1 Configuration of SRv6 protocol on Nokia 7750 SR

Goal

The goal of this lab exercise is for students to familiarise themselves with Containerlab and some of its basic features, to gain hands-on experience in configuring high-performance network devices, specifically Nokia 7750 Service Routers, that are used in provider backbone networks, and to correctly and securely configure SRv6 protocol.

Equipment

A remote server running Linux 22.04 with installed Containerlab, prepared topology file, startup configuration files for some of the nodes, and other necessary files; A computer with PuTTY, that is used for accessing remote server via SSH.

Assignment

1. Access remote server, familiarise with Containerlab and deploy network.
2. Perform basic configuration of nodes.
3. Configure IS-IS protocol with all the necessary functionalities.
4. Successfully configure SRv6 protocol.

1.1 Theoretical introduction

1.1.1 SRv6

The Segment Routing over IPv6 (SRv6) is a framework used to carry network traffic across multiple nodes using SR tunnels. In SRv6, every node and its function are included in a list, also known as *Segment List* (SL), that defines the traffic path and operation performed on the traffic, as it traverses across the nodes. Thanks to its large programmability, by utilizing the IPv6 address space, the data is encapsulated and routed in a shortest-path manner. Nodes are identified by *Segment Identifiers* (SIDs) in the SRv6 network, that specify individual nodes and the data handling actions performed on each node. These identifiers are usually advertised by *Intermediate System to Intermediate System* (IS-IS) protocol, that is regularly used in conjunction with SRv6 protocol, creating the bottom layer or the underlying infrastructure for SRv6 protocol routing. Optionally, for more advanced use cases, SRv6 can integrate *Border Gateway Protocol* (BGP), that is, on the other hand, creating the upper layer for this protocol – also known as *Ethernet VPN* (EVPN). However, BGP configuration is not included in this lab exercise and only IS-IS protocol will be used.[1]

1.1.2 Segment Routing Header

The SRv6 protocol was created by combining Segment Routing technology and the IPv6 protocol. This combination is represented by a foundation on IPv6, extended with a new header. This header is called the *Segment Routing Header* (SRH), and the structure of the SRH can be seen in Fig.1.

The Segment Routing Header consists of multiple fields. The two most important of these are the *Segments Left* and *Segment List* fields. Segments Left points to the currently active Segment List field. The Segment List field is written in the form `Segment`

