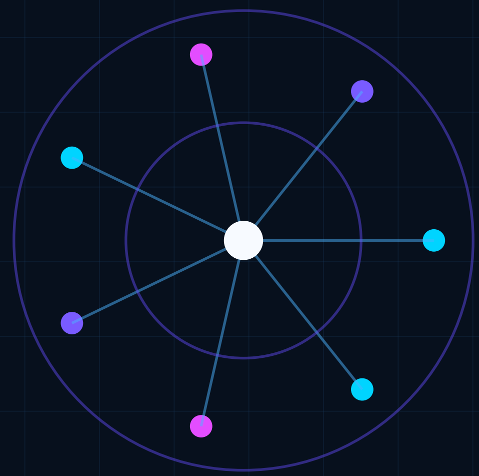
MYTHOS SYSTEMS

TECHNICAL LIBRARY / RESEARCH INTELLIGENCE

PROGRAMMABLE NETWORKING

Segment Routing (SRv6) Programmable Path Engineering

Current-source review, evidence-bounded adoption decision, explicit limitations, reproducibility controls, and preserved source research note.



PERMANENT ID	EVIDENCE	ADOPTION	FRESHNESS
RES-026	A	CONDITIONAL ADOPTION	STABLE WATCH

Freshness review: 2026-09-17 / Next scheduled review: 2027-03-16

CANDIDATE RESEARCH REPORT / 2.1.0-CANDIDATE / PUBLIC

RESEARCH CONTROL SURFACE

Required Research Fields

Each field remains independently reviewable; evidence strength does not imply production authority.

EVIDENCE GRADE — **A**

Strength of the retained source set and technical basis.

SOURCE AUTHORITY — **3 registered authorities**

RFC 8986 - SRv6 Network Programming; RFC 8754 - IPv6 Segment Routing Header; RFC 9800 - Compressed SRv6 Segment List Encoding

FRESHNESS — **STABLE WATCH**

Reviewed 2026-09-17; dynamic sources require event-driven revalidation.

CONFLICTS — **VISIBLE / NOT SILENT**

Differences between specification, vendor behavior, research claims, and reproduced evidence must remain explicit.

LIMITATIONS — **EXPLICIT**

No certification, procurement approval, legal conclusion, or unbounded production claim is created by this report.

REPRODUCIBILITY — **REQUIRED**

Material claims require exact versions, representative data, failure cases, artifacts, and repeatable acceptance criteria.

ADOPTION POSTURE — **CONDITIONAL ADOPTION**

Adopt SRv6 only where IPv6 maturity, hardware support, operations, security boundaries, MTU, telemetry, and control-plane integration justify the complexity.

REVIEW TRIGGER — **2027-03-16**

Scheduled at 180 days; earlier on material source, vulnerability, implementation, or contradictory-evidence change.

SOURCE AUTHORITY / FRESHNESS

Authority Register and Freshness Delta

Primary-source lineage is preserved; current-source changes are separated from unperformed implementation claims.

AUTHORITY 01

RFC 8986 - SRv6 Network Programming

https://www.rfc-editor.org/rfc/rfc8986

AUTHORITY 02

RFC 8754 - IPv6 Segment Routing Header

https://www.rfc-editor.org/rfc/rfc8754

AUTHORITY 03

RFC 9800 - Compressed SRv6 Segment List Encoding

https://www.rfc-editor.org/rfc/rfc9800

2026-09-17 FRESHNESS DELTA

Primary-source register retained and freshness controls advanced to the current review date. No new product or laboratory performance claim is introduced without reproduced evidence.

Freshness policy: scheduled review + immediate review on source supersession, material release, vulnerability, retraction, or contradictory evidence.

Evidence Must Survive Contact With Reality

SOURCE	CLAIM	TEST	EVIDENCE	DECISION
authority	bounded	representative	retained	conditional

- Source authority is not implementation evidence. Product behavior, scale, security, interoperability, and operator fit remain environment-specific.

- Conflicting evidence is recorded rather than averaged away. Specification behavior, vendor implementation, preprint results, and production observations are separate evidence classes.

