INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2025-2028

SG17-TD209/WP2

STUDY GROUP 17

Original: English

Question(s): 2/17 Geneva, 1-10 June 2026

TD

Source: Editor

Title: Agreement - XSTR.srsec: Security aspects of segment routing IPv6 for the convergence of computing and network for telecommunication operators

Contact: Chen Zhang
China Mobile
China
Tel: +86-0-13810642906
Fax: +86-10-52696688-3000
E-mail: zhangchen@cmdi.chinamobile.com

Contact: Gang Du
China Mobile
China
Tel: +86-0-13683558685
Fax: +86-10-52696688-3000
E-mail: dugang@cmdi.chinamobile.com

Contact: Yidi Xie
China Mobile
China
Tel: +86-0-13811473704
Fax: +86-10-52696688-3000
E-mail: xieyidi@cmdi.chinamobile.com

Abstract: This TD is the updated baseline text for XSTR.srsec: Security aspects of segment routing IPv6 for the convergence of computing and network for telecommunication operators. It is based on the discussion results of Q2/17 meeting on 5 June 2026.

C647 has been reviewed by Q2/17. According to comments made by delegates of Q2/17, several modifications were texted as following:

- Fix the typo of the title of the main body;
- Add a new abbreviation of IP;
- Delete the improper sentences to avoid misunderstanding in Summary and Clause 5;
- Furthermore, corresponded improvement was made in Summary also.

This TD of XSTR.srsec would be expected to be finalized and go for agreement in this meeting.

Draft Technical Report ITU-T XSTR.srsec

Error! Use the Home tab to apply TRtitle to the text that you want to appear here.

Summary

In order to effectively meet the diverse needs of different businesses, telecommunication operators have begun to use cloud computing and network virtualization technologies to implement the convergence of computing and network resources to optimize computing and network resources jointly. SRv6 (Segment Routing IPv6) can support the convergence of computing and network resources effectively. However, it brings security risks. It is necessary for telecommunication operators to identify and respond to the risks of SRv6 while taking advantage of it based on the outputs of SDOs and academies. ~~However, there is no related work. Therefore, a new work item as a technical report would be established to outline the security aspects of SRv6 for the convergence of computing and networks for telecommunication operators.~~

Keywords

Computing and network convergence, Segment Routing IPv6.

Draft Technical Report ITU-T XSTR.srsec

Security aspects of segment routing IPv6 for the convergence of computing and network for telecommunication operators

1 Scope

This report intends to identify the security risks of SRv6 in the convergence of computing and network resources for telecommunication operators. It outlines related technologies to help telecommunication operators to mitigate the security risks and enhance the security abilities.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), Framework of software-defined networking.

[ITU-T X.1038] Recommendation ITU-T X.1038 (2016), Security requirements and reference architecture for software-defined networking.

3 Terms and definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 Software-defined networking [ITU-T Y.3300]:

Software-defined networking (SDN) is a network management method that supports dynamic programmable network configuration. As such, it improves network performance and management efficiency, and enables network services to provide flexible customization capabilities like cloud computing. Decoupling the forwarding plane and control plane of network devices, SDN uses the controller for network device management, network service orchestration, and service traffic scheduling, which features low costs, centralized management, and flexible scheduling.

3.1.2 Network functions virtualization [b-ETSI GS NFV 003]:

Network functions virtualization (NFV) is a network architecture concept. Traditional network devices, such as routers, switches, firewalls, and load balancers, have their own hardware and software systems. Different from traditional devices, x86-based servers provide network functions after corresponding operating systems and software are installed. NFV uses the same architecture as that of x86-based servers. It decouples network functions from hardware, and instantiates them as independent software to run on general-purpose hardware.

3.1.3 Segment Routing IPv6 [b-IETF RFC 8986]:

Segment Routing IPv6 (SRv6) is a next-generation IP bearer protocol that combines Segment Routing (SR) and IPv6. Utilizing existing IPv6 forwarding technology, SRv6 implements network programming through flexible IPv6 extension headers. SRv6 reduces the number of required protocol types, offers great extensibility and programmability, and meets the diversified

requirements of more new services. It also provides high reliability and offers exciting cloud service application potential.