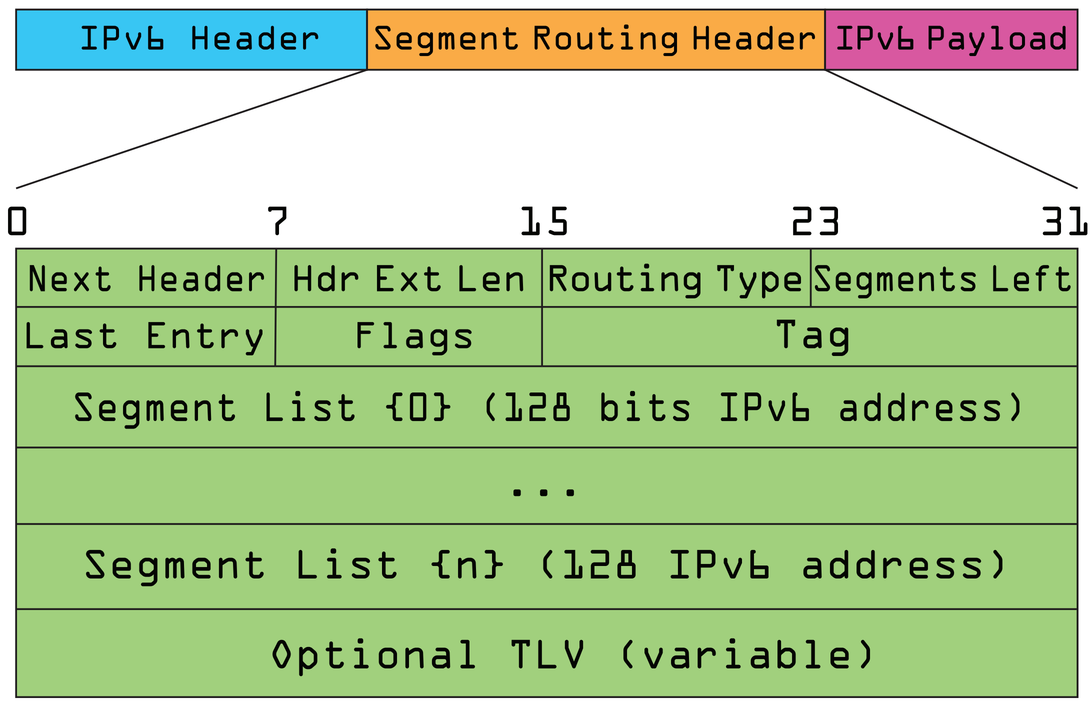

Figure 1: Segment Routing Header

`List[`n`]`, where n indicates the position where the Segment List is located. This field is in IPv6 address format, where each value of SL is SID, representing specific node and the processing of the packet performed by this node. A grouping of multiple Segment List fields forms a path, with the fields sorted in a stack where they are processed from bottom to the top. This processing is inverted compared to how MPLS – the SRv6 predecessor – is processing the labels.[2]

1.1.3 SRv6 routing

A group of nodes capable of SRv6 processing creates an SRv6 domain. In this domain, three types of nodes are specified – Source node, Transit node and End node. The source node encapsulates the information and sends it across the network, while transit node routes the information across multiple nodes and does not perform SRv6 processing. The end node, after receiving information, removes SRH header and processes the packet as specified. The focus of this exercise aims at the End nodes, how they process information and what functionalities need to be enabled, for the node to operate properly.

When reaching the final node, two modes of SRH removal exist. *Ultimate Segment Pop* (USP) and *Penultimate Segment Pop* (PSP). USP is used when router is the last segment of the list. This means that when the router is the last node of SRv6 domain, it removes the SRH and then the packet is routed as a plain IPv6 packet. PSP, on the other hand, removes SRH when the router is the penultimate segment in the segment list. By doing so, this helps to reduce computational load on the final node, where the penultimate nodes remove the SRH before forwarding the packet to the final node.[3, 4, 5]

1.1.4 IS-IS protocol

Intermediate System to Intermediate System protocol is a link-state, high-scalable dynamic routing protocol. This protocol operates on data link layer and is often deployed as an IGP on a large networks, thanks to its high scalability and the use of *Shortest Path First* (SPF) algorithm for path computation.

The IS-IS protocol allows further network segmentation using network areas, where each area is represented with unique ID. Subsequently, IS-IS supports a two-level hierarchical structure. Routers inside of an IS-IS network can be either Level 1, Level 2 or Level 1/2. Level 1 devices manage intra-area routing. Level 2 devices manage inter-area routing. Level 1/2 devices usually connect different areas and are contained in both Level 1 area and Level 2 area.[6]

1.1.5 Containerlab

Containerlab is a versatile network lab tool, that can be used to create different network topologies in a containerized environments. Users can create different network topologies that can be deployed as an interconnected Docker containers. Containerlab supports high variety of network devices from different vendors. This allows users to create plethora of topologies, interconnecting different network devices, while the hardware resource consumption is minimal.

The network topology is defined in a file with .clab.yml suffixes. This file contains specific devices used within topology and links interconnecting them. Additionally, management IP addresses, names of individual devices or startup configuration can be defined in this file.[7]

1.1.6 Nokia 7750 SR

Nokia 7750 Service Routers are primarily used in data centers, core and backbone networks or as a PE or peering routers.[8] With a wide range of routing capabilities, comprehensive technologies and mechanisms, advanced telemetry models and countless features, Nokia SRs are suitable for not only implementing SRv6 functionalities, but also for comparing the differences between standard and high-performance routers in terms of the configuration approach, overall ideology and philosophy they follow.

Because SRv6 requires some additional functionalities for it to work properly, these features are only implementable in a devices like Nokia 7750 Service Routers, or devices with similar processing capabilities and advanced networking features. The specific configuration features required for correct SRv6 configuration and processing are:

- *Port Cross-Connect* (PXC) configuration – specific ports, that internally loop SRv6 traffic, for correct management and policy application,
- *Forwarding Path Extension* (FPE) configuration – necessary to define internal logic and associations with PXC ports.

After correct implementation of aforementioned functionalities, the configuration of the SRv6 does not require additional specific services for it to operate properly.

