Versa FlexVNF
Network and System Guide

v16.1R1

General Disclaimer

Although Versa Networks has attempted to provide accurate information in this guide, Versa Networks does not warrant or guarantee the accuracy of the information provided herein. Versa Networks may change the programs or products mentioned at any time without prior notice. Mention of non-Versa Networks products or services is for information purposes only and constitutes neither an endorsement nor a recommendation of such products or services or of any company that develops or sells such products or services.

ALL INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS," WITH ALL FAULTS, AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED OR STATUTORY. VERSA NETWORKS AND ITS SUPPLIERS HEREBY DISCLAIM ALL WARRANTIES RELATED TO THIS GUIDE AND THE INFORMATION CONTAINED HEREIN, WHETHER EXPRESSED OR IMPLIED OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON--INFRINGEMENT, OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

VERSA NETWORKS AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR REVENUES, COSTS OF REPLACEMENT GOODS OR SERVICES, LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF THE GUIDE OR ANY VERSA NETWORKS PRODUCT OR SERVICE, OR DAMAGES RESULTING FROM USE OF OR RELIANCE ON THE INFORMATION PROVIDED IN THIS GUIDE, EVEN IF VERSA NETWORKS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and other information used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Many of the Versa Networks products and services identified in this guide are provided with, and subject to, written software licenses and limited warranties. Those licenses and warranties provide the purchasers of those products with certain rights. Nothing in this guide shall be deemed to expand, alter, or modify any warranty or license or any other agreement provided by Versa Networks with any Versa Networks product, or to create any new or additional warranties or licenses.

Table of Contents

Preface

Introduction

This guide explains the network and system configuration for Versa FlexVNF using Versa Director.

Audience

This document is for experienced network and system administrators who are responsible for configuring and managing public and private cloud infrastructure. It is presumed that admins are aware of virtualization concepts, technologies, and setup of network devices.

Document conventions

Convention	Description
Bold	Represents UI elements.
Italics	Values to enter in the text fields or values in drop down menus.
Monospace	CLI or system code.
	Notes contain incidental information about the subject and call attention to exceptions.
	Tips provide great shortcuts, hints, and recommended settings/configurable values.
	Caution notes are used to call attention to information that helps prevent loss of configured settings/values or loss of data.

Glossary

Term	Description/Full Form
Address Pool	Address pool is the IP address list from which IP addresses are dynamically allocated by the DHCP server to clients requesting an IP address.
Aggregate interface	An aggregate interface is a bundle of Ethernet interfaces.
ARP	Address Resolution Protocol
CFM	CFM (Connectivity Fault Management) is a protocol to monitor the health of network links. Depending on network events (blocked port, blocked interface), an action is configured. This is done in an action profile.
DHCP	Dynamic Host Configuration Pool
Dot IP Address	A dot IP address (also known as a dotted quad address) refers to the notation to write four-byte IP address as a sequence of four decimal numbers separated by dots.
DSCP	Differentiated Services Code Point (DSCP) refers to the value or cost of the policy.
LEF	Log Export Functionality (LEF) is used to generate logs on an external device.

MPLS	Multiprotocol Label Switching
MTU	Maximum transmission unit. The size in bytes of largest protocol data unit that the port can receive or transmit.
RED	Random Early Detection
Router	A router is a device that forwards data packets along networks. A router is connected to at least two networks and is located at gateways, where two or more networks connect.
Service Node Group	A service node group is a logical grouping of network services, which include individual network services (for example, NAT, DHCP, and NTP). Additionally, various policies and quotas can be applied for the service node group (for example, elastic policy, traffic policing and shaping).
TTL	Time to Live (TTL) Condition is the number of hops that a packet can travel before being discarded by a router. It indicates the lifespan of a data packet.
VNI	Virtual Network Interface
Versa Director	VNF Manager for all controllers, SD-WAN hubs, and branch nodes. Versa Director is provisioned at one or more data centers with connectivity to management and control networks for the SD-WAN.
Versa Analytics	The Versa Analytics node provides a pre-integrated solution to a full operational visibility into the SD-WAN topology. The Analytics node gathers IPFIX data from the controller, hub, and branch sites and archives and displays this data in readily accessible formats.
VRRP	Virtual Router Redundancy Protocol

Related documentation

- Versa Director Installation and Basic Configuration Guide
- Versa FlexVNF Installation and Basic Configuration Guide
- Versa Analytics Installation Guide
- Versa FlexVNF Basic SD-WAN Configuration Guide
- Versa FlexVNF Advanced SD-WAN Configuration Guide
- Versa FlexVNF Security Configuration Guide
- Versa Director Monitor Guide

Technical support

support@versa-networks.com

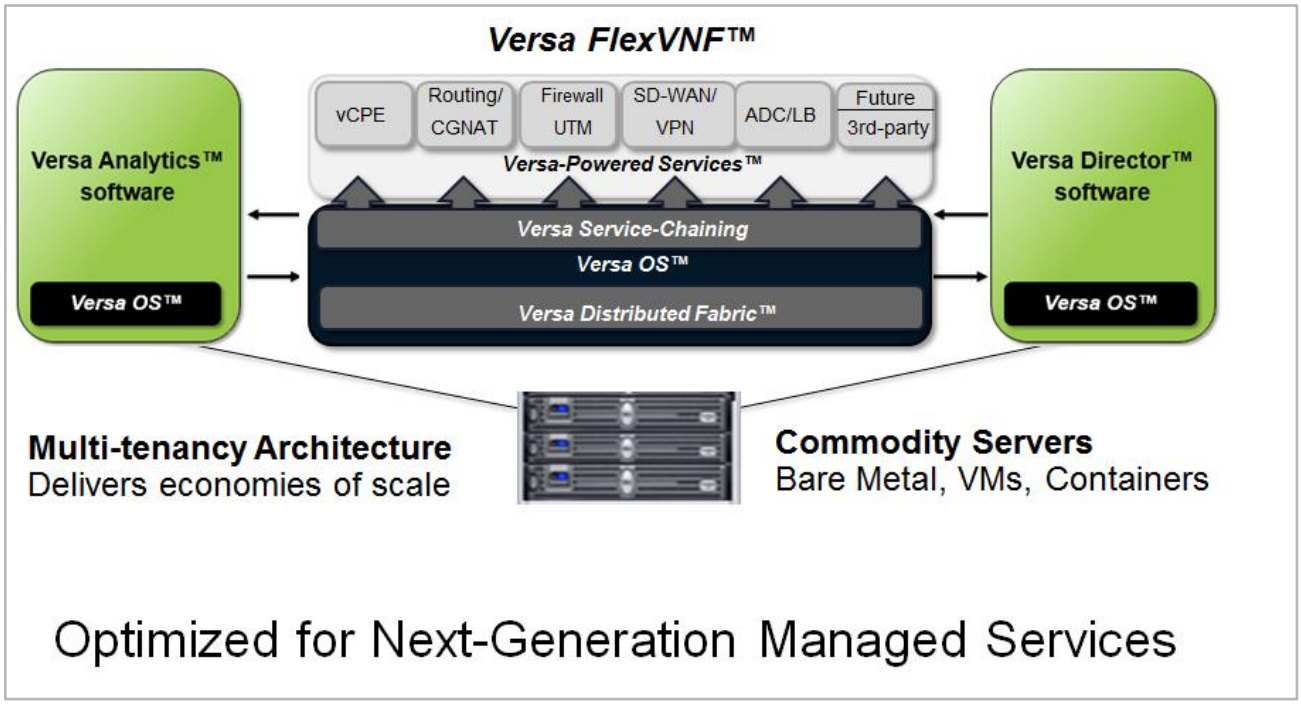
Chapter 1. Versa FlexVNF overview

Versa FlexVNF appliance is a virtual machine that lets you seamlessly configure and manage layer 4 through layer 7 network services for your data center. Versa FlexVNF can be installed on vCloud Director, bare metal, or OpenStack infrastructure. Versa FlexVNF enables you to configure and deploy the following network services:

- Next Generation Firewall
- Software Defined WAN
- Address Translation (CGNAT)
- vCPE
- Site to Site VPN Connectivity
- Application Delivery Controller (ADC)

The following illustration displays a Versa FlexVNF in a data center, with the deployed Versa virtual service nodes.

Versa Director enables you to create and deploy a Versa FlexVNF network service (firewall, ADC, etc.) on one or more service nodes in the cloud or physical network layer. Versa Analytics provides real time security and network reports on various services run by FlexVNF and managed by Versa Director. The following network topology illustration displays active Versa service nodes in a data center, configured and managed centrally via Versa Director.



Chapter 2. Configuring network services on Versa FlexVNF appliances

After installing Versa FlexVNF appliances in the network, you can set up the following network services on the appliances via Versa Director:

Versa Director v15.2R4 and higher supports HTTPS protocol, instead of HTTP.

Configuring interfaces

This section covers the following topics:

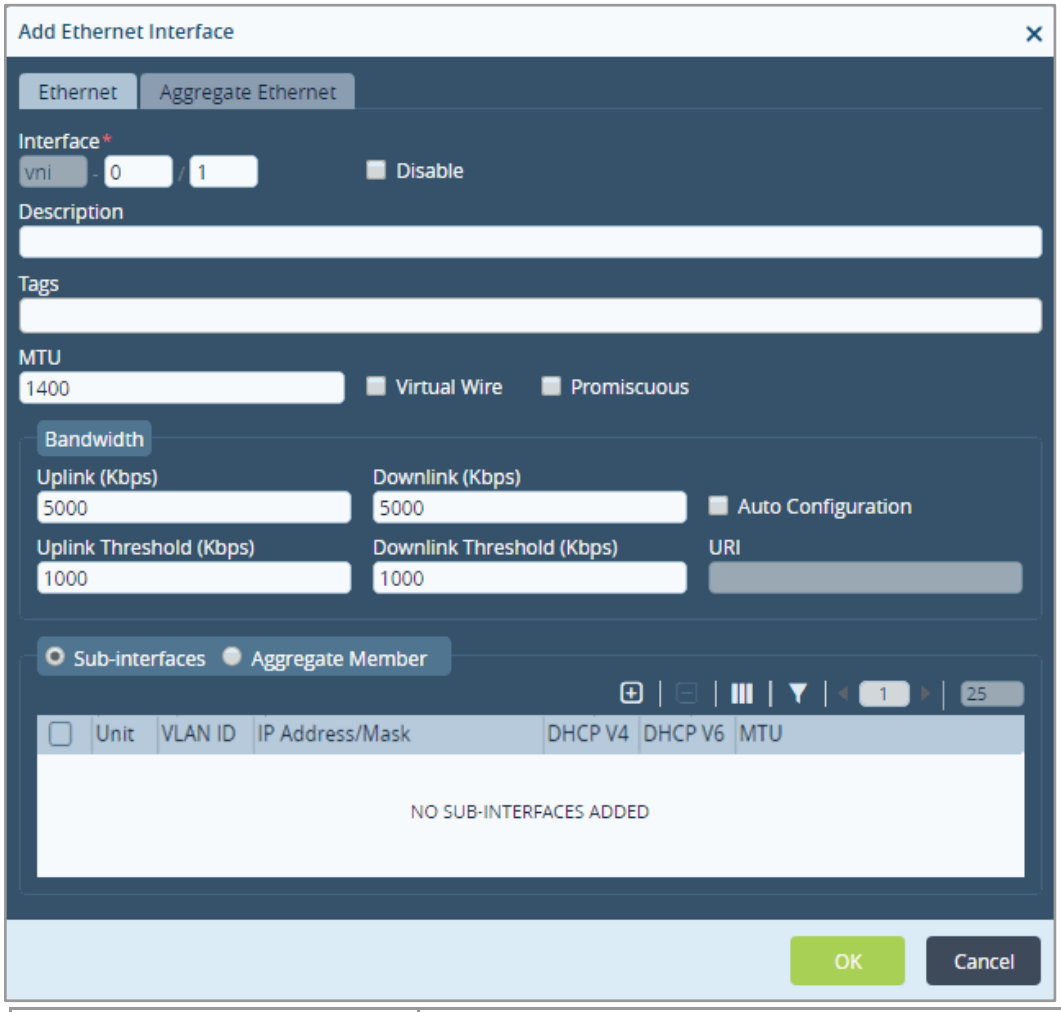
- Configuring Ethernet interfaces
- Configuring tunnel interfaces

Configuring Ethernet interfaces

Versa supports Ethernet interfaces (Gigabit Ethernet,10-Gigabit Ethernet and Aggregated Ethernet interface—a logical linkage of Gigabit Ethernet or 10-Gigabit Ethernet connections).

