7450 Ethernet Service Switch
7750 Service Router
7950 Extensible Routing System
Virtualized Service Router

Release 26.3.R1

Services Configuration Quick Reference Guide

3HE 22324 AAAA TQZZA 01
Edition: 01
March 2026

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Table of contents

List of tables **6**

List of figures **7**

1 Getting started **8**
1.1 About this guide 8
1.2 Conventions 8
1.2.1 Precautionary and information messages 8
1.2.2 Options or substeps in procedures and sequential workflows 9
1.3 SR OS service configuration 10
1.4 Topology 10
1.5 Containerlab reference 11
1.6 MD-CLI command reference 11

2 Management IP address **13**

3 Hardware configuration **14**

4 Ports and interfaces **15**

5 Underlay routing **16**
5.1 IGP - OSPF 16
5.2 IGP - IS-IS 16
5.3 BGP 16

6 Transport protocol **18**
6.1 LDP 18
6.2 RSVP-TE 18
6.3 Segment routing 19
6.4 SR-TE 19

7 ACL **20**

8 QoS **21**

8.1 Classification....21
8.2 Queuing....22
8.3 Scheduling....22
8.4 Remarking....23

9 Service components....24
9.1 SAP....24
9.2 SDP....25

10 Epipe....26

11 VPLS....28

12 VPRN....30

13 IES....34

14 EVPN-VPWS....37

15 EVPN-MPLS with multihoming....40

16 Show commands....43
16.1 Hardware and system....43
16.2 Port and interfaces....43
16.3 OSPF....44
16.4 IS-IS....45
16.5 BGP....45
16.6 LDP....46
16.7 RSVP-TE....46
16.8 Segment routing....47
16.9 SR-TE....47
16.10 ACL....47
16.11 QoS....48
16.12 Services general....48
16.13 Epipe....49
16.14 VPLS....49
16.15 VPRN....49

16.16 IES 50
16.17 EVPN-VPWS 50
16.18 EVPN-MPLS 51

List of tables

Table 1: Commonly used MD-CLI commands..... 12

List of figures

Figure 1: Scope of services configuration and show command examples in this guide..... 10
Figure 2: Topology used for configuration examples..... 11
Figure 3: IPv4 addressing used for configuration examples.....11
Figure 4: Epipe topology used in this example..... 26
Figure 5: VPLS topology used this example..... 28
Figure 6: VPRN topology used in this example.....30
Figure 7: IES topology used in this example.....34
Figure 8: EVPN-VPWS topology used in this example..... 37
Figure 9: EVPN-MPLS topology used in this example..... 40

1 Getting started

1.1 About this guide

This guide provides the basic, step-by-step configuration required to set up services on the following Nokia routers:

- 7450 ESS
- 7750 SR
- 7950 XRS
- Virtualized Service Router (VSR)

Required feature sets for each service type are described with configuration examples in this guide; related **show** commands that you can use to view and verify specific configuration information are included in Show commands.

Use this guide as a one-stop reference for basic service configuration. Where applicable, links to the SR OS customer documentation are provided in this guide for additional reading.

This guide does not provide detailed information about service types and is not intended to replace the SR OS customer documentation listed in the *7450 ESS, 7750 SR, and 7950 XRS Guide to Documentation*. For detailed information about service features and options, see the SR OS customer documentation WebHelp or the Nokia Doc Center.

This guide is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.

Command outputs shown in this guide are examples only; actual displays may differ depending on supported functionality and user configuration.

Note: This guide generically covers Release 26.*x*.R*x* content and may contain some content that will be released in later maintenance loads. For information about features supported in each load of the Release 26.*x*.R*x* software or for a list of unsupported features by platform and chassis, see the *SR OS R26.x.Rx Software Release Notes*, part number 3HE 29176 000*x* TQZZA.

1.2 Conventions

This section describes the general conventions used in this guide.

1.2.1 Precautionary and information messages

The following information symbols are used in the documentation.

DANGER: Danger warns that the described activity or situation may result in serious personal injury or death. An electric shock hazard could exist. Before you begin work on this equipment,

be aware of hazards involving electrical circuitry, be familiar with networking environments, and implement accident prevention procedures.

WARNING: Warning indicates that the described activity or situation may, or will, cause equipment damage, serious performance problems, or loss of data.

Caution: Caution indicates that the described activity or situation may reduce your component or system performance.

Note: Note provides additional operational information.

Tip: Tip provides suggestions for use or best practices.

1.2.2 Options or substeps in procedures and sequential workflows

Options in a procedure or a sequential workflow are indicated by a bulleted list. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform one of the listed options to complete the step.

Example: Options in a procedure

1. User must perform this step.
2. This step offers three options. User must perform one option to complete this step.
   - This is one option.
   - This is another option.
   - This is yet another option.

Substeps in a procedure or a sequential workflow are indicated by letters. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform two substeps (a. and b.) to complete the step.

Example: Substeps in a procedure

1. User must perform this step.
2. User must perform all substeps to complete this action.
   a. This is one substep.
   b. This is another substep.

Nested substeps within a procedure or a sequential workflow are indicated by roman numerals. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform two substeps (a. and b.) to complete the step. At substep b, the user must perform two additional substeps (i. and ii.) to complete the step.

Example: Nested substeps in a procedure

1. User must perform this step.
2. User must perform all substeps to complete this action.
   a. This is one substep.
   b. User must perform all nested substeps to complete this action.

i. This is a nested substep.

ii. This is another nested substep.

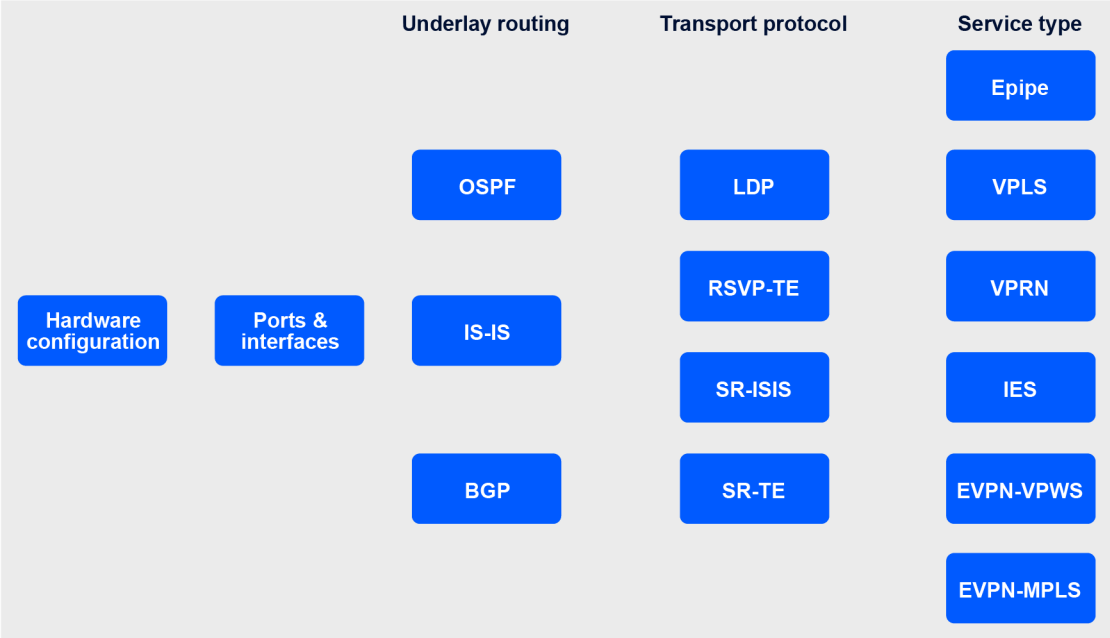
1.3 SR OS service configuration

Unless otherwise indicated, this guide uses MD-CLI command syntax. Required feature sets for each service type are described with configuration examples; related **show** command examples are described in Show commands. All configuration examples shown in this guide are in the MD-CLI full context format. The reference chassis used is the 7750 SR-1, and the software version is SR OS Release 25.7.R1. Use the `show system info` command to verify the chassis model and software version of your router.

The following figure shows the services for which basic step-by-step configurations and **show** command examples are described in this guide.

Note: This figure does not represent a comprehensive list of all features and associated options available for services on the SR OS. For detailed information about supported service features and options, see the SR OS customer documentation WebHelp or the Nokia Doc Center.

Figure 1: Scope of services configuration and show command examples in this guide

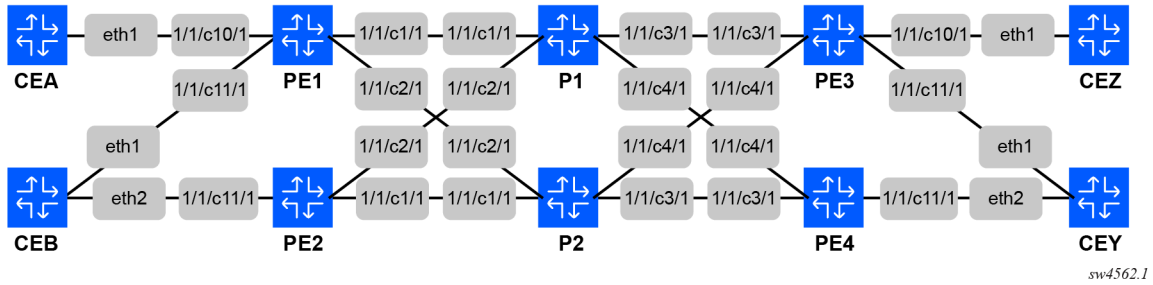


1.4 Topology

The following figure shows the topology used for the configuration examples in this guide. The topology consists of four Provider Edge (PE) routers, two Provider (P) routers, and four Customer Edge (CE)

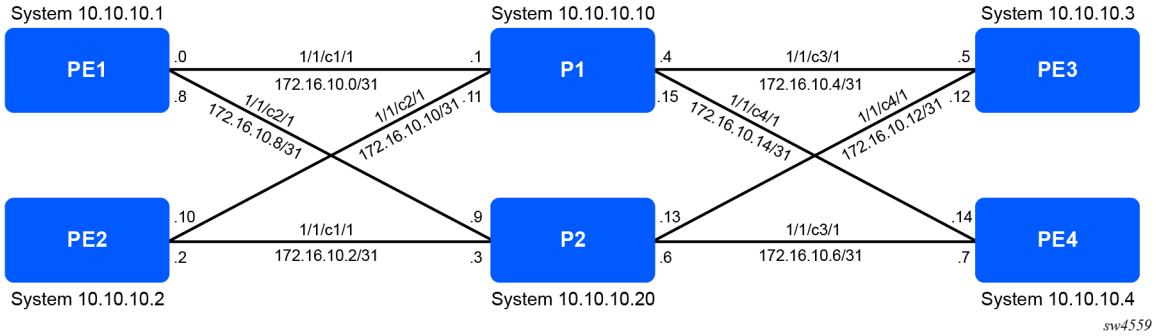
routers. All configuration examples in this guide are specific to PE routers. For configuration on other routers, see their containerlab startup configuration files for details.

