gateway Protocol (BGP)

The Border Gateway Protocol (BGP) is the protocol used to exchange routing information between different autonomous systems on the Internet.

4.13 Intermediate System to Intermediate System (IS-IS)

Intermediate System to Intermediate System (IS-IS) is an interior gateway protocol used to move information efficiently within a computer network.

4.14 Operations, Administration, and Maintenance (OAM)

Operations, Administration, and Maintenance (OAM) is a set of network management tools and protocols used to monitor, troubleshoot, and ensure the proper operation of a network, including SRv6.

4.15 Source node

A Source node is the originating node in an SRv6 network that initiates a data packet and determines the entire path the packet will take by encoding the routing information within the packet headers.

4.16 Transit node

A Transit node is an 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.

4.17 Endpoint node

An endpoint node is the destination node in an SRv6 network where the data packet's journey ends. It processes the final segment in the routing instruction and consumes the data packet, typically delivering it to the intended application or service.

4.18 Flexible Algorithm (Flex-Algo)

Flexible Algorithm (Flex-Algo) is 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 to provide these customised routing capabilities.

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. Refer to Figure 1.

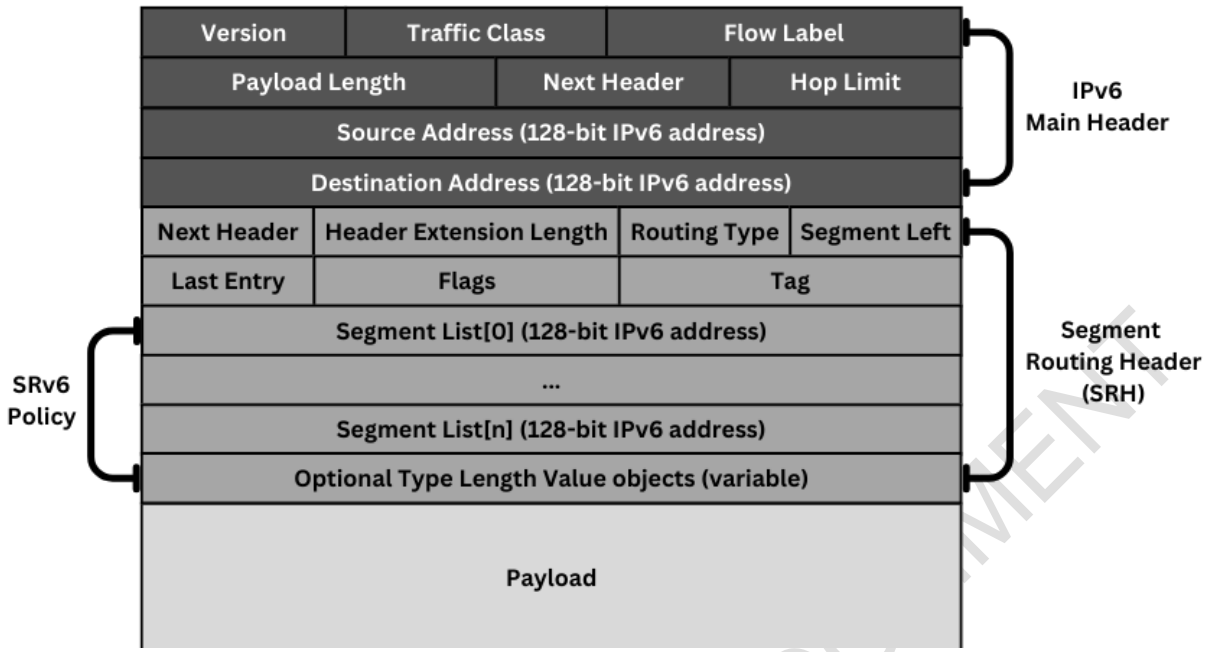

Figure 1. Structure of the SRH and its encapsulation in the IPv6-Packet

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. As illustrated in Figure 2, which provides an overview of the Segment Routing architecture, routing protocols enhanced with SRv6 extensions, such as BGP-LS, IS-IS, and OSPFv3, distribute network topology and SID information, enabling efficient routing and network management. The PCE calculates optimal network paths based on policy constraints and traffic engineering goals, ensuring efficient and effective traffic routing.

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 2.

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.