3.1.4 Multi-Protocol Label Switching [b-IETF RFC 3031]:

Multi-Protocol Label Switching (MPLS) is a protocol that uses labels to guide forwarding of data packets at a high speed over the IP backbone network. MPLS is a more efficient alternative to traditional IP routing and works by mapping an IP address to a short and fixed-length label of local significance, replacing IP table lookups with label swapping. In addition, MPLS labels can be used to establish a logical tunnel on the IP network.

3.2 Terms defined here

This Technical Report defines the following terms:

4 Abbreviations

IP	Internet Protocol
SDN	Software-Defined Networking
NFV	Network Function Virtualization
SRv6	Segment Routing IPv6
SID	Segment Identifier
SRH	Segment Routing Header
MPLS	Multi-Protocol Label Switching
SR-TE	Segment Routing Traffic Engineering
SR-BE	Segment Routing Best Effort
TLV	Type-Length-Value
BSID	Binding SID
LLDP	Link Layer Discovery Protocol
DDoS	Distributed Denial of Service
TCP	Transmission Control Protocol
PKI	Public Key Infrastructure
HMAC	Hash-based Message Authentication Code
BGP-SRv6	Border Gateway Protocol-Segment Routing Ipv6
MTD	Moving Target Defense

5 Introduction

With the development of digital economy in various countries, more and more enterprises are starting to embrace digital transformation. In order to effectively meet the diverse needs of different businesses, telecommunication operators have begun to optimize the computing and network resources jointly by converging computing and network resources using cloud computing and network virtualization technologies. The convergence of computing and network resources enables the integration of network-based technologies such as SDN (Software-Defined Networking) and

NFV (Network Function Virtualization) with cloud-based resources, creating an environment that is more flexible and adaptable to changing business needs.

SRv6 (Segment Routing IPv6) is a routing protocol that uses the source routing paradigm. In the source routing paradigm, the path of a packet is determined by the sender rather than by the routers in the network. SRv6 uses a new type of routing header, called a Segment Routing Header (SRH), which contains a list of segments, or instructions, that the packet must follow.

SRv6 plays an important role in the convergence of computing and network resources. Its three key functions are listed as follows:

- **Network slicing:** SRv6 allows for the creation of multiple, isolated virtual networks within a physical infrastructure, which can be used to provide different services to different customers or groups of customers.
- **Service Orchestration:** SRv6 can be used to support the virtualization of network functions, such as routers and firewalls, by allowing packets to be directed to specific virtual machines or containers.
- **Traffic Engineering:** SRv6 allows for more fine-grained control over the path that packets take through the network, which can be used to optimize network performance and reduce congestion.

~~Research and surveys indicate that SRv6 may introduce specific security risks while also enhancing existing security capabilities. Therefore, some technical work at ITU-T level would be meaningful.~~

6 Risks Analysis

The opportunities provided by SRv6 in the convergence of computing and network resources are listed as follows:

- **Strong scalability and programmability:** An SRv6 segment has 128-b~~B~~it programmable space, which well meets the diverse needs of network slicing and service orchestration.
- **Simplicity of service function chaining:** Compared with MPLS segment routing, SRv6 provides a stateless and underlay-agnostic service function chaining solution in service orchestration.
- **Cross-domain segment routing:** SRv6 supports multi-domain segment routing by using SR-TE (Segment Routing Traffic Engineering) and SR-BE (Segment Routing Best Effort). This feature helps operators perform computation and network resource orchestration on a large geospatial scale.
- **Enhance security capabilities:** SRv6 might strengthen the security capabilities for telecommunication operators, by supporting security orchestration, secured routing, subnetwork masking, etc.

The security risks for SRv6 in the convergence of computing and network resources are listed as follows, and Figure6-1 provides the location of risks in the network.

