Configure Interchassis HA

For supported software information, click here.

Interchassis high availability (HA) facilitates high resiliency and increases IP network availability between pairs of Versa Operating System™ (VOS™) devices located in branches or hubs, where one VOS device acts as the active device and the second acts as the standby. Interchassis HA provides continuous access to applications, data, and content in the control plane and in the data plane. When links in the control or data path become unavailable, interchassis HA automatically reroutes traffic flow to ensure continuous access.

To deploy interchassis HA, you install two VOS devices in a branch or as a hub, one configured to be the active device and the other configured as the standby.

In Releases 22.1.1 and later, you can deploy active-standby redundant pairs at the branch level using templates. For more information, see Create and Manage Staging and Post-Staging Templates. For information about the capabilities of branch-HA active-standby deployments compared to active-active deployments, see the Branch HA section in Branch Deployment Options.

Interchassis HA Overview

Control Plane and Data Plane Operation for HA

To implement interchassis HA, the software synchronizes the control plane and data plane information between the active and the standby VOS devices. This active-standby synchronization is a stateful model, in which the data and the flows on both the active and standby VOS devices are constantly being synchronized. A stateful model minimizes the switchover time if the active device should fail.

For the control plane, HA synchronizes the control plane state, including the resource management tables for traffic steering, and it provides control plane support for applications such as NAT and ADC. For HA to operate, the control plane creates the following connections between the active and standby VOS devices:

- Control connection—TCP connection over an external management or a LAN interface. HA uses this TCP connection to discover its HA peer and to negotiate each peer's role (the roles being active and standby). The preferred standby VOS device establishes this connection from its ephemeral port to port 9878 on the preferred active device. (You configure the preferred active and standby devices when you configure interchassis HA.)
- Data connection—TCP connection over a loopback IP interface. This connection is used to synchronize the control information related to resource management tables for traffic steering and applications, such as NAT and ADC. The

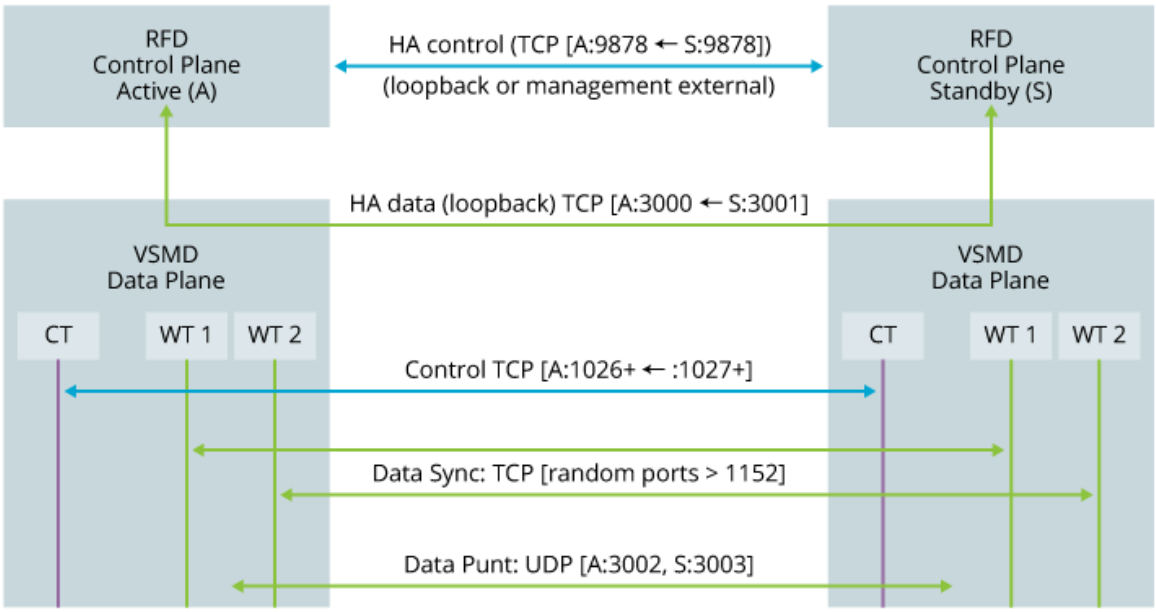
information is synchronized from the active HA VOS device to the standby device. The standby device initiates this connection from its port 3001 to port 3000 on the active device. This connection is routed over a dedicated sync interface, called the data sync interface, which is a dedicated interface that you configure between the active and standby devices.

For the data plane, HA synchronizes the data plane state, including sessions, NAT bindings, and ADC persistency information. To service the simultaneous parallel packets that carry the state information between the active and backup devices, the data plane runs multiple threads, which are called worker threads (WTs). Each worker thread on the active service node synchronizes information with the peer worker thread on the standby service node.

For HA to operate, the data plane creates the following connections between the active and standby VOS devices:

- Control connection—TCP connection between the active and standby Versa service nodes (VSNs). This TCP connection is used to negotiate which ports to use for the data synchronization connections that are used by the worker threads. The standby service node initiates this connection on a loopback IP interface from its port 3003 to port 3002 on the active service node.
- Data connection—TCP connection between each pair of worker threads on the active and standby service nodes. HA uses this TCP connection to synchronize data plane state, including sessions, NAT bindings, and ADC persistency information, between the active and standby service nodes. The worker thread on the standby service node initiates this TCP connection to its peer worker thread on the active service node. The port numbers to use for this channel are negotiated over the control channel and are allocated dynamically.
- Data punt connection—If a neighboring router directs packets to the standby service node, the standby node forwards them to the active service node, and the active node applies any configured services to the packets and continues forwarding them. This redirection is called *data punting*. Before forwarding the packets, the standby service node adds a proprietary UDP-based encapsulation header to the packets called the Versa service header (VSH). The standby node sends these packets from its port 3002 to port 3002 on the active service node. To avoid packet fragmentation, it is recommended that you configure jumbo MTUs (MTUs of 1600 bytes or larger) on the path between the active and standby nodes.

The following figure illustrates the control plane and data plane HA connections.



VSMD: Versa Services Manager Daemon
RFD: Resource and Flow Distribution Manager
CT: Control Thread
WT: Worker Thread
A ← S: Standby node initiates TCP connection to Active node

HA Topology

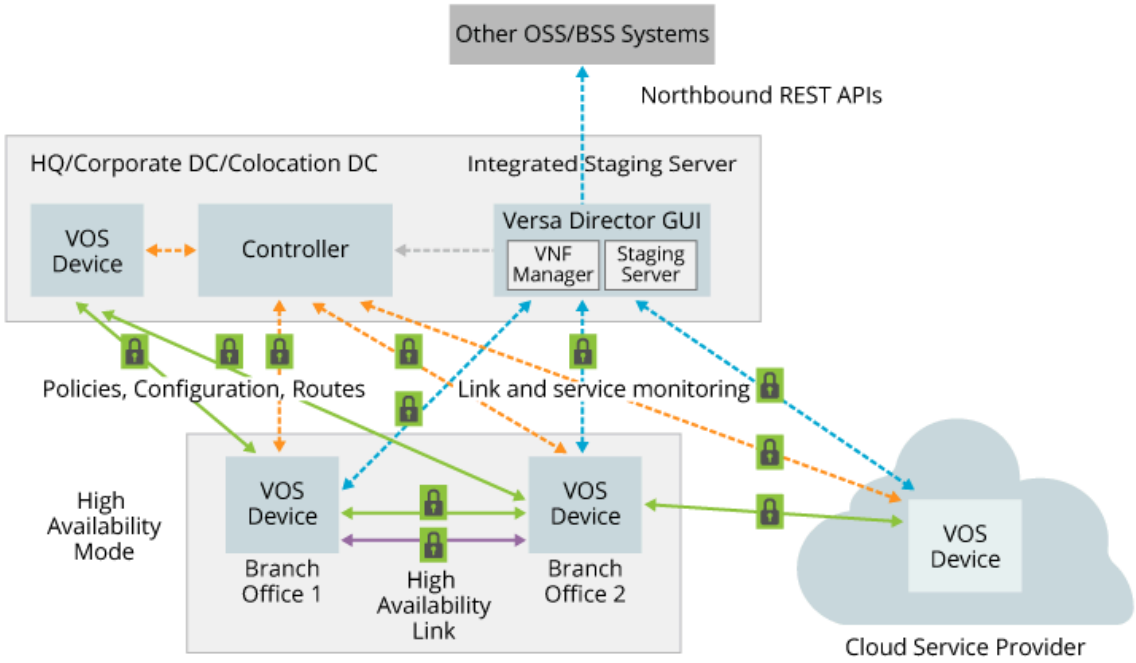
To deploy interchassis HA, you install two VOS devices in a branch or as a hub, you configure one to be the active device and the other to be the standby. Each active and standby device in the pair must have the same configuration, including the same interface and service configuration.

To provide routing information redundancy, the active and standby devices have separate connections to the SD-WAN Controller, and each connection establishes a Multiprotocol Border Gateway Protocol (MP-BGP) session over which the VOS device and the Versa Control exchange routing information about other branches and about client networks is served by the branches. In this way, the routing information on both the active and standby devices remains synchronized, thus providing resiliency in case of link failures with neighboring routers.

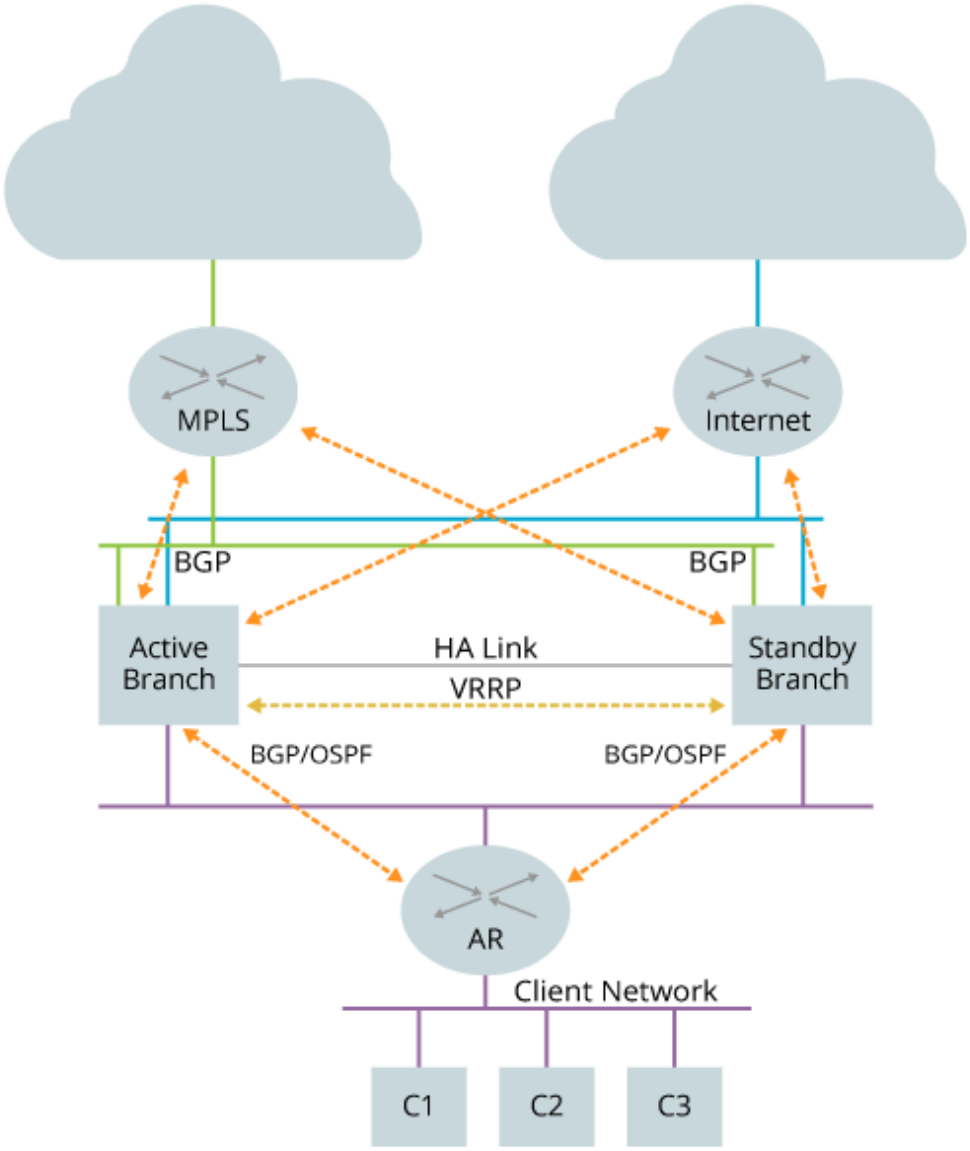
To provide redundant connections with neighbor routers, the active and standby devices establish External Border Gateway Protocol (EBGP) sessions with the internet transport (WAN) interface on the neighbor routers. Having EBGP sessions from both the active and standby devices provides resiliency in case a link to a neighbor router fails. You specify the preferred path between the neighbor router and the active VOS device by setting the EBGP local preference and path metric attributes. The active and standby devices learn about southbound LAN routes from routing protocols,

such as Interior Border Gateway Protocol (IBGP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP), and from manually configured static routes.

The following figure provides a high-level view of an SD-WAN interchassis HA deployment.



The following figure illustrates the connections and protocols that are typically used in an interchassis HA deployment. In this figure, Active Branch and Standby Branch are the VOS devices. The access router (AR) is a client-facing router, and the MPLS and Internet routers face their respective external networks. The active and standby branch nodes establish EBGP sessions on their northbound interfaces to connect to the MPLS and internet routers, and they establish IBGP or OSPF sessions on their southbound interfaces with the access router. The forward path direction traffic flows from south to north.



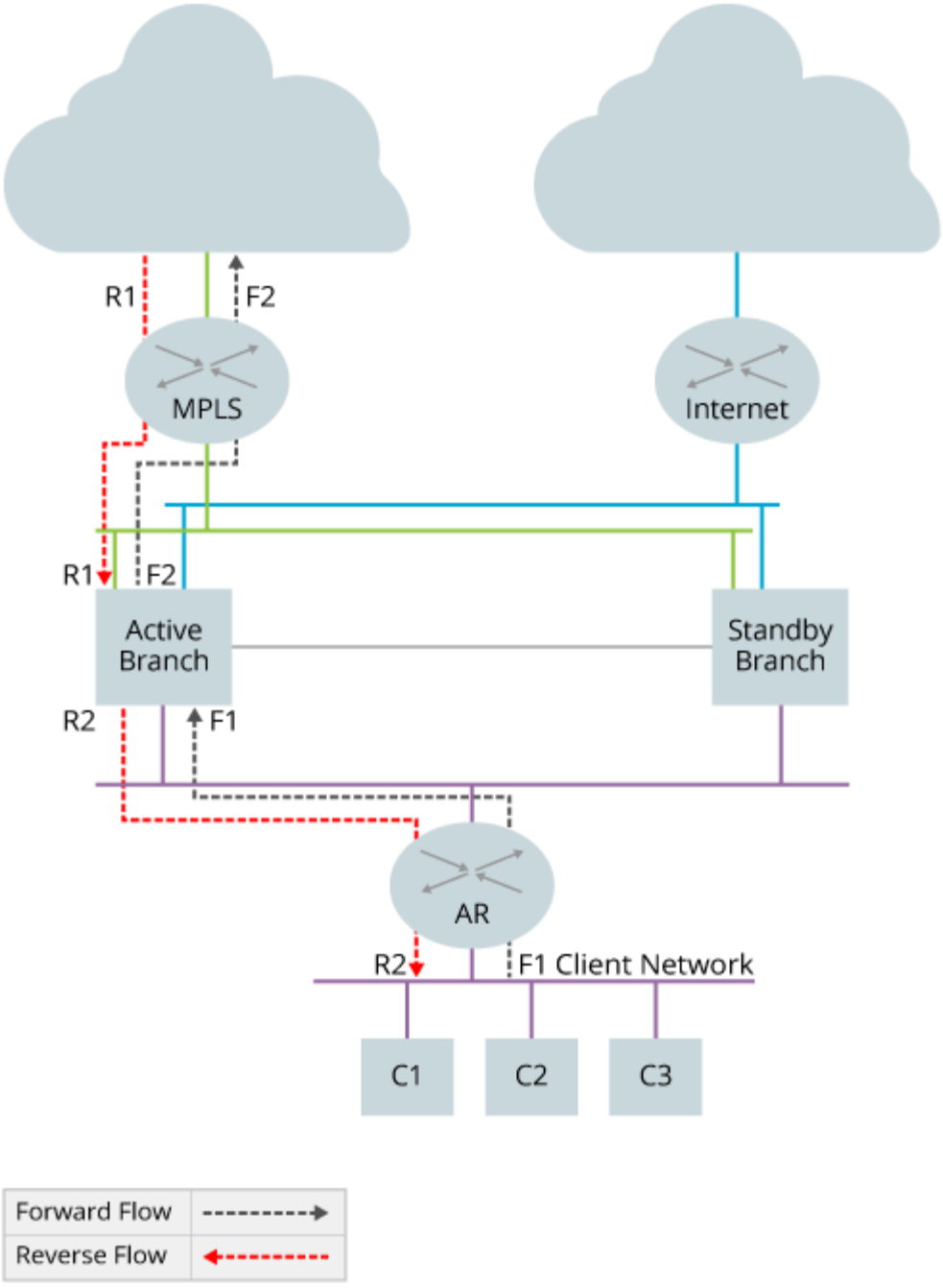
BGP/OSPF Session	
MPLS Network	
Internal Network	
Client Network	

Data Path Failure Scenarios

This section provides various data path failure scenarios for interchassis HA deployments and describes how the failure

is mitigated by the software.

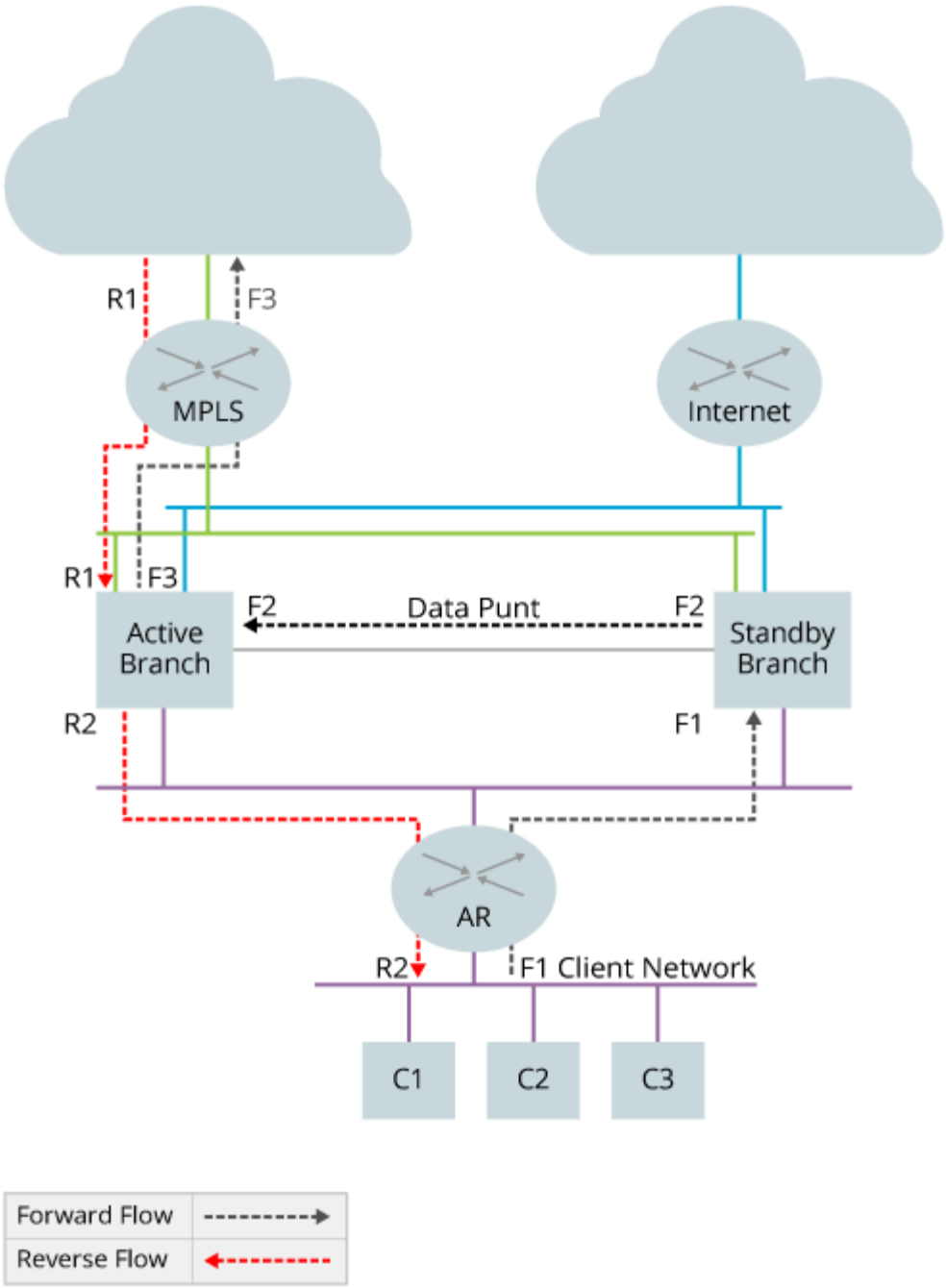
Before discussing the data path failures, it is useful to understand what a data path looks like in normal operation, when there are no failures in the data path. The following illustrates this situation. Here, forward direction traffic flows south to north on the two black paths labeled F1 and F2. Traffic traveling in the reverse direction flows along the two red paths labeled R1 and R2. Because there are no data path failures, all traffic in both directions flows through the active node.



Route Packets to Standby Node

In the forward direction traffic path, an access router might route packet traffic to the standby VOS device. The following figure illustrates this scenario. The standby device forwards the packets on the data punt path to the active VOS device.

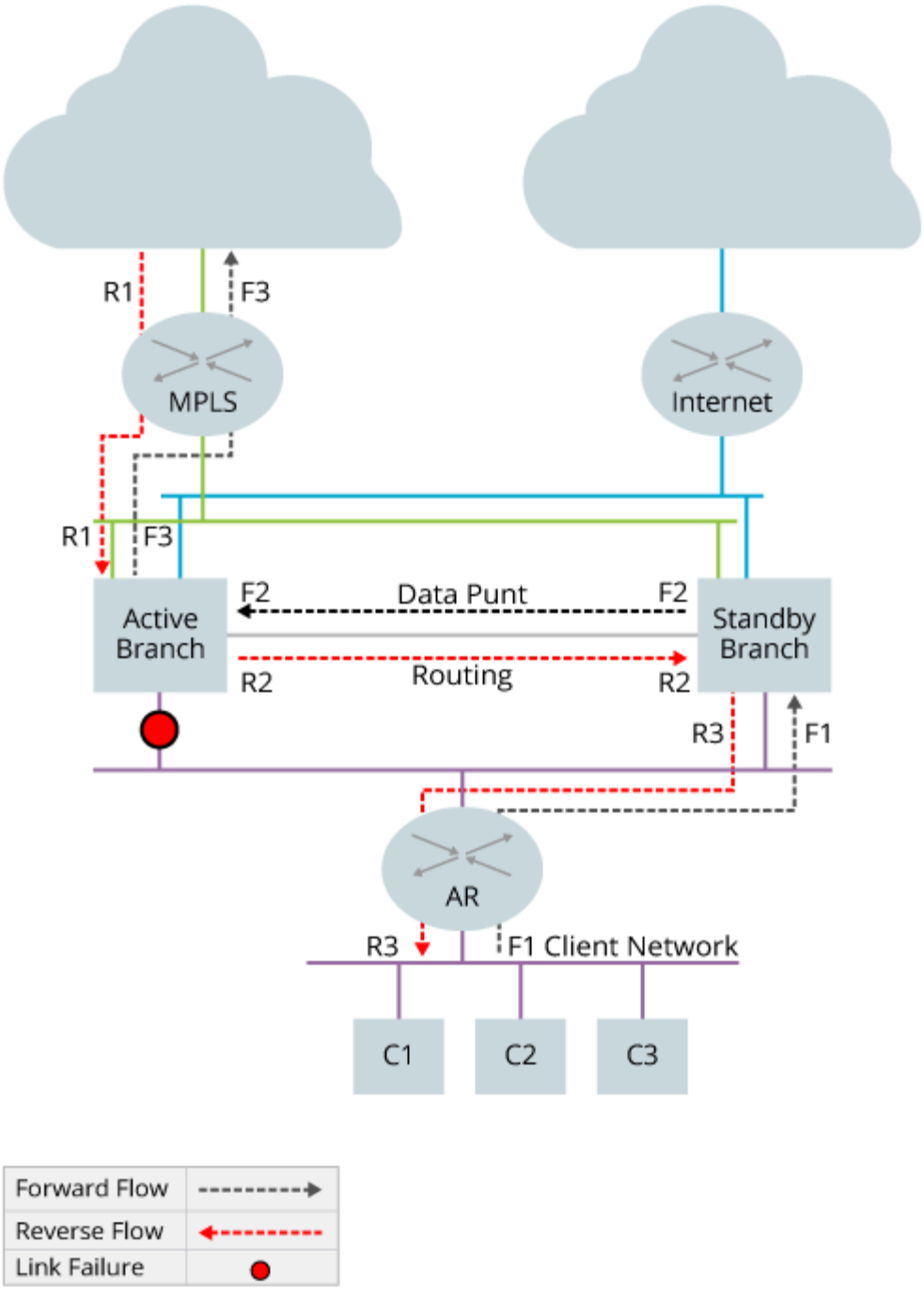
The active device applies any configured services to the packet traffic and then forwards it to the MPLS router. In the reverse direction, the packet traffic flows through the active VOS device and then to the access router.



Client-Side Link Failure

The figure below illustrates a case in which a client-side link failure occurs. Specifically, the link between the active VOS node and the access router in the client network fails, and the access router updates its routes so that traffic in the forward path direction is forwarded to the standby VOS node. For traffic traveling in the reverse direction, the Controller node updates its routes so that the next hop for return traffic is the standby VOS node, and the standby VOS node updates its routes to use the access router as the next hop for traffic heading south.

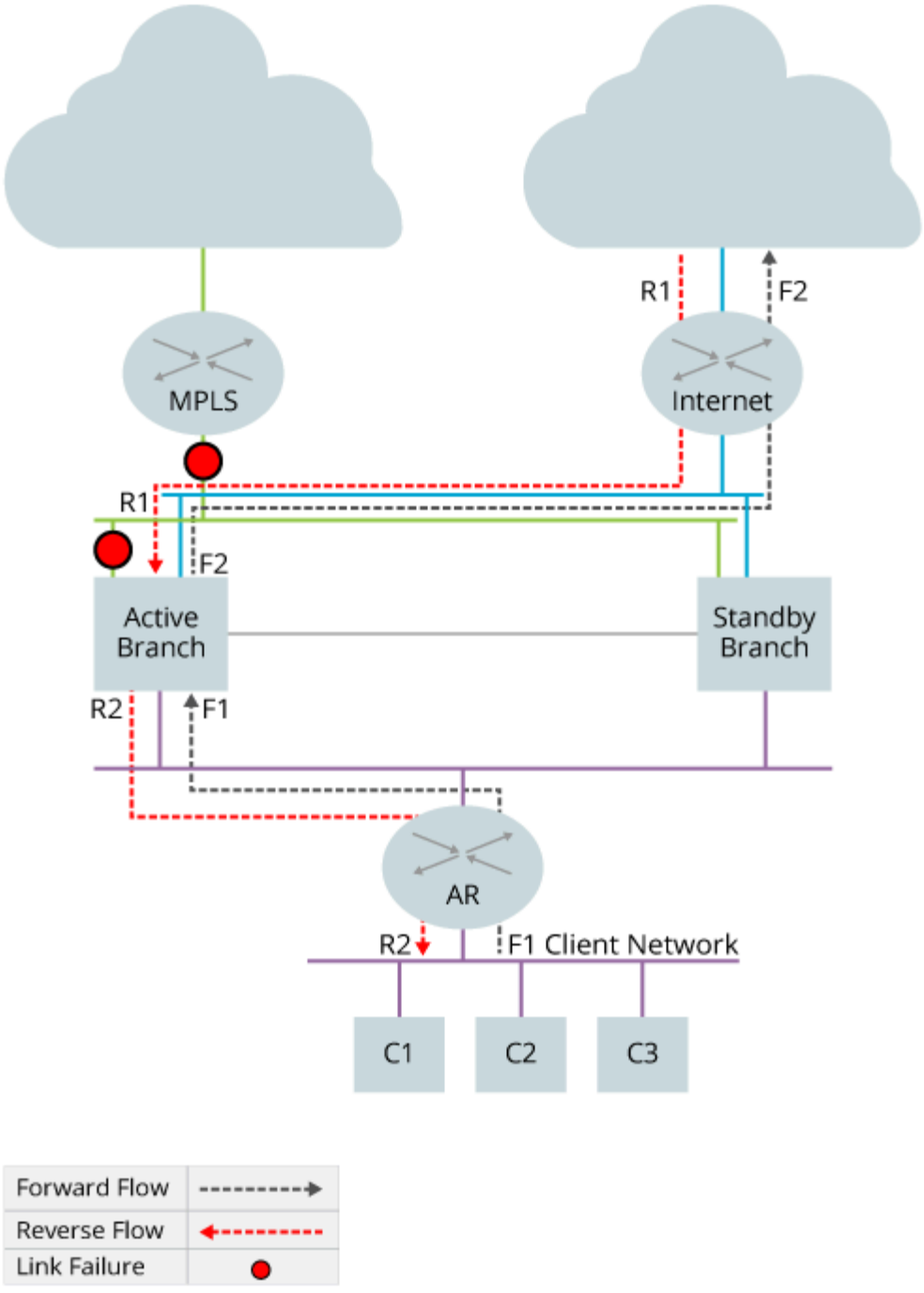
The standby VOS node passes traffic traveling in the forward direction to the active VOS node so that the active node can apply any configured services to the traffic. The active node then forwards the traffic to the MPLS router. In the reverse direction, the packet traffic flows through the active VOS device, which applies any configured services and forwards it to the standby VOS device. The standby device then forwards the traffic to the access router.



Access-Side Link Failure

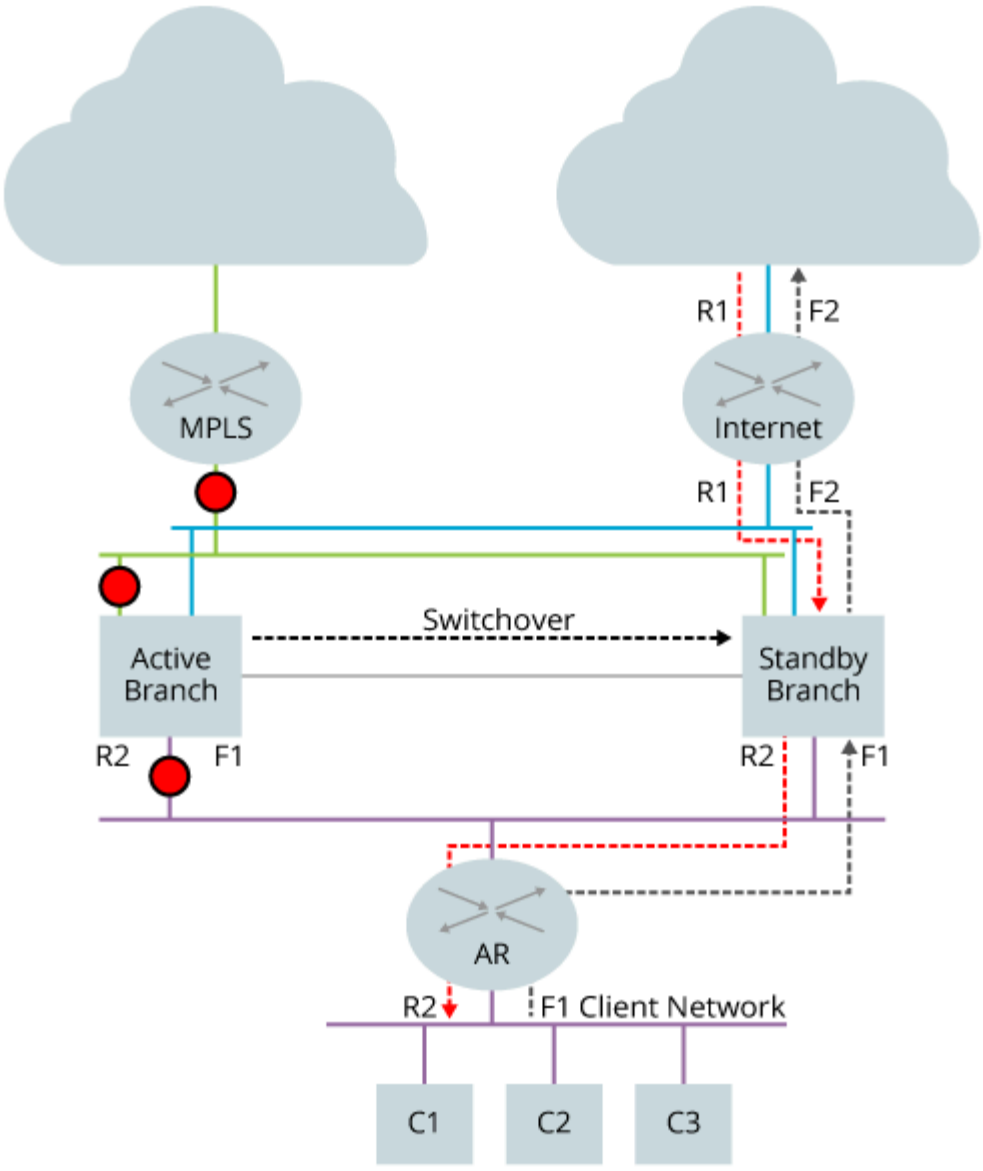
If the link between the active VOS node and the external network (which in this case is the MPLS network) fails, the SD-WAN Controller updates the routes on the active node so that the internet router is the preferred next hop for all

northbound traffic. In the reverse direction, the active node passes traffic to the access router. The following figure illustrates this failure scenario.