Steps

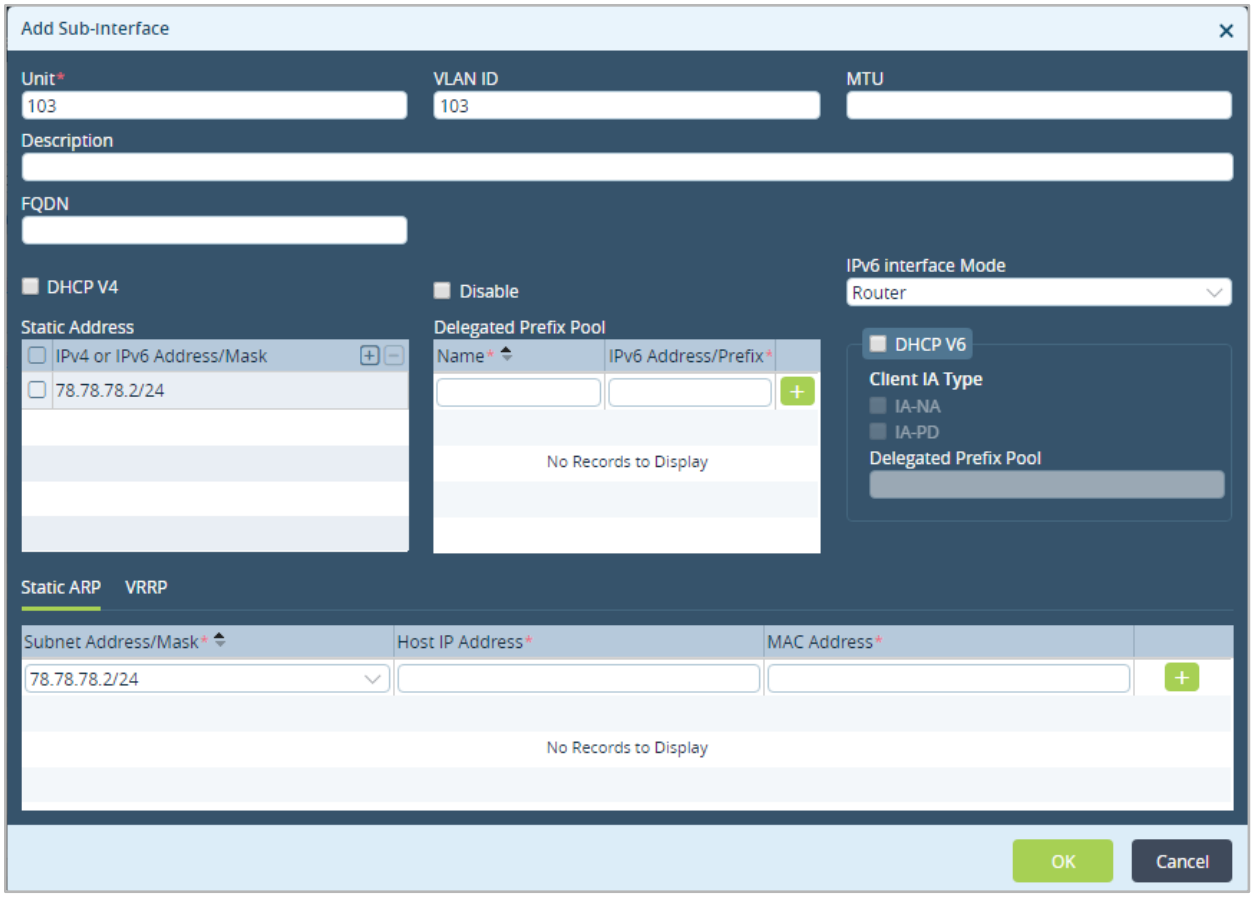
1. Under the *Appliance Context*, go to Configurations and select a controller. The Interfaces > Ethernet configuration page displays in the Networking panel.
2. Click on the top right corner to add an Ethernet interface.



Field	Description
Interface	vni interface port and slot numbers.

Disable	Indicates whether to not activate this interface after configuring it.
Description	Explanation for this interface—a string of a maximum of 255 characters.
MTU	Maximum transmission unit. The size in bytes of largest protocol data unit that the port can receive or transmit.
Virtual Wire	Indicates if the interface is part of a virtual wire. Upon selecting the check box, no other parameters can be configured.
Promiscuous	Indicates if the interface would accept all the data packet sent towards it.
Uplink and Downlink	Bandwidth of the link in kilobytes per second.
Uplink Threshold and Downlink Threshold	Base values required for uplink and downlink transmission. Uplink Threshold is the threshold bandwidth value required for uplink transmission. Any bandwidth below this value makes this link unusable. Downlink Threshold is the threshold bandwidth value required for downlink transmission. Any bandwidth below this value is not acceptable and the link becomes unusable. You do not need to configure Uplink and Downlink to configure these fields. When the uplink bandwidth goes beyond/below the given threshold, a trap and an alarm is generated. The same behavior replicates for downlink bandwidth.
Auto Configuration	Indicates whether to do an automated test of the system's downlink and uplink transmission bandwidth.
URI	Website to be used for auto testing.

3. Select the **Sub-interfaces** button and click  to add a sub-interface. An interface can have up to 4095 sub-interfaces.



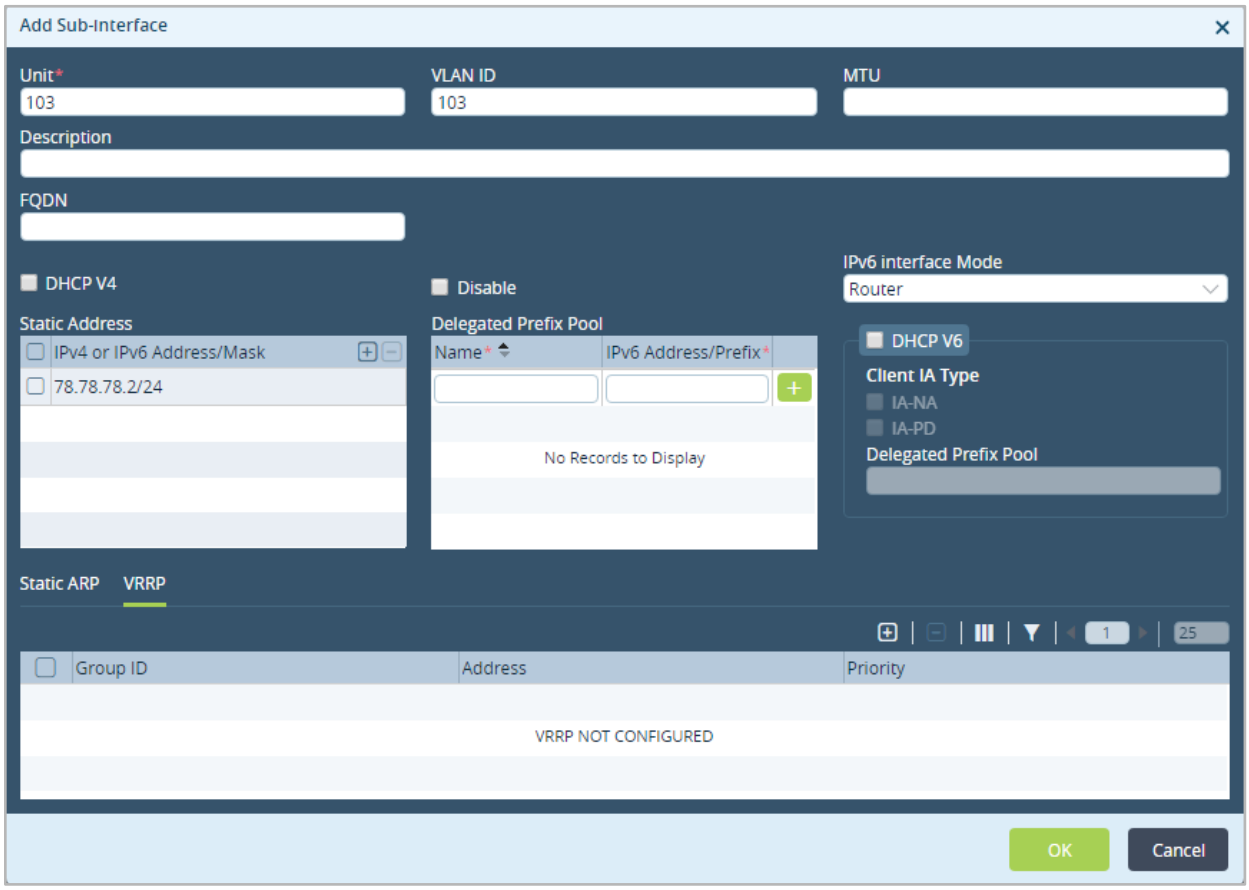
Field	Description
Unit	Unit number of the sub-interface.
VLAN ID	VLAN ID is the virtual LAN ID with a value of 0-4094.
MTU	Maximum transmission unit. The size in bytes of largest protocol data unit that the port can receive or transmit.
Description	Explanation for this interface—a string of a maximum of 255 characters.
FQDN	Fully qualified domain name (FQDN) is the complete domain name for the sub-interface.
DHCP V4	Dynamic Host Configuration Protocol (DHCP version IPv4) is a standardized network protocol used on Internet Protocol (IP) networks.
Disable	Indicates whether to not activate this sub-interface after configuring it.
IPv6 interface Mode	Select **Router** or **Host** as the IPv6 interface mode.
Static Address	IP address and subnet mask of the sub-interface.
Delegated Prefix Pool	Indicates the name and IP address of the delegated prefix pool.
DHCP V6	Dynamic Host Configuration Protocol (DHCP version IPv6) is a standardized network protocol used on Internet Protocol (IP) networks.

a. In the **Static ARP** (Address Resolution Protocol) tab, for a particular IP address, configure a static MAC address.

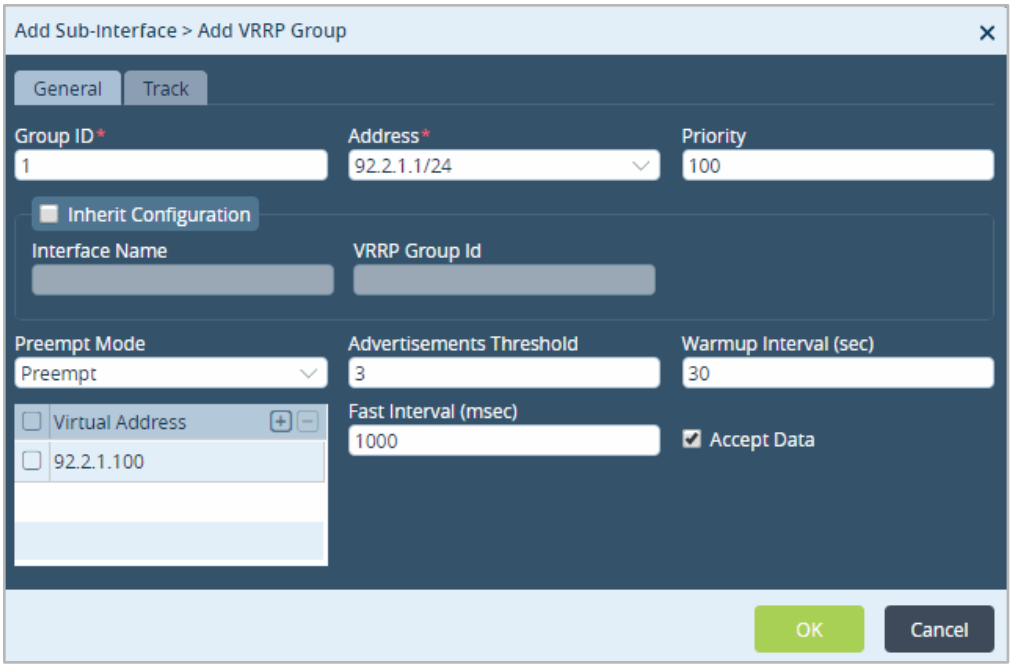
Field	Description
Subnet Address/Mask	This is the same as the provided static address.
Host IP Address	The value of this address must be within the given subnet.
MAC Address	This is the MAC address.

b. Click  . This configures a static ARP.