Figure 2: Topology used for configuration examples



The following figure shows the IPv4 addressing used for the configuration examples in this guide.

Figure 3: IPv4 addressing used for configuration examples



1.5 Containerlab reference

All configuration used in this guide, along with complete working configurations for the reference topology, are available for deployment in Containerlab at https://github.com/nokia/sros-docs-lab.

Note: A license is required for SR OS node deployment. Contact your Nokia account representative to obtain the necessary license required to proceed with deployment.

1.6 MD-CLI command reference

The following table lists the MD-CLI commands commonly used in this guide. For a complete list of SR OS CLI trees and command descriptions, see *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI Command Reference Guide*. For a comparison of the SR OS MD-CLI with those used by other OS, see *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI Quick Reference Guide*.

Table 1: Commonly used MD-CLI commands

Action	Command
Enter private candidate mode	**configure private**
Commit configuration changes	**commit**
Delete configuration elements	**delete** *command path*
Discard configuration changes	**discard**
Compare candidate to running	**compare** */*
View configuration in current context	**info**
View configuration in full context format	**info full-context**
View full configuration of router	**admin show configuration**
Search for keyword in output	*command* **| match** *keyword*
Find a command	**tree flat detail | match** *keyword*
Exit candidate mode	**exit**
Exit the router	**logout**

2 Management IP address

Configure the management IP address to allow remote access for configuration and management purposes using an in-band or out-of-band management port on the device.

See Ports and Interfaces for information about configuring IP address on the in-band management port.

Perform the following steps to configure IP address on the out-of-band management port of the device.

1. Enter the BOF configuration context.

```
bof private
```

2. Configure the management IP.

```
/bof router "management" interface "management" cpm active ipv4 ip-address 172.20.20.2
/bof router "management" interface "management" cpm active ipv4 prefix-length 24
/bof router "management" interface "management" cpm active ipv6 ipv6-address
 3fff:172:20:20::2
/bof router "management" interface "management" cpm active ipv6 prefix-length 64
```

3. Configure static routes for management access, if required.

```
/bof router "management" static-routes route 0.0.0.0/0 next-hop 172.20.20.1
```

4. Commit the configuration changes, and exit the BOF configuration context.
5. To view the full BOF configuration, use the following command.

```
admin show configuration bof
```

3 Hardware configuration

If you are starting with a new router, configure the cards as described in this chapter before proceeding with the peering configuration. If you have already completed this step, skip this section and continue with the configuration.

The card and MDA types depend on the variant of the 7750 SR in use. Use the `show card state` command to display the equipped card and MDA types.

The topology in this guide uses the 7750 SR-1, which is a fixed form factor chassis that does not require any additional hardware configuration.

For modular systems, complete the following configuration to bring up the line card modules. This example configuration applies to the 7750 SR-2se. Choose the correct card type and level for your chassis.

See Hardware and system for information about applicable hardware **show** commands.

Configure the power modules:

```
/configure chassis router chassis-number 1 power-shelf 1 power-shelf-type ps-a4-shelf-dc
/configure chassis router chassis-number 1 power-shelf 1 power-module 1 power-module-type ps-a-
dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 2 power-module-type ps-a-
dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 3 power-module-type ps-a-
dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 4 power-module-type ps-a-
dc-6000
```

Configure the fabric cards:

```
/configure sfm 1 sfm-type sfm-2se
/configure sfm 2 sfm-type sfm-2se
/configure sfm 3 sfm-type sfm-2se
/configure sfm 4 sfm-type sfm-2se
```

Configure the line card:

```
/configure card 1 card-type xcm-2se
/configure card 1 mda 1 mda-type x2-s36-800g-qsfpdd-12.0t

# On systems with XIOM:
/configure card 1 card-type xcm-2se
/configure card 1 xiom "x1" xiom-type x2-s36-800g-qsfpdd-6.0t
/configure card 1 xiom "x1" mda 1 mda-type m36-800g-qsfpdd
```

4 Ports and interfaces

The physical port is configured first, followed by an interface with an IPv4 or IPv6 address.

Each port acts as a "connector" and supports breakout functionality. You must first configure the breakout type used on the connector, which then allows you to configure the individual breakout ports.

All ports have an associated port mode. Network-facing ports in the base routing instance should operate in the "network" mode (default). Client-facing ports used in a service should be in "access" mode. If a port is both network- and client-facing, it can be set to "hybrid" mode. The minimum encapsulation required on a hybrid port is dot1q.

See Port and interfaces for information about the relevant port, interfaces, and BFD **show** commands.

In the following example, the connector is configured to use a 1x100G breakout.

```
/configure port 1/1/c1 admin-state enable
/configure port 1/1/c1 connector breakout c1-100g
/configure port 1/1/c1/1 admin-state enable
/configure port 1/1/c1/1 description "To P1"
```

In the following example, a client-facing port is configured in "access" mode with dot1q encapsulation.

```
/configure port 1/1/c10 admin-state enable
/configure port 1/1/c10 connector breakout c4-10g
/configure port 1/1/c10/1 admin-state enable
/configure port 1/1/c10/1 ethernet mode access
/configure port 1/1/c10/1 ethernet encap-type dot1q
/configure port 1/1/c10/1 ethernet mtu 5000
```

As shown in the following example, the core-facing interface is given a name and IP address, and associated with a physical port.

```
/configure router "Base" interface "To-P1" port 1/1/c1/1
/configure router "Base" interface "To-P1" ipv4 primary address 172.16.10.0 prefix-length 31
```

The `system` interface refers to the loopback interface of the router, such as lo0 or loopback0. This interface name cannot be modified. If a router ID is not explicitly configured, the `system` interface IPv4 address is used. The `system` interface should be assigned a /32 IP address.

```
/configure router "Base" interface "system" ipv4 primary address 10.10.10.1 prefix-length 32
```

BFD can be enabled on an interface for both IPv4 and IPv6. In SR OS, BFD is enabled once under the interface,where the timers are also configured. The BFD state is shared with various protocols running over that interface by enabling **bfd-liveness** for each protocol.

```
/configure router "Base" interface "To-P1" ipv4 bfd admin-state enable
```

Use the following command to enable BFD state sharing on OSPF.

```
/configure router ospf area 0 interface "To-P1" bfd-liveness remain-down-on-failure true
```

5 Underlay routing

This section provides configuration examples for underlay routing. All sample configurations in this section are specific to the PE1 router.

5.1 IGP - OSPF

This example configures an OSPFv2 neighbor. The port and interface configuration is similar to that shown in Ports and interfaces. OSPF is assigned a higher preference value, so that IS-IS is preferred in the topology.

See "Configuring OSPF" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide* for detailed information about OSPF configuration.

See OSPF for information about relevant OSPF **show** commands.

```
/configure router "Base" ospf 0 admin-state enable
/configure router "Base" ospf 0 preference 20
/configure router "Base" ospf 0 area 0.0.0.0 interface "To-P1" interface-type point-to-point
/configure router "Base" ospf 0 area 0.0.0.0 interface "system" interface-type point-to-point
```

5.2 IGP - IS-IS

This example configures the router as an IS-IS Level 1 and 2 (default). The port and interface configuration is similar to that described in Port and interfaces.

See "Configuring IS-IS" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide* for detailed information about IS-IS configuration.

See IS-IS for information about relevant IS-IS **show** commands.

```
/configure router "Base" isis 0 admin-state enable
/configure router "Base" isis 0 area-address [49.0000]
/configure router "Base" isis 0 interface "To-P1" interface-type point-to-point
/configure router "Base" isis 0 interface "system" interface-type point-to-point
```

5.3 BGP

In this example, BGP is used to advertise the VPN-IPv4 address family for the VPRN service and the EVPN address family for the EVPN-MPLS service. The following applies:

- only PE1 and PE3 will participate in VPRN service
- all four PEs will participate in EVPN-MPLS service

See "BGP" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide* for detailed information about BGP configuration.

See BGP for information about relevant BGP **show** commands.

```
/configure router "Base" bgp router-id 10.10.10.1
/configure router "Base" bgp group "pe" peer-as 64500
/configure router "Base" bgp neighbor "10.10.10.2" group "pe"
/configure router "Base" bgp neighbor "10.10.10.2" family evpn true
/configure router "Base" bgp neighbor "10.10.10.3" group "pe"
/configure router "Base" bgp neighbor "10.10.10.3" family vpn-ipv4 true
/configure router "Base" bgp neighbor "10.10.10.3" family evpn true
/configure router "Base" bgp neighbor "10.10.10.4" group "pe"
/configure router "Base" bgp neighbor "10.10.10.4" family evpn true
```

6 Transport protocol

This section provides transport protocol configuration examples. All sample configurations in this section are specific to the PE1 router.

6.1 LDP

In this example, LDP is enabled for use as a transport tunnel for services.

See "Label Distribution Protocol" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR MPLS Guide* for detailed information about LDP configuration.

See LDP for relevant information about LDP **show** commands.

```
/configure router "Base" ldp interface-parameters interface "To-P1" ipv4 admin-state enable
/configure router "Base" ldp interface-parameters interface "To-P2" ipv4 admin-state enable
```

6.2 RSVP-TE

In this example, RSVP-TE is enabled for use as a transport tunnel for services.

See "MPLS and RSVP" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR MPLS Guide* for detailed information about RSVP configuration.

See RSVP-TE for information about relevant MPLS and RSVP **show** commands.