Failure of All Links

When the link between the access router and the active VOS node and the link between the active node and the MPLS network fail, a switchover occurs, and the standby VOS becomes the active router. The now-active node begins advertising better metrics to its neighboring routing peers, which then begin to direct traffic to this node instead of the previous active node. See the following figure.



Forward Flow	---------→
Reverse Flow	←---------
Link Failure	●

Before You Begin

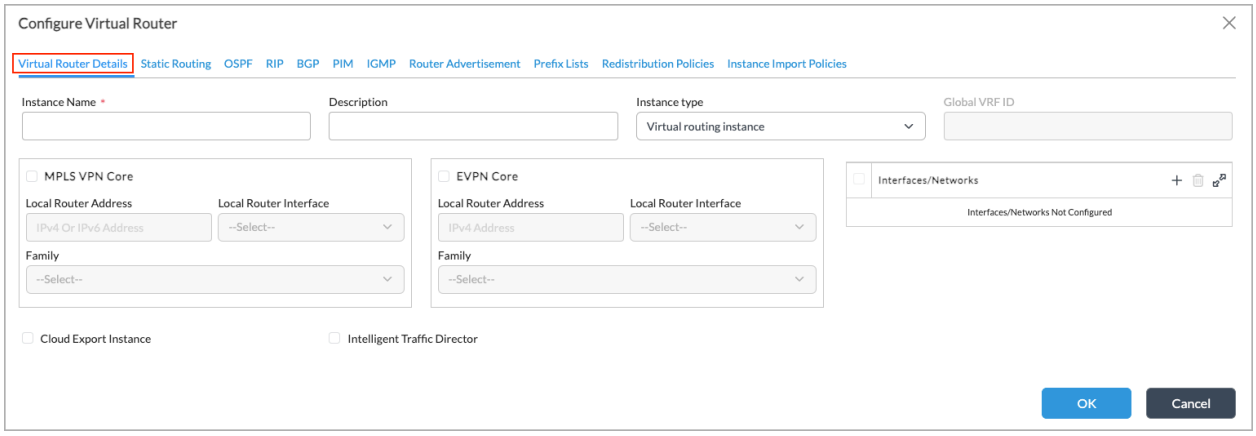
Before you begin configuring interchassis HA, ensure that you have met the software and hardware prerequisites.

Software Prerequisites

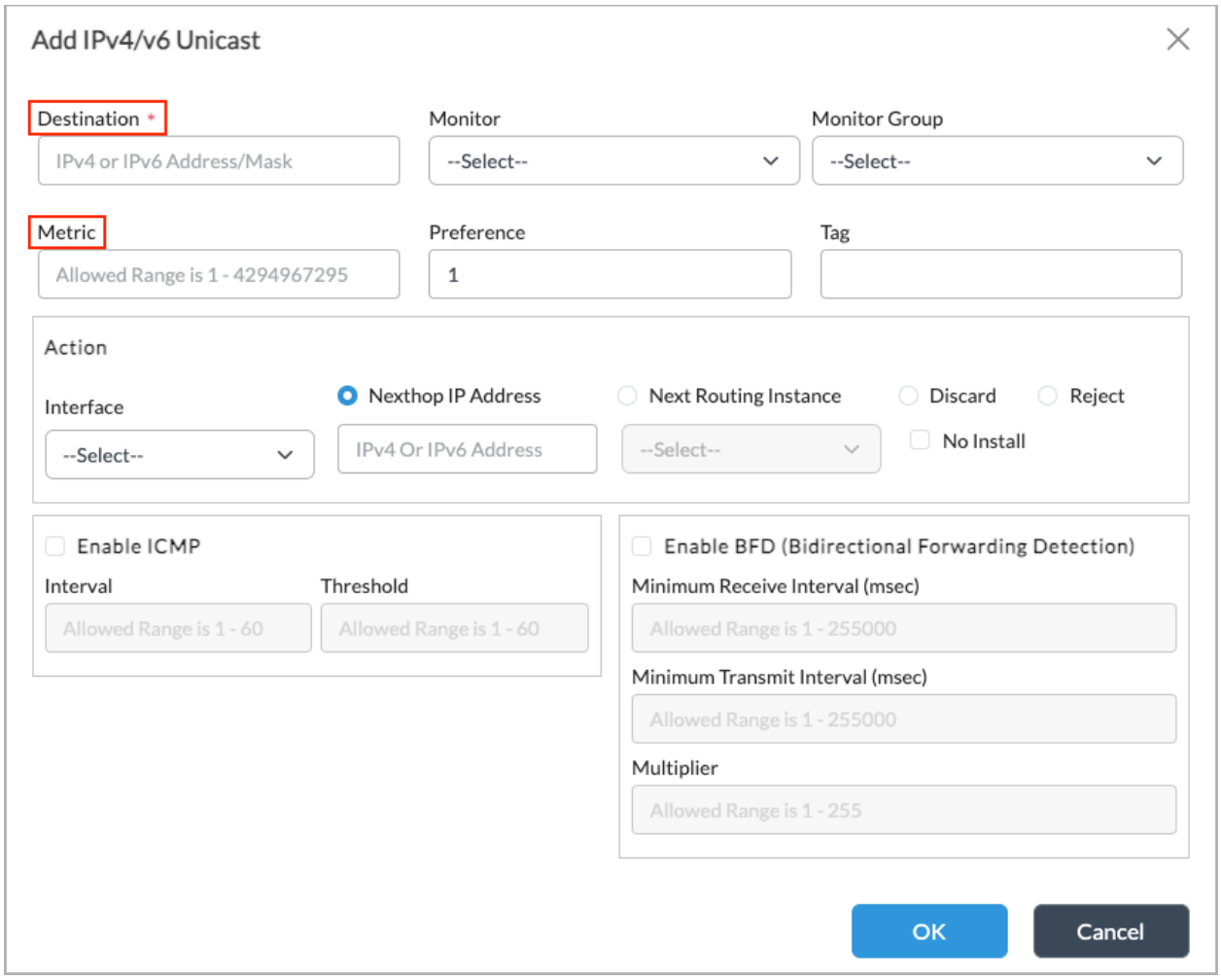
- Software version on both the active and standby VOS devices must be Release 16.1R2S8 or later.
- Ensure that the active and standby VOS devices have the same number of cores.
- Ensure that the active and standby VOS devices have the same amount of memory.
- Ensure that the active and standby VOS devices are running identical configurations.
- For the interface configuration:
  - Ensure that the active and standby VOS devices have the same number of interfaces.
  - Ensure that the interface numbering is the same on both devices.
  - In the devices template for the two VOS devices, in the Edit Templates > Interfaces tab, do not create a cross-connect interface.
  - Ensure that one physical interface is configured as a link over the back-to-back physical connection between the active and standby VOS devices.
  - Ensure that you have configured an external management interface or subinterface, to use for the HA control plane connection. The first figure in the overview section of this article illustrates this connection. If you use an external management or a loopback interface, this is a logical, or virtual, interface. For transferring HA control plane information, HA uses the back-to-back physical connection between the two VOS devices.
  - Ensure that you have configured a loopback interface to use for the HA data plane connection. The first figure in the overview section of this article illustrates this connection. The loopback interface is a logical, or virtual, interface, and the actual HA data plane information is transferred on the back-to-back physical connection between the two VOS devices.
- When you are configuring interchassis HA in the Interchassis > General screen, you need to select a routing instance and a control routing instance. You must create this new HA routing instance before you begin the interchassis HA configuration.
  - For the routing instance, create a new virtual router (for example, HA-Control-VR). This routing instance is used for the data sync connection over the dedicated sync interface. In the Interchassis > General screen, select this virtual router in the Routing Instance field. The procedure for creating this virtual router is given below.
  - For the control routing instance, you can configure this connection to go over a LAN interface using static routes, or you can configure it to go over the management interface. In the Interchassis > General screen, select this VR in the Control Routing Instance field.

  To create a new virtual router for the data sync connection:

  1. In Director view, select Configuration > Devices > Devices.
  2. Select an organization in the horizontal menu bar, and then select an appliance from the dashboard. The view changes to Appliance view.
  3. Select Configuration > Networking > Virtual Routers.
  4. Click the + Add icon. The Configure Virtual Router popup window displays.



5. Select the Virtual Router Details tab and specify an instance name. For more information, see the Configure Virtual Routers article.
6. Select the Static Routing tab and click the Add icon to add a static route for the virtual route instance.
    - Destination—Enter the IP address to monitor.
    - Metric—Enter the cost to reach the destination metric. The metric is used to choose between multiple paths learned with the same routing protocol.
    - For information about the remaining fields in this window, see the Configure Virtual Routers article.



7. Click OK.

- The control plane and the data plane must run on separate links, so ensure that you have created separate links for them. You can route the inter-RFD control connection over a LAN interface to avoid cascading faults on the data sync interface. Configuring the data sync connection over a dedicated interface helps to aggregate the sync data from the user data, and also the bandwidth used is directly proportional to the number of sessions.

- If you are updating the active and standby VOS devices in an interchassis HA pair, you must update the device template of the standby VOS device first, before you update the device template of the active VOS device. You must perform the operations in this sequence so that the two VOS devices synchronize properly. If you perform the update out of order, the state of the standby VOS device becomes SYNC-DISABLED. If this occurs, a workaround is to first ensure that the active and standby VOS device configurations are identical and then to restart the standby VOS device.

Hardware Prerequisites

To support stateful HA, the active and standby VOS devices must each have at least four cores. In addition, the device's

CPU and memory specifications must match for Active-Standby synchronization to function properly.

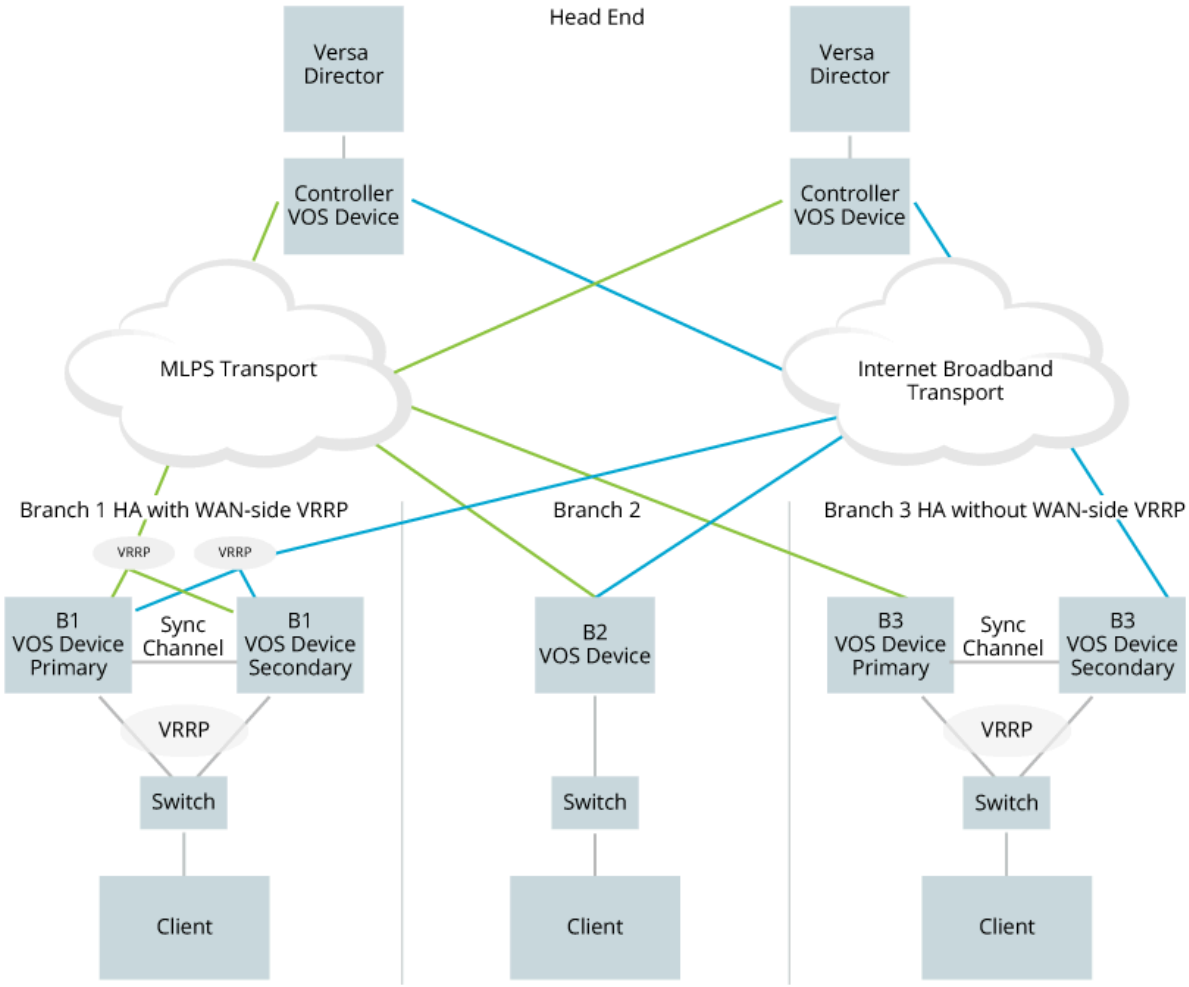
For additional hardware requirements, contact Versa Customer Support.

Configure Interchassis HA

You configure the pair of VOS devices to be interchassis HA peers by choosing one of the peer devices, which is referred to as the local device, and configuring interchassis HA on that device. In the process of configuring interchassis HA, you define the VOS device that is the other interchassis HA peer. This peer is referred to as the remote device. It does not matter which of the two devices you perform the configuration on. As a result of the configuration, one of the interchassis HA peers becomes the active peer and the other one becomes the standby.

Note: You can configure interchassis HA using Device templates or, for Releases 22.1.1 and later, using Workflow templates, as described in this article. You can also use the Workflow template to configure an active-active device configuration, but that is different from the active-standby configuration for interchassis HA.

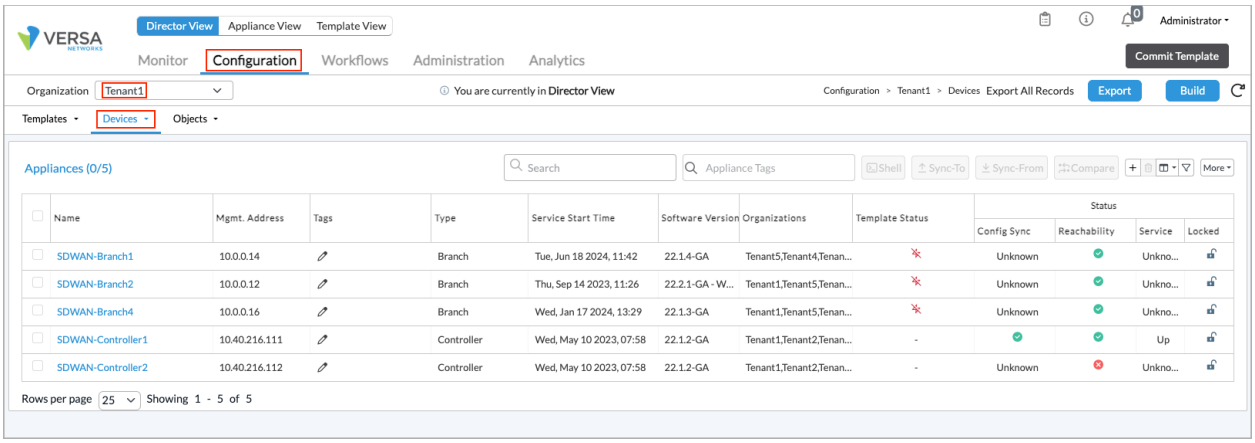
You can deploy interchassis HA with a single transport or a dual transport, and with or without VRRP enabled on the WAN side. The figure below illustrates these deployments.



Configure Basic Interchassis HA Using Device Templates

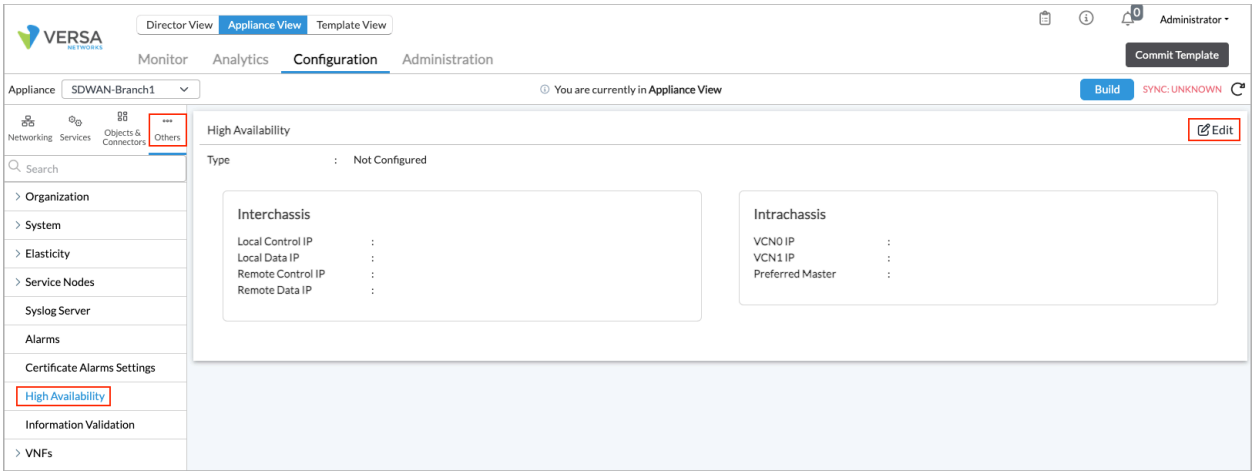
To configure basic interchassis HA using device templates, follow these steps. To configure interchassis HA using Workflow templates, see Configure Basic Interchassis HA Using Workflow Templates.

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select an organization in the horizontal menu bar.
    c. Select Devices > Devices in the horizontal submenu bar.

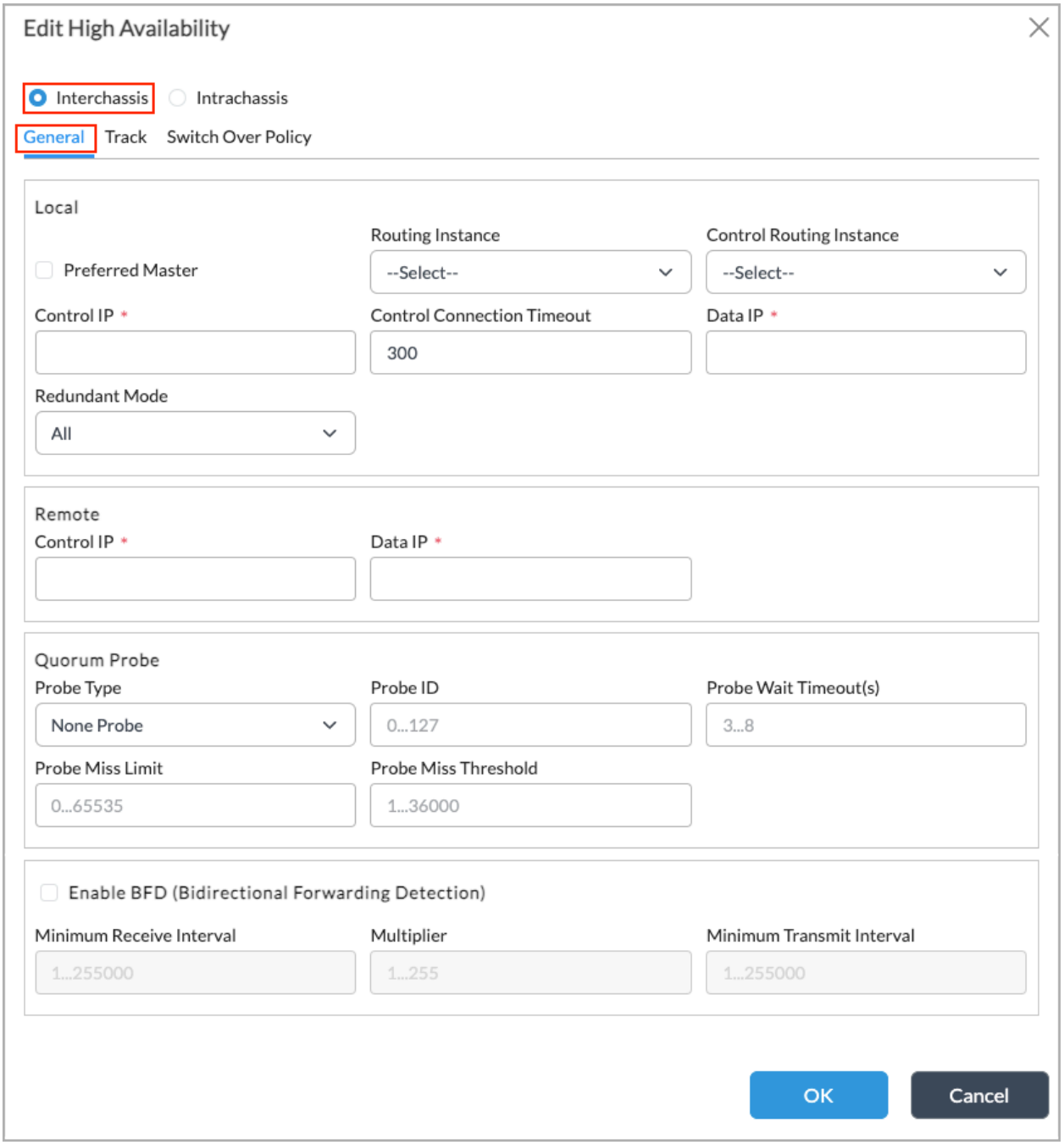


d. Select a device in the Devices table in the main pane. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.
3. Select Others > High Availability in the left menu bar. The High Availability window displays.



4. In the High Availability pane, click the Edit icon. The Edit High Availability popup window displays.



5. Click Interchassis. In the General tab, you configure the active and standby VOS devices. Enter information for the following fields. You must configure all the fields on this popup window.

Field	Description
Local (Group of Fields)	Configure interchassis HA parameters for the local VOS device, which is the device you selected in Step 1d, above.
◦ Preferred Master	Click to have the local VOS device be the active HA device. If you do not click this box, the remote VOS device is the active HA device. The preferred active HA device is the VOS device that takes the active role when the interchassis HA peers come up for the first time. It also that takes the active role when there is a conflict between the two peers.
◦ Routing Instance	Select the routing instance on the active device that contains the interface to use for the data TCP connection, which performs stateful synchronization and replication. You need to select this routing instance if you configure the data TCP connection interface in a different routing instance (VNF). If you do not select a routing instance, the interface is assigned to a global routing instance (a routing instance with ID 0), and you do not need to configure the routing interface in the redundancy configuration. Ensure that the interface for the data TCP connection belongs to a tenant. Traffic that does not belong to a tenant is dropped.
◦ Control Routing Instance	Select the routing instance to use for the control TCP connection, which is used for peer discovery and role negotiation. You need to select this routing instance if you configure the control TCP connection interface in a different routing instance (VNF). If you do not select a routing instance, the interface is assigned to a global routing instance (a routing instance with ID 0), and you do not need to configure the routing interface in the redundancy configuration. Ensure that the interface for the control TCP connection belongs to a tenant. Traffic that does not

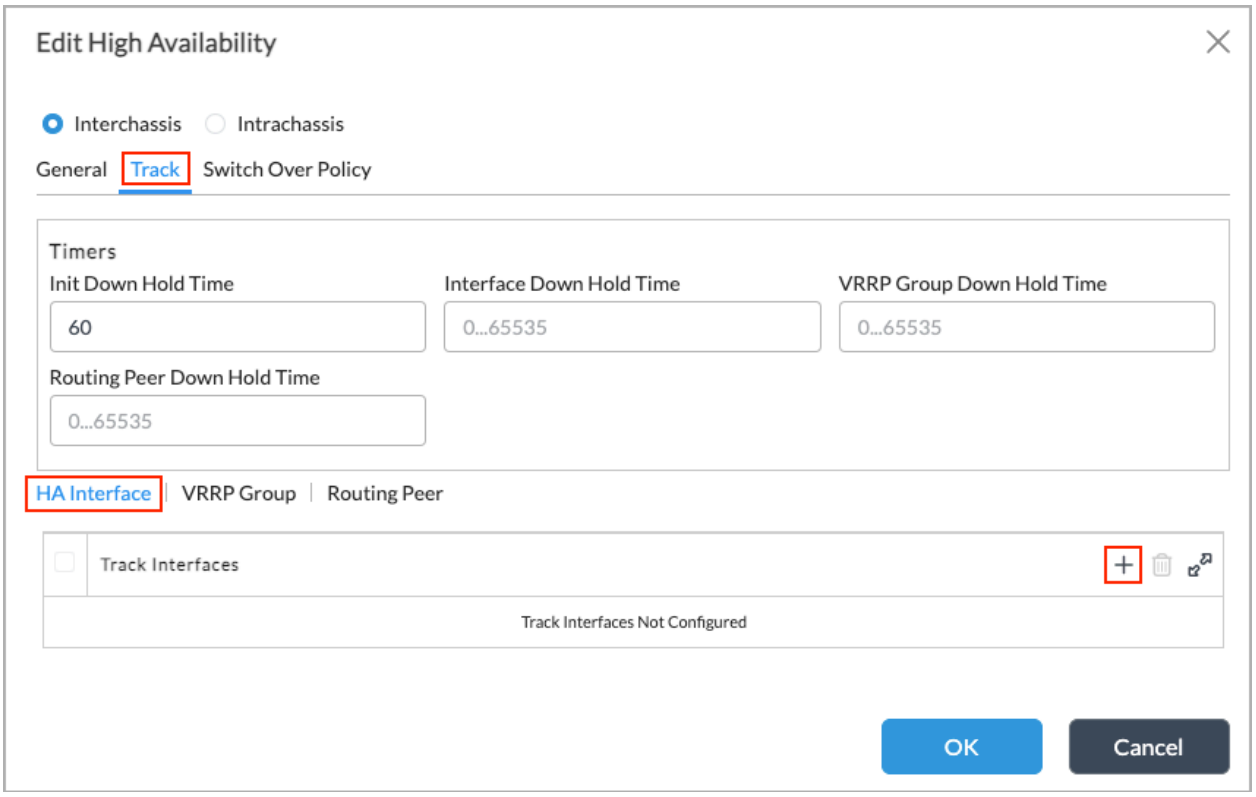
	belong to a tenant is dropped.
◦ Control IP	Enter the IP address of the external management interface on the local device to use for the control plane connection. If you assign the external management interface to a separate routing instance (VRF), ensure that the redundancy configuration refers to the same routing instance. If you do not configure a routing instance, the interface is assigned to a global routing instance (a routing instance with ID 0), and you do not need to configure the routing interface in the redundancy configuration. Ensure that the external management interface belongs to a tenant. Traffic that does not belong to a tenant is dropped.
◦ Control Connection Timeout	During the boot process, enter how long a VOS device waits for its peer to connect before declaring itself to be the active device. *Range*: 5 through 10000 seconds *Default*: 180 seconds; 300 seconds (for Releases 20.2 and later) *Recommended:* 180 seconds
◦ Data IP	Enter the IP address of the loopback interface on the local device to use for the HA data plane connection. Note that interchassis HA uses a loopback IP address for stateful replication. You can assign this IP address to a loopback interface (for example, lo0) or to a physical interface. If you assign it to a loopback interface, add the static route to the routing instance configuration so that the loopback address is reachable over a VNI interface (for example, over vni-0/3). Both the lo0 and vni-0/3 interfaces must

	belong to the same routing instance. If you assign the loopback interface to a different routing instance (VNF), ensure that the redundancy configuration refers to the same routing instance Ensure that the loopback interface belongs to a tenant. Traffic that does not belong to a tenant is dropped.
◦ Redundant Mode	Select All to allow the control plane, services, and all nodes to fail over to a redundant supervisor node when the software detects unrecoverable critical failures, service restartability errors, kernel errors, or hardware failures.
Remote (Group of Fields)	Configure interchassis HA parameters for the HA peer VOS device.
◦ Control IP	Enter the IP address of the external management interface on the remote device to use for the control plane connection. If you assign the external management interface to a separate routing instance (VNF), ensure that the redundancy configuration refers to the same routing instance. If you do not configure a routing instance, the interface is assigned to a global routing instance (a routing instance with ID 0), and you do not need to configure the routing interface in the redundancy configuration. Ensure that the external management interface belongs to a tenant. Traffic that does not belong to a tenant is dropped.
◦ Data IP	Enter the IP address of the loopback address on the remote device to use for the HA data plane connection. If you assign the loopback interface to a separate

	routing instance (VNF), ensure that the redundancy configuration refers to the same routing instance. If you do not configure a routing instance (VNF), the interface is assigned to a global routing instance (a routing instance with ID 0), and you do not need to configure the routing interface in the redundancy configuration. Ensure that the loopback interface belongs to a tenant. Traffic that does not belong to a tenant is dropped.
Quorum Probe (Group of Fields)	Configure the quorum properties used to arbitrate disputes between the active and standby interchassis HA peers
◦ Probe Type	By default, quorum probes are disabled, and the probe type is set to None-Probe. To enable the sending of quorum probes, select the probe type: ◦ Monitor-VOAE-Probe—Interchassis HA quorum uses both Director and monitor probes. It is recommended that you use this probe type. ◦ Monitor-Probe—Interchassis HA quorum uses only monitor probes. To use quorum probes, you must configure two or more monitor probes, as described in Configure Monitor Probes, below.
◦ Probe ID	Enter a unique integer that is included in quorum probe packets to identify the HA pair. *Range:* 0 through 127 *Default:* 2
◦ Probe Wait Timeouts	Enter how long the VOS device waits for a reply from the Director node regarding the status of its peer active node. *Range:* 3 to 8 seconds *Default:* 4 seconds *Recommended:* 4 seconds
◦ Probe Miss Limit	Enter how long the standby VOS device waits after seeing no probes before it declares the active VOS device to be dead. *Range:* 0 to 4294967295 seconds

	Default: 3 seconds *Recommended:* 3 seconds, or probe wait timeout value minus 1
Enable BFD	Click to enable the Bidirectional Forwarding Detection protocol between the interchassis HA peer devices. BFD checks the health of the TCP data connection between the HA peers.
◦ Minimum Receive Interval	Enter the minimum tine interval in which an HA peer device must receive a reply from its HA peer device, in milliseconds. *Range:* 1 through 255000 milliseconds *Default:* None *Recommended:* 500 milliseconds
◦ Multiplier	Enter the BFD multiplier value. This value is multiplied by the minimum receive interval time. The resulting value is the number of consecutive BFD packet drops that can occur before the receiving HA peer devices assumes that the TCP data connection to its HA peer is down. If you have configured quorum, when the TCP data connection is declared to be down, a quorum evaluation is triggered. If you have not configured quorum, when the TCP data connection is declared to be down, the standby HA peer switches over to become the active HA peer. *Range:* 1 through 255 *Default:* none *Recommended:* 8 milliseconds
◦ Minimum Transmit Interval	Enter how often to send BFD packets to the HA peer device, in milliseconds. *Range:* 1 to 255000 milliseconds *Default: N*one *Recommended:* 500 milliseconds

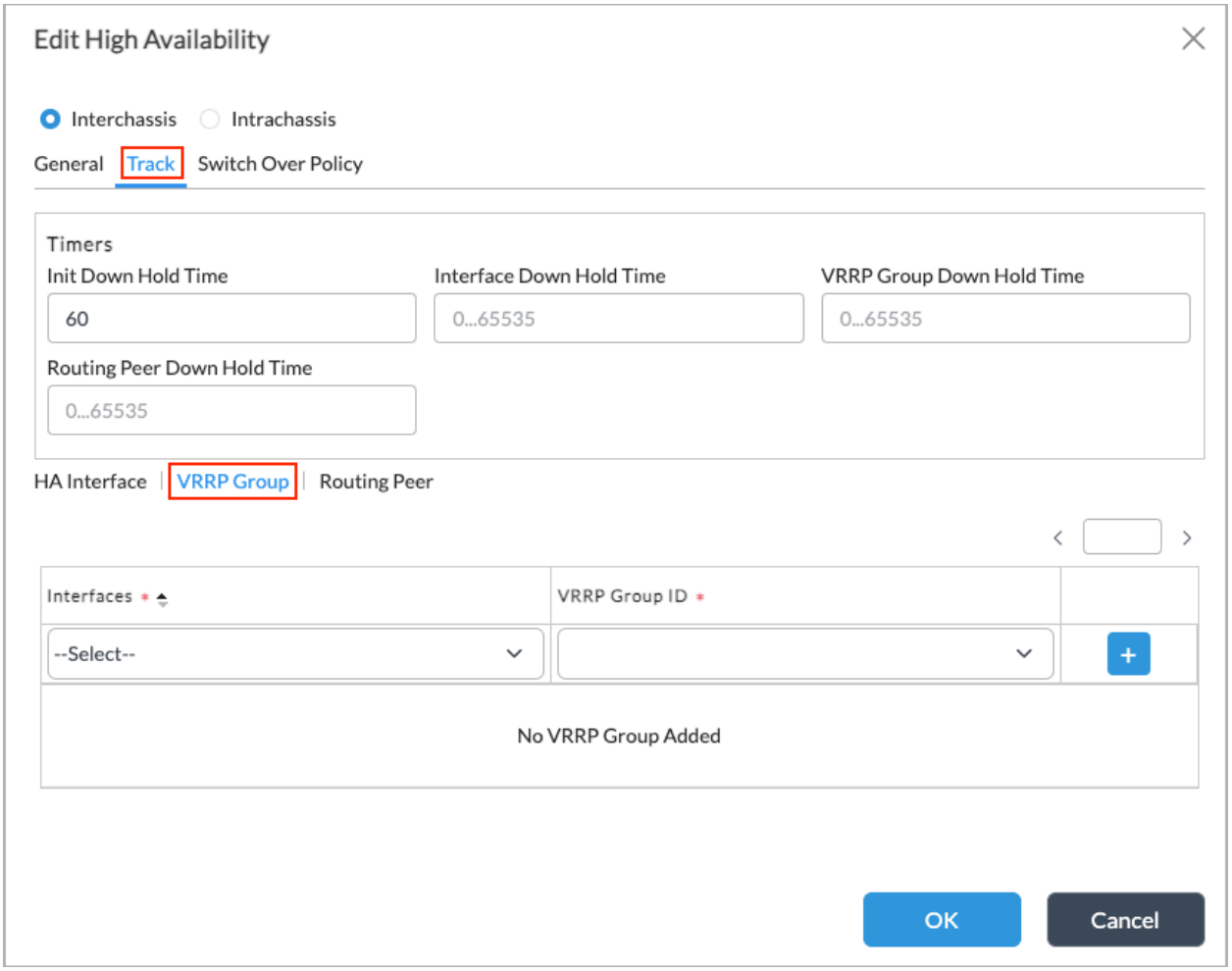
6. Click the Track tab. In this tab, configure the downtime settings for the active interchassis HA device. Configure information for the following fields. You must configure all fields on the Interchassis > Track screen and on the HA Interface tab.