4. Click the **VRRP** (Virtual Router Redundancy Protocol) tab. Configure a VRRP master and VRRP slave device to function in the redundancy mode. This is the hidden HA (high availability) mode where the VRRP slave device takes over as the VRRP master device when the master device is down. This helps in ensuring an uninterrupted traffic flow.



a. In the **VRRP** tab, click  to add a VRRP group and enter the required values.

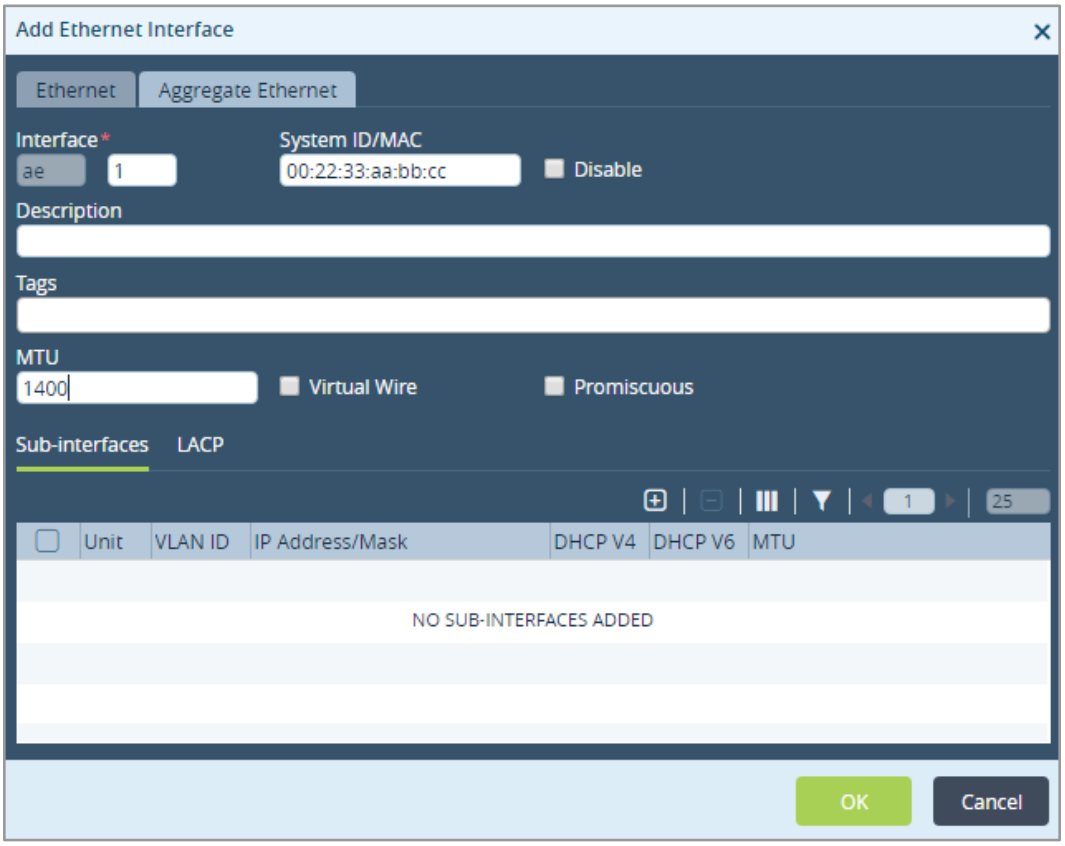


Field	Description
Group ID	ID of the VRRP group.
Address	IP address of the VRRP group.
Priority	Priority assigned to the group. A higher priority indicates that the VRRP device is a master device.
Inherit Configuration	Indicates if VRRP must inherit the properties of another sub-interface. After enabling the check box, select the name of the interface from the **Interface Name** list and enter the **VRRP Group ID**. All the other fields are disabled upon selecting **Inherit Configuration**.
Preempt Mode	• *Preempt* indicates that when the master device is down and the slave takes over as the master, the original master device would retake as the master as soon as it is back up. • *Non Preempt* indicates that when the master device is down and the slave takes over as the master, the original master would continue to function as the slave even after it is up again. The slave would continue as the master device.
Advertisements Threshold	The number of keep alive messages that are exchanged between two VRRP devices (master and slave).
Warm Threshold	Duration for which the sub-interface must wait to determine which of the two VRRP devices is the master and slave, respectively.
Fast Interval	Frequency at which the keep alive messages are exchanged between the master and slave VRRP devices. This is used in VRRP version 3.
Virtual Address	The virtual address(es) to be assigned to the VRRP device.
Accept Data	Indicates whether this sub-interface must accept data when received.

	Otherwise, the data is routed to another interface.

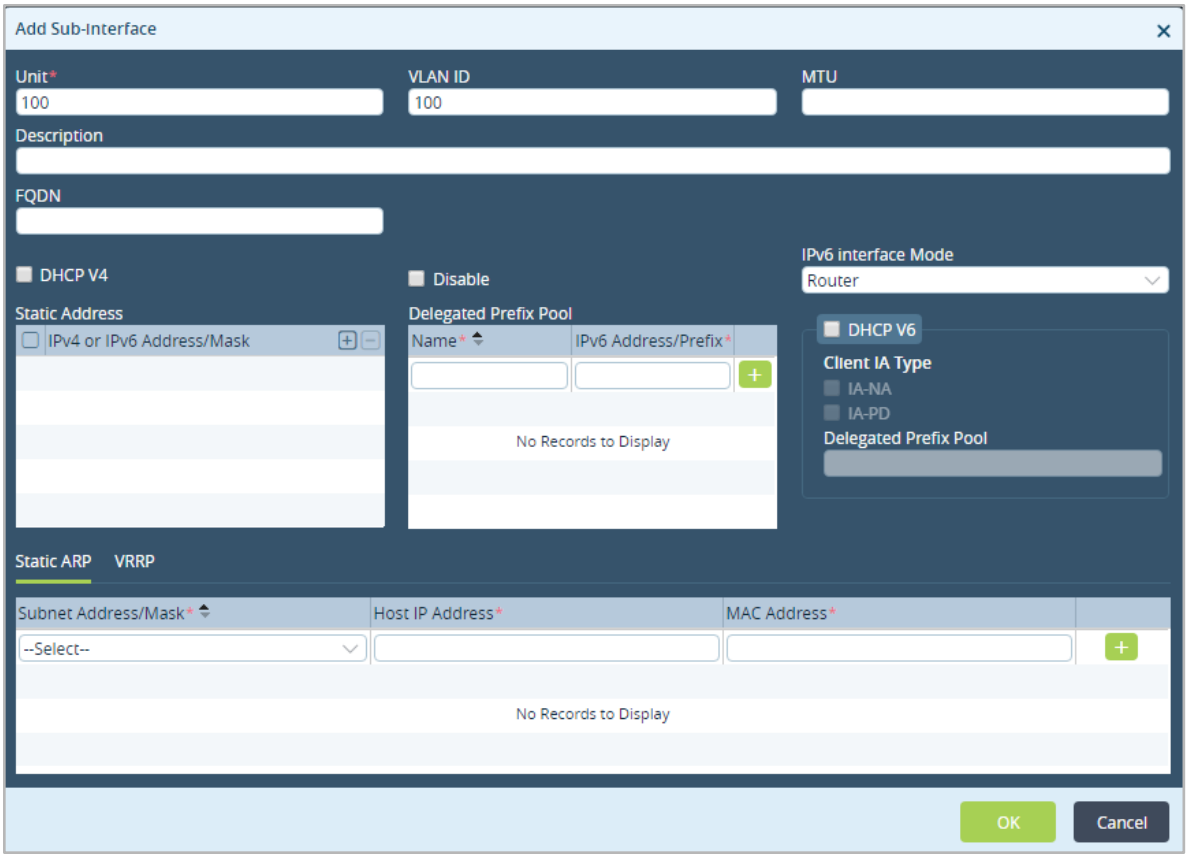
b. Click **OK** twice to complete adding the VRRP group and sub-interface.

5. Next, click the **Aggregate Ethernet** tab in the **Add Ethernet Interface** screen to configure an aggregate Ethernet interface. An aggregate interface is a bundle of Ethernet interfaces. It is the parent interface and has vni (Ethernet) interfaces as its children. The name of an aggregate interface starts with **aes**.



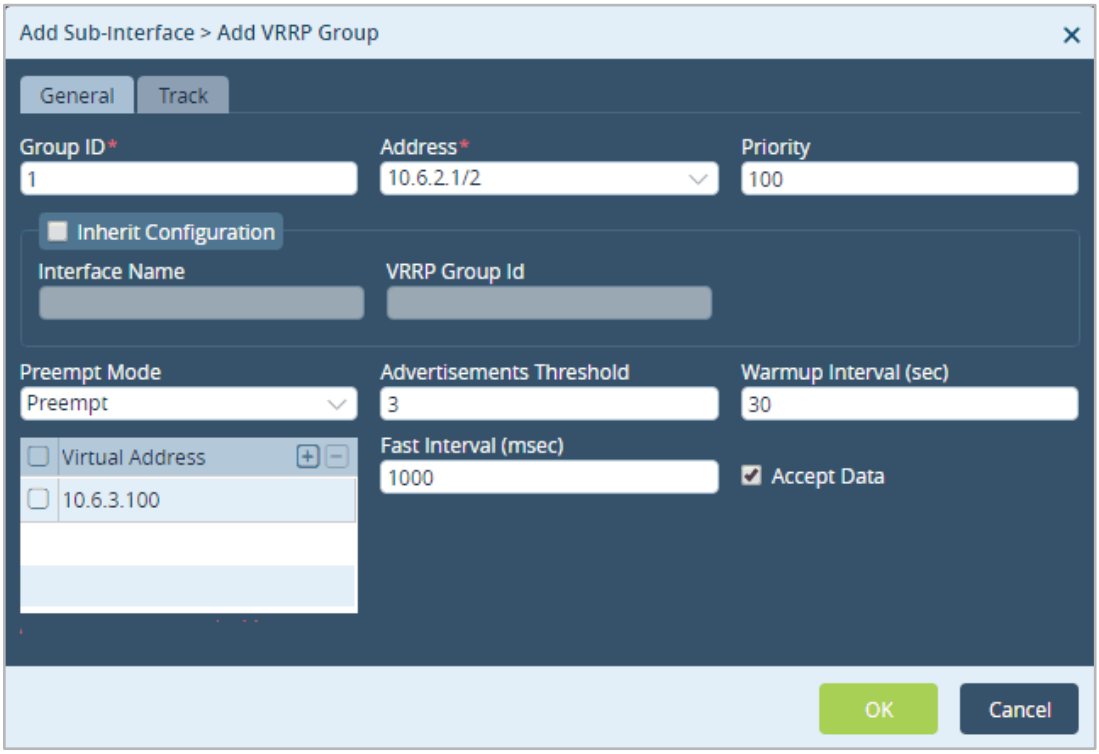
Field	Description
Interface	Interface port number.
System ID/MAC	MAC address of the interface.
Disable	Indicates whether to not activate this interface after configuring it.
Description	Explanation for this interface—a string of a maximum of 255 characters.
MTU	Maximum transmission unit. The size in bytes of largest protocol data unit that the port can receive or transmit.
Virtual Wire	Indicates whether the interface is a part of the virtual wire.
Promiscuous	Indicates whether to make this aggregate interface accept all the data packets that it receives.

a. In the **Sub-Interfaces** tab, click ⊞ on the top right corner to add a sub-interface.