- Quantitative claims are informative until reproduced under documented hardware, software, data, topology, load, and failure conditions.

- Adoption posture is reversible. A stronger source set can coexist with a pilot-only or research-only recommendation when maturity, safety, economics, or operability remain unresolved.

Decision Gate and Validation Plan

ADOPTION POSTURE

CONDITIONAL ADOPTION

Adopt SRv6 only where IPv6 maturity, hardware support, operations, security boundaries, MTU, telemetry, and control-plane integration justify the complexity.

1 / SOURCE	Pin exact versions, publication state, retrieved artifacts, and source hashes.
2 / PROTOTYPE	Demonstrate the core mechanism with representative data and instrumented execution.
3 / FAILURE	Exercise malformed input, dependency loss, stale state, overload, recovery, rollback, and misuse.
4 / BASELINE	Compare against an incumbent, classical, or simpler architecture using the same workload.
5 / ACCEPT	Record acceptance criteria, residual limitations, owner, expiration, and revalidation triggers.

EXPIRATION / REVIEW TRIGGER

Next scheduled review: 2027-03-16 (180-day cadence). Review sooner after material source revision, breaking implementation release, critical vulnerability, retraction, benchmark contradiction, changed workload, or changed legal/safety boundary.

8. Complete Source Research Note

SOURCE-LINEAGE NOTICE

The following material preserves the complete original source note, excluding only the conversational wrapper and outer Markdown fence. Legacy status labels and absolute language are retained for traceability and do not override the candidate status, limitations, or adoption decision in this edition.

Document ID: RES-026 Version: 1.0.0 (Definitive Registry Edition) Status: Published Research Note Classification: Public Organization: Mythos Systems (MYTHOS AI) Owner: Aaron Stovall Effective Date: 2026-07-16 Applies To: Network architects, service provider engineers, and datacenter fabric designers evaluating IPv6 Segment Routing (SRv6), TI-LFA failover, and Software-Defined Networking (SDN) transport fabrics Companion Standards: MYTHOS-NET-0006 (Segment Routing & Next-Gen Transport), MYTHOS-NET-0001 (Network Architecture), MYTHOS-NET-0002 (Multi-Vendor Automation), MYTHOS-NET-0008 (OSI Troubleshooting)

The architecture of service provider and large-scale datacenter transport has failed. For decades, organizations have relied on MPLS (Multiprotocol Label Switching) combined with LDP (Label Distribution Protocol) and RSVP-TE (Resource Reservation Protocol - Traffic Engineering) to engineer traffic paths. This paradigm is fundamentally flawed: it requires every node in the network to maintain complex, stateful control-plane adjacencies with its neighbors to distribute labels. When a link fails, the network must wait for IGP (OSPF/IS-IS) reconvergence, causing seconds of packet loss—unacceptable for real-time AI agent traffic and distributed state machines.

Segment Routing over IPv6 (SRv6) shatters this stateful legacy. It moves the path state out of the routers and into the packet header. Utilizing the IPv6 Segment Routing Header (SRH), an ingress node encodes a list of instructions (Segment Identifiers, or SIDs) directly into the data plane.

This research note defines the architectural dynamics of SRv6. It dissects the mechanics of encoding network functions as 128-bit IPv6 SIDs, the decoupling of the control plane (IGP/BGP-LS) from the data plane, and the implementation of Topology-Independent Loop-Free Alternate (TI-LFA) to achieve mathematically bounded sub-50ms failover. Understanding these dynamics is a prerequisite for building the ultra-resilient, programmable transport fabrics mandated by the Mythos Network Standards.

To understand SRv6, we must move from distributed stateful protocols to source-routed programmable packets.

1.1 The Segment Routing Header (SRH)

SRv6 is an extension of the IPv6 protocol. A new extension header—the SRH—is inserted into the IPv6 packet.