Field	Description
Timers (Group of Fields)	
◦ Init Down Hold Time	Enter the length of time after the active HA VOS device finishes booting for the first time before evaluating the switchover policy. This timer runs once, when the active VOS device completes booting. This warmup timer allows a period of time to pass so that the VOS can establish itself as the active HA device. *Range:* 0 through 4294967295 seconds *Default:* 60 seconds
◦ Interface Down Hold Time	Enter the length of time after an interface on the active HA VOS device goes down before generating an alarm that triggers the evaluation of the switchover policy. This damping time allows an interface to recover from a down event, with the intent of minimizing the number of times that the standby device becomes the active device. If you do not configure a value for this hold time, an interface down event generates an alarm immediately. *Range:* 0 through 4294967295 seconds *Default:* None *Recommended:* 5 seconds
◦ VRRP Group Down Hold Time	Enter the length of time after a VRRP group on the active HA VOS device transitions from Active state to Backup state or from Active state to Init state before generating an alarm that triggers the evaluation of the switchover policy. This damping time allows a VRRP group to recover to the Active state, with the intent of minimizing the number of times that the standby device becomes the active device. If you do not configure a value for this hold time, a VRRP group state transition generates an alarm immediately. *Range:* 0 through 4294967295 seconds *Default:* None *Recommended:* 5 seconds
◦ Routing Peer Down Hold Time	Enter the length of time after the state of a BGP routing peer of the active HA VOS device transitions to a state other than Established before generating an alarm that triggers the evaluation of the switchover policy. This damping time allows a BGP peering session to recover, with the intent of minimizing the number of times that the standby device becomes the active device. If you do not configure a value for this hold time, a BGP peer state transition to Disconnected generates an alarm immediately. *Range:* 0 through 4294967295 seconds *Default:* None

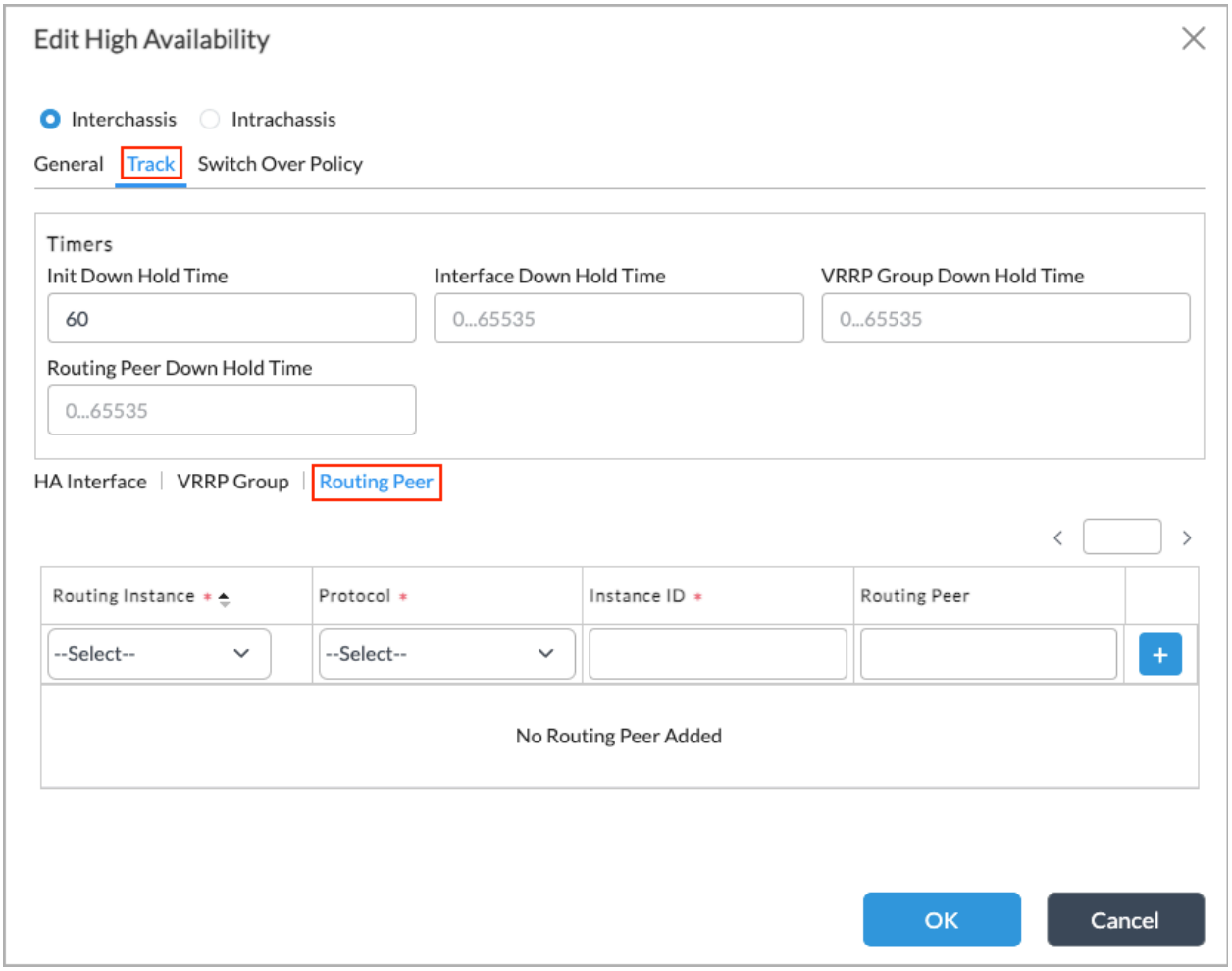
	Recommended: 5 seconds
HA Interface	In the HA Interface tab in the Track tab, if you are tracking HA interface initialization, click Track Interfaces and specify the interfaces to track.

7. In the Track tab, if you are tracking VRRP group initialization, click the VRRP Group tab. You must configure all fields on this tab.



Field	Description
Interfaces	Select the interface for the VRRP group.
VRRP Group ID	Select the VRRP group ID.

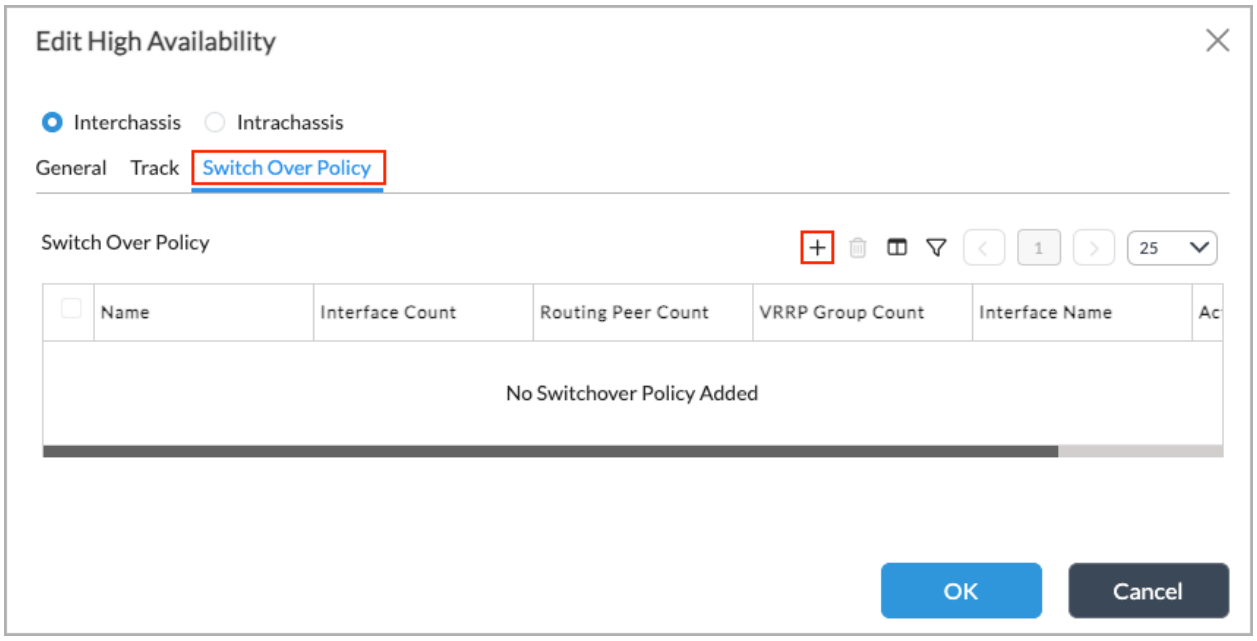
8. Click the Add icon to add the interface.
9. In the Track tab, if you are tracking route establishment, click the Routing Peer tab. Configuring the fields on this popup window is optional.



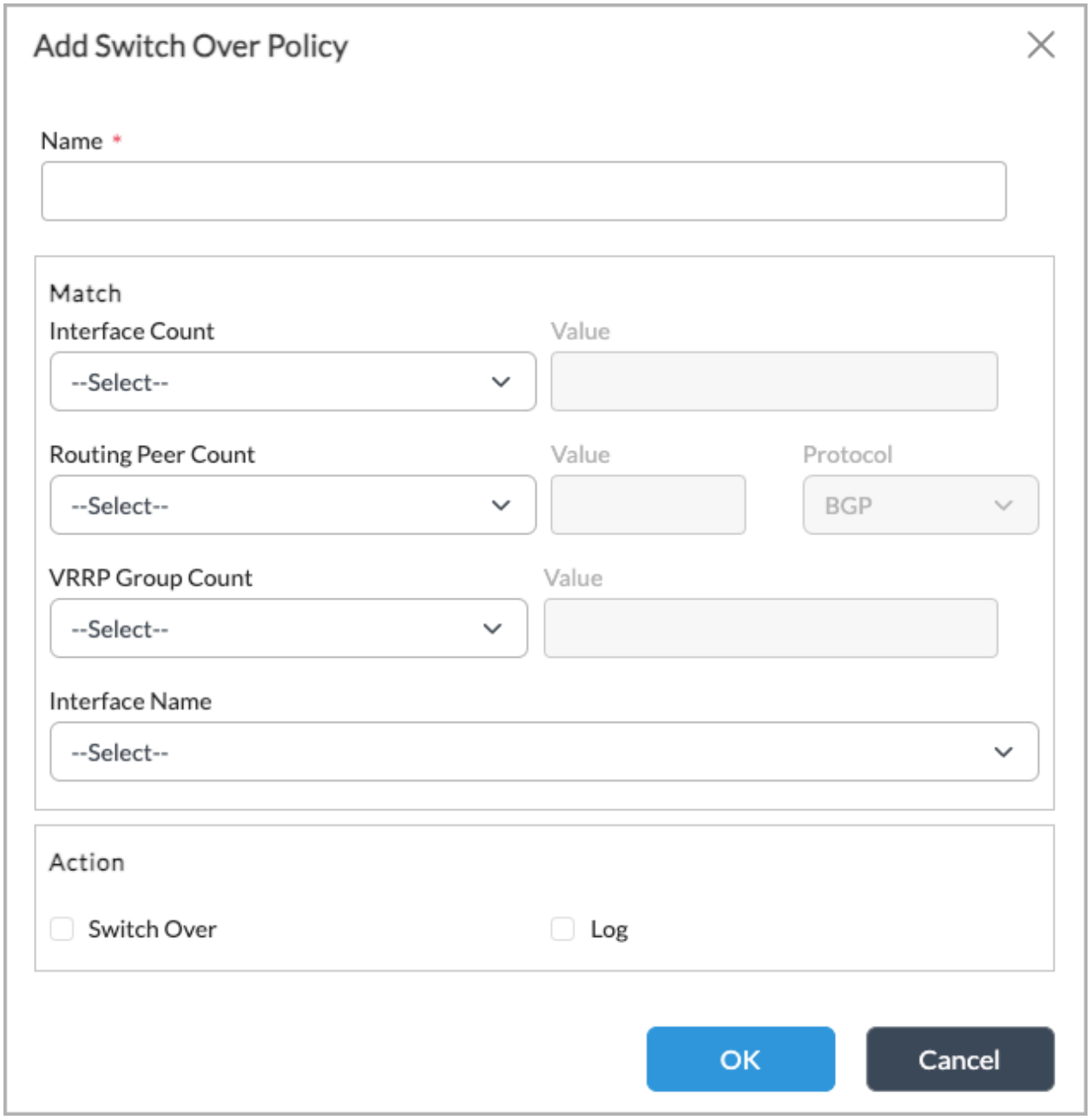
Field	Description
Routing Instance	Select the routing instance of the data links.
Protocol	Displays the protocol used by the routing peer.
Instance ID	Select the instance ID of the routing peer.
Routing Peer	Select the name of the routing peer.

10. Click the Add icon to add the routing peer.
11. Click the Switchover Policy tab to configure the policies to use for switching between the active and standby HA nodes. You must configure a switchover policy.
    A switchover trigger policy defines how and when to switch from the active to the standby node. You define the switchover triggers based on the interface, routing peers, and VRRP groups you want to track. For each of these, you configure a condition, and when all the conditions are met, the system takes the configured action. If the action you configure is to switch over, and if the standby node has a greater number of tracked routing peers, active interfaces, and active VRRP groups, the system switches over so that the standby node becomes the active node.

The lower watermark values defined by the interface count, routing peer count, and VRRP group count match conditions in a rule are a logical AND operation. Different rules are evaluated with a logical OR operational. That is, when you configure more than one rule, the first rule that matches is executed, and no further rules are evaluated.
Note that if the LAN interface on the active VOS device is down, it is recommended that you perform a switchover to make the standby VOS device into the active VOS device. To have the switchover happen automatically, configure a switchover policy with redundancy so that when a LAN interface on the active VOS device goes down, the switchover is triggered automatically.



12. Click the + Add icon, and enter information for the following fields.



Field	Description
Name	Enter a name for the switchover policy.
Match (Group of Fields)	
◦ Interface Count	Select whether the interface count is less than or less than or equal to the number given in the Value field.
◦ Value	Enter the number of interfaces to match to trigger a switchover.
◦ Routing Peer Count	Select whether the routing peer count is less than or less than or equal to the number given in the Value field.
◦ Value	Enter the number of routing peers to match to trigger a switchover.
◦ Protocol	Displays the protocol running on the interface.
◦ VRRP Group Count	Select whether the VRRP group count is less than or less than or equal to the number given in the Value field.
◦ Value	Enter the number of VRRP groups to match to trigger a switchover.
◦ Interface Name	Select the interface to match to trigger a switchover.
Action (Group of Fields)	Specify the actions to take when the switchover match conditions are met.
◦ Switch Over	Have standby device take over as the active device.
◦ Log	Log the switchover event.

11. Click OK.
12. If you have configured or modified any of the fields on any screens on the Edit High Availability window, you must issue a vsh restart command to restart all Versa services so that the HA service can take affect. Issuing this command does affect the availability of services until they restart.

After you have deployed the Device template on the first VOS device, configure the second device. To maintain consistency between the configurations on the active and standby HA VOS devices, it is recommend that you place them both into a single device group template.

Configure Basic Interchassis HA Using Workflow Templates

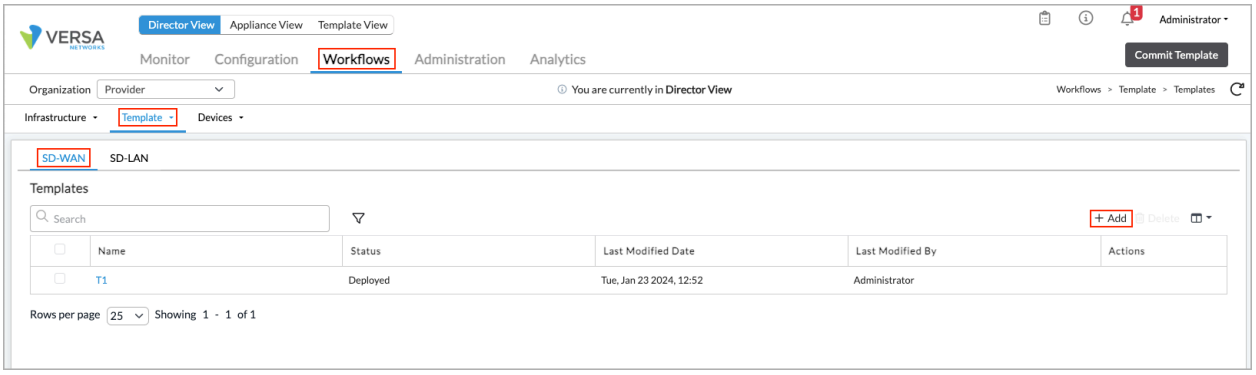
You can use Workflow templates to configure active-standby appliances in an HA configuration. Unlike an active-active redundant pair configuration, which generates two temples (one for each active device), the active-standby interchassis HA configuration generates only one template, which is associated with both the active and standby appliances. The standby appliance receives traffic but only the active appliance can take action on the traffic. A cross-connect link between the active and standby devices provides the communication path between the devices.

To configure basic interchassis HA using workflow templates:

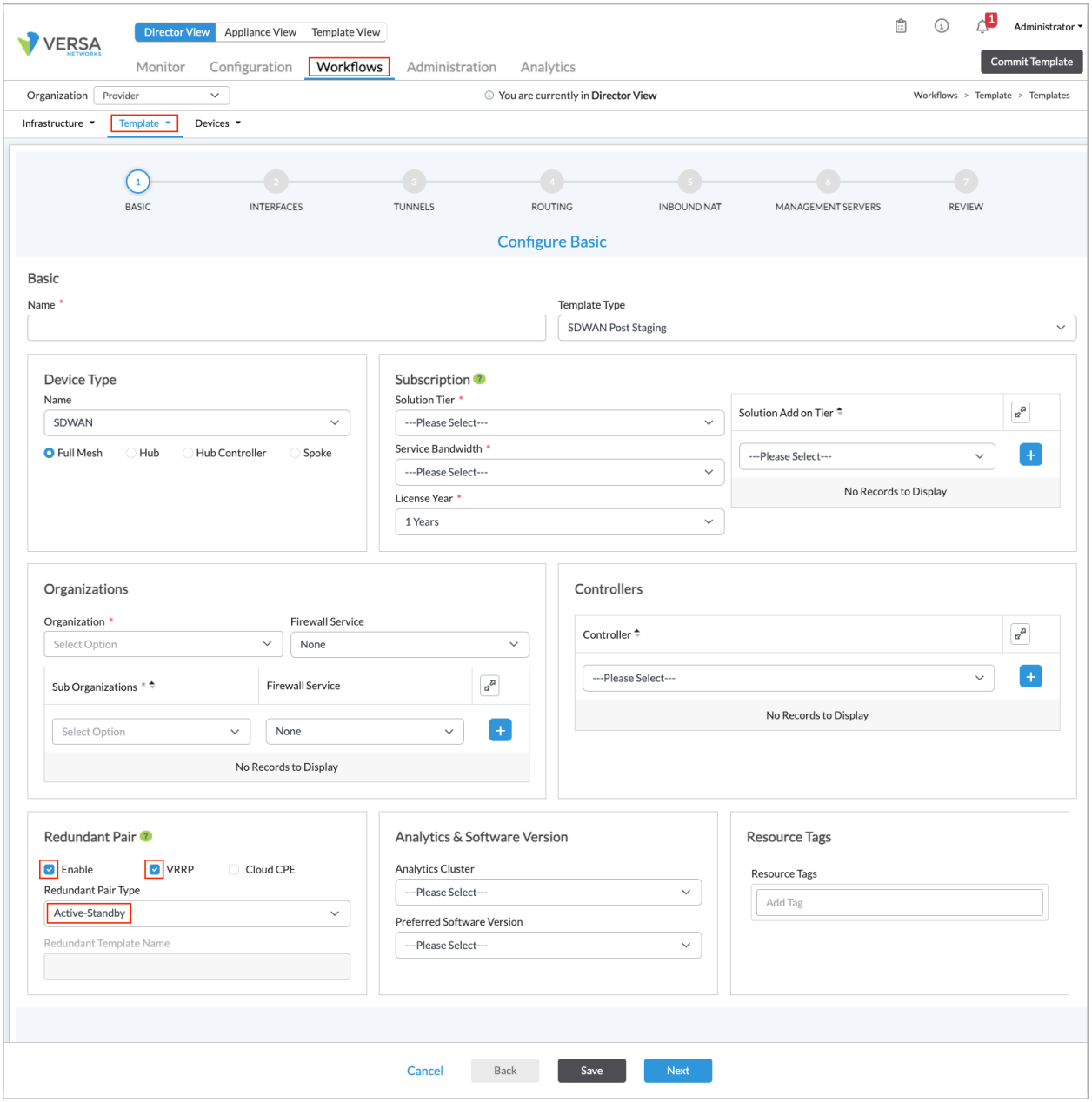
- Create an active-standby template
- Onboard an appliance using the template

Create an Active-Standby Template

1. In Director view, select the Workflows tab in the top menu bar, then select Template > Templates from the horizontal menu bar and SD-WAN from the horizontal submenu.
2. Select SD-WAN in the horizontal submenu.

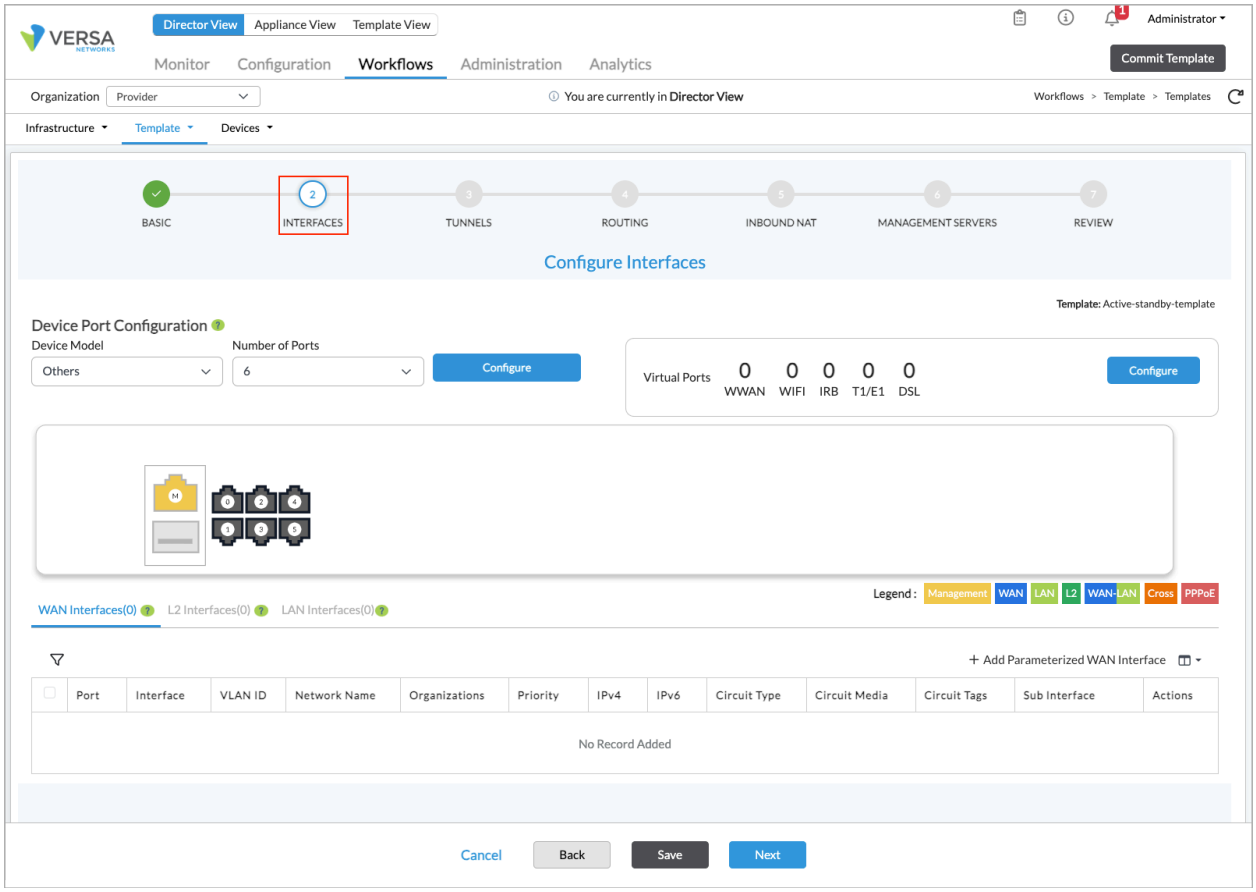


3. Select an existing template, or click the + Add icon to create a new template. The following screen displays with Step 1, Basic, selected by default.

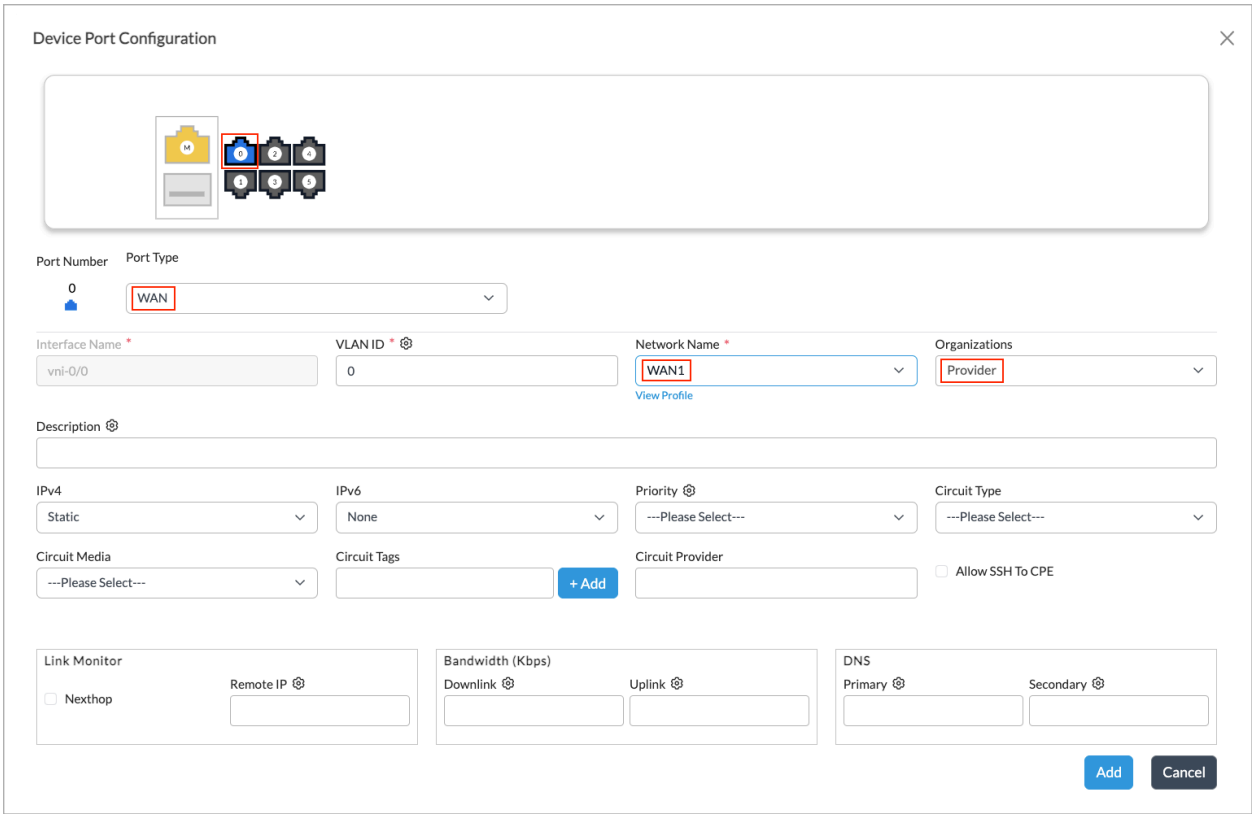


4. In the Redundant Pair section, click Enable to enable the redundant pair. It is recommended that you also click VRRP to enable the virtual router redundancy protocol, which allows the standby appliance to take over if the active appliance fails.
5. Click Next to go to Step 2, Interfaces. In the Configure Interfaces screen. The screen displays a representation of the interfaces on an appliance. You can choose a specific appliance model using the Device Model drop-down menu. Depending on the model selected, you can configure the following interface types:
    - Management
    - WAN
    - LAN
    - L2

- WAN-LAN
- Cross
- PPoE

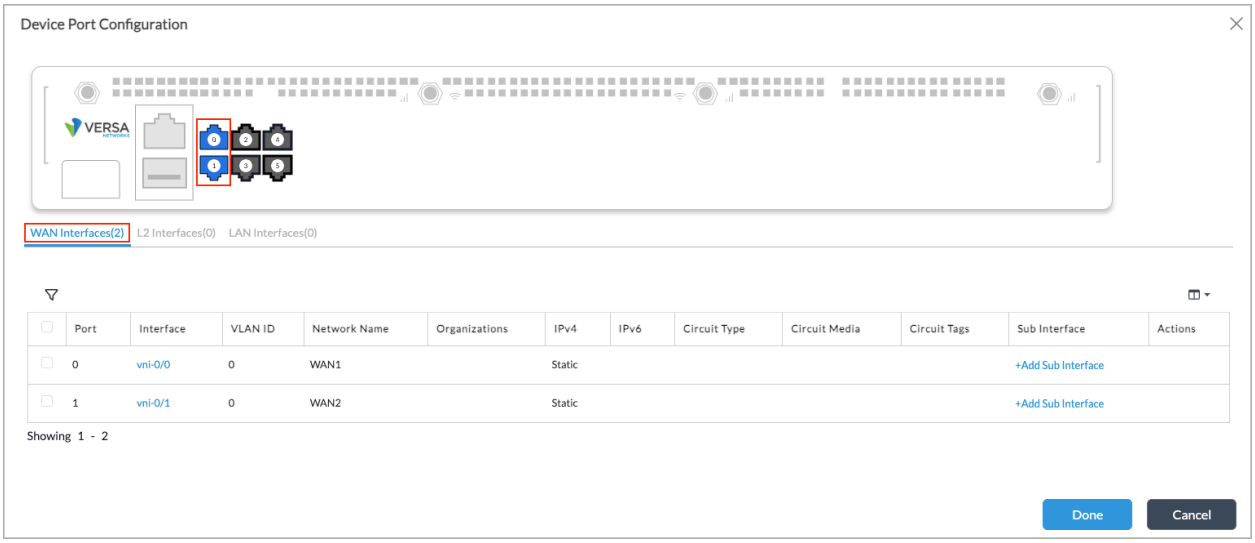


6. Configure one or more WAN interfaces by entering information for the following fields.

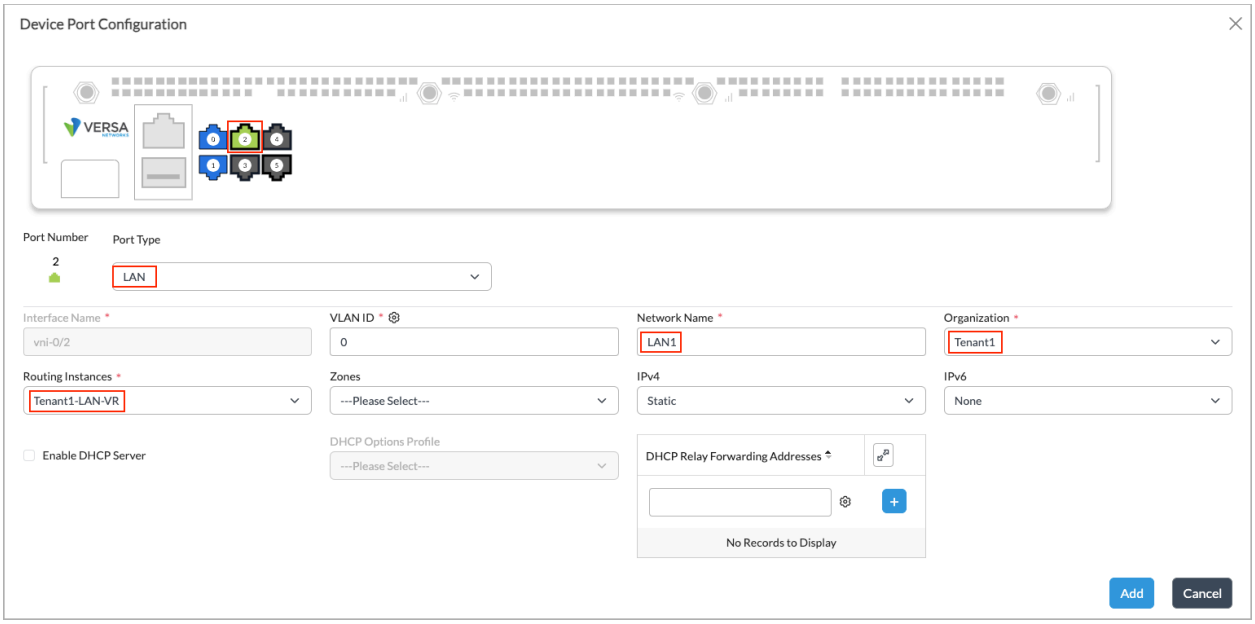


Field	Description
Device Port Configuration	Click a port in the diagram.
Port Type	Select WAN from the list.
Network Name	Select the name of a WAN network.
Organization	Select the organization to which the appliance belongs.