1.2 Instructions

1.2.1 Initial deployment of network

1. Open program PuTTY and connect to remote server with IP address 192.168.200.3 via SSH.
2. Navigate to the folder `srv/srv6` and enter command `ls` to see all the files located in the folder.
3. Print out the contents of the `srv6.clab.yml` file to see the nodes used in the topology, their management IP addresses and other information. The network topology represented in the configuration file can be seen in Fig. 2

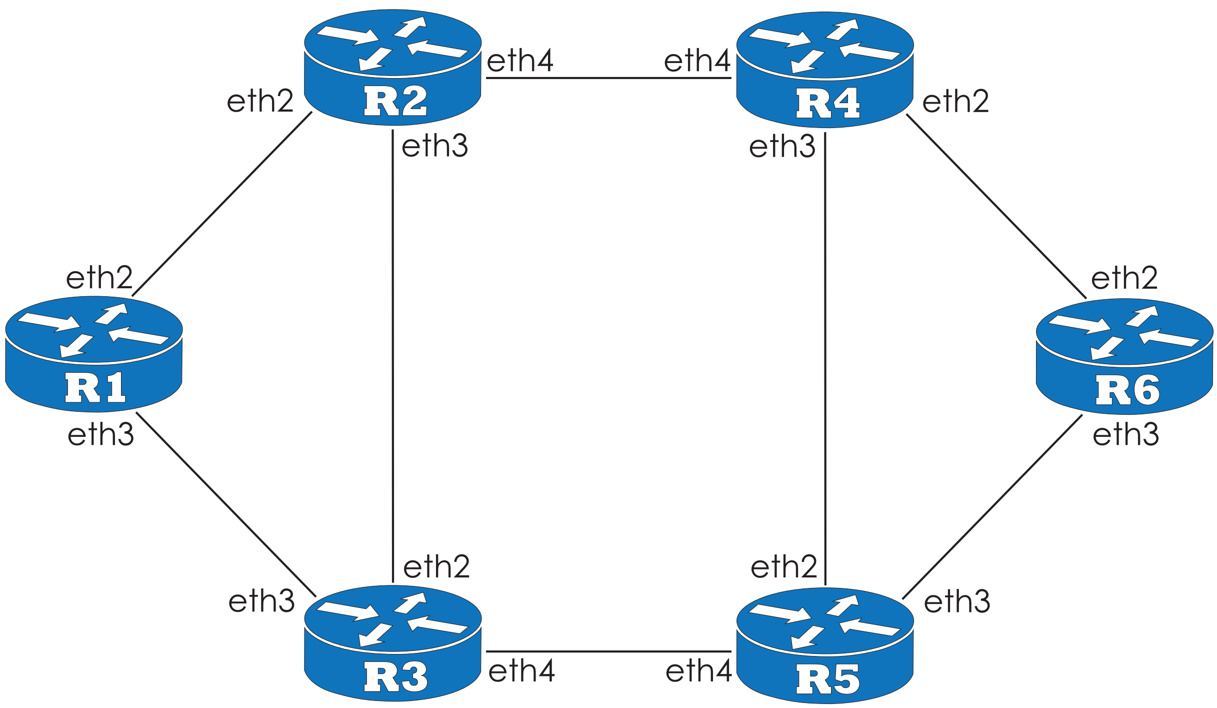

Figure 2: Defined Topology

4. As you can see, all the routers except for R1 and R6 are provided with startup configuration. Your task will be to configure the remaining routers.
5. To deploy the network, enter command `sudo clab deploy --topo srv6.clab.yml --network srv6-network`.
6. It takes around 3 minutes for the nodes to boot up. You can check their status by entering command `watch docker ps`. The nodes are ready, when their status is displayed as **healthy**.
7. Use command `ssh admin@clab-srv6-r1` to log into R1. For R6, use command `ssh admin@clab-srv6-r6`. The password is **admin**.