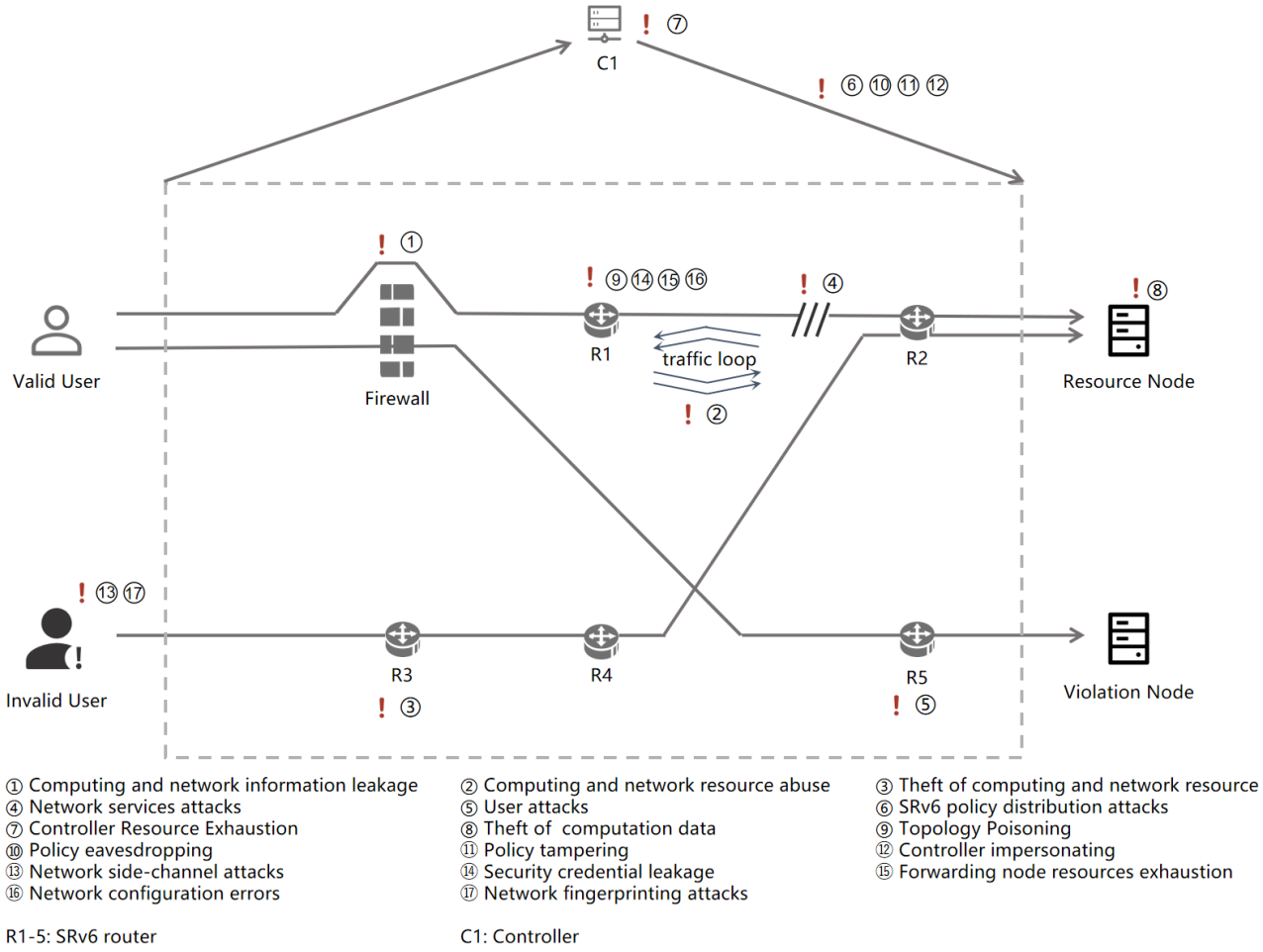

Figure 6-1 Location of risks for SRv6 in CNC

① **Computing and network information leakage:** By eavesdropping on segment routing information in SRv6 packets, an attacker can make inference of the topology of computing and network resources.

② **Computing and network resource abuse:** After an attacker obtains the network information, the attacker~~he~~ can abuse computing and network resources, by replaying or forging SRv6 packets.

③ **Theft of computing and network resource**: After intercepting the data packets, an attacker can forward the traffic to the specified node by modifying the last hop node of the SRv6 path, which will lead to the theft of traffic and loss of computing and network resources. In another case, an attacker can copy the SRv6 segment list and obtain unauthorized services illegally.

④ **Network service attacks:** An attacker can tamper with or forge SIDs in SRv6 packets to exploit vulnerabilities of network services in virtual machines or containers by invoking specific function code, and eventually the scheduling strategy fails and important services will be interrupted.