7. Click Add to add the WAN interfaces. The Device Port Configuration screen now shows the configured WAN interfaces. Port 0 and port 1 are now blue WAN interfaces and they are listed under the WAN Interfaces tab.



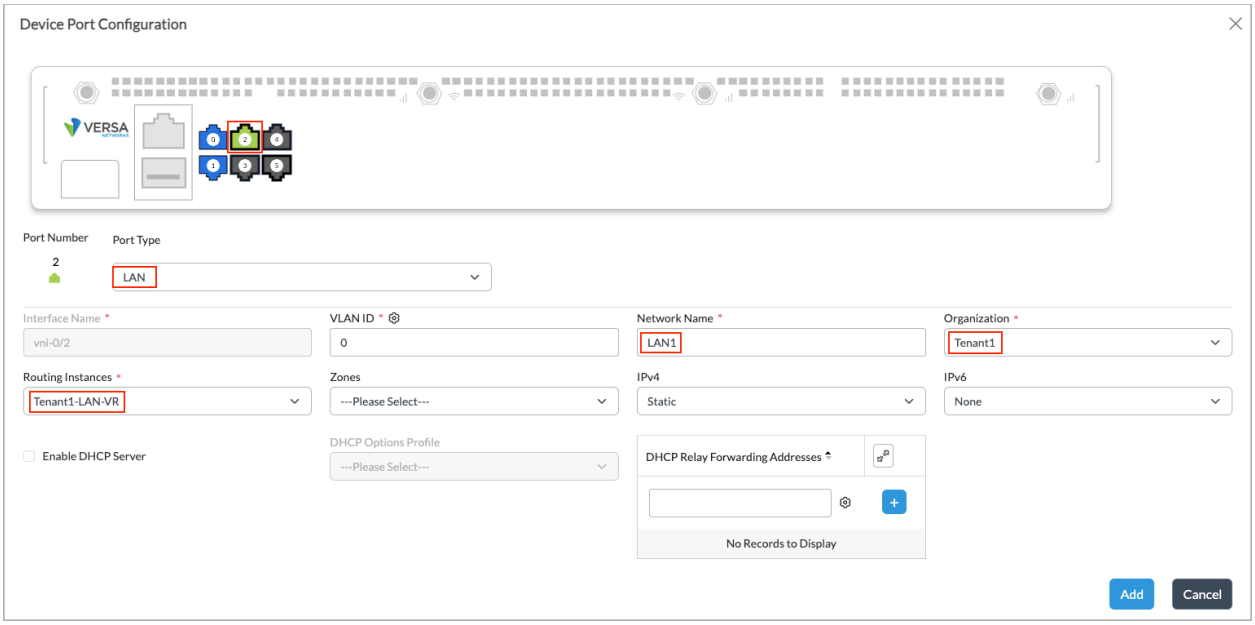
8. Configure a LAN interface by entering information for the following fields.



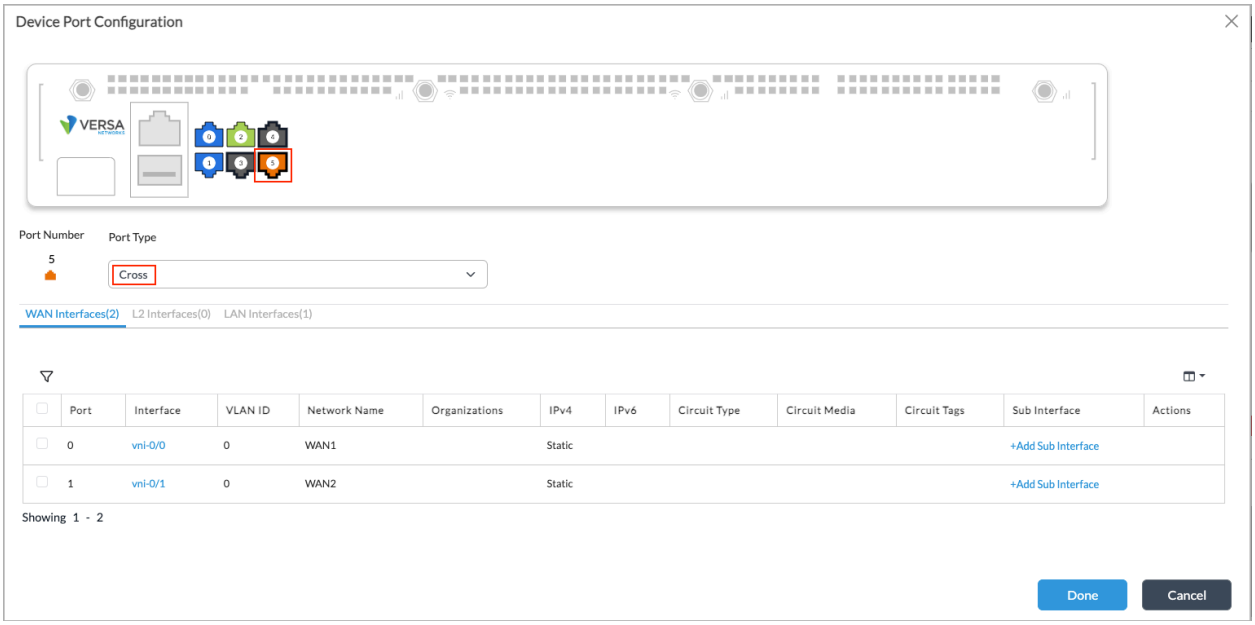
Field	Description
Device Port Configuration	Click a port in the diagram.
Port Type	Select LAN from the list.
Network Name	Select or enter a name for the LAN network.
Organization	Select the organization to which the appliance belongs.

Field	Description
Routing Instances	Select a LAN-VR routing instance.

9. Click Add to add the LAN interface. The Device Port Configuration screen now shows the configured LAN interface. Port 2 is now a green LAN interfaces and they is listed under the LAN Interfaces tab.

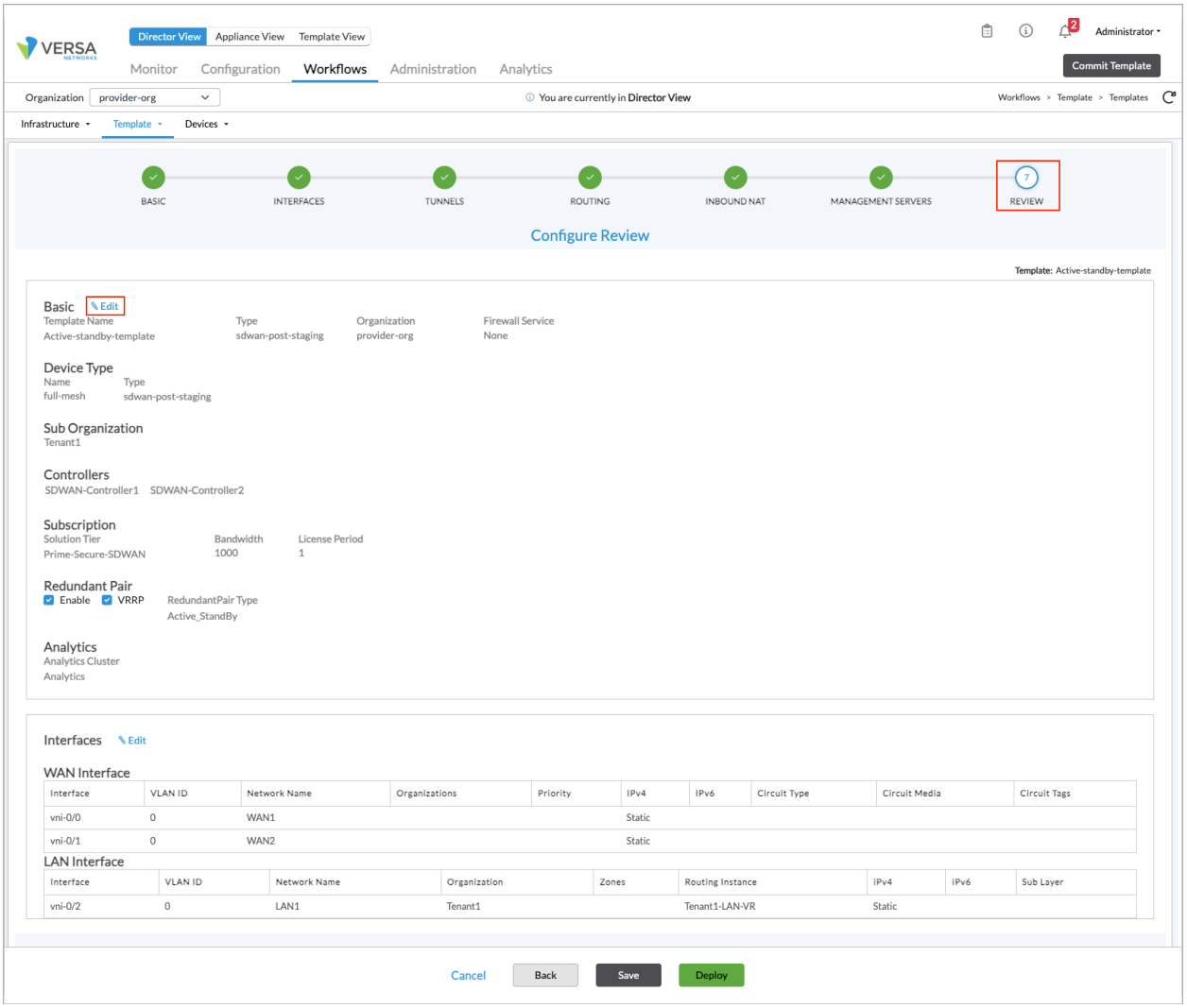


10. Configure a cross-connect interface by entering information for the following fields. The cross-connect interface provides the communication link between the active and standby appliance. When the standby device receives traffic, it forwards the traffic to the active device for processing over the cross-connect link. Note that the cross-connect interfaces between the active and standby devices must have the same configuration.

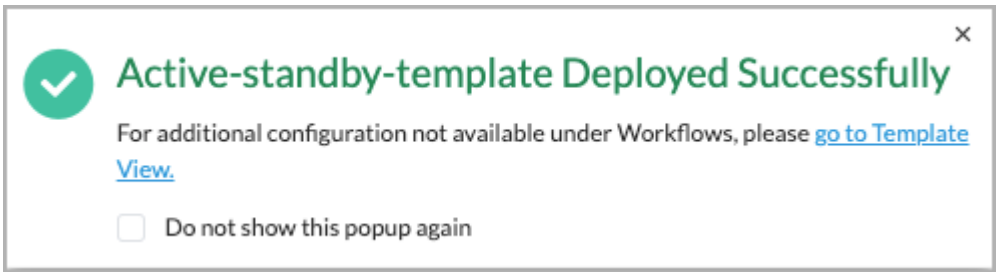


Field	Description
Device Port Configuration	Click a port in the diagram.
Port Type	Select Cross from the list.

11. Click Done to add the cross-connect interface.
12. Click Next to go to Step 3, Tunnels. Continue configuring the remaining steps—Interfaces, Tunnels, Routing, Switching (for Releases 21.1.1 and later), Inbound NAT, and Management Servers—as you would for a standard post-staging template. See Create and Manage Staging and Post-Staging Templates for more information.
13. Once you have finished configuring the workflow template, go to Step 7, Review, to review the details. You can click the Edit icon to make changes. The screen shot below shows that you have enabled a redundant pair of devices in active-standby mode, and you have also enabled VRRP.

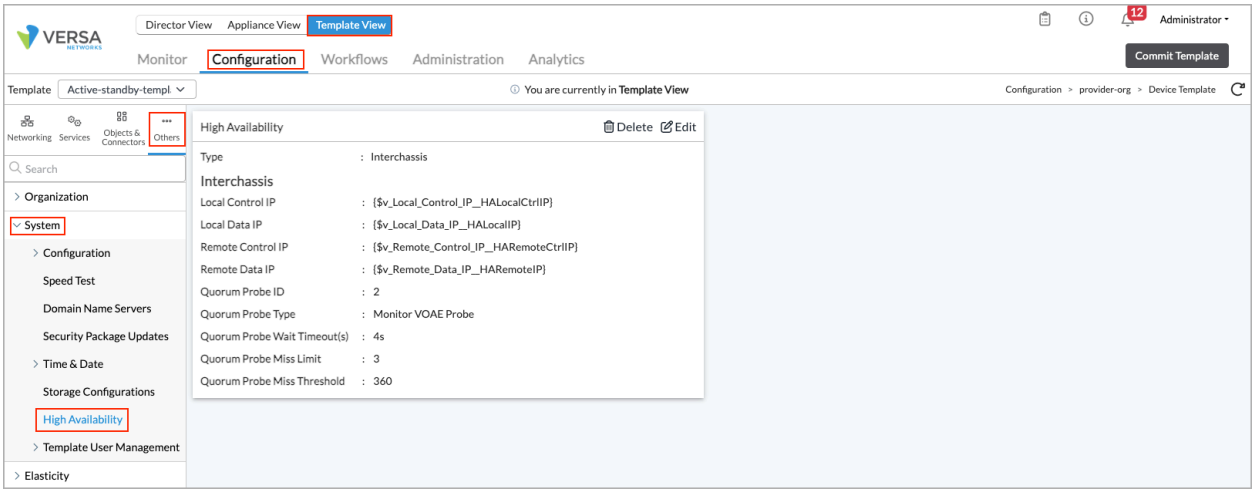


14. Click Deploy to deploy the new active-standby workflow template. When the template is deployed successfully, a popup window similar to the following displays.



15. You can click the Go to Template View link in the popup window to go to Template view, from which you can associate the active-standby workflow template with devices.
16. To verify that the active-standby workflow template was created:
    a. In Template view, select Configuration in the top menu bar.

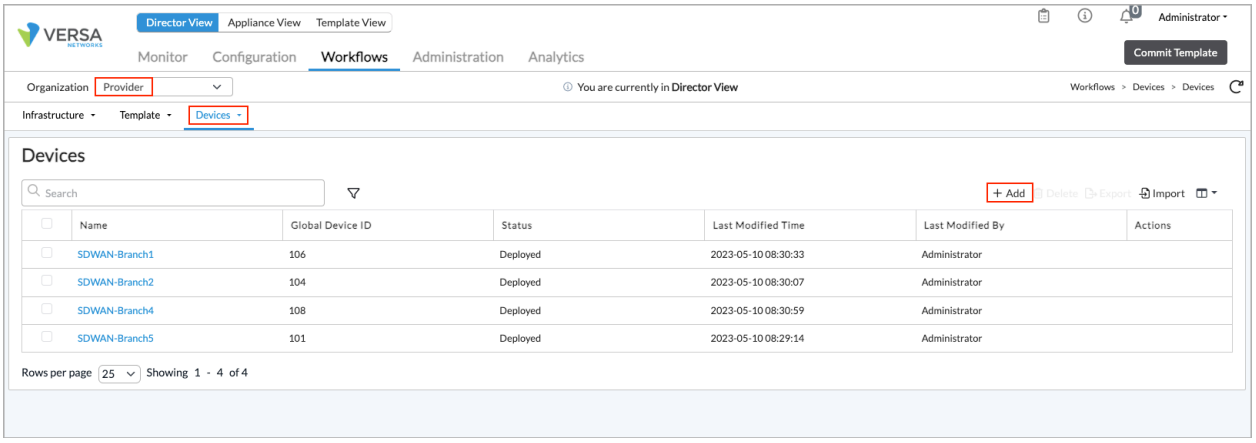
b. Select Others > System > High Availability in the left menu bar. The High Availability screen displays the configuration that was generated by deploying the active-standby workflow template.



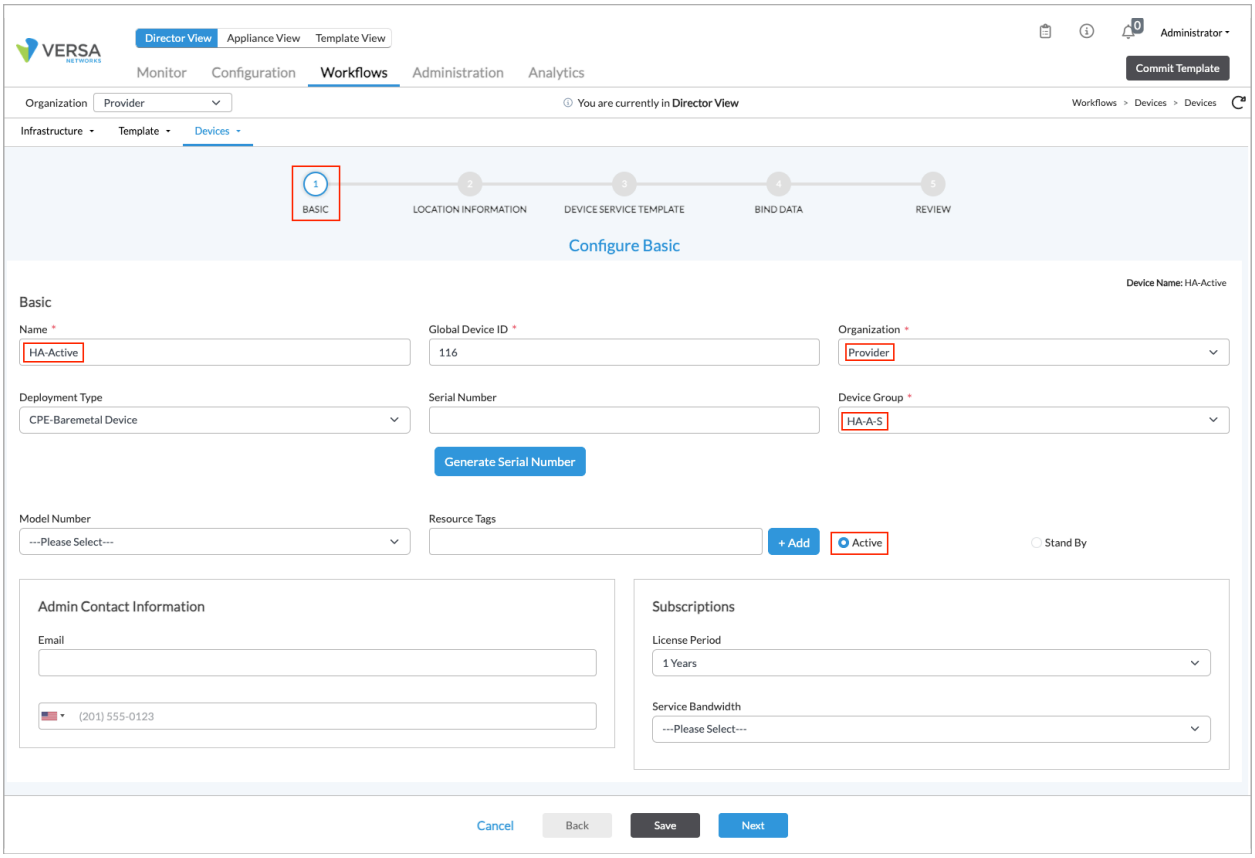
Configure Devices for Interchassis HA Using Workflows

After you create an active-standby interchassis HA template using workflows, you can create devices and associate them with the active-standby template. You first create the active device, then you create the standby device. Note that when creating a device for interchassis HA, you must select a device group that points to an active-standby interchassis HA template, as described below.

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Devices > Devices in the second horizontal submenu bar. The following screen displays.

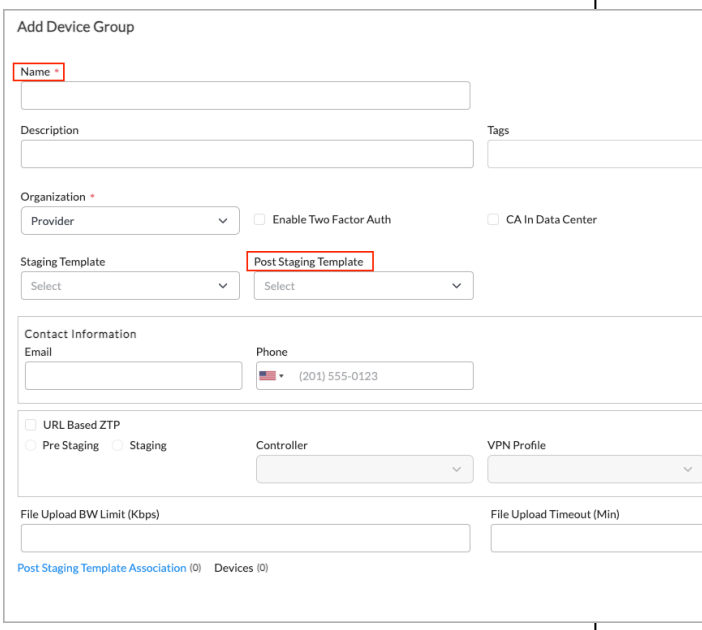


3. Select an organization from the horizontal submenu bar.
4. Click the + Add to add a device.
5. Click Step 1, Basic. The Configure Basic screen displays. Enter information for the following fields.



Field	Description
Name	Enter a name for the new device.
Organization	Select an organization.
Device Group	Select a device group to assign to the device. Note that the device group template must be associated with an active-standby interchassis HA template. If you have not already configured this type of device group template, click + Add New in the Device Group pull-down menu and then configure the new device group template. For information on configuring an active-standby interchassis HA template, see Create an Active-Standby Template. To create a device group: 1. Click + Add New in the Device Group pull-down menu.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
2. In the Add Device Group screen, enter information for the following fields.

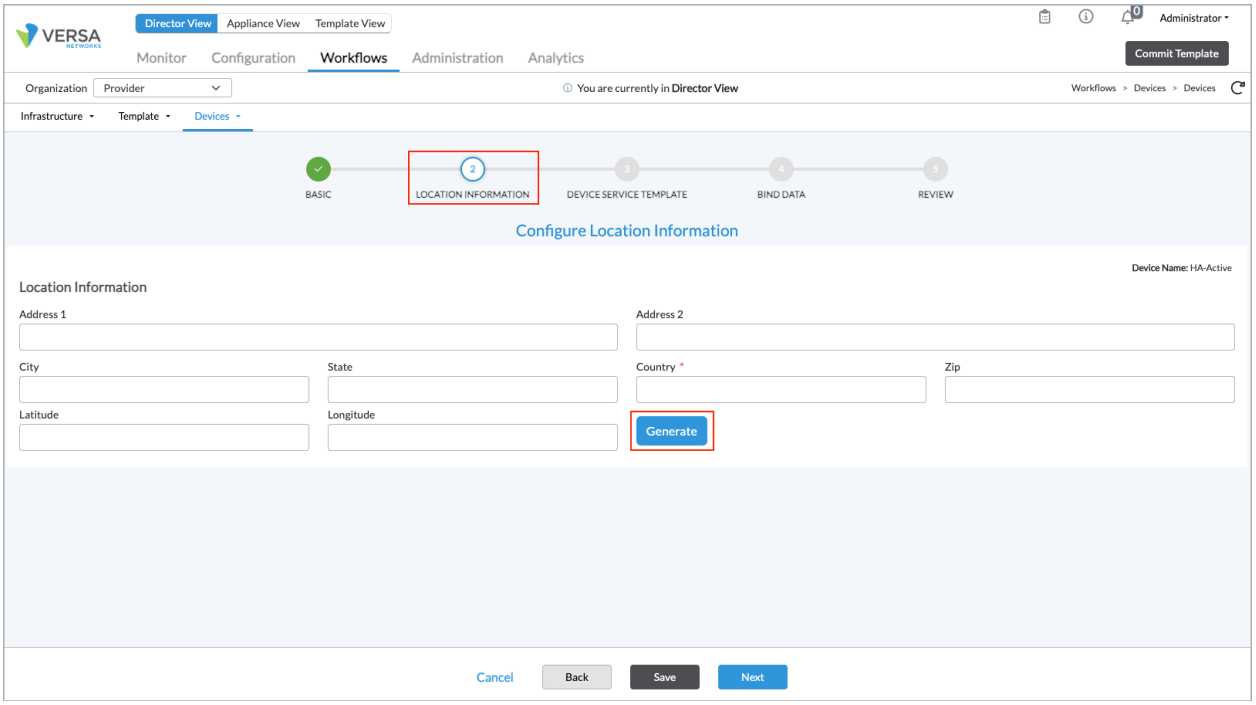


<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Name</td><td>Enter a name for the device group.</td></tr>
<tr><td>Post-Staging Template</td><td>Select the interchassis HA post-staging template for the device group.</td></tr>
</table>

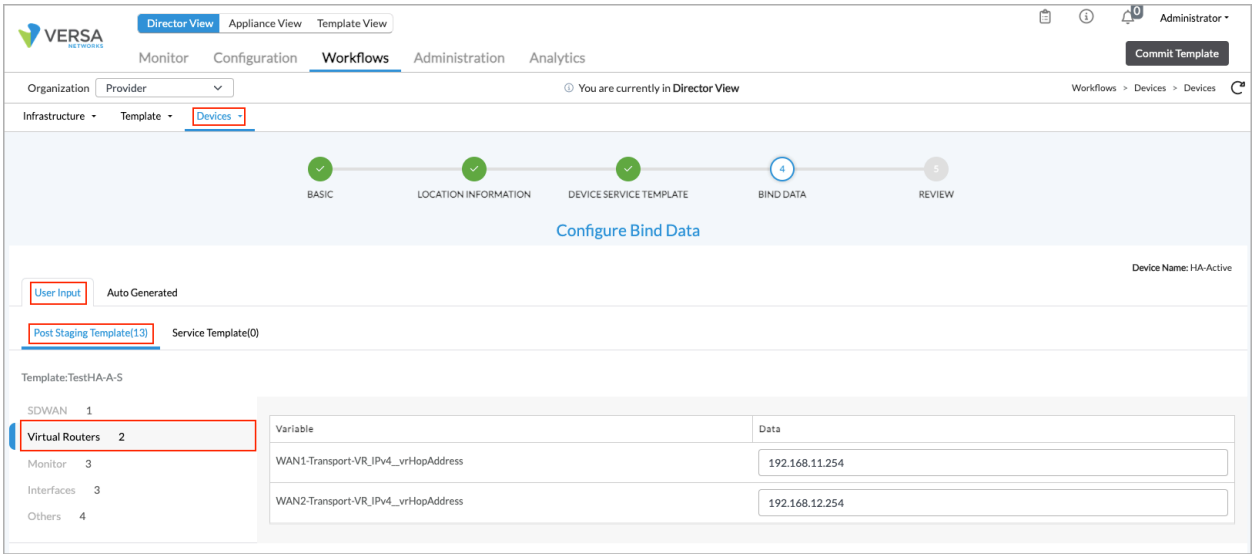
3. Click OK.

For more information about device groups, see Create Devices and Device Groups in Configure Basic Features.
</td></tr>
<tr><td>Active</td><td>Select active to make this device the active device in the active-standby pair. Note that the Active and Standby buttons only appear if the chosen device group has active-standby interchassis HA configured.</td></tr>
</table>

6. Configure the remaining fields as desired for your deployment.
7. Click Next to go to Step 2, Location Information, enter the required information about the device's location, then click the Generate button to generate the Latitude and Longitude coordinates.

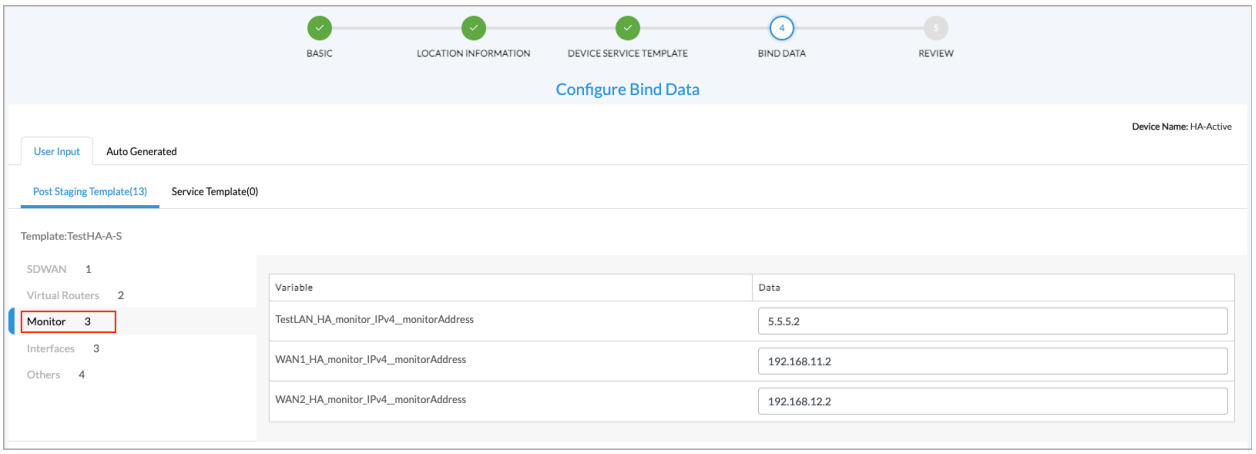


8. Click Next to go to Step 3, Device Service Template and enter device service template information, if desired.
9. Click Next to go to Step 4, Bind Data.