1.2.2 Basic configuration of nodes

1. Enter commands `edit-config exclusive` and `configure` to enter configuration context of the device.
2. The first step of configuration is to configure connectors into breakout mode, to create ports. Ethernet interfaces displayed in topology are mapped to connectors 1/1/c. Eth2, for example, is mapped to 1/1/c2 and eth3 is mapped to 1/1/c3. To create a specific port, for eth2, enter commands `port 1/1/c2`, `connector breakout c1-100g` and `admin-state enable`. This creates port 1/1/c2/1, that can be assigned to interfaces with speed 100 Gb and enables the port.
3. To return back to the configuration context, use command `exit` or `back`. To return back to the exclusive configuration mode, keyboard shortcut `Ctrl+Z` can be used.
4. Repeat the process for eth3.
5. Nokia 7750 SR saves uncommitted changes in a candidate configuration. To apply these changes, use command `commit`. The uncommitted changes are indicated by a star sign in the CLI. If a mistake is noticed before committing changes, enter command `discard` to delete uncommitted changes.
6. Verify the configuration with command `show port`. You should see both ports, 1/1/c2/1 and 1/1/c3/1 having both admin state and port state as **Up**.
7. Repeat the process for R6.
8. Now the ports need to be assigned with IP addresses. The address space for R1 and R6 can be seen below:

R1

Interface	IPv4 Address	IPv6 Address	Link-local
Eth2	172.16.0.1/30	2001:db8:acad:0::1/64	fe80::1:2
Eth3	172.16.0.5/30	2001:db8:acad:1::1/64	fe80::1:3
Loopback	172.16.0.101/32	2001:db8:acad:f::1/128	
System	1.1.1.1/32		

Router ID: 1.1.1.1 **IP-prefix:** 2001:db8:aaaa:101::/64

R6

Interface	IPv4 Address	IPv6 Address	Link-local
Eth2	172.16.0.26/30	2001:db8:acad:6::2/64	fe80::6:4
Eth3	172.16.0.30/30	2001:db8:acad:7::2/64	fe80::6:5
Loopback	172.16.0.106/32	2001:db8:acad:f::6/128	
System	6.6.6.6/32		

Router ID: 6.6.6.6 **IP-prefix:** 2001:db8:aaaa:106::/64

9. Execute command `router "Base"` to enter base routing instance of the router.
10. From here, command `interface eth2` creates virtual interface named "eth2". Then to configure eth2 interface properly, enter command `port 1/1/c2/1` to assign cre-

ated port to this interface. Command `ipv4 primary address 172.16.0.1 prefix-length 30` assigns IPv4 address to this interface. Afterwards, command `ipv6 address 2001:db8:acad:0::1 prefix-length 64` assigns IPv6 address. By entering command `ipv6 link-local-address address fe80::1:2`, a link-local address is assigned. **Do not forget** to apply the changes and enable the interface.

11. Repeat the process for eth3 interface.
12. For loopback, create interface named “lo0”. The configuration process is the same, except instead of command `port x/x/x/x`, enter command `loopback`. This specifies, that the interface is indeed loopback.
13. System interface already exist. Simply enter its configuration context and assign IPv4 address and enable the interface.
14. Router ID is assigned by command `router-id 1.1.1.1`.
15. Repeat the configuration for the R6 router.
16. Check the configuration by entering command `show router interface`. For R1, the output of this command should match the following output:

```
(ex)[/configure router "Base"]
A:admin@r1# show router interface

===========================================================================
Interface Table (Router: Base)
===========================================================================
Interface-Name                   Adm       Opr(v4/v6)  Mode    Port/SapId
   IP-Address                                                  PfxState
---------------------------------------------------------------------------
eth2                             Up        Up/Up       Network 1/1/c2/1
   172.16.0.1/30                                               n/a
   2001:db8:acad::1/64                                         PREFERRED
   fe80::1:2/64                                                PREFERRED
eth3                             Up        Up/Up       Network 1/1/c3/1
   172.16.0.5/30                                               n/a
   2001:db8:acad:1::1/64                                       PREFERRED
   fe80::1:3/64                                                PREFERRED
lo0                              Up        Up/Up       Network loopback
   172.16.0.101/32                                             n/a
   2001:db8:acad:f::1/128                                      PREFERRED
   fe80::e00:bcff:fe01:eb00/64                                 PREFERRED
system                           Up        Up/Down     Network system
   1.1.1.1/32                                                  n/a
---------------------------------------------------------------------------
Interfaces : 4
===========================================================================
```