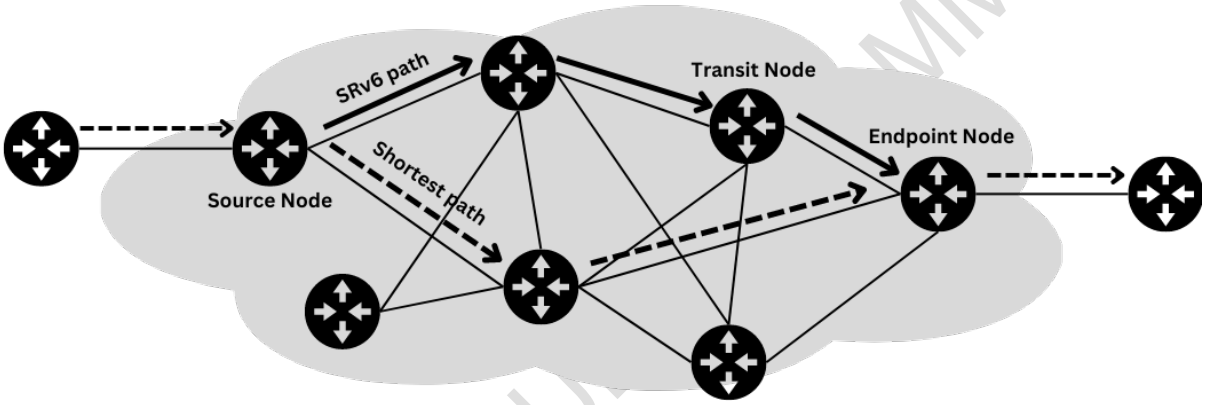

Figure 2. Segment Routing path options

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. SFCs 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.

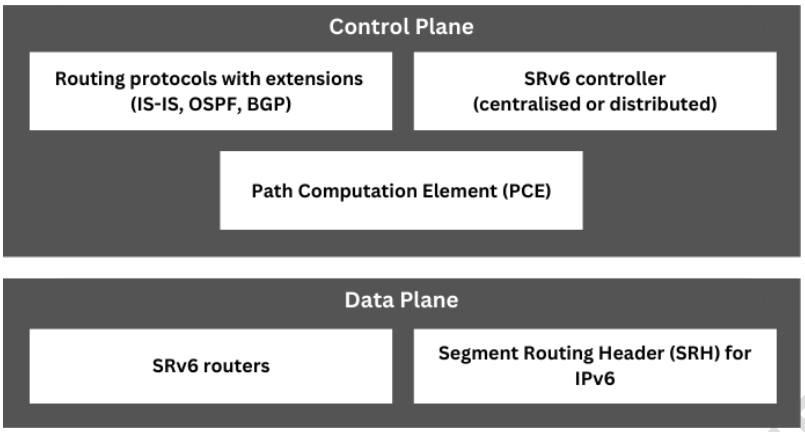

Figure 3. SR architecture overview

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.

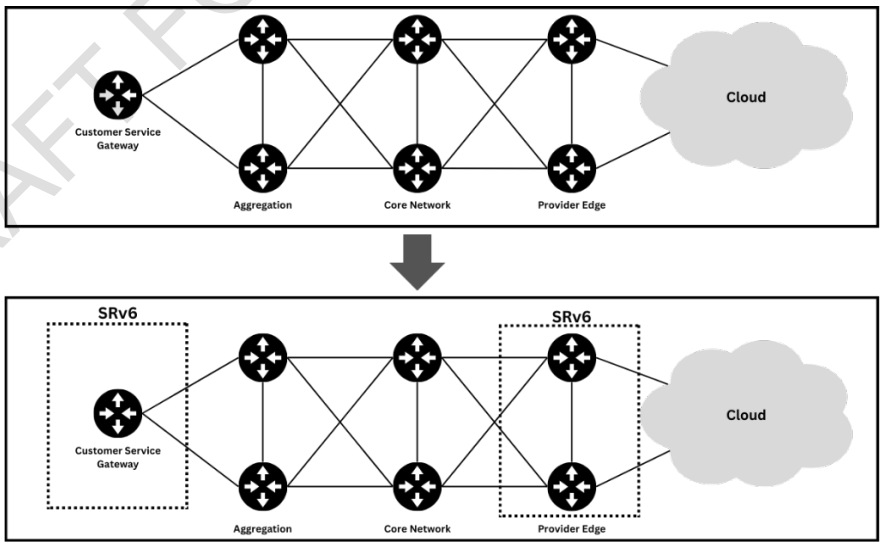

Figure 4. On-Demand SRv6 upgrade

6.1.1 Planning and preparation

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

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.