10. Select the User Input tab, then select the Post Staging Template tab.
11. Click Virtual Routers, then in the Data column, add the IP addresses for the WAN next-hop address variables.

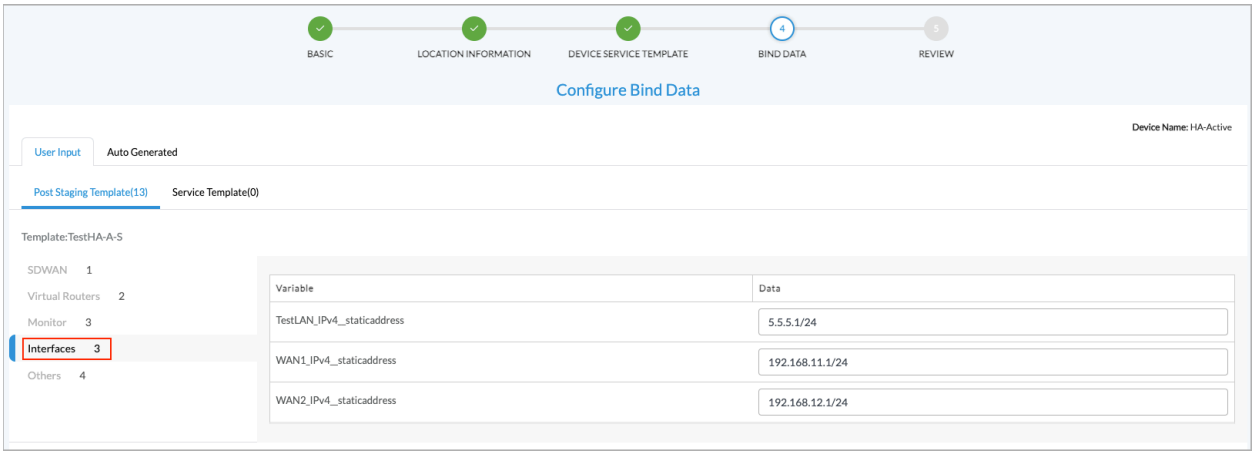
12. Click Monitor under the Post Staging Template tab.



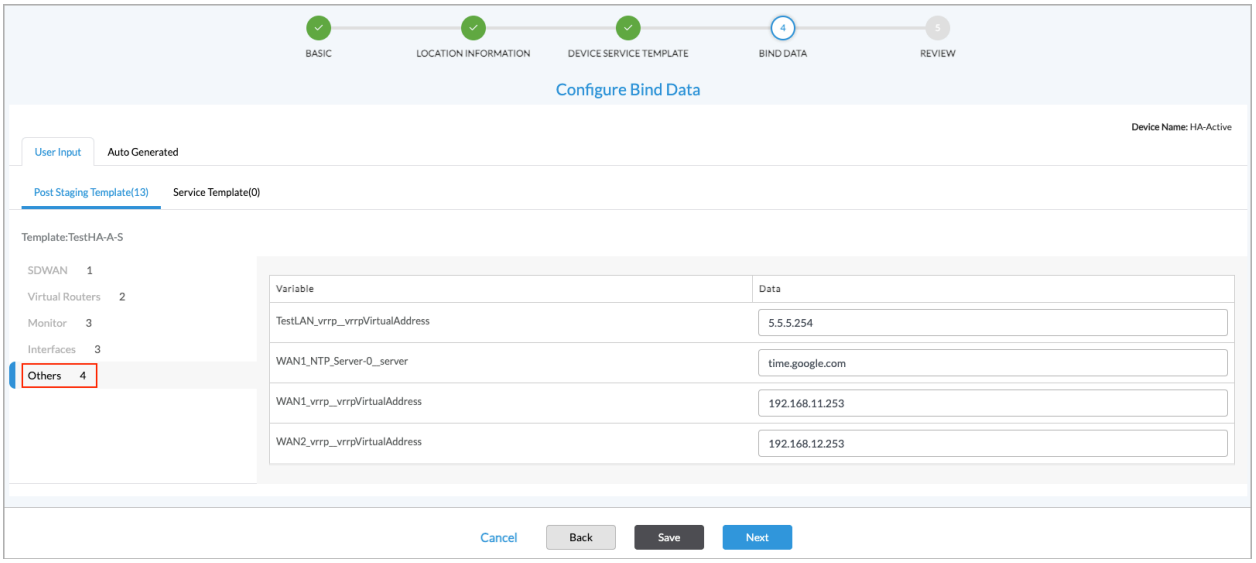
13. In the Data column, add the IP addresses of the peer devices for the LAN and WAN monitors. The IP-SLA monitors will be created with these IP addresses.

    Note: IP-SLA monitors are used to check the availability of the peer device in an active-standby configuration. The active device is the peer of the standby device, and the standby device is the peer of the active device. The screen shot above shows the configuration for the active device, so the monitor IP addresses that you enter are the addresses of the peer (standby) devices.

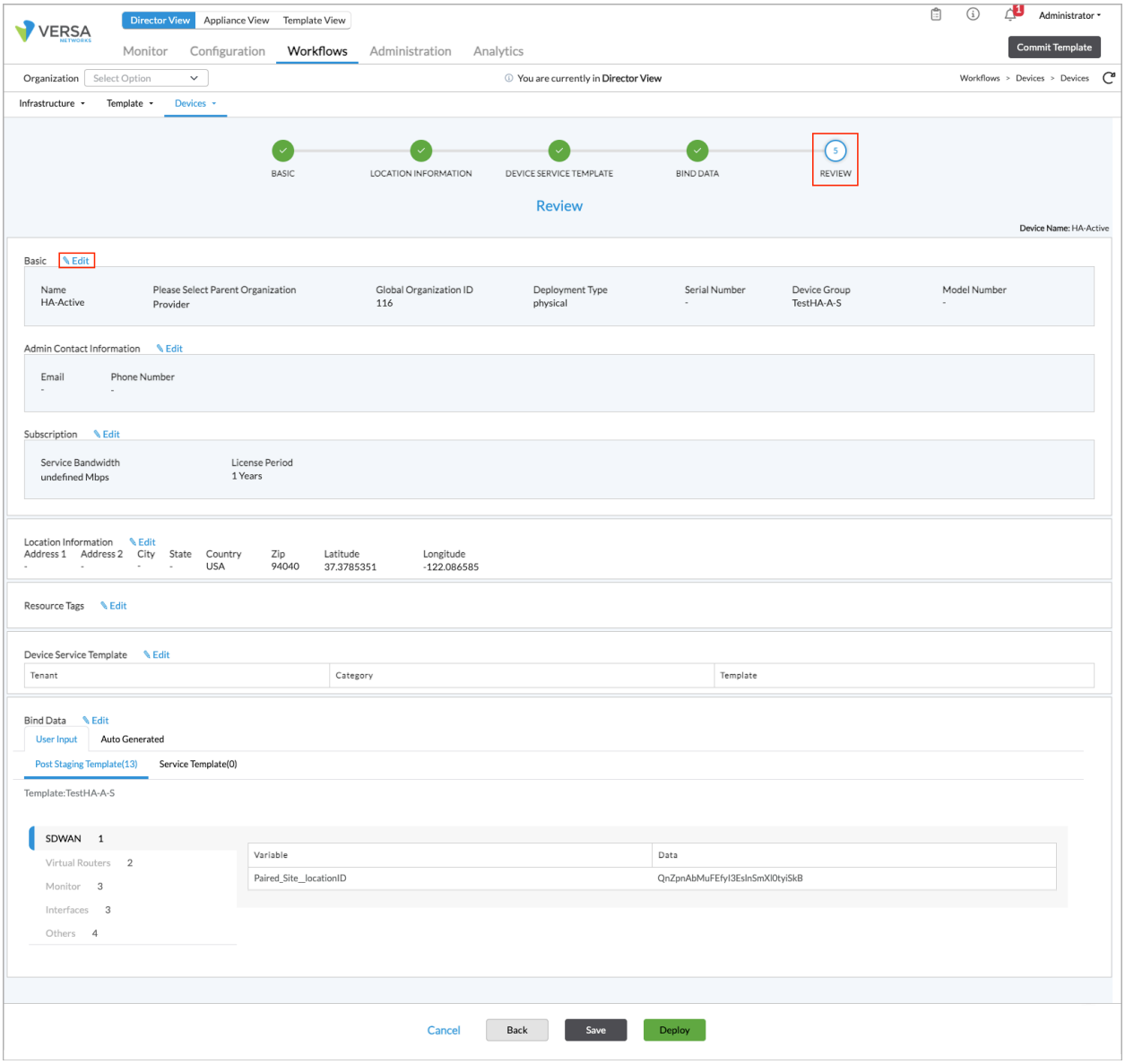
14. Click Interfaces under the Post Staging Template tab.



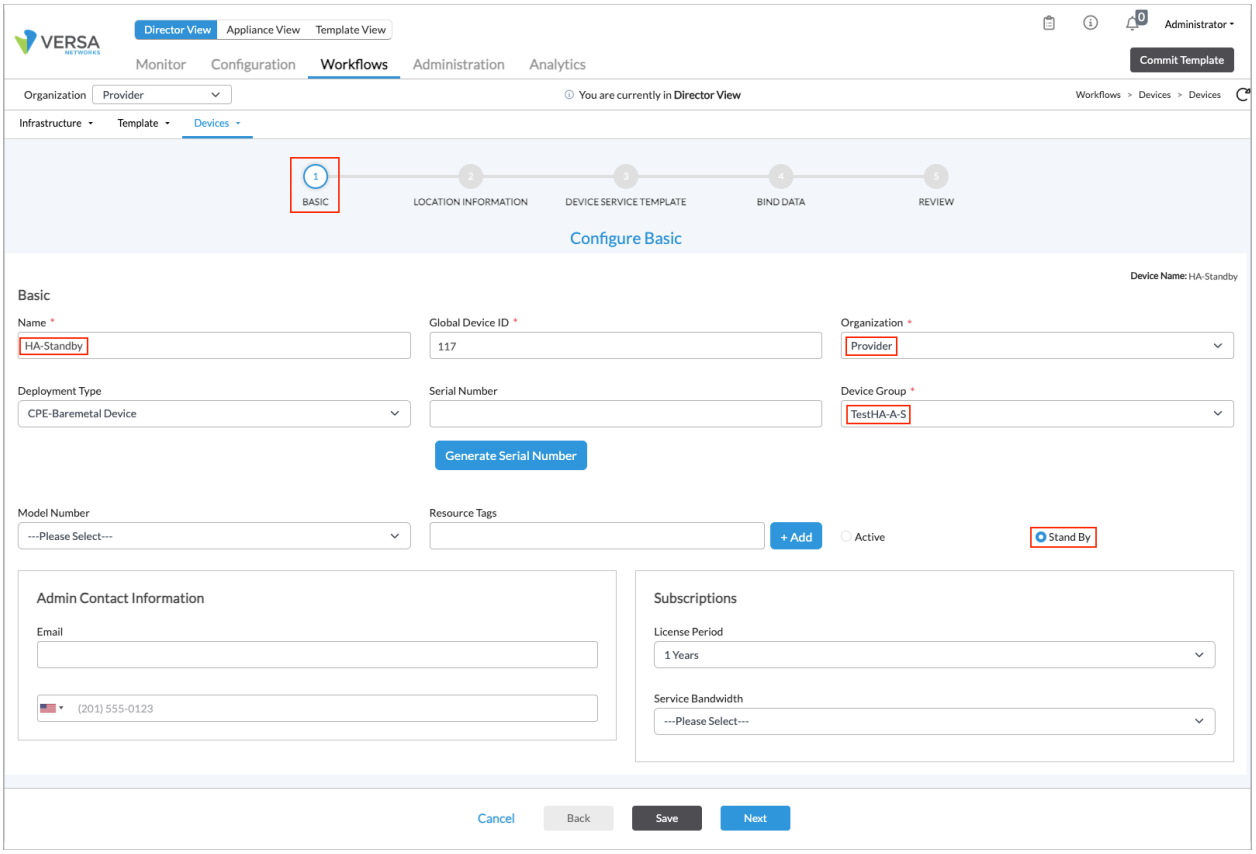
15. In the Data column, add the IP addresses for the LAN and WAN interfaces variables.
16. Click Others under the Post Staging Template tab.



17. In the Data column, add the information required for the LAN VRRP virtual address, the WAN NTP server IP address or FQDN, and the WAN VRRP virtual address variables for the peer devices. For example, the address for the LAN variable is the address of the peer LAN device, and the addresses for the WAN variables are the addresses of the peer WAN devices.
18. Click Next to go to Step 5, Review.



19. Review the configuration details. Click the Edit icon to make changes in any of the sections.
20. Click Save to save the device template, or click Deploy to deploy the template.
21. Repeat Step 1 through Step 20 to create the standby device. The following screen displays Step 1, Basic, for the standby device configuration.

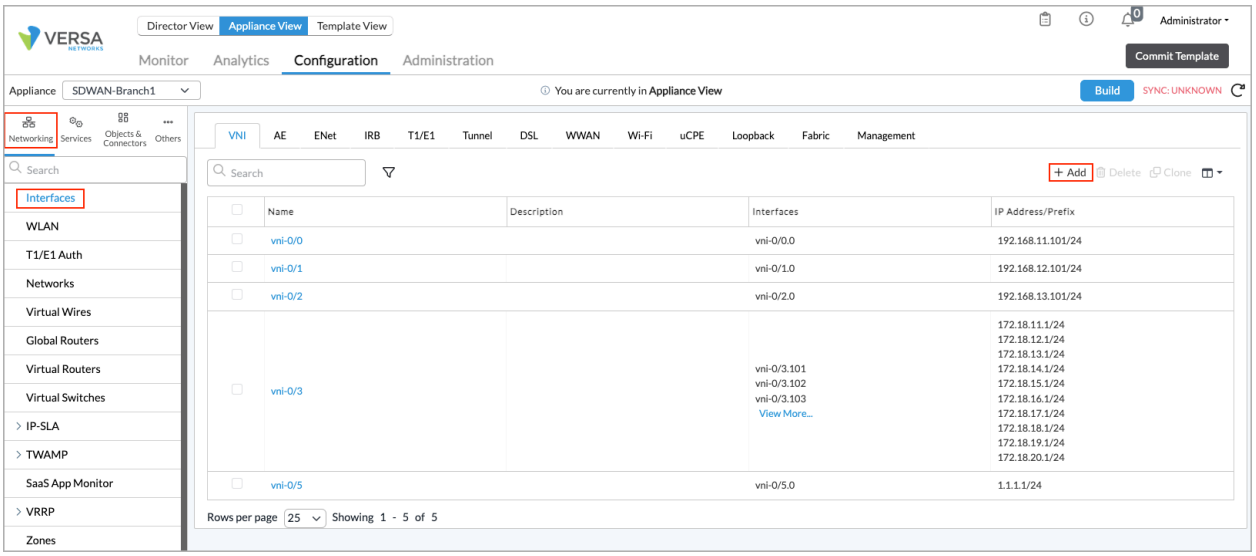


Configure HA Punt

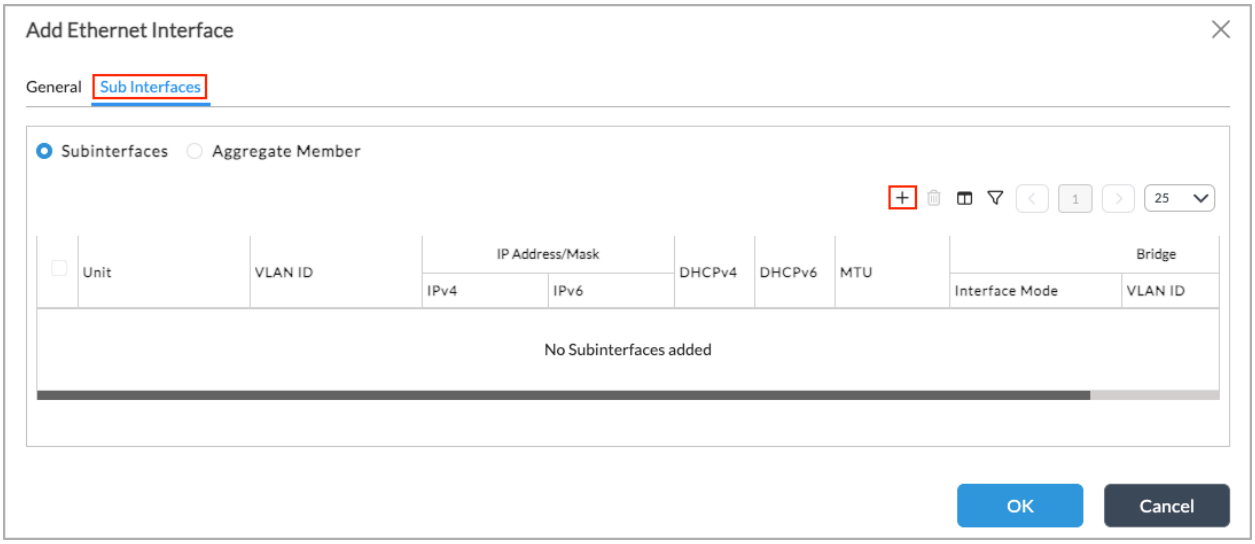
If the LAN interface on the active device in an interchassis HA pair stops working, you can redirect, or punt, traffic from the active device to the standby device. To do this, you create a WAN interface on both the active and standby devices. You must also enable SLA and quorum probes.

To configure HA punt:

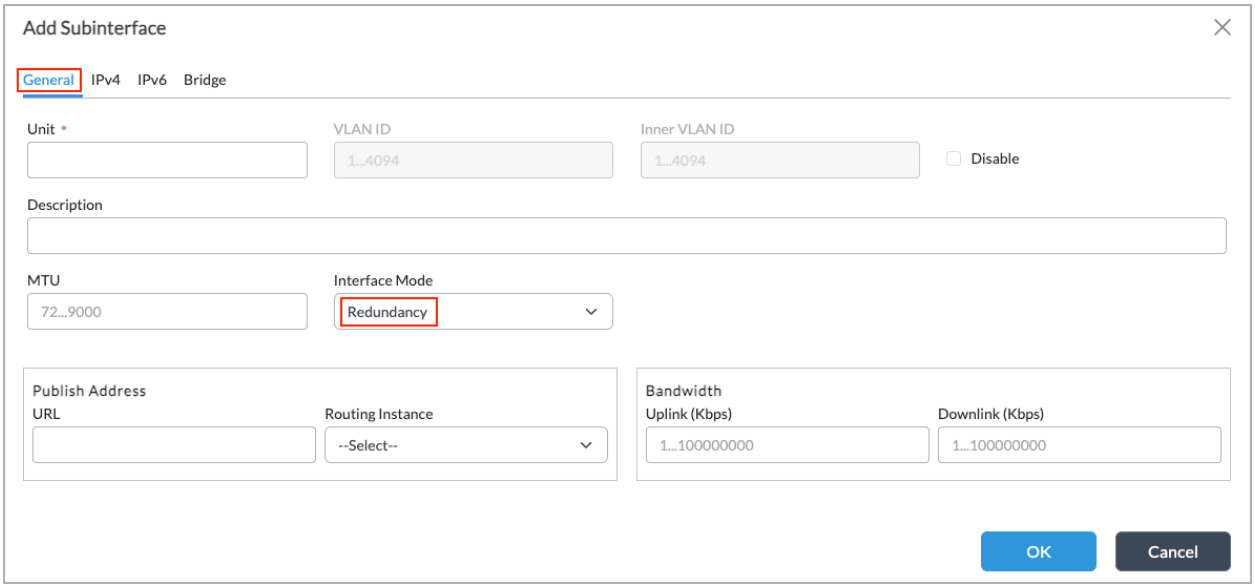
1. Create a WAN interface on both the active and standby devices:
   a. In Director view, select the Configuration tab in the top menu bar.
   b. Select the organization in the horizontal menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select Configuration in the top menu bar.
3. Select Networking > Interfaces in the left menu bar, and click the + Add icon.



a. In the Add Ethernet Interface screen, click Subinterfaces and then click the + Add icon.



b. In the Add Subinterface popup window, select the General tab. In the Interface Mode field, select Redundancy. For information about configuring the other fields, see the Configure Interfaces article.

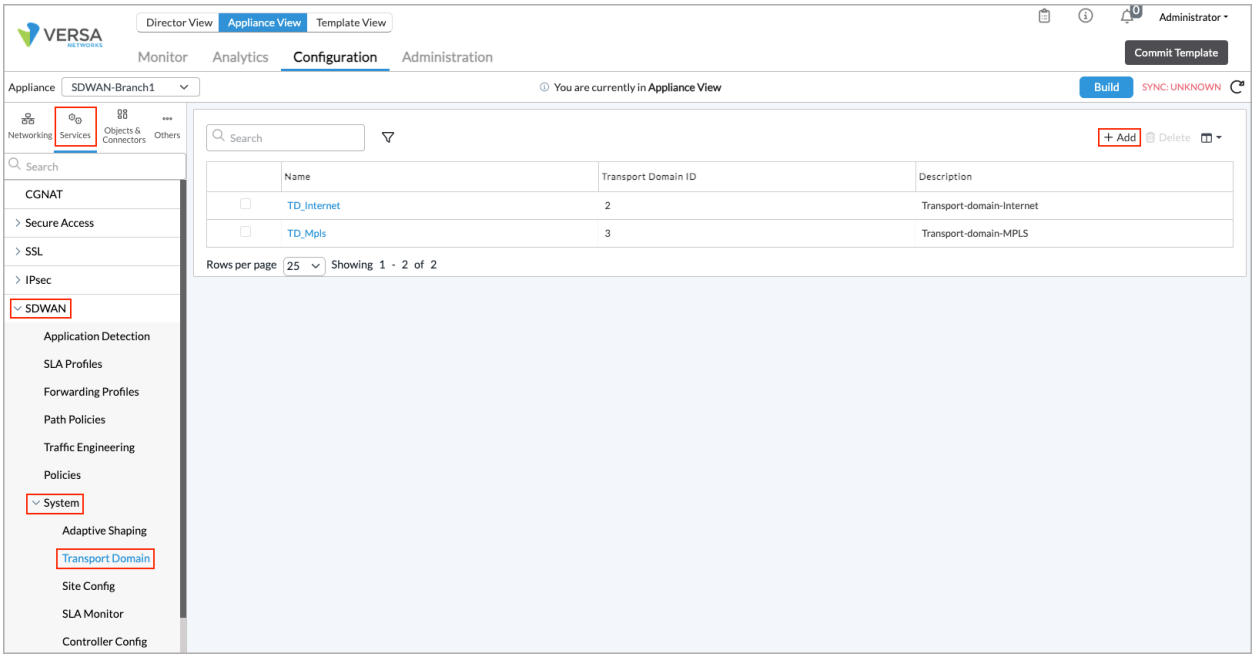


c. Click OK.

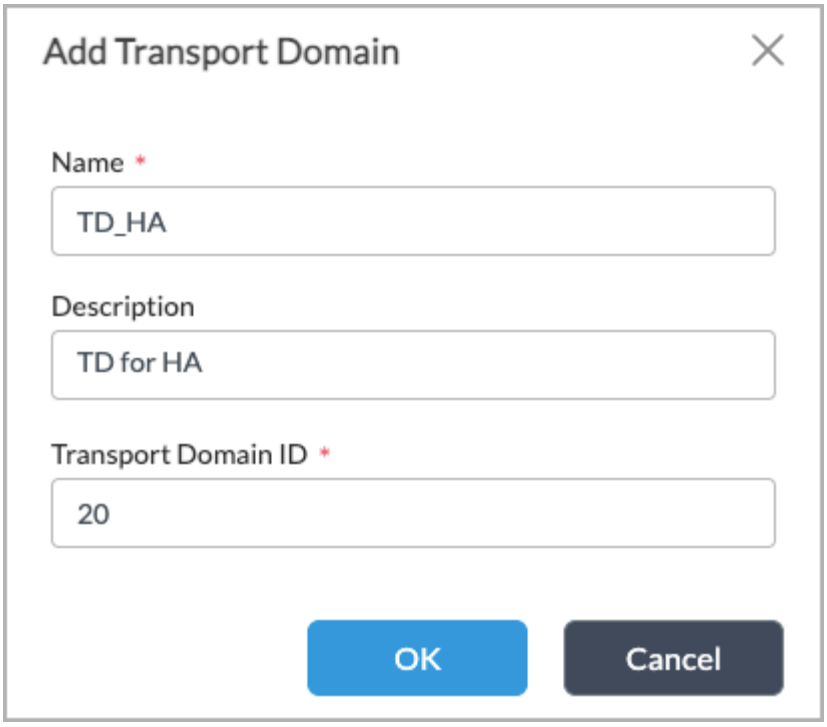
4. Create a transport domain:

a. In Appliance view, select the Configuration tab in the top menu bar.

b. Select Services > SD-WAN > System > Transport Domain in the left menu bar.



c. Click the + Add icon. The Add Transport Domain popup window displays. In this example, you configure TD_HA transport domain.



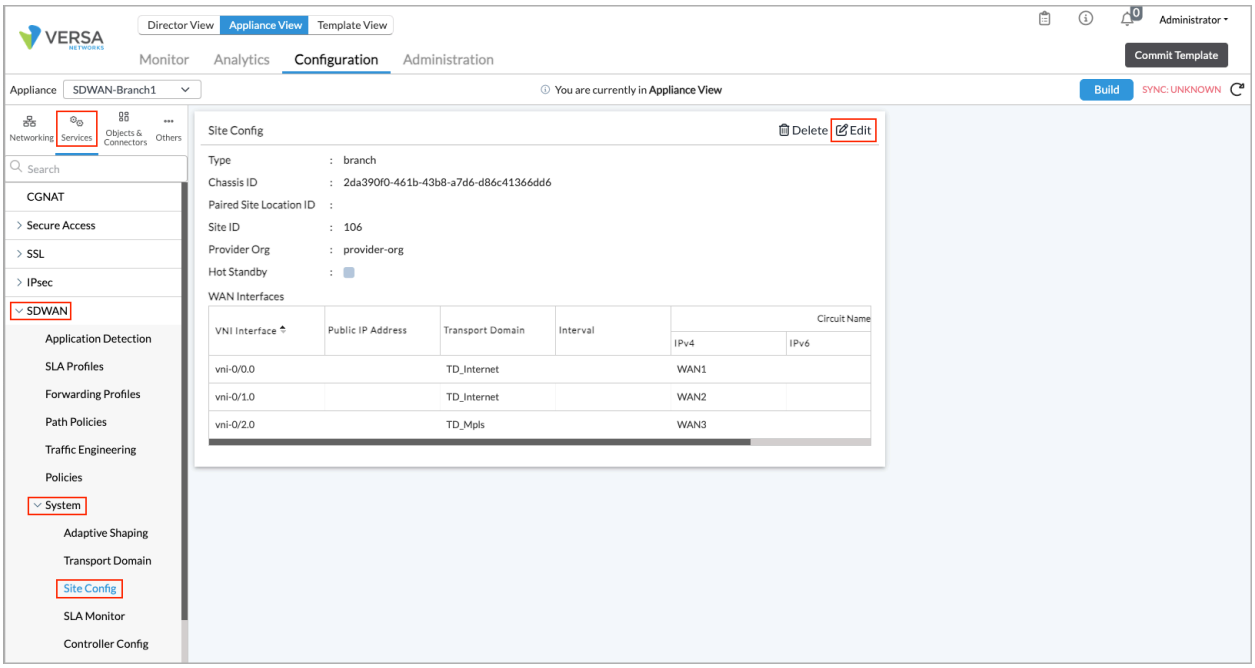
d. Enter the name, description, and identifier for the transport domain. For more information, see Configure Transport Domains.

e. Click OK.

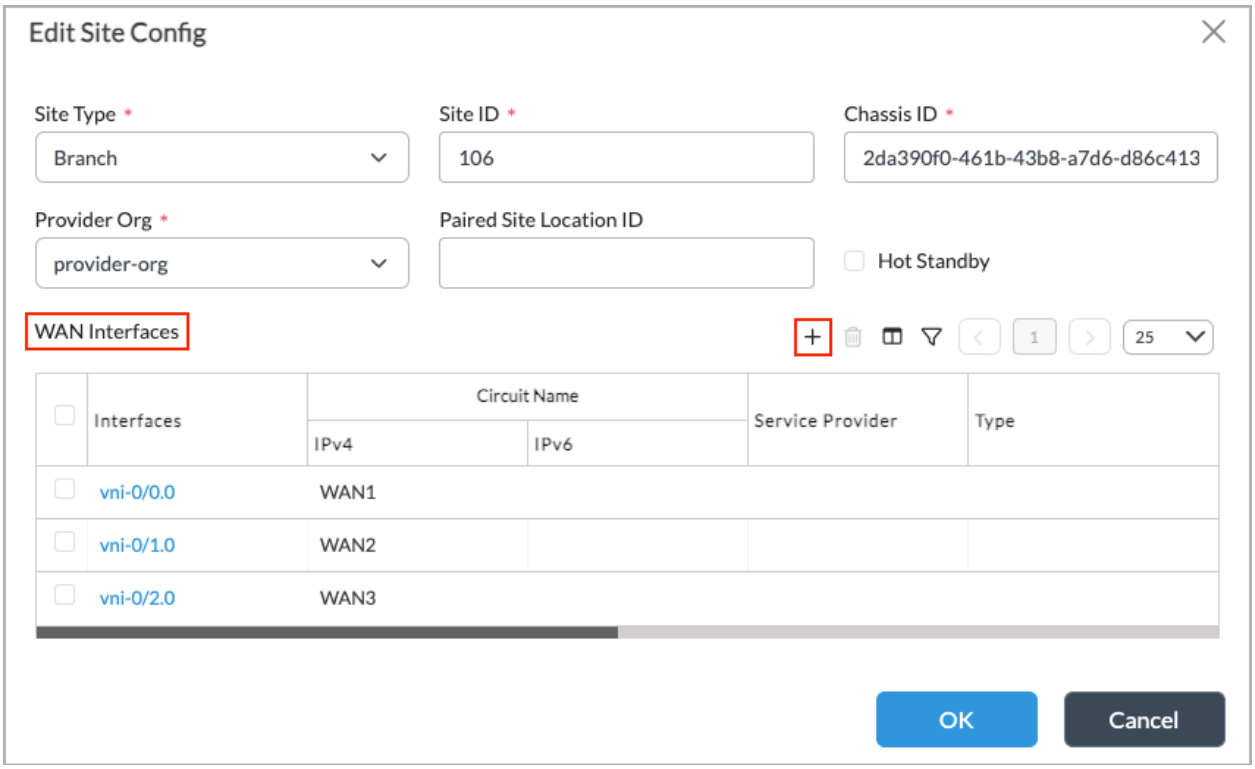
5. Associate the transport domain with the WAN interface:

a. In Appliance view, select the Configuration tab in the top menu bar.

b. Select Services > SD-WAN > System > Site Configuration in the left menu bar, and click the Edit icon.