Field	Description
Unit	Unit number of the sub-interface.
VLAN ID	VLAN ID is the virtual LAN ID with a value of 0-4094.
MTU	Maximum transmission unit. The size in bytes of largest protocol data unit that the port can receive or transmit.
Description	Explanation for this interface—a string of a maximum of 255 characters.
FQDN	Fully qualified domain name (FQDN) is the complete domain name for the sub-interface.
DHCP V4	Dynamic Host Configuration Protocol (DHCP-version 4) is a standardized network protocol used on Internet Protocol (IP) networks.
Disable	Indicates whether to not activate this sub-interface after configuring it.
IPv6 interface Mode	Select **Router** or **Host** as the IPv6 interface mode.
Static Address	IP address and subnet mask of the sub-interface.
Delegated Prefix Pool	Indicates the name and IP address of the delegated prefix pool.
DHCPv6	Dynamic Host Configuration Protocol (DHCP-version 6) is a standardized network protocol used on Internet Protocol (IP) networks.

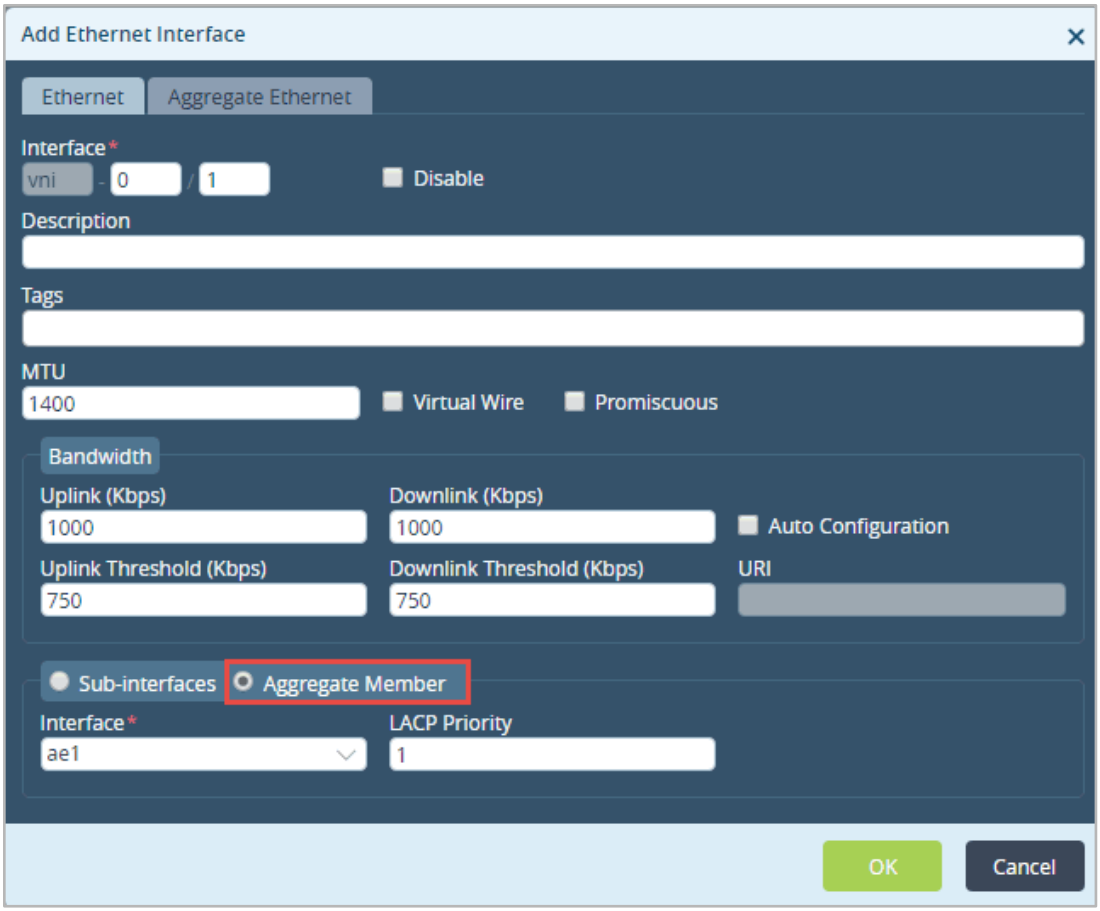
b. Click **VRRP** to configure a master and slave VRRP device for the hidden HA (high availability) mode. Refer to the steps in *Configuring Ethernet Interfaces* for information on how to configure a VRRP for an Ethernet interface.



c. Click **OK**. Repeat the above steps to add multiple sub-interfaces.

This configures an aggregate interface.

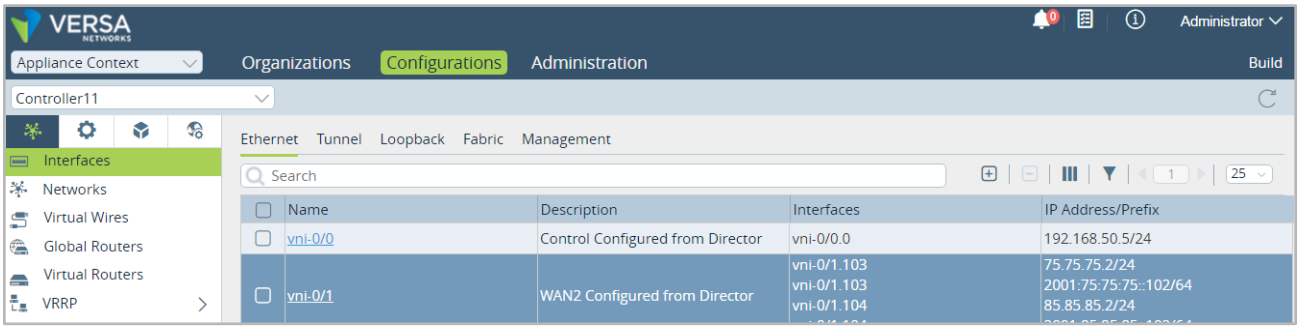
d. If an Ethernet interface is a part of an aggregate interface, you can specify the name of its parent aggregate interface. Select the **Aggregate Member** button on the **Add Ethernet Interface** page.



e. From the list shown under **Interface**, select the name of the aggregate interface and enter its **LACP (Link Aggregation Control Protocol) Priority** number. A LACP system priority is configured on each router running LACP. LACP uses the system priority with the router MAC address to form the system ID and also during negotiation with other systems. The LACP system ID is the combination of the LACP system priority value and the MAC address of the router.

6. Click **OK** on the **Add Ethernet Interface** screen .

This configures an Ethernet interface.



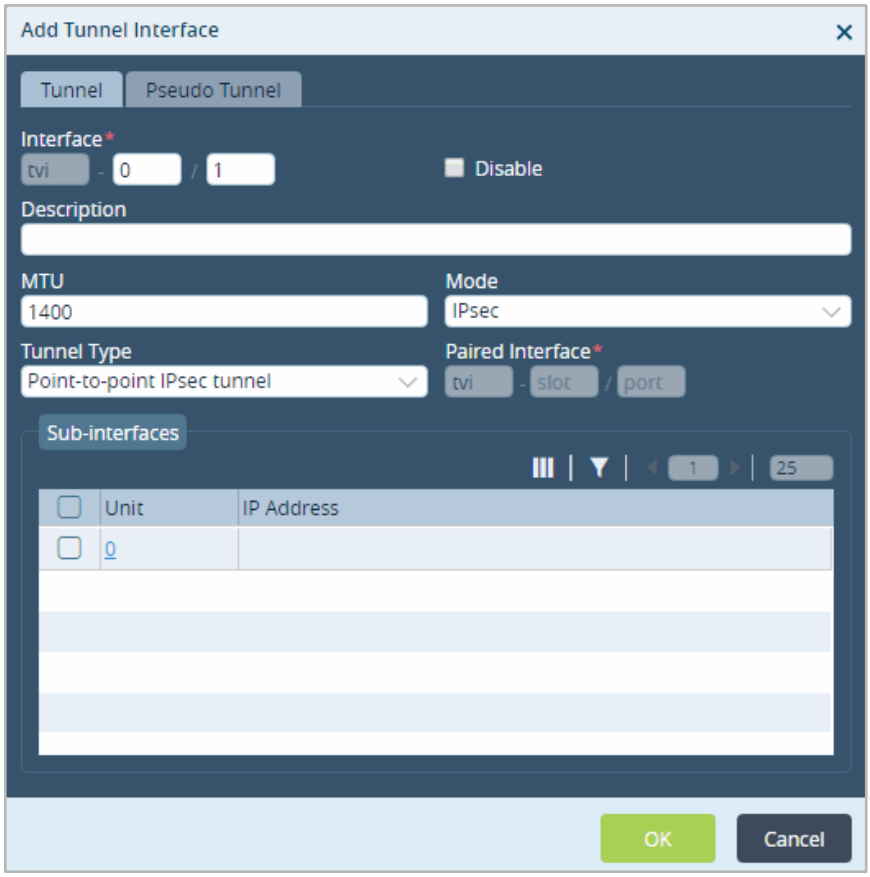
Next, configure tunnel interfaces.

Configuring Tunnel interfaces

Tunnel interfaces help configure an IPsec tunnel and High Availability (HA) between two Versa FlexVNF devices. In SD-WAN there are multiple tunnel interfaces to connect a branch with a controller.

Steps

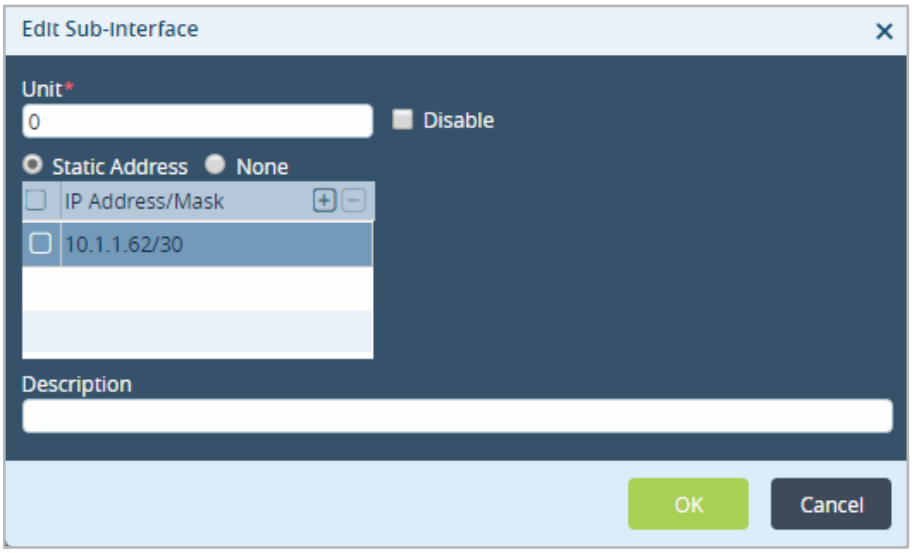
1. Under the *Appliance Context*, go to Configurations and select a controller. Click the Tunnel tab in the Networking panel. Click
2. Click on the top right corner to add a tunnel interface.



Field	Description
Interface	TVI interface port and slot numbers.
Disable	Indicates whether to not activate the tunnel interface after configuring it.
Description	Explanation for this interface—a string of a maximum of 255 characters.
MTU	Maximum transmission unit. The size in bytes of largest protocol data unit that the port can receive or transmit.
Mode	Mode of configuring the tunnel interface. There are two modes: ● *IPsec*. Select for IPsec configuration. ● *Redundancy*. Select for HA configuration.
Tunnel Type	There are multiple tunnel types: ● *Point-to-Point IPSec tunnel.* Select when configuring IPsec. ● *Point-to-multi-point VXLAN tunnel.* Select the IKE tunnel of IPsec configuration, which has two stages—IKE and IPsec—in that order. ● *Point-to-multi-point ESP tunnel.* Select for the IPsec tunnel of IPsec configuration. ● *Point-to-multi-point GRE tunnel.* To enable IPsec configuration between a local controller and a controller in the cloud, the tunnel

	interface mode is Point-to-multipoint GRE.
Paired Interface	TVI address as a paired address. Traffic directed to a paired interface is switched to the parent interface and vice versa.