The following 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. Begin by upgrading the source node and endpoint node to support SRv6 encapsulation. This approach minimises network disruption and allows for rapid service deployment. Next, 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 involve a phased approach to gradually enhance the network's SRv6 capabilities. Begin by planning future upgrades of transit nodes to achieve full SRv6 functionality. 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. Conduct comprehensive testing to prevent any integration issues and ensure seamless operation. This methodical approach guarantees a smooth transition while maximising the benefits of SRv6 deployment.

6.1.5 Full deployment and optimisation

In the full deployment phase, focus on improving network performance and security. Using SRv6, organisations can manage traffic efficiently and protect data effectively.

Specifically, attention should be given to the following aspects.

a) Traffic engineering

Use SRv6 to improve network performance. Create policies that take advantage of SRv6 features for better traffic management.

b) Security integration

Enhance data security by implementing encryption, network slicing and integrating security devices with SFC to ensure strong traffic isolation and effective path control.

6.2 Best practices for SRv6 deployment

For a successful SRv6 deployment, follow these 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) Use SRv6's traffic engineering to improve network performance. Create policies that take advantage of SRv6's ability to manage traffic efficiently.

e) Provide comprehensive training for network staff on SRv6. Ensure detailed documentation is available to support ongoing maintenance and troubleshooting.

f) Implement monitoring tools to track SRv6 performance. Regularly review network metrics to identify and address potential issues proactively.

g) 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.

h) Work closely with vendors 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 MTFSB TC G046.

8. Technical SRv6 advantages

8.1 Service Function Chaining

SFC allows the creation of complex network services by forwarding packets through a sequence of VNFs. 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 SLA-based network slices from user applications through the transport network to the datacentre. 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 (VPNs)

SRv6 integrates seamlessly with IPv6 infrastructure, simplifying network management. SRv6 VPNs 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 AS, essential for large-scale networks where traffic traverses multiple administrative domains. This capability ensures efficient and reliable inter-AS routing.

Annex A
(informative)

SRv6 Functions

Table A.1. SRv6 features support checklist for network components

IETF Specification	Document Title	Node Functions		
		Source Node	Transit Node	Endpoint 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.

Table A.1. SRv6 features support checklist for network components *(continued)*

IETF Specification	Document Title	Node Functions		
		Source Node	**Transit Node**	**Endpoint 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	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 RFCs for SRv6 implementation

SRv6-capable network devices should support the following RFCs to ensure a comprehensive SRv6 implementation. This 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

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:

a) SRv6 Locator SID Advertisement by IS-IS

Check that IS-IS correctly advertises SRv6 Locator SIDs.

b) Signalling BGP-Based L3 Services Over SRv6 Core and Verifying BGP Peer Establishment:

Test the signalling of Layer 3 services over the SRv6 core and ensure BGP peers are correctly established.

c) IPv6 Segment Routing Header (SRH) Encapsulation to the Packet

Make sure the SRH is correctly added to IPv6 packets.

d) Forwarding Both IPv4 and IPv6 Packets Over SRv6 Core

Verify that both IPv4 and IPv6 packets can be forwarded over the SRv6 core.

e) Flex-Algo Locator Advertisement and Reception

Test the advertisement and reception of Flex-Algo Locators to ensure they work properly.

f) SRv6 Network Programming Validation

Check the functionalities of SRv6 network programming, including Endpoint and SR Policy Headend behaviours.

g) Segment Routing Policy Architecture Verification

Ensure the SR policy architecture works correctly, including controller-based policy installation.

h) Operations, Administration, and Maintenance (OAM) Testing

Make sure OAM features for SRv6, like PING and Traceroute, are working.

i) 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.

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
Dr Mohamed Elnour Abdelhafez Fadul	Persatuan IPv6 Malaysia
Ts Adil Hidayat Rosli	My6 Initiatives Berhad
Mr Lee Wei Han	Maxis Broadband Sdn Bhd
Ts Mohd Faizal Abdul Raup	TM Technology Services Sdn Bhd
Ts Hanaffy Geoffrey Ramli	CelcomDigi Berhad
Dr Navaneethan A/L C. Arjuman	Multimedia University

Contributors

Ts Salim Mohammad Ghani	American Malaysian Chamber of Commerce
Mr Wang Xiaoqing	Huawei Technologies (Malaysia Sdn Bhd)
Mohd Suffian Bin Ramli	Digital Nasional Berhad