⑤ **User attacks:** An attacker can tamper with the SID in SRv6 packets to an unexpected or nonexistent address, preventing users from using computing and network resource.

⑥ **SRv6 policy distribution attacks:** When resource nodes are subjected to network attacks such as DDoS, the SDN controller distributes the near-source cleaning SRv6 policy to edge network devices, or when a forwarding node fails, the SDN controller reprograms the forwarding path and distributes the forwarding policy to the ingress device. An attacker can exploit the SRv6 policy distribution process to cooperate with other network attacks, thereby compromising the

network's security defense capabilities or rendering the SDN controller unable to dynamically allocate computing and network resources, ultimately leading to network stagnation.

⑦ **Controller Resource Exhaustion:** When an attacker has the ability to send data packets to forwarding devices, they can generate massive traffic from the forwarding devices to the SDN controller, exceeding the SDN controller's processing capacity in a short period. This eventually causes the SDN controller to overflow its memory, lose its ability to respond to other services, and simultaneously consume bandwidth resources between the SDN controller and the forwarding plane. For example, suppose the forwarding devices already have forwarding policies, an attacker can generate a large number of data packets with random characteristics that do not conform to the forwarding policies and send them to the forwarding devices. The forwarding devices will then package these data packets into Packet-in messages and send them to the SDN controller, thus creating a Packet-in storm.

⑧ **Theft of computation data:** When a user utilizes computing resources, they send sensitive data as input to the resource node. After the resource node completes the computation, the result is returned to the user. If an adversary intrudes into the network in advance and hijacks the resource node, sensitive input data, computation task context, and computation result may be stolen.

⑨ **Topology Poisoning:** The adversary causes the controller to collect incorrect network topology, making it unable to perform proper path planning. For example, an adversary that compromises a forwarding node in the network injects forged LLDP packets into the network. After receiving these forged LLDP packets, the controller mistakenly assumes that fake links or hosts exist in the network, thereby constructing a poisoned and incorrect global network topology graph, which may further result in path planning that traverses pre-controlled nodes by the adversary.

⑩ **Policy eavesdropping:** The policies issued by the controller to the forwarding plane carry core network configuration information. Attackers can eavesdrop on this type of traffic using methods such as network sniffing, and then analyze the SRv6 path planning, SID allocation, flow table rules, and other information contained in the traffic to obtain network topology, node deployment relationships, and traffic scheduling patterns for various services. Once this information is leaked, attackers will gain access to network defense vulnerabilities, facilitating malicious activities such as path tampering, traffic hijacking, and targeted DDoS attacks.

11 **Policy tampering:** An attacker can directly render security policies ineffective by intercepting or tampering with SRv6 policy commands sent from the controller to forwarding devices. For example, they can allow traffic carrying malicious code to bypass detection and be forwarded normally to the target node. They can also forge malicious routing policies and distribute them to all forwarding devices on the network, causing the network forwarding plane to execute data forwarding according to the forged policies. This can lead to traffic hijacking, redirecting legitimate business traffic to nodes controlled by the attacker, resulting in data leakage and service interruption.

12 **Controller impersonation~~ng~~:** An attacker forges their own address to resemble the address of the real controller configured on the switch, moves onto the communication path between the switch and the real controller, and then sends TCP reset packets to both the real controller and the switch. This disrupts communication between the real controller and the switch, allowing the fake controller to establish a new TCP connection with the switch. In this way, the fake controller convinces the network switches that it is the legitimate controller, sending them data plane traffic and accepting commands from the fake controller, thus disrupting or completely taking over the network.

13 **Network side-channel attacks:** Without requiring access rights to the packet payload, an

attacker could observe information leakage from packet-level characteristics. In timing analysis, an attacker could infer packet processing operations from differences in processing delays. For example, packets forwarded directly between ports would typically experience lower latency than those redirected to a controller. Such temporal differences could be exploited to determine whether the network is operating in a reactive or a proactive mode. In traffic pattern analysis, an attacker could also utilize packet structure to infer additional information about network devices. For example, by analyzing the distribution of packet sizes, the attacker could derive insights into device characteristics and network configuration.