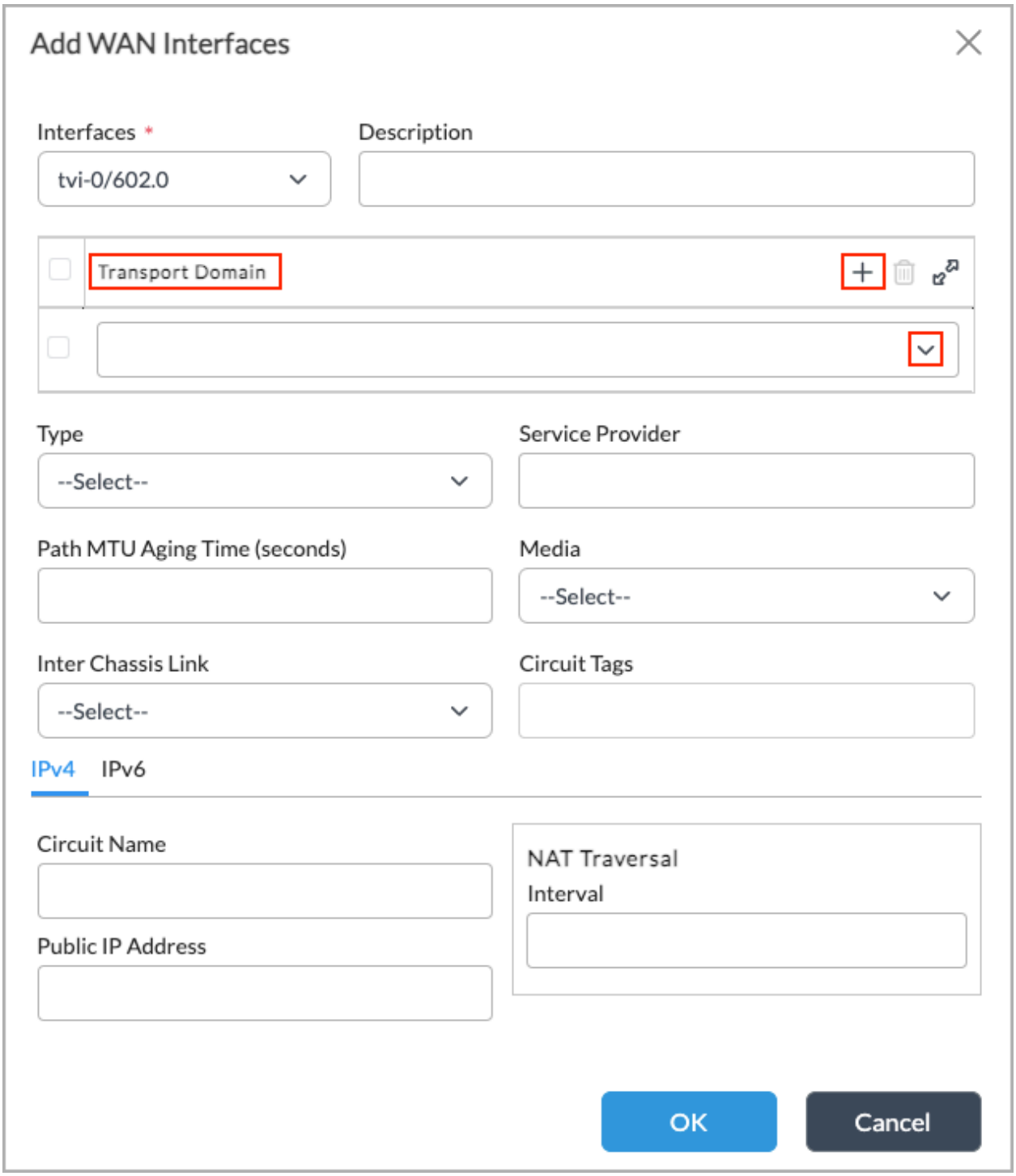


c. In the Edit Site Configuration popup window, click the + Add icon.



d. In the Add WAN Interfaces popup window, click the + Add icon in the Transport Domain box and then

select the transport domain you created in Step 2.



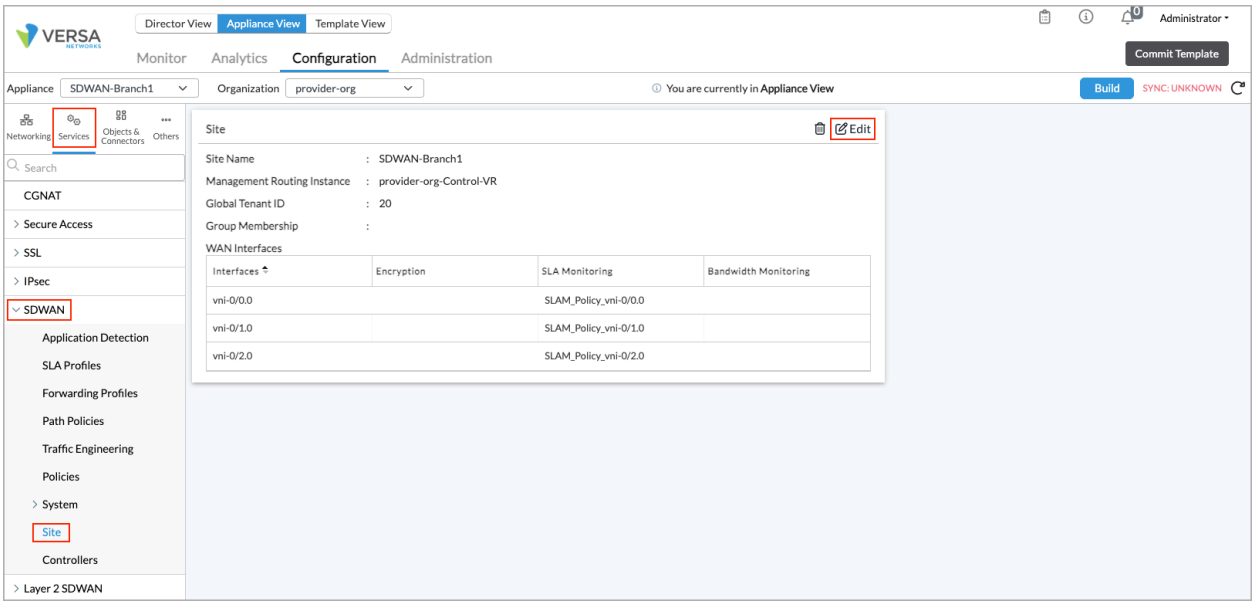
e. click OK.

6. Enable SLA on the interfaces:

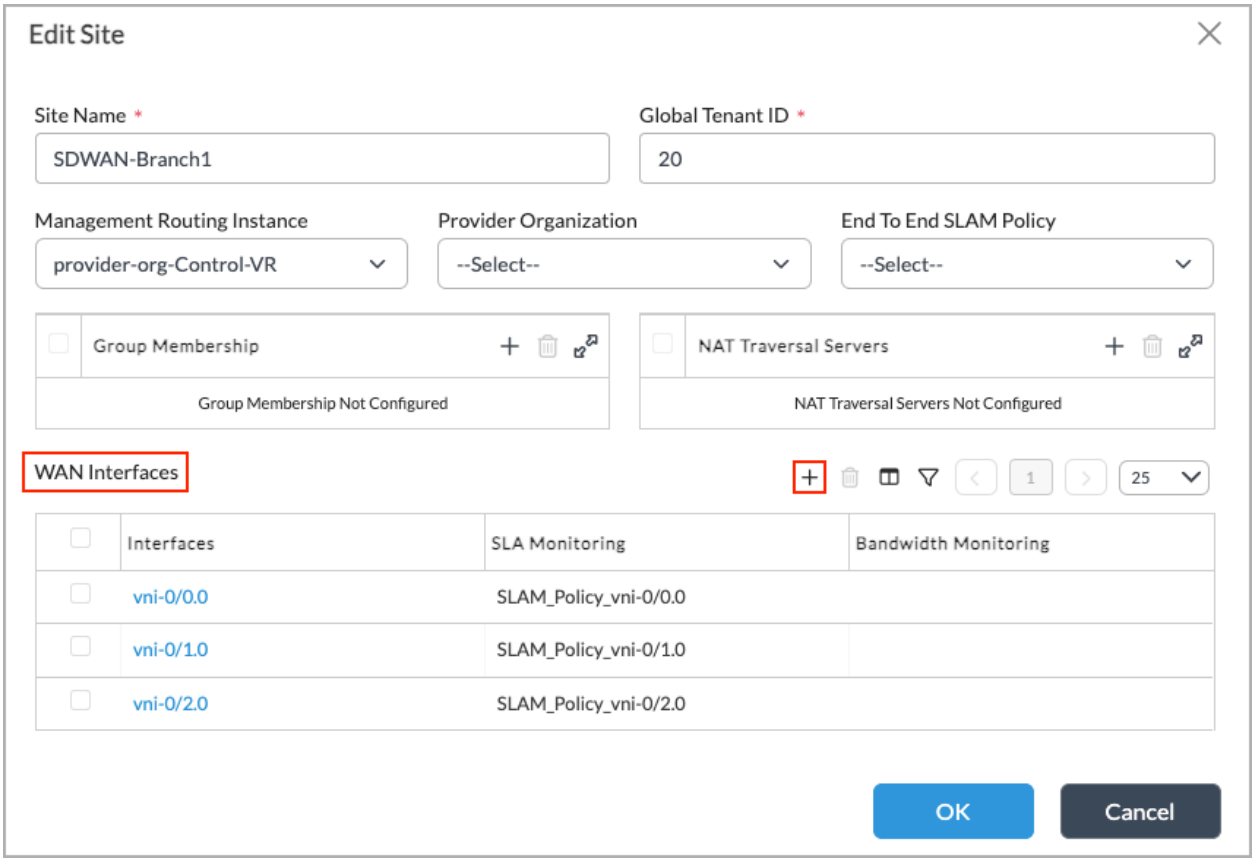
a. In Appliance view, select the Configuration tab in the top menu bar.

b. Select Services > SD-WAN > Site in the left menu bar.

c. In the Site pane, click the Edit icon.

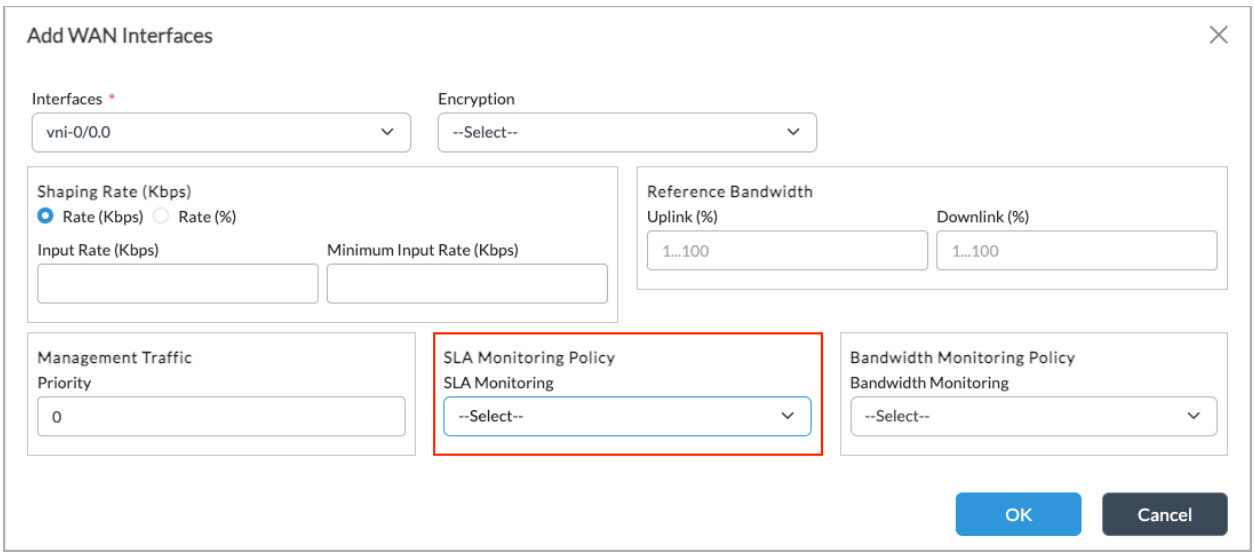


d. In the WAN Interfaces tab, select the WAN interface, and then click the + Add icon.



e. In the Add WAN Interfaces popup window, configure information about the WAN interface.

f. In the SLA Monitoring Policy box, select an SLA policy. For information about configuring the other fields, see Configure SLA Monitoring for SD-WAN Traffic Steering.



g. Click OK.

h. Restart services on both the active and standby devices in the interchassis HA pair.

Configure TACACS+ for HA Authentication

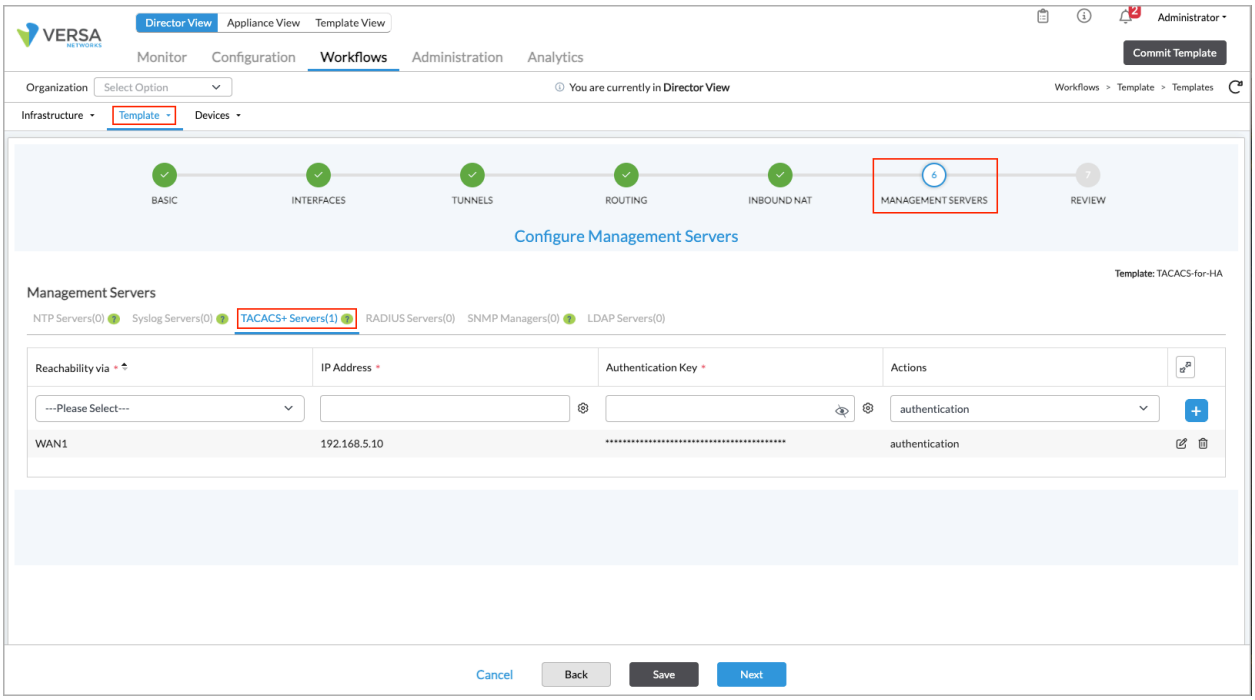
This section discusses how to configure TACACS+ to authenticate the active and standby nodes of an interchassis HA pair. For more information about TACACS+, see Configure AAA.

To configure TACACS+ for use with HA:

1. Configure the TACACS+ server:
   a. In Director view, select the Workflows tab in the top menu bar.
   b. Select Template > Templates in horizontal menu bar, then select the SD-WAN tab.
   c. Click the + Add icon to create a new template. The Create Template popup window displays.
   d. Select the Management Servers tab.

      Note: Before you can access the Management Servers tab, you need to enter some configuration information in the preceding tabs. See Create Post-Staging Templates for more information.

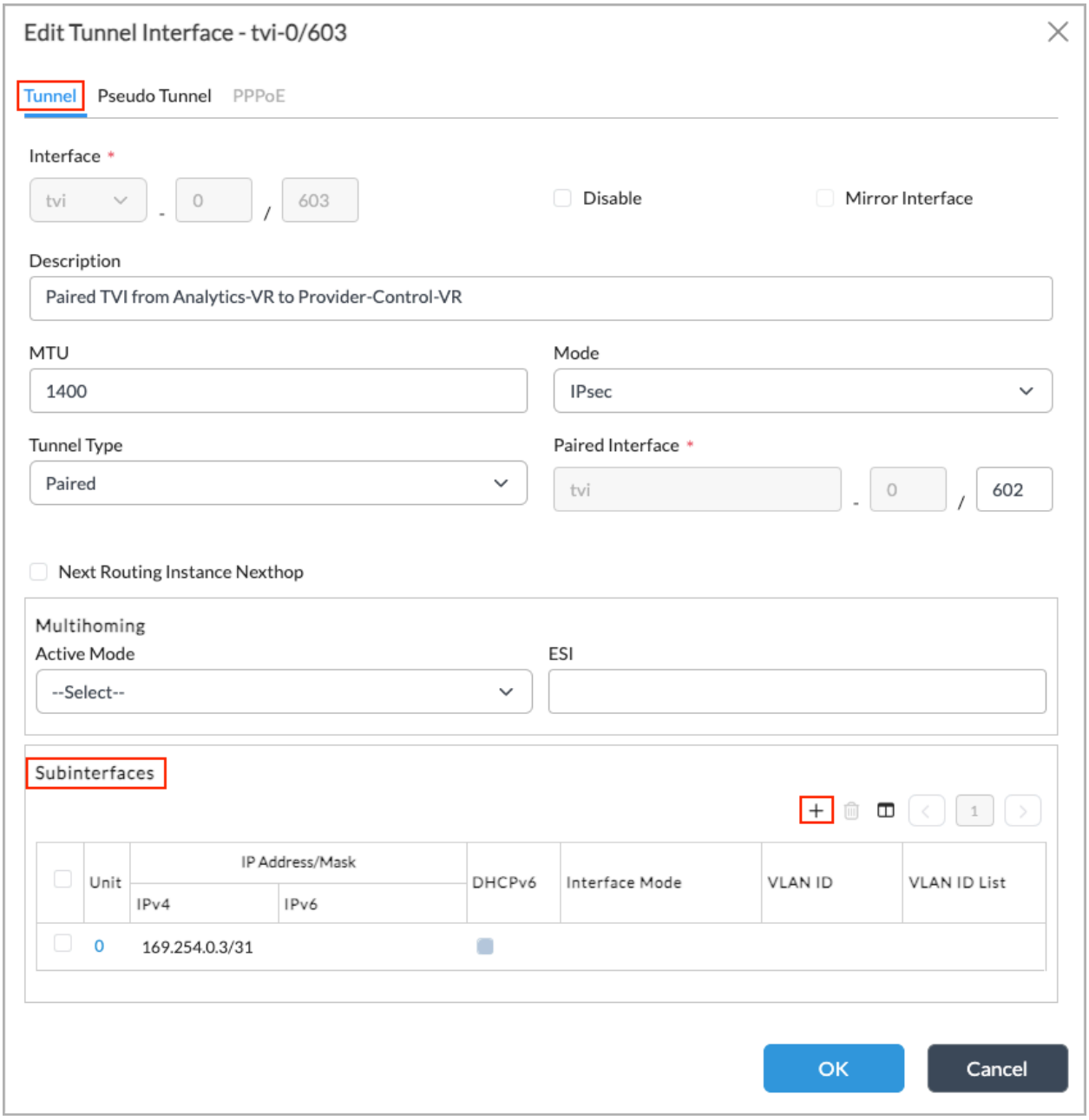
   e. Select the TACACS+ Servers tab. Configure the TACACS+ server, as described in the Create Device Templates section of the Configure Basic Features article. Here, the interface is WAN1.



2. Update the IP address of the paired tunnel interface (TVI). You need to do this to allow SSH pairing on the TVI for the interface you are using to reach the TACACS+ server, here WAN1. When you use a Workflow to add a management server for HA, the TVI interface that is created has an IP address of 169.254.x.x. However, with this

IP address, packets cannot be transmitted through virtual routing and forwarding (VRF) or across the branch, so, you must change this address.

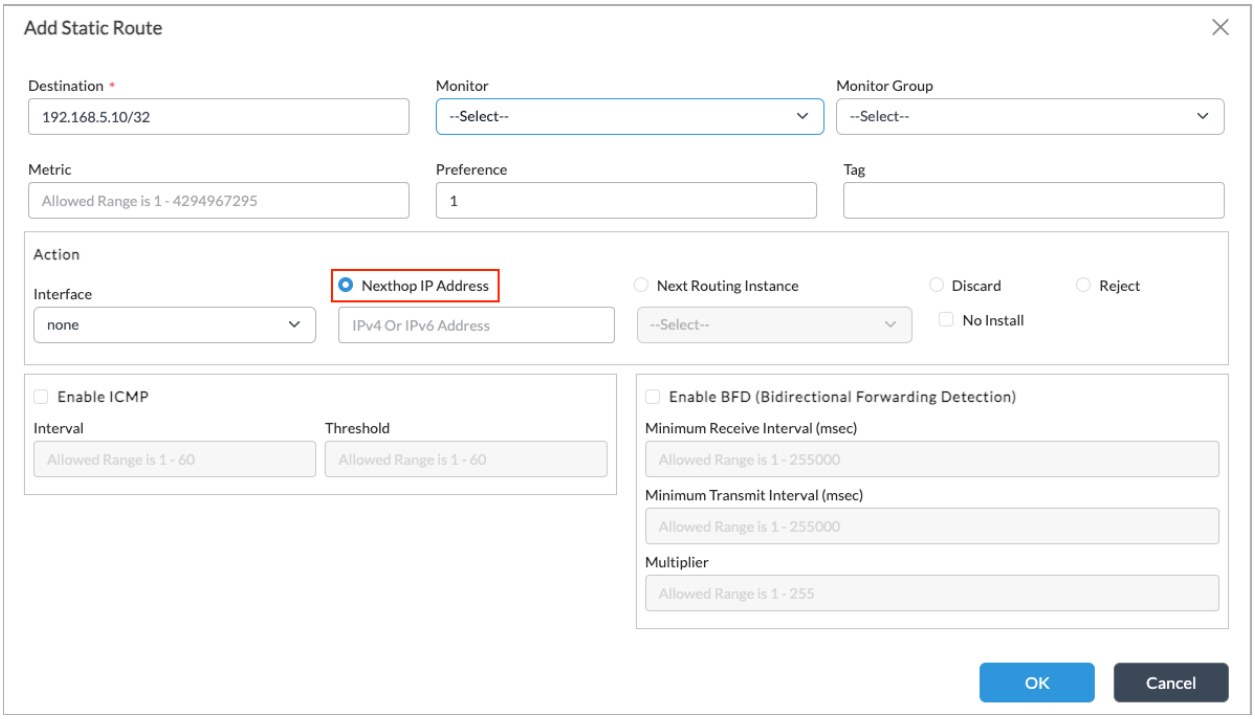
a. In Director view, select the Configuration tab in the top menu bar.
b. Select Devices > Devices in the horizontal menu bar.
c. Select an organization in the left menu bar.
d. Select a Controller from the dashboard. The view changes to Appliance view.
e. Select the Configuration tab in the top menu bar.
f. Select Networking > Interfaces in the left menu bar.
g. Select the Tunnel tab in the main pane.
h. Click the + Add icon.
i. Select an existing subinterface and enter the port and slot numbers for the TVI with which to pair. For more information, see Configure Tunnel Interfaces.



3. Add a static route in the global router for the TACACS+ server.
    a. In Director view, select the Configuration tab in the top menu bar.
    b. Select Devices > Devices in the horizontal menu bar.
    c. Select an organization in the left menu bar.
    d. Select a Controller in the main pane. The view changes to Appliance view.
    e. Select the Configuration tab in the top menu bar.
    f. Select Networking > Global Routers in the left menu bar.
    g. Select the Global Router Instance in the main pane. The Edit Global Router Instance popup window displays.

h. Select the Static Routing tab in the left menu bar, then click the + Add icon.

i. In the Add Static Route popup window, configure the static route as described in Configure Static Routes. In the Next-Hop IP Address field, enter the paired TVI IP address of the interface you are using to reach the TACACS+ server, here WAN1.



j. Click OK.

4. Create an interface.

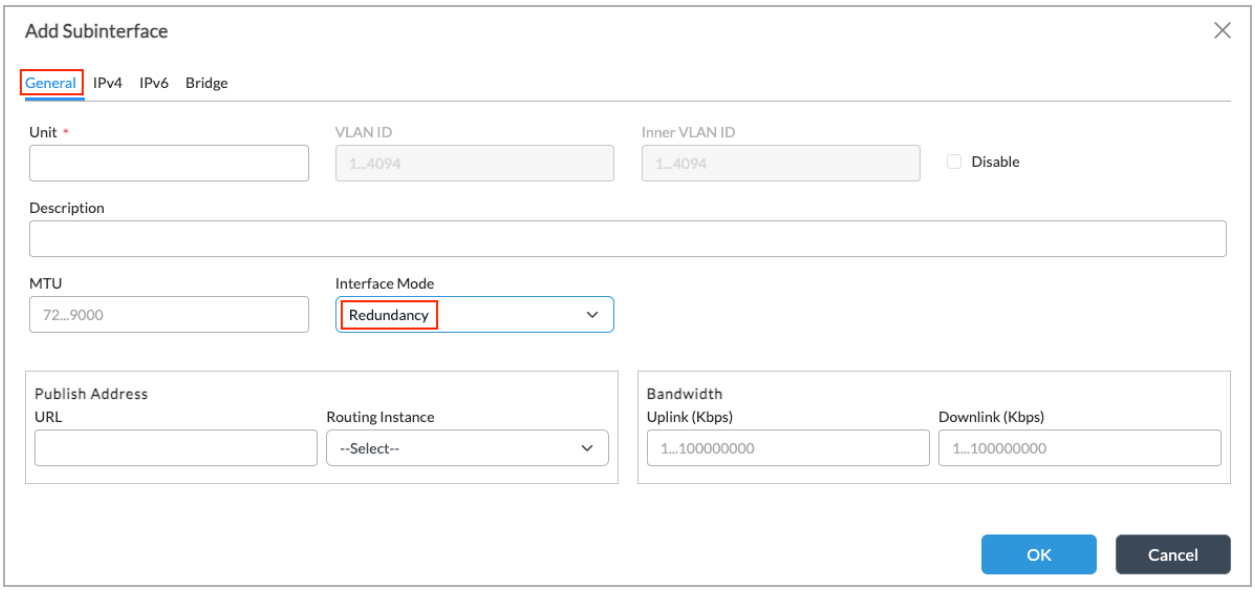
a. In Appliance view, select the Configuration tab from the top menu bar.

b. Select Networking > Interfaces in the left menu bar, then select the VNI tab in the horizontal menu bar.

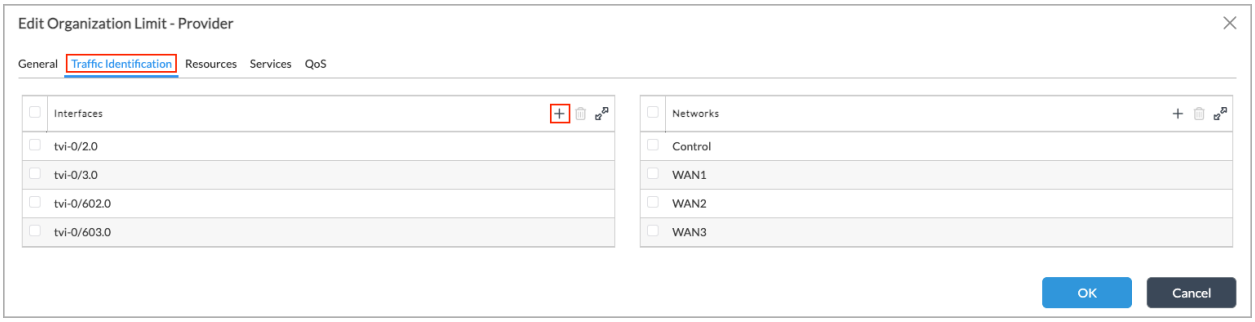
c. Click the + Add icon in the main pane.

d. In the Add Ethernet Interface popup screen, select the Subinterfaces tab in the horizontal menu bar, click the Subinterfaces button, and then click the + Add icon. The Add Subinterface popup window displays.

e. In the Interface Mode field, select Redundancy. Configure other fields as described in Configure Interfaces.

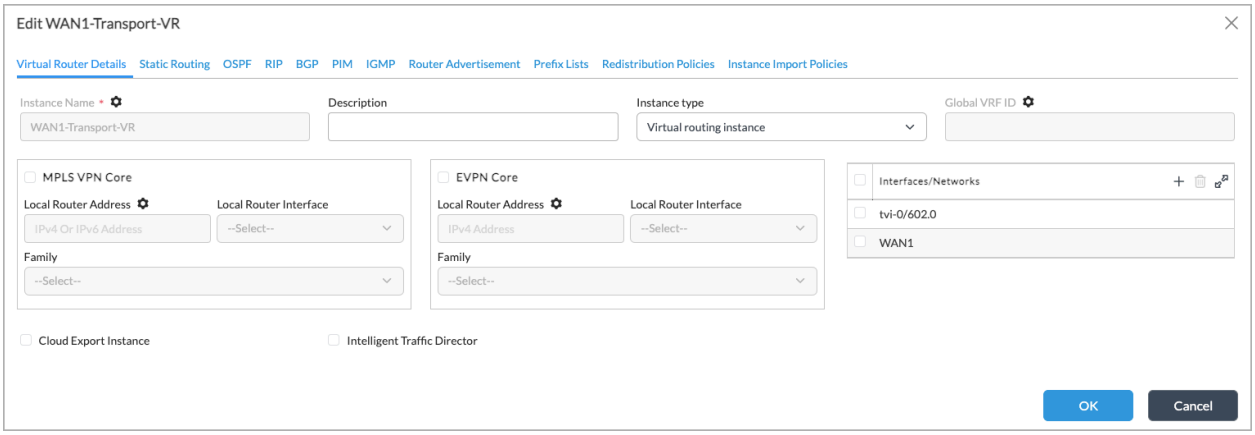


5. Add the interface that you created in Step 4 to the Traffic Identification tab for the organization's limit.
   a. In Appliance view, select the Configuration tab in the top menu bar.
   b. Select Others > Organization > Limits in the left menu bar.
   c. Select the organization name in the main pane. The Edit Organization Limit popup window displays.
   d. Select the Traffic Identification tab.
   e. Click the + Add icon in the Interfaces table and select the interface.



   f. Click OK.
6. Configure the interface (here, vni-0/4.400) for the WAN 1 virtual routing instance.
   a. In Director view, select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a template in the main pane. The view changes to Appliance view.
   e. Select the Configuration tab in the top menu bar.
   f. Select Networking > Virtual Routers in the left menu bar.

g. Click the + Add icon. The Configure Virtual Router popup window displays. Enter information as described in Set Up a Virtual Router.



7. For the overlay and WAN to be reachable, add a static route for the active WAN routing instance (here, WAN1). The next hop of this static route must be the interface whose mode is set to redundancy.

Considerations for Configuring Interchassis HA and VRRP

When you deploy interchassis HA and also enable VRRP on the WAN side, note that the HA active and standby states are separate from and independent of the VRRP active and backup states. It is recommended that the VRRP active always run on the active interchassis HA device. To configure the VRRP state so that it follows the interchassis HA state, you set appropriate values for the HA slave priority cost when you configure the VRRP group. The HA slave priority is a tracking object, and the HA slave priority cost is a value that is subtracted from the VRRP priority value when the VOS device changes its HA state from active to standby.

For example, if the VRRP group priority on a VOS device is 150, the HA slave priority cost is 100, and the HA state is standby, the VRRP priority becomes (150 – 100), or 50. This reduction of the VRRP priority value ensures that VRRP on the standby VOS device remains in backup state. When the VOS HA state transitions from standby to active, the VRRP priority does not remain at the reduced priority, but rather it returns to its configured value of 150. The change in VRRP priority occurs because the VOS device sends VRRP advertisements periodically (by default, once per second) that advertise, among other things, its priority value. Before the VOS device sends a VRRP advertisement, it computes its current priority based on the configured priority and the current state of its tracking objects. When a VOS device transitions to active state, it no longer subtracts the HA slave priority cost from the configured priority value, and as a result, its current priority becomes the same as configured priority, 150 (150 – 0).

To have the VRRP active to always run on the active interchassis HA device, it is recommended that on the active VOS device you configure the VRRP group priority value to 200, and that on the standby HA peer you configure the VRRP group priority to 150. On the standby HA peer, if you are using the default HA slave priority cost of 100, do not configure a VRRP priority value less than 100. These configuration values ensure that the VRRP priority on the HA standby device never becomes 0 or less than 0.

For information about configuring VRRP and VRRP groups, see Configure Interfaces and Configure VRRP.

Configure Switchover Policies for Unsynched Flows

Some sessions that rely on state information are not synced to the standby HA device, and when a switchover occurs, these sessions do not continue. So that these sessions can be re-established quickly, instead of waiting for the idle timeout period to expire, they are torn down.