- The Mechanic: The SRH contains a "Segment List"—a stack of 128-bit IPv6 addresses representing the path the packet must take. The destination address of the IPv6 packet is set to the active SID. When a router processes the active SID, it updates the destination address to the next SID in the list.
- The Advantage: The core routers no longer need to maintain label tables or run LDP. They simply route based on the destination IPv6 address, which happens to be an instruction.

1.2 Segment Identifiers (SIDs) as Instructions

In SRv6, a SID is not just a destination; it is an executable instruction bound to a physical node or a specific function.

- Node SIDs: Represent a specific router in the topology (shortest path to that node).
- Adjacency SIDs: Represent a specific physical link between two routers. Forcing a packet through an Adjacency SID forces it onto that exact cable.

- Function SIDs (END.X, END.DX4): Represent advanced behaviors. `END.X` forces traffic onto a specific engineered path. `END.DX4` instructs a node to decapsulate the packet and hand it directly to a specific IPv4 endpoint (acting as a VPN endpoint).

1.3 The Stateless Core

Unlike MPLS, where every node must hold state for every label switched path (LSP) passing through it, an SRv6 core is stateless.

- The Paradigm Shift: The ingress PE (Provider Edge) router holds the state (the SID list). The core P (Provider) routers simply execute the instructions in the packet header. Adding a new service or traffic-engineered path does not require touching the core routers.

While SRv6 simplifies the control plane and enables ultimate programmability, it introduces severe physical and hardware constraints.

2.1 The IPv6 Overhead (MTU Penalty)

Every SID in the SRH is a 128-bit IPv6 address. A deeply engineered path with 10 SIDs adds 140+ bytes of overhead to every packet.

- The Flaw: Standard Ethernet MTU is 1500 bytes. Deep SID stacks easily exceed this, causing fragmentation or packet drops if ICMP "Fragmentation Needed" is blocked.
- The Mitigation: SRv6 deployments MUST implement jumbo frames (9000 byte MTU) end-to-end across the core, or utilize "SRv6 Compression" (e.g., uSID / G-SID) which compresses 128-bit SIDs into 16-bit micro-segments, drastically reducing header overhead.

2.2 Hardware ASIC Limitations

Standard switching ASICs were historically designed to parse fixed-length IPv4 and IPv6 headers. The SRH is a variable-length extension header.

- The Flaw: Older switches or white-box routers lacking SRv6-capable NPUs (Network Processing Units) will punt SRv6 packets to the CPU for processing. This causes instant wire-rate throughput collapse and microbursts.
- The Mitigation: The architecture MUST verify SRv6 hardware offload capabilities (via digital twins/Batfish) before deployment. If the ASIC cannot parse the SRH in hardware, the node is invalid for the core.

The true power of SRv6 is realized in its ability to guarantee packet delivery during physical failures and dynamically steer traffic based on application intent.

3.1 Topology-Independent Loop-Free Alternate (TI-LFA)

Traditional IP routing relies on IGP reconvergence when a link fails. The network detects the failure, floods new LSAs, runs SPF (Dijkstra), and installs new routes. This takes 200ms to 2 seconds.

- The SRv6 Mechanic: TI-LFA pre-computes a backup path for every destination before a failure occurs. Because SRv6 is source-routed, the router can instantly insert a "repair SID list" into the packet header, tunneling it around the failed link without waiting for IGP reconvergence.
- The Impact: Sub-50ms failover. The failure is mathematically invisible to the application layer, guaranteeing zero dropped sessions for real-time AI agent workflows.

3.2 Per-Flow Traffic Engineering (SR-TE)

In MPLS, traffic engineering requires complex RSVP-TE tunnels. In SRv6, the ingress node can dynamically program the SID list based on the application type.

- The Mechanic: An AI training job requires ultra-low latency. The SDN controller (PCEP) calculates a path utilizing low-latency fiber routes and pushes an SRv6 policy to the ingress router. The router stamps the packets with the specific SID list.
- The Impact: The network becomes application-aware. Bulk data takes the cheapest path; real-time agent commands take the fastest path, encoded entirely in the data plane.

The fundamental shift of SRv6 is the decoupling of topology from transport.