14 **Security credential leakage:** To support user instances and resource virtualization, multiple logical forwarding instances exist on the forwarding device, each assigned independent identity identifier, key, certificate, and other security credentials for secure authentication and communication with the controller. If strict security isolation is not implemented between these logical forwarding instances, issues such as unauthorized access, unauthorized acquisition, or plaintext transmission may occur, ultimately leading to security credential leakage. Attackers can use the leaked credentials to forge legitimate identities, access the control plane, and launch further cyberattacks.

15 **Forwarding node resource~~s~~ exhaustion:** When the controller centrally controls the switch's forwarding rules, attackers can forge a large number of fake SRv6 flow establishment requests, triggering the controller to issue a large number of flow rules to the switch, rapidly consuming the switch's flow table storage resources. Similarly, attackers can exploit the programmable path feature of SRv6 to construct differentiated flow characteristics, circumventing the flow table aggregation mechanism and consuming flow table resources. Furthermore, once flow table resources are exhausted, legitimate SRv6 flow establishment requests will fail to generate forwarding rules and will be discarded, leading to network outages.

16 **Network configuration errors:** Conflicting flow tables configured in the forwarding nodes can lead to inconsistent network states. Conflicting, missing, or redundant flow table entries can cause the switch's actual forwarding behavior to deviate from the controller's intent. For example, the same traffic matching condition may correspond to different forwarding actions, or the switch may match traffic but not perform any action. When multiple switches' flow tables operate collaboratively, global logical conflicts can cause the overall network's operational state to deviate from its design intent. For example, cross-device traffic forwarding may form loops, or traffic may fail to reach its destination node.

17 **Network fingerprinting attacks:** In network environments where the controller centrally controls forwarding devices, distinct characteristics could be observed from an attacker's perspective. Detecting these fingerprint features can prepare for stealing network information. For example, an attacker can send forged packets representing a specific protocol to the network. If a response matching this protocol is received, the attacker can infer the communication protocol used in the network. For instance, the controller needs to periodically synchronize network state information with forwarding nodes. The traffic characteristics generated by this interaction can be detected by an attacker's sniffing attack. By comparing these traffic characteristics with specific protocols, the attacker can infer that the network uses an architecture such as SDN. For example, an attacker can analyze the SRH structure to derive characteristics associated with the SRv6 forwarding plane.

7 Security-enhancing features of SRv6

- **Programmable~~Editable~~ instruction:** SRv6 SID uses the programmable capability of IPv6 addresses to make the network functions expressed by instructions. In addition to identifying the node position in the SRv6 path, it can also identify the network function. By defining new instructions, new network functions can be deployed without modifying the protocol.
- **Programmable~~Editable~~ path:** SRv6 SRH specifies an IPv6 explicit path and stores IPv6 Segment List information. Segment List is an SRv6 path obtained by orderly arranging segments and network nodes. Segment List can be dynamically set and adjusted to control the forwarding path of data packets.
- **Programmable~~Editable~~ header:** Optional TLV in SRH supports network programming. When the data packet is transmitted in the network, the irregular information encapsulated in the forwarding plane can be processed by any node corresponding to the SID in the Segment List.
- **Cross-domain capability:** SRv6 has the characteristics of native IPv6 and can work based on IPv6 reachability. In cross-domain scenarios, cross-domain service deployment can be carried out by simply importing the IPv6 route of one domain into another domain. At the same time, the native IPv6 feature enables SRv6 to work based on aggregated routing. In large cross-domain scenarios, only limited aggregated routing table entries need to be configured at the border node.
- **Security policy orchestration:** SRv6 policy can allocate BSID to identify the entire SRv6 policy and provide traffic guidance and tunnel splicing functions. SRv6 policy belongs to the subscription and publication model. It subscribes to network security services according to service requirements, and then provides BSID to the service. With the centralized control capability of the controller, SRv6 policy is sent to the head node, which can realize the dynamic execution of network security policies.
- **Fast rerouting:** SRv6's end-to-end local protection mechanism enables rapid path switching in the event of a security breach or network failure. When a security threat or network failure occurs, nodes adjacent to the failure point can quickly switch to a pre-provisioned suboptimal backup path, and then gradually revert to the optimal path. This feature effectively safeguards the security of critical services and mitigates the further spread of security threats.
- **TLV-based security capabilities:** The TLV field in the SRH header has flexible security extension capabilities, which can encapsulate various security-related identifiers and verification information as needed. It supports custom security TLV types to carry exclusive security policies. TLVs can carry HMAC verification information, encryption algorithm identifiers, SID permission markers, etc., providing a basic carrier for identity authentication and integrity verification of data packets. At the same time, the type and length of TLVs are configurable, enabling information transmission in secure scenarios.
- **Controller path calculation:** The controller collects SRv6-related information in real time, including the entire network topology, link bandwidth and latency, node status and SID allocation, and SRH configuration, using protocols such as LLDP and BGP-SRv6, to construct a unified view of network resources and SRv6 parameters. Using this view, and combining it with service QoS requirements and security policy requirements, the controller plans the optimal SRv6 forwarding path using path calculation algorithms such as shortest path and load balancing. The path policy is then distributed to the head node, achieving centralized path planning and dynamic scheduling.
- **Topology verification:** SRv6 provides support for topology verification through its inherent path awareness, SID structure validation, and end-to-end forwarding consistency. The Segment List in SRH records the complete forwarding path of a packet, allowing the network to identify