17. Verify, that the R6 router is also configured correctly.

1.2.3 IS-IS configuration

1. To begin the configuration of an IS-IS protocol, enter the configuration context of IS-IS with command `router isis`.
2. Firstly you need to correctly configure interfaces. Enter the configuration context of eth2 interface and type commands `level-capability 2`, `interface-type point-to-point`, `ipv6-unicast` and `admin-state enable`. These commands set the interface to level 2, simplify the exchange of Hello messages by specifying there is only one router on the other end of the link, and enable the interface to participate in both IPv6 routing and in IS-IS routing.
3. Repeat the same process for eth3 interface.
4. For loopback interface, the configuration process is the same, except for command `interface-type point-to-point`, which is not used.
5. Interface "system" needs to be also assigned to level 2 and enabled. Additionally, command `passive` on this interface needs to be entered. This prevents interface from sending Hello messages to try to form adjacencies, but still allows it to advertise its presence and be available across the domain.
6. Verify the configuration with command `info`, running it from the IS-IS configuration context. The output on R1 router should be following:

```
(ex)[/configure router "Base" isis 0]
A:admin@r1# info
    interface "eth2" {
        admin-state enable
        interface-type point-to-point
        ipv6-unicast true
        level-capability 2
    }
    interface "eth3" {
        admin-state enable
        interface-type point-to-point
        ipv6-unicast true
        level-capability 2
    }
    interface "lo0" {
        admin-state enable
        ipv6-unicast true
        level-capability 2
    }
    interface "system" {
        admin-state enable
        passive true
        level-capability 2
    }
```

7. Configure the router R6 in the same way and remember to **commit the changes**.
8. The MD5 authentication is enabled by executing commands `authentication-type`

message-digest and authentication-key secret-isis-key. These commands enable MD5 authentication and define key "secret-isis-key" to be used to authenticate. Generally, devices need to use the same key, otherwise they are not able to communicate. Make sure to configure the same key on router R6.

9. Configure additional IS-IS features by executing commands area-address 49.00, level-capability 2 and ipv6-routing-native. This assigns router to IS-IS area 49.00, specifies the router as level 2 router and enables the support for IPv6 routing within the IS-IS protocol.
10. Next, to enable advertisement of router capabilities within area, enter command advertise-router-capabilities area.
11. Enable use of wide metrics within level 2, for more precise control of link metrics by issuing commands level 2 and wide-metrics-only. Enter command router-id x.x.x.x within IS-IS configuration context, to set router ID for IS-IS instance. Match the IS-IS instance router ID with the router ID you have configured before. Use the same values, as specified in the address space above.
12. To configure traffic engineering, enter command traffic-engineering to enable it, traffic-engineering-options to enter traffic engineering configuration context, and commands ipv6 and application-link-attributes. These two commands enable TE for IPv6 and advertisement of TE attributes.
13. Make sure to apply these commands also to the R6 router.
14. Issue command advertise-passive-only. This ensures, that only passive interfaces will be advertised within an IS-IS.
15. Execute command loopfree-alternate and from within this context, enter commands remote-lfa and ti-lfa. These commands enable mechanisms, that provide quick network convergence in case an error occurs, and provide backup paths independently of network topology.
16. Commit the changes and apply these command to R6.
17. Verify the configuration by entering commands show router route-table, where you should see **9 routes**. 5 routes should be **Remote** and the remaining routes should be **Local**.
18. You can verify your configuration by entering command info within an IS-IS configuration context.
19. To verify the IS-IS configuration, enter command show router isis status. The printout on R1 should be similar to the printout below:

```
(ex)[/configure router "Base" isis 0]
A:admin@r1# show router isis status
=================================================================
Rtr Base ISIS Instance 0 Status
=================================================================
ISIS Cfg System Id           : 0000.0000.0000
ISIS Oper System Id          : 0010.0100.1001
ISIS Cfg Router Id           : 1.1.1.1
ISIS Oper Router Id          : 1.1.1.1
------OUTPUT OMITTED------
```

```
Admin State                  : Up
Oper State                   : Up
Ipv4 Routing                 : Enabled
Ipv6 Routing                 : Enabled, Native
Mcast Ipv4 Routing           : Enabled, Native
Mcast Ipv6 Routing           : Enabled, Native
Last Enabled                 : 05/19/2024 22:50:35
Level Capability             : L2
Authentication Check         : True
Auth Keychain                : Disabled
Authentication Type          : MD5
------OUTPUT OMITTED------
Loopfree-Alternate           : Enabled
Remote-LFA                   : Enabled
Max PQ Cost                  : 4261412864
Remote-LFA (node-protect)    : Disabled
Max PQ nodes (node-protect)  : 16
Augment-route-table          : Disabled
TI-LFA                       : Enabled
------OUTPUT OMITTED------
```