The following state information is not synced with the standby HA device:

- TCP state information for terminated and proxied TCP sessions
- Some ALG state information

After a switchover, the following sessions are marked for rejection; that is, they are torn down after they send a TCP reset (RST) packet:

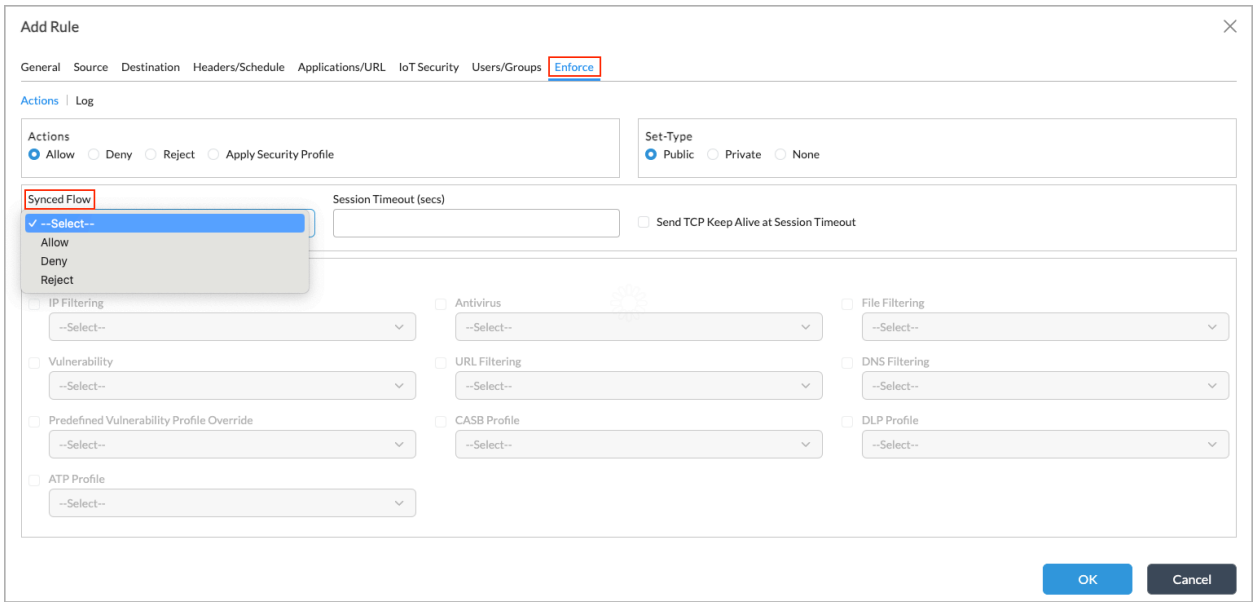
- Terminated and proxied TCP
- IDP
- Antivirus

In some cases, critical sessions continue after the switchover instead of being torn down, but they operate with only minimal services.

You should configure switchover policies for unsynchronized flows if you enable unified threat management (UTM) and next-generation firewall (NGFW) on the VOS devices. Otherwise, configuring these policies is optional.

To configure a security policy so that flows are synchronized when a switchover occurs:

1. In Director view:
   a. Select Configuration in the top menu bar.
   b. Select an organization in the horizontal menu bar
   c. Select Devices > Devices in the left menu bar.
   d. Select a device in the Devices table in the main pane. The view changes to Appliance view.
2. Select Configuration in the top menu bar.
3. Select Services > NextGen Firewall in the left menu bar.
4. Select Security > Policies, and select the Rules tab.
5. Click the + Add icon. In the Add window, select where to insert the new rule, then click OK.
6. In the Add Rule window, select the Enforce tab and then select the Synced Flow action to take after an HA switchover:
   - Allow—Allow the sessions for a minimal subset of service modules to continue running.
   - Deny—Drop all packets belonging to the matching synced sessions.
   - Reject—Send a TCP RST or an ICMP Unreachable message to the sender and tear down the matching synced.



7. Click OK.

For more information about configuring security policy and about the remaining fields on the Add Rule window, see the Configure User and Group Policy.

Configure HA To Avoid a Split-Brain State

In HA, a split-brain state can occur if both VOS devices in a HA pair take over mastership and become active at same time. To avoid, detect, and recover from a split-brain state, you configure quorum evaluation, either by configuring quorum probes, as discussed above, or by using static route monitors. When you enable quorum probes, if the control connection, the data connection, or the BFD session between the active and standby interchassis HA devices fails, the standby VOS device checks for the presence of the active VOS device in parallel, using all enabled modes. If this check indicates that the active device is operational and that the failure was due to transient connectivity issues, the standby device remains in its standby role. However, if the check confirms that a restart, reboot, or other failure of the active VOS device is the reason for the connection failure, the standby device takes over as the active device.

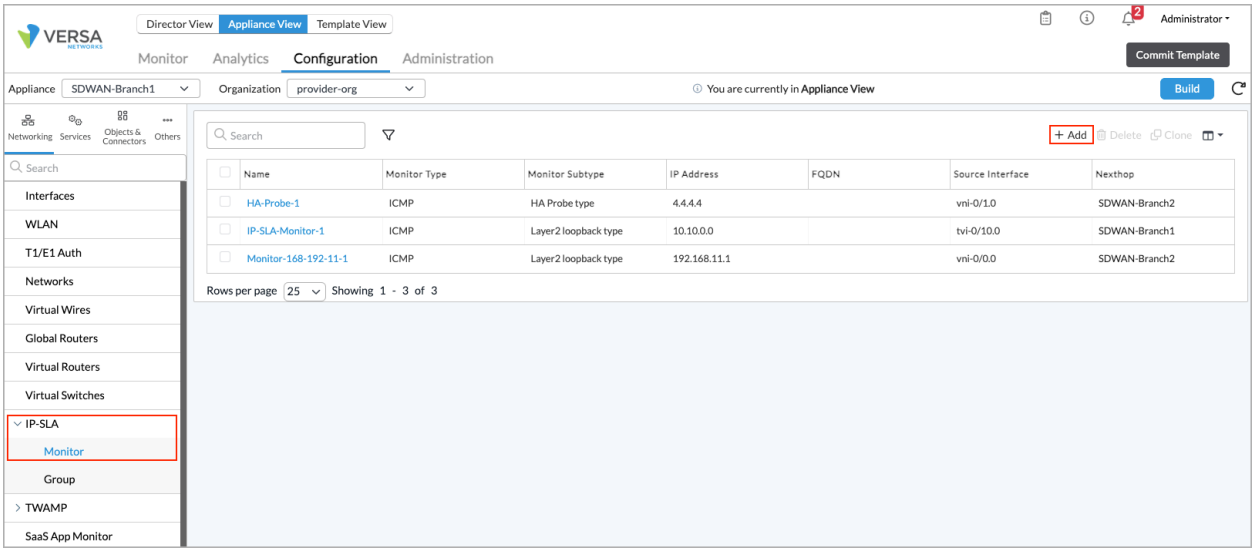
The IP-SLA monitor framework monitors a single destination (specified as an IP address or as a fully qualified domain name) or a list of destinations. To use the monitor framework, you configure a monitor object and then you attach it to one or more static routes or to one or more policies, such as an interchassis HA pair policy. The monitor element probes the status of the destination or destinations by continuously sending probes and flags that determine whether the destination is up or down. The static route or the policy then takes the appropriate action depending on the state of the destination.

When you enable interchassis HA, you must configure monitor probes.

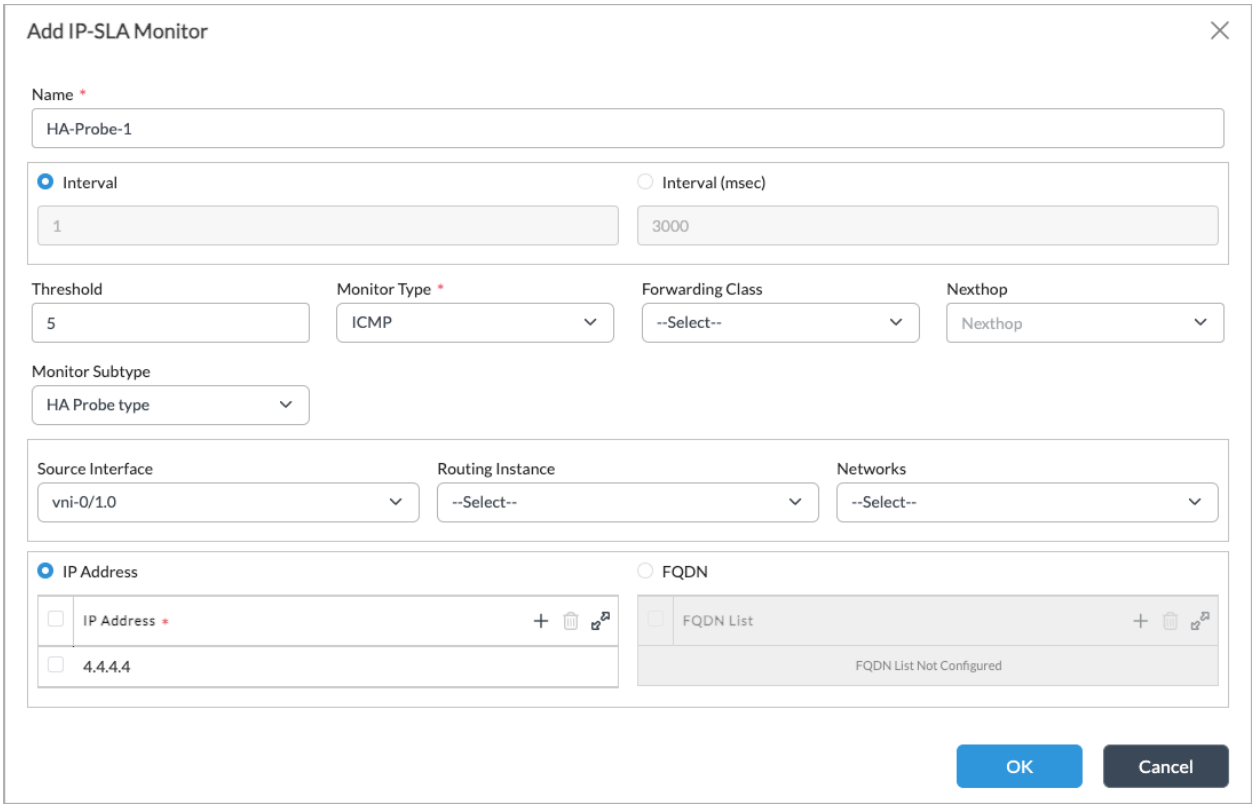
Configure Monitor Probes

To configure monitor probes for an interchassis HA pair:

1. In Director view:
   a. Select Configuration in the top menu bar.
   b. Select an organization in the horizontal menu bar.
   c. Select Devices > Devices in the horizontal submenu bar.
   d. Select a device in the Devices table in the main pane. The view changes to Appliance view.
2. Select Configuration in the top menu bar.
3. Select Networking > IP-SLA > Monitor in the left menu bar.
4. Click the + Add icon to create an HA monitor probe.



5. Click the + Add icon. The Add IP SLA Monitor popup window displays.



Field	Description
Name	Enter a name for the HA probe monitor element.
Interval	Enter how often, in seconds, to send ICMP packets to the IP address. If you select HA Probe Type in the Monitor Subtype field, you must set this interval to 1 second. *Range:* 1 through 60 seconds *Default:* 3 seconds
Threshold	Enter the maximum number of ICMP packets to send to the IP address. If the IP address does not respond after this number, the destination is considered to be down. *Range:* 1 through 60 *Default:* 5 *Recommended:* 15 (when you select Monitor in the Monitor Subtype field)
Monitor Type	Select the type of packet to send to the IP address. This can be ICMP.
Monitor Subtype	Select HA Probe Type from the drop-down list.

Field	Description
Source Interface	Select the interface corresponding to the routing instance over which the probe packets are to be sent.
IP Address	Enter the IP address of the directly connected interface of the HA peer node.

6. Click OK.

For more information about configuring IP-SLA, see Configure IP SLA Monitor Objects.

Sample Configuration for Monitor Probes

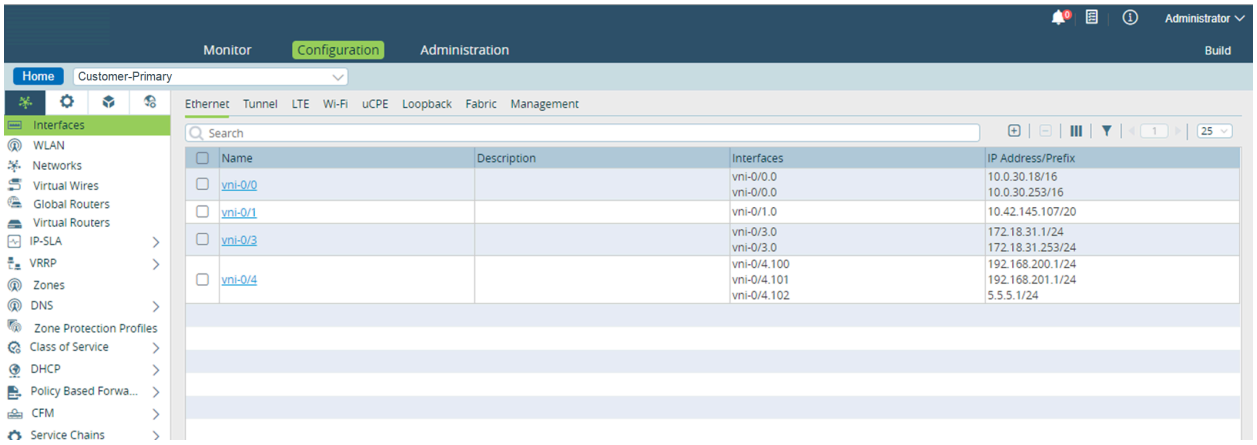
This section provides a sample of how to configure monitor probes for an HA interchassis pair of VOS devices. This example shows the following steps in the configuration process:

- Identify the physical interface, corresponding virtual routers, and IP addresses to use for the HA interchassis configuration.
- Create loopback interfaces and assign the IP addresses for the HA probe configuration.
- Add loopback interfaces to the virtual routers based on the virtual router's assigned IP address and on the physical interface through which the IP address is routed.
- Add HA monitor probes, which install routes and monitor next hops for each loopback interface.
- Attach the HA monitor probe to the corresponding the static route.

To create the sample configuration and view the HA monitor probes:

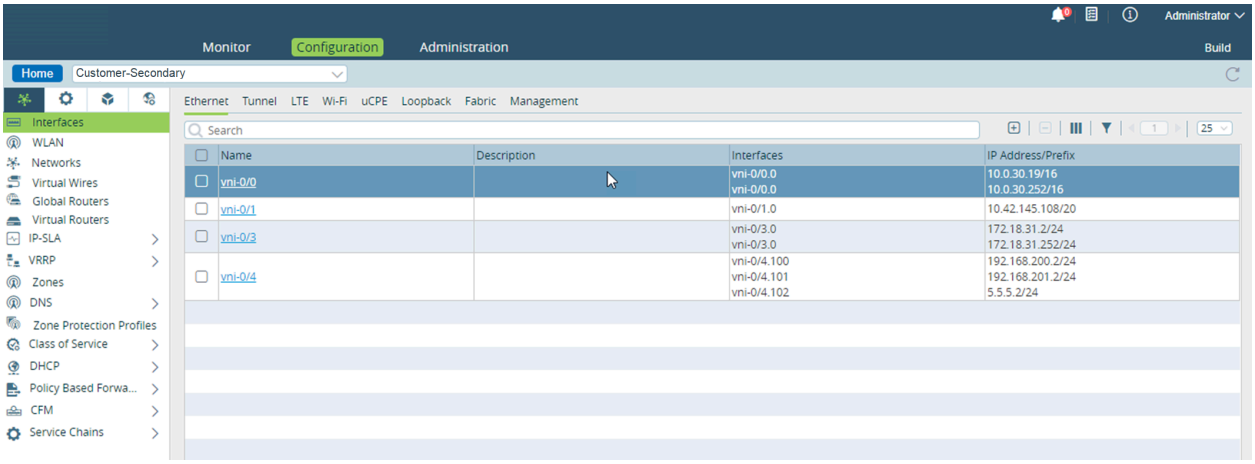
1. In Director mode, from the Configuration tab, select Devices > Devices, and then select the active device. In this example, the active device is called Customer-Primary.

2. In the Customer-Primary appliance view, select Configuration > Networking > Interfaces > Ethernet. On this screen, identify the physical interface on the primary device and its assigned IP address.



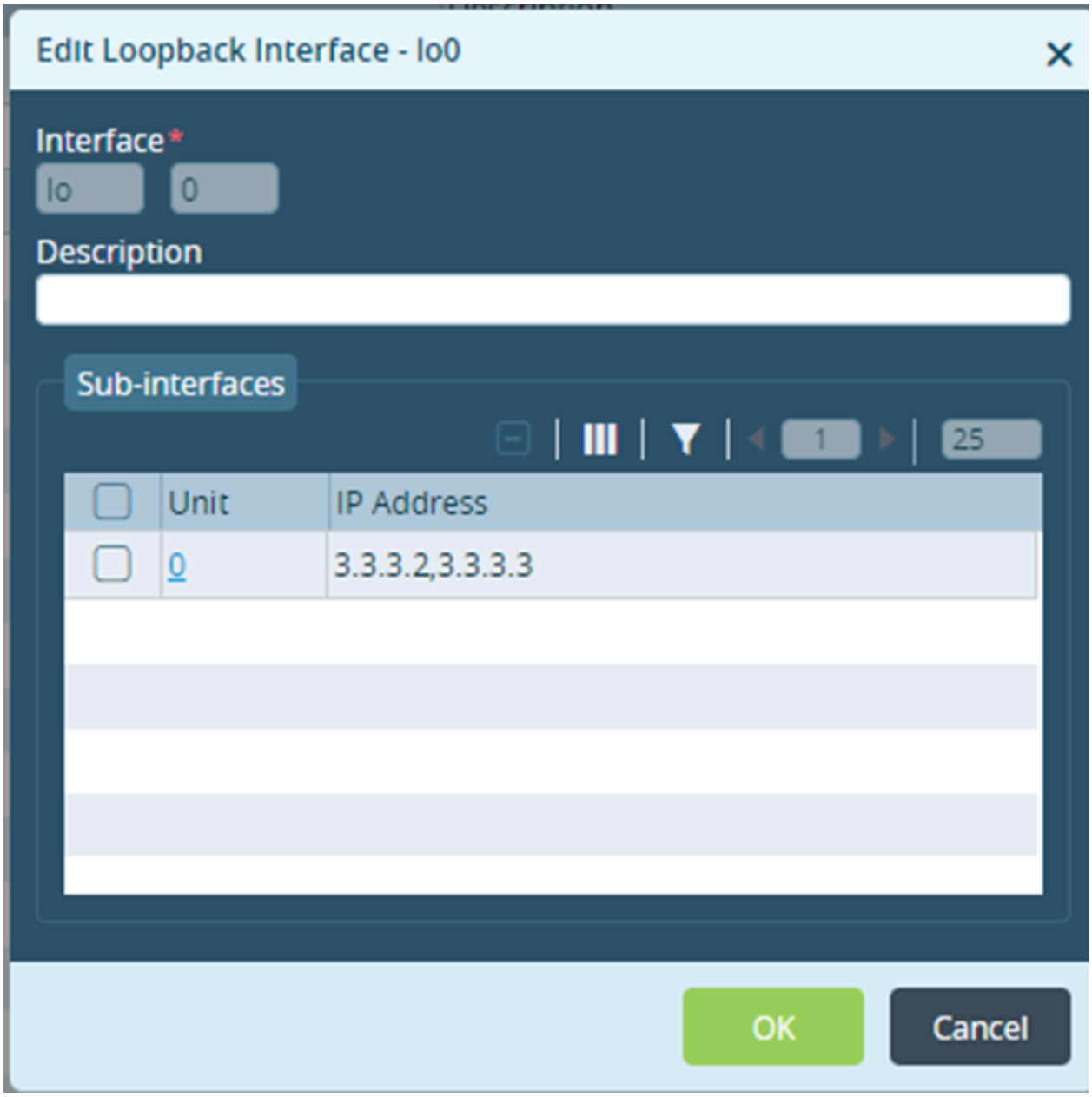
3. Similarly, for the standby device, in Director mode, from the Configuration tab, select Devices > Devices, and then select the standby device. In this example, the standby device is called Customer-Secondary

4. In the Customer-Secondary appliance view, select Configuration > Networking > Interfaces > Ethernet. On this screen, identify the physical interface on the secondary device and its assigned IP address.



5. In Customer-Primary appliance view, select Configuration > Networking > Interfaces > Loopback.

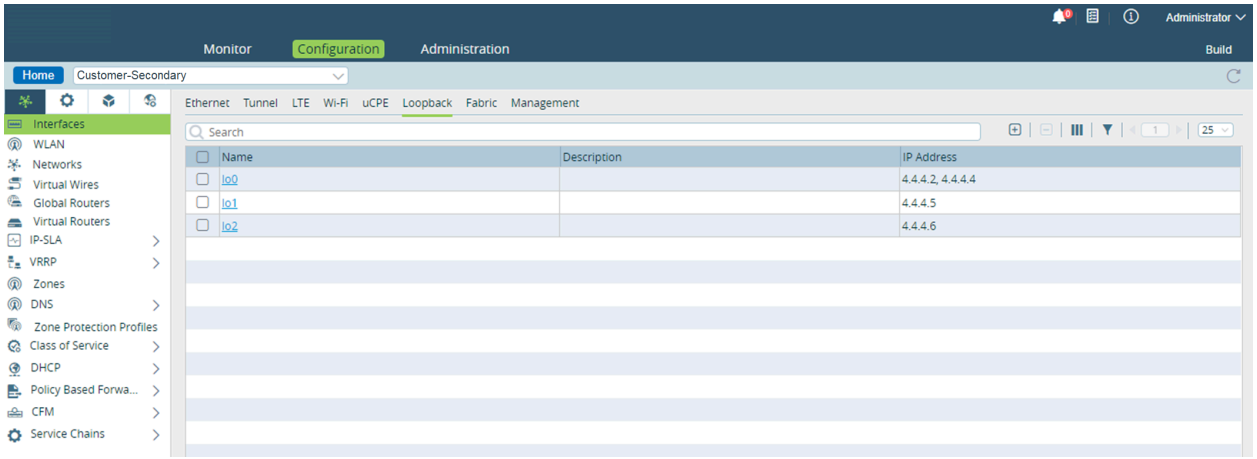
6. Click the Add icon, and create one loopback interface for each virtual router physical interface on which the primary device can reach the secondary device. Loopback interfaces are lo0, lo1, lo2, and so forth.



To view the virtual router physical interface that you configured on the primary device, select Configuration > Networking > Networks:

7. In Customer-Secondary appliance view, select Configuration > Networking > Interfaces > Loopback.

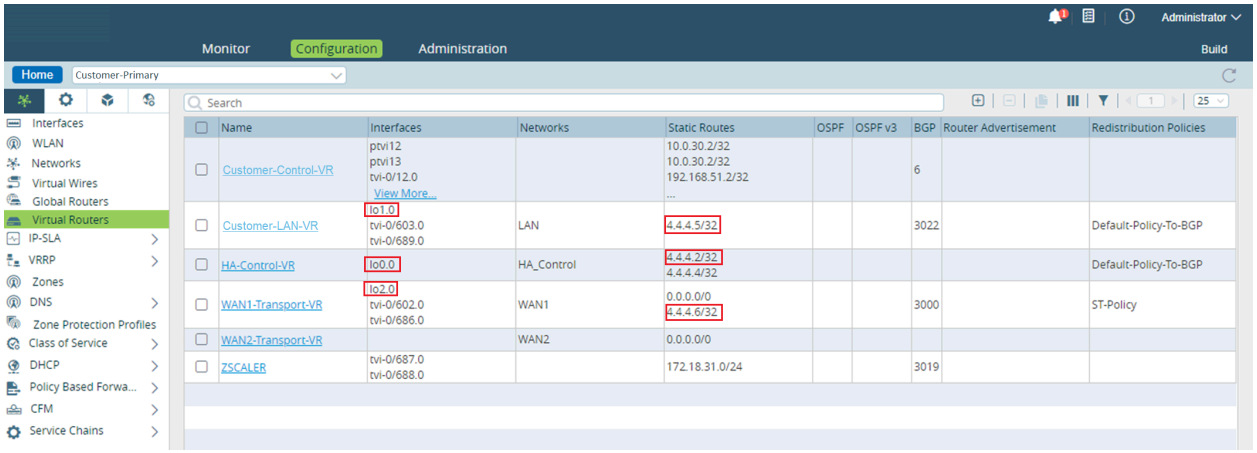
8. Click the Add icon, and create one loopback interface for each virtual router physical interface on which the secondary device can reach the primary device. Loopback interfaces are lo0, lo1, lo2, and so forth.



To view the virtual router physical interface that you configured on the secondary device, select Configuration > Networking > Networks:

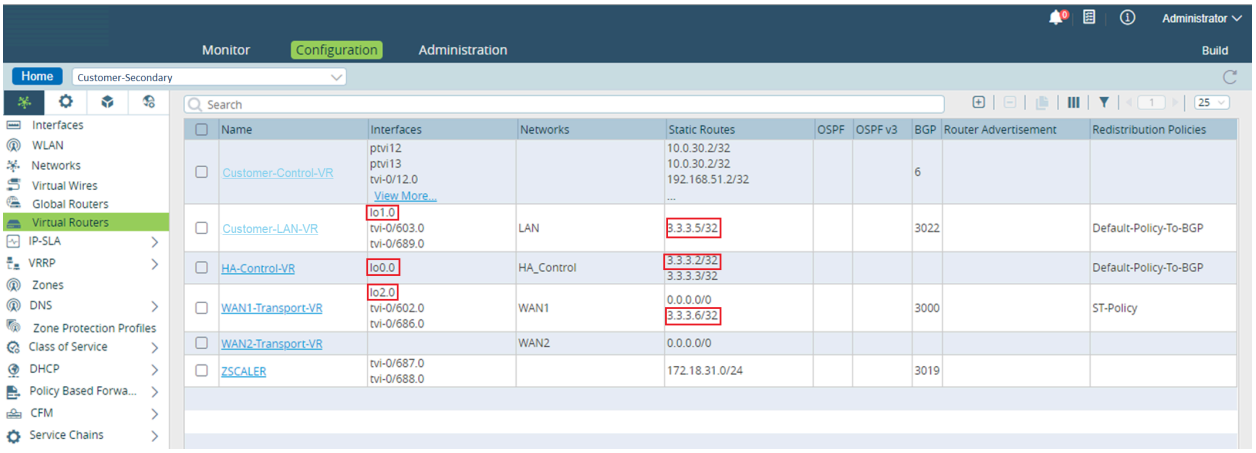
9. In Customer-Primary appliance view, select Configuration > Networking > Virtual Routers.

10. Click the Add icon and add the loopback interfaces to the correct virtual routers on the primary device. These are the loopback interfaces that you created on the primary device.



11. In Customer-Secondary appliance view, select Configuration > Networking > Virtual Routers.

12. Click the Add icon and add the loopback interfaces to the correct virtual routers on secondary appliance. These are the loopback interfaces that you created on the secondary device.

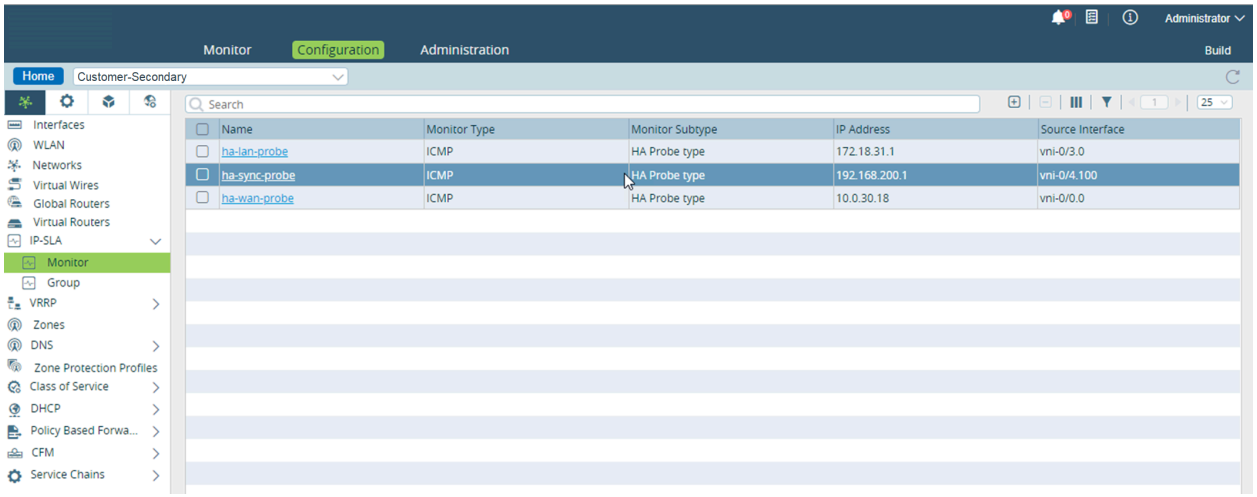


13. In Customer-Primary appliance view, select Configuration > Networking > IP-SLA > Monitor.

14. Click the Add icon, and add a monitor probe for each loopback interface pair that you have created on the primary device. This monitor probe periodically checks the reachability of peer interface on the VR.

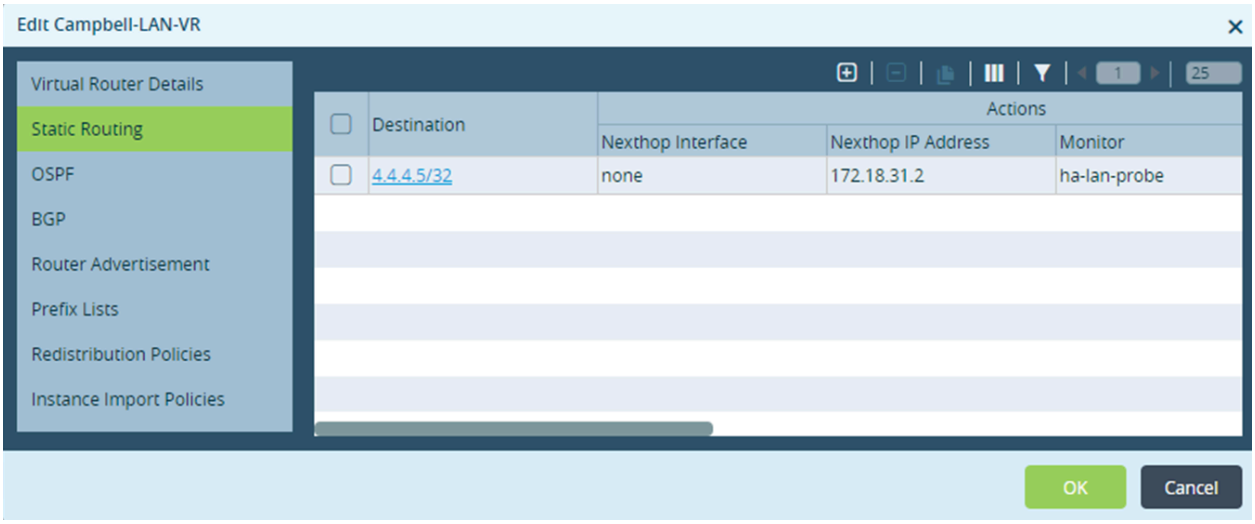
15. In Customer-Secondary appliance view, select Configuration > Networking > IP-SLA > Monitor.

16. Click the Add icon, and add a monitor probe for each loopback interface pair that you created on the standby device. This monitor probe periodically checks the reachability of peer interface on the VR.

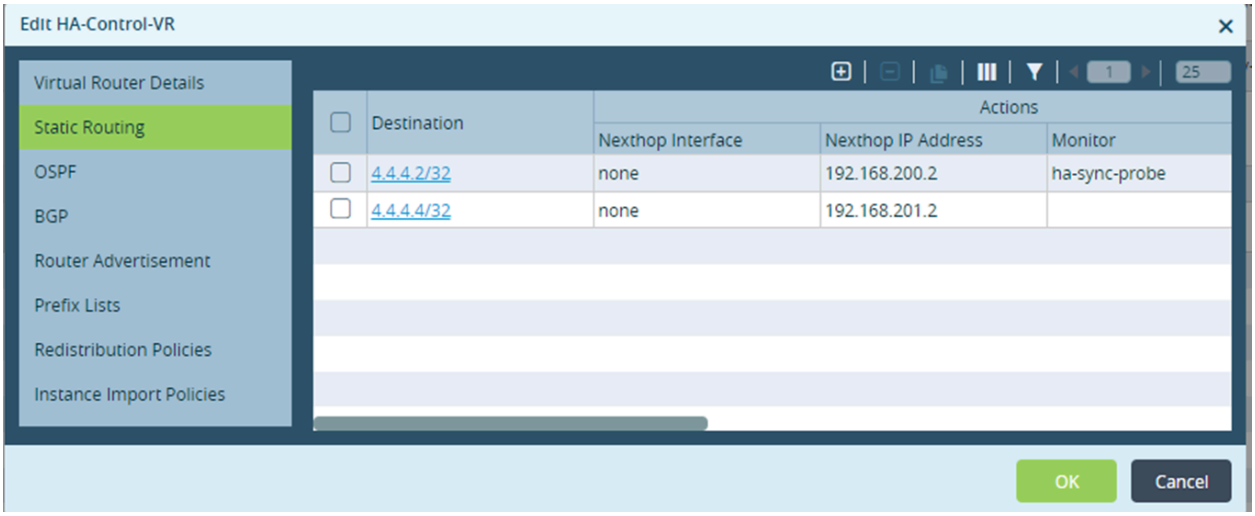


17. In Customer-Primary appliance view, select Configuration > Networking > Virtual Routers, and add static routes to the VRs. Adding a static route to a virtual router provides reachability to the loopback interface IP addresses through the physical interface IP addresses on the virtual router.