Configure RSVP-TE:

```
/configure router "Base" rsvp admin-state enable
/configure router "Base" rsvp interface "To-P1" { }
/configure router "Base" rsvp interface "To-P2" { }
/configure router "Base" rsvp interface "system" { }
```

Configure MPLS:

```
/configure router "Base" mpls admin-state enable
/configure router "Base" mpls interface "To-P1" { }
/configure router "Base" mpls interface "To-P2" { }
/configure router "Base" mpls interface "system" { }
```

Configure MPLS LSP:

```
/configure router "Base" mpls path "loose" admin-state enable
/configure router "Base" mpls path "loose" hop 1 ip-address 10.10.10.10
/configure router "Base" mpls path "loose" hop 1 type strict
/configure router "Base" mpls lsp "lsp-to-R3" admin-state enable
/configure router "Base" mpls lsp "lsp-to-R3" type p2p-rsvp
/configure router "Base" mpls lsp "lsp-to-R3" to 10.10.10.3
```

```
/configure router "Base" mpls lsp "lsp-to-R3" path-computation-method local-cspf
/configure router "Base" mpls lsp "lsp-to-R3" { primary "loose" }
```

6.3 Segment routing

In this example, SR-MPLS is configured over IS-IS (SR-ISIS). SR OS also supports SR-OSPF.

See "Segment routing with MPLS data plane" in the *7750 SR and 7950 XRS Segment Routing and PCE User Guide* for detailed information about SR-MPLS configuration.

See Segment routing relevant information about the SR-MPLS **show** commands.

Configure the MPLS label range for segment routing:

```
/configure router "Base" mpls-labels sr-labels start 21000
/configure router "Base" mpls-labels sr-labels end 22000
```

Configure segment routing for IS-IS:

```
/configure router "Base" isis 0 advertise-router-capability as
/configure router "Base" isis 0 traffic-engineering true
/configure router "Base" isis 0 segment-routing admin-state enable
/configure router "Base" isis 0 segment-routing prefix-sid-range global
/configure router "Base" isis 0 interface "system" ipv4-node-sid index 1
```

6.4 SR-TE

SR-TE can be used to build LSPs similar to RSVP-TE.

See "SR-TE MPLS support" in the *7750 SR and 7950 XRS Segment Routing and PCE User Guide* for detailed information about SR-TE configuration.

See SR-TE for relevant SR-TE **show** commands.

This example configures a SR-TE LSP using loose hops, which allows IGP path selection.

```
/configure router "Base" mpls path "loose" admin-state enable
/configure router "Base" mpls lsp "lsp-sr-te-R3" admin-state enable
/configure router "Base" mpls lsp "lsp-sr-te-R3" type p2p-sr-te
/configure router "Base" mpls lsp "lsp-sr-te-R3" to 10.10.10.3
/configure router "Base" mpls lsp "lsp-sr-te-R3" path-computation-method local-cspf
/configure router "Base" mpls lsp "lsp-sr-te-R3" primary "loose" { }
```

7 ACL

ACL filter policies, also referred to as Access Control Lists (ACLs) or just "filters", are sets of ordered rule entries that specify packet match criteria and actions to be performed to a packet upon a match. Filter policies are created with a unique filter ID and filter name. After the filter policy is created, the policy must be associated with services.

See "Filter policies" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide* for detailed information about ACL.

See the applicable section for each service type for examples of applying ACL to that specific service type.

See ACL for information about relevant ACL **show** commands.

The following is an example of an IPv4 ACL.

```
/configure filter ip-filter "Epipe-ACL" filter-id 101
/configure filter ip-filter "Epipe-ACL" entry 10 match protocol icmp
/configure filter ip-filter "Epipe-ACL" entry 10 match dst-ip address 192.168.10.2
/configure filter ip-filter "Epipe-ACL" entry 10 match dst-ip mask 255.255.255.255
/configure filter ip-filter "Epipe-ACL" entry 10 action accept
```

The ACL is applied to the service SAP in either ingress or egress direction.

```
/configure service epipe "Epipe-VLAN100" sap 1/1/c10/1:100 ingress filter ip "Epipe-ACL"
```

8 QoS

SR OS implements Quality of Service (QoS) with a four-step process: classification, queueing, scheduling, and (re)marking.

QoS policies can be applied under the following contexts:

- SAP ingress (for traffic ingressing a service)
- SAP egress (for traffic egressing a service)
- network ingress (for traffic ingressing a network-facing port or uplink)
- network egress (for traffic egressing a network-facing port or uplink)

See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide* for detailed information about QoS configuration.

8.1 Classification

At service ingress, classification is configured in a `sap-ingress` policy.

```
/configure qos sap-ingress "CE-ingress-QoS" dscp cs1 fc "af"
```

The `sap-ingress` policy is applied to the service SAP.

```
/configure service epipe "Epipe-VLAN100" sap 1/1/c10/1:100 ingress qos sap-ingress policy-name
 "CE-ingress-QoS"
```

At network ingress, classification is configured in a `network` policy.

```
/configure qos network "Network-QoS" policy-id 10
/configure qos network "Network-QoS" ingress dscp cs1 fc af
/configure qos network "Network-QoS" ingress dscp cs1 profile in
/configure qos network "Network-QoS" ingress lsp-exp 6 fc h1
/configure qos network "Network-QoS" ingress lsp-exp 6 profile in
```

The network classification policy is applied to the network-facing interface.

```
/configure router "Base" interface "To-P1" qos network-policy "Network-QoS"
```

See the relevant section for each service type for examples of applying QoS classification to that specific service type.

8.2 Queuing

At service ingress, queuing is configured in a **sap-ingress** policy.

```
/configure qos sap-ingress "CE-ingress-QoS" policy-id 11
/configure qos sap-ingress "CE-ingress-QoS" queue 2 rate pir 100
/configure qos sap-ingress "CE-ingress-QoS" queue 2 rate cir 100
/configure qos sap-ingress "CE-ingress-QoS" fc "af" queue 2
/configure qos sap-ingress "CE-ingress-QoS" fc "af" profile in
```

At service egress, queuing is configured in a **sap-egress** policy.

```
/configure qos sap-egress "CE-egress-QoS" policy-id 12
/configure qos sap-egress "CE-egress-QoS" queue 3 rate pir 100
/configure qos sap-egress "CE-egress-QoS" queue 3 rate cir 100
/configure qos sap-egress "CE-egress-QoS" fc be queue 3
```

Both **sap-ingress** and **sap-egress** policies are applied under the service SAP.

```
/configure service epipe "Epipe-VLAN100" sap 1/1/c10/1:100 ingress qos sap-ingress policy-name
 "CE-ingress-QoS"
/configure service epipe "Epipe-VLAN100" sap 1/1/c10/1:100 egress qos sap-egress policy-name
 "CE-egress-QoS"
```

At network ingress and egress, queuing is configured in a **network-queue** policy.

```
/configure qos network-queue "Network-queue" fc af queue 3
/configure qos network-queue "Network-queue" fc ef queue 2
/configure qos network-queue "Network-queue" queue 2 rate pir 15
/configure qos network-queue "Network-queue" queue 2 rate cir 10
/configure qos network-queue "Network-queue" queue 3 rate pir 10
/configure qos network-queue "Network-queue" queue 3 rate cir 5
```

For ingress network queueing, the queuing policy is applied under the FP context of the line card.

```
/configure card 1 fp 1 ingress network queue-policy "Peering-Queue"
```

For egress network queuing, the queuing policy is applied under the physical port.

```
/configure port 1/1/c1/1 ethernet network egress queue-policy "Network-queue"
```

8.3 Scheduling

This example shows a simple port-based scheduler that can be applied to schedule traffic out of a network-facing port. SR OS also supports hierarchical schedulers and slope policies.

Similar policies can also be applied under a `sap-egress` policy to schedule multiple traffic types at service egress.

```
/configure qos port-scheduler-policy "simple-scheduler" max-rate 100000000
/configure qos port-scheduler-policy "simple-scheduler" level 1 rate pir 90
/configure qos port-scheduler-policy "simple-scheduler" level 1 rate cir 10
```

```
/configure qos port-scheduler-policy "simple-scheduler" level 6 rate pir max
/configure qos port-scheduler-policy "simple-scheduler" level 6 rate cir max
/configure qos port-scheduler-policy "simple-scheduler" level 7 rate pir max
/configure qos port-scheduler-policy "simple-scheduler" level 7 rate cir max
/configure qos port-scheduler-policy "simple-scheduler" level 8 rate pir max
/configure qos port-scheduler-policy "simple-scheduler" level 8 rate cir max
```

The port-based scheduler policy is applied to the physical port.

```
/configure port 1/1/c1/1 ethernet egress port-scheduler-policy policy-name "simple-scheduler"
```

8.4 Remarking

At service egress, remarking is configured in the `sap-egress` policy.

```
/configure qos sap-egress "CE-egress-QoS" fc be dscp in-profile cp31
/configure qos sap-egress "CE-egress-QoS" fc be dscp out-profile cp31
/configure qos sap-egress "CE-egress-QoS" fc af dscp in-profile cs4
/configure qos sap-egress "CE-egress-QoS" fc af dscp out-profile cs4
```

The `sap-egress` policy is applied under the service SAP context.

```
/configure service epipe "Epipe-VLAN100" sap 1/1/c10/1:100 egress qos sap-egress policy-name
 "CE-egress-QoS"
```

At network egress, remarking is configured in the `network` policy.

```
/configure qos network "Network-QoS" egress fc be lsp-exp-in-profile 0
/configure qos network "Network-QoS" egress fc be lsp-exp-out-profile 0
/configure qos network "Network-QoS" egress fc af dscp-in-profile cs1
/configure qos network "Network-QoS" egress fc h1 lsp-exp-in-profile 6
```

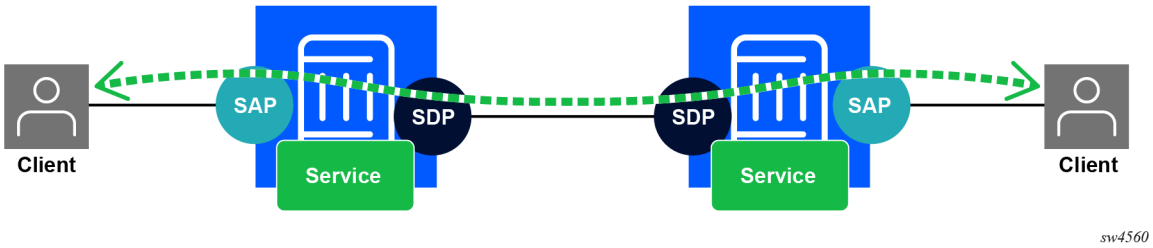
The remarking policy is applied under the interface.

```
/configure router "Base" interface "To-P1" qos network-policy "Network-QoS"
```

See QoS for information about relevant QoS **show** commands.