whether the actual path is consistent with the intended path. The fixed format and hierarchical structure of SID enable forwarding nodes to validate the validity and legitimacy of path segments. By using these characteristics, SRv6 could assist to detect abnormal links, forged nodes, and inconsistent paths, thereby improving the reliability of network topology information.

- **Node protection:** When planning the primary path, the controller pre-calculates an independent backup segment list for each node based on the network topology. No node on the backup path has a direct adjacency with any node on the primary path. When a node triggers a security risk or hardware failure, its upstream node uses SRv6's local repair mechanism to invoke the pre-configured backup segment list to complete the path switchover, forwarding traffic to the backup path. This mechanism, through independent segment list planning, ensures that the backup segment list has no path overlap with the failed node.
- **Security risk identification and source tracing:** Leveraging the unique addressing of SRv6 SIDs and the scalability of SRH, source tracing SIDs are added during packet forwarding to record information such as the entry node, forwarding path, and service type of traffic, stored in the TLV. When network security anomalies occur, the source of traffic can be located by parsing the source tracing SIDs in the packets, providing data support for attack behavior analysis and handling.

8 Countermeasures

- **Prevention of computing and network information leakage:** The problem of SID confidentiality in the trusted domain needs to be solved. The SRv6 trusted domain has an independent address space. The information published in the domain cannot exceed the boundary of the SRv6 trusted domain. Information such as SID can only be published to the devices in the domain. When the data packet leaves the SRv6 trusted domain, it cannot carry the information in the domain.
- **Prevention of misuse of computing and network resource:** Whether the packet comes from a trusted source needs to be confirmed. The sender of the data packet enables HMAC TLV when encapsulating the data packet, including HMAC Key ID and HMAC verification code and other related information, and the network device enables the HMAC verification policy on the network interface. When the network device receives a data packet conforming to the policy, it verifies the HMAC value using a pre-shared secret key.
- **Prevention of computing and network resource theft:** It is necessary to ensure the security and credibility of the traffic. On the basis of ACL technology, filter rules are deployed on the edge of the network and internally, in detail: first, configure ACL rules on external interfaces, if the source address or destination address of the data packet is from the address block assigned the SID, it will be discarded; Second, configure ACL rules on internal interfaces, if the destination address of the SRv6 message is the local SID, but the source address is not in the trusted domain, it will be discarded; third, when the SRv6 node checks the data packet, only packet whose destination address is a local SID will be processed, others will be discarded.
- **Securing network services:** Payload information needs to be protected from tampering. Based on IPsec technology, use AH, ESP or a combination of both to verify data integrity.
- **Securing users:** While basic security technology is applied, hierarchical policy orchestration is required according to the sensitivity of users and services. Integrate security services with policy orchestration and establish a security service center. First, judge the type of current business traffic and the type of users, and then select an appropriate security policy, configure, deliver and start it, so as to improve the efficiency of security protection and CNC business.