3. Select an existing sub-interface and enter the required parameter values.

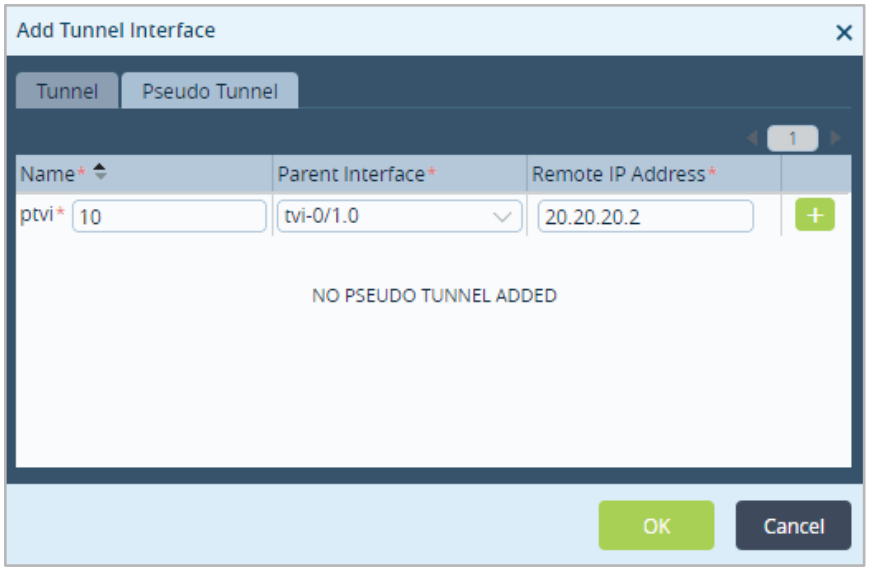


Field	Description
Unit	Unit number of the sub-interface. If the unit value is 0, VLAN ID is disabled. Else, enter the VLAN ID, which is the virtual LAN ID of the sub-interface.
Static Address	IP address and subnet mask of the sub-interface.

   a. In **Static Address**, enter an IP address or select the **None** button. For **None**, the controller assigns an IP address when the branch comes up.

4. Click **OK** to complete editing the sub-interface.

5. Now click the **Pseudo Tunnel** tab in the **Add Tunnel Interface** page and add the required values.

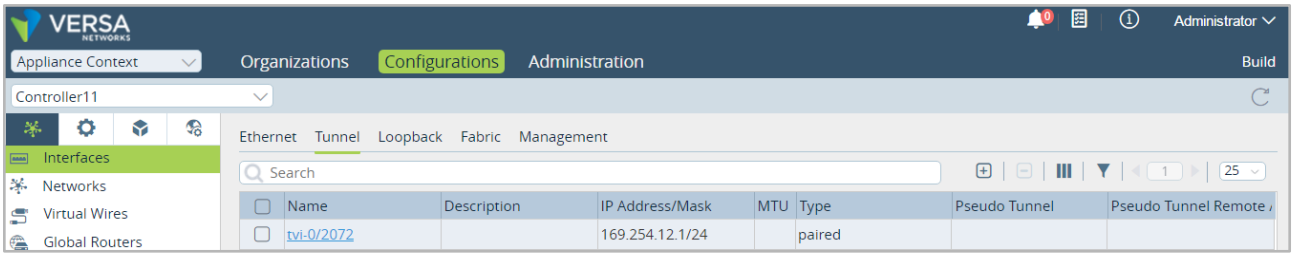


Field	Description
Name	Name of the PTVI (pseudo tunnel virtual interface).
Parent Interface	Name of the parent interface.
Remote IP Address	Remote address of the controller.

a. Click  . This adds a PTVI interface.
b. Click **OK**.

6. Click **OK** on the **Add Tunnel Interface** screen.

This configures a tunnel interface.



Configuring GRE tunnels

Versa Director supports configuring three types of GRE tunnels.

- IPv4 GRE
- Ethernet over GRE
- IPv6 GRE

All the above three tunnels have the following common input parameters:

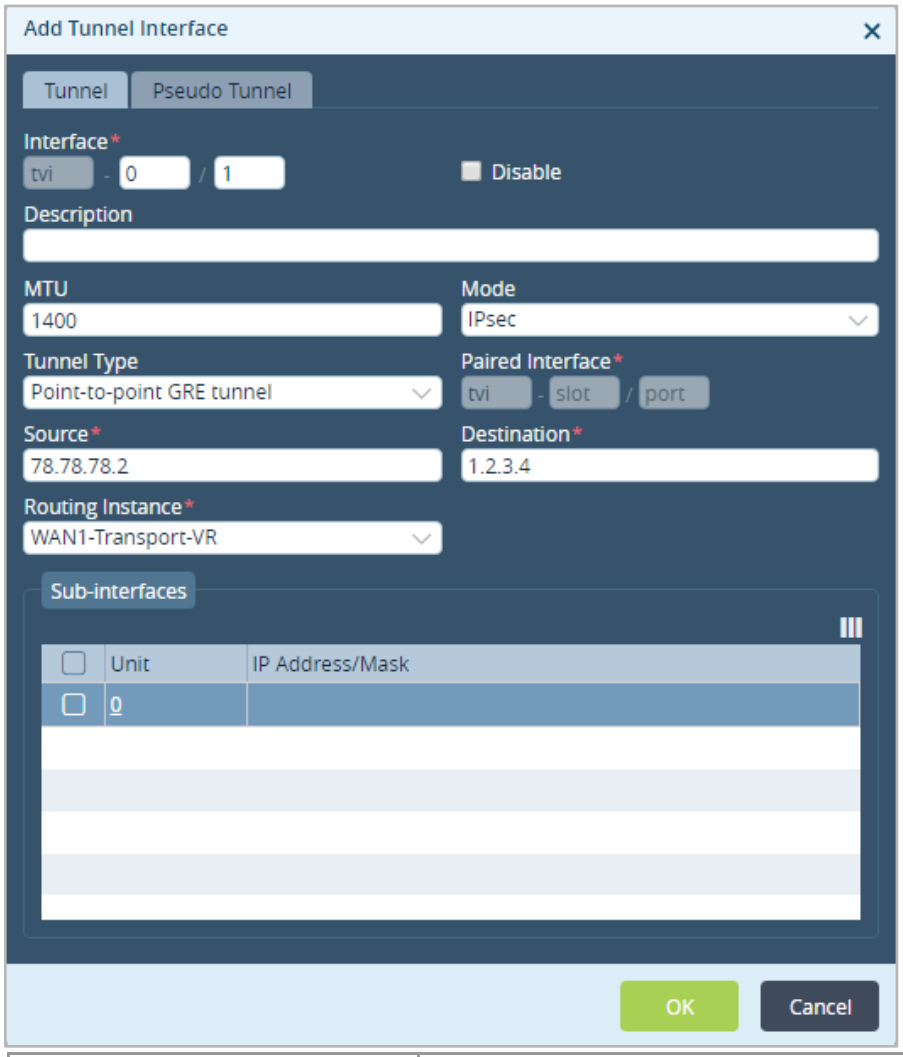
- **Source.** This is the IPv4 (GRE, Ethernet over GRE) or IPv6 (IPv6 GRE) address that must be configured on any of the local VNI/TVI interfaces. This parameter uses the source IP in the IPv4 header and adds as GRE encapsulation. The remote end sends packets back to this IP, so that if the packet is not configured in any local interface, then the packet does not terminate in FlexVNF.
- **Destination.** This is the IPv4 (GRE, Ethernet over GRE) or IPv6 (IPv6 GRE) address of the remote tunnel endpoint that can be any device supporting the GRE tunnel.

- **Routing instance.** This is the routing instance in which the VNI/TVI interface resides, using its IP address as a source in the GRE tunnel configuration.

GRE and IPv6 GRE can have only unit 0, while Ethernet over GRE can have VLANS from 0 to 4095. Unit supports both IPv4 and IPv6 addresses. Thus, TVI interface applies in the routing instance and organization like other TVIs. To send packets over the GRE tunnel, the administrator needs to route traffic to the GRE TVI interface.

Steps

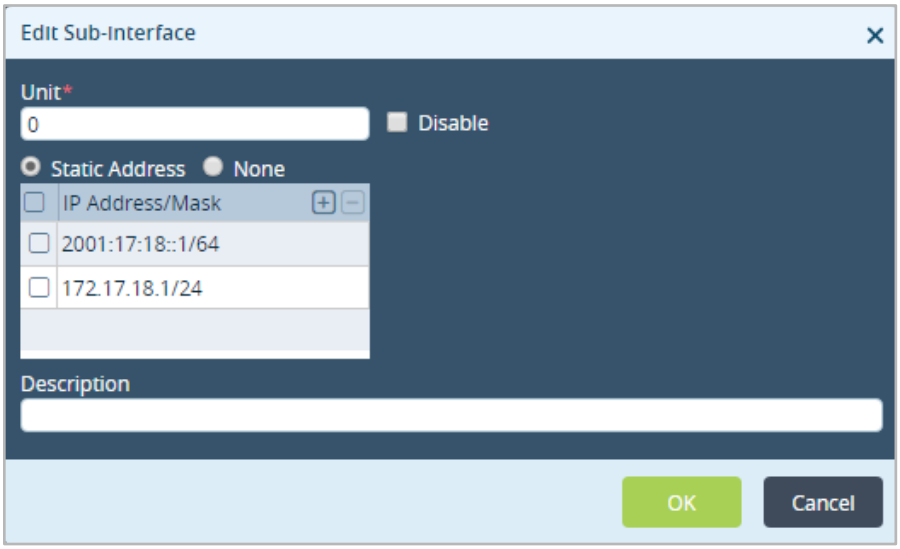
1. Under the *Appliance Context*, go to Configurations and select a controller/branch. In the Networking panel, click Interfaces > Tunnel tab.
2. Click on the top right corner to add a GRE tunnel and add the required parameters.



Field	Description
Interface	TVI interface port and slot numbers.
Disable	Indicates whether to not activate the tunnel interface after configuring it.
Description	Explanation for this interface—a string of a maximum of 255 characters.
MTU	Maximum transmission unit. The size in bytes of largest protocol data unit that the port can receive or transmit.

Mode	Mode of configuring the tunnel interface. There are two modes: ● *IPSec*. Select for IPsec configuration. ● *Redundancy*. Select for HA configuration.
Tunnel Type	There are multiple tunnel types: ● *Point-to-point GRE tunnel* ● *Ethernet over GRE* ● *Point-to-point IPv6 GRE tunnel*
Source	Source IP address.
Destination	Destination IP address.
Routing Instance	There are multiple routing instances.

3. Select an existing sub-interface and enter the required parameter values.

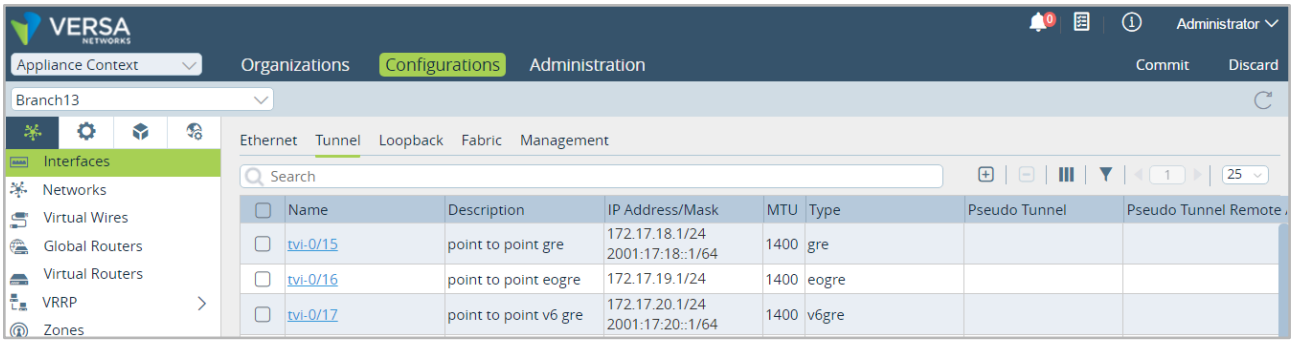


Field	**Description**
Unit	Unit number of the sub-interface. If the unit value is 0, VLAN ID is disabled. Else, enter the VLAN ID, which is the virtual LAN ID of the sub-interface.
Static Address	IP address and subnet mask of the sub-interface.