9 Service components

The following figure shows the logical entities used by a service model in SR OS to construct a service.



In the preceding figure:

- The Service Access Point (SAP) identifies the customer-facing interface with null, dot1, or qinq encapsulation.
- The Service Distribution Point (SDP) is the unidirectional transport tunnel that connects services between two routers. SDPs can use GRE, LDP, RSVP-TE, or segment routing tunnels. SDP is independent of service or type of service. Multiple services, whether of the same or different type, can share the same SDP. In such cases, traffic for each service is separated using a unique `vc-id`, which is defined when the SDP is attached to a service.

For services that use BGP for transport signalling (such as VPRN, EVPN, VPLS), the SDP configuration can be replaced with the `auto-bind` feature. This allows the router to select from a variety of tunnel types.

9.1 SAP

A SAP is a client-facing interface and is the ingress point of the packets that will be carried over a service to the remote destination.

To configure a port as a SAP, set the Ethernet mode of the port to either `access` or `hybrid`. If necessary, set the required Ethernet encapsulation and MTU.

Note: In the `hybrid` mode, minimum encapsulation is dot1q.

```
/configure port 1/1/c10/1 admin-state enable
/configure port 1/1/c10/1 ethernet mode access
/configure port 1/1/c10/1 ethernet encap-type dot1q
/configure port 1/1/c10/1 ethernet mtu 5000
```

SAPs are configured within a service configuration context.

```
/configure service epipe "Epipe-VLAN100" sap 1/1/c10/1:100
```

9.2 SDP

An SDP is a unidirectional transport tunnel used to carry one or more services. SDP is identified by a numerical ID.

Before configuring an SDP, configure the transport protocol that the SDP will use: GRE, LDP, RSVP-TE, SR, SR-TE.

The following example creates an SDP on PE1 to PE3 that will use LDP.

```
/configure service sdp 510 admin-state enable
/configure service sdp 510 delivery-type mpls
/configure service sdp 510 ldp true
/configure service sdp 510 far-end ip-address 10.10.10.3
```

The association of the service with the SDP is configured under the **service** context. The SDP ID is used along with a unique **vc-id**, which is used to identify the service on the remote end. An MPLS label, generated for each unique **vc-id**, is used as the service label in MPLS encapsulation.

```
/configure service epipe "Epipe-VLAN100" spoke-sdp 510:100
```

10 Epipe

An Epipe service is a Layer 2 point-to-point service that encapsulates and transports customer data across a service provider's IP or MPLS network. This service is completely transparent to the customer data and protocols. The Epipe service does not perform any MAC learning. A local Epipe service comprises two SAPs on the same node, whereas a distributed Epipe service consists of two SAPs on different nodes. SDPs are not used in local Epipe services.

See "Ethernet pipe service" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide* for detailed information about Epipe.

See Epipe for information about relevant **show** commands.

The following figure shows the Epipe topology used in this example.

Figure 4: Epipe topology used in this example

An Epipe will be created to establish communication between the two CE devices. LDP will be used as the tunneling protocol.

See LDP for information about LDP configuration.

Configuration

CE-facing port configuration on PE1 and PE3:

```
/configure port 1/1/c10/1 admin-state enable
/configure port 1/1/c10/1 ethernet mode access
/configure port 1/1/c10/1 ethernet encap-type dot1q
/configure port 1/1/c10/1 ethernet mtu 5000
```

SDP configuration on PE1:

```
/configure service sdp 510 admin-state enable
/configure service sdp 510 delivery-type mpls
/configure service sdp 510 ldp true
/configure service sdp 510 far-end ip-address 10.10.10.3
```

SDP configuration on PE3:

```
/configure service sdp 511 admin-state enable
/configure service sdp 511 delivery-type mpls
/configure service sdp 511 ldp true
/configure service sdp 511 far-end ip-address 10.10.10.1
```

ACL configuration on PE1:

```
/configure filter ip-filter "Epipe-ACL" filter-id 101
```

```
/configure filter ip-filter "Epipe-ACL" entry 10 match protocol icmp
/configure filter ip-filter "Epipe-ACL" entry 10 match dst-ip address 192.168.10.2
/configure filter ip-filter "Epipe-ACL" entry 10 match dst-ip mask 255.255.255.255
/configure filter ip-filter "Epipe-ACL" entry 10 action accept
```

Epipe configuration on PE1:

```
/configure service epipe "Epipe-VLAN100" admin-state enable
/configure service epipe "Epipe-VLAN100" description "Epipe-CEA1-VLAN100-CEZ1-VLAN100"
/configure service epipe "Epipe-VLAN100" service-id 10
/configure service epipe "Epipe-VLAN100" customer "1"
/configure service epipe "Epipe-VLAN100" spoke-sdp 55:100 { }
/configure service epipe "Epipe-VLAN100" sap 1/1/c10/1:100 ingress qos sap-ingress policy-name
 "CE-ingress-QoS"
/configure service epipe "Epipe-VLAN100" sap 1/1/c10/1:100 ingress filter ip "Epipe-ACL"
/configure service epipe "Epipe-VLAN100" sap 1/1/c10/1:100 egress qos sap-egress policy-name
 "CE-egress-QoS"
```

Epipe configuration on PE3:

```
/configure service epipe "Epipe-VLAN100" admin-state enable
/configure service epipe "Epipe-VLAN100" description "Epipe-CEA1-VLAN100-CEZ1-VLAN100"
/configure service epipe "Epipe-VLAN100" service-id 10
/configure service epipe "Epipe-VLAN100" customer "1"
/configure service epipe "Epipe-VLAN100" spoke-sdp 511:100 { }
/configure service epipe "Epipe-VLAN100" sap 1/1/c10/1:100 { }
```

See QoS for information about respective QoS configuration.

Customer verification

Login to CEA:

```
docker exec -it cea bash
```

Ping CEZ VLAN 100 from CEA:

```
└──> ping -c 100 -Q 34  192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
64 bytes from 192.168.10.2: icmp_seq=1 ttl=64 time=10.3 ms
64 bytes from 192.168.10.2: icmp_seq=2 ttl=64 time=5.03 ms
64 bytes from 192.168.10.2: icmp_seq=3 ttl=64 time=5.07 ms

--- 192.168.10.2 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 5.030/6.805/10.316/2.482 ms
```

While the ping is in progress, check the SAP, ACL, and QoS statistics.

11 VPLS

VPLS is a class of virtual private network service that allows the connection of multiple sites in a single bridged domain over a provider-managed IP/MPLS network. The customer sites in a VPLS instance appear to be on the same LAN, regardless of their location. VPLS uses an Ethernet interface on the customer-facing (access) side, which simplifies the LAN/WAN boundary and allows rapid and flexible service provisioning.

A VPLS service provides connectivity between two or more SAPs on one (local service) or more (distributed service) service routers. To the customer sites, the connection appears to be a bridged domain, allowing protocols (including routing protocols) to traverse the VPLS service.

See "Virtual Private LAN Service" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide* for detailed information about VPLS.

The following figure shows the VPLS topology used in this example.

Figure 5: VPLS topology used this example

A VPLS service will be created to establish communication between the two clients. RSVP-TE LSP will be used as the tunnelling protocol.

See RSVP-TE for information about relevant LSP configuration.

See VPLS for information about relevant VPLS **show** commands.

Configuration

CE-facing port configuration on PE1 and PE3:

```
/configure port 1/1/c10/1 admin-state enable
/configure port 1/1/c10/1 ethernet mode access
/configure port 1/1/c10/1 ethernet encap-type dot1q
/configure port 1/1/c10/1 ethernet mtu 5000
```

SDP configuration on PE1:

```
/configure service sdp 520 admin-state enable
/configure service sdp 520 description "RSVP to PE3"
/configure service sdp 520 delivery-type mpls
/configure service sdp 520 far-end ip-address 10.10.10.3
/configure service sdp 520 lsp "lsp-to-R3" { }
```

SDP configuration on PE3:

```
/configure service sdp 521 admin-state enable
/configure service sdp 521 description "RSVP to PE1"
/configure service sdp 521 delivery-type mpls
```

```
/configure service sdp 521 far-end ip-address 10.10.10.1
/configure service sdp 521 lsp "lsp-to-R1" { }
```

MAC ACL filter configuration on PE1

In this example, we will use a MAC ACL.

```
/configure filter mac-filter "VPLS-MAC-Filter" filter-id 1021
/configure filter mac-filter "VPLS-MAC-Filter" entry 10 match src-mac address aa:c2:ab:00:02:02
/configure filter mac-filter "VPLS-MAC-Filter" entry 10 match src-mac mask ff:ff:ff:ff:ff:ff
/configure filter mac-filter "VPLS-MAC-Filter" entry 10 action accept
```

VPLS service configuration on PE1:

```
/configure service vpls "VPLS-VLAN200" admin-state enable
/configure service vpls "VPLS-VLAN200" description "VPLS-CEA-VLAN200-CEZ-VLAN200"
/configure service vpls "VPLS-VLAN200" service-id 20
/configure service vpls "VPLS-VLAN200" customer "1"
/configure service vpls "VPLS-VLAN200" spoke-sdp 520:200 { }
/configure service vpls "VPLS-VLAN200" sap 1/1/c10/1:200 ingress qos sap-ingress policy-name
 "CE-ingress-QoS"
/configure service vpls "VPLS-VLAN200" sap 1/1/c10/1:200 ingress filter mac "VPLS-MAC-Filter"
/configure service vpls "VPLS-VLAN200" sap 1/1/c10/1:200 egress qos sap-egress policy-name "CE-
egress-QoS"
```

VPLS service configuration on PE3:

```
/configure service vpls "VPLS-VLAN200" admin-state enable
/configure service vpls "VPLS-VLAN200" description "VPLS-CEA-VLAN200-CEZ-VLAN200"
/configure service vpls "VPLS-VLAN200" service-id 20
/configure service vpls "VPLS-VLAN200" customer "1"
/configure service vpls "VPLS-VLAN200" spoke-sdp 521:200 { }
/configure service vpls "VPLS-VLAN200" sap 1/1/c10/1:200 { }
```

Customer verification

Login to CEA:

```
docker exec -it cea bash
```

Ping CEZ VLAN 200 from CEA:

```
└──> ping -c 100 -Q 34  192.168.20.2
PING 192.168.20.2 (192.168.20.2) 56(84) bytes of data.
64 bytes from 192.168.20.2: icmp_seq=1 ttl=64 time=10.7 ms
64 bytes from 192.168.20.2: icmp_seq=2 ttl=64 time=5.51 ms
64 bytes from 192.168.20.2: icmp_seq=3 ttl=64 time=5.44 ms

--- 192.168.20.2 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99151ms
rtt min/avg/max/mdev = 4.583/5.901/14.539/1.815 ms
```

While the ping is in progress, check the SAP, ACL, and QoS statistics.