- **Securing SRv6 network control plane policy delivery:** Encrypt the communication process and implement two-way authentication when the SDN controller delivers policies to devices. This communication process can be protected using the TLS protocol. Certificates are pre-installed on the controller and forwarding devices. When policy delivery is required, the certificates of both parties are authenticated first, and the policy is transmitted through an encrypted TLS tunnel.
- **Prevention of SRv6 network control plane resource exhaustion:** At the control plane, rate limiting is applied to specific traffic flows to ensure they do not exceed the SDN controller's processing capacity. Simultaneously, abnormal traffic is analyzed at the control plane; for example, IP blocking is implemented when large volumes of random-characteristic packets from the same IP address are detected.
- **Prevention of computation data leakage:** The PKI scheme is employed at the resource node, and a digital certificate is issued to each computing node. The computing task is only issued after the authentication process is completed. For sensitive data, Homomorphic Encryption and other technologies are used for data preprocessing, so that the data passing through the resource nodes is in an encrypted state during the computing process. The input data of large computing tasks is segmented, and each part is distributed to different resource nodes as input data for the computing tasks. Even if an attacker can obtain partial data, they will not be able to restore the original input data or obtain the complete computing results.
- **Prevention of topology poisoning:** To defend against topology poisoning attacks, operators should deploy authentication and verification mechanisms for topology discovery protocols. LLDP authentication validates the legitimacy of received LLDP packets during topology discovery, forwarding nodes verify packet integrity through a pre-shared key to reject forged link information. BGP-SRv6 anti-spoofing ensures the validity of node and SID information during control plane advertisement, forwarding nodes check the source legitimacy and prefix range of advertised information to filter fake entries. Dual topology verification cross-checks the topology information collected by the controller with actual network forwarding state before path computation, the controller compares path reachability and link status to identify and isolate abnormal topology data in a timely manner.
- **Periodic data statistics:** The controller uses a polling mechanism to obtain flow table statistics from the switch, including the number of matched packets, the number of bytes, the forwarding port, and the timeout period. This data is then aggregated by flow identifier to form a real-time traffic baseline. Through threshold comparison and rate mutation detection, abnormal behaviors such as abnormal surges/drops in flow table matches and unauthorized port traffic forwarding are identified. The controller collects link status information, cross-validates flow table forwarding anomalies with link connectivity, and detects topology changes caused by topology tampering and device malfunctions, thereby achieving anomaly awareness in network behavior and topology status.
- **Prevention of flow table resource exhaustion at forwarding nodes:** Employ SRv6 flow table intelligent aggregation technology, classifying flow rules based on hierarchical topology features and service attributes of SRv6 SIDs. Merge flow rules with the same forwarding path, similar SID prefixes, or originating services, simplifying matching fields and reusing forwarding actions to reduce resource consumption of flow table entries per traffic item and improve flow table utilization. Perform fine-grained flow table resource management in the SDN controller, pre-setting differentiated flow table resource allocation schemes based on service importance and historical traffic characteristics. Clearly define the flow table usage limits and priorities for various types of traffic to prevent malicious traffic or low-priority services from excessively preempting flow table resources.
- **Network configuration verification:** The controller collects network topology and flow rule information to check for issues with forwarding paths and flow rules. For example, verified

flow rules are treated as existing rules, while flow rules awaiting verification are treated as new rules. Before the flow rules are sent to the switch flow tables, the matching fields and execution actions of the new rules are compared with those of the existing rules to ensure that the new rules do not conflict with existing rules or network security policies, and that there are no loops or unreachable paths in the network topology.

- **Prevention of network fingerprinting attacks:** Embed custom identifiers in the SRH reserved fields to distinguish legitimate traffic from probe traffic. Ensure SRv6 path information is encrypted. Randomly fill optional fields in the SRH to make the header length and format random. The controller does not communicate with forwarding devices through fixed ports, but uses dynamic port mapping as an alternative. For commonly used ports of typical protocols, return randomized responses when probe packets are received, interfering with attackers' judgment of port attributes.