20. Verify, that the R6 router is also configured correctly.

1.2.4 SRv6 configuration

1. There are two functionalities, that need to be configured before SRv6 – PXC ports and FPE. To configure first PXC port, start with commands `configure port-xc` and `pxc 1`. These commands enter configuration mode of PXC and create first PXC with value 1. Enter commands `port-id 1/1/c1/1` and `admin-state enable` to allocate port 1/1/c1/1 to PXC 1 and administratively enable the port.
2. Enter configuration context of port 1/1/c1, create a port 1/1/c1/1 with speed 100 Gb and enable it.
3. Enter configuration context of port 1/1/c1/1 and apply commands `ethernet dot1x tunneling` and `ethernet mode hybrid`. Do not forget to enable the port. These commands ensure correct data flow across logical subports, because each PXC subport is tagged with an internal VLAN tag invisible to the user, but necessary for traffic management.
4. Enter configuration context of port pxc-1.a and enable it. Repeat for pxc-1.b.
5. Repeat the previous steps for PXC 10, with port 1/1/c10/1 and subports pxc-10.a and pxc-10.b.[1]
6. Verify the configuration by entering command `show port`, where you should see all four subinterfaces. Also, you should see ports 1/1/c1/1 and 1/1/c10/1 in Port Mode **Hybrid** and Port Encapsulation should be **Dot1q**.

[1] It is not necessary to choose these ports specifically. Any unused physical port can be used for this configuration.

7. To configure FPE, enter command `configure fwd-path-ext` to enter FPE configuration mode.
8. Afterwards, enter command `fpe 1` which creates FPE with identifier 1. By entering command `path pxc 1`, PXC 1 is associated with FPE 1. Execute commands `application srv6 type origination`, `application srv6 interface-a` and `application srv6 interface-b`. These commands define FPE 1 to be used for origination of SRv6 traffic and specify, which logical interfaces are going to be used to handle SRv6 processing.
9. Repeat the process for FPE 10, assign PXC 10 to FPE 10, and instead of origination type, enter command `application srv6 type termination`. The rest of the configuration is the same.
10. Apply the same configuration to R6 router.
11. Configuration is verified by executing commands `show fwd-path-ext fpe 1` and `show fwd-path-ext fpe 10`. FPE 1 should have SRv6 Type **origination** and Path **pxc 1** displayed. FPE 10 should have **termination** SRv6 type and Path **pxc 10** assigned. Both FPE 1 and FPE 10 should have Segment-Routing V6 **enabled** and Operation state as **up**.
12. Verify the configuration of R6 router with the same commands.
13. To enter SRv6 configuration context, enter command `configure router "Base" segment-routing segment-routing-v6`.
14. Issue command `locator r1_loc` to create SRv6 locator named "r1_loc".
15. From within locator configuration context, execute commands `block-length 48` and `function-length 20`. These commands reserve 48 bits from SRv6 locator for network identification and 20 bits for specific functions. Additionally, command `prefix ip-prefix 2001:db8:aaaa:101::/64` assigns specific SRv6 prefix to the node.
16. Administratively enable the locator and enter command `termination-fpe 10`, that assigns termination FPE to locator "r1_loc".
17. Return back to SRv6 configuration context and run commands `origination-fpe 1` and `source-address 2001:db8:acad:f::1`. These commands assign loopback address of the router, to be used as source address of SRv6 traffic and enable FPE 1 to be used for SRv6 traffic originating from within the node.
18. Apply the same configuration to R6 router. Create locator "r6_loc" and assign IP prefix address and source address from table displayed above.
19. Verify the configuration using command `info`, where the output of R1 router should be as seen below:

```
(ex)[/configure router "Base" segment-routing segment-routing-v6]
A:admin@r1# info
    origination-fpe [1]
    source-address 2001:db8:acad:f::1
    locator "r1_loc" {
        admin-state enable
        block-length 48
        function-length 20
        termination-fpe [10]
        prefix {
            ip-prefix 2001:db8:aaaa:101::/64
        }
    }
```