12 VPRN

Virtual Private Routed Network (VPRN), commonly referred to as VRF, is a method of distributing routing information using BGP and MPLS to forward data, providing a Layer 3 Virtual Private Network (VPN) service to end customers.

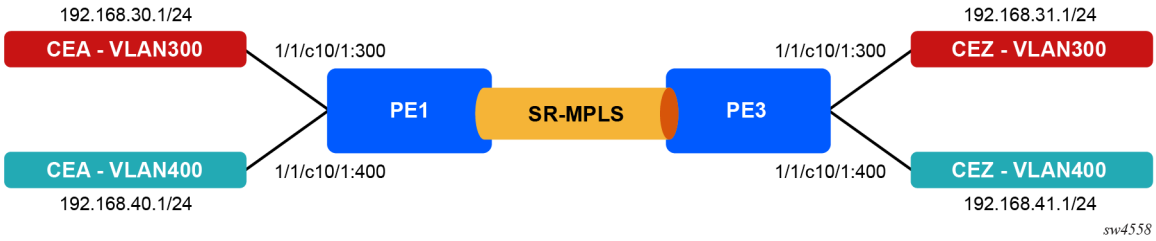
Each VPRN consists of a set of customer sites connected to one or more PE routers. Each associated PE router maintains a separate IP forwarding table for each VPRN. Additionally, the PE routers exchange the routing information configured or learned from all customer sites via MP-BGP peering. Each route exchanged via the MP-BGP protocol includes a Route Distinguisher (RD), which identifies the VPRN association and handles the possibility of IP address overlap.

See "VPRN service" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN* for detailed information about VPRN configuration.

See VPRN for information about relevant **show** commands.

The following figure shows the VPRN topology used in this example.

Figure 6: VPRN topology used in this example



Two VPRNs - RED and BLUE - will be created on PE1 and PE3 to establish communication between the clients on either sides. SR-ISIS will be used as the tunneling protocol. See Segment routing for information about SR-ISIS configuration.

The route targets for both VPRNs will be exchanged with each other using route policies, enabling each VPRN's client to reach the other VPRN's client.

Configuration

CE-facing Port configuration on PE1 and PE3:

```
/configure port 1/1/c10/1 admin-state enable
/configure port 1/1/c10/1 ethernet mode access
/configure port 1/1/c10/1 ethernet encap-type dot1q
/configure port 1/1/c10/1 ethernet mtu 5000
```

BGP configuration on PE1 to advertise the VPN-IPv4 family to PE3:

```
/configure router "Base" bgp router-id 10.10.10.1
/configure router "Base" bgp group "pe" peer-as 64500
/configure router "Base" bgp neighbor "10.10.10.3" group "pe"
/configure router "Base" bgp neighbor "10.10.10.3" family vpn-ipv4 true
```

BGP configuration on PE3 to advertise VPN-IPv4 family to PE1:

```
/configure router "Base" bgp router-id 10.10.10.3
/configure router "Base" bgp group "pe" peer-as 64500
/configure router "Base" bgp neighbor "10.10.10.1" group "pe"
/configure router "Base" bgp neighbor "10.10.10.1" family vpn-ipv4 true
```

VPRN ACL configuration on PE1:

```
/configure filter ip-filter "VPRN-RED-ACL" filter-id 103
/configure filter ip-filter "VPRN-RED-ACL" entry 10 match protocol icmp
/configure filter ip-filter "VPRN-RED-ACL" entry 10 match dst-ip address 192.168.31.1
/configure filter ip-filter "VPRN-RED-ACL" entry 10 match dst-ip mask 255.255.255.255
/configure filter ip-filter "VPRN-RED-ACL" entry 10 action accept

/configure filter ip-filter "VPRN-BLUE-ACL" filter-id 104
/configure filter ip-filter "VPRN-BLUE-ACL" entry 10 match protocol icmp
/configure filter ip-filter "VPRN-BLUE-ACL" entry 10 match dst-ip address 192.168.41.1
/configure filter ip-filter "VPRN-BLUE-ACL" entry 10 match dst-ip mask 255.255.255.255
/configure filter ip-filter "VPRN-BLUE-ACL" entry 10 action accept
```

VPRN route policies on PE1 and PE3:

The route policies configure the route targets to be exported and imported in each VPRN. In this example, both RED and BLUE VPRN targets are imported, enabling them to communicate with each other. Additional communities can be added as needed.

```
/configure policy-options community "BLUE" { member "target:64565:40" }
/configure policy-options community "RED" { member "target:64555:30" }
/configure policy-options policy-statement "export-blue" entry-type named
/configure policy-options policy-statement "export-blue" named-entry "blue" action action-type
 accept
/configure policy-options policy-statement "export-blue" named-entry "blue" action community
 add ["BLUE"]
/configure policy-options policy-statement "export-red" entry-type named
/configure policy-options policy-statement "export-red" named-entry "red" action action-type
 accept
/configure policy-options policy-statement "export-red" named-entry "red" action community add
 ["RED"]
/configure policy-options policy-statement "import-red-blue" entry-type named
/configure policy-options policy-statement "import-red-blue" named-entry "red" from community
 name "RED"
/configure policy-options policy-statement "import-red-blue" named-entry "red" from protocol
 name [bgp-vpn]
/configure policy-options policy-statement "import-red-blue" named-entry "red" action action-
type accept
/configure policy-options policy-statement "import-red-blue" named-entry "blue" from community
 name "BLUE"
/configure policy-options policy-statement "import-red-blue" named-entry "blue" from protocol
 name [bgp-vpn]
/configure policy-options policy-statement "import-red-blue" named-entry "blue" action action-
type accept
```

RED VPRN service configuration on PE1:

```
/configure service vprn "RED" admin-state enable
/configure service vprn "RED" service-id 30
/configure service vprn "RED" customer "1"
/configure service vprn "RED" autonomous-system 64555
/configure service vprn "RED" bgp-ipvpn mpls admin-state enable
/configure service vprn "RED" bgp-ipvpn mpls route-distinguisher "10.10.10.1:64555"
```

```
/configure service vprn "RED" bgp-ipvpn mpls vrf-import policy ["import-red-blue"]
/configure service vprn "RED" bgp-ipvpn mpls vrf-export policy ["export-red"]
/configure service vprn "RED" bgp-ipvpn mpls auto-bind-tunnel resolution filter
/configure service vprn "RED" bgp-ipvpn mpls auto-bind-tunnel resolution-filter sr-isis true
/configure service vprn "RED" interface "to-cea" ipv4 primary address 192.168.30.254
/configure service vprn "RED" interface "to-cea" ipv4 primary prefix-length 24
/configure service vprn "RED" interface "to-cea" sap 1/1/c10/1:300 ingress qos sap-ingress
 policy-name "CE-ingress-QoS"
/configure service vprn "RED" interface "to-cea" sap 1/1/c10/1:300 ingress filter ip "VPRN-RED-
ACL"
/configure service vprn "RED" interface "to-cea" sap 1/1/c10/1:300 egress qos sap-egress
 policy-name "CE-egress-QoS"
```

BLUE VPRN service configuration on PE1:

```
/configure service vprn "BLUE" admin-state enable
/configure service vprn "BLUE" service-id 40
/configure service vprn "BLUE" customer "1"
/configure service vprn "BLUE" autonomous-system 64565
/configure service vprn "BLUE" bgp-ipvpn mpls admin-state enable
/configure service vprn "BLUE" bgp-ipvpn mpls route-distinguisher "10.10.10.1:64565"
/configure service vprn "BLUE" bgp-ipvpn mpls vrf-import policy ["import-red-blue"]
/configure service vprn "BLUE" bgp-ipvpn mpls vrf-export policy ["export-blue"]
/configure service vprn "BLUE" bgp-ipvpn mpls auto-bind-tunnel resolution filter
/configure service vprn "BLUE" bgp-ipvpn mpls auto-bind-tunnel resolution-filter sr-isis true
/configure service vprn "BLUE" interface "to-cea" ipv4 primary address 192.168.40.254
/configure service vprn "BLUE" interface "to-cea" ipv4 primary prefix-length 24
/configure service vprn "BLUE" interface "to-cea" sap 1/1/c10/1:400 ingress qos sap-ingress
 policy-name "CE-ingress-QoS"
/configure service vprn "BLUE" interface "to-cea" sap 1/1/c10/1:400 ingress filter ip "VPRN-
BLUE-ACL"
/configure service vprn "BLUE" interface "to-cea" sap 1/1/c10/1:400 egress qos sap-egress
 policy-name "CE-egress-QoS"
```

See QoS for QoS policy configuration.