9 Security enabled by SRv6

- **Security service chain:** Operators can use SRv6 to dynamically create security service chains to ensure that traffic passes through multiple security services in a specified order, such as firewalls, DDoS protection. Due to the flexibility and programmability of SRv6, operators can dynamically adjust service chains according to real-time network conditions and security requirements, optimize the performance of security services, and improve the overall performance of the network.
- **Network traffic steering:** Network security services analyze and process network traffic to reduce network security risks. After the network security service processes the traffic, it is necessary to prevent the traffic from returning to the network security service or flowing to the wrong network location. Since SRv6 is based on Native IPv6, it has better scalability in traffic steering scenarios.
- **Service security isolation:** To provide business security and ensure exclusive business channels, the application of network slicing is gradually increasing. Taking advantage of the flexible and scalable characteristics of the SRv6 data plane, specific fields in the data packet are associated with the forwarding resources of the network slice to achieve service isolation and differentiated network service management.
- **Precise access control:** SRv6 can be combined with access control lists and security policies to achieve more refined access control. For example, path selection and security checks for each data packet. Operators can define complex access control policies based on service needs to ensure that only authenticated and authorized traffic can pass through, so that only legitimate users and devices can access specific resources, enhancing network security.
- **Security domain isolation:** SRv6 can help operators isolate and protect against internal network threats. SRv6 supports the creation of isolated domains in the internal network, and implements independent security policies for each domain. Traffic between different domains must undergo strict security checks to prevent the transfer and spread of security threats.
- **Joint MTD:** The centralized control of SDN and programmability of SRv6 facilitate the implementation of MTD policies. For example, the controller can implement IP address randomization policies, periodically assigning virtual IP addresses to internal servers, rendering information obtained by attackers through scanning ineffective. The controller can also implement path transformation policies, dynamically and randomly adjusting the transmission paths of traffic in the network, making it difficult for attackers to intercept traffic.
- **Conflict-free network configuration:** The controller orchestrates forwarding policies uniformly across all switches in the network. Based on the SRv6 path planning mechanism, it

generates exclusive and mutually exclusive flow table rules for different forwarding nodes. Before issuing policies, the controller verifies the global consistency of SID forwarding mapping relationships, flow table matching conditions, and actions to ensure that the SRv6 forwarding policies of each switch have no rule conflicts or path overlaps. The generated forwarding rules can be accurately mapped to the corresponding SID segments, avoiding traffic forwarding anomalies caused by policy conflicts.

- **Dynamic security policy enforcement:** The controller collects security event data from the forwarding plane, including port anomalies, flow table tampering, and traffic exceeding limits. It then normalizes and performs correlation analysis on events according to risk level. The controller pre-defines security policies and event types to form a mapping rule base. After matching event characteristics, the controller triggers the corresponding policy, issuing instructions such as flow table blocking, port blocking, and path rerouting to the forwarding plane. Simultaneously, it records the event handling process, supporting real-time feedback and dynamic optimization of policy execution effects.

Bibliography

[IETF RFC 8754] Filsfils, C., et al., "IPv6 Segment Routing Header (SRH)", RFC 8754, March 2020.

[IETF RFC 8986] Filsfils, C., et al., "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, February 2021.

[IETF RFC 3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[ETSI GS NFV 003] ETSI GS NFV 003 V1.6.1 (2021-01), "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[I-D.SPRING-SRV6-SEC] Buraglio, N., Mizrahi, T., Tian, T., Contreras, L.M., and F. Gont, "Segment Routing IPv6 Security Considerations", Work in Progress, Internet-Draft, draft-ietf-spring-srv6-security-14, 13 April 2026, https://datatracker.ietf.org/doc/html/draft-ietf-spring-srv6-security-14.

[I-D.YANG-VER] Yang, F., Zhang, X., Lin, C., and H. Zhang, "SRv6 Path Verification", Work in Progress, Internet-Draft, draft-yang-spring-srv6-verification-04, 11 February 2026, https://datatracker.ietf.org/doc/html/draft-yang-spring-srv6-verification-04.

[I-D.YANG-SID-SA] Yang, F. and C. Lin, "SID as source address in SRv6", Work in Progress, Internet-Draft, draft-yang-spring-sid-as-source-address-10, 19 March 2026, https://datatracker.ietf.org/doc/html/draft-yang-spring-sid-as-source-address-10.

[I-D.SPRING-PATHSEG] Li, C., Cheng, W., Zeng, G., Dhody, D., and Y. Zhu, "Path Segment Identifier (PSID) in SRv6", Work in Progress, Internet-Draft, draft-ietf-spring-srv6-path-segment-15, 2 March 2026, https://datatracker.ietf.org/doc/html/draft-ietf-spring-srv6-path-segment-15.

[Kreutz] Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., Uhlig, S., Software-defined networking: A comprehensive survey, Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, 2015.

_____