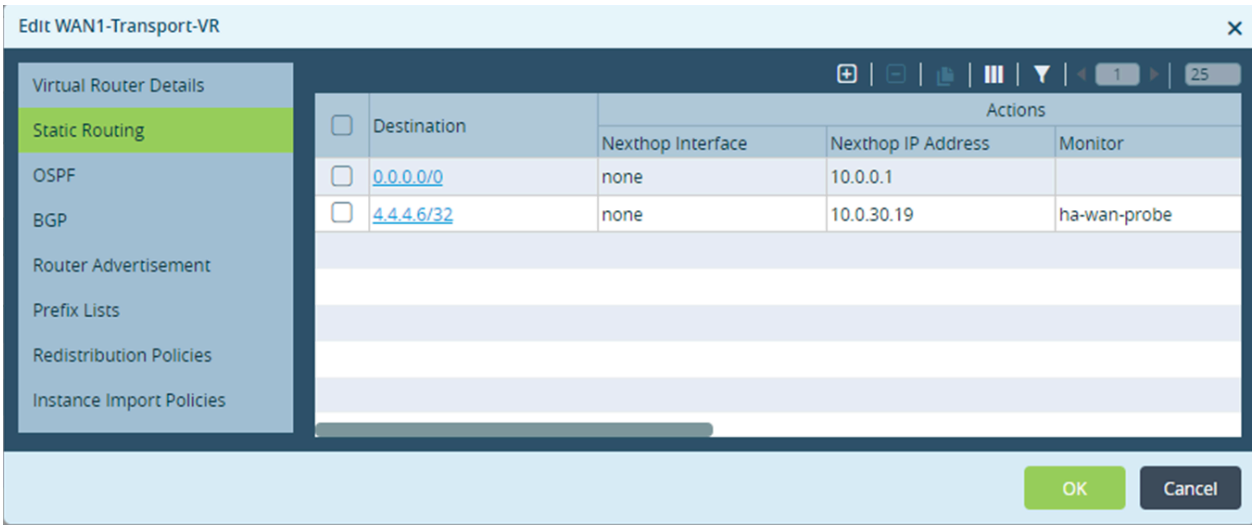
    a. Configure the static route for the LAN VR:



    b. Configure the static route for the HA control virtual router:

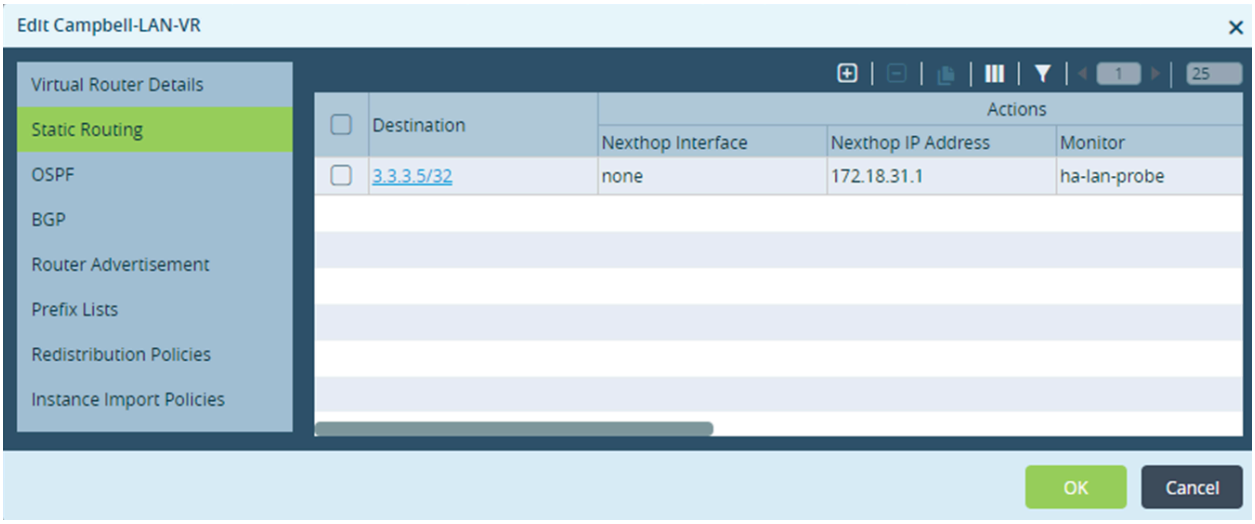


c. Configure the static route for the WAN transport virtual router:

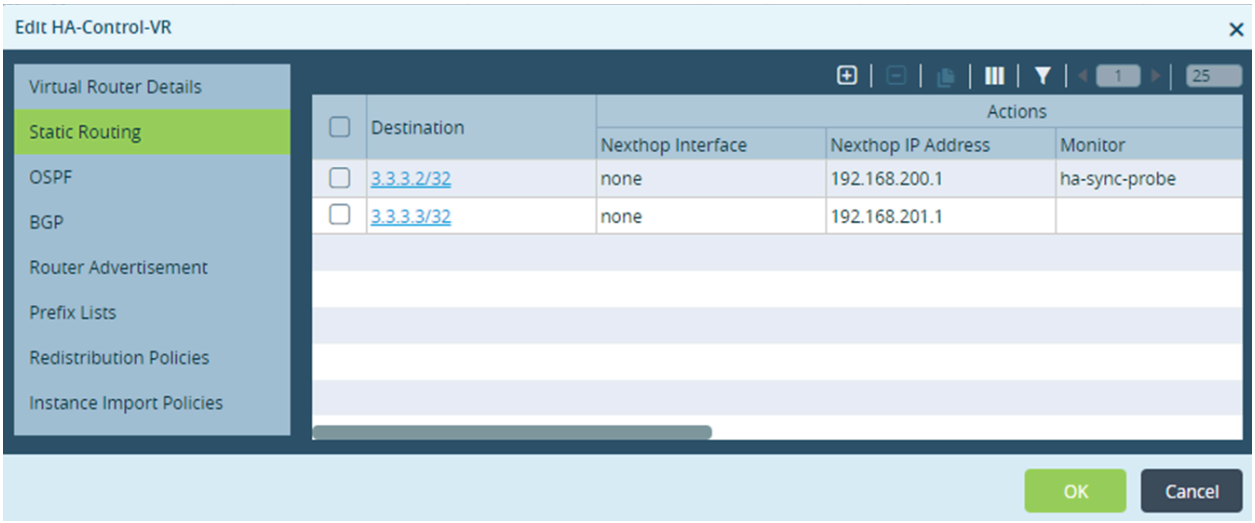


18. In Customer-Secondary appliance view, select Configuration > Networking > Virtual Routers, and add static routes to its virtual routers.

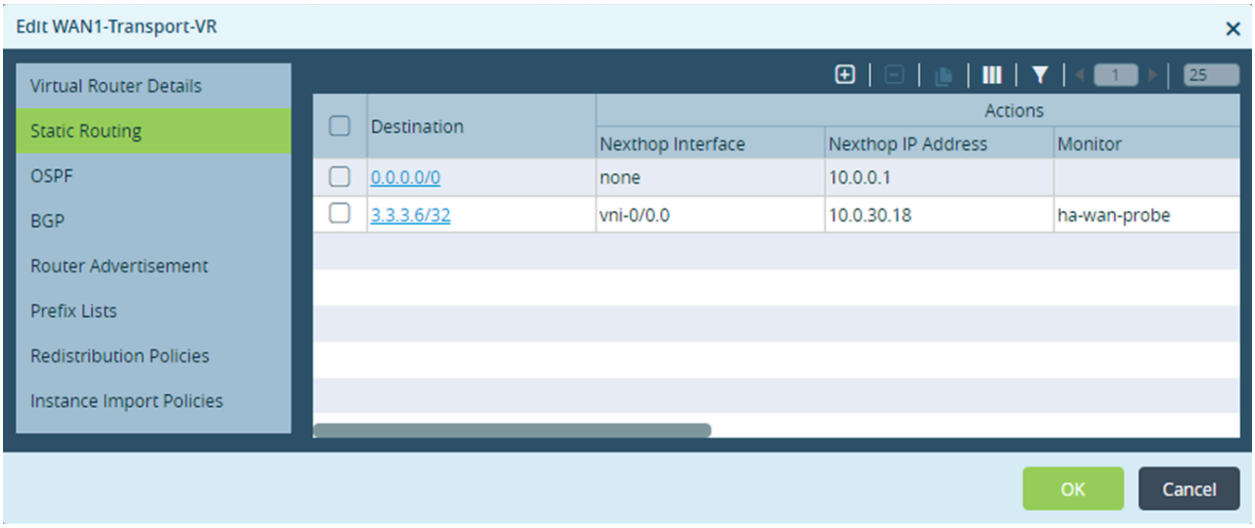
    a. Configure the static route for the LAN virtual router:



b. Configure the static route for the HA control virtual router:



c. Configure the static route for the WAN transport virtual router:



Verify HA Peers

(For Releases 20.2.3 and later.) This section describes CLI commands for displaying status information about HA redundancy peers. To access the CLI on a peer, see Access the CLI on a VOS Device.

To display summary information about HA nodes, issue the **show info-validation summary** command. For example:

```
admin@SDWAN-Branch1-cli> show info-validation summary
                                                    CONTROL  DATA
            WAIT  SELF IP        PEER IP        REGISTERED  CLIENT   PEER       SYNC     SYNC
MODE        TIME  ADDRESS       ADDRESS        APP COUNT   STARTED  REGISTERED  PAUSE
PAUSE  LAST PEER CONNECT
Active-Standby  1     10.230.122.107  10.230.122.108  1         true     true       true     true   2020-04-17
01:23:37 PDT
```

To display information about synchronization between HA peers, issue the **show info-validation conf-validation summary** command. For example:

```
admin@SDWAN-Branch1-cli> show info-validation conf-validation summary
                                  LAST
LAST CONFIGURATION      LAST CONFIGURATION      CONFIGURATION  LAST CONFIGURATION
COMPARE                 SYNC                    RECEIVED       UPDATE
2020-04-17 01:23:37 PDT  2020-04-17 01:23:37 PDT  -            2020-04-17 01:23:37 PDT
```

To display HA connection timeout information, issue the **show info-validation conf-validation app redundancy summary** command. For example:

```
admin@SDWAN-Branch1-cli> show info-validation conf-validation app redundancy summary
                                       SELF  PEER
DB KEY                                 VAL   VAL
/config/redundancy/inter-chassis/ctrl-connection-timeout  180   300
```

To display HA parameter values for both the local HA device (self) and its peer, issue the **show info-validation conf-validation app redundancy list** command. For example:

```
admin@SDWAN-Branch1-cli> show info-validation conf-validation app redundancy list
                                                                                                IS
DB KEY                                                                                SELF VAL        PEER VAL        MATCH
/config/redundancy/inter-chassis/bfd-liveness-detection/minimum-receive-interval          1000
1000            true
/config/redundancy/inter-chassis/bfd-liveness-detection/multiplier                        3               3               true
/config/redundancy/inter-chassis/bfd-liveness-detection/transmit-interval/minimum-interval 1000
1000            true
/config/redundancy/inter-chassis/ctrl-connection-timeout                                  180             300             false
/config/redundancy/inter-chassis/ctrl-routing-instance                                    HA-CONTROL-VR   HA-
CONTROL-VR      true
/config/redundancy/inter-chassis/local-ctrl-ip                                          172.16.1.107    172.16.1.107    true
/config/redundancy/inter-chassis/local-ip                                               10.1.1.107      10.1.1.107      true
/config/redundancy/inter-chassis/preferred-master                                         local-appliance  remote-appliance
true
/config/redundancy/inter-chassis/quorum-probe/probe-id                                    1               1               true
/config/redundancy/inter-chassis/quorum-probe/probe-miss-limit                            30              30              true
/config/redundancy/inter-chassis/quorum-probe/probe-miss-threshold                        30              30
true
/config/redundancy/inter-chassis/quorum-probe/probe-type                                  monitor-probe   monitor-
probe     true
```

To display HA parameter values for the peer only, issue the **show info-validation conf-validation app redundancy peer** command. For example:

```
admin@SDWAN-Branch1-cli> show info-validation conf-validation app redundancy peer
DB KEY                                                                                PEER VAL
/config/redundancy/inter-chassis/bfd-liveness-detection/minimum-receive-interval          1000
/config/redundancy/inter-chassis/bfd-liveness-detection/multiplier                        3
/config/redundancy/inter-chassis/bfd-liveness-detection/transmit-interval/minimum-interval 1000
/config/redundancy/inter-chassis/ctrl-connection-timeout                                  300
/config/redundancy/inter-chassis/ctrl-routing-instance                                    HA-CONTROL-VR
/config/redundancy/inter-chassis/local-ctrl-ip                                          172.16.1.107
/config/redundancy/inter-chassis/local-ip                                               10.1.1.107
/config/redundancy/inter-chassis/preferred-master                                         remote-appliance
/config/redundancy/inter-chassis/quorum-probe/probe-id                                    1
/config/redundancy/inter-chassis/quorum-probe/probe-miss-limit                            30
/config/redundancy/inter-chassis/quorum-probe/probe-miss-threshold                        30
/config/redundancy/inter-chassis/quorum-probe/probe-type                                  monitor-probe
```

To display HA parameter values for the local HA device (self) only, issue the **show info-validation conf-validation app redundancy self** command. For example:

```
admin@SDWAN-Branch1-cli> show info-validation conf-validation app redundancy self
/config/redundancy/inter-chassis/bfd-liveness-detection/minimum-receive-interval          1000
/config/redundancy/inter-chassis/bfd-liveness-detection/multiplier                        3
/config/redundancy/inter-chassis/bfd-liveness-detection/transmit-interval/minimum-interval 1000
/config/redundancy/inter-chassis/ctrl-connection-timeout                                  180
/config/redundancy/inter-chassis/ctrl-routing-instance                                    HA-CONTROL-VR
```

```
/config/redundancy/inter-chassis/local-ctrl-ip                    172.16.1.107
/config/redundancy/inter-chassis/local-ip                         10.1.1.107
/config/redundancy/inter-chassis/preferred-master                 local-appliance
/config/redundancy/inter-chassis/quorum-probe/probe-id            1
/config/redundancy/inter-chassis/quorum-probe/probe-miss-limit    30
/config/redundancy/inter-chassis/quorum-probe/probe-miss-threshold 30
/config/redundancy/inter-chassis/quorum-probe/probe-type          monitor-probe
/config/redundancy/inter-chassis/redundant-mode                   all
/config/redundancy/inter-chassis/remote-ctrl-ip                   172.16.1.108
```

Troubleshoot Interchassis HA

Debug Control Plane HA

To debug HA control plane issues:

1. On the active device, check the redundancy status:

```
admin@active-ha-cli> show redundancy inter-chassis
APPLIANCE  VCN       VCN
INSTANCE   INSTANCE  SLOT  RED ROLE           IP
-------------------------------------------------------------------
Local      VCN0      0    *Active   (IN-SYNC)   192.168.46.134
Remote     VCN0      0     Standby   (UP)       192.168.46.135

                       RED
APPLIANCE  SNG              GROUP  VSN
INSTANCE   ID   SNG NAME     ID     ID   VID  RED ROLE
-------------------------------------------------------------------
Local      0    default-sng  1      0    2    Active(IN-SYNC)
Remote     0    default-sng  1      0    18   Standby(UP)
```

2. On the standby device, check the redundancy status:

```
admin@standby-ha-cli> show redundancy inter-chassis
  APPLIANCE  VCN       VCN
  INSTANCE   INSTANCE  SLOT  RED ROLE           IP
  -------------------------------------------------------------------
  Local      VCN0      0    *Standby   (IN-SYNC)  192.168.46.135
  Remote     VCN0      0     Active     (UP)       192.168.46.134

                         RED
  APPLIANCE  SNG              GROUP  VSN
  INSTANCE   ID   SNG NAME     ID     ID   VID  RED ROLE
  -------------------------------------------------------------------
  Remote     0    default-sng  1      0    2    Active(IN-SYNC)
  Local      0    default-sng  1      0    18   Standby(UP)
```

3. On the active device, access the debug CLI and check the status of the HA peers:

```
admin@active-ha-cli> vsh connect rfd
rfd> show rfd ha peers
Peer      Role      IP      Peer-Role  Ctrl-State Data-State   BFD-State
=============================================================================
Local     Standalone -      -         -      -            -
Remote    Active    4.4.4.4 Standby    Up        In Sync      Up
```

4. On the standby device, access the debug CLI and check the status of the HA peers:

```
admin@standby-ha-cli> vsh connect rfd
rfd> show rfd ha peers
Peer      Role      IP      Peer-Role  Ctrl-State Data-State   BFD-State
=============================================================================
Local     Standalone -      -         -      -            -
Remote    Standby   3.3.3.3 Active     Up      In Sync       Up
```

5. On the active device, check connectivity to the standby device for the loopback and external management addresses:

```
admin@active-ha-cli> ping 192.168.46.135 routing-instance wan1-vrf
PING 192.168.46.135 (192.168.46.135) 56(84) bytes of data.
64 bytes from 192.168.46.135: icmp_seq=1 ttl=64 time=3.65 ms
64 bytes from 192.168.46.135: icmp_seq=2 ttl=64 time=4.51 ms
64 bytes from 192.168.46.135: icmp_seq=3 ttl=64 time=31.2 ms
64 bytes from 192.168.46.135: icmp_seq=4 ttl=64 time=4.55 ms
--- 192.168.46.135 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 3.650/10.998/31.273/11.711 ms
```

```
admin@active-ha-cli> ping 10.40.122.23
PING 10.40.122.23 (10.40.122.23) 56(84) bytes of data.
64 bytes from 10.40.122.23: icmp_seq=1 ttl=64 time=0.274 ms
64 bytes from 10.40.122.23: icmp_seq=2 ttl=64 time=0.212 ms
64 bytes from 10.40.122.23: icmp_seq=3 ttl=64 time=0.244 ms
64 bytes from 10.40.122.23: icmp_seq=4 ttl=64 time=0.254 ms
--- 10.40.122.23 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.212/0.246/0.274/0.022 ms
```

6. On the standby device, check connectivity to the active device for the loopback and external management addresses:

```
admin@standby-ha-cli> ping 192.168.46.134 routing-instance wan1-vrf
PING 192.168.46.134 (192.168.46.134) 56(84) bytes of data.
64 bytes from 192.168.46.134: icmp_seq=1 ttl=64 time=3.38 ms
64 bytes from 192.168.46.134: icmp_seq=2 ttl=64 time=10.2 ms
64 bytes from 192.168.46.134: icmp_seq=3 ttl=64 time=2.34 ms
64 bytes from 192.168.46.134: icmp_seq=4 ttl=64 time=3.38 ms

--- 192.168.46.134 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3013ms
rtt min/avg/max/mdev = 2.346/4.831/10.207/3.132 ms
```

```
admin@standby-ha-cli> ping 10.40.122.22
```

```
PING 10.40.122.22 (10.40.122.22) 56(84) bytes of data.
64 bytes from 10.40.122.22: icmp_seq=1 ttl=64 time=0.268 ms
64 bytes from 10.40.122.22: icmp_seq=2 ttl=64 time=0.233 ms
64 bytes from 10.40.122.22: icmp_seq=3 ttl=64 time=0.203 ms
64 bytes from 10.40.122.22: icmp_seq=4 ttl=64 time=0.218 ms

--- 10.40.122.22 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.203/0.230/0.268/0.028 ms
```

Debug Data Plane HA

To debug HA data plane issues:

1. On the active device, check the redundancy status of the service nodes:

```
admin@active-ha-cli> show redundancy inter-chassis service nodes
                          RED
APPLIANCE  SNG              GROUP  VSN
INSTANCE   ID   SNG NAME     ID     ID   VID  RED ROLE
-------------------------------------------------------------
Local      0    default-sng  1      0    2    Active(IN-SYNC)
Remote     0    default-sng  1      0    18   Standby(UP)
```

2. On the active device, check the redundancy status of the service nodes:

```
admin@standby-ha-cli> show redundancy inter-chassis service nodes
                        RED
APPLIANCE  SNG             GROUP  VSN
INSTANCE   ID   SNG NAME    ID     ID   VID  RED ROLE
-------------------------------------------------------------
Remote     0    default-sng  1     0    2    Active(IN-SYNC)
Local      0    default-sng  1     0    18   Standby(UP)
```

3. View the following entries in the routing table:

```
admin@ha-cli> vsh connect vsmd
vsm-vcsn0> show filter global table v4 | grep 9878
 | 0x00280403 | A |  19 |   6 | 0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |   0-65535   |  9878-9878  |
 | 0x00290403 | A |  19 |   6 | 0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |  9878-9878  |     0-65535 |
```

```
vsm-vcsn0> show filter global table v4 | grep 3000
 | 0x00270403 | A |  19 |   6 | 0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |   0-65535 |  3000-3001  |
```

```
 vsm-vcsn0> show filter global table v4 | grep 3002
 | 0x00260403 | A |  19 |   6 | 0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |   0-65535 |  3002-3003  |
 | 0x00442403 | A |  19 |  17 | 0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |   0-65535 |  3002-3003  |
```

4. On the active device, check the peer connections:

```
admin@active-ha-cli> vsh connect vsmd
vsm-vcsn0> show vsm ha peer-connections
```

```
List of srvr connections:
Thread-Id     Srvr-IP       Srvr-Port
1             192.168.46.134    1024    (Listen)

List of peer connections:
Thread-Id     My IP           My-Port     Peer-IP         Peer-Port   State
1             192.168.46.134   1024        192.168.46.135  1026        (Accept)State-Up
```

5. On the active device, check the IPC statistics:

```
vsm-vcsn0> show vsm ha ipc-stats

 HA_CNTR_CONN_LISTEN              1
 HA_CNTR_CONN_ACCEPT              2
 HA_CNTR_CONN_NEW                 2
 HA_CNTR_CONN_DESTROY             1
```

6. View the following entries in the routing table:

```
admin@ha-cli> vsh connect vsmd
vsm-vcsn0> show filter global table v4 | grep 9878
 | 0x00280403 | A |  19 |   6 | 0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |   0-65535 |  9878-9878  |
 | 0x00290403 | A |  19 |   6 | 0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |  9878-9878  |     0-65535 |
```

```
vsm-vcsn0> show filter global table v4 | grep 3000
 | 0x00270403 | A |  19 |   6 | 0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |   0-65535 |  3000-3001  |
```

```
vsm-vcsn0> show filter global table v4 | grep 3002
 | 0x00260403 | A |  19 |   6 | 0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |   0-65535 |  3002-3003  |
 | 0x00442403 | A |  19 |  17 | 0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |   0-65535 |  3002-3003  |
```

Debug Data Plane Session Synchronization

1. On the active device, after it has sent traffic, check the customer NAT sessions:

```
admin@Active-cli> show orgs org Customer sessions nat
sessions nat 2 120
 source-ip         192.168.51.2
 destination-ip      192.168.61.2
 source-port       46040
 destination-port    80
 protocol          6
 nat-source-ip     102.70.201.2
 nat-destination-ip      192.168.61.2
 nat-source-port     46040
 nat-destination-port   80
```

2. On the active device, view the details of all sessions:

```
admin@active-ha-cli> vsh connect vsmd
vsm-vcsn> show vsf session all detail
Session ID: 200006b (NFP), Tenant ID: 101, Owner WT: 1
```

```
Protocol - Layer-3: 102, Layer-4: 6
Src Address: 192.168.51.2, Port: 46039
Dst Address: 192.168.61.2, Port: 80
Session Start Timestamp: 2743661
Session Last Active Timestamp: 2839029
Session Idle Timeout: 524288  Session Hard Timeout: 0
Session FDT key: 0x4600
Session First-Packet Mask: 0  Session Close Mask: 0x3b
Session Flags: 0xa8
Forward Flow:  (VRF ID: 0)
  Service Chain: 25 2 7 4 10 22
  Pkt-In Interest Mask: 0
  Pkt-Out Interest Mask: 0
  Data Interest Mask: 0
  Total Packets Count: 437, Dropped Packets Count: 0
  Total Bytes Count: 22853, Dropped Bytes Count: 0
  QOS Gen ID: 0
Reverse Flow:  (VRF ID: 0)
  Service Chain: 25 2 7 4 10 22
  Pkt-In Interest Mask: 0
  Pkt-Out Interest Mask: 0
  Data Interest Mask: 0
  Total Packets Count: 437, Dropped Packets Count: 0
  Total Bytes Count: 454236, Dropped Bytes Count: 0
  QOS Gen ID: 0
HA Information:
  Mapped session-id: 200006b
  Apps Sync Checkpoint Mask:  0x1040
NAT Flow (Installed):  (VRF ID: 0)
  L4 Protocol: 6
  Src Address: 102.70.201.2, Port: 46039
  Dst Address: 192.168.61.2, Port: 80
  Service Chain: 25 2 7 4 10 22
```

3. On the standby device, check the sessions. Ensure that you see an entry that is identical to the one on the active device.

```
admin@Standby-cli> show orgs org Customer sessions nat
sessions nat 2 20
 source-ip         192.168.51.2
 destination-ip      192.168.61.2
 source-port       46040
 destination-port    80
 protocol          6
 nat-source-ip     102.70.201.2
 nat-destination-ip 192.168.61.2
 nat-source-port     46040
 nat-destination-port  80
```

4. Run the vsh connect vsmd command to access debug CLI.
5. On the standby device, view the details of all sessions. Ensure that the mapped session ID matches the session ID of the active device.

```
admin@standby-ha-cli> vsh connect vsmd
vsm-vcsn> show vsf session all detail 101 all
Session ID: 2000012 (NFP), Tenant ID: 101, Owner WT: 1
  Protocol - Layer-3: 102, Layer-4: 6
  Src Address: 192.168.51.2, Port: 46039
  Dst Address: 192.168.61.2, Port: 80
  Session Start Timestamp: 2680569
  Session Last Active Timestamp: 2680569
  Session Idle Timeout: 524288  Session Hard Timeout: 0
  Session FDT key: 0x4600
  Session First-Packet Mask: 0  Session Close Mask: 0x1
  Session Flags: 0xa0
  Forward Flow:  (VRF ID: 0)
    Service Chain: 25 2 7 4 10 22
    Pkt-In Interest Mask: 0
    Pkt-Out Interest Mask: 0
    Data Interest Mask: 0
    Total Packets Count: 0, Dropped Packets Count: 0
    Total Bytes Count: 0, Dropped Bytes Count: 0
    QOS Gen ID: 0
  Reverse Flow:  (VRF ID: 0)
    Service Chain: 25 2 7 4 10 22
    Pkt-In Interest Mask: 0
    Pkt-Out Interest Mask: 0
    Data Interest Mask: 0
    Total Packets Count: 0, Dropped Packets Count: 0
    Total Bytes Count: 0, Dropped Bytes Count: 0
    QOS Gen ID: 0
  HA Information:
    Mapped session-id: 200006b
    Apps Sync Checkpoint Mask:  0x1040
  NAT Flow (Installed):  (VRF ID: 0)
    L4 Protocol: 6
    Src Address: 102.70.201.2, Port: 46039
    Dst Address: 192.168.61.2, Port: 80
    Service Chain: 25 2 7 4 10 22
```

Debug the Packet Punt Path

1. On the active device, check connectivity of TVI address that connects the active device to the standby device:

```
admin@active-ha-cli> ping 192.168.46.135 routing-instance wan1-vrf
PING 192.168.46.135 (192.168.46.135) 56(84) bytes of data.
64 bytes from 192.168.46.135: icmp_seq=1 ttl=64 time=3.65 ms
64 bytes from 192.168.46.135: icmp_seq=2 ttl=64 time=4.51 ms
64 bytes from 192.168.46.135: icmp_seq=3 ttl=64 time=31.2 ms
64 bytes from 192.168.46.135: icmp_seq=4 ttl=64 time=4.55 ms
--- 192.168.46.135 ping statistics ---
```

2. On the active device, view the following routing table entries:

```
admin@active-ha-cli> vsh connect vsmd
```

```
vsm-vcsn0> show filter global table v4 | grep 3002
 | 0x00260403 | A |  19 |   6 | 0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |   0-65535 |  3002-3003  |
 | 0x00442403 | A |  19 |  17 | 0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |   0-65535 |  3002-3003  |
```

3. On the standby device, check connectivity of TVI address that connects the standby device to the active device:

```
admin@standby-ha-cli> ping 192.168.46.134 routing-instance wan1-vrf
PING 192.168.46.134 (192.168.46.134) 56(84) bytes of data.
64 bytes from 192.168.46.134: icmp_seq=1 ttl=64 time=3.38 ms
64 bytes from 192.168.46.134: icmp_seq=2 ttl=64 time=10.2 ms
64 bytes from 192.168.46.134: icmp_seq=3 ttl=64 time=2.34 ms
64 bytes from 192.168.46.134: icmp_seq=4 ttl=64 time=3.38 ms
^C
--- 192.168.46.134 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3013ms
rtt min/avg/max/mdev = 2.346/4.831/10.207/3.132 ms
```

4. On the standby device, view the following routing table entries:

```
admin@standby-ha-cli> vsh connect vsmd
vsm-vcsn0> show filter global table v4 | grep 3000
 | 0x00270403 | A |  19 |   6 |    0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |   0-65535 |  3000-3001  |
```

```
vsm-vcsn0> show filter global table v4 | grep 3002
 | 0x00260403 | A |  19 |   6 |    0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |   0-65535 |  3002-3003  |
 | 0x00442403 | A |  19 |  17 |    0-1024 |  0.0.0.0/0  |  0.0.0.1/32 |   0-65535 |  3002-3003  |
```

Debug Quorum Probes

After you enable quorum probes on the pair of HA VOS devices, the standby VOS device might restart every few minutes. To debug this problem:

1. Check whether the HA monitor probes that the active VOS device is sending are reaching the standby device. On the Active VOS device, check the status of the HA monitor probes:

```
vsm-vcsn0> show monitor details
```

   In the command output, check that at least one HA monitor probe sent to the standby device has a status of Up. If no monitor probe has a status of Up, check the HA monitor probe configuration.

2. If at least one monitor probe has a status of Up and the standby device continues to restart every few minutes, capture the HA monitor probes that the active VOS device is sending to the standby device:

```
vsm-vcsn0> tcpdump vni-x filter 'icmp -w icmp.pcap'
```

   In the command output, verify that the HA header in the monitor probes is intact.

3. Check that the HA monitor probes that the standby VOS device received are in the expected format:

```
vty# show vsm rfm-common globals | grep HA
vty# show vsm statistics datapath | grep Probe
```

If you cannot change the HA monitor probe immediately, you can avoid restarting the Versa services on the standby VOS device by temporarily changing the quorum probe type configuration on the standby device from Monitor-VOAE-Probe to None-Probe.

If the **show alarms** command displays the haPeerStateReq alarm, but the /var/log/versa/versa-rfd.log log file shows no response from the Director:

1. Ensure that the active and standby VOS devices are able to reach the Director node.
2. Check the SLA metrics on both the active and standby VOS devices to verify that they can reach the Controller and Director nodes:

```
VOS# show orgs org organization-name sd-wan sla-monitor metrics
```

Track Downtime Settings for the Active HA Device

If you configure tracking of downtime settings when you configure interchassis HA, you can view the tracking status for the active interchassis HA device.

To display the tracking status for interchassis HA interfaces:

```
admin@SDWAN-Branch-cli> show redundancy inter-chassis track interfaces
INTERFACE  INTERFACE   VRF        INTERFACE COUNT     TENANT
NAME       INDEX       ID         STATUS              ID

vni-0/3    1056        wan2-vrf        Yes            Provider
```

To display the tracking status of interchassis HA routing peers:

```
admin@SDWAN-Branch5-cli> show redundancy inter-chassis track route-peers
RIB INST  ROUTE     ROUTE                 TRACKING  COUNT   ROUTE
IDX       PROTOCOL  INSTANCE   ROUTE PEER     STATUS    STATUS  STATUS

1         BGP       wan1-vrf   192.168.44.10  Enabled   No      Down
```

To display the tracking status of interchassis HA VRRP groups:

```
admin@SDWAN-Branch5-cli> show redundancy inter-chassis track vrrp-groups
VRRP   VRRP       VRRP    VRRP     MASTER    VRRP
GROUP  GROUP      GROUP   TRACK    DOWN      GROUP
ID     INTERFACE  STATE   STATUS   TIME      IPS

100    vni-0/1.0  Master  Enabled  0       [ 192.168.42.100 ]
```

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 20.2.3 adds the following CLI commands:
  - show info-validation summary
  - show info-validation conf-validation summary
  - show info-validation conf-validation app redundancy summary
  - show info-validation conf-validation app redundancy list
  - show info-validation conf-validation app redundancy peer
  - show info-validation conf-validation app redundancy self
- Release 22.1.1 supports configuring Interchassis HA using Workflow templates.

Additional Information

Configure ALG
Configure CGNAT
Configure Interfaces
Configure IP SLA Monitor Objects
Configure Paired CPE Devices and Location IDs
Configure User and Group Policy
Configure Virtual Routers
Configure VRRP
High Availability Alarms