RED VPRN service configuration on PE3:

```
/configure service vprn "RED" admin-state enable
/configure service vprn "RED" service-id 30
/configure service vprn "RED" customer "1"
/configure service vprn "RED" autonomous-system 64555
/configure service vprn "RED" bgp-ipvpn mpls admin-state enable
/configure service vprn "RED" bgp-ipvpn mpls route-distinguisher "10.10.10.3:64555"
/configure service vprn "RED" bgp-ipvpn mpls vrf-import policy ["import-red-blue"]
/configure service vprn "RED" bgp-ipvpn mpls vrf-export policy ["export-red"]
/configure service vprn "RED" bgp-ipvpn mpls auto-bind-tunnel resolution filter
/configure service vprn "RED" bgp-ipvpn mpls auto-bind-tunnel resolution-filter sr-isis true
/configure service vprn "RED" interface "to-cez" ipv4 primary address 192.168.31.254
/configure service vprn "RED" interface "to-cez" ipv4 primary prefix-length 24
/configure service vprn "RED" interface "to-cez" { sap 1/1/c10/1:300 }
```

BLUE VPRN service configuration on PE3:

```
/configure service vprn "BLUE" admin-state enable
/configure service vprn "BLUE" service-id 40
/configure service vprn "BLUE" customer "1"
/configure service vprn "BLUE" autonomous-system 64565
/configure service vprn "BLUE" bgp-ipvpn mpls admin-state enable
/configure service vprn "BLUE" bgp-ipvpn mpls route-distinguisher "10.10.10.3:64565"
/configure service vprn "BLUE" bgp-ipvpn mpls vrf-import policy ["import-red-blue"]
/configure service vprn "BLUE" bgp-ipvpn mpls vrf-export policy ["export-blue"]
```

```
/configure service vprn "BLUE" bgp-ipvpn mpls auto-bind-tunnel resolution filter
/configure service vprn "BLUE" bgp-ipvpn mpls auto-bind-tunnel resolution-filter sr-isis true
/configure service vprn "BLUE" interface "to-cez" ipv4 primary address 192.168.41.254
/configure service vprn "BLUE" interface "to-cez" ipv4 primary prefix-length 24
/configure service vprn "BLUE" interface "to-cez" { sap 1/1/c10/1:400 }
```

Customer verification

Login to CEA:

```
docker exec -it cea bash
```

Ping CEZ VLAN 300 from CEA:

```
└──> ping -c 100 -Q 34  192.168.31.1
PING 192.168.31.1 (192.168.31.1) 56(84) bytes of data.
64 bytes from 192.168.31.1: icmp_seq=1 ttl=62 time=9.81 ms
64 bytes from 192.168.31.1: icmp_seq=2 ttl=62 time=5.93 ms
64 bytes from 192.168.31.1: icmp_seq=3 ttl=62 time=6.45 ms

--- 192.168.31.1 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99151ms
rtt min/avg/max/mdev = 4.360/6.300/14.803/2.373 ms
```

While the ping is in progress, check the SAP, ACL, and QoS statistics.

13 IES

IES is a routed connectivity service that enables subscribers to communicate with an IP router interface to send and receive Internet traffic. An IES has one or more logical IP routing interfaces, each with a SAP that acts as the access point to the subscriber network.

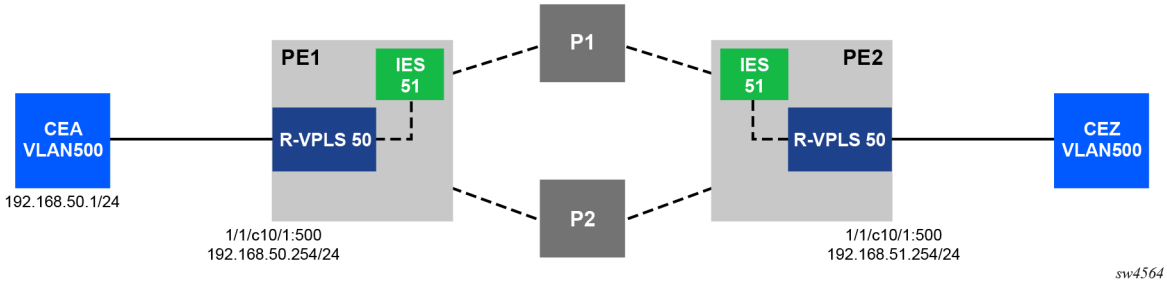
IES allows IP interfaces to participate in the same routing instance used for service network core routing connectivity.

See "Internet Enhanced Service" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN* for detailed information about IES.

See IES for information about relevant verification commands.

The following figure shows the IES topology for this example.

Figure 7: IES topology used in this example



An IES service will be created to establish communication between the Layer 2 clients. The routes are exchanged from the global routing table to the IES service. Routed VPLS or RVPLS (commonly called IRB) is configured toward the customer to collect traffic and forward it to the IES service. The RVPLS service is configured with a SAP that acts as the access point.

To connect Layer 3 clients, a direct Layer 3 interface can be created facing the Layer 3 client.

Configuration

CE-facing port configuration on PE1 and PE3:

```
/configure port 1/1/c10/1 admin-state enable
/configure port 1/1/c10/1 ethernet mode access
/configure port 1/1/c10/1 ethernet encap-type dot1q
/configure port 1/1/c10/1 ethernet mtu 5000
```

VPLS SAP IPv4 filter configuration on PE1:

```
/configure filter ip-filter "RVPLS-ACL" filter-id 105
/configure filter ip-filter "RVPLS-ACL" entry 10 match protocol icmp
/configure filter ip-filter "RVPLS-ACL" entry 10 match dst-ip address 192.168.51.1
/configure filter ip-filter "RVPLS-ACL" entry 10 match dst-ip mask 255.255.255.255
/configure filter ip-filter "RVPLS-ACL" entry 10 action accept
```

VPLS configuration on PE1:

```
/configure service vpls "RVPLS-VLAN500" service-id 50
/configure service vpls "RVPLS-VLAN500" customer "1"
/configure service vpls "RVPLS-VLAN500" admin-state enable
/configure service vpls "RVPLS-VLAN500" routed-vpls { }
/configure service vpls "RVPLS-VLAN500" sap 1/1/c10/1:500 ingress qos sap-ingress policy-name
 "CE-ingress-QoS"
/configure service vpls "RVPLS-VLAN500" sap 1/1/c10/1:500 ingress filter ip "RVPLS-ACL"
/configure service vpls "RVPLS-VLAN500" sap 1/1/c10/1:500 egress qos sap-egress policy-name
 "CE-egress-QoS"
```

VPLS configuration on PE3:

```
/configure service vpls "RVPLS-VLAN500" service-id 50
/configure service vpls "RVPLS-VLAN500" customer "1"
/configure service vpls "RVPLS-VLAN500" admin-state enable
/configure service vpls "RVPLS-VLAN500" routed-vpls { }
/configure service vpls "RVPLS-VLAN500" sap 1/1/c10/1:500 { }
```

IES configuration on PE1:

```
/configure service ies "IES-500" admin-state enable
/configure service ies "IES-500" service-id 51
/configure service ies "IES-500" customer "1"
/configure service ies "IES-500" interface "to-CEA-VLAN500" { vpls "RVPLS-VLAN500" }
/configure service ies "IES-500" interface "to-CEA-VLAN500" ipv4 primary address 192.168.50.254
/configure service ies "IES-500" interface "to-CEA-VLAN500" ipv4 primary prefix-length 24
```

IES configuration on PE3:

```
/configure service ies "IES-500" admin-state enable
/configure service ies "IES-500" service-id 51
/configure service ies "IES-500" customer "1"
/configure service ies "IES-500" interface "to-CEZ-VLAN500" { vpls "RVPLS-VLAN500" }
/configure service ies "IES-500" interface "to-CEZ-VLAN500" ipv4 primary address 192.168.51.254
/configure service ies "IES-500" interface "to-CEZ-VLAN500" ipv4 primary prefix-length 24
```

To establish reachability between the client subnets in the global routing table, we will create a static route on PE1 and PE3 that will resolve to a SR-ISIS tunnel.

Static route on PE1:

```
/configure router "Base" static-routes route 192.168.51.0/24 route-type unicast indirect
 10.10.10.3 admin-state enable
/configure router "Base" static-routes route 192.168.51.0/24 route-type unicast indirect
 10.10.10.3 tunnel-next-hop resolution filter
/configure router "Base" static-routes route 192.168.51.0/24 route-type unicast indirect
 10.10.10.3 tunnel-next-hop resolution-filter sr-isis true
```

Static route on PE3:

```
/configure router "Base" static-routes route 192.168.50.0/24 route-type unicast indirect
 10.10.10.1 admin-state enable
/configure router "Base" static-routes route 192.168.50.0/24 route-type unicast indirect
 10.10.10.1 tunnel-next-hop resolution filter
/configure router "Base" static-routes route 192.168.50.0/24 route-type unicast indirect
 10.10.10.1 tunnel-next-hop resolution-filter sr-isis true
```

Customer verification

Login to CEA:

```
docker exec -it cea bash
```

Ping CEZ VLAN 600 from CEA:

```
└──> ping -c 100 -Q 34 192.168.51.1
PING 192.168.51.1 (192.168.51.1) 56(84) bytes of data.
64 bytes from 192.168.51.1: icmp_seq=1 ttl=61 time=17.8 ms
64 bytes from 192.168.51.1: icmp_seq=2 ttl=61 time=9.91 ms
64 bytes from 192.168.51.1: icmp_seq=3 ttl=61 time=5.03 ms

--- 192.168.51.1 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99142ms
rtt min/avg/max/mdev = 4.955/7.436/17.811/3.667 ms
```

While the ping is in progress, check the SAP, ACL, and QoS statistics.

14 EVPN-VPWS

EVPN is an IETF technology as defined in RFC 7432, *BGP MPLS-Based Ethernet VPN*, which uses a specific BGP address family and allows VPLS services to operate as IP-VPNs. BGP is used to distribute MAC addresses and flooding tree setup information.

EVPN-VPWS provides Epipe point-to-point services.

See "Ethernet Virtual Private Networks" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide* for detailed information about EVPN-VPWS.

See EVPN-VPWS for information about relevant verification commands.

The following figure shows the EVPN-VPWS topology for this example.

Figure 8: EVPN-VPWS topology used in this example

An EVPN-VPWS service is created to establish communication between the clients. SR-TE is used as the transport protocol. See SR-TE for information about the relevant SR-TE configuration.