- Simplified Operations: The elimination of LDP and RSVP-TE removes millions of lines of configuration and dozens of failure modes. The network relies purely on the IGP (IS-IS/OSPF) for topology discovery.
- Datacenter Interconnect (DCI): Multi-cloud and sovereign datacenter fabrics can be stitched together using SRv6. A packet leaving a Kubernetes cluster in Datacenter A can carry an SRH that instructs it to traverse a specific subsea cable, bypass a congested public internet exchange, and terminate directly into a specific pod in Datacenter B.
- Service Function Chaining (SFC): Forcing traffic through firewalls and load balancers no longer requires VLAN hairpinning. A SID simply represents the firewall service. The packet is routed to the firewall SID, processed, and routed to the next SID.

To deploy SRv6 in production, the Mythos Architecture (specifically the NetBox SoT and continuous reconciliation pipelines) enforces strict operational boundaries.

5.1 Topology-Aware SID Allocation

SIDs MUST NOT be hardcodded. They must be dynamically allocated and tracked.

- The Mitigation: The Mythos SoT (NetBox/Nautobot) MUST act as the SRv6 SID allocator. When a new node is provisioned via IaC, the SoT assigns it a 128-bit SID block. The IGP automatically advertises this SID. The SDN controller queries the SoT to calculate paths, ensuring the SID list mathematically matches the physical topology.

5.2 Continuous TI-LFA Verification

A misconfigured TI-LFA policy can create routing loops during a failure.

- The Mitigation: The continuous reconciliation plane MUST run Batfish or Containerlab simulations that inject link failures into the digital twin. The simulation mathematically proves that the pre-computed TI-LFA backup paths are loop-free and converge in < 50ms before the configuration is pushed to production.

5.3 SRv6 Security (HMAC)

Because SRv6 allows source routing, a malicious actor could craft an SRH to bypass security checkpoints or force traffic down a specific path.

- The Mitigation: The architecture MUST enforce SRv6 HMAC (Hash-based Message Authentication Code) for sensitive domains. Packets containing an SRH targeting infrastructure SIDs MUST possess a cryptographic signature. Routers drop SRv6 packets lacking a valid HMAC, preventing source-routing abuse.

The strategy of distributing path state to every router in the network is an artifact of the 1990s. As AI and distributed state machines demand ultra-low latency and zero-packet-loss transport, the network must become stateless and programmable. SRv6 achieves this by encoding the path into the packet itself. By leveraging TI-LFA for sub-50ms failover and source-routed SID lists for per-flow engineering, we transform the transport fabric from a fragile, protocol-dependent web into a deterministic, application-aware data plane.

```
An LDP label is distributed state; an SRv6 SID is packet state.
An IGP reconvergence is a delay; a TI-LFA repair is an instant.
A fixed path is rigid; a programmable SID list is fluid.

The network is no longer a topology; it is an instruction set.
```

```
> Packets may traverse physical links.
> Path engineering must be absolute.
```

End of Research Note RES-026

9. Source Register

Source	Authority and Status	Freshness Control
RFC 8986 - SRv6 Network Programming https://www.rfc-editor.org/rfc/rfc8986	Primary standard Standards Track RFC Published: 2021	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
RFC 8754 - IPv6 Segment Routing Header https://www.rfc-editor.org/rfc/rfc8754	Primary standard Standards Track RFC; updated by RFC 9800 Published: 2020	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
RFC 9800 - Compressed SRv6 Segment List Encoding https://www.rfc-editor.org/rfc/rfc9800	Primary standard Standards Track RFC Published: 2025	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.

10. Lineage, Review, and Publication Record

Record	Value
Original source file	RES-026_Segment_Routing_SRv6_Programmable_Path_Engineering.md
Original source words	1563
Upgrade type	Enterprise research report; source and freshness validation; limitations; adoption decision; reproducibility plan
Generated on	2026-07-22
Current status	Candidate Research Report
Publication authority	Formal Mythos approval not yet recorded
Next review	180 days or event-driven trigger, whichever occurs first