7. Click **OK** to complete editing the sub-interface.

8. Click **OK** on the **Add Tunnel Interface** screen.

This configures a GRE tunnel interface.



Next, configure loopback interfaces.

Configuring Loopback interfaces

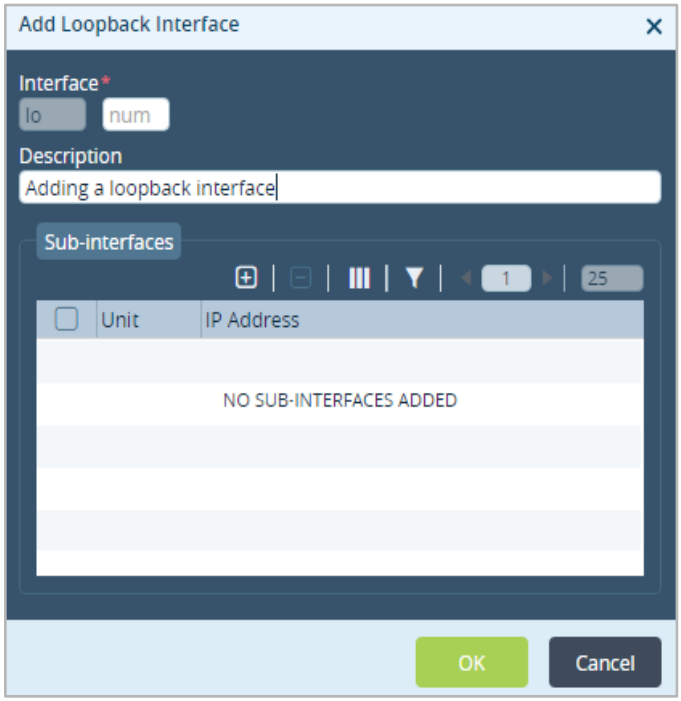
Loopback interface exists in routing instances that route heavy data traffic with high connectivity. Such interfaces are always up. In a routing instance or domain, there can only be one loopback interface.

Loopback interfaces are primarily used in the Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP) as the connectivity is never down. A loopback interface can be an interface without a standard IP address. However, the mask is always out of 32 and you cannot configure it.

For a service provider with two routers, there is a loopback interface in each of the routers and data connectivity maintains between the loopback interfaces.

Steps

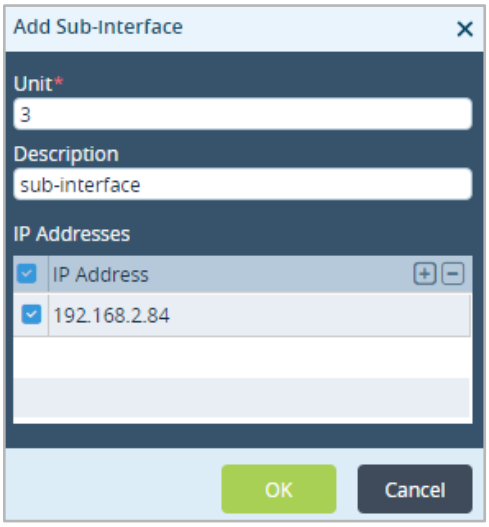
1. Under the *Appliance Context*, go to Configurations and select a controller. The Interfaces configuration screen displays in the Networking panel. Select the Loopback tab.
2. Click to add a loopback interface.
3. Add the required parameters.



Field	Description
Interface	Slot number for the loopback interface. You cannot edit the name of the loopback interface,

	which is ***Io*** (by default).
Description	Explanation for this interface—a string of a maximum of 255 characters.

a. Click ⊞ to add a sub-interface for the loopback interface and add the required parameters.

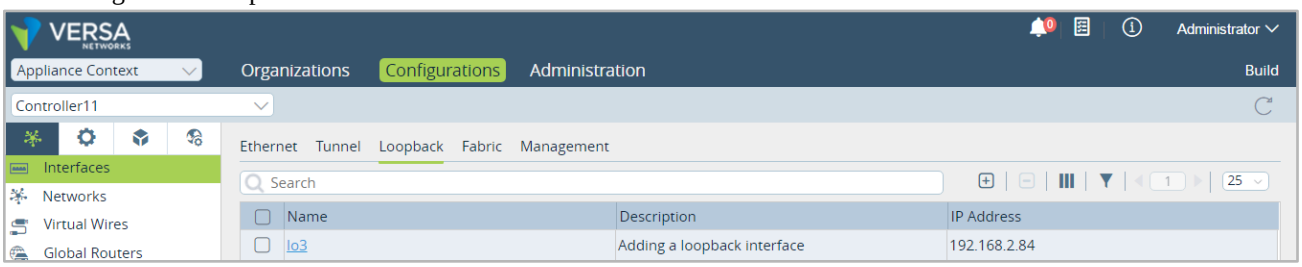


Field	Description
Unit	Sub-interface unit number.
Description	Explanation for this interface—a string of a maximum of 255 characters.

b. To add an IP address to the sub-interface, click ⊞, enter the IP address, and click **OK**. You can add multiple IP addresses to a sub-interface.

4. Click **OK** on the **Add Loopback Interface** screen.

This configures the loopback interface.

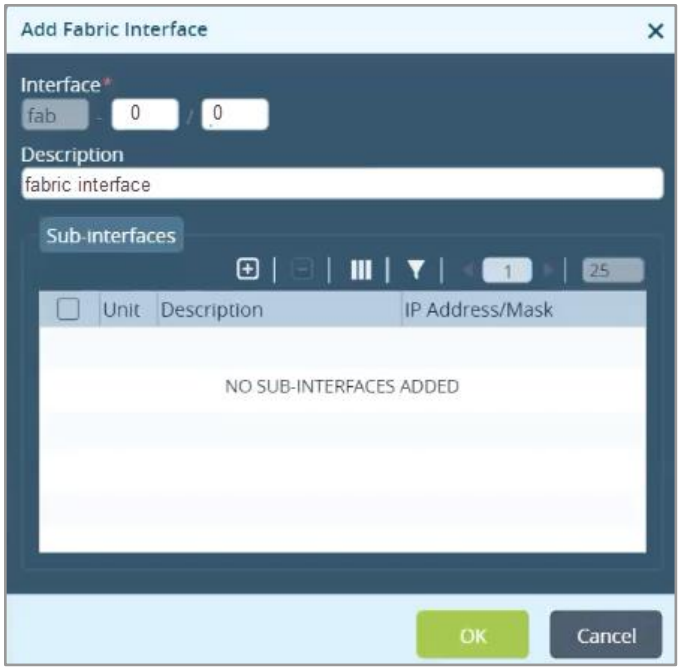


Configuring Fabric interfaces

Fabric interface is an internal bridge that allows traffic between two Virtual Machines (VM). If the traffic through a VM is significant, you can spawn another VM to ease the traffic flow.

Steps

1. Under the *Appliance Context*, go to Configurations and select a controller. The Interfaces configuration screen displays in the Networking panel. Select the Fabric tab.
2. Click ⊞ to add a fabric interface and enter the required parameters.



Field	Description
Interface	Slot and port numbers for the fabric interface. You cannot edit the name of the fabric interface, which is ***fab*** (by default).
Description	Description for the fabric interface.

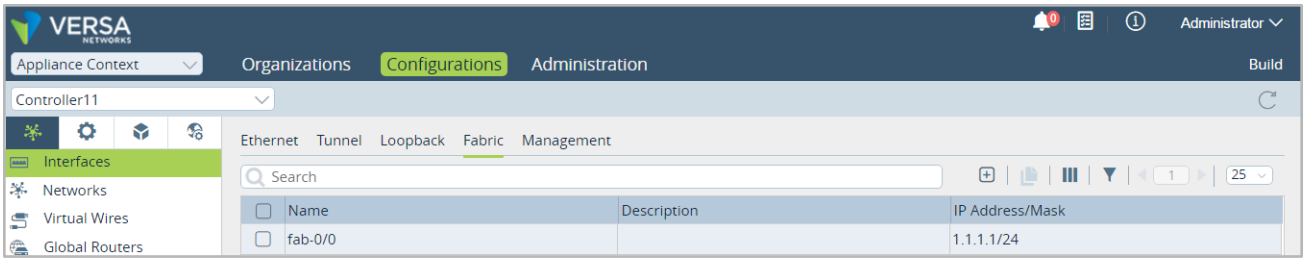
a. Click ⊞ to add a sub-interface for the fabric interface and add the required parameters.

Field	Description
Unit	Sub-interface unit number.
Description	Information about this interface.
IP Address/Mask	IP address and mask for the sub-interface.

b. Click **OK**.

3. Click **OK** on the **Add Fabric Interface** screen.

This configures the fabric interface.



Configuring Management interfaces

Management interface is a gateway to log in to a FlexVNF appliance by using the SSH protocol. By using this interface, you can log in, log out, make configuration changes in the box, and manage a device. However, management interface does not enable you to manage the data traffic. By default, every appliance has a management interface.

You can use the management IP address (public or private) to log in to a box. An appliance is connected to Versa Director through a management interface. A new appliance does not have any initial configuration apart from a management IP. Hence, you create an appliance on Versa Director, load the configuration in the appliance through CLI, and sync the appliance from Versa Director.

If the management port is connected to an Ethernet cable, ensure that it is secure by a firewall. Else, a user can SSH into the port using the regular user credentials.

Updating the Management interface using CLI

You cannot update the management interface directly. However, you can access the CLI for an appliance and update the parameter values. These values are auto-populated in the management interface when the appliance is synced with Versa Director.