Configuration

CE-facing port configuration on PE1 and PE3:

```
/configure port 1/1/c10/1 admin-state enable
/configure port 1/1/c10/1 ethernet mode access
/configure port 1/1/c10/1 ethernet encap-type dot1q
/configure port 1/1/c10/1 ethernet mtu 5000
```

BGP configuration on PE1:

```
/configure router "Base" bgp router-id 10.10.10.1
/configure router "Base" bgp group "pe" peer-as 64500
/configure router "Base" bgp neighbor "10.10.10.3" group "pe"
/configure router "Base" bgp neighbor "10.10.10.3" family evpn true
```

BGP configuration on PE3:

```
/configure router "Base" bgp router-id 10.10.10.3
/configure router "Base" bgp group "pe" peer-as 64500
/configure router "Base" bgp neighbor "10.10.10.1" group "pe"
/configure router "Base" bgp neighbor "10.10.10.1" family evpn true
```

ACL configuration on PE1:

```
/configure filter ip-filter "VPWS-ACL" filter-id 106
/configure filter ip-filter "VPWS-ACL" entry 10 match protocol icmp
/configure filter ip-filter "VPWS-ACL" entry 10 match dst-ip address 192.168.60.2
```

```
/configure filter ip-filter "VPWS-ACL" entry 10 match dst-ip mask 255.255.255.255
/configure filter ip-filter "VPWS-ACL" entry 10 action accept
```

EVPN-VPWS configuration on PE1:

```
/configure service epipe "VPWS-VLAN600" admin-state enable
/configure service epipe "VPWS-VLAN600" description "EVPN-VPWS-VLAN600"
/configure service epipe "VPWS-VLAN600" service-id 60
/configure service epipe "VPWS-VLAN600" customer "1"
/configure service epipe "VPWS-VLAN600" bgp 1 route-distinguisher "10.10.10.1:60"
/configure service epipe "VPWS-VLAN600" bgp 1 route-target export "target:64500:60"
/configure service epipe "VPWS-VLAN600" bgp 1 route-target import "target:64500:60"
/configure service epipe "VPWS-VLAN600" sap 1/1/c10/1:600 ingress qos sap-ingress policy-name
 "CE-ingress-QoS"
/configure service epipe "VPWS-VLAN600" sap 1/1/c10/1:600 ingress filter ip "VPWS-ACL"
/configure service epipe "VPWS-VLAN600" sap 1/1/c10/1:600 egress qos sap-egress policy-name
 "CE-egress-QoS"
/configure service epipe "VPWS-VLAN600" bgp-evpn local-attachment-circuit "local" eth-tag 1111
/configure service epipe "VPWS-VLAN600" bgp-evpn remote-attachment-circuit "remote" eth-tag
 9999
/configure service epipe "VPWS-VLAN600" bgp-evpn mpls 1 admin-state enable
/configure service epipe "VPWS-VLAN600" bgp-evpn mpls 1 auto-bind-tunnel resolution filter
/configure service epipe "VPWS-VLAN600" bgp-evpn mpls 1 auto-bind-tunnel resolution-filter sr-
te true
```

EVPN-VPWS configuration on PE3:

```
/configure service epipe "VPWS-VLAN600" admin-state enable
/configure service epipe "VPWS-VLAN600" description "EVPN-VPWS-VLAN600"
/configure service epipe "VPWS-VLAN600" service-id 60
/configure service epipe "VPWS-VLAN600" customer "1"
/configure service epipe "VPWS-VLAN600" bgp 1 route-distinguisher "10.10.10.3:60"
/configure service epipe "VPWS-VLAN600" bgp 1 route-target export "target:64500:60"
/configure service epipe "VPWS-VLAN600" bgp 1 route-target import "target:64500:60"
/configure service epipe "VPWS-VLAN600" sap 1/1/c10/1:600 { }
/configure service epipe "VPWS-VLAN600" bgp-evpn local-attachment-circuit "local" eth-tag 9999
/configure service epipe "VPWS-VLAN600" bgp-evpn remote-attachment-circuit "remote" eth-tag
 1111
/configure service epipe "VPWS-VLAN600" bgp-evpn mpls 1 admin-state enable
/configure service epipe "VPWS-VLAN600" bgp-evpn mpls 1 auto-bind-tunnel resolution filter
/configure service epipe "VPWS-VLAN600" bgp-evpn mpls 1 auto-bind-tunnel resolution-filter sr-
te true
```

Customer verification

Login to CEA:

```
docker exec -it cea bash
```

Ping CEZ VLAN 600 from CEA:

```
└──> ping -c 100 -Q 34 192.168.60.2
PING 192.168.60.2 (192.168.60.2) 56(84) bytes of data.
64 bytes from 192.168.60.2: icmp_seq=1 ttl=64 time=9.93 ms
64 bytes from 192.168.60.2: icmp_seq=2 ttl=64 time=5.25 ms
64 bytes from 192.168.60.2: icmp_seq=3 ttl=64 time=4.81 ms

--- 192.168.60.2 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99142ms
rtt min/avg/max/mdev = 4.488/5.589/16.327/1.665 ms
```

While the ping is in progress, check the SAP, ACL, and QoS statistics.

15 EVPN-MPLS with multihoming

EVPN is an IETF technology defined in RFC 7432, *BGP MPLS-Based Ethernet VPN*, which uses a specific BGP address family and allows VPLS services to operate as IP-VPNs. BGP is used to distribute MAC addresses and flooding tree setup information.

EVPN-MPLS is supported where PEs are connected by any type of MPLS tunnel. EVPN-MPLS is typically used as an evolution of VPLS services in the WAN, with Data Center Interconnect being on of its main applications.

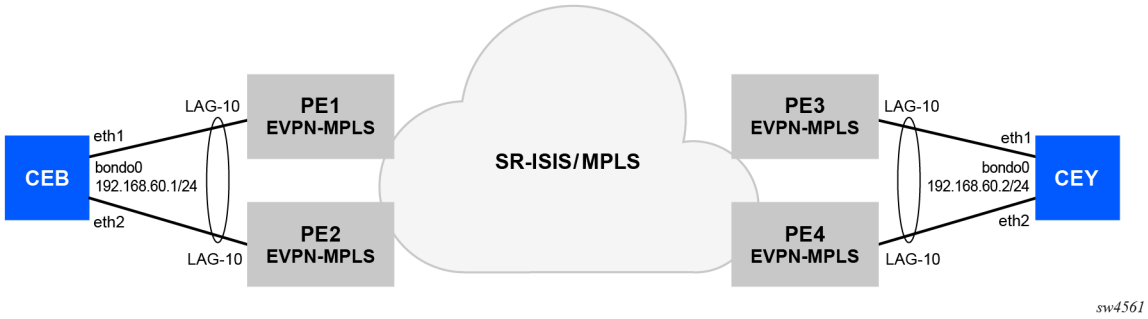
EVPN can be used in MPLS networks where PEs are interconnected through any type of tunnel, including RSVP-TE, SR-TE, LDP, BGP, SR-ISIS, segment routing OSPF, RIB-API, MPLS forwarding policy, SR policy, or MPLS over UDP (MPLSoUDP).

See "Ethernet Virtual Private Networks" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide* for detailed information about EVPN-MPLS.

See EVPN-MPLS for information about relevant verification commands.

The following figure shows the EVPN-MPLS topology for this example.

Figure 9: EVPN-MPLS topology used in this example



The client on either side is multihomed to two PE devices. An EVPN-MPLS service will be created to establish communication between the clients. SR-ISIS will be used as the transport protocol. See Segment routing for information about the relevant SR-ISIS configuration.

Configuration

CE-facing port configuration on PE1, PE2, PE3 and PE4:

```
/configure port 1/1/c11/1 admin-state enable
/configure port 1/1/c11/1 ethernet mode access
```

LAG configuration on PE1 and PE2:

```
/configure lag "lag-10" admin-state enable
/configure lag "lag-10" mode access
/configure lag "lag-10" lacp mode active
/configure lag "lag-10" lacp system-id 00:00:00:00:01:02
/configure lag "lag-10" lacp administrative-key 32768
```

```
/configure lag "lag-10" port 1/1/c11/1 { }
```

LAG configuration on PE3 and PE4:

```
/configure lag "lag-10" admin-state enable
/configure lag "lag-10" mode access
/configure lag "lag-10" lacp mode active
/configure lag "lag-10" lacp system-id 00:00:00:00:03:04
/configure lag "lag-10" lacp administrative-key 32768
/configure lag "lag-10" port 1/1/c11/1 { }
```

BGP configuration on PE1:

```
/configure router "Base" bgp router-id 10.10.10.1
/configure router "Base" bgp group "pe" peer-as 64500
/configure router "Base" bgp neighbor "10.10.10.2" group "pe"
/configure router "Base" bgp neighbor "10.10.10.2" family evpn true
/configure router "Base" bgp neighbor "10.10.10.3" group "pe"
/configure router "Base" bgp neighbor "10.10.10.3" family evpn true
/configure router "Base" bgp neighbor "10.10.10.4" group "pe"
/configure router "Base" bgp neighbor "10.10.10.4" family evpn true
```

BGP configuration on PE2:

```
/configure router "Base" bgp router-id 10.10.10.2
/configure router "Base" bgp group "pe" peer-as 64500
/configure router "Base" bgp neighbor "10.10.10.1" group "pe"
/configure router "Base" bgp neighbor "10.10.10.1" family evpn true
/configure router "Base" bgp neighbor "10.10.10.3" group "pe"
/configure router "Base" bgp neighbor "10.10.10.3" family evpn true
/configure router "Base" bgp neighbor "10.10.10.4" group "pe"
/configure router "Base" bgp neighbor "10.10.10.4" family evpn true
```

BGP configuration on PE3:

```
/configure router "Base" bgp router-id 10.10.10.3
/configure router "Base" bgp group "pe" peer-as 64500
/configure router "Base" bgp neighbor "10.10.10.1" group "pe"
/configure router "Base" bgp neighbor "10.10.10.1" family evpn true
/configure router "Base" bgp neighbor "10.10.10.2" group "pe"
/configure router "Base" bgp neighbor "10.10.10.2" family evpn true
/configure router "Base" bgp neighbor "10.10.10.4" group "pe"
/configure router "Base" bgp neighbor "10.10.10.4" family evpn true
```

BGP configuration on PE4:

```
/configure router "Base" bgp router-id 10.10.10.4
/configure router "Base" bgp group "pe" peer-as 64500
/configure router "Base" bgp neighbor "10.10.10.1" group "pe"
/configure router "Base" bgp neighbor "10.10.10.1" family evpn true
/configure router "Base" bgp neighbor "10.10.10.2" group "pe"
/configure router "Base" bgp neighbor "10.10.10.2" family evpn true
/configure router "Base" bgp neighbor "10.10.10.3" group "pe"
/configure router "Base" bgp neighbor "10.10.10.3" family evpn true
```