20. Now to configure End function, first enter command `base-routing-instance locator "r1_loc"` from within SRv6 configuration context.
21. To specify End function with identificator 1 and USP mode, execute command `function end 1 srh-mode usp`.
22. End.X function needs to be configured for the router to be able to identify other nodes and propagate SID. Command `function end-x-auto-allocate srh-mode usp protection protected` enables this propagation with USP mode and *Loop Free Alternate* (LFA) protection, therefore providing backup routes in case of link failure.
23. Apply this configuration also within R6 router.
24. To configure additional level capabilities and metrics, enter IS-IS configuration context and issue command `segment-routing-v6`. Here enable locator advertisement and enter command `locator r1_loc` to enter configuration context of locator within IS-IS.
25. Issue commands `level-capability 2`, `level 1 delete metric` and `level 2 metric 10`. This enables the locator advertisement only within IS-IS level 2 and sets the metric of locator to 10.
26. Configure router R6 in a similar way.
27. Verify the configuration with commands `show router segment-routing-v6 local-sid`, where on both routers, you should see **three functions**. One End function and two End.X functions. By executing commands `show router tunnel-table ipv6` and `show router route-table ipv6 2001:db8:aaaa::/48 longer`, you should see the locators of the other nodes.
28. Verify the configuration within R6 router.
29. If the configuration is correct, enter command `logout`, to exit the router CLI. Then from `/srv6` folder, enter command `containerlab destroy` to tear down topology. Additionally remove *clab-srv6* folder and *.srv6.clab.yml.bak* file.

1.3 Control questions

1. What information is typically contained in a .clab.yml file?
2. What is the purpose of `commit` command in Nokia 7750 SR CLI?
3. What is the difference between port 1/1/c2 and 1/1/c2/1?
4. Explain the difference between USP and PSP modes in SRv6.
5. Why do you need to configure PXC ports?

1.4 Symbols and abbreviations

BGP	Border Gateway Protocol
EVPN	Ethernet Virtual Private Network
FPE	Forwarding Path Extension
IGP	Interior Gateway Protocol
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
LFA	Loop Free Alternate
MD5	Message-Digest Algorithm 5
MPLS	Multiprotocol Label Switching
PE	Provider Edge
PSP	Penultimate Segment Pop
PXC	Port Cross-Connect
SID	Segment Identifier
SL	Segment List
SPF	Shortest Path First
SRH	Segment Routing Header
SRv6	Segment Routing over IPv6
SSH	Secure Shell
TE	Traffic Engineering
USP	Ultimate Segment Pop

1.5 Bibliography

[1] NOKIA. *Segment Routing over IPv6*. Online. C2024. Available from: `https://documentation.nokia.com/acg/23-10-2/books/classic-cli-part-i/c233-seg-rout-ipv6.html`. [viewed 2024-05-23].

[2] ZHANG, Yan. *What Is SRv6?* Online. C2023. Available from: `https://info.support.huawei.com/info-finder/encyclopedia/en/SRv6.html`. [viewed 2023-05-24].

[3] HUAWEI TECHNOLOGIES CO. *Understanding Segment Routing IPv6*. Online. C2023. Available from: `https://support.huawei.com/enterprise/en/doc/EDOC1000173015/d169625f/understanding-segment-routing-ipv6`. [viewed 2023-05-24].

[4] FILSFILS, Clarence et al. *IPv6 Segment Routing Header (SRH)*. Online. 2020. Available from: `https://datatracker.ietf.org/doc/rfc8754/`. [viewed 2023-05-24].

[5] LI, Zhenbin; HU, Zhibo and LI, Cheng. *SRv6 Network Programming: Ushering in a New Era of IP Networks*. CRC Press, 2021. ISBN 978-1-032-01624-5.

[6] HUAWEI TECHNOLOGIES CO. *What Is IS-IS?* Online. 2023. Available from: `https://info.support.huawei.com/info-finder/encyclopedia/en/IS-IS.html`. [viewed 2024-05-24].

[7] CONTAINERLAB. *Containerlab*. Online. [2024]. Available from: `https://containerlab.dev/`. [viewed 2024-05-24].

[8] NOKIA CORPORATION. *7750 Service Router*. Online. C2024. Available from: `https://www.nokia.com/networks/ip-networks/7750-service-router/`. [viewed 2024-05-24].