Steps

1. Under the *Director Context*, go to Appliances.
2. Select a controller and click >_. This displays the CLI.

```
CLI
login as: admin
The authenticity of host '10.40.40.77 (10.40.40.77)' can't be established.
ECDSA key fingerprint is 9a:d5:5a:9e:e2:05:d6:57:18:bd:19:9b:5d:3f:c6:4c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.40.40.77' (ECDSA) to the list of known hosts.
admin@10.40.40.77's password:
```

3. Access the management interface through the CLI.

```
[error][2016-05-26 19:00:56]
admin@PoP2-Controller2-cli> configure
Entering configuration mode private
[ok][2016-05-26 19:00:59]

[edit]
admin@PoP2-Controller2-cli(config)% show interfaces
eth-0/0 {
    type external;
    mtu  1500;
    mac  00:50:56:b2:18:f5;
    unit 0 {
```

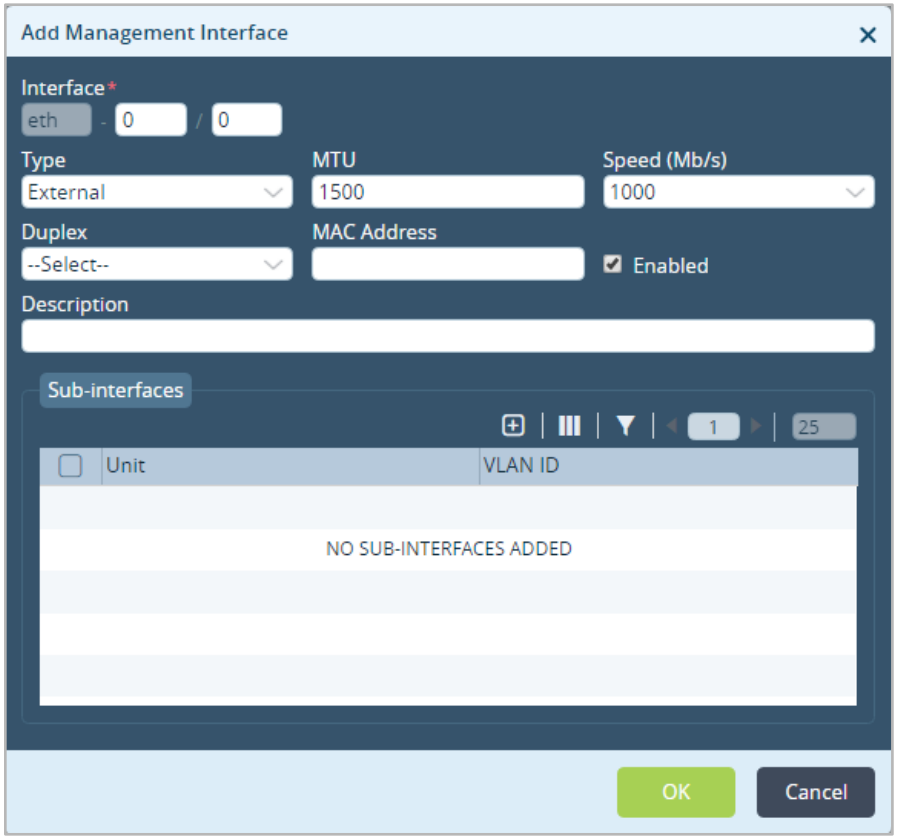
```
        family {
            inet {
               address 10.40.40.77 {
                    prefix-length 16;
                    gateway       10.40.0.1;
                }
            }
        }
    }
}
[ok][2016-05-26 19:01:18]

[edit]
admin@PoP2-Controller2-cli(config)%
```

You can now edit the management interface values through the CLI. Once the appliance syncs with Versa Director, the same information displays on the Edit Management Interface page.

Configuring Management interfaces using Versa Director

Steps

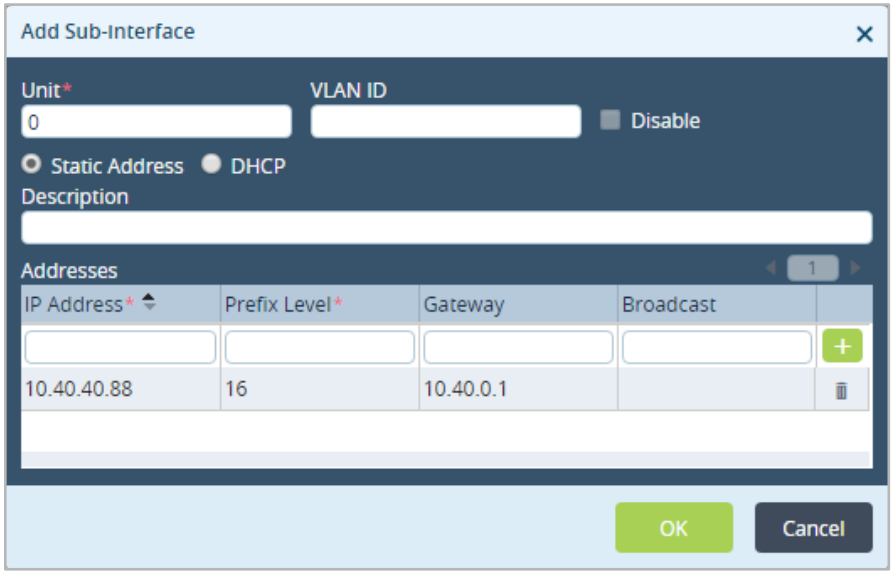
1. Under the *Appliance Context*, go to Configurations and select a controller. The Interfaces configuration screen displays in the Networking panel. Select the Management tab.
2. Click to add a management interface and enter the required parameters.



Field	Description
Interface	Ethernet port and slot numbers.
Type	Indicates whether the interface is external or internal.

MTU	Maximum transmission rate of packets in bytes/second.
Speed (Mb/s)	Speed of data transfer in megabits per second.
Duplex	Negotiation between the device interface and switch interface. Full-duplex data transmission means that data can be transmitted in both directions on a signal carrier at the same time.
MAC Address	MAC address of the interface.
Description	Explanation for this interface—a string of a maximum of 255 characters.
Unit	Indicates the unit number of the sub-interface.
VLAN ID	VLAN ID is the virtual LAN ID with a value of 0-4094 .
IP Address/Mask	Indicates the IP address and mask of the sub-interface.

3. Click ⊞ on the **Sub-Interfaces** section to add a sub-interface.

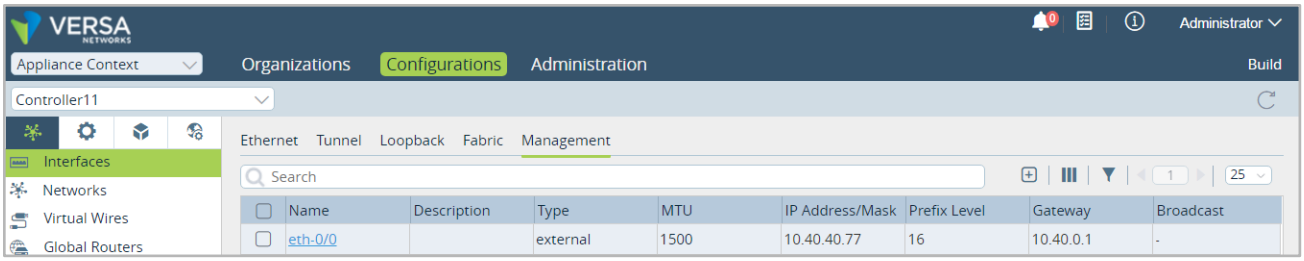


Field	Description
Unit	Indicates the unit number of the sub-interface.
VLAN ID	VLAN ID is the virtual LAN ID with a value of 0-4094.
IP Address/Mask	Indicates the IP address and mask of the sub-interface.
Prefix Level	Prefix to be used with the IP address.
Gateway	Gateway IP address.

Click + to add the IP address row.

4. Click **OK** to add the management interface.

This adds the management interface.



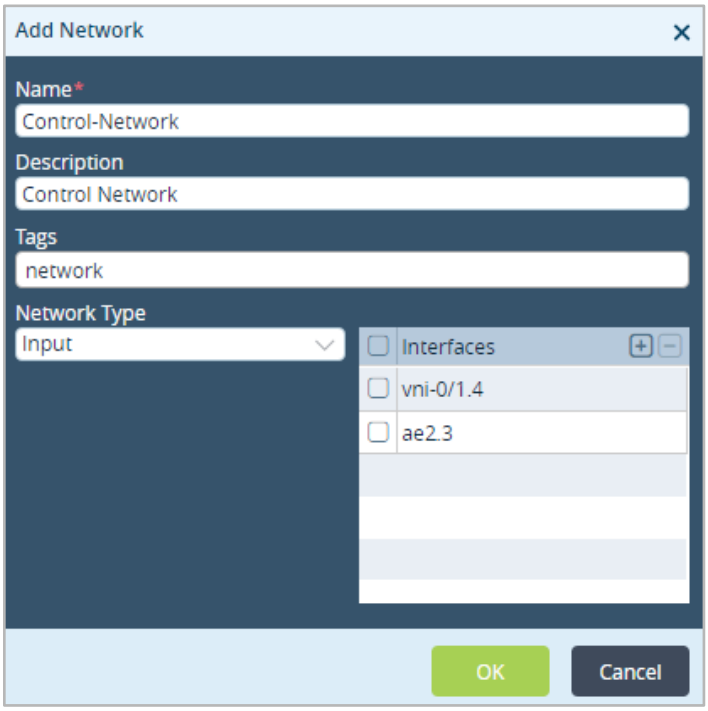
Next, configure networks.

Configuring networks

A network is a collection of similar interfaces that run on similar routing instances. To help manage multiple interfaces, you can create a network by combining such interfaces. For example, you can create a network with VNI interface that runs on the BGP routing protocol. One interface can be a part of only one network.

Steps

1. Under the *Appliance Context*, go to Configurations and select a controller. In the Networking tab , select Networks to display its configuration screen.
2. Click on the top right corner to add a network and enter the required parameters.



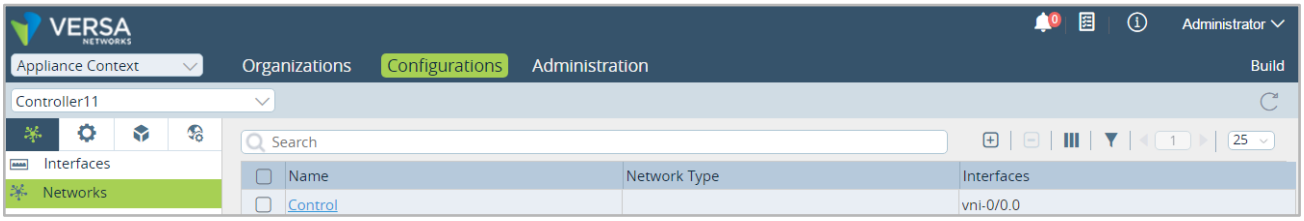
Field	Description
Name	Name for the network.
Description	Description for the network.
Tags	Tag to identify the network.
Network Type	Type of network: • *Input* • *Output*

a. Click ⊞ to add interfaces to the network. The system displays the pre-configured interfaces in the **Interfaces** drop-down list.

> ⚠ You can add only mutually exclusive interfaces. For example, you cannot create a network with *vni-0/1.4* and *ae2.5* interfaces, if *ae2*.5 already has *vni-0/1.4*.

3. Click **OK**.

This configures a network.



Next, configure virtual wires.

Configuring virtual wires

Virtual wire allows you to establish a connection between two interfaces that do not have any IP addresses. Virtual wire operates between physical interfaces at layer-2, similar to a switch or bridge. The interacting interfaces can contain sub-interfaces. Only Virtual Network Interface (vni) and Aggregated Ethernet (ae) interfaces are compatible with virtual wires.

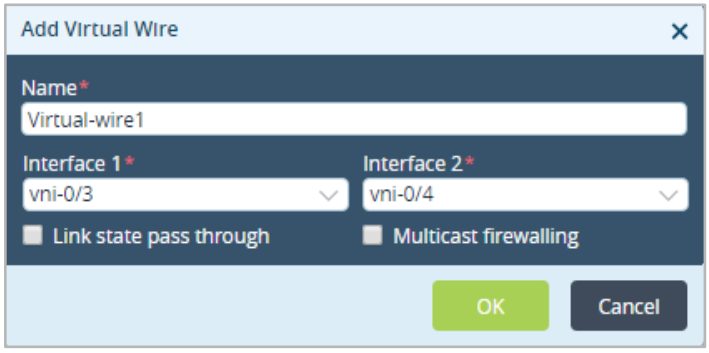
By configuring a virtual wire as a switch, you can send the traffic from one interface to another interface without any packet inspection.

You can create a virtual wire only if there are two similar interfaces (*vni* or *ae*) available. For example, you can use virtual wire between *vni-0/1* and *vni-0/2* or *ae-0/1* and *ae-0/2* and not *vni-0/1* and *ae-0/1*.

> ⚠ You cannot delete an interface that is used in a virtual wire. To delete such interfaces, you must first delete the virtual wire using them.

Steps

1. Under the *Appliance Context*, go to Configurations and select a controller. In the Networking panel, select Virtual Wires to open its configuration page.
2. Click ⊞ on the top right corner to add a virtual wire.



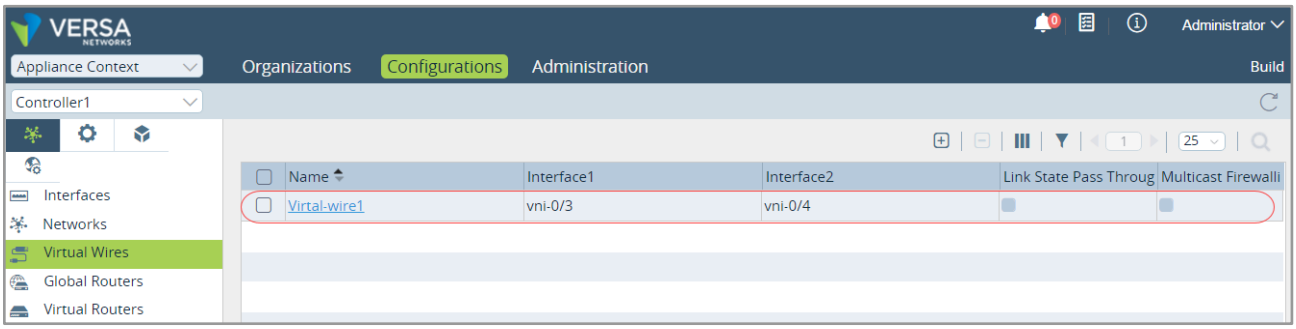
3. Add the required parameters.

Field	Description
Name	Name for the virtual wire.

Interface 1	Type of egress interface. The drop-down displays only the interfaces that you have configured as virtual wires.
Interface 2	Type of egress interface.
Link state pass through	Used to inform the second interface about the state of the first interface. For example, you can select this check box to inform the second interface that the first interface is down and so the traffic must be sent through an alternate route to the second interface.
Multicast firewalling	Currently not supported.

4. Click **OK**.

This configures the virtual wire interface.



Next, configure global routers.

Configuring global routers

The procedure to configure global routers is the same as followed for virtual routers (in the next topic). Under the *Appliance Context*, go to Configurations and select a controller. In the Networking tab , select Global Routers. Refer to *Configuring Virtual Routers* below for more information.

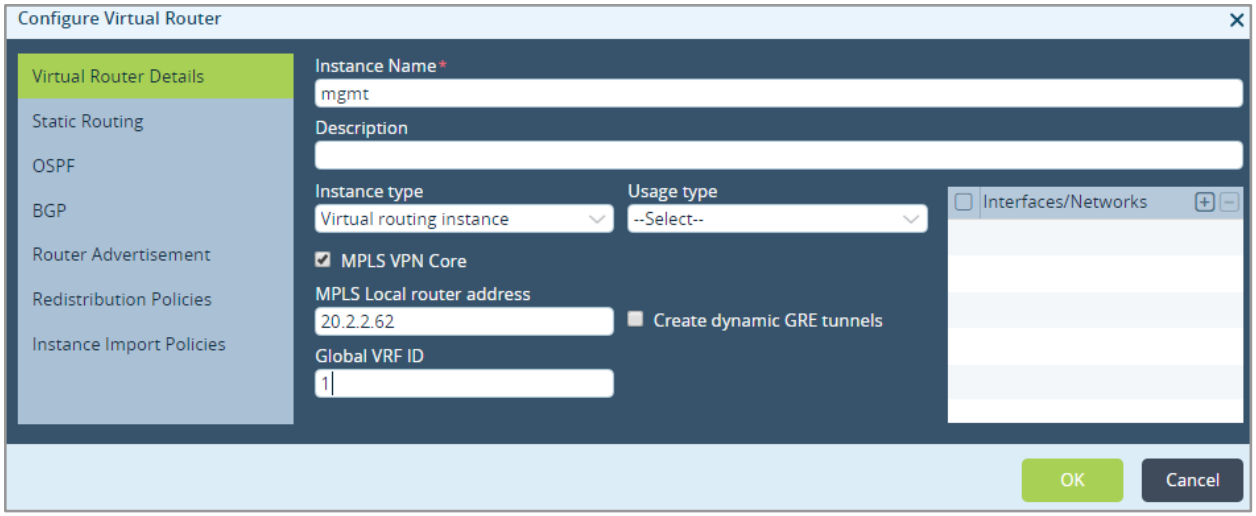
Configuring virtual routers

Virtual router is a software that replicates the functionality of a hardware-based Layer 3 Internet Protocol (IP) routing. A virtual router enables a computer to perform the functions of a full-fledged router. Only a single instance can be configured.

Setting up virtual router details

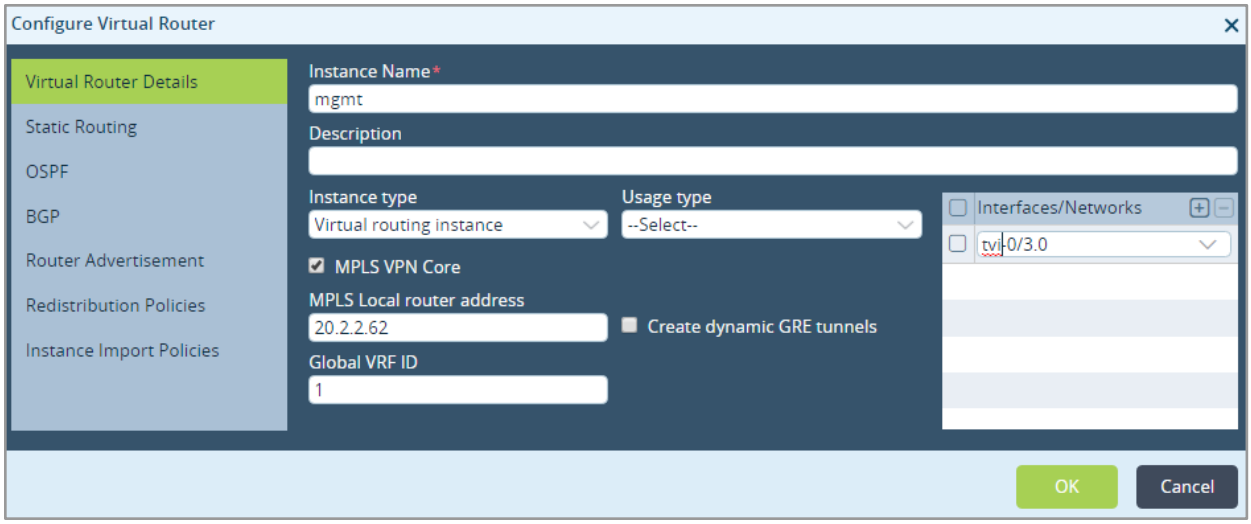
Steps

1. Under the *Appliance Context*, go to Configurations and select a controller. In the Networking tab , select Virtual Routers.
2. Click on the top right corner and enter the required parameters.



Field	Description
Instance Name	Each virtual router has a unique name.
Description	Information about the virtual router.
Instance Type	There are two instance types: • *Virtual Routing Instance***.** Select this when configuring a simple VPN. This is the basic instance type. • *Virtual* Routing Forwarding Instance. Select this when configuring a router for an L3VPN.
Usage Type	Usage type of a virtual router.
MPLS VPN Core	Multiprotocol label switching protocol (MPLS) VPN Indicates whether the virtual router is the core routing instance. This is applicable in a MPLS protocol.
MPLS Local Router Address	Router IP address or ID.
Create dynamic GRE tunnels	Indicates whether to create a Generic Routing Tunneling (GRE) protocol.
Global VRF ID	ID assigned to the global virtual router.
Interfaces/Networks	Interface assigned to the routing instance. There can be multiple interfaces or networks assigned to a routing instance.

3. Click ⊞ on the top right corner of the **Interfaces/Networks** section to select and add interfaces.



This configures the router details.

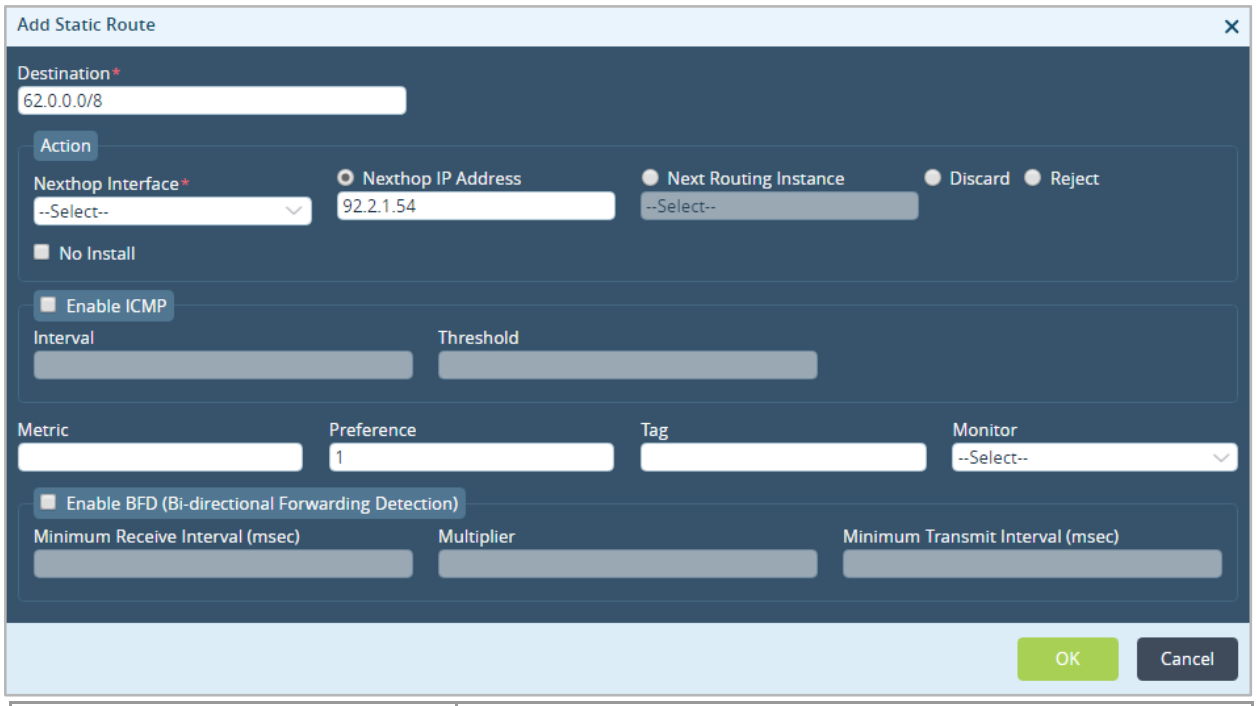
Next, set up static routing.

Setting up static routing

Static routing occurs when a router uses a manually-configured routing. Static routes do not change unlike dynamic routes.

Steps

1. Click Static Routing on the left panel of the Configure Virtual Router screen.
2. Click ⊞ on the top right corner and enter the required parameters in the **Add Static Route**.



Field	Description
Destination	Destination address or network.
Nexthop Interface	Interface to select when going to the destination network.

Nexthop IP Address	IP address of the next network.
Next Routing Instance	Indicates the next routing instance.
Discard	Indicates whether to discard the static route in the routing table.
Reject	Indicates whether to configure the static route and take no action.
No Install	Indicates whether to not install the route in the the routes table.
Enable ICMP	To enable the Internet Control Message Protocol (ICMP) protocol, select the **Enable ICMP** check box.
Interval	Indicates the interval for ICMP.
Threshold	Indicates the threshold for ICMP.
Metric	Cost to reach the destination network.
Preference	Preference of the static route. Each route can be assigned a preference.
Tag	Indicates the tag for the static route.
Monitor	Name of the liveness-detection monitor, which should be UP for the static route to become active.
Enable BFD (Bi-directional Forwarding Detection)	If the static route goes down, indicates whether to mark the link as down.
Minimum Receive Interval (msec)	The minimum time interval to receive routes.
Multiplier	Value used to calculate the final minimum receive interval and minimum transmit interval.
Minimum Transmit Interval (msec)	The time after which routes can be retransmitted.

3. Click **OK**.

This configures a static route.The next step is to set up an OSPF instance.

Setting up Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4.

Steps

1. Click OSPF on the left panel of the Configure Virtual Router screen.
2. Click ⊞ on the top right corner and enter the required parameters.