Ethernet Segment (ES) configuration on PE1 and PE2:

```
/configure service system bgp evpn ethernet-segment "ES-1" admin-state enable
/configure service system bgp evpn ethernet-segment "ES-1" esi 0x00121212121212000101
```

```
/configure service system bgp evpn ethernet-segment "ES-1" multi-homing-mode all-active
/configure service system bgp evpn ethernet-segment "ES-1" association { lag "lag-10" }
```

Ethernet Segment (ES) configuration on PE3 and PE4:

```
/configure service system bgp evpn ethernet-segment "ES-1" admin-state enable
/configure service system bgp evpn ethernet-segment "ES-1" esi 0x00343434343434000103
/configure service system bgp evpn ethernet-segment "ES-1" multi-homing-mode all-active
/configure service system bgp evpn ethernet-segment "ES-1" association { lag "lag-10" }
```

EVPN-MPLS configuration on PE1, PE2, PE3, and PE4:

```
/configure service vpls "EVPN-MPLS" admin-state enable
/configure service vpls "EVPN-MPLS" service-id 70
/configure service vpls "EVPN-MPLS" customer "1"
/configure service vpls "EVPN-MPLS" bgp 1 route-distinguisher "64500:70"
/configure service vpls "EVPN-MPLS" bgp 1 route-target export "target:64500:70"
/configure service vpls "EVPN-MPLS" bgp 1 route-target import "target:64500:70"
/configure service vpls "EVPN-MPLS" bgp-evpn evi 70
/configure service vpls "EVPN-MPLS" bgp-evpn mpls 1 admin-state enable
/configure service vpls "EVPN-MPLS" bgp-evpn mpls 1 ingress-replication-bum-label true
/configure service vpls "EVPN-MPLS" bgp-evpn mpls 1 auto-bind-tunnel resolution filter
/configure service vpls "EVPN-MPLS" bgp-evpn mpls 1 auto-bind-tunnel resolution-filter sr-isis
 true
/configure service vpls "EVPN-MPLS" sap lag-10 { }
```

ACL and QoS policies can be applied under the SAP context.

Customer verification

Login to CEB:

```
docker exec -it ceb bash
```

Ping CEY from CEB:

```
└──> ping -c 100 192.168.60.2
PING 192.168.60.2 (192.168.60.2) 56(84) bytes of data.
64 bytes from 192.168.60.2: icmp_seq=1 ttl=64 time=9.93 ms
64 bytes from 192.168.60.2: icmp_seq=2 ttl=64 time=5.25 ms
64 bytes from 192.168.60.2: icmp_seq=3 ttl=64 time=4.81 ms

--- 192.168.60.2 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99142ms
rtt min/avg/max/mdev = 4.488/5.589/16.327/1.665 ms
```

16 Show commands

This chapter provides information about the **show** commands you can use to display and verify specific configuration information.

For a complete list of SR OS CLI trees and command descriptions, see *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools CLI Command Reference Guide*.

16.1 Hardware and system

To verify chassis information including fan, power supply status:

```
show chassis detail
```

To verify control and line card status:

```
show card state
```

To view control card details:

```
show card A detail
```

To view line card details:

```
show card 1 detail
```

To verify the current software version:

```
show version
```

To view routing table details:

```
show router route-table
```

To view tunnel table details:

```
show router tunnel-table
```

16.2 Port and interfaces

To view a summary of all ports:

```
show port
```

To view port details:

```
show port 1/1/c1/1 detail
```

To view a port's optics information:

```
show port 1/1/c1 optical
```

To view a port's statistics:

```
show port 1/1/c1/1 statistics
```

To view LAG status:

```
show lag lag-10 description
```

To view all router interfaces:

```
show router interface
```

To view an interface's detail:

```
show router interface To-P1 detail
```

To view BFD session status:

```
show router bfd session
```

16.3 OSPF

To view OSPF adjacency status:

```
show router ospf neighbor
```

To view interfaces participating in OSPF:

```
show router ospf interface
```

To view a summary of OSPF:

```
show router ospf status
```

To view OSPF RIB routes:

```
show router ospf routes
```

To view OSPF database:

```
show router ospf database
```

16.4 IS-IS

To view ISIS adjacency status:

```
show router isis adjacency
```

To view interfaces participating in ISIS:

```
show router isis interface
```

To view a summary of ISIS:

```
show router isis status
```

To view ISIS RIB routes:

```
show router isis routes
```

To view ISIS database:

```
show router isis database
```

16.5 BGP

To view BGP neigbor status:

```
show router bgp summary
```

To view BGP routes advertised to a neighbor:

```
show router bgp neighbor "10.10.10.3" advertised-routes evpn
```

To view BGP routes received from a neighbor:

```
show router bgp neighbor "10.10.10.3"  received-routes evpn
```

To view BGP IPv4 routes:

```
show router bgp routes
```

To view BGP VPN-IPv4 routes:

```
show router bgp routes vpn-ipv4
```

To view EVPN Type 1 routes:

```
show router bgp routes evpn auto-disc
```

To view EVPN Type 2 routes:

```
show router bgp routes evpn mac
```

To view EVPN Type 3 routes:

```
show router bgp routes evpn incl-mcast
```

To view EVPN Type 4 routes:

```
show router bgp routes evpn eth-seg
```

To view EVPN Type 5 routes:

```
show router bgp routes evpn ip-prefix
```

16.6 LDP

To verify LDP adjacency:

```
show router ldp discovery
```

To view LDP sessions:

```
show router ldp session
```

To view T-LDP sessions:

```
show router ldp targ-peer
```

To view LDP bindings:

```
show router ldp bindings
```

To view service label bindings:

```
show router ldp bindings services service-id "Epipe-VLAN100"
```

16.7 RSVP-TE

To verify MPLS interface status:

```
show router mpls interface
```

To verify RSVP interface status:

```
show router rsvp interface
```

To verify LSP status:

```
show router mpls lsp
```

To verify LSP path:

```
show router mpls lsp "lsp-to-R3" path detail
```

16.8 Segment routing

To verify SR-MPLS label allocation:

```
show router mpls-labels summary
```

To view SR-MPLS tunnels and labels:

```
tools dump router segment-routing tunnel
```

16.9 SR-TE

To verify SR-TE LSP status:

```
show router mpls sr-te-lsp
```

To verify SR-TE LSP path:

```
show router mpls sr-te-lsp "lsp-sr-te-R3" path detail
```

16.10 ACL

To view IPv4 ACL status and statistics:

```
show filter ip "Epipe-ACL"
```

To verify IPv4 ACL filter associations:

```
show filter ip "Epipe-ACL" associations
```

To view MAC ACL status and statistics:

```
show filter mac "VPLS-MAC-Filter"
```

16.11 QoS

To view SAP ingress policy details:

```
show qos sap-ingress "CE-ingress-QoS" detail
```

To view SAP egress policy details:

```
show qos sap-egress "CE-egress-QoS" detail
```

To view SAP QoS statistics:

```
show service id "Epipe-VLAN100" sap "1/1/c10/1:100" stats
```

16.12 Services general

To list all services:

```
show service service-using
```

To list all SAPs:

```
show service sap-using
```

To list SDPs and their status:

```
show service sdp
```

To list SDPs binded to a service:

```
show service sdp-using
```

To view status of a service:

```
show service id "Epipe-VLAN100" base
```

To view service details:

```
show service id "Epipe-VLAN100" all
```

To view service SAP statistics:

```
show service id "Epipe-VLAN100" sap "1/1/c10/1:100" stats
```

16.13 Epipe

To view Epipe service status:

```
show service id "Epipe-VLAN100" base
```

To view Epipe service details:

```
show service id "Epipe-VLAN100" all
```

To view Epipe SAP statistics:

```
show service id "Epipe-VLAN100" sap "1/1/c10/1:100" stats
```

16.14 VPLS

To view VPLS service status:

```
show service id "VPLS-VLAN200" base
```

To view VPLS service details:

```
show service id "VPLS-VLAN200" all
```

To view VPLS SAP stats:

```
show service id "VPLS-VLAN200" sap "1/1/c10/1:200" stats
```

To view VPLS MAC FDB table:

```
show service id "VPLS-VLAN200" fdb detail
```

16.15 VPRN

To view VPRN service status:

```
show service id "RED" base
```

To view VPRN service details:

```
show service id "RED" all
```

To view VPRN SAP stats:

```
show service id "RED" sap "1/1/c10/1:300" stats
```

To view VPRN route table:

```
show router service-name "RED" route-table
```

To view VPN-IPv4 routes:

```
show router bgp routes vpn-ipv4
```

16.16 IES

To view RVPLS service status:

```
show service id "RVPLS-VLAN500" base
```

To view RVPLS service details:

```
show service id "RVPLS-VLAN500" all
```

To view RVPLS SAP stats:

```
show service id "RVPLS-VLAN500" sap "1/1/c10/1:500" stats
```

To view VPLS MAC FDB table:

```
show service id "RVPLS-VLAN500" fdb detail
```

To view IES service status:

```
show service id "IES-500" base
```

To view IES interface status:

```
show router interface
```

To view static route status:

```
show router static-route
```

16.17 EVPN-VPWS

To view VPWS service status:

```
show service id "VPWS-VLAN600" base
```

To view VPWS service details:

```
show service id "VPWS-VLAN600" all
```

To view VPWS SAP stats:

```
show service id "VPWS-VLAN600" sap "1/1/c10/1:300" stats
```

To view EVPN Route Type 1 with details:

```
show router bgp routes evpn auto-disc detail
```

16.18 EVPN-MPLS

To view EVPN service status:

```
show service id "EVPN-MPLS" base
```

To view EVPN service details:

```
show service id "EVPN-MPLS" all
```

To view EVPN SAP stats:

```
show service id "EVPN-MPLS" sap "EVPN-MPLS" stats
```

To view EVPN Route Type 1 with details:

```
show router bgp routes evpn auto-disc detail
```

To view EVPN Route Type 2 with details:

```
show router bgp routes evpn mac detail
```

To view EVPN Route Type 3 with details:

```
show router bgp routes evpn incl-mcast detail
```

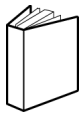
To view ethernet segment status:

```
show service system bgp-evpn ethernet-segment name "ES-1"
```

To view VPLS MAC FDB table:

```
show service id "EVPN-MPLS" fdb detail
```

Customer document and product support



Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback